

Hitachi Command Suite

# Compute Systems Manager

導入・設定ガイド

3021-9-097-A0

## 対象製品

Hitachi Compute Systems Manager 8.5.0

適用 OS の詳細については「ソフトウェア添付資料」でご確認ください。

## 輸出時の注意

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

なお、不明な場合は、弊社担当営業にお問い合わせください。

## 商標類

HITACHI, HiRDB, JP1 は、株式会社日立製作所の商標または登録商標です。

Active Directory は、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。

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

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 .NET は、お客様、情報、システムおよびデバイスを繋ぐソフトウェアです。

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

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

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

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

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

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

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

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

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

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

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

その他記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。

Hitachi Compute Systems Manager には、日本電気株式会社が著作権を有している部分が含まれています。

Hitachi Compute Systems Manager は、米国 EMC コーポレーションの RSA BSAFE<sup>®</sup> ソフトウェアを搭載しています。

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

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

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

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

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

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


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

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

This product includes software developed by Andy Clark.

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

**HITACHI**  
Inspire the Next

 株式会社 日立製作所



**発行**

2016年10月 3021-9-097-A0

**著作権**

All Rights Reserved. Copyright © 2014, 2016, Hitachi, Ltd.



# 目次

はじめに.....	17
対象読者.....	18
マニュアルの構成.....	18
マイクロソフト製品の表記について.....	19
このマニュアルで使用している記号.....	20
<b>1. Compute Systems Manager の概要.....</b>	<b>21</b>
1.1 Compute Systems Manager の概要.....	22
1.1.1 Compute Systems Manager とは.....	22
1.1.2 Compute Systems Manager の管理対象.....	22
1.2 システム構成.....	23
1.2.1 システムの構成要素.....	23
1.2.2 基本的なシステム構成.....	23
1.2.3 ネットワーク構成.....	25
1.3 関連製品.....	25
1.4 作業フローの全体像.....	25
1.5 導入の作業フロー.....	27
1.5.1 インストールの流れ.....	27
1.5.2 新規インストール後に必要な作業の流れ.....	27
1.6 環境設定の作業フロー.....	29
1.6.1 SNMP トラップの設定の流れ.....	29
1.6.2 管理対象ホストの設定の流れ.....	29
1.6.3 管理クライアントとの通信のセキュリティ設定の流れ.....	31
1.6.4 SMTP サーバとの通信のセキュリティ設定の流れ.....	32
1.6.5 管理対象サーバとの通信のセキュリティ設定の流れ.....	32
1.6.6 Device Manager サーバとの通信のセキュリティ設定の流れ.....	33
1.6.7 LDAP ディレクトリサーバとの通信のセキュリティ設定の流れ.....	33
1.6.8 外部認証サーバとの連携の流れ.....	34
1.6.9 デプロイメントマネージャーの環境設定の流れ.....	35
1.7 運用と保守の作業フロー.....	36
1.7.1 管理サーバの移行の流れ.....	36
1.7.2 データベースの管理の流れ.....	37
1.7.3 ネットワーク構成の変更の流れ.....	37
1.7.4 トラブルシューティングの流れ.....	38
<b>2. インストールとアンインストール.....</b>	<b>41</b>
2.1 Compute Systems Manager のインストール方法について.....	42
2.2 インストール環境の確認.....	42

2.2.1	インストール環境の確認とは.....	42
2.2.2	システム要件を確認する.....	43
2.2.3	ポート番号が競合していないことを確認する.....	43
2.2.4	管理サーバのシステム環境を確認する (Linux) .....	43
2.2.5	カーネルパラメーターとシェル制限を設定する (Linux) .....	44
2.2.6	ファイアウォールの例外登録をする (Linux) .....	44
2.2.7	管理サーバの時刻を調整する.....	44
2.2.8	IPv6 を使用する場合は設定を確認する.....	45
2.2.9	32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定を確認する.....	45
2.3	インストール時の入力項目の検討.....	46
2.3.1	インストール時の入力項目の検討とは.....	46
2.3.2	パスの指定規則.....	47
2.3.3	インストールに使用するディレクトリの内容を確認する.....	48
2.3.4	管理サーバの情報を確認する.....	49
2.4	インストール.....	49
2.4.1	インストールとは.....	49
2.4.2	インストールする前の確認事項.....	50
2.4.3	Compute Systems Manager をインストールする (Windows) .....	51
2.4.4	Compute Systems Manager をインストールする (Linux) .....	52
2.4.5	ウイルス検出プログラムを使用する場合に必要な設定.....	53
2.4.6	32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を有効にする.....	54
2.4.7	32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を無効にする.....	55
2.5	新規インストール後に必要な作業.....	56
2.5.1	新規インストール後に必要な作業とは.....	56
2.5.2	管理サーバにアクセスできるか確認する.....	56
2.5.3	プラグインライセンスを登録する.....	57
2.5.4	System アカウントのパスワードを変更する.....	58
2.5.5	System アカウントにメールアドレスを設定する.....	58
2.5.6	E メール通知を設定する.....	59
2.5.7	E メールで通知するアラートレベルを設定する.....	59
2.5.8	管理対象リソースを登録する.....	59
2.5.9	サーバ管理者のユーザーアカウントを作成する.....	60
2.5.10	リソースグループを設定する.....	60
2.5.11	ユーザーグループを設定する.....	60
2.5.12	初期設定作業を完了する.....	61
2.6	アンインストール.....	61
2.6.1	アンインストールとは.....	61
2.6.2	アンインストールするための確認事項.....	62
2.6.3	アンインストールする (Windows) .....	62
2.6.4	アンインストールする (Linux) .....	63
<b>3.</b>	<b>管理サーバの環境設定.....</b>	<b>65</b>
3.1	SNMP トラップの設定.....	66
3.1.1	SNMP トラップの設定とは.....	66
3.1.2	MIB ファイルを登録する.....	66
3.1.3	インバンド SNMP トラップの監視とは.....	67
3.1.4	インバンド SNMP トラップを監視する.....	67
3.2	ユーザーアカウントのポリシーの設定.....	68
3.2.1	ユーザーアカウントのポリシーの設定とは.....	68
3.2.2	System アカウントをロックの対象にする.....	68
3.2.3	アカウントのロックを解除する.....	69
3.3	JP1/IM でのアラート監視設定.....	70

3.3.1 JP1/IM でのアラート監視とは.....	70
3.3.2 JP1/IM でアラート監視できるよう設定する.....	70
3.4 JP1/IM からの Compute Systems Manager のラウンチ.....	71
3.4.1 JP1/IM からの Compute Systems Manager のラウンチとは.....	71
3.4.2 JP1/IM から Compute Systems Manager をラウンチできるように設定する.....	71
3.5 管理サーバの設定変更.....	72
3.5.1 ポート番号の変更.....	72
(1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ.....	72
(2) ポート変更時に編集する Compute Systems Manager サーバのプロパティ.....	75
(3) ポートを変更する.....	76
3.5.2 管理サーバのホスト名または IP アドレスの変更.....	76
(1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ.....	76
(2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ.....	78
(3) 管理サーバのホスト名または IP アドレスを変更する.....	79
3.5.3 Compute Systems Manager の URL の変更.....	80
(1) Compute Systems Manager の URL を変更するタイミング.....	80
(2) Compute Systems Manager の URL を変更する.....	81
3.5.4 JDK を変更する.....	82
3.5.5 管理サーバの時刻設定の更新.....	83
(1) Compute Systems Manager で適用される時刻について.....	83
(2) 運用開始後に管理サーバの時刻を調整する.....	83
3.5.6 アラート発生時に実行するコマンドのタイムアウト時間を変更する.....	83
3.5.7 管理クライアントに表示される温度の単位を設定する.....	84
3.5.8 管理サーバのファイアウォールに例外登録をする (Windows) .....	85
3.5.9 管理サーバのファイアウォールに例外登録をする (Linux) .....	85
3.5.10 管理サーバのファイアウォールに例外登録が必要なポート (Linux) .....	86
3.5.11 WinRM の設定を反映する (Linux) .....	86
<b>4. 管理対象の設定.....</b>	<b>89</b>
4.1 管理対象ホストの設定.....	90
4.1.1 WoL を有効にする.....	90
4.1.2 BMC 監視を有効にする.....	90
4.2 管理対象サーバの設定.....	90
4.2.1 日立製のブレードサーバを管理対象にするための確認事項.....	90
4.2.2 日立製のラックマウントサーバを管理対象にするための確認事項.....	91
4.3 管理対象ホストの設定 (Windows ホスト) .....	91
4.3.1 ホストを管理対象にするための確認事項 (Windows ホスト) .....	91
4.3.2 Windows ファイアウォールを設定する (Windows ホスト) .....	92
4.3.3 DCOM を有効にする (Windows ホスト) .....	92
4.3.4 WinRM を有効にする (Windows ホスト) .....	93
4.3.5 UAC を使用したリモート接続を設定する (Windows ホスト) .....	93
4.3.6 SNMP トラップを設定する (Windows ホスト) .....	94
4.4 管理対象ホストの設定 (Linux ホスト) .....	94
4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト) .....	94
4.4.2 OS のファイルおよびディレクトリ構成の確認項目 (Linux ホスト) .....	95
4.4.3 Compute Systems Manager で使用するアカウントを設定する (Linux ホスト) .....	95
4.4.4 IP 接続を許可する (Linux ホスト) .....	96
4.4.5 管理対象ホストへのログインの許可とは.....	96
4.4.6 root ユーザーでのログインを許可する (Linux ホスト) .....	97
4.4.7 一般ユーザーでログインし、su コマンドを利用することを許可する (Linux ホスト) .....	98
4.4.8 一般ユーザーでログインし、sudo コマンドを利用することを許可する (Linux ホスト) .....	99
4.4.9 SNMP トラップを設定する (Linux ホスト) .....	100
4.5 移行する管理対象ホストを探索するための設定を変更する.....	100

4.6 シャーシのマネジメントモジュールの IP アドレスを変更する.....	101
<b>5. セキュリティ設定.....</b>	<b>103</b>
5.1 セキュリティの設定とは.....	104
5.2 管理クライアントとの通信のセキュリティ設定.....	104
5.2.1 管理クライアントの通信のセキュリティ設定とは.....	104
5.2.2 管理サーバで SSL 通信するよう設定する（管理クライアントとの通信路）.....	105
5.2.3 管理クライアントで SSL 通信するよう設定する（GUI との通信路）.....	109
5.2.4 管理クライアントで SSL 通信するよう設定する（CLI との通信路）.....	110
5.3 SMTP サーバとの通信のセキュリティ設定.....	111
5.3.1 SMTP サーバとの通信のセキュリティ設定とは.....	111
5.3.2 管理サーバで SSL 通信するよう設定する（SMTP サーバとの通信路）.....	111
5.4 管理対象サーバとの通信のセキュリティ設定.....	112
5.4.1 管理対象サーバとの通信のセキュリティ設定とは.....	112
5.4.2 管理サーバで SSL 通信するよう設定する（管理対象サーバとの通信路）.....	112
5.5 Device Manager サーバとの通信のセキュリティ設定.....	115
5.5.1 Device Manager サーバとの通信のセキュリティ設定とは.....	115
5.5.2 管理サーバで SSL 通信するよう設定する（Device Manager サーバとの通信路）.....	116
5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは.....	116
5.7 管理クライアントからの接続を制限する設定.....	117
5.7.1 管理クライアントからの接続の制限とは.....	117
5.7.2 管理クライアントからの接続を制限する.....	117
5.8 サーバ証明書の有効期限を確認する.....	118
5.9 トラストストアにインポートされたサーバ証明書を削除する.....	119
<b>6. 外部認証サーバとの連携.....</b>	<b>121</b>
6.1 外部認証サーバとの連携の概要.....	122
6.1.1 外部認証サーバとの連携とは.....	122
6.1.2 外部認可サーバとの連携とは.....	122
6.2 外部認証サーバと連携するための操作フロー.....	123
6.2.1 LDAP ディレクトリサーバと連携するための操作フロー.....	123
6.2.2 Kerberos サーバと連携するための操作フロー.....	124
6.3 複数の外部認証サーバと連携している場合の構成.....	126
6.4 LDAP ディレクトリサーバの構造モデル.....	128
6.4.1 BaseDN とは.....	128
6.4.2 階層構造モデルとは.....	128
6.4.3 フラットモデルとは.....	129
6.5 LDAP ディレクトリサーバで認証する場合に必要な設定.....	130
6.5.1 LDAP ディレクトリサーバを接続するための前提条件.....	130
6.5.2 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の条件.....	130
6.6 LDAP ディレクトリサーバとの接続.....	131
6.6.1 LDAP ディレクトリサーバと接続するよう設定する.....	131
6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する.....	133
6.7 Kerberos サーバとの接続.....	135
6.7.1 Kerberos 認証に使用できる暗号タイプ.....	135
6.7.2 Kerberos サーバと接続するよう設定する.....	135
6.8 LDAP ディレクトリサーバと接続するための設定項目.....	137
6.8.1 exauth.properties ファイルの設定項目（LDAP ディレクトリサーバの情報を直接指定する場合で、外部認証サーバとだけ連携するとき）.....	137
6.8.2 exauth.properties ファイルの設定項目（LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき）.....	138



6.8.3 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する場合で、外部認可サーバとも連携するとき) .....	139
6.8.4 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき) .....	140
6.9 Kerberos サーバと接続するための設定項目 .....	141
6.9.1 exauth.properties ファイルの設定項目 (Kerberos サーバの情報を直接指定する場合で、外部認証サーバとだけ連携するとき) .....	141
6.9.2 exauth.properties ファイルの設定項目 (Kerberos サーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき) .....	142
6.9.3 exauth.properties ファイルの設定項目 (Kerberos サーバの情報を直接指定する場合で、外部認可サーバとも連携するとき) .....	142
6.9.4 exauth.properties ファイルの設定項目 (Kerberos サーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき) .....	143
6.10 外部認証サーバと接続するためのコマンド .....	144
6.10.1 外部認証サーバとの連携設定で使用するコマンドに関する注意事項 .....	144
6.10.2 外部認証サーバとの接続を確認するコマンド (hcmds64checkauth) の書式 .....	144
6.11 情報検索用のユーザーアカウントを使用して LDAP ディレクトリサーバに接続する .....	146
6.11.1 情報検索用のユーザーアカウントの条件 .....	146
6.11.2 情報検索用のユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式 .....	147
6.11.3 管理サーバで情報検索用のユーザーアカウントの登録状況を確認する .....	148
6.11.4 管理サーバから情報検索用のユーザーアカウントを削除する .....	149
6.12 LDAP ディレクトリサーバの証明書のインポート .....	149
6.12.1 LDAP ディレクトリサーバの証明書の条件 .....	149
6.12.2 LDAP ディレクトリサーバの証明書をインポートする場合の注意事項 .....	149
6.12.3 LDAP ディレクトリサーバの証明書をインポートするコマンド (hcmds64keytool または keytool) の書式 .....	150
<b>7. デプロイメントマネージャーの環境設定 .....</b>	<b>153</b>
7.1 デプロイメントマネージャーの環境設定とは .....	154
7.2 デプロイメントマネージャーをインストールするための前提条件 .....	154
7.3 IIS をインストールする .....	155
7.4 .NET Framework をインストールする (デプロイメントマネージャーを使用する場合) .....	156
7.5 デプロイメントマネージャーをインストールする .....	156
7.6 デプロイメントマネージャーを運用するための前提条件 .....	157
7.7 管理対象リソースのブートの設定を変更する .....	158
7.8 デプロイメントマネージャーが使用するポート番号を変更する .....	158
7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル .....	159
<b>8. 管理サーバの運用 .....</b>	<b>161</b>
8.1 Compute Systems Manager の起動と停止 .....	162
8.1.1 Compute Systems Manager の起動と停止とは .....	162
8.1.2 Compute Systems Manager を起動する .....	162
8.1.3 Compute Systems Manager を停止する .....	163
8.1.4 Compute Systems Manager の常駐プロセス .....	163
8.1.5 Compute Systems Manager の稼働状況を確認する .....	165
8.2 データベースの管理 .....	166
8.2.1 データベースの管理とは .....	166
8.2.2 データベースをバックアップするための確認事項 .....	167
8.2.3 データベースをバックアップする .....	168
8.2.4 データベースをリストアするための確認事項 .....	169
8.2.5 データベースをリストアする .....	169
8.2.6 データベースを移行するための確認事項 .....	170

8.2.7 移行元サーバからデータベースをエクスポートする.....	170
8.2.8 移行先サーバにデータベースをインポートする.....	171
<b>9. クラスタを使用するための環境設定と運用.....</b>	<b>175</b>
9.1 クラスタを使用するための環境設定と運用とは.....	176
9.2 クラスタを運用するために使用する Compute Systems Manager のサービス.....	177
9.3 クラスタ運用を開始する前の確認事項.....	178
9.3.1 クラスタ運用を開始する環境設定手順の確認.....	178
9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認.....	183
9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認.....	184
9.4 クラスタ環境へのインストール.....	185
9.4.1 クラスタ環境にインストールする (Windows) .....	185
9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux) .....	187
9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux) .....	190
9.4.4 実行系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux) .....	192
9.4.5 待機系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux) .....	193
9.5 クラスタ環境への移行.....	195
9.5.1 クラスタ環境に移行する (Windows) .....	195
9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux) .....	197
9.6 クラスタ管理アプリケーションへのサービスの登録と削除.....	201
9.6.1 クラスタ管理アプリケーションにサービスを登録する (Windows) .....	201
9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux) .....	202
9.6.3 クラスタ管理アプリケーションからサービスを削除する (Windows) .....	203
9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux) .....	204
9.7 新規インストールまたはクラスタ環境に移行した後の環境設定.....	205
9.7.1 クラスタ環境でウィルス検出プログラムを使用する場合に必要な設定.....	205
9.7.2 クラスタ環境で同期が必要な設定.....	205
9.7.3 デプロイメントマネージャーを使用する場合のクラスタ環境を設定する.....	206
9.8 クラスタ環境での Compute Systems Manager の起動と停止.....	206
9.8.1 Compute Systems Manager のクラスタ運用を一時停止する (Windows) .....	206
9.8.2 Compute Systems Manager のクラスタ運用を一時停止する (Red Hat Enterprise Linux) .....	207
9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows) .....	207
9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux) .....	208
9.9 クラスタ環境でのデータベースの管理.....	208
9.9.1 クラスタ環境でデータベースをバックアップする (Windows) .....	208
9.9.2 クラスタ環境でデータベースをバックアップする (Red Hat Enterprise Linux) .....	209
9.9.3 クラスタ環境でデータベースをリストアする (Windows) .....	211
9.9.4 クラスタ環境でデータベースをリストアする (Red Hat Enterprise Linux) .....	211
9.9.5 クラスタ環境でデータベースをエクスポートする (Windows) .....	212
9.9.6 クラスタ環境でデータベースをエクスポートする (Red Hat Enterprise Linux) .....	214
9.9.7 クラスタ環境でデータベースをインポートする (Windows) .....	215
9.9.8 クラスタ環境でデータベースをインポートする (Red Hat Enterprise Linux) .....	216
9.9.9 データベースを移行するコマンド (hcmds64dbclustersetup) の書式 (Red Hat Enterprise Linux) .....	218
9.10 クラスタ環境からのアンインストール.....	219
9.10.1 クラスタ環境からデプロイメントマネージャーをアンインストールする.....	219
9.10.2 クラスタ環境から Compute Systems Manager をアンインストールする (Windows) .....	220
9.10.3 クラスタ環境から Compute Systems Manager をアンインストールする (Red Hat Enterprise Linux) .....	221
<b>10. トラブルシューティング.....</b>	<b>223</b>
10.1 トラブルシューティングについて.....	224
10.2 トラブルシューティング事例.....	224
10.2.1 トラブルシューティング事例 (ログイン画面が表示されない) .....	224

