HITACHI
Inspire the Next

JP1 Version 11

JP1/Audit Management - Manager 構築・運用ガイド

解説・手引・操作書

3021-3-A17

前書き

■ 対象製品

P-2A42-7DB4 JP1/Audit Management - Manager 11-00（適用 OS：Windows Server 2008, Windows Server 2012）

注※　この製品は日本語環境だけで動作する製品です。

■ 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

■ 商標類

HITACHI，JP1 は，（株）日立製作所の商標または登録商標です。

AMD は，Advanced Micro Devices, Inc.の商標です。

IBM，AIX は，世界の多くの国で登録された International Business Machines Corporation の商標です。

IBM，AIX 5L は，世界の多くの国で登録された International Business Machines Corporation の商標です。

IBM，PowerHA は，世界の多くの国で登録された International Business Machines Corporation の商標です。

Intel Xeon は，アメリカ合衆国およびその他の国における Intel Corporation の商標です。

Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Itanium は，アメリカ合衆国およびその他の国における Intel Corporation の商標です。

Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

ODBC は，米国 Microsoft Corporation が提唱するデータベースアクセス機構です。

Oracle と Java は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です。

Red Hat は，米国およびその他の国で Red Hat, Inc. の登録商標もしくは商標です。

RSA および BSAFE は，米国 EMC コーポレーションの米国およびその他の国における商標または登録商標です。

SUSE は，米国およびその他の国における SUSE LLC の登録商標または商標です。

UNIX は，The Open Group の米国ならびに他の国における登録商標です。

VERITAS および VERITAS ロゴは，Symantec Corporation の米国およびその他の国における商標または登録商標です。

Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

その他記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

This product includes software developed by Andy Clark.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

JP1/Audit Management - Manager は，米国 EMC コーポレーションの RSA BSAFE(R)ソフトウェアを搭載しています。

■ マイクロソフト製品の表記について

このマニュアルでは，マイクロソフト製品の名称を次のように表記しています。

表記		製品名
Internet Explorer または Internet Explorer 8 以降		Windows(R) Internet Explorer(R) 8
		Windows(R) Internet Explorer(R) 9
		Windows(R) Internet Explorer(R) 10
		Windows(R) Internet Explorer(R) 11
Microsoft Internet Information Services または IIS		Microsoft(R) Internet Information Services 7.5
		Microsoft(R) Internet Information Services 8.0
		Microsoft(R) Internet Information Services 8.5
Windows Server 2008※	Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Server 2012※	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard

注※

OS による機能差がない場合，Windows Server 2012，Windows Server 2008 を総称して Windows と表記します。

■ 発行

2016 年 1 月　3021-3-A17

■ 著作権

All Rights Reserved. Copyright (C) 2016, Hitachi, Ltd.

All Rights Reserved. Copyright (C) 2016, Hitachi Solutions, Ltd.

はじめに

このマニュアルは，JP1/Audit Management - Manager を導入して内部統制の証跡記録を管理するシステムの，機能，システム構築方法，および運用方法について説明したものです。

以降，このマニュアルでは JP1/Audit Management - Manager を導入して構築するシステムを**監査証跡管理システム**と呼びます。

■ 対象読者

JP1/Audit Management - Manager を導入して，監査証跡管理システムを構築および運用する管理者の方や，監査証跡管理システムの監査ログ情報を基に，監査の報告用資料を作成する方を対象にしています。

なお，管理者の方が，次の知識をお持ちであることを前提にしています。

- Windows Server 2012 または Windows Server 2008 に関する基本的な知識
- 監査ログ収集対象サーバで使用する OS に関する基本的な知識
- データベースに関する基本的な知識
- JP1/Base に関する基本的な知識
- 連携する製品に関する基本的な知識
- 内部統制に関する基本的な知識

■ マニュアルの構成

このマニュアルは，次に示す編から構成されています。なお，このマニュアルは各 OS に共通のマニュアルです。

第 1 編　概要・機能編

監査証跡管理システムの目的，特長，代表的な運用例の紹介，および運用サイクルについて説明しています。また，監査証跡管理システムの機能およびシステム構成について説明しています。

第 2 編　設計・構築編

監査証跡管理システムの導入から運用開始までの検討項目と作業内容について説明しています。また，監査証跡管理システムの構築方法（各プログラムのインストールとセットアップ方法，データベースの構築方法，およびクラスタ環境でのシステム構築方法）について説明しています。

第 3 編　運用編

監査証跡管理システムを運用する上で必要な監査ログ管理画面の操作方法，監査ログの管理方法，システム構成変更，およびデータベースのメンテナンスについて説明しています。

第 4 編　リファレンス編

JP1/Audit Management - Manager が提供するコマンド，定義ファイル，および出力するメッセージについて説明しています。また，監査証跡管理システムの運用中にトラブルが発生した場合の対処方法について説明しています。

■ 読書手順

このマニュアルは，利用目的に合わせて章を選択して読むことができます。利用目的別にお読みいただくことをお勧めします。

利用目的	記述個所
監査証跡管理システムの概要について知りたい	1 章　概要
監査証跡管理システムの機能について知りたい	2 章　機能
監査証跡管理システムのシステム構成について知りたい	3 章　システム構成
監査証跡管理システムの導入から運用開始までの検討項目について知りたい	4 章　システム設計
監査証跡管理システムを構築したい	5 章　システム構築
	6 章　クラスタ環境でのシステム構築
監査証跡管理システムの運用方法を知りたい	7 章　監査ログ管理画面での運用
	8 章　監査ログのバックアップ運用
	9 章　監査ログ収集対象の確認と変更
	10 章　データベースのメンテナンス
監査ログ管理画面の各部の名称と使い方について知りたい	11 章　監査ログ管理画面
JP1/Audit Management - Manager で使用するコマンドについて知りたい	12 章　コマンド
JP1/Audit Management - Manager で使用する定義ファイルについて知りたい	13 章　定義ファイル
画面に出力されたメッセージの意味や，メッセージの対処方法を知りたい	14 章　メッセージ
トラブル発生時の対処方法を知りたい	15 章　トラブルシューティング

利用目的	記述個所
JP1/Audit Management - Manager で使用するファイルの一覧について知りたい	付録 A　ファイル一覧
JP1/Audit Management - Manager で使用するポート番号について知りたい	付録 B　ポート番号一覧
正規化ルールファイルの作成例について知りたい	付録 C　正規化ルールファイルの作成例
JP1/Audit Management - Manager の監査ログの出力情報について知りたい	付録 D　JP1/Audit Management - Manager の監査ログの出力情報
JP1/Audit Management - Manager が対応しているプログラムの監査ログについて知りたい	付録 E　JP1/Audit Management - Manager が対応するプログラムの監査ログ一覧
バージョンごとの変更内容について知りたい	付録 F　各バージョンの変更内容
このマニュアルを読むに当たっての参考情報について知りたい	付録 G　このマニュアルの参考情報
監査証跡管理システムで使用する用語について知りたい	付録 H　用語解説

■ このマニュアルで使用する記号

このマニュアルで使用する記号を，次のように定義します。

記号	意味
[　]	この記号で囲まれている項目は，ダイアログ，ボタン，メニュー，またはキーボードのキーであることを示します。
[　] ― [　]	メニューを連続して選択することを示します。 （例）［プログラム］ ― ［JP1_NETM_Audit］
「　」	画面中に表示されている項目を示します。
△	半角の空白を示します。
太字	太字で示している項目は，重要な用語または任意に指定する項目を示します。
↓	定義ファイルで使用する，改行コードを示します。

■ このマニュアルで使用する日時の表記

このマニュアルで使用する日時の表記を，次のように定義します。

記号	意味
YYYY-MM	年-月（YYYY：年，MM：月）を示します。

記号	意味
YYYY/MM/DD YYYY-MM-DD YYYYMMDD	年/月/日，年-月-日，または年月日（YYYY：年，MM：月，DD：日）を示します。
YYYY-MM-DD△hh:mm:ss	年-月-日 時:分:秒（YYYY：年，MM：月，DD：日，hh：時，mm：分，ss：秒）を示します。
YYYY/MM/DD△hh:mm:ss.ttt YYYY-MM-DD△hh:mm:ss.ttt YYYYMMDDhhmmss.ttt	年/月/日 時:分:秒.ミリ秒，年-月-日 時:分:秒.ミリ秒，または年月日時分秒.ミリ秒（YYYY：年，MM：月，DD：日，hh：時，mm：分，ss：秒，ttt：ミリ秒）を示します。

■ コマンドの文法で使用する記号

コマンドの説明で使用する記号を，次のように定義します。

記号	意味
[ ]	この記号で囲まれている項目は省略できることを示します。
{ }	この記号で囲まれている複数の項目のうちから一つを選択することを示します。 項目の区切りは｜で示します。 （例） {A ｜ B} A または B のどちらかを指定することを示します。
△	半角の空白を示します。
…	この記号の直前に示された項目を繰り返して複数個，指定できます。 （例）「A, …」は「A を必要個数指定する」ことを示します。
太字	太字で示している項目は，任意に指定する項目を示します。 （例 1） admdbexport△-o△**バックアップ先フォルダ**△[-y] （例 2） admdbexport△-o△**バックアップ先フォルダ**△[-y] 「admdbexport△-o△C:¥temp¥csvbackup」のように，**バックアップ先フォルダ**の部分には，任意のバックアップ先のフォルダパスを指定することを示します。

■ このマニュアルで使用する構文要素

このマニュアルで使用する構文要素（ユーザの指定値の範囲）の種類を，次のように定義します。

種類	定義
数字	0～9
英字	A～Z　a～z

種類	定義
英数字	A～Z　a～z　0～9
記号	！　"　#　$　%　&　'　(　)　*　+　,　-　.　/　： ；　<　=　>　@　[　]　^　_　{　}　?　¥　~ スペース

注　すべて半角で指定してください。

■ 図中で使用する記号

このマニュアルの図中で使用する記号を，次のように定義します。

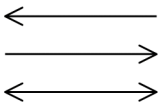
●コンピュータ

●サーバ

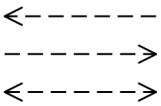
●ノートPC

●入出力の動作

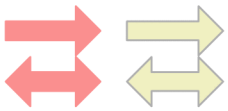
●作業の流れ



●制御の流れ

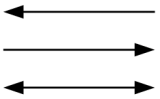


●データの流れ

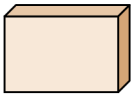


●工程，作業項目の流れ

●その他の流れ

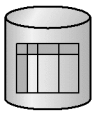


●プログラム

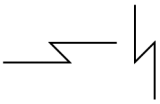


●データベース※ またはディスク

●リレーショナルデータベース

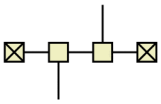


●通信回線

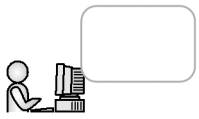


●ネットワーク

●バス形のLAN



●画面の表示



●ファイル

●管理者またはユーザ

●ソフトウェア

注※　データベースをDBと省略して表記することがあります。

■ フォルダパスの表記

このマニュアルでは，インストール先フォルダのパスを次のように表記しています。

製品名	インストール先フォルダの表記	デフォルトのインストール先フォルダ※
JP1/Audit Management - Manager	JP1/Audit Management - Manager のインストール先フォルダ	システムドライブ¥Program Files (x86)¥HITACHI¥jp1netmaudit¥manager

注※

製品をデフォルトのままインストールした場合のインストール先フォルダを示しています。

また，このマニュアルでは，仮想ディレクトリのパスを次のように表記しています。

製品名	仮想ディレクトリの表記	デフォルトの仮想ディレクトリ
JP1/Audit Management - Manager	JP1/Audit Management - Manager の仮想ディレクトリ	JP1/Audit Management - Manager のインストール先フォルダ¥wwwroot

目次

前書き　2
はじめに　6

第 1 編　概要・機能編

1　概要　23
1.1　監査証跡管理システムの目的　24
1.1.1　内部統制の評価や監査に有効な情報を収集します　24
1.1.2　証跡記録をバックアップします　25
1.1.3　証跡記録の管理業務の効率を向上し，管理コストを削減します　25
1.1.4　内部統制の監査を支援します　25
1.2　監査証跡管理システムの特長　26
1.2.1　内部統制の証跡記録の一元管理　26
1.2.2　監査目的に合わせた検索・集計　33
1.2.3　統計による事象推移の把握　34
1.2.4　監査ログのバックアップと閲覧専用サーバの構築　34
1.2.5　内部統制の報告用資料や監査用資料の作成支援　35
1.2.6　操作画面のカスタマイズ　36
1.3　代表的な運用方法の紹介　38
1.3.1　企業内の IT システムの運用実態について把握する　38
1.3.2　企業内の IT システムが正しく運用されているかどうかを確認する　41
1.3.3　監査ログを利用して報告用資料を作成する　43
1.3.4　監査ログのバックアップを自動的に取得する　45
1.3.5　バックアップの取得履歴を確認する　46
1.3.6　監査ログ閲覧サーバで監査ログを閲覧する　48
1.3.7　運用の変化に対応して監査ログの収集対象を追加・解除する　50
1.4　監査証跡管理システムを利用した内部統制の運用サイクル　51

2　機能　53
2.1　機能の概要　54
2.2　監査ログの収集　56
2.2.1　監査ログの収集の仕組み　56
2.2.2　監査ログの収集タイミング　61
2.2.3　監査ログの収集カテゴリ　63
2.2.4　監査ログの正規化　64

2.2.5 IPv6 環境での監査ログの収集 67
2.3 監査ログの一元管理 68
2.3.1 データベースマネージャを使用した管理 68
2.3.2 データベースのコマンドを使用した管理 70
2.3.3 監査ログのコマンドを使用した管理 71
2.4 JP1/Base のユーザ管理機能を使ったユーザ管理 75
2.4.1 ユーザ認証 75
2.4.2 アクセス制御 76
2.5 監査ログの検索と集計 77
2.5.1 監査ログの検索 77
2.5.2 監査ログの集計 78
2.6 監査ログの統計情報の生成と統計結果の出力 79
2.7 監査ログのバックアップ履歴管理 81
2.8 監査ログ管理画面のカスタマイズ 82
2.9 JP1/Audit Management - Manager の監査ログ出力 84

3 システム構成 85
3.1 プログラム構成 86
3.1.1 監査ログ管理サーバのプログラム構成 86
3.1.2 監査ログ閲覧サーバのプログラム構成 88
3.1.3 監査ログ収集対象サーバのプログラム構成 90
3.1.4 クライアントのプログラム構成 91
3.2 前提 OS および前提プログラム 93
3.2.1 前提 OS 93
3.2.2 前提プログラム 96
3.3 システム構成例 102
3.3.1 基本構成 102
3.3.2 監査ログ閲覧サーバを構築した構成 103
3.3.3 クラスタ環境での構成 104
3.3.4 IPv6 環境での構成 105
3.3.5 システム構成の注意事項 106

第 2 編 設計・構築編

4 システム設計 107
4.1 システム設計の流れ 108
4.2 監査ログの収集対象の検討 110
4.3 監査ログを正規化するための検討 112
4.3.1 正規化ルールで定義できる監査ログの条件 112
4.3.2 監査ログのフォーマットへの対応づけの検討 114

4.3.3 正規化ルールの定義方法を変更する場合の注意事項 115
4.4 運用方法の検討 116
4.4.1 監査ログの収集時期の決定 116
4.4.2 収集した監査ログの取り扱い方法 116
4.4.3 システムの運用方法（クラスタ環境への導入有無） 119
4.4.4 データベースの運用方法 119
4.4.5 ユーザ管理 121
4.5 システム構成の検討 122
4.6 容量の見積もり 125
4.6.1 メモリ所要量の見積もり 125
4.6.2 ディスク占有量の見積もり 127
4.6.3 データベース容量の見積もり 128

5 システム構築 132
5.1 システム構築の流れ 133
5.1.1 サーバの構築の流れ 133
5.1.2 クライアントの構築の流れ 135
5.2 監査ログ管理サーバのプログラムのインストール 136
5.2.1 Microsoft Internet Information Services をインストールする 136
5.2.2 JP1/Base をインストールする 136
5.2.3 EUR をインストールする 136
5.2.4 JP1/Audit Management - Manager を新規インストールする 137
5.2.5 JP1/Audit Management - Manager を上書きインストールする 142
5.2.6 JP1/Audit Management - Manager をアンインストールする 144
5.3 監査ログ収集対象サーバのプログラムのインストール 146
5.3.1 JP1/Base をインストールする 146
5.3.2 監査ログ収集対象プログラムをインストールする 146
5.4 監査ログ収集対象サーバのセットアップ 147
5.4.1 セットアップに必要なファイルをインストールする 148
5.4.2 JP1/Base のイベントサービスを設定する 151
5.4.3 JP1/Base のイベントログトラップ機能を設定する 165
5.4.4 ログファイルトラップ機能の設定を確認する 177
5.4.5 UNIX システムログの変換設定をする 178
5.4.6 監査ログ収集対象プログラムをセットアップする 181
5.5 監査ログ管理サーバのセットアップ 182
5.5.1 Microsoft Internet Information Services をセットアップする 182
5.5.2 services ファイルを確認する 185
5.5.3 JP1/Base のユーザ管理機能を設定する 185
5.5.4 JP1/Base の jevsend コマンドを実行する 186

5.5.5 JP1/Base の API 設定ファイル（api ファイル）を編集する 187
5.5.6 監査ログ管理サーバの環境設定をする 189
5.5.7 監査ログ管理サーバのデータベースをセットアップする 198
5.5.8 監査ログ管理サーバのデータベースをアップグレードする 203
5.6 監査ログ管理サーバで監査ログを収集するための設定 204
5.6.1 標準サポートしているプログラムを収集対象とするための準備をする 205
5.6.2 標準サポート外のプログラムを収集対象とするための準備をする 208
5.6.3 製品定義ファイルを設定する 212
5.6.4 JP1/Audit Management - Manager で監査ログの収集対象を設定する 215
5.6.5 監査ログを定期的に収集する 223
5.7 監査ログ管理サーバの開始・停止 226
5.7.1 監査ログ管理サーバを開始する 226
5.7.2 監査ログ管理サーバを停止する 226
5.8 監査ログ閲覧サーバのプログラムのインストール 228
5.9 監査ログ閲覧サーバのセットアップ 229
5.10 クライアントのプログラムのインストール 230
5.11 監査ログ管理画面を使うための Internet Explorer の設定 231
5.12 JP1/Audit Management - Manager のバージョンアップ 233
5.12.1 JP1/Audit Management - Manager のバージョンアップの流れ 233
5.12.2 JP1/Audit Management - Manager のバージョンアップの手順 233
5.13 監査ログ収集対象の解除 235
5.13.1 ファイルに出力される監査ログの収集をやめる 235
5.13.2 Windows イベントログに出力される監査ログの収集をやめる 236
5.13.3 UNIX システムログに出力される監査ログの収集をやめる 238
5.13.4 すべての監査ログの収集をやめる 238

6 クラスタ環境でのシステム構築 242
6.1 クラスタ環境でのシステム構築の流れ 243
6.2 監査ログ管理サーバのプログラムのインストール（クラスタ環境） 244
6.2.1 前提プログラムをインストールする（クラスタ環境） 244
6.2.2 JP1/Audit Management - Manager を新規インストールする（クラスタ環境） 244
6.2.3 JP1/Audit Management - Manager を上書きインストールする（クラスタ環境） 245
6.2.4 JP1/Audit Management - Manager をアンインストールする（クラスタ環境） 247
6.3 監査ログ管理サーバのセットアップ（クラスタ環境） 249
6.3.1 Microsoft Internet Information Services をセットアップする（クラスタ環境） 249
6.3.2 共有ディスクに引き継ぐ情報をコピーする 249
6.3.3 JP1/Base をセットアップする（クラスタ環境） 250
6.3.4 監査ログ管理サーバの環境設定をする（クラスタ環境） 250
6.3.5 監査ログ管理サーバのデータベースをセットアップする（クラスタ環境） 252

6.3.6 監査ログ管理サーバのデータベースをアップグレードする（クラスタ環境） 253
6.3.7 監査ログ管理サーバでリソースを作成する 254
6.4 監査ログ収集対象サーバのプログラムのインストール（クラスタ環境） 257
6.5 監査ログ収集対象サーバのセットアップ（クラスタ環境） 258
6.5.1 セットアップに必要なファイルをインストールする（クラスタ環境） 258
6.5.2 監査ログ収集対象サーバで JP1/Base をセットアップする（クラスタ環境） 258
6.5.3 JP1/Base のイベントサービスを設定する（クラスタ環境） 259
6.5.4 論理ホスト環境を設定する 260
6.5.5 監査ログ収集対象サーバでリソースを作成する 261
6.6 監査ログ管理サーバで監査ログを収集するための設定（クラスタ環境） 270
6.7 監査ログ管理サーバの開始・停止（クラスタ環境） 271
6.7.1 監査ログ管理サーバを開始する（クラスタ環境） 271
6.7.2 監査ログ管理サーバを停止する（クラスタ環境） 271
6.7.3 監査ログ管理サーバを開始または停止する場合の注意事項（クラスタ環境） 272
6.8 監査ログ収集対象サーバの開始・停止（クラスタ環境） 273
6.8.1 監査ログ収集対象サーバを開始する（クラスタ環境） 273
6.8.2 監査ログ収集対象サーバを停止する（クラスタ環境） 273
6.8.3 監査ログ収集対象サーバを開始または停止する場合の注意事項（クラスタ環境） 273
6.9 JP1/Audit Management - Manager のバージョンアップ（クラスタ環境） 274
6.9.1 JP1/Audit Management - Manager のバージョンアップの流れ（クラスタ環境） 274
6.9.2 JP1/Audit Management - Manager のバージョンアップの手順（クラスタ環境） 275
6.10 監査ログ収集対象の解除（クラスタ環境） 276
6.10.1 ファイルに出力される監査ログの収集をやめる 276
6.10.2 すべての監査ログの収集をやめる 276
6.11 フェールオーバー発生後の対処 280

第 3 編 運用編

7 監査ログ管理画面での運用 281
7.1 監査ログ管理画面での操作 282
7.1.1 監査ログ管理画面の操作の流れ 282
7.1.2 監査ログ管理機能 283
7.1.3 監査ログ管理画面の表示編集 285
7.2 監査ログ管理画面へのログインとログアウト 286
7.2.1 監査ログ管理画面にログインする 286
7.2.2 監査ログ管理画面からログアウトする 287
7.3 監査ログ検索 288
7.3.1 監査ログの検索 288
7.3.2 監査ログの検索条件項目 290

7.3.3 監査ログ検索結果の確認 294
7.3.4 監査ログ検索結果のレポート表示 299
7.3.5 監査ログ検索パターンの編集 303
7.4 監査ログ集計 307
7.4.1 監査ログの集計 307
7.4.2 監査ログの集計条件項目 309
7.4.3 監査ログ集計結果の確認 313
7.4.4 監査ログ集計結果のグラフ表示 318
7.4.5 監査ログ集計パターンの編集 320
7.5 監査ログ統計 324
7.5.1 監査ログの統計 324
7.5.2 監査ログの統計出力条件項目 325
7.5.3 監査ログ統計結果の確認 327
7.5.4 監査ログ統計パターンの設定 330
7.6 バックアップ履歴の確認 331
7.6.1 バックアップ履歴を検索する 331
7.6.2 バックアップ履歴の検索条件項目 331
7.6.3 バックアップ履歴検索結果の確認 333
7.6.4 バックアップファイルをダウンロードする 334
7.7 監査ログ管理画面の表示設定 335
7.7.1 監査ログ検索画面の表示項目を設定する 335
7.7.2 監査ログ集計画面の表示項目を設定する 337
7.7.3 監査ログ統計画面の表示項目を設定する 339
7.7.4 バックアップ履歴画面の表示項目を設定する 342
7.8 機能ツリーのパターン表示編集 345
7.8.1 パターンを保存するフォルダを作成する 346
7.8.2 パターン名やフォルダ名を変更する 347
7.8.3 パターンやフォルダを移動する 348
7.8.4 パターンやフォルダをコピーする 349
7.8.5 パターンやフォルダを削除する 351
7.8.6 パターンやフォルダの表示・非表示を設定する 351
7.8.7 パターンやフォルダの情報を移行する 352

8 監査ログのバックアップ運用 353
8.1 監査ログのバックアップ運用の流れ 354
8.2 監査ログのバックアップ 356
8.2.1 期間指定のバックアップ 356
8.2.2 差分指定のバックアップ 357
8.3 監査ログのバックアップファイルのインポート 359

8.4 監査ログのバックアップファイルの移動 360
8.5 監査ログのバックアップファイルの削除 362

9 監査ログ収集対象の確認と変更 363
9.1 システムの変更の概要 364
9.2 監査ログの収集対象の情報確認 365
9.3 監査ログの収集対象の設定変更 369
9.3.1 監査ログ収集対象を追加する 370
9.3.2 監査ログ収集対象を編集する 371
9.3.3 監査ログ収集対象を解除する 372
9.3.4 監査ログの監視を開始する 372
9.3.5 監査ログの監視を停止する 373
9.3.6 監査ログを定期的に収集する時刻や曜日を変更する 374
9.3.7 監査ログを即時に収集する 374
9.3.8 製品定義ファイルを作成して収集対象を追加する 375
9.3.9 作成した製品定義ファイルを編集する 375
9.3.10 作成した製品定義ファイルを削除する 376

10 データベースのメンテナンス 377
10.1 データベースのメンテナンスの概要 378
10.1.1 データベースマネージャの起動方法 378
10.1.2 データベースの再セットアップ 379
10.1.3 データベースのバックアップ 380
10.1.4 データベースのリストア 382
10.1.5 データベースの再編成 384
10.1.6 データベースのパスワード変更 385
10.1.7 データベースの CSV バックアップ 387
10.1.8 データベースの CSV リストア 388
10.1.9 データベースのデータ移行 390
10.1.10 データベースのデータ削除 391
10.2 データベースのディスク容量の管理 392
10.2.1 データベースの使用状況に応じて対処する 392

第 4 編 リファレンス編

11 監査ログ管理画面 395
11.1 監査ログ管理画面の各部の名称と使い方 396
11.2 機能ツリー 398
11.2.1 機能ツリーのツリー項目 398
11.2.2 機能ツリーのアイコンの動作 401

11.3 監査ログ検索画面　403
11.4 監査ログ集計画面　407
11.5 監査ログ統計画面　410
11.6 バックアップ履歴画面　412
11.7 表示設定画面　414
11.7.1 監査ログ検索画面・監査ログ集計画面・バックアップ履歴画面の表示項目の設定　414
11.7.2 監査ログ統計画面の表示項目の設定と統計パターンの設定　416
11.8 監査ログレポート画面　418
11.9 集計結果グラフ表示画面　419
11.10 パターン表示編集画面　420
11.11 パターン保存画面　425
11.12 検索パターンおよび集計パターンの一覧　426
11.12.1 テンプレートとして登録されている検索パターンおよび集計パターン一覧　426

12 コマンド　444
コマンド一覧　445
コマンドの詳細　447
admagtinstall（監査ログ収集対象サーバのファイルのインストール）　448
admagtsetup（監査ログ専用イベントサーバの環境セットアップ）　451
admcoldata（監査ログの収集）　457
admcsvmove（監査ログのバックアップファイルの移動）　459
admcsvremove（監査ログのバックアップファイルの削除）　461
admdbbackup（データベースのバックアップ）　463
admdbdelete（データベースのデータ削除）　465
admdbexport（データベースの CSV バックアップ）　468
admdbimport（データベースの CSV リストア）　470
admdbrorg（データベースの再編成）　473
admdbstat（データベースの使用状況確認）　475
admdbstop（データベースの停止）　477
admexport（監査ログのバックアップ）　479
admhasetup（論理ホスト環境の作成）　484
admimport（監査ログのインポート）　487
admlog.vbs（障害発生時の保守資料採取）　490
admrrexport（正規化ルールのバックアップ）　492
admrrimport（正規化ルールのインポート）　494
admstdel（監査ログの統計情報削除）　497
admstgen（監査ログの統計情報生成）　499
admuxlogcol（UNIX システムログ情報の変換）　501

13 定義ファイル　504
13.1 定義ファイル一覧　505
13.2 正規化ルールファイル　506
13.2.1 ファイル名および格納先　506

13.2.2 書式 508
13.2.3 定義内容（標準サポート外のプログラムを収集する場合） 508
13.2.4 定義内容（標準サポート外の Windows イベントログを収集する場合） 520
13.2.5 指定例 525
13.2.6 注意事項 525
13.3 製品定義ファイル 527
13.3.1 ファイル名および格納先 527
13.3.2 書式 529
13.3.3 定義内容 529
13.3.4 指定例 530
13.4 動作定義ファイル 531
13.4.1 ファイル名および格納先 531
13.5 監査ログ標準レポート定義ファイル 534
13.5.1 ファイル名および格納先 534
13.5.2 書式 534
13.5.3 定義内容 534
13.5.4 指定例 535
13.6 監査ログレポート定義ファイル 536
13.6.1 ファイル名および格納先 536
13.6.2 書式 536
13.6.3 定義内容 536
13.6.4 指定例 537
13.6.5 監査ログレポート画面の表示例 537
13.7 バックアップオプション定義ファイル 539
13.7.1 ファイル名および格納先 539
13.7.2 書式 539
13.7.3 定義内容 539
13.7.4 指定例 540
13.8 パターン情報ファイル 541
13.8.1 ファイル名および格納先 541
13.8.2 書式 541
13.8.3 定義内容 541
13.8.4 指定例 546
13.9 監査ログ収集対象サーバセットアップ定義ファイル 547
13.9.1 ファイル名および格納先 547
13.9.2 書式 547
13.9.3 定義内容 548
13.9.4 指定例 551

14 メッセージ 552
14.1 メッセージの形式 553
14.1.1 メッセージの出力形式 553
14.1.2 メッセージの記載形式 553
14.2 メッセージの出力先一覧 555
14.2.1 KDSO0001-I～KDSO2477-W のメッセージの出力先 555
14.2.2 KDSO3001-E～KDSO3853-E のメッセージの出力先 566
14.2.3 KDSP0001-I～KDSP2903-E のメッセージの出力先 572
14.3 メッセージ一覧 576

15 トラブルシューティング 799
15.1 トラブル発生時の対処手順 800
15.2 トラブル発生時に採取が必要な資料 801
15.2.1 トラブル発生時に一括採取する資料 801
15.2.2 トラブル発生時に個別採取する資料 801
15.2.3 そのほかに採取する資料 802
15.3 トラブルへの対処方法 803
15.3.1 監査ログ管理画面でのトラブル 803
15.3.2 データベースのトラブル 805
15.3.3 監査ログの監視および収集のトラブル 806
15.3.4 監査ログの正規化でのトラブル 808
15.3.5 インストールでのトラブル 809
15.4 監査ログ管理サーバのバックアップおよびリストア 810
15.4.1 JP1/Audit Management - Manager のバックアップ 810
15.4.2 JP1/Audit Management - Manager のリストア 810

付録 812
付録 A ファイル一覧 813
付録 A.1 JP1/Audit Management - Manager のファイル一覧 813
付録 A.2 JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧 820
付録 A.3 監査ログ収集対象サーバに配布されるファイル一覧 823
付録 B ポート番号一覧 827
付録 B.1 JP1/Audit Management - Manager のポート番号 827
付録 B.2 JP1/Audit Management - Manager で使用するポート番号の変更方法 828
付録 B.3 ファイアウォールの通過方向 829
付録 C 正規化ルールファイルの作成例 830
付録 C.1 TYPE が KEY の場合 830
付録 C.2 TYPE が VALUE の場合 833
付録 C.3 TYPE が WINEVENT の場合 835

付録 D　JP1/Audit Management - Manager の監査ログの出力情報　840
付録 D.1　監査ログに出力される事象の種別　840
付録 D.2　監査ログの保存形式　842
付録 D.3　監査ログの出力形式　843
付録 D.4　監査ログを出力するための設定　847
付録 E　JP1/Audit Management - Manager が対応するプログラムの監査ログ一覧　848
付録 E.1　Hitachi Storage Command Suite の監査ログ出力情報　854
付録 E.2　JP1/AJS2 および JP1/AJS3 の監査ログ（スケジューラログ）出力情報　856
付録 E.3　Oracle の監査ログ出力情報　870
付録 E.4　UNIX システムログの監査ログ出力情報　871
付録 E.5　Windows イベントログ（セキュリティに関する情報）の監査ログ出力情報（Windows Server 2003 および Windows XP の場合）　873
付録 E.6　Windows イベントログ（セキュリティに関する情報）の監査ログ出力情報（Windows Server 2012 または Windows Server 2008 の場合）　877
付録 F　各バージョンの変更内容　882
付録 F.1　11-00 の変更内容　882
付録 F.2　10-10 の変更内容　883
付録 F.3　10-00 の変更内容　885
付録 F.4　09-50 の変更内容　886
付録 F.5　09-10 の変更内容　886
付録 F.6　09-00 の変更内容　887
付録 F.7　08-51 の変更内容　889
付録 F.8　08-50 の変更内容　890
付録 F.9　08-11 の変更内容　892
付録 G　このマニュアルの参考情報　896
付録 G.1　関連マニュアル　896
付録 G.2　このマニュアルでの表記　896
付録 G.3　このマニュアルで使用する英略語　900
付録 G.4　KB（キロバイト）などの単位表記について　901
付録 H　用語解説　902

索引　909

1 概要

JP1/Audit Management - Manager は，企業内の IT システムの証跡記録を管理し，内部統制の評価や監査を支援するプログラムです。証跡記録を収集・一元管理し，長期間にわたる保存を実現する機能を提供します。なお，この JP1/Audit Management - Manager を導入して構築するシステムを**監査証跡管理システム**と呼びます。

この章では，監査証跡管理システムの目的，特長，代表的な運用例の紹介，および運用サイクルについて説明します。

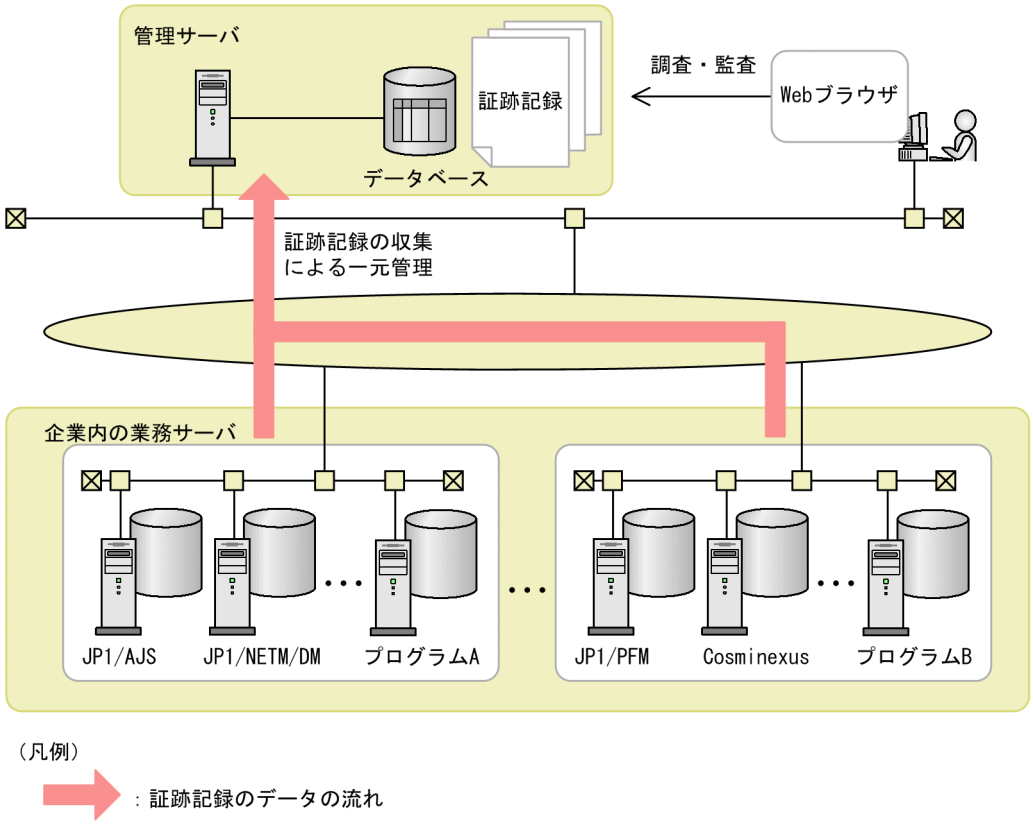
1.1　監査証跡管理システムの目的

企業内での IT システムの活用が必要不可欠となっている近年，IT システムの多様化や複雑化を悪用した違法行為や不正などの不祥事が，企業の信頼性に大きな損害を与えています。今後，企業にとって内部統制強化への取り組みが重要な課題となってきます。

JP1/Audit Management - Manager を導入して構築した**監査証跡管理システム**では，企業内の内部統制が規則どおりに機能していることを証明するために必要な証跡記録を収集し，一元管理します。さらに，内部統制の監査や IT システム運用の実態調査などのために，一元管理している証跡記録を保存できます。ユーザ情報やシステム構成の変更などの証跡記録を利用して業務の正当性を確認したり，リソースへの操作やアクセス状況を監査したりできます。

監査証跡管理システムの概要を次の図に示します。

図 1-1　監査証跡管理システムの概要



1.1.1　内部統制の評価や監査に有効な情報を収集します

監査証跡管理システムでは，企業内の各業務サーバから，内部統制の評価・監査を行う場合に役立つ証跡記録を自動的に収集し，一元管理します。

従来は，IT システムが出力する操作ログや変更履歴など，いろいろな形式の情報を証跡記録として個々に収集する必要がありましたが，監査証跡管理システムを導入することによって，多種・多様な証跡記録を

自動的に収集できるようになります。この証跡記録を基に，IT システムの運用実態を調査・検証することで，内部統制が正しく機能していることを証明したり，内部統制の強化対策を検討したりできます。

1.1.2 証跡記録をバックアップします

監査証跡管理システムでは，証跡記録を保存するためのバックアップ機能を提供します。さらに，いつからいつまでの証跡記録を保存したかというバックアップ実行履歴も管理できます。参照したい過去の証跡記録が，どのバックアップファイルに保存されているかを，証跡記録の発生期間の情報から調べることができます。

1.1.3 証跡記録の管理業務の効率を向上し，管理コストを削減します

監査証跡管理システムでは，証跡記録をデータベースで一元管理することによって，証跡記録の管理業務の効率向上および管理コストの削減を実現します。

従来は，形式の異なる証跡記録を別々に管理する必要がありましたが，監査証跡管理システムを導入することによって，形式の異なる証跡記録でも同一の形式で一元管理できるようになります。これによって，証跡記録を操作画面で一括して確認したり，CSV 形式ファイルや PDF ファイルに出力して管理できるようになるため，証跡記録の管理や内部統制の監査に掛かる時間を削減できます。

1.1.4 内部統制の監査を支援します

監査証跡管理システムは，Web ブラウザから表示する操作画面を使用して，監査証跡の情報を管理します。このため，監査証跡管理システムに Web ブラウザでアクセスができる環境であれば，どこからでも JP1/Audit Management - Manager にログインして監査証跡の情報を管理できます。

また，内部統制の監査者も，従来は証跡記録の書類や報告書を確認する必要があった監査業務が，Web ブラウザを使用して監査証跡の情報を閲覧して確認できるようになります。

1.2　監査証跡管理システムの特長

監査証跡管理システムの特長を次に示します。

- 内部統制の証跡記録の一元管理
- 監査目的に合わせた検索・集計
- 統計による事象推移の把握
- 監査ログのバックアップと閲覧専用サーバの構築
- 内部統制の報告用資料や監査用資料の作成支援
- 操作画面のカスタマイズ

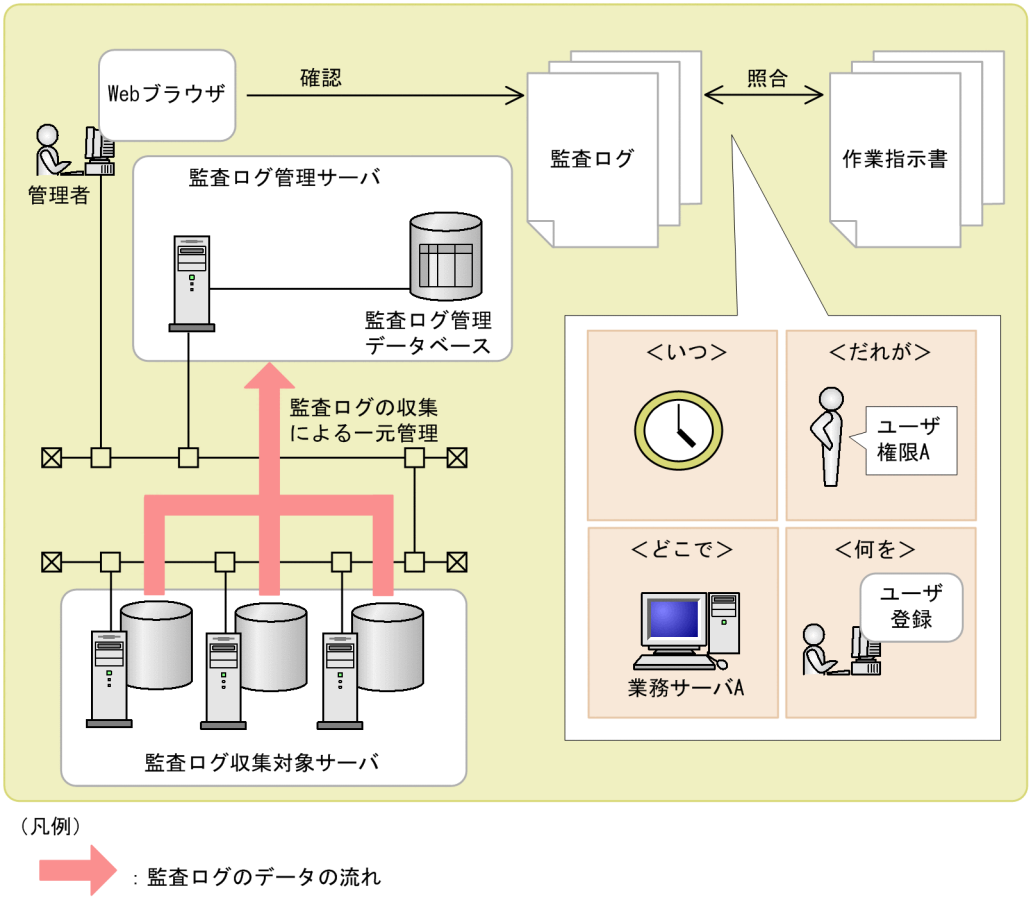
1.2.1　内部統制の証跡記録の一元管理

監査証跡管理システムでは，企業内に分散している業務サーバが出力する内部統制の証跡記録を収集し，一元管理します。この内部統制の証跡記録として出力されるログのことを**監査ログ**と呼びます。監査ログを収集する対象サーバを**監査ログ収集対象サーバ**，監査ログ収集対象サーバから監査ログを収集して管理するサーバを**監査ログ管理サーバ**，と呼びます。また，収集した監査ログを一元管理するデータベースを**監査ログ管理データベース**と呼びます。なお，この監査ログのことを，製品によっては操作ログや動作ログなどの別の名称で呼ぶこともあります。

一元管理されている監査ログと，業務規則書や作業指示書などのさまざまな資料とを照合することで，「いつ」「だれが」「どこで」「何を」したかといった内部統制の評価や監査に有効な情報を確認できます。

監査ログの一元管理の概要を次の図に示します。

図 1-2　監査ログの一元管理



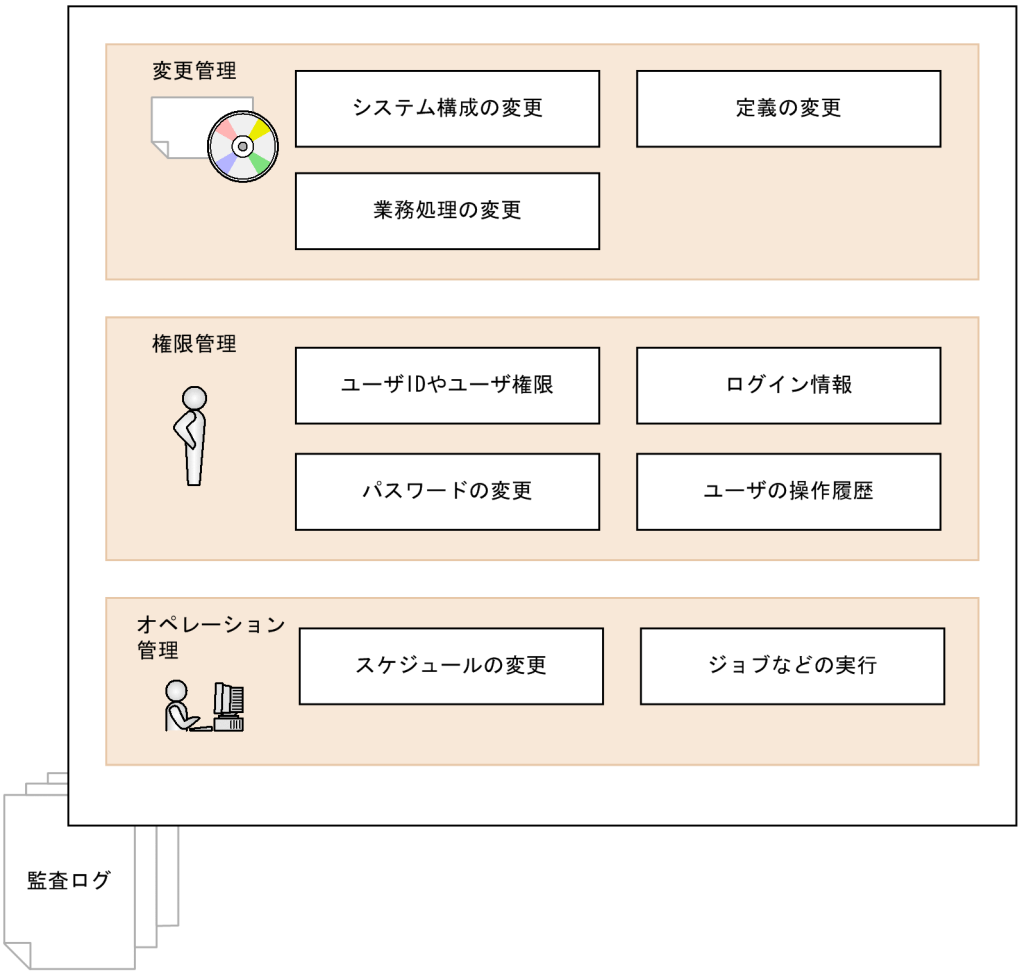
例えば，監査ログ収集対象サーバに対して行われた操作の情報を監査ログとして収集し，企業内の規則どおりに業務が実施されたかどうか，業務規則書や作業指示書などの資料と照合して確認できます。

(1)　監査証跡管理システムで管理できる情報の種類

監査証跡管理システムで管理できる情報には，大きく分けて変更管理に関する情報，権限管理に関する情報，およびオペレーション管理に関する情報があります。

監査証跡管理システムで管理できる情報を次の図に示します。

図 1-3　監査証跡管理システムで管理できる情報



変更管理

システム構成，業務処理，および製品の各定義についての変更内容や変更履歴を確認するための監査ログを管理します。

変更管理に関する情報には，JP1/AJS が出力するジョブネットの登録や各システムが出力する環境設定や定義ファイルの変更などが該当します。

権限管理

ユーザ情報の更新，パスワードの変更，システムへのログイン・ログアウト，および高いユーザ権限を持つユーザの操作についての状況を確認するための監査ログを管理します。

権限管理に関する情報には，JP1/Base が出力する JP1 ユーザの登録・削除の操作や各システムが出力するログイン・ログアウトなどが該当します。

オペレーション管理

スケジュールの変更やジョブの実行についての操作履歴を確認するための監査ログを管理します。

オペレーション管理に関する情報には，JP1/AJS が出力するジョブネットの再実行やカレンダーの変更などが該当します。

(2) 監査証跡管理システムで収集できるプログラムの種類

監査証跡管理システムでは，次の表に示すプログラムおよび OS が出力する監査ログを収集できます。

表 1-1 監査証跡管理システムの収集対象プログラム

項番	分類	名称
1	プログラム	Collaboration
2		Cosminexus
3		HiRDB
4		Hitachi Navigation Platform
5		Hitachi Storage Command Suite
6		JP1/AJS2
7		JP1/AJS3
8		JP1/AO
9		JP1/Audit
10		JP1/Base
11		JP1/IM - NP
12		JP1/IM - SS
13		JP1/ITDM
14		JP1/ITDM2
15		JP1/ITRM
16		JP1/NETM/AIM
17		JP1/NETM/CSC
18		JP1/NETM/DM
19		JP1/NETM/NM
20		JP1/PFM
21		JP1/秘文
22		OpenTP1
23		Oracle
24		TRUST E2
25		uCosminexus EUR Server
26		uCosminexus Navigation Platform
27		uCosminexus Portal Framework

項番	分類	名称
28		XDM/BASE E2
29		活文 NAVIstaff
30	OS	UNIX システムログ
31		Windows イベントログ

各収集対象プログラムが出力する監査ログ情報を次に示します。

Collaboration

ユーザによる各種操作の記録など，Collaboration の監査ログを収集できます。

Cosminexus

サーバプロセスの起動・停止やプロセスへの通信・共有メモリへのアクセス状況に関する情報など，Cosminexus の監査ログを収集できます。

uCosminexus Application Server Enterprise，uCosminexus Application Server Standard，uCosminexus Client，uCosminexus Service Platform，および uCosminexus Web Redirector に対応しています。

HiRDB

どのユーザがどのような権限を使用してどのような操作を行ったかなど，HiRDB の監査ログを収集できます。

Hitachi Navigation Platform

ログインや業務手順の実行に関する情報など，Hitachi Navigation Platform の監査ログを収集できます。

Hitachi Storage Command Suite

ユーザの作成やログインの結果に関する情報など，Hitachi Storage Command Suite の監査ログを収集できます。

Hitachi Storage Command Suite および Hitachi Command Suite に対応しています。

JP1/AJS2

ジョブネットの登録・変更やスケジューラサービスの開始・終了に関する情報など，JP1/AJS2 のスケジューラログを監査ログとして収集できます。

JP1/AJS3

ジョブネットの登録・変更やスケジューラサービスの開始・終了に関する情報など，JP1/AJS3 のスケジューラログを監査ログとして収集できます。

JP1/AO

ログイン認証やシステム管理の更新操作，構成管理情報の更新操作に関する情報など，JP1/AO の監査ログを収集できます。

JP1/Audit

監査ログ収集対象の追加・変更・削除や監査ログ管理データへのアクセスに関する情報など，JP1/Auditの監査ログを収集できます。

JP1/Audit Management - Manager およびバージョンが 09-50 以前の JP1/NETM/Audit - Manager に対応しています。

JP1/Base

認証サーバの起動・停止や JP1 ユーザの登録・削除の操作に関する情報など，JP1/Base の操作ログを監査ログとして収集できます。

JP1/IM - NP

ログインや業務手順の実行に関する情報など，JP1/IM - NP の監査ログを収集できます。

JP1/IM - SS

案件の作成・編集・削除やエスカレーション，案件操作履歴に関する情報など，JP1/IM - SS の監査ログを収集できます。

JP1/IM - SS および JP1/SS に対応しています。

JP1/ITDM

ログインやセットアップ，セキュリティポリシーの更新に関する情報など，JP1/ITDM の監査ログを収集できます。

JP1/ITDM2

ログインやセットアップ，セキュリティポリシーの更新に関する情報など，JP1/ITDM2 の監査ログを収集できます。

JP1/ITRM

ログインやサービスの起動に関する情報など，JP1/ITRM の監査ログを収集できます。

JP1/NETM/AIM

ログインやセットアップ，AIM 資産管理情報への更新操作に関する情報など，JP1/NETM/AIM の監査ログを収集できます。

JP1/NETM/CSC

セキュリティポリシーの設定や判定・アクションの結果に関する情報など，JP1/NETM/CSC の監査ログを収集できます。

JP1/NETM/CSC - Agent，JP1/NETM/CSC - Manager，および JP1/NETM/CSC - Manager Remote Option に対応しています。

JP1/NETM/DM

JP1/NETM/DM Manager のサービス（Remote Install Server）の起動・停止や GUI を持つプログラムの起動・停止に関する情報など，JP1/NETM/DM の監査ログを収集できます。

JP1/NETM/DM Manager，JP1/NETM/DM Client，および JP1/NETM/DM Client - Base に対応しています。

JP1/NETM/NM

ログイン，許可機器一覧，および固定機器一覧の編集に関する情報など，JP1/NETM/NM の監査ログを収集できます。

JP1/PFM

しきい値オーバーや通信の異常を知らせるアラーム発生やアラーム・アクション定義の作成・更新に関する情報など，JP1/PFM の動作ログを監査ログとして収集できます。

JP1/PFM - Manager，JP1/PFM - Base に対応しています。

JP1/秘文

管理サーバやファイルサーバで管理者が実行した操作に関する情報など，JP1/秘文の監査ログを収集できます。

JP1/秘文 Advanced Edition サーバに対応しています。

OpenTP1

トランザクションの開始・停止やクライアントのユーザ認証に関する情報など，OpenTP1 の監査ログを収集できます。

Oracle

Windows イベントログに出力される Oracle の監査ログのうち，ユーザの作成や権限の作成に関する情報を監査ログとして収集できます。

TRUST E2

VOS3 システムの利用開始・終了やアクセスの失敗に関する情報など，TRUST E2 の監査ログを収集できます。

uCosminexus EUR Server

帳票のスプール監査に関する情報など，EUR の監査ログを収集できます。

uCosminexus EUR Server Enterprise および EUR Server Enterprise に対応しています。

uCosminexus Navigation Platform

ログインや業務手順の実行に関する情報など，uCosminexus Navigation Platform の監査ログを収集できます。

uCosminexus Portal Framework

ユーザの作成・削除や，ログイン・ログアウトに関する情報など，uCosminexus Portal Framework の監査ログを収集できます。

XDM/BASE E2

監査ユーザ ID の設定・変更や重要情報へのアクセスに関する情報など，XDM/BASE E2 の監査ログを収集できます。

活文 NAVIstaff

ドキュメントの保護・印刷・閲覧に関する情報など，活文 NAVIstaff の監査ログを収集できます。

UNIX システムログ

ログイン・ログアウトやユーザの権限変更に関する情報など，UNIX システムログのセキュリティに関する情報を監査ログとして収集できます。

Windows イベントログ

ログオンの成功・失敗やユーザアカウントの作成・変更・削除に関する情報など，Windows イベントログのセキュリティに関する情報を監査ログとして収集できます。

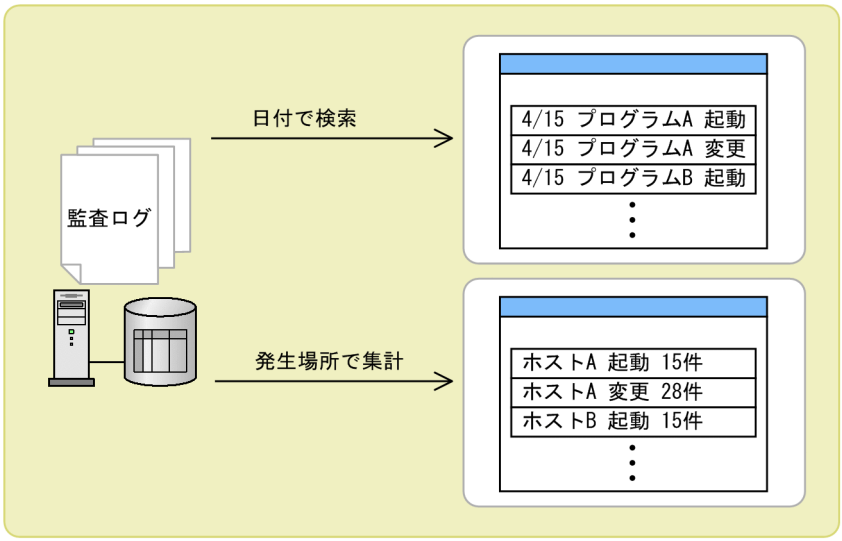
また，JP1/Audit Management - Manager の監査ログ管理データベースに格納するための定義ファイルを作成することで，ほかの JP1 シリーズ製品，日立オープンミドルウェア製品，およびその他のプログラムが出力する監査ログについても収集できるようになります。

1.2.2　監査目的に合わせた検索・集計

監査証跡管理システムでは，監査ログ管理サーバのデータベースで管理している監査ログを，監査目的に合わせて検索・集計して，企業内の IT システムの運用実態を調査したり，内部統制の報告用資料や監査用資料を作成したりできます。

監査ログの検索と集計の概念を次の図に示します。

図 1-4　監査ログの検索と集計の概念



例えば，監査ログを日付で検索したり発生場所で集計したりして，企業内の IT システムの運用実態について調査できます。

なお，監査証跡管理システムでは，目的に合わせた検索および集計パターンをテンプレートとして提供しています。このテンプレートをそのまま利用したり，カスタマイズして利用したりすることによって，検索・集計を効率的に実施できます。

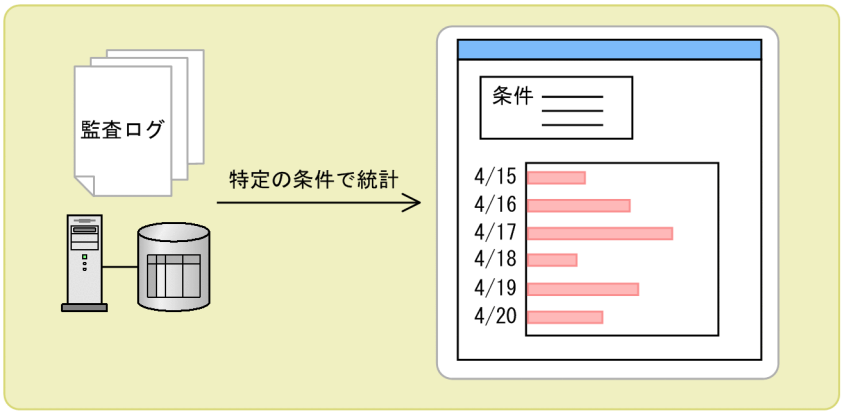
また，検索結果をレポート表示したり，集計結果をグラフ表示したりすることによって，視覚的に確認することもできます。

1.2.3　統計による事象推移の把握

監査証跡管理システムでは，監査ログ管理データベースで管理している監査ログの統計結果をグラフ形式で表示することによって，企業内の IT システム運用時に発生した事象推移を視覚的に把握したり，内部統制の報告用資料や監査用資料を作成したりできます。

監査ログの統計の概念を次の図に示します。

図 1-5　監査ログの統計の概念



例えば，ある特定の条件での監査ログの集計結果を，月単位にグラフ形式で表示することによって，IT システムの運用実態が毎月どのように推移しているかを調査できます。

なお，監査ログの統計結果は，監査ログ管理データベース内に生成した統計情報を基にして出力します。統計情報は，統計パターンの条件を基に生成されます。

1.2.4　監査ログのバックアップと閲覧専用サーバの構築

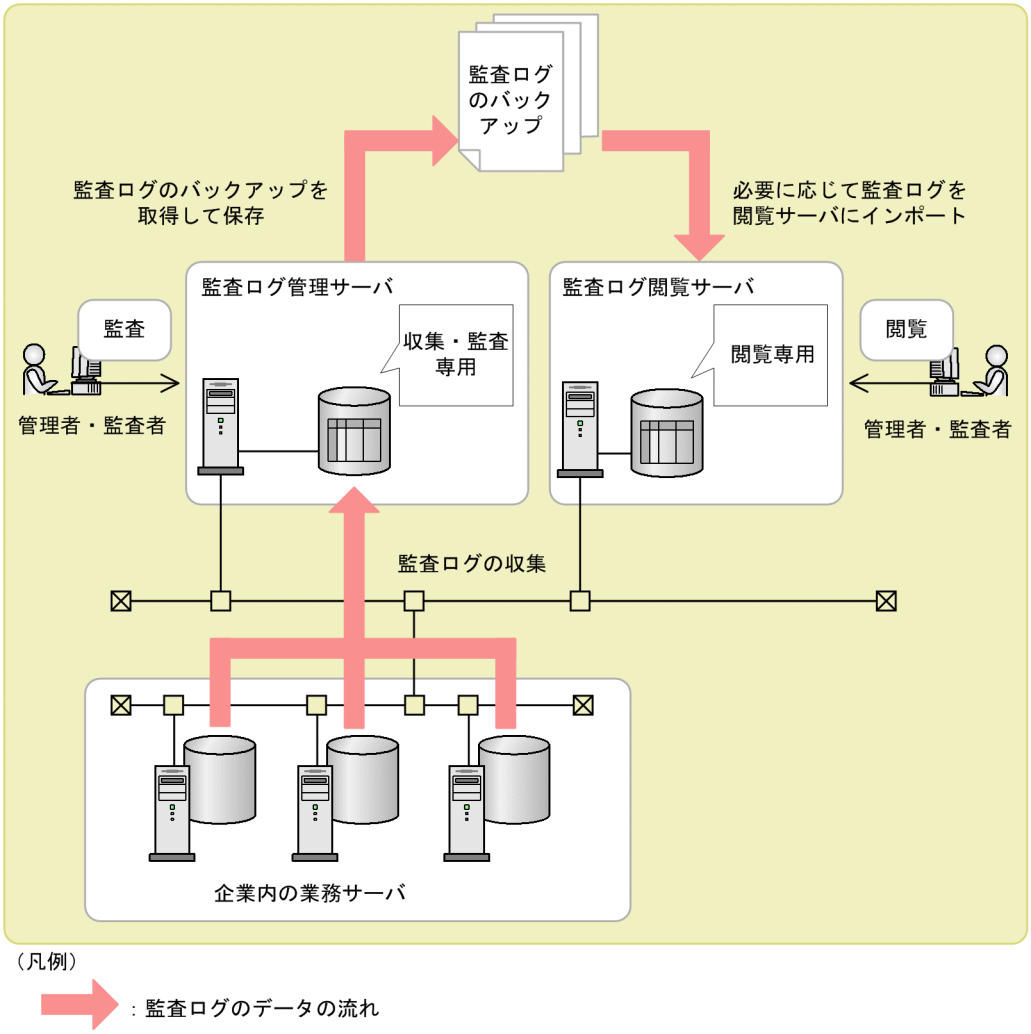
監査証跡管理システムでは，収集した監査ログをバックアップとして取得し，保存できます。また，媒体などに保存した監査ログのバックアップを必要に応じて閲覧できる閲覧専用のサーバを構築できます。この閲覧専用のサーバを**監査ログ閲覧サーバ**と呼びます。

監査ログ閲覧サーバは，バックアップした過去の監査ログを参照するためのサーバとして使用し，日々の確認には監査ログ閲覧サーバを使用せず監査ログ管理サーバを使用します。

監査ログ閲覧サーバを構築することによって，監査ログの収集・監査専用のサーバと監査が完了した監査ログを閲覧する閲覧専用のサーバに分けて，監査ログを管理できます。

監査ログ閲覧サーバの運用例を次の図に示します。

図 1-6　監査ログ閲覧サーバの運用例



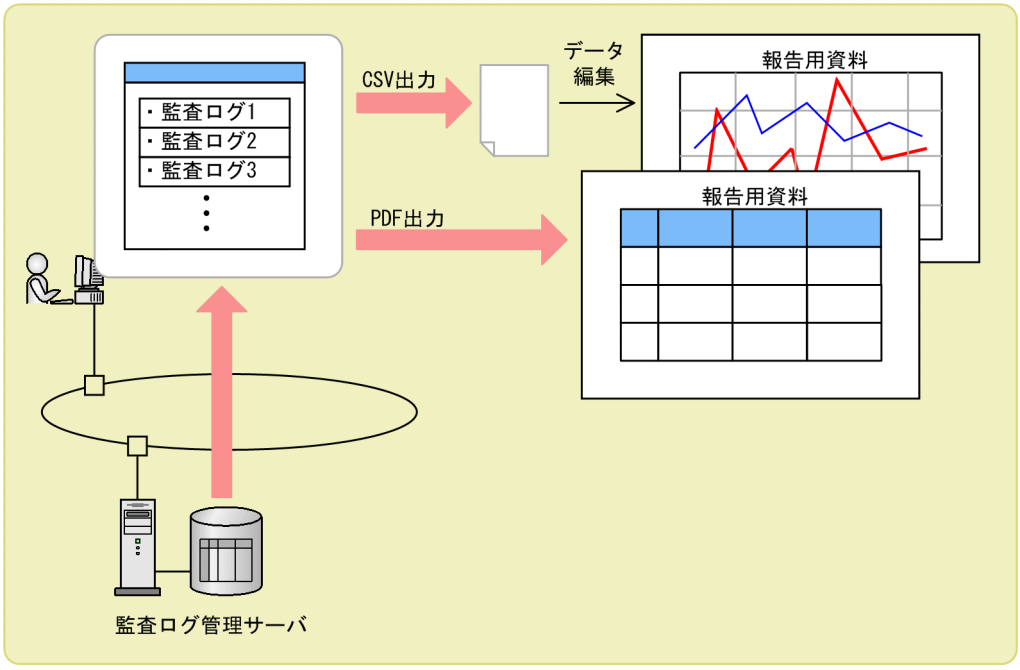
監査が完了した監査ログや保存期限が経過した監査ログについては，監査ログ管理サーバから削除することで，監査ログ管理サーバの負荷を軽減できます。さらに，バックアップとして保存している監査ログは，監査ログ閲覧サーバにインポートすることによって閲覧できるため，過去の監査ログの記録に関する問い合わせの対応や，長期間にわたるシステムの運用の実態を調査したい場合などに活用できます。

1.2.5　内部統制の報告用資料や監査用資料の作成支援

監査ログ管理データベースで管理している情報は，CSV 形式ファイルや PDF ファイルに出力できます。出力した各ファイルは，内部統制の報告用資料や監査用資料の作成に役立てることができます。

内部統制の報告用資料の作成例を次の図に示します。

図 1-7　内部統制の報告用資料の作成例



（凡例）

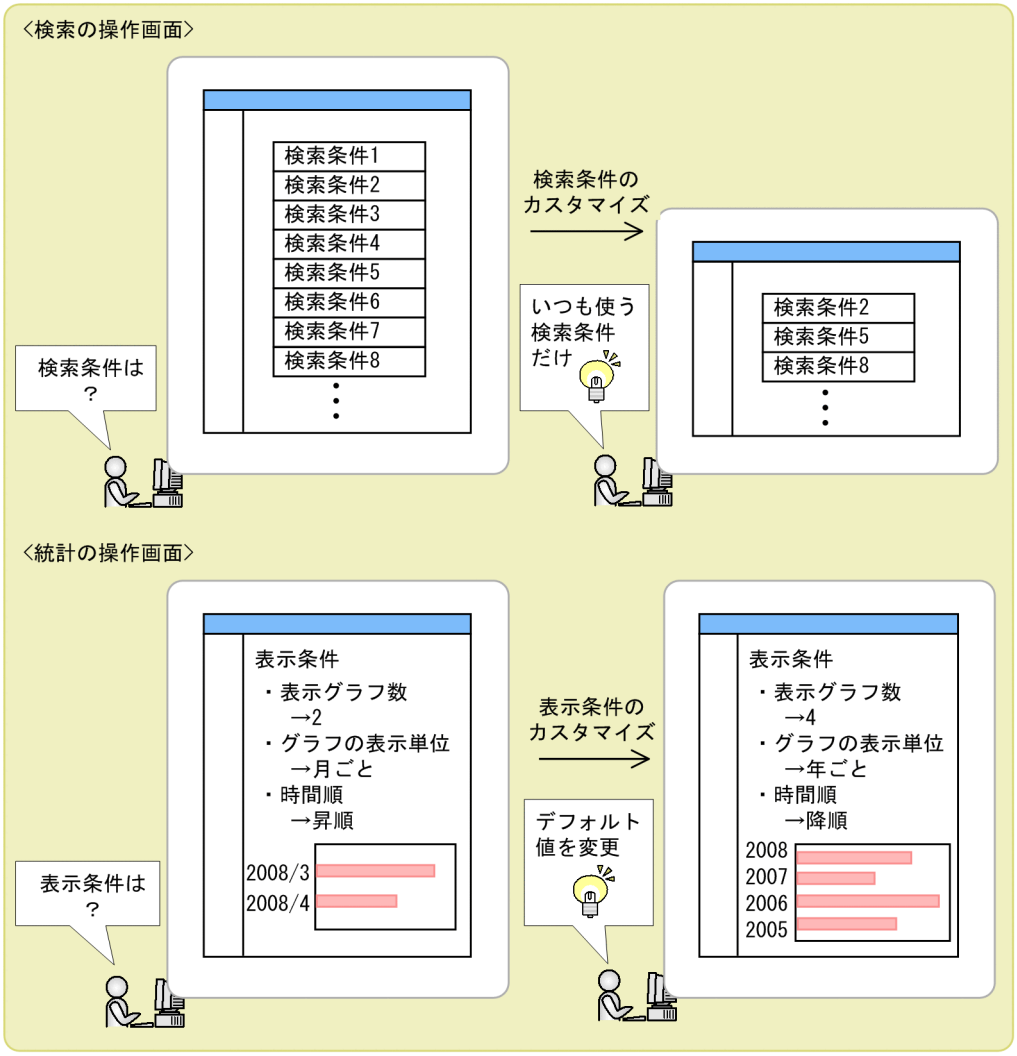
：監査ログのデータの流れ

1.2.6　操作画面のカスタマイズ

監査証跡管理システムで使用する検索や集計などの操作画面では，入力項目や結果項目の表示・非表示や表示順についてカスタマイズできます。また，統計結果を出力する操作画面の入力項目のデフォルトなどをカスタマイズできます。これらは監査ログ管理画面で実施します。使用頻度に合わせて操作画面をカスタマイズすることで，作業の効率を向上できます。

操作画面をカスタマイズする例を次の図に示します。

図 1-8　操作画面のカスタマイズ



例えば，監査ログの検索や集計などの画面では，通常では使用しない検索条件や検索結果の項目を非表示にすることで，必要な情報だけを確認できるようになります。また，監査ログの統計の画面では，統計出力条件のデフォルトを設定することで，効率よく統計結果を確認できるようになります。

1.3　代表的な運用方法の紹介

監査証跡管理システムを使用した代表的な運用方法を紹介します。

表 1-2　監査証跡管理システムを使用した代表的な運用例

項番	運用例	説明個所
1	企業内の IT システムの運用実態について把握する	1.3.1
2	企業内の IT システムが正しく運用されているかどうかを確認する	1.3.2
3	監査ログを利用して報告用資料を作成する	1.3.3
4	監査ログのバックアップを自動的に取得する	1.3.4
5	バックアップの取得履歴を確認する	1.3.5
6	監査ログ閲覧サーバで監査ログを閲覧する	1.3.6
7	運用の変化に対応して監査ログの収集対象を追加・解除する	1.3.7

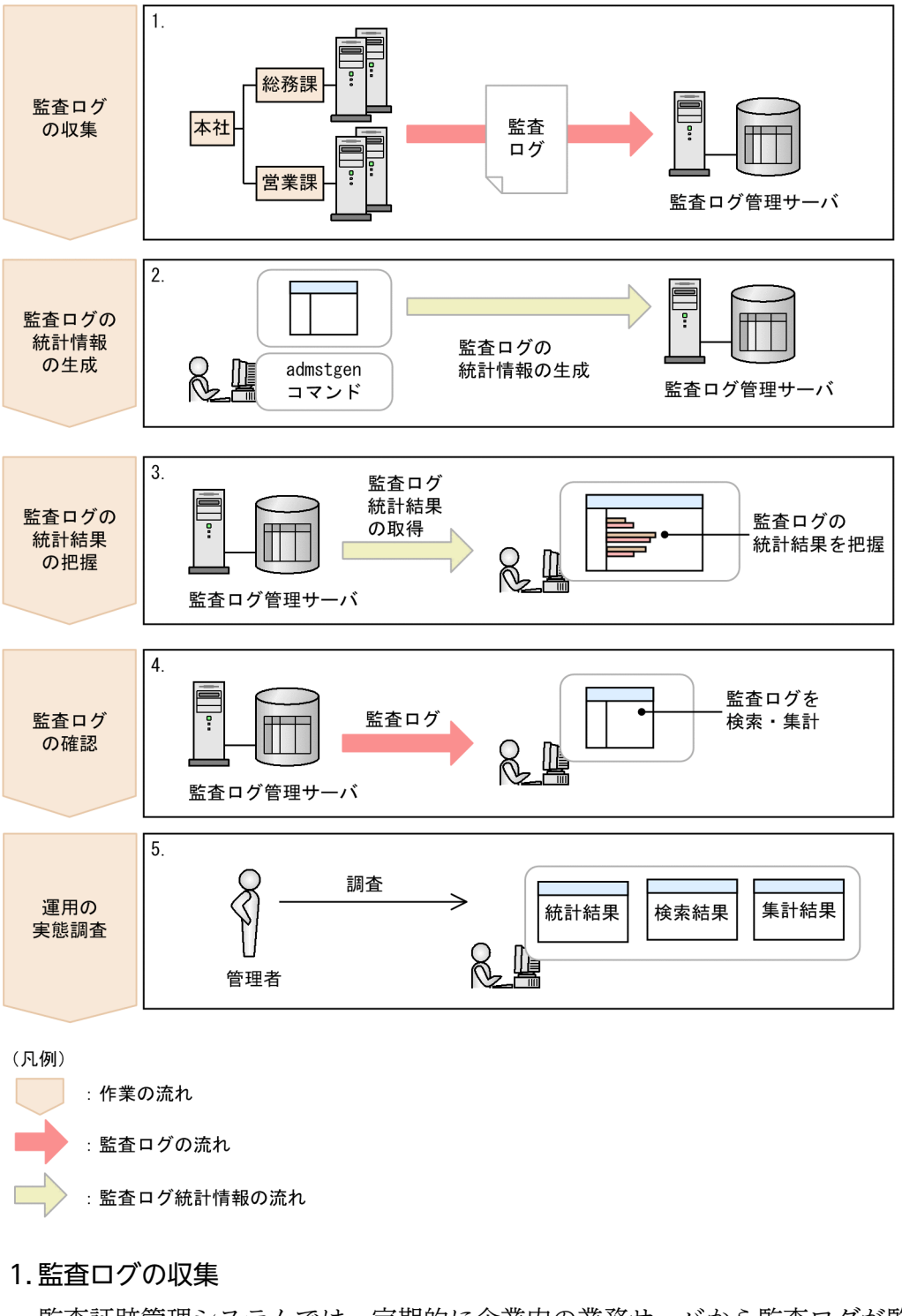
1.3.1　企業内の IT システムの運用実態について把握する

監査証跡管理システムを使用して，監査ログの統計結果から，企業内の IT システムの運用実態を把握する運用例を紹介します。

特定の条件に基づいた監査ログの統計結果から「どのような操作を実施したか」や「操作結果はどうだったのか」などの事象推移を視覚的に把握でき，企業内の IT システムの運用実態を調査する手助けとして活用できます。

企業内の IT システムの運用実態を把握する運用例を次の図に示します。

図 1-9　企業内の IT システムの運用実態を把握する運用例



1. 監査ログの収集

監査証跡管理システムでは，定期的に企業内の業務サーバから監査ログが監査ログ管理サーバに収集されます。

2. 監査ログの統計情報の生成

監査ログ管理データベースに蓄積されている監査ログを基に，監査ログの統計情報を生成します。監査ログの統計情報は，マネージャセットアップで設定またはコマンドを実行することによって，監査ログ管理サーバの監査ログ管理データベースに生成されます。

3. 監査ログの統計結果の把握

生成された統計情報を基に，特定の条件を設定して統計結果をグラフ形式で表示します。この統計結果から，ある期間にシステムで発生した事象推移を把握できます。監査ログの統計結果は，次の図に示す監査ログ統計画面で確認できます。

図 1-10　監査ログ統計画面

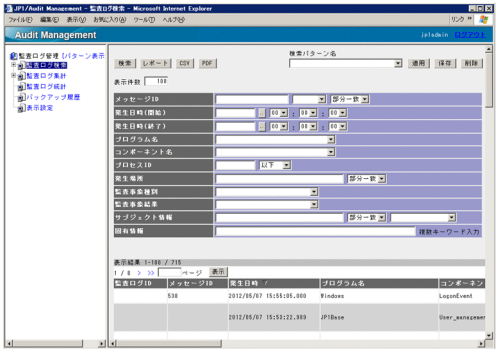
4. 監査ログの確認

把握した統計結果を基に，さらに詳しい情報を知りたい場合は，検索・集計を実施して監査ログを確認します。

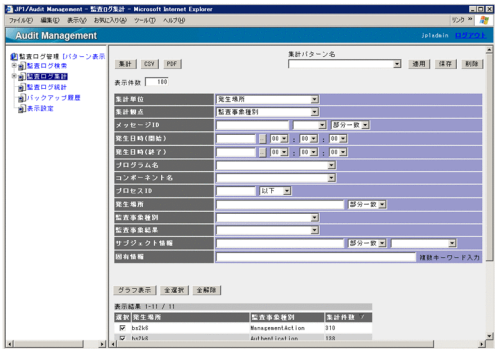
監査ログの検索・集計は，次の図に示す監査ログ検索画面および監査ログ集計画面で実施します。

図 1-11　監査ログ検索画面と監査ログ集計画面

監査ログ検索画面



監査ログ集計画面



監査ログ検索画面や監査ログ集計画面で，統計結果の条件と同等の条件を入力することによって，実際に取得されている監査ログの詳細を把握できます。

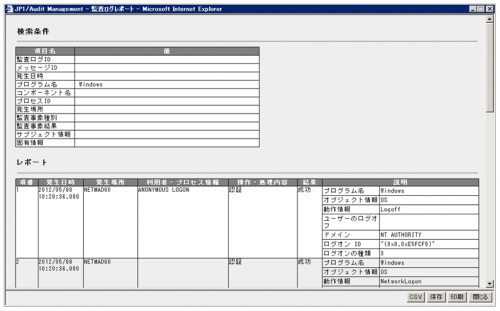
5. 運用の実態調査

管理者は，監査ログの統計結果，検索結果，および集計結果を基に，企業内の IT システムの運用実態を調査できます。検索結果の場合はレポートを表示したり，集計結果の場合はグラフを表示したりして確認することもできます。

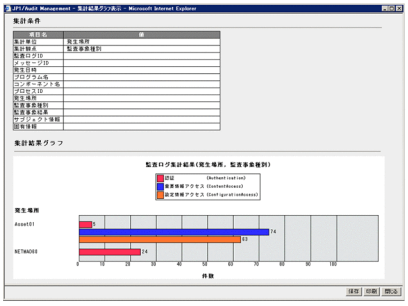
検索結果のレポート表示および集計結果のグラフ表示の例を次に示します。

図 1-12　監査ログ検索結果のレポートと監査ログ集計結果のグラフ

監査ログ検索結果のレポート



監査ログ集計結果のグラフ



また，画面で確認するだけでなく，CSV 形式ファイルや PDF ファイルに結果を出力して調査資料を作成することもできます。

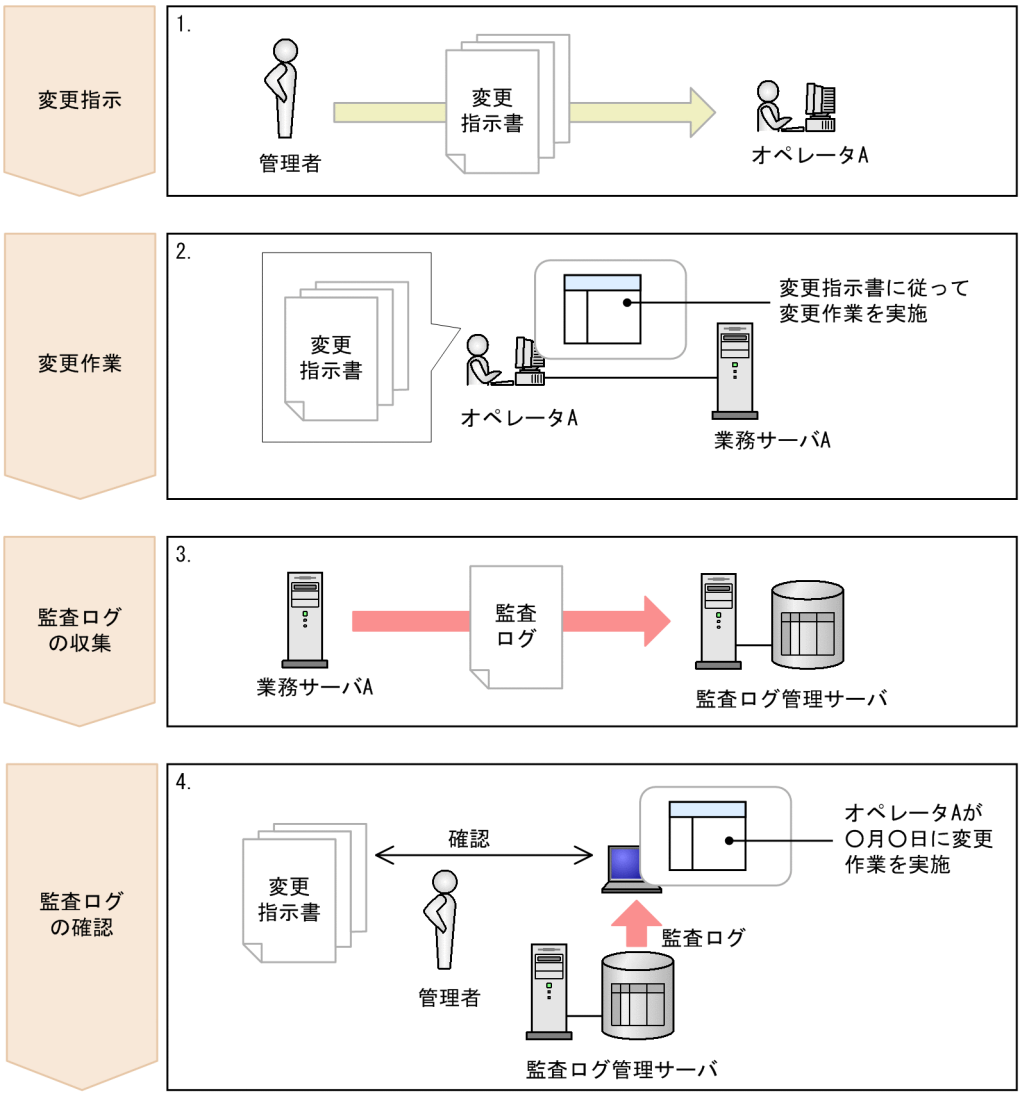
1.3.2　企業内の IT システムが正しく運用されているかどうかを確認する

監査証跡管理システムを使用して，企業内の規則や管理者の変更指示どおりに IT システムの操作が実施されているかどうかを確認する運用例を紹介します。

監査ログと，業務規則書や作業指示書などを照合することによって，「どのユーザが」「いつ」「どのクライアントから」「どのような操作を実施したか」を確認でき，不正操作や問題を発見する手助けとして活用できます。IT システム上の重要な変更を実施した場合やオペレータの作業内容に不安がある場合などには，個々の監査ログを確認するのも有効な手法です。

管理者の変更指示どおりに IT システムの操作が実施されているか監査ログを確認する運用例を次の図に示します。

図 1-13　監査ログを確認する運用例



1. 変更指示

管理者は，企業内の IT システムに対する設定変更を，決裁済みの変更指示書でオペレータ A に依頼します。

2. 変更作業

オペレータ A は，変更指示書に従って，業務サーバ A に対する設定の変更作業を実施します。

3. 監査ログの収集

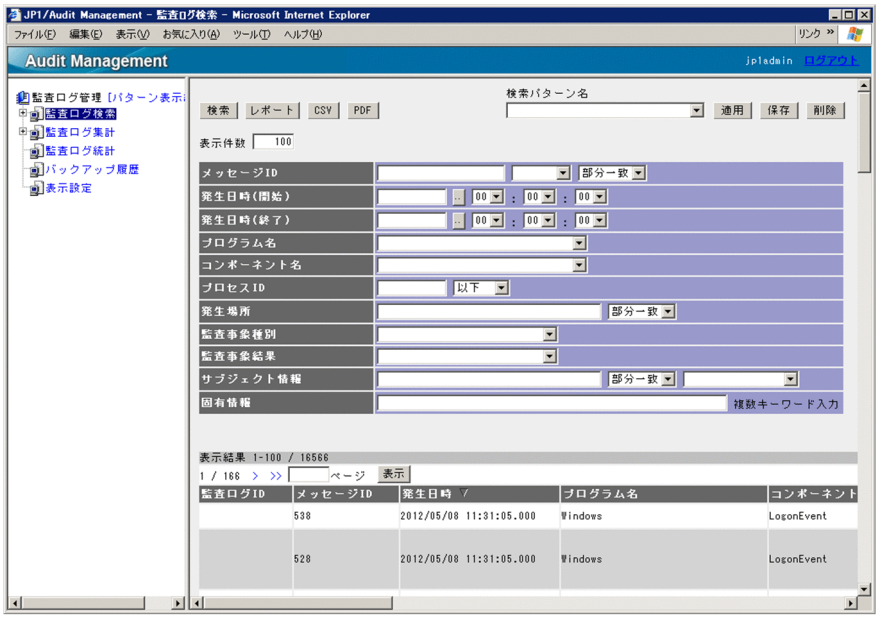
監査証跡管理システムでは，定期的に業務サーバ A の監査ログが監査ログ管理サーバに収集されます。

4. 監査ログの確認

管理者は，変更指示書と監査ログを比較し，変更指示書どおりに IT システムの設定が変更されているか，オペレータ A の変更作業に問題がないかどうかを確認します。

監査ログの確認は，次の図に示す監査ログ検索画面で実施します。

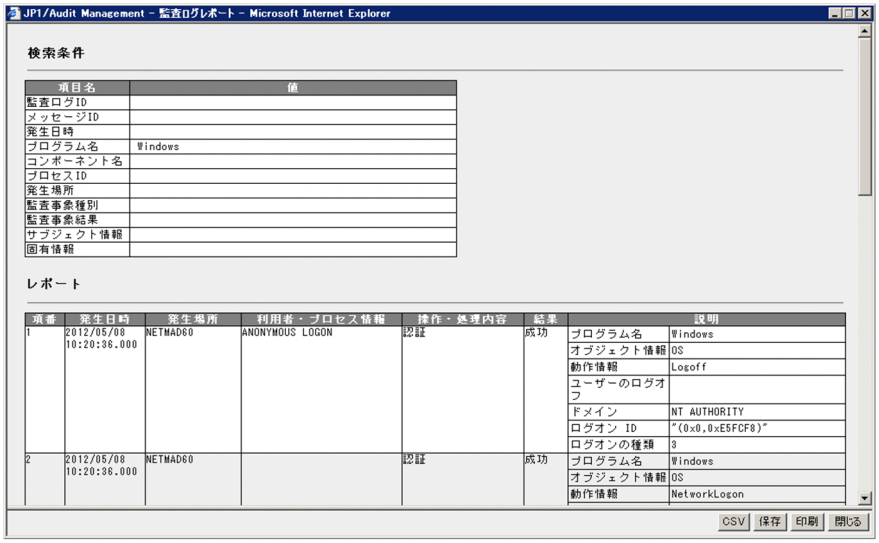
図 1-14　監査ログ検索画面



プログラム名や発生場所などの検索条件を入力して監査ログを検索し，目的の監査ログの内容を確認します。また，検索結果をレポート表示して確認することもできます。

検索結果のレポート表示の例を次に示します。

図 1-15　監査ログ検索結果のレポート

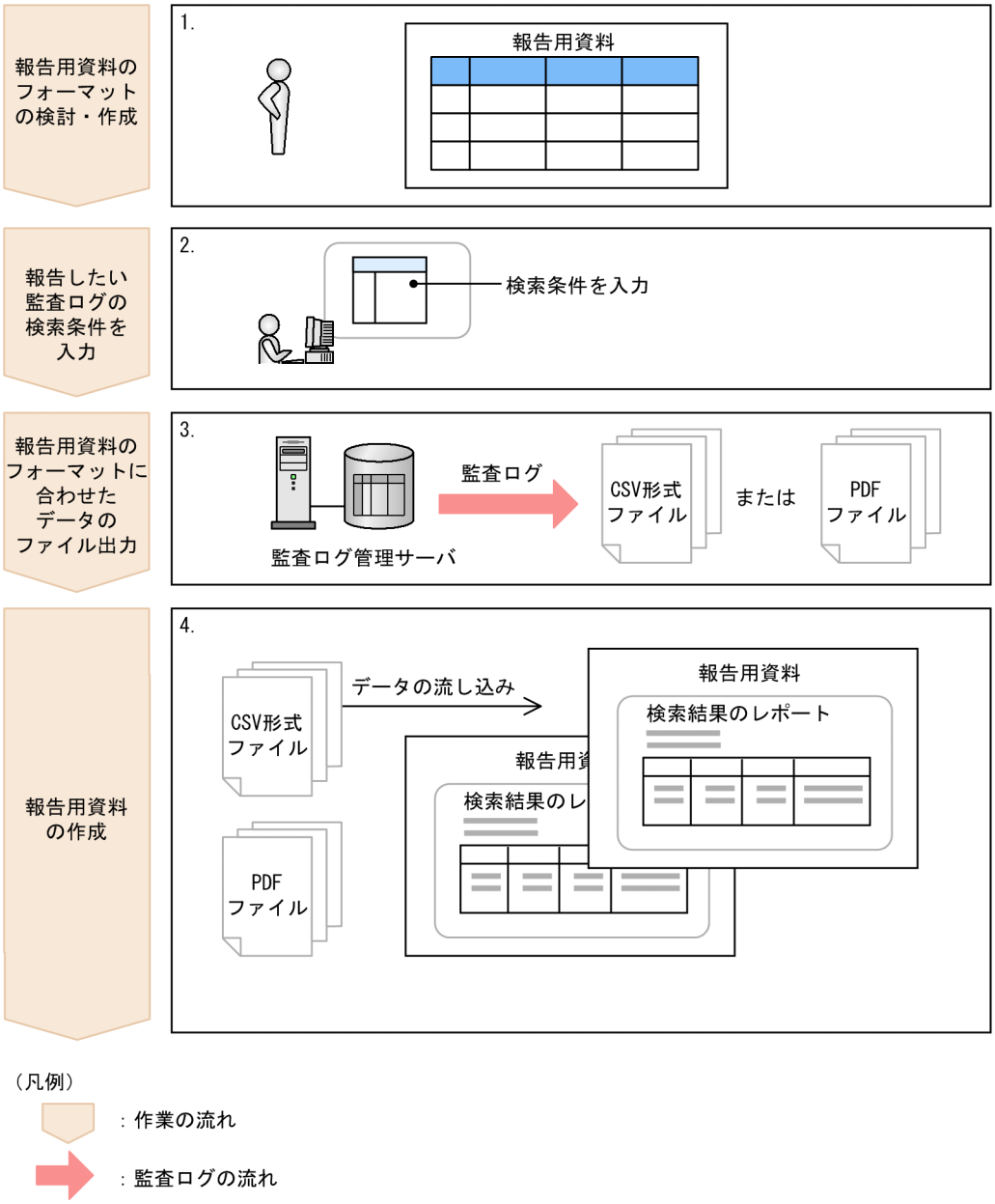


1.3.3　監査ログを利用して報告用資料を作成する

収集し蓄積された監査ログから，ある特定の条件で監査ログを検索し，検索結果を利用して内部統制の報告用資料や監査用資料を作成する運用例を紹介します。

監査ログの検索結果を，CSV 形式ファイルまたは PDF ファイルに出力して報告用資料を作成する運用例を次の図に示します。

図 1-16　監査ログを利用して報告用資料を作成する運用例



1. 報告用資料のフォーマットの検討・作成

監査ログを利用して，報告用資料をどのように作成するか検討した上で，必要に応じて報告用資料のフォーマットを作成しておきます。

2. 報告したい監査ログの検索条件を入力

監査ログ検索画面で，報告する必要がある情報を含む監査ログの検索条件を入力し，検索結果を取得します。

3. 報告用資料のフォーマットに合わせたデータのファイル出力

監査ログの検索結果を，手順 1 で検討した報告用資料のフォーマットに合わせてファイル出力します。監査証跡管理システムでは，検索結果を CSV 形式ファイルまたは PDF ファイルに出力できます。

- CSV 形式ファイルに出力する場合

  手順 2 で検索条件を入力したあと，［CSV］ボタンをクリックすると，検索結果が CSV 形式ファイルに出力されます。

- PDF ファイルに出力する場合

  手順 2 で検索条件を入力したあと，［PDF］ボタンをクリックすると，手順 1 で作成した報告用資料のフォーマットに従って，検索結果が PDF ファイルに出力されます。

4. 報告用資料の作成

- 監査ログの検索結果を CSV 形式ファイルに出力した場合

  出力された CSV 形式ファイルを，手順 1 で作成した報告用資料のフォーマットに従って加工し，報告用資料を作成します。

- 監査ログの検索結果を PDF ファイルに出力した場合

  出力された PDF ファイルを報告用資料としてそのまま使用できます。

なお，検索結果の CSV 形式ファイルや PDF ファイルだけでなく，検索結果のレポート，集計結果の CSV 形式ファイル，PDF ファイル，グラフ，統計結果の CSV 形式ファイルやグラフも報告用資料として使用できます。

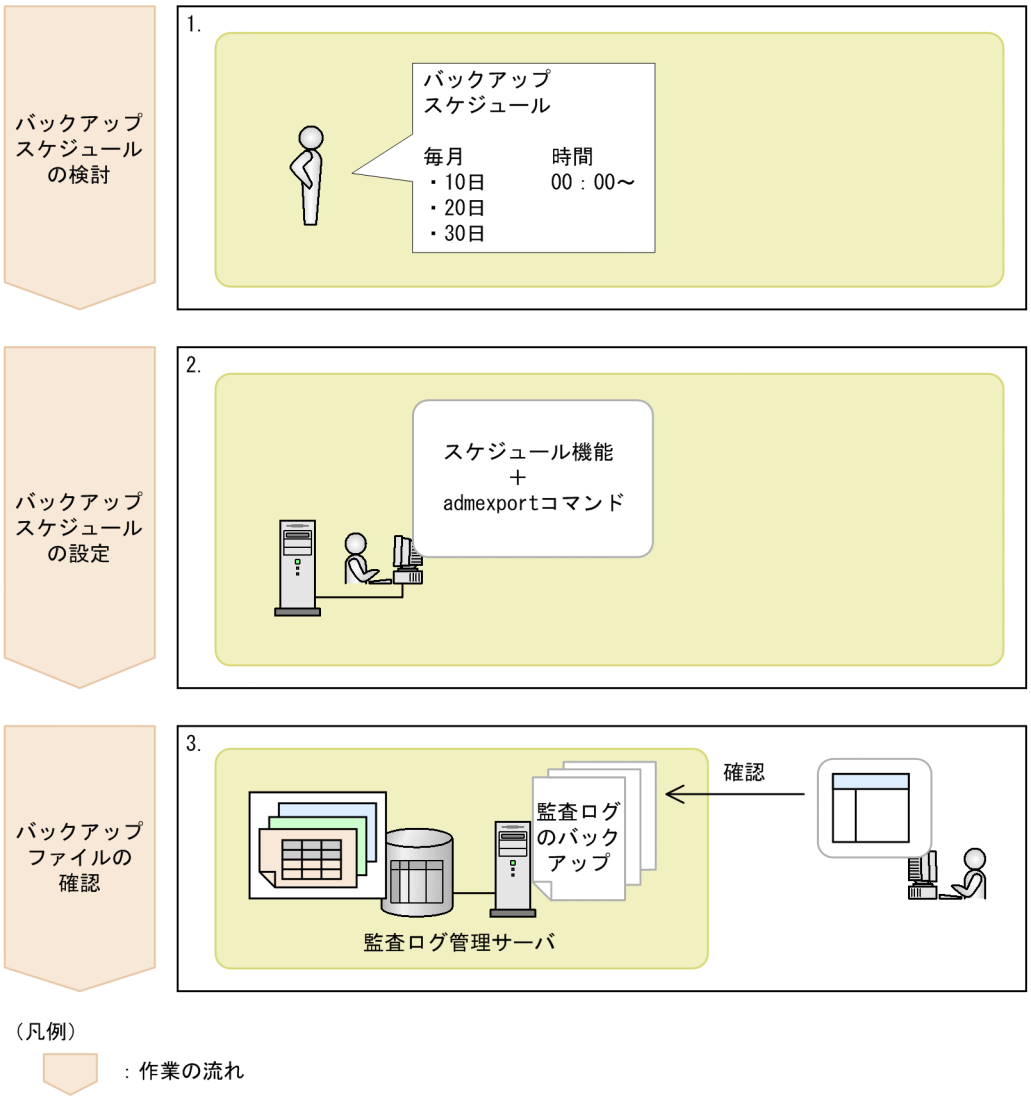
1.3.4 監査ログのバックアップを自動的に取得する

監査ログのバックアップを自動的に取得することによって，定期的なバックアップ運用を実現できます。監査ログ管理データベースから監査ログを自動的にバックアップする運用例を紹介します。

JP1/AJS や Windows のタスクスケジューラのスケジュール機能を利用するなどして，定期的に自動で監査ログのバックアップを取得できます。なお，自動バックアップでは，前回バックアップした監査ログからの差分をバックアップします。

監査ログのバックアップを自動的に取得する運用例を次の図に示します。

図 1-17　監査ログのバックアップを自動的に取得する運用例



1. バックアップスケジュールの検討

監査ログのバックアップを自動化するために，あらかじめバックアップスケジュールを検討しておきます。

2. バックアップスケジュールの設定

JP1/AJS や Windows のタスクスケジューラを利用するなどして，バックアップスケジュールを設定します。

3. バックアップファイルの確認

監査ログのバックアップファイルが作成されているかどうかを確認します。

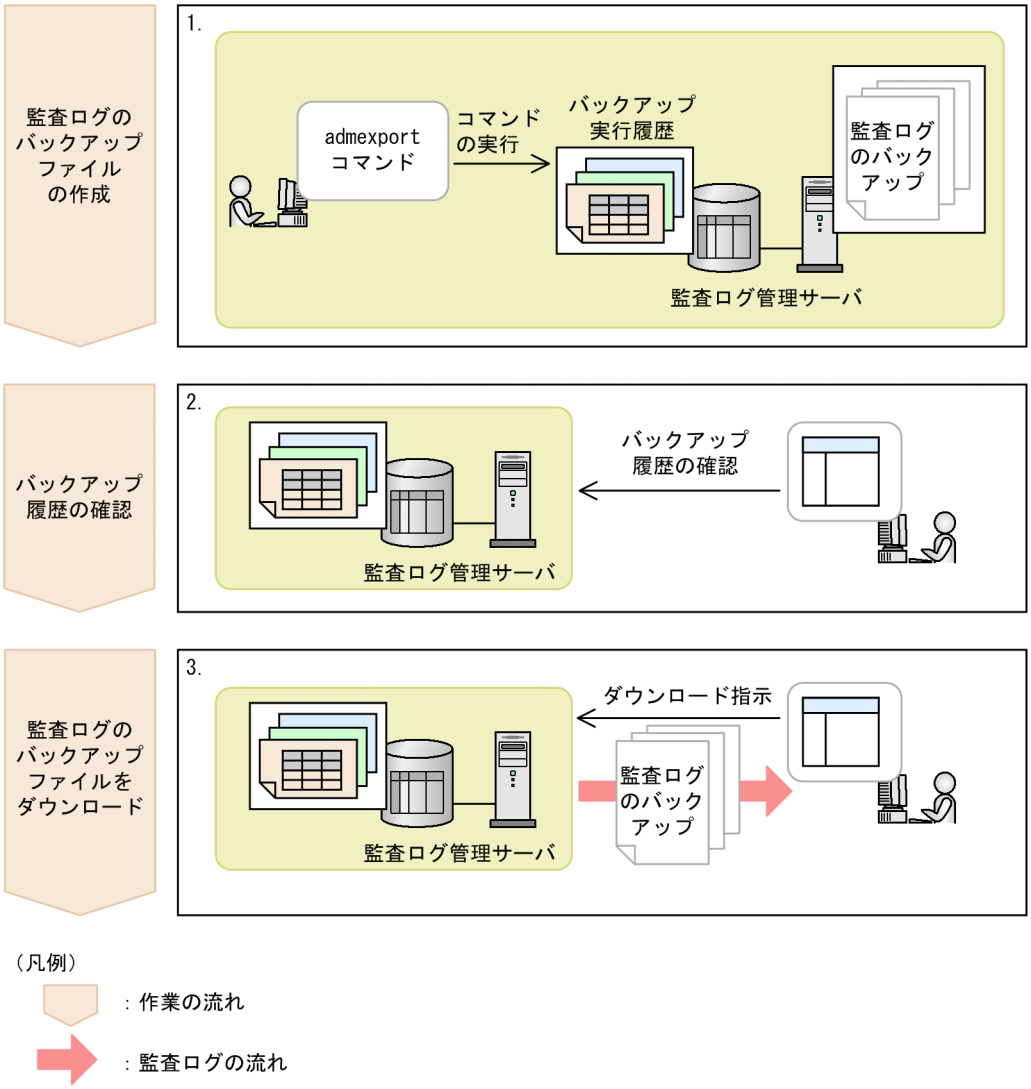
1.3.5　バックアップの取得履歴を確認する

監査ログをバックアップしたときの履歴を確認する運用例を紹介します。

監査ログをバックアップすると，バックアップの実行情報がバックアップ実行履歴としてデータベースに格納されます。この監査ログのバックアップ実行履歴を検索して，目的の監査ログが保存されているバックアップファイルがどのファイルか確認できます。また，必要に応じて，このバックアップ実行履歴からバックアップファイルをダウンロードできます。

管理している監査ログの履歴を確認する運用例を次の図に示します。

図 1-18　管理している監査ログの履歴を確認する運用例



1. 監査ログのバックアップファイルの作成

監査ログ管理データベースに格納されている監査ログを，監査ログ管理サーバに，コマンドを使用してバックアップします。

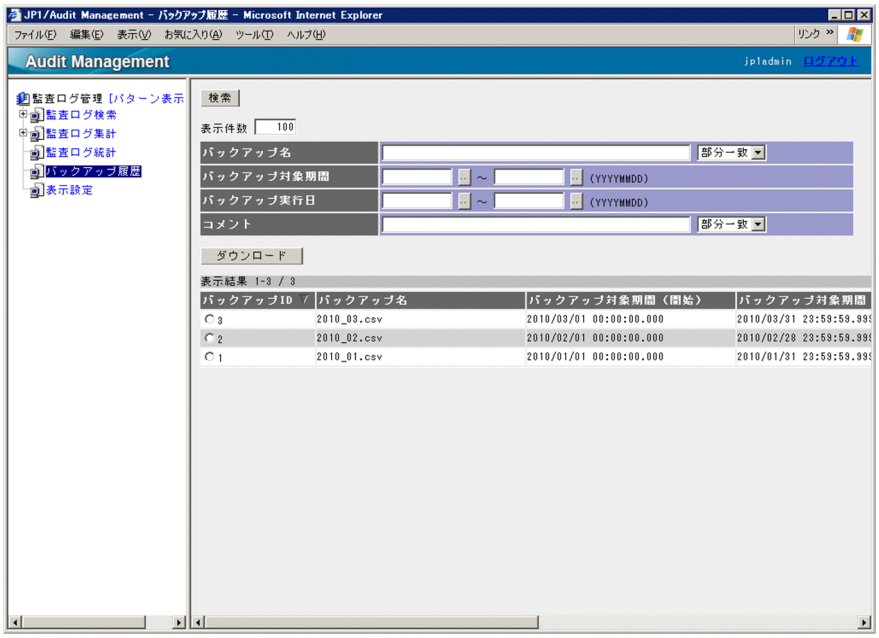
バックアップを実行すると，バックアップ実行履歴が監査ログ管理データベースに格納され，バックアップファイルが監査ログ管理サーバ上に作成されます。

2. バックアップ履歴の確認

監査ログのバックアップ履歴を検索して，目的の監査ログが保存されているバックアップファイルがどのファイルか確認します。

監査ログのバックアップ履歴の確認は，次の図に示すバックアップ履歴画面で実施します。

図 1-19　バックアップ履歴画面



バックアップ日時やバックアップ名などの検索条件を入力して，監査ログのバックアップ履歴を検索します。

3. 監査ログのバックアップファイルをダウンロード

監査ログ管理サーバ内に保存されている監査ログのバックアップファイルを，バックアップ履歴画面を使用して，ダウンロードします。

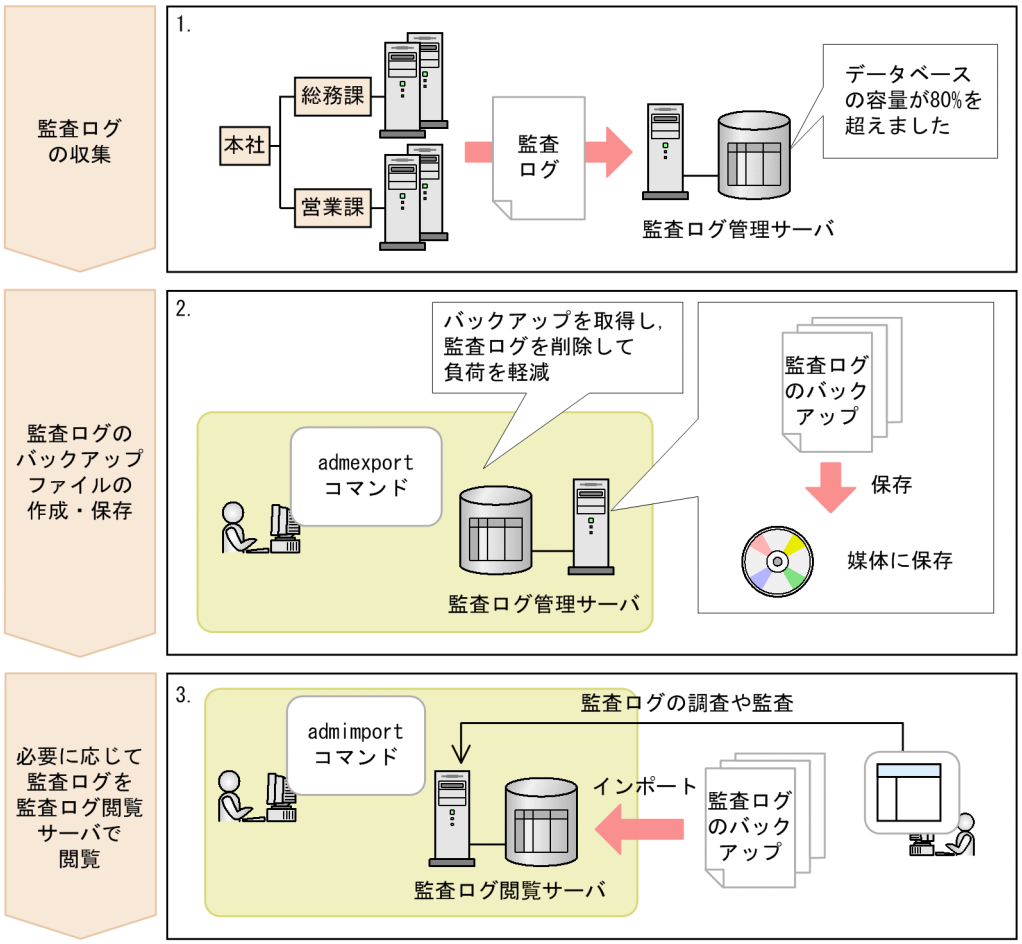
1.3.6　監査ログ閲覧サーバで監査ログを閲覧する

監査ログ管理サーバとは別に，監査ログを閲覧する専用サーバを構築して，企業内の IT システムの監査ログを管理する運用例を紹介します。

収集された監査ログは，監査ログ管理サーバのデータベース（監査ログ管理データベース）に格納されます。一定量以上の監査ログが収集されると，監査ログ管理データベースの容量がいっぱいになり，監査ログの検索時間やデータベースのメンテナンス時間が増加し，監査証跡管理システムの運用に支障を来すおそれがあります。この場合，監査が完了した監査ログを，バックアップとして媒体などに保存したあとに監査ログ管理サーバから削除することで，監査ログ管理データベースの負荷を軽減できます。また，保存した監査ログのバックアップは，別に構築した監査ログ閲覧サーバにインポートして閲覧できます。

監査ログ閲覧サーバで監査ログを閲覧する運用例を次の図に示します。

図 1-20　監査ログ閲覧サーバで監査ログを閲覧する運用例



（凡例）

：作業の流れ

：監査ログの流れ

1. 監査ログの収集

監査証跡管理システムでは，企業内の業務サーバから出力された監査ログが監査ログ管理サーバに定期的に収集されます。

なお，監査ログ管理データベースの容量がしきい値（図の例では 80%）を超えると，データベースの容量が不足していることを示すメッセージが出力されます。

2. 監査ログのバックアップファイルの作成・保存

監査ログ管理データベースに格納されている監査ログを，コマンドを使用して監査ログ管理サーバ内にバックアップします。

なお，監査ログ管理データベースの負荷を軽減するには，バックアップを取得した監査ログを削除してください。バックアップを取得した監査ログは，媒体に保存したり，監査ログ閲覧サーバにダウンロードしたりするなどの保存方法があります。

3. 必要に応じて，監査ログを監査ログ閲覧サーバで閲覧

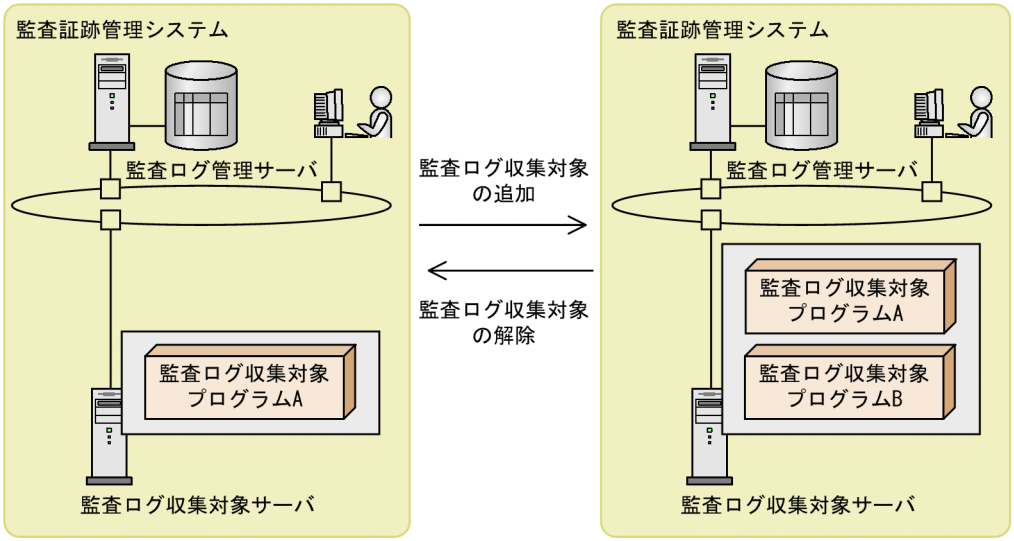
必要に応じて，保存している監査ログのバックアップファイルを監査ログ閲覧サーバにインポートします。これで，監査ログ閲覧サーバから監査ログを閲覧できるようになります。

1.3.7　運用の変化に対応して監査ログの収集対象を追加・解除する

運用の変化に対応して，運用開始後に監査ログ収集対象を追加・解除する運用例を紹介します。

新規プログラムの導入によって，監査ログ収集対象サーバを新たに構築したり，使用していたプログラムの運用を停止したりするなど，運用の変化に対応して，運用開始後に監査ログの収集対象を追加・解除する運用例を次の図に示します。

図 1–21　監査ログ収集対象を追加・解除する運用例

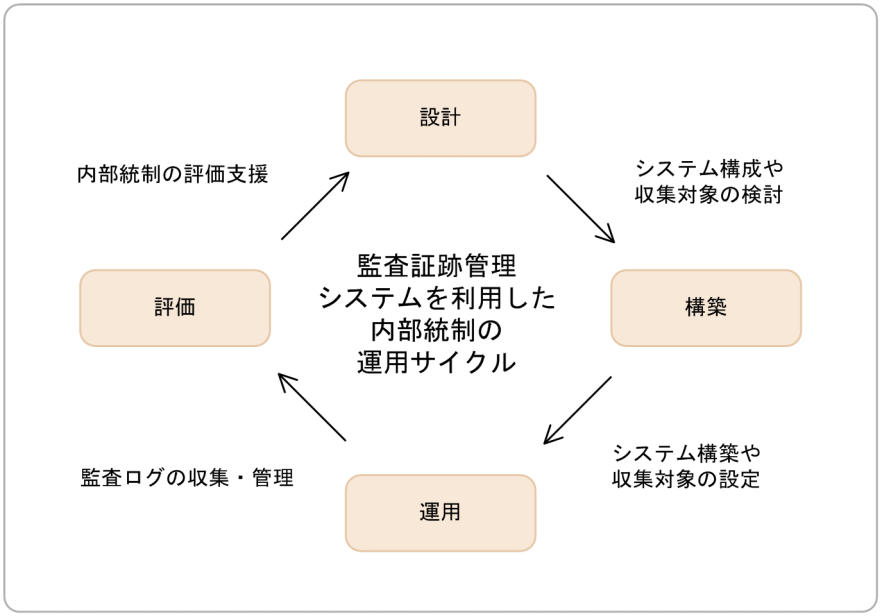


- 監査ログ収集対象の追加
  新しく監査ログを収集するサーバまたはプログラムを収集対象として追加します。
- 監査ログ収集対象の解除
  収集対象として設定していたサーバまたはプログラムを解除します。

1.4　監査証跡管理システムを利用した内部統制の運用サイクル

監査証跡管理システムを利用して，企業内の業務サーバから内部統制の証跡記録を収集・管理する運用サイクルを次の図に示します。

図 1-22　監査証跡管理システムを利用した運用サイクル



（凡例）

：フェーズ

：フェーズの移行

設計

企業内の業務サーバから内部統制の証跡記録を収集・管理するために，監査証跡管理システムを設計するフェーズです。次に示す項目の検討をします。

- 監査ログの収集対象の検討

  監査証跡管理システムを利用して監査ログを収集・管理したい業務サーバやプログラムを検討します。

- 監査ログの収集方法や取り扱い方法などの運用方法の検討

  業務サーバやプログラムから監査ログをどのように収集するか，どのように取り扱うかなどの運用方法を検討します。

- システム構成の検討

  検討した運用方法を基に，監査証跡管理システムをどのようなシステム構成にするか検討します。

システム設計については「4.　システム設計」を参照してください。

構築

設計フェーズで検討した内容に従い，監査証跡管理システムを導入して各サーバを構築するフェーズです。次に示す項目の構築をします。

- 監査ログ管理サーバの構築

監査ログを収集し，一元管理するためのサーバを構築します。

- 監査ログ閲覧サーバの構築（任意）

  収集した監査ログを閲覧するための専用サーバを構築します。

- 監査ログ収集対象サーバの構築

  監査ログの収集対象となるサーバを構築します。

システム構築については「5.　システム構築」および「6.　クラスタ環境でのシステム構築」を参照してください。

運用

監査証跡管理システムを運用するフェーズです。監査ログを収集・管理します。

監査証跡管理システムの運用については「第３編　運用編」を参照してください。

評価

監査証跡管理システムで収集した監査ログと業務規則書や作業指示書などの資料を照合し，企業内の内部統制を評価するフェーズです。

企業内の内部統制を評価する際にも，監査ログの統計結果を出力することで，システム運用時の事象推移を視覚的に把握できます。また，検索・集計・統計結果を利用して，内部統制の報告用資料や監査用資料を作成できます。

内部統制を評価する上で利用できる監査ログ管理画面の操作方法については「第３編　運用編」を参照してください。

2 機能

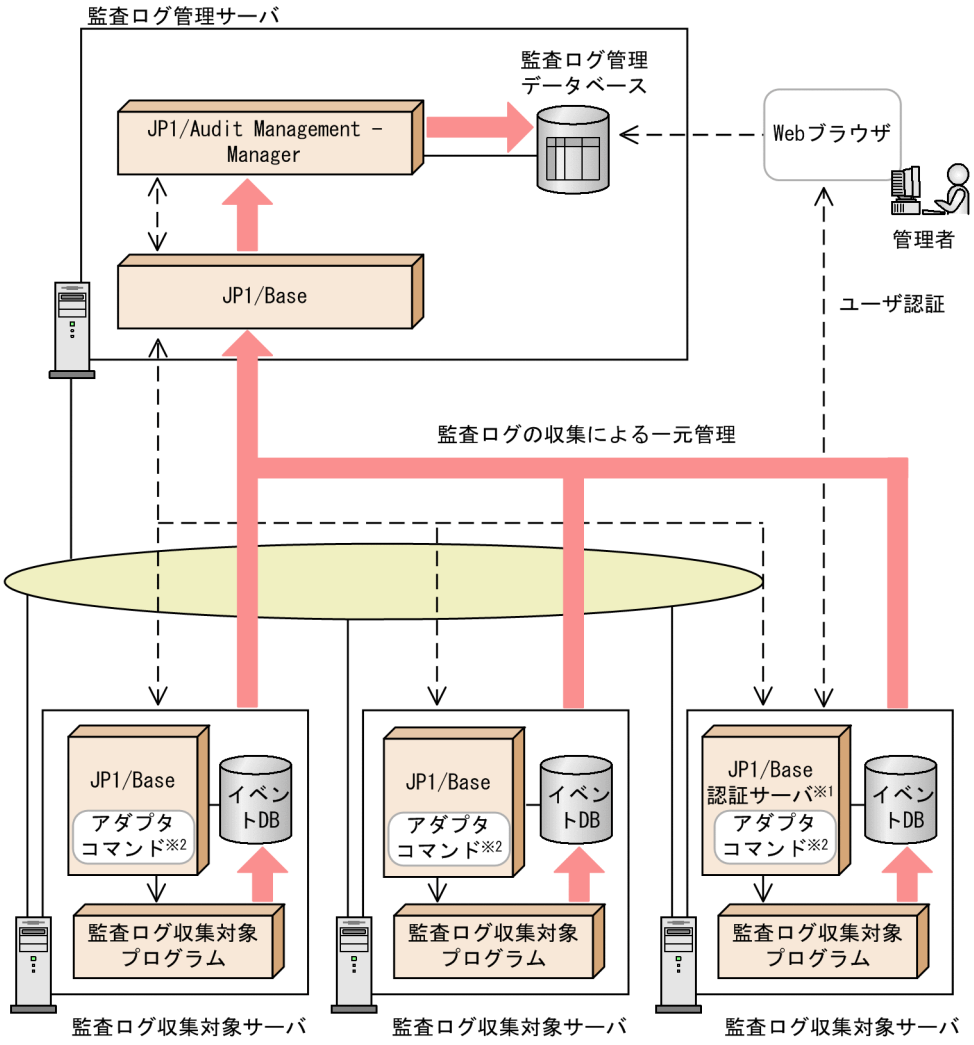
この章では，監査証跡管理システムの機能について説明します。

2.1　機能の概要

監査証跡管理システムは，JP1/Base と連携して JP1 シリーズやその他プログラムの監査ログの収集・管理を実現します。

監査証跡管理システムの全体構成を次の図に示します。

図 2-1　監査証跡管理システムの全体構成



（凡例）

：監査ログのデータの流れ

注※1 監査証跡管理システムには，JP1/Baseの認証サーバが必要です。ただし，JP1/Baseの認証サーバの構築場所は任意です。

注※2 JP1/Audit Management - Managerが提供するコマンドです。監査ログ収集対象サーバのセットアップ時にインストールされます。

監査証跡管理システムの機能一覧を次の表に示します。

表 2-1　監査証跡管理システムの機能一覧

項番	機能	説明	参照先
1	監査ログの収集	監査ログ収集対象サーバに導入されているプログラムが出力した監査ログを収集します。	2.2
2	監査ログの一元管理	JP1/Audit Management - Manager に組み込まれているデータベースを使用して監査ログを一元管理します。	2.3
3	JP1/Base のユーザ管理機能を使ったユーザ管理	JP1/Base のユーザ管理機能によって，JP1 専用のアカウントによるユーザ認証やアクセス制御を実施します。	2.4
4	監査ログの検索と集計	JP1/Audit Management - Manager の監査ログ管理画面の検索・集計機能によって，監査ログを管理します。	2.5
5	監査ログの統計情報の生成と統計結果の出力	監査ログ統計機能によって，監査ログ管理データベースに監査ログの統計情報を生成します。また，生成した統計情報を基に，監査ログ管理画面に統計結果を出力します。	2.6
6	監査ログのバックアップ履歴管理	監査ログのバックアップ履歴一覧を表示して，監査ログのバックアップ実行履歴を管理します。	2.7
7	監査ログ管理画面のカスタマイズ	監査ログ管理画面で使用する項目の表示または非表示を設定します。	2.8
8	JP1/Audit Management - Manager の監査ログ出力	JP1/Audit Management - Manager の監査ログを出力します。	2.9

2.2　監査ログの収集

監査証跡管理システムは，監査ログ収集対象サーバに導入されているプログラムが出力した監査ログを収集します。

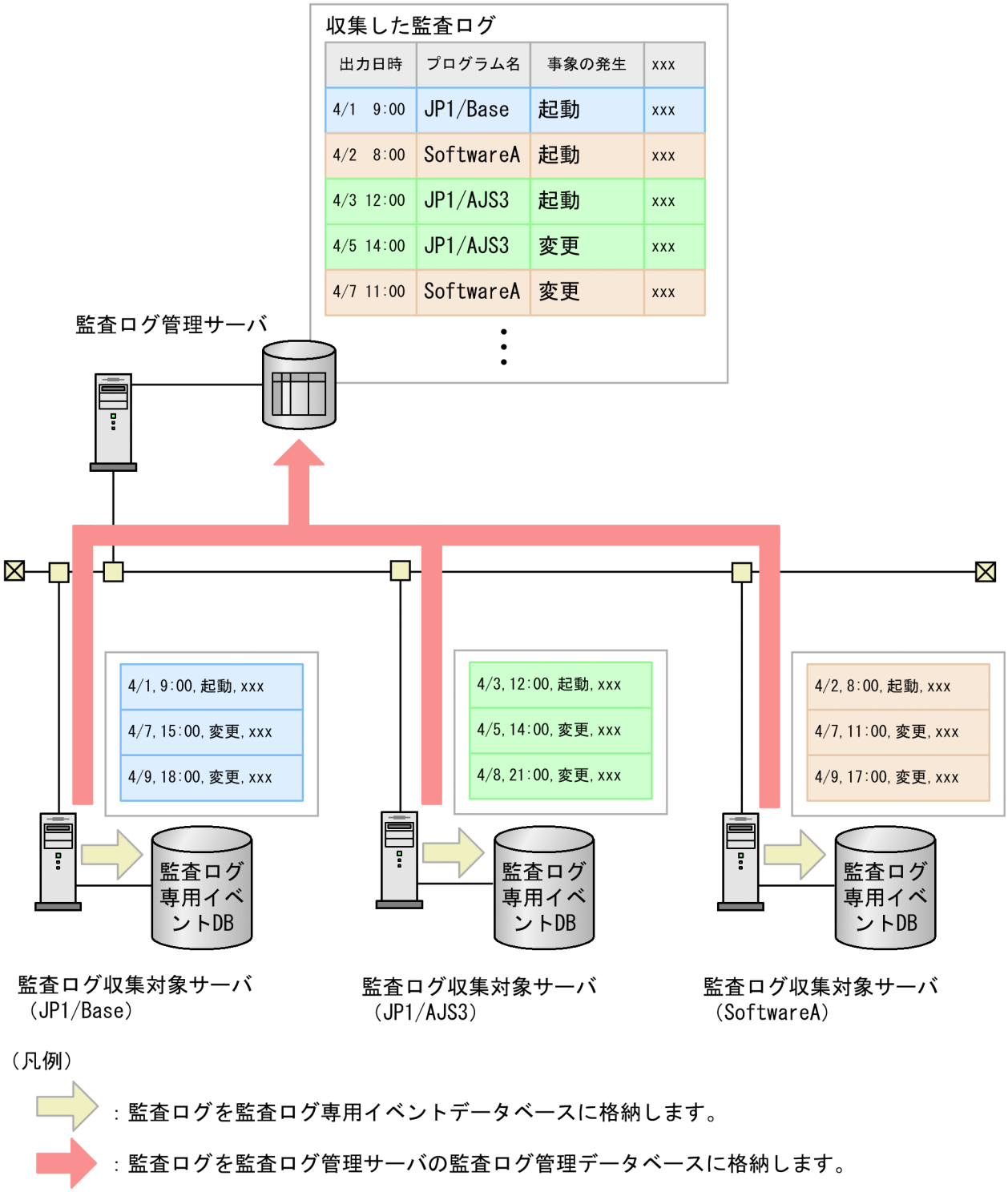
この節では，次に示す内容について説明します。

- 監査ログの収集の仕組み
- 監査ログの収集のタイミング
- 監査ログの収集カテゴリ
- 監査ログの正規化

2.2.1　監査ログの収集の仕組み

各業務で使用している監査ログ収集対象サーバから，監査ログ管理サーバに監査ログを収集する仕組みを次の図に示します。

図 2-2　監査ログ収集の仕組み



監査ログを収集する仕組みを，監査ログ管理サーバおよび監査ログ収集対象サーバに分けて説明します。

(1)　監査ログ管理サーバ

監査ログ専用イベントサーバのイベントデータベースに格納されている監査ログを，JP1 イベントとして収集し，監査ログ管理サーバのデータベース（**監査ログ管理データベース**）で一元管理します。

(2) 監査ログ収集対象サーバ

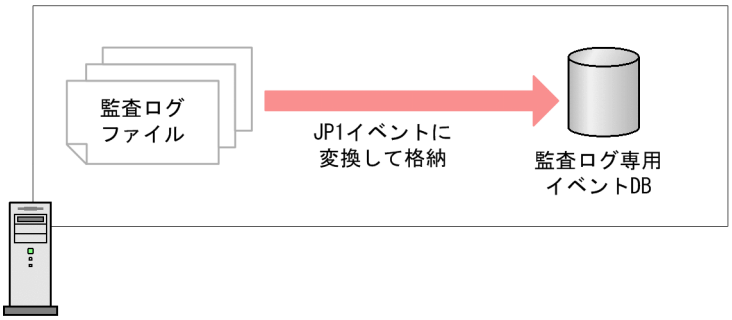
監査ログ収集対象プログラムからファイルに出力される監査ログ，Windows イベントログに出力される監査ログ，および UNIX システムログは，自動的に監査ログ専用イベントサーバのイベントデータベースに格納されます。

ファイルに出力される監査ログ

ファイルに出力される監査ログは，JP1/Base のログファイルトラップ機能によって，JP1 イベントに変換され，監査ログ専用イベントサーバのイベントデータベースに格納されます。

監査ログ専用サーバのイベントデータベースに格納される仕組みを次の図に示します。

図 2-3 監査ログ専用サーバのイベントデータベースに格納される仕組み



Windows イベントログに出力される監査ログ

Windows イベントログに出力される監査ログは，JP1/Base のイベントサーバ（物理イベントサーバ）のイベントデータベースに格納されます。

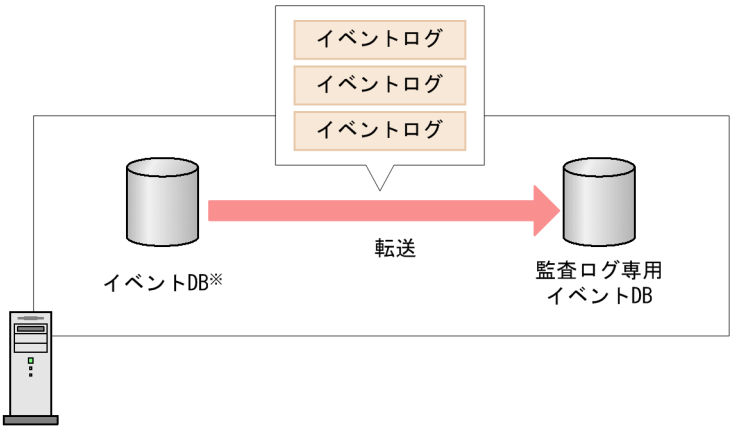
Windows イベントログに出力される監査ログを次に示します。

- Windows イベントログ
- Oracle のログ
- Hitachi Storage Command Suite のログ（Windows の場合）

これらのログは，JP1/Base のイベントサーバのイベントデータベースから監査ログ専用イベントサーバへ転送が必要になります。監査ログ専用イベントサーバへの転送設定をすることで，JP1/Base のイベントログトラップ機能によって，イベントサーバ（物理イベントサーバ）のイベントデータベースから，監査ログ専用イベントサーバのイベントデータベースに転送されます。

このイベント転送の仕組みを次の図に示します。

図 2-4　イベント転送の仕組み



注※　JP1/Baseのイベントサーバ（物理イベントサーバ）のイベントDBです。

UNIX システムログ

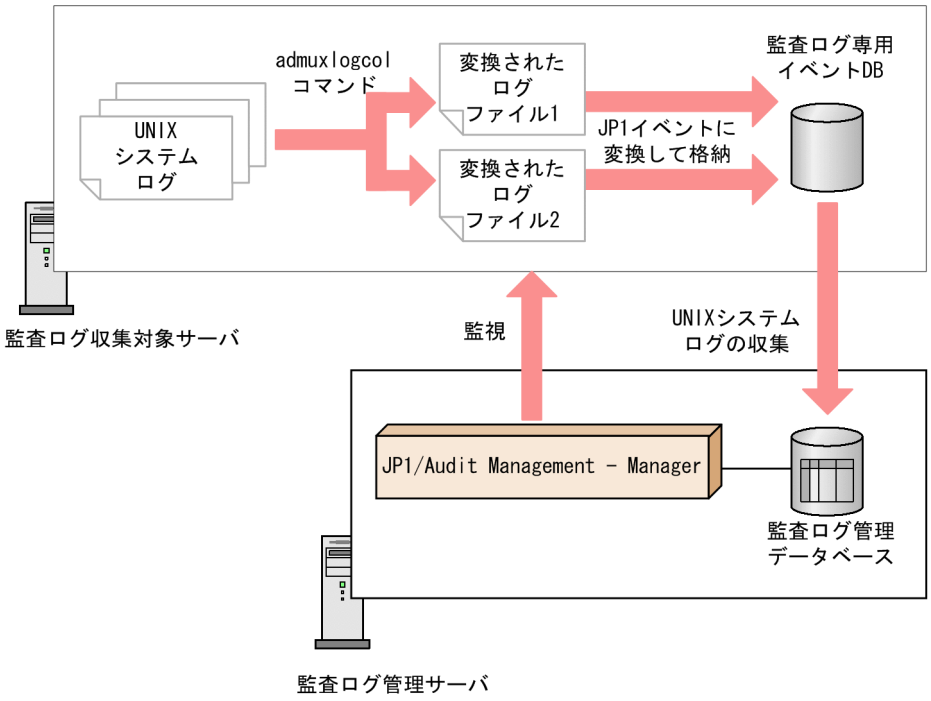
ユーザの操作としてログイン・ログアウトなどの事象が発生すると，UNIX システムログに成功や失敗などの情報が出力されます。出力された UNIX システムログの情報は，JP1/Audit Management - Manager が提供する admuxlogcol コマンドによって，監査ログの統一フォーマットに従った形式に変換されます。その後，変換されたログは，JP1/Base のログファイルトラップ機能によって，JP1 イベントに変換され，監査ログ専用イベントサーバのイベントデータベースに格納されます。

監査ログ専用イベントデータベースに格納された UNIX システムログの情報は，監査ログ収集マネージャで JP1/Audit Management - Manager の収集対象に設定することで，監査ログとして収集できるようになります。

監査ログとして収集する前に，UNIX システムログを変換しておく必要があるため，定期的に admuxlogcol コマンドが実行されるように cron へ登録してください。また，admuxlogcol コマンドが実行されるタイミングは，監査ログを収集するタイミングに合わせることをお勧めします。

UNIX システムログが収集される仕組みを次の図に示します。

図 2-5　UNIX システムログが収集される仕組み



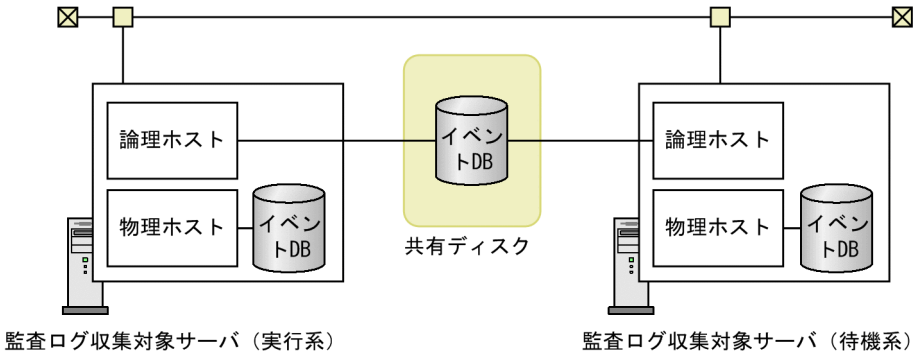
JP1/Base のイベントログトラップ機能およびログファイルトラップ機能については，マニュアル「JP1/Base 運用ガイド」を参照してください。

(a)　クラスタ環境の場合

監査ログ収集対象サーバをクラスタ環境で運用している場合も，基本的な仕組みはクラスタ環境で運用していない場合と同様ですが，さらに次のような仕組みになっています。

- ローカルディスクに出力される監査ログ，および共有ディスクに出力される監査ログを収集できます。
- ローカルディスク上に監査ログが存在する場合は物理ホストで収集し，共有ディスク上に監査ログが存在する場合は論理ホスト経由で収集します。
- 共有ディスク上の監査ログを収集している場合に，実行系サーバから待機系サーバにフェールオーバーするときは，実行系サーバでの監査ログの収集が停止され，待機系サーバで監査ログの収集が開始されます。その間に出力された監査ログについては収集できません。

図 2-6　クラスタ環境での監査ログ収集の仕組み（監査ログ収集対象サーバ）



2.2.2　監査ログの収集タイミング

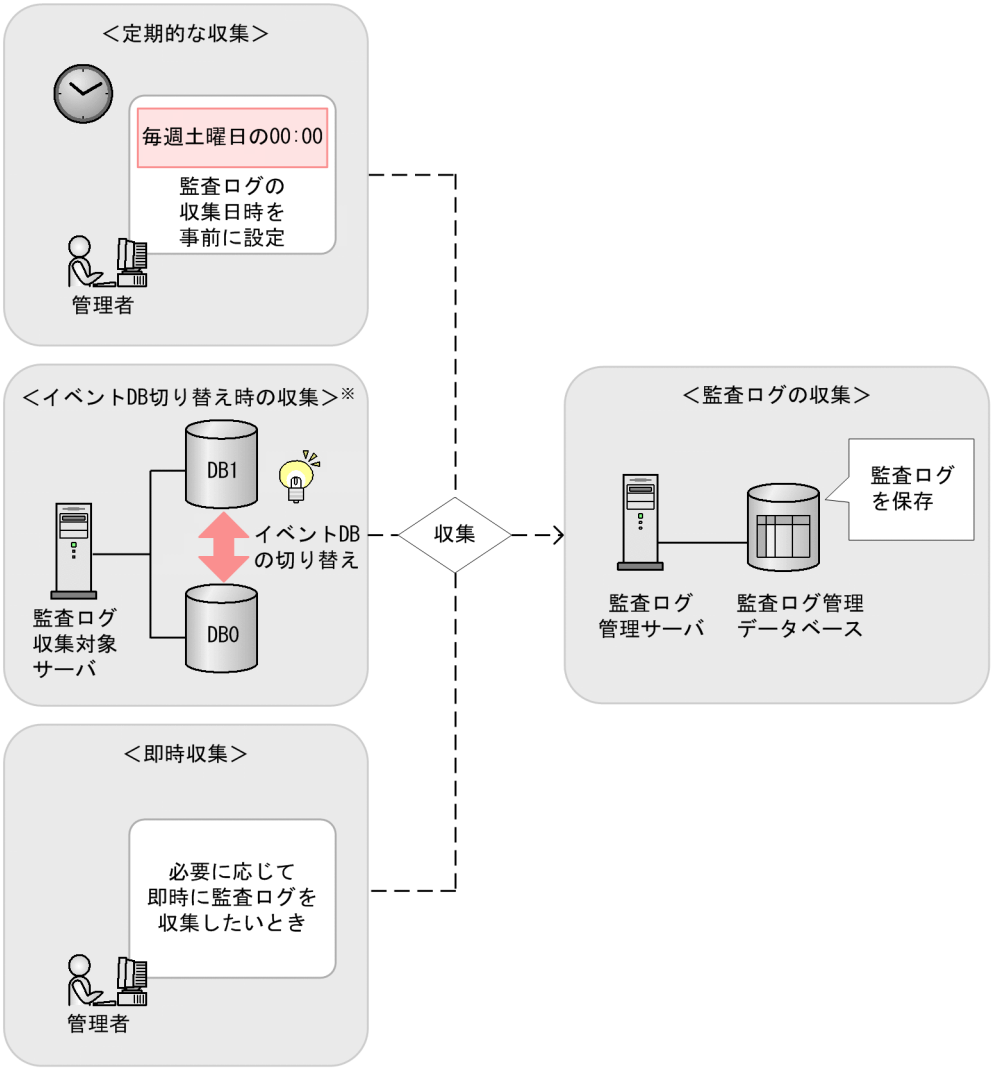
監査ログの収集タイミングには，定期的な収集，監査ログ専用イベントデータベース切り替え時の収集，および即時収集の 3 種類があります。どれかの条件に該当したときに，監査ログの収集が開始されます。

ただし，JP1/Audit Management - Manager のサービス停止中は，監査ログを収集できません。監査ログ収集対象サーバのイベントデータベースの容量を十分に確保してください。イベントデータベースの容量を十分に確保できない場合および JP1/Audit Management - Manager のサービス停止中に，イベントデータベースの切り替えが発生したタイミングで監査ログを収集する必要がある場合は，［マネージャセットアップ］ダイアログで「監査ログ収集情報」を設定してください。

監査ログ収集では，管理サーバの負荷を軽減するため，各監査ログ収集対象サーバで出力された監査ログをリアルタイムで収集するのではなく，監査ログ管理サーバ側から各監査ログ収集対象サーバに対して定期的または即時的な収集をするようにしています。このため，監査ログ収集対象サーバの停止などで監査ログを収集できなかった場合，次回の収集タイミングで収集されます。

監査ログの収集タイミングを次の図に示します。

図 2-7　監査ログの収集タイミング



注※　監査ログ専用イベントデータベース切り替え時の収集

定期的な収集

管理者があらかじめ設定した収集日時に従って，監査ログ収集対象サーバから監査ログを定期的に自動で収集します。

毎週土曜日の 00:00 のように，曜日と分単位の時間で設定できます。監査ログを毎日決まった時間に収集するように設定することもできます。

収集日時の設定は，JP1/Audit Management - Manager で監査ログの収集対象を設定したあとに実施します。収集日時の設定については「5.6.5　監査ログを定期的に収集する」を参照してください。

監査ログ専用イベントデータベース切り替え時の収集

イベントデータベースの切り替えを実施したことを知らせる JP1 イベントが，監査ログ収集対象サーバから監査ログ管理サーバへ転送されてきた場合に，監査ログ収集対象サーバから監査ログを収集します。

イベントデータベースの切り替えについては，マニュアル「JP1/Base 運用ガイド」を参照してください。

なお，JP1/Audit Management - Manager サービスの停止中に，イベントデータベース切り替えが発生した場合，収集した監査ログを退避することで監査ログの収集漏れを防ぐことができます。

即時収集

監査ログ収集対象サーバから監査ログを手動で収集できます。

必要に応じ，管理者の判断で即時に監査ログを収集したいときに実施してください。収集方法には，監査ログ収集マネージャを使用して収集する方法と admcoldata コマンドを実行して収集する方法があります。詳細については「9.3.7　監査ログを即時に収集する」を参照してください。

2.2.3　監査ログの収集カテゴリ

監査証跡管理システムでは，監査ログは次の表に示すカテゴリで収集されます。

表 2-2　監査ログの収集カテゴリ

項番	カテゴリ	説明
1	StartStop	ソフトウェアの起動と終了を示す事象です。 主な事象の例を次に示します。 • ソフトウェアの起動と終了 • サービスの起動と停止
2	Authentication	管理者やユーザが，接続・認証を試みて成功・失敗したことを示す事象です。 主な事象の例を次に示します。 • ログインまたはログアウト • 管理者またはエンドユーザ認証
3	AccessControl	管理者やユーザが，管理リソースまたはセキュリティリソースへのアクセスを試みて成功・失敗したことを示す事象です。 主な事象の例を次に示します。 • 日立オープンミドルウェア製品のアクセスコントロール • 管理者またはエンドユーザのアクセスコントロール
4	ConfigurationAccess	管理者が許可された運用操作を実行し，操作が正常終了・失敗したことを示す事象です。 主な事象の例を次に示します。 • 構成情報の参照・更新 • アカウントの追加や削除などのアカウント設定の更新 • セキュリティ設定の参照・更新 • 監査ログ設定の参照・更新
5	Failure	ソフトウェアの異常を示す事象です。 主な事象の例を次に示します。 • ソフトウェア障害（メモリエラーなど）
6	LinkStatus	機器間のリンク状態を示す事象です。 主な事象の例を次に示します。 • イーサネットの Link Up・Link Down

項番	カテゴリ	説明
7	ExternalService	日立オープンミドルウェア製品と外部サービスとの通信結果を示す事象です。 主な事象の例を次に示します。 • データベースや LDAP などとの通信 • 管理サーバとの通信 • 日立オープンミドルウェア製品が提供するサービス
8	ContentAccess	重要なデータへのアクセスを試みて成功・失敗したことを示す事象です。 主な事象の例を次に示します。 • 日立オープンミドルウェア製品上の重要なファイル（ユーザデータ）へのアクセス
9	Maintenance	管理者や保守員が保守操作を実行し，操作が正常終了・失敗したことを示す事象です。 主な事象の例を次に示します。 • ソフトウェアのインストール，アンインストール，バージョンアップの発生 • ソフトウェアの構成変更
10	AnomalyEvent	しきい値オーバーなどの異常が発生したことを示す事象です。 主な事象の例を次に示します。 • ネットワークトラフィックのしきい値オーバー • CPU 負荷のしきい値オーバー • 監査ログの上限到達前通知やラップアラウンド
		異常な通信の発生を示す事象です。 主な事象の例を次に示します。 • 通常使用するポートへの SYN flood やプロトコル違反 • 未使用ポートへのアクセス（ポートスキャンなど）
11	ManagementAction	プログラムの重要なアクションの実行を示す事象や，ほかの監査カテゴリを契機とし実行するアクションを示す事象です。 主な事象の例を次に示します。 • セキュリティ事象に対するアラーム機能に関連づけられたアクション（管理者への通知など）の実行

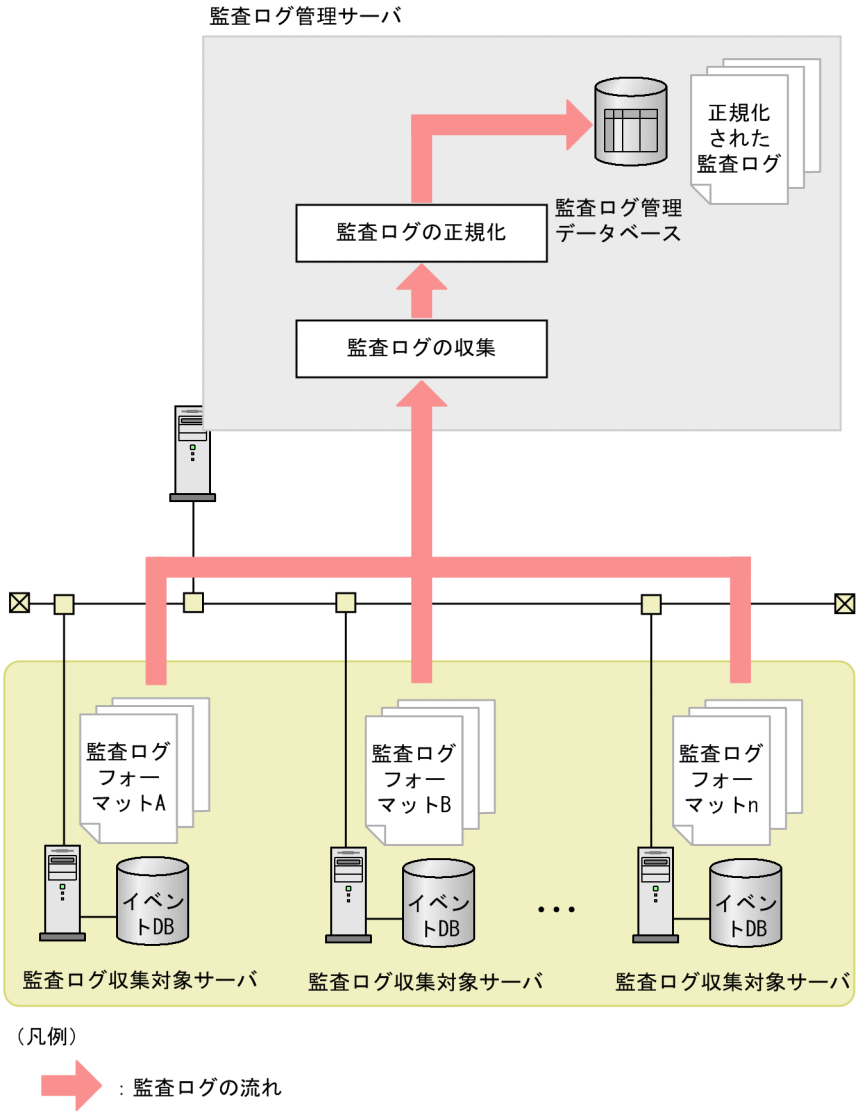
2.2.4　監査ログの正規化

監査ログ収集対象サーバのプログラムから出力される監査ログの出力形式を，JP1/Audit Management - Manager の監査ログ管理データベースに格納できる形式に変換することを**監査ログの正規化**といいます。

監査ログ管理サーバでは，監査ログ収集対象サーバに蓄積された監査ログを収集し，収集した監査ログを正規化します。その後，正規化した監査ログを監査ログ管理データベースに格納することで，一元管理を実現します。

監査ログの正規化の概念を次の図に示します。

図 2-8　監査ログの正規化の概念



(1)　正規化ルールファイル

JP1/Audit Management - Manager では，監査ログ収集対象サーバから収集した監査ログを正規化するために，定義ファイル群を提供しています。この定義ファイル群を**正規化ルールファイル**と呼びます。

監査証跡管理システムがサポートしている JP1/AJS3 - Manager や JP1/NETM/DM などの監査ログ収集対象プログラムは，正規化ルールファイルが自動的に適用されています。監査証跡管理システムがサポートしている監査ログ収集対象プログラムについては「1.2.1　内部統制の証跡記録の一元管理」を参照してください。

提供している正規化ルールファイルを次に示します。

統一フォーマット用の正規化ルールファイル

日立オープンミドルウェア製品の監査ログを正規化するための標準定義ファイルです。UNIX のシステムログに関する情報を監査ログとして正規化するための定義ファイルとしても使用します。

JP1/AJS 製品ログ用の正規化ルールファイル

JP1/AJS の製品ログを監査ログとして正規化するための定義ファイルです。

JP1/AJS の製品ログを正規化して監査ログにすると，日時やメッセージ ID などの情報が先頭に追加され，JP1/AJS の製品ログ形式を変えずに固有情報として転記されます。

JP1/AJS のログ種別が A001 の場合の例を次に示します。

JP1/AJS の製品ログの情報：

A001△日付△時刻△［プロセスID］△KAVS0200-I△スケジューラサービス名

監査ログとして正規化された情報：

日時：日付＋時刻

メッセージ ID：KAVS0200-I

プロセス ID：プロセスID

固有情報：A001△日付△時刻△[プロセスID]△KAVS0200-I△スケジューラサービス名

なお，JP1/AJS のスケジューラログでは，年の情報が出力されていない場合があります。この場合，次の方法で年の情報を追加して正規化します。

- ログ中の月＜＝ログ取得の月：「取得した時点の年」の情報追加
- ログ中の月＞ログ取得の月：「取得した時点の年 - 1」の情報追加

  例えば，ログ中の月が 12 月で，2007 年 1 月に取得した場合，2006 年 12 月として情報が追加されます。

正規化ルールエディタで定義した製品用の正規化ルールファイル

正規化ルールエディタで正規化ルールを定義した場合に使用する定義ファイルです。

Windows イベントログ用の正規化ルールファイル

Windows イベントログに出力されるログを監査ログとして正規化するための定義ファイルです。JP1/Audit Management - Manager ではログオン イベントおよびアカウント管理のイベントを標準サポートしています。

なお，標準サポートしていない Windows イベントログを監査ログとして正規化する場合は，この正規化ルールファイルを編集して正規化ルールを定義します。

ほかの JP1 シリーズ製品，日立オープンミドルウェア製品，またはその他のプログラムなど，監査証跡管理システムで標準サポート外となっているプログラムが出力する監査ログについては，正規化ルールを定義する必要があります。

出力する監査ログについて，正規化ルールを定義する必要があるプログラムや OS のことを，このマニュアルでは**標準サポート外のプログラム**と呼びます。標準サポート外のプログラムは，次に示すどちらかの方法で正規化ルールを定義してください。

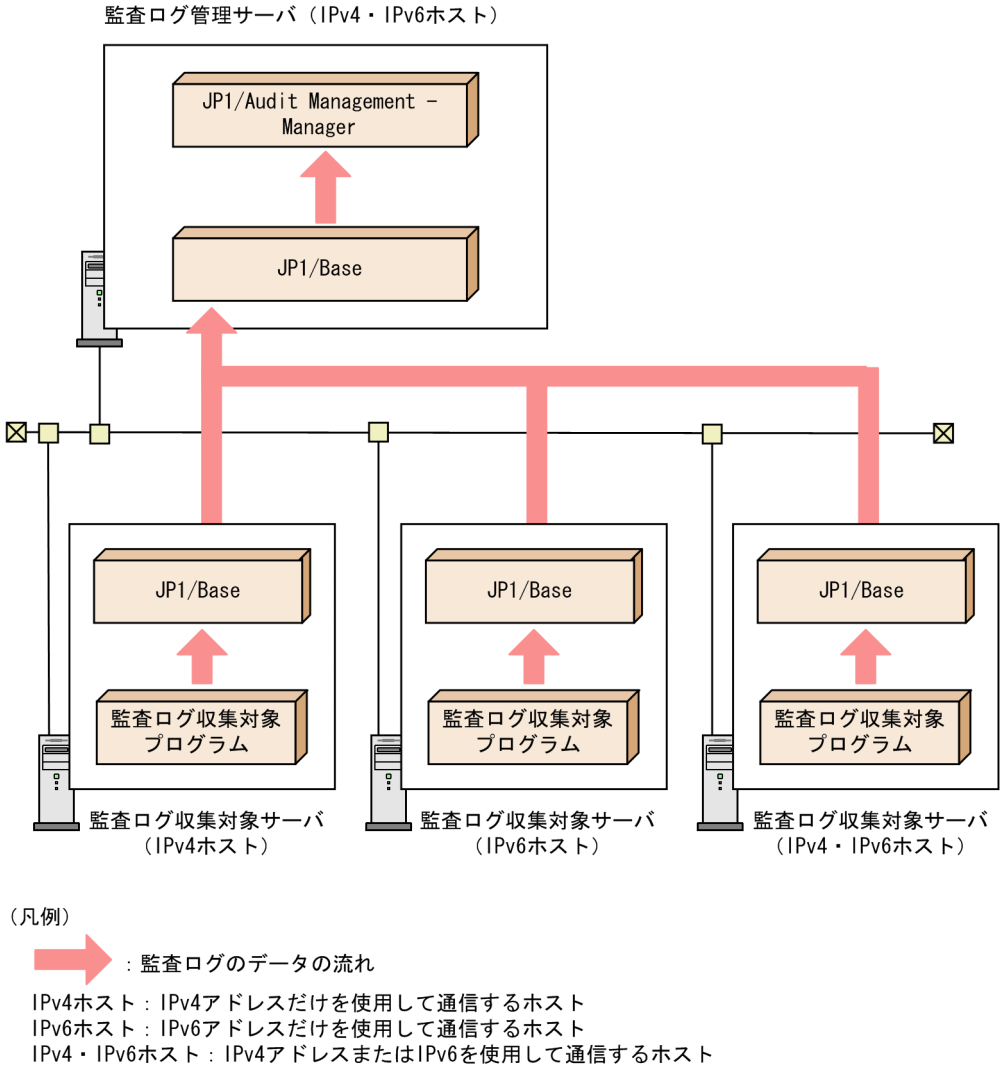
- 正規化ルールエディタで定義する
- 正規化ルールファイルで定義する

正規化ルールの定義については「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。

2.2.5　IPv6 環境での監査ログの収集

監査証跡管理システムは，IPv6 アドレスを使用して通信する監査ログ収集対象サーバの監査ログも，収集できます。

図 2-9　IPv6 環境での監査ログの収集

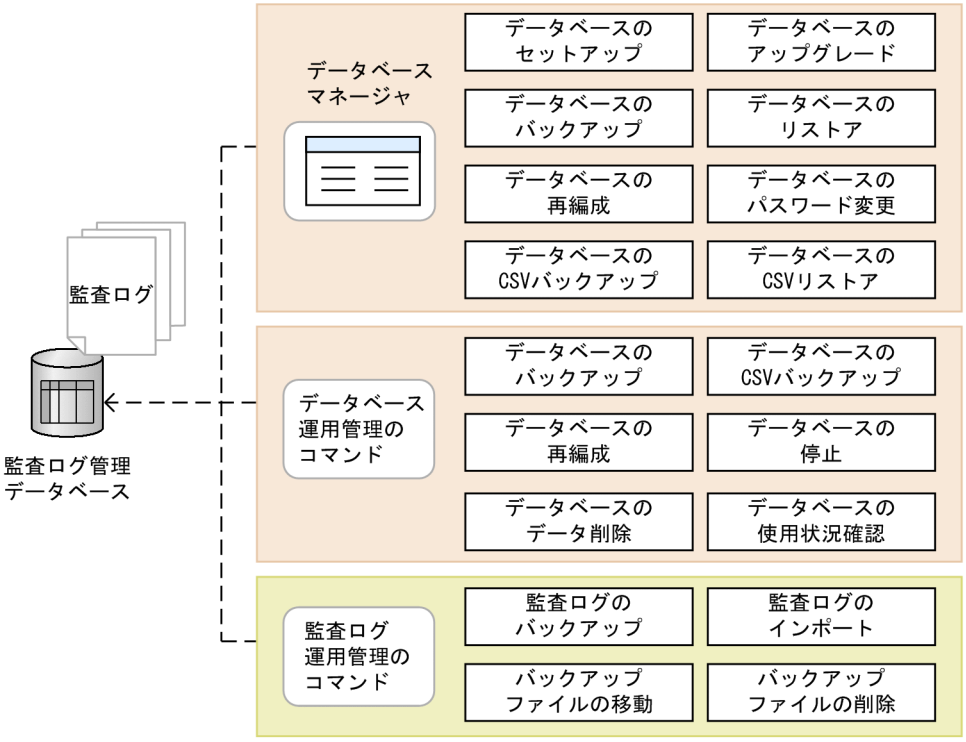


2.3　監査ログの一元管理

監査ログの一元管理は，JP1/Audit Management - Manager に組み込まれているデータベースを使用して実施します。このデータベースを，**監査ログ管理データベース**と呼びます。

監査ログ管理データベースの機能の概要を次の図に示します。

図 2-10　監査ログ管理データベースの機能の概要



監査ログ管理データベースは，データベースマネージャおよびコマンドで管理します。また，監査ログ管理データベースで管理している監査ログは，コマンドで管理します。

2.3.1　データベースマネージャを使用した管理

JP1/Audit Management - Manager は，監査ログ管理データベースを管理するためのコンポーネントとして，データベースマネージャを提供しています。このデータベースマネージャで，データベースの構築やメンテナンスを実施します。

データベースマネージャの機能を次に示します。

データベースのセットアップ

データベースをセットアップします。データベースのサイズは，使用環境に合わせて LL サイズ，L サイズ，M サイズ，および S サイズの四つから選択できます。

データベースのバックアップ

データベースのバックアップファイルを取得します。

データベースにトラブルが発生した場合やシステムが壊れた場合などに備えて，定期的にデータベースのバックアップを実施することをお勧めします。

データベースのバックアップはオフラインモードのフルバックアップだけをサポートします。オンラインバックアップや差分バックアップはサポートしていませんので注意してください。

なお，この作業は admdbbackup コマンドを使用しても実施できます。

admdbbackup コマンドについては「12.　コマンド」の「admdbbackup（データベースのバックアップ）」を参照してください。

データベースのアップグレード

JP1/Audit Management - Manager を新しいバージョンに上書きインストールするときに，既存のデータを保持したまま，データベースを最新の状態にアップグレードします。

データベースのリストア

データベースのバックアップで取得したバックアップファイルをデータベースにリストアして，データベースを復元します。

データベースの再編成

データベースを再編成します。

データベースを運用し続けると，データの格納効率が悪くなり検索性能が低下することがあります。性能低下を防ぐため，1 か月に 1 回を目安にデータベースの再編成を実施することをお勧めします。

なお，この作業は admdbrorg コマンドを使用しても実施できます。

admdbrorg コマンドについては「12.　コマンド」の「admdbrorg（データベースの再編成）」を参照してください。

データベースのパスワード変更

データベースとの接続に使用するパスワードを変更します。

データベースの CSV バックアップ

データベースのバックアップファイルを取得します。

データベース内のデータを別サーバに移行したい場合や，データベースのサイズを変更したい場合に，データベースに格納されている全データを CSV 形式ファイルでバックアップします。

なお，この作業は admdbexport コマンドを使用しても実施できます。

admdbexport コマンドについては「12.　コマンド」の「admdbexport（データベースの CSV バックアップ）」を参照してください。

データベースの CSV リストア

データベースの CSV バックアップで取得した CSV 形式ファイルをデータベースにリストアして，データベースを復元します。

データベースのセットアップ方法については「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照してください。また，データベースのメンテナンス方法については「10.　データベースのメンテナンス」を参照してください。

2.3.2 データベースのコマンドを使用した管理

JP1/Audit Management - Manager では，監査ログ管理データベースを管理するためのコマンドを提供しています。このコマンドで，データベースのバックアップや再編成などを実施します。

データベースのコマンドの機能を次に示します。

admdbbackup（データベースのバックアップ）

データベースのバックアップファイルを取得します。

データベースにトラブルが発生した場合やシステムが壊れた場合などに備えて，定期的にデータベースのバックアップを実施することをお勧めします。

なお，この作業はデータベースマネージャのデータベースのバックアップを使用しても実施できます。また，データベースのバックアップで取得したバックアップファイルをデータベースにリストアする場合には，データベースマネージャのデータベースのリストアを使用してください。

admdbexport（データベースの CSV バックアップ）

データベースのバックアップファイルを取得します。

データベース内のデータを別サーバに移行したい場合や，データベースのサイズを変更したい場合に，データベースに格納されている全データを CSV 形式ファイルでバックアップします。

なお，この作業はデータベースマネージャのデータベースの CSV バックアップを使用しても実施できます。また，データベースの CSV バックアップで取得した CSV 形式ファイルをデータベースにリストアする場合には，データベースマネージャのデータベースの CSV リストアを使用してください。

admdbrorg（データベースの再編成）

データベースを再編成します。

データベースを運用し続けると，データの格納効率が悪くなり検索性能が低下することがあります。性能低下を防ぐため，1 か月に 1 回を目安にデータベースの再編成を実施することをお勧めします。

なお，この作業はデータベースマネージャのデータベースの再編成を使用しても実施できます。

admdbstop（データベースの停止）

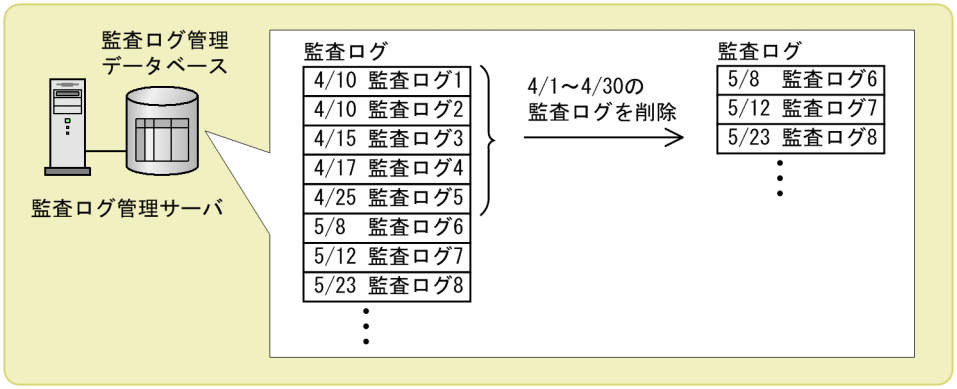
クラスタ環境で，データベースを停止します。

admdbdelete（データベースのデータ削除）

データベースに格納されている監査ログを，日時を指定して削除します。

admdbdelete コマンドの概念を次の図に示します。

図 2-11　admdbdelete コマンドの概念



監査ログを収集し続けると，データベース領域の容量不足が発生することがあります。また，データベースの検索性能は格納されている監査ログの量に応じて徐々に低下します。このため，監査が完了して不要になった期間の監査ログや監査ログ閲覧サーバに移動した監査ログなどは，監査ログのバックアップを取得したあとに削除する運用をお勧めします。

admdbstat（データベースの使用状況確認）

格納されているデータの件数や領域の使用率など，データベースの使用状況を確認します。

データベースのコマンドについては「12.　コマンド」を参照してください。

2.3.3　監査ログのコマンドを使用した管理

JP1/Audit Management - Manager が提供する監査ログを管理するためのコマンドで，監査ログのバックアップや削除などを実施します。

監査ログのコマンドの機能を次に示します。

admexport（監査ログのバックアップ）

監査ログ管理データベースに格納されている監査ログのバックアップファイルをローカルディスク上の任意のフォルダに取得します。

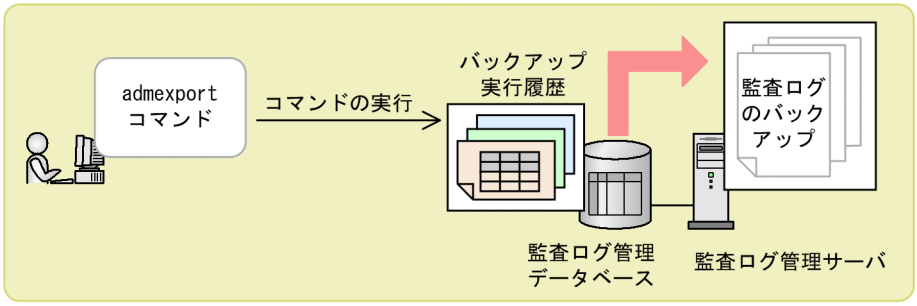
監査ログのバックアップは，監査ログの収集の期間を指定してバックアップ（期間指定バックアップ）することも，前回のバックアップから実行日前日までの差分をバックアップ（差分バックアップ）することもできます。

差分バックアップはコマンド実行時に日時を設定する必要がないため，監査ログのバックアップを自動化することができます。

監査ログのバックアップを実施すると，監査ログ管理データベース内にバックアップ実行履歴が登録されます。バックアップオプション定義ファイルを使用すると，バックアップ実行履歴にバックアップ名やコメントなどを一緒に登録できます。このバックアップ実行履歴は，監査ログ管理画面のバックアップ履歴画面から参照できます。

admexport コマンドの概念を次に示します。

図 2-12　admexport コマンドの概念



（凡例）

：監査ログのバックアップファイルの流れ

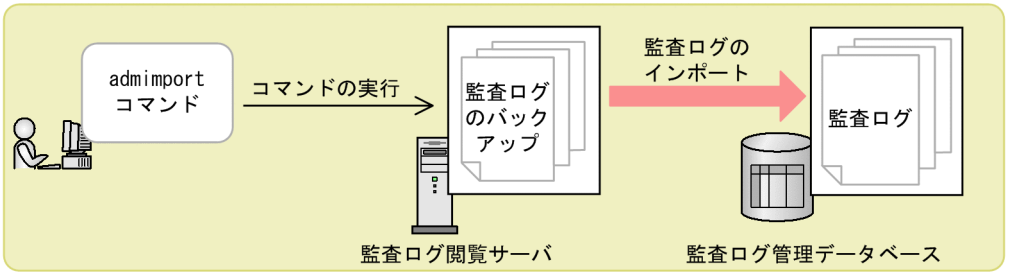
バックアップデータは，監査ログ閲覧サーバの監査ログ管理データベースにインポートして，監査ログ閲覧サーバの監査ログ管理画面から検索や集計などの監査業務を実施できます。また，任意のツールに取り込んで利用することもできます。

admimport（監査ログのインポート）

監査ログのバックアップで取得した CSV 形式ファイルを監査ログ閲覧サーバの監査ログ管理データベースにインポートします。

admimport コマンドの概念を次の図に示します。

図 2-13　admimport コマンドの概念



（凡例）

：監査ログの流れ

監査ログ閲覧サーバでは，監査ログ管理サーバと同様に，インポートした監査ログを基に，監査ログ閲覧サーバの監査ログ管理画面から，検索や集計などの監査業務を実施できます。

なお，監査ログ閲覧サーバにインポートするための監査ログのバックアップファイルは，監査ログ管理画面のバックアップ履歴画面からダウンロードすることができます。

admcsvmove（監査ログのバックアップファイルの移動）

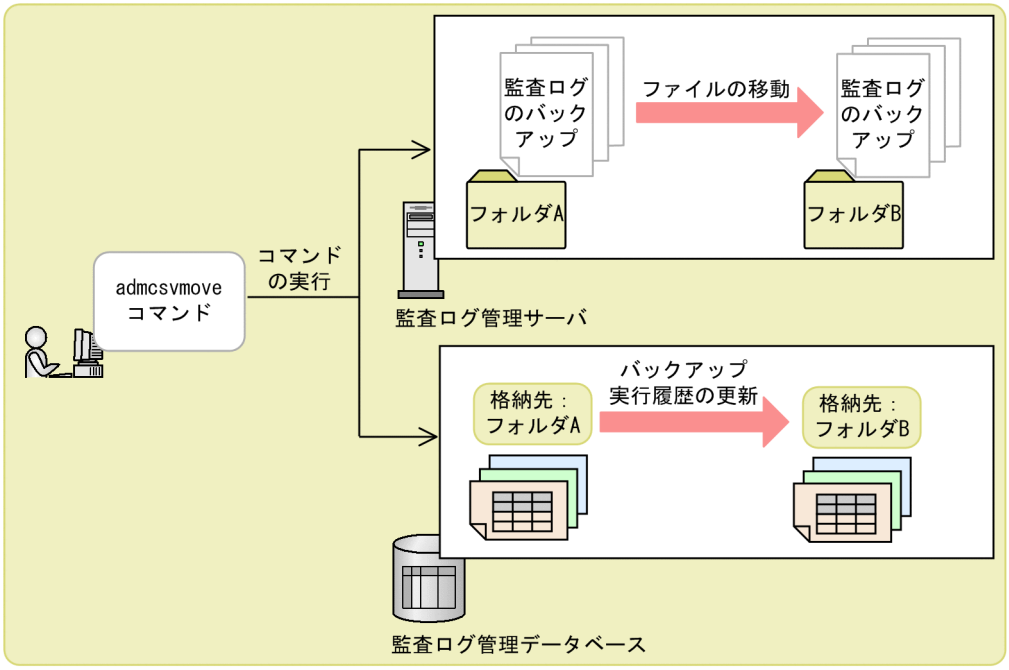
監査ログのバックアップで取得した監査ログのバックアップファイルを，同一サーバ内で移動します。

監査ログのバックアップファイルの格納先フォルダを変更したい場合やファイル名を変更したい場合に，このコマンドを使用します。

ファイルの移動が完了した時点で，監査ログ管理データベースで管理されている監査ログのバックアップ実行履歴の格納先フォルダやファイル名などの情報が更新されます。バックアップオプション定義ファイルを使用すると，バックアップ実行履歴にバックアップ名やコメントなどを一緒に登録できます。

admcsvmove コマンドの概念を次の図に示します。

図 2-14　admcsvmove コマンドの概念



（凡例）

：監査ログまたはバックアップ実行履歴の流れ

注意事項

監査ログのバックアップファイルの格納先フォルダやファイル名を変更する場合には，必ず admcsvmove コマンドを使用してください。

監査ログのバックアップファイルの格納先フォルダやファイル名を，Windows のエクスプローラや他ツールを利用して変更した場合，バックアップ実行履歴で管理されているファイル名と実ファイル名が不一致となり，監査ログ管理画面のバックアップ履歴画面からファイルのダウンロードができなくなります。

admcsvremove（監査ログのバックアップファイルの削除）

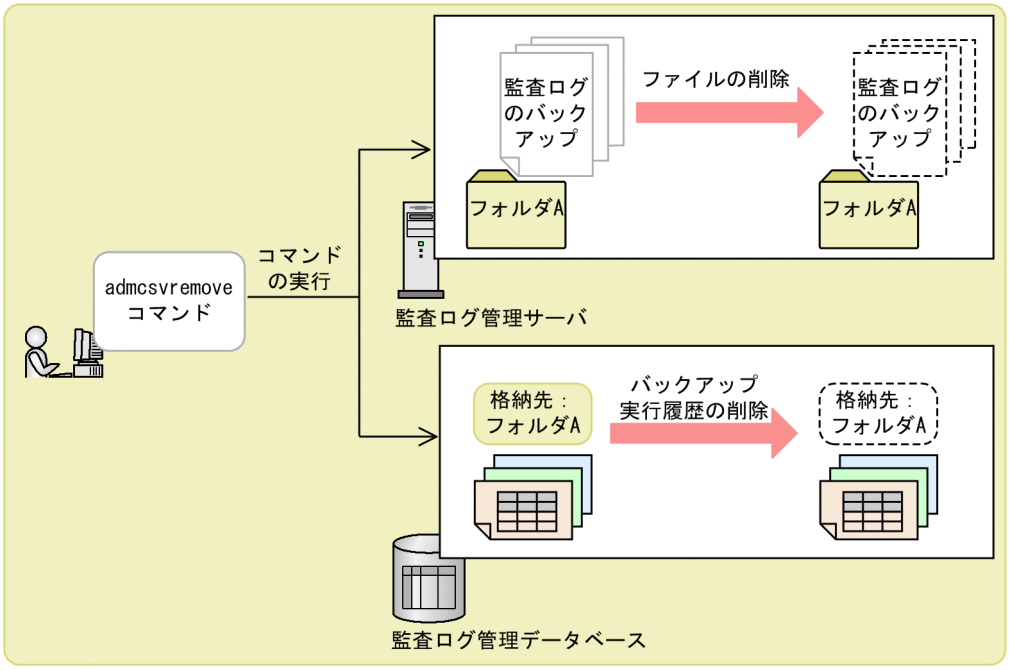
監査ログのバックアップで取得した監査ログのバックアップファイルとそのバックアップ履歴を削除します。

削除するバックアップファイルは，バックアップファイル名またはバックアップ ID で指定します。バックアップ ID は，監査ログ管理画面のバックアップ履歴確認画面で確認できます。

監査ログ管理データベースにバックアップファイルはなく，バックアップ履歴だけが残っている場合は，バックアップ履歴の情報を削除します。

admcsvremove コマンドの概念を次の図に示します。

図 2-15　admcsvremove コマンドの概念



（凡例）

：監査ログまたはバックアップ実行履歴の流れ

：削除情報

注意事項

監査ログのバックアップファイルを削除する場合には，必ず admcsvremove コマンドを使用してください。

監査ログのバックアップファイルを，Windows のエクスプローラやほかツールを利用して削除した場合，バックアップ履歴は削除されません。そのため，削除したバックアップファイルと同じファイル名ではバックアップができなくなります。

監査ログのコマンドについては「12.　コマンド」を参照してください。

2.4　JP1/Base のユーザ管理機能を使ったユーザ管理

監査証跡管理システムでは，JP1/Base のユーザ管理機能で，JP1 ユーザによるユーザ認証やアクセス制御を実施します。

JP1/Base のユーザ管理機能には，次に示す機能があります。

- ユーザ認証
- アクセス制御

ここでは，各ユーザ管理機能の概要について説明します。各ユーザ管理機能の詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

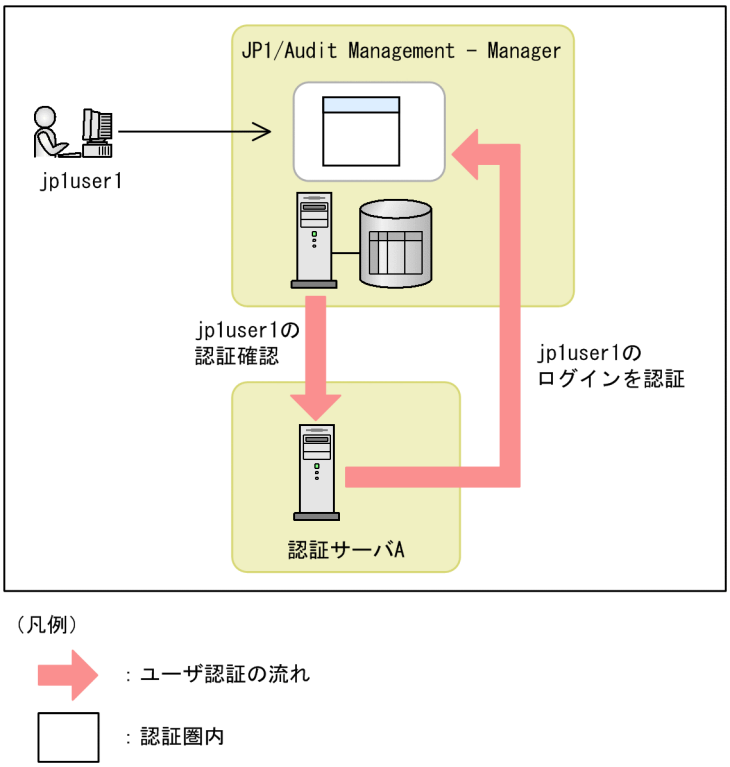
2.4.1　ユーザ認証

監査証跡管理システムでは，Web ブラウザから JP1/Audit Management - Manager の監査ログ管理画面にアクセスして監査ログの調査や監査を実施します。不正なユーザによるアクセスを防止するために，JP1/Audit Management - Manager のログオン時に，JP1/Base のユーザ認証機能によってユーザ認証を行います。

ユーザ認証をする JP1/Base を**認証サーバ**と呼びます。また，ユーザ認証に同一の認証サーバを参照しているサーバの集まりを**認証圏**と呼びます。

ユーザ認証の概念を次の図に示します。

図 2-16　ユーザ認証の概念



2.4.2　アクセス制御

JP1/Audit Management - Manager に対して JP1 ユーザがどのような操作ができるかを特定する操作権限のレベルを JP1 ユーザごとに設定します。この操作権限のレベルを **JP1 権限レベル**と呼びます。

