NEC

iStorage V100/V300

HA Command Suite システム構成ガイド

iStorage

IV-UG-203-001-07

対象製品

HA Device Manager 8.8.6

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

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

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

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

Google Chrome は，Google Inc.が所有する商標または登録商標です。

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

Itanium は，アメリカ合衆国および / またはその他の国における Intel Corporation またはその子会社の商標です。

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

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

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

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.

RC4 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。

Red Hat, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

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.

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Java is a registered trademark of Oracle and/or its affiliates.

発行

2024 年 4 月（IV-UG-203）

著作権

目次

はじめに

このマニュアルは，HA Device Manager および HA Command Suite 共通コンポーネントのシステム構成，環境設定およびトラブルシューティングについて説明したものです。

以降，このマニュアルでは，HA Device Manager を Device Manager と略します。

対象読者

このマニュアルは，Device Manager を使用してシステムを運用管理される方を対象としています。また，対象読者には次のような知識があることを前提としています。

- ストレージシステム固有の管理ツールに関する基本的な知識
- SAN（Storage Area Network）に関する基本的な知識
- 前提 OS に関する基本的な知識
- 前提クラスタソフトウェアに関する基本的な知識

マニュアルの構成

このマニュアルは，次に示す章と付録から構成されています。

第 1 章　概要

Device Manager を使用する場合のシステム構成とシステム要件について説明しています。

第 2 章　ネットワーク構成に応じた設定

ネットワーク構成に応じて必要な HA Command Suite 製品での設定について説明しています。

第 3 章　ユーザーアカウントを管理するために必要な設定

HA Command Suite 製品のユーザーアカウントを管理するために必要な設定について説明しています。

第 4 章　外部認証サーバでのユーザー管理

外部認証サーバでユーザー認証する方法について説明しています。

第 5 章　通信に関するセキュリティ設定

HA Command Suite 製品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。

第 6 章　ログおよびアラートの設定

HA Command Suite 製品でシステムの状態や障害を監視するために必要な設定について説明しています。

第 7 章　サービスの起動と停止

管理サーバ上の HA Command Suite 製品のサービスを起動したり停止したりする方法について説明しています。

第 8 章　データベースの管理

HA Command Suite 製品のデータベースをバックアップしたり，復元したりする方法について説明しています。

第 9 章　Device Manager の監査ログ

Device Manager の監査ログを採取するために必要な設定や，監査ログで確認できる情報について説明しています。

第 10 章　トラブルシューティング

Device Manager の運用中に発生した問題の解決策や保守情報の取得方法について説明しています。

付録 A　Device Manager サーバのプロパティ

Device Manager サーバのプロパティファイルについて説明しています。

付録 B　管理クライアントに関するセキュリティ設定

管理クライアントに関するセキュリティ設定について説明しています。

付録 C　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
Active Directory	Microsoft Active Directory
Hyper-V	Microsoft Hyper-V
Windows	Microsoft Windows

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，次に示す記号を使用しています。

<table>
<tr><th>記号</th><th>意味と例</th></tr>
<tr><td>［ ］
（角括弧）</td><td>画面，メニュー，ボタン，キーボードのキーなどを示します。
また，表示項目を連続して選択する場合には，［ ］を－でつないで説明しています。</td></tr>
<tr><td>< >
（山括弧）</td><td>可変値であることを示します。</td></tr>
</table>

また，このマニュアルでは，次に示す記号を使用してコマンドの文法を説明しています。

<table>
<tr><th>記号</th><th>意味と例</th></tr>
<tr><td>|
（ストローク）</td><td>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。</td></tr>
<tr><td>{ }
（波括弧）</td><td>この記号で囲まれている複数の項目の中から，必ず一組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。</td></tr>
<tr><td>[ ]
（角括弧）</td><td>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）。</td></tr>
<tr><td>...点線
（リーダー）</td><td>記述が省略されていることを示します。この記号の直前に示された項目を繰り返し複数個指定できます。
（例）
「A,B,C...」は，「A と B の後ろに C を複数個指定できる」ことを示します。</td></tr>
</table>

OS，仮想化ソフトウェア，ブラウザーなどのサポートについて

OS，仮想化ソフトウェア，ブラウザーなどの最新のサポート状況は，「ソフトウェア添付資料」を参照してください。

サポートが終了したソフトウェアに関するマニュアル中の記載は無視してください。

新しいバージョンをサポートしたソフトウェアについては，特に記載がないかぎり，従来サポートしているバージョンと同等のものとしてサポートします。

エンドユーザライセンスについて

デスクトップアプリケーションの GUI には，Adobe AIR を使用しています。

- Prohibitions against distribution and/or copying of the Object Code Redistributables separately from a Developer Application.
- Prohibitions against creating modifications and/or derivative works of, and against decompiling and reverse engineering, the Object Code Redistributables;
- A disclaimer of indirect, special, incidental, punitive, and consequential damages, and of all applicable statutory warranties, to the full extent allowed by law;
- A provision indicating ownership of the Sample Code, SDK Source Files and Object Code Redistributables by HARMAN and its licensors.

第 1 章
概要

この章では，Device Manager のシステム構成とシステム要件について説明します。

1.1　システム構成

Device Manager を使用する場合の基本的なシステム構成を次の図に示します。

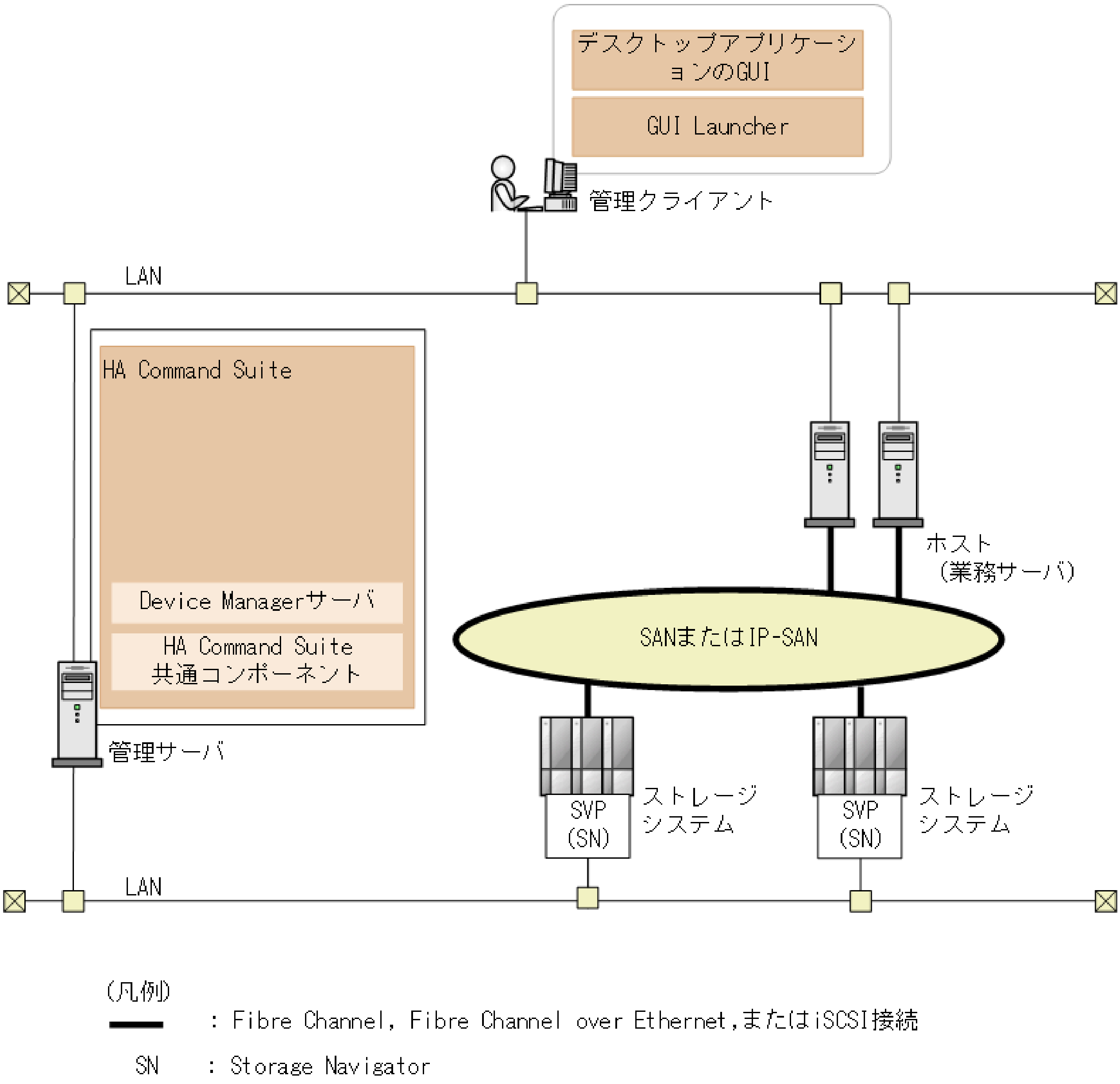


図 1-1　基本的なシステム構成

管理クライアント

Device Manager を操作する際に使用するマシンです。

GUI

グラフィカルユーザーインターフェースです。

- デスクトップアプリケーションの GUI（Adobe AIR 環境で動作する GUI）

GUI についてはマニュアル『HA Command Suite ユーザーズガイド』を参照してください。

管理サーバ

ストレージシステムやホストなどを統合管理するマシンです。HA Command Suite をインストールします。2 台のマシンを使用した Active-Standby 型のクラスタリングにも対応しています。

HA Command Suite は，次のコンポーネントから構成され，常に一緒にインストールおよびアンインストールされます。

HA Command Suite 共通コンポーネント

ユーザーアカウントの管理やセキュリティ監視など HA Command Suite 製品で共通する機能を提供するコンポーネントです。

Device Manager サーバ

Device Manager で，ストレージシステムのボリュームを管理するために必要なコンポーネントです。

ホスト（業務サーバ）

ストレージシステム内のボリュームを利用するマシンです。

ストレージシステム

HA Command Suite 製品で管理するストレージシステムです。次に示す機種のストレージシステムを管理できます。

- iStorage V シリーズ

SVP

ストレージシステムを管理するためのコンピュータです。iStorage V シリーズの場合に使用されます。iStorage V シリーズの場合，ストレージシステムの管理機能を提供するサーバを SVP として設置して使用します。

メモ

iStorage V シリーズを使用する場合，管理サーバと SVP の時刻を合わせてください。

Storage Navigator

Device Manager のコンポーネントです。ストレージシステムの構成やリソースの設定をより詳細な条件で行うための機能を提供します。

ネットワーク（LAN および SAN）

管理サーバと管理クライアント間，管理サーバとストレージシステム間は TCP/IP ネットワークで接続する必要があります。また，ホストとストレージシステム間は SAN または IP-SAN を構成します。

システム構成を検討する場合，次の点に注意してください。

- 1 台のストレージシステムは，1 台の管理サーバで管理してください。1 台のストレージシステムを複数の管理サーバで管理するシステムは構成しないでください。

1.2 セキュリティ構成

iStorage V シリーズは， SVP と通信します。

SVP には，次の 2 種類の Ethernet アダプターがあります。

- プライベート（内部）Ethernet LAN 用アダプター

  ストレージシステム内の通信に使用されます。

- パブリック LAN 用アダプター

  ストレージシステムの外部にあるほかのコンピュータのアプリケーションが, SVP と通信するために使用されます。Device Manager は，ストレージシステムおよび構成変更に関する SVP との通信に，このパブリック LAN を使用します。

注意

どのような状況下でも，外部ネットワークにプライベート LAN を接続しないでください。ストレージシステムで深刻な問題が発生するおそれがあります。

1.2.1 セキュリティについての一般的なリスク

システム管理者は，多くの場合，管理用の LAN と業務用の LAN を切り離します。そうすることで，管理用の LAN を独立させ，業務用のネットワークから管理用のトラフィックを切り離し，セキュリティ上の危険性を減らしています。もし，業務に使用する LAN に SVP のような管理端末が共存していたら, IP ネットワーク上のどのエンティティからでもストレージシステムにアクセスできてしまいます。アクセスが意図的なものであるかどうかに関わらず，結果として生じるリスクから，ストレージサービス拒否という現実の障害が発生するおそれがあります。DoS 攻撃によって，I/O 操作中のポートからストレージの領域がアンバインドされるなど，悪意のある目的で管理用のセッションが乗っ取られる危険性があります。

管理用の LAN の構成に関するガイドラインを以下に示します。

- 業務に使用する LAN からのトラフィックが管理用の LAN を流れたり, 経由したりしてはいけません。
- 管理用の LAN 上にある管理インターフェースまたはコントローラーを搭載したすべてのホストを最大限に強化して危険性を減らし，ステーションまたはデバイス全体が管理インターフェース以外のソフトウェアによって使用されないようにします（この場合の強化とは，不要なソフトウェアの削除，不要なサービスのシャットダウン，および最新のパッチへの更新を含みます）。
- 管理用の LAN は，例えば Device Manager サーバのように，管理用の LAN と業務用の LAN の間で仲立ちとして動作しているマシンでだけ，業務用の LAN とつながるようにします。
- プライベート LAN と管理用の LAN の両方につながるマシンを, ファイアウォールの後ろに置くと，意図しないアクセスをさらに防げます。

1.2.2 Device Manager で推奨するセキュリティ構成

管理サーバをデュアルホームにするか, NIC を 2 つ搭載してください。一方の NIC を管理用のマシンと管理対象のストレージシステムとの間の管理用の LAN に接続し，もう一方の NIC をファイアウォールによってアクセスが管理されている LAN に接続します。「図 1-2　管理用の LAN を分離し，ファイアウォールを設置した構成（5 ページ）」に示すように，各業務サーバは，個別のファイアウォールを持つ異なる LAN に接続することもできます。ファイアウォールには，Device Manager のクライアントまたは特定の管理アプリケーションのクライアントにだけ管理サーバへのアクセスを許可する，厳しいアクセス規則を設定してください。

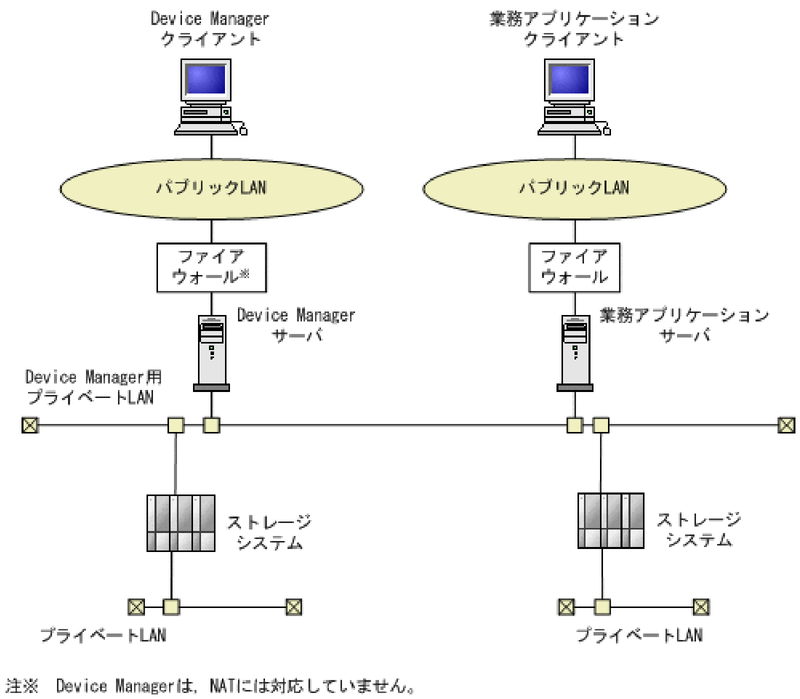


図 1-2　管理用の LAN を分離し，ファイアウォールを設置した構成

1.3　管理サーバのシステム要件

ここでは管理サーバのシステム要件について説明します。

1.3.1　管理リソース数の上限

Device Manager で管理できるリソース数には上限があります。

次の表に示す値を超えない構成で各製品を運用することを推奨します。

表 1-1　管理リソース数の上限値

リソース	Device Manager サーバの上限
LDEV 数※1	1,000,000
LDEV 数とパス数※2 の合計	5,000,000

注※1

オープンシステム用の LDEV 数の合計値です。

注※2

パス数 = ＜ LDEV 数＞ × ＜ 1LDEV 当たりの平均パス数＞

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）

1.3.2　メモリーヒープサイズの変更

Device Manager サーバのメモリーヒープサイズを変更するには，HA Command Suite の上書きインストールを実行し，インストールウィザードでメモリーヒープサイズを選択します。上書きインストールの前提条件やメモリーヒープサイズの設定値は，HA Command Suite インストールガイドを参照してください。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

1.4　Device Manager で管理できるホスト

Device Manager では，管理対象のストレージシステムのボリュームを使用するマシンをホストとして管理できます。各ホストのディスクリソースを Device Manager で一元管理することで，利用状況に応じて最適なボリュームを割り当てることができます。 ホスト（業務サーバ）にストレージシステムのボリュームを割り当てたり，各ホストでのボリュームの使用状況を確認したりするためには，Device Manager のリソースとして登録する必要があります。

Device Manager では，次の表に示すホストでのボリュームの利用状況を管理できます。

表 1-2　Device Manager で管理できるホスト

ホスト		説明
オープンホスト	通常ホスト	仮想化ソフトウェアがインストールされていない環境
	仮想マシン	仮想化ソフトウェア上に作成された仮想環境
	仮想化サーバ	仮想化ソフトウェアがインストールされた物理環境

メモ

Device Manager で管理するホストのホスト名は，50 バイト以内であることが前提です。

1.5　コマンドを実行する場合の注意事項

Windows で UAC（User Account Control）機能が有効になっている場合，コマンドを実行するには，管理者権限でコマンドプロンプトを起動してください。

第 2 章
ネットワーク構成に応じた設定

この章では，ネットワーク構成に応じて必要な HA Command Suite 製品での設定について説明します。

2.1　HA Command Suite 製品で使用されるポート

HA Command Suite 製品で使用されるポート番号が，同一マシンに共存するほかのプログラムと重複しないように調整してください。

重複する場合は，そのプログラムの設定を変更するか，HA Command Suite 製品の設定を変更してください。

ヒント

ポート番号によっては，OS の一時割り当てポートと重複しているものもあります。HA Command Suite 製品で使用するポート番号を OS の `services` ファイルに設定することで，一時割り当て対象から外すこともできます。

2.1.1　HA Command Suite 共通コンポーネントで使用されるポート

管理サーバでは，HA Command Suite 共通コンポーネントで使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-1　HA Command Suite 共通コンポーネントで使用されるポート

ポート番号	説明
22015/tcp※	管理クライアント（GUI）と通信する際に，HBase 64 Storage Mgmt Web Service へのアクセスで使用されます。 このポート番号は変更できます。
22016/tcp	管理クライアント（GUI）と SSL で通信する際に，HBase 64 Storage Mgmt Web Service へのアクセスで使用されます。 このポート番号は変更できます。
22017/tcp～22030/tcp 22033/tcp 22034/tcp	HA Command Suite 共通コンポーネントで予約済みのポートです。
22031/tcp	HA 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。 このポート番号は変更できます。
22032/tcp	HA Command Suite 共通コンポーネントの内部通信（HiRDB）で使用されます。 このポート番号は変更できます。

ポート番号	説明
22035/tcp 22037/tcp 22038/tcp	HA 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。 このポート番号は変更できます。
22036/tcp	HA 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。 このポート番号は変更できます。
22121/tcp 22123/tcp 22124/tcp	Device Manager Web Service で使用されるポートです。 HA 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。 このポート番号は変更できます。
22122/tcp	Device Manager Web Service で使用されるポートです。 HA 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。 このポート番号は変更できます。

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。

関連リンク

HA Command Suite 共通コンポーネントで使用されるポートの変更（10 ページ）
Device Manager のファイアウォールの例外登録（13 ページ）
SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集（84 ページ）

2.1.2 Device Manager サーバで使用されるポート

管理サーバでは，Device Manager サーバで使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-2 Device Manager サーバで使用されるポート

ポート番号	説明
162/udp	SNMP トラップを受信する際に使用されます。 ほかの製品でこのポートが使用されていると，Device Manager サーバが起動しません。 Device Manager サーバでは使用するポート番号を変更できません。このポートを使用する製品が同一マシンにインストールされている場合は，その製品の設定を変更するか，Device Manager サーバの `server.dispatcher.daemon.receiveTrap` プロパティに `false` を設定してください。
2001/tcp※	Device Manager サーバの内部通信，管理クライアント（GUI），ストレージシステムと通信する際に使用されます。 ほかの製品でこのポートが使用されていると，Device Manager サーバが起動しません。 このポートは，Device Manager サーバの `server.properties` ファイルにある `server.http.port` プロパティで変更できます。

ポート番号	説明
2443/tcp	Device Manager サーバの内部通信，管理クライアント（GUI）との SSL 通信，およびストレージシステム（iStorage V シリーズ）との SSL 通信で使用されます。 このポートは，Device Manager サーバの `server.properties` ファイルにある `server.https.port` プロパティで変更できます。
23055/tcp	Device Manager サーバの内部通信で使用されます。 このポートは，Device Manager サーバの `server.properties` ファイルにある `server.rmi.port` プロパティで変更できます。

注※

SSL を設定している場合でも使用されます。SSL 通信だけを許可したい場合は，ファイアウォールを設定してください。

関連リンク

Device Manager のファイアウォールの例外登録（13 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
server.http.port（180 ページ）
server.https.port（180 ページ）
server.rmi.port（180 ページ）

2.1.3 ストレージシステムで使用されるポート

Device Manager でストレージシステムを管理するためには，管理サーバや管理クライアント（GUI）との通信用ポートを用意する必要があります。

表 2-3 ストレージシステムで使用されるポート

対象ストレージシステム	ポート番号	説明
iStorage V シリーズ（SVP）	443/tcp	管理クライアント（GUI）から SSL で Storage Navigator を起動する際に使用されます。 このポート番号は変更できます。
	1099/tcp	管理サーバまたは管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できます。
	51099/tcp	管理サーバまたは管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できます。
	51100/tcp	管理サーバまたは管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できます。 デフォルトでは 51100/tcp～51355/tcp の範囲で使用されます。
iStorage V シリーズ（コントローラー）	443/tcp	管理クライアント（GUI）から SSL で Maintenance Utility を起動する際に使用されます。

対象ストレージシステム	ポート番号	説明
		このポート番号は変更できません。

iStorage V シリーズ（SVP）で使用されるポート番号を変更した場合には，Device Manager で次の設定が必要です。

- ファイアウォールの例外登録を設定し直す
- 変更後のポート番号を Device Manager に設定する

  1099/tcp を変更した場合には，Device Manager GUI の［ストレージシステム編集］画面で，変更後のポート番号を設定してください。443/tcp を変更した場合には，Device Manager の GUI でストレージシステムをリフレッシュしてください。

ポート番号の変更方法および `services` ファイルの設定方法については，各ストレージシステムのマニュアルを参照してください。

2.2 HA Command Suite 共通コンポーネントで使用されるポートの変更

HA Command Suite 製品のインストール後に，HA Command Suite 共通コンポーネントで使用されるポートを変更する場合は，HA Command Suite 共通コンポーネントの設定ファイルを編集する必要があります。

操作手順

1. HA Command Suite 製品のサービスを停止します。
2. HA Command Suite 共通コンポーネントの設定ファイルを編集して，ポート番号の設定を変更します。

表 2-4 HA Command Suite 共通コンポーネントのポート番号設定ファイル

デフォルトのポート番号	設定ファイル	変更場所
22015/tcp	＜*HA Command Suite のインストールフォルダ*＞`\Base64\uCPSB11\httpsd\conf\user_httpsd.conf`※1	`Listen`
22016/tcp	＜*HA Command Suite のインストールフォルダ*＞`\Base64\uCPSB11\httpsd\conf\user_httpsd.conf`※1	• `VirtualHost` ＜*ホスト名*＞`:`＜*ポート*＞ • `Listen`※2
22031/tcp	＜*HA Command Suite のインストールフォルダ*＞`\Base64\uCPSB11\httpsd\conf\user_hsso_httpsd.conf`	`Listen 127.0.0.1:`＜*ポート番号*＞
22032/tcp	＜*HA Command Suite のインストールフォルダ*＞`\Base64\HDB\CONF\emb\HiRDB.ini`	`PDNAMEPORT`
	＜*HA Command Suite のインストールフォルダ*＞`\Base64\HDB\CONF\pdsys`	`pd_name_port`

デフォルトのポート番号	設定ファイル	変更場所
	< *HA Command Suite のインストールフォルダ*>\Base64\database\work\def_pdsys	pd_name_port
22035/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	webserver.connector.nio_http.port※3
22036/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	ejbserver.rmi.naming.port
22037/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	ejbserver.http.port
22038/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties	ejbserver.rmi.remote.listener.port
22121/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties	webserver.connector.nio_http.port※4
22122/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties	ejbserver.rmi.naming.port
22123/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties	ejbserver.http.port
22124/tcp	< *HA Command Suite のインストールフォルダ*>\Base64\uCPSB11\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties	ejbserver.rmi.remote.listener.port

注※1

httpsd.conf ファイルは編集しないでください。

注※2

SSL が有効の場合に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 Listen 22015 行を編集する必要があります。

注※3

下記のファイル内に当該ポート番号が記載されている場合，それらのポート番号も併せて変更してください。

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\reverse_proxy.conf`

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\reverse_proxy_before.conf`

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\reverse_proxy_after.conf`

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\hsso_reverse_proxy.conf`

注※4

下記のファイル内に当該ポート番号が記載されている場合，それらのポート番号も併せて変更してください。

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\reverse_proxy.conf`

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\reverse_proxy_before.conf`

< *HA Command Suite のインストールフォルダ*>`\Base64\uCPSB11\httpsd\conf\reverse_proxy_after.conf`

メモ

次のポート番号に変更しないでください。

1，7，9，11，13，15，17，19，20，21，22，23，25，37，42，43，53，77，79，87，95，101，102，103，104，109，110，111，113，115，117，119，123，135，139，143，179，389，465，512，513，514，515，526，530，531，532，540，556，563，587，601，636，993，995，2049，4045，6000

3. HA Command Suite 製品のサービスを起動します。
4. 次のポート番号を変更した場合には，管理サーバにインストールされている HA Command Suite 製品の 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。

   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。

関連リンク

HA Command Suite 共通コンポーネントで使用されるポート（7 ページ）
HA Command Suite 製品の URL の変更（hcmds64chgurl コマンド）（23 ページ）
SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集（84 ページ）
ポップアップブロックの設定変更（109 ページ）
Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）
Device Manager サーバのプロパティの変更（178 ページ）

2.3　Device Manager のファイアウォールの例外登録

HA Command Suite 製品で使用されるポートやプロセスをファイアウォールに例外登録すると，登録されたポートやプロセスへの外部からの接続が許可されます。

メモ

運用開始後に Windows ファイアウォールを有効にした場合，管理サーバに接続されているネットワーク上にファイアウォールが設置されているときは，管理サーバで使用されるポートについては，Device Manager のインストール後にユーザーが手動で例外登録を行う必要があります。

Device Manager を構成する各コンポーネントをファイアウォールの例外リストに登録します。

2.3.1　Device Manager でファイアウォールへの例外登録が必要なポート

管理サーバや管理クライアント，ストレージシステムなどをつなぐネットワーク上にファイアウォールが設置されている環境では，HA Command Suite 製品で使用されるポートをファイアウォールの例外として登録する必要があります。

- 表 2-5　管理サーバと管理クライアントとの間のファイアウォールで例外登録が必要なポート番号（14 ページ）
- 表 2-6　管理サーバとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号（14 ページ）
- 表 2-7　管理クライアントとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号（15 ページ）
- 表 2-8　管理サーバとメールサーバとの間のファイアウォールで例外登録が必要なポート番号（15 ページ）
- 表 2-9　管理サーバと外部認証サーバとの間のファイアウォールで例外登録が必要なポート番号（16 ページ）

表 2-5　管理サーバと管理クライアントとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理クライアント（GUI）	2001/tcp※	管理サーバ	非 SSL 通信の場合に設定が必要です。
any/tcp	管理クライアント（GUI）	2443/tcp※	管理サーバ	SSL 通信の場合に設定が必要です。
any/tcp	管理クライアント（GUI）	22015/tcp※	管理サーバ	非 SSL 通信の場合に設定が必要です。
any/tcp	管理クライアント（GUI）	22016/tcp※	管理サーバ	SSL 通信の場合に設定が必要です。

注※

ポート番号は変更できます。

表 2-6　管理サーバとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/udp	iStorage V シリーズ（コントローラー）	162/udp	管理サーバ	-
any/tcp	管理サーバ	443/tcp※1	iStorage V シリーズ（SVP）	-
any/tcp	管理サーバ	1099/tcp※1	iStorage V シリーズ（SVP）	-
any/tcp	iStorage V シリーズ（SVP）	2443/tcp※2	管理サーバ	-
any/tcp	管理サーバ	51099/tcp※1	iStorage V シリーズ（SVP）	-
any/tcp	管理サーバ	51100/tcp※1	iStorage V シリーズ（SVP）	デフォルトでは 51100/tcp～51355/tcp の範囲で使用されます。

（凡例）

- : 該当なし

注※1

iStorage V シリーズ（SVP）の場合，ポート番号は変更できます。

注※2

ポート番号は変更できます。

表 2-7　管理クライアントとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理クライアント （GUI）	443/tcp※1	iStorage V シリーズ（SVP およびコントローラー）	SSL で Storage Navigator を使用する場合に設定が必要です。
any/tcp	管理クライアント （GUI）	1099/tcp※1	iStorage V シリーズ（SVP）	-
any/tcp	管理クライアント （GUI）	51099/tcp※1	iStorage V シリーズ（SVP）	-
any/tcp	管理クライアント （GUI）	51100/tcp※1	iStorage V シリーズ（SVP）	デフォルトでは 51100/tcp～51355/tcp の範囲で使用されます。
any/tcp	管理クライアント （GUI）	161/udp	iStorage V シリーズ（コントローラー）	管理クライアントを SNMP マネージャーとして使用する場合に設定が必要です。

（凡例）

- : 該当なし

注※1

iStorage V シリーズ（SVP）の場合，ポート番号は変更できます。

表 2-8　管理サーバとメールサーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ（Device Manager サーバ）	25/tcp※1	メールサーバ※2	次の事象を E メールでユーザーに通知する場合に設定が必要です。 • ストレージシステムでのアラートの発生 • ［データマイグレーション］ウィザードから実行したタスクの完了

注※1

ポート番号は変更できます。

注※2

Device Manager サーバの `server.mail.smtp.host` プロパティに指定したメールサーバです。

表 2-9　管理サーバと外部認証サーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	88/tcp※	Kerberos サーバ	-
any/udp	管理サーバ	88/udp※	Kerberos サーバ	-
any/tcp	管理サーバ	389/tcp※	LDAP ディレクトリサーバ	-
any/udp	管理サーバ	1812/udp※	RADIUS サーバ	-

（凡例）

- : 該当なし

注※

一般的に使用されるポート番号です。外部認証サーバで変更されていることがあります。

関連リンク

Device Manager でのファイアウォールの例外登録（Windows）（16 ページ）

2.3.2　Device Manager でのファイアウォールの例外登録（Windows）

`hcmds64fwcancel` コマンドおよび `netsh` コマンドを実行して，Device Manager を構成する各コンポーネントをファイアウォールの例外リストに登録します。

操作手順

1. 次のコマンドを実行して，HA Command Suite 共通 Web サービスを例外リストに登録します。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\bin\hcmds64fwcancel`

2. 次のコマンドを実行して，Device Manager で使用するそのほかのコンポーネントを例外リストに登録します。

   `netsh advfirewall firewall add rule name="`＜*例外登録名*＞`" dir=in action=allow program="`＜*パス*＞`" description="`＜*パス*＞`" enable=yes`

表 2-10　netsh コマンドで指定する例外登録名とパス

コンポーネント	例外登録名	パス
Device Manager サーバ	Device Manager	＜ *HA Command Suite のインストールフォルダ*＞`\DeviceManager\Server\DeviceManagerServer.exe`

コンポーネント	例外登録名	パス
JDK	Device Manager - HBase64(java)	*< HA Command Suite のインストールフォルダ>*`\Base64\uCPSB11\hjdk\jdk\bin\java.exe`

3. 設定を有効にするために，HA Command Suite 製品のサービスを再起動します。

関連リンク

Device Manager でファイアウォールへの例外登録が必要なポート（13 ページ）
Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

2.4 IP アドレスが複数ある場合のネットワーク設定

複数のネットワーク構成の場合の通信設定について説明します。

2.4.1 管理サーバでブリッジ機能を使用する場合のネットワークの設定

管理サーバに NIC を複数搭載してブリッジ機能を使用する場合，管理サーバ，管理クライアント，およびストレージシステム間でお互いに通信できるようにネットワークを設定してください。

次の図に示す構成を例に，設定が必要な個所を説明します。

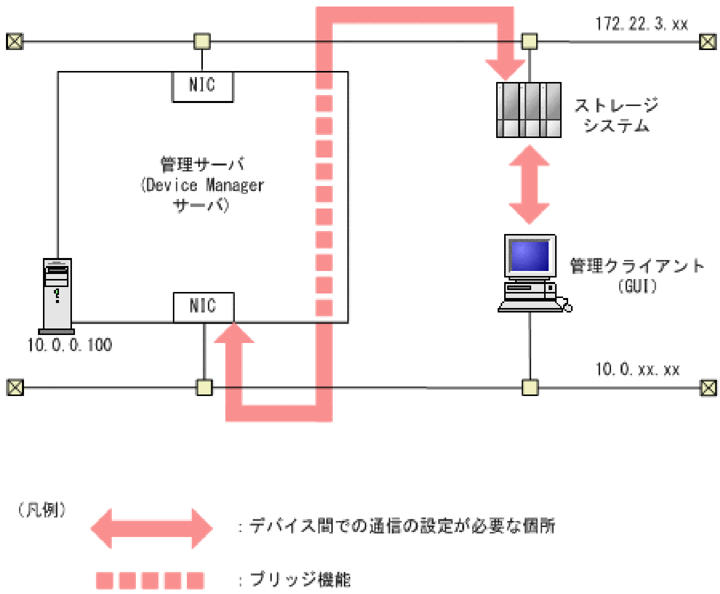


図 2-1　管理サーバのブリッジ機能を使用したネットワークの構成例

図中の矢印に示すデバイス間でお互いに通信できるように，ルーター，管理クライアント，および管理サーバを設定してください。

- ストレージシステムと，管理クライアントの間
- ストレージシステムと，管理サーバの間

注意

HA Command Suite 製品の次の設定で IP アドレスを指定するときは，管理クライアントに接続されているネットワーク側の IP アドレス（「図 2-1　管理サーバのブリッジ機能を使用したネットワークの構成例（17 ページ）」中の `10.0.0.100`）を指定してください。ホスト名は指定しないでください。

