HITACHI
Inspire the Next

Hitachi Global Link Manager

導入・設定ガイド

4010-1J-169-40

対象製品

Hitachi Global Link Manager 8.8.7
適用 OS の詳細については「ソフトウェア添付資料」でご確認ください。

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。
なお、不明な場合は、弊社担当営業にお問い合わせください。

商標類

HITACHI，HiRDB，JP1 は，株式会社 日立製作所の商標または登録商標です。
Active Directory は，マイクロソフト 企業グループの商標です。
AIX は，世界の多くの国で登録された International Business Machines Corporation の商標です。
AMD は，Advanced Micro Devices, Inc.の商標です。
Hyper-V は，マイクロソフト 企業グループの商標です。
IBM は，世界の多くの国で登録された International Business Machines Corporation の商標です。
Intel は，Intel Corporation またはその子会社の商標です。
Itanium は，Intel Corporation またはその子会社の商標です。
Linux は，Linus Torvalds 氏の米国およびその他の国における登録商標です。
Microsoft は，マイクロソフト 企業グループの商標です。
Microsoft Edge は，マイクロソフト 企業グループの商標です。
Oracle と Java は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です。
This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
This product includes software developed by IAIK of Graz University of Technology.
Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.
Red Hat は，米国およびその他の国における Red Hat, Inc.の登録商標です。
Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.
Red Hat Enterprise Linux は，米国およびその他の国における Red Hat, Inc.の登録商標です。
RSA および BSAFE は，米国 EMC コーポレーションの米国およびその他の国における商標または登録商標です。
UNIX は，The Open Group の商標です。
Visual C++は，マイクロソフト 企業グループの商標です。
Windows は，マイクロソフト 企業グループの商標です。
Windows Server は，マイクロソフト 企業グループの商標です。
This product includes software developed by the JDOM Project (http://www.jdom.org/).
その他記載の会社名，製品名などは，それぞれの会社の商標もしくは登録商標です。
Hitachi Global Link Manager は，米国 EMC コーポレーションの RSA BSAFE® ソフトウェアを搭載しています。
This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.
Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.
This product includes software developed by the University of California, Berkeley and its contributors.
This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).
Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).
This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).
This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).
This product includes software developed by Andy Clark.

発行
2023 年 2 月 4010-1J-169-40

目次

図目次

表目次

はじめに

このマニュアルは Hitachi Global Link Manager（以降，Global Link Manager と表記します）のプログラムのインストール，セットアップ，サーバ運用について説明したものです。

対象読者

Global Link Manager のシステムを構築，運用する方を対象にしています。対象読者によって，次の知識があることを前提にしています。

- HDLM の環境設定や運用方法の知識
- サーバの OS（Windows）の知識

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。

1. Global Link Manager のシステム構成と要件

   Global Link Manager のシステム構成および要件について説明しています。

2. Global Link Manager のインストール

   Global Link Manager のインストール方法について説明しています。

3. Global Link Manager の設定

   Global Link Manager の起動と停止，Global Link Manager のデータベースのバックアップとリストアなど，Global Link Manager の設定について説明しています。

4. クラスタ環境での Global Link Manager のインストール

   管理サーバをクラスタ構成にする場合の設定について説明しています。

5. 通信に関するセキュリティの設定

   Global Link Manager で利用できる通信に関するセキュリティ設定について説明しています。

6. ほかの製品と連携するための Global Link Manager の設定

   ほかの製品と連携するための Global Link Manager での設定について説明しています。

7. Global Link Manager のトラブルシューティング

   Global Link Manager の運用中に発生したトラブルの対処方法について説明しています。

付録 A. 共通エージェントコンポーネントの設定

ホストの共通エージェントコンポーネントの設定，起動手順などについて説明しています。

付録 B. このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報について説明しています。

マイクロソフト製品の表記について

このマニュアルでは，マイクロソフト製品の名称を次のように表記しています。

表記	製品名
Hyper-V	Microsoft® Hyper-V®
Microsoft Edge	Microsoft® Edge
Windows 10	次の製品を区別する必要がない場合の表記です。 ・ Windows 10(32-bit) ・ Windows 10(64-bit)
Windows 10(32-bit)	次の製品を区別する必要がない場合の表記です。 ・ Windows® 10 Pro 32-bit

表記	製品名
	• Windows® 10 Education 32-bit • Windows® 10 Enterprise 32-bit
Windows 10(64-bit)	次の製品を区別する必要がない場合の表記です。 • Windows® 10 Pro 64-bit • Windows® 10 Education 64-bit • Windows® 10 Enterprise 64-bit
Windows 11(64-bit)	次の製品を区別する必要がない場合の表記です。 • Windows® 11 Pro 64-bit • Windows® 11 Education 64-bit • Windows® 11 Enterprise 64-bit
Windows Server 2012	次の製品を区別する必要がない場合の表記です。 • Windows Server 2012(x64) • Windows Server 2012 R2
Windows Server 2012(x64)	次の製品を区別する必要がない場合の表記です。 • Microsoft® Windows Server® 2012 Datacenter • Microsoft® Windows Server® 2012 Essentials • Microsoft® Windows Server® 2012 Standard
Windows Server 2012 R2	次の製品を区別する必要がない場合の表記です。 • Microsoft® Windows Server® 2012 R2 Datacenter • Microsoft® Windows Server® 2012 R2 Essentials • Microsoft® Windows Server® 2012 R2 Standard
Windows Server 2016	Windows Server 2016(x64)
Windows Server 2016(x64)	次の製品を区別する必要がない場合の表記です。 • Microsoft® Windows Server® 2016 Datacenter • Microsoft® Windows Server® 2016 Standard
Windows Server 2019	Windows Server 2019(x64)
Windows Server 2019(x64)	次の製品を区別する必要がない場合の表記です。 • Microsoft® Windows Server® 2019 Datacenter • Microsoft® Windows Server® 2019 Standard
Windows Server 2022	Windows Server 2022(x64)
Windows Server 2022(x64)	次の製品を区別する必要がない場合の表記です。 • Microsoft® Windows Server® 2022 Datacenter • Microsoft® Windows Server® 2022 Standard

このマニュアルでは，Windows 10，Windows 11，Windows Server 2012，Windows Server 2016，Windows Server 2019，および Windows Server 2022 を区別する必要がない場合，Windows と表記しています。

このマニュアルで使用している記号

このマニュアルでは，GUI に表示される項目について，次に示す記号を使用しています。

記号	意味
［］	メニュー，タブ，ボタンなど GUI に表示される項目の名称を［］で囲んで示します。メニュー項目を連続して選択する場合は，［］を「－」（ハイフン）でつないで説明しています。 （例）［リソース］－［ホスト］ ［リソース］メニューから［ホスト］メニューを選択することを意味します。

記号	意味
「 」	GUI に表示される値や入力する値を示します。
＜ ＞	該当する要素が表示されることを示します。 （例）＜ホスト名＞サブウィンドウ

また，コマンドの記述方法については，次に示す記号を用いて説明しています。

記号	意味と例
|	複数の項目に対して項目間の区切りを示し，「または」の意味を示します。 （例） 「A|B|C」は，「A，B，または C」を示します。
{ }	この記号で囲まれている複数の項目の中から，必ず 1 つの項目を選択します。項目と項目の区切りは「|」で示します。 （例） 「{A|B|C}」は，「A，B，または C のどれかを必ず指定する」ことを示します。
[ ]	この記号で囲まれている項目は，任意に指定できます（省略できます）。 （例） 「[A]」は，「必要に応じて A を指定する」ことを示します（必要でない場合は，A を省略できます）。 「[B|C]」は，「必要に応じて B，または C を指定する」ことを示します（必要でない場合は，B および C を省略できます）。
＜ ＞	該当する要素を指定することを示します。 （例） 「-p ＜*パスワード*＞」は，「-p と入力したあと，パスワードとなる任意の文字列を指定する」ことを示します。

1

Global Link Manager のシステム構成と要件

この章では，Global Link Manager のシステム構成および要件について説明します。

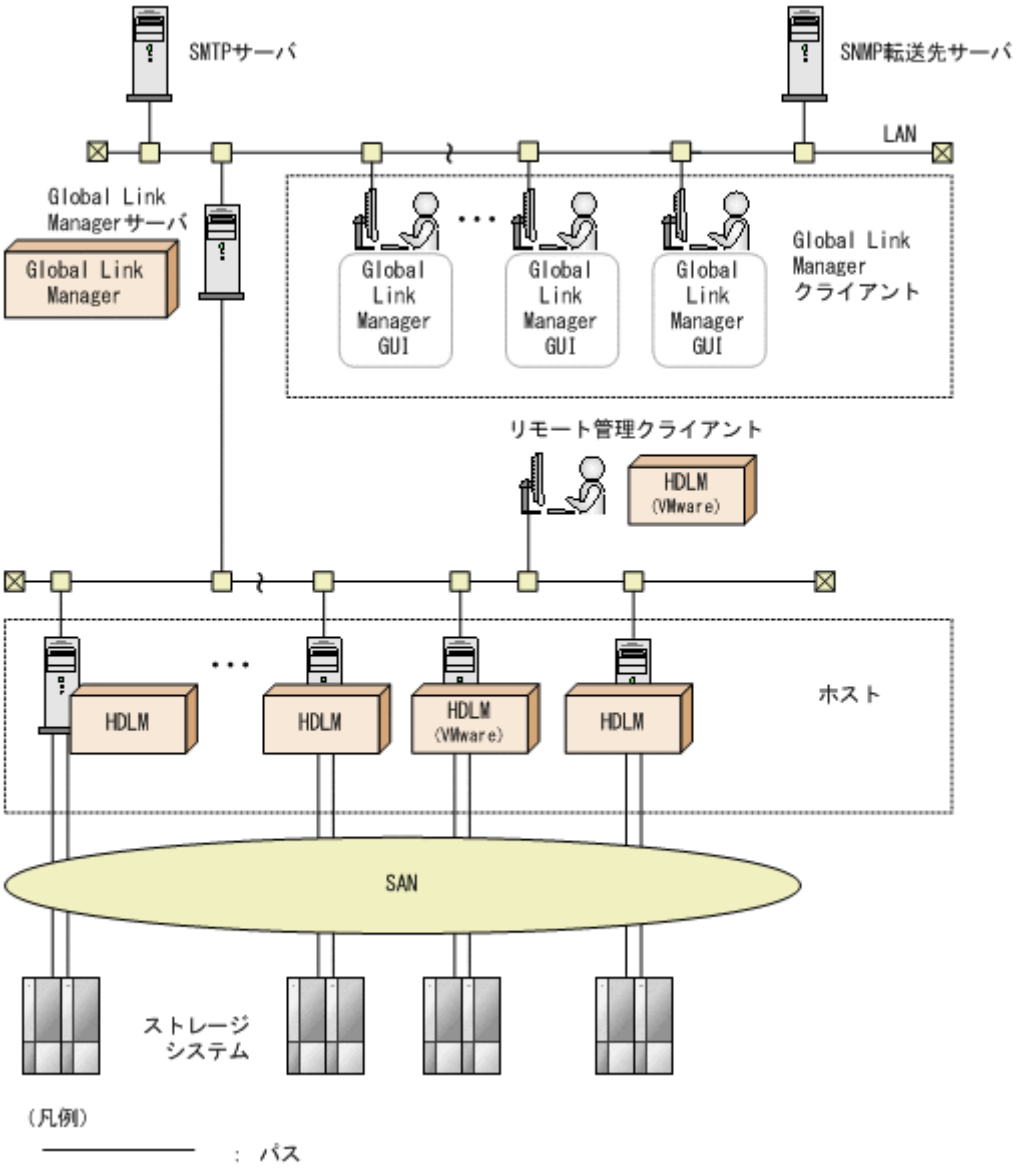
1.1 Global Link Manager とは

Global Link Manager は，HDLM（Hitachi Dynamic Link Manager および Hitachi Dynamic Link Manager EX）のパス制御機能を利用して，大規模なシステム構成で統合的にパスを管理する製品です。HDLM ではホストごとにパスを管理するのに対して，Global Link Manager では複数のホストのパスを一括して管理します。

ホストを何台も使用した大規模なシステム構成の場合，各ホストでパスを管理するための作業負荷は，規模の大きさに比例して増大します。Global Link Manager を使用すると，複数ホストのパス情報を一元管理することによって，作業負荷を低減できます。また，システム全体での負荷バランスを考慮してパスの稼働状態を切り替えたり，各ホストから障害情報を通知させ，いち早く障害に対処したりすることによって，システムの信頼性を向上できます。

Global Link Manager では，複数のホストにインストールされた HDLM からパスに関する情報を収集し，Global Link Manager サーバで一括して管理します。一元化された情報は，ホストを管理する複数のユーザーがクライアントマシンから参照したり制御したりできます。Global Link Manager のシステム構成例を次の図に示します。

図 1-1 Global Link Manager のシステム構成例



Global Link Manager には次の特長があります。

複数ホストのパス情報を一括して管理します

Global Link Manager GUI を使用した遠隔操作で，ホストの HDLM からの情報取得や設定を一括して実行します。各ホストにそれぞれログインしなくても，1 つのコンソールで管理できます。複数のホストを一元管理できるため，パス情報は，ホスト単位や HBA ポート単位に加え，ストレージシステム単位，CHA ポート単位，パス状態単位など，複数ホストにわたる視点で一覧を表示することもできます。

システム全体のパスの稼働状況をサマリーで確認できます

目的に応じた視点でパスの一覧を表示するとともに，パスが正常か障害が発生しているかを集約した情報（状態ごとのパス本数）を表示します。各ホストでそれぞれ確認しなくても，システム全体のパスの稼働状況を把握できます。

パスの帯域幅制御を支援します

ストレージシステム単位，CHA ポート単位などでパス情報を表示し，複数のユーザーアプリケーションまたはホストの間でパスの帯域幅（オンラインパスの本数）を調整できます。

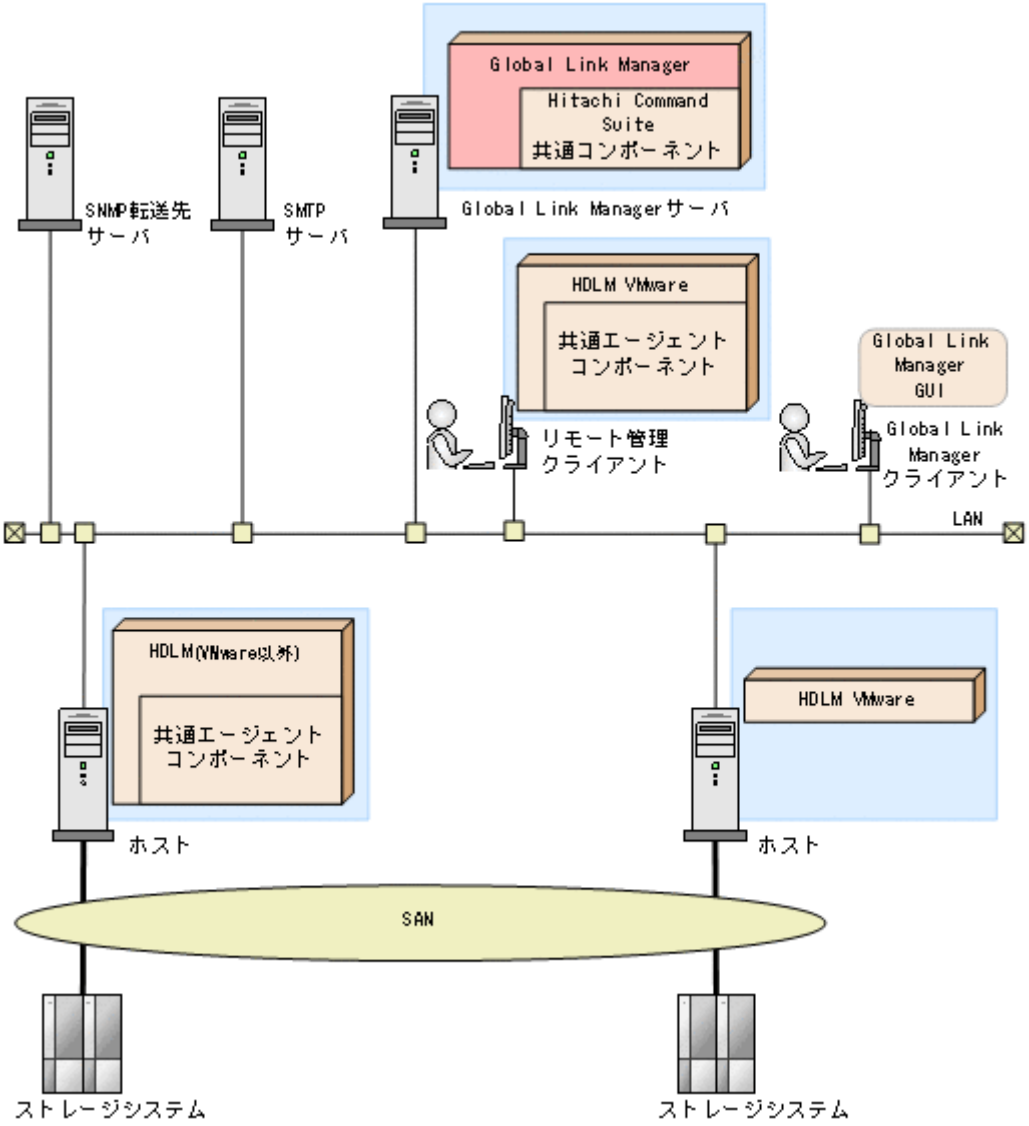
複数ホストの障害情報を一元管理できます

多数のホストで起こる障害をいち早く発見して対処するためには，障害情報が発生源から通知されて，障害個所を特定できる環境が必要です。Global Link Manager では，各ホストの HDLM が検知したパスの障害情報をアラートとして通知するように設定し，一元管理できます。また，アラート情報を Global Link Manager サーバからほかのサーバ（SNMP 転送先サーバ）に転送して，ユーザーが任意のアプリケーションで管理することもできます。

1.2 Global Link Manager のシステム構成

Global Link Manager は，複数ストレージシステムと複数ホストから構成される中規模から大規模の SAN 環境のパス管理を実現します。次の図に Global Link Manager の基本的なシステム構成を示します。

図 1-2 Global Link Manager の基本的なシステム構成



上記の図に示したシステムの構成の要素について説明します。

Global Link Manager サーバ

Global Link Manager をインストールするマシンです。Global Link Manager サーバは，各ホストに対してシステム構成情報を要求し，収集した情報を Global Link Manager クライアントに提供します。

Global Link Manager は，Global Link Manager GUI からの要求に対して，ホストから情報を収集したり，ホストに対して設定を実施したりします。

Hitachi Command Suite 共通コンポーネントは，Hitachi Command Suite 製品のサーバ，GUI の基盤機能を提供します。Hitachi Command Suite 共通コンポーネントは Global Link Manager，Device Manager，Tuning Manager などの Hitachi Command Suite のサーバ製品の一部としてインストールされ，常に最新のバージョンに上書きされます。

Global Link Manager クライアント

Global Link Manager GUI を実行するためのマシンです。Global Link Manager GUI は Global Link Manager でホストを管理するためのユーザーインターフェースを提供します。

リモート管理クライアント

LAN を経由してホストに接続し，制御する共通エージェントコンポーネント，またはそれをインストールするマシンです。リモート管理クライアントが管理できるのは，VMware 版 HDLM だけです。ホストの OS が VMware の場合，必須です。

ホスト

業務プログラムをインストールするためのマシンです。Global Link Manager を使用するシステムの場合，ホストはストレージシステムを外部記憶装置として使用していて，HDLM がストレージシステムとホストを結ぶパスを管理しています。OS が VMware の場合，ESXi のハイパーバイザが稼働しているサーバマシンを，ホストと呼びます。

HDLM は，ストレージシステムとホストとを結ぶパスを管理します。HDLM を使用することで，パスに掛かる負荷を分散したり，障害発生時にパスを切り替えたりして，システムの信頼性を向上できます。

Global Link Manager サーバとホストの情報通信のために，共通エージェントコンポーネントが必要になります。

共通エージェントコンポーネントは，HDLM に含まれるコンポーネントです。

ストレージシステム

ホストに接続された外部記憶装置です。Global Link Manager の管理対象は, HDLM によってパスが管理されているストレージシステムです。

SNMP 転送先サーバ

Global Link Manager サーバから SNMP Trap によって転送されたアラート情報を受信するマシンです。SNMP 転送先サーバにアラート情報を転送するには，Global Link Manager サーバの設定が必要です。アラート転送の設定については，「3.13 アラート転送の設定」を参照してください。

SMTP サーバ

Global Link Manager サーバが受信したアラート情報を，E-mail で通知するためのマシンです。メールサーバとして使用します。

Global Link Manager のシステム構成については次の個所でも説明しています。使用する環境に応じて，該当する個所を参照してください。

- クラスタ環境のシステム構成：「4.1 Global Link Manager のクラスタ環境でのシステム構成」
- ほかの Hitachi Command Suite 製品と連携する場合のシステム構成：「6.1 Hitachi Command Suite 製品のシングルサインオンおよびユーザー管理の統合の概要」

1.3 Global Link Manager のシステム要件

Global Link Manager のシステム要件は次のとおりです。

1.3.1 Global Link Manager サーバの要件

Global Link Manager をインストールするサーバの要件を次の表に示します。

表 1-1 Global Link Manager をインストールするサーバの要件

項目	要件
適用 OS※1	・ Windows Server 2012（x64）※2 （Datacenter，Essentials，Standard） ・ Windows Server 2012 R2※2 ※5 （Datacenter，Essentials，Standard） ・ Windows Server 2016（x64）※2 （Datacenter，Standard） ・ Windows Server 2019（x64）※2 （Datacenter，Standard） ・ Windows Server 2022（x64）※2 （Datacenter，Standard）
ディスクの空き容量 （新規インストールの場合）	6.5GB 以上※3 ※4
クラスタ構成の場合の適用クラスタソフトウェア	次に示す OS のクラスタサービス ・ Windows Server 2012（x64）※2 （Datacenter，Standard） ・ Windows Server 2012 R2※2 （Datacenter，Standard） ・ Windows Server 2016（x64）※2 （Datacenter，Standard） ・ Windows Server 2019（x64）※2 （Datacenter，Standard） ・ Windows Server 2022（x64）※2 （Datacenter，Standard）
サポートしている仮想化プラットフォームと OS の組み合わせ	・ VMware ESX/ESXi Server 5 （Windows Server 2012 （x64）（SP なし）） ・ VMware ESX/ESXi Server 5 （Windows Server 2012 R2（SP なし）） ・ VMware ESX/ESXi Server 6 （Windows Server 2012 （x64）（SP なし）） ・ VMware ESX/ESXi Server 6 （Windows Server 2012 R2（SP なし）） ・ Windows Server 2012 Hyper-V 3 （Windows Server 2012（x64）（SP なし）） ・ Windows Server 2012 R2 Hyper-V 3 （Windows Server 2012 R2（SP なし）） ・ Windows Server 2016 Hyper-V （Windows Server 2016（x64）（SP なし）） ・ Windows Server 2019 Hyper-V （Windows Server 2019（x64）（SP なし）） ・ Windows Server 2022 Hyper-V （Windows Server 2022（x64）（SP なし））

注※1

Global Link Manager を Hyper-V 上の仮想マシンで動作させる場合には，その仮想マシンに 1GB のメモリを割り当てて，製品の推奨構成と同じになるように構成定義してください。

注※2

IPv4 環境および IPv6 環境で運用できます。

注※3

Global Link Manager のインストール先とデータベースファイルの格納先に異なるドライブを指定する場合，次の空き容量が必要です。

Global Link Manager インストール先のディスク：3GB 以上（HDLM インストーラーのダウンロード機能を有効にする場合は，さらに 1GB が必要です。）

データベースファイル格納先のディスク：4GB 以上

注※4

HDLM インストーラーのダウンロード機能を有効にする場合は，さらに 1GB が必要です。

注※5

KB2919442 と KB2919355 がインストールされている必要があります。

管理するホスト，マルチパス LU およびパスの上限の目安は，次に示す表を参考にしてください。

表 1-2 Global Link Manager 管理対象の上限の目安

管理対象	上限値
ホスト	1500
マルチパス LU※1	15000
パス※1※2	60000

注※1

1 ホスト当たりのマルチパス LU またはパスの上限値は，下記を目安にしてください。

マルチパス LU またはパスの上限値 / 管理対象のホスト数

注※2

パス稼働情報のレポートを出力するためにホストのパス稼働情報（パスステータスログ）の取得を有効に設定している場合には, HDLM バージョンが 5.9 以降のホスト当たりのパスの上限値は，1000 パスを目安にしてください。

デフォルトでは，ホストのパス稼働情報（パスステータスログ）の取得は無効になっています。取得の有効，無効は，プロパティファイル（server.properties）の server.pathreport.enable で指定します。プロパティファイルの設定方法については，「3.5 Global Link Manager の環境設定の変更」を参照してください。

パス稼働情報のレポート出力については, マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

注意事項

- Global Link Manager のバージョンが v8.0 以降の場合，v8.0 より前のバージョンの Hitachi Command Suite 製品と共存できません。そのため, インストール/アップグレードする Hitachi Command Suite 製品のバージョンは，すべて v8.0 以降にしてください。
- Global Link Manager は，次に示す HiRDB 製品と共存できません。そのため，すでに HiRDB 製品がインストールされているマシンに Global Link Manager をインストールしないでください。また，Global Link Manager がインストールされているマシンに，該当する HiRDB 製品をインストールしないでください。
  - HiRDB/Single Server
  - HiRDB/Parallel Server
  - HiRDB/Workgroup Server
  - HiRDB/Run Time
  - HiRDB/Developer's Kit
  - HiRDB SQL Executer

- Global Link Manager サーバの IP アドレスには，静的なアドレスを設定しておく必要があります。DHCP は使用しないでください。IPv4，IPv6 の両方のプロトコルでの接続をサポートします。IPv6 プロトコルを使用する場合は，管理サーバで IPv4 と IPv6 の両方が有効になっている必要があります。使用できる IPv6 アドレスはグローバルアドレスだけです。
- Global Link Manager をインストールする前に，インストールするマシンのローカル時間は現在の日時を設定しておいてください。現在の日時に設定していない場合，パス稼働情報（パスステータスログ）が正しく取得されないおそれがあります。インストール後に時刻を変更する場合，またはほかの Hitachi Command Suite 製品がインストールされている環境で時刻を変更する場合は，「3.3 Global Link Manager をインストールするマシンの時刻の変更」を参照してください。

1.3.2 Global Link Manager クライアントの要件

Global Link Manager GUI を使用するためのクライアントの要件を次の表に示します。

表 1-3 Global Link Manager GUI を使用するためのクライアントの要件

適用 OS，または項目		適用 Web ブラウザー，または要件
Windows	• Windows 10（32-bit）※ （Windows 10 Pro，Windows 10 Education，Windows 10 Enterprise） • Windows 10（64-bit）※ （Windows 10 Pro，Windows 10 Education，Windows 10 Enterprise）	• Chrome Browser for enterprise（Latest version of stable channel） • Microsoft Edge（Latest version of stable channel）
	Windows 11（64-bit）※ （Windows 11 Pro，Windows 11 Education，Windows 11 Enterprise）	• Chrome Browser for enterprise（Latest version of stable channel） • Microsoft Edge（Latest version of stable channel）
モニターのビデオ解像度		SVGA（800×600）以上

注※

IPv4 環境および IPv6 環境で運用できます。

1.3.3 ホストの要件

Global Link Manager で管理するホストには，HDLM がインストールされ，環境設定が済んでいることが前提になります。

ホストの HDLM のバージョンが 6.0 以降の場合は，Global Link Manager と IPv4 および IPv6 で接続できます。

注意事項

- 複数のネットワークインターフェースカードを搭載している場合は，各ホストの共通エージェントコンポーネントの `server.properties` ファイルで，`server.http.socket.agentAddress` プロパティおよび `server.http.socket.bindAddress` プロパティ※に複数搭載されているネットワークインターフェースカードのいずれかの IP アドレスを指定しておく必要があります。この設定を行わないと，ホストを正常に追加できない場合があります。

  ホスト名を指定してホストを追加する場合には，ホスト名から `server.http.socket.agentAddress` プロパティおよび

server.http.socket.bindAddress プロパティで指定した IP アドレスに名前解決ができるようにネットワークを設定しておく必要があります。

注※

server.properties ファイルの server.http.socket.agentAddress プロパティおよび server.http.socket.bindAddress プロパティについては，「付録 A. 共通エージェントコンポーネントの設定」を参照してください。

IPv4 と IPv6 のアドレスが有効になっているホストの場合，IPv6 アドレスでホストを追加しても，IPv4 アドレスでホスト情報が追加されることがあります。この現象を回避するには，server.properties ファイルで，
server.http.socket.agentAddress プロパティおよび
server.http.socket.bindAddress プロパティに IPv6 アドレスを指定してください。

- ホストの IP アドレスには，静的なアドレスを設定しておく必要があります。DHCP は使用しないでください。
- HDLM をインストールする前に，インストールするマシンのローカル時間は現在の日時を設定しておいてください。現在の日時に設定していない場合，HDLM を使用しているホストから，パス稼働情報（パスステータスログ）が正しく取得されないおそれがあります。

(1) HDLM の要件

HDLM の要件については，HDLM のマニュアルを参照してください。VMware 版の HDLM を使用している場合は，リモート管理クライアントも必要になります。リモート管理クライアントについては，VMware 版の HDLM のマニュアルを参照してください。

HDLM のインストールおよび環境設定については，HDLM のマニュアルおよびこのマニュアルの「付録 A. 共通エージェントコンポーネントの設定」を参照してください。

注意事項

HDLM のバージョンが 6.0 より前の場合は，Global Link Manager と IPv6 で接続できません。IPv6 の設定が有効になっている場合，ホストの IPv6 の設定を無効にしてください。IPv6 の設定が有効になっていると，共通エージェントコンポーネントのサービスは起動できません。

1.4 IPv6 環境での運用

Global Link Manager は IPv6 環境をサポートしています。Global Link Manager が IPv6 環境での動作をサポートする OS については，「1.3 Global Link Manager のシステム要件」を参照してください。

1.4.1 IPv6 環境で運用するための制限事項

Global Link Manager を IPv6 環境で使用する場合，次に示す制限事項があります。

- IPv6 だけの環境をサポートしていません。IPv4 と IPv6 の両方で使用できるよう OS を設定してください。
- 使用できる IPv6 アドレスはグローバルアドレスだけです。グローバルユニークローカルアドレス（サイトローカルアドレス）やリンクローカルアドレスは使用できません。
- Global Link Manager サーバの IP アドレスまたはホスト名を指定する場合は，ホスト名で指定することを推奨します。IPv6 アドレスを指定した場合，画面遷移ができないことがあります。

- Global Link Manager GUI のホスト一覧は，IP アドレスごとに管理されています。このため，IPv4 および IPv6 の IP アドレスを両方持つホストの場合は，2 つのホストとして登録されます。IPv6 環境へ移行した際は，手動で IPv4 アドレスをホスト一覧から削除してください。Global Link Manager GUI のホスト一覧については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。
- ホストのパス稼働情報（パスステータスログ）は IP アドレスごとに管理されるため，ホストとの通信処理を IPv4 から IPv6 へ変更しても IPv6 アドレスへ移行されません。

1.4.2 IPv6 環境で運用するための設定項目

IPv4 環境で運用していた Global Link Manager を IPv6 環境で運用する場合，user_httpsd.conf ファイルを編集します。user_httpsd.conf ファイルの格納先を次に示します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥httpsd¥conf¥user_httpsd.conf

注意事項

Global Link Manager および Hitachi Command Suite 共通コンポーネントを停止してから，user_httpsd.conf ファイルを編集してください。編集が終わったら，変更内容を有効にするために，Global Link Manager および Hitachi Command Suite 共通コンポーネントを開始してください。

管理ホストと IPv6 で SNMP Trap 通信する場合，server.properties ファイルの設定をする必要があります。プロパティファイルの設定方法については，「3.5 Global Link Manager の環境設定の変更」を参照してください。

参考

Global Link Manager を IPv6 が有効になっている環境に新規インストールした場合，下記の内容はインストーラーが自動的に設定します。

(1) IPv6 用の設定

「Listen [::]:22015」（デフォルト時）行の先頭から番号記号（#）を削除します。ポート番号は IPv4 の Listen 行と同じ番号を指定してください。ポート番号のデフォルトは 22015 です。

設定例を次に示します。

```
Listen [::]:22015
Listen 22015
```

注意事項

既存の Listen 行を削除したり編集したりしないでください。誤って変更，削除した場合，IPv4 での通信ができなくなります。

(2) SSL 通信をする場合の設定

「Listen [::]:22016」（デフォルト時）行の先頭から番号記号（#）を削除します。ポート番号は IPv4 の Listen 行と同じ番号を指定してください。SSL 通信のポート番号のデフォルトは 22016 です。SSL 通信時の設定については，「5. 通信に関するセキュリティの設定」を参照してください。

設定例を次に示します。

```
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
```

注意事項

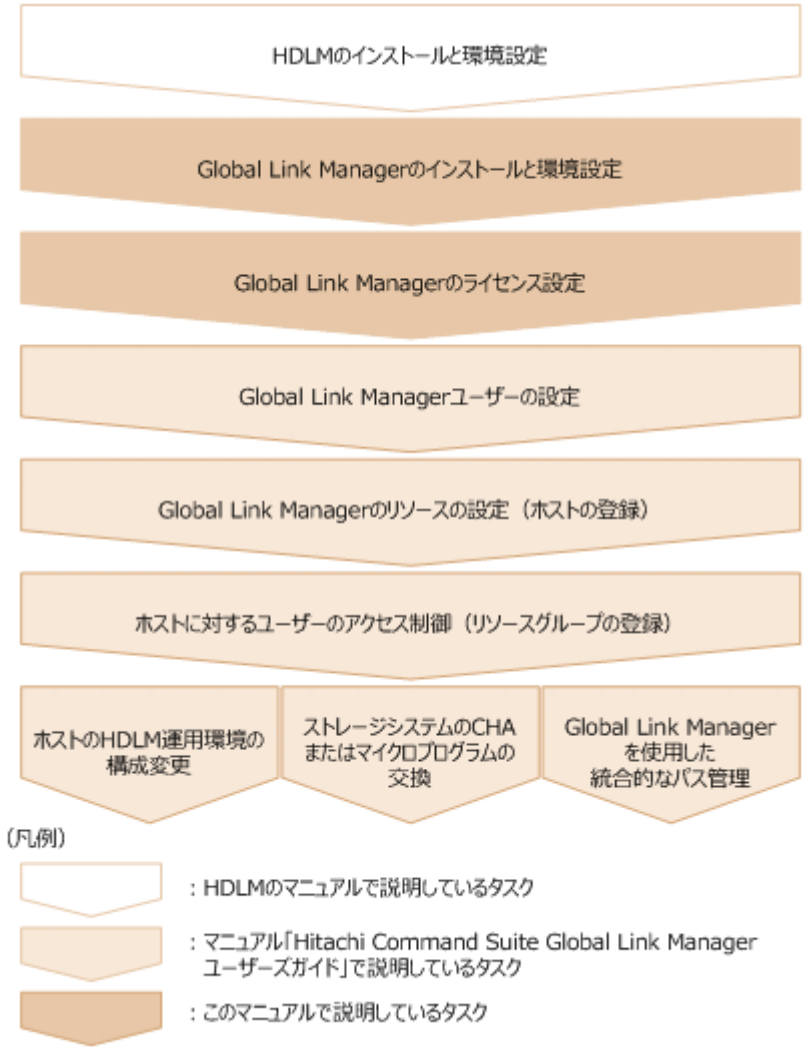
既存の Listen 行を削除したり編集したりしないでください。誤って変更，削除した場合，IPv4 での通信ができなくなります。

1.5 Global Link Manager を運用するために

ここでは，セットアップから運用までの全体の流れについて説明します。また，運用を開始するために必要な設定，Global Link Manager へのログイン手順などについて説明します。

Global Link Manager を運用するために行うタスクの流れを次の図に示します。

図 1-3 Global Link Manager のタスクフロー



HDLM のインストールと環境設定

Global Link Manager で統合して管理する各ホストで，HDLM をセットアップします。ホストにインストールする HDLM の要件については，「1.3.3 ホストの要件」を参照してください。各ホストでの HDLM のインストールおよび環境設定の手順については，HDLM のマニュアルを参照してください。

HDLM を Global Link Manager で管理するには，HDLM のセットアップ後に共通エージェントコンポーネントを使用するための設定が必要です。設定方法については，「付録 A. 共通エージェントコンポーネントの設定」を参照してください。

Global Link Manager のインストールと環境設定

Global Link Manager をセットアップし，Global Link Manager サーバを起動します。インストールおよび Global Link Manager サーバの環境設定については，サーバの環境に合わせて「2. Global Link Manager のインストール」から「6. ほかの製品と連携するための Global Link Manager の設定」を参照してください。

Global Link Manager のライセンス設定

Global Link Manager のセットアップ後に，Global Link Manager GUI でライセンスの初期設定を行います。ライセンスの設定方法については，「2.2 ライセンスの初期設定」を参照してください。

そのほかのタスクでの操作の流れ，各機能の説明，および手順については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

1.6 Global Link Manager をインストールした場合に必要な設定

ここでは，Global Link Manager をインストールした場合に必要な設定について説明します。

1.6.1 ウィルス検出プログラムを使用する場合に必要な設定

ウィルス検出プログラムで Hitachi Command Suite 製品が使用するデータベース関連のファイルにアクセスを行うと，I/O 遅延やファイル排他などによって障害が発生することがあります。

障害を防止するため，Hitachi Command Suite 製品の稼働中は，ウィルス検出プログラムのスキャン対象から，次のディレクトリを除外してください。

- *<Hitachi Command Suite 製品のインストール先フォルダ>*¥Base64¥HDB
- *<Hitachi Command Suite 製品のインストール先フォルダ>*¥HGLAM¥database※

注※

データベースフォルダは任意に指定できます。例として，デフォルトインストール先で説明しています。

1.6.2 バックアップソフトウェアを使用する場合の注意事項

バックアップソフトウェアで Hitachi Command Suite 製品が使用するデータベース関連のファイルにアクセスを行うと，I/O 遅延やファイル排他などによって障害が発生することがあります。

バックアップソフトウェアで*<Hitachi Command Suite 製品のインストール先ディレクトリ>*を含む領域をバックアップしたい場合は，Hitachi Command Suite 製品のすべてのサービスを停止したあとに，バックアップを実施してください。

2

Global Link Manager のインストール

この章では，Global Link Manager のインストールについて説明します。クラスタ環境にインストールする場合は「4. クラスタ環境での Global Link Manager のインストール」をあわせて参照してください。

2.1 Global Link Manager のインストールの種類

この節では Global Link Manager サーバのインストールについて説明します。インストールには次の種類があります。

- 新規インストール※
- 再インストール※
- アップグレードインストール※
- アンインストール

注※

サイレントインストールでインストールすることもできます。サイレントインストールとは，Global Link Manager のインストール時に，応答処理を省略できるインストール方法です。

「2.1.1 Global Link Manager のインストールの準備」を実施したあと，それぞれのインストール手順に従ってください。

なお，Global Link Manager v8.2.1 以降をインストールするマシンの Hitachi Command Suite 製品のバージョンは，v8.2.1 以降にしてください。

注意事項

新規インストール，またはアップグレードインストールする場合の注意事項を次に示します。

- バージョンが 8.2.1 未満の Global Link Manager は，最新バージョンにアップグレードインストールできません。いったんバージョン 8.2.1～8.8.0 にアップグレードインストールしてから，最新バージョンに再度アップグレードインストールしてください。
- OS をアップグレードする場合，OS をアップグレードする前に Hitachi Command Suite をアンインストールしてください。例えば，Windows Server 2012 から Windows Server 2012 R2 にアップグレードする場合も，Hitachi Command Suite をいったんアンインストールする必要があります。

  OS をアップグレードしたあと，アップグレードした OS に対応する Hitachi Command Suite を新規インストールして，Hitachi Command Suite のデータベースを移行してください。
- バージョンが v8 より前の Global Link Manager を v8 以降にアップグレードインストールする場合は，32 ビットのプログラムを 64 ビットのプログラムにデータ移行するため，データが退避されます。退避されたデータは，Global Link Manager 以外の製品でも使用するため，次の製品をすべて v8 以降にアップグレードするまで削除しないでください。

  - Device Manager
  - Tiered Storage Manager
  - Replication Manager
  - Tuning Manager
  - Compute Systems Manager

  すべて v8 以降にアップグレードしたあとは，退避されたデータを削除しても問題ありません。
- バージョンが v8 より前の Global Link Manager を v8 以降にアップグレードインストールする場合は，Windows の［サービス］ウィンドウに次に示すサービスがある場合，そのサービスが起動していることを確認し，起動していない場合は起動してください。

  - HiRDB/EmbeddedEdition _HD0
  - HiRDB/EmbeddedEdition _HD1

- v8.7.1 以前の Global Link Manager をインストールすると，Microsoft Visual C++ 2008 再頒布可能パッケージ（Microsoft Visual C++ 2008 Redistributable Package (x86)および Microsoft Visual C++ 2008 Redistributable Package (x64)）が一緒にインストールされます。
- v8.7.2 以降の Global Link Manager をインストールすると，Microsoft Visual C++ 2013 再頒布可能パッケージ（Microsoft Visual C++ 2013 Redistributable Package (x86)および Microsoft Visual C++ 2013 Redistributable Package (x64)）が一緒にインストールされます。
- v8.8.3 以降の Global Link Manager をインストールすると，Microsoft Visual C++ 2015 再頒布可能パッケージ（Microsoft Visual C++ 2015 Redistributable Package (x86)および Microsoft Visual C++ 2015 Redistributable Package (x64)）が一緒にインストールされます。

参考：

- Global Link Manager では修正プログラム（サービスパック）が提供されることがあります。サービスパックのインストールについては，サービスパックと一緒に提供されるドキュメントを参照してください。
- ダウングレードインストール（バージョンをさかのぼるインストール）はできません。

注意事項

アンインストールする場合の注意事項を次に示します。

- Global Link Manager のアンインストール時に，Microsoft Visual C++ 2008 再頒布可能パッケージ（Microsoft Visual C++ 2008 Redistributable Package (x86)および Microsoft Visual C++ 2008 Redistributable Package (x64)）は，アンインストールされません。 ほかの製品が Microsoft Visual C++ 2008 再頒布可能パッケージを使用していない場合は, コントロールパネルの［プログラムと機能］からアンインストールすることができます。
- Global Link Manager のアンインストール時に，Microsoft Visual C++ 2013 再頒布可能パッケージ（Microsoft Visual C++ 2013 Redistributable Package (x86)および Microsoft Visual C++ 2013 Redistributable Package (x64)）は，アンインストールされません。 ほかの製品が Microsoft Visual C++ 2013 再頒布可能パッケージを使用していない場合は, コントロールパネルの［プログラムと機能］からアンインストールすることができます。
- Global Link Manager のアンインストール時に，Microsoft Visual C++ 2015 再頒布可能パッケージ（Microsoft Visual C++ 2015 Redistributable Package (x86)および Microsoft Visual C++ 2015 Redistributable Package (x64)）は，アンインストールされません。 ほかの製品が Microsoft Visual C++ 2015 再頒布可能パッケージを使用していない場合は, コントロールパネルの［プログラムと機能］からアンインストールすることができます。

2.1.1 Global Link Manager のインストールの準備

インストールする前には，Global Link Manager をインストールするサーバで次のことを確認してください。

- Administrator または Administrators グループのユーザーで Windows にログオンしていること
- 次のプログラムがインストールされていないこと
  - v8.0 より前のバージョンの Device Manager および Tuning Manager
  - HiRDB 製品（HiRDB/Single Server，HiRDB/Parallel Server，HiRDB/Workgroup Server，HiRDB/Run Time，HiRDB/Developer's Kit，HiRDB SQL Executer）
- ポート番号 22620 をほかの製品が使用していないこと

Global Link Manager では，SNMP Trap を受信するポート番号のデフォルト値を 22620 に設定しています。ほかの製品でこのポート番号を使用している場合，Global Link Manager のインストール時にほかのポート番号を指定してください。ほかの製品とポート番号が重複した場合，Global Link Manager のインストールが正常終了しても，Global Link Manager を開始できなくなります。この場合は，プロパティファイル（server.properties）で，SNMP Trap 受信機能を無効にするか，ポート番号の設定を変更する必要があります。プロパティファイルの設定方法については，「3.5 Global Link Manager の環境設定の変更」を参照してください。

- ポート番号 22015，22016，22031，22032，22035，22036，22037，22038，22125，22126，22127，および 22128 を Hitachi Command Suite 製品以外の製品が使用していないこと

  ほかの製品がこれらのポート番号を使用している場合，Global Link Manager のインストールが正常終了しても，Global Link Manager を開始できなくなります。これらのポートを使用している製品がないことを確認してから，インストールを開始してください。これらのポート番号は，インストール後に変更できます。ポート番号の変更方法については「3.7 Hitachi Command Suite 共通コンポーネントのポート番号の変更」を参照してください。すでに Hitachi Command Suite 共通コンポーネントがインストールされた環境で，これらのポート番号を変更して運用している場合は，そのポート番号を利用してインストールできます。デフォルトのポート番号に戻す必要はありません。

- ファイアウォールの設定が，ローカルホスト内のソケット通信を遮断しないよう設定されていること

  OS にバンドルされているファイアウォール機能の中には，ローカルホスト内のソケット通信も遮断するものがあります。ローカルホスト内のソケット通信が遮断される環境では，Hitachi Command Suite 製品のインストールおよび運用ができません。OS が提供しているファイアウォールを設定する場合，ローカルホスト内のソケット通信を遮断しないように設定してください。

- セキュリティ監視プログラムまたはウィルス検出プログラムのインストールの有無

  セキュリティ監視プログラムまたはウィルス検出プログラムがインストールされている場合，停止しておいてください。

- プロセス監視プログラムのインストールの有無

  プロセス監視プログラムがインストールされている場合，停止するか，または設定を変更して，Hitachi Command Suite 共通コンポーネントおよび Hitachi Command Suite 製品のサービス（プロセス）を監視しないようにしてください。

- リモートデスクトップ機能を使用する場合，コンソールセッションに接続していること

  Windows 版の Hitachi Command Suite 製品は，Windows のリモートデスクトップ機能をサポートしています。リモートデスクトップ機能にはご使用の OS によって次の呼び方があります。

  - 管理用リモートデスクトップ
  - リモートデスクトップ接続

  Hitachi Command Suite 製品を操作（インストールおよびアンインストールを含む）する場合にリモートデスクトップ機能を使用するとき，接続先サーバのコンソールセッションに接続する必要があります。ただし，コンソールセッションに接続しても，接続中に別のユーザーがコンソールセッションに接続すると，製品が正しく動作しなくなるおそれがあります。

- Windows のサービスを操作するウィンドウを表示していないこと（コンピュータの管理，サービスなど）

- すでに Hitachi Command Suite 製品がインストールされている場合，HiRDB/EmbeddedEdition _HD1 が起動していること

  Hitachi Command Suite 製品は常に HiRDB/EmbeddedEdition _HD1 が起動している必要があります。［サービス］ウィンドウの一覧にある HiRDB/EmbeddedEdition _HD1 が起動してい

ることを確認してください。停止していた場合は，HiRDB/EmbeddedEdition _HD1 を起動してください。

- インストールするマシンのローカル時間は，現在の日時を設定しておくこと

注意事項

- Global Link Manager をインストールするマシンに，ほかの Hitachi Command Suite 製品がインストールされている場合は，Global Link Manager をインストールする前に，Hitachi Command Suite 製品のデータベースのバックアップを取っておいてください。データベースをバックアップする方法は「3.4.1 Global Link Manager のデータベースのバックアップ」を参照してください。
- Hitachi Command Suite 共通コンポーネントがドライブ直下（C:¥，D:¥など）にインストールされている場合，Global Link Manager はインストールできません。
- バージョンが 6.3 未満の Tuning Manager - Agent for SAN Switch がインストールされているマシンに Global Link Manager をインストールする場合は，事前に必ず Tuning Manager - Agent for SAN Switch のサービスを停止してください。Tuning Manager - Agent for SAN Switch のサービスを停止するコマンドを次に示します。

  ＜*Tuning Manager - Agent for SAN Switch のインストールフォルダ*＞¥tools¥jpcstop agtw

  Hitachi Command Suite 製品のサービスを停止するコマンド（hcmds64srv /stop コマンド）を実行しても Tuning Manager - Agent for SAN Switch のサービスは停止しません。

データ実行防止機能を使用している場合は，次の設定が必要になります。

データ実行防止機能を有効にしているときの設定

データ実行防止機能（DEP：Data Execution Prevention）を有効にしている場合，インストールが開始できないことがあります。次の手順でデータ実行防止機能を解除したあと，再度インストールを実行してください。

1. ［スタート］－［コントロールパネル］－［システム］を選択します。
   システムのプロパティダイアログが表示されます。
2. ［詳細設定］タブの［パフォーマンス］の［設定］ボタンをクリックします。
   パフォーマンス オプションダイアログが表示されます。
3. ［データ実行防止］タブで［次に選択するものを除くすべてのプログラムおよびサービスについて DEP を有効にする］ラジオボタンを選択します。
4. ［追加］ボタンをクリックし，Global Link Manager のインストーラー（setup.exe）を指定します。
   リストに Global Link Manager のインストーラー（setup.exe）が追加されます。
5. Global Link Manager のインストーラー（setup.exe）の横のチェックボックスをオンにして，［OK］ボタンをクリックします。

2.1.2 Global Link Manager の新規インストール

新規インストールでは，次の項目をインストール時に設定します。事前に確認しておいてください。

表 2-1 インストール前に確認しておく項目

項目	説明
サーバの IP アドレスまたはホスト名	Global Link Manager にログインするための URL を設定するために必要な情報です。Global Link Manager をインストールするサーバの IP

項目	説明
HBase 64 Storage Mgmt Web Service のポート番号	アドレスまたはホスト名，および HBase 64 Storage Mgmt Web Service のポート番号を確認しておいてください。ポート番号のデフォルト値は 22015 です。すでにほかの Hitachi Command Suite 製品がインストールされている場合，入力は不要です。
SNMP Trap 受信機能を使用するかどうか	ホストのパスに障害が発生した場合に，障害情報を SNMP Trap を使用して Global Link Manager に通知する機能を使用するかどうかをあらかじめ決めておきます。
SNMP Trap を受信する IP アドレス	SNMP Trap 受信機能を使用する場合，SNMP Trap の通知先の IP アドレスを確認しておきます。IP アドレスのデフォルトは Global Link Manager サーバの IP アドレスです。
SNMP Trap を受信するポート番号	SNMP Trap 受信機能を使用する場合，SNMP Trap が使用する専用のポート番号を確認しておきます。ポート番号のデフォルト値は 22620 です。ほかのプログラムでポート番号に 22620 を使用している場合は，22620 以外を使用してください。

新規インストールの手順は次のとおりです。

1. Global Link Manager のインストール DVD-ROM をセットします。

   インストーラー（setup.exe）を直接実行してください。

   インストーラーは，*＜インストール DVD-ROM をセットしたドライブ＞*:¥HGLM に格納されています。

   インストーラーが起動すると，Microsoft Visual C++ 2015 再頒布可能パッケージ（Microsoft Visual C++ 2015 Redistributable Package (x86)および Microsoft Visual C++ 2015 Redistributable Package (x64)）が自動的にインストールされます。

   - 再頒布可能パッケージのインストールが完了した時点で再起動を要求される場合があります。その場合は，再起動後に Global Link Manager のインストールが開始されます。
   - インストール先の環境に，すでに同じバージョン以上の Microsoft Visual C++ 2015 再頒布可能パッケージがインストールされている場合，この処理はスキップされます。

   この処理が完了すると，Hitachi Global Link Manager のインストールへようこそ（新規）ダイアログが表示されます。

2. ［次へ］ボタンをクリックします。

   Dynamic Link Manager インストーラーダウンロード機能ダイアログが表示されます。

   HDLM インストーラーのダウンロード機能を有効にする場合は，チェックボックスをオンにします。ダウンロード機能を有効にすると，HDLM インストーラーのファイルが Global Link Manager サーバに格納され，クライアントの Web ブラウザーからダウンロードできるようになります。

3. ［次へ］ボタンをクリックします。

   ほかの Hitachi Command Suite 製品がインストールされている場合で，Hitachi Command Suite 共通コンポーネントまたはほかの Hitachi Command Suite 製品のサービスが起動しているときは，Hitachi Command Suite 製品のサービスの停止ダイアログが表示されます。［次へ］ボタンをクリックすると，Hitachi Command Suite 共通コンポーネントおよびほかの Hitachi Command Suite 製品のサービスが停止されます。

4. ［次へ］ボタンをクリックします。

   インストールフォルダの設定ダイアログが表示されます。

   デフォルトとは別のフォルダにインストールする場合は，インストール先のフォルダを指定します。インストール先のフォルダを指定するときは，次の規則に従ってください。

   - インストールフォルダとして，ドライブ直下（C:¥，D:¥など）を指定しないでください。
   - 62 バイト以下の絶対パスで指定します。

- 次の半角文字で指定します。

  A～Z a～z 0～9 . _ スペース

  ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

  また，スペースを 2 文字以上続けて指定できません。

- OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1～COM9，LPT1～LPT9）を含まないように指定します。

なお，次のフォルダにはインストールできません。

- %ProgramFiles(x86)%¥以下
- %CommonProgramFiles(x86)%¥以下
- %SystemRoot%¥SysWOW64¥以下
- %SystemRoot%¥system32¥以下
- %ProgramFiles%¥WindowsApps¥以下

Global Link Manager のデフォルトのインストールフォルダは，次のとおりです。

＜システムドライブ＞:¥Program Files¥HiCommand

Hitachi Command Suite 共通コンポーネントのデフォルトのインストールフォルダは，次のとおりです。

＜システムドライブ＞:¥Program Files¥HiCommand¥Base64

ほかの Hitachi Command Suite 製品がインストールされていないサーバに Global Link Manager をインストールする場合，Global Link Manager と Hitachi Command Suite 共通コンポーネントはインストールフォルダの設定ダイアログで設定したフォルダにインストールされます。すでにほかの Hitachi Command Suite 製品がインストールされているサーバに Global Link Manager をインストールする場合，Global Link Manager はインストールフォルダの設定ダイアログで設定したフォルダにインストールされますが，Hitachi Command Suite 共通コンポーネントは，すでにインストールされているフォルダに上書きされます。Hitachi Command Suite 共通コンポーネントのインストールフォルダを確認する場合は，次のレジストリーキーを確認してください。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi¥HiCommand Base 64¥InstallPath

5. ［次へ］ボタンをクリックします。

Hitachi Global Link Manager のデータベースファイル格納先の設定ダイアログが表示されます。

デフォルトとは別のフォルダに格納する場合は，格納先のフォルダを指定します。格納先のフォルダを指定するときは，次の規則に従ってください。

- データベースファイル格納先フォルダとして，ドライブ直下（C:¥，D:¥など）を指定しないでください。
- 62 バイト以下の絶対パスで指定します。
- 次の半角文字で指定します。