JP1 権限レベルには，次の 2 種類があります。

表 2-3　JP1 権限レベル

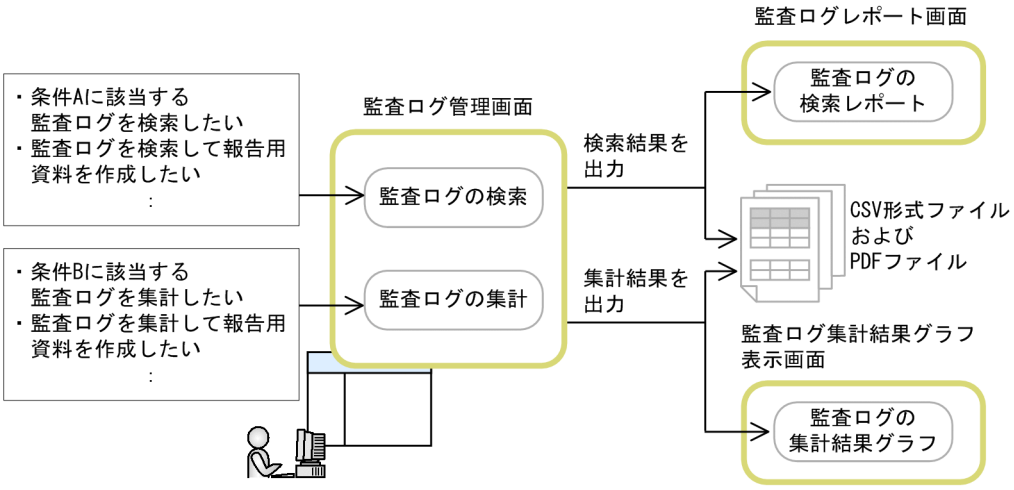
項番	JP1 権限レベル	説明
1	JP1_Audit_Admin	監査証跡管理システムの監査ログ管理画面を操作するための JP1 ユーザです。どちらも同じ JP1 権限レベルです。JP1 権限レベルを使い分ける必要がない場合は，「JP1_Audit_Admin」を使用してください。
2	JP1_Audit_Operator	

2.5　監査ログの検索と集計

監査ログ管理画面を使って，監査ログの検索と集計ができます。

監査ログの検索と集計の流れを次の図に示します。

図 2-17　監査ログの検索と集計の流れ



この節では，監査ログの検索および集計について説明します。

2.5.1　監査ログの検索

収集した監査ログを監査ログ管理画面で検索し，検索結果を一覧表示できます。また，検索結果をレポート形式で表示できます。

この機能によって，実施したい監査方法に合わせて目的の監査ログを検索し，抽出できます。検索する条件には，処理を開始した日時やプログラム名など，さまざまな条件を指定できます。監査方法に合わせて任意の条件を指定してください。

指定した検索条件は，監査証跡管理システムにログインするユーザごとに検索パターンとして保存できます。また，監査ログ検索画面には，テンプレートの検索パターンが用意されています。検索パターンを使用することで，検索条件の入力作業を簡略化し，効率的な検索ができます。

検索パターンは，次のどちらかで指定できます。

- 監査ログ管理画面左フレームの機能ツリーのメニューで選択します。
- 監査ログ検索画面のリストボックスで選択します。

なお，一度検索パターンとして保存した検索条件は変更や削除ができますが，テンプレートの検索パターンは変更も削除もできません。

監査ログの検索結果を，CSV 形式ファイルまたは PDF ファイルに出力できます。出力したファイルには，結果のほかに検索したときに指定した条件も出力されます。ファイルは一定のフォーマットで出力されるので，定期的に出力して分析し，報告用資料を作成するのに便利です。また，検索結果を監査ログレポートとして表示することもできます。監査ログレポート画面では，レポート形式で検索結果の固有情報などが見やすく編集されています。

2.5.2　監査ログの集計

収集した監査ログを監査ログ集計画面で集計し，集計結果を一覧表示できます。また，集計結果をグラフで表示できます。

この機能によって，どのプログラムでどの処理が頻繁に行われているか，どのサーバでどれだけエラーが起きているかなどを集計できます。集計する条件は，処理を開始した日時やプログラム名など，さまざまな条件を指定できます。監査方法に合わせて任意の条件を指定してください。

指定した集計条件は集計パターンとして保存できます。また，監査ログ集計画面には，テンプレートの集計パターンが用意されています。集計パターンを使用することで，集計条件の入力作業を簡略化し，効率的な集計ができます。

集計パターンは，次のどちらかで指定できます。

- 監査ログ管理画面左フレームの機能ツリーのメニューで選択します。
- 監査ログ集計画面のリストボックスで選択します。

なお，一度集計パターンとして保存した集計条件は変更や削除ができますが，テンプレートの集計パターンは変更も削除もできません。

監査ログを集計した結果を，CSV 形式ファイルまたは PDF ファイルに出力できます。出力したファイルには，結果のほかに集計したときに指定した条件も出力されます。ファイルは一定のフォーマットで出力されるので，定期的に出力して分析し，報告用資料を作成するのに便利です。また，集計結果を基に，グラフ表示することもできます。集計結果グラフ表示画面では，分類された集計結果を見やすくグラフで表示します。

2.6　監査ログの統計情報の生成と統計結果の出力

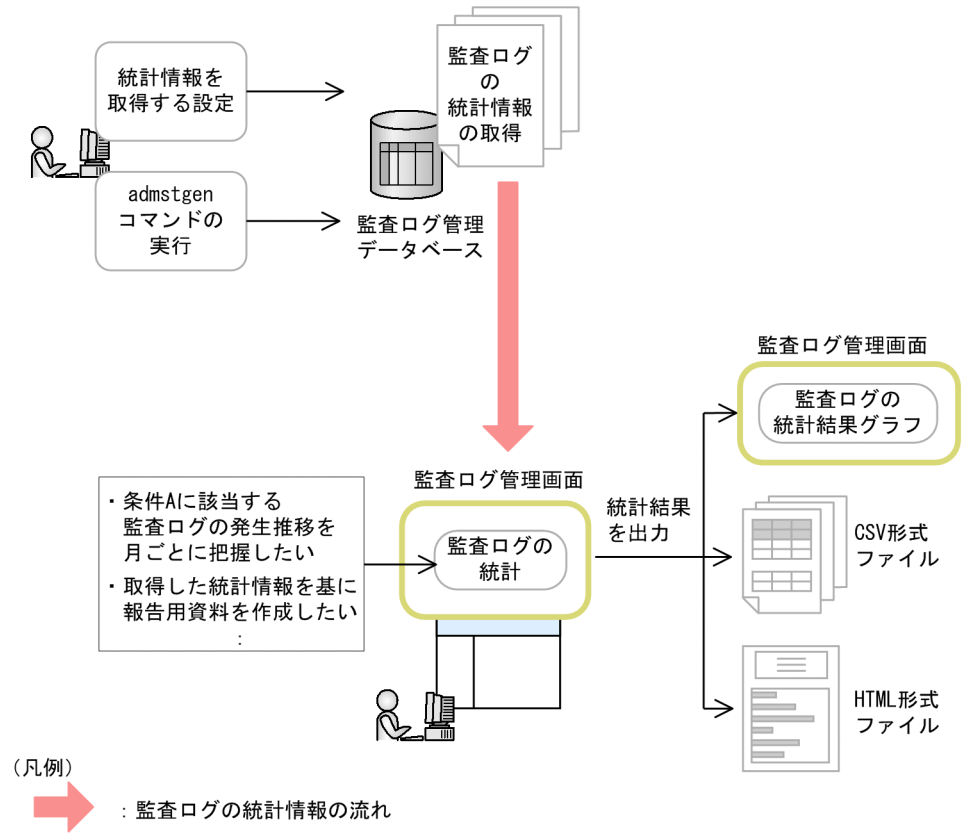
収集した監査ログを基に，統計情報を生成し，監査ログ管理画面を使って，統計結果をグラフ形式で出力できます。

この機能によって，監査ログとして出力されている事象の種別や結果について，その発生の推移を視覚的に把握できます。

なお，収集した監査ログを基に，監査ログ管理データベースに生成される統計データを**統計情報**と呼びます。また，統計情報を基に，監査ログ管理画面で条件を設定して出力するデータを**統計結果**と呼びます。統計情報は統計パターンの条件を基に生成されます。この条件のことを**統計パターン条件**と呼びます。

監査ログの統計の流れを次の図に示します。

図 2-18　監査ログの統計の流れ



統計情報は，次に示す方法で生成できます。

［マネージャセットアップ］ダイアログで設定する

［マネージャセットアップ］ダイアログの「監査ログ統計情報の収集時生成」で統計情報を生成する設定にすると，監査ログの定時収集時に統計情報を生成します。この設定にすると，定期的に統計情報を生成できます。

定時収集時に統計情報を生成する設定方法については「5.5.6(2)　［マネージャセットアップ］ダイアログの設定内容」を参照してください。

admstgen コマンドを実行する

任意の日数または日付を指定して admstgen コマンドを実行すると，コマンド実行日を起点として指定した日数分または日付以降の監査ログを基に，統計情報を生成します。

admstgen コマンドについては「12.　コマンド」の「admstgen（監査ログの統計情報生成）」を参照してください。

また，監査ログ管理データベースに生成された統計情報は，次に示す方法で削除できます。

admstdel コマンドを実行する

任意の日数または日付を指定して admstdel コマンドを実行すると，コマンド実行日を起点として指定した日数以前または日付以前の統計情報を削除します。

admstdel コマンドについては「12.　コマンド」の「admstdel（監査ログの統計情報削除）」を参照してください。

監査ログの統計情報が監査ログデータベース内に蓄積されると，データベースの容量を圧迫する要因となります。このため，不要となった監査ログの統計情報は，削除することをお勧めします。

生成した監査ログの統計情報を基に，監査ログ管理画面で，統計結果をグラフ形式で出力します。

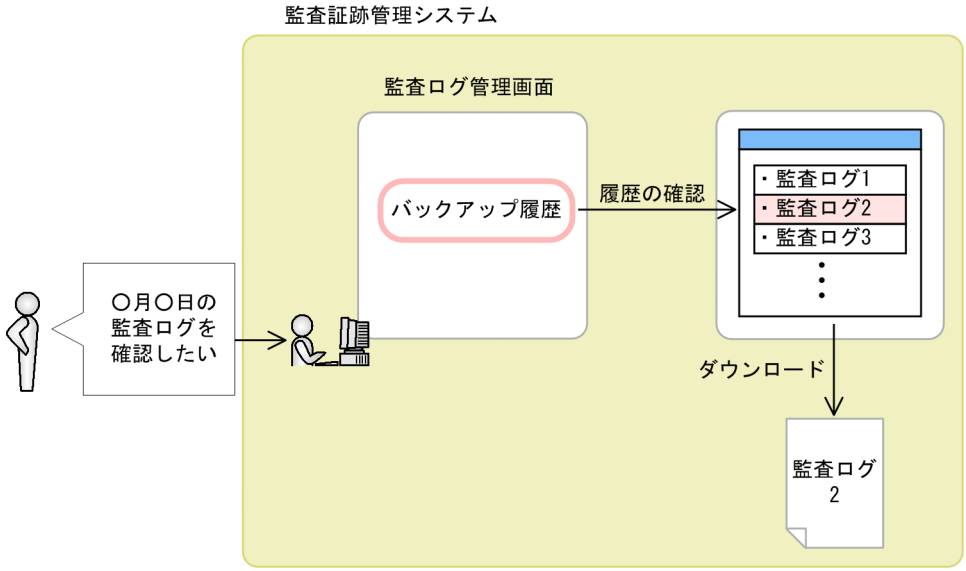
監査ログの統計結果は，CSV 形式ファイルにも出力できます。ファイルには，統計結果のほかに，統計出力条件や統計パターン条件も出力されます。また，グラフ形式で表示した統計結果は HTML 形式で出力できます。ファイルは一定のフォーマットで出力されるため，定期的に出力して分析し，報告用資料を作成するのに便利です。

2.7　監査ログのバックアップ履歴管理

監査ログ管理画面から，監査ログのバックアップ履歴一覧を表示して，過去のバックアップの実施状況やバックアップ情報を確認したり，監査ログのバックアップ実行履歴を基に，監査ログのバックアップファイルをダウンロードしたりできます。

バックアップ履歴の利用方法を次の図に示します。

図 2-19　バックアップ履歴の利用方法



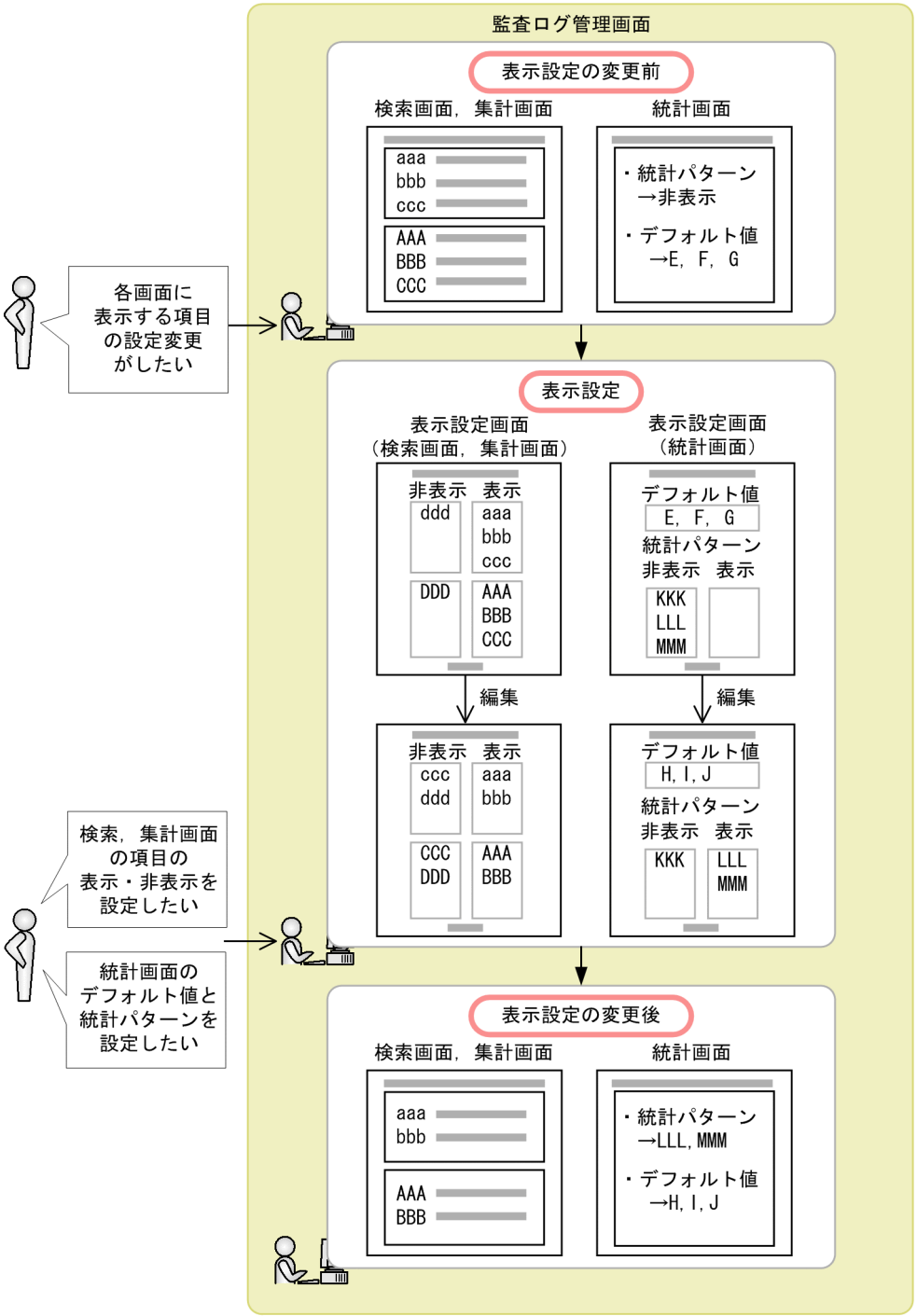
例えば，監査ログ管理画面のバックアップ履歴画面で，2007 年 4 月 8 日の監査ログのバックアップ情報について検索し，監査ログのバックアップファイルが格納されているファイル名などをバックアップ履歴一覧で確認しながら，目的のバックアップファイルをダウンロードできます。

2.8　監査ログ管理画面のカスタマイズ

監査ログ管理画面は項目の表示・非表示や表示順について変更できます。また，監査ログ統計画面で指定する統計出力条件のデフォルトについて変更することもできます。

監査ログ管理画面のカスタマイズの流れを次の図に示します。

図 2-20　監査ログ管理画面のカスタマイズの流れ



監査ログ管理画面をカスタマイズできる項目を次に示します。

- 監査ログ検索画面

  条件項目の表示・非表示と表示順，結果項目の表示・非表示と表示順，検索結果一覧で 1 ページ分として表示するレコード数，［PDF］ボタンの表示・非表示
- 監査ログ集計画面

  条件項目の表示・非表示と表示順，結果項目の表示・非表示と表示順，集計結果一覧で 1 ページ分として表示するレコード数，［PDF］ボタンの表示・非表示
- 監査ログ統計画面

  表示データ数や観点など統計出力条件のデフォルト，統計パターンの表示・非表示
- バックアップ履歴画面

  条件項目の表示・非表示と表示順，結果項目の表示・非表示と表示順，検索結果一覧で 1 ページ分として表示するレコード数

なお，それぞれのカスタマイズ項目については，初期状態に戻す（初期化）ことができます。ただし，監査ログ統計画面での統計パターンの設定内容については，初期化できません。

監査ログ管理画面のカスタマイズと初期化については「7.7　監査ログ管理画面の表示設定」を参照してください。

2.9　JP1/Audit Management - Manager の監査ログ出力

監査証跡管理システムでは，JP1/Audit Management - Manager 自体も監査ログを出力しており，ほかのサーバから出力される監査ログと同様に，監査証跡管理システムで監査ログを収集できます。

JP1/Audit Management - Manager の監査ログには，次の 2 種類があります。

- JP1/Audit Management - Manager（サーバ）が出力する監査ログ
- JP1/Audit Management - Manager の監査ログ管理画面（Web）が出力する監査ログ

JP1/Audit Management - Manager の監査ログについては「付録 D　JP1/Audit Management - Manager の監査ログの出力情報」を参照してください。

3 システム構成

この章では，監査証跡管理システムのプログラム構成，前提 OS，前提プログラム，およびシステム構成例について説明します。

3.1　プログラム構成

この節では，監査証跡管理システムを構成するサーバとクライアントのプログラム構成について説明します。

監査証跡管理システムは，次に示す三つのサーバとクライアントで構成されます。ただし，監査ログ閲覧サーバは必要に応じて構築してください。

- 監査ログ管理サーバ
- 監査ログ閲覧サーバ（任意）
- 監査ログ収集対象サーバ
- クライアント

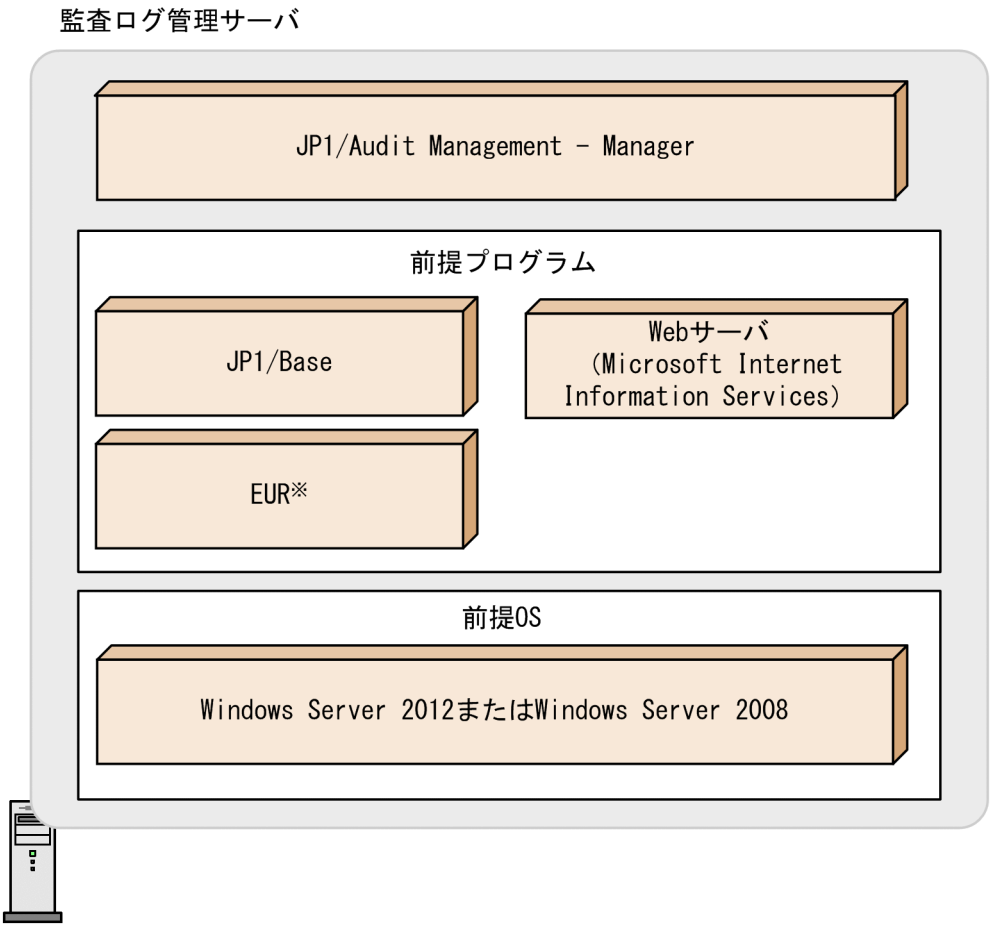
次に，プログラム構成を監査証跡管理システムの構成要素ごとに説明します。

3.1.1　監査ログ管理サーバのプログラム構成

監査ログ管理サーバは，監査証跡管理システムの主要サーバです。監査ログ収集対象サーバから監査ログを収集し，監査ログ管理サーバ上の監査ログ管理データベースで一元管理する機能を持っています。

監査ログ管理サーバのプログラム構成を次の図に示します。

図 3-1　監査ログ管理サーバのプログラム構成



注※　PDFファイルを出力する場合に必要なプログラムです。必要に応じてインストールしてください。

JP1/Audit Management - Manager

監査ログ収集対象サーバ上で運用されているプログラムが出力する監査ログを JP1/Base と連携して収集し，収集した監査ログを一元管理するプログラムです。収集した監査ログは，監査ログ管理サーバ上の監査ログ管理データベースで管理・保存します。また，監査ログの検索，集計，統計の結果を利用して，報告用資料の作成や監査業務を支援します。なお，JP1/Audit Management - Manager には，リレーショナルデータベースがあらかじめ用意されています。

前提 OS

監査ログ管理サーバは，Windows Server 2012 または Windows Server 2008 上で動作します。

前提プログラム

JP1/Base

監査証跡管理システムでは，JP1/Base のイベント変換機能によって，監査ログ収集対象サーバのイベントデータベースに蓄積された監査ログを，JP1 イベントとして取得します。取得した JP1 イベントは，監査ログ管理サーバ上の監査ログ管理データベースで一元管理されます。また，JP1/Base のユーザ管理機能によって，監査ログ管理画面へのユーザ認証やアクセス制御を実施します。JP1/Base の機能については，マニュアル「JP1/Base 運用ガイド」を参照してください。

なお，一つの監査証跡管理システムが管理する範囲は，JP1/Base の認証サーバによって管理されている一つの認証圏内です。複数の認証圏内を管理する場合は，認証サーバの数だけ監査証跡管理システムが必要となります。

Web サーバ

Web サーバには，Microsoft Internet Information Services が必要です。また，Windows コンポーネントとして WWW（World Wide Web）サービスをインストールする必要があります。

EUR

監査ログ管理画面で検索や集計した監査ログを，PDF ファイルの帳票として表示したり印刷したりする場合に必要なプログラムです。

このプログラムのインストールは任意です。必要に応じてインストールしてください。EUR の機能概要については，EUR のマニュアルを参照してください。

3.1.2 監査ログ閲覧サーバのプログラム構成

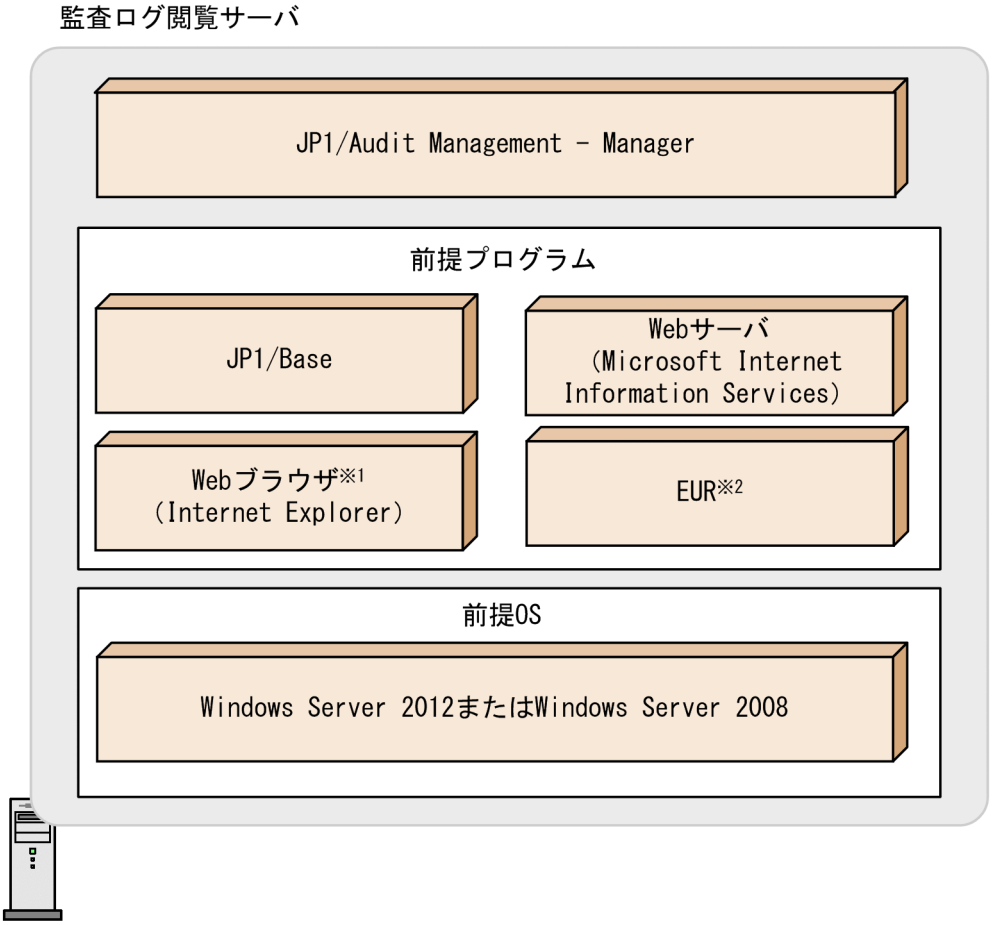
監査ログ閲覧サーバは，収集した監査ログを閲覧するための専用サーバです。監査ログ管理サーバ上の監査ログ管理データベースで一元管理されている監査ログのバックアップを監査ログ閲覧サーバ上の監査ログ管理データベースにインポートすることによって，管理・保存していた監査ログを閲覧できます。監査ログ管理サーバに蓄積された監査ログの量が膨大になったり，監査ログの保存期間が長くなったりする場合は，監査ログ閲覧サーバを構築することをお勧めします。

収集する監査ログが少ない場合や，監査ログの保存期間が短い場合には，この監査ログ閲覧サーバを構築する必要はありません。監査ログ管理サーバ上の監査ログ管理データベースで管理・保存してください。

監査ログ閲覧サーバのプログラム構成は，監査ログ管理サーバのプログラム構成と基本的に同一となります。

監査ログ閲覧サーバのプログラム構成を次の図に示します。

図 3-2　監査ログ閲覧サーバのプログラム構成



注※1　監査ログ管理画面を表示する場合に必要なプログラムです。
注※2　PDFファイルを出力する場合に必要なプログラムです。必要に応じてインストールしてください。

JP1/Audit Management - Manager

監査ログ閲覧サーバ上の JP1/Audit Management - Manager では，監査ログのバックアップを，監査ログ閲覧サーバ上の監査ログ管理データベースにインポートして閲覧できます。

また，監査ログ管理サーバと同様に，監査ログの検索，集計，統計の結果を利用して，報告用資料の作成や監査業務を支援します。

前提 OS

監査ログ閲覧サーバは，Windows Server 2012 または Windows Server 2008 上で動作します。

前提プログラム

JP1/Base

監査ログ閲覧サーバでは，JP1/Base のユーザ管理機能によって，監査ログ管理画面へのユーザ認証やアクセス制御を実施します。JP1/Base の機能については，マニュアル「JP1/Base 運用ガイド」を参照してください。

Web サーバ

Web サーバには，Microsoft Internet Information Services が必要です。また，Windows コンポーネントとして WWW（World Wide Web）サービスをインストールする必要があります。

Web ブラウザ

監査ログ管理画面を表示して，監査ログの検索，集計，統計などの操作を実行するために使用するプログラムです。

Internet Explorer が必要です。監査ログ管理サーバからバックアップファイルを監査ログ閲覧サーバにダウンロードする場合に必要です。

EUR

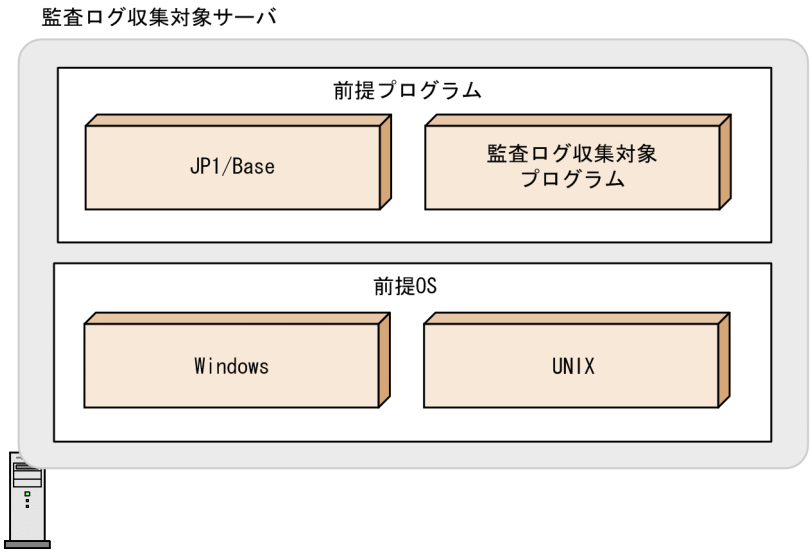
監査ログ管理画面で検索や集計した監査ログを，PDF ファイルの帳票として表示したり印刷したりする場合に必要なプログラムです。なお，このプログラムのインストールは任意です。必要に応じてインストールしてください。EUR の機能概要については，EUR のマニュアルを参照してください。

3.1.3　監査ログ収集対象サーバのプログラム構成

監査ログ収集対象サーバは，監査ログを収集するプログラムの対象サーバです。監査ログ収集対象サーバ上で運用されているプログラムが出力する監査ログを収集し，監査ログ収集対象サーバ上の JP1/Base のイベントデータベースに蓄積します。

監査ログ収集対象サーバのプログラム構成を次の図に示します。

図 3-3　監査ログ収集対象サーバのプログラム構成



前提 OS

監査ログ収集対象サーバは，OS が Windows または UNIX のプログラムを対象とします。監査ログ収集対象プログラムの前提 OS については「3.2.1　前提 OS」を参照してください。

OS が Windows の場合，監査ログ収集対象プログラムの監査ログのほかに，Windows イベントログ（セキュリティに関する情報）を監査ログとして収集できます。また，OS が UNIX の場合，UNIX システムログ（ユーザに関する情報）を監査ログとして収集できます。

前提プログラム

JP1/Base

監査ログ収集対象サーバ上の JP1/Base は，監査ログ収集対象プログラムが出力する監査ログを，JP1/Base のイベントデータベースに蓄積します。

JP1/Base の機能については，マニュアル「JP1/Base 運用ガイド」を参照してください。

監査ログ収集対象プログラム

システム利用状況や操作履歴などの監査ログを収集する対象プログラムを指します。

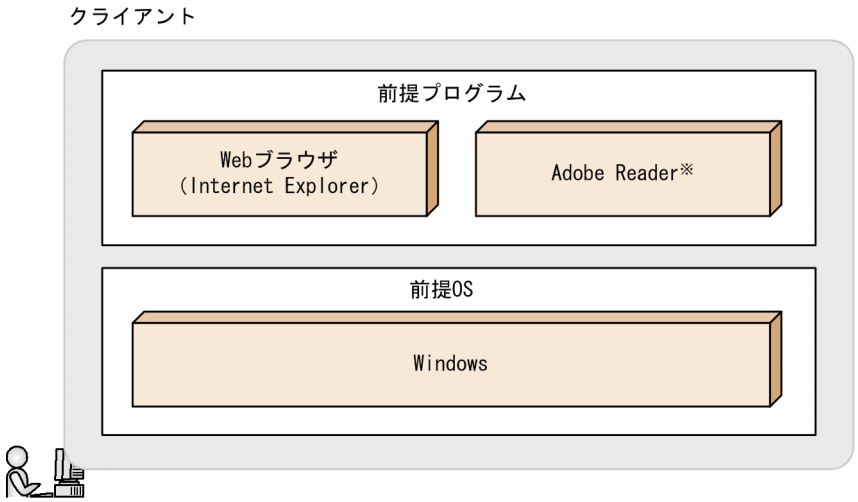
監査ログ収集対象プログラムとして JP1/Audit Management - Manager が標準サポートしているプログラムには，JP1/AJS3 - Manager や JP1/NETM/DM などがあります。標準サポートしているプログラムについては「3.2.2(3)　監査ログ収集対象サーバの前提プログラム」を参照してください。なお，標準サポート外のプログラムも監査ログ収集対象プログラムとして設定できます。標準サポート外のプログラムを監査ログ収集対象プログラムにするための検討については「4.3　監査ログを正規化するための検討」を参照してください。また，設定する方法については「5.6　監査ログ管理サーバで監査ログを収集するための設定」を参照してください。

3.1.4　クライアントのプログラム構成

クライアントでは，監査ログ管理サーバ上の監査ログ管理データベースを監査ログ管理画面から参照して各サーバの監査ログを管理したり，各サーバでのリソースへの操作やアクセス状況を監査したりできます。また，監査ログ閲覧サーバを構築した場合は，監査ログ閲覧サーバ上の監査ログ管理データベースを監査ログ管理画面から参照して，過去の監査ログを確認できます。

クライアントのプログラム構成を次の図に示します。

図 3-4　クライアントのプログラム構成



注※　PDFファイルを表示・印刷する場合に必要なプログラムです。

前提 OS

Internet Explorer 8 以降が使用できる Windows です。

前提プログラム

Web ブラウザ

監査ログ管理画面を表示して，監査ログの検索，集計，統計などの操作を実行するために使用するプログラムです。Internet Explorer が必要です。

Adobe Reader

JP1/Audit Management - Manager で検索や集計した監査ログを，PDF ファイルの帳票として表示・印刷する場合に必要です。

3.2　前提 OS および前提プログラム

この節では，監査証跡管理システムの構成要素ごとに前提 OS および前提プログラムについて説明します。

3.2.1　前提 OS

監査証跡管理システムの前提 OS を次に示します。

(1)　監査ログ管理サーバおよび監査ログ閲覧サーバの前提 OS

監査ログ管理サーバおよび監査ログ閲覧サーバは，次に示す OS 上で動作します。

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise
- Microsoft(R) Windows Server(R) 2008 R2 Standard

なお，リモートデスクトップ機能は利用できません。また，監査ログ管理サーバをクラスタ環境で運用する場合は，次に示す OS 上で動作します。

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise

監査ログ管理サーバを IPv6 環境で運用する場合は，次に示す OS 上で動作します。

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise

- Microsoft(R) Windows Server(R) 2008 R2 Standard

(2) 監査ログ収集対象サーバの前提 OS

監査ログ収集対象プログラムは，次に示す OS を使用しているプログラムを対象とします。

Windows

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise
- Microsoft(R) Windows Server(R) 2008 R2 Standard

UNIX

- HP-UX 11i V3 (IPF)
- Solaris 11
- Solaris 10
- AIX 7.1
- AIX 6.1
- Linux 7.1 (AMD/Intel 64)
- Linux 6.1 (AMD/Intel 64)
- Linux 6.1 (x86)
- Oracle Linux 6 (AMD64 & EM64T)
- Oracle Linux 7 (AMD64 & EM64T)
- SUSE Linux Enterprise Server 12 (AMD64 & EM64T)
- CentOS 6 (AMD64 & EM64T)
- CentOS 7 (AMD64 & EM64T)

なお，監査ログ収集対象サーバがクラスタ環境で運用されている場合は，次に示す OS を使用しているプログラムを対象とします。

Windows

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter

- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise

UNIX

- HP-UX 11i V3 (IPF)
- Solaris 11
- Solaris 10
- AIX 7.1
- AIX 6.1
- Linux 7.1 (AMD/Intel 64)
- Linux 6.1 (AMD/Intel 64)
- Linux 6.1 (x86)

監査ログ収集対象サーバを IPv6 環境で運用する場合は，次に示す OS 上で動作します。

Windows

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise
- Microsoft(R) Windows Server(R) 2008 R2 Standard

UNIX

- Linux 7.1 (AMD/Intel 64)
- Linux 6.1 (AMD/Intel 64)
- Linux 6.1 (x86)
- Oracle Linux 6 (AMD64 & EM64T)
- Oracle Linux 7 (AMD64 & EM64T)
- SUSE Linux Enterprise Server 12 (AMD64 & EM64T)
- CentOS 6 (AMD64 & EM64T)
- CentOS 7 (AMD64 & EM64T)

(3) クライアントの前提 OS

Internet Explorer 8 以降が使用できる Windows です。

3.2.2 前提プログラム

監査証跡管理システムの構成要素ごとに前提プログラムを次に示します。

(1) 監査ログ管理サーバの前提プログラム

JP1/Audit Management - Manager で監査ログを収集して一元管理するために，監査ログ管理サーバで必要となる前提プログラムについて次の表に示します。

表 3-1 監査ログ管理サーバの前提プログラム

項番	前提プログラム			導入区分	プログラムの概要
	プログラム名称		バージョン		
1	JP1/Base※1		11-00 以降	○	監査ログ収集対象サーバのイベントデータベースで管理する監査ログを JP1 イベントとして送受信するためのプログラムです。
2	Microsoft Internet Information Services※2		7.5 以降	○	Web サーバを構築するためのプログラムです。
3	EUR※3	EUR Print Service	07-60 以降	△	PDF ファイルの帳票を出力する場合に必要なプログラムです。
4		EUR Print Service - Portable Document Format option			
5		uCosminexus EUR Print Service Enterprise	08-00 以降		
6		uCosminexus EUR Server Standard	09-00 以降		
7		uCosminexus EUR Server Enterprise			

（凡例）

○：導入が必須のプログラム

△：必要に応じて導入するプログラム

注※1

監査証跡管理システムには，JP1/Base 08-10 以降の認証サーバが必要です。認証サーバは監査証跡管理システム内であれば，どのサーバ上に構築しても問題ありません。

注※2

監査ログ管理サーバの OS が Windows Server 2008 の場合は，7.5 が前提バージョンとなります。Windows Server 2012 の場合，IIS のバージョンは 8.0 になります。また，Windows Server 2012 R2 の場合は，8.5 が前提バージョンとなります。

注※3

Windows Server 2012 または Windows Server 2008 で PDF 帳票を出力する場合は，uCosminexus EUR V8 以降が必要となります。

EUR の機能概要については，EUR のマニュアルを参照してください。

監査ログ管理サーバをクラスタ環境のシステムに導入して運用する場合は，次に示すクラスタソフトが必要になります。

表 3-2　クラスタ環境のシステムに導入して運用する場合に必要となるクラスタソフト

項番	OS	クラスタソフト
1	Microsoft(R) Windows Server(R) 2012 R2 Datacenter	Windows Server(R) Failover Cluster
2	Microsoft(R) Windows Server(R) 2012 R2 Standard	
3	Microsoft(R) Windows Server(R) 2012 Datacenter	
4	Microsoft(R) Windows Server(R) 2012 Standard	
5	Microsoft(R) Windows Server(R) 2008 R2 Enterprise	

(2)　監査ログ閲覧サーバの前提プログラム

JP1/Audit Management - Manager で収集した監査ログを閲覧するために，監査ログ閲覧サーバで必要となる前提プログラムを次の表に示します。

表 3-3　監査ログ閲覧サーバの前提プログラム

項番	前提プログラム			導入区分	プログラムの概要
	プログラム名称		バージョン		
1	JP1/Base※1		11-00 以降	○	JP1/Base の機能によってユーザ認証を実施するためのプログラムです。
2	Microsoft Internet Information Services※2		7.5 以降	○	Web サーバを構築するためのプログラムです。
3	Internet Explorer		8 以降	△	Web ページを閲覧するためのプログラムです。
4	EUR※3	EUR Print Service	07-60 以降	△	PDF ファイルの帳票を出力する場合に必要なプログラムです。
5		EUR Print Service - Portable Document Format option			
6		uCosminexus EUR Print Service Enterprise	08-00 以降		

項番	前提プログラム			導入区分	プログラムの概要
	プログラム名称		バージョン		
7		uCosminexus EUR Server Standard	09-00 以降		
8		uCosminexus EUR Server Enterprise			

（凡例）

○：導入が必須のプログラム

△：必要に応じて導入するプログラム

注※1

監査証跡管理システムには，JP1/Base 08-10 以降の認証サーバが必要です。認証サーバは監査証跡管理システム内であれば，どのサーバ上に構築しても問題ありません。

注※2

監査ログ閲覧サーバの OS が Windows Server 2008 の場合は，7.5 が前提バージョンとなります。Windows Server 2012 の場合，IIS のバージョンは 8.0 になります。また，Windows Server 2012 R2 の場合は，8.5 が前提バージョンとなります。

注※3

Windows Server 2012 または Windows Server 2008 で PDF 帳票を出力する場合は，uCosminexus EUR V8 以降が必要となります。

EUR の機能概要については，EUR のマニュアルを参照してください。

(3) 監査ログ収集対象サーバの前提プログラム

監査ログ収集対象サーバの前提プログラムを次に示します。

表 3-4 監査ログ収集対象サーバの前提プログラム

項番	前提プログラム		導入区分	プログラムの概要
	プログラム名称	バージョン		
1	JP1/Base※1	07-10 以降 ※2	○	監査ログ収集対象サーバのイベントデータベースで管理する監査ログを，JP1 イベントとして送受信するためのプログラムです。 また，監査ログ収集対象プログラムとしても設定できます。

（凡例）

○：導入が必須のプログラム

注※1

IPv6 アドレスを使用して通信する場合は，JP1/Base 10-00 以降が必要です。

注※2

JP1/Base の操作ログを収集する場合や JP1/Base に認証サーバを構築する場合は，08-10 以降を導入する必要があります。また，JP1/Base のバージョンによって，イベントデータベースに格納できる監査ログのデータの最大長が異なります。1 行のデータが最大長を超えた場合，それ以降のデータは切り捨てられます。イベントデータベースに格納できるデータの最大長を次に示します。

・JP1/Base 08-10 以降の場合：1,023 バイト
・JP1/Base 08-10 より前の場合：511 バイト

監査ログ収集対象サーバがクラスタ環境で運用されている場合は，次に示すクラスタソフトが必要になります。

表 3-5　クラスタ環境で運用されている場合に必要となるクラスタソフト

項番	OS	クラスタソフト
1	Microsoft(R) Windows Server(R) 2012 R2 Datacenter	Windows Server(R) Failover Cluster
2	Microsoft(R) Windows Server(R) 2012 R2 Standard	
3	Microsoft(R) Windows Server(R) 2012 Datacenter	
4	Microsoft(R) Windows Server(R) 2012 Standard	
5	Microsoft(R) Windows Server(R) 2008 R2 Enterprise	
6	HP-UX 11i V3 (IPF)	HP Serviceguard
7	AIX 7.1	PowerHA
8	AIX 6.1	
9	Solaris 11	VERITAS Cluster Server
10	Solaris 10	
11	Linux 6.1 (AMD/Intel 64)	HA モニタ
12	Linux 6.1 (x86)	
13	Linux 5 (AMD64 & Intel EM64T)	
14	Linux 5 (x86)	

JP1/Audit Management - Manager が監査ログを標準で収集できるプログラムを次の表に示します。

表 3-6　JP1/Audit Management - Manager が標準サポートしているプログラム（日本語版 OS）

項番	プログラム名称		バージョン
1	Collaboration	Groupmax Collaboration	07-50 以降
		uCosminexus Collaboration	06-50 以降
2	Cosminexus		07-50 以降
3	HiRDB		08-04 以降

項番	プログラム名称		バージョン
4	Hitachi Navigation Platform		10-00 以降
5	Hitachi Storage Command Suite	Hitachi Storage Command Suite	5.6 以降
		Hitachi Command Suite	7 および 8
6	JP1/AJS2		07-10 以降
7	JP1/AJS3		09-00 以降
8	JP1/AO		10-00 以降
9	JP1/Base		08-10 以降
10	JP1/IM - NP		10-10 以降
11	JP1/IM - SS	JP1/IM - SS	10-10 以降
		JP1/SS	11-00 以降
12	JP1/ITDM		09-50 以降
13	JP1/ITDM2		10-50 以降
14	JP1/ITRM		09-10 以降
15	JP1/NETM/AIM		09-50 以降
16	JP1/NETM/CSC		08-11 以降
17	JP1/NETM/DM		08-10 以降
18	JP1/NETM/NM		09-00 以降
19	JP1/PFM		08-10 以降
20	JP1/秘文		09-00 以降
21	OpenTP1		07-02 以降
22	Oracle		9i，10g，11g，11gR2 および 12c
23	TRUST E2		09-00 以降
24	uCosminexus EUR Server		09-60 以降
25	uCosminexus Navigation Platform		09-60 以降
26	uCosminexus Portal Framework		08-01 以降
27	XDM/BASE E2		10-10 以降
28	活文 NAVIstaff		02-02 以降

表 3–7　JP1/Audit Management - Manager が標準サポートしているプログラム（英語版 OS）

項番	プログラム名称	バージョン
1	JP1/AJS3	11-00 以降

項番	プログラム名称	バージョン
2	JP1/AO	
3	JP1/Base	
4	JP1/SS	
5	JP1/ITDM2※	
6	JP1/PFM	

注※

監査ログの固有情報に日本語が含まれる場合，固有情報は文字化けします。

なお，JP1/Audit Management - Manager では標準サポート外のプログラムの監査ログも収集できます。標準サポート外のプログラムを監査ログ収集対象プログラムにするための検討については「4.3　監査ログを正規化するための検討」を参照してください。また，設定する方法については「5.6　監査ログ管理サーバで監査ログを収集するための設定」を参照してください。

(4)　クライアントの前提プログラム

クライアントの前提プログラムを次の表に示します。

表 3-8　クライアントの前提プログラム

項番	前提プログラム	導入区分	プログラムの概要
1	Internet Explorer	○	Web ページを閲覧するためのプログラムです。
2	Adobe Reader	△	PDF ファイルの帳票を表示や印刷する場合に必要なプログラムです。

（凡例）

○：導入が必須のプログラム

△：必要に応じて導入するプログラム

3.3　システム構成例

この節では，監査証跡管理システムを運用する上でのシステム構成例を示します。

- 基本構成
  監査ログ管理サーバ，監査ログ収集対象サーバ，およびクライアントで構成されたシステム構成です。
- 監査ログ閲覧サーバを構築した構成
  基本構成に監査ログ閲覧サーバを加えたシステム構成です。閲覧専用のサーバを構築することによって，監査ログのバックアップを閲覧することができます。また，監査ログをまとめた報告用資料の作成や監査業務を迅速に実施できます。
- クラスタ環境でのシステム構成
  監査証跡管理システムの監査ログ管理サーバまたは監査ログ収集対象サーバをフェールオーバーさせる場合のシステム構成です。監査ログ閲覧サーバについてはクラスタ環境のシステムに対応していません。
- IPv6 環境でのシステム構成
  IPv6 アドレスを使用して通信する場合のシステムの構成です。IPv6 アドレスを使用して通信する監査ログ収集対象サーバの監査ログを収集できます。

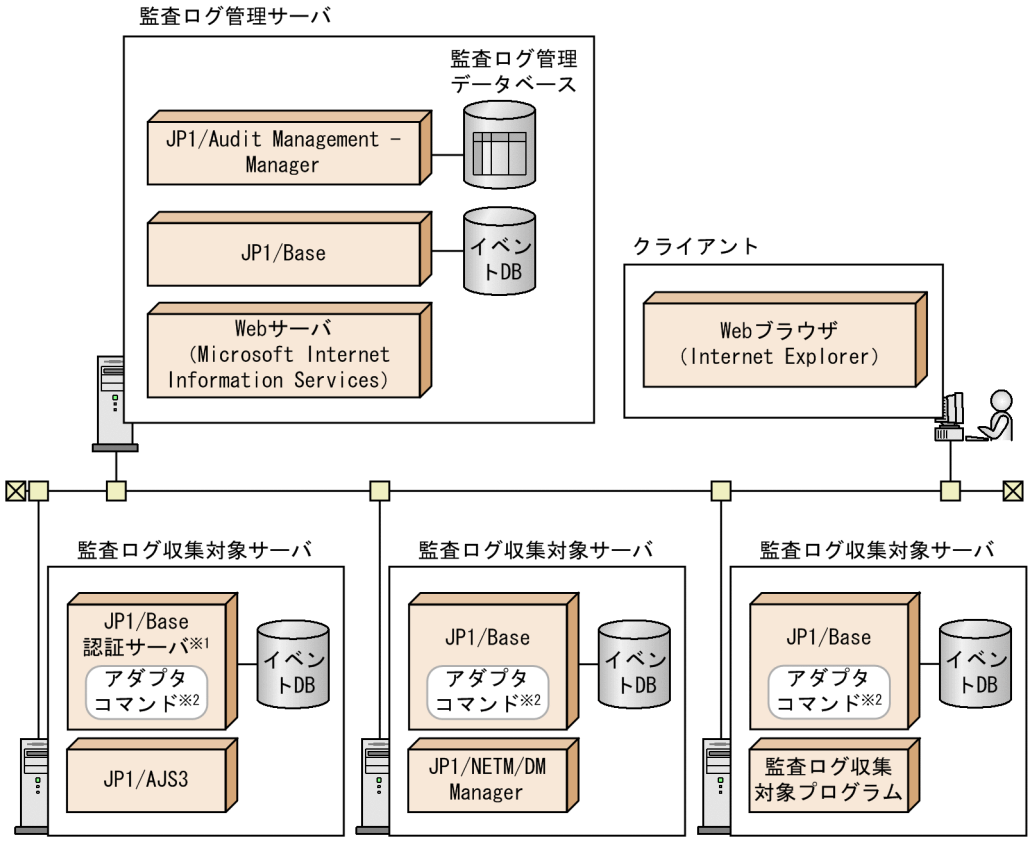
なお，システムを構成する各要素については「3.1　プログラム構成」を参照してください。

3.3.1　基本構成

監査証跡管理システムの基本的なシステム構成例を次の図に示します。

このシステム構成例は，監査ログ収集対象サーバ上にある収集対象プログラムが出力する監査ログを，監査ログ管理サーバで収集する場合の基本的な構成を示しています。

図 3-5　監査証跡管理システムのシステム構成（基本構成）



注※1 監査証跡管理システムには，JP1/Baseの認証サーバが必要です。ただし，JP1/Baseの認証サーバの構築場所は任意です。

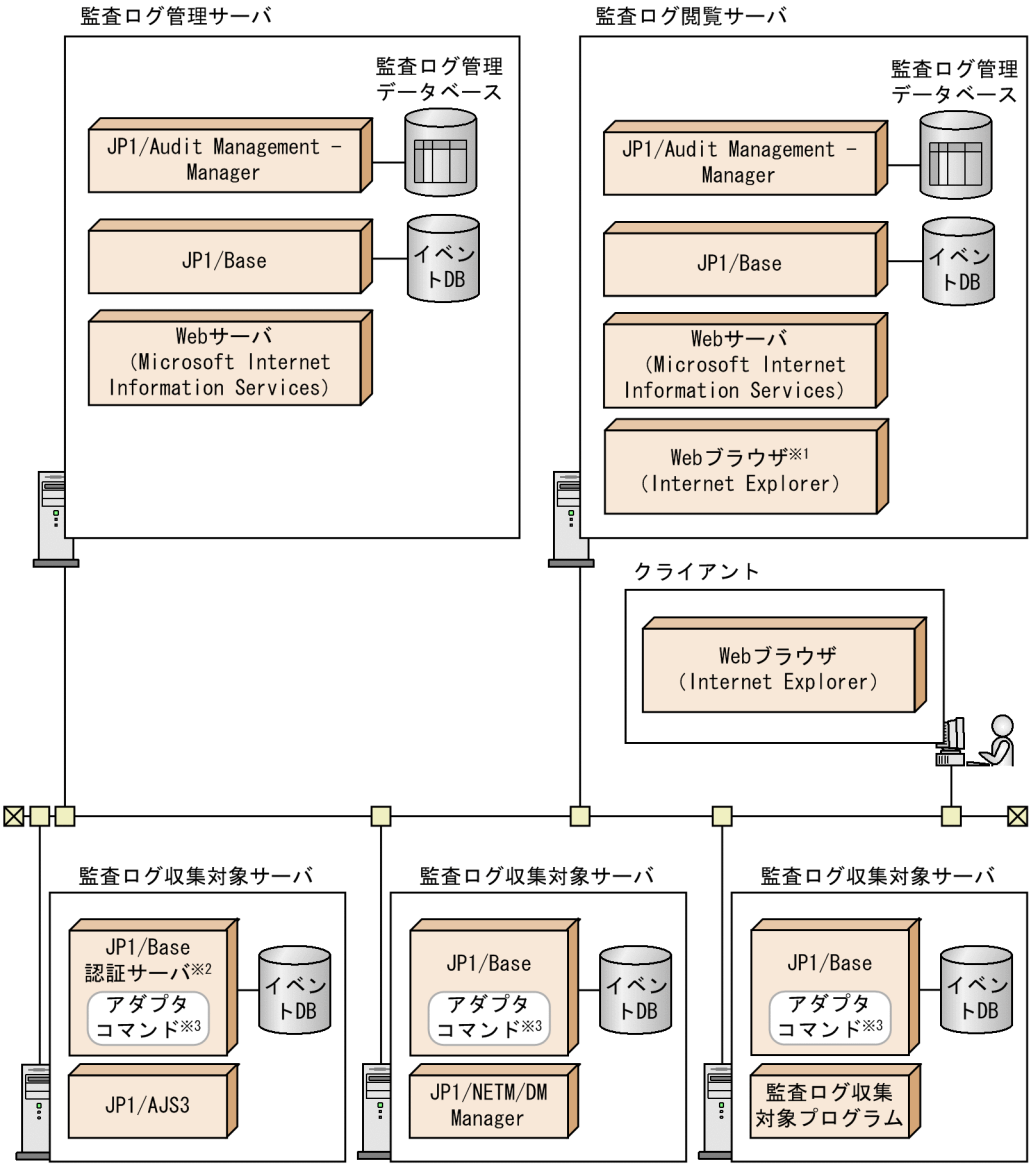
注※2 JP1/Audit Management - Managerが提供するコマンドです。監査ログ収集対象サーバのセットアップ時にインストールされます。

3.3.2　監査ログ閲覧サーバを構築した構成

基本構成に監査ログ閲覧サーバを加えたシステム構成例を次の図に示します。

このシステム構成例は「3.3.1　基本構成」で示したシステム構成に監査ログ閲覧サーバを追加して運用する構成を示しています。監査ログ閲覧サーバは，監査ログ管理サーバに蓄積された監査ログのバックアップをインポートし，監査ログを調査したり監査したりする閲覧専用のサーバです。

図 3-6　監査証跡管理システムのシステム構成（監査ログ閲覧サーバを構築した構成）



注※1 監査ログ管理画面を表示する場合に必要なプログラムです。

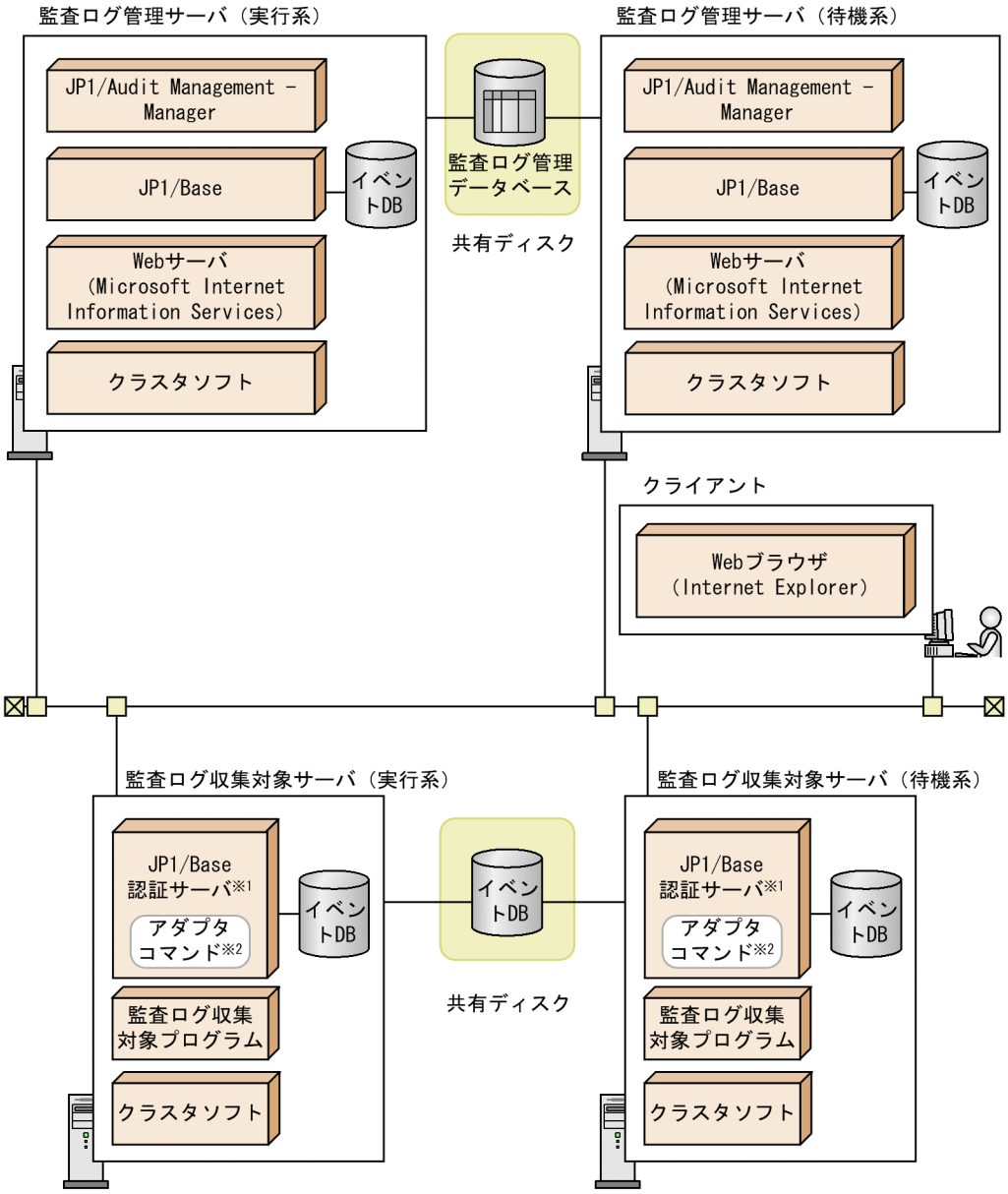
注※2 監査証跡管理システムには，JP1/Baseの認証サーバが必要です。ただし，JP1/Baseの認証サーバの構築場所は任意です。

注※3 JP1/Audit Management - Managerが提供するコマンドです。監査ログ収集対象サーバのセットアップ時にインストールされます。

3.3.3　クラスタ環境での構成

監査証跡管理システムをフェールオーバーさせる場合のシステムの構成を次の図に示します。

図 3-7　監査証跡管理システムのシステム構成（クラスタ環境での構成）



注※1 監査証跡管理システムには，JP1/Baseの認証サーバが必要です。ただし，JP1/Baseの認証サーバの構築場所は任意です。

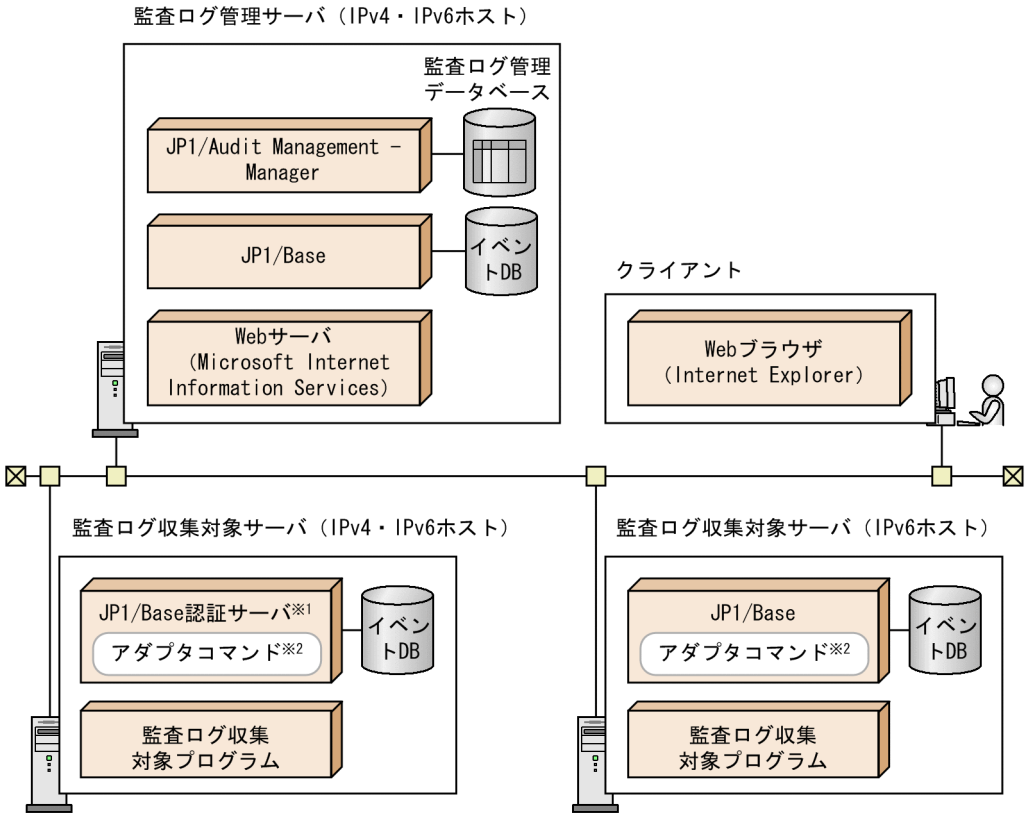
注※2 JP1/Audit Management - Managerが提供するコマンドです。監査ログ収集対象サーバのセットアップ時にインストールされます。

クラスタ環境でのシステムの構成の検討については「4.4.3　システムの運用方法（クラスタ環境への導入有無）」を参照してください。クラスタ環境でのシステムの構築については「6.　クラスタ環境でのシステム構築」を参照してください。

3.3.4　IPv6 環境での構成

IPv6 アドレスを使用して通信する場合のシステムの構成を次の図に示します。

図 3-8　監査証跡管理システムのシステム構成（IPv6 環境での構成）



（凡例）
IPv4・IPv6ホスト：IPv4アドレスまたはIPv6アドレスを使用して通信するホスト
IPv6ホスト：IPv6アドレスだけを使用して通信するホスト

注※1 監査証跡管理システムには，JP1/Baseの認証サーバが必要です。ただし，JP1/Baseの認証サーバの構築場所は任意です。

注※2 JP1/Audit Management - Managerが提供するコマンドです。監査ログ収集対象サーバのセットアップ時にインストールされます。

IPv6 アドレスを使用して通信する場合の注意事項

- 監査ログ管理サーバは，IPv4・IPv6 ホスト（IPv4 アドレスまたは IPv6 アドレスを使用して通信するホスト）に構築する必要があります。IPv6 ホスト（IPv6 アドレスだけ使用して通信するホスト）には構築できません。
- 監査ログ収集対象サーバは，IPv4・IPv6 ホストおよび IPv6 ホストに構築できます。

3.3.5　システム構成の注意事項

JP1/Audit Management - Manager は，JP1/Base の認証サーバによって管理される認証圏内に構築する必要があります。

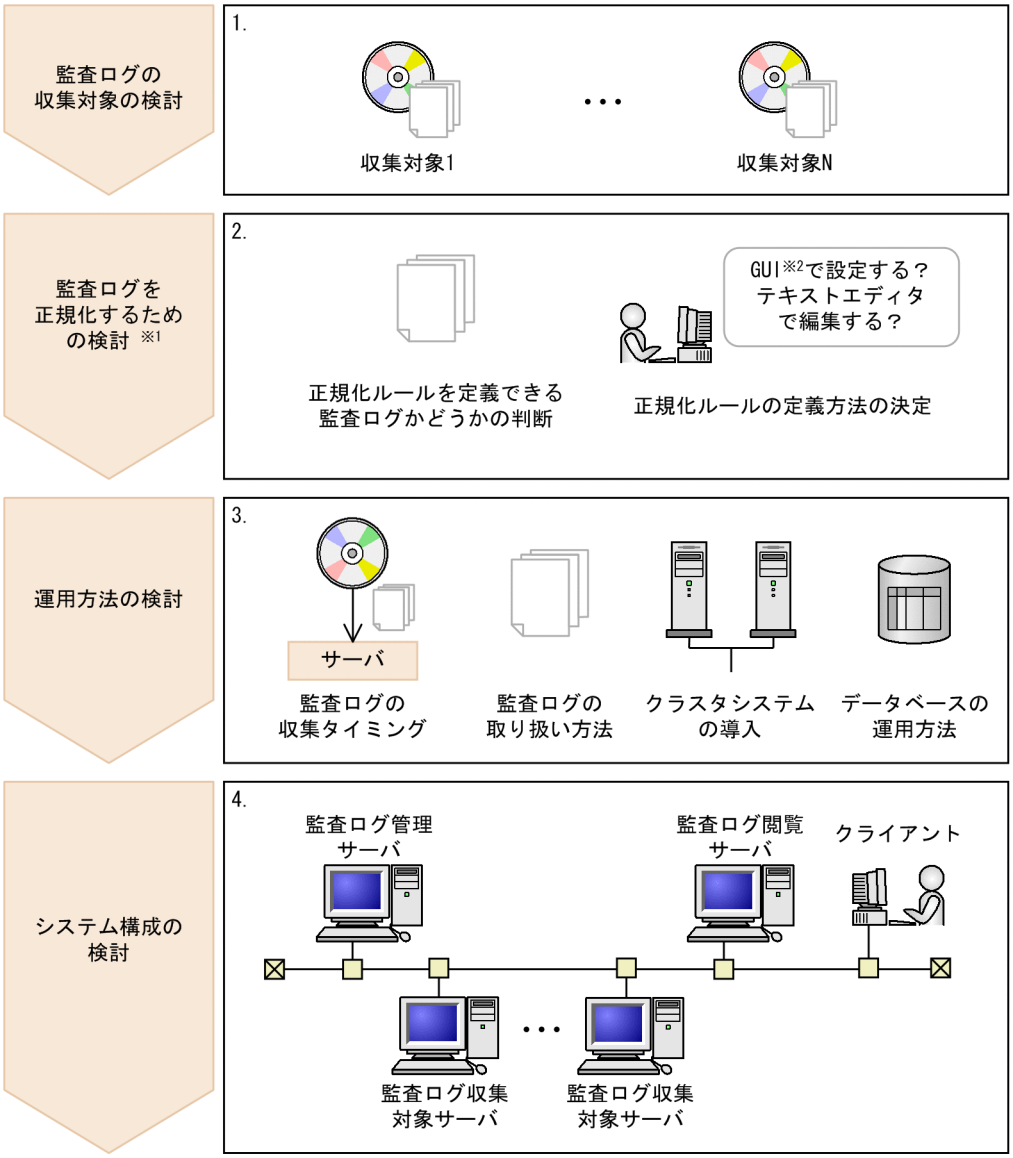
4 システム設計

この章では，JP1/Audit Management - Manager を使用した監査証跡管理システムの設計作業の概要として，設計の流れと各設計工程の中で検討する項目の例について説明します。

4.1　システム設計の流れ

JP1/Audit Management - Manager を使用した監査証跡管理システムを設計する流れを次の図に示します。

図 4-1　設計の流れ



注※1　監査ログを正規化するための検討は，JP1/Audit Management - Managerで標準サポート外となっているプログラムの監査ログを収集する場合に必要です。標準サポートしているプログラムの監査ログだけを収集する場合，検討する必要はありません。

注※2　［正規化ルールエディタ］ダイアログ

1. 監査ログの収集対象の検討

どのプログラムの監査ログを収集するかを証跡管理内容に合わせて決定します。

2. 監査ログを正規化するための検討

JP1/Audit Management - Manager で標準サポート外となっているプログラムの監査ログを収集する場合，正規化ルールを定義する必要があります。収集する監査ログのファイル形式やフォーマットを基に，正規化ルールで定義できるかどうかを判断した上で，正規化ルールの定義方法を決定します。

3. 運用方法の検討

監査ログの収集タイミングやバックアップ方法など，日々の運用の方法を決定します。

4. システム構成の検討

手順 1 から手順 3 で決めた内容を基に，必要なサーバの種類や台数および必要なプログラムを決定します。

4.2 監査ログの収集対象の検討

監査ログを収集する対象を検討します。

JP1/Audit Management - Manager を使用した監査証跡管理システムでは，次のプログラムや OS が出力する監査ログを収集できます。なお，プログラムによっては監査ログのことを，操作ログまたは動作ログと呼ぶ場合があります。

- Collaboration
- Cosminexus
- HiRDB
- Hitachi Navigation Platform
- Hitachi Storage Command Suite
- JP1/AJS2
- JP1/AJS3
- JP1/AO
- JP1/Audit
- JP1/Base
- JP1/IM - NP
- JP1/IM - SS
- JP1/ITDM
- JP1/ITDM2
- JP1/ITRM
- JP1/NETM/AIM
- JP1/NETM/CSC
- JP1/NETM/DM
- JP1/NETM/NM
- JP1/PFM
- JP1/秘文
- OpenTP1
- Oracle
- TRUST E2
- uCosminexus EUR Server
- uCosminexus Navigation Platform

- uCosminexus Portal Framework
- UNIX システムログ
- Windows イベントログ（セキュリティに関する情報）※
- XDM/BASE E2
- 活文 NAVIstaff

注※

監査証跡管理システムでは，一部のログオン イベントやアカウント管理のログを標準サポートしています。このほかの Windows イベントログ（セキュリティに関する情報）については標準サポート外になります。

標準サポートする Windows イベントログのイベント ID については「5.4.3　JP1/Base のイベントログトラップ機能を設定する」を参照してください。

これらの標準サポートしているプログラムについては，各プログラムが出力した監査ログを JP1/Audit Management - Manager の監査ログ管理データベースに格納するための定義ファイル群があらかじめ用意されています。

標準サポート外のプログラムについては，監査証跡管理システムで収集できる監査ログかどうかを判断し，対応する定義ファイル群を用意することで，監査ログを収集できるようになります。標準サポート外のプログラムの監査ログを収集する場合に検討する内容については，次の「4.3　監査ログを正規化するための検討」で説明します。

標準サポート外のプログラムを収集対象とする場合に作成する定義ファイル群の説明および定義ファイル群の作成手順については「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。

なお，監査ログの収集対象を設定する際には，プログラム名とそのプログラムが出力するログファイルの格納先フォルダを指定します。あらかじめこれらの内容を明確にしておいてください。

4.3　監査ログを正規化するための検討

標準サポート外のプログラムの監査ログを監査証跡管理システムで収集するには，正規化ルールを定義する必要があります。収集したいログのファイル形式やフォーマットなどから正規化ルールを定義できる監査ログかどうかを判断した上で，定義方法を検討します。

標準サポートしているプログラムの監査ログだけを収集する場合，監査ログの正規化について検討する必要はありません。

正規化ルールの定義方法には次の二つがあります。

- 正規化ルールエディタで定義する方法
- 正規化ルールファイルで定義する方法

それぞれの定義方法によって，定義できる監査ログの条件が異なります。このため，定義できる監査ログかどうかを判断する際は，どちらの方法で正規化ルールを定義するかについてもあわせて検討してください。

4.3.1　正規化ルールで定義できる監査ログの条件

監査ログのファイル形式やフォーマットを確認し，監査証跡管理システムで収集できる監査ログかどうかを目安として判断します。

(1)　ファイル形式の有効性を判断する

監査証跡管理システムで収集できる監査ログのファイル形式かどうかを判断します。

次の条件をすべて満たしている場合，監査証跡管理システムで監査ログを収集できます。

- ラップアラウンド形式またはシフト形式である
- ファイル名称は動的な名称ではない
- バイナリデータが含まれていない（監査ログファイル中の 1 行の終了文字以外にバイナリデータを含まないファイル）
- ログ情報が蓄積されるファイルである（常に 1 行しか出力されないファイルではない）
- 文字コードは次の表のどれかである（プラットフォームによって異なる）

表 4–1　収集できる監査ログの文字コード

文字コード		Windows	UNIX	Linux
日本語	シフト JIS	○	○	×
	EUC	×	○	×
	UTF-8	×	×	○

文字コード		Windows	UNIX	Linux
	注 LANG=ja_JP.UTF-8 または ja_JP.utf8			
英語	8859_1(ASCII) 注 UNIX/Linux の場合 LANG=C	○	○	○

（凡例）

○：収集可

×：収集不可

なお，これらの条件を満たしていない場合は，ファイル形式の変換が必要です。また，文字コードの条件は，収集対象サーバのプラットフォームによって異なるため，マニュアル「JP1/Base 運用ガイド」を参照してください。

参考

ラップアラウンド形式およびシフト形式について説明します。

ラップアラウンド形式は，監査ログが最初に出力されるときに audit1.log を作成してログを書き込み，監査ログファイルが一定の容量に達すると auditlog2.log を作成してログを書き込む形式です。ファイル名末尾の数値+1 をしたファイル名称のファイルを作成して新たにログを書き込む動作が，監査ログファイル数まで繰り返されます。ファイル数が設定値を超えると，古いログファイルから上書き保存されます。

シフト形式は，監査ログファイルが一定の容量に達するとファイル名を変更して保存したあと，変更前と同じ名称のファイルを作成して新たにログを書き込む形式です。監査ログファイルが audit.log の場合，一定の容量に達して監査ログファイルが切り替わるときに audit.log を audit1.log に変更して保存し，新たに audit.log を作成してログを書き込みます。再び audit.log が一定量に達すると保存済みの audit1.log を audit2.log に変更したあと，audit.log を audit1.log に変更して保存します。ファイル数が設定値を超えると，古いファイル（つまり，ファイル末尾の数値が最も大きいファイル）から削除されます。

(2) ファイルフォーマットの有効性を判断する

監査ログのファイルフォーマットを判断します。

収集したい監査ログが，次の条件を満たしているかどうかを確認してください。

正規化ルールエディタで定義する場合の条件

- 監査ログの最終行に改行がある
- プロダクト名および Windows イベント ID ごとに，監査ログの出力フォーマットが固定（イベントログトラップ機能によって収集されるログの場合）

- プロダクト名ごとに，監査ログの出力フォーマットが固定（ログファイルトラップ機能によって収集されるログの場合）

正規化ルールエディタで定義する方法については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

正規化ルールファイルで定義する場合の条件

- 監査ログの最終行に改行がある
- 区切り文字が「△（半角スペース）」または「,」である
- フォーマットの形式が次のどちらかである
  ・Tag1=Value1[区切り文字]Tag2=Value2[区切り文字]Tagn=Valuen
  ・Value1[区切り文字]Value2[区切り文字]Valuen
- 監査ログレコードの種類や種別を特定することができる値（以降ユニークキーと呼びます）が次のどちらかである
  ・ユニークキーがあり，ユニークキーごとに監査ログの出力フォーマットが固定
  ・ユニークキーはないが，すべての監査ログの出力フォーマットは固定

正規化ルールファイルの定義内容については「13.2　正規化ルールファイル」を参照してください。

4.3.2　監査ログのフォーマットへの対応づけの検討

標準サポート外のプログラムから出力されるログのフォーマットと，監査ログ管理データベースに格納する監査ログのフォーマットを対応づけるための検討をします。

標準サポート外のプログラムから出力されるログの情報が，次に示す各項目に該当するよう対応づけることをお勧めします。

- 監査ログの通番
- メッセージ識別番号
- 日付・時刻
- プログラム名
- コンポーネント名
- プロセス ID
- 発生場所
- 監査ログの収集カテゴリ
- 監査ログの結果
- 操作を実施したユーザ名

監査ログのフォーマットの例を次に示します。

- Tag = Value 形式の場合

```
num=<監査ログの通番>,msgid=<メッセージ識別番号>,date=<日付・時刻>,
prog=<プログラム名>,comp=<コンポーネント名>,pid=<プロセスID>,place=<発生場所>,
ctgy=<監査ログの収集カテゴリ>,result=<監査ログの結果>,
user=<操作を実施したユーザ名>,msg=<その他>
```

監査ログを正規化した結果の例を次に示します。

```
num=1,msgid=123,date=2007-01-01T10:10:10.100+09:00,prog=Program,comp=Component,
pid=1234,place=Host1,ctgy=Authentication,result=Success,user=User1,
msg="認証に成功しました。認証サーバ=[Host2]"
```

- Value 形式の場合

```
<監査ログの通番> <メッセージ識別番号> <日付・時刻> <プログラム名>
<コンポーネント名> <プロセスID> <発生場所> <監査ログの収集カテゴリ>
<監査ログの結果> <操作を実施したユーザ名> <その他>
```

監査ログを正規化した結果の例を次に示します。

```
1 123 2007/01/01 10:10:10 Program Component 1234 Host1 Authentication Success
User1 "認証に成功しました。認証サーバ=[Host2]"
```

正規化ルールファイルで定義する場合，出力されるログ情報を監査ログのフォーマットにどのように対応づけるかについては「13.2　正規化ルールファイル」を参照し，検討してください。

また，正規化ルールエディタで定義する場合，出力されるログ情報を監査ログフォーマットにどのように対応づけるかについては，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照し，検討してください。

4.3.3　正規化ルールの定義方法を変更する場合の注意事項

正規化ルールファイルで定義している，すでに収集中の監査ログの正規化ルールを，正規化ルールエディタで定義したい場合に，定義し直すことができます。ただし，定義方法を変更すると，変更前と変更後とで，同じプログラムの監査ログとして監査ログ管理画面に表示されないことがあります。

4.4　運用方法の検討

監査ログをいつ収集するか，収集した監査ログをどのように使用するかなど，監査証跡管理システムの運用方法について検討します。

4.4.1　監査ログの収集時期の決定

監査ログをいつ収集するかを決定します。

JP1/Audit Management - Manager を使用した監査証跡管理システムには，「定期的な収集」，「監査ログ専用イベントデータベース切り替え時の収集」，および「即時収集」の 3 種類の収集タイミングがあります。

「定期的な収集」については，監査ログ管理サーバの構築時に収集日時を指定する必要があります。「監査ログ専用イベントデータベース切り替え時の収集」については，特定のイベントの出力が監査証跡管理システムで検知されて自動的に収集されるため，タイミングに関しての設定は不要です。また，「即時収集」については，監査ログを収集したいときに，［監査ログ収集マネージャ］ウィンドウまたは admcoldata コマンドを使用して監査ログの収集を指示するため，タイミングに関しての設定は不要です。

収集タイミングの詳細については「2.2.2　監査ログの収集タイミング」を参照してください。

監査ログ管理サーバの構築時，JP1/Audit Management - Manager について設定する際は，「定期的な収集」に関して次の項目を指定します。あらかじめこれらの内容を決定しておいてください。

監査ログ収集日

監査ログを収集する曜日です。「毎日」という指定もできます。

監査ログ収集時間

監査ログの収集を開始する時間（何時何分）です。

4.4.2　収集した監査ログの取り扱い方法

収集した監査ログをどのように取り扱うかを決定します。

JP1/Audit Management - Manager では，監査ログ管理データベースに収集された監査ログに対して，次の表のような操作ができます。

表 4-2　監査ログに対してできる主な操作

項目	内容
検索および検索結果の表示・ファイル出力	監査ログ管理データベースに収集した監査ログから，指定された条件に合うものだけを検索して一覧表示します。検索結果は，CSV 形式ファイルや PDF ファイルに出力したり，レポート画面に表示したりすることもできます。

項目	内容
集計および集計結果の表示・ファイル出力	監査ログ管理データベースに収集した監査ログを，指定された条件で集計し，件数を一覧表示します。集計結果は，CSV 形式ファイルや PDF ファイルに出力したり，画面にグラフ表示したりすることもできます。
統計および統計結果の出力	監査ログ管理データベースに収集した監査ログの統計情報を，指定された条件で生成し，グラフ形式で表示します。統計結果は，CSV 形式ファイルや HTML 形式ファイルに出力することもできます。
バックアップ	監査ログ管理データベースから監査ログを CSV 形式ファイルにバックアップします。 監査ログのバックアップには，開始・終了日時を指定してバックアップする方法と，前回のバックアップ取得からコマンド実行日前日までの差分をバックアップする方法があります。 バックアップファイルの格納先フォルダはあらかじめ用意しておく必要があります。 監査証跡管理システムでは，バックアップ履歴として，格納先フォルダや実行日を管理します。これによって，必要であれば監査ログ管理画面からバックアップファイルをダウンロードできます。
インポート	監査ログをバックアップした CSV 形式ファイルを監査ログ閲覧サーバにインポートして，閲覧できるようにします。
削除	保存期限を経過した監査ログや，閲覧サーバに移行した監査ログをデータベースから削除します。

検討項目を次に示します。

1. **検索結果，集計結果，および統計結果の出力形式**

   検索や集計の結果は，次に示す形式で出力できます。これらの出力形式をどのように使用するかを検討しておくと便利です。

   - CSV 形式ファイル（検索結果，集計結果，および統計結果）
   - PDF ファイル（検索結果および集計結果）
   - HTML 形式ファイル（統計結果）
   - レポート画面（検索結果）
   - グラフ画面（集計結果および統計結果）

   注意事項

   PDF ファイルに出力するには，表 3-1 に示す EUR のインストールが必要です。

   ただし，Windows Server 2012 または Windows Server 2008 で PDF 帳票を出力する場合は，uCosminexus EUR V8 以降が必要となります。

   また，このとき，EUR Professional Edition 07-60 以降，uCosminexus EUR Designer 08-00 以降，または uCosminexus EUR Developer 08-00 以降を使用すれば，PDF ファイルの帳票のフォームを作成できます。

   帳票のフォームを作成する際に使用する CSV 形式のファイルフォーマットについては，次に示すフォルダ配下に用意されているサンプルファイル（CSV 形式）を参考にしてください。

JP1/Audit Management - Manager の仮想ディレクトリ¥pdf

各ファイルの内容については「付録 A.2　JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧」を参照してください。

2. 監査ログのバックアップ方法

監査ログのバックアップ方法には次の 2 種類があります。

- 開始・終了日時を指定してバックアップする方法
- 前回のバックアップ取得からコマンド実行日前日までの差分をバックアップする方法

前回のバックアップ取得からコマンド実行日前日までの差分をバックアップする場合には，JP1/AJS や Windows のタスクスケジューラなどを利用できます。この場合，バックアップの日程を検討し，スケジュールを登録しておく必要があります。

あらかじめどのような方法でバックアップするかを決定しておいてください。

3. 監査ログのバックアップファイルの格納先

監査ログのバックアップファイルを格納するフォルダは，監査ログ管理画面（バックアップ履歴）からのバックアップファイルのダウンロードにも使用されるため，監査ログ管理サーバの構築時に作成し，設定します。

あらかじめ，このフォルダの作成場所を決定しておいてください。

4. 監査ログのバックアップおよび削除のタイミング（監査ログ閲覧サーバの運用方法）

監査ログのバックアップおよび削除のタイミングは，監査ログ閲覧サーバの運用方法によって異なります。監査ログ閲覧サーバの運用例を次に示します。例を参考に，監査ログ閲覧サーバの運用方法，監査ログをバックアップするタイミング，および監査ログを削除するタイミングについて検討してください。

例 1：監査済みの監査ログを監査ログ閲覧サーバで閲覧する

監査が完了するまでは監査ログを監査ログ管理サーバ上で閲覧する運用です。監査済みの監査ログについても，保存期限までは閲覧できるように監査ログ閲覧サーバで管理します。

この場合，監査完了のタイミングで監査ログ管理サーバ上の監査ログをバックアップして削除し，監査ログ閲覧サーバにインポートします。

また，監査ログ閲覧サーバでも，保存期限を過ぎたタイミングで監査ログをバックアップして削除します。

例 2：保存期限を過ぎた監査ログを監査ログ閲覧サーバで閲覧する

保存期限までは監査ログを監査ログ管理サーバ上で閲覧する運用です。所定の保存期限を過ぎた監査ログについては，必要に応じて監査ログ閲覧サーバで閲覧します。

この場合，監査ログ管理サーバ上の監査ログのうち，保存期限を過ぎたものをバックアップして削除し，バックアップデータを閲覧する必要があるときにだけ監査ログ閲覧サーバにインポートします。

例 3：監査ログ閲覧サーバを使用しない

監査ログはすべて監査ログ管理サーバ上で閲覧し，所定の期限を過ぎた監査ログについてはバックアップして削除する（監査ログ管理画面上では閲覧しない）運用です。

この場合，監査ログ管理サーバ上の監査ログのうち，保存期限後，一定の期間を過ぎた監査ログはバックアップして削除します。

なお，監査ログ閲覧サーバの運用方法は，監査ログ管理サーバ，監査ログ閲覧サーバそれぞれに必要なデータベース容量にも影響します。各サーバのデータベース容量も考慮して決定してください。データベース容量については「4.6.3　データベース容量の見積もり」を参照してください。

4.4.3　システムの運用方法（クラスタ環境への導入有無）

クラスタ環境でのシステムの導入について次に説明します。

(1)　監査ログ管理サーバの場合

監査ログ管理サーバをクラスタ環境に導入して運用するかどうかを決定します。監査ログ管理サーバをクラスタ環境に導入して運用するかどうかによって，システム構成や監査ログ管理サーバの構築手順が異なります。

クラスタ環境で運用する場合の前提 OS については「3.2.1(1)　監査ログ管理サーバおよび監査ログ閲覧サーバの前提 OS」を参照してください。

監査ログ管理サーバは，アクティブ・スタンバイ構成のクラスタ環境に対応しています。アクティブ・スタンバイ構成は，2 ノード・クラスタシステムで，それぞれのサーバを実行系と待機系として設定します。

(2)　監査ログ収集対象サーバの場合

監査ログ収集対象サーバがクラスタ環境で運用されているかどうかによって，システム構成や監査ログ収集対象サーバの構築手順が異なります。なお，監査ログ収集対象サーバがクラスタ環境で運用されている場合，ローカルディスクに出力される監査ログ，および共有ディスクに出力される監査ログを収集できます。

クラスタ環境で運用する場合の前提 OS については「3.2.1(2)　監査ログ収集対象サーバの前提 OS」を参照してください。

監査ログ収集対象サーバは，アクティブ・スタンバイ構成およびアクティブ・アクティブ構成のクラスタ環境に対応しています。

- アクティブ・スタンバイ構成は，2 ノード・クラスタシステムで，それぞれのサーバを実行系と待機系として設定します。この構成では一つの論理ホストが稼働します。
- アクティブ・アクティブ構成は，2 ノード・クラスタシステムで，それぞれのサーバを実行系かつ待機系として設定します。この構成では複数の論理ホストが稼働します。

4.4.4　データベースの運用方法

収集した監査ログを格納するデータベースをどのように作成し，運用するかを決定します。

(1)　データベースのセットアップ時に必要となる項目

監査ログ管理サーバまたは監査ログ閲覧サーバの構築時，データベースをセットアップする際は次の項目を指定します。あらかじめこれらの内容を決定しておいてください。

ログイン ID およびパスワード

データベースへの接続に使用するログイン名とパスワードです。

サービス名

データベースへの接続に使用するサービス名です。ODBC データソース名として使用されます。

ポート番号

データベース用のポート番号です。ほかで使用しないポート番号が必要です。

サイズ

データベースのサイズです。システムの規模に合わせて設定する必要があります。見積もり方法については「4.6.3　データベース容量の見積もり」を参照してください。

ローカルディスク上の格納先

ローカルディスク上のデータベース領域の格納先フォルダです。

共有ディスク上の格納先

クラスタ環境の場合に必要な設定です。共有ディスク上のデータベース領域の格納先フォルダです。

(2)　データベースの取り扱い方法

JP1/Audit Management - Manager では，セットアップしたデータベースに対して，次の表に示す操作ができます。

表 4-3　データベースに対してできる主な操作

項目	内容
バックアップとリストア	使用中のデータベースのトラブルに備え，バックアップを取得します。また，バックアップファイルを使用して，トラブルが発生したデータベースをバックアップ時点の状態にリストアします。
CSV バックアップと CSV リストア	ほかのデータベースへのデータの移行や，データベースの再セットアップが必要になったときに，必要に応じて行う操作です。 使用中のデータベースに格納されているデータを CSV 形式ファイルにバックアップします。また，CSV 形式のバックアップファイルを使用して，ほかのデータベースまたは新しいデータベースにバックアップ時点の監査ログの情報を移行（リストア）します。
再編成	データベースを運用し続けると，データの格納効率が悪くなり，検索機能が低下したりデータベースの容量不足になったりすることがあります。これらの現象を防ぐために，定期的に行う操作です。 データベース内で再利用できなくなった領域を解放し，データベース領域の使用率を低減します。
パスワード変更	設定されているデータベースのパスワードを変更します。

検討項目を次に示します。

1. データベースのバックアップのタイミング
   バックアップを取得するタイミングを決定します。トラブルの発生に備えて，データベースのバックアップは定期的に取得することをお勧めします。
2. パスワード変更のタイミング
   パスワードを変更するタイミングを決定します。パスワードは定期的に変更することをお勧めします。

4.4.5 ユーザ管理

監査証跡管理システムでは，JP1/Base のユーザ管理機能を使って，JP1 ユーザによるユーザ認証やアクセス制御を実施します。このため，あらかじめ次に示す項目について検討しておく必要があります。

認証サーバ

JP1/Audit Management - Manager の監査ログ管理画面を使用するには，JP1 ユーザのユーザ認証が必要になります。このユーザ認証のための認証サーバとして使用する JP1/Base の構築場所を決めておく必要があります。認証サーバの構築場所は任意です。監査ログ管理サーバや監査ログ収集対象サーバに兼用で構築することもできます。

JP1 権限レベル

監査ログ管理画面を操作するための JP1 ユーザの JP1 権限レベルを決めておく必要があります。

JP1 権限レベルには，次の 2 種類があります。

- JP1_Audit_Admin
- JP1_Audit_Operator

どちらも同じ JP1 権限レベルですが，JP1 権限レベルを使い分ける必要がない場合は，「JP1_Audit_Admin」を使用してください。

そのほかに JP1 ユーザ名，パスワード，および JP1 資源グループ名を決めておく必要があります。

4.5　システム構成の検討

監査証跡管理システムに設置するサーバの種類と台数，および各サーバで使用するプログラムを確認しておきます。

監査証跡管理システムを構成する各サーバの設置に関する条件を次の表に示します。この条件を参考に，設置するサーバの種類と台数を確認してください。

表 4-4　監査証跡管理システムを構成するサーバの種類

サーバの種類	説明	設置に関する条件
監査ログ管理サーバ	指定された監査ログを収集するサーバです。	通常，一つのシステムに 1 台以上設置します。 クラスタ環境の場合は，実行系サーバ，および待機系サーバをそれぞれ 1 台ずつ設置します。
監査ログ収集対象サーバ	収集対象の監査ログが出力されるサーバです。	収集対象に応じて，1 台以上設置します。
監査ログ閲覧サーバ	監査ログ管理サーバからバックアップした監査ログのデータを閲覧するためのサーバです。	設置は任意です。※

注※

監査ログ閲覧サーバの運用例については「4.4.2　収集した監査ログの取り扱い方法」を参照してください。

各サーバに必要なプログラム，およびシステム構成例については「3.　システム構成」を参照してください。

監査ログ管理サーバの注意事項

監査ログ管理サーバ 1 台の監査ログ収集性能は，1 日当たり 2,000 万件程度※が上限となります。これを超えるようなログ収集が続くと，未収集の監査ログが増加し，監査ログが収集できなくなります。監査ログ数が収集の上限を超える場合は，監査ログ管理サーバを複数台設置して，1 台の監査ログ管理サーバで収集するログ件数を減らしてください。なお，収集対象プログラムの追加や収集対象サーバの追加といったシステム変更をする場合には，収集性能を超えないか検証してください。

注※

サービスが 24 時間動作して収集した場合の件数です。監査ログのサイズやシステムのスペック，ネットワークなどによって件数は異なります。

また，監査ログ管理データベースの容量がいっぱいになると，データベースのメンテナンス，監査ログの検索に時間がかかり，監査証跡管理システムの運用に支障を来すおそれがあります。参考として，データベースのメンテナンス，監査ログの検索性能を次に示します。次に示す時間よりも短い時間で完了したい場合，監査が完了した監査ログを，バックアップとして媒体などに保存したあとに監査ログ管理サーバから削除することで，監査ログ管理データベースの負荷を軽減してください。また，監査ログ閲覧サーバを構築して，監査ログを閲覧することを推奨します。監査ログ閲覧サーバは，バックアップした過去の監査ログを参照するためのサーバとして使用し，日々の確認には監査ログ閲覧サーバを使用しないで監査ログ管理サーバを使用します。監査ログ閲覧サーバを構築することによって，監査ログの

収集・監査専用のサーバと監査が完了した監査ログを閲覧する閲覧専用のサーバに分けて，監査ログを管理できます。

表 4-5　データベースのメンテナンスおよび監査ログの検索性能

大項目	小項目	時間	備考
データベースのメンテナンス	データベースのバックアップ	約 2 時間	[測定環境] 機種：HA8000/TS20(AM1) CPU：Intel(R) Xeon(R) CPU E5-2470 0 @2.30GHz 2.30GHz (2 プロセッサ) HDD：2TB（RAID5） 実装メモリ(RAM)：128GB OS：Windows Server 2012 R2 Datacenter [データベース情報] サイズ：LL 監査ログ件数：109,500,000 件 データ領域使用率：69% インデクス領域使用率：29% [監査ログ情報] 監査ログ収集対象サーバの数：150 台 サーバ 1 台 1 日当たりの監査ログ件数：400 件/台 プログラム数：100 プログラム当たりの監査ログ件数：1,095,000 件
	データベースのリストア	約 7.5 時間	
	データベースの CSV バックアップ	約 2 時間	
	データベースの CSV リストア	約 25 時間	
	データベースの再編成	約 28 時間	
	データベースの使用状況確認	約 1 分	
	監査ログのバックアップ(1 日)	約 30 秒	
	監査ログのバックアップ(1 か月)	約 40 分	
	監査ログのバックアップ(全件)	約 24.5 時間	
	監査ログの移動	約 1.5 時間	
	監査ログのインポート(バルクモード)(1 日)※	約 1.5 分	
	監査ログのインポート(バルクモード)(1 か月)※	約 36.5 分	
	監査ログのインポート(バルクモード)(全件)※	約 34 時間	
	監査ログのインポート(マイナーモード)(1 日)※	約 4.5 分	
	監査ログのインポート(マイナーモード)(1 か月)※	約 2.5 時間	
	データ削除(バルクモード)(1 件)	約 30.5 時間	
	データ削除(バルクモード)(全件)	約 14 秒	
	データ削除(マイナーモード)(1 日)	約 20.5 分	
	データ削除(マイナーモード)(1 か月)	約 4 時間	
監査ログの検索	検索条件なし	約 16 時間	
	検索条件　日付範囲(1 か月)	約 6.5 分	
	検索条件　プログラム名だけ	約 29 分	
	検索条件　日付範囲(1 か月)+プログラム名	約 21.5 分	

大項目	小項目	時間	備考
	検索条件　日付範囲(1 か月)+プログラム名+事象結果	約 20 分	

注※

インポート時のデータベース内のデータ件数は 0 件

データベースのメンテナンスや監査ログのバックアップなどの運用で JP1/Audit Management - Manager のサービスを停止する場合は，ログ件数などを検討して，サービスを停止するまでに定時収集が終了するように運用してください。監査ログ数が収集の上限を超える状況，かつ JP1/Audit Management - Manager のサービスが停止しているときに，イベントデータベースの切り替えが発生すると，監査ログが収集できない状態になるおそれがあります。

JP1/Audit Management - Manager のサービス停止中に監査ログを退避する設定をしている場合，サービスの再起動後の収集で退避した監査ログを格納します。そのため，退避したデータの件数分，収集件数が通常時よりも多くなります。サービスの再起動後の収集では，ログ件数に注意してください。

4.6　容量の見積もり

この節では，JP1/Audit Management - Manager のメモリ所要量，ディスク占有量，および監査ログ管理データベースの容量の見積もりについて説明します。

4.6.1　メモリ所要量の見積もり

JP1/Audit Management - Manager で使用するメモリ所要量を次の表に示します。

表 4-6　メモリ所要量

項番	種別	メモリ所要量の値または計算式 (単位：メガバイト)
1	固定値	170
2	変動値	(0.004×a) ＋ b
3	データベース値	S サイズの場合：853 M サイズの場合：1,489 L サイズの場合：1,510 LL サイズの場合：1,530

（凡例）

a：一つの収集対象サーバから一度に収集する監査ログのレコード数（最大レコード数：250,000 件）

b：JP1/Audit Management - Manager のインストール先フォルダ¥conf¥rule 配下の使用する正規化ルールファイルのサイズの和（単位：メガバイト）

監査ログ収集対象サーバ上で使用するメモリ所要量を次に示します。

admagtinstall コマンド

コマンド実行時に必要とするメモリ量（単位：バイト）を次に示します。

1,163,000

admagtsetup コマンド

コマンド実行時に必要とするメモリ量（単位：バイト）を次に示します。

1,163,000 ＋ 946×e

（凡例）

e：admagtsetup で設定しているサーバの数

admhasetup コマンド

コマンド実行時に必要とするメモリ量（単位：バイト）を次に示します。

1,163,000

admuxlogcol コマンド

コマンド実行時に必要とするメモリ量（単位：バイト）を次に示します。

1,049,000 ＋ 1,300×変換するデータ件数

adm_adaptercmd コマンド

- 「監視の開始」実行時に必要とするメモリ量（単位：バイト）を次に示します。
  1,154,000 ＋ p×2 ＋ d ＋ n ＋ f ＋ s ＋ t ＋ w ＋ a
  （凡例）
  p：製品名の長さ
  d：監査ログ収集マネージャで指定したログファイルディレクトリのパスの長さ
  n：ファイル数の桁数（製品定義ファイルの AuditLogNum で指定している数値の桁数）
  f：ファイル名の長さの合計（製品定義ファイルの AuditLogName で指定しているファイル名の長さの合計＋ファイル数－1）
  s：監査ログ収集マネージャで指定しているサーバ名の長さ
  t：動作定義情報のサイズ（動作定義ファイルのサイズ＋c×2-(L＋1)）
  （凡例）
  c：半角スペース，パーセント（%），ダブルクォーテーション（”），シングルクォーテーション（’），コンマ（,），およびタブの文字数
  L：行数
  w：16,384（サーバが Windows の場合に加算する）
  a：1,048,576（「OS 起動時に自動的に監視を開始する」を指定している場合，またはサーバが UNIX の場合に加算する）
- 「監視の停止」実行時に必要とするメモリ量（単位：バイト）を次に示します。
  1,154,000 ＋ p ＋ w ＋ a
  （凡例）
  p：製品名の長さ
  w：8,192（サーバが Windows の場合に加算する）
  a：1,048,576（「OS 起動時に自動的に監視を開始する」を指定している場合に加算する）
- 「最新の情報に更新」実行時に必要とするメモリ量（単位：バイト）を次に示します。
  1,155,000 ＋ 25×p ＋ n×4 ＋ w
  （凡例）
  p：プログラム数（収集対象サーバ上で監視しているプログラムの数）
  n：プログラム名の長さの合計（収集対象サーバ上で監視しているすべてのプログラム名の長さの合計）
  w：8,192（サーバが Windows の場合に加算する）

admlogtrapd サービス

サービス実行時に必要とするメモリ量（単位：バイト）を次に示します。

1,163,000

4.6.2　ディスク占有量の見積もり

JP1/Audit Management - Manager で使用するファイルのディスク占有量を次の表に示します。

表 4-7　ファイルごとのディスク占有量

項番	種別	ディスク占有量の値または見積もり式 (単位：メガバイト)
1	固定部分ファイル	3,226※1
2	ログファイル	(a×b) ＋ (c×d)※2
3	監査ログファイル	(e×f) ＋ (g×h)※2

（凡例）

a：JP1/Audit Management - Manager のログファイル数（デフォルト値は 10）

b：JP1/Audit Management - Manager のログファイルサイズ（単位：メガバイト。デフォルト値は 5 メガバイト）

c：監査ログ管理画面のログファイル数（デフォルト値は 10）

d：監査ログ管理画面のログファイルサイズ（単位：メガバイト。デフォルト値は 5 メガバイト）

e：JP1/Audit Management - Manager の監査ログファイル数（デフォルト値は 10）

f：JP1/Audit Management - Manager の監査ログファイルサイズ（単位：メガバイト。デフォルト値は 5 メガバイト）

g：監査ログ管理画面の監査ログファイル数（デフォルト値は 10）

h：監査ログ管理画面の監査ログファイルサイズ（単位：メガバイト。デフォルト値は 5 メガバイト）

注※1

200（インストールに必要なサイズ）＋ 1,043（製品内部トレース）＋ 1,983（その他）

注※2

a～h については，JP1/Audit Management - Manager のセットアップ（[マネージャセットアップ] ダイアログ）で値を変更できます。設定内容の変更については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

なお，c および d は，JP1/Audit Management - Manager のセットアップで監査ログファイルを出力するように設定している場合の値です。

監査ログ収集対象サーバ上で使用するディスク占有量を次に示します。

表 4-8　OS ごとのディスク占有量

項番	OS	種別	ディスク占有量の値または見積もり式 (単位：メガバイト)
1	AIX	固定値	28
2	HP-UX	固定値	28
3	Linux	固定値	28

項番	OS	種別	ディスク占有量の値または見積もり式 (単位：メガバイト)
4	Solaris	固定値	28
5	Windows	固定値	20
6	Windows 以外	変換ログ	12,000

4.6.3 データベース容量の見積もり

システム構築時に，監査証跡管理システムで使用するデータベースのサイズを設定します。サイズは運用中に変更できないため，あらかじめ必要なディスク容量を算出し，設定してください。

なお，データベースに関する一部の操作では，一時的に作業用フォルダを使用する場合があります。作業用フォルダで使用するディスク容量も考慮して，必要なディスク容量を算出してください。

(1) システムに必要なディスク容量

システム構築時に選択するデータベースのサイズの種類と，各サイズのシステム規模の目安について，次の表に示します。

表 4-9 データベースのサイズの種類

サイズの 種類	ディスク容量 (単位：ギガバイト)	監査ログの 格納領域の目安 (単位：ギガバイト)	システム規模の目安
S サイズ	12.0	約 3.0	総監査ログ量： 1,095,000 行 なお，総監査ログ量は，次の場合を想定したサイズです。 • 監査ログ収集対象サーバの数：30 台以内 • システムの運用期間：1 年 • マシン 1 台 1 日当たりの監査ログの収集量：100 行以内
M サイズ	56.0	約 15.0	総監査ログ量： 5,475,000 行 なお，総監査ログ量は，次の場合を想定したサイズです。 • 監査ログ収集対象サーバの数：150 台以内 • システムの運用期間：1 年 • マシン 1 台 1 日当たりの監査ログの収集量：100 行以内
L サイズ	190.0	約 64.0	総監査ログ量： 27,375,000 行 なお，総監査ログ量は，次の場合を想定したサイズです。

サイズの種類	ディスク容量（単位：ギガバイト）	監査ログの格納領域の目安（単位：ギガバイト）	システム規模の目安
			• 監査ログ収集対象サーバの数：150 台以内 • システムの運用期間：5 年 • マシン 1 台 1 日当たりの監査ログの収集量：100 行以内
LL サイズ	760.0	約 256.0	総監査ログ量： 109,500,000 行 なお，総監査ログ量は，次の場合を想定したサイズです。 • 監査ログ収集対象サーバの数：150 台以内 • システムの運用期間：5 年 • マシン 1 台 1 日当たりの監査ログの収集量：400 行以内

また，クラスタ環境で運用する場合には，共有ディスク上とローカルディスク上にそれぞれ次の表に示すディスク容量が必要です。

表 4-10　クラスタ環境で運用する場合のディスク容量

サイズの種類	容量の合計（単位：ギガバイト）	共有ディスクに必要な容量（単位：ギガバイト）	ローカルディスクに必要な容量（単位：ギガバイト）
S サイズ	12.0	9.8	2.2
M サイズ	56.0	44.0	12.0
L サイズ	190.0	137.0	53.0
LL サイズ	760.0	510.0	250.0

なお，収集する監査ログの量が運用途中で大幅に増加することを想定して，余裕を持ったデータベースのサイズを設定することをお勧めします。

また，JP1/Audit Management - Manager の運用を安定して継続するため，監査ログ管理データベースの使用率を定期的に確認することをお勧めします。ディスク容量の管理については「10.2　データベースのディスク容量の管理」を参照してください。

(2)　データベースの操作時に必要なディスク容量

データベースに関する次の操作では，ディスク上に一時的な作業用フォルダが作成されます。このため，作業用フォルダで使用するディスク容量が必要となります。

- データベースの再編成
- データベースの CSV リストア

- データベースのデータ削除（バルク削除モードの場合）
- 監査ログのインポート（バルク挿入モードの場合）

各操作で必要なディスク容量の目安について，次に説明します。

(a) データベースの再編成で必要なディスク容量

見積もり式を次の表に示します。二つの見積もり式のうち，値が大きい方を必要なディスク容量として見積もってください。

表 4-11 データベースの再編成で必要なディスク容量の見積もり式

項番	見積もり式（単位：バイト）
1	a が 3,856,290 以下の場合：3,876×a + 3,376 a が 3,856,291 以上の場合：4,920×a + 3,888
2	136×14×b×c + 2,512

（凡例）

a：データベースに格納する監査ログデータの総件数

b：監査ログ統計パターンとして設定する集計パターンの数

c：監査ログ統計情報を生成する日数

(b) データベースの CSV リストアで必要なディスク容量

見積もり式を次の表に示します。二つの見積もり式のうち，値が大きい方を必要なディスク容量として見積もってください。

表 4-12 データベースの CSV リストアで必要なディスク容量の見積もり式

項番	見積もり式（単位：バイト）
1	a が 3,856,290 以下の場合：2,084×a + 1,024 a が 3,856,291 以上の場合：3,128×a + 1,536
2	48×14×b×c + 1,024

（凡例）

a：リストアの対象となる監査ログデータの総件数

b：監査ログ統計パターンとして設定する集計パターンの数

c：監査ログ統計情報を生成する日数

(c) データベースのデータ削除で必要なディスク容量（バルク削除モードの場合）

見積もり式を次の表に示します。なお，この見積もりは admdbdelete コマンドでバルク削除モードを指定する場合に必要となるディスク容量です。

表 4-13　データベースのデータ削除で必要なディスク容量の見積もり式（バルク削除モードの場合）

見積もり式（単位：バイト）
a が 3,856,290 以下の場合：3,784×a ＋ 1,024 a が 3,856,291 以上の場合：4,828×a ＋ 1,536

（凡例）

a：削除対象外となる監査ログデータの総件数

(d)　監査ログのインポートで必要なディスク容量（バルク挿入モードの場合）

見積もり式を次の表に示します。なお，この見積もりは admimport コマンドでバルク挿入モードを指定する場合に必要となるディスク容量です。

表 4-14　監査ログのインポートで必要なディスク容量の見積もり式（バルク挿入モードの場合）

見積もり式（単位：バイト）
(a ＋ b)が 3,856,290 以下の場合：2,084×(a ＋ b)＋ 1,024 (a ＋ b)が 3,856,291 以上の場合：3,128×(a ＋ b)＋ 1,536

（凡例）

a：データベースに格納されている監査ログデータの総件数

b：インポートする監査ログデータの総件数

5 システム構築

この章では，監査証跡管理システムで使用する各サーバおよびクライアントの構築作業について説明します。

5.1　システム構築の流れ

この節では，監査証跡管理システムの構築の流れについて説明します。

監査証跡管理システムを使用するために，サーバとクライアントを構築する必要があります。

5.1.1　サーバの構築の流れ

サーバの構築方法の流れについて説明します。

構築が必須のサーバと構築が任意のサーバをそれぞれ次に示します。

構築が必須のサーバ

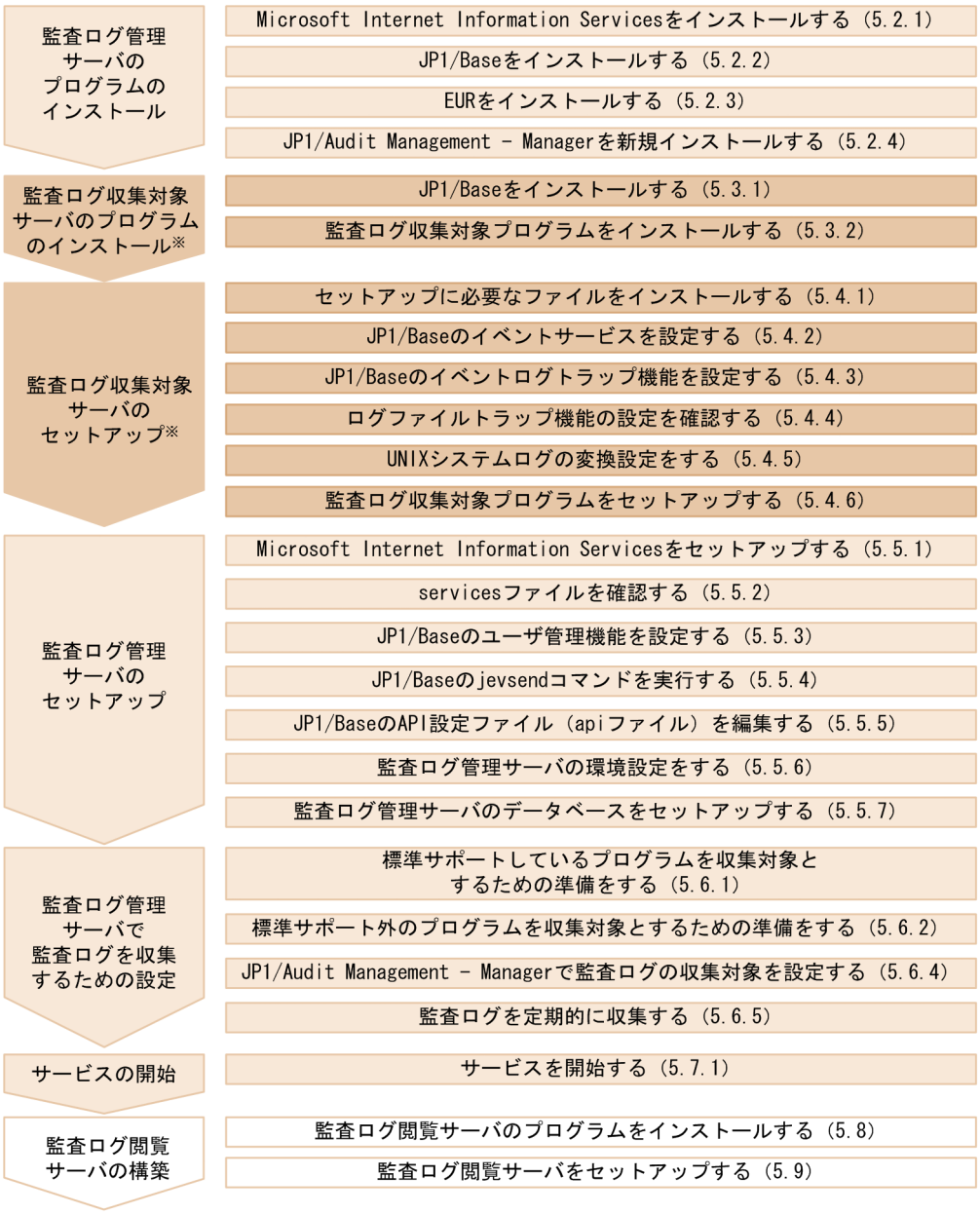
- 監査ログ管理サーバ
- 監査ログ収集対象サーバ

構築が任意のサーバ

- 監査ログ閲覧サーバ

各サーバの構築の流れを次の図に示します。各項目の内容については，括弧内の個所を参照してください。

図 5-1　各サーバでの構築の流れ



注※

監査ログ管理サーバ上にあるプログラムの監査ログを収集対象とする場合は，監査ログ収集対象サーバのセットアップ手順と同様の手順を，監査ログ管理サーバで実施してください。

なお，JP1/Audit Management - Manager をバージョンアップする場合の構築の流れについては「5.12 JP1/Audit Management - Manager のバージョンアップ」を参照してください。

参考

サーバの構築前の準備として，監査ログ管理サーバで監査ログ収集対象サーバのホスト名を名前解決できるようにしてください。また，監査ログ収集対象サーバでも監査ログ管理サーバのホスト名を名前解決できるようにしてください。

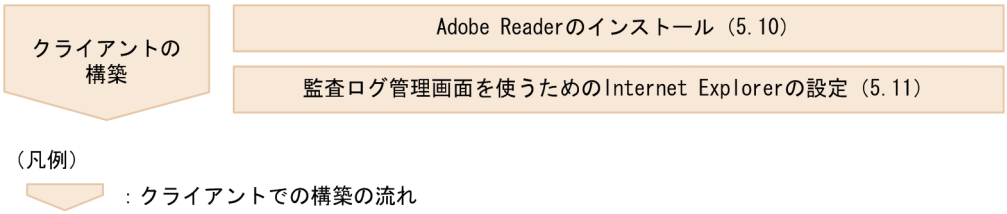
5.1.2　クライアントの構築の流れ

クライアントの構築方法の流れについて説明します。

サーバの構築が完了したら，クライアントを構築します。クライアントを構築することによって，監査ログ管理画面を操作したり，閲覧したりできるようになります。

クライアントの構築の流れを次の図に示します。各項目の内容については，括弧内の個所を参照してください。

図 5-2　クライアントでの構築の流れ



5.2　監査ログ管理サーバのプログラムのインストール

監査ログ管理サーバで必要なプログラムをインストールします。

まず，次に示す前提プログラムをインストールしてください。

- Microsoft Internet Information Services
- JP1/Base
- EUR（任意）

これらの前提プログラムのインストール完了後，JP1/Audit Management - Manager をインストールしてください。

なお，すでに JP1/Audit Management - Manager がインストールされている場合は，上書きインストールを実施します。JP1/Audit Management - Manager をバージョンアップする場合などは，上書きインストールを実施してください。JP1/Audit Management - Manager の上書きインストールの詳細については「5.2.5　JP1/Audit Management - Manager を上書きインストールする」を参照してください。

5.2.1　Microsoft Internet Information Services をインストールする

Microsoft Internet Information Services をインストールします。

なお，Microsoft Internet Information Services のほかに，Microsoft Internet Information Services の役割サービスの追加で，「ASP」および「IIS 6 管理互換」もインストールしてください。

「IIS 6 管理互換」をインストールする際は，「IIS 6 メタベース互換」「IIS 6 WMI 互換」「IIS 6 スクリプトツール」にチェックが付いていることを確認してください。

Microsoft Internet Information Services のインストール手順については，Windows のマニュアルで Microsoft Internet Information Services のインストール方法に関する記述を参照してください。

5.2.2　JP1/Base をインストールする

JP1/Base をインストールします。

JP1/Base のインストール手順については，マニュアル「JP1/Base 運用ガイド」を参照してください。

5.2.3　EUR をインストールする

EUR のインストールは任意です。

EUR は監査ログの検索結果や集計結果を PDF ファイルに出力したい場合にインストールしてください。

EUR のインストール手順については，EUR のマニュアルを参照してください。

5.2.4　JP1/Audit Management - Manager を新規インストールする

JP1/Audit Management - Manager を新規インストールします。

JP1/Audit Management - Manager を上書きインストールする場合は「5.2.5　JP1/Audit Management - Manager を上書きインストールする」を参照してください。

JP1/Audit Management - Manager の新規インストールは，提供媒体を使用してインストールするかまたは JP1/NETM/DM を使用してリモートインストールします。JP1/NETM/DM を使ったリモートインストールについては，マニュアル「JP1/NETM/DM 運用ガイド 1(Windows(R)用)」を参照してください。

> **参考**
>
> リモートインストールによって新規インストールした場合，プログラムフォルダとして「JP1_NETM_Audit」が，仮想ディレクトリとして「**JP1/Audit Management - Manager のインストール先フォルダ**¥wwwroot」がそれぞれ自動的に設定されます。これらの値は変更できません。

JP1/Audit Management - Manager の新規インストールについて説明します。

(1)　新規インストール前の作業

JP1/Audit Management - Manager をインストールする前に，次に示す作業を実施してください。

- Administrator の権限で Windows にログオンする
- 次に示すプログラムのインストールが完了しているかを確認する
  - Microsoft Internet Information Services
  - JP1/Base
- World Wide Web Publishing Service サービスを停止する

また，必要に応じて次に示す作業も実施してください。

- 32 ビットのアプリケーションを動作させるための設定をする
  x64 マシンへ JP1/Audit Management - Manager をインストールする場合に必要な作業です。
  コマンドプロンプトでカレントディレクトリを「**システムドライブ**¥Inetpub¥AdminScripts」に移動したあと，次に示すコマンドを実行してください。

```
cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 "true"
```

- **インターネットゲストアカウントのパスワードを設定する**

  Microsoft Internet Information Services のインストール後，かつ JP1/Audit Management - Manager のインストール前にコンピュータ名を変更する場合は，次に示す手順でインターネットゲストアカウントを作成し，パスワードを設定してください。

  1. インターネットゲストアカウントとして，「IUSR_**変更後のマシン名**」を追加する。
  2. 「IUSR_**変更後のマシン名**」のパスワードを設定する。
  3. そのほかの「IUSR_**変更後のマシン名**」の内容を設定する。

     既存のインターネットゲストアカウント「IUSR_**変更前のマシン名**」と同様の内容で設定してください。
  4. JP1/Audit Management - Manager をインストールする。
  5. 仮想ディレクトリ「jp1netmaudit」のアクセスユーザのパスワードを設定する。

     「IUSR_**変更後のマシン名**」のパスワードを設定してください。

- **拡張子「VBS」の関連づけの設定を確認する**

  拡張子「VBS」の関連づけの設定が，「Microsoft (r) Windows Based Script Host」で設定されているかどうか確認してください。

- **インストール先に十分な空き容量があるかどうかを確認する**

  インストール先の空き容量が 250 メガバイト未満または仮想ディレクトリの空き容量が 20 メガバイト未満の場合はインストールが中断されます。このため，インストール先に十分な空き容量があるかどうかを確認してください。

(2) 新規インストール

新規インストールの手順を次に示します。

1. **提供媒体を CD-ROM ドライブに入れる。**

   起動したインストーラの指示に従ってインストールを進めます。インストール時は，インストール先フォルダを設定してください。

   インストーラを起動すると，インストールする対象を選択するダイアログが表示されます。JP1/Audit Management - Manager のコンポーネントを選択してください。

2. **［インストール実行］ボタンをクリックする。**

   インストールの開始を確認するダイアログが表示されます。インストールの開始を確認するダイアログで［OK］ボタンをクリックすると，インストールを開始するダイアログが表示されます。

3. **［次へ］ボタンをクリックする。**

   ユーザ情報を入力するダイアログが表示されます。

4. **ユーザ名，会社名を入力する。**

5. **［次へ］ボタンをクリックする。**

インストール先フォルダを指定するダイアログが表示されます。

6. インストール先フォルダを指定する。

指定したフォルダにインストールされます。

必ずローカルディスク上のフォルダを指定してください。なお，パス中にフォルダ名またはファイル名として使用できる文字は，半角英数字，「△（半角スペース）」，「_」，「.」，「(」，および「)」です。デフォルトのインストール先は「**システムドライブ¥**Program Files¥HITACHI¥jp1netmaudit ¥manager」です。ネットワークドライブや共有ディスク上のフォルダにはインストールできません。

7. [次へ] ボタンをクリックする。

プログラムフォルダを確認するためのダイアログが表示されます。

プログラムアイコンを追加するフォルダを確認してください。デフォルトのフォルダ名は「JP1_NETM_Audit」です。

8. [次へ] ボタンをクリックする。

監査ログ管理サーバの仮想ディレクトリを設定するダイアログが表示されます。デフォルトの仮想ディレクトリは「**JP1/Audit Management - Manager のインストール先フォルダ¥**wwwroot」です。ファイルを大量にアップロードする場合など，仮想ディレクトリを変更する必要がある場合は，仮想ディレクトリに設定したいフォルダを指定してください。

9. [次へ] ボタンをクリックする。

データベースの内容を変更するコマンド（admdbdelete，admimport）を実行する際に，パスワード入力を要求するかどうかを設定するダイアログが表示されます。[パスワード入力を要求する] を選択すると，コマンド実行時にデータベースのパスワード入力が要求されます。[パスワード入力を要求しない] を選択すると，コマンド実行時にデータベースのパスワード入力は要求されません。コマンドを自動実行する場合は，[パスワード入力を要求しない] を選択してください。

10. [次へ] ボタンをクリックする。

現在の設定内容を確認するためのダイアログが表示されます。設定内容を確認してください。

11. [次へ] ボタンをクリックする。

インストールを開始します。インストールが終了すると，インストールが終了したことを通知するダイアログが表示されます。

12. [完了] ボタンをクリックする。

インストールを終了します。

13. Windows を再起動する。

インストールが正常に終了したら，必ず Windows を再起動してください。

なお，JP1/Audit Management - Manager を新規インストールすることによって，すでにインストールしている Microsoft Internet Information Services の設定内容が変更されます。ほかのアプリケーションで Microsoft Internet Information Services を使用する場合に留意してください。変更される設定内容について説明します。

インストール時に変更される Microsoft Internet Information Services の設定内容

- 「Web サイト」
  「既定の Web サイト」に，JP1/Audit Management - Manager の仮想ディレクトリ「jp1netmaudit」が作成されます。「既定の Web サイト」は，Microsoft Internet Information Services のバージョンによって「Default Web Site」と表示されることがあります。
- 「アプリケーションプール」
  「DefaultAppPool」に「jp1netmaudit」が作成されます。また，「DefaultAppPool」のプロパティには，「識別」タブの「アプリケーションプール ID」に，「定義済み」－「Local System」が設定されます。
- 「Web サービス拡張」
  「Active Server Pages」に「許可」が設定されます。

(a) Microsoft Internet Information Services の自動設定をしていない場合の対処方法

JP1/Audit Management - Manager のインストール前に，Microsoft Internet Information Services の役割サービスで「IIS 6 管理互換」をインストールしておく必要があります。

インストールしていない場合は，仮想ディレクトリの設定を次に示す手順で実施してください。

- 役割サービスをインストールする
  役割サービスをインストールする手順を次に示します。
  1. [サーバーマネージャ] ウィンドウの［役割］－［役割サービスの追加］を選択する。
     役割サービスを選択するダイアログが表示されます。
  2. 「ASP」サービスと「IIS 6 管理互換」サービスをチェックする。
     「IIS 6 メタベース互換」「IIS 6 WMI 互換」「IIS 6 スクリプトツール」にチェックが付いていない場合はチェックを付けます。
  3. [次へ] ボタンをクリックする。
     インストールオプションを確認するダイアログが表示されます。
  4. 手順 2 で選択した役割サービスが表示されていることを確認して［インストール］ボタンをクリックする。
     インストールが完了するとインストール結果を示すダイアログが表示されます。
  5. [閉じる] ボタンをクリックする。
- アプリケーションプールを設定する
  アプリケーションプールを設定する手順を次に示します。
  1. インターネットインフォメーションサービスマネージャを起動する。
  2. [アプリケーションプール] をクリックする。
  3. [操作] －［詳細設定］を選択する。
     ［詳細設定］ダイアログが表示されます。

4. 全般項目の 32 ビットアプリケーションの有効化に「True」を指定する。
5. プロセスモデル項目の ID に「LocalSystem」を指定する。
6. [OK] ボタンをクリックする。
7. World Wide Web Publishing Service サービスを再起動する。

- **アプリケーション（仮想ディレクトリ）を設定する**

  アプリケーション（仮想ディレクトリ）を設定する手順を次に示します。

  1. [サイト] − [Default Web Site] を右クリックして [アプリケーションの追加] を選択する。
     [アプリケーションの追加] ダイアログが表示されます。
  2. [選択] ボタンをクリックして設定したアプリケーションプールを指定する。
  3. 「エイリアス」に「jp1netmaudit」を指定して [OK] ボタンをクリックする。
  4. 「物理パス」に「インストール時に指定した仮想ディレクトリ」を指定して [OK] ボタンをクリックする。

- **ハンドラマッピングを設定する**

  ハンドラマッピングを設定する手順を次に示します。

  1. 「サイト」から [Default Web Site] − [jp1netmaudit] − [ハンドラマッピング] を選択する。
  2. [操作] − [機能を開く] を選択する。
  3. [操作] − [機能のアクセス許可の編集] を選択する。
     [機能のアクセス許可の編集] ダイアログが表示されます。
  4. 「読み取り」と「スクリプト」をチェックして [OK] ボタンをクリックする。

- **ディレクトリ参照を設定する**

  ディレクトリ参照を設定する手順を次に示します。

  1. 「サイト」から [Default Web Site] − [jp1netmaudit] − [ディレクトリの参照] を選択する。
  2. [操作] − [機能を開く] を選択する。
  3. [操作] − [無効にする] を選択する。

- **ログ記録を設定する**

  ログ記録を設定する手順を次に示します。

  1. 「サイト」から [Default Web Site] − [jp1netmaudit] − [ログ記録] を選択する。
  2. [操作] − [機能を開く] を選択する。
  3. [操作] − [有効にする] を選択する。

- **既定のドキュメントを設定する**

  既定のドキュメントを設定する手順を次に示します。

  1. 「サイト」から [Default Web Site] − [jp1netmaudit] − [既定のドキュメント] を選択する。
  2. [操作] − [機能を開く] を選択する。

3. [操作] − [追加] を選択する。
4. 「ALM_Login.asp」を指定して［OK］ボタンをクリックする。

- **認証を設定する**

  認証を設定する手順を次に示します。

  1. 「サイト」から［Default Web Site］−［jp1netmaudit］−［認証］を選択する。
  2. [操作] −［機能を開く］を選択する。
  3. [匿名認証] を選択して［操作］−［編集］を選択する。
     ［匿名認証視覚情報の編集］ダイアログが表示されます。
  4. 「特定のユーザ」を選択したあと「IUSR」を指定して［OK］ボタンをクリックする。
  5. 「匿名認証」を選択して［操作］−［有効にする］を選択する。

- **アクセス許可を設定する**

  アクセス許可を設定する手順を次に示します。

  1. エクスプローラで［インストール時に設定した仮想ディレクトリ］を選択する。
  2. [ファイル] −［プロパティ］を選択する。
  3. [セキュリティ] タブを選択して［編集］ボタンをクリックする。
  4. [追加] ボタンをクリックする。
  5. 「IUSR」を指定して［OK］ボタンをクリックする。
  6. 「IUSR」を選択したあと許可項目の「変更」をチェックして［OK］ボタンをクリックする。
  7. エクスプローラで「インストールディレクトリ¥log」ディレクトリを選択する。
  8. 手順 2 から手順 6 までの操作を再度実施する。

5.2.5 JP1/Audit Management - Manager を上書きインストールする

JP1/Audit Management - Manager を上書きインストールします。

上書きインストールする JP1/Audit Management - Manager のバージョンが，すでにインストールされている JP1/Audit Management - Manager のバージョンより古い場合，上書きインストールは実施できません。

JP1/Audit Management - Manager の上書きインストールは，提供媒体を使用してインストールするかまたは JP1/NETM/DM を使用してリモートインストールします。JP1/NETM/DM を使ったリモートインストールについては，マニュアル「JP1/NETM/DM 運用ガイド 1(Windows(R)用)」を参照してください。

JP1/Audit Management - Manager の上書きインストールについて説明します。

(1)　上書きインストール前の作業

JP1/Audit Management - Manager を上書きインストールする前に，次に示す作業を実施してください。

- **新規インストール前の作業と同様の作業を実施する**

  作業の詳細は「5.2.4(1)　新規インストール前の作業」を参照してください。

- **JP1/Audit Management - Manager のバックアップを取得する**

  上書きインストール中にエラーが発生した場合に備えて，作業する前の監査ログ管理データベースの内容に戻せるように，JP1/Audit Management - Manager の環境定義のバックアップを取得してください。バックアップの取得が必要なフォルダを次に示します。

  - JP1/Audit Management - Manager のインストール先フォルダ¥conf
  - JP1/Audit Management - Manager の仮想ディレクトリ¥conf

  バックアップを取得する前に，JP1/Audit Management - Manager のサービスを停止させてください。JP1/Audit Management - Manager のサービスの開始および停止については「5.7　監査ログ管理サーバの開始・停止」を参照してください。

- **監査ログ管理データベースのバックアップまたは CSV バックアップを取得する**

  上書きインストール中にエラーが発生した場合に備えて，監査ログ管理データベースのバックアップまたは CSV バックアップを取得してください。監査ログ管理データベースのバックアップや CSV バックアップは，データベースマネージャまたはコマンドを使用して取得します。データベースのバックアップの取得方法については「10.1.3　データベースのバックアップ」を参照してください。また，データベースの CSV バックアップの取得方法については「10.1.7　データベースの CSV バックアップ」を参照してください。

- **JP1/Audit Management - Manager が配布するファイルのバックアップを取得する**

  上書きインストールを実施すると，動作定義ファイル，製品定義ファイル，および正規化ルールファイルなど，インストーラで配布しているファイルが上書きされます。このため，これらのファイルを編集している場合は，事前にバックアップを取得してください。また，必要に応じて，取得したバックアップファイルを上書きインストール後の環境に反映させてください。

  なお，JP1/Audit Management - Manager が配布するファイルの一覧については「付録 A.1　JP1/Audit Management - Manager のファイル一覧」および「付録 A.2　JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧」を参照してください。

(2)　上書きインストール

上書きインストールする手順は，新規インストールの手順と同様です。新規インストールの手順については「5.2.4(2)　新規インストール」を参照してください。また，新規インストール時と同様に，上書きインストールの場合も必ず Windows を再起動してください。

なお，次の情報については上書きインストール時に自動で引き継がれます。

- ユーザ情報
- インストール先フォルダ

- プログラムフォルダ
- 仮想ディレクトリ

上書きインストール中にエラーが発生した場合，表示されるメッセージに従ってエラーを取り除いてから，上書きインストールをし直してください。

注意事項

監査ログ閲覧サーバを導入している場合は，監査ログ閲覧サーバの JP1/Audit Management - Manager を，監査ログ管理サーバの JP1/Audit Management - Manager と同じバージョンにバージョンアップしてください。バージョンアップ方法は，監査ログ管理サーバと同様です。

5.2.6　JP1/Audit Management - Manager をアンインストールする

JP1/Audit Management - Manager のアンインストールについて説明します。

(1)　アンインストール前の作業

JP1/Audit Management - Manager をアンインストールする前に，次に示す作業を実施してください。

- Administrator の権限で Windows にログオンする
- World Wide Web Publishing Service サービスを停止する
- JP1/Audit Management - Manager のサービスを停止する

  停止するサービスの詳細は「5.7.2　監査ログ管理サーバを停止する」を参照してください。

さらに，必要に応じて次に示す作業も実施してください。

- データベースのバックアップまたは CSV バックアップを取得する

  アンインストールするとデータベース内の領域が削除されます。このため，アンインストール後にデータベース上のデータを使用する場合は，あらかじめデータベースのバックアップまたはデータベースの CSV バックアップを取得してください。

  データベースのバックアップの取得方法については「10.1.3　データベースのバックアップ」を参照してください。また，データベースの CSV バックアップの取得方法については「10.1.7　データベースの CSV バックアップ」を参照してください。
- 設定している収集対象の監視を停止し，削除する

  JP1/Audit Management - Manager を再度インストールしない場合，監査ログ収集対象サーバで監査ログを収集する必要がない収集対象は監視を停止し，［監査ログ収集マネージャ］ウィンドウから削除してください。削除することによって，収集対象サーバ上の監査ログ専用イベントサーバへ監査ログが蓄積されなくなります。もし，実施しないでアンインストールすると，収集対象サーバ上の監査ログ専用イベントサーバに監査ログが蓄積し，ディスク容量が圧迫されるおそれがあります。

(2) アンインストール

1. コントロールパネルの「プログラムと機能」を開いて「JP1/Audit Management - Manager」を選択する。

2. [アンインストール] をクリックする。

   削除を確認するダイアログが表示されます。[はい] ボタンをクリックすると，JP1/Audit Management - Manager がアンインストールされます。アンインストールが終了すると，アンインストールが終了したことを通知するダイアログが表示されます。アンインストールの終了時，再起動が必要な場合があります。再起動を促すメッセージがダイアログに表示されたら，OS を再起動してください。

   なお，インストール後に作成されたファイルまたはフォルダは削除されません。必要に応じて手動で削除してください。

3. [完了] ボタンをクリックする。

   アンインストールが終了します。

5.3　監査ログ収集対象サーバのプログラムのインストール

監査ログ収集対象サーバで必要なプログラムをインストールします。

JP1/Audit Management - Manager によって監査ログを収集するために，次に示す前提プログラムをインストールしてください。

- JP1/Base
- **監査ログの収集対象プログラム**

すでにこれらのプログラムがインストールされている場合，この作業は不要です。ただし，前提プログラムのバージョンは JP1/Audit Management - Manager がサポート対象としているバージョンである必要があります。JP1/Audit Management - Manager がサポート対象としているプログラムのバージョンについては「3.2.2　前提プログラム」を参照してください。

5.3.1　JP1/Base をインストールする

JP1/Base をインストールします。

JP1/Base のインストール手順については，マニュアル「JP1/Base 運用ガイド」を参照してください。

5.3.2　監査ログ収集対象プログラムをインストールする

必要に応じて，監査ログ収集対象プログラムをインストールします。

収集対象とするプログラムがすでにインストールされている場合，この作業は不要です。

監査ログ収集対象プログラムのインストール手順については，各プログラムのマニュアルを参照してください。

5.4　監査ログ収集対象サーバのセットアップ

監査ログ収集対象サーバをセットアップします。

監査ログ管理サーバ上にあるプログラムの監査ログを収集対象とする場合は，監査ログ収集対象サーバのセットアップ手順と同様の手順を，監査ログ管理サーバで実施してください。

セットアップする内容を次に示します。

セットアップに必要なファイルをインストールする

JP1/Audit Management - Manager では，監査ログ収集対象サーバのセットアップに必要な設定ファイルをアーカイブして提供しています。

セットアップに必要なファイルをインストールする方法については「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。

JP1/Base のイベントサービスを設定する

イベントサービスによって，監査ログ収集対象サーバで出力された監査ログをイベントサーバに蓄積します。イベントサービスの設定については「5.4.2　JP1/Base のイベントサービスを設定する」を参照してください。

なお，監査ログの蓄積には，専用のイベントサーバやイベントデータベースを使用します。このため，監査ログ収集対象サーバで監査ログ専用のイベントサーバを登録し，設定する必要があります。以降，これらのイベントサーバやイベントデータベースのことを「**監査ログ専用イベントサーバ**」，「**監査ログ専用イベントデータベース**」と呼びます。

JP1/Base のイベントログトラップ機能を設定する

監査ログ収集対象サーバの OS が Windows の場合に実施します。

Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要な設定です。

イベントログトラップ機能の設定については「5.4.3　JP1/Base のイベントログトラップ機能を設定する」を参照してください。

ログファイルトラップ機能の設定を確認する

ログファイルトラップ機能が起動されているかどうかを確認します。確認する方法については「5.4.4 ログファイルトラップ機能の設定を確認する」を参照してください。

UNIX システムログの変換設定をする

収集対象サーバの OS が UNIX の場合に実施します。

ログファイルトラップ機能によって，UNIX システムログを監査ログとして収集したい場合に必要な設定です。

UNIX システムログの変換設定については「5.4.5　UNIX システムログの変換設定をする」を参照してください。

監査ログ収集対象プログラムをセットアップする

監査ログ収集対象サーバで収集対象とするプログラムをセットアップします。監査ログ収集対象プログラムのセットアップについては「5.4.6　監査ログ収集対象プログラムをセットアップする」を参照してください。

5.4.1　セットアップに必要なファイルをインストールする

監査ログ収集対象サーバのセットアップに必要なファイルをインストールします。

この作業は，監査ログ収集対象サーバの OS が Windows と UNIX のどちらの場合でも必要です。

(1)　アーカイブファイルをコピーする

JP1/Audit Management - Manager では，監査ログ収集対象サーバのセットアップに必要な設定ファイルをアーカイブして提供しています。このアーカイブファイルを監査ログ管理サーバから監査ログ収集対象サーバにコピーします。

アーカイブファイルのコピー先のフォルダは任意です。なお，アーカイブファイルを FTP を使用してコピーする場合は，バイナリモードで転送してください。

監査ログ管理サーバから監査ログ収集対象サーバにコピーするアーカイブファイルは，監査ログ収集対象サーバの OS ごとに異なります。監査ログ収集対象サーバにコピーするアーカイブファイルを次の表に示します。

表 5-1　監査ログ収集対象サーバにコピーするアーカイブファイル

項番	OS の種類 (監査ログ収集対象サーバ)	コピー元のアーカイブ ファイルの格納先 (監査ログ管理サーバ)	コピー元の アーカイブファイル
1	• Windows Server 2012 • Windows Server 2008	JP1/Audit Management - Manager のインストール先フォルダ¥agent¥windows	admagent_windows.EXE
2	HP-UX	JP1/Audit Management - Manager のインストール先フォルダ¥agent¥hpux_ipf	admagent_hpux_ipf.tar
3	Solaris	JP1/Audit Management - Manager のインストール先フォルダ¥agent¥solaris	admagent_solaris.tar
4	AIX	JP1/Audit Management - Manager のインストール先フォルダ¥agent¥aix	admagent_aix.tar
5	Linux	JP1/Audit Management - Manager のインストール先フォルダ¥agent¥linux	admagent_linux.tar

(2) アーカイブファイルを展開する

監査ログ収集対象サーバにコピーしたアーカイブファイルを，任意のフォルダに展開します。

監査ログ収集対象サーバの OS が Windows の場合，アーカイブファイルは拡張子が「.EXE」の自己展開型ファイルになります。監査ログ収集対象サーバにコピーしたアーカイブファイルを直接実行し，任意のフォルダに展開してください。

監査ログ収集対象サーバの OS が UNIX の場合，アーカイブファイルは拡張子が「.tar」のファイルになります。監査ログ収集対象サーバにコピーしたアーカイブファイルの格納先ディレクトリに移動してから tar コマンドを実行し，任意のディレクトリに展開してください。

監査ログ収集対象サーバの OS が AIX の場合の tar コマンドの実行例を次に示します。なお，この実行例は「/tmp/jp1netmaudit」にコピーしたアーカイブファイル（admagent_aix.tar）を，コピー先と同じディレクトリに展開する場合を示しています。

```
cd /tmp/jp1netmaudit
tar xvf admagent_aix.tar
```

監査ログ収集対象サーバにコピーしたアーカイブファイルを展開すると，展開先のフォルダに admagtinstall コマンドと DATA フォルダが作成されます。admagtinstall コマンドは，監査ログ収集対象サーバのセットアップに必要なファイルをインストールするコマンドです。また，DATA フォルダには，admagtinstall コマンドの実行時に必要なデータが格納されています。

(3) admagtinstall コマンドを実行する

アーカイブファイルを展開したフォルダの配下にある admagtinstall コマンドを実行します。admagtinstall コマンドの詳細については「12. コマンド」の「admagtinstall（監査ログ収集対象サーバのファイルのインストール）」を参照してください。

admagtinstall コマンドを実行すると，監査ログ収集対象サーバのセットアップに必要なファイルがインストールされます。インストールされるファイルの一覧と格納先については「付録 A.3 監査ログ収集対象サーバに配布されるファイル一覧」を参照してください。

なお，監査ログ収集対象サーバのセットアップ時に使用したファイルとフォルダは，監査ログ収集対象サーバの運用中は不要となります。不要なファイルとフォルダを次に示します。

- 監査ログ収集対象サーバにコピーしたアーカイブファイル
- アーカイブファイルを展開して作成された DATA フォルダ

ただし，アーカイブファイルを展開して作成された admagtinstall コマンドについては，監査ログの収集をやめるときなど，監査ログ収集対象サーバにインストールしたファイルを削除するときにも使用します。このため，admagtinstall コマンドは削除しないで残しておいてください。

(a) 所有者，グループおよびパーミッションの値（UNIX の場合）

監査ログ収集対象サーバの OS が UNIX の場合，admagtinstall コマンドを実行してインストールされたディレクトリやファイルに対して，所有者，グループおよびパーミッションの値が設定されます。

インストールされたディレクトリに設定される所有者，グループおよびパーミッションの値を次の表に示します。

表 5-2　ディレクトリの所有者，グループおよびパーミッションの設定値

項番	対象ディレクトリ	所有者	グループ	パーミッション
1	/etc/opt/jp1netmaudit	root	sys※	755
2	/etc/opt/jp1netmaudit/agent			
3	/etc/opt/jp1netmaudit/agent/conf			
4	/opt/jp1netmaudit			
5	/opt/jp1netmaudit/agent			
6	/opt/jp1netmaudit/agent/bin			
7	/var/opt/jp1netmaudit			
8	/var/opt/jp1netmaudit/agent			
9	/var/opt/jp1netmaudit/agent/log			

注※

OS の種類が AIX の場合は，グループの設定値は「system」になります。

インストールされたファイルに設定される所有者，グループおよびパーミッションの値を次の表に示します。

表 5-3　ファイルの所有者，グループおよびパーミッションの設定値

項番	対象ファイル	所有者	グループ	パーミッション
1	admagtsetup	root	sys※	500
2	admhasetup			
3	admhastart			
4	admhastop			
5	admuxlogcol			
6	adm_adaptercmd			
7	Adapter_HITACHI_JP1_NETM_AUDIT.conf			644
8	admagtsetup.conf.model			

注※

OS の種類が AIX の場合は，グループの設定値は「system」になります。

5.4.2　JP1/Base のイベントサービスを設定する

イベントサービスを使用するために，監査ログ収集対象サーバで監査ログ専用イベントサーバを設定します。

監査ログ専用イベントサーバ名は，監査ログ収集対象サーバのホスト名のあとに「-adm」を付けて設定してください。監査ログ収集対象サーバのホスト名が「Host01」の場合，監査ログ専用イベントサーバ名は「Host01-adm」になります。なお，監査ログ専用イベントサーバ名の大文字と小文字は区別されます。

この作業は，監査ログ収集対象サーバの OS が Windows と UNIX のどちらの場合でも必要です。

監査ログ専用イベントサーバの設定内容について，次に説明します。

(1)　監査ログ専用イベントサーバの構築前に準備すること

監査ログ専用イベントデータベースを作成するために，次の事前準備をします。

- **監査ログ専用イベントサーバの定義ファイルやイベントデータベースなどを格納する任意のフォルダを，ローカルディスク上に作成する。**

  この作業は，監査ログ収集対象サーバの OS が Windows と UNIX のどちらの場合でも必要です。

  以降，ここで作成したフォルダのことを Windows の場合は「**監査ログ専用フォルダ**」，UNIX の場合は「**監査ログ専用ディレクトリ**」と呼びます。

- **監査ログ専用イベントデータベースに割り当てるポート番号を決める。**

  既存の JP1/Base とは別に，監査ログ専用イベントデータベースのポート番号を設定する必要があります。推奨するポート番号を次に示します。

  - 転送用ポート番号「24101」
  - AP 用ポート番号「24102」

  ただし，監査ログ収集対象サーバで使用されている場合は，ほかのポート番号にする必要があります。

- **監査ログ専用イベントデータベースのサイズを決める。**

  JP1/Base のイベントデータベースの見積もり式を基に，監査ログ専用イベントデータベースのサイズを算出します。見積もり式を次の表に示します。

  表 5-4　監査ログ専用イベントデータベースのサイズの見積もり式

見積もり式（単位：バイト）
((a×(b ＋ 64)＋(c×64))×d)÷2

（凡例）

a：1 日当たりに収集する監査ログの件数

b：取得する監査ログの平均サイズ（一つのログ当たり最大 1 キロバイトとして計算）

c：1 日当たりに転送されるイベントの総件数（Windows イベントログから取得する監査ログの総件数）

d：保存する日数（収集間隔の 4 倍が目安。例えば［定時収集の設定］ダイアログで設定した収集スケジュールが「毎日」の場合は 4 日）

なお，監査ログ専用イベントデータベースは，デフォルトでは 10 メガバイトのサイズで作成されます。

(2)　監査ログ専用イベントサーバを構築する

admagtsetup コマンドを実行し，監査ログ専用イベントサーバを構築します。構築に必要な環境情報を次の表に示します。

表 5-5　監査ログ専用イベントサーバの構築に必要な環境情報

項番	対象サーバ	項目
1	監査ログ管理サーバ	ホスト名
2		IP アドレス
3		JP1/Base のイベントサーバの転送用ポート番号
4	監査ログ収集対象サーバ	ホスト名
5		IP アドレス
6		監査ログ専用フォルダ（監査ログ専用ディレクトリ）
7		監査ログ専用イベントデータベースのサイズ
8		監査ログ専用イベントサーバの転送用ポート番号
9		監査ログ専用イベントサーバの AP 用ポート番号

これらの環境情報は次のどちらかの方法で指定してください。

コマンドの引数で指定する

引数で指定する方法については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

監査ログ収集対象サーバセットアップ定義ファイルで指定する

JP1/Audit Management - Manager で提供するモデルファイル（admagtsetup.conf.model）をコピーして指定します。コピー先のファイル名は任意です。

モデルファイルの格納先および監査ログ収集対象サーバセットアップ定義ファイルの設定方法については「13.9　監査ログ収集対象サーバセットアップ定義ファイル」を参照してください。

admagtsetup コマンドを実行すると，監査ログ専用イベントサーバの環境が，次のように構築されます。

- 引数または監査ログ収集対象サーバセットアップ定義ファイルで指定した監査ログ専用フォルダ（監査ログ専用ディレクトリ）の配下に「jp1netmaudit¥event」（「jp1netmaudit/event」）が作成される。
- 「監査ログ専用フォルダ¥jp1netmaudit¥event」（「監査ログ専用ディレクトリ/jp1netmaudit/event」）配下に，監査ログ専用イベントサーバ用の環境設定ファイルが作成される。
- JP1/Base の定義ファイルに監査ログ専用イベントデータベースの定義が追加される。

- JP1/Base の jp1hosts2 情報が更新される。

なお，すでに構築されている監査ログ専用イベントサーバに上書きしてセットアップすることはできません。監査ログ専用イベントサーバの設定を変更する方法については「(3)　監査ログ専用イベントサーバの環境情報を変更する」を参照してください。

作成される監査ログ専用イベントサーバ用の環境設定ファイルについて，次の表に示します。

表 5-6　作成される監査ログ専用イベントサーバ用の環境設定ファイル

項番	OS の種類 (監査ログ収集対象サーバ)	格納先	対象ファイル	定義内容
1	Windows	**監査ログ専用フォルダ** ¥jp1netmaudit¥event	イベントサービスのイベントサーバ設定ファイル（conf）	• 監査ログ管理サーバのホスト名 • 監査ログ管理サーバの IP アドレス • 監査ログ収集対象サーバの IP アドレス • JP1/Base のイベントサーバの転送用ポート番号 • 監査ログ専用イベントデータベースのサイズ • 監査ログ専用イベントサーバの転送用ポート番号 • 監査ログ専用イベントサーバの AP 用ポート番号
2			イベントサービスの転送設定ファイル（forward）	• 監査ログ管理サーバのホスト名
3	UNIX	**監査ログ専用ディレクトリ**/jp1netmaudit/event	イベントサービスのイベントサーバ設定ファイル（conf）	• 監査ログ管理サーバのホスト名 • 監査ログ管理サーバの IP アドレス • 監査ログ収集対象サーバの IP アドレス • JP1/Base のイベントサーバの転送用ポート番号 • 監査ログ専用イベントデータベースのサイズ • 監査ログ専用イベントサーバの転送用ポート番号 • 監査ログ専用イベントサーバの AP 用ポート番号
4			イベントサービスの転送設定ファイル（forward）	• 監査ログ管理サーバのホスト名

イベントサービスのイベントサーバ設定ファイル（conf）と転送設定ファイル（forward）の設定例について，それぞれ次に示します。

(a)　イベントサービスのイベントサーバ設定ファイル（conf）

設定例の条件を次の表に示します。

表 5-7　設定例の条件（イベントサービスのイベントサーバ設定ファイル（conf））

項番	項目	この例での値
1	監査ログ管理サーバのホスト名	audithost
2	監査ログ管理サーバの IP アドレス	172.16.1.100
3	監査ログ収集対象サーバの IP アドレス	172.16.1.10
4	JP1/Base のイベントサーバの転送用ポート番号	jp1imevt
5	監査ログ専用イベントデータベースのサイズ	10,000,000 バイト
6	監査ログ専用イベントサーバの転送用ポート番号	24101
7	監査ログ専用イベントサーバの AP 用ポート番号	24102

イベントサービスのイベントサーバ設定ファイル（conf）は次のように設定されます。

```
#portsパラメーターのデフォルトの記述が変更される。
ports 172.16.1.10 24101 24102
     :
db-size 10000000
     :
#デフォルトで記述されている行の下に，remote-serverパラメーターの記述が新しく追加される。
remote-server * close
remote-server audithost close 172.16.1.100 jp1imevt
```

なお，IPv6 アドレスで通信する場合は，ports パラメーターの監査ログ収集対象サーバの IP アドレスおよび remote-server パラメーターの監査ログ管理サーバの IP アドレスに<jp1hosts2>が設定されます。

IPv6 アドレスで通信する場合の設定例の条件を次の表に示します。

表 5-8　IPv6 アドレスで通信する場合の設定例の条件（イベントサービスのイベントサーバ設定ファイル（conf））

項番	項目	この例での値
1	監査ログ管理サーバのホスト名	audithost
2	監査ログ管理サーバの IP アドレス	2001:db8::64
3	監査ログ収集対象サーバの IP アドレス	2001:db8::a
4	JP1/Base のイベントサーバの転送用ポート番号	jp1imevt
5	監査ログ専用イベントデータベースのサイズ	10,000,000 バイト
6	監査ログ専用イベントサーバの転送用ポート番号	24101
7	監査ログ専用イベントサーバの AP 用ポート番号	24102

イベントサービスのイベントサーバ設定ファイル（conf）は次のように設定されます。

```
#portsパラメーターのデフォルトの記述が変更される。
ports <jp1hosts2> 24101 24102
     :
db-size 10000000
     :
#デフォルトで記述されている行の下に，remote-serverパラメーターの記述が新しく追加される。
remote-server * close
remote-server audithost close <jp1hosts2> jp1imevt
```

(b) イベントサービスの転送設定ファイル（forward）

設定例の条件を次の表に示します。

表 5-9 設定例の条件（イベントサービスの転送設定ファイル（forward））

項番	項目	この例での値
1	監査ログ管理サーバのホスト名	audithost
2	イベントデータベースの切り替えの発生を知らせるイベント ID	00003D00

イベントサービスの転送設定ファイル（forward）は次のように設定されます。デフォルトで記述されている行の下に，記述が新しく追加されます。

```
to audithost
B.ID IN 00003D00
B.REASON IN 1
end-to
```

監査ログ専用イベントデータベースの定義が追加される JP1/Base の定義ファイルについて，次の表に示します。

表 5-10 監査ログ専用イベントデータベースの定義が追加される JP1/Base の定義ファイル

項番	OS の種類（監査ログ収集対象サーバ）	格納先	対象ファイル	定義内容
1	Windows	JP1/Base のインストール先フォルダ¥conf¥event	イベントサーバインデックスファイル（index）	• 監査ログ専用フォルダ¥jp1netmaudit¥event • 監査ログ専用イベントサーバ名
2			API 設定ファイル（api）	• 監査ログ収集対象サーバの IP アドレス • 監査ログ専用イベントサーバの AP 用ポート番号 • 監査ログ専用イベントサーバ名
3	UNIX	/etc/opt/jp1base/conf/event	イベントサーバインデックスファイル（index）	• 監査ログ専用ディレクトリ/jp1netmaudit/event • 監査ログ専用イベントサーバ名
4			API 設定ファイル（api）	• 監査ログ収集対象サーバの IP アドレス

項番	OS の種類（監査ログ収集対象サーバ）	格納先	対象ファイル	定義内容
				• 監査ログ専用イベントサーバの AP 用ポート番号 • 監査ログ専用イベントサーバ名

JP1/Base のイベントサーバインデックスファイル（index），API 設定ファイル（api），および jp1hosts2 ファイルの設定例について，それぞれ次に示します。

(c) イベントサーバインデックスファイル（index）

設定例の条件を次の表に示します。

表 5-11 設定例の条件（JP1/Base のイベントサーバインデックスファイル（index））

項番	項目	この例での値
1	**監査ログ専用フォルダ**¥jp1netmaudit¥event	E:¥audit¥jp1netmaudit¥event※
2	監査ログ専用イベントサーバ名	host01-adm

注※

Windows の場合の例を挙げています。UNIX の場合，この部分については UNIX 用のパス（「/shdhd/audit/jp1netmaudit/event」など）に置き換えてください。

イベントサーバインデックスファイル（index）は次のように設定されます。デフォルトで記述されている行の下に，server パラメーターの記述が新しく追加されます。

```
server host01-adm E:¥audit¥jp1netmaudit¥event
```

(d) API 設定ファイル（api）

設定例の条件を次の表に示します。

表 5-12 設定例の条件（JP1/Base の API 設定ファイル（api））

項番	項目	この例での値
1	監査ログ専用イベントサーバの IP アドレス	172.16.1.10
2	監査ログ専用イベントサーバの AP 用ポート番号	24102
3	監査ログ専用イベントサーバ名	host01-adm

API 設定ファイル（api）は次のように設定されます。デフォルトで記述されている行の下に，server パラメーターの記述が新しく追加されます。

```
server host01-adm keep-alive 172.16.1.10 24102
```

なお，IPv6 アドレスで通信する場合は，server パラメーターの監査ログ専用イベントサーバの IP アドレスに<jp1hosts2>が設定されます。

IPv6 アドレスで通信する場合の設定例の条件を次の表に示します。

表 5-13　IPv6 アドレスで通信する場合の設定例の条件（JP1/Base の API 設定ファイル（api））

項番	項目	この例での値
1	監査ログ専用イベントサーバの IP アドレス	2001:db8::a
2	監査ログ専用イベントサーバの AP 用ポート番号	24102
3	監査ログ専用イベントサーバ名	host01-adm

API 設定ファイル（api）は次のように設定されます。デフォルトで記述されている行の下に，server パラメーターの記述が新しく追加されます。

```
server host01-adm keep-alive <jp1hosts2> 24102
```

(e)　jp1hosts2 情報（IPv6 アドレスで通信する場合だけ）

設定例の条件を次の表に示します。監査ログ専用イベントサーバ名に対応する IP アドレスが新しく追加されます。

表 5-14　設定例の条件（jp1hosts2 ファイル）

項番	項目	この例での値
1	監査ログ収集対象サーバの IPv6 アドレス	2001:db8::a
2	監査ログ専用イベントサーバ名	host01-adm

(3)　監査ログ専用イベントサーバの環境情報を変更する

すでに構築している監査ログ専用イベントサーバの環境情報を変更する方法について説明します。

変更できる環境情報を次に示します。

監査ログ管理サーバの環境情報

- ホスト名
- IP アドレス
- JP1/Base のイベントサーバの転送用ポート番号

監査ログ収集対象サーバの環境情報

- IP アドレス
- 監査ログ専用フォルダ（監査ログ専用ディレクトリ）
- 監査ログ専用イベントデータベースのサイズ

- 監査ログ専用イベントサーバの転送用ポート番号
- 監査ログ専用イベントサーバの AP 用ポート番号

監査ログ収集対象サーバのホスト名を変更したい場合は，監査ログ専用イベントサーバを構築し直す必要があります。監査ログ専用イベントサーバを構築する方法については「(2)　監査ログ専用イベントサーバを構築する」を参照してください。

監査ログ専用イベントサーバを admagtsetup コマンドで構築した場合と手動で構築した場合で変更する方法が異なります。それぞれについて次に説明します。

(a)　admagtsetup コマンドで監査ログ専用イベントサーバを構築した場合

admagtsetup コマンドで構築した監査ログ専用イベントサーバの環境情報を変更する方法について説明します。

監査ログ専用イベントサーバの環境情報を変更する手順について説明します。

1. 監査ログ管理サーバの監査ログ収集マネージャで監視中の収集対象の監視を停止する。

2. 監査ログ専用イベントサーバが起動している場合は，監査ログ専用イベントサーバを停止する。

   Windows の場合

   コントロールパネルの「管理ツール」の「サービス」を開いて監査ログ専用イベントサーバのサービスを停止させてください。

   UNIX の場合

   次に示すコマンドを実行して停止させます。

```
/opt/jp1base/bin/jevstop 監査ログ専用イベントサーバ名
```

3. 監査ログ専用イベントデータベースのバックアップを取得する。

   監査ログ専用イベントデータベースの設定ファイルをコピーするなど，任意の方法でバックアップを取得してください。監査ログ専用イベントデータベースの設定ファイルの格納先を次に示します。

   Windows の場合

   監査ログ専用フォルダ¥jp1netmaudit¥event¥IMEvent*.*

   UNIX の場合

   監査ログ専用ディレクトリ/jp1netmaudit/event/IMEvent*.*

4. admagtsetup コマンドを実行して監査ログ専用イベントサーバを削除する。

   admagtsetup コマンドで監査ログ専用イベントサーバを削除する方法については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

5. admagtsetup コマンドを実行して監査ログ専用イベントサーバを構築する。

   admagtsetup コマンドで監査ログ専用イベントサーバを構築する方法については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

6. 手順 3 で取得した監査ログ専用イベントデータベースの設定ファイルのバックアップを反映する。

バックアップの反映先を次に示します。

Windows の場合

監査ログ専用フォルダ¥jp1netmaudit¥event

UNIX の場合

監査ログ専用ディレクトリ/jp1netmaudit/event

7. 新しく作成した監査ログ専用イベントサーバを起動する。

Windows の場合

コントロールパネルの「管理ツール」の「サービス」を開いて監査ログ専用イベントサーバのサービスを開始させてください。

UNIX の場合

次に示すコマンドを実行して起動させます。

```
/opt/jp1base/bin/jevstart 監査ログ専用イベントサーバ名
```

8. 監査ログ管理サーバの API 設定ファイル（api ファイル）を編集する。

手順 5 で監査ログ収集対象サーバの IP アドレスやポート番号も変更した場合は，監査ログ管理サーバの API 設定ファイル（api ファイル）に設定されている IP アドレスとポート番号の設定もあわせて変更してください。

9. 監査ログ管理サーバの JP1/Audit Management - Manager のサービスを再起動する。

手順 8 で監査ログ管理サーバの API 設定ファイル（api ファイル）を編集した場合は，監査ログ管理サーバの JP1/Audit Management - Manager のサービスを再起動してください。

10. 監査ログ管理サーバの監査ログ収集マネージャで収集対象の監視を開始する。

(b) 手動で監査ログ専用イベントサーバを構築した場合

JP1/NETM/Audit - Manager 09-00 より前のバージョンで構築した監査ログ専用イベントサーバの環境情報を変更する方法について説明します。

監査ログ専用イベントサーバの環境情報を変更する手順について説明します。

1. 監査ログ管理サーバの監査ログ収集マネージャで監視中の収集対象の監視を停止する。

2. 監査ログ専用イベントサーバが起動している場合は，監査ログ専用イベントサーバを停止する。

Windows の場合

コントロールパネルの「管理ツール」の「サービス」を開いて監査ログ専用イベントサーバのサービスを停止させてください。

UNIX の場合

次に示すコマンドを実行して停止させます。

```
/opt/jp1base/bin/jevstop 監査ログ専用イベントサーバ名
```

3. 監査ログ専用イベントサービスを削除する。

この操作は，ホスト名を変更する場合に必要な操作です。IP アドレスの変更では操作不要です。

登録している監査ログ専用イベントサービスを削除します。この手順は OS が Windows の場合に実施してください。

次のコマンドを実行します。

```
jevregsvc -u 監査ログ専用イベントサーバ名
```

jevregsvc コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

4. 監査ログ専用イベントサーバの設定ファイルを変更する。

変更する設定ファイルを次に示します。

- イベントサーバインデックスファイル（index）
- API 設定ファイル（api）
- 監査ログ専用イベントサーバ設定ファイル（conf）
- 監査ログ専用イベントサーバ転送設定ファイル（forward）

イベントサーバインデックスファイル（index）と API 設定ファイル（api）の格納先については「5.4.2(2)　監査ログ専用イベントサーバを構築する」を参照してください。また，監査ログ専用イベントサーバ設定ファイル（conf）と監査ログ専用イベントサーバ転送設定ファイル（forward）の格納先は，監査ログ専用イベントサーバの構築時に作成した任意のフォルダ（ディレクトリ）です。

各設定ファイルの設定内容の詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

5. 監査ログ専用イベントサービスを登録する

この操作は，ホスト名を変更する場合に必要な操作です。IP アドレスの変更では操作不要です。

監査ログ専用イベントサービスを削除します。この手順は OS が Windows の場合に実施してください。

次のコマンドを実行します。

```
jevregsvc -r 監査ログ専用イベントサーバ名
```

jevregsvc コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

6. 監査ログ専用イベントサーバを起動する。

Windows の場合

コントロールパネルの「管理ツール」の「サービス」を開いて監査ログ専用イベントサーバのサービスを開始させてください。

UNIX の場合

次に示すコマンドを実行して起動させます。

```
/opt/jp1base/bin/jevstart 監査ログ専用イベントサーバ名
```

7. 監査ログ管理サーバの API 設定ファイル（api ファイル）を編集する。

   手順 3 で監査ログ収集対象サーバの IP アドレスやポート番号も変更した場合は，監査ログ管理サーバの API 設定ファイル（api ファイル）に設定されている IP アドレスとポート番号の設定もあわせて変更してください。

8. 監査ログ管理サーバの監査ログ収集マネージャで監視対象を再設定する。

   この操作は，ホスト名を変更する場合に必要な操作です。IP アドレスの変更では操作不要です。

   変更前のサーバ名の監視対象を削除して，変更後のサーバ名で監視対象を再登録してください。

9. 監査ログ管理サーバの JP1/Audit Management - Manager のサービスを再起動する。

   手順 5 で監査ログ管理サーバの API 設定ファイル（api ファイル）を編集した場合は，監査ログ管理サーバの JP1/Audit Management - Manager のサービスを再起動してください。

10. 監査ログ管理サーバの監査ログ収集マネージャで収集対象の監視を開始する。

(4) イベントサービスを自動的に起動する

監査ログ収集対象サーバで出力された監査ログを監査ログ専用イベントサーバに蓄積するために，イベントサービスを起動させておく必要があります。

イベントサービスを OS 起動時に自動的に起動するように設定します。

この作業は，監査ログ収集対象サーバの OS が Windows と UNIX のどちらの場合でも，必要です。ただし，OS によって設定方法が異なります。OS が Windows と UNIX の場合について，それぞれ説明します。

(a) Windows の場合

JP1/Base の起動順序定義ファイル（**JP1/Base のインストール先フォルダ**¥conf¥boot¥Jp1svprm.dat）をテキストエディタで開いて記述を編集します。

設定例を次に示します。

起動順序定義ファイルの設定例

起動順序定義ファイルに次の記述を追加します。デフォルトの記述は残したまま，新しい記述を追加してください。

```
#イベントログトラップ機能を定義する記述より前に記述を追加し，先に起動されるように設定する。
[Jp1BaseEvent_監査ログ専用イベントサーバ名]
Name=JP1/BaseEvent_監査ログ専用イベントサーバ名
ServiceName=JP1_Base_Event 監査ログ専用イベントサーバ名
```

監査ログ専用イベントサーバ名は，監査ログ収集対象サーバのホスト名のあとに「-adm」を付けて設定してください。

なお，デフォルトで自動起動する設定になっていて，かつ監査ログ収集対象サーバとしてインストールされていない製品については，不要なサービスとしてコメント化してください。

イベントサービスは手動でも起動できます。必ずイベントサービスの起動後に，イベントログトラップ機能を起動してください。イベントログトラップ機能を起動する方法については「5.4.3(5)　イベントログトラップ機能を自動的に起動する」を参照してください。

イベントサービスを手動で開始する方法を次に示します。

1. コントロールパネルの「管理ツール」から「サービス」を開く。
2. 「JP1/Base Event 監査ログ専用イベントサーバ名」を選択し，プロパティで［開始］ボタンをクリックする。
3. 「JP1/Base Event」を選択し，プロパティで［開始］ボタンをクリックする。

開始する場合と同様の方法でイベントサービスを停止できます。

(b)　UNIX の場合

自動起動用のスクリプトを作成し，作成したスクリプトにリンクの設定をすることで自動起動を設定します。

OS ごとのスクリプトの格納先および作成例を次に示します。OS ごとのリンクの設定方法については，マニュアル「JP1/Base 運用ガイド」を参照してください。

- HP-UX

  スクリプトの格納先：/sbin/init.d/jp1_service_cluster

  スクリプトの作成例：

```
#!/bin/sh

## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jp1base/bin
export PATH
JP1_HOSTNAME=監査ログ専用イベントサーバ名
export JP1_HOSTNAME

case $1 in
start_msg)
 echo "Start JP1 Service $JP1_HOSTNAME"
 ;;

stop_msg)
 echo "Stop JP1 Service $JP1_HOSTNAME"
 ;;

'start')
 if [ -x /opt/jp1base/bin/jevstart ]
 then
 /opt/jp1base/bin/jevstart $JP1_HOSTNAME
 fi
 ;;

'stop')
 if [ -x /opt/jp1base/bin/jevstop ]
 then
```

```
 /opt/jp1base/bin/jevstop $JP1_HOSTNAME
 fi
 ;;

esac

exit 0
```

- Solaris

  スクリプトの格納先：/etc/init.d/jp1_service_cluster

  スクリプトの作成例：

```
#!/bin/sh

## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jp1base/bin
export PATH
JP1_HOSTNAME=監査ログ専用イベントサーバ名
export JP1_HOSTNAME

case $1 in
start_msg)
 echo "Start JP1 Service $JP1_HOSTNAME"
 ;;

stop_msg)
 echo "Stop JP1 Service $JP1_HOSTNAME"
 ;;

'start')
 if [ -x /opt/jp1base/bin/jevstart ]
 then
 /opt/jp1base/bin/jevstart $JP1_HOSTNAME
 fi
 ;;

'stop')
 if [ -x /opt/jp1base/bin/jevstop ]
 then
 /opt/jp1base/bin/jevstop $JP1_HOSTNAME
 fi
 ;;

esac

exit 0
```

- AIX

  スクリプトの作成方法：mkitab コマンドで，/etc/inittab ファイルに次に示す記述を追加します。監査ログの収集対象として設定したプログラムを起動する記述の前に追加してください。

  /etc/inittab ファイルに追加する記述：

```
# mkitab -i jp1base "jp1netmadm:2:wait:/opt/jp1base/bin/jevstart 監査ログ専用イベントサーバ名"
```

また，/etc/rc.shutdown ファイルをテキストエディタで開き，次に示す記述を追加します。監査ログの収集対象として設定したプログラムを停止する記述のあとに追加してください。

/etc/rc.shutdown ファイルに追加する記述：

```
test -x /opt/jp1base/bin/jevstop && /opt/jp1base/bin/jevstop 監査ログ専用イベントサーバ名
test -x /opt/hitachi/HNTRLib2/etc/D002stop && /opt/hitachi/HNTRLib2/etc/D002stop
```

- Linux

  スクリプトの格納先：/etc/rc.d/init.d/jp1_service_cluster

  スクリプトの作成例：

```
#!/bin/sh

## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jp1base/bin
export PATH
JP1_HOSTNAME=監査ログ専用イベントサーバ名
export JP1_HOSTNAME

case $1 in
start_msg)
 echo "Start JP1 Service $JP1_HOSTNAME"
 ;;

stop_msg)
 echo "Stop JP1 Service $JP1_HOSTNAME"
 ;;

'start')
 if [ -x /opt/jp1base/bin/jevstart ]
 then
 /opt/jp1base/bin/jevstart $JP1_HOSTNAME
 touch /var/lock/subsys/_JP1_BASE_EVENT_$JP1_HOSTNAME
 fi
 ;;

'stop')
 if [ -x /opt/jp1base/bin/jevstop ]
 then
 /opt/jp1base/bin/jevstop $JP1_HOSTNAME
 rm -f /var/lock/subsys/_JP1_BASE_EVENT_$JP1_HOSTNAME
 fi

 ;;
esac

exit 0
```

  監査ログ専用イベントサーバ名は，監査ログ収集対象サーバのホスト名のあとに「-adm」を付けて設定してください。

イベントサービスは手動でも起動や停止ができます。

次に示すコマンドを実行して起動します。

```
jevstart 監査ログ専用イベントサーバ名
```

次に示すコマンドを実行して停止します。

```
jevstop 監査ログ専用イベントサーバ名
```

なお，監査ログ専用イベントサーバ名の大文字と小文字は区別されます。

jevstart コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

5.4.3 JP1/Base のイベントログトラップ機能を設定する

Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして収集したい場合に，イベントログトラップ機能を設定します。

Windows イベントログに出力されるログを次に示します。

- Windows イベントログ（セキュリティに関する情報）
- Oracle のログ
- Hitachi Storage Command Suite または Hitachi Command Suite のログ（Windows の場合）

これらのログを JP1/Audit Management - Manager の監査ログとして収集しない場合，この作業は不要です。

(1) JP1/Audit Management - Manager の監査ログとして出力するための設定

Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして出力するための設定をします。

(a) Windows の監査ポリシーを設定する

Windows イベントログ（セキュリティに関する情報）を JP1/Audit Management - Manager の監査ログとして出力するために，Windows の監査ポリシーを設定します。

Windows イベントログ（セキュリティに関する情報）を JP1/Audit Management - Manager の監査ログとして収集しない場合，この作業は不要です。

コントロールパネルの「管理ツール」から「ローカルセキュリティポリシー」，「ドメインセキュリティポリシー」，または「ドメインコントローラセキュリティポリシー」を開いて，「ローカルポリシー」下の「監査ポリシー」の設定を変更してください。

ここでは，ログオン イベントおよびアカウント管理のイベントを出力するための設定方法を説明します。

「監査ポリシー」で「ログオン イベントの監査」および「アカウント管理の監査」を設定することで，ログオン イベントおよびアカウント管理のイベントを出力できます。それぞれの設定内容を次に示します。

- 「ログオン イベントの監査」

  ログオン イベントを出力するために設定します。「ログオン イベントの監査」を開いて，監査する条件を設定してください。成功，失敗，またはそれらの両方を監査するよう設定できます。
- 「アカウント管理の監査」

  アカウント管理のイベントを出力するために設定します。「アカウント管理の監査」を開いて，監査する条件を設定してください。成功，失敗，またはそれらの両方を監査するよう設定できます。

このほかの Windows イベントログ（セキュリティに関する情報）の監査ポリシーを設定する方法については，Windows のマニュアルを参照してください。

(b) Oracle のパラメーターファイル（init.ora）を編集する

Oracle のログを JP1/Audit Management - Manager の監査ログとして出力するために，Oracle のパラメーターファイル（init.ora）を編集します。

Oracle のログを JP1/Audit Management - Manager の監査ログとして収集しない場合，この作業は不要です。

なお，パラメーターファイルの「audit_trail」には「OS」を設定してください。「OS」を設定すると，監視されたレコードがシステム単位でイベントビューアに書き込まれ，イベントログとして出力されます。

設定例を次に示します。

Oracle のパラメーターファイル（init.ora）の設定例

```
##init.ora#######################
##標準監査を有効にし，OSファイル(イベントビューア)に出力させる
audit_trail=OS
##DBA監査の有効化
audit_sys_operations=TRUE
################################
```

パラメーターファイルの編集方法の詳細は，Oracle のマニュアルを参照してください。

(2) JP1/Base の動作定義ファイル（ntevent.conf）を編集する

動作定義ファイル（ntevent.conf）で，イベントログトラップ機能の動作環境を設定します。

この作業は，Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。

Windows イベントログに出力されるログについての定義を，次に示すファイルへ追加します。

- JP1/Base のインストール先フォルダ¥conf¥event¥ntevent.conf

動作定義ファイル（ntevent.conf）の定義内容は，収集対象となるプログラムによって異なります。定義内容については，プログラムごとに次に示す個所を参照してください。

- Windows イベントログ（セキュリティに関する情報）を収集する場合

  「(a)　Windows イベントログを収集する場合の定義内容（動作定義ファイル（ntevent.conf））」を参照してください。

- Oracle のログを収集する場合

  「(b)　Oracle のログを収集する場合の定義内容（動作定義ファイル（ntevent.conf））」を参照してください。

- Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを収集する場合

  「(c)　Hitachi Storage Command Suite または Hitachi Command Suite のログを収集する場合の定義内容（動作定義ファイル（ntevent.conf））」を参照してください。

(a)　Windows イベントログを収集する場合の定義内容（動作定義ファイル（ntevent.conf））

Windows イベントログ（セキュリティに関する情報）を収集する場合に，動作定義ファイル（ntevent.conf）で定義する内容について説明します。

この作業は，Windows イベントログ（セキュリティに関する情報）を JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。

JP1/Audit Management - Manager で標準サポートしている Windows イベントログ（セキュリティに関する情報）のイベント ID を次に示します。

ログオン イベントの Windows イベントログ（セキュリティに関する情報）

標準サポートしているイベント ID は「4624～4625」および「4634」です。

アカウント管理の Windows イベントログ（セキュリティに関する情報）

標準サポートしているイベント ID は「4720」，「4722～4735」，「4737～4738」，「4740」，および「4744～4763」です。

ここに示す Windows イベントログ（セキュリティに関する情報）以外のイベント ID は，JP1/Audit Management - Manager では標準サポート外となります。標準サポート外のイベント ID については，Windows のマニュアルを参照してください。

