HITACHI
Inspire the Next

JP1 Version 9

JP1/NETM/Audit 正規化ルール定義ガイド

手引・操作書

3020-3-S91-20

マニュアルの購入方法

このマニュアル，および関連するマニュアルをご購入の際は，巻末の「ソフトウェアマニュアルのサービス ご案内」をご参照ください。

■対象製品

P-2642-7D94 JP1/NETM/Audit - Manager 09-10（適用 OS：Windows Server 2003）
P-2A42-7D94 JP1/NETM/Audit - Manager 09-10（適用 OS：Windows Server 2008）

■輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標類

Internet Explorer は，米国 Microsoft Corporation の米国及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。
Sun，Sun Microsystems は，米国 Sun Microsystems, Inc. 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。
活文，NAVIstaff は，日立ソフトウエアエンジニアリング株式会社の登録商標です。

■発行

2009 年 7 月（第 1 版）3020-3-S91
2010 年 6 月（第 2 版）3020-3-S91-20

■著作権

変更内容

変更内容（3020-3-S91-20）JP1/NETM/Audit - Manager 09-10

変更内容	変更個所
適用 OS に Windows Server 2008 R2 を追加した。	－
製品情報を 100 件まで定義できるようにした。	1.2
Windows イベントログの正規化ルールは，各製品情報に 100 件まで定義できるようにした。	1.2
標準サポート製品の製品情報や正規化ルールをテンプレート化し，誤って編集したり削除したりしても，定義を初めの状態に戻せるようにした。	2.2，3.2.4，3.3.4，4.5，5.2，5.11
［正規化ルール定義］ダイアログの［メッセージ分割］タブで，行の挿入および削除をできるようにした。	3.2.3，3.2.4，3.3.3，3.3.4，5.7
メイン画面の詳細エリア（ツリーエリアで正規化ルールを選択した場合）および［正規化ルール定義］ダイアログに，行番号の表示エリアを追加した。また，正規化ルール定義の選択行をフォーカスされた状態に，編集個所にカーソルを表示するようにした。	3.2.3，3.2.4，3.2.5，3.3.3，3.3.4，3.3.5，4.4，5.5.2，5.7
インポート・エクスポートコマンドを追加し，別のホストへ定義を移行できるようにした。	4.6
メイン画面のツリーエリアを右クリックメニューで操作できるようにした。	5.4
ほかの正規化ルールの定義内容を流用する場合に，標準サポート製品のテンプレートから正規化ルールを選択できるようにした。	5.8
次のメッセージを追加・変更した。 KDSQ4086-Q，KDSQ4256-E，KDSQ4809-E，KDSQ4811-E，KDSQ4813-E	6.3

単なる誤字・脱字などはお断りなく訂正しました。

はじめに

このマニュアルは，JP1/NETM/Audit - Manager で内部統制の証跡記録を管理するために，製品の監査ログを JP1/NETM/Audit - Manager で管理できる監査ログフォーマットに変換するためのルール（正規化ルール）を定義する方法について説明したものです。正規化ルールの定義方法は，GUI で定義する方法と正規化ルールファイルに記述する方法とがありますが，このマニュアルでは，GUI で定義する方法を説明します。
以降，このマニュアルでは，正規化ルールを定義する GUI を「正規化ルールエディタ」と呼びます。

■対象読者

JP1/NETM/Audit で標準サポートされていない製品が出力する監査ログの正規化ルールを，正規化ルールエディタを利用して定義する方を対象としています。
次の知識をお持ちであることを前提にしています。

- Windows に関する基本的な知識
- JP1/NETM/Audit の概要についての知識
- JP1/Base のイベントログトラップ機能とログファイルトラップ機能の設定，および JP1 イベントの属性値についての知識
- 正規化ルールを定義しようとしている製品（監査ログ収集対象プログラム）のログ出力に関する知識
- データベースに関する基本的な知識
- 内部統制に関する基本的な知識

なお，このマニュアルをお読みになる前に，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の設計・構築編で，JP1/NETM/Audit で標準サポートされていない製品の正規化について検討しておいてください。

■マニュアルの構成

このマニュアルは，次に示す章と付録から構成されています。

第 1 章　正規化ルールを定義するための検討

正規化ルールエディタを利用して正規化ルールを定義するために，事前に検討しておくことについて説明しています。

第 2 章　正規化ルールエディタの起動と終了

正規化ルールエディタを起動する方法，操作時の注意事項，および終了方法について説明しています。

第 3 章　正規化ルールの定義操作

正規化ルールエディタを利用して，正規化ルールを新規に定義する手順を，例題に沿って説明しています。

第 4 章　定義の変更と削除

定義した製品情報，および正規化ルールを変更したり削除したりする操作について説明しています。

第 5 章　正規化ルールエディタの画面

正規化ルールエディタの各画面の使い方について説明しています。

第 6 章　メッセージ

正規化ルールエディタが出力するメッセージについて説明しています。

■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。

監査証跡管理システムの概要と構築方法，および証跡記録を管理する方法について知りたい場合

JP1 Version 9 JP1/NETM/Audit 構築・運用ガイド（3020-3-S90）

JP1 管理基盤（JP1/Base）の構築方法，運用方法，および JP1 イベントの属性値の詳細を知りたい場合

- JP1 Version 9 JP1/Base 運用ガイド（3020-3-R71）
- JP1 Version 9 JP1/Base メッセージ（3020-3-R72）

■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
Hitachi Storage Command Suite	Hitachi Storage Command Suite 06-00
	JP1/HiCommand 05-10 以降
Internet Explorer	Internet Explorer(R) 6 SP1 以降
JP1/NETM/Audit	JP1/NETM/Audit - Manager

このマニュアルでの表記		正式名称
Windows Server 2003 ※	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition
	Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
	Windows Server 2003 R2	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
	Windows Server 2003 R2 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
Windows Server 2008 ※	Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
		Microsoft(R) Windows Server(R) 2008 Standard
	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
活文 NAVIstaff		活文 (R) NAVIstaff(R)

注※

OS による機能差がない場合，Windows Server 2003 および Windows Server 2008 を総称して Windows と表記します。

■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
ASCII	American Standard Code for Information Interchange
DB	Database
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
IP	Internet Protocol

英略語	正式名称
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
JIS	Japanese Industrial Standard code
OS	Operating System
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
WWW	World Wide Web

■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。
↓	定義ファイルで使用する，改行コードを示します。
_	定義ファイルで使用する，スペースを示します。

■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 YY	年を示します（YYYY：西暦 4 けたの数字，YY：西暦の下 2 けたの数字）。
MMM MM	月を示します（MMM：3 けたの英字，MM：2 けたの数字）。
DD	日を示します。（DD：2 けたの数字）
hh	時を示します。（hh：2 けたの数字）
mm	分を示します。（mm：2 けたの数字）
ss ss.s ss.sss ss.ssssss	秒を示します（ss：秒，.s：1/10 秒，.sss：ミリ秒，.ssssss：マイクロ秒）。
TZD	タイムゾーンを示します。

■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
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。

●入力の動作　●ユーザーの動作　●監査ログフォーマットの要素　●区切り位置

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外の漢字を使用しています。

個所（かしょ）　必須（ひっす）

■ 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。

目次

1 正規化ルールを定義するための検討

この章では，正規化ルールエディタを利用して正規化ルールを定義するために，事前に検討しておくことについて説明します。まず，「1.1 「正規化ルールを定義する」とは」で，検討する大まかな内容をつかんでください。1.2 以降で，具体的な検討内容について説明します。

1.1 「正規化ルールを定義する」とは

正規化ルールは，監査ログ収集対象プログラムから収集された監査ログ※を，JP1/NETM/Audit で管理できる監査ログフォーマットに変換するためのルールを定義するものです。正規化ルールには，監査ログの情報を JP1/NETM/Audit で管理できる監査ログフォーマットにどのように対応づけるかを定義します。

注※

監査ログ収集対象プログラムから出力された監査ログは，監査ログ収集対象プログラムと同じホストにある JP1/Base によって JP1 イベントに変換され，JP1/NETM/Audit で収集されます。

監査ログ収集対象プログラムが Windows イベントログに監査ログを出力する場合は，JP1/Base のイベントログトラップ機能によって JP1 イベントに変換されます。

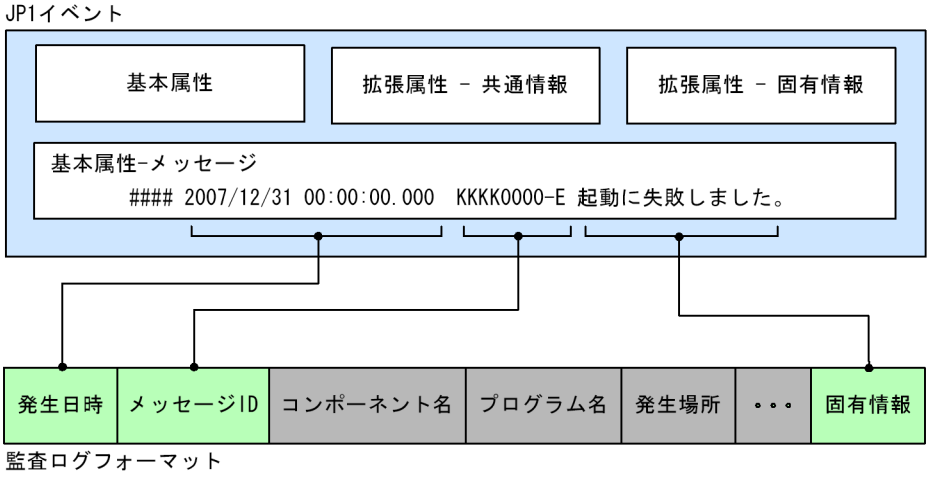
監査ログ収集対象プログラムがログファイルに監査ログを出力する場合は，JP1/Base のログファイルトラップ機能によって JP1 イベントに変換されます。

正規化ルールエディタを使用すると，正規化ルールを GUI で定義できます。正規化ルールエディタを使用して正規化ルールを定義するイメージを次に示します。

● メッセージテキストを監査ログフォーマットに対応づける

JP1 イベントに変換された監査ログのメッセージテキストの要素を，監査ログフォーマットに合わせて分割し，対応づけます。イメージを次の図に示します。

図 1-1 メッセージテキストを監査ログフォーマットに対応づける



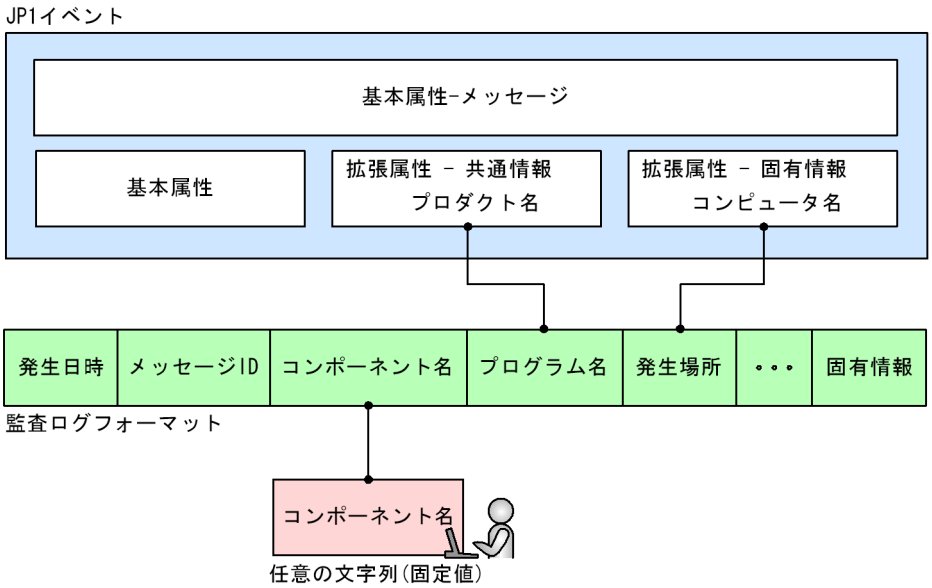
（凡例） ●——● ：メッセージテキストと監査ログフォーマットとの対応づけを示します。

ただし，メッセージテキストの要素だけでは，監査ログフォーマットに対応づけられない場合があります。不足している情報は，次の方法で補います。

● **メッセージテキストに不足している情報を補う**

メッセージテキストに不足している情報は，JP1 イベントの属性値，または任意の文字列（固定値）を，変換後の監査ログに埋め込むことで補います。イメージを次の図に示します。

図 1-2　メッセージテキストに不足している情報を補う



（凡例）●――● ：JP1イベント属性値および任意の文字列（固定値）と，監査ログフォーマットとの対応づけを示します。

正規化ルールエディタで正規化ルールを定義するために，事前に次の事項を検討しておく必要があります。

● **メッセージテキストを監査ログフォーマットにどのように対応づけるか**

監査ログフォーマットの各要素の意味を把握した上で，メッセージテキストを分割し，分割した要素を監査ログフォーマットに対応づけます。

● **メッセージテキストに不足している情報をどのように補うか**

監査ログとして必要な情報がメッセージテキストにない場合，不足している情報をどのように補うかを検討します。

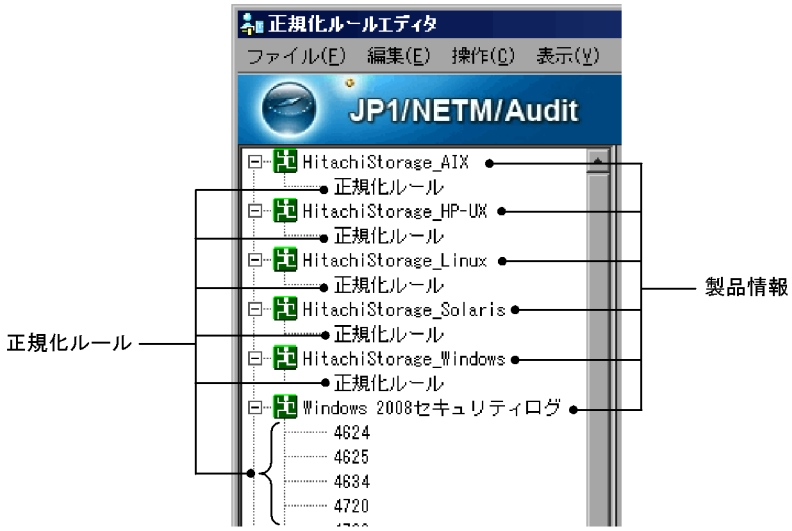
次節から，具体的に検討内容を説明します。

1.2 検討する前に正規化ルールを幾つ定義できるか把握する

正規化ルールエディタでは，定義できる正規化ルールの件数が決まっています。ここでは，定義できる正規化ルールの件数について説明します。定義できる正規化ルールの件数を考慮した上で，正規化ルールの定義内容を検討してください。

正規化ルールエディタでは，正規化ルールを次の図のように定義します。

図 1-3 正規化ルールエディタで正規化ルールを定義するイメージ



「製品情報」は，ログを出力する監査ログ収集対象プログラムの情報です。イベントログトラップ機能によって収集されたログなのか，ログファイルトラップ機能によって収集されたログなのかなどの情報を定義します。製品情報は，正規化ルールを定義する前に必ず定義します。正規化ルールは，対応する「製品情報」の下に定義します。

製品情報および正規化ルールには，定義できる件数に限りがあります。定義できる件数を次に示します。

表 1-1 製品情報および正規化ルールの定義件数

定義する情報	件数制限
製品情報	製品情報は，標準サポート製品を含んで 100 件まで定義できます。

定義する情報	件数制限
正規化ルール	• Windows **イベントログに対応する正規化ルール** 各製品情報に，100 件まで定義できます。 図 1-3 の「Windows 2008 セキュリティログ」のように，Windows イベント ID ごとに 1 件ずつ定義します。 Windows イベントログ 1 件に適用できる正規化ルールを検討してください。 • **ログファイルに対応する正規化ルール** 図 1-3 の「HitachiStorage」のように，各製品情報につき 1 件だけ定義できます。 製品が出力するすべてのログに適用できる正規化ルールを検討してください。

ここで示す件数分だけ，正規化ルールの定義内容を検討してください。

1.3 メッセージテキストを監査ログフォーマットにどのように対応づけるか

次の流れで検討します。

1. 監査ログフォーマットを把握する。
   メッセージテキストを監査ログフォーマットに対応づけるためには，まず，監査ログフォーマットを知っておく必要があります。「1.3.1 監査ログフォーマットを把握する」で，監査ログフォーマットの各要素の意味を把握してください。
2. メッセージテキストの分割位置を検討する。
   監査ログフォーマットに合わせて，メッセージテキストを分割します。
   「1.3.2 メッセージテキストの分割位置を検討する」で，メッセージテキストとの対応づけを検討してください。

各作業の詳細を説明します。

1.3.1 監査ログフォーマットを把握する

監査ログフォーマットには，対応づけが必須な要素，推奨されている要素，および任意の要素があります。それぞれの要素について説明します。

(1) 対応づけが必須な要素

次の監査ログフォーマットの要素は，監査ログとして必要な要素です。まず，メッセージテキストに次の情報があるか確認し，ある場合は対応づけます。ない場合は，「1.4 メッセージテキストに不足している情報をどのように補うか」で，JP1 イベント属性値，または任意の文字列を埋め込むことで対応づけます。

- 日付情報
- 監査ログの収集カテゴリ
- 監査ログの結果

各要素の詳細を説明します。

(a) 日付情報

監査ログの日付情報のフォーマットは，次の表から選択できます。

表 1-2 監査ログフォーマットの要素（日付情報）

項番	種別	形式
1	日時	YYYY/MM/DD hh:mm:ss
2		YYYY-MM-DD hh:mm:ss
3		YYYY-MM-DDThh:mm:ss.sTZD
4		YYYY-MM-DDThh:mm:ss.sssTZD
5		1970/01/01 からの経過秒数
6	日付	YYYY/MM/DD
7		YYYY-MM-DD
8		YY/MM/DD
9		DD/MMM/YYYY
10	年	YY※
11		YYYY
12	月	MM※
13		MMM
14	日	DD※
15	時刻	hh:mm:ss
16		hh:mm:ss.sss
17		hh:mm:ss.ssssss
18	時	hh※
19	分	mm※
20	秒	ss※
21		ss.sss
22		ss.ssssss

注※

メッセージテキスト中の日付情報が 1 けたで出力される場合でも，対応づけができます。

例えば，1 月 1 日が 1/1 と出力される場合でも，「月：MM」と「日：DD」に対応づけができます。

例えば，メッセージテキストに次のような日付情報があるとします。

```
2008/01/09△14:48:26.687△[Information]△KMMV4010-I△業務プログラムAを開始します。△[MANAGER01,3388(gyoumu.exe),GYOUMU001,StartStop]
```

（凡例）

下線部：日付情報に当たる情報を示します。

△：半角スペースを示します。

「2008/01/09 △ 14:48:26.687」のままでは，表 1-2 の監査ログフォーマットに該当する種別および形式がありません。このような場合は，「2008/01/09」と「14:48:26.687」に分割して，次のように対応づけます。

- 「2008/01/09」は，表 1-2 の「日付」種別の「YYYY/MM/DD」形式に該当するので，「YYYY/MM/DD」形式に対応づけます。
- 「14:48:26.687」は，表 1-2 の「時刻」種別の「hh:mm:ss.sss」形式に該当するので，「hh:mm:ss.sss」形式に対応づけます。

表 1-2 の形式に該当するように，メッセージテキストを分割して，対応づけてください。

なお，メッセージテキストに年の情報がない場合は，自動的に年の情報が付加されます。年の情報は，次のように付加されます。

- メッセージテキストに出力された月情報が，ログが収集された月以前の場合
  「ログが収集された時点の年」の情報が付加されます。
- メッセージテキストに出力された月情報が，ログが収集されたの月よりも後の場合
  「ログが収集された時点の年 - 1」の情報が付加されます。

例えば，メッセージテキストに出力された月が 12 月で，2009 年 1 月にログが収集された場合，2008 年 12 月として年の情報が付加されます。

(b) 監査ログの収集カテゴリ

監査ログの収集カテゴリは，ログが出力される契機となった事象の種別を指します。正規化ルールエディタでは，「監査事象の種別」と表示されます。

メッセージテキストに，監査ログの収集カテゴリが次の表のどれかで表示される場合は，そのメッセージテキストの要素を対応づけます。

表 1-3 監査ログ収集カテゴリ

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。
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。
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。
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。
5	Failure	ソフトウェアの異常を示す事象です。
6	LinkStatus	機器間のリンク状態を示す事象です。
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。

項番	カテゴリ	説明
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。
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。
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。
		異常な通信の発生を示す事象です。
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。

注

各カテゴリの事象例については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の，監査ログの収集カテゴリについて説明している個所を参照してください。

例えば，次のメッセージテキストの場合は，下線部の情報を対応づけます。

```
2008/01/09△14:48:26.687△[Information]△KMMV4010-I△業務プログラムAを開始します。△[MANAGER01,3388(gyoumu.exe),GYOUMU001,StartStop]
```

（凡例）

△：半角スペースを示します。

下線部：監査ログの収集カテゴリに当たる情報を示します。

監査ログの収集カテゴリに当たる情報がメッセージテキストにない場合は，次のように対処してください。

● Windows イベントログに対応する正規化ルールを定義する場合

表 1-3 のうち，該当するカテゴリの文字列を，変換後の監査ログに埋め込んでください。例えば，サービスの起動と終了に関するイベントログの場合は，「StartStop」という文字列を，変換後の監査ログに埋め込みます。文字列の埋め込みについては，「1.4.2　文字列の埋め込みを検討する」を参照してください。

● ログファイルに対応する正規化ルールを定義する場合

メッセージテキスト中に，監査ログの収集カテゴリに当たる情報がない場合，正規化ルールエディタで正規化ルールを定義できません。

ただし，監査ログ収集対象プログラムから収集されるログの監査ログの収集カテゴリが，すべて同じ場合にかぎり，正規化ルールエディタで正規化ルールを定義できます。例えば，ある監査ログ収集対象プログラムから収集される全ログの監査ログの収集カテゴリが起動／終了であれば，文字列「StartStop」を変換後の監査ログに埋め込めます。一つでも監査ログの収集カテゴリが「Authentication」のログがある場合は，文字列を埋め込めません。文字列の埋め込みについては，「1.4.2　文字列の埋め込みを検討する」を参照してください。

(c) 監査ログの結果

監査ログの結果は，成功か失敗かなどの事象の結果情報を指します。正規化ルールエディタでは，「監査事象の結果」と表示されます。

メッセージテキストに，監査ログの結果が次のどれかで表示される場合は，そのメッセージテキストの要素を対応づけます。

- Success
- Audit_Success
- Failure
- Error
- Critical
- Audit_Failure
- Failed
- Occurrence
- Warning
- Information
- Verbose
- None
- Occurred

例えば，次のメッセージテキストの場合は，下線部の情報を対応づけます。

```
2008/01/09△14:48:26.687△[Information]△KMMV4010-I△業務プログラムAを開始します。△[MANAGER01,3388(gyoumu.exe),GYOUMU001,StartStop]
```

（凡例）
△：半角スペースを示します。
下線部：監査ログの結果に当たる情報を示します。

なお，対応づけた監査ログの結果は，監査ログフォーマットに変換されると，次の 3 種類で表示されます。

表 1-4 監査ログの結果

変換前の監査ログの結果	変換後の監査ログの結果
Success	Success
Audit_Success	

変換前の監査ログの結果	変換後の監査ログの結果
Failure	Failure
Error	
Critical	
Audit_Failure	
Failed	
Occurrence	Occurrence
Warning	
Information	
Verbose	
None	
Occurred	

監査ログの結果に当たる情報がメッセージテキストにない場合は，次のように対処してください。

● Windows イベントログに対応する正規化ルールを定義する場合

JP1 イベント属性値の「拡張属性（固有情報）－ Windows ログ種類」を対応づけてください。

JP1 イベント属性値については，「1.4.1　JP1 イベント属性値との対応づけを検討する」を参照してください。

● ログファイルに対応する正規化ルールを定義する場合

メッセージテキストに，監査ログの結果に当たる情報がない場合，正規化ルールエディタで正規化ルールを定義できません。

ただし，監査ログ収集対象プログラムから収集されるログの監査ログの結果が，すべて同じ場合にかぎり，正規化ルールエディタで正規化ルールを定義できます。

例えば，ある監査ログ収集対象プログラムから収集される全ログの監査ログの結果が「成功」であれば，文字列「Success」を変換後の監査ログに埋め込めます。一つでも監査ログの結果が「失敗」のログがある場合は，文字列を埋め込めません。文字列の埋め込みについては，「1.4.2　文字列の埋め込みを検討する」を参照してください。

（2）対応づけが推奨されている要素

次の表に示す要素は，監査ログにあることが推奨されている要素です。メッセージテキスト，JP1 イベント属性値，または任意の文字列を対応づけてください。

表 1-5　対応づけが推奨されている監査ログフォーマットの要素

項番	種別	形式	説明
1	共通情報	通番	監査ログの通し番号に当たる情報を対応づけます。

項番	種別	形式	説明
2		メッセージ ID	メッセージ ID に当たる情報を対応づけます。
3		プログラム名	プログラム名に当たる情報を対応づけます。
4		コンポーネント名	コンポーネント名に当たる情報を対応づけます。
5		プロセス ID	プロセス ID に当たる情報を対応づけます。
6		発生場所	ログ出力の契機となった事象が起こった場所（ホスト名または IP アドレス）を対応づけます。
7		サブジェクト識別情報	ログ出力の契機となった事象を起こしたユーザの情報を対応づけます。ユーザと対応づけられない場合は，事象を起こしたプロセスの ID を対応づけます。

(3) 任意に対応づける要素

任意で対応づけられる要素を次の表に示します。必要に応じて対応づけてください。

表 1-6 任意で対応づける監査ログフォーマットの要素

項番	種別	形式	説明
1	固有情報（事象）	オブジェクト情報	ログ出力の契機となった事象で，ユーザが参照，追加，更新，削除などを実行したファイルなどの情報を対応づけます。
2		動作情報	ログ出力の契機となった事象を起こしたユーザの行為（参照，追加，更新，削除など）を対応づけます。
3		オブジェクトロケーション情報	オブジェクト情報を特定するために必要に応じて出力される，位置情報（設定ファイル名，親パラメーター名など）を対応づけます。
4		変更前情報	ファイルなどが変更された場合に必要に応じて出力される，変更前の情報を対応づけます。
5		変更後情報	ファイルなどが変更された場合に必要に応じて出力される，変更後の情報を対応づけます。
6		権限情報	ログ出力の契機となった事象を起こしたユーザに付与されている権限の情報を対応づけます。
7		サービスインスタンス名	日立オープンミドルウェア製品が提供するサービスの識別子を対応づけます。
8		冗長化識別情報	ログ出力の契機となった事象の発生場所が冗長化構成を採っている場合に，冗長化構成に関する識別情報（実行系／待機系など）を対応づけます。
9	固有情報（送信）	リクエスト送信元ホスト	リクエスト送信元ホストの識別情報（ホスト名または IP アドレス）を対応づけます。
10		リクエスト送信元ポート番号	リクエスト送信元のポート番号を対応づけます。

項番	種別	形式	説明
11		リクエスト送信先ホスト	リクエスト送信先ホストの識別情報（ホスト名またはIPアドレス）を対応づけます。
12		リクエスト送信先ポート番号	リクエスト送信先のポート番号を対応づけます。
13	固有情報（識別）	一括操作識別子	ログを基本ログと詳細ログに分割して出力した場合に出力される，両者を関連づけるための識別子を対応づけます。
14		ログ種別情報	ログの種別（基本ログまたは詳細ログ）を示す情報を対応づけます。
15		出力元の場所	ログを出力したホストの識別情報（ホスト名またはIPアドレス）を対応づけます。
16		指示元の場所	ログ出力の契機となった事象でユーザが使用したホストの識別情報（ホスト名，IPアドレス，または完全修飾ドメイン名）を対応づけます。
17		検出場所	ログ出力の契機となった事象を検出したホストの識別情報（ホスト名またはIPアドレス）を対応づけます。
18		ロケーション識別情報（loc）	ユーザが日立オープンミドルウェア製品の運用管理のために設定したロケーション識別情報を対応づけます。
19		エージェント情報	マネージャ／エージェント型システムでの，エージェント型プログラムの場所を示す識別情報（ホスト名またはIPアドレス）を対応づけます。
20	固有情報（自由）		これまで紹介した監査ログフォーマットに対応づけないで，自由に表示させたい情報を対応づけます。 固有情報（自由）は，30件まで対応づけられます。
21	その他		メッセージテキスト中の情報で，監査ログとして表示したくない情報がある場合に，対応づけます。

1.3.2 メッセージテキストの分割位置を検討する

「1.3.1 監査ログフォーマットを把握する」に示した監査ログフォーマットの各要素に，メッセージテキストの要素を対応づけます。

対応づけに当たって，メッセージテキストの分割位置を検討する必要があります。次のメッセージテキストを例に説明します。

```
2008/01/09△14:48:26.687△[Information]△KMMV4010-I△業務プログラムAを開始します。△[MANAGER01,3388(gyoumu.exe),GYOUMU001,StartStop]
```

（凡例）△：半角スペースを示します。

分割位置の例を次に示します。

図 1-4　メッセージテキストを分割する例

（凡例）　：監査ログフォーマットに対応づけるメッセージテキストの要素を示します。

がない個所：区切りとなる位置を示します。

：対応づける監査ログフォーマットの要素を示します。

この例のように，監査ログフォーマットに合わせて，メッセージテキストを先頭から分割します。分割位置は，文字列またはバイト単位（何バイトまでで区切るか）で指定します。例のように，分割したい位置に半角スペースや「,」（コンマ）などの文字列がある場合は，文字列で区切ります。分割位置に文字列がない場合は，バイト単位で区切ります。

メッセージテキストを分割し，監査ログフォーマットに対応づけたとき，監査ログとして必要な情報が不足していた場合は，「1.4　メッセージテキストに不足している情報をどのように補うか」で，不足している情報を補う検討をしてください。

1.4　メッセージテキストに不足している情報をどのように補うか

「1.3.1　監査ログフォーマットを把握する」で説明したように，監査ログフォーマットには，対応づけが必須な要素，および対応づけが推奨されている要素があります。

メッセージテキストに，対応づけが必須な要素や対応づけが推奨されている要素がない場合，JP1 イベントの属性値，または任意の文字列を，変換後の監査ログに埋め込みます。ただし，日付情報には，任意の文字列を埋め込めません。

そのほかにも，監査ログに表示させたい情報がある場合は，同じ方法で監査ログにその情報を埋め込みます。

メッセージテキストに不足している情報を埋め込むために，次の順に検討してください。

1. JP1 イベント属性値との対応づけを検討する。
   JP1 イベントの属性値に，メッセージテキストに不足していた情報があるか調査します。
2. 文字列の埋め込みを検討する。
   メッセージテキストに不足していた情報が JP1 イベント属性値になかった場合，文字列を埋め込めるかどうか調査します。

各作業の詳細を説明します。

1.4.1　JP1 イベント属性値との対応づけを検討する

正規化ルールエディタで対応づけができる JP1 イベントの属性値を次の表に示します。

表 1-7　正規化ルールエディタで埋め込める JP1 イベントの属性値一覧

項番	属性種別	属性名
1	基本属性	JP1 イベント DB 内の通し番号
2		JP1 イベント ID
3		登録要因
4		発行元プロセス ID
5		登録時刻※ 1
6		到着時刻※ 1
7		発行元ユーザー ID
8		発行元グループ ID
9		発行元ユーザー名
10		発行元グループ名

項番	属性種別	属性名
11		発行元イベントサーバ名※2※3
12		送信先イベントサーバ名※3
13		発行元別通し番号
14		コードセット
15		メッセージ
16	拡張属性（共通情報）	重大度
17		プロダクト名
18		オブジェクトタイプ
19		オブジェクト名
20		登録名タイプ
21		登録名
22	拡張属性（固有情報）	Windows ログ登録日時※1※4
23		コンピューター名※2※4
24		Windows ログ種別※4
25		Windows ログ種類※4※5
26		Windows ログ分類※4
27		Windows イベント ID※4
28		Windows ユーザー名※4
29		プラットフォーム
30		PP 名

注※ 1

メッセージテキストに，監査ログフォーマットの日付情報に当たる情報がない場合に対応づけます。監査ログフォーマットの「日時」種別の「1970/01/01 からの経過秒数」形式に対応づけてください。

注※ 2

メッセージテキストに，監査ログフォーマットの発生場所に当たる情報がない場合に対応づけます。Windows イベントログの場合は「コンピューター名」，ログファイルの場合は「発行元イベントサーバ名」を対応づけます。

注※ 3

監査ログフォーマットのうち，ホスト名が出力される要素に対応づける場合，監査ログ専用イベントサーバ名として付加した「-adm」は，監査ログに変換されると削除されます。

監査ログ専用イベントサーバの設定については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の設計・構築編にある，JP1/Base のイベントサービスの設定について説明している個所を参照してください。