10.2.2	トラブルシューティング事例 (Compute Systems Manager が起動しない)	224
10.2.3	トラブルシューティング事例 (データベースをリストアできない)	225
10.2.4	トラブルシューティング事例 (Windows のクラスタ環境でデータベースをリストアできない)	226
10.2.5	トラブルシューティング事例 (Red Hat Enterprise Linux のクラスタ環境でデータベースをリストアできない)	227
10.3	保守情報の採取	228
10.3.1	保守情報の採取とは	228
10.3.2	管理サーバの保守情報を採取する (hcmts64getlogs)	229
10.3.3	管理サーバの Java VM スレッドダンプを採取する (Windows)	231
10.3.4	管理サーバの Java VM スレッドダンプを採取する (Linux)	232
10.3.5	管理対象ホストの保守情報を採取する (Windows ホスト)	233
10.3.6	管理対象ホストの保守情報を採取する (Linux ホスト)	234
10.4	監査ログの確認	234
10.4.1	監査ログとは	234
10.4.2	監査ログの環境設定ファイルを設定する	234
10.4.3	監査ログを確認する	235
10.4.4	監査ログの種別	236
10.4.5	監査ログのメッセージ部の出力形式	241
10.4.6	タスクの操作で出力される情報	242
10.4.7	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	243
10.4.8	リクエスト受理時に監査ログの詳細メッセージに出力される情報	243
10.5	ログの設定	245
10.5.1	ログの設定とは	245
10.5.2	Compute Systems Manager のログの設定を変更する	245
<b>付録 A ポートの設定</b>		<b>247</b>
A.1	Compute Systems Manager サーバで使用されるポート	248
A.2	Hitachi Command Suite 共通コンポーネントで使用されるポート	248
A.3	デプロイメントマネージャーで使用されるポート	249
A.4	用途ごとのポートの詳細	250
<b>付録 B プロパティ</b>		<b>257</b>
B.1	Compute Systems Manager サーバのプロパティ	258
B.1.1	Compute Systems Manager サーバのプロパティとは	258
B.1.2	Compute Systems Manager サーバのプロパティの一覧	258
B.1.3	Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)	258
B.1.4	ログ出力に関するプロパティ (logger.properties)	260
B.2	Hitachi Command Suite 共通コンポーネントのプロパティ	260
B.2.1	Hitachi Command Suite 共通コンポーネントのプロパティとは	260
B.2.2	Hitachi Command Suite 共通コンポーネントのプロパティの一覧	261
B.2.3	Web サーバに関するプロパティ (user_httpsd.conf)	263
B.2.4	Web コンテナサーバに関するプロパティ (usrconf.properties)	266
B.2.5	Web コンテナサーバに関するプロパティ (workers.properties)	267
B.2.6	シングルサインオン用 Web サーバに関するプロパティ (user_hssso_httpsd.conf)	267
B.2.7	データベースに関するプロパティ (HiRDB.ini)	268
B.2.8	データベースに関するプロパティ (pdsys)	268
B.2.9	データベースに関するプロパティ (def_pdsys)	269
B.2.10	データベースに関するプロパティ (pdutysys)	269
B.2.11	データベースに関するプロパティ (def_pdutysys)	270
B.2.12	ユーザーアカウントに関するプロパティ (user.conf)	270
B.2.13	LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)	271
B.2.14	LDAP ディレクトリサーバとの連携に関するプロパティの設定例	274
B.2.15	Kerberos サーバとの連携に関するプロパティ (exauth.properties)	276
B.2.16	Kerberos サーバとの連携に関するプロパティの設定例	280

B.2.17 監査ログに関するプロパティ (auditlog.conf) .....	281
B.2.18 管理サーバをクラスタ構成にする場合に設定が必要なプロパティ (cluster.conf) .....	282
B.3 デプロイメントマネージャーで使用するポートに関するプロパティ (Port.ini) .....	283
<b>付録 C Compute Systems Manager が発行する JP1 イベント</b> .....	<b>285</b>
C.1 Compute Systems Manager が発行する JP1 イベントの属性.....	286
C.2 事象種別ごとの JP1 イベント拡張属性.....	286
<b>付録 D バージョン 7xx からのアップグレード</b> .....	<b>293</b>
D.1 バージョン 7xx からのアップグレードとは.....	294
D.2 アップグレードする前の確認事項.....	294
D.3 バージョン 7xx からアップグレードする (非クラスタ環境の場合) .....	295
D.4 バージョン 7xx からアップグレードする (クラスタ環境の場合) .....	297
<b>付録 E このマニュアルの参考情報</b> .....	<b>301</b>
E.1 関連マニュアル.....	302
E.2 このマニュアルでの表記.....	302
E.3 英略語.....	303
E.4 KB (キロバイト) などの単位表記について.....	304
E.5 ディレクトリとフォルダの表記について.....	304
 用語解説.....	 305
 索引.....	 309

# 目次

図 1-1 Windows の管理対象ホストを設定する作業フロー（管理サーバが Windows の場合） .....	30
図 1-2 Windows の管理対象ホストを設定する作業フロー（管理サーバが Linux の場合） .....	30
図 1-3 Linux の管理対象ホストを設定する作業フロー.....	31
図 1-4 LDAP ディレクトリサーバと連携する作業フロー.....	34
図 1-5 Kerberos サーバと連携する作業フロー.....	35
図 6-1 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいるユーザー ID の場合） .....	127
図 6-2 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいないユーザー ID の場合） .....	127
図 9-1 管理サーバがクラスタ環境の場合のクラスタ環境設定手順（Windows） .....	178
図 9-2 管理サーバがクラスタ環境で、Compute Systems Manager がインストールされていない場合のクラスタ環境設定手順（Red Hat Enterprise Linux） .....	179
図 9-3 管理サーバがクラスタ環境で、Compute Systems Manager がインストールされている場合のクラスタ環境設定手順（Red Hat Enterprise Linux） .....	180
図 9-4 管理サーバが非クラスタ環境の場合のクラスタ環境設定手順（Windows） .....	181
図 9-5 管理サーバが非クラスタ環境の場合のクラスタ環境設定手順（Red Hat Enterprise Linux） .....	182



# 表目次

表 3-1 管理サーバのファイアウォールに例外登録が必要なポート (Linux) .....	86
表 7-1 ポート変更時の編集箇所 (Port.ini) .....	159
表 7-2 ポート変更時の編集箇所 (MgrServerList.xml) .....	159
表 8-1 Compute Systems Manager の常駐プロセス一覧 (Windows) .....	164
表 8-2 デプロイメントマネージャーの常駐プロセス一覧.....	164
表 8-3 Compute Systems Manager の常駐プロセス一覧 (Linux) .....	165
表 9-1 クラスタ管理アプリケーションでサービスを登録する順番および各項目に指定する値.....	203
表 10-1 監査ログの種類.....	236
表 10-2 監査ログに出力される監査事象 (種別が StartStop の場合) .....	236
表 10-3 監査ログに出力される監査事象 (種別が Authentication の場合) .....	236
表 10-4 監査ログに出力される監査事象 (種別が ExternalService の場合) .....	237
表 10-5 監査ログに出力される監査事象 (種別が ConfigurationAccess の場合) .....	238
表 10-6 詳細メッセージの<コマンド>に出力される文字列と内容.....	244
表 10-7 詳細メッセージの<ターゲット>に出力される文字列と内容.....	244
表 10-8 詳細メッセージの<パラメーター>に出力される<エレメント>と<属性値>の出力内容.....	244
表 A-1 管理サーバと管理クライアントの通信に使用されるポート.....	250
表 A-2 管理サーバと管理対象の通信に使用されるポート.....	251
表 A-3 Windows の管理サーバと管理対象の通信に使用されるポート (デプロイメントマネージャー) .....	252
表 A-4 管理サーバと外部連携サーバの通信に使用されるポート.....	254
表 A-5 管理クライアントと管理対象の通信に使用されるポート.....	254
表 A-6 管理対象と外部連携サーバの通信に使用されるポート.....	255
表 B-1 Hitachi Command Suite 共通コンポーネントのシングルサインオン用 Web コンテナサーバに関するプロパ ティ (usrconf.properties) .....	266
表 B-2 Compute Systems Manager 用 Web コンテナサーバに関するプロパティ (usrconf.properties) .....	266
表 C-1 SNMP トラップに関するアラートで通知される JP1 イベントの拡張属性.....	286
表 C-2 性能監視に関するアラートで通知される JP1 イベントの拡張属性.....	287
表 C-3 SVP に関するアラートで通知される JP1 イベントの拡張属性.....	288
表 C-4 N+M コールドスタンバイの構成変更に関するアラートで通知される JP1 イベントの拡張属性.....	289
表 C-5 HVM に関するアラートで通知される JP1 イベントの拡張属性.....	290







# はじめに

このマニュアルは **Hitachi Compute Systems Manager** のインストール方法および基本的な環境設定方法、ならびにシステム構成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、**Hitachi Compute Systems Manager** を **Compute Systems Manager** と呼びます。

- 対象読者
- マニュアルの構成
- マイクロソフト製品の表記について
- このマニュアルで使用している記号

# 対象読者

このマニュアルは、**Compute Systems Manager** を使用したサーバ管理システムを構築するシステム管理者の方を対象としています。次のことについて理解していることを前提としています。

- 前提 OS に関する基本的な知識
- TCP/IP ネットワークについての基本的な知識

# 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。

## 1. Compute Systems Manager の概要

基本的なシステム構成、作業フローなど、**Compute Systems Manager** の概要について説明しています。

## 2. インストールとアンインストール

**Compute Systems Manager** のインストール時の前提条件、インストールの手順、新規インストール時の環境設定、およびアンインストール手順について説明しています。

## 3. 管理サーバの環境設定

SNMP トラップ、ユーザーアカウントの設定など、管理サーバの環境設定について説明しています。

## 4. 管理対象の設定

**Compute Systems Manager** の管理対象を設定するための前提条件および手順について説明しています。

## 5. セキュリティ設定

SSL 通信などセキュリティ設定について説明しています。

## 6. 外部認証サーバとの連携

外部認証サーバと連携して認証する方法について説明しています。

## 7. デプロイメントマネージャーの環境設定

デプロイメントマネージャーの前提ソフトウェアおよびデプロイメントマネージャーのインストール手順、デプロイメントマネージャーで使用されるポートおよび管理対象リソースの設定などについて説明しています。

## 8. 管理サーバの運用

**Compute Systems Manager** の起動と停止、データベースの管理など、管理サーバの運用について説明しています。

## 9. クラスタを使用するための環境設定と運用

クラスタを使用して運用するための **Compute Systems Manager** のインストールと環境設定、起動と停止、データベースの管理などについて説明しています。

## 10. トラブルシューティング

**Compute Systems Manager** 運用中に障害が発生した場合に必要な保守情報の採取方法、ログの設定について説明しています。

## 付録 A. ポートの設定

**Compute Systems Manager** で使用されるポートについて説明しています。

## 付録 B. プロパティ

Compute Systems Manager のプロパティについて説明しています。

#### 付録 C. Compute Systems Manager が発行する JP1 イベント

Compute Systems Manager で発行される JP1 イベントの内容について説明しています。

#### 付録 D. バージョン 7.x.x からのアップグレード

Compute Systems Manager をバージョン 7.x.x からアップグレードする手順について説明しています。

#### 付録 E. 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。

#### 用語解説

Compute Systems Manager を使用するために理解しておきたい用語の意味について解説しています。

## 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
.NET Framework	Microsoft® .NET Framework
Hyper-V	Microsoft® Hyper-V®
IIS	Microsoft® Internet Information Services
Internet Explorer	Windows® Internet Explorer®
SQL Server	Microsoft® SQL Server
Windows	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Microsoft® Windows® 7</li><li>• Windows® 8</li><li>• Windows® 8.1</li><li>• Windows® 10</li><li>• Microsoft® Windows Server® 2008</li><li>• Microsoft® Windows Server® 2008 R2</li><li>• Microsoft® Windows Server® 2012</li><li>• Microsoft® Windows Server® 2012 R2</li><li>• Microsoft® Windows Vista®</li></ul>
Windows PowerShell	Microsoft® Windows® PowerShell
Windows Server 2008	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Microsoft® Windows Server® 2008</li><li>• Microsoft® Windows Server® 2008 R2</li></ul>
Windows Server 2008 R2	Microsoft® Windows Server® 2008 R2
Windows Server 2012	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Microsoft® Windows Server® 2012</li><li>• Microsoft® Windows Server® 2012 R2</li></ul>
Windows Server Failover Clustering	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Windows Server® Failover Clustering</li><li>• Microsoft® Failover Cluster</li></ul>

## 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。

記号	意味
[ ] (角括弧)	GUI 操作の説明 メニュータイトル、メニュー項目、タブ名、およびボタンの名称を示します。メニュー項目を連続して選択する場合は、[ ] を「-」（ハイフン）でつないで説明しています。 キー操作の説明 キーの名称を示します。
< > (山括弧)	可変値であることを示します。

コマンドの書式の説明では、次に示す記号を使用しています。

記号	意味と例
 (ストローク)	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。
{ } (波括弧)	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。
[ ] (角括弧)	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)。
... 点線 (リーダー)	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。

# Compute Systems Manager の概要

この章では、基本的なシステム構成、作業フローなど、Compute Systems Manager の概要について説明します。

- 1.1 Compute Systems Manager の概要
- 1.2 システム構成
- 1.3 関連製品
- 1.4 作業フローの全体像
- 1.5 導入の作業フロー
- 1.6 環境設定の作業フロー
- 1.7 運用と保守の作業フロー

# 1.1 Compute Systems Manager の概要

## 1.1.1 Compute Systems Manager とは

Compute Systems Manager は、大規模なシステム環境上で遠隔地に分散されたサーバリソースの管理・運用を支援するソフトウェアです。Compute Systems Manager は Hitachi Command Suite 製品のラインアップの 1 つです。Hitachi Command Suite 製品を使用している環境に Compute Systems Manager を導入すると、ストレージリソースとサーバリソースを一元的に管理および運用できます。

さらに、Device Manager と Compute Systems Manager を同じ環境で使用する場合、Device Manager で管理するホストの情報と Compute Systems Manager で管理するホストの情報が自動で同期するため、ホスト管理業務の効率が向上します。

Compute Systems Manager には、システムを円滑に構築し、運用できる次の特徴があります。

- 新規インストール後、画面のガイダンスに従えば運用を開始するまでに最低限必要な設定を完了できます。
- GUI の操作でシステム設定できます。
- Compute Systems Manager のユーザーを外部認証サーバで管理できます。
- ユーザーおよびセキュリティに関する設定を、Hitachi Command Suite 製品共通の機能を使用して管理できます。

### 関連項目

- [1.1.2 Compute Systems Manager の管理対象](#)
- [1.2.1 システムの構成要素](#)
- [1.2.2 基本的なシステム構成](#)
- [1.2.3 ネットワーク構成](#)
- [1.3 関連製品](#)

## 1.1.2 Compute Systems Manager の管理対象

Compute Systems Manager では、次のリソースを管理できます。

- Windows ホスト、および Linux ホスト  
ホストは物理環境だけでなく、仮想環境も管理対象です。
- ハイパーバイザー  
Hyper-V および VMware ESXi が管理対象です。
- 仮想マシン  
仮想マシンはハイパーバイザー単位で管理されます。
- 日立製のサーバ  
シャーシおよびラックマウントサーバが管理対象です。  
ブレードサーバはシャーシ単位で管理されます。
- LPAR  
LPAR はブレードサーバ単位で管理されます。

### 関連項目

- [1.1.1 Compute Systems Manager とは](#)

- [1.2.1 システムの構成要素](#)
- [1.2.2 基本的なシステム構成](#)
- [1.4 作業フローの全体像](#)

## 1.2 システム構成

### 1.2.1 システムの構成要素

Compute Systems Manager を使用したシステムは、次の要素で構成されています。

- 管理クライアント

Compute Systems Manager を GUI または CLI で操作する際に使用するマシンです。GUI は Web ブラウザーで使用できます。CLI を利用するためには、管理クライアントに CLI をインストールする必要があります。

- 管理サーバ

Compute Systems Manager をインストールしたマシンです。管理サーバでリソースを一元管理します。

管理サーバは次のコンポーネントから構成されています。

- Hitachi Command Suite 共通コンポーネント  
ユーザーおよびセキュリティに関する Hitachi Command Suite 製品共通の機能を提供します。
- Compute Systems Manager サーバ  
リソースを管理します。

- 管理対象リソース

Compute Systems Manager で管理されるホスト、サーバ、関連するシステムなどのリソースです。

- LAN

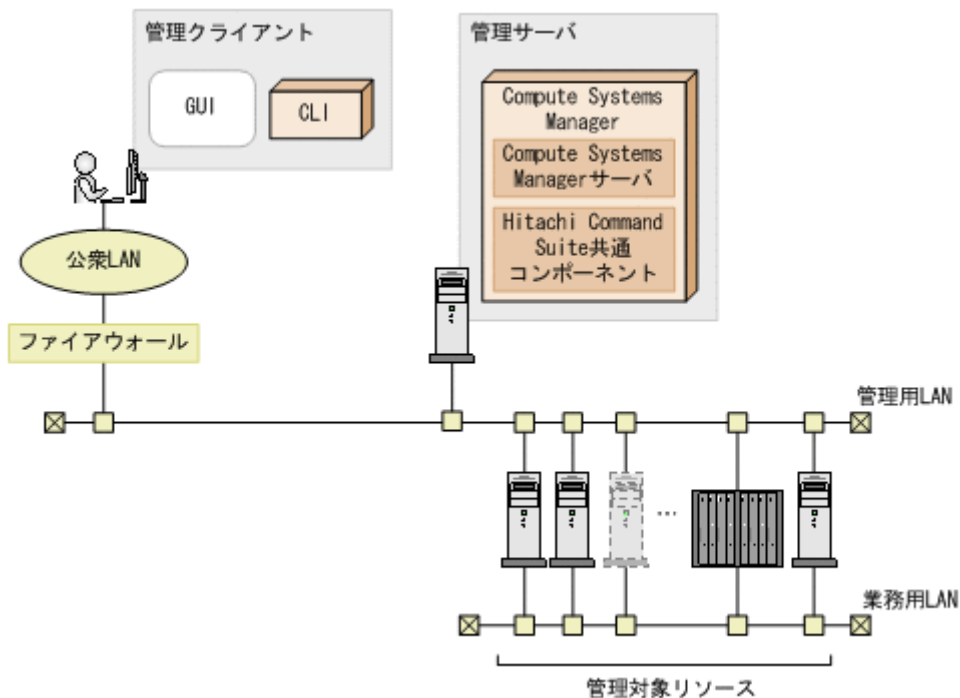
管理サーバと管理クライアント間、および管理サーバと管理対象リソース間を TCP/IP で接続します。