Windows イベントログ（セキュリティに関する情報）を収集する場合の動作定義ファイル（ntevent.conf）の設定例について次に説明します。

設定例の条件を次に示します。

設定例の条件（Windows イベントログ（セキュリティに関する情報）を収集する場合の動作定義ファイル（ntevent.conf））

次に示すイベント ID のイベントログを取得します。

- 「4624～4625」
- 「4634」

設定例を次に示します。

Windows イベントログ（セキュリティに関する情報）を収集する場合の動作定義ファイル（ntevent.conf）の設定例

動作定義ファイル（ntevent.conf）を次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
filter "Security"
 id '^4624$' '^4625$' '^4634$'
end-filter
```

動作定義ファイル（ntevent.conf）の詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

(b) Oracle のログを収集する場合の定義内容（動作定義ファイル（ntevent.conf））

Oracle のログを収集する場合に，動作定義ファイル（ntevent.conf）で定義する内容について説明します。

この作業は，Oracle のログを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。

JP1/Audit Management - Manager で収集できる Oracle のログのイベント ID を次に示します。

Oracle のログ

収集できるイベント ID は「34」です。

Oracle のログを収集する場合の動作定義ファイル（ntevent.conf）の設定例について次に説明します。

設定例の条件を次に示します。

設定例の条件（Oracle のログを収集する場合の動作定義ファイル（ntevent.conf））

イベント ID「34」のイベントログを取得します。

設定例を次に示します。

Oracle のログを収集する場合の動作定義ファイル（ntevent.conf）の設定例

動作定義ファイル（ntevent.conf）を次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
filter "Application"
 id '^34$'
```

```
 source !'^Oracle¥.+asm$'
 source '^Oracle'
end-filter
```

JP1/Base の動作定義ファイル（ntevent.conf）の詳細は，マニュアル「JP1/Base 運用ガイド」を参照してください。

(c) Hitachi Storage Command Suite または Hitachi Command Suite のログを収集する場合の定義内容（動作定義ファイル（ntevent.conf））

Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを収集する場合に，動作定義ファイル（ntevent.conf）で定義する内容について説明します。

この作業は，Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。

JP1/Audit Management - Manager で収集できる Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログのイベント ID を次に示します。

Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログ

収集できるイベント ID は「1」です。

Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを収集する場合の動作定義ファイル（ntevent.conf）の設定例について次に説明します。

設定例の条件を次に示します。

設定例の条件（Hitachi Storage Command Suite または Hitachi Command Suite 7 のログを収集する場合の動作定義ファイル（ntevent.conf））

- イベント ID「1」で，メッセージに「CELFSS」を含むイベントログを取得します。
- イベントソース名は HBase Storage Mgmt Log です。

設定例を次に示します。

Hitachi Storage Command Suite または Hitachi Command Suite 7（Windows の場合）のログを収集する場合の動作定義ファイル（ntevent.conf）の設定例

動作定義ファイル（ntevent.conf）を次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
filter "Application"
 id '^1$'
 source '^HBase Storage Mgmt Log$'
 message 'CELFSS'
end-filter
```

設定例の条件（Hitachi Command Suite 8 のログを収集する場合の動作定義ファイル（ntevent.conf））

- イベント ID「1」で，メッセージに「CELFSS」を含むイベントログを取得します。

- イベントソース名は HBase64 Event または HBase64 Storage Mgmt Log です。

設定例を次に示します。

Hitachi Command Suite 8（Windows の場合）のログを収集する場合の動作定義ファイル（ntevent.conf）の設定例

動作定義ファイル（ntevent.conf）を次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
filter "Application"
 id '^1$'
 source '^HBase64 Event$' '^HBase64 Storage Mgmt Log$'
 message 'CELFSS'
end-filter
```

JP1/Base の動作定義ファイル（ntevent.conf）の詳細は，マニュアル「JP1/Base 運用ガイド」を参照してください。

(3) イベントログトラップ機能のイベントサーバ設定ファイル（conf ファイル）を編集する

イベントログトラップ機能のイベントサーバ設定ファイル（conf ファイル）を編集します。

この作業は，Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。

次に示すファイルを編集して，イベントログトラップ機能の動作環境を設定します。

- JP1/Base のインストール先フォルダ¥conf¥event¥servers¥default¥conf

イベントログトラップ機能の conf ファイルの設定例について次に説明します。

設定例の条件を次の表に示します。

表 5-15　設定例の条件（イベントログトラップ機能の conf ファイル）

項番	項目	この例での値
1	監査ログ専用イベントサーバ名	Host01-adm
2	監査ログ専用イベントサーバの IP アドレス	172.16.1.10
3	監査ログ専用イベントサーバの転送用ポート番号※	24101

注※

ポート番号は監査ログ収集対象サーバで未使用の番号を指定してください。

設定例を次に示します。

イベントログトラップ機能の conf ファイルの設定例

conf ファイルを次のように編集します。

remote-server パラメーターは，デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
remote-server Host01-adm close 172.16.1.10 24101
```

なお，IPv6 アドレスで通信する場合は，remote-server パラメーターの監査ログ専用イベントサーバの IP アドレスに<jp1hosts2>を設定します。

IPv6 アドレスで通信する場合の設定例の条件を次の表に示します。

表 5-16　IPv6 アドレスで通信する場合の設定例の条件（イベントログトラップ機能の conf ファイル）

項番	項目	この例での値
1	監査ログ専用イベントサーバ名	Host01-adm
2	監査ログ専用イベントサーバの IP アドレス	2001:db8::a
3	監査ログ専用イベントサーバの転送用ポート番号※	24101

注※

ポート番号は監査ログ収集対象サーバで未使用の番号を指定してください。

設定例を次に示します。

イベントログトラップ機能の conf ファイルの設定例（IPv6 アドレスで通信する場合）

conf ファイルを次のように編集します。

remote-server パラメーターは，デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
remote-server Host01-adm close <jp1hosts2> 24101
```

(4)　イベントログトラップ機能の転送設定ファイル（forward ファイル）を編集する

イベントログトラップ機能の転送設定ファイル（forward ファイル）を編集します。

この作業は，Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。

監査ログ収集対象サーバのイベントサーバで収集したイベントログが監査ログ専用イベントサーバに転送させるための設定を，次に示すファイルへ追加します。

- JP1/Base のインストール先フォルダ¥conf¥event¥servers¥default¥forward

forward ファイルの定義内容は，収集対象となるプログラムによって異なります。さらに，Windows イベントログに出力される複数のプログラムのログを収集する場合も forward ファイルの定義内容が異なります。定義内容については，プログラムごとに次に示す個所を参照してください。

- Windows イベントログ（セキュリティに関する情報）だけを収集する場合

  「(a)　Windows イベントログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。
- Oracle のログだけを収集する場合

  「(b)　Oracle のログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。
- Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログだけを収集する場合

  「(c)　Hitachi Storage Command Suite または Hitachi Command Suite のログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。
- Windows イベントログに出力される複数のプログラムのログを収集する場合

  「(d)　Windows イベントログに出力される複数のプログラムのログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。

(a)　Windows イベントログを収集する場合の定義内容（転送設定ファイル（forward ファイル））

Windows イベントログ（セキュリティに関する情報）を収集する場合に，forward ファイルで定義する内容について説明します。

この作業は，Windows イベントログ（セキュリティに関する情報）だけを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。Windows イベントログに出力されるほかのログも収集したい場合は「(d)　Windows イベントログに出力される複数のプログラムのログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。

JP1/Audit Management - Manager で標準サポートしている Windows イベントログ（セキュリティに関する情報）のイベント ID を次に示します。

ログオン イベントの Windows イベントログ（セキュリティに関する情報）

標準サポートしているイベント ID は「4624～4625」および「4634」です。

アカウント管理の Windows イベントログ（セキュリティに関する情報）

標準サポートしているイベント ID は「4720」，「4722～4735」，「4737～4738」，「4740」，および「4744～4763」です。

ここに示す Windows イベントログ（セキュリティに関する情報）以外のイベント ID は，JP1/Audit Management - Manager では標準サポート外となります。標準サポート外のイベント ID については，Windows のマニュアルを参照してください。

Windows イベントログ（セキュリティに関する情報）を収集する場合の forward ファイルの設定例について次に説明します。

設定例の条件を次の表に示します。

表 5-17　設定例の条件（Windows イベントログ（セキュリティに関する情報）を収集する場合の forward ファイル）

項番	項目	この例での値
1	監査ログ専用イベントサーバ名	Host01-adm
2	転送するイベントログ	次に示すイベント ID のイベントログ 「4624～4625」,「4634」

設定例を次に示します。

forward ファイルの設定例（Windows イベントログ（セキュリティに関する情報）を収集する場合）

forward ファイルを編集します。デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
to host01-adm
E.PRODUCT_NAME IN /HITACHI/JP1/NTEVENT_LOGTRAP/Microsoft%20Windows%20security%20auditing.
E.A5 IN 4624 4625 4634
end-to
```

(b)　Oracle のログを収集する場合の定義内容（転送設定ファイル（forward ファイル））

Oracle のログを収集する場合に，forward ファイルで定義する内容について説明します。

この作業は，Oracle のログだけを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。Windows イベントログに出力されるほかのログも収集したい場合は「(d)　Windows イベントログに出力される複数のプログラムのログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。

JP1/Audit Management - Manager で収集できる Oracle のログのイベント ID を次に示します。

Oracle のログ

収集できるイベント ID は「34」です。

Oracle のログを収集する場合の forward ファイルの設定例について次に説明します。

設定例の条件を次の表に示します。

表 5-18　設定例の条件（Oracle のログを収集する場合の forward ファイル）

項番	項目	この例での値
1	監査ログ専用イベントサーバ名	Host01-adm

項番	項目	この例での値
2	転送するイベントログ	次に示すイベント ID のイベントログ 「34」

設定例を次に示します。

forward ファイルの設定例（Oracle のログを収集する場合）

forward ファイルを次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
to Host01-adm
E.PRODUCT_NAME BEGIN /HITACHI/JP1/NTEVENT_LOGTRAP/Oracle
E.A5 IN 34
end-to
```

(c) Hitachi Storage Command Suite または Hitachi Command Suite のログを収集する場合の定義内容（転送設定ファイル（forward ファイル））

Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを収集する場合に，forward ファイルで定義する内容について説明します。

この作業は，Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログだけを JP1/Audit Management - Manager の監査ログとして収集したい場合に必要です。Windows イベントログに出力されるほかのログも収集したい場合は「(d)　Windows イベントログに出力される複数のプログラムのログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。

JP1/Audit Management - Manager で収集できる Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログのイベント ID を次に示します。

Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログ

収集できるイベント ID は「1」です。

Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを収集する場合の forward ファイルの設定例について次に説明します。

設定例の条件を次の表に示します。

表 5-19　設定例の条件（Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のログを収集する場合の forward ファイル）

項番	項目	この例での値
1	監査ログ専用イベントサーバ名	Host01-adm
2	転送するイベントログ	次に示すイベント ID のイベントログ 「1」

設定例を次に示します。

forward ファイルの設定例（Hitachi Storage Command Suite または Hitachi Command Suite 7（Windows の場合）のログを収集する場合）

forward ファイルを次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
to Host01-adm
E.PRODUCT_NAME IN /HITACHI/JP1/NTEVENT_LOGTRAP/HBase%20Storage%20Mgmt%20Log
E.A5 IN 1
end-to
```

forward ファイルの設定例（Hitachi Command Suite 8（Windows の場合）のログを収集する場合）

forward ファイルを次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
to Host01-adm
E.PRODUCT_NAME IN /HITACHI/JP1/NTEVENT_LOGTRAP/HBase64%20Storage%20Mgmt%20Log
E.A5 IN 1
OR
E.PRODUCT_NAME IN /HITACHI/JP1/NTEVENT_LOGTRAP/HBase64%20Event
E.A5 IN 1
end-to
```

(d) Windows イベントログに出力される複数のプログラムのログを収集する場合の定義内容（転送設定ファイル（forward ファイル））

Windows イベントログに出力される複数のプログラムのログを収集したい場合に，forward ファイルで定義する内容について説明します。

ここでは，Windows イベントログ（セキュリティに関する情報）と Oracle のログの両方を監査ログとして収集する場合の設定例を示します。

Windows イベントログにログが出力されるプログラムを，複数設定するときの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

JP1/Audit Management - Manager で収集できるログのイベント ID については，プログラムごとに次に示す個所を参照してください。

- Windows イベントログ（セキュリティに関する情報）のイベント ID

  「(a)　Windows イベントログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。
- Oracle のログのイベント ID

  「(b)　Oracle のログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。
- Hitachi Storage Command Suite または Hitachi Command Suite（Windows の場合）のイベント ID

「(c)　Hitachi Storage Command Suite または Hitachi Command Suite のログを収集する場合の定義内容（転送設定ファイル（forward ファイル））」を参照してください。

設定例の条件を次の表に示します。

表 5-20　設定例の条件（Windows イベントログ（セキュリティに関する情報）および Oracle のログを収集する場合の forward ファイル）

項番	項目	この例での値
1	監査ログ専用イベントサーバ名	Host01-adm
2	転送するイベントログ（Windows イベントログ（セキュリティに関する情報））	次に示すイベント ID のイベントログ 「4624～4625」,「4634」
3	転送するイベントログ（Oracle のログ）	次に示すイベント ID のイベントログ 「34」

設定例を次に示します。

forward ファイルの設定例（Windows イベントログ（セキュリティに関する情報）および Oracle のログを収集する場合）

forward ファイルを次のように編集します。

デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
to Host01-adm
E.PRODUCT_NAME IN /HITACHI/JP1/NTEVENT_LOGTRAP/Microsoft%20Windows%20security%20auditing.
E.A5 IN 4624 4625 4634
OR
E.PRODUCT_NAME BEGIN /HITACHI/JP1/NTEVENT_LOGTRAP/Oracle
E.A5 IN 34
end-to
```

(5)　イベントログトラップ機能を自動的に起動する

Windows イベントログに出力されるログを JP1/Audit Management - Manager の監査ログとして出力するために，イベントログトラップ機能を起動させておく必要があります。

JP1/Base のイベントログトラップ機能が OS 起動時に自動的に起動するように設定します。

イベントサービスの起動後にイベントログトラップ機能が起動するように，JP1/Base の起動順序定義ファイル（**JP1/Base のインストール先フォルダ**¥conf¥boot¥Jp1svprm.dat）を編集します。「5.4.2(4)　イベントサービスを自動的に起動する」で編集した起動順序定義ファイルをテキストエディタで開いて記述を編集します。

設定例を次に示します。

起動順序定義ファイルの設定例

起動順序定義ファイルに次の記述を追加します。デフォルトの記述は残したまま，新しい記述を追加してください。

```
#イベントサービスを定義する記述よりあとに記述を追加し，イベントサービスが先に起動されるように設定する。
[Jp1BaseEventlogTrap]
Name=JP1/BaseEventlogTrap
ServiceName=JP1_Base_EventlogTrap
```

起動順序定義ファイルの設定内容については，マニュアル「JP1/Base 運用ガイド」を参照してください。

イベントログトラップ機能を自動的に起動する設定にしたあと，OS を再起動し，イベントサービスおよびイベントログトラップ機能が自動的に起動されるかどうかを確認してください。確認方法は Windows と UNIX で異なります。それぞれの確認方法を次に示します。

Windows の場合

コントロールパネルの「管理ツール」から「サービス」を開いて，イベントサービスおよびイベントログトラップ機能が起動されているかどうかを確認してください。または，jevstat コマンドを実行して確認してください。ただし，jevstat コマンドを実行することで確認できるのは，イベントサービスの起動だけです。イベントログトラップ機能の起動は確認できません。

UNIX の場合

jevstat コマンドを実行して確認してください。ただし，jevstat コマンドを実行することで確認できるのは，イベントサービスの起動だけです。イベントログトラップ機能の起動は確認できません。jevstat コマンドの詳細は，マニュアル「JP1/Base 運用ガイド」を参照してください。

なお，イベントサービスおよびイベントログトラップ機能が起動されても，収集対象の監視は開始されません。収集対象の監視は，［監査ログ収集マネージャ］ウィンドウで監視を開始するための設定をした時点から開始されます。

イベントログトラップ機能は手動でも起動できます。必ずイベントサービスを起動後に，イベントログトラップ機能を起動してください。イベントサービスを起動する方法については「5.4.2(4)　イベントサービスを自動的に起動する」を参照してください。

イベントログトラップ機能を手動で開始する方法を次に示します。

1. コントロールパネルの「管理ツール」から「サービス」を開く。
2. 「JP1/Base EventlogTrap」を選択し，プロパティで［開始］ボタンをクリックする。

開始する場合と同様の方法でイベントログトラップ機能を停止できます。

5.4.4　ログファイルトラップ機能の設定を確認する

ログファイルトラップ機能が起動されているかどうかを確認します。

この作業は，監査ログ収集対象サーバの OS が Windows と UNIX のどちらの場合でも必要です。ただし，確認方法は Windows と UNIX で異なります。それぞれの確認方法を次に示します。

Windows の場合

コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Base LogTrap のサービスが起動されていることを確認してください。起動されていることを確認後，ログファイルトラップ機能が自動起動されるよう設定されているかどうかを確認してください。確認方法については，マニュアル「JP1/Base 運用ガイド」を参照してください。

UNIX の場合

ログファイルトラップ管理デーモン（jevlogd）が動作していることを確認してください。動作していない場合は，次に示すコマンドを実行し，ログファイルトラップ管理デーモンを起動させてください。

```
jevlogdstart
```

ログファイルトラップ管理デーモンおよび jevlogdstart コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

5.4.5 UNIX システムログの変換設定をする

監査ログ収集対象サーバで出力された UNIX システムログを監査ログとして収集したい場合，UNIX システムログを変換するのに必要な設定をします。

この作業は，UNIX システムログを JP1/Audit Management - Manager の監査ログとして収集しない場合は不要です。

(1) 情報を出力するためのシステムログファイルを作成する

UNIX システムログを収集するには，ログイン，ログアウト，またはユーザ権限変更などの収集対象を格納するためのシステムログファイルが必要です。収集対象を格納するシステムログファイルが存在するかどうかを確認し，存在しない場合はログファイルを作成してください。なお，ユーザ権限変更を格納するためのシステムログファイルが存在する場合は，必要に応じて，ファイルをバックアップ後，ファイルを再作成してください。

システムログファイルの作成方法の詳細については，各 OS のマニュアルを参照してください。

OS が出力する収集情報およびシステムログのファイル名を次の表に示します。

表 5-21 OS が出力する収集情報およびファイル名

項番	収集情報	ファイル名
1	ログイン，ログアウト	• HP-UX の場合 /var/adm/wtmps • AIX の場合 /var/adm/wtmp

項番	収集情報	ファイル名
		• Solaris の場合 /var/adm/wtmpx • Linux の場合 /var/log/wtmp
2	ログイン失敗	• HP-UX の場合 /var/adm/btmps • AIX の場合 /etc/security/failedlogin • Solaris の場合 /var/adm/loginlog • Linux の場合 /var/log/btmp
3	ユーザ権限の変更※	• HP-UX の場合 /var/adm/sulog • AIX の場合 /var/adm/sulog • Solaris の場合 /var/adm/sulog

注※

OS の種類が Linux の場合は，ユーザ権限の変更情報は収集できません。

(2) UNIX のログファイルの変換コマンドを cron デーモンへ登録する

UNIX システムログを定期的にデータ変換したり収集したりするために，UNIX のログファイルの変換コマンドを cron デーモンへ登録します。crontab への登録は，root ユーザで実施してください。

なお，UNIX のログファイルの変換コマンドを実行する周期は，監査ログ管理サーバで監査ログを収集する周期を考慮し，設定してください。

cron デーモンへの登録例

ログイン，ログアウト情報を毎日 20 時に変換したい場合の登録例を次に示します。

```
0 20 * * * /opt/jp1netmaudit/agent/bin /admuxlogcol -t login
```

注

JP1/NETM/Audit - Manager 09-00 より前のバージョンから上書きインストールした場合，admuxlogcol コマンドのインストール先ディレクトリは「/opt/jp1netmaudit/manager/bin」になります。

cron デーモンへの登録の詳細は，各 OS のマニュアルを参照してください。

(3) UNIX システムログを収集する場合の注意事項

UNIX システムログを監査ログとして収集する場合の注意事項を次に示します。

- sulog を収集する場合，ユーザ名に「-」が含まれていると，情報が正しく収集できません。
- sulog を収集する場合，OS が出力するログには年の情報は出力されません。UNIX システムログの変換コマンドでは，次の方法で年の情報を追加して出力します。

  「ログ中の月＜＝ UNIX システムログの変換を実施した月」の場合

  「変換を実施した時点の年」の情報を追加。

  「ログ中の月＞ UNIX システムログの変換を実施した月」の場合

  「変換を実施した時点の年 - 1」の情報を追加。

  例えば，ログ中の月が 11 月で，2007 年 10 月に UNIX ログ変換を実施した場合，2006 年 11 月として情報が追加されます。なお，ファイルに 1 年以上のデータが蓄積されていた場合，年が正しく設定されないことがあります。

- 使用している OS によって，JP1/Audit Management - Manager が収集対象としているファイルが単調増加ファイルになっている場合があります。定期的にファイルサイズを確認し，ファイルのバックアップおよび再作成を実施してください。なお，ファイルのバックアップおよび再作成を実施する場合は，バックアップ前に一度，UNIX システムログの変換コマンドを実行し，ログ情報を変換してください。
- 使用している OS によっては，システムの起動時またはランレベルの変更時に動作するシェルスクリプトで，JP1/Audit Management - Manager が収集対象としているファイルのバックアップを実行していることがあります。この場合，システムを再起動したり，ランレベルを変更したりすると，情報が収集されないことがあります。UNIX システムログの変換コマンドを実行するシェルスクリプトを作成し，バックアップのシェルスクリプトが実行される前に動作するようシステムへ登録してください。

  シェルスクリプトの記載例（sulog を変換する場合）

  シェルスクリプトの記載例を次に示します。

```
#!/sbin/sh
#
ADMUXLOGCOL=/opt/jp1netmaudit/agent/bin/admuxlogcol
export ADMUXLOGCOL

case $1 in
'start')
        if [ -x ${ADMUXLOGCOL} ]; then
                    ${ADMUXLOGCOL} -t su
                    if [ $? -ne 0 ]; then
                                echo "ERROR CODE $?"
                    fi
        fi
        ;;

*)
        echo "usage: $0 {start}"
        ;;
```

```
esac
exit 0
```

5.4.6　監査ログ収集対象プログラムをセットアップする

監査ログ収集対象サーバで監査ログの収集対象プログラムをセットアップし，JP1/Audit Management - Manager で監査ログを収集できるようにします。

監査ログの収集対象となるすべてのプログラムは，必要に応じて監査ログが出力されるように設定してから運用を開始してください。

監査ログ出力の設定方法については，各プログラムのマニュアルを参照してください。

5.5　監査ログ管理サーバのセットアップ

監査ログ管理サーバをセットアップします。

セットアップの詳細について，次に説明します。

5.5.1　Microsoft Internet Information Services をセットアップする

監査ログ管理サーバで，Microsoft Internet Information Services をセットアップします。

Microsoft Internet Information Services をセットアップすることによって，監査ログ管理画面から，検索結果や集計結果の出力ファイルおよび監査ログのバックアップファイルがダウンロードできるようになります。

なお，Microsoft Internet Information Services の各種タイムアウトの設定については，必要に応じて適切に設定してください。このほかの Microsoft Internet Information Services のセットアップについては，Windows のマニュアルを参照し，必要に応じて実施してください。

(1)　バックアップファイルの格納先フォルダの設定

監査ログ管理サーバに，バックアップファイルの格納先フォルダを作成し，そのフォルダへリンクさせる仮想ディレクトリを設定します。この設定によって，監査ログ管理画面から監査ログのバックアップファイルをダウンロードできるようになります。

なお，仮想ディレクトリは，IIS マネージャで設定します。仮想ディレクトリは，JP1/Audit Management - Manager のインストール時に自動的に作成される仮想ディレクトリ「jp1netmaudit」の配下に「backupdata」という名称で追加します。

仮想ディレクトリの設定手順を次に示します。

1. 監査ログ管理サーバ上に，バックアップファイルの格納先として使用するフォルダを作成する。
   任意のフォルダ名を設定してください。

2. コントロールパネルの「管理ツール」から「インターネット インフォメーション（IIS）マネージャ」を開く。
   IIS マネージャが起動します。

3. IIS マネージャの左フレームで，［サーバ名］－［サイト］－［Default Web Site］にある［jp1netmaudit］を右クリックし，［仮想ディレクトリの追加］を選択する。
   仮想ディレクトリの追加ダイアログが表示されます。

4. 仮想ディレクトリの追加ダイアログで，追加する仮想ディレクトリを設定する。
   ダイアログの各項目で次のように設定します。

- エイリアス
  エイリアス名として，「backupdata」を指定してください。
- 物理パス
  コンテンツの場所として，手順 1 で作成したフォルダのパスを指定してください。
- アクセス許可
  この仮想ディレクトリへのアクセスは許可しません。「backupdata」の「ハンドラマッピング」を開いて，「機能のアクセス許可の編集...」のすべてのチェックを外してください。

なお，監査ログ管理サーバ上で監査ログのバックアップを取得するときは，ここで作成したフォルダを指定してください。

(2) アプリケーションプールのプロパティ設定変更

アプリケーションプールのプロパティ設定を変更します。

設定の変更手順を次に示します。

1. コントロールパネルの「管理ツール」から「インターネット インフォメーション（IIS）マネージャ」を開く。
   IIS マネージャが起動します。
2. IIS マネージャの左フレームの［サーバ名］にある［アプリケーションプール］を選択する。
   ［アプリケーションプール］画面が表示されます。
3. [DefaultAppPool] を右クリックし，「リサイクルの設定」をクリックする。
   リサイクル条件に表示されるすべてのチェックを外してください。
4. [DefaultAppPool] を右クリックし，「詳細設定」をクリックする。
   次の項目を「False」に設定します。
   - 「プロセス モデル」－「Ping の有効化」
   - 「ラピッド フェール保護」－「有効」

   さらに，「プロセスモデル」－「アイドル状態のタイムアウト」を「0」に設定してください。

(3) IIS 送信バッファの最大サイズの設定

監査ログ管理画面からファイルをダウンロードするときなどの最大サイズを設定します。また，監査ログ管理画面でユーザ作成のフォルダやパターンを大量に作成する場合も，IIS 送信バッファの最大サイズは，デフォルトより大きい値を設定しておく必要があります。

設定手順を次に示します。

1. コントロールパネルの「管理ツール」から「インターネット インフォメーション（IIS）マネージャ」を開く。

IIS マネージャが起動します。

2. IIS マネージャの左フレームで，［サーバ名］－［サイト］－［Default Web Site］にある［jp1netmaudit］を選択し，「ASP」を開く。

3. 「動作」－「制限プロパティ」－「応答バッファ処理の制限」にダウンロード時の最大バッファサイズを指定する。

次に示すダウンロードするファイルより十分大きいサイズを指定してください。

- 検索結果，集計結果，および統計結果の出力ファイル（CSV 形式ファイルまたは PDF ファイル）
- 監査ログのバックアップファイル

最大サイズは，最低でも 1 ギガバイト以上の値を設定してください。設定できる値は，2,147,483,647 バイト以内の整数です。デフォルト値は 4,194,304 バイト（4 メガバイト）です。

なお，それぞれのファイルのサイズは，検索，集計，統計，またはバックアップ時の指定内容によって異なります。また，作成するフォルダやパターンの数によっても異なります。

4. コントロールパネルの「管理ツール」から「サービス」を開いて，World Wide Web Publishing Service サービスを再起動する。

(4) IIS 受信バッファの最大サイズの設定

監査ログ管理画面からファイルをアップロードするときの最大サイズを設定します。

設定手順を次に示します。

1. コントロールパネルの「管理ツール」から「インターネット インフォメーションサービス（IIS）マネージャ」を開く。

IIS マネージャが起動します。

2. IIS マネージャの左フレームで，［サーバ名］－［サイト］－［Default Web Site］にある［jp1netmaudit］を選択し，「ASP」を開く。

3. 「動作」－「制限プロパティ」－「最大要求エンティティボディ制限」にアップロード時の最大バッファサイズを指定する。

次に示すアップロードするファイルより十分大きいサイズを指定してください。

- パターン情報ファイル

4. コントロールパネルの「管理ツール」から「サービス」を開いて，World Wide Web Publishing Service サービスを再起動する。

5.5.2　services ファイルを確認する

JP1/Audit Management - Manager のセットアップ時，次に示すサービスのポート番号が services ファイルに設定されます。

JP1/NETM/Audit - Manager Define サービス

デフォルトで設定されているポート番号は「24105」です。

JP1/NETM/Audit - Manager Convert サービス

デフォルトで設定されているポート番号は「24106」です。

ただし，デフォルトで設定されているポート番号をほかで使用している場合は，未使用のポート番号に設定し直す必要があります。services ファイルの下線部分の値を，適切な値に変更してください。

```
#JP1/NETM/Audit - Manager Define
auditd_monsrv   24105/tcp
#JP1/NETM/Audit - Manager Convert
audita_admsrv   24106/tcp
```

services ファイルを変更した場合，JP1/NETM/Audit - Manager Define サービスおよび JP1/NETM/Audit - Manager Convert サービスを再起動してください。

5.5.3　JP1/Base のユーザ管理機能を設定する

JP1/Base の JP1 ユーザ管理機能を設定することによって，監査ログ管理画面を操作するユーザを指定できます。JP1 ユーザ管理機能では，次に示す内容を設定します。

- 認証サーバの指定
- JP1 ユーザの登録および操作権限
- ユーザマッピング

このほかの JP1/Base のセットアップ項目については，環境に合わせて実施してください。JP1/Base のセットアップに必要な準備，JP1/Base のセットアップ全体の内容，およびユーザ管理機能の設定の詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

(1)　認証サーバを指定する

認証サーバのホスト名を指定します。

監査ログ管理サーバにインストールされている JP1/Base を認証サーバに指定する場合は，監査ログ管理サーバをホスト名として指定してください。

(2) JP1 ユーザの登録および操作権限を設定する

JP1/Audit Management - Manager の監査ログ管理画面を操作するユーザの JP1 ユーザ名，パスワード，および操作権限を設定します。

この設定は，認証サーバ上で実施してください。

監査証跡管理システム内には認証サーバが一つ以上必要です。監査ログ管理サーバ以外のサーバを認証サーバとして指定している場合は，そのサーバ上で，JP1 ユーザの登録および操作権限の設定を実施してください。

監査ログ管理画面のユーザに必要な操作権限を次に示します。

- 「JP1_Audit_Admin」または「JP1_Audit_Operator」
  どちらも同じ JP1 権限レベルですが，JP1 権限レベルを使い分ける必要がない場合は，「JP1_Audit_Admin」を使用してください。

(3) ユーザマッピングの設定

監査ログ管理画面を操作するユーザとして設定した JP1 ユーザと，監査ログ管理サーバの OS ユーザ名とのユーザマッピングを設定します。

監査ログ管理サーバの情報を基に，監査ログ管理画面を操作するため，監査ログ管理画面を操作するユーザとして設定した JP1 ユーザは，監査ログ管理サーバの OS ユーザ権限も必要となります。これをユーザマッピングと呼びます。

5.5.4 JP1/Base の jevsend コマンドを実行する

監査ログ管理サーバのイベントサーバに何もデータが格納されていない場合，転送されてくる JP1 イベントを監視できないため，事前に JP1 イベントを登録しておく必要があります。

監査ログ収集対象サーバから監査ログ管理サーバへ転送されてくる JP1 イベントを監視できるようにするため，jevsend コマンドを実行してイベントサーバに JP1 イベントを登録します。

コマンド実行例を次に示します。

```
jevsend
```

なお，監査ログ管理サーバをクラスタ環境で運用する場合には，jevsend コマンドの-d オプションに，監査ログ管理サーバの論理ホスト名を指定してください。

クラスタ環境で運用する場合のコマンド実行例を次に示します。

```
jevsend -d 論理ホスト名
```

jevsend コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

5.5.5 JP1/Base の API 設定ファイル（api ファイル）を編集する

監査ログ収集対象サーバの監査ログ専用イベントサーバに蓄積した監査ログを，監査ログ管理サーバで収集できるように，JP1/Base の api ファイルを編集します。

api ファイルのファイルパスや設定内容を次に示します。

api ファイルのファイルパスと設定内容

ファイルパス

JP1/Base のインストール先フォルダ¥conf¥event¥api

設定内容

server パラメーターを追加して，監査ログ収集対象サーバにある監査ログ専用イベントサーバの IP アドレスと AP 用ポート番号を定義します。

api ファイルの設定例について次に説明します。なお，説明する設定例では，次に示す二つの監査ログ収集対象サーバから監査ログを収集することとします。

- Host01
- Host02

設定例の条件を次の表に示します。

表 5-22 設定例の条件（管理サーバにある JP1/Base の api ファイル）

項番	ホスト名	項目	この例での値
1	Host01	監査ログ専用イベントサーバ名※1	Host01-adm
2		監査ログ専用イベントサーバの IP アドレス	172.16.1.10
3		監査ログ専用イベントサーバの AP 用ポート番号※2	24102
4	Host02	監査ログ専用イベントサーバ名※1	Host02-adm
5		監査ログ専用イベントサーバの IP アドレス	172.16.1.20
6		監査ログ専用イベントサーバの AP 用ポート番号※2	24102

注※1

監査ログ専用イベントサーバ名は，監査ログ収集対象サーバのホスト名のあとに「-adm」を付けて設定してください。

注※2

監査ログ収集対象サーバで設定したポート番号を指定してください。

設定例を次に示します。

api ファイルの設定例

api ファイルを次のように編集します。

server パラメーターは，デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
server Host01-adm keep-alive 172.16.1.10 24102
server Host02-adm keep-alive 172.16.1.20 24102
```

(1) IPv6 アドレスで通信する場合

IPv6 アドレスで通信する場合は，server パラメーターの監査ログ収集対象サーバの IP アドレスに<jp1hosts2>を設定します。

また，jp1hosts2 定義ファイルに，監査ログ専用イベントサーバ名と監査ログ専用イベントサーバの IP アドレスの対応を定義して，jp1hosts2 情報に設定します。

IPv6 アドレスで通信する場合の設定例の条件を次の表に示します。

表 5-23 IPv6 アドレスで通信する場合の設定例の条件（管理サーバにある JP1/Base の api ファイル）

項番	ホスト名	項目	この例での値
1	Host01	監査ログ専用イベントサーバ名※1	Host01-adm
2		監査ログ専用イベントサーバの IP アドレス	2001:db8::a
3		監査ログ専用イベントサーバの AP 用ポート番号※2	24102
4	Host02	監査ログ専用イベントサーバ名※1	Host02-adm
5		監査ログ専用イベントサーバの IP アドレス	2001:db8::14
6		監査ログ専用イベントサーバの AP 用ポート番号※2	24102

注※1

監査ログ専用イベントサーバ名は，監査ログ収集対象サーバのホスト名のあとに「-adm」を付けて設定してください。

注※2

監査ログ収集対象サーバで設定したポート番号を指定してください。

api ファイルの設定例を次に示します。

api ファイルの設定例

api ファイルを次のように編集します。

server パラメーターは，デフォルトで記述されている行の下に，次に示す記述を新しく追加してください。

```
server Host01-adm keep-alive <jp1hosts2> 24102
server Host02-adm keep-alive <jp1hosts2> 24102
```

jp1hosts2 情報の設定例および設定手順を次に示します。

jp1hosts2 情報の設定例および設定手順

1. jp1hosts2 定義ファイルに監査ログ専用イベントサーバ名と監査ログ専用イベントサーバの IP アドレスの対応を定義する。

   jp1hosts2 定義ファイルに，次に示す記述を新しく追加してください。なお，jp1hosts2 定義ファイルのファイル名は任意です。

```
Host01-adm 2001:db8::a
Host02-adm 2001:db8::14
```

2. 手順 1 で定義した jp1hosts2 定義ファイルを，jbshosts2import コマンドでインポートする。

   次に示すコマンドを実行してください。

```
jbshosts2import -o jp1hosts2 定義ファイル
```

   コマンドが正常に終了すると，jp1hosts2 定義ファイルに定義した内容が jp1hosts2 情報に設定されます。

5.5.6 監査ログ管理サーバの環境設定をする

監査ログ管理サーバの環境設定をします。

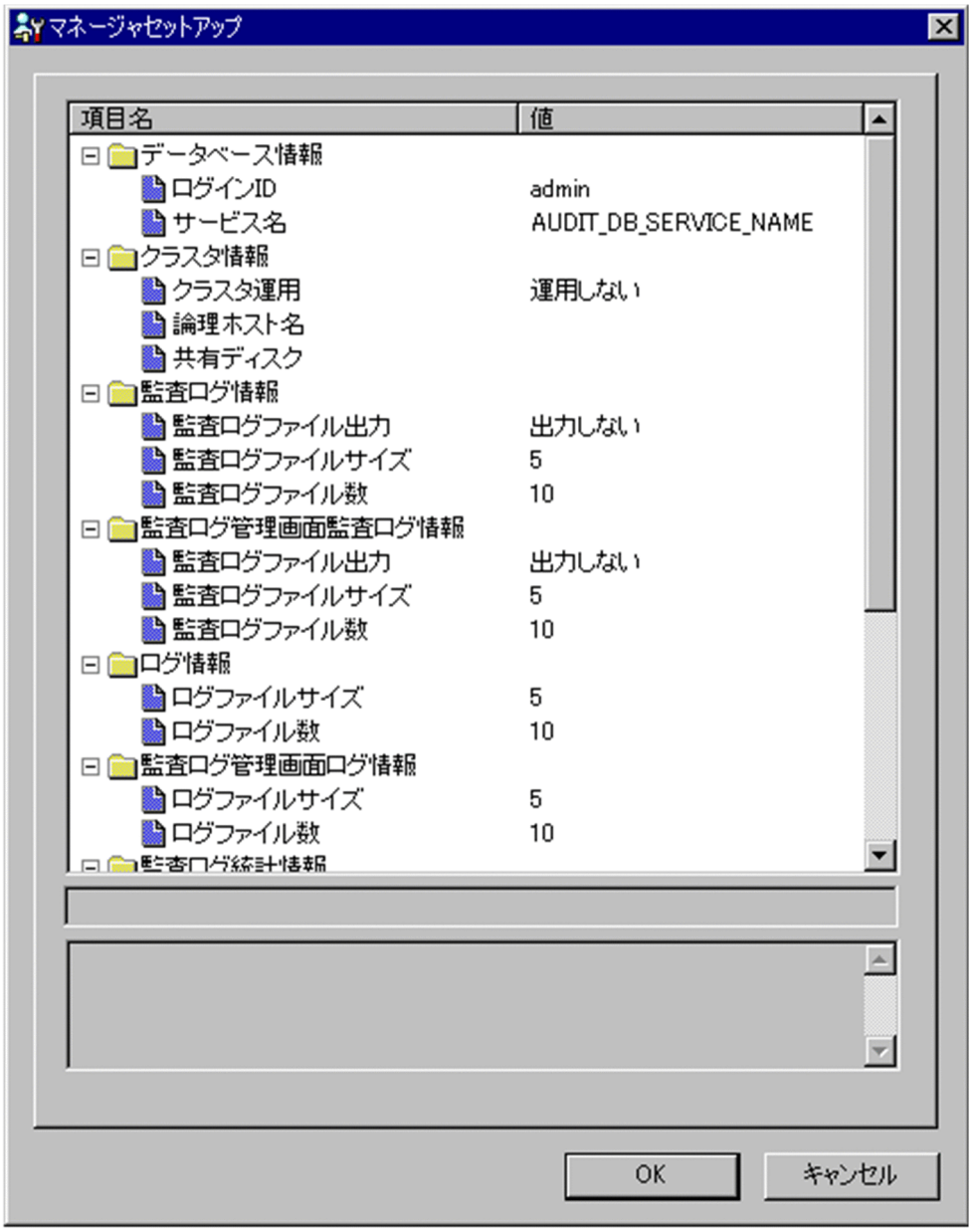
(1) 監査ログ管理サーバの環境設定手順

監査ログ管理サーバの環境設定は，［マネージャセットアップ］ダイアログで実施します。

1. **［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［マネージャセットアップ］を選択する。**

   次の図に示す［マネージャセットアップ］ダイアログが表示されます。

図 5-3 ［マネージャセットアップ］ダイアログ



2. 必要な項目を選択し，使用する環境に合わせて値を設定する。

   設定内容については「(2) ［マネージャセットアップ］ダイアログの設定内容」を参照してください。

3. ［OK］ボタンをクリックする。

   設定内容を確認するダイアログが表示されます。［OK］ボタンをクリックすると，設定内容が保存されて，［マネージャセットアップ］ダイアログが閉じます。

(2) ［マネージャセットアップ］ダイアログの設定内容

［マネージャセットアップ］ダイアログでは，次の情報について設定します。

- データベース情報

- クラスタ情報
- 監査ログ情報
- 監査ログ管理画面監査ログ情報
- ログ情報
- 監査ログ管理画面ログ情報
- 監査ログ統計情報
- 監査ログ管理画面情報
- 監査ログ収集情報

各情報の項目を選択すると，値や文字列を入力するボックスが項目一覧の下に表示されます。入力ボックスで，値や文字列を直接入力するか，プルダウンメニューから値を選択してください。

また，［マネージャセットアップ］ダイアログの設定を変更した場合は，JP1/Audit Management - Manager のサービスおよび World Wide Web Publishing Service サービスを再起動してください。

注意事項

JP1/Audit Management - Manager の設定を変更する前に，JP1/Audit Management - Manager のサービスを停止してください。停止するサービスの詳細は「5.7.2　監査ログ管理サーバを停止する」を参照してください。ただし，［定時収集の設定］ダイアログの「収集時刻」に指定した時間帯は避けてください。指定した時間帯に JP1/Audit Management - Manager のサービスを停止すると，監査ログが収集されません。［定時収集の設定］ダイアログの詳細については「5.6.5　監査ログを定期的に収集する」を参照してください。

(a)　データベース情報

［マネージャセットアップ］ダイアログの「データベース情報」で設定する項目を次の表に示します。

表 5-24　「データベース情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	ログイン ID	データベース接続に使用するユーザのログイン ID を設定します。 この項目はデータベースを作成する前までに設定してください。なお，この項目は，一度設定したら変更できません。	8 バイト以内の文字列を設定します。 使用できる文字を次に示します。 • 半角英数字 • 「#」「@」「¥」	admin	○
2	パスワード※1	データベース接続に使用するユーザのパスワードを設定します。 この項目は，データベースの作成前までに設定してください。 設定時は次に示すことに注意してください。	28 バイト以内の文字列を設定します。 使用できる文字を次に示します。 • 半角英数字 • 「#」「@」「¥」	なし	○

項番	項目	説明	設定値	デフォルト値	必須
		• パスワードの大文字・小文字は区別される • 数字は先頭文字として使用できない			
3	サービス名※2	データベース接続に使用するサービス名を設定します。 ここで設定したサービス名は，データベースを作成する際に ODBC データソース名として使用されます。この項目は，データベースの作成前までに設定してください。	63 バイト以内の文字列を設定します。 使用できる文字を次に示します。 • 半角英数字 • 「#」「"」「$」「%」「&」「'」「^」「~」「|」「`」「:」「+」「_」「/」「.」「>」「<」「-」	AUDIT_DB_SERVICE_NAME	○

（凡例）

○：必ず設定する

注※1

パスワードは，「ログイン ID」を選択した状態のときに，項目一覧の下に表示される［パスワード］ボタンをクリックすると表示される［パスワードの設定］ダイアログで設定します。

なお，一度データベースのパスワードを設定している場合，それ以降でのパスワード変更は次の手順で実施してください。

1. データベースマネージャでパスワードを変更する。

   データベースマネージャでデータベースのパスワードを変更する方法については「10.1.6　データベースのパスワード変更」を参照してください。

2. 「データベース情報」の「ログイン ID」を選択した状態で，［パスワード］ボタンをクリックし，パスワードを変更する。

   パスワード変更時は，［パスワードの設定］ダイアログではなく［パスワードの変更］ダイアログが表示されます。［パスワードの変更］ダイアログでは，変更前パスワードと変更後パスワードを入力します。

   ［パスワードの設定］ダイアログと［パスワードの変更］ダイアログをそれぞれ次の図に示します。

図 5-4　［パスワードの設定］ダイアログ

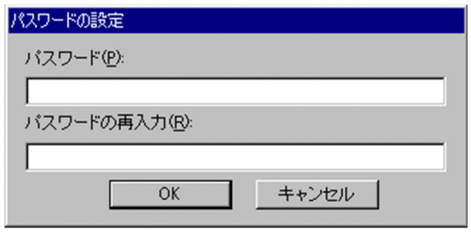
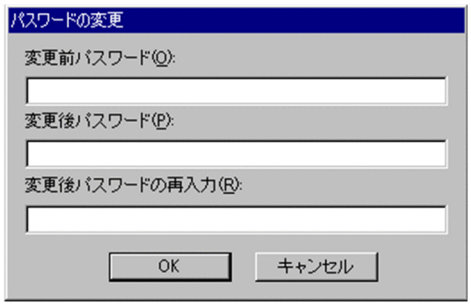


図 5-5 ［パスワードの変更］ダイアログ



注※2

一度サービス名を設定している場合，それ以降でのサービス名の変更は次の手順を実施してください。

1. OS の［ODBC データソースアドミニストレータ］ダイアログでデータソース名を変更する。
［ODBC データソースアドミニストレータ］ダイアログは，コントロールパネルの「管理ツール」から，「データソース（ODBC)」を開いて表示します。「システム DSN」タブで，「データソース名」を変更してください。なお，このほかの項目は変更しないでください。
2.「データベース情報」の「サービス名」を変更する。

(b) クラスタ情報

［マネージャセットアップ］ダイアログの「クラスタ情報」で設定する項目を次の表に示します。なお，クラスタ情報の項目は，JP1/Audit Management - Manager のサービス実行中には設定できません。

表 5-25 「クラスタ情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	クラスタ運用	監査ログ管理サーバをクラスタ環境で運用するかどうかを設定します。	次に示すどちらかを選択します。 •「運用する」 •「運用しない」	運用しない	○
2	論理ホスト名	クラスタ環境での運用の場合に，論理ホスト名を設定します。 「クラスタ運用」で「運用する」を設定した場合は，必ず設定してください。 「クラスタ運用」で「運用しない」を設定した場合は，この項目の設定は無効です。	195 バイト以内の文字列を設定します。 使用できる文字を次に示します。 • 半角英数字 •「-」「_」「.」	なし	△
3	共有ディスク	クラスタ環境での運用の場合に，共有ディスクのフォルダ名をフルパスで設定します。 「クラスタ運用」で「運用する」を設定した場合は，必ず設定してください。	200 バイト以内の文字列を設定します。 使用できない文字を次に示します。 •「:」「*」「?」「"」「<」「>」「|」 「△（半角スペース)」を含んだパスを指定する場合でも，「"」で囲む必要はありません。	なし	△

項番	項目	説明	設定値	デフォルト値	必須
		「クラスタ運用」で「運用しない」を設定した場合は，この項目の設定は無効です。	JP1/Audit Management - Manager は，実行系・待機系の切り替え時，ここで指定した共有ディスク上のフォルダへ引き継ぎが必要な情報を作成します。		

（凡例）

○：必ず設定する

△：必要に応じて設定する

注

クラスタ環境でのシステム運用中は，「論理ホスト名」や「共有ディスク」は変更できません。クラスタ環境のシステムを停止させた状態で変更してください。クラスタ環境のシステムを停止する方法については「6.7.2　監査ログ管理サーバを停止する（クラスタ環境）」を参照してください。

(c)　監査ログ情報

［マネージャセットアップ］ダイアログの「監査ログ情報」で設定する項目を次の表に示します。

表 5-26　「監査ログ情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	監査ログファイル出力	JP1/Audit Management - Manager の監査ログをファイルに出力するかどうかを設定します。	次に示すどちらかを選択します。 • 「出力する」 • 「出力しない」	出力しない	○
2	監査ログファイルサイズ	JP1/Audit Management - Manager が出力する監査ログファイルの最大サイズを設定します。	1～10 の整数（単位：メガバイト）を設定します。	5	○
3	監査ログファイル数	JP1/Audit Management - Manager が出力する監査ログファイルの最大ファイル数を設定します。	1～32 の整数を設定します。	10	○

（凡例）

○：必ず設定する

(d)　監査ログ管理画面監査ログ情報

［マネージャセットアップ］ダイアログの「監査ログ管理画面監査ログ情報」で設定する項目を次の表に示します。

表 5-27 「監査ログ管理画面監査ログ情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	監査ログファイル出力	JP1/Audit Management - Manager の監査ログファイルを監査ログ管理画面で出力するかどうかを設定します。	次に示すどちらかを選択します。 • 「出力する」 • 「出力しない」	出力しない	○
2	監査ログファイルサイズ	監査ログ管理画面で出力する JP1/Audit Management - Manager の監査ログファイルの最大サイズを設定します。	1～10 の整数（単位：メガバイト）を設定します。	5	○
3	監査ログファイル数	監査ログ管理画面で JP1/Audit Management - Manager が出力する監査ログファイルの最大ファイル数を設定します。	1～32 の整数を設定します。	10	○

（凡例）

○：必ず設定する

(e) ログ情報

［マネージャセットアップ］ダイアログの「ログ情報」で設定する項目を次の表に示します。

表 5-28 「ログ情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	ログファイルサイズ	JP1/Audit Management - Manager が出力する製品ログファイルの最大サイズを設定します。	1～10 の整数（単位：メガバイト）を設定します。	5	○
2	ログファイル数	JP1/Audit Management - Manager が出力する製品ログファイルの最大ファイル数を設定します。	1～99 の整数を設定します。	10	○

（凡例）

○：必ず設定する

(f) 監査ログ管理画面ログ情報

［マネージャセットアップ］ダイアログの「監査ログ管理画面ログ情報」で設定する項目を次の表に示します。

表 5-29 「監査ログ管理画面ログ情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	ログファイルサイズ	監査ログ管理画面で JP1/Audit Management - Manager が出力する製品ログファイルの最大サイズを設定します。	1～10 の整数（単位：メガバイト）を設定します。	5	○
2	ログファイル数	監査ログ管理画面で JP1/Audit Management - Manager が出力する製品ログファイルの最大ファイル数を設定します。	1～99 の整数を設定します。	10	○

（凡例）

○：必ず設定する

(g) 監査ログ統計情報

［マネージャセットアップ］ダイアログの「監査ログ統計情報」で設定する項目を次の表に示します。

表 5-30 「監査ログ統計情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	監査ログ統計情報の収集時生成	監査ログの統計情報を自動生成するかどうか設定します。 なお，統計情報は［定時収集の設定］ダイアログで設定した曜日や時刻に自動生成されます。	次に示すどちらかを選択します。 •「生成する」 •「生成しない」	生成しない	○
2	相対日数	監査ログの統計情報の自動生成時に，何日前からの監査ログ情報を基に，統計情報を生成するかを設定します。 「監査ログ統計情報の収集時生成」で「生成する」を設定した場合は，必ず設定してください。	1～366 の整数（単位：日）を設定します。	14	○

（凡例）

○：必ず設定する

(h) 監査ログ管理画面情報

［マネージャセットアップ］ダイアログの「監査ログ管理画面情報」で設定する項目を次の表に示します。

表 5-31 「監査ログ管理画面情報」の設定内容

項目	説明	設定値	デフォルト値	必須
監査ログレポートの表示件数	監査ログレポート画面に表示するレポートの表示最大件数を設定します。	1～99999999 の整数（単位：件）を設定します。	500	○

（凡例）

○：必ず設定する

(i) 監査ログ収集情報

［マネージャセットアップ］ダイアログの「監査ログ収集情報」で設定する項目を次の表に示します。

表 5-32 「監査ログ収集情報」の設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	サービス起動時の監査ログ収集	JP1/NETM/Audit - Manager サービスを起動したときに，監査ログを収集するかどうかを指定します。「収集する」を指定すると，サービス起動後に監査ログの即時収集が実行されます。	次に示すどちらかを選択します。 • 「収集する」 • 「収集しない」	収集しない	○
2	サービス停止中の監査ログ退避※1	JP1/NETM/Audit - Manager サービスの停止中に，イベントデータベースの切り替えが発生した場合，監査ログを収集して退避するかどうかを指定します。	次に示すどちらかを選択します。 • 「退避する」 • 「退避しない」	退避しない	○
3	監査ログ退避フォルダ※2	監査ログの退避先のフォルダを指定します。指定するフォルダのドライブには，最大で（収集対象サーバ数）×（監査ログ退避ファイルサイズ）の空き容量が必要です。	150 バイト以内の文字列を設定します。 使用できない文字を次に示します。 • 「:」「*」「?」「"」「<」「>」「|」	なし	△
4	監査ログ退避ファイルサイズ※3	監査ログの退避ファイル（収集対象サーバ単位）の最大サイズを指定します。 収集対象サーバのイベントデータベースのサイズや切り替えの発生頻度などからサイズを求め，最大となる値を指定してください。	10～10,240 の整数（単位：メガバイト）を設定します。	50	○

（凡例）

○：必ず設定する

△：必要に応じて設定する

注※1

設定を変更する前に，監査ログ退避フォルダ内に監査ログ退避ファイルが存在しないことを確認してください。監査ログ退避ファイルが存在する状態で設定を変更すると，監査ログが重複して収集されます。監査ログ退避ファイルが存在する場合は，次の処理を実施してください。

「退避しない」に変更する場合

次のどちらかの処理を実施してください。

- 即時収集を実行して，監査ログ退避ファイルを取り込む。

- 不要な監査ログ退避ファイルを監査ログ退避フォルダから削除する。

「退避する」に変更する場合

監査ログ退避フォルダから監査ログ退避ファイルを削除する。

注※2

監査ログ退避フォルダを変更する場合は，次の手順で変更してください。

1. 次のサービスを停止する。
   - JP1/NETM/Audit - Manager
   - JP1/NETM/Audit - Manager SubCollect
2. 監査ログ退避フォルダを変更する。
3. 変更前の監査ログ退避フォルダのファイルを変更後の退避フォルダにコピーする。
4. 手順 1 で停止したサービスを再起動する

注※3

監査ログ退避ファイルを処理する際，ファイルサイズの約 5 倍のメモリ容量が必要となります。監査ログ退避ファイルサイズを指定する場合は，監査ログ管理サーバに搭載されているメモリ容量も考慮して指定してください。

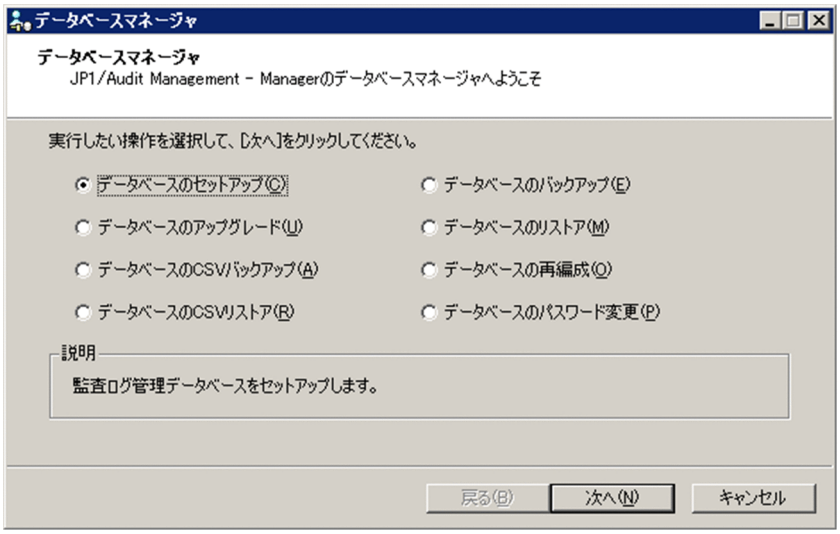
5.5.7 監査ログ管理サーバのデータベースをセットアップする

監査ログ管理サーバで，JP1/Audit Management - Manager が監査ログの管理に使用するデータベースをセットアップします。

データベースのセットアップは，［データベースマネージャ］ダイアログで実施します。

［データベースマネージャ］ダイアログを次の図に示します。

図 5-6 ［データベースマネージャ］ダイアログ



データベースのセットアップは，監査ログ管理サーバの環境設定が完了してから実施してください。監査ログ管理サーバの環境設定の内容については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

データベースは，次に示す設定をして作成します。

- **データベースの基本設定**
  データベースのポート番号を設定します。
  なお，ODBC データソース名および接続ユーザ ID には，監査ログ管理サーバの環境設定をするときに［マネージャセットアップ］ダイアログで指定した内容が反映されます。
- **データベースの詳細設定**
  データベースのサイズおよびデータベース領域の格納先フォルダを設定します。
- **クラスタシステム環境の設定**
  クラスタ環境で使用するかどうかを設定します。

ここでは，監査ログ管理サーバをクラスタ環境で運用しない場合のデータベースのセットアップ手順を説明します。クラスタ環境の場合の構築手順については「6.　クラスタ環境でのシステム構築」を参照してください。

(1)　データベースのセットアップ前の作業

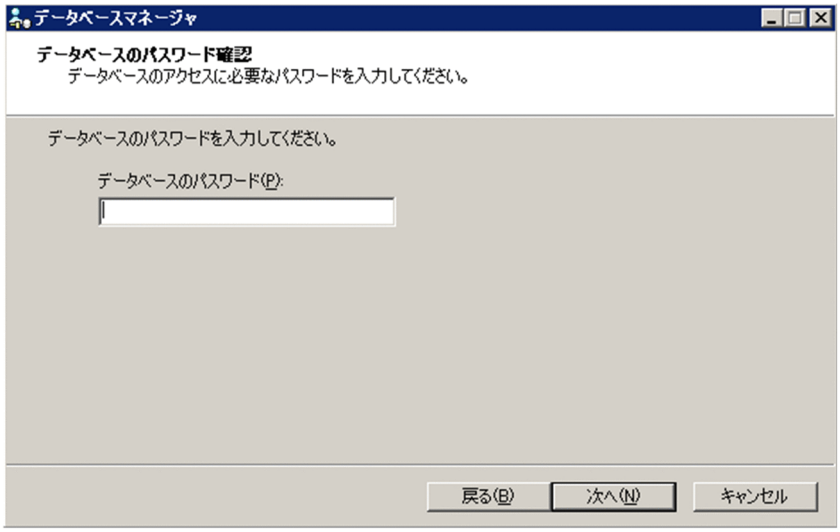
JP1/Base および JP1/Base の認証サーバが起動していないと，JP1 ユーザ情報の取得に失敗し，データベースのセットアップに失敗するおそれがあります。このため，監査ログ管理サーバのデータベースをセットアップする前に，JP1/Base および JP1/Base の認証サーバが起動しているかどうかを確認してください。確認方法については，マニュアル「JP1/Base 運用ガイド」を参照してください。

(2)　データベースのセットアップ手順

1. **［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［データベースマネージャ］を選択する。**
   ［データベースマネージャ］ダイアログが表示されます。

2. **「データベースのセットアップ」を選択して，［次へ］ボタンをクリックする。**
   次の図に示す［データベースのパスワード確認］画面が表示されます。

図 5-7 ［データベースのパスワード確認］画面

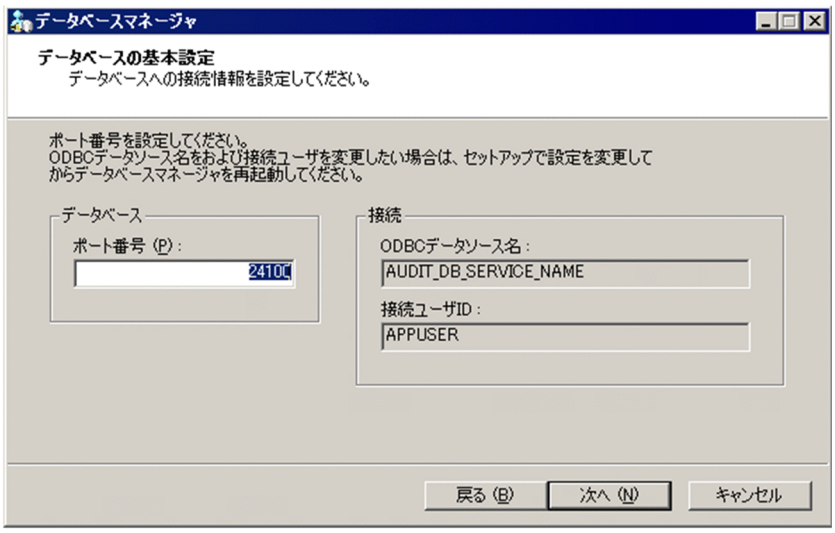


3.「データベースのパスワード」にパスワードを入力して，［次へ］ボタンをクリックする。

次の図に示す［データベースの基本設定］画面が表示されます。

なお，パスワードは，監査ログ管理サーバの環境設定をするときに［パスワードの設定］ダイアログで設定したパスワードを入力してください。

図 5-8 ［データベースの基本設定］画面



4.［データベースの基本設定］画面で，必要な情報を設定する。

画面の各項目について説明します。

- 「ポート番号」

  接続するデータベースサーバのポート番号を指定します。使用されていないポート番号を 5001～65535 の整数で指定してください。デフォルトでは，「24100」が指定されます。

- 「ODBC データソース名」

  ［マネージャセットアップ］ダイアログの「サービス名」に指定した値が表示されます。値を確認してください。

値を変更したい場合は，［マネージャセットアップ］ダイアログで再設定してください。

なお，データベースのセットアップが完了すると，ODBC データソース名は［マネージャセットアップ］ダイアログだけでは変更できなくなります。データベースのセットアップ完了後に ODBC データソース名を変更する方法については「5.5.6(2)(a)　データベース情報」を参照してください。

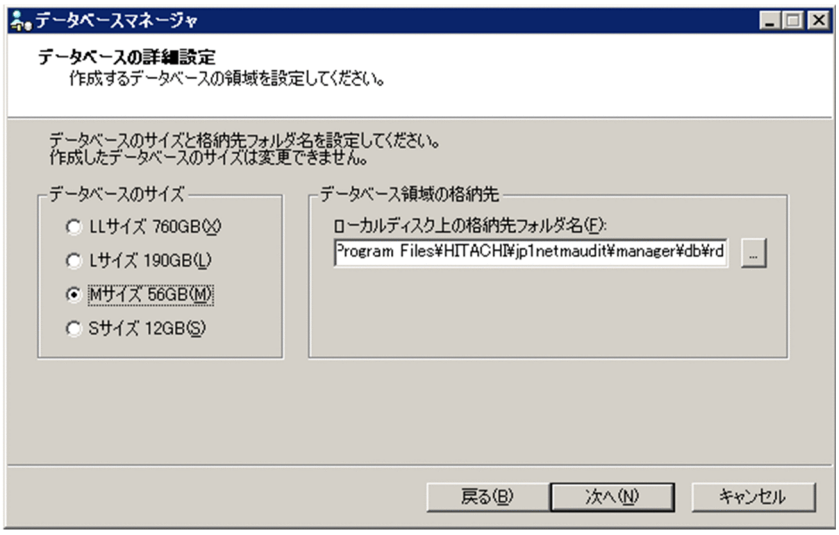
- 「接続ユーザ ID」

  ［マネージャセットアップ］ダイアログの「ログイン ID」に指定した値が表示されます。値を確認してください。なお，［マネージャセットアップ］ダイアログで一度設定したログイン ID は変更できません。

5. ［次へ］ボタンをクリックする。

次の図に示す［データベースの詳細設定］画面が表示されます。

図 5-9　［データベースの詳細設定］画面



6. ［データベースの詳細設定］画面で「データベースのサイズ」および「データベース領域の格納先」を設定する。

画面の各項目について説明します。

- 「データベースのサイズ」

  データベースの最大サイズを「LL サイズ」，「L サイズ」，「M サイズ」，または「S サイズ」から選択します。デフォルトでは「M サイズ」が指定されています。

  データベース容量の見積もり方法については「4.6.3　データベース容量の見積もり」を参照してください。

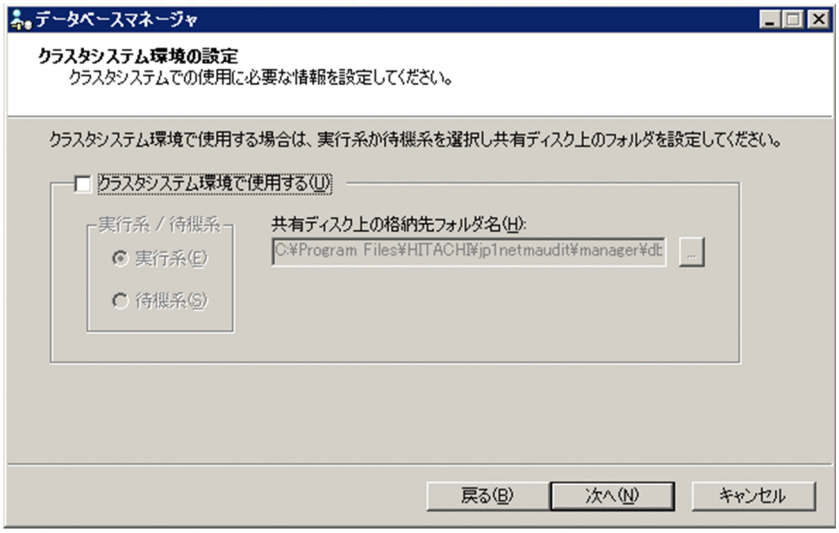
- 「データベース領域の格納先」

  「ローカルディスク上の格納先フォルダ名」に，データベースを格納するフォルダ名を指定します。100 バイト以内でパスを指定してください。デフォルトのフォルダパスは「JP1/Audit Management - Manager のインストール先フォルダ¥db¥rd」です。なお，［...］ボタンをクリックすると，フォルダを参照するダイアログからフォルダ名を指定できます。任意のローカルフォルダを指定してください。

7. [次へ] ボタンをクリックする。

次の図に示す［クラスタシステム環境の設定］画面が表示されます。監査ログ管理サーバをクラスタ環境で運用しない場合，この画面での設定は不要です。クラスタ環境で運用する場合は，「クラスタシステム環境で使用する」チェックボックスにチェックしてください。

図 5-10 ［クラスタシステム環境の設定］画面

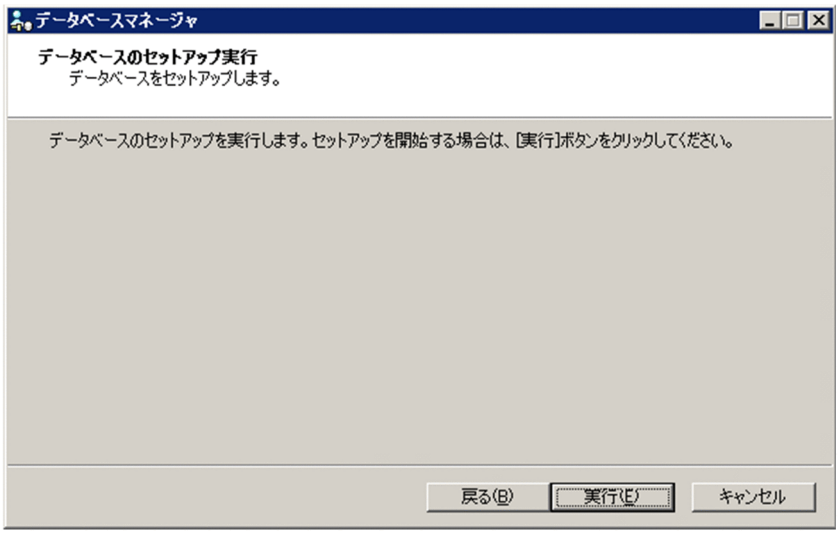


［クラスタシステム環境の設定］画面の詳細については「6.3.5　監査ログ管理サーバのデータベースをセットアップする（クラスタ環境）」を参照してください。

8. [次へ] ボタンをクリックする。

次の図に示す［データベースのセットアップ実行］画面が表示されます。

図 5-11 ［データベースのセットアップ実行］画面



9. [実行] ボタンをクリックする。

データベースがセットアップされます。セットアップが完了すると，完了を示すメッセージが表示されます。作成に失敗した場合はメッセージが表示されるので，メッセージの内容に従って対処してください。

5.5.8　監査ログ管理サーバのデータベースをアップグレードする

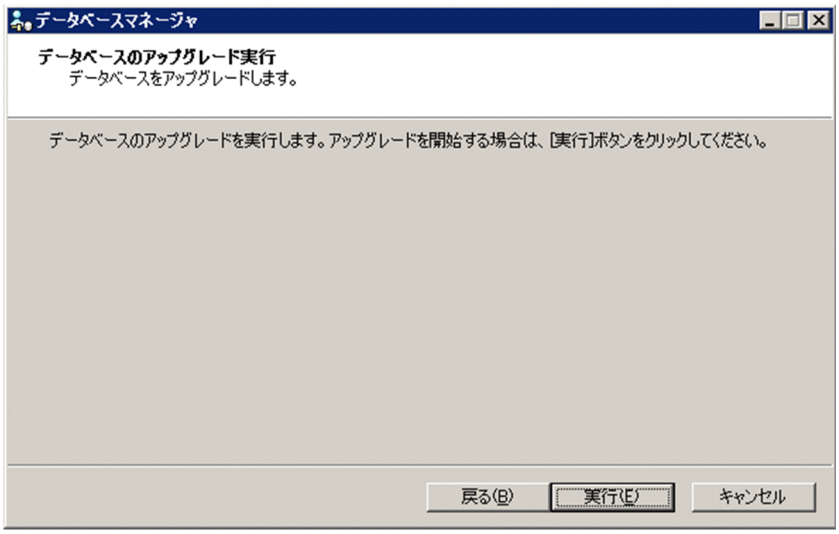
監査ログ管理サーバで JP1/Audit Management - Manager をバージョンアップした場合，監査ログ管理サーバのデータベースをアップグレードする必要があります。

アップグレードの手順を次に示します。

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［データベースマネージャ］を選択する。
   ［データベースマネージャ］ダイアログが表示されます。

2. 「データベースのアップグレード」を選択して，［次へ］ボタンをクリックする。
   次の図に示す［データベースのアップグレード実行］画面が表示されます。

   図 5-12　［データベースのアップグレード実行］画面



3. ［実行］ボタンをクリックする。
   データベースがアップグレードされます。

注意事項

アップグレード中にトラブルが発生した場合に備えて，アップグレード前に，データベースのバックアップを取得することをお勧めします。データベースのバックアップの取得方法については「10.1.3　データベースのバックアップ」を参照してください。なお，アップグレード完了後，アップグレード前に取得したデータベースのバックアップファイルを使用して，データベースへリストアしないでください。誤ってリストアすると，監査ログ管理画面を参照できなくなり，JP1/Audit Management - Manager のサービスの起動やコマンドを実行できなくなります。

5.6　監査ログ管理サーバで監査ログを収集するための設定

監査ログ管理サーバで監査ログを収集するための設定について説明します。

監査ログを収集するには，監査ログを収集したいサーバやプログラムを収集対象として設定する必要があります。

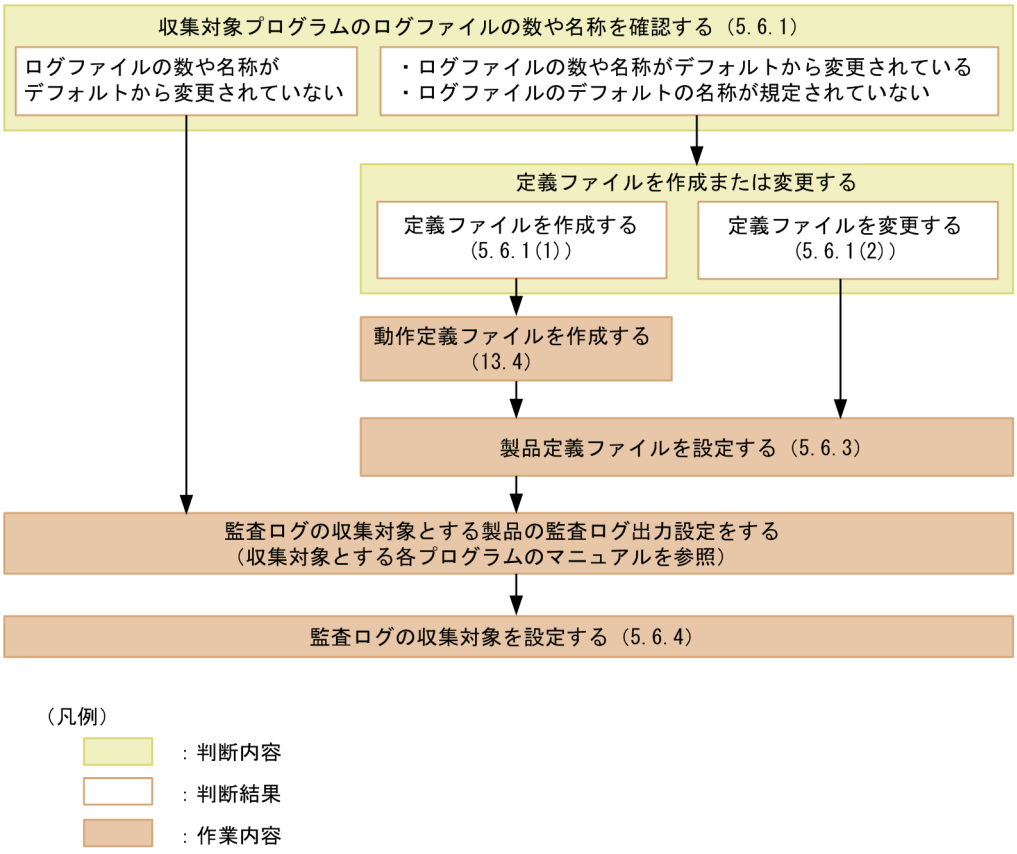
JP1/Audit Management - Manager で標準サポートしているプログラムかどうか，また，標準サポート外のプログラムの場合は正規化ルールをどのように定義するかなどによって，設定の流れが異なります。

収集対象サーバがクラスタ構成の場合に，物理ホストと論理ホストの両方で同じ製品を監視するときは，製品名（プログラム）を分けて定義してください。

JP1/Audit Management - Manager で標準サポートしているプログラムを収集する場合

この場合の設定の流れを次の図に示します。各項目の詳細については括弧内の個所を参照してください。

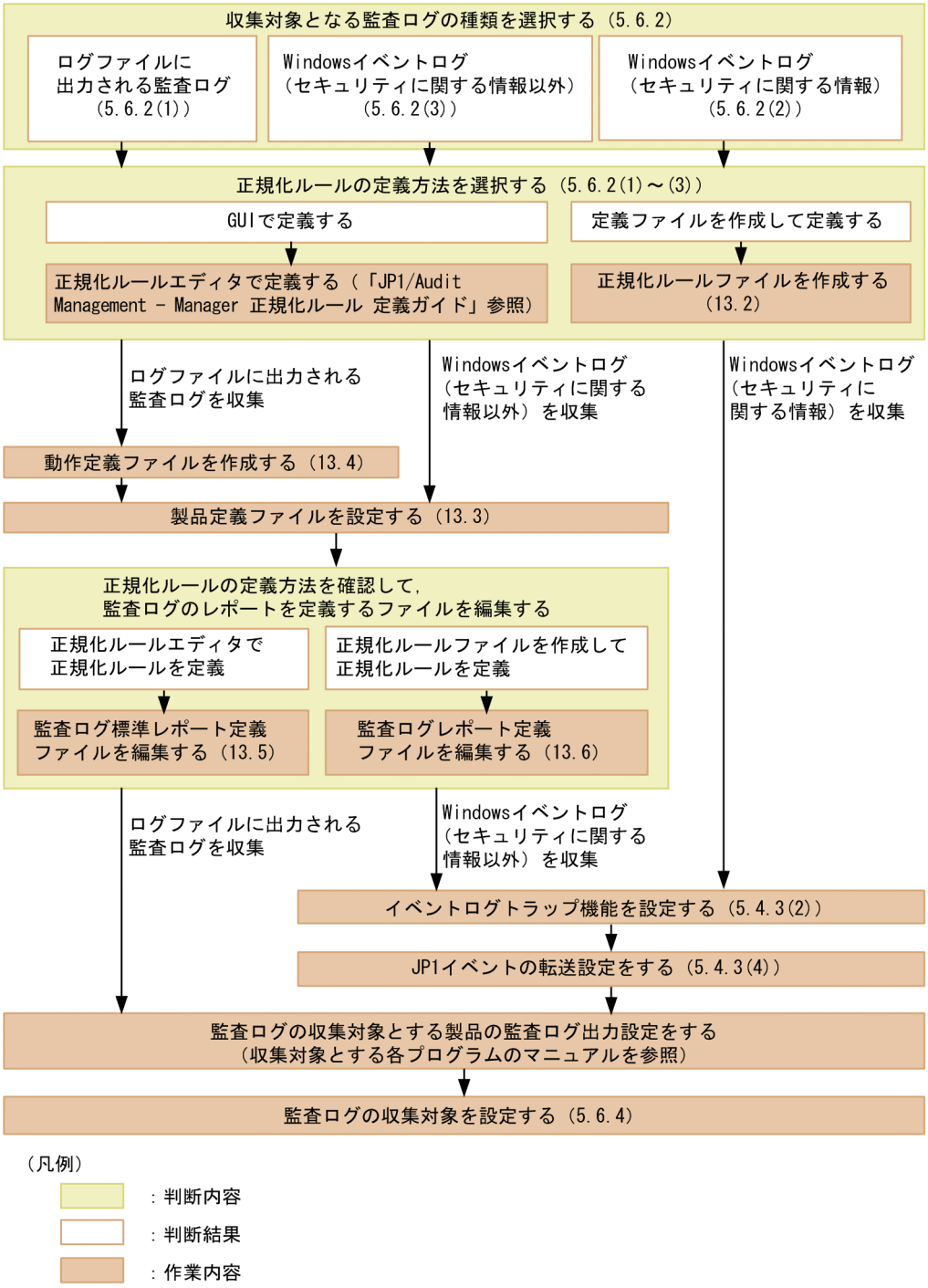
図 5-13　監査ログを収集するための設定の流れ（標準サポートしているプログラムの場合）



JP1/Audit Management - Manager で標準サポート外のプログラムを収集する場合

この場合の設定の流れを次の図に示します。各項目の詳細については括弧内の個所を参照してください。

図 5-14　監査ログを収集するための設定の流れ（標準サポート外のプログラムの場合）



5.6.1　標準サポートしているプログラムを収集対象とするための準備をする

JP1/Audit Management - Manager で標準サポートしているプログラムを収集対象とする場合で，次のどちらかの条件に該当するときは，JP1/Audit Management - Manager の定義ファイルを事前に手動で作成または変更する必要があります。

- ログファイルの数や名称がデフォルトと異なる場合

- ログファイルのデフォルトの名称が規定されていない場合

これらの条件に該当しない場合，ここでの作業は不要です。［収集対象の設定］ダイアログでの設定を実施してください。設定方法の詳細は「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

作成と変更のうち，どちらの方法を選択するかは任意です。ただし，複数の監査ログ収集対象サーバから同一プログラムの監査ログを収集する場合，監査ログ収集対象サーバ間でログファイル名を統一しておく必要があります。統一されていないと，監査ログ収集マネージャで「監視中」と表示されていても，監査ログは収集されません。また，上書きインストールを実施すると，既存の定義ファイルが上書きされます。したがって，新規で作成する方法をお勧めします。

定義ファイルを新規で作成する方法と変更する方法について，それぞれ次に説明します。

(1)　定義ファイルを新規で作成する

JP1/Audit Management - Manager の定義ファイルのうち，動作定義ファイルと製品定義ファイルを新規で作成します。ほかの定義ファイルの作成は不要です。

- **動作定義ファイルを作成する**

  動作定義ファイルの作成方法については「13.4　動作定義ファイル」を参照してください。ファイルの作成後は，所定の場所に動作定義ファイルを格納する必要があります。格納先については，表 5-33 を参照してください。

- **製品定義ファイルを作成する**

  製品定義ファイルは［製品定義一覧］ダイアログから［製品定義の編集］ダイアログを表示して作成します。製品定義ファイルの作成方法については「5.6.3　製品定義ファイルを設定する」を参照してください。

  なお，製品定義ファイルは動作定義ファイルの作成後に作成してください。

これらの定義ファイルの作成が完了したら，監査ログ収集対象プログラムで監査ログを出力させる設定を実施します。設定の詳細は，各プログラムのマニュアルを参照してください。

監査ログ収集対象プログラムでの設定が完了したら，JP1/Audit Management - Manager の［収集対象の設定］ダイアログでの設定を実施します。設定方法の詳細は「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

(2)　定義ファイルを変更する

JP1/Audit Management - Manager の定義ファイルのうち，製品定義ファイルを変更します。製品定義ファイルの定義内容のうち，AuditLogNum（ログファイル数）と AuditLogName（ログファイル名）が変更の対象となります。ほかの定義内容の変更は不要です。

- **ログファイル数がデフォルトと異なる場合**

ログファイル数がデフォルトと異なる場合は，製品定義ファイルの AuditLogNum（ログファイル数）と AuditLogName（ログファイル名）を変更する必要があります。

この場合の製品定義ファイルの変更手順について説明します。

なお，監査ログ収集マネージャで収集対象を監視中の場合は，すべての監査ログ収集対象サーバの監視を停止してから製品定義ファイルを変更してください。

1. すべての監査ログ収集対象サーバ上で収集対象プログラムのログファイル数を変更する。

   各収集対象プログラムの設定方法に従って，ログファイル数を変更します。設定方法の詳細については，各プログラムのマニュアルを参照してください。

2. 製品定義ファイルを変更する。

   テキストエディタで製品定義ファイルを開き，AuditLogNum（ログファイル数）と AuditLogName（ログファイル名）の値を編集します。製品定義ファイルの詳細については「13.3　製品定義ファイル」を参照してください。

   Cosminexus のログファイル数を 4 個から 5 個に変更する場合の製品定義ファイル（Cosminexus.conf）の変更例について次に示します。

   変更前

```
AuditLogNum=4
AuditLogName=audit1.log
AuditLogName=audit2.log
AuditLogName=audit3.log
AuditLogName=audit4.log
RegularPattern=admrglrule_AdmConvert.conf
ReadOnly=1
```

   変更後

```
AuditLogNum=5 #4から5に変更する。
AuditLogName=audit1.log
AuditLogName=audit2.log
AuditLogName=audit3.log
AuditLogName=audit4.log
AuditLogName=audit5.log #この行を追加する。
RegularPattern=admrglrule_AdmConvert.conf
ReadOnly=1
```

製品定義ファイルの変更が完了したら，監査ログ収集マネージャで収集対象の監視を開始してください。変更後のログファイル数が反映された状態で収集対象が監視されるようになります。

- **ログファイル名がデフォルトと異なる場合，またはログファイル名がデフォルトで規定されていない場合**

  ログファイル名がデフォルトと異なる場合は，製品定義ファイルのログファイル名（AuditLogName）を変更する必要があります。

この場合の製品定義ファイルの変更手順について説明します。なお，監査ログ収集マネージャで収集対象を監視中の場合は，すべての監査ログ収集対象サーバの監視を停止してから製品定義ファイルを変更してください。

1. すべての監査ログ収集対象サーバ上で収集対象プログラムのログファイル名を変更する。

   各収集対象プログラムの設定方法に従って，ログファイル名を変更します。設定方法の詳細については，各プログラムのマニュアルを参照してください。

2. 製品定義ファイルを変更する。

   テキストエディタで製品定義ファイルを開き，ログファイル名（AuditLogName）の値を編集します。製品定義ファイルの詳細については「13.3　製品定義ファイル」を参照してください。

   JP1/AJS2 のログファイル名を ajs-log1.log と ajs-log2.log から schedule1.log と schedule2.log に変更する場合の製品定義ファイル（JP1_AJS2.conf）の変更例について次に示します。

   変更前

```
AuditLogNum=2
AuditLogName=ajs-log1.log
AuditLogName=ajs-log2.log
RegularPattern=admrglrule_JP1_AJS2.conf
ReadOnly=1
```

   変更後

```
AuditLogNum=2
AuditLogName=schedule1.log #この行を変更する。
AuditLogName=schedule2.log #この行を変更する。
RegularPattern=admrglrule_JP1_AJS2.conf
ReadOnly=1
```

製品定義ファイルの変更が完了したら，監査ログ収集マネージャで収集対象の監視を開始してください。変更後のログファイル名が反映された状態で収集対象が監視されるようになります。

5.6.2　標準サポート外のプログラムを収集対象とするための準備をする

JP1/Audit Management - Manager で標準サポート外となっているプログラムを収集対象として設定する場合に，事前に定義する内容について説明します。標準サポートしているプログラムの監査ログだけを収集する場合，この作業は不要です。

定義内容は，次に示す監査ログの種類によって異なります。

- ログファイルに出力される監査ログ
- Windows イベントログ（セキュリティに関する情報）
- Windows イベントログ（セキュリティに関する情報以外）

(1) ログファイルに出力される監査ログを収集する場合

ログファイルに出力される監査ログを収集する場合の定義内容について説明します。

まず，収集したいログが監査証跡管理システムで収集できる条件に該当するかどうかを判断します。判断方法の詳細は「4.3.1　正規化ルールで定義できる監査ログの条件」を参照してください。収集できることが判断できたら，それぞれの定義ファイルを定義します。

- **正規化ルールを定義する**

  正規化ルールの定義方法には，次の二つの方法があります。

  正規化ルールエディタで定義する

  ［正規化ルールエディタ］ダイアログで定義します。定義方法については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

  正規化ルールファイルを定義する

  正規化ルールファイルの定義内容については「13.2　正規化ルールファイル」を参照してください。ファイルの作成後，所定の場所に正規化ルールファイルを格納する必要があります。格納先については，表 5-33 を参照してください。

- **動作定義ファイルを作成する**

  動作定義ファイルの作成方法については「13.4　動作定義ファイル」を参照してください。ファイルの作成後，所定の場所に動作定義ファイルを格納する必要があります。格納先については，表 5-33 を参照してください。

- **製品定義ファイルを作成する**

  製品定義ファイルは［製品定義一覧］ダイアログから［製品定義の編集］ダイアログを表示して作成します。製品定義ファイルの作成方法については「5.6.3　製品定義ファイルを設定する」を参照してください。

  なお，製品定義ファイルは動作定義ファイルの作成後に作成してください。

- **監査ログ標準レポート定義ファイルを編集する**

  正規化ルールエディタで正規化ルールを定義した場合に編集する必要があります。

  監査ログ標準レポート定義ファイルの編集方法については「13.5　監査ログ標準レポート定義ファイル」を参照してください。

- **監査ログレポート定義ファイルを編集する**

  正規化ルールファイルで正規化ルールを定義した場合に編集する必要があります。

  監査ログレポート定義ファイルの編集方法については「13.6　監査ログレポート定義ファイル」を参照してください。

それぞれの定義ファイルの格納場所を次の表に示します。

表 5-33　定義ファイルの格納先

項番	定義ファイル名	格納先
1	正規化ルールファイル	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥rule
2	動作定義ファイル	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥logdef
3	製品定義ファイル	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥product※
4	監査ログ標準レポート定義ファイル	JP1/Audit Management - Manager の仮想ディレクトリ¥conf
5	監査ログレポート定義ファイル	

注※

監査ログ収集マネージャの［製品定義の編集］ダイアログで作成した製品定義ファイルは，自動的にこの格納先に格納されます。

これらの定義が完了したら，監査ログ収集対象プログラムで監査ログを出力させる設定を実施します。設定の詳細は，各プログラムのマニュアルを参照してください。

監査ログ収集対象プログラムでの設定が完了したら，JP1/Audit Management - Manager の［収集対象の設定］ダイアログでの設定を実施します。設定方法の詳細は「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

(2)　Windows イベントログ（セキュリティに関する情報）を収集する場合

Windows イベントログ（セキュリティに関する情報）を収集する場合の定義内容について説明します。

まず，対象となるイベント ID のメッセージフォーマットを調査し，収集したい Windows イベントログ（セキュリティに関する情報）が監査証跡管理システムで収集できるかどうかを判断します。

OS が Windows Server 2012 または Windows Server 2008 の場合は，正規化ルールエディタを使用して変換できるかどうか，Windows Server 2012 および Windows Server 2008 以外の場合は，正規化ルールファイルを使用して変換できるかどうかを判断してください。

- **正規化ルールを定義する**

  対象となるイベント ID のメッセージを監査ログとして収集するための正規化ルールを定義します。Windows Server 2012 または Windows Server 2008 と Windows Server 2012 および Windows Server 2008 以外で定義方法が異なります。

  Windows Server 2012 または Windows Server 2008 の場合

  必ず正規化ルールエディタを使用して正規化ルールを定義してください。正規化ルールファイルでの定義はできません。

  定義方法については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

Windows Server 2012 または Windows Server 2008 以外の場合

必ず正規化ルールファイルを編集して正規化ルールを定義してください。編集対象となるファイルは，admrglrule_WinEventLog_Security.conf です。正規化ルールエディタでの定義はできません。

定義内容の詳細については「13.2　正規化ルールファイル」を参照してください。

なお，ファイルの作成後，所定の場所に正規化ルールファイルを格納する必要があります。格納先については，表 5-33 を参照してください。

- **イベントログトラップ機能を設定する**

  Windows イベントログ（セキュリティに関する情報）に出力されるログを収集するために，JP1/Base の動作定義ファイルでイベントログトラップ機能を設定します。

  動作定義ファイル（ntevent.conf）の設定方法については「5.4.3(2)　JP1/Base の動作定義ファイル（ntevent.conf）を編集する」を参照してください。

- **JP1 イベントの転送設定をする**

  監査ログ収集対象サーバのイベントサーバで収集したイベントログを監査ログ専用イベントサーバへ転送させる設定をします。

  転送設定ファイル（forward ファイル）の設定方法については「5.4.3(4)　イベントログトラップ機能の転送設定ファイル（forward ファイル）を編集する」を参照してください。

これらの定義が完了したら，JP1/Audit Management - Manager の［収集対象の設定］ダイアログでの設定を実施します。設定方法の詳細は「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

(3)　Windows イベントログ（セキュリティに関する情報以外）を収集する場合

Windows イベントログ（セキュリティに関する情報以外）を収集する場合の定義内容について説明します。

まず，対象となるイベント ID のメッセージフォーマットを調査し，収集したい Windows イベントログが監査証跡管理システムで収集できるかどうかを判断します。

- **正規化ルールを定義する**

  対象となるイベント ID のメッセージを監査ログとして収集するために正規化ルールを定義します。正規化ルールは［正規化ルールエディタ］ダイアログで定義します。定義方法については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

- **製品定義ファイルを作成する**

  製品定義ファイルは［製品定義一覧］ダイアログから［製品定義の編集］ダイアログを表示して作成します。製品定義ファイルの作成方法については「5.6.3　製品定義ファイルを設定する」を参照してください。

- **監査ログ標準レポート定義ファイルを編集する**

  正規化ルールエディタで正規化ルールを定義した場合に編集する必要があります。

監査ログ標準レポート定義ファイルの編集方法については「13.5　監査ログ標準レポート定義ファイル」を参照してください。

- **監査ログレポート定義ファイルを編集する**

  正規化ルールファイルで正規化ルールを定義した場合に編集する必要があります。

  監査ログレポート定義ファイルの編集方法については「13.6　監査ログレポート定義ファイル」を参照してください。

- **イベントログトラップ機能を設定する**

  Windows イベントログ（セキュリティに関する情報以外）に出力されるログを収集するために，JP1/Base の動作定義ファイルでイベントログトラップ機能を設定します。

  動作定義ファイル（ntevent.conf）の設定方法については「5.4.3(2)　JP1/Base の動作定義ファイル（ntevent.conf）を編集する」を参照してください。

- **JP1 イベントの転送設定をする**

  監査ログ収集対象サーバのイベントサーバで収集したイベントログを監査ログ専用イベントサーバへ転送させる設定をします。

  転送設定ファイル（forward ファイル）の設定方法については「5.4.3(4)　イベントログトラップ機能の転送設定ファイル（forward ファイル）を編集する」を参照してください。

これらの定義が完了したら，JP1/Audit Management - Manager の［収集対象の設定］ダイアログでの設定を実施します。設定方法の詳細は「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

5.6.3　製品定義ファイルを設定する

製品定義ファイルの設定は，［製品定義一覧］ダイアログから［製品定義の編集］ダイアログを表示して実施します。

なお，この作業は，正規化ルールの定義および動作定義ファイルの作成後に実施してください。

(1)　製品定義ファイルの設定手順

製品定義ファイルの作成手順を次に示します。

1. **［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。**

   ［監査ログ収集マネージャ］ウィンドウが表示されます。

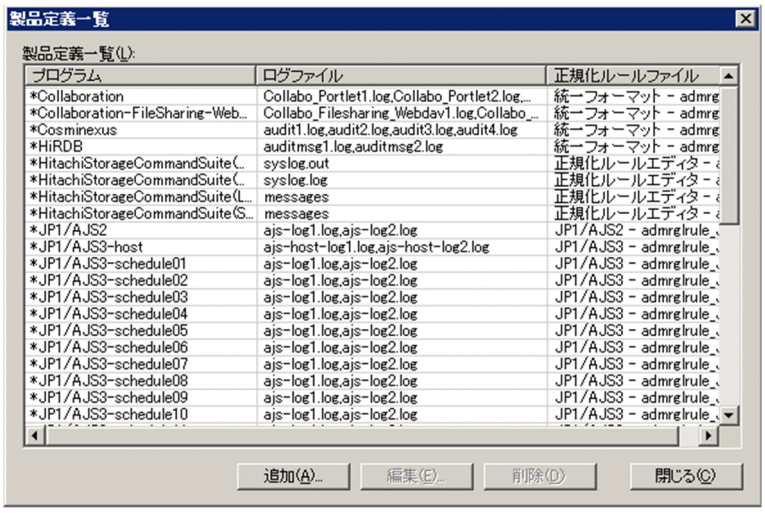
2. **［操作］－［製品定義一覧］を選択する。**

   次の図に示す［製品定義一覧］ダイアログが表示されます。

「プログラム」に表示されるプログラムのうち，「*」が表示されるプログラムは，JP1/Audit Management - Manager で標準サポートしているプログラムです。なお，UNIX システムログの場合，プログラム名は「*UNIX System Log」と表示されます。

また，JP1/Audit Management - Manager で標準サポートしている，Windows イベントログにログが出力されるプログラムは，プログラム名が表示されません。

図 5-15 ［製品定義一覧］ダイアログ

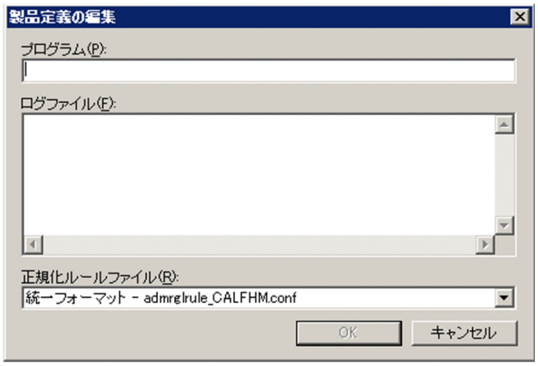


なお，「 」ボタンをクリックしても，同様の操作ができます。

3. ［追加］ボタンをクリックする。

次の図に示す［製品定義の編集］ダイアログが表示されます。

図 5-16 ［製品定義の編集］ダイアログ



4. ［製品定義の編集］ダイアログで，使用する環境に合わせて項目を入力する。

入力後に［OK］ボタンをクリックすると，入力した内容が［製品定義一覧］ダイアログに反映されます。設定内容については「(2) ［製品定義の編集］ダイアログの設定内容」を参照してください。

すでに作成した製品定義ファイルを，編集したり，削除したりすることもできます。製品定義ファイルを編集する方法については「9.3.9 作成した製品定義ファイルを編集する」を参照してください。また，製品定義ファイルを削除する方法については「9.3.10 作成した製品定義ファイルを削除する」を参照してください。

ここで定義したプログラムの監査ログを監視したい場合は，これらの手順を実施したあとに収集対象として設定する必要があります。収集対象として設定する方法については「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

(2)　［製品定義の編集］ダイアログの設定内容

［製品定義の編集］ダイアログで設定する項目を次の表に示します。

表 5-34　［製品定義の編集］ダイアログの設定内容

項番	項目	説明	設定値	デフォルト値
1	プログラム※	監査ログを出力する収集対象プログラム名を入力します。 入力規則は監査ログの出力形式によって，次のように異なります。 **ログファイルに出力される形式の場合** 動作定義ファイル名から「admjevlog_」および「.conf」を除いた名称を入力してください。 なお，「/」を入力すると「_」に置換されます。 **Windows イベントログに出力される形式の場合** 「WinEventLog_」のあとにイベントソース名を付けた名称を入力してください。また，イベントソース名に「/」または「△（半角スペース）」を含む場合は，「_」に置換して入力してください。	64 バイト以内の文字列を設定します。 使用できる文字を次に示します。1 文字目は必ず半角英数字にしてください。 • 半角英数字 • 「!」「#」「$」「&」「(」「)」「+」「,」「-」「/」「;」「=」「@」「[」「]」「_」「`」「{」「}」「~」	なし
2	ログファイル	監査ログのファイル名を入力します。 複数のファイルを指定できます。複数のファイルを指定する場合は，ファイルごとに改行してください。また，同一ファイル名は指定できません。 なお，監査ログの出力形式が Windows イベントログに出力される形式の場合，この項目は非活性となります。	1 行当たり 64 バイト以内の文字列を設定します。32 行設定できます。 使用できる文字を次に示します。 • 半角英数字 • 「!」「#」「$」「&」「(」「)」「+」「-」「.」「;」「=」「@」「[」「]」「_」「`」「{」「}」「~」	なし
3	正規化ルールファイル	正規化ルールファイルの統一フォーマットを設定します。	プルダウンメニューに「JP1/Audit Management - Manager のインストール先フォルダ¥conf¥rule」フォルダ内のファイルが表示されます。	統一フォーマット - admrglrule_CALFHM.conf

項番	項目	説明	設定値	デフォルト値
			統一フォーマット，JP1/AJS2 および JP1/AJS3 は次のように表示されます。 **統一フォーマット（admrglrule_CALFHM.conf）の場合** 「統一フォーマット - admrglrule_CALFHM.conf」 **JP1/AJS2（admrglrule_JP1_AJS2.conf）の場合** 「JP1/AJS2 - admrglrule_JP1_AJS2.conf」 **JP1/AJS3（admrglrule_JP1_AJS3.conf）の場合** 「JP1/AJS3 - admrglrule_JP1_AJS3.conf」 **正規化ルールエディタで定義したプログラム（admrglrule_AdmConvert.conf）の場合** 「正規化ルールエディタ - admrglrule_AdmConvert.conf」	

注※

正規化ルールエディタで正規化ルールを定義した場合，「プログラム」に入力する内容は製品情報のプロダクト名と一致させてください。製品情報の詳細については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

5.6.4 JP1/Audit Management - Manager で監査ログの収集対象を設定する

監査ログ管理サーバで，監査ログの収集対象を設定します。

収集対象となるプログラムや監査ログおよびログファイルの格納先フォルダなどを設定します。

監査ログの収集対象についての設定は，［監査ログ収集マネージャ］ウィンドウから［収集対象の設定］ダイアログを表示して実施します。

ただし，JP1/Audit Management - Manager で標準サポート外となっているプログラムを収集対象とする場合は，事前に収集対象として設定するための準備が必要です。収集対象とするための準備内容については「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。

なお，ログファイルがラップアラウンド形式の場合は，収集対象のログファイル面数に合わせて設定を変更してください。

注意事項

収集対象サーバがクラスタ構成の場合に，物理ホストと論理ホストの両方で同じ製品を監視するときは，製品名（プログラム）を分けて定義してください。

例えば，監視対象のプログラムが JP1/Base の場合，製品名を「JP1/Base」と「JP1/Base2」に分けて定義します。この場合に使用する製品定義ファイルと動作定義ファイルを次に示します。

物理ホスト

- 標準提供の JP1/Base 用の製品定義ファイル（JP1_Base.conf）を使用する。
- 標準提供の JP1/Base 用の動作定義ファイル（admjevlog_JP1_Base.conf）を使用する。

論理ホスト

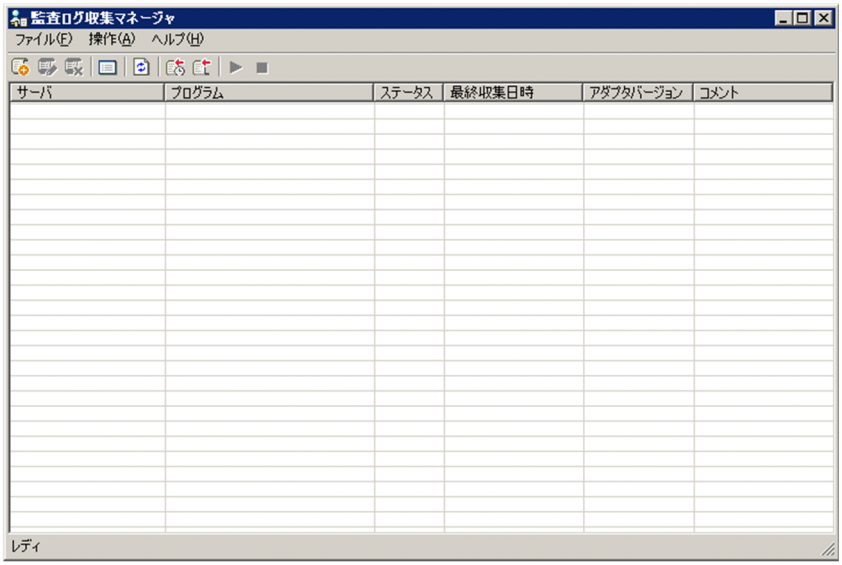
- JP1_Base.conf をコピーして，ファイル名を JP1_Base2.conf に変更して使用する。
- admjevlog_JP1_Base.conf をコピーして，ファイル名を admjevlog_JP1_Base2.conf に変更して使用する。

(1) 収集対象の設定の手順

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。

   次の図に示す［監査ログ収集マネージャ］ウィンドウが表示されます。

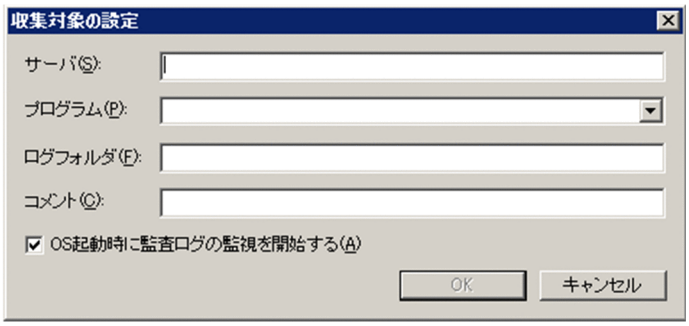
   図 5-17 ［監査ログ収集マネージャ］ウィンドウ



2. [操作] − [収集対象] − [追加] を選択する。

次に示す［収集対象の設定］ダイアログが表示されます。

図 5-18 ［収集対象の設定］ダイアログ



なお，「 」ボタンをクリックしても，同様の操作ができます。

3. [収集対象の設定] ダイアログで，使用する環境に合わせて値を設定する。

設定内容については「(2) ［収集対象の設定］ダイアログの設定内容」を参照してください。

4. [OK] ボタンをクリックする。

監査ログファイルについての設定が登録され，［監査ログ収集マネージャ］ウィンドウに反映されます。複数の収集対象を追加する場合は，手順 2～手順 4 を繰り返してください。

5. JP1/Audit Management - Manager のサービスを再起動する。

収集対象を追加した場合，JP1/Audit Management - Manager のサービスを再起動する必要があります。再起動するサービスの詳細は「5.7.1 監査ログ管理サーバを開始する」を参照してください。

6. [監査ログ収集マネージャ] ウィンドウに表示された項目から，監視を開始したい収集対象を選択し，[操作] − [監査ログの監視] − [開始] を選択する。

選択した監査ログ収集対象に対応するログファイルトラップ機能が起動され，監査ログの監視を開始します。複数の収集対象を一度に選択して，監視を開始することもできます。

また，収集対象サーバの起動時に，監査ログの監視を自動的に開始するよう設定することもできます。

なお，監視の開始後に出力された監査ログが収集対象となります。

監査ログの収集は，監査ログ収集対象サーバの監査ログ専用イベントデータベースに格納されているすべてのデータが対象になります。

(2) ［収集対象の設定］ダイアログの設定内容

［収集対象の設定］ダイアログで設定する項目を次の表に示します。

表 5-35 ［収集対象の設定］ダイアログの設定内容

項番	項目	説明	設定値	デフォルト値	必須
1	サーバ	監査ログ収集対象サーバのホスト名を指定します。クラスタ環境で共有ディスク上の監査ログを収集する場合は，監査ログ収集対象サーバの論理ホスト名を指定します。 設定時は次に示すことに注意してください。 • IP アドレスでは指定できない • 指定したサーバ名の大文字・小文字は区別される	64 バイト以内の文字列を設定します。 使用できる文字を次に示します。 • 半角英数字 • 「-」「_」「.」	なし	○
2	プログラム	収集対象の監査ログを出力するプログラムの名称を指定します。	プルダウンメニューからプログラムの名称を選択します。※1 指定するプログラムが標準サポート外で，かつログがファイルに出力される場合，製品定義ファイル名から拡張子「.conf」が除かれ，かつ「_」が「/」に置換された名称がプログラム名として表示されます。また，ログが Windows イベントログに出力される場合，製品定義ファイル名から拡張子「.conf」が除かれた名称がプログラム名として表示されます。 収集対象となるプログラムのログが Windows イベントログに出力される場合または OS が UNIX の場合は，次のように表示されます。 • Hitachi Storage Command Suite または Hitachi Command Suite の場合 「HitachiStorageCommandSuite（Windows イベントログ)」※2 「HitachiStorageCommandSuiteV8 (Windows イベントログ)」※2 「HitachiStorageCommandSuite（HP-UX)」※2 「HitachiStorageCommandSuite（Solaris)」※2 「HitachiStorageCommandSuite（AIX)」※2 「HitachiStorageCommandSuite（Linux)」※2 • Oracle の場合 「Oracle（Windows イベントログ)」※3 • UNIX の場合 「UNIX System Log」※4 • Windows Server 2003 または Windows XP の場合 「Windows イベントログ（セキュリティ)」※5 • Windows Server 2008 または Windows Server 2012 の場合	なし	○

項番	項目	説明	設定値	デフォルト値	必須
			「Windows2008 イベントログ（セキュリティ）」※5 なお，標準サポートしているプログラムで，実際のログファイル名と製品定義ファイルで指定されているファイル名が一致していない場合，製品定義ファイルの設定を変更する必要があります。 設定方法の詳細については「5.6.1　標準サポートしているプログラムを収集対象とするための準備をする」を参照してください。		
3	ログフォルダ	収集対象の監査ログの格納先を指定します。 「プログラム」に指定したプログラムの監査ログが出力されるフォルダをフルパスで指定します。監査ログの出力先が共有ディスク上なのかローカルディスク上なのかによって，正しい出力先を指定してください。	255 バイト以内の文字列を設定します。 指定したフォルダ下に出力される監査ログファイルのフルパスが 256 バイト以内になるように指定してください。 使用できる文字を次に示します。 Windows の場合 ・半角英数字 ・「△（半角スペース）」「!」「#」「$」「&」「(」「)」「+」「,」「-」「.」「;」「=」「@」「[」「]」「¥」「_」「`」「{」「}」「~」 UNIX の場合 ・半角英数字 ・「△（半角スペース）」「!」「#」「$」「&」「(」「)」「+」「,」「-」「.」「/」「;」「=」「@」「[」「]」「_」「`」「{」「}」「~」	なし	○
4	コメント	コメントを入力できます。それぞれの項目を識別するための情報などを必要に応じて記入してください。	255 バイト以内の文字列を設定します。	なし	△
5	OS 起動時に監査ログの監視を開始する	監査ログ収集対象サーバの OS が起動した時点で，収集対象の監査ログの監視を開始するかどうかを指定します。 この項目をチェックした場合，監査ログ収集対象サーバの JP1/Base の起動順序定義ファイル（**JP1/Base のインストール先フォルダ**¥conf¥boot¥Jp1svprm.dat）に，監査ログの監視を開始するログファイルトラップ機能の起動設定が追加されます。※6 ただし，ログファイルトラップ機能の起動設定を追加した時点では，監査ログの監視は開始されません。すぐに監視を開始したい場合は，手動で監査ログの監視を開始する必要があります。監査ログの監視を開始する方法につい	監査ログの監視を開始する場合は，チェックボックスにチェックします。	ON	△

項番	項目	説明	設定値	デフォルト値	必須
		ては「9.3.4　監査ログの監視を開始する」を参照してください。 なお，次の場合はチェックボックスが非活性となり，OS 起動時に監査ログの監視は開始されません。 • 監査ログ収集対象サーバの OS が UNIX の場合※7 • Windows イベントログに出力されるログを収集対象とする場合 また，「サーバ」で監査ログ収集対象サーバの論理ホスト名を指定している場合は，この項目のチェックの有無にかかわらず，OS 起動時に監査ログの監視は開始されません。※8			

（凡例）

○：必ず設定する

△：必要に応じて設定する

注※1

プログラムによっては，収集する監査ログごとに対応するプログラムの名称が異なります。また，JP1/AJS3 の場合は物理・論理ホストまたはスケジューラサービスごとにスケジューラログが出力されます。このため，それぞれのホストやスケジューラサービスを一つの収集対象として追加する必要があります。

収集する監査ログと，それに対応するプログラムの名称を次の表に示します。

表 5-36　収集する監査ログと，それに対応するプログラムの名称

項番	収集する監査ログ		対応するプログラムの名称
1	JP1/Audit Management - Manager（サーバ）の操作に関する監査ログ		「JP1/NETM/Audit-Manager」
2	JP1/Audit Management - Manager の監査ログ管理画面（Web）の操作に関する監査ログ		「JP1/NETM/Audit-ManagerWeb」
3	JP1/ITDM2 の監査ログ	Manager の監査ログ	「JP1/ITDM2」
		Manager のリモートインストールマネージャを使用した配布機能の監査ログ	「JP1/ITDM2-DM」
		Agent のリモートインストールマネージャを使用した配布機能の監査ログ	「JP1/ITDM2-DMClient」
		Asset Console の監査ログ	「JP1/ITDM2-AC」

項番	収集する監査ログ		対応するプログラムの名称
4	JP1/NETM/DM の監査ログ	JP1/NETM/DM Manager がインストールされている場合	「JP1/NETM/DM-Manager」
		JP1/NETM/DM Client（または JP1/NETM/DM Client - Base）がインストールされている場合	「JP1/NETM/DM-Client」
		JP1/NETM/DM Client（または JP1/NETM/DM Client - Base）と JP1/NETM/DM Manager が同一マシンにインストールされている場合	「JP1/NETM/DM」
5	JP1/AJS3 の物理ホストや論理ホストの監査ログ		「JP1/AJS3-host」
6	JP1/AJS3 のスケジューラサービスの監査ログ		「JP1/AJS3-schedule01」～「JP1/AJS3-schedule20」
7	Collaboration のポートレット操作に関する監査ログ，およびコマンド実行に関する監査ログ		「Collaboration」
8	Collaboration の Web フォルダの操作に関する監査ログ		「Collaboration-FileSharing-Webdav」

注※2

Hitachi Storage Command Suite または Hitachi Command Suite のログを監査ログとして収集したい場合に，それぞれの OS ごとに次のプログラムの名称を選択してください。

- Windows かつ Hitachi Command Suite 7 以前の場合：「HitachiStorageCommandSuite（Windows イベントログ）」
- Windows かつ Hitachi Command Suite 8 の場合：「HitachiStorageCommandSuiteV8（Windows イベントログ）」
- HP-UX の場合：「HitachiStorageCommandSuite（HP-UX）」
- Solaris の場合：「HitachiStorageCommandSuite（Solaris）」
- AIX の場合：「HitachiStorageCommandSuite（AIX）」
- Linux の場合：「HitachiStorageCommandSuite（Linux）」

注※3

Oracle のログを監査ログとして収集したい場合に選択してください。

注※4

UNIX システムログを監査ログとして収集したい場合に選択してください。

注※5

Windows イベントログ（セキュリティに関する情報）を監査ログとして収集したい場合に選択してください。なお，Windows Server 2012 または Windows Server 2008 と Windows Server 2012 または Windows Server 2008 以外（Windows Server 2003 または Windows XP）は区別して選択してください。

注※6

起動順序定義ファイルの［Command］セクションの「ReadyCommand」キーにすでにほかの登録がある場合は設定されません。このような場合は，「ReadyCommand」キーにすでに登録されているバッチファイルに，次に示すバッチファイルを呼び出す処理を追加することで，OS 起動時に監査ログの監視を自動的に開始できます。同じログが重複して収集される場合があるため，OS 起動後にバッチファイルを手動で起動しないでください。

JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合

```
システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥agent¥bin¥admlogtrap.bat
```

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合

```
システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥manager¥bin¥admlogtrap.bat
```

このバッチファイルを呼び出す際は，引数「-y」が必要です。すでに登録されているバッチファイルに追加する処理の記述例を次に示します。

```
call ”システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥agent¥bin¥admlogtrap.bat” -y
```

起動順序定義ファイルについての詳細は，マニュアル「JP1/Base 運用ガイド」を参照してください。

注※7

「ログフォルダ」で指定したパスの先頭が「/」になっている場合，監査ログ収集対象サーバの OS は UNIX であると判断されます。

監査ログ収集対象サーバの OS が UNIX の場合，OS 起動時に自動的に監視を開始するには，収集対象の監視を開始時，次に示すディレクトリに出力されるスクリプト（拡張子が「.sh」のファイル）を実行するように設定します。同じログが重複して収集される場合があるため，OS 起動後にスクリプトを手動で起動しないでください。

JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合

```
/opt/jp1netmaudit/agent/bin
```

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合

```
/opt/jp1netmaudit/manager/bin
```

このディレクトリには，収集対象として設定したプログラムごとにスクリプトファイルが出力されます。このスクリプトファイルを OS 起動時に実行させるには，自動開始用のスクリプトファイルを作成する必要があります。自動開始用のスクリプトファイルは，JP1/Base と監査ログ専用イベントサービスの起動後に実行されるように設定してください。設定方法の詳細は，各 OS のマニュアルを参照してください。

自動開始用のスクリプトファイルを作成するときの注意事項を次に示します。

- 監視の開始時，プログラムごとに出力されるスクリプトファイルを実行する際は，引数「-y」を指定してください。
- プログラムごとに出力されるスクリプトファイルは，プログラムの監視を停止すると削除されます。このため，監視を停止している状態で OS を再起動すると，スクリプトファイルが存在しません。

スクリプトファイルを実行する際は，スクリプトファイルが存在しているかどうかを確認してください。

注※8

「サーバ」で監査ログ収集対象サーバの論理ホスト名を指定した場合，OS 起動時に自動的に監視を開始するには，JP1/Base の起動後に，クラスタソフトに登録したリソースまたはコマンドをオンラインにするように設定します。リソースまたはコマンドの詳細については「6.8.1　監査ログ収集対象サーバを開始する（クラスタ環境）」を参照してください。

なお，OS 起動時に監査ログの監視を自動的に開始するように設定しない場合，OS を再起動するたびに［監査ログ収集マネージャ］ウィンドウから手動で監査ログの監視を開始する必要があります。

5.6.5　監査ログを定期的に収集する

設定した収集対象の監査ログを収集する曜日や時刻などを設定します。この設定によって，定期的に監査ログを収集できるようになります。

監査ログを収集する曜日や時刻の設定は，［監査ログ収集マネージャ］ウィンドウから［定時収集の設定］ダイアログを表示して実施します。

監査ログを定期的に収集するための設定手順を次に示します。

(1)　監査ログを定時収集するための設定手順

監査ログを定時収集するための設定手順を次に示します。

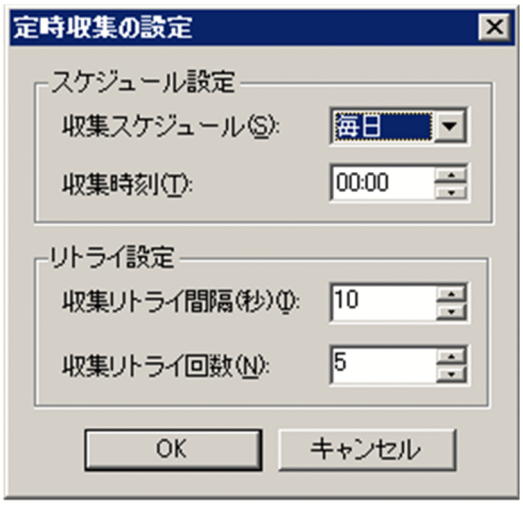
1. **［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。**

   ［監査ログ収集マネージャ］ウィンドウが表示されます。

2. **［操作］－［監査ログの収集］－［定時収集］を選択する。**

   次の図に示す［定時収集の設定］ダイアログが表示されます。

図 5-19　[定時収集の設定] ダイアログ



なお，「 」ボタンをクリックしても，同様の操作ができます。

3. [定時収集の設定] ダイアログで必要な情報を設定する。

   設定内容については「(2) [定時収集の設定] ダイアログの設定内容」を参照してください。

4. [OK] ボタンをクリックする。

   設定された収集対象に対して，設定した時間に監査ログの収集を開始します。

   収集対象の設定については「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

なお，監査ログの収集は，定期的に収集するだけでなく，必要に応じて即時に収集することもできます。即時に収集する方法については「9.3.7　監査ログを即時に収集する」を参照してください。

(2)　[定時収集の設定] ダイアログの設定内容

[定時収集の設定] ダイアログで設定する項目を次の表に示します。

表 5-37　[定時収集の設定] ダイアログの設定内容

項番	項目	説明	設定値	デフォルト値
1	収集スケジュール	監査ログの定時収集を行う曜日を選択します。	ドロップダウンから次のどれかを選択します。 • 毎日 • 日曜日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日	毎日

項番	項目	説明	設定値	デフォルト値
2	収集時刻	監査ログの定時収集を開始する時刻を指定します。	00:00～23:59 の範囲で時刻を設定します。	00:00
3	収集リトライ間隔（秒）	監査ログの収集に失敗した場合のリトライ間隔を指定します。秒単位で指定してください。	1～3600 の整数（単位：秒）を設定します。	10
4	収集リトライ回数	監査ログの収集に失敗した場合のリトライ回数を指定します。	0～255 の整数（単位：回）を設定します。	5

5.7　監査ログ管理サーバの開始・停止

JP1/Audit Management - Manager のサービスの開始および停止について説明します。

5.7.1　監査ログ管理サーバを開始する

監査ログ管理サーバで JP1/Audit Management - Manager のサービスを開始することで，監査証跡管理システムを開始します。

この節では，開始する JP1/Audit Management - Manager のサービスについて説明します。

コントロールパネルの「管理ツール」から「サービス」を開いて，次に示すサービスを開始してください。

- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define
- JP1/NETM/Audit - Manager SubCollect
- JP1/NETM/Audit - Manager

注意事項

これらのサービスは，自動起動するように設定変更することをお勧めします。

なお，監査証跡管理システムを開始するには，これらのサービスのほかに，次に示すサービスが開始されている必要があります。JP1/Audit Management - Manager のサービスを開始するときは，これらのサービスが開始されているかどうかを確認してください。

- IIS Admin Service
- World Wide Web Publishing Service
- HiRDB/EmbeddedEdition _AL1
- JP1/Base Event

5.7.2　監査ログ管理サーバを停止する

監査ログ管理サーバで JP1/Audit Management - Manager のサービスを停止し，監査証跡管理システムを停止します。

この節では，停止する JP1/Audit Management - Manager のサービスについて説明します。

コントロールパネルの「管理ツール」から「サービス」を開いて，次に示すサービスを停止してください。

- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

- JP1/NETM/Audit - Manager SubCollect
- JP1/NETM/Audit - Manager

5.8　監査ログ閲覧サーバのプログラムのインストール

監査ログ閲覧サーバに必要なプログラムをインストールします。

Internet Explorer を除き，監査ログ閲覧サーバに必要なプログラムは，監査ログ管理サーバに必要なプログラムと同様です。

監査ログ閲覧サーバに必要なプログラムを次に示します。ここに示した順にプログラムをインストールしてください。

1. Microsoft Internet Information Services
   インストールの詳細については「5.2.1　Microsoft Internet Information Services をインストールする」を参照してください。
2. JP1/Base
   インストールの詳細については「5.2.2　JP1/Base をインストールする」を参照してください。
3. EUR（任意）
   インストールの詳細については「5.2.3　EUR をインストールする」を参照してください。
4. JP1/Audit Management - Manager
   インストールの詳細については「5.2.4　JP1/Audit Management - Manager を新規インストールする」を参照してください。

5.9　監査ログ閲覧サーバのセットアップ

監査ログ閲覧サーバをセットアップします。

監査ログ閲覧サーバのセットアップ方法は，監査ログを収集するのに必要な設定や，監査ログのインポートを除いて，監査ログ管理サーバのセットアップ方法と同様です。監査ログ閲覧サーバでは，監査ログを収集するのに必要な設定は不要となります。

監査ログ閲覧サーバのセットアップの手順を次に示します。

1. Microsoft Internet Information Services をセットアップする。

   セットアップの詳細については「5.5.1　Microsoft Internet Information Services をセットアップする」を参照してください。

2. JP1/Base のユーザ管理機能を設定する。

   ユーザ管理機能の設定方法については「5.5.3　JP1/Base のユーザ管理機能を設定する」を参照してください。

3. 監査ログ閲覧サーバの環境設定をする。

   セットアップの詳細については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

4. 監査ログ閲覧サーバのデータベースをセットアップする。

   データベースのセットアップの詳細については「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照してください。なお，JP1/Audit Management - Manager をバージョンアップした場合には，セットアップではなくアップグレードを実施する必要があります。データベースのアップグレードについては「5.5.8　監査ログ管理サーバのデータベースをアップグレードする」を参照してください。

5. 必要なサービスを開始していることを確認する。

   コントロールパネルの「管理ツール」から「サービス」を開いて，次に示すサービスが開始していることを確認してください。

   - IIS Admin Service
   - World Wide Web Publishing Service
   - HiRDB/EmbeddedEdition _AL1

6. 監査ログをインポートする。

   監査ログ管理サーバで管理していた監査ログのバックアップファイルを監査ログ管理サーバから監査ログ閲覧サーバへインポートすることで，監査ログ閲覧サーバから監査ログを閲覧できるようになります。監査ログのバックアップファイルは，監査ログ管理画面からダウンロードします。

   インポートの詳細については「8.3　監査ログのバックアップファイルのインポート」を参照してください。

5.10　クライアントのプログラムのインストール

クライアントで必要なプログラムをインストールします。

クライアントには次に示すプログラムをインストールしてください。

- Adobe Reader（任意）

インストール手順については，Adobe Reader のマニュアルを参照してください。

5.11　監査ログ管理画面を使うための Internet Explorer の設定

クライアントで監査ログ管理画面を使用するために，Internet Explorer の設定を変更する必要があります。

監査ログ管理画面を使用する前に，必要な設定を次に示します。

1. Internet Explorer を起動する。

2. メニューから［ツール］－［インターネットオプション］を選択する。
［インターネット オプション］ダイアログが表示されます。

3.「セキュリティ」タブを選択し，［レベルのカスタマイズ］ボタンをクリックする。
［セキュリティの設定］ダイアログが表示されます。

4. 必要な項目を設定する。
次の表に示す項目を設定してください。設定後に［OK］ボタンをクリックすると設定した内容が適用され，［インターネット オプション］ダイアログが閉じます。

表 5-38 「セキュリティ」タブで設定する項目

項番	分類	設定項目	設定値	説明
1	スクリプト	アクティブ スクリプト	有効にする	ログイン後，監査ログ管理画面が表示できるようになります。
2	その他	暗号化されていないフォームデータの送信	有効にする	監査ログ管理画面へログインできるようになります。
3		ポップアップ ブロックの使用	無効にする	監査ログレポート画面および集計結果グラフ表示画面を表示するときに，ポップアップがブロックされることを回避できるようになります。
4	ダウンロード	ファイルのダウンロード	有効にする	監査ログ管理画面でファイルをダウンロードできるようになります。
5		ファイルのダウンロード時に自動的にダイアログを表示する	有効にする	ファイルのダウンロード時に，ダイアログが表示されるようになります。

注
OS または Internet Explorer のバージョンによっては表示されない場合があります。表示されない場合，設定は不要です。

5.「詳細設定」タブを選択する。

6. 必要な項目を設定する。
次の表に示す項目を設定してください。設定後に［OK］ボタンをクリックすると設定した内容が適用され，［インターネット オプション］ダイアログが閉じます。

表 5-39 「詳細設定」タブで設定する項目

項番	分類	設定項目	設定値	説明
1	セキュリティ	マイコンピュータのファイルでのアクティブコンテンツの実行を許可する	チェックボックスをチェックする	監査ログレポート画面および集計結果グラフ表示画面で保存した HTML 形式ファイルを開くときに，セキュリティ保護のための情報バーの表示を回避できるようになります。
2	印刷	背景の色とイメージを印刷する	チェックボックスをチェックする	集計結果グラフ表示画面の内容をカラーで印刷できるようになります。

5.12　JP1/Audit Management - Manager のバージョンアップ

JP1/Audit Management - Manager をバージョンアップする場合の作業の流れおよび手順について説明します。

5.12.1　JP1/Audit Management - Manager のバージョンアップの流れ

各サーバの構築の流れを次の図に示します。各項目の内容については，括弧内の個所を参照してください。

図 5-20　各サーバでの構築の流れ（バージョンアップする場合）

なお，監査ログ閲覧サーバを導入している場合で，かつ監査ログ管理サーバの JP1/Audit Management - Manager をバージョンアップする場合は，必ず監査ログ閲覧サーバも JP1/Audit Management - Manager をバージョンアップしてください。

5.12.2　JP1/Audit Management - Manager のバージョンアップの手順

JP1/Audit Management - Manager をバージョンアップする場合のインストールおよびセットアップ手順を次に示します。

1. 監査ログ管理サーバで，JP1/Audit Management - Manager を上書きインストールする。

   上書きインストールの手順については「5.2.5　JP1/Audit Management - Manager を上書きインストールする」を参照してください。

2. 監査ログ収集対象サーバのセットアップに必要なファイルをインストールする。

インストールする方法については「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。

3. 監査ログ管理サーバの［マネージャセットアップ］ダイアログで設定値を確認し，［OK］ボタンをクリックして設定を保存する。

   JP1/Audit Management - Manager のバージョンアップ後に，［マネージャセットアップ］ダイアログで環境設定を確認してください。内容を確認後，［OK］ボタンをクリックして設定を保存してください。環境設定の確認方法については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

4. 監査ログ管理サーバで，JP1/Audit Management - Manager のデータベースをアップグレードする。

   データベースのアップグレード手順については「5.5.8　監査ログ管理サーバのデータベースをアップグレードする」を参照してください。

5. 監査ログ管理サーバで，JP1/Audit Management - Manager のサービスを開始する。

   開始するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

監査ログを収集したいプログラムの監査ログ収集対象サーバでの設定内容については「5.4　監査ログ収集対象サーバのセットアップ」を参照してください。また，監査ログ管理サーバでの設定内容については「5.6　監査ログ管理サーバで監査ログを収集するための設定」を参照してください。

5.13　監査ログ収集対象の解除

ここでは，ローカルディスク上から収集している監査ログのうち，その一部またはすべての収集をやめる場合に必要な手順を説明します。

手順は，収集をやめる監査ログの種類や範囲によって異なります。次に示すそれぞれの場合について，手順を説明します。

- ファイルに出力される監査ログの収集をやめる
- Windows イベントログに出力される監査ログの収集をやめる
  - 特定の Windows イベントログについてやめる場合
  - すべての Windows イベントログについてやめる場合
- UNIX システムログに出力される監査ログの収集をやめる
- すべての監査ログの収集をやめる

5.13.1　ファイルに出力される監査ログの収集をやめる

ファイルに出力される監査ログの収集をやめるには，監査ログ管理サーバ上の監査ログ収集マネージャで監査ログ収集対象プログラムを削除し，収集対象から解除してください。手順を次に示します。

1. **［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。**

   ［監査ログ収集マネージャ］ウィンドウが表示されます。

2. **［監査ログ収集マネージャ］ウィンドウに表示された項目から，解除したい収集対象を選択し，［操作］－［監査ログの監視］－［停止］を選択する。**

   選択した監査ログの監視を停止するかどうかを確認するメッセージが表示されます。［OK］ボタンをクリックすると，選択した監査ログ収集対象サーバに対応するログファイルトラップ機能が停止され，監査ログの監視を停止します。なお，複数の収集対象を一度に選択して，監視を停止することもできます。

   監査ログの監視を停止する方法については「9.3.5　監査ログの監視を停止する」を参照してください。

3. **［操作］－［収集対象］－［削除］を選択する。**

   削除するかどうかを確認するダイアログが表示されます。［OK］ボタンをクリックすると，監査ログ収集マネージャから削除され，収集対象から解除されます。

4. **設定を反映するため，JP1/Audit Management - Manager サービスを再起動する。**

   サービスの開始・停止については「5.7　監査ログ管理サーバの開始・停止」を参照してください。

5.13.2　Windows イベントログに出力される監査ログの収集をやめる

特定の Windows イベントログの収集をやめる場合と，すべての Windows イベントログの収集をやめる場合に分けて，説明します。

(1)　特定の Windows イベントログの収集をやめる場合

まず，監査ログ管理サーバで監査ログ収集対象を解除し，次に，監査ログ収集対象サーバでイベントログトラップ機能を解除します。

(a)　監査ログ管理サーバでの作業

監査ログ収集マネージャで，監査ログ収集対象を解除します。この作業の詳細については「5.13.1　ファイルに出力される監査ログの収集をやめる」を参照してください。

(b)　監査ログ収集対象サーバでの作業

イベントログトラップ機能を解除してください。手順を次に示します。

1. Windows イベントログを JP1/Audit Management - Manager の監査ログとして出力するための設定を解除する。
   「5.4.3(1)　JP1/Audit Management - Manager の監査ログとして出力するための設定」を参照し，その作業で設定した内容を解除します。
2. JP1/Base の転送設定ファイル（forward）を編集し，監査ログ専用イベントデータベースへの転送を解除する。
   「5.4.3(4)　イベントログトラップ機能の転送設定ファイル（forward ファイル）を編集する」を参照し，その作業で設定した内容から不要な定義を削除します。
3. 設定を反映するため，転送設定ファイル（forward）をリロードする，または，JP1/Base のイベントサービスを再起動する。
4. JP1/Base の動作定義ファイル（ntevent.conf）を編集し，Windows イベントログを JP1/Audit Management - Manager の監査ログとして収集する定義を削除する。
   「5.4.3(2)　JP1/Base の動作定義ファイル（ntevent.conf）を編集する」を参照し，その作業で設定した内容から不要な定義を削除します。
5. 設定を反映するため，動作定義ファイル（ntevent.conf）をリロードする，または，JP1/Base のイベントログトラップサービスを再起動する。

(2)　すべての Windows イベントログの収集をやめる場合

まず，監査ログ管理サーバで監査ログ収集対象を解除し，次に，監査ログ収集対象サーバでイベントログトラップ機能を解除します。監査ログ収集対象を解除する手順は「(1)　特定の Windows イベントログの収集をやめる場合」と同様ですが，イベントログトラップ機能を解除する手順が異なります。

注意事項

この作業ではイベントサービスを再起動するため，その間イベントログトラップサービスを停止させる必要があります。作業中はイベントログトラップ機能を使用できません。

(a)　監査ログ管理サーバでの作業

監査ログ収集マネージャで，監査ログ収集対象を解除します。この作業の詳細については「5.13.1　ファイルに出力される監査ログの収集をやめる」を参照してください。

(b)　監査ログ収集対象サーバでの作業

イベントログトラップ機能を解除してください。手順を次に示します。

1. Windows イベントログを JP1/Audit Management - Manager の監査ログとして出力するための設定を解除する。

   「5.4.3(1)　JP1/Audit Management - Manager の監査ログとして出力するための設定」を参照し，その作業で設定した内容を解除します。

2. JP1/Base のイベントログトラップ機能が起動している場合は，この機能を停止させる。

3. JP1/Base の動作定義ファイル（ntevent.conf）を編集し，イベントログトラップ機能の動作環境を解除する。

   「5.4.3(2)　JP1/Base の動作定義ファイル（ntevent.conf）を編集する」を参照し，その作業で追加した定義を削除します。

4. JP1/Base のイベントサーバ設定ファイル（conf）を編集し，監査ログ専用イベントサーバの remote-server パラメーターを削除する。

   「5.4.3(3)　イベントログトラップ機能のイベントサーバ設定ファイル（conf ファイル）を編集する」を参照し，その作業で追加した定義を削除します。

5. JP1/Base の転送設定ファイル（forward）を編集し，監査ログ専用イベントデータベースへの転送を解除する。

   「5.4.3(4)　イベントログトラップ機能の転送設定ファイル（forward ファイル）を編集する」を参照し，その作業で設定した内容から不要な定義を削除します。

6. 設定を反映するため，イベントサービスを再起動する。

   JP1/Base Event サービスを再起動します。

7. イベントログトラップ機能を引き続き使用する場合は，JP1/Base のイベントログトラップサービスを再起動する。イベントログトラップ機能を使用しない場合は，起動順序定義ファイルを編集し，自動的に起動しないように設定する。

5.13.3　UNIX システムログに出力される監査ログの収集をやめる

UNIX システムログに出力される監査ログの収集をやめるには，まず，監査ログ管理サーバで監査ログ収集対象を解除し，次に，監査ログ収集対象サーバで UNIX システムログの収集を解除します。

(1)　監査ログ管理サーバでの作業

監査ログ収集マネージャで，監査ログ収集対象を解除します。この作業の詳細については「5.13.1　ファイルに出力される監査ログの収集をやめる」を参照してください。

(2)　監査ログ収集対象サーバでの作業

cron デーモンへ UNIX のログファイルの変換コマンドを登録している場合は，このコマンドの登録を削除して，UNIX システムログの収集を解除します。

5.13.4　すべての監査ログの収集をやめる

すべての監査ログの収集をやめるには，監査ログ管理サーバおよび監査ログ収集対象サーバでそれぞれ作業を行ってください。作業の概要を次の表に示します。

表 5-40　すべての監査ログの収集をやめる作業の概要

項番	作業対象となるサーバ	作業の概要
1	監査ログ管理サーバ	監査ログ収集対象の解除
2	監査ログ収集対象サーバ	イベントログトラップ機能の設定解除
3		UNIX システムログ収集の設定解除
4		イベントサーバの削除
5		セットアップ時にインストールしたファイルの削除

(1)　監査ログ管理サーバでの作業

監査ログ収集マネージャで，すべての監査ログ収集対象を解除します。この作業の詳細については「5.13.1　ファイルに出力される監査ログの収集をやめる」を参照してください。

(2)　監査ログ収集対象サーバでの作業

(a)　イベントログトラップ機能の設定解除

この作業の詳細については「5.13.2(2)(b)　監査ログ収集対象サーバでの作業」を参照してください。

(b)　UNIX システムログ収集の設定解除

この作業の詳細については「5.13.3(2)　監査ログ収集対象サーバでの作業」を参照してください。

(c)　イベントサーバの削除

監査ログ専用イベントサーバを削除する方法について説明します。

監査ログ専用イベントサーバを admagtsetup コマンドで構築した場合と手動で構築した場合で削除する方法が異なります。また，Windows の場合と UNIX の場合とで，手順の一部が異なります。それぞれについて次に説明します。

■ admagtsetup コマンドで監査ログ専用イベントサーバを構築した場合

admagtsetup コマンドで構築した監査ログ専用イベントサーバを削除する方法について説明します。

1. 監査ログ専用イベントサービスが起動している場合は，このサービスを停止させる。

   Windows の場合

   コントロールパネルの「管理ツール」から「サービス」を開いて，監査ログ専用イベントサービスを停止させます。

   UNIX の場合

   次のコマンドを実行して，サービスを停止させます。

```
/opt/jp1base/bin/jevstop 監査ログ専用イベントサーバ名
```

   jevstop コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

2. admagtsetup コマンドを実行する。

   次のコマンドを実行して，監査ログ専用イベントサービスを削除します。

```
admagtsetup -h 監査ログ収集対象サーバのホスト名 -u
```

   admagtsetup コマンドの詳細については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

3. 設定を反映するためにイベントサービスを再起動する。

   監査ログ収集対象サーバで JP1/Base Event サービスを再起動します。

4. 監査ログ専用イベントサービスの自動起動設定を解除する。

   OS 起動時に監査ログ専用イベントサービスが自動起動する設定にしていた場合は，起動順序定義ファイルに追加した定義を削除します。起動順序定義ファイルについては「5.4.2(4)　イベントサービスを自動的に起動する」を参照してください。

■ 手動で監査ログ専用イベントサーバを構築した場合

JP1/NETM/Audit - Manager 09-00 より前のバージョンで構築した監査ログ専用イベントサーバを削除する方法について説明します。

1. 監査ログ専用イベントサービスが起動している場合は，このサービスを停止させる。

Windows の場合

コントロールパネルの「管理ツール」から「サービス」を開いて，監査ログ専用イベントサービスを停止させます。

UNIX の場合

次のコマンドを実行して，サービスを停止させます。

```
/opt/jp1base/bin/jevstop 監査ログ専用イベントサーバ名
```

jevstop コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

2. 監査ログ専用イベントサーバの設定ファイルを変更する。

変更する設定ファイルを次に示します。

- イベントサーバインデックスファイル（index）

  JP1/Base のイベントサーバインデックスファイル（index）を編集し，環境構築時に追加した監査ログ専用イベントデータベースの定義を削除してください。

- API 設定ファイル（api）

  JP1/Base の API 設定ファイル（api）を編集し，環境構築時に追加した監査ログ専用イベントデータベースの定義を削除してください。

3. 設定を反映するためにイベントサービスを再起動する。

監査ログ収集対象サーバで JP1/Base Event サービスを再起動します。

4. 監査ログ専用イベントサービスの自動起動設定を解除する。

OS 起動時に監査ログ専用イベントサービスが自動起動する設定にしていた場合は，起動順序定義ファイルに追加した定義を削除します。起動順序定義ファイルについては「5.4.2(4)　イベントサービスを自動的に起動する」を参照してください。

5. 監査ログ専用イベントサービスを削除する。

登録している監査ログ専用イベントサービスを削除します。この手順は OS が Windows の場合に実施してください。

次のコマンドを実行します。

```
jevregsvc -u 監査ログ専用イベントサーバ名
```

6. 監査ログ専用フォルダ（監査ログ専用ディレクトリ）を削除する。

7. 作業用フォルダ（作業ディレクトリ）を削除する。

作業用に使用していた次のフォルダまたはディレクトリを削除します。

Windows の場合

%ProgramFiles%¥Hitachi¥jp1netmaudit¥manager

UNIX の場合

/opt/jp1netmaudit/manager

ただし，OS が Window の場合は，監査ログ管理サーバのインストール先フォルダに指定されている場合があります。監査ログ管理サーバのインストール先が「%ProgramFiles%」配下の場合は削除しないでください。

(d) セットアップ時にインストールしたファイルの削除

JP1/NETM/Audit - Manager 09-00 以降で監査ログ収集対象サーバをセットアップしているとき

次のコマンドを実行して，セットアップ時に監査ログ収集対象サーバにインストールしたファイルを削除します。

```
admagtinstall -u
```

admagtinstall コマンドの詳細については「12. コマンド」の「admagtinstall（監査ログ収集対象サーバのファイルのインストール)」を参照してください。

なお，admagtinstall コマンドを実行して削除されるのは，セットアップ時に admagtinstall コマンドを実行してインストールしたファイルだけです。インストール後に作成された設定ファイルやログファイルなどは削除されません。また，インストール後に作成された設定ファイルやログファイルを含むフォルダも削除されません。削除されなかったファイルやフォルダは，必要に応じて手動で削除してください。

JP1/NETM/Audit - Manager 09-00 より前のバージョンで監査ログ収集対象サーバをセットアップしているとき

セットアップ時に監査ログ収集対象サーバにコピーした，アダプタコマンドおよびアダプタコマンド定義ファイルを削除します。削除するファイルについて次の表に示します。

表 5-41 削除するアダプタコマンドおよびアダプタコマンド定義ファイル

項番	OS の種類 (監査ログ収集対象サーバ)	格納先フォルダまたはディレクトリ (監査ログ収集対象サーバ)	アダプタコマンドおよびアダプタコマンド定義ファイル
1	Windows	JP1/Base のインストール先フォルダ¥bin	adm_adaptercmd.exe
2		JP1/Base のインストール先フォルダ¥plugin¥conf	Adapter_HITACHI_JP1_NETM_AUDIT.conf
3	UNIX	/opt/jp1base/bin	adm_adaptercmd
4		/opt/jp1base/plugin/conf	Adapter_HITACHI_JP1_NETM_AUDIT.conf

削除方法の詳細については，JP1/NETM/Audit - Manager 08-51 以前のマニュアルを参照してください。

6 クラスタ環境でのシステム構築

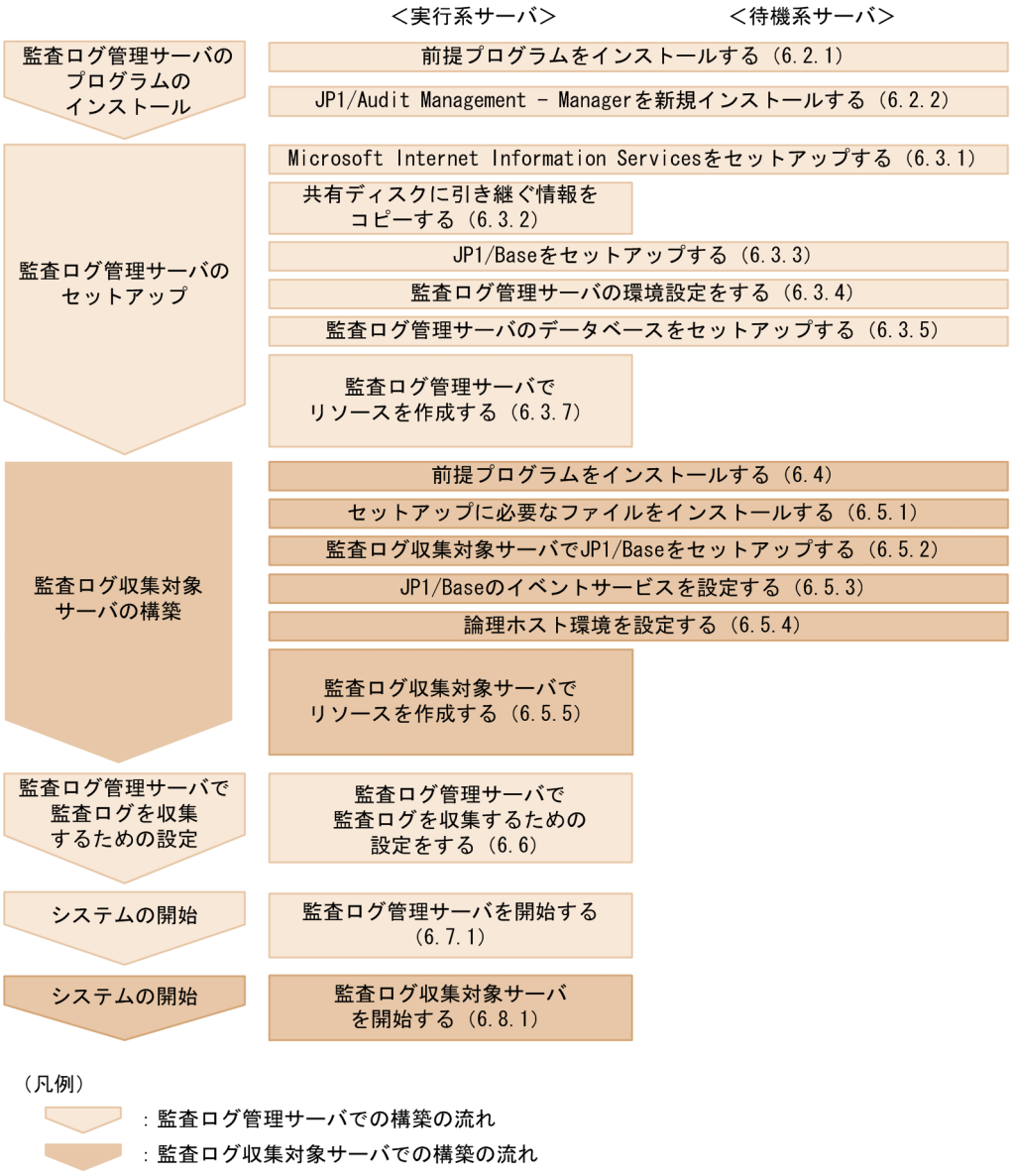
この章では，監査証跡管理システムをクラスタ環境で運用する場合のインストールとセットアップについて説明します。また，クラスタ環境からの JP1/Audit Management - Manager のアンインストールについても説明します。

6.1　クラスタ環境でのシステム構築の流れ

この節では，監査証跡管理システムをクラスタ環境で運用する場合の構築の流れについて説明します。

各サーバでの構築の流れを次の図に示します。各項目の内容については，括弧内の個所を参照してください。

図 6-1　各サーバでの構築の流れ（クラスタ環境）



なお，クラスタ環境で JP1/Audit Management - Manager をバージョンアップする場合の構築の流れについては「6.9　JP1/Audit Management - Manager のバージョンアップ（クラスタ環境）」を参照してください。

6.2　監査ログ管理サーバのプログラムのインストール（クラスタ環境）

監査ログ管理サーバをクラスタ環境で運用する場合は，実行系および待機系のサーバマシンをセットアップしてから，監査ログ管理サーバで必要なプログラムをインストールします。

クラスタ環境で運用する場合はクラスタソフトをインストールする必要があります。クラスタソフトを除いて，クラスタ環境で運用する場合と運用しない場合で，インストールするプログラムは同様です。

監査ログ管理サーバで必要なプログラムのインストールの詳細について，次に説明します。なお，このマニュアルでは，クラスタソフトのインストールおよびセットアップについては，すでに完了していることを前提として説明します。

注意事項

監査ログ管理サーバをクラスタ環境で運用する場合は，次のことに注意してください。

- OS でワトソンログを取得するよう設定している場合は，フェールオーバーされません。監査ログ管理サーバをクラスタ環境で運用する場合は，ワトソンログを取得しない設定にしてください。
- クラスタソフトでオンラインにするとサービスが開始します。以降，World Wide Web Publishing Service サービスを停止または開始するときは，クラスタソフトで状態をオフラインまたはオンラインにしてください。

6.2.1　前提プログラムをインストールする（クラスタ環境）

実行系サーバと待機系サーバの両方に，JP1/Audit Management - Manager の前提プログラムをインストールします。

前提プログラムを次に示します。

- Microsoft Internet Information Services
- JP1/Base
- EUR（任意）

各プログラムは，クラスタ環境での運用に対応するようにインストールしてください。

インストールする各プログラムの詳細については「5.2　監査ログ管理サーバのプログラムのインストール」を参照してください。

6.2.2　JP1/Audit Management - Manager を新規インストールする（クラスタ環境）

実行系サーバと待機系サーバの両方に，JP1/Audit Management - Manager をインストールします。

実行系サーバへのインストールは共有ディスクを実行系に切り替えてから，待機系サーバへのインストールは共有ディスクを待機系に切り替えてから実施してください。どちらの場合も，ローカルディスクにインストールしてください。また，仮想ディレクトリには共有ディスク上のフォルダを設定してください。

インストール手順については「5.2.4　JP1/Audit Management - Manager を新規インストールする」を参照してください。

6.2.3　JP1/Audit Management - Manager を上書きインストールする（クラスタ環境）

実行系サーバと待機系サーバの両方に，JP1/Audit Management - Manager を上書きインストールします。

上書きインストールする JP1/Audit Management - Manager のバージョンが，すでにインストールされている JP1/Audit Management - Manager のバージョンより古い場合，上書きインストールは実施できません。

JP1/Audit Management - Manager の上書きインストールは，提供媒体を使用してインストールするかまたは JP1/NETM/DM を使用してリモートインストールします。JP1/NETM/DM を使ったリモートインストールについては，マニュアル「JP1/NETM/DM 運用ガイド 1(Windows(R)用)」を参照してください。

JP1/Audit Management - Manager の上書きインストールについて説明します。

(1)　上書きインストール前の作業

JP1/Audit Management - Manager を上書きインストールする前に，次に示す作業を実施してください。

- **JP1/Audit Management - Manager のバックアップを取得する**
  上書きインストール中にエラーが発生した場合に備えて，監査ログ管理データベースの内容を作業前に戻せるように，JP1/Audit Management - Manager の環境定義のバックアップを取得してください。バックアップの取得が必要なフォルダを次に示します。
  - **共有ディスク¥**conf
  - **JP1/Audit Management - Manager の仮想ディレクトリ¥**conf

  バックアップを取得する前に，JP1/Audit Management - Manager のリソースをオフラインにしてください。JP1/Audit Management - Manager のリソースのオンラインおよびオフラインについては「6.7　監査ログ管理サーバの開始・停止（クラスタ環境）」を参照してください。
- **監査ログ管理データベースのバックアップまたは CSV バックアップを取得する**
  上書きインストール中にエラーが発生した場合に備えて，監査ログ管理データベースのバックアップまたは CSV バックアップを取得してください。監査ログ管理データベースのバックアップや CSV バックアップは，データベースマネージャまたはコマンドを使用して取得します。データベースのバックアップの取得方法については「10.1.3　データベースのバックアップ」を参照してください。また，

データベースの CSV バックアップの取得方法については「10.1.7　データベースの CSV バックアップ」を参照してください。

- **インストール先に十分な空き容量があるかどうかを確認する**

  インストール先の空き容量が 250 メガバイト未満または仮想ディレクトリの空き容量が 20 メガバイト未満の場合はインストールが中断されます。このため，インストール先に十分な空き容量があるかどうかを確認してください。

なお，同じバージョンの JP1/Audit Management - Manager を上書きインストールする場合は，データベースをアップグレードする必要がないため，インストール前の作業として，ディスクの空き容量を確保する必要はありません。

(2)　上書きインストール

上書きインストールする手順を次に示します。

1. **実行系サーバ上のクラスタソフトで JP1/Audit Management - Manager のサービスおよび Microsoft Internet Information Services のサービスのリソースをオフラインにする。**

   オフラインにする JP1/Audit Management - Manager のサービスのリソースについては「6.7.2　監査ログ管理サーバを停止する（クラスタ環境）」を参照してください。

2. **実行系サーバ上で admdbstop コマンドを実行してデータベースを停止する。**

   次のコマンドを実行します。

   ```
   admdbstop
   ```

   admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

3. **実行系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオフラインにする。**

4. **実行系サーバ上のクラスタソフトで共有ディスクを実行系から待機系に切り替える。**

5. **待機系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオンラインにする。**

6. **待機系サーバ上で admdbstop コマンドを実行してデータベースを停止する。**

   次のコマンドを実行します。

   ```
   admdbstop
   ```

   admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

7. **待機系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオフラインにする。**

8. 待機系サーバ上で，上書きインストールする。

   上書きインストールする手順は，新規インストールの手順と同様です。新規インストールの手順については「6.2.2　JP1/Audit Management - Manager を新規インストールする（クラスタ環境）」を参照してください。なお，上書きインストールの完了後，必ずシステムを再起動してください。

9. 待機系サーバ上のクラスタソフトで共有ディスクを待機系から実行系に切り替える。

10. 実行系サーバ上で，上書きインストールする。

    上書きインストールする手順は，新規インストールの手順と同様です。新規インストールの手順については「6.2.2　JP1/Audit Management - Manager を新規インストールする（クラスタ環境）」を参照してください。なお，上書きインストールの完了後，必ずシステムを再起動してください。

11. 実行系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオンラインにする。

6.2.4　JP1/Audit Management - Manager をアンインストールする（クラスタ環境）

クラスタ環境から JP1/Audit Management - Manager をアンインストールする場合の手順を次に示します。

1. 実行系サーバ上のクラスタソフトで JP1/Audit Management - Manager のサービスおよび Microsoft Internet Information Services のサービスのリソースをオフラインにする。

   オフラインにする JP1/Audit Management - Manager のサービスのリソースについては「6.7.2　監査ログ管理サーバを停止する（クラスタ環境）」を参照してください。

2. 実行系サーバ上で，admdbstop コマンドを実行してデータベースを停止する。

   次のコマンドを実行します。

   ```
   admdbstop
   ```

   admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

3. 実行系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオフラインにする。

4. 実行系サーバ上のクラスタソフトで共有ディスクを実行系から待機系に切り替える。

5. 待機系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオンラインにする。

6. 待機系サーバ上で admdbstop コマンドを実行してデータベースを停止する。

   次のコマンドを実行します。

```
admdbstop
```

admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

7. 待機系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオフラインにする。

8. 待機系サーバ上で，JP1/Audit Management - Manager をアンインストールする。

   実行系サーバでアンインストールする前に，待機系サーバをアンインストールしてください。

   アンインストールの手順については「5.2.6　JP1/Audit Management - Manager をアンインストールする」を参照してください。

9. 待機系サーバ上のクラスタソフトで共有ディスクを待機系から実行系に切り替える。

10. 実行系サーバ上で，JP1/Audit Management - Manager をアンインストールする。

    アンインストールの手順については「5.2.6　JP1/Audit Management - Manager をアンインストールする」を参照してください。

11. 実行系サーバ上で，監査ログ管理サーバ用に作成した JP1/Audit Management - Manager のサービスのリソースをクラスタソフトから削除する。

    削除する JP1/Audit Management - Manager のサービスのリソースについては「6.7.2　監査ログ管理サーバを停止する（クラスタ環境）」を参照してください。

12. 共有ディスク上に作成されたファイルを削除する。

    共有ディスク上のファイルはアンインストールでは削除されません。必要に応じて，手動で削除してください。

6.3　監査ログ管理サーバのセットアップ（クラスタ環境）

監査ログ管理サーバにインストールしたプログラムをセットアップします。

6.3.1　Microsoft Internet Information Services をセットアップする（クラスタ環境）

実行系サーバと待機系サーバの両方で，Microsoft Internet Information Services をセットアップします。セットアップする内容を次に示します。なお，実行系サーバと待機系サーバで，同様の設定内容にしてください。

- バックアップファイルの格納先フォルダの設定

  初めに，共有ディスク上にバックアップファイルの格納先とするフォルダを作成してください。次に，作成した共有ディスク上のフォルダにリンクさせる仮想ディレクトリを，実行系サーバと待機系サーバの両方の IIS マネージャで設定します。
- ダウンロードファイルの最大サイズの設定

  実行系サーバと待機系サーバの両方で，監査ログ管理画面からファイルをダウンロードするときの最大サイズを，コマンドを使用して設定します。
- IIS 受信バッファの最大サイズの設定

  実行系サーバと待機系サーバの両方で，監査ログ管理画面からファイルをアップロードするときの最大サイズを設定します。
- アプリケーションプールのプロパティ設定変更

  実行系サーバと待機系サーバの両方で，アプリケーションプールのプロパティ設定を変更します。

操作の詳細については「5.5.1　Microsoft Internet Information Services をセットアップする」を参照してください。

6.3.2　共有ディスクに引き継ぐ情報をコピーする

フェールオーバーが発生した場合，共有ディスクの接続は，実行系サーバから待機系サーバへ切り替わります。待機系サーバは，共有ディスクに保存されている JP1/Audit Management - Manager の情報を基に，実行系サーバから処理を引き継ぎます。

処理を引き継ぐために必要な JP1/Audit Management - Manager の情報を次に示します。

- 正規化ルールファイル
- 製品定義ファイル
- 動作定義ファイル

このため，共有ディスクにこれらの情報を保存しておく必要があります。情報を保存するには，JP1/Audit Management - Manager のインストール先フォルダ配下にある次の表のフォルダを，共有ディスクに手動でコピーする必要があります。また，共有ディスクにはフォルダとして，「**共有ディスク¥**spool」を作成してください。

共有ディスクにコピーするフォルダについて，次の表に示します。

表 6-1　共有ディスクにコピーするフォルダ

項番	フォルダの内容	コピー元	コピー先
1	正規化ルールファイル	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥rule	共有ディスク¥conf¥rule
2	製品定義ファイル	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥product	共有ディスク¥conf¥product
3	動作定義ファイル	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥logdef	共有ディスク¥conf¥logdef

6.3.3　JP1/Base をセットアップする（クラスタ環境）

実行系サーバと待機系サーバの両方で，JP1/Base をセットアップします。クラスタ環境での運用に対応するようにセットアップしてください。

なお，クラスタソフトに登録する JP1/Base のリソースは，監査ログ管理サーバ用のグループに登録する必要があります。すでに別のグループに JP1/Base のリソースが登録されている場合は，監査ログ管理サーバ用に論理ホスト環境を作成してください。

JP1/Base をクラスタ環境で運用する場合の設定については，マニュアル「JP1/Base 運用ガイド」を参照してください。また，監査ログ管理サーバで使用する JP1/Base に必要な設定については「5.5.3　JP1/Base のユーザ管理機能を設定する」，「5.5.4　JP1/Base の jevsend コマンドを実行する」および「5.5.5 JP1/Base の API 設定ファイル（api ファイル）を編集する」を参照してください。

6.3.4　監査ログ管理サーバの環境設定をする（クラスタ環境）

監査ログ管理サーバの環境を設定します。

実行系サーバ，待機系サーバの順に，［マネージャセットアップ］ダイアログで実施します。実行系サーバの環境設定は共有ディスクを実行系に切り替えてから，待機系サーバの環境設定は共有ディスクを待機系に切り替えてから実施してください。各項目には，実行系サーバ，待機系サーバで同じ内容を設定してください。なお，待機系サーバでの初回設定時に，「KDSO2044-W」のメッセージが表示されることがあります。

ここでは，［マネージャセットアップ］ダイアログでの設定のうち，監査ログ管理サーバをクラスタ環境で運用する場合に特に必要な情報について説明します。このほかの設定については「5.5.6　監査ログ管理サーバの環境設定をする」を参照し，環境に合わせて実施してください。

クラスタ環境の場合に必要な設定は次のとおりです。

［マネージャセットアップ］ダイアログ

クラスタ情報について設定する必要があります。次の表に示す項目について設定してください。

表 6-2 「クラスタ情報」の設定内容（クラスタシステムの場合）

項番	項目		内容	設定値	デフォルト値	必須
1	クラスタ情報	クラスタ運用	監査ログ管理サーバをクラスタ環境で運用するかどうかを設定します。	次のどちらかを選択します。 • 「運用する」 • 「運用しない」 クラスタ環境で運用する場合は必ず「運用する」を指定してください。	運用しない	○
2		論理ホスト名	クラスタ環境での運用の場合に，論理ホスト名を設定します。 「クラスタ運用」を「運用する」に指定した場合は，必ず指定してください。 なお，クラスタ環境でシステムを運用中は変更できません。	195 バイト以内の文字列を設定します。 使用できる文字を次に示します。 • 半角英数字 • 「-」「_」「.」	なし	○
3		共有ディスク	クラスタ環境での運用の場合に，共有ディスクのディレクトリ名をフルパスで設定します。 「クラスタ運用」を「運用する」に指定した場合は，必ず設定してください。 なお，クラスタ環境でシステムを運用中は変更できません。	共有ディスクのパスを 200 バイト以内で設定します。 使用できない文字の種類は次のとおりです。 • 「:」「*」「?」「"」「<」「>」「|」 半角スペースを含んだパスを指定する場合でも，「"」で囲む必要はありません。 JP1/Audit Management - Manager は，ここで指定された共有ディスク上のフォルダに，実行系・待機系の切り替え時に引き継ぎが必要な情報を作成します。	なし	○

（凡例）

○：必ず設定する

6.3.5　監査ログ管理サーバのデータベースをセットアップする（クラスタ環境）

まず，実行系サーバでデータベースをセットアップし，共有ディスクを切り替えたあと，待機系サーバでデータベースをセットアップします。手順を次に示します。

1. 実行系サーバで［データベースマネージャ］ダイアログからデータベースをセットアップする。

   ここでは，［データベースマネージャ］ダイアログでの設定のうち，監査ログ管理サーバをクラスタ環境で運用する場合に特に必要な情報について説明します。このほかの設定については「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照し，環境に合わせて実施してください。

   クラスタ環境の場合に必要な設定は次のとおりです。

   ［データベースの詳細設定］画面（データベースマネージャ）

   - 「データベース領域の格納先」

     「ローカルディスク上の格納先フォルダ名」に，待機系への引き継ぎが不要な領域を格納するフォルダを指定します。ローカルディスク上のフォルダを 100 バイト以内で指定してください。なお，［...］ボタンをクリックすると，フォルダを参照するダイアログからフォルダ名を指定できます。

   ［クラスタシステム環境の設定］画面（データベースマネージャ）

   - 「クラスタシステム環境で使用する」

     チェックします。

   - 「実行系/待機系」

     「実行系」を選択します。

   - 「共有ディスク上の格納先フォルダ名」

     待機系への引き継ぎが必要な領域を格納するフォルダを指定します。共有ディスク上のフォルダを 100 バイト以内で指定してください。なお，［...］ボタンをクリックすると，フォルダを参照するダイアログからフォルダ名を指定できます。

2. 実行系サーバ上で admdbstop コマンドを実行してデータベースを停止する。

   次のコマンドを実行します。

   ```
   admdbstop
   ```

   admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

3. 実行系サーバ上のクラスタソフトで共有ディスクを実行系から待機系に切り替える。

4. 待機系サーバで［データベースマネージャ］ダイアログからデータベースをセットアップする。

   手順 1 で設定した実行系サーバと同じ内容を設定してください。ただし，次の項目については，待機系サーバ用の設定が必要です。

   - ［クラスタシステム環境の設定］画面の「実行系/待機系」

     「待機系」を選択します。

5. 待機系サーバ上のクラスタソフトで共有ディスクを待機系から実行系に切り替える。

6.3.6　監査ログ管理サーバのデータベースをアップグレードする（クラスタ環境）

監査ログ管理サーバで JP1/Audit Management - Manager をバージョンアップした場合，監査ログ管理サーバのデータベースをアップグレードする必要があります。

(1)　データベースのアップグレード前の作業

JP1/Audit Management - Manager をバージョンアップすると，ローカルディスク上の定義ファイルが更新されます。このため，データベースをアップグレードする前に，手動で定義ファイルをローカルディスクから共有ディスクへコピーする必要があります。

アップグレード前に定義ファイルをコピーする作業手順を次に示します。

1. ローカルディスク上のフォルダを共有ディスクへコピーする。
   ローカルディスク上のコピー元フォルダおよび共有ディスク上の格納先フォルダを次の表に示します。

   表 6-3　共有ディスクにコピーするフォルダ

項番	コピー元フォルダ	格納先
1	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥logdef	共有ディスク¥conf
2	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥product	
3	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥rule	

(2)　データベースのアップグレード手順

実行系サーバおよび待機系サーバでデータベースをアップグレードします。手順を次に示します。

1. 実行系サーバ上で，データベースのアップグレードを実施する。
   データベースのアップグレード手順については「5.5.8　監査ログ管理サーバのデータベースをアップグレードする」を参照してください。

2. 実行系サーバ上で admdbstop コマンドを実行してデータベースを停止する。
   次のコマンドを実行します。

   ```
   admdbstop
   ```

   admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

3. 実行系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオフラインにする。

4. 実行系サーバ上のクラスタソフトで共有ディスクを実行系から待機系に切り替える。

5. 待機系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオンラインにする。

6. 待機系サーバ上で，データベースのアップグレードを実施する。
   データベースのアップグレード手順については「5.5.8　監査ログ管理サーバのデータベースをアップグレードする」を参照してください。

7. 待機系サーバ上で，admdbstop コマンドを実行してデータベースを停止する。
   次のコマンドを実行します。

   ```
   admdbstop
   ```

   admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

8. 待機系サーバ上のクラスタソフトで HiRDB/ClusterService _AL1 サービスのリソースをオフラインにする。

9. 待機系サーバ上のクラスタソフトで共有ディスクを待機系から実行系に切り替える。

10. 実行系サーバ上のクラスタソフトでフェールオーバーさせるサービスのリソースを作成する。
    作成するサービスのリソースについては「6.3.7　監査ログ管理サーバでリソースを作成する」を参照してください。

6.3.7　監査ログ管理サーバでリソースを作成する

実行系サーバのクラスタソフトで，フェールオーバーさせるリソースを作成します。作成するリソースを次に示します。

- HiRDB/ClusterService _AL1 サービスのリソース
  監査ログ管理サーバのデータベースをクラスタ環境で制御するためのリソースです。
- JP1/NETM/Audit - Manager サービスのリソース
  JP1/NETM/Audit - Manager サービスに対応するリソースです。
- JP1/NETM/Audit - Manager Convert サービスのリソース
  JP1/NETM/Audit - Manager Convert サービスに対応するリソースです。
- JP1/NETM/Audit - Manager Define サービスのリソース
  JP1/NETM/Audit - Manager Define サービスに対応するリソースです。
- JP1/NETM/Audit - Manager SubCollect サービスのリソース
  JP1/NETM/Audit - Manager SubCollect サービスに対応するリソースです。
- Microsoft Internet Information Services のリソース

Microsoft Internet Information Services のリソースです。

なお，クラスタソフトの初期導入時には，あらかじめ「クラスタグループ」というグループが作成されています。これとは別に監査ログ管理サーバ用のクラスタグループを作成します。以降，ここで作成したグループを**監査ログ管理サーバクラスタグループ**と呼びます。

次に，各リソースの登録内容を説明します。HiRDB/ClusterService _AL1 サービスのリソースは，必ず最初に登録してください。クラスタソフトの操作方法については，各クラスタソフトのマニュアルを参照してください。

(1) HiRDB/ClusterService _AL1 サービスのリソース

HiRDB/ClusterService _AL1 サービスのリソースの登録内容について，次の表に示します。

表 6-4 HiRDB/ClusterService _AL1 サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	HiRDB/ClusterService _AL1	「共有ディスク」と「クライアントアクセスポイント」のリソースを設定します。

(2) JP1/NETM/Audit - Manager サービスのリソース

JP1/NETM/Audit - Manager サービスのリソースの登録内容について，次の表に示します。

表 6-5 JP1/NETM/Audit - Manager サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	JP1/NETM/Audit - Manager	「HiRDB/ClusterService _AL1 サービス」のリソースを設定します。

(3) JP1/NETM/Audit - Manager Convert サービスのリソース

JP1/NETM/Audit - Manager Convert サービスのリソースの登録内容について，次の表に示します。

表 6-6 JP1/NETM/Audit - Manager Convert サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	JP1/NETM/Audit - Manager Convert	「HiRDB/ClusterService _AL1 サービス」のリソースを設定します。

(4) JP1/NETM/Audit - Manager Define サービスのリソース

JP1/NETM/Audit - Manager Define サービスのリソースの登録内容について，次の表に示します。

表 6-7　JP1/NETM/Audit - Manager Define サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	JP1/NETM/Audit - Manager Define	「HiRDB/ClusterService _AL1 サービス」のリソースを設定します。

(5)　JP1/NETM/Audit - Manager SubCollect サービスのリソース

JP1/NETM/Audit - Manager SubCollect サービスのリソースの登録内容について，次の表に示します。

表 6-8　JP1/NETM/Audit - Manager SubCollect サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	JP1/NETM/Audit - Manager SubCollect	「共有ディスク」と「クライアントアクセスポイント」のリソースを設定します。

(6)　Microsoft Internet Information Services のリソース

Microsoft Internet Information Services サービスのリソースの登録内容について，次の表に示します。

表 6-9　Microsoft Internet Information Services のリソースの登録内容

項番	リソースの種類	スクリプトファイルパスへの入力内容	依存関係
1	汎用スクリプト	%SystemRoot%¥System32¥Inetsrv¥Clusweb.vbs	「共有ディスク」と「クライアントアクセスポイント」のリソースを設定します。

注

マイクロソフト社の Web サイトを参照しスクリプトを作成する必要があります。

6.4　監査ログ収集対象サーバのプログラムのインストール（クラスタ環境）

監査ログ収集対象サーバをクラスタ環境で運用する場合は，実行系および待機系のサーバマシンをセットアップしてから，監査ログ収集対象サーバで必要なプログラムをインストールします。

クラスタ環境で運用する場合は，実行系サーバと待機系サーバの両方にクラスタソフトをインストールする必要があります。各 OS に対応するクラスタソフトについては「3.2.2(3)　監査ログ収集対象サーバの前提プログラム」を参照してください。

クラスタソフト以外は，クラスタ環境で運用しない場合とインストールするプログラムは同様です。監査ログ収集対象サーバで必要なプログラムのインストールについては「5.3　監査ログ収集対象サーバのプログラムのインストール」を参照してください。

6.5　監査ログ収集対象サーバのセットアップ（クラスタ環境）

監査ログ収集対象サーバにインストールしたプログラムをセットアップします。なお，このマニュアルでは，クラスタソフトのセットアップについては，すでに完了していることを前提として説明します。

また，ここでは，監査ログ収集対象サーバ上で「共有ディスク上に出力される監査ログ」を収集する場合について説明します。「共有ディスク上に出力される監査ログ」を収集する場合は，監査ログ収集対象サーバで論理ホストをセットアップします。監査ログ管理サーバ上で「共有ディスク上に出力される監査ログ」を収集する場合は，監査ログ管理サーバで論理ホストをセットアップしてください。

「ローカルディスク上に出力される監査ログ」を収集する場合は，物理ホストをセットアップします。物理ホストのセットアップ手順は，通常の監査ログ収集対象サーバのセットアップ手順と同様です。物理ホストは「5.4　監査ログ収集対象サーバのセットアップ」を参照し，セットアップしてください。ただし，クラスタ環境にある監査ログ収集対象サーバから Windows イベントログを収集する場合で，イベントログの複製機能が有効になっているときは，自ホストのイベントログだけが監査ログ専用イベントデータベースに転送されるように設定してください。または，イベントログの複製機能を無効に設定してください。イベントログの複製機能については，各クラスタソフトのマニュアルを参照してください。

6.5.1　セットアップに必要なファイルをインストールする（クラスタ環境）

実行系サーバと待機系サーバの両方で，セットアップに必要なファイルをインストールします。

セットアップに必要なファイルのインストールについての詳細は「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。

なお，すでに物理ホストのセットアップが完了し，監査ログ収集対象サーバのセットアップに必要なファイルがインストールされている場合，この作業は不要です。

6.5.2　監査ログ収集対象サーバで JP1/Base をセットアップする（クラスタ環境）

実行系サーバと待機系サーバの両方で，JP1/Base をクラスタ環境での運用に対応するようにセットアップします。なお，クラスタソフトに登録する JP1/Base のリソースは，監視対象プログラムと同一のグループに登録する必要があります。

JP1/Base をクラスタ環境で運用する場合の設定については，マニュアル「JP1/Base 運用ガイド」を参照してください。

6.5.3　JP1/Base のイベントサービスを設定する（クラスタ環境）

イベントサービスを使用するために，監査ログ収集対象サーバで監査ログ専用イベントサーバを設定します。

共有ディスク上の監査ログを収集する場合は，論理ホスト用の監査ログ専用イベントサーバを設定します。複数の論理ホストが存在し，それぞれの共有ディスク上の監査ログを収集する場合は，各論理ホストに監査ログ専用イベントサーバを設定します。次に，設定手順についてサーバごとに説明します。

実行系サーバでの設定手順

実行系サーバでの設定手順は，次の設定を除いて，クラスタ環境で運用しない場合の手順と同様です。

IP アドレス，ホスト名およびイベントサーバ名

IP アドレスは「論理 IP アドレス」，ホスト名は「論理ホスト名」，イベントサーバ名は「論理ホスト名-adm」にそれぞれ置き換えてください。

監査ログ専用イベントサーバの構築時に指定する環境情報

実行系サーバで論理ホスト用の監査ログ専用イベントサーバを設定します。

環境情報をコマンドの引数で指定する場合は，「-c online」を指定してください。監査ログ収集対象サーバセットアップ定義ファイルで指定する場合は，ファイル内の［Cluster］セクションで「ClusterFlag=Y」，「ClusterMode=ONLINE」を指定してください。

クラスタ環境で運用しない場合の手順については「5.4.2　JP1/Base のイベントサービスを設定する」を参照してください。また，待機系サーバで監査ログ専用イベントサーバの情報をコピーするために，実行系サーバの監査ログ専用イベントサーバの情報をファイルに出力します。監査ログ専用イベントサーバの情報をファイルに出力するには，admagtsetup コマンドを実行します。

admagtsetup コマンドの実行例を次に示します。

```
admagtsetup -v -h 論理ホスト名 > 監査ログ収集対象サーバセットアップ定義ファイル
```

admagtsetup コマンドの詳細については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

待機系サーバでの設定手順

待機系サーバでは，次に示す設定を実施します。

- 監査ログ専用イベントサーバの情報をコピーする。

  実行系サーバで出力した監査ログ収集対象サーバセットアップ定義ファイルを待機系サーバにコピーします。コピー先フォルダは任意です。

- コピーした監査ログ収集対象サーバセットアップ定義ファイルを編集する。

  コピーした監査ログ収集対象サーバセットアップ定義ファイルを待機系サーバ用の定義に変更します。変更するパラメーターを次に示します。

  変更前

```
ClusterMode=ONLINE
```

  変更後

```
ClusterMode=STANDBY
```

監査ログ収集対象サーバセットアップ定義ファイルの詳細については「13.9　監査ログ収集対象サーバセットアップ定義ファイル」を参照してください。

- 監査ログ専用イベントサーバを構築する。

  admagtsetup コマンドを実行して，論理ホスト用の監査ログ専用イベントサーバを構築します。なお，admagtsetup コマンドの-f オプションには，待機系サーバ用に編集した監査ログ収集対象サーバセットアップ定義ファイルを指定します。

  admagtsetup コマンドの実行例を次に示します。

```
admagtsetup -f 監査ログ収集対象サーバセットアップ定義ファイル
```

admagtsetup コマンドの詳細については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

監査ログ収集対象サーバセットアップ定義ファイルは，セットアップが完了したあとは不要になります。

なお，監査ログ専用イベントサーバの構築の詳細については「5.4.2　JP1/Base のイベントサービスを設定する」を参照してください。

注意事項

実行系サーバの環境設定は共有ディスクを実行系に切り替えてから，待機系サーバの環境設定は共有ディスクを待機系に切り替えてから実施してください。

6.5.4　論理ホスト環境を設定する

共有ディスク上に出力される監査ログを収集する場合は，実行系サーバと待機系サーバの両方で，admhasetup コマンドを実行して論理ホスト環境を設定します。このコマンドを実行することで，共有ディスク上の監査ログを収集する場合に必要となるサービス，およびフェールオーバー時に情報を引き継ぐために使用する共有ディレクトリが作成されます。また，複数の論理ホストが存在し，それぞれの共有ディスク上の監査ログを収集する場合は，各論理ホストにセットアップを実行します。コマンド実行例を次に示します。

```
admhasetup -h 論理ホスト名 -c online -r 共有ディレクトリ
```