  A～Z a～z 0～9 . _ スペース

  ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

  また，スペースを 2 文字以上続けて指定できません。

- OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1～COM9，LPT1～LPT9）を含まないように指定します。

なお，次のフォルダにはインストールできません。

- %ProgramFiles(x86)%¥以下
- %CommonProgramFiles(x86)%¥以下

- %SystemRoot%¥SysWOW64¥以下
- %SystemRoot%¥system32¥以下
- %ProgramFiles%¥WindowsApps¥以下

注意事項

- Hitachi Global Link Manager のデータベースファイルは，"*<指定した格納先>*¥x64"フォルダ以下に作成されます。

6. ［次へ］ボタンをクリックします。

32 ビット版の Hitachi Command Suite 共通コンポーネントが存在する環境に，このインストールによって，64 ビット版 Hitachi Command Suite 共通コンポーネントが初めてインストールされる場合，データベース退避先設定ダイアログが表示されます。

Hitachi Command Suite 製品を v7 以前から v8 へアップグレードするために，Hitachi Command Suite 製品のデータベースファイルの退避先を指定してください。デフォルトとは別のフォルダを指定する場合，次の規則に従ってください。

- 148 バイト以下の絶対パスで指定します。
- 次の半角文字で指定します。

  A～Z a～z 0～9 ． _ スペース

  ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

  また，スペースを 2 文字以上続けて指定できません。
- OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1～COM9，LPT1～LPT9）を含まないように指定します。

Hitachi Command Suite 製品のデフォルトのデータベース退避先は，次のとおりです。

<指定した Global Link Manager のインストール先フォルダ>¥databackup

7. ［次へ］ボタンをクリックします。

Hitachi Global Link Manager サーバ情報の設定ダイアログが表示されます。

あらかじめ確認しておいた次の情報を指定します。

- サーバの IP アドレスまたはホスト名
- HBase 64 Storage Mgmt Web Service のポート番号
- SNMP Trap 受信機能（［有効にする］または［有効にしない］）

ほかの Hitachi Command Suite 製品がインストールされていない環境に Global Link Manager をインストールする場合，サーバの IP アドレスまたはホスト名には，自動検出された IP アドレスが入力されています。空欄の場合は，サーバの IP アドレスまたはホスト名を入力してください。IPv6 アドレスを指定する場合は，入力する IP アドレスを[ ]で囲んでください。

すでにほかの Hitachi Command Suite 製品がインストールされている場合，次の情報は非活性になります。

- サーバの IP アドレスまたはホスト名
- HBase 64 Storage Mgmt Web Service のポート番号

注意事項

- ネットワーク環境によっては，複数の IP アドレスを持っていることがあり，その場合には，最初に検出された IP アドレスが入力されています。検出された IP アドレスが正しいかどうか確認してください。
- ホスト名は 128 バイト以内である必要があります。また，使用できる文字は次のとおりです。

  A～Z a～z 0～9 ． -

ただし，ホスト名の先頭と末尾にはハイフン（-）は使用できません。

8. ［次へ］ボタンをクリックします。

   SNMP Trap 受信機能で［有効にする］を選んだ場合，Hitachi Global Link Manager SNMP Trap 接続情報の設定ダイアログが表示されます。［有効にしない］を選んだ場合は，手順 9 へ進んでください。

   あらかじめ確認しておいた次の情報を指定します。

   - SNMP Trap を受信する IP アドレス（IPv4 アドレスまたは IPv6 アドレス）
   - SNMP Trap を受信するポート番号

   SNMP Trap を受信する IP アドレスには，Global Link Manager サーバの IP アドレスが入力されています。空欄の場合は，サーバの IP アドレスを入力してください。

   IPv6 アドレスを指定する場合は，入力する IP アドレスを[ ]で囲んでください。

   注意事項

   Device Manager がインストールされているサーバに Global Link Manager をインストールする場合，SNMP Trap を受信するポート番号は，162 以外の番号を指定してください。Device Manager で SNMP Trap 受信機能を使用している場合に，Global Link Manager のインストール時に SNMP Trap を受信するポート番号に 162 を指定すると，Device Manager を起動できなくなります。

9. ［次へ］ボタンをクリックします。

   Windows ファイアウォール機能がインストールされている場合, Windows ファイアウォール例外登録ダイアログが表示されます。ダイアログの内容を確認して，［次へ］ボタンをクリックしてください。Hitachi Command Suite 共通コンポーネントおよび SNMP Trap を受信するポート番号が，Windows ファイアウォールの例外として登録されます。

   注意事項

   Windows ファイアウォールの例外登録を実行することで，インストールの時間は約 15 分多く掛かることがあります。Global Link Manager のインストール後にファイアウォールを有効にした場合は，手動で例外に登録する必要があります。手動で例外に登録する方法は，「3.9.2 Windows ファイアウォールを有効にした場合の設定」を参照してください。

10. インストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを選択します。

    インストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを確認するダイアログが表示されます。インストール後にライセンスキーを入力する場合，［はい］ボタンをクリックすることをお勧めします。

    ［はい］または［いいえ］ボタンをクリックすると，インストール前の確認ダイアログが表示されます。

11. インストール情報を確認し，［インストール］ボタンをクリックします。

    インストール処理が開始され，途中の処理状況を示す幾つかのダイアログが表示されます。HGLM 設定の完了ダイアログが表示されたら，インストールで設定した情報を確認してください。

    HGLM ログイン画面 URL に設定されている値が，Global Link Manager をインストールしたサーバの情報と異なる場合，次を参照し，変更してください。

    - IP アドレスの変更：「3.8.1 Global Link Manager にログインするための URL の変更」
    - ホスト名の変更：「3.6.2 Global Link Manager サーバのホスト名の変更」
    - HBase 64 Storage Mgmt Web Service のポート番号の変更：「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」

12. ［次へ］ボタンをクリックします。

    正常にインストールが完了した場合は，インストールの完了ダイアログが表示されます。

13. ［完了］ボタンをクリックして，インストールを完了します。

Hitachi Command Suite 共通コンポーネントのサービスの稼働状態は，インストールで設定した状態に応じて異なります。

Global Link Manager にログインして運用を開始するには，ライセンスの初期設定が必要です。「2.2 ライセンスの初期設定」を参照してください。

パス稼働情報のレポート出力を使用する場合

HDLM のバージョンが 5.9 以降のホストを対象に，パスの稼働実績に関する情報をレポートで出力できます。パス稼働情報のレポート出力機能を使用するには，プロパティファイル（server.properties）の server.pathreport.enable を変更する必要があります。プロパティファイルの設定方法については，「3.5 Global Link Manager の環境設定の変更」を参照してください。

2.1.3 Global Link Manager の再インストール

インストールした Global Link Manager のファイルが破損した場合，すでにインストールされているバージョンと同じバージョンの Global Link Manager を上書きでインストール（再インストール）することで，破損したデータを修復できます。

再インストールする前には，インストールの準備が整っていることを確認してください。インストールの準備が整っているかどうかを確認するには，「2.1.1 Global Link Manager のインストールの準備」を参照してください。

再インストールの手順は次のとおりです。

1. Global Link Manager のインストール DVD-ROM をセットします。

   インストーラー（setup.exe）を直接実行してください。

   インストーラーは，＜*インストール DVD-ROM をセットしたドライブ*＞:¥HGLM に格納されています。

   インストーラーが起動すると，Microsoft Visual C++ 2015 再頒布可能パッケージ（Microsoft Visual C++ 2015 Redistributable Package (x86)および Microsoft Visual C++ 2015 Redistributable Package (x64)）が自動的にインストールされます。

   - 再頒布可能パッケージのインストールが完了した時点で再起動を要求される場合があります。その場合は，再起動後に Global Link Manager のインストールが開始されます。
   - インストール先の環境に，すでに同じバージョン以上の Microsoft Visual C++ 2015 再頒布可能パッケージがインストールされている場合，この処理はスキップされます。

   この処理が完了すると，Hitachi Global Link Manager のインストールへようこそ（上書き）ダイアログが表示されます。

2. ［次へ］ボタンをクリックします。

   Dynamic Link Manager インストーラーダウンロード機能ダイアログが表示されます。

   HDLM インストーラーのダウンロード機能を有効にする場合は，チェックボックスをオンにします。ダウンロード機能を有効にすると，HDLM インストーラーのファイルが Global Link Manager サーバに格納され，クライアントの Web ブラウザーからダウンロードできるようになります。

   すでにダウンロード機能を有効にしてインストール済みの場合は，このダイアログは表示されません。

3. ［次へ］ボタンをクリックします。

   Hitachi Command Suite 共通コンポーネントまたはほかの Hitachi Command Suite 製品のサービスが起動しているときは，次の画面が表示されます。

- Hitachi Command Suite 製品のサービスの停止ダイアログが表示されます。［次へ］ボタンをクリックすると，Hitachi Command Suite 共通コンポーネントおよびほかの Hitachi Command Suite 製品のサービスが停止されます。

4. ［次へ］ボタンをクリックします。

   Windows ファイアウォール機能がインストールされている場合，Windows ファイアウォール例外登録ダイアログが表示されます。ダイアログの内容を確認して，［次へ］ボタンをクリックしてください。Hitachi Command Suite 共通コンポーネントおよび SNMP Trap を受信するポート番号が，Windows ファイアウォールの例外として登録されます。

   注意事項

   Windows ファイアウォールの例外登録を実行することで，インストールの時間は約 15 分多く掛かることがあります。Global Link Manager のインストール後にファイアウォールを有効にした場合は，手動で例外に登録する必要があります。手動で例外に登録する方法は，「3.9.2 Windows ファイアウォールを有効にした場合の設定」を参照してください。

5. インストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを選択します。

   インストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを確認するダイアログが表示されます。

   - インストール後にサービスを起動するかどうかを選択します（任意）。

   ［はい］または［いいえ］ボタンをクリックすると，インストール前の確認ダイアログが表示されます。

6. インストール情報を確認し，［インストール］ボタンをクリックします。

   インストール処理が開始され，途中の処理状況を示す幾つかのダイアログが表示されます。上書きインストールでは，Global Link Manager のデータベースは初期化されません（データベースファイルが壊れている場合を除く）。HGLM 設定の完了ダイアログが表示されたら，インストールで設定した情報を確認してください。

   HGLM ログイン画面 URL に設定されている値が，Global Link Manager をインストールしたサーバの情報と異なる場合，次を参照し，変更してください。

   - IP アドレスの変更：「3.8.1 Global Link Manager にログインするための URL の変更」
   - ホスト名の変更：「3.6.2 Global Link Manager サーバのホスト名の変更」
   - HBase 64 Storage Mgmt Web Service のポート番号の変更：「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」

7. ［次へ］ボタンをクリックします。

   正常にインストールが完了した場合は，インストールの完了ダイアログが表示されます。

8. ［完了］ボタンをクリックして，インストールを完了します。

   Hitachi Command Suite 共通コンポーネントのサービスの稼働状態は，インストールで設定した状態に応じて異なります。クラスタ構成で待機系ノードとしてインストールした場合は，サービスは開始されません。クラスタ構成で運用するための設定を続けてください。

2.1.4 Global Link Manager のアップグレードインストール

すでにインストールされている Global Link Manager のバージョンよりも新しいバージョンにしたい場合，アップグレードインストールを行います。

アップグレードインストールをする前には，インストールの準備が整っていることを確認してください。インストールの準備が整っているかどうかを確認するには，「2.1.1 Global Link Manager のインストールの準備」を参照してください。

注意事項

- Global Link Manager をアップグレードインストールする場合，ディスクの空き容量を十分に確保してください。データベースファイルの格納先のディスクに必要な空き容量は 4GB です。

アップグレードインストールについて，次の場合の手順を説明します。

同じバージョン間でアップグレードインストールする場合

同じバージョン間でアップグレードインストールする場合のアップグレードインストールの手順は次のとおりです。

1. Global Link Manager のインストール DVD-ROM をセットします。

   インストーラー（setup.exe）を直接実行してください。

   インストーラーは，*＜インストール DVD-ROM をセットしたドライブ＞*:¥HGLM に格納されています。

   インストーラーが起動すると，Microsoft Visual C++ 2015 再頒布可能パッケージ（Microsoft Visual C++ 2015 Redistributable Package (x86)および Microsoft Visual C++ 2015 Redistributable Package (x64)）が自動的にインストールされます。

   - 再頒布可能パッケージのインストールが完了した時点で再起動を要求される場合があります。その場合は，再起動後に Global Link Manager のインストールが開始されます。
   - インストール先の環境に，すでに同じバージョン以上の Microsoft Visual C++ 2015 再頒布可能パッケージがインストールされている場合，この処理はスキップされます。

   この処理が完了すると，Hitachi Global Link Manager のインストールへようこそ（アップグレード）ダイアログが表示されます。

2. ［次へ］ボタンをクリックします。

   Dynamic Link Manager インストーラーダウンロード機能ダイアログが表示されます。

   HDLM インストーラーのダウンロード機能を有効にする場合は，チェックボックスをオンにします。ダウンロード機能を有効にすると，HDLM インストーラーのファイルが Global Link Manager サーバに格納され，クライアントの Web ブラウザーからダウンロードできるようになります。

   すでにダウンロード機能を有効にしてインストール済みの場合は，このダイアログは表示されません。

3. ［次へ］ボタンをクリックします。

   Hitachi Command Suite 共通コンポーネントまたはほかの Hitachi Command Suite 製品のサービスが起動しているときは，次の画面が表示されます。

   - Hitachi Command Suite 製品のサービスの停止ダイアログが表示されます。［次へ］ボタンをクリックすると，Hitachi Command Suite 共通コンポーネントおよびほかの Hitachi Command Suite 製品のサービスが停止されます。

4. ［次へ］ボタンをクリックします。

   Windows ファイアウォール機能がインストールされている場合，Windows ファイアウォール例外登録ダイアログが表示されます。ダイアログの内容を確認して，［次へ］ボタンをクリックしてください。Hitachi Command Suite 共通コンポーネントおよび SNMP Trap を受信するポート番号が，Windows ファイアウォールの例外として登録されます。

   注意事項

   Windows ファイアウォールの例外登録を実行することで，インストールの時間は約 15 分多く掛かることがあります。Global Link Manager のインストール後にファイアウォールを有効にした場合は，手動で例外に登録する必要があります。手動で例外に登録する方法は，「3.9.2 Windows ファイアウォールを有効にした場合の設定」を参照してください。

5. インストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを選択します。

   インストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを確認するダイアログが表示されます。

   - インストール後にサービスを起動するかどうかを選択します（任意）。

   ［はい］または［いいえ］ボタンをクリックすると，インストール前の確認ダイアログが表示されます。

6. インストール情報を確認し，［インストール］ボタンをクリックします。

   インストール処理が開始され，途中の処理状況を示す幾つかのダイアログが表示されます。アップグレードインストールでは，Global Link Manager のデータベースは更新されます（データベースファイルが壊れている場合を除く）。HGLM 設定の完了ダイアログが表示されたら，インストールで設定した情報を確認してください。

   HGLM ログイン画面 URL に設定されている値が，Global Link Manager をインストールしたサーバの情報と異なる場合，次を参照し，変更してください。

   - IP アドレスの変更：「3.8.1 Global Link Manager にログインするための URL の変更」
   - ホスト名の変更：「3.6.2 Global Link Manager サーバのホスト名の変更」
   - HBase 64 Storage Mgmt Web Service のポート番号の変更：「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」

7. ［次へ］ボタンをクリックします。

   正常にインストールが完了した場合は，インストールの完了ダイアログが表示されます。

8. ［完了］ボタンをクリックして，インストールを完了します。

   Hitachi Command Suite 共通コンポーネントのサービスの稼働状態は，インストールで設定した状態に応じて異なります。クラスタ構成で待機系ノードとしてインストールした場合は，サービスは開始されません。クラスタ構成で運用するための設定を続けてください。

パス稼働情報のレポート出力を使用する場合

HDLM のバージョンが 5.9 以降のホストを対象に，パスの稼働実績に関する情報をレポートで出力できます。パス稼働情報のレポート出力機能を使用するには，プロパティファイル（server.properties）の server.pathreport.enable を変更する必要があります。プロパティファイルの設定方法については，「3.5 Global Link Manager の環境設定の変更」を参照してください。

データベースの更新に失敗した場合

メッセージ ID「KAIF40094-E」のデータベースの更新に失敗した旨のメッセージが表示された場合，手動でデータベースを更新する必要があります。

Global Link Manager のデータベースを更新する手順を次に示します。

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントが起動していることを確認します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /status

   Hitachi Command Suite 共通コンポーネントが起動している場合は，次のコマンドを実行してください。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. 次のコマンドを実行して，HiRDB を起動します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /start

3. 次のコマンドを実行して，データベースを更新します。
＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamdbupdate

実行を確認するメッセージが表示されます。実行する場合は，「Y」を入力します。
"Are you sure to execute the database update command? (Y/N)"

hglamdbupdate コマンドには，次の表に示すオプションを指定できます。

表 2-2 hglamdbupdate コマンドのオプション

項目	説明
-x	データベース更新時のメッセージやエラーメッセージを出力させないときに指定します。ただし，このオプションを指定しても，オプションエラーのメッセージは表示されます。
-f ＜*メッセージの出力ファイル*＞	データベース更新時のメッセージやエラーメッセージをファイルに記録するときに指定します。相対パス，絶対パスのどちらでも指定できます。255 バイト以内のパスを指定してください。使用できる文字を次に示します。 A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)が使用できます。
-s	実行を確認するメッセージを出力させないときに指定します。

4. 次のコマンドを実行して，HiRDB を停止します。
＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /stop

5. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを起動します。
＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start

2.1.5 Global Link Manager のサイレントインストール

サイレントインストールとは，Global Link Manager のインストール時に，応答処理を省略できるインストール方法です。応答内容をあらかじめインストール情報設定ファイルに定義しておきます。サイレントインストールの処理の流れを次に示します。

1. インストールに必要な情報を，インストール情報設定ファイルに定義します。定義を省略することもできます。インストール情報設定ファイルについては，「(2) インストール情報設定ファイルの定義内容」を参照してください。
2. インストールコマンド（installhglm）※でインストールを実行します。
3. 応答処理は，インストール情報設定ファイルの内容に従って自動的に行われます。
4. インストールが完了します。インストールの状況や結果について，ログが出力されます。

注※

UAC 機能をサポートしている Windows OS では，UAC 機能が有効になっている場合，コマンドの実行時に管理者権限への昇格が求められることがあります。管理者権限に昇格してコマンドを実行してください。

(1) サイレントインストール

サイレントインストールの手順は次のとおりです。

1. Global Link Manager のインストール DVD-ROM をセットします。

   インストーラー（setup.exe）を直接実行してください。

   インストーラーは，*＜インストール DVD-ROM をセットしたドライブ＞*:¥HGLM に格納されています。

   インストーラーが起動すると，Microsoft Visual C++ 2015 再頒布可能パッケージ（Microsoft Visual C++ 2015 Redistributable Package (x86)および Microsoft Visual C++ 2015 Redistributable Package (x64)）が自動的にインストールされます。

   - 再頒布可能パッケージのインストールが完了した時点で再起動を要求される場合があります。その場合は，再起動後に Global Link Manager のインストールが開始されます。
   - インストール先の環境に，すでに同じバージョン以上の Microsoft Visual C++ 2015 再頒布可能パッケージがインストールされている場合，この処理はスキップされます。

   この処理が完了すると，Hitachi Global Link Manager のインストールへようこそダイアログが表示されます。

2. ［キャンセル］ボタンをクリックします。

   キャンセルを問い合わせるダイアログが表示されます。

3. ［はい］ボタンをクリックします。

   ダイアログが閉じます。

4. 次のコマンドを実行して，サイレントインストールを実行します。

   ＜インストール DVD-ROM をセットしたドライブ＞:¥HGLM¥GLMTools¥installhglm [/f *＜インストール情報設定ファイル名＞*] [/s]

   installhglm コマンドには，次の表に示すオプションを指定できます。

表 2-3 installhglm コマンドのオプション

項目	説明
/f *＜インストール情報設定ファイル＞*	インストール情報設定ファイルを作成している場合，格納場所を指定します。相対パス，絶対パスのどちらでも指定できます。255 バイト以内のパスを指定してください。使用できる文字を次に示します。 A～Z，a～z，0～9，'.'，'_'，' '（半角スペース），そのほかにパスの区切り文字として(¥)，(:)が使用できます。 このオプションを指定しない場合，インストール情報設定ファイルのデフォルトの値が適用されます。 インストール情報設定ファイルについては，「(2)」を参照してください。
/s	実行を確認するメッセージを出力させないときに指定します。

   コマンドを実行すると，インストールが開始します。インストール中は，インストールの中断はできません。［Ctrl］+［C］などによって強制終了しないでください。

   インストールが正常終了すると，KAIF40111-I のメッセージが出力されます。KAIF40111-I のメッセージが出力されない場合は，出力されたメッセージに従って対処してください。

   また，インストールの結果がログファイル（installhglm_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss*.log※）にも出力されます。installhglm.log については，「(3) ログファイルについて」を参照してください。

   注※

   yyyy-*mm*-*dd*_*hh*-*mm*-*ss* は，年-月-日-時-分-秒を示します。

(2) インストール情報設定ファイルの定義内容

Global Link Manager では，インストール情報設定ファイルのサンプルファイルを提供しています。格納場所を次に示します。

<インストール DVD-ROM をセットしたドライブ>:¥HGLM¥GLMTools¥sample_installhglm.ini

サンプルファイルの内容を次に示します。

```
[INSTALLATION_SETTINGS]
HGLM_INSTDIR="C:¥Program Files¥HiCommand"
HGLM_DBDIR="C:¥Program Files¥HiCommand¥HGLAM¥database"
HGLM_IPADDRESS=
HGLM_PORT=22015
HGLM_SNMPTRAP=TRUE
HGLM_SNMPIPADDRESS=
HGLM_SNMPIPV6ADDRESS=
HGLM_SNMPTRAPPORT=22620
HGLM_RUNSERVICE=TRUE
HGLM_DBTMPDIR="C:¥Program Files¥HiCommand¥databackup"
HGLM_DATATMPDIR="C:¥Program Files¥HiCommand¥databackup"
HGLM_HDLMINSTALLDOWNLOAD=FALSE
[EOF]
```

クラスタ環境をセットアップする場合は，HGLM_CLUSTER_SETUP などのキーを指定してください。クラスタ環境をセットアップする場合の定義内容の例を次に示します。

```
[INSTALLATION_SETTINGS]
HGLM_INSTDIR="C:¥Program Files¥HiCommand"
HGLM_DBDIR="X:¥HiCommand¥HGLAM¥database"
HGLM_IPADDRESS=HCSClientAccessPoint
HGLM_PORT=22015
HGLM_SNMPTRAP=TRUE
HGLM_SNMPIPADDRESS=
HGLM_SNMPIPV6ADDRESS=
HGLM_SNMPTRAPPORT=22620
HGLM_RUNSERVICE=FALSE
HGLM_DBTMPDIR="C:¥Program Files¥HiCommand¥databackup"
HGLM_DATATMPDIR="C:¥Program Files¥HiCommand¥databackup"
HGLM_CLUSTER_SETUP=TRUE
HGLM_CLUSTER_MODE=2
HGLM_CLUSTER_RESOURCEGROUPNAME=HCSClusterServices
HGLM_CLUSTER_HOSTNAME_ACTIVE=activenodehost
HGLM_CLUSTER_HOSTNAME_STANDBY=standbynodehost
HGLM_HDLMINSTALLDOWNLOAD=FALSE
[EOF]
```

sample_installhglm.ini ファイルを編集する場合は，任意のフォルダにコピーしてください。

[INSTALLATION_SETTINGS]セクションにインストール応答処理の内容を定義します。

- 「#」で始まる行はコメントして見なされます。セクション名の先頭に「#」を付けると，セクション内の定義はすべてコメントとして見なされ，デフォルト値が適用されます。
- 空行は無視されます。

定義内容

[INSTALLATION_SETTINGS]セクションのキーの内容および指定できるインストールの種別を次の表に示します。

表 2-4 [INSTALLATION_SETTINGS]セクションで指定するキー名

キー名	説明	指定できるインストールの種別
HGLM_INSTDIR	インストール先のフォルダを絶対パス名で指定します。64 バイト以内のパスを指定します。使用できる文字を次に示します。	新規インストール，または v6 もしくは v7 からのアップグレードインストール

キー名	説明	指定できるインストールの種別
	A～Z，a～z，0～9，'.'，'_'，' '（半角スペース），そのほかにパスの区切り文字として(¥)，(:)が使用できます。 デフォルトは「C:¥Program Files¥HiCommand」です。 次のフォルダは指定できません。 • %ProgramFiles(x86)%¥以下 • %CommonProgramFiles(x86)%¥以下 • %SystemRoot%¥SysWOW64¥以下 • %SystemRoot%¥system32¥以下 • %ProgramFiles%¥WindowsApps¥以下	
HGLM_DBDIR	データベース格納先を絶対パス名で指定します。64 バイト以内のパスを指定します。使用できる文字を次に示します。 A～Z，a～z，0～9，'.'，'_'，' '（半角スペース），そのほかにパスの区切り文字として(¥)，(:)が使用できます。 デフォルトは「C:¥Program Files¥HiCommand¥HGLAM¥database」です。 次のフォルダは指定できません。 • %ProgramFiles(x86)%¥以下 • %CommonProgramFiles(x86)%¥以下 • %SystemRoot%¥SysWOW64¥以下 • %SystemRoot%¥system32¥以下 • %ProgramFiles%¥WindowsApps¥以下	新規インストール，または v6 もしくは v7 からのアップグレードインストール
HGLM_IPADDRESS	Global Link Manager サーバの IP アドレスまたはホスト名を指定します。IPv6 アドレスで指定する場合，IP アドレスを[]で囲んで指定します。 デフォルトは＜*Global Link Manager サーバの IP アドレス*＞です。 クラスタ設定の場合は論理ホスト名を指定します。	新規インストール
HGLM_PORT	Global Link Manager サーバのポート番号を指定します。 デフォルトは「22015」です。	新規インストール，または v6 もしくは v7 からのアップグレードインストール
HGLM_SNMPTRAP	SNMP Trap 受信機能を使用するかどうか指定します。 TRUE：使用します。 FALSE：使用しません。 デフォルトは「TRUE」です。	新規インストール
HGLM_SNMPIPADDRESS	SNMP Trap を受信する IPv4 アドレスを指定します。 デフォルトは＜*Global Link Manager サーバの IP アドレス*＞です。	新規インストール
HGLM_SNMPIPV6ADDRESS	SNMP Trap を受信する IPv6 アドレスを指定します。IP アドレスを[]で囲んで指定します。 デフォルトは＜*Global Link Manager サーバの IP アドレス*＞です。	新規インストール
HGLM_SNMPTRAPPORT	SNMP Trap を受信するポート番号を指定します。 デフォルトは「22620」です。	新規インストール
HGLM_RUNSERVICE	インストール後にサービス起動するかどうか指定します。 TRUE：起動します。 FALSE：起動しません。 デフォルトは「TRUE」です。	新規インストール，アップグレードインストール，または再インストール

キー名	説明	指定できるインストールの種別
	クラスタ環境への新規インストール，アップグレードインストール，または上書きインストールの場合は，「TRUE」を指定してもインストール後にサービスを起動しません。	
HGLM_DBTMPDIR	Hitachi Command Suite 製品（Global Link Manager を含む）のデータベース情報退避フォルダを絶対パス名で指定します。 デフォルトは「C:¥Program Files¥HiCommand ¥databackup」です。	v6 または v7 からのアップグレードインストール
HGLM_DATATMPDIR	Global Link Manager のパスステータスログ，プロパティファイル，ログファイルの退避先フォルダを絶対パス名で指定します。 デフォルトは「C:¥Program Files¥HiCommand ¥databackup」です。	v6 または v7 からのアップグレードインストール
HGLM_CLUSTER_SETUP	Hitachi Command Suite 共通コンポーネントおよび HiRDB が，クラスタ構成と非クラスタ構成のどちらでもない場合に，クラスタ環境または非クラスタ環境のどちらをセットアップするかを指定します。 TRUE：クラスタ環境をセットアップします。 FALSE：非クラスタ環境をセットアップします。 デフォルトは「FALSE」です。 HGLM_CLUSTER_SETUP で「TRUE」を指定した場合，次のキー名の指定は必須です。 ・ HGLM_CLUSTER_RESOURCEGROUPNAME ・ HGLM_CLUSTER_HOSTNAME_ACTIVE ・ HGLM_CLUSTER_HOSTNAME_STANDBY	新規インストール，アップグレードインストール，または再インストール
HGLM_CLUSTER_MODE	クラスタ構成でインストールする場合に，動作モードを指定します。 2：実行系 3：待機系 デフォルトは「2」です。	新規インストール，アップグレードインストール，または再インストール
HGLM_CLUSTER_RESOURCEGROUPNAME	リソースグループ名を指定します。 クラスタ構成で，ユーザーが設定しないでサイレントインストールした場合，エラーになります。	新規インストール，アップグレードインストール，または再インストール
HGLM_CLUSTER_HOSTNAME_ACTIVE	実行系のホスト名を指定します。 クラスタ構成で，ユーザーが設定しないでサイレントインストールした場合，エラーになります。	新規インストール，アップグレードインストール，または再インストール
HGLM_CLUSTER_HOSTNAME_STANDBY	待機系のホスト名を指定します。 クラスタ構成で，ユーザーが設定しないでサイレントインストールした場合，エラーになります。	新規インストール，アップグレードインストール，または再インストール
HGLM_HDLMINSTALLDOWNLOAD	HDLM インストーラーのダウンロード機能を使用するかどうか指定します。 TRUE：使用します。 FALSE：使用しません。 デフォルトは「FALSE」です。 アップグレードインストールまたは再インストールの場合で，ダウンロード機能を有効にしてすでにインストール済みのときは，このキー項目は使用されません。指定値に関係なく，ダウンロード機能は有効となります。	新規インストール，アップグレードインストール，または再インストール

(3) ログファイルについて

サイレントインストールを使用したインストールでは，インストール処理結果がログファイル（installhglm_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss*.log）に出力されます。

installhglm_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss*.log ファイルの出力先を次に示します。

＜*システムドライブ*＞:¥installhglm_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss*.log

ログファイルに KAIF40111-I のメッセージが出力されていない場合は，出力されたメッセージに従って対処してください。

注意事項

installhglm_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss*.log ファイルおよび setup_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss*.log ファイル※のサイレントインストールのログファイルはシステムドライブの直下に生成され，Global Link Manager のアンインストールと同時に削除されることはありません。したがって，サイレントインストールのログファイルが不要になったときは，手動で削除してください。

注※

内部処理で出力されるログファイル

2.1.6 Global Link Manager のアンインストール

アンインストールする前には次のことを確認してください。

- Administrator または Administrators グループのユーザーで Windows にログオンしていること。
- Windows のサービスを操作するウィンドウを表示していないこと（コンピュータの管理，サービスなど）。
- Global Link Manager の管理対象に OS が VMware のホストを設定している場合，Global Link Manager をアンインストールする前に，OS が VMware のホストを削除していること※。

注※

ホストを削除する手順については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。OS が VMware のホストを削除する前に Global Link Manager をアンインストールした場合，次の対処を実施してください。

a. リモート管理クライアント上の Windows に，Administrators グループのユーザーでログオンします。

b. HDLM マネージャを停止します。
［スタート］－［コントロールパネル］－［管理ツール］－［サービス］を選択します。
サービスの一覧で「DLMManager」をダブルクリックして，［停止］ボタンをクリックします。

c. 次のフォルダ内にある，すべてのフォルダとファイルを削除します。
＜*HDLM のインストール先フォルダ*＞¥host

d. HDLM マネージャを起動します。
［スタート］－［コントロールパネル］－［管理ツール］－［サービス］を選択します。
サービスの一覧で「DLMManager」をダブルクリックして，［開始］ボタンをクリックします。

注意事項

同一パス使用回数機能を Global Link Manager から LU 単位で設定した状態のまま Global Link Manager をアンインストールした場合，LU 単位の設定値はそのまま有効となりますが，LU 単位の設定値の表示や変更ができなくなります。

そのため，システム単位の同一パス使用回数機能を有効にする場合は，次のどちらかの方法で設定してください。

- Global Link Manager をアンインストールする前の場合

  マニュアル「Hitachi Global Link Manager ユーザーズガイド」の「マルチパス LU 設定」を参照して，同一パス使用回数に［ホストの設定に従う］を設定し，システム単位の同一パス使用回数を設定してください。

- Global Link Manager をアンインストールしたあとの場合

  HDLM のコマンドの set オペレーションで，システム単位の同一パス使用回数を設定してください。

  HDLM のコマンドの実行方法については, HDLM のマニュアルを参照してください。

アンインストールの手順は次のとおりです。

1. ［スタート］－［コントロールパネル］－［プログラムの追加と削除］の順に選択し，［現在インストールされているプログラム］の一覧から Hitachi Global Link Manager を選択して［変更と削除］ボタンをクリックします。

   Hitachi Global Link Manager のアンインストールダイアログが表示されます。

2. ［次へ］ボタンをクリックします。

   Hitachi Command Suite 共通コンポーネントまたは Hitachi Command Suite 製品のサービスが起動しているときは，次の画面が表示されます。

   - Hitachi Command Suite 製品のサービスの停止ダイアログが表示されます。［次へ］ボタンをクリックすると，Hitachi Command Suite 共通コンポーネントおよびほかの Hitachi Command Suite 製品のサービスが停止されます。

3. ［次へ］ボタンをクリックします。

   ほかの Hitachi Command Suite 製品がインストールされている場合は，アンインストール後に Hitachi Command Suite 製品のサービスを起動するかどうかを確認するダイアログが表示されます。アンインストール後にサービスを起動するかどうかを選択します（任意）。ダイアログが表示されない場合は，手順 4 へ進んでください。

   ［はい］または［いいえ］ボタンをクリックすると，アンインストール前の確認ダイアログが表示されます。

4. アンインストール情報を確認し，［アンインストール］ボタンをクリックします。

   ソフトウェア情報の設定が解除され，Global Link Manager のデータベースが削除されたあと，アンインストール処理が開始されます。SNMP Trap 受信機能を使用していた場合で，ファイアウォールの例外に SNMP Trap を受信するポート番号が登録されていたときは，HGLM 設定解除の完了ダイアログが表示されます。ダイアログの内容を確認してください。

5. ［次へ］ボタンをクリックします。

   正常にアンインストールが完了した場合は，アンインストールの完了ダイアログが表示されます。

6. ［完了］ボタンをクリックして，アンインストールを完了します。

注意事項

- Global Link Manager をアンインストール時，次の製品がインストールされている環境の場合，該当製品を一度アンインストールしたあと，再インストールしてください。各製品のデータ移行手順については，各製品のユーザーズガイドマニュアルを参照してください。
  - Hitachi Command Suite v7 以前
  - Hitachi File Services Manager
  - Storage Navigator Modular 2

2.2 ライセンスの初期設定

Global Link Manager にログインして運用を開始するために，Global Link Manager のセットアップ後に，Global Link Manager GUI からライセンスの初期設定を行います。

Global Link Manager のライセンスを設定する手順を次に説明します。

1. Web ブラウザーのアドレスバーに次の形式でログイン URL を入力します。

   http://＜*Global Link Manager サーバの IP アドレスまたはホスト名*＞:＜*Global Link Manager サーバの HBase 64 Storage Mgmt Web Service のポート番号*＞/GlobalLinkAvailabilityManager/

   例：http://127.0.0.1:22015/GlobalLinkAvailabilityManager/

   IPv6 形式の IP アドレスを入力する場合は，IP アドレスの部分を[ ]で囲んでください。

   ログインする URL を確認するには，次のコマンドを実行します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64chgurl /list

   ログインページへウィンドウが表示されます。続いて，ユーザーログインウィンドウが表示されます。
2. ［ライセンス情報］ボタンをクリックします。

   ライセンスダイアログが表示されます。
3. ライセンス情報を登録します。

   ライセンスキーには次の表に示す 3 種類があります。

表 2-5 ライセンスキー種別

ライセンスキー種別	説明
永久ライセンスキー	永久的な製品の使用を可能とするためのライセンスキーです。
一時ライセンスキー	ユーザーが製品の評価などを行う場合に使用するライセンスキーです。ライセンス期間は 120 日間です。
非常ライセンスキー	永久ライセンスキーの発行が間に合わない場合などに，一時的に使用するライセンスキーです。ライセンス期間は 30 日間です。

3

Global Link Manager の設定

この章では，Global Link Manager の起動と停止，Global Link Manager のデータベースのバックアップとリストアなど，Global Link Manager の設定について説明します。

なお，Windows Server 2012 以外と Windows Server 2012 で名称が異なる項目について，特に断り書きがない場合，Windows Server 2012 以外での名称を記載しています。そのため，Windows Server 2012 使用時には，「リソースグループ」を「役割」に読み替えてください。

3.1 コマンドを実行するときの注意事項

Global Link Manager の設定に必要なコマンドを実行するときの注意事項を説明します。

3.1.1 ログインユーザー

このマニュアルに記載されているコマンドを実行するには，Administrators グループのユーザーでログインしてください。

3.1.2 管理者権限の昇格

UAC 機能をサポートしている Windows OS では，UAC 機能が有効になっている場合，コマンドの実行時に管理者権限への昇格が求められることがあります。管理サーバの運用に必要なコマンドにも，管理者権限に昇格して実行しなければならないコマンドがあります。UAC 機能が有効な OS でこのマニュアルに記載されているコマンドを実行する場合は，特別な注意書きがないかぎり，管理者権限に昇格してコマンドを実行してください。

管理者権限に昇格してコマンドを実行する方法を次に示します。

1. ［コマンドプロンプト］のアイコンを右クリックします。
2. 右クリックメニューの一覧から［管理者として実行］を選択します。
   管理者権限に昇格済みのコマンドプロンプトが起動されます。

3.2 Global Link Manager の起動と停止

Global Link Manager の起動と停止は, Hitachi Command Suite 共通コンポーネントを起動または停止することで実行します。

通常，Global Link Manager は自動的に起動されますが，プロパティファイルを更新した場合など，手動で起動および停止を実行する必要があります。

3.2.1 Global Link Manager の起動

Global Link Manager を起動するには，Hitachi Command Suite 共通コンポーネントを起動します。

起動には，次の方法があります。

Windows のスタートメニューから起動：

Windows Server 2012 以外の場合

［スタート］－［すべてのプログラム］－［Hitachi Command Suite］－［Global Link Manager］－［Start - HGLM］を選択します。

Windows Server 2012 の場合

スタート画面から［すべてのアプリ］を選択し，［Hitachi Command Suite］－［Global Link Manager］－［Start - HGLM］を選択します。

コマンドを実行して起動：

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64srv /start

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Global Link Manager と一緒にほかの Hitachi Command Suite 製品のサービスも起動されます。ただし，次の場合は，サービスは起動されません。

・ すでに Hitachi Command Suite 共通コンポーネントが起動している場合

この場合は，各製品のマニュアルを参照して，サービスを起動してください。

3.2.2 Global Link Manager の停止

Global Link Manager を停止するには，Hitachi Command Suite 共通コンポーネントを停止します。

停止には，次の方法があります。

Windows のスタートメニューから停止：

Windows Server 2012 以外の場合

［スタート］－［すべてのプログラム］－［Hitachi Command Suite］－［Global Link Manager］－［Stop - HGLM］を選択します。

Windows Server 2012 の場合

スタート画面から［すべてのアプリ］を選択し，［Hitachi Command Suite］－［Global Link Manager］－［Stop - HGLM］を選択します。

コマンドを実行して停止：

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Global Link Manager と一緒にほかの Hitachi Command Suite 製品のサービスも停止されます。

注意事項

- Hitachi Command Suite 共通コンポーネントのサービス起動直後に，サービスの停止を実施しないでください。サービスの起動直後に停止する場合は，数秒時間を空けてから停止してください。
- 05-60 より前のバージョンの Replication Monitor がインストールされている環境で，Hitachi Command Suite 共通コンポーネントを停止させるには，先に Device Manager のサービスを停止する必要があります。サービスの停止方法については，マニュアル「Hitachi Command Suite システム構成ガイド」を参照してください。

3.2.3 Global Link Manager の起動状態の確認

Global Link Manager の起動状態を確認するには，Hitachi Command Suite 共通コンポーネントの起動状態を確認します。Hitachi Command Suite 共通コンポーネントの起動状態を確認するには，次のコマンドを実行します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /status

次のメッセージが出力された場合は，Hitachi Command Suite 共通コンポーネントが正常に起動しています。

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
Web Service
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
Web SSO Service
KAPM05007-I Already started service. service-name=HBase 64 Storage Mgmt
```

```
SSO Service
KAPM05007-I Already started service. service-name=Global Link Manager
Web Service
```

3.2.4 Hitachi Command Suite 共通コンポーネントの常駐プロセス

Hitachi Command Suite 共通コンポーネントの常駐プロセスを次の表に示します。

表 3-1 Hitachi Command Suite 共通コンポーネントの常駐プロセス

プロセス名	サービス名	機能
hcmdssvctl.exe cjstartsv.exe	Global Link Manager Web Service	Global Link Manager の J2EE サービス
hcmdssvctl.exe cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	シングルサインオン用の Hitachi Command Suite J2EE サービス
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web Service	Hitachi Command Suite 共通 Web サービス このプロセスは複数起動されていることがあります。
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web SSO Service	シングルサインオン用の Hitachi Command Suite 共通 Web サービス
hntr2mon.exe	Hitachi Network Objectplaza Trace Monitor 2 Hitachi Network Objectplaza Trace Monitor 2 (x64)	Hitachi Command Suite 共通トレースログ採取
hntr2srv.exe		Hitachi Command Suite 共通トレースサービス ([サービス] ウィンドウからのイベントの処理)
pdservice.exe※	HiRDB/EmbeddedEdition_HD1	HiRDB のプロセスサーバの制御

注※

常に起動していることが前提です。手動での停止や，クラスタリソースへの登録はしないでください。

3.3 Global Link Manager をインストールするマシンの時刻の変更

Global Link Manager をインストールする前に，現在の時刻に設定しておきます。ここでは，すでにほかの Hitachi Command Suite 製品がインストールされている環境に Global Link Manager をインストールする場合の時刻変更について，または Global Link Manager をインストールしたあとで時刻を変更する必要がある場合について説明します。

注意事項

Hitachi Command Suite 共通コンポーネントの起動中にマシンの時刻が変更されると，Global Link Manager を含む Hitachi Command Suite 製品が正しく動作しなくなるおそれがあります。マシンの時刻は，インストールの前に変更しておくことをお勧めします。

時刻の調整機能を使用する場合の設定

NTP などの時刻を自動的に調整する機能を使用する場合，マシンの時刻が実際の時刻よりも進んだときに，マシンの時刻を一度にさかのぼらせないで少しずつ時間を掛けて調整する機能を使用してください。機能の中には，時刻のずれ幅が一定時間内であれば少しずつ時刻を調整し，一定時間を

超えると時刻を一度にさかのぼらせて調整するものがあります。時刻のずれ幅が，少しずつ調整される範囲を超えないように，使用する機能での時刻調整の頻度を設定してください。

例えば，Windows Time サービスを使用した場合，マシンの時刻が実際の時刻よりも進んだ幅が一定時間内であれば，マシンの時刻を一度にさかのぼらせることなく少しずつ時刻を調整できます。Windows Time サービスで少しずつ時刻を調整できる範囲を確認し，マシンの時刻と実際の時刻のずれ幅がその範囲を超えないように，Windows Time サービスでの時刻の調整頻度を設定してください。

時刻の調整機能が使用できない場合，または直ちに時刻を変更する必要がある場合

時刻を自動的に調整する機能を使用できない場合や，直ちに時刻を変更する必要がある場合，次の手順でマシンの時刻を変更してください。

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。
   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin¥hcmds64srv /stop
   同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，一緒にほかの Hitachi Command Suite 製品のサービスも停止されます。
2. マシンの時刻を変更します。
3. マシンを再起動します。

3.4 Global Link Manager のデータベースの操作

Global Link Manager のデータベースに対する次の操作について説明します。

- データベースのバックアップとリストア
- データベースの移行（エクスポートとインポート）
- データベースの格納先の変更

データベースの操作を実行する場合，Global Link Manager のプロパティファイルおよびパス稼働情報（パスステータスログ）についてもバックアップやリストアを実行する必要があります。バックアップやリストアの対象となるプロパティファイルは次のファイルです。

- `server.properties`
- `logger.properties`
- `database.properties`

バックアップとリストア，エクスポートとインポートについて，機能の違いを次の表に示します。

表 3-2 バックアップとリストア，エクスポートとインポートの違い

項目	バックアップとリストア	エクスポートとインポート
Hitachi Command Suite 共通コンポーネントのバージョンの条件	制限なし。	エクスポート元およびインポート先に，バージョン 5.5 以降の Hitachi Command Suite 共通コンポーネントがインストールされていること。
主な使用目的	サーバマシンに障害が発生したときに，現状の運用環境を回復すること。	サーバマシンを，別の OS のマシンなど現状とは異なる環境に移行すること。
対象となるデータ	• Hitachi Command Suite 製品のデータベース	• Hitachi Command Suite 製品のデータベース

項目	バックアップとリストア	エクスポートとインポート
	• Hitachi Command Suite 共通コンポーネントのデータベース	• Hitachi Command Suite 共通コンポーネントのデータベースに含まれるユーザー情報
リストア先，またはインポート先のマシンの条件	次の点が同じであること。 • インストールされている Hitachi Command Suite 製品の種類，バージョン，リビジョン • 各 Hitachi Command Suite 製品，共通コンポーネント，各 Hitachi Command Suite 製品のデータベース，および共通コンポーネントのデータベースのインストール先 • マシンの IP アドレスとホスト名	• データベースをインポートする Hitachi Command Suite 製品がインストールされていること。 • インストールされている Hitachi Command Suite 製品のバージョンが，エクスポート元と同じかそれ以上であること。

3.4.1 Global Link Manager のデータベースのバックアップ

万が一のときに備えて，Global Link Manager およびそのほかの Hitachi Command Suite 製品のデータベースは，定期的にバックアップを取得しておくことをお勧めします。また，次の操作を実行する場合は，必ず事前にデータベースのバックアップを取得しておいてください。

- Global Link Manager を再インストールまたはアップグレードインストールする場合
- Global Link Manager がインストールされているサーバにほかの Hitachi Command Suite 製品をインストールまたはアンインストールする場合
- ほかの Hitachi Command Suite 製品がインストールされているサーバに Global Link Manager をインストールまたはアンインストールする場合

Global Link Manager およびほかの Hitachi Command Suite 製品のデータベースのバックアップを取得する手順を次に示します。このとき，データベースのほかに，Global Link Manager のプロパティファイルおよびパス稼働情報（パスステータスログ）のバックアップも取得しておきます。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

(1) 非クラスタ構成の場合

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. 次のコマンドを実行して，HiRDB を起動します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /start

3. 次のコマンドを実行して，データベースをバックアップします。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64backups /dir ＜*バックアップ先フォルダ名*＞

   ＜*バックアップ先フォルダ名*＞はローカルディスク上のフォルダを絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   コマンドを実行すると，コマンドを実行したサーバにインストールされている Hitachi Command Suite 製品のデータベースのバックアップ（backup.hdb）が取得されます。このと

き，Hitachi Command Suite 共通コンポーネントおよびほかの Hitachi Command Suite 製品の設定ファイルもバックアップされます。

4. 次のコマンドを実行して，プロパティファイルおよびパス稼働情報（パスステータスログ）をバックアップします。

   ＜Global Link Manager のインストールフォルダ＞¥bin¥hglambackup /dir *＜バックアップ先フォルダ名＞*

   *＜バックアップ先フォルダ名＞*は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   *＜バックアップ先フォルダ名＞*に使用できる文字を次に示します。

   A〜Z，a〜z，0〜9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

   コマンドの実行例を次に示します。

   ```
   "C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglambackup" /dir "C:¥hglam
   backup"
   ```

   *＜バックアップ先フォルダ名＞*で指定したフォルダ以下のファイル構成は，変更しないでください。

5. 必要に応じて，次のコマンドを実行し，Hitachi Command Suite 共通コンポーネントのサービスを起動します。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin ¥hcmds64srv /start

(2) クラスタ構成の場合

サービス停止およびフェールオーバー無効操作

1. クラスタソフトウェアで，次のリソースをオフラインにします。
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース
2. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin ¥hcmds64srv /stop
3. クラスタソフトウェアで，次のサービスをオフラインにします。
   - HiRDBClusterService_HD1
4. クラスタソフトウェアで，リソースグループのフェールオーバーを抑止します。

   Microsoft Failover Cluster を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，再起動しない］を選択します。
5. 次のコマンドを実行して，HiRDB を起動します。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin ¥hcmds64dbsrv /start
6. 次のコマンドを実行して，データベースをバックアップします。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin ¥hcmds64backups /dir *＜バックアップ先フォルダ名＞*

   *＜バックアップ先フォルダ名＞*はローカルディスク上のフォルダを絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

コマンドを実行すると，コマンドを実行したサーバにインストールされている Hitachi Command Suite 製品のデータベースのバックアップ（backup.hdb）が取得されます。このとき，Hitachi Command Suite 共通コンポーネントおよびほかの Hitachi Command Suite 製品の設定ファイルもバックアップされます。

7. 次のコマンドを実行して，プロパティファイルおよびパス稼働情報（パスステータスログ）をバックアップします。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglambackup /dir ＜*バックアップ先フォルダ名*＞

   ＜*バックアップ先フォルダ名*＞は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   ＜*バックアップ先フォルダ名*＞に使用できる文字を次に示します。

   A〜Z，a〜z，0〜9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

   コマンドの実行例を次に示します。

   ```
   "C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglambackup" /dir "C:¥hglam backup"
   ```

   ＜*バックアップ先フォルダ名*＞で指定したフォルダ以下のファイル構成は，変更しないでください。

8. 必要に応じて，次のコマンドを実行し，Hitachi Command Suite 共通コンポーネントのサービスを起動します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start

サービス起動およびフェールオーバー有効操作

1. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. クラスタソフトウェアで，次のリソースのフェールオーバーを有効にします。

   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする］を選択します。

   Microsoft Failover Cluster（Windows Server 2012）を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，この役割のすべてのリソースをフェールオーバーする］を選択します。

3. クラスタソフトウェアで，リソースグループをオンラインにします。

3.4.2 Global Link Manager のデータベースのリストア

Global Link Manager およびほかの Hitachi Command Suite 製品のデータベースをリストアする手順を次に示します。このとき，データベースのほかに，Global Link Manager のプロパティファイルおよびパス稼働情報（パスステータスログ）もリストアします。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

(1) 非クラスタ構成の場合

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. 次のコマンドを実行して，Global Link Manager のデータベースをリストアします。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64db /restore ＜バックアップファイル名＞ /type HGLAM

   ＜*バックアップファイル名*＞は，リストアするバックアップデータ（backup.hdb）を絶対パスで指定します。

   Global Link Manager のデータベースをリストアするには，「/type HGLAM」または「/type GlobalLinkAvailabilityManager」を指定します。

   Global Link Manager のデータベースだけではなく，ほかの Hitachi Command Suite 製品のデータベースも一括してリストアする場合は，「/type ALL」を指定してコマンドを実行します。

   Hitachi Command Suite 製品をすべてアンインストールしたあとで，Hitachi Command Suite 製品を再度インストールした場合に，データベースをリストアするときは「/type ALL」を指定してください。

   注意事項

   「/type ALL」を指定してデータベースをリストアすると，ほかの Hitachi Command Suite 製品の状態が，バックアップデータを取得したときの状態に戻ります。コマンドを実行するときは，ほかの製品の状態をバックアップデータ取得したときの状態に戻しても問題がないことを十分に確認してください。

3. 次のコマンドを実行して，プロパティファイルおよびパス稼働情報（パスステータスログ）をリストアします。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamrestore /dir ＜*バックアップデータ格納先フォルダ名*＞

   ＜*バックアップデータ格納先フォルダ名*＞には，hglambackup コマンドでバックアップしたデータの格納先フォルダを絶対パスで指定します。

4. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを起動します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start

(2) クラスタ構成の場合

サービス停止およびフェールオーバー無効操作

1. クラスタソフトウェアで，次のリソースをオフラインにします。
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース
2. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

3. クラスタソフトウェアで，次のサービスをオフラインにします。

   - HiRDBClusterService_HD1

4. クラスタソフトウェアで，リソースグループのフェールオーバーを抑止します。

   Microsoft Failover Cluster を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，再起動しない］を選択します。

5. 次のコマンドを実行して，Global Link Manager のデータベースをリストアします。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64db /restore ＜バックアップファイル名＞ /type HGLAM

   ＜*バックアップファイル名*＞は，リストアするバックアップデータ（backup.hdb）を絶対パスで指定します。

   Global Link Manager のデータベースをリストアするには，「/type HGLAM」または「/type GlobalLinkAvailabilityManager」を指定します。

   Global Link Manager のデータベースだけではなく，ほかの Hitachi Command Suite 製品のデータベースも一括してリストアする場合は，「/type ALL」を指定してコマンドを実行します。

   Hitachi Command Suite 製品をすべてアンインストールしたあとで，Hitachi Command Suite 製品を再度インストールした場合に，データベースをリストアするときは「/type ALL」を指定してください。

   注意事項

   「/type ALL」を指定してデータベースをリストアすると，ほかの Hitachi Command Suite 製品の状態が，バックアップデータを取得したときの状態に戻ります。コマンドを実行するときは，ほかの製品の状態をバックアップデータ取得したときの状態に戻しても問題がないことを十分に確認してください。

6. 次のコマンドを実行して，プロパティファイルおよびパス稼働情報（パスステータスログ）をリストアします。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamrestore /dir ＜*バックアップデータ格納先フォルダ名*＞

   ＜*バックアップデータ格納先フォルダ名*＞には，hglambackup コマンドでバックアップしたデータの格納先フォルダを絶対パスで指定します。

7. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを起動します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start

サービス起動およびフェールオーバー有効操作

1. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. クラスタソフトウェアで，次のリソースのフェールオーバーを有効にします。

   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用している場合：

リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする］を選択します。

Microsoft Failover Cluster（Windows Server 2012）を使用している場合：

リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，この役割のすべてのリソースをフェールオーバーする］を選択します。

3. クラスタソフトウェアで，リソースグループをオンラインにします。

3.4.3 Global Link Manager のデータベースの移行

Hitachi Command Suite 製品を長期間使用していると，Hitachi Command Suite 製品のバージョンアップや管理対象となるオブジェクトの増加によって，今までよりも高性能なマシンが必要になる場合があります。このような場合，マシンの入れ替え作業の 1 つとしてデータベースを移行する必要があります。Hitachi Command Suite 製品では，hcmds64dbtrans コマンドを使用してデータベースを移行できます。hcmds64dbtrans コマンドは，各 Hitachi Command Suite 製品のデータベースに格納されているすべての情報と，Hitachi Command Suite 共通コンポーネントが管理しているユーザー情報を移行するコマンドです。

hcmds64dbtrans コマンドを使用すると，次に示すように，使用中のサーバマシンとは異なる環境のマシンにも，Global Link Manager のデータベースを移行できます。

- Hitachi Command Suite 製品のインストール先が異なるマシンへの移行
- Hitachi Command Suite 製品のバージョンが移行元のバージョンよりも新しいマシンへの移行

(1) データベースを移行する場合の注意事項

移行先と移行元の Hitachi Command Suite 製品の種類，バージョン，およびユーザー情報についての注意事項を次に示します。

移行先と移行元の Hitachi Command Suite 製品の種類とバージョンについての注意事項

- 移行先にインストールされていない Hitachi Command Suite 製品のデータベースは移行できません。移行先には，必要な Hitachi Command Suite 製品を漏れなくインストールしてください。
- 移行先にインストールされている Hitachi Command Suite 製品のバージョンがどれか 1 つでも移行元より古い場合，移行はできません。移行先のサーバには，移行元と同じか，またはそれ以上のバージョンの Hitachi Command Suite 製品をインストールしてください。
- バージョン 04-20 以前の Replication Monitor のデータベースを移行する場合は，事前に移行元および移行先の Replication Monitor を 05-00 以降のバージョンにアップグレードしてください。
- Replication Monitor のデータベースを Replication Manager のデータベースに移行する場合は，移行元の Replication Monitor を Replication Manager にアップグレードしてからデータベースを移行してください。
- Tuning Manager のデータベースを移行する場合，次の制約があります。
  - Tuning Manager のバージョンが 6.0 より前の場合，事前に移行元および移行先の Tuning Manager を 6.0 以降のバージョンにアップグレードしてください。
  - Tuning Manager のデータベースは，移行元と移行先で同じ総容量に設定してください。データベースの総容量を変更する方法については，マニュアル「Hitachi Command Suite Tuning Manager 運用管理ガイド」を参照してください。

- 移行元と移行先のデータベースの構成（Small または Medium）が同じか，または移行先のデータベースの構成が大きくなる組み合わせの場合に移行できます。
- 移行元のデータベースの構成で，管理対象となるリソース数が管理限界の 70%を超える場合には，同じデータベースの構成には移行できません。

ユーザー情報についての注意事項

- 移行先にユーザー情報がある場合，そのユーザー情報は移行元のユーザー情報に置き換えられます。このため，すでに Hitachi Command Suite 製品のユーザー情報があるマシンへは移行しないでください。
- 1 台の管理サーバに複数の Hitachi Command Suite 製品がインストールされている場合，データベースを数回に分けて移行すると，移行するたびにユーザー情報が置き換えられ，最後に移行した製品のユーザー情報しか残りません。複数の製品を移行する場合は，各製品のユーザー情報をすべて移行できるよう，必ず 1 回の操作でデータベースを移行してください。
- ユーザー情報が置き換えられるため，複数の管理サーバで稼働していた Hitachi Command Suite 製品を 1 台の管理サーバに集約するような移行はできません。

(2) データベースを移行する手順の流れ

データベースを移行する手順の流れは次のとおりです。

1. 移行先サーバに，データベースを移行する Hitachi Command Suite 製品をインストールする。
2. 移行元サーバでデータベースをエクスポートする。
3. 移行元サーバから移行先サーバへアーカイブファイルを転送する。
4. 移行先サーバでデータベースをインポートする。

(3) 移行先サーバへの Hitachi Command Suite 製品のインストール

移行先サーバに，データベースを移行する Hitachi Command Suite 製品をインストールしてください。移行先サーバにインストールする Hitachi Command Suite 製品のバージョンは，移行元の Hitachi Command Suite 製品と同じか，それ以上にしてください。

(4) 移行元サーバでのデータベースのエクスポート

Global Link Manager のデータベースをエクスポートするときには，データベースの情報を一時的に格納するためのフォルダと，アーカイブファイルを格納するフォルダが必要です。それぞれのフォルダには，次に示す 2 つのフォルダの合計サイズと同等の容量を確保してください。

- Global Link Manager のデータベースの格納先フォルダ
- Hitachi Command Suite 共通コンポーネントのデータベースの格納先フォルダから SYS フォルダ以下を除いたもの

Global Link Manager のデータベースの格納先フォルダは，インストール時に指定した場所になります。＜*Global Link Manager のデータベースの格納先フォルダ*＞¥GlobalLinkAvailabilityManager です。

Hitachi Command Suite 共通コンポーネントのデータベースの格納先フォルダは，＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥database です。

この容量は，Global Link Manager のデータベースだけがインストールされているときの目安です。Global Link Manager 以外の Hitachi Command Suite 製品がインストールされている場合は，それらのデータベースの容量も考慮してください。

注意事項

データベースはアーカイブファイルとしてエクスポートされます。アーカイブファイルの作成先のディスク容量が不足している場合，データベースのエクスポート時に，アーカイブファイルの作成に失敗します。この場合は，アーカイブファイルの代わりに，エクスポート時に収集されるデータベース情報を手動で移行先に転送してください。

移行元サーバで，データベースをエクスポートする手順を次に示します。このとき，データベースのほかに，Global Link Manager のプロパティファイルおよびパス稼働情報（パスステータスログ）もエクスポートします。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

非クラスタ構成の場合

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. HiRDB を起動します。

   次のコマンドを実行してください。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /start

3. 次のコマンドを実行して，データベースをエクスポートします。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbtrans /export /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞

   ＜*作業用フォルダ*＞には，データベース情報を一時的に格納するためのフォルダを，絶対パスで指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，エクスポート処理が中断します。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。

   ＜*アーカイブファイル*＞には，エクスポートするデータベースのアーカイブファイルを絶対パスで指定します。

   コマンドの実行例を次に示します。

   ```
   "C:¥Program Files¥HiCommand¥Base64¥bin¥hcmds64dbtrans" /export /
   workpath D:¥trans_work /file D:¥trans_file¥db_arc
   ```

4. 次のコマンドを実行して，プロパティファイルおよびパス稼働情報（パスステータスログ）をエクスポートします。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamexport /dir ＜*エクスポート先フォルダ名*＞

   ＜*エクスポート先フォルダ名*＞は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   ＜*エクスポート先フォルダ名*＞に使用できる文字を次に示します。

   A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

   コマンドの実行例を次に示します。

   ```
   "C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglamexport" /dir "C:¥hglam
   export"
   ```

5. アーカイブファイルを移行先サーバに転送します。

6. 手順 4 のエクスポート先フォルダを移行先サーバに転送します。
   ＜*エクスポート先フォルダ名*＞で指定したフォルダ以下のファイル構成は，変更しないでください。

クラスタ構成の場合

サービス停止およびフェールオーバー無効操作

1. クラスタソフトウェアで，次のリソースをオフラインにします。
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース
2. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop
3. クラスタソフトウェアで，次のサービスをオフラインにします。
   - HiRDBClusterService_HD1
4. クラスタソフトウェアで，リソースグループのフェールオーバーを抑止します。

   Microsoft Failover Cluster を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，再起動しない］を選択します。
5. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを起動します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start
6. 次のコマンドを実行して，データベースをエクスポートします。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbtrans /export /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞

   ＜*作業用フォルダ*＞には，データベース情報を一時的に格納するためのフォルダを，絶対パスで指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，エクスポート処理が中断します。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。

   ＜*アーカイブファイル*＞には，エクスポートするデータベースのアーカイブファイルを絶対パスで指定します。

   コマンドの実行例を次に示します。

   ```
   "C:¥Program Files¥HiCommand¥Base64¥bin¥hcmds64dbtrans" /export /
   workpath D:¥trans_work /file D:¥trans_file¥db_arc
   ```

7. 次のコマンドを実行して，プロパティファイルおよびパス稼働情報（パスステータスログ）をエクスポートします。
   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamexport /dir ＜*エクスポート先フォルダ名*＞

   ＜*エクスポート先フォルダ名*＞は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   ＜*エクスポート先フォルダ名*＞に使用できる文字を次に示します。

   A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

   コマンドの実行例を次に示します。