- Device Manager の Web サーバ機能が動作するマシンの設定（`server.http.host` プロパティ）

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
server.http.host（179 ページ）

2.5　IPv6 環境で運用する場合の Device Manager の設定

Device Manager は，IPv6 による通信をサポートしています。IPv6 環境で運用する場合，環境に応じて Device Manager の設定を変更する必要があります。

IPv6 環境で運用する際は，次に示す前提条件を満たすようにしてください。

- IPv6 を使用する場合も，製品内部で IPv4 の処理をする必要があるため，IPv6 と IPv4 の両方を使用できるように 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。
- Device 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。

2.5.1　Device Manager を IPv6 環境に移行するときの設定

IPv4 環境で運用していた Device Manager を IPv6 環境で運用する場合は，`user_httpsd.conf` ファイルを編集します。

メモ

IPv6 環境に Device Manager を新規インストールした場合，インストーラーが自動的に設定を変更するため，この作業は不要です。

操作手順

1. HA Command Suite 製品のサービスを停止します。
2. `user_httpsd.conf` ファイルを開きます。

   `user_httpsd.conf` ファイルの格納先を次に示します。

   < *HA Command Suite のインストールフォルダ* >\Base64\uCPSB11\httpsd\conf\user_httpsd.conf

   メモ

   `user_httpsd.conf` ファイルと同じ場所に格納されている `httpsd.conf` ファイルは編集しないでください。

3. 「`#Listen [::]:`< *ポート番号* >」の先頭にある番号記号（`#`）を削除して，IPv6 での通信を有効にします。

   注意

   - 非 SSL 通信の場合，`SSLEngine off` の下にある `Listen` 行の番号記号（`#`）を削除する必要はありません。
   - デフォルトでは，すべての IPv6 アドレスと通信できるように設定されています。
   - ポート番号は IPv4 の `Listen` 行と同じ番号を指定してください。
   - IPv4 の `Listen` 行を削除したり編集したりしないでください。誤って削除，編集した場合，IPv4 での通信ができなくなります。

4. HA Command Suite 製品のサービスを起動します。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

2.6 管理サーバの IP アドレスまたはホスト名の変更

ネットワーク構成の変更などに伴い，管理サーバの IP アドレスまたはホスト名が変更になった場合は，HA Command Suite 製品の設定も変更する必要があります。

2.6.1 管理サーバのホスト名の変更

変更後のホスト名を HA Command Suite 製品に反映するには，`user_httpsd.conf` ファイル，および `cluster.conf` ファイル（クラスタ構成の場合）を編集したあと，マシンを再起動します。

前提条件

- 次の情報の確認
  - 変更後の管理サーバのホスト名

    ホスト名は 128 バイト以内である必要があります。HA Command Suite 製品では，大文字と小文字は区別されます。

    ヒント

    事前に管理サーバのホスト名を変更した場合，`hostname` コマンドで表示させた変更後のホスト名を控えておいてください。Windows の場合は `ipconfig /ALL` コマンドでも表示できます。

操作手順

1. HA Command Suite 製品のサービスを停止します。
2. 次のコンポーネント間の通信に SSL/TLS を使用している場合は，変更後のホスト名を使用して，管理サーバのサーバ証明書を作成し直します。
   - 管理サーバと管理クライアント（GUI）間
   - 管理サーバとストレージシステム（iStorage V シリーズ）間
3. 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。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\uCPSB11\httpsd\conf\user_httpsd.conf`

   管理サーバと管理クライアントとの通信に TLS/SSL を使用している場合は，さらに次の設定も変更してください。
   - `<VirtualHost>`タグにホスト名が指定されている場合は，アスタリスク（`*`）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。

   メモ

   `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。
4. `cluster.conf` ファイルを編集します（クラスタ構成の場合だけ）。

   論理ホスト名，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。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\conf\cluster.conf`
5. 管理サーバのホスト名を変更し，マシンを再起動します。

HA 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は，ここではマシンの再起動だけを実行してください。

6. HA Command Suite 製品のサービスが起動していることを確認します。
7. HA Command Suite 製品の URL にホスト名を使用している場合は，管理サーバにインストールされている HA Command Suite 製品の設定を変更します。
8. 運用環境によって，HA Command Suite 製品の設定を見直します。
9. データベースをバックアップします。

   ホスト名を変更するとバックアップしたデータベースは使用できなくなります。

関連リンク

管理サーバの IP アドレスまたはホスト名の変更後に必要な作業（22 ページ）
HA Command Suite 製品の URL の変更（hcmds64chgurl コマンド）（23 ページ）
Device Manager のサービスの停止（134 ページ）
Device Manager のサービスの稼働状態の確認（135 ページ）
データベースのバックアップ（137 ページ）

2.6.2 管理サーバの IP アドレスの変更

変更後の IP アドレスを HA Command Suite 製品に反映するには，`user_httpsd.conf` ファイルを編集したあと，マシンを再起動します。

前提条件

次の情報の確認

- 変更後の管理サーバの IP アドレス

注意

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。

操作手順

1. HA 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。

   `ServerName` ディレクティブに変更前の IP アドレスが指定されている場合は，ホスト名または変更後の IP アドレスに変更します。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\uCPSB11\httpsd\conf\user_httpsd.conf`

メモ

- `httpsd.conf` ファイルは編集しないでください。
- `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。

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。

   HA 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いた場合は，ここではマシンの再起動だけを実行してください。

4. HA Command Suite 製品のサービスが起動していることを確認します。

5. HA Command Suite 製品の URL に IP アドレスを使用している場合は，管理サーバにインストールされている HA Command Suite 製品の設定を変更します。

6. 運用環境によって，HA Command Suite 製品の設定を見直します。

7. データベースをバックアップします。

   IP アドレスを変更するとバックアップしたデータベースは使用できなくなります。

関連リンク

管理サーバの IP アドレスまたはホスト名の変更後に必要な作業（22 ページ）
HA Command Suite 製品の URL の変更（hcmds64chgurl コマンド）（23 ページ）
Device Manager のサービスの停止（134 ページ）
Device Manager のサービスの稼働状態の確認（135 ページ）
データベースのバックアップ（137 ページ）

2.6.3　管理サーバの IP アドレスまたはホスト名の変更後に必要な作業

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，運用環境によっては Device Manager の設定を見直す必要があります。

- `server.http.host` プロパティに変更前のホスト名または IP アドレスを設定している場合

  変更後のホスト名または IP アドレスに設定し直したあと，HA Command Suite 製品のサービスを再起動する必要があります。

- 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。

- iStorage V シリーズを操作する場合

  Device Manager に同梱されたデフォルトの証明書以外を使用して Device Manager とストレージシステム間でセキュリティ通信をしているときは，Device Manager GUI の[ストレージシステム編集]画面で，ユーザーアカウント認証を設定し直してください。

そのほかに IP アドレスやホスト名が設定されているスクリプトファイルやバッチファイルなどがあれば設定を見直してください。

関連リンク

外部認証サーバと外部認可サーバの登録（40 ページ）
Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
server.http.host（179 ページ）

2.7　HA Command Suite 製品の URL の変更（hcmds64chgurl コマンド）

GUI に登録されている HA Command Suite 製品の URL を `hcmds64chgurl` コマンドで変更します。

次の構成変更に伴い，運用開始後に HA Command Suite 製品の URL が変更になった場合には，GUI に登録されている HA Command Suite 製品の URL も `hcmds64chgurl` コマンドで変更する必要があります。

- HBase 64 Storage Mgmt Web Service が使用するポートの変更
- 管理サーバのホスト名または IP アドレスの変更
- SSL を使用するため，または SSL の使用を中止するための設定変更
- クラスタ環境への移行

操作手順

1. `hcmds64chgurl` コマンドを実行します。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\bin\hcmds64chgurl {/print | /list | /change` ＜*変更前の URL* ＞＜*変更後の URL* ＞ `| /change` ＜*変更後の URL* ＞ `/type` ＜ *HA Command Suite 製品の名称*＞`}`

   - `print`

     現在登録されている URL とプログラムのリストを表示する場合に指定します。

   - `list`

     `print` オプションと同じ内容を異なるフォーマットで表示する場合に指定します。

   - `change`

     URL を変更する場合に指定します。

- `type`

  `DeviceManager` と指定します。

注意

- 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。以下にその例を示します。

  `http://hostname:22015`

- クラスタ環境への移行に伴い URL を変更する場合は，＜*変更後の URL* ＞は次の形式で指定してください。

  `http://`＜*論理ホスト名*＞`:`＜*ポート番号*＞

関連リンク

HA Command Suite 共通コンポーネントで使用されるポートの変更（10 ページ）
管理サーバのホスト名の変更（19 ページ）
管理サーバの IP アドレスの変更（21 ページ）
管理サーバと管理クライアント（GUI）間のセキュリティ通信のための操作フロー（75 ページ）

第 3 章
ユーザーアカウントを管理するために必要な設定

この章では，HA Command Suite 製品のユーザーアカウントを管理するために必要な設定について説明します。

3.1 パスワードポリシーとは

パスワードポリシーとは，ユーザーアカウントのパスワードに使用できる文字数や，文字種の組み合わせなどに関する条件のことです。

パスワードポリシーを設定することで，推測されやすいパスワードをユーザーが設定することを防ぎ，第三者から不正にアクセスされるリスクを軽減できます。

パスワードポリシーには，次の条件を指定できます。

- パスワードの最小文字数
- パスワードに含める大文字の最小数
- パスワードに含める小文字の最小数
- パスワードに含める数字の最小数
- パスワードに含める記号の最小数
- ユーザー ID と同じパスワードの設定可否

ユーザーアカウントを管理サーバで管理する場合は，これらの条件を設定してパスワードを複雑にすることをお勧めします。

3.1.1 パスワードポリシーの設定

HA Command Suite 製品のパスワードポリシーは，`security.conf` ファイルで設定します。

操作手順

1. `security.conf` ファイルを編集します。

   `security.conf` ファイルの格納先を次に示します。
   ＜*HA Command Suite のインストールフォルダ*＞`\Base64\conf\sec\security.conf`

   `security.conf` ファイルで指定できるパスワードポリシーを次の表に示します。

表 3-1　security.conf ファイルで指定できるパスワードポリシー

項目	説明
password.min.length	パスワードの最小文字数を指定します。指定できる値の範囲は，1～256 です。 デフォルト：4
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。指定できる値の範囲は，0～256 です。0 を指定した場合，大文字の数に制限はなくなります。 デフォルト：0
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。指定できる値の範囲は，0～256 です。0 を指定した場合，小文字の数に制限はなくなります。 デフォルト：0
password.min.numeric	パスワードに含める数字の最小数を指定します。指定できる値の範囲は，0～256 です。0 を指定した場合，数字の数に制限はなくなります。 デフォルト：0
password.min.symbol	パスワードに含める記号の最小数を指定します。指定できる値の範囲は，0～256 です。0 を指定した場合，記号の数に制限はなくなります。 デフォルト：0
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。 デフォルト：false

注意

- 設定したパスワードポリシーは，HA Command Suite 製品で，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，設定した条件をパスワードが満たしていない場合でも，システムにログインできます。
- パスワードポリシーは GUI からも設定できます。ただし，クラスタ構成の環境の場合には，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。
- 外部認証サーバと連携してユーザー認証を行う場合，パスワードの文字種の組み合わせは外部認証サーバでの設定が適用されます。ただし，HA Command Suite 製品にユーザーのパスワードを登録する場合は，HA Command Suite 製品で規定された文字種を使用する必要があります。

操作結果

security.conf ファイルの設定値を変更すると，直ちに変更後のパスワードポリシーが有効になります。

3.2 アカウントロックとは

アカウントロックを有効にすることで，第三者による不正アクセスのリスクを軽減できます。ユーザーアカウントを管理サーバで管理する場合は，アカウントロックを有効にすることをお勧めします。

HA Command Suite 製品では，ユーザーが複数回連続して GUI へのログインに失敗した場合に，ユーザーアカウントを自動的にロックできます。

アカウントロックを有効にするには，アカウントロックポリシー（アカウントをロックするログイン連続失敗回数）を設定する必要があります。

ヒント

GUI では，アカウントロックの方法として，任意のユーザーアカウントのロック状態を変更することもできます。

なお，ロック状態の変更は，User Management の Admin 権限を持つユーザーだけが操作できます。

注意

- System アカウントは，HA Command Suite 製品の初期導入時にはアカウントロックの対象になっていません。System アカウントには HA Command Suite 製品の Admin 権限が設定されています。セキュリティを強化するために System アカウントもロックの対象にする場合は，設定を変更する必要があります。
- 外部認証サーバと連携してユーザー認証を行う場合，自動ロックの制御は，外部認証サーバでの設定が適用されます。

3.2.1 アカウントロックポリシーとは

アカウントロックポリシーとは，ユーザーが複数回連続して GUI へのログインに失敗した場合に，そのユーザーアカウントを自動的にロックするログイン連続失敗回数のことです。

3.2.2 アカウントロックポリシーの設定

HA Command Suite 製品のアカウントロックポリシーは，security.conf ファイルで設定します。

操作手順

1. security.conf ファイルを編集します。

   security.conf ファイルの格納先を次に示します。
   ＜*HA Command Suite のインストールフォルダ*＞\Base64\conf\sec\security.conf

   security.conf ファイルで指定できるアカウントロックポリシーを次の表に示します。

表 3-2　security.conf ファイルで指定できるアカウントロックポリシー

項目	説明
account.lock.num	自動的にアカウントをロックするまでのログイン連続失敗回数を指定します。指定できる値の範囲は，0～10 です。 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。 デフォルト：0

⚠ 注意

- ログイン連続失敗回数を変更した場合，その値は，変更後にログインに失敗したときから適用されます。ログイン中のユーザーがいるときに，再度そのユーザーでログインを試行し，失敗回数が指定値に達すると，そのユーザーアカウントはロックされます。ただし，すでにログインしているユーザーは操作を継続できます。
- アカウントロックポリシーは GUI からも設定できます。ただし，クラスタ構成の環境の場合には，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。

操作結果

security.conf ファイルの設定値を変更すると，直ちに変更後のアカウントロックポリシーが有効になります。

3.2.3 System アカウントのロックに関する設定

System アカウントもアカウントロックの対象にする場合は，user.conf ファイルで設定します。

操作手順

1. HA Command Suite 製品のサービスを停止します。
2. user.conf ファイルを開きます。

user.conf ファイルの格納先を次に示します。
< HA Command Suite のインストールフォルダ>\Base64\conf\user.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。

3. 次の形式で account.lock.system プロパティを指定します。

```
account.lock.system=true
```

4. HA Command Suite 製品のサービスを起動します。

操作結果

HA Command Suite 製品で，System アカウントがアカウントロックの対象になります。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

3.2.4 アカウントロックの解除

ロックされたユーザーアカウントは，hcmds64unlockaccount コマンドで解除できます。

前提条件

- Administrator 権限でのログイン
- ロックされたユーザーアカウントに User Management の Admin 権限があることの確認

  User Management の Admin 権限がないユーザーアカウントの場合は，User Management の Admin 権限を持つほかのユーザーにアカウントロックの解除を依頼してください。
- 次の情報の確認
  - ロックされたユーザーアカウントのユーザー ID とパスワード

操作手順

1. hcmds64unlockaccount コマンドを実行して，ロックを解除します。

   < HA Command Suite のインストールフォルダ>\Base64\bin\hcmds64unlockaccount [/user *<ユーザー ID>* /pass *<パスワード>*]

   user オプションおよび pass オプションを省略してコマンドを実行すると，対話形式でユーザー ID およびパスワードを入力できます。

注意

ユーザー ID またはパスワードに記号が含まれる場合は，コマンドライン上でエスケープする必要があります。

円記号（\）が末尾にある場合は，末尾の円記号（\）を円記号（\）でエスケープしてください。

また，アンパサンド（&），縦線（|）またはアクサンシルコンフレックス（^）が含まれる場合は，記号 1 文字ごとに引用符（"）で囲むか，アクサンシルコンフレックス（^）でエスケープしてください。

第 4 章
外部認証サーバでのユーザー管理

この章では，外部認証サーバでユーザー認証する方法について説明します。

4.1　外部認証サーバとの連携とは

HA Command Suite 製品では，外部認証サーバに登録されているユーザーアカウントを使って，GUI にログインしたりできます。

外部認証サーバと連携すると，HA 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。

HA Command Suite 製品では，次の外部認証サーバとの連携をサポートしています。

- LDAP ディレクトリサーバ
- RADIUS サーバ
- Kerberos サーバ

4.2　外部認可サーバとの連携とは

外部認証サーバでユーザー認証を行う場合には，外部認可サーバも併用することで，管理サーバ（HA Command Suite 製品）に対するアクセス可否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，HA 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，HA 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。

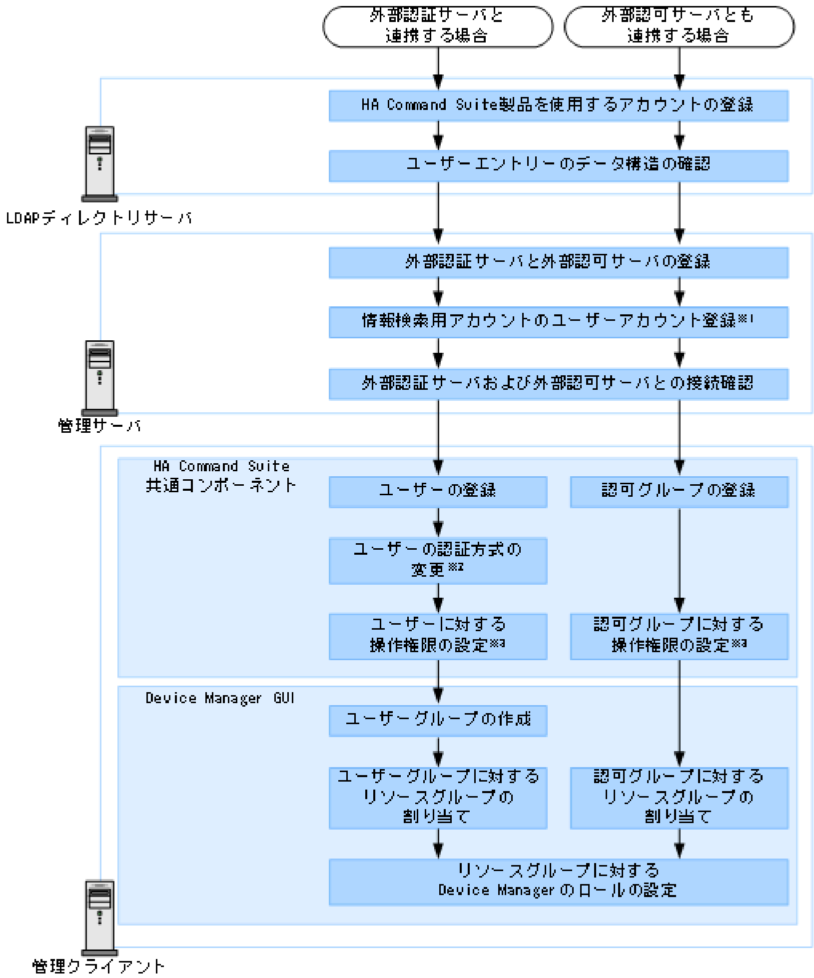
HA Command Suite 製品では，LDAP ディレクトリサーバ（Active Directory）との連携をサポートしています。

4.3　外部認証サーバでユーザー認証するための操作フロー

外部認証サーバで一元管理されているユーザーアカウントを使って，HA Command Suite 製品の GUI を使用できるようにするためには，外部認証サーバ，管理サーバおよび管理クライアントで環境設定が必要です。

4.3.1　LDAP ディレクトリサーバでユーザー認証するための操作フロー

LDAP ディレクトリサーバでユーザー認証するためには，HA Command Suite 製品で，管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。



注※1 外部認証サーバとだけ連携する場合，ユーザーエントリーのデータ構造がフラットモデルのときは，不要な操作です。
注※2 既存のユーザーの認証方式を変更する場合に必要な操作です。
注※3 ユーザーの作業範囲に応じて操作権限を設定します。
- ユーザー管理（User Management）

図 4-1　LDAP ディレクトリサーバでユーザー認証するための操作フロー

メモ

- HA Command Suite 製品の運用開始後に，外部認可サーバと連携したシステム構成に切り替える場合は，HA Command Suite 共通コンポーネントに登録されている同名のユーザー ID は削除するか，変更してください。ユーザー ID にドメイン名が含まれている場合（例：user1@example.com）も同様に，同名のユーザー ID を削除するか，変更してください。同名のユーザー ID が登録されている場合，そのユーザーが HA Command Suite 製品にログインした際には，HA Command Suite 共通コンポーネントでの認証（内部認証）となります。
- 登録した認可グループのネストグループに属するユーザーも，認可グループに設定されたロール（権限）で HA Command Suite 製品を操作できるようになります。

- LDAP ディレクトリサーバと管理サーバとの通信に StartTLS を使用する場合は，セキュリティ通信のための環境設定が別途必要です。
- 管理クライアントでの作業については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

関連リンク

HA Command Suite 製品のアカウントの条件（36 ページ）
ユーザーエントリーのデータ構造とは（37 ページ）
外部認証サーバと外部認可サーバの登録（40 ページ）
情報検索用のユーザーアカウントとは（63 ページ）
外部認証サーバおよび外部認可サーバとの接続確認（69 ページ）
Device Manager のセキュリティ通信路（73 ページ）

4.3.2 RADIUS サーバでユーザー認証するための操作フロー

RADIUS サーバでユーザー認証するためには，HA Command Suite 製品で，管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。

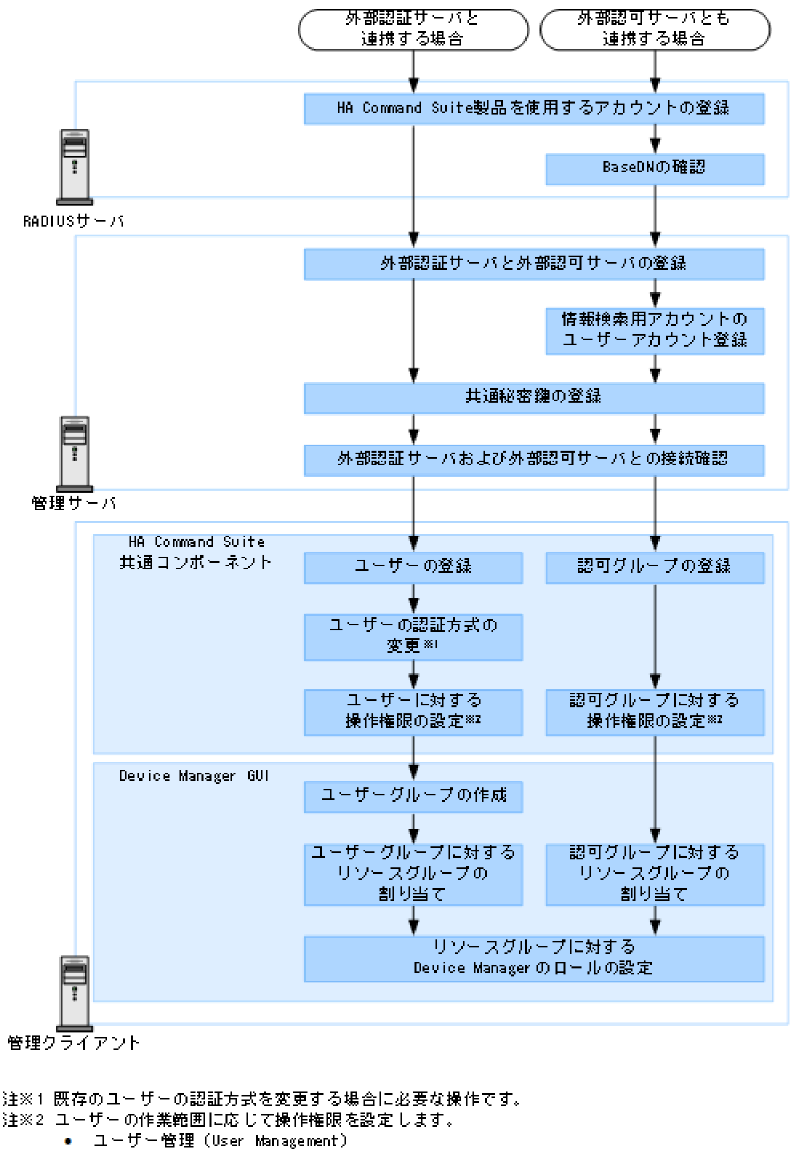


図 4-2　RADIUS サーバでユーザー認証するための操作フロー

メモ

- HA Command Suite 製品の運用開始後に，外部認可サーバと連携したシステム構成に切り替える場合は，HA Command Suite 共通コンポーネントに登録されている同名のユーザー ID は削除するか，変更してください。同名のユーザー ID が登録されている場合，そのユーザーが HA Command Suite 製品にログインした際には, HA Command Suite 共通コンポーネントでの認証（内部認証）となります。
- 登録した認可グループのネストグループに属するユーザーも，認可グループに設定されたロール（権限）で HA Command Suite 製品を操作できるようになります。
- LDAP ディレクトリサーバと管理サーバとの通信に StartTLS を使用する場合は，セキュリティ通信のための環境設定が別途必要です。
- 管理クライアントでの作業については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

関連リンク

HA Command Suite 製品のアカウントの条件（36 ページ）
ユーザーエントリーのデータ構造とは（37 ページ）
外部認証サーバと外部認可サーバの登録（40 ページ）
情報検索用のユーザーアカウントとは（63 ページ）
共有秘密鍵の登録（68 ページ）
外部認証サーバおよび外部認可サーバとの接続確認（69 ページ）
Device Manager のセキュリティ通信路（73 ページ）

4.3.3 Kerberos サーバでユーザー認証するための操作フロー

Kerberos サーバでユーザー認証するためには，HA Command Suite 製品で，管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。

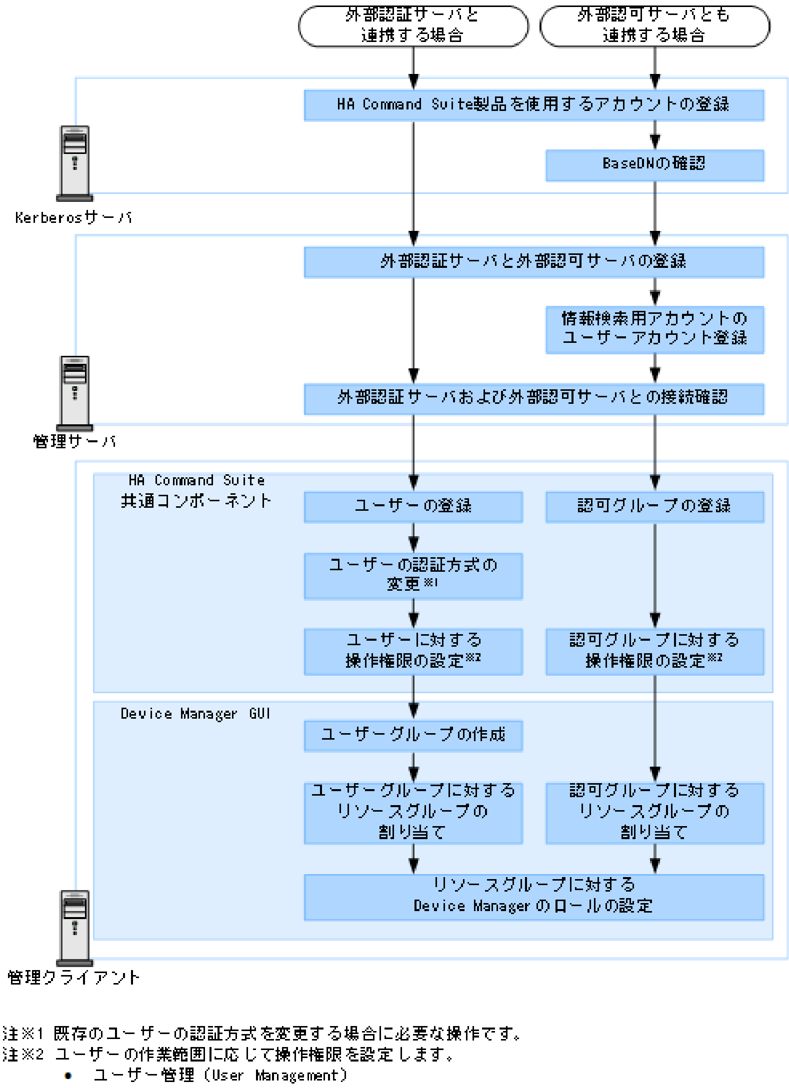


図 4-3　Kerberos サーバでユーザー認証するための操作フロー

メモ

- HA Command Suite 製品の運用開始後に，外部認可サーバと連携したシステム構成に切り替える場合は，HA Command Suite 共通コンポーネントに登録されている同名のユーザー ID は削除するか，変更してください。ユーザー ID にレルム名が含まれている場合（例：user1@EXAMPLE.COM）も同様に，同名のユーザー ID を削除するか，変更してください。同名のユーザー ID が登録されている場合，そのユーザーが HA Command Suite 製品にログインした際には，HA Command Suite 共通コンポーネントでの認証（内部認証）となります。
- 登録した認可グループのネストグループに属するユーザーも，認可グループに設定されたロール（権限）で HA Command Suite 製品を操作できるようになります。
- LDAP ディレクトリサーバと管理サーバとの通信に StartTLS を使用する場合は，セキュリティ通信のための環境設定が別途必要です。
- 管理クライアントでの作業については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

関連リンク

HA Command Suite 製品のアカウントの条件（36 ページ）
ユーザーエントリーのデータ構造とは（37 ページ）
外部認証サーバと外部認可サーバの登録（40 ページ）
情報検索用のユーザーアカウントとは（63 ページ）
外部認証サーバおよび外部認可サーバとの接続確認（69 ページ）
Device Manager のセキュリティ通信路（73 ページ）

4.4 HA Command Suite 製品のアカウントの条件

HA Command Suite 製品を使用するユーザーのアカウント（ユーザー ID およびパスワード）は，外部認証サーバと HA Command Suite 製品の両方で使用できる文字で構成されている必要があります。

次の条件をすべて満たすように，ユーザーアカウントを設定してください。

- 256 バイト以内であること。
- 次の文字を使用していること。

  `A～Z a～z 0～9 ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

HA 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。

4.5 ユーザーエントリーのデータ構造とは

LDAP ディレクトリサーバのユーザーエントリーのデータ構造には階層構造モデルとフラットモデルがあります。

LDAP ディレクトリサーバでユーザー認証を行う場合，管理サーバに登録する LDAP ディレクトリサーバの情報や管理サーバで必要な作業がデータ構造によって異なるため，ユーザーエントリーがどちらに該当しているかを確認してください。

また，LDAP ディレクトリサーバでユーザー認証・認可する場合には，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。

4.5.1 BaseDN とは

認証および認可の際にユーザーを検索する起点となるエントリーを BaseDN といいます。

BaseDN より下の階層のユーザーエントリーが認証・認可の対象となります。HA Command Suite 製品で認証・認可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。BaseDN は，管理サーバに LDAP ディレクトリサーバの情報を登録する際に必要になります。

4.5.2 階層構造モデルとは

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。

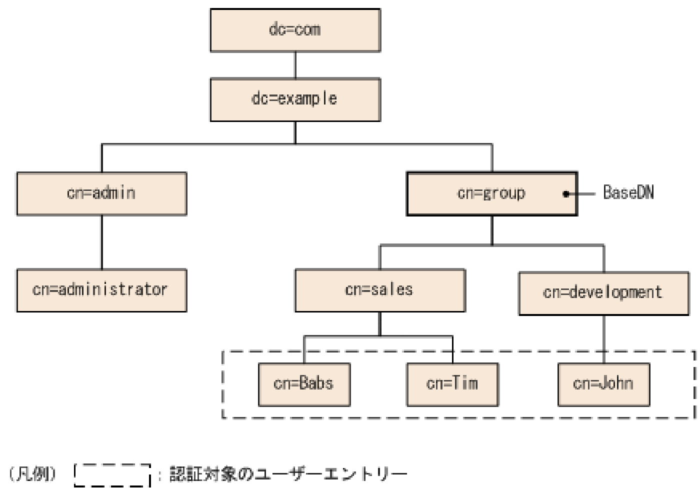


図 4-4　階層構造モデルの例

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。

4.5.3　フラットモデルとは

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。

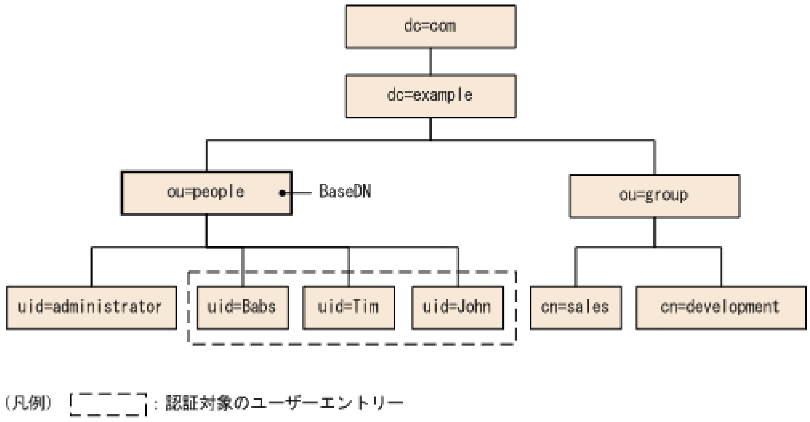


図 4-5　フラットモデルの例

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。

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。

- HA 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，HA 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 HA Command Suite 製品のユーザー ID として使用します。そのため，HA 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）

4.6　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。

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 4-1　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	Y※1	Y※1
RADIUS サーバ	Y	-
Kerberos サーバ	Y	Y※2

（凡例）

Y：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。

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，ログイン時に入力したユーザー 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。

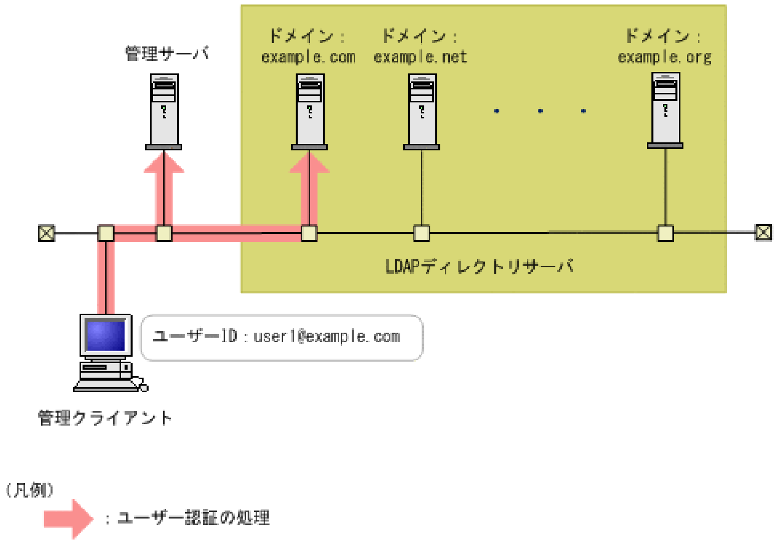


図 4-6　マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいるユーザー ID の場合）

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ユーザー認証ができるまで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掛かるため，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。