実行系サーバで論理ホストの環境を設定する場合は「-c△online」，待機系サーバで論理ホストの環境を設定する場合は「-c△standby」を指定してください。

共有ディレクトリは，共有ディスク上のディレクトリをフルパスで指定してください。また，実行系サーバと待機系サーバで同じディレクトリを指定してください。

admhasetup コマンドの詳細については「12.　コマンド」の「admhasetup（論理ホスト環境の作成）」を参照してください。

注意事項

実行系サーバの環境設定は共有ディスクを実行系に切り替えてから，待機系サーバの環境設定は共有ディスクを待機系に切り替えてから実施してください。

6.5.5　監査ログ収集対象サーバでリソースを作成する

共有ディスク上に出力される監査ログを収集する場合は，実行系サーバでリソースを作成します。共有ディスクを実行系に切り替えてから作業を実施してください。

次に，作成方法について OS ごとに説明します。

(1)　Windows の場合

実行系サーバのクラスタソフトで，フェールオーバーさせるリソースを作成します。作成するリソースを次に示します。

- JP1/Base Event **監査ログ専用イベントサーバ名**サービスのリソース
  論理ホスト用の監査ログ専用イベントサービスに対応するリソースです。
- JP1/NETM/Audit LogTrap **論理ホスト名**サービスのリソース
  共有ディスク上の監査ログを収集するためのログファイルトラップ起動/停止デーモンに対応するリソースです。

次に，各リソースの登録内容を説明します。リソースの作成方法の詳細については，各クラスタソフトのマニュアルを参照してください。

(a)　JP1/Base Event 監査ログ専用イベントサーバ名サービスのリソース

JP1/Base Event **監査ログ専用イベントサーバ名**サービスのリソースの登録内容を次の表に示します。

表 6-10　JP1/Base Event 監査ログ専用イベントサーバ名サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	JP1/Base Event 監査ログ専用イベントサーバ名	「共有ディスク」と「クライアントアクセスポイント」のリソースを設定します。

(b)　JP1/NETM/Audit LogTrap 論理ホスト名サービスのリソース

JP1/NETM/Audit LogTrap **論理ホスト名**サービスのリソースの登録内容を次の表に示します。

表 6-11　JP1/NETM/Audit LogTrap 論理ホスト名サービスのリソースの登録内容

項番	リソースの種類	選択するサービス名	依存関係
1	汎用サービス	JP1/NETM/Audit LogTrap 論理ホスト名	「JP1/Base Event 監査ログ専用イベントサーバ名」のリソースを設定します。※

注※

JP1/NETM/Audit LogTrap **論理ホスト名**サービスは，監査ログ収集対象プログラムより前に起動されるように依存関係を設定してください。

(2)　UNIX の場合

実行系サーバで，フェールオーバーさせるコマンドを，クラスタソフトに登録します。クラスタソフトに登録するコマンドと，その機能を次の表に示します。

表 6-12　クラスタソフトに登録するコマンドと機能

項番	登録するコマンド	機能	説明
1	admhastart **論理ホスト名**※	起動	次の二つを起動します。 • 論理ホスト用の監査ログ専用イベントサーバのサービス • 監査ログを収集するためのログファイルトラップ機能
2	admhastop **論理ホスト名**※	停止	次の二つを停止します。 • 論理ホスト用の監査ログ専用イベントサーバのサービス • 監査ログを収集するためのログファイルトラップ機能

注※

コマンドの格納先は，「付録 A.3　監査ログ収集対象サーバに配布されるファイル一覧」を参照してください。

注意事項

クラスタソフトにコマンドを登録する際には，次のことに注意してください。

- admhastart コマンドを登録する場合は，JP1/Base の論理ホスト環境の起動，admhastart コマンドの実行，共有ディスク上に監査ログを出力する収集対象製品の起動，の順になるように設定してください。
- admhastop コマンドを登録する場合は，共有ディスク上に監査ログを出力する収集対象製品の停止，admhastop コマンドの実行，JP1/Base の論理ホスト環境の停止，の順になるように設定してください。

次に，コマンド登録方法の概要をクラスタソフトごとに説明します。登録方法の詳細については，各クラスタソフトのマニュアルを参照してください。

(a) HP Serviceguard の場合

HP Serviceguard では JP1/Audit Management - Manager の定義を，共有ディスク上に監査ログを出力する収集対象製品，および JP1/Base と同じパッケージに登録します。また，「プロセスを終了させないスクリプト」を作成して，パッケージ制御スクリプトの SERVICE_CMD に指定する監視コマンドに登録します。

次に，スクリプトの作成，パッケージ構成ファイルの編集，およびパッケージ制御スクリプトの編集について説明します。

■ スクリプトの作成

ここでは「プロセスを終了させないスクリプト」を作成します。スクリプトは，実行系および待機系のそれぞれで作成し，実行系と待機系で同じパスに配置してください。

スクリプトの作成例を次に示します。ここではファイル名を「nop.sh」と仮定します。

```
#!/bin/sh

INTERVAL_TIME=2147483647
while true; do
    sleep ${INTERVAL_TIME}
done
```

■ パッケージ構成ファイルの編集

パッケージ構成ファイルにサービス名などを設定します。パッケージ構成ファイルは実行系で編集してから，待機系にコピーしてください。編集の際に設定する項目を，次の表に示します。

表 6-13　パッケージ構成ファイルの設定項目

項番	設定項目	設定内容
1	SERVICE_NAME	サービス名を指定します。クラスタ内で一意となる名称を指定してください。
2	SERVICE_FAIL_FAST_ENABLED	NO を指定します。
3	SERVICE_HALT_TIMEOUT	停止のタイムアウト時間（単位：秒）を指定します。

パッケージ構成ファイルの設定例を次に示します。

```
SERVICE_NAME                    jp1netmaudit_1
SERVICE_FAIL_FAST_ENABLED       NO
SERVICE_HALT_TIMEOUT            300
```

■ パッケージ制御スクリプトの編集

パッケージ制御スクリプトに，サービス名や作成したスクリプトなどを設定します。パッケージ制御スクリプトは実行系で編集してから，待機系にコピーしてください。編集の際に設定する項目を，次に示します。

- SERVICE_NAME の追加
  パッケージ構成ファイルの SERVICE_NAME の値を指定します。
- SERVICE_CMD の追加
  作成したスクリプト（nop.sh）をフルパスで指定します。
- 起動処理の追加
  起動コマンドの設定個所で，JP1/Base が起動したあとで admhastart コマンドを実行するように設定します。
- 停止処理の追加
  停止コマンドの設定個所で，JP1/Base が停止するより前に admhastop コマンドを実行するように設定します。

パッケージ制御スクリプトの設定例を次に示します。

```
.
.
SERVICE_NAME[0]="jp1base_1"
SERVICE_CMD[0]="/opt/jp1/hatool/bin/jp1_base.sh -m -h hpipfpkg1 -l"
SERVICE_RESTART[0]=""

SERVICE_NAME[1]="jp1netmaudit_1"
SERVICE_CMD[1]="/opt/jp1netmaudit/manager/bin/nop.sh"
SERVICE_RESTART[1]=""
.
.
function customer_defined_run_cmds
{

/opt/jp1/hatool/bin/jp1_base.sh -s -h 論理ホスト名 -l
/opt/jp1netmaudit/manager/bin/admhastart 論理ホスト名

    test_return 51
}

function customer_defined_halt_cmds
{

/opt/jp1netmaudit/manager/bin/admhastop 論理ホスト名
/opt/jp1/hatool/bin/jp1_base.sh -t -h 論理ホスト名 -l

    test_return 52
}
.
.
```

注意事項

SERVICE_NAME，SERVICE_CMD，および SERVICE_RESTART に指定する配列の添え字には，0 から始まる連続した数字を指定してください。重複した数字は指定しないでください。

(b) PowerHA の場合

PowerHA では，JP1/Audit Management - Manager 用のアプリケーション・サーバーを作成して，リソース・グループへ登録します。ただし，アプリケーション・サーバー作成時に指定する始動スクリプト，および停止スクリプトには引数の指定ができません。そこで，admhastart コマンドおよび admhastop コマンドを実行するスクリプトを作成し，これをアプリケーション・サーバーの始動スクリプトおよび停止スクリプトとして登録します。

次に，スクリプトの作成，アプリケーション・サーバーの設定，リソース・グループへの登録，および設定の同期化について説明します。

■ スクリプトの作成

ここでは，admhastart コマンドおよび admhastop コマンドを実行するスクリプトを作成します。スクリプトは，実行系および待機系のそれぞれで作成し，実行系と待機系で同じパスに配置してください。

スクリプトの作成例を次に示します。ここでは始動スクリプトを「auditstart.sh」，停止スクリプトを「auditstop.sh」と仮定します。

- 始動スクリプト（auditstart.sh）の作成例：

```
#!/bin/sh

LOGICAL_HOST_NAME=論理ホスト名

if [ -x /opt/jp1netmaudit/manager/bin/admhastart ]; then
    /opt/jp1netmaudit/manager/bin/admhastart ${LOGICAL_HOST_NAME}
    RET=$?
else
    RET=1
fi

exit ${RET}
```

- 停止スクリプト（auditstop.sh）の作成例：

```
#!/bin/sh

LOGICAL_HOST_NAME=論理ホスト名

if [ -x /opt/jp1netmaudit/manager/bin/admhastop ]; then
    /opt/jp1netmaudit/manager/bin/admhastop ${LOGICAL_HOST_NAME}
    RET=$?
else
    RET=1
fi

exit ${RET}
```

■ アプリケーション・サーバーの設定

JP1/Audit Management - Manager 用のアプリケーション・サーバーを作成します。作成の際に設定する項目を，次の表に示します。

表 6-14　アプリケーション・サーバーの設定項目

項番	設定項目	設定内容
1	サーバー名	任意の名称を指定します。
2	始動スクリプト	作成した始動スクリプト（auditstart.sh）をフルパスで指定します。
3	停止スクリプト	作成した停止スクリプト（auditstop.sh）をフルパスで指定します。
4	アプリケーション・モニター名	何も指定しません。

■ リソース・グループへの登録

作成したアプリケーション・サーバーを，リソース・グループに登録します。なお，登録の際は，共有ディスク上に監査ログを出力する収集対象製品，および JP1/Base と同じグループを指定してください。

■ 設定の同期化

リソース・グループへの登録までが完了したら，クラスタ設定を同期化してください。

(c)　VERITAS Cluster Server の場合

VERITAS Cluster Server では，Application エージェントを使用してコマンドを登録します。Application エージェントでは，起動コマンドと停止コマンド以外に，強制停止コマンドと監視コマンドの設定が必要です。そこで，それぞれの処理を実行するスクリプトを作成して，リソース定義に登録します。

次に，スクリプトの作成，およびリソースの定義について説明します。

■ スクリプトの作成

ここでは，起動，停止，強制停止，および監視の各処理を実行するスクリプトを作成します。スクリプトは，実行系および待機系のそれぞれで作成し，実行系と待機系で同じパスに配置してください。

各スクリプトで処理する内容を，次に示します。

- 起動

  admhastart コマンドを実行します。また，開始に成功した場合はオンラインを示す一時ファイルを作成します。
- 停止

  admhastop コマンドを実行します。また，停止に成功した場合は起動時に作成した一時ファイルを削除します。
- 強制停止

  起動時に作成した一時ファイルが存在するかどうかを確認し，存在する場合は削除します。
- 監視

起動時に作成した一時ファイルが存在するかどうかを監視します。存在する場合は戻り値として「110」を，存在しない場合は戻り値として「100」を返します。

スクリプトの作成例を次に示します。ここでは，上記四つの処理を実行するスクリプトを「admhactrl.sh」と仮定します。

```
#!/bin/sh
#  Syntax:  admhactrl logical-host-name {-s|-t|-c|-m}
#  Flags :  -s  : start
#           -t  : terminate
#           -c  : clear
#           -m  : monitor

# StartProgram
if [ "$2" = "-s" ]; then
    /opt/jp1netmaudit/manager/bin/admhastart $1
    RET=$?
    case ${RET} in
        0|7|8)
            touch /opt/jp1netmaudit/manager/bin/.$1 > /dev/null 2>&1
            ;;
        *)  ;;
    esac
else
# StopProgram
if [ "$2" = "-t" ]; then
    /opt/jp1netmaudit/manager/bin/admhastop $1
    RET=$?
    if [ $RET -eq 0 ]; then
        rm -f /opt/jp1netmaudit/manager/bin/.$1 > /dev/null 2>&1
    fi
else
# CleanProgram
if [ "$2" = "-c" ]; then
    if [ -f /opt/jp1netmaudit/manager/bin/.$1 ]; then
        rm -f /opt/jp1netmaudit/manager/bin/.$1 > /dev/null 2>&1
    fi
    RET=0
else
# MonitorProgram
if [ "$2" = "-m" ]; then
    #ファイルが存在する場合は開始状態とする
    if [ -f /opt/jp1netmaudit/manager/bin/.$1 ]; then
        RET=110
    else
        RET=100
    fi
else
    RET=1
fi
fi
fi
fi

exit $RET
```

■ リソースの定義

クラスタ構成の設定ファイル（/etc/VRTSvcs/conf/config/main.cf）を編集して，リソース定義を追加します。起動，停止，強制停止，および監視の各コマンドに，作成したスクリプトを指定します。なお，リソースは，共有ディスク上に監査ログを出力する収集対象製品，およびJP1/Baseと同じグループに登録してください。

クラスタ構成の設定ファイルの定義例を次に示します。

```
Application jp1netmaudit_1 (
    StartProgram = "/opt/jp1netmaudit/manager/bin/admhactrl.sh 論理ホスト名 -s"
    StopProgram = "/opt/jp1netmaudit/manager/bin/admhactrl.sh 論理ホスト名 -t"
    CleanProgram = "/opt/jp1netmaudit/manager/bin/admhactrl.sh 論理ホスト名 -c"
    MonitorProgram = "/opt/jp1netmaudit/manager/bin/admhactrl.sh 論理ホスト名 -m"
    Critical = 0
)
```

また，JP1/Baseのリソースが起動したあとにJP1/Audit Management - Managerのリソースが起動するように，依存関係を設定してください。例えば，JP1/Baseのリソース名が「jp1base_1」の場合は，次のように設定します。

```
jp1netmaudit_1 requires jp1base_1
```

(d) HAモニタの場合

HAモニタではadmhastartコマンドおよびadmhastopコマンドを実行するスクリプトを作成して，そのスクリプトをservers（サーバ対応定義ファイル）に登録します。

次に，スクリプトの作成，およびservers（サーバ対応定義ファイル）の編集について説明します。

■ スクリプトの作成

ここでは，admhastartコマンドおよびadmhastopコマンドを実行するスクリプトを作成します。スクリプトは，実行系および待機系のそれぞれで作成し，実行系と待機系で同じパスに配置してください。

スクリプトの作成例を次に示します。ここでは始動スクリプトを「auditstart.sh」，停止スクリプトを「auditstop.sh」と仮定します。

- 始動スクリプト（auditstart.sh）の作成例：

```
#!/bin/sh

LOGICAL_HOST_NAME=論理ホスト名

if [ -x /opt/jp1netmaudit/manager/bin/admhastart ]; then
    /opt/jp1netmaudit/manager/bin/admhastart ${LOGICAL_HOST_NAME}
    RET=$?
    case ${RET} in
        0|7|8)
            RET=0
            ;;
```

```
        *)  ;;
    esac
else
    RET=1
fi

exit ${RET}
```

- 停止スクリプト（auditstop.sh）の作成例：

```
#!/bin/sh

LOGICAL_HOST_NAME=論理ホスト名

if [ -x /opt/jp1netmaudit/manager/bin/admhastop ]; then
    /opt/jp1netmaudit/manager/bin/admhastop ${LOGICAL_HOST_NAME}
    RET=$?
else
    RET=1
fi

exit ${RET}
```

■ servers（サーバ対応定義ファイル）の編集

servers ファイルに JP1/Audit Management - Manager のサーバ定義を追加します。実行系および待機系のそれぞれで編集してください。

実行系の servers

group には，共有ディスク上に監査ログを出力する収集対象製品，および JP1/Base と同じグループを指定します。また，parent には JP1/Base のサーバ識別名を指定します。

```
server  name            /opt/jp1netmaudit/manager/bin/auditstart.sh  ,
        alias           audit1                                       ,
        acttype         monitor                                      ,
        termcommand      "/opt/jp1netmaudit/manager/bin/auditstop.sh",
        initial         online                                       ,
        group           group1                                       ,
        parent          server1                                      ,
        servexec_retry  0                                            ,
        waitserv_exec   yes                                          ,
        retry_stable    300                                          ;
```

待機系の servers

実行系サーバと同じ内容を設定します。ただし，次に示す項目「initial」については，待機系サーバなので「standby」を設定してください。

```
            .               .
            .               .
        initial         standby                                      ,
            .               .
            .               .
```

6.6　監査ログ管理サーバで監査ログを収集するための設定（クラスタ環境）

実行系サーバで，監査ログを収集するための設定をします。

設定内容および手順については「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

6.7　監査ログ管理サーバの開始・停止（クラスタ環境）

ここでは，監査ログ管理サーバをクラスタ環境で運用する場合の開始手順と停止手順について説明します。

6.7.1　監査ログ管理サーバを開始する（クラスタ環境）

監査ログ管理サーバを開始するときは，クラスタソフトを使用して監査ログ管理サーバクラスタグループに含まれるすべてのリソースをオンラインにします。

オンラインにするリソースを次に示します。

- IP アドレスリソース※
- ネットワーク名リソース※
- 共用ディスクリソース
- JP1/NETM/Audit - Manager サービスのリソース
- JP1/NETM/Audit - Manager Convert サービスのリソース
- JP1/NETM/Audit - Manager Define サービスのリソース
- JP1/NETM/Audit - Manager SubCollect サービスのリソース
- HiRDB/ClusterService _AL1 サービスのリソース
- Microsoft Internet Information Services のリソース

注※

IP アドレスリソースとネットワーク名リソースは，Windows Server 2003 の場合にオンラインにするリソースです。Windows Server 2012 または Windows Server 2008 の場合は，クライアントアクセスポイントのリソースをオンラインにしてください。

6.7.2　監査ログ管理サーバを停止する（クラスタ環境）

監査ログ管理サーバを停止するときは，次の操作を実施します。

1. クラスタソフトで JP1/Audit Management - Manager のサービスのリソースをオフラインにする。

   オフラインにする JP1/Audit Management - Manager のサービスのリソースを次に示します。

   - JP1/NETM/Audit - Manager サービスのリソース
   - JP1/NETM/Audit - Manager Convert サービスのリソース
   - JP1/NETM/Audit - Manager Define サービスのリソース
   - JP1/NETM/Audit - Manager SubCollect サービスのリソース

2. admdbstop コマンドを実行してデータベースを停止する。

次のコマンドを実行します。

```
admdbstop
```

admdbstop コマンドの詳細については「12.　コマンド」の「admdbstop（データベースの停止）」を参照してください。

3. クラスタソフトで監査ログ管理サーバクラスタグループの残りのリソースをオフラインにする。

オフラインにするリソースを次に示します。

- クライアントアクセスポイントのリソース
- 共用ディスクリソース
- HiRDB/ClusterService _AL1 サービスのリソース
- Microsoft Internet Information Services のリソース

6.7.3　監査ログ管理サーバを開始または停止する場合の注意事項（クラスタ環境）

- クラスタ環境のシステム上で動作するサービスは，コントロールパネルの「管理ツール」の「サービス」から開始または停止しないでください。
- クラスタ環境でコマンドを実行する場合に，JP1/Audit Management - Manager を停止する必要があるときは，JP1/Audit Management - Manager のサービスのリソースをオフラインにしてください。
- 「サービス」の JP1/Audit Management - Manager のサービスは自動起動する設定にしないでください。すでに設定している場合は，実行系サーバと待機系サーバのそれぞれで，JP1/Audit Management - Manager のサービスの起動方法を「手動」に戻してください。
- フェールオーバー発生後，アクティブ状態になっていない World Wide Web Publishing Service サービスは停止してください。

6.8　監査ログ収集対象サーバの開始・停止（クラスタ環境）

ここでは，監査ログ収集対象サーバをクラスタ環境で運用する場合の開始手順と停止手順について説明します。

6.8.1　監査ログ収集対象サーバを開始する（クラスタ環境）

Windows 環境の場合

共有ディスクに出力される監査ログの収集を開始するときは，クラスタソフトに登録した JP1/NETM/Audit LogTrap **論理ホスト名**サービスのリソースをオンラインにします。

UNIX 環境の場合

共有ディスク上に出力される監査ログの収集を開始するときは，クラスタソフトに登録した admhastart コマンドを，クラスタソフトから起動します。admhastart コマンドをクラスタソフトへ登録する方法については「6.5.5(2)　UNIX の場合」を参照してください。

6.8.2　監査ログ収集対象サーバを停止する（クラスタ環境）

Windows 環境の場合

共有ディスクに出力される監査ログの収集を停止するときは，クラスタソフトに登録した JP1/NETM/Audit LogTrap **論理ホスト名**サービスのリソースをオフラインにします。

UNIX 環境の場合

共有ディスクに出力される監査ログの収集を停止するときは，クラスタソフトに登録した admhastop コマンドを実行します。admhastop コマンドをクラスタソフトへ登録する方法については「6.5.5(2) UNIX の場合」を参照してください。

6.8.3　監査ログ収集対象サーバを開始または停止する場合の注意事項（クラスタ環境）

- クラスタ環境のシステム上で動作するサービスは，コントロールパネルの「管理ツール」の「サービス」から開始または停止しないでください。
- OS が Windows の場合，クラスタ環境のシステムに登録する次のサービスは「手動」に設定してください。
  - JP1/Base Event **監査ログ専用イベントサーバ名（論理ホスト用）**
  - JP1/NETM/Audit LogTrap **論理ホスト名**
- クラスタ環境で共有ディスク上の監査ログを収集する場合，実行系から待機系にフェールオーバーするときに出力された監査ログは，収集されないことがあります。

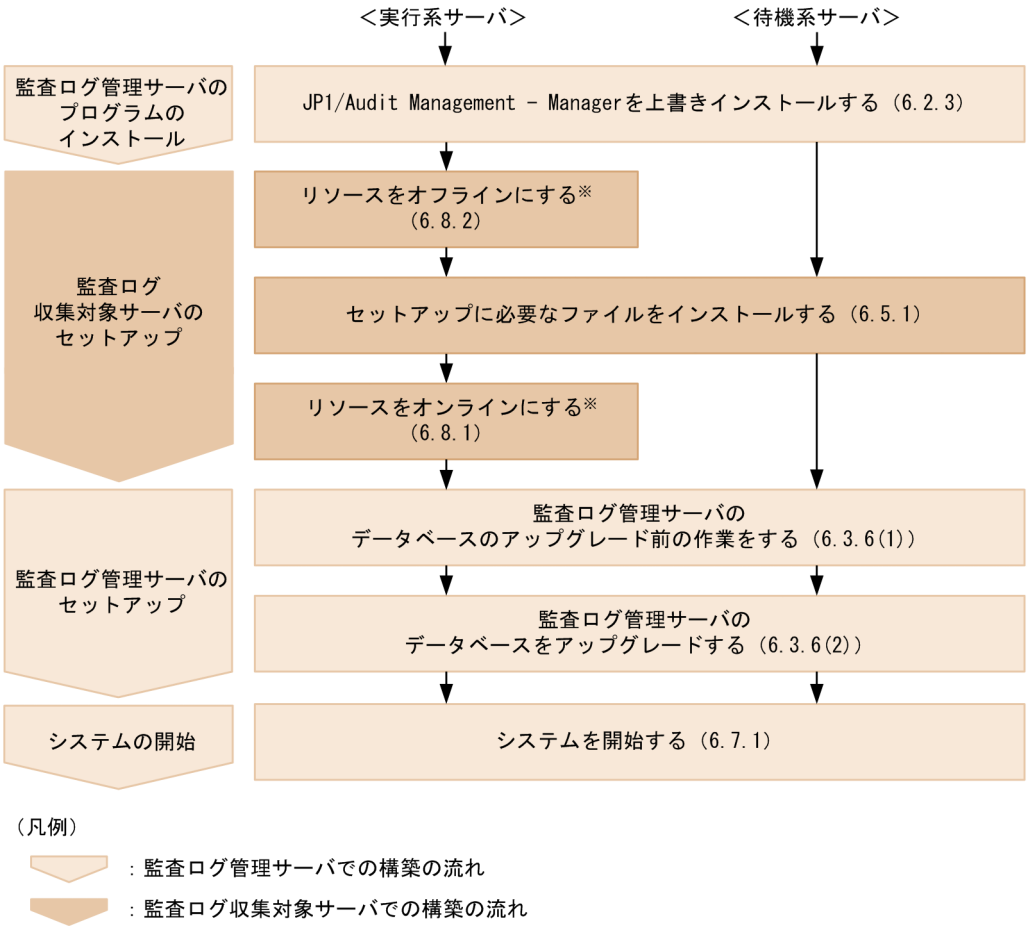
6.9 JP1/Audit Management - Manager のバージョンアップ（クラスタ環境）

クラスタ環境で，JP1/Audit Management - Manager をバージョンアップする場合の作業の流れおよび手順について説明します。

6.9.1 JP1/Audit Management - Manager のバージョンアップの流れ（クラスタ環境）

クラスタ環境での各サーバの構築の流れを次の図に示します。各項目の内容については，括弧内の個所を参照してください。

図 6-2 各サーバでの構築の流れ（クラスタ環境でバージョンアップする場合）



（凡例）

：監査ログ管理サーバでの構築の流れ

：監査ログ収集対象サーバでの構築の流れ

注※ 監査ログ収集対象サーバがWindowsの場合だけ実施してください。

6.9.2 JP1/Audit Management - Manager のバージョンアップの手順（クラスタ環境）

クラスタ環境で，JP1/Audit Management - Manager をバージョンアップする場合のインストールおよびセットアップ手順を次に示します。

1. 監査ログ管理サーバで，JP1/Audit Management - Manager を上書きインストールする。

   実行系サーバと待機系サーバの両方に，JP1/Audit Management - Manager を上書きインストールします。上書きインストールの手順については「6.2.3　JP1/Audit Management - Manager を上書きインストールする（クラスタ環境）」を参照してください。

2. 監査ログ収集対象サーバでリソースをオフラインにする。

   監査ログ収集対象サーバが Windows の場合，実行系サーバでリソースをオフラインにします。リソースをオフラインにする方法については「6.8.2　監査ログ収集対象サーバを停止する（クラスタ環境）」を参照してください。

3. 監査ログ収集対象サーバのセットアップに必要なファイルをインストールする。

   インストールする方法については「6.5.1　セットアップに必要なファイルをインストールする（クラスタ環境）」を参照してください。

4. 監査ログ収集対象サーバでリソースをオンラインにする。

   監査ログ収集対象サーバが Windows で共有ディスク上に出力される監査ログを収集する場合，実行系サーバでリソースをオンラインにします。リソースをオンラインにする方法については「6.8.1　監査ログ収集対象サーバを開始する（クラスタ環境）」を参照してください。

5. 監査ログ管理サーバで JP1/Audit Management - Manager のデータベースをアップグレードする。

   データベースのアップグレード手順については「6.3.6　監査ログ管理サーバのデータベースをアップグレードする（クラスタ環境）」を参照してください。

6. システムを開始する。

   システムを開始する方法については「6.7　監査ログ管理サーバの開始・停止（クラスタ環境）」を参照してください。

監査ログを収集したいプログラムの監査ログ収集対象サーバでの設定内容については「6.5　監査ログ収集対象サーバのセットアップ（クラスタ環境）」を参照してください。また，監査ログ管理サーバでの設定内容については「6.6　監査ログ管理サーバで監査ログを収集するための設定（クラスタ環境）」を参照してください。

6.10　監査ログ収集対象の解除（クラスタ環境）

ここでは，共有ディスク上から収集している監査ログのうち，その一部またはすべての収集をやめる場合に必要な手順を説明します。

手順は，収集をやめる監査ログの種類や範囲によって異なります。次に示すそれぞれの場合について，手順を説明します。

- ファイルに出力される監査ログの収集をやめる
- すべての監査ログの収集をやめる

また，「ローカルディスク上から収集している監査ログ」の収集をやめる方法については「5.13　監査ログ収集対象の解除」を参照してください。

6.10.1　ファイルに出力される監査ログの収集をやめる

ファイルに出力される監査ログの収集をやめるには，監査ログ管理サーバ上の監査ログ収集マネージャで，監査ログ収集対象を解除します。この作業の詳細については「5.13.1　ファイルに出力される監査ログの収集をやめる」を参照してください。

6.10.2　すべての監査ログの収集をやめる

すべての監査ログの収集をやめるには，監査ログ管理サーバおよび監査ログ収集対象サーバでそれぞれ作業を行ってください。作業の概要を次の表に示します。

表 6-15　すべての監査ログの収集をやめる作業の概要

項番	作業対象となるサーバ	作業の概要
1	監査ログ管理サーバ	監査ログ収集対象の解除
2	監査ログ収集対象サーバ	リソースの削除（Windows の場合）※ コマンドの削除（UNIX の場合）※
3		監査ログ専用イベントサーバのデーモンの停止（UNIX の場合）※
4		監査ログ専用イベントサーバの削除
5		論理ホスト環境の削除
6		セットアップ時にインストールしたファイルの削除

注※

これらの作業は実行系サーバで実施してください。

(1)　監査ログ管理サーバでの作業

監査ログ収集マネージャで，すべての監査ログ収集対象を解除します。この作業の詳細については「5.13.1 ファイルに出力される監査ログの収集をやめる」を参照してください。

(2)　監査ログ収集対象サーバでの作業

最初に実行系サーバで作業を実施し，次に，同様の作業を待機系サーバでも実施します。

(a)　実行系サーバでの作業

■ リソースまたはコマンドの削除

手順を次に示します。ただし，Windows の場合と UNIX の場合とで，手順が異なります。Windows の場合はリソースを，UNIX の場合はコマンドを削除してください。

Windows の場合

1. クラスタソフトの JP1/NETM/Audit LogTrap 論理ホスト名サービスおよび JP1/Base Event 監査ログ専用イベントサーバ名サービスのリソースをオフラインにする。
2. クラスタソフトからリソースを削除する。
   セットアップ時にクラスタソフトに登録した次のリソースを削除します。

表 6-16　クラスタソフトから削除するリソース

リソース名	機能
JP1_NETM_Audit LogTrap 論理ホスト名	ログトラップ制御サービス
JP1_Base_Event 監査ログ専用イベントサーバ名	監査ログ専用イベントサーバのサービス

UNIX の場合

セットアップ時にクラスタソフトに登録した次のコマンドを削除してください。

表 6-17　クラスタソフトから削除するコマンド

コマンド名	機能
admhastart 論理ホスト名	起動
admhastop 論理ホスト名	停止

■ 監査ログ専用イベントサーバのデーモンの停止

監査ログ専用イベントサーバのデーモンが起動している場合，監査ログ専用イベントサーバのデーモンを停止します。この作業は，OS が UNIX の場合に必要となる作業です。次のコマンドを実行してください。

```
/opt/jp1base/bin/jevstop 監査ログ専用イベントサーバ名
```

jevstop コマンドの詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

■ 監査ログ専用イベントサーバの削除

admagtsetup コマンドを実行して，監査ログ専用イベントサーバを削除します。次のコマンドを実行してください。

```
admagtsetup -h 論理ホスト名 -c online -u
```

admagtsetup コマンドの詳細については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

■ 論理ホスト環境の削除

admhasetup コマンドを実行して論理ホスト環境を削除します。次のコマンドを実行してください。

```
admhasetup -h 論理ホスト名 -c online -u
```

admhasetup コマンドの詳細については「12.　コマンド」の「admhasetup（論理ホスト環境の作成）」を参照してください。

■ セットアップ時にインストールしたファイルの削除

admagtinstall コマンドを実行して，セットアップ時に監査ログ収集対象サーバにインストールしたファイルを削除します。次のコマンドを実行してください。

```
admagtinstall -u
```

admagtinstall コマンドの詳細については「12.　コマンド」の「admagtinstall（監査ログ収集対象サーバのファイルのインストール）」を参照してください。

なお，admagtinstall コマンドを実行して削除されるのは，セットアップ時に admagtinstall コマンドを実行してインストールしたファイルだけです。インストール後に作成された設定ファイルやログファイルなどは削除されません。また，インストール後に作成された設定ファイルやログファイルを含むフォルダも削除されません。削除されなかったファイルやフォルダは，必要に応じて手動で削除してください。

(b)　待機系サーバでの作業

待機系サーバでの作業は，共有ディスクを待機系に切り替えてから実施します。

■ 監査ログ専用イベントサーバの削除

admagtsetup コマンドを実行して監査ログ専用イベントサーバを削除します。次のコマンドを実行してください。実行系サーバでは「online」と入力した部分が，待機系では「standby」になります。

```
admagtsetup -h 論理ホスト名 -c standby -u
```

admagtsetup コマンドの詳細については「12.　コマンド」の「admagtsetup（監査ログ専用イベントサーバの環境セットアップ）」を参照してください。

■ 論理ホスト環境の削除

待機系サーバ上で，admhasetup コマンドを実行して論理ホスト環境を削除します。次のコマンドを実行してください。実行系サーバでは「online」と入力した部分が，待機系では「standby」になります。

```
admhasetup -h 論理ホスト名 -c standby -u
```

admhasetup コマンドの詳細については「12.　コマンド」の「admhasetup（論理ホスト環境の作成）」を参照してください。

■ セットアップ時にインストールしたファイルの削除

admagtinstall コマンドを実行して，セットアップ時に監査ログ収集対象サーバにインストールしたファイルを削除します。次のコマンドを実行してください。

```
admagtinstall -u
```

admagtinstall コマンドの詳細については「12.　コマンド」の「admagtinstall（監査ログ収集対象サーバのファイルのインストール）」を参照してください。

なお，admagtinstall コマンドを実行して削除されるのは，セットアップ時に admagtinstall コマンドを実行してインストールしたファイルだけです。インストール後に作成された設定ファイルやログファイルなどは削除されません。また，インストール後に作成された設定ファイルやログファイルを含むフォルダも削除されません。削除されなかったファイルやフォルダは，必要に応じて手動で削除してください。

6.11　フェールオーバー発生後の対処

監査ログ管理サーバがフェールオーバーするタイミングの例を次に示します。

- JP1/Audit Management - Manager が起動管理機能（Windows のサービス）上で終了した状態になった場合
- ハードウェアにトラブルが起きた場合
- OS にトラブルが起きた場合
- 電源が切れた場合
- ネットワークにトラブルが起きた場合
- Microsoft Internet Information Services のサービスが停止した場合

フェールオーバーが発生すると，待機系サーバが起動して実行系サーバの処理を引き継ぎます。

監査ログ管理データベースへのデータ格納中にフェールオーバーが発生した場合は，ログファイルで，データベースにすべてのデータが格納されているかを確認します。データの格納が完了していない場合は，手動でデータを格納してください。

また，正規化ルールエディタの起動中に実行系サーバでトラブルが発生した場合は，JP1/NETM/Audit - Manager Define サービスのフェールオーバー後，待機系サーバで正規化ルールエディタを再起動してください。

7 監査ログ管理画面での運用

監査ログ管理画面では，監査ログの検索，監査ログの集計，監査ログの統計，およびバックアップ操作の履歴確認ができます。この章では，監査ログ管理画面の操作方法および監査ログ管理画面の各画面の表示設定について説明します。

7.1　監査ログ管理画面での操作

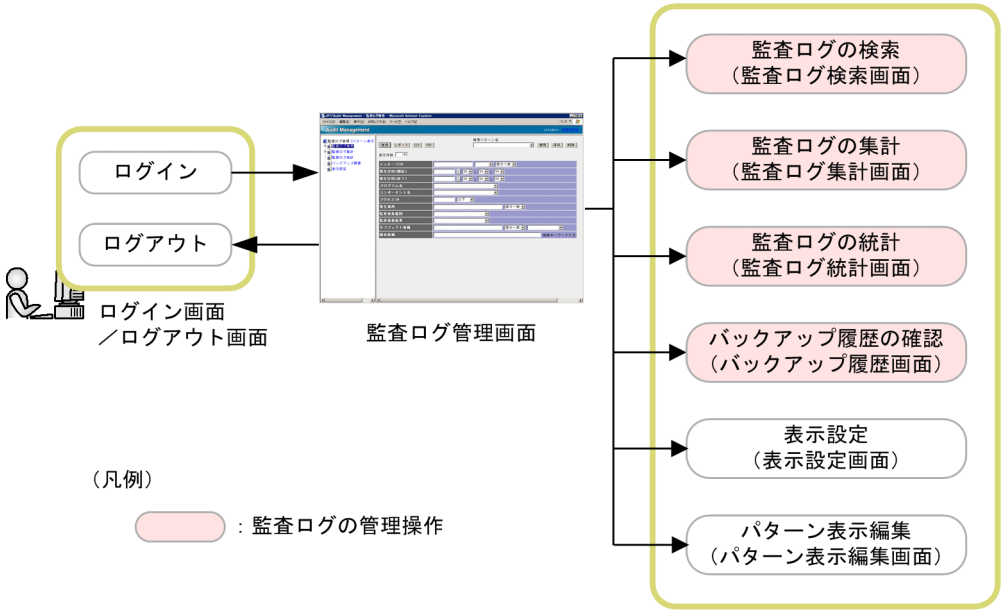
監査ログ管理画面で，監査ログ管理データベースに収集した監査ログを管理することができます。

この節では，監査ログ管理画面の操作の流れと監査ログ管理画面の各画面でできることを説明します。監査ログ管理画面の各部の名称と使い方については「11.　監査ログ管理画面」を参照してください。

7.1.1　監査ログ管理画面の操作の流れ

監査ログ管理画面の操作の流れを次の図に示します。

図 7-1　監査ログ管理画面の操作の流れ



監査ログ管理画面を使用するには，Web ブラウザとして Internet Explorer の設定が必要です。Internet Explorer の設定については「5.11　監査ログ管理画面を使うための Internet Explorer の設定」を参照してください。

監査ログ管理画面の操作手順を次に示します。

1. 監査ログ管理画面にログインする。

   監査ログ管理画面へのログインについては「7.2　監査ログ管理画面へのログインとログアウト」を参照してください。

2. 監査ログ管理画面の左フレームの機能ツリーで，監査ログ管理機能のメニューを選択する。

   選択したメニューに対応する画面が監査ログ管理画面の右フレームに表示されます。監査ログ管理画面の各画面でできることについては「7.1.2　監査ログ管理機能」を参照してください。

なお，監査ログ管理画面の表示は編集できます。監査ログ管理画面の各画面の表示設定については「7.7 監査ログ管理画面の表示設定」を参照してください。機能ツリーのパターン表示編集については「7.8 機能ツリーのパターン表示編集」を参照してください。

3. **操作が終了したら，監査ログ管理画面を終了する。**

   監査ログ管理画面からのログアウトします。監査ログ管理画面からのログアウトについては「7.2　監査ログ管理画面へのログインとログアウト」を参照してください。

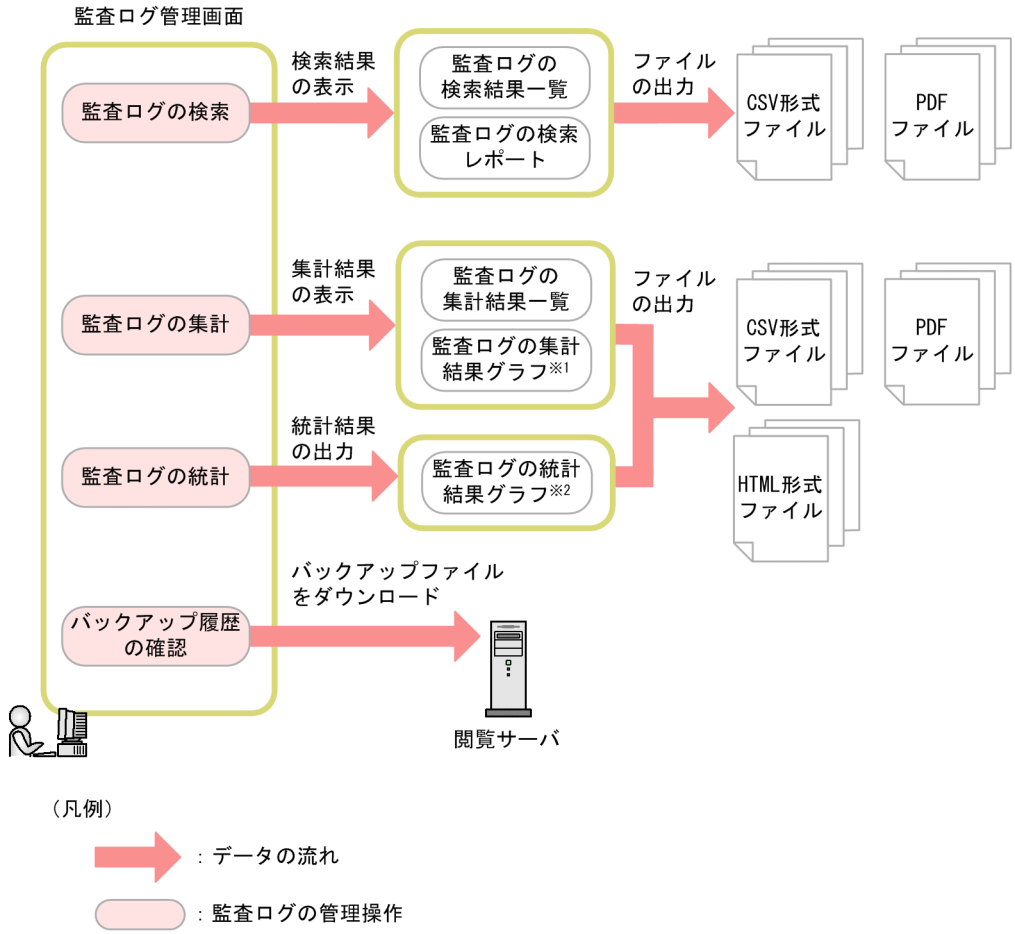
7.1.2　監査ログ管理機能

監査ログ管理画面では，監査ログについて次の管理ができます。

- 監査ログの検索
- 監査ログの集計
- 監査ログの統計
- バックアップ履歴の確認

監査ログ管理画面でできる監査ログの管理操作の概要を次の図に示します。

図 7-2　監査ログ管理画面での監査ログの管理操作



（凡例）

：データの流れ

：監査ログの管理操作

注※1　監査ログの集計結果グラフは，CSV形式ファイルおよびPDFファイルでの出力はできません。

注※2　監査ログの統計結果グラフは，PDFファイルでの出力はできません。

監査ログ管理画面でできる監査ログの管理機能について説明します。

監査ログの検索

収集された監査ログは条件を指定して検索できます。検索した結果は画面上で確認したり，CSV 形式ファイルや PDF ファイルに出力したりできます。また，検索結果をレポート形式で表示することもできます。

監査ログの検索については「7.3　監査ログ検索」を参照してください。

監査ログの集計

収集された監査ログは条件を指定して集計できます。集計した結果は画面上で確認したり，CSV 形式ファイルや PDF ファイルに出力したりできます。また，集計結果はグラフ表示することもできます。

監査ログの集計については「7.4　監査ログ集計」を参照してください。

監査ログの統計

収集された監査ログの推移が把握できる統計結果をグラフ形式で表示できます。統計結果は画面上で確認したり，CSV 形式ファイルに出力したりできます。

監査ログの統計については「7.5　監査ログ統計」を参照してください。

バックアップ履歴の確認

監査ログをバックアップした履歴を検索し，バックアップファイルをダウンロードできます。

バックアップ履歴の確認については「7.6　バックアップ履歴の確認」を参照してください。

7.1.3　監査ログ管理画面の表示編集

監査ログ管理画面の表示編集について説明します。

表示設定

監査ログ管理画面の表示設定画面で，監査ログ管理画面の各画面で使用する項目の表示設定ができます。また，監査ログ統計画面で指定する統計出力条件のデフォルトも変更できます。表示設定については「7.7　監査ログ管理画面の表示設定」を参照してください。

パターン表示編集

監査ログ管理画面のパターン表示編集画面で，機能ツリーのパターン表示について編集できます。パターン表示編集については「7.8　機能ツリーのパターン表示編集」を参照してください。

7.2　監査ログ管理画面へのログインとログアウト

この節では，JP1/Audit Management - Manager の監査ログ管理画面へのログインとログアウトの手順について説明します。

7.2.1　監査ログ管理画面にログインする

監査ログ管理画面を使用するには，Web ブラウザで専用のログイン画面を呼び出し，ログインする必要があります。監査ログ管理画面へログインする手順を次に示します。

1. Web ブラウザを起動して，監査ログ管理画面のログイン画面を呼び出す。

   監査ログ管理画面のログイン画面を呼び出すには，Web ブラウザから URL にアクセスします。監査ログ管理画面のログイン画面の URL を次に示します。

   ```
   http://ホスト名※/jp1netmaudit/
   ```

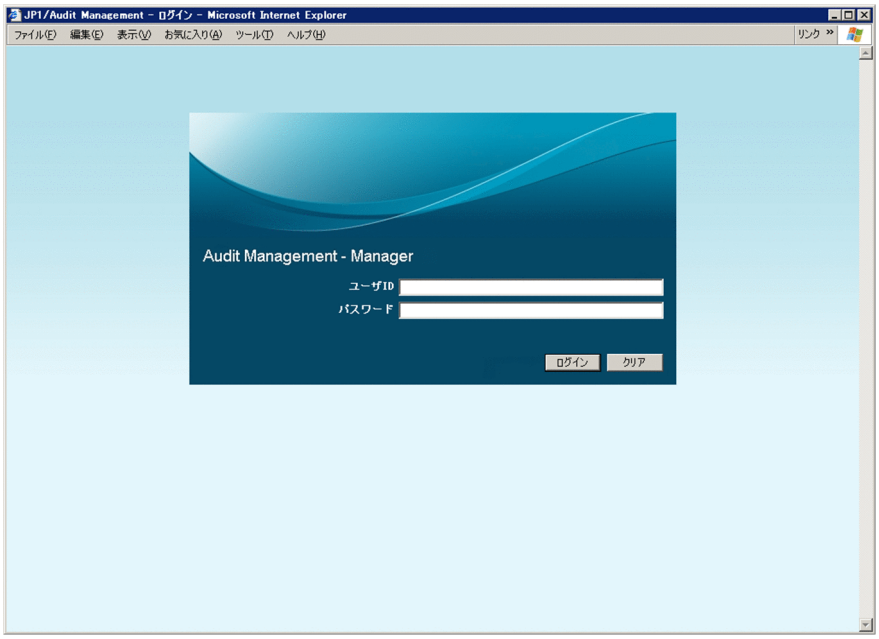
   注※

   TCP ポート番号が「80」でない場合は，「**ホスト名:TCP ポート番号**」になります。TCP ポート番号は Microsoft Internet Information Services の「既定の Web サイト」で確認してください。「既定の Web サイト」は，Microsoft Internet Information Services のバージョンによって「Default Web Site」と表示されることがあります。

   なお，接続先のサーバがクラスタ構成の場合は，論理ホスト名になります。

   監査ログ管理画面のログイン画面を次に示します。

図 7-3　監査ログ管理画面のログイン画面



「ユーザ ID」

接続先サーバの JP1/Base で登録されている，JP1/Audit Management - Manager の監査ログ管理画面用の JP1 ユーザ名を入力します。

「パスワード」

パスワードを入力します。

［ログイン］ボタン

監査ログ管理画面にログインします。

［クリア］ボタン

「ユーザ ID」および「パスワード」に指定した値がクリアされます。

2. ユーザ ID とパスワードを入力する。

3. ［ログイン］ボタンをクリックする。

JP1 ユーザの認証が成功すると，監査ログ管理画面が表示されます。

注意事項

セキュリティを確保するため，定期的なパスワードの変更をお勧めします。パスワードの変更については，マニュアル「JP1/Base 運用ガイド」を参照してください。

7.2.2 監査ログ管理画面からログアウトする

監査ログ管理画面での操作が終了したら，ログアウトします。監査ログ管理画面からログアウトする手順を次に示します。

1. 画面の右上に表示されている「ログアウト」アンカーをクリックする。

ログアウトが成功すると，「ログアウトに成功しました。」のメッセージが表示されたあと，監査ログ管理画面のログイン画面が表示されます。

図 7-4 「ログアウト」アンカー

なお，監査ログ管理画面のセッションは，Microsoft Internet Information Services のセッションに依存しています。このため，監査ログ管理画面でログアウトの操作をしない場合でも，Microsoft Internet Information Services で設定したタイムアウトの時間になると，自動的にログアウトされます。自動的にログアウトされた状態で画面を操作すると，「サーバとの接続が切断されました。ログインしてください。」のメッセージが監査ログ管理画面のログイン画面に表示されます。

デフォルトのタイムアウトの時間は 20 分です。必要に応じて，Microsoft Internet Information Services でタイムアウトの時間の設定を変更してください。設定方法の詳細については，Microsoft Internet Information Services のヘルプを参照してください。

7.3　監査ログ検索

監査ログ管理画面で必要な条件を指定して，監査ログ管理データベースに収集された監査ログを検索できます。

例えば，次のような条件で監査ログを検索します。

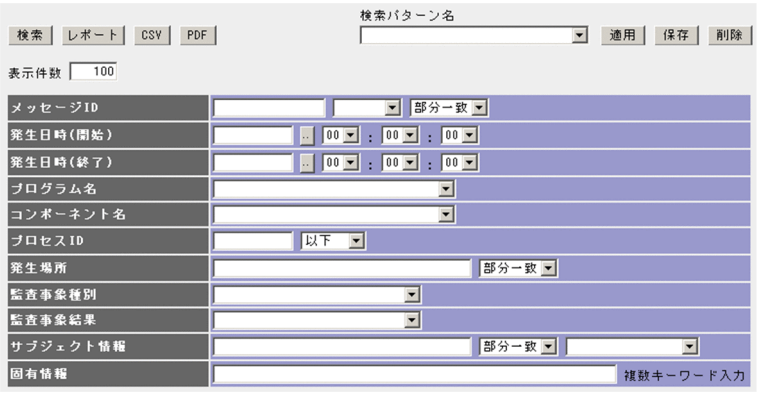
- ログインに失敗したログを検索する。
- ここ一年間に収集された JP1/NETM/DM のログを検索する。
- 指定した期間内にパスワードが変更されているかどうかを検索する。

なお，指定した検索条件を検索パターンとして保存できます。検索パターンとは，監査ログを同じ条件で何度も検索するために保存する検索条件のことであり，同じ検索条件を設定する手間を省くことができます。

監査ログの検索結果は画面上に表示したり，ファイルに出力したりできます。また，監査ログレポート画面で検索結果を見やすくして確認することもできます。

監査ログの検索は，監査ログ検索画面で実行できます。監査ログ検索画面を次に示します。

図 7-5　監査ログ検索画面



この節では，監査ログを検索する手順，検索条件として指定できる項目，検索結果の確認方法，および検索パターンの作成方法を説明します。

監査ログ検索画面の各部の名称と使い方については「11.3　監査ログ検索画面」を参照してください。

7.3.1　監査ログの検索

ここでは収集された監査ログを検索する手順と検索パターンの使用方法について説明します。

(1)　監査ログの検索手順

監査ログを検索する手順を次に示します。

1. 監査ログ検索画面を表示する。

   監査ログ管理画面にログインすると，最初に監査ログ検索画面が表示されます。ほかの画面から遷移する場合は，機能ツリーで「監査ログ検索」をクリックすると，監査ログ検索画面が表示されます。

2. 検索条件を指定する。

   検索条件は，直接入力するか，保存されている検索パターンで指定します。

   指定できる検索条件の詳細については「7.3.2　監査ログの検索条件項目」を参照してください。検索パターンを使用して検索条件を指定する方法については「(2)　検索パターンを利用する」を参照してください。

3. 検索結果を取得する。

   - 画面上で検索結果を確認したい場合は，［検索］ボタンをクリックしてください。
   - CSV 形式ファイルを出力したい場合は，［CSV］ボタンをクリックしてください。
   - PDF ファイルを出力したい場合は，［PDF］ボタンをクリックしてください。
   - レポート形式で検索結果を確認したい場合は，［レポート］ボタンをクリックしてください。

   検索条件に一致した監査ログの検索結果が出力されます。監査ログの検索結果の見方については「7.3.3 監査ログ検索結果の確認」を参照してください。

(2)　検索パターンを利用する

検索パターンを使って，監査ログを検索する手順を次に示します。

1. 検索パターンを選択する。

   次の方法のどちらかで，検索条件として使用する検索パターンを選択します。

   - 監査ログ管理画面の左フレームの機能ツリーで検索パターン名を選択します。
   - 監査ログ検索画面の「検索パターン名」リストで検索パターン名を選択し，［適用］ボタンをクリックします。

   監査ログ検索画面に，検索パターンとして作成した検索条件が表示されます。

2. 必要に応じて検索条件を変更する。

   監査ログ検索画面に表示された検索条件は変更できます。必要に応じて変更してください。

3. 検索結果を取得する。

   ［検索］ボタンをクリックすると，検索条件に一致した監査ログが，監査ログ検索画面の検索結果一覧に表示されます。検索結果をファイルに出力する場合は，［CSV］ボタンや［PDF］ボタンをクリックしてください。検索結果をレポート表示する場合は，［レポート］ボタンをクリックしてください。

手順 2.で変更した検索条件は，検索パターン名を変更しないで［保存］ボタンをクリックすると，変更後の検索パターンで上書きされます。テンプレートの検索パターンを変更して保存したい場合は，別の名称を指定して保存してください。テンプレートの検索パターンについては「11.12　検索パターンおよび集計パターンの一覧」を参照してください。

検索パターン名を変更して監査ログ検索画面で［保存］ボタンをクリックすると，パターン保存画面が表示されます。パターン保存画面では，作成したパターンの保存場所を指定します。パターン保存画面で［保存］ボタンをクリックすると，新規に検索パターンが保存されます。なお，検索パターン名の先頭に「@」は指定できません。検索パターンの作成については「7.3.5　監査ログ検索パターンの編集」を参照してください。

7.3.2　監査ログの検索条件項目

監査ログ検索画面で，検索条件として指定できる項目について説明します。

指定した検索条件は保存できます。同じ条件で何度も検索したい場合は，検索条件を保存しておくと便利です。検索条件を保存する方法については「7.3.5　監査ログ検索パターンの編集」を参照してください。

検索条件として指定できる項目を，次の表に示します。なお，表示設定画面で検索条件項目の表示および並び順を設定している場合は，検索条件項目に設定内容が反映されます。

表 7-1　検索条件として指定できる項目（監査ログの検索）

項番	検索条件	説明
1	メッセージ ID※1，※2	監査ログメッセージのメッセージ ID を次の方法で指定します。 **プレフィクス定義と製品ごとの ID**※3 テキストボックスに 64 バイト以内の文字列を入力します。 **メッセージレベル**※4 プルダウンメニューから「エラー」，「警告」，「情報」のどれかを選択します。 検索したいメッセージ ID の種別が「-E」の場合は「エラー」，「-W」の場合は「警告」，「-I」の場合は「情報」を選択してください。 なお，メッセージ ID は「完全一致」，「部分一致」，「前方一致」，または「後方一致」を選択して検索できます。デフォルトは「部分一致」です。
2	発生日時 （開始/終了）	監査を開始した日時または監査を終了した日時を次の方法で指定します。 **年月日** テキストボックスに YYYYMMDD※5 の形式で指定するかまたはカレンダーで指定します。 **時間，分，秒** 年月日を指定したときに，時間，分，および秒をプルダウンメニューから選択します。
3	プログラム名	JP1/Audit Management - Manager の監査ログ収集対象プログラムを次の方法で指定します。 **プログラム名** プルダウンメニューからプログラム名を選択します。
4	コンポーネント名	「プログラム名」に対応するコンポーネント名を指定します。

項番	検索条件	説明
		コンポーネント名 ［プログラム名］プルダウンメニューからプログラムを選択すると，選択したプログラムに該当するコンポーネント名がプルダウンメニューに表示されます。プルダウンメニューからコンポーネント名を選択します。
5	プロセス ID	プロセス ID を次の方法で指定します。 **プロセス ID** テキストボックスに 0～2147483647 の整数を入力します。 なお，プロセス ID の範囲は「以下」，「等しい」，または「以上」を選択して検索できます。デフォルトは「以下」です。
6	発生場所※1	監査事象が発生した場所を指定します。 **監査事象が発生した場所** テキストボックスに，256 バイト以内の文字列でホスト名または IP アドレスのどちらかを入力します。 なお，発生場所は「完全一致」，「部分一致」，「前方一致」，または「後方一致」を選択して検索できます。デフォルトは「部分一致」です。
7	監査事象種別	監査事象の種別を指定します。 **監査事象種別** プルダウンメニューから次のどれかを選択します。 • 「StartStop」（開始/停止） • 「Authentication」（認証） • 「AccessControl」（アクセス制御） • 「ContentAccess」（重要情報アクセス） • 「Failure」（障害発生） • 「LinkStatus」（リンク状態） • 「ExternalService」（外部通信） • 「ConfigurationAccess」（設定情報アクセス） • 「Maintenance」（メンテナンス） • 「AnomalyEvent」（しきい値オーバー） • 「ManagementAction」（アクション実行） 各項目の詳細については「2.2.3　監査ログの収集カテゴリ」を参照してください。
8	監査事象結果	監査イベントの結果を指定します。 **監査事象結果** プルダウンメニューから次のどれかを選択します。 • 「Success」（成功） • 「Failure」（失敗） • 「Occurrence」（成功または失敗の分類がない事象の発生）
9	サブジェクト情報※1	監査事象の発生元を指定します。 **サブジェクト情報** テキストボックスに，256 バイト以内の文字列でアカウント識別子，実行ユーザ ID，またはプロセス ID のどれかを入力します。

項番	検索条件	説明
		サブジェクト種別 プルダウンメニューから次のどれかを選択します。 •「アカウント識別子」 •「実行ユーザ ID」 •「プロセス ID」 なお，サブジェクト情報は「完全一致」，「部分一致」，「前方一致」，または「後方一致」を選択して検索できます。デフォルトは「部分一致」です。
10	固有情報※1	メッセージやジョブ名など，製品固有の情報を指定します。 **固有情報** テキストボックスに 1,024 バイト以内の文字列を入力します。 複数の文字列も AND 条件および OR 条件で指定できます。なお，固有情報は部分一致で検索されます。 複数の文字列を指定する場合は，「AND」，「△」，「OR」，および「( )」を使用して，条件式を作ることができます。それぞれの使い方を次に示します。 • AND 前後の文字列の AND 条件を指定するのに使います。AND の前後には半角スペースが必要です。大文字と小文字のどちらでも指定できます。 • △ 半角スペース 前後の文字列の AND 条件を指定するのに使います。文字列間の単一スペースで記述します。 • OR 前後の文字列の OR 条件を指定するのに使います。OR の前後には半角スペースが必要です。大文字と小文字のどちらでも指定できます。 • ( ) 括弧 演算子の評価順序を指定するのに使います。次の規則に従って論理演算をします。 ・論理演算の評価順序は，括弧内，AND，OR の順です。 ・論理演算の最大ネスト数は，255 個です。 ・論理演算のネスト数は，論理演算子 AND，または OR の評価順序を表す括弧を省略しないで指定した場合の括弧のネスト数です。 エスケープ対象文字およびエスケープ対象文字列を次に示します。 • エスケープ対象文字 「'」，「(」，「)」，「△」 • エスケープ対象文字列 「AND」，「OR」 「'」（シングルクォート）で検索文字列を囲むと，エスケープ対象文字およびエスケープ対象文字列はエスケープされます。また，「'」を検索文字列に含む場合は，「'」の直前に「'」を一つ付ける必要があります。 入力例を次に示します。 •「Add」と「JP1_AJS_Admin」を含んだ監査ログを検索する場合 Add△AND△JP1_AJS_Admin Add△JP1_AJS_Admin •「JP1_Audit_Admin」または「JP1_DM_Admin」を含んだ監査ログを検索する場合

項番	検索条件	説明
		JP1_Audit_Admin△OR△JP1_DM_Admin • 「JP1△DM△Admin」または「JP1NETMAudit['Admin']」を含んだ監査ログを検索する場合 'JP1△DM△Admin'△OR△'JP1NETMAudit["Admin"]' • 「JP1_Audit_Admin」または「JP1_DM_Admin」を含み，かつ「Add」を含んだ監査ログを検索する場合 (JP1_Audit_Admin△OR△JP1_DM_Admin)△AND△Add • 「JP1NETMDM(dm-manager)」を含んだ監査ログを検索する場合 'JP1NETMDM(dm-manager)'
11	監査ログ ID※6	製品または製品のコンポーネントに対応する監査ログを特定するための ID を指定します。 **監査ログ ID** テキストボックスに 0～2147483647 の整数を入力します。

注

監査ログ検索画面で検索条件が空白の場合，その検索条件については，すべての監査ログが検索対象となります。

注※1

監査ログを検索する場合，文字列条件の設定によって，大文字小文字の区別は次のようになります。なお，「固有情報」は常に部分一致で検索されるため，大文字小文字の区別はありません。

文字列条件	大文字小文字の区別
完全一致	区別する
部分一致	区別しない
前方一致	
後方一致	

注※2

標準サポート外のプログラムのメッセージ ID については，正規化ルールファイルでの指定を参照してください。

注※3

Windows など，一部の製品メッセージのプレフィクス定義については「付録 E　JP1/Audit Management - Manager が対応するプログラムの監査ログ一覧」を参照してください。

注※4

メッセージレベルは，メッセージの種別（エラー：E，警告：W，情報：I）に対応します。

メッセージレベルの指示は，日立オープンミドルウェア製品の監査ログを検索する場合に使用すると便利です。その他の製品を検索するときに使用すると，監査ログが検出されない場合があります。

注※5

YYYY は年，MM は月，DD は日です。「/」は入力できません。

注※6

デフォルトでは非表示です。この項目を表示する方法については「7.7　監査ログ管理画面の表示設定」を参照してください。

注意事項

テンプレートの検索パターンを使用して，検索条件を指定するときの注意事項を次に示します。

- 効率良く検索するために，「発生日時」で期間を指定することをお勧めします。

- 「サブジェクト情報」および「固有情報」に次の文字列が表示された場合は，表示された文字列を削除してそれぞれに該当する任意の値を入力してください。
  - ・権限レベルを入力してください。
  - ・JP1 資源グループ名を入力してください。
  - ・ユーザ名を入力してください。
  - ・グループ名を入力してください。
- 監査ログが収集されていない監査ログ収集対象プログラムおよびコンポーネントのテンプレートの検索パターンを適用すると，プログラム名およびコンポーネントには空白が設定されます。

7.3.3　監査ログ検索結果の確認

検索結果は，検索結果一覧を画面に表示するか，ファイルに出力して確認します。また，検索した監査ログは，監査ログレポート画面で見やすく表示することができます。

検索結果の出力方法を，次に示します。

表 7-2　監査ログの検索結果の出力方法

項番	検索結果の出力方法	説明
1	検索結果一覧を表示する	検索結果を画面上で確認できます。検索結果一覧を表示する場合については「(1)　検索結果一覧を表示する場合」を参照してください。
2	CSV 形式ファイルを出力する	検索結果を CSV 形式で出力できます。CSV 形式ファイルを出力する場合については「(2)　CSV 形式ファイルを出力する場合」を参照してください。
3	PDF ファイルを出力する	検索結果を PDF ファイルに出力できます。PDF ファイルを出力する場合は，EUR を使用したシステムが必要です。PDF ファイルを出力する場合については「(3)　PDF ファイルを出力する場合」を参照してください。
4	レポート形式で表示する	検索結果を監査ログレポート画面に表示できます。監査ログのレポート表示については「7.3.4　監査ログ検索結果のレポート表示」を参照してください。

ここでは，監査ログ検索画面に表示される検索結果の見方について説明します。

監査ログの検索結果一覧を次に示します。

図 7-6　監査ログ検索結果一覧

表示結果 1-20 / 1636

1 / 82 > >> ページ 表示

監査ログID	メッセージID	発生日時 ▽	プログラム名	コンポーネント
1	KDSD10001-I	2007/02/25 17:06:57.140	JP1/NETM/DM	JP1_DM_SERVICE
1	KDSD10001-I	2007/02/25 17:06:57.140	JP1/NETM/DM	JP1_DM_SERVICE
1	KDSD10001-I	2007/02/25 17:06:57.140	JP1/NETM/DM	JP1_DM_SERVICE
2	KDSD10002-I	2007/02/24 23:56:02.593	JP1/NETM/DM	JP1_DM_SERVICE
2	KDSD10002-I	2007/02/24 23:56:02.593	JP1/NETM/DM	JP1_DM_SERVICE
2	KDSD10002-I	2007/02/24 23:56:02.593	JP1/NETM/DM	JP1_DM_SERVICE
2	KDSD10002-I	2007/02/24 23:56:02.593	JP1/NETM/DM	JP1_DM_SERVICE
8	KDSD10002-I	2007/02/23 10:17:35.171	JP1/NETM/DM	JP1_DM_NETMDM
8	KDSD10002-I	2007/02/23 10:17:35.171	JP1/NETM/DM	JP1_DM_NETMDM
8	KDSD10002-I	2007/02/23 10:17:35.171	JP1/NETM/DM	JP1_DM_NETMDM
8	KDSD10002-I	2007/02/23 10:17:35.171	JP1/NETM/DM	JP1_DM_NETMDM
7	KDSD4066-I	2007/02/22 22:10:25.968	JP1/NETM/DM	JP1_DM_NETMDM
7	KDSD4066-I	2007/02/22 22:10:25.968	JP1/NETM/DM	JP1_DM_NETMDM
7	KDSD4066-I	2007/02/22 22:10:25.968	JP1/NETM/DM	JP1_DM_NETMDM
7	KDSD4066-I	2007/02/22 22:10:25.968	JP1/NETM/DM	JP1_DM_NETMDM
6	KDSD4066-I	2007/02/22 21:16:21.125	JP1/NETM/DM	JP1_DM_NETMDM
4	KDSD10002-I	2007/02/21 18:01:50.593	JP1/NETM/DM	JP1_DM_DMCSVUTY

検索結果として表示される項目を，次の表に示します。

表 7-3　検索結果として表示される項目

項番	項目名	説明
1	監査ログ ID	製品または製品のコンポーネントに対応する監査ログを特定するための ID です。
2	メッセージ ID	監査ログメッセージのメッセージ ID です。JP1/AJS を除く日立オープンミドルウェア製品の場合，次に示す形式で表示されます。 Kxxxnnnnn-y Kxxx：監査ログ収集対象プログラムのプレフィクス定義 nnnnn：監査ログ収集対象プログラムで任意に定義された ID y：メッセージレベル 次のどれかが表示されます。 •「E」（エラー） •「W」（警告） •「I」（情報）
3	発生日時	監査事象が発生した日時です。次に示す形式で表示されます。 YYYY/MM/DD hh:mm:ss.ttt（年/月/日 時:分:秒.ミリ秒）
4	プログラム名	監査事象が発生したプログラムの名称が表示されます。
5	コンポーネント名	監査事象が発生したプログラムに対応する，コンポーネントの名称が表示されます。
6	プロセス ID	監査事象が発生したプロセスのプロセス ID が表示されます。
7	発生場所	監査事象が発生した場所です。ホスト名，IPv4 アドレス，または IPv6 アドレスのどれかが表示されます。
8	監査事象種別	監査事象の種別です。次のどれかが表示されます。 •「StartStop」（開始/停止） •「Authentication」（認証） •「AccessControl」（アクセス制御） •「ContentAccess」（重要情報アクセス） •「Failure」（障害発生） •「LinkStatus」（リンク状態） •「ExternalService」（外部通信） •「ConfigurationAccess」（設定情報アクセス） •「Maintenance」（メンテナンス） •「AnomalyEvent」（しきい値オーバー） •「ManagementAction」（アクション実行） 各項目の詳細については「2.2.3　監査ログの収集カテゴリ」を参照してください。
9	監査事象結果	監査事象の結果です。次のどれかが表示されます。 •「Success」（成功） •「Failure」（失敗） •「Occurrence」（成功または失敗の分類がない事象の発生）
10	サブジェクト情報	利用者情報またはプロセス情報です。次のどれかの値が表示されます。

項番	項目名	説明
		• アカウント識別子 • 実行ユーザ ID • プロセス ID
11	サブジェクト種別	サブジェクト情報の種別です。次のどれかが表示されます。 •「アカウント識別子」 •「実行ユーザ ID」 •「プロセス ID」
12	固有情報※	メッセージやジョブ名など，製品固有の情報が表示されます。

注※

監査ログに日付および時刻情報が出力されている場合は，固有情報としてタイムゾーン情報が「TZD=+hh:mm」と表示されます。

(1) 検索結果一覧を表示する場合

監査ログ検索画面で検索条件を指定して［検索］ボタンをクリックすると，検索結果一覧が表示されます。検索結果が複数ページにわたる場合のページの移動は，検索結果一覧のページリンク（「<<」，「<」，「>」，「>>」）をクリックするかまたはページ番号を直接指定してください。

検索結果一覧には，表 7-3 にある項目が表示されます。ただし，表示設定画面で項目の数や並び順などを設定している場合は，検索結果一覧に設定内容が反映されます。表示設定の方法については「7.7 監査ログ管理画面の表示設定」を参照してください。なお，表示設定画面で設定した「レコード件数/ページ」の値は，監査ログ検索画面の「表示件数」で変更できます。また，監査ログ検索画面で指定した「表示件数」の値は，検索パターンとして保存できます。

注意事項

テンプレートの検索パターンの表示件数は変更できません。表示件数を変更する場合は，別の名称で新規の検索パターンとして保存してください。

(2) CSV 形式ファイルを出力する場合

監査ログ検索画面で検索条件を指定して［CSV］ボタンをクリックすると，検索結果が CSV 形式でファイルに出力されます。［ファイルのダウンロード］ダイアログが表示されるので，ファイルを開く場合は［開く］ボタンを，ファイルを保存する場合は［保存］ボタンをクリックします。

CSV 形式ファイルには，指定した検索条件と検索結果が出力されます。なお，表示設定画面上で非表示に設定した項目もすべて出力されます。

CSV 形式ファイルの出力例を次に示します。

```
"監査ログ検索結果"
"検索条件"
"項目名","値","検索オプション 1","検索オプション 2"
```

"監査ログ ID","","",""
"メッセージ ID","","","部分一致"
"発生日時(開始)","","",""
"発生日時(終了)","","",""
"プログラム名","Windows","",""
"コンポーネント名","LogonEvent","",""
"プロセス ID","","以下",""
"発生場所","","部分一致",""
"監査事象種別","Authentication","",""
"監査事象結果","Success","",""
"サブジェクト情報","Administrator","部分一致","実行ユーザ ID"
"固有情報","obj=OS,op=Logon","",""
"検索結果"
"監査ログ ID","メッセージ ID","発生日時","プログラム名","コンポーネント名","発生場所","プロセス ID","監査事象種別","監査事象結果","サブジェクト情報","サブジェクト種別","固有情報"
"","528","2007/02/26
15:27:42.000","Windows","LogonEvent","7H548300","","Authentication","Success","Administrator","実行ユーザ ID","obj=OS,op=Logon,objloc:from=7H548300,ログオンの成功:,ドメイン:7H548300,ログオン ID:(0x0,0x28EECA0),ログオンの種類:7,ログオン プロセス:User32 ,認証パッケージ:Negotiate,ログオン GUID:-,呼び出し側ユーザー名:7H548300$,呼び出し側ドメイン:WORKGROUP,呼び出し側ログオン ID:(0x0,0x3E7),呼び出し側プロセス ID: 744,移行されたサービス: -,ソース ネットワーク アドレス:127.0.0.1,ソース ポート:0 "
"","528","2007/02/26
14:56:11.000","Windows","LogonEvent","7H548300","","Authentication","Success","Administrator","実行ユーザ ID","obj=OS,op=Logon,objloc:from=7H548300,ログオンの成功:,ドメイン:7H548300,ログオン ID:(0x0,0x28CCA79),ログオンの種類:7,ログオン プロセス:User32 ,認証パッケージ:Negotiate,ログオン GUID:-,呼び出し側ユーザー名:7H548300$,呼び出し側ドメイン:WORKGROUP,呼び出し側ログオン ID:(0x0,0x3E7),呼び出し側プロセス ID: 744,移行されたサービス: -,ソース ネットワーク アドレス:127.0.0.1,ソース ポート:0 "
"","528","2007/02/26
14:13:09.000","Windows","LogonEvent","7H548300","","Authentication","Success","Administrator","実行ユーザ ID","obj=OS,op=Logon,objloc:from=7H548300,ログオンの成功:,ドメイン:7H548300,ログオン ID:(0x0,0x28A314F),ログオンの種類:7,ログオン プロセス:User32 ,認証パッケージ:Negotiate,ログオン GUID:-,呼び出し側ユーザー名:7H548300$,呼び出し側ドメイン:WORKGROUP,呼び出し側ログオン ID:(0x0,0x3E7),呼び出し側プロセス ID: 744,移行されたサービス: -,ソース ネットワーク アドレス:127.0.0.1,ソース ポート:0 "
：

(3) PDF ファイルを出力する場合

PDF ファイルに出力する場合は，EUR が必要です。

監査ログ検索画面で検索条件を指定して［PDF］ボタンをクリックすると，検索結果が PDF ファイルに出力されます。［ファイルのダウンロード］ダイアログが表示されるので，ファイルを開く場合は［開く］ボタンを，保存する場合は［保存］ボタンをクリックします。

PDF ファイルには，指定した検索条件と検索結果の一部が表示されます。なお，出力される PDF ファイルには表示設定画面での設定は反映されません。

検索結果として出力される項目を次に示します。

- メッセージ ID
- 発生日時
- プログラム名
- 発生場所
- 監査事象種別
- 監査事象結果
- サブジェクト情報

PDF ファイルの出力例を次に示します。

図 7-7　PDF ファイルの出力例（監査ログの検索）

監査ログ検索結果

作成日 2008/ 8/25

検索条件

項目名	値		
監査ログID			
メッセージID			部分一致
発生日時(開始)	2008/01/01 00:00:00		
発生日時(終了)	2008/09/01 00:00:00		
プログラム名	Windows		
コンポーネント名	LogonEvent		
プロセスID		以下	
発生場所		部分一致	
監査事象種別	Authentication		
監査事象結果	Success		
サブジェクト情報		部分一致	
固有情報	obj=OS,op=Log		

検索結果

メッセージID	発生日時	プログラム名	発生場所	監査事象種別	監査事象結果	サブジェクト情報
528	2008/08/07 13:03:21.000	Windows	VM-AUDIT-0851	Authentication	Success	Administrator

メッセージID	発生日時	プログラム名	発生場所	監査事象種別	監査事象結果	サブジェクト情報
538	2008/02/27 12:12:48.000	Windows	VM-AUDIT-0850	Authentication	Success	IUSR_VM-AUDIT-0850
538	2008/02/15 11:29:23.000	Windows	VM-AUDIT-0850	Authentication	Success	IUSR_VM-AUDIT-0850
538	2008/02/14 18:43:58.000	Windows	VM-AUDIT-0850	Authentication	Success	IUSR_VM-AUDIT-0850
538	2008/02/12 17:26:12.000	Windows	VM-AUDIT-0850	Authentication	Success	IUSR_VM-AUDIT-0850

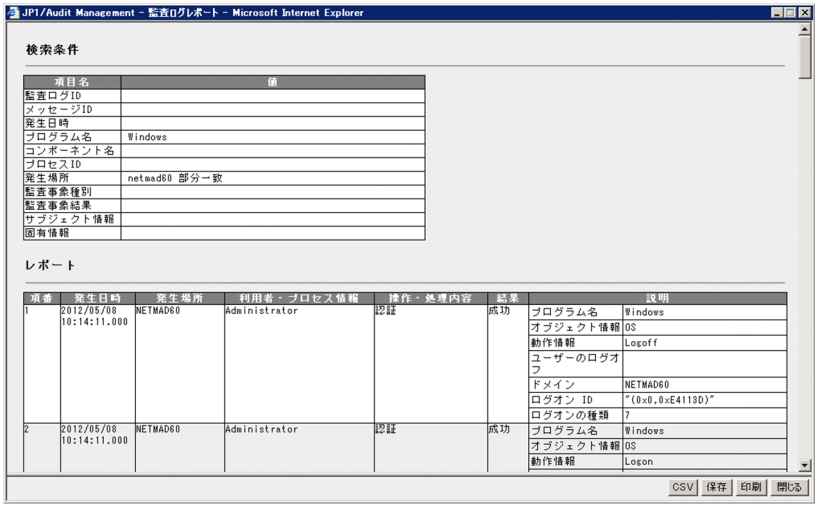
7.3.4　監査ログ検索結果のレポート表示

監査ログの検索結果を見やすくしたレポート（監査ログレポート）は，監査ログレポート画面で表示できます。監査ログレポート画面には，検索条件の項目と監査ログ検索結果のレポートが表示されます。

検索条件の項目は，監査ログ検索画面で設定した検索条件が表示されます。また，表示されたレポートはファイルに出力したり，印刷したりできます。

監査ログ検索結果のレポート表示を次に示します。

図 7-8　監査ログ検索結果のレポート表示



監査ログレポートの出力方法を次に示します。

表 7-4　レポート表示の出力方法

項番	レポート表示の出力方法	説明
1	レポート一覧を表示する	監査ログ検索結果を見やすくしたレポートを画面上で確認できます。監査ログのレポートを表示する場合については「(1)　監査ログレポート一覧を表示する場合」を参照してください。
2	CSV 形式ファイルを出力する	監査ログ検索結果を見やすくしたレポートを CSV 形式ファイルで出力できます。CSV 形式ファイルを出力する場合については「(2)　CSV 形式ファイルを出力する場合」を参照してください。
3	HTML 形式ファイルで保存する	監査ログレポート画面を HTML 形式で保存できます。監査ログレポート一覧を保存する場合については「(3)　保存する場合」を参照してください。
4	印刷する	監査ログレポート一覧を印刷できます。監査ログレポート一覧の印刷については「(4)　印刷する場合」を参照してください。

監査ログレポート一覧として表示される項目を次に示します。

表 7-5　監査ログレポート一覧として表示される項目

項番	項目名	説明
1	項番	レポートに表示される監査ログの番号です。「発生日時」の昇順にソートされています。
2	発生日時	監査ログ検索結果の「発生日時」の値が表示されます。 次に示す形式で表示されます。 YYYY/MM/DD hh:mm:ss.ttt（年/月/日 時:分:秒.ミリ秒）
3	発生場所	監査ログ検索結果の「発生場所」の値が表示されます。
4	利用者・プロセス情報	監査ログ検索結果の「サブジェクト情報」の値が表示されます。

項番	項目名	説明
5	操作・処理内容	監査ログ検索結果の「監査事象種別」の値が，操作・処理内容の文字列で表示されます。※1
6	結果	監査ログ検索結果の「監査事象結果」の値が，結果の文字列で表示されます。※2
7	説明	監査ログ検索結果の「プログラム名」と「固有情報」の値が編集され，説明が表示されます。 検索条件の設定と表示の例を次に示します。 検索条件： プログラム名　JP1Base 固有情報　obj=jp1user,op=Add,auth=Administrator 表示例： プログラム名:JP1Base オブジェクト情報:jp1user 動作情報:Add 権限情報:Administrator

注※1

「監査事象種別」の値と「操作・処理内容」に表示される文字列を次に示します。

「監査事象種別」の値	「操作・処理内容」に表示される文字列
StartStop	開始/停止
Authentication	認証
AccessControl	アクセス制御
ContentAccess	重要情報アクセス
Failure	障害発生
LinkStatus	リンク状態
ExternalService	外部通信
ConfigurationAccess	設定情報アクセス
Maintenance	メンテナンス
AnomalyEvent	しきい値オーバー
ManagementAction	アクション実行

注※2

「監査事象結果」の値と「結果」に表示される文字列を次に示します。

「監査事象結果」の値	「結果」に表示される文字列
Success	成功
Failure	失敗

「監査事象結果」の値	「結果」に表示される文字列
Occurrence	発生

(1)　監査ログレポート一覧を表示する場合

監査ログ検索画面の検索結果画面で，［レポート］ボタンをクリックすると，検索結果が監査ログレポート画面に表示されます。

なお，レポートの最大表示件数は［マネージャセットアップ］ダイアログで設定できます。なお，デフォルトでは 500 件が設定されています。最大表示件数の設定方法については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。また，監査ログレポート画面は複数表示することができます。

監査ログレポート一覧に表示される項目については，表 7-5 を参照してください。

(2)　CSV 形式ファイルを出力する場合

監査ログレポート画面で［CSV］ボタンをクリックすると，指定した検索条件と検索結果のレポートが CSV 形式ファイルに出力されます。［ファイルのダウンロード］ダイアログが表示されるので，ファイルを開く場合は［開く］ボタンを，ファイルを保存する場合は［保存］ボタンをクリックします。

CSV 形式ファイルの出力例を次に示します。

```
"監査ログレポート"
"検索条件"
"項目名","値"
"監査ログ ID",""
"メッセージ ID",""
"発生日時",""
"プログラム名",""
"コンポーネント名",""
"プロセス ID",""
"発生場所","",
"監査事象種別",""
"監査事象結果",""
"サブジェクト情報",""
"固有情報",""
"レポート"
"項番","発生日時","発生場所","利用者・プロセス情報","操作・処理内容","結果","説明"
"1","20061203232312","Host2","Administrator","認証","成功","オブジェクト情報:PASSWORD
動作情報:Update
ロケーション認証サーバ:A2"
```

(3)　保存する場合

監査ログレポート画面で，［保存］ボタンをクリックすると，［HTML ドキュメントの保存］ダイアログが表示され，監査ログレポート画面が HTML 形式で保存されます。

(4)　印刷する場合

監査ログレポート画面で［印刷］ボタンをクリックすると，［印刷］ダイアログが表示され，監査ログレポート画面が印刷できます。

> **参考**
>
> 監査ログレポートの印刷サイズは A4 横が想定されています。

7.3.5　監査ログ検索パターンの編集

監査ログ検索画面では，指定した検索条件を保存できます。監査ログを同じ条件で何度も検索したいときなどに便利です。保存した検索条件のことを**検索パターン**と呼びます。

ここでは，検索パターンの作成，変更，および削除について説明します。検索パターンの利用方法については「7.3.1(2)　検索パターンを利用する」を参照してください。

なお，監査ログ検索画面には，テンプレートの検索パターンが用意されています。テンプレートの検索パターンについては「11.12　検索パターンおよび集計パターンの一覧」を参照してください。

(1)　検索パターンを作成する

監査ログの検索パターンの作成には，次に示す方法があります。

- 新規に検索パターンを作成します。
  検索条件を新たに作成したい場合，新規に検索パターンを定義します。
- 既存の検索パターンを利用します。
  次に示す方法があります。
  - テンプレートの検索パターンをカスタマイズします。
    監査ログ検索画面にあらかじめ用意されているテンプレートの検索パターンを表示して，収集された監査ログに合わせて検索条件をカスタマイズします。
  - 作成済みの検索パターンをカスタマイズします。
    作成済みの検索パターンを表示して，収集された監査ログに合わせて検索条件をカスタマイズします。

(a)　新規に検索パターンを作成する場合

新規に検索パターンを作成する手順を次に示します。

1. 監査ログの検索条件を入力する。

   監査ログ検索画面で検索条件を入力します。入力できる検索条件の詳細については「7.3.2　監査ログの検索条件項目」を参照してください。

2. 検索パターン名を指定する。

   「検索パターン名」に検索パターンの名称を指定します。64 バイト以内の文字列を入力してください。ただし，検索パターン名の先頭に「@」は指定できません。また，作成先の業務メニュー内にすでに存在するフォルダと同じ名称は，指定できません。

3. ［保存］ボタンをクリックする。

   既存の検索パターンと同じ名称を指定した場合，内容が上書きされます。新規の検索パターン名を指定した場合，パターン保存画面が表示されます。

4. パターン保存画面で，作成する検索パターンの保存場所を指定する。

   検索パターンの保存場所をツリー上で指定します。ただし，ルートおよびテンプレートフォルダは保存場所として指定できません。

5. パターン保存画面の［保存］ボタンをクリックする。

   指定した検索条件が検索パターンとして保存されます。保存された検索パターンは，ユーザ作成の検索パターンとして「検索パターン名」のリストおよび機能ツリーに追加されます。

(b)　既存の検索パターンを利用する場合

既存の検索パターンをカスタマイズして，検索パターンを作成する手順を次に示します。

1. 検索パターンを選択する。

   次のどちらかの方法で，検索条件として使用する検索パターンを選択します。

   - 監査ログ管理画面の左フレームの機能ツリーで検索パターン名を選択します。
   - 監査ログ検索画面の「検索パターン名」リストで検索パターン名を選択し，［適用］ボタンをクリックします。

   監査ログ検索画面に，検索パターンとして保存されている検索条件が表示されます。

2. 検索条件を変更する。

   監査ログ検索画面に表示された検索条件を変更します。指定できる検索条件の詳細については「7.3.2 監査ログの検索条件項目」を参照してください。

3. 検索パターン名を指定する。

   「検索パターン名」に新たな検索パターンの名称を指定します。64 バイト以内の文字列を入力してください。ただし，検索パターン名の先頭に「@」は指定できません。また，作成先の業務メニュー内にすでに存在するフォルダと同じ名称は，指定できません。

4. ［保存］ボタンをクリックする。

既存の検索パターンと同じ名称を指定した場合，内容が上書きされます。新規の検索パターン名を指定した場合，パターン保存画面が表示されます。

5. パターン保存画面で作成する検索パターンの保存場所を指定します。

   検索パターンの保存場所をツリー上で指定します。ただし，ルートおよびテンプレートフォルダは保存場所として指定できません。

6. パターン保存画面の［保存］ボタンをクリックする。

   指定した検索条件が検索パターンとして保存されます。保存された検索パターンは，ユーザ作成の検索パターンとして「検索パターン名」のリストおよび機能ツリーに追加されます。

(2) 検索パターンを変更する

既存の検索パターンの検索条件を変更する手順を次に示します。

なお，テンプレートの検索パターンは変更できません。テンプレートの検索パターンを変更して保存したい場合は，別の名称を指定して保存してください。

1. 検索パターンを選択する。

   次のどちらかの方法で，検索条件として使用する検索パターンを選択します。

   - 監査ログ管理画面の左フレームの機能ツリーで検索パターン名を選択します。
   - 監査ログ検索画面の「検索パターン名」リストで検索パターン名を選択し，［適用］ボタンをクリックします。

   監査ログ検索画面に，検索パターンとして保存されている検索条件が表示されます。

2. 検索条件を変更する。

   監査ログ検索画面に表示された検索条件を変更します。指定できる検索条件の詳細については「7.3.2 監査ログの検索条件項目」を参照してください。

3. 検索パターン名を変更しないで，［保存］ボタンをクリックする。

   監査ログ検索画面に表示されている検索条件が，検索パターンとして上書き保存されます。別の名称を指定して保存すると，新規に検索パターンが作成されます。

(3) 検索パターンを削除する

監査ログの検索パターンを削除する手順を次に示します。

なお，テンプレートの検索パターンは削除できません。

1. 検索パターンを選択する。

   次のどちらかの方法で，検索条件として使用する検索パターンを選択します。

   - 監査ログ管理画面の左フレームの機能ツリーで検索パターン名を選択します。
   - 監査ログ検索画面の「検索パターン名」リストで検索パターン名を選択します。

2. [削除] ボタンをクリックする。

選択した検索パターン名が削除されます。

上記の手順以外に，パターン表示編集画面で検索パターンを削除することもできます。詳細については「7.8.5　パターンやフォルダを削除する」を参照してください。

7.4　監査ログ集計

監査ログ管理画面で必要な条件を指定して，監査ログ管理データベースに収集された監査ログを集計できます。

例えば，次のような条件で監査ログを集計します。

- ログインに失敗したログを集計する。
- ここ一年間に収集された JP1/NETM/DM のログの数を集計する。
- 指定した期間内にパスワード変更が何回実施されたかを集計する。

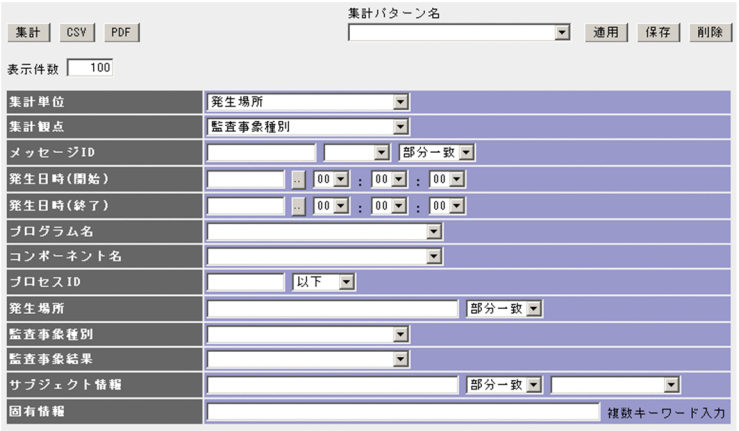
なお，指定した集計条件を集計パターンとして保存できます。集計パターンとは，監査ログを同じ条件で何度も集計するために保存してある集計条件のことであり，同じ集計条件を設定する手間を省くことができます。

作成した集計パターンは，統計パターンとしても使用できます。統計パターンの詳細については「7.5.4 監査ログ統計パターンの設定」を参照してください。

監査ログの集計結果は画面上に表示したり，ファイルに出力したりできます。また，集計した監査ログは，集計結果のグラフで見やすく表示することもできます。

監査ログの集計は，監査ログ集計画面で実行できます。監査ログ集計画面を次に示します。

図 7-9　監査ログ集計画面



この節では，監査ログを集計する手順，集計条件として指定できる項目，集計結果の確認方法，および集計パターンの作成方法を説明します。

監査ログ集計画面の各部の名称と使い方については「11.4　監査ログ集計画面」を参照してください。

7.4.1　監査ログの集計

ここでは収集された監査ログを集計する手順と集計パターンの使用方法について説明します。

(1)　監査ログの集計手順

監査ログを集計する手順を次に示します。

1. 監査ログ集計画面を表示する。

   機能ツリーで「監査ログ集計」をクリックすると，監査ログ集計画面が表示されます。

2. 集計条件を指定する。

   集計条件は，直接入力するか，保存されている集計パターンで指定します。

   指定できる集計条件の詳細については「7.4.2　監査ログの集計条件項目」を参照してください。集計パターンを使用して集計条件を指定する方法については「(2)　集計パターンを利用する」を参照してください。

3. 集計結果を取得する。

   - 画面上で集計結果を確認したい場合は，［集計］ボタンをクリックしてください。
   - CSV 形式ファイルを出力したい場合は，［CSV］ボタンをクリックしてください。
   - PDF ファイルを出力したい場合は，［PDF］ボタンをクリックしてください。
   - 集計結果をグラフで確認したい場合は，集計結果の「選択」チェックボックスにチェックを入れて，［グラフ表示］ボタンをクリックしてください。デフォルトではすべての集計結果がチェックされています。

     なお，現在表示しているページのすべての集計結果を選択する場合は，［全選択］ボタンをクリックしてください。また，現在表示しているページのすべての選択をクリアする場合は，［全解除］ボタンをクリックしてください。

   集計条件に一致した監査ログの集計結果が出力されます。監査ログの集計結果の見方については「7.4.3 監査ログ集計結果の確認」を参照してください。

(2)　集計パターンを利用する

集計パターンを使って，監査ログを集計する手順を次に示します。

1. 集計パターンを選択する。

   次の方法のどちらかで，集計条件として使用する集計パターンを選択します。

   - 監査ログ管理画面の左フレームの機能ツリーで集計パターン名を選択します。
   - 監査ログ集計画面の「集計パターン名」リストで集計パターン名を選択し，［適用］ボタンをクリックします。

   監査ログ集計画面に，集計パターンとして作成した集計条件が表示されます。

2. 必要に応じて集計条件を変更する。

   監査ログ集計画面に表示された集計条件は変更できます。必要に応じて変更してください。

3. 集計結果を取得する。

［集計］ボタンをクリックすると，集計条件に一致した監査ログが，監査ログ集計画面の集計結果一覧に表示されます。集計結果をファイルに出力する場合は，［CSV］ボタンや［PDF］ボタンをクリックしてください。

手順 2.で変更した集計条件は，集計パターン名を変更しないで［保存］ボタンをクリックすると，変更後の集計パターンで上書き保存されます。上書き保存された集計パターンを統計パターンとして設定している場合，統計パターンも連動して変更されます。統計パターンが変更されると，変更前の統計パターンを基にした統計結果を正しく出力できないことがあります。この場合，統計情報を生成し直してください。

テンプレートの集計パターンを変更して保存したい場合は，別の名称を指定して保存してください。テンプレートの集計パターンについては「11.12　検索パターンおよび集計パターンの一覧」を参照してください。

集計パターン名を変更して監査ログ集計画面で［保存］ボタンをクリックすると，パターン保存画面が表示されます。パターン保存画面では，作成したパターンの保存場所を指定します。パターン保存画面で［保存］ボタンをクリックすると，新規に集計パターンが保存されます。なお，集計パターン名の先頭に「@」は指定できません。集計パターンの作成については「7.4.5　監査ログ集計パターンの編集」を参照してください。

7.4.2　監査ログの集計条件項目

監査ログ集計画面で，集計条件として指定できる項目について説明します。

指定した集計条件は保存できます。同じ条件で何度も集計したい場合は，集計条件を保存しておくと便利です。集計条件を保存する方法については「7.4.5　監査ログ集計パターンの編集」を参照してください。

集計条件として指定できる項目を，次の表に示します。なお，表示設定画面で集計条件項目の表示および並び順を設定している場合は，集計条件項目に設定内容が反映されます。

表 7-6　集計条件として指定できる項目

項番	集計条件	説明
1	集計単位	監査ログを集計する単位を指定します。 **集計単位** プルダウンメニューから次のどれかを選択します。 • 「発生場所」 監査事象が発生した場所です。 • 「プログラム名」 監査事象が発生したプログラム名です。 • 「サブジェクト情報」 監査事象が発生したユーザ ID です。
2	集計観点	監査ログを集計する観点を指定します。

項番	集計条件	説明
		集計観点 プルダウンメニューから次のどちらかを指定します。 • 「監査事象種別」 監査事象の種別です。 • 「監査事象結果」 監査事象の結果です。
3	メッセージ ID※1，※2	監査ログメッセージのメッセージ ID を次の方法で指定します。 **プレフィクス定義と製品ごとの ID**※3 テキストボックスに 64 バイト以内の文字列を入力します。 **メッセージレベル**※4 プルダウンメニューから「エラー」,「警告」,「情報」のどれかを選択します。 なお，メッセージ ID は「完全一致」,「部分一致」,「前方一致」，または「後方一致」を選択して集計できます。デフォルトは「部分一致」です。
4	発生日時 (開始/終了)	監査を開始した日時または監査を終了した日時を指定します。 **年月日** テキストボックスに YYYYMMDD※5 の形式で指定するかまたはカレンダーで指定します。 **時間，分，秒** それぞれをプルダウンメニューから選択します。年月日を指定したときだけ選択できます。
5	プログラム名	JP1/Audit Management - Manager の監査ログ収集対象プログラムを指定します。 **プログラム名** プルダウンメニューから，集計したいプログラム名を選択します。
6	コンポーネント名	「プログラム名」に対応するコンポーネント名を指定します。 **コンポーネント名** [プログラム名] プルダウンメニューからプログラムを選択すると，選択したプログラムに該当するコンポーネント名がプルダウンメニューに表示されます。プルダウンメニューからコンポーネント名を選択します。
7	プロセス ID	プロセス ID を指定します。 **プロセス ID** テキストボックスに 0～2147483647 の整数を入力します。 なお，プロセス ID の範囲は「以下」,「等しい」，または「以上」を選択して集計できます。デフォルトは「以下」です。
8	発生場所※1	監査事象が発生した場所を指定します。 **監査事象が発生した場所** テキストボックスに，256 バイト以内の文字列でホスト名または IP アドレスのどちらかを入力します。 なお，発生場所は「完全一致」,「部分一致」,「前方一致」，または「後方一致」を選択して集計できます。デフォルトは「部分一致」です。

項番	集計条件	説明
9	監査事象種別	監査事象の種別を指定します。 **監査事象種別** プルダウンメニューから次のどれかを選択します。 • 「StartStop」（開始/停止） • 「Authentication」（認証） • 「AccessControl」（アクセス制御） • 「ContentAccess」（重要情報アクセス） • 「Failure」（障害発生） • 「LinkStatus」（リンク状態） • 「ExternalService」（外部通信） • 「ConfigurationAccess」（設定情報アクセス） • 「Maintenance」（メンテナンス） • 「AnomalyEvent」（しきい値オーバー） • 「ManagementAction」（アクション実行） 各項目の詳細については「2.2.3　監査ログの収集カテゴリ」を参照してください。
10	監査事象結果	監査イベントの結果を指定します。 **監査事象結果** プルダウンメニューから次のどれかを指定します。 • 「Success」（成功） • 「Failure」（失敗） • 「Occurrence」（成功または失敗の分類がない事象の発生）
11	サブジェクト情報※1	監査事象の発生元を指定します。 **サブジェクト情報** テキストボックスに，256 バイト以内の文字列でアカウント識別子，実行ユーザ ID，またはプロセス ID のどれかを入力します。 **サブジェクト種別** プルダウンメニューから次のどれかを選択します。 • 「アカウント識別子」 • 「実行ユーザ ID」 • 「プロセス ID」 なお，サブジェクト情報は「完全一致」，「部分一致」，「前方一致」，または「後方一致」を選択して集計できます。デフォルトは「部分一致」です。
12	固有情報※1	メッセージやジョブ名など，製品固有の情報を指定します。 **固有情報** テキストボックスに 1,024 バイト以内の文字列を入力します。 複数の文字列も AND 条件および OR 条件で指定できます。なお，固有情報は部分一致で集計されます。 複数の文字列を指定する場合は，「AND」，「△」，「OR」，および「( )」を使用して，条件式を作ることができます。それぞれの使い方を次に示します。 • AND

項番	集計条件	説明
		前後の文字列の AND 条件を指定するのに使います。AND の前後には半角スペースが必要です。大文字と小文字のどちらでも指定できます。 • △ 半角スペース 前後の文字列の AND 条件を指定するのに使います。文字列間の単一スペースで記述します。 • OR 前後の文字列の OR 条件を指定するのに使います。OR の前後には半角スペースが必要です。大文字と小文字のどちらでも指定できます。 • ( ) 括弧 演算子の評価順序を指定するのに使います。次の規則に従って論理演算をします。 ・論理演算の評価順序は，括弧内，AND，OR の順です。 ・論理演算の最大ネスト数は，255 個です。 ・論理演算のネスト数は，論理演算子 AND，または OR の評価順序を表す括弧を省略しないで指定した場合の括弧のネスト数です。 エスケープ対象文字およびエスケープ対象文字列を次に示します。 • エスケープ対象文字 「'」，「(」，「)」，「△」 • エスケープ対象文字列 「AND」，「OR」 「'」（シングルクォート）で集計文字列を囲むと，エスケープ対象文字およびエスケープ対象文字列はエスケープされます。また，「'」を集計文字列に含む場合は，「'」の直前に「'」を一つ付ける必要があります。 入力例を次に示します。 •「Add」と「JP1_AJS_Admin」を含んだ監査ログを集計する場合 Add△AND△JP1_AJS_Admin Add△JP1_AJS_Admin •「JP1_Audit_Admin」または「JP1_DM_Admin」を含んだ監査ログを集計する場合 JP1_Audit_Admin△OR△JP1_DM_Admin •「JP1△DM△Admin」または「JP1NETMAudit['Admin']」を含んだ監査ログを集計する場合 'JP1△DM△Admin'△OR△'JP1NETMAudit[''Admin'']' •「JP1_Audit_Admin」または「JP1_DM_Admin」を含み，かつ「Add」を含んだ監査ログを集計する場合 (JP1_Audit_Admin△OR△JP1_DM_Admin)△AND△Add •「JP1NETMDM(dm-manager)」を含んだ監査ログを集計する場合 'JP1NETMDM(dm-manager)'
13	監査ログ ID※6	製品または製品のコンポーネントに対応する監査ログを特定するための ID を指定します。 **監査ログ ID** テキストボックスに 0～2147483647 の整数を入力します。

注

監査ログ集計画面で集計条件が空白の場合，その集計条件については，すべての監査ログが集計対象となります。

注※1

監査ログを集計する場合，文字列条件の設定によって，大文字小文字の区別は次のようになります。なお，「固有情報」は常に部分一致で集計されるため，大文字小文字の区別はありません。

文字列条件プルダウンメニューの選択	大文字小文字の区別
完全一致	区別する
部分一致	区別しない
前方一致	
後方一致	

注※2

標準サポート外のプログラムのメッセージ ID については，正規化ルールファイルでの指定を参照してください。

注※3

Windows など，一部の製品メッセージのプレフィクス定義については「付録 E　JP1/Audit Management - Manager が対応するプログラムの監査ログ一覧」を参照してください。

注※4

メッセージレベルは，メッセージの種別（エラー：E，警告：W，情報：I）に対応します。

メッセージレベルの指示は，日立オープンミドルウェア製品の監査ログを集計する場合に使用すると便利です。その他の製品を集計するときに使用すると，監査ログが検出されない場合があります。

注※5

YYYY は年，MM は月，DD は日です。「/」は入力できません。

注※6

デフォルトでは非表示です。この項目を表示する方法については「7.7　監査ログ管理画面の表示設定」を参照してください。

注意事項

テンプレートの集計パターンを使用して，集計条件を指定するときの注意事項を次に示します。

- 効率良く集計するために，「発生日時」で期間を指定することをお勧めします。
- 「サブジェクト情報」および「固有情報」に次の文字列が表示された場合は，表示された文字列を削除してそれぞれに該当する任意の値を入力してください。
  - ・権限レベルを入力してください。
  - ・JP1 資源グループ名を入力してください。
  - ・ユーザ名を入力してください。
  - ・グループ名を入力してください。
- 監査ログが収集されていない監査ログ収集対象プログラムおよびコンポーネントのテンプレートの集計パターンを適用すると，プログラム名およびコンポーネントには空白が設定されます。

7.4.3　監査ログ集計結果の確認

集計結果は，集計結果一覧を画面に表示するか，ファイルに出力して確認します。また，集計した監査ログは，集計結果のグラフで見やすく表示できます。

集計結果の出力方法を，次に示します。

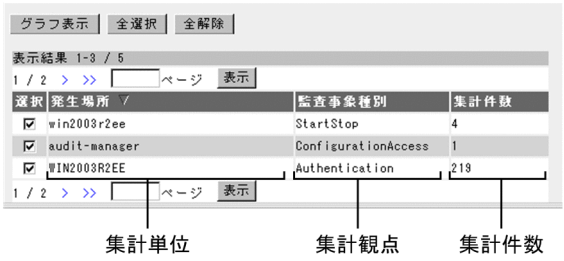
表 7-7　監査ログ集計結果の出力方法

項番	集計結果の出力方法	説明
1	集計結果一覧を表示する	集計結果を画面上で確認できます。集計結果一覧を表示する場合については「(1)　集計結果一覧を表示する場合」を参照してください。
2	CSV 形式ファイルを出力する	集計結果を CSV 形式で出力できます。CSV 形式ファイルを出力する場合については「(2)　CSV 形式ファイルを出力する場合」を参照してください。
3	PDF ファイルを出力する	集計結果を PDF ファイルに出力できます。PDF ファイルを出力する場合は，EUR を使用したシステムが必要です。PDF ファイルを出力する場合については「(3)　PDF ファイルを出力する場合」を参照してください。
4	集計結果をグラフ表示する	集計結果を集計結果グラフ表示画面に表示できます。監査ログの集計結果のグラフ表示については「7.4.4　監査ログ集計結果のグラフ表示」を参照してください。

ここでは，監査ログ集計画面に表示される集計結果の見方について説明します。

監査ログの集計結果一覧を次に示します。

図 7-10　監査ログ集計結果一覧



集計結果一覧に表示される項目を次の表に示します。

表 7-8　集計結果として表示される項目

項番	項目名	説明
1	集計単位	集計条件として指定した集計単位が表示されます。「発生場所」，「プログラム名」，または「サブジェクト情報」のどれかが表示されます。 **発生場所** 監査事象が発生した場所です。ホスト名，IPv4 アドレス，または IPv6 アドレスのどれかが表示されます。 **プログラム名** 監査事象が発生したプログラム名です。 **サブジェクト情報** 監査事象が発生したユーザ ID です。
2	集計観点	集計条件として指定した集計観点が表示されます。「監査事象種別」と「監査事象結果」のどちらかが表示されます。

項番	項目名	説明
		監査事象種別 監査事象の種別です。次のどれかが表示されます。 • 「StartStop」（開始/停止） • 「Authentication」（認証） • 「AccessControl」（アクセス制御） • 「ContentAccess」（重要情報アクセス） • 「Failure」（障害発生） • 「LinkStatus」（リンク状態） • 「ExternalService」（外部通信） • 「ConfigurationAccess」（設定情報アクセス） • 「Maintenance」（メンテナンス） • 「AnomalyEvent」（しきい値オーバー） • 「ManagementAction」（アクション実行） 各項目の詳細については「2.2.3　監査ログの収集カテゴリ」を参照してください。 **監査事象結果** 監査事象の結果です。次のどれかが表示されます。 • 「Success」（成功） • 「Failure」（失敗） • 「Occurrence」（成功または失敗の分類がない事象の発生）
3	集計件数	集計結果の件数が表示されます。

(1)　集計結果一覧を表示する場合

監査ログ集計画面で集計条件を指定して［集計］ボタンをクリックすると，集計結果一覧が表示されます。集計結果が複数ページにわたる場合のページの移動は，集計結果一覧のページリンク（「<<」，「<」，「>」，「>>」）をクリックするかまたはページ番号を直接指定してください。

集計結果一覧の「集計結果」は，集計条件（集計単位，集計観点）ごとに表示されます。集計条件の組み合わせを次の表に示します。

表 7-9　集計条件の組み合わせ一覧

項番	集計単位	集計観点
1	発生場所	監査事象種別
2	発生場所	監査事象結果
3	プログラム名	監査事象種別
4	プログラム名	監査事象結果
5	サブジェクト情報	監査事象種別
6	サブジェクト情報	監査事象結果

表示設定画面で項目の数や並び順などを設定している場合は，集計結果一覧に設定内容が反映されます。表示設定の方法については「7.7　監査ログ管理画面の表示設定」を参照してください。なお，表示設定画面で設定した「レコード件数/ページ」の値は，監査ログ集計画面の「表示件数」で変更できます。また，監査ログ集計画面で指定した「表示件数」の値は，集計パターンとして保存できます。

注意事項

テンプレートの集計パターンの表示件数は変更できません。表示件数を変更する場合は，別の名称で新規の検索パターンとして保存してください。

(2)　CSV 形式ファイルを出力する場合

監査ログ集計画面で集計条件を指定して［CSV］ボタンをクリックすると，集計結果が CSV 形式でファイルに出力されます。［ファイルのダウンロード］ダイアログが表示されるので，ファイルを開く場合は［開く］ボタンを，ファイルを保存する場合は［保存］ボタンをクリックします。

CSV 形式ファイルには，指定した集計条件と集計結果が出力されます。なお，表示設定画面上で非表示に設定した項目もすべて出力されます。

CSV 形式ファイルの出力例を次に示します。

```
"監査ログ集計結果"
"集計条件"
"項目名","値","集計オプション 1","集計オプション 2"
"集計単位","発生場所","",""
"集計観点","監査事象種別","",""
"監査ログ ID","","",""
"メッセージ ID","","","部分一致"
"発生日時(開始)","","",""
"発生日時(終了)","","",""
"プログラム名","Windows","",""
"コンポーネント名","LogonEvent","",""
"プロセス ID","","以下",""
"発生場所","","部分一致",""
"監査事象種別","Authentication","",""
"監査事象結果","Success","",""
"サブジェクト情報","Administrator","部分一致","実行ユーザ ID"
"固有情報","obj=OS,op=Logon","",""
"集計結果"
"発生場所","監査事象種別","集計件数"
"7H548300","Authentication","45"
```

(3)　PDF ファイルを出力する場合

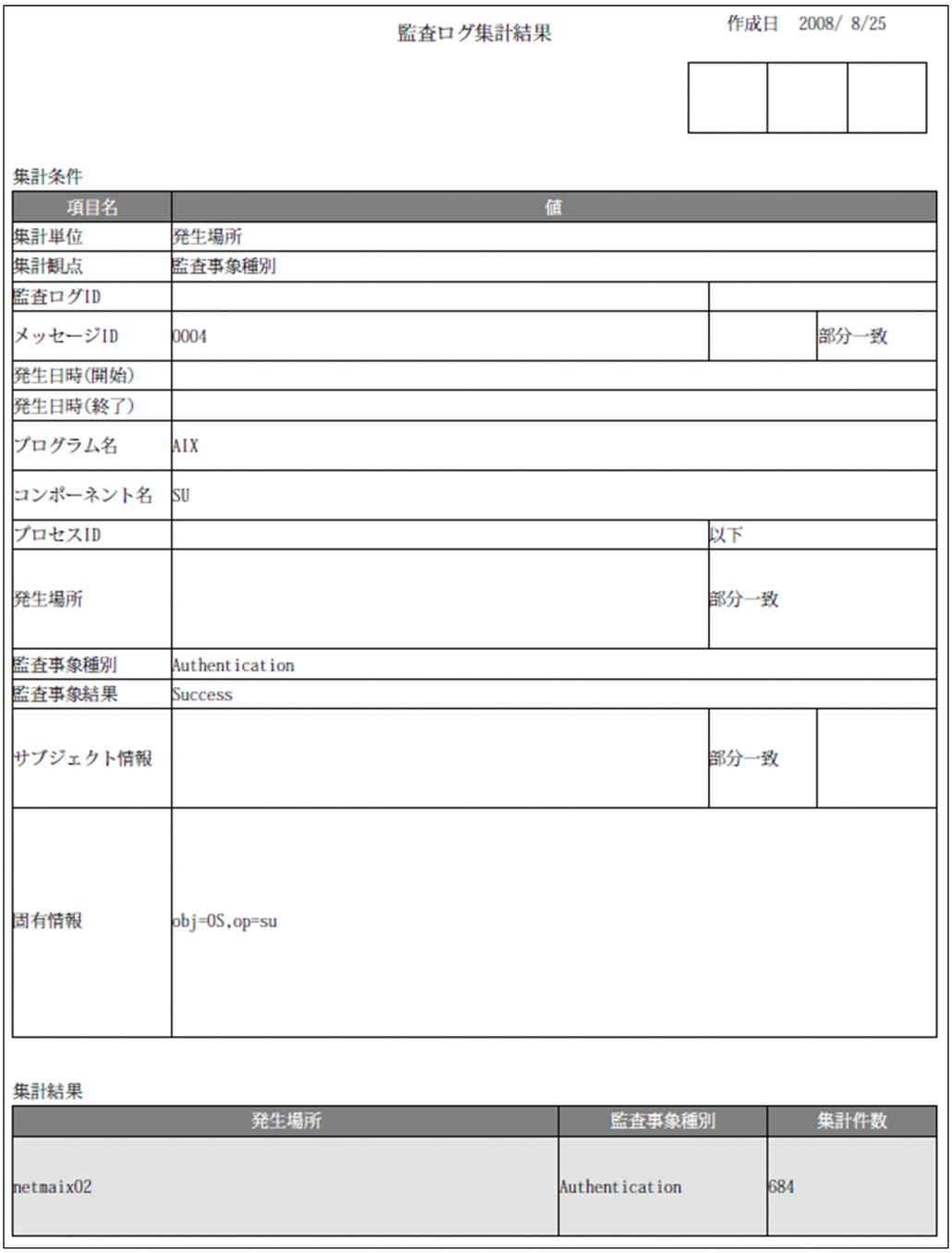
PDF ファイルに出力する場合は，EUR が必要です。

監査ログ集計画面で集計条件を指定して［PDF］ボタンをクリックすると，集計結果が PDF ファイルに出力されます。［ファイルのダウンロード］ダイアログが表示されるので，ファイルを開く場合は［開く］ボタンを，保存する場合は［保存］ボタンをクリックします。

PDF ファイルには，指定した集計条件と集計結果が出力されます。なお，表示設定画面上で非表示に設定した項目もすべて出力されます。

PDF ファイルの出力例を次の図に示します。

図 7-11　PDF ファイルの出力例（監査ログの集計）



監査ログ集計結果

作成日　2008/ 8/25

集計条件

項目名	値		
集計単位	発生場所		
集計観点	監査事象種別		
監査ログID			
メッセージID	0004		部分一致
発生日時(開始)			
発生日時(終了)			
プログラム名	AIX		
コンポーネント名	SU		
プロセスID		以下	
発生場所		部分一致	
監査事象種別	Authentication		
監査事象結果	Success		
サブジェクト情報		部分一致	
固有情報	obj=OS,op=su		

集計結果

発生場所	監査事象種別	集計件数
netmaix02	Authentication	684

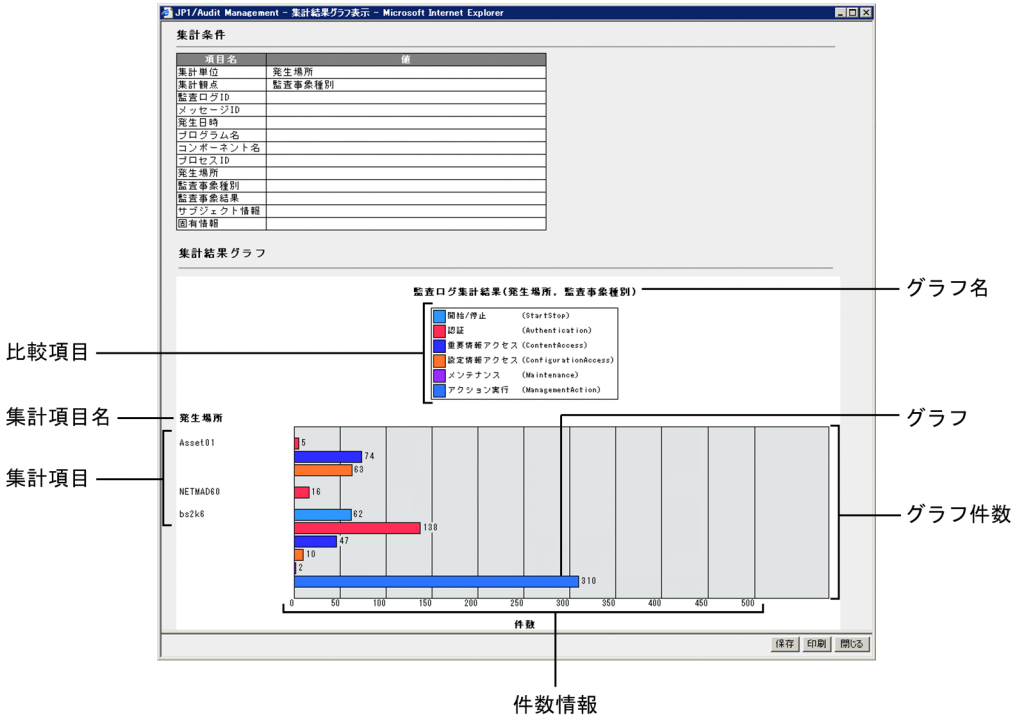
7.4.4　監査ログ集計結果のグラフ表示

監査ログの集計結果は，監査ログ集計結果グラフ表示画面で表示できます。監査ログ集計結果グラフ表示画面には，集計条件の項目と監査ログ集計結果のグラフが表示されます。

集計条件の項目には，監査ログ集計画面で設定した集計条件が表示されます。また，表示された集計結果のグラフはファイルに出力したり，印刷したりできます。

監査ログ集計結果のグラフを次に示します。

図 7-12　監査ログ集計結果のグラフ表示



監査ログ集計結果のグラフの表示方法を次に示します。

表 7-10　監査ログ集計結果のグラフの表示方法

項番	監査ログ集計結果のグラフの表示方法	説明
1	集計結果をグラフ表示する	監査ログ集計結果のグラフを画面上で確認できます。監査ログの集計結果をグラフ表示する場合については「(1)　監査ログ集計結果をグラフ表示する場合」を参照してください。
2	HTML 形式ファイルで保存する	監査ログ集計結果グラフ表示画面を HTML 形式で保存できます。監査ログ集計結果のグラフを保存する場合については「(2)　保存する場合」を参照してください。
3	印刷する	監査ログ集計結果のグラフを印刷できます。監査ログ集計結果のグラフの印刷については「(3)　印刷する場合」を参照してください。

監査ログ集計結果のグラフとして表示される項目を次に示します。

表 7-11　監査ログ集計結果のグラフとして表示される項目

項番	項目名	説明
1	グラフ名	グラフ名が表示されます。
2	比較項目	集計観点に対応して，グラフの比較対象が表示されます。 • 集計観点に「監査事象種別」を設定した場合 「監査事象種別」の値と操作・処理内容※1 • 集計観点に「監査事象結果」を設定した場合 「監査事象結果」の値と結果※2
3	集計項目名	グラフの縦軸項目として，次のどれかの集計単位が表示されます。 •「発生場所」（固定値） •「プログラム名」（固定値） •「サブジェクト情報」（固定値）
4	集計項目	監査ログ集計画面で選択した集計結果のグラフ対象名が表示されます。 • 集計単位に，「発生場所」を設定した場合 選択した集計結果の「発生場所」 • 集計単位に，「プログラム名」を設定した場合 選択した集計結果の「プログラム名」 • 集計単位に，「サブジェクト情報」を設定した場合 選択した集計結果の「サブジェクト情報」
5	グラフ	集計結果が，グラフで集計項目ごとに昇順に表示されます。
6	グラフ件数	表示されているグラフの件数が表示されます。
7	件数情報	グラフの横軸として，集計件数の目盛りの数値が表示されます。横軸の長さは固定で，それぞれの数値はグラフの最大件数によって調整されます。

注※1

「監査事象種別」の値と操作・処理内容を次の表に示します。

「監査事象種別」の値	操作・処理内容
StartStop	開始/停止
Authentication	認証
AccessControl	アクセス制御
ContentAccess	重要情報アクセス
Failure	障害発生
LinkStatus	リンク状態
ExternalService	外部通信
ConfigurationAccess	設定情報アクセス
Maintenance	メンテナンス
AnomalyEvent	しきい値オーバー

「監査事象種別」の値	操作・処理内容
ManagementAction	アクション実行

注※2

「監査事象結果」の値と結果を次の表に示します。

「監査事象結果」の値	結果
Success	成功
Failure	失敗
Occurrence	発生

(1)　監査ログ集計結果をグラフ表示する場合

監査ログ集計画面の集計結果画面で，集計結果の「選択」チェックボックスにチェックを入れて，［グラフ表示］ボタンをクリックすると，選択した集計結果に対応する監査ログ集計結果グラフ表示画面が表示されます。デフォルトではすべての集計結果がチェックされています。

複数のページの集計結果をグラフ表示したい場合は，ページを切り替えて，集計結果を選択し，［グラフ表示］ボタンをクリックしてください。なお，集計結果グラフ表示画面は複数表示することができます。

監査ログ集計結果のグラフに表示される項目については，表 7-11 を参照してください。

(2)　保存する場合

監査ログ集計結果グラフ表示画面で［保存］ボタンをクリックすると，［HTML ドキュメントの保存］ダイアログが表示され，監査ログ集計結果グラフ表示画面が HTML 形式で保存されます。

(3)　印刷する場合

監査ログ集計結果グラフ表示画面で，［印刷］ボタンをクリックすると，［印刷］ダイアログが表示され，集計結果グラフ表示画面が印刷できます。

参考

監査ログ集計結果グラフ表示の印刷サイズは A4 横が想定されています。

7.4.5　監査ログ集計パターンの編集

監査ログ集計画面では，指定した集計条件を保存できます。監査ログを同じ条件で何度も集計したいときなどに便利です。保存した集計条件のことを**集計パターン**と呼びます。

また，作成した集計パターンは，統計パターンとしても使用できます。統計パターンの詳細については「7.5.4　監査ログ統計パターンの設定」を参照してください。

ここでは，集計パターンの作成，変更，および削除について説明します。集計パターンの利用方法については「7.4.1(2)　集計パターンを利用する」を参照してください。

なお，監査ログ集計画面には，テンプレートの集計パターンが用意されています。テンプレートの集計パターンについては「11.12　検索パターンおよび集計パターンの一覧」を参照してください。

(1)　集計パターンを作成する

監査ログの集計パターンの作成には，次に示す方法があります。

- 新規に集計パターンを作成します。
  集計条件を新たに作成したい場合，新規に集計パターンを定義します。
- 既存の集計パターンを利用します。
  次に示す方法があります。
  - テンプレートの集計パターンをカスタマイズします。
    監査ログ集計画面にあらかじめ用意されているテンプレートの集計パターンを表示して，収集された監査ログに合わせて集計条件をカスタマイズします。
  - 作成済みの集計パターンをカスタマイズします。
    作成済みの集計パターンを表示して，収集された監査ログに合わせて集計条件をカスタマイズします。

(a)　新規に集計パターンを作成する場合

新規に集計パターンを作成する手順を次に示します。

1. 監査ログの集計条件を入力する。
   監査ログ集計画面で集計条件を入力します。入力できる集計条件の詳細については「7.4.2　監査ログの集計条件項目」を参照してください。

2. 集計パターン名を指定する。
   「集計パターン名」に集計パターンの名称を指定します。64 バイト以内の文字列を入力してください。ただし，集計パターン名の先頭に「@」は指定できません。また，作成先の業務メニュー内にすでに存在するフォルダと同じ名称は，指定できません。

3. [保存] ボタンをクリックする。
   既存の集計パターンと同じ名称を指定した場合，内容が上書きされます。新規の集計パターン名を指定した場合，パターン保存画面が表示されます。

4. パターン保存画面で，作成する集計パターンの保存場所を指定する。
   集計パターンの保存場所をツリー上で指定します。ただし，ルートおよびテンプレートフォルダは保存場所として指定できません。

5. パターン保存画面の［保存］ボタンをクリックする。

指定した集計条件が集計パターンとして保存されます。保存された集計パターンは，ユーザ作成の集計パターンとして「集計パターン名」のリストおよび機能ツリーに追加されます。

(b)　既存の集計パターンを利用する場合

既存の集計パターンをカスタマイズして，集計パターンを作成する手順を次に示します。

1. 集計パターンを選択する。

次のどちらかの方法で，集計条件として使用する集計パターンを選択します。

- 監査ログ管理画面の左フレームの機能ツリーで集計パターン名を選択します。
- 監査ログ集計画面の「集計パターン名」リストで集計パターン名を選択し，［適用］ボタンをクリックします。

監査ログ集計画面に，集計パターンとして保存されている集計条件が表示されます。

2. 集計条件を変更する。

監査ログ集計画面に表示された集計条件を変更します。指定できる集計条件の詳細については「7.4.2 監査ログの集計条件項目」を参照してください。

3. 集計パターン名を指定する。

「集計パターン名」に新たな集計パターンの名称を指定します。64 バイト以内の文字列を入力してください。ただし，集計パターン名の先頭に「@」は指定できません。また，作成先の業務メニュー内にすでに存在するフォルダと同じ名称は，指定できません。

4. ［保存］ボタンをクリックする。

既存の集計パターンと同じ名称を指定した場合，内容が上書きされます。新規の集計パターン名を指定した場合，パターン保存画面が表示されます。

5. パターン保存画面で作成する集計パターンの保存場所を指定します。

集計パターンの保存場所をツリー上で指定します。ただし，ルートおよびテンプレートフォルダは保存場所として指定できません。

6. パターン保存画面の［保存］ボタンをクリックする。

指定した集計条件が集計パターンとして保存されます。保存された集計パターンは，ユーザ作成の集計パターンとして「集計パターン名」のリストおよび機能ツリーに追加されます。

(2)　集計パターンを変更する

既存の集計パターンの集計条件を変更する手順を次に示します。

なお，テンプレートの集計パターンは変更できません。テンプレートの集計パターンを変更して保存したい場合は，別の名称を指定して保存してください。

1. 集計パターンを選択する。

次のどちらかの方法で，集計条件として使用する集計パターンを選択します。

- 監査ログ管理画面の左フレームの機能ツリーで集計パターン名を選択します。
- 監査ログ集計画面の「集計パターン名」リストで集計パターン名を選択し，［適用］ボタンをクリックします。

監査ログ集計画面に，集計パターンとして保存されている集計条件が表示されます。

2. 集計条件を変更する。

監査ログ集計画面に表示された集計条件を変更します。指定できる集計条件の詳細については「7.4.2 監査ログの集計条件項目」を参照してください。

3. 集計パターン名を変更しないで，［保存］ボタンをクリックする。

監査ログ集計画面に表示されている集計条件が，集計パターンとして上書き保存されます。

なお，別の名称を指定して保存すると，新規に集計パターンが作成されます。

(3) 集計パターンを削除する

監査ログの集計パターンを削除する手順を次に示します。

なお，テンプレートの集計パターンは削除できません。

1. 集計パターンを選択する。

次のどちらかの方法で，集計条件として使用する集計パターンを選択します。

- 監査ログ管理画面の左フレームの機能ツリーで集計パターン名を選択します。
- 監査ログ集計画面の「集計パターン名」リストで集計パターン名を選択します。

2. ［削除］ボタンをクリックする。

選択した集計パターン名が削除されます。

上記の手順以外に，パターン表示編集画面で集計パターンを削除することもできます。詳細については「7.8.5 パターンやフォルダを削除する」を参照してください。

注意事項

上書き保存された集計パターンを統計パターンとして設定している場合，統計パターンも連動して変更されます。統計パターンが変更されると，変更前の統計パターンを基にした統計結果を正しく出力できないことがあります。この場合，統計情報を生成し直してください。

また，集計パターンを削除すると，連動して統計パターンも削除されます。統計パターンが削除されると，削除した統計パターンを基にした統計結果を出力できなくなります。

7.5　監査ログ統計

監査ログ管理画面で必要な条件を指定して，監査ログ管理データベースに生成された監査ログの統計情報を基に，統計結果をグラフ形式で表示したり，CSV 形式で出力したりできます。監査ログの統計情報の生成や統計結果の出力の詳細については「2.6　監査ログの統計情報の生成と統計結果の出力」を参照してください。

例えば，次のような条件で監査ログの統計結果を出力します。

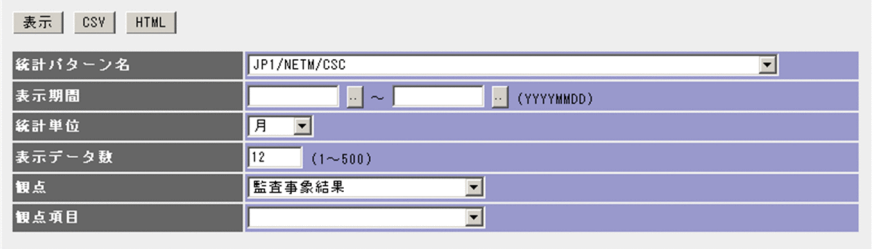
- ログインに失敗したログ件数の推移を月ごとにグラフ形式で表示する。
- JP1/AJS で発生したジョブ登録数の推移を月ごとにグラフ形式で表示する。

なお，統計情報は統計パターンに従って生成されます。統計パターンとは，集計パターンの集計条件を基にして設定する条件のことです。

統計情報によって，統計結果を画面上に表示したり，ファイルに出力したりできます。

監査ログの統計結果の出力は，監査ログの統計画面で実行できます。監査ログの統計画面を次に示します。

図 7-13　監査ログ統計画面



この節では，監査ログの統計結果を出力する手順，統計出力条件として指定できる項目，統計結果の確認方法，および統計パターンの設定方法を説明します。

監査ログ統計画面の各部の名称と使い方については「11.5　監査ログ統計画面」を参照してください。

7.5.1　監査ログの統計

収集された監査ログの統計結果を出力する手順を次に示します。

1. 監査ログ統計画面を表示する。
   機能ツリーで「監査ログ統計」をクリックすると，監査ログ統計画面が表示されます。

2. 統計出力条件を指定する。
   指定できる統計出力条件の詳細については「7.5.2　監査ログの統計出力条件項目」を参照してください。
   なお，統計出力条件のうち，統計パターンは事前に設定しておく必要があります。統計パターンを設定していない場合，統計結果を出力できません。

また，統計出力条件はデフォルトを設定できます。統計パターンおよび統計出力条件のデフォルトを設定する方法については「7.7.3　監査ログ統計画面の表示項目を設定する」を参照してください。

3. 統計情報を生成する。

統計情報は次のどちらかの方法で生成できます。

- ［マネージャセットアップ］ダイアログの「監査ログ統計情報の収集時生成」で設定する
  詳細については「5.5.6(2)　［マネージャセットアップ］ダイアログの設定内容」を参照してください。
- admstgen コマンドを実行する
  コマンドの詳細については「12.　コマンド」の「admstgen（監査ログの統計情報生成）」を参照してください。

4. 統計結果を出力する。

- 統計結果をグラフ形式で表示したい場合は，［表示］ボタンをクリックしてください。
- 統計結果を CSV 形式ファイルで出力したい場合は，［CSV］ボタンをクリックしてください。
- グラフ形式の統計結果を HTML 形式で出力したい場合は，［HTML］ボタンをクリックしてください。

統計出力条件に一致した監査ログの統計結果が出力されます。監査ログの統計結果の見方については「7.5.3　監査ログ統計結果の確認」を参照してください。

7.5.2　監査ログの統計出力条件項目

監査ログ統計画面で，統計出力条件として指定できる項目について説明します。

統計情報を基にして統計結果を出力するときの表示条件を**統計出力条件**と呼びます。

なお，統計出力条件は表示設定画面でデフォルトを設定できます。使用する頻度の高い統計出力条件は，デフォルトとして設定しておくと便利です。統計出力条件のデフォルトを設定する方法については「7.7.3 監査ログ統計画面の表示項目を設定する」を参照してください。

統計出力条件として指定できる項目を，次の表に示します。それぞれの統計出力条件項目のデフォルトは，表示設定画面での設定内容が反映されます。

表 7-12　統計出力条件として指定できる項目

項番	統計出力条件	説明
1	統計パターン名	統計情報を生成するための統計パターンを指定します。この項目は必ず指定してください。 なお，統計パターンは事前に表示設定画面で設定しておく必要があります。設定していない場合，統計結果を出力できません。

項番	統計出力条件	説明
		統計パターンの設定については「7.5.4　監査ログ統計パターンの設定」を参照してください。
2	表示期間	統計結果として出力されるグラフの表示期間を指定します。次の日付を指定してください。 **表示開始日付と表示終了日付** テキストボックスに YYYYMMDD の形式で指定するかまたはカレンダーで指定します。
3	統計単位	統計結果として出力されるグラフの統計単位を指定します。 プルダウンメニューから次のどれかを選択します。 •「日」 •「月」 •「年」
4	表示データ数	統計結果として出力されるグラフの表示数を指定します。 指定できる値は，1～500 です。
5	観点	統計結果を出力する観点を指定します。 プルダウンメニューから次のどちらかを指定します。 •「監査事象種別」 監査事象の種別です。 •「監査事象結果」 監査事象の結果です。
6	観点項目	統計結果を出力する観点項目を指定します。 項番 5 で指定した観点から，さらに項目を絞って統計結果を出力したい場合に指定します。「観点」で指定した内容によって指定できる項目が異なります。 **「観点」で「監査事象種別」を指定した場合** 次に示す監査事象の種別のどれかを指定します。 何も指定しない場合は，すべての種別を対象とした統計結果のグラフが表示されます。 • 開始/停止 • 認証 • アクセス制御 • 重要情報アクセス • 障害発生 • リンク状態 • 外部通信 • 設定情報アクセス • メンテナンス • しきい値オーバー • アクション実行 **「観点」で「監査事象結果」を指定した場合** 次に示す監査事象の結果のどれかを指定します。

項番	統計出力条件	説明
		何も指定しない場合は，すべての種別を対象とした統計結果のグラフが表示されます。 • 成功 • 失敗 • 発生

7.5.3　監査ログ統計結果の確認

監査ログの統計結果は，グラフ形式で画面に表示するか，ファイルに出力して確認します。

統計結果の出力方法を，次に示します。

表 7-13　監査ログ統計結果の出力方法

項番	統計結果の出力方法	説明
1	グラフ形式で表示する	画面上に統計結果をグラフ形式で表示して確認できます。統計結果をグラフ形式で表示する場合については「(1)　監査ログ統計結果をグラフ形式で表示する場合」を参照してください。
2	CSV 形式ファイルを出力する	統計結果を CSV 形式で出力できます。CSV 形式ファイルを出力する場合については「(2)　CSV 形式ファイルを出力する場合」を参照してください。
3	HTML 形式ファイルを出力する	統計結果を HTML 形式で出力できます。HTML 形式ファイルを出力する場合については「(3)　HTML 形式ファイルを出力する場合」を参照してください。

それぞれの出力方法での，統計結果の見方を次に説明します。

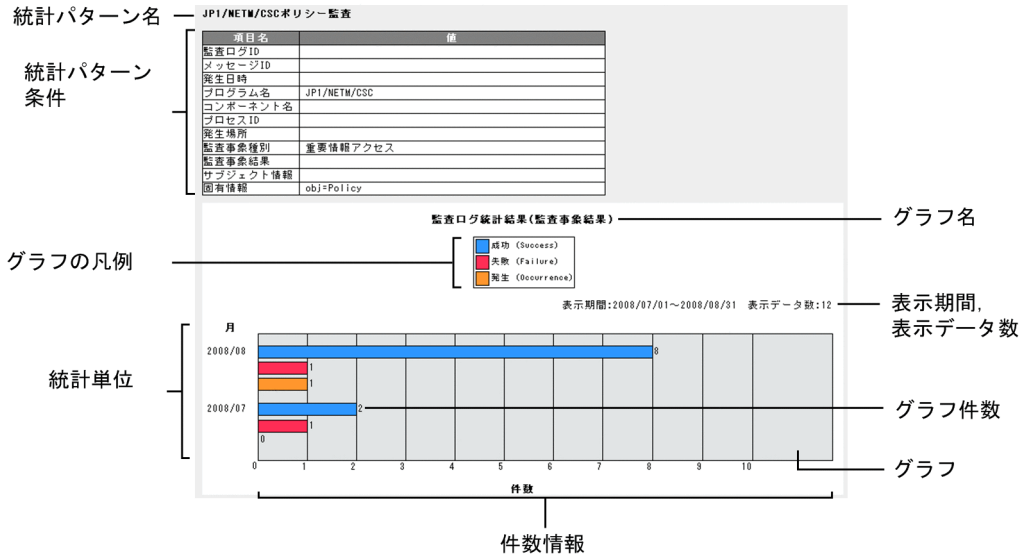
(1)　監査ログ統計結果をグラフ形式で表示する場合

監査ログ統計画面で統計出力条件を指定して［表示］ボタンをクリックすると，統計結果をグラフ形式で表示できます。

ここでは，監査ログ統計画面に表示される統計結果の見方について説明します。

グラフ形式で表示された監査ログ統計結果を次に示します。

図 7-14　監査ログ統計結果



統計結果として出力される項目を次に示します。

表 7-14　統計結果として出力される項目

項番	項目名	説明
1	統計パターン名	統計出力条件として指定した統計パターン名が表示されます。
2	統計パターン条件	統計出力条件として指定した統計パターン条件が表示されます。 統計パターン条件の各項目の詳細については，表 7-6 を参照してください。
3	グラフ名	グラフ名が表示されます。
4	グラフの凡例	統計出力条件として指定した観点や観点項目に基づいたグラフの凡例が表示されます。
5	表示期間	統計出力条件として指定した表示期間が表示されます。
6	表示データ数	統計出力条件として指定した表示データ数が表示されます。
7	統計単位	グラフの縦軸として，統計出力条件として指定した統計単位が表示されます。
8	グラフ	指定した統計単位ごとに，統計結果がグラフで表示されます。
9	グラフ件数	統計結果のグラフ件数が表示されます。
10	件数情報	グラフの横軸として，集計件数の目盛りの数値が表示されます。横軸の長さは固定で，それぞれの数値はグラフの最大件数によって調整されます。

(2)　CSV 形式ファイルを出力する場合

監査ログ統計画面で統計出力条件を指定して［CSV］ボタンをクリックすると，ファイルをダウンロードするダイアログが表示され，監査ログ統計結果が CSV 形式で出力されます。

CSV 形式ファイルには，指定した統計出力条件，統計パターン条件，および統計結果が出力されます。

CSV 形式ファイルの出力例を次に示します。

```
"監査ログ統計"
"統計出力条件"
"項目名","値"
"統計パターン名","JP1/AJS3 監査"
"統計単位","月"
"表示データ数","12"
"観点","監査事象結果"
"観点項目",""
"統計パターン条件"
"項目名","値"
"監査ログ ID",""
"メッセージ ID",""
"発生日時","2009/08/19 00:00:00 ～ 2009/11/19 00:00:00"
"プログラム名","JP1/AJS3"
"コンポーネント名",""
"プロセス ID",""
"発生場所",""
"監査事象種別",""
"監査事象結果",""
"サブジェクト情報",""
"固有情報",""
"統計結果"
"統計単位","成功","失敗","発生"
"2009/08","149","1","150"
"2009/09","200","0","200"
"2009/10","98","2","100"
```

CSV 形式ファイルに出力される項目のうち，統計出力条件として表示される項目については，表 7-14 を参照してください。また，統計パターン条件として表示される項目については，表 7-6 を参照してください。

統計結果として出力される項目を次の表に示します。

表 7-15　統計結果として出力される項目

項番	項目名		説明
1	統計単位		グラフの縦軸として表示されている統計単位として「日」，「月」，または「年」が表示されます。
2	監査事象種別	開始/停止	グラフの凡例として表示されているそれぞれの監査事象種別の集計件数が表示されます。 なお，表示される監査事象種別は，統計出力条件の観点項目として指定した値です。
		認証	
		アクセス制御	
		重要情報アクセス	

項番	項目名		説明
		障害発生	
		リンク状態	
		外部通信	
		設定情報アクセス	
		メンテナンス	
		しきい値オーバー	
		アクション実行	
3	監査事象結果	成功	グラフの凡例として表示されている監査事象結果の集計件数が表示されます。 なお，表示される監査事象結果は，統計出力条件の観点項目として指定した値です。
		失敗	
		発生	

(3) HTML 形式ファイルを出力する場合

監査ログ統計画面で統計出力条件を指定して［HTML］ボタンをクリックすると，ファイルをダウンロードするダイアログが表示され，監査ログ統計結果が HTML 形式で出力されます。

7.5.4 監査ログ統計パターンの設定

監査ログ統計画面では，統計結果の基となる統計情報を生成するための条件を設定する必要があります。統計情報を生成するために設定する条件のことを**統計パターン**と呼びます。

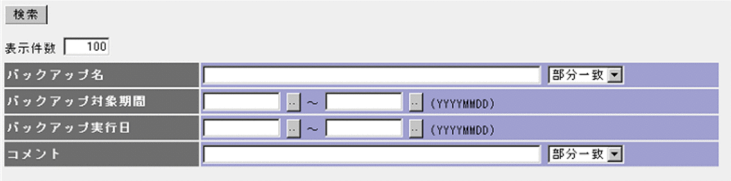
この統計パターンは，監査ログ統計画面で統計出力条件として設定する前に，表示設定画面で設定しておく必要があります。設定していない場合，統計結果を出力できません。なお，統計パターンは作成した集計パターンを基にして設定します。統計パターンの設定方法については「7.7.3 監査ログ統計画面の表示項目を設定する」を参照してください。

7.6　バックアップ履歴の確認

監査ログ管理画面で，バックアップ操作を実行した日付や，バックアップファイルに含まれる監査ログが収集された日付から，バックアップ履歴を検索できます。また，検索したバックアップ履歴から，バックアップファイルをダウンロードできます。

バックアップ履歴の検索は，バックアップ履歴画面で実行できます。バックアップ履歴画面を次に示します。

図 7-15　バックアップ履歴画面



この節では，バックアップ履歴を検索する手順，検索条件として指定できる項目，検索結果の確認方法，およびバックアップファイルをダウンロードする手順を説明します。バックアップ履歴画面の各部の名称と使い方については「11.6　バックアップ履歴画面」を参照してください。

7.6.1　バックアップ履歴を検索する

バックアップ履歴を検索する手順を次に示します。

1. バックアップ履歴画面を表示する。
   機能ツリーで「バックアップ履歴」をクリックすると，バックアップ履歴画面が表示されます。
2. 検索条件を指定する。
   指定できる検索条件の詳細については「7.6.2　バックアップ履歴の検索条件項目」を参照してください。
3. [検索] ボタンをクリックする。
   検索条件に一致したバックアップ操作の履歴がバックアップ履歴一覧に表示されます。バックアップ履歴一覧の見方については「7.6.3　バックアップ履歴検索結果の確認」を参照してください。

7.6.2　バックアップ履歴の検索条件項目

バックアップ履歴の検索条件として指定できる項目を次の表に示します。

表 7-16　バックアップ履歴の検索条件として指定できる項目

項番	検索条件	説明
1	バックアップ名※1	バックアップファイルの名称を指定します。

項番	検索条件	説明
		バックアップ名 テキストボックスに，256 バイト以内の文字列を入力します。 なお，バックアップ名は「完全一致」，「部分一致」，「前方一致」，または「後方一致」を選択して検索できます。デフォルトは「部分一致」です。
2	バックアップ対象期間	バックアップファイルに保存された監査ログが収集された期間（開始日と終了日）を指定します。 **バックアップ対象期間** テキストボックスに YYYYMMDD※2 の形式で指定するか，カレンダーで指定します。
3	バックアップ実行日	バックアップ操作を実施した期間（開始日と終了日）を指定します。 **バックアップ実行日** テキストボックスに YYYYMMDD※2 の形式で指定するか，カレンダーで指定します。
4	コメント※1	バックアップ操作を行ったときに付与したコメントを指定します。 **コメント** テキストボックスに 256 バイト以内の文字を入力します。 なお，コメントは「完全一致」，「部分一致」，「前方一致」，または「後方一致」を選択して検索できます。デフォルトは「部分一致」です。
5	バックアップ ID※3	バックアップファイルを特定するための ID を指定します。 **バックアップ ID** テキストボックスに 1～2147483647 の整数を入力します。 なお，バックアップ ID の範囲は「以下」，「等しい」，または「以上」を選択して検索できます。デフォルトは「以下」です。

注※1

バックアップ履歴を検索する場合，文字列条件プルダウンメニューの選択によって，大文字小文字の区別は次のようになります。

文字列条件プルダウンメニューの選択	大文字小文字の区別
完全一致	区別する
部分一致	区別しない
前方一致	
後方一致	

注※2

YYYY は年，MM は月，DD は日です。「/」は入力できません。

注※3

デフォルトでは非表示です。この項目を表示する方法については「7.7　監査ログ管理画面の表示設定」を参照してください。

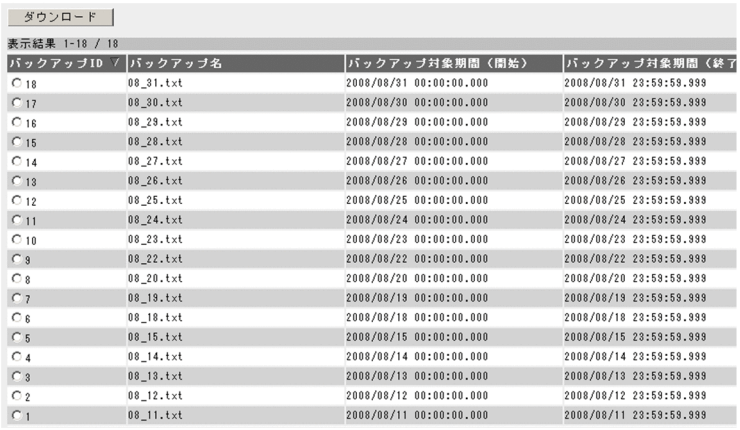
7.6.3　バックアップ履歴検索結果の確認

検索結果は，バックアップ履歴画面のバックアップ履歴一覧で確認します。検索結果が複数ページにわたる場合のページの移動は，検索結果一覧のページリンク（「<<」，「<」，「>」，「>>」）をクリックするかまたはページ番号を直接指定してください。

検索結果一覧には，表 7-17 の項目が表示されます。ただし，表示設定画面で項目の数や並び順などを設定している場合は，検索結果一覧に設定内容が反映されます。表示設定の方法については「7.7　監査ログ管理画面の表示設定」を参照してください。なお，表示設定画面で設定した「レコード件数/ページ」の値は，バックアップ履歴画面の「表示件数」で変更できます。

バックアップ履歴検索結果一覧を次に示します。

図 7-16　バックアップ履歴検索結果一覧



バックアップ履歴一覧に表示される項目を次の表に示します。

表 7-17　バックアップ履歴の検索結果として表示される項目

項番	項目名	説明
1	バックアップ ID	バックアップ操作を特定する ID です。
2	バックアップ名	バックアップファイルの名称です。
3	バックアップ対象期間（開始/終了）	バックアップファイルに保存された監査ログが収集された期間（開始日と終了日）です。次に示す形式で表示されます。 YYYY/MM/DD hh:mm:ss.ttt（年/月/日 時:分:秒.ミリ秒）
4	バックアップ実行日	バックアップ操作をした日時です。次に示す形式で表示されます。 YYYY/MM/DD hh:mm:ss.ttt（年/月/日 時:分:秒.ミリ秒）
5	コメント	バックアップ操作時にバックアップファイルに付与したコメントです。

7.6.4　バックアップファイルをダウンロードする

バックアップ履歴画面で検索したバックアップ履歴一覧から，バックアップファイルをダウンロードする手順を次に示します。

1. バックアップ履歴画面の検索結果一覧から，取得したいバックアップファイルの「バックアップ ID」を選択する。
2. [ダウンロード] ボタンをクリックする。
   ファイルをダウンロードするダイアログが表示されます。
3. [保存] のボタンをクリックする。
   バックアップファイルの保存先は，ローカルディスク上の任意のフォルダを指定してください。

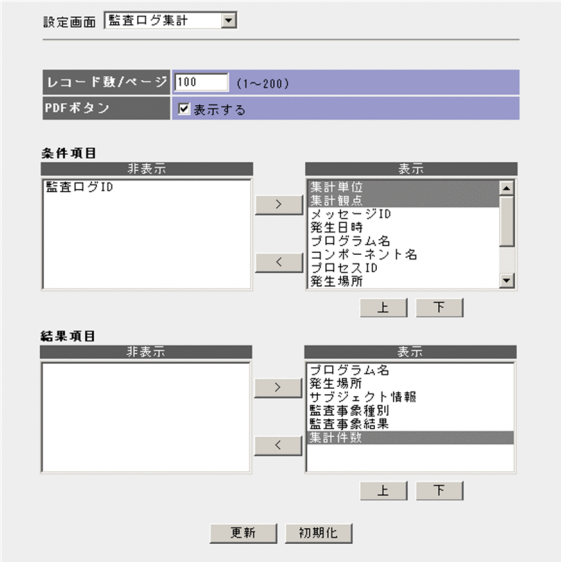
なお，監査ログのバックアップファイルをダウンロードするには，監査ログ管理サーバで，Microsoft Internet Information Services のセットアップが必要です。Microsoft Internet Information Services の設定については「5.5.1　Microsoft Internet Information Services をセットアップする」を参照してください。

7.7　監査ログ管理画面の表示設定

監査ログ管理画面の各画面で使用する項目の表示設定ができます。

各画面の項目の表示設定は，表示設定画面で実行できます。表示設定画面は，機能ツリーで「表示設定」をクリックすると表示されます。表示設定画面を次に示します。

図 7-17　表示設定画面



この節では，監査ログ管理画面の各画面の表示を設定する手順と各画面の設定項目について説明します。表示設定画面の詳細については「11.7　表示設定画面」を参照してください。

7.7.1　監査ログ検索画面の表示項目を設定する

表示設定画面では，監査ログ検索画面をカスタマイズできます。また，カスタマイズした画面設定を初期状態に戻すこともできます。

ここでは，監査ログ検索画面のカスタマイズと初期化について説明します。

(1)　監査ログ検索画面をカスタマイズする

監査ログ検索画面で使用する項目の表示・非表示を変えたり，項目の並び順を入れ替えたりできます。

監査ログ検索画面の表示項目を設定する手順を次に示します。

1. **［設定画面］プルダウンメニューから「監査ログ検索」を選択する。**
   監査ログ検索画面の表示項目を設定するための表示設定画面が表示されます。

2. **監査ログ検索画面で使用する項目の表示・非表示を設定する。**
   必要に応じて，検索条件および検索結果として使用する項目の表示・非表示を設定します。

検索条件として使用する項目の表示・非表示を設定したい場合

「条件項目」にある［>］または［<］ボタンをクリックして，項目の表示・非表示を設定します。

検索結果として使用する項目の表示・非表示を設定したい場合

「結果項目」にある［>］または［<］ボタンをクリックして，項目の表示・非表示を設定します。

表示設定できる項目については「(3)　監査ログ検索画面の表示設定項目」を参照してください。

3. 監査ログ検索画面で表示する項目の並び順を設定する。

必要に応じて，手順 2 で表示する設定にした項目の並び順を，「上」または「下」ボタンをクリックして，設定します。

4. ［更新］ボタンをクリックする。

設定した情報に更新されます。

注意事項

設定した表示項目の変更は，操作結果を出力した CSV 形式ファイルまたは PDF ファイルには反映されません。

(2)　監査ログ検索画面を初期化する

監査ログ検索画面を初期化する手順を次に示します。

1. ［設定画面］プルダウンメニューから「監査ログ検索」を選択する。

監査ログ検索画面の表示項目を設定するための表示設定画面が表示されます。

2. ［初期化］ボタンをクリックする。

設定した情報が初期状態に戻ります。

(3)　監査ログ検索画面の表示設定項目

表示設定画面に表示される監査ログ検索画面の項目を次の表に示します。

なお，表は条件項目と結果項目で分かれています。

表 7-18　監査ログ検索画面の条件項目（表示設定）

項番	項目名	デフォルト
1	メッセージ ID	表示
2	発生日時	表示
3	プログラム名	表示
4	コンポーネント名	表示
5	プロセス ID	表示
6	発生場所	表示

項番	項目名	デフォルト
7	監査事象種別	表示
8	監査事象結果	表示
9	サブジェクト情報	表示
10	固有情報	表示
11	監査ログ ID	非表示

各項目の詳細については「7.3.2　監査ログの検索条件項目」を参照してください。

表 7-19　監査ログ検索画面の結果項目（表示設定）

項番	項目名	デフォルト
1	監査ログ ID	表示
2	メッセージ ID	表示
3	発生日時	表示
4	プログラム名	表示
5	コンポーネント名	表示
6	プロセス ID	表示
7	発生場所	表示
8	監査事象種別	表示
9	監査事象結果	表示
10	サブジェクト情報	表示
11	固有情報	表示

各項目の詳細については「7.3.3　監査ログ検索結果の確認」を参照してください。

7.7.2　監査ログ集計画面の表示項目を設定する

表示設定画面では，監査ログ集計画面をカスタマイズできます。また，カスタマイズした画面設定を初期状態に戻すこともできます。

ここでは，監査ログ集計画面のカスタマイズと初期化について説明します。

(1)　監査ログ集計画面をカスタマイズする

監査ログ集計画面で使用する項目の表示・非表示を変えたり，項目の並び順を入れ替えたりできます。

監査ログ集計画面の表示項目を設定する手順を次に示します。

1. [設定画面] プルダウンメニューから「監査ログ集計」を選択する。
   監査ログ集計画面の表示項目を設定するための表示設定画面が表示されます。

2. 監査ログ集計画面で使用する項目の表示・非表示を設定する。
   必要に応じて，集計条件および集計結果として使用する項目の表示・非表示を設定します。

   集計条件として使用する項目の表示・非表示を設定したい場合
   「条件項目」にある［>］または［<］ボタンをクリックして，項目の表示・非表示を設定します。

   集計結果として使用する項目の表示・非表示を設定したい場合
   「結果項目」にある［>］または［<］ボタンをクリックして，項目の表示・非表示を設定します。

   表示設定できる項目については「(3)　監査ログ集計画面の表示設定項目」を参照してください。

3. 監査ログ集計画面で表示する項目の並び順を設定する。
   必要に応じて，手順 2 で表示する設定にした項目の並び順を，「上」または「下」ボタンをクリックして，設定します。

4. [更新] ボタンをクリックする。
   設定した情報に更新されます。

注意事項
設定した表示項目の変更は，操作結果を出力した CSV 形式ファイルまたは PDF ファイルには反映されません。

(2)　監査ログ集計画面を初期化する

監査ログ集計画面を初期化する手順を次に示します。

1. [設定画面] プルダウンメニューから「監査ログ集計」を選択する。
   監査ログ集計画面の表示項目を設定するための表示設定画面が表示されます。

2. [初期化] ボタンをクリックする。
   設定した情報が初期状態に戻ります。

(3)　監査ログ集計画面の表示設定項目

表示設定画面に表示される監査ログ集計画面の項目を次の表に示します。

なお，表は条件項目と結果項目で分かれています。

表 7-20　監査ログ集計画面の条件項目（表示設定）

項番	項目名	デフォルト
1	集計単位	表示※
2	集計観点	表示※

項番	項目名	デフォルト
3	メッセージ ID	表示
4	発生日時	表示
5	プログラム名	表示
6	コンポーネント名	表示
7	プロセス ID	表示
8	発生場所	表示
9	監査事象種別	表示
10	監査事象結果	表示
11	サブジェクト情報	表示
12	固有情報	表示
13	監査ログ ID	非表示

注※

これらの項目は非表示にできません。

各項目の詳細については「7.4.2　監査ログの集計条件項目」を参照してください。

表 7-21　監査ログ集計画面の結果項目（表示設定）

項番	項目名	デフォルト
1	プログラム名	表示
2	発生場所	表示
3	サブジェクト情報	表示
4	監査事象種別	表示
5	監査事象結果	表示
6	集計件数	表示※

注※

この項目は非表示にできません。

各項目の詳細については「7.4.3　監査ログ集計結果の確認」を参照してください。

7.7.3　監査ログ統計画面の表示項目を設定する

表示設定画面では，監査ログ統計画面のデフォルトや，統計パターンを設定できます。また，設定内容を初期状態に戻すこともできます。

ここでは，監査ログ統計画面のカスタマイズと初期化について説明します。

(1)　監査ログ統計画面をカスタマイズする

監査ログ統計画面で使用する項目のデフォルトを設定できます。また，作成した集計パターンを基にして統計パターンを設定できます。

監査ログ統計画面の表示項目を設定する手順を次に示します。

1. [設定画面] プルダウンメニューから「監査ログ統計」を選択する。
   監査ログ統計画面の表示項目を設定するための表示設定画面が表示されます。

2. 監査ログ統計画面で使用する項目のデフォルトを設定する。
   必要に応じて，統計出力条件として使用する項目のデフォルトを設定します。
   デフォルトの設定項目については「(3)　監査ログ統計画面の表示設定項目」を参照してください。

3. 監査ログ統計画面の統計出力条件で使用する統計パターンを設定する。
   「統計パターン」の「非表示」には，すでに作成されている集計パターンが表示されます。これらを「表示」に設定すると，集計単位および集計観点を除いた集計パターンの集計条件が，統計パターンとして設定されます。「表示」に設定した統計パターンを基に，統計情報が生成されます。
   「統計パターン」にある［>］または［<］ボタンをクリックして統計パターンを設定してください。

4. [更新] ボタンをクリックする。
   設定した情報に更新されます。

(2)　監査ログ統計画面を初期化する

監査ログ統計画面を初期化する手順を次に示します。

なお，初期化できるのは統計出力条件のデフォルトの設定だけです。統計パターンの設定内容は初期化できません。

1. [設定画面] プルダウンメニューから「監査ログ統計」を選択する。
   監査ログ統計画面の表示項目を設定するための表示設定画面が表示されます。

2. [初期化] ボタンをクリックする。
   設定した情報が初期状態に戻ります。ただし，統計パターンの設定内容は初期化されません。

(3)　監査ログ統計画面の表示設定項目

表示設定画面に表示される監査ログ統計画面の項目を次の表に示します。

表 7-22　監査ログ統計画面のデフォルトの設定項目

項番	項目名	説明	デフォルト
1	時間順	指定した統計単位ごとに表示されるグラフの表示順の，監査ログ統計画面でのデフォルトを指定します。	「昇順」

項番	項目名	説明	デフォルト
		次のどちらかを選択します。 •「昇順」 •「降順」	
2	統計単位	グラフの統計単位の，監査ログ統計画面でのデフォルトを指定します。 プルダウンメニューから次のどれかを選択します。 •「日」 •「月」 •「年」	「月」
3	表示データ数	グラフの表示数の，監査ログ統計画面でのデフォルトを指定します。 指定できる値は，1～500 です。	12
4	観点	統計結果を出力する観点の，監査ログ統計画面でのデフォルトを指定します。 プルダウンメニューから次のどちらかを選択します。 •「監査事象種別」 •「監査事象結果」 ただし，次に示す場合，表示設定画面の設定内容は監査ログ統計画面には反映されません。 **統計パターン条件として監査事象結果を指定している場合** 監査事象結果がデフォルトで表示されます。 **統計パターン条件として監査事象種別だけを指定している場合** 監査事象種別がデフォルトで表示されます。 統計パターン条件として両方とも指定していない場合は，表示設定画面で設定した内容が反映されます。	「監査事象結果」
5	観点項目	必要に応じて，統計結果を出力する観点項目の，監査ログ統計画面でのデフォルトを指定します。 「観点」で指定した内容によって指定する項目が異なります。 **「観点」で「監査事象種別」を指定した場合** 次に示す監査事象の種別のどれかを指定します。 • 開始/停止 • 認証 • アクセス制御 • 重要情報アクセス • 障害発生 • リンク状態 • 外部通信 • 設定情報アクセス • メンテナンス • しきい値オーバー • アクション実行	なし

項番	項目名		説明	デフォルト
			「観点」で「監査事象結果」を指定した場合 次に示す監査事象の結果のどれかを指定します。 • 成功 • 失敗 • 発生	
6	統計パターン	非表示	統計パターンとして設定していない集計パターンが表示されます。	－
7		表示	統計パターンとして設定している集計パターンが表示されます。	

（凡例）

－：該当しない

7.7.4　バックアップ履歴画面の表示項目を設定する

表示設定画面では，バックアップ履歴画面をカスタマイズできます。また，カスタマイズした画面設定を初期状態に戻すこともできます。

ここでは，バックアップ履歴画面のカスタマイズと初期化について説明します。

(1)　バックアップ履歴画面をカスタマイズする

バックアップ履歴画面で使用する項目の表示・非表示を変えたり，項目の並び順を入れ替えたりできます。

バックアップ履歴画面の表示項目を設定する手順を次に示します。

1. ［設定画面］プルダウンメニューから「バックアップ履歴」を選択する。
   バックアップ履歴画面の表示項目を設定するための表示設定画面が表示されます。

2. バックアップ履歴画面で使用する項目の表示・非表示を設定する。
   必要に応じて，検索条件および検索結果として使用する項目の表示・非表示を設定します。

   検索条件として使用する項目の表示・非表示を設定したい場合
   「条件項目」にある［＞］または［＜］ボタンをクリックして，項目の表示・非表示を設定します。

   検索結果として使用する項目の表示・非表示を設定したい場合
   「結果項目」にある［＞］または［＜］ボタンをクリックして，項目の表示・非表示を設定します。

   表示設定できる項目については「(3)　バックアップ履歴画面の表示設定項目」を参照してください。

3. バックアップ履歴画面で表示する項目の並び順を設定する。
   必要に応じて，手順 2 で表示する設定にした項目の並び順を，「上」または「下」ボタンをクリックして，設定します。

4. ［更新］ボタンをクリックする。

設定した情報に更新されます。

(2) バックアップ履歴画面を初期化する

バックアップ履歴画面を初期化する手順を次に示します。

1. [設定画面] プルダウンメニューから，「バックアップ履歴」を選択する。
   バックアップ履歴画面の表示項目を設定するための表示設定画面が表示されます。

2. [初期化] ボタンをクリックする。
   設定した情報が初期状態に戻ります。

(3) バックアップ履歴画面の表示設定項目

表示設定画面に表示されるバックアップ履歴画面の項目を次の表に示します。

なお，表は検索条件と結果項目で分かれています。

表 7-23 バックアップ履歴画面の条件項目（表示設定）

項番	項目名	デフォルト
1	バックアップ名	表示
2	バックアップ対象期間	表示※
3	バックアップ実行日	表示※
4	コメント	表示
5	バックアップ ID	非表示

注※
これらの項目は非表示にできません。

各項目の詳細については「7.6.2 バックアップ履歴の検索条件項目」を参照してください。

表 7-24 バックアップ履歴画面の結果項目（表示設定）

項番	項目名	デフォルト
1	バックアップ ID	表示※
2	バックアップ名	表示
3	バックアップ対象期間	表示
4	バックアップ実行日	表示
5	コメント	表示

注※
この項目は非表示にできません。

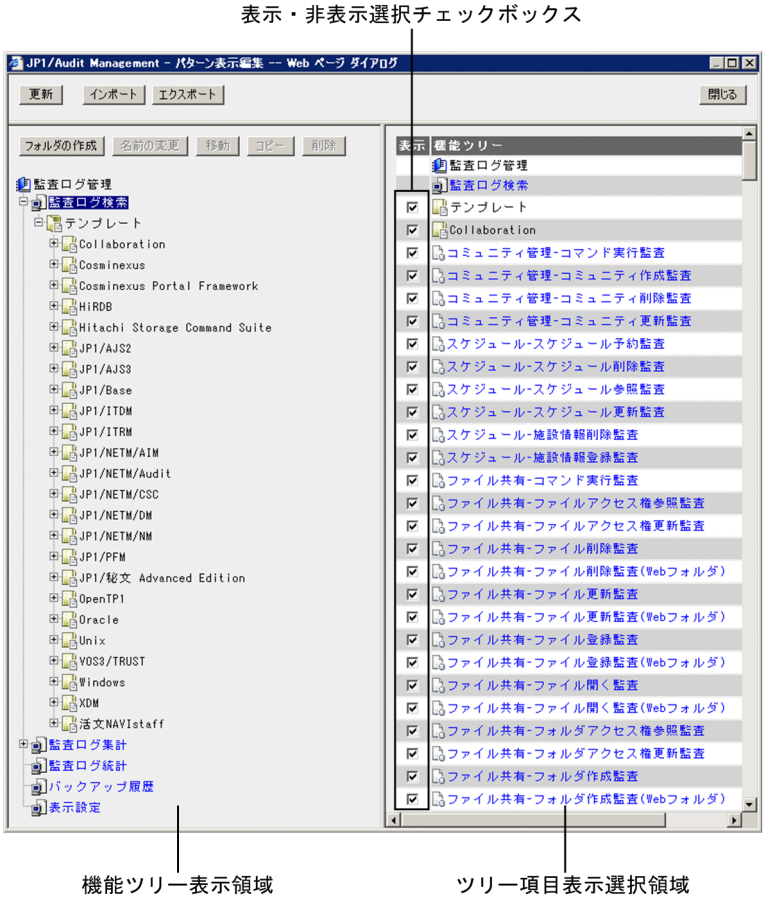
各項目の詳細については「7.6.3　バックアップ履歴検索結果の確認」を参照してください。

7.8　機能ツリーのパターン表示編集

機能ツリーのパターン表示について編集できます。ユーザ作成のパターンを格納するフォルダを作成できるので，プログラム単位や観点単位など，パターンを分類して管理できます。また，不要なパターンを非表示にすることで機能ツリーの利便性が向上します。

編集は，パターン表示編集画面で実行できます。パターン表示編集画面は，機能ツリーで［パターン表示編集］のリンクをクリックすると表示されます。パターン表示編集画面を次に示します。

図 7-18　パターン表示編集画面



［更新］ボタンをクリックすると，編集内容を監査ログ管理画面の機能ツリーに反映して，この画面を閉じます。［閉じる］ボタンまたは［×］ボタンをクリックすると，編集内容を破棄して，この画面を閉じます。

このほか，パターン表示編集画面では，ユーザ作成のフォルダやパターンの情報をエクスポートおよびインポートできます。これらの操作によって，ほかのサーバ環境との間で情報の移行ができます。例えば，監査ログ管理サーバで使用しているフォルダやパターンの情報を，監査ログ閲覧サーバで流用するなど，環境移行時の利便性が向上します。

この節では，機能ツリーのパターン表示を編集する手順とユーザ作成のフォルダやパターンを移行する手順について説明します。パターン表示編集画面の各部の名称と使い方については「11.10　パターン表示編集画面」を参照してください。

次の表に，ツリー項目ごとに実行できる操作を示します。

表 7-25　ツリー項目ごとに実行できる操作

項番	ツリー項目の種類	実行できる操作				
		フォルダの作成	名前の変更	移動	コピー	削除
1	ルート	－※1	－※1	－※1	－※1	－※1
2	業務メニュー※1	○※1	－※1	－※1	－※1	－※1
3	ユーザ作成のフォルダ	○※2	○※1	○※2，※3	○※2，※3	○※1
4	ユーザ作成のパターン	－※1	○※1	○※1	○※1	○※1
5	テンプレート※4	－※1	－※1	－※1	－※1	－※1

（凡例）

○：操作できる

－：操作できない

注※1

業務メニューのうち「監査ログ検索」および「監査ログ集計」を示します。

注※2

フォルダは 10 階層まで作成できます。また，最上位の「ユーザ作成のフォルダ」配下には，ツリー項目を 4,096 個まで作成できます。ただし，ツリー項目を大量（2,000 個が目安）に作成する場合，IIS の送信バッファの最大サイズは，デフォルトより大きい値を設定しておく必要があります。設定方法については「5.5.1(3)　IIS 送信バッファの最大サイズの設定」を参照してください。

注※3

フォルダを選択した場合，配下のすべてのフォルダおよびパターンに対して操作が反映されます。

注※4

「テンプレートのフォルダ」，「テンプレートのプログラムフォルダ」，および「テンプレートのパターン」を示します。

7.8.1　パターンを保存するフォルダを作成する

パターンを保存するフォルダの作成手順を次に示します。

1. 作成先のツリー項目を選択する。

   業務メニューとユーザ作成フォルダだけが選択できます。選択したツリー項目の直下にフォルダが作成されます。

2. ［フォルダの作成］ボタンをクリックする。

   ［フォルダの作成］画面が表示されます。［フォルダの作成］画面については「11.10　パターン表示編集画面」を参照してください。

3. フォルダ名を指定する。

パターンを保存するフォルダの名称を指定します。指定の際は，次のことに注意してください。

- 作成先の業務メニュー内にすでに存在するパターンまたはフォルダと同じ名称は，指定できません。
- 64 バイト以内の文字列で入力してください。
- 名称の先頭に「@」は使用できません。
- 名称中に「¥」は使用できません。

4. [OK] ボタンをクリックする。

選択したツリー項目の直下にフォルダが作成され，パターン表示編集画面に表示が反映されます。

5. [更新] ボタンをクリックする。

パターン表示編集画面で［更新］ボタンをクリックすると，編集した内容が監査ログ管理画面の機能ツリーに反映されます。

7.8.2 パターン名やフォルダ名を変更する

パターン名やフォルダ名を変更する手順を次に示します。

注意事項

集計パターン名を変更すると，連動して統計パターン名も変更されますが，統計情報には影響ありません。

1. 名前を変更したいツリー項目を選択する。

ユーザ作成のパターン名とフォルダ名だけが変更できます。

2. [名前の変更] ボタンをクリックする。

［名前の変更］画面が表示されます。［名前の変更］画面については「11.10 パターン表示編集画面」を参照してください。

3. パターン名やフォルダ名を指定する。

デフォルトでは，選択したツリー項目の名称が入力されています。指定の際は，次のことに注意してください。

- 同じ業務メニュー内にすでに存在するパターンまたはフォルダと同じ名称は，指定できません。
- 64 バイト以内の文字列で入力してください。
- 名称の先頭に「@」は指定できません。
- （フォルダ名の場合）名称中に「¥」は使用できません。

4. [OK] ボタンをクリックする。

パターン名またはフォルダ名が変更され，パターン表示編集画面に表示が反映されます。

5. [更新] ボタンをクリックする。

パターン表示編集画面で［更新］ボタンをクリックすると，編集した内容が監査ログ管理画面の機能ツリーに反映されます。

7.8.3 パターンやフォルダを移動する

パターンやフォルダを移動する手順を次に示します。

注意事項

集計パターンまたは［監査ログ集計］業務メニューのフォルダを［監査ログ検索］業務メニュー配下に移動すると，連動して統計パターンおよび統計情報が削除されます。検索パターンまたは［監査ログ検索］業務メニューのフォルダを［監査ログ集計］業務メニュー配下に移動すると，連動して統計パターンが作成されます。

1. 移動したいツリー項目を選択する。

フォルダを選択した場合，フォルダ配下のツリー項目すべてが移動対象になります。

2. [移動] ボタンをクリックする。

［移動］画面が表示されます。［移動］画面については「11.10 パターン表示編集画面」を参照してください。なお，［移動］画面の機能ツリーには，移動先として指定できるツリー項目だけが表示されます。

3. [OK] ボタンをクリックする。

パターンまたはフォルダが指定先に移動して，パターン表示編集画面に表示が反映されます。

指定先に同じ名称のパターンまたはフォルダが存在した場合

［OK］ボタンをクリックしたあとに警告ダイアログが表示され，［パターン名］または［フォルダ名］に値の入力ができるようになります。

フォルダ名を入力する際は，操作対象のフォルダ名だけを変更できます。操作対象のフォルダ配下のツリー項目は名称を変更できません。

パターン名やフォルダ名を入力してから，再度［OK］ボタンをクリックしてください。

4. [更新] ボタンをクリックする。

パターン表示編集画面で［更新］ボタンをクリックすると，編集した内容が監査ログ管理画面の機能ツリーに反映されます。

パターンまたはフォルダの移動先は，移動先のツリー項目および業務メニューの種類によって指定できるかどうかが異なります。移動先のツリー項目および業務メニューの種類ごとに，移動先として指定できるかどうかについて次の表に示します。

表 7-26　パターンまたはフォルダの移動先の指定可否

項番	移動先のツリー項目	移動先の業務メニューの種類	移動元の業務メニューの種類	
			監査ログ検索	監査ログ集計
1	ルート	なし	−	−
2	業務メニュー※1	監査ログ検索	○	○
3		監査ログ集計	○※2	○
4	ユーザ作成の フォルダ	監査ログ検索	○	○
5		監査ログ集計	○※2	○
6	テンプレート※3	監査ログ検索	−	−
7		監査ログ集計	−	−

（凡例）

○：移動できる

−：移動できない

注

移動先の業務メニュー内に同じ名称のパターンまたはフォルダが存在するときは，移動元のフォルダまたはパターンの名称を変更してください。

注※1

業務メニューのうち［監査ログ検索］および［監査ログ集計］を示します。

注※2

集計単位や集計観点にはデフォルト値が設定されます。集計単位および集計観点のデフォルト値を次に示します。

・集計単位のデフォルト値：発生場所

・集計観点のデフォルト値：監査事象種別

注※3

「テンプレートのフォルダ」および「テンプレートのプログラムフォルダ」を示します。

7.8.4　パターンやフォルダをコピーする

パターンやフォルダをコピーする手順を次に示します。

注意事項

検索パターンまたは［監査ログ検索］業務メニューのフォルダを［監査ログ集計］業務メニュー配下にコピーすると，連動して統計パターンが作成されます。

1. コピーしたいツリー項目を選択する。

フォルダを選択した場合，フォルダ配下のツリー項目すべてがコピー対象になります。

2. ［コピー］ボタンをクリックする。

［コピー］画面が表示されます。［コピー］画面については「11.10　パターン表示編集画面」を参照してください。なお，［コピー］画面の機能ツリーには，コピー先として指定できるツリー項目だけが表示されます。

3. ［OK］ボタンをクリックする。

パターンまたはフォルダが指定先にコピーされ，パターン表示編集画面に表示が反映されます。

指定先に同じ名称のパターンまたはフォルダが存在した場合

［OK］ボタンをクリックしたあとに警告ダイアログが表示され，［パターン名］または［フォルダ名］に値の入力ができるようになります。

フォルダ名を入力する際は，操作対象のフォルダ名だけを変更できます。操作対象のフォルダ配下のツリー項目は名称を変更できません。

パターン名やフォルダ名を入力してから，再度［OK］ボタンをクリックしてください。

4. ［更新］ボタンをクリックする。

パターン表示編集画面で［更新］ボタンをクリックすると，編集した内容が監査ログ管理画面の機能ツリーに反映されます。

パターンまたはフォルダのコピー先は，コピー先のツリー項目および業務メニューの種類によって指定できるかどうかが異なります。コピー先のツリー項目および業務メニューの種類ごとに，コピー先として指定できるかどうかについて次の表に示します。

表 7-27　パターンまたはフォルダのコピー先の指定可否

項番	コピー先のツリー項目	コピー先の業務メニューの種類	コピー元の業務メニューの種類	
			監査ログ検索	監査ログ集計
1	ルート	なし	－	－
2	業務メニュー※1	監査ログ検索	－	○
3		監査ログ集計	○※2	－
4	ユーザ作成のフォルダ	監査ログ検索	－	○
5		監査ログ集計	○※2	－
6	テンプレート※3	監査ログ検索	－	－
7		監査ログ集計	－	－

（凡例）

○：コピーできる

－：コピーできない

注

コピー先の業務メニュー内に同じ名称のパターンまたはフォルダが存在するときは，コピー元のフォルダまたはパターンの名称を変更してください。

注※1

業務メニューのうち［監査ログ検索］および［監査ログ集計］を示します。

注※2

集計単位や集計観点にはデフォルト値が設定されます。集計単位および集計観点のデフォルト値を次に示します。

・集計単位のデフォルト値：発生場所

・集計観点のデフォルト値：監査事象種別

注※3

「テンプレートのフォルダ」および「テンプレートのプログラムフォルダ」を示します。

7.8.5　パターンやフォルダを削除する

パターンやフォルダを削除する手順を次に示します。

注意事項

集計パターンまたは［監査ログ集計］業務メニューのフォルダを削除すると，連動して統計パターンおよび統計情報が削除されます。

1. 削除したいツリー項目を選択する。

ユーザ作成のパターンとフォルダだけが削除できます。フォルダを選択した場合，フォルダ配下のツリー項目すべてが削除対象になります。

2. ［削除］ボタンをクリックする。

3. ［OK］ボタンをクリックする。

パターンまたはフォルダが削除され，パターン表示編集画面に表示が反映されます。

4. ［更新］ボタンをクリックする。

パターン表示編集画面で［更新］ボタンをクリックすると，編集した内容が監査ログ管理画面の機能ツリーに反映されます。集計パターンを削除すると，連動して統計パターンも削除されます。

7.8.6　パターンやフォルダの表示・非表示を設定する

パターンやフォルダの表示・非表示を設定する手順を次に示します。

1. 表示・非表示選択チェックボックスを設定する。

パターンやフォルダを表示する場合

チェックボックスをチェックしてください。デフォルトでは，すべてのチェックボックスがチェックされています。

パターンやフォルダを非表示にする場合

チェックボックスのチェックを外してください。フォルダのチェックを外すと，フォルダ配下のツリー項目すべてが非表示になります。

2. ［更新］ボタンをクリックする。

パターン表示編集画面で［更新］ボタンをクリックすると，編集した内容が監査ログ管理画面の機能ツリーに反映されます。

7.8.7　パターンやフォルダの情報を移行する

機能ツリー表示領域にあるパターンやフォルダの情報をエクスポートとインポートによって移行する手順について，次に示します。なお，エクスポートの対象となるのは，ユーザ作成のパターンとフォルダだけです。