```
"C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglamexport" /dir "C:¥hglam
export"
```

8. アーカイブファイルを移行先サーバに転送します。
9. 手順 7 のエクスポート先フォルダを移行先サーバに転送します。

   *<エクスポート先フォルダ名>*で指定したフォルダ以下のファイル構成は，変更しないでください。

サービス起動およびフェールオーバー有効操作

1. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

   <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥bin¥hcmds64srv /stop
2. クラスタソフトウェアで，次のリソースのフェールオーバーを有効にします。
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする］を選択します。

   Microsoft Failover Cluster（Windows Server 2012）を使用している場合：

   リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，この役割のすべてのリソースをフェールオーバーする］を選択します。
3. クラスタソフトウェアで，リソースグループをオンラインにします。
4. アーカイブファイルを移行先サーバに転送します。
5. 「サービス停止およびフェールオーバー無効操作」の手順 7 のエクスポート先フォルダを移行先サーバに転送します。

   *<エクスポート先フォルダ名>*で指定したフォルダ以下のファイル構成は，変更しないでください。

アーカイブファイルを作成できなかった場合

*<作業用フォルダ>*で指定したフォルダに格納されているすべてのファイルを，移行先サーバに転送してください。このとき，*<作業用フォルダ>*で指定したフォルダ以下のファイル構成は変更しないでください。

(5) 移行先サーバでのデータベースのインポート

移行先サーバで，データベースをインポートする手順を次に示します。このとき，データベースのほかに，パス稼働情報（パスステータスログ）もリストアします。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

非クラスタ構成の場合

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. HiRDB を起動します。

   次のコマンドを実行してください。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /start

3. 次のコマンドを実行して，データベースをインポートします。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbtrans /import /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞ /type HGLAM

   ＜*作業用フォルダ*＞には，アーカイブファイルを展開するためのフォルダを，絶対パスで指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，インポート処理は中断されます。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。＜*アーカイブファイル*＞には，移行元サーバから転送したデータベースのアーカイブファイルを，絶対パスで指定します。

   アーカイブファイルを使用しない場合

   - ＜*作業用フォルダ*＞には移行元から転送したデータベース情報を格納したフォルダを指定してください。このとき，転送したフォルダ以下のファイル構成は変更しないでください。
   - /file オプションは指定しないでください。

   Global Link Manager のデータベースをインポートするには，「/type HGLAM」または「/type GlobalLinkAvailabilityManager」を指定します。

   Global Link Manager のデータベースだけではなく，ほかの Hitachi Command Suite 製品のデータベースもインポートする場合は，「/type ALL」を指定するか，またはデータベースを移行する Hitachi Command Suite 製品の名称をコンマで区切って指定します。/type オプションに指定するほかの Hitachi Command Suite 製品の名称は，それぞれのマニュアルを参照してください。

   ALL を指定した場合は，移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され，移行されます。複数の製品を指定した場合は，指定したすべての製品のデータベースが，アーカイブファイルまたは＜*作業用フォルダ*＞に指定したフォルダにあり，かつ，指定したすべての製品が移行先にインストールされている必要があります。条件を満たさない製品が 1 つでもある場合，移行は実行されません。

   注意事項

   - Hitachi Command Suite 製品によってインポートの手順が異なります。Global Link Manager 以外のデータベースを移行する場合は，それぞれの Hitachi Command Suite 製品のマニュアルを参照してください。
   - 移行元のマシンに，Replication Monitor 04-20 以前のバージョンがインストールされている場合，データベースを移行できません。事前に移行元および移行先の Replication Monitor を 05-00 以降にバージョンアップしてから移行してください。05-00 以降にバージョンアップできない場合，またはデータベースの移行が不要な場合，/type オプションで Replication Monitor 以外の製品をすべて指定してコマンドを実行してください。

4. 次のコマンドを実行して，パス稼働情報（パスステータスログ）のインポートおよびデータベースを更新します。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamimport /dir ＜*エクスポートデータ格納先フォルダ名*＞

＜*エクスポートデータ格納先フォルダ名*＞には，hglamexport コマンドでエクスポートしたデータの格納先フォルダを絶対パスで指定します。

インポート処理のあと，Global Link Manager のデータベースが更新されます。

注意事項

移行元と移行先で環境が異なる場合があるため，プロパティファイルはインポートされません。プロパティファイルを変更したい場合は，hglamexport コマンドでエクスポートしたデータの格納先フォルダ，または移行元サーバのプロパティファイルを確認し，移行先サーバのプロパティファイルを編集してください。

5. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを起動します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start

クラスタ構成の場合

サービス停止およびフェールオーバー無効操作

1. クラスタソフトウェアで，次のリソースをオフラインにします。
   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース
2. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

3. クラスタソフトウェアで，次のサービスをオフラインにします。
   - HiRDBClusterService_HD1
4. クラスタソフトウェアで，リソースグループのフェールオーバーを抑止します。

Microsoft Failover Cluster を使用している場合：

リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，再起動しない］を選択します。

5. 次のコマンドを実行して HiRDB を起動します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /start

6. 次のコマンドを実行して，データベースをインポートします。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbtrans /import /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞ /type HGLAM

＜*作業用フォルダ*＞には，アーカイブファイルを展開するためのフォルダを，絶対パスで指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，インポート処理は中断されます。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。＜*アーカイブファイル*＞には，移行元サーバから転送したデータベースのアーカイブファイルを，絶対パスで指定します。

アーカイブファイルを使用しない場合

- ＜*作業用フォルダ*＞には移行元から転送したデータベース情報を格納したフォルダを指定してください。このとき，転送したフォルダ以下のファイル構成は変更しないでください。
- /file オプションは指定しないでください。

Global Link Manager のデータベースをインポートするには，「/type HGLAM」または「/type GlobalLinkAvailabilityManager」を指定します。

Global Link Manager のデータベースだけではなく，ほかの Hitachi Command Suite 製品のデータベースもインポートする場合は，「/type ALL」を指定するか，またはデータベースを移行する Hitachi Command Suite 製品の名称をコンマで区切って指定します。/type オプションに指定するほかの Hitachi Command Suite 製品の名称は，それぞれのマニュアルを参照してください。

ALL を指定した場合は，移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され，移行されます。複数の製品を指定した場合は，指定したすべての製品のデータベースが，アーカイブファイルまたは＜*作業用フォルダ*＞に指定したフォルダにあり，かつ，指定したすべての製品が移行先にインストールされている必要があります。条件を満たさない製品が 1 つでもある場合，移行は実行されません。

注意事項

- Hitachi Command Suite 製品によってインポートの手順が異なります。Global Link Manager 以外のデータベースを移行する場合は，それぞれの Hitachi Command Suite 製品のマニュアルを参照してください。
- 移行元のマシンに，Replication Monitor 04-20 以前のバージョンがインストールされている場合，データベースを移行できません。事前に移行元および移行先の Replication Monitor を 05-00 以降にバージョンアップしてから移行してください。05-00 以降にバージョンアップできない場合，またはデータベースの移行が不要な場合，/type オプションで Replication Monitor 以外の製品をすべて指定してコマンドを実行してください。

7. 次のコマンドを実行して，パス稼働情報（パスステータスログ）のインポートおよびデータベースを更新します。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamimport /dir ＜*エクスポートデータ格納先フォルダ名*＞

   ＜*エクスポートデータ格納先フォルダ名*＞には，hglamexport コマンドでエクスポートしたデータの格納先フォルダを絶対パスで指定します。

   インポート処理のあと，Global Link Manager のデータベースが更新されます。

   注意事項

   移行元と移行先で環境が異なる場合があるため，プロパティファイルはインポートされません。プロパティファイルを変更したい場合は，hglamexport コマンドでエクスポートしたデータの格納先フォルダ，または移行元サーバのプロパティファイルを確認し，移行先サーバ（実行系ノードおよび待機系ノード）のプロパティファイルを編集してください。

サービス起動およびフェールオーバー有効操作

1. 次のコマンドを実行して，Hitachi Command Suite 製品のサービスを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. クラスタソフトウェアで，次のリソースのフェールオーバーを有効にします。

   - HBase 64 Storage Mgmt Web Service
   - Global Link Manager Web Service
   - 上記以外の Hitachi Command Suite 製品のリソース

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用している場合：

リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする］を選択します。

Microsoft Failover Cluster（Windows Server 2012）を使用している場合：

リソース名を右クリックし，［プロパティ］－［ポリシー］タブで，［リソースが失敗状態になった場合は，現在のノードで再起動を試みる］と［再起動に失敗した場合は，この役割のすべてのリソースをフェールオーバーする］を選択します。

3. クラスタソフトウェアで，リソースグループをオンラインにします。

3.4.4 Global Link Manager のデータベースの格納先の変更（非クラスタ環境の場合）

アップグレードインストール時に，データベースファイルの格納先のディスク容量が足りない場合は，データベースファイルの格納先を変更します。データベースファイルの格納先を変更する手順を説明します。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

注意事項

- この手順を実施すると，同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，ほかの Hitachi Command Suite 製品のデータベースファイルの格納先も変更されます。その場合，変更先のディスクの空き容量には，Global Link Manager のデータベースファイルの容量のほかに，ほかの Hitachi Command Suite 製品のデータベースファイルの容量も必要になります。インストールされている Hitachi Command Suite 製品全体のデータベースファイルの容量を考慮して，ディスクの空き容量を確保してください。ほかの Hitachi Command Suite 製品のデータベースファイルの容量については，各製品のマニュアルを参照してください。
- この手順で使用する hcmds64dbinit コマンドを実行すると，HiRDB が使用するポートの設定がデフォルト値（22032）に戻ります。ポート番号を変更して運用している場合は，あとで設定し直す必要があるので，使用しているポート番号を控えておいてください。
- この手順で使用する hcmds64dbinit コマンドを実行すると，ビルトインアカウント（ユーザー ID：System）のパスワードを含む認証情報が初期化されます。
- この手順の実行後，Hitachi Command Suite 製品の URL を確認し，変更がある場合は，再度設定してください。

  Hitachi Command Suite 製品の URL を確認する場合，次のコマンドを実行します。

  ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64chgurl /list

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. 次のコマンドを実行して，HiRDB を起動します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64dbsrv /start

3. 次のコマンドを実行して，データベースをバックアップします。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64dbtrans /export /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞

注意事項

- ＜*作業用フォルダ*＞には，データベース情報を一時的に格納するためのフォルダを絶対パス名で指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，エクスポート処理が中断します。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。
- ＜*アーカイブファイル*＞には，エクスポートするデータベースのアーカイブファイルを絶対パス名で指定します。
- アーカイブファイルの作成先のディスク容量が不足している場合，データベースのエクスポート時に，アーカイブファイルの作成に失敗します。

4. ローカルディスクにデータベースシステムを再作成します。

次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64dbinit /databasepath ＜*データベースの再作成先フォルダ*＞

コマンド実行前に＜*データベースの再作成先フォルダ*＞は削除，または空にしておいてください。

＜*データベースの再作成先フォルダ*＞は，ローカルディスク上に配置します。63 バイト以内の絶対パスで指定してください。

＜*データベースの再作成先フォルダ*＞に使用できる文字を次に示します。

A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。

5. 手順 3 でエクスポートしたデータベースをインポートします。

次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64dbtrans /import /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞ /type ALL

注意事項

- ＜*作業用フォルダ*＞には，アーカイブファイルを展開するためのフォルダを絶対パス名で指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，インポート処理が中断します。データベース情報を一時的に格納するためのフォルダを絶対パス名で指定します。
- ＜*アーカイブファイル*＞には，手順 3 で指定したデータベースのアーカイブファイルを，絶対パス名で指定します。
- アーカイブファイルを使用しない場合は，＜*作業用フォルダ*＞には手順 3 で指定したデータベース情報を格納したフォルダを指定します。このとき，指定したフォルダ以下のファイル構成は変更しないでください。また，/file オプションは指定しないでください。

6. HiRDB が使用するポート番号を変更して運用している場合は，ポート番号を設定し直します。

hcmds64dbinit コマンドを実行すると，HiRDB が使用するポート番号の設定がデフォルト値（22032）に戻るため，ポート番号を設定し直してください。

3.4.5 Global Link Manager のデータベースの格納先の変更（クラスタ環境の場合）

ここでは，Windows Server Failover Clustering を使用している場合に，Windows クラスタ環境のデータを移動する手順について説明します。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

注意事項

- この手順を実施すると，同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，ほかの Hitachi Command Suite 製品のデータベースファイルの格納先も変更されます。その場合，変更先のディスクの空き容量には，Global Link Manager のデータベースファイルの容量のほかに，ほかの Hitachi Command Suite 製品のデータベースファイルの容量も必要になります。インストールされている Hitachi Command Suite 製品全体のデータベースファイルの容量を考慮して，ディスクの空き容量を確保してください。ほかの Hitachi Command Suite 製品のデータベースファイルの容量については，各製品のマニュアルを参照してください。
- この手順で使用する hcmds64dbclustersetup コマンドを実行すると，HiRDB が使用するポートの設定がデフォルト値（22032）に戻ります。ポート番号を変更して運用している場合は，あとで設定し直す必要があるので，使用しているポート番号を控えておいてください。

(1) 実行系ノードでの手順

1. 実行系ノードで，Hitachi Command Suite 共通コンポーネントのサービスがオンラインで，実行系ノードがサービスと共有ディスクを所有していることを確認します。
2. 次のコマンドを実行して，Global Link Manager のサービスをオフラインにします。
   この手順によって，ほかの Hitachi Command Suite 製品がインストールされている場合は，それらのサービスもオフラインになります。

   Hitachi Command Suite v8.1.2 以降の製品がインストールされている場合：

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞
   ¥ClusterSetup¥hcmds64clustersrvstate /soff /r *＜リソースグループ名＞*

   Hitachi Command Suite v8.1.2 以降の製品がインストールされていない場合：

   ＜インストール DVD-ROM をセットしたドライブ＞:¥HGLM¥Hbase¥ClusterSetup
   ¥hcmds64clustersrvstate /soff /r *＜リソースグループ名＞*

   hcmds64clustersrvstate コマンドのオプションは次のとおりです。

   - /soff
     クラスタ管理アプリケーションに設定した Hitachi Command Suite 製品のサービスをオフラインにし，フェールオーバーを抑止します。
   - /r
     リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

     , ; = スペース

     また，次に示す文字は使用できません。

     ! " &) * ^ | < >
3. 次のコマンドを実行して，データベースの内容をローカルディスク上の退避データ格納先フォルダにバックアップしたあと，指定した共有ディスクのフォルダにデータベースを再作成します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64dbclustersetup /createcluster /databasepath ＜*共有ディスク上のデータベース再作成先フォルダ*＞ /exportpath ＜*ローカルディスク上の退避データ格納先フォルダ*＞ /auto

＜*共有ディスク上のデータベース再作成先フォルダ*＞

クラスタ環境で使用する共有ディスク上のデータベースの再作成先フォルダを指定します。

＜*ローカルディスク上の退避データ格納先フォルダ*＞

移行する前のデータベースを退避するフォルダを指定します。

注意

- hcmds64dbclustersetup の実行前に，＜*共有ディスク上のデータベース再作成先フォルダ*＞および＜*ローカルディスク上の退避データ格納先フォルダ*＞を削除または空にしておいてください。
- hcmds64dbclustersetup を実行すると，HiRDB が使用するポートのポート番号がデフォルト値（22032）に戻ります。
- 共有ディスク上の＜*共有ディスク上のデータベースの再作成先フォルダ*＞には，次に示すデータベース容量を合計した空き容量が必要です。

  空き容量不足が原因で hcmds64dbclustersetup コマンドの実行に失敗した場合は，フォルダの空き容量を増やし，hcmds64dbclustersetup コマンドを再度実行してください。

  - Hitachi Command Suite 共通コンポーネントのデータベース容量
  - Global Link Manager と同一ホストにインストールされているすべての Hitachi Command Suite 製品（Global Link Manager を含む）のデータベース容量
- hcmds64dbclustersetup コマンドが正常終了するまでは，共有ディスクを実行系ノードから切り離さないでください。hcmds64dbclustersetup コマンドが異常終了した状態でホストを再起動すると，共有ディスクの接続先が待機系ノードに切り替わることがあります。
- auto オプションを使用すると，コマンド実行後に Hitachi Command Suite 共通コンポーネントおよび HiRDB が停止された状態になります。
- 共有ディスク上の＜*共有ディスク上のデータベース再作成先フォルダ*＞のパスを指定してください。ローカルディスク上の＜*ローカルディスク上の退避データ格納先フォルダ*＞のパスを指定してください。
- ＜*共有ディスク上のデータベース再作成先フォルダ*＞および＜*ローカルディスク上の退避データ格納先フォルダ*＞は，63 バイト以内の絶対パスを指定してください。
- ＜*共有ディスク上のデータベース再作成先フォルダ*＞および＜*ローカルディスク上の退避データ格納先フォルダ*＞に使用できる文字を次に示します。

  A～Z，a～z，0～9，「.」，「_」

  パス区切り文字として「¥」，「:」，「/」も使用できます。

4. パス稼働情報のレポート出力機能を使用していた場合は，すでに出力済みのパス稼働情報（パスステータスログ）をデータベースの格納先の共有ディスクへ移動します。レポート出力機能を使用しない場合は，手順 4～6 は不要です。手順 7 へ進んでください。

   パス稼働情報（パスステータスログ）をエクスポートします。

   次のコマンドを実行してください。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamexport /dir ＜*エクスポート先フォルダ名*＞

   ＜*エクスポート先フォルダ名*＞は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   ＜*エクスポート先フォルダ名*＞に使用できる文字を次に示します。

   A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

   コマンドの実行例を次に示します。

```
"C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglamexport" /dir "C:
¥hglamexport"
```

5. プロパティファイル（server.properties）を編集します。

   server.properties ファイルの格納先を次に示します。

   ＜*Global Link Manager インストールフォルダ*＞¥conf

   レポートの保存先フォルダを，データベースの格納先の共有ディスク上のフォルダに変更します。

   server.pathreport.log_location に＜*レポートの保存先フォルダ*＞を指定します。＜*レポートの保存先フォルダ*＞は，データベースの格納先の共有ディスク上に配置します。150 バイト以内の絶対パスで指定してください。パスの区切り文字の (¥) は，2 つ続けて指定してください。

   記述例を次に示します。

   ```
   server.pathreport.log_location=E:¥¥HGLAM¥¥pathreport
   ```

6. パス稼働情報（パスステータスログ）をインポートします。

   次のコマンドを実行してください。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamimport /report ＜*エクスポートデータ格納先フォルダ名*＞

   ＜*エクスポートデータ格納先フォルダ名*＞には，hglamexport コマンドでエクスポートしたローカルディスク上の退避データ格納先フォルダを絶対パスで指定します。

   注意事項

   コマンド実行前に手順 5 で指定した保存先のフォルダは削除，または空にしておいてください。

   フォルダが空ではない場合，フォルダの中身は削除されます。

7. Global Link Manager が使用するサービスを登録しているグループを待機系に切り替えます。

   Global Link Manager が使用するサービスは次の 5 つです。

   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Global Link Manager Web Service
   - HiRDB/ClusterService _HD1

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用する場合：

   フェールオーバークラスタ管理で Global Link Manager が使用するサービスを登録しているリソースグループを右クリックし，［このサービスまたはアプリケーションを別のノードに移動］を選択します。

   Microsoft Failover Cluster（Windows Server 2012）を使用する場合：

   フェールオーバークラスタマネージャーで Global Link Manager が使用するサービスを登録している役割を右クリックし，［移動］－［ノードの選択］を選択します。

(2) 待機系ノードでの手順

1. 待機系ノードで，Hitachi Command Suite 共通コンポーネントのサービスおよび共有ディスクを，待機系ノードが所有していることを確認します。
2. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントのサービスが停止していることを確認します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64srv /status
サービスが停止していない場合，次のコマンドを実行して，Global Link Manager のサービスをオフラインにします。

この手順によって，ほかの Hitachi Command Suite 製品がインストールされている場合は，それらのサービスもオフラインになります。

Hitachi Command Suite v8.1.2 以降の製品がインストールされている場合：

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞
¥ClusterSetup¥hcmds64clustersrvstate /soff /r ＜*リソースグループ名*＞

Hitachi Command Suite v8.1.2 以降の製品がインストールされていない場合：

＜*インストール DVD-ROM をセットしたドライブ*＞:¥HGLM¥Hbase¥ClusterSetup
¥hcmds64clustersrvstate /soff /r ＜*リソースグループ名*＞

hcmds64clustersrvstate コマンドのオプションは次のとおりです。

- /soff

  クラスタ管理アプリケーションに設定した Hitachi Command Suite 製品のサービスをオフラインにし，フェールオーバーを抑止します。

- /r

  リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

  , ; = スペース

  また，次に示す文字は使用できません。

  ! " &) * ^ | < >

3. 次のコマンドを実行して，データベースの内容をローカルディスク上の退避データ格納先フォルダにバックアップしたあと，指定した共有ディスクのデータベース再作成先フォルダを使用するように設定を変更します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64dbclustersetup /createcluster /databasepath ＜*共有ディスク上のデータベース再作成先フォルダ*＞ /exportpath ＜*ローカルディスク上の退避データ格納先フォルダ*＞ /auto

＜*共有ディスク上のデータベース再作成先フォルダ*＞には，実行系ノードでデータベースを共有ディスクに移行したときに指定したフォルダと同じフォルダを指定してください。

＜*共有ディスク上のデータベース再作成先フォルダ*＞

実行系ノードで指定した，クラスタ環境で使用する共有ディスク上のデータベースの再作成先フォルダを指定します。

＜*ローカルディスク上の退避データ格納先フォルダ*＞

移行する前のデータベースを退避するフォルダを指定します。

注意

- hcmds64dbclustersetup の実行前に，＜*共有ディスク上のデータベース再作成先フォルダ*＞および＜*ローカルディスク上の退避データ格納先フォルダ*＞を削除または空にしておいてください。
- auto オプションを使用すると，コマンド実行後に Hitachi Command Suite 共通コンポーネントおよび HiRDB が停止された状態になります。
- ＜*ローカルディスク上の退避データ格納先フォルダ*＞には，ローカルディスク上のフォルダを指定します。
- ＜*ローカルディスク上の退避データ格納先フォルダ*＞は，63 バイト以内の絶対パスを指定してください。
- ＜*ローカルディスク上の退避データ格納先フォルダ*＞に使用できる文字を次に示します。

  A～Z，a～z，0～9，「.」，「_」

パス区切り文字として「¥」,「:」,「/」も使用できます。

4. パス稼働情報のレポート出力機能を使用する場合は，プロパティファイル（server.properties）を編集します。

   server.properties ファイルの格納先を次に示します。
   ＜*Global Link Manager インストールフォルダ*＞¥conf

   レポートの保存先フォルダを，共有ディスク上のフォルダに変更します。

   server.pathreport.log_location に＜*レポートの保存先フォルダ*＞を指定します。＜*レポートの保存先フォルダ*＞は，実行系ノードで指定したフォルダと同じフォルダを指定してください。

5. Global Link Manager が使用するサービスを登録しているグループを実行系に切り替えます。

   Global Link Manager が使用するサービスは次の 5 つです。

   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Global Link Manager Web Service
   - HiRDB/ClusterService _HD1

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用する場合：

   フェールオーバークラスタ管理で Global Link Manager が使用するサービスを登録しているリソースグループを右クリックし，［このサービスまたはアプリケーションを別のノードに移動］を選択します。

   Microsoft Failover Cluster（Windows Server 2012）を使用する場合：

   フェールオーバークラスタマネージャーで Global Link Manager が使用するサービスを登録している役割を右クリックし，［移動］－［ノードの選択］を選択します。

6. 次のコマンドを実行して，リソースグループおよび Global Link Manager 製品のサービスをオンラインにします。

   Hitachi Command Suite v8.1.2 以降の製品がインストールされている場合：

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞
   ¥ClusterSetup¥hcmds64clustersrvstate /son /r ＜*リソースグループ名*＞

   Hitachi Command Suite v8.1.2 以降の製品がインストールされていない場合：

   ＜*インストール DVD-ROM をセットしたドライブ*＞:¥HGLM¥Hbase¥ClusterSetup
   ¥hcmds64clustersrvstate /son /r ＜*リソースグループ名*＞

   hcmds64clustersrvstate コマンドのオプションは次のとおりです。

   - /son

     クラスタ管理アプリケーションに設定した Hitachi Command Suite 製品のサービスをオフラインにし，フェールオーバーを抑止します。

   - /r

     リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

     , ; = スペース

     また，次に示す文字は使用できません。

     ! " &) * ^ | < >

注意事項

Microsoft Failover Cluster を使用している場合で，HBase 64 Storage Mgmt Web Service が起動しない場合は，HBase 64 Storage Mgmt Web Service を［サービス］ウィンドウで起動後，フェールオーバークラスタ管理でサービスをオンラインにしてください。

3.5 Global Link Manager の環境設定の変更

Global Link Manager の環境設定を変更するには，変更する内容に応じてプロパティファイルを修正してください。

プロパティファイルの場所

＜*Global Link Manager インストールフォルダ*＞¥conf

プロパティファイルの種類

- server.properties（Global Link Manager サーバの設定用）
- logger.properties（Global Link Manager のログファイルの設定用）
- database.properties（Global Link Manager のデータベースの設定用）

プロパティファイルの書式

```
＜プロパティ名＞=＜値＞
#＜注釈＞
```

- ＜*プロパティ名*＞と＜*値*＞は「=」で区切ります。
- ＜*注釈*＞を指定する場合，行の先頭に「#」を付けます。

プロパティファイルの編集手順

1. プロパティファイルをテキストエディターなどで開き，プロパティを編集します。
   各プロパティに指定する値については，次の項を参照してください。
   - 「3.5.1 Global Link Manager サーバの設定の変更」
   - 「3.5.2 Global Link Manager のログファイルの設定の変更」
   - 「3.5.3 Global Link Manager のデータベースの設定の変更」
2. Global Link Manager を再起動します。
   Global Link Manager を再起動するには，いったんサービスを停止してから，再度サービスを起動します。サービスの起動および停止については，「3.2 Global Link Manager の起動と停止」を参照してください。

   注意事項

   server.properties ファイルまたは database.properties ファイルのプロパティの書式または値が不正な場合，Hitachi Command Suite 共通コンポーネントが起動されても，Global Link Manager は起動されません。Global Link Manager のメッセージログファイル（HGLAM_Message ＜*n*＞.log）に「KAIF10002-E」のメッセージが出力されているかどうかを確認してください。「KAIF10002-E」のメッセージが出力されている場合，「KAIF10002-E」およびその直前に出力される「KAIF24101-E」を参照し，エラーに対処したあとで，Global Link Manager を再起動してください。プロパティの値が未設定の場合および logger.properties ファイルの値または書式が不正な場合は，デフォルト値が適用され，Global Link Manager が起動されます。

   Global Link Manager のメッセージログファイルは次の場所に格納されます。

＜*Global Link Manager* のインストールフォルダ＞¥logs

3.5.1 Global Link Manager サーバの設定の変更

Global Link Manager サーバの設定を変更する場合，server.properties ファイルの各プロパティの値を変更します。プロパティの値の入力規則は次のとおりです。

- ASCII コードの文字を指定します。
- true または false を指定する場合，それ以外の値が指定されたときは，false が指定されたものとします。
- フォルダを指定する場合，パスの区切り文字 (¥) は 2 つ続けて入力します。

  記述例：

  ```
  server.pathreport.log_location=C:¥¥Program Files¥¥HiCommand¥¥HGLAM¥
  ¥pathreport
  ```

Global Link Manager サーバの設定を変更するためのプロパティの一覧を次の表に示します。

表 3-3 サーバの設定を変更するためのプロパティ（server.properties）

項番	プロパティ名	内容
1	server.thread.max_size	同時実行スレッドの最大数を指定します。 注意事項 この値は，次のプロパティで指定した値の合計より大きい値を指定してください。 ◦ server.auto_refresh.thread_num ◦ server.network_scan.thread_num 指定できる値：1～50（個） デフォルト値：15
2	server.task.max_queue_size	タスクキューの最大数を指定します。この値は，Global Link Manager GUI から一度に操作できるホストの最大数になります。 注意事項 この値は通常変更しないでください。100 台以上のホストに対して操作する場合は，分割して操作してください。 指定できる値：100～10000（個） デフォルト値：100
3	server.dbms.sweep_init	サーバ起動時から初回の空きページを回収するまでの時間を指定します。 指定できる値：1～60（分） デフォルト値：5
4	server.dbms.sweep_interval	前回実行から次の空きページを回収するまでの間隔を指定します。 指定できる値：60～100000（分） デフォルト値：10080
5	server.agent.max_retry_count	処理中の共通エージェントコンポーネントに対して，処理が完了したかどうか確認するための最大リトライ回数を指定します。 指定できる値：1～350（回） デフォルト値：110
6	server.agent.timeout	HDLM からの応答が無かったときに，タイムアウトを検知する時間を指定します。 指定できる値：60～3600（秒） デフォルト値：1200

項番	プロパティ名	内容
7	server.snmp.trap	SNMP Trap 受信機能を有効にするかどうかを指定します。有効にする場合は true を，無効にする場合は false を指定します※6。 指定できる値：true または false デフォルト値：true※1
8	server.snmp.trap_port_num	SNMP Trap を受信するポート番号を指定します※6。 注意事項 Windows ファイアウォール機能を使用している場合，この値を変更した時は，Windows ファイアウォールの例外に登録しているポート番号も変更してください。 指定できる値：1～65535 デフォルト値：22620※1
9	server.snmp.trap_thread_num	SNMP Trap を処理するスレッド数を指定します。 指定できる値：1～10（個） デフォルト値：3
10	server.snmp.trap_max	SNMP Trap（アラート）を最大何件保持するかを指定します。 指定できる値：1000～30000（件） デフォルト値：10000
11	server.snmp.auto_set	ホストの追加時またはホスト情報の更新時に，そのホストに対してアラートの通知設定を自動で実行するかどうかを指定します。自動で実行する場合は true を，自動で実行しない場合は false を指定します。 注意事項 アラート通知をホストごとに設定する場合は，false を指定してください。 指定できる値：true または false デフォルト値：true※9
12	server.snmp.trap_community	SNMP Community 値を指定します※6。 指定できる値：15 文字以下の英数字(a～z，A～Z，0～9)※7 デフォルト値：public
13	server.snmp.trap_ip_address	SNMP Trap の通知先の IP アドレスを指定します。IPv4 アドレスで指定します。SNMP Trap の通知先は，Global Link Manager をインストールしたサーバになります。Global Link Manager をインストールしたサーバの IP アドレスを変更した場合は，このプロパティの値も必ず変更してください※6。 注意事項 Global Link Manager をインストールしたサーバの IP アドレスを変更した場合に，このプロパティの値を変更しないと，SNMP Trap を受信できなくなります。 指定できる値：15 文字以下の値 デフォルト値：–※1
14	server.snmp.trap_ipv6_address	SNMP Trap の通知先の IP アドレスを指定します。IPv6 アドレスで指定します。SNMP Trap の通知先は，Global Link Manager をインストールしたサーバになります。Global Link Manager をインストールしたサーバの IP アドレスを変更した場合は，このプロパティの値も必ず変更してください※6。 注意事項

項番	プロパティ名	内容
		Global Link Manager をインストールしたサーバの IP アドレスを変更した場合に，このプロパティの値を変更しないと，SNMP Trap を受信できなくなります。 指定できる値：39 文字以下の値 デフォルト値：–※1
15	gui.indicator.auto_refresh_interval	Global Link Manager GUI のダッシュボードの自動更新間隔を指定します。 指定できる値：1～10000（分） デフォルト値：1
16	server.snmp_transfer.enable	アラート転送を有効にするかどうかを指定します。有効にする場合は true を，無効にする場合は false を指定します。 注意事項 アラート転送を有効にした場合 snmp のバージョンが指定できます。詳細については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」のアラート転送設定ダイアログの説明個所を参照してください。 アラート転送を無効にした場合 アラート転送設定ダイアログで設定した内容が削除されます。 指定できる値：true または false デフォルト値：false
17	server.snmp_transfer.ip_address	アラート転送の転送先サーバの IP アドレスを指定します。IPv4 アドレスまたは IPv6 アドレスで指定します。 Global Link Manager サーバと転送先サーバとの間にファイアウォールが設置されている場合は，あらかじめファイアウォールに転送先サーバの IP アドレスやポート番号などの情報を設定しておいてください。 注意事項 次の値は指定しないでください。 ◦ server.snmp.trap_ip_address で指定した IP アドレス ◦ Global Link Manager サーバの IP アドレス（複数の IP アドレスを持っているマシンの場合，どの IP アドレスとも同じにしないでください） ◦ 「127.0.0.1」および「0.0.0.0」（IPv4 の場合） ◦ 「0:0:0:0:0:0:0:1」および「0:0:0:0:0:0:0:0」(IPv6 の場合) ◦ マルチキャストアドレス（IPv6 の場合） ネットワーク内のすべてのホストに同じマルチキャストアドレスを設定し，IPv4 のブロードキャストと同じ動作をさせた場合に限ります。 ◦ ブロードキャストアドレス（IPv4 の場合） 指定できる値：文字列 デフォルト値：なし
18	server.snmp_transfer.port_num	アラート転送の転送先サーバのポート番号を指定します。 Global Link Manager サーバと転送先サーバとの間にファイアウォールが設置されている場合は，あらかじめファイアウォールに転送先サーバの IP アドレスやポート番号などの情報を設定しておいてください。 指定できる値：1～65535（番号） デフォルト値：162

項番	プロパティ名	内容
19	server.snmp_transfer.critical_enable	アラート転送の際に Critical レベルのアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
20	server.snmp_transfer.error_enable	アラート転送の際に Error レベルのアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
21	server.snmp_transfer.warning_enable	アラート転送の際に Warning レベルのアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
22	server.snmp_transfer.information_enable	アラート転送の際に Information レベルのアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
23	server.snmp_transfer.path_enable	アラート転送の際にカテゴリーが Path のアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
24	server.snmp_transfer.host_enable	アラート転送の際にカテゴリーが Host のアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
25	server.snmp_transfer.hdlm_enable	アラート転送の際にカテゴリーが HDLM のアラートを転送するかどうかを指定します。転送する場合は true を，転送しない場合は false を指定します。 指定できる値：true または false デフォルト値：true※2
26	server.snmp.alert_refresh_enable	パス障害時のアラート受信時にホストの自動更新を有効にするかどうかを指定します※8。有効にする場合は true を，無効にする場合は false を指定します。 指定できる値：true または false デフォルト値：true
27	server.auto_refresh.enable	ホストの自動更新を有効にするかどうかを指定します。有効にする場合は true を，無効にする場合は false を指定します。 指定できる値：true または false デフォルト値：true
28	server.auto_refresh.interval	ホストの自動更新の更新間隔を指定します。 指定できる値：180～2880（分） デフォルト値：180
29	server.auto_refresh.thread_num	ホストの自動更新で同時に実行できる最大数を指定します。 注意事項 この値を変更するときは， server.network_scan.thread_num の値と合計

項番	プロパティ名	内容
		した値が，server.thread.max_size の値より小さくなるように指定してください。 指定できる値：1～50（個） デフォルト値：5
30	server.pathreport.enable	レポートを出力するために，Global Link Manager が HDLM からパス稼働情報（パスステータスログ）を取得するかどうかを指定します。取得する場合は true を，取得しない場合は false を指定します。※3 注意事項 ◦ この値を変更した場合は，ホストの情報を更新してください。 ◦ この値を true にした場合は，次の内容を確認してください。 • server.auto_refresh.enable が true であること。 • パス稼働情報（パスステータスログ）を取得するための十分なディスク空き容量があること。ホスト当たりに必要なログファイルのサイズは，server.pathreport.log_total_size_per_host を参照してください。 ◦ パス稼働情報（パスステータスログ）が不要となり，false を指定した場合，server.pathreport.log_location をデフォルト値に戻してください。デフォルト値に戻さない場合，値に指定したフォルダが作成されます。 指定できる値：true または false デフォルト値：false
31	server.pathreport.log_location	パス稼働情報（パスステータスログ）を保存するフォルダを指定します。このフォルダの配下には，サブフォルダ「¥PathStatusLog¥<*ホストの IP アドレス*>」が作成され，次の形式で CSV ファイルが出力されます。 PathStatusLog_<*ホストの IP アドレス*>_<*日付*>.csv IPv6 形式の場合，<*ホストの IP アドレス*>は「:」が「-」に置き換わります。 すでにパス稼働情報（パスステータスログ）を出力している場合に，保存するフォルダを変更するときは，出力済みのパス稼働情報（パスステータスログ）を変更後のフォルダへ移動する必要があります。移動する手順については，「(1)」を参照してください。 フォルダがデフォルト値の場合は，Global Link Manager のアンインストール時に削除されます。デフォルト値以外のフォルダを指定した場合は削除されないため，手動で削除する必要があります。 注意事項 ◦ ネットワーク上のパスは指定できません。ローカルディスクを指定してください。 ◦ デフォルト値以外が指定されている場合，server.pathreport.enable の設定に関係なくフォルダが作成されます。フォルダが作成できなかった場合，Global Link Manager の起動時にエラーとなります。

項番	プロパティ名	内容
		◦ このフォルダに格納されるファイルは，Global Link Manager GUI で出力するレポートに使用されるため，編集しないでください。レポートが正しく出力されないおそれがあります。 指定できる値：150 バイト以下の有効な絶対パス※4 デフォルト値：＜*Global Link Manager のインストールフォルダ*＞¥pathreport
32	server.pathreport.log_total_size_per_host	ホスト当たりのパス稼働情報（パスステータスログ）のサイズを指定します。 指定した値を超えた場合，ファイル名に含まれる日付の古いファイルから削除されます。必要に応じてバックアップを取得してください。大規模構成の場合，デフォルト値で約 90 日が目安となります。 指定できる値：10～1024（MB） デフォルト値：100
33	server.network_scan.thread_num	ネットワークスキャンで同時にホストを追加できる最大数を指定します。 注意事項 この値を変更するときは，server.auto_refresh.thread_num の値と合計した値が，server.thread.max_size の値より小さくなるように指定してください。 指定できる値：1～20（個） デフォルト値：3
34	server.trouble_detection.enable	パス障害検知機能を有効にするかどうかを指定します。有効にする場合は true を，無効にする場合は false を指定します。 指定できる値：true または false デフォルト値：true
35	server.alert_gathering.interval	アラートの E-mail 通知機能でアラート情報の集約期間を指定します。 指定できる値：0～1440（分） デフォルト値：10
36	server.alert_email.from.address	アラートの E-mail 通知機能で Global Link Manager サーバから送信する E-mail の送信元アドレスを変更する場合に指定します。 注意事項 ◦ 大文字と小文字は区別されます。 ◦ 「¥」を文字として使用する場合は，「¥¥」と記述してください。 指定できる値：E-mail アドレスのフォーマット（RFC822）に従った文字列 デフォルト値：なし（匿名アドレスを使用する）
37	gui.export.version	管理情報の CSV ファイルを出力するときに，Global Link Manager のどのバージョンの形式で出力するか指定します。値が指定されていない場合，または不正な値を指定した場合は，最新バージョンの形式で出力します。 指定できる値：5.0，5.6，5.7，6.0，6.1，6.2，6.3，7.2，7.3，7.6 または 8.0 デフォルト値：なし（最新バージョンの形式で出力する）
38	gui.report.version	レポートを出力するときに，Global Link Manager のどのバージョンの形式で出力するか指定します。値が指定されていない場合，または不正な値を指定した場合は，最新バージョンの形式で出力します。 指定できる値：7.2，7.6 または 8.0

項番	プロパティ名	内容
		デフォルト値：なし（最新バージョンの形式で出力する）
39	gui.id_take_over.view	gui.export.version または gui.report.version が v7.6 以前で，仮想 ID を使用する場合，次に示す情報を CSV ファイルにエクスポートするかどうか指定します。エクスポートする場合は true を，エクスポートしない場合は false を指定します。 ・ 物理 LDEV ID ・ 物理ストレージシステム名 ・ 物理 CHA 指定できる値：true または false デフォルト値：false
40	gui.physical.view	管理対象ホストから取得したパスが次の情報の場合，物理情報を Hitachi Global Link Manager 管理画面上のパス一覧に表示するかどうか指定します。表示する場合は true を，表示しない場合は false を指定します。 ・ ID take over ・ H-UVM 構成 注意事項 gui.export.version または gui.report.version が v8.0 以降の場合，CSV ファイルのエクスポートについて，H-UVM の物理情報を出力する場合は true を指定します。なお，gui.id_take_over.view が true の場合，ID take over の移行先の物理情報も出力します。物理情報を出力しない場合は false を指定します。 指定できる値：true または false デフォルト値：true
41	getlogs.pathreport.get_mode	Global Link Manager の保守情報※5 として，パス稼働情報（パスステータスログ）を取得する方法を指定します。 指定できる値：0～3 0：取得しない 1：すべてのホストを対象に，現在日から 90 日前までのログを取得する 2：特定のホストを対象に，ログの取得開始日と終了日を指定する（この値を指定する場合，getlogs.pathreport.host，getlogs.pathreport.startDate および getlogs.pathreport.endDate を設定してください） 3：server.pathreport.log_location で指定したフォルダすべてを取得する デフォルト値：0
42	getlogs.pathreport.host	Global Link Manager の保守情報※5 として，パス稼働情報（パスステータスログ）を取得する際に，対象となるホストの IP アドレスを指定します。IPv4 アドレスまたは IPv6 アドレスで指定します。複数指定する場合，コンマで区切って指定します。 getlogs.pathreport.get_mode の値が 2 の場合だけ，この値は有効となります。 指定できる値：文字列 デフォルト値：なし（すべてのホストを対象とする）
43	getlogs.pathreport.startDate	Global Link Manager の保守情報※5 として，パス稼働情報（パスステータスログ）を取得する開始日を指定します。 「yyyymmdd」の形式で指定します。 getlogs.pathreport.get_mode の値が 2 の場合だけ，この値は有効となります。 指定できる値：文字列

項番	プロパティ名	内容
		デフォルト値：なし（ファイル名の日付が最も古いものから取得する）
44	getlogs.pathreport.endDate	Global Link Manager の保守情報※5 として，パス稼働情報（パスステータスログ）を取得する終了日を指定します。「yyyymmdd」の形式で指定します。 getlogs.pathreport.get_mode の値が 2 の場合だけ，この値は有効となります。 指定できる値：文字列 デフォルト値：なし（ファイル名の日付が最新のものまで取得する）
45	server.https.enable	SSL 通信を有効にするかどうかを指定します。有効にする場合は true を，無効にする場合は false を指定します。 指定できる値：true または false デフォルト値：false
46	server.https.truststore	hglamkeytool ユーティリティで指定したトラストストアーファイルを指定します。255 バイト以内の絶対パスで指定します。 注意事項 ＜*インストーラーで指定したインストールフォルダ*＞¥¥Base64¥¥uCPSB11¥¥jdk¥¥lib¥¥security¥¥jssecacerts のように，シンボリックリンクを含むパスを指定した場合は，参照先が変わることがあります。 指定できる値：文字列 デフォルト値：なし
47	gui.hdlm_installer.downloadfromdvd.enable	DVD-ROM からの HDLM インストーラーのダウンロードを有効にするかどうかを指定します。有効にする場合は true を，無効にする場合は false を指定します。 指定できる値：true または false デフォルト値：true
48	gui.hdlm_installer.fromdvd.location	DVD-ROM のマウント先のフォルダを指定します。 gui.hdlm_installer.downloadfromdvd.enable の値が true の場合だけ，この値は有効となります。 指定できる値：文字列 デフォルト値：＜*Global Link Manager のインストール時に使用した DVD のドライブ*＞¥¥HGLM

注※1

インストール実行時に設定した値に置き換わります。

注※2

HDLM のホストでアラート転送を使用している場合，デフォルトでは，すべてのアラート情報を転送する設定になっているため，大量にアラート情報が転送されるおそれがあります。アラートを大量に転送させたくない場合，カテゴリーが Host のアラートだけを転送するように設定することをお勧めします。さらに，server.snmp.alert_refresh_enable を true に設定することで，SNMP Trap を受信するマシンがアラートを受信したときに，アラートを通知したホストを自動で更新するため，即時にアラートが転送されるようになります。

カテゴリーが Host のアラートだけを転送するには，次のプロパティを true に設定し，それ以外の※2 が付いているプロパティは false にしてください。

- server.snmp_transfer.host_enable
- server.snmp_transfer.critical_enable（Critical レベルのアラートを転送する場合）

- server.snmp_transfer.error_enable（Error レベルのアラートを転送する場合）

注※3

設定に関係なく，すでに取得していた情報はレポートとして出力できます。ただし，指定した期間のパス稼働情報（パスステータスログ）が存在しない場合には，レポートは情報が空のまま出力されます。

注※4

指定したフォルダ配下および出力される CSV ファイル（パス稼働情報ファイル）は，Windows のローカルシステムアカウント（SYSTEM）がフルコントロール権限である必要があります。また，このフォルダおよびファイルには，Windows のローカルシステムアカウント（SYSTEM）および Global Link Manager 管理者以外のアクセス権限は設定しないでください。

注※5

Global Link Manager の保守情報を取得する方法は，「7.3.1 Global Link Manager サーバの保守情報の一括採取」を参照してください。

注※6

この値を変更した場合は，SNMP の監視対象のホストに設定値を反映させるため，該当するホストの更新も必要です（ただしホスト更新時に該当するホストに値を反映させるためには，server.snmp.auto_set=true と設定されていることが前提となります）。

注※7

Global Link Manager に 6.4 以降のバージョンの HDLM が動作する HDLM ホストだけが登録されている環境に限り，英数字に加えて記号（`~!#$%()*+,-./:;?@[¥]^_{|}）も指定できます（ただし，「¥」を指定する場合は，「¥¥」と指定してください）。

注※8

パス障害のアラートは，次のメッセージを含みます。

- KAIF60100-E
- KAIF60145-E
- KAIF60155-E
- KAPL08022-E

注※9

インストール実行時の設定に応じて，server.snmp.trap と同じ値に置き換わります。

(1) パス稼働情報（パスステータスログ）の保存先フォルダを変更する場合

パス稼働情報（パスステータスログ）の保存先フォルダを変更する場合，出力済みのパス稼働情報（パスステータスログ）を変更後のフォルダへ移動する必要があります。次の手順を実行してください。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. パス稼働情報（パスステータスログ）をエクスポートします。

次のコマンドを実行してください。

＜Global Link Manager のインストールフォルダ＞¥bin¥hglamexport /dir *＜エクスポート先フォルダ名＞*

*＜エクスポート先フォルダ名＞*は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

*＜エクスポート先フォルダ名＞*に使用できる文字を次に示します。

A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

コマンドの実行例を次に示します。