#### 関連項目

- [1.2.2 基本的なシステム構成](#)

### 1.2.2 基本的なシステム構成

Compute Systems Manager を使用する場合の基本的なシステム構成を次に示します。



上記の図で示すシステム構成は、次の条件で構築されています。

- Compute Systems Manager 以外の Hitachi Command Suite 製品を導入していない  
Compute Systems Manager 以外の Hitachi Command Suite 製品を導入する場合は、管理サーバに、導入する Hitachi Command Suite 製品のサーバが追加されます。
- 外部認証サーバを使用していない  
Compute Systems Manager の機能でユーザーを管理しています。
- 管理サーバと管理クライアント間の通信に SSL 通信を使用していない



**重要** 複数の Compute Systems Manager から、同一の管理対象リソースを操作しないでください。次に示す操作を複数の Compute Systems Manager から実施すると、障害が発生するおそれがあります。

- 管理対象リソースの構成変更を伴う操作  
例：N+M コールドスタンバイ、論理分割、デプロイメントマネージャー
- 管理対象リソースの状態変更を伴う操作  
例：管理対象リソースの電源管理

Compute Systems Manager を、サービスのダウンに備えた冗長構成にする場合は、クラスタを使用してください。



**参考** 管理サーバとシャード間の通信では、IPv6 も使用できます。

#### 関連項目

- 1.2.1 システムの構成要素
- 1.2.3 ネットワーク構成
- 1.4 作業フローの全体像
- 2.2.8 IPv6 を使用する場合は設定を確認する
- 9.1 クラスタを使用するための環境設定と運用とは



## 1.2.3 ネットワーク構成

セキュリティ上のリスクを低減する目的で、一般的に、管理用 LAN と業務用 LAN は切り離されています。

管理用 LAN の構成に関する指針を次に示します。

- 公衆 LAN と管理用 LAN の間にファイアウォールを設置することを推奨します。
- 業務用 LAN からのトラフィックが、管理用 LAN を流れたり経由したりしないようにしてください。

### 関連項目

- [1.1.2 Compute Systems Manager の管理対象](#)
- [1.4 作業フローの全体像](#)

## 1.3 関連製品

Compute Systems Manager は、Hitachi Command Suite 製品のラインアップの 1 つです。

Compute Systems Manager 以外の Hitachi Command Suite 製品を次に示します。

- Device Manager
- Tiered Storage Manager
- Dynamic Link Manager
- Replication Manager
- Tuning Manager
- Global Link Manager

Hitachi Command Suite 製品を同じマシンで運用すると、ユーザー、ライセンス、およびセキュリティに関する設定を共通で管理できます。また、Device Manager と Compute Systems Manager を同じマシンで運用すると、Device Manager で管理するホストの情報と Compute Systems Manager で管理するホストの情報が自動で同期されるため、ホスト管理業務の効率が向上します。



**重要** Compute Systems Manager と Device Manager 間で自動的に同期されるのは、ホスト情報だけです。その他のリソースの情報は、同期されません。

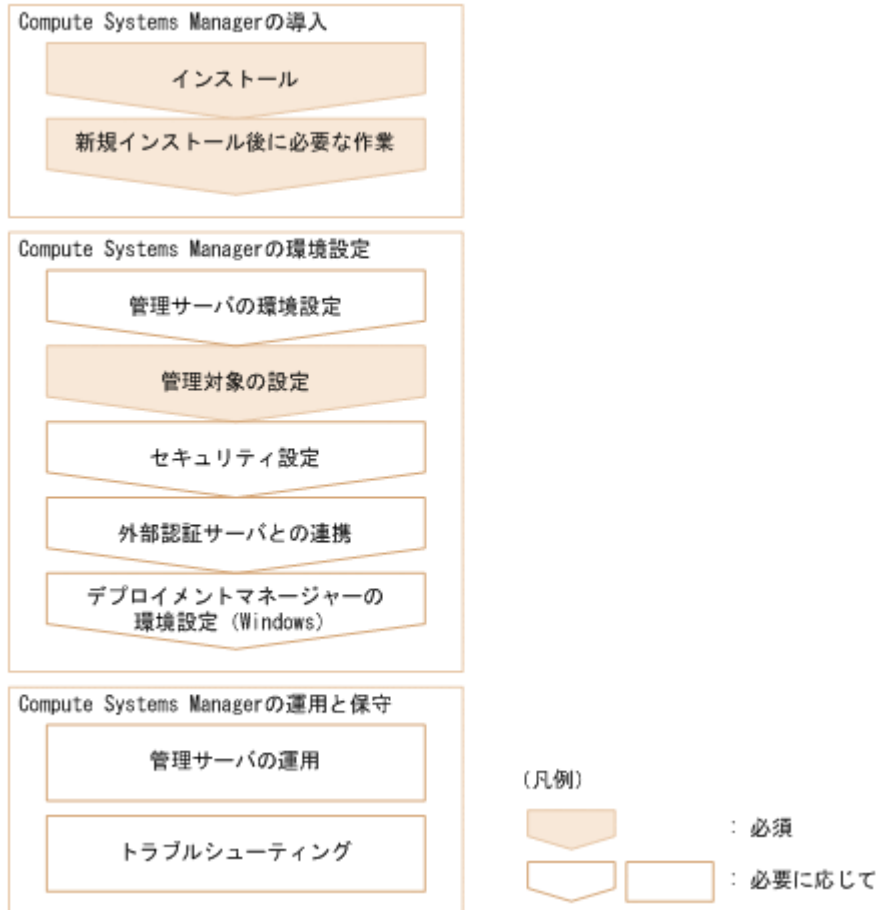
---

### 関連項目

- [1.1.1 Compute Systems Manager とは](#)

## 1.4 作業フローの全体像

Compute Systems Manager の導入から運用までの作業フローを次に示します。



このマニュアルでは、インストール、システム設定、システム運用、および保守について説明します。管理クライアントでの運用および保守については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

## 関連項目

- 1.5.1 インストールの流れ
- 1.5.2 新規インストール後に必要な作業の流れ
- 1.6.1 SNMP トラップの設定の流れ
- 1.6.2 管理対象ホストの設定の流れ
- 1.6.3 管理クライアントとの通信のセキュリティ設定の流れ
- 1.6.4 SMTP サーバとの通信のセキュリティ設定の流れ
- 1.6.5 管理対象サーバとの通信のセキュリティ設定の流れ
- 1.6.6 Device Manager サーバとの通信のセキュリティ設定の流れ
- 1.6.7 LDAP ディレクトリサーバとの通信のセキュリティ設定の流れ
- 1.6.8 外部認証サーバとの連携の流れ
- 1.7.1 管理サーバの移行の流れ
- 1.7.2 データベースの管理の流れ
- 1.7.3 ネットワーク構成の変更の流れ
- 1.7.4 トラブルシューティングの流れ

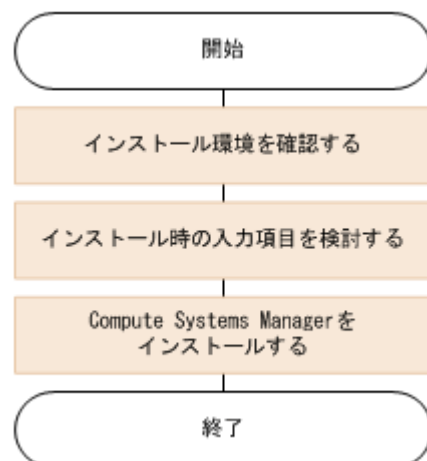
## 1.5 導入の作業フロー

### 1.5.1 インストールの流れ

管理サーバに Compute Systems Manager をインストールします。

インストールには、インストールメディアを利用する方法と、Hitachi Command Suite の仮想アプライアンスを利用する方法があります。

Compute Systems Manager をインストールメディアからインストールする作業フローを次に示します。



Hitachi Command Suite の仮想アプライアンスを利用する場合は、作成される仮想マシンに Compute Systems Manager がインストールされているため、このフローで説明しているインストールの各作業は不要です。

仮想アプライアンスを利用したインストールについては、マニュアル「*Hitachi Command Suite 仮想アプライアンス インストールガイド*」を参照してください。

#### 関連項目

- [1.5.2 新規インストール後に必要な作業の流れ](#)
- [1.6.2 管理対象ホストの設定の流れ](#)
- [2.1 Compute Systems Manager のインストール方法について](#)
- [2.2.1 インストール環境の確認とは](#)
- [2.4.1 インストールとは](#)

### 1.5.2 新規インストール後に必要な作業の流れ

新規インストール後に必要な作業フローを次に示します。作業には Compute Systems Manager の System アカウントを使用します。



#### 関連項目

- 1.6.2 管理対象ホストの設定の流れ
- 2.5.1 新規インストール後に必要な作業とは
- 2.5.2 管理サーバにアクセスできるか確認する
- 2.5.3 プラグインライセンスを登録する
- 2.5.4 System アカウントのパスワードを変更する
- 2.5.5 System アカウントにメールアドレスを設定する
- 2.5.6 E メール通知を設定する
- 2.5.7 E メールで通知するアラートレベルを設定する
- 2.5.8 管理対象リソースを登録する
- 2.5.9 サーバ管理者のユーザーアカウントを作成する
- 2.5.10 リソースグループを設定する
- 2.5.11 ユーザーグループを設定する

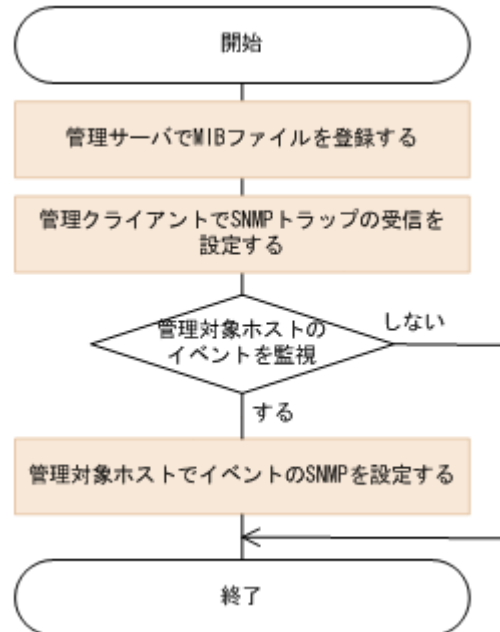
## 1.6 環境設定の作業フロー

### 1.6.1 SNMP トラップの設定の流れ

管理対象ホストから送信される SNMP トラップを Compute Systems Manager で受信するには、管理サーバおよび管理クライアントでそれぞれ設定する必要があります。

また、管理対象ホストの OS で発生したイベントを送信するには、管理対象ホストでイベントの SNMP を設定する必要があります。

SNMP トラップの設定の作業フローを次に示します。



#### 関連項目

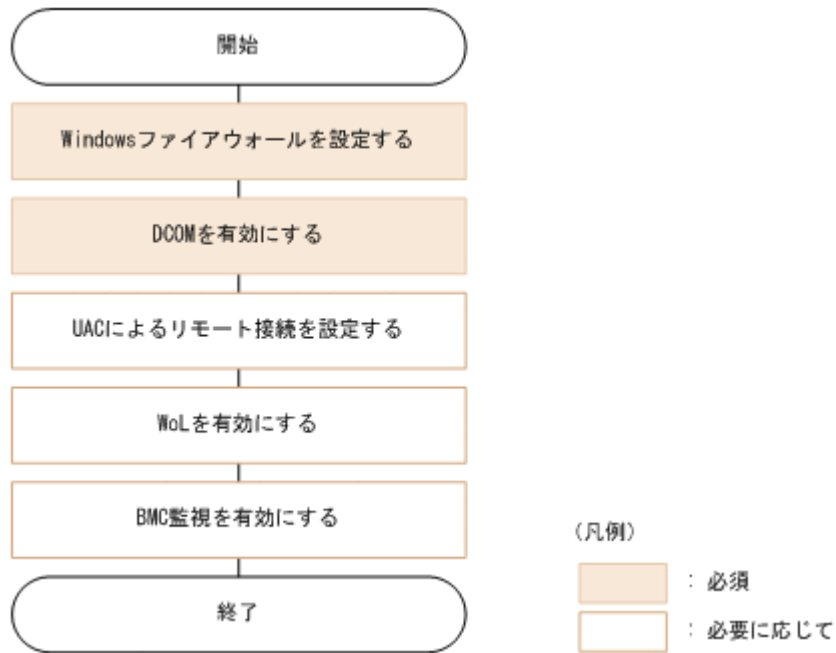
- ・ 3.1.1 SNMP トラップの設定とは
- ・ 3.1.3 インバンド SNMP トラップの監視とは

### 1.6.2 管理対象ホストの設定の流れ

管理対象として追加したホストに、Compute Systems Manager で管理できるよう設定します。設定内容は管理サーバおよび管理対象ホストの OS によって異なります。

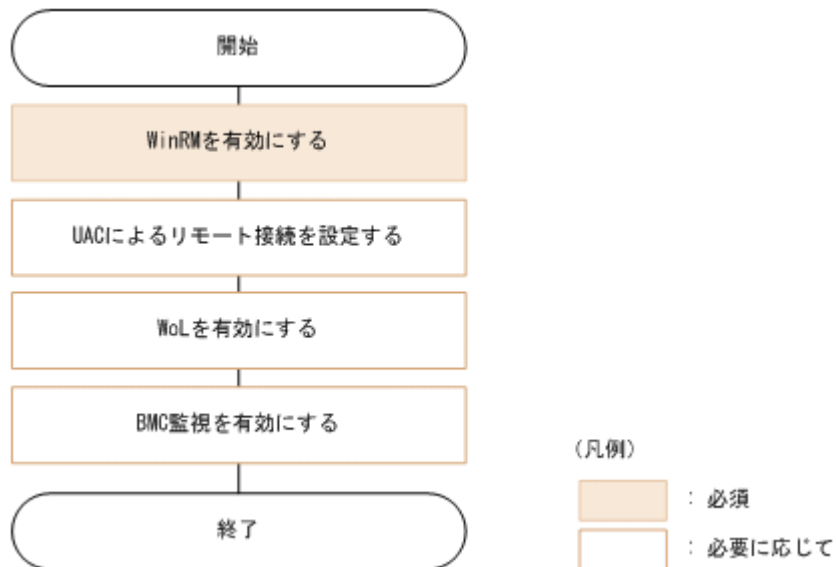
管理サーバが Windows の場合、Windows の管理対象ホストを設定する作業フローを次に示します。

図 1-1 Windows の管理対象ホストを設定する作業フロー（管理サーバが Windows の場合）



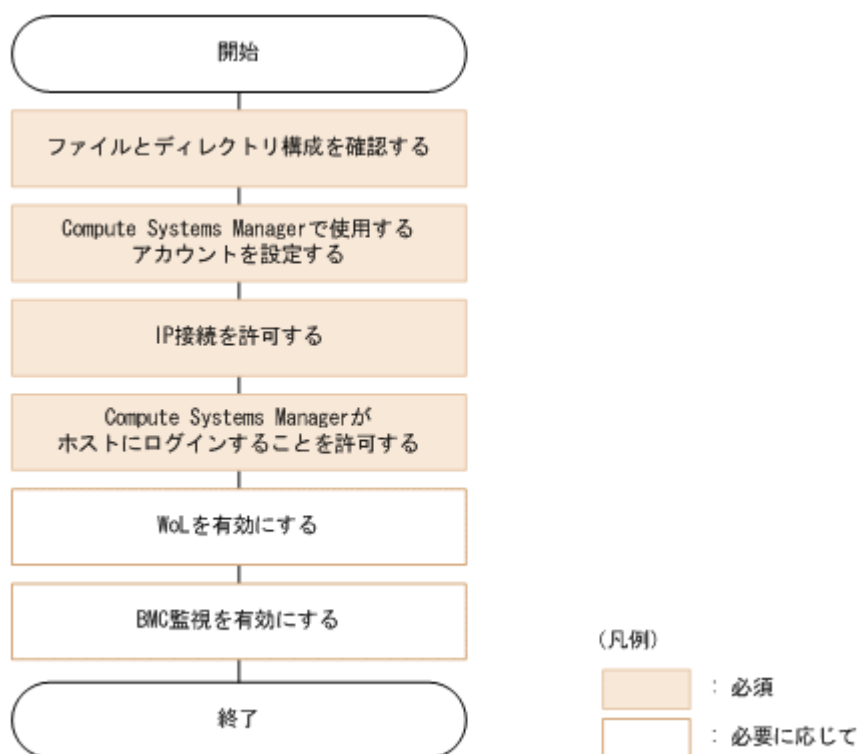
管理サーバが Linux の場合，Windows の管理対象ホストを設定する作業フローを次に示します。