1. 移行元サーバのパターン表示編集画面で［エクスポート］ボタンをクリックする。

   ファイルをダウンロードするダイアログが表示されます。

   ユーザ作成のパターンやフォルダが存在しない場合，［エクスポート］ボタンは選択できません。

2. ［保存］ボタンをクリックする。

   エクスポートした情報が，パターン情報ファイルに出力されます。パターン情報ファイルの詳細については「13.8　パターン情報ファイル」を参照してください。

3. 移行先サーバのパターン表示編集画面で［インポート］ボタンをクリックする。

   ［インポート］画面が表示されます。［インポート］画面については「11.10　パターン表示編集画面」を参照してください。

4. ［上書きしない］または［上書きする］ラジオボタンを選択する。

   インポートする情報と機能ツリー表示領域の情報とで，同一名称のパターンやフォルダが存在する場合に，上書きするかどうかを指定します。

5. 「インポートファイル」にパターン情報ファイルを指定する。

   インポートしたいパターン情報ファイルをフルパスで入力します。［参照］ボタンをクリックすると，ファイルを参照するダイアログからファイル名を指定できます。

6. ［OK］ボタンをクリックする。

   インポート処理が実行され，移行先サーバのパターン表示編集画面に反映されます。なお，［上書きしない］ラジオボタンを選択している場合で，同一名称のパターンやフォルダが存在するときは，インポート処理は実行されません。

インポート処理によって既存のユーザ作成の集計パターンが更新された場合は，統計パターンも更新されるため，統計情報を生成し直してください。

8 監査ログのバックアップ運用

監査証跡管理システムでは，監査ログをバックアップして管理します。この章では，監査ログ管理サーバおよび監査ログ閲覧サーバでのバックアップの運用について説明します。

8.1　監査ログのバックアップ運用の流れ

監査ログをバックアップすることで次に示す運用ができます。

監査ログのバックアップ

監査ログ管理サーバで，admexport コマンドを使用して監査ログをバックアップします。バックアップ方法には日時を指定する期間指定と定期的なバックアップを目的とした差分指定があります。

監査ログのバックアップについては「8.2　監査ログのバックアップ」を参照してください。

監査ログのバックアップファイルのインポート

監査が終了した監査ログを監査ログ閲覧サーバに移動する運用の場合，admimport コマンドを使用して，監査ログ閲覧サーバで監査ログのバックアップファイルをインポートします。

監査ログのバックアップファイルのインポートについては「8.3　監査ログのバックアップファイルのインポート」を参照してください。

監査ログのバックアップファイルの移動

監査ログ管理サーバで admcsvmove コマンドを使用して，監査ログのバックアップファイルを別のフォルダに移動したり，ファイル名を変更したりできます。

監査ログのバックアップファイルの移動については「8.4　監査ログのバックアップファイルの移動」を参照してください。

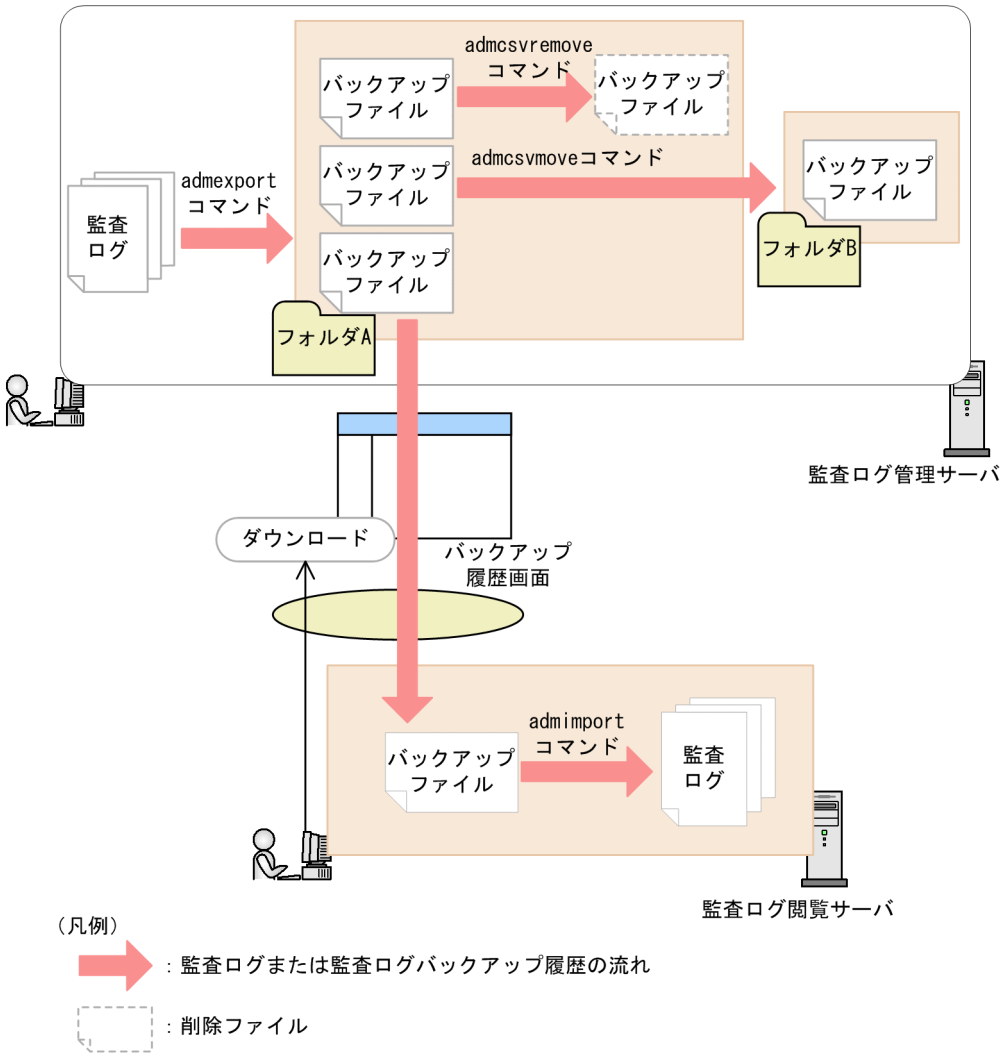
監査ログのバックアップファイルの削除

監査ログ管理サーバで admcsvremove コマンドを使用して，不要な監査ログのバックアップファイルとそのバックアップ履歴を削除できます。

監査ログのバックアップファイルの削除については「8.5　監査ログのバックアップファイルの削除」を参照してください。

監査ログのバックアップ運用の流れを次の図に示します。

図 8-1　監査ログのバックアップ運用の流れ



8.2　監査ログのバックアップ

監査ログ管理サーバでは，監査ログのバックアップファイルを CSV 形式で取得できます。

監査ログのバックアップでは，収集が完了し監査の終了した監査ログやデータベース内への保存期間を経過した監査ログをバックアップします。収集されてデータベースに格納された監査ログが，バックアップの対象となります。収集されていない監査ログは，バックアップの対象となりません。

監査ログをバックアップすると，監査ログ管理データベースにバックアップの実行履歴が登録されます。監査ログのバックアップ履歴は，監査ログ管理画面のバックアップ履歴画面で参照できます。

監査ログ管理画面から監査ログのバックアップファイルをダウンロードできるようにするには，バックアップファイルの格納先フォルダを作成し，そのフォルダにリンクさせる仮想ディレクトリを IIS マネージャで設定しておく必要があります。IIS マネージャでの設定については「5.5.1　Microsoft Internet Information Services をセットアップする」を参照してください。

監査ログをバックアップする手順を次に示します。

1. バックアップオプション定義ファイルを作成する（任意）。

   バックアップオプション定義ファイルは，監査ログのバックアップを実行したときに作成されるバックアップ実行履歴のバックアップの名称およびコメントを定義するファイルです。

   監査ログ管理画面のバックアップ履歴画面の「バックアップ名」および「コメント」を変更したい場合に作成します。バックアップオプション定義ファイルを使用しない場合，バックアップのファイル名が「バックアップ名」になります。また，「コメント」は空白となります。

   バックアップオプション定義ファイルについては「13.7　バックアップオプション定義ファイル」を参照してください。

2. admexport コマンドを実行する。

   監査ログのバックアップには次の二つの方法があります。

   - 期間指定による監査ログのバックアップ
   - 前回からコマンド実行日前日までの差分指定による監査ログのバックアップ

それぞれの監査ログのバックアップ方法について，次に説明します。

8.2.1　期間指定のバックアップ

指定した期間の監査ログをバックアップします。期間は admexport コマンドの引数で開始日時と終了日時を指定します。指定した期間の監査ログは指定したファイルに出力されます。

期間を指定した場合の admexport コマンドの実行例を，次に示します。

実行例

2007/4/1 の 00:00:00 から 2007/9/30 の 23:59:59 までの監査ログを，「C:¥www¥jp1netmaudit¥backupdata¥backup.csv」ファイルにバックアップする場合

```
admexport -s 2007-04-01 -e 2007-09-30 -o "C:¥www¥jp1netmaudit¥backupdata¥backup.csv"
```

admexport コマンドの詳細については「12. コマンド」の「admexport（監査ログのバックアップ）」を参照してください。

8.2.2 差分指定のバックアップ

差分バックアップはコマンド実行時に日時を設定する必要がないため，監査ログのバックアップを自動化できる利点があります。JP1/AJS2 と連携したり，Windows のタスクスケジューラを利用したりすることで，差分バックアップを自動化することができます。

前回のバックアップからコマンド実行の前日までの監査ログをバックアップします。指定した差分の監査ログは指定したフォルダ下に出力されます。なお，監査ログのバックアップファイル名はシステムで自動的に付与されます。

差分バックアップでは，差分として前回実行日時からコマンド実行の前日までの期間のデータベースの監査ログをバックアップするもので，前回実行日時からコマンド実行の前日までの期間のデータベースの差分をバックアップするものではありません。

また，admexport コマンドに引数を指定して，差分バックアップを初期化することもできます。再度，運用開始からの監査ログのバックアップを取得し直す場合などに指定します。差分バックアップを初期化すると，次回の差分バックアップでの出力ファイル名は初回のバックアップファイル名に戻ります。

差分バックアップを指定した場合の admexport コマンドの実行例を，次に示します。

実行例 1

2007/4/1 に運用を開始し，毎月 10 日，20 日，30 日に監査ログを，「C:¥www¥jp1netmaudit¥backupdata」フォルダ配下にバックアップする場合

```
admexport -d -b C:¥www¥jp1netmaudit¥backupdata
```

バックアップ取得期間（実行結果）

- 1 回目（2007/4/10）：2007/4/1 00:00:00 から 2007/4/9 23：59：59 までの監査ログをバックアップ（ファイル名：adm00001.csv）
- 2 回目（2007/4/20）：2007/4/10 00:00:00 から 2007/4/19 23：59：59 までの監査ログをバックアップ（ファイル名：adm00002.csv）
- 3 回目（2007/4/30）：2007/4/20 00:00:00 から 2007/4/29 23：59：59 までの監査ログをバックアップ（ファイル名：adm00003.csv）

実行例 2

2007/4/1 に運用を開始し，毎月 10 日，20 日，30 日に監査ログを，「C:¥www¥backup」フォルダ配下にバックアップしたあと，2007/5/6 に差分バックアップを初期化して，再度 2007/4/1 から 2007/5/5 までの監査ログを，「C:¥www¥jp1netmaudit¥backupdata」フォルダ配下にバックアップする場合

- 毎月 10 日，20 日，30 日に監査ログをバックアップします。

```
admexport -d -b "C:¥www¥jp1netmaudit¥backupdata"
```

バックアップ取得期間（実行結果）

- 1 回目（2007/4/10）：2007/4/1 00:00:00 から 2007/4/9 23：59：59 までの監査ログをバックアップ（ファイル名：adm00001.csv）
- 2 回目（2007/4/20）：2007/4/10 00:00:00 から 2007/4/19 23：59：59 までの監査ログをバックアップ（ファイル名：adm00002.csv）
- 3 回目（2007/4/30）：2007/4/20 00:00:00 から 2007/4/29 23：59：59 までの監査ログをバックアップ（ファイル名：adm00003.csv）

- 2007/5/6 に差分情報を初期化します。

```
admexport -d -r -y
```

差分情報を初期化すると，次回の差分バックアップでの出力ファイル名は初回のバックアップファイル名（adm00001.csv）に戻ります。差分情報を初期化したあと，出力先フォルダを変更しないで差分バックアップを実行する場合は，取得した監査ログのバックアップファイルを移動または削除するか，出力先フォルダ名を変更してください。

- 2007/5/6 に再度，差分バックアップを実行します。

```
admexport -d -b "C:¥www¥jp1netmaudit¥backupdata"
```

バックアップ取得期間（実行結果）

- （2007/5/6）：2007/4/1 00:00:00 から 2007/5/5 23：59：59 までの監査ログをバックアップ（ファイル名：adm00001.csv）

admexport コマンドの詳細については「12.　コマンド」の「admexport（監査ログのバックアップ）」を参照してください。

8.3　監査ログのバックアップファイルのインポート

監査ログ管理サーバから監査ログ閲覧サーバにダウンロードしたバックアップファイルを，監査ログ閲覧サーバの監査ログ管理データベースに入力（インポート）します。インポートした監査ログは監査ログ閲覧サーバで閲覧できます。バックアップファイルのダウンロード方法は「7.6.4　バックアップファイルをダウンロードする」を参照してください。

ダウンロードしたバックアップファイルを，次の操作で監査ログ閲覧サーバの監査ログ管理データベースにインポートします。

1. 監査ログ閲覧サーバで admimport コマンドを実行する。

   引数に監査ログ管理サーバからダウンロードしたバックアップファイルを指定します。ただし，指定したバックアップファイルのデータ内容が改ざんされている場合は，インポートできないことがあります。

admimport コマンドの実行例を，次に示します。

実行例

ダウンロードした「C:¥backupdata.csv」ファイルをインポートする場合

```
admimport -i "C:¥backupdata.csv"
```

admimport コマンドについては「12.　コマンド」の「admimport（監査ログのインポート）」を参照してください。

8.4　監査ログのバックアップファイルの移動

監査ログ管理サーバに格納されている監査ログのバックアップファイルを別のフォルダへ移動したり，ファイル名を変更したりできます。

監査ログのバックアップファイルの移動およびファイル名の変更と同時に，監査ログのバックアップを実行したときに作成されるバックアップ実行履歴の情報が更新されます。更新されたバックアップ実行履歴は，監査ログ管理画面のバックアップ履歴画面で参照できます。

移動後のバックアップファイルの格納先フォルダを作成し，そのフォルダにリンクさせる仮想ディレクトリを IIS マネージャで設定しておくことで，監査ログ管理画面から移動後のバックアップファイルをダウンロードできるようになります。IIS マネージャでの設定については「5.5.1　Microsoft Internet Information Services をセットアップする」を参照してください。

監査ログのバックアップファイルを移動する手順を次に示します。

1. バックアップオプション定義ファイルを作成する（任意）。

   バックアップオプション定義ファイルは，監査ログの移動を実行したときに更新されるバックアップ実行履歴のバックアップの名称およびコメントを定義するファイルです。

   監査ログ管理画面のバックアップ履歴画面の「バックアップ名」および「コメント」を変更したい場合に作成します。バックアップオプション定義ファイルを使用しない場合，「バックアップ名」および「コメント」は変更されません。

   バックアップオプション定義ファイルについては「13.7　バックアップオプション定義ファイル」を参照してください。

2. admcsvmove コマンドを実行する。

   引数に移動元のファイル名および移動先のファイル名を指定します。

   注意事項

   バックアップファイルの移動は，admcsvmove コマンドを使用してください。Windows のエクスプローラでファイル名の変更やフォルダを移動した場合，バックアップ実行履歴で管理されているファイル名と実際のファイル名が不一致となり，監査ログ管理画面のバックアップ履歴画面からバックアップファイルがダウンロードできなくなります。

admcsvmove コマンドの実行例を，次に示します。

実行例

監査ログのバックアップで取得したバックアップファイルを「C:¥www¥backup.csv」から「D:¥www¥backup.csv」に移動する場合

```
admcsvmove -s C:¥www¥backup.csv -d D:¥www¥backup.csv
```

admcsvmove コマンドについては「12.　コマンド」の「admcsvmove（監査ログのバックアップファイルの移動）」を参照してください。

8.5　監査ログのバックアップファイルの削除

監査ログ管理サーバ内に格納されている監査ログのバックアップファイルを削除できます。また，監査ログのバックアップファイルの削除と同時に，監査ログのバックアップを実行したときに作成されるバックアップ実行履歴も削除されます。

監査ログのバックアップファイルを削除する手順を次に示します。

1. admcsvremove コマンドを実行する。

   引数に削除するバックアップファイルのファイル名またはバックアップ ID を指定します。バックアップ ID は，バックアップファイルを特定するための ID で，監査ログ管理画面のバックアップ履歴画面で確認できます。

admcsvremove コマンドの実行例を，次に示します。

実行例 1

監査ログのバックアップファイル名「C:¥www¥backupdata¥backup.csv」を指定して削除する場合

```
admcsvremove -r C:¥www¥backupdata¥backup.csv
```

実行例 2

バックアップ履歴確認画面のバックアップ ID「3」を指定して削除する場合

```
admcsvremove -n 3
```

admcsvremove コマンドの詳細については「12.　コマンド」の「admcsvremove（監査ログのバックアップファイルの削除）」を参照してください。

9 監査ログ収集対象の確認と変更

この章では，システムの変更について説明します。システムの変更として，JP1/Audit Management - Manager の設定変更および監査ログを収集する対象の設定変更について説明します。

9.1　システムの変更の概要

運用しているシステムの設定を確認および変更する方法について説明します。

説明する内容を次に示します。

- 監査ログの収集対象の情報確認
- 監査ログの収集対象の設定変更

監査ログの収集対象の情報や設定は［監査ログ収集マネージャ］ウィンドウで確認したり，変更したりできます。

9.2　監査ログの収集対象の情報確認

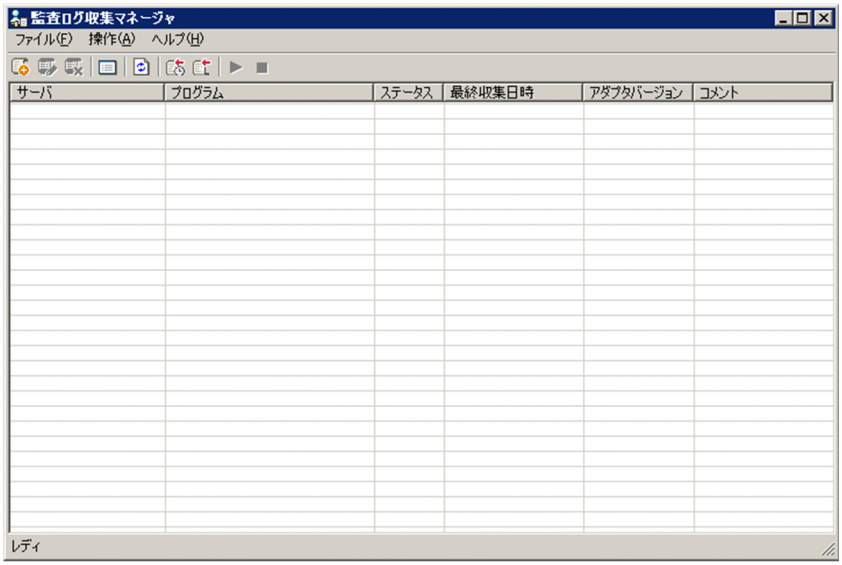
監査ログの収集対象についての情報を［監査ログ収集マネージャ］ウィンドウで確認できます。

［監査ログ収集マネージャ］ウィンドウの表示方法を次に示します。

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。

   次に示す［監査ログ収集マネージャ］ウィンドウが表示されます。

   図 9-1　［監査ログ収集マネージャ］ウィンドウ



［監査ログ収集マネージャ］ウィンドウのメニューを次の表に示します。

表 9-1　［監査ログ収集マネージャ］ウィンドウのメニュー

項番	項目名			説明	対応するボタン※
1	ファイル	終了		［監査ログ収集マネージャ］ウィンドウを終了します。	－
2	操作	収集対象	追加	［収集対象の設定］ダイアログが表示されます。収集対象を追加する方法の詳細については「9.3.1　監査ログ収集対象を追加する」を参照してください。	
3			編集	［収集対象の設定］ダイアログが表示されます。［監査ログ収集マネージャ］ウィンドウで選択した収集対象のサーバ名やプログラム名などの情報を編集できます。［収集対象の設定］ダイアログで編集できる内容については「9.3.2　監査ログ収集対象を編集する」を参照してください。	
4			削除	［監査ログ収集マネージャ］ウィンドウで選択した収集対象を解除するかどうかを確認するダイ	

項番	項目名			説明	対応するボタン※
				アログが表示されます。[OK] ボタンをクリックすると，[監査ログ収集マネージャ] ウィンドウで選択した収集対象を解除します。ただし，ネットワークの状況によって収集対象が解除されるまで時間が掛かる場合があります。 収集対象を解除する方法の詳細については「9.3.3　監査ログ収集対象を解除する」を参照してください。	
5		監査ログの監視	開始	[監査ログ収集マネージャ] ウィンドウで選択した収集対象の監視を開始するかどうかを確認するダイアログが表示されます。[OK] ボタンをクリックすると，監査ログの監視を開始します。ただし，ネットワークの状況によって監視が開始されるまで時間が掛かる場合があります。 監査ログの監視を開始する方法の詳細については「9.3.4　監査ログの監視を開始する」を参照してください。	
6			停止	[監査ログ収集マネージャ] ウィンドウで選択した収集対象の監視を停止するかどうかを確認するダイアログが表示されます。[OK] ボタンをクリックすると，監査ログの監視を停止します。ただし，ネットワークの状況によって監視が停止されるまで時間が掛かる場合があります。 監査ログの監視を停止する方法の詳細については「9.3.5　監査ログの監視を停止する」を参照してください。	
7		監査ログの収集	定時収集の設定	[定時収集の設定] ダイアログが表示されます。 監査ログを定時収集する方法の詳細については「5.6.5　監査ログを定期的に収集する」を参照してください。	
8			即時収集	収集対象として設定されているサーバから監査ログを即時に収集します。[監査ログ収集マネージャ] ウィンドウに登録されているすべての収集対象の監査ログを収集します。 監査ログを即時収集する方法の詳細については「9.3.7　監査ログを即時に収集する」を参照してください。	
9		製品定義一覧		[製品定義一覧] ダイアログが表示されます。 製品定義ファイルを設定する方法については「5.6.3　製品定義ファイルを設定する」を参照してください。	
10		最新の情報に更新		[監査ログ収集マネージャ] ウィンドウに表示されているすべての収集対象のステータス，最終収集日時，およびアダプタバージョンの表示内容を更新します。ただし，ネットワークの状況	

項番	項目名		説明	対応するボタン※
			によって表示内容が更新されるまでに時間が掛かる場合があります。	
11	ヘルプ		JP1/Audit Management - Manager のバージョン情報を表示します。	－

（凡例）

－：該当なし

注※

ここで示すツールバーのボタンをクリックすると，メニューと同様の操作ができます。

［監査ログ収集マネージャ］ウィンドウで確認できる項目を次の表に示します。

表 9-2 ［監査ログ収集マネージャ］ウィンドウで確認できる項目

項番	項目名	説明
1	サーバ	収集対象となるサーバ名を表示します。
2	プログラム	収集対象となるプログラム名を表示します。 なお，収集対象となるプログラムのログが Windows イベントログに出力される場合や OS が UNIX の場合は，次のように表示されます。 • Hitachi Storage Command Suite または Hitachi Command Suite の場合 「HitachiStorageCommandSuite（Windows イベントログ)」※ 「HitachiStorageCommandSuiteV8（Windows イベントログ)」※ 「HitachiStorageCommandSuite（HP-UX)」※ 「HitachiStorageCommandSuite（Solaris)」※ 「HitachiStorageCommandSuite（AIX)」※ 「HitachiStorageCommandSuite（Linux)」※ • Oracle の場合 「Oracle（Windows イベントログ)」 • UNIX の場合 「UNIX System Log」 • Windows Server 2003 または Windows XP の場合 「Windows イベントログ（セキュリティ)」 • Windows Server 2008 または Windows Server 2012 の場合 「Windows2008 イベントログ（セキュリティ)」
3	ステータス	［監査ログ収集マネージャ］ウィンドウ起動時の，ログファイルトラップ状況に関する情報について，次のどれかが表示されます。 •「更新中」 ステータスが更新中の場合に表示されます。 •「監視中」 監査ログが監視されている場合に表示されます。 •「停止」 監査ログの監視が停止している場合に表示されます。

項番	項目名	説明
		• 「不明」 収集対象を設定した直後の場合，または最新の情報に更新してエラーが発生した場合に表示されます。 なお，最新の情報に更新してエラーが発生した場合，同一サーバのプログラムのステータスがすべて「不明」と表示されます。 • 「対象外」 収集対象となるログが Windows イベントログに出力される場合に表示されます。 ステータスの情報は，最新の情報へ更新する場合または監査ログの監視を開始・停止する場合に更新されます。
4	最終収集日時	最終収集日時はサーバごとに取得されます。[監査ログ収集マネージャ] ウィンドウ起動時の，監査ログデータの最終収集日時情報について，次のどれかを表示します。 • 「更新中」 最終収集日時の更新中に表示されます。 • 最終収集日時を表示 最終収集日時を表示します。表示形式は「YYYY/MM/DD hh:mm:ss」です。 • 「−」 最終収集日時を取得していない場合に表示されます。 最終収集日時の情報は，「最新の情報に更新」メニューを実行したときだけ更新されます。
5	アダプタバージョン	[監査ログ収集マネージャ] ウィンドウ起動時の，監査ログ収集対象サーバのアダプタコマンドのバージョン情報について，次のどれかが表示されます。 • 「更新中」 アダプタコマンドのバージョンの更新中に表示されます。 • バージョン表示 アダプタコマンドのバージョンが表示されます。 • 「不明」 収集対象を設定した直後の場合，または最新の情報に更新してエラーが発生した場合に表示されます。 なお，最新の情報に更新してエラーが発生した場合，同一サーバのプログラムのアダプタバージョンがすべて「不明」と表示されます。 アダプタバージョンの情報は，最新の情報へ更新する場合または監視を開始・停止する場合に更新されます。
6	コメント	[収集対象の設定] ダイアログで入力したコメントが表示されます。

注※

OS ごとに次のプログラム名が表示されます。

・Windows かつ Hitachi Command Suite 7 以前の場合：「HitachiStorageCommandSuite（Windows イベントログ)」
・Windows かつ Hitachi Command Suite 8 の場合：「HitachiStorageCommandSuiteV8（Windows イベントログ)」
・HP-UX の場合：「HitachiStorageCommandSuite（HP-UX)」
・Solaris の場合：「HitachiStorageCommandSuite（Solaris)」
・AIX の場合：「HitachiStorageCommandSuite（AIX)」
・Linux の場合：「HitachiStorageCommandSuite（Linux)」

9.3　監査ログの収集対象の設定変更

収集対象を追加，編集，または解除したり，監査ログを収集する時刻や曜日を設定し直したりするなど，監査ログの収集対象の設定を変更します。

監査ログの収集対象の設定は，［監査ログ収集マネージャ］ウィンドウで変更できます。

次のような場合に，収集対象の設定を変更します。

監査ログの収集対象を追加したい場合

収集対象を追加する方法については「9.3.1　監査ログ収集対象を追加する」を参照してください。

監査ログの収集対象を編集したい場合

収集対象を編集する方法については「9.3.2　監査ログ収集対象を編集する」を参照してください。

監査ログの収集対象を解除したい場合

収集対象を解除する方法については「9.3.3　監査ログ収集対象を解除する」を参照してください。

収集対象プログラムの監視を開始したい場合

監査ログの監視を開始する方法については「9.3.4　監査ログの監視を開始する」を参照してください。

収集対象プログラムの監視を停止したい場合

監査ログの監視を停止する方法については「9.3.5　監査ログの監視を停止する」を参照してください。

監査ログを収集する時刻や曜日を変更したい場合

定期的に収集している監査ログの収集する時刻や曜日を変更したい場合は「9.3.6　監査ログを定期的に収集する時刻や曜日を変更する」を参照してください。

監査ログを即時収集したい場合

監査ログを即時に収集したい場合は「9.3.7　監査ログを即時に収集する」を参照してください。

製品定義ファイルを作成して収集対象を追加したい場合

標準サポート外のプログラムの製品定義ファイルを作成し，収集対象として追加する方法については「9.3.8　製品定義ファイルを作成して収集対象を追加する」を参照してください。

製品定義ファイルを編集したい場合

標準サポート外のプログラムの製品定義ファイルを編集する方法については「9.3.9　作成した製品定義ファイルを編集する」を参照してください。JP1/Audit Management - Manager が標準サポートしているプログラムの製品定義ファイルは編集できません。

製品定義ファイルを削除したい場合

標準サポート外のプログラムの製品定義ファイルを削除する方法については「9.3.10　作成した製品定義ファイルを削除する」を参照してください。JP1/Audit Management - Manager が標準サポートしているプログラムの製品定義ファイルは削除できません。

9.3.1　監査ログ収集対象を追加する

この項では，監査ログを収集する対象を追加するときの事前準備と，追加する手順を説明します。

なお，ログファイルがラップアラウンド形式の場合は，収集対象のログファイル面数に合わせて設定を変更してください。

(1)　監査ログ収集対象を追加するときの事前準備

サーバに新たに追加したプログラムを監査ログの収集対象として追加したい場合，収集対象を追加するための準備が必要です。状況に応じて次の設定をしてください。

すでに収集対象として設定されているサーバにプログラムを追加して収集対象とする場合

OS の設定や各プログラムの設定など，追加するプログラムのセットアップが必要です。監査ログの収集対象プログラムのセットアップについては「5.4.6　監査ログ収集対象プログラムをセットアップする」を参照してください。

新たに構築するサーバのプログラムを収集対象とする場合

監査ログ収集対象サーバとして，サーバを構築する必要があります。監査ログ収集対象サーバの構築には，次に示す順序で作業が必要です。

1. JP1/Base および監査ログの収集対象プログラムのインストール
   「5.3　監査ログ収集対象サーバのプログラムのインストール」を参照してください。
2. セットアップに必要なファイルのインストール
   「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。
3. JP1/Base のイベントサービスの設定
   「5.4.2　JP1/Base のイベントサービスを設定する」を参照してください。
4. イベントログトラップ機能の設定
   「5.4.3　JP1/Base のイベントログトラップ機能を設定する」を参照してください。
5. ログファイルトラップ機能の設定の確認
   「5.4.4　ログファイルトラップ機能の設定を確認する」を参照してください。
6. UNIX システムログの変換設定
   「5.4.5　UNIX システムログの変換設定をする」を参照してください。
7. 監査ログ収集対象プログラムのセットアップ
   「5.4.6　監査ログ収集対象プログラムをセットアップする」を参照してください。

(2)　監査ログ収集対象を追加する手順

監査ログ収集対象の追加は，監査ログ収集対象を初めて設定する場合と同様の方法で実施できます。監査ログ収集対象の追加方法の詳細については「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。なお，監査ログ収集対象を追加した場合は，JP1/Audit

Management - Manager のサービスを再起動してください。再起動するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

9.3.2　監査ログ収集対象を編集する

この項では，監査ログの収集対象について編集する手順を説明します。

編集できるのは次の項目です。

- 収集する監査ログが格納されているフォルダ
- OS 起動時に監査ログの監視を開始するかどうかの設定
- コメントの内容

監査ログの収集対象について編集する手順を次に示します。監視中の収集対象の場合は，コメントの内容だけ編集できます。収集した監査ログファイルを格納するフォルダを編集したり，OS 起動時に監査ログの監視を開始するかどうかを設定したりする場合には，監査ログの監視を停止してから編集または設定してください。なお，編集または設定した内容を反映して監査ログを収集したい場合は，JP1/Audit Management - Manager のサービスを再起動してください。再起動するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

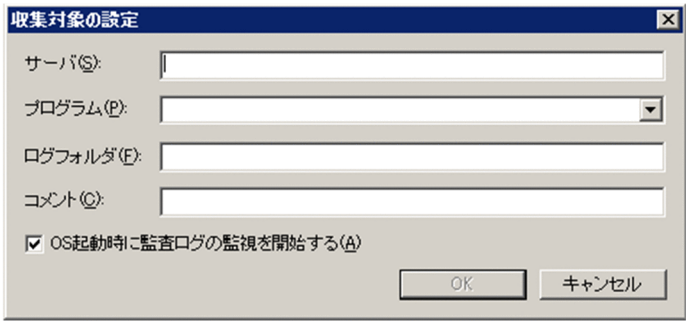
1. **［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。**
   ［監査ログ収集マネージャ］ウィンドウが表示されます。

2. **［監査ログ収集マネージャ］ウィンドウに表示された項目から，設定を編集したい監査ログの収集対象を選択する。**

3. **監査ログの監視が停止していない場合は，［操作］－［監査ログの監視］－［停止］を選択する。**
   選択した監査ログの監視を停止するかどうかを確認するメッセージが表示されます。
   監査ログの監視を停止する方法の詳細については「9.3.5　監査ログの監視を停止する」を参照してください。

4. **［操作］－［収集対象］－［編集］を選択する。**
   次に示す［収集対象の設定］ダイアログが表示されます。

図 9-2 ［収集対象の設定］ダイアログ



なお，「 」ボタンをクリックしても，このダイアログを表示できます。

5. 監査ログの収集対象の設定項目を編集する。

   編集できるのは，「ログフォルダ」，「コメント」，および「OS 起動時に監査ログの監視を開始する」チェックボックスです。これらの設定項目の詳細については「5.6.4(2) ［収集対象の設定］ダイアログの設定内容」を参照してください。

6. ［OK］ボタンをクリックする。

   監査ログの収集対象の設定が更新されたら，［収集対象の設定］ダイアログが閉じて［監査ログ収集マネージャ］ウィンドウに戻ります。

7. ［監査ログ収集マネージャ］ウィンドウに表示された項目から，監視を開始したい収集対象を選択し，［操作］－［監査ログの監視］－［開始］を選択する。

   選択した監査ログ収集対象サーバに対応するログファイルトラップ機能が起動され，監査ログの監視を開始します。複数の収集対象を一度に選択して，監視を開始することもできます。

9.3.3 監査ログ収集対象を解除する

この項では，監査ログを収集する対象を解除する方法について説明します。

監査ログの監視が停止していない場合は，一度，監視を停止してから解除します。解除する手順の詳細については「5.13 監査ログ収集対象の解除」または「6.10 監査ログ収集対象の解除（クラスタ環境）」を参照してください。

9.3.4 監査ログの監視を開始する

この項では，監査ログの監視を開始する方法について説明します。

［監査ログ収集マネージャ］ウィンドウで監査ログの監視を開始するための設定をします。

なお，ここでは，すでに監査ログ収集対象として設定されている収集対象の監視を開始する方法について説明しています。

収集対象の追加については「9.3.1　監査ログ収集対象を追加する」を参照してください。

(1)　監査ログの監視の開始

監査ログの監視を開始する手順を次に示します。

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。
   ［監査ログ収集マネージャ］ウィンドウが表示されます。
2. ［監査ログ収集マネージャ］ウィンドウで，監視を開始したい収集対象を選択する。
3. ［操作］－［監査ログの監視］－［開始］を選択する。
   監査ログの監視を開始するかどうかを確認するダイアログが表示されます。［OK］ボタンをクリックすると，監査ログの監視が開始されます。監視の開始後に出力された監査ログが収集対象となります。なお，「 ▶ 」ボタンをクリックしても同様の操作ができます。
   選択した収集対象プログラムのサーバ内にある JP1/Base で，収集対象プログラムに対して，ログファイルトラップ機能を起動します。

(2)　監査ログの監視の自動開始

監査ログ収集対象のサーバの OS が Windows の場合は，監査ログ収集対象サーバの起動時，自動的に監査ログの監視を開始する設定にできます。監視の自動開始を設定すると，監査ログ収集対象サーバを起動するたびに［監査ログ収集マネージャ］ウィンドウで［操作］－［監査ログの監視］－［開始］を選択する手間が省けます。

監視の自動開始は，［収集対象の設定］ダイアログで収集対象を追加するときに「OS 起動時に監査ログの監視を開始する」チェックボックスをチェックして設定します。監査ログ収集対象の追加については「9.3.1　監査ログ収集対象を追加する」を参照してください。

9.3.5　監査ログの監視を停止する

この項では，監査ログの収集を停止する方法について説明します。

監査ログの収集は，［監査ログ収集マネージャ］ウィンドウで停止できます。

なお，この項ではすでに監査ログの収集対象として設定されている収集対象の監視の停止について説明しています。

監査ログの監視を停止する手順を次に示します。

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。
   ［監査ログ収集マネージャ］ウィンドウが表示されます。

2. [監査ログ収集マネージャ] ウィンドウで，監視を停止したい収集対象を選択する。

3. [操作] − [監査ログの監視] − [停止] を選択する。
   監査ログの監視を停止するかどうかを確認するダイアログが表示されます。[OK] ボタンをクリックすると，監視ログの監視が停止します。なお，「 ■ 」ボタンをクリックしても同様の操作ができます。選択した収集対象プログラムのサーバ内にある JP1/Base で，収集対象プログラムのログファイルトラップ機能を停止します。

9.3.6　監査ログを定期的に収集する時刻や曜日を変更する

設定した収集対象の監査ログを収集する時刻や曜日を変更します。

監査ログを収集する時刻や曜日を変更する方法は，最初に監査ログを収集する時刻や曜日を設定した場合と同様です。収集する時刻や曜日を変更する方法については「5.6.5　監査ログを定期的に収集する」を参照してください。

収集する時刻や曜日の変更は [定時収集の設定] ダイアログで実施します。[定時収集の設定] ダイアログで設定を変更した場合は，JP1/Audit Management - Manager のサービスを再起動してください。再起動するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

なお，[マネージャセットアップ] ダイアログで統計情報を自動生成する設定にしている場合，[定時収集の設定] ダイアログで設定した日時に，監査ログ管理データベース内に統計情報が生成されます。したがって，[定時収集の設定] ダイアログで設定変更した時間帯に連動して，統計情報が自動生成される時間帯も変更されます。

9.3.7　監査ログを即時に収集する

この項では，監査ログを即時に収集する方法について説明します。

この方法は，定期的に監査ログを収集するほかに，即時に監査ログを収集したい場合に実施してください。監査ログを即時に収集するには，監査ログ収集マネージャを使用して収集する方法と admcoldata コマンドを実行して収集する方法があります。なお，JP1/Audit Management - Manager のサービスが停止しているときは，監査ログを即時に収集できません。

(1)　監査ログ収集マネージャを使用して収集する場合

監査ログを即時に収集する手順を次に示します。

1. [スタート] ボタンをクリックして [プログラム] − [JP1_NETM_Audit] − [監査ログ収集マネージャ] を選択する。
   [監査ログ収集マネージャ] ウィンドウが表示されます。

2. [操作] − [監査ログの収集] − [即時収集] を選択する。

設定されたすべての収集対象に対して，監査ログの即時収集を開始します。

収集対象の設定については「5.6.4　JP1/Audit Management - Manager で監査ログの収集対象を設定する」を参照してください。

なお，「 」ボタンをクリックしても同様の操作ができます。

(2)　コマンドを実行して収集する場合

admcoldata コマンドを実行して，監査ログを即時に収集します。コマンドの詳細については，「12.　コマンド」の「admcoldata（監査ログの収集）」を参照してください。

9.3.8　製品定義ファイルを作成して収集対象を追加する

JP1/Audit Management - Manager で標準サポート外となっているプログラムを収集対象として指定するには，製品定義ファイルを作成し，収集対象として追加する必要があります。

製品定義ファイルを作成する方法については「5.6.3　製品定義ファイルを設定する」を参照してください。

9.3.9　作成した製品定義ファイルを編集する

すでに作成している製品定義ファイルを編集します。ただし，JP1/Audit Management - Manager で標準サポートしている製品定義ファイルは編集できません。

製品定義ファイルを新しく作成する方法については「5.6.3　製品定義ファイルを設定する」を参照してください。

製品定義ファイルを編集する手順を次に示します。

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。

   ［監査ログ収集マネージャ］ウィンドウが表示されます。

2. ［操作］－［製品定義一覧］を選択する。

   ［製品定義一覧］ダイアログが表示されます。

3. 編集したいプログラムを選択した状態で［編集］ボタンをクリックする。

   ［製品定義の編集］ダイアログが表示されます。

4. ［製品定義の編集］ダイアログで，使用する環境に合わせて項目を編集する。

   設定内容については「5.6.3(2)　［製品定義の編集］ダイアログの設定内容」を参照してください。

5. ［OK］ボタンをクリックする。

   入力した内容が［製品定義一覧］ダイアログに反映されます。

9.3.10　作成した製品定義ファイルを削除する

すでに作成している製品定義ファイルを削除します。ただし，JP1/Audit Management - Manager で標準サポートしている製品定義ファイルは削除できません。

製品定義ファイルを削除する手順を次に示します。

1. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［監査ログ収集マネージャ］を選択する。

   ［監査ログ収集マネージャ］ウィンドウが表示されます。

2. ［操作］－［製品定義一覧］を選択する。

   ［製品定義一覧］ダイアログが表示されます。

3. 削除したいプログラムを選択した状態で［削除］ボタンをクリックする。

   削除するかどうかを確認するダイアログが表示され，［OK］ボタンをクリックすると，選択したプログラムが削除されます。

10 データベースのメンテナンス

この章では，監査ログの管理に使用するデータベースをメンテナンスする方法について説明します。

10.1　データベースのメンテナンスの概要

データベースは運用や状況に合わせて，適宜メンテナンスする必要があります。

データベースのメンテナンスは，データベースマネージャまたはコマンドを使用して実行します。

実行できるデータベースのメンテナンス内容と説明を次の表に示します。なお，表の右 2 列は，各メンテナンスの手段を示しています。

表 10–1　データベースのメンテナンスの概要

項番	メンテナンス内容	説明	データベースマネージャ	コマンド
1	データベースの再セットアップ	データベースを再セットアップします。	○	−
2	データベースのバックアップ	データベースのバックアップを取得します。	○	○
3	データベースのリストア	取得したバックアップファイルからデータベースを復元します。	○	−
4	データベースの再編成	データベースを再編成します。	○	○
5	データベースのパスワード変更	データベースに接続するときに使用するパスワードを変更します。	○	−
6	データベースの CSV バックアップ	データベースに格納されているデータを，CSV 形式ファイルでバックアップします。	○	○
7	データベースの CSV リストア	取得した CSV バックアップファイルからデータベースを復元します。	○	−
8	データベースのデータ移行	あるサーバから別のサーバにデータベースのデータを移行します。	○	−
9	データベースのデータ削除	データベースに格納された監査ログのデータを削除します。	−	○

(凡例)

○：実行できる

−：実行できない

10.1.1　データベースマネージャの起動方法

データベースマネージャを起動する手順を次に示します。

1. JP1/Audit Management - Manager のサービスを停止する。

   JP1/Audit Management - Manager の次のサービスを停止してください。

   - JP1/NETM/Audit - Manager Define

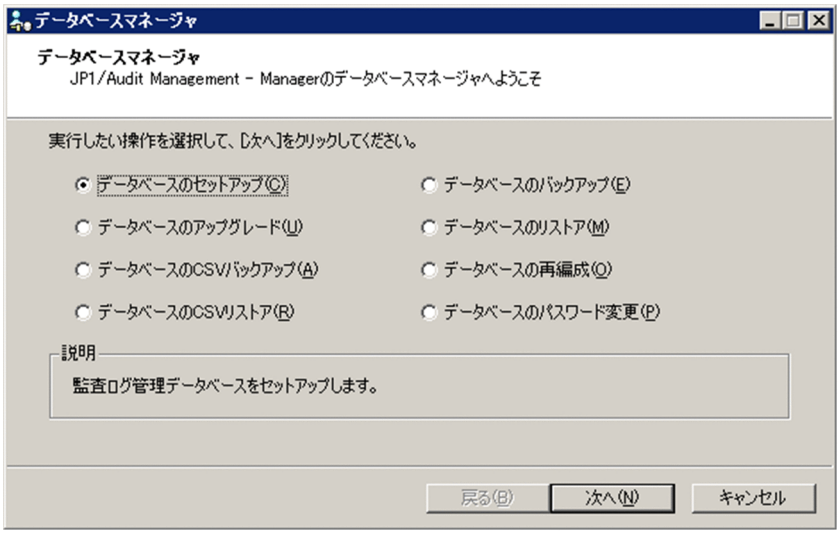
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager

なお，JP1/Audit Management - Manager のサービスのほかに，World Wide Web Publishing Service サービスも停止する必要があります。

2. ［スタート］ボタンをクリックして［プログラム］－［JP1_NETM_Audit］－［データベースマネージャ］を選択する。

次の図に示す［データベースマネージャ］ダイアログが表示されます。

図 10-1　［データベースマネージャ］ダイアログ



3. 実行したい操作を選択し，［次へ］ボタンをクリックする。

選択した作業が完了すると，確認画面が表示されます。［OK］ボタンをクリックすると，［データベースマネージャ］ダイアログが閉じます。

10.1.2　データベースの再セットアップ

データベースの再セットアップについて説明します。

データベースの再セットアップ方法は，データベースのセットアップ方法と同様です。データベースのセットアップの詳細については「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照してください。

データベースの再セットアップは，セットアップ中やセットアップ後に必要になることがあります。再セットアップが必要な場合と，その場合に実施する内容について次に示します。

データベースのセットアップ中に再セットアップが必要になる場合

セットアップ中にエラーが発生した場合，再セットアップが必要になることがあります。エラーメッセージに従って対処し，必要に応じてデータベースの再セットアップを実施してください。

データベースのセットアップ後に再セットアップが必要になる場合

セットアップ後にデータベースのサイズを変更したい場合，再セットアップする必要があります。データベースのサイズの変更方法については「10.2　データベースのディスク容量の管理」を参照してください。

なお，データベースのセットアップが正常に完了している場合に再セットアップを実行しようとすると確認ダイアログが表示されます。[OK] ボタンをクリックするとデータベースの再セットアップが実行されます。

注意事項

データベースを再セットアップすると，監査ログのデータやバックアップ実行履歴や正規化ルールエディタの定義情報など，データベースに格納されているすべてのデータが消去されます。データベースを再セットアップする場合は，必ず CSV バックアップを取得してください。

クラスタ構成の場合，実行系と待機系を入れ替えて再セットアップしないでください。

10.1.3　データベースのバックアップ

データベースでトラブルが発生し，環境を再構築する場合などに備えて，定期的にデータベースのバックアップを取得することをお勧めします。

データベースのバックアップは，次のどちらかの方法で実施します。

- データベースマネージャを使用する方法
- コマンドを使用する方法

ここでは，データベースマネージャからデータベースのバックアップを実行する方法を説明します。コマンドから実行する方法については「12.　コマンド」の「admdbbackup（データベースのバックアップ）」を参照してください。

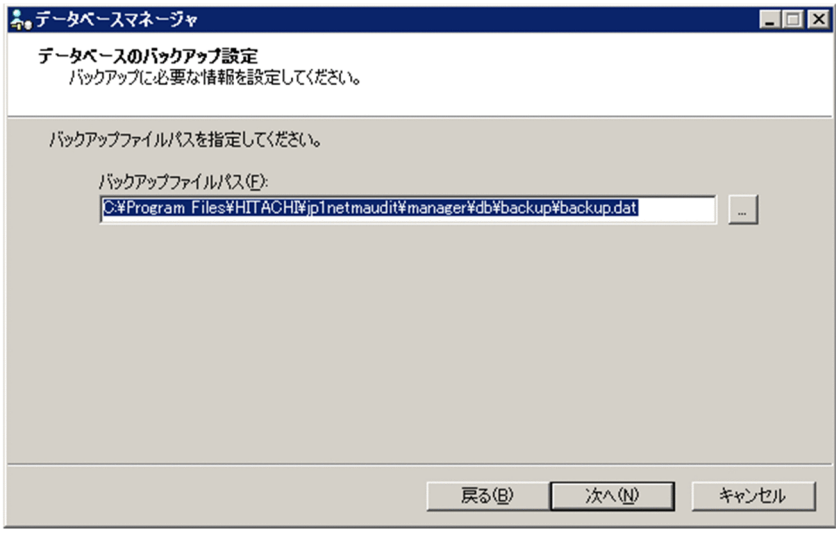
注意事項

データベースのバックアップ実行前に，バックアップ先に十分な空き容量があることを確認してください。

1. [データベースマネージャ] ダイアログで「データベースのバックアップ」を選択して，[次へ] ボタンをクリックする。

   次の図に示す［データベースのバックアップ設定］画面が表示されます。

図 10-2 ［データベースのバックアップ設定］画面



2. バックアップファイル名を指定する。

「バックアップファイルパス」に，取得するバックアップファイルのパスを指定します。[...] ボタンをクリックすると，ファイルを参照するダイアログからファイル名を指定できます。

バックアップファイルのパスを指定するとき，次のことに注意してください。

- バックアップファイルのパスは，255 バイト以内の文字列で指定してください。
- バックアップファイルの格納先としては，ローカルディスク上のフォルダを指定してください。ネットワークドライブ上のフォルダにはバックアップファイルを格納できません。
- 指定したバックアップファイル名がすでにある場合，既存のファイルは上書きされます。

デフォルトのバックアップファイルのパスを次に示します。

```
JP1/Audit Management - Managerのインストール先フォルダ¥db¥backup¥backup.dat
```

3. ［次へ］ボタンをクリックする。

［データベースのバックアップ実行］画面が表示されます。

4. ［実行］ボタンをクリックする。

データベースのバックアップが取得されます。バックアップが完了すると，バックアップが完了したことを示すメッセージが表示されます。

なお，バックアップファイルの取得に掛かる時間は，データベースの容量と取得するバックアップファイルのデータ量に比例します。

5. ［OK］ボタンをクリックする。

［データベースマネージャ］ダイアログが閉じます。

必要に応じて，コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Audit Management - Manager のサービスを開始します。開始するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

10.1.4　データベースのリストア

データベースのバックアップで取得したバックアップファイルから，データベースを復元します。

なお，データベースのリストアを実施するサーバは，バックアップを取得するサーバと次の条件が一致している必要があります。

- インストールされている OS
- ホスト名
- IP アドレス
- JP1/Audit Management - Manager のバージョン
- データベースにアクセスするためのユーザ ID とパスワード
- JP1/Audit Management - Manager のインストール先フォルダ
- データベース領域の格納先
- データベースの容量
- データベースのセットアップが完了していること

データベースのリストアは，データベースマネージャから実行します。データベースのリストアを実行する手順を次に示します。

注意事項

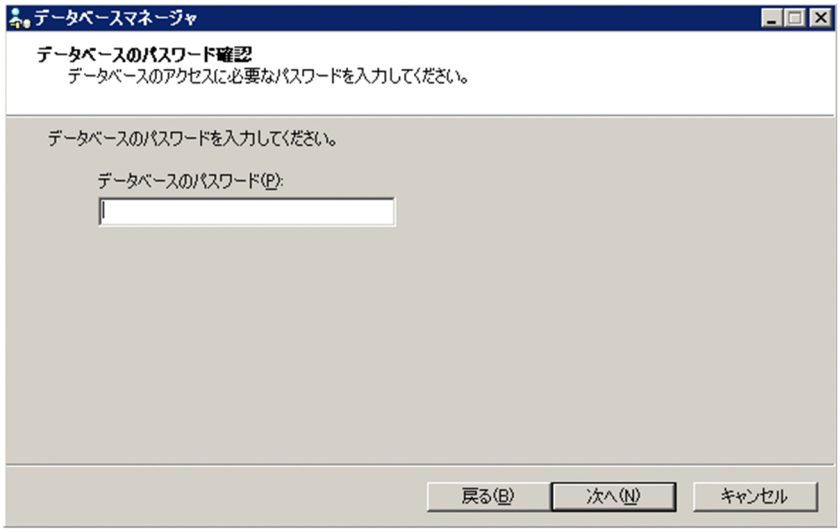
データベースのリストアを実行するときは，次のことに注意してください。

- データベースのリストアは，リストアを実施するサーバがデータベースのセットアップを完了している状態で実施してください。
- データベースをリストアすると，データベースはバックアップを取得した時点の状態に戻ります。データベースのバックアップファイルを取得してからリストアを実行するまでに更新されたデータは，すべて削除されます。

1. **［データベースマネージャ］ダイアログで「データベースのリストア」を選択して，［次へ］ボタンをクリックする。**

   次の図に示す［データベースのパスワード確認］画面が表示されます。

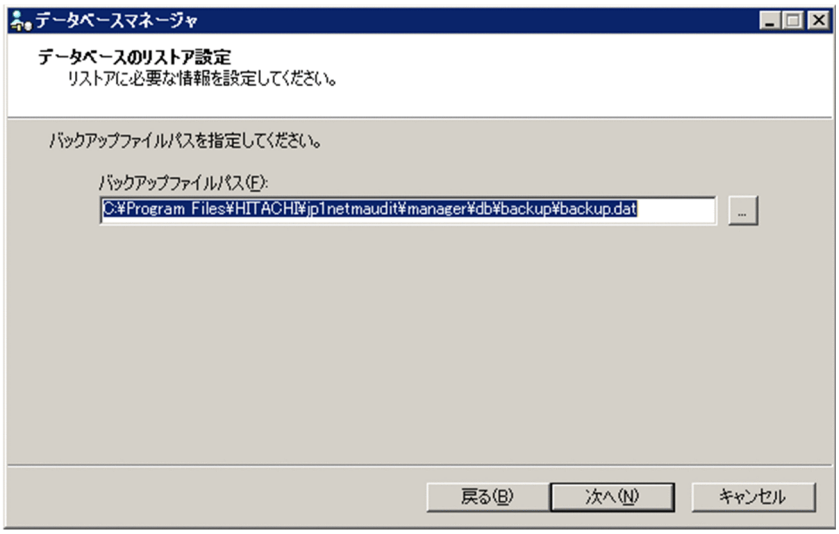
図 10-3 ［データベースのパスワード確認］画面



2. データベースのパスワードを入力して，［次へ］ボタンをクリックする。

次の図に示す［データベースのリストア設定］画面が表示されます。

図 10-4 ［データベースのリストア設定］画面



3. バックアップファイル名を指定する。

「バックアップファイルパス」に，データベースのバックアップで取得したバックアップファイルのパスを入力します。[...] ボタンをクリックすると，ファイルを参照するダイアログからファイル名を指定できます。

デフォルトのバックアップファイルのパスを次に示します。

```
JP1/Audit Management - Managerのインストール先フォルダ¥db¥backup¥backup.dat
```

4. ［次へ］ボタンをクリックする。

［データベースのリストア実行］画面が表示されます。

5. ［実行］ボタンをクリックする。

データベースのリストアが実行されます。リストアが完了すると，リストアが完了したことを示すメッセージが表示されます。

なお，リストアの実行時間は，データベースの容量とリストアするバックアップファイルのデータ量に比例します。

6. [OK] ボタンをクリックする。

［データベースマネージャ］ダイアログが閉じます。

必要に応じて，コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Audit Management - Manager のサービスを開始します。開始するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

10.1.5　データベースの再編成

データベースを運用し続けると，データの格納効率が悪くなり，検索機能が低下したりデータベースの容量不足になったりすることがあります。これを防ぐため，1 か月に 1 回を目安にデータベースを再編成します。

データベースの再編成は，次のどちらかの方法で実施します。

- データベースマネージャを使用する方法
- コマンドを使用する方法

ここでは，データベースマネージャからデータベースを再編成する方法を説明します。コマンドから再編成する方法については「12.　コマンド」の「admdbrorg（データベースの再編成）」を参照してください。

なお，データベースの再編成を実行してもデータベースの容量不足が解消されない場合は，データベースのデータを削除する必要があります。データベースのデータを削除する方法については「10.1.10　データベースのデータ削除」を参照してください。

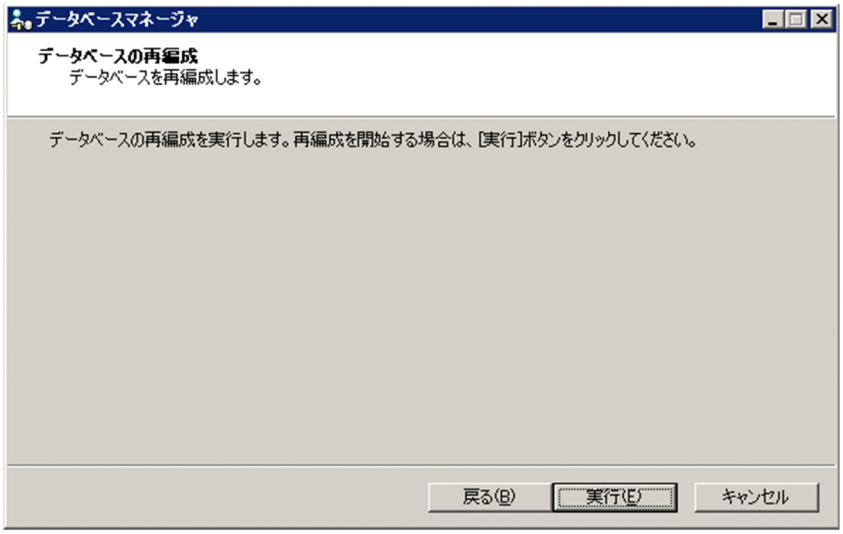
注意事項

再編成の実行中にトラブルが発生した場合などに備えて，再編成の実行前にデータベースのバックアップを取得することをお勧めします。データベースのバックアップについては「10.1.3　データベースのバックアップ」を参照してください。

1. ［データベースマネージャ］ダイアログで「データベースの再編成」を選択して，［次へ］ボタンをクリックする。

次の図に示す［データベースの再編成］画面が表示されます。

図 10-5 ［データベースの再編成］画面



2. ［実行］ボタンをクリックする。

   データベースが再編成されます。再編成が完了すると，再編成が完了したことを示すメッセージが表示されます。

   なお，再編成に掛かる時間は，データベースの容量とデータ量に比例します。

3. ［OK］ボタンをクリックする。

   ［データベースマネージャ］ダイアログが閉じます。

   必要に応じて，コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Audit Management - Manager のサービスを開始します。開始するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

10.1.6　データベースのパスワード変更

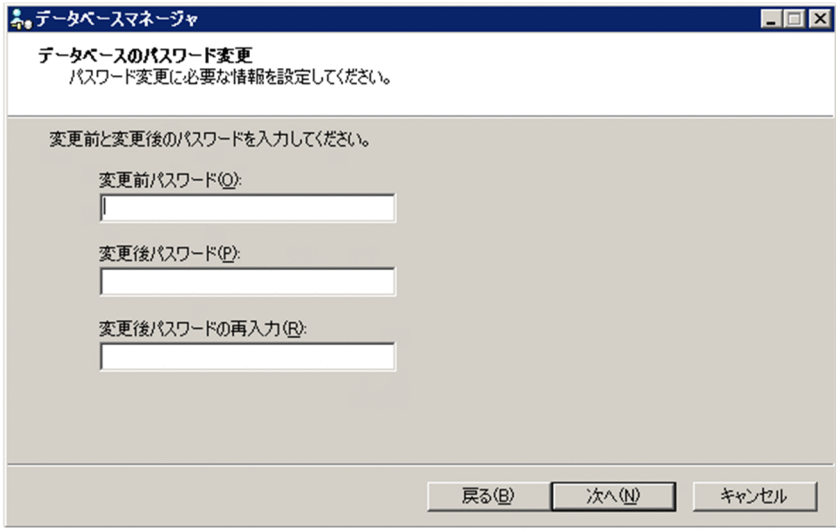
データベースとの接続に使用するパスワードを変更できます。データベースのパスワードは，運用に合わせて適宜変更してください。

データベースのパスワードは，データベースマネージャから変更します。データベースのパスワードを変更する手順を次に示します。

1. ［データベースマネージャ］ダイアログで「データベースのパスワード変更」を選択して，［次へ］ボタンをクリックする。

   次の図に示す［データベースのパスワード変更］画面が表示されます。

図 10-6 ［データベースのパスワード変更］画面



2. 変更前および変更後のパスワードを入力する。

「変更前パスワード」，「変更後パスワード」，および「変更後パスワードの再入力」にそれぞれ入力します。

データベースのパスワードとして設定できる値については「5.5.6(2) ［マネージャセットアップ］ダイアログの設定内容」を参照してください。

3. ［次へ］ボタンをクリックする。

［データベースのパスワード変更の実行］画面が表示されます。

4. ［実行］ボタンをクリックする。

データベースのパスワードが変更されます。パスワード変更が完了すると，パスワード変更が完了したことを示すメッセージが表示されます。

5. ［OK］ボタンをクリックする。

［データベースマネージャ］ダイアログが閉じます。

6. ［マネージャセットアップ］ダイアログを起動し，［データベース情報］の［ログイン ID］に設定してあるパスワードを，新しいパスワードに変更する。

［データベースマネージャ］ダイアログでパスワードを変更した場合，必ず［マネージャセットアップ］ダイアログでもパスワードを変更してください。［マネージャセットアップ］ダイアログで設定するパスワードは，必ず［データベースマネージャ］で変更したパスワードと同じパスワードを設定してください。

［マネージャセットアップ］ダイアログの使用方法については「5.5.6(2) ［マネージャセットアップ］ダイアログの設定内容」を参照してください。

必要に応じて，コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Audit Management - Manager のサービスを開始します。開始するサービスの詳細は「5.7.1 監査ログ管理サーバを開始する」を参照してください。

10.1.7　データベースの CSV バックアップ

データベースに格納されているデータを CSV 形式ファイルでバックアップします。データベースのサイズ変更およびデータベースのデータ移行で使用します。

データベースの CSV バックアップは，次のどちらかの方法で実施します。

- データベースマネージャを使用する方法
- コマンドを使用する方法

ここでは，データベースマネージャからデータベースの CSV バックアップを取得する方法を説明します。コマンドから CSV バックアップを取得する方法については「12.　コマンド」の「admdbexport（データベースの CSV バックアップ）」を参照してください。

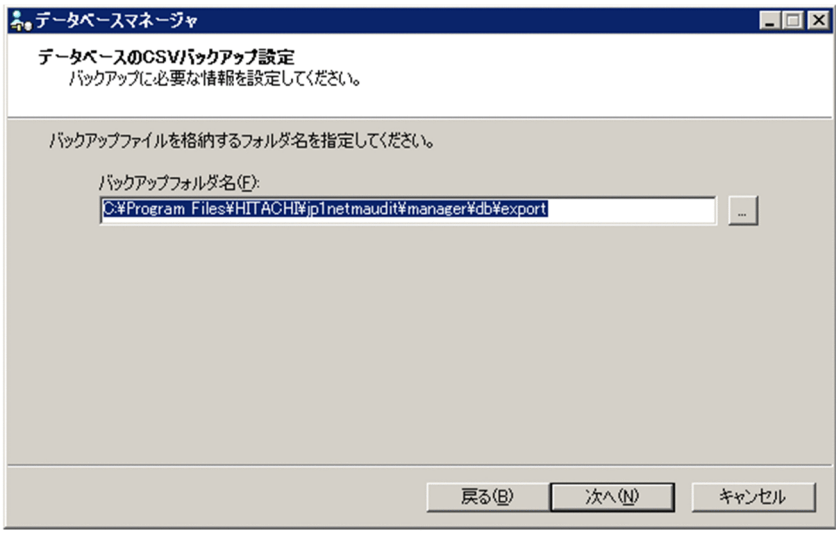
注意事項

データベースの CSV バックアップを実行する前に，バックアップ先に十分な空き容量があることを確認してください。

1. **［データベースマネージャ］ダイアログで，［データベースの CSV バックアップ］を選択して，［次へ］ボタンをクリックする。**

   次の図に示す［データベースの CSV バックアップ設定］画面が表示されます。

   図 10–7　［データベースの CSV バックアップ設定］画面



2. **CSV バックアップフォルダ名を指定する。**

   「バックアップフォルダ名」に，CSV バックアップファイルを格納するフォルダを指定します。［...］ボタンをクリックすると，フォルダを参照するダイアログからフォルダを指定できます。

   CSV バックアップフォルダのパスを指定するとき，次のことに注意してください。

   - CSV バックアップフォルダのパスは，200 バイト以内の文字列で指定してください。
   - CSV バックアップファイルの格納先として，ローカルディスク上のフォルダを指定してください。ネットワークドライブ上のフォルダには CSV バックアップファイルを格納できません。

- CSV バックアップファイルの格納先として，NTFS 上のフォルダを指定してください。FAT または FAT32 上のフォルダを指定した場合，利用する環境によっては，ファイルシステムの制限によってバックアップに失敗するおそれがあります。
- CSV バックアップファイルの名称は固定です。すでに CSV バックアップファイルが存在する場合，ファイルは上書きされます。

デフォルトの CSV バックアップフォルダのパスを次に示します。

```
JP1/Audit Management - Managerのインストール先フォルダ¥db¥export
```

3. [次へ] ボタンをクリックする。

   [データベースの CSV バックアップ実行] 画面が表示されます。

4. [実行] ボタンをクリックする。

   データベースの CSV バックアップが取得されます。CSV バックアップが完了すると，CSV バックアップが完了したことを示すメッセージが表示されます。

   なお，CSV バックアップの取得に掛かる時間は，データベースの容量と取得する CSV バックアップファイルのデータ量に比例します。

5. [OK] ボタンをクリックする。

   [データベースマネージャ] ダイアログが終了します。

   必要に応じて，コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Audit Management - Manager のサービスを開始します。開始するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

注意事項

取得した CSV バックアップファイルのファイル名および内容は変更しないでください。データベースの CSV リストアができなくなります。データベースの CSV リストアについては「10.1.8　データベースの CSV リストア」を参照してください。

10.1.8　データベースの CSV リストア

データベースの CSV バックアップで取得した CSV バックアップファイルから，データベースを復元（CSV リストア）します。

CSV リストアの対象となるサーバは，次の条件を満たしている必要があります。

- バックアップを取得したサーバと JP1/Audit Management - Manager のバージョンが同じ
- データベースのセットアップが完了している

注意事項

CSV バックアップのデータ内容が改ざんされている場合は，リストアできないことがあります。

データベースの CSV リストアは，次のどちらかの方法で実施します。

- データベースマネージャを使用する方法
- コマンドを使用する方法

ここでは，データベースマネージャからデータベースの CSV リストアを実行する方法を説明します。コマンドから CSV リストアする方法については「12.　コマンド」の「admdbimport（データベースの CSV リストア）」を参照してください。

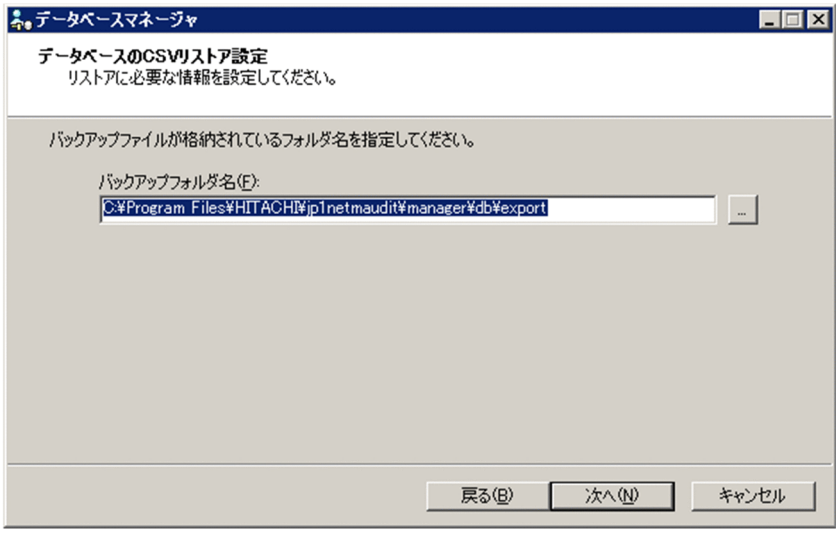
1. [データベースマネージャ] ダイアログで，「データベースの CSV リストア」を選択して，[次へ] ボタンをクリックする。

   [データベースのパスワード確認] 画面が表示されます。[データベースのパスワード確認] 画面については，図 10-3 を参照してください。

2. データベースのパスワードを入力して，[次へ] ボタンをクリックする。

   次の図に示す［データベースの CSV リストア設定］画面が表示されます。

   図 10-8　［データベースの CSV リストア設定］画面



3. CSV バックアップフォルダ名を指定する。

   「バックアップフォルダ名」に，CSV バックアップファイルが格納されているフォルダ名をフルパスで入力します。[...] ボタンをクリックすると，フォルダを参照するダイアログからフォルダ名を指定できます。

   デフォルトの CSV バックアップフォルダのパスを次に示します。

```
JP1/Audit Management - Managerのインストール先フォルダ¥db¥export
```

4. [次へ] ボタンをクリックする。
   [データベースの CSV リストア実行] 画面ダイアログが表示されます。

5. [実行] ボタンをクリックする。
   データベースの CSV バックアップがリストアされます。CSV リストアが完了すると，CSV リストアが完了したことを示すメッセージが表示されます。
   なお，リストアの実行時間は，データベースの容量とリストアする CSV バックアップファイルのデータ量に比例します。

6. [OK] ボタンをクリックする。
   [データベースマネージャ] ダイアログが閉じます。
   必要に応じて，コントロールパネルの「管理ツール」から「サービス」を開いて，JP1/Audit Management - Manager のサービスを開始します。開始するサービスの詳細は「5.7.1　監査ログ管理サーバを開始する」を参照してください。

10.1.9　データベースのデータ移行

監査ログのデータやバックアップ実行履歴など，データベースに格納されているすべてのデータを，データベースの CSV バックアップおよびデータベースの CSV リストアをすることによって移行できます。マシンのリプレースなどで別のサーバにデータを移行したいときに実施してください。

移行先のサーバが異なるホスト名である場合や JP1/Audit Management - Manager のインストール先フォルダを設定している場合でも，データを移行できます。

ただし，移行元サーバと移行先サーバの JP1/Audit Management - Manager のバージョンは一致している必要があります。

ここでは，データの移行元のサーバを「**移行元サーバ**」，データの移行先のサーバを「**移行先サーバ**」と呼びます。

> **参考**
>
> 「データベースのバックアップ」および「データベースのリストア」では，バックアップ時と同じ環境条件でのリストアしかできないため，別のサーバへデータを移行するときには利用できません。

データベースのデータ移行の手順を次に示します。

1. 移行元サーバで，データベースの CSV バックアップを実行する。
   データベースの CSV バックアップ方法については「10.1.7　データベースの CSV バックアップ」を参照してください。

2. 移行先サーバで，JP1/Audit Management - Manager をインストールする。

JP1/Audit Management - Manager のインストール方法については「5.2.4　JP1/Audit Management - Manager を新規インストールする」を参照してください。

3. 移行先サーバで，データベースのセットアップをする。

   データベースのセットアップをするときに，移行先サーバのデータベース容量は移行元サーバのデータベース容量と同じまたはそれ以上に設定してください。移行元サーバよりもデータベース容量が小さい場合，データが入りきらないことがあります。

   データベースのセットアップについては「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照してください。

4. 移行先サーバで，データベースの CSV リストアを実行する。

   データベースの CSV リストアについては「10.1.8　データベースの CSV リストア」を参照してください。

10.1.10　データベースのデータ削除

データベースに格納された監査ログのデータを削除します。

監査ログのデータを格納するデータベースの領域は，データベースのセットアップ時に作成されます。このデータベース領域は，長期間運用し続けると容量が不足します。また，格納しているデータ量が増加すると，検索機能も低下します。このため，監査が完了して不要になったデータは，定期的に削除することをお勧めします。

データベースのデータの削除はコマンドで実行します。コマンドの使い方については「12.　コマンド」の「admdbdelete（データベースのデータ削除）」を参照してください。

注意事項

削除するデータを誤った場合などに備え，データの削除前にはデータベースのバックアップも取得することをお勧めします。データベースのバックアップについては「10.1.3　データベースのバックアップ」を参照してください。

10.2　データベースのディスク容量の管理

JP1/Audit Management - Manager が使用するデータベースは，データベースのセットアップ時に指定されたサイズの領域を確保します。このため，運用中にデータベース領域のディスク容量が増加することはありません。データベースのセットアップ時には運用環境に適切なデータベースのサイズを設定してください。

データベースのディスク容量の管理方法について次に示します。

- データベースを再編成する

  長期間運用し続けると，データの格納効率が悪くなることがあります。データの格納効率を良くするため，1 か月に 1 回を目安にデータベースを再編成することをお勧めします。

  データベースの再編成については「10.1.5　データベースの再編成」を参照してください。

- データベースの使用状況に応じて対処する

  補助的な手段ですが，データベースの使用状況を確認し，その結果に応じて，データベースのデータ削除やサイズ変更で対処することもできます。

- データベースの使用状況を定期的に確認する

  運用に合わせてデータベースの使用状況を定期的に確認し，データベースのディスク容量に十分な空き容量があるかを確認してください。

  また，イベントログに「KFPH00211-I」（ソース：「HiRDBEmbeddedEdition_AL1」）のメッセージが出力されていないかを確認してください。

  1 か月に 1 回を目安にデータベースの使用状況を確認することをお勧めします。

10.2.1　データベースの使用状況に応じて対処する

データベースの使用状況は，admdbstat コマンドで確認できます。admdbstat コマンドの詳細については「12.　コマンド」の「admdbstat（データベースの使用状況確認）」を参照してください。admdbstat コマンドの実行結果は標準出力に出力されます。出力例を次に示します。

```
[監査ログ情報]
監査ログ件数　　　　：1095000
データ領域使用率　　：27%
インデクス領域使用率：18%

[監査ログ統計情報]
統計パターン数　　　：200
データ領域使用率　　：8%
インデクス領域使用率：5%
```

「監査ログ情報」および「監査ログ統計情報」のそれぞれについて，データ件数と領域使用率が表示されます。データ領域またはインデクス領域の使用率が高い場合は，データベースのデータを削除する，またはデータベースのサイズを変更して再作成することで対処してください。

(1)　データベースのデータを削除する

監査が完了した期間のデータをバックアップしたあと，データベースからデータを削除します。使用率が高い領域について次の対処を実施してください。

(a)　監査ログ情報のデータ領域またはインデクス領域の使用率が高い場合

データベースに格納されている監査ログを，次の手順で削除します。

1. admexport コマンドを実行して監査ログをバックアップする。
   admexport コマンドの詳細については「12.　コマンド」の「admexport（監査ログのバックアップ）」を参照してください。

2. admdbdelete コマンドを実行して監査ログを削除する。
   admdbdelete コマンドの詳細については「12.　コマンド」の「admdbdelete（データベースのデータ削除）」を参照してください。

(b)　監査ログ統計情報のデータ領域またはインデクス領域の使用率が高い場合

データベースに格納されている監査ログの統計情報を，次の手順で削除します。

なお，直前に「(a)　監査ログ情報のデータ領域またはインデクス領域の使用率が高い場合」の手順を実施している場合，監査ログ統計情報の領域の使用率もすでに下がっていることがあります。「(a)　監査ログ情報のデータ領域またはインデクス領域の使用率が高い場合」の手順を実施している場合は，再度 admdbstat コマンドを実行してデータベースの使用状況を確認してください。

1. 監査ログの統計結果をファイルに出力する。
   監査ログの統計結果をファイルに出力する手順については「7.5.1　監査ログの統計」を参照してください。

2. admstdel コマンドを実行して統計情報を削除する。
   admstdel コマンドの詳細については「12.　コマンド」の「admstdel（監査ログの統計情報削除）」を参照してください。

(2)　データベースのサイズを変更する

運用中に監査ログの収集量や監査ログ収集対象サーバが増加したり，監査ログの保存期間が長くなったりすることによって，容量不足になる場合が考えられます。この場合，データベースのサイズを，セットアップ済みの領域サイズより大きなサイズに変更してください。データベースのサイズを変更する場合は，データベースを再セットアップする必要があります。ただし，再セットアップすると，データベースのデータがすべて削除されてしまいます。したがって，サイズを変更する場合は，必ず CSV バックアップを取得してください。

データベースのサイズは，次の手順で変更します。

1. データベースの CSV バックアップを実行する。

データベースの CSV バックアップ方法については「10.1.7　データベースの CSV バックアップ」を参照してください。

2. データベースの再セットアップを実行する。

［データベースの詳細設定］画面で，データベースのサイズを変更します。

データベースの再セットアップ方法はセットアップ方法と同様です。データベースのセットアップについては「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照してください。

3. データベースの CSV リストアを実行する。

データベースの CSV リストアについては「10.1.8　データベースの CSV リストア」を参照してください。

11 監査ログ管理画面

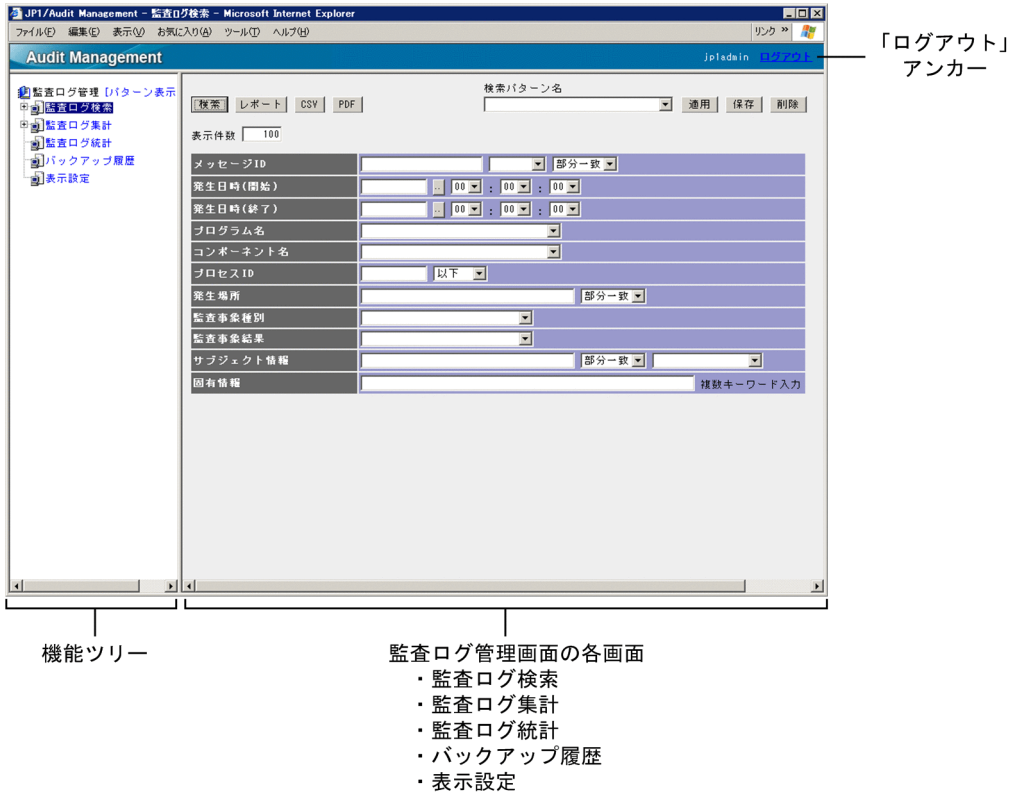
監査ログ管理画面は，監査ログの検索，監査ログの集計，監査ログの統計，およびバックアップファイルをダウンロードするときに使用する画面です。この章では，監査ログ管理画面の各部の名称と使い方について説明します。

11.1　監査ログ管理画面の各部の名称と使い方

ログインすると，監査ログ管理画面が表示されます。監査ログ管理画面へログインする手順については「7.2　監査ログ管理画面へのログインとログアウト」を参照してください。

ここでは，監査ログ管理画面の各部の名称と使い方を説明します。

図 11-1　監査ログ管理画面の各部の名称



「ログアウト」アンカー

クリックすると監査ログ管理画面からログアウトします。

機能ツリー

実行したい操作に合わせてメニューを選択します。実行したいメニューをクリックすると，それに応じた画面が，右フレームに表示されます。

機能ツリーの詳細については「11.2　機能ツリー」を参照してください。

監査ログ管理画面の各画面

監査ログ管理画面にログインすると，監査ログ検索画面が表示されます。また，機能ツリーでメニューを選択すると，メニュー対応した監査ログ管理画面の各画面が表示されます。

機能ツリーで次の画面が選択できます。

- 監査ログ検索画面

  監査ログ検索画面の詳細については「11.3　監査ログ検索画面」を参照してください。

- 監査ログ集計画面

監査ログ集計画面の詳細については「11.4　監査ログ集計画面」を参照してください。

- 監査ログ統計画面
  監査ログ統計画面の詳細については「11.5　監査ログ統計画面」を参照してください。
- バックアップ履歴画面
  バックアップ履歴画面の詳細については「11.6　バックアップ履歴画面」を参照してください。
- 表示設定画面
  表示設定画面の詳細については「11.7　表示設定画面」を参照してください。

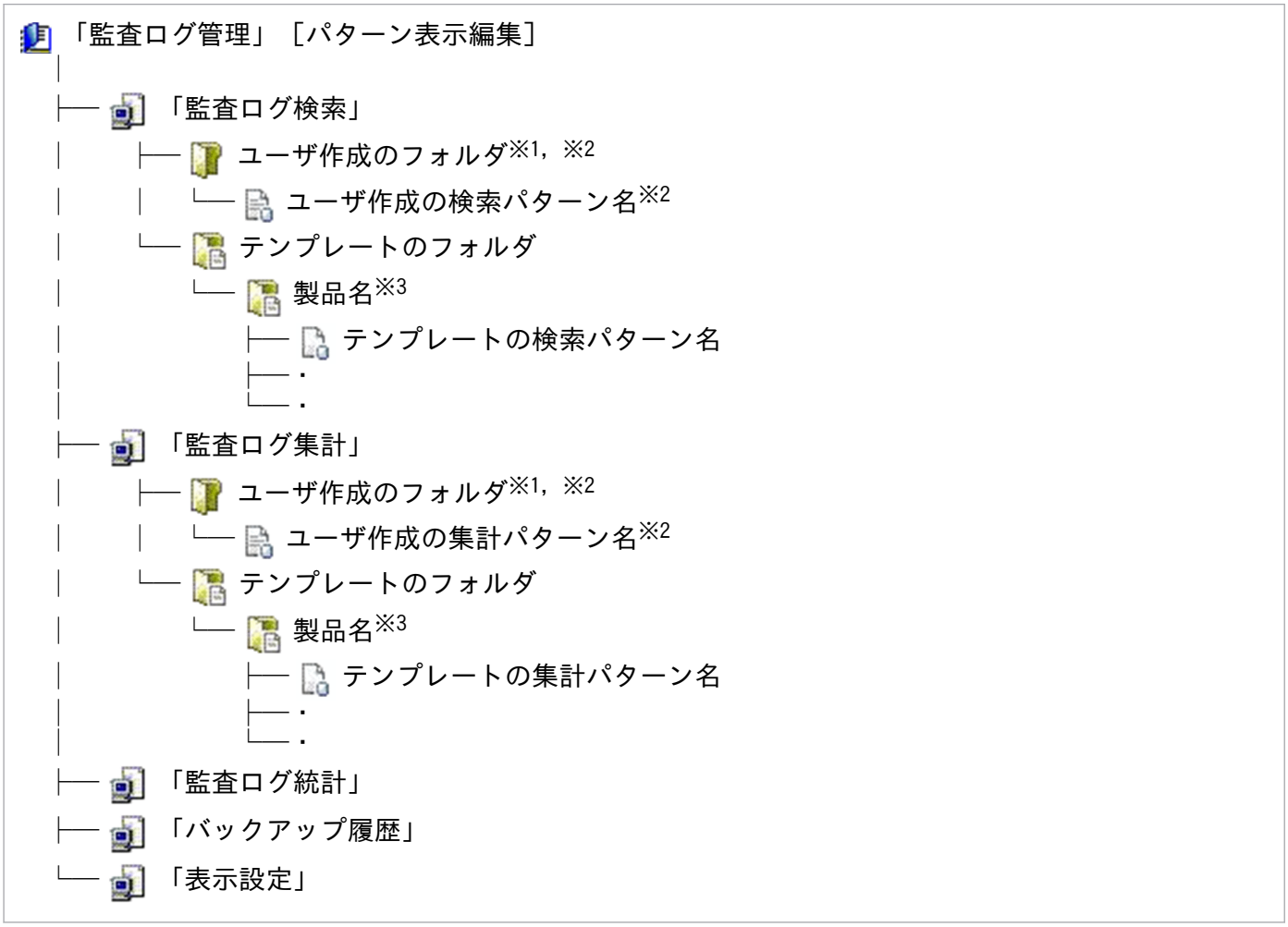
11.2　機能ツリー

機能ツリーには，監査ログ管理操作の対象がツリー項目として表示されています。

ここでは，機能ツリーのツリー項目とアイコンの動作について説明します。

11.2.1　機能ツリーのツリー項目

機能ツリーに表示されるツリー項目を次に示します。



注※1

フォルダは 10 階層まで作成できます。また，最上位の「ユーザ作成のフォルダ」配下には，ツリー項目を 4,096 個まで作成できます。ただし，ツリー項目を大量（2,000 個が目安）に作成する場合，IIS の送信バッファの最大サイズは，デフォルトより大きい値を設定しておく必要があります。設定方法については「5.5.1(3)　IIS 送信バッファの最大サイズの設定」を参照してください。

注※2

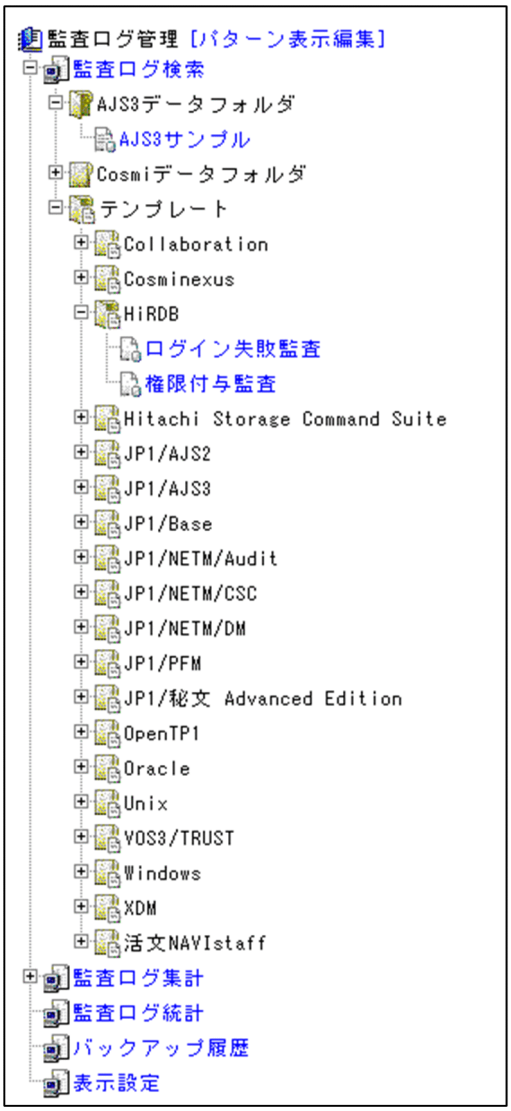
ユーザが作成した名称が表示されます。

注※3

JP1/Audit Management - Manager が標準サポートしている製品ごとにフォルダが分かれ，それぞれテンプレートの検索パターン名または集計パターン名が表示されます。

機能ツリーの構成例を次の図に示します。

図 11-2　機能ツリーの構成例



機能ツリーのうちフォルダやパターンについては，パターン表示編集画面で表示・非表示をカスタマイズできます。

機能ツリーのツリー項目をクリックしたときに表示される画面を次の表に示します。

表 11-1　機能ツリーのクリックと画面表示

項番	ツリー項目の種類	表示内容	クリック時の画面表示
1	ルート	「監査ログ管理」が表示されます。	－
2	［パターン表示編集］のリンク	［パターン表示編集］が表示されます。	パターン表示編集画面が表示されます。

項番	ツリー項目の種類	表示内容	クリック時の画面表示
3	業務メニュー	次の監査ログ管理操作が表示されます。 • 監査ログ検索 • 監査ログ集計 • 監査ログ統計 • バックアップ履歴 • 表示設定	それぞれ次に示す画面が表示されます。 • 監査ログ検索画面 • 監査ログ集計画面 • 監査ログ統計画面 • バックアップ履歴画面 • 表示設定画面
4	ユーザ作成のフォルダ	ユーザが作成した検索パターン，および集計パターンを格納するフォルダ名が表示されます。	−
5	ユーザ作成のパターン	ユーザが作成した検索パターン名，および集計パターン名が表示されます。	• 検索パターンをクリックした場合 選択した検索パターンを適用した監査ログ検索画面が表示されます。 • 集計パターンをクリックした場合 選択した集計パターンを適用した監査ログ集計画面が表示されます。
6	テンプレートのフォルダ	テンプレートのプログラムフォルダを格納するフォルダ名が表示されます。	−
7	テンプレートのプログラムフォルダ	テンプレートの検索パターン，集計パターンを持つ製品名が表示されます。 表示される製品名を次に示します。 • Collaboration • Cosminexus • HiRDB • Hitachi Navigation Platform • Hitachi Storage Command Suite • JP1/AJS2 • JP1/AJS3 • JP1/AO • JP1/Base • JP1/IM - NP • JP1/IM - SS • JP1/ITDM • JP1/ITDM2 • JP1/ITRM • JP1/NETM/AIM • JP1/NETM/Audit • JP1/NETM/CSC • JP1/NETM/DM	−

項番	ツリー項目の種類	表示内容	クリック時の画面表示
		• JP1/NETM/NM • JP1/PFM • JP1/秘文 Advanced Edition • OpenTP1 • Oracle • uCosminexus EUR Server • uCosminexus Navigation Platform • uCosminexus Portal Framework • UNIX • VOS3/TRUST※ • Windows • XDM • 活文 NAVIstaff	
8	テンプレートのパターン	製品名に対応したテンプレートの検索パターン名，および集計パターン名が表示されます。	• 検索パターンをクリックした場合 選択した検索パターンを適用した監査ログ検索画面が表示されます。 • 集計パターンをクリックした場合 選択した集計パターンを適用した監査ログ集計画面が表示されます。

（凡例）

－：画面遷移なし

注※

TRUST E2 用のテンプレートのフォルダです。

11.2.2　機能ツリーのアイコンの動作

監査ログ管理画面にログインすると，機能ツリーは，ルートアイコン以外はすべて格納された状態で表示されます。機能ツリーの項目名の左にあるアイコンをクリックすることで，ツリー項目の格納や展開ができます。

アイコンの種類とアイコンをクリックしたときの動作を，次の表に示します。

表 11-2　アイコンの動作

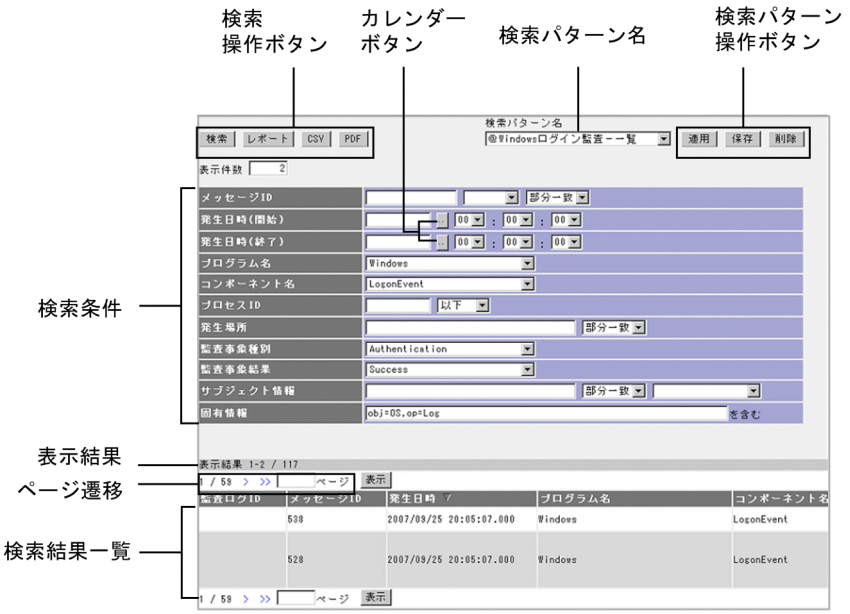
項番	アイコンの種類		アイコンの動作
1	格納アイコン（プラスアイコン）		クリックすると，下位のツリー項目が展開され，展開アイコンに変化します。
2	展開アイコン（マイナスアイコン）		クリックすると，下位のツリー項目が格納され，格納アイコンに変化します。

項番	アイコンの種類		アイコンの動作
3	ルートアイコン		クリックしても変化しません。
4	業務メニューアイコン		クリックしても変化しません。
5	ユーザ作成フォルダアイコン（格納フォルダアイコン）		クリックすると，格納アイコン（プラスアイコン）と同じ動作をします。
6	ユーザ作成フォルダアイコン（展開フォルダアイコン）		クリックすると，展開アイコン（マイナスアイコン）と同じ動作をします。
7	ユーザ作成パターンアイコン		クリックすると，アイコンの右に表示されている項目名をクリックしたときと同じ動作をします。
8	テンプレートフォルダアイコン（格納フォルダアイコン）		クリックすると，格納アイコン（プラスアイコン）と同じ動作をします。
9	テンプレートフォルダアイコン（展開フォルダアイコン）		クリックすると，展開アイコン（マイナスアイコン）と同じ動作をします。
10	テンプレートパターンアイコン		クリックすると，アイコンの右に表示されている項目名をクリックしたときと同じ動作をします。

11.3　監査ログ検索画面

監査ログ検索画面は，監査ログを検索するときに使います。監査ログ検索画面の各部の名称と使い方を説明します。

図 11–3　監査ログ検索画面の各部の名称



検索条件

監査ログを検索するための条件を指定します。各項目の詳細については「7.3.2　監査ログの検索条件項目」を参照してください。

検索条件の項目は必要に応じて非表示にしたり，並べ替えたりできます。詳細については「7.7.1(3) 監査ログ検索画面の表示設定項目」を参照してください。

カレンダーボタン

カレンダーを使って，日付を指定できます。カレンダーボタンをクリックすると，カレンダーが表示されます。

カレンダーを使った日付の指定方法を次の図に示します。

図 11-4　カレンダーを使った日付の指定方法

検索操作ボタン

監査ログの検索を実行するボタンについて次に説明します。

- ［検索］ボタン

  監査ログの検索結果を，検索結果一覧に表示します。検索結果一覧の見方については「7.3.3(1) 検索結果一覧を表示する場合」を参照してください。

- ［レポート］ボタン

  監査ログの検索結果を，監査ログレポート画面に表示します。監査ログレポート画面については「11.8　監査ログレポート画面」を参照してください。

- ［CSV］ボタン

  監査ログの検索結果を CSV 形式で出力します。CSV 形式ファイルの見方については「7.3.3(2) CSV 形式ファイルを出力する場合」を参照してください。

- ［PDF］ボタン

  監査ログの検索結果を PDF ファイルに出力します。PDF ファイルに出力する場合は，EUR が必要です。PDF ファイルの見方については「7.3.3(3)　PDF ファイルを出力する場合」を参照してください。

「表示件数」

監査ログの検索結果一覧の 1 ページに表示されるレコード数を，1～200 の半角数字で入力します。ほかの画面に移動した場合，指定した値は保持されません。また，［保存］ボタンをクリックすると，表示件数は検索パターン名と合わせて保存されます。

デフォルト値は，表示設定画面の「レコード数/ページ」で指定している値です。

検索パターン名

検索パターンとは，保存した検索条件のことです。作成した検索パターンは，プルダウンメニューに一覧表示されます。ここで検索パターンを選択し，保存した検索条件を呼び出して検索できます。検索条件を保存する方法については「7.3.5　監査ログ検索パターンの編集」を参照してください。

検索パターン操作ボタン

検索パターンを利用するためのボタンについて説明します。

- ［適用］ボタン

  検索パターンを適用して，保存した検索条件を呼び出します。検索パターンを適用する方法については「7.3.1(2)　検索パターンを利用する」を参照してください。

- ［保存］ボタン

  指定した検索条件を検索パターンとして保存します。同じ業務メニュー内の既存のフォルダと同じ名称を指定することはできません。

  既存の検索パターンと同じ名称を指定した場合，内容が上書きされます。新規の検索パターン名を指定した場合，パターン保存画面が表示されます。検索条件を保存する方法については「7.3.5 監査ログ検索パターンの編集」を参照してください。

- ［削除］ボタン

  検索パターンを削除します。検索パターンを削除する方法については「7.3.5(3)　検索パターンを削除する」を参照してください。

検索結果一覧

検索条件と一致する監査ログが一覧で表示されます。各項目のヘッダーをクリックすると，項目ごとに一覧を昇順または降順にソートできます。デフォルトでは「発生日時」で降順にソートされます。表示設定画面で「発生日時」を非表示に設定している場合でも，検索結果一覧は「発生日時」でソートされた状態で表示されます。

検索結果の見方については「7.3.3　監査ログ検索結果の確認」を参照してください。

表示結果

現在のページに表示されているレコード番号が，「先頭のレコード番号 - 末尾のレコード番号）/レコード総数」で表示されています。

ページ遷移

検索結果が複数ページにわたる場合は，ページリンクをクリックしてほかのページを表示します。また，ページ番号を指定して，指定したページを表示することもできます。

ページリンク

各ページリンクをクリックすると表示されるページを次に示します。

- 「<<」

  最初のページが表示されます。

- 「<」

  一つ前のページが表示されます。

- 「>」

  次のページが表示されます

- 「>>」

  最後のページが表示されます。

現在のページ番号/合計ページ数

現在のページ番号とページの総数を示します。

「ページ」

表示するページ番号を，1～最終ページ番号の半角数字で入力します。

デフォルト値は空白です。

［表示］ボタン

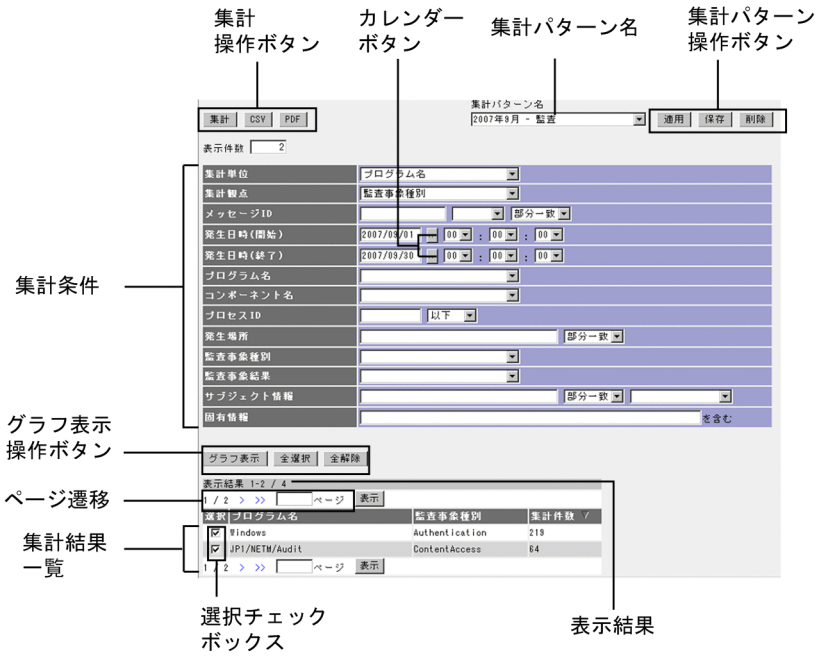
指定したページ番号の検索結果が表示されます。

なお，ページ遷移の実行中に検索条件と一致する新たな監査ログが追加された場合は，表示されている情報が最新の状態に更新されます。再度ページを遷移すると，追加された監査ログの件数だけ検索結果に反映して表示されます。

11.4　監査ログ集計画面

監査ログ集計画面は，監査ログを集計するときに使います。監査ログ集計画面の各部の名称と使い方を説明します。

図 11-5　監査ログ集計画面の各部の名称



集計条件

監査ログを集計するための条件を指定します。詳細については「7.4.2　監査ログの集計条件項目」を参照してください。

集計条件の項目は必要に応じて非表示にしたり，並べ替えたりできます。詳細については「7.7.2(3) 監査ログ集計画面の表示設定項目」を参照してください。

カレンダーボタン

カレンダーを使って，日付を指定できます。カレンダーボタンをクリックすると，カレンダーが表示されます。カレンダーを使った日付の指定方法については「11.3　監査ログ検索画面」の「カレンダーボタン」を参照してください。

集計操作ボタン

監査ログの集計を実行するボタンについて説明します。

- ［集計］ボタン

  監査ログの集計結果を，集計結果一覧に表示します。集計結果一覧の見方については「7.4.3(1) 集計結果一覧を表示する場合」を参照してください。

- ［CSV］ボタン

  監査ログの集計結果を CSV 形式で出力します。CSV 形式ファイルの見方については「7.4.3(2) CSV 形式ファイルを出力する場合」を参照してください。

- ［PDF］ボタン

  監査ログの集計結果を PDF ファイルに出力します。PDF ファイルに出力する場合は，EUR が必要です。PDF ファイルの見方については「7.4.3(3)　PDF ファイルを出力する場合」を参照してください。

「表示件数」

監査ログの集計結果一覧の 1 ページに表示されるレコード数を，1～200 の半角数字で入力します。ほかの画面に移動した場合，指定した値は保持されません。また，［保存］ボタンをクリックすると，表示件数は集計パターン名と合わせて保存されます。

デフォルト値は，表示設定画面の「レコード数/ページ」で指定している値です。

集計パターン名

集計パターンとは，保存した集計条件のことです。作成した集計パターンは，プルダウンメニューに一覧表示されます。ここで集計パターンを選択し，保存した集計条件を呼び出して集計できます。集計条件を保存する方法については「7.4.5　監査ログ集計パターンの編集」を参照してください。

集計パターン操作ボタン

集計パターンを利用するためのボタンについて説明します。

- ［適用］ボタン

  集計パターンを適用して，保存した集計条件を呼び出します。集計パターンを適用する方法については「7.4.1(2)　集計パターンを利用する」を参照してください。

- ［保存］ボタン

  指定した集計条件を集計パターンとして保存します。同じ業務メニュー内の既存のフォルダと同じ名称を指定することはできません。

  既存の集計パターンと同じ名称を指定した場合，内容が上書きされます。新規の集計パターン名を指定した場合，パターン保存画面が表示されます。集計条件を保存する方法については「7.4.5 監査ログ集計パターンの編集」を参照してください。

- ［削除］ボタン

  集計パターンを削除します。集計パターンを削除する方法については「7.4.5(3)　集計パターンを削除する」を参照してください。

注意事項

作成した集計パターンを統計パターンとして設定している場合，集計パターンの集計条件を変更して保存すると，統計パターンも連動して変更されます。統計パターンが変更されると，変更前の統計パターンを基にした統計結果を正しく出力できないことがあります。この場合，統計情報を生成し直してください。

また，集計パターンを削除した場合，連動して統計パターンも「統計パターン」から削除されます。統計パターンが削除されると，削除した統計パターンを基にした統計結果を出力できなくなります。統計パターンについては「7.5.4　監査ログ統計パターンの設定」を参照してください。

集計結果一覧

集計条件と一致する監査ログが一覧で表示されます。項目のヘッダーをクリックすると，一覧を昇順または降順にソートできます。デフォルトでは，「集計件数」で降順にソートされます。

集計結果の見方については「7.4.3　監査ログ集計結果の確認」を参照してください。

選択チェックボックス

集計結果グラフ表示画面で表示する集計結果を選択します。選択する集計結果の選択チェックボックスにチェックを入れてください。デフォルトではすべての集計結果がチェックされています。

グラフ表示操作ボタン

集計結果をグラフ表示するためのボタンについて説明します。

- ［グラフ表示］ボタン

  監査ログの集計結果グラフ表示画面が表示されます。集計一覧表示で選択されている監査ログ集計結果のグラフが表示されます。集計結果グラフ表示画面については「11.9　集計結果グラフ表示画面」を参照してください。

- ［全選択］ボタン

  現在表示しているページのすべての選択チェックボックスにチェックが入り，選択されます。

- ［全解除］

  現在表示しているページのすべての選択チェックボックスのチェックが外されます。

表示結果

現在のページに表示されているレコード番号が，「先頭のレコード番号 - 末尾のレコード番号）/レコード総数」で表示されています。

ページ遷移

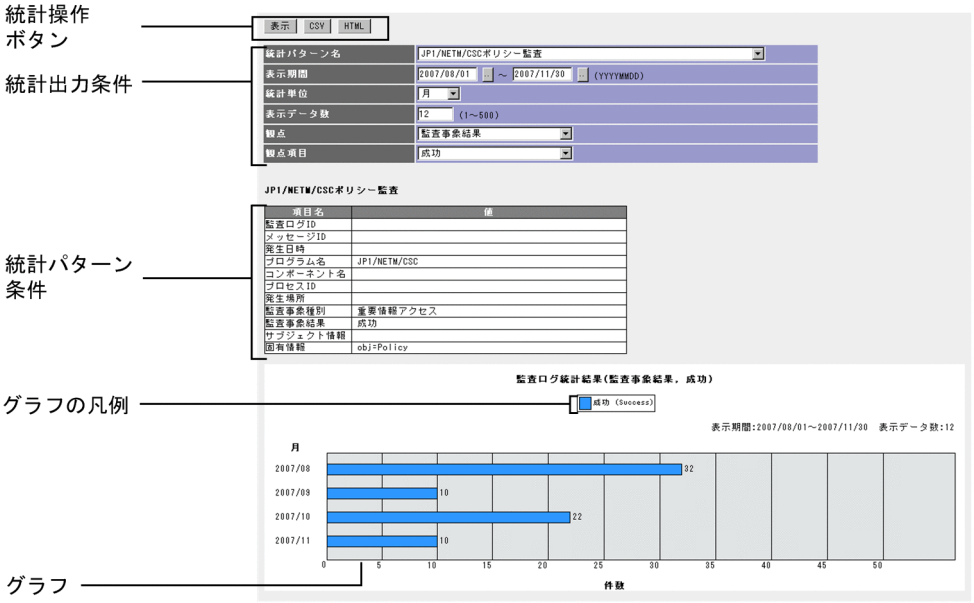
集計結果が複数ページにわたる場合は，ページリンクをクリックしてほかのページを表示します。また，ページ番号を指定して，指定したページを表示することもできます。

ページ遷移の方法については「11.3　監査ログ検索画面」の「ページ遷移」を参照してください。

11.5　監査ログ統計画面

監査ログ統計画面は，生成された監査ログの統計情報を基にして統計結果を出力するときに使います。監査ログ統計画面の各部の名称と使い方を説明します。

図 11-6　監査ログ統計画面の各部の名称



統計出力条件

統計結果を出力するための統計出力条件を指定します。指定できる統計出力条件の詳細については「7.5.2　監査ログの統計出力条件項目」を参照してください。なお，統計出力条件のうち，統計パターンは事前に設定しておく必要があります。設定していない場合，統計結果を出力できません。統計パターンの設定については「7.5.4　監査ログ統計パターンの設定」を参照してください。また，統計パターンを除いた統計出力条件は，デフォルト値を設定できます。統計出力条件のデフォルト値を設定する方法については「7.7.3　監査ログ統計画面の表示項目を設定する」を参照してください。

統計操作ボタン

監査ログの統計結果を出力するボタンについて説明します。

- ［表示］ボタン

  監査ログの統計結果をグラフ形式で表示します。統計結果のグラフの見方については「7.5.3(1) 監査ログ統計結果をグラフ形式で表示する場合」を参照してください。

- ［CSV］ボタン

  監査ログの統計結果を CSV 形式で出力します。CSV 形式ファイルの見方については「7.5.3(2) CSV 形式ファイルを出力する場合」を参照してください。

- ［HTML］ボタン

  監査ログの統計結果を HTML 形式で出力します。保存対象となるのは，統計パターン名，統計パターン条件，凡例，およびグラフです。

統計パターン条件

統計パターンとして設定されている集計条件が表示されます。詳細については「7.5.3　監査ログ統計結果の確認」を参照してください。

グラフの凡例

観点項目で指定した内容に従って，グラフの凡例が表示されます。詳細については「7.5.3　監査ログ統計結果の確認」を参照してください。

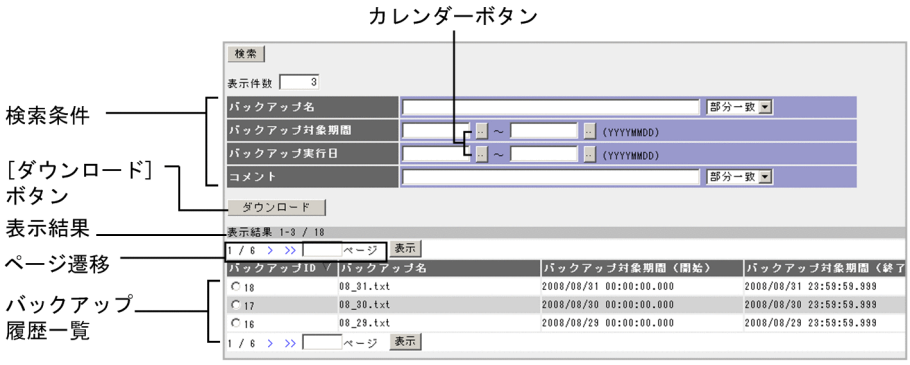
グラフ

指定した統計単位ごとに，統計結果がグラフ形式で表示されます。詳細については「7.5.3　監査ログ統計結果の確認」を参照してください。

11.6　バックアップ履歴画面

バックアップ履歴画面は，バックアップ履歴を検索し，バックアップファイルをダウンロードするときに使います。バックアップ履歴画面の各部の名称と使い方を説明します。

図 11-7　バックアップ履歴画面の各部の名称



検索条件

バックアップ履歴を検索するための条件を指定します。詳細については「7.6.2　バックアップ履歴の検索条件項目」を参照してください。

検索条件の項目は必要に応じて非表示にしたり，並べ替えたりできます。詳細については「7.7.4(3) バックアップ履歴画面の表示設定項目」を参照してください。

カレンダーボタン

カレンダーを使って，日付を指定できます。カレンダーボタンをクリックすると，カレンダーが表示されます。カレンダーを使った日付の指定方法については「11.3　監査ログ検索画面」の「カレンダーボタン」を参照してください。

［検索］ボタン

バックアップ履歴の検索結果をバックアップ履歴一覧に表示します。バックアップ履歴の検索方法については「7.6.1　バックアップ履歴を検索する」を参照してください。

「表示件数」

バックアップ履歴の検索結果一覧の 1 ページに表示されるレコード数を，1～200 の半角数字で入力します。ほかの画面に移動した場合，指定した値は保存されません。バックアップ履歴画面が再描画されたときは，デフォルト値が設定されます。

デフォルト値は，表示設定画面の「レコード数/ページ」で指定している値です。

［ダウンロード］ボタン

バックアップファイルをダウンロードするときに使用します。バックアップファイルのダウンロード方法については「7.6.4　バックアップファイルをダウンロードする」を参照してください。

バックアップ履歴一覧

検索条件と一致するバックアップファイルが一覧で表示されます。項目のヘッダーをクリックすると，一覧を昇順または降順にソートできます。デフォルトでは，「バックアップ ID」で降順にソートされます。

検索結果の見方については「7.6.3　バックアップ履歴検索結果の確認」を参照してください。

表示結果

現在のページに表示されているレコード番号が，「先頭のレコード番号 - 末尾のレコード番号）/レコード総数」で表示されています。

ページ遷移

検索結果が複数ページにわたる場合は，ページリンクをクリックしてほかのページを表示します。また，ページ番号を指定して，指定したページを表示することもできます。

ページ遷移の方法については「11.3　監査ログ検索画面」の「ページ遷移」を参照してください。

11.7　表示設定画面

表示設定画面は，次の画面での表示項目を設定するのに使用します。

- 監査ログ検索画面
- 監査ログ集計画面
- 監査ログ統計画面
- バックアップ履歴画面

表示設定画面の［設定画面］プルダウンメニューから設定したい画面を選択して表示項目を設定してください。

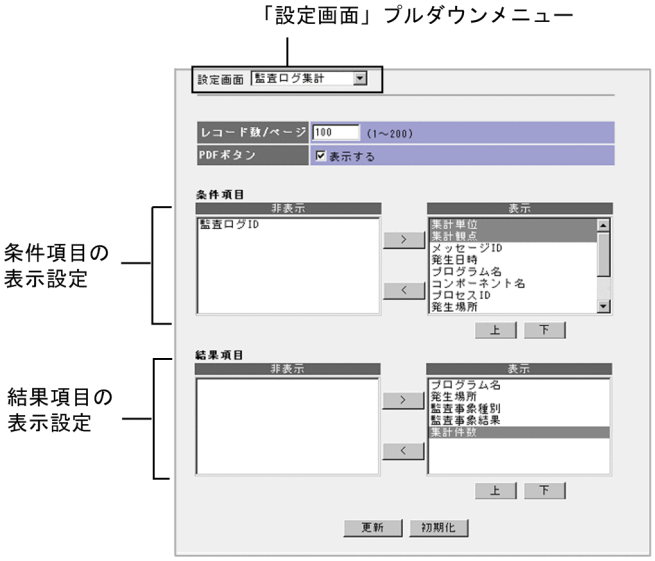
監査ログ管理画面の表示項目を設定する手順については「7.7　監査ログ管理画面の表示設定」を参照してください。

11.7.1　監査ログ検索画面・監査ログ集計画面・バックアップ履歴画面の表示項目の設定

表示設定画面から監査ログ検索画面・監査ログ集計画面・バックアップ履歴画面について設定する場合の各部の名称と使い方について説明します。

表示設定画面の［設定画面］プルダウンメニューで「監査ログ集計」を選択して表示される画面を次の図に示します。

図 11–8　表示設定画面



「レコード数/ページ」

検索結果および集計結果一覧に表示されるレコード数を，1～200 の半角数字で入力します。設定した値は，監査ログ管理画面の各画面の［表示件数］に反映されます。

デフォルト値は「100」です。

「PDF ボタン」，「表示する」チェックボックス

チェックを外すと，検索画面および集計画面の［PDF］ボタンを非表示にできます。EUR を使用していないシステムの場合はチェックを外してください。

条件項目の表示設定

条件項目とは，検索条件または集計条件として表示される項目です。各画面の条件項目が，「表示」または「非表示」に一覧表示されます。表示される項目は，［設定画面］プルダウンメニューで選択する画面名によって異なります。

なお，灰色の項目は非表示にできません。

結果項目の表示設定

結果項目とは，検索結果一覧，集計結果一覧，またはバックアップ履歴一覧に表示される項目のことです。各画面の結果項目が，「表示」または「非表示」に一覧表示されます。表示される項目は，［設定画面］プルダウンメニューで選択する画面名によって異なります。

なお，灰色の項目は非表示にできません。

表示または非表示の変更

次のボタンを使用して，表示または非表示にする項目を変更します。

- ［>］ボタン

  選択した「非表示」の項目を「表示」に移動します。

- ［<］ボタン

  選択した「表示」の項目を「非表示」に移動します。

項目の並び順の変更

次のボタンを使用して，項目の並び順を変更します。

- ［上］ボタン

  選択した「表示」の項目を上に移動します。

- ［下］ボタン

  選択した「表示」の項目を下に移動します。

［更新］ボタン

変更した表示設定を保存します。

［初期化］ボタン

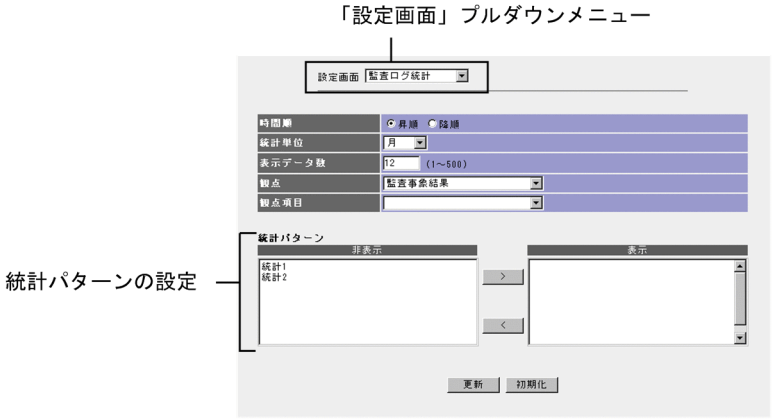
設定対象画面の表示設定を初期状態に戻し，初期化した状態で保存します。

11.7.2　監査ログ統計画面の表示項目の設定と統計パターンの設定

表示設定画面から監査ログ統計画面について設定する場合の各部の名称と使い方について説明します。

表示設定画面の［設定画面］プルダウンメニューで「監査ログ統計」を選択して表示される画面を次の図に示します。

図 11–9　表示設定画面



「時間順」

指定した時間単位ごとに表示されるグラフの表示順のデフォルト値を，「降順」または「昇順」から選択します。デフォルト値は「昇順」です。

「統計単位」

グラフの時間単位のデフォルト値を，「日」，「月」，または「年」から選択します。デフォルト値は「月」です。

「表示データ数」

グラフの表示データ数のデフォルト値を 1～500 の半角数字で入力します。設定した値は，監査ログ統計画面の［表示データ数］に反映されます。デフォルト値は「12」です。

「観点」

統計結果を出力する観点のデフォルト値を「監査事象種別」または「監査事象結果」から選択します。デフォルト値は「監査事象結果」です。

「観点項目」

統計結果を出力する観点項目のデフォルト値を指定します。「観点」で指定した内容によって指定する項目が異なります。

「統計パターン」

統計パターンとして設定する集計パターンを設定します。

統計パターンの設定

次のボタンを使用し，統計パターンとして設定する集計パターンを設定します。「表示」に移動すると，統計パターンとして設定されます。

- ［>］ボタン

選択した「非表示」の項目を「表示」に移動します。

- ［<］ボタン

  選択した「表示」の項目を「非表示」に移動します。

［更新］ボタン

変更した表示設定を保存します。

［初期化］ボタン

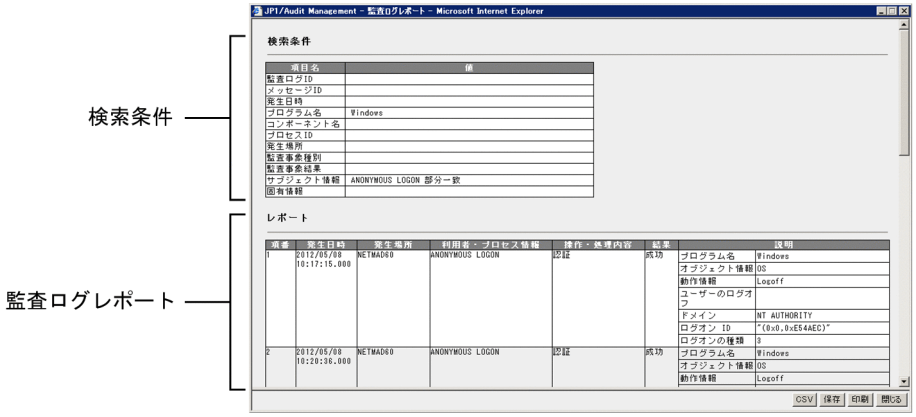
監査ログ統計画面の表示設定を初期状態に戻し，初期化した状態で保存します。

ただし，統計パターンの設定内容は初期化されません。

11.8　監査ログレポート画面

監査ログレポート画面は，監査ログの検索結果をレポート形式で表示するときに使用します。監査ログレポート画面の各部の名称と使い方を説明します。

図 11-10　監査ログレポート画面の各部の名称



検索条件

監査ログ検索画面の検索条件で指定した値が表示されます。

監査ログレポート

検索条件で検索した結果の監査ログ情報が解析され，レポート形式で表示されます。レポート表示結果の見方については「7.3.4　監査ログ検索結果のレポート表示」を参照してください。

[CSV] ボタン

監査ログレポートを CSV 形式で出力します。CSV 形式ファイルの見方については「7.3.4(2)　CSV 形式ファイルを出力する場合」を参照してください。

[保存] ボタン

監査ログレポートの画面表示を HTML 形式で出力します。

[印刷] ボタン

監査ログレポートを印刷します。

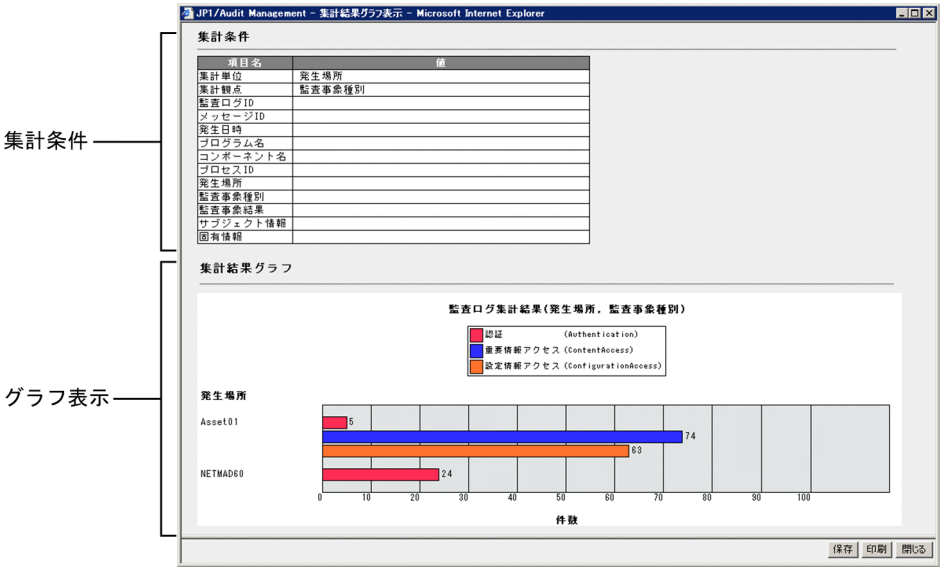
[閉じる] ボタン

監査ログレポート画面を閉じます。

11.9　集計結果グラフ表示画面

集計結果グラフ表示画面は，集計結果一覧で選択した集計結果をグラフで表示するときに使用します。集計結果グラフ表示画面の各部の名称と使い方を説明します。

図 11–11　集計結果グラフ表示画面の各部の名称



集計条件

監査ログ集計画面の集計条件で選択した値が表示されます。

グラフ表示

監査ログ集計画面で選択した集計結果がグラフで表示されます。グラフの見方については「7.4.4　監査ログ集計結果のグラフ表示」を参照してください。

[保存] ボタン

集計結果グラフ表示画面を HTML 形式で出力します。

[印刷] ボタン

集計結果グラフを印刷します。

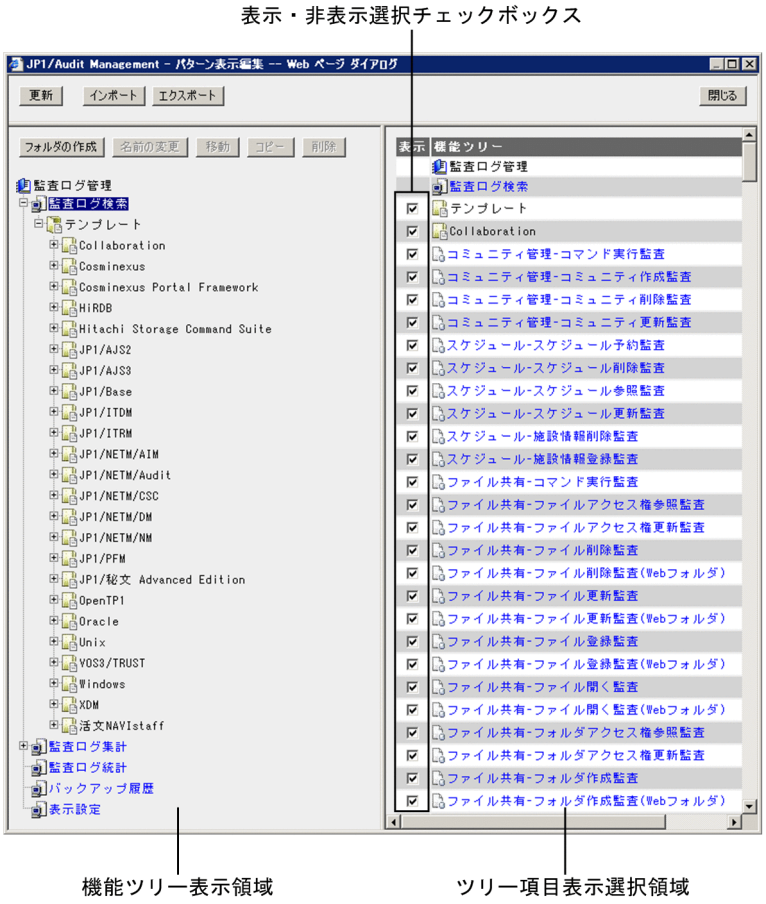
[閉じる] ボタン

集計結果グラフ表示画面を閉じます。

11.10　パターン表示編集画面

パターン表示編集画面は，機能ツリーを編集するとき，またはユーザ作成のフォルダやパターンの情報をエクスポートしたり，インポートしたりするときに使用します。また，監査ログ管理画面のプレビューとしても使用できます。パターン表示編集画面の各部の名称と使い方を説明します。

図 11-12　パターン表示編集画面の名称



機能ツリー表示領域

表示・非表示選択チェックボックスがチェックされているツリー項目を表示します。パターン表示編集画面のツリー項目は，監査ログ管理画面のツリー項目と表示順序が異なる場合があります。

ツリー項目表示選択領域

機能ツリーの項目を順に表示します。パターンやフォルダの表示・非表示を設定します。

表示・非表示選択チェックボックス

ツリー項目の表示・非表示を設定します。

- **チェックボックスがチェックされている場合**

  パターンやフォルダを表示します。デフォルトでは，すべてのチェックボックスがチェックされています。

- **チェックボックスのチェックが外されている場合**

パターンやフォルダを非表示にします。フォルダのチェックが外されている場合，フォルダの下の項目すべてを非表示にします。

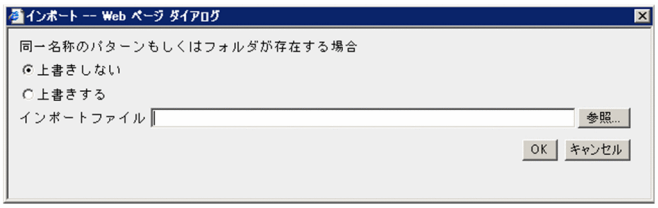
［更新］ボタン

編集した内容を監査ログ管理画面の機能ツリーに反映してパターン表示編集画面を閉じます。

［インポート］ボタン

次の図に示す［インポート］画面を表示します。

図 11-13 ［インポート］画面



インポートする情報と機能ツリー表示領域の情報とで，同一名称のパターンやフォルダが存在する場合に，上書きするかどうかを指定します。［上書きしない］または［上書きする］ラジオボタンを選択してください。デフォルトでは，［上書きしない］ラジオボタンが指定されています。

また，「インポートファイル」にインポートしたいパターン情報ファイルを指定します。［OK］ボタンをクリックすると，指定したパターン情報ファイルの情報がパターン表示編集画面に反映されます。

［エクスポート］ボタン

ファイルをダウンロードするダイアログが表示されます。［保存］ボタンをクリックすると，パターン情報ファイルが保存されます。パターン情報ファイルの詳細については「13.8 パターン情報ファイル」を参照してください。

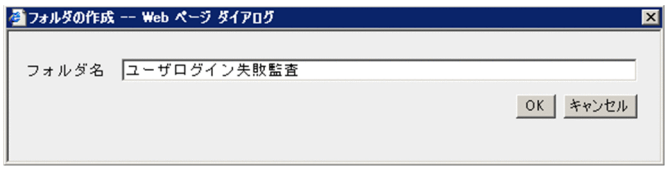
［閉じる］ボタン

編集した内容を破棄してパターン表示編集画面を閉じます。

［フォルダの作成］ボタン

次の図に示す［フォルダの作成］画面を表示します。

図 11-14 ［フォルダの作成］画面



作成するフォルダの名称を指定します。［OK］ボタンをクリックすると，選択したツリー項目の直下にフォルダを作成し，パターン表示編集画面に表示が反映されます。

フォルダの名称を指定する際の注意事項を次に示します。

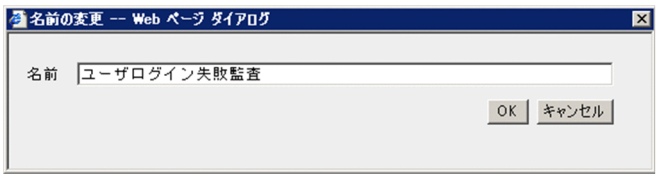
- 作成先の業務メニュー内にすでに存在するパターンまたはフォルダと同じ名称は，指定できません。
- 64 バイト以内の文字列で入力できます。
- 名称の先頭に「@」は使用できません。

- 名称中に「¥」は使用できません。
- フォルダは 10 階層まで作成できます。
- 最上位の「ユーザ作成のフォルダ」配下には，ツリー項目を 4,096 個まで作成できます。

［名前の変更］ボタン

次の図に示す［名前の変更］画面を表示します。

図 11–15　［名前の変更］画面



変更後のパターン名やフォルダ名を指定します。デフォルトでは，選択したツリー項目の名称が入力されています。［OK］ボタンをクリックすると，パターン名またはフォルダ名が変更され，パターン表示編集画面に表示が反映されます。

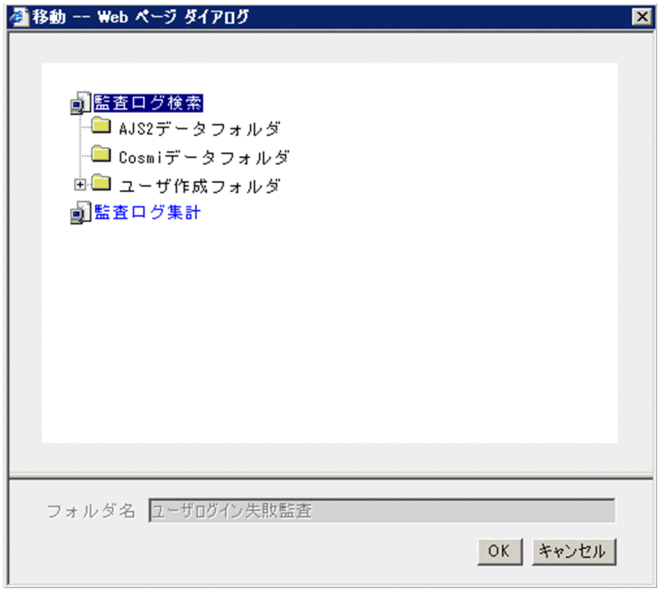
パターン名やフォルダ名を指定する際の注意事項を次に示します。

- 同じ業務メニュー内にすでに存在するパターンまたはフォルダと同じ名称は，指定できません。
- 64 バイト以内の文字列で入力してください。
- 名称の先頭に「@」は指定できません。
- （フォルダ名の場合）名称中に「¥」は使用できません。

［移動］ボタン

次の図に示す［移動］画面を表示します。

図 11–16　［移動］画面



移動先のフォルダを選択します。なお，［移動］画面を表示した時点では，［パターン名］または［フォルダ名］の値は非活性になっています。［OK］ボタンをクリックすると，パターンまたはフォルダが指定先に移動され，パターン表示編集画面に表示が反映されます。

移動先の業務メニュー内に，同じ名称のパターンまたはフォルダが存在する場合だけ，［OK］ボタンをクリックしたあとに警告ダイアログが表示され，［パターン名］または［フォルダ名］に値の入力ができるようになります。

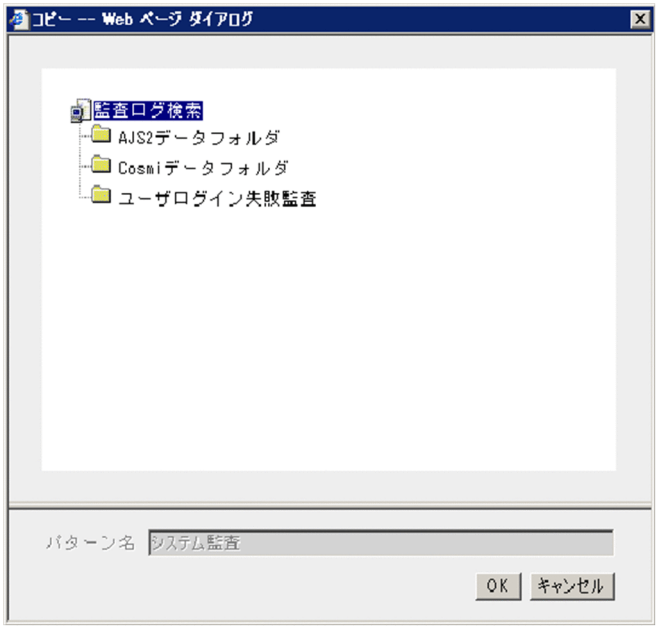
値を入力する際の注意事項を次に示します。

- 同じ業務メニュー内にすでに存在するパターンまたはフォルダと同じ名称は，指定できません。
- 64 バイト以内の文字列で入力してください。
- 名称の先頭に「@」は指定できません。
- フォルダは 10 階層まで作成できます。
- 最上位の「ユーザ作成のフォルダ」配下には，ツリー項目を 4,096 個まで作成できます。
- （フォルダ名の場合）名称中に「¥」は使用できません。

［コピー］ボタン

次の図に示す［コピー］画面を表示します。

図 11-17 ［コピー］画面



コピー先のフォルダを選択します。なお，［コピー］画面を表示した時点では，［パターン名］または［フォルダ名］の値は非活性になっています。［OK］ボタンをクリックすると，パターンまたはフォルダが指定先にコピーされ，パターン表示編集画面に表示が反映されます。

コピー先の業務メニュー内に，同じ名称のパターンまたはフォルダが存在する場合だけ，［OK］ボタンをクリックしたあとに警告ダイアログが表示され，［パターン名］または［フォルダ名］に値の入力ができるようになります。

値を入力する際の注意事項を次に示します。

- 同じ業務メニュー内にすでに存在するパターンまたはフォルダと同じ名称は，指定できません。
- 64 バイト以内の文字列で入力してください。
- 名称の先頭に「@」は指定できません。
- フォルダは 10 階層まで作成できます。
- 最上位の「ユーザ作成のフォルダ」配下には，ツリー項目を 4,096 個まで作成できます。
- （フォルダ名の場合）名称中に「¥」は使用できません。

［削除］ボタン

選択したツリー項目を削除します。フォルダを選択した場合，フォルダの下の項目すべてが削除対象になります。集計パターンを削除すると，連動して統計パターンも削除されます。

11.11　パターン保存画面

パターン保存画面は，新規の検索パターンまたは集計パターンを保存するときに使用します。監査ログ検索画面または監査ログ集計画面で，新規のパターン名を指定して［保存］ボタンをクリックすると表示されます。パターン保存画面の各部の名称と使い方を説明します。

図 11-18　パターン保存画面の名称

パターン名

新規に保存するパターン名を表示します。パターン保存画面ではパターン名は非活性で表示され，編集できません。

機能ツリー表示領域

パターンの保存場所をツリー項目として表示します。ルートおよびテンプレートのフォルダは保存場所として指定できません。

［保存］ボタン

指定したツリー項目の直下にパターンを保存します。保存されたパターンは，ユーザ作成のパターンとして「検索パターン名」または「集計パターン名」のリストおよび機能ツリーに追加されます。

［閉じる］ボタン

パターン保存画面を閉じます。

11.12　検索パターンおよび集計パターンの一覧

監査ログ検索画面および監査ログ集計画面には，あらかじめ登録されているテンプレートの検索パターンおよび集計パターンがあります。

ここでは，テンプレートの検索パターンおよび集計パターンの一覧と用途を説明します。なお，プルダウンメニューでは，テンプレートの検索パターン名および集計パターン名の先頭に「@」が表示されます。

11.12.1　テンプレートとして登録されている検索パターンおよび集計パターン一覧

次の監査ログ収集対象プログラムについて，あらかじめ登録されているテンプレートの検索パターンおよび集計パターンがあります。

- Collaboration
- Cosminexus
- HiRDB
- Hitachi Navigation Platform
- Hitachi Storage Command Suite
- JP1/AJS2
- JP1/AJS3
- JP1/AO
- JP1/Audit
- JP1/Base
- JP1/IM - NP
- JP1/IM - SS
- JP1/ITDM
- JP1/ITDM2
- JP1/ITRM
- JP1/NETM/AIM
- JP1/NETM/CSC
- JP1/NETM/DM
- JP1/NETM/NM
- JP1/PFM
- JP1/秘文

- OpenTP1
- Oracle
- TRUST E2
- uCosminexus EUR Server
- uCosminexus Navigation Platform
- uCosminexus Portal Framework
- UNIX
- Windows
- XDM/BASE E2
- 活文 NAVIstaff

各収集対象プログラムのテンプレートの検索パターンおよび集計パターンの一覧を，次に示します。

(1) Collaboration のテンプレートの検索パターンおよび集計パターン

表 11-3 Collaboration のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Collaboration ファイル共有-フォルダアクセス権更新監査	指定した期間にファイル共有でアクセス権を更新したフォルダを検出します。
2	@Collaboration ファイル共有-ファイルアクセス権更新監査	指定した期間にファイル共有でアクセス権を更新したファイルを検出します。
3	@Collaboration ファイル共有-フォルダアクセス権参照監査	指定した期間にファイル共有でアクセス権を参照したフォルダを検出します。
4	@Collaboration ファイル共有-ファイルアクセス権参照監査	指定した期間にファイル共有でアクセス権を参照したファイルを検出します。
5	@Collaboration ファイル共有-フォルダ開く監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で開いたフォルダを検出します。
6	@Collaboration ファイル共有-ファイル開く監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で開いたファイルを検出します。
7	@Collaboration ファイル共有-フォルダ作成監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で作成したフォルダを検出します。
8	@Collaboration ファイル共有-ファイル登録監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で新規登録したファイルを検出します。
9	@Collaboration ファイル共有-ファイル更新監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で更新したファイルを検出します。
10	@Collaboration ファイル共有-フォルダ削除監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で削除したフォルダを検出します。

項番	パターン名	用途
11	@Collaboration ファイル共有-ファイル削除監査(Web フォルダ)	指定した期間にファイル共有（Web フォルダ)で削除したファイルを検出します。
12	@Collaboration ファイル共有-フォルダ開く監査	指定した期間にファイル共有で開いたフォルダを検出します。
13	@Collaboration ファイル共有-ファイル開く監査	指定した期間にファイル共有で開いたファイルを検出します。
14	@Collaboration ファイル共有-フォルダ作成監査	指定した期間にファイル共有で作成したフォルダを検出します。
15	@Collaboration ファイル共有-ファイル登録監査	指定した期間にファイル共有で新規登録したファイルを検出します。
16	@Collaboration ファイル共有-ファイル更新監査	指定した期間にファイル共有で更新したファイルを検出します。
17	@Collaboration ファイル共有-フォルダ削除監査	指定した期間にファイル共有で削除したフォルダを検出します。
18	@Collaboration ファイル共有-ファイル削除監査	指定した期間にファイル共有で削除したファイルを検出します。
19	@Collaboration ファイル共有-コマンド実行監査	指定した期間にファイル共有で実行した運用コマンドを検出します。
20	@Collaboration メール-グループ宛先台帳作成監査	指定した期間に宛先台帳で作成したグループ宛先台帳を検出します。
21	@Collaboration メール-グループ宛先台帳削除監査	指定した期間に宛先台帳で削除したグループ宛先台帳を検出します。
22	@Collaboration メール-グループ宛先台帳更新監査	指定した期間に宛先台帳で更新したグループ宛先台帳を検出します。
23	@Collaboration メール-メール送信監査	指定した期間に送信したメールを検出します。
24	@Collaboration メール-受信メール参照監査	指定した期間に参照した受信メールを検出します。
25	@Collaboration スケジュール-スケジュール予約監査	指定した期間にスケジュールで予約したスケジュールを検出します。
26	@Collaboration スケジュール-スケジュール削除監査	指定した期間にスケジュールで削除した予約スケジュールを検出します。
27	@Collaboration スケジュール-スケジュール更新監査	指定した期間にスケジュールで更新した予約スケジュールを検出します。
28	@Collaboration スケジュール-スケジュール参照監査	指定した期間にスケジュールで参照した予約スケジュールを検出します。
29	@Collaboration スケジュール-施設情報登録監査	指定した期間にスケジュールで施設情報を登録した施設を検出します。
30	@Collaboration スケジュール-施設情報削除監査	指定した期間にスケジュールで施設情報を削除した施設を検出します。
31	@Collaboration ＴｏＤｏ-タスク登録監査	指定した期間にＴｏＤｏで登録したタスクを検出します。
32	@Collaboration ＴｏＤｏ-タスク削除監査	指定した期間にＴｏＤｏで削除したタスクを検出します。
33	@Collaboration ＴｏＤｏ-タスク更新監査	指定した期間にＴｏＤｏで更新したタスクを検出します。

項番	パターン名	用途
34	@Collaboration 電子会議室-議題・発言作成監査	指定した期間に電子会議室で作成した議題および発言を検出します。
35	@Collaboration 電子会議室-議題・発言参照監査	指定した期間に電子会議室で参照した議題および発言を検出します。
36	@Collaboration 電子会議室-添付ファイルダウンロード監査	指定した期間に電子会議室でダウンロードした添付ファイルを検出します。
37	@Collaboration 電子会議室-コマンド実行監査	指定した期間に電子会議室で実行した運用コマンドを検出します。
38	@Collaboration 電子掲示板-記事作成監査	指定した期間に電子掲示板で作成または追記した記事を検出します。
39	@Collaboration 電子掲示板-記事編集監査	指定した期間に電子掲示板で編集した記事を検出します。
40	@Collaboration 電子掲示板-記事参照監査	指定した期間に電子掲示板で参照した記事を検出します。
41	@Collaboration 電子掲示板-添付ファイルダウンロード監査	指定した期間に電子掲示板でダウンロードした添付ファイルを検出します。
42	@Collaboration 電子掲示板-コマンド実行監査	指定した期間に電子掲示板で実行した運用コマンドを検出します。
43	@Collaboration コミュニティ管理-コミュニティ作成監査	指定した期間にコミュニティ管理で作成したコミュニティを検出します。
44	@Collaboration コミュニティ管理-コミュニティ更新監査	指定した期間にコミュニティ管理で更新したコミュニティを検出します。
45	@Collaboration コミュニティ管理-コミュニティ削除監査	指定した期間にコミュニティ管理で削除したコミュニティを検出します。
46	@Collaboration コミュニティ管理-コマンド実行監査	指定した期間にコミュニティ管理で実行したコマンドを検出します。

(2) Cosminexus のテンプレートの検索パターンおよび集計パターン

表 11-4 Cosminexus のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Cosminexus コマンド実行監査	指定した期間に実行したコマンドを検出します。

(3) HiRDB のテンプレートの検索パターンおよび集計パターン

表 11-5 HiRDB のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@HiRDB 権限付与監査	指定した期間に実行した権限付与を検出します。
2	@HiRDB ログイン失敗監査	指定した期間でログインに失敗しているユーザを検出します。

(4) Hitachi Storage Command Suite のテンプレートの検索パターンおよび集計パターン

表 11-6 Hitachi Storage Command Suite のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Hitachi Storage Command Suite ユーザ作成監査	指定した期間に作成されたユーザを検出します。
2	@Hitachi Storage Command Suite ユーザログイン成功監査	指定した期間にログインしたユーザを検出します。

(5) JP1/AJS2 のテンプレートの検索パターンおよび集計パターン

表 11-7 JP1/AJS2 のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/AJS2-SO 接続監査	指定した期間に JP1/AJS2 - SO に接続したホストを検出します。
2	@JP1/AJS2-View 接続監査	指定した期間に JP1/AJS2 - View に接続したホストを検出します。
3	@JP1/AJS2 サスペンド/サスペンド解除ジョブネット監査	指定した期間にサスペンド／サスペンド解除されたジョブネットを検出します。
4	@JP1/AJS2 一時変更ジョブネット監査	指定した期間に一時変更されたジョブネットを検出します。
5	@JP1/AJS2 強制終了ジョブネット監査	指定した期間に強制終了されたジョブネットを検出します。
6	@JP1/AJS2 再実行ジョブネット監査	指定した期間に再実行されたジョブネットを検出します。
7	@JP1/AJS2 実行中断ジョブネット監査	指定した期間に実行中断されたジョブネットを検出します。
8	@JP1/AJS2 登録ジョブネット監査	指定した期間に登録されたジョブネットを検出します。
9	@JP1/AJS2 登録取り消しジョブネット監査	指定した期間に登録が取り消されたジョブネットを検出します。

(6) JP1/AJS3 のテンプレートの検索パターンおよび集計パターン

表 11-8 JP1/AJS3 のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/AJS2-SO 接続監査（JP1/AJS3）	指定した期間に JP1/AJS2 - SO に接続したホストを検出します。
2	@JP1/AJS3-View 接続監査	指定した期間に JP1/AJS3 - View に接続したホストを検出します。
3	@JP1/AJS3 サスペンド／サスペンド解除ジョブネット監査	指定した期間にサスペンド／サスペンド解除されたジョブネットを検出します。

項番	パターン名	用途
4	@JP1/AJS3 一時変更ジョブネット監査	指定した期間に一時変更されたジョブネットを検出します。
5	@JP1/AJS3 強制終了ジョブネット監査	指定した期間に強制終了されたジョブネットを検出します。
6	@JP1/AJS3 再実行ジョブネット監査	指定した期間に再実行されたジョブネットを検出します。
7	@JP1/AJS3 実行中断ジョブネット監査	指定した期間に実行中断されたジョブネットを検出します。
8	@JP1/AJS3 登録ジョブネット監査	指定した期間に登録されたジョブネットを検出します。
9	@JP1/AJS3 登録取り消しジョブネット監査	指定した期間に登録が取り消されたジョブネットを検出します。

(7) JP1/AO のテンプレートの検索パターンおよび集計パターン

表 11-9 JP1/AO のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/AO ログイン認証監査	指定した期間の AO へのログイン操作を抽出します。
2	@JP1/AO システム管理の更新操作監査	指定した期間の AO システム管理情報への更新操作を抽出します。
3	@JP1/AO 構成管理情報の更新操作監査	指定した期間の AO 構成管理情報への更新操作を抽出します。

(8) JP1/Audit のテンプレートの検索パターンおよび集計パターン

表 11-10 JP1/Audit のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/NETM/Audit バックアップ監査	指定した期間に実行したバックアップを検出します。
2	@JP1/NETM/Audit ログイン監査	指定した期間にログインしたユーザを検出します。

(9) JP1/Base のテンプレートの検索パターンおよび集計パターン

表 11-11 JP1/Base のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/Base パスワード監査	期間内にパスワード変更されていることを検出します。
2	@JP1/Base ユーザ作成監査－ユーザ	指定したユーザが作成されていることを検出します。
3	@JP1/Base ユーザ作成監査－期間	指定した期間に作成されたユーザを検出します。
4	@JP1/Base ユーザ削除監査－期間	指定した期間に削除されたユーザを検出します。
5	@JP1/Base ユーザ変更監査－期間	指定した期間に変更されたユーザを検出します。

項番	パターン名	用途
6	@JP1/Base 権限レベル監査	不要な権限レベルが割り当てられていないか，必要な権限レベルが割り当てられているかを検出します。
7	@JP1/Base 資源グループ監査	不要な資源グループが割り当てられていないか，必要な資源グループが割り当てられているかを検出します。
8	@JP1/Base 不要ユーザ削除監査	不要となったユーザが削除されていることを検出します。

(10) JP1/IM - NP のテンプレートの検索パターンおよび集計パターン

表 11–12 JP1/IM - NP のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/IM-NP ログイン監査	指定した期間の IM - NP へのログイン操作を抽出します。
2	@JP1/IM-NP ログアウト監査	指定した期間の IM - NP からのログアウト操作を抽出します。
3	@JP1/IM-NP 業務手順の実行監査	指定した期間の IM - NP の業務手順の実行操作を抽出します。

(11) JP1/IM - SS のテンプレートの検索パターンおよび集計パターン

表 11–13 JP1/IM - SS のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/IM-SS 案件作成	指定した期間に作成された案件一覧を抽出します。
2	@JP1/IM-SS 案件編集	指定した期間に編集された案件一覧を抽出します。
3	@JP1/IM-SS 案件削除	指定した期間に削除された案件一覧を抽出します。
4	@JP1/IM-SS 案件エスカレーション	指定した期間にエスカレーションされた案件一覧を抽出します。
5	@JP1/IM-SS 案件操作履歴	指定した案件の操作履歴を抽出します。

(12) JP1/ITDM のテンプレートの検索パターンおよび集計パターン

表 11–14 JP1/ITDM のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/ITDM ログイン成功監査	指定した期間のログイン成功一覧を抽出します。
2	@JP1/ITDM ログイン失敗監査	指定した期間のログイン失敗一覧を抽出します。
3	@JP1/ITDM セットアップ監査	指定した期間に行われたセットアップを抽出します。
4	@JP1/ITDM セキュリティポリシー更新監査	指定した期間に成功したセキュリティポリシー更新を抽出します。

(13) JP1/ITDM2 のテンプレートの検索パターンおよび集計パターン

表 11-15 JP1/ITDM2 のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/ITDM2 ログイン成功監査	指定した期間に成功したログインを抽出します。
2	@JP1/ITDM2 ログイン失敗監査	指定した期間に失敗したログインを抽出します。
3	@JP1/ITDM2 配布管理ログイン監査	指定した期間に配布管理（リモートインストールマネージャ，パッケージャ）にログインしたユーザ一覧を抽出します。
4	@JP1/ITDM2AssetConsole ログイン認証監査	指定した期間の AssetConsole へのログイン操作を抽出します。
5	@JP1/ITDM2 セットアップ監査	指定した期間に行われたセットアップを抽出します。
6	@JP1/ITDM2 セキュリティポリシー更新監査	指定した期間に成功したセキュリティポリシー更新を抽出します。
7	@JP1/ITDM2AssetConsole セットアップ実行監査	指定した期間の AssetConsole のセットアップ実行操作を抽出します。
8	@JP1/ITDM2AssetConsole システム管理・定義情報の更新操作監査	指定した期間の AssetConsole システム管理およびシステム定義カテゴリ関連情報への更新操作を抽出します。
9	@JP1/ITDM2AssetConsole 構成管理情報の更新操作監査	指定した期間の AssetConsole 資産管理情報への更新操作を抽出します。
10	@JP1/ITDM2 登録パッケージ監査	指定した期間にソフトウェアパッケージャからソフトウェアをパッケージングした一覧を抽出します。
11	@JP1/ITDM2 再実行ジョブ監査	指定した期間に再実行されたジョブの一覧を抽出します。
12	@JP1/ITDM2 実行ジョブ監査	指定した期間に実行されたジョブの一覧を抽出します。
13	@JP1/ITDM2 実行ジョブ成功監査	指定した期間に正常に実行されたジョブの一覧を抽出します。
14	@JP1/ITDM2 実行ジョブ失敗監査	指定した期間に失敗したジョブの一覧を抽出します。

(14) JP1/ITRM のテンプレートの検索パターンおよび集計パターン

表 11-16 JP1/ITRM のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/ITRM ログイン成功監査	指定した期間にログインしたユーザを抽出します。
2	@JP1/ITRM ログイン失敗監査	指定した期間にログインに失敗したユーザを抽出します。
3	@JP1/ITRM サービス起動監査	指定した期間の起動履歴を抽出します。

(15) JP1/NETM/AIM のテンプレートの検索パターンおよび集計パターン

表 11-17 JP1/NETM/AIM のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/NETM/AIM ログイン認証監査	指定した期間の JP1/NETM/AIM へのログイン操作を抽出します。
2	@JP1/NETM/AIM セットアップ実行監査	指定した期間の JP1/NETM/AIM のセットアップ実行操作を抽出します。
3	@JP1/NETM/AIM システム管理・定義情報の更新操作監査	指定した期間の JP1/NETM/AIM システム管理およびシステム定義カテゴリ関連情報への更新操作を抽出します。
4	@JP1/NETM/AIM 構成管理情報の更新操作監査	指定した期間の JP1/NETM/AIM 資産管理情報への更新操作を抽出します。

(16) JP1/NETM/CSC のテンプレートの検索パターンおよび集計パターン

表 11-18 JP1/NETM/CSC のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/NETM/CSC ネットワーク制御監査	指定した期間に実行したネットワーク制御を検出します。
2	@JP1/NETM/CSC ポリシー監査	指定した期間に実行したポリシー変更を検出します。
3	@JP1/NETM/CSC ログイン監査	指定した期間にログインしたユーザを検出します。
4	@JP1/NETM/CSC 判定・アクション監査	指定した期間に実行した判定・アクションを検出します。

(17) JP1/NETM/DM のテンプレートの検索パターンおよび集計パターン

表 11-19 JP1/NETM/DM のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/NETM/DM ログイン監査	指定した期間に JP1/NETM/DM システムにログインしたユーザを検出します。
2	@JP1/NETM/DM 再実行ジョブ監査	指定した期間に再実行されたジョブを検出します。
3	@JP1/NETM/DM 実行ジョブ監査	指定した期間に実行されたジョブを検出します。
4	@JP1/NETM/DM 実行ジョブ失敗監査	指定した期間に失敗したジョブを検出します。
5	@JP1/NETM/DM 実行ジョブ成功監査	指定した期間に正常に実行されたジョブを検出します。
6	@JP1/NETM/DM 登録パッケージ監査	指定した期間にパッケージングしたパッケージを検出します。

(18) JP1/NETM/NM のテンプレートの検索パターンおよび集計パターン

表 11-20 JP1/NETM/NM のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/NETM/NM ログイン監査	指定した期間にログインしたユーザを抽出します。
2	@JP1/NETM/NM 許可機器一覧編集監査	指定した期間に許可機器一覧に対して，追加または削除された MAC アドレスを抽出します。
3	@JP1/NETM/NM 固定機器一覧編集監査	指定した期間に固定機器一覧に対して，追加または削除された MAC アドレスを抽出します。

(19) JP1/PFM のテンプレートの検索パターンおよび集計パターン

表 11-21 JP1/PFM のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/PFM アラームアンバインド監査	指定した期間にアンバインドされたアラームを検出します。
2	@JP1/PFM アラームバインド監査	指定した期間にバインドされたアラームを検出します。
3	@JP1/PFM アラーム監査	指定した期間に発生したシステム負荷を検出します。
4	@JP1/PFM アラーム更新監査	指定した期間に更新されたアラーム・アクション定義を検出します。
5	@JP1/PFM アラーム作成監査	指定した期間に作成されたアラーム・アクション定義を検出します。
6	@JP1/PFM アラーム削除監査	指定した期間に削除されたアラーム・アクション定義を検出します。
7	@JP1/PFM アラーム無効化監査	指定した期間に無効化されたアラーム・アクション定義を検出します。
8	@JP1/PFM アラーム有効化監査	指定した期間に有効化されたアラーム・アクション定義を検出します。
9	@JP1/PFM パスワード監査	期間内にパスワードが変更されていることを検出します。
10	@JP1/PFM ユーザ作成監査－ユーザ	指定したユーザが作成されていることを検出します。
11	@JP1/PFM ユーザ作成監査－期間	指定した期間に作成されたユーザを検出します。
12	@JP1/PFM ユーザ削除監査－ユーザ	指定した不要となったユーザが削除されていることを検出します。
13	@JP1/PFM ユーザ削除監査－期間	指定した期間に変更されたユーザを検出します。
14	@JP1/PFM ユーザ変更監査－期間	指定した期間に変更されたユーザを検出します。
15	@JP1/PFM ログイン監査－ユーザ	指定したユーザがログインしていることを検出します。

項番	パターン名	用途
16	@JP1/PFM ログイン監査－一覧	指定した期間にログインしていたユーザを検出します。
17	@JP1/PFM ログイン失敗監査	指定した期間でログインに失敗しているユーザを検出します。

(20) JP1/秘文のテンプレートの検索パターンおよび集計パターン

表 11-22 JP1/秘文のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@JP1/秘文 Advanced Edition 管理サーバ操作監査	指定した期間に管理者が実施した管理サーバでの操作を検出します。
2	@JP1/秘文 Advanced Edition 操作監査	指定した期間に管理者が実施した操作を検出します。
3	@JP1/秘文 Advanced Edition ファイルサーバ操作監査	指定した期間に管理者が実施したファイルサーバでの操作を検出します。
4	@JP1/秘文 Advanced Edition ログサーバ操作監査	指定した期間に管理者が実施したログサーバでの操作を検出します。

(21) OpenTP1 のテンプレートの検索パターンおよび集計パターン

表 11-23 OpenTP1 のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@OpenTP1 クライアントユーザ認証成功監査	指定した期間に認証に成功したクライアントユーザを検出します。
2	@OpenTP1 クライアントユーザ認証失敗監査	指定した期間に認証に失敗したクライアントユーザを検出します。
3	@OpenTP1 開始監査	指定した期間に開始した OpenTP1 を検出します。
4	@OpenTP1 待機監査	指定した期間に待機状態になった OpenTP1 を検出します。
5	@OpenTP1 正常終了監査	指定した期間に正常終了した OpenTP1 を検出します。
6	@OpenTP1 異常終了監査	指定した期間に異常終了した OpenTP1 を検出します。
7	@OpenTP1 プロセスサービス重大エラー監査	指定した期間にプロセスサービスの重大エラーが発生した OpenTP1 を検出します。
8	@OpenTP1 不正電文破棄監査	指定した期間に不正電文を破棄したかどうかを検出します。
9	@OpenTP1rap 不正電文破棄監査	指定した期間に rap が不正電文を破棄したかどうかを検出します。
10	@OpenTP1 コマンド実行監査	指定した期間に実行したコマンドを検出します。

(22) Oracle のテンプレートの検索パターンおよび集計パターン

表 11-24 Oracle のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Oracle CREATE ROLE 監査	指定した期間に実行した権限作成を検出します。
2	@Oracle CREATE USER 監査	指定した期間に実行したユーザ作成を検出します。
3	@Oracle LOGON 監査	指定した期間に実行したログオンを検出します。

(23) TRUST E2 のテンプレートの検索パターンおよび集計パターン

表 11-25 TRUST E2 のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@VOS3/TRUST ＤＡＳＤボリュームアクセス監査	DASD ボリュームアクセス事象を検出します。
2	@VOS3/TRUST ＩＦＩＴでのデータセットアクセス監査	IFIT コマンドによるデータセットアクセス事象を検出します。
3	@VOS3/TRUST ＴＲＵＳＴ環境監査	TRUST 環境操作事象を検出します。
4	@VOS3/TRUST アクセス失敗監査	アクセス失敗の事象を検出します。
5	@VOS3/TRUST サスペンドユーザ監査	サスペンド状態になったユーザを検出します。
6	@VOS3/TRUST システム利用監査	システム利用開始終了事象を検出します。
7	@VOS3/TRUST データセットアクセス監査	データセットアクセス事象を検出します。
8	@VOS3/TRUST 特定ユーザによる操作監査	特定ユーザによる操作の事象を検出します。
9	@VOS3/TRUST 特定リソースに対する操作監査	特定リソースに対する操作の事象を検出します。
10	@VOS3/TRUST パスワード変更監査	本人によるパスワード変更事象を検出します。
11	@VOS3/TRUST 保護情報操作監査	保護情報操作事象を検出します。

(24) uCosminexus Navigation Platform のテンプレートの検索パターンおよび集計パターン

表 11-26 uCosminexus Navigation Platform のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Cosminexus Navigation Platform ログイン監査	指定した期間の uCosminexus Navigation Platform へのログイン操作を抽出します。

項番	パターン名	用途
2	@Cosminexus Navigation Platform ログアウト監査	指定した期間の Cosminexus Navigation Platform からのログアウト操作を抽出します。
3	@Cosminexus Navigation Platform 業務手順の実行監査	指定した期間の Cosminexus Navigation Platform の業務手順の実行操作を抽出します。

(25) uCosminexus Portal Framework のテンプレートの検索パターンおよび集計パターン

表 11-27 uCosminexus Portal Framework のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Cosminexus Portal Framework 新規ユーザ作成監査	指定した期間に新規ユーザを作成したユーザを抽出します。
2	@Cosminexus Portal Framework ユーザ情報変更監査	指定した期間にユーザ情報を変更したユーザを抽出します。
3	@Cosminexus Portal Framework ユーザ削除監査	指定した期間にユーザを削除したユーザを抽出します。
4	@Cosminexus Portal Framework 管理者条件編集監査	指定した期間に管理者条件を編集したユーザを抽出します。
5	@Cosminexus Portal Framework 利用者条件編集監査	指定した期間に利用者条件を編集したユーザを抽出します。
6	@Cosminexus Portal Framework ログイン監査	指定した期間にログインしたユーザを抽出します。
7	@Cosminexus Portal Framework ログアウト監査	指定した期間にログアウトしたユーザを抽出します。

(26) UNIX のテンプレートの検索パターンおよび集計パターン

UNIX のテンプレートの検索パターンおよび集計パターンを次に示します。

- AIX
- HP-UX
- Linux
- Solaris

(a) AIX のテンプレートの検索パターンおよび集計パターン

表 11–28 AIX のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@AIX su コマンド監査	指定した期間に実行した su コマンドを検出します。
2	@AIX su コマンド失敗監査	指定した期間に実行に失敗した su コマンドを検出します。
3	@AIX ログアウト監査	指定した期間にログアウトしたユーザを検出します。
4	@AIX ログイン監査	指定した期間にログインしたユーザを検出します。
5	@AIX ログイン失敗監査	指定した期間にログインに失敗しているユーザを検出します。

(b) HP-UX のテンプレートの検索パターンおよび集計パターン

表 11–29 HP-UX のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@HP-UX su コマンド監査	指定した期間に実行した su コマンドを検出します。
2	@HP-UX su コマンド失敗監査	指定した期間に実行に失敗した su コマンドを検出します。
3	@HP-UX ログアウト監査	指定した期間にログアウトしたユーザを検出します。
4	@HP-UX ログイン監査	指定した期間にログインしたユーザを検出します。
5	@HP-UX ログイン失敗監査	指定した期間にログインに失敗しているユーザを検出します。

(c) Linux のテンプレートの検索パターンおよび集計パターン

表 11–30 Linux のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Linux su コマンド監査	指定した期間に実行した su コマンドを検出します。
2	@Linux su コマンド失敗監査	指定した期間に実行に失敗した su コマンドを検出します。
3	@Linux ログアウト監査	指定した期間にログアウトしたユーザを検出します。
4	@Linux ログイン監査	指定した期間にログインしたユーザを検出します。
5	@Linux ログイン失敗監査	指定した期間にログインに失敗しているユーザを検出します。

(d) Solaris のテンプレートの検索パターンおよび集計パターン

表 11–31 Solaris のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Solaris su コマンド監査	指定した期間に実行した su コマンドを検出します。
2	@Solaris su コマンド失敗監査	指定した期間に実行に失敗した su コマンドを検出します。

項番	パターン名	用途
3	@Solaris ログアウト監査	指定した期間にログアウトしたユーザを検出します。
4	@Solaris ログイン監査	指定した期間にログインしたユーザを検出します。
5	@Solaris ログイン失敗監査	指定した期間にログインに失敗しているユーザを検出します。

(27) Windows のテンプレートの検索パターンおよび集計パターン

表 11-32 Windows のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Windows グローバルグループ作成監査	指定したユーザ権限グループが作成されているかどうかを検出します。
2	@Windows グローバルグループ作成監査（Windows Server 2008）	
3	@Windows パスワード監査	期間内にパスワード変更されていることを検出します。
4	@Windows パスワード監査（Windows Server 2008）	
5	@Windows ユーザ作成監査－ユーザ	指定したユーザが作成されていることを検出します。
6	@Windows ユーザ作成監査－ユーザ（Windows Server 2008）	
7	@Windows ユーザ作成監査－期間	指定した期間に作成されたユーザを検出します。
8	@Windows ユーザ作成監査－期間（Windows Server 2008）	
9	@Windows ユーザ削除監査－期間	指定した期間に削除されたユーザを検出します。
10	@Windows ユーザ削除監査－期間（Windows Server 2008）	
11	@Windows ユーザ変更監査－期間	指定した期間に変更されたユーザを検出します。
12	@Windows ローカルグループ作成監査	指定したユーザ権限グループが作成されているかどうかを検出します。
13	@Windows ローカルグループ作成監査（Windows Server 2008）	
14	@Windows ログイン監査－ユーザ	指定したユーザがログインしていることを検出します。
15	@Windows ログイン監査－一覧	指定した期間にログインしていたユーザを検出します。
16	@Windows ログイン監査－許可時間	許可時間以上ログインしているユーザがいないことを検出します。
17	@Windows ログイン失敗監査	一定期間内に指定した回数よりも多くログインに失敗しているユーザを検出します。
18	@Windows ロックアウト監査	指定した期間にロックアウトされたユーザを検出します。

項番	パターン名	用途
19	@Windows ロックアウト監査（Windows Server 2008）	
20	@Windows 不要グローバルグループ削除監査	不要となったユーザ権限グループが削除されていることを検出します。
21	@Windows 不要グローバルグループ削除監査（Windows Server 2008）	
22	@Windows 不要ユーザ削除監査	不要となったユーザが削除されていることを検出します。
23	@Windows 不要ユーザ削除監査（Windows Server 2008）	
24	@Windows 不要ローカルグループ削除監査	不要となったユーザ権限グループが削除されていることを検出します。
25	@Windows 不要ローカルグループ削除監査（Windows Server 2008）	
26	@Windows ユニバーサルグループ作成監査（Windows Server 2008）	指定したユーザ権限グループが作成されているかどうかを検出します。
27	@Windows 不要ユニバーサルグループ削除監査（Windows Server 2008）	不要となったユーザ権限グループが削除されていることを検出します。

(28) XDM/BASE E2 のテンプレートの検索パターンおよび集計パターン

表 11-33 XDM/BASE E2 のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@XDM アクセス情報監査	指定した期間に取得したアクセス情報を検出します。
2	@XDM 仮想端末名称監査	指定した期間に取得した仮想端末名称を検出します。
3	@XDM 監査ユーザＩＤ監査	指定した期間に設定・変更した監査ユーザ ID を検出します。
4	@XDM 重要情報のアクセス監査	指定した期間に重要情報にアクセスした一覧を検出します。
5	@XDM 動作情報監査	指定した期間に取得した動作情報を検出します。
6	@XDM 判定した権限監査(XDM/RD)	指定した期間に判定した権限を検出します（XDM/RD）。
7	@XDM ポート番号監査(XDM/DCCM3)	指定した期間に取得したポート番号を検出します（XDM/DCCM3）。

(29) 活文 NAVIstaff のテンプレートの検索パターンおよび集計パターン

表 11-34 活文 NAVIstaff のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@活文 NAVIstaff 失効監査	指定した期間のドキュメントの失効を検出します。
2	@活文 NAVIstaff ドキュメント印刷監査	指定した期間にあるドキュメントを印刷した操作を検出します。
3	@活文 NAVIstaff ドキュメント閲覧監査	指定した期間にあるドキュメントを閲覧した操作を検出します。
4	@活文 NAVIstaff ドキュメント操作監査	指定した期間にあるドキュメントの操作を検出します。
5	@活文 NAVIstaff 保護監査	指定した期間にドキュメントを保護した操作を検出します。
6	@活文 NAVIstaff ログイン失敗監査	指定した期間にログインに失敗した操作を検出します。

(30) Hitachi Navigation Platform のテンプレートの検索パターンおよび集計パターン

表 11-35 Hitachi Navigation Platform のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@Hitachi Navigation Platform ログイン監査	指定した期間の Hitachi Navigation Platform へのログイン操作を抽出します。
2	@Hitachi Navigation Platform ログアウト監査	指定した期間の Hitachi Navigation Platform からのログアウト操作を抽出します。
3	@Hitachi Navigation Platform 業務手順の実行監査	指定した期間の Hitachi Navigation Platform の業務手順の実行操作を抽出します。

(31) uCosminexus EUR Server のテンプレートの検索パターンおよび集計パターン

表 11-36 uCosminexus EUR Server のテンプレートとして登録されている検索パターンおよび集計パターン一覧

項番	パターン名	用途
1	@uCosminexus EUR Server 帳票のスプール監査	指定した期間にスプールした帳票の一覧を抽出します。
2	@uCosminexus EUR Server スプールデータのユーザ操作監査	指定したユーザが操作したスプールデータの一覧を抽出します。
3	@uCosminexus EUR Server スプールデータの印刷監査	指定した期間に印刷したスプールデータ一覧を抽出します。

項番	パターン名	用途
4	@uCosminexus EUR Server Spool Service 起動	Spool Service の起動を抽出します。
5	@uCosminexus EUR Server Spool Service 停止	Spool Service の停止を抽出します。

12 コマンド

この章では，監査証跡管理システムのコマンドについて説明します。

コマンド一覧

監査ログ管理サーバ，監査ログ閲覧サーバ，および監査ログ収集対象サーバで使用できるコマンドの一覧を示します。

監査ログ管理サーバおよび監査ログ閲覧サーバのコマンド一覧

監査ログ管理サーバおよび監査ログ閲覧サーバで使用できるコマンドの一覧を次の表に示します。

表 12-1　監査ログ管理サーバおよび監査ログ閲覧サーバで使用できるコマンド一覧

項番	分類	コマンド名	機能
1	データベースの運用管理	admdbbackup	データベースのバックアップを取得します。
2		admdbdelete	指定した日時までに出力された監査ログをデータベースから削除します。
3		admdbexport	データベースに格納されているすべてのデータを CSV 形式でバックアップします。
4		admdbimport	データベースの CSV バックアップで取得した CSV 形式のデータから，データベースを復元します。
5		admdbrorg	データベースを再編成します。
6		admdbstat	データベースの使用状況を確認します。
7		admdbstop	データベースを停止します。 クラスタ環境のシステムで，系の切り替えやシステムの停止に使用するコマンドです。
8	監査ログの運用管理	admcoldata	収集対象として設定されているサーバから監査ログを収集します。
9		admcsvmove	監査ログのバックアップファイルを，指定したパスに移動します。また，バックアップ実行履歴を更新します。
10		admcsvremove	指定した監査ログのバックアップファイルおよびバックアップ実行履歴を削除します。
11		admexport	監査ログを CSV 形式でバックアップします。また，バックアップの実行履歴が監査ログ管理データベースに登録されます。 監査ログは，期間指定または前回からの差分指定でバックアップできます。
12		admimport	admexport コマンドで出力した監査ログのバックアップファイルを監査ログ管理データベースにインポートして，監査ログを閲覧できるようにします。
13	監査ログの統計情報の運用管理	admstdel	監査ログの統計情報を監査ログ管理データベースから削除します。
14		admstgen	監査ログの統計情報を監査ログ管理データベースに生成します。
15	トラブルシュート	admlog.vbs	JP1/Audit Management - Manager でトラブルが発生したときに，保守資料を一括で取得します。

項番	分類	コマンド名	機能
16	正規化ルールの運用管理	admrrexport	正規化ルールエディタで作成した正規化ルールをバックアップします。
17		admrrimport	admrrexport コマンドで出力した正規化ルール定義エクスポートファイルをインポートします。

監査ログ収集対象サーバのコマンド一覧

監査ログ収集対象サーバで使用できるコマンドの一覧を次の表に示します。

表 12–2　監査ログ収集対象サーバで使用できるコマンド一覧

項番	分類	コマンド名	機能
1	監査ログ収集対象サーバのセットアップ	admagtinstall	監査ログ収集対象サーバのセットアップに必要なファイルをインストールまたはアンインストールします。
2		admagtsetup	監査ログ専用イベントサーバの環境を作成または削除します。
3	UNIX システムログ収集	admuxlogcol	監査対象である UNIX のシステムログ情報ファイルを，統一ログフォーマットに変換して，UNIX ログ変換ファイルに出力します。 このコマンドは，監査ログ収集対象の UNIX サーバで使用します。
4	クラスタ環境でのシステムの運用管理	admhasetup	監査ログ収集対象サーバがクラスタ構成の場合に，共有ディスク上の監査ログを監視するための環境を作成または削除します。

コマンドの詳細

ここでは，コマンドの説明形式と説明順序について説明します。

コマンドの説明形式

各コマンドで説明する項目は次のとおりです。ただし，コマンドによっては説明しない項目もあります。

機能

コマンドの機能およびコマンドの実行に必要なユーザの権限について説明しています。

形式

コマンドの形式を説明しています。

コマンドを実行できるサーバ

コマンドを実行できるサーバについて説明しています。

格納先フォルダまたはディレクトリ

コマンドの格納場所について説明しています。

引数

コマンドの引数について説明しています。なお，スペースを含むパスを指定する場合は，「"」で囲んで指定してください。

注意事項

注意事項を説明しています。

戻り値

コマンドの戻り値について説明しています。

なお，コマンド実行時に表示されるメッセージについては「14.3　メッセージ一覧」を参照してください。

コマンドの説明順序

コマンドは，コマンド名のアルファベット順で説明しています。

admagtinstall（監査ログ収集対象サーバのファイルのインストール）

機能

監査ログ収集対象サーバのセットアップに必要なファイルをインストールまたはアンインストールします。Windows 環境では Administrator 権限を持つユーザで実行してください。UNIX 環境ではスーパーユーザ権限を持つユーザで実行してください。

このコマンドを実行してインストールされるファイルの一覧については「付録 A.3　監査ログ収集対象サーバに配布されるファイル一覧」を参照してください。

形式

- Windows の場合

```
admagtinstall {[△-d△インストール先フォルダ] | △-u}
              [△-w△作業用フォルダ]
```

- UNIX の場合

```
admagtinstall [△-u]
              [△-w△作業用ディレクトリ]
```

コマンドを実行できるサーバ

- 監査ログ収集対象サーバ

格納先フォルダまたはディレクトリ

アーカイブファイルの展開先フォルダ（ディレクトリ）

引数

-d△インストール先フォルダ

監査ログ収集対象サーバに必要なファイルのインストール先フォルダをフルパスで指定します。80 バイト以内の文字列で指定してください。使用できる文字を次に示します。

- 半角英数字
- 「△（半角スペース）」，「_」，「.」，「(」，「)」

この引数は，OS が Windows の場合にだけ指定できます。指定したフォルダが存在しない場合は，コマンド実行時に作成されます。この引数を省略した場合，「**システムドライブ**¥Program Files¥Hitachi¥jp1netmaudit¥agent」がインストール先フォルダとして設定されます。

OS が UNIX の場合，この引数は指定できません。/etc/opt/jp1netmaudit/agent がインストール先ディレクトリとして設定されます。

なお，上書きインストール時はこの引数は指定できません。JP1/NETM/Audit - Manager 09-00 より前のバージョンから上書きインストールした場合は，前バージョンのフォルダ構成が引き継がれます。

-u

監査ログ収集対象サーバのセットアップに必要なファイルを削除する場合に指定します。この引数を指定してファイルを削除する場合は，監査ログ収集対象サーバのアンセットアップを実施してから，このコマンドを実行してください。監査ログ収集対象サーバのアンセットアップについては「5.13　監査ログ収集対象の解除」を参照してください。

なお，JP1/NETM/Audit - Manager 09-00 より前のバージョンで手動でコピーしたセットアップファイルも削除の対象となります。ただし，セットアップに必要なファイル以外がフォルダ（ディレクトリ）に存在する場合，フォルダ（ディレクトリ）は削除されません。必要に応じて，手動で削除してください。