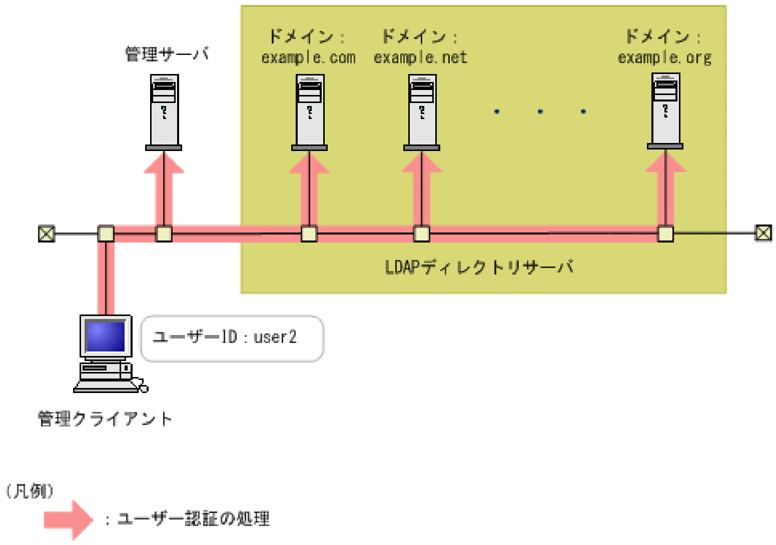


図 4-7　マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいないユーザー ID の場合）

4.7　外部認証サーバと外部認可サーバの登録

exauth.properties ファイルに，使用する外部認証サーバの種類やサーバ識別名，外部認証サーバと外部認可サーバのマシン情報などを設定します。

前提条件

- Administrator 権限でのログイン
- `exauth.properties` ファイルのひな形のコピー
  ＜*HA Command Suite のインストールフォルダ*＞`\Base64\sample\conf\exauth.properties`
- ユーザーエントリーのデータ構造の確認（認証方式が LDAP の場合）
- LDAP ディレクトリサーバの OS での DNS サーバの環境設定※
- DNS サーバの SRV レコードへの LDAP ディレクトリサーバ情報の登録※
- 次の情報の確認
  - 共通

    ・外部認証サーバの種類
  - 認証方式が LDAP の場合

    ・外部認証サーバおよび外部認可サーバのマシン情報（ホスト名または IP アドレス，ポート番号）

    ・BaseDN

    ・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名（外部認可サーバと連携する場合）

    ・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名（マルチドメイン構成の場合）
  - 認証方式が RADIUS の場合

    ・外部認証サーバおよび外部認可サーバのマシン情報（ホスト名または IP アドレス，ポート番号）

    ・認証プロトコル

    ・管理サーバのホスト名または IP アドレス

    ・LDAP ディレクトリサーバが管理するドメイン名（外部認可サーバと連携する場合）

    ・BaseDN（外部認可サーバと連携する場合）
  - 認証方式が Kerberos の場合

    ・外部認証サーバおよび外部認可サーバのマシン情報（ホスト名または IP アドレス，ポート番号）

    ・レルム名

    ・LDAP ディレクトリサーバが管理するドメイン名（外部認可サーバと連携する場合）

・BaseDN（外部認可サーバと連携する場合）

注※　LDAP ディレクトリサーバの情報を DNS サーバに照会する場合に必要な作業です。

操作手順

1. コピーした `exauth.properties` ファイルに必要事項を指定します。
2. `exauth.properties` ファイルを次の場所に格納します。

   ＜*HA Command Suite のインストールフォルダ*＞`\Base64\conf\exauth.properties`

3. `auth.ocsp.enable` プロパティと `auth.ocsp.responderURL` プロパティの設定値を変更した場合には，HA Command Suite 製品のサービスを再起動します。

   それ以外のプロパティまたは属性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。

関連リンク

ユーザーエントリーのデータ構造とは（37 ページ）
複数の外部認証サーバと連携している場合の構成（39 ページ）
Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

4.7.1　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

`exauth.properties` ファイルには，使用する外部認証サーバの種類やサーバ識別名，外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ

  表 4-2　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）（43 ページ）

- 外部認証サーバと外部認可サーバのプロパティ

  接続先の LDAP ディレクトリサーバの情報を `exauth.properties` ファイルに直接指定する場合と，DNS サーバに照会する場合とで設定する項目が異なります。

  - LDAP ディレクトリサーバの情報を直接指定する場合

    表 4-3　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）（43 ページ）

    表 4-4　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（外部認証サーバと StartTLS で通信するとき）（46 ページ）

  - LDAP ディレクトリサーバの情報を DNS サーバに照会する場合

表 4-5　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）（46 ページ）

メモ

- プロパティの設定値は，大文字と小文字を区別してください。
- 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。
- 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。

表 4-2　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 4-3　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）（43 ページ）」および「表 4-5　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）（46 ページ）」）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.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 4-3　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。

属性	説明
	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_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY305_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_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
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 HA Command Suite 製品のユーザー ID として使用します。※3 例えば，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の 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。 例えば，ユーザーの DN が uid=John,ou=People,dc=example,dc=com の場合，uid=John の属性名である 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
	• 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。 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 文字ごとに円記号（\）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。 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，HA 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。

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

HA 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 4-4　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（外部認証サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に，OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を，検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に，OCSP レスポンダーの URL を指定します。省略した場合は，AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 4-5　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 HA Command Suite 製品のユーザー ID として使用します。※ 例えば，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の 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。 例えば，ユーザーの DN が uid=John,ou=People,dc=example,dc=com の場合，uid=John の属性名である 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

属性	説明
`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。 • 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。 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 文字ごとに円記号（\）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
`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

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※

HA 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。

4.7.2　LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例

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
```

4.7.3　RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目

exauth.properties ファイルには，使用する外部認証サーバの種類やサーバ識別名，外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ

  表 4-6　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）（51 ページ）

- 外部認証サーバのプロパティ

  RADIUS サーバごとに設定します。

  表 4-7　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）（51 ページ）

- 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。

  接続先の LDAP ディレクトリサーバの情報を直接指定する場合と，DNS サーバに照会する場合とで exauth.properties ファイルに設定する項目が異なります。

  - LDAP ディレクトリサーバの情報を直接指定する場合

    表 4-8　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）（52 ページ）

    表 4-9　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）（53 ページ）

    表 4-10　RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）（54 ページ）

  - LDAP ディレクトリサーバの情報を DNS サーバに照会する場合

    表 4-8　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）（52 ページ）

    表 4-11　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）（55 ページ）

メモ

- プロパティの設定値は，大文字と小文字を区別してください。
- 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。
- 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。

表 4-6　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 4-7　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）（51 ページ））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 4-7　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`	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。

属性	説明
	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	Device 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
`attr.NAS-IP-Address`※2	Device 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	Device 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 アドレスは必ず角括弧（`[ ]`）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 4-8　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）

属性	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を指定します。

属性	説明
	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 4-9　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_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA 指定できる値：ldap または tls デフォルト値：ldap
host※2	外部認証サーバと外部認可サーバが異なるマシンで稼働している場合に，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。 省略した場合は，外部認証サーバと外部認可サーバが同一マシンで稼働しているものと見なされます。 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。

属性	説明
	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，HA 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。

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 4-10　RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）

プロパティ名	説明
`auth.ocsp.enable`	LDAP ディレクトリサーバと StartTLS で通信する場合に，OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は `true` を，検証しない場合は `false` を指定します。 デフォルト値：`false`

プロパティ名	説明
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に，OCSP レスポンダーの URL を指定します。省略した場合は，AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 4-11　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。

4.7.4 RADIUS サーバで認証する場合の exauth.properties ファイルの設定例

RADIUS サーバで認証する場合の exauth.properties ファイルの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
```

4.7.5　Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目

exauth.properties ファイルには，使用する外部認証サーバの種類やサーバ識別名，外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ

  表 4-12　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）（58 ページ）

- 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。

  接続先の Kerberos サーバの情報を直接指定する場合と，DNS サーバに照会する場合とで exauth.properties ファイルに設定する項目が異なります。

  - Kerberos サーバの情報を直接指定する場合

    表 4-13　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）（58 ページ）

  - Kerberos サーバの情報を DNS サーバに照会する場合

    表 4-14　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）（60 ページ）

- 外部認可サーバのプロパティ

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。

表 4-15 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）（60 ページ）

表 4-16 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）（62 ページ）

メモ

- プロパティの設定値は，大文字と小文字を区別してください。
- 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。
- 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。

表 4-12 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 4-13 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。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`
`default_tkt_enctypes`	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは，管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc 複数指定する場合は，コンマ（,）で区切ってください。 指定した暗号タイプのうち，管理サーバの OS と Kerberos サーバの両方でサポートされているものが使用されます。

属性	説明
	デフォルト：なし（DES-CBC-MD5 での認証）
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
＜ *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ポート番号である場合は，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＞*

注※

外部認可サーバの接続プロトコルに StartTLS を使用する場合は，外部認可サーバのサーバ証明書の 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 4-14　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。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`
`default_tkt_enctypes`	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは，管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc 複数指定する場合は，コンマ（`,`）で区切ってください。 指定した暗号タイプのうち，管理サーバの OS と Kerberos サーバの両方でサポートされているものが使用されます。 デフォルト：なし（DES-CBC-MD5 での認証）
`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 4-15　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。

属性	説明
	• TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA 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，HA 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。

表 4-16　Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に，OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を，検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に，OCSP レスポンダーの URL を指定します。省略した場合は，AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

4.7.6　Kerberos サーバで認証する場合の exauth.properties ファイルの設定例

Kerberos サーバで認証する場合の exauth.properties ファイルの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
```

4.8　情報検索用のユーザーアカウントとは

情報検索用のユーザーアカウントとは，認証・認可対象のアカウントが存在するか LDAP ディレクトリサーバ内の情報を検索する際に使用されるユーザーアカウントです。

次の運用を行う場合には，管理サーバに情報検索用のユーザーアカウントを登録しておく必要があります。

- LDAP ディレクトリサーバを外部認証サーバとして利用し，データ構造が階層モデルの場合
- 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※

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。

注※

GUI で認可グループを HA 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 HA 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。

4.8.1 情報検索用のユーザーアカウントの条件

情報検索用のユーザーアカウントの条件は，認証方式によって異なります。

次の条件を満たすユーザーアカウントを LDAP ディレクトリサーバに準備してください。

認証方式が LDAP の場合

- `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
- `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 下にある認可グループを参照できること（外部認可サーバとも連携するとき）
- `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 下にある認可グループの属性と，認可グループのネストグループの属性を検索できること（外部認可サーバとも連携するとき）

認証方式が RADIUS の場合

- `exauth.properties` ファイルの `auth.group.`＜ *ドメイン名*＞`.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.group.`＜ *ドメイン名*＞`.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.group.`＜ *ドメイン名*＞`.basedn` で指定した DN を参照できること

- exauth.properties ファイルの auth.group.< *ドメイン名* >.basedn で指定した DN 下にある認可グループを参照できること
- exauth.properties ファイルの auth.group.< *ドメイン名* >.basedn で指定した DN 下にある認可グループの属性と，認可グループのネストグループの属性を検索できること

認証方式が Kerberos の場合

- exauth.properties ファイルの auth.group.< *レルム名* >.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.group.< *レルム名* >.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.group.< *レルム名* >.basedn で指定した DN を参照できること
- exauth.properties ファイルの auth.group.< *レルム名* >.basedn で指定した DN 下にある認可グループを参照できること
- exauth.properties ファイルの auth.group.< *レルム名* >.basedn で指定した DN 下にある認可グループの属性と，認可グループのネストグループの属性を検索できること

4.8.2　情報検索用のユーザーアカウントの登録

hcmds64ldapuser コマンドを実行して，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。

前提条件

- LDAP ディレクトリサーバへの情報検索用のユーザーアカウントの登録
- 次の情報の確認
  - 情報検索用ユーザーの DN とパスワード
  - LDAP ディレクトリサーバのサーバ識別名または外部認可サーバ用のドメイン名（認証方式が LDAP の場合）

    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。
  - RADIUS サーバのドメイン名（認証方式が RADIUS の場合）

    exauth.properties ファイルの auth.radius.< *auth.server.name に指定した値*> .domain.name に指定したドメイン名を指定します。

- Kerberos サーバのレルム名（認証方式が Kerberos の場合）

  `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。

操作手順

1. `hcmds64ldapuser` コマンドを実行します。

   ＜ *HA Command Suite* ***のインストールフォルダ***＞`\Base64\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` ＜***名前***＞

   - ＜*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。`pass` オプションを省略してコマンドを実行すると，対話形式でパスワードを入力できます。

メモ

- LDAP ディレクトリサーバでは DN やパスワードに引用符（"）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引用符（"）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。
- 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"
  ```

- 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" /p
  ass administrator_pass /name ServerName
  ```

関連リンク

外部認証サーバとの連携設定に使用するコマンドに関する注意事項（72 ページ）

4.8.3 情報検索用のユーザーアカウントの削除

`hcmds64ldapuser` コマンドを実行して，情報検索用のユーザーアカウントを管理サーバから削除します。

前提条件

次の情報の確認

- LDAP ディレクトリサーバのサーバ識別名または外部認可サーバ用のドメイン名（認証方式が LDAP の場合）
- RADIUS サーバのドメイン名（認証方式が RADIUS の場合）
- Kerberos サーバのレルム名（認証方式が Kerberos の場合）

操作手順

1. `hcmds64ldapuser` コマンドを実行します。

   <*HA Command Suite のインストールフォルダ*>`\Base64\bin\hcmds64ldapuser /delete /name` <*名前*>

関連リンク

外部認証サーバとの連携設定に使用するコマンドに関する注意事項（72 ページ）

4.8.4 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の確認

`hcmds64ldapuser` コマンドを実行して，情報検索用ユーザーアカウントを管理サーバに登録済みの LDAP ディレクトリサーバを確認します。

操作手順

1. `hcmds64ldapuser` コマンドを実行します。

   <*HA Command Suite のインストールフォルダ*>`\Base64\bin\hcmds64ldapuser /list`

4.9　共有秘密鍵の登録

hcmds64radiussecret コマンドを実行して，RADIUS サーバの共有秘密鍵（shared secret）を 管理サーバに登録します。

前提条件

次の情報の確認

- 共有秘密鍵
- RADIUS サーバのサーバ識別名

  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。

操作手順

1. hcmds64radiussecret コマンドを実行します。

   ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64radiussecret [/set ＜*共有秘密鍵*＞] /name ＜ *RADIUS サーバのサーバ識別名*＞

   - set オプションを省略してコマンドを実行すると，対話形式で共有秘密鍵を入力できます。

関連リンク

外部認証サーバとの連携設定に使用するコマンドに関する注意事項（72 ページ）

4.9.1　共有秘密鍵の削除

hcmds64radiussecret コマンドを実行して，共有秘密鍵（shared secret）を削除します。

前提条件

次の情報の確認

- RADIUS サーバのサーバ識別名

操作手順

1. hcmds64radiussecret コマンドを実行します。

   ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64radiussecret /delete /name ＜ *RADIUS サーバのサーバ識別名*＞

関連リンク

外部認証サーバとの連携設定に使用するコマンドに関する注意事項（72 ページ）

4.9.2　共有秘密鍵が登録されている RADIUS サーバの確認

`hcmds64radiussecret` コマンドを実行して，共有秘密鍵（shared secret）を管理サーバに登録済みの RADIUS サーバを確認します。

操作手順

1. `hcmds64radiussecret` コマンドを実行します。

   < *HA Command Suite のインストールフォルダ*>`\Base64\bin\hcmds64radiussecret /list`

操作結果

RADIUS サーバのサーバ識別名が表示されます。

関連リンク

外部認証サーバとの連携設定に使用するコマンドに関する注意事項（72 ページ）

4.10　外部認証サーバおよび外部認可サーバとの接続確認

`hcmds64checkauth` コマンドを実行して，管理サーバから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。

前提条件

- 外部認証サーバと外部認可サーバの登録
- 次の情報の確認
  - 認証方式が LDAP の場合

    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を確認してください。ユーザー ID 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。
  - 認証方式が RADIUS の場合

RADIUS サーバに登録されているユーザーアカウントを確認してください。

- 認証方式が Kerberos の場合

外部認証サーバとだけ連携する場合：

HA 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確認してください。

外部認可サーバとも連携する場合：

HA Command Suite 製品に登録されていないユーザーアカウントを確認してください。

なお，`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。

なお，ユーザー ID または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使用できません。

操作手順

1. `hcmds64checkauth` コマンドを実行します。

＜HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64checkauth [/user` *＜ユーザー ID＞* `/pass` *＜パスワード＞*`] [/summary]`

- `user` オプションおよび `pass` オプションを省略してコマンドを実行すると，対話形式でユーザー ID およびパスワードを入力できます。
- `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。

メモ

- 認証方式が Kerberos の場合，`exauth.properties` ファイルでレルム名を複数指定したときは，レルムごとに接続確認してください。また，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。

- 認証方式が LDAP で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。

操作結果

`exauth.properties` ファイルの設定や，外部認証サーバおよび外部認可サーバとの接続状況がチェックされ，結果がフェーズごとに表示されます（全 4 フェーズ）。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 ＜phase-number＞
 was normal.
```

フェーズ 1

`exauth.properties` ファイルの共通のプロパティ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。

エラーが発生した場合は，マニュアル『HA Command Suite メッセージ』で出力されたメッセージ ID を検索し，要因や対処方法を確認してください。

関連リンク

外部認証サーバと外部認可サーバの登録（40 ページ）
外部認証サーバとの連携設定に使用するコマンドに関する注意事項（72 ページ）

4.11　外部認証サーバとの連携設定に使用するコマンドに関する注意事項

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，円記号（\）はコマンドラインでは特殊な扱いとなるため，引数に円記号（\）が含まれる場合には注意が必要です。

hcmds64ldapuser コマンド，hcmds64radiussecret コマンド，および hcmds64checkauth コマンドを実行する際のエスケープ方法は次のとおりです。

次の文字が含まれる場合は，引数を引用符（"）で囲むか，1 文字ごとにアクサンシルコンフレックス（^）でエスケープしてください。

空白文字 & | ^ < > ( )

円記号（\）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，引数に円記号（\）と上記の文字が含まれる場合には，引用符（"）で囲まないで，上記文字を 1 文字ごとにアクサンシルコンフレックス（^）でエスケープしてください。

また，引数の末尾に円記号（\）がある場合は，円記号（\）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
```

4.12　Kerberos 認証に使用できる暗号タイプ

HA Command Suite 製品でサポートされている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。

HA 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。

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

第 5 章
通信に関するセキュリティ設定

この章では，HA Command Suite 製品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　Device Manager のセキュリティ通信路

Device Manager ではマシン間でセキュリティ通信を利用できます。

Device Manager のセキュリティ通信路について，次の 2 つの図に示します。

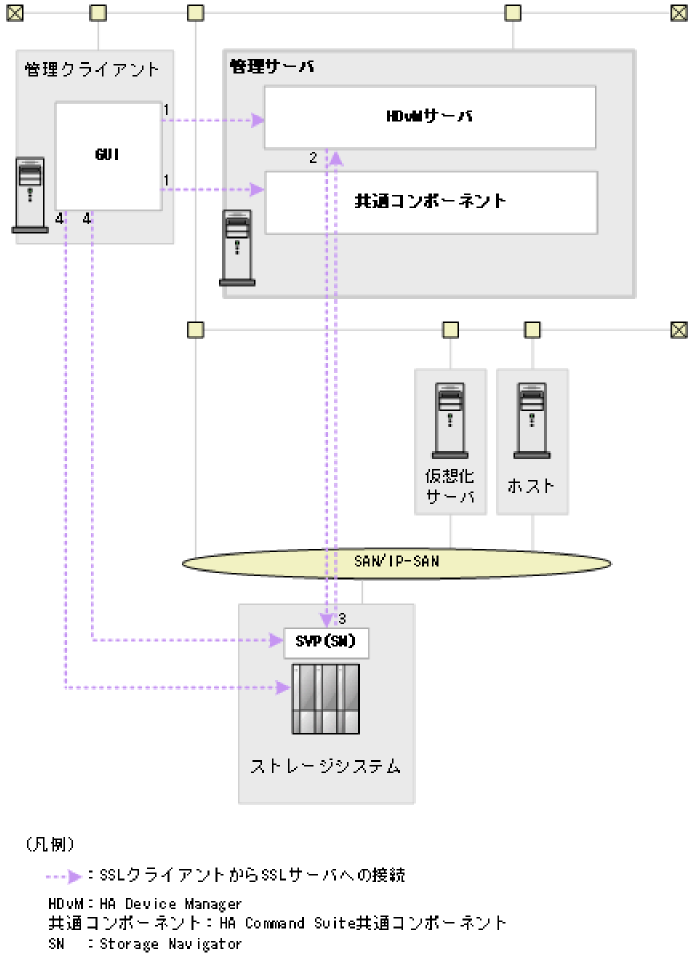


図 5-1　Device Manager のセキュリティ通信路（1/2）

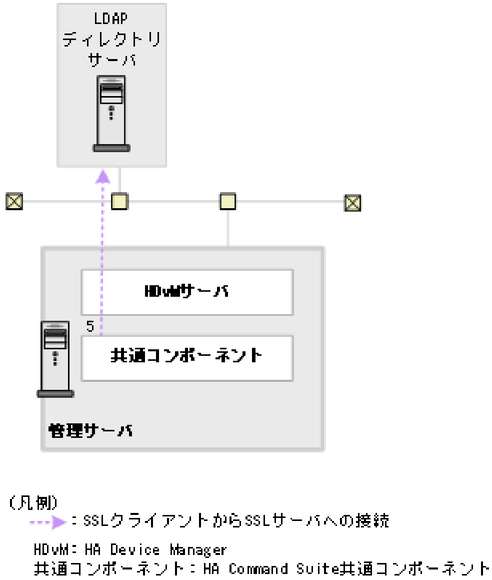


図 5-2　Device Manager のセキュリティ通信路（2/2）

Device Manager で利用できるセキュリティ通信路について，次に示します。表中の項番は，図中の番号と対応しています。

表 5-1　Device Manager で利用できるセキュリティ通信路

項番	SSL サーバ	SSL クライアント	備考
1	管理サーバ • HA Command Suite 共通コンポーネント • Device Manager サーバ	管理クライアント（GUI）	-
2	ストレージシステム • iStorage V シリーズ	管理サーバ（Device Manager サーバ）	iStorage V シリーズとの通信は常にセキュリティ通信が使用されます。 管理サーバ（Device Manager サーバ）は TLS バージョン 1.2 を利用可能です。 セキュリティ通信で使用するプロトコルは，ストレージシステムによって利用できる条件が異なります。詳細は，各ストレージシステムのマニュアルを参照してください。
3	管理サーバ（Device Manager サーバ）	ストレージシステム（iStorage V シリーズ）	Device Manager サーバとストレージシステム（iStorage V シリーズ）間でセキュリティ通信を利用するための設定が必要です。 iStorage V シリーズの場合，デフォルトではセキュリティ通信の設定が有効になります。
4	ストレージシステム	管理クライアント（GUI）	Device Manager GUI から Storage Navigator または Maintenance Utility を使用する場合に，管理クライアントから，SVP またはコントローラーに対するセキュリティ通信を利用できます。 デフォルトではセキュリティ通信の設定が有効になります。

項番	SSL サーバ	SSL クライアント	備考
5	LDAP ディレクトリサーバ	管理サーバ（HA Command Suite 共通コンポーネント）	-

（凡例）

- : 該当なし

5.1.1　Device Manager サーバのデフォルトの証明書

Device Manager を新規インストールした場合，または Device Manager サーバの証明書が存在しない状態でアップグレードインストールをした場合，デフォルトの証明書がキーストアーに登録され，SSL/TLS 通信の設定が有効になります。

デフォルトの証明書は，ストレージシステム（iStorage V シリーズ）と Device Manager の間でユーザーアカウント認証の連携をする際の通信路を暗号化するための自己署名証明書です。HiKeytool を使って証明書の内容を表示し，セキュリティの要件を満たしているか確認してください。よりセキュリティを高めるために別の自己署名証明書または認証局の署名済みの証明書を使用する場合は，デフォルトの証明書を削除して SSL/TLS 通信の設定をやり直してください。

ストレージシステム（iStorage V シリーズ）以外のコンポーネントと Device Manager サーバ間でセキュリティ通信を利用する場合は，デフォルトの証明書を削除して SSL/TLS 通信の設定をやり直してください。

メモ

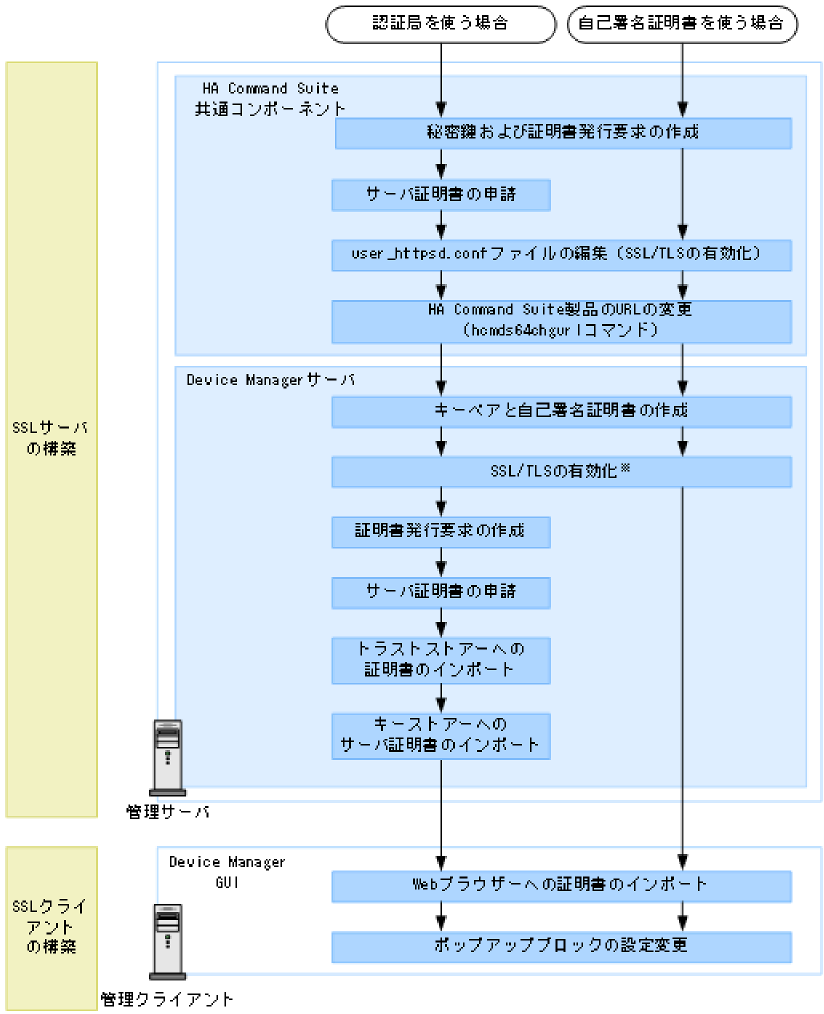
- デフォルトの証明書の内容を確認する，またはキーストアーから削除するには，HiKeytool を使用してください。
- デフォルトの証明書を Device Manager サーバの通信相手のトラストストアーにインポートしないでください。インポートした場合，通信に失敗します。

関連リンク

Device Manager サーバのキーペア情報の参照（詳細モード）（97 ページ）
Device Manager サーバのキーストアーからのキーペアの削除（98 ページ）

5.1.2　管理サーバと管理クライアント（GUI）間のセキュリティ通信のための操作フロー

管理サーバで HA Command Suite 共通コンポーネントと Device Manager サーバのサーバ証明書を作成し，管理クライアント（GUI）の Web ブラウザーにインポートする必要があります。



注※　デフォルトではSSL/TLSが有効に設定されます。

図 5-3　管理サーバと管理クライアント（GUI）間のセキュリティ通信のための操作フロー

メモ

- Web ブラウザーへ証明書をインポートする際に，著名な認証局を使用する場合，証明書が Web ブラウザーにすでにインポートされていることもあります。その場合，証明書を改めてインポートする必要はありません。
- SSL/TLS 通信で使用する暗号方式を制限したい場合は，Device Manager サーバの `server.properties` ファイルにある `server.https.enabledCipherSuites` プロパティの値を変更してください。

関連リンク

HA Command Suite 製品の URL の変更（hcmds64chgurl コマンド）（23 ページ）
SSL サーバの構築（HA Command Suite 共通コンポーネント）（80 ページ）
SSL サーバの構築（Device Manager サーバ）（89 ページ）
SSL クライアントの構築（106 ページ）
Device Manager サーバのプロパティの変更（178 ページ）

server.https.enabledCipherSuites（199 ページ）

5.1.3 LDAP ディレクトリサーバと管理サーバ間のセキュリティ通信のための操作フロー

管理サーバで外部認証サーバと連携するための設定をしたあと，証明書をトラストストアー（ldapcacerts）にインポートする必要があります。

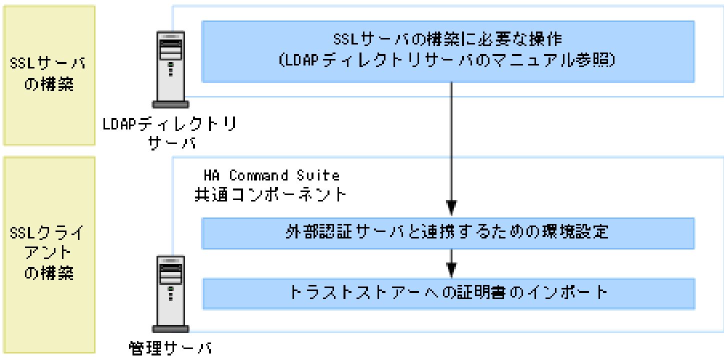


図 5-4 LDAP ディレクトリサーバと管理サーバ間のセキュリティ通信のための操作フロー

なお，LDAP ディレクトリサーバのサーバ証明書が著名な認証局で発行されている場合は，認証局の証明書がトラストストアー（jssecacerts）にすでにインポートされていることがあります。その場合，証明書を改めて ldapcacerts にインポートする必要はありません。

関連リンク

LDAP ディレクトリサーバでユーザー認証するための操作フロー（32 ページ）
SSL クライアントの構築（106 ページ）

5.1.4 管理サーバとストレージシステム（iStorage V シリーズ）間のセキュリティ通信のための操作フロー

iStorage V シリーズは，デフォルトで管理サーバと暗号化通信ができるよう設定されているため，デフォルトのサーバ証明書を使用する場合は，設定は不要です。ストレージシステムを操作する際に発生する通信のセキュリティを高めたい場合，デフォルトの証明書を削除して，Device Manager サーバのサーバ証明書を作成し，SVP にインポートする必要があります。Device Manager サーバのサーバ証明書の作成時に指定したホスト名から，Device Manager サーバの IP アドレスへの名前解決ができるように，SVP で設定をしてください。

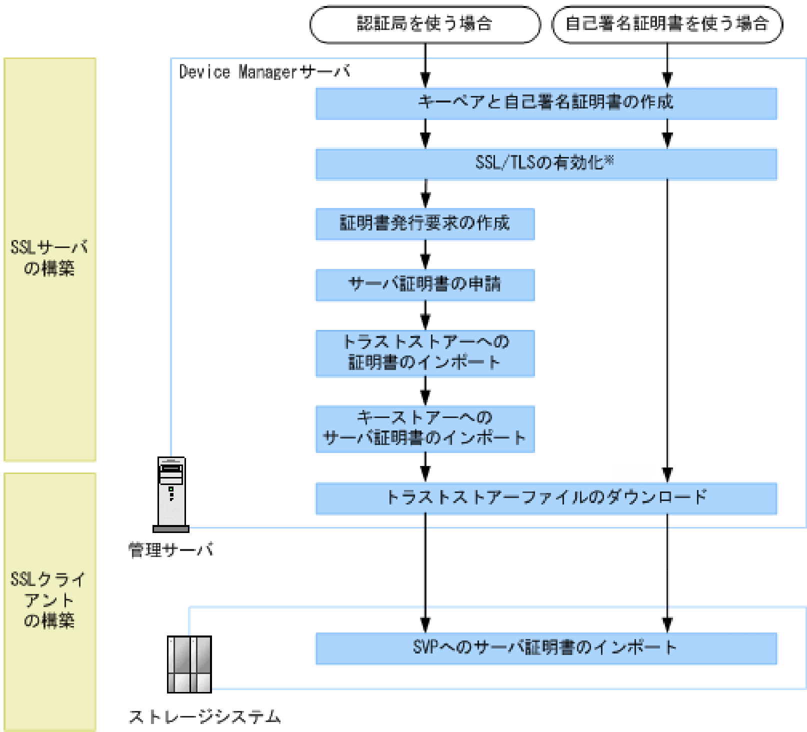


図 5-5　管理サーバとストレージシステム（iStorage V シリーズ）間のセキュリティ通信のための操作フロー

SVP での設定方法については，ストレージシステムのマニュアルを参照してください。

関連リンク

Device Manager サーバのデフォルトの証明書（75 ページ）
SSL サーバの構築（Device Manager サーバ）（89 ページ）
Device Manager サーバのトラストストアーファイルのダウンロード（106 ページ）

5.1.5　ストレージシステムと管理クライアント（GUI）間のセキュリティ通信のための操作フロー

Device Manager GUI から Storage Navigator または Maintenance Utility を使用してストレージシステムを操作する場合， ストレージシステムに格納されているデフォルトのサーバ証明書を使用したセキュリティ通信が利用できます。

iStorage V シリーズを操作する場合は，Device Manager GUI から Storage Navigator または Maintenance Utility を起動すると Web ブラウザーに 証明書の警告メッセージが表示されますが，無視してください。この警告メッセージが表示されても，ストレージシステムと Device Manager GUI 間の通信は暗号化されています。Storage Navigator の起動時に表示される警告メッセージエラーを解消するには，次の操作フローに従ってストレージシステムのサーバ証明書を再作成してください。 サーバ証明書の `Common Name` には，ストレージシス

テムのホスト名を指定してください。このホスト名は，Device Manager GUI で登録する際に指定するストレージシステムのホスト名と一致している必要があります。iStorage V シリーズの場合は，SVP のホスト名を指定してください。

Maintenance Utility の場合，Device Manager GUI で iStorage V シリーズのコントローラーを IP アドレスで登録するため，警告メッセージの表示を解消できません。

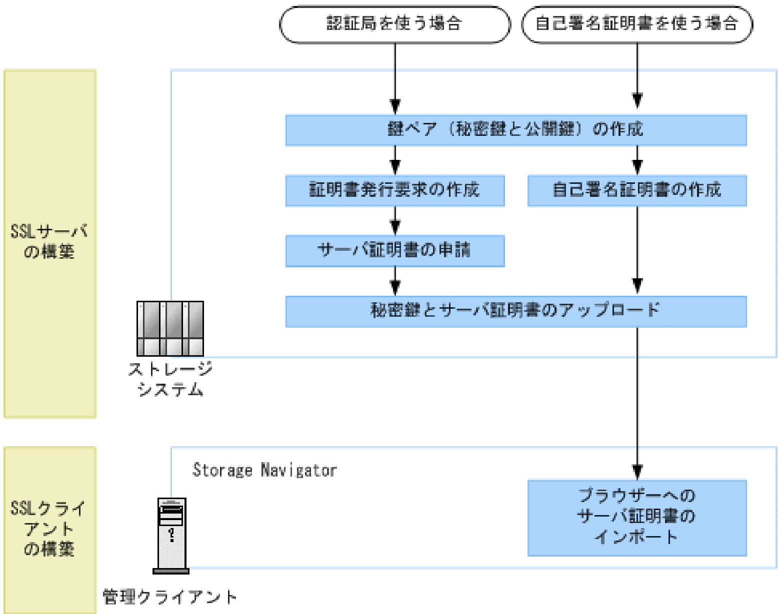


図 5-6　ストレージシステムと管理クライアント（GUI）間のセキュリティ通信のための操作フロー

ヒント

iStorage V シリーズ を操作する場合，よりセキュリティを高めるために，Device Manager GUI から Storage Navigator に送信する情報を簡略化することもできます。

Storage Navigator に送信する情報を簡略化するには，Device Manager サーバの `client.properties` ファイルにある `client.launch.em.secure` プロパティに `true` を指定してください。

サーバ証明書の作成およびインポート方法については，ストレージシステムのマニュアルを参照してください。

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
client.launch.em.secure（195 ページ）

5.1.6　トラストストアー

トラストストアーの格納場所を次に示します。

- `jssecacerts`

  HA Command Suite 共通コンポーネントのトラストストアーです。

＜ HA Command Suite のインストールフォルダ＞\Base64\uCPSB11\jdk\lib\security\jssecacerts

- ldapcacerts

  HA Command Suite 共通コンポーネントのトラストストアーです。LDAP ディレクトリサーバと StartTLS 通信する場合には，ldapcacerts に証明書をインポートします。

  ＜ HA Command Suite のインストールフォルダ＞\Base64\conf\sec\ldapcacerts

- dvmcacerts

  Device Manager サーバのトラストストアーです。

  管理サーバと管理クライアント（GUI）間の通信に使用する Device Manager サーバのサーバ証明書を認証局に申請した場合には，証明書を dvmcacerts にインポートします。

  ＜ HA Command Suite のインストールフォルダ＞\DeviceManager\Server\dvmcacerts

メモ

- トラストストアーファイルは, Device Manager サーバの server.properties ファイルにある server.https.security.truststore プロパティで変更できます。
- 初期パスワードは changeit です。変更する場合は，必ず HiKeytool を使用してください。ほかのツールやコマンドを使って変更した場合，HiKeytool でサーバ証明書のインポートや参照ができなくなります。

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
server.https.security.truststore（199 ページ）

5.2　SSL サーバの構築（HA Command Suite 共通コンポーネント）

HA Command Suite 共通コンポーネントを SSL サーバとして使用するためには，秘密鍵とサーバ証明書を準備し, それぞれの格納場所を user_httpsd.conf ファイルに設定する必要があります。

5.2.1　HA Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成

HA 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。

前提条件

- Administrator 権限でのログイン
- 次の情報の確認
  - 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。

操作手順

1. 次のコマンドを実行します。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\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＞*`] [/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 5-2　DN に指定する属性型および属性値

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（HA 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。
ST	State or Province Name	州名を指定します。
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。`SHA256withRSA` または `SHA1withRSA` 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。

`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。

RSA 暗号用の秘密鍵のキーサイズは 2048 ビット（固定）です。

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。

< HA Command Suite のインストールフォルダ>`\Base64\uCPSB11\httpsd\conf\ssl\server\`

5.2.2　HA 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 HA 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。

前提条件

- HA Command Suite 共通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

    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。

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

認証局からの返答は保存しておいてください。

メモ

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。

関連リンク

証明書の有効期限の確認（HA Command Suite 共通コンポーネント）（87 ページ）

5.2.3　SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集

HA Command Suite 共通コンポーネントの SSL/TLS を有効にする場合は，`user_httpsd.conf` ファイルを編集します。

前提条件

- HA 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）※
- HA 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。
- 次の情報の確認
  - 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）

注※

次の場所にコピーしておくことをお勧めします。

＜ HA Command Suite のインストールフォルダ＞`\Base64\uCPSB11\httpsd\conf\ssl\server`

操作手順

1. HA 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。

   `user_httpsd.conf` ファイルの格納場所

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\uCPSB11\httpsd\conf\user_httpsd.conf`

   `user_httpsd.conf` ファイルの例（デフォルト）