```
"C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglamexport" /dir "C:¥hglam
export"
```

3. プロパティファイルの server.pathreport.log_location に保存先のフォルダ名を指定します。

   プロパティファイルの設定方法については，「3.5 Global Link Manager の環境設定の変更」を参照してください。

4. パス稼働情報（パスステータスログ）をインポートします。

   次のコマンドを実行してください。

   ＜Global Link Manager のインストールフォルダ＞¥bin¥hglamimport /report *＜エクスポートデータ格納先フォルダ名＞*

   *＜エクスポートデータ格納先フォルダ名＞*には，hglamexport コマンドでエクスポートしたデータの格納先フォルダを絶対パスで指定します。

   注意事項

   コマンド実行前に手順 3 で指定した保存先のフォルダは削除，または空にしておいてください。

   フォルダが空ではない場合，フォルダの中身は削除されます。

5. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを起動します。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin¥hcmds64srv /start

3.5.2 Global Link Manager のログファイルの設定の変更

Global Link Manager のログファイル（HGLAM_Message ＜*n*＞.log）の設定を変更する場合，logger.properties ファイルを変更します。Global Link Manager のログファイルの設定を変更するためのプロパティの一覧を次の表に示します。

表 3-4 ログファイルの設定を変更するためのプロパティ（logger.properties）

項番	プロパティ名	内容
1	logger.max_backup_index	ログファイルのバックアップの最大数を指定します。 指定できる値：1～16（個） デフォルト値：10
2	logger.max_file_size	ログファイルの最大サイズを指定します。 指定できる値：4096～2147483647（バイト）（4KB～約 2GB） デフォルト値：16777216（約 16MB）
3	logger.syslog_level	OS のイベントログまたは syslog に出力するレベル（しきい値）を指定します。 指定できる値：0，10，20，または 30（左から重要度の高い順）※ デフォルト値：0

項番	プロパティ名	内容
4	logger.log_level	ログファイルに出力するレベル（しきい値）を指定します。 指定できる値：0，10，20，または 30（左から重要度の高い順）※ デフォルト値：20

注※

ログファイルの出力レベルと，出力されるメッセージの内容を次に示します。

0：重大なエラー，優先度の高い情報

10：通常のエラー，通常の情報

20：警告

30：すべてのデバッグ情報

3.5.3 Global Link Manager のデータベースの設定の変更

Global Link Manager のデータベースの設定を変更する場合，database.properties ファイルを変更します。Global Link Manager のデータベースの設定を変更するためのプロパティの一覧を次の表に示します。

表 3-5 データベースの設定を変更するためのプロパティ（database.properties）

項番	プロパティ名	内容
1	database.poolsize	コネクションプール数を指定します。 指定できる値：4～20（個） デフォルト値：20
2	database.connection_check_interval	接続チェックの間隔を指定します。 指定できる値：600～7200（秒） デフォルト値：3600
3	database.connection_retry_times	接続リトライ回数を指定します。 指定できる値：18～180（回） デフォルト値：30
4	database.connection_retry_interval	接続リトライ間隔を指定します。 指定できる値：10～100（秒） デフォルト値：30
5	database.connectionpool_retry_times	コネクションプールからコネクションが取得できない場合のリトライ回数を指定します。 指定できる値：0～5（回） デフォルト値：3
6	database.connectionpool_retry_interval	コネクションプールからコネクションが取得できない場合のリトライ間隔を指定します。 指定できる値：1～180（秒） デフォルト値：15
7	database.transaction_retry_times	トランザクションリトライ回数を指定します。 指定できる値：0～10（回） デフォルト値：5
8	database.transaction_retry_interval	トランザクションリトライ間隔を指定します。 指定できる値：0～5（秒） デフォルト値：1

3.5.4 Global Link Manager のデータベースのパスワードの変更

Global Link Manager がデータベースにアクセスする際の認証パスワードを変更できます。

データベースのパスワードを変更する場合，hcmds64dbuser コマンドを使用します。

hcmds64dbuser コマンドの書式は次のとおりです。

コマンドの書式

```
hcmds64dbuser /type {GlobalLinkAvailabilityManager | HGLAM} {/newpass <パスワード> | /default}
```

コマンドは次の場所に格納されています。

<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥bin
¥hcmds64dbuser

オプションの説明

表 3-6 hcmds64dbuser コマンドのオプション

オプション	説明
/newpass <パスワード>	Global Link Manager がデータベースにアクセスする際の認証パスワードを指定します。このオプションで指定した値が認証パスワードになります。 このオプションを省略した場合，対話式の応答でパスワードを入力できます。 指定できる値：28 バイト以内の次の文字列 先頭に指定できる文字：A～Z，a～z，'¥'，'@'，'#' 先頭以外に指定できる文字：A～Z，a～z，0-9，'¥'，'@'，'#'
/default	認証情報の設定を初期値に戻します（HiRDB および Hitachi Command Suite 共通コンポーネントのリソース）。 クラスタ構成化やデータベースのバックアップのリストアなどをする場合に指定すると，認証情報の設定が初期値に戻ることで認証情報の再設定が不要となり，操作が簡略化できます。

注意事項

hcmds64dbuser コマンドは，Hitachi Command Suite 共通コンポーネントが稼働中でも実行できます。

3.6 Global Link Manager サーバの IP アドレスまたはホスト名の変更

Global Link Manager がインストールされている管理サーバの IP アドレスまたはホスト名を変更する場合は，Hitachi Command Suite 共通コンポーネントの設定ファイルも変更する必要があります。

3.6.1 Global Link Manager サーバの IP アドレスの変更

Global Link Manager がインストールされている管理サーバの IP アドレスを変更する方法を説明します。

注意事項

- Hitachi Command Suite 製品の設定ファイルを変更する前に管理サーバの IP アドレスを変更していた場合，変更後の IP アドレスを記録しておいてください。
- クラスタ構成ファイル（cluster.conf ファイル）の設定は変更しないでください。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

管理サーバの IP アドレスを変更する手順を次に示します。

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop
2. user_httpsd.conf ファイルを編集します。
   user_httpsd.conf ファイルの設定で変更前の IP アドレスが使用されている場合は，ホスト名または変更後の IP アドレスに変更します。user_httpsd.conf ファイルの設定ではホスト名を指定することをお勧めします。
   user_httpsd.conf ファイルの格納先を次に示します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥httpsd¥conf¥user_httpsd.conf
3. 管理サーバの IP アドレスを変更し，マシンを再起動します。
   Hitachi Command Suite 共通コンポーネントの設定ファイルを変更する前に，管理サーバの IP アドレスを変更してあった場合は，ここではマシンの再起動だけを実行してください。
4. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントのサービスが起動していることを確認します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /status
5. Global Link Manager にログインするための URL に IP アドレスを使用している場合は，設定を変更します。
   URL の変更方法については，「3.8.1 Global Link Manager にログインするための URL の変更」を参照してください。

なお，管理サーバの IP アドレスを変更した場合には，各 Hitachi Command Suite 製品の設定も見直す必要があります。変更が必要な設定については「3.6.3 Global Link Manager サーバの IP アドレスまたはホスト名の変更後に必要な設定」を参照してください。

3.6.2 Global Link Manager サーバのホスト名の変更

Global Link Manager がインストールされている管理サーバのホスト名を変更する方法を説明します。

注意事項

- ホスト名は 32 バイト以内である必要があります。また，使用できる文字は次のとおりです。
  A～Z a～z 0～9 -
  ただし，ホスト名の先頭と末尾にはハイフン（-）は使用できません。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

管理サーバのホスト名を変更する手順を次に示します。

1. ホスト名を変更する前に，変更前のホスト名を記録しておきます。
   hostname コマンドを実行して，ホスト名を確認してください（ipconfig /ALL コマンドでもホスト名を表示できます）。設定ファイルに指定するホスト名は，大文字と小文字を区別する必要があります。

2. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop
3. 管理クライアントと管理サーバとの通信に SSL を使用している場合は，再度 SSL の設定をします。
   変更後のホスト名を使用して，再度 SSL の設定を行ってください。SSL の設定については，「5.1 サーバとクライアント間のセキュリティ設定」を参照してください。
4. user_httpsd.conf ファイルを編集します。
   ServerName ディレクティブの値を変更後のホスト名に変更します。
   user_httpsd.conf ファイルの格納先を次に示します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥httpsd¥conf¥user_httpsd.conf
   管理クライアントと管理サーバとの通信に SSL を使用している場合は，さらに次の設定も変更します。
   - <VirtualHost>タグにホスト名が指定されている場合は，「*」に変更します。
   - <VirtualHost>タグ内の ServerName ディレクティブの値を変更後のホスト名に変更します。

   注意事項
   - httpsd.conf ファイルおよび hsso_httpsd.conf ファイルは編集しないでください。
5. クラスタ構成の場合，cluster.conf ファイルを編集します。
   仮想ホスト名，実行系ノードのホスト名，待機系ノードのホスト名のうち，該当するホスト名を変更後のホスト名に変更します。
   cluster.conf ファイルの格納先を次に示します。
   - ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥conf¥cluster.conf
6. 管理サーバのホスト名を変更し，マシンを再起動します。
   Hitachi Command Suite 共通コンポーネントの設定ファイルを変更する前に，管理サーバのホスト名を変更していた場合，マシンの再起動だけを実行してください。
7. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントのサービスが起動していることを確認します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /status
8. Global Link Manager にログインするための URL にホスト名を使用している場合は，設定を変更します。
   URL の変更方法については，「3.8.1 Global Link Manager にログインするための URL の変更」を参照してください。

なお，管理サーバのホスト名を変更した場合には，各 Hitachi Command Suite 製品の設定も見直す必要があります。変更が必要な設定については「3.6.3 Global Link Manager サーバの IP アドレスまたはホスト名の変更後に必要な設定」を参照してください。

3.6.3 Global Link Manager サーバの IP アドレスまたはホスト名の変更後に必要な設定

Global Link Manager サーバがインストールされている管理サーバの IP アドレスまたはホスト名を変更した場合に，Global Link Manager で必要な設定について説明します。同じマシンにほかの

Hitachi Command Suite 製品がインストールされている場合は，各製品のマニュアルを参照してください。

Global Link Manager では次の設定を見直してください。

ホスト一覧の設定

Global Link Manager GUI のホスト一覧でホストを再登録してください。ホストを再登録しないと，アラートが受信できません。ホストを再登録するには，ホスト一覧ですべてのホストをいったん削除し，そのあとで削除したホストを再び追加します。Global Link Manager GUI のホスト一覧については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

また，運用環境によっては，次の設定も見直す必要があります。

RADIUS サーバを利用してアカウントを認証している場合

exauth.properties ファイルの設定を見直してください。exauth.properties ファイルの設定方法については，「(1) exauth.properties ファイルの設定（認証方式が RADIUS の場合)」を参照してください。

3.7 Hitachi Command Suite 共通コンポーネントのポート番号の変更

Hitachi Command Suite 共通コンポーネントは次の表に示すポート番号を使用します。

表 3-7 Hitachi Command Suite 共通コンポーネントによって使用されるポート

ネットワークポート	説明
22015/tcp※	SSL 未対応の HBase 64 Storage Mgmt Web Service にアクセスするために使用されます。このポート番号を変更する場合は，「3.7.1 」を参照してください。
22016/tcp	Web ブラウザーによって，SSL 対応の HBase 64 Storage Mgmt Web Service にアクセスするために使用されます。このポート番号を変更する場合は，「3.7.1 」を参照してください。
22031/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（シングルサインオン）で使用されます。このポートを変更する場合は，「3.7.2 」を参照してください。
22032/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（HiRDB）で使用されます。このポート番号を変更する場合は，「3.7.3 」を参照してください。
22035/tcp 22037/tcp 22038/tcp 22125/tcp 22127/tcp 22128/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバとの通信）で使用されます。このポートを変更する場合は，「3.7.4 」を参照してください。
22036/tcp 22126/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（ネーミングサービス）で使用されます。このポートを変更する場合は，「3.7.5 」を参照してください。
22019/tcp から 22030/tcp，22033/tcp および 22034/tcp	予約済みのポート番号です。

注※

SSL を設定している場合でも使用されます。外部から管理サーバへの非 SSL 通信を遮断するには，user_httpsd.conf ファイルの編集が必要です。

Global Link Manager をインストールしたあとに，Hitachi Command Suite 共通コンポーネントのポート番号を変更する場合の手順を次に示します。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントのサービスを停止します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop

2. ポート番号を変更します。

   ポート番号の変更方法は，変更するポート番号によって異なります。変更するポート番号に応じて，次の個所を参照してください。

   - 「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」
   - 「3.7.2 Hitachi Command Suite 共通コンポーネントの内部通信（シングルサインオン）で使用するポート番号の変更」
   - 「3.7.3 Hitachi Command Suite 共通コンポーネントの内部通信（HiRDB）で使用するポート番号の変更」
   - 「3.7.4 Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバとの通信）で使用するポート番号の変更」
   - 「3.7.5 Hitachi Command Suite 共通コンポーネントの内部通信（ネーミングサービス）で使用するポート番号の変更」

3. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントのサービスを開始します。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /start

4. 次のポート番号を変更した場合には，Hitachi Command Suite 製品にアクセスするための URL を変更する必要があります。

   - 22015/tcp（HBase 64 Storage Mgmt Web Service へのアクセスに使用）

     非 SSL で管理サーバと管理クライアント間の通信を行うときには，URL を変更する必要があります。

   - 22016/tcp（SSL 対応の HBase 64 Storage Mgmt Web Service へのアクセスに使用）

     SSL で管理サーバと管理クライアント間の通信を行うときには，URL を変更する必要があります。

   URL の変更方法については，「3.8.1 Global Link Manager にログインするための URL の変更」を参照してください。

   なお，ファイアウォールが設置されている場合など，管理サーバと管理クライアントとの間のネットワーク環境によっては，URL の変更が不要なこともあります。

3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更

HBase 64 Storage Mgmt Web Service へのアクセスに使用されるポートを変更するには，user_httpsd.conf ファイルに記述されているポートの番号を変更する必要があります。

1. 次の場所にある user_httpsd.conf ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞
   ¥uCPSB11¥httpsd¥conf¥user_httpsd.conf

2. HTTP 通信のポート番号を変更する場合，デフォルトで 22015 と記述されている「Listen」の値を変更します。HTTPS 通信（SSL 使用）のポート番号を変更する場合，デフォルトで 22016 と記述されている，「Listen」※の値および「VirtualHost」の値を変更します。

```
Listen 22015
SSLDisable

Listen 22016
<VirtualHost www.example.com:22016>
```

   注※

   HBase 64 Storage Mgmt Web Service へのアクセスで SSL を有効にする場合でも，Listen 22015 行を削除したり，コメント行にしたりしないでください。

   外部から管理サーバへの非 SSL 通信を遮断するには，user_httpsd.conf ファイルの編集が必要です。

   SSL を使用する場合，ポート番号の変更のほかにも設定が必要になります。「5. 通信に関するセキュリティの設定」を参照してください。

3.7.2 Hitachi Command Suite 共通コンポーネントの内部通信（シングルサインオン）で使用するポート番号の変更

Hitachi Command Suite 共通コンポーネントの内部通信（シングルサインオン）で使用されるポートを変更するには，次のファイルに記述されているポートを変更する必要があります。

1. 次の場所にある user_hsso_httpsd.conf ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞
   ¥uCPSB11¥httpsd¥conf¥user_hsso_httpsd.conf

2. 「Listen」に次の形式でポート番号を指定します。
   Listen 127.0.0.1:＜*ポート番号*＞

3.7.3 Hitachi Command Suite 共通コンポーネントの内部通信（HiRDB）で使用するポート番号の変更

Hitachi Command Suite 共通コンポーネントの内部通信（HiRDB）で使用されるポートを変更するには，HiRDB.ini，pdsys および def_pdsys に記述されているポートを変更する必要があります。

(1) HiRDB.ini の編集

1. 次の場所にある HiRDB.ini ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥HDB¥CONF¥emb¥HiRDB.ini

2. 「PDNAMEPORT=22032」のポート番号を変更します。

(2) pdsys の編集

1. 次の場所にある pdsys ファイルを開きます。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥HDB¥CONF¥pdsys

2. 「pd_name_port=22032」のポート番号を変更します。

(3) def_pdsys の編集

1. 次の場所にある def_pdsys ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥database¥work¥def_pdsys

2. 「pd_name_port=22032」のポート番号を変更します。

3.7.4 Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバとの通信）で使用するポート番号の変更

Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバとの通信）で使用されるポートを変更するには，workers.properties ファイルおよび usrconf.properties ファイルに記述されているポートの番号を変更する必要があります。

(1) workers.properties の編集

22035/tcp を変更する場合

1. 次の場所にある workers.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥web¥redirector¥workers.properties
2. 「worker.HBase64StgMgmtSSOService.port=22035」のポート番号を変更します。

22125/tcp を変更する場合

1. 次の場所にある workers.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥web¥redirector¥workers.properties
2. 「worker.GlobalLinkManagerWebService.port=22125」のポート番号を変更します。

(2) usrconf.properties の編集

22035/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties

2. 「webserver.connector.ajp13.port=22035」のポート番号を変更します。

22037/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties

2. 「ejbserver.http.port=22037」のポート番号を変更します。

22038/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties
2. 「ejbserver.rmi.remote.listener.port=22038」のポート番号を変更します。

22125/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥¥GlobalLinkManagerWebService¥usrconf.properties
2. 「webserver.connector.ajp13.port=22125」のポート番号を変更します。

22127/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥¥GlobalLinkManagerWebService¥usrconf.properties
2. 「ejbserver.http.port=22127」のポート番号を変更します。

22128/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥¥GlobalLinkManagerWebService¥usrconf.properties
2. 「ejbserver.rmi.remote.listener.port=22128」のポート番号を変更します。

3.7.5 Hitachi Command Suite 共通コンポーネントの内部通信（ネーミングサービス）で使用するポート番号の変更

Hitachi Command Suite 共通コンポーネントの内部通信（ネーミングサービス）で使用されるポートを変更するには，usrconf.properties ファイルにポート番号を変更する必要があります。

22036/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties
2. 「ejbserver.rmi.naming.port=22036」のポート番号を変更します。

22126/tcp を変更する場合

1. 次の場所にある usrconf.properties ファイルを開きます。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥usrconf¥ejb¥¥GlobalLinkManagerWebService¥usrconf.properties
2. 「ejbserver.rmi.naming.port=22126」のポート番号を変更します。

3.8 Global Link Manager GUI を使用するための Global Link Manager サーバでの設定

Global Link Manager GUI を起動するための URL を変更する設定，および Global Link Manager GUI にリンクメニューを追加するための設定を説明します。

3.8.1 Global Link Manager にログインするための URL の変更

次に示す Global Link Manager の設定を変更した場合，Global Link Manager GUI を起動するための URL を変更する必要があります。

- Global Link Manager をインストールしたサーバの IP アドレスまたはホスト名
- HBase 64 Storage Mgmt Web Service が使用するポート番号
- SSL を使用するための設定，または SSL の使用を中止するための設定
- 非クラスタ構成からクラスタ構成へ変更

Global Link Manager GUI を起動するための URL を変更するには，次のコマンドを実行します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin
¥hcmds64chgurl /change *＜変更前の URL ＞ ＜変更後の URL ＞*

URL は「http://*＜サーバの IP アドレスまたはホスト名＞*:*＜HBase 64 Storage Mgmt Web Service のポート番号＞*」の形式で指定します。

注意事項

指定する URL は，プロトコルとポートを含む完全な URL である必要があります。IPv6 アドレスは使用できません。IPv6 環境ではホスト名で指定してください。次にその例を示します。

```
http://127.0.0.1:22015
http://hostname:22015
```

複数の Hitachi Command Suite 製品がインストールされているマシンで，Global Link Manager の URL だけを変更したい場合は，次のように指定します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin
¥hcmds64chgurl /change *＜変更後の URL ＞* /type GlobalLinkAvailabilityManager

*＜変更前の URL ＞*を確認する場合，次のコマンドを実行します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin
¥hcmds64chgurl /list

3.8.2 Global Link Manager GUI へのリンクメニューの追加

Global Link Manager GUI に，任意の Web アプリケーションや Web ページへのリンクを登録できます。リンクを登録すると，Global Link Manager GUI のグローバルタスクバーエリアに［起動］ー［リンク］メニューが追加されます。

リンクを登録するには，次のコマンドを実行します。

hcmds64link {/add | /delete } /file *＜ユーザー設定アプリケーションファイル＞*[/nolog] /user *＜ユーザー ID ＞* /pass *＜パスワード＞*

オプション

表 3-8 hcmds64link コマンドのオプション

項目	説明
/add	リンクを追加するときに指定します。
/delete	リンクを解除するときに指定します。
/file <*ユーザー設定アプリケーションファイル*>	リンク情報を登録するためのファイル（ユーザー設定アプリケーションファイル）を指定します。
/nolog	メッセージの出力をコマンドラインに制限します。ただし，このオプションを指定しても，オプションエラーのメッセージは表示されます。
/user <*ユーザー ID*> /pass <*パスワード*>	Global Link Manager にログインするためのユーザー ID およびパスワードを指定します。Global Link Manager 管理の Admin 権限を持つユーザー ID を指定してください。

ユーザー設定アプリケーションファイルの作成方法

<*ユーザー設定アプリケーションファイル*>に指定するファイルは，リンク情報を次の形式で作成しておきます。

表 3-9 ユーザー設定アプリケーションファイルの形式

```
@TOOL-LINK
@NAME <登録キー名>
@URL <起動用の URL>
@DISPLAYNAME <リンクダイアログでの表示名>
@DISPLAYORDER <リンクダイアログでの表示順>
@ICONURL <アイコンの URL>
@TOOL-END
```

表 3-10 ユーザー設定アプリケーションファイルに設定する項目

項目	説明
@TOOL-LINK	ユーザー設定アプリケーションファイルの開始キーです。この項目は必須です。
@NAME <*登録キー名*>	登録用のキーとして使用される情報です。<*登録キー名*>にはリンク情報が一意になるように名称を指定します。英数字を使って，256 バイト以内で指定します。この項目は必須です。
@URL <*起動用の URL*>	Global Link Manager GUI から起動する URL を指定します。<*起動用の URL*>は 256 バイト以内で指定します。IPv6 アドレスは使用できません。IPv6 環境ではホスト名で指定してください。
@DISPLAYNAME <*リンクダイアログでの表示名*>	リンクダイアログで表示するリンクの名称を指定します。<*リンクダイアログでの表示名*>は，Unicode のコードポイント U+10000～U+10FFFF の範囲で，80 文字以内で指定します。この項目を省略すると，「@NAME」に指定した値がリンクの名称になります。
@DISPLAYORDER <*リンクダイアログでの表示順*>	リンクダイアログで表示する順番を指定します。<*リンクダイアログでの表示順*>は，-2147483648～2147483647 の範囲で指定します。ここで設定した値が小さい順にリンクダイアログに表示されます。
@ICONURL <*アイコンの URL*>	リンクの横に表示するアイコンの場所を指定します。<*アイコンの URL*>は，256 バイト以内で指定します。IPv6 アドレスは使用できません。IPv6 環境ではホスト名で指定してください。
@TOOL-END	ユーザー設定アプリケーションファイルの終了キーです。この項目は必須です。

ユーザー設定のアプリケーションファイルは，ASCII コードで作成します。使用できる制御コードは CR および LF です。

表 3-11 ユーザー設定アプリケーションファイルの例

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 1
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

3.9 ファイアウォールを使用する場合の設定

ファイアウォールが設置されている場合，Global Link Manager をインストール後に Windows ファイアウォールを有効にした場合は設定が必要になります。

3.9.1 ファイアウォールを設置したネットワークでの設定

管理サーバと管理クライアント，管理サーバと管理ホストの間にファイアウォールが設置されている場合は，次の表に従って，各ポートで通信できるようにファイアウォールを設定してください。

表 3-12 管理サーバと管理クライアントの通信に必要なポート番号

ポート番号	通信元	通信先	備考
22015/tcp※	管理クライアント	管理サーバ	非 SSL 通信の場合に設定が必要です。
22016/tcp※	管理クライアント	管理サーバ	SSL 通信の場合に設定が必要です。

注※ ポート番号は可変です。管理サーバと管理クライアントの通信に使用するポート番号については，「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」を参照してください。

表 3-13 管理サーバと管理ホストの通信に必要なポート番号

ポート番号	通信元	通信先	備考
24041/tcp※	管理サーバ	管理ホスト	設定が必要です。
24042/tcp※	管理サーバ	管理ホスト	非 SSL 通信の場合に設定が必要です。
24045/tcp※	管理サーバ	管理ホスト	SSL 通信の場合に設定が必要です。
22620/udp※	管理ホスト	管理サーバ	SNMP Trap を受信する場合に設定が必要です。

注※ ポート番号は可変です。管理サーバと管理ホストとの通信に必要なポート番号については，「A.3 共通エージェントコンポーネントの設定の変更」を参照してください。SNMP Trap を受信する場合に必要なポート番号については，「3.5.1 Global Link Manager サーバの設定の変更」の`server.snmp.trap_port_num` を参照してください。

3.9.2 Windows ファイアウォールを有効にした場合の設定

Global Link Manager をインストールしたあとに Windows ファイアウォールを有効にした場合，Hitachi Command Suite 共通コンポーネントおよび SNMP Trap を受信するポート番号を Windows ファイアウォールに例外として登録する必要があります。例外として登録するには，次の手順を実行します。

1. 次のコマンドを実行し，Hitachi Command Suite 共通コンポーネントを例外として登録します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
   ¥hcmds64fwcancel.bat
2. Windows ファイアウォールのダイアログで SNMP Trap を受信するポート番号を例外として登録します。
   登録する項目は次のとおりです。
   名前：SNMP Trap を受信するポート番号を示す名前を指定します（例：HGLAM_SNMP）。
   ポート番号：SNMP Trap を受信するポート番号を指定します。プロトコルは［UDP］を選択してください。

3.10 ユーザーアカウントに関するセキュリティの設定

Global Link Manager では，ユーザーのパスワードが第三者に推測されないように，パスワードの条件（文字数，種別など）を設定できます。また，同じユーザー ID に対して不正なパスワードが繰り返し入力された場合に，そのユーザーアカウントを自動的にロックできます。ユーザーアカウントがロックされると，解除するまでロックされたユーザーアカウントを使ってログインすることはできません。なお，ロックされているユーザーがログインするときには，通常の認証エラーが通知され，ロックされていることはユーザー自身には通知されません。

セキュリティの設定は Global Link Manager GUI からも操作できます。ただし，クラスタ構成の環境の場合には，Global Link Manager GUI から設定すると実行系ノードだけに反映されます。待機系ノードに反映するときは，ノードを切り替えてから同一の設定を実施してください。Global Link Manager GUI での操作方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

外部認証サーバと連携してユーザー認証を行う場合，パスワードの管理やユーザーアカウントの制御は，外部認証サーバ側の設定が有効になります。ただし，Hitachi Command Suite 製品へ新規にユーザーを登録する際には，Hitachi Command Suite 製品で設定したパスワードの条件が適用されます。

注意事項

Hitachi Command Suite 共通コンポーネントのバージョン 5.1 以降をインストールすると，ユーザーアカウントのロック機能，およびパスワードの複雑性チェック機能が使用できるようになります。これらの機能は，すべての Hitachi Command Suite 製品のユーザーに対して有効になるので，バージョン 5.0 以前の Hitachi Command Suite 製品の操作で，次の現象が起こるおそれがあります。

- 正しいユーザー ID とパスワードを指定しても，ログインできない。
  ユーザーアカウントがロックされているおそれがあります。該当するアカウントのロックを解除するか，または新しいユーザーアカウントを登録するなどの適切な対処をしてください。
- パスワードが変更できない，またはユーザーアカウントが追加できない。
  指定したパスワードが，パスワードの入力規則に従っていないおそれがあります。出力されるメッセージに従って，適切なパスワードを指定してください。

3.10.1 ユーザー定義ファイルを使用したセキュリティの設定

ユーザー定義ファイルを使用して，ユーザーアカウントに対するセキュリティを設定する方法について説明します。

(1) security.conf ファイルを使用したセキュリティの設定

パスワードの条件や，アカウントのロックに関する設定は，security.conf ファイルを使って実施します。

security.conf ファイルは次のフォルダに格納されています。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥conf¥sec

security.conf ファイルでの設定値を変更した場合は，直ちに変更後の値が有効になります。security.conf ファイルで設定するパスワードの条件は，ユーザーアカウントを追加するとき，またはパスワードを変更するときに適用されます。既存のユーザーアカウントのパスワードには適用されないため，パスワードが設定した条件を満たしていない場合でも，システムにログインできます。

security.conf ファイルに設定する項目を次の表に示します。

表 3-14 security.conf ファイルに設定する項目

項番	プロパティ名	内容
1	password.min.length	パスワードの最小文字数を指定します。 指定できる値：1～256（文字） デフォルト値：4
2	password.min.uppercase	パスワードに含める大文字の最小数を指定します。0 を指定した場合，大文字の数に制限はなくなります。 指定できる値：0～256（文字） デフォルト値：0（制限なし）
3	password.min.lowercase	パスワードに含める小文字の最小数を指定します。0 を指定した場合，小文字の数に制限はなくなります。 指定できる値：0～256（文字） デフォルト値：0（制限なし）
4	password.min.numeric	パスワードに含める数字の最小数を指定します。0 を指定した場合，記号の数に制限はなくなります。 指定できる値：0～256（文字） デフォルト値：0（制限なし）
5	password.min.symbol	パスワードに含める記号の最小数を指定します。0 を指定した場合，記号の数に制限はなくなります。 指定できる値：0～256（文字） デフォルト値：0（制限なし）
6	password.check.userID	ユーザー ID と同じパスワードを設定できるようにするかを指定します。true を指定した場合，ユーザー ID と同じパスワードは設定できなくなります。false を指定した場合，ユーザー ID と同じパスワードを設定できます。 指定できる値：true または false デフォルト値：false
7	account.lock.num※1	ユーザーアカウントが自動的にロックされるまでの，ログインの失敗回数を指定します。ユーザーがログインに連続して失敗した回数が指定値に達すると，ユーザーアカウントが自動的にロックされます。0 を指定した場合，ユーザーがログインに何度失敗しても，ユーザーアカウントはロックされません。※2 指定できる値：0～10（回） デフォルト値：0

注※1

外部認証サーバで認証を行うユーザーの場合，この設定は無効です。

注※2

シングルサインオン機能を利用している場合

あるユーザーがほかの Hitachi Command Suite 製品でログインに失敗した回数も，そのユーザーの失敗回数としてカウントされます。ユーザーの失敗回数は，ログインに成功したとき，またはアカウントがロックされたときにクリアーされます。

失敗回数を変更したときのユーザーへの影響

失敗回数を変更しても，すでに変更後の失敗回数を超えているユーザーや，ユーザーアカウントがロックされているユーザーにはその時点では適用されません。

(2) user.conf ファイルを使用したセキュリティの設定

ビルトインアカウント（ユーザー ID：System）は，デフォルトでは自動ロックおよび手動ロックの対象外となっています。ビルトインアカウントを自動ロックおよび手動ロックできるようにするには，user.conf ファイルの account.lock.system プロパティで設定します。user.conf ファイルの格納先を次に示します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥conf

user.conf ファイルが存在しない場合は，新規に作成してください。

account.lock.system プロパティは次の形式で指定してください。

account.lock.system = ＜*値*＞

指定できる値は，true または false です。ビルトインアカウントをロックできるようにする場合は true を，ロックできないようにする場合は false を指定します。デフォルト値は false です。

true を指定した場合，ビルトインアカウントでのログインに連続して失敗した回数が security.conf ファイルの account.lock.num プロパティでの指定値に達すると，ビルトインアカウントが自動的にロックされます。

ビルトインアカウントのロックを有効にする場合の設定例を次に示します。

```
account.lock.system = true
```

user.conf ファイルの設定値を変更した場合は，次の操作が必要です。

- Global Link Manager を再起動してください。再起動するには，いったんサービスを停止してから，再度サービスを起動します。サービスの起動および停止については，「3.2 Global Link Manager の起動と停止」を参照してください。
- 管理サーバをクラスタ環境で運用している場合，実行系ノードと待機系ノードの user.conf ファイルの値を同じにする必要があります。実行系ノードの user.conf ファイルを変更したときは，待機系ノードの user.conf ファイルを同じ値に変更してください。

3.10.2 アカウントロックの解除

ユーザーアカウントのロックは，Global Link Manager GUI で解除します。ユーザーアカウントのロックを解除する方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

ただし，すべてのユーザーアカウントがロックされた場合，またはすべての User Management の Admin 権限ユーザーのアカウントがロックされた場合は，Global Link Manager GUI から解除す

ることができません。次の手順で User Management の Admin 権限ユーザーのアカウントロックを解除してください。

1. Hitachi Command Suite 共通コンポーネントが起動していることを確認します。

   次のコマンドを実行してください。

   ```
   <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥bin
   ¥hcmds64srv /status
   ```

   Hitachi Command Suite 共通コンポーネントが停止している場合は，「3.2.1 Global Link Manager の起動」を参照して起動してください。

2. User Management の Admin 権限ユーザーのアカウントロックを解除します。

   次のコマンドを実行してください。

   ```
   <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥bin
   ¥hcmds64unlockaccount /user <ユーザー ID > /pass <パスワード>
   ```

   引数の末尾に「¥」を指定する場合は，「¥」1 文字ごとに「¥」を追加してください。

   <パスワード>が「a¥b¥c¥」の場合の実行例を次に示します。

   ```
   hcmds64unlockaccount /user system /pass a¥b¥c¥¥
   ```

   <パスワード>が「a¥b¥c¥¥¥」の場合の実行例を次に示します。

   ```
   hcmds64unlockaccount /user system /pass a¥b¥c¥¥¥¥¥
   ```

   引数が「&」，「|」または「^」を含む場合は，記号 1 文字ごとに「"」で囲むか，記号の前に「^」を入力してください。<パスワード>が「&a&b&c&」の場合の実行例を次に示します。

   ```
   hcmds64unlockaccount /user system /pass ^&a^&b^&c^&
   ```

   <ユーザー ID >，<パスワード>には，User Management の Admin 権限ユーザーのアカウントのものを指定してください。

   対象のユーザーにパスワードが設定されていない場合は，hcmds64unlockaccount コマンドではロックを解除できません。

User Management の Admin 権限ユーザーのアカウントロックを解除したあと，このアカウントで Global Link Manager GUI にログインし，ほかのユーザーアカウントのロックを解除してください。

3.11 警告バナーの設定

バージョン 5.1 以降の Hitachi Command Suite 製品では，ログイン時のセキュリティリスク対策として，任意のメッセージ（警告バナー）を表示できます。不正なアクセスを試みようとする第三者に対し，事前に警告を発することで，データの破壊や情報の漏洩などのリスクを軽減できます。

ログイン画面に表示できるメッセージは，1,000 文字以内です。同じ内容のメッセージをロケールごとに別の言語で登録しておくと，Web ブラウザーのロケールに合わせて，メッセージを自動的に切り替えられます。

メッセージを設定する場合は，OS の Administrator 権限を持つユーザーでログインする必要があります。

警告バナーの設定は Global Link Manager GUI からも操作できます。ただし，クラスタ構成の環境の場合には，Global Link Manager GUI から設定すると実行系ノードだけに反映されます。待機

系ノードに反映するときは，ノードを切り替えてから同一の設定を実施してください。Global Link Manager GUI での操作方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

3.11.1 メッセージの編集

HTML ファイル形式でメッセージを編集します。使用できる最大文字数は 1,000 文字です。通常の文字のほかに，HTML タグを使用して，フォント属性の変更や任意の位置での改行などの操作もできます（タグも文字数としてカウントされます）。使用できる文字コードは Unicode（UTF-8）です。

メッセージに使用する文字は，文字コードが Unicode（UTF-8）であること以外，制限はありません。HTML の構文で使用する文字（<，>，"，'，&）を表示する場合は，HTML のエスケープシーケンスを使用してください。例えば，ログイン画面に「&」を表示する場合は，HTML ファイルでは「&」と記述します。表示するメッセージを任意の位置で改行したい場合，HTML タグの
を使用してください。メッセージ中で改行しても，登録時には無視されます。

メッセージの編集例を次に示します。

メッセージの編集例：

```
<center><b>警告</b></center>
これは{会社名}のコンピュータシステムです。このコンピュータシステムは，承認を受けた人だけがその業務のためにのみ使用できます。承認を受けない人からのアクセスや使用があった場合，侵入者として刑事，民事，および行政上の訴訟を提起する場合があります。<br>
犯罪捜査を含む公の目的のために，このコンピュータシステムに対するすべてのアクセスの履歴は，責任者によって傍受，記録，読み取り，複写，および開示される場合があります。アクセスした人に関する私的な機密情報についても機密性とプライバシーの要件に従って暗号化され，アクセス履歴として記録されます。このシステムを使用する人は，承認を受けているかどうかに関係なく，上記の条件に同意したものとみなします。このシステムにおいてプライバシーの権利はありません。
```

注意事項

メッセージを登録する際，HTML の構文のチェックおよび修正はされません。ユーザーが編集した状態のまま登録されるので，HTML の構文規則に従って正しく編集してください。メッセージ中の HTML の構文に問題がある場合，メッセージが正しく表示されないおそれがあります。

参考

英語（bannermsg.txt）と日本語（bannermsg_ja.txt）のメッセージのサンプルファイルが次の場所にあります。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥sample¥resource

このサンプルファイルはインストールの際に上書きされるため，利用する場合はコピーしたファイルを編集してください。

3.11.2 メッセージの登録

編集したメッセージを登録するには，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64banner /add /file ＜*ファイル名*＞ [/locale ＜*ロケール名*＞]

コマンドの実行例を次に示します。

```
"C:¥Program Files¥HiCommand¥Base64¥bin¥hcmds64banner" /add /file C:¥W_Banner¥wbfile1 /locale en
```

/locale <*ロケール名*>を省略して設定した場合，Global Link Manager GUI でも登録した内容を編集できます。ただし，Global Link Manager GUI で編集するときには使用できる HTML タグに制限があります。

Global Link Manager クライアントを複数のロケールで運用する場合には，<*ロケール名*>には，メッセージに使用した言語のロケールを指定することもできます。英語は en，日本語は ja です。

Global Link Manager GUI で表示される警告バナーのロケールは，Global Link Manager クライアントの Web ブラウザーに設定されている言語の優先順位に従います。

注意事項

指定したロケールのメッセージが，すでに登録されていた場合，上書き更新されます。

3.11.3 メッセージの削除

編集したメッセージを削除するには，次のコマンドを実行してください。

<*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*>¥bin
¥hcmds64banner /delete [/locale <*ロケール名*>]

コマンドの実行例を次に示します。

```
"C:¥Program Files¥HiCommand¥Base64¥bin¥hcmds64banner" /delete /locale en
```

<*ロケール名*>には，削除したいメッセージのロケールを指定します。英語は en，日本語は ja です。省略するとデフォルトのロケールを指定したことになります。

3.12 監査ログの採取

Global Link Manager をはじめ，日立のストレージ関連製品では，法規制，セキュリティ評価基準，業界ごとの各種基準に準拠していることなどを監査者や評価者に証明するために，監査ログを採取できます。日立のストレージ関連製品で採取できる監査ログを次の表に示します。

表 3-15 監査ログの種別と説明

種別	説明
StartStop	ハードウェアまたはソフトウェアの起動と終了を示す事象。 • OS の起動と終了 • ハードウェアコンポーネント（マイクロ含む）の起動と終了 • ストレージシステム上のソフトウェア，SVP 上のソフトウェア，Hitachi Command Suite 製品の起動と終了
Failure	ハードウェアまたはソフトウェアの異常を示す事象。 • ハードウェア障害 • ソフトウェア障害（メモリーエラーなど）
LinkStatus	機器間のリンク状態を示す事象。 • リンクアップまたはダウン
ExternalService	日立のストレージ関連製品と外部サービスとの通信結果を示す事象。 • RADIUS サーバ，LDAP サーバ，NTP サーバ，DNS サーバとの通信 • 管理サーバとの通信（SNMP）
Authentication	機器，管理者，またはエンドユーザーが接続また認証を試みて成功または失敗したことを示す事象。 • FC ログイン • 機器認証（FC-SP 認証，iSCSI ログイン認証，SSL サーバ/クライアント認証） • 管理者またはエンドユーザー認証

種別	説明
AccessControl	機器，管理者，またはエンドユーザーがリソースへのアクセスを試みて成功または失敗したことを示す事象。 ・ 機器のアクセスコントロール ・ 管理者またはエンドユーザーのアクセスコントロール
ContentAccess	重要なデータへのアクセスを試みて成功または失敗したことを示す事象。 ・ NAS 上の重要なファイルまたは HTTP サポート時のコンテンツへのアクセス ・ 監査ログファイルへのアクセス
ConfigurationAccess	管理者が許可された運用操作を実行し，操作が正常終了または失敗したことを示す事象。 ・ 構成情報の参照または更新 ・ アカウントの追加，削除などのアカウント設定の更新 ・ セキュリティの設定 ・ 監査ログ設定の参照または更新
Maintenance	保守操作を実行し，操作が正常終了または失敗したことを示す事象。 ・ ハードウェアコンポーネント増設または減設 ・ ソフトウェアコンポーネント増設または減設
AnomalyEvent	しきい値のオーバーなどの異常が発生したことを示す事象。 ・ ネットワークトラフィックのしきい値オーバー ・ CPU 負荷のしきい値オーバー ・ 内部に一時保存した監査ログの上限到達前通知やラップアラウンド
	異常な通信の発生を示す事象。 ・ 通常使用するポートへの SYN フラッド攻撃やプロトコル違反 ・ 未使用ポートへのアクセス（ポートスキャンなど）

採取できる監査ログは，製品ごとに異なります。Global Link Manager で採取できる監査ログの種別および監査事象について，次の項で説明します。ほかの製品の監査ログについては，それぞれのマニュアルを参照してください。

3.12.1 Global Link Manager で監査ログに出力する種別と監査事象

Global Link Manager で監査ログに出力する種別と，それに含まれる監査事象について説明します。種別には，次の種類があります。

- StartStop
- Authentication
- ConfigurationAccess

それぞれの監査事象には，重要度（Severity）が設定されています。

種別ごとの監査事象をそれぞれ表に示します。

表 3-16 StartStop の監査事象

種別の説明	監査事象	Severity	メッセージ ID
ソフトウェアの起動と終了	SSO サーバの起動成功	6	KAPM00090-I
	SSO サーバの起動失敗	3	KAPM00091-E
	SSO サーバの停止	6	KAPM00092-I

表 3-17 Authentication の監査事象

種別の説明	監査事象	Severity	メッセージ ID
管理者またはエンドユーザーの認証	ログインの成功	6	KAPM01124-I
	ログインの成功（外部認証サーバログイン）	6	KAPM02450-I
	ログインの失敗（ユーザー ID またはパスワードに誤りがある場合）	4	KAPM02291-W
	ログインの失敗（ロック中のユーザーでログイン）	4	KAPM02291-W
	ログインの失敗（存在しないユーザーでログイン）	4	KAPM02291-W
	ログインの失敗（権限なし）	4	KAPM01095-E
	ログインの失敗（認証失敗）	4	KAPM01125-E
	ログインの失敗（外部認証サーバ認証失敗）	4	KAPM02451-W
	ログアウトの成功	6	KAPM08009-I
	ログアウトの失敗	4	KAPM01126-W
アカウントの自動ロック	アカウントの自動ロック（認証の連続失敗またはアカウントの有効期限切れ）	4	KAPM02292-W

表 3-18 ConfigurationAccess の監査事象

種別の説明	監査事象	Severity	メッセージ ID
ユーザーの登録（GUI）	ユーザーの登録成功	6	KAPM07230-I
	ユーザーの登録失敗	3	KAPM07240-E KAPM07237-E KAPM07238-E
ユーザーの登録（GUI および CLI）	ユーザーの登録成功	6	KAPM07241-I
	ユーザーの登録失敗	3	KAPM07242-E
ユーザーの削除（GUI）	ユーザーの削除成功	6	KAPM07231-I
	ユーザーの削除失敗	3	KAPM07240-E
ユーザーの削除（GUI および CLI）	ユーザーの削除成功	6	KAPM07245-I
	ユーザーの削除失敗	3	KAPM07246-E
ユーザー情報の更新（GUI および CLI）	ユーザー情報の更新成功	6	KAPM07243-I
	ユーザー情報の更新失敗	3	KAPM07244-E
パスワードの変更（管理者画面から変更）	管理者によるパスワード変更成功	6	KAPM07232-I
	管理者によるパスワード変更失敗	3	KAPM07240-E KAPM07237-E
パスワードの変更（自ユーザー用画面から変更）	旧パスワードが正しいかどうかを判断するための認証処理で失敗	3	KAPM07239-E
	ログインユーザー自身のパスワード変更成功（自ユーザー画面から変更）	6	KAPM07232-I
	ログインユーザー自身のパスワード変更失敗（自ユーザー画面から変更）	3	KAPM07240-E KAPM07237-E
プロファイルの変更	プロファイルの変更成功	6	KAPM07233-I
	プロファイルの変更失敗	3	KAPM07240-E KAPM07238-E
権限の変更	権限の変更成功	6	KAPM02280-I
	権限の変更失敗	3	KAPM07240-E

種別の説明	監査事象	Severity	メッセージ ID
アカウントのロック	アカウントのロック成功※1	6	KAPM07235-I
	アカウントのロック失敗	3	KAPM07240-E
アカウントのロック解除	アカウントのロック解除成功※2	6	KAPM07236-I
	アカウントのロック解除失敗	3	KAPM07240-E
認証方式の変更	認証方式の変更成功	6	KAPM02452-I
	認証方式の変更失敗	3	KAPM02453-E
データベースのバックアップまたはリストア	hcmds64backups コマンドによるバックアップ成功	6	KAPM05561-I
	hcmds64backups コマンドによるバックアップ失敗	3	KAPM05562-E
	hcmds64db コマンドによる全体リストアの成功	6	KAPM05563-I
	hcmds64db コマンドによる全体リストアの失敗	3	KAPM05564-E
	hcmds64db コマンドによる部分リストアの成功	6	KAPM05565-I
	hcmds64db コマンドによる部分リストアの失敗	3	KAPM05566-E
データベースのデータの入出力	hcmdsdbmove コマンドによるデータ出力の成功	6	KAPM06543-I
	hcmdsdbmove コマンドによるデータ出力の失敗	3	KAPM06544-E
	hcmdsdbmove コマンドによるデータ入力の成功	6	KAPM06545-I
	hcmdsdbmove コマンドによるデータ入力の失敗	3	KAPM06546-E
認証データの入出力	hcmds64authmove コマンドによるデータ出力の成功	6	KAPM05832-I
	hcmds64authmove コマンドによるデータ出力の失敗	3	KAPM05833-E
	hcmds64authmove コマンドによるデータ入力の成功	6	KAPM05834-I
	hcmds64authmove コマンドによるデータ入力の失敗	3	KAPM05835-E
パスのオンラインまたはオフライン	パスのオンラインまたはオフラインの受付成功	6	KAIF50200-I
	パスのオンラインまたはオフラインの受付失敗	3	KAIF50201-E
	パスのオンラインまたはオフライン成功	6	KAIF50202-I
	パスのオンラインまたはオフライン一部失敗	4	KAIF50203-W
	パスのオンラインまたはオフライン失敗	3	KAIF50204-E
マルチパス LU 設定	マルチパス LU 設定の受付成功	6	KAIF50200-I
	マルチパス LU 設定の受付失敗	3	KAIF50201-E
	マルチパス LU 設定成功	6	KAIF50202-I
	マルチパス LU 設定一部失敗	4	KAIF50203-W
	マルチパス LU 設定失敗	3	KAIF50204-E

種別の説明	監査事象	Severity	メッセージ ID
HDLM 設定	HDLM 設定の受付成功	6	KAIF50200-I
	HDLM 設定の受付失敗	3	KAIF50201-E
	HDLM 設定成功	6	KAIF50202-I
	HDLM 設定一部失敗	4	KAIF50203-W
	HDLM 設定失敗	3	KAIF50204-E
アラート設定	アラート設定の受付成功	6	KAIF50200-I
	アラート設定の受付失敗	3	KAIF50201-E
	アラート設定成功	6	KAIF50202-I
	アラート設定一部失敗	4	KAIF50203-W
	アラート設定失敗	3	KAIF50204-E
パスの I/O 回数および I/O 障害回数のリセット	パスの I/O 回数および I/O 障害回数のリセットの受付成功	6	KAIF50200-I
	パスの I/O 回数および I/O 障害回数のリセットの受付失敗	3	KAIF50201-E
	パスの I/O 回数および I/O 障害回数のリセット成功	6	KAIF50202-I
	パスの I/O 回数および I/O 障害回数のリセット一部失敗	4	KAIF50203-W
	パスの I/O 回数および I/O 障害回数のリセット失敗	3	KAIF50204-E

注※1

パスワードが設定されていないユーザーの認証方式を変更したことによるアカウントのロックについては，監査ログに記録されません。

注※2

ユーザーにパスワードを設定したことによるアカウントのロックの解除については，監査ログに記録されません。

3.12.2 監査ログの環境設定ファイルの編集

Global Link Manager の監査ログを採取するには，環境設定ファイル（auditlog.conf）を編集する必要があります。環境設定ファイルの Log.Event.Category で採取する監査事象の種別を設定することで，監査ログを取得できるようになります。監査ログは Windows のイベントログに出力されます。イベントログの出力形式については，「7.4.1 イベントログの出力形式」を参照してください。

注意事項

監査ログを採取すると，イベントが大量に出力されます。イベントログのログサイズの変更，採取したログファイルの退避，保管などを実施してください。

auditlog.conf ファイルは次の場所にあります。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥conf¥sec

auditlog.conf ファイルに設定する項目を次の表に示します。

表 3-19 auditlog.conf に設定する項目

項目	説明
Log.Facility	使用しません。設定しても無視されます。

項目	説明
Log.Event.Category	採取する監査事象の種別を指定します。複数指定する場合は，「,（コンマ）」で区切ります。「,」と種別の間にスペースは入れないでください。デフォルトでは，種別が指定されていません。指定されていない場合，監査ログは出力されません。指定できる種別については，「3.12.1 」を参照してください。
Log.Level	採取する監査事象の重要度（Severity）を指定します。指定した値以下の重要度の項目が出力されます。Global Link Manager で出力する監査事象および監査事象の重要度（Severity）については，「3.12.1 」を参照してください。監査事象の重要度とイベントログの種類との対応については，「表 3-20 」を参照してください。 イベントログの種類に対応する監査事象の重要度を次に示します。例えば，エラーおよび警告を出力する場合，4 を指定します。 • エラー：3 • 警告：4 • 情報：6 指定できる値：0～7（重要度（Severity）） デフォルト値：6

次に監査事象の重要度とイベントログの種類との対応を示します。

表 3-20 監査事象の重要度とイベントログの種類との対応

監査事象の重要度	イベントログの種類
0	エラー
1	
2	
3	
4	警告
5	情報
6	
7	

次に auditlog.conf ファイルの例を示します。

```
# Specify an integer for Facility. (specifiable range: 1-23)
Log.Facility 1

# Specify the event category.
# You can specify any of the following:
# StartStop, Failure, LinkStatus, ExternalService,
# Authentication, AccessControl, ContentAccess,
# ConfigurationAccess, Maintenance, or AnomalyEvent.
Log.Event.Category Authentication,ConfigurationAccess

# Specify an integer for Severity. (specifiable range: 0-7)
Log.Level 6
```

この例の場合，Authentication または ConfigurationAccess の監査事象のうち，エラー，警告および情報の監査ログが出力されます。

3.12.3 監査ログの出力形式

監査ログは，Windows のイベントログに出力されます。イベントの出力形式とその内容を説明します。

イベントの出力形式

＜日付＞ ＜時刻＞ ＜種類＞ ＜ユーザー＞ ＜コンピュータ＞ ＜ソース＞ ＜分類＞ ＜イベント ID ＞ ＜説明＞

表 3-21 イベントログに出力される情報（監査ログ）

項目	内容
日付	メッセージが出力された日付が「yyyy/mm/dd」の形式で出力されます。
時刻	メッセージが出力された時刻が「hh:mm」の形式で出力されます。
種類	次の 3 つの種類があります。 ・ 情報 ・ 警告 ・ エラー
ユーザー	「N/A」と出力されます。
コンピュータ	コンピュータ名が表示されます。
ソース	「HBase64 Event」と出力されます。
分類	「なし」と出力されます。
イベント ID	「1」と出力されます。
説明	「*＜プログラム名＞* [*＜プロセス ID ＞*]: CELFSS」で始まるの監査ログのメッセージです。表示される内容の詳細は，「「説明」の出力形式」および「表 3-22 」を参照してください。

「説明」の出力形式

＜プログラム名＞ [*＜プロセス ID ＞*]: *＜統一識別子＞*,*＜統一仕様リビジョン番号＞*,*＜通番＞*,*＜メッセージ ID ＞*,*＜日付・時刻＞*,*＜検出エンティティ＞*,*＜検出場所＞*,*＜監査事象の種別＞*,*＜監査事象の結果＞*,*＜監査事象の結果サブジェクト識別情報＞*,*＜ハードウェア識別情報＞*,*＜発生場所情報＞*,*＜ロケーション識別情報＞*,*＜ FQDN ＞*,*＜冗長化識別情報＞*,*＜エージェント情報＞*,*＜リクエスト送信元ホスト＞*,*＜リクエスト送信元ポート番号＞*,*＜リクエスト送信先ホスト＞*,*＜リクエスト送信先ポート番号＞*, *＜一括操作識別子＞*,*＜ログ種別情報＞*,*＜アプリケーション識別情報＞*,*＜予約領域＞*,*＜メッセージテキスト＞*

表 3-22 監査ログの「説明」に出力される情報

項目※1	内容
プログラム名	コンポーネント名やプロセス名が出力されます。
プロセス ID	プロセス ID が出力されます。
統一識別子	「CELFSS」と出力されます。
統一仕様リビジョン番号	「1.1」と出力されます。
通番	監査ログのメッセージの通番が出力されます。
メッセージ ID※2	メッセージ ID が出力されます。
日付・時刻	メッセージが出力された日付と時刻が「*yyyy-mm-ddThh:mm:ss.s ＜タイムゾーン＞*」の形式で出力されます。
検出エンティティ	コンポーネント名やプロセス名が出力されます。
検出場所	ホスト名が出力されます。
監査事象の種別	事象の種別が出力されます。
監査事象の結果	事象の結果が出力されます。
監査事象の結果サブジェクト識別情報	事象に応じて，アカウント ID，プロセス ID または IP アドレスが出力されます。
ハードウェア識別情報	ハードウェアの型名や製番が出力されます。

項目※1	内容
発生場所情報	ハードウェアのコンポーネントの識別情報が出力されます。
ロケーション識別情報	ロケーション識別情報が出力されます。
FQDN	完全修飾ドメイン名が出力されます。
冗長化識別情報	冗長化識別情報が出力されます。
エージェント情報	エージェント情報が出力されます。
リクエスト送信元ホスト	リクエストの送信元のホスト名が出力されます。
リクエスト送信元ポート番号	リクエストの送信元のポート番号が出力されます。
リクエスト送信先ホスト	リクエストの送信先のホスト名が出力されます。
リクエスト送信先ポート番号	リクエストの送信先のポート番号が出力されます。
一括操作識別子	プログラム内で操作の通番が出力されます。
ログ種別情報	「BasicLog」と出力されます。
アプリケーション識別情報	プログラムの識別情報が出力されます。
予約領域	出力されません。予約領域です。
メッセージテキスト※2	監査事象に応じた内容が出力されます。 メッセージテキストに含まれる「コマンド ID」は，Global Link Manager GUI から実行された 1 つの操作を一意に識別するための ID です。複数のメッセージに同じコマンド ID が含まれる場合，それらは 1 つの操作に対して出力されたメッセージであることを示します。

注※1 監査事象によっては，出力されない項目もあります。

注※2 監査事象に対応するメッセージ ID については，「3.12.1 Global Link Manager で監査ログに出力する種別と監査事象」を参照してください。メッセージ ID に対応するメッセージテキストについては，マニュアル「Hitachi Global Link Manager メッセージ」を参照してください。

監査事象「ログイン」の例