-w△作業用フォルダ（作業用ディレクトリ）

このコマンドの実行時に使用する作業用フォルダ（作業用ディレクトリ）をフルパスで指定します。80 バイト以内の文字列で指定してください。この引数を省略した場合，次に示すフォルダ（ディレクトリ）が作業用フォルダ（作業用ディレクトリ）に設定されます。

Windows の場合

　%TEMP%

UNIX の場合

　/tmp

注意事項

- OS が UNIX の場合は，アーカイブファイルを展開したディレクトリに移動してから，このコマンドを実行してください。
- このコマンドを実行する場合は，「JP1/NETM/Audit LogTrap **論理ホスト名**」サービスが停止していることを確認してください。
- 引数の順序は，形式で示している順序には関係なく，任意の順序で指定できます。
- このコマンドを実行すると，実行確認のメッセージが表示されます。実行する場合は Y または y を，中断する場合は N または n を入力してください。Y，N，y，n 以外の値を入力した場合は，Y または N の入力を促すメッセージが表示されます。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにコマンドが実行されています。

戻り値	説明
4	インストールするバージョンより新しいバージョンのファイルが，すでにインストールされています。
5	上書きインストール時，-d オプションは指定できません。
6	指定されたフォルダまたはディレクトリが存在しません。
7	フォルダまたはディレクトリの作成に失敗しました。
8	フォルダまたはディレクトリの削除に失敗しました。
9	ファイルのアクセスでエラーが発生しました。
10	ファイルのコピーに失敗しました。
11	ファイルの削除に失敗しました。
12	インストール用データディレクトリがカレントディレクトリに存在しません。
13	ユーザによってコマンドの実行が中止されました。
14	前提プログラムがインストールされていません。
99	その他のエラーが発生しました。

admagtsetup（監査ログ専用イベントサーバの環境セットアップ）

機能

監査ログ専用イベントサーバの環境を作成または削除します。また，作成済みの監査ログ専用イベントサーバの環境情報を表示します。Windows 環境では Administrator 権限を持つユーザで実行してください。UNIX 環境ではスーパーユーザ権限を持つユーザで実行してください。

なお，このコマンドで監査ログ専用イベントサーバの環境を作成する際，環境情報の指定方法は，次に示す二つの方法があります。

- 各オプションの引数に指定する
- 監査ログ収集対象サーバセットアップ定義ファイルに指定する

形式

- 各オプションの引数に環境情報を指定して監査ログ専用イベントサーバを作成する場合

```
admagtsetup △-h△監査ログ収集対象サーバのホスト名
          [△-c△{online | standby}]
           △-i△監査ログ収集対象サーバのIPアドレス
           △-d△監査ログ専用フォルダ（監査ログ専用ディレクトリ）
          [△-t△転送用ポート番号]
          [△-a△AP用ポート番号]
          [△-s△監査ログ専用イベントデータベースのサイズ]
           △-mh△監査ログ管理サーバのホスト名
           △-mi△監査ログ管理サーバのIPアドレス
          [△-mt△転送用ポート番号]
```

- 監査ログ収集対象サーバセットアップ定義ファイルに環境情報を指定して監査ログ専用イベントサーバを作成する場合

```
admagtsetup △-f△監査ログ収集対象サーバセットアップ定義ファイル名
```

- 監査ログ専用イベントサーバを削除する場合

```
admagtsetup △-h△監査ログ収集対象サーバのホスト名
          [△-c△{online | standby}]
           △-u
```

- 監査ログ専用イベントサーバの環境情報を表示する場合

```
admagtsetup △-v
          [△-h△監査ログ収集対象サーバのホスト名]
```

コマンドを実行できるサーバ

- 監査ログ収集対象サーバ

格納先フォルダまたはディレクトリ

- Windows の場合

  JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき

  任意のインストール先フォルダ※¥bin

  JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき

  システムドライブ¥Program Files¥HITACHI¥jp1netmaudit¥manager¥bin

  注※

  監査ログ収集対象サーバのセットアップに必要なファイルをインストールする際に指定します。監査ログ収集対象サーバのセットアップに必要なファイルのインストールについては「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。

- UNIX の場合

  JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき

  /opt/jp1netmaudit/agent/bin

  JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき

  /opt/jp1netmaudit/manager/bin

引数

-h△監査ログ収集対象サーバのホスト名

監査ログ収集対象サーバのホスト名を指定します。64 バイト以内の文字列で指定してください。使用できる文字を次に示します。

- 半角英数字
- 「-」

-c△{online | standby}

クラスタ環境で論理ホスト用の監査ログ専用イベントサーバを作成または削除する場合に指定します。実行系サーバ上で作成または削除する場合は，「-c online」を指定します。待機系サーバ上で作成または削除する場合は，「-c standby」を指定します。

-i△監査ログ収集対象サーバの IP アドレス

監査ログ収集対象サーバの IP アドレス（IPv4 アドレスまたは IPv6 アドレス）を指定します。IP アドレスの形式については，「指定できる IP アドレスの形式」を参照してください。

-d△監査ログ専用フォルダ（監査ログ専用ディレクトリ）

監査ログ専用フォルダ（監査ログ専用ディレクトリ）をフルパスで指定します。128 バイト以内の文字列で指定してください。指定するフォルダ（ディレクトリ）はコマンド実行前にあらかじめ作成しておいて

ください。クラスタシステムで運用する場合は，共有ディスク上のフォルダ（ディレクトリ）を指定してください。フォルダ（ディレクトリ）名に使用できる文字を次に示します。

- 半角英数字
- 「△(半角スペース)」，「!」，「#」，「$」，「&」，「(」，「)」，「+」，「-」，「,」，「;」，「=」，「@」，「_」，「`」，「{」，「}」，「[」，「]」，「~」，「%」，「^」

この引数で指定した監査ログ専用フォルダ（監査ログ専用ディレクトリ）の配下に，「jp1netmaudit¥event」（「jp1netmaudit/event」）が作成され，監査ログ専用イベントサーバに必要なファイルが生成されます。なお，クラスタ環境で運用する場合は，共有ディスク上の監査ログ専用フォルダ（監査ログ専用ディレクトリ）を指定してください。

-t△転送用ポート番号

監査ログ専用イベントサーバの転送用ポート番号を指定します。監査ログ収集対象サーバで使用されていないポート番号を 5001～65535 の整数で指定してください。この引数を省略した場合は，転送用ポート番号に「24101」が指定されます。

-a△AP 用ポート番号

監査ログ専用イベントサーバの AP 用ポート番号を指定します。監査ログ収集対象サーバで使用されていないポート番号を 5001～65535 の整数で指定してください。この引数を省略した場合は，AP 用ポート番号に「24102」が指定されます。

-s△監査ログ専用イベントデータベースのサイズ

監査ログ専用イベントデータベースのサイズをバイト単位で指定します。10000000～2147483647 の整数で指定してください。この引数を省略した場合は，監査ログ専用イベントデータベースのサイズに「10000000」が指定されます。

-mh△監査ログ管理サーバのホスト名

監査ログ管理サーバのホスト名を指定します。64 バイト以内の文字列で指定してください。使用できる文字を次に示します。

- 半角英数字
- 「-」

-mi△監査ログ管理サーバの IP アドレス

監査ログ管理サーバの IP アドレス（IPv4 アドレスまたは IPv6 アドレス）を指定します。IP アドレスの形式については，「指定できる IP アドレスの形式」を参照してください。

-mt△転送用ポート番号

監査ログ管理サーバ上の JP1/Base のイベントサーバの転送用ポート番号を指定します。監査ログ管理サーバで使用されていないポート番号を 5001～65535 の整数で指定してください。この引数を省略した場合は，JP1/Base のデフォルトの転送用ポート番号「jp1imevt」が指定されます。

-u

監査ログ収集対象サーバから，監査ログ専用イベントサーバの環境を削除する場合に指定します。-u オプションを指定してコマンドを実行すると，実行確認のメッセージが表示されます。実行する場合は Y または y を，中断する場合は N または n を入力してください。Y，N，y，n 以外の値を入力した場合は，Y または N の入力を促すメッセージが表示されます。

監査ログ専用イベントサーバの環境を削除する場合，次に示す操作を実施してから，コマンドを実行してください。

- 対象となる監査ログ収集対象サーバで監視しているプログラムを，監査ログ収集マネージャですべて解除する。
- 対象となる監査ログ収集対象サーバの OS が Windows の場合，「JP1/Base Event **監査ログ専用イベントサーバ名**」サービスを停止する。
- 対象となる監査ログ収集対象サーバの OS が UNIX の場合，削除する監査ログ専用イベントサーバを停止する。

-f△監査ログ収集対象サーバセットアップ定義ファイル名

監査ログ収集対象サーバセットアップ定義ファイル名をフルパスで指定します。255 バイト以内の文字列で指定してください。フォルダ名やファイル名に使用できる文字を次に示します。

- 半角英数字
- 「△(半角スペース)」，「!」，「#」，「$」，「&」，「(」，「)」，「+」，「-」，「,」，「;」，「=」，「@」，「_」，「`」，「{」，「}」，「[」，「]」，「~」，「%」，「^」

指定した監査ログ収集対象サーバセットアップ定義ファイルの定義内容に従って，監査ログ専用イベントサーバの環境が作成されます。監査ログ収集対象サーバセットアップ定義ファイルの詳細については「13.9 監査ログ収集対象サーバセットアップ定義ファイル」を参照してください。

-v

監査ログ専用イベントサーバの環境情報を表示させる場合に指定します。-h オプションを指定している場合は，-h オプションの引数で指定したホストだけを対象として監査ログ専用イベントサーバの環境情報を表示します。-h オプションを省略している場合は，admagtsetup コマンドでセットアップしたすべてのホストを対象として監査ログ専用イベントサーバの環境情報を表示します。

指定できる IP アドレスの形式

-i オプションと-mi オプションに指定できる IP アドレスの形式を次に示します。

IPv4 アドレスの場合

aaa.bbb.ccc.ddd の形式で指定します。aaa～ddd は，最大 3 けたの 10 進数で指定してください。なお，aaa～ddd の先頭の 0 は省略してください。例えば，012 の場合は 12 と指定してください。

IPv6 アドレスの場合

- eeee:ffff:gggg:hhhh:iiii:jjjj:kkkk:llll の形式で指定します。eeee～llll は，最大 4 けたの 16 進数で指定してください。なお，eeee～llll の先頭の 0 は省略してください。例えば，0123 の場合は 123 と指定してください。
- 16 進数の英字部分（a～f）は，大文字と小文字の区別はありません。
- 0000 が一つ以上連続する場合，1 回だけ「::」で省略できます。
- IPv4 互換アドレス（上位 96bit が 0 のアドレス）は指定できません。
- IPv4 射影アドレス（上位 80bit が 0，かつ上位 81bit から 96bit までの 16bit が 1 のアドレス）は指定できません。

注意事項

- 引数の順序は，形式で示している順序には関係なく，任意の順序で指定できます。
- 監査ログ専用イベントサーバの環境を再作成する場合は，すでにある環境を削除してから，このコマンドを実行し，再作成してください。
- -u オプションと-v オプションは，このコマンドによって監査ログ専用イベントサーバの環境を作成した場合にだけ有効となります。手動で環境を作成した場合は，コマンドで環境を削除したり，表示したりすることはできません。
- -i オプションまたは-mi オプションに IPv6 アドレスを指定する場合，JP1/Base が IPv6 アドレスに対応した環境になっている必要があります。IPv6 アドレスに対応した環境になっていない場合は，IPv6 アドレスを指定できません。
- -i オプションと-mi オプションは，同じ形式の IP アドレスを指定してください。IPv4 アドレスと IPv6 アドレスが混在した指定はできません。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにコマンドが実行されています。
4	サービスの登録に失敗しました。
5	サービスの登録削除に失敗しました。
6	コマンドの引数に指定されたフォルダまたはディレクトリは存在しません。
7	フォルダまたはディレクトリの作成に失敗しました。
8	フォルダまたはディレクトリの削除に失敗しました。
9	環境設定ファイルのアクセスでエラーが発生しました。

戻り値	説明
10	すでに環境が設定されています。
11	環境が設定されていないホスト名が指定されました。
12	指定されたフォルダまたはディレクトリは，ほかのホストで使用されています。
13	ユーザによってコマンドの実行が中止されました。
14	前提プログラムがインストールされていません。
15	監査ログ収集対象サーバセットアップ定義ファイルに誤りがあります。
16	監査ログ専用イベントサーバが停止されていません。
17	jp1hosts2 の設定に失敗しました。
99	その他のエラーが発生しました。

admcoldata（監査ログの収集）

機能

収集対象として設定されているサーバから監査ログを収集します。監査ログを即時に収集したいときに実行します。Administrator 権限を持つユーザで実行してください。

形式

```
admcoldata△[-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- このコマンドを実行する前に，JP1/Audit Management - Manager のサービスを起動してください。
- 監査ログ収集マネージャで収集対象サーバを追加後，JP1/Audit Management - Manager のサービスを再起動していない場合，該当するサーバの監査ログは収集されません。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	コマンドがすでに実行されています。
4	ユーザによってコマンド実行が中断されました。
9	JP1/Audit Management - Manager のサービスが停止しています。

戻り値	説明
99	その他のエラーが発生しました。

admcsvmove（監査ログのバックアップファイルの移動）

機能

監査ログのバックアップファイルを，指定したパスに移動します。また，バックアップ実行履歴を更新します。Administrator 権限を持つユーザで実行してください。

形式

```
admcsvmove △-s△移動元ファイル名
           △-d△移動先ファイル名
         [△-f△バックアップオプション定義ファイル名]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-s△移動元ファイル名

移動前の監査ログのバックアップファイル名をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダに格納されている監査ログのバックアップファイルは移動できません。

-d△移動先ファイル名

移動後の監査ログのバックアップファイル名をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダには監査ログのバックアップファイルを移動できません。

-f△バックアップオプション定義ファイル名

バックアップ実行履歴に登録されているバックアップ名称およびコメントを更新したい場合に，バックアップオプション定義ファイル名をフルパスで指定します。

バックアップオプション定義ファイルは，バックアップ名称およびコメントの内容を記述したファイルです。ユーザが作成します。バックアップオプション定義ファイルについては「13.7　バックアップオプション定義ファイル」を参照してください。

この引数を省略した場合，バックアップ実行履歴のバックアップ名称およびコメントは更新されません。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
5	定義ファイルの内容に誤りがあります。
11	移動元の監査ログファイルが存在しません。
12	移動先の監査ログファイルがすでに存在します。
99	その他のエラーが発生しました。

admcsvremove（監査ログのバックアップファイルの削除）

機能

指定した監査ログのバックアップファイルおよびバックアップ実行履歴を削除します。また，バックアップ実行履歴に登録されていて，対応する監査ログのバックアップファイルがない場合，バックアップ実行履歴だけを削除します。Administrator 権限を持つユーザで実行してください。

形式

```
admcsvremove {△-r△バックアップファイル名 | △-n△バックアップID}
             [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-r△バックアップファイル名

削除する監査ログのバックアップファイル名をフルパスで指定します。

ローカルディスク上のパスを指定してください。バックアップデータはネットワークドライブ上のフォルダには格納できません。

-n△バックアップ ID

削除する監査ログのバックアップファイルのバックアップ ID を指定します。バックアップ ID は監査ログ管理画面のバックアップ履歴画面で確認してください。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

戻り値

戻り値	説明
0※	コマンドの処理が正常に終了しました。

戻り値	説明
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
99	その他のエラーが発生しました。

注※

バックアップ実行履歴に登録されていて，対応する監査ログのバックアップファイルがない場合，バックアップ実行履歴だけが削除され，コマンドは正常終了します。

admdbbackup（データベースのバックアップ）

機能

データベースのバックアップを取得します。また，実行結果ファイルに処理結果を出力します。
Administrator 権限を持つユーザで実行してください。

形式

```
admdbbackup △-b△バックアップファイル名
          [△-o△実行結果ファイル名]
          [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-b△バックアップファイル名

取得するバックアップファイル名をフルパスで指定します。

ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダにはバックアップデータを格納できません。また，十分な空き容量のあるディスクのパスを指定してください。

指定したファイルがすでに存在する場合，既存のファイルは上書きされます。また，指定したフォルダが存在しない場合，コマンド実行時に作成されます。

-o△実行結果ファイル名

実行結果ファイル名をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダには実行結果ファイルを格納できません。

実行結果ファイルは，処理の実行結果を出力するためのファイルです。バックアップをいつ取得したかを確認できます。

指定したファイルがすでに存在する場合，既存のファイルは上書きされます。また，指定したフォルダが存在しない場合，コマンド実行時に作成されます。

この引数を省略した場合，JP1/Audit Management - Manager のインストール先フォルダ¥db¥backup¥backup.log が実行結果ファイル名として設定されます。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- このコマンドを実行する前に JP1/Audit Management - Manager のサービスと World Wide Web Publishing Service サービスを停止してください。JP1/Audit Management - Manager のサービスの動作中にコマンドを実行した場合，サービス動作中を示すメッセージが表示され，コマンドの実行は中断されます。停止する JP1/Audit Management - Manager のサービスの詳細は「10.1.1　データベースマネージャの起動方法」の手順 1 を参照してください。
- このコマンドの実行時間は，データベースのサイズと格納されているデータ量に依存します。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
99	その他のエラーが発生しました。

admdbdelete（データベースのデータ削除）

機能

指定した日時までに出力された監査ログを，データベースから削除します。Administrator 権限を持つユーザで実行してください。

形式

```
admdbdelete [△-k△{mnr | bulk}]
             △-e△削除終了日時
            [△-w△作業用フォルダ]
            [△-c]
            [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-k {mnr | bulk}

データを削除する処理方法を次の二つのモードから指定します。この引数を省略した場合は，バルク削除モードが指定されます。

- mnr（マイナー削除モード）

  -e オプションで指定した削除終了日時以前のデータをデータベースから削除します。大量の監査ログがデータベースに格納されている環境から，少量の監査ログを削除する場合は，マイナー削除モードを指定することをお勧めします。

  なお，この引数でマイナー削除モードを指定した場合，-w オプションで指定した値は無視されます。

- bulk（バルク削除モード）

  -e オプションで指定した削除終了日時よりあとのデータを除き，データベースの領域を初期化することで，データを削除します。データベースに格納されている監査ログを全件削除する場合や，格納されている監査ログに対して，削除する監査ログの割合が多い場合は，バルク削除モードを指定することをお勧めします。

  -e オプションで指定した削除終了日時よりあとに格納されたデータは，-w オプションで指定した作業用フォルダに一時的に退避され，初期化後，再度格納されます。作業用フォルダで必要なディスク容量については「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

  なお，この引数でバルク削除モードを指定した場合，-c オプションを指定して，サイズの空き容量があるかどうかをチェックするようにしてください。

-e△削除終了日時

ここで指定した日時までに出力された監査ログのデータを削除します。日時は，YYYY=年，MM=月，DD=日，hh=時，mm=分，ss=秒として次の形式で指定します。

- YYYY-MM
  指定した月の最終日の 23 時 59 分 59 秒までのデータを削除します。
- YYYY-MM-DD
  指定した日の 23 時 59 分 59 秒までのデータを削除します。
- "YYYY-MM-DD△hh:mm:ss"
  指定した日時までのデータを削除します。

なお，次の場合はエラーとなります。

- 指定した日時が 1900 年 01 月 01 日 00 時 00 分 00 秒～9999 年 12 月 31 日 23 時 59 分 59 秒の範囲外の場合

-w△作業用フォルダ

この引数は，-k オプションでバルク削除モードを指定した場合に有効です。マイナー削除モードを指定した場合，-w オプションで指定した値は無視されます。

データ削除に使用する作業用フォルダをフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダは作業用フォルダとして使用できません。ドライブ直下のパスは指定しないでください。

指定したフォルダが存在しない場合，コマンド実行時に作成されます。

この引数を省略した場合，JP1/Audit Management - Manager のインストール先フォルダ¥db¥tmp が作業用フォルダとして設定されます。

-c

データ削除実行前に-w オプションで指定した作業用フォルダに必要なサイズの空き容量があるかどうかをチェックする場合に指定します。作業用フォルダで必要なディスク容量については「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

次のことに注意してください。

- 必要なサイズの空き容量がない場合は，データ削除しないでエラーとなります。
- このオプションを指定しないときに正常に実行できた場合でも，このオプションを指定して実行した場合，作業用領域不足によるエラーとなることがあります。

この引数は，-k オプションでバルク削除モードを指定した場合に有効です。マイナー削除モードを指定した場合は，指定しても無視されます。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- このコマンドを実行する前に JP1/Audit Management - Manager のサービスと World Wide Web Publishing Service サービスを停止してください。JP1/Audit Management - Manager のサービスの動作中にコマンドを実行した場合，サービス動作中を示すメッセージが表示され，コマンドの実行は中断されます。停止する JP1/Audit Management - Manager のサービスの詳細は「10.1.1　データベースマネージャの起動方法」の手順 1 を参照してください。
- 日時の指定を誤った場合などに備えて，実行前にデータベースのバックアップを取得することをお勧めします。
- このコマンドの実行時間は，データベースのサイズと格納されているデータ量に依存します。
- 引数の順序は，形式で示している順序には関係なく，任意の順序で指定できます。
- JP1/Audit Management - Manager のインストール時の設定によっては，データベースのパスワード入力が要求されることがあります。パスワードに誤りがある場合は，メッセージが表示され，コマンドの実行は中断されます。
- このコマンドを実行して監査ログを削除しても，削除した監査ログを基にして生成されていた統計情報はデータベースに残ったままになります。監査ログを削除した場合は，admstdel コマンドを実行して削除した期間の監査ログの統計情報も削除することをお勧めします。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
7	データベースのパスワードの指定に誤りがあります。
12	作業用領域として必要なサイズの空き容量がありません。
99	その他のエラーが発生しました。

admdbexport（データベースの CSV バックアップ）

機能

データベースに格納されているすべてのデータを CSV 形式でバックアップします。Administrator 権限を持つユーザで実行してください。

形式

```
admdbexport △-o△バックアップ先フォルダ
          [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-o△バックアップ先フォルダ

バックアップファイルの格納先フォルダをフルパスで指定します。次のことに注意してください。

- ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダにはバックアップファイルを格納できません。
- バックアップ先フォルダには，NTFS 上のフォルダ名を指定してください。FAT，FAT32 上のフォルダ名を指定した場合，環境によっては，ファイルシステムの制限によって処理に失敗する場合があります。
- 十分な空き容量のあるディスクのパスを指定してください。

なお，指定したフォルダにバックアップファイルがすでに存在する場合，データは上書きされます。また，指定したフォルダが存在しない場合，コマンド実行時に作成されます。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- このコマンドを実行する前に JP1/Audit Management - Manager のサービスと World Wide Web Publishing Service サービスを停止してください。JP1/Audit Management - Manager のサービスの動作中にコマンドを実行した場合，サービス動作中を示すメッセージが表示され，コマンドの実行は中断されます。停止する JP1/Audit Management - Manager のサービスの詳細は「10.1.1　データベースマネージャの起動方法」の手順 1 を参照してください。
- このコマンドを実行して取得したバックアップファイルのファイル名および内容は変更しないでください。データベースマネージャを使ったデータベースへの CSV リストアができなくなります。
- このコマンドの実行時間は，データベースのサイズと格納されているデータ量に依存します。

戻り値

戻り値	意味
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
99	その他のエラーが発生しました。

admdbimport（データベースの CSV リストア）

機能

データベースの CSV バックアップで取得した CSV 形式のデータから，データベースを復元します。

形式

```
admdbimport△-i△バックアップ格納先フォルダ
           △[-w△作業用フォルダ]
           △[-c]
           △[-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-i△バックアップ格納先フォルダ

admdbexport コマンドで CSV バックアップしたバックアップファイル格納先フォルダをフルパスで指定します。

次のことに注意してください。

- ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダにはバックアップファイルを格納できません。

-w△作業用フォルダ

CSV リストア実行時に使用する作業用ディレクトリをフルパスで指定します。

次のことに注意してください。

- ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダにはバックアップファイルを格納できません。ドライブ直下のパスは指定しないでください。
- 作業用ディレクトリに指定するフォルダに十分な空き容量があることを確認してください。

なお，指定したフォルダが存在しなかった場合，コマンド実行時に作成されます。この引数を省略した場合，次に示すフォルダが作業用フォルダとして設定されます。

JP1/Audit Management - Manager のインストール先フォルダ¥db¥tmp

-c

CSV リストア実行前に-w オプションで指定した作業用フォルダに必要なサイズの空き容量があるかどうかをチェックする場合に指定します。作業用フォルダで必要なディスク容量については「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

次のことに注意してください。

- 必要なサイズの空き容量がない場合は，CSV リストアを実行しないでエラーとなります。
- バックアップファイル内のデータ件数によって，サイズの空き容量のチェックに時間が掛かります。
- このオプションを指定しないときに正常に実行できた場合でも，このオプションを指定して実行した場合，作業用領域不足によるエラーとなることがあります。

作業用領域が不足した場合，データベースが閉塞するなどの障害になるので，このオプションを指定して実行するようにしてください。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。また，この引数を省略した場合には，データベースのパスワード認証，コマンドの実行確認の順番で確認が実行されます。

注意事項

- このコマンドを実行する前に JP1/Audit Management - Manager のサービスと World Wide Web Publishing Service サービスを停止してください。JP1/Audit Management - Manager のサービスの動作中にコマンドを実行した場合，サービス動作中を示すメッセージが表示され，コマンドの実行は中断されます。停止する JP1/Audit Management - Manager のサービスの詳細は「10.1.1　データベースマネージャの起動方法」の手順 1 を参照してください。
- このコマンドの実行時間は，データベースのサイズとリストアするデータ量に依存します。
- JP1/Audit Management - Manager のインストール時の設定によっては，データベースのパスワード入力が要求されることがあります。パスワードに誤りがある場合は，メッセージが表示され，コマンドの実行は中断されます。

戻り値

戻り値	意味
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。

戻り値	意味
4	ユーザによってコマンド実行が中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
7	データベースのパスワードの指定に誤りがあります。
8	バックアップファイルの正当性の確認に失敗しました。
12	作業用領域として必要なサイズの空き容量がありません。
99	その他のエラーが発生しました。

admdbrorg（データベースの再編成）

機能

データベースを再編成します。Administrator 権限を持つユーザで実行してください。

形式

```
admdbrorg [△-w△作業用フォルダ]
          [△-c]
          [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-w△作業用フォルダ

データベースの再編成時に使用する作業用フォルダをフルパスで指定します。

次のことに注意してください。

- ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダは作業用フォルダとして使用できません。ドライブ直下のパスは指定しないでください。
- 作業用フォルダには，NTFS 上のフォルダ名を指定してください。FAT，FAT32 上のフォルダ名を指定した場合，環境によっては，ファイルシステムの制限によって処理に失敗する場合があります。
- 十分な空き容量があるディスクのフォルダを指定してください。

指定したフォルダが存在しない場合，コマンド実行時に作成されます。

なお，この引数を省略した場合，JP1/Audit Management - Manager のインストール先フォルダ¥db¥tmp が作業用フォルダとして設定されます。

-c

再編成実行前に-w オプションで指定した作業用フォルダに必要なサイズの空き容量があるかどうかをチェックする場合に指定します。作業用フォルダで必要なディスク容量については「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

次のことに注意してください。

- 必要なサイズの空き容量がない場合は，再編成処理を実行しないでエラーとなります。

- このオプションを指定しないときに正常に実行できた場合でも，このオプションを指定して実行した場合，作業用領域不足によるエラーとなることがあります。

作業用領域が不足した場合，データベースが閉塞するなどの障害になるので，このオプションを指定して実行するようにしてください。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- このコマンドを実行する前に JP1/Audit Management - Manager のサービスと World Wide Web Publishing Service サービスを停止してください。JP1/Audit Management - Manager のサービスの動作中にコマンドを実行した場合，サービス動作中を示すメッセージが表示され，コマンドの実行は中断されます。停止する JP1/Audit Management - Manager のサービスの詳細は「10.1.1　データベースマネージャの起動方法」の手順 1 を参照してください。
- このコマンドを実行して正常終了しなかった場合，データベースが不整合な状態になり，使用できなくなる場合があります。そのため，事前にデータベースのバックアップを取得してください。
- このコマンドの実行時間は，データベースのサイズと格納されているデータ量に依存します。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
12	作業用領域として必要なサイズの空き容量がありません。
99	その他のエラーが発生しました。

admdbstat（データベースの使用状況確認）

機能

データベースの使用状況を確認し，標準出力に出力します。Administrator 権限を持つユーザで実行してください。出力例を次に示します。

```
[監査ログ情報]
監査ログ件数          : 1095000
データ領域使用率      : 27%
インデクス領域使用率  : 18%

[監査ログ統計情報]
統計パターン数        : 200
データ領域使用率      : 8%
インデクス領域使用率  : 5%
```

表 12-3　出力項目の説明

項番	分類	項目名	説明
1	監査ログ情報	監査ログ情報 (単位：件)	監査ログ管理データベースに格納されている監査ログデータの総件数を表示します。0～2147483647 の整数で出力されます。
2		データ領域使用率 (単位：%)	監査ログのデータを格納する領域の使用率を表示します。小数点以下を繰り上げた 0～100 の整数で出力されます。
3		インデクス領域使用率 (単位：%)	監査ログのインデクスを格納する領域の使用率を表示します。小数点以下を繰り上げた 0～100 の整数で出力されます。
4	監査ログ統計情報	統計パターン数 (単位：件)	監査ログ管理画面で統計パターンとして登録した集計パターンの総数を表示します。各ユーザが統計した統計パターン数の合計した値が出力されます。0～2147483647 の整数で出力されます。
5		データ領域使用率 (単位：%)	監査ログ統計情報のデータを格納する領域の使用率を表示します。小数点以下を繰り上げた 0～100 の整数で出力されます。
6		インデクス領域使用率 (単位：%)	監査ログ統計情報のインデクスを格納する領域の使用率を表示します。小数点以下を繰り上げた 0～100 の整数で出力されます。

形式

```
admdbstat
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

注意事項

- このコマンドは，JP1/Audit Management - Manager のサービスの動作中でも実行できます。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンドの引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでに admdbstat コマンドが実行されています。
99	その他のエラーが発生しました。

admdbstop（データベースの停止）

機能

データベースを停止します。

クラスタ環境のシステムで，系の切り替えやシステムの停止に使用するコマンドです。Administrator 権限を持つユーザで実行してください。

形式

```
admdbstop [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- このコマンドは，対象となるサーバをクラスタ環境で運用している場合だけ使用してください。
- このコマンドを実行する前にクラスタシステムに登録した JP1/Audit Management - Manager のサービスのリソースと Microsoft Internet Information Services のリソースをオフラインにしてください。JP1/Audit Management - Manager のサービスのリソースがオンライン中にこのコマンドを実行した場合，サービス動作中を示すメッセージが表示され，コマンドの実行は中断されます。
- データベースが正常に停止したかどうかは，コマンドの実行後，イベントビューアに出力される，次に示すメッセージの内容を確認してください。

メッセージ ID	確認ポイント
KFPS01850-I	終了モード（「mode=」の部分）が「NORMAL」であれば正常に終了しています。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
99	その他のエラーが発生しました。

admexport（監査ログのバックアップ）

機能

監査ログを CSV 形式でバックアップします。また，バックアップの実行履歴を監査ログ管理データベースに登録します。Administrator 権限を持つユーザで実行してください。バックアップする監査ログの範囲は，次のどちらかで指定します。

- 期間（開始日時と終了日時）指定
- 前回からの差分指定

形式

- 期間（開始日時と終了日時）を指定して出力する場合

```
admexport △-s△開始日時
          △-e△終了日時
          △-o△出力ファイル名
         [△-f△バックアップオプション定義ファイル名]
         [△-v]
```

- 前回との差分を出力する場合

```
admexport △-d
          △-b△出力先フォルダ名
         [△-f△バックアップオプション定義ファイル名]
         [△-v]
```

- 差分バックアップを初期化する場合

```
admexport △-d
          △-r
         [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-s△開始日時

どの時点からの監査ログのデータをバックアップするか，バックアップの開始日時を指定します。日時は，YYYY＝年，MM＝月，DD＝日，hh＝時，mm＝分，ss＝秒として次の形式で指定します。

- YYYY-MM-DD

指定した日の 0 時 0 分 0 秒からのデータをバックアップします。

- "YYYY-MM-DD△hh:mm:ss"
  指定した日時からのデータをバックアップします。

なお，次の場合はエラーとなります。

- 指定した日時が 1900 年 01 月 01 日 00 時 00 分 00 秒～9999 年 12 月 31 日 23 時 59 分 59 秒の範囲外の場合
- 指定した日時が現在日時を超えている場合
- 指定した日時が-e オプションに指定した終了日時を超えている場合

-e△終了日時

どの時点までの監査ログのデータをバックアップするか，バックアップの終了日時を指定します。日時は，YYYY=年，MM=月，DD=日，hh=時，mm=分，ss=秒として次の形式で指定します。

- YYYY-MM-DD
  指定した日の 23 時 59 分 59 秒までのデータをバックアップします。
- "YYYY-MM-DD△hh:mm:ss"
  指定した日時までのデータをバックアップします。

なお，次の場合はエラーとなります。

- 指定した日時が 1900 年 01 月 01 日 00 時 00 分 00 秒～9999 年 12 月 31 日 23 時 59 分 59 秒の範囲外の場合
- 指定した日時が-s オプションに指定した開始日時より前の場合

-o△出力ファイル名

バックアップファイル名をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダには監査ログのバックアップファイルを格納できません。

また，すでにあるバックアップファイル名を指定すると，ファイルは上書きされないでコマンドが終了します。

-f△バックアップオプション定義ファイル名

バックアップ実行履歴にバックアップ名称およびコメントを登録したい場合に，バックアップオプション定義ファイル名をフルパスで指定します。

バックアップオプション定義ファイルは，バックアップ名称およびコメントの内容を記述したファイルです。ユーザが作成します。バックアップオプション定義ファイルについては「13.7　バックアップオプション定義ファイル」を参照してください。

この引数を省略した場合，次のようになります。

- バックアップ名称

  期間指定の場合

  -o で指定したファイル名が登録されます。

  例えば，-o に「C:¥www¥backup.csv」を指定した場合は「backup.csv」になります。

  前回からの差分指定の場合

  システムで自動的に付与されるファイル名が登録されます。

- コメント

  登録されません。

-v

インポートするバックアップファイルが改ざんされていないことを確認したい場合に指定します。インポートするためのバックアップファイルを出力したい場合に，この引数を指定することをお勧めします。ただし，ほかの製品と連携するためにバックアップファイルを使用するなどの場合には，この引数を指定しないでください。

-d

差分バックアップを取得する場合に指定します。

このオプションを指定してコマンドを実行すると，前回の差分バックアップ以降からコマンド実行日の前日までの監査ログが，-b オプションで指定したフォルダに出力されます。コマンドの初回実行時の開始日時は，データベース内に格納されている監査ログで最も古い日付の 00 時 00 分 00 秒が設定されます。

なお，差分バックアップを取得したあと，同日に差分バックアップを再度取得しようとしても，バックアップは取得できません。また，このオプションを-s オプション，-e オプションまたは-o オプションと同時には指定できません。

-b△出力先フォルダ名

差分バックアップファイルを出力するフォルダ名をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダには監査ログのバックアップファイルを格納できません。

指定したフォルダが存在しない場合は，指定したフォルダが新規に作成されます。

-r

差分バックアップを初期化するときに指定します。この引数では，差分バックアップは取得されません。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に，差分バックアップ出力情報の初期化を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
5	定義ファイルの内容に誤りがあります。
11	指定した出力ファイルまたはフォルダに，すでに同じファイルが存在します。
99	その他のエラーが発生しました。

出力項目

項番	出力項目	ヘッダ
1	監査ログ ID	AuditLogID
2	メッセージ ID	MessageID
3	発生日時	MessageDate
4	プログラム名	ProgramName
5	コンポーネント名	ComponentName
6	プロセス ID	ProcessID
7	発生場所	PlaceInfo
8	監査事象種別	EventCategory
9	監査事象結果	EventResult
10	サブジェクト種別	SubjectCategory
11	サブジェクト情報	SubjectInfo
12	固有情報	PeculiarInfo

出力例

```
”AuditLogID”,”MessageID”,”MessageDate”,”ProgramName”,”ComponentName”,”ProcessID”,”PlaceInfo”,”EventCategory”,”EventResult”,”SubjectCategory”,”SubjectInfo”,”PeculiarInfo”
”0”,”4634”,”2015-02-03 12:11:08.000”,”Windows”,”LogonEvent”,”-1”,”IITSSX11.itpf.local”,”Authentication”,”Success”,”実行ユーザID”,”opadmin”,”obj=OS,op=Logoff,TZD=+09:00,アカウントがログオフしました。:,サブジェクト:,セキュリティ ID:S-1-5-21-3332803836-1137917765-3285037227-1107,アカウント ドメイ
```

```
ン:ITPF,ログオン ID:0xA2ECA808,ログオン タイプ:3”
”0”,”KAVS0200-I”,”2015-03-03 16:04:54.000”,”JP1/
AJS3”,”SchedulerLog”,”14789”,”ADWin2008x86SCH”,”StartStop”,”Success”,””,””,”A001 Mar  3
16:04:54 [14789] KAVS0200-I AJSROOT1”
```

admhasetup（論理ホスト環境の作成）

機能

監査ログ収集対象サーバがクラスタ構成の場合に，共有ディスク上の監査ログを監視するための環境を作成または削除します。このコマンドは，実行系サーバと待機系サーバの両方で実行する必要があります。なお，Windows 環境で実行した場合は，論理ホスト環境のログファイルトラップ機能を開始および停止するサービス（JP1/NETM/Audit LogTrap **論理ホスト名**）が登録されます。

Windows 環境では Administrator 権限を持つユーザで実行してください。UNIX 環境ではスーパーユーザ権限を持つユーザで実行してください。

形式

```
admhasetup △-h△論理ホスト名
           △-c△{online | standby}
          {△-r△共有フォルダ（共有ディレクトリ） | △-u}
```

コマンドを実行できるサーバ

- 監査ログ収集対象のサーバ（クラスタ環境）

格納先フォルダまたはディレクトリ

- Windows の場合

  JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき

  任意のインストール先フォルダ※¥bin

  JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき

  システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥manager¥bin

  注※

  監査ログ収集対象サーバのセットアップに必要なファイルをインストールする際に指定します。監査ログ収集対象サーバのセットアップに必要なファイルのインストールについては「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。

- UNIX の場合

  JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき

  /opt/jp1netmaudit/agent/bin

  JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき

  /opt/jp1netmaudit/manager/bin

引数

-h△論理ホスト名

論理ホスト環境を作成または削除する論理ホスト名を指定します。64 バイト以内の文字列で指定してください。論理ホスト名に指定できる文字を次に示します。

- 半角英数字
- 「-」

-c△{online | standby}

実行系サーバの論理ホスト環境を作成または削除する場合は「-c△online」，待機系サーバの論理ホスト環境を作成または削除する場合は「-c△standby」を指定します。

-r△共有フォルダ（共有ディレクトリ）

論理ホスト環境を作成する場合に指定します。フェールオーバー時に引き継ぐ情報を格納するための共有ディスク上のフォルダ（ディレクトリ）をフルパスで指定します。128 バイト以内の文字列で指定してください。共有フォルダ（共有ディレクトリ）に指定できる文字を次に示します。

- 半角英数字
- 「△(半角スペース)」「!」「#」「$」「&」「(」「)」「+」「-」「,」「;」「=」「@」「_」「`」「{」「}」「[」「]」「~」「%」「^」

指定したフォルダ（ディレクトリ）の配下に次のディレクトリが作成されます。

フォルダまたはディレクトリ	格納するファイル
共有フォルダ（共有ディレクトリ）¥jp1netmaudit¥bin	ログファイルトラップ起動用スクリプト
共有フォルダ（共有ディレクトリ）¥jp1netmaudit¥conf	動作定義ファイル

-u

論理ホスト環境を削除する場合に指定します。-u オプションを指定してコマンドを実行すると，実行確認のメッセージが表示されます。実行する場合は Y または y を，中断する場合は N または n を入力してください。Y，N，y，n 以外の値を入力した場合は，Y または N の入力を促すメッセージが表示されます。

論理ホスト環境を削除する場合，監査ログ管理サーバの監査ログ収集マネージャで，該当するサーバで監視しているプログラムを削除してから実行してください。

注意事項

- このコマンドを実行する場合は，監査ログ管理サーバの監査ログ収集マネージャで，該当するサーバのプログラム監視を停止してください。また，「JP1/NETM/Audit LogTrap **論理ホスト名**」サービスが停止していることを確認してください。監査ログの監視中やサービスが開始されている状態でこのコマ

ンドを実行した場合，フェールオーバー時にログファイルトラップ機能の開始または停止が正常にできないことがあります。

- 共有フォルダ（共有ディレクトリ）には，実行系サーバと待機系サーバで同じフォルダ（ディレクトリ）を指定してください。異なるフォルダ（ディレクトリ）を指定した場合，フェールオーバー時にログファイルトラップ機能の開始または停止が正常にできません。
- -r オプションで指定する共有フォルダ（共有ディレクトリ）配下に，ほかの用途で作成した「jp1netmaudit」が存在している場合，別の共有フォルダ（共有ディレクトリ）を指定してください。また，admhasetup コマンドで作成した「**共有フォルダ（共有ディレクトリ）¥**jp1netmaudit」配下には，フォルダ（ディレクトリ）やファイルを作成しないでください。「**共有フォルダ（共有ディレクトリ）¥**jp1netmaudit」配下にほかの用途で作成したフォルダ（ディレクトリ）またはファイルが存在している場合，論理ホスト環境の削除が正常にできません。
- 共有フォルダ（共有ディレクトリ）などを変更する場合は，一度論理ホスト環境を削除したあとで再作成してください。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンドの引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにコマンドが実行されています。
4	サービスの登録に失敗しました。
5	サービスの登録削除に失敗しました。
6	指定された共有フォルダまたは共有ディレクトリが存在しません。
7	共有フォルダまたは共有ディレクトリの作成に失敗しました。
8	共有フォルダまたは共有ディレクトリの削除に失敗しました。
9	環境設定ファイルのアクセスでエラーが発生しました。
10	すでに環境が設定されています。
11	環境が設定されていないホスト名で削除を実行しました。
12	指定された共有フォルダまたは共有ディレクトリは，ほかの論理ホストで使用されています。
13	ユーザによってコマンドの実行が中止されました。
99	その他のエラーが発生しました。

admimport（監査ログのインポート）

機能

admexport コマンドで出力した監査ログのバックアップファイルを監査ログ管理データベースにインポートして，監査ログを閲覧できるようにします。Administrator 権限を持つユーザで実行してください。

なお，admexport コマンドで-v オプションを指定し，バックアップファイルを出力した場合は，データ内容が改ざんされていないかどうかを確認します。データ内容が改ざんされている場合は，インポートできません。

形式

```
admimport [△-k△{mnr | bulk}]
          △-i△入力ファイル名[,入力ファイル名…]
          [△-w△作業用フォルダ]
          [△-c]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-k {mnr | bulk}

監査ログをインポートする処理方法を次の二つのモードから指定します。この引数を省略した場合は，マイナー挿入モードが指定されます。

- mnr（マイナー挿入モード）

  -i オプションで指定した入力ファイルのデータを，1 件ずつデータベースのデータ領域とインデクス領域に挿入します。大量の監査ログがデータベースに格納されている環境に，少量の監査ログをインポートする場合は，マイナー挿入モードを指定することをお勧めします。

  なお，この引数でマイナー挿入モードを指定した場合，-w オプションで指定した値は無視されます。

- bulk（バルク挿入モード）

  -i オプションで指定した入力ファイルのデータを，一括でデータベースのデータ領域とインデクス領域に挿入します。データベースに大量の監査ログをインポートする場合は，バルク挿入モードを指定することをお勧めします。

  入力ファイルのデータを一括で挿入するため一時ファイルが，-w オプションで指定した作業用フォルダに格納されます。作業用フォルダで必要なディスク容量については「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

なお，この引数でバルク挿入モードを指定した場合，-c オプションを指定して，サイズの空き容量があるかどうかをチェックするようにしてください。

-i△入力ファイル名[,入力ファイル名…]

監査ログのバックアップファイル名をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダからは監査ログのバックアップファイルをインポートできません。-k オプションでバルク挿入モードを指定した場合は，入力ファイル名を「,（半角コンマ）」で区切って 10 ファイルまで複数指定できます。バルク挿入モードを指定すると，admimport コマンドを実行するたびに，データベースのすべてのデータを対象として，インデクスが再作成されます。このため，複数のファイルをインポートしたい場合は，-i オプションで入力ファイル名を複数指定してインポートすることをお勧めします。

-w△作業用フォルダ

この引数は，-k オプションでバルク挿入モードを指定した場合に有効です。マイナー挿入モードを指定した場合，-w オプションで指定した値は無視されます。

監査ログのインポートで使用する作業用フォルダをフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダは作業用フォルダとして使用できません。ドライブ直下のパスは指定しないでください。

指定したフォルダが存在しない場合，コマンド実行時に作成されます。

この引数を省略した場合は「JP1/Audit Management - Manager のインストール先フォルダ¥db¥tmp」が作業用フォルダとして設定されます。

-c

インポート実行前に-w オプションで指定した作業用フォルダに必要なサイズの空き容量があるかどうかをチェックする場合に指定します。作業用フォルダで必要なディスク容量については「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

次のことに注意してください。

- 必要なサイズの空き容量がない場合は，処理インポートを実行しないでエラーとなります。
- バックアップファイル内のデータ件数によって，サイズの空き容量のチェックに時間が掛かります。
- このオプションを指定しないときに正常に実行できた場合でも，このオプションを指定して実行した場合，作業用領域不足によるエラーとなることがあります。

この引数は，-k オプションでバルク挿入モードを指定した場合に有効です。マイナー挿入モードの場合は，指定しても無視されます。

注意事項

- このコマンドを実行する前に JP1/Audit Management - Manager のサービスを停止してください。JP1/Audit Management - Manager のサービスの動作中にコマンドを実行した場合，サービス動作中

を示すメッセージが表示され，コマンドの実行は中断されます。停止するサービスの詳細は「5.7.2 監査ログ管理サーバを停止する」を参照してください。

- JP1/Audit Management - Manager のインストール時の設定によっては，データベースのパスワード入力が要求されることがあります。パスワードに誤りがある場合は，メッセージが表示され，コマンドの実行は中断されます。
- インポートするファイルのデータが改ざんされていたり，バージョンが 08-11 以前の JP1/Audit Management - Manager で取得した監査ログのバックアップファイルをインポートしたりする場合，インポートを実行するかどうかを確認するメッセージが表示されます。インポートを実行する場合は，Y または y を指定してください。インポートを中断する場合は，N または n を指定してください。
- admexport コマンドでエクスポートしたファイルを編集してインポートしないでください。
- 監査ログのバックアップファイルを定期的にインポートする場合は，インポートの完了後，データベースのバックアップを取得することをお勧めします。データベースのバックアップの取得方法については「10.1.3　データベースのバックアップ」を参照してください。
- マイナー挿入モードによるインポート実行中に「データベース書き込み中にエラーが発生しました。」のメッセージが出力され，監査ログのインポートに失敗した場合は，データベースのバックアップファイルからリストアを実行して，データベースを回復してください。データベースのバックアップデータがない場合は，データベースを再セットアップ後，監査ログのバックアップファイルをインポートしてください。
- データベースに大量のデータが格納されている場合や，インポートする監査ログのバックアップファイルに大量のデータが格納されている場合は，インポートに時間が掛かることがあります。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンドが中断されました。
6	JP1/Audit Management - Manager のサービスが動作しています。
7	データベースのパスワードの指定に誤りがあります。
8	バックアップファイルが改ざんされています。
12	作業用領域として必要なサイズの空き容量がありません。
99	その他のエラーが発生しました。

admlog.vbs（障害発生時の保守資料採取）

機能

JP1/Audit Management - Manager でトラブルが発生したときに，保守資料を一括で取得します。このコマンドは，スクリプトファイルで提供されているため，スクリプトをダブルクリックしても実行できます。Administrator 権限を持つユーザで実行してください。

採取する資料については「15.2.1　トラブル発生時に一括採取する資料」を参照してください。

形式

```
cscript △JP1/Audit Management - Managerのインストール先フォルダ¥tools¥admlog.vbs
       [△/d:資料格納先フォルダ]
       [△/a]
       [△/s]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥tools

引数

/d:資料格納先フォルダ

採取した資料の格納先フォルダをフルパス名称で指定します。

次のことに注意してください。

- 資料格納先フォルダはあらかじめ作成しておいてください。
- ローカルディスク上のパスを指定してください。ネットワークドライブ上のフォルダには採取した資料を格納できません。
- 指定したフォルダが存在していた場合，指定したフォルダ配下のすべてのフォルダおよびファイルは削除されます。

なお，この引数を省略した場合，次のフォルダ配下に採取した資料が格納されます。

JP1/Audit Management - Manager のインストール先フォルダ¥troubleshoot¥YYYY-MM-DD_hh-mm-ss

YYYY-MM-DD_hh-mm-ss：YYYY=年，MM=月，DD=日，hh=時，mm=分，ss=秒

/a

データベースの詳細資料も含めたすべての資料を採取する場合に指定します。データベースの詳細資料は障害の一次調査をする上で必須ではないため，通常はこの引数を指定する必要はありません。

/s

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

コマンド実行時の処理について次の表に示します。

表 12–4　コマンド実行時の処理

引数	処理
なし	コマンドを実行すると確認ダイアログが表示され，応答するまで処理が実行されません。データベースの詳細資料も含めて採取するかどうかを選択します。データベースの詳細資料も含める場合は［はい］ボタンを，含めない場合は［いいえ］ボタンを，実行を中断する場合は［キャンセル］ボタンをクリックしてください。通常は［いいえ］ボタンを選択して資料を採取してください。
/a	コマンドを実行すると確認ダイアログが表示され，応答するまで処理が実行されません。実行する場合は［OK］ボタンを，実行を中断する場合は［キャンセル］ボタンをクリックしてください。
/s	コマンドの実行と同時に，資料の採取を開始します。
/a△/s	コマンドの実行と同時に，データベースの詳細資料も含めたすべての資料の採取を開始します。

戻り値

戻り値※	説明
0	資料採取に成功しました。
0 以外	資料採取に失敗（キャンセルを含む）しました。

注※

資料採取を終了すると，資料採取の成功および失敗を示すダイアログが表示されます。

admrrexport（正規化ルールのバックアップ）

機能

正規化ルールエディタで作成した正規化ルールをバックアップします。Administrator 権限を持つユーザで実行してください。

形式

```
admrrexport [△-p△製品情報名[,製品情報名…]]
            [△-u]
             △-o△正規化ルール定義エクスポートファイル名称
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥convert¥server¥bin

引数

-p△製品情報名[,製品情報名…]

正規化ルール定義エクスポートファイルへ出力する製品情報名を指定します。コマンドを実行すると，オプションに指定された製品情報定義と，その製品情報定義に属する正規化ルール定義，およびサンプルメッセージを，正規化ルール定義エクスポートファイルに出力します。このオプションを指定するときは，次のことに注意してください。

- 製品情報名は最大 100 件指定できます。複数指定する場合は「,（半角コンマ）」で区切って指定してください。同じ製品情報名を複数回指定したときは，1 回目の指定だけが有効となり，2 回目以降の指定は無視して処理されます。
- 製品情報名に半角スペースが含まれる場合は，製品情報名ごとに「"」で囲んで指定してください。
- このオプションを省略した場合は，定義されているすべての製品情報定義を出力します。

-u

-o オプションで指定したファイルがすでに存在している場合に，上書きして定義情報を出力するときに指定します。

このオプションの指定を省略し，-o オプションの指定値と同じファイルがすでに存在する場合はエラーとなり，戻り値として「11」を返します。

-o△正規化ルール定義エクスポートファイル名称

正規化ルール定義を出力するファイル名称をフルパスで指定します。ローカルディスク上のパスを指定してください。ネットワークドライブ上のパスを指定するとエラーになります。指定したフォルダが存在しない場合，コマンド実行時に作成されます。正規化ルール定義エクスポートファイル名称は 255 バイト以内の文字列で指定してください。

注意事項

- このコマンドを実行する前に，JP1/NETM/Audit - Manager Define サービスを起動してください。
- このコマンドは多重実行できません。多重実行を試みるとエラーになります。
- このコマンドは admrrimport コマンドが実行中の場合，実行できません。実行を試みるとエラーになります。
- このコマンドは正規化ルールエディタが実行中の場合，実行できません。実行を試みるとエラーになります。
- 正規化ルールの定義が未完了で，一時的に保存している状態の製品情報や正規化ルールもバックアップ対象となります。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかの正規化ルール管理コマンド，または正規化ルールエディタが実行されています。
9	JP1/NETM/Audit - Manager Define サービスが停止しています。
10	指定された製品情報名が存在しないか，または同じ製品情報名が複数回指定されています。
11	指定した出力ファイルがすでに存在します。
99	その他のエラーが発生しました。

admrrimport（正規化ルールのインポート）

機能

admrrexport コマンドで出力した正規化ルール定義エクスポートファイルをインポートします。
Administrator 権限を持つユーザで実行してください。

形式

```
admrrimport [△-m△{addproduct | addrule | update}]
            △-i△正規化ルール定義エクスポートファイル名称
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥convert¥server¥bin

引数

-m△{addproduct | addrule | update}

インポートする定義と同じ定義がすでに存在する場合の処理方法を，次の三つのモードから指定します。引数を省略したときは，addproduct（製品情報単位の追加モード）が指定されます。

- addproduct（製品情報単位の追加モード）

  データベースに登録されていない製品情報定義と，それに属する正規化ルール定義だけを追加する場合に指定します。新たに構築した環境に，別の環境で定義した製品情報および正規化ルールを追加するときは，製品情報単位の追加モードを指定します。

- addrule（正規化ルール単位の追加モード）

  データベースに登録されていない製品情報定義および正規化ルール定義をすべて追加する場合に指定します。インポートする正規化ルール定義が属する製品情報がリリース状態のときは，リリース編集状態になります。すでに存在する製品情報に，別の環境の正規化ルールエディタで作成した正規化ルールを追加するときは，正規化ルール単位の追加モードを指定します。

- update（更新モード）

  データベースに登録されていない製品情報定義および正規化ルール定義をすべて追加し，データベースに登録されている定義を更新する場合に指定します。インポートする定義と同じ製品情報および正規化ルールは更新され，リリース状態のときはリリース編集状態になります。製品情報や正規化ルールを，admrrexport コマンドで出力した定義と同じ内容に更新するときは更新モードを指定します。

  なお，更新モードでインポートを実行し更新された定義を元に戻すには，データベースを復元してください。データベースの復元については，「10.1.4　データベースのリストア」を参照してください。

-i△正規化ルール定義エクスポートファイル名称

admrrexport コマンドで出力した正規化ルール定義エクスポートファイル名称をフルパスで指定します。このオプションを指定する場合は，次のことに注意してください。

- admrrexport コマンドで出力した，正規化ルール定義エクスポートファイル以外のファイルを指定しないでください。正規化ルール定義エクスポートファイル以外のファイルを指定した場合は，エラーとなります。
- ローカルディスク上のパスを指定してください。ネットワークドライブ上のパスを指定した場合はエラーとなります。
- 255 バイト以内の文字列で指定してください。

注意事項

- このコマンドを実行する前に，データベースのバックアップを取得してください。データベースのバックアップの取得方法については「10.1.3　データベースのバックアップ」を参照してください。
- このコマンドを実行する前に，JP1/NETM/Audit - Manager Define サービスを起動してください。
- admrrexport コマンドが実行中の場合，このコマンドは実行できません。実行を試みるとエラーになります。
- 正規化ルールエディタが実行中の場合，このコマンドは実行できません。実行を試みるとエラーになります。
- このコマンドは多重実行できません。多重実行を試みるとエラーになります。
- このコマンドは，リリース許可状態およびリリース解除許可状態の定義を更新しません。
- インポートした製品情報定義数が 100 件を超えた場合，データベースを再編成してください。データベースを再編成する方法については，「10.1.5　データベースの再編成」を参照してください。
- 正規化ルールの定義が未完了で，一時的に保存している状態の正規化ルール定義をインポートすると，インポートした定義を正規化ルールエディタを使用して定義を完了するまで，その正規化ルール定義を含む製品情報定義はリリースできません。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかの正規化ルール管理コマンドまたは正規化ルールエディタが実行されています。
8	正規化ルール定義エクスポートファイルに誤りがあります。
9	JP1/NETM/Audit - Manager Define サービスが停止しています。

戻り値	説明
10	インポートできなかった定義があります。
99	その他のエラーが発生しました。

admstdel（監査ログの統計情報削除）

機能

監査ログ管理データベースに格納されている監査ログの統計情報を削除します。Administrator 権限を持つユーザで実行してください。

形式

```
admstdel {△-e△削除終了日 | △-d△保持日数}
        [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-e△削除終了日

ここで指定した日付までに監査ログ管理データベースに生成された監査ログの統計情報を削除します。日付は，YYYY=年，MM=月，DD=日として次の形式で指定します。

- YYYY-MM
  指定した月の最終日の 23 時 59 分 59 秒までのデータを削除します。
- YYYY-MM-DD
  指定した日の 23 時 59 分 59 秒までのデータを削除します。

なお，次の場合はエラーとなります。

- 指定した日付が 1900 年 01 月 01 日～9999 年 12 月 31 日の範囲外の場合
- 指定形式に誤りがある場合

-d△保持日数

コマンド実行日を含め，何日前までの監査ログの統計情報を保持したいか 0～366 の整数で指定し，それより過去のデータを削除します。保持されるデータは，コマンド実行日を含め，さかのぼって指定した日数分のデータです。0 を指定するとコマンド実行日以前のデータを削除します。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- コマンドの実行時間は，データベースのサイズや格納されているデータ量に依存します。
- 引数の順序は，形式で示している順序には関係なく，任意の順序で指定できます。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
99	その他のエラーが発生しました。

admstgen（監査ログの統計情報生成）

機能

監査ログ管理データベースに監査ログの統計情報を生成します。Administrator 権限を持つユーザで実行してください。

形式

```
admstgen {△-s△絶対日付 | △-d△相対日数}
        [△-y]
```

コマンドを実行できるサーバ

- JP1/Audit Management - Manager をインストールしたサーバ

格納先フォルダ

JP1/Audit Management - Manager のインストール先フォルダ¥bin

引数

-s△絶対日付

ここで指定した日付から現在までの監査ログ管理データベース内の監査ログ情報を基として，監査ログの統計情報を生成します。日付は，YYYY=年，MM=月，DD=日として次の形式で指定します。

- YYYY-MM-DD
  指定した日の 0 時 0 分 0 秒から現在までの監査ログ管理データベース内の監査ログ情報を基として，監査ログの統計情報を生成します。

なお，次の場合はエラーとなります。

- 指定した日付が 1900 年 01 月 01 日～9999 年 12 月 31 日の範囲外の場合
- 指定した日付がコマンド実行日を超えている場合
- 指定形式に誤りがある場合

-d△相対日数

コマンド実行日から何日前までの監査ログ情報を基にして，監査ログの統計情報を生成したいか 0～366 の整数で指定します。生成されるデータは，コマンド実行日を起点とし，さかのぼって指定した日数の 0 時 0 分 0 秒以降のデータです。0 を指定するとコマンド実行日の 0 時 0 分 0 秒からの監査ログ情報を基にして，統計情報を生成します。

-y

確認メッセージの出力を省略して，コマンドの実行と同時に処理を開始したい場合に指定します。

この引数を省略した場合，コマンドを実行すると確認メッセージが表示され，メッセージに応答するまで処理が実行されません。実行する場合は Y または y を，実行を中断する場合は N または n を入力してください。

注意事項

- コマンドの実行時間は，データベースのサイズや格納されているデータ量に依存します。
- 引数の順序は，形式で示している順序には関係なく，任意の順序で指定できます。
- このコマンドは，表示設定画面で設定している統計パターンを対象に監査ログの統計情報を生成します。

戻り値

戻り値	説明
0	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	コマンドの実行権限がありません。
3	同一マシン上で，すでにほかのデータベース管理コマンドが実行されています。
4	ユーザによってコマンド実行が中断されました。
99	その他のエラーが発生しました。

admuxlogcol（UNIX システムログ情報の変換）

機能

監査対象である UNIX のシステムログ情報ファイルを，統一フォーマットに変換して，UNIX ログ変換ファイルに出力します。コマンドを cron デーモンに登録することで，監査ログ変換ファイルを定期的に出力できます。実行権限があるのは，root ユーザ権限を持つユーザです。

このコマンドは，監査ログ収集対象の UNIX サーバで使用します。

形式

```
admuxlogcol △-t△{login | loginfail | su}
```

コマンドを実行できるサーバ

- 監査ログ収集対象の UNIX サーバ

格納先フォルダ

- JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合
  /opt/jp1netmaudit/agent/bin
- JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合
  /opt/jp1netmaudit/manager/bin

引数

-t {login | loginfail | su}

変換出力するログの種類を次の三つから指定します。

- login
  ログインおよびログアウト情報が格納されたファイルのデータを変換出力します。
  変換対象とする UNIX の情報ファイル名と変換したログ情報の格納先を次の表に示します。

表 12–5　UNIX ログ変換ファイルの出力（ログインおよびログアウト情報）

項番	OS（UNIX）	変換対象ファイル	格納先ファイル
1	HP-UX	/var/adm/wtmps	ラップアラウンド形式で，次のファイル※のどちらかに格納されます。 • login.1 • login.2
2	AIX	/var/adm/wtmp	
3	Solaris	/var/adm/wtmpx	
4	Linux	/var/log/wtmp	

注※

ファイルの格納先を次に示します。

JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合

/var/opt/jp1netmaudit/agent/log

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合

/opt/jp1netmaudit/manager/log

- loginfail

ログイン失敗情報が格納されたファイルのデータを変換出力します。

変換対象とする UNIX の情報ファイル名と変換したログ情報の格納先を次の表に示します。

表 12–6　UNIX ログ変換ファイルの出力（ログイン失敗情報）

項番	OS（UNIX）	変換対象ファイル	格納先ファイル
1	HP-UX	/var/adm/btmps	ラップアラウンド形式で，次のファイル※のどちらかに格納されます。 • loginfailed.1 • loginfailed.2
2	AIX	/etc/security/failedlogin	
3	Solaris	/var/adm/loginlog	
4	Linux	/var/log/btmp	

注※

ファイルの格納先を次に示します。

JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合

/var/opt/jp1netmaudit/agent/log

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合

/opt/jp1netmaudit/manager/log

- su

su コマンドの情報が格納されたファイルのデータを変換出力します。

変換対象とする UNIX の情報ファイル名と変換したログ情報の格納先を次の表に示します。

表 12–7　UNIX ログ変換ファイルの出力（su コマンドの情報）

項番	OS（UNIX）	変換対象ファイル	格納先ファイル
1	HP-UX	/var/adm/sulog	ラップアラウンド形式で，次のファイル※1 のどちらかに格納されます。 • sulog.1 • sulog.2
2	AIX	/var/adm/sulog	
3	Solaris	/var/adm/sulog	
4	Linux	—※2	—

（凡例）

—：対象外

注※1

ファイルの格納先を次に示します。

JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合

/var/opt/jp1netmaudit/agent/log

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合

/opt/jp1netmaudit/manager/log

注※2

Linux で su を指定してコマンドを実行した場合，何も処理されないため，変換出力はありません。

注意事項

- このコマンドの実行時間は，変換対象の UNIX システムログ情報のデータ量に依存します。
- 変換出力するログの種類ごとに，引数を指定してコマンドを実行してください。また，同じコマンド引数を指定したコマンドが実行中の場合には，コマンドはエラー終了します。
- 変換対象となる UNIX のシステムログ情報ファイルのサイズが 2 ギガバイトを超えている場合は変換できません。
- 出力先となる UNIX ログ変換ファイルのサイズが 2 ギガバイトを超えると，それ以降のデータは変換されないで，戻り値 4 で終了します。変換されないデータは，次回のコマンド実行時にラップアラウンドしたファイルに出力されます。
- 変換対象となる UNIX のシステムログ情報ファイル（変換対象ファイル）のローテートについて，次のようにローテートしたファイル名の形式だけに対応しています。

  ファイル名形式：<変換対象ファイル>.<番号>※

  注※

  番号は 10 進数 0 または 1 から INT の最大値までの通番

  （例）wtmp.1，wtmp.2 など
- ログアウト時のユーザ名は，該当プロセス ID またはデバイス名を基に対応するログイン時の情報を検索し設定します。該当するログイン情報が検索できなかった場合は，ユーザ名に「UNKNOWN」を出力し，リモートホスト名は出力しません。また，変換を開始した変換対象ファイルの先頭から検索し，変換対象ファイルがローテートしている場合，変換を開始した変換対象ファイルより古いファイルは検索しません。

戻り値

戻り値	説明
0※	コマンドの処理が正常に終了しました。
1	コマンド引数の指定に誤りがあります。
2	すでに同じログの種類を指定したコマンドが実行中です。
3	変換対象とするログファイルがありません。
4	UNIX ログ変換ファイルのサイズが 2 ギガバイトを超えました。
99	その他のエラーが発生しました。

注※

Linux で su を指定してコマンドを実行した場合は，何も処理されないで正常終了します。

13 定義ファイル

この章では，監査証跡管理システムの定義ファイルについて説明します。

13.1　定義ファイル一覧

監査証跡管理システムで使用する定義ファイルを次の表に示します。

表 13–1　監査証跡管理システムの運用で使用する定義ファイル一覧

項番	定義ファイル	定義内容	参照先
1	正規化ルールファイル	監査ログ収集対象サーバから収集した監査ログを，監査ログ管理データベースへ格納できるようにするための正規化パターンを定義したファイルです。	13.2
2	製品定義ファイル	監査ログ収集対象サーバの監査ログを収集するためのログファイルトラップ機能の動作を定義するファイルです。	13.3
3	動作定義ファイル	監査ログ収集対象サーバ側からログファイルトラップ機能を起動するときの動作を定義したファイルです。	13.4
4	監査ログ標準レポート定義ファイル	監査ログの検索結果をレポート表示する際に，監査ログレポート画面の説明欄に表示する固有情報の内容を定義するファイルです。	13.5
5	監査ログレポート定義ファイル	JP1/Audit Management - Manager で標準サポート外となっているプログラムを収集対象とした場合で，かつ監査ログの検索結果をレポート表示する場合に，監査ログレポート画面の説明欄に表示する固有情報の内容を定義するファイルです。	13.6
6	バックアップオプション定義ファイル	監査ログのバックアップおよび監査ログの移動をする際に，バックアップ実行履歴のバックアップ名称およびコメントを定義するファイルです。	13.7
7	パターン情報ファイル	機能ツリーのパターンやフォルダの情報をエクスポートする際に，監査ログ管理サーバ上に出力される CSV 形式ファイルです。このファイルをインポートすることによって，パターンやフォルダの情報をほかのサーバに移行できます。	13.8
8	監査ログ収集対象サーバセットアップ定義ファイル	監査ログ専用イベントサーバの環境情報を定義するファイルです。 監査ログ収集対象サーバのセットアップ時に，admagtsetup コマンドでこのファイルを指定すると，定義内容に従って，監査ログ専用イベントサーバの環境が監査ログ収集対象サーバに作成されます。	13.9

注

　これらのファイルを編集する場合は，事前にバックアップを取得することをお勧めします。

13.2　正規化ルールファイル

監査ログ収集対象サーバ上のプログラムから出力される監査ログの出力形式を，監査ログ管理データベースに格納できる監査ログの出力形式へ変換するための規則が正規化ルールです。正規化ルールを定義しているファイルを正規化ルールファイルと呼びます。

ここでは，正規化ルールファイルの格納先や定義内容について説明します。

JP1/Audit Management - Manager で標準サポート外となっているプログラムの場合でも，正規化ルールファイルとあわせて，製品定義ファイル，動作定義ファイル，および監査ログレポート定義ファイルを作成することによって，監査ログを管理・収集できるようになります。

標準サポート外のプログラムから監査ログを収集する方法については「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。なお，標準サポートしているプログラムの正規化ルールファイルは編集できません。

13.2.1　ファイル名および格納先

正規化ルールファイル名およびファイルの格納フォルダを次の表に示します。

表 13–2　正規化ルールファイル名とファイルの格納フォルダ

項番	収集対象	ファイル名	ファイル格納フォルダ
1	• Collaboration • Cosminexus • HiRDB • Hitachi Navigation Platform • JP1/AO • JP1/Audit • JP1/Base • JP1/IM - NP • JP1/IM - SS • JP1/ITDM • JP1/ITDM2 • JP1/ITRM • JP1/NETM/AIM • JP1/NETM/CSC • JP1/NETM/DM • JP1/NETM/NM • JP1/PFM • JP1/秘文 • OpenTP1 • TRUST E2	admrglrule_CALFHM.conf※1	JP1/Audit Management - Manager のインストール先フォルダ¥conf¥rule

項番	収集対象	ファイル名	ファイル格納フォルダ
	• XDM/BASE E2 • uCosminexus EUR Server • uCosminexus Navigation Platform • uCosminexus Portal Framework • UNIX のシステムログ • 活文 NAVIstaff		
2	JP1/AJS2	admrglrule_JP1_AJS2.conf※2	
3	JP1/AJS3	admrglrule_JP1_AJS3.conf※3	
4	Windows イベントログ（セキュリティに関する情報）	admrglrule_WinEventLog_Security.conf※4	
5	標準サポート外のプログラム	admrglrule_任意.conf※5	
6	正規化ルールエディタで定義するプログラム	admrglrule_AdmConvert.conf※6	

注※1

統一フォーマット用の正規化ルールファイルです。

注※2

JP1/AJS2 製品ログ用の正規化ルールファイルです。

注※3

JP1/AJS3 製品ログ用の正規化ルールファイルです。

注※4

Windows イベントログ用の正規化ルールファイルです。

標準サポート外となっている Windows Server 2003 または Windows XP の Windows イベントログ（セキュリティに関する情報）を収集する場合は，このファイルに定義を追加します。

注※5

JP1/Audit Management - Manager で標準サポート外となっているプログラム用の正規化ルールファイルです。ファイル名は製品定義ファイルに記述する正規化ルールファイル名と一致させてください。製品定義ファイルについては「13.3　製品定義ファイル」を参照してください。

注※6

正規化ルールエディタで定義するプログラム用の正規化ルールファイルです。Hitachi Storage Command Suite 製品ログ用にも適用されます。

13.2.2　書式

```
[LOGTYPE]↓
TYPE={KEY｜VALUE｜WINEVENT}↓
SEPARATE={space｜comma｜CRLF｜nothing}↓
SECTION={0｜1}↓
LOGSTART=区切り文字の位置↓
ESCTYPE={0｜1｜2}↓
FRONTESC=開始記号↓
REARESC=終了記号↓
SKIPSPACE={0｜1}↓
↓
[正規化パターン]↓
番号=種別:正規化ルール:項目1:項目2:次番号1:次番号2↓
番号=種別:正規化ルール:項目1:項目2:次番号1:次番号2↓
番号=種別:正規化ルール:項目1:項目2:次番号1:次番号2↓
：
```

注

- 標準サポート外のプログラムを収集する場合と標準サポート外の Windows イベントログを収集する場合とで，指定できる値が異なります。それぞれで指定する値については「(3)　定義内容（標準サポート外のプログラムを収集する場合)」および「(4)　定義内容（標準サポート外の Windows イベントログを収集する場合)」を参照してください。
- 記述行の最後には，必ず改行を記述してください。
- 各項目は「:」で区切ってください。
- 項目に「:」を含む場合は，項目全体を「"」で囲んでください。
- 「KEY=」以降の文字列の最大長は 1,024 バイトです。

13.2.3　定義内容（標準サポート外のプログラムを収集する場合）

JP1/Audit Management - Manager で標準サポート外となっているプログラムを収集する場合に，［LOGTYPE］および［正規化パターン］で記述する内容についてそれぞれ説明します。

(1)　［LOGTYPE］の設定項目

［LOGTYPE］で記述する内容について，次の表に示します。

表 13-3　［LOGTYPE］設定項目（標準サポート外のプログラムを収集する場合）

項番	項目名	説明
1	［LOGTYPE］	定義の始まりを示す［LOGTYPE］を指定します。
2	TYPE	ログの記述形式を指定します。次のどちらかを指定します。 • KEY：「KEY=値［SEPARATE に指定した文字］KEY=値・・・・」形式

項番	項目名	説明
		• VALUE：「値 1［SEPARATE に指定した文字］値 2・・・」（値の羅列）形式
3	SEPARATE	ログの区切り文字の種別です。次のどちらかを指定します。 • space：「半角スペース」 • comma：「,（半角コンマ）」
4	SECTION	監査ログの最初の区切り文字までの文字列を正規化パターン名として使用するかどうかを指定します。 • 0：使用しない • 1：使用する 0 を指定した場合は，［**正規化パターン**］に「PATTERN」と指定します。 1 を指定した場合は，［**正規化パターン**］に「監査ログの最初の区切り文字までの文字列」を指定します。 この場合，監査ログの最初の区切り文字までの文字列の パターンすべてについて定義します。
5	LOGSTART	ログの先頭から文字を読み飛ばして，正規化で使用しない文字までの位置を指定します。「0」を指定した場合は，先頭から正規化されます。
6	ESCTYPE	ログ中でエスケープに使用する記号を指定します。次のどれかを指定します。 • 0：なし（エスケープしないログの場合） • 1：「"」 • 2：「"」以外の記号 なお，前後の文字が同じ場合は，「2」を指定できません。「0」を指定してください。
7	FRONTESC※	ESCTYPE が「2」の場合，エスケープに使用する開始記号を指定します。開始記号には，1 バイトの文字だけ指定できます。
8	REARESC※	ESCTYPE が「2」の場合，エスケープに使用する終了記号を指定します。終了記号には，1 バイトの文字だけ指定できます。
9	SKIPSPACE	連続する複数のスペースを一つのスペースとして処理するかどうかを指定します。SEPARATE が「space」の場合だけ指定し，「comma」の場合は指定しないでください。 • 0：複数のスペースのまま処理する • 1：一つのスペースとして処理する 1 を指定した場合は，ログのすべての連続スペースが一つのスペースに置き換えられてから，正規化されます。

注

- ログの項目位置は，次のようにカウントします。
  ログ：value1［SEPARATE に指定した文字］value2・・・
  位置：　1　　2　・・・
- 各項目の設定値は省略できません。値を指定しない場合は，その項目も指定しないでください。

注※

FRONTESC と REARESC には同一の文字は指定できません。

(2) ［正規化パターン］の設定項目

［正規化パターン］で記述する内容について，次に示します。

(a) ［正規化パターン］の各項目の設定値

［正規化パターン］の各設定項目での設定値を次の表に示します。

表 13–4 ［正規化パターン］の各項目の設定値（標準サポート外のプログラムを収集する場合）

項番	番号	種別	正規化ルール	項目 1	項目 2	次番号 1	次番号 2	「正規化ルール」に「*」を指定したときの「項目 1」の範囲
1	1～の通番	CHECK※1	「J」	判定する項目位置を設定します。	真偽を判定する対象となる値	判定が真の場合に適用する次の番号	判定が偽の場合に適用する次の番号	－
2		AuditLogID※2	「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。	×	次の番号	×	－
			「*」※3	値や文字列を設定します。				0～2147483647 の整数
3		MessageID	「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。	×	次の番号	×	－
			「*」※3	値や文字列を設定します。				64 バイト以内の文字列
4		MessageDate	「D」	TYPE=KEY の場合 日時を示す KEY 名称を設定します。 TYPE=VALUE の場合 日時を示す値の項目位置を示す番号を設定します。	×	次の番号	×	－
			「UD」※3	TYPE=KEY の場合 日時を示す KEY 名称を設定します。	任意の日時形式を設定します。			

項番	番号	種別	正規化ルール	項目 1	項目 2	次番号 1	次番号 2	「正規化ルール」に「*」を指定したときの「項目 1」の範囲
				TYPE=VALUE の場合 日時を示す値の項目位置を示す番号を設定します。	設定値については，表 13-7 を参照してください。			
5		ProgramName	「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。	×	次の番号	×	－
			「*」※3	値や文字列を設定します。				64 バイト以内の文字列
6		ComponentName	「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。	×	次の番号	×	－
			「*」※3	値や文字列を設定します。				64 バイト以内の文字列
7		ProcessID※2	「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。	×	次の番号	×	－
			「*」※3	値や文字列を設定します。				「-1」
8		PlaceInfo	「S」※3	KEY 名称を設定します。	×	次の番号	×	－
			「H」	×				
			「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。				
9		EventCategoryName	「-」	TYPE=KEY の場合 KEY 名称を設定します。	×	次の番号	×	－

項番	番号	種別	正規化ルール	項目 1	項目 2	次番号 1	次番号 2	「正規化ルール」に「*」を指定したときの「項目 1」の範囲
				TYPE=VALUE の場合 項目位置を示す番号を設定します。				
			「*」	次に示す文字列のどれかを設定します。 • StartStop • Authentication • AccessControl • ConfigurationAccess • Failure • LinkStatus • ExternalService • ContentAccess • Maintenance • AnomalyEvent • ManagementAction				
10		EventResultName	「-」	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示す番号を設定します。	×	次の番号	×	−
			「*」	次に示す文字列のどれかを設定します。 • Success • Failure • Occurrence				
11		SubjectInfo	「S」 ※3	対応する KEY 名称を設定します。	×	次の番号	×	−
			「C」	次に示すカテゴリ名のどれかを設定します。 • "subj:euid"：実行ユーザ • "subj:uid"：アカウント識別子 • "subj:pid"：プロセス ID	TYPE=KEY の場合 KEY 名称を設定します。 TYPE=VALUE の場合 項目位置を示			

項番	番号	種別	正規化ルール	項目 1	項目 2	次番号 1	次番号 2	「正規化ルール」に「*」を指定したときの「項目 1」の範囲
					す番号を設定します。			
			「*」※3	値や文字列を設定します。	×			「""」
12		PeculiarInfo※4	「M」※3	先頭に配置してデータベースに格納したい KEY 名称を設定します。	×	次の番号	×	－
13			「N」	項目位置を示す番号を設定します。				

（凡例）

×：指定しない。区切りの「:」も指定しない。

－：該当なし

注

KEY 名称は「KEY=値,・・・」の KEY に該当する文字列を表します。

注※1

［LOGTYPE］の TYPE を VALUE に設定した場合だけ指定できます。

注※2

「項目 1」に次の値を指定した場合，監査ログ管理画面上は空白が表示されます。

・AuditLogID：0

・ProcessID：-1

注※3

項目に「:」を含む場合は，「項目 1」に指定する項目全体を「"」で囲みます。

注※4

PeculiarInfo は，「M」を指定する場合，最後に定義する必要があります。

(b) ［正規化パターン］の設定項目

［正規化パターン］の設定項目を次の表に示します。

表 13–5 ［正規化パターン］設定項目（標準サポート外のプログラムを収集する場合）

項番	項目名	説明
1	［正規化パターン］	定義の始まりを示す［正規化パターン］を指定します。 SECTION で指定した値が，0 の場合は［PATTERN］を指定します。SECTION で指定した値が，1 の場合は，監査ログの最初の区切り文字までの文字列を正規化パターン名として指定します。
2	番号	正規化ルールを適用する順番を 1 からの整数で指定します。
3	種別※1	正規化の対象となるデータ種別を指定します。指定値を次に示します。

項番	項目名	説明
		• CHECK 判定条件を設定する場合に指定します。[LOGTYPE] の TYPE を VALUE に設定した場合だけ指定できます。 • AuditLogID 監査ログの通番を設定する場合に指定します。 • MessageID 監査ログのメッセージ ID を設定する場合に指定します。 • MessageDate 監査ログの発生日時を設定する場合に指定します。 • ProgramName※2 監査ログの発生プログラム名を設定する場合に指定します。 • ComponentName※2 監査ログの発生コンポーネント名を設定する場合に指定します。 • ProcessID 監査ログの発生プロセス ID を設定する場合に指定します。 • PlaceInfo 監査ログの発生場所を設定する場合に指定します。 • EventCategoryName 監査ログのカテゴリ名を設定する場合に指定します。 • EventResultName 監査ログの結果を設定する場合に指定します。 • SubjectInfo 監査ログを発生させたユーザ名を設定する場合に指定します。 • PeculiarInfo※3 監査ログの詳細情報を設定する場合に指定します。
4	正規化ルール	正規化のルールを指定します。指定できる値を次に示します。 • 「J」 [LOGTYPE] の TYPE が VALUE の場合にだけ指定できます。判定条件を指定する場合に指定します。「J」を指定し，かつ項目 1 で判定する項目位置を定義すると，定義した項目位置の値を判定します。判定する項目位置に項目 2 で定義する文字列が存在する場合は真となり，次番号 1 で定義する値を読み込みます。判定する項目位置に項目 2 で定義する文字列が存在しない場合は偽となり，次番号 2 で定義する値を読み込みます。 • 「-」 監査ログに存在する KEY 名称または項目位置の値を使用する場合に指定します。 [LOGTYPE] の TYPE が KEY の場合は，KEY 名称を定義します。[LOGTYPE] の TYPE が VALUE の場合は，値の項目位置を定義します。 • 「*」 項目 1 で定義する値または文字列を使用し，データベースへ格納する場合に指定します。値または文字列に「:」が含まれる場合は，項目全体を「"」で囲みます。 • 「D」 監査ログに存在する KEY 名称または項目位置の値を，日時として使用する場合に指定します。なお，日時として使用する値は，JP1/Audit Management - Manager 定型の日時形式である必要があります。日時形式については，表 13-6 を参照してください。KEY 名称また

項番	項目名	説明
		は項目位置は，項目 1 で定義します。[LOGTYPE] の TYPE が KEY の場合は，KEY 名称を使用します。[LOGTYPE] の TYPE が VALUE の場合は，指定した項目位置の値を使用します。 また，複数の項目を指定する場合は，コンマで区切って指定します。 (SEPARATER=space の場合) 複数項目指定時は次の順番になるように項目位置を指定します。 ・「YYYY/MM/DD」「hh:mm:ss」 ・「MMM」「DD」「hh:mm:ss」 日時形式を詳細に指定する場合は，「UD」を使用します。 • 「UD」 監査ログに存在する KEY 名称または項目位置の値を，日時として使用する場合に指定します。ただし，日時形式を項目 2 で定義する必要があります。文字列中に「:」を含む場合は，「"」で囲む必要があります。日付形式の設定方法については，表 13-7 を参照してください。 また，複数の項目を指定する場合は，コンマで区切って指定します。 複数項目を指定している場合，各項目間は半角スペースで連結されるものとして，日時形式を指定します。 なお，項目 1 で指定した項目名称の値にエスケープ文字が含まれる場合は，エスケープ文字も日時の文字列に含まれるものとして日付形式を指定します。 例) ログ：date="2001/01/02 01:02:34" 項目 1 の指定：date 項目 2 の指定："#%Y/%m/%d %H:%M:%s#" • 「H」 監査ログ収集対象サーバ名を使用し，データベースに格納する場合に指定します。 • 「S」 [LOGTYPE] の TYPE が KEY の場合にだけ指定できます。監査ログごとに出力される発生場所の KEY 名称が異なる場合に，複数の異なる KEY 名称を指定します。 異なる複数の KEY 名称は項目 1 で定義します。※4 • 「C」 [LOGTYPE] の TYPE が VALUE の場合，項目 2 で指定した項目位置の値を項目 1 で指定したカテゴリで使用する場合に指定します。 [LOGTYPE] の TYPE が KEY の場合，項目 2 で指定した KEY 名称の値を項目 1 で指定したカテゴリで使用する場合に指定します。 項目 1 でカテゴリの値として指定できる文字列は，「subj:euid（実行ユーザ)」，「subj:uid（アカウント識別子)」，または「subj:pid（プロセス ID)」のどれかです。このうちの一つを項目 1 に指定してください。 • 「M」 [LOGTYPE] の TYPE が KEY の場合にだけ指定できます。「M」の前までに使用されていない KEY 名称をすべて使用する場合に指定します。使用するデータのうち，先頭に配置してデータベースに格納したい KEY 名称を，項目 1 で指定します。文字列中に「:」を含む場合は，「"」で囲む必要があります。 • 「N」 [LOGTYPE] の TYPE が VALUE の場合にだけ指定できます。項目 1 で指定した位置以降の値のうち，「N」の前に指定したルールで使用していないデータをすべてデータベースに格納する場合に指定します。

項番	項目名	説明
5	項目 1	項番 4 の正規化ルールに設定する値によって指定する情報が変わります。正規化ルールに設定した値の説明に記載されている情報を設定します。
6	項目 2	
7	次番号 1	適用する正規化ルールの次の key 値（項番 1）を指定します。最後の正規化ルールの場合は「0」を指定します。
8	次番号 2	

注

各項目は「:」で区切ります。

注※1

「CHECK」を除いて，すべて必須項目です。

注※2

「ProgramName」は「ComponentName」の前に定義してください。

注※3

「PeculiarInfo」の場合で，かつ正規化ルールでの設定値が「M」または「N」の項目は最後に定義してください。

注※4

種別で「SubjectInfo」を設定し，かつ正規化ルールで「S」を指定した場合の指定例を次に示します。指定例の「n」は番号に指定する値です。

A=SubjectInfo，B=SubjectInfo，または C=SubjectInfo のどれか一つを含む場合

```
n:SubjectInfo:S:A,B,C:n+1
```

(c) ［正規化パターン］の正規化ルールで「D」を指定した場合の日時形式

［正規化パターン］の正規化ルールで「D」を指定した場合の，KEY 名称または項目位置の記述形式を次の表に示します。なお，KEY 名称または項目位置の記述形式は JP1/Audit Management - Manager で設定している日時形式と一致している必要があります。

表 13-6 「D」を指定した場合の日時形式

項番	記述形式		記述形式の意味
1	TYPE=KEY の場合	"YYYY-MM-DDThh:mm:ss.tttTZD"	• YYYY：年 • MM：月 • DD：日 • hh：時 • mm：分 • ss：秒 • ttt：ミリ秒 • T：日付と時刻の区切り文字 • TZD：タイムゾーン指定子 なお，TZD は次のどれかを指定してください。 • +hh:mm

項番	記述形式		記述形式の意味
			UTC（協定世界時）から hh:mm だけ進んでいることを示します。 • -hh:mm UTC（協定世界時）から hh:mm だけ遅れていることを示します。 • Z UTC（協定世界時）と同じことを示します。 なお，半角英数文字を使用してください。
2	TYPE=VALUE の場合	"YYYY/MM/DD△hh:mm:ss"または"MMM△DD△hh:mm:ss"	• YYYY：年 • MM：月 • DD：日 • hh：時 • mm：分 • ss：秒 • MMM：英語の月名称の省略形 月名称の省略形は，次のどれかを指定してください。 • Jan：1 月 • Feb：2 月 • Mar：3 月 • Apr：4 月 • May：5 月 • Jun：6 月 • Jul：7 月 • Aug：8 月 • Sep：9 月 • Oct：10 月 • Nov：11 月 • Dec：12 月 なお，複数の項目位置を定義する場合には，「,」で区切ってください。半角英数文字を使用してください。

(d) ［正規化パターン］の正規化ルールで「UD」を指定した場合の日時形式

［**正規化パターン**］の正規化ルールで「UD」を指定した場合に，項目 2 で定義する設定値について次の表に示します。

設定値を任意に組み合わせて，項目 2 で任意の日時形式を定義してください。監査ログの日時を示す値が，JP1/Audit Management - Manager で設定している日時形式と一致していない場合は，「UD」を指定し，監査ログの日時を示す値に合わせて日時形式を設定します。

表 13–7 「UD」を指定した場合に項目 2 で定義できる設定値

項番	項目 2 で定義する設定値	内容	設定値と対応する監査ログの値
1	%Y	西暦を指定します。	4 けたの数値です。
2	%y	西暦の下 2 けたを指定します。	2 けたの数値です。 なお，数字によって次のように認識します。 • 数字が 70～99 の場合 1970 年～1999 年と認識します。 • 数字が 00～69 の場合 2000 年～2069 年と認識します。
3	%m	月を数字で指定します。	01～12 または 1～12 の数値です。※
4	%B	月を英字の正式名で指定します。	対応する値を次に示します。なお，文字列の大文字・小文字を区別します。 • January：1 月 • February：2 月 • March：3 月 • April：4 月 • May：5 月 • June：6 月 • July：7 月 • August：8 月 • September：9 月 • October：10 月 • November：11 月 • December：12 月
5	%b	月を英字の省略名で指定します。	対応する値を次に示します。なお，文字列の大文字・小文字を区別します。 • Jan：1 月 • Feb：2 月 • Mar：3 月 • Apr：4 月 • May：5 月 • Jun：6 月 • Jul：7 月 • Aug：8 月 • Sep：9 月 • Oct：10 月 • Nov：11 月 • Dec：12 月
6	%d	日付を指定します。	01～31 または 1～31 の数値です。※

項番	項目 2 で定義する設定値	内容	設定値と対応する監査ログの値
7	%H	時単位の時刻を 24 時間表記で指定します。	00～23 または 0～23 の数値です。※
8	%I	時単位の時刻を 12 時間表記で指定します。	00～11 または 0～11 の数値です。※
9	%p	午前または午後のどちらかを指定します。	AM または PM です。
10	%M	分単位の時刻を指定します。	00～59 または 0～59 の数値です。※
11	%S	秒単位の時刻を指定します。	00～59 または 0～59 の数値です。※
12	%w	曜日を数字で指定します。	対応する値を次に示します。 • 0：日曜日 • 1：月曜日 • 2：火曜日 • 3：水曜日 • 4：木曜日 • 5：金曜日 • 6：土曜日
13	%A	曜日の英字の正式名で指定します。	対応する値を次に示します。なお，文字列の大文字・小文字を区別します。 • Sunday：日曜日 • Monday：月曜日 • Tuesday：火曜日 • Wednesday：水曜日 • Thursday：木曜日 • Friday：金曜日 • Saturday：土曜日
14	%a	曜日を英字の省略名で指定します。	対応する値を次に示します。なお，文字列の大文字・小文字を区別します。 • Sun：日曜日 • Mon：月曜日 • Tue：火曜日 • Wed：水曜日 • Thu：木曜日 • Fri：金曜日 • Sat：土曜日
15	%G	GMT 時間（世界標準時間）との時差を分単位で指定します。	-720～+720 の値の範囲です。
16	#	文字を読み飛ばしたい場合に指定します。	任意の 1 バイトを表します。

注※

日時を示す値が 1 文字（0～9）の場合は，「2007/9/11 3:15:10」のように，「/」や「:」などの区切り文字が必要です。

(e) ［正規化パターン］の正規化ルールで「UD」を指定した場合の日時形式の定義例

［正規化パターン］の正規化ルールで「UD」を指定した場合の，項目 2 での定義例を次の表に示します。

表 13–8 「UD」を指定した場合の項目 2 での定義例

項番	ログの日時形式	項目 2 の定義例
1	20070911031510	%Y%m%d%H%M%S
2	20070911031510+150	%Y%m%d%H%M%S%G
3	2007/9/11 03:15:10	"%Y/%m/%d %H:%M:%S"
4	2007/9/11 03:15:10.100	"%Y/%m/%d %H:%M:%S####"
5	2007 September 11 Wednesday 03-15-10	%Y %B %d %A %H-%M-%S
6	2007 Sep 11 Wed 03-15-10	%Y %b %d %a %H-%M-%S
7	2007/09/11 AM 03:15:10	"%Y/%m/%d %p %I:%M:%S"
8	07/09/11 03:15:10	"%y/%m/%d %I:%M:%S"
9	007/09/11 03:15:10	"%3Y/%m/%d %I:%M:%S"

注

項目 2 の定義の文字列に「:」が含まれる場合は，文字列全体を「"」で囲んでください。

13.2.4 定義内容（標準サポート外の Windows イベントログを収集する場合）

JP1/Audit Management - Manager で標準サポート外となっている Windows イベントログ（セキュリティに関する情報）を収集する場合に，［LOGTYPE］および［正規化パターン］で記述する内容についてそれぞれ説明します。

(1) ［LOGTYPE］の設定項目

［LOGTYPE］で記述する内容について，次の表に示します。

表 13–9 ［LOGTYPE］設定項目（標準サポート外の Windows イベントログを収集する場合）

項番	項目名	説明
1	［LOGTYPE］	定義の始まりを示す［LOGTYPE］を指定します。
2	TYPE	ログの記述形式として，次の値を指定します。 • WINEVENT

項番	項目名	説明
		Windows イベントログ（セキュリティに関する情報）用の正規化ルールファイルでは「WINEVENT」が指定されています。
3	SEPARATE	ログの区切り文字の種別です。次のどちらかを指定します。 • CRLF：改行コード（CR+LF） • nothing：区切り文字なし
4	SECTION	必ず「1」を指定します。 Windows イベント ID がセクション名として使用されます。
5	LOGSTART	必ず「0」を指定します。
6	ESCTYPE	ログ中でエスケープに使用する記号を指定します。次のどれかを指定します。 • 0：なし（エスケープしないログの場合） • 1：「"」 • 2：「"」以外の記号 なお，前後の文字が同じ場合は，「2」を指定できません。「0」を指定してください。この場合，エスケープ対象の文字列内に区切り文字が入らないようにしてください。
7	FRONTESC※	ESCTYPE が「2」の場合，エスケープに使用する開始記号を指定します。開始記号には，1 バイトの文字だけ指定できます。
8	REARESC※	ESCTYPE が「2」の場合，エスケープに使用する終了記号を指定します。終了記号には，1 バイトの文字だけ指定できます。
9	SKIPSPACE	連続する複数のスペースを一つのスペースとして処理するかどうかを指定します。SEPARATE が「CRLF」や「nothing」の場合，指定する必要はありません。

注

項番 9 以外の各項目名および各項目名の設定値は省略できません。

注※

FRONTESC と REARESC には同一の文字は指定できません。

(2) ［正規化パターン］の設定項目

［正規化パターン］で記述する内容について，次に示します。

(a) ［正規化パターン］の各項目の設定値

［正規化パターン］の各設定項目での設定値を次の表に示します。

表 13–10 ［正規化パターン］の各項目の設定値（標準サポート外の Windows イベントログ（セキュリティに関する情報）を収集する場合）

項番	番号	種別	正規化ルール	項目 1	項目 2	次番号 1	次番号 2	「正規化ルール」に「*」を指定したときの「項目 1」の範囲
1	1～の通番	AuditLogID※1	「*」	値や文字列を設定します。	×	次の番号	×	0～9999 の整数
2		MessageID	「W」	次に示す Windows イベントログの項目名を設定します。 • WinEventID：イベント ID	×	次の番号	×	－
3		MessageDate	「W」	次に示す Windows イベントログの項目名を設定します。 • WinEventDate：イベント発生日時	×	次の番号	×	－
4		ProgramName	「*」	値や文字列を設定します。	×	次の番号	×	63 バイト以内の文字列
5		ComponentName	「*」	値や文字列を設定します。	×	次の番号	×	63 バイト以内の文字列
			「W」	次に示す Windows イベントログの項目名を設定します。 • WinEventSource：イベントソース名				－
6		ProcessID※1	「*」	値や文字列を設定します。	×	次の番号	×	「-1」
7		PlaceInfo	「W」	次に示す Windows イベントログの項目名を設定します。 • WinEventPlace：コンピュータ名	×	次の番号	×	－
8		EventCategoryName	「*」	次に示す文字列のどれかを設定します。 • StartStop • Authentication • AccessControl • ConfigurationAccess • Failure • LinkStatus • ExternalService • ContentAccess • Maintenance	×	次の番号	×	－

項番	番号	種別	正規化ルール	項目 1	項目 2	次番号 1	次番号 2	「正規化ルール」に「*」を指定したときの「項目 1」の範囲
				• AnomalyEvent • ManagementAction				
9		EventResultName	「*」	次に示す文字列のどれかを設定します。 • Success • Failure • Occurrence	×	次の番号	×	−
			「W」	次に示す Windows イベントログの項目名を設定します。 • WinEventType：Windows イベントログの種類				
10		SubjectInfo	「*」	値や文字列を設定します。	×	次の番号	×	256 バイト以内の文字列
			「C」	次に示すカテゴリ名のどれかを設定します。 • "subj:euid"：実行ユーザ • "subj:uid"：アカウント識別子 • "subj:pid"：プロセス ID	項目名称			−
11		PeculiarInfo※2	「*」	値や文字列を設定します。	×	次の番号	×	1,024 バイト以内の文字列
			「A」	付加するタグ値	項目名称			−
			「E」	×	×			
			「L」					

（凡例）

×：指定しない。区切りの「:」も指定しない。

−：該当なし

注※1

「項目 1」に次の値を指定した場合，監査ログ管理画面上は空白が表示されます。

・AuditLogID：0

・ProcessID：-1

注※2

PeculiarInfo は，「E」を指定する場合，最後に定義する必要があります。

(b) ［正規化パターン］の設定項目

［正規化パターン］の設定項目を次の表に示します。

表 13–11 ［正規化パターン］設定項目（標準サポート外の Windows イベントログ（セキュリティに関する情報）を収集する場合）

項番	項目名	説明
1	［正規化パターン］	定義の始まりを示す［正規化パターン］を指定します。 Windows イベント ID を正規化パターン名として指定します。
2	番号	正規化ルールを適用する順番を 1 からの整数で指定します。
3	種別	正規化の対象となるデータ種別を指定します。指定値を次に示します。これらの値はすべて必須項目です。 • AuditLogID 監査ログの通番を設定する場合に指定します。 • MessageID 監査ログのメッセージ ID を設定する場合に指定します。 • MessageDate 監査ログの発生日時を設定する場合に指定します。 • ProgramName※1 監査ログの発生プログラム名を設定する場合に指定します。 • ComponentName※1 監査ログの発生コンポーネント名を設定する場合に指定します。 • ProcessID 監査ログの発生プロセス ID を設定する場合に指定します。 • PlaceInfo 監査ログの発生場所を設定する場合に指定します。 • EventCategoryName 監査ログのカテゴリ名を設定する場合に指定します。 • EventResultName 監査ログの結果を設定する場合に指定します。 • SubjectInfo 監査ログを発生させたユーザ名を設定する場合に指定します。 • PeculiarInfo※2 監査ログの詳細情報を設定する場合に指定します。
4	正規化ルール	正規化のルールを指定します。指定できる値を次に示します。 •「W」 項目 1 で定義する Windows イベントログの項目名を使用します。 •「*」 項目 1 で定義する値または文字列を使用します。 •「C」 項目 1 で定義するカテゴリの値を使用します。 •「A」

項番	項目名	説明
		項目 1 と項目 2 の値を使用します。 例えば，項目 1 で「"from：ipv4="」，項目 2 で指定した項目名称の値が「1.2.3.4」の場合，「from：ipv4=1.2.3.4」の値がデータベースに格納されます。 • 「E」 取得したメッセージのうち，利用していない部分をそのまま使用します。正規化ルールで「L」を指定した場合，「E」は指定できません。 • 「L」 取得したメッセージのすべてを使用します。正規化ルールで「E」，「*」を指定した場合，「L」は指定できません。
5	項目 1	項番 4 の正規化ルールに設定する値によって指定する情報が変わります。正規化ルールに設定した値の説明に記載されている情報を設定します。
6	項目 2	
7	次番号 1	適用する正規化ルールの次の key 値（項番 1）を指定します。最後の正規化ルールの場合は「0」を指定します。
8	次番号 2	

注

各項目は「:」で区切ります。

注※1

「ProgramName」は「ComponentName」の前に定義してください。

注※2

「PeculiarInfo」の場合で，かつ正規化ルールでの設定値が「E」の項目は最後に定義してください。

13.2.5 指定例

正規化ルールファイルの指定例については「付録 C 正規化ルールファイルの作成例」を参照してください。

13.2.6 注意事項

- JP1/AJS のスケジューラログでは，年の情報が出力されていない場合があります。この場合，次の方法で年の情報を追加して正規化します。
  - ログ中の月＜＝ログ取得の月：「取得した時点の年」の情報追加
  - ログ中の月＞ログ取得の月：「取得した時点の年 - 1」の情報追加

  例えば，ログ中の月が 12 月で，2007 年 1 月に取得した場合，2006 年 12 月として情報が追加されます。
- UNIX システムログの sulog を収集する場合，OS が出力するログには年の情報は出力されません。UNIX システムログ変換コマンドでは，次の方法で年の情報を追加して出力します。
  - 「ログ中の月＜＝ UNIX システムログの変換を実施した月」の場合
    「変換を実施した時点の年」の情報を追加。

- 「ログ中の月＞ UNIX システムログの変換を実施した月」の場合
  「変換を実施した時点の年 - 1」の情報を追加。

例えば，ログ中の月が 11 月で，2007 年 10 月に UNIX ログ変換を実施した場合，2006 年 11 月として情報が追加されます。なお，ファイルに 1 年以上のデータが蓄積されていた場合，年が正しく設定されないことがあります。

13.3　製品定義ファイル

製品定義ファイルは，監査ログを収集するためのログファイルトラップ機能の動作を決めるファイルです。このファイルは，監査ログ収集マネージャの［製品定義の編集］ダイアログで作成します。

ここでは，製品定義ファイルの格納先，書式，定義内容，および指定例について説明します。

JP1/Audit Management - Manager で標準サポート外となっているプログラムの場合でも，製品定義ファイルとあわせて，正規化ルールファイル，動作定義ファイル，および監査ログレポート定義ファイルを作成することによって，監査ログを管理・収集できるようになります。

標準サポート外のプログラムから監査ログを収集する方法については「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。なお，標準サポートしているプログラムの製品定義ファイルは編集しないでください。

13.3.1　ファイル名および格納先

製品定義ファイル名を次の表に示します。これらのファイルは削除しないでください。なお，製品定義ファイルを格納するフォルダは「JP1/Audit Management - Manager のインストール先フォルダ¥conf¥product」です。

表 13-12　製品定義ファイル名

項番	収集対象	ファイル名
1	Collaboration	Collaboration.conf
		Collaboration-FileSharing-Webdav.conf
2	Cosminexus	Cosminexus.conf
3	HiRDB	HiRDB.conf
4	Hitachi Navigation Platform	HitachiNavigationPlatform.conf
5	Hitachi Storage Command Suite（HP-UX）	HitachiStorageCommandSuite(HP-UX).conf
6	Hitachi Storage Command Suite（Solaris）	HitachiStorageCommandSuite(Solaris).conf
7	Hitachi Storage Command Suite（AIX）	HitachiStorageCommandSuite(AIX).conf
8	Hitachi Storage Command Suite（Linux）	HitachiStorageCommandSuite(Linux).conf
9	JP1/AJS2	JP1_AJS2.conf
10	JP1/AJS3	JP1_AJS3-host.conf
		JP1_AJS3-schedule[01-20].conf※1
11	JP1/AO	JP1_AO.conf
12	JP1/Base	JP1_Base.conf

項番	収集対象	ファイル名
13	JP1/Audit	JP1_NETM_Audit-Manager.conf
14	JP1/Audit の監査ログ管理画面（Web）	JP1_NETM_Audit-ManagerWeb.conf
15	JP1/IM - NP	JP1_IM-NP.conf
16	JP1/IM - SS	JP1_IM-SS.conf
17	JP1/ITDM	JP1_ITDM.conf
18	JP1/ITDM2	JP1_ITDM2.conf JP1_ITDM2-AC.conf JP1_ITDM2-DM.conf JP1_ITDM2-DMClient.conf
19	JP1/ITRM	JP1_ITRM.conf
20	JP1/NETM/AIM	JP1_NETM_AIM.conf
21	JP1/NETM/CSC - Agent	JP1_NETM_CSC-Agent.conf
22	JP1/NETM/CSC - Manager	JP1_NETM_CSC-Manager.conf
23	JP1/NETM/CSC - ManagerRemoteOption	JP1_NETM_CSC-ManagerRemoteOption.conf
24	JP1/NETM/DM	JP1_NETM_DM.conf
25	JP1/NETM/DM Client	JP1_NETM_DM-Client.conf
26	JP1/NETM/DM Manager	JP1_NETM_DM-Manager.conf
27	JP1/NETM/NM	JP1_NETM_NM-Manager.conf
28	JP1/PFM	JP1_PFM.conf
29	JP1/秘文	JP1_HIBUN.conf
30	OpenTP1	OpenTP1.conf
31	TRUST E2	VOS3_TRUST.conf
32	uCosminexus EUR Server	EUR.conf
33	uCosminexus Navigation Platform	CosminexusNavigationPlatform.conf
34	uCosminexus Portal Framework	CosminexusPortalFramework.conf
35	UNIX システムログ	UNIX_System_Log.conf
36	XDM/BASE E2	XDM.conf
37	活文 NAVIstaff	NAVIstaff.conf
38	標準サポート外のプログラム	製品名称※2.conf

注※1

JP1_AJS3-schedule01.conf～JP1_AJS3-schedule20.conf のファイルを表します。

注※2

監査ログを出力する収集対象プログラム名です。動作定義ファイルで定義した名称を使用します。なお製品名称に「_」を指定すると，［監査ログ収集マネージャ］ウィンドウでは「/」で表示されます。

13.3.2 書式

```
AuditLogNum=ログファイルの数↓
AuditLogName=ログファイル1↓
AuditLogName=ログファイル2↓
 :
RegularPattern=対応する正規化ルールファイルの名称↓
ReadOnly=編集権限の指定値↓
```

注

記述行の最後には，必ず改行を記述してください。

13.3.3 定義内容

製品定義ファイルに記述する内容を次の表に示します。なお，これらはすべて必須項目です。

表 13–13 製品定義ファイルの定義内容

項番	パラメーター	説明	設定値
1	AuditLogNum	監査対象プログラムの監査ログの数を定義します。	1～32 の整数を指定します。
2	AuditLogName	監査ログのファイル名を定義します。 AuditLogNum の数だけ存在します。	64 バイト以内の文字列で指定します。 使用できる文字を次に示します。 • 半角英数字 • 「¥」「:」「*」「?」「"」「<」「>>」「|」「△（半角スペース）」以外の半角記号 Windows イベントログから監査ログを収集する場合は，「nothing」と指定します。
3	RegularPattern	対応する正規化ルールファイル名を定義します。	255 バイト以内の文字列で指定します。 使用できる文字を次に示します。 • 半角英数字 • 「¥」「:」「*」「?」「"」「<」「>>」「|」「△（半角スペース）」以外の半角記号
4	ReadOnly	編集する権限を定義します。	次のどちらかを指定します。 • 0：監査ログ収集マネージャで編集できる • 1：監査ログ収集マネージャで編集できない（読み取り専用）

製品定義ファイルを記述する際の注意事項を次に示します。

- 1 カラム目から入力します。
- パラメーター行の最後には必ず改行を記述します。改行コードは，OS が Windows の場合は 0x0d0a，UNIX の場合は 0x0a を指定してください。

13.3.4 指定例

製品定義ファイルの指定例を次に示します。

指定例での条件

- 監査ログ収集対象プログラムの監査ログの数が 2
- 監査ログのファイル名が「log01.log」および「log02.log」
- 対応する正規化ルールファイル名が「xxxx.conf」

```
AuditLogNum=2
AuditLogName=log01.log
AuditLogName=log02.log
RegularPattern=xxxx.conf
ReadOnly=1
```

13.4　動作定義ファイル

動作定義ファイルは，監査ログ収集対象サーバ上の監査ログを収集するためのログファイルトラップ機能を起動するときに必要となるファイルです。

ここでは，動作定義ファイルの格納先について説明します。書式や定義内容は JP1/Base のログファイルトラップ機能の場合と同様です。書式，定義内容，および指定例の詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

JP1/Audit Management - Manager で標準サポート外となっているプログラムの場合でも，動作定義ファイルとあわせて，正規化ルールファイル，製品定義ファイル，および監査ログレポート定義ファイルを作成することによって，監査ログを管理・収集できるようになります。

標準サポート外のプログラムから監査ログを収集する方法については「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。なお，標準サポートしているプログラムの動作定義ファイルは編集しないでください。

13.4.1　ファイル名および格納先

動作定義ファイル名を次の表に示します。これらのファイルは削除しないでください。なお，動作定義ファイルを格納するフォルダは「JP1/Audit Management - Manager のインストール先フォルダ¥conf¥logdef」です。

表 13-14　動作定義ファイル名

項番	収集対象	ファイル名
1	Collaboration	admjevlog_Collaboration.conf
		admjevlog_Collaboration-FileSharing-Webdav.conf
2	Cosminexus	admjevlog_Cosminexus.conf
3	HiRDB	admjevlog_HiRDB.conf
4	Hitachi Navigation Platform	admjevlog_HitachiNavigationPlatform.conf
5	Hitachi Storage Command Suite（HP-UX）	admjevlog_HitachiStorageCommandSuite(HP-UX).conf
6	Hitachi Storage Command Suite（Solaris）	admjevlog_HitachiStorageCommandSuite(Solaris).conf
7	Hitachi Storage Command Suite（AIX）	admjevlog_HitachiStorageCommandSuite(AIX).conf
8	Hitachi Storage Command Suite（Linux）	admjevlog_HitachiStorageCommandSuite(Linux).conf
9	JP1/AJS2	admjevlog_JP1_AJS2.conf
10	JP1/AJS3	admjevlog_JP1_AJS3-host.conf
		admjevlog_JP1_AJS3-schedule[01-20].conf※1

項番	収集対象	ファイル名
11	JP1/AO	admjevlog_JP1_AO.conf
12	JP1/Base	admjevlog_JP1_Base.conf
13	JP1/Audit	admjevlog_JP1_NETM_Audit-Manager.conf
14	JP1/Audit の監査ログ管理画面（Web）	admjevlog_JP1_NETM_Audit-ManagerWeb.conf
15	JP1/IM - NP	admjevlog_JP1_IM-NP.conf
16	JP1/IM - SS	admjevlog_JP1_IM-SS.conf
17	JP1/ITDM	admjevlog_JP1_ITDM.conf
18	JP1/ITDM2	admjevlog_JP1_ITDM2.conf admjevlog_JP1_ITDM2-AC.conf admjevlog_JP1_ITDM2-DM.conf admjevlog_JP1_ITDM2-DMClient.conf
19	JP1/ITRM	admjevlog_JP1_ITRM.conf
20	JP1/NETM/AIM	admjevlog_JP1_NETM_AIM.conf
21	JP1/NETM/CSC - Agent	admjevlog_JP1_NETM_CSC-Agent.conf
22	JP1/NETM/CSC - Manager	admjevlog_JP1_NETM_CSC-Manager.conf
23	JP1/NETM/CSC - ManagerRemoteOption	admjevlog_JP1_NETM_CSC-ManagerRemoteOption.conf
24	JP1/NETM/DM	admjevlog_JP1_NETM_DM.conf
25	JP1/NETM/DM Client	admjevlog_JP1_NETM_DM-Client.conf
26	JP1/NETM/DM Manager	admjevlog_JP1_NETM_DM-Manager.conf
27	JP1/NETM/NM	admjevlog_JP1_NETM_NM-Manager.conf
28	JP1/PFM	admjevlog_JP1_PFM.conf
29	JP1/秘文	admjevlog_JP1_HIBUN.conf
30	OpenTP1	admjevlog_OpenTP1.conf
31	TRUST E2	admjevlog_VOS3_TRUST.conf
32	uCosminexus EUR Server	admjevlog_EUR.conf
33	uCosminexus Navigation Platform	admjevlog_CosminexusNavigationPlatform.conf
34	uCosminexus Portal Framework	admjevlog_CosminexusPortalFramework.conf
35	UNIX システムログ	admjevlog_UNIX_System_Log.conf
36	XDM/BASE E2	admjevlog_XDM.conf
37	活文 NAVIstaff	admjevlog_NAVIstaff.conf
38	標準サポート外のプログラム	admjevlog_製品名称※2.conf

注※1

admjevlog_JP1_AJS3-schedule01.conf～admjevlog_JP1_AJS3-schedule20.conf のファイルを表します。

注※2

監査ログを出力する収集対象プログラム名です。ここで指定した製品名称を製品定義ファイル名として使用します。ただし，製品名称に「/」が含まれる場合は，「_」に置き換えた製品名称を指定してください。動作定義ファイル名に使用できる文字を次に示します。

・半角英数字

・「¥」「:」「*」「?」「"」「<」「>」「|」「△（半角スペース）」以外の半角記号

また，正規化ルールエディタで正規化ルールを定義した場合，製品名称は製品情報のプロダクト名と一致させてください。製品情報の詳細については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

13.5　監査ログ標準レポート定義ファイル

監査ログの検索結果をレポート表示する際に，監査ログレポート画面の説明欄に表示する固有情報の内容を定義するファイルです。JP1/Audit Management - Manager で標準サポートしているプログラムについてはすでに定義されています。標準サポート外となっているプログラムの正規化ルールを正規化ルールエディタで定義する場合にだけ，このファイルを定義する必要があります。

なお，標準サポート外となっているプログラムの監査ログを収集する場合，この監査ログレポート定義ファイルのほかにも，定義するファイルが複数あります。標準サポート外となっているプログラムの監査ログを収集する場合の定義ファイルについては「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。

13.5.1　ファイル名および格納先

監査ログ標準レポート定義ファイル名およびファイル格納フォルダを次の表に示します。

表 13–15　監査ログ標準レポート定義ファイル名およびファイル格納フォルダ

ファイル名	ファイル格納フォルダ
admAnalysis.ini	JP1/Audit Management - Manager の仮想ディレクトリ¥conf

13.5.2　書式

```
[監査ログ上のプログラム名]↓
TYPE=Common↓
```

注

記述行の最後には，必ず改行を記述してください。

13.5.3　定義内容

監査ログ標準レポート定義ファイルに記述する内容を次の表に示します。

表 13–16　監査ログ標準レポート定義ファイルの定義内容

パラメーター	説明
[監査ログ上のプログラム名]	監査ログ上のプログラム名を指定します。監査ログ検索画面や監査ログ集計画面の「プログラム名」に表示される名前と一致させてください。

13.5.4 指定例

監査ログ標準レポート定義ファイルの指定例を次に示します。デフォルトで記述されている行の下に，記述を新しく追加してください。

```
[ProgramA]
TYPE=Common
```

13.6　監査ログレポート定義ファイル

JP1/Audit Management - Manager で標準サポート外となっているプログラムを収集対象とした場合で，かつ監査ログの検索結果をレポート表示する際に，監査ログレポート画面の説明欄に表示する固有情報の内容を定義するファイルです。

JP1/Audit Management - Manager で標準サポート外となっているプログラムの正規化ルールを正規化ルールファイルで定義した場合に，このファイルを定義する必要があります。

標準サポート外となっているプログラムの監査ログを収集する場合，この監査ログレポート定義ファイルのほかにも，定義するファイルが複数あります。標準サポート外となっているプログラムの監査ログを収集する場合の定義ファイルについては「5.6.2　標準サポート外のプログラムを収集対象とするための準備をする」を参照してください。

13.6.1　ファイル名および格納先

監査ログレポート定義ファイル名およびファイル格納フォルダを次の表に示します。

表 13-17　監査ログレポート定義ファイル名およびファイル格納フォルダ

ファイル名	ファイル格納フォルダ
admCommonAnalysis.ini	JP1/Audit Management - Manager の仮想ディレクトリ¥conf

13.6.2　書式

```
[監査ログ上のプログラム名]↓
DELIMITER=区切り文字↓
TAGn※=変換表示文字列↓
```

注

記述行の最後には，必ず改行を記述してください。

注※

n には 1～50 の半角数字を昇順で記述します。

13.6.3　定義内容

監査ログレポート定義ファイルに記述する内容を次の表に示します。

表 13–18　監査ログレポート定義ファイルの定義内容

項番	パラメーター	説明
1	[監査ログ上のプログラム名]	監査ログ上のプログラム名を指定します。監査ログ検索画面や監査ログ集計画面の「プログラム名」に表示される名前と一致させてください。
2	DELIMITER	区切り文字列を指定します。
3	TAGn	変換表示文字列を指定します。

13.6.4　指定例

監査ログレポート定義ファイルの指定例を次に示します。

```
[ProgramA]
DELIMITER=,
TAG1=ID1
TAG2=ID2
TAG3=ID3
[ProgramB]
DELIMITER=::
TAG1=MSG
TAG2=OBJ
[ProgramC]
DELIMITER=_
TAG1=固有情報
```

また，固有情報の例を次の表に示します。

項番	項目	固有情報の値
1	ProgramA の固有情報	Data1,Data2,Data3
2	ProgramB の固有情報	Message1::object1
3	ProgramC の固有情報	Content1

13.6.5　監査ログレポート画面の表示例

監査ログレポート画面の表示例を次の図に示します。

図 13–1　監査ログレポート画面の表示例

ProgramAの表示例

レポート

項番	発生日時	発生場所	利用者・プロセス情報	操作・処理内容	結果	説明	
1	2006/11/24 00:09:30.000	This is PlaceInfo 0020.	a	メンテナンス	失敗	プログラム名	ProgramA
						ID1	Data1
						ID2	Data2
						ID3	Data3

ProgramBの表示例

レポート

項番	発生日時	発生場所	利用者・プロセス情報	操作・処理内容	結果	説明	
1	2006/11/24 00:09:30.000	This is PlaceInfo 0020.	a	メンテナンス	失敗	プログラム名	ProgramB
						MSG	Message1
						OBJ	Object1

ProgramCの表示例

レポート

項番	発生日時	発生場所	利用者・プロセス情報	操作・処理内容	結果	説明	
1	2006/11/24 00:09:30.000	This is PlaceInfo 0020.	a	メンテナンス	失敗	プログラム名	ProgramC
						固有情報	Content1

13.7　バックアップオプション定義ファイル

バックアップオプション定義ファイルは，監査ログのバックアップおよび監査ログの移動をする際に，バックアップ実行履歴のバックアップ名称およびコメントを定義するファイルです。

次のコマンドを実行する際に，バックアップオプション定義ファイルを指定できます。

- admexport（監査ログのバックアップ）コマンド
- admcsvmove（監査ログバックアップファイルの移動）コマンド

13.7.1　ファイル名および格納先

バックアップオプション定義ファイル名および格納先のフォルダは，任意です。

13.7.2　書式

```
BackupName=バックアップ名↓
BackupComment=バックアップコメント↓
↓
```

注

記述行の最後には，必ず改行を記述してください。

バックアップ名およびバックアップコメントは省略できます。ただし，省略する場合でも「BackupName=」および「BackupComment=」は，必ず記述してください。

13.7.3　定義内容

バックアップオプション定義ファイルに記述する内容を次の表に示します。

表 13–19　バックアップオプション定義ファイルの定義内容

項番	パラメーター	説明	設定値
1	BackupName	バックアップ実行履歴に登録するバックアップ名称を指定します。 省略した場合は，次の名称が設定されます。 admexport コマンド実行時 -o オプションで指定した出力ファイル名 admcsvmove コマンド実行時 -d オプションで指定した移動先ファイル名	256 バイト以内の文字列
2	BackupComment	バックアップ実行履歴に登録するコメントを指定します。	

項番	パラメーター	説明	設定値
		省略した場合は，空文字が設定されます。	

13.7.4 指定例

バックアップオプション定義ファイルの指定例を次に示します。

```
BackupName=20070401-20070930
BackupComment=2007年度上半期の監査ログバックアップ
```

13.8　パターン情報ファイル

機能ツリーのパターンやフォルダの情報をエクスポートする際に，監査ログ管理サーバ上に出力されるCSV 形式ファイルです。このファイルをインポートすることによって，パターンやフォルダの情報をほかのサーバやユーザに移行できます。なお，インポートできるパターンやフォルダは 4,096 個までです。

13.8.1　ファイル名および格納先

パターン情報ファイル名および格納先のフォルダは，任意です。

13.8.2　書式

```
Path,NodeName,DisplayPage,Kind,AuditLogID,AuditLogIDCond,MessageID,Messagelevel,MessageIDCond,StartTimeStamp,EndTimeStamp,ProgramName,ComponentName,PlaceInfo,PlaceInfoCond,ProcessID,ProcessIDCond,EventCategoryID,EventResultID,SubjectInfo,SubjectCategoryID,SubjectInfoCond,PeculiarInfo,UnitTotal,TotalViewPoint,RecordCount↓
パス,ノード名,表示画面,種別,通番,通番条件,メッセージID,メッセージレベル,メッセージID条件,開始日時,終了日時,プログラム名,コンポーネント名,発生場所,発生場所条件,プロセスID,プロセスID条件,監査事象種別,監査事象結果,サブジェクト情報,サブジェクト情報の種別ID,サブジェクト情報の種別条件,固有情報,集計単位,集計観点,表示件数↓
```

注

記述行の最後には，必ず改行を記述してください。

各項目は「半角コンマ（,）」で区切って指定してください。

13.8.3　定義内容

パターン情報ファイルに記述する内容を次の表に示します。

表 13–20　パターン情報ファイルの定義内容

項番	分類	項目名	設定内容	設定値	デフォルト値	必須
1	機能ツリー情報	パス	パターンまたはフォルダのパスを設定します。 対象となるパターンまたはフォルダの一つ上のパスまでを設定してください。 例えば，ツリー項目の「監査ログ検索」配下の「フォルダ」にある「パターン」を対象とする場合は「¥監査ログ管理	1,024 バイト以内の文字列を設定します。	−	○

項番	分類	項目名	設定内容	設定値	デフォルト値	必須
			¥監査ログ検索¥フォルダ」と設定します。 設定時は次に示すことに注意してください。 • ルートは「¥」で示す			
2		ノード名	対象となるパターン名またはフォルダ名を設定します。 設定時は次に示すことに注意してください。 • 先頭に「@」は指定できない • 対象がフォルダの場合「¥」は指定できない • 同じノード名は指定できない	64 バイト以内の文字列を設定します。	−	○
3		表示画面	対象となる画面名を設定します。	次のどちらかを設定します。 • 0：「監査ログ検索画面」 この場合，パス（項番 1）はツリー項目の「監査ログ検索」配下を設定しておく必要があります。 • 1：「監査ログ集計画面」 この場合，パス（項番 1）はツリー項目の「監査ログ集計」配下を設定しておく必要があります。	−	○
4		種別	対象がフォルダかパターンかを設定します。	次のどちらかを設定します。 • 0：フォルダの場合 • 1：検索パターンまたは集計パターンの場合	−	○
5	パターン情報※1	通番	製品または製品のコンポーネントに対応する監査ログを特定するために連続した ID を設定します。	「1～2147483647」を設定します。	−	△
6		通番条件	通番で設定した数値に付加する条件を設定します。	次のどれかを設定します。	0	△

項番	分類	項目名	設定内容	設定値	デフォルト値	必須
				• 0：以下 • 1：等しい • 2：以上		
7		メッセージ ID	メッセージ ID を設定します。	64 バイト以内の文字列を設定します。	−	△
8		メッセージレベル	メッセージ ID のメッセージレベルを設定します。	次のどれかを設定します。 • 0：空白 • 1：「エラー」 • 2：「警告」 • 3：「情報」	0	△
9		メッセージ ID 条件	メッセージ ID の文字列付加条件を設定します。	次のどれかを設定します。 • 0：「完全一致」 • 1：「部分一致」 • 2：「前方一致」 • 3：「後方一致」	1	△
10		開始日時	監査ログの開始日時を設定します。	次の形式で設定します。 • YYYY/MM/DD△hh:mm:ss（年/月/日△時:分:秒） 「1900/01/01 00:00:00～9999/12/31 23:59:59」の範囲で設定してください。	−	△
11		終了日時	監査ログの終了日時を設定します。	次の形式で設定します。 • YYYY/MM/DD△hh:mm:ss（年/月/日△時:分:秒） 「1900/01/01 00:00:00～9999/12/31 23:59:59」の範囲で設定してください。	−	△
12		プログラム名	監査ログを収集しているプログラム名を設定します。 設定時は次に示すことに注意してください。	64 バイト以内の文字列を設定します。	−	△

項番	分類	項目名	設定内容	設定値	デフォルト値	必須
			• 1 文字当たり 2 バイト以上の文字列は使用できない			
13		コンポーネント名	監査ログを収集しているコンポーネント名を設定します。 設定時は次に示すことに注意してください。 • 1 文字当たり 2 バイト以上の文字列は使用できない	64 バイト以内の文字列を設定します。	−	△
14		発生場所	発生場所の IP アドレスおよびホスト名を設定します。	64 バイト以内の文字列を設定します。	−	△
15		発生場所条件	発生場所の文字列付加条件を設定します。	次のどれかを設定します。 • 0：「完全一致」 • 1：「部分一致」 • 2：「前方一致」 • 3：「後方一致」	1	△
16		プロセス ID	プロセス ID を設定します。	「0～2147483647」を設定します。	−	△
17		プロセス ID 条件	プロセス ID の数値付加条件を設定します。	次のどれかを設定します。 • 0：以下 • 1：等しい • 2：以上	0	△
18		監査事象種別	監査事象種別を設定します。	次のどれかを設定します。 • 0：空白 • 1：「StartStop」 • 2：「Authentication」 • 3：「AccessControl」 • 4：「ContentAccess」 • 5：「Failure」 • 6：「LinkStatus」 • 7：「ExternalService」 • 8：「ConfigurationAccess」 • 9：「Maintenance」	0	△

項番	分類	項目名	設定内容	設定値	デフォルト値	必須
				• 10：「AnomalyEvent」 • 11：「ManagementAction」		
19		監査事象結果	監査事象結果を設定します。	次のどれかを設定します。 • 0：空白 • 1：「Success」 • 2：「Failure」 • 3：「Occurrence」	0	△
20		サブジェクト情報	サブジェクト情報を設定します。	256 バイト以内の文字列を設定します。	−	△
21		サブジェクト情報の種別 ID	サブジェクト情報の種別 ID を設定します。	次のどれかを設定します。 • 0：空白 • 1：「AccountID」 • 2：「Effective UserID」 • 3：「ProcessID」	0	△
22		サブジェクト情報の種別条件	サブジェクト情報の文字列付加条件を設定します。	次のどれかを設定します。 • 0：「完全一致」 • 1：「部分一致」 • 2：「前方一致」 • 3：「後方一致」	1	△
23		固有情報	固有情報を設定します。	1,024 バイト以内の文字列を設定します。	−	△
24		集計単位 ※2	集計単位の種別を設定します。	次のどれかを設定します。 • 0：「発生場所」 • 1：「プログラム名」 • 2：「サブジェクト情報」	0	△
25		集計観点 ※2	集計観点の種別を設定します。	次のどちらかを設定します。 • 0：「監査事象種別」 • 1：「監査事象結果」	0	△
26		表示件数	表示件数を設定します。	「1～200」を設定します。	100	△

（凡例）

○：必ず設定する

△：必要に応じて設定する

－：なし

注※1

対象となるレコードが検索パターンまたは集計パターンの場合に設定します。対象となるレコードがフォルダの場合，各項目は空白を設定してください。

注※2

対象となるレコードが集計パターンの場合に設定します。対象となるレコードが検索パターンの場合，各項目は空白を設定してください。

13.8.4　指定例

パターン情報ファイルの指定例を次に示します。

```
"Path","NodeName","DisplayPage","Kind","AuditLogID","AuditLogIDCond","MessageID","Messagelevel","MessageIDCond",
"StartTimeStamp","EndTimeStamp","ProgramName","ComponentName","PlaceInfo","PlaceInfoCond","ProcessID","ProcessID
Cond","EventCategoryID","EventResultID","SubjectInfo","SubjectCategoryID","SubjectInfoCond","PeculiarInfo","Unit
Total","TotalViewPoint","RecordCount"
"¥監査ログ管理¥監査ログ検索¥","クライアントセキュリティ
","0","0","","","
```

13.9　監査ログ収集対象サーバセットアップ定義ファイル

監査ログ専用イベントサーバの環境情報を定義するファイルです。監査ログ収集対象サーバのセットアップ時に，admagtsetup コマンドでこのファイルを指定すると，定義内容に従って，監査ログ専用イベントサーバの環境が監査ログ収集対象サーバに作成されます。

13.9.1　ファイル名および格納先

監査ログ収集対象サーバセットアップ定義ファイル名および格納先のフォルダは任意です。

なお，JP1/Audit Management - Manager では，監査ログ収集対象サーバセットアップ定義ファイルのモデルファイルを提供しています。モデルファイルの格納先を次の表に示します。

表 13–21　監査ログ収集対象サーバセットアップ定義ファイルのモデルファイル名およびファイル格納先

項番	ファイル名	OS の種類 (監査ログ収集対象サーバ)	ファイルの格納先 (監査ログ収集対象サーバ)
1	admagtsetup.conf.model	Windows	• JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合 任意のインストールフォルダ¥conf • JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合 システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥manager¥conf
2		UNIX	• JP1/NETM/Audit - Manager 09-00 以降を新規インストールした場合 /etc/opt/jp1netmaudit/agent/conf • JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップした場合 /opt/jp1netmaudit/manager/conf

13.9.2　書式

```
[Host]↓
HostName=監査ログ収集対象サーバのホスト名↓
IPAddress=監査ログ収集対象サーバのIPアドレス↓
↓
[Cluster]↓
ClusterFlag={Y | N}↓
ClusterMode={ONLINE | STANDBY}↓
↓
[EventServer]↓
Directory=監査ログ専用フォルダ（監査ログ専用ディレクトリ）↓
```

```
TargetTransPort=監査ログ専用イベントサーバの転送用ポート番号↓
TargetAPPort=監査ログ専用イベントサーバのAP用ポート番号↓
DatabaseSize=監査ログ専用イベントデータベースのサイズ↓
ManagerHostName=監査ログ管理サーバのホスト名↓
ManagerIPAddress=監査ログ管理サーバのIPアドレス↓
ManagerTransPort=監査ログ管理サーバ上JP1/Baseのイベントサーバの転送用ポート番号↓
```

注

- 記述行の最後には，必ず改行を記述してください。なお，改行だけの行は無視されます。
- セクション名は，途中で改行を含めずに 1 行で記述してください。
- パラメーターおよび設定値は，途中で改行を含めずに 1 行で記述してください。
- パラメーターと「=」の間および「=」と設定値の間にスペースを記述しないでください。
- 行の先頭に「#」を記述すると，その行はコメントとして扱われます。

13.9.3 定義内容

監査ログ収集対象サーバセットアップ定義ファイルに記述する内容を次の表に示します。

表 13–22 監査ログ収集対象サーバセットアップ定義ファイルの定義内容

項番	セクション※1	パラメーター※2	説明	設定値	デフォルト※3	必須
1	Host	HostName	監査ログ収集対象サーバのホスト名を設定します。	64 バイト以内の文字列を設定します。使用できる文字を次に示します。 • 半角英数字 • 「-」	−	○
2		IPAddress	監査ログ収集対象サーバの IP アドレス（IPv4 アドレスまたは IPv6 アドレス）を設定します。 HostName に設定したホスト名に対応する IP アドレスを設定します。	IPv4 の場合は，「.」で区切った 10 進数を設定します。IPv6 の場合は，「:」で区切った 16 進数を設定します。※4，※5	−	○
3	Cluster	ClusterFlag	クラスタ環境用のセットアップをするかどうかを設定します。	次のどちらかを設定します。 • Y：クラスタ環境用のセットアップをする • N：クラスタ環境用のセットアップをしない	N	△

項番	セクション※1	パラメーター※2	説明	設定値	デフォルト※3	必須
4		ClusterMode	論理ホストが実行系サーバであるか，または待機系サーバであるかを設定します。	次のどちらかを設定します。 • ONLINE：論理ホストが実行系サーバである • STANDBY：論理ホストが待機系サーバである	−	△※6
5	EventServer	Directory	監査ログ専用フォルダ(監査ログ専用ディレクトリ）をフルパスで設定します。	128 バイト以内の文字列を設定します。使用できる文字を次に示します。 • 半角英数字 • 「△(半角スペース)」「!」「#」「$」「&」「(」「)」「+」「-」「,」「;」「=」「@」「_」「`」「{」「}」「[」「]」「~」「%」「^」	−	○
6		TargetTransPort	監査ログ専用イベントサーバの転送用ポート番号を設定します。デフォルトのポート番号がすでに使用されている場合に設定します。通常は設定する必要はありません。	5001～65535 の整数を設定します。	24101	△
7		TargetAPPort	監査ログ専用イベントサーバの AP 用ポート番号を設定します。デフォルトのポート番号がすでに使用されている場合に設定します。通常は設定する必要はありません。	5001～65535 の整数を設定します。	24102	△
8		DatabaseSize	監査ログ専用イベントデータベースのサイズをバイト単位で設定します。	10000000～2147483647 の整数で設定します。	10000000	△
9		ManagerHostName	監査ログ管理サーバのホスト名を設定します。	64 バイト以内の文字列を設定します。使用できる文字を次に示します。 • 半角英数字 • 「-」	−	○

項番	セクション※1	パラメーター※2	説明	設定値	デフォルト※3	必須
10		ManagerIPAddress	監査ログ管理サーバの IP アドレス（IPv4 アドレスまたは IPv6 アドレス）を設定します。 ManagerHostName に設定したホスト名に対応した IP アドレスを設定します。	IPv4 の場合は，「.」で区切った 10 進数を設定します。IPv6 の場合は，「:」で区切った 16 進数を設定します。※4，※5	−	○
11		ManagerTransPort	監査ログ管理サーバ上の JP1/Base のイベントサーバの転送用ポート番号を設定します。通常は設定する必要はありません。	5001～65535 の整数を設定します。	jp1imevt	△

（凡例）

○：必ず設定する

△：必要に応じて設定する

−：なし

注※1

ファイル内で同名のセクションが複数定義されている場合は，最初に定義されているセクションの定義内容が設定されます。

注※2

セクション内で同名のパラメーターが複数定義されている場合は，最初に定義されているパラメーターの値が設定されます。

注※3

デフォルトは，次のような場合に設定されます。

・省略できるパラメーターおよびその設定値を省略した場合

・省略できるパラメーターの設定値だけを省略した場合

注※4

設定できる IP アドレスの形式を次に示します。

IPv4 アドレスの場合：

aaa.bbb.ccc.ddd の形式で指定します。aaa～ddd は，最大 3 けたの 10 進数で設定してください。

IPv6 アドレスの場合：

・eeee:ffff:gggg:hhhh:iiii:jjjj:kkkk:llll の形式で指定します。eeee～llll は，最大 4 けたの 16 進数で設定してください。

・16 進数の英字部分（a～f）は，大文字と小文字の区別はありません。

・0000 が一つ以上連続する場合，1 回だけ「::」で省略できます。

・IPv4 互換アドレス（上位 96bit が 0 のアドレス）は設定できません。

・IPv4 射影アドレス（上位 80bit が 0，かつ上位 81bit から 96bit までの 16bit が 1 のアドレス）は設定できません。

注※5

IPAddress と ManagerIPAddress は，同じ形式の IP アドレスを設定してください。IPv4 アドレスと IPv6 アドレスが混在した設定はできません。

注※6

ClusterFlag の設定値が Y の場合は，必ず設定してください。ClusterFlag の設定値が N の場合は，設定不要です。

13.9.4　指定例

監査ログ収集対象サーバセットアップ定義ファイルの指定例を次に示します。

```
[Host]
HostName=logical-host01
IPAddress=172.16.1.10
[Cluster]
ClusterFlag=Y
ClusterMode=ONLINE
[EventServer]
Directory=S:¥Hitachi
TargetTransPort=
TargetAPPort=
DatabaseSize=
ManagerHostName=mgr-host01
ManagerIPAddress=172.16.1.100
ManagerTransPort=
```

14 メッセージ

この章では，監査証跡管理システムが出力するメッセージについて説明します。

14.1　メッセージの形式

この節では，監査証跡管理システムが出力するメッセージの形式とマニュアルでの記載形式について説明します。

14.1.1　メッセージの出力形式

ここでは，標準出力，標準エラー出力，およびメッセージログファイルに出力されるメッセージの見方について説明します。個々のメッセージについては「14.3　メッセージ一覧」を参照してください。

(1)　標準出力または標準エラー出力の場合

標準出力または標準エラー出力に出力されるメッセージの形式を次に示します。

```
KDSxnnnn-m メッセージテキスト
```

- KDSx：メッセージを出力したプログラムが JP1/Audit Management - Manager であることを示す識別子です。「KDSO」と「KDSP」の 2 種類があります。
- nnnn：メッセージの通番です。
- m：メッセージの種別（E：エラー，W：警告，I：情報）です。
- メッセージテキスト：メッセージの内容です。

(2)　メッセージログファイルの場合

メッセージログファイルに出力されるメッセージの形式を次に示します。

```
YYYYMMDDhhmmss.ttt pid(tid) KDSxnnnn-m メッセージテキスト
```

- YYYYMMDDhhmmss.ttt：メッセージの出力日時です。YYYY：年，MM：月，DD：日，hh：時，mm：分，ss：秒，ttt：ミリ秒を示します。
- pid：メッセージを出力したプロセス ID です。
- tid：メッセージを出力したスレッド ID です。

「KDSx」以降は「(1)　標準出力または標準エラー出力の場合」と同様です。

14.1.2　メッセージの記載形式

このマニュアルでのメッセージの記載形式を次に示します。メッセージは，メッセージ ID 順に記載しています。また，メッセージ中の可変値を斜体（イタリック）で示しています。

メッセージ ID

メッセージテキスト

メッセージの説明文

(S)

システムの処置を示します。

(O)

メッセージが出力されたときに，ユーザが取る処置を示します。

14.2　メッセージの出力先一覧

メッセージの出力先について説明します。

14.2.1　KDSO0001-I～KDSO2477-W のメッセージの出力先

KDSO0001-I～KDSO2477-W のメッセージの出力先には，次に示す種類があります。

- 標準出力
- 標準エラー出力
- メッセージログファイル
- Windows イベントログ
- メッセージダイアログ

メッセージ ID ごとの出力先を次の表に示します。

表 14–1　KDSO0001-I～KDSO2477-W のメッセージ ID ごとの出力先

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0001-I～KDSO0002-I	－	－	○	－	－	－
KDSO0004-E～KDSO0016-E	－	－	○	－	－	－
KDSO0101-E	－	○	－	－	－	－
KDSO0102-E	－	○	○	－	－	－
KDSO0103-I	○	－	○	－	－	－
KDSO0104-I～KDSO0105-E	○	－	○	－	－	○
KDSO0106-E～KDSO0111-E	－	○	○	－	－	－
KDSO0112-I	○	－	○	－	－	－
KDSO0113-W	－	○	○	－	－	－
KDSO0114-E～KDSO0121-E	－	○	－	－	－	－
KDSO0122-E～	－	○	○	－	－	－

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0123-W						
KDSO0124-I	○	−	○	−	−	−
KDSO0125-E～KDSO0127-W	−	○	○	−	−	−
KDSO0128-E～KDSO0130-E	−	○	−	−	−	−
KDSO0131-E	−	○	○	−	−	−
KDSO0132-I	○	−	○	−	−	−
KDSO0133-E	−	○	○	−	−	−
KDSO0134-I	○	−	○	−	−	−
KDSO0135-E	−	○	○	−	−	−
KDSO0136-I～KDSO0137-I	○	−	○	−	−	−
KDSO0138-E～KDSO0141-E	−	○	○	−	−	−
KDSO0151-E	−	○	−	−	−	−
KDSO0152-E	−	○	○	−	−	−
KDSO0153-I	○	−	○	−	−	−
KDSO0154-I～KDSO0155-E	○	−	○	−	−	○
KDSO0156-E～KDSO0160-E	−	○	○	−	−	−
KDSO0162-E	−	○	○	−	−	−
KDSO0164-E～KDSO0168-E	−	○	−	−	−	−
KDSO0169-E～KDSO0170-E	−	○	○	−	−	−
KDSO0172-E～KDSO0174-E	−	○	○	−	−	−
KDSO0175-E	−	○	−	−	−	−
KDSO0176-E	−	○	○	−	−	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0177-I	○	−	○	−	−	−
KDSO0178-E～KDSO0179-E	−	○	○	−	−	−
KDSO0180-E～KDSO0181-E	−	○	−	−	−	−
KDSO0182-E～KDSO0183-E	−	○	○	−	−	−
KDSO0184-E	−	○	−	−	−	−
KDSO0185-E～KDSO0188-E	−	○	○	−	−	−
KDSO0189-I	○	−	○	−	−	−
KDSO0190-E～KDSO0192-E	−	○	○	−	−	−
KDSO0193-E～KDSO0194-E	−	○	−	−	−	−
KDSO0195-I～KDSO0198-I	○	−	○	−	−	−
KDSO0199-E	−	○	○	−	−	−
KDSO0200-I	○	−	○	−	−	−
KDSO0201-E	−	○	−	−	−	−
KDSO0202-E	−	○	○	−	−	−
KDSO0203-I	○	−	○	−	−	−
KDSO0204-I～KDSO0205-E	○	−	○	−	−	○
KDSO0206-E～KDSO0208-E	−	○	○	−	−	−
KDSO0211-E～KDSO0213-E	−	○	○	−	−	−
KDSO0214-E～KDSO0218-E	−	○	−	−	−	−
KDSO0219-E～KDSO0221-E	−	○	○	−	−	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0222-E	−	○	−	−	−	−
KDSO0223-E～KDSO0226-E	−	○	○	−	−	−
KDSO0227-E～KDSO0230-E	−	○	−	−	−	−
KDSO0231-E～KDSO0232-E	−	○	○	−	−	−
KDSO0233-E	−	○	−	−	−	−
KDSO0401-E～KDSO0406-E	−	○	−	−	−	−
KDSO0407-E	−	○	○	−	−	−
KDSO0408-I	○	−	○	−	−	−
KDSO0409-I～KDSO0410-E	○	−	○	−	−	○
KDSO0411-I	○	−	○	−	−	−
KDSO0412-E～KDSO0416-E	−	○	○	−	−	−
KDSO0417-E～KDSO0421-E	−	○	−	−	−	−
KDSO0422-E～KDSO0424-E	−	○	○	−	−	−
KDSO0425-E	−	○	−	−	−	−
KDSO0451-E～KDSO0456-E	−	○	−	−	−	−
KDSO0457-E	−	○	○	−	−	−
KDSO0458-I	○	−	○	−	−	−
KDSO0459-I～KDSO0460-E	○	−	○	−	−	○
KDSO0461-I	○	−	○	−	−	−
KDSO0462-E～KDSO0466-E	−	○	○	−	−	−
KDSO0467-E～	−	○	−	−	−	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0471-E						
KDSO0472-E～KDSO0475-E	－	○	○	－	－	－
KDSO0476-E	－	○	－	－	－	－
KDSO0501-E～KDSO0506-E	－	○	－	－	－	－
KDSO0507-E	－	○	○	－	－	－
KDSO0508-I	○	－	○	－	－	－
KDSO0509-I～KDSO0510-E	○	－	○	－	－	○
KDSO0511-I	○	－	○	－	－	－
KDSO0512-E～KDSO0514-E	－	○	○	－	－	－
KDSO0515-E～KDSO0518-E	－	○	－	－	－	－
KDSO0519-E～KDSO0523-E	－	○	○	－	－	－
KDSO0551-E～KDSO0556-E	－	○	－	－	－	－
KDSO0557-E	－	○	○	－	－	－
KDSO0558-I	○	－	○	－	－	－
KDSO0559-I～KDSO0560-E	○	－	○	－	－	－
KDSO0561-E～KDSO0562-E	－	○	○	－	－	－
KDSO0563-E	－	○	－	－	－	－
KDSO0564-I	○	－	○	－	－	－
KDSO0565-W	－	○	○	－	－	－
KDSO0601-E～KDSO0606-E	－	○	－	－	－	－
KDSO0607-E	－	○	○	－	－	－
KDSO0608-I	○	－	○	－	－	－

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0609-I～KDSO0610-E	○	−	○	−	−	○
KDSO0611-I	○	−	○	−	−	−
KDSO0612-E～KDSO0614-E	−	○	○	−	−	−
KDSO0615-E～KDSO0618-E	−	○	−	−	−	−
KDSO0619-E～KDSO0621-E	−	○	○	−	−	−
KDSO0651-E～KDSO0656-E	−	○	−	−	−	−
KDSO0657-E	−	○	○	−	−	−
KDSO0658-I	○	−	○	−	−	−
KDSO0659-I～KDSO0660-E	○	−	○	−	−	○
KDSO0661-I	○	−	○	−	−	−
KDSO0662-E～KDSO0666-E	−	○	○	−	−	−
KDSO0667-E～KDSO0671-E	−	○	−	−	−	−
KDSO0672-E～KDSO0678-E	−	○	○	−	−	−
KDSO0701-E～KDSO0706-E	−	○	−	−	−	−
KDSO0707-E	−	○	○	−	−	−
KDSO0708-I	○	−	○	−	−	−
KDSO0709-I～KDSO0710-E	○	−	○	−	−	○
KDSO0711-I	○	−	○	−	−	−
KDSO0712-E～KDSO0713-E	−	○	○	−	−	−
KDSO0715-E～KDSO0717-E	−	○	○	−	−	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0718-E	−	○	−	−	−	−
KDSO0719-E	−	○	○	−	−	−
KDSO0720-E～KDSO0721-E	−	○	−	−	−	−
KDSO0723-E	−	○	○	−	−	−
KDSO0724-E	−	○	−	−	−	−
KDSO0725-E～KDSO0727-E	−	○	○	−	−	−
KDSO0728-I	○	−	○	−	−	−
KDSO0729-E～KDSO0732-E	−	○	○	−	−	−
KDSO0751-E～KDSO0756-E	−	○	−	−	−	−
KDSO0757-E	−	○	○	−	−	−
KDSO0758-I	○	−	○	−	−	−
KDSO0759-I～KDSO0760-E	○	−	○	−	−	○
KDSO0761-I	○	−	○	−	−	−
KDSO0762-E～KDSO0768-E	−	○	○	−	−	−
KDSO0769-E～KDSO0773-E	−	○	−	−	−	−
KDSO0774-E～KDSO0777-E	−	○	○	−	−	−
KDSO0801-E～KDSO0806-E	−	○	−	−	−	−
KDSO0807-E	−	○	○	−	−	−
KDSO0808-I	○	−	○	−	−	−
KDSO0809-I～KDSO0810-E	○	−	○	−	−	○
KDSO0811-I	○	−	○	−	−	−
KDSO0812-E	−	○	−	−	−	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO0813-E～KDSO0816-E	－	○	○	－	－	－
KDSO0817-E～KDSO0818-E	－	○	－	－	－	－
KDSO0819-I	○	－	○	－	－	－
KDSO0851-E～KDSO0856-E	－	○	－	－	－	－
KDSO0857-E	－	○	○	－	－	－
KDSO0858-I	○	－	○	－	－	－
KDSO0859-I～KDSO0860-E	○	－	○	－	－	○
KDSO0861-I	○	－	○	－	－	－
KDSO0862-E	－	○	－	－	－	－
KDSO0863-E～KDSO0866-E	－	○	○	－	－	－
KDSO0868-E～KDSO0869-E	－	○	－	－	－	－
KDSO0901-E～KDSO0911-E	－	○	－	－	－	－
KDSO1000-E	－	－	○	－	－	－
KDSO1019-E	－	－	○	－	－	－
KDSO1030-E～KDSO1032-E	－	－	○	－	－	－
KDSO1036-W～KDSO1041-W	－	－	○	－	－	－
KDSO1043-E～KDSO1044-E	－	－	○	－	－	－
KDSO1046-W	－	－	○	－	－	－
KDSO1101-I	○	－	○	－	－	－
KDSO1102-E～KDSO1103-E	－	○	○	－	－	－
KDSO1500-I～	－	－	○	○	－	○

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO1502-E						
KDSO1503-E	−	−	○	○	−	−
KDSO1504-E～KDSO1518-W	−	−	○	−	−	−
KDSO1601-I～KDSO1603-E	−	−	○	○	−	○
KDSO1604-E	−	−	○	○	−	−
KDSO1605-I～KDSO1611-W	−	−	○	−	−	−
KDSO1651-E～KDSO1656-E	−	○	−	−	−	−
KDSO1657-E～KDSO1658-E	−	○	○	−	−	−
KDSO1659-I～KDSO1660-E	○	−	○	−	−	○
KDSO1661-I	○	−	○	−	−	−
KDSO1662-E	−	○	−	−	−	−
KDSO2001-I	−	−	○	−	−	○
KDSO2002-E～KDSO2003-E	−	−	○	−	○	−
KDSO2004-E	−	−	○	−	○	○
KDSO2009-I	−	−	−	−	○	−
KDSO2018-W	−	−	−	−	○	−
KDSO2020-E～KDSO2024-E	−	−	−	−	○	−
KDSO2026-E～KDSO2030-E	−	−	−	−	○	−
KDSO2033-E	−	−	−	−	○	−
KDSO2040-E	−	−	−	−	○	−
KDSO2043-E～KDSO2044-W	−	−	−	−	○	−
KDSO2052-I～	−	−	○	−	−	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO2053-I						
KDSO2054-E	−	−	○	−	○	−
KDSO2055-E～KDSO2056-E	−	−	−	−	○	−
KDSO2200-W～KDSO2201-E	−	−	○	−	○	−
KDSO2202-E～KDSO2205-E	−	−	−	−	○	−
KDSO2206-E	−	−	○	−	○	−
KDSO2207-E～KDSO2209-E	−	−	−	−	○	−
KDSO2211-E～KDSO2216-I	−	−	−	−	○	−
KDSO2225-I	−	−	○	−	○	○
KDSO2226-I～KDSO2230-I	−	−	−	−	○	−
KDSO2231-I～KDSO2232-E	−	−	○	−	○	−
KDSO2233-E	−	−	○	−	○	○
KDSO2234-E～KDSO2238-E	−	−	−	−	○	−
KDSO2239-E	−	−	○	−	○	−
KDSO2240-E～KDSO2241-E	−	−	○	−	−	−
KDSO2244-E	−	−	○	−	○	−
KDSO2245-E～KDSO2247-E	−	−	−	−	○	−
KDSO2248-E～KDSO2250-E	−	−	○	−	○	○
KDSO2251-I～KDSO2252-I	−	−	○	−	−	○
KDSO2253-I	−	−	○	−	○	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO2254-I	−	−	○	−	−	−
KDSO2255-I～KDSO2256-E	−	−	○	−	○	○
KDSO2257-E	−	−	−	−	○	−
KDSO2258-E～KDSO2260-E	−	−	○	−	○	−
KDSO2261-E～KDSO2262-E	−	−	−	−	○	−
KDSO2400-W～KDSO2404-E	−	−	○	−	○	−
KDSO2405-I～KDSO2408-I	−	−	○	−	−	−
KDSO2409-I～KDSO2415-I	−	−	−	−	○	−
KDSO2416-W～KDSO2419-E	−	−	○	−	○	−
KDSO2420-E～KDSO2425-E	−	−	−	−	○	−
KDSO2426-E～KDSO2432-E	−	−	○	−	○	−
KDSO2434-E	−	−	−	−	○	−
KDSO2435-I～KDSO2440-E	−	−	○	−	−	○
KDSO2442-E～KDSO2443-E	−	−	−	−	○	−
KDSO2444-I～KDSO2445-I	−	−	○	−	−	−
KDSO2446-I～KDSO2447-E	−	−	○	−	−	○
KDSO2448-E～KDSO2449-E	−	−	○	−	○	−
KDSO2450-E～KDSO2452-E	−	−	−	−	○	−

メッセージ ID	出力先					
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	メッセージダイアログ	監査ログ
KDSO2453-I～KDSO2455-E	－	－	○	－	－	－
KDSO2456-W	－	－	－	－	○	－
KDSO2457-I～KDSO2458-E	－	－	○	－	○	○
KDSO2459-I～KDSO2461-I	－	－	－	－	○	－
KDSO2462-I～KDSO2467-E	－	－	○	－	－	○
KDSO2468-I～KDSO2477-W	－	－	－	－	○	－

（凡例）

○：メッセージの出力あり

－：メッセージの出力なし

14.2.2 KDSO3001-E～KDSO3853-E のメッセージの出力先

KDSO3001-E～KDSO3853-E のメッセージの出力先には，次に示す種類があります。

- ログファイル
- ダイアログ
- 監査ログ管理画面
- 監査ログ

メッセージ ID ごとの出力先を次の表に示します。なお，メッセージの種別が「E：エラー」の場合，メッセージテキストに続けて詳細情報が追加されることがあります。

表 14–2 KDSO3001-E～KDSO3853-E のメッセージ ID ごとの出力先

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3001-E～KDSO3004-E	○	－	○	○
KDSO3005-W～KDSO3006-I	－	－	○	－

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3007-E～ KDSO3009-E	○	−	○	○
KDSO3010-I	○	−	−	−
KDSO3011-I	○	−	○	○
KDSO3012-I	○	−	−	−
KDSO3013-I	○	−	−	○
KDSO3014-I	○	−	○	−
KDSO3015-E～ KDSO3017-E	○	−	○	○
KDSO3050-E	○	−	○	○
KDSO3053-W	−	○	−	−
KDSO3054-E～ KDSO3060-E	○	−	○	○
KDSO3061-I	○	−	−	−
KDSO3062-I	○	−	−	○
KDSO3063-I	○	−	−	−
KDSO3064-I	○	−	−	○
KDSO3101-W～ KDSO3102-W	−	○	−	−
KDSO3103-E～ KDSO3108-E	○	−	○	−
KDSO3112-I～ KDSO3113-I	○	−	−	−
KDSO3116-I～ KDSO3117-I	○	−	−	−
KDSO3118-I～ KDSO3123-I	−	○	−	−
KDSO3124-I～ KDSO3125-I	○	−	−	−
KDSO3126-E～ KDSO3128-E	○	−	○	−
KDSO3151-E	○	−	−	○

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3152-W～ KDSO3154-I	－	○	－	－
KDSO3156-E～ KDSO3157-I	○	－	－	○
KDSO3161-E～ KDSO3163-E	○	－	○	○
KDSO3165-E～ KDSO3172-E	○	－	○	○
KDSO3173-E～ KDSO3181-E	○	－	○	－
KDSO3182-W～ KDSO3183-W	－	○	－	－
KDSO3186-I	○	－	－	－
KDSO3187-I	○	－	－	○
KDSO3188-I	○	－	－	－
KDSO3189-I	○	－	－	○
KDSO3190-I～ KDSO3195-I	○	－	－	－
KDSO3196-E	○	－	○	○
KDSO3197-I	○	－	－	－
KDSO3198-I	○	－	－	○
KDSO3199-I	○	－	－	－
KDSO3200-I	○	－	－	○
KDSO3201-E～ KDSO3203-E	○	－	○	○
KDSO3204-I～ KDSO3206-W	－	○	－	－
KDSO3207-I	○	－	－	－
KDSO3208-I	○	－	－	○
KDSO3209-E～ KDSO3211-E	○	－	○	○
KDSO3212-E	○	－	○	－

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3213-I	−	−	○	−
KDSO3214-I～ KDSO3215-I	○	−	−	−
KDSO3216-E～ KDSO3217-E	○	−	○	−
KDSO3218-W	−	○	−	−
KDSO3219-E	○	−	○	−
KDSO3220-E～ KDSO3221-E	○	−	○	○
KDSO3225-E～ KDSO3227-E	○	−	○	−
KDSO3228-E	○	−	○	○
KDSO3229-E	○	−	○	−
KDSO3230-E～ KDSO3231-I	○	−	−	○
KDSO3232-E	○	−	○	○
KDSO3233-I～ KDSO3234-I	○	−	−	−
KDSO3235-I～ KDSO3236-I	○	−	−	○
KDSO3237-E～ KDSO3243-E	○	−	○	○
KDSO3244-I	○	−	−	−
KDSO3245-I	○	−	−	○
KDSO3246-E～ KDSO3249-E	○	−	○	○
KDSO3251-E～ KDSO3252-E	○	−	−	−
KDSO3253-E～ KDSO3257-E	○	−	○	−
KDSO3258-I～ KDSO3263-I	○	−	−	−
KDSO3264-E～	○	−	○	−

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3266-E				
KDSO3267-I～ KDSO3269-W	○	−	−	−
KDSO3270-I～ KDSO3273-I	−	○	−	−
KDSO3274-E～ KDSO3276-E	○	−	○	○
KDSO3301-I～ KDSO3302-I	○	−	−	−
KDSO3303-E～ KDSO3305-E	○	−	○	−
KDSO3306-W～ KDSO3318-W	−	○	−	−
KDSO3320-W～ KDSO3321-W	−	○	−	−
KDSO3323-W	−	○	−	−
KDSO3325-E～ KDSO3328-E	○	−	○	−
KDSO3329-I	○	−	−	−
KDSO3330-E～ KDSO3338-W	○	−	○	−
KDSO3339-I～ KDSO3340-I	○	−	−	−
KDSO3341-E～ KDSO3345-E	○	−	○	−
KDSO3346-I	○	−	−	−
KDSO3347-E～ KDSO3348-E	○	−	○	−
KDSO3349-I	−	○	−	−
KDSO3350-E	○	−	○	−
KDSO3502-I～ KDSO3503-E	○	−	−	○
KDSO3505-I～ KDSO3506-E	○	−	−	−

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3508-I～ KDSO3509-E	○	−	−	−
KDSO3511-I～ KDSO3512-E	○	−	−	−
KDSO3514-I～ KDSO3515-E	○	−	−	−
KDSO3517-I～ KDSO3518-E	○	−	−	−
KDSO3520-I～ KDSO3521-E	○	−	−	○
KDSO3523-I～ KDSO3524-E	○	−	−	○
KDSO3526-I～ KDSO3527-E	○	−	−	−
KDSO3529-I～ KDSO3540-E	○	−	−	−
KDSO3541-I～ KDSO3544-E	○	−	−	○
KDSO3547-I～ KDSO3548-E	○	−	−	○
KDSO3549-E～ KDSO3575-I	○	−	−	−
KDSO3752-I～ KDSO3753-E	○	−	−	○
KDSO3754-E～ KDSO3762-I	○	−	−	−
KDSO3763-E	○	−	−	○
KDSO3764-E	○	−	−	−
KDSO3802-I	○	−	−	○
KDSO3804-E	○	−	−	○
KDSO3805-E～ KDSO3807-E	○	−	−	−
KDSO3851-I	○	−	−	○
KDSO3852-W～	○	−	−	−

メッセージ ID	出力先			
	ログファイル	ダイアログ	監査ログ管理画面※	監査ログ
KDSO3853-E				

（凡例）

○：メッセージの出力あり

－：メッセージの出力なし

注※

監査ログ管理画面に出力される場合には，パラメーターは表示されません。

14.2.3 KDSP0001-I～KDSP2903-E のメッセージの出力先

KDSP0001-I～KDSP2903-E のメッセージの出力先には，次に示す種類があります。

- 標準出力
- 標準エラー出力
- メッセージログファイル
- Windows イベントログ

メッセージ ID ごとの出力先を次の表に示します。

表 14–3 KDSP0001-I～KDSP2903-E のメッセージ ID ごとの出力先

メッセージ ID	出力先				
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	監査ログ
KDSP0001-I	－	－	○	○	－
KDSP0002-I	－	－	○	○	○
KDSP0008-I～KDSP0009-E	－	－	○	－	○
KDSP0010-I	－	－	○	－	－
KDSP0011-I～KDSP0012-I	－	－	○	－	－
KDSP0016-I	－	－	○	－	－
KDSP0119-W	－	－	○	－	－
KDSP0200-E	－	－	○	○	－
KDSP0402-W～KDSP0404-E	－	－	○	○	－

メッセージ ID	出力先				
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	監査ログ
KDSP0405-I～ KDSP0406-I	－	－	○	－	○
KDSP0407-I～ KDSP0408-I	－	－	○	－	－
KDSP0602-E～ KDSP0603-I	－	－	○	－	－
KDSP0610-E	－	－	○	－	－
KDSP0612-E～ KDSP0614-E	－	－	○	○	－
KDSP0616-E～ KDSP0617-E	－	－	○	○	－
KDSP0618-I	－	－	○	－	－
KDSP0628-E	－	－	○	○	－
KDSP0702-W～ KDSP0703-E	－	－	○	○	－
KDSP0711-E	－	－	○	－	－
KDSP0715-I～ KDSP0716-I	－	－	○	－	－
KDSP0719-I	－	－	○	－	－
KDSP0721-W～ KDSP0723-W	－	－	○	－	－
KDSP0725-E	－	－	○	○	－
KDSP0736-W～ KDSP0737-W	－	－	○	－	－
KDSP0800-E	－	－	○	○	－
KDSP0801-E～ KDSP0803-E	－	－	○	－	－
KDSP0900-E～ KDSP0904-E	－	－	○	○	－
KDSP0906-E	－	－	○	○	－
KDSP0911-E	－	－	○	－	－
KDSP0912-E～	－	－	○	○	－

メッセージ ID	出力先				
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	監査ログ
KDSP0915-E					
KDSP0916-E	−	−	○	−	−
KDSP0997-E	−	−	−	○	−
KDSP2000-I	○	−	○	−	−
KDSP2001-I	○	−	○	−	○
KDSP2002-E	−	○	○	−	○
KDSP2003-I～ KDSP2004-I	○	−	○	−	−
KDSP2005-E	−	○	○	−	−
KDSP2006-I	○	−	○	−	−
KDSP2007-I	○	−	○	−	○
KDSP2008-E	−	○	○	−	○
KDSP2009-I	○	−	○	−	−
KDSP2010-I	○	−	○	−	○
KDSP2011-E	−	○	○	−	○
KDSP2100-E～ KDSP2103-E	−	○	○	−	−
KDSP2104-E～ KDSP2107-E	−	○	○	−	−
KDSP2108-E	−	○	○	−	−
KDSP2110-E	−	−	○	−	−
KDSP2120-E	−	○	○	−	−
KDSP2202-I～ KDSP2203-I	○	−	○	−	−
KDSP2210-E～ KDSP2211-E	−	○	○	−	−
KDSP2500-E～ KDSP2502-E	−	○	○	−	−
KDSP2600-E～ KDSP2615-W	−	○	○	−	−
KDSP2620-I～	○	−	○	−	−

メッセージ ID	出力先				
	標準出力	標準エラー出力	メッセージログファイル	Windows イベントログ	監査ログ
KDSP2623-I					
KDSP2630-E～ KDSP2631-E	－	○	○	－	－
KDSP2800-I～ KDSP2801-I	○	－	○	－	－
KDSP2810-W	－	○	○	－	－
KDSP2820-W	－	○	○	－	－
KDSP2830-W	－	○	○	－	－
KDSP2900-E	－	○	○	－	－
KDSP2901-E	－	－	○	－	－
KDSP2902-E～ KDSP2903-E	－	○	○	－	－

（凡例）

○：メッセージの出力あり

－：メッセージの出力なし

14.3 メッセージ一覧

JP1/Audit Management - Manager が出力するメッセージの一覧を次に示します。

KDSO0001-I

正規化処理を開始しました。

(S)

監査ログの正規化処理を開始します。

KDSO0002-I

正規化処理を終了しました。

(S)

監査ログの正規化処理を終了します。

KDSO0004-E

文字コード変換処理に失敗しました。 イベントサーバ名=［*イベントサーバ名*］ 製品名=［*製品名*］ イベントデータベース内通し番号=［*イベントデータベース内通し番号*］

(S)

次の監査ログの処理を続行します。

(O)

このメッセージの前に出力されているエラーメッセージの対処法を参照してください。

KDSO0005-E

正規化処理に失敗しました。 イベントサーバ名=［*イベントサーバ名*］ 製品名=［*製品名*］ イベントデータベース内通し番号=［*イベントデータベース内通し番号*］

(S)

次の監査ログの処理を続行します。

(O)

このメッセージの前に出力されているエラーメッセージの対処法を参照してください。

KDSO0006-E

データベース書き込み処理に失敗しました。 イベントサーバ名=［*イベントサーバ名*］ 製品名=［*製品名*］ イベントデータベース内通し番号=［*イベントデータベース内通し番号*］

(S)

次の監査ログの処理を続行します。

(O)

このメッセージの前に出力されているエラーメッセージの対処法を参照してください。

KDSO0007-E

非サポートの文字コードを検出しました。文字コード=［*文字コード*］

(S)

次の監査ログの処理を続行します。

(O)

監査ログ収集対象サーバ上のプログラムが出力した監査ログの文字コードが，シフト JIS，EUC，または UTF-8 のどれかであることおよび文字コードが統一されていることを確認してください。

KDSO0008-E

製品定義ファイルの読み込みに失敗しました。

(S)

次の監査ログの処理を続行します。

(O)

製品定義ファイルの内容を確認してください。

KDSO0009-E

正規化パターンのパラメーター指定に誤りがあります。 パラメーター=［*パラメーター*］

(S)

次の監査ログの処理を続行します。

(O)

正規化ルールファイルに指定している正規化パターンのパラメーターに誤りがあります。パラメーターで使用できる値を確認してください。

KDSO0010-E

正規化パターンの展開に失敗しました。 パラメーター=［*パラメーター*］

(S)

次の監査ログの処理を続行します。

(O)

正規化ルールファイルに指定している正規化パターンのパラメーターに誤りがあります。パラメーターで使用できる値を確認してください。

KDSO0011-E

監査ログのパターンと正規化パターンが一致しません。 パラメーター=［*パラメーター*］

(S)

次の監査ログの処理を続行します。

(O)

正規化ルールファイルに指定している正規化パターンが，収集対象プログラムの監査ログに対応できていません。正規化パターンの確認，修正を行った上で再実行してください。

KDSO0012-E

監査ログを正規化できません。内部エラーが発生しました。

(S)

正規化処理を中止します。

(O)

システム管理者に連絡してください。

KDSO0013-E

監査ログを正規化できません。メモリ不足が発生しました。

(S)

正規化処理を中止します。

(O)

システム管理者に連絡してください。

KDSO0014-W

一時ファイルへの出力に失敗しました。イベントサーバ名=［*イベントサーバ名*］ 製品名=［*製品名*］ イベントデータベース内通し番号=［*イベントデータベース内通し番号*］ ログ=［*監査ログ*］

(S)

次の監査ログの処理を続行します。

(O)

監査ログ収集対象サーバ上のプログラムが出力した監査ログを，一時ファイルへ出力できませんでした。必要に応じてこのメッセージで出力されている該当ログを保存してください。

KDSO0015-W

一時ファイルへの出力に失敗しました。イベントサーバ名=［*イベントサーバ名*］ イベントデータベース内通し番号=［*イベントデータベース内通し番号*］ Windows イベント ID=［*Windows イベント ID*］ Windows ログ登録日時=［*Windows ログ登録日時*］ コンピュータ名=［*コンピュータ名*］ ログ=［*監査ログ*］

(S)

次の監査ログの処理を続行します。

(O)

監査ログ収集対象サーバ上のプログラムが出力した監査ログを，一時ファイルへ出力できませんでした。必要に応じてこのメッセージで出力されている該当ログを保存してください。

KDSO0016-E

JP1/NETM/Audit - Manager Convert サービスでの正規化処理に失敗しました。イベントサーバ名=［*イベントサーバ名*］ 製品名=［*製品名*］ イベントデータベース内通し番号=［*イベントデータベース内通し番号*］

(S)

次の監査ログの処理を続行します。

(O)

該当するイベントサーバで収集されたログが，JP1/NETM/Audit - Manager Convert サービスで正規化できませんでした。正規化処理エラー用 CSV ファイルに出力されているログ情報が必要なログか確認してください。必要に応じて，正規化ルールエディタの設定を確認・修正してください。

KDSO0101-E

コマンドのオプションが誤っています。

(S)

admimport コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0102-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admimport コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0103-I

監査ログのインポートを開始します。

(S)

admimport コマンドを開始します。

KDSO0104-I

監査ログのインポートが完了しました。

(S)

admimport コマンドを終了します。

KDSO0105-E

監査ログのインポートに失敗しました。

(S)

admimport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0106-E

データベースへの接続に失敗しました。

(S)

admimport コマンドを終了します。

(O)

- [マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0107-E

データベース読み込み中にエラーが発生しました。

(S)

admimport コマンドを終了します。

(O)

データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0108-E

データベース書き込み中にエラーが発生しました。

(S)

admimport コマンドを終了します。

(O)

データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0109-E

指定したインポート対象ファイルのオープンに失敗しました。ファイル名=［*ファイル名*］

(S)

admimport コマンドを終了します。

(O)

- インポート対象のファイルが指定した場所にあるか確認してください。
- インポート対象のファイルのアクセス権を確認してください。

KDSO0110-E

指定したインポート対象ファイルの読み込みに失敗しました。ファイル名=［*ファイル名*］

(S)

admimport コマンドを終了します。

(O)

- インポート対象のファイルのアクセス権を確認してください。
- インポート対象のファイルが破損していないか確認してください。

KDSO0111-E

インポート対象ファイルの解析に失敗しました。

(S)

admimport コマンドを終了します。

(O)

インポート対象のファイルが admexport コマンドを使って取得されたファイルかどうか確認してください。

KDSO0112-I

インポート対象ファイルにデータがありません。ファイル名=［*ファイル名*］

(S)

admimport コマンドを終了します。

KDSO0113-W

インポート対象ファイルの不正な行を無視しました。項目=［*項目*］，内容=［*内容*］

(S)

問題があった行のデータを無視して処理を続行します。

(O)

インポート対象のファイルが admexport コマンドを使って取得されたファイルかどうか確認してください。

KDSO0114-E

インストールパスの取得に失敗しました。

(S)

admimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0115-E

ログの初期化に失敗しました。

(S)

admimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0116-E

コマンドの実行権限がありません。

(S)

admimport コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0117-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admimport コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0118-E

プロセス間のロックに失敗しました。

(S)

admimport コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0119-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admimport コマンドを終了します。

(O)

[マネージャセットアップ] ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0120-E

指定したファイル名はフルパス名称ではありません。ファイル名=［*ファイル名*］

(S)

admimport コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0121-E

指定したファイル名はローカルディスク上のファイルではありません。ファイル名=［*ファイル名*］

(S)

admimport コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定し，コマンドを再実行してください。

KDSO0122-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admimport コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0123-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admimport コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0124-I

監査ログのインポートを中止しました。

(S)

admimport コマンドを終了します。

KDSO0125-E

データベースのパスワードが正しくありません。

(S)

admimport コマンドを終了します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO0126-E

バックアップファイルの正当性確認に失敗しました。

(S)

admimport コマンドを終了します。

(O)

入力ファイル名に指定したファイルが，監査ログのバックアップコマンドで取得したファイルであるか確認してください。

KDSO0127-W

バックアップファイルの正当性確認をスキップしました。

(S)

バックアップファイルの正当性を確認できなかったため，admimport コマンドを続行するかどうかを確認します。

(O)

コマンドを続行するかどうかの確認メッセージが出力されるため，インポートを実行する場合は Y または y を入力してください。実行を中断する場合は N または n を入力してください。

KDSO0128-E

指定した入力ファイル数が不正です。

(S)

admimport コマンドを終了します。

(O)

マイナー挿入モードを指定した場合は 1 ファイル，バルク挿入モードを指定した場合は 1～10 ファイルを指定し，コマンドを再実行してください。

KDSO0129-E

入力ファイル名に同一ファイルが指定されています。ファイル名=［*ファイル名*］

(S)

admimport コマンドを終了します。

(O)

入力ファイル名に重複しないファイル名を指定し，コマンドを再実行してください。

KDSO0130-E

指定した作業用ディレクトリのパスが不正です。ディレクトリ名=［*ディレクトリ名*］

(S)

admimport コマンドを終了します。

(O)

- 指定したフォルダ名が正しい形式のフルパス名になっているか確認してください。
- 指定したフォルダ名がローカルディスク上のパスになっているか確認してください。

KDSO0131-E

インポートの実行に必要なファイルがありません。

(S)

admimport コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0132-I

入力ファイルのデータ変換が完了しました。ファイル名=[*ファイル名*]

(S)

コマンドの処理を続行します。

KDSO0133-E

入力ファイルのデータ変換中にエラーが発生しました。ファイル名=[*ファイル名*]

(S)

admimport コマンドを終了します。

(O)

監査ログのインポートで使用する作業用フォルダに十分な空き容量があるか確認して，コマンドを再実行してください。作業用フォルダで使用されるディスク容量の見積もりについては「4.6.3(2)　データベースの操作時に必要なディスク容量」を参照してください。

再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0134-I

データベースのデータ格納が完了しました。ファイル名=[*ファイル名*]

(S)

コマンドの処理を続行します。

KDSO0135-E

データベースのデータ格納中にエラーが発生しました。ファイル名=[*ファイル名*]

(S)

admimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0136-I

データベースのインデクス再作成を開始します。

(S)

コマンドの処理を続行します。

KDSO0137-I

データベースのインデクス再作成が完了しました。

(S)

コマンドの処理を続行します。

KDSO0138-E

データベースのインデクス再作成中にエラーが発生しました。

(S)

admimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0139-E

作業用ディレクトリへのアクセスに失敗しました。ディレクトリ名=[*ディレクトリ名*]

(S)

admimport コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0140-E

ディスクに作業用領域として必要なサイズの空きがありません。(必要な作業用領域サイズ： *サイズ* MB)

(S)

admimport コマンドを終了します。

(O)

作業用フォルダに指定したディスクに作業用領域として必要なサイズの空きを確保してコマンドを再実行してください。

KDSO0141-E

作業用領域の空きサイズチェックでエラーが発生しました。

(S)

admimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0151-E

コマンドのオプションが誤っています。

(S)

admexport コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0152-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admexport コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0153-I

監査ログのバックアップを開始します。

(S)

admexport コマンドを開始します。

KDSO0154-I

監査ログのバックアップが完了しました。

(S)

admexport コマンドを終了します。

KDSO0155-E

監査ログのバックアップに失敗しました。

(S)

admexport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0156-E

データベースへの接続に失敗しました。

(S)

admexport コマンドを終了します。

(O)

- ［マネージャセットアップ］ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0157-E

データベース読み込み中にエラーが発生しました。

(S)

admexport コマンドを終了します。

(O)

データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0158-E

データベース書き込み中にエラーが発生しました。

(S)

admexport コマンドを終了します。

(O)

データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0159-E

指定した出力ファイルのオープンに失敗しました。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

- 指定したファイルがあるか確認してください。
- 指定したファイルのアクセス権を確認してください。

KDSO0160-E

指定した出力ファイルへの書き込みに失敗しました。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

出力ファイルの格納先フォルダに十分な空き容量があるか確認してください。

KDSO0162-E

指定した出力ファイルがすでに存在しています。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

ファイル名を変更してコマンドを再実行してください。

KDSO0164-E

インストールパスの取得に失敗しました。

(S)

admexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0165-E

ログの初期化に失敗しました。

(S)

admexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0166-E

コマンドの実行権限がありません。

(S)

admexport コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0167-E

admexport コマンドはすでに実行中です。

(S)

admexport コマンドを終了します。

(O)

実行中の admexport コマンドが終了してから，再実行してください。

KDSO0168-E

プロセス間のロックに失敗しました。

(S)

admexport コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0169-E

指定した開始日時が現在日時よりあとです。

(S)

admexport コマンドを終了します。

(O)

開始日時に，現在の日時（コマンド実行日時）よりも前の日時を指定してください。

KDSO0170-E

指定した開始日時が指定した終了日時よりあとです。

(S)

admexport コマンドを終了します。

(O)

開始日時に，終了日時よりも前の日時を指定してください。

KDSO0172-E

バックアップオプション定義ファイルの読み込みに失敗しました。ファイル名＝［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