```
ServerName < 管理サーバのホスト名>
Listen 22015                  ――― 非SSL通信用のポート番号
#Listen [::]:22015            ――― 非SSL通信用のポート番号（IPv6環境用）
#Listen 127.0.0.1:22015
SSLEngine Off
#Listen 22016                 ――― SSL通信用のポート番号
#Listen [::]:22016            ――― SSL通信用のポート番号（IPv6環境用）
#<VirtualHost *:22016>        ――― SSL通信用のポート番号
#  ServerName < 管理サーバのホスト名>
#  SSLEngine On
#  SSLProtocol TLSv12
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-
AES256-SHA:ECDHE-ECDSA-AES128-SHA:AES256-SHA256:AES256-SHA:AES128-
SHA256:AES128-SHA:DES-CBC3-SHA
#  SSLRequireSSL
#  SSLCertificateKeyFile "< HA Command Suiteのインストールフォルダ>
/Base64/uCPSB11/httpsd/conf/ssl/server/httpsdkey.pem"
#  SSLCertificateFile "< HA Command Suiteのインストールフォルダ>/Base64/uCPSB11/
httpsd/conf/ssl/server/httpsd.pem"
#  SSLCertificateKeyFile "< HA Command Suiteのインストールフォルダ>/Base64/
uCPSB11/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
#  SSLCertificateFile "< HA Command Suiteのインストールフォルダ>/Base64/uCPSB11/
httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "< HA Command Suiteのインストールフォルダ>
/Base64/uCPSB11/httpsd/conf/ssl/cacert/anycert.pem"
#</VirtualHost>
#HWSLogSSLVerbose On
```

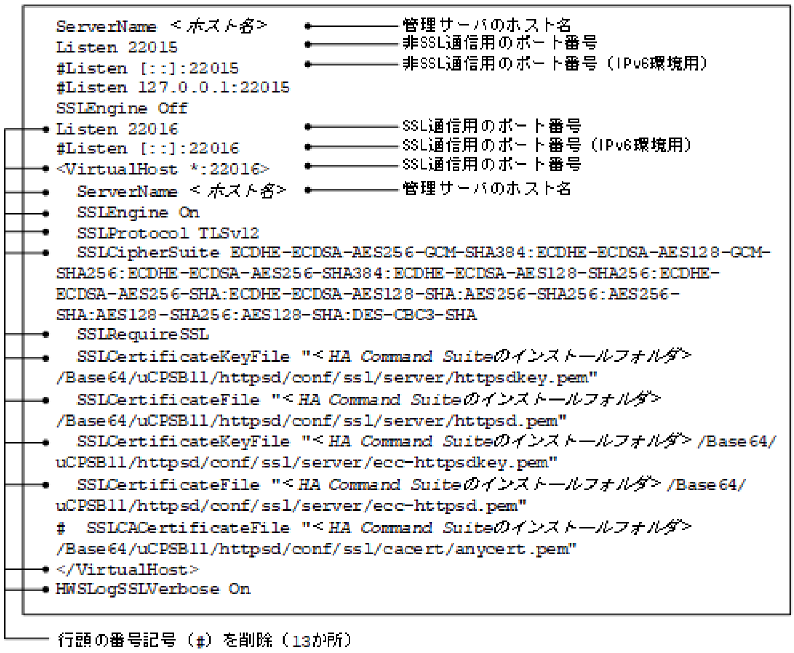
   SSL/TLS の有効化に必要な設定

メモ

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。ただし,以下のディレクティブについては，RSA 暗号と楕円曲線暗号用にそれぞれ各一組指定できます。
  - `SSLCertificateKeyFile`
  - `SSLCertificateFile`
- 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 暗号または楕円曲線暗号の HA 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 暗号と楕円曲線暗号を両方使用する場合，それぞれ指定する必要があります。

- SSLCertificateFile ディレクティブに，RSA 暗号または楕円曲線暗号の HA 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 暗号と楕円曲線暗号を両方使用する場合，それぞれ指定する必要があります。
- HA 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。

メモ

- SSL を有効にする場合や Device 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。
- 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，SSLCipherSuite ディレクティブ，SSLCertificateKeyFile ディレクティブおよび SSLCertificateFile ディレクティブの内容をコピーして使用してください。

  ＜ *HA Command Suite のインストールフォルダ*＞\Base64\sample\httpsd\conf\user_httpsd.conf

ヒント

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。

3. HA Command Suite 製品のサービスを起動します。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

5.2.4　証明書の有効期限の確認（HA Command Suite 共通コンポーネント）

HA 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。有効期限切れに注意してください。

前提条件

- user_httpsd.conf ファイルの編集

  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。

  - HA 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

- Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して，証明書の有効期限を確認してください。

   < *HA Command Suite のインストールフォルダ*>\Base64\bin\hcmds64checkcerts { [/days *<日数>*] [/log] | /all }

   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，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

   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。

関連リンク

SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集（84 ページ）

5.3　SSL サーバの構築（Device Manager サーバ）

Device Manager サーバを SSL サーバとして使用するためには，秘密鍵とサーバ証明書を準備する必要があります。

5.3.1　Device Manager サーバのキーペアと自己署名証明書の作成

Device Manager サーバのキーペアと自己署名証明書を作成するには，HiKeytool のメインメニューから[SSL configuration for Device Manager Server] - [Make KeyPair/Self-Signed Certificate]を選択します。

暗号および Java セキュリティの分野に精通しているか，特に指定がある場合を除き，デフォルト値を使用してください。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 権限でのログイン
- 既存のキーペアの削除（再作成する場合）

  キーストアーに格納できるキーペアは 1 つだけです。複数のキーペアが格納されていると，Device Manager サーバをセキュアモードで使用する際に問題が発生するおそれがあります。
- 次の情報の確認
  - 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。

操作手順

1. 次のとおり実行して，HiKeytool を起動します。

   ＜*HA Command Suite のインストールフォルダ*＞`\DeviceManager\Server\HiKeytool.bat`
2. メインメニューで，`1`（[SSL configuration for Device Manager Server]）を指定します。
3. サーバ用メインメニューで，`1`（[Make KeyPair/Self-Signed Certificate]）を指定します。
4. ホスト名を指定します。

   管理クライアントから管理サーバ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。クラスタ環境で管理サーバを運用している場合は，論理ホスト名を指定してください。

使用しているマシンが LAN または WAN の別名で認識される場合を除き，デフォルト値を使用してください。別名で認識される場合には，Device Manager サーバが認識される名前を指定する必要があります。

手順 4〜手順 9 で指定する値に，円記号（\）は指定できません。

5. 組織の構成単位を指定します。

   デフォルト値を推奨しますが，`Marketing` のようにわかりやすい別の名前も使用できます。

6. 組織名を指定します。

   通常はデフォルト値のホスト名を使用しますが，会社名など別の名前も使用できます。

7. 市区町村名または地域名を指定します。
8. 都道府県名を指定します。
9. 2 文字の国コードを指定します。
10. キーエイリアスを指定します。

    手順 4 で指定したホスト名と同じ文字列を指定してください。

11. 秘密鍵のパスワードを指定します。
12. キーアルゴリズムを指定します。

    RSA だけがサポートされています。

13. キーサイズを指定します。

    2048 ビットだけがサポートされています。

14. 署名アルゴリズムを指定します。

    SHA256withRSA，SHA1withRSA および MD5withRSA がサポートされています。

15. キーペアと自己署名証明書の有効日数を指定します。
16. キーストアーパスワードを指定します（最低 6 文字）。
17. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

    HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

操作結果

キーペアと自己署名証明書が作成され，Device Manager サーバのキーストアーファイル（デフォルト：`keystore`）に登録されます。

< *HA Command Suite のインストールフォルダ*>`\DeviceManager\Server\keystore`

ヒント

Device Manager サーバのキーストアーファイルは，Device Manager サーバの server.properties ファイルにある server.https.security.keystore プロパティで変更できます。

```
>1


Enter Server Name [default=example]:example.com

Enter Organizational Unit [default=Device Manager Administration]:

Enter Organization Name [default=example]:example

Enter your City or Locality:Yokohama

Enter your State or Province:Kanagawa

Enter your two-character country-code [default=JP]:

Enter Key Alias [default=example]:example.com

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespa
ces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter Key Password (6 characters minimum) [default=passphrase]:

Enter Key Algorithm [default=RSA]:

Enter Key Size [default=2048]:

Enter Signature Algorithm [default=SHA256withRSA]:

Enter number of days valid [default=365]:

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespa
ces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter KeyStore Password (6 characters minimum) [default=passphrase]:

Creating new X500Name for
example.com...

Creating the Device Manager Server KeyPair for example.com at:
        C:\Program Files\NEC\HA\DeviceManager\Server\keystore
        <this can take up to a minute>
        Updating KeyStore password in server.properties ...
        Saving new KeyStore password to disk...
        Updating keypass in server properties...
        Saving new keypass to disk...

All done.
```

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
server.https.security.keystore（198 ページ）

5.3.2 Device Manager サーバの SSL/TLS の有効化

Device Manager サーバの SSL/TLS を有効にするには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Set Device Manager Server Security Level]を選択します。

前提条件

- Administrator 権限でのログイン
- Device Manager サーバの自己署名証明書とキーペアの作成

操作手順

1. HiKeytool を起動し，メインメニューで 1（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，2（[Set Device Manager Server Security Level]）を指定します。
3. 2（[TLS/SSL]）を指定します。
4. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

操作結果

```
>2

Current Device Manager Server Security Level = User Logon (Basic Authentica
tion)

Options:
1) User Logon (Basic Authentication)
2) TLS/SSL (Secure Sockets)
Enter selection: [default=2]:2

Device Manager Server Security level set to: TLS/SSL Secure Socket
You must restart the Device Manager Server for this change to take effect.
```

5.3.3 Device Manager サーバの証明書発行要求の作成

Device Manager サーバで証明書発行要求（CSR）を作成するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Generate CSR]を選択します。

前提条件

- Administrator 権限でのログイン
- Device Manager サーバのキーペアの作成
- Device Manager サーバでの SSL/TLS の有効化

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`3`（[Generate CSR]）を指定します。

操作結果

証明書発行要求が，次の場所に＜*ホスト名*＞`.csr` というファイル名で保存されます。

＜ *HA Command Suite のインストールフォルダ*＞`\DeviceManager\Server`

```
>3

Generating CSR...
CSR has been written to disk and saved at:
C:\Program Files\NEC\HA\DeviceManager\Server\example.com.csr
All done!
```

作成される証明書発行要求の例を次に示します。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC0zCCAbsCAQAwgY0xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTERMA8GA1UEBxM
IWW9rb2hhbWExEjAQBgNVBAoTCVMxMDM4NDc3MzEwMC4GA1UECxMnSGlDb21tYW5kIERldmljZS
BNYW5hZ2VyIEFkbWluaXN0cmF0aW9uMRIwEAYDVQQDEwlTMTAzODQ3NzMwggEiMA0GCSqGSIb3D
QEB
:
省略
:
wEYfCLrKBtlGrzv9eRpcelQIs5bRbzM9S4KGPwbnYKym31281m6MiN27U7t0XWOoI73xC/jJVlK
25+s0tVyerxO9zVYvtirWO2Q+H4KUeQ6tJHo79nY5W2OCVsWr/Vuyh+XvbVtVnLI8oVPkMUIFnh
OQijq+VPSaSlKjiba6NA/+jgT4Fe0dfq31zJ8ELIN/YtlKCl8txEhO2MXwOQ==
-----END NEW CERTIFICATE REQUEST-----
```

メモ

実際の CSR にはキャリッジリターンや改行が余計に含まれています。これらがないと，認証局への送信時に正しく処理されません。

5.3.4 Device Manager サーバ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 Device Manager サーバの証明書発行要求（CSR）を任意の認証局に送信し，電子署名を受けます。

前提条件

- Device Manager サーバ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

      X.509 DER 形式または 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。

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。次の場所に*＜ホスト名＞*`.cer` というファイル名で保存しておくことをお勧めします。

＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server`

認証局によっては，サーバ証明書が`.cer` 拡張子付きの添付書類として返送されることがあります。また，認証局が応答を E メールの本文にテキストとして埋め込んで返送してきた場合は，テキストエディターを使用して応答を新規ファイルに保存してください。

メモ

- 認証局からの返答は保存しておいてください。
- 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，HiKeytool を使用して確認してください。
- 認証局によってサーバ証明書に設定された有効日数は，HiKeytool で設定した値よりも優先されます。キーペアとそれに関連するサーバ証明書の期限が切れると，SSL/TLS を介した安全な接続を確立できなくなります。

  サーバ証明書を更新する必要がある期日を書き留めておいてください。

次に認証局で発行されたサーバ証明書の例を示します。

```
-----BEGIN CERTIFICATE-----
MIIDMDCCApmgAwIBAgIDOBcYMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
```

```
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
:
省略
:
ADANBgkqhkiG9w0BAQQFAAOBgQBtzeFG4IfvpPnA7G/khD4rrT1TvjbK4Y1pcROM
cel43uUfKgNYgY35UukoNtd120XOoudLwKvJu5JK7846zWIbEJmCr5BYlmywZuao
MQdXMyPOUnqucgg44/JG2F27xqP4atWEZsNlj5R7XGGXi4RPAO5Y0YbbbvMJD0QR
yV0Oxw==
-----END CERTIFICATE-----
```

関連リンク

Device Manager サーバのサーバ証明書の確認（105 ページ）

5.3.5　Device Manager サーバのキーストアーへのサーバ証明書のインポート

Device Manager サーバのキーストアーに，認証局で発行されたサーバ証明書をインポートするには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Import Digitally Signed Certificate]を選択します。

前提条件

- Administrator 権限でのログイン
- 既存のキーペアの削除

  キーストアーに格納できるキーペアは 1 つだけです。複数のキーペアが格納されていると，Device Manager サーバをセキュアモードで使用する際に問題が発生するおそれがあります。
- Device Manager サーバのサーバ証明書の入手
- 証明書のインポート

  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を，Device Manager サーバのトラストストアーにインポートします。

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`4`（[Import Digitally Signed Certificate]）を指定します。
3. サーバ証明書の格納場所を絶対パスで指定します。
4. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

操作結果

サーバ証明書が Device Manager サーバのキーストアーファイル（デフォルト：`keystore`）にインポートされます。

< *HA Command Suite のインストールフォルダ*>`\DeviceManager\Server\keystore`

ヒント

Device Manager サーバのキーストアーファイルは，Device Manager サーバの `server.properties` ファイルにある `server.https.security.keystore` プロパティで変更できます。

```
>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate [default=C:\Program
Files\NEC\HA\DeviceManager\Server\example.com.cer]:
Beginning import...

Digitally signed certificate imported. You must restart the Device Manager
Server for the changes to take effect.
```

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
server.https.security.keystore（198 ページ）

5.3.6 Device Manager サーバのキーペア情報の参照（標準モード）

Device Manager サーバのキーストアーに登録されたキーペアの情報を標準モードで参照するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Display contents of Device Manager Server KeyStore]を選択します。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。

2. サーバ用メインメニューで，5（[Display contents of Device Manager Server KeyStore]）を指定します。

操作結果

キーペアのエイリアス名，作成日，MD5 Fingerprints が次のように表示されます。

```
>5
Listing Contents of Device Manager Server KeyStore

   Alias
   ==========
1) example.com, Tue Apr 01 09:48:02 JST 2008
   MD5  Fingerprints:FC:59:A5:8A:5A:27:5E:70:E4:6B:21:30:39:D1:00:1D
```

5.3.7　Device Manager サーバのキーペア情報の参照（詳細モード）

Device Manager サーバのキーストアーに登録されたキーペアの情報を詳細モードで参照するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Display verbose contents of Device Manager Server KeyStore]を選択します。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで 1（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，6（[Display verbose contents of Device Manager Server KeyStore]）を指定します。

操作結果

キーペアの詳細情報が次のように表示されます。

```
>6

Listing Contents of Device Manager Server KeyStore

1)
alias: example.com
Certificate chain length: 1
Issued by: example.com: example
Server Name: example.com
Organizational Unit: Device Manager Administration
Organization: example
```

```
Locality: Yokohama
State: Kanagawa
Country: JP
Created: Tue Apr 01 09:48:02 JST 2008
Entry Type: Key Entry
Certificate Version: 1
Serial Number: 47f18642
Valid from: Tue Apr 01 09:48:02 JST 2008
Valid to: Wed Apr 01 09:48:02 JST 2009
Certificate: VALID
MD5  Fingerprints: FC:59:A5:8A:5A:27:5E:70:E4:6B:21:30:39:D1:00:1D
SHA1 Fingerprints: F7:C4:2D:F3:E3:F3:5A:AB:E1:57:D1:E8:9C:80:07:89:2C:2A:48
:7A
```

5.3.8 Device Manager サーバのキーストアーからのキーペアの削除

Device Manager サーバのキーストアーからキーペアを削除するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Delete an entry from the Device Manager Server KeyStore]を選択します。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで 1（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，7（[Delete an entry from the Device Manager Server KeyStore]）と指定します 。
3. 削除するキーペアの番号を指定します。
4. 表示されたメッセージを確認して，[y]キーを押します。
5. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

操作結果

```
>7

Delete an entry from the Device Manager Server KeyStore.

   Alias
```

```
   ==========
1) example.com, Tue Apr 01 09:48:02 JST 2008
   MD5  Fingerprints:FC:59:A5:8A:5A:27:5E:70:E4:6B:21:30:39:D1:00:1D
Enter number of alias to delete (0 to abort) [default=0]:1

Delete example.com [1] ? [default=No]:y
```

5.3.9 Device Manager サーバのキーペアのパスワードの変更

Device Manager サーバのキーペアのパスワードを変更するには，HiKeytool のメインメニュー[SSL configuration for Device Manager Server]-[Change Device Manager Server KeyPair/Self-Signed Certificate Keypass]を選択します。

前提条件

- Administrator 権限でのログイン
- 次の情報の確認
  - Device Manager サーバのキーストアーパスワード
  - Device Manager サーバのキーペアの現在のパスワード

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`8`（[Change Device Manager Server KeyPair/Self-Signed Certificate Keypass]）を指定します。
3. Device Manager サーバのキーストアーパスワードを指定します。
4. 現在のキーペアのパスワードを指定します。
5. 新しいキーペアのパスワードを指定します。

   使用できる文字は次のとおりです。

   `A～Z a～z 0～9` 空白文字

   大文字と小文字は区別されます。ほかの文字を指定すると，キーストアーを使用できなくなります。
6. 新しいパスワードを再指定します。
7. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

5.3.10　Device Manager サーバのキーストアーパスワードの変更

Device Manager サーバのキーストアーのパスワードを変更するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Change Device Manager Server KeyStore Password]を選択します。

前提条件

次の情報の確認

- Device Manager サーバの現在のキーストアーパスワード

操作手順

1. HiKeytool を起動し，メインメニューで 1（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，9（[Change Device Manager Server KeyStore Password]）を指定します。
3. 現在の Device Manager サーバのキーストアーパスワードを指定します。
4. 新しいキーストアーパスワードを指定します。

   使用できる文字は次のとおりです。

   A～Z a～z 0～9 空白文字

   大文字と小文字は区別されます。ほかの文字を指定すると，キーストアーを使用できなくなります。
5. 新しいパスワードを再指定します。
6. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

5.3.11　Device Manager サーバのトラストストアーへの証明書のインポート

Device Manager サーバのトラストストアーに，証明書をインポートするには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Import Certificate to Device Manager Server TrustStore]を選択します。

前提条件

- Administrator 権限でのログイン

- 証明書の入手

  X.509 DER 形式または X.509 PEM 形式の証明書が必要です。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を準備してください。

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`10`（[Import Certificate to Device Manager Server TrustStore]）を指定します。
3. インポートする証明書のエイリアス名を指定します。
4. インポートする証明書の絶対パスを指定します。
5. インポートする証明書が複数ある場合は，手順 2〜手順 4 を繰り返します。
6. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

関連リンク

トラストストアー（79 ページ）

5.3.12　Device Manager サーバのトラストストアー情報の参照（標準モード）

Device Manager サーバのトラストストアーに登録されたサーバ証明書の情報を標準モードで参照するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Display contents of Device Manager Server TrustStore]を選択します。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`11`（[Display contents of Device Manager Server TrustStore]）を指定します。

操作結果

サーバ証明書のエイリアス名，作成日，および MD5 Fingerprints が表示されます。

```
>11

Listing Contents of Device Manager Server TrustStore

   Alias
   ==========
1) verisignclass3ca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E
```

関連リンク

トラストストアー（79 ページ）

5.3.13　Device Manager サーバのトラストストアー情報の参照（詳細モード）

Device Manager サーバのトラストストアーに登録されたサーバ証明書の情報を詳細モードで参照するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Display verbose contents of Device Manager Server TrustStore]を選択します。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで 1（[SSL configuration for Device Manager Server]）を指定します。

2. サーバ用メインメニューで，12（[Display verbose contents of Device Manager Server TrustStore]）を指定します。

操作結果

サーバ証明書の詳細情報が次のように表示されます。

```
>12

Listing Contents of Device Manager Server TrustStore

1)
alias: verisignclass3ca
Issued by: "VeriSign, Inc."
Organizational Unit: Class 3 Public Primary Certification Authority
Organization: "VeriSign, Inc."
Country: US
Created: Fri Nov 25 12:04:38 JST 2005
Entry Type: Trusted Certificate
Certificate Version: 1
Serial Number: 70bae41d10d92934b638ca7b03ccbabf
Valid from: Mon Jan 29 09:00:00 JST 1996
Valid to: Wed Aug 02 08:59:59 JST 2028
Certificate: VALID
MD5  Fingerprints: 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
SHA1 Fingerprints: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74
:E2
```

関連リンク

トラストストアー（79 ページ）

5.3.14　Device Manager サーバのトラストストアーからのサーバ証明書の削除

Device Manager サーバのトラストストアーに登録されたサーバ証明書を削除するには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Delete an entry from the Device Manager Server TrustStore]を選択します。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで 1（[SSL configuration for Device Manager Server]）を指定します。

2. サーバ用メインメニューで，`13`（[Delete an entry from the Device Manager Server TrustStore]）を指定します。
3. 削除するサーバ証明書の番号を指定します。
4. 表示されたメッセージを確認して，[y]キーを押します。
5. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

操作結果

指定したエントリーが削除され，Device Manager サーバのトラストストアーの内容が再び表示されます。 削除が完了したことを確認してください。

```
>13

Delete an entry from the Device Manager Server TrustStore.

   Alias
   ==========
1) verisignclass3ca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E

Enter number of alias to delete (0 to abort) [default=0]:1

Delete verisignclass3ca [1] ?  [default=No]:
```

関連リンク

トラストストアー（79 ページ）

5.3.15　Device Manager サーバのトラストストアーパスワードの変更

Device 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，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Change Device Manager Server TrustStore Password]を選択します。

前提条件

- Administrator 権限でのログイン
- 次の情報の確認
  - Device Manager サーバのトラストストアーの現在のパスワード

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`14`（[Change Device Manager Server TrustStore Password]）を指定します。
3. 現在のトラストストアーパスワードを指定します。
4. 新しいトラストストアーパスワードを指定します。

   使用できる文字は次のとおりです。

   `A`～`Z` `a`～`z` `0`～`9` 空白文字

   大文字と小文字は区別されます。ほかの文字を指定すると，キーストアーを使用できなくなります。
5. 新しいパスワードを再指定します。
6. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

   HiKeytool でセキュリティ設定を続けて実施する場合，設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば，変更が有効になります。

関連リンク

トラストストアー（79 ページ）

5.3.16　Device Manager サーバのサーバ証明書の確認

Device Manager サーバのサーバ証明書を確認するには，HiKeytool 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。

前提条件

Administrator 権限でのログイン

操作手順

1. HiKeytool を起動し，メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。
2. サーバ用メインメニューで，`6`（[Display verbose contents of Device Manager Server KeyStore]）を指定します。

操作結果

サーバ証明書の詳細情報が表示されます。「`Valid to:`」行を確認してください。

関連リンク

Device Manager サーバのキーペア情報の参照（詳細モード）（97 ページ）

5.4　SSL クライアントの構築

SSL/TLS で通信するためには，SSL サーバで作成されたサーバ証明書を SSL クライアントにインポートする必要があります。

5.4.1　Device Manager サーバのトラストストアーファイルのダウンロード

Web ブラウザー経由で，Device Manager サーバのトラストストアーファイル（`DeviceManagerCerts`）をダウンロードします。

前提条件

- Device Manager サーバのサーバ証明書のインポート（認証局が発行したサーバ証明書を使用する場合）
  - トラストストアーへの証明書のインポート
  - キーストアーへのサーバ証明書のインポート
- Device Manager サーバの自己署名証明書の作成（自己署名証明書を使用する場合）

  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。
- 次の情報の確認
  - Device Manager サーバの非 SSL 通信用のポート番号（デフォルト：2001）

Device Manager サーバの `server.properties` ファイルにある `server.http.port` プロパティで確認できます。

- Device Manager のユーザーアカウント

操作手順

1. 管理サーバで Web ブラウザーや OS のコマンドなどを使用して，次の URL からトラストストアーファイルをダウンロードします。

   ユーザーアカウントを指定してダウンロードしてください。

   http://*<ループバックの IP アドレスまたはループバックのホスト名>*:*<Device Manager サーバのポート番号>*/service/DeviceManagerCerts

関連リンク

Device Manager サーバのキーペアと自己署名証明書の作成（89 ページ）
Device Manager サーバのキーストアーへのサーバ証明書のインポート（95 ページ）
Device Manager サーバのトラストストアーへの証明書のインポート（100 ページ）
server.http.port（180 ページ）

5.4.2 Device Manager サーバの自己署名証明書のエクスポート

ダウンロードしたトラストストアーファイル（`DeviceManagerCerts`）から，Device Manager サーバの自己署名証明書をエクスポートするには，`hcmds64keytool` ユーティリティを使用します。

前提条件

- Device Manager サーバのトラストストアーファイルのダウンロード
- 次の情報の確認
  - Device Manager サーバのキーペアのエイリアス名

    HiKeytool で確認できます。

操作手順

1. 次のコマンドを実行します。

   <HA Command Suite のインストールフォルダ>\Base64\bin\hcmds64keytool -export -keystore *<トラストストアーファイル>* -alias *<エイリアス名>* -file *<サーバ証明書>*

   - `keystore`：トラストストアーファイルのパスを指定します。

- `alias`：キーペアのエイリアス名を指定します。
- `file`：出力する自己署名証明書ファイルのパスを指定します。

2. Device Manager サーバのトラストストアーファイルのパスワードには何も入力しないで，[Enter]キーを押します。

関連リンク

Device Manager サーバのキーペア情報の参照（標準モード）（96 ページ）

5.4.3　Web ブラウザーへの証明書のインポート（Microsoft Edge の場合）

GUI を使用するためには，証明書を管理クライアント（GUI）の Web ブラウザーにインポートしておく必要があります。

前提条件

- 証明書の入手

  認証局を使用する場合は，次のサーバ証明書を発行した認証局から，ルート認証局までの全認証局の証明書がチェインされた状態で必要です。

  - HA Command Suite 共通コンポーネント
  - Device Manager サーバ

操作手順

1. Microsoft Edge を起動し，[設定など]－[設定]を選択します。
2. [プライバシー、検索、サービス]で[証明書の管理]ボタンをクリックし，Web ブラウザーに証明書をインポートします。

関連リンク

HA Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成（80 ページ）
HA 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（84 ページ）
Device Manager サーバのサーバ証明書の認証局への申請（94 ページ）

5.4.4　Web ブラウザーへの証明書のインポート（Google Chrome の場合）

GUI を使用するためには，証明書を管理クライアント（GUI）の Web ブラウザーにインポートしておく必要があります。

前提条件

- 証明書の入手

  認証局を使用する場合は，次のサーバ証明書を発行した認証局から，ルート認証局までの全認証局の証明書がチェインされた状態で必要です。

  - HA Command Suite 共通コンポーネント
  - Device Manager サーバ

操作手順

1. Google Chrome を起動し，[Google Chrome の設定]－[設定]を選択します。
2. [詳細設定を表示]をクリックします。
3. [HTTPS/SSL]メニューの[証明書の管理]ボタンをクリックし，Web ブラウザーに証明書をインポートします。

関連リンク

HA Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成（80 ページ）
HA 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（84 ページ）
Device Manager サーバのサーバ証明書の認証局への申請（94 ページ）

5.4.5 ポップアップブロックの設定変更

HA Command Suite 製品の URL を SSL 通信用に変更したら，Web ブラウザーのポップアップブロックの設定にも，SSL 通信用の URL を登録する必要があります。

前提条件

- HA Command Suite 製品の URL の変更
- 次の情報の確認
  - 管理サーバの IP アドレスまたはホスト名

操作手順

1. Web ブラウザーのポップアップブロックの設定で，許可する Web サイトのアドレスに次の URL を登録します。

   `https://`*<管理サーバの IP アドレスまたはホスト名>*

関連リンク

HA Command Suite 製品の URL の変更（hcmds64chgurl コマンド）（23 ページ）

5.4.6　HA Command Suite 共通コンポーネントのトラストストアーへの証明書のインポート

証明書をトラストストアー（`ldapcacerts` または `jssecacerts`）にインポートするには，`hcmds64keytool` ユーティリティを使用します。

前提条件

- 証明書の準備

  安全な方法で取得してください。

  - LDAP ディレクトリサーバとの通信に使う場合

    LDAP ディレクトリサーバのサーバ証明書を発行した認証局から，ルート認証局までの全認証局の証明書がチェインされた状態で必要です。HA Command Suite 製品の要件に合ったものである必要があります。

- 次の情報の確認

  - トラストストアーファイルのパス
  - トラストストアーへのアクセスパスワード（トラストストアーがすでに存在する場合）

操作手順

1. 次のコマンドを実行します。

   `<`*HA Command Suite のインストールフォルダ*`>\Base64\bin\hcmds64keytool -import -alias <`*エイリアス名*`> -file <`*証明書*`> -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*`>`

   - `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。

     サーバ証明書が複数ある場合は，トラストストアー内で使用されていない任意のエイリアス名を指定してください。

   - `file`：証明書を指定します。

   - `keystore`：インポート先のトラストストアーファイルのパスを指定します。存在しない場合は，自動的に作成されます。

     LDAP ディレクトリサーバのサーバ証明書は，`ldapcacerts` にインポートすることをお勧めします。ほかのプログラムと証明書を共有する場合は `jssecacerts` にインポートしてもかまいません。

   - `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。

メモ

- `hcmds64keytool` ユーティリティまたは `keytool` 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引用符（"）を含めないでください。