図 1-2 Windows の管理対象ホストを設定する作業フロー（管理サーバが Linux の場合）



Linux の管理対象ホストを設定する作業フローを次に示します。

図 1-3 Linux の管理対象ホストを設定する作業フロー



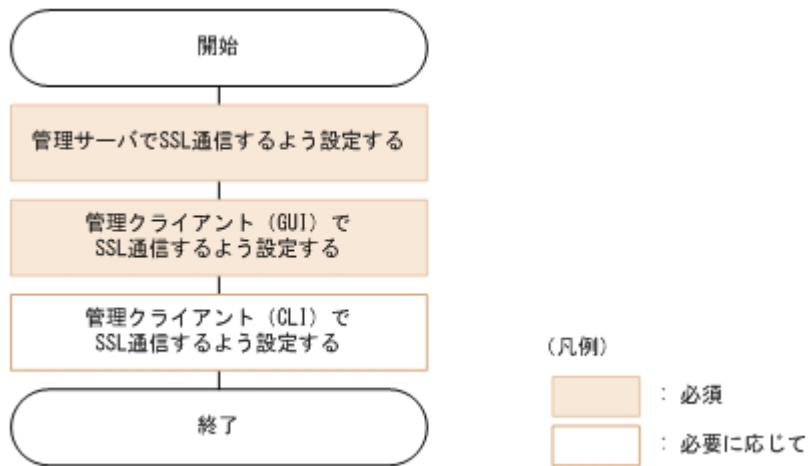
#### 関連項目

- 4.1.1 WoL を有効にする
- 4.1.2 BMC 監視を有効にする
- 4.3.2 Windows ファイアウォールを設定する (Windows ホスト)
- 4.3.3 DCOM を有効にする (Windows ホスト)
- 4.3.4 WinRM を有効にする (Windows ホスト)
- 4.3.5 UAC を使用したリモート接続を設定する (Windows ホスト)
- 4.4.2 OS のファイルおよびディレクトリ構成の確認項目 (Linux ホスト)
- 4.4.3 Compute Systems Manager で使用するアカウントを設定する (Linux ホスト)
- 4.4.4 IP 接続を許可する (Linux ホスト)
- 4.4.5 管理対象ホストへのログインの許可とは

### 1.6.3 管理クライアントとの通信のセキュリティ設定の流れ

Compute Systems Manager の設定を変更することで、管理サーバと管理クライアントの通信に SSL 通信を利用できます。

管理サーバと管理クライアントの通信のセキュリティを設定する作業フローを次に示します。



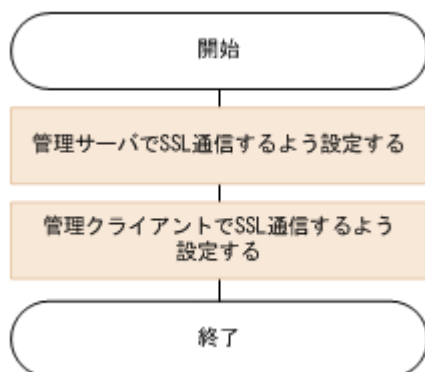
#### 関連項目

- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.2.2 管理サーバで SSL 通信するよう設定する (管理クライアントとの通信路)
- 5.2.3 管理クライアントで SSL 通信するよう設定する (GUI との通信路)
- 5.2.4 管理クライアントで SSL 通信するよう設定する (CLI との通信路)

## 1.6.4 SMTP サーバとの通信のセキュリティ設定の流れ

Compute Systems Manager の設定を変更することで、管理サーバと SMTP サーバの通信に SSL 通信を利用できます。

管理サーバと SMTP サーバの通信のセキュリティを設定する作業フローを次に示します。



#### 関連項目

- 5.3.1 SMTP サーバとの通信のセキュリティ設定とは
- 5.3.2 管理サーバで SSL 通信するよう設定する (SMTP サーバとの通信路)

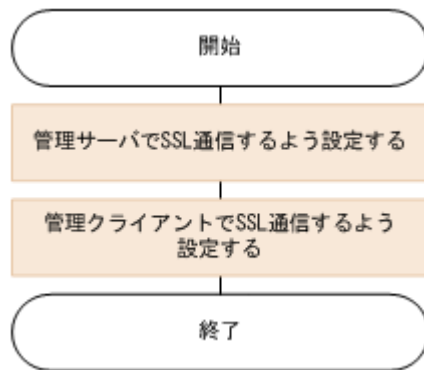
## 1.6.5 管理対象サーバとの通信のセキュリティ設定の流れ

管理サーバと日立製のサーバの情報の送受信には、SSL 通信が適用されます。

デフォルトの設定で運用する場合、Compute Systems Manager に同梱されている証明書が使用されますが、セキュリティを確保するために設定を変更することもできます。

管理サーバと日立製のサーバの通信のセキュリティをデフォルトの設定から変更する作業フローを次に示します。





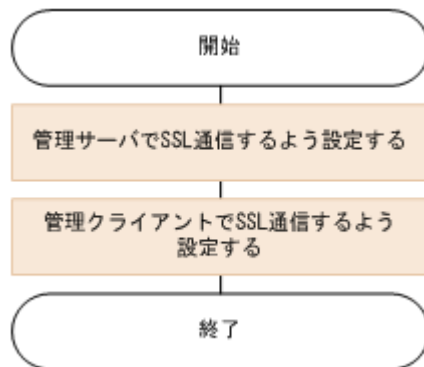
#### 関連項目

- ・ 5.4.1 管理対象サーバとの通信のセキュリティ設定とは
- ・ 5.4.2 管理サーバで SSL 通信するよう設定する（管理対象サーバとの通信路）

### 1.6.6 Device Manager サーバとの通信のセキュリティ設定の流れ

Compute Systems Manager の設定を変更することで、管理サーバと Device Manager サーバの通信に SSL 通信を利用できます。

管理サーバと Device Manager サーバの通信のセキュリティを設定する作業フローを次に示します。



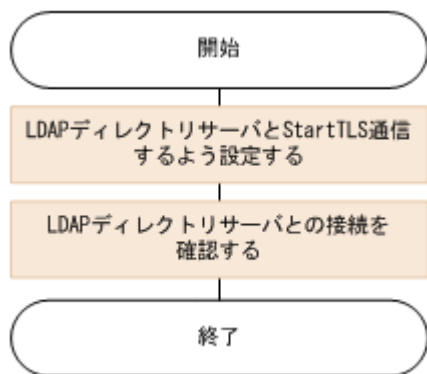
#### 関連項目

- ・ 5.5.1 Device Manager サーバとの通信のセキュリティ設定とは
- ・ 5.5.2 管理サーバで SSL 通信するよう設定する（Device Manager サーバとの通信路）

### 1.6.7 LDAP ディレクトリサーバとの通信のセキュリティ設定の流れ

Compute Systems Manager の設定を変更することで、管理サーバと LDAP ディレクトリサーバの通信に StartTLS 通信を利用できます。

管理サーバと LDAP ディレクトリサーバの通信のセキュリティを設定する作業フローを次に示します。



#### 関連項目

- ・ 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは
- ・ 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する

## 1.6.8 外部認証サーバとの連携の流れ

管理サーバと管理クライアントで設定すれば、外部認証サーバと連携してユーザーアカウントを管理できます。

LDAP ディレクトリサーバと連携する場合と、Kerberos サーバと連携する場合とに分けて次に示します。

図 1-4 LDAP ディレクトリサーバと連携する作業フロー

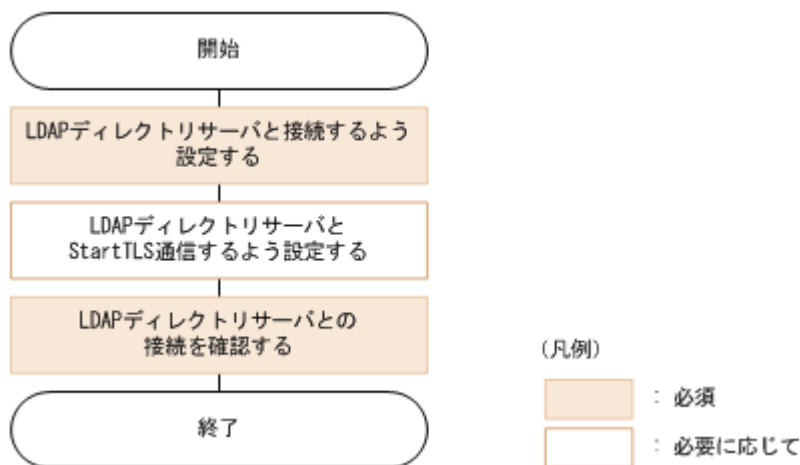


図 1-5 Kerberos サーバと連携する作業フロー



#### 関連項目

- ・ 6.1.1 外部認証サーバとの連携とは
- ・ 6.2.1 LDAP ディレクトリサーバと連携するための操作フロー
- ・ 6.2.2 Kerberos サーバと連携するための操作フロー
- ・ 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- ・ 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する
- ・ 6.7.2 Kerberos サーバと接続するよう設定する

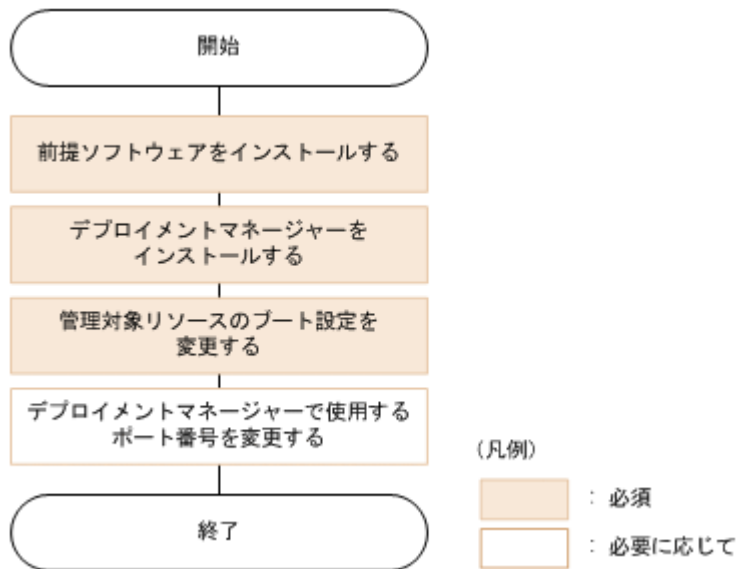
## 1.6.9 デプロイメントマネージャーの環境設定の流れ

デプロイメントマネージャーを運用すると、ディスクの障害や破損が発生した場合に管理対象リソースのディスクデータを過去の状態に戻したり、同じ環境の管理対象リソースを複数複製したりできます。

デプロイメントマネージャーは、管理サーバの OS が Windows の場合に運用できます。

デプロイメントマネージャーを運用するための環境を設定する作業フローを次に示します。

Compute Systems Manager のインストール時にデプロイメントマネージャーをインストールできます。



#### 関連項目

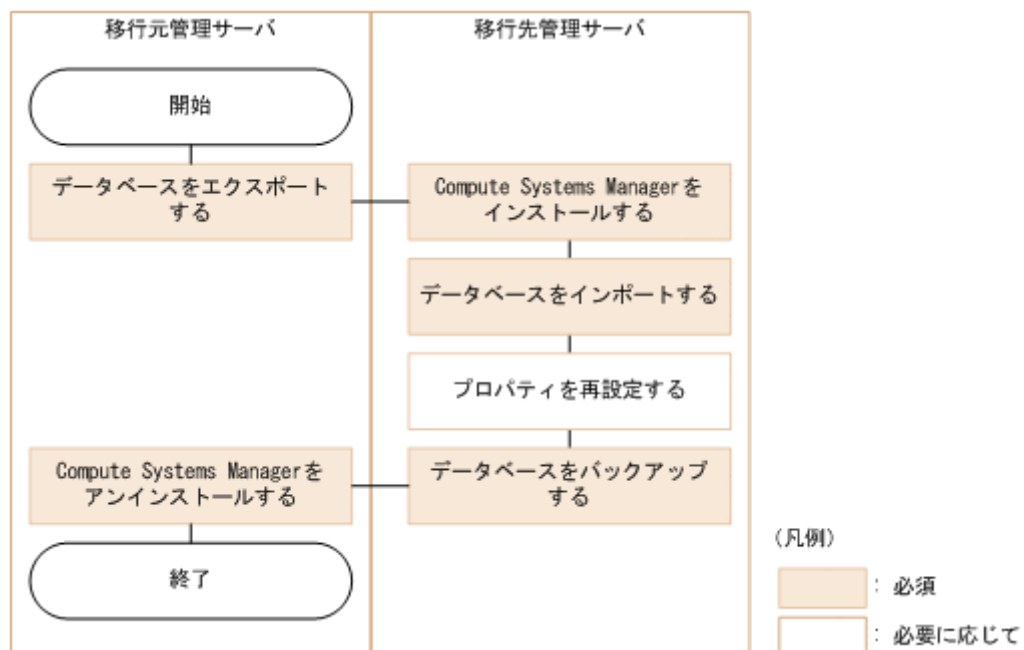
- 7.1 デプロイメントマネージャーの環境設定とは
- 7.7 管理対象リソースのブートの設定を変更する
- 7.8 デプロイメントマネージャーが使用するポート番号を変更する

## 1.7 運用と保守の作業フロー

### 1.7.1 管理サーバの移行の流れ

管理サーバをリプレースしたいときに、管理サーバにある Compute Systems Manager の環境を移行できます。

管理サーバの環境を移行する作業フローを次に示します。



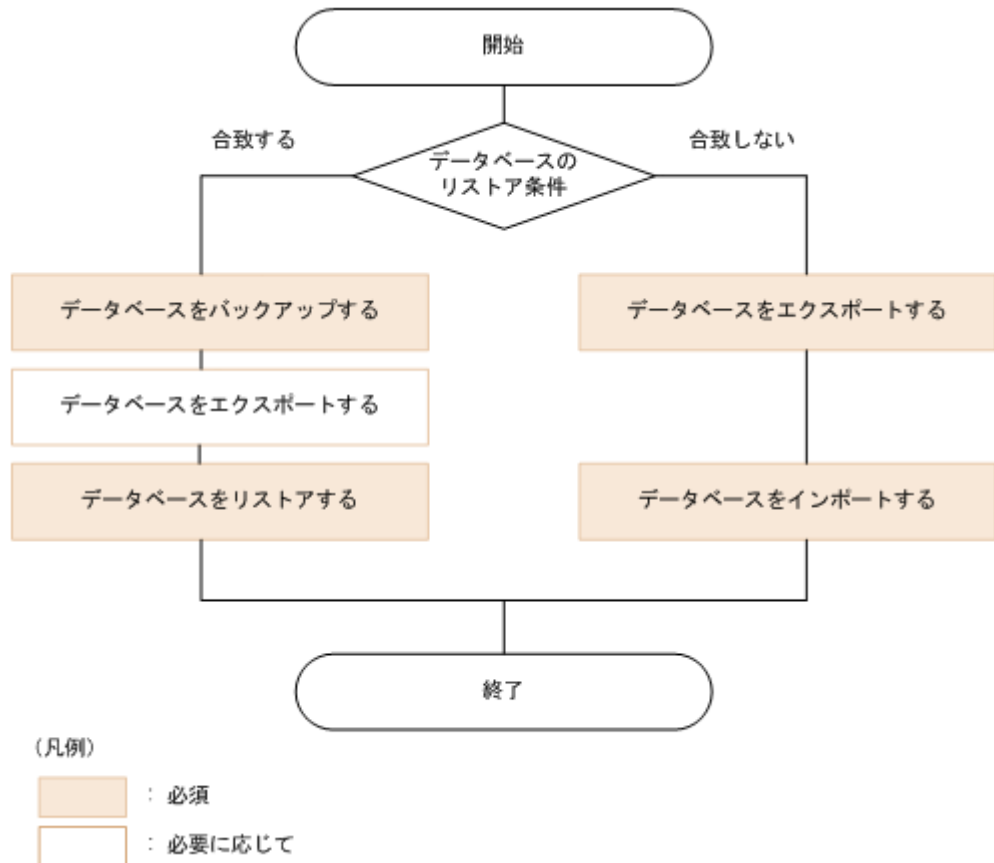
## 関連項目

- ・ 1.5.1 インストールの流れ
- ・ 1.7.2 データベースの管理の流れ
- ・ 2.6.1 アンインストールとは
- ・ 8.2.7 移行元サーバからデータベースをエクスポートする
- ・ 8.2.8 移行先サーバにデータベースをインポートする

## 1.7.2 データベースの管理の流れ

データベースの障害に備えて、データベースをバックアップします。

データベースを管理する作業フローを次に示します。



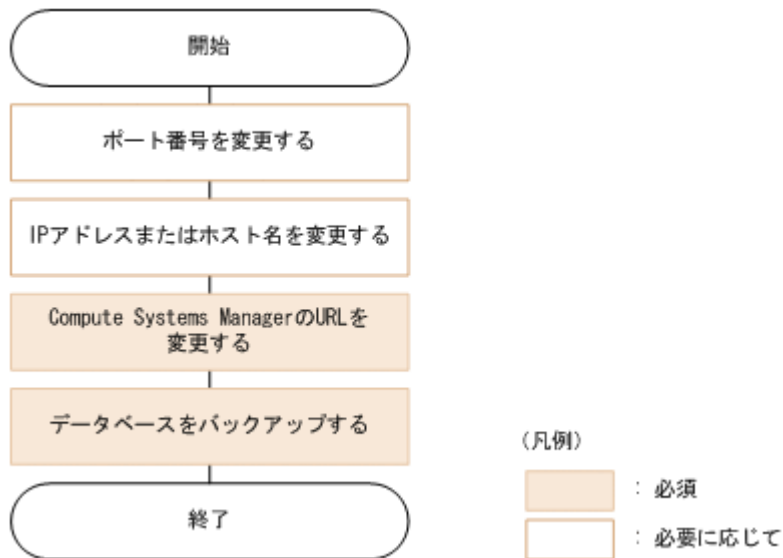
## 関連項目

- ・ 8.2.1 データベースの管理とは
- ・ 8.2.3 データベースをバックアップする
- ・ 8.2.5 データベースをリストアする
- ・ 8.2.7 移行元サーバからデータベースをエクスポートする
- ・ 8.2.8 移行先サーバにデータベースをインポートする

## 1.7.3 ネットワーク構成の変更の流れ

ネットワーク構成を変更した場合、管理サーバの設定も変更する必要があります。

ネットワーク構成を変更する作業フローを次に示します。



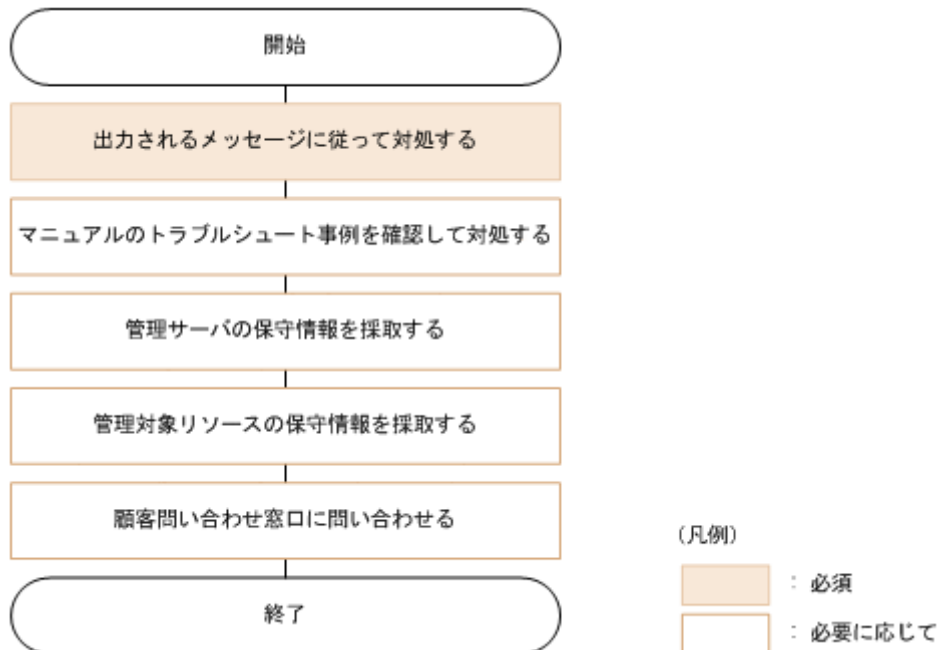
#### 関連項目

- 1.7.2 データベースの管理の流れ
- (3) ポートを変更する
- (3) 管理サーバのホスト名または IP アドレスを変更する
- (2) Compute Systems Manager の URL を変更する
- 8.2.3 データベースをバックアップする