- 指定したファイルがあるか確認してください。
- 指定したファイルのアクセス権を確認してください。
- 指定したファイルの終端に改行があるか確認してください。

KDSO0173-E

バックアップオプション定義ファイル内の内容が不正です。キー名=［*キー名*］ キー値=［*キー値*］

(S)

admexport コマンドを終了します。

(O)

バックアップオプション定義ファイルを修正してから，コマンドを再実行してください。

KDSO0174-E

バックアップオプション定義ファイル内に項目が指定されていません。キー名=［*キー名*］

(S)

admexport コマンドを終了します。

(O)

- バックアップオプション定義ファイル内に，定義が記述されているか確認してください。
- 記述されている定義の形式に誤りがないことを確認してください。

KDSO0175-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admexport コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0176-E

指定した出力ファイル格納先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admexport コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0177-I

指定した期間のデータがデータベース内に存在しません。開始日時=［*開始日時*］ 終了日時=［*終了日時*］

(S)

エクスポート対象ファイルの出力およびバックアップ履歴への登録はされないで，admexport コマンドを終了します。

(O)

指定した開始日時，終了日時に誤りがないことを確認してください。

KDSO0178-E

指定した開始日時が有効範囲外です。開始日時=［*開始日時*］

(S)

admexport コマンドを終了します。

(O)

開始日時に，有効範囲内の日時を指定してください。

有効範囲は，1900 年 1 月 1 日 0 時 0 分 0 秒から 9999 年 12 月 31 日 23 時 59 分 59 秒までです。ただし，次の場合はエラーとなります。

- 指定した日時が現在時刻を超えている場合
- 指定した日時が終了日時を超えている場合

KDSO0179-E

指定した終了日時が有効範囲外です。終了日時=［*終了日時*］

(S)

admexport コマンドを終了します。

(O)

終了日時に，有効範囲内の日時を指定してください。

有効範囲は，1900 年 1 月 1 日 0 時 0 分 0 秒から 9999 年 12 月 31 日 23 時 59 分 59 秒までです。ただし，次の場合はエラーとなります。

- 指定した日時が開始時刻より前の場合

KDSO0180-E

指定したファイル名がフルパス名称ではありません。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0181-E

指定したファイル名がローカルディスク上のファイルではありません。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定し，コマンドを再実行してください。

KDSO0182-E

指定した開始日時が不正です。開始日時=［*開始日時*］

(S)

admexport コマンドを終了します。

(O)

正しい開始日時を指定し，コマンドを再実行してください。

KDSO0183-E

指定した終了日時が不正です。終了日時=［*終了日時*］

(S)

admexport コマンドを終了します。

(O)

正しい終了日時を指定し，コマンドを再実行してください。

KDSO0184-E

指定した出力ファイル名のパスが長すぎます。

(S)

admexport コマンドを終了します。

(O)

出力ファイル名を変更し，コマンドを再実行してください。

KDSO0185-E

指定した出力ファイル名はすでにバックアップ履歴に登録されています。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

出力ファイル名を変更し，コマンドを再実行してください。

KDSO0186-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admexport コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0187-E

差分バックアップ出力情報の読み込み中にエラーが発生しました。

(S)

admexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0188-E

差分バックアップ出力情報の書き込み中にエラーが発生しました。

(S)

admexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0189-I

差分バックアップはすでに同一日に実行済みです。

(S)

admexport コマンドを終了します。

KDSO0190-E

指定した差分バックアップ格納先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admexport コマンドを終了します。

(O)

- フォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルが存在しないか確認してください。

KDSO0191-E

出力ファイルと同名のファイルまたはディレクトリが存在します。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

- admcsvmove コマンドまたは admcsvremove コマンドを実行して，既存のバックアップファイルを移動または削除してください。
- 出力先フォルダ名を変更し，コマンドを再実行してください。

KDSO0192-E

出力ファイルへのアクセスに失敗しました。ファイル名=［*ファイル名*］

(S)

admexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0193-E

指定したディレクトリ名はローカルディスク上のディレクトリではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admexport コマンドを終了します。

(O)

ローカルディスク上のフォルダ名を指定し，コマンドを再実行してください。

KDSO0194-E

指定したディレクトリ名はフルパス名称ではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admexport コマンドを終了します。

(O)

フォルダ名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0195-I

差分バックアップ出力情報の初期化を開始します。

(S)

admexport コマンドを開始します。

KDSO0196-I

差分バックアップ出力情報の初期化が完了しました。

(S)

admexport コマンドを終了します。

KDSO0197-E

差分バックアップ出力情報の初期化に失敗しました。

(S)

admexport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0198-I

コマンドの実行を中止しました。

(S)

admexport コマンドを終了します。

KDSO0199-E

指定したディレクトリ名のパスが長すぎます。ディレクトリ名=［*ディレクトリ名*］

(S)

admexport コマンドを終了します。

(O)

出力先フォルダ名を変更し，コマンドを再実行してください。

KDSO0200-I

差分バックアップを取得します。開始日時=［*開始日時*］ 終了日時=［*終了日時*］ 出力ファイル名=［*ファイル名*］

(S)

admexport コマンドの処理を継続します。

KDSO0201-E

コマンドのオプションが誤っています。

(S)

admcsvmove コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0202-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admcsvmove コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0203-I

バックアップファイルの移動を開始します。

(S)

admcsvmove コマンドを開始します。

KDSO0204-I

バックアップファイルの移動が完了しました。

(S)

admcsvmove コマンドを終了します。

KDSO0205-E

バックアップファイルの移動に失敗しました。

(S)

admcsvmove コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0206-E

データベースへの接続に失敗しました。

(S)

admcsvmove コマンドを終了します。

(O)

- [マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0207-E

データベース読み込み中にエラーが発生しました。

(S)

admcsvmove コマンドを終了します。

(O)

データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0208-E

データベース書き込み中にエラーが発生しました。

(S)

admcsvmove コマンドを終了します。

(O)

データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0211-E

指定した移動元ファイルはバックアップ履歴に登録されていません。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

移動元ファイル名には，admexport コマンドで取得したファイル名を指定してください。

KDSO0212-E

指定した移動元ファイルがありません。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

指定した移動元ファイルがあるか確認してください。

KDSO0213-E

指定した移動先ファイルがすでに存在します。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

移動先ファイル名を変更し，コマンドを再実行してください。

KDSO0214-E

インストールパスの取得に失敗しました。

(S)

admcsvmove コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0215-E

ログの初期化に失敗しました。

(S)

admcsvmove コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0216-E

コマンドの実行権限がありません。

(S)

admcsvmove コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0217-E

admcsvmove コマンドはすでに実行中です。

(S)

admcsvmove コマンドを終了します。

(O)

実行中の admcsvmove コマンドが終了してから，再実行してください。

KDSO0218-E

プロセス間のロックに失敗しました。

(S)

admcsvmove コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0219-E

バックアップオプション定義ファイルの読み込みに失敗しました。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

- 指定したファイルがあるか確認してください。
- 指定したファイルのアクセス権を確認してください。
- 指定したファイルの終端に改行があるか確認してください。

KDSO0220-E

バックアップオプション定義ファイル内の内容が不正です。キー名=［*キー名*］ キー値=［*キー値*］

(S)

admcsvmove コマンドを終了します。

(O)

バックアップオプション定義ファイルを修正してから，コマンドを再実行してください。

KDSO0221-E

バックアップオプション定義ファイル内に項目が指定されていません。キー名=［*キー名*］

(S)

admcsvmove コマンドを終了します。

(O)

- バックアップオプション定義ファイル内に，定義が記述されているか確認してください。
- 記述されている定義の形式に誤りがないことを確認してください。

KDSO0222-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admcsvmove コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0223-E

指定した移動元ファイルへのアクセスに失敗しました。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

指定したファイルのアクセス権を確認してください。

KDSO0224-E

指定した移動先ファイルへのアクセスに失敗しました。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

指定したファイルのアクセス権を確認してください。

KDSO0225-E

指定した移動先ファイル格納先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admcsvmove コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0226-E

バックアップファイルの移動中にエラーが発生しました。

(S)

admcsvmove コマンドを終了します。

(O)

ファイルの移動先フォルダに十分な空き容量があるか確認してください。

KDSO0227-E

指定したファイル名がフルパス名称ではありません。ファイル名=［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0228-E

指定したファイル名がローカルディスク上のファイルではありません。ファイル名＝［*ファイル名*］

(S)

admcsvmove コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定し，コマンドを再実行してください。

KDSO0229-E

指定した移動元ファイル名のパスが長すぎます。

(S)

admcsvmove コマンドを終了します。

(O)

移動元のファイル名を変更し，コマンドを再実行してください。

KDSO0230-E

指定した移動先ファイル名のパスが長すぎます。

(S)

admcsvmove コマンドを終了します。

(O)

移動先のファイル名を変更し，コマンドを再実行してください。

KDSO0231-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admcsvmove コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0232-E

指定した移動先ファイルはバックアップ履歴に登録されています。ファイル名=[*ファイル名*]

(S)

admcsvmove コマンドを終了します。

(O)

移動先ファイル名を変更し，コマンドを再実行してください。

KDSO0233-E

移動元ファイルと移動先ファイルに同一ファイルが指定されています。

(S)

admcsvmove コマンドを終了します。

(O)

ファイル名を変更し，コマンドを再実行してください。

KDSO0401-E

コマンドの実行権限がありません。

(S)

admdbbackup コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0402-E

インストールパスの取得に失敗しました。

(S)

admdbbackup コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0403-E

ほかのデータベースのコマンドがすでに実行中です。

(S)

admdbbackup コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0404-E

プロセス間のロックに失敗しました。

(S)

admdbbackup コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0405-E

コマンドのオプションが誤っています。

(S)

admdbbackup コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0406-E

ログの初期化に失敗しました。

(S)

admdbbackup コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0407-E

メモリ不足が発生しました。詳細情報＝［*詳細情報*］

(S)

admdbbackup コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0408-I

データベースのバックアップを開始します。

(S)

admdbbackup コマンドを開始します。

KDSO0409-I

データベースのバックアップが完了しました。

(S)

admdbbackup コマンドを終了します。

KDSO0410-E

データベースのバックアップに失敗しました。

(S)

admdbbackup コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0411-I

データベースのバックアップを中止しました。

(S)

admdbbackup コマンドを終了します。

KDSO0412-E

バックアップの実行に必要なファイルがありません。

(S)

admdbbackup コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0413-E

バックアップ実行中にエラーが発生しました。

(S)

admdbbackup コマンドを終了します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- バックアップファイルの出力先に十分な空き容量があるか確認してください。

KDSO0414-E

バックアップファイル格納先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbbackup コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0415-E

実行結果ファイル格納先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbbackup コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0416-E

バックアップファイル名と実行結果ファイル名が同じです。

(S)

admdbbackup コマンドを終了します。

(O)

バックアップファイル名とバックアップの実行結果ファイル名に異なる名称を指定してください。

KDSO0417-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbbackup コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0418-E

指定したファイル名がフルパス名称ではありません。ファイル名=［*ファイル名*］

(S)

admdbbackup コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0419-E

指定したファイル名がローカルディスク上のファイルではありません。ファイル名=［*ファイル名*］

(S)

admdbbackup コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定し，コマンドを再実行してください。

KDSO0420-E

指定したバックアップファイル名のパスが長すぎます。

(S)

admdbbackup コマンドを終了します。

(O)

ファイル名を変更し，コマンドを再実行してください。

KDSO0421-E

指定した実行結果ファイル名のパスが長すぎます。

(S)

admdbbackup コマンドを終了します。

(O)

ファイル名を変更し，コマンドを再実行してください。

KDSO0422-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbbackup コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0423-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbbackup コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0424-E

データベースへの接続に失敗しました。

(S)

admdbbackup コマンドを終了します。

(O)

- マネージャセットアップ画面で設定したデータベースのログイン ID，およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0425-E

指定したファイルと同名のディレクトリが存在します。ファイル名=［*ファイル名*］

(S)

admdbbackup コマンドを終了します。

(O)

- ファイル名を変更し，コマンドを再実行してください。

KDSO0451-E

コマンドの実行権限がありません。

(S)

admdbrstr コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0452-E

インストールパスの取得に失敗しました。

(S)

admdbrstr コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0453-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admdbrstr コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0454-E

プロセス間のロックに失敗しました。

(S)

admdbrstr コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0455-E

コマンドのオプションが誤っています。

(S)

admdbrstr コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0456-E

ログの初期化に失敗しました。

(S)

admdbrstr コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0457-E

メモリ不足が発生しました。詳細情報＝［*詳細情報*］

(S)

admdbrstr コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0458-I

データベースのリストアを開始します。

(S)

admdbrstr コマンドを開始します。

KDSO0459-I

データベースのリストアが完了しました。

(S)

admdbrstr コマンドを終了します。

KDSO0460-E

データベースのリストアに失敗しました。

(S)

admdbrstr コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0461-I

データベースのリストアを中止しました。

(S)

admdbrstr コマンドを終了します。

KDSO0462-E

リストアの実行に必要なファイルがありません。

(S)

admdbrstr コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0463-E

リストア実行中にエラーが発生しました。

(S)

admdbrstr コマンドを終了します。

(O)

次に示す項目を確認したあと，再実行してください。

- データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- バックアップファイル名に指定したファイルが，admdbbackup コマンドで取得したバックアップファイルであるか確認してください。
- リストアする環境が前提条件を満たしているか確認してください。前提条件については「10.1.4 データベースのリストア」を参照してください。

KDSO0464-E

バックアップファイルが存在しません。ファイル名=［*ファイル名*］

(S)

admdbrstr コマンドを終了します。

(O)

指定したバックアップファイルがあるか確認してください。

KDSO0465-E

実行結果ファイル格納先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbrstr コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0466-E

バックアップファイル名と実行結果ファイル名が同じです。

(S)

admdbrstr コマンドを終了します。

(O)

バックアップファイル名とリストアの実行結果ファイル名に異なる名称を指定してください。

KDSO0467-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbrstr コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0468-E

指定したファイル名がフルパス名称ではありません。ファイル名=［*ファイル名*］

(S)

admdbrstr コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0469-E

指定したファイル名がローカルディスク上のファイルではありません。ファイル名=［*ファイル名*］

(S)

admdbrstr コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定し，再実行してください。

KDSO0470-E

指定したバックアップファイル名のパスが長すぎます。

(S)

admdbrstr コマンドを終了します。

(O)

ファイル名を変更し，再実行してください。

KDSO0471-E

指定した実行結果ファイル名のパスが長すぎます。

(S)

admdbrstr コマンドを終了します。

(O)

ファイル名を変更し，再実行してください。

KDSO0472-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbrstr コマンドを終了します。

(O)

- データベースマネージャでデータベースをアップグレードしてください。

- データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0473-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbrstr コマンドを終了します。

(O)

次のサービスを停止した上で，再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0474-E

データベースのパスワードが正しくありません。

(S)

admdbrstr コマンドを終了します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO0475-E

データベースへの接続に失敗しました。

(S)

admdbrstr コマンドを終了します。

(O)

- [マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0476-E

指定したファイルと同名のディレクトリが存在します。ファイル名=［*ファイル名*］

(S)

admdbrstr コマンドを終了します。

(O)

ファイル名を変更し，コマンドを再実行してください。

KDSO0501-E

コマンドの実行権限がありません。

(S)

admdbrorg コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0502-E

インストールパスの取得に失敗しました。

(S)

admdbrorg コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0503-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admdbrorg コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0504-E

プロセス間のロックに失敗しました。

(S)

admdbrorg コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0505-E

コマンドのオプションが誤っています。

(S)

admdbrorg コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0506-E

ログの初期化に失敗しました。

(S)

admdbrorg コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0507-E

メモリ不足が発生しました。詳細情報＝［*詳細情報*］

(S)

admdbrorg コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0508-I

データベースの再編成を開始します。

(S)

admdbrorg コマンドを開始します。

KDSO0509-I

データベースの再編成が完了しました。

(S)

admdbrorg コマンドを終了します。

KDSO0510-E

データベースの再編成に失敗しました。

(S)

admdbrorg コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0511-I

データベースの再編成を中止しました。

(S)

admdbrorg コマンドを終了します。

KDSO0512-E

再編成の実行に必要なファイルがありません。

(S)

admdbrorg コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0513-E

再編成実行中にエラーが発生しました。

(S)

admdbrorg コマンドを終了します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- 再編成に使用する作業用フォルダに十分な空き容量があるか確認してください。

KDSO0514-E

作業用ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbrorg コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0515-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbrorg コマンドを終了します。

(O)

[マネージャセットアップ] ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0516-E

指定したディレクトリ名がフルパス名称ではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbrorg コマンドを終了します。

(O)

フォルダ名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0517-E

指定したディレクトリ名がローカルディスク上のディレクトリではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbrorg コマンドを終了します。

(O)

ローカルディスク上のフォルダ名を指定し，コマンドを再実行してください。

KDSO0518-E

指定した作業用ディレクトリのパスが長すぎます。

(S)

admdbrorg コマンドを終了します。

(O)

フォルダ名を変更し，コマンドを再実行してください。

KDSO0519-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbrorg コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0520-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbrorg コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0521-E

データベースへの接続に失敗しました。

(S)

admdbrorg コマンドを終了します。

(O)

- マネージャセットアップ画面で設定したデータベースのログイン ID，およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0522-E

ディスクに作業用領域として必要なサイズの空きがありません。(必要な作業用領域サイズ： *サイズ* MB)

(S)

admdbrorg コマンドを終了します。

(O)

作業用フォルダに指定したディスクに作業用領域として必要なサイズの空きを確保してコマンドを再実行してください。

KDSO0523-E

作業用領域の空きサイズチェックでエラーが発生しました。

(S)

admdbrorg コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0551-E

コマンドの実行権限がありません。

(S)

admdbstop コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0552-E

インストールパスの取得に失敗しました。

(S)

admdbstop コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0553-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admdbstop コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0554-E

プロセス間のロックに失敗しました。

(S)

admdbstop コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0555-E

コマンドのオプションが誤っています。

(S)

admdbstop コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0556-E

ログの初期化に失敗しました。

(S)

admdbstop コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0557-E

メモリ不足が発生しました。詳細情報＝［*詳細情報*］

(S)

admdbstop コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0558-I

データベースの停止処理を開始します。

(S)

admdbstop コマンドを開始します。

KDSO0559-I

データベースの停止処理が完了しました。

(S)

admdbstop コマンドを終了します。

(O)

イベントログに出力される KFPS01850-I メッセージを参照し，データベースが正常に停止したかどうかを確認してください。確認方法の詳細については「15.3.2　データベースのトラブル」を参照してください。

KDSO0560-E

データベースの停止処理に失敗しました。

(S)

admdbstop コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0561-E

停止処理の実行に必要なファイルがありません。

(S)

admdbstop コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0562-E

停止処理実行中にエラーが発生しました。

(S)

admdbstop コマンドを終了します。

(O)

データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0563-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbstop コマンドを終了します。

(O)

[マネージャセットアップ] ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0564-I

データベースの停止処理を中止しました。

(S)

admdbstop コマンドを終了します。

KDSO0565-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbstop コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0601-E

コマンドの実行権限がありません。

(S)

admdbexport コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0602-E

インストールパスの取得に失敗しました。

(S)

admdbexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0603-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admdbexport コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0604-E

プロセス間のロックに失敗しました。

(S)

admdbexport コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0605-E

コマンドのオプションが誤っています。

(S)

admdbexport コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0606-E

ログの初期化に失敗しました。

(S)

admdbexport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0607-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admdbexport コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0608-I

データベースの CSV バックアップを開始します。

(S)

admdbexport コマンドを開始します。

KDSO0609-I

データベースの CSV バックアップが完了しました。

(S)

admdbexport コマンドを終了します。

KDSO0610-E

データベースの CSV バックアップに失敗しました。

(S)

admdbexport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0611-I

データベースの CSV バックアップを中止しました。

(S)

admdbexport コマンドを終了します。

KDSO0612-E

CSV バックアップの実行に必要なファイルがありません。

(S)

admdbexport コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0613-E

CSV バックアップ実行中にエラーが発生しました。

(S)

admdbexport コマンドを終了します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- CSV バックアップファイルの出力先に十分な空き容量があるか確認してください。

KDSO0614-E

バックアップ出力先ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbexport コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0615-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbexport コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0616-E

指定したディレクトリ名がフルパス名称ではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbexport コマンドを終了します。

(O)

フォルダ名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0617-E

指定したディレクトリ名がローカルディスク上のディレクトリではありません。ディレクトリ名=[*ディレクトリ名*]

(S)

admdbexport コマンドを終了します。

(O)

ローカルディスク上のフォルダ名を指定し，コマンドを再実行してください。

KDSO0618-E

指定したバックアップ先ディレクトリのパスが長すぎます。

(S)

admdbexport コマンドを終了します。

(O)

フォルダ名を変更し，コマンドを再実行してください。

KDSO0619-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbexport コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0620-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbexport コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0621-E

データベースへの接続に失敗しました。

(S)

admdbexport コマンドを終了します。

(O)

- マネージャセットアップ画面で設定したデータベースのログイン ID，およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0651-E

コマンドの実行権限がありません。

(S)

admdbimport コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0652-E

インストールパスの取得に失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0653-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admdbimport コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0654-E

プロセス間のロックに失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0655-E

コマンドのオプションが誤っています。

(S)

admdbimport コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0656-E

ログの初期化に失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0657-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admdbimport コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0658-I

データベースの CSV リストアを開始します。

(S)

admdbimport コマンドを開始します。

KDSO0659-I

データベースの CSV リストアが完了しました。

(S)

admdbimport コマンドを終了します。

KDSO0660-E

データベースの CSV リストアに失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0661-I

データベースの CSV リストアを中止しました。

(S)

admdbimport コマンドを終了します。

KDSO0662-E

CSV リストアの実行に必要なファイルがありません。

(S)

admdbimport コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0663-E

CSV リストア実行中にエラーが発生しました。

(S)

admdbimport コマンドを終了します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- バックアップ格納先フォルダに指定したフォルダが，admdbexport コマンドによって取得したバックアップフォルダであるか確認してください。
- CSV リストアに使用する作業用フォルダに十分な空き容量があるか確認してください。

KDSO0664-E

バックアップ格納先ディレクトリが存在しません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbimport コマンドを終了します。

(O)

指定した CSV バックアップ格納先フォルダがあるか確認してください。

KDSO0665-E

バックアップ格納先ディレクトリ内に CSV リストアに必要なファイルがありません。

(S)

admdbimport コマンドを終了します。

(O)

指定したフォルダが CSV バックアップ格納先フォルダであるか確認してください。

KDSO0666-E

作業用ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbimport コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0667-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0668-E

指定したディレクトリ名がフルパス名称ではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbimport コマンドを終了します。

(O)

フォルダ名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0669-E

指定したディレクトリ名がローカルディスク上のディレクトリではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbimport コマンドを終了します。

(O)

ローカルディスク上のフォルダ名を指定し，コマンドを再実行してください。

KDSO0670-E

指定したバックアップ格納先ディレクトリのパスが長すぎます。

(S)

admdbimport コマンドを終了します。

(O)

フォルダ名を変更し，コマンドを再実行してください。

KDSO0671-E

指定した作業用ディレクトリのパスが長すぎます。

(S)

admdbimport コマンドを終了します。

(O)

フォルダ名を変更し，コマンドを再実行してください。

KDSO0672-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbimport コマンドを終了します。

(O)

- データベースマネージャでデータベースをアップグレードしてください。
- データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0673-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbimport コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0674-E

データベースのパスワードが正しくありません。

(S)

admdbimport コマンドを終了します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO0675-E

バックアップファイルの正当性確認に失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

バックアップ格納先ディレクトリに指定したディレクトリが，データベースの CSV バックアップで取得したディレクトリであるか確認してください。

KDSO0676-E

データベースへの接続に失敗しました。

(S)

admdbimport コマンドを終了します。

(O)

- [マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0677-E

ディスクに作業用領域として必要なサイズの空きがありません。(必要な作業用領域サイズ： *サイズ* MB)

(S)

admdbimport コマンドを終了します。

(O)

作業用フォルダに指定したディスクに作業用領域として必要なサイズの空きを確保してコマンドを再実行してください。

KDSO0678-E

作業用領域の空きサイズチェックでエラーが発生しました。

(S)

admdbimport コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0701-E

コマンドの実行権限がありません。

(S)

admdbdelete コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0702-E

インストールパスの取得に失敗しました。

(S)

admdbdelete コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0703-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admdbdelete コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSO0704-E

プロセス間のロックに失敗しました。

(S)

admdbdelete コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0705-E

コマンドのオプションが誤っています。

(S)

admdbdelete コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0706-E

ログの初期化に失敗しました。

(S)

admdbdelete コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0707-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admdbdelete コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0708-I

データベースのデータ削除を開始します。

(S)

admdbdelete コマンドを開始します。

KDSO0709-I

データベースのデータ削除が完了しました。

(S)

admdbdelete コマンドを終了します。

KDSO0710-E

データベースのデータ削除に失敗しました。

(S)

admdbdelete コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0711-I

データベースのデータ削除を中止しました。

(S)

admdbdelete コマンドを終了します。

KDSO0712-E

データベースへの接続に失敗しました。

(S)

admdbdelete コマンドを終了します。

(O)

- ［マネージャセットアップ］ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0713-E

データベース読み込み中にエラーが発生しました。

(S)

admdbdelete コマンドを終了します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- 削除終了日時に指定した値が，正しい日時であることを確認してください。

KDSO0715-E

データ削除の実行に必要なファイルがありません。

(S)

admdbdelete コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0716-E

データ削除の実行中にエラーが発生しました。

(S)

admdbdelete コマンドを終了します。

(O)

データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0717-E

作業用ディレクトリへのアクセスに失敗しました。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbdelete コマンドを終了します。

(O)

- 指定したフォルダのアクセス権を確認してください。
- 指定したフォルダ名と同じ名称のファイルがないことを確認してください。

KDSO0718-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbdelete コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0719-E

指定した削除終了日時が有効範囲外です。削除終了日時=［*削除終了日時*］

(S)

admdbdelete コマンドを終了します。

(O)

削除終了日時に，有効範囲内の日時を指定してください。

有効範囲は，1900 年 1 月 1 日 0 時 0 分 0 秒から 9999 年 12 月 31 日 23 時 59 分 59 秒までです。

KDSO0720-E

指定したディレクトリ名がフルパス名称ではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbdelete コマンドを終了します。

(O)

フォルダ名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0721-E

指定したディレクトリ名がローカルディスク上のディレクトリではありません。ディレクトリ名=［*ディレクトリ名*］

(S)

admdbdelete コマンドを終了します。

(O)

ローカルディスク上のフォルダ名を指定し，コマンドを再実行してください。

KDSO0723-E

指定した削除終了日時が不正です。削除終了日時=［*削除終了日時*］

(S)

admdbdelete コマンドを終了します。

(O)

正しい削除終了日時を指定し，コマンドを再実行してください。

KDSO0724-E

指定した作業用ディレクトリのパスが長すぎます。

(S)

admdbdelete コマンドを終了します。

(O)

フォルダ名を変更し，コマンドを再実行してください。

KDSO0725-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbdelete コマンドを終了します。

(O)

- データベースマネージャでデータベースをアップグレードしてください。
- データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0726-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

admdbdelete コマンドを終了します。

(O)

次のサービスを停止した上で，コマンドを再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO0727-E

データベースのパスワードが正しくありません。

(S)

admdbdelete コマンドを終了します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO0728-I

指定した日時以前のデータがデータベース内に存在しません。削除終了日時=［*削除終了日時*］

(S)

データを削除しないで admdbdelete コマンドを終了します。

KDSO0729-E

削除対象外のデータ退避中にエラーが発生しました。

(S)

admdbdelete コマンドを終了します。

(O)

データベースのデータ削除で使用する作業用フォルダに十分な空き容量があるか確認して，コマンドを再実行してください。作業用フォルダで使用されるディスク容量の見積もりについては「4.6.3(2) データベースの操作時に必要なディスク容量」を参照してください。

再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0730-E

削除対象外のデータ格納中にエラーが発生しました。

(S)

admdbdelete コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0731-E

ディスクに作業用領域として必要なサイズの空きがありません。(必要な作業用領域サイズ： *サイズ* MB)

(S)

admdbdelete コマンドを終了します。

(O)

作業用フォルダに指定したディスクに作業用領域として必要なサイズの空きを確保してコマンドを再実行してください。

KDSO0732-E

作業用領域の空きサイズチェックでエラーが発生しました。

(S)

admdbdelete コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0751-E

コマンドの実行権限がありません。

(S)

admcsvremove コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0752-E

インストールパスの取得に失敗しました。

(S)

admcsvremove コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0753-E

admcsvremove コマンドはすでに実行中です。

(S)

admcsvremove コマンドを終了します。

(O)

実行中の admcsvremove が終了してから再実行してください。

KDSO0754-E

プロセス間のロックに失敗しました。

(S)

admcsvremove コマンドを終了します。

(O)

システムのリソースが不足していないかどうかを確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0755-E

コマンドのオプションが誤っています。

(S)

admcsvremove コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0756-E

ログの初期化に失敗しました。

(S)

admcsvremove コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0757-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admcsvremove コマンドを終了します。

(O)

不要なアプリケーションを終了し，コマンドを再実行してください。

KDSO0758-I

バックアップファイルの削除を開始します。

(S)

admcsvremove コマンドを開始します。

KDSO0759-I

バックアップファイルの削除が完了しました。

(S)

admcsvremove コマンドを終了します。

KDSO0760-E

バックアップファイルの削除に失敗しました。

(S)

admcsvremove コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0761-I

バックアップファイルの削除を中止しました。

(S)

admcsvremove コマンドを終了します。

KDSO0762-E

データベースへの接続に失敗しました。

(S)

admcsvremove コマンドを終了します。

(O)

[マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいかどうかを確認してください。また，データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0763-E

データベース読み込み中にエラーが発生しました。

(S)

admcsvremove コマンドを終了します。

(O)

データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0764-E

データベース書き込み中にエラーが発生しました。

(S)

admcsvremove コマンドを終了します。

(O)

データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0765-E

指定したバックアップファイルはバックアップ履歴に登録されていません。バックアップファイル名＝[*バックアップファイル名*]

(S)

admcsvremove コマンドを終了します。

(O)

admexport コマンドによって取得した監査ログのバックアップファイル名を，削除対象ファイル名として指定してください。

KDSO0766-W

指定したバックアップファイルがありません。バックアップファイル名=［*バックアップファイル名*］

(S)

バックアップファイルを削除しないで処理を続行します。

KDSO0767-E

指定したバックアップファイルへのアクセスに失敗しました。バックアップファイル名=［*バックアップファイル名*］

(S)

admcsvremove コマンドを終了します。

(O)

ファイルのアクセス権を確認してください。

KDSO0768-E

バックアップファイルの削除中にエラーが発生しました。

(S)

admcsvremove コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0769-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admcsvremove コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているかどうかを確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0770-E

指定したファイル名がフルパス名称ではありません。ファイル名=［*ファイル名*］

(S)

admcsvremove コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSO0771-E

指定したファイル名がローカルディスク上のファイルではありません。ファイル名=［*ファイル名*］

(S)

admcsvremove コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定し，コマンドを再実行してください。

KDSO0772-E

指定したバックアップファイル名のパスが長すぎます。

(S)

admcsvremove コマンドを終了します。

(O)

ファイル名を変更し，コマンドを再実行してください。

KDSO0773-E

指定したバックアップ ID が不正です。

(S)

admcsvremove コマンドを終了します。

(O)

バックアップ ID を変更し，コマンドを再実行してください。

KDSO0774-E

指定したバックアップ ID はバックアップ履歴に登録されていません。バックアップ ID=［*バックアップ ID*］

(S)

admcsvremove コマンドを終了します。

(O)

バックアップ ID として，バックアップ履歴画面の一覧にあるバックアップ ID を指定してください。

KDSO0775-W

指定したバックアップ ID のバックアップファイルがありません。バックアップ ID=［*バックアップ ID*］ バックアップファイル名=［*バックアップファイル名*］

(S)

バックアップファイルを削除しないで処理を続行します。

KDSO0776-E

指定したバックアップ ID のバックアップファイルへのアクセスに失敗しました。バックアップ ID=［*バックアップ ID*］ バックアップファイル名=［*バックアップファイル名*］

(S)

admcsvremove コマンドを終了します。

(O)

ファイルのアクセス権を確認してください。

KDSO0777-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admcsvremove コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0801-E

コマンドの実行権限がありません。

(S)

admstgen コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0802-E

インストールパスの取得に失敗しました。

(S)

admstgen コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0803-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admstgen コマンドを終了します。

(O)

実行中のデータベース管理コマンドが終了してから，再実行してください。

KDSO0804-E

プロセス間のロックに失敗しました。

(S)

admstgen コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0805-E

コマンドのオプションが誤っています。

(S)

admstgen コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0806-E

ログの初期化に失敗しました。

(S)

admstgen コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0807-E

メモリ不足が発生しました。詳細情報＝［*詳細情報*］

(S)

admstgen コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0808-I

監査ログ統計情報の生成を開始します。生成開始日時＝［*生成開始日*※］

(S)

admstgen コマンドを開始します。

注※

YYYY-MM-DD 形式で表示されます。YYYY：年，MM：月，DD：日を示します。

KDSO0809-I

監査ログ統計情報の生成が完了しました。

(S)

admstgen コマンドを終了します。

KDSO0810-E

監査ログ統計情報の生成に失敗しました。

(S)

admstgen コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0811-I

監査ログ統計情報の生成を中止しました。

(S)

admstgen コマンドを終了します。

KDSO0812-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admstgen コマンドを終了します。

(O)

［マネージャセットアップ］ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0813-E

データベースへの接続に失敗しました。

(S)

admstgen コマンドを終了します。

(O)

- ［マネージャセットアップ］ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0814-E

データベース読み込み中にエラーが発生しました。

(S)

admstgen コマンドを終了します。

(O)

データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0815-E

データベース書き込み中にエラーが発生しました。

(S)

admstgen コマンドを終了します。

(O)

データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0816-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admstgen コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0817-E

指定した絶対日付が不正です。絶対日付=［*絶対日付*］

(S)

admstgen コマンドを終了します。

(O)

- 正しい日付を指定してコマンドを再実行してください。
- コマンド実行日以前の日付を指定してください。

KDSO0818-E

指定した絶対日付が有効範囲外です。絶対日付=［*絶対日付*］

(S)

admstgen コマンドを終了します。

(O)

有効範囲内の日付を指定してください。有効範囲は，1900 年 1 月 1 日から 9999 年 12 月 31 日までです。

KDSO0819-I

統計パターンが設定されていないため，監査ログ統計情報は生成されませんでした。

(S)

admstgen コマンドを終了します。

(O)

統計パターンを設定して再実行してください。

KDSO0851-E

コマンドの実行権限がありません。

(S)

admstdel コマンドを終了します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO0852-E

インストールパスの取得に失敗しました。

(S)

admstdel コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0853-E

ほかのデータベース管理コマンドがすでに実行中です。

(S)

admstdel コマンドを終了します。

(O)

実行中のデータベース管理コマンドが終了してから，再実行してください。

KDSO0854-E

プロセス間のロックに失敗しました。

(S)

admstdel コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0855-E

コマンドのオプションが誤っています。

(S)

admstdel コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO0856-E

ログの初期化に失敗しました。

(S)

admstdel コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0857-E

メモリ不足が発生しました。詳細情報＝［*詳細情報*］

(S)

admstdel コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO0858-I

監査ログ統計情報の削除を開始します。削除終了日時＝［*削除終了日*※］

(S)

admstdel コマンドを開始します。

注※

YYYY-MM-DD 形式で表示されます。YYYY：年，MM：月，DD：日を示します。

KDSO0859-I

監査ログ統計情報の削除が完了しました。

(S)

admstdel コマンドを終了します。

KDSO0860-E

監査ログ統計情報の削除に失敗しました。

(S)

admstdel コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO0861-I

監査ログ統計情報の削除を中止しました。

(S)

admstdel コマンドを終了します。

KDSO0862-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admstdel コマンドを終了します。

(O)

[マネージャセットアップ] ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0863-E

データベースへの接続に失敗しました。

(S)

admstdel コマンドを終了します。

(O)

- [マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0864-E

データベース読み込み中にエラーが発生しました。

(S)

admstdel コマンドを終了します。

(O)

データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0865-E

データベース書き込み中にエラーが発生しました。

(S)

admstdel コマンドを終了します。

(O)

データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0866-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admstdel コマンドを終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO0868-E

指定した削除終了日が不正です。削除終了日＝［*削除終了日*］

(S)

admstdel コマンドを終了します。

(O)

- 正しい日付を指定してコマンドを再実行してください。
- コマンド実行日以前の日付を指定してください。

KDSO0869-E

指定した削除終了日が有効範囲外です。削除終了日＝［*削除終了日*］

(S)

admstdel コマンドを終了します。

(O)

有効範囲内の日付を指定してください。有効範囲は，1900 年 1 月 1 日から 9999 年 12 月 31 日までです。

KDSO0901-E

コマンドの実行権限がありません。

(S)

admdbstat コマンドを終了します。

(O)

管理者権限を持つユーザで，再度実行してください。

KDSO0902-E

インストールパスの取得に失敗しました。

(S)

admdbstat コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0903-E

admdbstat コマンドはすでに実行中です。

(S)

admdbstat コマンドを終了します。

(O)

実行中の admdbstat コマンドが終了してから，再度実行してください。

KDSO0904-E

プロセス間のロックに失敗しました。

(S)

admdbstat コマンドを終了します。

(O)

システムのリソースが不足していないか確認してください。再度実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0905-E

コマンドのオプションが誤っています。

(S)

admdbstat コマンドを終了します。

(O)

正しい引数を指定してコマンドを再度実行してください。

KDSO0906-E

メモリ不足が発生しました。詳細情報=［*詳細情報*］

(S)

admdbstat コマンドを終了します。

(O)

不要なアプリケーションを終了して，コマンドを再度実行してください。

KDSO0907-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

admdbstat コマンドを終了します。

(O)

- マネージャセットアップによるセットアップが完了しているか確認してください。
- クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO0908-E

データベースの状況確認に必要なファイルがありません。

(S)

admdbstat コマンドを終了します。

(O)

データベースのセットアップが完了しているか確認してください。再度実行しても回復しない場合は，システム管理者に連絡してください。

KDSO0909-E

データベースの状況確認中にエラーが発生しました。

(S)

admdbstat コマンドを終了します。

(O)

システム管理者に連絡してください。

KDSO0910-E

データベースへの接続に失敗しました。

(S)

admdbstat コマンドを終了します。

(O)

- マネージャセットアップ画面で設定したデータベースのログイン ID，およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO0911-E

データベースのバージョンが製品バージョンに対応していません。

(S)

admdbstat コマンドを終了します。

(O)

データベースマネージャでデータベースのアップグレードを実施してください。

KDSO1000-E

定義ファイルの読込みに失敗しました。

(S)

処理を中止します。

(O)

［監査ログ収集マネージャ］ウィンドウの設定および製品定義ファイルと動作定義ファイルの記述を確認し，再実行してください。回復しない場合は，システム管理者に連絡してください。

KDSO1019-E

内部エラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1030-E

jevlogstart コマンド実行時にエラーが発生しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定および製品定義ファイルと動作定義ファイルの記述を確認し，再実行してください。回復しない場合は，システム管理者に連絡してください。

KDSO1031-E

jevlogstop コマンド実行時にエラーが発生しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定を確認し，再実行してください。回復しない場合は，管理者へ連絡してください。

KDSO1032-E

jevlogstat コマンド実行時にエラーが発生しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定を確認し，再実行してください。回復しない場合は，管理者へ連絡してください。

KDSO1036-W

起動順序定義ファイルへの登録用バッチファイルのパスの登録に失敗しました。

(S)

処理を終了します。

(O)

監査ログ収集対象サーバ上の JP1/Base の起動順序定義ファイルを確認してください。必要に応じて，登録用バッチファイルを追加してください。

KDSO1037-W

起動用バッチファイルの出力に失敗しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定を確認してください。

KDSO1038-W

登録用バッチファイルへの登録に失敗しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定を確認してください。

KDSO1039-W

起動順序定義ファイルから登録用バッチファイルのパスの削除に失敗しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定と登録用バッチファイルの名称を確認してください。

KDSO1040-W

起動用バッチファイルの削除に失敗しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定を確認してください。

KDSO1041-W

登録用バッチファイルから起動用バッチファイルのパスの削除に失敗しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの設定を確認してください。

KDSO1043-E

レジストリの取得に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1044-E

動作定義ファイルの作成に失敗しました。

(S)

処理を終了します。

(O)

監査ログ専用イベントサーバの JP/1Base の設定を確認し，再実行してください。

KDSO1046-W

動作定義ファイルの削除に失敗しました。

(S)

処理を終了します。

(O)

動作定義ファイルがあるか，動作定義ファイルの格納場所を確認してください。

KDSO1101-I

JP1 ユーザ情報の収集が完了しました。

(S)

処理を終了します。

KDSO1102-E

コマンドの実行権限がありません。

(S)

処理を中止します。

(O)

管理者権限を持つユーザでログインし直して，コマンドを再実行してください。

KDSO1103-E

JP1 ユーザ情報の収集に失敗しました。

(S)

処理を中止します。

(O)

JP1/Base の認証サーバの設定が完了しているかどうか，また認証サーバが正常に動作しているかどうかを確認してください。

KDSO1500-I

JP1/NETM/Audit - Manager サービスを起動しました。

(S)

処理を続行します。

KDSO1501-I

JP1/NETM/Audit - Manager サービスを停止しました。

(S)

処理を終了します。

KDSO1502-E

JP1/NETM/Audit - Manager サービスの起動に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1503-E

JP1/NETM/Audit - Manager サービスが異常終了しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1504-E

監査ログの収集に失敗しました。イベントサーバ名=［*イベントサーバ名*］

(S)

処理を続行します。

(O)

システム管理者に連絡してください。

KDSO1505-E

データベースのバージョンが製品バージョンに対応していません。

(S)

処理を終了します。

(O)

データベースマネージャでデータベースをアップグレードしてください。

KDSO1506-I

イベントデータベースの切り替えが通知されました。イベントサーバ名=［*イベントサーバ名*］

(S)

処理を続行します。

KDSO1507-I

監査ログの定時収集を開始します。

(S)

処理を続行します。

KDSO1508-I

監査ログの即時収集を開始します。

(S)

処理を続行します。

KDSO1509-I

監査ログの収集を開始しました。イベントサーバ名＝［*イベントサーバ名*］

(S)

処理を続行します。

KDSO1510-I

監査ログの収集が完了しました。イベントサーバ名＝［*イベントサーバ名*］

(S)

処理を続行します。

KDSO1511-E

データベースへの接続に失敗しました。

(S)

処理を終了します。

(O)

- マネージャセットアップ画面で設定したデータベースのログイン ID，およびパスワードの指定が正しいか確認してください。
- データベースが正常に動作しているか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。

KDSO1512-I

監査ログ退避ファイルの取り込みを開始しました。

(S)

処理を続行します。

KDSO1513-I

監査ログ退避ファイルの取り込みが完了しました。

(S)

処理を続行します。

KDSO1514-E

ファイルのオープンに失敗しました。ファイル名=［*ファイル名*］

(S)

処理を終了します。

(O)

- ファイルがあるか確認してください。
- ファイルのアクセス権を確認してください。

KDSO1515-E

監査ログ退避ファイルの取り込み中にエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1516-E

監査ログ収集の開始に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1517-E

監査ログ退避ファイルのデータ不正を検出しました。

(S)

監査ログ退避ファイルの取り込み処理をスキップし，イベントデータベースからの収集を実行します。

(O)

システム管理者に連絡してください。

KDSO1518-W

監査ログ退避ファイルが不正状態のため，監査ログ退避ファイルの取り込み処理をスキップしました。

(S)

監査ログ退避ファイルの取り込み処理をスキップし，イベントデータベースからの収集を実行します。

(O)

システム管理者に連絡してください。

KDSO1601-I

JP1/NETM/Audit - Manager SubCollect サービスを起動しました。

(S)

処理を続行します。

KDSO1602-I

JP1/NETM/Audit - Manager SubCollect サービスを停止しました。

(S)

処理を終了します。

KDSO1603-E

JP1/NETM/Audit - Manager SubCollect サービスの起動に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1604-E

JP1/NETM/Audit - Manager SubCollect サービスが異常終了しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1605-I

イベントデータベースの切り替えが通知されました。イベントサーバ名=[*イベントサーバ名*]

(S)

処理を続行します。

KDSO1606-I

監査ログの収集を開始しました。イベントサーバ名=[*イベントサーバ名*]

(S)

処理を続行します。

KDSO1607-I

監査ログの収集が完了しました。イベントサーバ名=[*イベントサーバ名*]

(S)

処理を続行します。

KDSO1608-E

監査ログの収集に失敗しました。イベントサーバ名=[*イベントサーバ名*]

(S)

処理を続行します。

(O)

システム管理者に連絡してください。

KDSO1609-E

ファイルのオープンに失敗しました。ファイル名=[*ファイル名*]

(S)

処理を続行します。

(O)

ファイルのアクセス権を確認してください。

KDSO1610-E

ファイルへの書き込みに失敗しました。ファイル名=[*ファイル名*]

(S)

処理を続行します。

(O)

ファイルサイズが最大サイズに達していないか確認してください。また，ファイルの格納先ディレクトリに十分な空き容量があるか確認してください。

KDSO1611-W

監査ログ退避ファイルが不正状態のため，監査ログの収集処理をスキップしました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO1651-E

コマンドの実行権限がありません。

(S)

処理を中止します。

(O)

管理者権限を持つユーザで，再実行してください。

KDSO1652-E

インストールパスの取得に失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO1653-E

admcoldata コマンドは既に実行中です。

(S)

処理を中止します。

(O)

実行中の admcoldata コマンドが終了してから，再実行してください。

KDSO1654-E

プロセス間のロックに失敗しました。

(S)

処理を中止します。

(O)

システムのリソースが不足していないか確認してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO1655-E

コマンドのオプションが誤っています。

(S)

処理を中止します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSO1656-E

ログの初期化に失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO1657-E

メモリ不足が発生しました。詳細情報=[*詳細情報*]

(S)

処理を中止します。

(O)

不要なアプリケーションを終了して，コマンドを再実行してください。

KDSO1658-E

JP1/Audit Management - Manager のサービスが停止しています。

(S)

処理を中止します。

(O)

次のサービスを起動した上で，再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert

KDSO1659-I

監査ログ収集の開始に成功しました。

(S)

処理を終了します。

KDSO1660-E

監査ログ収集の開始に失敗しました。

(S)

処理を中止します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSO1661-I

監査ログ収集の開始を中止しました。

(S)

処理を中止します。

KDSO1662-E

コマンドの動作に必要な定義ファイルの読み込みに失敗しました。

(S)

処理を終了します。

(O)

[マネージャセットアップ] ダイアログによるセットアップが完了しているか確認してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO2001-I

環境設定に成功しました。

(S)

処理を終了します。

KDSO2002-E

管理者権限がありません。

(S)

処理を中止します。

(O)

管理者権限を持つユーザで，再実行してください。

KDSO2003-E

環境設定に失敗しました。ファイル I/O エラーが発生しました。

(S)

処理を中止します。

(O)

空きディスク容量が十分か，ファイルシステムでトラブルが発生していないかを確認してください。回復しない場合は，システム管理者に連絡してください。

KDSO2004-E

環境設定に失敗しました。内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2009-I

環境設定情報を設定します。
設定した内容は次回サービス起動時に有効になります。

(S)

処理を続行します。

KDSO2018-W

マネージャセットアップはすでに起動しています。

(S)

処理を中止します。

(O)

すでに起動しているマネージャセットアップを終了し，再実行してください。

KDSO2020-E

入力した値の文字数が最小文字数より小さいです。

(S)

処理を中止します。

(O)

選択している項目名の最小文字数を確認し，再入力してください。

KDSO2021-E

入力した値の文字数が最大文字数より大きいです。

(S)

処理を中止します。

(O)

選択している項目名の最大文字数を確認し，再入力してください。

KDSO2022-E

入力した値の数値が最小値より小さいです。

(S)

処理を中止します。

(O)

選択している項目名の最小値を確認し，再入力してください。

KDSO2023-E

入力した値の数値が最大値より大きいです。

(S)

処理を中止します。

(O)

選択している項目名の最大値を確認し，再入力してください。

KDSO2024-E

使用できない文字が使われています。

(S)

処理を中止します。

(O)

選択している項目名の使用できない文字を確認し，再入力してください。

KDSO2026-E

共有ディスクの値に誤りがあります。

(S)

処理を中止します。

(O)

共有ディスクのパスを確認し，再入力してください。

KDSO2027-E

入力必須項目が入力されていません。

(S)

処理を中止します。

(O)

必須項目が入力されているか確認してください。

KDSO2028-E

パスワードを入力してください。

(S)

処理を中止します。

(O)

パスワードを設定し，再実行してください。

KDSO2029-E

再入力したパスワードが異なります。

(S)

処理を中止します。

(O)

パスワードを再入力してください。

KDSO2030-E

パスワードに使用できない文字が入力されました。パスワードに使用できるのは以下の文字です。
1 文字目：半角英字または記号
2 文字目以降：半角英数字または記号
入力可能な記号：# @ ¥

(S)

処理を中止します。

(O)

入力できる文字または文字数を確認し，パスワードを再入力してください。

KDSO2033-E

クラスタ関連の設定値は，サービス実行中に変更できません。

(S)

処理を中止します。

(O)

次のサービスを停止した上で，再度，クラスタ関連の設定をしてください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define
- JP1/NETM/Audit - Manager SubCollect

KDSO2040-E

定義ファイルの読み込みに失敗しました。ファイル I/O エラーが発生しました。

(S)

処理を中止します。

(O)

ファイルシステムにトラブルが発生していないか確認し，再実行してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO2043-E

内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2044-W

定義ファイルを正しく読み込めません。一部の項目をデフォルト値で起動します。

(S)

一部の設定項目をデフォルト値で起動し，処理を続行します。

(O)

マネージャセットアップの設定を確認してください。なお，このメッセージは，クラスタシステムの待機系サーバの初回設定時にも表示されることがあります。待機系サーバの初回設定時に表示された場合は，対処の必要はありません。そのまま設定してください。

KDSO2052-I

マネージャセットアップを起動しました。

(S)

マネージャセットアップを開始します。

KDSO2053-I

マネージャセットアップを終了しました。

(S)

マネージャセットアップを終了します。

KDSO2054-E

変更前パスワードが正しくありません。

(S)

処理を中止します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO2055-E

変更後パスワードに使用できない文字が入力されました。パスワードに使用できるのは以下の文字です。
1 文字目：半角英字または記号
2 文字目以降：半角英数字または記号
入力可能な記号：# @ ¥

(S)

処理を中止します。

(O)

入力できる文字または文字数を確認し，パスワードを再入力してください。

KDSO2056-E

再入力したパスワードが変更後パスワードと異なります。

(S)

処理を中止します。

(O)

パスワードを再入力してください。

KDSO2200-W

データベースマネージャはすでに起動しています。

(S)

処理を中止します。

(O)

起動しているデータベースマネージャを終了し，再実行してください。

KDSO2201-E

管理者権限がありません。

(S)

処理を中止します。

(O)

管理者権限を持つユーザで，再実行してください。

KDSO2202-E

入力した値の文字数が最小文字数より小さいです。

(S)

処理を中止します。

(O)

選択している項目名の最小文字数を確認し，再入力してください。

KDSO2203-E

入力した値の文字数が最大文字数より大きいです。

(S)

処理を中止します。

(O)

選択している項目名の最大文字数を確認し，再入力してください。

KDSO2204-E

入力した値の数値が最小値より小さいです。

(S)

処理を中止します。

(O)

選択している項目名の最小値を確認し，再入力してください。

KDSO2205-E

入力した値の数値が最大値より大きいです。

(S)

処理を中止します。

(O)

選択している項目名の最大値を確認し，再入力してください。

KDSO2206-E

プログラムの初期化に失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2207-E

フルパスで指定してください。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2208-E

該当ファイルが存在しません。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2209-E

該当フォルダが存在しません。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2211-E

フォルダは指定できません。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2212-E

パスワードに使用できない文字が入力されました。パスワードに使用できるのは以下の文字です。
1 文字目：半角英字または記号
2 文字目以降：半角英数字または記号
入力可能な記号：# @ ¥

(S)

処理を中止します。

(O)

正しい文字列を入力し，再実行してください。

KDSO2213-E

パスの指定に誤りがあります。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2214-E

再入力したパスワードが変更後パスワードと異なります。

(S)

処理を中止します。

(O)

正しい文字列を入力し，再実行してください。

KDSO2215-W

JP1/Audit Management - Manager のサービスが実行中です。

(S)

処理を中止します。

(O)

次のサービスを停止した上で，再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO2216-I

データベースは作成済みです。
再セットアップを行いますか？

(S)

処理を続行します。

(O)

再セットアップする場合は，［OK］ボタンをクリックしてください。再セットアップしない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2225-I

データベースのセットアップが完了しました。

(S)

処理を終了します。

KDSO2226-I

データベースのバックアップが完了しました。

(S)

処理を終了します。

KDSO2227-I

データベースのリストアが完了しました。

(S)

処理を終了します。

KDSO2228-I

データベースの再編成が完了しました。

(S)

処理を終了します。

KDSO2229-I

データベースの CSV バックアップが完了しました。

(S)

処理を終了します。

KDSO2230-I

データベースの CSV リストアが完了しました。

(S)

処理を終了します。

KDSO2231-I

データベースのパスワードの変更が完了しました。

(S)

処理を終了します。

KDSO2232-E

データベースとの接続に失敗しました。

(S)

処理を中止します。

(O)

- データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- [マネージャセットアップ] ダイアログで設定したデータベースのログイン ID およびパスワードの指定が正しいか確認してください。

KDSO2233-E

データベースのセットアップに失敗しました。その他のエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO2234-E

データベースのバックアップに失敗しました。

(S)

処理を中止します。

(O)

メッセージログファイルに出力されているメッセージ ID が KDSO04nn-Z のエラーメッセージに従って対処してください。

KDSO2235-E

データベースのリストアに失敗しました。

(S)

処理を中止します。

(O)

メッセージログファイルに出力されているメッセージ ID が KDSO04nn-Z のエラーメッセージに従って対処してください。

KDSO2236-E

データベースの再編成に失敗しました。

(S)

処理を中止します。

(O)

メッセージログファイルに出力されているメッセージ ID が KDSO05nn-Z のエラーメッセージに従って対処してください。

KDSO2237-E

データベースの CSV バックアップに失敗しました。

(S)

処理を中止します。

(O)

メッセージログファイルに出力されているメッセージ ID が KDSO06nn-Z のエラーメッセージに従って対処してください。

KDSO2238-E

データベースの CSV リストアに失敗しました。

(S)

処理を中止します。

(O)

メッセージログファイルに出力されているメッセージ ID が KDSO06nn-Z のエラーメッセージに従って対処してください。

KDSO2239-E

データベースのパスワードの変更に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO2240-E

データソースの削除に失敗しました。

(S)

処理を続行します。

(O)

[ODBC データソースアドミニストレータ] ダイアログの「システム DSN」タブから，マネージャセットアップのサービス名に指定した値と同じ名前のデータソースを削除してください。

KDSO2241-E

データソースの作成に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSO2244-E

マネージャセットアップによる設定が完了していません。

(S)

処理を終了します。

(O)

マネージャセットアップで設定したあと，再実行してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO2245-E

フォルダが作成できません。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2246-E

ローカルディスクに指定されたフォルダが作成できません。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2247-E

共有ディスクに指定されたフォルダが作成できません。

(S)

処理を中止します。

(O)

正しいパスを指定し，再実行してください。

KDSO2248-E

データベースのセットアップに失敗しました。ポート番号が重複しています。

(S)

処理を終了します。

(O)

重複しないポート番号を指定し，再実行してください。

KDSO2249-E

データベースのセットアップに失敗しました。ディスクの空き領域が不足しています。

(S)

処理を終了します。

(O)

空き領域を確保し，再実行してください。

KDSO2250-E

データベースのセットアップに失敗しました。メモリ不足が発生しました。

(S)

処理を終了します。

(O)

不要なアプリケーションを終了し，再実行してください。

KDSO2251-I

データベースマネージャを起動しました。

(S)

データベースマネージャを開始します。

KDSO2252-I

データベースマネージャを終了しました。

(S)

データベースマネージャを終了します。

KDSO2253-I

データベースのアップグレードはすでに実行済みです。

(S)

処理を終了します。

KDSO2254-I

データベースのアップグレードを開始します。

(S)

処理を開始します。

KDSO2255-I

データベースのアップグレードが完了しました。

(S)

処理を終了します。

KDSO2256-E

データベースのアップグレードに失敗しました。

(S)

処理を終了します。

(O)

バージョンアップ前の環境を復元した上で，再度，データベースをバージョンアップしてください。詳細については「15.3.2(2)　データベースのアップグレードができない」を参照してください。

KDSO2257-E

パスワードを入力してください。

(S)

処理を中止します。

(O)

パスワードを設定し，再実行してください。

KDSO2258-E

JP1 ユーザ情報の確認に失敗しました。

(S)

処理を終了します。

(O)

JP1/Base の認証サーバの設定が完了しているか，また認証サーバが正常に動作しているか確認してください。

KDSO2259-E

パスワードが正しくありません。

(S)

処理を中止します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO2260-E

変更前パスワードが正しくありません。

(S)

処理を中止します。

(O)

指定したパスワードに誤りがないか確認し，パスワードを再入力してください。

KDSO2261-E

変更後パスワードに使用できない文字が入力されました。パスワードに使用できるのは以下の文字です。
1 文字目：半角英字または記号
2 文字目以降：半角英数字または記号
入力可能な記号：# @ ¥

(S)

処理を中止します。

(O)

入力できる文字または文字数を確認し，パスワードを再入力してください。

KDSO2262-E

バックアップファイルの正当性確認に失敗しました。

(S)

処理を終了します。

(O)

バックアップ格納先ディレクトリに指定したディレクトリが，データベースの CSV バックアップで取得したディレクトリであるか確認してください。

KDSO2400-W

監査ログ収集マネージャはすでに起動しています。

(S)

処理を中止します。

(O)

起動している監査ログ収集マネージャを終了し，再実行してください。

KDSO2401-E

管理者権限がありません。

(S)

処理を中止します。

(O)

管理者権限を持つユーザで再実行してください。

KDSO2402-E

マネージャセットアップによる設定が完了していません。

(S)

処理を中止します。

(O)

マネージャセットアップによる設定を完了したあと，再実行してください。クラスタ環境で運用している場合，操作しているホストがアクティブ状態であるか確認してください。

KDSO2403-E

ファイル I/O エラーが発生しました。

(S)

処理を中止します。

(O)

空きディスク容量が十分か，ファイルシステムでトラブルが発生していないか確認してください。回復しない場合は，システム管理者に連絡してください。

KDSO2404-E

内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2405-I

監視を開始しました。サーバ＝［*サーバ名*］ プログラム＝［*プログラム名*］

(S)

処理を終了します。

KDSO2406-I

監視を停止しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

KDSO2407-I

監視はすでに開始しています。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

KDSO2408-I

監視はすでに停止しています。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

KDSO2409-I

設定情報を保存します。設定した内容は次回サービス起動時に有効になります。

(S)

処理を続行します。

KDSO2410-I

収集設定を変更します。設定した内容は次回監視開始時に有効になります。

(S)

処理を続行します。

KDSO2411-I

収集対象を一覧から削除しますか？
削除後はサービスの再起動が必要となります。

(S)

処理を続行します。

(O)

選択した収集対象を削除する場合は，［OK］ボタンをクリックし，サービスを再起動してください。選択した収集対象を削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2412-I

監視を開始しますか?

(S)

処理を続行します。

(O)

選択した収集対象の監視を開始する場合は，［OK］ボタンをクリックしてください。選択した収集対象の監視を開始しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2413-I

監視を停止しますか？

(S)

処理を続行します。

(O)

選択した収集対象の監視を停止する場合は，［OK］ボタンをクリックしてください。選択した収集対象の監視を停止しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2414-I

即時収集を開始しますか?

(S)

処理を続行します。

(O)

監査ログの即時収集を開始する場合は，［OK］ボタンをクリックしてください。監査ログの即時収集を開始しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2415-I

製品定義を一覧から削除しますか?

(S)

処理を続行します。

(O)

選択した収集対象の製品定義を削除する場合は，［OK］ボタンをクリックしてください。選択した収集対象の製品定義を削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2416-W

監視の開始は成功しましたが自動起動の設定に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

(O)

サーバの JP1/Base の設定とファイルシステムに異常が発生していないかどうかを確認し，再実行してください。

KDSO2417-W

監視の停止は成功しましたが自動起動の設定解除に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

(O)

サーバの JP1/Base の設定とファイルシステムに異常が発生していないかどうかを確認し，再実行してください。

KDSO2418-E

監視の開始に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

監査ログ収集対象サーバの JP1/Base の設定，監査ログ専用イベントサーバの設定，および動作定義ファイルの記述を確認し，再実行してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO2419-E

監視の停止に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

監査ログ収集対象サーバの JP1/Base の設定，監査ログ専用イベントサーバの設定を確認し，再実行してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO2420-E

入力した値の文字数が最小文字数より小さいです。

(S)

処理を中止します。

(O)

入力項目の最小文字数を確認し，再入力してください。

KDSO2421-E

入力した値の文字数が最大文字数より大きいです。

(S)

処理を中止します。

(O)

入力項目の最大文字数を確認し，再入力してください。

KDSO2422-E

入力した値の数値が最小値より小さいです。

(S)

処理を中止します。

(O)

入力項目の最小値を確認し，再入力してください。

KDSO2423-E

入力した値の数値が最大値より大きいです。

(S)

処理を中止します。

(O)

入力項目の最大値を確認し，再入力してください。

KDSO2424-E

使用できない文字が使われています。

(S)

処理を中止します。

(O)

入力項目に使用できない文字を確認し，再入力してください。

KDSO2425-E

指定したプログラムはすでに設定されています。

(S)

処理を中止します。

(O)

サーバ名およびプログラム名を再確認してください。

KDSO2426-E

指定したディレクトリが見つかりません。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

監視するログファイルのフォルダが存在していることを確認し，再実行してください。

KDSO2427-E

サービスまたはデーモンが起動していません。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

JP1/Base のログファイルトラップのサービスを起動し，再実行してください。

KDSO2428-E

サーバの設定が完了していません。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。「最新の情報に更新」を実行すると，次のサーバの処理を継続します。

(O)

該当サーバにアダプタコマンドがコピーされているか確認し，再実行してください。「最新の情報に更新」を実行したときにこのメッセージが表示された場合，プログラム名には「－」が出力されます。

KDSO2429-E

サーバでメモリが不足しています。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。「最新の情報に更新」を実行すると，次のサーバの処理を継続します。

(O)

不要なアプリケーションを終了し，再実行してください。「最新の情報に更新」を実行したときにこのメッセージが表示された場合，プログラム名には「－」が出力されます。

KDSO2430-E

サーバへの接続に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。「最新の情報に更新」を実行すると，次のサーバの処理を継続します。

(O)

イベントサーバと TCP/IP 通信が確立されているか，JP1/Base の環境設定が正しいか確認し，再実行してください。「最新の情報に更新」を実行したときにこのメッセージが表示された場合，プログラム名には「－」が出力されます。

KDSO2431-E

サーバとの通信中にエラーが発生しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。「最新の情報に更新」を実行すると，次のサーバの処理を継続します。

(O)

JP1/Base の設定を確認し，再実行してください。「最新の情報に更新」を実行したときにこのメッセージが表示された場合，プログラム名には「－」が出力されます。また，該当サーバで，古いバージョンのアダプタコマンドを利用していることがあります。「最新の情報に更新」を実行する場合は，最新バージョンのアダプタコマンドに入れ替えたあと，再実行してください。

KDSO2432-E

定義ファイルの読み込みに失敗しました。ファイル I/O エラーが発生しました。

(S)

処理を中止します。

(O)

ファイルシステムにトラブルが発生していないか確認し，再実行してください。

KDSO2434-E

パスの指定に誤りがあります。

(S)

処理を中止します。

(O)

監視するログファイルが格納されているフォルダを確認し，再入力してください。

KDSO2435-I

収集設定を追加しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

KDSO2436-I

収集設定を編集しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

KDSO2437-I

収集設定を削除しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を終了します。

KDSO2438-E

収集設定の追加に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2439-E

収集設定の編集に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2440-E

収集設定の削除に失敗しました。サーバ=［*サーバ名*］ プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2442-E

指定したプログラム名はすでに定義されています。

(S)

処理を中止します。

(O)

別のプログラム名を指定してください。

KDSO2443-E

プログラム名に対応する動作定義ファイルが存在しません。

(S)

処理を中止します。

(O)

動作定義ファイルを作成してください。

KDSO2444-I

監査ログ収集マネージャを起動しました。

(S)

監査ログ収集マネージャを開始します。

KDSO2445-I

監査ログ収集マネージャを終了しました。

(S)

監査ログ収集マネージャを終了します。

KDSO2446-I

定時収集の設定に成功しました。

(S)

処理を続行します。

KDSO2447-E

定時収集の設定に失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2448-E

製品定義ファイルの読み込みに失敗しました。

(S)

処理を中止します。

(O)

製品定義ファイルが存在していることを確認し，再実行してください。

KDSO2449-E

正規化ルールファイルの読み込みに失敗しました。

(S)

処理を中止します。

(O)

正規化ルールファイルが存在していることを確認し，再実行してください。

KDSO2450-E

入力した値の行数が最大行数より大きいです。

(S)

処理を中止します。

(O)

入力項目の最大文行数を確認し，再入力してください。

KDSO2451-E

入力した値の文字数が一行あたりの最大文字数より大きいです。

(S)

処理を中止します。

(O)

入力項目の最大文字数を確認し，再入力してください。

KDSO2452-E

空行が設定されています。

(S)

処理を中止します。

(O)

ログファイル名を再入力してください。

KDSO2453-I

状態取得に成功しました。サーバ=［*サーバ名*］

(S)

処理を続行します。

KDSO2454-E

状態取得に失敗しました。サーバ=［*サーバ名*］

(S)

処理を続行します。

(O)

監査ログ収集対象サーバの JP1/Base の設定，監査ログ専用イベントサーバの設定を確認し，再実行してください。再実行しても回復しない場合は，システム管理者に連絡してください。

KDSO2455-E

メモリ不足が発生しました。

(S)

処理を中止します。

(O)

不要なアプリケーションを終了し，再実行してください。

KDSO2456-W

JP1/Audit Management - Manager のサービスが停止しています。

(S)

処理を中止します。

(O)

次のサービスを起動した上で，再実行してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

KDSO2457-I

即時収集の開始に成功しました。

(S)

処理を終了します。

KDSO2458-E

即時収集の開始に失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2459-I

最新の情報に更新しますか? この処理には数分掛かる場合があります。

(S)

処理を続行します。

(O)

［監査ログ収集マネージャ］ウィンドウの表示内容を最新の情報に更新する場合は，［OK］ボタンをクリックしてください。［監査ログ収集マネージャ］ウィンドウの表示内容を最新の情報に更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2460-I

収集対象を一覧から削除しますか？

削除後はサービスの再起動が必要となります。

監視中の項目は停止後に削除されます。

(S)

処理を続行します。

(O)

選択した収集対象を削除する場合は，［OK］ボタンをクリックし，サービスを再起動してください。選択した収集対象を削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2461-I

収集設定を追加します。設定した内容は監視開始時に有効になります。

(S)

処理を続行します。

KDSO2462-I

製品定義を追加しました。プログラム＝［*プログラム名*］

(S)

処理を終了します。

KDSO2463-I

製品定義を編集しました。プログラム＝［*プログラム名*］

(S)

処理を終了します。

KDSO2464-I

製品定義を削除しました。プログラム＝［*プログラム名*］

(S)

処理を終了します。

KDSO2465-E

製品定義の追加に失敗しました。プログラム＝［*プログラム名*］

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2466-E

製品定義の編集に失敗しました。プログラム＝［*プログラム名*］

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2467-E

製品定義の削除に失敗しました。プログラム＝［*プログラム名*］

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO2468-I

製品定義を一覧から削除しますか? 標準提供の製品定義は削除されません。

(S)

処理を続行します。

(O)

選択した収集対象の製品定義を削除する場合は，［OK］ボタンをクリックしてください。選択した収集対象の製品定義を削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2469-I

製品定義を一覧から削除しますか? 収集設定に指定されている製品定義は削除されません。

(S)

処理を続行します。

(O)

選択した収集対象の製品定義を削除する場合は，［OK］ボタンをクリックしてください。選択した収集対象の製品定義を削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2470-I

製品定義を一覧から削除しますか? 標準提供と収集設定に指定されている製品定義は削除されません。

(S)

処理を続行します。

(O)

選択した収集対象の製品定義を削除する場合は，［OK］ボタンをクリックしてください。選択した収集対象の製品定義を削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO2471-E

入力したログファイルに重複が存在します。ファイル名=［*ファイル名*］

(S)

処理を中止します。

(O)

入力項目の重複を確認し，再入力してください。

KDSO2472-I

製品定義を追加しました。

(S)

処理を終了します。

KDSO2473-I

製品定義を編集しました。

(S)

処理を終了します。

KDSO2474-E

プログラム名に使用できない文字が使われています。サーバ=［*サーバ名*］プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

プログラム名として使用できる文字を確認し，製品定義を再作成してから再実行してください。

KDSO2475-E

ログフォルダ名に使用できない文字が使われています。サーバ=［*サーバ名*］プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

ログフォルダ名として使用できる文字を確認し，収集対象の設定を修正してから再実行してください。

KDSO2476-E

ログファイル名に使用できない文字が使われています。サーバ=［*サーバ名*］プログラム=［*プログラム名*］

(S)

処理を中止します。

(O)

ログファイル名として使用できる文字を確認し，製品定義を修正してから再実行してください。

KDSO2477-W

JP1/AJS3 では，ホストまたはスケジューラサービス毎に登録を行ってください。

(S)

処理を続行します。

(O)

JP1/AJS3 では，ホストまたはスケジューラサービスごとにスケジューラログが出力されます。それぞれを収集対象として登録してください。

KDSO3001-E

ログインに失敗しました。ユーザ ID もしくはパスワードが不正です。

(S)

処理を中止します。

(O)

ユーザ ID またはパスワードを確認してください。

KDSO3002-E

ログインに失敗しました。論理ホスト名の取得に失敗しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3003-E

ログインに失敗しました。ユーザ認証でエラーが発生しました。

(S)

処理を中止します。

(O)

JP1/Base の設定を確認してください。

KDSO3004-E

ログインに失敗しました。内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3005-W

ユーザ ID が入力されていません。

(S)

処理を中止します。

(O)

ユーザ ID を入力してください。

KDSO3006-I

サーバとの接続が切断されました。ログインしてください。

(S)

処理を中止します。

KDSO3007-E

ログアウトに失敗しました。ログアウト処理でエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3008-E

ログアウトに成功しました。一時ファイルの削除に失敗しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を続行します。

(O)

システム管理者に連絡してください。

KDSO3009-E

ログアウトに失敗しました。内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3010-I

ログアウトを開始しました。

(S)

処理を続行します。

KDSO3011-I

ログアウトに成功しました。

(S)

処理を終了します。

KDSO3012-I

ログインを開始しました。

(S)

処理を続行します。

KDSO3013-I

ログインに成功しました。

(S)

処理を終了します。

KDSO3014-I

既にログアウトされています。

(S)

処理を中止します。

KDSO3015-E

ログインに失敗しました。データベースのバージョンが製品バージョンに対応していません。

(S)

処理を中止します。

(O)

データベースのアップグレードを実行してください。

KDSO3016-E

ログインに失敗しました。データベースのバージョンチェックでエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3017-E

ログインに失敗しました。データベースの接続でエラーが発生しました。

(S)

処理を中止します。

(O)

- データベースマネージャでデータベースをアップグレードしてください。
- データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- マネージャセットアップのデータベース情報の設定を確認してください。

KDSO3053-W

バックアップ情報を選択してください。

(S)

処理を中止します。

(O)

バックアップ情報を選択してください。

KDSO3054-E

バックアップ履歴の検索に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3055-E

バックアップ履歴の検索に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3056-E

バックアップ履歴の検索に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3057-E

バックアップ情報のダウンロードに失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3058-E

バックアップ情報のダウンロードに失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3059-E

バックアップ情報のダウンロードに失敗しました。バックアップファイルが見つかりませんでした。

(S)

処理を中止します。

(O)

再度検索を実行したあと，バックアップ情報を確認してください。または，バックアップファイルがあるか確認してください。

KDSO3060-E

バックアップ情報のダウンロードに失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3061-I

バックアップ情報のダウンロードを開始しました。(File Name=*詳細情報*)

(S)

処理を続行します。

KDSO3062-I

バックアップ情報のダウンロード要求に成功しました。(File Name=*詳細情報*)

(S)

処理を終了します。

KDSO3063-I

バックアップ履歴の検索を開始しました。

(S)

処理を続行します。

KDSO3064-I

バックアップ履歴の検索に成功しました。

(S)

処理を終了します。

KDSO3101-W

条件項目に表示する項目がありません。

(S)

処理を中止します。

(O)

条件項目に表示する項目を最低一つは設定してください。

KDSO3102-W

結果項目に表示する項目がありません。

(S)

処理を中止します。

(O)

結果項目に表示する項目を最低一つは設定してください。

KDSO3103-E

表示設定情報の取得に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3104-E

表示設定情報の取得に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3105-E

表示設定情報の取得に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3106-E

表示設定情報の更新に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3107-E

表示設定情報の更新に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3108-E

表示設定情報の更新に失敗しました。内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3112-I

表示設定情報の更新を開始しました。(Screen Name=*詳細情報*)

(S)

処理を続行します。

KDSO3113-I

表示設定情報の更新に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3116-I

表示設定情報の取得を開始しました。(Screen Name=*詳細情報*)

(S)

処理を続行します。

KDSO3117-I

表示設定情報の取得に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3118-I

監査ログ検索画面の表示設定情報を更新します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を更新する場合は，［OK］ボタンをクリックしてください。表示設定情報を更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3119-I

監査ログ集計画面の表示設定情報を更新します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を更新する場合は，［OK］ボタンをクリックしてください。表示設定情報を更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3120-I

バックアップ履歴管理画面の表示設定情報を更新します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を更新する場合は，［OK］ボタンをクリックしてください。表示設定情報を更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3121-I

監査ログ検索画面の表示設定情報を初期化します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を初期化する場合は，［OK］ボタンをクリックしてください。表示設定情報を初期化しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3122-I

監査ログ集計画面の表示設定情報を初期化します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を初期化する場合は，［OK］ボタンをクリックしてください。表示設定情報を初期化しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3123-I

バックアップ履歴画面の表示設定情報を初期化します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を初期化する場合は，［OK］ボタンをクリックしてください。表示設定情報を初期化しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3124-I

表示設定情報の初期化を開始しました。(Screen Name=*詳細情報*)

(S)

処理を続行します。

KDSO3125-I

表示設定情報の初期化に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3126-E

表示設定情報の初期化に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3127-E

表示設定情報の初期化に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3128-E

表示設定情報の初期化に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3151-E

EUR Print Service でエラーが発生しました。(ProgramID=*詳細情報 1,*Error Code=*詳細情報 2*,Reason=*詳細情報 3*,Source=*詳細情報 4*)

(S)

処理を中止します。

(O)

EUR がインストールされているかを確認してください。

KDSO3152-W

パターン名を指定してください。

(S)

処理を中止します。

(O)

パターン名を指定してください。

KDSO3153-I

パターンを更新します。よろしいですか？

(S)

処理を続行します。

(O)

パターンを更新する場合は，［OK］ボタンをクリックしてください。パターンを更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3154-I

パターンを削除します。よろしいですか？

(S)

処理を続行します。

(O)

パターンを削除する場合は，［OK］ボタンをクリックします。パターンを削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3156-E

ファイルの作成に失敗しました。(File Name=*詳細情報 1*,Error Code=*詳細情報 2*,Reason=*詳細情報 3*,Source=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3157-I

ファイルの作成に成功しました。(File Name=*詳細情報*)

(S)

処理を続行します。

KDSO3161-E

CSV ファイルの出力に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3162-E

CSV ファイルの出力に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3163-E

CSV ファイルの出力に失敗しました。ファイルの生成でエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3165-E

CSV ファイルの出力に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3166-E

PDF ファイルの出力に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3167-E

PDF ファイルの出力に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3168-E

PDF ファイルの出力に失敗しました。EUR Print Service でエラーが発生しました。

(S)

処理を中止します。

(O)

EUR がインストールされているかを確認してください。

KDSO3169-E

PDF ファイルの出力に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3170-E

検索に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3171-E

検索に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3172-E

検索に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3173-E

パターンの適用に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3174-E

パターンの適用に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3175-E

パターンの適用に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3176-E

パターンの保存に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3177-E

パターンの保存に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3178-E

パターンの保存に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3179-E

パターンの削除に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3180-E

パターンの削除に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3181-E

パターンの削除に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3182-W

既定のパターンを保存もしくは削除することはできません。

(S)

処理を中止します。

KDSO3183-W

選択されたパターンは存在していません。

(S)

処理を中止します。

(O)

画面を更新してパターンを確認してください。

KDSO3186-I

CSV ファイルの出力を開始しました。

(S)

処理を続行します。

KDSO3187-I

CSV ファイルの出力に成功しました。

(S)

処理を終了します。

KDSO3188-I

PDF ファイルの出力を開始しました。

(S)

処理を続行します。

KDSO3189-I

PDF ファイルの出力に成功しました。

(S)

処理を終了します。

KDSO3190-I

パターンの適用を開始しました。(Pattern Name=*詳細情報*)

(S)

処理を続行します。

KDSO3191-I

パターンの適用に成功しました。(Pattern Name=*詳細情報*)

(S)

処理を終了します。

KDSO3192-I

パターンの保存を開始しました。(Pattern Name=*詳細情報 1*,Path=*詳細情報 2*)

(S)

処理を続行します。

KDSO3193-I

パターンの保存に成功しました。(Pattern Name=*詳細情報 1*,Path=*詳細情報 2*)

(S)

処理を終了します。

KDSO3194-I

パターンの削除を開始しました。(Pattern Name=*詳細情報*)

(S)

処理を続行します。

KDSO3195-I

パターンの削除に成功しました。(Pattern Name=*詳細情報*)

(S)

処理を終了します。

KDSO3196-E

PDF ファイルの出力に失敗しました。ファイルの生成でエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3197-I

検索を開始しました。

(S)

処理を続行します。

KDSO3198-I

検索に成功しました。

(S)

処理を終了します。

KDSO3199-I

集計を開始しました。

(S)

処理を続行します。

KDSO3200-I

集計に成功しました。

(S)

処理を終了します。

KDSO3201-E

集計に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3202-E

集計に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3203-E

集計に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3204-I

パターンを保存します。よろしいですか？

(S)

処理を続行します。

(O)

パターンを保存する場合は，［OK］ボタンをクリックします。パターンを保存しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3205-W

画面を更新してください。

(S)

処理を中止します。

(O)

画面を更新して再実行してください。

KDSO3206-W

「@」から始まるパターン名は保存できません。

(S)

処理を中止します。

(O)

「@」以外から始まるパターン名で保存してください。

KDSO3207-I

監査ログレポートの表示を開始しました。

(S)

処理を続行します。

KDSO3208-I

監査ログレポートの表示に成功しました。

(S)

処理を終了します。

KDSO3209-E

監査ログレポートの表示に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3210-E

監査ログレポートの表示に失敗しました。データベースでエラーが発生しました。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3211-E

監査ログレポートの表示に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3212-E

固有情報の分析に失敗しました。(Program Name=*詳細情報 1*,Peculiar Information=*詳細情報 2*)

(S)

処理を続行します。

(O)

監査ログレポート定義ファイルの内容を確認してください。

KDSO3213-I

サーバとの接続が切断されました。

(S)

処理を中止します。

KDSO3214-I

集計結果グラフの表示を開始しました。

(S)

処理を続行します。

KDSO3215-I

集計結果グラフの表示に成功しました。

(S)

処理を終了します。

KDSO3216-E

集計結果グラフの表示に失敗しました。グラフの生成でエラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3217-E

集計結果グラフの表示に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3218-W

集計結果を選択してください。

(S)

処理を中止します。

(O)

集計結果を選択してください。

KDSO3219-E

パターンの適用に失敗しました。パターンが見つかりません。

(S)

処理を中止します。

(O)

再度ログインしたあと，パターンを確認してください。

KDSO3220-E

監査ログレポートの表示に失敗しました。定義ファイルが見つかりませんでした。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

監査ログ標準レポート定義ファイルまたは監査ログレポート定義ファイルの内容を確認してください。

KDSO3221-E

監査ログレポート CSV ファイルのダウンロードに失敗しました。ファイルが見つかりませんでした。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

再度レポートを実行したあと，CSV を実行してください。

KDSO3225-E

業務メニュー内に，同じ名前のフォルダが存在する場合，パターンを保存することはできません。

(S)

処理を中止します。

(O)

パターン名を変更して再度保存してください。

KDSO3226-E

集計結果グラフの表示に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3227-E

集計結果グラフの表示に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3228-E

監査ログレポートの表示に失敗しました。ファイルの生成でエラーが発生しました。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3229-E

集計結果グラフの表示に失敗しました。ファイルの生成でエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3230-E

ファイルの作成に失敗しました。(File Name=*詳細情報 1*,Error Code=*詳細情報 2*,Reason=*詳細情報 3*,Source=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3231-I

ファイルの作成に成功しました。(File Name=*詳細情報*)

(S)

処理を続行します。

KDSO3232-E

監査ログレポートの表示に失敗しました。定義ファイルが不正です。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

監査ログ標準レポート定義ファイルまたは監査ログレポート定義ファイルの内容を確認してください。

KDSO3233-I

監査ログ統計情報のグラフ表示を開始しました。

(S)

処理を続行します。

KDSO3234-I

監査ログ統計情報の CSV 出力を開始しました。

(S)

処理を続行します。

KDSO3235-I

監査ログ統計情報のグラフ表示に成功しました。

(S)

処理を終了します。

KDSO3236-I

監査ログ統計情報の CSV 出力に成功しました。

(S)

処理を終了します。

KDSO3237-E

監査ログ統計情報のグラフ表示に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3238-E

監査ログ統計情報のグラフ表示に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3239-E

監査ログ統計情報のグラフ表示に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3240-E

監査ログ統計情報の CSV ファイルの出力に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3241-E

監査ログ統計情報の CSV ファイルの出力に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3242-E

監査ログ統計情報の CSV ファイルの出力に失敗しました。ファイルの生成でエラーが発生しました。(File Name=*詳細情報 1*,Error Code=*詳細情報 2*,Reason=*詳細情報 3*,Source=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3243-E

監査ログ統計情報の CSV ファイルの出力に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3244-I

監査ログ統計情報の HTML 出力を開始しました。

(S)

処理を続行します。

KDSO3245-I

監査ログ統計情報の HTML 出力に成功しました。

(S)

処理を終了します。

KDSO3246-E

監査ログ統計情報の HTML ファイルの出力に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3247-E

監査ログ統計情報の HTML ファイルの出力に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3248-E

監査ログ統計情報の HTML ファイルの出力に失敗しました。ファイルの生成でエラーが発生しました。(File Name=*詳細情報 1*,Error Code=*詳細情報 2*,Reason=*詳細情報 3*,Source=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3249-E

監査ログ統計情報の HTML ファイルの出力に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3251-E

内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3252-E

オブジェクトの生成に失敗しました。(ProgramID=*詳細情報 1*,Error Code=*詳細情報 2*,Reason=*詳細情報 3*,Source=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3253-E

画面表示に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3254-E

画面表示に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3255-E

画面表示に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3256-E

パターンの保存に失敗しました。不要な監査ログ統計情報を削除してください。

(S)

処理を中止します。

(O)

不要な監査ログ統計情報を削除してください。

KDSO3257-E

パターンの保存もしくは更新に失敗しました。不要な集計パターンを削除してください。

(S)

処理を中止します。

(O)

不要な集計パターンを削除してください。

KDSO3258-I

監査ログ管理画面の Web アプリケーションが開始しました。

(S)

システムの処置はありません。

KDSO3259-I

監査ログ管理画面の Web アプリケーションが終了しました。

(S)

システムの処置はありません。

KDSO3260-I

画面表示を開始しました。

(S)

処理を続行します。

KDSO3261-I

画面表示に成功しました。

(S)

処理を終了します。

KDSO3262-I

機能ツリーの表示を開始しました。

(S)

処理を続行します。

KDSO3263-I

機能ツリーの表示に成功しました。

(S)

処理を終了します。

KDSO3264-E

機能ツリーの表示に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3265-E

機能ツリーの表示に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3266-E

機能ツリーの表示に失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3267-I

サーバとの接続が切断されます。

(S)

システムの処置はありません。

KDSO3268-I

サーバとの接続が切断されました。(UserID=*詳細情報*)

(S)

システムの処置はありません。

KDSO3269-W

サーバとの接続が切断されました。一時ファイルの削除に失敗しました。

(S)

システムの処置はありません。

(O)

システム管理者に連絡してください。

KDSO3270-I

パターンを更新します。よろしいですか？

統計パターンとして使用している場合は，統計パターンも更新されるため，再度統計情報を生成してください。

(S)

処理を続行します。

(O)

パターンを更新する場合は，［OK］ボタンをクリックしてください。パターンを更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3271-I

パターンを削除します。統計パターンの条件も削除されます。よろしいですか？

(S)

処理を続行します。

(O)

パターンを削除する場合は，［OK］ボタンをクリックしてください。パターンを削除しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3272-I

監査ログ統計画面の表示設定情報を更新します。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を更新する場合は，［OK］ボタンをクリックしてください。表示設定情報を更新しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3273-I

監査ログ統計画面の表示設定情報を初期化します。統計パターンの登録は初期化されません。よろしいですか？

(S)

処理を続行します。

(O)

表示設定情報を初期化する場合は，［OK］ボタンをクリックしてください。表示設定情報を初期化しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3274-E

監査ログ統計情報のグラフ表示に失敗しました。統計パターンが見つかりませんでした。(Pattern Name=*詳細情報*)

(S)

処理を中止します。

(O)

統計パターンの設定を確認してください。

KDSO3275-E

監査ログ統計情報の CSV ファイルの出力に失敗しました。統計パターンが見つかりませんでした。(Pattern Name=*詳細情報*)

(S)

処理を中止します。

(O)

統計パターンの設定を確認してください。

KDSO3276-E

監査ログ統計情報の HTML ファイルの出力に失敗しました。統計パターンが見つかりませんでした。(Pattern Name=*詳細情報*)

(S)

処理を中止します。

(O)

統計パターンの設定を確認してください。

KDSO3301-I

機能ツリーの更新を開始しました。

(S)

処理を続行します。

KDSO3302-I

機能ツリーの更新に成功しました。

(S)

処理を終了します。

KDSO3303-E

機能ツリーの更新に失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3304-E

機能ツリーの更新に失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3305-E

機能ツリーの更新に失敗しました。内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3306-W

同一業務メニュー内に，同じ名前のフォルダまたはパターンが存在します。異なる名前を入力してください。

(S)

処理を中止します。

(O)

重複しない名前を入力し，再度実行してください。

KDSO3307-W

フォルダ階層が制限を超えるため，フォルダの作成を実行できません。

(S)

処理を中止します。

(O)

フォルダ階層を確認してください。

KDSO3308-W

移動先またはコピー先の業務メニュー内に，同じ名前のフォルダまたはパターンが存在する場合，移動またはコピーすることはできません。(*詳細情報*)

(S)

処理を中止します。

(O)

移動先またはコピー先の業務メニューのフォルダ名またはパターン名を確認してください。

KDSO3309-W

フォルダ階層が制限を超えるため，移動またはコピーを実行できません。

(S)

処理を中止します。

(O)

フォルダ階層を確認してください。

KDSO3310-I

集計パターンを監査ログ検索の業務メニューに移動する場合，統計パターンの条件も削除されます。よろしいですか？

(S)

処理を続行します。

(O)

パターンを移動する場合は［OK］ボタンをクリックしてください。パターンを移動しない場合は［キャンセル］ボタンをクリックしてください。

KDSO3311-I

選択したフォルダとフォルダ内のすべてのフォルダおよびパターンを削除します。よろしいですか？

(S)

処理を続行します。

(O)

フォルダを削除する場合は［OK］ボタンをクリックしてください。フォルダを削除しない場合は［キャンセル］ボタンをクリックしてください。

KDSO3312-I

選択したパターンを削除します。よろしいですか？

(S)

処理を続行します。

(O)

パターンを削除する場合は［OK］ボタンをクリックしてください。パターンを削除しない場合は［キャンセル］ボタンをクリックしてください。

KDSO3313-I

選択したフォルダとフォルダ内のすべてのフォルダおよびパターンを削除します。統計パターンの条件も削除されます。よろしいですか？

(S)

処理を続行します。

(O)

フォルダを削除する場合は［OK］ボタンをクリックしてください。フォルダを削除しない場合は［キャンセル］ボタンをクリックしてください。

KDSO3314-I

選択したパターンを削除します。統計パターンの条件も削除されます。よろしいですか？

(S)

処理を続行します。

(O)

パターンを削除する場合は［OK］ボタンをクリックしてください。パターンを削除しない場合は［キャンセル］ボタンをクリックしてください。

KDSO3315-I

機能ツリーを更新します。よろしいですか？

(S)

処理を続行します。

(O)

機能ツリーを更新する場合は［OK］ボタンをクリックしてください。機能ツリーを更新しない場合は［キャンセル］ボタンをクリックしてください。

KDSO3316-W

操作を実行できません。更新を実行後，再度操作を実行してください。

(S)

処理を中止します。

(O)

操作数が多いため，操作を実行できません。更新を実行後，再度操作を実行してください。

KDSO3317-W

「@」から始まるフォルダ名および「¥」を含むフォルダ名は作成できません。

(S)

処理を中止します。

(O)

「@」以外から始まり，「¥」を含まないフォルダ名で作成してください。

KDSO3318-W

指定したフォルダには移動できません。

(S)

処理を中止します。

(O)

指定したフォルダ以外のフォルダへ移動してください。

KDSO3320-W

操作対象のフォルダおよびパターン数が多すぎるため，操作を実行できません。

(S)

処理を中止します。

(O)

操作対象の配下にあるフォルダおよびパターン数が少ないフォルダで操作を実行してください。

KDSO3321-W

フォルダおよびパターン数が制限を超えるため，フォルダまたはパターンを作成できません。

(S)

処理を中止します。

(O)

ユーザ作成の最上位フォルダ内にあるフォルダおよびパターン数が制限を超えないように，フォルダまたはパターンを作成してください。

KDSO3323-W

同一業務メニュー内に，同じ名前のフォルダまたはパターンが存在します。更新を実行後，再度操作を実行してください。

(S)

処理を中止します。

(O)

画面を表示したときのフォルダ名またはパターン名が重複しているため，操作を実行できません。更新を実行後，再度操作を実行してください。

KDSO3325-E

機能ツリーの更新に失敗しました。既に機能ツリーが更新されています。画面を閉じて，再度実行してください。

(S)

処理を中止します。

(O)

画面を表示し直して，機能ツリーを確認後，再度実行してください。

KDSO3326-E

パターンの保存に失敗しました。格納先フォルダが見つかりません。

(S)

処理を中止します。

(O)

格納先のフォルダが存在するかどうかを確認してください。

KDSO3327-E

パターンの保存に失敗しました。フォルダおよびパターン数が制限を超えました。

(S)

処理を中止します。

(O)

保存先の最上位フォルダ内のフォルダおよびパターン数が制限を超えたため，不要なフォルダまたはパターンを削除し，再度保存してください。

KDSO3328-E

パターンの保存に失敗しました。業務メニュー内に，同じ名前のフォルダが存在します。

(S)

処理を中止します。

(O)

保存先の業務メニュー内のフォルダを確認してください。

KDSO3329-I

パターン情報のインポートを開始しました。

(S)

処理を続行します。

KDSO3330-E

パターン情報のインポートに失敗しました。ファイル形式が不正です。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

ファイル形式が正しいか確認してください。

KDSO3331-E

パターン情報のインポートに失敗しました。レコード形式が不正です。(File Name=*詳細情報 1*,Line No=*詳細情報 2*)

(S)

処理を中止します。

(O)

ファイル内のレコード形式が正しいか確認してください。

KDSO3332-E

パターン情報のインポートに失敗しました。パターン情報ファイル内に重複するノード情報が存在します。(File Name=*詳細情報 1*,Line No=*詳細情報 2*)

(S)

処理を中止します。

(O)

ファイル内に整合性のないデータがないかを確認してください。

KDSO3333-E

パターン情報のインポートに失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3334-E

パターン情報のインポートに失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。セットアップの設定が正しい場合，インポートするデータ数が多過ぎる可能性があります。インポートするデータ数を減らして，再度実行してください。

KDSO3335-E

パターン情報のインポートに失敗しました。パターン情報ファイルに，データベースと整合性のないデータが存在します。(File Name=*詳細情報 1*,Line No=*詳細情報 2*)

(S)

処理を中止します。

(O)

パターン情報ファイル内のデータに，最新の機能ツリーやパターンのデータと整合性がないデータが存在する可能性があります。次の項目に該当する場合は，修正してください。

- 格納先のフォルダが存在しない。
- 上書きするときの種別が異なっている。
- 上書きするときのパスが異なっている。
- 上書きするときの表示画面が異なっている。

KDSO3336-E

パターン情報のインポートに失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3337-W

パターン情報の上書きを実行しませんでした。パターンまたはフォルダが重複しました。(File Name=*詳細情報 1*,Line No=*詳細情報 2*)

(S)

処理を続行します。

KDSO3338-W

パターン情報の上書きを実行しました。パターンまたはフォルダが重複しました。(File Name=*詳細情報 1*,Line No=*詳細情報 2*)

(S)

処理を続行します。

KDSO3339-I

パターン情報のインポートに成功しました。(File Name=*詳細情報*)

(S)

処理を終了します。

KDSO3340-I

パターン情報のエクスポートを開始しました。

(S)

処理を続行します。

KDSO3341-E

パターン情報のエクスポートに失敗しました。データベース接続情報の取得でエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3342-E

パターン情報のエクスポートに失敗しました。データベースでエラーが発生しました。

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3343-E

パターン情報のエクスポートに失敗しました。ファイルの出力でエラーが発生しました。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3344-E

パターン情報のエクスポートに失敗しました。ダウンロード要求でエラーが発生しました。(File Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3345-E

パターン情報のエクスポートに失敗しました。内部エラーが発生しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*,Source=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3346-I

パターン情報のエクスポートに成功しました。(File Name=*詳細情報*)

(S)

処理を終了します。

KDSO3347-E

パターン情報のインポートに失敗しました。ファイルの生成でエラーが発生しました。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3348-E

パターン情報のインポートに失敗しました。ノード制限数を超えました。(File Name=*詳細情報 1*,Line No=*詳細情報 2*)

(S)

処理を中止します。

(O)

- 対象となるユーザ作成の最上位フォルダ内のフォルダやパターン数が制限を超える場合，不要なフォルダまたはパターンを削除してください。
- 最大フォルダ階層を超える場合，フォルダ階層を超えないようにフォルダを作成してください。

KDSO3349-I

パターン情報ファイルをインポートします。よろしいですか？

集計パターンを統計パターンとして使用している場合は，統計パターンも更新されるため，再度統計情報を生成してください。

(S)

処理を続行します。

(O)

インポートを実行する場合は，［OK］ボタンをクリックしてください。インポートを実行しない場合は，［キャンセル］ボタンをクリックしてください。

KDSO3350-E

パターン情報のインポートに失敗しました。ファイルが存在しない，またはファイル内にデータがありません。(File Name=*詳細情報*)

(S)

処理を中止します。

(O)

指定したファイルが存在するか，またはファイル内にデータが存在するかを確認してください。

KDSO3502-I

監査ログの検索に成功しました。(Screen Name=*詳細情報 1*,Operation=*詳細情報 2*)

(S)

処理を終了します。

KDSO3503-E

監査ログの検索に失敗しました。(Screen Name=*詳細情報 1*,Operation=*詳細情報 2*,Reason=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3505-I

パターンの取得に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3506-E

パターンの取得に失敗しました。(Screen Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3508-I

画面表示情報の取得に成功しました。(Screen Name=*詳細情報 1*,Field Name=*詳細情報 2*)

(S)

処理を終了します。

KDSO3509-E

画面表示情報の取得に失敗しました。(Screen Name=*詳細情報 1*,Field Name=*詳細情報 2*,Reason=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3511-I

パターンの適用に成功しました。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*)

(S)

処理を終了します。

KDSO3512-E

パターンの適用に失敗しました。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*,Reason=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3514-I

パターンの保存に成功しました。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を終了します。

KDSO3515-E

パターンの保存に失敗しました。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*,Path=*詳細情報 3*,Reason=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3517-I

パターンの削除に成功しました。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*)

(S)

処理を終了します。

KDSO3518-E

パターンの削除に失敗しました。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*,Reason=*詳細情報 3*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3520-I

バックアップ情報の検索に成功しました。

(S)

処理を終了します。

KDSO3521-E

バックアップ情報の検索に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3523-I

バックアップ情報の取得に成功しました。

(S)

処理を終了します。

KDSO3524-E

バックアップ情報の取得に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

バックアップファイルがあるか確認してください。

KDSO3526-I

表示設定情報の取得に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3527-E

表示設定情報の取得に失敗しました。(Screen Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3529-I

表示設定情報の更新に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3530-E

表示設定情報の更新に失敗しました。(Screen Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3531-I

データベースの接続に成功しました。

(S)

処理を終了します。

KDSO3532-E

データベースの接続に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3533-I

データベースの切断に成功しました。

(S)

処理を終了します。

KDSO3534-E

データベースの切断に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3535-I

データベース接続情報の取得に成功しました。

(S)

処理を終了します。

KDSO3536-E

データベース接続情報の取得に失敗しました。(Error Code=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3537-I

表示設定情報の削除に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3538-E

表示設定情報の削除に失敗しました。(Screen Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3539-I

機能ツリー情報の取得に成功しました。

(S)

処理を終了します。

KDSO3540-E

機能ツリー情報の取得に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3541-I

監査ログ統計情報の取得に成功しました。(Operation=*詳細情報*)

(S)

処理を続行します。

KDSO3542-E

監査ログ統計情報の取得に失敗しました。(Operation=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3543-I

統計パターンの取得に成功しました。(Screen Name=*詳細情報*)

(S)

処理を続行します。

KDSO3544-E

統計パターンの取得に失敗しました。(Screen Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3547-I

統計パターン情報の更新に成功しました。

(S)

処理を終了します。

KDSO3548-E

統計パターン情報の更新に失敗しました。(Pattern Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3549-E

パターンの保存に失敗しました。不要な監査ログ統計情報を削除してください。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を中止します。

(O)

不要な監査ログ統計情報を削除してください。

KDSO3550-E

パターンの保存もしくは更新に失敗しました。不要な集計パターンを削除してください。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を中止します。

(O)

不要な集計パターンを削除してください。

KDSO3551-I

パターンの更新に成功しました。同一条件のため更新しませんでした。(Screen Name=*詳細情報 1*,Pattern Name=*詳細情報 2*)

(S)

処理を続行します。

KDSO3552-I

機能ツリーの更新に成功しました。

(S)

処理を終了します。

KDSO3553-E

機能ツリーの更新に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3554-I

機能ツリー情報の取得に成功しました。(Screen Name=*詳細情報*)

(S)

処理を終了します。

KDSO3555-E

機能ツリー情報の取得に失敗しました。(Screen Name=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3556-I

*ノード*の作成に成功しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を終了します。

KDSO3557-I

*ノード*の名前の変更に成功しました。(Node Type=*詳細情報 1*,Old Name=*詳細情報 2*,New Name=*詳細情報 3*,Path=*詳細情報 4*)

(S)

処理を終了します。

KDSO3558-I

*ノード*の移動に成功しました。(Node Type=*詳細情報 1*,Old Name=*詳細情報 2*,New Name=*詳細情報 3*,From Path=*詳細情報 4*,To Path=*詳細情報 5*)

(S)

処理を終了します。

KDSO3559-I

*ノード*のコピーに成功しました。(Node Type=*詳細情報 1*,Old Name=*詳細情報 2*,New Name=*詳細情報 3*,From Path=*詳細情報 4*,To Path=*詳細情報 5*)

(S)

処理を終了します。

KDSO3560-I

ノードの削除に成功しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を終了します。

KDSO3561-E

ノードの作成に失敗しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*,Reason=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3562-E

ノードの名前の変更に失敗しました。(Node Type=*詳細情報 1*,Old Name=*詳細情報 2*,New Name=*詳細情報 3*,Path=*詳細情報 4*,Reason=*詳細情報 5*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3563-E

ノードの移動に失敗しました。(Node Type=*詳細情報 1*,Old Name=*詳細情報 2*,New Name=*詳細情報 3*,From Path=*詳細情報 4*,To Path=*詳細情報 5*,Reason=*詳細情報 6*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3564-E

ノードのコピーに失敗しました。(Node Type=*詳細情報 1*,Old Name=*詳細情報 2*,New Name=*詳細情報 3*,From Path=*詳細情報 4*,To Path=*詳細情報 5*,Reason=*詳細情報 6*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3565-E

ノードの削除に失敗しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*,Reason=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3566-I

ノードの表示設定に成功しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を終了します。

KDSO3567-E

ノードの表示設定に失敗しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*,Reason=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3568-I

ノードの非表示設定に成功しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*)

(S)

処理を終了します。

KDSO3569-E

ノードの非表示設定に失敗しました。(Node Type=*詳細情報 1*,Name=*詳細情報 2*,Path=*詳細情報 3*,Reason=*詳細情報 4*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3570-E

機能ツリーまたはパターンのインポートに失敗しました。(Line No=*詳細情報 1*,Reason=*詳細情報 2*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3571-I

機能ツリーおよびパターンのインポートに成功しました。

(S)

処理を終了します。

KDSO3572-E

機能ツリーまたはパターンのエクスポートに失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

- セットアップの設定を確認してください。
- 最大ノード作成数を超えた場合，不要なフォルダまたはパターンを削除してください。
- 統計項目 ID の最大値を超えた場合，不要な集計パターンを削除してください。
- パターン情報ファイルのデータと，最新の機能ツリーやパターンの画面表示に不整合がないかを確認してください。

KDSO3573-I

機能ツリーおよびパターンのエクスポートに成功しました。

(S)

処理を終了します。

KDSO3574-I

機能ツリーおよびパターンのインポートに成功しました。重複したノードを上書きしませんでした。

(S)

処理を続行します。

KDSO3575-I

機能ツリーおよびパターンのインポートに成功しました。重複したノードを上書きしました。

(S)

処理を続行します。

KDSO3752-I

ユーザ認証に成功しました。(UserID=*詳細情報 1*,Virtual Hostname=*詳細情報 2*)

(S)

処理を終了します。

KDSO3753-E

ユーザ認証に失敗しました。(UserID=*詳細情報 1*,Virtual Hostname=*詳細情報 2*,Error Code=*詳細情報 3*)

(S)

処理を中止します。

(O)

ユーザ ID やパスワードを確認するか，またはセットアップの設定を確認してください。

KDSO3754-E

JP1/Base の API でエラーが発生しました。(API Name=*詳細情報 1*,Error Code=*詳細情報 2*)

(S)

処理を中止します。

(O)

ユーザ ID やパスワードを確認するか，またはセットアップの設定を確認してください。

KDSO3755-I

論理ホスト名の取得に成功しました。(Virtual Hostname=*詳細情報*)

(S)

処理を終了します。

KDSO3756-E

論理ホスト名の取得に失敗しました。(Error Code=*詳細情報*)

(S)

処理を中止します。

(O)

セットアップの設定を確認してください。

KDSO3757-I

ユーザを認証しました。(Authentication Server Version=V6 or V6i)

(S)

処理を続行します。

KDSO3758-I

ユーザを認証しました。(Authentication Server Version=07-00 or 07-10 or 07-11)

(S)

処理を続行します。

KDSO3759-I

ユーザを認証しました。(Authentication Server Version=07-50)

(S)

処理を続行します。

KDSO3760-I

ユーザを認証しました。(Authentication Server Version is greater than 07-50)

(S)

処理を続行します。

KDSO3761-I

ユーザを認証しました。(Authentication Server Version cannot be acquired)

(S)

処理を続行します。

KDSO3762-I

ユーザを認証しました。(Authentication Server Version=08-10)

(S)

処理を続行します。

KDSO3763-E

ユーザ認証に失敗しました。ログイン権限がありません。(UserID=*詳細情報 1*,Virtual Hostname=*詳細情報 2*)

(S)

処理を中止します。

(O)

JP1/Base のログインユーザのログイン権限を確認してください。

KDSO3764-E

データベースのバージョンチェックの処理中に失敗しました。(Error Code=*詳細情報*)

(S)

処理を中止します。

(O)

- データベースマネージャでデータベースをアップグレードしてください。
- データベースが正常に動作しているかどうか HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- マネージャセットアップのデータベース情報の設定を確認してください。
- 監査ログ管理サーバの不要なアプリケーションを終了して，再度実行してください。
- 上記の対処を行っても回復しない場合は，システム管理者に連絡してください。

KDSO3802-I

JP1/Base のログアウトに成功しました。(UserID=*詳細情報*)

(S)

処理を終了します。

KDSO3804-E

JP1/Base のログアウトに失敗しました。(UserID=*詳細情報 1*,Error Code=*詳細情報 2*)

(S)

処理を続行します。

(O)

システム管理者に連絡してください。

KDSO3805-E

監査ログモジュールのロードに失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3806-E

監査ログの出力に失敗しました。(Reason=*詳細情報*)

(S)

処理を続行します。

(O)

システム管理者に連絡してください。

KDSO3807-E

内部エラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSO3851-I

監査ログファイルをラップアラウンドしました。(File Name=*詳細情報 1*,File Size=*詳細情報 2*)

(S)

処理を続行します。

KDSO3852-W

環境情報ファイルが存在しないか環境情報が不正です。デフォルトの環境情報を適用します。

(S)

処理を続行します。

(O)

環境情報ファイルを確認してください。

KDSO3853-E

ファイルの操作に失敗しました。(Reason=*詳細情報*)

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSP0001-I

サービス名 サービスを起動します。

*サービス名*サービスを起動します。

(S)

サービスを起動します。

KDSP0002-I

サービス名 サービスを停止します。

*サービス名*サービスを停止します。

(S)

サービスを停止します。

KDSP0008-I

サービス名 サービスを起動しました。

*サービス名*サービスを起動しました。

(S)

処理を続行します。

KDSP0009-E

サービス名 サービスの起動に失敗しました。

*サービス名*サービスの起動に失敗しました。

(S)

処理を終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSP0010-I

親プロセスからの停止要求を受信しました。プロセスを停止します。

親プロセスからの停止要求を受信しました。

(S)

子プロセスおよび自プロセスを停止します。

KDSP0011-I

プロセス(*プロセス名*)を起動します。(*保守情報 1*, *保守情報 2*)

プロセスを起動します。

(S)

処理を続行します。

KDSP0012-I

プロセス(*プロセス名*)を停止します。(*保守情報 1*, *保守情報 2*)

プロセスを停止します。

(S)

プロセスを停止します。

KDSP0016-I

プロセス(*子プロセス名*)の再起動に成功しました。

プロセスの再起動に成功しました。

(S)

処理を続行します。

KDSP0119-W

取得したサービス(*サービス名*)の通信待ち受け用ポート番号が OS が予約している番号(5000 以内)であるため，デフォルト値(*デフォルト値*)を使用して動作します。

取得したサービス（*サービス名*）の TCP/IP 通信のポート番号は，OS が予約している番号（5,000 以内）です。このため，デフォルト値（*デフォルト値*）を使用して処理を続行します。

(S)

*デフォルト値*を使用して処理を続行します。

(O)

services ファイルで*サービス名*に設定されているポート番号を確認してください。

KDSP0200-E

起動方法が不正なため，プロセス(*プロセス名*)を停止します。正しい手順で*サービス名* サービスを起動してください。

コマンドプロンプトから実行ファイルを起動するなど，誤った手順でプロセスの起動を試みています。

(S)

プロセスを停止します。

(O)

「5.7.1　監査ログ管理サーバを開始する」を参照し，正しい手順でサービスを起動してください。

KDSP0402-W

正規化ルールエディタからの通信待ち受け用ポート番号の取得に失敗しました。デフォルト値(*デフォルト値*)を使用して動作します。

services ファイルからのポート番号の読み込みに失敗しました。

(S)

処理を続行します。

(O)

services ファイルにサービス名「auditd_monsrv」に対するポート番号が設定されているか確認してください。

KDSP0404-E

正規化ルールエディタからの通信待ち受け用ポートのオープンに失敗しました。ポート番号(*ポート番号*)が既に使用されていない事を確認してください。

正規化ルールエディタからの通信待ち受け用ポートのオープンに失敗しました。

(S)

処理を終了します。

(O)

services ファイルで指定したポートが，すでにほかのプロセスで使用されていないか確認してください。ほかのプロセスで未使用のポートを services ファイルで指定したあと，JP1/NETM/Audit - Manager Define サービスを再起動してください。

KDSP0405-I

正規化ルールエディタとの接続を確立しました。(*保守情報*)

正規化ルールエディタとの接続を確立しました。

(S)

処理を続行します。

KDSP0406-I

正規化ルールエディタとの接続が終了しました。(*保守情報*)

正規化ルールエディタとの接続が終了しました。

(S)

処理を終了します。

KDSP0407-I

コマンドとの接続を確立しました。(*保守情報*)

コマンドとの接続を確立しました。

(S)

コマンドとの通信を開始します。

KDSP0408-I

コマンドとの接続が終了しました。(*保守情報*)

コマンドとの接続が終了しました。

(S)

コマンドとの通信を終了します。

KDSP0602-E

通信待ち受け用ポートのオープンに失敗しました。プロセス(*プロセス名*)を停止します。

通信待ち受け用ポートのオープンに失敗しました。

(S)

プロセスを停止します。

(O)

JP1/NETM/Audit - Manager Convert サービスおよび JP1/NETM/Audit - Manager Define サービスの状態を確認し，サービスが停止している場合は再起動してください。サービスを再起動しても回復しない場合は，システム管理者に連絡してください。

KDSP0603-I

通信待ち受け用ポート番号は *ポート番号* です。

通信待ち受け用ポートのオープンに成功しました。

(S)

処理を続行します。

KDSP0610-E

データベース接続情報の取得に失敗しました。(*保守情報 1*，*保守情報 2*)

データベースへ接続するための環境変数の取得に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0612-E

データベースへの接続のリトライが失敗しました。プロセス(*プロセス名*)を停止します。

データベースへの接続のリトライが失敗しました。

(S)

プロセスを停止します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- データベースが正常に動作していてこのメッセージが表示される場合は，システム管理者に連絡してください。

KDSP0614-E

データベースに対するアクセスで接続エラーが発生しました。データベースへの接続のリトライを実行します。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *データベースのエラーメッセージ*)

データベースに対するアクセスで接続エラーが発生しました。

(S)

処理を続行します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- データベースが正常に動作していてこのメッセージが表示される場合は，システム管理者に連絡してください。

KDSP0616-E

データベースに対するアクセスでエラーが発生しました。プロセス(*プロセス名*)を停止します。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *データベースのエラーメッセージ*)

データベースに対するアクセスで処理を続行できないエラーが発生しました。

(S)

プロセスを停止します。

(O)

- 保守情報 3 に出力されている数値が「-756」の場合は，データベースの再編成を行ってください。データベースの再編成については，「10.1.5　データベースの再編成」を参照してください。
- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- データベース再編成後，またはデータベースが正常に動作している場合にこのメッセージが表示されるときは，システム管理者に連絡してください。

KDSP0617-E

データベースに対するアクセスでエラーが発生しました。処理を終了します。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *データベースのエラーメッセージ*)

データベースに対するアクセスでエラーが発生しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSP0618-I

データベースへの接続のリトライに成功しました。

データベースへの接続のリトライに成功しました。

(S)

処理を続行します。

KDSP0628-E

データベース管理コマンドが実行中のため，プロセス(*プロセス名*)を停止します。

データベース管理コマンドが実行中です。

(S)

プロセスを停止します。

(O)

実行中のデータベース管理コマンドが終了してから，JP1/NETM/Audit - Manager Define サービスを再起動してください。

KDSP0702-W

通信待ち受け用ポート番号の取得に失敗しました。デフォルト値(*デフォルト値*)を使用して動作します。

services ファイルからのポート番号の読み込みに失敗しました。

(S)

*デフォルト値*を使用して処理を続行します。

(O)

services ファイルにサービス名「audita_admsrv」に対するポート番号が設定されているか確認してください。services ファイルの設定を確認する方法については「5.5.2　services ファイルを確認する」を参照してください。

KDSP0703-E

通信待ち受け用ポートのオープンに失敗しました。ポート番号(*ポート番号*)が既に使用されていない事を確認してください。

通信待ち受け用のポートのオープンに失敗しました。

(S)

プロセスを停止します。

(O)

services ファイルでサービス名「audita_admsrv」に対して指定しているポート番号が，ほかのプロセスですでに使用されていないか確認してください。services ファイルでサービス名「audita_admsrv」に対してほかのプロセスで未使用のポート番号を指定したあと，次のサービスを再起動してください。

- JP1/NETM/Audit - Manager
- JP1/NETM/Audit - Manager Convert
- JP1/NETM/Audit - Manager Define

services ファイルの設定を確認する方法については「5.5.2　services ファイルを確認する」を参照してください。

KDSP0711-E

正規化ルール定義の取得でエラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

正規化ルール定義の取得処理中にエラーが発生しました。

(S)

次のメッセージの正規化処理を行います。

(O)

システム管理者に連絡してください。

KDSP0715-I

正規化ルールが定義されていません。(*イベント ID*, *イベント DB 内通し番号*, *プロダクト名*)

正規化ルールが定義されていません。

(S)

次のメッセージの正規化処理を行います。

(O)

該当する監査ログメッセージの正規化を行う場合は，正規化ルールを定義してください。

KDSP0716-I

監査ログメッセージの正規化処理が完了しました。(*イベント ID*, *イベント DB 内通し番号*, *製品情報名*, *正規化ルール名*)

該当する監査ログのメッセージに対する正規化処理が完了しました。

(S)

処理を続行します。

KDSP0719-I

サポートしていないメッセージのため，正規化処理を行ないません。(*イベント ID*, *イベント DB 内通し番号*)

サポートしていないメッセージです。

(S)

次のメッセージの正規化処理を行います。

KDSP0721-W

正規化したメッセージ長が 1023byte を超えています。(*イベント ID*, *イベント DB 内通し番号*, *製品情報名*, *正規化ルール名*)

正規化したメッセージのメッセージ長が 1,023 バイトを超えています。

(S)

1,023 バイト以内に切り詰めて処理を続行します。

(O)

正規化ルールエディタの定義項目を見直してください。

KDSP0722-W

フィールドの形式が正しくないため，正規化処理に失敗しました。(*イベント ID*, *イベント DB 内通し番号*, *製品情報名*, *正規化ルール名*, *詳細コード*)

正規化ルールエディタで定義したフィールドの種別・形式と，収集した監査ログの種別・形式が異なっています。

(S)

次のメッセージの正規化処理を行います。

(O)

正規化ルールのメッセージ分割定義で，日付情報を定義したフォールドの種別および形式を確認してください。

KDSP0723-W

メッセージ分割の区切り情報定義が不正のため，正規化できません。(*イベント ID*, *イベント DB 内通し番号*, *製品情報名*, *正規化ルール名*)

正規化ルールのメッセージ分割で指定されている区切り情報定義（先頭区切または後区切）に誤りがあるため，定義どおりにメッセージを分割することができませんでした。

(S)

次のメッセージの正規化処理を行います。

(O)

正規化ルールのメッセージ分割定義のフィールド区切り情報（先頭区切および後区切）の定義内容を確認してください。

KDSP0725-E

正規化処理で論理矛盾が発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

正規化処理でエラーが発生しました。

(S)

正規化処理を中止します。

(O)

システム管理者に連絡してください。

KDSP0736-W

正規化ルールエディタで定義した項目に誤りがあるため，正規化できません。(*イベント ID, イベント DB 内通し番号*, *製品情報名*, *正規化ルール名*, *種別*, *詳細コード*)

フィールドの値が不正であったため，正規化処理に失敗しました。

(S)

次のメッセージの正規化処理を行います。

(O)

- 詳細コードに 21007 が出力された場合

正規化ルールエディタで定義したフィールド(種別:「共通情報」，形式:「監査事象の種別」)の指定を確認してください。

- 詳細コードに 21008 が出力された場合

  正規化ルールエディタで定義したフィールド(種別:「共通情報」，形式:「監査事象の結果」)の指定を確認してください。

KDSP0737-W

正規化ルールエディタでフィールド生成定義に指定した JP1 イベントの属性値が存在しないため，正規化できません。(*イベント ID*, *イベント DB 内通し番号*, *製品情報名*, *正規化ルール名*, *拡張属性名*)

処理中の JP1 イベントに正規化ルールで指定された JP1 イベント拡張属性が存在しなかったため，フィールドの生成に失敗しました。

(S)

次のメッセージの正規化処理を行います。

(O)

正規化ルールエディタでフィールド生成定義に指定した JP1 イベント属性値を確認してください。

KDSP0800-E

ソケット通信でエラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

ソケット通信でエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0801-E

データベース処理中に内部エラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

データベース処理中に内部エラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0802-E

プロセス(*プロセス名*)との通信のオープンに失敗しました。

親プロセスとの通信の確立に失敗しました。

(S)

プロセスを再起動します。

(O)

JP1/NETM/Audit - Manager Convert サービスおよび JP1/NETM/Audit - Manager Define サービスの状態を確認し，サービスが停止している場合は再起動してください。サービスを再起動しても回復しない場合は，システム管理者に連絡してください。

KDSP0803-E

プロセス(*プロセス名*)への起動完了通知の送信に失敗しました。

親プロセスへの起動完了通知の送信に失敗しました。

(S)

プロセスを再起動します。

(O)

JP1/NETM/Audit - Manager Convert サービスおよび JP1/NETM/Audit - Manager Define サービスの状態を確認し，サービスが停止している場合は再起動してください。サービスを再起動しても回復しない場合は，システム管理者に連絡してください。

KDSP0900-E

プロセス(*子プロセス名*)の再起動に失敗しました。*サービス名* サービスを停止します。

プロセス(*子プロセス名*)の再起動に失敗したため，*サービス名*サービスを停止します。

(S)

*サービス名*に表示されたサービスを停止します。

(O)

システム管理者に連絡してください。

KDSP0901-E

入出力エラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

通信のイベント待ちでエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0902-E

メモリ不足が発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

メモリ不足が発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0903-E

システムエラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

システムエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0904-E

予期しないエラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

処理中に予期しないエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0906-E

プロセス(*子プロセス名*)が起動できないため，*サービス名* サービスを停止します。

プロセス(*子プロセス名*)が起動できません。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0911-E

プロセス(*親プロセス名*)との通信の再接続に失敗しました。

親プロセスとの通信の再接続に失敗しました。

(S)

処理を中止します。

(O)

システム管理者に連絡してください。

KDSP0912-E

プロセス(*子プロセス名*)が処理続行不可能なエラーで終了しました。*サービス名* サービスを停止します。(*保守情報*)

プロセス（*子プロセス名*）が，処理を続行できないエラーで終了しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0913-E

プロセス(*子プロセス名*)が異常終了しました。プロセスを再起動します。(*保守情報*)

子プロセスの停止を検知しました。

(S)

プロセスを再起動します。

(O)

JP1/NETM/Audit - Manager Convert サービスおよび JP1/NETM/Audit - Manager Define サービスの状態を確認し，サービスが停止している場合は再起動してください。サービスを再起動しても回復しない場合は，システム管理者に連絡してください。

KDSP0915-E

プロセス(*子プロセス名*)の起動に失敗しました。*サービス名* サービスの起動を停止します。

サービスの起動処理中に，子プロセスの起動に失敗しました。

(S)

*サービス名*に表示されたサービスを停止します。

(O)

システム管理者に連絡してください。

KDSP0916-E

処理中に内部エラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

処理中に内部エラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP0997-E

ログの出力に失敗しました。:*プロセス名* [*詳細コード*] *ログファイル名*

ログの出力に失敗しました。

(S)

処理を継続します。ただし，次に示すユーザが取る処置を実施して，エラーが回復するまでログを出力しません。

(O)

- ログファイル名のファイルのアクセス権限を確認してください。
- 空きディスク容量が十分か，ファイルシステムで障害が発生していないかを確認してください。回復しない場合は，システム管理者に連絡してください。

KDSP2000-I

リリース処理を開始します。

リリース処理を開始します。

(S)

リリース処理を開始します。

KDSP2001-I

リリース処理が完了しました。(*終了コード*)

リリース処理を終了します。

(S)

リリース処理を終了します。

KDSP2002-E

リリース処理に失敗しました。(*終了コード*)

リリース処理に失敗しました。

(S)

リリース処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2003-I

内部コマンドの処理を開始します。(*コマンド名*)

内部コマンドの処理を開始します。

(S)

処理を続行します。

KDSP2004-I

内部コマンドの処理が完了しました。(*コマンド名*,*終了コード*)

内部コマンドの処理を終了します。

(S)

処理を終了します。

KDSP2005-E

内部コマンドの処理に失敗しました。(*終了コード*)

内部コマンドの処理に失敗しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2006-I

正規化ルール定義のインポートを開始します。

(S)

admrrimport コマンドを開始します。

KDSP2007-I

正規化ルール定義のインポートが完了しました。(*終了コード*)

(S)

admrrimport コマンドを終了します。

KDSP2008-E

正規化ルール定義のインポートに失敗しました。(*終了コード*)

(S)

admrrimport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSP2009-I

正規化ルール定義のエクスポートを開始します。

(S)

admrrexport コマンドを開始します。

KDSP2010-I

正規化ルール定義のエクスポートが完了しました。(*終了コード*)

(S)

admrrexport コマンドを終了します。

KDSP2011-E

正規化ルール定義のエクスポートに失敗しました。(*終了コード*)

(S)

admrrexport コマンドを終了します。

(O)

このメッセージの前に出力されているエラーメッセージを確認し，対処してください。

KDSP2100-E

内部コマンドの設定情報が不正です。(*コマンド名*, *保守情報*)

内部コマンドの設定情報が不正です。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2101-E

内部コマンドの処理を実行するためには管理者権限が必要です。

管理者権限のないユーザによって処理が実行されました。

(S)

処理を終了します。

(O)

管理者権限を持つユーザで，再実行してください。

KDSP2102-E

コマンド(*コマンド名*)はすでに実行中です。コマンドの多重起動はできません。

(S)

コマンドを終了します。

(O)

再度コマンドを実行する必要がある場合は，実行中のコマンドが終了してから，再実行してください。

KDSP2103-E

コマンド(*コマンド名*)が実行中のため，コマンド(*コマンド名*)が実行できません。

(S)

コマンドを終了します。

(O)

実行中のコマンドが終了してから，再実行してください。

KDSP2104-E

JP1/NETM/Audit - Manager Define サービスが起動していないため，処理が実行できません。JP1/NETM/Audit - Manager Define サービスを起動してください。

JP1/NETM/Audit - Manager Define サービスが起動していないため，処理が実行できません。

(S)

処理を終了します。

(O)

JP1/NETM/Audit - Manager Define サービスを起動したあと，正規化ルールエディタを再起動し，再実行してください。

KDSP2105-E

JP1/NETM/Audit - Manager Define サービスとの通信が切断されました。処理を終了します。

JP1/NETM/Audit - Manager Define サービスとの通信が予期しないタイミングで切断されました。

(S)

処理を終了します。

(O)

JP1/NETM/Audit - Manager Define サービスを起動したあと，正規化ルールエディタを再起動し，再実行してください。

KDSP2106-E

JP1/NETM/Audit - Manager Define サービスへの要求で応答待ちがタイムアウトしました。(*保守情報 1*，*保守情報 2*)

JP1/NETM/Audit - Manager Define サービスへの要求の応答待ちがタイムアウトしました。

(S)

処理を終了します。

(O)

JP1/NETM/Audit - Manager Define サービスの状態を確認したあと，正規化ルールエディタを再起動し，再実行してください。

KDSP2107-E

JP1/NETM/Audit - Manager Define サービスへの要求に対してエラー応答が返りました。(*保守情報 1*, *保守情報 2*, *保守情報 3*)

(S)

コマンドを終了します。

(O)

正規化定義サービスログファイルを確認して，エラーの原因を取り除いてから，コマンドを再実行してください。

KDSP2108-E

Windows API(*Windows API 名*)でエラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*)

処理中に，Windows API でエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2110-E

処理中に内部エラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

処理中に内部エラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2120-E

コマンドのオプションが誤っています。

(S)

コマンドを終了します。

(O)

正しい引数を指定してコマンドを再実行してください。

KDSP2202-I

定義情報(*定義名*)のリリース処理を開始します。

*定義名*のリリース処理を開始します。

(S)

処理を続行します。

KDSP2203-I

定義情報(*定義名*)のリリース処理を終了しました。

*定義名*のリリース処理を終了しました。

(S)

処理を終了します。

KDSP2210-E

定義情報(*定義名*)が見つかりません。

定義情報が見つかりません。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2211-E

定義情報(*定義名*)が不正です。

定義情報が不正です。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2500-E

データベースへの接続に失敗しました。

データベースへのコネクトに失敗しました。

(S)

処理を終了します。

(O)

- データベースが正常に動作しているか，HiRDB/EmbeddedEdition _AL1 サービスの状態を確認してください。
- データベースが正常に動作していてこのメッセージが表示される場合は，システム管理者に連絡してください。

KDSP2501-E

処理中にデータベースでエラーが発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*)

データベースに対するアクセス（レコードの検索，更新，削除，追加）でエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2502-E

処理中に内部エラーが発生しました。(*保守情報 1*, *保守情報 2*)

処理中に内部エラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2600-E

正規化ルール定義エクスポートファイルのオープンに失敗しました。
ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

- 正規化ルール定義エクスポートファイルが指定したパスに存在するか確認してください。
- 正規化ルール定義エクスポートファイルのアクセス権を確認してください。

KDSP2601-E

正規化ルール定義エクスポートファイルの解析に失敗しました。
ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

正規化ルール定義エクスポートファイルが admrrexport コマンドを使用して出力されたファイルかどうか確認してください。

KDSP2602-E

正規化ルール定義エクスポートファイルの読み込みに失敗しました。
ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

正規化ルール定義エクスポートファイルのアクセス権を確認してください。

KDSP2603-E

正規化ルール定義エクスポートファイルへの書き込みに失敗しました。
ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

- 正規化ルール定義エクスポートファイルのアクセス権を確認してください。
- 出力ファイルの格納先フォルダに十分な空き容量があるか確認してください。

KDSP2604-E

正規化ルール定義エクスポートファイルがすでに存在しています。
ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

- 正規化ルール定義エクスポートファイルに上書きする場合は，-u オプションを指定して，コマンドを再実行してください。
- 正規化ルール定義エクスポートファイルを上書きしない場合は，-o オプションで指定する正規化ルール定義エクスポートファイル名を変更してから，コマンドを再実行してください。

KDSP2605-E

正規化ルールエディタが実行中のため，コマンドを実行できません。
コマンド名=[*コマンド名*]

(S)

コマンドを終了します。

(O)

正規化ルールエディタを終了してから，コマンドを再実行してください。

KDSP2606-E

指定した正規化ルール定義エクスポートファイルは上位バージョンでエクスポートされたものであるため，インポートできません。ファイル名=[*ファイル名*]
バージョン=[*バージョン*]

(S)

コマンドを終了します。

(O)

指定した正規化ルール定義エクスポートファイルを出力した JP1/Audit Management - Manager と同じバージョンにバージョンアップしたあと，コマンドを再実行してください。

KDSP2607-E

指定したファイル名はローカルディスク上のファイルではありません。
ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

ローカルディスク上のファイル名を指定してから，コマンドを再実行してください。

KDSP2608-E

リリース処理が実行中のため，コマンドを実行できません。コマンド名=[*コマンド名*]

(S)

コマンドを終了します。

(O)

ログファイル（正規化定義データベースリリースログファイル）にリリース処理の完了または失敗を示すメッセージが出力されたあと，コマンドを再実行してください。

リリース処理の実行時間はリリース，リリース解除を行う正規化ルール定義の件数に依存します。大量の正規化ルール定義を同時にリリースすると数十分掛かることがあります。

KDSP2609-E

指定した製品情報数が不正です。

(S)

コマンドを終了します。

(O)

100 件以下の製品情報名を指定し，コマンドを再実行してください。

KDSP2610-W

同じ定義が存在するため，定義をインポートできません。定義の種別=[*定義の種別*] 定義名=[*定義名*] 識別情報=[*識別情報*]

(S)

次の定義のインポート処理を続行します。

(O)

インポートを行わなかった定義をインポートする場合は，次の手順で実施してください。

定義の種別が「製品情報」の場合

1. 正規化ルールエディタでメッセージ中に表示されている定義名（*製品情報名*）または識別情報（*JP1 イベント種別/プロダクト名*）が同じ定義を削除する。
2. admrrimport コマンドを再実行する。

定義の種別が「正規化ルール」で，定義名に表示されている製品情報の JP1 イベント種別が「イベントログトラップ」の場合

1. 正規化ルールエディタでメッセージ中に表示されている定義名（*製品情報名*¥*正規化ルール名*）または，製品情報名と識別情報（Windows イベント ID）が同じ定義を削除する。
2. admrrimport コマンドを再実行する。

定義の種別が「正規化ルール」で，定義名に表示されている製品情報の JP1 イベント種別が「ログファイルトラップ」の場合

1. 正規化ルールエディタでメッセージ中に表示されている定義名（*製品情報名*¥*正規化ルール名*）が同じ定義を削除する。

2. admrrimport コマンドを再実行する。

KDSP2611-W

追加も更新も行えないため，定義をインポートできません。定義の種別=[*定義の種別*] 定義名=[*定義名*] 識別情報=[*識別情報*]

(S)

次の定義のインポート処理を続行します。

(O)

インポートを行わなかった定義をインポートする場合は，次の手順で実施してください。

定義の種別が「製品情報」の場合

1. 正規化ルールエディタでメッセージ中に表示されている定義名（*製品情報名*）または識別情報（*JP1 イベント種別/プロダクト名*）が同じ定義を削除する。
2. admrrimport コマンドを再実行する。

定義の種別が「正規化ルール」の場合

1. 正規化ルールエディタでメッセージ中に表示されている定義名（*製品情報名*¥*正規化ルール名*）または製品情報名と識別情報（Windows イベント ID）が同じ定義を削除する。
2. admrrimport コマンドを再実行する。

KDSP2612-W

定義が更新できない状態であるため，インポートできません。
定義の種別=[*定義の種別*] 定義名=[*定義名*]

(S)

次の定義のインポート処理を続行します。

(O)

インポートを行わなかった定義をインポートする場合は，次の手順で実施してください。

1. 正規化ルールエディタでリリースを実行し，リリース許可状態およびリリース解除許可状態の定義がない状態にする。
2. admrrimport コマンドを再実行する。

KDSP2613-W

定義数が最大件数に達しているため，インポートできません。
定義の種別=[*定義の種別*] 定義名=[*定義名*]

(S)

次の定義のインポート処理を続行します。

(O)

インポートを行わなかった定義をインポートする場合は，次の手順で実施してください。

1. 正規化ルールエディタで不要な製品情報定義を削除する。
2. admrrimport コマンドを再実行する。

KDSP2614-W

指定された製品情報定義が存在しないため，エクスポートできません。
製品情報名＝[*製品情報名*]

(S)

指定された次の製品情報定義のエクスポート処理を続行します。

(O)

指定した製品情報名を確認してください。

KDSP2615-W

指定された製品情報はすでにエクスポートされています。製品情報名＝[*製品情報名*]

(S)

指定された次の製品情報定義のエクスポート処理を続行します。

(O)

指定した製品情報名を確認してください。

KDSP2620-I

定義を追加しました。定義の種別＝[*定義の種別*] 定義名＝[*定義名*]

(S)

処理を続行します。

KDSP2621-I

定義を更新しました。定義の種別＝[*定義の種別*] 定義名＝[*定義名*]

(S)

処理を続行します。

KDSP2622-I

定義をエクスポートしました。定義の種別＝[*定義の種別*] 定義名＝[*定義名*]

(S)

処理を続行します。

KDSP2623-I

エクスポートする定義情報が存在しませんでした。

(S)

コマンドを終了します。

KDSP2630-E

指定した正規化ルール定義エクスポートファイルのパスが長すぎます。

(S)

コマンドを終了します。

(O)

指定するパスを変更し，コマンドを再実行してください。

KDSP2631-E

指定したファイル名がフルパス名称ではありません。ファイル名=[*ファイル名*]

(S)

コマンドを終了します。

(O)

ファイル名を確認したあと，正しい形式のフルパス名を指定してください。

KDSP2800-I

標準サポートの正規化ルール定義を追加しました。製品情報名=[*製品情報名*]
正規化ルール名=[*正規化ルール名*]

(S)

次の正規化ルール定義のアップグレード処理を続行します。

KDSP2801-I

標準サポートの正規化ルール定義を更新しました。製品情報名=[*製品情報名*]
正規化ルール名=[*正規化ルール名]*

(S)

次の正規化ルール定義のアップグレード処理を続行します。

KDSP2810-W

標準サポート製品の正規化ルール定義が変更または削除されているため，アップグレード処理に失敗しました。アップグレード処理内容=［*製品情報名*，*正規化ルール名*，*アップグレード処理内容*］

(S)

次の正規化ルール定義のアップグレード処理を続行します。

(O)

アップグレード処理内容に出力されている正規化ルールを正規化ルールエディタで確認し，必要に応じて次のように対処してください。

- アップグレード処理内容に出力されている正規化ルールをアップグレードする必要がない場合，対処は不要です。
- アップグレード処理内容に出力されている正規化ルールをアップグレードする場合，正規化ルールエディタを用いて，メッセージ中に表示されている製品情報を削除し，［標準サポート製品情報追加］ダイアログで標準提供定義を再作成して，リリースしてください。

KDSP2820-W

新たな標準サポート製品の正規化ルール定義を追加することができません。製品情報名=[*製品情報名*] 正規化ルール名=[*正規化ルール名*]

新たに追加する標準サポート製品と同じ製品情報名または製品情報識別子を持つ製品情報がすでに存在するため，標準サポート製品の正規化ルール定義を追加することができませんでした。

(S)

次の正規化ルール定義のアップグレード処理を続行します。

(O)

標準提供定義を使用せず，すでに定義されている製品情報や正規化ルールを使用する場合は，対処する必要はありません。

製品情報名および正規化ルール名に出力されている標準提供定義の追加を行う場合は以下の手順で行ってください。

1. 正規化ルールエディタで，製品情報名および正規化ルール名に出力されている文字列と同じ名前の定義の名称を変更する，または削除する。
2. 正規化ルールエディタの[標準提供製品情報定義]ダイアログを使用し，追加できなかった定義をテンプレート定義から作成する。

KDSP2830-W

製品情報または正規化ルールの定義件数が上限値に達しているため，新たな標準サポート製品の正規化ルール定義を追加することができません。

製品情報名=[*製品情報名*] 正規化ルール名=[*正規化ルール名*]

(S)

次の正規化ルール定義のアップグレード処理を続行します。

(O)

製品情報名および正規化ルール名に出力されている定義の追加を行う場合は，次の手順で実施してください。

1. 正規化ルールエディタで不要な製品情報定義を削除する。
2. 正規化ルールエディタの［標準サポート製品情報追加］ダイアログを使用し，追加できなかった定義をテンプレート定義から作成する。

KDSP2900-E

メモリ不足が発生しました。(*保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

メモリ不足が発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2901-E

ファイルの入出力中にエラーが発生しました。(*関数名*, *エラーコード*, *保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

ファイルの入出力中にエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2902-E

通信中にエラーが発生しました。(*関数名*, *エラーコード*, *保守情報 1*, *保守情報 2*, *保守情報 3*, *保守情報 4*)

通信処理中にエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

KDSP2903-E

システムエラーが発生しました。(関数名, エラーコード, 保守情報 1, 保守情報 2, 保守情報 3, 保守情報 4)

システムエラーが発生しました。

(S)

処理を終了します。

(O)

システム管理者に連絡してください。

15 トラブルシューティング

この章では，JP1/Audit Management - Manager を使用した監査証跡管理システムの運用中にトラブルが発生した場合の対処方法について説明します。

15.1　トラブル発生時の対処手順

JP1/Audit Management - Manager を使用した監査証跡管理システムでトラブルが発生した場合は，次の手順で対処してください。

1. エラーメッセージを確認する。

   監査ログ管理画面を操作しているときのエラー

   画面に表示されたエラーメッセージを確認してください。

   コマンド入力中または入力後のエラー

   標準出力，標準エラー出力，および JP1/Audit Management - Manager のログファイルでメッセージを確認してください。

   正規化ルールエディタ操作中のエラー

   正規化ルールエディタのログファイルでメッセージを確認してください。

   そのほかのエラー

   JP1/Audit Management - Manager のログファイルにエラーメッセージが出力されていないか確認してください。

   JP1/Audit Management - Manager が出力するメッセージの見方，要因，および対処方法については「14.　メッセージ」を参照してください。正規化ルールエディタが出力するメッセージの見方，要因，および対処方法については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。また，ログファイルの出力先については「付録 A　ファイル一覧」を参照してください。

2. トラブルの要因および対処方法を確認して，対処する。

   - 標準出力，標準エラー出力，および JP1/Audit Management - Manager のログファイルに出力されたメッセージの見方，要因，および対処方法については「14.　メッセージ」を参照してください。
   - 正規化ルールエディタのログファイルに出力されたメッセージの見方，要因，および対処方法については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。
   - 監査証跡管理システムの操作で想定されるトラブルと，その対処方法については「15.3　トラブルへの対処方法」を参照してください。

3. トラブルが解消されない場合や内部エラーなどの場合は，必要な資料を採取して対処する。

   資料の採取方法については「15.2　トラブル発生時に採取が必要な資料」を参照してください。

また，JP1/Audit Management - Manager のデータベースや環境定義をバックアップしておくことで，トラブルが発生した場合に，JP1/Audit Management - Manager の環境をリストアできます。JP1/Audit Management - Manager 環境のバックアップとリストアの手順については「15.4　監査ログ管理サーバのバックアップおよびリストア」を参照してください。

15.2　トラブル発生時に採取が必要な資料

JP1/Audit Management - Manager を使用した監査証跡管理システムで通信エラーなどが発生した場合や，対処してもトラブルが解消されない場合は，次の資料を採取して管理者に連絡し，弊社にお問い合わせください。

15.2.1　トラブル発生時に一括採取する資料

Administrator 権限を持つユーザで admlog.vbs コマンドを実行して，トラブル発生時の資料を一括採取します。採取した資料は，次のフォルダ配下に格納されます。

JP1/Audit Management - Manager のインストール先フォルダ¥troubleshoot**¥YYYY-MM-DD_hh-mm-ss**

YYYY-MM-DD_hh-mm-ss：YYYY=年，MM=月，DD=日，hh=時，mm=分，ss=秒

資料の格納先を変更する場合は，admlog.vbs コマンドの引数で格納フォルダを指定します。

admlog.vbs コマンドについては「12.　コマンド」の「admlog.vbs（障害発生時の保守資料採取）」を参照してください。

15.2.2　トラブル発生時に個別採取する資料

admlog.vbs コマンドで一括して取得できる資料に加えて，次の表に示す資料を取得してください。

表 15–1　監査証跡管理システムのトラブル発生時に取得する資料（個別取得）

項番	対象サーバ	資料内容	格納場所
1	監査ログ管理サーバ	IIS ログ情報	次に示すフォルダ配下のすべてのファイルです。 • **IIS マネージャで設定したログファイルフォルダ** 格納場所のデフォルト値： システムドライブ¥inetpub¥logs¥LogFiles
2		IIS 設定情報	次に示すファイルまたはフォルダ配下のすべてのファイルです。 各取得ファイルの格納場所のデフォルト値 • **システム環境変数 windir の設定値¥**system32¥inetsrv¥config • システムドライブ¥inetpub¥history • システムドライブ¥inetpub¥temp¥appPools
3		正規化ルール定義情報	admrrexport コマンドを実行して，すべての製品情報をバックアップした正規化ルール定義エクスポートファイルをコピーしてください。格納場所は admrrexport コマンドの-o オプションに指定したパスです。
4	監査ログ収集対象サーバ	ログ	次に示すファイルをコピーしてください。

項番	対象サーバ	資料内容	格納場所
			Windows の場合 • JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき **任意のインストール先フォルダ**¥log¥*.log • JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき **システムドライブ**¥Program Files¥Hitachi¥jp1netmaudit¥manager¥log¥*.log UNIX の場合 • JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき /var/opt/jp1netmaudit/agent/log/*.log • JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき /opt/jp1netmaudit/manager/log/*.log
5		設定情報	次に示すファイルをコピーしてください。 Windows の場合 • JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき **任意のインストール先フォルダ**¥conf¥* • JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき **システムドライブ**¥Program Files¥Hitachi¥jp1netmaudit¥manager¥conf¥* UNIX の場合 • JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき /etc/opt/jp1netmaudit/agent/conf/* • JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき /opt/jp1netmaudit/manager/conf/*
6		監査ログ専用イベントデータベースの設定情報	次に示すファイルをコピーしてください。 • **監査ログ専用フォルダ（監査ログ専用ディレクトリ）**¥jp1netmaudit¥event¥conf • **監査ログ専用フォルダ（監査ログ専用ディレクトリ）**¥jp1netmaudit¥event¥forward

15.2.3 そのほかに採取する資料

一括採取および個別採取する資料のほかに，JP1/Base の情報も採取が必要です。JP1/Base の情報については，マニュアル「JP1/Base 運用ガイド」を参照してください。

15.3　トラブルへの対処方法

この節では，監査証跡管理システムの操作で想定されるトラブルと，その対処方法を示します。

15.3.1　監査ログ管理画面でのトラブル

監査ログ管理画面で想定されるトラブルの対処方法を示します。

なお，構築時または運用時にユーザが設定する内容については，括弧内に参照先を示しています。参考にしてください。

(1)　ログイン画面が表示されない

- 次に示すサービスが開始されていないことがあります。このサービスが開始されているかどうかを確認してください。
  - World Wide Web Publishing Service
- Microsoft Internet Information Services をインストールしたあと，JP1/Base および JP1/Audit Management - Manager をインストールする前にマシン名を変更していることがあります。インターネットゲストアカウントのパスワードを再設定してください。(参照先：5.2.4)

  なお，JP1/Base 認証サーバが同じマシン上にある場合は，JP1/Base 認証サーバのホスト名も適切に変更してください。
- Microsoft Internet Information Services の「既定の Web サイト※」の TCP ポート番号を確認してください。TCP ポート番号が「80」以外の場合には，次の URL でアクセスしてください。

  http://**ホスト名:TCP ポート番号**/jp1netmaudit/

  注※

  「既定の Web サイト」は，Microsoft Internet Information Services のバージョンによって「Default Web Site」と表示されることがあります。

(2)　ログイン画面は表示されるがログインできない

- Internet Explorer で，必要な設定が無効になっていることがあります。インターネットオプションの「セキュリティ」タブで，［レベルのカスタマイズ］ボタンをクリックすると表示される［セキュリティの設定］ダイアログで次の項目を有効にしてください。(参照先：5.11)
  - 「アクティブスクリプト」
  - 「暗号化されていないフォームデータの送信」
- ログインに使用した JP1 ユーザが正しく登録されていないことがあります。JP1/Base でユーザ名，パスワード，および権限を確認してください。(参照先：5.5.3)
- 次に示すサービスが開始されていないことがあります。このサービスが開始されているかどうかを確認してください。

- JP1/Base

- JP1/Audit Management - Manager をバージョンアップしたあとに，監査ログ管理データベースをアップグレードしていないことがあります。データベースをアップグレードしているかどうか確認してください。未実施の場合は，データベースをアップグレードしてください。

(3) 画面が正しく表示されない

- 接続先サーバ（監査ログ管理サーバまたは監査ログ閲覧サーバ）で，必要な設定が正しく行われていないことがあります。[マネージャセットアップ] ダイアログで，次の項目が正しく設定されているか確認してください。(参照先：5.5.7)
  - データベース情報
  - クラスタ情報
- データベースが起動していないことがあります。次に示すデータベースのサービスが開始されているか確認してください。
  - HiRDB/EmbeddedEdition _AL1（または HiRDB/ClusterService _AL1）
- データベースの接続パスワードが正しく指定されていないことがあります。データベースの接続パスワードを確認してください。(参照先：5.5.6)
- ファイルのサイズがデータベースの最大容量を超えていることがあります。データベースのメンテナンスを実行してください。(参照先：10.1.2)
- 監査ログの検索中に，「ページが表示できません」と表示された場合，Internet Explorer のタイムアウト値を超えていることがあります。タイムアウト値を再設定してください。
- 監査ログレポート画面のレポートが途中までしか表示されない場合，最大レポート件数を超えていることがあります。検索条件を再設定してください。

(4) ファイルをダウンロードできない

- Internet Explorer の設定で，必要な設定が無効になっていることがあります。インターネットオプションの「セキュリティ」タブで，[レベルのカスタマイズ] ボタンをクリックすると表示される [セキュリティの設定] ダイアログで次の項目を有効にしてください。(参照先：5.11)
  - 「ファイルのダウンロード」
  - 「ファイルのダウンロード時に自動的にダイアログを表示する」
- バックアップファイルの格納先フォルダにリンクする仮想ディレクトリが正しく設定されていないことがあります。IIS マネージャで，仮想ディレクトリ名および設定されているフォルダパスを確認してください。(参照先：5.5.1)
- 指定したファイルが，監査ログ管理画面からファイルをダウンロードするときの最大サイズを超えていることがあります。接続先サーバ（監査ログ管理サーバまたは監査ログ閲覧サーバ）で，監査ログ管理画面の最大ダウンロードファイルサイズを適切に設定してください。(参照先：5.5.1)

(5) ダウンロード対象に指定した，監査ログのバックアップファイルが見つからない

監査ログのバックアップファイルを移動する際に，admcsvmove コマンドを使用していない場合があります。手動で移動したファイルをバックアップ先のフォルダに戻してください。監査ログのバックアップファイルをバックアップ先のフォルダ以外の場所に移動するには，admcsvmove コマンドを使用してください。(参照先：8.4)

15.3.2 データベースのトラブル

データベースの運用で想定されるトラブルの対処方法を示します。対処の手順については，括弧内に示す個所を参照してください。

(1) データベースの容量が不足していることを示すメッセージが出力される

Windows のイベントログ（アプリケーション）に，「HiRDBEmbeddedEdition_AL1」に関する次のメッセージが出力された場合は，データベースの再編成を実施してください。(参照先：10.1.5)

- KFPH00211-I
- KFPH00212-I

データベースを再編成してもこのメッセージが出力される場合は，さらに次のどれかを実施してください。

- データベース内の不要な監査ログを削除する。(参照先：10.1.10)
- データベースのサイズを変更する。(参照先：10.1.2)
- 監査ログ閲覧サーバの利用範囲を広げる。(参照先：8.2 および 8.3)
  データベースのサイズを大きくできない場合に実施してください。
  適当な範囲の監査ログのデータをバックアップして削除し，監査ログ閲覧サーバにインポートします。

(2) データベースのアップグレードができない

アップグレード中の処理状況によって対処方法が異なります。次に示す処理状況ごとに対処方法を説明します。

- データベースのアップグレードができない。
- データベースの CSV バックアップができない。
- データベースの CSV リストアができない。

(a)　データベースのアップグレード中にエラーが発生した場合

データベースのアップグレードに失敗した場合，アップグレードする前のバージョンを復元したあとで，再度，新しいバージョンの JP1/Audit Management - Manager のインストールとデータベースのアップグレードを実行してください。

アップグレードする前のバージョンを復元する作業手順を次に示します。

1. 新しいバージョンの JP1/Audit Management - Manager をアンインストールする。(参照先：5.2.6)
2. アップグレードする前のバージョンの JP1/Audit Management - Manager をインストールする。(参照先：5.2.5)
3. 新しいバージョンの JP1/Audit Management - Manager を上書きインストールしたときに取得しているバックアップを使用して，設定情報およびデータベースを復元する。(参照先：10.1.4)

(b)　データベースの CSV バックアップ中にエラーが発生した場合

データベースの CSV バックアップに失敗した場合，出力されたメッセージに従い対処したあと，再度データベースの CSV バックアップを実行してください。(参照先：10.1.7)

(c)　データベースの CSV リストア中にエラーが発生した場合

データベースの CSV リストアに失敗した場合は，出力されたメッセージに従い対処したあと，再度 CSV リストアを実行してください。[データベースの CSV リストア設定] 画面の「バックアップフォルダ名」には，データベースの CSV バックアップで指定したバックアップ取得先フォルダ名を指定してください。(参照先：10.1.7)

15.3.3　監査ログの監視および収集のトラブル

監査ログの監視および収集で想定されるトラブルの対処方法を示します。

(1)　収集対象の監視が開始できない

アダプタコマンドのバージョンが古いことがあります。監査ログ収集対象サーバに必要なファイルをインストールし直して，アダプタコマンドを最新のものにバージョンアップしてください。監査ログ収集対象サーバに必要なファイルをインストールする方法については「5.4.1　セットアップに必要なファイルをインストールする」を参照してください。

(2)　UNIX システムログの変換コマンドでログ情報を正しく変換できない

JP1/Audit Management - Manager が収集対象としている OS のファイルが壊れているおそれがあります。OS のファイルが壊れていると，UNIX システムログの変換コマンドでログ情報を正しく変換できません。また，UNIX システムログの変換コマンドがエラーで終了します。ファイルが壊れて正しくログが変換できない場合は，該当するファイルを再作成してください。

(3)　定時収集時に KDSO1504-E が出力される

定時収集時にメッセージ「KDSO1504-E」が出力される場合には，次に示す内容を確認してください。

- JP1/NETM/Audit - Manager Convert サービスの起動前または起動中に，監査ログの定時収集が実施された可能性があります。JP1/NETM/Audit - Manager Convert サービスが起動しているか確認してください。

  すぐに監査ログを収集したい場合は，JP1/NETM/Audit - Manager Convert サービスを起動し，［監査ログ収集マネージャ］ウィンドウから即時収集を実行してください。

- 監査ログ収集対象サーバに接続できていない可能性があります。

  監査ログ管理サーバおよび監査ログ収集対象サーバで次の内容を確認してください。

  監査ログ管理サーバ

  1. JP1/Base の API 設定ファイルの内容を確認してください。
  2. JP1/Base の設定を変更した場合は，JP1/Base Event サービスを再起動してください。

  監査ログ収集対象サーバ

  1. JP1/Base の設定内容を確認してください。
  2. 「JP1/Base Event **監査ログ専用イベントサーバ名**」のイベントサービスが起動しているか確認してください。

(4)　共有ディスク上に出力される監査ログの監視が開始できない

共有ディスク上に出力される監査ログの監視が開始できない場合には，次に示す内容を確認してください。

- 共有ディスク上の監査ログを監視する場合，あらかじめ監査ログ収集対象サーバ側で論理ホストの環境を作成しておく必要があります。監査ログ収集対象サーバ側の論理ホストの設定に誤りがないか見直してください。論理ホストのセットアップ手順については「6.5　監査ログ収集対象サーバのセットアップ（クラスタ環境）」を参照してください。
- 監査ログ収集マネージャで［収集対象の設定］ダイアログのログフォルダに指定した共有ディスク上のディレクトリに対して正常にアクセスできるか，収集対象となるクラスタ環境のアクティブ状態のホストで確認してください。

(5)　監査ログ収集マネージャで最終収集日時が「-」のまま更新されない

監査ログ収集マネージャで収集対象の追加後に，JP1/Audit Management - Manager のサービスを再起動していない可能性があります。

JP1/Audit Management - Manager のサービスを再起動したあと，再度収集を実行してください。

15.3.4　監査ログの正規化でのトラブル

正規化エラーによって監査ログ管理データベースに格納されなかったログが，正規化処理エラーファイルに出力されます。このため，監査ログ収集対象サーバを監視する際は，監査ログ管理画面に加えて，正規化処理エラーファイルの内容も確認してください。

期待した監査ログが監査ログ管理データベースに格納されていない場合の原因としては次のことが考えられます。

- 正規化ルールファイルや正規化ルールエディタの定義に誤りがある。
- 収集対象とするプログラムのログが，JP1/Audit Management - Manager で正規化できるログの条件に当てはまらない。

ログファイルに KDSO0004-E～KDSO0016-E のエラーメッセージが出力されるため，これらのメッセージに従って対処してください。また，メッセージに出力された情報を基に，正規化処理エラーファイル内から該当するログを参照してください。

また，JP1/Audit Management - Manager で標準サポート外となっているプログラムの場合は，正規化ルールファイルまたは正規化ルールエディタの定義を確認してください。正規化ルールファイルについては「13.2　正規化ルールファイル」を参照してください。正規化ルールエディタの定義については，マニュアル「JP1/Audit Management - Manager 正規化ルール定義ガイド」を参照してください。

注意事項

正規化処理エラーファイルからは，監査ログをデータベースへ格納できません。必要に応じてファイルをバックアップまたは削除してください。

正規化処理エラーファイルの格納先およびファイルの出力内容を，次に示します。

(1)　ファイル名および格納先

正規化処理エラーファイルの格納先フォルダとファイル名を次に示します。

- 格納先フォルダ

  JP1/Audit Management - Manager のインストール先フォルダ¥spool¥
- ファイル名

  admrglerrordatYYYYMMDD.csv

  YYYY が年，MM が月，DD が日を示しています。

(2)　出力形式と出力パラメーター

正規化処理エラーファイルの出力形式およびパラメーターを，次に示します。

- 出力形式

  イベント ID，イベントサーバ名，製品名，監査ログ↓

イベント ID，イベントサーバ名，製品名，監査ログ↓
：

- パラメーター

表 15-2　正規化処理エラーファイルのパラメーター

項番	パラメーター	説明
1	イベント ID	JP1 イベント ID です。
2	イベントサーバ名	取得対象のイベントサーバ名です。
3	製品名	取得対象の製品名称です。
4	監査ログ	文字コードをシフト JIS に変換した監査ログです。

- 出力例

```
120637,Host1,JP1_NETM_Audit-Manager,
”20070227205936.859 2256(2260) KDSO2001-I 環境設定に成功しました。”
：
```

15.3.5　インストールでのトラブル

インストールで想定されるトラブルの対処方法を示します。

(1)　COM DLL の登録または解除に失敗する

インストール時に「COM DLL 登録解除コマンドが失敗しました。」のメッセージダイアログが表示される場合，メッセージダイアログに表示されている内容を確認し，次の手順を実施してください。

なお，ASP および IIS6 管理互換がインストールされていない場合は，インストールしたあとに，JP1/Audit Management - Manager を再度インストールしてください。

1. JP1/Audit Management - Manager のインストール完了後に OS を再起動し，管理者権限を持つユーザでログインする。
2. コマンドプロンプトを起動する。
3. 「JP1/Audit Management - Manager の仮想ディレクトリ¥bin」に移動する。
4. 次に示すコマンドを実行する。

```
regsvr32 登録に失敗したDLLファイル名
```

「登録に失敗した DLL ファイル名」には，メッセージダイアログの［DLL 名称］に表示されている DLL ファイル名を指定してください。

15.4　監査ログ管理サーバのバックアップおよびリストア

データベースと定義ファイルのバックアップを取得しておくことで，トラブルが発生したときに，監査ログ管理サーバの環境を復元できます。

この節では，JP1/Audit Management - Manager のデータベースと環境定義のバックアップおよびリストアの方法について説明します。

15.4.1　JP1/Audit Management - Manager のバックアップ

JP1/Audit Management - Manager のデータベースと定義ファイルのバックアップについて説明します。

(1)　データベースのバックアップ

［データベースマネージャ］ダイアログまたはコマンドを使用して，データベースのバックアップを取得してください。手順の詳細については「10.1.3　データベースのバックアップ」を参照してください。

(2)　環境定義のバックアップ

次に示すフォルダ配下のファイルをすべてコピーしてください。

クラスタ環境で運用していない場合

- JP1/Audit Management - Manager のインストール先フォルダ¥conf
- JP1/Audit Management - Manager の仮想ディレクトリ¥conf

クラスタ環境で運用している場合

- 共有ディスク¥conf
- JP1/Audit Management - Manager の仮想ディレクトリ¥conf

なお，これらのファイルはシステムで自動的に記述されるものです。編集はしないでください。

15.4.2　JP1/Audit Management - Manager のリストア

ここでは，バックアップデータを使用した JP1/Audit Management - Manager のリストアについて説明します。

バックアップしたデータを利用することで，監査ログ管理サーバの構築手順のうち，JP1/Audit Management - Manager のセットアップの手順を省略できます。

(1)　リストアの準備

JP1/Audit Management - Manager を上書きインストールしてください。JP1/Audit Management - Manager の上書きインストールについては「5.2.5　JP1/Audit Management - Manager を上書きインストールする」を参照してください。

(2)　環境定義のリストア

バックアップした環境定義のファイルを次のフォルダに格納してください。

クラスタ環境で運用していない場合

- JP1/Audit Management - Manager のインストール先フォルダ¥conf
- JP1/Audit Management - Manager の仮想ディレクトリ¥conf

クラスタ環境で運用している場合

- 共有ディスク¥conf
- JP1/Audit Management - Manager の仮想ディレクトリ¥conf

(3)　データベースのリストア

［データベースマネージャ］ダイアログを使用してデータベースのリストアを実施してください。手順の詳細については「10.1.4　データベースのリストア」を参照してください。

(4)　JP1/Audit Management - Manager の開始

JP1/Audit Management - Manager のサービスを開始してください。JP1/Audit Management - Manager のサービスの開始方法については「5.7.1　監査ログ管理サーバを開始する」を参照してください。

付録

付録 A　ファイル一覧

ここでは，JP1/Audit Management - Manager で使用するファイルの一覧を示します。

付録 A.1　JP1/Audit Management - Manager のファイル一覧

JP1/Audit Management - Manager のファイル一覧を次の表に示します。

表 A–1　JP1/Audit Management - Manager のファイル一覧

項番	フォルダ名	ファイル名	説明
1	¥agent¥aix	−	監査ログ収集対象サーバへの配布モジュール（AIX 用）格納フォルダ
		admagent_aix.tar	監査ログ収集対象サーバへの配布モジュール（AIX 用）
2	¥agent¥hpux_ipf	−	監査ログ収集対象サーバへの配布モジュール（HP-UX (IPF)用）格納フォルダ
		admagent_hpux_ipf.tar	監査ログ収集対象サーバへの配布モジュール（HP-UX(IPF)用）
3	¥agent¥linux	−	監査ログ収集対象サーバへの配布モジュール（Linux 用）格納フォルダ
		admagent_linux.tar	監査ログ収集対象サーバへの配布モジュール（Linux 用）
4	¥agent¥solaris	−	監査ログ収集対象サーバへの配布モジュール（Solaris 用）格納フォルダ
		admagent_solaris.tar	監査ログ収集対象サーバへの配布モジュール（Solaris 用）
5	¥agent¥windows	−	監査ログ収集対象サーバへの配布モジュール（Windows 用）格納フォルダ
		admagent_windows.EXE	監査ログ収集対象サーバへの配布モジュール（Windows 用）
6	¥bin	−	ライブラリ格納フォルダ
		admcold.exe	JP1/NETM/Audit - Manager サービスのプロセス
		admcoldata.exe	監査ログ収集コマンド
		admcolmgr.exe	監査ログ収集マネージャのプロセス
		admcolsubd.exe	監査ログ収集サブプロセス
		admcsvmove.exe	監査ログのバックアップファイル移動コマンド

項番	フォルダ名	ファイル名	説明
		admcsvremove.exe	監査ログのバックアップファイル削除コマンド
		admdbbackup.exe	データベースのバックアップコマンド
		admdbdelete.exe	データベースのデータ削除コマンド
		admdbexport.exe	データベースの CSV バックアップコマンド
		admdbmgr.exe	データベースマネージャのプロセス
		admdbrorg.exe	データベースの再編成コマンド
		admdbstat.exe	データベースの使用状況確認コマンド
		admdbstop.exe	データベースの停止コマンド
		admexport.exe	監査ログのバックアップコマンド
		admimport.exe	監査ログのインポートコマンド
		admmgrsetup.exe	マネージャセットアップのプロセス
		admstdel.exe	監査ログの統計情報削除コマンド
		admstgen.exe	監査ログの統計情報生成コマンド
7	¥conf¥logdef	－	定義ファイル格納フォルダ
		admjevlog_Collaboration.conf	動作定義ファイル（Collaboration 用）
		admjevlog_Collaboration-FileSharing-Webdav.conf	
		admjevlog_Cosminexus.conf	動作定義ファイル（Cosminexus 用）
		admjevlog_HiRDB.conf	動作定義ファイル（HiRDB 用）
		admjevlog_HitachiNavigationPlatform.conf	動作定義ファイル（Hitachi Navigation Platform 用）
		admjevlog_HitachiStorageCommandSuite(HP-UX).conf	動作定義ファイル（Hitachi Storage Command Suite または Hitachi Command Suite（HP-UX）用）
		admjevlog_HitachiStorageCommandSuite(Solaris).conf	動作定義ファイル（Hitachi Storage Command Suite または Hitachi Command Suite（Solaris）用）
		admjevlog_HitachiStorageCommandSuite(AIX).conf	動作定義ファイル（Hitachi Storage Command Suite または Hitachi Command Suite（AIX）用）
		admjevlog_HitachiStorageCommandSuite(Linux).conf	動作定義ファイル（Hitachi Storage Command Suite または Hitachi Command Suite（Linux）用）

項番	フォルダ名	ファイル名	説明
		admjevlog_JP1_AJS2.conf	動作定義ファイル（JP1/AJS2 用）
		admjevlog_JP1_AJS3-host.conf	動作定義ファイル（JP1/AJS3（物理・ホスト）用）
		admjevlog_JP1_AJS3-schedule01.conf～admjevlog_JP1_AJS3-schedule20.conf	動作定義ファイル（JP1/AJS3（スケジューラサービス）用）
		admjevlog_JP1_AO.conf	動作定義ファイル（JP1/AO 用）
		admjevlog_JP1_Base.conf	動作定義ファイル（JP1/Base 用）
		admjevlog_JP1_IM-NP.conf	動作定義ファイル（JP1/IM - NP 用）
		admjevlog_JP1_IM-SS.conf	動作定義ファイル（JP1/IM - SS または JP1/SS 用）
		admjevlog_JP1_HIBUN.conf	動作定義ファイル（JP1/秘文用）
		admjevlog_JP1_ITDM.conf	動作定義ファイル（JP1/ITDM 用）
		admjevlog_JP1_ITDM2.conf	動作定義ファイル（JP1/ITDM2 用）
		admjevlog_JP1_ITDM2-AC.conf	動作定義ファイル（JP1/ITDM2 用）
		admjevlog_JP1_ITDM2-DM.conf	動作定義ファイル（JP1/ITDM2 用）
		admjevlog_JP1_ITDM2-DMClient.conf	動作定義ファイル（JP1/ITDM2 用）
		admjevlog_JP1_ITRM.conf	動作定義ファイル（JP1/ITRM 用）
		admjevlog_JP1_NETM_AIM.conf	動作定義ファイル（JP1/NETM/AIM 用）
		admjevlog_JP1_NETM_Audit-Manager.conf	動作定義ファイル（JP1/Audit Management - Manager（サーバ）用）
		admjevlog_JP1_NETM_Audit-ManagerWeb.conf	動作定義ファイル（JP1/Audit Management - Manager（Web）用）
		admjevlog_JP1_NETM_CSC-Agent.conf	動作定義ファイル（JP1/NETM/CSC - Agent 用）
		admjevlog_JP1_NETM_CSC-Manager.conf	動作定義ファイル（JP1/NETM/CSC - Manager 用）
		admjevlog_JP1_NETM_CSC-ManagerRemoteOption.conf	動作定義ファイル（JP1/NETM/CSC - Manager Remote Option 用）
		admjevlog_JP1_NETM_DM.conf	動作定義ファイル（JP1/NETM/DM 用）

項番	フォルダ名	ファイル名	説明
		admjevlog_JP1_NETM_DM-Client.conf	動作定義ファイル（JP1/NETM/DM Client，JP1/NETM/DM Client - Base 用）
		admjevlog_JP1_NETM_DM-Manager.conf	動作定義ファイル（JP1/NETM/DM Manager 用）
		admjevlog_JP1_NETM_NM-Manager.conf	動作定義ファイル(JP1/NETM/NM 用)
		admjevlog_JP1_PFM.conf	動作定義ファイル（JP1/PFM 用）
		admjevlog_NAVIstaff.conf	動作定義ファイル（活文 NAVIstaff 用）
		admjevlog_OpenTP1.conf	動作定義ファイル（OpenTP1 用）
		admjevlog_EUR.conf	動作定義ファイル（uCosminexus EUR Server 用）
		admjevlog_CosminexusNavigationPlatform.conf	動作定義ファイル（uCosminexus Navigation Platform 用）
		admjevlog_CosminexusPortalFramework.conf	動作定義ファイル（uCosminexus Portal Framework 用）
		admjevlog_UNIX_System_Log.conf	動作定義ファイル（UNIX System Log 用）
		admjevlog_VOS3_TRUST.conf	動作定義ファイル（TRUST E2 用）
		admjevlog_XDM.conf	動作定義ファイル（XDM/BASE E2 用）
		－	製品定義ファイル格納フォルダ
8	¥conf¥product	Collaboration.conf	製品定義ファイル（Collaboration 用）
		Collaboration-FileSharing-Webdav.conf	製品定義ファイル（Cosminexus 用）
		Cosminexus.conf	
		HiRDB.conf	製品定義ファイル（HiRDB 用）
		HitachiNavigationPlatform.conf	製品定義ファイル（Hitachi Navigation Platform 用）
		HitachiStorageCommandSuite(HP-UX).conf	製品定義ファイル（Hitachi Storage Command Suite（HP-UX）用）
		HitachiStorageCommandSuite(Solaris).conf	製品定義ファイル（Hitachi Storage Command Suite（Solaris）用）
		HitachiStorageCommandSuite(AIX).conf	製品定義ファイル（Hitachi Storage Command Suite（AIX）用）

項番	フォルダ名	ファイル名	説明
		HitachiStorageCommandSuite(Linux).conf	製品定義ファイル（Hitachi Storage Command Suite（Linux）用）
		JP1_AJS2.conf	製品定義ファイル（JP1/AJS2 用）
		JP1_AJS3-host.conf	製品定義ファイル（JP1/AJS3（物理・ホスト）用）
		JP1_AJS3-schedule01.conf～JP1_AJS3-schedule20.conf	製品定義ファイル（JP1/AJS3（スケジューラサービス）用）
		JP1_AO.conf	製品定義ファイル（JP1/AO 用）
		JP1_Base.conf	製品定義ファイル（JP1/Base 用）
		JP1_HIBUN.conf	製品定義ファイル（JP1/秘文用）
		JP1_IM-NP.conf	製品定義ファイル（JP1/IM - NP 用）
		JP1_IM-SS.conf	製品定義ファイル（JP1/IM - SS または JP1/SS 用）
		JP1_ITDM.conf	製品定義ファイル（JP1/ITDM 用）
		JP1_ITDM2.conf	製品定義ファイル（JP1/ITDM2 用）
		JP1_ITDM2-AC.conf	製品定義ファイル（JP1/ITDM2 用）
		JP1_ITDM2-DM.conf	製品定義ファイル（JP1/ITDM2 用）
		JP1_ITDM2-DMClient.conf	製品定義ファイル（JP1/ITDM2 用）
		JP1_ITRM.conf	製品定義ファイル（JP1/ITRM 用）
		JP1_NETM_Audit-Manager.conf	製品定義ファイル（JP1/Audit Management - Manager（サーバ）用）
		JP1_NETM_Audit-ManagerWeb.conf	製品定義ファイル（JP1/Audit Management - Manager（Web）用）
		JP1_NETM_AIM.conf	製品定義ファイル（JP1/NETM/AIM 用）
		JP1_NETM_CSC-Agent.conf	製品定義ファイル（JP1/NETM/CSC - Agent 用）
		JP1_NETM_CSC-Manager.conf	製品定義ファイル（JP1/NETM/CSC - Manager 用）
		JP1_NETM_CSC-ManagerRemoteOption.conf	製品定義ファイル（JP1/NETM/CSC - Manager Remote Option 用）
		JP1_NETM_DM.conf	製品定義ファイル（JP1/NETM/DM 用）
		JP1_NETM_DM-Client.conf	製品定義ファイル（JP1/NETM/DM Client，JP1/NETM/DM Client - Base 用）

項番	フォルダ名	ファイル名	説明
		JP1_NETM_DM-Manager.conf	製品定義ファイル（JP1/NETM/DM Manager 用）
		JP1_NETM_NM-Manager.conf	製品定義ファイル(JP1/NETM/NM 用)
		JP1_PFM.conf	製品定義ファイル（JP1/PFM 用）
		NAVIstaff.conf	製品定義ファイル（活文 NAVIstaff 用）
		OpenTP1.conf	製品定義ファイル（OpenTP1 用）
		EUR.conf	製品定義ファイル（uCosminexus EUR Server 用）
		CosminexusNavigationPlatform.conf	製品定義ファイル（uCosminexus Navigation Platform 用）
		CosminexusPortalFramework.conf	製品定義ファイル（uCosminexus Portal Framework 用）
		UNIX_System_Log.conf	製品定義ファイル（UNIX System Log 用）
		VOS3_TRUST.conf	製品定義ファイル（TRUST E2 用）
		WinEventLog_HBase_Storage_Mgmt_Log.conf	製品定義ファイル（Hitachi Storage Command Suite または Hitachi Command Suite 7（Windows）用）
		WinEventLog_HBase64_Storage_Mgmt_Log.conf	製品定義ファイル（Hitachi Command Suite 8（Windows）用）
		WinEventLog_HBase64_Event.conf	製品定義ファイル（Hitachi Command Suite 8（Windows）用）
		WinEventLog_Microsoft-Windows-Security-Auditing.conf	製品定義ファイル（Windows Server 2012 または Windows Server 2008 用）
		WinEventLog_Oracle.conf	製品定義ファイル（Oracle 用）
		WinEventLog_Security.conf	製品定義ファイル（Windows Server 2003 用）
		XDM.conf	製品定義ファイル（XDM/BASE E2 用）
		－	正規化ルールファイル格納フォルダ
9	¥conf¥rule	admrglrule_CALFHM.conf	正規化ルールファイル（統一フォーマット用）
		admrglrule_JP1_AJS2.conf	正規化ルールファイル（JP1/AJS2 製品ログ用）
		admrglrule_JP1_AJS3.conf	正規化ルールファイル（JP1/AJS3 製品ログ用）

項番	フォルダ名	ファイル名	説明
		admrglrule_WinEventLog_Security.conf	正規化ルールファイル（Windows Server 2003 用）
		admrglrule_WinEventLog_Oracle.conf	正規化ルールファイル（Oracle 用）
		admrglrule_AdmConvert.conf	正規化ルールファイル（正規化ルールエディタで変換した監査ログ用）
		−	正規化ルールエディタのインストールフォルダ
10	¥convert¥definer¥bin	ald.exe	正規化ルールエディタのプロセス
		−	正規化サービスのインストールフォルダ
11	¥convert¥server¥bin	admrrexport.exe	正規化ルールのバックアップコマンド
		admrrimport.exe	正規化ルールのインポートコマンド
		alsa_agent.exe	JP1/NETM/Audit - Manager Convert サービスの子プロセス
		alsa_dbacd.exe	JP1/NETM/Audit - Manager Convert サービスの制御プロセス
		alsa_logd.exe	
		alsa_service.exe	
		alsa_spmd.exe	JP1/NETM/Audit - Manager Convert サービスの親プロセス
		alsd_dbacd.exe	JP1/NETM/Audit - Manager Define サービスの子プロセス
		alsd_logd.exe	JP1/NETM/Audit - Manager Define サービスの制御プロセス
		alsd_monsrv.exe	
		alsd_service.exe	
		alsd_spmd.exe	JP1/NETM/Audit - Manager Define サービスの親プロセス
		−	正規化機能ログファイル出力フォルダ
12	¥convert¥server¥log¥server	admrrexport*.log	正規化ルールバックアップログファイル
		admrrimport*.log	正規化ルールインポートログファイル
		servera{1|2}.log	正規化サービスログファイル
		serverd{1|2}.log	正規化定義サービスログファイル
		alsa_spmd1.log	正規化サービス起動停止ログファイル
		alsd_spmd1.log	正規化定義サービス起動停止ログファイル

項番	フォルダ名	ファイル名	説明
		admlsedbsetup{1|2}.log	正規化定義データベースセットアップログファイル
		admlsrelease{1|2}.log	正規化定義データベースリリースログファイル
		−	データ出力フォルダ
13	¥dat	−	監査ログ管理データベースの運用フォルダ
14	¥db	−	ログファイル出力フォルダ
15	¥log	admlog*.log	ログメッセージの保存ファイル
		−	spool 格納フォルダ
16	¥spool	admrglerrordatYYYYMMDD※.csv	正規化処理エラーファイル
		−	ツール格納フォルダ
17	¥tools	admlog.vbs	トラブルシュート用資料採取スクリプト
		−	トラブルシュート用資料格納フォルダ
18	¥troubleshoot		

（凡例）

−：該当なし

注※

YYYY が年，MM が月，DD が日を示しています。

付録 A.2　JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧

JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧を次の表に示します。

表 A-2　JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧

項番	フォルダ名	ファイル名	説明
1	¥bin	−	ライブラリ格納フォルダ
2	¥conf	−	定義ファイル格納フォルダ
		admAnalysis.ini	分析方法定義ファイル
		admCommonAnalysis.ini	監査ログレポート定義ファイル
3	¥csv	−	csv 形式ファイル出力フォルダ
4	¥html	−	html 形式ファイル出力フォルダ

項番	フォルダ名	ファイル名	説明
5	¥log	−	製品ログ，監査ログ格納フォルダ
6	¥pdf	−	EUR フォームファイル格納，サンプル CSV 形式ファイル，PDF 出力フォルダ
		admConditionRetrieval.csv	監査ログ検索条件の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admConditionTotalPlaceCategory.csv	監査ログ集計条件（発生場所×監査事象種別）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admConditionTotalPlaceResult.csv	監査ログ集計条件（発生場所×監査事象結果）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admConditionTotalProgramCategory.csv	監査ログ集計条件（プログラム名×監査事象種別）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admConditionTotalProgramResult.csv	監査ログ集計条件（プログラム名×監査事象結果）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admConditionTotalSubjectCategory.csv	監査ログ集計条件（サブジェクト情報×監査事象種別）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admConditionTotalSubjectResult.csv	監査ログ集計条件（サブジェクト情報×監査事象結果）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admResultRetrieval.csv	監査ログ検索結果の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admResultTotalPlaceCategory.csv	監査ログ集計結果（発生場所×監査事象種別）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admResultTotalPlaceResult.csv	監査ログ集計結果（発生場所×監査事象結果）の帳票フォーム