```
CELFSS,1.1,0,KAPM01124-I,2014-07-22T14:08:23.1+09:00,HBase-SSO,management-
host,Authentication,Success,uid=hoge,,,,,,,,,,,,BasicLog,,,"The login was
successful. (session ID = <セッション ID>)"
```

3.13 アラート転送の設定

アラート情報を Global Link Manager サーバから SNMP 転送先サーバに転送し，任意のアプリケーションで管理できます。

アラートを転送する場合，Global Link Manager の MIB ファイルを SNMP 転送先サーバに登録することで，Global Link Manager から受信したアラート情報を文字列に変換できるようになります。

登録する MIB ファイル（hglam.mib）は，次のフォルダに格納されています。
＜*Global Link Manager のインストール DVD-ROM のドライブ*＞:¥HGLM¥mib

アラート転送を有効にするかどうかや SNMP 転送先サーバについては，プロパティファイル（server.properties）で設定します。プロパティファイルの設定方法については「3.5 Global Link Manager の環境設定の変更」を参照してください。

3.14 外部認証サーバでユーザー認証するために必要な設定

Hitachi Command Suite 製品では，外部認証サーバと連携してユーザー認証できます。外部認証サーバに登録されているユーザー ID を Hitachi Command Suite 製品にも登録しておくことで，外部認証サーバに登録されたユーザー ID を使って，Hitachi Command Suite 製品にログインできます。このため，Hitachi Command Suite 製品でのログインパスワードの管理やアカウントの制御が不要になります。

また，外部認証サーバと外部認可サーバを併用することで，Hitachi Command Suite 製品に対するユーザーのアクセス権限を外部認可サーバで制御できます。外部認可サーバとも連携する場合，Hitachi Command Suite 製品では，ユーザーを外部認可サーバのグループ（認可グループ）ごとに管理するため，Hitachi Command Suite 製品での個々のユーザーのアカウント管理や権限設定が不要になります。

外部認証サーバや外部認可サーバと連携するために必要な設定は，外部認証サーバでの認証方式によって異なります。以降は認証方式ごとに説明します。

注意事項

- JP1/IM は Hitachi Command Suite 製品とは別の認証システムを利用しています。ここでの設定は JP1/IM で使用するユーザーアカウントの管理方法を変更するものではありません。
- 外部認証サーバと連携するための設定で実行するコマンドの引数に，コマンドラインの制御文字が含まれる場合には，コマンドラインの仕様に従い正しくエスケープしてください。また，「¥」はコマンドラインでは特殊な扱いとなるため，引数に「¥」が含まれる場合には注意が必要です。

  次の文字が含まれる場合は，引数を「"」で囲むか，1 文字ごとに「^」でエスケープしてください。

  空白文字 `&` `|` `^` `<` `>` `(` `)`

  「¥」は，次に続く文字によってはエスケープ文字として扱われることがあります。このため，引数に「¥」と上記の文字が含まれる場合には，「"」で囲まないで，上記文字を 1 文字ごとに「^」でエスケープしてください。

  また，引数の末尾に「¥」がある場合は，「¥」でエスケープしてください。

  例えば，`hcmds64radiussecret` コマンドで登録する共有秘密鍵が「`secret01¥`」の場合は，次のとおりエスケープしてください。

  ```
  hcmds64radiussecret /set secret01¥¥ /name ServerName
  ```

3.14.1 複数の外部認証サーバと連携している場合の構成

複数の外部認証サーバと連携している場合，冗長構成またはマルチドメイン構成でユーザー認証します。

それぞれの外部認証サーバで同一のユーザー情報を管理する構成を，冗長構成と呼びます。ある外部認証サーバに障害が発生しても，ほかの外部認証サーバでユーザー認証できます。

それぞれの外部認証サーバごとに異なるユーザー情報を管理する構成を，マルチドメイン構成と呼びます。ドメイン名を含んでいるユーザー ID でログインすると，入力したドメインの外部認証サーバでユーザー認証されます。外部認証サーバが Kerberos サーバの場合は，レルムごとに異なるユーザー情報を管理することで，マルチドメイン構成と同様の構成にできます。

冗長構成およびマルチドメイン構成に対応している外部認証サーバは次のとおりです。

表 3-23 冗長構成およびマルチドメイン構成のサポート状況

外部認証サーバ	冗長構成	マルチドメイン構成
LDAP ディレクトリサーバ	○※1	○※1
RADIUS サーバ	○	-
Kerberos サーバ	○	○※2

（凡例）

○：サポートしている

-：サポートしていない

注※1

冗長構成またはマルチドメイン構成のどちらか一方の構成にできます。

Active Directory のグローバルカタログを設定している場合は，冗長構成とマルチドメイン構成の両方を構成できます。

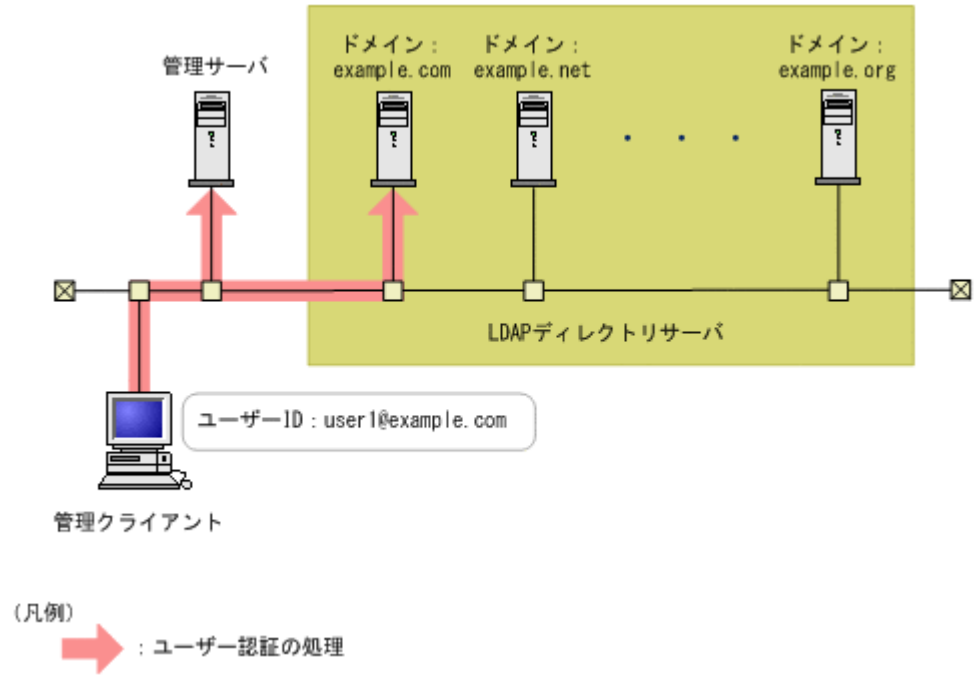
注※2

レルムごとに異なるユーザー情報を管理することで，マルチドメイン構成と同様の構成にできます。

マルチドメイン構成の LDAP ディレクトリサーバでユーザー認証する場合，ログイン時のユーザー ID にドメイン名を含んでいるかどうかで，ユーザー認証の処理が異なります。

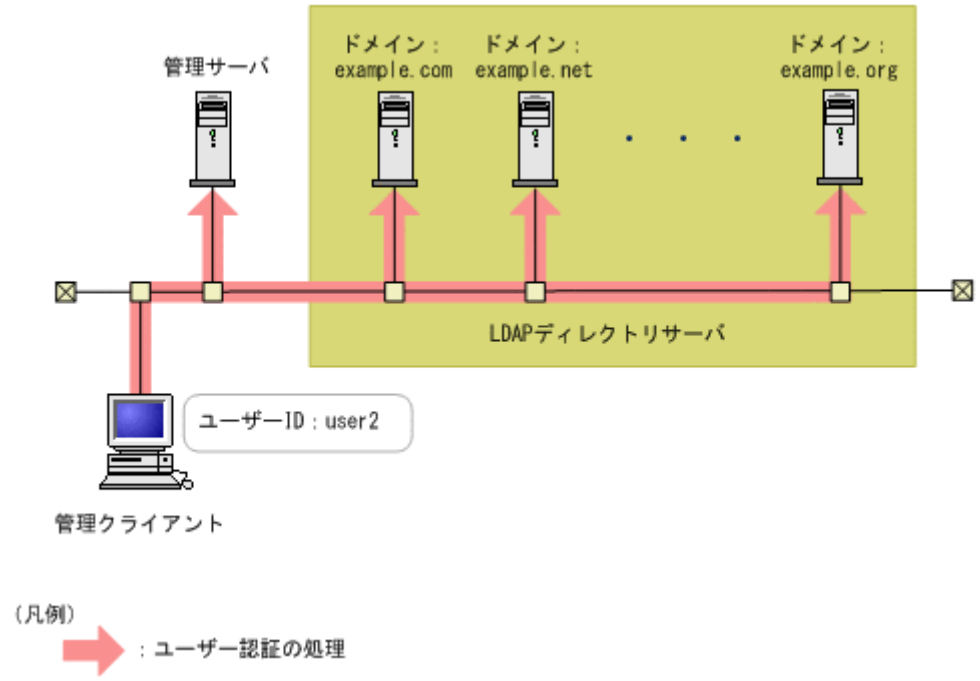
ドメイン名を含んでいるユーザー ID でログインすると，次の図に示すように，入力したドメインの LDAP ディレクトリサーバでユーザー認証されます。

図 3-1 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいるユーザー ID の場合）



ドメイン名を含んでいないユーザー ID でログインすると，次の図に示すように，連携しているすべての LDAP ディレクトリサーバへ順に認証処理が実行されます。このとき，多数の LDAP ディレクトリサーバと連携していると，ユーザー認証に時間がかかるため，ドメイン名を含んでいるユーザー ID でログインすることをお勧めします。

図 3-2 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいないユーザー ID の場合）



3.14.2 LDAP ディレクトリサーバで認証する場合に必要な設定

LDAP ディレクトリサーバでユーザー認証するために，Hitachi Command Suite 製品では次の設定が必要です。

1. LDAP ディレクトリサーバのデータ構造を確認し，Hitachi Command Suite 製品と連携して認証を行う方法を確認します。
2. 管理サーバの exauth.properties ファイルに必要な情報を設定します。 外部認証サーバとだけ連携する場合と，外部認可サーバとも連携する場合で設定が異なります。

   また，LDAP ディレクトリサーバは，次のどちらかの方法で定義できます。

   - exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する

     IP アドレスやポート番号などの情報を LDAP ディレクトリサーバごとに exauth.properties ファイルに指定します。
   - DNS サーバに接続先の LDAP ディレクトリサーバを照会する

     LDAP ディレクトリサーバの OS で DNS サーバの環境設定が完了している必要があります。また，DNS サーバの SRV レコードに，LDAP ディレクトリサーバのホスト名やポート番号，ドメイン名などを登録しておく必要があります。

   参考：

   管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は，exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。

   また，DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は，ユーザーがログインする際に処理に時間が掛かることがあります。

   接続先の LDAP ディレクトリサーバがマルチドメイン構成の場合，DNS サーバに LDAP ディレクトリサーバを照会できません。
3. 次の場合は，LDAP ディレクトリサーバ内のユーザー情報を検索するためのユーザーアカウント（情報検索用のユーザーアカウント）を管理サーバに登録します。

- データ構造が階層モデルのとき
- データ構造がフラットモデルで，かつ外部認可サーバとも連携するとき※

注※

Global Link Manager GUI で認可グループを Hitachi Command Suite 製品に登録する際（手順 5）に，認可グループの Distinguished Name が外部認可サーバに登録されているか確認したい場合，System アカウントなど Hitachi Command Suite 製品に登録されたユーザー ID で操作するためには，情報検索用のユーザーアカウントを管理サーバに登録しておく必要があります。

4. LDAP ディレクトリサーバに，Hitachi Command Suite 製品を使用するユーザーのアカウントを登録します。

ユーザー ID およびパスワードは，Hitachi Command Suite 製品で使用できる文字で構成されている必要があります。1 バイト以上 256 バイト以内で次の文字を使用できます。

A〜Z a〜z 0〜9 ! # $ % & ' ( ) * + - . = @ ¥ ^ _ |

Hitachi Command Suite 製品では，ユーザー ID の大文字と小文字の違いは区別されません。また，パスワードの文字種の組み合わせは，外部認証サーバでの設定に従ってください。

5. Global Link Manager GUI で，アカウントの登録や権限の設定などを実施します。

外部認証サーバとだけ連携する場合

ユーザーの登録

ユーザーの認証方式の変更※

ユーザーに対する権限の設定

ユーザーに対するリソースグループの割り当て

注※ 既存のユーザーの認証方式を変更する場合に必要です。

外部認可サーバとも連携する場合

認可グループの登録

認可グループに対する権限の設定

なお，認可グループに対するリソースグループの割り当ては不要です。認可グループに所属するユーザーにはリソースグループに「All Resources」が割り当てられます。

6. hcmds64checkauth コマンドを使用して，LDAP ディレクトリサーバに正しく接続できるか確認します。

ここでは，管理サーバで必要な作業について説明します。Global Link Manager GUI での操作方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

(1) データ構造と認証方法の確認

LDAP ディレクトリサーバのデータ構造には次の 2 つがあります。

- 階層構造モデル
- フラットモデルの場合

データ構造によって，exauth.properties ファイルに設定する情報や管理サーバで必要な作業が異なるため，どちらに該当しているかを確認してください。

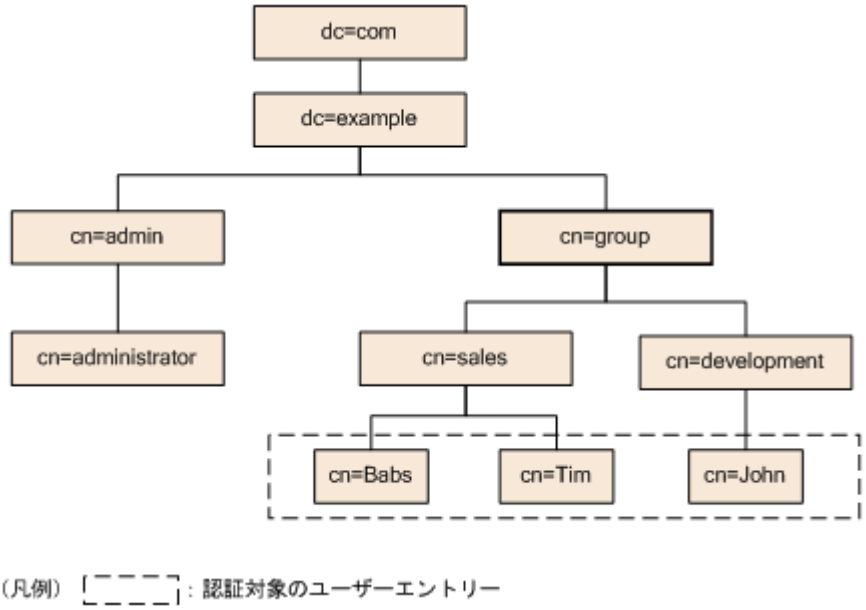
また，認証の際にユーザーを検索する起点となるエントリー（BaseDN）についても確認してください。BaseDN は exauth.properties ファイルの設定で必要な情報です。BaseDN より下の階層のユーザーエントリーが認証の対象となります。Hitachi Command Suite 製品で認証したいユーザーをすべて含むエントリーであることが必要です。

階層構造モデル

BaseDN より下の階層が分岐していて，かつ別の階層下にユーザーエントリーが登録されているデータ構造の場合は階層構造モデルになります。階層構造モデルの場合は，BaseDN より下のエントリーを対象に，ログイン ID とユーザー属性値が等しいエントリーが検索されます。

次の図に階層構造モデルの例を示します。点線で囲まれた範囲が，認証の対象となるユーザーエントリーです。この例では，対象のユーザーエントリーが「cn=sales」と「cn=development」の 2 つのエントリーにわたって属しているので，BaseDN は「cn=group,dc=example,dc=com」となります。

図 3-3 階層構造モデルの例

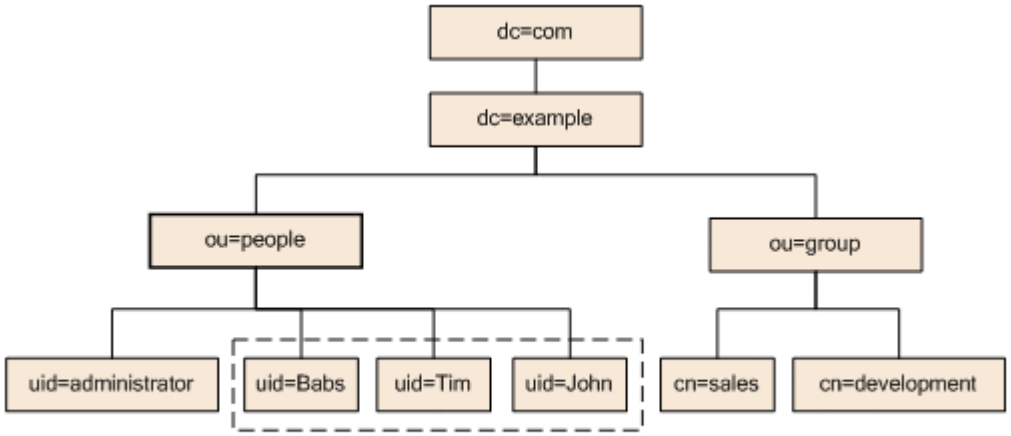


フラットモデル

BaseDN より下に分岐がなく，かつ直下にユーザーエントリーが登録されているデータ構造の場合はフラットモデルになります。フラットモデルの場合は，BaseDN より下のエントリーを対象に，ログイン ID と BaseDN を組み合わせた DN を持つエントリーが認証されます。

次の図にフラットモデルの例を示します。点線で囲まれた範囲が，認証の対象となるユーザーエントリーです。この例では，認証対象のすべてのユーザーエントリーが「ou=people」の直下に属しているので，BaseDN は「ou=people,dc=example,dc=com」となります。

図 3-4 フラットモデルの例



（凡例）：認証対象のユーザーエントリー

ただし，次のどちらかに該当する場合は，データ構造がフラットモデルであっても，階層構造モデルの場合の説明に従って設定してください。

- Hitachi Command Suite 製品のユーザー ID として，RDN の属性以外のユーザー属性の値を使用する

  ユーザーエントリーの RDN の属性値以外のユーザー属性値（Windows のログオン ID など）をユーザー ID として使用する場合には，階層構造モデルの場合の認証方法の設定が必要です。
- ユーザーエントリーの RDN の属性値に，Hitachi Command Suite 製品のユーザー ID として使用できない文字が使われている

  フラットモデルの場合の認証では，ユーザーエントリーの RDN の属性値を Hitachi Command Suite 製品のユーザー ID として使用します。そのため，Hitachi Command Suite 製品のユーザー ID として使用できない文字が使われている場合は，フラットモデルの場合の認証を行うことができません。

  - 使用できる RDN の例：

    `uid=John123S`

    `cn=John_Smith`
  - 使用できない RDN の例：

    `uid=John:123S`（コロン（:）が使用されている）

    `cn=John Smith`（スペースが使用されている）

(2) exauth.properties ファイルの設定（認証方式が LDAP の場合）

ここでは，LDAP ディレクトリサーバでユーザー認証する場合に `exauth.properties` ファイルで必要な設定について説明します。

1. `exauth.properties` ファイルで，次のプロパティに値を設定します。

   - 共通のプロパティ（「表 3-24 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」）
   - 外部認証サーバと外部認可サーバのプロパティ

     LDAP ディレクトリサーバごとに設定します。

     LDAP ディレクトリサーバの情報を直接指定する場合（「表 3-25 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）」）と，DNS サーバに照会する場合（「表 3-26 LDAP ディレクトリサーバで認

証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」）とで設定する項目が異なります。

exauth.properties ファイルのひな形は次の場所に格納されています。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥sample¥conf¥exauth.properties

注意事項

設定値の先頭および末尾には空白文字を指定しないでください。また，設定値は引用符（"）で囲まないでください。指定した場合，値は無視され，デフォルト値が採用されます。

2. exauth.properties ファイルを次の場所に格納します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥conf¥exauth.properties

exauth.properties ファイルの設定値を変更した場合は，直ちに変更後の値が有効になります。

exauth.properties ファイルの設定項目を「表 3-24 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」～「表 3-26 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」に示します。

表 3-24 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。ldap を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.server.name	LDAP ディレクトリサーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（「表 3-25 」および「表 3-26 」）を LDAP ディレクトリサーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。サーバ識別名を複数指定する場合は，サーバ識別名を「,（コンマ）」で区切って指定します。同じサーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 0～9 A～Z a～z ! # ( ) + - . = @ [ ] ^ _ { } ~ デフォルト値：なし
auth.ldap.multi_domain	LDAP ディレクトリサーバのサーバ識別名を複数指定する場合，各サーバがマルチドメイン構成であるか，冗長構成であるかを指定します。 マルチドメイン構成の場合は true を指定します。 冗長構成の場合は false を指定します。 デフォルト値：false
auth.ldap.default_domain	Active Directory のグローバルカタログの設定です。ログイン ID にドメイン名が付与されていない場合に，デフォルトの認証先とするサーバ構成のドメイン名を指定します。auth.server.name でサーバを複数指定した場合は，冗長構成ではなくマルチドメイン構成となります。 デフォルト値：なし
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 3-25 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
protocol※1	LDAP ディレクトリサーバ接続のプロトコルです。この項目は必須です。 平文による通信の場合は ldap，StartTLS による通信の場合は tls を指定します。 tls を指定する場合には，LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 ・ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ・ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ・ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ・ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ・ TLS_RSA_WITH_AES_256_GCM_SHA384 ・ TLS_RSA_WITH_AES_128_GCM_SHA256 ・ TLS_RSA_WITH_AES_256_CBC_SHA256 ・ TLS_RSA_WITH_AES_128_CBC_SHA256 指定できる値：ldap または tls デフォルト値：なし
host※2	LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合，IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには，IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず [ ] で囲んでください。グローバルカタログが有効（auth.ldap.default_domain を指定）の場合，複数のホスト名または IP アドレスをコンマで区切って指定すると，冗長構成にできます。この項目は必須です。 デフォルト値：なし
port	LDAP ディレクトリサーバのポート番号です。指定するポートが，LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。グローバルカタログが有効（auth.ldap.default_domain を指定）の場合，複数のポート番号をコンマで区切って指定すると，冗長構成にできます。ポート番号の個数は host に指定した個数と一致させてください。 指定できる値：1～65535 デフォルト値：389（グローバルカタログが無効の場合），3268（グローバルカタログが有効の場合）
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名（Attribute Type）です。 ・ 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を Hitachi Command Suite 製品のユーザー ID として使用します。※3 例：Active Directory を使用している場合で，Windows のログオン ID をユーザー ID として使用したいときは，Windows のログオン ID が値として定義されている属性名「sAMAccountName」を指定します。 ・ フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例：ユーザーの DN が「uid=John,ou=People,dc=example,dc=com」であるとき，RDN「uid=John」の属性名「uid」を指定します。 初期値として「sAMAccountName」が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP ディレクトリサーバの情報を検索する際に，起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。 ・ 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。

属性	説明
	例：図 3-1 の場合，「cn=group,dc=example,dc=com」を指定します。 ・ フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。 例：図 3-2 の場合，「ou=people,dc=example,dc=com」を指定します。 この項目は必須です。DN は RFC4514 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに「¥」でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合，リトライされません。 指定できる値：0～50 デフォルト値：20
domain.name	LDAP ディレクトリサーバが管理する外部認可サーバ用のドメインの名称です。外部認可サーバとも連携する場合，この項目は必須です。 デフォルト値：なし
domain	LDAP ディレクトリサーバが管理するマルチドメイン構成用のドメインの名称，またはグローバルカタログのドメインの名称です。 ログイン時に，この属性で指定したドメイン名をユーザー ID に含めると，指定したドメインに属する LDAP ディレクトリサーバが認証先となります。 LDAP ディレクトリサーバのサーバ識別名ごとにドメイン名を指定する際に，ドメイン名を重複しないように指定してください。大文字小文字は区別されません。 グローバルカタログが有効の場合，デフォルトの認証先とする構成は， auth.ldap.default_domain のドメイン名と一致させてください。 マルチドメイン構成の場合，この項目は必須です。 デフォルト値：なし
dns_lookup	false を指定します。 デフォルト値：false

注

各属性は，次のように指定します。

auth.ldap.＜*auth.server.name に指定した値*＞.＜*属性*＞=＜*値*＞

注※1

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には，Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。StartTLS を使用する場合の設定については，「5.2 サーバと LDAP ディレクトリサーバ間のセキュリティ設定」を参照してください。

注※2

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は，host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

注※3

Hitachi Command Suite 製品のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。

表 3-26 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。この項目は必須です。 指定できる値：ldap デフォルト値：なし
port	LDAP ディレクトリサーバのポート番号です。指定するポートが，LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名（Attribute Type）です。 ・ 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を Hitachi Command Suite 製品のユーザー ID として使用します。※ 例：Active Directory を使用している場合で，Windows のログオン ID をユーザー ID として使用したいときは，Windows のログオン ID が値として定義されている属性名「sAMAccountName」を指定します。 ・ フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例：ユーザーの DN が「uid=John,ou=People,dc=example,dc=com」であるとき，RDN「uid=John」の属性名「uid」を指定します。 初期値として「sAMAccountName」が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP ディレクトリサーバの情報を検索する際に，起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。 ・ 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。 例：図 3-1 の場合，「cn=group,dc=example,dc=com」を指定します。 ・ フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。 例：図 3-2 の場合，「ou=people,dc=example,dc=com」を指定します。 この項目は必須です。DN は RFC4514 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに「¥」でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合，リトライされません。 指定できる値：0～50 デフォルト値：20
domain.name	LDAP ディレクトリサーバが管理する外部認可サーバ用のドメインの名称です。この項目は必須です。 デフォルト値：なし

属性	説明
dns_lookup	true を指定します。 ただし，次の属性に値が設定されている場合は，DNS サーバには照会されず，ユーザーが指定した値を使用して LDAP ディレクトリサーバに接続されます。 ・ auth.ldap.＜*auth.server.name に指定した値*＞.host ・ auth.ldap.＜*auth.server.name に指定した値*＞.port デフォルト値：false

注

LDAP ディレクトリサーバ連携用のプロパティは，次のように指定します。

auth.ldap.＜*auth.server.name に指定した値*＞.＜*属性*＞=＜*値*＞

注※

Hitachi Command Suite 製品のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。

設定例を次に示します。

・ LDAP ディレクトリサーバの情報を直接指定する場合（外部認証サーバとだけ連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

・ LDAP ディレクトリサーバを DNS サーバに照会する場合（外部認証サーバとだけ連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

・ LDAP ディレクトリサーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- LDAP ディレクトリサーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- 冗長構成の場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- マルチドメイン構成の場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

- グローバルカタログを有効にする場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.default_domain=example.com
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap.example1.com,ldap.example2.com
auth.ldap.ServerName1.port=3268,3268
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
```

```
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap.example1.com,ldap.example2.com
auth.ldap.ServerName2.port=3268,3268
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

(3) 情報検索用のユーザーアカウントの登録（認証方式が LDAP の場合）

hcmds64ldapuser コマンドを使用して情報検索用のユーザーアカウントを管理サーバに登録します。登録後は，hcmds64ldapuser コマンドで，情報検索用のユーザーアカウントを削除したり，管理サーバに情報検索用のユーザーアカウントを登録済みの LDAP ディレクトリサーバを確認したりできます。

この作業は次の場合に必要です。

- データ構造が階層モデルのとき
- データ構造がフラットモデルで，かつ外部認可サーバとも連携するとき※

注※

Global Link Manager GUI で認可グループを Hitachi Command Suite 製品に登録する際に，認可グループの Distinguished Name が外部認可サーバに登録されているか確認したい場合，System アカウントなど Hitachi Command Suite 製品に登録されたユーザー ID で操作するためには，情報検索用のユーザーアカウントを管理サーバに登録しておく必要があります。

上記以外の場合は，認証・認可時にユーザー情報の検索を行わないため，この作業は不要です。すでに登録されている場合は，削除してください。

情報検索用のユーザーアカウントを登録する

hcmds64ldapuser コマンドで情報検索用のユーザーアカウントを登録します。

情報検索用のユーザーアカウントには，次の条件を満たすユーザーアカウントを登録してください。

- LDAP ディレクトリサーバに登録されていること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN にバインドできること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN を参照できること

hcmds64ldapuser コマンドの書式は次のとおりです。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64ldapuser /set /dn ＜*情報検索用ユーザーの DN*＞ /pass ＜*情報検索用ユーザーのパスワード*＞ /name ＜*サーバ識別名または外部認可サーバ用のドメイン名*＞

- ＜*情報検索用ユーザーの DN*＞

  DN は RFC4514 の規約に従って指定してください。例えば，次の文字が含まれる場合は，1 文字ごとに円記号（¥）でエスケープする必要があります。

  空白文字 # + , ; < = > ¥

- *＜情報検索用ユーザーのパスワード＞*

  大文字と小文字の違いも含めて，LDAP ディレクトリサーバに登録しているパスワードと完全に一致している必要があります。

- *＜サーバ識別名または外部認可サーバ用のドメイン名＞*

  exauth.properties ファイルの auth.server.name プロパティに指定したサーバ識別名または auth.ldap.＜*auth.server.name に指定した値*＞.domain.name プロパティに指定したドメイン名を指定します。

注意事項

LDAP ディレクトリサーバでは DN やパスワードに「"」を使用できますが，管理サーバには DN およびパスワードに「"」が含まれていないユーザーアカウントを登録してください。

図 3-1 のようなデータ構造の場合の実行例を説明します。この図では，検索の起点となるエントリーの DN は「cn=group,dc=example,dc=com」となります。この DN 以下のすべてのユーザー「Babs」「Tim」「John」に対し，属性を検索する権限を持つユーザーが「administrator」である場合，/dn オプションには「administrator」の DN「cn=administrator,cn=admin,dc=example,dc=com」を指定します。コマンドの実行例を次に示します。「administrator」のパスワードは「administrator_pass」とします。

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example,dc=com" /
pass administrator_pass /name ServerName
```

参考：

Active Directory を使用している場合は，Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して，ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

なお，DN が「cn=administrator,cn=admin,dc=example,com」の場合など，DN に「,（コンマ）」が含まれる場合は次のように指定します。

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example¥,com" /
pass administrator_pass /name ServerName
```

情報検索用のユーザーアカウントを削除する

情報検索用のユーザーアカウントを削除するには，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64ldapuser /delete /name ＜*サーバ識別名または外部認可サーバ用のドメイン名*＞

情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバを確認する

どの LDAP ディレクトリサーバの情報検索用ユーザーアカウントが管理サーバに登録されているかを確認する場合は，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64ldapuser /list

(4) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が LDAP の場合）

hcmds64checkauth コマンドを使用して，LDAP ディレクトリサーバに正しく接続できるか確認します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin

¥hcmds64checkauth /user <ユーザー*ID*> /pass <*パスワード*> [/summary]

/summary オプションを指定すると，コマンド実行時に表示される確認メッセージが簡略化されます。

<ユーザー*ID*>，<*パスワード*>には，LDAP ディレクトリサーバに登録されているユーザーアカウントのものを指定してください。<ユーザー*ID*>には，exauth.properties ファイルの auth.ldap.<*auth.server.name に指定した値*>.attr で指定した属性に格納されている値を指定してください。ただし，<ユーザー*ID*>，<*パスワード*>の先頭に，「/」は指定できません。

重要 マルチドメイン構成の場合，hcmds64checkauth コマンドを実行すると，連携しているすべての外部認証サーバに対してチェックし外部認証サーバごとにチェック結果が表示されます。
hcmds64checkauth コマンドで指定したユーザーアカウントが登録されていない外部認証サーバでは，チェック結果のフェーズ 3 でユーザーアカウントが登録されていないことを示すエラーメッセージが表示され，フェーズ 3 での確認で失敗することがあります。
この場合，接続確認したい外部認証サーバごとに，外部認証サーバに登録されているユーザーアカウントで確認してください。

hcmds64checkauth コマンドでは，次の 4 フェーズに分けて確認が行われます。フェーズごとに確認結果が表示されます。

フェーズ 1

exauth.properties ファイルの共通のプロパティ（「表 3-24 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」）が正しく設定されているかチェックします。

フェーズ 2

exauth.properties ファイルの外部認証サーバと外部認可サーバのプロパティ（「表 3-25 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）」または「表 3-26 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」）が正しく設定されているかチェックします。

フェーズ 3

外部認証サーバに接続できるかチェックします。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に，外部認可サーバに接続できるか，および認可グループを検索できるかをチェックします。

各フェーズでの確認が正常に終了した場合，次のメッセージが表示されます。

KAPM15004-I The result of the configuration check of Phase X※ was normal.

注※ 「X」にはフェーズ番号が入ります。

階層構造モデルの場合の実行例

図 3-1 のユーザー「John」のアカウントを使用して，hcmds64checkauth コマンドを実行する例を次に示します。

この例では，exauth.properties ファイルの auth.ldap.<*auth.server.name に指定した値*>.attr に「sAMAccountName」が指定されていることとします。LDAP ディレクトリサーバで設定された「John」の sAMAccountName 属性の値が「John_Smith」であるとき，<ユーザー*ID*>には「John_Smith」を指定します。「John」の，LDAP ディレクトリサーバ上のパスワードが「John_pass」であるとき，<*パスワード*>には「John_pass」を指定します。

```
hcmds64checkauth /user John_Smith /pass John_pass
```

フラットモデルの場合の実行例

図 3-2 のユーザー「John」のアカウントを使用して，hcmds64checkauth コマンドを実行する例を次に示します。

この例では，exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.attr に「uid」が指定されていることとします。「John」の RDN は「uid=John」であるため，＜*ユーザー ID* ＞には RDN の属性値「John」を指定します。「John」の，LDAP ディレクトリサーバ上のパスワードが「John_pass」であるとき，＜*パスワード*＞には「John_pass」を指定します。

```
hcmds64checkauth /user John /pass John_pass
```

3.14.3 RADIUS サーバで認証する場合に必要な設定

RADIUS サーバでユーザー認証するために，Hitachi Command Suite 製品では次の設定が必要です。

1. 管理サーバの exauth.properties ファイルに必要な情報を設定します。

   外部認証サーバとだけ連携する場合と，外部認可サーバとも連携する場合で設定が異なります。

   また，外部認可サーバとして使用する LDAP ディレクトリサーバは，次のどちらかの方法で定義できます。

   - exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する

     IP アドレスやポート番号などの情報を LDAP ディレクトリサーバごとに exauth.properties ファイルに指定します。
   - DNS サーバに接続先の LDAP ディレクトリサーバを照会する

     LDAP ディレクトリサーバの OS で DNS サーバの環境設定が完了している必要があります。また，DNS サーバの SRV レコードに，LDAP ディレクトリサーバのホスト名やポート番号，ドメイン名などを登録しておく必要があります。

   参考：

   管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は，exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。

   また，DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は，ユーザーがログインする際に処理に時間が掛かることがあります。
2. 外部認可サーバとも連携する場合は，LDAP ディレクトリサーバ内のユーザー情報を検索するためのユーザーアカウント（情報検索用のユーザーアカウント）を管理サーバに登録します。
3. RADIUS サーバに，Hitachi Command Suite 製品を使用するユーザーのアカウントを登録します。

   ユーザー ID およびパスワードは，Hitachi Command Suite 製品で使用できる文字で構成されている必要があります。1 バイト以上 256 バイト以内で次の文字を使用できます。

   A～Z a～z 0～9 ! # $ % & ' ( ) * + - . = @ ¥ ^ _ |

   Hitachi Command Suite 製品では，ユーザー ID の大文字と小文字の違いは区別されません。また，パスワードの文字種の組み合わせは，外部認証サーバでの設定に従ってください。
4. RADIUS サーバとの通信用に共有秘密鍵（Shared secret）を管理サーバに設定します。
5. Global Link Manager GUI で，アカウントの登録や権限の設定などを実施します。

   外部認証サーバとだけ連携する場合

   ユーザーの登録

ユーザーの認証方式の変更※

ユーザーに対する権限の設定

ユーザーに対するリソースグループの割り当て

注※ 既存のユーザーの認証方式を変更する場合に必要です。

外部認可サーバとも連携する場合

認可グループの登録

認可グループに対する権限の設定

なお，認可グループに対するリソースグループの割り当ては不要です。認可グループに所属するユーザーにはリソースグループに「All Resources」が割り当てられます。

6. hcmds64checkauth コマンドを使用して，RADIUS サーバに正しく接続できるか確認します。

ここでは，管理サーバで必要な作業について説明します。Global Link Manager GUI での操作方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

(1) exauth.properties ファイルの設定（認証方式が RADIUS の場合）

ここでは，RADIUS サーバでユーザー認証する場合に exauth.properties ファイルで必要な設定について説明します。

1. exauth.properties ファイルで，次のプロパティに値を設定します。

   - 共通のプロパティ（「表 3-27 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」）
   - 外部認証サーバのプロパティ（「表 3-28 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定）」）

     RADIUS サーバごとに設定します。
   - 外部認可サーバのプロパティ

     外部認可サーバとも連携する場合に必要な設定です。LDAP ディレクトリサーバの情報をドメインごとに設定します。

     LDAP ディレクトリサーバの情報を直接指定する場合（「表 3-29 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）」および「表 3-30 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を直接指定するとき）」）と，DNS サーバに照会する場合（「表 3-29 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）」および「表 3-31 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）」）とで設定する項目が異なります。

   exauth.properties ファイルのひな形は次の場所に格納されています。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥sample¥conf¥exauth.properties

   注意事項

   設定値の先頭および末尾には空白文字を指定しないでください。また，設定値は「"」で囲まないでください。指定した場合，値は無視され，デフォルト値が採用されます。

2. exauth.properties ファイルを次の場所に格納します。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥conf¥exauth.properties

exauth.properties ファイルの設定値を変更した場合は，直ちに変更後の値が有効になります。

exauth.properties ファイルの設定項目を「表 3-27 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」～「表 3-31 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）」に示します。

表 3-27 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。radius を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.server.name	RADIUS サーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（「表 3-28 」）を RADIUS サーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。RADIUS サーバを冗長構成にする場合は，各サーバのサーバ識別名を「,（コンマ）」で区切って指定します。 サーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 0～9 A～Z a～z ! # ( ) + - . = @ [ ] ^ _ { } ~ デフォルト値：なし
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 3-28 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定）

属性	説明
protocol	RADIUS サーバ認証に使用する認証プロトコルです。この項目は必須です。 指定できる値：PAP または CHAP デフォルト値：なし
host※1	RADIUS サーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合，IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには，IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず[ ]で囲んでください。この項目は必須です。 デフォルト値：なし
port	RADIUS サーバの認証用ポート番号です。指定するポートが RADIUS サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：1812
timeout	RADIUS サーバと接続するときの接続待ち時間です。 指定できる値：1～65535（秒） デフォルト値：1
retry.times	RADIUS サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合，リトライされません。 指定できる値：0～50 デフォルト値：3
attr.NAS-Identifier※2	Global Link Manager の管理サーバのホスト名です。RADIUS サーバが管理サーバを識別するために使用します。初期値として，管理サーバのホスト名が設定されています。 指定できる値：253 バイト以内の次の文字列 0～9 A～Z a～z ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ デフォルト値：なし

属性	説明
attr.NAS-IP-Address※2	Global Link Manager の管理サーバの IPv4 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。 IPv4 アドレスの形式が不正な場合，この属性は無効です。 デフォルト値：なし
attr.NAS-IPv6-Address※2	Global Link Manager の管理サーバの IPv6 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。IPv6 アドレスは必ず [ ] で囲んでください。 IPv6 アドレスの形式が不正な場合，この属性は無効です。 デフォルト値：なし

注

各属性は，次のように指定します。

auth.radius.＜*auth.server.name に指定した値*＞.＜*属性*＞=＜*値*＞

注※1

同一マシンで稼働する外部認可サーバとも連携し，かつ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は，host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

注※2

attr.NAS-Identifier，attr.NAS-IP-Address，attr.NAS-IPv6-Address はどれか 1 つを必ず指定してください。

表 3-29 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）

プロパティ名	説明
domain.name	LDAP ディレクトリサーバが管理するドメインの名称です。外部認可サーバとも連携する場合，この項目は必須です。 デフォルト値：なし
dns_lookup	LDAP ディレクトリサーバの情報を DNS サーバに照会するかどうかの設定です。 exauth.properties ファイルに LDAP ディレクトリサーバの情報を直接指定する場合は false を指定します。 DNS サーバに照会する場合は，true を指定します。ただし，次の属性に値が設定されている場合は，DNS サーバには照会されず，ユーザーが指定した値を使用して LDAP ディレクトリサーバに接続されます。 ・ auth.group.＜*ドメイン名*＞.host ・ auth.group.＜*ドメイン名*＞.port デフォルト値：false

注

各属性は，次のように指定します。

auth.radius.＜*auth.server.name に指定した値*＞.＜*属性*＞=＜*値*＞

表 3-30 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を直接指定するとき）

属性	説明
protocol※1	LDAP ディレクトリサーバ接続のプロトコルです。 平文による通信の場合は ldap，StartTLS による通信の場合は tls を指定します。 tls を指定する場合には，LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 ・ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ・ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

属性	説明
	・ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ・ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ・ TLS_RSA_WITH_AES_256_GCM_SHA384 ・ TLS_RSA_WITH_AES_128_GCM_SHA256 ・ TLS_RSA_WITH_AES_256_CBC_SHA256 ・ TLS_RSA_WITH_AES_128_CBC_SHA256 指定できる値：ldap または tls デフォルト値：ldap
host※2	LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合，IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには，IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧（[ ]）で囲んでください。この項目は必須です。 デフォルト値：なし
port	LDAP ディレクトリサーバのポート番号です。指定するポートが，LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に，起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに円記号（¥）でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。 省略した場合は，Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合，リトライされません。 指定できる値：0～50 デフォルト値：20

注

各属性は，次のように指定します。

auth.group.＜*ドメイン名*＞.＜*属性*＞=＜*値*＞

＜*ドメイン名*＞には，auth.radius.＜*auth.server.name に指定した値*＞.domain.name の値を指定します。

注※1

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には，Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。StartTLS を使用する場合の設定については，「5.2 サーバと LDAP ディレクトリサーバ間のセキュリティ設定」を参照してください。

注※2

外部認証サーバと外部認可サーバが別のマシンで稼働していて，かつ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は，host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

表 3-31 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。 指定できる値：ldap デフォルト値：ldap
port	LDAP ディレクトリサーバのポート番号です。指定するポートが，LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に，起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに円記号（¥）でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。 省略した場合は，Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合，リトライされません。 指定できる値：0～50 デフォルト値：20

注

各属性は，次のように指定します。

auth.group.＜*ドメイン名*＞.＜*属性*＞=＜*値*＞

＜*ドメイン名*＞には，auth.radius.＜***auth.server.name** に指定した値*＞.domain.name の値を指定します。

設定例を次に示します。

- 外部認証サーバとだけ連携する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- 外部認可サーバの情報を直接設定する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- 外部認可サーバを DNS サーバに照会する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- 冗長構成の場合

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

(2) 情報検索用のユーザーアカウントの登録（認証方式が RADIUS の場合）

LDAP ディレクトリサーバを外部認可サーバとして利用する場合に，hcmds64ldapuser コマンドを使用して，情報検索用のユーザーアカウントを管理サーバに登録します。登録後は，hcmds64ldapuser コマンドで，情報検索用のユーザーアカウントを削除したり，管理サーバに情報検索用のユーザーアカウントを登録済みの LDAP ディレクトリサーバを確認したりできます。

情報検索用のユーザーアカウントを登録する

hcmds64ldapuser コマンドで情報検索用のユーザーアカウントを登録します。

情報検索用のユーザーアカウントには，次の条件を満たすユーザーアカウントを登録してください。

- LDAP ディレクトリサーバに登録されていること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN にバインドできること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN を参照できること

hcmds64ldapuser コマンドの書式は次のとおりです。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64ldapuser /set /dn ＜*情報検索用ユーザーの DN*＞ /pass ＜*情報検索用ユーザーのパスワード*＞ /name ＜*ドメイン名*＞

- ＜*情報検索用ユーザーの DN*＞

  DN は RFC4514 の規約に従って指定してください。例えば，次の文字が含まれる場合は，1 文字ごとに円記号（¥）でエスケープする必要があります。

  空白文字 # + , ; < = > ¥
- ＜*情報検索用ユーザーのパスワード*＞

  大文字と小文字の違いも含めて，LDAP ディレクトリサーバに登録しているパスワードと完全に一致している必要があります。
- ＜*ドメイン名*＞

  exauth.properties ファイルの auth.server.name プロパティに指定したドメイン名を指定します。

注意事項

LDAP ディレクトリサーバでは DN やパスワードに「"」を使用できますが，管理サーバには DN およびパスワードに「"」が含まれていないユーザーアカウントを登録してください。

参考

Active Directory を使用している場合は，Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して，ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

なお，DN が「cn=administrator,cn=admin,dc=example,com」の場合など，DN に「,（コンマ）」が含まれる場合は次のように指定します。

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example¥,com" /
pass administrator_pass /name ServerName
```

情報検索用のユーザーアカウントを削除する

情報検索用のユーザーアカウントを削除するには，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64ldapuser /delete /name ＜*ドメイン名*＞

情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバを確認する

どの LDAP ディレクトリサーバの情報検索用ユーザーアカウントが管理サーバに登録されているかを確認する場合は，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64ldapuser /list

(3) 共有秘密鍵の設定

RADIUS サーバと通信するための共有秘密鍵を，hcmds64radiussecret コマンドを使用して管理サーバに設定します。設定後は，hcmds64radiussecret コマンドで，共有秘密鍵を削除したり，共有秘密鍵が設定されている外部認証サーバのサーバ識別名を一覧表示したりできます。

共有秘密鍵を設定する

hcmds64radiussecret コマンドで共有秘密鍵を設定するには，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64radiussecret /set ＜*共有秘密鍵*＞ /name ＜*RADIUS サーバのサーバ識別名*＞

＜*RADIUS サーバのサーバ識別名*＞は，exauth.properties ファイルの auth.server.name プロパティに指定するサーバ識別名と一致している必要があります。

共有秘密鍵が「secret01」で，RADIUS サーバのサーバ識別名が「ServerName」の場合の hcmds64radiussecret コマンドの実行例を次に示します。

```
hcmds64radiussecret /set secret01 /name ServerName
```

共有秘密鍵を削除する

共有秘密鍵を削除するには，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64radiussecret /delete /name ＜*RADIUS サーバのサーバ識別名*＞

共有秘密鍵が設定されている RADIUS サーバのサーバ識別名を一覧表示する

共有秘密鍵が設定されている RADIUS サーバのサーバ識別名を一覧表示するには，次のコマンドを実行してください。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64radiussecret /list

(4) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が RADIUS の場合）

hcmds64checkauth コマンドを使用して，RADIUS サーバに正しく接続できるか確認します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
¥hcmds64checkauth /user ＜*ユーザー ID*＞ /pass ＜*パスワード*＞ [/summary]

＜*ユーザー ID*＞，＜*パスワード*＞には，RADIUS サーバに登録されているユーザーアカウントのものを指定してください。ただし，＜*ユーザー ID*＞，＜*パスワード*＞の先頭に，「/」は指定できません。

/summary オプションを指定すると，コマンド実行時に表示される確認メッセージが簡略化されます。

hcmds64checkauth コマンドでは，次の 4 フェーズに分けて確認が行われます。フェーズごとに確認結果が表示されます。

フェーズ 1

exauth.properties ファイルの共通のプロパティ（「表 3-27 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」）が正しく設定されているかチェックします。

フェーズ 2

exauth.properties ファイルの外部認証サーバのプロパティ（「表 3-28 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定）」）と，外部認可サーバのプロパティ（「表 3-29 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）」～「表 3-31 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）」）が正しく設定されているかチェックします。

フェーズ 3

外部認証サーバに接続できるかチェックします。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に，外部認可サーバに接続できるか，および認可グループを検索できるかをチェックします。

各フェーズでの確認が正常に終了した場合，次のメッセージが表示されます。

```
KAPM15004-I The result of the configuration check of Phase X※ was normal.
```

注※ 「X」にはフェーズ番号が入ります。

3.14.4 Kerberos サーバで認証する場合に必要な設定

Kerberos サーバでユーザー認証するために，Hitachi Command Suite 製品では次の設定が必要です。

1. 管理サーバの exauth.properties ファイルに必要な情報を設定します。
   外部認証サーバとだけ連携する場合と，外部認可サーバとも連携する場合で設定が異なります。
   また，外部認証サーバとして使用する Kerberos サーバは，次のどちらかの方法で定義できます。

   - exauth.properties ファイルに接続先の Kerberos サーバの情報を直接指定する
     レルムごとに，IP アドレスやポート番号などの Kerberos サーバの情報を exauth.properties ファイルに指定します。
   - DNS サーバに接続先の Kerberos サーバを照会する
     Kerberos サーバを管理する DNS サーバの情報を exauth.properties ファイルに指定します。また，DNS サーバの SRV レコードに，Kerberos サーバのホスト名やポート番号，レルム名などを登録しておく必要があります。

   参考：

   管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は，exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。

   また，DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は，ユーザーがログインする際に処理に時間が掛かることがあります。
2. 外部認可サーバとも連携する場合は，LDAP ディレクトリサーバ内のユーザー情報を検索するためのユーザーアカウント（情報検索用のユーザーアカウント）を管理サーバに登録します。

3. Kerberos サーバに，Hitachi Command Suite 製品を使用するユーザーのアカウントを登録します。

   ユーザー ID およびパスワードは，Hitachi Command Suite 製品で使用できる文字で構成されている必要があります。1 バイト以上 256 バイト以内で次の文字を使用できます。

   A〜Z a〜z 0〜9 ! # $ % & ' ( ) * + - . = @ ¥ ^ _ |

   Hitachi Command Suite 製品では，ユーザー ID の大文字と小文字の違いは区別されません。また，パスワードの文字種の組み合わせは，外部認証サーバでの設定に従ってください。

4. Global Link Manager GUI で，アカウントの登録や権限の設定などを実施します。

   外部認証サーバとだけ連携する場合

   ユーザーの登録

   ユーザーの認証方式の変更※

   ユーザーに対する権限の設定

   ユーザーに対するリソースグループの割り当て

   注※ 既存のユーザーの認証方式を変更する場合に必要です。

   外部認可サーバとも連携する場合

   認可グループの登録

   認可グループに対する権限の設定

   なお，認可グループに対するリソースグループの割り当ては不要です。認可グループに所属するユーザーにはリソースグループに「All Resources」が割り当てられます。

5. 管理サーバで hcmds64checkauth コマンドを使用して，外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

ここでは，管理サーバで必要な作業について説明します。Global Link Manager GUI での操作方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

(1) exauth.properties ファイルの設定（認証方式が Kerberos の場合）

ここでは，Kerberos サーバでユーザー認証する場合に exauth.properties ファイルで必要な設定について説明します。

1. exauth.properties ファイルで，必要なプロパティに値を設定します。

   - 共通のプロパティ（「表 3-32 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」）
   - 外部認証サーバのプロパティ

     Kerberos サーバごとに設定します。

     Kerberos サーバの情報を直接指定する場合（「表 3-33 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）」）と，DNS サーバに照会する場合（「表 3-34 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」）とで設定する項目が異なります。
   - 外部認可サーバのプロパティ（「表 3-35 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）」）

     Kerberos サーバの情報を直接指定し，かつ外部認可サーバとも連携する場合にだけ必要な設定です。レルムごとに指定します。

   exauth.properties ファイルのひな形は次の場所に格納されています。

   ＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥sample¥conf¥exauth.properties

注意事項

設定値の先頭および末尾には空白文字を指定しないでください。また，設定値は「"」で囲まないでください。指定した場合，値は無視され，デフォルト値が採用されます。

2. exauth.properties ファイルを次の場所に格納します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥conf¥exauth.properties

exauth.properties ファイルの設定値を変更した場合は，直ちに変更後の値が有効になります。

exauth.properties ファイルの設定項目を「表 3-32 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」～「表 3-35 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）」に示します。

表 3-32 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。kerberos を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 3-33 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
default_realm	デフォルトのレルム名を指定します。Global Link Manager GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に，この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	false を指定します。 デフォルト値：false
clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合，認証エラーになります。 指定できる値：0～300（秒） デフォルト値：300
timeout	Kerberos サーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：3
realm_name	レルム識別名を指定します。レルムごとに Kerberos サーバの情報を区別するために付ける任意の名称です。必ず 1 つ以上のレルム識別名を指定してください。レルム識別名を複数指定する場合は，レルム識別名をコンマ（,）で区切って指定します。同じレルム識別名は重複して登録しないでください。 デフォルト値：なし
＜*realm_name に指定した値*＞.realm	Kerberos サーバに設定してあるレルム名を指定します。この項目は必須です。 デフォルト値：なし

属性	説明
＜*realm_name に指定した値*＞.kdc	Kerberos サーバの情報を次の形式で指定します。 ＜*ホスト名または IP アドレス*＞[:＜ポート番号＞] この項目は必須です。 ＜ホスト名または IP アドレス＞ ホスト名を指定する場合，IP アドレスへの名前解決ができることを事前に確認してください。 IP アドレスは，IPv4 アドレスで指定してください。IPv6 環境では，ホスト名で指定してください。 ただし，ループバックアドレス（localhost または 127.0.0.1）を指定しないでください。 ＜ポート番号＞ 指定するポートが Kerberos サーバで待ち受けポート番号として設定されていることを事前に確認してください。ポート番号を省略した場合，または指定したポート番号が Kerberos サーバで使用できない場合は，「88」を指定したと見なされます。 Kerberos サーバを冗長構成にする場合は，次のように「,（コンマ）」で区切って指定します。 ＜*ホスト名または IP アドレス*＞[:＜*ポート番号*＞],＜*ホスト名または IP アドレス*＞[:＜*ポート番号*＞],...