## 1.7.4 トラブルシューティングの流れ

Compute Systems Manager 運用時にトラブルが発生した場合、エラーメッセージを見てトラブルに対処したり、トラブルの原因を突き止めるために資料を採取したりします。

トラブルシューティング時の作業フローを次に示します。



## 関連項目

- 10.1 [トラブルシューティングについて](#)
- 10.3.2 [管理サーバの保守情報を採取する \(hcmds64getlogs\)](#)
- 10.3.5 [管理対象ホストの保守情報を採取する \(Windows ホスト\)](#)
- 10.3.6 [管理対象ホストの保守情報を採取する \(Linux ホスト\)](#)





# インストールとアンインストール

この章では、Compute Systems Manager のインストール時の前提条件、インストールの手順、新規インストール時の環境設定、およびアンインストール手順について説明します。

- 2.1 Compute Systems Manager のインストール方法について
- 2.2 インストール環境の確認
- 2.3 インストール時の入力項目の検討
- 2.4 インストール
- 2.5 新規インストール後に必要な作業
- 2.6 アンインストール

## 2.1 Compute Systems Manager のインストール方法について

Compute Systems Manager のインストール方法には、次に示す 2 つの方法があります。

### インストールメディアからインストールする

Compute Systems Manager には、単体インストールメディアと統合インストールメディアの 2 種類があります。

ほかの Hitachi Command Suite 製品をあわせて購入した場合は、統合インストールメディアが提供されます。

インストールメディアからインストールする場合は、あらかじめインストール環境を確認してください。

### Hitachi Command Suite の仮想アプライアンスを利用してインストールする

ハイパーバイザーに VMware ESXi を利用する場合、Hitachi Command Suite の仮想アプライアンスを利用して、Compute Systems Manager を含む Hitachi Command Suite 製品がインストールされた仮想マシンを作成できます。

仮想アプライアンスを利用する場合は、このマニュアルで説明しているインストールの準備作業、およびインストールメディアを使用したインストール作業は不要です。ただし、仮想マシンに Hitachi Command Suite 製品を追加でインストールしたり、アップグレードしたりする場合は、インストールメディアから対象となる製品をインストールしてください。

仮想アプライアンスを利用したインストールについては、マニュアル「*Hitachi Command Suite 仮想アプライアンス インストールガイド*」を参照してください。

### 関連項目

- 1.5.1 インストールの流れ
- 2.2.1 インストール環境の確認とは

## 2.2 インストール環境の確認

### 2.2.1 インストール環境の確認とは

Compute Systems Manager のインストールを開始する前に、運用できる環境か確認する必要があります。Windows の管理サーバにインストールする場合は、デプロイメントマネージャーをインストールするかどうかを検討します。



#### 重要

- インストールやインストール後の設定のためには、Administrator 権限 (Windows)、または root (Linux) でのログインが必要です。
- Hitachi Command Suite の仮想アプライアンスを利用する場合は、作成される仮想マシンに Compute Systems Manager がインストールされています。また、Compute Systems Manager の動作に必要な設定がデフォルトで設定されているため、このマニュアルで説明しているインストール環境の確認は不要です。仮想アプライアンスを利用したインストールについては、マニュアル「*Hitachi Command Suite 仮想アプライアンス インストールガイド*」を参照してください。

## 関連項目

- 2.2.2 システム要件を確認する
- 2.2.3 ポート番号が競合していないことを確認する
- 2.2.4 管理サーバのシステム環境を確認する (Linux)
- 2.2.5 カーネルパラメーターとシェル制限を設定する (Linux)
- 2.2.6 ファイアウォールの例外登録をする (Linux)
- 2.2.8 IPv6 を使用する場合の設定を確認する
- 2.2.9 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定を確認する
- 2.3.1 インストール時の入力項目の検討とは
- 7.1 デプロイメントマネージャーの環境設定とは

## 2.2.2 システム要件を確認する

管理サーバの前提ハードウェア要件、前提ソフトウェア要件などについて確認します。詳細は、ソフトウェア添付資料を参照してください。

### 関連項目

- 2.2.1 インストール環境の確認とは

## 2.2.3 ポート番号が競合していないことを確認する

Compute Systems Manager を新規インストールする前に、Compute Systems Manager が使用するポートが管理サーバでほかの製品によって使用されていないか確認する必要があります。

Compute Systems Manager が使用するポートをほかの製品が使用している場合、Compute Systems Manager やそのほかの製品が正常に動作しなくなるおそれがあります。

管理サーバで使用されているポートの使用状況は、netstat コマンドを使って確認します。



**重要** Compute Systems Manager は、SNMP トラップの受信で 162/udp を使用します。Compute Systems Manager 以外の製品がすでに 162/udp を使用している場合、インストール中に Compute Systems Manager が使用するポート変更を促すメッセージが表示されます。この場合、メッセージの表示内容に従い、Compute Systems Manager で使用するポートを変更してください。

### 関連項目

- 2.2.1 インストール環境の確認とは
- (3) ポートを変更する
- A.1 Compute Systems Manager サーバで使用されるポート
- A.2 Hitachi Command Suite 共通コンポーネントで使用されるポート

## 2.2.4 管理サーバのシステム環境を確認する (Linux)

/etc/hosts ファイルには、localhost と管理サーバのホスト名が記述されている必要があります。

/etc/hosts ファイルに、localhost と管理サーバのホスト名が記述されていない場合、インストール時にエラーが発生するおそれがあります。

#### 関連項目

- ・ 2.2.1 インストール環境の確認とは

## 2.2.5 カーネルパラメーターとシェル制限を設定する (Linux)

Linux の場合、Compute Systems Manager をインストールする前に、カーネルパラメーターとシェル制限を設定する必要があります。

設定するカーネルパラメーターとシェル制限の値については、「ソフトウェア添付資料」を参照してください。

#### 事前に完了しておく操作

- ・ カーネルパラメーターおよびシェル制限のファイルのバックアップ取得
- ・ カーネルパラメーターおよびシェル制限の値の見積もり

カーネルパラメーターとシェル制限を設定する手順を次に示します。

1. 見積もり結果に従って、各パラメーターに値を設定します。
2. OS を再起動します。

#### 関連項目

- ・ 2.2.1 インストール環境の確認とは

## 2.2.6 ファイアウォールの例外登録をする (Linux)

Linux 環境でのファイアウォールの例外登録は、ユーザーが手動で実施する必要があります。

ファイアウォールの例外リストに、Compute Systems Manager で使用されるポート番号を登録してください。

#### 関連項目

- ・ 2.2.1 インストール環境の確認とは
- ・ 3.5.9 管理サーバのファイアウォールに例外登録をする (Linux)

## 2.2.7 管理サーバの時刻を調整する

Compute Systems Manager のタスクやアラートに関する時刻などは、管理サーバの時刻に基づいています。

ただし、管理サーバの時刻を Compute Systems Manager の起動中に変更した場合、Compute Systems Manager が正しく動作しなくなるおそれがあります。時刻を変更する必要がある場合には、インストールの前に調整してください。

NTP などで管理サーバの時刻を自動的に変更する場合、次の内容に注意してください。

- ・ マシンの時刻が実際の時刻よりも進んだときに、少しずつ時間を掛けてマシンの時刻と実際の時刻を合わせるように設定してください。
- ・ Windows Time サービスなど使用する時刻修正ツールによっては、時刻のずれ幅が一定時間内であれば少しずつ時刻が修正され、一定時間を超えると時刻をさかのぼらせて一気に実際の時刻に合うよう時刻が修正されるものがあります。時刻のずれ幅が、少しずつ修正される範囲を超えないように設定してください。



**重要** 米国およびカナダのタイムゾーンで Compute Systems Manager を使用する場合、2007 年から米国およびカナダで適用された新しい DST (サマータイム) に対応するよう、管理サーバの OS の設定を変更してください。OS が新しい DST に対応していない場合、Compute Systems Manager も対応しません。

#### 関連項目

- 2.2.1 インストール環境の確認とは
- (1) Compute Systems Manager で適用される時刻について
- (2) 運用開始後に管理サーバの時刻を調整する

## 2.2.8 IPv6 を使用する場合の設定を確認する

Compute Systems Manager は、管理サーバとシャーン間の通信で IPv6 をサポートしています。

IPv6 を使用する場合は、管理サーバで IPv6 と IPv4 の両方が使用できることを確認してください。IPv4 は、ほかの管理対象との通信、内部通信などで使用されます。

#### 関連項目

- 2.2.1 インストール環境の確認とは

## 2.2.9 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定を確認する

32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品と、Compute Systems Manager を同じホストで運用する場合は、両方の製品でユーザーアカウントを共有するかどうかを検討します。

ユーザーアカウントの共有には、次に示す特徴があります。これらの特徴を考慮して、ユーザーアカウントを共有するかどうかをインストール前に検討してください。

- Compute Systems Manager と同じユーザーアカウントで、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品にもログインできます。
- 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品のユーザーアカウントは、Compute Systems Manager が使用する Hitachi Command Suite 共通コンポーネントで管理されます。



**重要** ユーザーアカウントの共有を無効にできるのは、Compute Systems Manager を含む Hitachi Command Suite 製品をインストールした直後だけです。ユーザーアカウントの共有を有効にして運用を開始すると、運用の途中で共有を無効にできません。

製品のインストール環境、およびユーザーアカウントの共有の有無に応じたインストール手順の概要を次に示します。32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品のインストール手順については、各製品のマニュアルを参照してください。

### 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品、および Compute Systems Manager の両方をインストールする場合

- ユーザーアカウントの共有を無効にして運用する場合は、次の手順でインストールしてください。
  - a. Compute Systems Manager をインストールします。
  - b. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品をインストールします。
- ユーザーアカウントの共有を有効にして運用する場合は、上記の手順を逆の順序でインストールしてください。

### すでに 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされているホストに、Compute Systems Manager をインストールする場合

- ユーザーアカウントの共有を無効にして運用する場合は、次の手順でインストールしてください。
  - a. Compute Systems Manager をインストールします。
  - b. Hitachi Command Suite 製品によるシステムの運用を開始する前に、`hcmdsprmset` コマンドを実行します。
- ユーザーアカウントの共有を有効にして運用する場合は、そのまま Compute Systems Manager をインストールしてください。自動的にユーザーアカウントの共有が有効になります。

### すでに Compute Systems Manager がインストールされているホストに、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品をインストールする場合

- ユーザーアカウントの共有を無効にして運用する場合は、そのまま 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品をインストールしてください。ユーザーアカウントの共有は無効のままとなります。
- ユーザーアカウントの共有を有効にして運用する場合は、次の手順でインストールしてください。
  - a. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品をインストールします。
  - b. `hcmdsprmset` コマンドを実行します。

#### 関連項目

- 2.2.1 インストール環境の確認とは
- 2.4.6 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を有効にする
- 2.4.7 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を無効にする

## 2.3 インストール時の入力項目の検討

### 2.3.1 インストール時の入力項目の検討とは

インストールの際、インストールウィザードでは、インストール先や管理サーバの情報などを入力する必要があります。デフォルト値が用意されている項目については、デフォルト値を使用することをお勧めします。

デフォルト値と異なる値を設定する項目については、入力する値をあらかじめ決めておいてください。



**重要** Hitachi Command Suite の仮想アプライアンスを利用する場合は、作成される仮想マシンに Compute Systems Manager がインストールされています。また、Compute Systems Manager の動作に必要な設定がデフォルトで設定されているため、このマニュアルで説明しているインストール時の入力項目の検討は不要です。仮想アプライアンスを利用したインストールについては、マニュアル「*Hitachi Command Suite 仮想アプライアンス インストールガイド*」を参照してください。

指定できるインストール先とデフォルト値を次に示します。

- Compute Systems Manager のインストール先（新規インストールの場合）  
Windows :

< *Program Files* ディレクトリ > %HiCommand

- < *Program Files* ディレクトリ > は、環境変数 %ProgramFiles% に設定されているディレクトリです。

デプロイメントマネージャーは x86 アーキテクチャで動作するため、*Compute Systems Manager* とは異なるディレクトリにインストールされます。x86 アーキテクチャで動作するプログラムの場合、< *Program Files* ディレクトリ > は、環境変数 %ProgramFiles (x86)% に設定されているディレクトリです。

Linux :

/opt/HiCommand

- データベースの格納先 (新規インストールの場合)

Windows :

< *Compute Systems Manager* のインストールディレクトリ > %database%x64%HCSM

Linux :

/var/< *Compute Systems Manager* のインストールディレクトリ > /database/x64/HCSM

データベースの格納先を変更すると、指定したディレクトリに「x64%HCSM」(Windows の場合) または「x64/HCSM」(Linux の場合) ディレクトリが作成されます。

- データベースのバックアップ先 (*Hitachi Command Suite* 製品を構築済みの環境に *Compute Systems Manager* をインストールする場合)

Windows :

< *Compute Systems Manager* のインストールディレクトリ >

%ComputeSystemsManager\_backup

Linux :

/var/< *Compute Systems Manager* のインストールディレクトリ > /backup



参考 *Hitachi Command Suite* 共通コンポーネントは、デフォルトで次のディレクトリにインストールされます。

Windows :

< *Compute Systems Manager* のインストールディレクトリ > %Base64

Linux :

< *Compute Systems Manager* のインストールディレクトリ > /Base64

すでにほかの *Hitachi Command Suite* 製品が稼働しているサーバに *Compute Systems Manager* をインストールする場合は、ほかの *Hitachi Command Suite* 製品で指定した *Hitachi Command Suite* 共通コンポーネントのインストール先と同じ場所にインストールされます。

## 関連項目

- [2.3.2 パスの指定規則](#)
- [2.3.3 インストールに使用するディレクトリの内容を確認する](#)
- [2.3.4 管理サーバの情報を確認する](#)

## 2.3.2 パスの指定規則

デフォルト値とは異なるインストール先を指定する場合は、インストール前にディレクトリを作成しておいてください。インストール先として、任意のディレクトリを作成する場合は、条件を満たすディレクトリを用意してください。

インストールに使用する任意のディレクトリのパスに指定できる文字および文字数を次に示します。

- 指定できる文字 :

- Windows : A～Z a～z 0～9 . \_ 半角スペース ¥ :
- Linux : A～Z a～z 0～9 . \_ /  
Linux の場合、データベース格納先パスには"."も指定できます。
- 指定できる文字数 :
  - インストール先パス : 64 バイト以内
  - データベース格納先パス : 90 バイト以内
  - データベースのバックアップ先パス : 150 バイト以内

インストール先のパスに指定できない文字など、制限事項を次に示します。この項目のどれにもあてはまらないパスを指定してください。

#### Windows :

- 半角スペースが 2 文字以上続いている
- ピリオドおよび半角スペースがディレクトリ名の末尾に指定されている
- シンボリックリンクまたはジャンクションが指定されている
- ドライブ直下 (例えば, D:¥) のパスが指定されている
- 次のどれかのディレクトリまたはその下のディレクトリが指定されている
  - %ProgramFiles(x86)%に設定されているディレクトリ
  - %CommonProgramFiles(x86)%に設定されているディレクトリ
  - %systemroot%\¥system32 ディレクトリ
  - %systemroot%\¥SysWOW64 ディレクトリ
  - %ProgramFiles%\¥WindowsApps ディレクトリ (Windows Server 2012 の場合)
 %ProgramFiles(x86)%, %CommonProgramFiles(x86)%, %systemroot%, および%ProgramFiles%は Windows の環境変数です。
- ネットワークドライブのパスが指定されている

#### Linux :

- 次のディレクトリが指定されている
  - ルートディレクトリ
  - /usr ディレクトリ
  - /usr/local ディレクトリ
  - /var ディレクトリ
- シンボリックリンクが指定されている
- ディレクトリパスの最後にパスの区切り文字 (/) が指定されている

#### 関連項目

- 2.3.1 インストール時の入力項目の検討とは
- 2.3.3 インストールに使用するディレクトリの内容を確認する

## 2.3.3 インストールに使用するディレクトリの内容を確認する

Compute Systems Manager のインストール中に指定または作成されるディレクトリ内容の確認について説明します。



次に示すパスをデフォルトとは異なるディレクトリを作成して指定する場合は、そのディレクトリの内容を前もって確認してください。

- **Compute Systems Manager** のインストール先
- データベースの格納先
- データベースのバックアップ先



**参考** インストール中に取得されたデータベースのバックアップは、`hcmds64dbtrans` コマンドを使ってインポートできます。

また、デプロイメントマネージャーをインストールすると、次のディレクトリが作成されます。すでに作成されている場合、ディレクトリが使用できる状態かどうか、前もって確認してください。

- `<Compute Systems Manager のインストールドライブ>%Deploy`  
デプロイメントマネージャーが内部処理で使用するファイルなどが格納されるディレクトリです。
- `<システムドライブ>%DeployBackup`  
イメージファイルを格納するデフォルトのディレクトリです。デプロイメントマネージャーをインストールしたあと、GUI で異なるディレクトリのパスに変更できます。

#### 関連項目

- [2.3.1 インストール時の入力項目の検討とは](#)
- [2.3.2 パスの指定規則](#)
- [7.1 デプロイメントマネージャーの環境設定とは](#)

## 2.3.4 管理サーバの情報を確認する

**Compute Systems Manager** のインストール中には、管理サーバのホスト名の入力を求められます。

デフォルトは OS に設定されているホスト名です。ホスト名を指定する場合は、管理サーバに設定されているホスト名が次の条件をすべて満たすことを確認してください。

- 長さが 128 バイト以内であること。
- 次の文字で構成されていること。  
A~Z a~z 0~9 - .  
ただし、ハイフン (-) はホスト名の先頭と末尾には使用できません。

ホスト名または IP アドレスは、**Compute Systems Manager** にアクセスする URL に使用されません。

#### 関連項目

- [2.3.1 インストール時の入力項目の検討とは](#)