注※ 4

Windows イベントログの正規化ルールを定義するときだけ対応づけることができます。

注※5

Windows イベントログのメッセージテキストに，監査ログフォーマットの監査ログの結果に当たる情報がない場合に対応づけます。

JP1 イベントの属性値は，10 件まで対応づけできます。

1.4.2　文字列の埋め込みを検討する

メッセージテキストにも JP1 イベント属性値にもなかった情報は，文字列の埋め込みによって対応づけます。

例えば，コンポーネント名の情報が，メッセージテキストにも JP1 イベント属性値にもなかった場合，文字列（例：「LogonEvent」）を埋め込みます。

文字列は，30 件まで埋め込めます。

注意事項

埋め込む文字列は，固定値として対応づけられます。ログファイルに出力されたログの正規化ルールを定義する場合，一つの製品に定義できる正規化ルールは 1 件です。したがって，その製品が出力するすべてのログに共通する監査ログフォーマットの要素にだけ，固定値を対応づけることができます。例えば，監査ログフォーマットの「発生場所」に当たる情報が，ログによって異なる場合は，文字列を対応づけできません。
Windows イベントログの正規化ルールを定義する場合は，イベント ID ごとに正規化ルールを定義できるため，固定値を埋め込んでも問題ありません。

監査ログフォーマットの各要素に埋められる文字列の規則を次の表に示します。規則に従って検討してください。

表 1-8　監査ログフォーマットの各要素に埋められる文字列の規則

項番	種別	形式	埋められる文字列の規則	
			文字列長	入力形式
1	共通情報	通番	1 ～ 10 バイト	1 ～ 2147483647 の範囲で指定してください。
2		メッセージ ID	9 ～ 11 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。
3		プログラム名	1 ～ 32 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」および「,」は除く。

項番	種別	形式	埋められる文字列の規則	
			文字列長	入力形式
4		コンポーネント名	1 ～ 32 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。
5		プロセス ID	1 ～ 10 バイト	半角数字で指定してください。
6		発生場所	1 ～ 255 バイト	ホスト名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は，XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。
7		監査事象の種別	1 ～ 32 バイト	Windows イベントログに対応する正規化ルールを定義する場合，次の中から選択して指定します。 • StartStop • Authentication • AccessControl • ConfigurationAccess • Failure • LinkStatus • ExternalService • ContentAccess • Maintenance • AnomalyEvent • ManagementAction 各事象の意味については，「1.3.1(1)(b) 監査ログの収集カテゴリ」を参照してください。 ログファイルに対応する正規化ルールを定義する場合，監査ログ収集対象プログラムから収集されるログの監査ログの収集カテゴリが，すべて同じ場合にかぎり，正規化ルールエディタで正規化ルールを定義できます。 例えば，ある監査ログ収集対象プログラムから収集される全ログの監査ログの収集カテゴリが起動／終了であれば，文字列「StartStop」を変換後の監査ログに埋め込めます。一つでも監査ログの収集カテゴリが「Authentication」のログがある場合は，文字列を埋め込めません。

項番	種別	形式	埋められる文字列の規則	
			文字列長	入力形式
8		監査事象の結果	7 ～ 10 バイト	次の中から選択して指定します。 • Success • Failure • Occurrence ログファイルに対応する正規化ルールを定義する場合，監査ログ収集対象プログラムから収集されるログの監査ログの結果が，すべて同じ場合にかぎり，正規化ルールエディタで正規化ルールを定義できます。 例えば，ある監査ログ収集対象プログラムから収集される全ログの監査ログの結果が「成功」であれば，文字列「Success」を変換後の監査ログに埋め込めます。一つでも監査ログの結果が「失敗」のログがある場合は，文字列を埋め込めません。
9		サブジェクト識別情報	1 ～ 256 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字 pid 形式の場合は，半角数字で指定します。
10	固有情報（事象）	オブジェクト情報	1 ～ 256 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。
11		動作情報	1 ～ 32 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。
12		オブジェクトロケーション情報	1 ～ 64 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字
13		変更前情報	1 ～ 64 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字

項番	種別	形式	埋められる文字列の規則	
			文字列長	入力形式
14		変更後情報	1 ～ 64 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字
15		権限情報	1 ～ 128 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字
16		サービスインスタンス名	1 ～ 128 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字
17		冗長化識別情報	1 ～ 2 バイト	1 ～ 99 の範囲で指定できます。
18	固有情報（送信）	リクエスト送信元ホスト	1 ～ 255 バイト	ホスト名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は， XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。
19		リクエスト送信元ポート番号	1 ～ 5 バイト	0 ～ 65535 の範囲でポート番号を指定できます。
20		リクエスト送信先ホスト	1 ～ 255 バイト	ホスト名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は， XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。

項番	種別	形式	埋められる文字列の規則	
			文字列長	入力形式
21		リクエスト送信先ポート番号	1 ～ 5 バイト	0 ～ 65535 の範囲でポート番号を指定できます。
22	固有情報（識別）	一括操作識別子	1 ～ 10 バイト	1 ～ 2147483647 の範囲で指定します。
23		ログ種別情報	8 ～ 9 バイト	次のどちらかを指定します。 • BasicLog • DetailLog
24		出力元の場所	1 ～ 255 バイト	ホスト名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は，XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。
25		指示元の場所	1 ～ 255 バイト	ホスト名または完全修飾ドメイン名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は，XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。
26		検出場所	1 ～ 255 バイト	ホスト名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は，XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。

項番	種別	形式	埋められる文字列の規則	
			文字列長	入力形式
27		ロケーション識別情報	1 ～ 64 バイト	次の文字で指定できます。 • 半角英数字 • 半角記号 ただし，「"」，「,」，および半角スペースは除く。 • 全角文字
28		エージェント情報	1 ～ 255 バイト	ホスト名を指定する場合は，次の文字で指定してください。 • 半角英数字 •「-」または「.」 IPv4 形式の IP アドレスを指定する場合は，xxx.xxx.xxx.xxx 形式（xxx：0 ～ 255 の数字）で指定してください。 IPv6 形式の IP アドレスを指定する場合は，XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX 形式（XXXX：4 バイトの 16 進数字）で指定してください。
29	固有情報（自由）	自由記述 1 ～ 30	1 ～ 256 バイト	任意の文字列を文字列長の範囲で指定してください。

2 正規化ルールエディタの起動と終了

この章では，正規化ルールエディタを起動する方法，操作時の注意事項，および終了する方法について説明します。

2.1　正規化ルールエディタを起動する

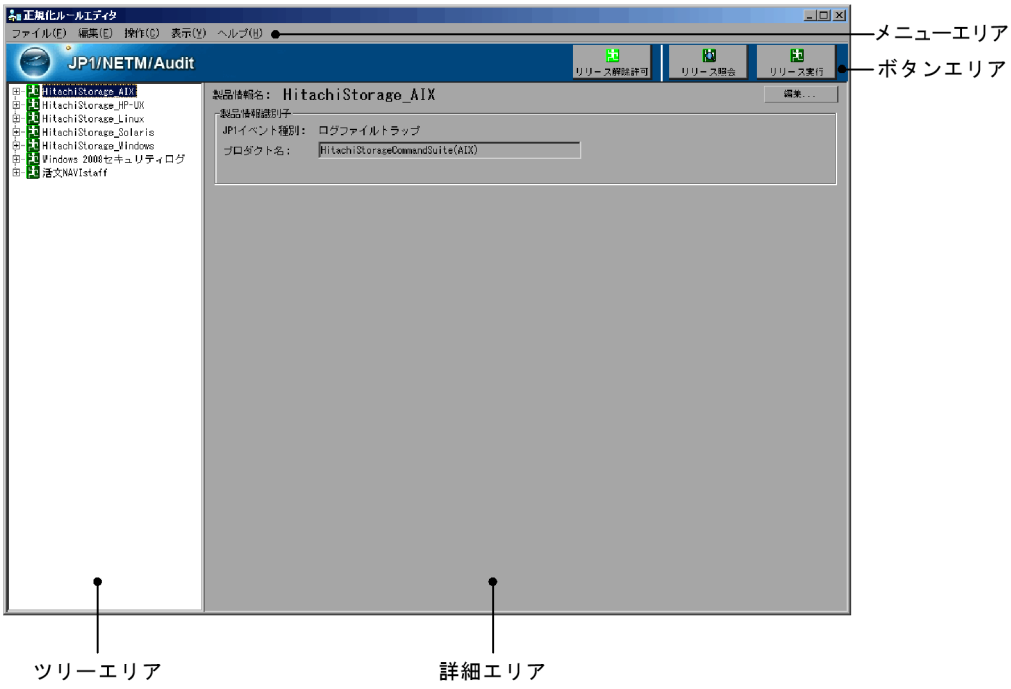
正規化ルールエディタを起動する前に，次に示すサービスを開始しているか確認してください。

- 正規化サービス（JP1/NETM/Audit - Manager Convert）
- 正規化定義サービス（JP1/NETM/Audit - Manager Define）

サービスの開始については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の，JP1/NETM/Audit - Manager のサービスの開始・停止について説明している個所を参照してください。

正規化ルールエディタは，［スタート］ボタンをクリックして，［プログラム］－［JP1_NETM_Audit］－［正規化ルールエディタ］を選択すると起動します。起動すると，正規化ルールエディタのメイン画面が表示されます。

図 2-1　正規化ルールエディタのメイン画面



メイン画面の詳細については，「5.1　メイン画面の各部の名称と使い方」を参照してください。

2.2　操作時の注意事項

正規化ルールエディタを操作するに当たって，次の点に注意してください。

- 正規化ルールエディタには，シフト JIS コードで入力してください。
- 「Hitachi Storage」，「Windows 2008 セキュリティログ」，および「活文 NAVIstaff」の正規化ルールは，JP1/NETM/Audit の標準サポート製品として，正規化ルールエディタに初めから定義されています。
  標準サポート製品の正規化ルールは，編集しないでください。標準サポート製品の正規化ルールを誤って削除したり編集したりした場合には，定義を再作成して定義を初めの状態に戻すことができます。標準サポート製品の正規化ルールを再作成する操作については，「4.5　標準サポート製品の定義を再作成する」を参照してください。
  なお，標準サポート製品の「Windows 2008 セキュリティログ」は，Windows イベント ID ごとに正規化ルールが定義されています。その中に目的の Windows イベント ID がない場合は，新たに目的の Windows イベント ID の正規化ルールを定義しても問題ありません。
- 半角スペース，全角スペース，タブ，および改行コードは，正規化ルールエディタでは次のように表示されます。

表 2-1　正規化ルールエディタで表示される文字

文字列	正規化ルールエディタで表示される文字
半角スペース	
全角スペース	
タブ	
改行コード	

  なお，タブと改行コード以外の，0x00 ～ 0x1F，および 0x7F の制御コードをテキストフィールドに入力した場合，正しく表示されないことがあります。
- 正規化ルールエディタに読み込まれた情報の中に，対応しない文字コードが含まれていた場合，その文字が「?」で表示されます。
- ディスプレイの解像度を 1,024 × 768 ピクセル以上に設定してください。1,024 × 768 ピクセル未満に設定すると，一部のダイアログが画面内に収まらないことがあります。
- 正規化ルールエディタのメイン画面は，初期サイズより小さくなりません。
- 正規化ルールエディタを起動したあとにデスクトップテーマを変更すると，正規化ルールエディタが正しく表示されないことがあります。この場合は，いったん正規化ルールエディタを終了してから，再度起動してください。

2.3 正規化ルールエディタを終了する

必要な操作を終えたら，正規化ルールエディタを終了します。

正規化ルールエディタの終了手順を次に示します。

1. **［ファイル］－［終了（ログアウト）］をクリックする。**
   終了確認メッセージが表示されます。
2. **終了確認メッセージの［はい］ボタンをクリックする。**
   メイン画面が閉じ，正規化ルールエディタが終了します。

3 正規化ルールの定義操作

この章では，正規化ルールエディタを利用して新規に正規化ルールを定義する手順を，例題に沿って説明します。まずは，「3.1　例題の説明」で例題の大まかな内容をつかんでください。3.2 以降で，定義操作の流れと操作を説明します。

3.1 例題の説明

これから，次のログの正規化ルールを定義します。

● **アプリケーション** A **が** Windows Server 2008 **のアプリケーションログに出力するログ（メッセージ** ID：A0001）

アプリケーション A が，Windows Server 2008 のイベントログのアプリケーションログに出力するログメッセージに対応する正規化ルールを定義します。

● **業務プログラム** B **のログ**

業務プログラム B が出力したログファイルのログメッセージに対応する正規化ルールを定義します。

ログメッセージの出力先（Windows イベントログまたはログファイル）によって，正規化ルールの定義操作が異なります。それぞれの場合に分けて，正規化ルールを定義する操作を説明します。

表 3-1 **正規化ルールの定義操作の参照先**

収集したログの種類	参照先
Windows イベントログに対応する正規化ルールの定義操作	3.2
ログファイルに出力されたログメッセージに対応する正規化ルールの定義操作	3.3

3.2 正規化ルールの定義操作（Windows イベントログの場合）

Windows イベントログの正規化ルールを定義します。

ここでは，アプリケーション A が Windows Server 2008 のアプリケーションログに出力する次のログメッセージ（メッセージ ID：A0001）に対応する正規化ルールを定義する例に沿って説明します。

```
アカウントが正常にログオンしました。↓
↓
サブジェクト:↓
→セキュリティ△ID:→→SYSTEM↓
→アカウント名:→→WIN-DOM$↓
→アカウント△ドメイン:→→AUDIT↓
→ログオン△ID:→→0x1e6↓
↓
ログオン△タイプ:→→→2↓
↓
新しいログオン:↓
→セキュリティ△ID:→→S-1-5-21↓
→アカウント名:→→Administrator↓
→アカウント△ドメイン:→→AUDIT↓
→ログオン△ID:→→0xd7ff4↓
→ログオン△GUID:→→{00000000-0000}↓
↓
プロセス情報:↓
→プロセス△ID:→→0x750↓
→プロセス名:→→C:¥Windows¥System32¥winlogon.exe↓
↓
ネットワーク情報:↓
→ワークステーション名:→WIN-DOM↓
→ソース△ネットワーク△アドレス:→127.0.0.1↓
→ソース△ポート:→→0↓
      （以降省略）
```

（凡例）

↓：改行を示します。

→：タブを示します。

△：半角スペースを示します。

3.2.1 定義の流れ

Windows イベントログの正規化ルールを定義する流れを次の表に示します。

表 3-2 Windows イベントログの正規化ルールを定義する流れ

手順	作業		作業の説明	参照先
1	監査ログ収集対象プログラムの製品情報を定義する		Windows イベントログを出力するプログラムの製品情報を定義します。製品情報は，監査ログへの変換で使用する正規化ルールを特定するための情報になります。	3.2.2
2	正規化ルールを定義する	正規化ルールの名称を定義する	ツリーエリアに表示する正規化ルールの名称を定義します。	3.2.3
3		メッセージテキストを監査ログフォーマットに対応づける	収集した Windows イベントログのメッセージテキストを監査ログフォーマットに対応づけます。	3.2.4
4		メッセージテキストに不足している情報を監査ログに埋め込む	監査ログに必要な情報が，メッセージテキストに含まれていない場合に，不足している情報を監査ログに埋め込みます。	3.2.5
5	正規化ルールを変換で使用できる状態にする		定義した正規化ルールを，監査ログへの変換で使用できるようにします。	3.2.6

3.2.2 監査ログ収集対象プログラムの製品情報を定義する

監査ログへの変換では，JP1/NETM/Audit に登録されている正規化ルールのうち，どれを使用するかを決めるための情報が必要です。その情報となる，監査ログ収集対象プログラムの製品情報を定義します。ここでは，アプリケーション A の製品情報を定義します。

注意事項

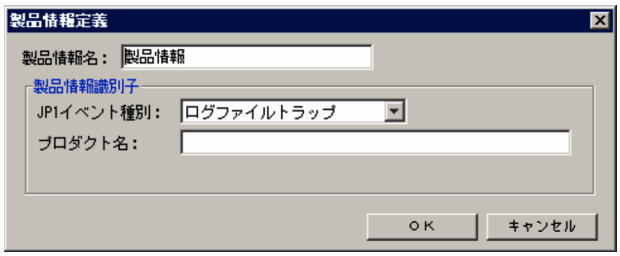
製品情報の定義は，Windows イベントログにログメッセージを出力する製品の情報が，ツリーエリアに定義されていない場合に定義します。例えば，Windows Server 2008 が出力する Windows イベントログのセキュリティログの正規化ルールを定義する場合，「Windows2008 セキュリティログ」の製品情報はすでに定義されているので，製品情報の定義は不要です。ここで採り上げている例では，アプリケーション A が Windows Server 2008 の Windows イベントログにログメッセージを出力するため，アプリケーション A の製品情報の定義が必要です。

手順を次に示します。

(1) 手順

1. **メイン画面で，[ファイル] − [新規作成] − [製品情報] を選択する。**
   [製品情報定義] ダイアログが表示されます。

図 3-1　［製品情報定義］ダイアログ



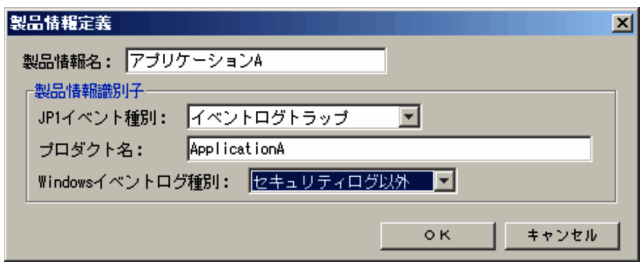
2. **「製品情報名」に，定義する製品情報の名称を入力する。**
   定義した製品情報名は，ツリーエリアに表示されます。
   ここでは，「アプリケーション A」と入力します。

3. **「JP1 イベント種別」で，「イベントログトラップ」を選択する。**
   Windows イベントログは，JP1/Base のイベントログトラップで収集されるので，「イベントログトラップ」を選択します。

4. **「プロダクト名」に，Windows イベントログのソース情報を入力する。**
   ここでは，Windows Server 2008 のアプリケーションログのソース情報である「ApplicationA」を入力します。

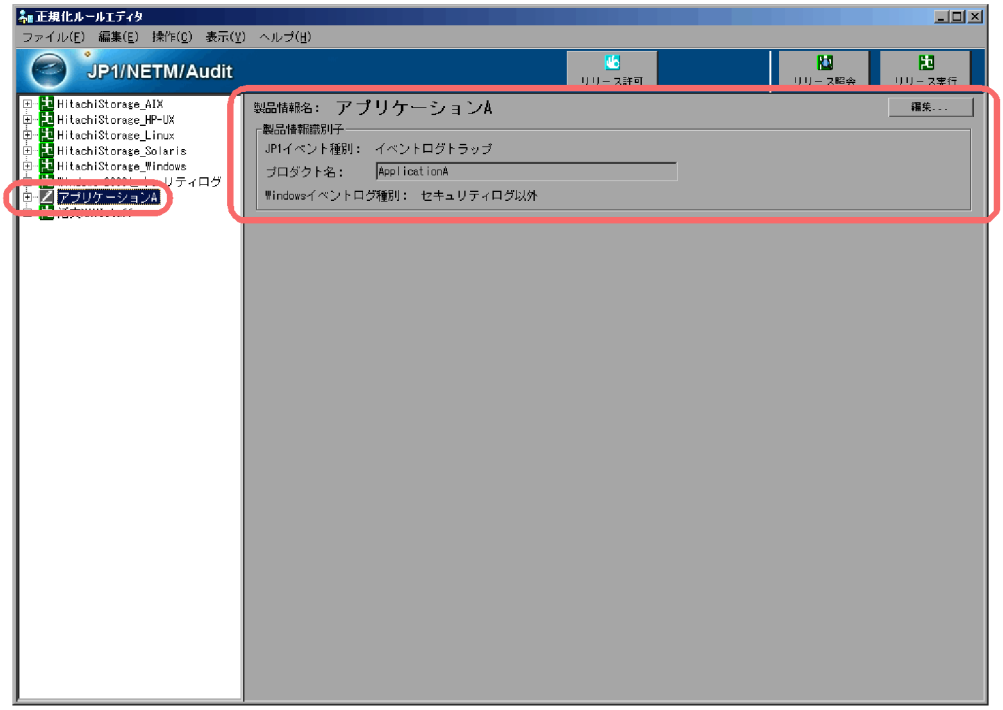
5. **「Windows イベントログ種別」で，Windows イベントログの種別を選択する。**
   セキュリティログなのか，セキュリティログ以外なのかを選択します。
   アプリケーション A は，Windows Server 2008 のアプリケーションログを出力するので，ここでは「セキュリティログ以外」を選択します。

図 3-2　アプリケーション A の情報を入力した［製品情報定義］ダイアログ



6. **［OK］ボタンをクリックする。**
   定義した製品情報がツリーエリアと詳細エリアに表示されます。

図 3-3　アプリケーション A の製品情報が表示されたツリーエリアと詳細エリア



(2) 関連情報

［製品情報定義］ダイアログの項目の詳細については，「5.6 ［製品情報定義］ダイアログ」を参照してください。

3.2.3 正規化ルールの名称を定義する

製品情報を定義したら，監査ログ収集対象プログラムの正規化ルールを定義します。

まず，Windows イベントログの ID を登録します。手順を次に示します。

(1) 手順

1. **ツリーエリアで，製品情報「アプリケーション A」の製品情報のアイコンを確認する。**
   製品情報の隣にあるアイコンは，正規化ルールの定義の状態を表します。
   正規化ルールの定義は，正規化ルールの定義の状態（製品情報のアイコン）が次の場合に実施できます。
   - 「編集」状態

      正規化ルールが一つも定義されていない状態，または定義が完了している状態（「編集（完了）状態」）

      正規化ルールの定義が未完了のまま，一時的に保存している状態（「編集（未

完了）状態」）

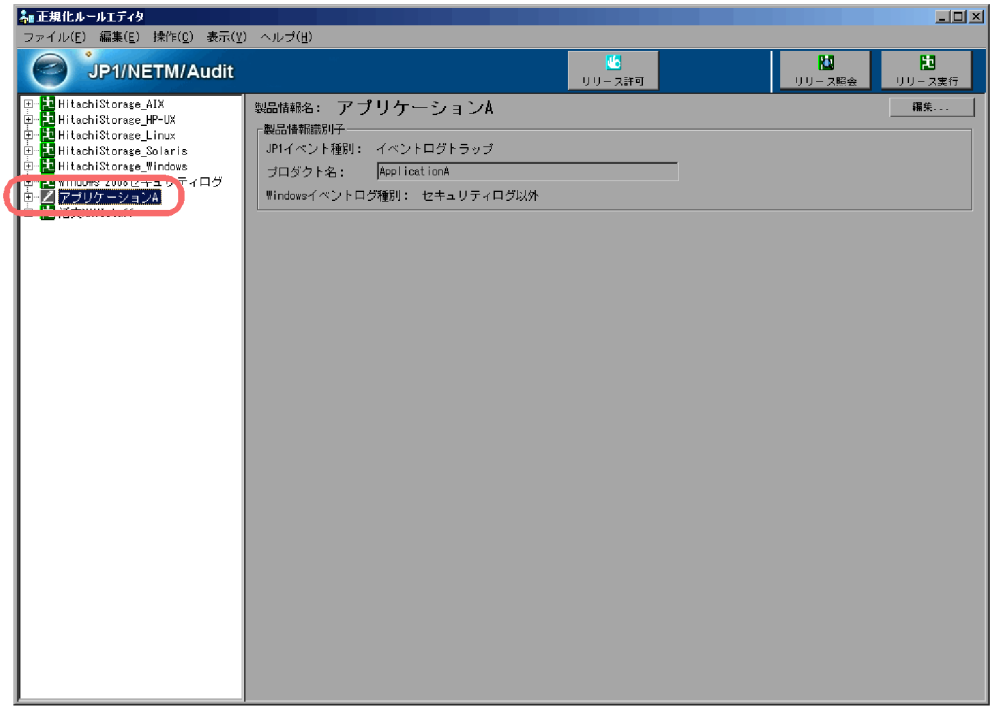
- 「リリース」状態

- 「リリース編集」状態


正規化ルールの定義が完了している状態（「リリース編集（完了）状態」）


正規化ルールの定義が未完了のまま，一時的に保存している状態（「リリース編集（未完了）状態」）

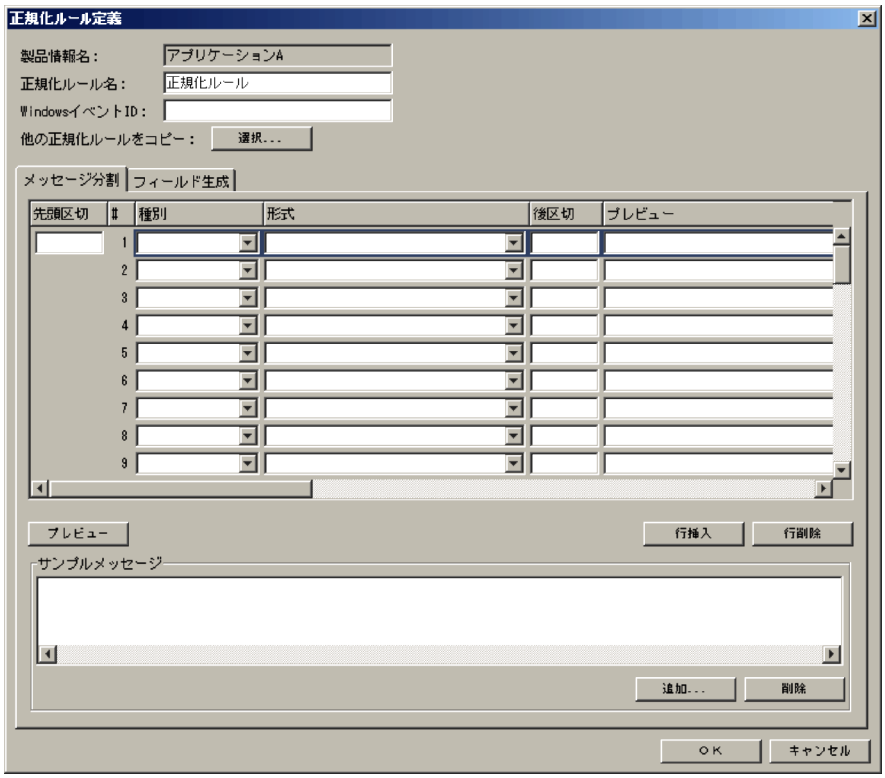
図 3-4　ツリーエリアでアプリケーション A の製品情報のアイコンが「編集」状態になっている例



「アプリケーション A」の正規化ルールの定義の状態が，「  （「リリース許可」状態）」または「  （「リリース解除許可」状態）」の場合は，正規化ルールの定義の状態を変更してください。
正規化ルールの定義の状態，および状態を変更する方法については，「5.4　メイン画面－ツリーエリア」を参照してください。

2. **ツリーエリアで，製品情報「アプリケーション A」を選択して，［ファイル］－［新規作成］－［正規化ルール］を選択する。**
［正規化ルール定義］ダイアログが表示されます。

図 3-5 ［正規化ルール定義］ダイアログ



3. **「正規化ルール名」に，定義する正規化ルールの名称を入力する。**
   定義した正規化ルール名は，ツリーエリアに表示されます。
   ここでは，メッセージ ID「A0001」を入力します。

4. **「Windows イベント ID」に，定義する Windows イベント ID を入力する。**
   ここでは，「0001」と入力します。

これで，正規化ルールの名称と Windows イベント ID を登録できました。次に，メッセージテキストを監査ログフォーマットに対応づけます。［正規化ルール定義］ダイアログを開いた状態で，次項を参照してください。

(2) 関連情報

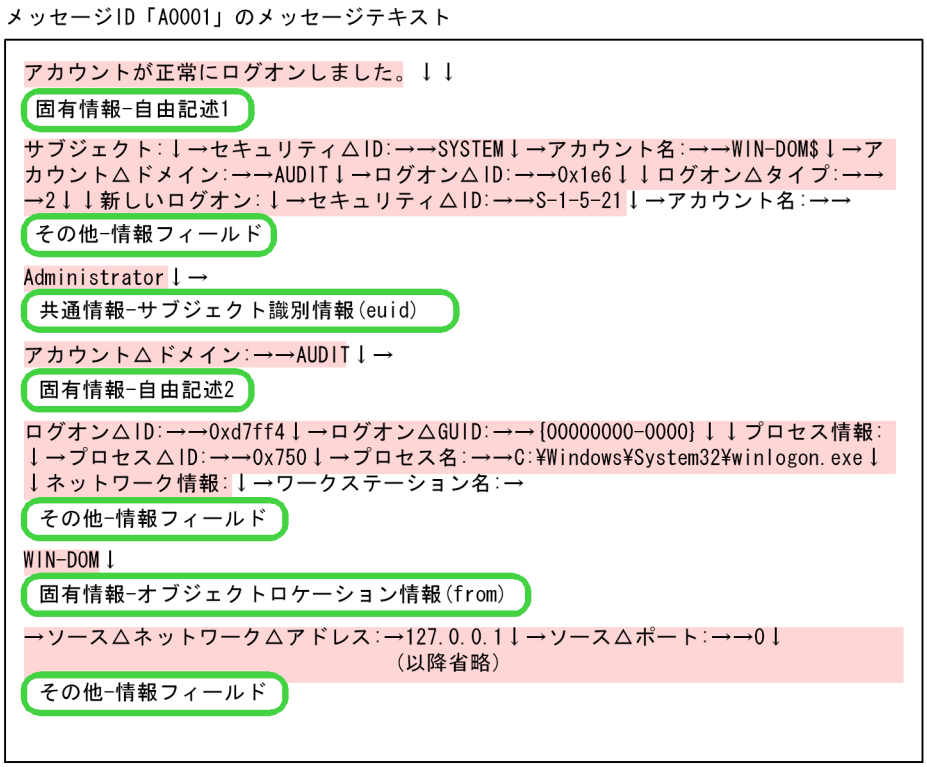
［正規化ルール定義］ダイアログの項目の詳細については，「5.7 ［正規化ルール定義］ダイアログ」を参照してください。

3.2.4　メッセージテキストを監査ログフォーマットに対応づける

Windows イベントログのメッセージテキストを，「1.3　メッセージテキストを監査ログフォーマットにどのように対応づけるか」で検討した内容に沿って分割し，監査ログフォーマットに対応づけます。

ここでは，メッセージ ID「A0001」のメッセージテキストを次の図のように分割し，監査ログフォーマットに対応づけます。

図 3-6　メッセージ ID「A0001」のメッセージテキストの分割

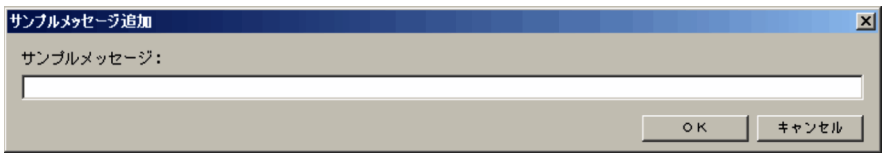


メッセージテキストを分割するために，まず，サンプルとなるメッセージテキストを登録します。手順を次に示します。

(1) 手順

1. **［正規化ルール定義］ダイアログの［メッセージ分割］タブにある，「サンプルメッセージ」の［追加］ボタンをクリックする。**
［サンプルメッセージ追加］ダイアログが表示されます。

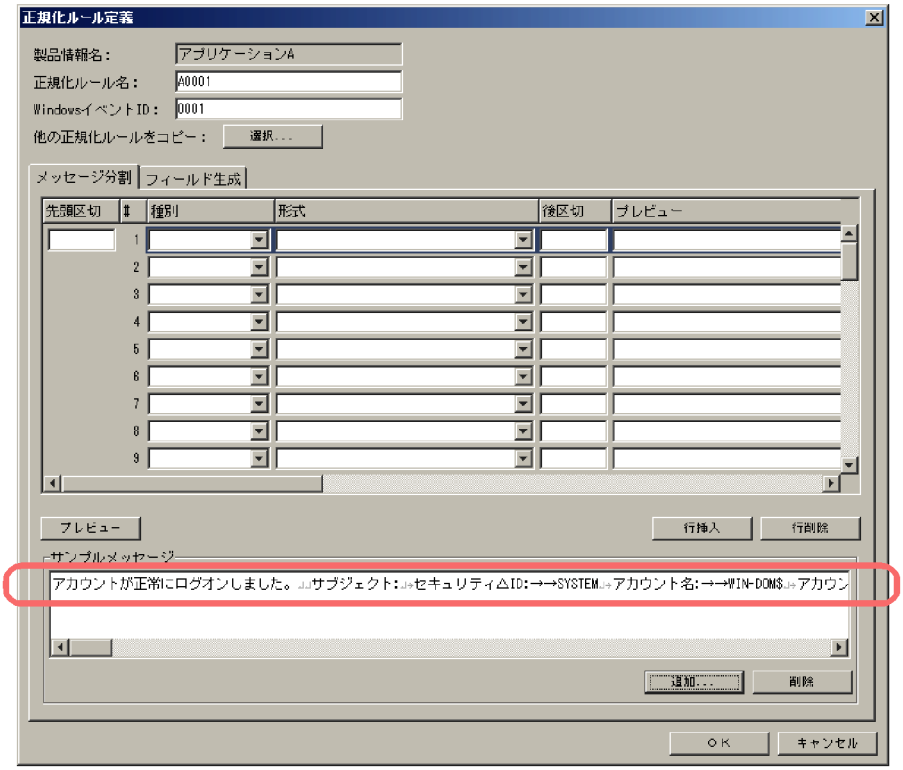
図 3-7 ［サンプルメッセージ追加］ダイアログ



2. **サンプルとなるメッセージテキストを「サンプルメッセージ」に入力する。**
ここでは，メッセージ ID「A0001」のメッセージテキストを入力します。

3. **［OK］ボタンをクリックする。**
［正規化ルール定義］ダイアログの［メッセージ分割］タブの「サンプルメッセージ」に，入力したサンプルメッセージが表示されます。