注

各属性は，次のように指定します。

auth.kerberos.＜*属性*＞=＜*値*＞

表 3-34 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）

属性	説明
default_realm	デフォルトのレルム名を指定します。Global Link Manager GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に，この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	true を指定します。この項目は必須です。 ただし，次のすべての属性に値を設定していると，Kerberos サーバは DNS サーバに照会されません。 • realm_name • ＜*realm_name に指定した値*＞.realm • ＜*realm_name に指定した値*＞.kdc
clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合，認証エラーになります。 指定できる値：0～300（秒） デフォルト値：300
timeout	Kerberos サーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：3

注

各属性は，次のように指定します。

auth.kerberos.＜*属性*＞=＜*値*＞

表 3-35 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）

属性	説明
protocol※	LDAP ディレクトリサーバ接続のプロトコルです。 平文による通信の場合は ldap，StartTLS による通信の場合は tls を指定します。 Kerberos サーバの情報を直接指定する場合にだけ，StartTLS で通信できます。 tls を指定する場合には，LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 ・ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ・ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ・ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ・ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ・ TLS_RSA_WITH_AES_256_GCM_SHA384 ・ TLS_RSA_WITH_AES_128_GCM_SHA256 ・ TLS_RSA_WITH_AES_256_CBC_SHA256 ・ TLS_RSA_WITH_AES_128_CBC_SHA256 指定できる値：ldap または tls デフォルト値：ldap
port	LDAP ディレクトリサーバのポート番号です。指定するポートが，LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に，起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに円記号（¥）でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。 省略した場合は，Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合，タイムアウトしないで，通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合，リトライされません。 指定できる値：0～50 デフォルト値：20

注

各属性は，次のように指定します。

auth.group.＜*レルム名*＞.＜*属性*＞=＜*値*＞

＜*レルム名*＞には auth.kerberos.＜*realm_name に指定した値*＞.realm の値を指定します。

注※

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には，Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。StartTLS を使用する

場合の設定については，「5.2 サーバと LDAP ディレクトリサーバ間のセキュリティ設定」を参照してください。

設定例を次に示します。

- Kerberos サーバの情報を直接指定する場合（外部認可サーバと連携しないとき）

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- Kerberos サーバを DNS サーバに照会する場合（外部認可サーバと連携しないとき）

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- Kerberos サーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- Kerberos サーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- 冗長構成の場合

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- レルム識別名を複数指定した場合

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
```

```
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

(2) 情報検索用のユーザーアカウントの登録（認証方式が Kerberos の場合）

LDAP ディレクトリサーバを外部認可サーバとして利用する場合に，hcmds64ldapuser コマンドを使用して，情報検索用のユーザーアカウントを管理サーバに登録します。登録後は，hcmds64ldapuser コマンドで，情報検索用のユーザーアカウントを削除したり，管理サーバに情報検索用のユーザーアカウントを登録済みの LDAP ディレクトリサーバを確認したりできます。

情報検索用のユーザーアカウントを登録する

hcmds64ldapuser コマンドで情報検索用のユーザーアカウントを登録します。

情報検索用のユーザーアカウントには，次の条件を満たすユーザーアカウントを登録してください。

- LDAP ディレクトリサーバに登録されていること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN にバインドできること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.basedn で指定した DN を参照できること

hcmds64ldapuser コマンドの書式は次のとおりです。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64ldapuser /set /dn ＜*情報検索用ユーザーの DN* ＞ /pass ＜*情報検索用ユーザーのパスワード*＞ /name ＜*レルム名*＞

- ＜*情報検索用ユーザーの DN* ＞

  DN は RFC4514 の規約に従って指定してください。例えば，次の文字が含まれる場合は，1 文字ごとに円記号（¥）でエスケープする必要があります。

  空白文字 # + , ; < = > ¥
- ＜*情報検索用ユーザーのパスワード*＞

  大文字と小文字の違いも含めて，LDAP ディレクトリサーバに登録しているパスワードと完全に一致している必要があります。
- ＜*レルム名*＞

  exauth.properties ファイルで Kerberos サーバの情報を直接指定した場合は，auth.kerberos.default_realm の値，または auth.kerberos.＜*auth.kerberos.realm_name 値*＞.realm の値を指定します。

  exauth.properties ファイルで Kerberos サーバの情報を DNS サーバに照会するよう設定した場合は，DNS サーバに登録されたレルム名を指定します。

注意事項

LDAP ディレクトリサーバでは DN やパスワードに「"」を使用できますが，管理サーバには DN およびパスワードに「"」が含まれていないユーザーアカウントを登録してください。

参考

Active Directory を使用している場合は，Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して，ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

なお，DN が「cn=administrator,cn=admin,dc=example,com」の場合など，DN に「,（コンマ）」が含まれる場合は次のように指定します。

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example¥,com" /
pass administrator_pass /name ServerName
```

情報検索用のユーザーアカウントを削除する

情報検索用のユーザーアカウントを削除するには，次のコマンドを実行してください。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin
¥hcmds64ldapuser /delete /name *＜レルム名＞*

情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバを確認する

どの LDAP ディレクトリサーバの情報検索用ユーザーアカウントが管理サーバに登録されているかを確認する場合は，次のコマンドを実行してください。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin
¥hcmds64ldapuser /list

(3) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が Kerberos の場合）

hcmds64checkauth コマンドを使用して，Kerberos サーバに正しく接続できるか確認します。exauth.properties ファイルでレルム名を複数指定した場合は，レルムごとに接続確認してください。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥bin
¥hcmds64checkauth /user *＜ユーザー ID ＞* /pass *＜パスワード＞* [/summary]

外部認証サーバとだけ連携する場合と，外部認可サーバとも連携する場合で，*＜ユーザー ID ＞*，*＜パスワード＞*に指定するユーザーアカウントが異なります。

外部認証サーバとだけ連携する場合：

Hitachi Command Suite 製品に登録されていて，かつ認証方式が Kerberos のユーザーアカウントを指定してください。

外部認可サーバとも連携する場合：

Hitachi Command Suite 製品に登録されていないユーザーアカウントを指定してください。

exauth.properties ファイルの default_realm で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合，ユーザーが所属するレルムも確認してください。
exauth.properties ファイルでレルム名を複数指定した場合，指定したレルム名をすべて確認してください。また，*＜ユーザー ID ＞*，*＜パスワード＞*の先頭に，スラント（/）が含まれるユーザーアカウントは指定できません。

/summary オプションを指定すると，コマンド実行時に表示される確認メッセージが簡略化されます。

重要 exauth.properties ファイルでレルム名を複数指定したときは，ユーザー ID は次の形式で指定してください。

- exauth.properties ファイルの default_realm で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合：

  ＜ユーザー *ID* ＞@＜*レルム名*＞

- exauth.properties ファイルの default_realm で設定したレルムに所属するユーザーを指定する場合：

  レルム名を省略して入力できます。

hcmds64checkauth コマンドでは，次の 4 フェーズに分けて確認が行われます。フェーズごとに確認結果が表示されます。

フェーズ 1

exauth.properties ファイルの共通のプロパティ（「表 3-32 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」）が正しく設定されているかチェックします。

フェーズ 2

exauth.properties ファイルの外部認証サーバのプロパティ（「表 3-33 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）」または「表 3-34 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」）と，外部認可サーバのプロパティ（「表 3-35 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）」）が正しく設定されているかチェックします。

フェーズ 3

Kerberos サーバと接続できるかどうかを確認します。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に，外部認可サーバに接続できるか，および認可グループを検索できるかをチェックします。

各フェーズでの確認が正常に終了した場合，次のメッセージが表示されます。

KAPM15004-I The result of the configuration check of Phase X※ was normal.

注※ 「X」にはフェーズ番号が入ります。

(4) Kerberos 認証に使用できる暗号タイプ

Hitachi Command Suite 製品で，Kerberos 認証に使用できる暗号タイプ（encryption types）は次のとおりです。どれかの暗号タイプを使用できるように Kerberos サーバを構築してください。

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC

4

クラスタ環境での Global Link Manager のインストール

この章では，クラスタ環境で Global Link Manager をインストールする場合の手順について説明します。

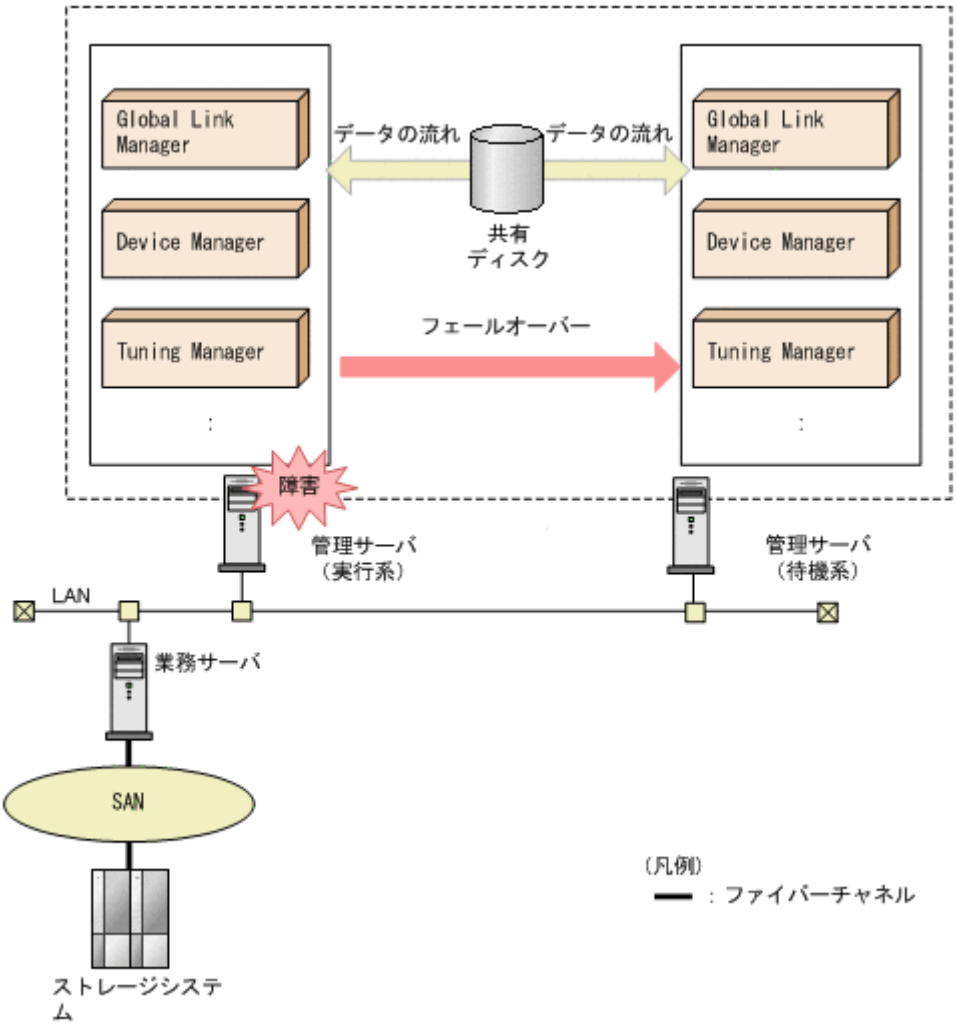
なお，Windows Server 2012 以外と Windows Server 2012 で名称が異なる項目について，特に断り書きがない場合，Windows Server 2012 以外での名称を記載しています。そのため，Windows Server 2012 使用時には，「フェールオーバークラスタ管理」を「フェールオーバークラスタマネージャー」に，「リソースグループ」を「役割」にそれぞれ読み替えてください。

4.1 Global Link Manager のクラスタ環境でのシステム構成

Hitachi Command Suite 製品の管理サーバでは，Active/Standby 型のフェールオーバークラスタリングに対応しています。クラスタシステムを構成するそれぞれのサーバシステムのうち，業務を実行中のシステムを「実行系ノード」，実行系ノードの障害時に業務を引き継げるように待機しているシステムを「待機系ノード」と呼びます。障害が発生したときに，業務を実行するサーバを実行系ノードから待機系ノードに切り替えるため，障害が発生しても運用が継続できます。これによって，障害発生時の業務の中断を防ぎ，稼働率が高くなります。

Hitachi Command Suite 製品の管理サーバでのクラスタ構成の概念図を次の図に示します。

図 4-1 クラスタ構成の概念図



クラスタシステム全体を制御するソフトウェアを「クラスタソフトウェア」といいます。クラスタソフトウェアは，システムが正常に動作しているかを監視し，異常を検知した場合にフェールオーバーすることで，業務の中断を防ぎます。

4.2 クラスタ環境をセットアップする場合の前提環境

クラスタ環境をセットアップする場合，管理サーバ上にデータベースを再作成したり，バックアップしたりするための空き容量が必要です。管理サーバ上に次の空き容量があることを確認してください。

データベースの再作成先に必要な空き容量

新規インストールする場合：

＜*Hitachi Command Suite 共通コンポーネントのデータベース容量*＞＋＜*Global Link Manager サーバと同一ホストにインストールされている，Global Link Manager を含むすべての Hitachi Command Suite 製品のデータベース容量*＞

アップグレードインストールする場合：

＜*Hitachi Command Suite 共通コンポーネントのデータベース容量*＞＋＜*Global Link Manager サーバと同一ホストにインストールされている，Global Link Manager を含むすべての Hitachi Command Suite 製品のデータベース容量*＞＋ 0.7GB

データベースのバックアップに必要な空き容量

（＜*バックアップ対象となる Hitachi Command Suite 製品のデータベースサイズの総和*＞×2）＋ 20MB

注意事項

Global Link Manager および Hitachi Command Suite 共通コンポーネントのデータベースの容量については，データベースファイルの格納先ディレクトリの容量としてください。ほかの Hitachi Command Suite 製品のデータベースの容量については，各製品のマニュアルを参照してください。

4.3 クラスタ環境で運用する場合の注意事項

クラスタ環境で運用する場合の注意事項は次のとおりです。

- クラスタを構成するすべてのノードは，同じディスク構成にして，Hitachi Command Suite 製品のインストール先（ドライブ文字やパス名など）も同じにする必要があります。
- クラスタ環境でのインストール後に Hitachi Command Suite 製品の設定を変更する場合には，すべてのノードで同一の設定を実施してください。
- Global Link Manager は，次に示すストレージシステムの SVP プログラムと同一のホストにインストールして運用できます。ただし，その場合の SVP プログラムはクラスタ構成をサポートしていないため，Global Link Manager も非クラスタ構成で構築してください。
  - VSP Gx00 モデル
  - VSP Fx00 モデル
- HiRDB が使用するポート番号をデフォルト（22032/tcp）以外の番号に変更して運用する場合は，実行系ノードおよび待機系ノードで同じポート番号を設定する必要があります。
- ほかの Hitachi Command Suite 製品をクラスタ構成で運用するための設定をしている場合は，それらの作業が完了してから Global Link Manager のインストール作業を開始してください。
- ここでは，クラスタ化するサービスの集まり（サービスのフェールオーバーの単位）をリソースグループと呼びます。
- Global Link Manager を含む，Hitachi Command Suite 製品にアクセスするためのネットワーク名（論理ホスト名）と IP アドレス（クラスタ管理 IP アドレス）は，クライアントアクセス

ポイントとしてリソースグループに登録してください。IP アドレスとして登録している場合は，クライアントアクセスポイントとして登録し直してください。このマニュアルでは，クライアントアクセスポイントとして登録したクラスタ管理 IP アドレスのネットワーク名を論理ホスト名と呼びます。

- 次の文字はリソースグループ名に使用できません。次の文字を使用している場合には，次の文字を含まないリソースグループ名に変更してください。

  ! " &) * ^ | < >

- クラスタ管理アプリケーションへアクセスするには，Administrator 権限を持つドメインユーザーでログインする必要があります。
- インストール前に，次の設定になっていることを確認してください。
  - クラスタソフトウェアにリソースグループを作成している。
  - リソースグループに実行系ノードと待機系ノードが登録されている。
  - クラスタ管理 IP アドレスと共有ディスクがオンラインになっている。
- Global Link Manager のインストールフォルダは，実行系ノードおよび待機系ノードで同じフォルダ構成にしてください。
- Global Link Manager のデータベース格納先は，共有ディスクを指定してください。
- 待機系のインストールが完了するまで，次のコマンドは実行しないでください。
  - Hitachi Command Suite 共通コンポーネントの `hcmds64dbclustersetup` コマンド

4.4 クラスタ環境でのインストールの種類

ここでは，クラスタ環境でのインストールの種類について説明します。

クラスタ環境での Global Link Manager のインストールには，次の 5 つがあります。

- Global Link Manager を新規インストールする場合のクラスタ設定
- Global Link Manager を再インストールまたはアップグレードインストールする場合のクラスタ設定
- Global Link Manager がインストール済み場合のクラスタ設定
- ほかの Hitachi Command Suite 製品がクラスタ構成で運用中の環境に Global Link Manager をインストールする場合のクラスタ設定
- Global Link Manager をアンインストールする場合のクラスタ設定

各インストールを実施するには，次を参照してください。

表 4-1 インストール実施時のマニュアルの参照先

インストールおよびクラスタ設定の種類	ほかの Hitachi Command Suite 製品がインストールされていない場合	ほかの Hitachi Command Suite 製品がクラスタ構成で運用中の場合
新規インストール	4.4.1	4.4.1
再インストールまたはアップグレードインストール	4.4.2	4.4.2 ※
アンインストール	4.4.4	4.4.4
非クラスタ構成からクラスタ構成へ変更	4.4.3	4.4.3 ※

注※ ほかの Hitachi Command Suite 製品はインストールされていないことを前提に，設定手順を記載しています。ほかの Hitachi Command Suite 製品のクラスタ設定については，各製品のマニュアルを参照してください。

4.4.1 クラスタ環境での Global Link Manager の新規インストール

新規インストール時に設定が必要な項目については，「2.1.2 Global Link Manager の新規インストール」を参照してください。

「サーバの IP アドレスまたはホスト名」の設定では，論理ホスト名を入力する必要があります。

注意事項

- ほかの Hitachi Command Suite 製品をインストールする場合は，あわせてインストールしてください。
- 待機系ノードで複数の Hitachi Command Suite 製品を新規インストールする場合は，実行系ノードでインストールした順番で製品をインストールしてください。

(1) Global Link Manager の新規インストール

1. 実行系ノードへの新規インストールから開始します。

   ほかの Hitachi Command Suite 製品がクラスタ構成でインストールされている場合，Hitachi Command Suite 製品のサービスを登録しているリソースグループの所有者を待機系ノードから実行系ノードに移動し，IP アドレスと共有ディスクをオンラインにします。

2. 実行系ノードに Global Link Manager のインストール DVD-ROM をセットします。

   表示されたウィンドウの［Hitachi Global Link Manager Software］の横にある［Install］ボタンをクリックします。

   ウィンドウが表示されない場合は，インストーラー（`setup.exe`）を直接実行してください。

   インストーラーは，*＜インストール DVD-ROM をセットしたドライブ＞*:¥HGLM に格納されています。

   インストーラーが起動すると，Hitachi Global Link Manager のインストールへようこそ（新規）ダイアログが表示されます。

3. ［次へ］ボタンをクリックします。

   クラスタ構成の選択ダイアログが表示されます。「クラスタ構成でインストールする」にチェックを入れてください。ほかの Hitachi Command Suite 製品ですでにクラスタ構成としてセットアップされている場合，クラスタ構成の選択ダイアログは表示されません。

4. ［次へ］ボタンをクリックします。

   クラスタ環境の設定ダイアログが表示されます。次の項目を設定してください。

   ほかの Hitachi Command Suite 製品ですでにクラスタ構成としてセットアップされている場合，クラスタ環境の設定ダイアログは表示されません。

   - 動作モード

     実行系を選択してください。ほかの Hitachi Command Suite 製品がすでにクラスタ構成としてセットアップされている場合は選択不要です。

   - リソースグループ名

     Global Link Manager のサービスを登録するリソースグループ名を指定してください。

     ほかの Hitachi Command Suite 製品でクラスタ構成のセットアップを完了している場合，入力不要です。Hitachi Command Suite 製品のサービスを登録しているリソースグループ名を変更した場合は，変更後のリソースグループ名を指定してください。

   - 論理ホスト名

論理ホスト名を指定してください。ほかの Hitachi Command Suite 製品がすでにクラスタ構成としてセットアップされている場合は指定不要です。

- 実行系ノードのホスト名

  実行系ノードのホスト名を指定してください。ほかの Hitachi Command Suite 製品がすでにクラスタ構成としてセットアップされている場合は指定不要です。

- 待機系ノードのホスト名

  待機系ノードのホスト名を指定してください。ほかの Hitachi Command Suite 製品がすでにクラスタ構成としてセットアップされている場合は指定不要です。

5. ［次へ］ボタンをクリックします。

   Dynamic Link Manager インストーラーダウンロード機能ダイアログが表示されます。

   HDLM インストーラーのダウンロード機能を有効にする場合は，チェックボックスをオンにします。ダウンロード機能を有効にすると，HDLM インストーラーのファイルが Global Link Manager サーバに格納され，クライアントの Web ブラウザーからダウンロードできるようになります。

6. ［次へ］ボタンをクリックします。

   ほかの Hitachi Command Suite 製品がインストールされている場合で，Hitachi Command Suite 製品のサービスがオンラインとなっているときは，Hitachi Command Suite 製品のサービスの停止ダイアログが表示されます。［次へ］ボタンをクリックすると，Hitachi Command Suite 製品のサービスがオフラインとなり，フェールオーバーが抑止されます。

   注意事項

   - Global Link Manager の新規インストールをインストール実行前にキャンセルした場合，Hitachi Command Suite 製品のサービスはオフラインで，フェールオーバーが抑止された状態のままとなります。Global Link Manager を新規インストールしないで Hitachi Command Suite 製品の運用を継続する場合，「(3) クラスタ管理アプリケーションでのサービスオンライン」を参照して Hitachi Command Suite 製品のサービスをオンラインかつフェールオーバーが有効な状態にしてください。

7. ［次へ］ボタンをクリックします。

   インストールフォルダの設定ダイアログが表示されます。

   デフォルトとは別のフォルダにインストールする場合は，インストール先のフォルダを指定します。インストール先のフォルダを指定するときは，次の規則に従ってください。

   - インストールフォルダとして，ドライブ直下（C:¥，D:¥など）を指定しないでください。
   - 62 バイト以下の絶対パスで指定します。
   - 次の半角文字で指定します。

     A〜Z a〜z 0〜9 ． _ スペース

     ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

     また，スペースを 2 文字以上続けて指定できません。

   - OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1〜COM9，LPT1〜LPT9）を含まないように指定します。

   なお，次のフォルダにはインストールできません。

   - %ProgramFiles(x86)%¥以下
   - %CommonProgramFiles(x86)%¥以下
   - %SystemRoot%¥SysWOW64¥以下
   - %SystemRoot%¥system32¥以下
   - %ProgramFiles%¥WindowsApps¥以下

Global Link Manager のデフォルトのインストールフォルダは，次のとおりです。

＜システムドライブ＞:¥Program Files¥HiCommand

Hitachi Command Suite 共通コンポーネントのデフォルトのインストールフォルダは，次のとおりです。

＜システムドライブ＞:¥Program Files¥HiCommand¥Base64

ほかの Hitachi Command Suite 製品がインストールされていないサーバに Global Link Manager をインストールする場合，Global Link Manager と Hitachi Command Suite 共通コンポーネントはインストールフォルダの設定ダイアログで設定したフォルダにインストールされます。すでにほかの Hitachi Command Suite 製品がインストールされているサーバに Global Link Manager をインストールする場合，Global Link Manager はインストールフォルダの設定ダイアログで設定したフォルダにインストールされますが，Hitachi Command Suite 共通コンポーネントは，すでにインストールされているフォルダに上書きされます。Hitachi Command Suite 共通コンポーネントのインストールフォルダを確認する場合は，次のレジストリーキーを確認してください。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi¥HiCommand Base 64¥InstallPath

8. ［次へ］ボタンをクリックします。

Hitachi Global Link Manager のデータベースファイル格納先の設定ダイアログが表示されます。

デフォルトとは別のフォルダに格納する場合は，格納先のフォルダを指定します。格納先のフォルダを指定するときは，次の規則に従ってください。

- データベースファイル格納先フォルダとして，ドライブ直下（C:¥，D:¥など）を指定しないでください。
- 62 バイト以下の絶対パスで指定します。
- 次の半角文字で指定します。

  A〜Z a〜z 0〜9 ． _ スペース

  ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

  また，スペースを 2 文字以上続けて指定できません。
- OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1〜COM9，LPT1〜LPT9）を含まないように指定します。

注意事項

- Hitachi Global Link Manager のデータベースファイルは，"*＜指定した格納先＞*¥x64"フォルダ以下に作成されます。

9. ［次へ］ボタンをクリックします。

32 ビット版の Hitachi Command Suite 共通コンポーネントが存在する環境に，このインストールによって，64 ビット版 Hitachi Command Suite 共通コンポーネントが初めてインストールされる場合，データベース退避先設定ダイアログが表示されます。

Hitachi Command Suite 製品を v7 以前から v8 へアップグレードするために，Hitachi Command Suite 製品のデータベースファイルの退避先を指定してください。デフォルトとは別のフォルダを指定する場合，次の規則に従ってください。

- 148 バイト以下の絶対パスで指定します。
- 次の半角文字で指定します。

  A〜Z a〜z 0〜9 ． _ スペース

  ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

  また，スペースを 2 文字以上続けて指定できません。

- OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1～COM9，LPT1～LPT9）を含まないように指定します。

Hitachi Command Suite 製品のデフォルトのデータベース退避先は，次のとおりです。

<指定した Global Link Manager のインストール先フォルダ>¥databackup

10. ［次へ］ボタンをクリックします。

Hitachi Global Link Manager サーバ情報の設定ダイアログが表示されます。

あらかじめ確認しておいた次の情報を指定します。

- HBase 64 Storage Mgmt Web Service のポート番号
- SNMP Trap 受信機能（［有効にする］または［有効にしない］）

「サーバの IP アドレスまたはホスト名」欄には，クラスタ環境の設定ダイアログで指定した論理ホスト名が非活性で表示され，編集できません。

すでにほかの Hitachi Command Suite 製品がインストールされている場合，次の情報は非活性になります。

- HBase 64 Storage Mgmt Web Service のポート番号

11. ［次へ］ボタンをクリックします。

SNMP Trap 受信機能で［有効にする］を選んだ場合，Hitachi Global Link Manager SNMP Trap 接続情報の設定ダイアログが表示されます。［有効にしない］を選んだ場合は，次の手順へ進んでください。

あらかじめ確認しておいた次の情報を指定します。

- SNMP Trap を受信する IP アドレス（クラスタの論理 IP アドレス）
- SNMP Trap を受信するポート番号

SNMP Trap を受信する IP アドレスには，Global Link Manager サーバの IP アドレスが入力されています。空欄の場合は，サーバの IP アドレスを入力してください。

IPv6 アドレスを指定する場合は，入力する IP アドレスを[ ]で囲んでください。

注意事項

Device Manager がインストールされているサーバに Global Link Manager をインストールする場合，SNMP Trap を受信するポート番号は，162 以外の番号を指定してください。Device Manager で SNMP Trap 受信機能を使用している場合に，Global Link Manager のインストール時に SNMP Trap を受信するポート番号に 162 を指定すると，Device Manager を起動できなくなります。

12. ［次へ］ボタンをクリックします。

Windows ファイアウォール機能がインストールされている場合, Windows ファイアウォール例外登録ダイアログが表示されます。ダイアログの内容を確認して，［次へ］ボタンをクリックしてください。Hitachi Command Suite 共通コンポーネントおよび SNMP Trap を受信するポート番号が，Windows ファイアウォールの例外として登録されます。

注意事項

Windows ファイアウォールの例外登録を実行することで，インストールの時間は約 15 分多く掛かることがあります。Global Link Manager のインストール後にファイアウォールを有効にした場合は，手動で例外に登録する必要があります。手動で例外に登録する方法は，「3.9.2 Windows ファイアウォールを有効にした場合の設定」を参照してください。

13. インストール情報を確認し，［インストール］ボタンをクリックします。

インストール処理が開始され，途中の処理状況を示す幾つかのダイアログが表示されます。

HGLM 設定の完了ダイアログが表示されたら，インストールで設定した情報を確認してください。

HGLM ログイン画面 URL に設定されている値が，Global Link Manager をインストールしたサーバの情報と異なる場合，次を参照し，変更してください。

- IP アドレスの変更：「3.8.1 Global Link Manager にログインするための URL の変更」
- ホスト名の変更：「3.6.2 Global Link Manager サーバのホスト名の変更」
- HBase 64 Storage Mgmt Web Service のポート番号の変更：「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」

14. ［次へ］ボタンをクリックします。

正常にインストールが完了した場合は，インストールの完了ダイアログが表示されます。

15. ［完了］ボタンをクリックして，インストールを完了します。

注意事項

ほかの Hitachi Command Suite 製品がインストールされていない環境への新規インストールの場合，この時点では Global Link Manager が使用するサービスは，リソースグループに登録されていません。

16. パス稼働情報のレポート出力機能を使用する場合は，プロパティファイル（server.properties）を編集します。

server.properties ファイルの格納先を次に示します。
＜*Global Link Manager インストールフォルダ*＞¥conf

レポートの保存先フォルダを，共有ディスク上のフォルダに変更します。

server.pathreport.log_location に＜*レポートの保存先フォルダ*＞を指定します。＜*レポートの保存先フォルダ*＞は，共有ディスク上に配置します。150 バイト以内の絶対パスで指定してください。パスの区切り文字の (¥) は，2 つ続けて指定してください。

記述例を次に示します。

```
server.pathreport.log_location=E:¥¥HGLAM¥¥pathreport
```

パス稼働情報に関するプロパティファイルの設定については，「3.5.1 Global Link Manager サーバの設定の変更」をあわせて参照してください。

17. Hitachi Command Suite 製品のサービスを登録しているリソースグループの所有者を実行系ノードから待機系ノードに移動します。

Microsoft Failover Cluster（Windows Server 2012 以外）を使用する場合：

フェールオーバークラスタ管理で Global Link Manager が使用するサービスを登録しているリソースグループを右クリックし，［このサービスまたはアプリケーションを別のノードに移動］を選択します。

Microsoft Failover Cluster（Windows Server 2012）を使用する場合：

フェールオーバークラスタマネージャーで Global Link Manager が使用するサービスを登録している役割を右クリックし，［移動］－［ノードの選択］を選択します。

18. 待機系ノードに Global Link Manager をインストールします。

クラスタ構成の選択ダイアログで，動作モードとして「待機系」を選択してください。その他の項目は実行系と同じ値を設定してください。

19. クラスタ環境での運用を開始します。

詳細については，「4.4.5 クラスタ環境での Global Link Manager の運用開始」を参照してください。

(2) Microsoft Failover Cluster の設定

Windows Server Failover Clustering の設定をする前に，次の作業を実施してください。

- クラスタ化するサービスの集まり（サービスフェールオーバーの単位）であるクラスタグループ（リソースグループ）を用意してください。
- 実行系と待機系で引き継ぎできる共有ディスクとクラスタ管理 IP アドレスを含めてリソースグループを構成してください。
- リソースの割り当て，削除および動作監視が Windows Server Failover Clustering によって正常に制御できることを確認してください。
- ほかの Hitachi Command Suite 製品が登録されているリソースグループがすでにある場合は，そのリソースグループを使用してください。
- リソースグループは，Hitachi Command Suite 製品に関連するリソースだけで構成してください。

4.4.2 クラスタ環境での Global Link Manager の再インストールまたはアップグレードインストール

すでにクラスタ環境でシステムを構成している状態で，次のインストールを実施する手順について説明します。

- 同一バージョンの Global Link Manager を上書きで再インストール
- 新しいバージョンの Global Link Manager でアップグレードインストール

実行系にしたノードでサービスがオンラインになっていない場合は，オンラインにしてから再インストールまたはアップグレードインストールをしてください。

注意事項

- Global Link Manager の再インストールまたはアップグレードインストール時の注意事項については，「2.1.4 Global Link Manager のアップグレードインストール」を参照してください。

(1) Global Link Manager の再インストールまたはアップグレードインストール

1. クラスタソフトウェアを表示します。
   ［スタート］－［コントロールパネル］－［管理ツール］－［フェールオーバー クラスタ管理］を選択します。
2. Global Link Manager が使用するサービスを登録しているグループを実行系に切り替えます。

   Microsoft Failover Cluster（Windows Server 2012 以外）を使用する場合：

   フェールオーバークラスタ管理で Global Link Manager が使用するサービスを登録しているリソースグループを右クリックし，［このサービスまたはアプリケーションを別のノードに移動］を選択します。

   Microsoft Failover Cluster（Windows Server 2012）を使用する場合：

   フェールオーバークラスタマネージャーで Global Link Manager が使用するサービスを登録している役割を右クリックし，［移動］－［ノードの選択］を選択します。
3. HiRDB が使用するポート番号をデフォルト値※以外に変更して運用している場合は，使用しているポート番号を控えておきます。

   注※

   デフォルト値は次のとおりになります。

   バージョン v8.0.0 以降：22032/tcp
4. データベースのバックアップを取ります。

データベースのバックアップ方法については，「3.4.1 Global Link Manager のデータベースのバックアップ」を参照してください。

5. 実行系ノードに Global Link Manager のインストール DVD-ROM をセットします。

   表示されたウィンドウの［Hitachi Global Link Manager Software］の横にある［Install］ボタンをクリックします。

   ウィンドウが表示されない場合は，インストーラー（setup.exe）を直接実行してください。

   インストーラーは，＜*インストール DVD-ROM をセットしたドライブ*＞:¥HGLM に格納されています。

   インストーラーが起動すると，Hitachi Global Link Manager のインストールへようこそ（上書き）ダイアログが表示されます。

6. ［次へ］ボタンをクリックします。

   Dynamic Link Manager インストーラーダウンロード機能ダイアログが表示されます。

   HDLM インストーラーのダウンロード機能を有効にする場合は，チェックボックスをオンにします。ダウンロード機能を有効にすると，HDLM インストーラーのファイルが Global Link Manager サーバに格納され，クライアントの Web ブラウザーからダウンロードできるようになります。

   すでにダウンロード機能を有効にしてインストール済みの場合は，このダイアログは表示されません。

7. ［次へ］ボタンをクリックします。

   Hitachi Command Suite 共通コンポーネントまたはほかの Hitachi Command Suite 製品のサービスが起動しているときは，Hitachi Command Suite 製品のサービスの停止ダイアログが表示されます。

   ［次へ］ボタンをクリックすると，Hitachi Command Suite 製品のサービスがオフラインとなり，フェールオーバーが抑止されます。

   注意事項

   - Global Link Manager の新規インストールをインストール実行前にキャンセルした場合，Hitachi Command Suite 製品のサービスはオフラインで，フェールオーバーが抑止された状態のままとなります。Global Link Manager を新規インストールしないで Hitachi Command Suite 製品の運用を継続する場合，「(3) クラスタ管理アプリケーションでのサービスオンライン」を参照して Hitachi Command Suite 製品のサービスをオンラインかつフェールオーバーが有効な状態にしてください。

8. ［次へ］ボタンをクリックします。

   32 ビット版の Hitachi Command Suite 共通コンポーネントが存在する環境に，このインストールによって，64 ビット版 Hitachi Command Suite 共通コンポーネントが初めてインストールされる場合，データベース退避先設定ダイアログが表示されます。

   Hitachi Command Suite 製品を v7 以前から v8 へアップグレードするために，Hitachi Command Suite 製品のデータベースファイルの退避先を指定してください。デフォルトとは別のフォルダを指定する場合，次の規則に従ってください。

   - 148 バイト以下の絶対パスで指定します。
   - 次の半角文字で指定します。

     A～Z a～z 0～9 ． _ スペース

     ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

     また，スペースを 2 文字以上続けて指定できません。
   - OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1～COM9，LPT1～LPT9）を含まないように指定します。

   Hitachi Command Suite 製品のデフォルトのデータベース退避先は，次のとおりです。

<指定した Global Link Manager のインストール先フォルダ>¥databackup

9. ［次へ］ボタンをクリックします。

Global Link Manager のプロパティファイルおよび Hitachi Global Link Manager のパス稼働率情報およびプロパティファイルの退避先設定ダイアログが表示されます。デフォルトとは別のフォルダを指定する場合，次の規則に従ってください。

- 138 バイト以下の絶対パスで指定します。
- 次の半角文字で指定します。

  A～Z a～z 0～9 ． _ スペース

  ただし，スペースとピリオドはフォルダ名の先頭と終端には指定できません。

  また，スペースを 2 文字以上続けて指定できません。
- OS が予約済みの名称（CON，AUX，NUL，PRN，CLOCK$，COM1～COM9，LPT1～LPT9）を含まないように指定します。

Global Link Manager のプロパティファイルおよびパス稼働率情報の退避先は，次のとおりです。

<指定した Global Link Manager のインストール先フォルダ>¥databackup

10. ［次へ］ボタンをクリックします。

Windows ファイアウォール機能がインストールされている場合，Windows ファイアウォール例外登録ダイアログが表示されます。ダイアログの内容を確認して，［次へ］ボタンをクリックしてください。Hitachi Command Suite 共通コンポーネントおよび SNMP Trap を受信するポート番号が，Windows ファイアウォールの例外として登録されます。

注意事項

Windows ファイアウォールの例外登録を実行することで，インストールの時間は約 15 分多く掛かることがあります。Global Link Manager のインストール後にファイアウォールを有効にした場合は，手動で例外に登録する必要があります。手動で例外に登録する方法は，「3.9.2 Windows ファイアウォールを有効にした場合の設定」を参照してください。

11. インストール情報を確認し，［インストール］ボタンをクリックします。

インストール処理が開始され，途中の処理状況を示す幾つかのダイアログが表示されます。上書きインストールでは，Global Link Manager のデータベースは初期化されません（データベースファイルが壊れている場合を除く）。HGLM 設定の完了ダイアログが表示されたら，インストールで設定した情報を確認してください。

HGLM ログイン画面 URL に設定されている値が，Global Link Manager をインストールしたサーバの情報と異なる場合，次を参照し，変更してください。

- IP アドレスの変更：「3.8.1 Global Link Manager にログインするための URL の変更」
- ホスト名の変更：「3.6.2 Global Link Manager サーバのホスト名の変更」
- HBase 64 Storage Mgmt Web Service のポート番号の変更：「3.7.1 HBase 64 Storage Mgmt Web Service へのアクセスに使用するポート番号の変更」

12. ［次へ］ボタンをクリックします。

正常にインストールが完了した場合は，インストールの完了ダイアログが表示されます。

13. ［完了］ボタンをクリックして，インストールを完了します。

Hitachi Command Suite 共通コンポーネントのサービスは，オフラインとなっています。

14. パス稼働情報のレポート出力機能を使用する場合で，レポートの保存先が共有ディスクになっていないときは，プロパティファイル（server.properties）を編集します。

server.properties ファイルの格納先を次に示します。

< Global Link Manager インストールフォルダ >¥conf

レポートの保存先フォルダを，共有ディスク上のフォルダに変更します。

`server.pathreport.log_location` に＜*レポートの保存先フォルダ*＞を指定します。＜*レポートの保存先フォルダ*＞は，共有ディスク上に配置します。150 バイト以内の絶対パスで指定してください。パスの区切り文字の (¥) は，2 つ続けて指定してください。

記述例を次に示します。

```
server.pathreport.log_location=E:¥¥HGLAM¥¥pathreport
```

パス稼働情報に関するプロパティファイルの設定については，「3.5.1 Global Link Manager サーバの設定の変更」をあわせて参照してください。

15. アップグレードまたは上書きインストール前の環境で，HiRDB が使用するポート番号をデフォルト値以外に変更して運用していた場合，ポート番号を設定します。

    Global Link Manager のバージョンが v8 より前の場合，HiRDB が使用するポート番号の設定がデフォルト値（22032/tcp）に戻ります。このため，ポート番号をデフォルト値以外に変更して運用していた場合，控えておいたアップグレードまたは上書きインストール前の環境でのポート番号と同じ番号を設定します。

    重要：Hitachi File Services Manager を使用している場合は，控えておいたアップグレードまたは上書きインストール前の環境でのポート番号とは異なる番号を設定してください。

16. Global Link Manager のサービスを登録するリソースグループの所有者を実行系ノードから待機系ノードに移動します。

    Microsoft Failover Cluster（Windows Server 2012 以外）を使用する場合：

    フェールオーバークラスタ管理で Global Link Manager が使用するサービスを登録しているリソースグループを右クリックし，［このサービスまたはアプリケーションを別のノードに移動］を選択します。

    Microsoft Failover Cluster（Windows Server 2012）を使用する場合：

    フェールオーバークラスタマネージャーで Global Link Manager が使用するサービスを登録している役割を右クリックし，［移動］－［ノードの選択］を選択します。

17. 待機系ノードに Global Link Manager を上書きまたはアップグレードインストールします。

    クラスタ構成の選択ダイアログで，動作モードは「待機系」を選択してください。その他の項目は実行系と同じ値を設定してください。

18. クラスタ環境での運用を開始します。

    詳細については，「4.4.5 クラスタ環境での Global Link Manager の運用開始」を参照してください。

4.4.3 Global Link Manager がインストール済みの場合のクラスタ設定

非クラスタ構成で Global Link Manager のシステムの運用を開始したあとで，クラスタ構成に変更する場合の手順について説明します。ここでは，すでに運用を開始している Global Link Manager を実行系ノードとする場合を想定しています。

非クラスタ構成からクラスタ構成にする場合は，Global Link Manager のクラスタ設定として，次の設定が必要です。

- 実行系ノードの場合：手順 2，手順 7～8
- 待機系ノードの場合：手順 10

注意事項

- 一度アンインストールする手順になります。クラスタ構成に移行する前にカスタマイズしていた設定は，クラスタ構成へ移行後に再度設定し直す必要があります。移行する前に設定した情報を控えておいてください。

- Tuning Manager をクラスタ環境に移行する場合，製品のデータは移行できません。
- 手順を実施する前に，実行系ノードではクラスタ管理 IP アドレス，および共有ディスクが有効になっていることを確認してください。これらが有効になっていない場合は，次の手順を先に実施して，クラスタ管理 IP アドレス，および共有ディスクのリソースをオンラインにしてください。

  「(2) Microsoft Failover Cluster の設定」
- Global Link Manager のインストールフォルダは，実行系ノードおよび待機系ノードで同じフォルダ構成にしてください。
- この手順を実行すると，HiRDB が使用するポートの設定がデフォルト値（22032）に戻ります。ポート番号を変更して運用している場合は，あとで設定し直す必要があるので，使用しているポート番号を控えておいてください。

1. 次のコマンドを実行して，データベースをエクスポートします。Hitachi Command Suite 製品のデータベースが一括でエクスポートされます。

   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥Base64¥bin¥hcmds64dbtrans /export /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞ /auto

   ＜*作業用フォルダ*＞には，データベース情報を一時的に格納するためのフォルダを，絶対パスで指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，エクスポート処理が中断します。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。

   ＜*アーカイブファイル*＞には，エクスポートするデータベースのアーカイブファイルを絶対パスで指定します。

   /auto オプションを指定すると，Hitachi Command Suite 製品のサービスを自動的に起動または停止します。

2. パス稼働情報のレポート出力機能を使用していた場合は，すでに出力済みのパス稼働情報（パスステータスログ）を共有ディスクへ移動します。

   パス稼働情報（パスステータスログ）をエクスポートします。

   次のコマンドを実行してください。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamexport /dir ＜*エクスポート先フォルダ名*＞

   ＜*エクスポート先フォルダ名*＞は絶対パスで指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。

   ＜*エクスポート先フォルダ名*＞に使用できる文字を次に示します。

   A～Z，a～z，0～9，'.'，'_'，そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。

   コマンドの実行例を次に示します。

   ```
   "C:¥Program Files¥HiCommand¥HGLAM¥bin¥hglamexport" /dir "C:¥hglam
   export"
   ```

3. 非クラスタ環境で HiRDB が使用するポート番号をデフォルト（22032/tcp）以外に変更している場合は，ポート番号を控えてください。
4. Global Link Manager をアンインストールします。

   ほかの Hitachi Command Suite 製品（v8）がインストールされている場合は，あわせてアンインストールします。
5. 実行系ノードに Global Link Manager をインストールします。

   詳細については，「4.4.1 クラスタ環境での Global Link Manager の新規インストール」を参照してください。
6. 次のコマンドを実行して，データベースをインポートします。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥Base64¥bin¥hcmds64dbtrans /import /workpath ＜*作業用フォルダ*＞ /file ＜*アーカイブファイル*＞ /type ALL /auto

＜*作業用フォルダ*＞には，アーカイブファイルを展開するためのフォルダを，絶対パスで指定します。ローカルディスクの空のフォルダを指定してください。空のフォルダ以外を指定した場合は，インポート処理は中断されます。この場合は，空のフォルダを指定して，もう一度 hcmds64dbtrans コマンドを実行してください。＜*アーカイブファイル*＞には，移行元サーバから転送したデータベースのアーカイブファイルを，絶対パスで指定します。

アーカイブファイルを使用しない場合

- ＜*作業用フォルダ*＞には移行元から転送したデータベース情報を格納したフォルダを指定してください。このとき，転送したフォルダ以下のファイル構成は変更しないでください。
- /file オプションは指定しないでください。

/type オプションには，原則として ALL を指定します。

Global Link Manager のデータベースをインポートするには，「/type HGLAM」または「/type GlobalLinkAvailabilityManager」を指定します。

Global Link Manager のデータベースだけではなく，ほかの Hitachi Command Suite 製品のデータベースもインポートする場合は，「/type ALL」を指定するか，またはデータベースを移行する Hitachi Command Suite 製品の名称をコンマで区切って指定します。/type オプションに指定するほかの Hitachi Command Suite 製品の名称は，それぞれのマニュアルを参照してください。

ALL を指定した場合は，移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され，移行されます。複数の製品を指定した場合は，指定したすべての製品のデータベースが，アーカイブファイルまたは＜*作業用フォルダ*＞に指定したフォルダにあり，かつ，指定したすべての製品が移行先にインストールされている必要があります。条件を満たさない製品が 1 つでもある場合，移行は実行されません。

注意事項

- Hitachi Command Suite 製品によってインポートの手順が異なります。Global Link Manager 以外のデータベースを移行する場合は，それぞれの Hitachi Command Suite 製品のマニュアルを参照してください。
- 移行元のマシンに，Replication Monitor 04-20 以前のバージョンがインストールされている場合，データベースを移行できません。事前に移行元および移行先の Replication Monitor を 05-00 以降にバージョンアップしてから移行してください。05-00 以降にバージョンアップできない場合，またはデータベースの移行が不要な場合，/type オプションで Replication Monitor 以外の製品をすべて指定してコマンドを実行してください。

7. プロパティファイル（server.properties）を編集します。

server.properties ファイルの格納先を次に示します。
＜*Global Link Manager インストールフォルダ*＞¥conf

レポートの保存先フォルダを，共有ディスク上のフォルダに変更します。

server.pathreport.log_location に＜*レポートの保存先フォルダ*＞を指定します。＜*レポートの保存先フォルダ*＞は，共有ディスク上に配置します。150 バイト以内の絶対パスで指定してください。パスの区切り文字の (¥) は，2 つ続けて指定してください。

記述例を次に示します。