2. HA Command Suite 製品のサービスを再起動します。

関連リンク

トラストストアー（79 ページ）
HA Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成（80 ページ）
HA 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（84 ページ）
Device Manager サーバのサーバ証明書の認証局への申請（94 ページ）
Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

5.4.7　LDAP ディレクトリサーバのサーバ証明書の条件

管理サーバと LDAP ディレクトリサーバ間を StartTLS で通信する場合には，入手した LDAP ディレクトリサーバのサーバ証明書が次の条件を満たしていることを確認してください。

- `exauth.properties` ファイルの次の属性に，LDAP ディレクトリサーバのサーバ証明書の CN（Subject 欄の CN）が設定されていること。
  - 認証方式が LDAP の場合

    `auth.ldap.`＜ *auth.server.name に指定した値*＞`.host`
  - 認証方式が RADIUS で，外部認可サーバとも連携する場合

    外部認証サーバと外部認可サーバが同一マシンで稼働しているとき：

    `auth.radius.`＜ *auth.server.name に指定した値*＞`.host`

    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るとき：

    `auth.group.`＜ *ドメイン名*＞`.host`
  - 認証方式が Kerberos で，外部認可サーバとも連携する場合

    `auth.kerberos.`＜ *auth.kerberos.realm_name に指定した値*＞`.kdc`

関連リンク

外部認証サーバと外部認可サーバの登録（40 ページ）

5.4.8 HA 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された証明書の確認

HA Command Suite 共通コンポーネントのトラストストアー（ldapcacerts または jssecacerts）にインポートされた証明書を確認するには，hcmds64keytool ユーティリティを使用します。

前提条件

次の情報の確認

- トラストストアーファイルのパス
- トラストストアーへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

   ＜*HA Command Suite のインストールフォルダ*＞\Base64\bin\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：証明書が格納されているトラストストアーファイルのパスを指定します。
   - 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。

関連リンク

トラストストアー（79 ページ）

5.4.9 HA 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された証明書の削除

HA Command Suite 共通コンポーネントのトラストストアー（ldapcacerts または jssecacerts）にインポートされた証明書を削除するには，hcmds64keytool ユーティリティを使用します。

前提条件

次の情報の確認

- 削除する証明書のエイリアス名
- トラストストアーファイルのパス
- トラストストアーへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

   ＜HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64keytool -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＞*

   - `alias`：証明書のエイリアス名を指定します。
   - `keystore`：証明書が格納されているトラストストアーファイルのパスを指定します。
   - `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。

関連リンク

トラストストアー（79 ページ）
HA 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された証明書の確認（112 ページ）

5.4.10　Device Manager サーバのトラストストアーへの証明書のインポート

証明書を Device Manager サーバのトラストストアーにインポートするには，HiKeytool のメインメニューで[SSL configuration for Device Manager Server]-[Import Certificate to Device Manager Server TrustStore]を選択します。

前提条件

- Administrator 権限でのログイン

操作手順

1. 次のとおり実行して，HiKeytool を起動します。

   ＜HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\HiKeytool.bat`

2. メインメニューで `1`（[SSL configuration for Device Manager Server]）を指定します。

3. サーバ用メインメニューで，`10`（[Import Certificate to Device Manager Server TrustStore]）を指定します。
4. インポートする証明書のエイリアス名を指定します。
5. インポートする証明書の絶対パスを指定します。
6. インポートする証明書が複数ある場合は，手順 1～手順 5 を繰り返します。
7. 変更を有効にするために，HA Command Suite 製品のサービスを再起動します。

関連リンク

トラストストアー（79 ページ）
Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

5.4.11　Device 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

Device 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を確認するには，HiKeytool を使用します。

証明書の確認方法には，標準モードおよび詳細モードがあります。必要に応じて使い分けてください。

関連リンク

Device Manager サーバのトラストストアー情報の参照（標準モード）（101 ページ）
Device Manager サーバのトラストストアー情報の参照（詳細モード）（102 ページ）

第 6 章 ログおよびアラートの設定

この章では，HA Command Suite 製品でシステムの状態や障害を監視するために必要な設定について説明します。

6.1 アラートの設定

Device Manager では，管理対象のストレージシステムで発生した障害の情報を，アラートとして Device Manager GUI に表示します。アラートは E メールでも通知できます。

6.1.1 Device Manager での障害検知

Device Manager では，管理対象のストレージシステムの障害を，次の方法で検知します。

- ポーリング（デフォルト）

  Device Manager が，ストレージシステムの稼働状況を定期的に監視し，障害を検知した場合にアラートとして表示します。アラートには発生部位と障害の概要が含まれています。

  ポーリングの間隔は，Device Manager サーバの `server.dispatcher.daemon.pollingPeriod` プロパティで設定できます。

  メモ

  ポーリングでは，部位ごとに，前回のポーリング時の障害レベルと異なる障害レベルを検知した場合にのみアラートを検知します。このため，以下の場合に障害が検知できないことがあります。

  - 既に障害が発生している部位で発生した障害レベルが同じ障害
  - ポーリング間隔の間に発生し，回復した障害

  また，ポーリング間隔の間に同じ部位で複数の障害が発生した場合，１つの障害にまとめられます。

  ヒント

  - ポーリングでは，Device Manager がストレージシステムから受領した稼働状況をそのままアラートとして表示します。
  - ポーリングでは，Device Manager サーバが停止中に発生した障害が Device Manager の再起動後も継続している場合，検知できることがあります

- SNMP トラップ（オプション）

ストレージシステムから SNMP トラップを受信した時点で，SNMP トラップをアラートとして表示します。SNMP トラップには障害の発生部位だけでなく，発生場所の情報も含まれているため，障害要因を特定する際に便利です。なお，SNMP トラップを Device Manager で受信するためには，環境設定が必要です。

メモ

SNMP トラップ受信では，Device Manager サーバが停止中に発生した障害はアラートとして表示できません。

ヒント

Device Manager がストレージシステムから受信した SNMP トラップをそのままアラートとして表示します。

Device Manager で表示できるアラートは，ストレージシステムによって異なります。それぞれのサポート有無を次の表に示します。

表 6-1　Device Manager で表示できるアラート

管理対象		ポーリング	SNMP トラップ	アラートのメール通知
ストレージシステム	iStorage V シリーズ	Y	v1，v3	Y

（凡例）

Y：サポート

v1：SNMP v1 をサポート

v3：SNMP v3 をサポート

メモ

- ストレージシステムの場合，ポーリングと SNMP トラップでは，障害を検知するタイミングだけでなく，障害レベルも異なることがあります。これは，発生場所とその発生部位の障害が与える障害部位への影響度によって，障害部位の障害レベルが異なるためです。
- ポーリングと SNMP トラップの両方で同じ障害を検知している場合，それぞれをアラートとして表示します。ただし，同一の障害であっても，前述のとおり，ポーリングと SNMP トラップで障害レベルが異なることがあります。

関連リンク

SNMP トラップをアラートに表示するための設定（117 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
server.dispatcher.daemon.pollingPeriod（189 ページ）

6.1.2 SNMP トラップをアラートに表示するための設定

SNMP トラップをアラートに表示するには，次の設定が必要です。

- Device Manager で SNMP トラップを受信するための設定
  - 管理サーバの 162/udp ポートを Device Manager で使えるようにする
  - Device Manager サーバの `server.dispatcher.daemon.receiveTrap` プロパティに `true` を設定する
  - SNMP v3 を使用する場合は，`hdvmsnmpuser` コマンドで，SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする
- SNMP トラップを Device Manager に通知するための設定
  - ストレージシステムの場合は，SNMP Agent で，トラップの通知対象マシンとして管理サーバの IP アドレスを設定する（SNMP v1，SNMP v3 共通）

    SNMP Agent の設定方法については，マニュアル『SNMP Agent ユーザガイド』を参照してください。
  - SNMP v3 を使用する場合は，SNMP Agent で，SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする

    管理サーバと同じ内容を設定してください。認証情報の登録および暗号化の設定方法については，マニュアル『SNMP Agent ユーザガイド』を参照してください。

SNMP v1 で，Device Manager とストレージシステム間の通信をする場合，上記の設定が完了すると，Device Manager サーバはすべてのコミュニティの SNMP トラップを受信してアラートに表示します。

SNMP v3 で，Device Manager とストレージシステム間の通信をするときは，SNMP トラップ受信ユーザーに設定された認証情報に基づいて，すべての SNMP トラップを受信してアラートに表示します。

関連リンク

SNMP トラップ受信ユーザーを登録する（SNMP v3）（117 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
server.dispatcher.daemon.receiveTrap（190 ページ）

6.1.3 SNMP トラップ受信ユーザーを登録する（SNMP v3）

Device Manager でストレージシステムからの SNMP v3 トラップを受信するためには，SNMP トラップ受信ユーザーの登録が必要です。

前提条件

- Administrator 権限でのログイン

- 次の情報の確認
  - `hdvmsnmpuser` コマンド実行時に Device Manager との認証に使うユーザーアカウント

    `All Resources` が割り当てられ，Device Manager のロールとして `Admin` が設定されている Device Manager のユーザー ID およびパスワードを確認します。

操作手順

1. Device Manager サーバで `hdvmsnmpuser` コマンドを実行します。

なお，`hdvmsnmpuser` コマンドで設定した内容を有効にするために，Device Manager サーバを再起動する必要はありません。

関連リンク

SNMP トラップ受信ユーザーを管理するためのコマンド（hdvmsnmpuser）の形式（SNMP v3）（118 ページ）

6.1.4 SNMP トラップ受信ユーザーを管理するためのコマンド（hdvmsnmpuser）の形式（SNMP v3）

SNMP トラップ受信ユーザーの情報を設定するには，`hdvmsnmpuser` コマンドを実行します。

`hdvmsnmpuser` コマンドでは，ユーザー情報の登録，変更，削除，および取得ができます。

コマンドの形式

ユーザー情報を登録する場合：

`hdvmsnmpuser -u` ＜ *Device Manager のユーザー ID* ＞ `-p` ＜ *Device Manager のパスワード*＞ `add --user_name` ＜ *SNMP トラップ受信ユーザー名*＞ `--security_level` ＜*セキュリティレベル*＞ `[--auth_protocol` ＜*認証プロトコル*＞ `--auth_password` ＜*認証パスワード*＞ `[--encrypt_protocol` ＜*暗号化プロトコル*＞ `--encrypt_key` ＜*暗号キー*＞ `]]`

ユーザー情報を変更する場合：

`hdvmsnmpuser -u` ＜ *Device Manager のユーザー ID* ＞ `-p` ＜ *Device Manager のパスワード*＞ `modify --user_name` ＜ *SNMP トラップ受信ユーザー名*＞ `[--security_level` ＜*セキュリティレベル*＞ `] [--auth_protocol` ＜*認証プロトコル*＞ `] [--auth_password` ＜*認証パスワード*＞ `] [--encrypt_protocol` ＜*暗号化プロトコル*＞ `--encrypt_key` ＜*暗号キー*＞ `]`

ユーザー情報を削除する場合：

hdvmsnmpuser -u ＜ *Device Manager のユーザー ID* ＞ -p ＜ *Device Manager のパスワード*＞ delete --user_name ＜ *SNMP トラップ受信ユーザー名*＞

ユーザー情報を取得する場合

hdvmsnmpuser -u ＜ *Device Manager のユーザー ID* ＞ -p ＜ *Device Manager のパスワード*＞ get [--user_name ＜ *SNMP トラップ受信ユーザー名*＞]

コマンドの格納先

＜ *HA Command Suite のインストールフォルダ*＞\DeviceManager\Server\tools\hdvmsnmpuser.bat

オプション

SNMP トラップ受信ユーザー名，認証パスワード，および暗号キーに使用できる文字は次のとおりです。

A～Z a～z 0～9 空白文字 半角記号

次の記号は使用できません。

\ , / : ; * ? " < > | & % ^

大文字と小文字は区別されます。文字列の先頭または末尾に空白文字を指定しないでください。

-u ＜ *Device Manager のユーザー ID* ＞，-p ＜ *Device Manager のパスワード*＞

Device Manager のユーザー ID およびパスワードを指定します。

--user_name ＜ *SNMP トラップ受信ユーザー名*＞

SNMP トラップ受信ユーザー名を指定します。指定できる最大文字数は 32 文字です。

ユーザー情報を取得する場合，このオプションで指定した SNMP トラップ受信ユーザーの情報を出力します。このオプションを省略したときは，DeviceManager サーバに登録されているすべての SNMP トラップ受信ユーザーの情報を出力します。

--security_level ＜ *セキュリティレベル*＞

セキュリティレベルを指定します。指定できる値は次のとおりです。

authPriv（認証も暗号化もする）

authNoPriv（認証するが暗号化はしない）

noAuthNoPriv（認証も暗号化もしない）

--auth_protocol ***＜認証プロトコル＞***

認証時に使用するプロトコルとして，SHA または MD5 を指定します。

このオプションは，--security_level に authPriv または authNoPriv を設定する場合に指定します。

--auth_password ***＜認証パスワード＞***

認証用のパスワードを指定します。iStorage V シリーズの場合は，8 文字以上 64 文字以下で指定します。

このオプションは，--security_level に authPriv または authNoPriv を設定する場合に指定します。

--encrypt_protocol ***＜暗号化プロトコル＞***

通信時に使用する暗号化プロトコルとして，AES または DES を指定します。

このオプションは，--security_level に authPriv を設定する場合に指定します。

--encrypt_key ***＜暗号キー＞***

暗号化された情報を復元するためのキーを指定します。iStorage V シリーズの場合は，8 文字以上 64 文字以下で指定します。

このオプションは，--security_level に authPriv を設定する場合に指定します。

また，--encrypt_protocol を設定する場合は，必ず指定します。

6.1.5 アラートを E メール通知するための操作フロー

アラートが発生した場合に, ユーザーに自動的に E メールを通知できます。管理クライアントにログインしていない状況でも，ストレージシステムの障害を知ることができます。

アラートを E メール通知するために必要な設定を次に示します。

操作手順

1. SMTP サーバの環境設定

   使用する SMTP サーバの設定手順に従って，Device Manager サーバが SMTP サーバに接続できるように設定します。

2. 受信ユーザーの設定

   Device Manager GUI を使用して，E メールを受信するユーザーアカウントを設定します。

3. アラート通知のプロパティ設定

Device Manager サーバのプロパティに，SMTP サーバの情報や通知元のメールアドレスなどを設定します。

4. SMTP 認証ユーザーアカウントの登録（SMTP 認証を使用する場合）

   Device Manager サーバに SMTP 認証ユーザーアカウントを登録します。イベント通知やヘルスチェック結果の通知で登録済みの場合，再登録は不要です。

5. アラート通知テンプレートのカスタマイズ（任意）

   必要に応じてテンプレートファイルを編集し，E メールの出力内容を設定します。

メモ

- Device Manager が E メールを送信するのは，アラート検出時の 1 回だけです。送信に失敗した場合，E メールは再送されず，アラート情報および送信先の E メールアドレスが，Device Manager のトレースログファイルに出力されます。
- E メールを送信する前に Device Manager サーバのサービスが停止した場合，サービスが再起動しても E メールは送信されません。サービスの再起動後に，GUI で対処していないアラートがないか確認してください。
- Device Manager サーバの管理対象ストレージシステムに対して,環境の構築や保守を実施すると，ストレージシステムでアラートが多数発生することがあります。事前に Device Manager サーバの `server.mail.enabled.storagesystem` プロパティや `server.mail.enabled.fileserver` プロパティに `false` を指定し，E メール通知機能を無効にしておくことをお勧めします。

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
server.mail.enabled.storagesystem（182 ページ）

6.1.6 SMTP サーバの設定

Device Manager サーバが SMTP サーバに接続できるように設定します。

SMTP サーバで，Device Manager サーバがサポートしている SMTP 認証の認証方式を指定してください。Device Manager サーバがサポートする SMTP 認証の認証方式は，LOGIN，PLAIN です。

メモ

- SMTP サーバの認証方式が複数ある場合，Device Manager サーバは LOGIN，PLAIN の優先順で E メールを送信します。SMTP サーバで LOGIN または PLAIN が指定されていない場合は，SMTP 認証を使用しないで E メールを送信します。
- SMTP サーバで SMTP 認証の設定が無効な場合，Device Manager サーバ側で SMTP 認証の設定を有効にしていても，Device Manager サーバは SMTP 認証を使用しないで E メールを送信します。

6.1.7　受信ユーザーの設定

Device Manager GUI を使用して，E メールを受信するユーザーアカウントを設定します。

E メールを受信するユーザーの条件は次のとおりです。条件を満たすユーザーに同じ内容の E メールが送信されます。

- 管理対象のリソースに対応するリソースグループが割り当てられていること。
- 割り当てたリソースグループに対する Device Manager のロールとして `Modify` が設定されていること。
- ユーザーのプロファイルに E メールアドレスが登録されていること。

  ユーザーアカウントを HA Command Suite 製品に登録している場合に必要です。外部認可サーバでユーザーアカウントを管理している場合は, 外部認可サーバで E メールアドレスを登録してください。

  Device Manager GUI でのユーザーアカウントの設定については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

ヒント

Device Manager サーバが送信する E メールの文字コードは Unicode（UTF-8）です。E メールを受信するユーザーは，Unicode（UTF-8）に対応したメールソフトを使用してください。

6.1.8　アラート通知のプロパティ設定

アラートを E メールで通知するには，Device Manager サーバの `server.properties` ファイルのプロパティに，SMTP サーバの情報や通知元のメールアドレスなどを設定する必要があります。

設定が必要なプロパティは次のとおりです。

- `server.mail.enabled.storagesystem`
- `server.mail.enabled.fileserver`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`
- `server.mail.alert.type.storagesystem`
- `server.mail.alert.status`

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
server.mail.enabled.storagesystem（182 ページ）
server.mail.from（182 ページ）
server.mail.smtp.host（182 ページ）
server.mail.smtp.port（183 ページ）
server.mail.smtp.auth（183 ページ）
server.mail.errorsTo（183 ページ）
server.eventNotification.mail.to（184 ページ）
server.mail.alert.type.storagesystem（184 ページ）
server.mail.alert.status（184 ページ）

6.1.9 SMTP 認証ユーザーアカウントを Device Manager に登録する

SMTP 認証を使用する場合は，SMTP 認証ユーザーのアカウントを `hdvmmodmailuser` コマンドで Device Manager に登録します。イベント通知およびヘルスチェック結果の E メール通知で SMTP 認証ユーザーが設定済みの場合，再設定は不要です。

注意

- Device Manager サーバで SMTP 認証の設定を有効にしても, SMTP 認証ユーザーを登録していない場合，SMTP 認証を使用しないで，メールが送信されます。
- Device Manager サーバに設定できる SMTP 認証ユーザーは, 1 つだけです。コマンドを実行するたびに，設定されている SMTP 認証ユーザーの情報は更新されます。
- Device Manager サーバで設定した SMTP 認証ユーザーの情報は削除できません。

前提条件

- Administrator 権限でのログイン
- Device Manager サーバの `server.mail.smtp.auth` プロパティの設定

  `true` を指定してください。
- 次の情報の確認
  - リソースグループとして `All Resources` が割り当てられ，Device Manager のロールとして `Admin` が設定されている Device Manager のユーザー ID およびパスワード
  - SMTP 認証に使用するユーザー ID およびパスワード

操作手順

1. 次のコマンドを実行します。

   ＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\tools\hdvmmodmailuser.bat -u` *＜ Device Manager のユーザー ID ＞* `-p` *＜ Device Manager のパスワード＞ ＜ SMTP 認証ユーザー ID ＞* `[`*＜ SMTP 認証パスワード＞*`]`

2. HA Command Suite 製品のサービスを再起動します。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
server.mail.smtp.auth（183 ページ）

6.1.10 アラート通知テンプレートのカスタマイズ

E メールの内容は，テンプレートファイル（`mail-alert-detection.txt`）で変更できます。テンプレートファイルを変更したあとは，HA Command Suite 製品のサービスを再起動してください。

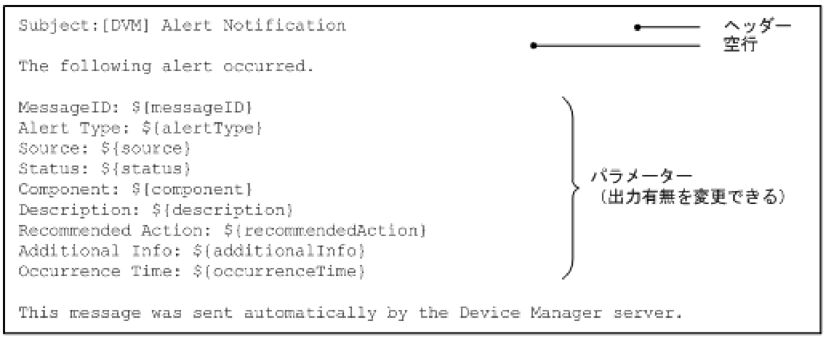
事前に完了しておく操作

- Administrator 権限でのログイン

次の場所に格納されているテンプレートファイル（`mail-alert-detection.txt`）を，テキストエディターで編集します。

＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\config`

デフォルトの `mail-alert-detection.txt` ファイルを次に示します。



```
Subject:[DVM] Alert Notification

The following alert occurred.

MessageID: ${messageID}
Alert Type: ${alertType}
Source: ${source}
Status: ${status}
Component: ${component}
Description: ${description}
Recommended Action: ${recommendedAction}
Additional Info: ${additionalInfo}
Occurrence Time: ${occurrenceTime}

This message was sent automatically by the Device Manager server.
```


`mail-alert-detection.txt` ファイルは，次に示す条件をすべて満たすようにしてください。条件を満たさない場合，デフォルトの設定内容で E メールが送信されます。

- ファイル名およびファイルの格納先は変更しないでください。

- 1 行目にヘッダー，2 行目に空行，3 行目以降に本文および出力するパラメーターを指定してください。
- ヘッダーは「`Subject:`＜*メールの件名*＞」の形式で 1 つだけ指定してください。
- パラメーターは「`${`＜*パラメーター名*＞`}`」の形式で指定してください。

  パラメーター名は大文字と小文字が区別されます。
- UTF-8 エンコーディングで記述してください。
- ファイルサイズは 64KB 以内になるようにしてください。
- 各行の長さは改行文字を除いて 1024 バイト以内になるようにしてください。

メモ

`mail-alert-detection.txt` ファイルを保存する際に，バイトオーダーマーク（BOM）を付与しないでください。

`mail-alert-detection.txt` ファイルに BOM が付与されていると，KAIC18797-E のエラーメッセージが出力され，E メールの送信に失敗します。

`mail-alert-detection.txt` ファイルに指定できるパラメーターを次の表に示します。

表 6-2　mail-alert-detection.txt ファイルに指定できるパラメーター

パラメーター名	説明
`messageID`	アラート ID
`alertType`	アラートの種別
`source`	アラートの発生元 ストレージシステムの場合は，ストレージシステム名
`status`	アラートの重要度
`component`	問題が発生したコンポーネント ストレージシステムの場合は，アラートが発生したストレージシステムの部位
`description`	アラートの説明
`recommendedAction`	アラートへの対処方法
`additionalInfo`	補足情報
`occurrenceTime`	ストレージシステムの場合は，Device Manager サーバがアラート情報を取得した時刻 表示形式：*yyyy*/*mm*/*dd hh*:*mm*:*ss* *hh* は 24 時間表示です。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

6.2 SNMP トラップをログファイルに出力するための設定

Device Manager では，ストレージシステムやネットワーク上の機器で発生した SNMP トラップを受信し，ログファイルに出力します。Device Manager の管理対象のストレージシステムだけでなく，管理対象外の機器の SNMP トラップ（SNMP v1，SNMP v3 限定）もログファイルに出力できます。

受信した SNMP トラップは，次のログファイルに出力されます。

- イベントログまたは syslog

SNMP トラップの情報のうち，ログファイルには次の情報が出力されます。

- トラップが受信されたことを示すメッセージ ID（プレフィックス：KAID）
- 送信元（agent）
- Enterprise ID（enterprise）
- 一般トラップ番号（generic）
- 固有トラップ番号（specific）

関連リンク

SNMP トラップをログファイルに出力するための設定（126 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
customizedsnmptrap.customizelist（201 ページ）

6.2.1 SNMP トラップをログファイルに出力するための設定

SNMP トラップを Device Manager で受信し，ログファイルに出力するためには，次の設定が必要です。

- Device Manager で SNMP トラップを受信するための設定※
  - 管理サーバの 162/udp ポートを Device Manager で使えるようにする
  - Device Manager サーバの `server.dispatcher.daemon.receiveTrap` プロパティに `true` を設定する
  - SNMP v3 を使用する場合は，`hdvmsnmpuser` コマンドで，SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする
- SNMP トラップを Device Manager に通知するための設定※
  - SNMP 関連ソフトウェアで，トラップの通知対象マシンに管理サーバの情報を登録する

例えば，ストレージシステムの SNMP トラップを受信するためには，SNMP Agent での設定が必要です。SNMP Agent の設定方法については，マニュアル『SNMP Agent ユーザガイド』を参照してください。

- SNMP v3 を使用する場合は，SNMP Agent で，SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする

  管理サーバと同じ内容を設定してください。認証情報の登録および暗号化の設定方法については，マニュアル『SNMP Agent ユーザガイド』を参照してください。

• SNMP トラップをログファイルに出力するための設定

  - `customizedsnmptrap.customizedSNMPTrapEnable` プロパティに `true` を設定する
  - `customizedsnmptrap.customizelist` プロパティにログファイルへの出力内容を設定する

注※　この設定は, SNMP トラップをアラートとして Device Manager GUI に表示する設定と同じです。

SNMP v1 で，Device Manager とストレージシステム間の通信をする場合，上記の設定が完了すると, Device Manager サーバはすべてのコミュニティの SNMP トラップを受信してログに出力します。

SNMP v3 で，Device Manager とストレージシステム間の通信をする場合，SNMP トラップ受信ユーザーに設定された認証情報に基づいて，すべての SNMP トラップを受信してログに出力します。

関連リンク

SNMP トラップ受信ユーザーを登録する（SNMP v3）（117 ページ）
Device Manager サーバのプロパティの変更（178 ページ）
server.dispatcher.daemon.receiveTrap（190 ページ）
customizedsnmptrap.customizedSNMPTrapEnable（201 ページ）
customizedsnmptrap.customizelist（201 ページ）

6.3 Device Manager のイベント通知を使用するために必要な設定

Device Manager GUI では，一部を除くすべての事象（イベント）の実行結果をメールでユーザーに通知できます。

ただし，次の HDvM タスクはメール通知が行われません。

• DT プールのモニタリングスケジュールのテンプレート編集
• DT プールのモニタリングスケジュールのテンプレート削除

Device Manager GUI のタスク作成時に E メール通知を有効にした場合，次の宛先へ実行結果が通知されます。

- Device Manager GUI のタスクを作成する際に設定したメールアドレス
- Device Manager サーバの server.properties ファイルにある server.eventNotification.mail.to プロパティに設定したメールアドレス

イベントを E メールで通知するためには，次の設定が必要です。アラートを E メールで通知するための設定をすでにしている場合は，1〜4 の設定は不要です。

操作手順

1. SMTP サーバの設定

   Device Manager サーバが SMTP サーバに接続できるように設定します。

2. 受信ユーザーの設定（任意）

   ログインユーザーの E メールアドレスを登録しておくと，Device Manager GUI でタスクを作成する際にメールアドレスが自動的に入力されます。

3. イベント通知のプロパティ設定

   Device Manager サーバのプロパティに，SMTP サーバの情報や通知元のメールアドレスなどを設定します。

4. SMTP 認証ユーザーの設定

   接続時に SMTP 認証を使用する場合は，hdvmmodmailuser コマンドで Device Manager サーバに認証用のユーザーアカウントを設定する必要があります。

5. イベント通知のテンプレート編集（任意）

   ユーザーにメールで通知する内容は，テンプレートファイルに設定されています。必要に応じてテンプレートファイルを編集してください。

関連リンク

SMTP サーバの設定（121 ページ）
受信ユーザーの設定（122 ページ）
Device Manager のイベント通知のためのプロパティの設定（129 ページ）
SMTP 認証ユーザーの設定（hdvmmodmailuser コマンド）（129 ページ）
Device Manager のイベント通知テンプレートの編集（130 ページ）
server.eventNotification.mail.to（184 ページ）

6.3.1　Device Manager のイベント通知のためのプロパティの設定

Device Manager に関するイベントの実行結果が E メールで通知されるようにするためには，Device Manager サーバの `server.properties` ファイルの次のプロパティに SMTP サーバの情報や通知元のメールアドレスなどを設定します。

- `server.mail.enabled.storagesystem`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`

関連リンク

server.mail.enabled.storagesystem（182 ページ）
server.mail.from（182 ページ）
server.mail.smtp.host（182 ページ）
server.mail.smtp.port（183 ページ）
server.mail.smtp.auth（183 ページ）
server.mail.errorsTo（183 ページ）
server.eventNotification.mail.to（184 ページ）

6.3.2　SMTP 認証ユーザーの設定（hdvmmodmailuser コマンド）

イベント通知機能を使用する場合，SMTP サーバに接続します。接続時に SMTP 認証を使用する場合は，`hdvmmodmailuser` コマンドで Device Manager サーバに認証用のユーザーアカウントを設定する必要があります。

`hdvmmodmailuser` コマンドを使用した SMTP 認証ユーザーの設定は，アラートおよびヘルスチェック結果の E メール通知と同じです。アラートまたはヘルスチェック結果の E メール通知で SMTP 認証ユーザーを設定した場合は，ここでの設定は不要です。

`hdvmmodmailuser` コマンドの記述形式を次に示します。

形式

＜ *HA Command Suite のインストールフォルダ*＞`\DeviceManager\Server\tools\hdvmmodmailuser.bat -u` ＜ *Device Manager のユーザー ID* ＞ `-p` ＜ *Device Manager のパスワード* ＞ ＜ *SMTP 認証ユーザー ID* ＞ `[`＜ *SMTP 認証パスワード*＞`]`

オプション

-u ＜ *Device Manager のユーザー ID* ＞

リソースグループとして All Resources が割り当てられ, Device Manager のロールとして Admin が設定されているユーザー ID を指定してください。

-p ＜ *Device Manager のパスワード*＞

u オプションに指定した＜ *Device Manager のユーザー ID* ＞で Device Manager にログインするときのパスワードを指定してください。

＜ *SMTP 認証ユーザー ID* ＞

SMTP 認証に使用するユーザー ID を指定してください。

＜ *SMTP 認証パスワード*＞

SMTP サーバにログインするときのパスワードを指定してください。

注意

- Device Manager サーバで SMTP 認証の設定を有効にしても, SMTP 認証ユーザーを登録していない場合，SMTP 認証を使用しないで，メールが送信されます。
- Device Manager サーバに設定できる SMTP 認証ユーザーは, 1 つだけです。コマンドを実行するたびに，設定されている SMTP 認証ユーザーの情報は更新されます。
- Device Manager サーバで設定した SMTP 認証ユーザーの情報は削除できません。

なお，hdvmmodmailuser コマンドで設定した内容を有効にするためには，hdvmmodmailuser コマンドを実行したあと，HA Command Suite 製品のサービスを再起動する必要があります。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

6.3.3 Device Manager のイベント通知テンプレートの編集

ユーザーにメールで通知する内容は, テンプレートファイルに設定されています。必要に応じてテンプレートファイルを編集し，項目の通知有無を変更できます。

テンプレートファイルは次の場所に格納されています。

＜ *HA Command Suite のインストールフォルダ*＞\DeviceManager\Server\config\mail-taskStatusNotification.txt

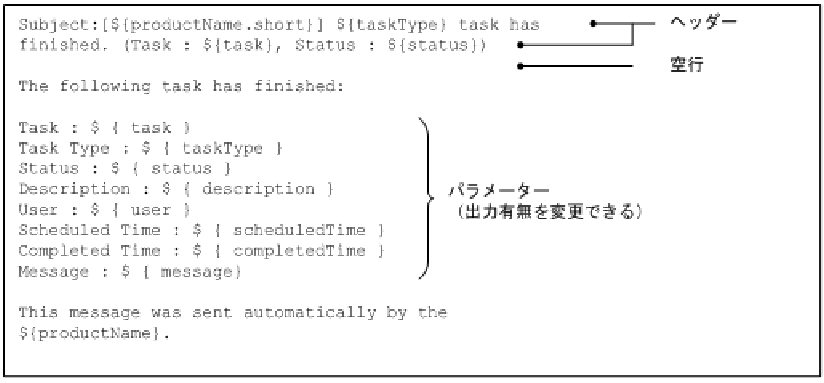
ヒント

テンプレートファイルを新規インストール時の設定に戻す場合には, 次の場所に格納されているひな形を使ってください。

＜HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\template\mail-taskStatusNotification.txt`

テンプレートにパラメーターを指定することで，イベントの情報をメールに埋め込みます。

テンプレートファイル（`mail-taskStatusNotification.txt`）の記述例を次に示します。



テンプレートファイルは，次に示す条件をすべて満たすように設定してください。

- 1 行目にはヘッダー，2 行目には空行を指定し，3 行目以降に本文を指定してください。
- ヘッダーは「`Subject:`*＜メールの件名＞*」の形式で 1 つだけ指定してください。
- パラメーターは「`${`*＜パラメーター名＞*`}`」の形式で指定してください。
- テンプレートファイルは，UTF-8 エンコーディングで記述してください。
- テンプレートファイルのサイズは，64KB 以内になるようにしてください。
- テンプレートファイルの各行の長さは，改行文字を除いて 1024 バイト以内になるようにしてください。

メモ

テンプレートファイルを保存する際に，バイトオーダーマーク（BOM）を付与しないでください。

テンプレートファイルに BOM が付与されていると，KAIC18797-E のエラーメッセージが出力され，E メールの送信に失敗します。

テンプレートに設定できるパラメーターを次に示します。

表 6-3　タスク終了イベントのパラメーター

パラメーター名	説明	ヘッダー	コンテンツ
`task`	タスク名	Y	Y
`taskType`	タスクの種類	Y	Y
`status`	タスクの状態	Y	Y
`description`	タスクの説明	--	Y
`user`	タスク作成者のユーザー ID	--	Y
`scheduledTime`	タスクの実行要求日時	--	Y
`completedTime`	タスクの実行終了日時	--	Y

パラメーター名	説明	ヘッダー	コンテンツ
message	エラーメッセージ	--	Y
productName	製品名称	--	Y
productName.short	製品名称（略称）	Y	Y

（凡例）

Y：指定できる。

--：指定できない。

第 7 章
サービスの起動と停止

この章では，HA Command Suite 製品のサービスを起動したり停止したりする方法について説明します。

7.1　Device Manager のサービスの起動と停止

ここでは，Device Manager のサービスを起動したり停止したりする方法について説明します。

7.1.1　Device Manager の常駐プロセス

Device Manager の運用では，常駐プロセスが OS 上で稼働していることが前提となります。

Device Manager の常駐プロセスを次の表に示します。

表 7-1　常駐プロセス

プロセス名	サービス名	機能
DeviceManagerServer	DeviceManagerServer	Device Manager サーバ
hcmdssvctl.exe cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	シングルサインオン用の HA Command Suite J2EE サービス
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web Service	HA 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 HA Command Suite 共通 Web サービス
hcmdssvctl.exe cjstartsv.exe	Device Manager Web Service	Device Manager の J2EE サービス
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。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）
Device Manager のサービスの稼働状態の確認（135 ページ）