図 3-8 サンプルメッセージが表示された［正規化ルール定義］ダイアログ



サンプルメッセージは，3 件まで登録できます。ここでは 1 件だけを登録しました。

次に，登録したサンプルメッセージテキストを分割し，分割した各要素に監査ログフォーマットの要素を対応づけます。

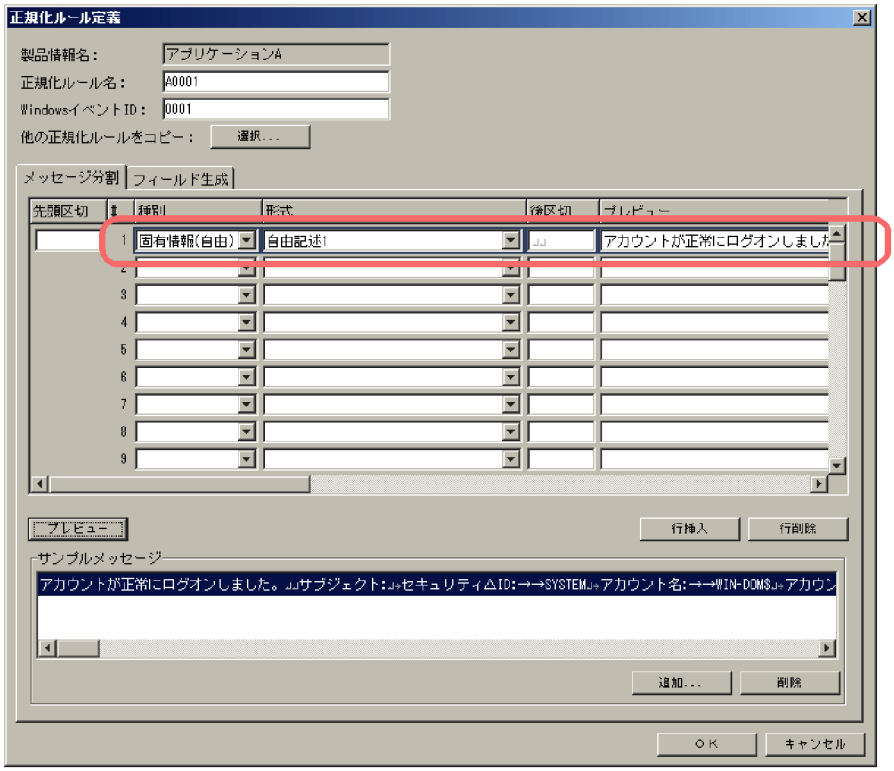
4. **メッセージテキストの先頭の要素に対応づける監査ログフォーマットの要素を，「種別」と「形式」プルダウンメニューから選択する。**
   ここでは，メッセージ ID「A0001」のメッセージテキストを図 3-6 のように分割します。先頭の要素は，「アカウントが正常にログオンしました。」です。「アカウントが正常にログオンしました。」には，固有情報（自由）を対応づけるので，「種別」プルダウンメニューで「固有情報（自由）」を，「形式」プルダウンメニューで「自由記述 1」を選択します。

   次に，メッセージテキストを「アカウントが正常にログオンしました。」で区切ります。

5. **先頭の要素「アカウントが正常にログオンしました。」で区切るために，「サンプルメッセージリスト」で分割するメッセージテキストを選択し，「後区切」に区切りとなる情報を入力する。**
   区切りとなるのは，「↓↓」（↓：改行コード）です。
   ［メッセージ分割］タブの 1 行目の「後区切」に「↓↓」を入力してください。

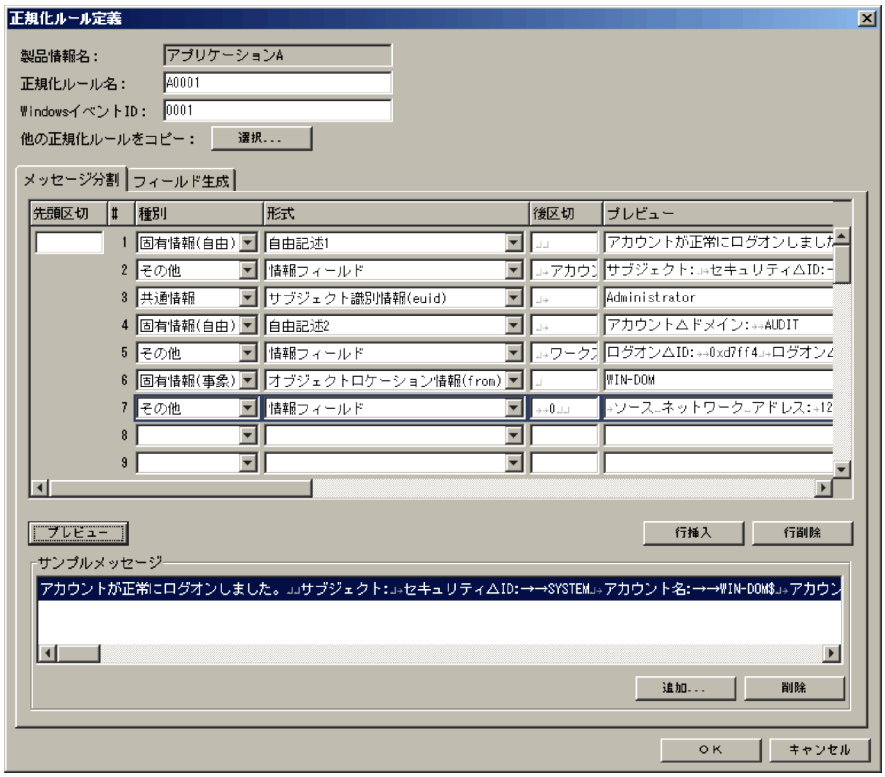
6. **［プレビュー］ボタンをクリックする。**
   「プレビュー」で，「アカウントが正常にログオンしました。」が正常に分割されていることを確認できます。

図 3-9 メッセージテキストの先頭の要素を定義した［正規化ルール定義］ダイアログ



7. **先頭の要素を定義した要領で，以降のメッセージテキストを分割し，監査ログフォーマットの要素を対応づける。**
   図 3-6 に従って，監査ログフォーマットの種別と形式を対応づけます。

図 3-10　メッセージテキストすべてを監査ログフォーマットに対応づけた［正規化ルール定義］ダイアログ



空行ができないように入力してください。
途中で分割位置を誤り，分割位置を増やしたり減らしたりしたい場合は，［行挿入］ボタンまたは［行削除］ボタンで修正してください。［行挿入］ボタンは，カーソルがある行の上に空行を挿入します。［行削除］ボタンは，カーソルがある行を削除します。［行挿入］ボタンまたは［行削除］ボタンを使用すると，「プレビュー」の内容がいったん削除されます。

これで，メッセージテキストを監査ログフォーマットの要素に対応づける操作は完了です。

次に，メッセージテキストに不足している情報を，監査ログに埋め込む定義をします。［正規化ルール定義］ダイアログを開いた状態で，次項を参照してください。

(2) 関連情報

● すでに定義してある正規化ルールの定義，および標準サポート製品のテンプレートを流用して，新規に正規化ルールを定義することもできます。［正規化ルール定義］ダイアログの［選択］ボタンで，流用する正規化ルールを選択します。［正規化ルール定義］ダイアログの項目については，「5.7 ［正規化ルール定義］ダイアログ」を参照し

てください。

- ［正規化ルール定義］ダイアログの，「種別」および「形式」プルダウンメニューの各項目については，「5.7(3) 「種別」および「形式」プルダウンメニューの内容」を参照してください。
- ここで説明した手順では，メッセージテキストを分割する際，区切り文字で分割しました。区切り文字以外に，バイト単位でメッセージテキストを分割することもできます。詳細は，「3.4 メッセージテキストを分割する方法」を参照してください。

3.2.5 メッセージテキストに不足している情報を監査ログに埋め込む

「3.2.4 メッセージテキストを監査ログフォーマットに対応づける」で，メッセージテキスト上にある情報は，監査ログフォーマットに対応づけました。

次に，監査ログとして必要な情報がメッセージテキスト上にない場合に，不足している情報を監査ログに埋め込みます。監査ログに情報を埋め込むことを「フィールドを生成する」ともいいます。

情報を監査ログに埋め込む方法は，次の 2 種類があります。

- JP1 イベントの属性値から埋め込む
- 任意の文字列を埋め込む

ここでは，次の情報を監査ログに埋め込みます。

表 3-3 監査ログに埋め込む情報と埋め込む方法

埋め込む情報	埋め込む方法
日時	JP1 イベントの属性値から埋め込む
共通情報－監査事象の結果	
共通情報－発生場所	
共通情報－メッセージ ID	
共通情報－監査事象の種別	任意の文字列を埋め込む
共通情報－プログラム名	
共通情報－コンポーネント名	
固有情報（事象情報）－オブジェクト情報	
固有情報（事象情報）－動作情報	

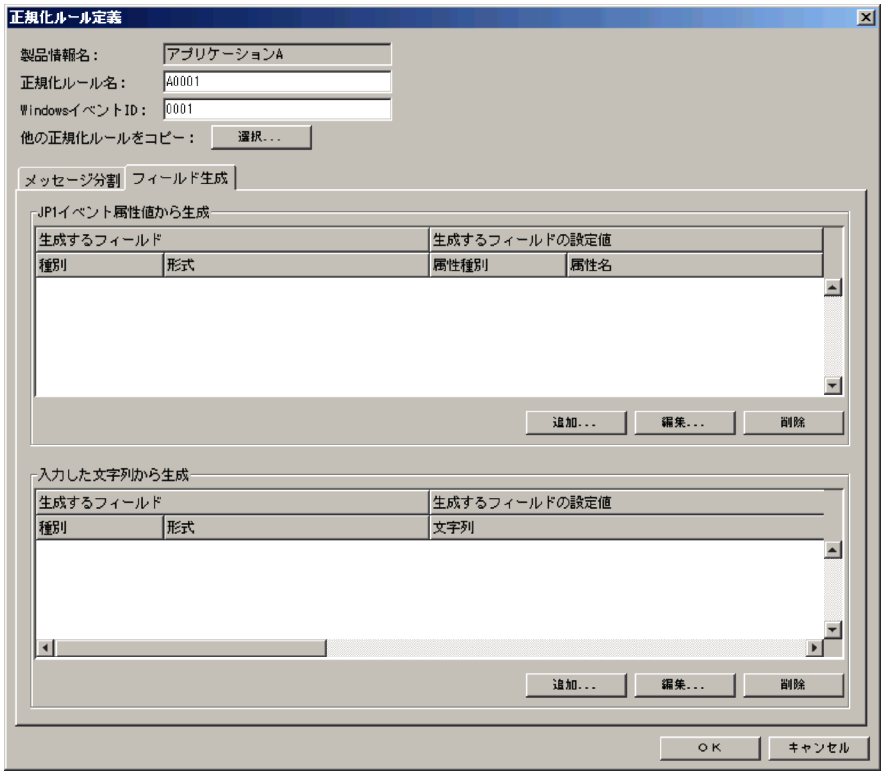
手順を次に示します。

(1) 手順

1. **［正規化ルール定義］ダイアログで，［フィールド生成］タブをクリックする。**

［フィールド生成］タブの項目が表示されます。

図 3-11　［フィールド生成］タブ



2.「JP1 イベント属性値から生成」の［追加］ボタンをクリックする。

［生成フィールド定義］ダイアログが表示されます。

図 3-12　［生成フィールド定義］ダイアログ（JP1 イベント属性値を埋め込む場合）

3. JP1 イベントの属性値から埋め込む情報を定義する。

ここでは，まず，日時の情報を埋め込む定義をします。［生成フィールド定義］ダイアログの各項目に，次の内容を指定します。

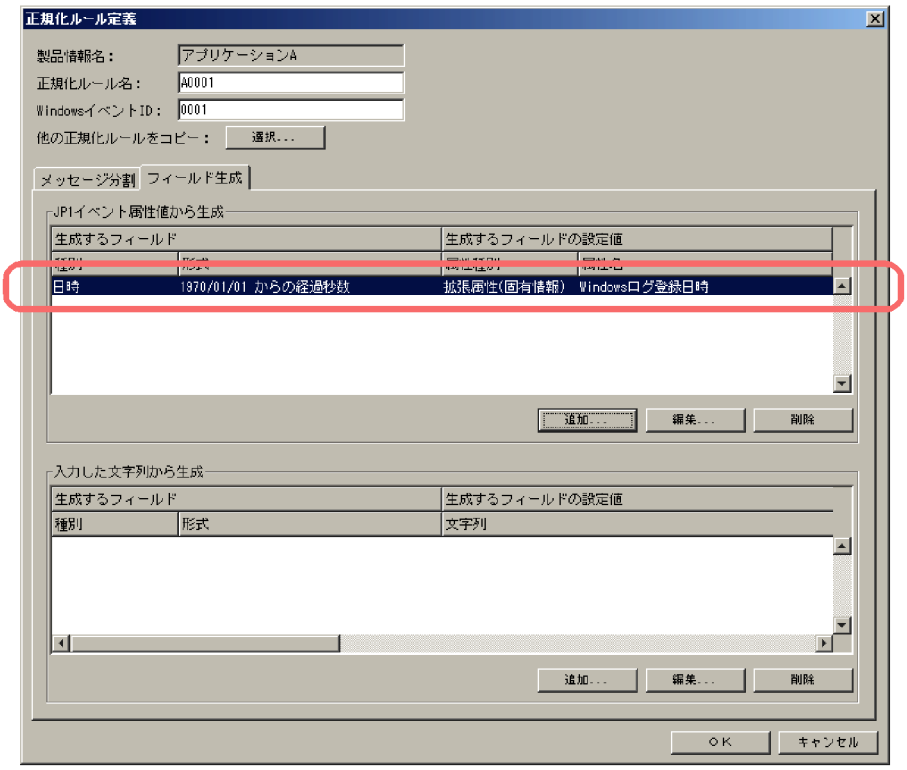
表 3-4 日時の情報を埋め込むための定義内容

項目	設定する内容	説明
種別	日時	埋め込む情報が，監査ログフォーマットのどの種別に当たるかを選択します。 ここでは，日時の情報を埋め込むので，「日時」を選択します。
形式	1970/01/01 からの経過秒数	埋め込む情報を，監査ログフォーマットのどの形式に変換するかを選択します。 ここでは，「1970/01/01 からの経過秒数」を選択します。
属性種別	拡張属性（固有情報）	埋め込む情報は，どの JP1 イベント属性値に当たるかを選択します。 ここでは，「拡張属性（固有情報）」の「Windows ログ登録日時」を選択します。
属性名	Windows ログ登録日時	

4. **［OK］ボタンをクリックする。**

［正規化ルール定義］ダイアログの「JP1 イベント属性値から生成」に，定義した内容が表示されます。

図 3-13 定義した日時の情報が表示された［フィールド生成］タブ

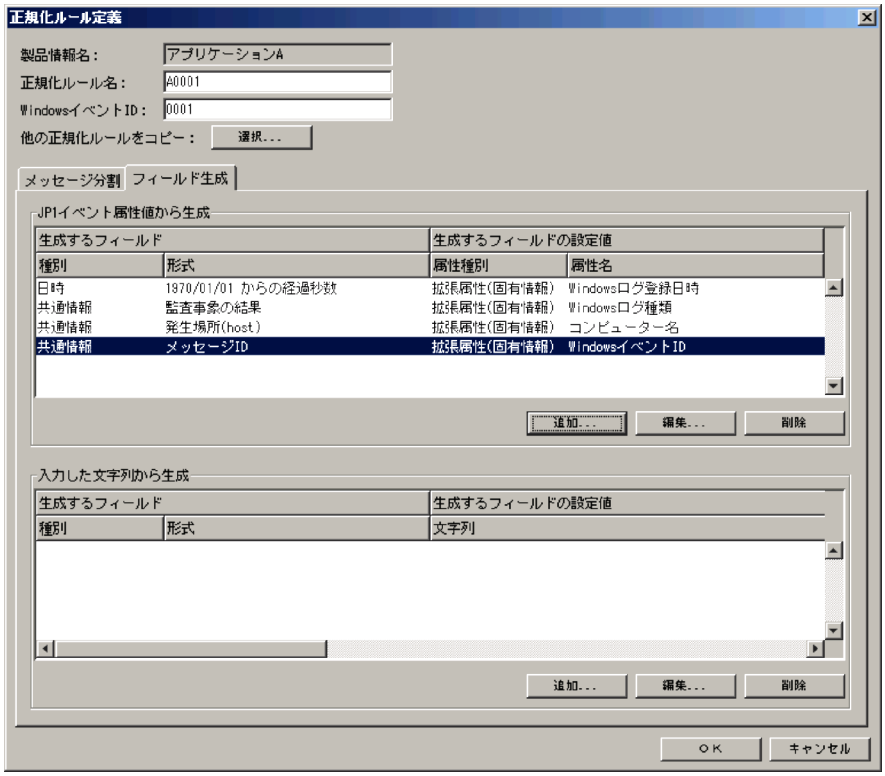


5. **日時の情報を埋め込んだ要領で，日時以外の情報も埋め込む。**

ここでは，「共通情報－監査事象の結果」，「共通情報－発生場所」，および「共通情報

－メッセージ ID」の情報を JP1 イベントの属性値から埋め込みます。

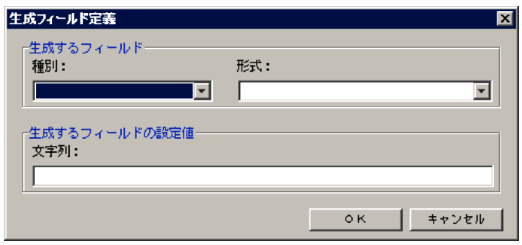
図 3-14　日時以外の情報を JP1 イベント属性値から対応づけた［フィールド生成］タブ



次に，監査ログに必要な情報が JP1 イベントの属性値にない場合に，任意の文字列を監査ログの情報として埋め込みます。

6. **［フィールド生成］タブの「入力した文字列から生成」で，［追加］ボタンをクリックする。**
［生成フィールド定義］ダイアログが表示されます。

図 3-15　［生成フィールド定義］ダイアログ（文字列を埋め込む場合）



7. **監査ログに埋め込む情報を入力する。**
ここでは，まず，「監査事象の種別」情報を入力し，監査ログに埋め込みます。［生成

フィールド定義］ダイアログの各項目に，次の内容を指定します。

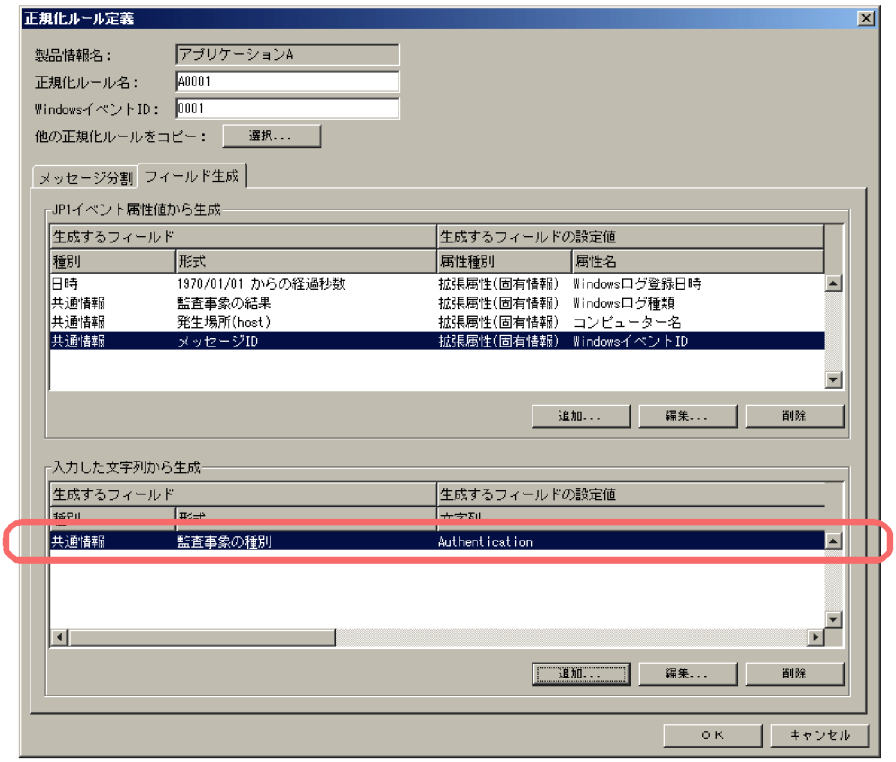
表 3-5 「コンポーネント名」情報を埋め込むための定義内容

項目	設定する内容	説明
種別	共通情報	埋め込む情報が，監査ログフォーマットのどの種別および形式に当たるかを選択します。 ここでは，「共通情報」および「監査事象の種別」を選択します。
形式	監査事象の種別	
文字列	Authentication	監査ログに埋め込む情報を入力します。 ここでは，メッセージ「A0001」の監査事象の種別に当たる「Authentication」を入力します。

8. **［OK］ボタンをクリックする。**

［正規化ルール定義］ダイアログの「入力した文字列から生成」に，定義した内容が表示されます。

図 3-16 定義した監査事象の種別が表示された［フィールド生成］タブ

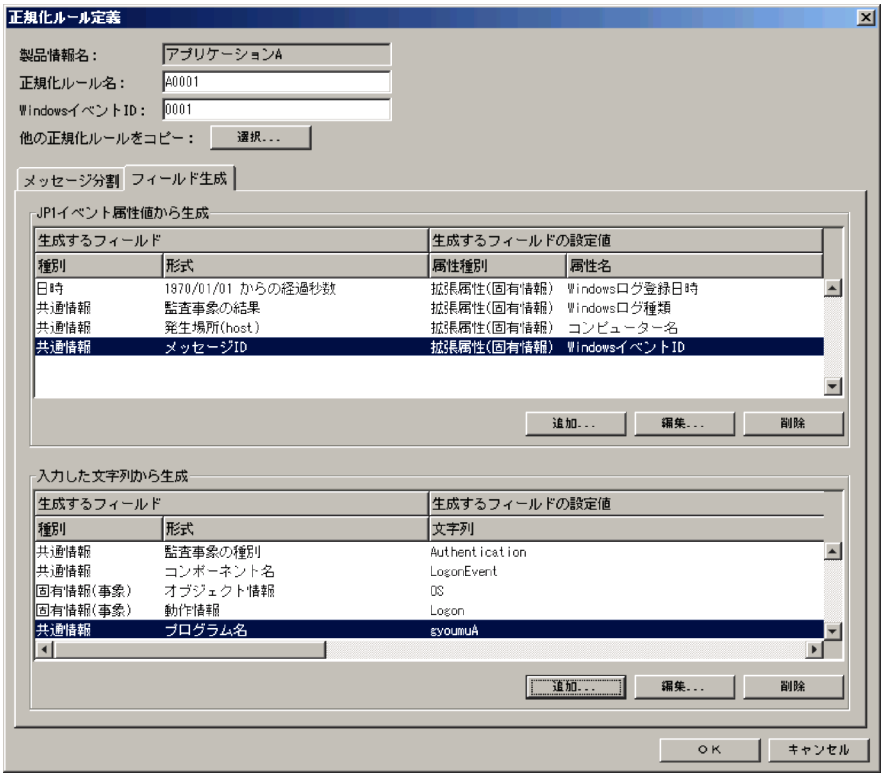


9. **コンポーネント名の情報を埋め込んだ要領で，コンポーネント名以外の情報も埋め込む。**

ここでは，「共通情報－コンポーネント名」，「固有情報（事象情報）－オブジェクト情報」，「固有情報（事象情報）－動作情報」，および「共通情報－プログラム名」の

情報を入力し，監査ログに埋め込みます。

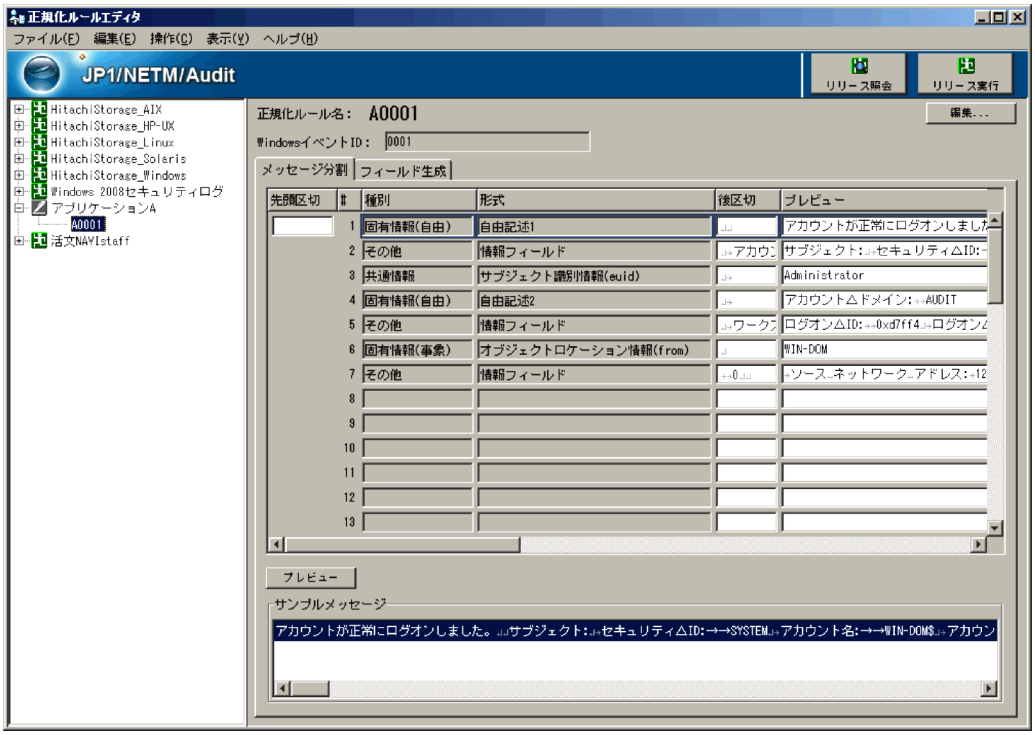
図 3-17　監査事象の種別以外の情報に任意の文字列を対応づけた［フィールド生成］タブ



10. **［正規化ルール定義］ダイアログの［OK］ボタンをクリックする。**

正規化ルール定義中にエラーがない場合は，メイン画面のツリーエリアに，定義した正規化ルールが表示されます。

図 3-18　正規化ルールの定義が完了したメイン画面



正規化ルール定義中にエラーがある場合，確認メッセージが表示されます。［はい］ボタンをクリックすると，正規化ルールを一時的に保存できます。一時的に保存した場合，製品情報のアイコンが「  （「編集（未完了）」状態）」に変わります。

図 3-19　製品状態のアイコンが「編集（未完了）」状態に変わったツリーエリア

次回編集時に，エラーのある個所を修正してください。一度定義した正規化ルールを変更する方法については，「4.2.1 「編集」状態の正規化ルールの定義を変更する」を参照してください。

注意事項

正規化ルール名と Windows イベント ID にエラーがある場合はエラーメッセージが表示され，保存できません。エラー部分を入力方法に従って修正してください。この項目の入力方法の詳細は「5.7 ［正規化ルール定義］ダイアログ」を参照してください。

これで，正規化ルールの定義は完了です。次に，正規化ルールを変換で使用できる状態にします。

(2) 関連情報

- ［フィールド生成］タブの項目の詳細については，「5.7(2) ［フィールド生成］タブ」を参照してください。
- ［生成フィールド定義］ダイアログの項目の詳細については，「5.10 ［生成フィールド定義］ダイアログ」を参照してください。

3.2.6 正規化ルールを変換で使用できる状態にする

正規化ルールを定義したら，正規化ルールを変換で使用できる状態に変更します。手順を次に示します。

(1) 手順

1. **ツリーエリアで，正規化ルールが定義されている製品情報を選択し，ボタンエリアにある［リリース許可］ボタンをクリックする。**
   製品情報のアイコンが次のように変わります。

図 3-20　製品情報のアイコンが「リリース許可」状態に変わったツリーエリア

このアイコンは，「リリース許可」状態であることを示します。
「リリース」とは，監査ログへの変換で正規化ルールを使用できるようにすることで，「リリース許可」とは，リリースを許可した状態のことです。

「リリース許可」状態に変わったことを確認できたら，リリースします。

2. **ボタンエリアにある［リリース実行］ボタンをクリックする。**
   確認メッセージが表示されます。［はい］ボタンをクリックすると，「リリース許可」状態の製品情報が，すべて「リリース」状態に変わります。

図 3-21　製品情報のアイコンが「リリース」状態に変わったツリーエリア

「リリース」状態の製品情報に定義されている正規化ルールは，監査ログへの変換で使用できる状態になります。

これで，正規化ルールエディタを使って正規化ルールを定義する作業は完了です。続いて，次のファイルを作成してください。

- 製品定義ファイル
- 監査ログレポートに関する定義ファイル（任意）

これらのファイルを作成する方法については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の設計・構築編にある，標準サポートされていないプログラムを収集対象とするための準備について説明している個所を参照してください。

注意事項

動作定義ファイルの作成は，Windows イベントログの正規化ルールを定義する場合は不要です。

(2) 関連情報

- ［リリース許可］ボタン，［リリース実行］ボタンなど，ボタンエリアにある項目の詳細については，「5.3　メイン画面－ボタンエリア」を参照してください。
- ツリーエリアで製品情報の隣に表示されるアイコンは，「リリース」状態や「リリース許可」状態以外にも種類があります。正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

3.3　正規化ルールの定義操作（ログファイルの場合）

ログファイルに出力されたログメッセージの正規化ルールを定義します。

ここでは，「業務プログラム B」というプログラムのログの正規化ルールを定義する例に沿って説明します。

「業務プログラム B」のログは，次のフォーマットで出力されます。

```
seqnum=1△2008/01/09△14:48:26.687△[Information]△KMMV4010-I△業務プログラムBを開始します。△[MANAGER01,3388,COMP001,StartStop]
```

（凡例）△：半角スペースを示します。

また，「業務プログラム B」は，gyoumu.exe というプログラムの実行によって動作します。

3.3.1　定義の流れ

ログファイルに出力されたログメッセージの正規化ルールを定義する流れを次の表に示します。

表 3-6　ログファイルに出力されたログメッセージの正規化ルールを定義する流れ

手順	作業		作業の説明	参照先
1	監査ログ収集対象プログラムの製品情報を定義する		監査ログ収集対象プログラムの製品情報を定義します。 製品情報は，監査ログへの変換で使用する正規化ルールを特定するための情報になります。	3.3.2
2	正規化ルールを定義する	正規化ルールの名称を定義する	ツリーエリアに表示する正規化ルールの名称を定義します。	3.3.3
3		メッセージテキストを監査ログフォーマットに対応づける	収集したログファイルのメッセージテキストを監査ログフォーマットに対応づけます。	3.3.4
4		メッセージテキストに不足している情報を監査ログに埋め込む	監査ログに必要な情報が，メッセージテキストには含まれていない場合に，不足している情報を監査ログに埋め込みます。	3.3.5
5	正規化ルールを変換で使用できる状態にする		定義した正規化ルールを，監査ログへの変換で使用できるようにします。	3.3.6

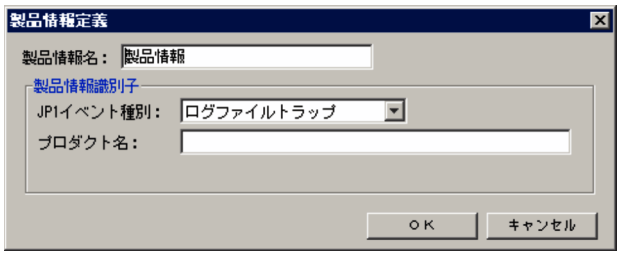
3.3.2　監査ログ収集対象プログラムの製品情報を定義する

監査ログへの変換では，JP1/NETM/Audit に登録されている正規化ルールのうち，どれを使用するかを決めるための情報が必要です。その情報となる，監査ログ収集対象プログラムの製品情報を定義します。手順を次に示します。

(1) 手順

1. **メイン画面で，[ファイル] − [新規作成] − [製品情報] を選択する。**
   [製品情報定義] ダイアログが表示されます。

図 3-22 [製品情報定義] ダイアログ



2. **「製品情報名」に，定義する製品情報の名称を入力する。**
   定義した製品情報名は，ツリーエリアに表示されます。
   ここでは，「業務プログラム B」と入力します。

3. **「JP1 イベント種別」で，「ログファイルトラップ」を選択する。**
   ログファイルは，JP1/Base のログファイルトラップで収集されるので，「ログファイルトラップ」を選択します。