```
server.pathreport.log_location=E:¥¥HGLAM¥¥pathreport
```

8. パス稼働情報（パスステータスログ）をインポートします。

次のコマンドを実行してください。

＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamimport /report ＜*エクスポートデータ格納先フォルダ名*＞

＜*エクスポートデータ格納先フォルダ名*＞には，hglamexport コマンドでエクスポートしたデータの格納先フォルダを絶対パスで指定します。

注意事項

コマンド実行前に手順 7 で指定した保存先のフォルダは削除，または空にしておいてください。

フォルダが空ではない場合，フォルダの中身は削除されます。

9. 待機系ノードに Global Link Manager をインストールします。

詳細については，「4.4.1 クラスタ環境での Global Link Manager の新規インストール」を参照してください。

10. パス稼働情報のレポート出力機能を使用する場合は，プロパティファイル（server.properties）を編集します。

パス稼働情報のレポート出力機能を使用しない場合は，この手順は不要です。

server.properties ファイルの格納先を次に示します。

＜*Global Link Manager インストールフォルダ*＞¥conf

レポートの保存先フォルダを，共有ディスク上のフォルダに変更します。

server.pathreport.log_location に＜*レポートの保存先フォルダ*＞を指定します。＜*レポートの保存先フォルダ*＞は，実行系ノードで指定したフォルダと同じフォルダを指定してください。

11. 非クラスタ環境で HiRDB が使用するポート番号をデフォルト（22032/tcp）以外に変更していた場合は，手順 3 で控えたポート番号と同じ番号を，実行系および待機系の両方で再設定します。

12. クラスタ環境での運用を開始します。

詳細については，「4.4.5 クラスタ環境での Global Link Manager の運用開始」を参照してください。

4.4.4 クラスタ環境での Global Link Manager のアンインストール

ここでは，クラスタ構成となっている場合の Global Link Manager をアンインストールする手順について説明します。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に停止されます。

1. クラスタソフトウェアを表示します。

［スタート］－［コントロールパネル］－［管理ツール］－［フェールオーバー クラスタ管理］を選択します。

2. Global Link Manager のサービスを登録しているリソースグループの所有者を待機系ノードから実行系ノードに移動します。

Microsoft Failover Cluster（Windows Server 2012 以外）を使用する場合：

フェールオーバークラスタ管理で Global Link Manager が使用するサービスを登録しているリソースグループを右クリックし，［このサービスまたはアプリケーションを別のノードに移動］を選択します。

Microsoft Failover Cluster（Windows Server 2012）を使用する場合：

フェールオーバークラスタマネージャーで Global Link Manager が使用するサービスを登録している役割を右クリックし，［移動］－［ノードの選択］を選択します。

3. 実行系ノードで，Global Link Manager をアンインストールします。

   Global Link Manager のアンインストールについては，「2.1.6 Global Link Manager のアンインストール」を参照してください。

4. Global Link Manager のサービスを登録しているリソースグループの所有者を実行系ノードから待機系ノードに移動します。

5. 待機系ノードで，Global Link Manager をアンインストールします。

6. 次のリソースがほかのアプリケーションによって使用されていない場合は，クラスタ管理アプリケーションで，そのリソースをオフラインにしてから削除します。

   - クラスタ管理 IP アドレス
   - 共有ディスク

   Hitachi Command Suite 製品のサービスを登録したリソースグループが不要になった場合は，そのリソースグループも削除してください。

7. クラスタ環境での運用を開始します。

   詳細については，「4.4.5 クラスタ環境での Global Link Manager の運用開始」を参照してください。

4.4.5 クラスタ環境での Global Link Manager の運用開始

ここでは，クラスタ構築完了後に運用を開始する手順（ライセンス登録，サービスのオンライン）について説明します。

(1) 新規インストール，または非クラスタ環境から移行した場合

1. Global Link Manager のサービスを登録しているリソースグループの所有者が待機系ノードのホスト名になっていることを確認します。待機系ノードのホスト名になっていない場合は，実行系ノードから待機系ノードに移動します。

2. `hcmds64clustersrvstate` コマンドを実行して，リソースグループおよび Global Link Manager 製品のサービスをオンラインにします。

   コマンドについては，「(3) クラスタ管理アプリケーションでのサービスオンライン」を参照してください。

3. 待機系ノードで，使用する製品のライセンスを GUI で登録します。論理ホスト名にアクセスしてください。インストールする製品ごとに，ライセンスキーの入力が必要です。

   ライセンスの設定方法については，「2.2 ライセンスの初期設定」を参照してください。

4. Hitachi Command Suite 製品のサービスを登録しているリソースグループの所有者を待機系ノードから実行系ノードに移動します。

5. 実行系ノードで，使用する製品のライセンスを GUI で登録します。論理ホスト名にアクセスしてください。インストールする製品ごとに，ライセンスキーの入力が必要です。

   ライセンスの設定方法については，「2.2 ライセンスの初期設定」を参照してください。

(2) バージョンアップ／上書きインストール，またはアンインストールした（アンインストール後にほかの Hitachi Command Suite 製品が残る）場合

1. Global Link Manager のサービスを登録しているリソースグループの所有者を待機系ノードから実行系ノードに移動します。

2. hcmds64clustersrvstate コマンドを実行して，リソースグループおよび Hitachi Command Suite 製品のサービスをオンラインにします。

   コマンドについては，「(3) クラスタ管理アプリケーションでのサービスオンライン」を参照してください。

4.5 クラスタ環境に登録する Global Link Manager のサービス

管理サーバでクラスタ管理アプリケーションに登録する Global Link Manager のサービスを次の表に示します。

表 4-2 管理サーバでクラスタ管理アプリケーションに登録する Global Link Manager のサービス

プログラムプロダクト名	サービス表示名	サービス名
Global Link Manager	HiRDB/ClusterService _HD1	HiRDBClusterService_HD1
	HBase 64 Storage Mgmt Web Service	HBase64StgMgmtWebService
	HBase 64 Storage Mgmt Web SSO Service	HBase64StgMgmtWebSSOService
	HBase 64 Storage Mgmt SSO Service	HBase64StgMgmtSSOService
	Global Link Manager Web Service	GlobalLinkManagerWebService

注

ほかの Hitachi Command Suite 製品のサービスについては，各マニュアルを参照してください。

4.6 クラスタ環境で使用するコマンド

ここでは，クラスタ環境で使用するコマンドについて説明します。

4.6.1 クラスタセットアップユーティリティ

クラスタセットアップユーティリティでは，クラスタ管理アプリケーションへの操作ができます。

クラスタ管理アプリケーションからリソースを削除してしまった場合や，インストール中のサービス登録を失敗した場合に，クラスタ管理アプリケーションへのリソース登録・削除・オンライン・オフラインが自動で行えます。

(1) クラスタ管理アプリケーションへのサービスの登録

クラスタ管理アプリケーションのリソースグループに Hitachi Command Suite 製品のサービスを登録するには，次のコマンドを実行します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞¥Base64¥ClusterSetup¥hcmds64clustersrvupdate /sreg /r *＜リソースグループ名＞* /sd *＜ドライブレター名＞* /ap *＜クライアントアクセスポイントとして設定したリソース名＞*

- /sreg

  指定したリソースグループに，Hitachi Command Suite 製品のサービスを登録します。

- /r

  リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

, ; = スペース

また，次に示す文字は使用できません。

! " &) * ^ | < >

- /sd

  リソースグループに登録している共有ディスクのドライブ名を指定します。

  このオプションには複数のドライブ名を指定できません。Hitachi Command Suite 製品のデータを複数の共有ディスクに分割している場合，共有ディスクごとに hcmds64clustersrvupdate コマンドを実行してください。

- /ap

  クライアントアクセスポイントとして設定したリソース名を指定します。

(2) クラスタ管理アプリケーションからサービスを削除

クラスタ管理アプリケーションのリソースグループから Hitachi Command Suite 製品のサービスを削除するには，次のコマンドを実行します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞
¥Base64¥ClusterSetup¥hcmds64clustersrvupdate /sdel /r *＜リソースグループ名＞*

- /sdel

  指定したリソースグループから，Hitachi Command Suite 製品のサービスを削除します。バージョン v7.x.x および v8.x.x のサービスが削除されます。

- /r

  リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

  , ; = スペース

  また，次に示す文字は使用できません。

  ! " &) * ^ | < >

注意事項

- Hitachi File Services Manager がインストールされている環境では，Hitachi File Services Manager に使用されるサービスは削除されません。
- リソースグループに登録されたサービスに任意の名称を設定している場合，削除前の名称は保持できません。次回サービス登録時に設定し直してください。

(3) クラスタ管理アプリケーションでのサービスオンライン

クラスタ管理アプリケーションに登録した Hitachi Command Suite 製品のサービスをオンラインにし，フェールオーバーを有効にするには，次のコマンドを実行します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞
¥Base64¥ClusterSetup¥hcmds64clustersrvstate /son /r *＜リソースグループ名＞*

- /son

  クラスタ管理アプリケーションに設定したリソースグループをオンラインにし，フェールオーバーを有効にします。

- /r

  リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

  , ; = スペース

  また，次に示す文字は使用できません。

  ! " &) * ^ | < >

(4) クラスタ管理アプリケーションでのサービスオフライン

クラスタ管理アプリケーションに登録した Hitachi Command Suite 製品のサービスをオフラインにし，フェールオーバーを抑止するには，次のコマンドを実行します。

＜Hitachi Command Suite 共通コンポーネントのインストールフォルダ＞
¥Base64¥ClusterSetup¥hcmds64clustersrvstate /soff /r *＜リソースグループ名＞*

- /soff

  クラスタ管理アプリケーションに設定した Hitachi Command Suite 製品のサービスをオフラインにし，フェールオーバーを抑止します。

- /r

  リソースグループ名を指定します。リソースグループ名に次の文字が含まれる場合は，リソースグループ名を引用符（"）で囲んでください。

  , ; = スペース

  また，次に示す文字は使用できません。

  ! " &) * ^ | < >

5

通信に関するセキュリティの設定

この章では，Global Link Manager で利用できる通信に関するセキュリティ設定について説明します。

5.1 サーバとクライアント間のセキュリティ設定

遠隔地からインターネットまたはイントラネットを介して，Global Link Manager GUI から Global Link Manager サーバにアクセスする場合，第三者によるデータの傍受や改ざんを防ぐため，SSL を使用して通信データを暗号化しておくことをお勧めします。

SSL を使用するには，次の設定が必要です。

1. Global Link Manager サーバで HBase 64 Storage Mgmt Web Service に SSL の設定をします。
2. Global Link Manager GUI で Global Link Manager にログインするときに，「`https://`」から始まる URL を設定します。

HBase 64 Storage Mgmt Web Service では，TLS のバージョン 1.2 をサポートしています。

SSL 通信のための HBase 64 Storage Mgmt Web Service の設定

HBase 64 Storage Mgmt Web Service では，公開鍵暗号方式を採用しています。SSL の設定は，サーバで次の流れで実施します。

認証局（CA）が署名した証明書を使用する場合：

1. 秘密鍵，および証明書発行要求（CSR）を作成します。
2. 認証局（CA）へ CSR を送付します。
3. CA から証明書を入手します。
4. プロパティファイルを編集します。
5. Hitachi Command Suite 共通コンポーネントを再起動します。

自己署名証明書を使用する場合：

1. 秘密鍵，証明書発行要求（CSR），および自己署名証明書を作成します。
2. プロパティファイルを編集します。
3. Hitachi Command Suite 共通コンポーネントを再起動します。

5.1.1 秘密鍵，証明書発行要求，および自己署名証明書の作成

Hitachi Command Suite 共通コンポーネントで秘密鍵および証明書発行要求（CSR）を作成するには，`hcmds64ssltool` コマンドを使用します。

`hcmds64ssltool` コマンドを実行すると，RSA 暗号および楕円曲線暗号（ECC）に対応した 2 種類の秘密鍵，証明書発行要求，および自己署名証明書が作成されます。 証明書発行要求は，PEM 形式で作成されます。なお，自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。

事前に完了しておく操作

- Administrator 権限でのログイン

事前に確認しておく情報

- 証明書発行要求の要件（認証局に確認）
- 管理クライアントで使用する Web ブラウザーのバージョン
  管理クライアント（GUI）で使用する Web ブラウザーが，サーバ証明書の署名アルゴリズムに対応している必要があります。

- 既存の秘密鍵，証明書発行要求，および自己署名証明書の格納先（再作成する場合）

  出力先パスに同じ名称のファイルがある場合，ファイルを上書きして作成できません。再作成する場合は，既存の格納先以外に出力してください。

コマンドの形式

- ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64ssltool [/key ＜*秘密鍵ファイル*＞] [/csr ＜*証明書発行要求ファイル*＞] [/cert ＜*自己署名証明書ファイル*＞] [/certtext ＜*自己署名証明書の内容ファイル*＞] [/validity ＜*有効日数*＞] [/dname ＜*DN*＞] [/sigalg ＜*RSA 暗号用のサーバ証明書の署名アルゴリズム*＞] [/keysize ＜*RSA 暗号用の秘密鍵のキーサイズ*＞] [/eccsigalg ＜*楕円曲線暗号用のサーバ証明書の署名アルゴリズム*＞] [/ecckeysize ＜*楕円曲線暗号用の秘密鍵のキーサイズ*＞]

オプション

key

秘密鍵の出力先パスを絶対パスで指定します。

RSA 暗号用の秘密鍵は指定したファイル名で出力されます。楕円曲線暗号用の秘密鍵は指定したファイル名の先頭に ecc-が付いて出力されます。

オプションの指定を省略すると，httpsdkey.pem ファイルおよび ecc-httpsdkey.pem ファイルが出力されます。※

csr

証明書発行要求の出力先パスを絶対パスで指定します。

RSA 暗号用の証明書発行要求は指定したファイル名で出力されます。楕円曲線暗号用の証明書発行要求は指定したファイル名の先頭に ecc-が付いて出力されます。

オプションの指定を省略すると，httpsd.csr ファイルおよび ecc-httpsd.csr ファイルが出力されます。※

cert

自己署名証明書の出力先パスを絶対パスで指定します。

RSA 暗号用の自己署名証明書は指定したファイル名で出力されます。楕円曲線暗号用の自己署名証明書は指定したファイル名の先頭に ecc-が付いて出力されます。

オプションの指定を省略すると，httpsd.pem ファイルおよび ecc-httpsd.pem ファイルが出力されます。※

certtext

自己署名証明書の内容（テキスト形式）の出力先パスを絶対パスで指定します。

RSA 暗号用の自己署名証明書の内容は指定したファイル名で出力されます。楕円曲線暗号用の自己署名証明書の内容は指定したファイル名の先頭に ecc-が付いて出力されます。

オプションの指定を省略すると，httpsd.txt ファイルおよび ecc-httpsd.txt ファイルが出力されます。※

validity

自己署名証明書の有効期間を日数で指定します。このオプションを指定すると，RSA 暗号用と楕円曲線暗号用で同じ内容が指定されます。指定を省略した場合は，有効期間は 3650 日になります。

dname

自己署名証明書と証明書発行要求に記述する DN を指定します。オプションの指定を省略すると，対話形式で DN を指定できます。

DN は属性型と属性値を等号（=）でまとめ，各属性をコンマ（,）で区切って指定します。DN には引用符（"）および円記号（¥）は指定できません。また，DN の属性値は RFC2253 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに円記号（¥）でエスケープしてください。

DN の先頭または末尾の空白文字

DN の先頭の番号記号（#）

DN に含まれる正符号（+），コンマ（,），セミコロン（;），始め山括弧（<），等号（=）および終わり山括弧（>）

DN に指定する属性型および属性値を次の表に示します。

表 5-1 DN に指定する属性型および属性値（hcmds64ssltool）

属性型	属性型の正式名称	属性値
CN	Common Name	管理サーバ（HBase 64 Storage Mgmt Web Service）のホスト名を指定します。この項目は必須です。 管理クライアント（GUI）から管理サーバ（Hitachi Command Suite 共通コンポーネントの HBase 64 Storage Mgmt Web Service）に接続するときに使用するホスト名（FQDN 形式でも可）を指定します。管理サーバをクラスタ環境で運用している場合には，論理ホスト名を指定してください。
OU	Organizational Unit Name	組織の構成単位名を指定します。
O	Organization Name	組織名を指定します。この項目は必須です。
L	Locality Name	市区町村名または地域名を指定します。
ST	State or Province Name	都道府県名を指定します。
C	Country Name	2 文字の国コードを指定します。

`sigalg`

RSA 暗号用のサーバ証明書の署名アルゴリズムを指定します。`SHA1withRSA`，`SHA256withRSA` または `SHA512withRSA` を指定できます。指定を省略した場合，署名アルゴリズムは SHA256withRSA になります。

`keysize`

RSA 暗号用の秘密鍵のキーサイズをビットで指定します。`2048`，`3072`，または `4096` を指定できます。指定を省略した場合，キーサイズは 2048 ビットになります。

`eccsigalg`

楕円曲線暗号用のサーバ証明書の署名アルゴリズムを指定します。`SHA512withECDSA`，`SHA384withECDSA`，`SHA256withECDSA`，または `SHA1withECDSA` を指定できます。指定を省略した場合，署名アルゴリズムは SHA384withECDSA になります。

`ecckeysize`

楕円曲線暗号用の秘密鍵のキーサイズをビットで指定します。`256` または `384` を指定できます。指定を省略した場合，キーサイズは 384 ビットになります。

注※

オプションの指定を省略すると，次の場所にファイルが出力されます。

- ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥httpsd¥conf¥ssl¥server¥

5.1.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請

作成した Hitachi Command Suite 共通コンポーネントの証明書発行要求（CSR）を認証局に送信し，電子署名を受けます。

事前に完了しておく操作

- Hitachi Command Suite 共通コンポーネントの証明書発行要求の作成

事前に確認しておく情報

- 認証局への申請方法や対応状況

  X.509 PEM 形式のサーバ証明書を発行してもらう必要があります。申請方法については，使用する認証局の Web サイトなどで確認してください。

  また，証明書の署名アルゴリズムに，認証局が対応していることを確認してください。

Hitachi Command Suite 共通コンポーネントのサーバ証明書を認証局に申請するには：

1. 作成した証明書発行要求を認証局に送付します。

認証局からの返答は保存しておいてください。

重要 認証局が発行する証明書には有効期限があります。期限が切れる前に再発行してもらう必要があります。証明書の有効期限は，`hcmds64checkcerts` コマンドを使用して確認してください。

5.1.3 SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集

Hitachi Command Suite 共通コンポーネントの SSL/TLS を有効にする場合や，管理サーバのホスト名やポート番号などを変更する場合は，`user_httpsd.conf` ファイルを編集します。

事前に完了しておく操作

- Hitachi Command Suite 共通コンポーネントの秘密鍵の作成（SSL/TLS の有効化に必要）※
- Hitachi Command Suite 共通コンポーネントのサーバ証明書の準備（SSL/TLS の有効化に必要）※

  認証局から返送されたサーバ証明書を準備します。暗号化通信のテストなどの目的の場合は，自己署名証明書でもかまいません。

注※

次の場所にコピーしておくことをお勧めします。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥httpsd¥conf¥ssl¥server

事前に確認しておく情報

- 証明書発行要求の `Common Name` に設定したホスト名（SSL/TLS の有効化に必要）

user_httpsd.conf ファイルを編集するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. `user_httpsd.conf` ファイルを編集します。
3. Hitachi Command Suite 製品のサービスを起動します。

user_httpsd.conf ファイルの格納場所

- ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥httpsd¥conf¥user_httpsd.conf

user_httpsd.conf ファイルの例（デフォルト）

```
ServerName ＜ホスト名＞          ●―――― 管理サーバのホスト名
Listen [::]:22015                ●―――― 非SSL通信用のポート番号（IPv6環境用）
Listen 22015                     ●―――― 非SSL通信用のポート番号
#Listen 127.0.0.1:22015
SSLEngine Off
#Listen [::]:22016               ●―――― SSL通信用のポート番号（IPv6環境用）
#Listen 22016                    ●―――― SSL通信用のポート番号
#<VirtualHost *:22016>           ●―――― SSL通信用のポート番号
#  ServerName ＜ホスト名＞       ●―――― 管理サーバのホスト名
#  SSLEngine On
#  SSLProtocol +TLSv1.2 +TLSv1.3
#  SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_
CHACHA20_POLY1305_SHA256
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
#  SSLCertificateKeyFile "＜Hitachi Command Suite共通コンポーネントのインストール
フォルダ＞/uCPSB11/httpsd/conf/ssl/server/httpsdkey.pem"
#  SSLCertificateFile "＜Hitachi Command Suite共通コンポーネントのインストールフォ
ルダ＞/uCPSB11/httpsd/conf/ssl/server/httpsd.pem"
#  SSLCertificateKeyFile "＜Hitachi Command Suite共通コンポーネントのインストール
フォルダ＞/uCPSB11/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
#  SSLCertificateFile "＜Hitachi Command Suite共通コンポーネントのインストールフォ
ルダ＞/uCPSB11/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "＜Hitachi Command Suite共通コンポーネントのインストールフ
ォルダ＞/uCPSB11/httpsd/conf/ssl/cacert/anycert.pem"
#  Header set Strict-Transport-Security max-age=31536000
#</VirtualHost>
#HWSLogSSLVerbose On
```

重要 非クラスタ環境の場合，user_httpsd.conf ファイルの VirtualHost と ServerName には，user_httpsd.conf ファイルの先頭に記載されている ServerName と同じホスト名が入力されていることを確認してください。ホスト名を変更した場合は，VirtualHost と ServerName（2 か所）も変更する必要があります。クラスタ環境の場合，VirtualHost と ServerName には，cluster.conf ファイルの virtualhost と同じ論理ホスト名を指定します。VirtualHost と ServerName を指定する場合は，大文字と小文字を区別する必要があります。

(1) SSL/TLS の有効化

SSL を有効にするには，次の手順を実行します。

同じマシンにほかの Hitachi Command Suite 製品がインストールされている場合，Hitachi Command Suite 共通コンポーネントを起動または停止すると，ほかの Hitachi Command Suite 製品のサービスも一緒に起動または停止されます。ただし，ほかの Hitachi Command Suite 製品のバージョンが 5.7 より前の場合は，手動でサービスを起動または停止する必要があります。ほかの Hitachi Command Suite 製品のサービスの起動および停止方法については，各製品のマニュアルを参照してください。

1. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを停止します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop
2. 秘密鍵ファイルと，CA から返送された署名済みの証明書ファイルまたは自己署名証明書ファイルを，適切なフォルダにコピーします。
   次のフォルダにコピーすることを推奨します。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞
¥uCPSB11¥httpsd¥conf¥ssl¥server

3. user_httpsd.conf ファイルを開きます。
4. 対応する行の先頭にあるシャープ記号（#）を削除して，SSL ポートとホスト名の設定を有効にします。
5. 「SSLCertificateFile」に CA から返送された証明書ファイル，または自己署名証明書ファイルを絶対パスで指定します。
6. 「SSLCertificateKeyFile」に Web サーバの秘密鍵ファイルを絶対パスで指定します。
7. チェインした CA によって発行された証明書を使用する場合，「SSLCACertificateFile」にチェインした CA の証明書ファイルを絶対パスで指定します。
   複数の証明書ファイル（PEM 形式）をテキストエディターで連結させることで，1 つのファイルに複数の証明書を混在させることができます。
8. 次のコマンドを実行して，Hitachi Command Suite 共通コンポーネントを起動します。
   ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin
   ¥hcmds64srv /start

次の図は，SSL/TLS を有効にする一例です。ここでは，CA から返送された証明書（httpsd.pem）と秘密鍵（httpsdkey.pem）が＜*Hitachi Command Suite 共通コンポーネントのインストールディレクトリ*＞/uCPSB11/httpsd/conf/ssl/server フォルダに格納されている場合を示しています。

参考

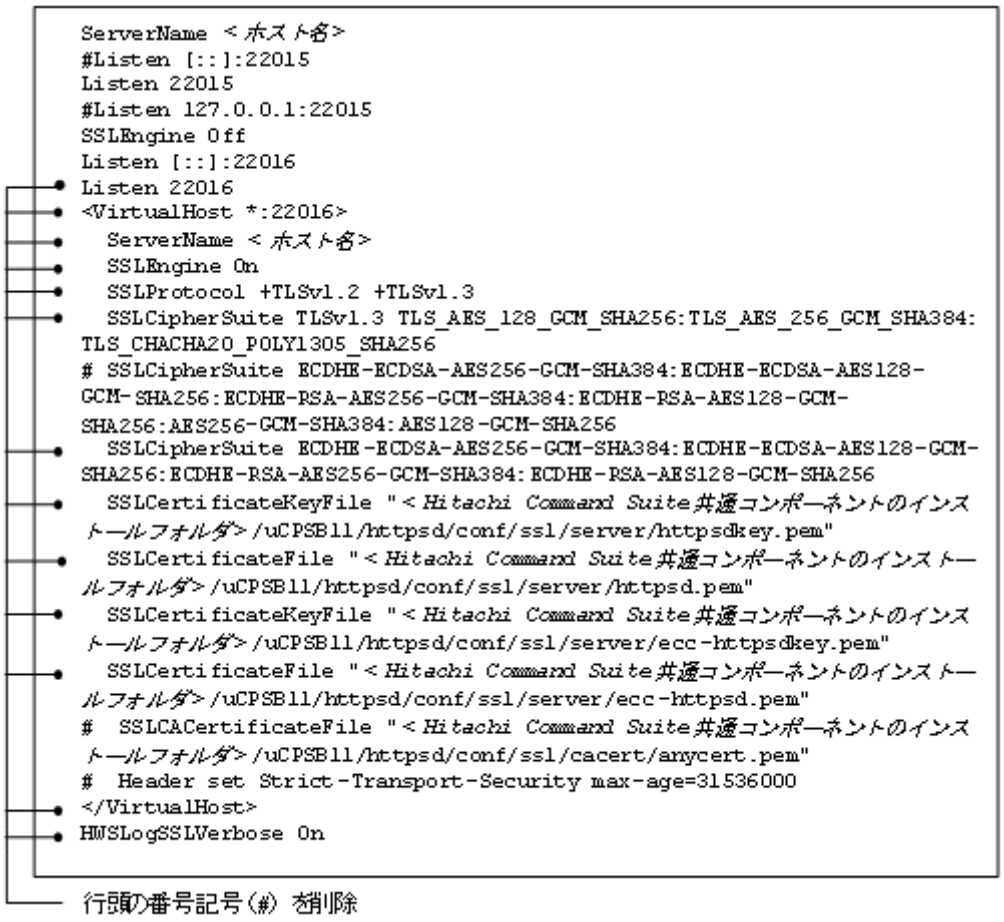
シャープ記号（#）で始まる行は，コメント行です。

SSL/TLS の有効化に必要な設定

重要 ディレクティブを編集する際は，次の点に注意してください。

- ディレクティブを重複して指定しないでください。
- 1 つのディレクティブの途中で改行しないでください。
- 各ディレクティブに指定するパスには，シンボリックリンクやジャンクションを指定しないでください。
- 各ディレクティブに指定する証明書および秘密鍵ファイルには，PEM 形式のファイルを指定してください。
- httpsd.conf ファイルおよび hsso_httpsd.conf ファイルは編集しないでください。

- 次の行頭の番号記号（#）を削除します。



- 先頭行の ServerName ディレクティブと<VirtualHost>タグ内の ServerName ディレクティブに，証明書発行要求の Common Name に設定したホスト名（クラスタ環境の場合は論理ホスト名）を指定します。大文字，小文字の区別も同じにしてください。
- SSLCertificateKeyFile ディレクティブに，RSA 暗号の Hitachi Command Suite 共通コンポーネントの秘密鍵ファイルを絶対パスで指定します。
- SSLCertificateFile ディレクティブに，RSA 暗号の Hitachi Command Suite 共通コンポーネントのサーバ証明書を絶対パスで指定します。
- SSLCertificateKeyFile ディレクティブに，楕円曲線暗号の Hitachi Command Suite 共通コンポーネントの秘密鍵ファイルを絶対パスで指定します。RSA 暗号だけを使用する場合，この設定は不要です。
- SSLCertificateFile ディレクティブに，楕円曲線暗号の Hitachi Command Suite 共通コンポーネントのサーバ証明書を絶対パスで指定します。RSA 暗号だけを使用する場合，この設定は不要です。
- Hitachi Command Suite 共通コンポーネントのサーバ証明書を発行した認証局が中間認証局の場合は，SSLCACertificateFile ディレクティブの行頭の番号記号（#）を削除して，すべての中間認証局の証明書を絶対パスで指定します。複数の証明書をテキストエディターで連結させることで，1 つのファイルに複数の証明書を混在させることができます。
- IPv6 環境の場合，#Listen [::]:22016 の行頭の番号記号（#）を削除します。

重要

- SSL を有効にする場合や Global Link Manager を IPv6 環境で運用する場合でも，Listen 22015 の行を削除したり，コメント行にしたりしないでください。

  外部から管理サーバへの非 SSL 通信を遮断したい場合は，Listen [::]:22015 と Listen 22015 の行頭に番号記号（#）を追記してコメント行にしたあと，#Listen 127.0.0.1:22015 の行頭の番号記号を

削除してください。この場合に，Hitachi File Services Manager や Storage Navigator Modular 2 と連携しているときは，Hitachi File Services Manager または Storage Navigator Modular 2 の hcmdsprmset コマンドに print オプションを指定して実行し，出力されたホスト名から 127.0.0.1 への名前解決ができることを確認してください。名前解決ができなければ，OS の環境設定で名前解決ができるようにしてください。OS の環境設定でも名前解決ができなければ，hosts ファイルに任意のホスト名と 127.0.0.1 を設定し，hcmdsprmset コマンドの host オプションに hosts ファイルに設定したホスト名を指定して実行してください。

- Hitachi Command Suite をバージョン 8.8.2 以前からアップグレードインストールしても，user_httpsd.conf ファイルに楕円曲線暗号の内容は反映されません。楕円曲線暗号を使用する場合，次の場所に格納されているサンプルファイルから，SSLRequiredCiphers ディレクティブ，SSLECCCertificateKeyFile ディレクティブおよび SSLECCCertificateFile ディレクティブの内容をコピーして使用してください。

  ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥sample¥httpsd¥conf¥user_httpsd.conf

- Hitachi File Services Manager や Storage Navigator Modular 2 と連携している場合に SSL/TLS を有効にするときは，次の場所に格納されている httpsd.conf ファイルも編集してください。

  ＜*Hitachi File Services Manager または Storage Navigator Modular 2 のインストールフォルダ*＞¥Base¥httpsd¥conf¥httpsd.conf

  編集方法については，Hitachi File Services Manager または Storage Navigator Modular 2 のマニュアルを参照してください。

参考 SSL/TLS を無効にするには，user_httpsd.conf ファイルの例（デフォルト）を参考に，Listen 22016 から HWSLogSSLVerbose On までの行頭に番号記号（#）を追記して，コメント行にしてください。

(2) SSL の無効化

SSL を無効にするには，user_httpsd.conf ファイルで SSL ポートとホストの設定をコメントにします。user_httpsd.conf ファイルを編集する前に，ほかの Hitachi Command Suite 製品のサービスおよび Hitachi Command Suite 共通コンポーネントを停止してください。編集した後は Hitachi Command Suite 共通コンポーネントを起動します。

次の表は，SSL を無効にする一例です。

参考

シャープ記号（#）で始まる行は，コメント行です。

表 5-2 SSL の無効化

```
ServerName www.example.com
#Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLEngine Off
#Listen [::]:22016
#Listen 22016
#<VirtualHost *:22016>
#  ServerName www.example.com
#  SSLEngine On
#  SSLProtocol +TLSv1.2 +TLSv1.3
#  SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
#  SSLCertificateKeyFile C:/Program Files/HiCommand/Base64/uCPSB11/httpsd/
conf/ssl/server/httpsdkey.pem
#  SSLCertificateFile C:/Program Files/HiCommand/Base64/uCPSB11/httpsd/conf/ssl/
server/httpsd.pem
#  SSLCertificateKeyFile C:/Program Files/HiCommand/Base64/uCPSB11/httpsd/
conf/ssl/server/ecc-httpsdkey.pem
#  SSLCertificateFile C:/Program Files/HiCommand/Base64/uCPSB11/httpsd/conf/ssl/
server/ecc-httpsd.pem
```

```
#  SSLCACertificateFile C:/Program Files/HiCommand/Base64/uCPSB11/httpsd/
conf/ssl/cacert/anycert.pem
#  Header set Strict-Transport-Security max-age=31536000
#</VirtualHost>
#HWSLogSSLVerbose On
```

(3) SSL に割り当てられたポート番号の変更

HBase 64 Storage Mgmt Web Service の SSL のデフォルトポートは，22016 です。ポートを変更するには，user_httpsd.conf ファイルで Listen 設定とホストのポートを変更します。user_httpsd.conf ファイルを編集する前に，ほかの Hitachi Command Suite 製品のサービスおよび Hitachi Command Suite 共通コンポーネントを停止してください。編集した後は Hitachi Command Suite 共通コンポーネントを起動します。

5.2 サーバと LDAP ディレクトリサーバ間のセキュリティ設定

Hitachi Command Suite 製品では，LDAP ディレクトリサーバと連携してユーザー認証を行う場合に，Hitachi Command Suite 共通コンポーネントと LDAP ディレクトリサーバ間のネットワーク伝送を StartTLS で暗号化できます。管理サーバと LDAP ディレクトリサーバ間の通信を StartTLS で保護するためには次の作業が必要です。

- LDAP ディレクトリサーバの証明書の入手
- トラストストアーファイルへの証明書のインポート

なお，Hitachi Command Suite 共通コンポーネントと LDAP ディレクトリサーバ間のネットワーク伝送を StartTLS で暗号化するためには，exauth.properties ファイルの設定も必要です。exauth.properties ファイルでの設定については，「(2) exauth.properties ファイルの設定（認証方式が LDAP の場合）」を参照してください。

注意事項

LDAP ディレクトリサーバのサーバ証明書の CN は，exauth.properties ファイルの auth.ldap.＜*auth.server.name に指定した値*＞.host プロパティに指定した値（LDAP ディレクトリサーバへアクセスするためのホスト名）と一致している必要があります。

5.2.1 LDAP ディレクトリサーバの証明書の入手

管理サーバと通信する LDAP ディレクトリサーバのサーバ証明書を入手します。詳細は，利用する LDAP ディレクトリサーバのマニュアルを参照してください。

著名な CA から LDAP ディレクトリサーバの証明書を取得している場合は，Hitachi Command Suite 共通コンポーネントが参照する標準のトラストストアーにすでに CA 証明書が設定されている可能性があるので，次のコマンドを実行して確認してください。すでに登録されている CA 証明書によって，LDAP ディレクトリサーバの証明書が認証される場合は，「5.2.2 トラストストアーファイルへの証明書のインポート」で説明するトラストストアー jssecacerts の設定は不要です。

hcmds64keytool -list -v -keystore ＜*トラストストアーファイル名*＞ -storepass ＜*トラストストアーへのアクセスパスワード*＞

- -keystore ＜*トラストストアーファイル名*＞には，参照するトラストストアーファイルを指定します。

  ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥jdk¥lib

¥security¥cacerts

- -storepass <*トラストストアーへのアクセスパスワード*>には，トラストストアー cacerts を参照するためのパスワードを指定します。デフォルトは「changeit」です。

実行例を次に示します。

```
"C:¥Program Files¥HiCommand¥Base64¥jdk¥bin¥hcmds64keytool" -list -v -
keystore "C:¥Program Files¥HiCommand¥Base64¥jdk¥lib¥security¥cacerts" -
storepass changeit
```

注意事項

- トラストストアー cacerts は，Hitachi Command Suite 共通コンポーネントをバージョンアップすると更新されるため，cacerts に独自の証明書をインポートして運用することは避けてください。
- 認証局が発行するサーバ証明書には有効期限があります。有効期限が切れないように注意してください。

  サーバ証明書の有効期限の確認については，「5.6.2 証明書の有効期限の確認」を参照してください。

5.2.2 トラストストアーファイルへの証明書のインポート

LDAP ディレクトリサーバの証明書を Hitachi Command Suite 共通コンポーネントで利用するトラストストアーにインポートします。Hitachi Command Suite 共通コンポーネントで利用するトラストストアー（jssecacerts）を次の場所に格納します。トラストストアーファイルが存在しない場合は新規に作成してください。

<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥uCPSB11¥jdk¥lib¥security¥jssecacerts

トラストストアーファイルの作成，証明書のインポートおよび内容確認には，hcmds64keytool ユーティリティを使用します。格納場所を次に示します。

<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥bin¥hcmds64keytool.exe

トラストストアーファイルの作成，および証明書のインポートには，次のコマンドを実行してください。

hcmds64keytool -import -alias *<トラストストアー内のユニーク名>* -file *<証明書ファイル>* -keystore *<トラストストアーファイル名>* -storepass *<トラストストアーへのアクセスパスワード>* -storetype JKS

- -alias *<トラストストアー内のユニーク名>*には，トラストストアー内で証明書を識別するための名称を指定します。
- -file *<証明書ファイル>*には，証明書ファイルを指定します。
- -keystore *<トラストストアーファイル名>*には，登録・作成するトラストストアーファイルとして，jssecacerts を指定してください。
- -storepass <*トラストストアーへのアクセスパスワード*>には，トラストストアー（jssecacerts）にアクセスするためのパスワードを指定します。

例えば，証明書ファイルが C:¥tmp¥ldapcert.der，トラストストアーへのアクセスパスワードが changeit で，トラストストアー内のユニーク名を ldaphost とする場合，hcmds64keytool ユーティリティを使用して証明ファイルをインポートするコマンドは次のようになります。

```
"C:¥Program Files¥HiCommand¥Base64¥jdk¥bin¥hcmds64keytool" -import -alias
ldaphost -file C:¥tmp¥ldapcert.der -keystore "C:¥Program Files¥HiCommand
¥Base64¥uCPSB11¥jdk¥lib¥security¥jssecacerts" -storepass changeit -
storetype JKS
```

また，トラストストアーの内容を表示するには，次のコマンドを実行してください。

```
hcmds64keytool -list -v -keystore <トラストストアーファイル名> -storepass <
トラストストアーへのアクセスパスワード>
```

- `-keystore <トラストストアーファイル名>`には，登録・作成するトラストストアーファイルとして，`jssecacerts` を指定してください。
- `-storepass <トラストストアーへのアクセスパスワード>`には，トラストストアー `jssecacerts` を更新するためのパスワードを指定します。

  ```
  "C:¥Program Files¥HiCommand¥Base64¥jdk¥bin¥hcmds64keytool" -list -v -
  keystore "C:¥Program Files¥HiCommand¥Base64¥uCPSB11¥jdk¥lib¥security
  ¥jssecacerts" -storepass changeit
  ```

なお，トラストストアーを適用するためには，Hitachi Command Suite 製品のサービスおよび Hitachi Command Suite 共通コンポーネントを再起動する必要があります。

注意事項

- 証明書ファイルが複数ある場合は，`jssecacerts` 内で使用されていない任意のエイリアス名を指定して，インポートしてください。
- `hcmds64keytool` ユーティリティで，トラストストアー内のユニーク名，トラストストアーのファイル名，およびパスワードを指定するときには，次の点に注意してください。
  - ファイル名には次の記号を使用しないでください。

    `: , ; * ? " < > |`
  - ファイル名は 255 バイト以内の文字列にしてください。
  - トラストストアー内のユニーク名，およびパスワードには「"」を含めないでください。

5.3 サーバと HDLM 間のセキュリティ設定

HDLM ホストと SSL 通信するには，HDLM ホストの共通エージェントコンポーネントを SSL サーバとして使用します。共通エージェントコンポーネントを SSL サーバとして使用するためには，キーペアとサーバ証明書を準備する必要があります。

共通エージェントコンポーネントを SSL サーバとして使用する要件を示します。

ホストの要件

- HDLM のバージョンが 8.5.0 以降の必要があります。

注意事項

共通エージェントコンポーネントでは，Windows 用および Linux 用の JRE をバンドルしています。

ただし，Red Hat Enterprise Linux 5，Red Hat Enterprise Linux 6，SUSE LINUX Enterprise Server 11，Oracle Linux 6，および Oracle Unbreakable Enterprise Kernel 6 でバンドルしている JRE は，`server.properties` の `server.agent.ciphers` プロパティのデフォルト値で指定し

た暗号方式に対応していません。Red Hat Enterprise Linux 5，Red Hat Enterprise Linux 6，SUSE LINUX Enterprise Server 11，Oracle Linux 6，または Oracle Unbreakable Enterprise Kernel 6 を SSL サーバとして使用するには，Oracle 社の JRE を使用する必要があります。使用できる Oracle 社の JRE については，HDLM のマニュアルを参照してください。なお，IPF マシンに対応する JRE はリリースされていないため，Linux の IPF マシンを SSL サーバとして使用できません。

使用する JRE にあわせて，共通エージェントコンポーネントの `server.properties` ファイルにある `server.agent.JRE.location` プロパティの値を変更してください。

5.3.1 共通エージェントコンポーネントのキーペアおよび証明書発行要求の作成

HDLM ホストマシンでキーペアと証明書発行要求を作成するには，`hbsa_ssltool` コマンドを使用します。なお，自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。

前提条件

- Administrator 権限（Windows の場合）または root（UNIX の場合）でのログイン
- 共通エージェントコンポーネントの既存のキーストアーファイルの削除（再作成する場合）
  共通エージェントコンポーネントで作成できるキーストアーファイルは 1 つだけです。

コマンドの形式

Windows の場合：

＜共通エージェントコンポーネントのインストールフォルダ＞¥bin¥hbsa_ssltool.bat -key *＜キーストアーファイル名＞* -csr *＜証明書発行要求ファイル＞* -keypass *＜秘密鍵のパスワード＞* -storepass *＜キーストアーパスワード＞* [-cert *＜自己署名証明書ファイル＞*] [-keyalg *＜選択する鍵アルゴリズム＞*] [-validity *＜有効日数＞*] [-dname *＜DN＞*]

注　VMware 版の HDLM を使用している場合は，リモート管理クライアントの Windows 上でコマンドを実行します。

UNIX の場合：

＜共通エージェントコンポーネントのインストールディレクトリ＞/bin/hbsa_ssltool.sh -key *＜キーストアーファイル名＞* -csr *＜証明書発行要求ファイル＞* -keypass *＜秘密鍵のパスワード＞* -storepass *＜キーストアーパスワード＞* [-cert *＜自己署名証明書ファイル＞*] [-keyalg *＜選択する鍵アルゴリズム＞*] [-validity *＜有効日数＞*] [-dname *＜DN＞*]

オプション

`key`

キーストアーファイルの出力先を絶対パスで指定します。パスに空白が含まれる場合は，パスの前後に`'"'`を指定します。Windows の場合は，パスの区切り文字にスラント（/）を指定してください。255 バイト以内の文字列で指定してください。指定できない特殊文字を示します。

: , ; * ? " < > | -

`csr`

証明書発行要求の出力先を絶対パスで指定します。パスに空白が含まれる場合は，パスの前後に'"'を指定します。Windows の場合は，パスの区切り文字にスラント（/）を指定してください。255 バイト以内の文字列で指定してください。指定できない特殊文字を示します。

: , ; * ? " < > | -

keypass

秘密鍵のパスワードを 6 文字以上で指定します。keypass オプションと storepass オプションには，同じパスワードを指定してくださ い。パスワードに空白が含まれる場合は，パスワードの前後に'"'を指 定します。次の半角文字で指定します。

A～Z a～z 0～9 スペース

storepass

キーストアーのパスワードを 6 文字以上で指定します。storepass オプションと keypass オプションには，同じパスワードを指定してくださ い。パスワードに空白が含まれる場合は，パスワードの前後に'"'を指 定します。次の半角文字で指定します。

A～Z a～z 0～9 スペース

cert

自己署名証明書の出力先を絶対パスで指定します。パスに空白が含まれる場合は，パスの前後に'"'を指定します。Windows の場合は，パスの区切り文字にスラント（/）を指定してください。255 バイト以内の文字列で指定してください。指定できない特殊文字を示します。

: , ; * ? " < > | -

keyalg

暗号アルゴリズムとして、以下の値のいずれかを指定します。RSA 暗号を使用する場合は RSA、楕円曲線暗号を使用する場合は EC を指定します。オプションの指定を省略した場合はデフォルト値の RSA が設定されます。

- RSA or EC

証明書発行要求および自己署名証明書は，RSA または EC の指定に応じて以下の値で作成されます。

RSA 暗号を使用する場合：

秘密鍵のキーサイズ 2048 ビット，キーアルゴリズム RSA，署名アルゴリズム SHA256withRSA

楕円曲線暗号を使用する場合：

秘密鍵のキーサイズ 384 ビット，キーアルゴリズム EC，署名アルゴリズム SHA384withECDSA

validity

自己署名証明書の有効期間を日数で指定します。指定を省略した場合，有効期間は 3650 日になります。

dname

自己署名証明書と証明書発行要求に記述する DN を指定します。オプションの指定を省略すると，対話形式で DN を指定できます。

DN は属性型と属性値を等号（=）でまとめ，各属性をコンマ（,）で区切って指定します。DN には引用符（"）および円記号（¥）は指定できません。また，DN の属性値は RFC2253 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに円記号（¥）でエスケープしてください。

DN の先頭または末尾の空白文字

DN の先頭の番号記号（#）

DN に含まれる正符号（+），コンマ（,），セミコロン（;），始め山括弧（<），等号（=）および終わり山括弧（>）

DN に指定する属性型および属性値を次の表に示します。

表 5-3 DN に指定する属性型および属性値（hbsa_ssltool）

属性型	属性型の正式名称	属性値
CN	Common Name	サーバマシンのホスト名を指定します。この項目は必須です。
OU	Organizational Unit Name	組織の構成単位名を指定します。
O	Organization Name	組織名を指定します。この項目は必須です。
L	Locality Name	市区町村名または地域名を指定します。
S	State or Province Name	都道府県名を指定します。
C	Country Name	2 文字の国コードを指定します。

5.3.2 共通エージェントコンポーネントのサーバ証明書の認証局への申請

認証局へのサーバ証明書の申請は，通常，オンラインで行えます。作成した共通エージェントコンポーネントの証明書発行要求（CSR）を認証局に送信し，電子署名を受けます。

前提条件

- 共通エージェントコンポーネントの証明書発行要求の作成
- 次の情報の確認
  - 認証局への申請方法や対応状況

    利用する認証局が SHA256withRSA および SHA384withECDSA での署名に対応していることを確認してください。 申請方法については，使用する認証局の Web サイトなどで確認してください。

操作手順

1. 作成した証明書発行要求を認証局に送付します。

操作結果

認証局で発行されたサーバ証明書は，通常，E メールで送付されます。認証局からの返答は保存しておいてください。

重要 認証局が発行する証明書には有効期限があります。期限が切れる前に再発行してもらう必要があります。

5.3.3 共通エージェントコンポーネントのサーバ証明書のキーストアーへのインポート

共通エージェントコンポーネントのキーストアーにサーバ証明書をインポートするには，keytool ユーティリティを使用します。

前提条件

- Administrator 権限（Windows の場合）または root（UNIX の場合）でのログイン
- 認証局の証明書の入手

サーバ証明書を発行した認証局から，中間認証局，ルート認証局に至る全認証局の証明書が必要です。

- 認証局で署名された共通エージェントコンポーネントのサーバ証明書の入手
- 次の情報の確認
  - キーストアーファイルの情報

    自己署名証明書の作成時に用意したキーストアーファイルの情報が必要です。

    ・絶対パス

    ・アクセスパスワード

操作手順

1. 次のコマンドを実行して，認証局の証明書および共通エージェントコンポーネントのサーバ証明書をインポートします。

   コマンドは証明書ごとに実行してください。

   Windows の場合：

   <共通エージェントコンポーネントのインストールフォルダ>¥bin¥hbsa_keytool.bat -import -alias *<エイリアス名>* -keystore *<キーストアーファイル名>* -file *<証明書のファイル名>* -storetype JKS

   注　VMware 版の HDLM を使用している場合は，リモート管理クライアントの Windows 上でコマンドを実行します。

   UNIX の場合：

   <JDK または JRE のインストールディレクトリ>/bin/keytool -import -alias *<エイリアス名>* -keystore *<キーストアーファイル名>* -file *<証明書のファイル名>* -storetype JKS

   - alias：キーストアー内で証明書を識別するための名称を指定します。
   - keystore：キーストアーファイルを絶対パスで指定します。
   - file：証明書のファイル名を絶対パスで指定します。

5.3.4 共通エージェントコンポーネントでの SSL/TLS の有効化

SSL/TLS を有効にするには，HDLM ホストで共通エージェントコンポーネントの server.properties を設定する必要があります。

「A.3 共通エージェントコンポーネントの設定の変更」を参照し，次のプロパティを必要に応じて設定してください。

- server.https.port
- server.agent.secure
- server.agent.ciphers

5.3.5 共通エージェントコンポーネントのサーバ証明書の確認

共通エージェントコンポーネントのサーバ証明書を確認するには，keytool ユーティリティを使用します。サーバ証明書には有効期限があります。有効期限切れに注意してください。

操作手順

1. 次のコマンドを実行します。

Windows の場合：

＜共通エージェントコンポーネントのインストールフォルダ＞¥bin
¥hbsa_keytool.bat -printcert -v -file ＜証明書のファイル名＞

注　VMware 版の HDLM を使用している場合は，リモート管理クライアントの Windows 上でコマンドを実行します。

UNIX の場合：

＜JDK または JRE のインストールディレクトリ＞/bin/keytool -printcert -v -file ＜証明書のファイル名＞

5.3.6 ファイアウォールの例外登録

共通エージェントコンポーネントが SSL 通信で使用するポート番号をファイアウォールの例外として登録します。登録方法については，「A.2 HDLM を使用する場合のファイアウォールの設定」を参照してください。

5.4 サーバと Device Manager 間のセキュリティ設定

Device Manager と SSL 通信するには，Device Manager サーバを SSL サーバとして使用します。

Device Manager サーバを SSL サーバとして構築する方法については，「Hitachi Command Suite システム構成ガイド」を参照してください。

5.5 SSL クライアントの構築

HDLM ホストまたは Device Manager サーバと SSL で通信するには，SSL サーバで作成されたサーバ証明書を SSL クライアント（Global Link Manager サーバ）にインポートする必要があります。

注意事項

次の操作を実行した場合は，Global Link Manager を再起動する必要があります。

- 5.5.2 Global Link Manager サーバのトラストストアーへの証明書のインポート
- 5.5.5 Global Link Manager サーバのトラストストアーにインポートされた証明書の削除

両方の操作を実行する場合は，操作のつど Global Link Manager を再起動する必要はありません。両方の操作を実行したあと，一度の再起動でかまいません。

5.5.1 HDLM ホストまたは Device Manager サーバの証明書の確認

HDLM ホストまたは Device Manager サーバのサーバ証明書を確認するには，hglamkeytool ユーティリティを使用します。サーバ証明書には有効期限があります。有効期限切れに注意してください。

操作手順

1. 次のコマンドを実行します。

   ＜Global Link Manager のインストールフォルダ＞¥bin¥hglamkeytool.bat -printcert -v -file ＜証明書のファイル名＞

オプション

`file`

証明書ファイルを絶対パスで指定します。

5.5.2 Global Link Manager サーバのトラストストアーへの証明書のインポート

HDLM ホストや Device Manager サーバのサーバ証明書を Global Link Manager サーバのトラストストアーへインポートするには，`hglamkeytool` ユーティリティを使用します。トラストストアーを適用するためには，Global Link Manager を再起動する必要があります。

注意事項

クラスタ環境で運用する際に，Global Link Manager で使用するトラストストアーファイルを共有ディスク以外に配置する場合は，待機系ノードにも実行系ノードと同様の手順で証明書をインポートする必要があります。

操作手順

1. 次のコマンドを実行します。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamkeytool.bat -importcert -alias ＜*エイリアス名*＞ -file ＜*証明書のファイル名*＞ -keystore ＜*トラストストアーファイル名*＞ -storepass ＜*トラストストアーへのアクセスパスワード*＞ -storetype JKS

オプション

`alias`

トラストストアー内で証明書を識別するための名称を指定します。

`file`

証明書ファイルを絶対パスで指定します。

`keystore`

インポート先のトラストストアーファイルを絶対パスで指定します。

トラストストアーファイルが存在しない場合は，指定先に自動生成されます。

`storepass`

トラストストアーへのアクセスパスワードを指定します。

5.5.3 Global Link Manager サーバのトラストストアーにインポートされた証明書の確認

Global Link Manager のトラストストアーの内容を表示するには，`hglamkeytool` ユーティリティを使用します。

サーバ証明書の有効期限の確認については，「5.6.2 証明書の有効期限の確認」を参照してください。

操作手順

1. 次のコマンドを実行します。

＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamkeytool.bat -list -keystore ＜*トラストストアーファイル名*＞ -storepass ＜*トラストストアーへのアクセスパスワード*＞

オプション

keystore

インポート先のトラストストアーファイルを絶対パスで指定します。

storepass

トラストストアーへのアクセスパスワードを指定します。

5.5.4 Global Link Manager サーバのトラストストアーパスワードの変更

Global Link Manager サーバのトラストストアーパスワードを変更するには，hglamkeytool ユーティリティを使用します。

操作手順

1. 次のコマンドを実行します。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamkeytool.bat -storepasswd -keystore ＜*トラストストアーファイル名*＞

オプション

keystore

パスワードを変更するトラストストアーファイルを絶対パスで指定します。

5.5.5 Global Link Manager サーバのトラストストアーにインポートされた証明書の削除

トラストストアーにインポートされた証明書を削除するには，hglamkeytool ユーティリティを使用します。トラストストアーを適用するためには，Global Link Manager を再起動する必要があります。

操作手順

1. 次のコマンドを実行します。

   ＜*Global Link Manager のインストールフォルダ*＞¥bin¥hglamkeytool.bat -delete -alias ＜*エイリアス名*＞ -keystore ＜*トラストストアーファイル名*＞ -storepass ＜*トラストストアーへのアクセスパスワード*＞

オプション

alias

トラストストアー内で証明書を識別するための名称を指定します。

keystore

削除したいサーバ証明書が格納されているトラストストアーファイルを絶対パスで指定します。

storepass

トラストストアーへのアクセスパスワードを指定します。

5.5.6 Global Link Manager サーバでの SSL/TLS の有効化

SSL/TLS を有効にするには，Global Link Manager サーバの server.properties ファイルで次のプロパティを設定する必要があります。

HDLM ホストと SSL 通信する場合：

- server.https.enable
- server.https.truststore

Device Manager と SSL 通信する場合：

- server.https.enable
- server.https.truststore
- server.hdvm.https.ipaddr

各プロパティの設定方法については，「3.5.1 Global Link Manager サーバの設定の変更」を参照してください。

各プロパティを設定後，Global Link Manager を再起動してください。

5.6 高度なセキュリティ設定

次のセキュリティ要件を満たす構成で Global Link Manager を運用するためには，SSL/TLS 通信のための設定やユーザーパスワードの設定が必要です。

デジタル署名のハッシュアルゴリズム

SHA-256 以上

暗号アルゴリズム

RSA（キーサイズ：2048 ビット以上）

AES（キーサイズ：128 ビット以上）

3KeyTDES

ここでは，Global Link Manager を高度なセキュリティ設定で運用するために必要な作業について説明します。

5.6.1 管理クライアントとの通信のために必要な設定（Hitachi Command Suite 共通コンポーネントの設定）

高度なセキュリティ設定で管理サーバと管理クライアント（GUI）の間を通信するためには，Hitachi Command Suite 共通コンポーネントで次の作業が必要です。

(1) 秘密鍵と証明書発行要求（CSR）の作成

秘密鍵，認証局（CA）に送信する証明書発行要求（CSR），および自己署名証明書を hcmds64ssltool コマンドを使用して作成します。hcmds64ssltool コマンドを実行すると，CSR および自己署名証明書が，次のように作成されます。

- RSA 暗号の場合：秘密鍵のキーサイズ 2048 ビット，署名アルゴリズム SHA256withRSA
- 楕円曲線暗号の場合：秘密鍵のキーサイズは ecckeysize で指定した値（ビット），署名アルゴリズム SHA384withECDSA

作成した CSR ファイルを CA に提出し，署名済みの証明書を発行してもらいます。CSR は，PEM 形式で作成されます。CSR に設定する情報に関する注意事項については，使用する CA に確認してください。なお，CA が発行する証明書には通常，有効期限があります。期限が切れる前に再発行してもらう必要があります。

注意事項

- 外部の CA を利用する場合は，SHA256withRSA および SHA384withECDSA での署名に対応していることを確認してください。
- hcmds64ssltool コマンドでは，自己署名証明書も作成できますが，暗号化通信のテストなどの目的でだけ使用することをお勧めします。

hcmds64ssltool コマンドについては，「5.1.1 秘密鍵，証明書発行要求，および自己署名証明書の作成」を参照してください。

5.6.2 証明書の有効期限の確認

証明書や認証局の証明書の有効期限を確認するには，hcmds64checkcerts コマンドを使用します。

サーバ証明書には有効期限がありますので，有効期限切れにご注意ください。

事前に完了しておく操作

- Administrator 権限でのログイン

事前に確認しておく情報

- Hitachi Command Suite 共通コンポーネントのサーバ証明書や認証局の証明書の有効期限を確認する場合

  hcmds64checkcerts コマンドでは，user_httpsd.conf ファイルで指定している証明書の有効期限が確認できます。このため，user_httpsd.conf ファイルに次の証明書のパスを指定してください。

  - Hitachi Command Suite 共通コンポーネントのサーバ証明書

    RSA 暗号および楕円曲線暗号の証明書を使用している場合，それぞれで指定が必要です。
  - すべての中間認証局の証明書
- Global Link Manager サーバのトラストストアーへインポートした HDLM ホストや Device Manager サーバのサーバ証明書の有効期限を確認する場合

  server.properties ファイルで次のプロパティを設定してください。

  - server.https.enable プロパティに true を設定
  - server.https.truststore プロパティにトラストストアーファイルを設定

  Global Link Manager サービスは起動されている必要があります。

コマンドの形式

- ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64checkcerts { [/days ＜*日数*＞] [/log] | /all }

オプション

days

有効期限切れの証明書があるか確認する日付を，コマンドの実行日からの日数で指定します。指定できる値の範囲は 30～3652（10 年）です。このオプションを指定すると，指定した日数

以内に有効期限が切れる証明書，およびすでに有効期限が切れている証明書が表示されます。オプションの指定を省略すると，日数に 30 が指定されます。

`log`

表示対象の証明書がある場合，Windows のイベントログに警告メッセージが出力されます。このコマンドを OS のタスクなどに登録して，定期的に証明書の有効期限を確認する場合，このオプションを指定してください。

`all`

Hitachi Command Suite 共通コンポーネントのサーバ証明書や認証局の証明書の場合は，`user_httpsd.conf` ファイルで指定したすべての証明書の有効期限が表示されます。

Global Link Manager サーバのトラストストアーへインポートした HDLM ホストや Device Manager サーバのサーバ証明書の場合は，`server.https.truststore` プロパティに指定したトラストストアーファイル内のすべての証明書の有効期限が表示されます。

5.6.3 LDAP ディレクトリサーバとの通信のために必要な設定

管理サーバと LDAP ディレクトリサーバの間を高度なセキュリティ設定で StartTLS 通信するためには，SHA256withRSA および SHA384withECDSA で署名されたサーバ証明書を Hitachi Command Suite 共通コンポーネントのトラストストアーにインポートする必要があります。

サーバ証明書の確認方法およびインポート方法については，「5.2 サーバと LDAP ディレクトリサーバ間のセキュリティ設定」を参照してください。

5.6.4 ユーザーパスワードの設定

Hitachi Command Suite 製品では，ユーザーのパスワードをハッシュ化してデータベースに保存しています。バージョン 6.4 以降では，より安全性が高いハッシュ方式に変更されています。

バージョン 6.4 以降を更新インストールした場合，またはバージョン 6.3 以前の Hitachi Command Suite 製品でエクスポートしたデータベースをインポートした場合，新しいハッシュ方式で保存するためには，GUI でユーザーパスワードを再設定する必要があります。

5.6.5 システム構成上の注意事項

管理クライアントで使用するブラウザーが SHA256withRSA および SHA384withECDSA で署名された証明書に対応している必要があります。

6

ほかの製品と連携するための Global Link Manager の設定

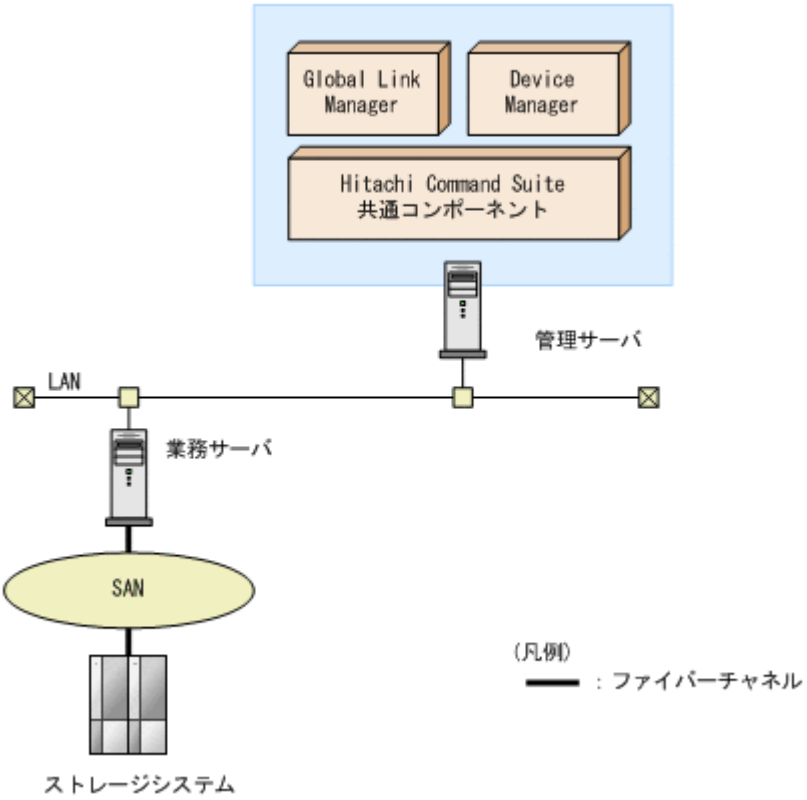
この章では，ほかの製品と連携するための Global Link Manager での設定について説明します。

6.1 Hitachi Command Suite 製品のシングルサインオンおよびユーザー管理の統合の概要

Device Manager など，ほかの Hitachi Command Suite 製品と連携することで，シングルサインオンおよびユーザー管理の統合を実現します。シングルサインオン機能を使用することによって，Global Link Manager GUI のダッシュボードからほかの Hitachi Command Suite 製品を起動する場合に，ユーザー ID およびパスワードを指定する必要がなくなります。ダッシュボードについては，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。

Hitachi Command Suite 製品が 1 台のサーバにインストールされている場合，特別な設定なしに，シングルサインオンおよびユーザー管理の統合を実現します。ほかの Hitachi Command Suite 製品と連携する場合のシステム構成例を次の図に示します。

図 6-1 ほかの Hitachi Command Suite 製品と連携する場合のシステム構成例



Device Manager と同じサーバにインストールする場合，SNMP Trap 受信機能を使用するときは，Device Manager で SNMP Trap 受信機能を設定しているかどうかを確認してください。Device Manager でも SNMP Trap 受信機能を設定している場合は，Global Link Manager をインストールするとき，ポート番号をデフォルトの 162 以外の番号を設定してください。インストールしたあとにポート番号を変更する場合は，`server.properties` ファイルの `server.snmp.trap_port_num` プロパティの値を修正してください。

注意事項

シングルサインオンおよびユーザー管理の統合ができるのは，同じサーバにインストールされているバージョン 5.0 以降の Hitachi Command Suite 製品です（Tuning Manager 5.0 は除く）。5.0 より前のバージョンの Hitachi Command Suite 製品およびほかのサーバにインストールされている Hitachi Command Suite 製品とは，シングルサインオンおよびユーザー管理の統合はできません。

6.2 JP1/IM と連携するための設定

JP1/IM と連携する場合のセットアップ手順について説明します。JP1/IM と連携する場合，次の製品のインストールとセットアップが必要です。

- JP1/Base
- JP1/IM - View
- JP1/IM - Manager

6.2.1 JP1/IM の統合機能メニュー画面から Global Link Manager GUI を呼び出す場合の設定

Global Link Manager を JP1/IM と連携させることによって，JP1/IM の統合機能メニュー画面から Global Link Manager GUI を呼び出して使用できるようになります。

Hitachi Command Suite 共通コンポーネントのシングルサインオン機能を利用すると，Global Link Manager のユーザー認証をしないで Global Link Manager GUI を表示できます。シングルサインオン機能を利用しない場合は，Global Link Manager のユーザー認証が必要になります。

ここでは，シングルサインオン機能を利用して JP1/IM と連携するためのセットアップ手順について説明します。シングルサインオン機能を利用しない場合のセットアップ手順については，マニュアル「JP1/Integrated Management - Manager システム構築・運用ガイド」を参照してください。シングルサインオン機能を利用する場合，次の条件があります。

- 08-10 以降のバージョンの JP1/IM - View が必要です。
- JP1/IM - View にログインするユーザーと同じアカウントを事前に Global Link Manager で作成しておく必要があります。パスワードには，6 文字以上の文字列を指定してください。ユーザー ID に使用できる文字は次のとおりです。

  a～z A～Z 0～9 ! $ - . @ _

次に示す手順で JP1/Base と JP1/IM のインストールおよびセットアップを実行してください。

1. 管理クライアントに JP1/IM - View をインストールしてください。
2. 管理サーバに JP1/Base と JP1/IM - Manager をインストールしてください。
3. JP1/Base の環境設定をしてください。

JP1 統合機能メニューから Global Link Manager GUI を起動するには，JP1/IM - View の構成定義ファイルを作成する必要があります。作成する構成定義ファイルのサンプルファイル（globallinkavailability_manager_ja.conf）は，次のフォルダにあります。

＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥sample¥JP1_IM_conf

サンプルファイル（globallinkavailability_manager_ja.conf）を次のフォルダの下にコピーして編集します。

＜*JP1/IM - View のインストール先*＞¥conf¥function¥ja

構成定義ファイルの内容を次に示します。