項番	フォルダ名	ファイル名	説明
			編集用サンプル CSV 形式ファイル（EUR 用）※1
		admResultTotalProgramCategory.csv	監査ログ集計結果（プログラム名×監査事象種別）の帳票フォーム編集用サンプル CSV 形式ファイル(EUR 用)※1
		admResultTotalProgramResult.csv	監査ログ集計結果（プログラム名×監査事象結果）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admResultTotalSubjectCategory.csv	監査ログ集計結果（サブジェクト情報×監査事象種別）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admResultTotalSubjectResult.csv	監査ログ集計結果（サブジェクト情報×監査事象結果）の帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）※1
		admRetrieval.fms	監査ログ検索結果の帳票フォームファイル※2
		admTotalPlaceCategory.fms	監査ログ集計結果（発生場所×監査事象種別）の帳票フォームファイル※2
		admTotalPlaceResult.fms	監査ログ集計結果（発生場所×監査事象結果）の帳票フォームファイル※2
		admTotalProgramCategory.fms	集計結果（プログラム名×監査事象種別）の帳票フォームファイル※2
		admTotalProgramResult.fms	監査ログ集計結果（プログラム名×監査事象結果）の帳票フォームファイル※2
		admTotalSubjectCategory.fms	集計結果（サブジェクト情報×監査事象種別）の帳票フォームファイル※2
		admTotalSubjectResult.fms	集計結果（サブジェクト情報×監査事象結果）の帳票フォームファイル※2

（凡例）

－：該当なし

注※1

帳票フォーム編集用サンプル CSV 形式ファイル（EUR 用）は，EUR Professional Edition 07-60 以降，uCosminexus EUR Designer 08-00 以降，または uCosminexus EUR Developer 08-00 以降を使用して帳票フォームをカスタマイズする際に参照する CSV 形式ファイルです。

注※2

帳票フォームファイルは，EUR と連携した PDF ファイル出力用の PDF 出力フォーマットを定義しているファイルです。

付録 A.3　監査ログ収集対象サーバに配布されるファイル一覧

admagtinstall コマンドを実行することで監査ログ収集対象サーバに配布されるファイルについて説明します。これらのファイルは，監査ログ収集対象サーバのセットアップに必要になります。

(1)　Windows の場合

Windows の場合の監査ログ収集対象サーバに配布されるファイル一覧について説明します。JP1/NETM/Audit - Manager 09-00 より前のバージョンから上書きインストールした場合は，前バージョンのフォルダ構成を引き継ぎます。

(a)　JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき

JP1/NETM/Audit - Manager 09-00 以降の新規インストール時に監査ログ収集対象サーバに配布されるファイルの一覧について次の表に示します。

表 A-3　JP1/NETM/Audit - Manager 09-00 以降の新規インストール時に監査ログ収集対象サーバに配布されるファイル一覧（Windows の場合）

項番	フォルダ名	ファイル名	説明
1	任意のインストール先フォルダ¥bin	－	ライブラリ格納フォルダ
		admagtsetup.exe	監査ログ専用イベントサーバの環境セットアップコマンド
		admhasetup.exe	監査ログ収集対象サーバのクラスタ環境用セットアップコマンド
		admlogtrapd.exe	監査ログ収集対象サーバのクラスタ環境用ログトラップ起動/停止コマンド
2	任意のインストール先フォルダ¥conf	－	設定ファイル格納フォルダ
		admagtsetup.conf.model	監査ログ収集対象サーバセットアップ定義ファイルのモデルファイル
3	任意のインストール先フォルダ¥log	－	ログファイル出力フォルダ
4	JP1/Base インストール先フォルダ¥bin	－	ライブラリ格納フォルダ
		adm_adaptercmd.exe	アダプタコマンド

項番	フォルダ名	ファイル名	説明
5	JP1/Base インストール先フォルダ¥plugin¥conf	−	アダプタコマンド定義ファイル格納フォルダ
		Adapter_HITACHI_JP1_NETM_AUDIT.conf	アダプタコマンド定義ファイル

（凡例）

−：該当なし

(b) JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたときに，監査ログ収集対象サーバに配布されるファイルの一覧について，次の表に示します。

表 A-4　JP1/NETM/Audit - Manager 09-00 より前のバージョンからのバージョンアップ時に監査ログ収集対象サーバに配布されるファイル一覧（Windows の場合）

項番	フォルダ名	ファイル名	説明
1	システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥manager¥bin	−	ライブラリ格納フォルダ
		admagtsetup.exe	監査ログ専用イベントサーバの環境セットアップコマンド
		admhasetup.exe	監査ログ収集対象サーバのクラスタ環境用セットアップコマンド
		admlogtrapd.exe	監査ログ収集対象サーバのクラスタ環境用ログトラップ起動/停止コマンド
2	システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥manager¥conf	−	設定ファイル格納フォルダ
		admagtsetup.conf.model	監査ログ収集対象サーバセットアップ定義ファイルのモデルファイル
3	システムドライブ¥Program Files¥Hitachi¥jp1netmaudit¥manager¥log	−	ログファイル出力フォルダ
4	JP1/Base インストール先フォルダ¥bin	−	ライブラリ格納フォルダ
		adm_adaptercmd.exe	アダプタコマンド
5	JP1/Base インストール先フォルダ¥plugin¥conf	−	アダプタコマンド定義ファイル格納フォルダ
		Adapter_HITACHI_JP1_NETM_AUDIT.conf	アダプタコマンド定義ファイル

（凡例）

−：該当なし

(2) UNIX の場合

UNIX の場合の監査ログ収集対象サーバに配布されるファイル一覧について説明します。JP1/NETM/Audit - Manager 09-00 より前のバージョンから上書きインストールした場合は，前バージョンのフォルダ構成を引き継ぎます。

(a) JP1/NETM/Audit - Manager 09-00 以降を新規インストールしたとき

JP1/NETM/Audit - Manager 09-00 以降の新規インストール時に監査ログ収集対象サーバに配布されるファイルの一覧について次の表に示します。

表 A-5 JP1/NETM/Audit - Manager 09-00 以降の新規インストール時に監査ログ収集対象サーバに配布されるファイル一覧（UNIX の場合）

項番	ディレクトリ名	ファイル名	説明
1	/etc/opt/jp1netmaudit/agent/conf	−	設定ファイル格納ディレクトリ
		admagtsetup.conf.model	監査ログ収集対象サーバセットアップ定義ファイルのモデルファイル
2	/opt/jp1base/bin	−	ライブラリ格納ディレクトリ
		adm_adaptercmd	アダプタコマンド
3	/opt/jp1base/plugin/conf	−	アダプタコマンド定義ファイル格納フォルダ
		Adapter_HITACHI_JP1_NETM_AUDIT.conf	アダプタコマンド定義ファイル
4	/opt/jp1netmaudit/agent/bin	−	ライブラリ格納ディレクトリ
		admagtsetup	監査ログ専用イベントサーバの環境セットアップコマンド
		admhasetup	監査ログ収集対象サーバのクラスタ環境用セットアップコマンド
		admhastart	監査ログ収集対象サーバのクラスタ環境用ログトラップ開始コマンド
		admhastop	監査ログ収集対象サーバのクラスタ環境用ログトラップ停止コマンド
		admuxlogcol	UNIX ログ変換コマンド
5	/var/opt/jp1netmaudit/agent/log	−	ログファイル出力ディレクトリ

（凡例）

−：該当なし

(b) JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたとき

JP1/NETM/Audit - Manager 09-00 より前のバージョンからバージョンアップしたときに，監査ログ収集対象サーバに配布されるファイルの一覧について，次の表に示します。

表 A-6　JP1/NETM/Audit - Manager 09-00 より前のバージョンからのバージョンアップ時に監査ログ収集対象サーバに配布されるファイル一覧（UNIX の場合）

項番	ディレクトリ名	ファイル名	説明
1	/opt/jp1netmaudit/manager/conf	−	設定ファイル格納ディレクトリ
		admagtsetup.conf.model	監査ログ収集対象サーバセットアップ定義ファイルのモデルファイル
2	/opt/jp1base/bin	−	ライブラリ格納ディレクトリ
		adm_adaptercmd	アダプタコマンド
3	/opt/jp1base/plugin/conf	−	アダプタコマンド定義ファイル格納フォルダ
		Adapter_HITACHI_JP1_NETM_AUDIT.conf	アダプタコマンド定義ファイル
4	/opt/jp1netmaudit/manager/bin	−	ライブラリ格納ディレクトリ
		admagtsetup	監査ログ専用イベントサーバの環境セットアップコマンド
		admhasetup	監査ログ収集対象サーバのクラスタ環境用セットアップコマンド
		admhastart	監査ログ収集対象サーバのクラスタ環境用ログトラップ開始コマンド
		admhastop	監査ログ収集対象サーバのクラスタ環境用ログトラップ停止コマンド
		admuxlogcol	UNIX ログ変換コマンド
5	/opt/jp1netmaudit/manager/log	−	ログファイル出力ディレクトリ

（凡例）

−：該当なし

付録 B　ポート番号一覧

JP1/Audit Management - Manager で使用するポート番号とポート番号の設定方法について説明します。

付録 B.1　JP1/Audit Management - Manager のポート番号

JP1/Audit Management - Manager で使用するサービスの各プロセスは，指定したポート番号に対して，TCP/IP のバインド処理をします。

監査ログ管理サーバ，および監査ログ収集対象サーバで使用するポート番号のデフォルトについて次の表に示します。ここで示すポート番号は，ほかのポート番号に変更することもできます。

表 B-1　ポート番号のデフォルト（監査ログ管理サーバ）

項番	サービス名	ポート番号/プロトコル	説明
1	−	24100/tcp	組み込みデータベースで使用されるポート番号です。 監査ログ管理データベースにアクセスする各プロセスからの接続を受け付けます。 このポート番号は，監査ログ管理サーバのローカルマシンで使用されます。
2	auditd_monsrv	24105/tcp	JP1/NETM/Audit - Manager Define サービスで使用されるポート番号です。 このポート番号は，監査ログ管理サーバのローカルマシンで使用されます。
3	audita_admsrv	24106/tcp	JP1/NETM/Audit - Manager Convert サービスで使用されるポート番号です。 このポート番号は，監査ログ管理サーバのローカルマシンで使用されます。
4	http	80/tcp	監査ログ管理画面から監査ログ管理サーバにアクセスする際に使用されるポート番号です。 監査ログ管理画面から監査ログ管理サーバにアクセスする際に使用されるポート番号は，Web サーバの設定に依存します。

（凡例）

−：なし

表 B-2　ポート番号のデフォルト（監査ログ収集対象サーバ）

項番	サービス名	ポート番号/プロトコル	説明
1	−	24101/tcp	監査ログ専用イベントサーバの転送用ポート番号です。
2	−	24102/tcp	監査ログ専用イベントサーバの AP 用ポート番号です。

（凡例）

－：なし

付録 B.2　JP1/Audit Management - Manager で使用するポート番号の変更方法

デフォルトのポート番号がすでに使用されている場合など，JP1/Audit Management - Manager で使用するポート番号を変更したい場合は，次に示す手順を実施します。デフォルトのポート番号については「付録 B.1　JP1/Audit Management - Manager のポート番号」を参照してください。

(1)　監査ログ管理サーバで使用するポート番号の変更方法

監査ログ管理サーバで使用する各ポート番号の変更方法について説明します。

- 組み込みデータベースのポート番号

  データベースのセットアップ時に，データベースマネージャの［データベースの基本設定］画面で，重複しないポート番号に変更します。

  ［データベースの基本設定］画面の設定については「5.5.7　監査ログ管理サーバのデータベースをセットアップする」を参照してください。

- JP1/NETM/Audit - Manager Define サービスのポート番号

  services ファイルで定義されている JP1/NETM/Audit - Manager Define サービス（auditd_monsrv）のポート番号を，重複しないポート番号に変更します。services ファイルの変更方法については「5.5.2　services ファイルを確認する」を参照してください。

- JP1/NETM/Audit - Manager Convert サービスのポート番号

  services ファイルで定義されている JP1/NETM/Audit - Manager Convert サービス（audita_admsrv）のポート番号を，重複しないポート番号に変更します。services ファイルの変更方法については「5.5.2　services ファイルを確認する」を参照してください。

- 監査ログ管理画面のポート番号

  IIS マネージャの設定で，重複しないポート番号に変更します。

(2)　監査ログ収集対象サーバで使用するポート番号の変更方法

- 監査ログ専用イベントデータベースのポート番号

  JP1/Base のイベントサーバ設定ファイル（conf）で定義されている監査ログ専用イベントサーバの転送用ポート番号および AP 用ポート番号を，重複しないポート番号に変更します。

  ポート番号の変更方法の詳細については「5.4.2(3)　監査ログ専用イベントサーバの環境情報を変更する」を参照してください。

付録 B.3　ファイアウォールの通過方向

JP1/Audit Management - Manager は，パケットフィルタリング型のファイアウォールと NAT 型（スタティックモード）のアドレス変換に対応しています。

ファイアウォールの通過方向について，次の表に示します。この表のポート番号は，JP1/Audit Management - Manager を動作させるのに必要なポート番号を示しています。このため，JP1/Audit Management - Manager を動作させるために JP1/Base で使用するポート番号も含みます。JP1/Base で使用するポート番号の詳細については，マニュアル「JP1/Base 運用ガイド」を参照してください。

表 B-3　ファイアウォールの通過方向

項番	サービス名	ポート番号/プロトコル	通過方向
1	jp1imevt	20098/tcp	監査ログ収集対象サーバ →監査ログ管理サーバ
2	jp1imevtapi	20099/tcp	監査ログ管理サーバ →監査ログ管理サーバ
3	jp1bsplugin	20306/tcp	監査ログ管理サーバ →監査ログ収集対象サーバ
4	jp1bsuser	20240/tcp	監査ログ管理サーバ →認証サーバ（JP1/Base）
5	－	24101/tcp	監査ログ収集対象サーバ →監査ログ収集対象サーバ
6	－	24102/tcp	監査ログ管理サーバ →監査ログ収集対象サーバ
7	auditd_monsrv	24105/tcp	監査ログ管理サーバ →監査ログ管理サーバ
8	audita_admsrv	24106/tcp	監査ログ管理サーバ →監査ログ管理サーバ
9	http	80/tcp	Web クライアント →監査ログ管理サーバ

（凡例）

－：なし

→：ファイアウォールの通過方向

注

- ここで示すポート番号を使用してコネクションを確立する場合，確立されたセッションへの返信は，ANY を必ず通すようにファイアウォールを設定してください。
- ファイアウォールサーバとなるマシンに JP1/Audit Management - Manager をインストールする場合でも，ファイアウォールの対象となることがあります。このため，同一マシン内でも通信できるように設定してください。

付録 C　正規化ルールファイルの作成例

正規化ルールファイルの作成例を次に示します。

正規化ルールファイルの定義内容については「13.2　正規化ルールファイル」を参照してください。

付録 C.1　TYPE が KEY の場合

TYPE が KEY の場合の監査ログについて，正規化ルールファイルの例を示します。

(1)　正規化前の監査ログの内容例（TYPE が KEY の場合）

```
num=1,msgid=1234,date=2007-01-01T10:10:10.100+09:00,prog=XYZ,comp=xyz,pid=1234,
host=HostA,ctgy=Authentication,result=Success,subj:euid=userA,authsrv=hostB,
msg=”認証に成功しました。”
```

監査ログの各項目の内容を次の表に示します。

表 C-1　正規化前の監査ログの内容（TYPE が KEY の場合）

項番	属性名	内容
1	num	ログの通番
2	msgid	メッセージ識別番号（メッセージ ID）
3	date	日時
4	prog	プログラム名称
5	comp	コンポーネント名称
6	pid	プロセス ID
7	host	発生場所
8	ctgy	ログのカテゴリ
9	result	ログの結果
10	subj:euid	ユーザ情報
11	authsrv	認証サーバ
12	msg	メッセージ

(2)　正規化ルールファイルの定義例（TYPE が KEY の場合）

```
[LOGTYPE]
TYPE=KEY
SEPARATE=comma
SECTION=0
```

```
LOGSTART=0
ESCTYPE=1
FRONTESC=
REARESC=
SKIPSPACE=1

[PATTERN]
1=AuditLogID:-:num:2
2=MessageID:-:msgid:3
3=MessageDate:D:date:4
4=ProgramName:-:prog:5
5=ComponentName:-:comp:6
6=ProcessID:-:pid:7
7=PlaceInfo:-:host:8
8=EventCategoryName:-:ctgy:9
9=EventResultName:-:result:10
10=SubjectInfo:S:"subj:euid":11
11=PeculiarInfo:M:"":0
```

正規化ルールファイルの定義例の説明を次の表に示します。

表 C-2　正規化ルールファイルの定義例の説明（TYPE が KEY の場合）

項番	設定項目	説明
1	[LOGTYPE]	定義の始まりを示す[LOGTYPE]を指定します。
2	TYPE=KEY	形式は「XX=XX」のため「KEY」を指定します。
3	SEPARATE=comma	区切り文字は「,」のため「comma」を指定します。
4	SECTION=0	セクションは特に指定しないため「0」を指定します。
5	LOGSTART=0	区切りは先頭から行うため「0」を指定します。
6	ESCTYPE=1	エスケープは「"」であるため「1」を指定します。
7	FRONTESC=	エスケープが「"」のため設定不要です。
8	REARESC=	エスケープが「"」のため設定不要です。
9	SKIPSPACE=	区切り文字が「,」のため設定不要です。
10	[PATTERN]	セクションは特に指定していないため「PATTERN」を指定します。
11	1=AuditLogID:-:num:2	監査ログ ID には「num」の値を使用し，2 番を実行します。
12	2=MessageID:-:msgid:3	メッセージ ID には「msgid」の値を使用し，3 番を実行します。
13	3=MessageDate:D:date:4	日時には「date」の値を使用し，4 番を実行します。
14	4=ProgramName:-:prog:5	プログラム名には「prog」の値を使用し，5 番を実行します。
15	5=ComponentName:-:comp:6	コンポーネント名には「comp」の値を使用し，6 番を実行します。

項番	設定項目	説明
16	6=ProcessID:-:pid:7	プロセス ID には「pid」の値を使用し，7 番を実行します。
17	7=PlaceInfo:-:host:8	発生場所には「host」の値を使用し，8 番を実行します。
18	8=EventCategoryName:-:ctgy:9	監査事象種別には「ctgy」の値を使用し，9 番を実行します。
19	9=EventResultName:-:result:10	監査事象結果には「result」の値を使用し，10 番を実行します。
20	10=SubjectInfo:S:"subj:euid":11	サブジェクト種別には「実行ユーザ ID」を使用し，サブジェクト情報には「subj:euid」の値を使用して，11 番を実行します。
21	11=PeculiarInfo:M:"":0	残りのデータを固有情報とし，正規化を終了します。

(3) 正規化後の監査ログ管理画面での表示例（TYPE が KEY の場合）

「正規化前の監査ログの内容例」を正規化した結果，監査ログ管理画面に表示される内容の例を次の表に示します。

表 C-3 正規化後の監査ログ管理画面での表示例（TYPE が KEY の場合）

項番	監査ログ管理画面での項目	内容
1	監査ログ ID	1
2	メッセージ ID	1234
3	日時	2007-01-01 10:10:10.100
4	プログラム名	XYZ
5	コンポーネント名	xyz
6	プロセス ID	1234
7	発生場所	HostA
8	監査事象種別	Authentication
9	監査事象結果	Success
10	サブジェクト種別	実行ユーザ ID
11	サブジェクト情報	userA
12	固有情報	TZD=+09:00,authsrv=hostB,msg="認証に成功しました。"

付録 C.2　TYPE が VALUE の場合

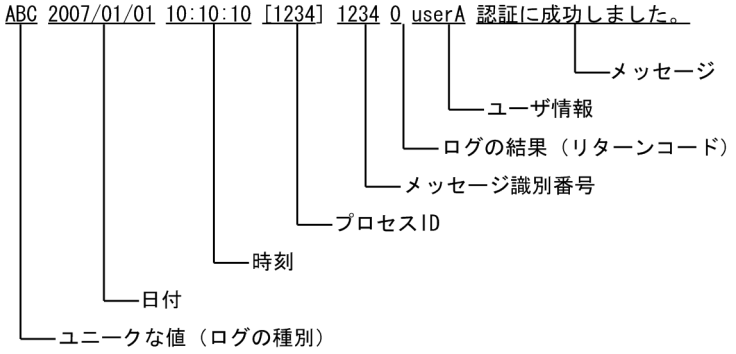
TYPE が VALUE の場合の監査ログについて，正規化ルールファイルの例を示します。

(1)　正規化前の監査ログの内容例（TYPE が VALUE の場合）

```
ABC 2007/01/01 10:10:10 [1234] 1234 0 userA 認証に成功しました。
```

監査ログの各項目の内容を次の図に示します。

図 C-1　正規化前の監査ログの内容



(2)　正規化ルールファイルの定義例（TYPE が VALUE の場合）

```
[LOGTYPE]
TYPE=VALUE
SEPARATE=space
SECTION=1
LOGSTART=1
ESCTYPE=2
FRONTESC=[
REARESC=]
SKIPSPACE=0

[ABC]
1=AuditLogID:*:0:2
2=ProgramName:*:XYZ:3
3=ComponentName:*:xyz:4
4=PlaceInfo:H:5
5=EventCategoryName:*:Authentication:6
6=CHECK:J:6:-1:8:7
7=CHECK:J:6:0:9:10
8=EventResultName:*:Failure:11
9=EventResultName:*:Success:11
10=EventResultName:*:Occurrence:11
11=SubjectInfo:C:"subj:euid":7:12
12=MessageDate:D:2,3:13
13=ProcessID:-:4:14
14=MessageID:-:5:15
15=PeculiarInfo:N:8:0
```

正規化ルールファイルの定義例の説明を次の表に示します。

表 C-4　正規化ルールファイルの定義例の説明（TYPE が VALUE の場合）

項番	設定項目	説明
1	[LOGTYPE]	定義の始まりを示す[LOGTYPE]を指定します。
2	TYPE=VALUE	形式は「**値 1，値 2・・・**」（値の羅列）のため「VALUE」を指定します。
3	SEPARATE=space	区切り文字は「△（半角スペース）」のため「space」を指定します。
4	SECTION=1	セクションは特に指定しないため「1」を指定します。
5	LOGSTART=1	区切りは先頭から行うため「1」を指定します。
6	ESCTYPE=2	エスケープは「[ ]」であるため「2」を指定します。
7	FRONTESC=[	エスケープが「[」のため「[」を指定します。
8	REARESC=]	エスケープが「]」のため「]」を指定します。
9	SKIPSPACE=0	スペースはまとめないため「0」を指定します。
10	[ABC]	セクション名として監査ログの先頭の文字列を使用します。
11	1=AuditLogID:*:0:2	監査ログ ID には固定値で「0」を使用し，2 番を実行します。
12	2=ProgramName:*:XYZ:3	プログラム名には固定値で「XYZ」を使用し，3 番を実行します。
13	3=ComponentName:*:xyz:4	コンポーネント名には固定値で「xyz」を使用し，4 番を実行します。
14	4=PlaceInfo:H:5	発生場所には監査ログ収集対象サーバ名を使用し，5 番を実行します。
15	5=EventCategoryName:*:Authentication:6	監査事象種別には固定値で「Authentication」を使用し，6 番を実行します。
16	6=CHECK:J:6:-1:8:7	監査ログの 6 番が「-1」の場合，8 番を実行し，それ以外は 7 番を実行します。
17	7=CHECK:J:6:0:9:10	監査ログの 6 番が「0」の場合，9 番を実行し，それ以外は 10 番を実行します。
18	8=EventResultName:*:Failure:11	監査事象結果には固定値で「Failure」を使用し，11 番を実行します。
19	9=EventResultName:*:Success:11	監査事象結果には固定値で「Success」を使用し，11 番を実行します。
20	10=EventResultName:*:Occurrence:11	監査事象結果には固定値で「Occurrence」を使用し，11 番を実行します。

項番	設定項目	説明
21	11=SubjectInfo:C:"subj:euid":7:12	サブジェクト種別には「実行ユーザ ID」を使用し，サブジェクト情報には 7 番の値を使用して，12 番を実行します。
22	12=MessageDate:D:2,3:13	日時には 2 番と 3 番の値を使用し，13 番を実行します。
23	13=ProcessID:-:4:14	プロセス ID には 4 番の値を使用し，14 番を実行します。
24	14=MessageID:-:5:15	メッセージ ID には 5 番の値を使用し，15 番を実行します。
25	15=PeculiarInfo:N:8:0	残りのデータを固有情報とし，正規化を終了します。

(3)　正規化後の監査ログ管理画面での表示例（TYPE が VALUE の場合）

「正規化前の監査ログの内容例」を正規化した結果，監査ログ管理画面に表示される内容の例を次の表に示します。

表 C-5　正規化後の監査ログ管理画面での表示例（TYPE が VALUE の場合）

項番	監査ログ管理画面での項目	内容
1	監査ログ ID	－
2	メッセージ ID	1234
3	日時	2007-01-01 10:10:10.100
4	プログラム名	XYZ
5	コンポーネント名	xyz
6	プロセス ID	1234
7	発生場所	**監査ログ収集対象サーバ名**
8	監査事象種別	Authentication
9	監査事象結果	Success
10	サブジェクト種別	実行ユーザ ID
11	サブジェクト情報	userA
12	固有情報	認証に成功しました。

（凡例）

－：空白

付録 C.3　TYPE が WINEVENT の場合

TYPE が WINEVENT の場合の監査ログについて，正規化ルールファイルの例を示します。

(1) 正規化前の監査ログの内容例（TYPE が WINEVENT の場合）

監査ログの各項目の内容例を次の表に示します。

表 C-6 正規化前の監査ログの内容例（TYPE が WINEVENT の場合）

項番	項目		値
1	イベントログの種類		成功の監査
2	イベントソース名		Security
3	イベントカテゴリ		オブジェクト アクセス
4	イベント ID		564
5	イベント発生日		2008/01/01
6	イベント発生時刻		10:10:10
7	ユーザー名		Host1¥Administrator
8	コンピュータ名		Host1
9	説明	削除されたオブジェクト	－
10		オブジェクトサーバー	Security
11		ハンドル ID	2284
12		プロセス ID	1456
13		イメージファイル名	C:¥WINDOWS¥explorer.exe

（凡例）

－：なし

(2) 正規化ルールファイルの定義例（TYPE が WINEVENT の場合）

```
[LOGTYPE]
TYPE=WINEVENT
SEPARATE=CRLF
SECTION=1
LOGSTART=0
ESCTYPE=0

[644]※1
1=AuditLogID:*:0:2
2=MessageID:W:WinEventID:3
3=MessageDate:W:WinEventDate:4
4=ProgramName:*:Windows:5
5=ComponentName:*:AccountManagement:6
6=ProcessID:*:-1:7
7=PlaceInfo:W:WinEventPlace:8
8=EventCategoryName:*:ConfigurationAccess:9
9=EventResultName:*:Success:10
10=SubjectInfo:C:"subj:uid":呼び出し側ユーザー名:11
11=PeculiarInfo:*:obj=OSUser,op=Change:12
```

```
12=PeculiarInfo:A:"objloc:from=":呼び出し側ドメイン:13
13=PeculiarInfo:E:0

[564]※2
1=AuditLogID:*:0:2
2=MessageID:W:WinEventID:3
3=MessageDate:W:WinEventDate:4
4=ProgramName:*:Windows:5
5=ComponentName:*:ObjectAccess:6
6=ProcessID:*:-1:7
7=PlaceInfo:W:WinEventPlace:8
8=EventCategoryName:*:ContentAccess:9
9=EventResultName:*:Success:10
10=SubjectInfo:C:"subj:pid":"プロセス ID":11
11=PeculiarInfo:E:0
```

注※1

JP1/Audit Management - Manager が標準サポートしている Windows イベントログ（セキュリティに関する情報）の正規化ルールです。標準サポートしている Windows イベントログ（セキュリティに関する情報）の正規化ルールはデフォルトで記述されています。この正規化ルールの記述の下に，標準サポート外の Windows イベントログ（セキュリティに関する情報）の正規化ルールを追加してください。

注※2

JP1/Audit Management - Manager で標準サポート外の Windows イベントログ（セキュリティに関する情報）の正規化ルールです。

イベント ID が「564」の監査ログについて，正規化ルールファイルの定義例の説明を次の表に示します。

表 C-7　正規化ルールファイルの定義例の説明（TYPE が WINEVENT の場合）

項番	設定項目	説明
1	[LOGTYPE]	定義の始まりを示す[LOGTYPE]を指定します。
2	TYPE=WINEVENT	Windows イベントログのため「WINEVENT」を指定します。
3	SEPARATE=CRLF	区切り文字は改行コード（CR+LF）のため，「CRLF」を指定します。
4	SECTION=1	セクションは Windows イベント ID を指定するため「1」を指定します。
5	LOGSTART=0	区切りは先頭から行うため「0」を指定します。
6	ESCTYPE=0	エスケープしないログのため「0」を指定します。
7	[564]	セクションはイベント ID「564」を指定します。
8	1=AuditLogID:*:0:2	監査ログ ID は「0」を使用し，2 番を実行します。
9	2=MessageID:W:WinEventID:3	メッセージ ID は Windows イベントのイベント ID「564」を使用し，3 番を実行します。

項番	設定項目	説明
10	3=MessageDate:W:WinEventDate:4	日時は Windows イベントの発生日時「2008-01-01」「10:10:10」を使用し，4 番を実行します。
11	4=ProgramName:*:Windows:5	プログラム名は「Windows」を使用し，5 番を実行します。
12	5=ComponentName:*:ObjectAccess:6	コンポーネント名は「ObjectAccess」を使用し，6 番を実行します。
13	6=ProcessID:*:-1:7	プロセス ID は「-1」を使用し，7 番を実行します。
14	7=PlaceInfo:W:WinEventPlace:8	発生場所は Windows イベントが発生した場所のコンピュータ名「Host1」を使用し，8 番を実行します。
15	8=EventCategoryName:*:ContentAccess:9	監査事象種別は「ContentAccess」を使用し，9 番を実行します。
16	9=EventResultName:*:Success:10	監査事象結果は「Success」を使用し，10 番を実行します。
17	10=SubjectInfo:C:"subj:pid":"プロセス ID":11	サブジェクト種別は「プロセス ID」を使用し，サブジェクト情報はプロセス ID の値「1456」を使用して，11 番を実行します。
18	11=PeculiarInfo:E:0	残りのデータを固有情報とし，正規化を終了します。

(3) 正規化後の監査ログ管理画面での表示例（TYPE が WINEVENT の場合）

「正規化前の監査ログの内容例」を正規化した結果，監査ログ管理画面に表示される内容の例を次の表に示します。

表 C-8 正規化後の監査ログ管理画面での表示例（TYPE が WINEVENT の場合）

項番	監査ログ管理画面での項目	内容
1	監査ログ ID	－
2	メッセージ ID	564
3	日時	2008/01/01 10:10:10.000
4	プログラム名	Windows
5	コンポーネント名	ObjectAccess
6	プロセス ID	－
7	発生場所	Host1
8	監査事象種別	ContentAccess
9	監査事象結果	Success
10	サブジェクト種別	プロセス ID
11	サブジェクト情報	1456

項番	監査ログ管理画面での項目	内容
12	固有情報	削除されたオブジェクト:,オブジェクト サーバー:Security,ハンドル ID:2284,イメージ ファイル名:C:¥WINDOWS¥explorer.exe

(凡例)

－：空白

付録 D　JP1/Audit Management - Manager の監査ログの出力情報

JP1/Audit Management - Manager の監査ログの出力情報について説明します。

JP1/Audit Management - Manager の監査ログは，次に示す 2 種類があります。

- JP1/Audit Management - Manager（サーバ）
- JP1/Audit Management - Manager の監査ログ管理画面（Web）

付録 D.1　監査ログに出力される事象の種別

監査ログを出力する対象となる事象の種別および JP1/Audit Management - Manager が監査ログを出力する契機を次の表に示します。事象の種別とは，監査ログに出力される事象を分類するための識別子です。

なお，この情報は，JP1/Audit Management - Manager（サーバ）と JP1/Audit Management - Manager の監査ログ管理画面（Web）の共通情報です。

表 D-1　監査ログに出力される事象の種別

項番	事象の種別	説明	JP1/Audit Management - Manager が出力する契機
1	StartStop	ソフトウェアの起動および終了を示す事象です。	JP1/NETM/Audit - Manager サービスに関して，次に示す記録を出力します。 • サービスの起動 • サービスの起動失敗 • サービスの停止 • サービスの異常終了 • コマンドの正常終了 • コマンドの異常終了
2	Authentication	管理者が，JP1/Audit Management - Manager への認証または接続に，成功または失敗したことを示す事象です。	JP1/Audit Management - Manager の各画面へのログイン・ログアウトに関して，次に示す記録を出力します。 • ログイン成功 • ログイン失敗 • ログアウト
3	ConfigurationAccess	管理者が許可された運用操作を実行し，操作が正常終了または異常終了したことを示す事象です。	製品定義の変更，データベースセットアップ，監査ログ収集対象変更に関して，次に示す記録を出力します。 • 製品定義変更の正常終了 • 製品定義変更の異常終了 • データベースセットアップの正常終了

項番	事象の種別	説明	JP1/Audit Management - Manager が出力する契機
			• データベースセットアップの異常終了 • 監査ログ収集対象の追加・削除の正常終了 • 監査ログ収集対象の追加・削除の異常終了 • 正規化ルール定義データ変更の正常終了 • 正規化ルール定義データ変更の異常終了 • 正規化ルール定義データへのアクセス成功 • 正規化ルール定義データへのアクセス失敗
4	ContentAccess	監査ログ管理データベースのデータへのアクセスに，成功または失敗したことを示す事象です。	監査ログ管理データへのアクセスに関して，次に示す記録を出力します。 • 監査ログ管理データへのアクセス成功 • 監査ログ管理データへのアクセス失敗 • CSV 形式ファイル，PDF ファイル，バックアップファイルなどへのアクセス成功 • CSV 形式ファイル，PDF ファイル，バックアップファイルなどへのアクセス失敗 監査ログ統計データへのアクセスに関して，次に示す記録を出力します。 • 監査ログ統計データへのアクセス成功 • 監査ログ統計データへのアクセス失敗 統計パターンデータへのアクセスに関して，次に示す記録を出力します。 • 統計パターンデータの取得または更新成功 • 統計パターンデータの取得または更新失敗
5	AnomalyEvent	しきい値オーバーなどの異常が発生したことを示す事象です。	監査ログファイルの出力に関して，次に示す記録を出力します。 • ラップアラウンド

付録 D.2　監査ログの保存形式

監査ログの保存形式について，次に示す場合に分けて説明します。

- JP1/Audit Management - Manager（サーバ）
- JP1/Audit Management - Manager の監査ログ管理画面（Web）

(1)　JP1/Audit Management - Manager（サーバ）の場合

監査ログは，監査ログファイル（admauditlog.log）に出力されます。監査ログファイルは，シーケンシャルファイルです。

監査ログファイルが一定の容量に達すると，ファイル名を変更して保存したあと，変更前と同じ名称のファイルを作成して新たにログを書き込みます。一定の容量に達して監査ログファイルが切り替わる際，admauditlog.log を，admauditlog1.log に変更して保存し，新たに admauditlog.log を作成して，ログを書き込みます。再び admauditlog.log が一定量に達すると，保存済みの admauditlog1.log を admauditlog2.log に変更したあと，admauditlog.log を admauditlog1.log に変更して保存します。

このように，保存済みのログファイルは，新たにファイルが作成されるごとにファイル名末尾の数値+1 をしたファイル名称に変更されます。つまり，数値が大きいログファイルほど古いログファイルとなります。なお，ファイル数が設定値を超えると，古いログファイルから削除されます。

監査ログの出力の有無，ファイルサイズ，およびファイル数は，JP1/Audit Management - Manager のセットアップで変更できます。監査ログファイルサイズのデフォルト値は 5 メガバイトです。監査ログファイル数のデフォルト値は 10 です。監査ログ出力の設定方法については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

(2)　JP1/Audit Management - Manager の監査ログ管理画面（Web）の場合

監査ログは，監査ログファイル（admwauditlogn.log）に出力されます。監査ログファイルは，シーケンシャルファイルです。

監査ログが最初に出力されるときに，admwauditlog1.log を作成してログを書き込みます。監査ログファイルが一定の容量に達すると，admwauditlog1.log を保存したあと，admwauditlog2.log を作成してログを書き込みます。このように，ファイル名末尾の数値+1 をしたファイル名称のファイルを作成して新たにログを書き込む動作が，監査ログファイル数まで繰り返されます。ファイル数が設定値を超えると，古いログファイルから上書き保存されます。

監査ログの出力の有無，ファイルサイズ，およびファイル数は，JP1/Audit Management - Manager のセットアップで変更できます。ログファイルサイズのデフォルト値は 5 メガバイトです。監査ログファイル数のデフォルト値は 10 です。監査ログ出力の設定方法については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

付録 D.3　監査ログの出力形式

監査ログの出力形式，出力先，出力項目，および出力例について説明します。

(1)　監査ログの出力形式

監査ログの出力形式は，監査ログのフォーマットであることを示す「CALFHM」，監査ログのリビジョン番号，該当する出力項目の順で出力されます。

なお，この情報は，JP1/Audit Management - Manager（サーバ）と JP1/Audit Management - Manager の監査ログ管理画面（Web）の共通情報です。

監査ログの出力形式を次に示します。

```
CALFHM X.X，出力項目1＝値1，出力項目2＝値2，・・・，出力項目n＝値n
```

(2)　監査ログの出力先

監査ログは，次に示すフォルダに出力されます。

```
JP1/Audit Management - Managerのインストール先フォルダ¥log
```

なお，クラスタ環境での運用時でも，共有ディスクに格納された監査ログは，収集対象にはなりません。各プログラムの監査ログは，ローカルディスクに出力するように設定しておく必要があります。

(3)　出力項目

出力項目は，共通出力項目と固有出力項目の 2 種類あります。それぞれについて説明します。

なお，この情報は，JP1/Audit Management - Manager（サーバ）と JP1/Audit Management - Manager の監査ログ管理画面（Web）の共通情報です。

- 共通出力項目
  監査ログを出力する日立オープンミドルウェア製品で共通して出力される項目です。
- 固有出力項目
  監査ログを出力する日立オープンミドルウェア製品ごとに，出力される項目です。

(a)　共通出力項目

共通出力項目に出力される値および内容を次の表に示します。

表 D-2　監査ログの共通出力項目

項番	出力項目		値	内容
	項目名	出力される属性名		
1	共通仕様識別子	−	「CALFHM」	監査ログのフォーマットであることを示す識別子です。
2	共通仕様リビジョン番号	−	X.X	監査ログを管理するためのリビジョン番号です。
3	通番	seqnum	通番	監査ログの通し番号です。
4	メッセージ ID	msgid	KDSOnnnn-x	製品ごとのメッセージ ID です。メッセージについては「14.3　メッセージ一覧」を参照してください。
5	日付・時刻	date	YYYY-MM-DDThh:mm:ss.tttTZD※1	監査ログの取得日時およびタイムゾーンです。
6	発生プログラム名	progid	「JP1/NETM/Audit」	事象が発生したプログラム名です。
7	発生コンポーネント名	compid	• CollectManager（監査ログ収集マネージャ） • Collector（監査ログ収集コンポーネント） • Command（コマンド） • DatabaseManager（データベースマネージャ） • ManagerConvert（正規化ルールエディタ） • ManagerSetup（マネージャセットアップ画面） • WebView（監査ログ管理画面）	事象が発生したコンポーネント名です。
8	発生プロセス ID	pid	プロセス ID	事象が発生を検出したプロセスの ID です。
9	発生場所	ocp:ipv4	IPv4 形式（xxx.xxx.xxx.xxx）	事象が発生したホストの IP アドレスです。なお，ホストの IP アドレスを取得できない場合は，「-」（ハイフン）が出力されます。
		ocp:ipv6	IPv6 形式	
		ocp:host	ホスト名	事象が発生したホスト名です。
10	事象の種別	ctgry	• StartStop • Authentication • ConfigurationAccess • ContentAccess • AnomalyEvent	監査ログに出力される事象を分類するための識別子です。事象の種別の詳細については，表 D-1 を参照してください。
11	事象の結果	result	• Success（成功）	発生した事象の結果です。

項番	出力項目		値	内容
	項目名	出力される属性名		
			• Failure（失敗） • Occurrence（成功または失敗の分類がない事象の発生）	
12	サブジェクト識別情報※2	subj:uid	JP1 ユーザ	事象を発生させたユーザの情報です。
		subj:euid	OS ユーザ	

（凡例）

－：属性名の出力なし

注※1

YYYY は年，MM は月，DD は日，hh は時間，mm は分，ss は秒，ttt はミリ秒です。

T は日付と時刻の区切りです。

TZD はタイムゾーン指定子です。次のどれかが出力されます。

+hh:mm：UTC（協定世界時）から hh:mm だけ進んでいることを示す。

-hh:mm：UTC（協定世界時）から hh:mm だけ遅れていることを示す。

Z：UTC（協定世界時）と同じであることを示す。

注※2

事象がユーザに関連しない場合またはユーザ管理の機能を使用しない場合は，プロセス ID が出力されます。

(b) 固有出力項目

固有出力項目に出力される値および内容を次の表に示します。

表 D–3 監査ログの固有出力項目

項番	出力項目		値	内容
	項目名	出力される属性名		
1	オブジェクト情報	obj	• [DB]AuditLogInfo（JP1/Audit Management - Manager が蓄積した監査ログ） • [DB]StatisticsValueInfo（監査ログの統計） • [DB]BackupHistoryInfo（監査ログのバックアップ履歴） • [DB]Database（データベース） • [DB]StatisticsPatternInfo（統計パターン）	事象を発生させたデータベースに関するオブジェクト名です。なお，値に該当しない動作の情報は，出力されません。
			• [File]AuditLog（JP1/Audit Management - Manager のログファイル）	事象を発生させたファイルに関するオブジェクト名です。なお，値に該当しない動作の情報は，出力されません。

項番	出力項目		値	内容
	項目名	出力される属性名		
			• [File]BackupData（バックアップファイル） • [File]Config（Config ファイル） • [File]CSV（CSV 形式ファイル） • [File]HTML（HTML 形式ファイル） • [File]PDF（PDF ファイル）	
			• [User]DB（データベースのログイン ID） • [User]JP1（JP1 ユーザ）	事象を発生させたユーザ情報に関するオブジェクト名です。なお，値に該当しない動作の情報は，出力されません。
2	動作情報	op	• Start（開始） • Stop（停止） • Login（ログイン） • Logout（ログアウト） • Refer（参照） • Add（追加） • Update（作成・更新） • Delete（削除）	事象を発生させたユーザの動作の情報です。なお，値に該当しない動作の情報は，出力されません。
3	権限情報	auth	• JP1 権限 • OS 権限	事象を発生させたユーザの権限です。なお，値に該当しない動作の情報は，出力されません。
4	リクエスト送信元ホスト	from:ipv4	IPv4 形式（xxx.xxx.xxx.xxx）	クライアントの IP アドレス（Web ブラウザを操作しているクライアント）です。なお，値に該当しない動作の情報は，出力されません。 また，固有情報の場合や値がない場合は「出力される属性名」も出力されません。
		from:ipv6	IPv6 形式	
5	メッセージ	msg	任意のメッセージ	事象の内容を示すメッセージです。

(4) 監査ログの出力例

監査ログの出力例を次に示します。

```
CALFHM 1.0, seqnum=1, msgid=KDSO2001-I, date=2007-03-01T20:49:54.912+09:00,
progid=JP1/NETM/Audit, compid=ManagerSetup, pid=1234, ocp:host=Hostname,
ctgry=ConfigurationAccess, result=Success, subj:euid=Administrator,
obj=[File]Config, op=Update, auth=Administrator, msg="環境設定に成功しました。"
```

付録 D.4　監査ログを出力するための設定

監査ログを出力するために，監査ログの出力の有無，監査ログファイルサイズ，監査ログファイル数の設定が必要です。監査ログを出力するための設定を次に示します。

(1)　JP1/Audit Management - Manager（サーバ）の場合

［マネージャセットアップ］ダイアログの「監査ログ情報」の各項目を設定します。

- 「監査ログファイル出力」を「出力する」にします。デフォルトは「出力しない」です。
- 「監査ログファイルサイズ」を必要に応じて変更します。デフォルトは 5 メガバイトです。
- 「監査ログファイル数」を必要に応じて変更します。デフォルトは 10 です。

監査ログ出力の設定方法については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

(2)　JP1/Audit Management - Manager の監査ログ管理画面（Web）の場合

JP1/Audit Management - Manager の監査ログ管理画面（Web）の監査ログを出力するには，監査ログの出力の有無，監査ログファイルサイズ，監査ログファイル数の設定が必要です。監査ログを出力するための設定を次に示します。

［マネージャセットアップ］ダイアログの「監査ログ管理画面監査ログ情報」の各項目を設定します。

- 「監査ログファイル出力」を「出力する」にします。デフォルトは「出力しない」です。
- 「監査ログファイルサイズ」を必要に応じて変更します。デフォルトは 5 メガバイトです。
- 「監査ログファイル数」を必要に応じて変更します。デフォルトは 10 です。

なお，設定値を変更した場合は，World Wide Web Publishing Service サービスを再起動してください。

監査ログ出力の設定方法については「5.5.6　監査ログ管理サーバの環境設定をする」を参照してください。

付録 E　JP1/Audit Management - Manager が対応するプログラムの監査ログ一覧

ここでは，JP1/Audit Management - Manager が対応しているプログラムの監査ログ一覧を次の表に示します。

表 E-1　JP1/Audit Management - Manager が対応しているプログラムの監査ログ一覧

項番	プログラム名	プラットフォーム	監査ログの出力先※1	ファイル名
1	Collaboration	Windows	ユーザ任意	• ポートレット，コマンド用 Collabo_portlet1.log～ Collabo_portlet32.log • Web フォルダ用 Collabo_Filesharing_Webdav1.log～ Collabo_Filesharing_Webdav32.log
2	Cosminexus	Windows	ユーザ任意	audit1.log～ audit4.log※2
		UNIX		
3	HiRDB	Windows	HiRDB 運用フォルダ¥auditlog※3	• auditmsg1.log • auditmsg2.log
		UNIX	HiRDB 運用ディレクトリ/auditlog※3	
4	Hitachi Navigation Platform	Windows	Hitachi Navigation Platform のインストール先フォルダ¥auditlog	ucnp_audit1.log～ ucnp_audit32.log
5	Hitachi Storage Command Suite または Hitachi Command Suite	Windows	Windows イベントログ（アプリケーション）	－
		HP-UX	ユーザ任意	syslog.log※4
		Solaris		messages※4
		AIX		syslog.out※4
		Linux		messages※4
6	JP1/AJS2	Windows	JP1/AJS2 のインストール先フォルダ¥log	ajs-log1.log～ajs-log2.log※5
		UNIX	/var/opt/jp1ajs2/log/	

項番	プログラム名	プラットフォーム	監査ログの出力先※1	ファイル名
7	JP1/AJS3※6	Windows	物理ホストの場合 JP1/AJS3 のインストール先フォルダ¥log 論理ホストの場合 論理ディスクパス¥log	物理ホスト用および論理ホスト用 • ajs-host-log1.log※5 • ajs-host-log2.log※5
			物理ホストの場合 JP1/AJS3 のインストール先フォルダ¥log¥schedule¥スケジューラサービス名 論理ホストの場合 論理ディスクパス¥log¥schedule¥スケジューラサービス名	スケジューラサービス用 • ajs-log1.log※5 • ajs-log2.log※5
		UNIX	物理ホストの場合 /var/opt/jp1ajs3/log 論理ホストの場合 論理ディスクパス/log	物理ホスト用および論理ホスト用 • ajs-host-log1.log※5 • ajs-host-log2.log※5
			物理ホストの場合 /var/opt/jp1ajs3/log/schedule/スケジューラサービス名 論理ホストの場合 論理ディスクパス/log/schedule/スケジューラサービス名	スケジューラサービス用 • ajs-log1.log※5 • ajs-log2.log※5
8	JP1/AO	Windows	JP1/AO のインストール先フォルダ¥logs	Audit1.log～Audit16.log※2
		Linux	/var/opt/jp1ao/logs	
9	JP1/Base	Windows	JP1/Base のインストール先フォルダ¥log¥BASE	base_log.log
		UNIX	/var/opt/jp1base/log/BASE	
10	JP1/IM - NP	Windows	JP1/IM - NP のインストール先フォルダ¥auditlog	ucnp_audit1.log～ucnp_audit32.log※2

項番	プログラム名		プラットフォーム	監査ログの出力先※1	ファイル名
11	JP1/IM - SS または JP1/SS		Windows	JP1/IM - SS のインストール先フォルダ¥log¥access	jp1imssaccesslog1.log ～ jp1imssaccesslog32.log※2
12	JP1/ITDM		Windows	JP1/ITDM のインストール先フォルダ¥mgr¥logs	JDNAUDT1.log～JDNAUDT9.log
13	JP1/ITDM2	JP1/ITDM2 - Manager	Windows	JP1/ITDM2 のインストール先フォルダ¥mgr¥logs	JDNAUDT1.log～JDNAUDT9.log NETMAuditManager.LOG
		JP1/ITDM2 - Agent	Windows	ユーザ任意	NETMAuditManager.LOG
		JP1/ITDM2 - Asset Console	Windows	JP1/ITDM2 のインストール先フォルダ¥auditlog	ASTAUDIT01.LOG～ASTAUDIT09.LOG
14	JP1/ITRM		Windows	JP1/ITRM のインストールフォルダ¥JP1ITRM¥logs※3	Auditlog1.log～Auditlog10.log※2
15	JP1/Audit	JP1/Audit Management - Manager (サーバ)	Windows	JP1/Audit Management - Manager のインストール先フォルダ¥log	almauditlog.log
		JP1/Audit Management - Manager の監査ログ管理画面 (Web)	Windows	JP1/Audit Management - Manager のインストール先フォルダ¥log	admwauditlog1.log～admwauditlog10.log※2
16	JP1/NETM/AIM		Windows	JP1/NETM/AIM のインストール先フォルダ¥auditlog	ASTAUDIT01.LOG～ASTAUDIT09.LOG
17	JP1/NETM/CSC	JP1/NETM/CSC - Agent	Windows	JP1/NETM/CSC - Agent のインストール先フォルダ¥log	jp1netmcscaauditlog.log
		JP1/NETM/CSC - Manager		JP1/NETM/CSC - Manager のインストール先フォルダ¥log	jp1netmcscmauditlog.log
		JP1/NETM/CSC - Manager - Remote Option		JP1/NETM/CSC - Manager - Remote Option のインストール先フォルダ¥log	jp1netmcscmrauditlog.log

項番	プログラム名		プラットフォーム	監査ログの出力先※1	ファイル名
18	JP1/NETM/DM	JP1/NETM/DM Manager※7	Windows	ユーザ任意	NETMAuditManager.LOG
		JP1/NETM/DM Client※7			
		JP1/NETM/DM Client - Base※7			
19	JP1/NETM/NM		Windows	ユーザ任意	nmmwebconsoleauditlog.log
20	JP1/PFM	JP1/PFM	Windows	JP1/PFM のインストール先フォルダ¥auditlog	jpcaudit.log
			UNIX	/opt/jp1pc/auditlog	
		JP1/PFM - Base	Windows	JP1/PFM - Base のインストール先フォルダ¥auditlog	
			UNIX	/opt/jp1pc/auditlog	
21	OpenTP1		Windows	ユーザ任意	audit.log
			HP-UX		
			AIX		
			Linux		
22	JP1/秘文		Windows	ユーザ任意	• sfAdtWatch1.log • sfAdtWatch2.log
23	Oracle		Windows	Windows イベントログ（アプリケーション）	−
24	TRUST E2		VOS3	ユーザ任意	V3TRUST.LOG※8
25	uCosminexus EUR Server		Windows	uCosminexus EUR Server のインストール先フォルダ¥log	eur_spool_audit.log
			UNIX/Linux	/var/opt/eur/log	
26	uCosminexus Navigation Platform		Windows	uCosminexus Navigation Platform のインストール先フォルダ¥auditlog	ucnp_audit1.log～ucnp_audit32.log※2

項番	プログラム名	プラットフォーム	監査ログの出力先※1	ファイル名
27	uCosminexus Portal Framework	Windows	ユーザ任意	audit1.log～audit4.log※2
		Linux		
28	UNIX システムログ	UNIX	/var/opt/jp1netmaudit/agent/log 注 JP1/NETM/Audit - Manager V8 からバージョンアップしている場合 /opt/jp1netmaudit/manager/log	• login.1～login.2 • loginfailed.1～loginfailed.2 • sulog.1～sulog.2
29	Windows イベントログ	Windows	セキュリティ	－
30	XDM/BASE E2	VOS3	ユーザ任意	• BASE.log※8 • SD.log※8 • DCCM3.log※8 • DBS.log※8 • RD.log※8
31	活文 NAVIstaff	Windows	ユーザ任意	• NAVIstaffAuditLog.csv

（凡例）

－：該当なし

注※1

クラスタ環境での運用時でも，共有ディスクに格納された監査ログは，収集対象にはなりません。各プログラムの監査ログを，ローカルディスクに出力するように設定してください。

注※2

デフォルト値の場合です。設定によってログ面数を変更できます。

- Cosminexus の場合は，ログ面数を 2～32 に変更できます。
- JP1/AO の場合は，ログ面数を 1～16 に変更できます。デフォルトは 7 です。
- JP1/IM - NP と uCosminexus Navigation Platform の場合は，ログ面数を 1～32 に変更できます。デフォルトは 16 です。
- JP1/IM - SS または JP1/SS の場合は，ログ面数を 1～32 に変更できます。デフォルトは 24 です。
- JP1/ITRM の場合は，ログ面数を 1～16 に変更できます。デフォルトは 10 です。
- JP1/Audit の監査ログ管理画面（Web）の場合は，ログ面数を 1～32 に変更できます。
- uCosminexus Portal Framework の場合は，ログ面数を 1～32 に変更できます。

ログ面数を変更するとファイル名も合わせて変更されます。ログ面数を変更した場合には，製品定義ファイルで指定している監査ログファイル名を変更する必要があります。製品定義ファイルについては「13.3　製品定義ファイル」を参照してください。

注※3

HiRDB および JP1/ITRM の監査ログの出力先フォルダはユーザが任意で指定できます。詳細については，HiRDB または JP1/ITRM のマニュアルを参照してください。

注※4

syslog の出力ファイルを変更している場合には，**JP1/Audit Management - Manager のインストール先フォルダ**¥conf¥product にある製品定義ファイル内のログファイル名称指定（AuditLogName）の値を変更する必要があります。

該当する製品定義ファイルを次に示します。

- HitachiStorageCommandSuite(HP-UX).conf
- HitachiStorageCommandSuite(Solaris).conf
- HitachiStorageCommandSuite(AIX).conf
- HitachiStorageCommandSuite(Linux).conf

製品定義ファイルについては「13.3　製品定義ファイル」を参照してください。

注※5

スケジューラログファイル名は「**JP1/Audit Management - Manager のインストール先フォルダ**¥conf¥product」にある製品定義ファイル内のログファイル名称指定（AuditLogName）の値と一致させる必要があります。詳細については「5.6.1　標準サポートしているプログラムを収集対象とするための準備をする」を参照してください。

JP1/AJS2 と JP1/AJS3 のそれぞれについて，該当する製品定義ファイルを次に示します。

JP1/AJS2 の場合

- JP1_AJS2.conf

JP1/AJS3 の場合

- JP1_AJS3-host.conf
- JP1_AJS3-schedule01.conf～JP1_AJS3-schedule20.conf

製品定義ファイルについては「13.3　製品定義ファイル」を参照してください。

注※6

JP1/AJS2 から JP1/AJS3 にバージョンアップした場合は，収集対象とするプログラムも JP1/AJS3 に変更してください。監査ログ収集対象の設定変更については「9.3　監査ログの収集対象の設定変更」を参照してください。

注※7

監査ログ収集マネージャの［収集対象の設定］ダイアログで，JP1/NETM/DM を収集対象として追加する際に，JP1/NETM/DM Client（または JP1/NETM/DM Client - Base）と JP1/NETM/DM Manager が同一マシンにインストールされている場合には，「プログラム」に「JP1/NETM/DM」を

指定してください。JP1/NETM/DM Client（または JP1/NETM/DM Client - Base）と JP1/NETM/DM Manager を別のマシンにインストールしている場合には，「プログラム」にそれぞれ「JP1/NETM/DM-Client」，「JP1/NETM/DM-Manager」を指定してください。

注※8

TRUST E2 や XDM/BASE E2 の監査ログを収集するには，ファイル転送プログラムなどを使用して，該当するファイルを VOS3 から監査ログ収集対象サーバに転送する必要があります。

転送方法の詳細については，TRUST E2 や XDM/BASE E2 のマニュアルを参照してください。

ファイルの格納先やファイル名は任意で指定できますが，ファイル名については「JP1/Audit Management - Manager のインストール先フォルダ¥conf¥product」にある製品定義ファイル内のログファイル名称指定（AuditLogName）の値と一致させる必要があります。したがって，ファイル名は転送するたびに変更しないでください。詳細については「5.6.1　標準サポートしているプログラムを収集対象とするための準備をする」を参照してください。

TRUST E2 と XDM/BASE E2 のそれぞれについて，該当する製品定義ファイルを次に示します。

TRUST E2 の場合

- VOS3_TRUST.conf

XDM/BASE E2 の場合

- XDM.conf

製品定義ファイルについては「13.3　製品定義ファイル」を参照してください。

このあと，次に示す監査ログの出力情報について説明します。

- Hitachi Storage Command Suite のログ
- JP1/AJS のスケジューラログ
- Oracle のログ
- UNIX システムログ
- Windows イベントログ（セキュリティ）

その他の JP1/Audit Management - Manager が標準サポートしている監査ログの出力情報については，各製品のマニュアルに記載されている監査ログの出力情報を参照してください。

付録 E.1　Hitachi Storage Command Suite の監査ログ出力情報

ここでは，Hitachi Storage Command Suite の監査ログ出力情報を次の表に示します。

表 E-2　Hitachi Storage Command Suite の監査ログ出力情報

項番	項目名		値
1	共通部※1	監査ログ ID	通番※2

項番	項目名		値
		メッセージ ID	**メッセージ ID**
		日時	**日時**
		プログラム名	Hitachi Storage Command Suite
		コンポーネント名	**検出エンティティ**
		プロセス ID	-1
		発生場所	**検出場所**
		監査事象種別	**監査事象の種別**
		監査事象結果	**監査事象の結果**
		サブジェクト種別	**サブジェクト識別情報**（uid=，pid=）※3
		サブジェクト情報	
2	固有部※4	obj	**ハードウェア識別情報**
		objloc	**ハードウェアコンポーネント識別情報**
		sins	**アプリケーション識別**
		loc	**ロケーション識別情報**
		haid	**冗長化識別情報**
		agent※5	**エージェントプログラム動作場所**（agent=）
		from※5	**リクエスト送信元ホスト**（from=）
		from:port	**リクエスト送信元ポート**
		to※5	**リクエスト送信先ホスト**（to=）
		to:port	**リクエスト送信先ポート**
		batid	**一括操作識別子**
		logtype	**ログ種別情報**
		subjp※5	• **サブジェクト識別情報**（hostname=，ipv4=，ipv6=，wwn=，isn=）※6 • **完全修飾ドメイン名**※7
		msg	**任意のメッセージ**

注※1

該当する値がない場合，監査ログ管理画面では空欄となります。

注※2

値が 0 の場合，監査ログ管理画面では空欄となります。

注※3

サブジェクト識別情報のうち，「uid=」，「pid=」，および値（system など）だけの情報は，サブジェクト情報として出力されます。

注※4

該当する値がない場合は出力されません。

注※5

「host」,「ipv4」,「ipv6」,または「wwn」などのサブタグが付いて出力されます。

注※6

サブジェクト識別情報のうち,「hostname=」,「ipv4=」,「ipv6=」,「wwn=」,または「isn=」の値が出力されます。なお,サブジェクト識別情報が subjp として出力された場合,サブジェクト情報は監査ログ管理画面では空欄となります。

注※7

完全修飾ドメイン名は,「fqdn」のサブタグが付いて出力されます。

付録 E.2　JP1/AJS2 および JP1/AJS3 の監査ログ（スケジューラログ）出力情報

ここでは,JP1/AJS2 および JP1/AJS3 の監査ログ（スケジューラログ）出力情報について説明します。

(1)　JP1/AJS2 の監査ログ（スケジューラログ）出力情報

JP1/AJS2 の監査ログ（スケジューラログ）出力情報を次の表に示します。

表 E–3　JP1/AJS2 の監査ログ（スケジューラログ）出力情報

項番	JP1/AJS2 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
1	A001	スケジューラサービス開始	KAVS0200-I	A	C	G	値なし	値なし
2	A002	スケジューラサービス終了	KAVS0201-I	A	C	G	値なし	値なし
3	A003	スケジューラサービスプロセス異常終了	KAVS0204-E	A	C	H	値なし	値なし
4	A007	JP1/AJS2 - View の接続	KAVS0534-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
5	A008	JP1/AJS2 - View の接続終了	KAVS0535-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
6	A009	JP1/AJS2 - SO の接続	KAVS0536-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
7	A010	JP1/AJS2 - SO の接続終了	KAVS0537-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS2 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
8	A011	スケジューラログ出力プロセス起動	KAVS0220-I	A	C	G	値なし	値なし
9	A012	スケジューラログ出力プロセス停止	KAVS0221-I	A	C	G	値なし	値なし
10	A013	認証（ログイン・ユーザマッピング）の拒否	KAVS1009-W	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
11	N001	ジョブネット開始	KAVS0260-I	A	C	G	値なし	値なし
12	N002	ジョブネット正常終了	KAVS0261-I	A	C	G	値なし	値なし
13	N003	ジョブネット異常終了	KAVS0262-E	A	C	H	値なし	値なし
14	N004	ジョブネット警告終了	KAVS0268-W	A	C	I	値なし	値なし
15	N005	ジョブネット保留	KAVS0270-I	A	C	I	値なし	値なし
16	N006	ジョブネット閉塞	KAVS0272-E	A	C	H	値なし	値なし
17	N007	ジョブネット閉塞	KAVS0273-E	A	C	H	値なし	値なし
18	N008	ジョブネット開始遅延	KAVS0275-I	A	C	I	値なし	値なし
19	N009	ジョブネット終了遅延	KAVS0276-I	A	C	I	値なし	値なし
20	N010	次回予定キューイング	KAVS0277-I	A	C	I	値なし	値なし
21	N011	ジョブネット起動条件監視開始	KAVS0240-I	A	C	G	値なし	値なし
22	N012	ジョブネット起動条件監視終了	KAVS0241-I	A	C	G	値なし	値なし
23	N013	ジョブネット繰り越し未実行	KAVS0279-E	A	C	H	値なし	値なし
24	N014	ジョブネット全登録解除	KAVS0267-I	A	C	I	値なし	値なし

項番	JP1/AJS2 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
25	J001	ジョブ開始	KAVS0263-I	A	C	G	値なし	値なし
26	J002	ジョブ正常終了	KAVS0264-I	A	C	G	値なし	値なし
27	J003	ジョブ異常終了	KAVS0265-E	A	C	H	値なし	値なし
28	J004	ジョブ警告終了	KAVS0269-W	A	C	I	値なし	値なし
29	J005	ジョブ保留	KAVS0271-I	A	C	I	値なし	値なし
30	J006	ジョブサブミット開始	KAVS0278-I	A	C	G	値なし	値なし
31	J007	イベントジョブ実行要求開始	KAVS0242-I	A	C	G	値なし	値なし
32	J008	ジョブ終了遅延	KAVS0248-I	A	C	I	値なし	値なし
33	C001	サービスの運用環境の一時的な変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
34	C002	サービスの停止	「0」または操作結果対応メッセージ ID	A	C	J	ユーザ ID または値なし	ユーザ ID または値なし
35	C003	サービスの起動	「0」または操作結果対応メッセージ ID	A	C	J	ユーザ ID または値なし	ユーザ ID または値なし
36	C101	ジョブネットの登録	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
37	C102	ジョブネットの登録の取り消し	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS2 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
38	C103	ジョブネットの一時変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
39	C104	ジョブネットの実行の中断	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
40	C105	ジョブネットの再実行	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
41	C106	ジョブネットのサスペンド/サスペンド解除	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
42	C107	登録予定情報のインポート	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
43	C108	登録予定情報のインポートによるジョブネットの登録	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
44	C201	ジョブネット・ジョブの強制終了	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
45	C202	ジョブの状態変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
46	C301	ユニットの定義内容変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
47	C302	ユニットの削除	「0」または操作結果対	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS2 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
			応メッセージ ID					
48	C303	ユニットの回復	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
49	C304	ユニットの作成	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
50	C305	ユニットの複写,移動	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
51	C306	ユニットのインポート	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
52	C401	カレンダーの変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
53	C502	ユニットの状態表示	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
54	C503	ユニットの定義内容出力	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
55	C504	ユニットの定義内容退避	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
56	C506	ユニットの予定情報出力	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
57	C507	ユニットの名称出力	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
58	C508	ユニットのエクスポート	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS2 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
59	C509	ユニットの状態表示（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
60	C510	ユニットの定義内容出力（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
61	C511	ユニットの定義内容の退避（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
62	C512	ユニット名称の出力（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
63	C513	登録予定情報のエクスポート	操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
64	C514	登録予定情報のエクスポートによるジョブネットの情報出力	操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
65	I001	コマンド該当処理開始	－	A	F	G	ユーザ ID または値なし	ユーザ ID または値なし
66	I002	コマンドからサービスへの処理要求開始	－	A	F	G	ユーザ ID または値なし	ユーザ ID または値なし

（凡例）

－：該当なし

A：**取得元サーバ名**（発生場所）

B：**ログ中のホスト名**（発生場所）

C：StartStop（監査事象種別）

D：ExternalService（監査事象種別）

E：ConfigurationAccess（監査事象種別）

F：AccessControl（監査事象種別）

G：Success（監査事象結果）

H：Failure（監査事象結果）

I：Occurrence（監査事象結果）

J：次のどれかになります（監査事象結果）。

-E：Failure

0：Success

上記以外：Occurrence

K：次のどちらかになります（監査事象結果）。

-E：Failure
上記以外：Occurrence

なお，次の表に示す項目は JP1/AJS2 のすべてのログ種別で共通です。

表 E-4　JP1/AJS2 の監査ログ（スケジューラログ）出力情報の共通項目

共通部					固有部
監査ログ ID	日時	プログラム名	コンポーネント名	プロセス ID	固有情報
0	ログ中の値	JP1/AJS2	SchedulerLog	ログにあれば利用	ログをそのまま出力

注意事項

JP1/AJS2 のスケジューラログでは，年の情報が出力されていない場合があります。この場合，次の方法で年の情報を追加して正規化します。

- ログ中の月＜＝ログ取得の月：「取得した時点の年」の情報追加
- ログ中の月＞ログ取得の月：「取得した時点の年 - 1」の情報追加

例えば，ログ中の月が 12 月で，2007 年 1 月に取得した場合，2006 年 12 月として情報が追加されます。

(2)　JP1/AJS3 の監査ログ（スケジューラログ）出力情報

JP1/AJS3 の監査ログ（スケジューラログ）出力情報を次の表に示します。

表 E-5　JP1/AJS3 の監査ログ（スケジューラログ）出力情報

項番	JP1/AJS3 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
1	A001	スケジューラサービス開始	KAVS0200-I	A	C	G	値なし	値なし
2	A002	スケジューラサービス終了	KAVS0201-I	A	C	G	値なし	値なし
3	A003	スケジューラサービスプロセス異常終了	KAVS0204-E	A	C	H	値なし	値なし
4	A007	JP1/AJS3 - View の接続※1	KAVS0534-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
5	A008	JP1/AJS3 - View の接続終了※2	KAVS0535-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS3 の スケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
6	A009	JP1/AJS2 - SO の接続	KAVS0536-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
7	A010	JP1/AJS2 - SO の接続終了	KAVS0537-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
8	A011	スケジューラログ出力プロセス起動	KAVS0220-I	A	C	G	値なし	値なし
9	A012	スケジューラログ出力プロセス停止	KAVS0221-I	A	C	G	値なし	値なし
10	A013	認証（ログイン・ユーザマッピング）の拒否	KAVS1009-W	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
11	A014	JP1/AJS3 - Software Development Kit の接続	KAVS0564-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
12	A015	JP1/AJS3 - Software Development Kit の接続終了	KAVS0565-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
13	A016	Manager 用接続元制限機能による接続拒否	KAVS8040-E	A	D	H	ユーザ ID または値なし	ユーザ ID または値なし
14	A017	JP1/AJS3 - Web Console の接続	KAVS0570-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
15	A018	JP1/AJS3 - Web Console の接続終了	KAVS0571-I	A	D	G	ユーザ ID または値なし	ユーザ ID または値なし
16	N001	ジョブネット開始	KAVS0260-I	A	C	G	値なし	値なし
17	N002	ジョブネット正常終了	KAVS0261-I	A	C	G	値なし	値なし
18	N003	ジョブネット異常終了	KAVS0262-E	A	C	H	値なし	値なし
19	N004	ジョブネット警告終了	KAVS0268-W	A	C	I	値なし	値なし

項番	JP1/AJS3 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
20	N005	ジョブネット保留	KAVS0270-I	A	C	I	値なし	値なし
21	N006	ジョブネット閉塞	KAVS0272-E	A	C	H	値なし	値なし
22	N007	ジョブネット閉塞	KAVS0273-E	A	C	H	値なし	値なし
23	N008	ジョブネット開始遅延	KAVS0275-I	A	C	I	値なし	値なし
24	N009	ジョブネット終了遅延	KAVS0276-I	A	C	I	値なし	値なし
25	N010	次回予定キューイング	KAVS0277-I	A	C	I	値なし	値なし
26	N011	ジョブネット起動条件監視開始	KAVS0240-I	A	C	G	値なし	値なし
27	N012	ジョブネット起動条件監視終了	KAVS0241-I	A	C	G	値なし	値なし
28	N013	ジョブネット繰り越し未実行	KAVS0279-E	A	C	H	値なし	値なし
29	N014	ジョブネット全登録解除	KAVS0267-I	A	C	I	値なし	値なし
30	N015	起動条件監視終了待ち	KAVS1420-I	A	C	I	値なし	値なし
31	N016	ジョブネットの待ち合わせ条件による待ち合わせの開始	KAVS4950-I	A	C	G	値なし	値なし
32	N017	ジョブネットの待ち合わせ条件の成立	KAVS4955-I	A	C	G	値なし	値なし
33	N018	ジョブネットの待ち合わせ条件による待ち合わせの滞留	KAVS4957-E	A	C	I	値なし	値なし
34	J001	ジョブ開始	KAVS0263-I	A	C	G	値なし	値なし
35	J002	ジョブ正常終了	KAVS0264-I	A	C	G	値なし	値なし

項番	JP1/AJS3 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
36	J003	ジョブ異常終了	KAVS0265-E	A	C	H	値なし	値なし
37	J004	ジョブ警告終了	KAVS0269-W	A	C	I	値なし	値なし
38	J005	ジョブ保留	KAVS0271-I	A	C	I	値なし	値なし
39	J006	ジョブサブミット開始	KAVS0278-I	A	C	G	値なし	値なし
40	J007	イベントジョブ実行要求開始	KAVS0242-I	A	C	G	値なし	値なし
41	J008	ジョブ終了遅延	KAVS0248-I	A	C	I	値なし	値なし
42	J009	ジョブのキューイング取り消し	KAVS0266-I	A	C	I	値なし	値なし
43	J010	ジョブの待ち合わせ条件による待ち合わせの開始	KAVS4951-I	A	C	G	値なし	値なし
44	J011	ジョブの待ち合わせ条件の成立	KAVS4956-I	A	C	G	値なし	値なし
45	J012	ジョブの待ち合わせ条件による待ち合わせの滞留	KAVS4971-E	A	C	I	値なし	値なし
46	J013	異常終了時の自動リトライによる間隔待ちの開始	KAVS4675-I	A	C	G	値なし	値なし
47	J014	異常終了時の自動リトライによるジョブ開始	KAVS4676-I	A	C	G	値なし	値なし
48	J015	異常終了時の自動リトライの終了	KAVS4677-E	A	C	I	値なし	値なし
49	J016	異常終了時の自動リトライによるジョブサブミット開始	KAVS4678-I	A	C	G	値なし	値なし
50	C001	サービスの運用環境の一時的な変更	「0」または操作結果対	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS3 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
			応メッセージ ID					
51	C002	サービスの停止	「0」または操作結果対応メッセージ ID	A	C	J	ユーザ ID または値なし	ユーザ ID または値なし
52	C003	サービスの起動	「0」または操作結果対応メッセージ ID	A	C	J	ユーザ ID または値なし	ユーザ ID または値なし
53	C101	ジョブネットの登録	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
54	C102	ジョブネットの登録の取り消し	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
55	C103	ジョブネットの一時変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
56	C104	ジョブネットの実行の中断	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
57	C105	ジョブネットの再実行	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
58	C106	ジョブネットのサスペンド/サスペンド解除	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
59	C107	登録予定情報のインポート	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS3 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
60	C108	登録予定情報のインポートによるジョブネットの登録	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
61	C201	ジョブネット・ジョブの強制終了	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
62	C202	ジョブの状態変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
63	C301	ユニットの定義内容変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
64	C302	ユニットの削除	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
65	C303	ユニットの回復	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
66	C304	ユニットの作成	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
67	C305	ユニットの複写,移動	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
68	C306	ユニットのインポート	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
69	C307	ジョブネットのリリース	「0」または操作結果対	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS3 のスケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
			応メッセージ ID					
70	C401	カレンダーの変更	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
71	C502	ユニットの状態表示	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
72	C503	ユニットの定義内容出力	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
73	C504	ユニットの定義内容退避	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
74	C506	ユニットの予定情報出力	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
75	C507	ユニットの名称出力	0	A	E	G	ユーザ ID または値なし	ユーザ ID または値なし
76	C508	ユニットのエクスポート	「0」または操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし
77	C509	ユニットの状態表示（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
78	C510	ユニットの定義内容出力（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
79	C511	ユニットの定義内容の退避（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
80	C512	ユニット名称の出力（異常終了時）	操作結果対応メッセージ ID	A	E	K	ユーザ ID または値なし	ユーザ ID または値なし
81	C513	登録予定情報のエクスポート	操作結果対応メッセージ ID	A	E	J	ユーザ ID または値なし	ユーザ ID または値なし

項番	JP1/AJS3 の スケジューラログ		共通部					
	ログ種別	ログ名称	メッセージ ID	発生場所	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報
82	C514	登録予定情報のエクスポートによるジョブネットの情報出力	操作結果対応メッセージ ID	A	E	J	**ユーザ ID** または値なし	**ユーザ ID** または値なし
83	C515	ジョブネットリリース情報の参照	操作結果対応メッセージ ID	A	E	J	**ユーザ ID** または値なし	**ユーザ ID** または値なし
84	I001	コマンド該当処理開始	－	A	F	G	**ユーザ ID** または値なし	**ユーザ ID** または値なし
85	I002	コマンドからサービスへの処理要求開始	－	A	F	G	**ユーザ ID** または値なし	**ユーザ ID** または値なし

（凡例）

－：該当なし

A：**取得元サーバ名**（発生場所）

B：**ログ中のホスト名**（発生場所）

C：StartStop（監査事象種別）

D：ExternalService（監査事象種別）

E：ConfigurationAccess（監査事象種別）

F：AccessControl（監査事象種別）

G：Success（監査事象結果）

H：Failure（監査事象結果）

I：Occurrence（監査事象結果）

J：次のどれかになります（監査事象結果）。

-E：Failure

0：Success

上記以外：Occurrence

K：次のどちらかになります（監査事象結果）。

-E：Failure

上記以外：Occurrence

注※1

監査ログレポート画面では，「JP1/AJS2 - View の接続」と表示されます。

注※2

監査ログレポート画面では，「JP1/AJS2 - View の接続終了」と表示されます。

なお，次の表に示す項目は JP1/AJS3 のすべてのログ種別で共通です。

表 E-6　JP1/AJS3 の監査ログ（スケジューラログ）出力情報の共通項目

共通部					固有部
監査ログ ID	日時	プログラム名	コンポーネント名	プロセス ID	固有情報
0	ログ中の値	JP1/AJS3	SchedulerLog	ログにあれば利用	ログをそのまま出力

注意事項

JP1/AJS3 のスケジューラログでは，年の情報が出力されていない場合があります。この場合，次の方法で年の情報を追加して正規化します。

- ログ中の月＜＝ログ取得の月：「取得した時点の年」の情報追加
- ログ中の月＞ログ取得の月：「取得した時点の年 - 1」の情報追加

例えば，ログ中の月が 12 月で，2010 年 1 月に取得した場合，2009 年 12 月として情報が追加されます。

付録 E.3　Oracle の監査ログ出力情報

ここでは，Oracle の監査ログ出力情報を次の表に示します。

表 E-7　Oracle の監査ログ出力情報

項番	項目名	項目名	値
1	Windows イベントログ	イベント ID	34
		ログ内容	監査ログ
2	共通部	監査ログ ID	0
		メッセージ ID	34（JP1 イベントの拡張属性の固有情報 A5 の値）
		日時	**発生日時**（JP1 イベントの拡張属性の固有情報 A0 の値）
		プログラム名	Oracle
		コンポーネント名	**イベントソース名**（JP1 イベントの拡張属性プロダクト名の値に含まれるソース）
		プロセス ID	-1
		発生場所	**コンピュータ名**（JP1 イベントの拡張属性の固有情報 A1 の値）
		監査事象種別	ContentAccess

項番	項目名	項目名	値
		監査事象結果	Occurrence
		サブジェクト種別	値なし
		サブジェクト情報	値なし
3	固有部	固有情報	すべてのログ

イベントソース名は，「Oracle.**インスタンス名**」で表示されます。JP1 イベントでは拡張属性の PRODUCTNAME に次のように出力されます。

```
/HITACHI/JP1/NTEVENT_LOGTRAP/イベントソース名
```

なお，**イベントソース名**が「Oracle.+asm」で出力されるログに関しては，Oracle 内部での接続情報などであるため，監査ログとして収集されません。

付録 E.4　UNIX システムログの監査ログ出力情報

ここでは，UNIX システムログの監査ログ出力情報を次の表に示します。

表 E-8　UNIX システムログの監査ログ出力情報

項番	UNIX システムログ	共通部					固有部		
	ログ内容	監査ログ ID	メッセージ ID	コンポーネント名	プロセス ID	監査事象結果	op	before:uid	after:uid
1	ログインの成功※1	1～2147483647※2	0001	LOGIN	ログ中の値を利用	Success	Login	出力項目名ごとなし	出力項目名ごとなし
2	ログアウト※1	1～2147483647※2	0002	LOGIN	ログ中の値を利用	Success	Logout	出力項目名ごとなし	出力項目名ごとなし
3	ログインの失敗※3	1～2147483647※2	0003	LOGIN	ログ中の値を利用	Failure	Login	出力項目名ごとなし	出力項目名ごとなし
4	su コマンドの成功	1～2147483647※2	0004	SU	-1	Success	su	**変更前ユーザ ID**	**変更後ユーザ ID**
5	su コマンドの失敗	1～2147483647※2	0005	SU	-1	Failure	su	**変更前ユーザ ID**	**変更後ユーザ ID**

注※1

収集対象とする製品によってはログアウトの情報を収集できない場合があります。また，ログイン，ログアウトの情報が二つ収集されることがあります。さらに，使用している OS によって出力するユーザ名やリモートホスト名の最大文字数が異なります。このためユーザ名やリモートホスト名が正しく出力されないことがあります。

注※2

監査ログ ID は，項番 1 と 2，項番 3，項番 4 と 5 のそれぞれで通番となります。

注※3

収集対象となる製品によってはログインの失敗情報を収集できないことがあります。

なお，次の表に示す項目は UNIX システムログのすべてのログで共通です。

表 E-9　UNIX システムログの監査ログ出力情報の共通項目

共通部						固有部	
日時	プログラム名	発生場所	監査事象種別	サブジェクト種別	サブジェクト情報	obj	msg
ログ中の値を利用	OS 名 • AIX • HP-UX • Solaris • Linux	ログ取得サーバ名	Authentication	ユーザ ID (uid)	ユーザ名※1	OS	Device_name※2

注※1

ユーザ名に制御文字が含まれる場合，制御文字は空白で出力されます。

注※2

Device_name は次の例のように出力されます。

デバイス名：/dev/pts/tb

出力情報：pts/tb または tb

また，Device_name には，「ftpxxxx」，「ftpdxxxx」，「FTP」，「rshxxxx」，「sshxxxx」などのデバイス名以外の情報が出力されます。OS によって出力される情報の形式が異なります。なお，「xxxx」は任意の半角英数字です。

注意事項

sulog を収集する場合，OS が出力するログには年の情報は出力されません。UNIX システムログ変換コマンドでは，次の方法で年の情報を追加して出力します。

「ログ中の月＜＝ UNIX システムログの変換を実施した月」の場合

「変換を実施した時点の年」の情報を追加。

「ログ中の月＞ UNIX システムログの変換を実施した月」の場合

「変換を実施した時点の年 - 1」の情報を追加。

例えば，ログ中の月が 11 月で，2007 年 10 月に UNIX ログ変換を実施した場合，2006 年 11 月として情報が追加されます。なお，ファイルに 1 年以上のデータが蓄積されていた場合，年が正しく設定されないことがあります。

付録 E.5　Windows イベントログ（セキュリティに関する情報）の監査ログ出力情報（Windows Server 2003 および Windows XP の場合）

ここでは，Windows Server 2003 および Windows XP の場合の Windows イベントログ（セキュリティ）の監査ログ出力情報を次の表に示します。

表 E-10　Windows イベントログ（セキュリティ）の監査ログ出力情報（Windows Server 2003 および Windows XP の場合）

項番	Windows イベントログ		共通部						固有部		
	イベント ID	メッセージ内容	メッセージ ID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc:from
1	528	ログオンの成功	528	A	C	E	F	H	OS	Logon	J
2	529	ログオンの失敗，ユーザ名が不明またはパスワードが無効	529	A	C	E	F	H	OS	Logon	J
3	530	ログオンの失敗 アカウントログオン時間の制限違反	530	A	C	E	F	H	OS	Logon	J
4	531	ログオンの失敗 アカウントが無効	531	A	C	E	F	H	OS	Logon	J
5	532	ログオンの失敗 指定されたユーザアカウントの有効期限切れ	532	A	C	E	F	H	OS	Logon	J
6	533	ログオンの失敗 ユーザはこのコンピュータへのログオンを許可されていない	533	A	C	E	F	H	OS	Logon	J
7	534	ログオンの失敗 要求された種類のログオンは，このコンピュータではユーザに許可されていない	534	A	C	E	F	H	OS	Logon	J
8	535	ログオンの失敗	535	A	C	E	F	H	OS	Logon	J

項番	Windows イベントログ		共通部						固有部		
	イベント ID	メッセージ内容	メッセージ ID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc: from
		指定されたアカウントのパスワードの有効期限切れ									
9	536	ログオンの失敗 NetLogon コンポーネントがアクティブではない	536	A	C	E	F	H	OS	Logon	J
10	537	ログオンの失敗 ログオン時に予期されていないエラーが発生	537	A	C	E	F	H	OS	Logon	J
11	538	ユーザのログオフ	538	A	C	E	F	H	OS	Logon	K
12	539	ログオンの失敗 アカウントのロックアウト	539	A	C	E	F	H	OS	Logon	J
13	540	ネットワークログオンの成功	540	A	C	E	F	H	OS	Network Logon	J
14	624	ユーザアカウントの作成	624	B	D	E	G	I	OSUser	Add	K
15	626	ユーザアカウントの有効化	626	B	D	E	G	I	OSUser	Change	L
16	627	パスワード変更	627	B	D	E	G	I	OSUser	Change	L
17	628	ユーザアカウントパスワードの設定	628	B	D	E	G	I	OSUser	Change	L
18	629	ユーザアカウントの無効化	629	B	D	E	G	I	OSUser	Change	L
19	630	ユーザアカウントの削除	630	B	D	E	G	I	OSUser	Delete	L
20	631	セキュリティが有効なグローバルグループの作成	631	B	D	E	G	I	OSGGrp	Add	L
21	632	セキュリティが有効なグローバル	632	B	D	E	G	I	OSGGrpUser	Add	L

項番	Windows イベントログ		共通部						固有部		
	イベントID	メッセージ内容	メッセージID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc:from
		グループメンバの追加									
22	633	セキュリティが有効なグローバルグループメンバの削除	633	B	D	E	G	I	OSGGrpUser	Delete	L
23	634	セキュリティが有効なグローバルグループの削除	634	B	D	E	G	I	OSGGrp	Delete	L
24	635	セキュリティが有効なローカルグループの作成	635	B	D	E	G	I	OSLGrp	Add	L
25	636	セキュリティが有効なローカルグループメンバの追加	636	B	D	E	G	I	OSLGrpUser	Add	L
26	637	セキュリティが有効なローカル グループメンバの削除	637	B	D	E	G	I	OSLGrpUser	Delete	L
27	638	セキュリティが有効なローカルグループの削除	638	B	D	E	G	I	OSLGrp	Delete	L
28	639	セキュリティが有効なローカルグループの変更	639	B	D	E	G	I	OSLGrp	Change	L
29	641	セキュリティが有効なグローバルグループの変更	641	B	D	E	G	I	OSGGrp	Change	L
30	642	ユーザアカウントの変更	642	B	D	E	G	I	OSUser	Change	L
31	644	ユーザアカウントのロックアウト	644	B	D	E	G	I	OSUser	Change	L

（凡例）

A：LogonEvent（コンポーネント名）

B：AccountManagement（コンポーネント名）

C：Authentication（監査事象種別）

D：ConfigurationAccess（監査事象種別）

E：Success または Failure（監査事象結果）※2

F：**実行ユーザ ID**（サブジェクト種別）

G：**ユーザ ID**（サブジェクト種別）

H：**ユーザ名**（サブジェクト情報）

I：**呼び出し側のユーザ名**（サブジェクト情報）

J：**ワークステーション名**（固有部の objloc:from）

K：出力項目名ごとなし（固有部の objloc:from）

L：**呼び出し側ドメイン**（固有部の objloc:from）

注※1

JP1 イベントの拡張属性の固有情報 A5 の値です。

注※2

Success か Failure かどうかは，JP1 イベントの拡張属性の固有情報 A3 の値によって判断されます。固有情報 A3 の値が「Audit_Success」の場合は Success，「Audit_Failure」の場合は Failure が設定されます。

なお，次の表に示す項目は Windows イベントログのすべてのイベント ID で共通です。

表 E-11　Windows イベントログ（セキュリティ）の監査ログ出力情報の共通項目（Windows Server 2003 および Windows XP の場合）

共通部					固有部
監査ログ ID	日時	プログラム名	プロセス ID	発生場所	出力項目名なしで出力するもの※1
0	**発生日時**※2	Windows	値なし	**コンピュータ名**※3	ログの残りの部分

注※1

適当な出力項目名がないログの項目または正規化できないログの項目を指します。

注※2

JP1 イベントの拡張属性の固有情報 A0 の値です。

注※3

JP1 イベントの拡張属性の固有情報 A1 の値です。

付録 E.6　Windows イベントログ（セキュリティに関する情報）の監査ログ出力情報（Windows Server 2012 または Windows Server 2008 の場合）

ここでは，Windows Server 2012 または Windows Server 2008 の場合の Windows イベントログ（セキュリティ）の監査ログ出力情報を次の表に示します。

表 E-12　Windows イベントログ（セキュリティ）の監査ログ出力情報（Windows Server 2012 または Windows Server 2008 の場合）

項番	Windows イベントログ		共通部						固有部		
	イベント ID	メッセージ内容	メッセージ ID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc:from
1	4624	ログオンの成功	4624	A	C	E	F	H	OS	Logon	K
2	4625	ログオンの失敗	4625	A	C	E	F	I	OS	Logon	K
3	4634	ユーザのログオフ	4634	A	C	E	F	J	OS	Logoff	L
4	4720	ユーザアカウントの作成	4720	B	D	E	G	J	OSUser	Add	M
5	4722	ユーザアカウントの有効化	4722	B	D	E	G	J	OSUser	Change	M
6	4723	パスワード変更	4723	B	D	E	G	J	OSUser	Change	M
7	4724	ユーザアカウントパスワードの設定	4724	B	D	E	G	J	OSUser	Change	M
8	4725	ユーザアカウントパスワードの無効化	4725	B	D	E	G	J	OSUser	Change	M
9	4726	ユーザアカウントの削除	4726	B	D	E	G	J	OSUser	Delete	M
10	4727	セキュリティが有効なグローバルグループの作成	4727	B	D	E	G	J	OSGGrp	Add	M
11	4728	セキュリティが有効なグローバルグ	4728	B	D	E	G	J	OSGGrpUser	Add	M

項番	Windows イベントログ		共通部						固有部		
	イベント ID	メッセージ内容	メッセージ ID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc: from
		ループメンバの追加									
12	4729	セキュリティが有効なグローバルグループメンバの削除	4729	B	D	E	G	J	OSGGrpUser	Delete	M
13	4730	セキュリティが有効なグローバルグループの削除	4730	B	D	E	G	J	OSGGrp	Delete	M
14	4731	セキュリティが有効なローカルグループの作成	4731	B	D	E	G	J	OSGGrp	Add	M
15	4732	セキュリティが有効なローカルグループメンバの追加	4732	B	D	E	G	J	OSGGrpUser	Add	M
16	4733	セキュリティが有効なローカルグループメンバの削除	4733	B	D	E	G	J	OSGGrpUser	Delete	M
17	4734	セキュリティが有効なローカルグループの削除	4734	B	D	E	G	J	OSGGrp	Delete	M
18	4735	セキュリティが有効なローカルグループの変更	4735	B	D	E	G	J	OSGGrp	Change	M
19	4737	セキュリティが有効なグローバルグループの変更	4737	B	D	E	G	J	OSGGrp	Change	M
20	4738	ユーザアカウントの変更	4738	B	D	E	G	J	OSUser	Change	M
21	4740	ユーザアカウントのロックアウト	4740	B	D	E	G	J	OSUser	Change	M
22	4744	セキュリティが無効なローカルグループの作成	4744	B	D	E	G	J	OSGGrp	Add	M

項番	Windows イベントログ		共通部						固有部		
	イベント ID	メッセージ内容	メッセージ ID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc: from
23	4745	セキュリティが無効なローカルグループの変更	4745	B	D	E	G	J	OSGGrp	Change	M
24	4746	セキュリティが無効なローカルグループメンバの追加	4746	B	D	E	G	J	OSGGrpUser	Add	M
25	4747	セキュリティが無効なローカルグループメンバの削除	4747	B	D	E	G	J	OSGGrpUser	Delete	M
26	4748	セキュリティが無効なローカルグループの削除	4748	B	D	E	G	J	OSGGrp	Delete	M
27	4749	セキュリティが無効なグローバルグループの作成	4749	B	D	E	G	J	OSGGrp	Add	M
28	4750	セキュリティが無効なグローバルグループの変更	4750	B	D	E	G	J	OSGGrp	Change	M
29	4751	セキュリティが無効なグローバルグループメンバの追加	4751	B	D	E	G	J	OSGGrpUser	Add	M
30	4752	セキュリティが無効なグローバルグループメンバの削除	4752	B	D	E	G	J	OSGGrpUser	Delete	M
31	4753	セキュリティが無効なグローバルグループの削除	4753	B	D	E	G	J	OSGGrp	Delete	M
32	4754	セキュリティが有効なユニバーサルグループの作成	4754	B	D	E	G	J	OSGGrp	Add	M

項番	Windows イベントログ		共通部						固有部		
	イベント ID	メッセージ内容	メッセージ ID ※1	コンポーネント名	監査事象種別	監査事象結果	サブジェクト種別	サブジェクト情報	obj	op	objloc: from
33	4755	セキュリティが有効なユニバーサルグループの変更	4755	B	D	E	G	J	OSGGrp	Change	M
34	4756	セキュリティが有効なユニバーサルグループメンバの追加	4756	B	D	E	G	J	OSGGrpUser	Add	M
35	4757	セキュリティが有効なユニバーサルグループメンバの削除	4757	B	D	E	G	J	OSGGrpUser	Delete	M
36	4758	セキュリティが有効なユニバーサルグループの削除	4758	B	D	E	G	J	OSGGrp	Delete	M
37	4759	セキュリティが無効なユニバーサルグループの作成	4759	B	D	E	G	J	OSGGrp	Add	M
38	4760	セキュリティが無効なユニバーサルグループの変更	4760	B	D	E	G	J	OSGGrp	Change	M
39	4761	セキュリティが無効なユニバーサルグループメンバの追加	4761	B	D	E	G	J	OSGGrpUser	Add	M
40	4762	セキュリティが無効なユニバーサルグループメンバの削除	4762	B	D	E	G	J	OSGGrpUser	Delete	M
41	4763	セキュリティが無効なユニバーサルグループの削除	4763	B	D	E	G	J	OSGGrp	Delete	M

（凡例）

A：LogonEvent（コンポーネント名）

B：AccountManagement（コンポーネント名）

C：Authentication（監査事象種別）

D：ConfigurationAccess（監査事象種別）

E：Success または Failure（監査事象結果）※2

F：**実行ユーザ ID**（サブジェクト種別）

G：**ユーザ ID**（サブジェクト種別）

H：新しいログオン：**アカウント名**（サブジェクト情報）

I：ログオンを失敗したアカウント：**アカウント名**（サブジェクト情報）

J：サブジェクト：**アカウント名**（サブジェクト情報）

K：ネットワーク情報：**ワークステーション名**（固有部の objloc:from）

L：出力項目名ごとなし（固有部の objloc:from）

M：サブジェクト：**アカウントドメイン**（固有部の objloc:from）

注※1

JP1 イベントの拡張属性の固有情報 A5 の値です。

注※2

Success か Failure かどうかは，JP1 イベントの拡張属性の固有情報 A3 の値によって判断します。固有情報 A3 の値が「Audit_Success」の場合は Success，「Audit_Failure」の場合は Failure を設定します。

なお，次の表に示す項目は Windows イベントログのすべてのイベント ID で共通です。

表 E-13　Windows イベントログ（セキュリティ）の監査ログ出力情報の共通項目（Windows Server 2012 または Windows Server 2008 の場合）

共通部					固有部
監査ログ ID	日時	プログラム名	プロセス ID	発生場所	出力項目名なしで出力するもの※1
0	**発生日時**※2	Windows	値なし	**コンピュータ名**※3	ログの残りの部分

注※1

適当な出力項目名がないログの項目または正規化できないログの項目を指します。

注※2

JP1 イベントの拡張属性の固有情報 A0 の値です。

注※3

JP1 イベントの拡張属性の固有情報 A1 の値です。

付録 F　各バージョンの変更内容

付録 F.1　11-00 の変更内容

- 次に示すプログラムの監査ログ収集を標準サポートした。
  - JP1/ITDM2
  - uCosminexus EUR Server
  - Hitachi Navigation Platform
- 標準サポートしているプログラムに次のバージョンを追加した。
  - Hitachi Command Suite 8
  - Oracle 11g R2 および 12c
- JP1/AO のプラットフォームに Linux を追加した。
- 次に示すプログラムの，英語版 OS における監査ログ収集を標準サポートした。
  - JP1/AJS3
  - JP1/AO
  - JP1/Base
  - JP1/IM - SS
  - JP1/ITDM2
  - JP1/PFM
- 監査ログ管理サーバ，監査ログ閲覧サーバ，および監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - Microsoft(R) Windows Server(R) 2012 R2 Datacenter
  - Microsoft(R) Windows Server(R) 2012 R2 Standard
- 監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - Linux 7.1 (AMD/Intel 64)
  - Oracle Linux 6 (AMD64 & EM64T)
  - Oracle Linux 7 (AMD64 & EM64T)
  - SUSE Linux Enterprise Server 12 (AMD64 & EM64T)
  - CentOS 6 (AMD64 & EM64T)
  - CentOS 7 (AMD64 & EM64T)
- 監査ログ管理サーバ，監査ログ閲覧サーバ，および監査ログ収集対象サーバの前提 OS から，次の OS を削除した。

    - Microsoft(R) Windows Server(R) 2003, Enterprise Edition
    - Microsoft(R) Windows Server(R) 2003, Standard Edition
    - Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
    - Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
    - Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
    - Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
    - Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
    - Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
    - Microsoft(R) Windows Server(R) 2008 Enterprise
    - Microsoft(R) Windows Server(R) 2008 Standard
- 監査ログ収集対象サーバの前提 OS から，次の OS を削除した。
    - Linux 5 (AMD64 & Intel EM64T)
    - Linux 5 (x86)
- 監査ログ閲覧サーバの前提プログラムについて，Internet Explorer のバージョンを 8 以降に変更した。
- 監査ログ管理サーバ，監査ログ閲覧サーバの前提プログラムについて，JP1/Base のバージョンを 11-00 以降に変更した。
- 監査ログ管理サーバ，監査ログ閲覧サーバの前提プログラムについて，Microsoft Internet Information Services のバージョンを 7.5 以降に変更した。
- 監査ログ閲覧サーバの前提プログラムについて，EUR のバージョンを 08-00 以降に変更した。
- JP1/AJS3 の監査ログ（スケジューラログ）出力情報を追加した。
- 監査ログ管理サーバの注意事項に，データベースのメンテナンスおよび監査ログの検索に関する注意事項を追加した。
- KDSP2820-W のメッセージの説明文およびユーザが取る処置の説明を変更した。
- UNIX システムログの監査ログの出力先を訂正した。
- 収集できる監査ログの文字コードについて表を追加した。
- Microsoft Internet Information Services をインストールする手順に確認事項を追加した。
- admexport コマンドの出力項目および出力例を記載した。
- admimport コマンドの注意事項を追加した。
- 監査ログ閲覧サーバのセットアップ手順で，必要なサービスを記載した。

付録 F.2　10-10 の変更内容

- 次に示す Web ブラウザをサポートした。

  - Windows(R) Internet Explorer(R) 9
  - Windows(R) Internet Explorer(R) 10
- 次に示すプログラムの監査ログ収集を標準サポートした。
  - JP1/AO
  - JP1/IM - NP
  - JP1/IM - SS
  - uCosminexus Navigation Platform
- 監査ログ管理サーバ，監査ログ閲覧サーバ，および監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - Microsoft(R) Windows Server(R) 2012 Datacenter
  - Microsoft(R) Windows Server(R) 2012 Standard
- 監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - Solaris 11
  - Linux 5 (AMD64 & Intel EM64T)
  - Linux 5 (x86)
- 次に示す容量の見積もりを変更した。
  - メモリ所要量の見積もり
  - ディスク占有量の見積もり
  - データベース容量の見積もり（データベースの操作時に必要なディスク容量）
- データベースの CSV バックアップで取得した CSV バックアップファイルから，データベースの復元（CSV リストア）をコマンドで実行できるようにした。
- 次に示すコマンドで-c オプションを指定して，作業用フォルダに必要なサイズの空き容量があるかどうかをチェックできるようにした。
  - admdbdelete（データベースのデータ削除）
  - admdbrorg（データベースの再編成）
  - admimport（監査ログのインポート）
- 次のメッセージを追加した。

  KDSO0140-E，KDSO0141-E，KDSO0522-E，KDSO0523-E，KDSO0677-E，KDSO0678-E，KDSO0731-E，KDSO0732-E
- JP1/AJS3 のスケジューラログを追加した。

付録 F.3　10-00 の変更内容

- 製品名称を JP1/NETM/Audit - Manager から JP1/Audit Management - Manager に変更した。
- 監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - Linux 6.1 (x86)
  - Linux 6.1 (AMD/Intel 64)
- 監査ログ収集対象サーバがクラスタ環境で運用されている場合の前提 OS に，次の OS を追加した。
  - AIX 6.1
  - AIX 7.1
  - Linux 6.1 (x86)
  - Linux 6.1 (AMD/Intel 64)
- 監査ログ収集対象サーバの前提 OS から，次の OS を削除した。
  - Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems
  - Solaris 9
  - AIX 5L V5.3
  - HP-UX 11i V2 (IPF)
  - Red Hat Enterprise Linux(R) AS 4 (AMD64 & Intel EM64T)
  - Red Hat Enterprise Linux(R) ES 4 (AMD64 & Intel EM64T)
  - Red Hat Enterprise Linux(R) 5 (AMD64 & Intel EM64T)
  - Red Hat Enterprise Linux(R) 5 Advanced Platform (AMD64 & Intel EM64T)
  - Red Hat Enterprise Linux(R) AS 4 (IPF)
  - Red Hat Enterprise Linux(R) 5 (IPF)
  - Red Hat Enterprise Linux(R) 5 Advanced Platform (IPF)
  - Red Hat Enterprise Linux(R) AS 4 (x86)
  - Red Hat Enterprise Linux(R) ES 4 (x86)
  - Red Hat Enterprise Linux(R) 5 (x86)
  - Red Hat Enterprise Linux(R) 5 Advanced Platform (x86)
- 次に示すプログラムの監査ログ収集を標準サポートした。
  - JP1/ITDM
  - JP1/NETM/AIM
- IPv6 アドレスを使用して通信する監査ログ収集対象サーバの監査ログを収集できるようにした。
- JP1/AJS3 のスケジューラログを追加した。
- 次のメッセージを変更した。

KDSO0123-E，KDSO0423-W，KDSO0473-W，KDSO0520-W，KDSO0565-W，KDSO0620-W，KDSO0673-W，KDSO0726-W，KDSO1658-E，KDSO2215-W，KDSO2456-W，KDSO3151-E，KDSO3219-E，KDSO3332-E，KDSO3350-E，KDSO3564-E

付録 F.4　09-50 の変更内容

- JP1/ITRM を監査ログ収集対象として標準サポートした。
- admcoldata コマンドを実行して，監査ログを即時収集できるようにした。
- データベースをメンテナンスする際，サービスを停止している間に，監査ログを収集できるようにした。また，それに伴い JP1/NETM/Audit - Manager SubCollect サービスを追加した。
- 監査ログ管理サーバおよび監査ログ閲覧サーバの前提 OS に，次の OS を追加した。
  - Microsoft(R) Windows Server(R) 2008 R2 Datacenter
  - Microsoft(R) Windows Server(R) 2008 R2 Enterprise
  - Microsoft(R) Windows Server(R) 2008 R2 Standard
- 監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - Microsoft(R) Windows Server(R) 2008 R2 Datacenter
  - Microsoft(R) Windows Server(R) 2008 R2 Enterprise
  - Microsoft(R) Windows Server(R) 2008 R2 Standard
  - AIX 7.1
- 次のメッセージを追加した。
  KDSO1512-I～KDSO1518-W，KDSO1601-I～KDSO1611-W，KDSO1651-E～KDSO1662-E
- JP1/AJS3 のスケジューラログを追加した。

付録 F.5　09-10 の変更内容

- 次に示すプログラムを監査ログ収集対象として標準サポートした。
  - JP1/NETM/NM
  - uCosminexus Portal Framework
- ユーザマッピングの項を削除した。
- 監査ログ収集対象サーバの前提 OS に，次の OS を追加した。
  - AIX 6.1
  - Linux 5 (IPF)
  - Linux 5 Advanced Platform (IPF)

  - Linux 5 (AMD64 & Intel EM64T)
  - Linux 5 Advanced Platform (AMD64 & Intel EM64T)
  - Linux 5 (x86)
  - Linux 5 Advanced Platform (x86)
- admrrexport コマンドで，正規化ルールをバックアップできるようにした。
- admrrimport コマンドで，正規化ルール定義エクスポートファイルをインポートできるようにした。
- 次のメッセージを追加した。
  KDSP2006-I～KDSP2011-E，KDSP2102-E～KDSP2103-E，KDSP2107-E，KDSP2120-E，KDSP2600-E～KDSP2615-W，KDSP2620-I～KDSP2623-I，KDSP2630-E～KDSP2631-E，KDSP2800-I～KDSP2801-I，KDSP2830-W
- 次のメッセージについて，オペレータの対処方法を変更した。
  KDSP0616-E，KDSP2810-W
- 監査証跡管理システムのトラブル発生時に取得する資料を追加した。
- JP1/NETM/Audit - Manager が監査ログを出力する契機，および共通出力項目に出力される値を追加した。
- OpenTP1 のプラットフォームに，AIX および HP-UX を追加した。

付録 F.6　09-00 の変更内容

- パターン表示編集画面で，機能ツリー表示領域にあるユーザ作成のパターンやフォルダの情報をインポートおよびエクスポートできるようにした。
- ユーザ作成のパターンやフォルダの情報をインポートおよびエクスポートするときに使用するファイルとして，パターン情報ファイルを追加した。
- 集計結果グラフの集計結果件数の表示位置を変更した。
- 監査ログ収集対象サーバのセットアップに必要なファイルを一つのアーカイブファイルで提供するようにした。
- 監査ログ収集対象サーバのセットアップに必要なファイルをインストールする admagtinstall コマンドを追加した。
- 監査ログ専用イベントサーバの環境をセットアップする admagtsetup コマンドを追加した。
- 監査ログ専用イベントサーバの環境情報を定義するファイルとして，監査ログ収集対象サーバセットアップ定義ファイルを追加した。
- 次に示すプログラムを監査ログ収集対象として標準サポートした。
  - JP1/AJS3
  - JP1/秘文

- OpenTP1（Windows 版）
- Oracle 11g
- TRUST E2
- XDM/BASE E2
- 活文 NAVIstaff

- ［データベースの詳細設定］ダイアログで指定できる監査ログ管理データベースのサイズに，「LL サイズ」を追加した。また，それに伴いデータベースのサイズの表現を次のとおり変更した。
  - 「大規模サイズ」を「L サイズ」に変更した。
  - 「中規模サイズ」を「M サイズ」に変更した。
  - 「小規模サイズ」を「S サイズ」に変更した。
- admdbdelete（データベースのデータ削除）コマンドで，データを削除する処理方法に，マイナー削除モードまたはバルク削除モードを指定できるようにした。
- admimport（監査ログのインポート）コマンドで，監査ログをインポートする処理方法に，マイナー挿入モードまたはバルク挿入モードを指定できるようにした。
- 標準サポート外の Windows イベントログ（セキュリティに関する情報）を監査ログとして収集する場合の設定方法を追加した。また，これに伴い Windows イベントログ用の正規化ルールファイルを追加した。
- 監査ログ管理サーバおよび監査ログ閲覧サーバとして，次に示す OS をサポートした。
  - Microsoft Windows Server 2008 Enterprise
  - Microsoft Windows Server 2008 Standard
- クラスタ環境で運用する場合の監査ログ管理サーバとして，次に示す OS をサポートした。
  - Microsoft Windows Server 2008 Enterprise
- 監査ログ管理サーバおよび監査ログ閲覧サーバの前提プログラムを JP1/Base 08-10 から JP1/Base 09-00 に変更した。
- 監査ログ管理サーバおよび監査ログ閲覧サーバの前提プログラムとして，Microsoft Internet Information Services 7.0 をサポートした。
- 監査ログ管理サーバおよび監査ログ閲覧サーバで，PDF ファイルの帳票を出力する場合の前提プログラムを次のとおり変更した。
  - 「EUR Print Service 05-06 以降」を「EUR Print Service 07-60 以降」に変更した。
  - 「EUR Print Service - Portable Document Format report 05-06 以降」を「EUR Print Service - Portable Document Format report 07-60 以降」に変更した。
  - 「EUR Professional Edition」を前提プログラムから削除した。
- JP1/NETM/Audit - Manager 09-00 を新規インストールした場合，admuxlogcol コマンドの格納先ディレクトリを変更した。

- JP1/NETM/Audit - Manager 09-00 を新規インストールした場合，admhasetup コマンドの格納先フォルダを変更した。
- JP1/NETM/Audit - Manager 09-00 を新規インストールした場合，admlogtrap.bat の格納先フォルダを変更した。
- JP1/NETM/Audit - Manager 09-00 を新規インストールした場合，監視対象のスクリプトファイルの出力先ディレクトリを変更した。
- データベースの操作時に必要なディスク容量の見積もり式を追加した。
- 次のメッセージを追加した。
  KDSO0128-E～KDSO0139-E，KDSO0232-E，KDSO0233-E，KDSO0728-I～KDSO0730-E，KDSO2477-W，KDSO3329-I～KDSO3350-E，KDSO3570-E～KDSO3575-I，KDSP2810-W，KDSP2820-W
- 次のメッセージを変更した。
  KDSO0117-E
- 次のメッセージについて，オペレータの対処方法を変更した。
  KDSO0716-E，KDSO2044-W
- 次のメッセージを削除した。
  KDSO0714-E，KDSO0722-E

付録 F.7　08-51 の変更内容

- 機能ツリーに「テンプレートのフォルダ」を追加したことに伴い，「デフォルトの検索パターン」および「デフォルトの集計パターン」の呼称を，それぞれ「テンプレートの検索パターン」および「テンプレートの集計パターン」に変更した。
- 次に示すプログラムの監査ログ収集を標準サポートした。
  - Collaboration
  - HiRDB
- 監査ログ収集対象サーバをクラスタシステムで運用できるようにした。
- データベースの使用状況を確認する admdbstat コマンドを追加した。
- admdbdelete コマンドまたは admimport コマンドを実行するとき，データベースのパスワード入力を要求するかどうかを，インストール時に設定できるようにした。
- パターン表示編集画面で，機能ツリーのパターン表示について編集できるようにした。
- パターン保存画面で，新規のパターンを保存できるようにした。
- 監査ログ検索画面および監査ログ集計画面の固有情報に，AND 条件および OR 条件で複数の文字列を指定できるようにした。
- カレンダーの日付表示幅を拡張した。

- admlog.vbs コマンド（スクリプト）で引数を指定しなかったとき，データベースの詳細資料を採取しないようにした。
- 次のメッセージを追加した。

  KDSO0424-E，KDSO0425-E，KDSO0476-E，KDSO0521-E，KDSO0621-E，KDSO0901-E～KDSO0911-E，KDSO1511-E，KDSO3017-E，KDSO3050-E，KDSO3225-E，KDSO3301-I～KDSO3318-W，KDSO3320-W～KDSO3321-W，KDSO3323-W，KDSO3325-W～KDSO3328-E，KDSO3552-I～KDSO3569-E，KDSO3764-E，KDSP0009-E，KDSP2002-E～KDSP2005-E
- 次のメッセージを削除した。

  KDSP2200-I～KDSP2201-I
- 次のメッセージについて，オペレータの対処方法を変更した。

  KDSO0422-E，KDSO0519-E，KDSO0619-E，KDSO1505-E，KDSO3016-E，KDSP0602-E，KDSP0802-E～KDSP0803-E，KDSP0913-E
- 次のメッセージを変更した。

  KDSO3192-I～KDSO3193-I，KDSO3514-I～KDSO3515-E，KDSO3549-E～KDSO3550-E，KDSP0001-I，KDSP0008-I，KDSP0012-I，KDSP0200-E，KDSP0602-E，KDSP0612-E，KDSP0616-E，KDSP0628-E，KDSP2000-I～KDSP2001-I
- 次のメッセージについて，システムの対処方法を変更した。

  KDSO3262-I，KDSP2000-I～KDSP2001-I

付録 F.8　08-50 の変更内容

- 次に示すプログラムの監査ログ収集を標準サポートした。
  - Hitachi Storage Command Suite
  - OpenTP1
- 監査ログ管理画面の監査ログ統計画面で，監査ログの統計を取れるようにした。
- 監査ログ管理画面の表示設定画面で，監査ログ統計画面で指定する統計出力条件のデフォルトを設定できるようにした。
- 従来，テキストエディタで編集し定義していた標準サポート外のプログラムの正規化ルールを，GUI（正規化ルールエディタ）でも定義できるようにした。
- 監査ログ管理画面の表示設定画面で，集計パターンを監査ログ統計画面で指定する統計パターンとして設定できるようにした。
- 監査ログ収集対象として，次の OS をサポートした。
  - Windows Server 2008
- ［データベースの詳細設定］ダイアログで指定できる監査ログ管理データベースのサイズを次のように変更した。

- 「大規模サイズ」のサイズを 182 ギガバイトから 190 ギガバイトに変更した。
- 「中規模サイズ」のサイズを 54 ギガバイトから 56 ギガバイトに変更した。
- 「小規模サイズ」のサイズを 10 ギガバイトから 12 ギガバイトに変更した。

- 監査証跡管理システムを開始するときに起動する必要がある次のサービスを追加した。
  - JP1/NETM/Audit - Manager Convert サービス
  - JP1/NETM/Audit - Manager Define サービス
- [マネージャセットアップ] ダイアログで，監査ログレポート画面に表示するレポートの表示最大件数を任意で設定できるようにした。
- データベースの接続時に使用するパスワードを変更するとき，変更前と変更後のパスワードを入力するように変更した。
- [データベースマネージャ] ダイアログで次に示す画面を表示するとき，[データベースのパスワード確認] 画面でパスワードを認証するようにした。
  - [データベースの基本設定] 画面
  - [データベースの CSV リストア設定] 画面
  - [データベースのリストア設定] 画面
- 監査ログ管理画面の監査ログ集計画面で集計条件を指定するとき，集計単位として「サブジェクト情報」が指定できるようにした。
- 監査ログのバックアップファイルのデータ内容が改ざんされている場合は，インポートできないようにした。
- データベースの CSV バックアップのデータ内容が改ざんされている場合は，データベースを CSV リストアできないようにした。
- 次に示すコマンドの実行時にパスワードを入力するよう変更した。
  - admdbdelete（データベースのデータ削除）
  - admimport（監査ログのインポート）
- 次のメッセージを追加した。

  KDSO0016-E，KDSO0125-E～KDSO0127-W，KDSO0474-E～KDSO0475-E，KDSO0674-E～KDSO0676-E，KDSO0727-E，KDSO0801-E～KDSO0819-I，KDSO0851-E～KDSO0866-E，KDSO0868-E～KDSO0869-E，KDSO2054-E～KDSO2056-E，KDSO2259-E～KDSO2262-E，KDSO2474-E～KDSO2476-E，KDSO3233-I～KDSO3249-E，KDSO3256-E～KDSO3257-E，KDSO3270-I～KDSO3276-E，KDSO3541-I～KDSO3544-E，KDSO3547-I～KDSO3551-I，KDSP0001-I～KDSP0002-I，KDSP0008-I，KDSP0010-I～KDSP0012-I，KDSP0016-I，KDSP0119-W，KDSP0200-E，KDSP0402-W，KDSP0404-E～KDSP0408-I，KDSP0602-E～KDSP0603-I，KDSP0610-E，KDSP0612-E，KDSP0614-E，KDSP0616-E～KDSP0618-I，KDSP0628-E，KDSP0702-W～KDSP0703-E，KDSP0711-E，KDSP0715-I～KDSP0716-I，KDSP0719-I，KDSP0721-W～KDSP0723-W，KDSP0725-E，KDSP0736-W～KDSP0737-W，KDSP0800-E～KDSP0803-E，KDSP0900-E～KDSP0904-E，KDSP0906-E，KDSP0911-E～

KDSP0913-E，KDSP0915-E～KDSP0916-E，KDSP0997-E，KDSP2000-I～KDSP2001-I，KDSP2100-E～KDSP2101-E，KDSP2104-E～KDSP2106-E，KDSP2108-E，KDSP2110-E，KDSP2200-I～KDSP2203-I，KDSP2210-E～KDSP2211-E，KDSP2500-E～KDSP2502-E，KDSP2900-E～KDSP2903-E

- 次のメッセージを変更した。

  KDSO0123-W，KDSO0423-W，KDSO0473-W，KDSO0520-W，KDSO0565-W，KDSO0620-W，KDSO0673-W，KDSO0726-W，KDSO2029-E，KDSO2214-W～KDSO2215-W，KDSO2456-W

- 次のメッセージについて，システムの対処方法を変更した。

  KDSO3231-I

- 次のメッセージについて，オペレータの対処方法を変更した。

  KDSO0119-E，KDSO0123-W，KDSO0175-E，KDSO0222-E，KDSO0417-E，KDSO0423-W，KDSO0467-E，KDSO0473-W，KDSO0515-E，KDSO0520-W，KDSO0563-E，KDSO0565-W，KDSO0615-E，KDSO0620-W，KDSO0667-E，KDSO0673-W，KDSO0718-E，KDSO0726-W，KDSO0769-E，KDSO2033-E，KDSO2040-E，KDSO2215-W，KDSO2244-E，KDSO2402-E，KDSO2456-W

- 次のメッセージについて，オペレータの対処方法を追加した。

  KDSO2216-I，KDSO2411-I～KDSO2415-I，KDSO2459-I～KDSO2460-I，KDSO2468-I～KDSO2470-I，KDSO3118-I～KDSO3123-I，KDSO3153-I～KDSO3154-I，KDSO3204-I

付録 F.9　08-11 の変更内容

- UNIX システムログのセキュリティに関する情報（ログイン・ログアウトやユーザの権限変更など）を収集できるようにした。
- 次に示す製品の監査ログ収集を標準サポートした。
  - Cosminexus
  - JP1/NETM/CSC
  - JP1/PFM
  - Oracle
- 監査ログ管理画面の監査ログ検索画面から，監査ログの検索結果をレポート表示できるようにした。
- 監査ログ管理画面の監査ログ集計画面から，監査ログの集計結果を基にグラフ表示できるようにした。
- 監査ログをバックアップする admexport コマンドで，前回からの差分をバックアップできるようにした。
- 従来，［マネージャセットアップ］ダイアログで実施していた監査ログ収集対象の設定を［監査ログ収集マネージャ］ウィンドウで実施するように変更した。
- 監査ログを即時収集できるようにした。

- データベースマネージャにデータベースのアップグレード機能を追加した。
- 監査ログのバックアップファイルおよびバックアップ履歴の情報を削除する admcsvremove コマンドを追加した。
- 検索パターンおよび集計パターンの条件設定を，監査ログ管理画面の機能ツリーから選択して設定できるようにした。
- 監査ログ収集対象として，次の OS をサポートした。
  - AIX 5L V5.2
  - HP-UX 11i (PA-RISC)
  - HP-UX 11i V2/11i V3 (IPF)
  - Linux AS 4 (AMD64 & Intel EM64T)
  - Linux ES 4 (AMD64 & Intel EM64T)
  - Linux AS 4 (IPF)
  - Solaris 10
  - Windows Server 2003 (IPF)
- 監査ログ収集対象サーバをクラスタ環境で運用する場合の監査ログの収集先を共有ディスクからローカルディスクに変更した。
- JP1/NETM/Audit - Manager のメモリ所要量およびディスク占有量の見積もりを変更した。
- データベースのサイズを変更した。
- [マネージャセットアップ] ダイアログで設定するログ情報および監査ログ情報の設定値の単位およびデフォルト値を変更した。
- 正規化ルールファイルおよび動作定義ファイルの格納フォルダを専用のフォルダに変更した。
- 監査ログ管理画面のログ情報および監査ログ情報を［マネージャセットアップ］ダイアログで設定できるようにした。
- データベースのセットアップの順番を，次のように変更した。

  1. [データベースの基本設定] 画面
  2. [データベースの詳細設定] 画面
  3. [クラスタシステム環境の設定] 画面

  また，［クラスタシステム環境の設定］画面で「共有ディレクトリ上の格納先フォルダ」を設定できるようにした。
- 収集対象プログラムを指定するための製品定義ファイルを編集できるようにした。
- 監査ログ管理画面での検索・集計時に，検索条件や集計条件の文字列を大文字・小文字で区別しないように変更した。
- 検索結果や集計結果の表示件数を，監査ログ検索画面，監査ログ集計画面，およびバックアップ履歴管理画面で設定できるようにした。

- 監査ログ管理画面の検索結果や集計結果のページ遷移を，ページ数を指定して表示できるようにした。
- 監査ログ管理画面の表示設定画面で，次の内容を変更した。
  - ［設定画面］プルダウンメニューから画面名を選択するだけで設定画面に遷移するようにした。
  - 表示設定情報を初期状態に戻せるようにした。
- 監査ログの監視ステータス，監査ログの最終収集日時，および監査ログ収集対象サーバのアダプタコマンドのバージョン情報を確認できるようにした。
- 最大 32 個の監査ログファイルを監視できるようにした。
- 障害調査に必要な情報を一括採取する admlog.vbs コマンド（スクリプト）を追加した。
- 標準サポートしていない製品の監査ログを収集するために定義する正規化ルールファイルで，任意の日時形式を設定できるようにした。
- 次のメッセージを追加した。

  KDSO0120-E～KDSO0124-I，KDSO0178-E～KDSO0200-I，KDSO0227-E～KDSO0231-E，KDSO0418-E～KDSO0423-W，KDSO0468-E～KDSO0473-W，KDSO0516-E～KDSO0520-W，KDSO0564-I～KDSO0565-W，KDSO0616-E～KDSO0620-W，KDSO0668-E～KDSO0673-W，KDSO0719-E～KDSO0726-W，KDSO0751-E～KDSO0777-E，KDSO1505-E～KDSO1510-I，KDSO2052-I～KDSO2053-I，KDSO2226-I～KDSO2230-I，KDSO2234-E～KDSO2238-E，KDSO2245-E～KDSO2258-E，KDSO2400-W～KDSO2432-E，KDSO2434-E～KDSO2440-E，KDSO2442-E～KDSO2473-I，KDSO3001-E～KDSO3016-E，KDSO3053-W～KDSO3064-I，KDSO3101-W～KDSO3108-E，KDSO3112-I～KDSO3113-I，KDSO3116-I～KDSO3128-E，KDSO3151-E～KDSO3154-I，KDSO3156-E～KDSO3157-I，KDSO3161-E～KDSO3163-E，KDSO3165-E～KDSO3183-W，KDSO3186-I～KDSO3221-E，KDSO3226-E～KDSO3232-E，KDSO3251-E～KDSO3255-E，KDSO3258-I～KDSO3269-W，KDSO3502-I～KDSO3503-E，KDSO3505-I～KDSO3506-E，KDSO3508-I～KDSO3509-E，KDSO3511-I～KDSO3512-E，KDSO3514-I～KDSO3515-E，KDSO3517-I～KDSO3518-E，KDSO3520-I～KDSO3521-E，KDSO3523-I～KDSO3524-E，KDSO3526-I～KDSO3527-E，KDSO3529-I～KDSO3540-E，KDSO3752-I～KDSO3763-E，KDSO3802-I，KDSO3804-E～KDSO3807-E，KDSO3851-I～KDSO3853-E
- 次のメッセージを変更した。

  KDSO0001-I～KDSO0002-I，KDSO0011-E，KDSO0103-I～KDSO0105-E，KDSO0153-I～KDSO0155-E，KDSO0159-E，KDSO0160-E，KDSO0162-E，KDSO0203-I～KDSO0205-E，KDSO0213-E，KDSO0226-E，KDSO0464-E，KDSO0614-E，KDSO1039-W，KDSO1504-E，KDSO2003-E～KDSO2004-E，KDSO2026-E，KDSO2030-E，KDSO2212-E～KDSO2214-E，KDSO2233-E
- 次のメッセージについて，システムの対処方法を変更した。

  KDSO0001-I～KDSO0002-I，KDSO0708-I，KDSO1000-E，KDSO1501-I，KDSO2233-E，KDSO2239-E，KDSO2241-E，KDSO2244-E
- 次のメッセージについて，オペレータの対処方法を変更した。

KDSO0007-E，KDSO0014-W，KDSO0015-W，KDSO0157-E，KDSO0159-E，KDSO0162-E，KDSO0172-E，KDSO0219-E，KDSO0226-E，KDSO0463-E，KDSO0559-I，KDSO0663-E，KDSO0713-E，KDSO1000-E，KDSO1030-E～KDSO1032-E，KDSO1036-W～KDSO1041-W，KDSO1044-E，KDSO1103-E，KDSO2232-E，KDSO2240-E

- 次のメッセージについては，対処が不要なため，オペレータの対処方法を削除した。

  KDSO0001-I～KDSO0002-I，KDSO0103-I～KDSO0104-I，KDSO0112-I，KDSO0153-I～KDSO0154-I，KDSO0203-I～KDSO0204-I，KDSO0408-I～KDSO0409-I，KDSO0411-I，KDSO0458-I～KDSO0459-I，KDSO0461-I，KDSO0508-I～KDSO0509-I，KDSO0511-I，KDSO0558-I，KDSO0608-I～KDSO0609-I，KDSO0611-I，KDSO0658-I～KDSO0659-I，KDSO0661-I，KDSO0708-I～KDSO0709-I，KDSO0711-I，KDSO1101-I，KDSO1500-I～KDSO1501-I，KDSO2001-I，KDSO2009-I，KDSO2216-I，KDSO2225-I，KDSO2231-I

- 次のメッセージを削除した。

  KDSO0171-E，KDSO1001-E～KDSO1004-E，KDSO1006-E～KDSO1007-I，KDSO1016-I～KDSO1017-I，KDSO1024-I，KDSO1026-E，KDSO1029-E，KDSO1033-E～KDSO1035-W，KDSO1042-E，KDSO1045-E，KDSO2005-I～KDSO2008-I，KDSO2010-I～KDSO2017-E，KDSO2019-E，KDSO2025-E，KDSO2031-E～KDSO2032-E，KDSO2034-E～KDSO2036-E，KDSO2038-E～KDSO2039-E，KDSO2041-E～KDSO2042-E，KDSO2210-E

付録 G　このマニュアルの参考情報

付録 G.1　関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- GUI（正規化ルールエディタ）を使用した正規化ルールの定義方法について知りたい場合
  JP1 Version 11 JP1/Audit Management - Manager 正規化ルール定義ガイド（3021-3-A18）
- JP1 管理基盤（JP1/Base）の構築方法，および運用方法について知りたい場合
  - JP1 Version 11 JP1/Base 運用ガイド（3021-3-A01）
  - JP1 Version 11 JP1/Base メッセージ（3021-3-A02）
- リモートインストール方法について知りたい場合
  JP1 Version 10 JP1/NETM/DM 運用ガイド 1(Windows(R)用)（3021-3-177）
- EUR について知りたい場合
  EUR V7
  - 帳票作成機能 EUR EUR 概説（3020-7-480）
  - 帳票作成機能 EUR EUR Print Service 帳票出力（3020-7-484）

  EUR V8
  - 帳票システム構築支援　uCosminexus EUR uCosminexus EUR 概説（3020-7-531）
  - 帳票システム構築支援　uCosminexus EUR uCosminexus EUR サーバ帳票出力（3020-7-536）

  EUR V9
  - uCosminexus EUR システム設計ガイド（3020-7-702）
  - uCosminexus EUR システム構築ガイド（3020-7-703）
  - uCosminexus EUR 帳票出力 機能解説 EUR Server 編（3020-7-708）
- 監査証跡管理システムで収集対象としている各プログラムについて知りたい場合
  各プログラムに同梱されているマニュアルを参照してください。

付録 G.2　このマニュアルでの表記

このマニュアルでは，製品名称を，略称を使って表記しています。正式名称と，このマニュアルでの表記を次の表に示します。

このマニュアルでの表記	正式名称
Adobe Reader	Adobe Reader 7.0

このマニュアルでの表記		正式名称
AIX※		AIX 6.1
		AIX 7.1
Collaboration	Groupmax Collaboration	Groupmax Collaboration Portal 07-50 以降
		Groupmax Collaboration Web Client - Forum/File Sharing 07-50 以降
		Groupmax Collaboration Web Client - Mail/Schedule 07-50 以降
	uCosminexus Collaboration	uCosminexus Collaboration Portal 06-50 以降
		uCosminexus Collaboration Portal - Forum/File Sharing 06-50 以降
Cosminexus		uCosminexus Application Server Enterprise
		uCosminexus Application Server Standard
		uCosminexus Client
		uCosminexus Service Platform
		uCosminexus Web Redirector
EUR		EUR Print Service - Portable Document Format option 07-60 以降
		EUR Print Service 07-60 以降
		uCosminexus EUR Print Service Enterprise 08-00 以降
		uCosminexus EUR Server Standard 09-00 以降
		uCosminexus EUR Server Enterprise 09-00 以降
HiRDB		HiRDB/Parallel Server Plus Version 8 08-04 以降
		HiRDB/Parallel Server Plus Version 8(64) 08-04 以降
		HiRDB/Parallel Server Version 8 08-04 以降
		HiRDB/Parallel Server Version 8(64) 08-04 以降
		HiRDB/Single Server Plus Version 8 08-04 以降
		HiRDB/Single Server Plus Version 8(64) 08-04 以降
		HiRDB/Single Server Version 8 08-04 以降
		HiRDB/Single Server Version 8(64) 08-04 以降
Hitachi Storage Command Suite		Hitachi Device Manager Software 6.0 以降または JP1/HiCommand Device Manager 5.6 以降
		Hitachi Dynamic Link Manager Software 6.0 以降

このマニュアルでの表記			正式名称
			Hitachi Provisioning Manager Software 6.0 以降または JP1/HiCommand Provisioning Manager 5.6 以降
			Hitachi Replication Manager Software 6.0 以降または JP1/HiCommand Replication Monitor 5.6 以降
			Hitachi Tiered Storage Manager Software 6.0 以降または JP1/Tiered Storage Manager 5.7 以降
			JP1/HiCommand Global Link Availability Manager 5.6 以降
Hitachi Command Suite			Hitachi Device Manager Software 7.0 以降
			Hitachi Tiered Storage Manager Software 7.0 以降
			Hitachi Replication Manager Software 7.0 以降
			Hitachi Tuning Manager Software 7.0 以降
			Hitachi Compute Systems Manager Software 7.4 以降
			Hitachi Global Link Manager Software 7.2 以降
HP-UX※または HP-UX (IPF)			HP-UX 11i V3 (IPF)
JP1/AJS	JP1/AJS2	JP1/AJS2 - Manager	JP1/Automatic Job Management System 2 - Manager
		JP1/AJS2 - SO	JP1/Automatic Job Management System 2 - Scenario Operation Manager
			JP1/Automatic Job Management System 2 - Scenario Operation View
		JP1/AJS2 - View	JP1/Automatic Job Management System 2 - View
	JP1/AJS3	JP1/AJS3 - Manager	JP1/Automatic Job Management System 3 - Manager
		JP1/AJS3 - View	JP1/Automatic Job Management System 3 - View
JP1/AO			JP1/Automatic Operation
JP1/Audit			JP1/Audit Management - Manager
JP1/IM - NP			JP1/Integrated Management - Navigation Platform
JP1/IM - SS			JP1/Integrated Management - Service Support
JP1/ITDM			JP1/IT Desktop Management - Manager
JP1/ITDM2			JP1/IT Desktop Management 2 - Manager
JP1/ITRM			JP1/IT Resource Management - Manager
JP1/NETM/AIM			JP1/NETM/Asset Information Manager
JP1/NETM/CSC		JP1/NETM/CSC - Agent	JP1/NETM/Client Security Control - Agent

このマニュアルでの表記		正式名称
	JP1/NETM/CSC - Manager	JP1/NETM/Client Security Control - Manager
	JP1/NETM/CSC - Manager Remote Option	JP1/NETM/Client Security Control - Manager Remote Option
JP1/NETM/DM	JP1/NETM/DM Client	JP1/NETM/DM Client
		JP1/NETM/DM Client - Base
	JP1/NETM/DM Manager	JP1/NETM/DM Manager
JP1/NETM/NM		JP1/NETM/Network Monitor - Manager
JP1/PFM	JP1/PFM - Base	JP1/Performance Management - Base
	JP1/PFM - Manager	JP1/Performance Management - Manager
JP1/SS		JP1/Service Support
JP1/秘文または JP1/秘文 Advanced Edition		JP1/秘文 Advanced Edition サーバ
Linux※	Linux 5 (AMD64 & Intel EM64T)	Red Hat Enterprise Linux(R) 5 (AMD64 & Intel EM64T)
	Linux 5 (x86)	Red Hat Enterprise Linux(R) 5 (x86)
	Linux 6.1 (AMD/Intel 64)	Red Hat Enterprise Linux(R) 6.1 (AMD/Intel 64)
	Linux 6.1 (x86)	Red Hat Enterprise Linux(R) 6.1 (x86)
	Linux 7.1 (AMD/Intel 64)	Red Hat Enterprise Linux(R) 7.1 (AMD/Intel 64)
	Oracle Linux 6 (AMD64 & EM64T)	Oracle Linux 6 (AMD64 & EM64T)
	Oracle Linux 7 (AMD64 & EM64T)	Oracle Linux 7 (AMD64 & EM64T)
	SUSE Linux Enterprise Server 12 (AMD64 & EM64T)	SUSE Linux Enterprise Server 12 (AMD64 & EM64T)
	CentOS 6 (AMD64 & EM64T)	CentOS 6 (AMD64 & EM64T)
	CentOS 7 (AMD64 & EM64T)	CentOS 7 (AMD64 & EM64T)
Oracle		Oracle 9i
		Oracle 10g
		Oracle Database 11g
		Oracle 11g Release 2
		Oracle Database 12c

このマニュアルでの表記	正式名称
Solaris※	Solaris 10
	Solaris 11
uCosminexus Portal Framework	uCosminexus Portal Framework
	uCosminexus Portal Framework - Light
VOS3	Virtual-storage Operating System 3

注※

OS による機能差がない場合，HP-UX，Solaris，AIX，および Linux を総称して UNIX と表記します。

付録 G.3　このマニュアルで使用する英略語

このマニュアルで使用する英略語を，次の表に示します。

英略語	正式名称
CSV	Comma Separated Value
DB	Database
FTP	File Transfer Protocol
GUI	Graphical User Interface
IP	Internet Protocol
IPF	Itanium (R) Processor Family
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PDF	Portable Document Format
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
Web	World Wide Web

付録 G.4　KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイトです。

付録 H　用語解説

(英字)

Collaboration

同じ目的や問題意識を持つ人が既存の組織を越えて集まり，協働作業の場所で情報を共有・交換して業務を進めていくための製品です。Collaboration には「Groupmax Collaboration」と「uCosminexus Collaboration」の 2 種類があります。

Cosminexus

アプリケーションサーバを中核とした，性能および信頼性の高い業務アプリケーションを実行および開発するためのシステム構築基盤製品です。

EUR（イーユーアール）

表形式のデータを入力して帳票を印刷するプログラムです。難しいプログラム作成や入力元のデータ形式を気にすることなく，さまざまな帳票を設計する機能を提供しています。

HiRDB

業務の規模に応じたリレーショナルデータベースを構築できるようにする，データベース管理システム（DBMS）の製品です。

Hitachi Storage Command Suite

Hitachi Storage Command Suite は，ストレージシステムの構築・運用・監視を支援するプログラムです。

JP1/AJS

JP1/AJS は，業務を自動的に運用するためのプログラムです。処理を順序づけて定期的に実行したり，特定の事象が発生したときに処理を開始したりできます。なお，JP1/Audit Management - Manager では，JP1/AJS2 と JP1/AJS3 を標準サポートとしています。

JP1/Audit Management - Manager

内部統制の有効性を評価するために必要な証跡記録を一元管理し，内部統制の報告書作成や監査業務を支援するプログラムです。

ユーザ情報やシステム構成の変更などの証跡記録を利用して，業務の正当性を確認したり，リソースへの操作やアクセス状況を監査したりできます。

JP1/Base

JP1 イベントの送受信や，ユーザの管理，起動の制御などの機能を提供するプログラムです。JP1/Base は，JP1/Audit Management - Manager や JP1/AJS などの前提プログラムです。

JP1/ITDM

組織内のセキュリティ対策や IT 資産管理を実現する製品です。業務に沿ったわかりやすい操作性，シンプルな設定項目やスケジューリングによる自動化機能を備え，セキュリティ管理や資産管理の観点から IT 機器の管理を支援します。JP1/Audit Management - Manager では，JP1/ITDM と JP1/ITDM2 を標準サポートとしています。

JP1/ITRM

多様化・複雑化する IT リソースの構成情報を一元管理して，IT リソースの効率的な運用を支援する製品です。仮想化によるサーバの統合やシステム構成の変更など，環境の変化に柔軟に対応して IT リソースを最適化する方法を提供します。

JP1/NETM/AIM

IT 資産を管理する場合に発生する問題の解決を支援する製品です。情報を一元管理して，IT 資産を効率良く管理する方法を提供します。

JP1/NETM/CSC

クライアントをセキュリティ管理するプログラムです。事前に定義された判定ポリシーによってクライアントの危険レベルを判定し，判定の結果を基に危険レベルに応じたアクションを実行します。

JP1/NETM/DM

ソフトウェアの配布およびクライアントの管理を，ネットワークを利用して一括で実行するシステムの総称です。

JP1/NETM/NM

許可されていない PC の企業内 LAN（TCP/IP ネットワーク）への接続を検出し，ネットワークから切り離すことで，企業のネットワークを保護するシステムです。ネットワーク管理者が管理していない PC を排除し，ウィルス感染や情報漏洩など，セキュリティ上の問題発生を防止します。

JP1/PFM

システムのパフォーマンスに関する問題を監視および分析するためプログラムです。プラットフォームが混在している分散システムで，データベース，アプリケーションプログラム，アプリケーションサーバなどの稼働状況を，一元的に監視できます。

JP1/秘文

さまざまな状況で企業内の機密データの漏えいを防止する製品です。クライアントが保持しているデータを暗号化する機能，FD などのリムーバブルメディアへの持ち出しを禁止する機能などを提供します。

JP1 イベント

システムで何らかの事象（ジョブの実行結果，サービスのエラーなど）が発生したときに通知される事象です。

JP1 権限レベル

管理対象に対して JP1 ユーザがどのような操作ができるかを表しています。イベントなどの管理対象の種類に応じて，操作項目を定めています。管理対象の種類と，それに対する操作項目の幾つかを組み合わせた形式で JP1 ユーザのアクセス権限を管理します。

JP1 ユーザ

JP1/Audit Management - Manager や JP1/AJS を使用する場合の JP1 専用のアカウントです。JP1 ユーザは，認証サーバに登録され，他ホストへのアクセス権限を認証サーバで管理されます。OS に登録されているユーザとは異なる場合があります。

OpenTP1

オープンシステム上でオンライントランザクション処理をできるようにする製品です。

TRUST E2

計算機システムの利用者の管理と，データセットなどの計算機資源（リソース）の機密保護を目的とするプログラムです。

uCosminexus Portal Framework

企業ポータルを構築および運用するフレームワークです。企業の内外にある多種多様なコンテンツ・業務システムの情報を集約する機能や，集約した情報をユーザ一人一人に対して最適な情報になるように組み合わせて提供する機能などを備えています。

XDM/BASE E2

複合化，大規模化，および多様化するシステムに対応し，高信頼・高性能 DB/DC システムを実現した XDM E2（Extensible Data Manager Extended Version 2）の標準プログラムです。

（ア行）

イベントサーバ

JP1/Base で JP1 イベントを管理する機能を持つプログラムです。イベントサーバを起動すると，JP1 イベントを収集・配布できる状態になります。通常，JP1/Base ではホスト名に対応するイベントサーバを使用しますが，監査ログ収集対象サーバの JP1/Base では，監査ログの収集だけに使用するイベントサーバを作成して使用します。

イベントサービス

システム内で発生した事象を JP1 イベントとして登録および管理する JP1/Base の機能です。

イベントログトラップ機能

Windows のイベントログを JP1 イベントに変換する JP1/Base の機能です。

（カ行）

活文 NAVIstaff

ドキュメントの運用を管理する製品です。ドキュメントを統制して，公開が必要なドキュメントを適切に保護することで，情報流出や不適切な利用を防止します。

監査証跡管理システム

JP1/Audit Management - Manager を導入して構築するシステムの総称です。

内部統制に基づいて，企業内の各 IT システムが許可された権限で正しく操作が実行されているかどうかなど，企業内の内部統制が規則どおりに機能していることを証明するために必要な証跡記録を収集し，一元管理や長期間にわたる保存管理を実現します。

監査ログ

内部統制の証跡記録として出力されるログのことです。「いつ」「だれが」「どこで」「何を」を示し，システムの内部統制の評価と監査に利用します。

監査ログ閲覧サーバ

監査ログのバックアップを閲覧するための閲覧専用サーバです。監査ログ管理サーバで収集・管理していた監査ログのバックアップファイルを監査ログ閲覧サーバにインポートすることによって，監査ログを閲覧できます。

監査ログ管理画面

監査ログの検索・集計やバックアップ履歴などの管理に使用する監査証跡管理システムの画面です。

監査ログ管理サーバ

監査ログを一元管理し，監査ログに関するサービスを提供するサーバです。

監査ログ管理データベース

監査ログを格納するデータベースです。JP1/Audit Management - Manager に組み込まれているデータベースを使用します。

監査ログ収集対象サーバ

JP1/Audit Management - Manager がログ収集を行う対象のサーバです。JP1/Base および監査ログを収集する JP1/AJS3 や JP1/NETM/DM などのプログラムがインストールされているサーバです。

監査ログの正規化

監査ログ収集対象サーバの各プログラムが出力する監査ログの出力形式を，JP1/Audit Management - Manager の監査ログ管理データベースが管理する監査ログの形式に変換することです。

クラスタシステム

クラスタシステムとは，複数のサーバシステムを連携して一つのシステムとして運用するシステムで，トラブルが発生しても業務を継続できるようにすることを目的としています。この処理を引き継ぐことをフェールオーバーといいます。業務を実行中のサーバ（実行系）でトラブルが発生すると，待機していた別のサーバ（待機系）が業務の処理を引き継ぎます。実行「系」から待機「系」へ業務を切り替えるため，「系切り替えシステム」とも呼びます。

なお，クラスタシステムの種類には，複数のサーバが並列処理をして負荷分散することを目的としたシステム構成などもありますが，このマニュアルでは，フェールオーバーによって業務の中断を防ぐ機能のことだけを指します。

系切り替えシステム

クラスタシステムを参照してください。

（サ行）

証跡記録

監査の証拠となる情報のことです。企業内の内部統制が規則どおりに機能していることを証明するために必要な情報として収集します。

正規化ルールエディタ

JP1/Audit Management - Manager の機能のうち，正規化ルールを定義する GUI のことです。

正規化ルールファイル

監査証跡管理システムでは，各監査ログ収集対象サーバから収集した監査ログを統一したフォーマットで管理するために，次に示す監査ログの正規化ルールファイルを提供しています。

- 統一フォーマット用の正規化ルールファイル
- JP1/AJS2 の製品ログ用の正規化ルールファイル
- JP1/AJS3 の製品ログ用の正規化ルールファイル
- Windows イベントログ用の正規化ルールファイル

（タ行）

テンプレート

検索パターンおよび集計パターンのひな型で，収集対象プログラムごとに用意されています。テンプレートをそのまま利用したり，カスタマイズして利用したりすることによって，検索・集計を効率的に実施できます。

統計結果

生成された統計情報を基に，監査ログ統計画面からグラフ形式で表示したり，CSV 形式ファイルで出力したりする，統計の結果を表すデータのことです。

統計情報

収集した監査ログを基に，監査ログ管理データベースに生成される統計データのことです。

（ナ行）

内部統制

企業の内部で社会に大きな影響を与える違法行為や不正などがなく，業務が正しく行われ，組織が健全に運営されるために必要な基準や手続きを定め，その基準や手続きに基づいて管理・監視・保証を行うことを指します。

認証サーバ

JP1 ユーザのアクセス権限を管理するサーバです。一つのユーザ認証圏に 1 台設置する必要があります。このサーバを利用して JP1 ユーザを一括で管理します。JP1/Audit Management - Manager を導入する場合，JP1 ユーザ名をこのサーバに登録する必要があります。

（ハ行）

フェールオーバー

JP1 を実行するサーバにトラブルが発生した場合に，ほかの正常なサーバに JP1 を移動させて処理を続行することです。または，システム管理者の操作によって，JP1 を実行するサーバを切り替えることです。

実行系サーバから待機系サーバにフェールオーバーするため，系切り替えともいいます。

物理ホスト

クラスタシステムを構成する各サーバに固有な環境のことです。物理ホストの環境は，フェールオーバー時にはほかのサーバに引き継がれません。

プロセス

Windows の場合のサービスプログラム，UNIX の場合のデーモンプログラムなどを示します。

（ヤ行）

ユーザ認証圏

分散システム内で認証サーバが管理するホスト群の範囲を表しています。JP1 ユーザは，認証サーバが管理するホスト群に対してジョブの実行，コマンドの実行，自動アクションなどの各種操作ができます。JP1/Audit Management - Manager を導入する場合，ユーザ認証圏を決める必要があります。

ユーザマッピング

JP1 ユーザに，OS に登録されているユーザの権限を与える機能です。

JP1 ユーザとして認証サーバに登録されたユーザが，各ホストの OS に登録されているユーザの権限で各ホストの操作を実行できるようになります。

（ラ行）

ルート

機能ツリーの最上位にあるツリー項目です。「監査ログ管理」という名称で表示されます。

ログファイルトラップ機能

アプリケーションプログラムがログファイルに出力するログを JP1 イベントに変換する JP1/Base の機能です。

論理ホスト

クラスタ環境での運用時に JP1 の実行環境となる論理上のサーバのことです。トラブルの発生時には，論理ホスト単位でフェールオーバーします。

論理ホストは専用の IP アドレスと共有ディスクを持ち，フェールオーバー時にはその IP アドレスと共有ディスクを引き継いで動作します。そのため，トラブルで物理的なサーバが切り替わった場合も，ほかのホストからは同じ IP アドレスでアクセスでき，一つのホストが常に動作しているように見えます。

索引

A

AccessControl〔監査ログの収集カテゴリ〕 63
admagtinstall〔コマンド〕 448
admagtsetup〔コマンド〕 451
admcoldata〔コマンド〕 457
admcsvmove〔コマンド〕 459
admcsvmove コマンドの概念〔機能〕 73
admcsvremove〔コマンド〕 461
admdbbackup〔コマンド〕 463
admdbdelete〔コマンド〕 465
admdbdelete コマンドの概念〔機能〕 71
admdbexport〔コマンド〕 468
admdbimport〔コマンド〕 470
admdbrorg〔コマンド〕 473
admdbstat〔コマンド〕 475
admdbstop〔コマンド〕 477
admexport〔コマンド〕 479
admexport コマンドの概念〔機能〕 72
admhasetup〔コマンド〕 484
admimport〔コマンド〕 487
admimport コマンドの概念〔機能〕 72
admlog.vbs〔コマンド〕 490
admrrexport〔コマンド〕 492
admrrimport〔コマンド〕 494
admstdel〔コマンド〕 497
admstgen〔コマンド〕 499
admuxlogcol〔コマンド〕 501
AIX のテンプレートの検索パターンおよび集計パターン 439
AnomalyEvent〔監査ログの収集カテゴリ〕 64
Authentication〔監査ログの収集カテゴリ〕 63

C

Collaboration のテンプレートの検索パターンおよび集計パターン 427
Collaboration〔用語解説〕 902
ConfigurationAccess〔監査ログの収集カテゴリ〕 63
ContentAccess〔監査ログの収集カテゴリ〕 64
Cosminexus のテンプレートの検索パターンおよび集計パターン 429
Cosminexus〔用語解説〕 902
CSV 形式ファイルを出力する場合〔監査ログの検索〕 296
CSV 形式ファイルを出力する場合〔監査ログの集計〕 316
CSV 形式ファイルを出力する場合〔監査ログの統計〕 328
CSV 形式ファイルを出力する場合〔監査ログレポート〕 302

E

EUR（イーユーアール）〔用語解説〕 902
EUR をインストールする 136
ExternalService〔監査ログの収集カテゴリ〕 64

F

Failure〔監査ログの収集カテゴリ〕 63
forward ファイル〔転送設定ファイル（サーバ内の転送）〕 171

H

HiRDB/EmbeddedEdition _AL1 226
HiRDB のテンプレートの検索パターンおよび集計パターン 429
HiRDB〔用語解説〕 902
Hitachi Navigation Platform のテンプレートの検索パターンおよび集計パターン 442
Hitachi Storage Command Suite の監査ログ出力情報 854
Hitachi Storage Command Suite のテンプレートの検索パターンおよび集計パターン 430
Hitachi Storage Command Suite のログ（Windows の場合） 58
Hitachi Storage Command Suite〔用語解説〕 902

HP-UX のテンプレートの検索パターンおよび集計パターン　439
HTML 形式ファイルを出力する場合〔監査ログの統計〕　330

I

IIS Admin Service　226
IIS 受信バッファの最大サイズの設定　184
IIS 送信バッファの最大サイズの設定　183
IIS マネージャ　182

J

JP1_Audit_Admin〔JP1 権限レベル〕　76
JP1_Audit_Operator〔JP1 権限レベル〕　76
JP1/AJS2 および JP1/AJS3 の監査ログ（スケジューラログ）出力情報　856
JP1/AJS2 のテンプレートの検索パターンおよび集計パターン　430
JP1/AJS3 のテンプレートの検索パターンおよび集計パターン　430
JP1/AJS 製品ログ用の正規化ルールファイル　66
JP1/AJS〔用語解説〕　902
JP1/AO のテンプレートの検索パターンおよび集計パターン　431
JP1/Audit Management - Manager　23
JP1/Audit Management - Manager が対応するプログラムの監査ログ一覧　848
JP1/Audit Management - Manager で監査ログの収集対象を設定する　215
JP1/Audit Management - Manager で使用するポート番号の変更方法　828
JP1/Audit Management - Manager の仮想ディレクトリのファイル一覧　820
JP1/Audit Management - Manager の監査ログ出力　84
JP1/Audit Management - Manager の監査ログの出力情報　840
JP1/Audit Management - Manager のバージョンアップ　233
JP1/Audit Management - Manager のバージョンアップ（クラスタ環境）　274
JP1/Audit Management - Manager のバージョンアップの手順　233
JP1/Audit Management - Manager のバージョンアップの手順（クラスタ環境）　275
JP1/Audit Management - Manager のバージョンアップの流れ　233
JP1/Audit Management - Manager のバージョンアップの流れ（クラスタ環境）　274
JP1/Audit Management - Manager のバックアップ　810
JP1/Audit Management - Manager のファイル一覧　813
JP1/Audit Management - Manager のポート番号　827
JP1/Audit Management - Manager のリストア　810
JP1/Audit Management - Manager〔用語解説〕　902
JP1/Audit Management - Manager をアンインストールする　144
JP1/Audit Management - Manager をアンインストールする（クラスタ環境）　247
JP1/Audit Management - Manager を上書きインストールする　142
JP1/Audit Management - Manager を上書きインストールする（クラスタ環境）　245
JP1/Audit Management - Manager を新規インストールする　137
JP1/Audit Management - Manager を新規インストールする（クラスタ環境）　244
JP1/Audit のテンプレートの検索パターンおよび集計パターン　431
JP1/Base Event　162, 226
JP1/Base EventlogTrap　177
JP1/Base Event 監査ログ専用イベントサーバ名サービスのリソース　261
JP1/Base の API 設定ファイル（api ファイル）を編集する　187
JP1/Base の jevsend コマンドを実行する　186
JP1/Base のイベントサービスを設定する　151
JP1/Base のイベントサービスを設定する（クラスタ環境）　259

JP1/Base のイベントログトラップ機能を設定する 165
JP1/Base のテンプレートの検索パターンおよび集計パターン 431
JP1/Base のユーザ管理機能を設定する 185
JP1/Base のユーザ管理機能を使ったユーザ管理 75
JP1/Base〔用語解説〕 902
JP1/Base をインストールする 136, 146
JP1/Base をセットアップする（クラスタ環境） 250
JP1/IM - NP のテンプレートの検索パターンおよび集計パターン 432
JP1/IM - SS のテンプレートの検索パターンおよび集計パターン 432
JP1/ITDM2 のテンプレートの検索パターンおよび集計パターン 433
JP1/ITDM のテンプレートの検索パターンおよび集計パターン 432
JP1/ITDM〔用語解説〕 903
JP1/ITRM のテンプレートの検索パターンおよび集計パターン 433
JP1/ITRM〔用語解説〕 903
JP1/NETM/AIM のテンプレートの検索パターンおよび集計パターン 434
JP1/NETM/AIM〔用語解説〕 903
JP1/NETM/Audit LogTrap 論理ホスト名サービスのリソース 261
JP1/NETM/CSC のテンプレートの検索パターンおよび集計パターン 434
JP1/NETM/CSC〔用語解説〕 903
JP1/NETM/DM のテンプレートの検索パターンおよび集計パターン 434
JP1/NETM/DM〔用語解説〕 903
JP1/NETM/NM のテンプレートの検索パターンおよび集計パターン 435
JP1/NETM/NM〔用語解説〕 903
JP1/PFM のテンプレートの検索パターンおよび集計パターン 435
JP1/PFM〔用語解説〕 903
JP1/秘文のテンプレートの検索パターンおよび集計パターン 436
JP1/秘文〔用語解説〕 903
JP1 イベント〔用語解説〕 904
JP1 権限レベル〔機能〕 76
JP1 権限レベル〔システム設計〕 121
JP1 権限レベル〔用語解説〕 904
JP1 ユーザ名 186
JP1 ユーザ〔用語解説〕 904

K

KFPH00211-I〔データベースのメッセージ〕 805
KFPH00212-I〔データベースのメッセージ〕 805

L

LinkStatus〔監査ログの収集カテゴリ〕 63
Linux のテンプレートの検索パターンおよび集計パターン 439

M

Maintenance〔監査ログの収集カテゴリ〕 64
ManagementAction〔監査ログの収集カテゴリ〕 64
Microsoft Internet Information Services をインストールする 136
Microsoft Internet Information Services をセットアップする 182
Microsoft Internet Information Services をセットアップする（クラスタ環境） 249

N

ntevent.conf〔動作定義ファイル（イベントログトラップ機能の設定）〕 166

O

OpenTP1 のテンプレートの検索パターンおよび集計パターン 436
OpenTP1〔用語解説〕 904
Oracle の監査ログ出力情報 870
Oracle のテンプレートの検索パターンおよび集計パターン 437
Oracle のログ 58
OS 起動時に監査ログの監視を開始する〔収集対象の設定〕 219

P

PDF ファイルを出力する場合〔監査ログの検索〕 297

PDF ファイルを出力する場合〔監査ログの集計〕 316

S

services ファイルを確認する 185

Solaris のテンプレートの検索パターンおよび集計パターン 439

StartStop〔監査ログの収集カテゴリ〕 63

T

TRUST E2 のテンプレートの検索パターンおよび集計パターン 437

TRUST E2〔用語解説〕 904

U

uCosminexus EUR Server のテンプレートの検索パターンおよび集計パターン 442

uCosminexus Navigation Platform のテンプレートの検索パターンおよび集計パターン 437

uCosminexus Portal Framework のテンプレートの検索パターンおよび集計パターン 438

uCosminexus Portal Framework〔用語解説〕 904

UNIX システムログ 59

UNIX システムログ情報の変換 501

UNIX システムログに出力される監査ログの収集をやめる 238

UNIX システムログの監査ログ出力情報 871

UNIX システムログの変換設定をする 178

UNIX のテンプレートの検索パターンおよび集計パターン 438

W

Windows イベントログ 58

Windows イベントログ（セキュリティに関する情報）の監査ログ出力情報（Windows Server 2003 および Windows XP の場合） 873

Windows イベントログ（セキュリティに関する情報）の監査ログ出力情報（Windows Server 2012 または Windows Server 2008 の場合） 877

Windows イベントログ（セキュリティに関する情報）用の正規化ルールファイル 66

Windows イベントログに出力される監査ログ 58

Windows イベントログに出力される監査ログの収集をやめる 236

Windows のテンプレートの検索パターンおよび集計パターン 440

World Wide Web Publishing Service 226

X

XDM/BASE E2 のテンプレートの検索パターンおよび集計パターン 441

XDM/BASE E2〔用語解説〕 904

あ

アクセス制御 76

新たに構築するサーバのプログラムを収集対象とする場合 370

い

移行先サーバ 390

移行元サーバ 390

イベントサーバ〔用語解説〕 904

イベントサービス〔用語解説〕 904

イベントログトラップ機能〔用語解説〕 905

印刷する場合〔監査ログレポート〕 303

印刷する場合〔グラフ表示の集計結果〕 320

う

運用の変化に対応して監査ログの収集対象を追加・解除する 50

運用方法の検討 116

お

オペレーション管理 28

か

概要 23

各バージョンの変更内容 882

活文 NAVIstaff のテンプレートの検索パターンおよび集計パターン 442

活文 NAVIstaff〔用語解説〕 905
監査証跡管理システム 24
監査証跡管理システムで管理できる情報の種類 27
監査証跡管理システムで収集できるプログラムの種類 29
監査証跡管理システムの特長 26
監査証跡管理システムの目的 24
監査証跡管理システム〔用語解説〕 905
監査証跡管理システムを利用した内部統制の運用サイクル 51
監査ポリシー〔Windows〕 165
監査目的に合わせた検索・集計 33
監査ログ 26
監査ログ閲覧サーバ 34
監査ログ閲覧サーバで監査ログを閲覧する 48
監査ログ閲覧サーバの運用例〔運用方法の検討〕 118
監査ログ閲覧サーバのセットアップ 229
監査ログ閲覧サーバの前提 OS 93
監査ログ閲覧サーバの前提プログラム 97
監査ログ閲覧サーバのプログラム構成 88
監査ログ閲覧サーバのプログラムのインストール 228
監査ログ閲覧サーバ〔用語解説〕 905
監査ログ閲覧サーバを構築した構成 103
監査ログ管理画面からログアウトする 287
監査ログ管理画面での運用 281
監査ログ管理画面での操作 282
監査ログ管理画面でのトラブル 803
監査ログ管理画面にログインする 286
監査ログ管理画面の概要と表示設定 395
監査ログ管理画面の各部の名称と使い方 396
監査ログ管理画面のカスタマイズ〔機能〕 82
監査ログ管理画面の操作の流れ 282
監査ログ管理画面の表示設定 335
監査ログ管理画面の表示編集 285
監査ログ管理画面へのログインとログアウト 286
監査ログ管理画面〔用語解説〕 905
監査ログ管理画面を使うための Internet Explorer の設定 231
監査ログ管理機能 283
監査ログ管理サーバ〔概要〕 26
監査ログ管理サーバクラスタグループ 255
監査ログ管理サーバ〔収集の仕組み〕 57
監査ログ管理サーバで監査ログを収集するための設定 204
監査ログ管理サーバで監査ログを収集するための設定（クラスタ環境） 270
監査ログ管理サーバでリソースを作成する 254
監査ログ管理サーバの開始・停止 226
監査ログ管理サーバの開始・停止（クラスタ環境） 271
監査ログ管理サーバの環境設定をする 189
監査ログ管理サーバの環境設定をする（クラスタ環境） 250
監査ログ管理サーバのセットアップ 182
監査ログ管理サーバのセットアップ（クラスタ環境） 249
監査ログ管理サーバの前提 OS 93
監査ログ管理サーバの前提プログラム 96
監査ログ管理サーバのデータベースをアップグレードする 203
監査ログ管理サーバのデータベースをアップグレードする（クラスタ環境） 253
監査ログ管理サーバのデータベースをセットアップする 198
監査ログ管理サーバのデータベースをセットアップする（クラスタ環境） 252
監査ログ管理サーバのバックアップおよびリストア 810
監査ログ管理サーバのプログラム構成 86
監査ログ管理サーバのプログラムのインストール 136
監査ログ管理サーバのプログラムのインストール（クラスタ環境） 244
監査ログ管理サーバ〔用語解説〕 905
監査ログ管理サーバを開始する 226
監査ログ管理サーバを開始する（クラスタ環境） 271
監査ログ管理サーバを開始または停止する場合の注意事項（クラスタ環境） 272
監査ログ管理サーバを停止する 226
監査ログ管理サーバを停止する（クラスタ環境） 271
監査ログ管理データベース〔概要〕 26

監査ログ管理データベース〔機能〕 68
監査ログ管理データベース〔収集の仕組み〕 57
監査ログ管理データベース〔用語解説〕 905
監査ログ検索〔運用〕 288
監査ログ検索画面 403
監査ログ検索画面の表示項目を設定する 335
監査ログ検索画面の表示設定項目 336
監査ログ検索画面をカスタマイズする〔運用〕 335
監査ログ検索画面を初期化する〔運用〕 336
監査ログ検索画面・監査ログ集計画面・バックアップ履歴画面の表示項目の設定 414
監査ログ検索結果の確認 294
監査ログ検索結果のレポート表示 299
監査ログ検索パターンの編集 303
監査ログ集計〔運用〕 307
監査ログ集計画面 407
監査ログ集計画面の表示項目を設定する 337
監査ログ集計画面の表示設定項目 338
監査ログ集計画面をカスタマイズする〔運用〕 337
監査ログ集計画面を初期化する〔運用〕 338
監査ログ集計結果の確認 313
監査ログ集計結果のグラフ表示 318
監査ログ集計結果をグラフ表示する場合 320
監査ログ集計パターンの編集 320
監査ログ収集対象サーバ〔概要〕 26
監査ログ収集対象サーバ〔収集の仕組み〕 58
監査ログ収集対象サーバセットアップ定義ファイル 547
監査ログ収集対象サーバで JP1/Base をセットアップする（クラスタ環境） 258
監査ログ収集対象サーバでリソースを作成する 261
監査ログ収集対象サーバに配布されるファイル一覧 823
監査ログ収集対象サーバの開始・停止（クラスタ環境） 273
監査ログ収集対象サーバのセットアップ 147
監査ログ収集対象サーバのセットアップ（クラスタ環境） 258
監査ログ収集対象サーバの前提 OS 94
監査ログ収集対象サーバの前提プログラム 98
監査ログ収集対象サーバのファイルのインストール〔コマンド〕 448
監査ログ収集対象サーバのプログラム構成 90
監査ログ収集対象サーバのプログラムのインストール 146
監査ログ収集対象サーバのプログラムのインストール（クラスタ環境） 257
監査ログ収集対象サーバ〔用語解説〕 905
監査ログ収集対象サーバを開始する（クラスタ環境） 273
監査ログ収集対象サーバを開始または停止する場合の注意事項（クラスタ環境） 273
監査ログ収集対象サーバを停止する（クラスタ環境） 273
監査ログ収集対象の解除 235
監査ログ収集対象の解除（クラスタ環境） 276
監査ログ収集対象の確認と変更 363
監査ログ収集対象プログラムをインストールする 146
監査ログ収集対象プログラムをセットアップする 181
監査ログ収集対象を解除する 372
監査ログ収集対象を追加する 370
監査ログ収集対象を追加する手順 370
監査ログ収集対象を追加するときの事前準備 370
監査ログ収集対象を編集する 371
監査ログ専用イベントサーバ 147
監査ログ専用イベントサーバの環境セットアップ〔コマンド〕 451
監査ログ専用イベントデータベース 147
監査ログ専用イベントデータベース切り替え時の収集 62
監査ログ専用ディレクトリ 151
監査ログ専用フォルダ 151
監査ログ退避ファイルサイズ〔監査ログ収集情報〕 197
監査ログ退避フォルダ〔監査ログ収集情報〕 197
監査ログ統計〔運用〕 324
監査ログ統計画面 410
監査ログ統計画面の表示項目の設定と統計パターンの設定 416
監査ログ統計画面の表示項目を設定する 339
監査ログ統計画面の表示設定項目 340

監査ログ統計画面をカスタマイズする〔運用〕 340
監査ログ統計画面を初期化する〔運用〕 340
監査ログ統計結果の確認 327
監査ログ統計結果をグラフ形式で表示する場合 327
監査ログ統計情報の収集時生成〔監査ログ統計情報〕 196
監査ログ統計パターンの設定 330
監査ログに出力される事象の種別 840
監査ログの一元管理 68
監査ログのインポート〔コマンド〕 487
監査ログの監視の自動開始 373
監査ログの監視を開始する 372
監査ログの監視を停止する 373
監査ログの検索 288
監査ログの検索〔機能〕 77
監査ログの検索条件項目 290
監査ログの検索手順 288
監査ログの検索と集計 77
監査ログのコマンドを使用した管理 71
監査ログの集計 307
監査ログの集計〔機能〕 78
監査ログの集計条件項目 309
監査ログの集計手順 308
監査ログの収集 56
監査ログの収集カテゴリ 63
監査ログの収集〔コマンド〕 457
監査ログの収集時期の決定〔運用方法の検討〕 116
監査ログの収集対象の検討 110
監査ログの収集対象の情報確認 365
監査ログの収集対象の設定変更 369
監査ログの収集タイミング〔機能〕 61
監査ログの収集の仕組み 56
監査ログの出力形式 843
監査ログの正規化 64
監査ログの正規化〔機能〕 64
監査ログの正規化でのトラブル 808
監査ログの正規化〔用語解説〕 906
監査ログの統計 324
監査ログの統計出力条件項目 325
監査ログの統計情報削除 497
監査ログの統計情報生成 499
監査ログの統計情報の生成と統計結果の出力 79
監査ログのバックアップ 356
監査ログのバックアップ運用 353
監査ログのバックアップ運用の流れ 354
監査ログのバックアップ〔コマンド〕 479
監査ログのバックアップと閲覧専用サーバの構築 34
監査ログのバックアップファイルの移動 360
監査ログのバックアップファイルの移動〔コマンド〕 459
監査ログのバックアップファイルのインポート 359
監査ログのバックアップファイルの削除 362
監査ログのバックアップファイルの削除〔コマンド〕 461
監査ログのバックアップ履歴管理 81
監査ログのバックアップを自動的に取得する 45
監査ログのフォーマットへの対応づけの検討 114
監査ログの保存形式 842
監査ログ標準レポート定義ファイル 534
監査ログファイルサイズ〔監査ログ管理画面監査ログ情報〕 195
監査ログファイルサイズ〔監査ログ情報〕 194
監査ログファイル出力〔監査ログ管理画面監査ログ情報〕 195
監査ログファイル出力〔監査ログ情報〕 194
監査ログファイル数〔監査ログ管理画面監査ログ情報〕 195
監査ログファイル数〔監査ログ情報〕 194
監査ログ〔用語解説〕 905
監査ログレポート一覧を表示する場合〔監査ログレポート〕 302
監査ログレポート画面 418
監査ログレポート定義ファイル 536
監査ログレポートの表示件数〔監査ログ管理画面情報〕 196
監査ログを出力するための設定 847
監査ログを正規化するための検討 112
監査ログを即時に収集する 374
監査ログを定期的に収集する 223

監査ログを定期的に収集する時刻や曜日を変更する 374
監査ログを利用して報告用資料を作成する 43

き

期間指定のバックアップ 356
企業内の IT システムが正しく運用されているかどうかを確認する 41
企業内の IT システムの運用実態について把握する 38
既存の検索パターンを利用する場合 304
既存の集計パターンを利用する場合 322
起動順序定義ファイル〔イベントログトラップ機能の自動起動設定〕 176
起動順序定義ファイル〔論理サーバの自動起動設定〕 161
機能 53
機能ツリー 398
機能ツリーのパターン表示編集 345
機能の概要 54
基本構成 102
共通出力項目 843
共有ディスクに引き継ぐ情報をコピーする 249

く

クライアントの構築の流れ 135
クライアントの前提 OS 96
クライアントの前提プログラム 101
クライアントのプログラム構成 91
クライアントのプログラムのインストール 230
クラスタ運用〔クラスタ情報〕 193
クラスタ環境での構成 104
クラスタ環境でのシステム構築 242
クラスタ環境でのシステム構築の流れ 243
クラスタシステム〔用語解説〕 906

け

系切り替えシステム〔用語解説〕 906
結果項目 415
権限管理 28
検索結果一覧 405
検索結果一覧を表示する場合〔監査ログの検索〕 296
検索パターン 303
検索パターンおよび集計パターンの一覧 426
検索パターンを削除する 305
検索パターンを作成する 303
検索パターンを変更する 305
検索パターンを利用する 289

こ

コマンド一覧 445
コマンドの詳細 447
コメント〔収集対象の設定〕 219
固有出力項目 845

さ

サーバ〔収集対象の設定〕 218
サーバの構築の流れ 133
サービス起動時の監査ログ収集〔監査ログ収集情報〕 197
サービス停止中の監査ログ退避〔監査ログ収集情報〕 197
サービス名〔データベース情報〕 192
作成した製品定義ファイルを削除する 376
作成した製品定義ファイルを編集する 375
差分指定のバックアップ 357

し

システム構成 85
システム構成の検討 122
システム構成例 102
システム構築 132
システム構築の流れ 133
システム設計 107
システム設計の流れ 108
システムの運用方法（クラスタ環境への導入有無） 119
システムの変更の概要 364
集計結果一覧 409
集計結果一覧を表示する場合〔監査ログの集計〕 315
集計結果グラフ表示画面 419

集計パターン　320
集計パターンを削除する　323
集計パターンを作成する　321
集計パターンを変更する　322
集計パターンを利用する　308
収集した監査ログの取り扱い方法　116
［収集対象の設定］ダイアログ〔収集対象の設定〕　217
障害発生時の保守資料採取〔コマンド〕　490
条件項目　415
証跡記録〔用語解説〕　906
新規に検索パターンを作成する場合　303
新規に集計パターンを作成する場合　321

す

すでに収集対象として設定されているサーバにプログラムを追加して収集対象とする場合　370
すべての監査ログの収集をやめる　238
すべての監査ログの収集をやめる〔クラスタ環境〕　276

せ

正規化ルールエディタで定義した製品用の正規化ルールファイル　66
正規化ルールエディタ〔用語解説〕　906
正規化ルールで定義できる監査ログの条件　112
正規化ルールのインポート　494
正規化ルールの定義方法を変更する場合の注意事項　115
正規化ルールのバックアップ　492
正規化ルールファイル〔機能〕　65
正規化ルールファイル〔製品定義の編集〕　214
正規化ルールファイル〔定義ファイル〕　506
正規化ルールファイルの作成例　830
正規化ルールファイル〔用語解説〕　906
製品定義ファイル　527
製品定義ファイルを作成して収集対象を追加する　375
製品定義ファイルを設定する　212
セットアップに必要なファイルをインストールする　148
セットアップに必要なファイルをインストールする（クラスタ環境）　258
前提 OS　93
前提 OS および前提プログラム　93
前提プログラム　96
前提プログラムをインストールする（クラスタ環境）　244

そ

操作画面のカスタマイズ　36
相対日数〔監査ログ統計情報〕　196
即時収集　63

た

代表的な運用方法の紹介　38

て

定期的な収集　62
定義ファイル　504
定義ファイル一覧　505
ディスク占有量の見積もり　127
データベースの CSV バックアップ　387
データベースの CSV バックアップ〔コマンド〕　468
データベースの CSV リストア　388
データベースの CSV リストア〔コマンド〕　470
データベースの運用方法　119
データベースのコマンドを使用した管理　70
データベースの再セットアップ　379
データベースの再編成　384
データベースの再編成〔コマンド〕　473
データベースの使用状況確認〔コマンド〕　475
データベースの使用状況に応じて対処する　392
データベースのセットアップ後に再セットアップが必要になる場合　380
データベースのセットアップ中に再セットアップが必要になる場合　379
データベースの停止〔コマンド〕　477
データベースのディスク容量の管理　392
データベースのデータ移行　390
データベースのデータ削除　391

データベースのデータ削除〔コマンド〕 465
データベースのトラブル 805
データベースのパスワード変更 385
データベースのバックアップ 380
データベースのバックアップ〔コマンド〕 463
データベースのメンテナンス 377
データベースのメンテナンスの概要 378
データベースのリストア 382
［データベースマネージャ］ダイアログ〔データベースのセットアップ〕 199, 203
データベースマネージャの起動方法 378
データベースマネージャを使用した管理 68
データベース容量の見積もり 128
デフォルトで登録されている検索パターンおよび集計パターン一覧 426
テンプレート〔用語解説〕 907

と

統一フォーマット用の正規化ルールファイル 66
統計結果 79
統計結果〔用語解説〕 907
統計出力条件 325
統計情報 79
統計情報〔用語解説〕 907
統計による事象推移の把握 34
統計パターン 330
統計パターン条件 79
動作定義ファイル 531
トラブルシューティング 799
トラブル発生時に一括採取する資料 801
トラブル発生時に個別採取する資料 801
トラブル発生時に採取が必要な資料 801
トラブル発生時の対処手順 800
トラブルへの対処方法 803

な

内部統制 24
内部統制の証跡記録の一元管理 26
内部統制の報告用資料や監査用資料の作成支援 35
内部統制〔用語解説〕 907

に

認証圏〔機能〕 75
認証サーバ〔機能〕 75
認証サーバ〔システム設計〕 121
認証サーバ〔用語解説〕 907

は

［パスワードの設定］ダイアログ〔データベース情報〕 192
パターン情報ファイル 541
パターン表示編集画面 420
パターン保存画面 425
パターン名やフォルダ名を変更する 347
パターンやフォルダの情報を移行する 352
パターンやフォルダの表示・非表示を設定する 351
パターンやフォルダを移動する 348
パターンやフォルダをコピーする 349
パターンやフォルダを削除する 351
パターンを保存するフォルダを作成する 346
バックアップオプション定義ファイル 539
バックアップの取得履歴を確認する 46
バックアップファイルの格納先フォルダの設定 182
バックアップファイルをダウンロードする 334
バックアップ履歴一覧 412
バックアップ履歴画面 412
バックアップ履歴画面の表示項目を設定する 342
バックアップ履歴画面の表示設定項目 343
バックアップ履歴画面をカスタマイズする〔運用〕 342
バックアップ履歴画面を初期化する〔運用〕 343
バックアップ履歴検索結果の確認 333
バックアップ履歴の確認 331
バックアップ履歴の検索条件項目 331
バックアップ履歴を検索する 331

ひ

表示設定画面 414
標準サポート外のプログラム 66

標準サポート外のプログラムを収集対象とするための準備をする　208
標準サポートしているプログラムを収集対象とするための準備をする　205
標準出力または標準エラー出力の場合〔メッセージの出力形式〕　553

ふ

ファイアウォールの通過方向　829
ファイル一覧　813
ファイルに出力される監査ログ　58
ファイルに出力される監査ログの収集をやめる　235
ファイルに出力される監査ログの収集をやめる〔クラスタ環境〕　276
フェールオーバー発生後の対処　280
フェールオーバー〔用語解説〕　907
物理ホスト〔用語解説〕　907
プログラム構成　86
プログラム〔収集対象の設定〕　218
プログラム〔製品定義の編集〕　214
プロセス〔用語解説〕　908

へ

変更管理　28

ほ

ポート番号一覧　827
保存する場合〔監査ログレポート〕　303
保存する場合〔グラフ表示の集計結果〕　320

め

メッセージ　552
メッセージ一覧　576
メッセージの記載形式　553
メッセージの形式　553
メッセージの出力形式　553
メッセージの出力先一覧　555
メッセージログファイルの場合〔メッセージの出力形式〕　553
メモリ所要量の見積もり　125

ゆ

ユーザ管理　121
ユーザ認証　75
ユーザ認証圏〔用語解説〕　908
ユーザマッピング　186
ユーザマッピング〔用語解説〕　908

よ

用語解説　902
容量の見積もり　125

る

ルート〔用語解説〕　908

ろ

ログイン ID〔データベース情報〕　191
ログファイルサイズ〔監査ログ管理画面ログ情報〕　196
ログファイルサイズ〔ログ情報〕　195
ログファイル数〔監査ログ管理画面ログ情報〕　196
ログファイル数〔ログ情報〕　195
ログファイル〔製品定義の編集〕　214
ログファイルトラップ機能の設定を確認する　177
ログファイルトラップ機能〔用語解説〕　908
ログフォルダ〔収集対象の設定〕　219
論理ホスト環境の作成〔コマンド〕　484
論理ホスト環境を設定する　260
論理ホスト〔用語解説〕　908