4. **「プロダクト名」に，ログファイルを出力する監査ログ収集対象プログラム名を入力する。**
   ここでは，「gyoumu」と入力します。

注意事項

「/」は「_」に置き換えて入力してください。また，ここで「プロダクト名」に入力する内容は，次のファイルに設定する内容と一致させる必要があります。

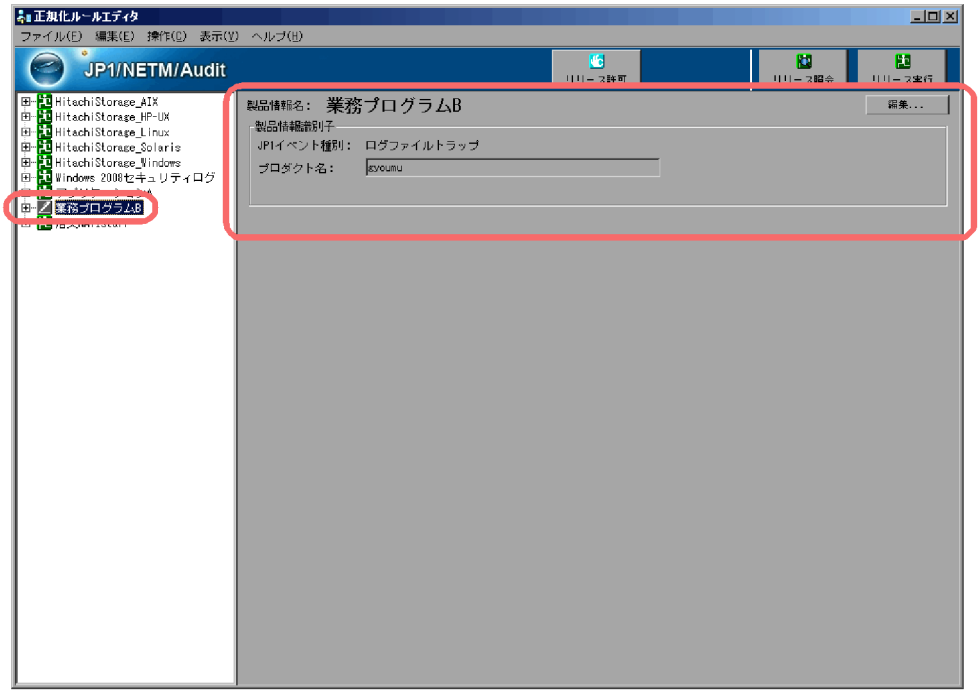
- 製品定義ファイルのパラメーター「プログラム」の値と一致させる。
  製品定義ファイルは，正規化ルールを定義したあとに，監査ログ収集マネージャの［製品定義の編集］ダイアログで作成します。
- 動作定義ファイル名「admjevlog_XXXXX.conf」の「XXXXX」と一致させる。
  動作定義ファイルは，正規化ルールを定義したあとに作成します。

製品定義ファイルおよび動作定義ファイルの作成については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の設計・構築編にある，標準サポートされていないプログラムを収集対象とするための準備について説明している個所を参照してください。

5. **[OK] ボタンをクリックする。**

定義した製品情報がツリーエリアと詳細エリアに表示されます。

図 3-23　業務プログラム B の製品情報が表示されたツリーエリアと詳細エリア



(2) 関連情報

［製品情報定義］ダイアログの項目の詳細については，「5.6　［製品情報定義］ダイアログ」を参照してください。

3.3.3　正規化ルールの名称を定義する

製品情報を定義したら，監査ログ収集対象プログラムの正規化ルールを定義します。

まず，正規化ルールの名称を登録します。手順を次に示します。

(1) 手順

1. **ツリーエリアで，製品情報「業務プログラム B」の製品情報のアイコンを確認する。**
   製品情報の隣にあるアイコンは，正規化ルールの定義の状態を表します。
   正規化ルールの定義は，正規化ルールの定義の状態（製品情報のアイコン）が次の場合に実施できます。
   - 「編集」状態

     
     正規化ルールが一つも定義されていない状態，または定義が完了している状態（「編集（完了）状態」）

正規化ルールの定義中が未完了のまま，一時的に保存している状態（「編集（未完了）状態」）

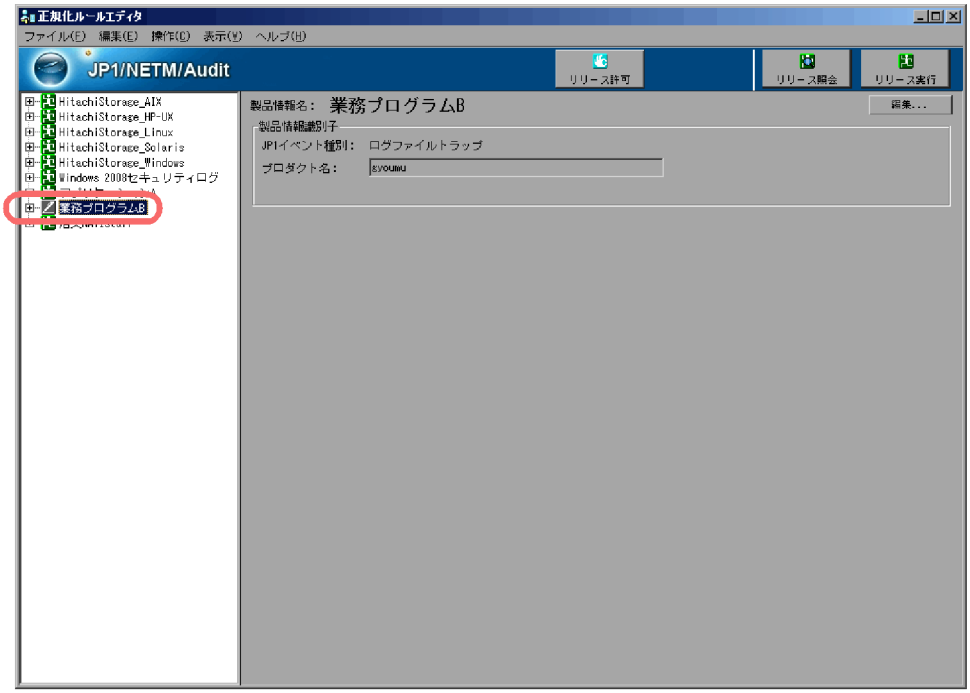
- 「リリース」状態

- 「リリース編集」状態

  正規化ルールの定義が完了している状態（「リリース編集（完了）状態」）

  正規化ルールの定義中が未完了のまま，一時的に保存している状態（「リリース編集（未完了）状態」）

図 3-24　ツリーエリアで業務プログラム B の製品情報のアイコンが「編集」状態になっている例

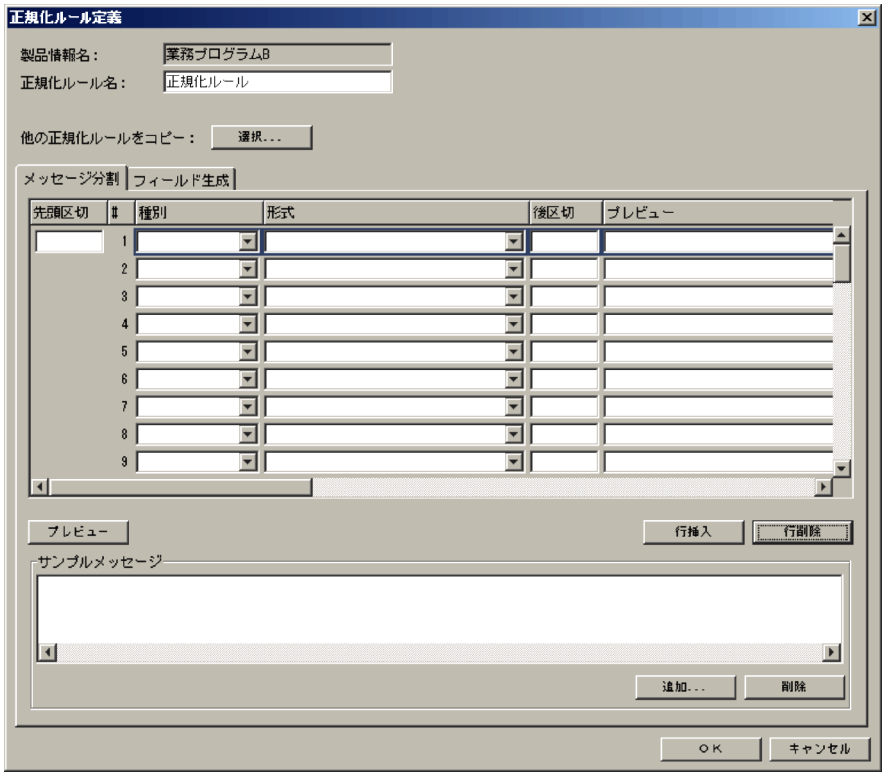


「業務プログラム B」の製品情報のアイコンが，「 (「リリース許可」状態)」または「 (「リリース解除許可」状態)」の場合は，正規化ルールの定義の状態を変更してください。
正規化ルールの定義の状態，および状態を変更する方法については，「5.4　メイン画面－ツリーエリア」を参照してください。

2. **ツリーエリアで製品情報を選択して，［ファイル］－［新規作成］－［正規化ルール］を選択する。**

［正規化ルール定義］ダイアログが表示されます。

図 3-25　［正規化ルール定義］ダイアログ



3. **「正規化ルール名」に，定義する正規化ルールの名称を入力する。**
定義した正規化ルール名は，ツリーエリアに表示されます。
ここでは，「正規化ルール」と入力します。

これで，正規化ルールの名称を登録できました。次に，メッセージテキストを監査ログフォーマットに対応づけます。［正規化ルール定義］ダイアログを開いた状態で，次項を参照してください。

(2) 関連情報

［正規化ルール定義］ダイアログの項目の詳細については，「5.7 ［正規化ルール定義］ダイアログ」を参照してください。

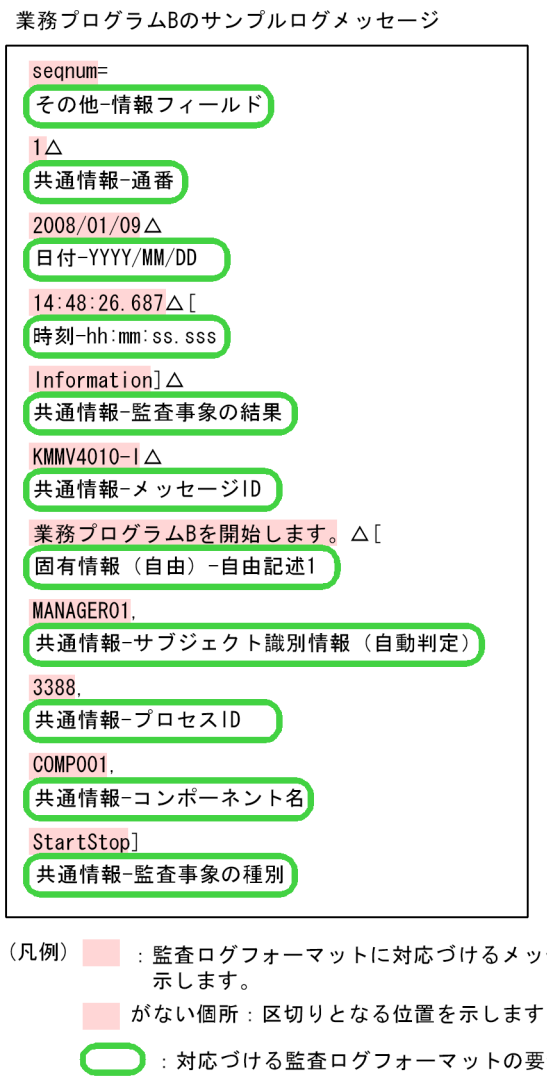
3.3.4 メッセージテキストを監査ログフォーマットに対応づける

「1.3　メッセージテキストを監査ログフォーマットにどのように対応づけるか」で検討

した内容に沿って，ログファイルのメッセージテキストを分割し，監査ログフォーマットに対応づけます。

ここでは，業務プログラム B のログファイルのメッセージテキストを次の図のように分割し，監査ログフォーマットに対応づけます。

図 3-26　業務プログラム B のメッセージテキストの分割



メッセージテキストを分割するために，まず，サンプルとなるメッセージテキストを登録します。手順を次に示します。

(1) 手順

1. **［正規化ルール定義］ダイアログの［メッセージ分割］タブにある，「サンプルメッ**

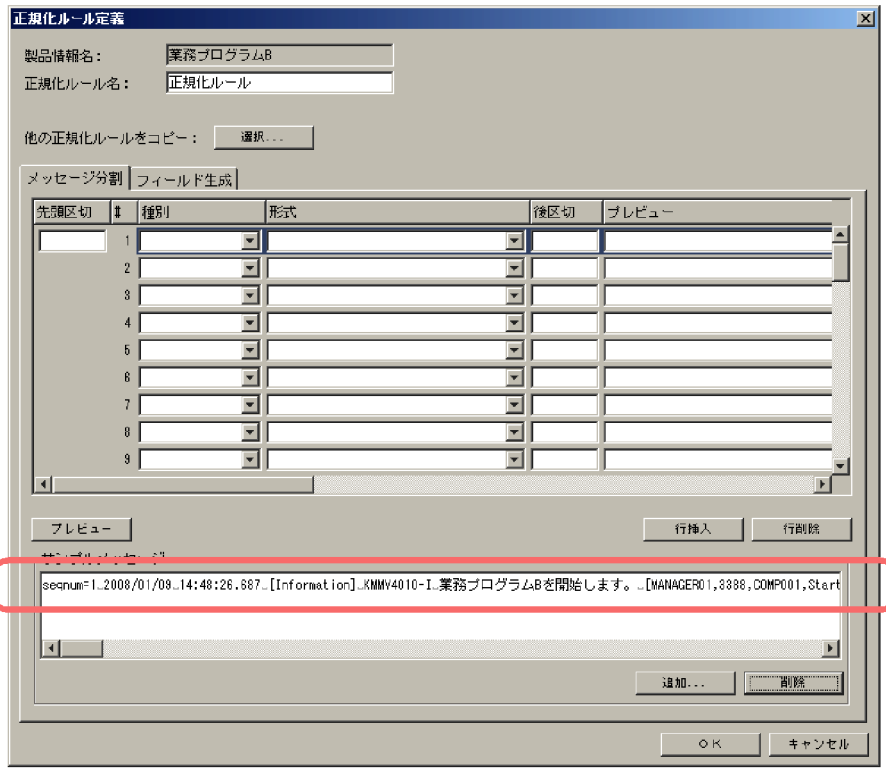
セージ」の［追加］ボタンをクリックする。
［サンプルメッセージ追加］ダイアログが表示されます。

図 3-27　［サンプルメッセージ追加］ダイアログ

2. **サンプルとなるメッセージテキストを「サンプルメッセージ」に入力する。**
ここでは，業務プログラム B のメッセージテキストを入力します。

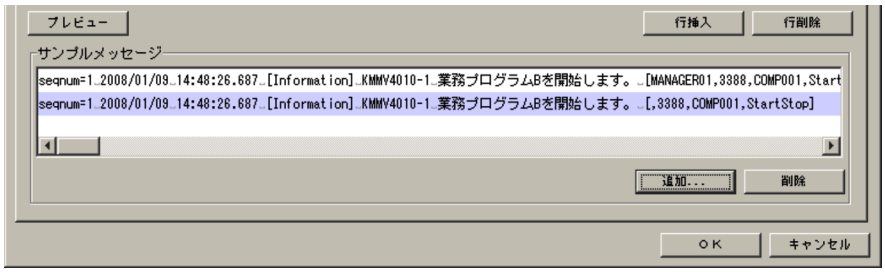
3. **［OK］ボタンをクリックする。**
［メッセージ分割］タブの「サンプルメッセージ」に，入力したサンプルメッセージが表示されます。

図 3-28　サンプルメッセージが表示された［正規化ルール定義］ダイアログ



サンプルメッセージは，3 件まで登録できます。参考に，もう 1 件，サンプルメッセージを登録します。

図 3-29 サンプルメッセージをもう 1 件追加した［正規化ルール定義］ダイアログ



次に，登録したサンプルメッセージテキストを分割し，分割した各要素に監査ログフォーマットの要素を対応づけます。

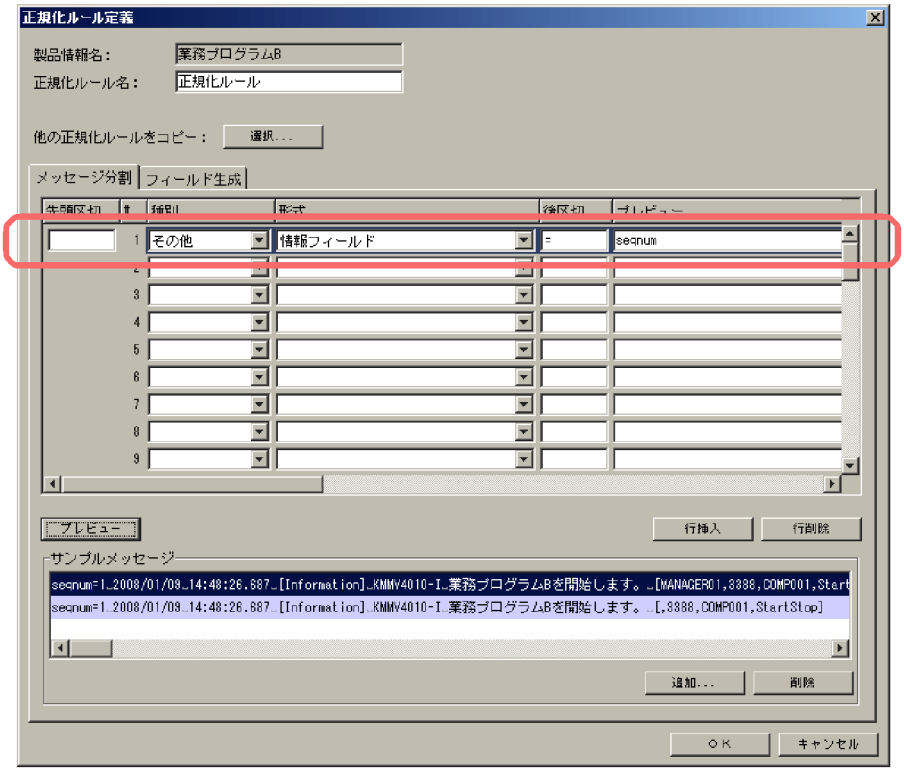
4. **メッセージテキストの先頭の要素に対応づける監査ログフォーマットの要素を，「種別」と「形式」プルダウンメニューから選択する。**
   ここでは，業務プログラム B のメッセージテキストを図 3-26 のように分割します。先頭の要素は，「seqnum」です。「seqnum」には，「その他」種別を対応づけるので，「種別」プルダウンメニューで「その他」を，「形式」プルダウンメニューで「情報フィールド」を選択します。

   次に，メッセージテキストを「seqnum」で区切ります。

5. **先頭の要素「seqnum」で区切るために，「サンプルメッセージリスト」で分割するメッセージテキストを選択し，「後区切」に区切りとなる情報を入力する。**
   区切りとなるのは，「=」です。
   ［メッセージ分割］タブの 1 行目の「後区切」に「=」を入力してください。

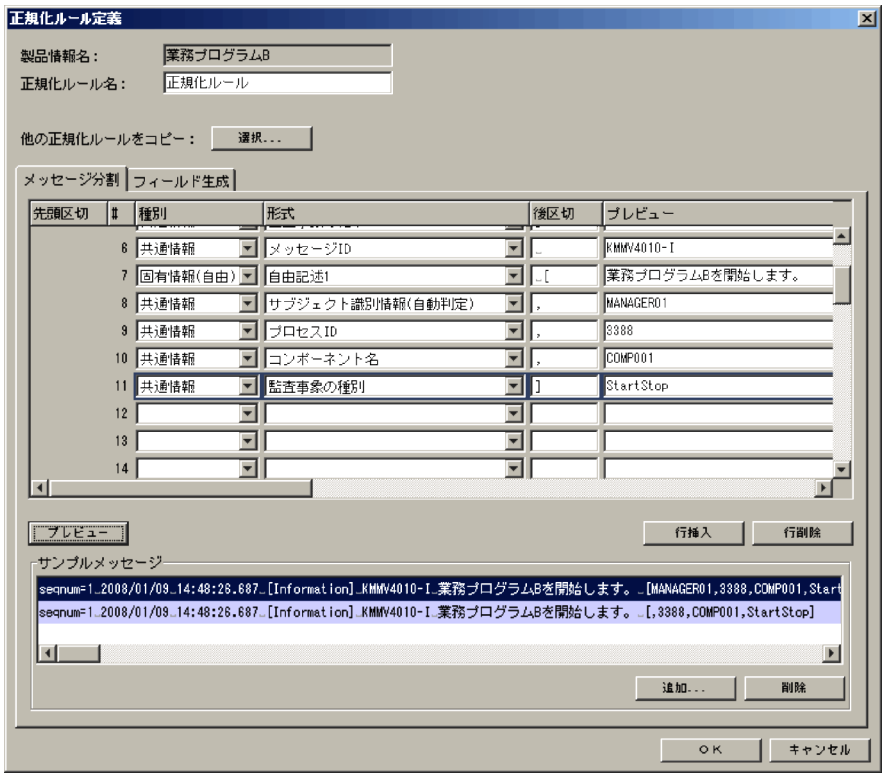
6. **［プレビュー］ボタンをクリックする。**
   「プレビュー」に「seqnum」が表示されていれば，正常に分割されています。

図 3-30　メッセージテキストの先頭の要素を定義した［正規化ルール定義］ダイアログ



7. **先頭の要素を定義した要領で，以降のメッセージテキストを分割し，監査ログフォーマットの要素を対応づける。**
   図 3-26 に従って，監査ログフォーマットの種別と形式を対応づけます。

図 3-31 メッセージテキストすべてを監査ログフォーマットに対応づけた［正規化ルール定義］ダイアログ



空行ができないように入力してください。
途中で分割位置を誤り，分割位置を増やしたり減らしたりしたい場合は，［行挿入］ボタンまたは［行削除］ボタンで修正してください。［行挿入］ボタンは，カーソルがある行の上に空行を挿入します。［行削除］ボタンは，カーソルがある行を削除します。［行挿入］ボタンまたは［行削除］ボタンを使用すると，「プレビュー」の内容がいったん削除されます。

これで，メッセージテキストを監査ログフォーマットの要素に対応づける操作は完了です。

次に，メッセージテキストに不足している情報を，監査ログに埋め込む定義をします。［正規化ルール定義］ダイアログを開いた状態で，次項を参照してください。

(2) 関連情報

- すでに定義してある正規化ルールの定義，および標準サポート製品のテンプレートを流用して，新規に正規化ルールを定義することもできます。［正規化ルール定義］ダイアログの［選択］ボタンで，流用する正規化ルールを選択します。［正規化ルール定義］ダイアログの項目については，「5.7 ［正規化ルール定義］ダイアログ」を参照し

てください。

- ［正規化ルール定義］ダイアログの，「種別」および「形式」プルダウンメニューの各項目については，「5.7(3) 「種別」および「形式」プルダウンメニューの内容」を参照してください。
- ここで説明した手順では，メッセージテキストを分割する際，区切り文字で分割しました。区切り文字以外に，バイト単位でメッセージテキストを分割することもできます。詳細は，「3.4 メッセージテキストを分割する方法」を参照してください。

3.3.5 メッセージテキストに不足している情報を監査ログに埋め込む

「3.3.4 メッセージテキストを監査ログフォーマットに対応づける」で，メッセージテキスト上にある情報は，監査ログフォーマットに対応づけました。

次に，監査ログとして必要な情報がメッセージテキスト上にない場合に，不足している情報を監査ログに埋め込みます。監査ログに情報を埋め込むことを「フィールドを生成する」ともいいます。

情報を監査ログに埋め込む方法は，次の 2 種類があります。

- JP1 イベントの属性値から埋め込む
- 任意の文字列を埋め込む

ここでは，次の情報を監査ログに埋め込みます。

表 3-7 監査ログに埋め込む情報と埋め込む方法

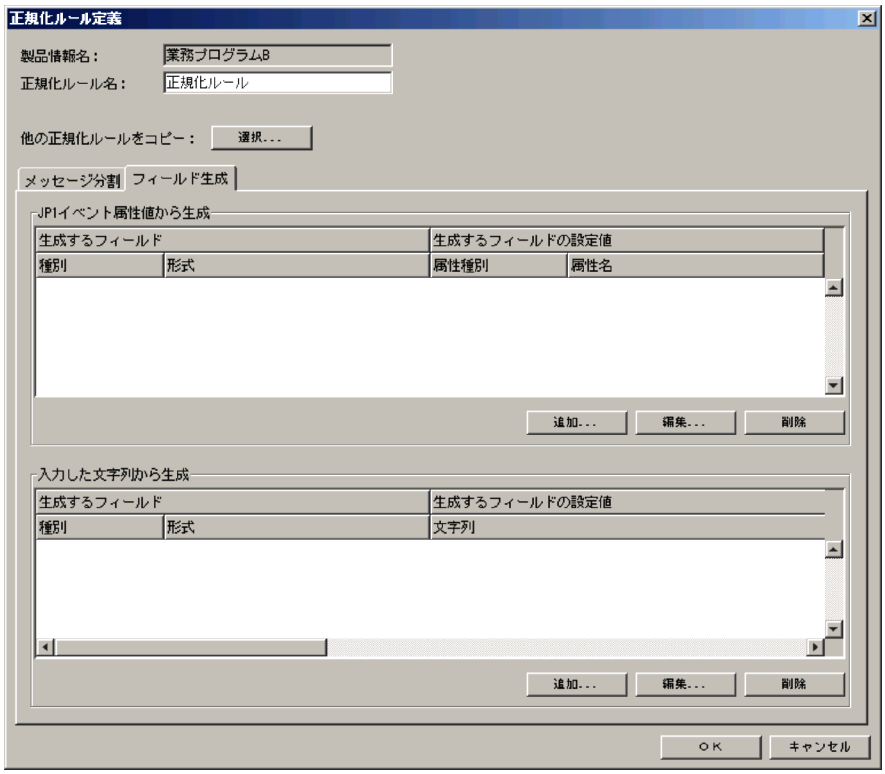
埋め込む情報	埋め込む方法
共通情報－発生場所（自動判定）	JP1 イベントの属性値から埋め込む
共通情報－プログラム名	任意の文字列を埋め込む

手順を次に示します。

(1) 手順

1. **［正規化ルール定義］ダイアログで，［フィールド生成］タブをクリックする。**
   ［フィールド生成］タブの項目が表示されます。

図 3-32 ［フィールド生成］タブ



2.「JP1 イベント属性値から生成」で，［追加］ボタンをクリックする。

［生成フィールド定義］ダイアログが表示されます。

図 3-33 ［生成フィールド定義］ダイアログ（JP1 イベント属性値を埋め込む場合）

3. JP1 イベントの属性値から埋め込む情報を定義する。

ここでは，「発生場所」の情報を埋め込む定義をします。［生成フィールド定義］ダイアログの各項目に，次の内容を指定します。

表 3-8 プログラム名の情報を埋め込むための定義内容

項目	設定する内容	説明
種別	共通情報	埋め込む情報が，監査ログフォーマットのどの種別に当たるかを選択します。 ここでは，プログラム名の情報を埋め込むので，「共通情報」を選択します。
形式	発生場所（自動判定）※	埋め込む情報を，監査ログフォーマットのどの形式に変換するかを選択します。 ここでは，「発生場所（自動判定）」を選択します。
属性種別	基本属性	埋め込む情報は，どの JP1 イベント属性値に当たるかを選択します。 ここでは，「基本属性」の「発行元イベントサーバ名」を選択します。
属性名	発行元イベントサーバ名	

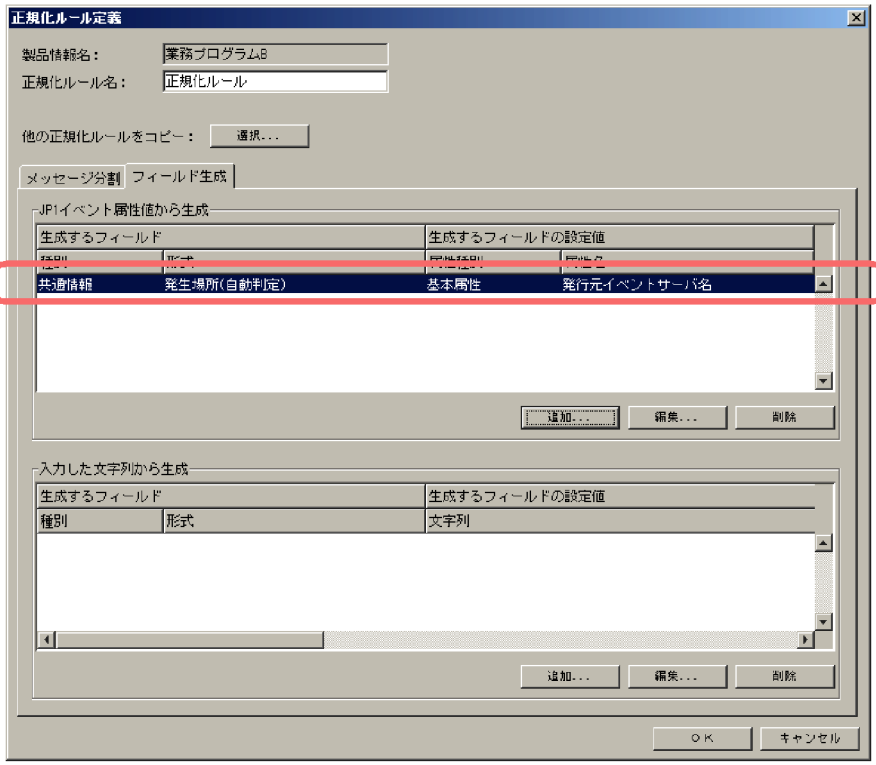
注※

「発生場所」形式には，「発生場所（host）」，「発生場所（ipv4）」，「発生場所（ipv6）」，および「発生場所（自動決定）」があります。JP1 イベント属性値に出力される情報が，確実にホスト名の場合は（host）を，IPv4 アドレスの場合は（ipv4）を，IPv6 アドレスの場合は（ipv6）を選択します。どの形式で出力されるかわからない場合は，（自動判定）を選択します。ここで対応づけている JP1 イベント属性値「基本属性－発行元イベントサーバ名」は，ホスト名で出力されたり IP アドレスで出力されたりすることがあるため，（自動判定）を対応づけます。

4. **［OK］ボタンをクリックする。**

［正規化ルール定義］ダイアログの「JP1 イベント属性値から生成」に，定義した内容が表示されます。

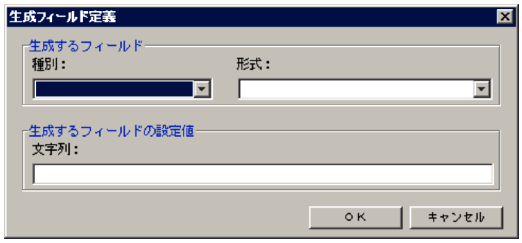
図 3-34 定義した発生場所の情報が表示された［フィールド生成］タブ



次に，監査ログに必要な情報が JP1 イベントの属性値にない場合に，任意の文字列を監査ログの情報として埋め込みます。

5. **［フィールド生成］タブの「入力した文字列から生成」で，［追加］ボタンをクリックする。**
［生成フィールド定義］ダイアログが表示されます。

図 3-35 ［生成フィールド定義］ダイアログ（文字列を埋め込む場合）



6. **監査ログに埋め込む情報を入力する。**
ここでは，「プログラム名」に当たる情報を入力し，監査ログに埋め込みます。［生成フィールド定義］ダイアログの各項目に，次の内容を指定します。

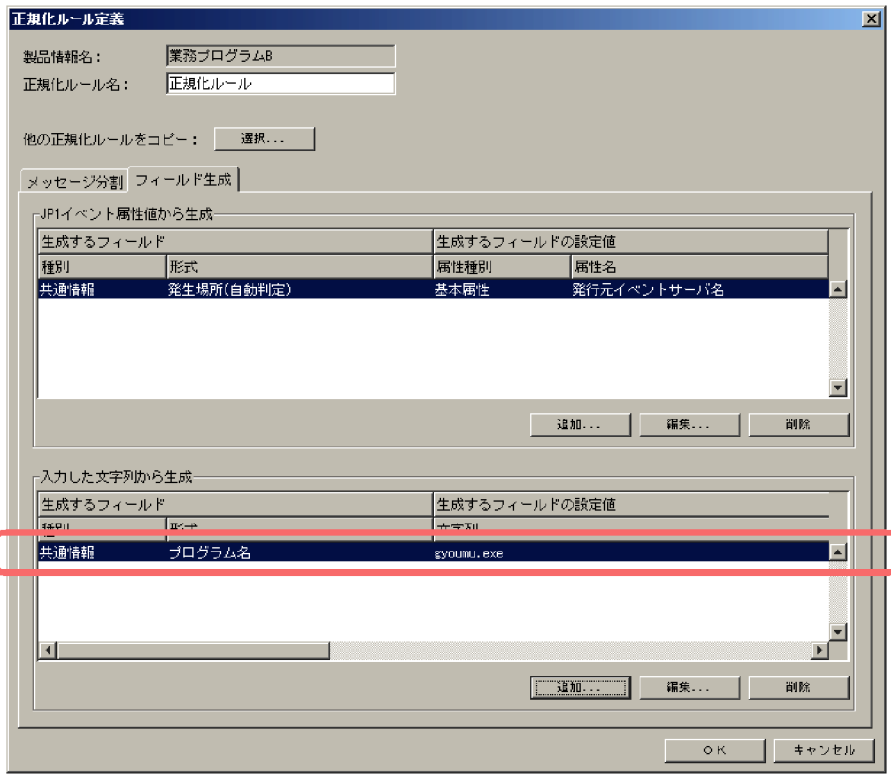
表 3-9 「オブジェクト情報」を埋め込むための定義内容

項目	設定する内容	説明
種別	共通情報	埋め込む情報が，監査ログフォーマットのどの種別および形式に当たるかを選択します。 ここでは，「共通情報」種別および「プログラム名」形式を選択します。
形式	プログラム名	
文字列	gyoumu.exe	監査ログに埋め込む情報を入力します。 ここでは，プログラム名に当たる「gyoumu.exe」を入力します。