```
@file type="function-definition", version="0300";
#----------------------------------------------------------
@define-block type="function-tree-def";
id="jco_HicommandGLAM";
parent_id="jco_folder_san";
name="グローバル入出力パス稼働管理";
icon="%JCO_INSTALL_PATH%¥image¥menu¥hicmd.gif";
```

```
execute_id="default_browser";
arguments="http://＜Global Link Manager サーバの IP アドレスまたはホスト名＞:＜接続先ポート＞/HiCommand/IMLogin?jp1userid=%JCO_JP1USER%&jp1token=%JCO_JP1TOKEN
%&launchurl=http://＜Global Link Manager サーバの IP アドレスまたはホスト名＞:＜接続先ポート＞/GlobalLinkAvailabilityManager/Login";
@define-block-end;
#------------------------------------------------------------
```

「arguments=」で始まる行を実行環境に合わせて修正してください。＜*Global Link Manager サーバの IP アドレスまたはホスト名*＞および＜*接続先ポート*＞の部分は，次のように指定します。

＜ Global Link Manager サーバの IP アドレスまたはホスト名＞

Global Link Manager をインストールしたサーバの IP アドレスまたはホスト名を指定します。IP アドレスを指定する場合は，IPv4 アドレスを指定してください。

＜接続先ポート＞

接続先ポート番号として，HBase 64 Storage Mgmt Web Service のポート番号を指定します。デフォルト値は 22015 です。

Global Link Manager で SSL の設定が有効な場合には，修正内容に含まれる 2 か所の URL を SSL 時に使用する URL に変更してください。

JP1/IM のコンソールを起動し，［オプション］メニューから［統合機能メニュー起動］を実行すると画面が表示されます。Global Link Manager GUI は［ストレージ管理］－［ストレージエリア管理］－［グローバル入出力パス稼働管理］をダブルクリックすると起動します。

注意事項

統合機能メニューが表示されている画面では，ブラウザーの「戻る」「進む」ボタンおよびブラウザーの履歴を使った画面の移動をしないでください。

6.2.2 Global Link Manager が出力した監査ログを JP1/IM の統合コンソールに通知する場合の設定

JP1/IM が提供する統合コンソールへ Global Link Manager の監査ログを通知する機能を利用できます。監査ログについては「3.12 監査ログの採取」を参照してください。

セットアップの手順は次のとおりです。JP1/IM - View については，マニュアル「JP1/Integrated Management - Manager システム構築・運用ガイド」を参照してください。JP1/Base については，マニュアル「JP1/Base 運用ガイド」を参照してください。

1. 管理クライアントに JP1/IM - View をインストールしてください。
2. 管理サーバに JP1/Base と JP1/IM - Manager をインストールしてください。
3. JP1/Base の環境設定をしてください。
4. Windows のイベントログに出力された監査ログのうち，JP1/IM の統合コンソールに通知する Global Link Manager の監査ログを抽出するために，JP1/Base の動作定義ファイルを編集します。

   JP1/Base の動作定義ファイルは次の場所に作成してください。

   格納場所：＜*JP1/Base のインストールフォルダ*＞¥conf¥event¥

   ファイル名：ntevent.conf

   （例）

   Global Link Manager が出力する監査ログをすべて JP1/IM の統合コンソールに通知するには動作定義ファイルに次の内容を追加してください。

   ```
   filter "Application"
   ```

```
   message '.*KAIF.*'
end-filter
```

動作定義ファイルについてはマニュアル「JP1/Base 運用ガイド」を参照してください。

5. “JP1/Base EventlogTrap”サービスを起動してください。

6.3 JP1/Automatic Operation と連携するための注意

バージョンが v8.0.0 以降の Global Link Manager，および JP1/Automatic Operation を同一マシンにインストールする場合，JP1/Automatic Operation のバージョンは 10-10 以降を使用してください。

7

Global Link Manager のトラブルシューティング

この章では，Global Link Manager の運用中に発生したトラブルの対処方法について説明します。

7.1 Global Link Manager のトラブルシューティングの流れ

トラブルが発生した場合，次の流れで対処します。

1. 出力されたメッセージを確認します。
   メッセージが出力されない場合は，「7.2 Global Link Manager のトラブルシューティングの事例」に該当する事例があるか確認します。
2. 出力されたメッセージやトラブルシューティングの事例を確認してもエラーの原因がわからない場合は，保守情報を採取します。
   保守情報の採取方法は，「7.3 Global Link Manager の保守情報の採取方法」を参照してください。
3. 手順 2 で採取したログファイルを確認します。
   ログファイルの確認方法は，「7.4 Global Link Manager のログファイルの確認」を参照してください。
4. ログファイルを確認しても，エラーの原因がわからない場合は問い合わせ窓口に連絡してください。
   問い合わせ窓口に連絡するときは，手順 2 で採取した保守情報を送付します。

7.2 Global Link Manager のトラブルシューティングの事例

Global Link Manager のインストールや環境設定，Global Link Manager GUI の操作で発生するおそれがあるトラブルの事例とその要因，対処を説明します。

7.2.1 Global Link Manager のインストール時のトラブルシューティング

表 7-1 トラブルシューティングの事例（Global Link Manager のインストール時）

問題	要因	対処
インストールに失敗する。	管理者権限がないユーザーでインストールを実行しました。	管理者権限があるユーザーでログインし直してから，インストールを実行してください。
	Global Link Manager をインストールするサーバの OS または OS のバージョンがサポート対象外です。	Global Link Manager サーバでサポートしている OS および OS のバージョンのサーバを準備して，インストールを実行してください。
	Global Link Manager をインストールするサーバのディスクの残り容量が不足しています。	サーバのディスク容量を見直してから，インストールを実行してください。

7.2.2 Global Link Manager の環境設定時のトラブルシューティング

表 7-2 トラブルシューティングの事例（Global Link Manager の環境設定時）

問題	要因	対処
プロパティファイルに指定した内容が反映されない。	プロパティファイルを更新したあと，Global Link Manager を再起動していません。	Global Link Manager を再起動してください。

問題	要因	対処
	プロパティファイルで指定した値が不正なため，デフォルト値で動作しています。	「3.5」を参照して，プロパティファイルの値を見直してください。

7.2.3 Global Link Manager GUI 操作時のトラブルシューティング

表 7-3 トラブルシューティングの事例（Global Link Manager GUI 操作時）

問題	要因	対処
日本語環境で，メッセージが英語で表示される。	Global Link Manager をインストールしたサーバのロケールが英語に設定されています。	Global Link Manager をインストールしたサーバのロケールを日本語に設定してください。
Web ブラウザーでページを表示できない。	Hitachi Command Suite 共通コンポーネントが起動していません。	Hitachi Command Suite 共通コンポーネントを起動してください。起動方法については，「3.2.1」を参照してください。
	Global Link Manager をインストールしたサーバのディスクの残り容量が不足しているため，Hitachi Command Suite 共通コンポーネントの起動に失敗しました。	Global Link Manager をインストールしたサーバのディスク容量を見直してから，Hitachi Command Suite 共通コンポーネントを起動してください。起動方法については，「3.2.1」を参照してください。
ホストが追加できない。	追加するホストの OS が AIX の場合に，パスが 1 本も設定されていません。	ホストの HDLM の運用環境を見直して，パスを追加してから，操作を再度実行してください。HDLM 運用環境の構成変更については，HDLM のマニュアルを参照してください。
	ホストにインストールされている Device Manager エージェントの設定が不正です。	Device Manager エージェントのバージョンが 7.0 より前の場合は `hdvmagt_account` コマンドを，バージョン 7.0 以降の場合は `hdvmagt_setting` コマンドを実行して，Device Manager サーバの情報またはホストの情報を設定してください。設定方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。
	共通エージェントコンポーネントが起動していません。	共通エージェントコンポーネントを起動してください。起動方法については，「A.4.1」を参照してください。
ホスト情報が更新できない。	ホストにインストールされている HDLM の各コンポーネントが起動されていません。	ホストで HDLM の各コンポーネントを起動してください。起動方法については，HDLM のマニュアルを参照してください。
	ホストにインストールされている HDLM の各コンポーネントでの設定が不正です。	ホストの HDLM の各コンポーネントでの設定を見直してください。設定方法については，HDLM のマニュアルを参照してください。

問題	要因	対処
	ホストにインストールされている HDLM のバージョンが Global Link Manager のサポート対象外です。	Global Link Manager でサポートしているバージョンの HDLM をインストールしてください。 HDLM のシステム要件については，HDLM のマニュアルを参照してください。あわせて，「(1) 」で Global Link Manager でサポートしていない OS を確認してください。
	Global Link Manager サーバとホスト間の通信で，次の障害が発生しているおそれがあります。 • ネットワークケーブルの接続不良または断線 • ルータまたはハブの故障 • ネットワークインターフェースカードの故障 • ルーティングの設定不正によるパケットの消失 • ファイアウォールなどのパケットフィルタリングによるブロック • IP アドレスの衝突による通信不良 • デフォルトゲートウェイの IP アドレスまたはサブネットマスクの設定誤り	要因に合わせてネットワークの障害を取り除いてください。 • ネットワークケーブルを接続または交換する。 • ルータまたはハブを交換する。 • ネットワークインターフェースカードを交換する。 • ルーティングの設定を見直す。 • HDLM および Global Link Manager のパケットが通過できるように設定する。 • IP アドレスを再設定する。 • デフォルトゲートウェイの IP アドレスまたはサブネットマスクの設定を見直す。 上記以外の対処については，ネットワーク管理者に確認してください。
	ホストの共通エージェントコンポーネントの `server.properties` ファイルで `server.agent.port` プロパティ（エージェントサービスポート）に指定しているポート番号が変更されました。	ホストをいったん削除してから，再度追加してください。追加および削除方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。
	ホストにインストールされている Device Manager エージェントの設定が不正です。	Device Manager エージェントのバージョンが 7.0 より前の場合は `hdvmagt_account` コマンドを，バージョン 7.0 以降の場合は `hdvmagt_setting` コマンドを実行して，Device Manager サーバの情報またはホストの情報を設定してください。設定方法については，マニュアル「Hitachi Global Link Manager ユーザーズガイド」を参照してください。
	ホストの OS が AIX の場合に，パスが 1 本も設定されていません。	ホストの HDLM の運用環境を見直して，パスを追加してから，操作を再度実行してください。 HDLM 運用環境の構成変更については，HDLM のマニュアルを参照してください。
	共通エージェントコンポーネントが起動していません。	共通エージェントコンポーネントを起動してください。起動方法に

問題	要因	対処
		ついては，「A.4.1 」を参照してください。
メッセージ KAIF22102-E で詳細情報に「The header information is invalid.」が出力される。	共通エージェントコンポーネントがサービス（またはデーモンプロセス）の停止処理中，またはほかのアプリケーションの処理を実行中です。	共通エージェントコンポーネントのサービス（またはデーモンプロセス）の状態を確認してください。停止している場合は起動してください。起動している場合は，時間をおいて，操作を再度実行してください。
ホストの情報が表示されない。	ログインユーザーには，ホストに対するアクセス権限がありません。	ログインユーザーのアクセス権限を見直してください。
ストレージの情報が表示されない。	ログインユーザーには，ストレージシステムに対するアクセス権限がありません。	ログインユーザーのアクセス権限を見直してください。

7.3 Global Link Manager の保守情報の採取方法

出力されたメッセージからエラーの原因が特定できない場合，「7.2 Global Link Manager のトラブルシューティングの事例」に該当する事例がない場合は，Global Link Manager サーバの保守情報を採取する必要があります。また，シングルサインオン機能を使用していて障害が発生した場合は，スレッドダンプを採取する必要があります。以降の項でそれぞれのファイルの採取方法を説明します。

7.3.1 Global Link Manager サーバの保守情報の一括採取

Global Link Manager の保守情報を採取するには，hcmds64getlogs コマンドを使用します。

hcmds64getlogs コマンドは，障害が発生した状態で使用してください。

(1) 保守情報のファイルの種類

hcmds64getlogs コマンドを実行すると，次のファイルを採取して，アーカイブします。

表 7-4 hcmds64getlogs コマンドで採取する情報

項番	ファイルの種類	アーカイブファイル名（デフォルト）
1	イベントログファイル	HiCommand_log.jar
2	メッセージログファイル	
3	インストーラートレースログファイル	
4	アンインストーラートレースログファイル	
5	トレースログファイル	
6	プロパティファイル	
7	InstallShield ログファイル	
8	バージョンファイル	
9	データベースの障害分析用ログファイル	
10	パス稼働情報（パスステータスログ）	
11	データベースの詳細ログファイル	HiCommand_log.hdb.jar
12	データベースファイル	HiCommand_log.db.jar
13	データベースのテーブルデータファイル	HiCommand_log.csv.jar

項番 1～4 のログファイルを参照しても，障害の原因がわからない場合は，項番 1～10 がアーカイブされたファイルを問い合わせ窓口に送付して，解析を依頼してください。項番 11～13 のアーカイブファイルを送付するかどうかは問い合わせ窓口の指示に従ってください。Hitachi Command Suite 共通コンポーネントが起動していないと，項番 12 のアーカイブファイルは取得できません。

項番 1～4 のログファイルの確認方法は「7.4 Global Link Manager のログファイルの確認」を参照してください。

(2) パス稼働情報（パスステータスログ）を取得する場合

ホストの追加，ホストの更新，またはレポート出力でエラーが発生し，保守情報が必要となった場合，「表 7-4 hcmds64getlogs コマンドで採取する情報」 の項番 11 のパス稼働情報（パスステータスログ）を取得します。パス稼働情報（パスステータスログ）を取得する場合は，プロパティファイル（server.properties）を変更してください。保守情報としてパス稼働情報（パスステータスログ）を取得する場合に，次のプロパティの値を変更するときは，Global Link Manager の再起動は不要です。

- getlogs.pathreport.get_mode
- getlogs.pathreport.host
- getlogs.pathreport.startDate
- getlogs.pathreport.endDate

パス稼働情報（パスステータスログ）を取得するとアーカイブファイルのサイズが大きくなるおそれがあるため，デフォルトでは取得しないようになっています。プロパティファイルについては「3.5 Global Link Manager の環境設定の変更」を参照してください。

(3) hcmds64getlogs コマンドの形式

コマンドの書式

```
hcmds64getlogs /dir <フォルダ名> [/type HGLAM] [/arc <アーカイブファイル名>]
[/logtypes <ログファイル種別>[ <ログファイル種別> ...]]
```

オプションの説明

表 7-5 hcmds64getlogs コマンドのオプションおよび引数

オプションおよび引数	説明
/dir <フォルダ名>	採取した保守情報を格納するローカルディスク上のフォルダ名を指定します。実在するフォルダを指定する場合は，空のフォルダを指定します。 指定できる文字： 指定できる文字は，A～Z，a～z，0～9，'.'，'_'です。そのほかにパスの区切り文字として(¥)，(:)，(/)が使用できます。パスに空白が含まれる場合は，パスの前後に'"'を指定します。 指定できる文字以外を指定した場合，メッセージが出力されコマンドが終了します。 指定できるパスの長さ： 指定できるパスの長さは，/type オプションを指定するかどうかによって異なります。指定できるパスの長さを次に示します。 • /type オプションを指定した場合：13 バイト • /type オプションを指定しない場合：71 バイト

オプションおよび引数	説明
/type HGLAM または GlobalLinkAvailabilityManager	Global Link Manager の保守情報だけを採取する場合に指定します。このオプションを省略すると，同じサーバにインストールされている場合はほかの Hitachi Command Suite 製品の保守情報も採取します。
/arc ＜*アーカイブファイル名*＞	アーカイブファイルの名称を指定する場合に指定します。このオプションを省略すると，「表 7-4 」に示すデフォルトのファイル名になります。アーカイブファイルは，/dir オプションで指定したフォルダの下に出力されます。 指定できる文字： 指定できる文字は，A～Z，a～z，0～9，'.'，'_'です。指定できる文字以外を指定した場合，メッセージが出力されコマンドが終了します。
/logtypes ＜*ログファイル種別*＞[＜*ログファイル種別*＞ ...]	障害などの理由によって，特定のログファイルしか取得できない場合に，取得対象のログファイルの種別を指定します。 log：.jar ファイルと.hdb.jar ファイルだけを取得する場合に指定します。 db：.db.jar ファイルだけを取得する場合に指定します。 csv:.csv.jar ファイルだけを取得する場合に指定します。 複数の種別を指定する場合は，半角スペースで区切ってください。このオプションを省略した場合，すべてのログファイルが取得されます。

注意事項

hcmds64getlogs コマンド終了時に，メッセージ KAPM05318-I または KAPM05319-E が出力されない場合，/dir オプションで指定するフォルダに十分な空き容量がないため hcmds64getlogs コマンドが途中で終了しています。/dir オプションで指定するフォルダに十分な空き容量を確保したあとで，再度 hcmds64getlogs コマンドを実行してください。

7.3.2 ホストの保守情報の一括採取

出力されたエラーの原因がホストにある場合，ホストの保守情報を採取する必要があります。

HDLM の DLMgetras ユーティリティを使用して保守情報を採取してください。DLMgetras ユーティリティについては，HDLM のマニュアルを参照してください。

7.3.3 スレッドダンプの採取

シングルサインオン機能を使用している場合，次のどれかのイベントが発生したときは，その問題の原因を確認するために，Java VM スレッドダンプを収集します。

- Global Link Manager を起動しようとしても，ユーザーログインウィンドウが表示されない。
- Global Link Manager へログインしても，メインウィンドウが表示されない。
- ほかの Hitachi Command Suite 製品から Global Link Manager を起動しようとしても，メインウィンドウが表示されない。

Java VM スレッドダンプを収集する手順を次に示します。

1. ＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥server¥public¥ejb¥GlobalLinkManagerWebService の下に，dump という名前のファイルを作成します。
2. Windows の［サービス］ウィンドウで，「Global Link Manager Web Service」を停止します。＜*Hitachi Command Suite 共通コンポーネントのインストールフォルダ*＞¥uCPSB11¥CC¥web¥containers¥HiCommand64 の下に，次のファイルが出力されます。

Global Link Manager に同梱されている JDK を使用している場合

```
javacore.xxxx.xxxx.txt
```

Oracle JDK を使用している場合

```
HiCommand64.log
```

3. Windows の［サービス］ウィンドウで，「Global Link Manager Web Service」を起動します。

7.4 Global Link Manager のログファイルの確認

「7.3.1 Global Link Manager サーバの保守情報の一括採取」で保守情報を採取したら，次のログファイルを確認してください。

表 7-6 ユーザーが確認するログファイルの種類

ログファイル	説明
イベントログファイル（ApplicationLog.evt）	メッセージログファイルに出力されるメッセージのうち，重要度が高いものが記録されます。同じサーバにほかの Hitachi Command Suite 製品がインストールされている場合，ほかの Hitachi Command Suite 製品のログも出力されます。 そのほかに，監査ログとして，Global Link Manager に関する操作や情報が記録されます。Global Link Manager へのアクセスやユーザーが操作した内容を監査する場合に確認します。
メッセージログファイル（HGLAM_Message＜*n*＞.log）	Global Link Manager の起動，停止および操作時に出力されるメッセージが記録されます。Global Link Manager の起動，停止および操作時にエラーが発生した場合に確認します。
インストーラートレースログファイルまたはアンインストーラートレースログファイル（HGLAM_TL_Install_*yyyy-mm-dd_hh-mm-ss*.log または HGLAM_TL_Remove_*yyyy-mm-dd_hh-mm-ss*.log）	Global Link Manager のインストールまたはアンインストール時に出力されるメッセージが記録されます。インストールまたはアンインストール時にエラーが発生した場合に確認します。

7.4.1 イベントログの出力形式

Windows のイベントログに出力されるイベントの出力形式とその内容を説明します。

イベントの出力形式

＜*日付*＞ ＜*時刻*＞ ＜*種類*＞ ＜*ユーザー*＞ ＜*コンピュータ*＞ ＜*ソース*＞ ＜*分類*＞ ＜*イベント ID*＞ ＜*説明*＞

表 7-7 イベントログに出力される情報

項目	内容
日付	メッセージが出力された日付が「yyyy/mm/dd」の形式で出力されます。
時刻	メッセージが出力された時刻が「hh:mm」の形式で出力されます。
種類	次の 3 つの種類があります。 ・ 情報 ・ 警告 ・ エラー

項目	内容
ユーザー	「N/A」と出力されます。
コンピュータ	コンピュータ名が表示されます。
ソース	「HBase64 Event」と出力されます。
分類	「なし」と出力されます。
イベント ID	「1」と出力されます。
説明	次の形式で出力されます。 ＜プログラム名＞ [＜プロセス ID ＞]: ＜メッセージ ID ＞ ＜メッセージテキスト＞ メッセージの要因と対処については，マニュアル「Hitachi Global Link Manager メッセージ」を参照してください。 「＜プログラム名＞ [＜プロセス ID ＞]: CELFSS」で始まる場合は，監査ログです。監査ログについては，「3.12 」を参照してください。

7.4.2 メッセージログファイルの出力形式

Global Link Manager のメッセージログファイルに出力されるメッセージの形式とその内容を説明します。

出力形式

＜通番＞ ＜日付＞ ＜時刻＞ ＜プログラム名＞ ＜プロセス ID ＞ ＜スレッド ID ＞ ＜メッセージ ID ＞ ＜イベント種別＞ ＜ユーザー ID ＞ ＜メッセージテキスト＞

表 7-8 メッセージログファイルに出力される情報

項目	内容
通番	メッセージログファイル内のメッセージの通番が出力されます。
日付	メッセージが出力された日付が「yyyy/mm/dd」の形式で出力されます。
時刻	メッセージが出力された時刻が「hh:mm:ss.sss」の形式で出力されます。
プログラム名	Global Link Manager のコンポーネント名やコマンド名が出力されます。
プロセス ID	プロセス ID が出力されます。
スレッド ID	スレッド ID が出力されます。
メッセージ ID	メッセージ ID が出力されます。
イベント種別	トレース出力の契機となったイベント種別が出力されます。
ユーザー ID	操作を実行したユーザーのユーザー ID が出力されます。操作によっては出力されません。
メッセージテキスト	メッセージの内容が出力されます。 メッセージの要因と対処については，マニュアル「Hitachi Global Link Manager メッセージ」を参照してください。

7.4.3 インストーラートレースログファイルおよびアンインストーラートレースログファイルの出力形式

出力形式

*** begin Hitachi Global Link Manager (Windows) setup process Trace Log
＜日付と時刻＞ : (＜レベル＞) ＜トレース情報＞ [＜補助情報＞]
*** end Hitachi Global Link Manager (Windows) setup process Trace Log

表 7-9 インストーラートレースログファイルおよびアンインストーラートレースログファイルに出力される情報

項目	内容
日付と時刻	メッセージが出力された日付と時刻が「yyyy/mm/dd hh:mm:ss」の形式で出力されます。
レベル	次の 3 つのレベルがあります。 • I：通常のトレース情報 • W：警告 • E：ユーザー通知レベルのエラー
トレース情報	メッセージの内容が出力されます。
補助情報	コマンド実行時のパラメーターおよび戻り値が出力されます。

A

共通エージェントコンポーネントの設定

Global Link Manager を運用する上で必要な，ホストの共通エージェントコンポーネントの設定や起動手順などについて説明します。

A.1 共通エージェントコンポーネント

共通エージェントコンポーネントは，HDLM に含まれるコンポーネントです。

ホストの OS が Windows の場合

共通エージェントコンポーネントのインストールフォルダは，ホストを Device Manager で管理しているかどうかなどの環境によって異なります。インストールフォルダを確認する場合は，次のレジストリーキーでデータを参照してください。

- キー名：HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi¥HBaseAgent¥＜バージョン＞¥PathName

  ＜バージョン＞は，共通エージェントコンポーネントのバージョンを表します。最新のバージョンのキー名で参照してください。
- 名前：Path00

ホストの OS が Windows Server 2012（x64）または Windows Server 2012 R2 の場合

ホストにインストールされているほかの Hitachi Command Suite 製品が，頻繁に共通エージェントコンポーネントにアクセスした場合，JavaVM が異常終了することがあります。JavaVM が異常終了する場合は，次のファイルを編集してください。

＜*共通エージェントコンポーネントのインストールフォルダ*＞¥agent¥bin¥Server.cmd

Server.cmd ファイルをテキストエディターで開き，java 起動オプションに「-Djava.compiler=NONE」を追加してください。Server.cmd ファイルの編集例を次に示します。

```
..java -Dalet.msglang -Djava.compiler=NONE -Xss5M -classpath
"C:¥Program Files¥HITACHI¥HDVM¥HBaseAgent¥agent¥jar¥agent4.jar;C:
¥Program Files¥HITACHI¥HDVM¥HBaseAgent¥agent¥jar¥jdom.jar;C:¥Program
Files¥HITACHI
¥HDVM¥HBaseAgent¥agent¥jar¥xerces.jar;C:¥Program Files¥HITACHI¥HDVM
¥HBaseAgent¥agent
¥jar¥servlet.jar;C:¥Program Files¥HITACHI¥HDVM¥HBaseAgent¥agent¥jar
¥log4j-1.2.3.jar" com.Hitachi.soft.HiCommand.DVM.agent4.as.
export.Server %*
exit /b %ERRORLEVEL%
```

A.2 HDLM を使用する場合のファイアウォールの設定

HDLM がインストールされているホストで，かつファイアウォールを有効に設定している場合は，Global Link Manager サーバでホストを追加するためにファイアウォールに共通エージェントコンポーネントを例外として登録しておく必要があります。

A.2.1 Windows 版 HDLM 6.6 以降の場合

例外の登録

次のコマンドを実行して，共通エージェントコンポーネントを例外登録してください。

＜*共通エージェントコンポーネントのインストールフォルダ*＞¥bin¥firewall_setup.bat -set

例外登録するサービスポートは「表 A-1 共通エージェントコンポーネントの設定を変更するためのプロパティ（server.properties）」を参照してください。

例外の設定解除

次のコマンドを実行して，例外の設定解除をします。

<共通エージェントコンポーネントのインストールフォルダ>¥bin¥firewall_setup.bat -unset

注意事項

例外登録をしたあとで「表 A-1 共通エージェントコンポーネントの設定を変更するためのプロパティ（server.properties）」のサービスポートのポート番号を変更した場合は，再度 firewall_setup コマンドを実行してください。

A.2.2 Linux 版 HDLM の場合

Linux 環境でのファイアウォールの例外登録は，ユーザーが手動で行う必要があります。

登録するポートの詳細については，「表 A-1 共通エージェントコンポーネントの設定を変更するためのプロパティ（server.properties）」を参照してください。

A.3 共通エージェントコンポーネントの設定の変更

共通エージェントコンポーネントでは，Global Link Manager との通信のためのポート番号に，デフォルトで 24041～24043 を設定しています。ほかの製品でこのポート番号を使用している場合は，共通エージェントコンポーネントのポート番号を変更してください。

また，ホストに複数のネットワークインターフェースカードを搭載して同一のネットワークに接続している場合には，Global Link Manager の通信に使用する IP アドレスを設定する必要があります。

共通エージェントコンポーネントの設定を変更するには，各ホストのプロパティファイルを編集します。

注意事項

HDLM と Device Manager エージェントを同じホストにインストールしている場合は，プロパティファイルを共有し，共通のプロパティを使用します。したがって，HDLM の共通エージェントコンポーネントと Device Manager エージェントは，同じ指定値を使用します。

プロパティファイルの場所

Windows の場合

<共通エージェントコンポーネントのインストールフォルダ>¥agent¥config¥server.properties
<共通エージェントコンポーネントのインストールフォルダ>¥agent¥config¥logger.properties

Solaris または Linux の場合

/opt/HDVM/HBaseAgent/agent/config/server.properties
/opt/HDVM/HBaseAgent/agent/config/logger.properties

AIX の場合

/usr/HDVM/HBaseAgent/agent/config/server.properties
/usr/HDVM/HBaseAgent/agent/config/logger.properties

プロパティファイルの内容

共通エージェントコンポーネントの設定を変更するためのプロパティの一覧を次の各表に示します。

表 A-1 共通エージェントコンポーネントの設定を変更するためのプロパティ（server.properties）

項番	プロパティ名	内容
サービス（またはデーモンプロセス）および Web サーバ機能で使用するポートの設定		
1	server.agent.port※	共通エージェントコンポーネントのサービス（またはデーモンプロセス）で使用するポートを指定します。 Global Link Manager の管理対象として Global Link Manager GUI でホストを追加するときには，このポート番号をエージェントサービスポートに指定します。 デフォルト値：24041
2	server.http.port※	共通エージェントコンポーネントの Web サーバ機能が非 SSL 通信で使用するポートを指定します。 デフォルト値：24042
3	server.http.localPort※	共通エージェントコンポーネントのサービス（またはデーモンプロセス）と Web サーバプロセスとの間の通信に使用するポートを指定します。 デフォルト値：24043
4	server.https.port※	共通エージェントコンポーネントの Web サーバ機能が SSL 通信で使用するポートを指定します。 デフォルト値：24045
Web サーバ機能で使用するホスト名，IP アドレスおよびネットワークインターフェースカードの設定		
5	server.http.host	ホスト名を指定します。指定しない場合，またはデフォルト値を指定した場合，共通エージェントコンポーネントはホスト名を自動で取得します。取得できなかった場合には，Global Link Manager からアクセスできるように手動で設定する必要があります。 デフォルト値：localhost
6	server.http.socket.agentAddress	ホストの IP アドレスを指定します。IPv6 環境で運用する場合は，グローバルアドレスを指定してください。サイトローカルアドレスまたはリンクローカルアドレスを指定した場合は IPv4 アドレスで動作します。指定しない場合，共通エージェントコンポーネントは IP アドレスを自動で取得します。取得できなかった場合には，Global Link Manager からアクセスできるように手動で設定する必要があります。 HDLM がインストールされたホストが複数のネットワークインターフェースカードを搭載して同一のネットワークに接続している場合に，複数搭載されているネットワークインターフェースカードのいずれかの IP アドレスを指定してください。この設定を行わないと，ホストを正常に追加できない場合があります。 上記の場合にこのプロパティを指定しないと，ネットワークインターフェースカードの数だけホストを登録できるため，ホストやパスが重複して表示されるおそれがあります。 デフォルト値：指定なし
7	server.http.socket.bindAddress	HDLM がインストールされたホストが複数のネットワークインターフェースカードを搭載して同一のネットワークに接続している場合に，複数搭載されているネットワークインターフェースカードのいずれかの IP アドレスを指定してください。この設定

項番	プロパティ名	内容
		を行わないと，ホストを正常に追加できない場合があります。 IPv6 環境で運用する場合は，グローバルアドレスを指定してください。サイトローカルアドレスまたはリンクローカルアドレスを指定した場合は IPv4 アドレスで動作します。 上記の場合にこのプロパティを指定しないと，ネットワークインターフェースカードの数だけホストを登録できるため，ホストやパスが重複して表示されるおそれがあります。 デフォルト値：指定なし
Web サーバ機能の基本動作の設定		
8	server.agent.maxMemorySize	共通エージェントコンポーネントの Web サーバ機能のプロセスの最大メモリーヒープサイズをメガバイト単位で指定します。メモリーヒープサイズの不足が原因で処理が停止する場合には，この値を大きくすることで解決できます。 32～4096 の範囲で指定します。 デフォルト値：指定なし（64 メガバイトで動作します）
9	server.agent.shutDownTime	共通エージェントコンポーネントの Web サーバ機能が最後の HTTP/XML メッセージを送信または受信してから停止するまでの時間をミリ秒で指定します。値を大きくした場合，共通エージェントコンポーネントから Global Link Manager への応答速度が速くなりますが，共通エージェントコンポーネントで用いるリソースが大きくなります。 デフォルト値：600000
10	server.agent.JRE.location	共通エージェントコンポーネントで使用する Java プログラムのインストール先を指定します。 Windows または Linux の場合のデフォルト値 なし Solaris または AIX の場合のデフォルト値 共通エージェントコンポーネントをインストールした時点でホストにインストールされている Java プログラムのインストールパス
Web サーバ機能のセキュリティ設定		
11	server.http.security.clientIP	アクセスを許可する IPv4 および IPv6 のアドレスを指定します。Global Link Manager サーバの IP アドレスを指定するか，すべての IP アドレスが接続できるように値を指定しないでください。値を指定する場合，Device Manager エージェントとプロパティファイルを共有しているときは，Global Link Manager サーバの IP アドレスだけでなく Device Manager エージェントに接続するサーバの IP アドレスをあわせて指定する必要があります。 この設定は，接続できる IP アドレスを制限することで，サービス妨害攻撃やバッファーのオーバーフローをねらった攻撃を防ぐのに役立ちます。 IPv4 アドレスの場合は*（アスタリスク）をワイルドカード文字として使用できます。IP アドレスを複数指定する場合は，,（コンマ）で区切ります。ドット付きの 10 進数の IP アドレスとして無効な指定や空白文字（スペース）は無視され，エラーは発生しません。

項番	プロパティ名	内容

		191.0.0.2 と 192.168.0.0～192.168.255.255 の接続を許可する場合の指定例を次に示します。
		`server.http.security.clientIP=191.0.0.2, 192.168.*.*`
		2001::203:baff:fe36:109a と 2001::203:baff:fe5b:7bac の接続を許可する場合の指定例を次に示します。
		`server.http.security.clientIP=2001::203:baff:fe36:109a,2001::203:baff:fe5b:7bac`
		デフォルト値：指定なし（すべての IP アドレスが接続できます）

12	`server.http.entity.maxLength`	Global Link Manager サーバが共通エージェントコンポーネントに送信する XML ファイルの最大長をバイト単位で設定できます。同時に多数のパスの状態を変える場合など，サイズの大きい XML ファイルを送信した場合にエラーが発生するときには，この値を大きくすることで解決する可能性があります。 デフォルト値：32768
13	`server.agent.secure`	通信路のセキュリティレベルを指定します。 1：非 SSL 通信だけの場合 2：非 SSL 通信と SSL 通信の場合 3：SSL 通信だけの場合 デフォルト値：1 注意事項 Device Manager エージェントがインストールされている場合は「3」を設定しないでください。
14	`server.agent.ciphers`	SSL 通信に使用する暗号方式を指定します。Java に設定できる暗号方式アルゴリズムの文字列で指定します。複数指定する場合はコンマで区切ります。 AIX の場合のデフォルト値（IBM Java 用） SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384,SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256,SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384,SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384,SSL_RSA_WITH_AES_128_GCM_SHA256,SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_128_CBC_SHA256 AIX 以外の場合のデフォルト値（Oracle Java 用） TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256

注※

各プロパティの指定値は，ほかのサービス（またはデーモンプロセス）と競合するおそれがあるので，小さい数字のポートは避けてください。通常は，1024～49151 のポートを選択します。

注意事項

インストールした時点の初期状態のプロパティファイルには，デフォルト値のプロパティが記載されていない場合があります。設定値をデフォルト値から変更したいときには，「*<プロパティ名>=<値>*」の形式でプロパティファイルに追加してください。

表 A-2 共通エージェントコンポーネントのログファイルの設定を変更するためのプロパティ（logger.properties）

項番	プロパティ名	内容
1	logger.loglevel	trace.log ファイルと error.log ファイルの出力レベルを指定できます。使用できる値は，詳細度が高い順に DEBUG，INFO，WARN，ERROR および FATAL です。デフォルト値の場合，DEBUG のエントリーはログに出力されないで，INFO，WARN，ERROR，および FATAL のエントリーがログに出力されます。 デフォルト値：INFO
2	logger.MaxBackupIndex	各ログファイルの最大バックアップファイル数を指定できます。ログファイル数が logger.MaxFileSize で指定された最大長に達すると，バージョンを示すカウンターが付けられ，ファイル名が更新されます（例えば access.log が access.log.1 となります）。ログファイルがさらに作成されると，指定された数のバックアップログファイルが作成されるまで，カウンターが増加していきます（例えば，access.log.1 が access.log.2 になります）。指定された数のバックアップログファイルが作成されたあとは，新しいバックアップログファイルが作成されるたびに，最も古いバックアップログファイルが削除されます。 指定できる値の範囲は，1～20 です。 デフォルト値：10
3	logger.MaxFileSize	各ログファイルの最大サイズを指定できます。ログファイルのサイズが指定値を超えた場合は，新しいログファイルが作成されます。 キロバイト単位のときは「KB」，メガバイト単位のときは「MB」と指定してください。指定しない場合には，バイト単位に見なされます。指定できる値の範囲は，512KB～32MB です。 デフォルト値：1MB

プロパティファイルの書式

```
<プロパティ名>=<値>
#<注釈>
```

- *<プロパティ名>*と*<値>*は「=」で区切ります。
- *<注釈>*を指定する場合，行の先頭に「#」を付けます。

プロパティファイルの編集手順

1. プロパティファイルをテキストエディターなどで開き，プロパティを編集します。

   server.properties ファイルまたは logger.properties ファイルで，共通エージェントコンポーネントの設定を変更します。

   注意事項

「表 A-1 共通エージェントコンポーネントの設定を変更するためのプロパティ（server.properties）」または「表 A-2 共通エージェントコンポーネントのログファイルの設定を変更するためのプロパティ（logger.properties）」に示したプロパティ以外のプロパティの指定値は変更しないでください。

2. 共通エージェントコンポーネントを再起動します。

   共通エージェントコンポーネントをいったん停止してから，再度，起動します。起動および停止方法については，「A.4 共通エージェントコンポーネントの起動と停止」を参照してください。

A.4 共通エージェントコンポーネントの起動と停止

HDLM のホストを Global Link Manager のリソースとして追加し，Global Link Manager の管理対象にする場合は，共通エージェントコンポーネントが起動されている必要があります。このほかに，HDLM が起動している必要があります。

ここでは，共通エージェントコンポーネントの起動と停止，および稼働状況の確認方法について説明します。

共通エージェントコンポーネントは，HDLM のインストール時に自動的に起動されますが，次の場合には手動で再起動（停止および起動）する必要があります。

- HDLM をインストールしたホストの IP アドレスを変更した場合
- 共通エージェントコンポーネントのプロパティファイルを更新した場合

注意事項

Windows Server 2012（x64）または Windows Server 2012 R2 のホストでは，共通エージェントコンポーネントは WOW64 上で動作します。共通エージェントコンポーネントが提供するコマンドを実行する場合，WOW64 用のコマンドプロンプトから実行してください。コマンドプロンプトの実行例を次に示します。

```
C:¥WINDOWS¥SysWOW64¥cmd.exe
```

A.4.1 共通エージェントコンポーネントの起動

共通エージェントコンポーネントを起動するには，ホストの OS に応じて次に示すコマンドを実行します。この操作には，Administrator 権限または root 権限が必要です。

Windows の場合

<共通エージェントコンポーネントのインストールフォルダ>¥bin¥hbsasrv.exe start

Solaris または Linux の場合

```
/opt/HDVM/HBaseAgent/bin/hbsasrv start
```

AIX の場合

```
/usr/HDVM/HBaseAgent/bin/hbsasrv start
```

A.4.2 共通エージェントコンポーネントの停止

共通エージェントコンポーネントを停止するには，ホストの OS に応じて次に示すコマンドを実行します。この操作には，Administrator 権限または root 権限が必要です。

Windows の場合

<共通エージェントコンポーネントのインストールフォルダ>¥bin¥hbsasrv.exe stop

Solaris または Linux の場合

/opt/HDVM/HBaseAgent/bin/hbsasrv stop

AIX の場合

/usr/HDVM/HBaseAgent/bin/hbsasrv stop

A.4.3 共通エージェントコンポーネントの稼働状況の確認

共通エージェントコンポーネントの稼働状況を確認するには，ホストの OS に応じて次に示すコマンドを実行します。この操作には，Administrator 権限または root 権限が必要です。

Windows の場合

<共通エージェントコンポーネントのインストールフォルダ>¥bin¥hbsasrv.exe status

Solaris または Linux の場合

/opt/HDVM/HBaseAgent/bin/hbsasrv status

AIX の場合

/usr/HDVM/HBaseAgent/bin/hbsasrv status

コマンド実行結果の Status に「Running」と表示された場合は，共通エージェントコンポーネントのサービス（またはデーモンプロセス）が稼働中であることを示します。「Stop」と表示された場合は，サービス（またはデーモンプロセス）が停止中であることを示します。

A.4.4 hbsasrv コマンドの構文

共通エージェントコンポーネントの起動と停止，および稼働状況の確認で使用する hbsasrv コマンドの構文について説明します。

hbsasrv コマンドの構文を次の表に示します。

表 A-3 hbsasrv コマンドの構文

項目	説明
構文	hbsasrv [start | stop [-f] | status]
機能	共通エージェントコンポーネントのサービス（またはデーモンプロセス）を起動，停止します。また，サービス（またはデーモンプロセス）の状態を表示します。
オプション	start：サービス（またはデーモンプロセス）を起動します。 stop [-f]：サービス（またはデーモンプロセス）を停止します。 ホストにほかの Hitachi Command Suite 製品がインストールされている場合，共通エージェントコンポーネントを停止できないことがあります。この場合，KAIE62604-E のエラーメッセージが表示されます。ほかの Hitachi Command Suite 製品の動作が完了するまで待ち，再度コマンドを実行してください。 共通エージェントコンポーネントを緊急に停止させたい場合，-f オプションを付けて実行することで，強制的に共通エージェントコンポーネントを停止できます。この場合，すべての処理が強制的に終了されますので，実行中のジョブの処理は保証されません。 status：サービス（またはデーモンプロセス）の稼働状態を表示します。 参考： 引数を指定しないでコマンドを実行した場合，コマンドの使用方法を表示します。

A.5 共通エージェントコンポーネントで使用する Java プログラムを変更する場合の設定

共通エージェントコンポーネントで使用する Java プログラムを変更する手順を次に示します。

Solaris または AIX の場合

「A.3 共通エージェントコンポーネントの設定の変更」の「表 A-1 共通エージェントコンポーネントの設定を変更するためのプロパティ（server.properties）」に記載されている server.agent.JRE.location の説明を参照して，Java プログラムのインストール先を指定してください。

Windows または Linux の場合

javapath_setup コマンドを実行して，使用する Java プログラムを変更してください。

注意事項

- HDLM がサポートしている Java の実行環境については，マニュアル「Hitachi Dynamic Link Manager ユーザーズガイド」を参照してください。
- Windows 版，VMware 版，および Linux 版の HDLM は，8.8.3 以降は共通エージェントコンポーネントに同梱された Java だけをサポートします。javapath_setup コマンドを実行して，使用する Java プログラムを変更しないでください。

A.5.1 javapath_setup コマンドを実行して使用する Java プログラムを変更する手順

1. 次のコマンドを実行して，使用する Java プログラムを変更します。

Windows の場合

＜共通エージェントコンポーネントのインストールフォルダ＞¥bin¥javapath_setup.exe

Linux の場合

/opt/HDVM/HBaseAgent/bin/javapath_setup.sh

javapath_setup コマンドには，次の表に示すオプションを指定できます。

コマンドの書式

javapath_setup {-set [new|bundle|＜*Java の実行環境のインストールパス*＞]|-check}

オプションの説明

表 A-4 javapath_setup コマンドのオプションと引数

オプションの引数	内容
-set	Java の実行環境を変更する場合に指定します。引数を省略した場合は，new を指定したものと見なされます。
new	ホストにインストールされている Oracle JDK または Oracle JRE のうち，最新バージョンの Java の実行環境を使用するときに指定します。 同じバージョンの Java の実行環境がインストールされている場合は JDK が優先されます。
bundle	共通エージェントコンポーネントに同梱された Java の実行環境を使用するときに指定します。
＜*Java の実行環境のインストールパス*＞	特定の Java の実行環境を使用するときに，インストールパスを絶対パスで指定します。
-check	ホストにインストールされている Oracle JDK または Oracle JRE のうち，最新バージョンの Java の実行環境を確認する場合に指定します。

2. コマンド実行後，共通エージェントコンポーネントを再起動します。

共通エージェントコンポーネントの起動と停止は「A.4 共通エージェントコンポーネントの起動と停止」を参照してください。

3. HDLM GUI を起動している場合は HDLM GUI を再起動します。

注意事項

- Java プログラムを再インストールした場合や，アップデートした場合は，Java プログラムのインストール先が変更されるため，再度コマンドを実行する必要があります。
- Java プログラムを変更して運用している場合に，Java プログラムをアンインストールすると，Windows 版 HDLM のアンインストールが失敗するため，使用する Java プログラムを元に戻したあとで Windows 版 HDLM をアンインストールしてください。

B

このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

B.1 関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- Hitachi Global Link Manager ユーザーズガイド（4010-1J-168）
- Hitachi Global Link Manager メッセージ（4010-1J-170）
- Hitachi Dynamic Link Manager EX ユーザーズガイド（AIX 用）（4010-1J-161）
- Hitachi Dynamic Link Manager ユーザーズガイド（AIX 用）（4010-1J-162）
- Hitachi Dynamic Link Manager ユーザーズガイド（Linux®用）（4010-1J-163）
- Hitachi Dynamic Link Manager ユーザーズガイド（Solaris 用）（4010-1J-164）
- Hitachi Dynamic Link Manager ユーザーズガイド（Windows®用）（4010-1J-165）
- Hitachi Dynamic Link Manager ユーザーズガイド（VMware®用）（4010-1J-166）
- Hitachi Command Suite ユーザーズガイド（3021-9-003）
- Hitachi Command Suite インストールガイド（3021-9-006）
- Hitachi Command Suite システム構成ガイド（3021-9-008）
- Hitachi Command Suite Tuning Manager 運用管理ガイド（3021-9-037）
- JP1 Version 8 JP1/Integrated Management - Manager システム構築・運用ガイド（3020-3-K01）
- JP1 Version 10 JP1/Base 運用ガイド（3021-3-001）
- JP1 Version 7i JP1/NETM/DM システム構築（Windows(R)用）（3020-3-G31）
- JP1 Version 7i JP1/NETM/DM システム運用 1（Windows(R)用）（3020-3-G32）
- JP1 Version 7i JP1/NETM/DM システム運用 2（Windows(R)用）（3020-3-G33）
- JP1 Version 10 JP1/NETM/DM 構築ガイド(Windows(R)用)（3021-3-176）
- JP1 Version 10 JP1/NETM/DM 運用ガイド 1(Windows(R)用)（3021-3-177）
- JP1 Version 10 JP1/NETM/DM 運用ガイド 2(Windows(R)用)（3021-3-178）
- JP1 Version 10 JP1/NETM/DM 導入・設計ガイド(Windows(R)用)（3021-3-175）
- JP1 Version 6 JP1/NETM/DM Manager（3000-3-841）
- JP1 Version 10 JP1/NETM/DM Client(UNIX(R)用)（3021-3-181）

B.2 このマニュアルでの表記

このマニュアルでは，製品の名称を省略して表記しています。このマニュアルでの表記と，製品の正式名称または意味を次に示します。

このマニュアルでの表記	製品名称または意味
Compute Systems Manager	Hitachi Compute Systems Manager
Device Manager	Hitachi Device Manager
Device Manager エージェント	Hitachi Device Manager に含まれる Device Manager エージェント
HDLM	次の製品を区別する必要がない場合の表記です。 ・ Hitachi Dynamic Link Manager ・ Hitachi Dynamic Link Manager EX
Itanium	Itanium®

このマニュアルでの表記	製品名称または意味
J2EE	次の製品を区別する必要がない場合の表記です。 ・ J2EE ・ Java 2 Platform, Enterprise Edition
JDK	Java Development Kit
JP1/IM	次の製品を区別する必要がない場合の表記です。 ・ JP1/Integrated Management - Manager ・ JP1/Integrated Management - View
JP1/IM - Manager	JP1/Integrated Management - Manager
JP1/IM - View	JP1/Integrated Management - View
JP1/NETM/DM	次の製品を区別する必要がない場合の表記です。 ・ JP1/NETM/DM Manager ・ JP1/NETM/DM Client
JRE	Java 2 Runtime Environment, Standard Edition
Linux	Linux®
Replication Manager	Hitachi Replication Manager
Replication Monitor	JP1/HiCommand Replication Monitor
Storage Navigator Modular 2	Hitachi Storage Navigator Modular 2
Tuning Manager	Hitachi Tuning Manager
VMware	VMware®
VSP Fx00 モデル	次の製品を区別する必要がない場合の表記です。 ・ Hitachi Virtual Storage Platform F350 ・ Hitachi Virtual Storage Platform F370 ・ Hitachi Virtual Storage Platform F400 ・ Hitachi Virtual Storage Platform F600 ・ Hitachi Virtual Storage Platform F700 ・ Hitachi Virtual Storage Platform F800 ・ Hitachi Virtual Storage Platform F900
VSP Gx00 モデル	次の製品を区別する必要がない場合の表記です。 ・ Hitachi Virtual Storage Platform G100 ・ Hitachi Virtual Storage Platform G130 ・ Hitachi Virtual Storage Platform G150 ・ Hitachi Virtual Storage Platform G200 ・ Hitachi Virtual Storage Platform G350 ・ Hitachi Virtual Storage Platform G370 ・ Hitachi Virtual Storage Platform G400 ・ Hitachi Virtual Storage Platform G600 ・ Hitachi Virtual Storage Platform G700 ・ Hitachi Virtual Storage Platform G800 ・ Hitachi Virtual Storage Platform G900

- AIX，Linux，および Solaris を区別する必要がない場合，UNIX と表記しています。
- このマニュアルでは，HDLM のバージョンを「＜*x*＞.＜*y*＞.＜*z*＞」形式に統一して表記しています（例：05-62 の場合は 5.6.2，05-80 の場合は 5.8 と表記）。

B.3 このマニュアルで使用している略語

このマニュアルでは，次に示す略語を使用しています。

略語	正式名称
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CHA	Channel Adapter
CN	Common Name
CPU	Central Processing Unit
CSR	Certificate Signing Request
CSV	Comma Separated Value
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
FC	Fibre Channel
FC-SP	Fibre Channel Security Protocol
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
IP	Internet Protocol
IPF	Itanium Processor Family
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer System Interface
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDEV	Logical Device
LU	Logical Unit
MIB	Management Information Base
NAS	Network Attached Storage
NTP	Network Time Protocol
OS	Operating System
RADIUS	Remote Authentication Dial In User Service
SAN	Storage Area Network
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SSL	Secure Sockets Layer
SSO	Single Sign-on
TLS	Transport Layer Security
URL	Uniform Resource Locator
XML	Extensible Markup Language

B.4 KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）は，それぞれ1KiB（キビバイト），1MiB（メビバイト），1GiB（ギビバイト），1TiB（テビバイト）と読み替えてください。

1KiB，1MiB，1GiB，1TiB は，それぞれ 1,024 バイト，1,024KiB，1,024MiB，1,024GiB です。

索引

数字

D

G

H

I

J

L

S

T

U

W

あ

い

う

え

か

き

く

け

こ

さ

し

す

せ

た

つ

て

と

は

ひ

へ

ほ

ま

ゆ

ら

り

ろ

株式会社 日立製作所

〒 100-8280　東京都千代田区丸の内一丁目 6 番 6 号