## 2.4 インストール

### 2.4.1 インストールとは

インストールメディアを使用して、管理サーバに **Compute Systems Manager** をインストールします。

Compute Systems Manager のインストール種別を次に示します。

- 新規インストール  
Compute Systems Manager がインストールされていない環境に、Compute Systems Manager をインストールすることを指します。
- 上書きインストール  
Compute Systems Manager がインストールされている環境に、同じバージョンの Compute Systems Manager をインストールすることを指します。上書きインストールは、次の場合に実施します。
  - Compute Systems Manager を構成するファイルが破損した場合
  - Compute Systems Manager のインストールまたはアンインストールに失敗した場合
- アップグレードインストール  
インストール済みの Compute Systems Manager よりも、バージョンが新しい Compute Systems Manager をインストールすることを指します。

Compute Systems Manager をインストールする手順は、バージョン 7.x.x からアップグレードする場合を除いて、どのインストール種別でも同じです。



#### 重要

- ウィルス検出プログラムを使用している環境に Compute Systems Manager をインストールする場合は、インストール後にウイルス検出プログラムの設定を変更する必要があります。
- クラスタ環境にインストールする場合は、あらかじめ環境設定が必要です。環境設定の詳細、およびクラスタ環境へのインストール手順については、クラスタを使用するための環境設定と運用についての説明を参照してください。
- Hitachi Command Suite の仮想アプライアンスを利用する場合は、作成される仮想マシンに Compute Systems Manager がインストールされているため、インストールメディアからのインストールは不要です。ただし、仮想マシンに Hitachi Command Suite 製品を追加でインストールしたり、アップグレードしたりする場合は、インストールメディアから対象となる製品をインストールしてください。  
仮想アプライアンスを利用したインストールについては、マニュアル「*Hitachi Command Suite 仮想アプライアンス インストールガイド*」を参照してください。

#### 関連項目

- [2.4.3 Compute Systems Manager をインストールする \(Windows\)](#)
- [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)
- [2.4.5 ウィルス検出プログラムを使用する場合に必要な設定](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [D.1 バージョン 7.x.x からのアップグレードとは](#)

## 2.4.2 インストールする前の確認事項

Compute Systems Manager をインストールする前に、次の操作を完了しておいてください。

- インストール環境の確認
- インストール時の入力項目の検討
- 統合インストールメディアからほかの Hitachi Command Suite 製品もインストールする場合は、各製品のインストール要件の確認
- Hitachi Command Suite 共通コンポーネントを利用する製品がインストールされている場合は、それらの製品の停止

Windows の管理サーバにインストールする場合は、次の操作も完了しておいてください。

- ・ デプロイメントマネージャーを新規インストールする場合は、インストールするための前提条件の確認
- ・ Windows ファイアウォールが有効になっている場合は、Windows ファイアウォールのサービスの起動
- ・ Windows の [サービス] ダイアログ、および [イベント ビューアー] ダイアログを閉じる



#### 重要

- ・ **Compute Systems Manager** は、ネットワークドライブ経由ではインストールできません。  
なお、ネットワークドライブには、Windows のリモートデスクトップ機能を使用したローカルデバイスの共有も含まれます。
- ・ インストール先の管理サーバにはほかの Hitachi Command Suite 製品がインストールされている場合は、すべての製品のバージョンが 8.0.1 以降であることを確認してください。バージョン 8.0.1 より前の Hitachi Command Suite 製品がインストールされている場合は、バージョン 8.0.1 以降にアップグレードしてください。
- ・ インストール先の管理サーバに Device Manager がインストールされていて、かつ別のマシンにインストールされた Tuning Manager が Device Manager とリモート接続している場合は、Tuning Manager をいったん停止しておく必要があります。

#### 関連項目

- ・ [2.2.1 インストール環境の確認とは](#)
- ・ [2.3.1 インストール時の入力項目の検討とは](#)
- ・ [2.4.1 インストールとは](#)
- ・ [2.4.3 Compute Systems Manager をインストールする \(Windows\)](#)
- ・ [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)

## 2.4.3 Compute Systems Manager をインストールする (Windows)

単体インストールメディア、または統合インストールメディアを使用して、Windows の管理サーバに Compute Systems Manager をインストールします。

#### 事前に完了しておく操作

- ・ インストールする前の確認作業

Compute Systems Manager のインストール手順を次に示します。

1. インストールメディアを管理サーバにセットします。  
統合インストールメディアでウィンドウが自動で表示されない場合は、<統合インストールメディア>%index.html をダブルクリックしてウィンドウを開いてください。
2. インストールウィザードを起動します。
  - 単体インストールメディアの場合  
<Compute Systems Manager のインストールメディア>%HCSM\_SERVER%setup.exe を実行します。
  - 統合インストールメディアの場合  
表示された画面の [HCSM] を選択して、[Install] ボタンをクリックします。
3. インストールウィザードの指示に従って、それぞれの画面で必要な情報を指定します。
4. [インストール完了] 画面で、[完了] ボタンをクリックします。

OS の再起動を促すメッセージが表示された場合は、OS の再起動が必要です。[インストール完了時に OS を再起動する。] チェックボックスを選択して [完了] ボタンをクリックしてください。

チェックボックスを選択しなかった場合は、運用を開始する前に必ず OS を再起動してください。

5. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされているホストに新規インストールした場合で、ユーザーアカウントの共有を無効にして運用するときは、Hitachi Command Suite 製品によるシステムの運用を開始する前に、`hcmdsprmset` コマンドを実行して共有を無効にします。



#### 重要

- SSL 通信をしている場合、または Hitachi Command Suite 共通コンポーネントのポート番号を変更している場合、[インストール完了] 画面で [インストール完了時に Hitachi Command Suite GUI を起動する。] チェックボックスを選択しても、GUI を起動できないことがあります。

その場合は、変更後の管理サーバの情報を確認して、Web ブラウザーのアドレスバーに Compute Systems Manager の URL を入力して GUI を起動してください。

また、次のショートカットの URL も変更してください。

Windows Server 2008 R2 の場合：

[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Compute Systems Manager] - [Login - HCSM] を右クリックすると表示される、[プロパティ] - [Web ドキュメント] タブの [URL]

Windows Server 2012 の場合：

[スタート] - [すべてのアプリ] - [Hitachi Command Suite] - [Compute Systems Manager] - [Login - HCSM] を右クリックすると表示される、[プロパティ] - [Web ドキュメント] タブの [URL]

- Web ブラウザーが Internet Explorer 11 の場合、Compute Systems Manager にログインしたあと、空白や遷移途中のウィンドウが表示されることがあります。

その場合は、再度 Web ブラウザーを起動し、アドレスバーに Compute Systems Manager の URL を入力してください。

- 管理サーバで Oracle JDK 7 を使用している場合、バージョン 8.2.1 より前の Compute Systems Manager からアップグレードすると、使用する JDK が Compute Systems Manager に同梱された JDK に変更されます。

SSL 通信をしている場合は、インストール後にサーバ証明書を管理サーバにインポートし直す必要があります。ただし、アップグレード後も Oracle JDK を使用する場合は、`hcmds64chgjdk` コマンドを実行して、使用する JDK を変更したあとにインポートし直してください。

Compute Systems Manager がインストールされ、DCOM が有効になります。

#### 関連項目

- 2.4.2 インストールする前の確認事項
- 2.4.5 ウィルス検出プログラムを使用する場合に必要な設定
- 2.4.7 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を無効にする
- 2.5.2 管理サーバにアクセスできるか確認する
- 3.5.4 JDK を変更する
- 7.2 デプロイメントマネージャーをインストールするための前提条件

## 2.4.4 Compute Systems Manager をインストールする (Linux)

単体インストールメディア、または統合インストールメディアを使用して、Linux の管理サーバに Compute Systems Manager をインストールします。

## 事前に完了しておく操作

- ・ インストールする前の確認作業

Compute Systems Manager のインストール手順を次に示します。

1. インストールメディアを管理サーバにセットします。  
自動的にマウントされない場合は、手動でマウントしてください。
2. 次のディレクトリに移動します。  
< *Compute Systems Manager* のインストールメディア > /HCSM\_SERVER/ <プラットフォーム名 >
3. 次のコマンドを実行して、インストールします。  
./install.sh



**重要** [Ctrl] + [C] を使用してインストールを中断しないでください。

4. 表示されたメッセージに従って、必要な情報を指定します。
5. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされているホストに新規インストールした場合で、ユーザーアカウントの共有を無効にして運用するときは、Hitachi Command Suite 製品によるシステムの運用を開始する前に、hcmdsprmset コマンドを実行して共有を無効にします。



### 重要

- ・ インストールメディアのマウントパスに指定できる文字は次のとおりです。  
A~Z a~z 0~9 \_ /
- ・ 管理サーバで Oracle JDK 7 を使用している場合、バージョン 8.2.1 より前の Compute Systems Manager からアップグレードすると、使用する JDK が Compute Systems Manager に同梱された JDK に変更されます。  
SSL 通信をしている場合は、インストール後にサーバ証明書を管理サーバにインポートし直す必要があります。ただし、アップグレード後も Oracle JDK を使用する場合は、hcmds64chgjdk コマンドを実行して使用する JDK を変更したあとにインポートし直してください。

## 関連項目

- ・ 2.4.2 インストールする前の確認事項
- ・ 2.4.5 ウィルス検出プログラムを使用する場合に必要な設定
- ・ 2.4.7 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を無効にする
- ・ 2.5.2 管理サーバにアクセスできるか確認する
- ・ 3.5.4 JDK を変更する

## 2.4.5 ウィルス検出プログラムを使用する場合に必要な設定

管理サーバでウィルス検出プログラムを使用する場合は、次のディレクトリをスキャン対象から外してください。

ウィルス検出プログラムが、次のディレクトリ配下にあるデータベース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によって障害が発生するおそれがあります。

- ・ 次に示す Hitachi Command Suite 共通コンポーネントのディレクトリ

Windows :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > %HDB

Linux :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > /HDB

- *Hitachi Command Suite* 共通コンポーネント, および *Compute Systems Manager* のデータベース格納先ディレクトリ

Windows :

< *Compute Systems Manager* のインストールディレクトリ > %database\*

Linux :

/var/< *Compute Systems Manager* のインストールディレクトリ > /database\*

注※

データベースの格納先ディレクトリをデフォルトから変更している場合は, そのディレクトリを指定してください。

#### 関連項目

- 2.4.1 インストールとは

## 2.4.6 32 ビットの *Hitachi Command Suite* 共通コンポーネントを使用する製品とのユーザーアカウントの共有を有効にする

*Compute Systems Manager* がインストールされているホストに, 32 ビットの *Hitachi Command Suite* 共通コンポーネントを使用する製品をインストールした場合, 両方の製品でユーザーアカウントの共有を有効にするには, `hcmdsprmset` コマンドを実行します。



**重要** 32 ビットの *Hitachi Command Suite* 共通コンポーネントを使用する製品がインストールされているホストに, *Compute Systems Manager* をインストールした場合は, *Compute Systems Manager* のインストール時に自動的にユーザーアカウントの共有が有効になるため, このトピックで説明している手順は不要です。

ユーザーアカウントの共有を有効にする手順を次に示します。

1. 次のコマンドを実行して, *Hitachi Command Suite* 共通コンポーネントの設定を変更します。

Windows :

< *Hitachi Command Suite* 製品 (32 ビット) のインストールディレクトリ > %Base%bin  
%hcmdsprmset /host <インストール先ホストの IP アドレス> /port <非 SSL 通信用の  
ポート番号>

Linux :

< *Hitachi Command Suite* 製品 (32 ビット) のインストールディレクトリ > /Base/bin/  
`hcmdsprmset -host <インストール先ホストの IP アドレス> -port <非 SSL 通信用の  
ポート番号>`

`host`

*Compute Systems Manager* をインストールしたホストの IP アドレスを指定します。ただし, 127.0.0.1 は指定しないでください。

インストール環境が非 SSL 通信, または非 SSL 通信と SSL 通信の両方で構成されている場合で, *Hitachi Command Suite* 共通コンポーネントの内部通信をネットワーク経由からサーバ内通信に変更するときは, `hosts` ファイルで任意のホスト名を 127.0.0.1 に定義したあと, `host` オプションにそのホスト名を指定して実行してください。

外部から管理サーバへの非 SSL 通信を遮断する設定にしている場合は,

`user_httpsd.conf` ファイルの `ServerName` プロパティに指定したホスト名を, `hosts` ファイルで 127.0.0.1 に定義したあと, `host` オプションにそのホスト名を指定して実行してください。

`hosts` ファイルの編集例を次に示します。

127.0.0.1 localhost < *hcmdsprmset* コマンドで指定するホスト名 >

port

HBase 64 Storage Mgmt Web Service への接続ポート番号を指定します。非 SSL 通信用のポート番号のデフォルトは 22015 です。

2. Compute Systems Manager を再起動します。
3. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品を再起動します。

#### 関連項目

- 2.2.9 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定を確認する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 2.4.7 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有を無効にする

32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされているホストに、Compute Systems Manager をインストールすると、自動的にユーザーアカウントの共有が有効となります。ユーザーアカウントの共有を無効にするには、*hcmdsprmset* コマンドを実行します。



#### 重要

- このトピックで説明する手順は、Compute Systems Manager をインストールした直後で、運用を開始していない場合にだけ有効です。すでに運用を開始した場合、ユーザーアカウントの共有を無効にするには、ホスト上にインストールされているすべての Hitachi Command Suite 製品（32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品も含みます）をアンインストールしたあと、再度インストールする必要があります。
- Compute Systems Manager がインストールされているホストに、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品をインストールした場合は、このトピックで説明している手順は不要です。

ユーザーアカウントの共有を無効にする手順を次に示します。

1. Compute Systems Manager を停止します。
2. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネントの設定を変更します。

Windows :

```
< Hitachi Command Suite 製品 (32 ビット) のインストールディレクトリ > %Base%\bin  
%hcmdsprmset /host 127.0.0.1 /port <非 SSL 通信用のポート番号 >
```

Linux :

```
< Hitachi Command Suite 製品 (32 ビット) のインストールディレクトリ > /Base/bin/  
hcmdsprmset -host 127.0.0.1 -port <非 SSL 通信用のポート番号 >
```

port

HBase Storage Mgmt Web Service への接続ポート番号を指定します。非 SSL 通信用のポート番号のデフォルトは 23015 です。

3. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品を再起動します。
4. Compute Systems Manager を起動します。



#### 関連項目

- 2.2.9 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定を確認する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 2.5 新規インストール後に必要な作業

### 2.5.1 新規インストール後に必要な作業とは

Compute Systems Manager を新たに導入するため、新規インストールした場合には、次の作業が必要です。

次のすべての作業は、**System** アカウントでログインして実行する必要があります。

- 管理サーバへのアクセス確認
- プラグインライセンスの登録（必要に応じて）
- System アカウントのパスワードの変更（推奨）
- ログインしてからリソースを管理するまでの初期設定作業

Compute Systems Manager に最初にログインしたとき、ダッシュボードの [To Do] リストに初期設定ウィザードが表示されます。初期設定ウィザードは、初めてのログインの場合にだけ表示され、指示どおりに設定すれば、必要事項を設定できます。

これらの作業が完了すると、Compute Systems Manager の運用を開始できます。

#### 関連項目

- 2.5.2 管理サーバにアクセスできるか確認する
- 2.5.3 プラグインライセンスを登録する
- 2.5.4 System アカウントのパスワードを変更する
- 2.5.5 System アカウントにメールアドレスを設定する
- 2.5.6 E メール通知を設定する
- 2.5.7 E メールで通知するアラートレベルを設定する
- 2.5.8 管理対象リソースを登録する
- 2.5.9 サーバ管理者のユーザーアカウントを作成する
- 2.5.10 リソースグループを設定する
- 2.5.11 ユーザーグループを設定する
- 2.5.12 初期設定作業を完了する

### 2.5.2 管理サーバにアクセスできるか確認する

インストールが成功したことを確認するために、管理クライアントの Web ブラウザーから管理サーバにアクセスできることを確認します。

#### 事前に確認しておく情報

- インストールした管理サーバの IP アドレスまたはホスト名



Web ブラウザーから管理サーバにアクセスする手順を次に示します。

1. Web ブラウザーを起動します。
2. Web ブラウザーの設定を確認し、必要に応じて設定を変更します。  
Web ブラウザーの設定については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

3. アドレスバーに Compute Systems Manager にアクセスする URL を次の形式で指定します。

<プロトコル>://<管理サーバの IP アドレスまたはホスト名>:<ポート番号>/  
ComputeSystemsManager/

<プロトコル>

非 SSL 通信の場合は http、SSL 通信の場合は https を指定します。

<管理サーバの IP アドレスまたはホスト名>

Compute Systems Manager をインストールした管理サーバの IP アドレスまたはホスト名を指定します。

<ポート番号>

user\_httpsd.conf ファイルの Listen 行に設定されているポート番号を指定します。

非 SSL 通信の場合は非 SSL 通信用のポート番号（デフォルト：22015）、SSL 通信の場合は SSL 通信用のポート番号（デフォルト：22016）を指定します。

user\_httpsd.conf ファイルの格納先は次のとおりです。

Windows :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥uCPSB  
¥httpsd¥conf¥user\_httpsd.conf

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/uCPSB/  
httpsd/conf/user\_httpsd.conf

Compute Systems Manager のログイン画面が表示され、管理サーバにアクセスできるようになります。

## 関連項目

- [2.5.1 新規インストール後に必要な作業とは](#)

## 2.5.3 プラグインライセンスを登録する

Compute Systems Manager で特定の機能を使用するためにはプラグインライセンスを登録する必要があります。

### 事前に確認しておく情報

- ライセンスキーまたはライセンスキーファイル

プラグインライセンスを登録する手順を次に示します。

1. Compute Systems Manager のログイン画面で、[ライセンス] ボタンをクリックします。
2. ライセンスキーを入力し、[保存] ボタンをクリックします。

[ライセンス] 画面にライセンスの内容が表示されます。

プラグインライセンスの登録については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

## 関連項目

- ・ 2.5.1 新規インストール後に必要な作業とは

## 2.5.4 System アカウントのパスワードを変更する

System アカウントは、ユーザー管理のための権限と Hitachi Command Suite 製品に対するすべての操作を実行できる権限を持つビルトインアカウントです。

ほかの Hitachi Command Suite 製品がインストールされていない環境に初めて Compute Systems Manager をインストールした場合、System アカウントのパスワードを変更することをお勧めします。