7. ［OK］ボタンをクリックする。

［正規化ルール定義］ダイアログの「入力した文字列から生成」に，定義した内容が表示されます。

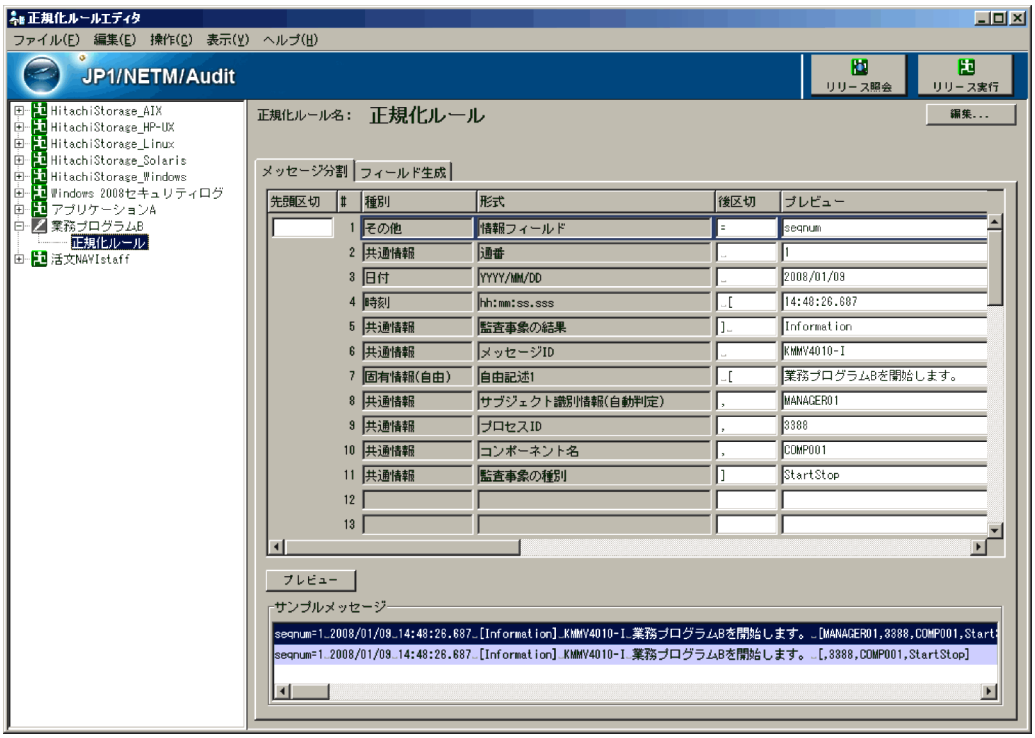
図 3-36　定義したプログラム名が表示された［フィールド生成］タブ



8. ［正規化ルール定義］ダイアログの［OK］ボタンをクリックする。

正規化ルール定義中にエラーがない場合は，メイン画面のツリーエリアに，定義した正規化ルールが表示されます。

図 3-37　正規化ルールの定義が完了したメイン画面



正規化ルール定義中にエラーがある場合，確認メッセージが表示されます。［はい］ボタンをクリックすると，正規化ルールを一時的に保存できます。一時的に保存した場合，製品情報のアイコンが「  （「編集（未完了）」状態）」に変わります。

図 3-38　製品状態のアイコンが「編集（未完了）」状態に変わったツリーエリア

次回編集時に，エラーのある個所を修正してください。一度定義した正規化ルールを変更する方法については，「4.2.1 「編集」状態の正規化ルールの定義を変更する」を参照してください。

注意事項

正規化ルール名にエラーがある場合はエラーメッセージが表示され，保存できません。エラー部分を入力方法に従って修正してください。この項目の入力方法の詳細は「5.7 ［正規化ルール定義］ダイアログ」を参照してください。

これで，正規化ルールの定義は完了です。次に，正規化ルールを変換で使用できる状態にします。

(2) 関連情報

- ［フィールド生成］タブの項目の詳細については，「5.7(2) ［フィールド生成］タブ」を参照してください。
- ［生成フィールド定義］ダイアログの項目の詳細については，「5.10 ［生成フィールド定義］ダイアログ」を参照してください。

3.3.6 正規化ルールを変換で使用できる状態にする

正規化ルールを定義したら，正規化ルールを変換で使用できる状態に変更します。手順を次に示します。

(1) 手順

1. **ツリーエリアで，正規化ルールが定義されている製品情報を選択し，［リリース許可］ボタンをクリックする。**
   製品情報のアイコンが次のように変わります。

図 3-39　製品情報のアイコンが「リリース許可」状態に変わったツリーエリア

このアイコンは，「リリース許可」状態であることを示します。
「リリース」とは，監査ログへの変換で正規化ルールを使用できるようにすることで，「リリース許可」とは，リリースを許可した状態のことです。

「リリース許可」状態に変わったことを確認できたら，リリースします。

2. **［リリース実行］ボタンをクリックする。**
「リリース許可」状態の製品情報が，すべて「リリース」状態に変わります。「リリース」状態の製品情報に定義されている正規化ルールは，監査ログへの変換で使用できる状態になります。

図 3-40　製品情報のアイコンが「リリース」状態に変わったツリーエリア

これで，正規化ルールエディタを使って正規化ルールを定義する作業は完了です。続いて，次のファイルを作成してください。

- 製品定義ファイル
- 動作定義ファイル
- 監査ログレポートに関する定義ファイル（任意）

これらのファイルを作成する方法については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の設計・構築編にある，標準サポートされていないプログラムを収集対象とするための準備について説明している個所を参照してください。

(2) 関連情報

●［リリース許可］ボタン，［リリース実行］ボタンなど，ボタンエリアにある項目の詳細については，「5.3　メイン画面－ボタンエリア」を参照してください。

●ツリーエリアで製品情報の隣に表示されるアイコンは，「リリース」状態や「リリース許可」状態以外にも種類があります。正規化ルールの定義の状態と，その状態のときに表示されるアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

3.4 メッセージテキストを分割する方法

メッセージテキストを分割する方法には，次の 2 種類があります。

● 文字列で区切る方法（推奨）

次のように，メッセージテキストを分割したい位置に，半角スペースや「,」（コンマ）などの文字列がある場合は，文字列で区切ります。

####△2007/12/31△00:00:00.000△△△△KKKK0000-E△起動に失敗しました。

（凡例）△：半角スペースを意味します。

区切り文字は，次の規則に従って指定する必要があります。

- 改行とタブ以外の，0x00 ～ 0x1f，および 0x7f の制御コードは，区切り文字に指定できません。
- 半角数字は，数字以外の文字列を組み合わせたときだけ，区切り文字に指定できます。半角数字だけの文字列は指定できません。

文字列でメッセージテキストを区切れない場合は，バイト単位で区切る方法を選択してください。

● バイト単位で区切る方法

次のように，メッセージテキストを分割したい位置に何も文字列がなく，文字列で区切れない場合は，バイト単位で区切ります。何バイトで区切るかを指定します。

#####2007/12/3100:00:00.000KKKK0000-E起動に失敗しました。

メッセージの形式に応じて，二つの方法を使い分けてください。一つのメッセージテキストを分割するのに，二つの方法を組み合わせてもかまいません。

それぞれの入力方法を説明します。

(1) 文字列で区切る方法

区切りとなる文字を［正規化ルール定義］ダイアログの「先頭区切」または「後区切」に入力します。次のメッセージの例を基に，「先頭区切」および「後区切」への入力方法を説明します。

####△2007/12/31△00:00:00.000△△△△KKKK0000-E△起動に失敗しました。

（凡例）△：半角スペースを意味します。

「2007/12/31」，「00:00:00.000」，「KKKK0000-E」，および「起動に失敗しました。」に分割する場合，「先頭区切」および「後区切」に，次のように入力します。

「先頭区切」

「2007/12/31」以降の要素を監査ログに対応づけるために，「#### △」を「先頭区

切」に定義します。
「先頭区切」に定義できるのは 1 件だけです。

「後区切」
次のように入力します。

表 3-10 「後区切」への入力方法（文字列で区切る場合）

種別	形式	後区切	プレビュー
日付	YYYY/MM/DD	△	2007/12/31
時刻	hh:mm:ss.sss	△	00:00:00.000
共通情報	メッセージ ID	△	KKKK0000-E
固有情報（自由）	自由記述 1	－	起動に失敗しました。

（凡例）－：何も指定しないことを示します。

時刻とメッセージ ID の間のように，連続する△（半角スペース）を区切り文字にする場合でも，△（半角スペース）1 文字だけを定義すると，連続する△（半角スペース）が区切り文字として認識されます。

なお，「#### △」を「先頭区切」に指定しないで，監査ログフォーマットの「その他」種別に対応づけても，同様に，「2007/12/31」以降の要素を監査ログに対応づけることができます。「先頭区切」に「#### △」を指定しないで，「その他」種別に対応づける場合，次のように「後区切」に入力します。

表 3-11 「先頭区切」に指定しない場合の「後区切」の入力方法（文字列で区切る場合）

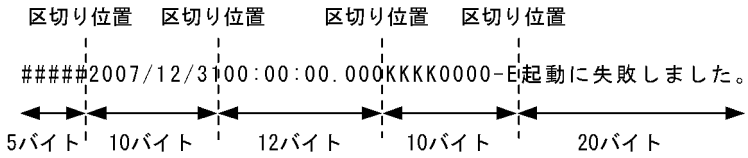
種別	形式	後区切	プレビュー
その他	情報フィールド	△	####
日付	YYYY/MM/DD	△	2007/12/31
時刻	hh:mm:ss.sss	△	00:00:00.000
共通情報	メッセージ ID	△	KKKK0000-E
固有情報（自由）	自由記述 1	－	起動に失敗しました。

（凡例）－：何も指定しないことを示します。

(2) バイト単位で区切る方法

区切り文字がないメッセージテキストを分割する場合は，バイト単位でメッセージテキストを分割します。次のメッセージの例を基に，「先頭区切」および「後区切」への入力方法を説明します。

図 3-41 バイト単位で区切る例



「2007/12/31」,「00:00:00.000」,「KKKK0000-E」, および「起動に失敗しました。」に分割する場合,「先頭区切」および「後区切」に, 次のように入力します。

「先頭区切」

「2007/12/31」以降の要素を監査ログに対応づけるために,「#####」を「先頭区切」にします。「#####」は 5 バイトなので,「先頭区切」に「5」を入力します。
先頭区切として定義できるのは 1 件だけです。

「後区切」

「後区切」には, 直前で区切った位置から何バイトのところで区切るかを指定します。次のように入力します。

表 3-12 「後区切」への入力方法（バイト単位で区切る場合）

種別	形式	後区切	プレビュー
日付	YYYY/MM/DD	10	2007/12/31
時刻	hh:mm:ss.sss	12	00:00:00.000
共通情報	メッセージ ID	10	KKKK0000-E
固有情報（自由）	自由記述 1	20	起動に失敗しました。

単位はバイトです。一度に区切れるのは, 1 ～ 1,023 バイトです。

なお,「#####」を「先頭区切」に指定しないで, 監査ログフォーマットの「その他」種別に対応づけても, 同様に,「2007/12/31」以降の要素を監査ログに対応づけることができます。「先頭区切」に「#####」のバイト数「5」を指定しないで,「その他」種別に対応づける場合, 次のように「後区切」に入力します。

表 3-13 「先頭区切」に指定しない場合の「後区切」の入力方法（バイト単位で区切る場合）

種別	形式	後区切	プレビュー
その他	情報フィールド	5	#####
日付	YYYY/MM/DD	10	2007/12/31
時刻	hh:mm:ss.sss	12	00:00:00.000
共通情報	メッセージ ID	10	KKKK0000-E
固有情報（自由）	自由記述 1	20	起動に失敗しました。

メッセージ中に可変値があり，バイト単位で区切れない場合，文字列で区切る方法と組み合わせてメッセージテキストを分割してもかまいません。

バイト単位で区切る場合の注意事項

バイト単位で区切る場合は，次のことに注意してください。

- 日付情報が 1 けたと 2 けたの両方で出力される場合は，文字列で区切ってください。
  例えば，2009/1/11 や 2009/10/1 のように，月または日が 1 けたで出力されるメッセージの場合，バイト単位で区切ると，バイト数にずれが生じます。このため，文字列で区切るようにしてください。
- メッセージ中にマルチバイトコードの文字列がある場合，1 バイトコードは 1 バイト，2 バイトコードは 2 バイトでカウントしてください。
- メッセージ中の空白（半角スペースおよび全角スペース），または 0x00 ～ 0x1F，および 0x7F の制御コード（タブ文字，改行コードなど）もバイト数でカウントしてください。

4 定義の変更と削除

この章では，定義した製品情報および正規化ルールを，変更したり削除したりする操作について説明します。また，リリースされている定義内容を確認する方法，標準サポート製品の定義を再作成する方法，定義の移行方法についても説明しています。

4.1 製品情報を変更する

ここでは，製品情報の定義を変更する操作について説明します。操作に入る前に，次の点に注意してください。

注意事項

- 「Hitachi Storage」，「Windows 2008 セキュリティログ」，および「活文 NAVIstaff」の正規化ルールは，JP1/NETM/Audit の標準サポート製品として，正規化ルールエディタに初めから定義されています。標準サポート製品の製品情報は，編集しないでください。
- 正規化ルールが定義されている製品情報は，変更しないでください。製品情報を変更する場合は，正規化ルールをいったん削除してください。正規化ルールを削除する方法については，「4.3.2　正規化ルールの定義を削除する」を参照してください。
- 「JP1 イベント種別」の情報は，一度保存すると，そのあと変更できません。変更する場合は，その製品情報を削除してから新規に製品情報の定義を追加してください。なお，正規化ルールが定義されている場合は，正規化ルールも削除する必要があります。

手順を次に示します。

1. **ツリーエリアで，変更する製品情報を選択する。**
   詳細エリアに，製品情報の定義内容が表示されます。
2. **詳細エリアの［編集］ボタンをクリックする。**
   ［製品情報定義］ダイアログが表示されます。
3. **定義内容を変更し，［OK］ボタンをクリックする。**
   変更した製品情報の定義が，詳細エリアに表示されます。

4.2　正規化ルールの定義を変更する

ここでは，正規化ルールの定義を変更する操作について説明します。

操作に入る前に，次の点に注意してください。

注意事項

「Hitachi Storage」，「Windows 2008 セキュリティログ」，および「活文 NAVIstaff」の正規化ルールは，JP1/NETM/Audit の標準サポート製品として，正規化ルールエディタに初めから定義されています。標準サポート製品の正規化ルールは，編集しないでください。

正規化ルールの定義には，正規化ルールの定義の状態が「編集」状態，の場合に変更する方法と，「リリース」状態の場合に変更する方法があります。「リリース」状態の場合に変更する方法では，変更前の正規化ルールがリリースされている状態と並行して，正規化ルールを変更できます。それぞれの手順を次に示します。

4.2.1　「編集」状態の正規化ルールの定義を変更する

ここでは，正規化ルールが定義されている正規化ルールの定義の状態が「編集」状態の場合に，正規化ルールを変更する手順を説明します。

1. **正規化ルールの定義の状態を「編集」状態に変更する。**
   正規化ルールの定義の状態が「編集」状態以外の場合，「編集」状態に変更してください。

図 4-1　正規化ルールを定義した製品情報のアイコンが「編集」状態の例

正規化ルールの定義の状態を変更する方法については，「5.4　メイン画面－ツリーエリア」の，正規化ルールの定義の状態を変更する操作方法についての説明を参照してください。

2. **ツリーエリアで，定義を変更する正規化ルールを選択する。**
   詳細エリアに，正規化ルールの定義内容が表示されます。
3. **詳細エリアの［編集］ボタンをクリックする。**

［正規化ルール定義］ダイアログが表示されます。

4. **定義内容を変更し，［OK］ボタンをクリックする。**
   正規化ルール定義中にエラーがない場合は，変更した正規化ルールの定義が，詳細エリアに表示されます。
   正規化ルール定義中にエラーがある場合，確認メッセージが表示されます。［はい］ボタンをクリックすると，エラーがある状態で，正規化ルールを一時的に保存できます。エラーがある状態で一時的に保存した場合，製品情報のアイコンが「  （「編集（未完了）」状態）」に変わります。
   次回編集時に，エラーのある個所を修正してください。

注意事項

正規化ルール名と Windows イベント ID にエラーがある場合はエラーメッセージが表示され，保存できません。エラー部分を入力方法に従って修正してください。この項目の入力方法の詳細は「5.7 ［正規化ルール定義］ダイアログ」を参照してください。

これで，正規化ルールの定義変更が終わりました。

次に，変更した正規化ルールをリリースします。リリースの操作については「3.2.6 正規化ルールを変換で使用できる状態にする」を参照してください。

4.2.2 「リリース」状態の正規化ルールの定義を変更する

ここでは，正規化ルールが定義されている製品情報が「リリース」状態の場合に，正規化ルールを変更する手順を説明します。

1. **ツリーエリアで，定義を変更する正規化ルールを選択する。**
   詳細エリアに，正規化ルールの定義内容が表示されます。
2. **詳細エリアの［編集］ボタンをクリックする。**
   ［正規化ルール定義］ダイアログが表示されます。
3. **定義内容を変更し，［OK］ボタンをクリックする。**
   正規化ルール定義中にエラーがない場合は，変更した正規化ルールの定義が，詳細エリアに表示されます。ツリーエリアでは，正規化ルールを定義した製品情報のアイコンが，「リリース編集」状態に変わります。

図 4-2　正規化ルールを定義した製品情報のアイコンが「リリース編集」状態に変わったツリーエリア

なお，正規化ルール定義の名称を変更した場合は，リリースするかどうか，確認のメッセージが表示されます。定義内容をすぐにリリースする場合は，［はい］ボタンをクリックしてください。製品情報が，「リリース」状態になります。
あとでリリース実行をする場合は，［後でリリースする］ボタンをクリックしてください。
正規化ルール定義中にエラーがある場合，確認メッセージが表示されます。［はい］ボタンをクリックすると，エラーがある状態で，正規化ルールを一時的に保存できます。エラーがある状態で一時的に保存した場合，製品情報のアイコンが「  （「リリース編集（未完了）」状態）」に変わります。
次回編集時に，エラーのある個所を修正してください。一度定義した正規化ルールを変更する方法については，「4.2.1 「編集」状態の正規化ルールの定義を変更する」を参照してください。

注意事項

正規化ルール名と Windows イベント ID にエラーがある場合はエラーメッセージが表示され，保存できません。エラー部分を入力方法に従って修正してください。この項目の入力方法の詳細は「5.7 ［正規化ルール定義］ダイアログ」を参照してください。

これで，正規化ルールの定義変更が終わりました。

このあと，リリースが必要な場合は，リリースしてください。リリースの操作については「3.2.6　正規化ルールを変換で使用できる状態にする」を参照してください。

参考

リリースされている正規化ルールの定義を変更し，手順 3 で［後でリリースする］を選択した場合，ツリーエリアと詳細エリアには，変更後の定義内容が表示されます。このため，現在リリースされている変更前の正規化ルールの定義内容が確認できません。例えば，正規化ルールの名称を「正規化ルール」から「正規化ルール - 業務プログラム B」に変更したとき，ツリーエリアには，「正規化ルール - 業務プログラム B」が表示され，元の「正規化ルール」の定義内容を表示できません。

図 4-3 正規化ルールの名称を「正規化ルール - 業務プログラム B」に変更したあとのツリーエリア

現在リリースされている変更前の正規化ルールの定義内容を確認するには，メイン画面をリリース照会モードに変更します。リリース照会モードに変更する方法については，「4.4 現在リリースされている定義内容を確認する」を参照してください。

4.3　定義を削除する

ここでは，製品情報または正規化ルールの定義を削除する方法について説明します。

4.3.1　製品情報の定義を削除する

ここでは，製品情報の定義を削除する方法について説明します。

製品情報を削除すると，その製品情報に正規化ルールが定義されていた場合，正規化ルールもすべて削除されます。

なお，操作に入る前に，次の点に注意してください。

注意事項

「Hitachi Storage」，「Windows 2008 セキュリティログ」，および「活文 NAVIstaff」の正規化ルールは，JP1/NETM/Audit の標準サポート製品として，正規化ルールエディタに初めから定義されています。標準サポート製品の製品情報は，削除しないでください。

手順を次に示します。

1. **削除する正規化ルールの定義の状態を「編集」状態に変更する。**
   削除する正規化ルールの定義の状態が「編集」状態以外の場合，「編集」状態に変更してください。

図 4-4　正規化ルールを定義した製品情報のアイコンが「編集」状態の例

正規化ルールの定義の状態を変更する方法については，「5.4　メイン画面－ツリーエリア」の，正規化ルールの定義の状態を変更する操作方法についての説明を参照してください。

2. **ツリーエリアで，削除する製品情報を選択した状態で，［編集］－［削除］－［製品情報］を選択する。**
   確認メッセージが表示されます。
3. **確認メッセージで［はい］を選択する。**

製品情報，および製品情報に定義されていた正規化ルールが削除されます。

4.3.2 正規化ルールの定義を削除する

ここでは，正規化ルールの定義を削除する方法について説明します。

操作に入る前に，次の点に注意してください。

注意事項

「Hitachi Storage」，「Windows 2008 セキュリティログ」，および「活文 NAVIstaff」の正規化ルールは，JP1/NETM/Audit の標準サポート製品として，正規化ルールエディタに初めから定義されています。標準サポート製品の正規化ルールは，削除しないでください。

手順を次に示します。

1. **削除する正規化ルールの定義の状態を「編集」状態，「リリース編集」状態，または「リリース」状態に変更する。**
   削除する正規化ルールの定義の状態が，「リリース許可」状態または「リリース解除許可」状態の場合，正規化ルールを削除できません。「編集」状態，「リリース編集」状態，または「リリース」状態に変更してください。
   正規化ルールの定義の状態を変更する方法については，「5.4　メイン画面－ツリーエリア」の，正規化ルールの定義の状態を変更する操作方法についての説明を参照してください。
2. **ツリーエリアで，削除する正規化ルールを選択した状態で，［編集］－［削除］－［製品情報］を選択する。**
   確認メッセージが表示されます。
3. **確認メッセージで［はい］を選択する。**
   正規化ルールが削除されます。
   リリースされていた正規化ルールを削除した場合，正規化ルールの定義の状態が「リリース編集」状態になります。
4. **リリースを実行する。**
   リリースを実行することで，削除した正規化ルールを，監査ログへの変換で使用できないようにします。リリースの操作については「3.2.6　正規化ルールを変換で使用できる状態にする」を参照してください。

4.4　現在リリースされている定義内容を確認する

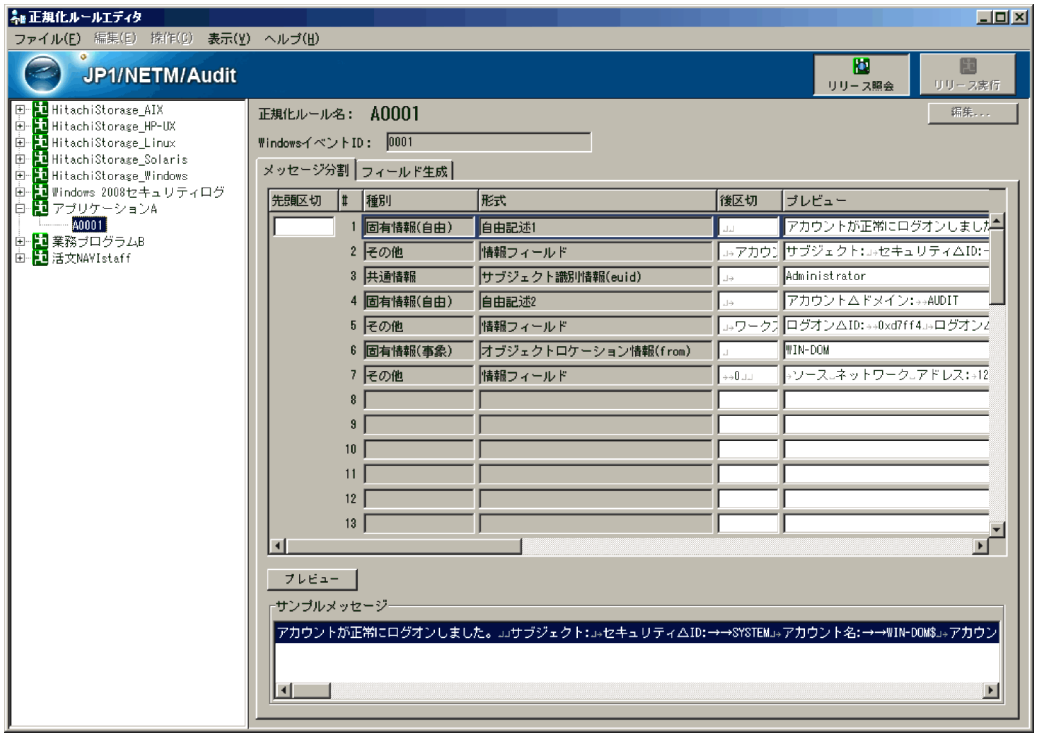
ここでは，現在リリースされている定義内容を確認する操作方法を説明します。

この操作は，現在リリースされている正規化ルールを変更し，そのリリースをあとにした場合に，現在リリースされている変更前の正規化ルールの定義内容を確認するときに実施します。

手順を次に示します。

1. **メイン画面のボタンエリアで，[リリース照会] ボタンをクリックする。**
   メイン画面がリリース照会モードになり，リリースされている定義情報が表示されます。

図 4-5　リリース照会モードのメイン画面



リリース照会モードに対して，通常のメイン画面を通常モードと呼びます。メイン画面をリリース照会モードから通常モードに戻す場合は，もう一度［リリース照会］ボタンをクリックします。

リリース照会モードでは，製品情報や正規化ルールの定義操作はできません。

4.5　標準サポート製品の定義を再作成する

標準サポート製品とは，JP1/NETM/Audit が正規化ルールを用意している製品です。

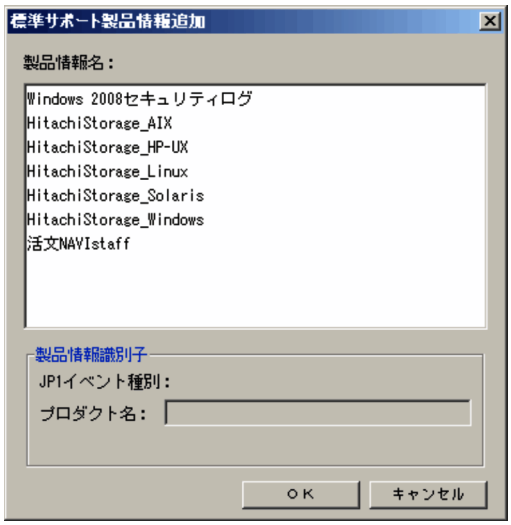
正規化ルールエディタを最初に起動したとき，すでにツリーエリアに表示されている Hitachi Storage，Windows 2008 セキュリティログ，および活文 NAVIstaff は標準サポート製品です。これらの製品情報は，データベースのセットアップ後に自動的に「リリース」状態になっています。

標準サポート製品の製品情報および正規化ルールを誤って削除したり，編集したりしてしまった場合，テンプレートから製品情報および正規化ルールを再作成できます。

誤って編集してしまった標準サポート製品の製品情報および正規化ルールを再作成する手順を次に示します。

1. **誤って編集した標準サポート製品の製品情報を削除する。**
   製品情報の削除方法については，「4.3.1　製品情報の定義を削除する」を参照してください。
2. **メイン画面で［ファイル］－［新規作成］－［標準サポート製品情報］を選択する。**
   ［標準サポート製品情報追加］ダイアログが表示されます。

図 4-6　［標準サポート製品情報追加］ダイアログ



3. **「製品情報名」から再作成したい標準サポート製品を選択する。**
4. **［OK］ボタンをクリックする。**

これで，標準サポート製品の製品情報および正規化ルールの再作成が終わりました。

このあと，リリースが必要な場合は，リリースしてください。リリースの操作については「3.2.6　正規化ルールを変換で使用できる状態にする」を参照してください。

4.6　定義を移行する

製品情報や正規化ルールの定義を別のホストに移行することができます。定義の移行には admrrexport コマンドおよび admrrimport コマンドを使用します。コマンドの詳細については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の，JP1/NETM/Audit - Manager のコマンドについて説明している個所を参照してください。

定義の移行方法には，次の二つがあります。

- すべての定義を移行する
- 特定の製品情報の定義だけを移行する

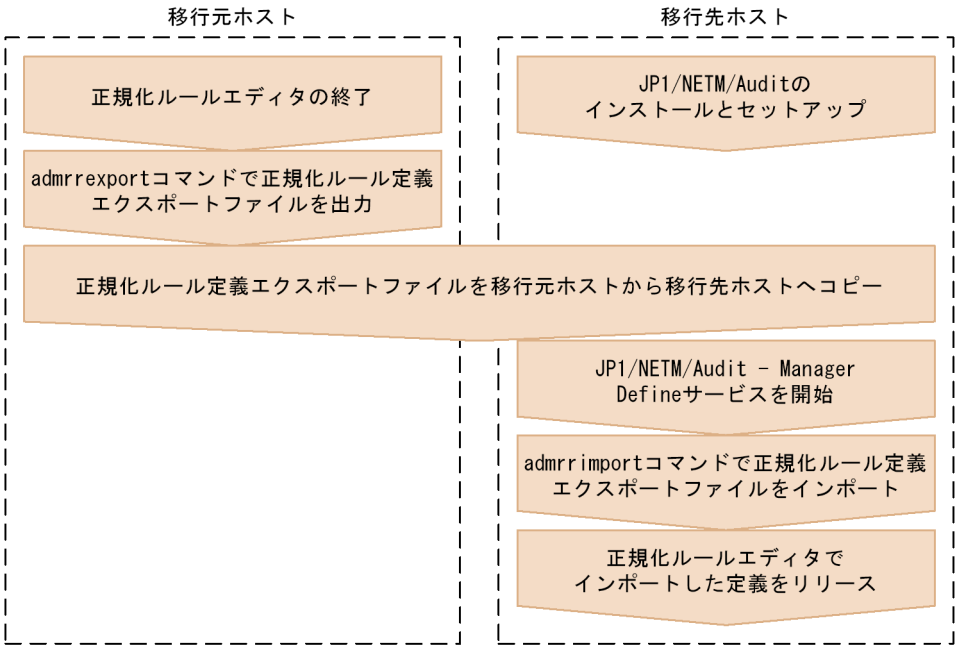
それぞれの移行方法について次に説明します。

4.6.1　すべての定義を移行する

新しいホストにすべての定義を移行する場合など，すべての定義を一括して移行できます。

すべての定義を移行する方法を次の図に示します。

図 4-7　すべての定義の移行方法



admrrexport コマンドおよび admrrimport コマンドのオプションはすべて省略した状態で実行できます。なお，移行先ホストでインポートを実行したとき，標準サポート製品の定義についてインポートしなかったことを示すメッセージ「KDSP2610-W」が出

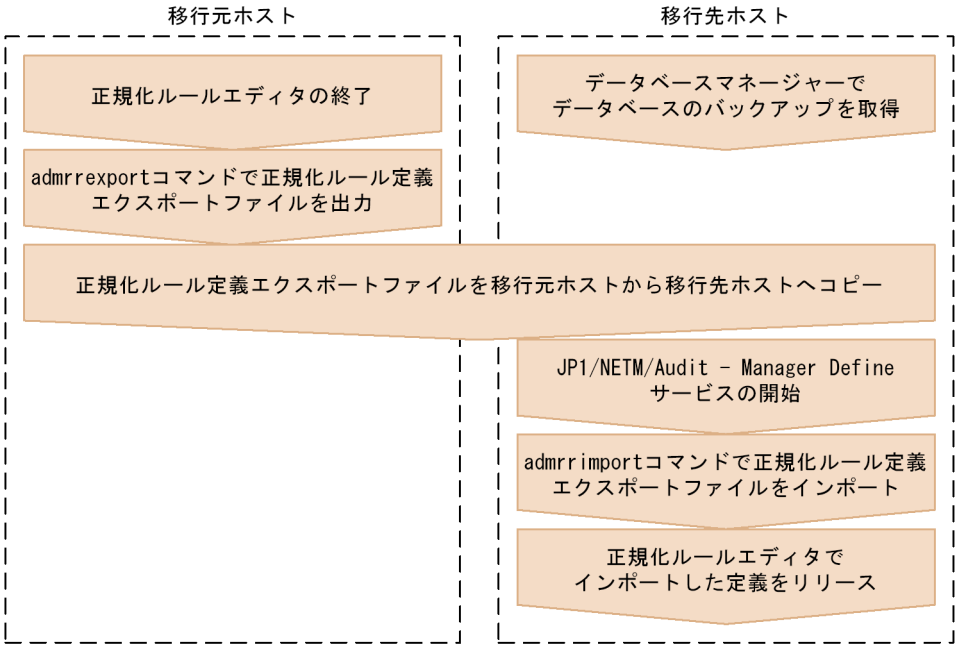
力されますが，これは無視してください。

4.6.2 特定の製品情報の定義だけを移行する

すでに稼働しているホストに製品情報の定義をマージする場合など，特定の製品情報の定義だけを移行できます。

特定の製品情報の定義だけを移行する方法を次の図に示します。

図 4-8 特定の製品情報の定義の移行方法



移行元ホストでのエクスポート時，および移行先ホストでのインポート時に指定するオプションについて次に説明します。

エクスポート時

admrrexport コマンドの -p オプションで移行対象の製品情報を指定してください。

インポート時

admrrimport コマンドの -m オプションで製品情報の定義のインポート方法を指定してください。指定できるインポート方法を次に示します。

- 製品情報を追加する場合
  admrrimport -m addproduct -i **正規化ルール定義エクスポートファイル名**
- 製品情報を置換する場合
  admrrimport -m update -i **正規化ルール定義エクスポートファイル名**