7.1.2　Device Manager のサービスの起動

Windows メニューまたは hcmds64srv コマンドを使って，Device Manager のサービスを起動します。

前提条件

Administrator 権限でのログイン

操作手順

1. 次の操作を実行します。

   スタート画面からアプリケーションの一覧画面を表示し，[HA Device Manager]の[Start - HCS]を選択します。

   コマンドを実行する場合：

   ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64srv /start

操作結果

次のサービスが一括で起動され，各サービスを起動した結果が画面に表示されます。

- HiRDB
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- Device Manager Web Service
- DeviceManagerServer

7.1.3　Device Manager のサービスの停止

Windows メニューまたは hcmds64srv コマンドを使って，Device Manager のサービスを停止します。

前提条件

Administrator 権限でのログイン

操作手順

1. 次の操作を実行します。

スタート画面からアプリケーションの一覧画面を表示し，[HA Device Manager]の[Stop - HCS]を選択します。

コマンドを実行する場合：

< *HA Command Suite のインストールフォルダ*>`\Base64\bin\hcmds64srv /stop`

操作結果

次のサービスが一括で停止され，各サービスを停止した結果が画面に表示されます。

- HiRDB
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- Device Manager Web Service
- DeviceManagerServer

7.1.4 Device Manager のサービスの稼働状態の確認

Windows メニューまたは `hcmds64srv` コマンドを使って，各 Device Manager のサービスの稼働状態を確認します。

前提条件

Administrator 権限でのログイン

操作手順

1. 次の操作を実行します。

   スタート画面からアプリケーションの一覧画面を表示し，[HA Device Manager]の[Status - HCS]を選択します。

   コマンドを実行する場合

   < *HA Command Suite のインストールフォルダ*>`\Base64\bin\hcmds64srv /status all`

操作結果

各サービスの稼働状態が画面に表示されます。

7.2　クラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス

ここでは，`hcmds64clustersrvstate` コマンドが対象としている HA Command Suite 製品のサービスについて説明します。

Windows のクラスタ環境で，データベースをバックアップする場合などに，次の表に示すサービスを一括でオンラインまたはオフラインにします。

表 7-2　管理サーバでクラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス

製品名	サービス表示名	サービス名	備考
HA Command Suite 共通コンポーネント	`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	-
Device Manager	`Device Manager Web Service`	DeviceManagerWebService64	-
	`DeviceManagerServer`	DeviceManagerServer	-

（凡例）

- : 該当なし

第 8 章
データベースの管理

この章では，HA Command Suite 製品のデータベースをバックアップしたり，復元したりする方法について説明します。

8.1 データベースを管理する前に

バックアップと復元，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 8-1　バックアップ・復元とエクスポート・インポートの違い

項目	バックアップと復元	エクスポートとインポート
HA Command Suite 製品のバージョンの条件	制限なし。	制限なし。
主な使用目的	サーバマシンに障害が発生したときに，現状の運用環境を復元すること。	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	• HA Command Suite 製品のデータベース • HA Command Suite 共通コンポーネントのデータベース	• HA Command Suite 製品のデータベース • HA 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
マシン条件	• バックアップ元マシンと復元先のマシンで，インストールされている HA Command Suite 製品のバージョンおよびリビジョンが一致していること	• インポート先のマシンに，インポート対象の HA Command Suite 製品がインストールされていること • インポート先のマシンにインストールされている HA Command Suite 製品のバージョンおよびリビジョンが，エクスポート元と同じか，それ以上であること

以降で，各操作の手順を説明します。

8.2 データベースのバックアップ

データベースに障害が発生した場合，管理サーバを運用できなくなるおそれがあります。障害の発生に備えて，データベースのバックアップを定期的に取ってください。

データベースをバックアップするときには，バックアップファイルを格納するディレクトリが必要です。バックアップファイルを格納するディレクトリには，バックアップ時に作成される一時ファイルの分も含めて次の空き容量が必要です。

必要な空き容量：

（<*バックアップ対象となる HA Command Suite 製品のデータベースサイズの総和*>＋4.6GB）×2

Device Manager を使用している環境の場合は，次のディレクトリの容量を考慮して，バックアップに必要な容量を見積もります。

- Device Manager のデータベースの格納先ディレクトリ
- HA Command Suite 共通コンポーネントのデータベースの格納先ディレクトリ※

注※　HA Command Suite 共通コンポーネントのデータベースの格納先ディレクトリには，`BASE` ディレクトリと `SYS` ディレクトリがあります。

注意

データベースのバックアップでは，Device Manager のサービスの停止を伴う操作を実行します。バックアップ中は，Device Manager にアクセスしないでください。

メモ

バックアップソフトウェアで HA 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すると，I/O 遅延やファイル排他などで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 Device Manager のインストールディレクトリを含めてバックアップしたい場合は，HA Command Suite 製品のすべてのサービスを停止したあとに，バックアップしてください。

8.2.1 データベースのバックアップ（非クラスタ構成の場合）

管理サーバが非クラスタ構成の場合に，データベースをバックアップする手順を説明します。

操作手順

1. Administrator 権限のユーザーで管理サーバにログインします。
2. `hcmds64backups` 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。

   < HA Command Suite のインストールフォルダ>`\Base64\bin\hcmds64backups /dir` *<バックアップファイルの格納先フォルダ>* `/auto`

   `dir`

   データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。

   `dir` オプションに指定するディレクトリの下には，ファイルおよびサブディレクトリがないことを確認してください。

   `auto`

   HA Command Suite 製品のサービスを自動的に起動/停止するオプションです。

hcmds64backups コマンドを実行すると，dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され，データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

メモ

dir オプションに指定したバックアップファイルの格納先ディレクトリに作成される database 以外のディレクトリには，HA Command Suite 共通コンポーネントの設定ファイルがバックアップされます。管理サーバの障害によって HA Command Suite 製品を再インストールすることになった場合には，バックアップされた設定ファイルで以前の設定内容を確認できます。

メモ

hcmds64backups コマンドに続けて，以下のいずれかのコマンドを実行する場合，hcmds64backups コマンドに auto オプションは指定しないでください。

- hcmds64dbtrans
- hcmds64srv /stop または hcmds64srv -stop
- hcmds64db
- hcmds64backups

hcmds64backups コマンドに auto オプションを指定しないときは，hcmds64backups コマンドを実行する前に，以下のコマンドを順に実行してください。また，すべての作業が終了後，hcmds64srv /start コマンドまたは hcmds64srv -start コマンドを実行して，HA Command Suite 製品のサービスを起動します。

1. ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64srv /stop
2. ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64dbsrv /start

8.2.2 データベースのバックアップ（クラスタ構成の場合）

管理サーバの OS がクラスタ構成の場合に，データベースをバックアップする手順を説明します。

注意

実行系ノード（cluster.conf ファイルの mode に online が設定されているマシン）でデータベースをバックアップしてください。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して，HA Command Suite 製品のサービスをオフラインにします。

   ＜ HA Command Suite 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のリソースグループに登録された HA Command Suite 製品のサービスをオフラインにして，フェールオーバーを抑止するためのオプションです。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。

   `r`

   リソースグループ名を指定します。

   上記コマンドにより，HA Command Suite 製品のサービスが停止されます。

2. 次のコマンドを実行して，HiRDB サービスを起動します。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64dbsrv /start`

3. `hcmds64backups` 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。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64backups /dir` *＜バックアップファイルの格納先フォルダ＞*

   `dir`

   データベースのバックアップファイルを格納する共有ディスク上のフォルダを絶対パスで指定します。

   `dir` オプションに指定するフォルダの下には，ファイルおよびサブフォルダがないことを確認してください。

4. 次のコマンドを実行して，HiRDB サービスを停止します。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64dbsrv /stop`

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

   ＜ HA Command Suite 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されたリソースグループをオンラインにして，フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。

上記コマンドにより，HA Command Suite 製品のサービスが起動されます。

関連リンク

Device Manager のサービスの停止（134 ページ）
Device Manager のサービスの稼働状態の確認（135 ページ）
クラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス（136 ページ）

8.3 データベースの復元

データベースに障害が発生した場合，状況に応じて，次の方法で復元できます。

- データベースに不整合が生じた場合

  `hcmds64backups` コマンドでバックアップしておいたデータベースを使用して，復元できます。

  データベースをバックアップした時点の管理サーバと，データベースを復元する時点の管理サーバとで，次のすべてが一致していることが前提です。

  - インストールされている HA Command Suite 製品のバージョンおよびリビジョン
  - HA Command Suite 製品のインストール先
  - HA Command Suite 共通コンポーネントのインストール先
  - HA Command Suite 製品のデータベースのインストール先
  - HA Command Suite 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

- データベースが破損した場合

  `hcmds64dbtrans` コマンドでエクスポートしておいたデータベースを使用して，復元できます。

  データベースをエクスポートした時点の管理サーバと，データベースを復元する時点の管理サーバとで，インストールされている HA Command Suite 製品のバージョンおよびリビジョンが一致していることが前提です。

  `hcmds64dbrepair` コマンドを実行すると，管理サーバにインストールされている HA Command Suite 製品のデータベースは強制削除され，エクスポートしておいたデータベースに置き換わります。

8.3.1　データベース不整合時のデータベースの復元（非クラスタ構成の場合）

管理サーバが非クラスタ構成の場合に，データベースを復元する手順を説明します。

注意

- 手順の途中で使用する `hcmds64db` コマンドは，実行時に一時ファイルを作成します。バックアップファイルの格納先ディレクトリが次の条件を満たしていることを確認してください。
  ・`hcmds64db` コマンドを実行するユーザーに書き込み権限がある。
  ・格納しているバックアップファイルと同じ分の空き容量がある。
- データベースの復元では, Device Manager のサービスの停止を伴う操作を実行します。復元中は，Device Manager にアクセスしないでください。

操作手順

1. Administrator 権限のユーザーで管理サーバにログインします。
2. `hcmds64db` コマンドを実行してデータベースを復元します。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\bin\hcmds64db /restore` ＜*バックアップファイル*＞ `/type` ＜*復元する HA Command Suite 製品の名称*＞ `/auto`

   restore

   `hcmds64backups` コマンドで取得したデータベースのバックアップファイル（`backup.hdb`）を絶対パスで指定します。

   type

   `ALL` を指定してください。

   auto

   HA Command Suite 製品のサービスを自動的に起動/停止するオプションです。
3. Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を設定します。
4. HA Command Suite 製品のサービスを起動します。
5. Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
6. Device Manager の GUI でストレージシステムをリフレッシュします。
7. Device Manager の GUI で，Device Manager のタスクの状態を確認します。

   完了していない，またはエラーになっているタスクがあれば，必要に応じてタスクを再作成するか，実行スケジュールを変更してください。

関連リンク

Device Manager のサービスの起動（134 ページ）

8.3.2　データベース不整合時のデータベースの復元（クラスタ構成の場合）

管理サーバの OS がクラスタ構成の場合に，データベースを復元する手順を説明します。

注意

- 実行系ノード（`cluster.conf` ファイルの `mode` に `online` が設定されているマシン）でデータベースを復元してください。
- 手順の途中で使用する `hcmds64db` コマンドは，実行時に一時ファイルを作成します。バックアップファイルの格納先ディレクトリが次の条件を満たしていることを確認してください。

  ・`hcmds64db` コマンドを実行するユーザーに書き込み権限がある。

  ・格納しているバックアップファイルと同じ分の空き容量がある。
- データベースの復元では, Device Manager のサービスの停止を伴う操作を実行します。復元中は，Device Manager にアクセスしないでください。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して，HA Command Suite 製品のサービスをオフラインにします。

   ＜ *HA Command Suite 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のリソースグループに登録された HA Command Suite 製品のサービスをオフラインにして，フェールオーバーを抑止するためのオプションです。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。

   `r`

   リソースグループ名を指定します。

2. `hcmds64db` コマンドを実行してデータベースを復元します。

＜ HA Command Suite のインストールフォルダ＞\Base64\bin\hcmds64db /restore *＜バックアップファイル＞* /type *＜復元する HA Command Suite 製品の名称＞*

restore

hcmds64backups コマンドで取得したデータベースのバックアップファイル（backup.hdb）を絶対パスで指定します。共有ディスクに保存したものを使用してください。

type

ALL を指定してください。

3. 実行系ノードおよび待機系ノードで，Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
4. 次のコマンドを実行して，リソースグループおよび HA Command Suite 製品のサービスをオンラインにします。

   ＜ HA Command Suite 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されたリソースグループをオンラインにして，フェールオーバーを有効にするためのオプションです。

   r

   リソースグループ名を指定します。
5. 実行系ノードおよび待機系ノードで，Device Manager サーバの server.base.initialsynchro プロパティを false に戻します。
6. Device Manager の GUI でストレージシステムをリフレッシュします。
7. Device Manager の GUI で，Device Manager のタスクの状態を確認します。

   完了していない，またはエラーになっているタスクがあれば，必要に応じてタスクを再作成するか，実行スケジュールを変更してください。

関連リンク

クラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス（136 ページ）

8.3.3　データベース破損時のデータベースの復元（非クラスタ構成の場合）

管理サーバが非クラスタ構成の場合に，データベースを復元する手順を説明します。

注意

データベースの復元では，Device Manager のサービスの停止を伴う操作を実行します。復元中は，Device Manager にアクセスしないでください。

操作手順

1. Administrator 権限のユーザーで管理サーバにログインします。
2. HA Command Suite 製品のサービスを停止します。
3. `hcmds64dbrepair` コマンドを実行してデータベースを復元します。

   < *HA Command Suite のインストールフォルダ*>`\Base64\bin\hcmds64dbrepair /trans` <*エクスポートファイル*>

   `trans`

   `hcmds64dbtrans` コマンドでエクスポート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。
4. Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を設定します。
5. HA Command Suite 製品のサービスを起動します。
6. Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
7. Device Manager の GUI でストレージシステムをリフレッシュします。
8. Device Manager の GUI で，Device Manager のタスクの状態を確認します。

   完了していない，またはエラーになっているタスクがあれば，必要に応じてタスクを再作成するか，実行スケジュールを変更してください。
9. `System` アカウントのパスワードはデータベースの復元によって設定が初期化されるため，必要に応じて再設定します。

   `System` アカウントのパスワードの変更方法については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

8.3.4　データベース破損時のデータベースの復元（クラスタ構成の場合）

管理サーバの OS がクラスタ構成の場合に，データベースを復元する手順を説明します。

注意

- 実行系ノード（`cluster.conf` ファイルの `mode` に `online` が設定されているマシン）でデータベースを復元してください。
- データベースの復元では, Device Manager のサービスの停止を伴う操作を実行します。復元中は，Device Manager にアクセスしないでください。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して，HA Command Suite 製品のサービスをオフラインにします。

   ＜ HA Command Suite 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のリソースグループに登録された HA Command Suite 製品のサービスをオフラインにして，フェールオーバーを抑止するためのオプションです。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。

   `r`

   リソースグループ名を指定します。

2. `hcmds64dbrepair` コマンドを実行してデータベースを復元します。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64dbrepair /trans` *＜エクスポートファイル＞*

   `trans`

   `hcmds64dbtrans` コマンドでエクスポート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。

3. 実行系ノードおよび待機系ノードで，Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を設定します。

4. HA Command Suite 製品のサービスを停止します。

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

   ＜ HA Command Suite 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されたリソースグループをオンラインにして，フェールオーバーを有効にするためのオプションです。

   r

   リソースグループ名を指定します。

6. 実行系ノードおよび待機系ノードで，Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
7. Device Manager の GUI でストレージシステムをリフレッシュします。
8. Device Manager の GUI で，Device Manager のタスクの状態を確認します。

   完了していない，またはエラーになっているタスクがあれば，必要に応じてタスクを再作成するか，実行スケジュールを変更してください。

9. `System` アカウントのパスワードはデータベースの復元によって設定が初期化されるため，必要に応じて再設定します。

   `System` アカウントのパスワードの変更方法については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

関連リンク

Device Manager のサービスの停止（134 ページ）
クラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス（136 ページ）

8.4　データベースの移行

HA Command Suite 製品を長期間使用していると，HA 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。

HA 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，HA 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，HA 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，次に示すような，使用中の管理サーバとは異なる環境のマシンにもデータベースを移行できます。

- 異なるプラットフォームのマシンへの移行
- HA Command Suite 製品のインストール先が異なるマシンへの移行
- HA 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

8.4.1　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 HA Command Suite 製品のユーザー情報についての注意事項を次に示します。

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 HA Command Suite 製品のユーザー情報があるマシンへの移行は行わないでください。
- 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 HA 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。

8.4.2　データベースを移行する流れ

データベースを移行する手順の流れは次のとおりです。

操作手順

1. 移行先サーバに，データベースを移行する HA Command Suite 製品をインストールします。
2. `hcmds64dbtrans` コマンドで移行元サーバでデータベースをエクスポートします。
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します。
4. `hcmds64dbtrans` コマンドで移行先サーバでデータベースをインポートします。

   以降で，各手順の詳細を説明します。

8.4.3　移行先サーバへの HA 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 HA Command Suite 製品を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ない HA 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 HA Command Suite 製品を漏れなく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 HA Command Suite 製品のバージョンは，移行元の HA Command Suite 製品と同じか，それ以上にしてください。移行先にインストールされている HA 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。

8.4.4　移行元サーバでデータベースをエクスポートする（非クラスタ構成の場合）

管理サーバが非クラスタ構成の場合に，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。

HA Command Suite 製品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ディレクトリと，アーカイブファイルを格納するディレクトリが必要です。それぞれのディレクトリには，次に示すディレクトリの合計サイズと同等の容量を確保してください。

- インストールされている HA Command Suite 製品の各データベースの格納先ディレクトリ
- HA Command Suite 共通コンポーネントのデータベースの格納先ディレクトリから `SYS` ディレクトリ以下を除いたもの

注意

- 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。
- データベースのエクスポートでは，Device Manager のサービスの停止を伴う操作を実行します。エクスポート中は，Device Manager にアクセスしないでください。

操作手順

1. Administrator 権限のユーザーで管理サーバにログインします。
2. `hcmds64dbtrans` 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。

   ＜ HA Command Suite 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`

   `workpath`

   データベース情報を一時的に配置するための作業用ディレクトリを，絶対パスで指定します。ローカルディスクのディレクトリを指定してください。

   `workpath` オプションに指定するディレクトリの下には，ファイルおよびサブディレクトリがないことを確認してください。

file

出力されるアーカイブファイルの名称を絶対パスで指定します。

auto

HA Command Suite 製品のサービスを自動的に起動/停止するオプションです。

3. アーカイブファイルを移行先サーバに転送します。

アーカイブファイルを作成できなかった場合，workpath オプションで指定したディレクトリに格納されているファイルをすべて転送してください。このとき，workpath オプションで指定したディレクトリ以下のファイル構成は変更しないでください。

メモ

hcmds64dbtrans コマンドに続けて，以下のコマンドを実行する場合，hcmds64dbtrans コマンドに auto オプションは指定しないでください。

- hcmds64dbtrans
- hcmds64srv /stop または hcmds64srv -stop
- hcmds64db
- hcmds64backups

hcmds64dbtrans コマンドに auto オプションを指定しないときは，hcmds64dbtrans コマンドを実行する前に，以下のコマンドを順に実行してください。また，すべての作業が終了後，hcmds64srv /start コマンドまたは hcmds64srv -start コマンドを実行して，HA Command Suite 製品のサービスを起動します。

1. ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64srv /stop
2. ＜ *HA Command Suite のインストールフォルダ*＞\Base64\bin\hcmds64dbsrv /start

8.4.5 移行元サーバでデータベースをエクスポートする（クラスタ構成の場合）

管理サーバの OS がクラスタ構成の場合に，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説明します。

HA Command Suite 製品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ディレクトリと，アーカイブファイルを格納するディレクトリが必要です。それぞれのディレクトリには，次に示すディレクトリの合計サイズと同等の容量を確保してください。

- インストールされている HA Command Suite 製品の各データベースの格納先ディレクトリ
- HA Command Suite 共通コンポーネントのデータベースの格納先ディレクトリから SYS ディレクトリ以下を除いたもの

注意

- 実行系ノード（`cluster.conf` ファイルの `mode` に `online` が設定されているマシン）でデータベースをエクスポートしてください。
- 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。
- データベースのエクスポートでは，Device Manager のサービスの停止を伴う操作を実行します。エクスポート中は，Device Manager にアクセスしないでください。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して，HA Command Suite 製品のサービスをオフラインにします。

   ＜ HA Command Suite 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のリソースグループに登録された HA Command Suite 製品のサービスをオフラインにして，フェールオーバーを抑止するためのオプションです。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。

   `r`

   リソースグループ名を指定します。

   上記コマンドにより，HA Command Suite 製品のサービスが停止されます。

2. 次のコマンドを実行して，HiRDB サービスを起動します。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64dbsrv /start`

3. `hcmds64dbtrans` 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。

   ＜ HA Command Suite 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＞*

`workpath`

データベース情報を一時的に配置するための作業用フォルダを，絶対パスで指定します。ローカルディスクのフォルダを指定してください。`workpath` オプションに指定するフォルダの下には，ファイルおよびサブフォルダがないことを確認してください。

`file`

出力されるアーカイブファイルの名称を絶対パスで指定します。

4. アーカイブファイルを移行先サーバに転送します。

   アーカイブファイルを作成できなかった場合，`workpath` オプションで指定したフォルダに格納されているファイルをすべて転送してください。このとき，`workpath` オプション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. 次のコマンドを実行して，HiRDB サービスを停止します。

   ＜ *HA Command Suite のインストールフォルダ*＞`\Base64\bin\hcmds64dbsrv /stop`

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

   ＜ *HA Command Suite 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されたリソースグループをオンラインにして，フェールオーバーを有効にするためのオプションです。

`r`

リソースグループ名を指定します。

上記コマンドにより，HA Command Suite 製品のサービスが起動されます。

関連リンク

Device Manager のサービスの停止（134 ページ）
クラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス（136 ページ）

8.4.6　移行先サーバでデータベースをインポートする（非クラスタ構成の場合）

管理サーバが非クラスタ構成の場合に，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。

注意

データベースのインポートでは，Device Manager のサービスの停止を伴う操作を実行します。インポート中は，Device Manager にアクセスしないでください。

操作手順

1. Administrator 権限のユーザーで管理サーバにログインします。
2. 移行元の管理サーバでプロパティにデフォルト値以外を設定していた場合は，必要に応じて，移行先サーバのプロパティファイルの設定値を見直してください。

   データベースをインポートしても，プロパティファイルは移行先サーバに引き継がれません。
3. `hcmds64dbtrans` コマンドを実行してデータベースをインポートします。

   ＜*HA Command Suite 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|`＜*データベースを移行する HA Command Suite 製品の名称*＞`} /auto`

   `workpath`

   アーカイブファイルを使用してインポートする場合：

   アーカイブファイルを展開するためのディレクトリを，絶対パスで指定します。ローカルディスクのディレクトリを指定してください。アーカイブファイルを使用する場合，`file` オプションの指定は必須です。

   `workpath` オプションに指定するディレクトリの下には，ファイルおよびサブディレクトリがないことを確認してください。

   アーカイブファイルを使用しないでインポートする場合：

   移行元から転送したデータベース情報を格納したディレクトリを指定してください。転送したディレクトリ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。

   `file`

   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。`workpath` に指定したディレクトリに移行元から転送したデータベース情報が格納されている場合，このオプションを指定する必要はありません。

   `type`

   `ALL` を指定してください。

auto

HA Command Suite 製品のサービスを自動的に起動/停止するオプションです。

4. Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。

   `hcmds64dbtrans` コマンドでは，ユーザー情報以外の HA Command Suite 共通コンポーネントのリポジトリーを移行しないため，インポートした Device Manager のデータベースの情報に合わせてリポジトリーの情報を同期する必要があります。

5. 移行先の HA Command Suite 製品のサービスを起動します。

6. Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。

7. 次の場合には，Device Manager の GUI でストレージシステムをリフレッシュします。

   - データベースをエクスポートしてから，インポートするまでの間にストレージシステムの構成を変更したとき

     構成を変更したストレージシステムをリフレッシュします。

   - 移行元と移行先で管理サーバにインストールされた HA Command Suite 製品のバージョンが異なるとき

     Device Manager に登録されたすべてのストレージシステムをリフレッシュします。

8. データベースをバックアップします。

   障害が発生した場合に備えて，インポート直後のデータベースをバックアップしておくことをお勧めします。

関連リンク

Device Manager のサービスの起動（134 ページ）
データベースのバックアップ（非クラスタ構成の場合）（138 ページ）

8.4.7　移行先サーバでデータベースをインポートする（クラスタ構成の場合）

管理サーバの OS がクラスタ構成の場合に，移行先サーバでデータベースをインポートする手順を説明します。

注意

- 実行系ノード（`cluster.conf` ファイルの `mode` に `online` が設定されているマシン）でデータベースをインポートしてください。
- データベースのインポートでは，Device Manager のサービスの停止を伴う操作を実行します。インポート中は，Device Manager にアクセスしないでください。

前提条件

- Administrator 権限でのログイン
- プロパティファイルの設定値の見直し（移行先の実行系ノードおよび待機系ノード）

  データベースをインポートしても，プロパティファイルは移行先サーバに引き継がれません。このため，移行元の管理サーバでプロパティにデフォルト値以外を設定していた場合は，必要に応じて設定値を見直してください。

操作手順

1. 次のコマンドを実行して，HA Command Suite 製品のサービスをオフラインにします。

   ＜ *HA Command Suite 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のリソースグループに登録された HA Command Suite 製品のサービスをオフラインにして，フェールオーバーを抑止するためのオプションです。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。

   `r`

   リソースグループ名を指定します。

2. `hcmds64dbtrans` コマンドを実行してデータベースをインポートします。

   ＜ *HA Command Suite 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|`＜*データベースを移行する HA Command Suite 製品の名称*＞`} /auto`

   `workpath`

   アーカイブファイルを使用してインポートする場合：

   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フォルダを指定してください。アーカイブファイルを使用する場合，`file` オプションの指定は必須です。

   `workpath` オプションに指定するフォルダの下には，ファイルおよびサブフォルダがないことを確認してください。

   アーカイブファイルを使用しないでインポートする場合：

   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。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。また，`file` オプションは指定しないでください。

file

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。workpath に指定したフォルダに移行元から転送したデータベース情報が格納されている場合，このオプションを指定する必要はありません。

type

ALL を指定してください。

auto

HA Command Suite 製品のサービスを自動的に起動/停止するオプションです。

3. 実行系ノードおよび待機系ノードで，Device Manager サーバの server.base.initialsynchro プロパティに true を指定します。

   hcmds64dbtrans コマンドでは，ユーザー情報以外の HA Command Suite 共通コンポーネントのリポジトリーを移行しないため，インポートした Device Manager のデータベースの情報に合わせてリポジトリーの情報を同期する必要があります。

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

   ＜HA Command Suite 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されたリソースグループをオンラインにして，フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。

5. 実行系ノードおよび待機系ノードで，Device Manager サーバの server.base.initialsynchro プロパティを false に戻します。

6. 次の場合には，Device Manager の GUI でストレージシステムをリフレッシュします。

   - データベースをエクスポートしてから，インポートするまでの間にストレージシステムの構成を変更したとき

     構成を変更したストレージシステムをリフレッシュします。

   - 移行元と移行先で管理サーバにインストールされた HA Command Suite 製品のバージョンが異なるとき

     Device Manager に登録されたすべてのストレージシステムをリフレッシュします

7. データベースをバックアップします。

関連リンク

Device Manager のサービスの起動（134 ページ）
クラスタ管理アプリケーションに登録されている HA Command Suite 製品のサービス（136 ページ）
データベースのバックアップ（クラスタ構成の場合）（139 ページ）

第 9 章
Device Manager の監査ログ

この章では，Device Manager の監査ログを採取するために必要な設定や，監査ログで確認できる情報について説明します。

9.1　監査ログを採取するために必要な設定

HA Command Suite 製品では，法規制やセキュリティ評価基準，業界ごとの各種基準などに従っていることを監査者や評価者に証明するために，監査ログにユーザーの操作内容を記録できます。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。環境設定ファイルについては，「9.1.2　監査ログの環境設定ファイルの編集（164 ページ）」を参照してください。

監査ログは，イベントログファイル（アプリケーションログファイル）に出力されます。

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 9-1　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，HA 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	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。 • NTP サーバや DNS サーバなどとの通信 • 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は認証を試みて成功または失敗したことを示す事象。 • Fibre Channel ログイン • 機器認証（Fibre Channel - Security Protocol 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
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。

種別	説明
	• 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。

また，監査ログの出力内容については「9.2　監査ログの確認（165 ページ）」を参照してください。

9.1.1　監査ログに出力される監査事象

Device Manager では，次の種別の監査事象が監査ログに出力されます。

- StartStop
- Authentication
- ConfigurationAccess
- AccessControl
- ExternalService

それぞれの監査事象には，重要度（Severity）が設定されています。重要度によって，出力する監査ログをフィルタリングできます。

Device Manager で監査ログに出力される監査事象を「表 9-2　監査ログに出力される監査事象（種別が StartStop の場合）（159 ページ）」～「表 9-5　監査ログに出力される監査事象（種別が ExternalService の場合）（163 ページ）」に示します。

表 9-2　監査ログに出力される監査事象（種別が StartStop の場合）

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

種別の説明	監査事象	Severity	メッセージ ID
	SSO サーバの停止	6	KAPM00092-I

表 9-3　監査ログに出力される監査事象（種別が Authentication の場合）

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
SNMP v3 トラップ受信時のユーザー認証	ユーザー認証の成功	6	KAIC52000-I
	ユーザー認証の失敗	3	KAIC52100-E

表 9-4　監査ログに出力される監査事象（種別が ConfigurationAccess の場合）

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
ユーザーの削除（GUI）	単一ユーザーの削除成功	6	KAPM07231-I
	単一ユーザーの削除失敗	3	KAPM07240-E
	複数ユーザーの削除成功	6	KAPM07231-I
	複数ユーザーの削除失敗	3	KAPM07240-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
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
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
権限の変更	権限の変更成功	6	KAPM02280-I

種別の説明	監査事象	Severity	メッセージ ID
	権限の変更失敗	3	KAPM07240-E
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
	`hcmds64unlockaccount` コマンドによるアカウントのロック解除成功	6	KAPM07236-I
	`hcmds64unlockaccount` コマンドによるアカウントのロック解除失敗	3	KAPM07240-E
認証方式変更	認証方式の変更成功	6	KAPM02452-I
	認証方式の変更失敗	3	KAPM02453-E
認可グループの追加 （GUI）	認可グループの追加成功	6	KAPM07247-I
	認可グループの追加失敗	3	KAPM07248-E
認可グループの削除 （GUI）	単一認可グループの削除成功	6	KAPM07249-I
	単一認可グループの削除失敗	3	KAPM07248-E
	複数認可グループの削除成功	6	KAPM07249-I
	複数認可グループの削除失敗	3	KAPM07248-E
認可グループの権限変更 （GUI）	認可グループの権限変更成功	6	KAPM07250-I
	認可グループの権限変更失敗	3	KAPM07248-E
ユーザーの登録 （GUI）	ユーザーの登録成功	6	KAPM07241-I
	ユーザーの登録失敗	3	KAPM07242-E
ユーザー情報の更新 （GUI）	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
ユーザーの削除 （GUI）	ユーザーの削除成功	6	KAPM07245-I
	ユーザーの削除失敗	3	KAPM07246-E
認可グループの登録 （GUI）	認可グループの登録成功	6	KAPM07251-I
	認可グループの登録失敗	3	KAPM07252-E
認可グループの削除 （GUI）	認可グループの削除成功	6	KAPM07253-I
	認可グループの削除失敗	3	KAPM07254-E
認可グループの権限変更 （GUI）	認可グループの権限変更成功	6	KAPM07255-I
	認可グループの権限変更失敗	3	KAPM07256-E
データベースのバックアップまたはリストア	`hcmds64backups` コマンドまたは `hcmds64db` コマンドによるバックアップ成功	6	KAPM05561-I
	`hcmds64backups` コマンドまたは `hcmds64db` 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

種別の説明	監査事象	Severity	メッセージ ID
	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
データベースのエクスポートまたはインポート	データベースのエクスポートに成功	6	KAPM06543-I
	データベースのエクスポートに失敗	3	KAPM06544-E
	データベースのインポートに成功	6	KAPM06545-I
	データベースのインポートに失敗	3	KAPM06546-E
データベース領域の作成または削除	データベース領域の作成成功	6	KAPM06348-I
	データベース領域の作成失敗	3	KAPM06349-E
	データベース領域の削除成功	6	KAPM06350-I
	データベース領域の削除失敗	3	KAPM06351-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
Device Manager サーバの処理	リクエスト受理（正常時）	6	KAIC51000-I KAIC51200-I KAIC51201-I
	リクエスト受理（共通・異常時）	3	KAIC51400-E
	レスポンス送信（正常時）	6	KAIC51100-I KAIC51300-I KAIC51301-I KAIC51302-I
	レスポンス送信（異常時）	3	KAIC51500-E KAIC51700-E KAIC51701-E
タスクに対する操作 （GUI）	タスク操作の成功	6	KAIC15984-I
	タスク操作の失敗	3	KAIC15985-E
ストレージシステムの構成変更 （GUI）	ストレージシステムの構成変更に成功	6	KAIC15986-I
	ストレージシステムの構成変更に失敗	3	KAIC15987-E
関連製品の起動（ラウンチ）	リクエスト受理（正常時）	6	KAIC53000-I
	リクエスト受理（異常時）	3	KAIC53200-E
	レスポンス送信（正常時）	6	KAIC53100-I
	レスポンス送信（異常時）	3	KAIC53300-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。

表 9-5　監査ログに出力される監査事象（種別が ExternalService の場合）

種別の説明	監査事象	Severity	メッセージ ID
外部認証サーバとの通信	LDAP ディレクトリサーバとの通信成功	6	KAPM10116-I
	LDAP ディレクトリサーバとの通信失敗	3	KAPM10117-E
	RADIUS サーバとの通信成功	6	KAPM10118-I
	RADIUS サーバとの通信失敗（応答なし）	3	KAPM10119-E
	Kerberos サーバとの通信成功	6	KAPM10120-I
	Kerberos サーバとの通信失敗（応答なし）	3	KAPM10121-E
	DNS サーバとの通信成功	6	KAPM10122-I
	DNS サーバとの通信失敗（応答なし）	3	KAPM10123-E
外部認証サーバとの認証	LDAP ディレクトリサーバとの TLS ネゴシエーションに成功	6	KAPM10124-I
	LDAP ディレクトリサーバとの TLS ネゴシエーションに失敗	3	KAPM10125-E
	LDAP ディレクトリサーバでの情報検索用ユーザーの認証成功	6	KAPM10126-I
	LDAP ディレクトリサーバでの情報検索用ユーザーの認証失敗	3	KAPM10127-W
外部認証サーバでのユーザー認証	LDAP ディレクトリサーバでのユーザーの認証成功	6	KAPM10128-I
	LDAP ディレクトリサーバにユーザーが存在しない	4	KAPM10129-W
	LDAP ディレクトリサーバでのユーザーの認証失敗	4	KAPM10130-W
	RADIUS サーバでのユーザーの認証成功	6	KAPM10131-I
	RADIUS サーバでのユーザーの認証失敗	4	KAPM10132-W
	Kerberos サーバでのユーザーの認証成功	6	KAPM10133-I
	Kerberos サーバでのユーザーの認証失敗	4	KAPM10134-W
外部認証サーバから情報取得	LDAP ディレクトリサーバからユーザー情報の取得に成功	6	KAPM10135-I
	LDAP ディレクトリサーバからユーザー情報の取得に失敗	3	KAPM10136-E
	DNS サーバから SRV レコードの取得に成功	6	KAPM10137-I
	DNS サーバから SRV レコードの取得に失敗	3	KAPM10138-E