System アカウントのパスワードを変更する手順を次に示します。

1. 管理クライアントから、次のユーザー ID およびパスワードで Compute Systems Manager にログインします。  
ユーザー ID : system  
パスワード : manager  
System アカウントの初期パスワードは「manager」です。
2. 表示された初期設定ウィザードの [To Do] リストで、[ユーザープロファイルの編集, E-mail アドレスの設定] を選択します。
3. 表示された [プロファイル] 画面で、パスワードを変更します。

System アカウントのパスワードが変更されます。

ユーザーアカウントのパスワードの変更については、マニュアル「Hitachi Command Suite Compute Systems Manager ユーザーズガイド」を参照してください。

## 関連項目

- ・ 2.5.1 新規インストール後に必要な作業とは

## 2.5.5 System アカウントにメールアドレスを設定する

Compute Systems Manager で E メール通知の機能を使用するためには、System アカウントにメールアドレスを登録しておく必要があります。

System アカウントのメールアドレスを登録する手順を次に示します。

1. 初期設定ウィザードの [To Do] リストで、[ユーザープロファイルの編集, E-mail アドレスの設定] を選択します。
2. 表示された [プロファイル] 画面で、[プロファイル編集] を選択し、メールアドレスと名前を登録します。

System アカウントのメールアドレスが登録されます。

プロファイルの変更については、マニュアル「Hitachi Command Suite Compute Systems Manager ユーザーズガイド」を参照してください。

## 関連項目

- ・ 2.5.1 新規インストール後に必要な作業とは

## 2.5.6 E メール通知を設定する

アラートが発生したことやタスクが終了したことなどを E メールで通知するかどうかを設定します。

E メールで通知する場合、E メール通知で使用する SMTP サーバも設定します。

Eメールの通知を設定するには、ログイン後に表示される [To Do] リストに従って、設定します。

Eメール通知を設定する詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

### 関連項目

- [2.5.1 新規インストール後に必要な作業とは](#)

## 2.5.7 E メールで通知するアラートレベルを設定する

どのレベルのアラートを E メールで通知するかを設定します。

Eメールで通知するアラートレベルを設定するには、ログイン後に表示される [To Do] リストに従って設定します。

Eメールで通知するアラートレベルの設定の詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

### 関連項目

- [2.5.1 新規インストール後に必要な作業とは](#)
- [2.5.6 E メール通知を設定する](#)

## 2.5.8 管理対象リソースを登録する

Compute Systems Manager でサーバリソースを管理するためには、管理対象リソースを登録する必要があります。

### 事前に完了しておく操作

- 管理対象リソース側の設定

管理対象リソースを登録するには、ログイン後に表示される [To Do] リストに従って、リソースを探索し、管理対象として Compute Systems Manager に登録します。

管理対象リソースの登録の詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。



**参考** 次の条件をどちらも満たす場合、Device Manager で探索されたホストの情報が同期され、自動的に Compute Systems Manager の管理対象となります。自動的に管理対象となったホストを管理対象から外す場合、管理対象にするホストを選択する画面でチェックを外してください。

- Compute Systems Manager と Device Manager が同じ管理サーバで稼働している
  - 探索条件に合ったホストが、すでに Device Manager で探索されている
- ただし、Device Manager で探索された VMware ESXi の情報は、Compute Systems Manager と同期されません。

### 関連項目

- [2.5.1 新規インストール後に必要な作業とは](#)

- 4.2.1 日立製のブレードサーバを管理対象にするための確認事項
- 4.2.2 日立製のラックマウントサーバを管理対象にするための確認事項
- 4.3.1 ホストを管理対象にするための確認事項 (Windows ホスト)
- 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)

## 2.5.9 サーバ管理者のユーザーアカウントを作成する

Compute Systems Manager を操作するサーバ管理者のユーザーアカウントを作成します。また、必要に応じて User Management 権限を設定します。

サーバ管理者のユーザーアカウントを作成するには、ログイン後に表示される [To Do] リストに従って、サーバ管理者のユーザーアカウントを作成します。作成したユーザーアカウントでほかのユーザーを管理する場合、User Management 権限を設定します。

詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

### 関連項目

- 2.5.1 新規インストール後に必要な作業とは

## 2.5.10 リソースグループを設定する

管理対象リソースへのアクセスを制御するために、リソースグループを設定します。

### 事前に完了しておく操作

- 管理対象リソースの登録

リソースグループを設定するには、ログイン後に表示される [To Do] リストに従って、リソースグループを作成し、管理対象リソースを追加します。

詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

### 関連項目

- 2.5.1 新規インストール後に必要な作業とは
- 2.5.8 管理対象リソースを登録する

## 2.5.11 ユーザーグループを設定する

管理対象リソースへのアクセスを制御するために、ユーザーグループを設定します。

### 事前に完了しておく操作

- サーバ管理者のユーザーアカウントの作成

ユーザーグループを設定するには、ログイン後に表示される [To Do] リストに従って、ユーザーグループを作成し、サーバ管理者のユーザーアカウントを追加します。ユーザーグループには、リソースグループとロールを割り当てます。

詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

#### 関連項目

- ・ 2.5.1 新規インストール後に必要な作業とは
- ・ 2.5.9 サーバ管理者のユーザーアカウントを作成する

## 2.5.12 初期設定作業を完了する

初期設定作業を完了するには、[ダッシュボード] タブにある情報レポートの [To Do] リストで、[ダッシュボードの表示] リンクをクリックします。

[情報] 画面の [To Do] リストから、初期設定作業の項目が削除され、初期設定作業が完了します。

#### 関連項目

- ・ 2.5.1 新規インストール後に必要な作業とは

## 2.6 アンインストール

### 2.6.1 アンインストールとは

次のような場合には、管理サーバから **Compute Systems Manager** をアンインストールします。

- ・ **Compute Systems Manager** を新しくインストールし直す
- ・ 異なる環境に **Compute Systems Manager** を移行する
- ・ **Compute Systems Manager** の運用を停止する
- ・ 管理サーバの OS をアップグレードする

**Compute Systems Manager** をアンインストールすると、プロパティファイル、データベースファイル、ログファイルなどが削除されます。

ただし、**Compute Systems Manager** をアンインストールしても削除されないファイルやディレクトリがあります。削除されない場合の条件とそのファイルまたはディレクトリを次に示します。

- ・ Hitachi Command Suite 共通コンポーネントを前提とする製品が、管理サーバにインストールされている場合  
Hitachi Command Suite 共通コンポーネントのプロパティファイル、データベースファイル、ログファイルなど
- ・ デプロイメントマネージャーをインストールしていた場合  
イメージファイルの格納先ディレクトリ（デフォルトの格納先は<システムドライブ>¥DeployBackup）  
デプロイメントマネージャーをアンインストールしたあと、上記のディレクトリが不要となる場合は、削除してください。



**重要** 管理サーバの OS をアップグレードする場合、事前に **Compute Systems Manager** をアンインストールしてください。例えば、Windows Server 2012 から Windows Server 2012 R2 にアップグレードする場合も、**Compute Systems Manager** をいったんアンインストールする必要があります。OS をアップグレードしたあと、アップグレードした OS に対応する **Compute Systems Manager** を新規インストールして、**Compute Systems Manager** のデータベースを移行してください。

#### 関連項目

- ・ 2.6.2 アンインストールするための確認事項

- 2.6.3 アンインストールする (Windows)
- 2.6.4 アンインストールする (Linux)
- 8.2.6 データベースを移行するための確認事項

## 2.6.2 アンインストールするための確認事項

Compute Systems Manager をアンインストールすると、Compute Systems Manager のインストール先ディレクトリおよびデータベースのインストール先ディレクトリが削除されます。これらのディレクトリの下の内容を再利用したい場合は、アンインストール前に退避しておく必要があります。

Compute Systems Manager をアンインストールする前に、次の操作を完了しておいてください。

- データベースのエクスポート  
新しくインストールし直したり、異なる環境に Compute Systems Manager を移行したりする場合に必要です。
- インストール先に追加したディレクトリまたはファイルの退避  
アンインストールすると、次の場所に作成したディレクトリも削除されます。再利用したい場合は、アンインストール前に退避してください。

Windows :

< Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager

Linux :

< Compute Systems Manager のインストールディレクトリ >/ComputeSystemsManager



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている管理サーバから、バージョン 8.0.0 以降の Hitachi Command Suite 製品をすべてアンインストールすると、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品が使用できなくなります。アンインストール後も引き続き使用する場合は、次の手順で再インストールしてください。

1. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品をアンインストールします。
2. バージョン 8.0.0 以降の Hitachi Command Suite 製品をアンインストールします。
3. 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品を再インストールします。

### 関連項目

- 2.6.1 アンインストールとは
- 8.2.6 データベースを移行するための確認事項

## 2.6.3 アンインストールする (Windows)

Windows の管理サーバから Compute Systems Manager をアンインストールします。

1. Windows の [プログラムと機能] を開きます。
2. [Hitachi Compute Systems Manager] を選択し、[削除] ボタンまたは [アンインストール] リンクをクリックします。
3. 画面指示に従います。
4. DCOM を利用しているプログラムがほかになければ、DCOM を無効にします。

Compute Systems Manager が管理サーバからアンインストールされます。

### 関連項目

- 2.6.1 アンインストールとは

- [2.6.2 アンインストールするための確認事項](#)

## 2.6.4 アンインストールする (Linux)

Linux の管理サーバから Compute Systems Manager をアンインストールします。

1. /root ディレクトリに移動します。

2. 次のコマンドを実行します。

```
< Compute Systems Manager のインストールディレクトリ >/CSMUninstall/  
uninstall.sh
```

3. 表示されたメッセージに従って操作します。

Compute Systems Manager が管理サーバからアンインストールされます。

### 関連項目

- [2.6.1 アンインストールとは](#)
- [2.6.2 アンインストールするための確認事項](#)





## 管理サーバの環境設定

この章では、SNMP トラップ、ユーザーアカウントの設定など、管理サーバの環境設定について説明します。

- 3.1 SNMP トラップの設定
- 3.2 ユーザーアカウントのポリシーの設定
- 3.3 JP1/IM でのアラート監視設定
- 3.4 JP1/IM からの Compute Systems Manager のラウンチ
- 3.5 管理サーバの設定変更

## 3.1 SNMP トラップの設定

### 3.1.1 SNMP トラップの設定とは

Compute Systems Manager では、日立製でないサーバに搭載されたホストが出力した SNMP トラップをアラートとして受信できます。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のに便利です。

SNMP トラップをアラートとして受信するには、次の設定が必要です。

- 管理サーバでの MIB ファイル登録
- 管理クライアントでの SNMP トラップの受信設定

管理クライアントでの設定については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

#### 関連項目

- [3.1.2 MIB ファイルを登録する](#)
- [3.1.3 インバンド SNMP トラップの監視とは](#)
- [3.1.4 インバンド SNMP トラップを監視する](#)

### 3.1.2 MIB ファイルを登録する

管理サーバで、SNMP トラップの定義が記述されている MIB ファイルを登録します。

#### 事前に完了しておく作業

- SNMP トラップ受信用のポート（デフォルトは 162/udp）を管理サーバで使えるようにする
- MIB ファイルを準備する  
MIB ファイル名は任意です。
- 管理サーバの OS が Red Hat Enterprise Linux または Oracle Linux の場合、64bit 版の net-snmp-libs パッケージをインストールする

MIB ファイルを登録する手順を次に示します。

1. 次のディレクトリに MIB ファイルを格納します。

Windows :

```
< Compute Systems Manager のインストールディレクトリ >%ComputeSystemsManager  
%mibs%mib
```

Linux :

```
< Compute Systems Manager のインストールディレクトリ >/ComputeSystemsManager/  
mibs/mib
```

2. Compute Systems Manager を停止します。

3. 次のコマンドを実行します。

Windows :

```
< Compute Systems Manager のインストールディレクトリ >%ComputeSystemsManager  
%bin%hcsmtraptoxml -c
```

Linux :

```
< Compute Systems Manager のインストールディレクトリ >/  
ComputeSystemsManager/bin/hcsmtraptoxml -c
```

4. Compute Systems Manager を起動します。

MIB ファイルに記述されている SNMP トラップの定義が Compute Systems Manager に登録されます。

#### 関連項目

- 3.1.1 SNMP トラップの設定とは
- 3.1.4 インバンド SNMP トラップを監視する
- (3) ポートを変更する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

### 3.1.3 インバンド SNMP トラップの監視とは

管理対象ホストの OS で発生するイベントを監視するために、管理対象ホストと管理サーバで SNMP トラップを設定します。

Compute Systems Manager で設定が必要な項目を次に示します。

- 管理対象ホストでの SNMP トラップの送信設定
- 管理サーバでの SNMP トラップの受信設定

#### 関連項目

- 3.1.4 インバンド SNMP トラップを監視する
- 4.3.6 SNMP トラップを設定する (Windows ホスト)
- 4.4.9 SNMP トラップを設定する (Linux ホスト)

### 3.1.4 インバンド SNMP トラップを監視する

管理対象ホストの OS で発生したイベントを Compute Systems Manager でアラートとして受信するには、管理サーバで SNMP 関連の MIB ファイルと SNMP トラップ受信を登録し、管理対象ホストで SNMP トラップの送信について設定する必要があります。

SNMP トラップを送信するよう設定する手順を次に示します。

1. 管理対象ホストで発生したイベントを監視するための MIB ファイルを登録します。  
インストールメディアに格納されている次のファイルをコピーして、MIB ファイルの登録に使用してください。
  - 管理対象ホストが Windows の場合に使用する MIB ファイル  
< Compute Systems Manager のインストールメディア >¥HCSM\_SERVER¥HCSM¥snmp¥mibs¥hfcwdd-win.mib
  - 管理対象ホストが Linux の場合に使用する MIB ファイル  
< Compute Systems Manager のインストールメディア >¥HCSM\_SERVER¥HCSM¥snmp¥mibs¥hfcldd-lin.mib上記のファイルパスは、管理サーバが Windows の場合の表記です。Linux の場合は、区切り文字の円記号 (¥) をスラント (/) に読み替えてください。
2. SNMP トラップの受信を設定します。  
SNMP トラップの受信設定については、マニュアル「Hitachi Command Suite Compute Systems Manager ユーザーズガイド」を参照してください。

3. 管理対象ホストでイベントの SNMP を設定します。

#### 関連項目

- 3.1.2 MIB ファイルを登録する
- 3.1.3 インバンド SNMP トラップの監視とは
- 4.3.6 SNMP トラップを設定する (Windows ホスト)
- 4.4.9 SNMP トラップを設定する (Linux ホスト)

## 3.2 ユーザーアカウントのポリシーの設定

### 3.2.1 ユーザーアカウントのポリシーの設定とは

Compute Systems Manager では、ユーザーの登録やパスワードの設定など、ユーザーアカウントに関する基本的な設定は GUI でできます。

このマニュアルでは、GUI で設定できないオプション設定について説明します。

オプション設定の種類を次に示します。

- System アカウントをロックの対象にする設定  
Compute Systems Manager の初期導入時には、System アカウントは自動ロックおよび手動ロックの対象にはなっていません。設定を変更することで、System アカウントをロックの対象にできます。
- アカウントのロック解除  
アカウントのロック解除は、通常は GUI で操作しますが、自分のアカウントのロックは解除できません。  
管理サーバで操作すると、自分のアカウントのロックを解除できます。



**重要** Compute Systems Manager 以外の Hitachi Command Suite 製品を使用している場合、Compute Systems Manager で設定した内容は Hitachi Command Suite 製品のすべてのユーザーアカウントに適用されます。

#### 関連項目

- 3.2.2 System アカウントをロックの対象にする
- 3.2.3 アカウントのロックを解除する

### 3.2.2 System アカウントをロックの対象にする

Compute Systems Manager の初期導入時には、System アカウントは自動ロックおよび手動ロックの対象にはなっていません。設定を変更することで、System アカウントをロックの対象にできます。

System アカウントをロックの対象にする手順を次に示します。

1. 次の場所に格納されている user.conf を開きます。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥conf  
¥user.conf
```

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/conf/  
user.conf

上記の場所に user.conf ファイルがない場合は新しく作成します。

2. account.lock.system プロパティの値を true に設定します。  
System アカウントをロックの対象にしない場合は false を指定します。

System アカウントが自動ロックおよび手動ロックの対象になります。

#### 関連項目

- 3.2.1 ユーザーアカウントのポリシーの設定とは
- B.2.12 ユーザーアカウントに関するプロパティ (user.conf)

### 3.2.3 アカウントのロックを解除する

アカウントがロックされた場合、ロックを解除するまでは、そのアカウントで Compute Systems Manager にアクセスできなくなります。次のどちらかの方法で、ロックを解除できます。

- アカウントがロックされていない User Management 権限を持つアカウントで Compute Systems Manager にログインし、アカウントのロックを解除する  
User Management 権限を持つアカウントでロックを解除する場合には、マニュアル「Hitachi Command Suite Compute Systems Manager ユーザーズガイド」を参照してください。
- コマンドを使って、アカウントのロックを解除する

ここでは、コマンドを使ってアカウントのロックを解除する方法について説明します。

コマンドを使ってアカウントのロックを解除する場合、次の条件を満たしている必要があります。

#### 必要条件

- 管理サーバが稼働している
- ロックを解除するアカウントにパスワードが設定されている  
パスワードが設定されていない場合は、hcms64unlockaccount コマンドではロックを解除できません。

管理者のアカウントで管理サーバにログインしたあと、次のコマンドを使用して、アカウントのロックを解除します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin  
%hcms64unlockaccount [/user <ユーザー ID >] [/pass <パスワード>]
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/  
hcms64unlockaccount [-user <ユーザー ID >] [-pass <パスワード>]
```

user : アカウントのロックを解除したいユーザー ID を指定します。

pass : user オプションで指定したアカウントのパスワードを指定します。

user または pass オプションを省略した場合は、ユーザー ID またはパスワードの応答入力求められます。メッセージの指示に従い入力してください。

#### 関連項目

- 3.2.1 ユーザーアカウントのポリシーの設定とは
- 8.1.2 Compute Systems Manager を起動する
- 8.1.5 Compute Systems Manager の稼働状況を確認する

## 3.3 JP1/IM でのアラート監視設定

### 3.3.1 JP1/IM でのアラート監視とは

Compute Systems Manager で発生するアラートを JP1 イベントとして転送することで、Compute Systems Manager のアラートを含む多様な製品の情報を JP1/IM で一括して監視できます。

JP1/IM でのアラート監視は、管理サーバの OS が Windows の場合に運用できます。

JP1 イベントとして転送される Compute Systems Manager のアラートは、JP1 イベントの属性に従って JP1/IM のイベントコンソール画面に表示されます。

JP1/IM でアラートを監視するためには、イベント拡張属性定義ファイルをホストに準備したあと、GUI で JP1 イベント転送を有効にする必要があります。

#### 関連項目

- 3.3.2 JP1/IM でアラート監視できるよう設定する

### 3.3.2 JP1/IM でアラート監視できるよう設定する

JP1/IM で Compute Systems Manager のアラートを監視するには、Compute Systems Manager が提供する JP1/IM のイベント拡張属性定義ファイルを準備する必要があります。