- イベントログに正規化ルールの定義を追加する場合
  `admrrimport -m addrule -i` **正規化ルール定義エクスポートファイル名**

移行先ホストで -m オプションに addrule を指定してインポートを実行したとき，すでに正規化ルールが定義されている場合は，追加する定義以外の正規化ルールをインポートしなかったことを示すメッセージ「KDSP2610-W」が出力されますが，これは無視してください。

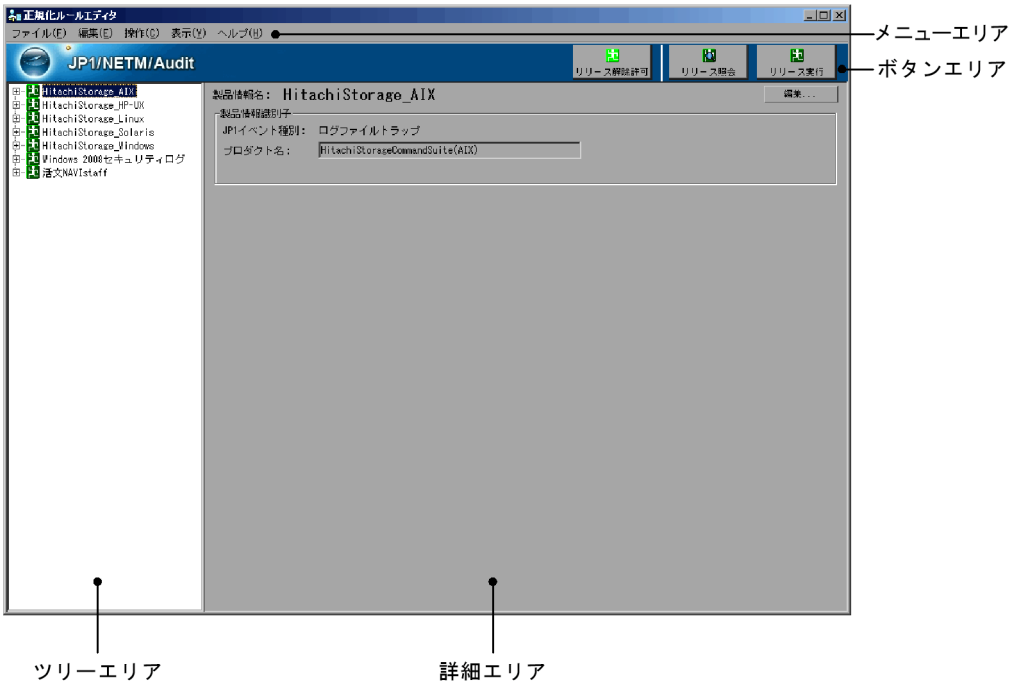
5 正規化ルールエディタの画面

この章では，正規化ルールエディタの各画面の使い方について説明します。

5.1　メイン画面の各部の名称と使い方

正規化ルールエディタを起動すると，メイン画面が表示されます。メイン画面の各部の名称は，次の図のとおりです。

図 5-1　メイン画面



次節から，メイン画面の各部の使い方を説明します。

5.2　メイン画面－メニューエリア

メニューエリアの各メニューについて説明します。

図 5-2　メイン画面のメニューエリア

(1)［ファイル］メニュー

［ファイル］メニューの各項目について説明します。

［ファイル］－［新規作成］－［製品情報］

監査ログ収集対象プログラムの製品情報を新規に追加します。
このメニューを選択すると，［製品情報定義］ダイアログが表示されます。
［製品情報定義］ダイアログの使い方については，「5.6　［製品情報定義］ダイアログ」を参照してください。

［ファイル］－［新規作成］－［正規化ルール］

正規化ルールを新規に追加します。
このメニューを選択すると，［正規化ルール定義］ダイアログが表示されます。
［正規化ルール定義］ダイアログの使い方については，「5.7　［正規化ルール定義］ダイアログ」を参照してください。
ただし，正規化ルールを追加できるのは，正規化ルールの定義の状態が，次の場合だけです。

- 「編集」状態
- 「リリース」状態
- 「リリース編集」状態

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［ファイル］－［新規作成］－［標準サポート製品情報］

標準サポート製品の正規化ルールを誤って編集したり削除したりした場合に，定義を再作成できます。
このメニューを選択すると，［標準サポート製品情報追加］ダイアログが表示されます。
［標準サポート製品情報追加］ダイアログの使い方については，「5.11　［標準サポート製品情報追加］ダイアログ」を参照してください。

［ファイル］－［終了（ログアウト）］

正規化ルールエディタを終了します。
このメニューを選択すると，終了確認メッセージが表示されたあと，正規化ルールエディタが終了します。

(2) ［編集］メニュー

［編集］メニューの各項目について説明します。

［編集］－［製品情報］

すでに定義してある製品情報の定義を編集します。
ツリーエリアで，編集する製品情報を選択した状態で，このメニューを選択すると，［製品情報定義］ダイアログが表示されます。
［製品情報定義］ダイアログの使い方については，「5.6 ［製品情報定義］ダイアログ」を参照してください。
ただし，正規化ルールが定義されている製品情報を編集しないでください。また，製品情報を編集できるのは，正規化ルールの定義の状態が，次の場合だけです。

- 「編集」状態
- 「リリース編集」状態
- 「リリース」状態

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4 メイン画面－ツリーエリア」を参照してください。

［編集］－［正規化ルール］

すでに定義してある正規化ルールの定義を編集します。
ツリーエリアで，編集する正規化ルールを選択した状態で，このメニューを選択すると，［正規化ルール定義］ダイアログが表示されます。
［正規化ルール定義］ダイアログの使い方については，「5.7 ［正規化ルール定義］ダイアログ」を参照してください。
ただし，正規化ルールを編集できるのは，正規化ルールの定義の状態が，次の場合だけです。

- 「編集」状態
- 「リリース編集」状態
- 「リリース」状態

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4 メイン画面－ツリーエリア」を参照してください。

［編集］－［削除］－［製品情報］

すでに定義してある製品情報の定義を削除します。
ツリーエリアで，削除する製品情報を選択した状態で，このメニューを選択すると，確認のメッセージが表示されます。確認のメッセージで［はい］を選択すると，製品情報が削除されます。
ただし，製品情報を削除できるのは，正規化ルールの定義が「編集」状態の場合だけです。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4 メイン画面－ツリーエリア」を参照してください。

［編集］－［削除］－［正規化ルール］

すでに定義してある正規化ルールの定義を削除します。

ツリーエリアで，削除する正規化ルールを選択した状態で，このメニューを選択すると，確認のメッセージが表示されます。確認のメッセージで［はい］を選択すると，正規化ルールが削除されます。
ただし，正規化ルールを削除できるのは，正規化ルールの定義の状態が，次の場合だけです。
- 「編集」状態
- 「リリース編集」状態
- 「リリース」状態

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

(3)［操作］メニュー

［操作］メニューの各項目について説明します。

［操作］－［リリース許可］

監査ログ収集対象プログラムの製品情報と正規化ルールの定義が終わったら，監査ログへの変換で正規化ルールを使用できるようにする（リリースする）前に，このメニューで，いったんリリースの許可をしておきます。
ただし，リリース許可ができるのは，正規化ルールの定義の状態が次の場合だけです。
- 「編集（完了）」状態
- 「リリース編集（完了）」状態

ツリーエリアで，正規化ルールの定義が「編集（完了）」状態，または「リリース編集（完了）」状態の製品情報を選択した状態で，このメニューを選択すると，確認のメッセージが表示されます。確認のメッセージで［はい］を選択すると，「リリース許可」状態になります。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［操作］－［リリース許可取消］

製品情報のリリース許可を取り消します。
ツリーエリアで，正規化ルールの定義が「リリース許可」状態の製品情報を選択した状態で，このメニューを選択すると，確認のメッセージが表示されます。確認のメッセージで［はい］を選択すると，「編集」状態になります。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［操作］－［リリース解除許可］

すでに監査ログへの変換で使用されている（リリースされている）製品情報のリリースを解除する場合に，このメニューで，いったんリリースの解除を許可しておく必要があります。
ただし，リリース解除許可ができるのは，正規化ルールの定義の状態が次の場合だけです。

- 「リリース」状態
- 「リリース編集」状態

ツリーエリアで，正規化ルールの定義が「リリース」状態または「リリース編集」状態の製品情報を選択した状態で，このメニューを選択すると，「リリース解除許可」状態になります。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［操作］－［リリース実行］

ツリーエリアの「リリース許可」状態の製品情報を，一括してリリースします。また，正規化ルールの定義が「リリース解除許可」状態の製品情報を，一括してリリース解除します。
正規化ルールの定義が「リリース許可」状態の製品情報は，「リリース」状態になります。また，正規化ルールの定義が「リリース解除許可」状態の製品情報は，「編集」状態になります。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

(4) ［表示］メニュー

［表示］メニューの各項目について説明します。

［表示］－［リリース照会］

リリースされている定義情報を確認できます。
このメニューを選択すると，詳細エリアが「リリース照会モード」になり，リリースされている定義情報だけが詳細エリアに表示されます。
リリースを解除しないで定義を変更したい場合，正規化ルールの定義を「リリース編集」状態に切り替えることで，リリースと並行して定義情報を変更できます。ただし，定義情報の変更をしたあと，変更する前の（リリース中の）定義情報を確認できません。このような場合に，編集する前の定義情報を「リリース照会モード」で確認できます。リリース編集の詳細は，「4.2.2 「リリース」状態の正規化ルールの定義を変更する」を参照してください。

［表示］－［最新の情報に更新］

ツリーエリアおよび詳細エリアに表示されている定義情報を最新の状態にします。

(5) ［ヘルプ］メニュー

［ヘルプ］メニューの各項目について説明します。

［ヘルプ］－［バージョン情報］

JP1/NETM/Audit のバージョン情報が表示されます。

5.3　メイン画面－ボタンエリア

ボタンエリアの各ボタンについて説明します。

図 5-3　メイン画面のボタンエリア

［リリース許可］ボタンが表示された時

［リリース許可取消］ボタンが表示された時

［リリース解除許可］ボタンが表示された時

［リリース許可］ボタン

監査ログ収集対象プログラムの製品情報と正規化ルールの定義が終わったら，監査ログへの変換で正規化ルールを使用できるようにする（リリースする）前に，このメニューで，いったんリリースを許可します。

ただし，リリース許可ができるのは，正規化ルールの定義の状態が次の場合だけです。

- 「編集（完了）」状態
- 「リリース編集（完了）」状態

ツリーエリアで，正規化ルールの定義が「編集（完了）」状態または「リリース編集（完了）」状態の製品情報を選択した状態で，このボタンをクリックすると，確認のメッセージが表示されます。確認のメッセージで［はい］を選択すると，「リリース許可」状態になります。

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［リリース許可取消］ボタン

正規化ルールが定義されている製品情報のリリース許可を取り消します。

ツリーエリアで，正規化ルールの定義が「リリース許可」状態の製品情報を選択した状態で，このボタンをクリックすると，確認のメッセージが表示されます。確認のメッセージで［はい］を選択すると，「編集」状態になります。

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［リリース解除許可］ボタン

すでに監査ログへの変換で使用されている（リリースされている）製品情報のリリースを解除する場合に，このメニューで，いったんリリースの解除を許可しておく必要があります。

ただし，リリース解除許可ができるのは，正規化ルールの定義の状態が次の場合だ

けです。
- 「リリース」状態
- 「リリース編集」状態

ツリーエリアで，正規化ルールの定義が「リリース」状態，または「リリース編集」状態の製品情報を選択した状態で，このボタンをクリックすると，「リリース解除許可」状態になります。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

［リリース照会］ボタン

リリースされている定義情報を確認できます。
このボタンをクリックすると，詳細エリアが「リリース照会モード」になり，リリースされている定義情報だけが詳細エリアに表示されます。
リリースを解除しないで定義を変更したい場合，正規化ルールの定義の状態を「リリース編集」状態に切り替えることで，リリースと並行して定義情報を変更できます。ただし，定義情報の変更をしたあと，変更する前の（リリース中の）定義情報を確認できません。このような場合に，編集する前の定義情報を「リリース照会モード」で確認できます。リリース編集の詳細は，「4.2.2 「リリース」状態の正規化ルールの定義を変更する」を参照してください。

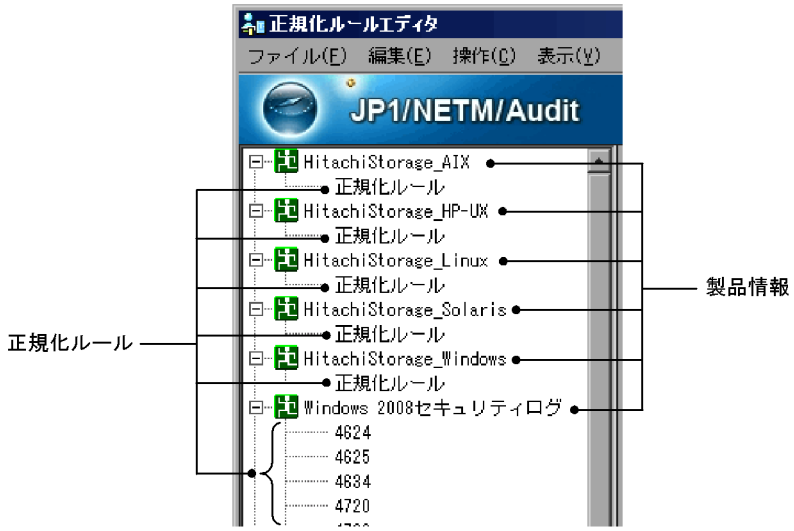
［リリース実行］ボタン

ツリーエリアの，正規化ルールの定義が「リリース許可」状態の製品情報を，一括してリリースします。また，正規化ルールの定義が「リリース解除許可」状態の製品情報を，一括してリリース解除します。
正規化ルールの定義が「リリース許可」状態の製品情報は，「リリース」状態になります。また，正規化ルールの定義の状態が「リリース解除許可」状態の製品情報は，「編集」状態になります。
正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

5.4　メイン画面－ツリーエリア

ツリーエリアの各要素について説明します。

図 5-4　画面のツリーエリア



「製品情報」

定義した製品情報の名称が表示されます。

製品情報を選択して右クリックするとメニューが表示され，その製品情報の編集，削除，正規化ルールの追加，リリース許可，リリース解除許可などの操作ができます。また，ツリーエリアの余白部分で右クリックすると，製品情報を新たに追加するメニューが表示されます。

製品情報の隣にあるアイコンは，正規化ルールの定義の状態を示します。

正規化ルールの定義の状態は，製品情報の下に定義する正規化ルールに対して，どのような操作ができるのかを表します。正規化ルールの定義の状態には，次に示す種類があります。

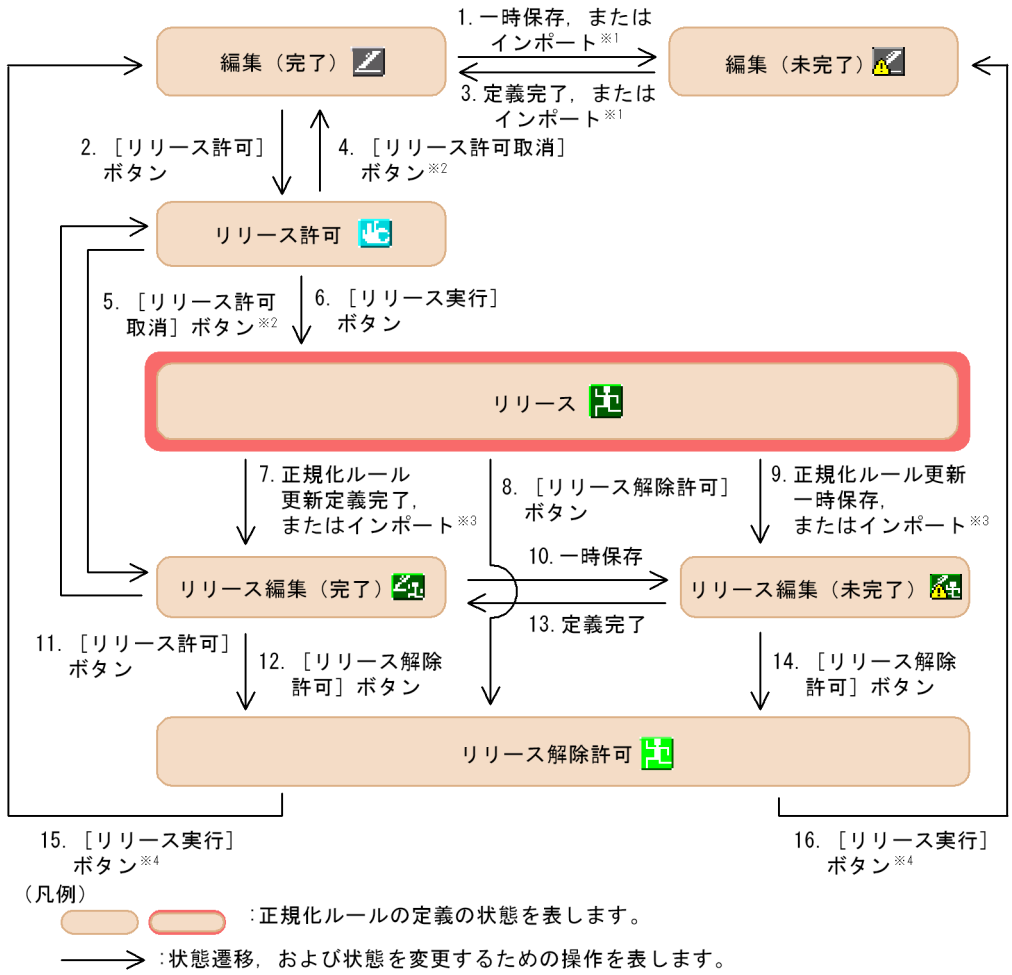
表 5-1　正規化ルールの定義の状態とアイコン

項番	正規化ルールの定義の状態		製品情報のアイコン	アイコンの意味
1	「編集」状態	完了 （正規化ルールが一つも定義されていない状態，または定義が完了している状態）		製品情報，または正規化ルールを新規に定義したり，編集したり，削除したりできる状態を意味します。
2		未完了 （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）		

項番	正規化ルールの定義の状態		製品情報のアイコン	アイコンの意味
3	「リリース許可」状態			製品情報，および正規化ルールの定義が終わって，監査ログへの変換で使用してもよい状態（「リリース」状態）にする前に，いったんリリースを許可している状態を意味します。 「リリース許可」状態の時は，製品情報および正規化ルールを新規に定義したり，編集したり，削除したりできません。
4	「リリース」状態			正規化ルールの定義が，監査ログへの変換で使用されている状態を意味します。 「リリース」状態の時は，製品情報を削除できません。
5	「リリース編集」状態	完了 （正規化ルールが一つも定義されていない状態，または定義が完了している状態）		「リリース」状態の定義情報を，リリースと並行して編集している状態を意味します。 「リリース編集」の状態の時は，製品情報を削除できません。
6		未完了 （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）		
7	「リリース解除許可」状態			リリース中の製品情報のリリースを解除する前に，いったんリリースの解除を許可している状態を意味します。 「リリース解除許可」状態の時は，製品情報および正規化ルールを作成したり，編集したり，削除したりできません。

正規化ルールに対して実施する操作に応じて，正規化ルールの定義の状態を変更する必要があります。例えば，正規化ルールの定義が完了したら，監査ログフォーマットへの変換で正規化ルールを使用するために，「編集」状態から「リリース」状態に変更する必要があります。
正規化ルールの定義の状態を変更する操作方法を次に示します。

図 5-5　正規化ルールの定義の状態を変更する操作と状態の遷移



注※ 1

「編集（未完了）」状態の定義に，定義が完了している定義をインポートすると「編集（完了）」状態になり，「編集（完了）」状態の定義に，未完了の定義をインポートすると「編集（未完了）」状態になります。

注※ 2

「リリース許可」状態になる前の状態が「編集（完了）」状態だった場合は，「編集（完了）」状態になります。

「リリース許可」状態になる前の状態が「リリース編集（完了）」状態だった場合は，「リリース編集（完了）」状態になります。

注※ 3

「リリース」状態の定義に，定義が完了している定義をインポートすると「リリース編集（完了）」状態になり，未完了の定義をインポートすると「リリース編集（未完了）」状態になります。

注※ 4

「リリース解除許可」状態になる前の状態が「リリース編集（完了）」状態だった場合は，「編集（完了）」状態になります。
「リリース解除許可」状態になる前の状態が「リリース編集（未完了）」状態だった場合は，「編集（未完了）」状態になります。

図中の各操作について，次の表で詳細を説明します。なお，表の項番は図中の番号に対応しています。

表 5-2 正規化ルールの定義の状態を変更する操作一覧

項番	変更前の状態	変更後の状態	操作の説明
1	編集（完了）	編集（未完了）	正規化ルールの定義が未完了のまま一時保存する。または，未完了の定義をインポートする。
2		リリース許可	［リリース許可］ボタン または ［操作］－［リリース許可］
3	編集（未完了）	編集（完了）	正規化ルールの定義が完了する。または，定義が完了している定義をインポートする。
4	リリース許可	編集（完了）	［リリース許可取消］ボタン または ［操作］－［リリース許可取消］
5		リリース編集（完了）	［リリース許可取消］ボタン または ［操作］－［リリース許可取消］
6		リリース	［リリース実行］ボタン または ［操作］－［リリース実行］
7	リリース	リリース編集（完了）	リリース中の正規化ルールを更新し，定義が完了する。または，定義が完了している定義をインポートする。
8		リリース解除許可	［リリース解除許可］ボタン または ［操作］－［リリース解除許可］
9		リリース編集 （未完了）	リリース中の正規化ルールを更新し，正規化ルールの定義が未完了のまま一時保存する。または，未完了の定義をインポートする。
10	リリース編集 （完了）	リリース編集 （未完了）	正規化ルールの定義が未完了のまま一時保存する。
11		リリース許可	［リリース許可］ボタン または ［操作］－［リリース許可］
12		リリース解除許可	［リリース解除許可］ボタン または ［操作］－［リリース解除許可］

項番	変更前の状態	変更後の状態	操作の説明
13	リリース編集 （未完了）	リリース編集 （完了）	正規化ルールの定義が完了する。
14		リリース解除許可	［リリース解除許可］ボタン または ［操作］－［リリース解除許可］
15	リリース解除許可	編集（完了）	［リリース実行］ または ［操作］－［リリース実行］
16		編集（未完了）	［リリース実行］ボタン または ［操作］－［リリース実行］

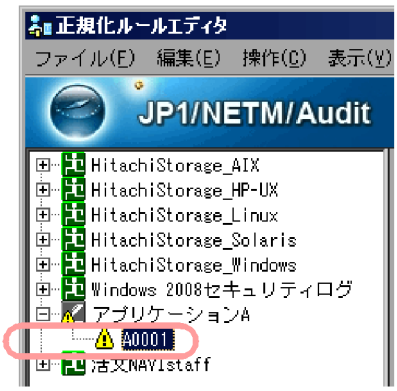
「正規化ルール」

定義した正規化ルールが，製品情報ごとに表示されます。

正規化ルールを選択して右クリックするとメニューが表示され，その正規化ルールを編集したり削除したりできます。

正規化ルールの定義を未完了で一時保存した場合，正規化ルールの隣に  が表示されます。

図 5-6　正規化ルールの隣に未完了のアイコンが表示されたツリーエリア



5.5　メイン画面－詳細エリア

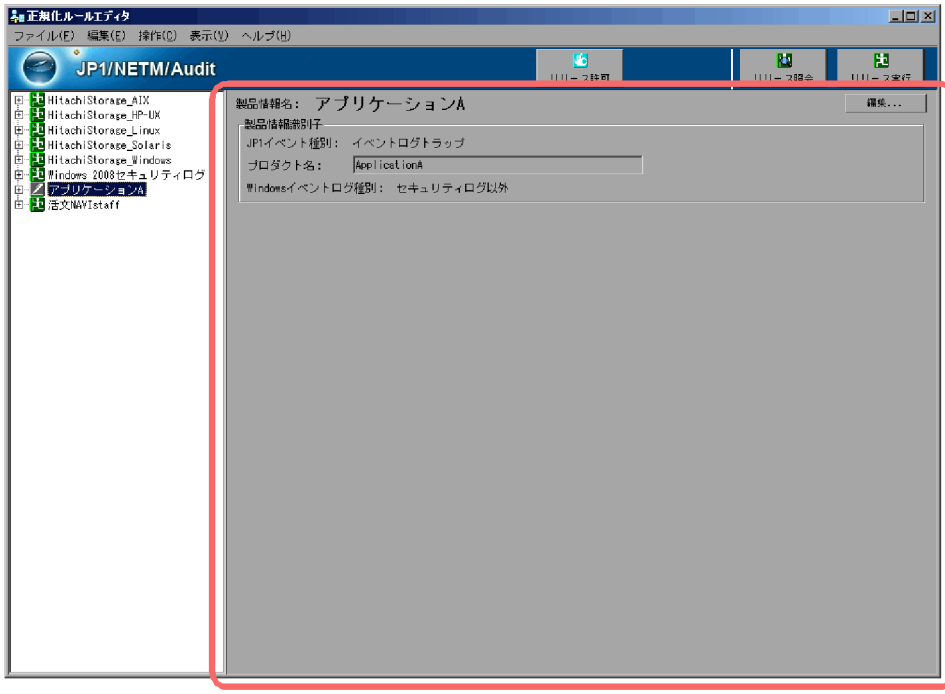
詳細エリアには，ツリーエリアで選択した製品情報や正規化ルールの定義内容が表示されます。

詳細エリアの各要素について説明します。

5.5.1　「製品情報」エリア

ツリーエリアで製品情報を選択すると，詳細エリアに，製品情報の定義内容が表示されます。

図 5-7　メイン画面の詳細エリア（ツリーエリアで製品情報を選択した場合）



「製品情報」エリアの各項目について説明します。

「製品情報名」

ツリーエリアで選択した製品情報の名称が表示されます。

［編集］ボタン

表示している製品情報の定義を編集します。

ツリーエリアで編集する製品情報を選択して，［編集］ボタンをクリックすると，［製品情報定義］ダイアログが表示されます。

［製品情報定義］ダイアログの使い方については，「5.6　［製品情報定義］ダイアログ」を参照してください。

ただし，正規化ルールが定義された製品情報を編集しないでください。また，製品情報を編集できるのは，正規化ルールの定義の状態が，次の場合だけです。

- 「編集」状態
- 「リリース編集」状態
- 「リリース」状態

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面－ツリーエリア」を参照してください。

「製品情報識別子」

監査ログへの変換では，JP1/NETM/Audit に登録されている正規化ルールのうち，どれを使用するかを決めるための情報が必要です。
製品情報識別子は，変換時に使用する正規化ルールを特定するための情報です。各項目について説明します。

「JP1 イベント種別」

ツリーエリアで選択した製品情報の JP1 イベント種別がイベントログトラップの場合に，Windows イベントログの種別が表示されます。
ツリーエリアで選択した製品情報の JP1 イベント種別がログファイルトラップの場合，この項目は表示されません。

「プロダクト名」

ツリーエリアで選択した製品情報のプロダクト名が表示されます。

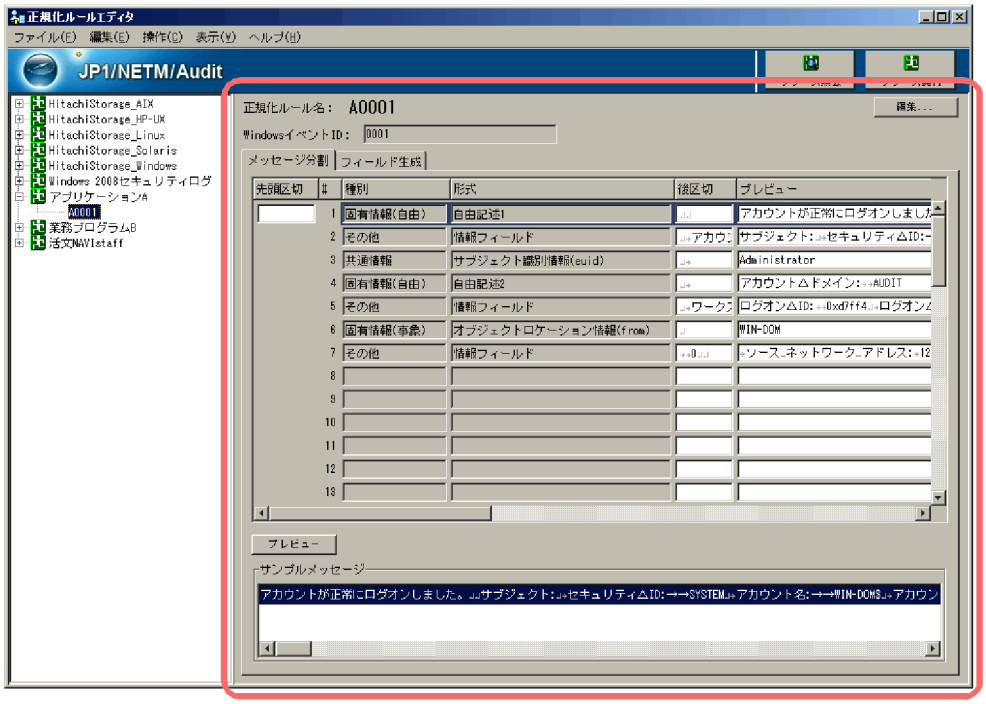
「Windows イベントログ種別」

ツリーエリアで選択した製品情報の Windows イベントログ種別が表示されます。

5.5.2 「正規化ルール」エリア

ツリーエリアで正規化ルールを選択すると，詳細エリアに，その正規化ルールの定義内容が表示されます。

図 5-8　メイン画面の詳細エリア（ツリーエリアで正規化ルールを選択した場合）



「正規化ルール」エリアの各項目について説明します。

「正規化ルール名」

ツリーエリアで選択した正規化ルールの名称が表示されます。

「Windows イベント ID」

ツリーエリアで選択した正規化ルールの Windows イベント ID が表示されます。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だけ表示されます。

［編集］ボタン

すでに定義してある正規化ルールの定義を編集します。

ツリーエリアで編集する正規化ルールを選択して，［編集］ボタンをクリックすると，［正規化ルール定義］ダイアログが表示されます。

［正規化ルール定義］ダイアログの使い方については，「5.7　［正規化ルール定義］ダイアログ」を参照してください。

ただし，正規化ルールを編集できるのは，正規化ルールの定義の状態が，次の場合だけです。

- 「編集」状態
- 「リリース編集」状態
- 「リリース」状態

正規化ルールの定義の状態と，その状態のときに表示される製品情報のアイコンについては，「5.4　メイン画面−ツリーエリア」を参照してください。

［メッセージ分割／フィールド生成］タブ

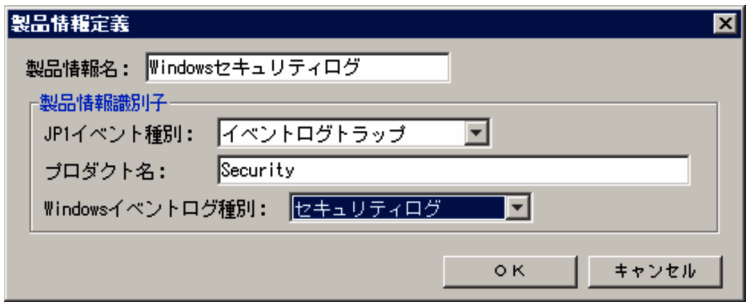
［メッセージ分割］タブには，メッセージテキストと監査ログフォーマットとの対応づけの定義が表示されます。メッセージテキストを監査ログフォーマットに対応づける操作は，［正規化ルール定義］ダイアログの［メッセージ分割］タブで実施します。［メッセージ分割］タブの各項目の詳細は，「5.7(1) ［メッセージ分割］タブ」を参照してください。

［フィールド生成］タブには，監査ログとして必要な情報がメッセージテキストにない場合に，その情報を監査ログに埋め込むための定義情報が表示されます。監査ログとして必要な情報を監査ログに埋め込む操作は，［正規化ルール定義］ダイアログの［フィールド生成］タブで実施します。［フィールド生成］タブの各項目の詳細は，「5.7(2) ［フィールド生成］タブ」を参照してください。

5.6　［製品情報定義］ダイアログ

［製品情報定義］ダイアログでは，正規化ルールを定義する監査ログ収集対象プログラムの製品情報を定義します。ここで定義した製品情報は，監査ログへの変換で使用する正規化ルールを特定するための情報になります。