メッセージテキストの出力形式については「9.3　監査ログのメッセージ部に出力されるメッセージテキスト（167 ページ）」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『HA Command Suite メッセージ』を参照してください。

9.1.2　監査ログの環境設定ファイルの編集

HA Command Suite 製品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` に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。

監査ログの環境設定ファイルの変更を反映するには，HA Command Suite 製品のサービスを再起動する必要があります。

注意

監査ログは大量に出力されるおそれがあるので，ログサイズの変更，採取したログの退避，保管などを実施してください。

`auditlog.conf` ファイルの格納先を次に示します。

< HA Command Suite のインストールフォルダ>`\Base64\conf\sec\auditlog.conf`

`auditlog.conf` ファイルに設定する項目を次の表に示します。

表 9-6　auditlog.conf ファイルに設定する項目

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。その場合，種別とコンマの間はスペースを空けずに詰めて指定してください。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，「表 9-2　監査ログに出力される監査事象（種別が StartStop の場合）（159 ページ）」～「表 9-5　監査ログに出力される監査事象（種別が ExternalService の場合）（163 ページ）」を参照してください。大文字，小文字は区別されません。指定できる種別以外の名称を指定した場合は，無視されます。 デフォルト値：指定なし
`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を持つ監査事象が，イベントログファイルに出力されます。 HA Command Suite 製品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，「表 9-2　監査ログに出力される監査事象（種別が StartStop の場合）（159 ページ）」～「表 9-5　監査ログに出力される監査事象（種別が ExternalService の場合）（163 ページ）」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の対応については，「表 9-7　監査事象の重要度とイベントログの種類の対応（165 ページ）」を参照してください。 指定できる値以外の数値，または，数値以外の文字を指定した場合は，デフォルト値が仮定されます。 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，イベントログの種類の対応を示します。

表 9-7　監査事象の重要度とイベントログの種類の対応

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 の監査事象が出力されます。「エラー」，「警告」および「情報」の監査ログが出力されます。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

9.2　監査ログの確認

Windows のイベントログに次の形式で出力されます。また，イベントログのソースは "HBase64 Event"，イベント ID は"1"です。

```
<プログラム名> [<プロセス ID >]: <メッセージ部>
```

*<メッセージ部>*の出力形式と内容を説明します。

メモ

*<メッセージ部>*には，半角で 953 文字まで表示されます。

メッセージ部の出力形式

＜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 9-8　メッセージ部に出力される情報

項目※	内容
統一識別子	「CELFSS」固定
統一仕様リビジョン番号	「1.1」固定
通番	監査ログのメッセージの通番
メッセージ ID	メッセージ ID 詳細については，「9.1.1　監査ログに出力される監査事象（159 ページ）」を参照してください。
日付・時刻	メッセージが出力された日付と時刻 「*yyyy-mm-dd*T*hh*:*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
検出場所	ホスト名
監査事象の種別	事象の種別
監査事象の結果	事象の結果
監査事象の結果サブジェクト識別情報	事象に応じた，アカウント ID，プロセス ID または IP アドレス
ハードウェア識別情報	ハードウェアの型名や製番
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
ロケーション識別情報	ロケーション識別情報
FQDN	完全修飾ドメイン名
冗長化識別情報	冗長化識別情報
エージェント情報	エージェント情報
リクエスト送信元ホスト	リクエストの送信元のホスト名
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
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
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
一括操作識別子	プログラム内で操作の通番
ログ種別情報	「BasicLog」または「DetailLog」
アプリケーション識別情報	プログラムの識別情報
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	監査事象に応じた内容 表示できない文字は，アスタリスク（*）に置き換えて出力されます。詳細については，「9.3　監査ログのメッセージ部に出力されるメッセージテキスト（167 ページ）」を参照してください。

注※

監査事象によっては，出力されない項目もあります。

監査事象「ログイン」で出力されるメッセージ部の例

```
CELFSS,1.1,0,KAPM01124-I,2006-05-15T14:08:23.1+09:00,HBase-SSO,management-h
ost,Authentication,Success,uid=system,,,,,,,,,,,,BasicLog,,,"The login was
successful. (session ID = ＜セッション ID＞)"
```

9.3 監査ログのメッセージ部に出力されるメッセージテキスト

監査ログ中のメッセージ部に出力されるメッセージテキストは，監査事象ごとに形式が異なります。ここでは，監査事象ごとにメッセージテキストの形式を説明します。メッセージテキストの形式で[ ]で囲んだ項目は，出力されないことがあります。

9.3.1 HA Command Suite 共通コンポーネントの処理として出力される場合

発生した監査事象の内容が，文字列で出力されます。

メッセージテキストの詳細については，マニュアル『HA Command Suite メッセージ』を参照してください。次にメッセージテキストの例を示します。

ログイン時の例

```
"The login was successful. (session ID = ＜セッション ID＞)"
```

9.3.2 Device Manager サーバの処理として出力される場合

構成変更，情報取得などのサーバの処理に関するリクエスト受理時，およびレスポンス送信時の情報が出力されます。メッセージテキストの形式とその内容を説明します。

リクエスト受理時（正常時）

```
＜ユニーク ID＞ ＜詳細メッセージ＞
```

レスポンス送信時（正常時）

```
＜ユニーク ID＞ [＜ステータス＞] [＜リクエスト操作開始ユニーク ID＞]
```

リクエスト受理時またはレスポンス送信時（異常時）

```
＜ユニーク ID＞ ＜エラーメッセージ ID＞
```

表 9-9　Device Manager サーバリクエスト受理時またはレスポンス送信時に出力される情報

項目	内容
ユニーク ID	リクエストごとに一意な ID です。レスポンス送信時は，対応するリクエストのユニーク ID です。SVP 経由の処理の場合，この ID は SVP 側の監査ログにも出力されます。
詳細メッセージ	リクエストの詳細な内容です。詳細については，「9.4　監査ログのメッセージ部に出力される詳細メッセージ（169 ページ）」を参照してください。
ステータス	リクエストと操作が非同期である場合，ポーリングの結果を示す文字列です。出力される文字列を次に示します。 • `COMPLETED`：操作成功 • `PROCESSING`：操作中 • `FAILED`：操作失敗
リクエスト操作開始ユニーク ID	リクエストと操作が非同期である場合，リクエストとその操作に対するポーリングの結果を対応付ける一意な ID です。 この ID は，リクエスト受理時の詳細メッセージに，`GetRequestStatus`（コマンド：Get，ターゲット：RequestStatus）の `RequestStatus` エレメントの属性として出力されるメッセージ ID と対応しています。詳細メッセージについては，「9.4　監査ログのメッセージ部に出力される詳細メッセージ（169 ページ）」を参照してください。
エラーメッセージ ID	エラーメッセージ ID です。メッセージ ID の詳細については，マニュアル『HA Command Suite メッセージ』を参照してください。

次に，リクエスト受理時（正常時），および，レスポンス送信時（異常時）に出力されるメッセージテキストの例を示します。

リクエスト受理時（正常時）の例

```
"123456789 AddLUN<SA info='D700-75010421'><Path info=',,0,4,15,0,'><LDEV in
fo='D700-75010421-31,,'/><LDEV info='D700-75010421-34,,'/></Path><Path info
=',,1,1,15,0,31'/><Path info=',,16,6,15,0,31'/><Path info=',,0,4,15,1,35'/>
</SA>"
```

レスポンス送信時（異常時）の例

```
"123456789 KAIC01014-E"
```

9.3.3　Device Manager GUI の処理として出力される場合

発生した監査事象の内容が，文字列で出力されます。

メッセージテキストの詳細については，マニュアル『HA Command Suite メッセージ』を参照してください。次にメッセージテキストの例を示します。

タスク登録時の例

```
The task operation (registerTask) succeeded.(task name=<タスク名>)
```

9.4　監査ログのメッセージ部に出力される詳細メッセージ

Device Manager サーバがリクエストを受理した場合，監査ログのメッセージ部のメッセージテキストに詳細メッセージとして操作内容が出力されます。

詳細メッセージの出力形式を次に示します。[　]で囲んだ項目は，出力されないことがあります。

<コマンド><ターゲット> ［*<オプション>*］［*<パラメーター>*］

詳細メッセージに出力される情報を次の表に示します。

表 9-10　詳細メッセージに出力される情報

項目	内容
コマンド	リソースに対しての操作（追加，削除，変更，参照など）を表す文字列（3 文字）です。出力される文字列の意味については，「9.4.1　詳細メッセージに出力されるコマンド（169 ページ）」を参照してください。
ターゲット	操作内容を特定する情報です。出力されるターゲットとその内容については，「9.4.2　詳細メッセージに出力されるターゲット（169 ページ）」を参照してください。
オプション	操作内容を特定する情報です。オプションが指定されたときだけ出力されます。 複数のオプションが指定された場合，セミコロン（;）で区切って出力されます。
パラメーター	操作内容，対象リソースを特定する情報です。リクエストで指定されたときだけ出力されます。タグ形式で出力されます。

出力される情報について項目ごとに以降で説明します。

9.4.1　詳細メッセージに出力されるコマンド

詳細メッセージに出力されるコマンドを次の表に示します。

表 9-11　詳細メッセージに出力されるコマンド

出力文字列	正式名	操作
`Get`	Get	取得

9.4.2　詳細メッセージに出力されるターゲット

詳細メッセージに出力されるターゲットの内容を次の表に示します。

表 9-12　詳細メッセージに出力されるターゲット

出力文字列	正式名	操作内容
`SrvI`	ServerInfo	Device Manager サーバの情報取得

注

表中にない文字が出力されることもあります。

第 10 章
トラブルシューティング

この章では，Device Manager の運用中に発生した問題の解決策や保守情報の取得方法について説明します。

10.1　管理サーバで発生したトラブルへの対処方法（Device Manager）

Device Manager に起因するトラブルが発生した場合の対処方法を示します。

10.1.1　Device Manager の GUI にログインできない

Device Manager の GUI にログインできない場合, ユーザーアカウントのロックを解除してください。

要因

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。

対処方法

User Management の `Admin` 権限を持っていないユーザーの場合：

User Management の `Admin` 権限を持つユーザーに，アカウントのロックを解除するよう依頼してください。

User Management の `Admin` 権限を持っているユーザーの場合：

User Management の `Admin` 権限を持つほかのユーザーにアカウントのロックを解除するよう依頼するか，`hcmds64unlockaccount` コマンドを実行して自分自身のアカウントのロックを解除してください。

関連リンク

アカウントロックの解除（29 ページ）

10.1.2　HA Command Suite 共通コンポーネントまたは Device Manager サーバのサービスを起動できない

HA Command Suite 共通コンポーネントまたは Device Manager サーバのサービスを起動できない場合，デスクトップヒープの領域を変更してください。

要因

デスクトップヒープが不足しているおそれがあります。

対処方法

レジストリーを編集して，デスクトップヒープの領域を変更してください。

デスクトップヒープの領域の変更方法については，Microsoft 社の Web サイトを参照してください。

10.1.3　管理サーバの起動後や HA Command Suite 製品のサービスの起動後に Device Manager サーバにアクセスできない

管理サーバの起動後や HA Command Suite 製品のサービスの起動後に，GUI から Device Manager サーバにアクセスできない場合，Device Manager のデータベースへの接続リトライ回数とリトライ間隔を延長してください。

要因

Device Manager トレースログファイルに KAIC03100-E が出力されている場合，Device Manager サーバからデータベースへの接続処理がタイムアウトしています。

対処方法

Device Manager のデータベースへの接続リトライ回数とリトライ間隔を延長します。

Device Manager サーバの `database.properties` ファイルにある，次のプロパティの値を変更してください。

- `dbm.startingCheck.retryCount`
- `dbm.startingCheck.retryPeriod`

関連リンク

Device Manager サーバのプロパティの変更（178 ページ）
dbm.startingCheck.retryCount（186 ページ）
dbm.startingCheck.retryPeriod（186 ページ）

10.2　トラブル発生時に採取が必要な保守情報

障害要因を特定できない場合や，障害を回復できない場合には，保守情報を収集して，PP サポートサービスに連絡してください。

トラブル発生時には，原因特定のために次の情報が必要です。

- 障害に伴うシステムの状況
- 障害の発生日時
- 障害の発生場面
- 管理サーバやホストなどのネットワーク構成
- 管理サーバやホストなどの OS
- 障害が発生したマシンの保守情報
  - 管理サーバの保守情報
- Java VM のスレッドダンプ

  次に示す問題が発生した場合，原因を見つけるために Device Manager Web Service のスレッドダンプが必要になります。
  - GUI を起動しても Device Manager ログインウィンドウが表示されない
  - Device Manager へのログイン後，Device Manager メインウィンドウが表示されない
- ストレージシステムダンプ

  ストレージシステムの障害を示すメッセージではない場合でも，障害内容によっては，ストレージシステムと合わせて調査が必要になります。

  下記のメッセージの障害が発生した場合，ストレージシステムのダンプ（詳細ダンプファイル）を併せて採取してください。

  ストレージシステムのダンプファイルの採取方法については,『システム管理者ガイド』または『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。
  - KAIC05601-E
  - KAIC05607-E
  - KAIC05610-E
  - KAIC05934-E
  - KAIC06400-E
  - KAIC06450-E
  - KAIC06500-E
  - KAIC17014-E
  - KAIC17015-E

- KAIC63501-E

上記のメッセージ以外でも，障害対応窓口の判断によって，ストレージシステムのダンプが必要になることがあります。

10.2.1　管理サーバの保守情報の取得（hcmds64getlogs コマンド）

管理サーバの保守情報を取得するには，`hcmds64getlogs` コマンドを実行します。

事前に完了しておく操作

- Administrator 権限でのログイン

コマンドの形式

＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64getlogs /dir` *＜フォルダ名＞* `[/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＞* `...]]`

注意

`hcmds64getlogs` コマンドは，2 つ以上同時に実行しないでください。

オプション

`dir`

採取した保守情報を格納するローカルディスク上のディレクトリを絶対パスで指定します。あらかじめディレクトリを作成している場合は，ディレクトリを空にしてください。

指定できるパスの最大長は 41 バイトです。パスには一部の特殊文字を除いた ASCII 印字可能文字コードを指定できます。指定できない特殊文字を示します。

`\ / : , ; * ? " < > | $ % & ' ``

ただし，パスの区切り文字として，円記号（`\`），コロン（`:`）およびスラント（`/`）を使用できます。パスの末尾にはパスの区切り文字を指定しないでください。

パス中に空白を指定するときは，パスを引用符（`"`）で囲んで指定してください。

`arc`

作成されるアーカイブファイルの名前を指定します。このオプションを省略した場合，ファイル名は「`HiCommand_log_64`」になります。

ファイル名には一部の特殊文字を除いた ASCII 印字可能文字コードを指定できます。指定できない特殊文字を次に示します。

`\ / : , ; * ? " < > | $ % & ' ``

logtypes

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，空白文字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。

このコマンドを実行すると，メッセージ KAPM05318-I または KAPM05319-E が出力されます。 また，保守情報（ログファイルとデータベースファイル）が取得され，dir オプションで指定したディレクトリの下に 4 つのアーカイブファイル（.jar，.hdb.jar，.db.jar および.csv.jar）が作成されます。

ヒント

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ディレクトリ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ディレクトリ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。

10.2.2　Device Manager Web Service のスレッドダンプ取得

Device Manager Web Service のスレッドダンプを取得するには，dump という名前のファイルを作成したあと，Device Manager Web Service を再起動します。

操作手順

1. ＜ *HA Command Suite のインストールフォルダ*＞\Base64\uCPSB11\CC\server\public\ejb\DeviceManagerWebService 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］ウィンドウにアクセスします。
3. Device Manager Web Service を停止します。
4. ［サービス］ウィンドウから，Device Manager Web Service を開始します。

操作結果

javacore*xxx*.*xxxx*.txt ファイルが次のフォルダへ出力されます。

＜*HA Command Suite のインストールフォルダ*＞`\Base64\uCPSB11\CC\server\public\ejb\DeviceManagerWebService`

付録 A.　Device Manager サーバのプロパティ

ここでは，Device Manager サーバのプロパティファイルについて説明します。

A.1　Device Manager サーバのプロパティファイル

Device Manager サーバのプロパティファイルには，Device Manager の構成情報に関するプロパティファイルやデータベースに関するプロパティファイルなどがあります。

Device Manager サーバのプロパティファイルを次の表に示します。

表 A-1　Device Manager サーバのプロパティファイル

プロパティファイル	説明
`server.properties` ファイル	Device Manager サーバの構成情報に関するプロパティファイルです。 **警告：** 専門知識のある方以外は，これらの属性を最適化する操作は実行しないでください。僅かな変更でも Device Manager サーバのパフォーマンスに重大な影響が出るおそれがあります。
`database.properties` ファイル	Device Manager のデータベースに関するプロパティファイルです。 **警告：** 専門知識のある方以外は，これらの属性を最適化する操作は実行しないでください。僅かな変更でも Device Manager サーバのパフォーマンスに重大な影響が出るおそれがあります。
`logger.properties` ファイル	Device Manager のログ出力に関するプロパティファイルです。
`dispatcher.properties` ファイル	Device Manager のスレッドに関するプロパティファイルです。
`mime.properties` ファイル	Device Manager の MIME（Multipurpose Internet Mail Extensions）に関するプロパティファイルです。
`client.properties` ファイル	Device Manager の GUI に関するプロパティファイルです。
`server.properties` ファイル	Device Manager のセキュリティに関するプロパティファイルです。
`customizedsnmptrap.properties` ファイル	Device Manager の SNMP トラップのログ出力に関するプロパティファイルです。
`launchapp.properties` ファイル	Device Manager からラウンチするアプリケーションに関するプロパティファイルです。

注意

- 通常，Device Manager サーバのプロパティファイルの設定値は特に変更する必要はありません。

  値を変更すると，サーバの故障や不具合の原因となることがあるので，十分に注意してください。結果の予測に必要な専門知識がないユーザーは，値を変更しないでください。
- デフォルト値は新規インストールした際に設定される値です。

- 上書きインストールまたはアップグレードインストールした場合，Device Manager サーバのプロパティファイルの設定値は，インストール前の値が引き継がれます。

A.1.1 Device Manager サーバのプロパティの変更

Device Manager サーバのプロパティファイルは，テキストエディターを使用して編集します。

前提条件

Administrator 権限でのログイン

操作手順

1. HA Command Suite 製品のサービスを停止します。
2. テキストエディターで，Device Manager サーバのプロパティファイルに適切な値を設定します。
3. HA Command Suite 製品のサービスを起動します。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）

A.1.2 Device Manager サーバのプロパティファイルの記述規則

プロパティファイルは，Java プロパティファイル形式です。

プロパティファイルは，次の記述規則に従って作成されている必要があります。

- 各プロパティは，`foo.bar=12345` のように，「=」で区切られた名前と値の対で指定します。
- 個々のプロパティは，行区切り文字（改行）で区切ります。
- 行頭に番号記号（#）がある場合，その行は注釈行になります。
- リテラル（文字列または数値）を引用符で囲む必要はありません。
- 円記号（\）はエスケープ文字を表す予約文字になります。Windows では，絶対パス名を表すときに円記号（\）を含むので，「\\」と指定する必要があります。

  例えば，ファイルパス名 `C:\Server\docroot\foo.bar` は，`C:\\Server\\docroot\\foo.bar` と入力します。プロパティの指定では，そのほかの文字にはエスケープ文字「\」を付ける必要はありません。

- プロパティファイル内に同じプロパティ名で複数の設定がされている場合，ファイルの最後に設定したプロパティの値が有効になります。
- 行末に円記号（\）がある場合，次の行は継続行になります。

A.2　Device Manager サーバの構成情報に関するプロパティ（server.properties ファイル）

構成情報に関するプロパティは，`server.properties` ファイルに含まれています。

＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\config\server.properties`

A.2.1　server.http.host

管理サーバ（Device Manager サーバ）のホスト名または IP アドレスを指定します。

IP アドレスを指定する場合の入力形式は次のとおりです。

IPv4 の場合：

x.*x*.*x*.*x*（*x* は 0〜255）

IPv6 の場合：

コロン付きの 16 進数で指定します。省略形も使用できます。使用できる IPv6 アドレスはグローバルアドレスだけです。

ホスト名および IP アドレスは，クライアント（GUI およびストレージシステム）からアクセスできる値を指定する必要があります。

デフォルト：インストール時に指定した管理サーバのホスト名または IP アドレス（URL の登録処理でエラーが発生した場合は `localhost` が設定されます）

注意

- Device Manager がインストールされているサーバマシンが，NIC を複数搭載している場合，クライアント（GUI およびストレージシステム）が接続されているネットワーク側の IP アドレスを指定してください。ホスト名は指定しないでください。
- クラスタ環境の場合は，クラスタ管理 IP アドレスを指定する必要があります。
- 次の場合，このプロパティの設定値を変更したときには，Device Manager GUI の[ストレージシステム編集]画面で，ユーザーアカウント認証を設定し直してください。

  ・iStorage V シリーズを操作する場合

A.2.2 server.http.port

Device Manager サーバが非 SSL で通信する際に使用するポートを指定します。

標準の Web サーバに使用されるポートは通常 80 ですが，このポートですでにイントラネットサーバが稼働しているおそれがあります。ほかのサービ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。

このプロパティにスペースを設定すると，ポートに 80 が割り当てられます。

デフォルト：`2001`

関連リンク

ポップアップブロックの設定変更（109 ページ）

A.2.3 server.https.port

Device Manager サーバが SSL で通信する際に使用するポートを指定します。

セキュア Web サーバ用のポートは通常 443 です。すでにこのポートでセキュアイントラネットサーバが稼働していることがあるため，1024～49151 のポートを専用（ミドルウェア）HTTP サーバに使用することを推奨します。HTTP リスナー用に指定したポートとは異なる値を割り当ててください。

デフォルト：`2443`

注意

次の場合，このプロパティの設定値を変更したときには，Device Manager GUI の[ストレージシステム編集]画面で，ユーザーアカウント認証を設定し直してください。

- iStorage V シリーズを操作する場合

関連リンク

ポップアップブロックの設定変更（109 ページ）

A.2.4 server.rmi.port

Device Manager の RMI サーバ機能が使用するポートを指定します。

ほかのサービ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，1024～65535 のポートを選択します。

デフォルト：`23055`

注意

このプロパティの値を変更した場合は，Device Manager サーバの `client.rmi.port` プロパティも同じ値に変更してください。

関連リンク

client.rmi.port（195 ページ）

A.2.5 server.http.entity.maxLength

Device Manager サーバが許容する HTTP 要求エンティティの最大長をバイト単位で指定します。

通常，この設定を変更する必要はありません。この設定では，異常に大きなデータ量のエンティティを持つ要求を制限することで，サービス妨害攻撃やバッファーのオーバーフローを狙った攻撃を防ぐのに役立ちます。Device Manager サーバがこれより長いポスト要求を検出すると，クライアントにエラー応答を送り，その要求の詳細をログに記録します。

デフォルト：`3000000`

A.2.6 server.base.home

Device Manager のインストーラーによって設定される HA Command Suite 共通コンポーネントのインストールディレクトリです。

通常，この設定を変更する必要はありません。

デフォルト：インストーラーによって設定された値

A.2.7 server.base.initialsynchro

Device Manager の起動時に管理情報データベースと表示情報（HA Command Suite 共通コンポーネントのリポジトリー）を同期するかどうかを指定します。

`true` に設定すると，情報が同期されます。`false` に設定すると，情報は同期されません。

デフォルト：`false`

注意

このプロパティを `true` に設定した場合，情報の同期には，数分掛かることがあります。プロパティを変更してすぐに Device Manager にログインしようとすると，エラーになる場合があります。この場合は，同期が完了するのを待って，ログインしてください。

A.2.8　server.logicalview.initialsynchro

Device Manager サーバを起動した際に，データベース内のストレージシステムの情報と，GUI で表示する情報を強制的に同期するかどうかを指定します。

`true` を指定した場合は同期されます。`false` を指定した場合は同期されません。

デフォルト：`false`

A.2.9　server.mail.enabled.storagesystem

次の内容をユーザーに E メールで通知するかどうかを指定します。

- ストレージシステムのアラート
- Device Manager GUI のイベント
- ヘルスチェック結果

E メールで通知する場合は `true` を指定してください。E メールで通知しない場合は `false` を指定してください。

デフォルト：`true`

注意

このプロパティに `true` を設定した場合は，`server.mail.smtp.host` プロパティも設定してください。

関連リンク

server.mail.smtp.host（182 ページ）

A.2.10　server.mail.from

アラート，イベント，およびヘルスチェック結果をユーザーに E メール通知する場合に，通知元（差出人）のメールアドレスを指定します。

運用環境によっては，ドメイン名がないアドレスからの E メールを受信できないことがあります。プロパティの設定値を変更するか，E メールの設定（SMTP サーバや通知先のメールフィルターなど）を変更してください。

値を指定していない場合または値が不正であった場合は，デフォルト値が設定されます。

デフォルト：`hdvmserver`

A.2.11　server.mail.smtp.host

SMTP サーバのホスト名または IP アドレスを指定します。

アラート，イベント，およびヘルスチェック結果をユーザーに E メール通知する場合に，設定が必要です。IP アドレスを指定する場合，IPv4 または IPv6 のどちらかで指定します。

デフォルト：なし

注意

このプロパティを設定した場合は，`server.mail.enabled.storagesystem` または `server.mail.enabled.fileserver` プロパティに `true` を指定してください。

関連リンク

server.mail.enabled.storagesystem（182 ページ）

A.2.12 server.mail.smtp.port

SMTP サーバのポート番号を指定します。

アラート，イベント，およびヘルスチェック結果をユーザーに E メール通知する場合に，設定が必要です。

指定できる値の範囲は 0～65535 です。

デフォルト：`25`

A.2.13 server.mail.smtp.auth

アラート，イベント，およびヘルスチェック結果をユーザーに E メール通知する場合に，SMTP 認証を使用するかどうかを指定します。

SMTP 認証を使用する場合は `true` を指定してください。SMTP 認証を使用しない場合は `false` を指定してください。

デフォルト：`false`

A.2.14 server.mail.errorsTo

アラート，イベント，およびヘルスチェック結果の通知メールが配信エラーとなったときに送信される配信不能通知の送信先メールアドレスを指定します。

このプロパティを指定していない場合は，Device Manager サーバの `server.properties` ファイルの `server.mail.from` に指定したメールアドレスに送信されます。ただし，配信不能通知が送信される条件は，SMTP サーバの設定によって異なります。SMTP サーバの設定を確認してください。

デフォルト：なし

関連リンク

server.mail.from（182 ページ）

A.2.15 server.eventNotification.mail.to

アラートおよびイベントの通知メールの送信先メールアドレスを指定します。

このプロパティに設定するメールアドレスには，すべてのアラートおよびイベントについて，E メール通知されます。

デフォルト：なし

A.2.16 server.mail.alert.type.storagesystem

ストレージシステムのアラートをユーザーに E メール通知する場合に，通知するアラートのタイプを指定します。

指定できる値は次のとおりです。

- `Trap`：SNMP トラップで検知した障害情報だけを通知します。
- `Server`：Device Manager によるポーリングで検知した障害情報だけを通知します。
- `All`：SNMP トラップで検知した障害情報と，Device Manager によるポーリングで検知した障害情報の両方を通知します。同じ障害であっても，SNMP トラップで検知した障害情報と Device Manager によるポーリングで検知した障害情報の両方について，それぞれ E メールが送信されます。

デフォルト：`Trap`

A.2.17 server.mail.alert.status

アラートをユーザーに E メール通知する場合に，通知するアラートの重要度を指定します。

Device Manager サーバはこのプロパティで指定した重要度以上のアラートを通知します。指定できる値は，重要度の低い順に，`Normal`，`Service`，`Moderate`，`Serious`，`Acute` です。

デフォルト：`Moderate`

A.2.18 server.subsystem.ssid.availableValues

Device Manager でボリュームを作成する際，ストレージシステムに対して自動的に設定する SSID の値の範囲を指定します。

このプロパティは，iStorage V シリーズで有効です。

指定できる値は次のとおりです。

- 4～FFFD の 16 進数：連続した複数の値を指定する場合は，ハイフン（-）で範囲を指定します。連続していない複数の値を指定する場合は，コンマ（,）で区切って指定します。大文字小文字は区別されません。範囲が重複して指定されている場合，その論理和を指定値とします。
- `All`：`All` を指定すると，指定できる全範囲を指定することになります。大文字小文字は区別されません。

値を指定しない場合，SSID の自動設定は行いません。

デフォルト：`All`

A.2.19 server.agent.differentialrefresh.manual.enabled

ストレージシステムの手動リフレッシュ時に，前回のリフレッシュ時点から構成に変化があったリソースについてだけ，データベースの情報を更新するかどうかを指定します。

このプロパティは，リフレッシュ対象のストレージシステムが iStorage V シリーズの場合だけ有効です。

`true` を指定した場合，前回のリフレッシュ時点から構成に変化がないリソースについてはデータベースの更新が省略されるため，リフレッシュ処理を効率化できます。

構成が変化したかどうかに関わらず，ストレージシステム上のすべてのリソースの情報をデータベースに反映する場合には，`false` を指定します。

デフォルト：`true`

A.2.20 server.agent.differentialrefresh.periodical.enabled

ストレージシステムの自動リフレッシュ時に，前回のリフレッシュ時点から構成に変化があったリソースについてだけ，データベースの情報を更新するかどうかを指定します。

このプロパティは，リフレッシュ対象のストレージシステムが iStorage V シリーズの場合だけ有効です。

`true` を指定した場合，前回のリフレッシュ時点から構成に変化がないリソースについてはデータベースの更新が省略されるため，リフレッシュ処理を効率化できます。

構成が変化したかどうかに関わらず，ストレージシステム上のすべてのリソースの情報をデータベースに反映する場合には，`false` を指定します。

デフォルト：`true`

A.3 Device Manager のデータベースに関するプロパティ（database.properties ファイル）

データベースに関するプロパティは，`database.properties` ファイルに含まれています。

＜ *HA Command Suite のインストールフォルダ*＞`\DeviceManager\Server\config\database.properties`

このプロパティファイルには，Device Manager サーバのデータベースとの接続の確立に関する設定が含まれています。Device Manager サーバを稼働する前には，これらの設定を正しく入力し，Database Management System（DBMS）を起動する必要があります。サーバが DBMS に接続できない場合には，エラーログにエントリーが書き込まれます（デフォルトディレクトリは，`logs` ディレクトリ）。この情報は，新規インストールのトラブルシューティング時に役立ちます。

A.3.1　dbm.traceSQL

SQL をトレースログに出力するかどうかを指定します。

`true` を設定すると，SQL を出力します。`false` を設定すると，SQL を出力しません。

デフォルト：`false`

A.3.2　dbm.startingCheck.retryCount

Device Manager サーバの起動時に，DBMS の起動確認をリトライする回数を指定します。

指定できる値の範囲は，0～100 です。通常，この設定を変更する必要はありません。

デフォルト：`18`

A.3.3　dbm.startingCheck.retryPeriod

Device Manager サーバの起動時に，DBMS の起動確認をリトライする間隔を秒単位で指定します。

指定できる値の範囲は，0～60（秒）です。通常，この設定を変更する必要はありません。

デフォルト：`10`（秒）

A.4　Device Manager のログ出力に関するプロパティ（logger.properties ファイル）

ログ出力に関するプロパティは，`logger.properties` ファイルに含まれています。

＜ *HA Command Suite のインストールフォルダ*＞`\DeviceManager\Server\config\logger.properties`

このプロパティファイルには，各種ログファイルの操作およびエラーログの名前，場所，および出力レベルなど，Device Manager サーバのロギングモジュールを構成する設定一式が含まれています。また，このファイルを使用して，デバッグおよび診断を目的としたトレースロギングを構成することもできます。

A.4.1　logger.loglevel

trace.log，error.log の出力レベルを指定します。

このフィールドで使用できる値は，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，INFO，WARN，ERROR，および FATAL のエントリーが trace.log に出力されます。この場合，DEBUG のエントリーはログに出力されません。

デフォルト：INFO

A.4.2　logger.MaxBackupIndex

access.log，error.log，service.log，stdout.log，stderr.log，statuscheck.log，trace.log の最大バックアップ数を指定します。

ログファイルが logger.MaxFileSize プロパティで指定された最大長に達すると，access.log.1 のようにカウンターが追加された形式にファイル名が変更されます。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 は 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：10

関連リンク

logger.MaxFileSize（187 ページ）

A.4.3　logger.MaxFileSize

access.log，error.log，service.log，stdout.log，stderr.log，statuscheck.log，trace.log の最大サイズを指定します。

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 と指定しないかぎり，指定したサイズはバイト単位であると見なされます。

指定できる値の範囲は，512KB～32MB です。

デフォルト：1MB

A.4.4　logger.hbase.loglevel

HA Command Suite 共通コンポーネントによって HDvMtrace*n*.log，HDvMGuiTrace*n*.log および HDvMGuiMessage*n*.log（*n* はファイルのバックアップ数を表す整数です）に書き込まれる操作（トレース）およびエラーログの出力レベルを指定します。

各ロギングイベントには，そのタイプ（エラー，警告，および情報）とは無関係に独自の出力レベルがあります。使用できるレベルは，重要度が低い順に 30，20，10，および 0 です。プロダクションシステムのデフォルトのログ出力レベルは，20 です。これは，ロギングイベントレベル 20，10，および 0 のメッセージは HDvMtrace1.log に書き込まれますが，ロギングイベントレベル 30 のメッセージは書き込まれないことを意味します。

デフォルト：20

A.4.5　logger.hbase.sysloglevel

HA Command Suite 共通コンポーネントによってイベントログに書き込まれるトレースログとエラーログの出力レベルを指定します。

各ロギングイベントには，そのタイプ（エラー，警告，および情報）とは無関係に独自の出力レベルがあります。使用できるレベルは，重要度が低い順に 30，20，10，および 0 です。プロダクションシステムのデフォルトのログ出力レベルは，0 です。これは，ロギングイベントレベル 0 のメッセージだけがイベントログに書き込まれ，ロギングイベントレベル 30，20，および 10 のメッセージは書き込まれないことを意味します。通常は，デフォルト値の使用を推奨します。