図 5-9　［製品情報定義］ダイアログ



注意事項

すでに定義した製品情報を変更する場合，正規化ルールが定義されている製品情報は，変更しないでください。正規化ルールが定義されている製品情報を変更する場合は，正規化ルールをいったん削除してください。正規化ルールを削除する方法については，「4.3.2　正規化ルールの定義を削除する」を参照してください。

［製品情報定義］ダイアログの各項目について説明します。

「製品情報名」

ツリーエリアに表示される製品情報の名称を入力します。
次の文字は，製品情報の名称に使用できません。

- 0x00 ～ 0x1F，および 0x7F の制御コード
- 「-」は，製品情報名の先頭に指定できません
- 「¥」「,」「;」「:」「*」「?」「"」「<」「>」「|」「(」「)」「=」

製品情報名は，Unicode のコード順でツリーエリアに表示されます。
一度登録したら，表示順を変更できません。
ツリーエリアに表示される順序を考慮して，製品情報名を登録してください。

「製品情報識別子」

製品情報識別子は，監査ログフォーマットへの変換で使用する正規化ルールを特定するための情報です。
監査ログが収集されると，ここで定義する製品情報識別子によって，どの正規化ルールを使用して変換するか判断されます。
製品情報識別子として，「JP1 イベント種別」，「プロダクト名」，および「Windows イベントログ種別」を設定します。

「JP1 イベント種別」

監査ログ収集対象プログラムの JP1 イベントの種別を選択します。選択肢を次に示します。

- ログファイルトラップ
  ログファイルに出力されたログメッセージを収集する場合に選択します。
- イベントログトラップ
  Windows イベントログを収集する場合に選択します。

注意事項

JP1 イベント種別は，一度指定して保存すると，そのあと変更できません。変更する場合は，いったん削除してから新規に製品情報の定義を追加してください。なお，正規化ルールがすでに定義されている場合は，正規化ルールも削除する必要があります。

「プロダクト名」

「JP1 イベント種別」によって指定方法が異なります。それぞれの場合の指定方法について説明します。

「JP1 イベント種別」でログファイルトラップを選択した場合

ログファイルを出力する監査ログ収集対象プログラム名を入力します。入力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

なお，「/」は「_」に置き換えて入力してください。

また，ここに入力する内容は，次のファイルに設定する内容と一致させる必要があります。

- **製品定義ファイルのパラメーター「プログラム」の値と一致させる**
  製品定義ファイルは，正規化ルールを定義したあとに，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。
- **動作定義ファイル名「admjevlog_XXXXX.conf」の「XXXXX」と一致させる**
  動作定義ファイルは，正規化ルールを定義したあとに作成します。

製品定義ファイルおよび動作定義ファイルの作成については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の設計・構築編にある，標準サポートされていないプログラムを収集対象とするための準備について説明している個所を参照してください。

「JP1 イベント種別」でイベントログトラップを選択した場合

Windows イベントログの「ソース」と同じ内容を入力してください。ただし，0x00 ～ 0x1F および 0x7F の制御コードは入力できません。

「Windows イベントログ種別」

JP1 イベント種別で「イベントログトラップ」を指定した場合に，Windows イベントログの種別を選択します。選択肢を次に示します。

- セキュリティログ
  Windows イベントログがセキュリティログの場合に選択します。
- セキュリティログ以外
  Windows イベントログがアプリケーションログ，システムログ，またはユーザ任意のイベントログである場合に選択します。

［OK］ボタン

定義した内容が保存されます。

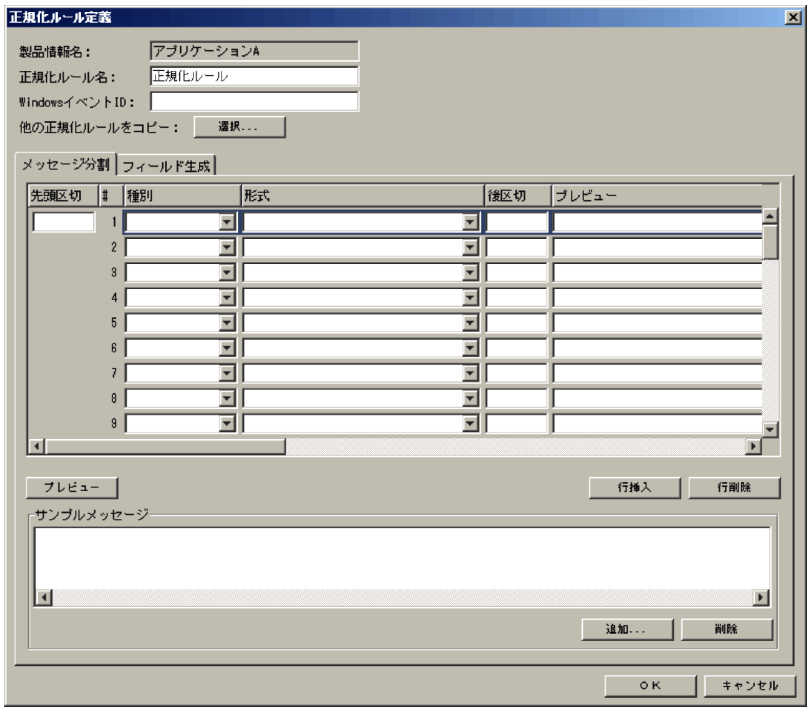
［キャンセル］ボタン

定義がキャンセルされます。

5.7 ［正規化ルール定義］ダイアログ

［正規化ルール定義］ダイアログでは，正規化ルールを定義します。

図 5-10 ［正規化ルール定義］ダイアログ



［正規化ルール定義］ダイアログの各項目について説明します。

「製品情報名」

定義する製品情報の名称が表示されます。

「正規化ルール名」

ツリーエリアに表示される正規化ルールの名称を入力します。
次の文字は，正規化ルールの名称に使用できません。

- 0x00 ～ 0x1F，および 0x7F の制御コード
- 「-」は，正規化ルール名の先頭に指定できません
- 「¥」「,」「;」「:」「*」「?」「"」「<」「>」「|」「(」「)」「=」

正規化ルール名は，Unicode のコード順でツリーエリアに表示されます。
一度登録したら，表示順を変更できません。
ツリーエリアに表示される順序を考慮して，正規化ルール名を登録してください。
すでに登録されている正規化ルール名と同じ名前の正規化ルール名では登録できません。

「Windows イベント ID」

Windows イベントログの正規化ルールを定義する場合に，Windows イベント ID を入力します。

ここで定義する Windows イベント ID は，Windows イベントログを監査ログへ変換する際に，使用する正規化ルールを特定するための情報になります。

すでに登録されている Windows イベント ID と同じ名前の Windows イベント ID では登録できません。

［選択］ボタン

ほかの正規化ルールの定義内容を流用して定義する場合にクリックします。

クリックすると，［正規化ルール選択］ダイアログが表示されます。流用する正規化ルールを選択すると，［正規化ルール定義］ダイアログに，流用する正規化ルールの定義内容が表示されます。変更したい項目だけ変更してください。［正規化ルール選択］ダイアログの詳細は，「5.8 ［正規化ルール選択］ダイアログ」を参照してください。

［メッセージ分割／フィールド生成］タブ

［メッセージ分割］タブでは，メッセージテキストを監査ログフォーマットに合わせて分割して対応づけます。また，［フィールド生成］タブでは，監査ログとして必要な情報がメッセージテキストに含まれていない場合に，その情報を監査ログに埋め込みます。

［メッセージ分割］タブの各項目については，「(1) ［メッセージ分割］タブ」を参照してください。

［フィールド生成］タブの各項目については，「(2) ［フィールド生成］タブ」を参照してください。

［OK］ボタン

定義した内容が保存されます。定義中にエラーがある場合，確認メッセージが表示されます。［はい］ボタンをクリックすると，正規化ルールを一時的に保存できます。

ただし，正規化ルール名と Windows イベント ID にエラーがある場合は保存できません。エラー部分を入力方法に従って修正してください。

［キャンセル］ボタン

定義がキャンセルされます。［キャンセル］ボタンをクリックすると，確認メッセージが表示されます。［はい］ボタンをクリックすると，定義した内容は破棄されます。

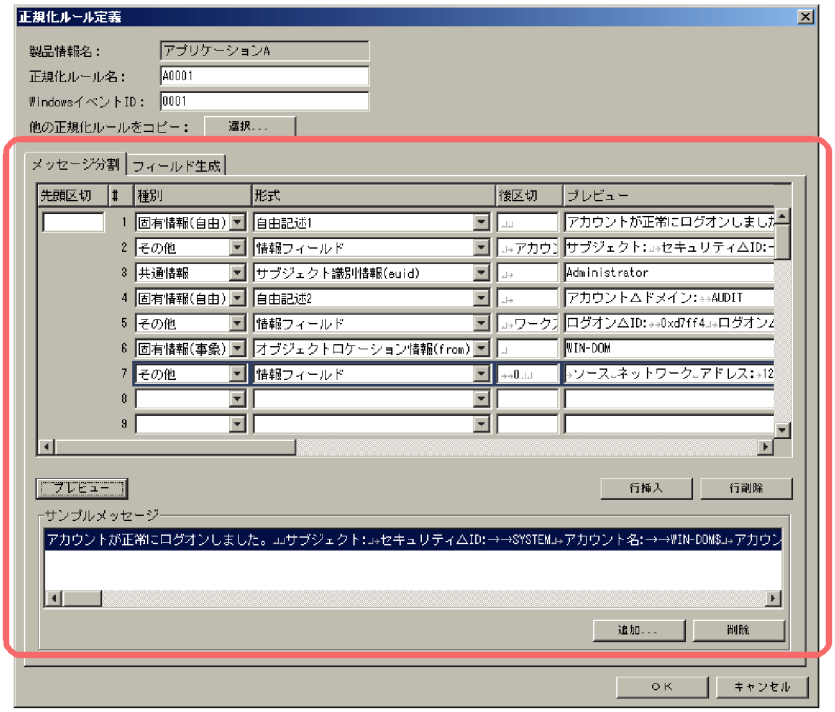
(1) ［メッセージ分割］タブ

［メッセージ分割］タブでは，メッセージテキストを監査ログフォーマットに合わせて分割し，監査ログフォーマットの要素に対応づけます。監査ログフォーマットに対応づけたメッセージテキストの要素を「フィールド」と呼びます。

メッセージは，50 件まで分割できます。

［メッセージ分割］タブの各項目について説明します。

図 5-11 ［正規化ルール定義］ダイアログの［メッセージ分割］タブ



「先頭区切」

メッセージテキストの先頭に，監査ログフォーマットとして対応づけない不要な情報がある場合に，その文字列またはバイト数を「先頭区切」として定義します。
例えば，次のメッセージテキストで「2007/12/31」以降の情報を監査ログフォーマットに対応づける場合，先頭の「#### △」は不要な情報になります。

```
####△2007/12/31△00:00:00.000△△△△KKKK0000-E△起動に失敗しました。
```

（凡例）△：半角スペースを意味します。

このような場合に，「#### △」を先頭区切として定義します。

「先頭区切」に定義する方法には，次の 2 種類あります。

- 文字列で定義する方法
- バイト単位で定義する方法

メッセージの形式に応じて，二つの方法を使い分けてください。詳細は，「3.4 メッセージテキストを分割する方法」を参照してください。
なお，「先頭区切」に定義できるのは 1 件だけです。

「#」

行の番号が表示されます。

「種別」プルダウンメニュー,「形式」プルダウンメニュー

「種別」および「形式」プルダウンメニューには，監査ログフォーマットの要素が表示されます。「プレビュー」に表示されたメッセージテキストの要素を，監査ログフォーマットのどの要素に対応づけるかを定義します。
プルダウンメニューの内容については,「(3) 「種別」および「形式」プルダウンメニューの内容」を参照してください。

「後区切」

メッセージテキストを分割するために，区切りとなる情報を入力します。
メッセージテキストを分割する方法には，次の 2 種類があります。

- 文字列で区切る方法
  メッセージテキストを分割したい位置に，半角スペースや「,」（コンマ）などの文字列がある場合は，その文字列で区切ります。
- バイト単位で区切る方法
  メッセージテキストを分割したい位置に何も文字列がない場合，バイト単位で区切ります。

メッセージの形式に応じて，二つの方法を使い分けてください。詳細は,「3.4 メッセージテキストを分割する方法」を参照してください。

「プレビュー」

「後区切」に区切り情報を指定して［プレビュー］ボタンをクリックすると,「プレビュー」に区切られたメッセージテキストの要素が表示されます。

［プレビュー］ボタン

「後区切」に指定した区切り情報に従って,「サンプルメッセージ」に表示されたメッセージテキストを分割します。分割されたメッセージテキストの要素は,「プレビュー」に表示されます。

［行挿入］ボタン

カーソルがある行の上に，新しい行を追加します。
分割位置を増やしたり変更したりする場合に使用します。行を追加すると,「プレビュー」に表示されていた内容がいったん削除されます。

［行削除］ボタン

カーソルがある行を削除します。
分割位置を減らしたり変更したりする場合に使用します。行を削除すると,「プレビュー」に表示されていた内容がいったん削除されます。

「サンプルメッセージ」リスト

メッセージテキストを分割するために，サンプルとなるメッセージテキストを登録します。登録されたサンプルが,「サンプルメッセージ」リストに表示されます。

［追加］ボタン

［追加］ボタンをクリックすると，［サンプルメッセージ追加］ダイアログが表示されます。メッセージテキストを分割するために，サンプルとなるメッセージテキストを追加してください。サンプルメッセージは，3 件まで登録できます。

［削除］ボタン

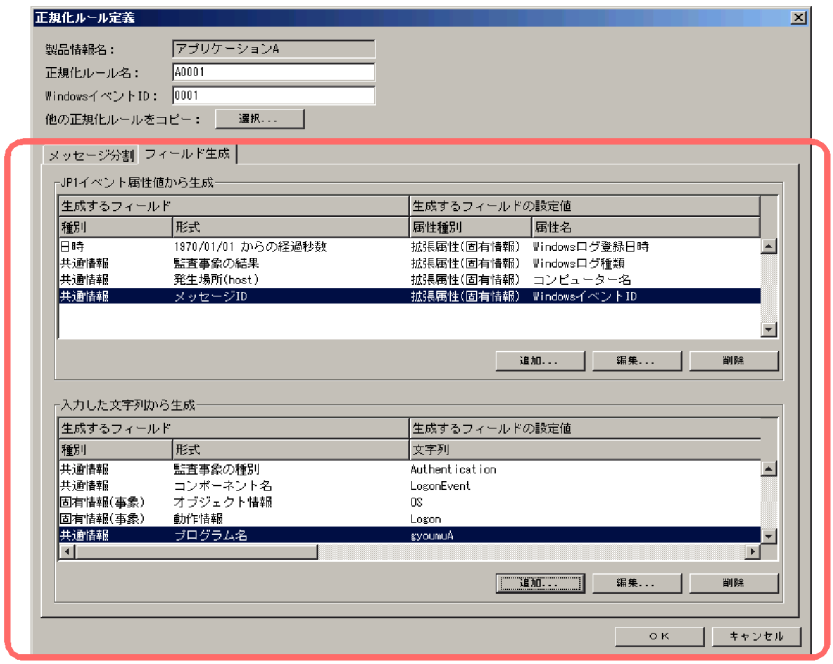
「サンプルメッセージ」リストで選択したサンプルメッセージテキストを削除します。［削除］ボタンをクリックすると，確認のメッセージが表示されます。［はい］ボタンをクリックするとサンプルメッセージテキストが破棄されます。

(2)［フィールド生成］タブ

［フィールド生成］タブでは，監査ログとして必要な情報がメッセージテキストに含まれていない場合に，その情報を変換後の監査ログに埋め込みます。監査ログに埋め込まれた各情報を「フィールド」と呼びます。

［フィールド生成］タブの各項目について説明します。

図 5-12　［正規化ルール定義］ダイアログの［フィールド生成］タブ



(a)「JP1 イベント属性値から生成」エリア

監査ログとして必要な情報がメッセージテキストにない場合でも，JP1 イベントの属性値に含まれているとき，JP1 イベントの属性値を監査ログに埋め込むことができます。「JP1 イベント属性値から生成」エリアでは，JP1 イベントの属性値を監査ログに埋め込む定義をします。JP1 イベントの属性値は，10 件まで埋め込むことができます。

「JP1 イベント属性値から生成」エリアの各項目について説明します。

「生成するフィールド」,「生成するフィールドの設定値」

定義したフィールドが一覧で表示されます。

「生成するフィールド」には，監査ログフォーマットの要素が表示されます。「生成するフィールドの設定値」には，「生成するフィールド」に対応する JP1 イベントの属性値が表示されます。

「種別」,「形式」

監査ログフォーマットの要素の種別および形式が表示されます。

「属性種別」,「属性名」

監査ログに埋め込む JP1 イベントの属性種別および属性名が表示されます。

［追加］ボタン

JP1 イベント属性値から生成するフィールドを新たに追加します。

クリックすると，［生成フィールド定義］ダイアログが表示されます。［生成フィールド定義］ダイアログの詳細は，「5.10(1)　JP1 イベントの属性値を監査ログに埋め込む場合」を参照してください。

［編集］ボタン

フィールドの定義を編集します。編集するフィールドの定義を選択して［編集］ボタンをクリックすると，［生成フィールド定義］ダイアログが表示されます。［生成フィールド定義］ダイアログの詳細は，「5.10(1)　JP1 イベントの属性値を監査ログに埋め込む場合」を参照してください。

［削除］ボタン

リストで選択したフィールドの定義を削除します。［削除］ボタンをクリックすると，確認のメッセージが表示されます。［はい］ボタンをクリックするとリストで選択したフィールドが破棄されます。

(b)「入力した文字列から生成」エリア

監査ログとして必要な情報が，メッセージテキストにも JP1 イベントの属性値にもない場合，任意の文字列を監査ログに埋め込むことができます。「入力した文字列から生成」エリアでは，任意の文字列を監査ログに埋め込む定義をします。任意の文字列は，30 件まで埋め込むことができます。

「入力した文字列から生成」エリアの各項目について説明します。

「生成するフィールド」,「生成するフィールドの設定値」

定義したフィールドが一覧で表示されます。

「生成するフィールド」には，監査ログフォーマットの要素が表示されます。「生成するフィールドの設定値」には，「生成するフィールド」に対応する入力情報が表示されます。

「種別」,「形式」

監査ログフォーマットの要素の種別および形式が表示されます。

「文字列」

監査ログに埋め込む入力情報が表示されます。

［追加］ボタン

任意の文字列から生成するフィールドを新たに追加します。
クリックすると，［生成フィールド定義］ダイアログが表示されます。［生成フィールド定義］ダイアログの詳細は，「5.10(2) 任意の文字列を監査ログに埋め込む場合」を参照してください。

［編集］ボタン

フィールドの定義を編集します。編集するフィールドの定義を選択して［編集］ボタンをクリックすると，［生成フィールド定義］ダイアログが表示されます。［生成フィールド定義］ダイアログの詳細は，「5.10(2) 任意の文字列を監査ログに埋め込む場合」を参照してください。

［削除］ボタン

リストで選択したフィールドの定義を削除します。［削除］ボタンをクリックすると，確認のメッセージが表示されます。［はい］ボタンをクリックするとリストで選択したフィールドが破棄されます。

(3)「種別」および「形式」プルダウンメニューの内容

ここでは，［正規化ルール定義］ダイアログおよび［生成フィールド定義］ダイアログの，「種別」および「形式」プルダウンメニューの項目について説明します。

表 5-3 「種別」および「形式」プルダウンメニューの項目

項番	種別	形式	必須 / 推奨 / 任意
1	日時	YYYY/MM/DD hh:mm:ss※1	◎
2		YYYY-MM-DD hh:mm:ss※1	
3		YYYY-MM-DDThh:mm:ss.sTZD※1	
4		YYYY-MM-DDThh:mm:ss.sssTZD※1	
5		1970/01/01 からの経過秒数	
6	日付※1	YYYY/MM/DD	
7		YYYY-MM-DD	
8		YY/MM/DD	
9		DD/MMM/YYYY	
10	年※1	YY	
11		YYYY	
12	月※1	MM	
13		MMM	
14	日※1	DD	
15	時刻※1	hh:mm:ss	

項番	種別	形式	必須 / 推奨 / 任意
16		hh:mm:ss.sss	
17		hh:mm:ss.ssssss	
18	時※1	hh	
19	分※1	mm	
20	秒※1	ss	
21		ss.sss	
22		ss.ssssss	
23	共通情報	通番	○
24		メッセージ ID	○
25		プログラム名	○
26		コンポーネント名	○
27		プロセス ID	○
28		発生場所（host）※2	○
29		発生場所（ipv4）※2	
30		発生場所（ipv6）※2	
31		発生場所（自動判定）※2	
32		監査事象の種別	◎
33		監査事象の結果	◎
34		サブジェクト識別情報（uid）※3	○
35		サブジェクト識別情報（euid）※3	
36		サブジェクト識別情報（pid）※3	
37		サブジェクト識別情報（自動判定）※3	
38	固有情報（事象）	オブジェクト情報	―
39		動作情報	―
40		オブジェクトロケーション情報※4	―
41		オブジェクトロケーション情報（from）※4	
42		変更前情報	―
43		変更後情報	―
44		権限情報	―
45		サービスインスタンス名	―
46		冗長化識別情報	―

項番	種別	形式	必須 / 推奨 / 任意
47	固有情報（送信）	リクエスト送信元ホスト（host）※2	－
48		リクエスト送信元ホスト（ipv4）※2	
49		リクエスト送信元ホスト（ipv6）※2	
50		リクエスト送信元ホスト（自動判定）※2	
51		リクエスト送信元ポート番号	－
52		リクエスト送信先ホスト（host）※2	－
53		リクエスト送信先ホスト（ipv4）※2	
54		リクエスト送信先ホスト（ipv6）※2	
55		リクエスト送信先ホスト（自動判定）※2	
56		リクエスト送信先ポート番号	－
57	固有情報（識別）	一括操作識別子	－
58		ログ種別情報	－
59		出力元の場所（host）※2	－
60		出力元の場所（ipv4）※2	
61		出力元の場所（ipv6）※2	
62		出力元の場所（自動判定）※2	
63		指示元の場所（host）※5	－
64		指示元の場所（ipv4）※5	
65		指示元の場所（ipv6）※5	
66		指示元の場所（fqdn）※5	
67		指示元の場所（自動判定）※5	
68		検出場所（host）※2	－
69		検出場所（ipv4）※2	
70		検出場所（ipv6）※2	
71		検出場所（自動判定）※2	
72		ロケーション識別情報	－
73		エージェント情報（host）※2	－
74		エージェント情報（ipv4）※2	
75		エージェント情報（ipv6）※2	
76		エージェント情報（自動判定）※2	

項番	種別	形式	必須 / 推奨 / 任意
77	固有情報（自由）	自由記述 1 ～ 30	－
78	その他※ 1	情報フィールド	－

（凡例）

◎：必ず対応づけます。

○：対応づけを推奨します。

－：必要に応じて対応づけます。

注※ 1

［生成フィールド定義］ダイアログの「種別」または「形式」プルダウンメニューには表示されません。

注※ 2

メッセージテキストまたは JP1 イベント属性値に出力される情報が，確実にホスト名の場合は（host）を，IPv4 アドレスの場合は（ipv4）を，IPv6 アドレスの場合は（ipv6）を選択してください。

どの形式で出力されるかわからない場合は，（自動判定）を選択してください。

注※ 3

メッセージテキストまたは JP1 イベント属性値に出力される情報が，確実に uid の場合は（uid）を，euid の場合は（euid）を，pid の場合は（pid）を選択してください。

どの形式で出力されるかわからない場合は，（自動判定）を選択してください。

注※ 4

Windows イベントログのセキュリティログの正規化ルールを定義する場合，オブジェクトロケーション情報に当たる情報は，「オブジェクトロケーション情報（from）」に対応づけてください。Windows イベントログのセキュリティログ以外の正規化ルールを定義する場合は，「オブジェクトロケーション情報」に対応づけてください。

注※ 5

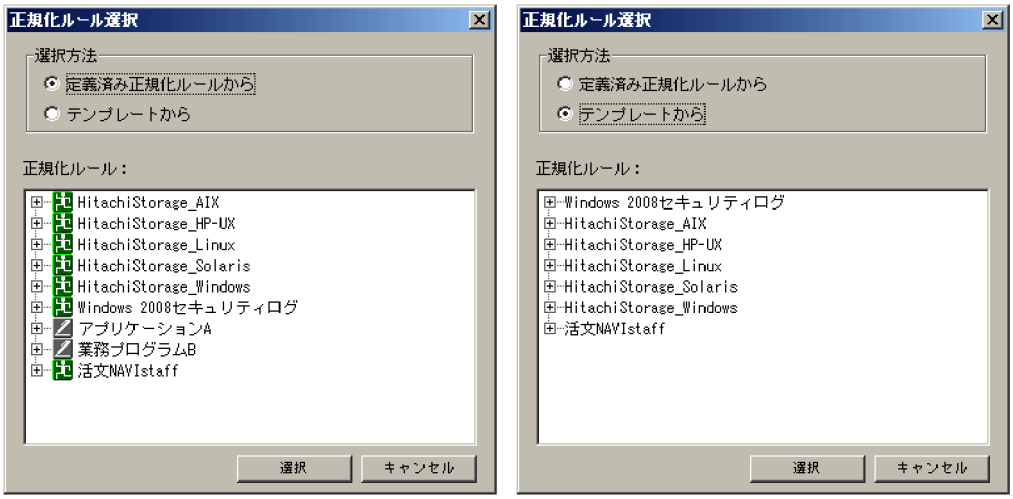
メッセージテキストまたは JP1 イベント属性値に出力される情報が，確実にホスト名の場合は（host）を，IPv4 アドレスの場合は（ipv4）を，IPv6 アドレスの場合は（ipv6）を，完全修飾ドメイン名の場合は（fqdn）を選択してください。

どの形式で出力されるかわからない場合は，（自動判定）を選択してください。

5.8 ［正規化ルール選択］ダイアログ

［正規化ルール選択］ダイアログでは，正規化ルールの定義で，ほかの正規化ルールの定義内容を流用する場合に，流用する正規化ルールを選択します。

図 5-13 ［正規化ルール選択］ダイアログ



［正規化ルール選択］ダイアログの各項目について説明します。

「選択方法」

流用する正規化ルールを次のどちらかから選択します。

［定義済み正規化ルールから］

これまでに追加，編集した正規化ルールを流用する場合に選択します。

［テンプレートから］

標準サポート製品の正規化ルールを流用する場合に選択します。

標準サポート製品の製品情報および正規化ルールを再作成する場合は，「4.5 標準サポート製品の定義を再作成する」を参照してください。

「正規化ルール」

定義された製品情報と正規化ルールの一覧が表示されます。流用する正規化ルールを選択してください。

［選択］ボタン

「製品情報および正規化ルール一覧」で選択した正規化ルールの定義内容が，［正規化ルール定義］ダイアログに反映されます。

［キャンセル］ボタン

正規化ルールの選択をキャンセルします。

5.9 ［サンプルメッセージ追加］ダイアログ

［サンプルメッセージ追加］ダイアログでは，正規化ルールの定義でメッセージテキストを分割するために，サンプルとなるメッセージテキストを追加します。サンプルメッセージは，一つの正規化ルールにつき，3 件まで登録できます。

図 5-14 ［サンプルメッセージ追加］ダイアログ

［サンプルメッセージ追加］ダイアログの各項目について説明します。

「サンプルメッセージ」

正規化ルールを定義する監査ログ収集対象プログラムのメッセージテキストを入力します。ここに入力したメッセージテキストを基に，正規化ルールを定義します。

［OK］ボタン

入力したメッセージテキストが，［正規化ルール定義］ダイアログの「サンプルメッセージ」リストに表示されます。

［キャンセル］ボタン

サンプルメッセージの追加をキャンセルします。

5.10　［生成フィールド定義］ダイアログ

［生成フィールド定義］ダイアログでは，次のどちらかの方法で，メッセージテキストにない情報を監査ログに埋め込みます。

- JP1 イベントの属性値を監査ログに埋め込む
- 任意の文字列を監査ログに埋め込む

方法ごとにダイアログの内容が異なります。

それぞれのダイアログの項目について説明します。

（1）JP1 イベントの属性値を監査ログに埋め込む場合

図 5-15　［生成フィールド定義］ダイアログ（JP1 イベントの属性値を監査ログに埋め込む場合）

各項目について説明します。

「生成するフィールド」

埋め込む情報が，監査ログフォーマットのどの要素に当たるかを選択します。

「種別」

埋め込む情報に対応する監査ログフォーマットの要素の種別を選択してください。

監査ログフォーマットの要素の種別については，「5.7(3)　「種別」および「形式」プルダウンメニューの内容」を参照してください。

「形式」

埋め込む情報に対応する監査ログフォーマットの要素の形式を選択してください。

監査ログフォーマットの要素の形式については，「5.7(3)　「種別」および「形式」プルダウンメニューの内容」を参照してください。

「生成するフィールドの設定値」

JP1 イベント属性値のうち，どの情報を監査ログに埋め込むかを選択します。

「属性種別」

埋め込む情報に対応する JP1 イベントの属性種別を選択します。

「属性名」

埋め込む情報に対応する JP1 イベントの属性名を選択します。

「属性種別」と「属性名」の選択肢については，「1.4.1　JP1 イベント属性値との対応づけを検討する」を参照してください。

［OK］ボタン

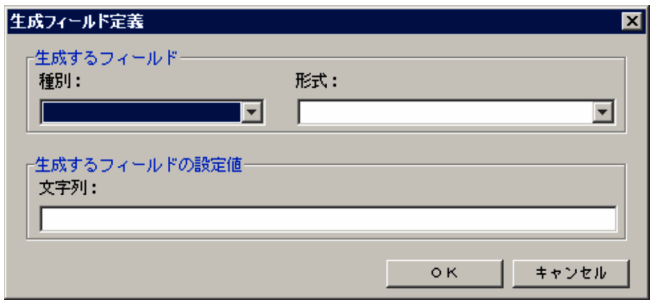
定義した内容が，［正規化ルール定義］ダイアログの［フィールド生成］タブに表示されます。

［キャンセル］ボタン

定義をキャンセルします。

(2) 任意の文字列を監査ログに埋め込む場合

図 5-16　［生成フィールド定義］ダイアログ（任意の文字列を監査ログに埋め込む場合）



各項目について説明します。

「生成するフィールド」

埋め込む情報が，監査ログフォーマットのどの要素に当たるかを選択します。

「種別」

埋め込む情報に対応する監査ログフォーマットの要素の種別を選択してください。

監査ログフォーマットの要素の種別については，「5.7(3)　「種別」および「形式」プルダウンメニューの内容」を参照してください。

「形式」

埋め込む情報に対応する監査ログフォーマットの要素の形式を選択してください。

監査ログフォーマットの要素の形式については，「5.7(3)　「種別」および「形式」プルダウンメニューの内容」を参照してください。

ただし，日付情報の種別と形式は，表示されません。

「生成するフィールドの設定値」

監査ログに埋め込む情報を定義します。

「文字列」

監査ログに埋め込む情報を入力します。監査ログフォーマットの各要素に埋められる文字列には規則があります。規則については,「1.4.2　文字列の埋め込みを検討する」を参照してください。

［OK］ボタン

定義した内容が,［正規化ルール定義］ダイアログの［フィールド生成］タブに表示されます。

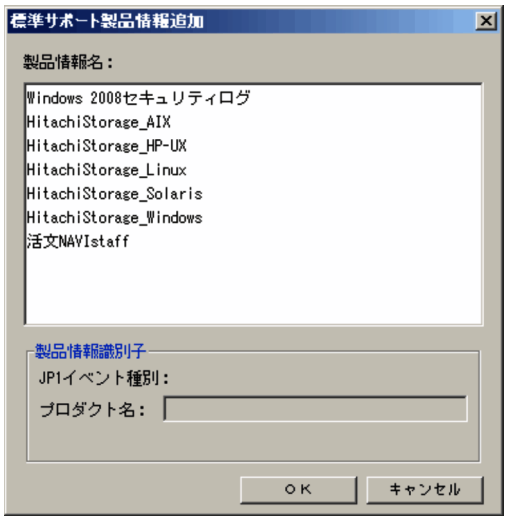
［キャンセル］ボタン

定義をキャンセルします。

5.11 ［標準サポート製品情報追加］ダイアログ

［標準サポート製品情報追加］ダイアログでは，標準サポート製品の製品情報および正規化ルールを誤って編集したり削除したりした場合に，削除した製品情報および正規化ルールの定義を再作成できます。

図 5-17 ［標準サポート製品情報追加］ダイアログ



注意事項

誤って編集した製品情報や正規化ルールの定義が残っていると，再作成できません。再作成するには，対象の製品情報，およびその製品情報に定義されている正規化ルールをすべて削除してください。

［標準サポート製品情報追加］ダイアログの各項目について説明します。

「製品情報名」

標準サポート製品の製品情報名が表示されます。再作成する標準サポート製品を選択してください。

「製品情報識別子」

「製品情報名」で標準サポート製品を選択すると，その製品情報の定義内容が表示されます。

［OK］ボタン

「製品情報名」で選択した標準サポート製品の製品情報，およびその製品情報に定義された正規化ルール定義が再作成されます。

［キャンセル］ボタン

再作成をキャンセルします。

6 メッセージ

この章では，正規化ルールエディタが出力するメッセージについて説明します。

6.1 メッセージの形式

この節では，正規化ルールエディタ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。

6.1.1 メッセージの出力形式

正規化ルールエディタが出力するメッセージの形式を次に示します。

```
KDSQnnnn-m メッセージテキスト
```

- KDSQ：メッセージを出力したプログラムが正規化ルールエディタであることを示す識別子です。
- 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：通知，Q：応答要求）です。
- **メッセージテキスト**：メッセージの内容です。

6.1.2 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

（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。

6.2 メッセージの出力先

正規化ルールエディタのメッセージは，すべてメッセージダイアログに出力されます。メッセージダイアログにメッセージが出力されたら，「6.3 メッセージ一覧」で，該当するメッセージの対処方法を参照してください。

6.3 メッセージ一覧

正規化ルールエディタが出力するメッセージの一覧を次に示します。

KDSQ4020-I

リリースまたはリリース解除処理が完了しました。

リリース処理が完了したことを通知するメッセージです。

(S)

画面を最新の情報に更新します。

(O)

リリース処理の結果を確認してください。

KDSQ4070-Q

***定義情報*のリリース処理を実行してもよろしいですか？**

*定義情報*が「リリース」状態で*定義情報*の名前を変更した場合，*定義情報*のリリース実行をするかどうかを確認します。

(S)

応答を待ちます。

(O)

*定義情報*のリリース処理を実行する場合は［はい］を，あとでリリース処理を実行する場合は［後でリリースする］を，名前の変更を中断する場合は［キャンセル］をクリックしてください。

［後でリリースする］を選択した場合，*定義情報*のリリース処理を実行するまでの間，正規化ルールエディタの通常モードでは変更後の名前で出力されますが，リリース照会モード，および JP1/NETM/Audit - Manager Convert サービスが出力するメッセージには，変更前の名前で出力されます。

KDSQ4071-Q

他の定義項目にも変更があります。*定義情報*のリリース処理を実行してもよろしいですか？

*定義情報*が「リリース」または「リリース編集」状態で，*定義情報*の名前の変更および，ほかの定義項目に変更がある場合，*定義情報*のリリース実行をするかどうかを確認します。

(S)

応答を待ちます。

(O)

*定義情報*のリリース処理を実行する場合は［はい］を，あとでリリース処理を実行する場合は［後でリリースする］を，名前の変更を中断する場合は［キャンセル］をクリックしてください。

［後でリリースする］を選択した場合，*定義情報*のリリース処理を実行するまでの

間，正規化ルールエディタの通常モードでは変更後の名前で出力されますが，リリース照会モード，および JP1/NETM/Audit - Manager Convert サービスが出力するメッセージには，変更前の名前で出力されます。

KDSQ4080-Q

正規化ルールエディタを終了します。よろしいですか？

正規化ルールエディタを終了するか確認します。

（S）

応答を待ちます。

（O）

正規化ルールエディタを終了する場合は［はい］を，取り消す場合は［いいえ］をクリックしてください。

KDSQ4081-Q

選択された*定義情報*を削除します。よろしいですか？

選択された*定義情報*を削除するか確認します。

（S）

応答を待ちます。

（O）

*定義情報*を削除する場合は［はい］を，取り消す場合は［いいえ］をクリックしてください。

KDSQ4085-Q

選択された*定義情報*をリリース解除許可します。よろしいですか？

選択された*定義情報*をリリース解除許可するか確認します。

（S）

応答を待ちます。

（O）

選択された*定義情報*をリリース解除許可する場合は［はい］を，取り消す場合は［いいえ］をクリックしてください。

KDSQ4086-Q

リリースまたはリリース解除処理を実行します。この処理には時間がかかることがあります。よろしいですか？

リリースまたはリリース解除処理を実行するか確認します。
この処理の実行時間は，リリースまたはリリース解除をする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またはリリース解除をすると数十分かかることがあります。

（S）

応答を待ちます。

(O)

リリースまたはリリース解除をする場合は［はい］を，取り消す場合は［いいえ］をクリックしてください。

KDSQ4090-Q

***定義情報*の編集内容を破棄します。よろしいですか？**

*定義情報*の編集内容を破棄して，［正規化ルール定義］ダイアログを閉じるか確認します。

(S)

応答を待ちます。

(O)

編集内容を破棄して，［正規化ルール定義］ダイアログを閉じる場合は［はい］を，取り消す場合は［いいえ］をクリックしてください。

KDSQ4108-W

接続先ポート番号の取得に失敗しました。［原因コード：*原因コード*］デフォルト値（*ポート番号*）を使用して動作します。

ポート番号を services ファイルから取得できませんでした。

(S)

デフォルトのポート番号を使用して処理を継続します。

(O)

サービス名 :auditd_monsrv に対応するポート番号が，services ファイルに設定されているかどうか確認してください。設定されていない場合は，設定したあとで再実行してください)。

KDSQ4109-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（*ポート番号*）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（5000 以内）です。このため，デフォルト値（*ポート番号*）を使用して処理を続行します。

(S)

デフォルトのポート番号を使用して処理を継続します。

(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。

KDSQ4201-E

***項目名*(必須) を指定してください。**

*項目名*が指定されていません。

(S)

処理を中止します。

(O)

*項目名*は，必須項目のため省略できません。項目を指定してください。

KDSQ4202-E

***項目名*を選択してください。**

*項目名*が選択されていません。

(S)

処理を中止します。

(O)

*項目名*を選択してください。

KDSQ4203-E

既に同じ名前の*定義情報*が存在します。別の名前を指定してください。

すでに同じ名前の*定義情報*があります。

(S)

処理を中止します。

(O)

すでにある*定義情報*と同じ名前は指定できません。別の名前を指定したあと，再実行してください。

KDSQ4204-E

***項目名*を追加してください。**

*項目名*が存在しません。

(S)

処理を中止します。

(O)

*項目名*を追加してください。

KDSQ4205-E

***項目名*に指定できない文字が入力されています。**

*項目名*に指定できない文字が入力されています。

(S)

処理を中止します。

(O)

指定できない文字を使わないで*項目名*を再入力してください。

KDSQ4221-E

ツリーエリアから 1 件選択してください。

ツリーエリアで項目が選択されていません。

(S)

処理を中止します。

(O)

ツリーエリアから 1 件選択して，再実行してください。

KDSQ4240-E

先頭区切のカラム位置指定に誤りがあります。1 ～ 1023 の範囲で指定してください。

「先頭区切」に指定しているバイト数に誤りがあります。

(S)

処理を中止します。

(O)

「先頭区切」に指定できるバイト数を 1 ～ 1023 の範囲で指定したあと，再実行してください。

KDSQ4241-E

***位置*件目の後区切を指定してください。**

*位置*件目の「後区切」が指定されていません。

(S)

処理を中止します。

(O)

*位置*件目の「後区切」を指定したあと，再実行してください。

KDSQ4242-E

***位置*件目の後区切のカラム位置指定に誤りがあります。1 ～ 1023 の範囲で指定してください。**

*位置*件目の「後区切」に指定しているバイト数に誤りがあります。

(S)

処理を中止します。

(O)

*位置*で指定された位置の「後区切」に指定したバイト数を，1 ～ 1023 の範囲で指定したあと，再実行してください。

KDSQ4243-E

フィールドおよび後区切はメッセージの先頭から間隔を空けずに指定してください。

フィールドおよび「後区切」が，メッセージの先頭から間隔を空けて指定されています。

(S)

処理を中止します。

(O)

フィールドおよび「後区切」を，メッセージの先頭から間隔を空けないように指定したあと，再実行してください。

KDSQ4244-E

***日付情報*の情報を持つ日付情報フィールドの指定が重複しています。**

日付の情報が重複して指定されています。

(S)

処理を中止します。

(O)

日付の情報は重複しないように設定してください。
例えば，「日付」種別と「月」種別を対応づけた場合，日付は月の情報を含むのでエラーとなります。

KDSQ4245-E

***定義情報*の種別：*種別名*，形式：*形式名*のフィールドと，*定義情報*の種別：*種別名*，形式：*形式名*のフィールドは同時に指定できません。**

フィールドの種別，形式の組み合わせで，同時に指定できない組み合わせを定義しています。

(S)

処理を中止します。

(O)

同時に指定できない組み合わせのフィールド定義を変更，または削除したあと，再実行してください。

KDSQ4247-E

***件数*件目のフィールドの種別と形式を指定してください。**

*件数*件目のフィールドの種別と形式が指定されていません。

(S)

処理を中止します。

(O)

フィールドの長さを指定したフィールドがある場合，「種別」と「形式」を指定したあと，再実行してください。

KDSQ4253-Q

_日付情報_の情報を持つ日付フィールドが指定されていないため，このままではリリースできません。

_定義情報_を保存してよろしいですか？

種別に_日付情報_を持つフィールドが指定されていません。

(S)

応答を待ちます。

(O)

_定義情報_を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4254-Q

種別：_種別名_，形式：_形式名_のフィールドが指定されていないため，このままではリリースできません。

_定義情報_を保存してよろしいですか？

種別に_種別名_，形式に_形式名_を持つフィールドが指定されていません。

(S)

応答を待ちます。

(O)

_定義情報_を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4256-E

これ以上フィールド行を挿入できません。

最終行の「種別」，「形式」，「後区切」のどれかのフィールドにデータが入っています。

(S)

処理を中止します。

(O)

不要なフィールド行があれば，削除して再実行してください。
不要なフィールド行がない場合，定義を見直して，最大行数に収まるように再定義してください。

KDSQ4260-Q

先頭区切のカラム位置が 1 ～ 1023 の範囲で指定されていないため，このままではリリースできません。

_定義情報_を保存してよろしいですか？

「先頭区切」に指定しているバイト数が，1 ～ 1023 の範囲で指定されていません。

(S)

応答を待ちます。

(O)

*定義情報*を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4261-Q

***位置*件目の後区切が指定されていないため，このままではリリースできません。**

***定義情報*を保存してよろしいですか？**

*位置*件目の「後区切」が指定されていません。

(S)

応答を待ちます。

(O)

*定義情報*を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4262-Q

***位置*件目のカラム位置が 1 ～ 1023 の範囲で指定されていないため，このままではリリースできません。**

***定義情報*を保存してよろしいですか？**

*位置*件目の「後区切」に指定しているバイト数が，1 ～ 1023 の範囲で指定されていません。

(S)

応答を待ちます。

(O)

*定義情報*を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4263-Q

フィールドおよび後区切がメッセージの先頭から間隔を空けて指定されているため，このままではリリースできません。

***定義情報*を保存してよろしいですか？**

フィールドおよび「後区切」が，メッセージの先頭から間隔を空けて指定されています。

(S)

応答を待ちます。

(O)

*定義情報*を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4264-Q

_日付情報_の情報を持つ日付情報フィールドの指定が重複しているため，このままではリリースできません。

_定義情報_を保存してよろしいですか？

日付の情報が重複して指定されています。例えば，「日付」種別と「月」種別を対応づけた場合，日付は月の情報を含むので，エラーとなります。

(S)

応答を待ちます。

(O)

_定義情報_を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4265-Q

_定義情報_の種別：_種別名_，形式：_形式名_のフィールドと，_定義情報_の種別：_種別名_，形式：_形式名_のフィールドが同時に指定されているため，このままではリリースできません。

_定義情報_を保存してよろしいですか？

フィールドの種別と形式の組み合わせで，同時に指定できない組み合わせを定義しています。

(S)

処理を中止します。

(O)

_定義情報_を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4267-Q

_件数_件目のフィールドの種別と形式が指定されていないため，このままではリリースできません。

_定義情報_を保存してよろしいですか？

_件数_件目のフィールドの種別と形式が指定されていません。

(S)

処理を中止します。

(O)

_定義情報_を保存する場合は［はい］を，編集を続ける場合は［いいえ］をクリックしてください。

KDSQ4270-E

選択した種別・形式のフィールドの設定値は_最小バイト数_バイト以上_最大バイト数_バイト以下で指定してください。

フィールドに設定した文字列のバイト長が誤っています。

（S）

処理を中止します。

（O）

文字列を*最小バイト数*バイト以上*最大バイト数*バイト以下で指定してから，再実行してください。

KDSQ4271-E

選択した種別・形式のフィールドの設定値に指定できない文字列です。

指定した文字列に誤りがあります。

（S）

処理を中止します。

（O）

生成するフィールドの設定値に指定した文字列に誤りがないか確認し，再実行してください。

生成するフィールドの設定値に指定できる文字列については，「1.4.2　文字列の埋め込みを検討する」を参照してください。

KDSQ4500-E

件数が上限値に達しているため*定義情報*を*処理名*することはできません。

件数が上限値に達しています。

（S）

処理を中止します。

（O）

*定義情報*を削除したあと，再実行します。

KDSQ4511-E

JP1/NETM/Audit - Manager Define **サービスから受信した定義情報が不正です。[詳細情報：*詳細情報 1*, *詳細情報 2*]**

JP1/NETM/Audit - Manager Define サービスから不正な定義情報を受信しました。

（S）

処理を中止します。

（O）

ダイアログの操作中にこのメッセージが表示された場合は，正規化ルールエディタを再起動してください。

繰り返し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。

KDSQ4543-E

正規化ルールが 1 件も定義されていないため，製品情報をリリース許可することができません。

選択された製品情報に正規化ルールが定義されていません。

(S)

処理を中止します。

(O)

選択された製品情報の正規化ルールを定義したあと，再実行してください。

KDSQ4583-E

メッセージ分割定義で指定した区切り文字が，サンプルメッセージ中に存在しないため，プレビューを完了することができません。

メッセージ分割定義で指定した区切り文字とサンプルメッセージ中の区切り文字が異なるためプレビューが完了できません。

(S)

不正な区切り文字が指定された行以降のプレビューを表示しません。

(O)

メッセージ分割定義の区切り文字とサンプルメッセージの区切り文字を確認し，メッセージ分割定義の区切り文字を変更したあと，再実行してください。

KDSQ4584-E

メッセージ分割定義で指定したカラム位置がマルチバイト文字を分断する位置であるか，またはサンプルメッセージの長さを超えているため，プレビューを完了することができません。

メッセージ分割定義で指定したバイト数がマルチバイト文字を分断する位置であるか，またはサンプルメッセージの長さを超えています。

(S)

不正なバイト数が指定された行以降のプレビューを表示しません。

(O)

メッセージ分割定義のバイト数をサンプルメッセージのフィールドのバイト数に合うように変更したあと，再実行してください。

KDSQ4585-E

メッセージ分割定義で指定したフィールドの日付の定義が誤っているか，サンプルメッセージ中の日付形式と異なるため，プレビューを完了することができません。

メッセージ分割定義で指定したフィールドの日付の定義が誤っているか，サンプルメッセージ中の日付形式と異なっています。

(S)

日付を指定した行よりあとのプレビューを表示しません。

(O)

メッセージ分割定義のフィールドの日付形式を確認し，サンプルメッセージの日付形式に合うように変更したあと，再実行してください。

KDSQ4588-E

メッセージ分割定義で指定した種別：*種別名*，形式：*形式名* フィールドの値に誤りがあるため，プレビューを完了することができません。

メッセージ分割で，「監査事象の種別」または「監査事象の結果」に対応づけた値が不正です。

(S)

「監査事象の種別」または「監査事象の結果」を指定した行よりあとのプレビューを表示しません。

(O)

正規化ルールのメッセージ分割で，「監査事象の種別」または「監査事象の結果」に対応づけた値を確認してください。

「監査事象の種別」に対応づけられる値については，「1.3.1(1)(b)　監査ログの収集カテゴリ」を参照してください。

「監査事象の結果」に対応づけられる値については，「1.3.1(1)(c)　監査ログの結果」を参照してください。

KDSQ4613-E

既に同じ製品情報が存在します。別の製品情報識別子を持つ製品情報を指定してください。[詳細情報：*詳細情報 1*，*詳細情報 2*]

同じ製品情報識別子を持つ製品情報がすでに存在します。

(S)

処理を中止します。

(O)

すでに定義された製品情報とは別の製品情報識別子を持つ製品情報を指定して，再実行します。

製品情報識別子とは，JP1 イベント種別，プロダクト名から構成される製品情報を一意に識別するための情報です。

KDSQ4614-E

既に同じ正規化ルールが存在します。別の Windows イベント ID を持つ正規化ルールを指定してください。[詳細情報：*詳細情報 1*，*詳細情報 2*]

選択された製品情報の中に，同じ Windows イベント ID を持つ正規化ルールがすでに定義されています。

(S)

処理を中止します。

(O)

すでに定義された正規化ルールとは別の Windows イベント ID を持つ正規化ルールを指定して，再実行します。

KDSQ4807-E

JP1/NETM/Audit - Manager Define **サービスに接続することができません。[詳細情報** : ***詳細情報 1，詳細情報 2*****]**

JP1/NETM/Audit - Manager Define サービスに接続できません。

(S)

処理を終了します。

(O)

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。
繰り返し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。

KDSQ4808-E

JP1/NETM/Audit - Manager Define **サービスとのデータの送受信に失敗しました。[詳細情報** : ***詳細情報 1，詳細情報 2*****]**

JP1/NETM/Audit - Manager Define サービスとのデータの送受信に失敗しました。

(S)

処理を中止します。

(O)

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。
繰り返し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。

KDSQ4809-E

JP1/NETM/Audit - Manager Define **サービスからの応答待ちでタイムアウトしました。[詳細情報** : ***詳細情報 1，詳細情報 2*****]**

タイムアウト時間が経過しても JP1/NETM/Audit - Manager Define サービスからの応答がありませんでした。

(S)

処理を中止します。

(O)

［リリース実行］ボタンクリック時にこのメッセージが出力された場合
admlsrelease プロセスが実行されていないことを確認したあとで，正規化ルールエディタを再起動してください。admlsrelease プロセスが実行されている場合は，admlsrelease プロセスが終了したあとで，正規化ルールエディタを再起動してください。admlsrelease プロセスの終了まで数十分かかることがありま

す。

上記以外の場合

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。

繰り返し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。

KDSQ4810-E

JP1/NETM/Audit - Manager Define **サービスとの通信回線の設定に失敗しました。(*詳細情報*)**

JP1/NETM/Audit - Manager Define サービスとの通信処理でエラーが発生しました。

(S)

処理を中止します。

(O)

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。

繰り返し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。

KDSQ4811-E

JP1/NETM/Audit - Manager Define **サービスにはすでに他の正規化ルールエディタが接続済み，または** JP1/NETM/Audit - Manager Define **サービスでリリース処理が実行中のため，接続することはできません。[詳細情報**：***詳細情報 1*，*詳細情報 2*]

JP1/NETM/Audit - Manager Define サービスに，ほかの正規化ルールエディタが接続中です。

(S)

処理を中止します。

(O)

接続中の正規化ルールエディタを終了し，admlsrelease プロセスが実行されていないことを確認したあとで，正規化ルールエディタを再起動してください。プロセス admlsrelease が実行されている場合は，admlsrelease プロセスが終了したあとで，正規化ルールエディタを再起動してください。admlsrelease プロセスの終了まで数十分かかることがあります。

繰り返しこのメッセージが表示される場合は，JP1/NETM/Audit - Manager Define サービスを再起動してください。

KDSQ4812-E

JP1/NETM/Audit - Manager Define **サービスとの回線が切断されています。再接続のためには，正規化ルールエディタを再起動してください。[詳細情報**：***詳細情報 1*，*詳細情報 2***]**

JP1/NETM/Audit - Manager Define サービスとの回線が切断されています。

(S)

処理を中止します。

(O)

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。
繰り返し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。

KDSQ4813-E

JP1/NETM/Audit - Manager Define サービスでインポート・エクスポートコマンドが実行中のため，接続することはできません。[詳細情報 : *詳細情報 1*，*詳細情報 2*]

JP1/NETM/Audit - Manager Define サービスでインポート・エクスポートコマンドが実行中です。

(S)

処理を中止します。

(O)

実行中のインポート・エクスポートコマンドが終了してから，再実行してください。

KDSQ4814-E

JP1/NETM/Audit - Manager Define サービスとの回線が正常に切断できませんでした。[詳細情報 : *詳細情報 1*，*詳細情報 2*]

JP1/NETM/Audit - Manager Define サービスとの回線が正常に切断できませんでした。

(S)

処理を中止します。

(O)

JP1/NETM/Audit - Manager Define サービスが実行中か確認してください。

KDSQ4900-E

回復不能なエラーが発生しました。正規化ルールエディタを終了します。[詳細情報 : *詳細情報 1*，*詳細情報 2*]

正規化ルールエディタで回復不能な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。

KDSQ4901-E

メモリ不足が発生しました。正規化ルールエディタを終了します。[詳細情報 : *詳細情報 1*，*詳細情報 2*]

正規化ルールエディタでメモリ不足が発生しました。

（S）

処理を強制終了します。

（O）

不要なアプリケーションプログラムを終了し，正規化ルールエディタを再起動してください。

KDSQ4902-E

起動処理中に予期しないエラーが発生したため，正規化ルールエディタを起動することができません。[詳細情報：*詳細情報 1*，*詳細情報 2*]

正規化ルールエディタの起動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）

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。

繰り返し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。

KDSQ4903-E

正規化ルールエディタでシステムエラーが発生したため，*処理名*に失敗しました。[終了コード：*終了コード*，詳細コード：*詳細コード*] [詳細情報：*詳細情報 1*，*詳細情報 2*]

正規化ルールエディタでシステム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。

KDSQ4904-E

JP1/NETM/Audit - Manager Define **サービスでシステムエラーが発生したため，*処理名*に失敗しました。[詳細情報：*詳細情報 1*，*詳細情報 2*]**

JP1/NETM/Audit - Manager Define サービスでシステムエラーが発生しました。

（S）

処理を中止します。

（O）

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。

繰り返し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。

KDSQ4905-E

JP1/NETM/Audit - Manager Define サービスとの通信処理にてエラーが発生したため，正規化ルールエディタの起動に失敗しました。[詳細情報 : *詳細情報 1*，*詳細情報 2*]

JP1/NETM/Audit - Manager Define サービスとの通信処理にてエラーが発生しました。

(S)

処理を終了します。

(O)

JP1/NETM/Audit - Manager Define サービスが実行中か確認し，正規化ルールエディタを再起動してください。繰り返し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。

KDSQ4906-E

設定ファイル (*設定ファイル名*) の入力でエラーが発生しました。[詳細情報 : *詳細情報 1*，*詳細情報 2*]

設定ファイルから値が取得できませんでした。

(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。

KDSQ4980-E

正規化ルールエディタの起動に失敗しました。[詳細情報 : *詳細情報 1*，*詳細情報 2*，*詳細情報 3*]

正規化ルールエディタの起動に失敗しました。

(S)

処理を終了します。

(O)

システムのリソースが不足していないか，または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。

付録

付録 A　バージョンごとの変更内容

付録 A.1　09-00 での変更内容

- 標準サポート製品に，活文 NAVIstaff を追加した。
- 定義できる製品情報は，あらかじめ定義されている標準サポート製品以外に 50 件までであることを追記した。
- メッセージテキスト中の日付情報が 1 けたで出力される場合でも，監査ログフォーマット「年：YY」，「月：MM」，「日：DD」，「時：hh」，「分：mm」，および「秒：ss」に対応づけられるよう変更した。例えば，1 月 1 日が 1/1 と出力される場合でも，「月：MM」と「日：DD」に対応づけができる。
- Windows Server 2008 のイベントログのレベルについて，「重大（Critical）」および「詳細（Verbose）」のレベルを，正規化ルールエディタを利用して，正規化し収集できるようにした。

付録 A.2　08-51 での変更内容

- 監査ログフォーマットと JP1 イベント属性とを対応づける際の注意事項を追加した。
- 画面項目の表記を次のように変更した。
  - 「関連ツリーエリア」を「ツリーエリア」に変更した。
  - 「詳細表示エリア」を「詳細エリア」に変更した。
- メイン画面の［編集］ボタンのボタン名に「...」を追加した。
- ［正規化ルール］ダイアログを次のように変更した。
  - ［正規化ルール］ダイアログのいちばん上に製品情報名を表示した。
  - ［編集］ボタン，［選択］ボタン，および［追加］ボタンのボタン名に「...」を追加した。
  - 横スクロールバーを追加し，プレビューをすべて確認できるようにした。
- 正規化ルールの定義が未完了の状態で一時的に保存した場合，製品情報が「編集（未完了）」状態，または「リリース編集（未完了）」状態になる旨を追加した。
- 正規化ルールの定義が未完了の状態でも，一時的に保存できる機能を追加した。
- 正規化ルールの定義の状態遷移を表す図を追加した。
- ［正規化ルール選択］ダイアログの［選択］ボタンのボタン名に「...」を追加した。
- メッセージを追加・変更した。

付録 B　用語解説

（英字）

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/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。
なお，JP1/Base は，JP1/NETM/Audit - Manager の前提プログラムです。

JP1 イベント

監査ログ収集対象プログラムで何らかの事象（ジョブの実行結果，サービスのエラーなど）が発生した時，Windows イベントログまたはログファイルが出力されます。JP1 イベントは，これらのログ出力を検知して，JP1/Base が発行するイベントです。

（ア行）

イベントログトラップ機能

Windows イベントログを JP1 イベントに変換する JP1/Base の機能です。

インポート

エクスポートした製品情報や正規化ルールの定義を，正規化ルールエディタに一括で定義することです。JP1/NETM/Audit を別ホストに移行する場合などに使用します。
インポートには，admrrimport コマンドを使用します。
定義を移行する流れについては，「4.6　定義を移行する」を参照してください。

エクスポート

正規化ルールエディタに定義された製品情報や正規化ルールを，まとめて一つのファイル（正規化ルール定義エクスポートファイル）にバックアップすることです。JP1/NETM/Audit を別ホストに移行する場合などに使用します。
エクスポートには，admrrexport コマンドを使用します。
定義を移行する流れについては，「4.6　定義を移行する」を参照してください。

（カ行）

監査証跡管理システム

JP1/NETM/Audit - 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管管理を実現します。

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/NETM/Audit - Manager に組み込まれているデータベースを使用します。

監査ログ収集対象プログラム
JP1/NETM/Audit - Manager がログ収集を行う対象のプログラムです。

監査ログの結果
成功か失敗か，起動か停止かなどの，事象の結果情報です。正規化ルール定義エディタでは，「監査事象の結果」と表示されます。

監査ログの収集カテゴリ
ログが出力される契機となった事象の種別です。正規化ルール定義エディタでは，「監査事象の種別」と表示されます。

監査ログフォーマット
JP1/NETM/Audit で管理できる監査ログのフォーマットのことです。

（サ行）

正規化ルール
監査ログ収集対象プログラムから収集された JP1 イベントを，JP1/NETM/Audit が管理できる監査ログフォーマットに変換するためのルールを定義するものです。

正規化ルールエディタ
JP1/NETM/Audit の機能のうち，正規化ルールを定義する GUI のことです。

正規化ルール定義エクスポートファイル
正規化ルールエディタに定義された製品情報や正規化ルールをエクスポートした際にできるファイルです。
JP1/NETM/Audit を別ホストに移行する場合などに使用します。
エクスポートには，admrrexport コマンドを使用します。
定義を移行する流れについては，「4.6　定義を移行する」を参照してください。

正規化ルールの定義の状態
正規化ルールの定義が，どのような状態にあるのかを示します。
状態には，「編集」状態，「リリース許可」状態，「リリース」状態，「リリース編集」状態，および「リリース解除許可」状態があります。
なお，これらの状態は，メイン画面のツリーエリアにある製品情報のアイコンで判断できます。

製品情報
正規化ルールエディタで定義する，監査ログ収集対象プログラムの情報です。Windows イベントログを収集するのか，ログファイルとして収集するのかなどの情報を定義します。

製品情報を定義すると，監査ログへの変換で，JP1/NETM/Audit に登録されている正規化ルールのうち，どれを使用するかを決めるための情報になります。

（タ行）

通常モード

リリース照会モードに対して，使用する用語です。
リリース照会モードではない状態のメイン画面を指します。

（ハ行）

標準サポート製品

JP1/NETM/Audit が正規化ルールを用意している製品です。
正規化ルールエディタを最初に起動したとき，すでにツリーエリアに表示されている Hitachi Storage，Windows 2008 セキュリティログ，および活文 NAVIstaff は標準サポート製品です。これらの製品情報は，データベースのセットアップ後に自動的に「リリース」状態になっています。
なお，正規化ルールエディタに定義されていない標準サポート製品もあります。JP1/AJS3 - Manager，JP1/NETM/DM などが該当します。標準サポート製品の一覧については，マニュアル「JP1/NETM/Audit 構築・運用ガイド」の前提プログラムについて説明している個所を参照してください。

フィールド生成

正規化ルールの定義で，JP1 イベント属性および入力文字列を変換後の監査ログに埋め込むことです。

編集状態

正規化ルールの定義の状態です。
製品情報，または正規化ルールを新規に定義したり，編集したり，削除したりできる状態を意味します。正規化ルールの定義が完了している状態（完了），および完了していない状態（未完了）があります。

（ラ行）

リリース

監査ログへの変換で正規化ルールを使用できるようにすることです。

リリース解除許可状態

正規化ルールの定義の状態です。
リリース中の製品情報のリリースを解除する前に，いったんリリースの解除を許可している状態を意味します。

リリース許可

リリースを許可することです。リリースするには，いったんリリースを許可しておく必要があります。

リリース許可状態

正規化ルールの定義の状態です。
製品情報，および正規化ルールの定義が終わって，監査ログへの変換で使用してもよい状態（「リリース」状態）にする前に，いったんリリースを許可している状態を意味します。

リリース照会モード

メイン画面に，現在リリースされている定義内容だけが表示されている状態のことをいいます。

リリース状態

正規化ルールの定義の状態です。
正規化ルールの定義が，監査ログへの変換で使用されている状態を意味します。

リリース編集状態

正規化ルールの定義の状態です。
「リリース」状態の定義情報を，リリースと並行して編集している状態を意味します。正規化ルールの定義が完了している状態（完了），および完了していない状態（未完了）があります。

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。

索引

A

H

J

い

う

え

お

か

き

け

こ

さ

し

す

せ

そ

つ

て

と

に

は

ひ

ふ

へ

ほ

め

り

れ

ろ

ソフトウェアマニュアルのサービス ご案内

１．マニュアル情報ホームページ

ソフトウェアマニュアルの情報をインターネットで公開しています。

URL　http://www.hitachi.co.jp/soft/manual/

ホームページのメニューは次のとおりです。

■マニュアル一覧	日立コンピュータ製品マニュアルを製品カテゴリ，マニュアル名称，資料番号のいずれかから検索できます。
■CD-ROMマニュアル	日立ソフトウェアマニュアルと製品群別CD-ROMマニュアルの仕様について記載しています。
■マニュアルのご購入	マニュアルご購入時のお申し込み方法を記載しています。
■オンラインマニュアル	一部製品のマニュアルをインターネットで公開しています。
■サポートサービス	ソフトウェアサポートサービスお客様向けページでのマニュアル公開サービスを記載しています。
■ご意見・お問い合わせ	マニュアルに関するご意見，ご要望をお寄せください。

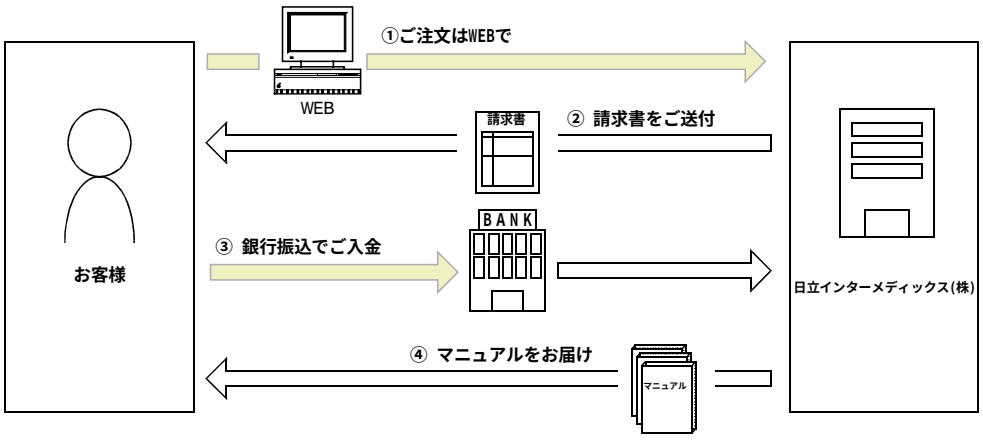
２．インターネットでのマニュアル公開

2 種類のマニュアル公開サービスを実施しています。

(1) マニュアル情報ホームページ「オンラインマニュアル」での公開
　製品をよりご理解いただくためのご参考として，一部製品のマニュアルを公開しています。

(2) ソフトウェアサポートサービスお客様向けページでのマニュアル公開
　ソフトウェアサポートサービスご契約のお客様向けにマニュアルを公開しています。公開しているマニュアルの一覧，本サービスの対象となる契約の種別などはマニュアル情報ホームページの「サポートサービス」をご参照ください。

３．マニュアルのご注文



① マニュアル情報ホームページの「マニュアルのご購入」にアクセスし，お申し込み方法をご確認のうえ WEB からご注文ください。ご注文先は日立インターメディックス(株)となります。

② ご注文いただいたマニュアルについて請求書をお送りします。

③ 請求書の金額を指定銀行へ振り込んでください。

④ 入金確認後 7 日以内にお届けします。在庫切れの場合は，納期を別途ご案内いたします。