デフォルト：0

A.4.6　logger.hbase.MaxBackupIndex

HA Command Suite 共通コンポーネントによって HDvMtrace*n*.log，HDvMGuiTrace*n*.log および HDvMGuiMessage*n*.log に書き込まれる操作（トレース）およびエラーログの最大バックアップ数を指定します（*n* はファイルのバックアップ数を表す整数です）。

ログファイルが logger.hbase.MaxFileSize プロパティで指定されたサイズに達すると，HDvMtrace2.log のようにカウンターが追加されたファイルが作成されます。ログファイルの数がこのプロパティで指定した値に達すると，最も古いファイルから上書きされます。

指定できる値の範囲は，1～16 です。

デフォルト：10

関連リンク

logger.hbase.MaxFileSize（188 ページ）

A.4.7　logger.hbase.MaxFileSize

HA Command Suite 共通コンポーネントによって HDvMtrace*n*.log，HDvMGuiTrace*n*.log および HDvMGuiMessage*n*.log に書き込まれる操作（トレース）およびエラーログの最大サイズを指定します（*n* はファイルのバックアップ数を表す整数です）。

キロバイト単位のときは KB，メガバイト単位のときは MB，ギガバイトのときは GB と指定しないかぎり，指定したサイズはバイト単位であると見なされます。

有効な値は，4096～2147483647（2GB 未満）です。

デフォルト：`5MB`

A.5　Device Manager のスレッドに関するプロパティ（dispatcher.properties ファイル）

スレッドに関するプロパティは，`dispatcher.properties` ファイルに含まれています。

＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\config\dispatcher.properties`

このプロパティファイルには，Device Manager サーバのディスパッチャーレイヤーの操作を構成する設定一式が含まれています。例えば，各種バックグラウンドプロセス（デーモン）の微調整やサービスエージェントに対するスレッド優先度の最適化などをするプロパティがあります。

A.5.1　server.dispatcher.message.timeout

保留されている応答メッセージが期限切れになる（パージされる）までのタイムアウトを分単位で指定します。

保留メッセージには, クライアントによるポーリングおよび Device Manager 通知サービスを介したクライアントへの送信がまだ行われていない長期実行プロセス（ストレージシステムの追加など）からの応答があります。

デフォルト：`15`（分）

A.5.2　server.dispatcher.message.timeout.in.processing

何らかの理由で完了していない GUI の処理のタイムアウト時間を分単位で指定します。

デフォルト：`720`（分）

A.5.3　server.dispatcher.daemon.pollingPeriod

コンポーネント状態と構成バージョンを確認するバックグラウンドのスレッドのポーリング間隔を分単位で指定します。

`0` を指定すると，ポーリングは無効になります。

デフォルト：`5`（分）

A.5.4　server.dispatcher.traps.purgePeriod

古くなった SNMP トラップまたはアラートのパージ間隔を分単位で指定します。

`0` を指定すると，サーバからのトラップのパージが無効になります。

デフォルト：`5`（分）

A.5.5　server.dispatcher.daemon.receiveTrap

ストレージシステムやスイッチなどのネットワークリソースで出力された SNMP トラップを Device Manager で受信するかどうかを指定します。

受信する場合は `true` を，受信しない場合は `false` を指定してください。

SNMP トラップの受信には 162/udp が使用されます。Device Manager を新規インストールした際に 162/udp が使用されていない場合は，自動的に `true` が設定されます。

デフォルト：`true`

A.5.6　server.dispatcher.daemon.configUpdate.detection.interval

iStorage V シリーズの構成が Device Manager 以外のストレージ管理ツール（RAID Manager や SVP など）で変更されたかどうかを，Device Manager サーバがチェックする間隔を分単位で指定します。

iStorage V シリーズの構成変更を Device Manager サーバが検知した場合には，Device Manager の GUI に警告メッセージが表示されます。

指定できる範囲は 0～1440（分）です。`0` を指定した場合，Device Manager サーバは，iStorage V シリーズの構成が変更されたかどうかをチェックしません。

デフォルト：`10`（分）

⚠ 注意

- GUI に警告メッセージが表示されていた場合は，該当するストレージシステムの情報を手動でリフレッシュしてください。

  なお，ストレージシステムの構成変更後にユーザーが手動でリフレッシュを実行し忘れた場合に備えて，データベース上の情報が自動的に更新されるよう設定することもできます。次のプロパティを設定してください。

  `server.dispatcher.daemon.autoSynchro.doRefresh` プロパティ

  `server.dispatcher.daemon.autoSynchro.type` プロパティ

- Device Manager サーバでは，次の構成変更については検知できません。

  ・LDEV の状態（正常や閉塞，コピー中など）が変更される

  ・コピーペアを作成，変更または削除する

- Device Manager サーバでは，次の契機にもストレージシステムの構成が変更されたものとして扱われます。

  ・Storage Navigator に表示されているストレージシステムの構成情報を更新する

  ・DKC の電源を入れる

  ・DP プールの構成が変更される※

  ・Snapshot のデータプールの構成が変更される※

  注※

  iStorage V シリーズの場合，`server.dispatcher.daemon.configUpdate.detection.variable.enabled` プロパティを `false` にすると，プールの構成変更については Device Manager の GUI に警告メッセージが表示されないようにできます。

関連リンク

server.dispatcher.daemon.autoSynchro.doRefresh（191 ページ）
server.dispatcher.daemon.autoSynchro.type（191 ページ）
server.dispatcher.daemon.configUpdate.detection.variable.enabled（193 ページ）

A.5.7　server.dispatcher.daemon.autoSynchro.doRefresh

Device Manager サーバが iStorage V シリーズの構成が変更されていることを検知した場合に，データベース上のそのストレージシステムの情報を自動的にリフレッシュするかどうかを指定します。

`true` を指定した場合，Device Manager サーバが検知したあと，ユーザーが手動でリフレッシュしなかったときには，`server.dispatcher.daemon.autoSynchro.type` プロパティに指定された周期でデータベース上の iStorage V シリーズの情報が自動的にリフレッシュされます。`false` を指定した場合は，自動的にはリフレッシュされません。

デフォルト：`true`

注意

`true` を指定した場合，iStorage V シリーズの情報だけがデータベースに反映されます。iStorage V シリーズのコマンドデバイスを認識しているホストの構成定義ファイルの情報は反映されません。

関連リンク

server.dispatcher.daemon.autoSynchro.type（191 ページ）

A.5.8　server.dispatcher.daemon.autoSynchro.type

データベース上のストレージシステム情報を自動的に更新（リフレッシュ）する周期を次のどれかの形式で指定します。

H：一定の時間ごとに自動リフレッシュする場合に指定します。server.dispatcher.daemon.autoSynchro.interval プロパティで間隔を指定してください。

D：1 日に 1 回，特定の時刻に自動リフレッシュする場合に指定します。server.dispatcher.daemon.autoSynchro.startTime プロパティで時刻を指定してください。

W：週に 1 回，特定の曜日の特定の時刻に自動リフレッシュする場合に指定します。server.dispatcher.daemon.autoSynchro.dayOfWeek プロパティで曜日を，server.dispatcher.daemon.autoSynchro.startTime プロパティで時刻を指定してください。

このプロパティは，server.dispatcher.daemon.autoSynchro.doRefresh プロパティで true を指定した場合にだけ有効になります。

デフォルト：D

関連リンク

server.dispatcher.daemon.autoSynchro.doRefresh（191 ページ）
server.dispatcher.daemon.autoSynchro.dayOfWeek（192 ページ）
server.dispatcher.daemon.autoSynchro.startTime（192 ページ）
server.dispatcher.daemon.autoSynchro.interval（193 ページ）

A.5.9 server.dispatcher.daemon.autoSynchro.dayOfWeek

データベース上のストレージシステム情報を自動的に更新（リフレッシュ）する曜日を次のどれかの形式で指定します。

Sun Mon Tue Wed Thu Fri Sat

このプロパティは server.dispatcher.daemon.autoSynchro.type プロパティで W を指定した場合にだけ有効になります。また，管理サーバのタイムゾーンの設定に従って，自動リフレッシュが実行されます。

デフォルト：Fri

関連リンク

server.dispatcher.daemon.autoSynchro.type（191 ページ）

A.5.10 server.dispatcher.daemon.autoSynchro.startTime

データベース上のストレージシステム情報の自動更新（リフレッシュ）を開始する時刻を「*hh*:*mm*」の形式で指定します。

hh は 00～23 の範囲で，*mm* は 00～59 の範囲で指定します。このプロパティは server.dispatcher.daemon.autoSynchro.type プロパティで D または W を指定した場合にだけ有効になります。また，管理サーバのタイムゾーンの設定に従って，自動リフレッシュが実行されます。

デフォルト：`23:00`

関連リンク

server.dispatcher.daemon.autoSynchro.type（191 ページ）

A.5.11 server.dispatcher.daemon.autoSynchro.interval

データベース上のストレージシステム情報を自動的に更新（リフレッシュ）する間隔を時間単位で指定します。

指定できる範囲は 1～24（時間）です。

このプロパティは `server.dispatcher.daemon.autoSynchro.type` プロパティで `H` を指定した場合にだけ有効になります。

デフォルト：`24`（時間）

関連リンク

server.dispatcher.daemon.autoSynchro.type（191 ページ）

A.5.12 server.dispatcher.daemon.configUpdate.detection.variable.enabled

Device Manager サーバが iStorage V シリーズの構成が変更されているかどうかをチェックする際に，DP プールなど，値が逐次変化する項目についても監視対象にするかどうかを指定します。

`true` を指定した場合は，監視対象になり，値の変化を検知した際には Device Manager の GUI に警告メッセージが表示されます。`false` を指定した場合，次の変更については監視対象にはならないで，警告メッセージも表示されません。

- 次のボリュームの利用率の変化
  - DP ボリューム
  - DP プール
  - DT プール
  - Snapshot のデータプール
- 次のボリュームの利用率のしきい値の変更
  - DP プール
  - DT プール
  - Snapshot のデータプール

- 次のボリュームの最大予約容量の変更
  - DP プール
  - DT プール
  - Snapshot のデータプール
- DT プールのモニタリングモードの変更
- DT プールの性能モニタリングと階層再配置に関する設定変更
- DT ボリュームの階層ポリシーに関する設定変更

  DT ボリュームとは，DT プールから作成（DT プールと関連づけ）する仮想ボリュームです。

なお，このプロパティは，server.dispatcher.daemon.configUpdate.detection.interval プロパティで 0 以外を指定した場合にだけ有効になります。

デフォルト：false

関連リンク

server.dispatcher.daemon.configUpdate.detection.interval（190 ページ）

A.5.13 server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh

論理グループの情報を自動的に更新するかどうかを指定します。

true を指定すると，次のタイミングで自動的に更新されます。

- ストレージシステムの登録
- ストレージシステムのリフレッシュ
- ストレージシステムの削除
- 論理グループの作成および編集
- ユーザーグループの作成，編集および削除
- リソースグループの編集および削除

なお，論理グループの情報が自動的に更新されるのは，上記の操作を GUI で実行した場合だけです。

デフォルト：true

A.6　Device Manager の MIME に関するプロパティ（mime.properties ファイル）

MIME に関するプロパティは，`mime.properties` ファイルに含まれています。

＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\config\mime.properties`

このプロパティファイルには, Device Manager サーバによって認識されるすべての MIME タイプの翻訳/検索テーブルが含まれています。検索テーブル内の各プロパティは，特定の拡張子をそのファイルの MIME タイプに割り当てます。通常，この設定を変更する必要はありません。また，このファイルへの追加は，専門知識のあるシステム管理者だけがするようにしてください。

A.7　Device Manager の GUI に関するプロパティ（client.properties ファイル）

GUI に関するプロパティは，`client.properties` ファイルに含まれています。

＜ HA Command Suite のインストールフォルダ＞`\DeviceManager\Server\config\client.properties`

このプロパティファイルには, Device Manager の GUI の表示および操作に関する設定が含まれています。

A.7.1　client.rmi.port

Device Manager の RMI サーバのポート番号を指定します。

Device Manager サーバの `server.rmi.port` プロパティに指定した値と同じ値を指定する必要があります。

デフォルト：`23055`

関連リンク

server.rmi.port（180 ページ）

A.7.2　client.launch.em.secure

iStorage V シリーズ を操作する場合，Device Manager GUI から Storage Navigator を起動する際に，セキュリティを高めるために Storage Navigator に送信する情報を簡略化するかどうかを指定します。

`true` を指定した場合，Storage Navigator に送信する情報を簡略化します。この場合，次の設定が必要です。

- ストレージシステムと管理クライアント（GUI）間のセキュリティ通信の設定を有効にすること。

  自己署名証明書または認証局の署名済みのサーバ証明書を使用してください。

- Device Manager GUI でストレージシステムを登録する際に，ホスト名で登録すること。

  サーバ証明書の Common Name に設定されているホスト名で登録してください。ストレージシステムを登録する方法については，マニュアル『HA Command Suite ユーザーズガイド』を参照してください。

`false` を指定した場合，Storage Navigator に送信する情報を簡略化しません。

デフォルト：`false`

関連リンク

ストレージシステムと管理クライアント（GUI）間のセキュリティ通信のための操作フロー（78 ページ）

A.7.3 client.externaltask.sn.fetch.enable

iStorage V シリーズにおける Storage Navigator での操作のタスクを Device Manager で監視するかどうかを指定します。おもに Storage Navigator の操作で構成変更を行う場合だけ，`false` を指定してください。

`true` を指定した場合，Device Manager が Storage Navigator での操作のタスクを監視し，Device Manager GUI で Storage Navigator での操作のタスクを表示できます。また，Storage Navigator での操作のタスクによる構成変更を自動的に Device Manager のデータベースに反映します。この構成変更を Device Manager のデータベースに反映する間は，該当ストレージシステムがロックされ，Storage Navigator の操作ができなくなることがあります。

`false` を指定した場合，Device Manager は Storage Navigator での操作のタスクを監視しません。この場合，Storage Navigator での操作のタスクによる構成変更を Device Manager のデータベースに反映するには，手動でのストレージシステムの更新が必要です。

デフォルト：`false`

関連リンク

client.externaltask.sn.fetch.pollinginterval（196 ページ）

A.7.4 client.externaltask.sn.fetch.pollinginterval

iStorage V シリーズにおける Storage Navigator での操作のタスクを Device Manager で監視する場合，タスクの監視間隔を秒単位で指定します。指定できる範囲は `1〜86400`（秒）です。

このプロパティは client.externaltask.sn.fetch.enable プロパティで true を指定した場合だけ有効になります。

デフォルト：5（秒）

関連リンク

client.externaltask.sn.fetch.enable（196 ページ）

A.8　Device Manager のセキュリティに関するプロパティ（server.properties ファイル）

セキュリティに関するプロパティは，server.properties ファイルに含まれています。

＜ *HA Command Suite のインストールフォルダ*＞\DeviceManager\Server\config\server.properties

A.8.1　server.http.security.clientIP

Device Manager サーバに接続できる IPv4 アドレスを指定します。

server.http.security.clientIP プロパティは server.properties ファイルに存在します。

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狙った攻撃を防ぐのに役立ちます。

172.16.0.1 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=172.16.0.1,192.168.*.*
```

1 つの IP アドレスで複数の接続元を指定する場合には，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。無効な IP アドレスや空白文字（スペース）は無視されます。

デフォルト：*.*.*.*（すべての IP アドレスが接続できます）

注意

- Device Manager サーバをインストールしたマシンを示す IP アドレス（ローカルループバックアドレス）は，設定する必要はありません。このプロパティでは，ローカルループバックアドレスからは常に Device Manager サーバに接続できるものと見なされます。
- HA Command Suite 共通コンポーネントの環境定義ファイル user_httpsd.conf にも IP アドレスを登録する必要があります。

関連リンク

管理サーバに接続できる管理クライアントを制限するための設定（207 ページ）

A.8.2　server.http.security.clientIPv6

Device Manager サーバに接続できる IPv6 アドレスを指定します。

`server.http.security.clientIPv6` プロパティは `server.properties` ファイルに存在します。

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狙った攻撃を防ぐのに役立ちます。

`12AB:0:0:CD30::`〜`12AB:0:0:CD3F:FFFF:FFFF:FFFF:FFFF` の接続を許可する場合の指定例を次に示します。

```
server.http.security.clientIPv6=12AB:0:0:CD30::/60
```

CIDR 形式で範囲を指定できます。IP アドレスを複数指定する場合は，コンマ（,）で区切ります。無効な IP アドレスの指定や空白文字（スペース）は無視されます。

デフォルト：`::`（すべての IP アドレスが接続できます）

注意

- Device Manager サーバをインストールしたマシンを示す IP アドレス（ローカルループバックアドレス）は，設定する必要はありません。このプロパティでは，ローカルループバックアドレスからは常に Device Manager サーバに接続できるものと見なされます。
- HA Command Suite 共通コンポーネントの環境定義ファイル `user_httpsd.conf` にも IP アドレスを登録する必要があります。

関連リンク

管理サーバに接続できる管理クライアントを制限するための設定（207 ページ）

A.8.3　server.https.security.keystore

SSL または TLS で暗号化された通信の確立に使用されるキーペアとサーバ証明書を格納するキーストアーファイルの名前を指定します。

`server.https.security.keystore` プロパティは `server.properties` ファイルに存在します。

Device Manager を新規インストールした場合，または Device Manager サーバの証明書が存在しない状態でアップグレードインストールをした場合，Device Manager サーバのキーストアーには，iStorage V シリーズに対するユーザーアカウント認証用のデフォルトの証明書が格納されています。 iStorage V シリーズとの通信をよりセキュアにしたい場合，またはほか

の用途でセキュリティ通信をする場合は，キーペアと自己署名証明書または信頼された証明書をキーストアーにインポートし直してください。

デフォルト：keystore

関連リンク

Device Manager サーバのデフォルトの証明書（75 ページ）

A.8.4 server.http.security.unprotected

サーバのドキュメントルートにある保護していないファイルリソースを指定します。

server.http.security.unprotected プロパティは server.properties ファイルに存在します。

複数のファイルリソースを指定する場合は，各項目をコンマ（,）で区切ります。スペースは無視されます。ファイルまたはディレクトリが未保護として指定されている場合，サーバのセキュリティモード設定に関わらず，これらはアクセス制御リストチェック（ユーザー認証）から除かれます。アスタリスクをワイルドカード文字として使用することで，ディレクトリ全体（ネストされたサブディレクトリも含む）を未保護としてフラグを設定できます。スペースを指定した場合には，すべてのリソースが保護されます。この結果，Device Manager へのすべての要求にユーザー認証が必要になります。

このプロパティは，ユーザー認証を必要とせず，誰でも index.html フロントページを Web ブラウザーに表示できるようにします。通常，この設定を変更する必要はありません。

デフォルト：index.html, Server/*, webstart/*, images/*, style/*, docs/*, favicon.ico, vasa/*

A.8.5 server.https.security.truststore

Device Manager サーバのトラストストアーファイルを指定します。

server.https.security.truststore プロパティは server.properties ファイルに存在します。

デフォルト：dvmcacerts

メモ

このプロパティは，HiKeytool で変更できません。値を変更するには，server.properties ファイルで値を編集する必要があります。

A.8.6 server.https.enabledCipherSuites

次の SSL/TLS 通信で使用する暗号方式（Cipher Suite）をコンマ（,）で区切って指定します。

- Device Manager サーバと Device Manager GUI 間

server.https.enabledCipherSuites プロパティは server.properties ファイルに存在します。

指定できる暗号方式は次のとおりです。

- 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_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

デフォルト：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

A.8.7 server.https.protocols

次の SSL/TLS 通信で使用するプロトコルをコンマ（,）で区切って指定します。

- Device Manager サーバと Device Manager GUI 間

server.https.protocols プロパティは server.properties ファイルに存在します。

指定できるプロトコルは次のとおりです。

- TLSv1
- TLSv1.1
- TLSv1.2

ただし，TLSv1，TLSv1.1 を指定しても使用されません。server.https.enabledCipherSuites プロパティを変更した場合も同様です。

デフォルト：TLSv1,TLSv1.1,TLSv1.2

A.9　Device Manager の SNMP トラップのログ出力に関するプロパティ（customizedsnmptrap.properties ファイル）

SNMP トラップのログ出力に関するプロパティは，customizedsnmptrap.properties ファイルに含まれています。

＜ HA Command Suite のインストールフォルダ＞\DeviceManager\Server\config\customizedsnmptrap.properties

A.9.1　customizedsnmptrap.customizedSNMPTrapEnable

Device Manager で受信した SNMP トラップをログファイルに出力するかどうかを指定します。

出力する場合は true，出力しない場合は false を指定します。

true を指定した場合は，customizedsnmptrap.customizelist プロパティも設定してください。

デフォルト：false

メモ

server.dispatcher.daemon.receiveTrap プロパティに true を指定している場合，同じ事象に関するストレージシステムの SNMP トラップについては，ログファイルに二重に出力されることがあります。

関連リンク

server.dispatcher.daemon.receiveTrap（190 ページ）

A.9.2　customizedsnmptrap.customizelist

Device Manager で受信した SNMP トラップをログファイルに出力する際の重要度や出力形式を指定します。

customizedsnmptrap.customizelist プロパティの指定形式を次に示します。

```
customizedsnmptrap.customizelist = \
＜EnterpriseID1＞:＜一般トラップ番号1＞:＜固有トラップ番号1＞:＜重要度1＞:＜出力内容1＞, \
＜EnterpriseID2＞:＜一般トラップ番号2＞:＜固有トラップ番号2＞:＜重要度2＞:＜出力内容2＞, \
...
＜EnterpriseIDn＞:＜一般トラップ番号n＞:＜固有トラップ番号n＞:＜重要度n＞:＜出力内容n＞
```

表 A-2　customizedsnmptrap.customizelist プロパティで指定する項目

項目	形式	説明
EnterpriseID	ドット表現 （例）.1.3.6.1.4.1.119.1.68.5.3.11.4.1.1	省略できません。
一般トラップ番号	0～6 の数値	省略できません。
固有トラップ番号	数値	省略できません。
重要度	次に示すどれかの文字列で各トラップの重要度を指定します。 次に示す文字列以外は指定できません。 • `Information` • `Warning` • `Error` • `Critical` • `Alert` • `Null`	省略できます。省略時は `Null` を指定したと見なされます。 メッセージ ID のインジケーターは次のとおりに出力されます。 • `Information`：`-I` • `Warning`：`-W` • `Error/Critical/Alert`：`-E` • `Null`：ログを出力しない
出力内容	次の文字列（変数）で出力内容を指定します。 次に示す文字列以外は指定できません。 • `$a` • `$e` • `$g` • `$s` • `$`*n*（*n*=1 以上の整数）	省略できます。省略時は`$a$e$g$s`の内容が出力されます。 重要度に `Null` を指定した場合この項目への指定は無効になります。 各変数の出力内容は次のとおりです。 • `$a`：エージェントアドレス（ドット形式） • `$e`：EnterpriseID（ドット形式） • `$g`：一般トラップ番号 • `$s`：固有トラップ番号 • `$`*n*（*n*=1 以上の整数）：*n* 番目のバリアブルバインディングの値

- 項目を省略した場合でも，区切り文字のコロン（:）は入力してください。
- 複数の定義を指定する場合，コンマ（,）を区切り文字として使用してください。ただし，最後のエントリーの終わりにはコンマ（,）を入力しないでください。
- 途中で改行したい場合は，その行の終わりに円記号（\）を入力してください。円記号（\）のあとの改行は無視されます。

`customizedsnmptrap.customizelist` プロパティの指定例を，次に示します。

```
customizedsnmptrap.customizelist = \
.1.2.3:6:1:Information:$a$e$g$s$1$2, \
.1.3.6.1.4.1.2854:6:1:Warning:$e$a$s$3$2$1$g, \
.1.3.6.1.4.1.119.1.68.5.3.11.4.1.1:6:1:Error:$a$s, \
.1.3.6.1.4.1.119.1.68.5.3.11.4.1.1:6:100:Information:$a$s
```

デフォルト：なし

注意

このプロパティが指定されていない場合，customizedsnmptrap.customizedSNMPTrapEnable プロパティに true が設定されていても，SNMP トラップの情報はログに出力されません。

関連リンク

customizedsnmptrap.customizedSNMPTrapEnable（201 ページ）

A.10　Device Manager からラウンチするアプリケーションに関するプロパティ（launchapp.properties ファイル）

ラウンチするアプリケーションに関するプロパティは，launchapp.properties ファイルに含まれています。

＜ *HA Command Suite のインストールフォルダ*＞\DeviceManager\Server\config\launchapp.properties

このプロパティファイルには，ラウンチされるアプリケーションがインストールされているサーバの情報が含まれています。

A.10.1　launchapp.elementmanager.usehostname

Device Manager GUI から Storage Navigator を使用し iStorage V シリーズに接続する場合，Storage Navigator の URL にホスト名を表示するかどうかを指定します。

true を指定すると，対象のストレージシステムをホスト名で指定して Device Manager に登録した場合，Storage Navigator の URL にホスト名を表示します。false を指定した場合，Storage Navigator の URL に IP アドレスを表示します。

デフォルト：true

付録 B. 管理クライアントに関するセキュリティ設定

ここでは，管理クライアントに関するセキュリティ設定について説明します。

B.1 警告バナーとは

警告バナーとは，HA Command Suite 製品のログイン画面に表示されるセキュリティメッセージ欄のことです。

HA 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，任意のメッセージを警告バナーに表示できます。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。

B.1.1 警告バナーに表示するメッセージの条件

`hcmds64banner` コマンドで警告バナーに表示するメッセージを登録する場合，文字数や文字コードに制限があります。

- HTML タグを使って記載してください。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。

  HTML タグの条件を次に示します。

  - 任意の位置で改行する場合は，`<BR>`タグを使用してください。
  - 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，ログイン画面にアンパサンド（`&`）を表示する場合は，HTML ファイルでは「`&`」と記述します。
- 使用できる最大文字数は 1,000 文字です（HTML 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。

B.1.2 警告バナーに表示するメッセージの作成と登録

HA Command Suite 製品の警告バナーに表示するメッセージは，テキストエディターなどを使って作成し，`hcmds64banner` コマンドを実行して登録します。

前提条件

Administrator 権限でのログイン

操作手順

1. テキストエディターなどを使い，メッセージを作成します。

   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。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\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てしまうので，利用する場合はコピーしたものを編集してください。

   メッセージのひな形を次に示します。

```
<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。
```

2. `hcmds64banner` コマンドを実行して，メッセージを登録します。

   ＜ HA Command Suite のインストールフォルダ＞`\Base64\bin\hcmds64banner /add /file` *＜ファイル名＞* `[/locale` *＜ロケール名＞*`]`

   ### ＜ファイル名＞

   メッセージを格納したファイルを絶対パスで指定します。

   ### ＜ロケール名＞

   メッセージに使用した言語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，ロケールに関係なく，登録したメッセージが常に警告バナーに表示されます（デフォルトのロケールのメッセージとして登録されます）。

   GUI を複数のロケールで使用する場合，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。

   1 つの Web ブラウザーに複数の言語が設定されている場合，警告バナーのロケールは Web ブラウザーの言語の優先順位に従います。

メモ

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に，`hcmds64banner` コマンドを実行すると，上書き更新されます。

ヒント

次の場合は GUI からも操作できます。

- ロケールを指定せずにメッセージを登録する場合
- `hcmds64banner` コマンドで `locale` オプションを省略して登録したメッセージを編集する場合

ただし，GUI から操作する場合は，次の制限があります。

- 使用できる HTML タグに制限があります。
- クラスタ構成の環境の場合は, 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操作を実施してください。

操作結果

メッセージが管理サーバに登録され，HA Command Suite 製品のログイン画面に表示されます。

B.1.3 警告バナーからのメッセージの削除

HA Command Suite 製品の警告バナーに表示されたメッセージを削除するには `hcmds64banner` コマンドを実行します。

前提条件

- Administrator 権限でのログイン
- 次の情報の確認
  - 削除するメッセージのロケール（英語は `en`，日本語は `ja` です）

操作手順

1. `hcmds64banner` コマンドを実行します。

   < HA Command Suite のインストールフォルダ>`\Base64\bin\hcmds64banner /delete [/locale` *<ロケール名>*`]`

   <ロケール名>

   削除する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が指定されます。

ヒント

次のメッセージは GUI からも削除できます。

- GUI から登録したメッセージ

- hcmds64banner コマンドで locale オプションを省略して登録したメッセージ

ただし，クラスタ構成の環境の場合，GUI から操作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操作を実施してください。

B.2　管理サーバに接続できる管理クライアントを制限するための設定

HA Command Suite 製品では，GUI 経由で管理サーバにアクセスする管理クライアントを制限できます。管理サーバに接続できる管理クライアントを制限するには, user_httpsd.conf ファイルと Device Manager サーバのプロパティファイルを編集します。

前提条件

次の情報の確認

- 管理サーバへの接続を許可する管理クライアントのマシン情報

  接続を許可する管理クライアントの情報は，次のどれかの形式で指定します。

  - ドメイン名（例 nec.datasystem.com）
  - ドメイン名の一部（例 nec）
  - IPv4 または IPv6 アドレス（例 10.1.2.3，127.0.0.1，2001::123:4567:89ab:cdef）
  - IPv4 アドレスの一部（例 10.1　この場合，10.1.0.0/16 と同じ意味になります）
  - IPv4 のネットワーク/ネットマスクの形式（例 10.1.0.0/255.255.0.0）
  - IPv4 または IPv6 のネットワーク/**c** の CIDR 形式（**c** は，ネットワークアドレスのビット数を表す 10 進の整数）（例 10.1.0.0/16，2001:0:0:1230::/64）

操作手順

1. HA Command Suite 製品のサービスを停止します。
2. 管理サーバへの接続を許可する管理クライアントの情報を，user_httpsd.conf ファイルの最終行に登録します。

   user_httpsd.conf ファイルの格納先

   ＜ *HA Command Suite のインストールフォルダ*＞\Base64\uCPSB11\httpsd\conf\user_httpsd.conf

   user_httpsd.conf ファイルへの指定形式

```
<Location /DeviceManagerWebService>
        order allow,deny
        allow from <管理クライアントの情報> [<管理クライアントの情報>...]
</Location>
```

- order は，必ず形式どおりに指定してください。余分な空白やタブなどを挿入すると動作しません。
- allow from 行は，複数記述できます。
- 1 行の allow from 内で管理クライアントを複数指定する場合は，空白で区切ってください。
- 管理サーバで HA Command Suite 製品の GUI を使用する場合は，ローカルループバックアドレス（127.0.0.1 または localhost）も指定する必要があります。

user_httpsd.conf ファイルの登録例

```
<Location /DeviceManagerWebService>
        order allow,deny
        allow from 127.0.0.1 10.0.0.1 2001::123:4567:89ab:cdef
        allow from 10.1.0.0/16 2001:0:0:1230::/64
</Location>
```

3. Device Manager サーバの server.properties ファイルにある server.http.security.clientIP プロパティまたは server.http.security.clientIPv6 プロパティに，管理クライアントの情報を登録します。
4. HA Command Suite 製品のサービスを起動します。

関連リンク

Device Manager のサービスの起動（134 ページ）
Device Manager のサービスの停止（134 ページ）
server.http.security.clientIP（197 ページ）
server.http.security.clientIPv6（198 ページ）

付録 C.　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。

C.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。

- 『HA Command Suite ユーザーズガイド』（IV-UG-201）
- 『HA Command Suite インストールガイド』（IV-UG-202）
- 『HA Command Suite メッセージ』（IV-UG-204）

C.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。

表記	製品名
Device Manager	HA Device Manager
Dynamic Provisioning	次の製品を区別する必要がない場合の表記です。 • Dynamic Provisioning Software • Dynamic Provisioning
DP	次の製品を区別する必要がない場合の表記です。 • Dynamic Provisioning
DT	次の製品を区別する必要がない場合の表記です。 • Dynamic Tiering Software
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
RAID Manager	次の製品を区別する必要がない場合の表記です。 • RAID Manager
Local Replication	次の製品を区別する必要がない場合の表記です。 • Local Replication • Local Replication Software
Storage Navigator	次の製品を区別する必要がない場合の表記です。 • Storage Navigator • HA Device Manager - Storage Navigator
Snapshot	次の製品を区別する必要がない場合の表記です。 • Snapshot
Synchronous Replication	次の製品を区別する必要がない場合の表記です。 • Synchronous Replication

表記	製品名
	• Synchronous Replication Software
Asynchronous Replication	次の製品を区別する必要がない場合の表記です。 • Asynchronous Replication Software • Asynchronous Replication
Universal Volume Manager	次の製品を区別する必要がない場合の表記です。 • Universal Volume Manager
Virtual Partition Manager	次の製品を区別する必要がない場合の表記です。 • Virtual Partition Manager • Virtual Partition Manager Software
VMware	VMware
VMware ESXi	VMware vSphere ESXi
iStorage V シリーズ	次の製品を区別する必要がない場合の表記です。 • iStorage V100 • iStorage V300

C.3　このマニュアルで使用している略語

このマニュアルで使用する主な英略語を次に示します。

略語	正式名称
AES	Advanced Encryption Standard
ALUA	Asymmetric Logical Unit Access
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLPR	Cache Logical PaRtition
CN	Common Name
CPU	Central Processing Unit
CSR	Certificate Signing Request
CSV	Comma Separated Value
CU	Control Unit
CVS	Custom Volume Size
DBMS	DataBase Management System
DER	Distinguished Encoding Rules
DKC	DisK Controller
DMTF	Distributed Management Task Force
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Services

略語	正式名称
ECC	Elliptic Curve Cryptography
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I/O	Input/Output
ID	IDentifier
IETF	Internet Engineering Task Force
IOPS	Input Output Per Second
IP	Internet Protocol
IP-SAN	Internet Protocol Storage Area Network
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer System Interface
JAR	Java ARchiver
LAN	Local Area Network
LBA	Logical Block Addressing
LDAP	Lightweight Directory Access Protocol
LDEV	Logical DEVice
LDKC	Logical DisK Controller
LU	Logical Unit
LUN	Logical Unit Number
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
OS	Operating System
P-VOL	Primary VOLume
PAP	Password Authentication Protocol
PDEV	Physical DEVice
PEM	Privacy Enhanced Mail
PID	Process ID
PNG	Portable Network Graphics
PP	Program Product
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RDN	Relative Distinguished Name

略語	正式名称
REST	Representational State Transfer
RFC	Request For Comments
RMI	Remote Method Invocation
S-VOL	Secondary VOLume
SAN	Storage Area Network
SCSI	Small Computer System Interface
SIM	Service Information Message
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SRV	SeRVice
SSH	Secure SHell
SSID	Storage System ID
SSL	Secure Sockets Layer
SSO	Single Sign - On
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
V-VOL	Virtual VOLume
WAN	Wide Area Network
WWN	World Wide Name
XML	eXtensible Markup Language

C.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

記号・数字

さ

た

な

は

ま

や

ら

iStorage V100/V300
HA Command Suite
システム構成ガイド

IV-UG-203-001-07

2024 年 4 月 第 7 版 発行

日本電気株式会社