JP1/IM でアラート情報を監視するよう設定するために、JP1/IM - Manager がインストールされているホストにイベント拡張属性定義ファイルをコピーしてください。

コピーするイベント拡張属性定義ファイルは、JP1/IM - Manager がインストールされているホストの環境によって異なります。

- 日本語環境の場合  
< Compute Systems Manager のインストールメディア >¥HCSM\_SERVER¥HCSM¥IM  
¥hitachi\_hcsm\_attr\_ja.conf
- 英語環境の場合  
< Compute Systems Manager のインストールメディア >¥HCSM\_SERVER¥HCSM¥IM  
¥hitachi\_hcsm\_attr\_en.conf

イベント拡張属性定義ファイルのコピー先については、JP1/IM のマニュアルを参照してください。

イベント拡張属性定義ファイルを準備したあと、Compute Systems Manager のアラートを JP1/IM で監視できるよう、Compute Systems Manager の GUI で JP1 イベント転送を有効にします。

#### 関連項目

- 3.3.1 JP1/IM でのアラート監視とは
- C.1 Compute Systems Manager が発行する JP1 イベントの属性
- C.2 事象種別ごとの JP1 イベント拡張属性

## 3.4 JP1/IM からの Compute Systems Manager のラウンチ

### 3.4.1 JP1/IM からの Compute Systems Manager のラウンチとは

JP1/IM の統合機能メニュー画面から Compute Systems Manager の GUI をラウンチできます。JP1/IM で Compute Systems Manager から通知されたアラートを確認したあと、Compute Systems Manager の GUI をラウンチしてアラートの詳細を確認できます。

JP1/IM からの Compute Systems Manager のラウンチは、管理サーバの OS が Windows の場合に運用できます。

JP1/IM から Compute Systems Manager の GUI をラウンチするためには、JP1/IM - View の統合機能メニュー定義ファイルを、管理サーバから JP1/IM - View がインストールされているホストにコピーしたあと、環境に合わせて編集する必要があります。

#### 関連項目

- 3.3.1 JP1/IM でのアラート監視とは
- 3.4.2 JP1/IM から Compute Systems Manager をラウンチできるように設定する

### 3.4.2 JP1/IM から Compute Systems Manager をラウンチできるように設定する

JP1/IM から Compute Systems Manager の GUI をラウンチできるようにするには、JP1/IM - View の統合機能メニュー定義ファイルを作成する必要があります。

#### 事前に完了しておく操作

- 管理サーバへの JP1/Base のインストール
- JP1/IM - View にログインするユーザーと同じアカウントを Compute Systems Manager に作成すること

JP1/IM から Compute Systems Manager の GUI をラウンチできるように設定する方法を次に示します。

1. JP1/IM - View の統合機能メニュー定義ファイルを、管理サーバから JP1/IM - View がインストールされているホストにコピーします。

コピー元

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %sample  
¥JP1_IM_conf¥compute_systems_manager_ja.conf
```

統合機能メニュー定義ファイルのコピー先については、JP1/IM のマニュアルを参照してください。

2. コピーした統合機能メニュー定義ファイルの arguments= で始まる行を環境に合わせて修正し、保存します。

```
arguments=" < URL のプロトコル > : // < IP アドレス > : < ポート > / HiCommand /  
IMLogin?jpluserid=%JCO_JP1USER%&jpltoken=%JCO_JP1TOKEN%&launchurl=<  
URL のプロトコル > : // < IP アドレス > : < ポート > / ComputeSystemsManager / Login";  
< URL のプロトコル > , < IP アドレス > および < ポート > を、次のように指定します。
```

< URL のプロトコル >

非 SSL 通信の場合は、http から変更する必要はありません。

SSL 通信の場合は、https を指定します。

< IP アドレス >

管理サーバの IP アドレスを指定します。

< ポート >

HBase 64 Storage Mgmt Web Service のポート番号を指定します。デフォルト値は、非 SSL 通信の場合は 22015、SSL 通信の場合は 22016 です。

JP1/IM の統合機能メニュー画面から [サーバ管理] - [サーバ管理(HCSM)] を選択して、Compute Systems Manager の GUI が表示されれば、正しく設定されています。

#### 関連項目

- 3.4.1 JP1/IM からの Compute Systems Manager のラUNCHとは

## 3.5 管理サーバの設定変更

### 3.5.1 ポート番号の変更

#### (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ

Hitachi Command Suite 共通コンポーネントで使用されるポート番号を変更する場合は、Hitachi Command Suite 共通コンポーネントのプロパティを編集する必要があります。



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている場合は、その製品が使用するポート番号と競合しないように設定してください。

ポート番号を変更する場合に、編集が必要なプロパティを次の表に示します。

デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
22015/TCP	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \u005CuCPSB ¥httpsd¥conf¥user_httpsd.conf Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /u005CuCPSB/ httpsd/conf/user_httpsd.conf	Listen
		Listen [::]: #Listen 127.0.0.1:
22016/TCP	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \u005CuCPSB ¥httpsd¥conf¥user_httpsd.conf Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /u005CuCPSB/ httpsd/conf/user_httpsd.conf	Listen
		Listen [::]: <VirtualHost>タグの<ホスト名>:<ポート番号>
22027/TCP	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \u005CuCPSB¥CC ¥web¥redirector¥workers.properties Linux :	worker.ComputeSystemsManagerWebService.port



デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
	<p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; / uCP SB/CC/web/redirector/ workers.properties</p>	
	<p>Windows : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %uCP SB%\CC%\server%\usrconf%\ejb\ComputeSystemsManagerWebService%\usrconf.properties</p> <p>Linux : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCP SB/CC/server/usrconf/ejb/ComputeSystemsManagerWebService/usrconf.properties</p>	webserver.connector.ajp13.port
22028/TCP	<p>Windows : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %uCP SB%\CC%\server%\usrconf%\ejb\ComputeSystemsManagerWebService%\usrconf.properties</p> <p>Linux : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCP SB/CC/server/usrconf/ejb/ComputeSystemsManagerWebService/usrconf.properties</p>	ejbserver.rmi.naming.port
22031/TCP	<p>Windows : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %uCP SB%\httpsd%\conf%\user_hssd_httpsd.conf</p> <p>Linux : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCP SB/httpsd/conf/user_hssd_httpsd.conf</p>	listen
22032/TCP	<p>Windows : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %HDB%\CONF%\emb%\HiRDB.ini</p> <p>Linux : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /HDB/CONF/emb/HiRDB.ini</p>	PDNAMEPORT
	<p>Windows : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %HDB%\CONF%\pdsys</p> <p>Linux : &lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /HDB/CONF/pdsys</p>	pd_name_port
	Windows :	pd_name_port

デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
	<p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt;¥database¥work¥def_pdsys</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /database/work/def_pdsys</p>	
22035/TCP	<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt;¥uCPSB¥CC¥web¥redirector¥workers.properties</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCPSB/CC/web/redirector/workers.properties</p>	worker.HBase64StgMgmtSSOService.port
	<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt;¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties</p>	webserver.connector.ajp13.port
22036/TCP	<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt;¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties</p>	ejbserver.rmi.naming.port
22037/TCP	<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt;¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties</p>	ejbserver.http.port
22038/TCP	<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt;¥uCPSB¥CC</p>	ejbserver.rmi.remote.listener.port

デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
	¥server¥usrconf¥ejb ¥HBase64StgMgmtSSOService ¥usrconf.properties Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/CC/server/usrconf/ejb/ HBase64StgMgmtSSOService/ usrconf.properties	
22613/TCP	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > ¥uCPSB¥CC¥server¥usrconf¥ejb ¥ComputeSystemsManagerWebService¥usrconf.properties Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/CC/server/usrconf/ejb/ ComputeSystemsManagerWebService/ usrconf.properties	ejbserver.http.port
22614/TCP	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > ¥uCPSB¥CC¥server¥usrconf¥ejb ¥ComputeSystemsManagerWebService¥usrconf.properties Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/CC/server/usrconf/ejb/ ComputeSystemsManagerWebService/ usrconf.properties	ejbserver.rmi.remote.listener.port

#### 関連項目

- (2) ポート変更時に編集する Compute Systems Manager サーバのプロパティ
- (3) ポートを変更する
- A.2 Hitachi Command Suite 共通コンポーネントで使用されるポート
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## (2) ポート変更時に編集する Compute Systems Manager サーバのプロパティ

Compute Systems Manager サーバで使用されるポート番号を変更する場合は、Compute Systems Manager サーバのプロパティを編集する必要があります。

ポート番号を変更する場合に、編集が必要なプロパティを次の表に示します。

デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
162/UDP	Windows : < Compute Systems Manager のインストールディレクトリ > ¥ComputeSystemsManager¥conf¥user.properties	snmp.trap.receive.port
22601/UDP※		
22610/TCP		server.rmi.port

デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
22611/TCP	Linux : < Compute Systems Manager のインストールディレクトリ > /ComputeSystemsManager/conf/user.properties	svp.alert.receive.port

**注※**

デフォルトは 162/UDP です。もし、162/UDP がほかの製品で使用されていた場合、22601/UDP がデフォルトになります。

**関連項目**

- (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (3) ポートを変更する
- A.1 Compute Systems Manager サーバで使用されるポート
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

### (3) ポートを変更する

Compute Systems Manager をインストールしたあとに、Compute Systems Manager で使用されるポート番号を変更する手順を次に示します。

1. Compute Systems Manager を停止します。
2. Compute Systems Manager サーバのプロパティ、または Hitachi Command Suite 共通コンポーネントのプロパティを編集します。
3. Compute Systems Manager を起動します。

ポートが変更されます。

管理サーバと管理クライアント間の通信に使用するポート（デフォルトは 22015/tcp または 22016/tcp）を変更した場合、Compute Systems Manager にアクセスする URL も変更してください。

**関連項目**

- (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (2) ポート変更時に編集する Compute Systems Manager サーバのプロパティ
- (2) Compute Systems Manager の URL を変更する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 3.5.2 管理サーバのホスト名または IP アドレスの変更

### (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ

管理サーバのホスト名を変更した場合、変更が必要な Hitachi Command Suite 共通コンポーネントのプロパティを次の表に示します。



**重要** user\_httpsd.conf ファイルには、ホスト名を指定することをお勧めします。

プロパティファイルの格納パス	プロパティ	編集内容
<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %uCPSEB %httpsd%conf%user_httpsd.conf</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /uCPSEB/ httpsd/conf/user_httpsd.conf</p>	<p>ServerName</p> <p>&lt;VirtualHost&gt;タグ</p> <p>&lt;VirtualHost&gt;タグ内の ServerName パラメーター</p>	<p>変更後のホスト名に変更します。</p> <p>管理サーバと管理クライアント間でセキュリティ通信していて、かつ、ホスト名が指定されていた場合は、アスタリスク (*) に変更します。</p> <p>管理サーバと管理クライアント間でセキュリティ通信している場合は変更後のホスト名に変更します。</p>
<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %HDB%CONF %pdsys</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /HDB/CONF/ pdsys</p>	<p>pdunit -x</p>	<p>ループバックアドレス 127.0.0.1 に変更します。</p>
<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %database %work%def_pdsys</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /database/ work/def_pdsys</p>		
<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %HDB%CONF %pdutsys</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /HDB/CONF/ pdutsys</p>	<p>pd_hostname</p>	
<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %database %work%def_pdutsys</p> <p>Linux :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; /database/ work/def_pdutsys</p>		
<p>Windows :</p> <p>&lt; Hitachi Command Suite 共通コンポーネントのインストールディレクトリ &gt; %HDB%CONF %emb%HiRDB.ini</p> <p>Linux :</p>	<p>PDHOST</p>	

プロパティファイルの格納パス	プロパティ	編集内容
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/ CONF/emb/HiRDB.ini		
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %conf %cluster.conf Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /conf/ cluster.conf	virtualhost onlinehost standbyhost	管理サーバがクラスタ構成の場合、該当するホスト名を変更後のホスト名に変更します。

#### 関連項目

- (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (3) 管理サーバのホスト名または IP アドレスを変更する
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ

管理サーバの IP アドレスを変更した場合、変更が必要な Hitachi Command Suite 共通コンポーネントのプロパティを次の表に示します。



重要 user\_httpsd.conf ファイルには、ホスト名を指定することをお勧めします。

プロパティファイルの格納パス	プロパティ	編集内容
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSPB %httpsd%conf%user_httpsd.conf Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSPB/ httpsd/conf/user_httpsd.conf	ServerName	変更後のホスト名または IP アドレスに変更します。
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %HDB%CONF %pdsys Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/CONF/ pdsys	pdunit -x	変更前の IP アドレスが指定されていた場合は、ループバックアドレス 127.0.0.1 に変更します。
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %database %work%def_pdsys Linux :		

プロパティファイルの格納パス	プロパティ	編集内容
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /database/work/def_pdsys		
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \HDB\CONF\pdsys Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/CONF/pdsys	pd_hostname	
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %database%work%def_pdsys Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /database/work/def_pdsys		
Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \HDB\CONF\emb\HiRDB.ini Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/CONF/emb/HiRDB.ini	PDHOST	

#### 関連項目

- (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (3) 管理サーバのホスト名または IP アドレスを変更する
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

### (3) 管理サーバのホスト名または IP アドレスを変更する

Compute Systems Manager をインストールしたあとに、管理サーバのホスト名または IP アドレスを変更できます。

#### 事前に確認しておく情報

- 変更後の管理サーバのホスト名（ホスト名を変更する場合）  
すでに管理サーバのホスト名を変更した場合は、hostname コマンドで表示されるホスト名を控えておいてください。Windows の場合、ホスト名は ipconfig /ALL コマンドでも表示できます。  
ホスト名は次の条件をすべて満たす必要があります。
  - 長さが 128 バイト以内であること。
  - 次の文字で構成されていること。  
A~Z a~z 0~9 - .  
ただし、ハイフン (-) はホスト名の先頭と末尾には使用できません。

- 変更後の管理サーバの IP アドレス (IP アドレスを変更する場合)

管理サーバのホスト名または IP アドレスを変更する手順を次に示します。

1. IP アドレスを変更する場合、すべてのシャーンを管理対象から外します。
2. Compute Systems Manager を停止します。
3. Hitachi Command Suite 共通コンポーネントのプロパティを編集します。
4. 管理サーバの OS が Linux であり、かつホスト名を変更する場合は、`/etc/hosts` ファイルを編集します。  
管理サーバのホスト名を変更後のホスト名に変更します。localhost が記述されている行よりも、上の行に変更後のホスト名を記述してください。
5. Compute Systems Manager 以外の Hitachi Command Suite 製品を使用している場合、必要に応じてそれぞれの製品の設定を見直します。
6. 管理サーバのホスト名または IP アドレスを変更します。  
管理サーバに設定する実際のホスト名を、大文字と小文字の区別も含めそのまま指定してください。
7. マシンを再起動したあと、Compute Systems Manager が正常に起動していることを確認します。
8. Compute Systems Manager にアクセスする URL に変更前のホスト名または IP アドレスが使われている場合、URL を変更します。
9. IP アドレスを変更した場合、管理対象から外したシャーンを管理対象に戻します。
10. データベースのバックアップを取得します。  
ホスト名または IP アドレスを変更すると、変更前にバックアップしたデータベースは使用できなくなるためです。

管理サーバのホスト名または IP アドレスが変更されます。

#### 関連項目

- (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (2) Compute Systems Manager の URL を変更する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## 3.5.3 Compute Systems Manager の URL の変更

### (1) Compute Systems Manager の URL を変更するタイミング

Compute Systems Manager の運用を開始したあとに、次のどれかの設定を変更した場合、Compute Systems Manager にアクセスするための URL を変更する必要があります。

- 管理クライアントと管理サーバ間で使用するポート番号の変更
- 管理サーバのホスト名または IP アドレスの変更
- SSL 通信を使用するため、または SSL 通信の使用を中止するための設定変更



## 関連項目

- (2) Compute Systems Manager の URL を変更する

## (2) Compute Systems Manager の URL を変更する

管理サーバのホスト名, IP アドレス, ポート番号, SSL 通信の設定などを変更した場合は, Compute Systems Manager にアクセスする URL を変更する必要があります。

### 事前に確認しておく情報

- 変更後の URL  
プロトコルとポートを含む完全な URL (例: `http://HostA:22015`) を指定する必要があります。

Compute Systems Manager の URL を変更する手順を次に示します。

1. 次のコマンドを実行して, 現在登録されている URL の情報を確認します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcms64chgurl /list
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64chgurl -list
```

2. 次のコマンドを実行して, Compute Systems Manager にアクセスする URL を変更します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcms64chgurl /change <変更後の URL > /type HCSM
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64chgurl -change <変更後の URL > -type HCSM
```

3. 同じ管理サーバにインストールされている Compute Systems Manager 以外の Hitachi Command Suite 製品の URL もすべて変更する場合には, 次の hcms64chgurl コマンドを実行します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcms64chgurl /change <変更前の URL > <変更後の URL >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64chgurl -change <変更前の URL > <変更後の URL >
```

4. Windows の場合, ショートカットファイルの URL を変更します。

Windows Server 2008 R2 の場合 :

[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Compute Systems Manager] - [Login - HCSM] を右クリックして, [プロパティ] - [Web ドキュメント] タブの URL を変更します。

Windows Server 2012 の場合 :

[スタート] - [すべてのアプリ] - [Hitachi Command Suite] - [Compute Systems Manager] - [Login - HCSM] を右クリックして, [プロパティ] - [Web ドキュメント] タブの URL を変更します。

URL の形式は次のとおりです。

<プロトコル>://<管理サーバの IP アドレスまたはホスト名>:<ポート番号>/  
ComputeSystemsManager/

<プロトコル>

非 SSL 通信の場合は http, SSL 通信の場合は https を指定します。

<管理サーバの IP アドレスまたはホスト名>

Compute Systems Manager をインストールした管理サーバの IP アドレスまたはホスト名を指定します。

<ポート番号>

user\_httpsd.conf ファイルの Listen 行に設定されているポート番号を指定します。  
非 SSL 通信の場合は非 SSL 通信用のポート番号 (デフォルト: 22015), SSL 通信の場合は SSL 通信用のポート番号 (デフォルト: 22016) を指定します。

user\_httpsd.conf ファイルの格納先は次のとおりです。

<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%uCPSE  
%httpsd%conf%user\_httpsd.conf

Compute Systems Manager にアクセスする URL が変更されます。

JP1/IM から Compute Systems Manager の GUI をラUNCHできるように設定している場合は、JP1/IM - View の統合機能メニュー定義ファイルも変更してください。

#### 関連項目

- [3.4.1 JP1/IM からの Compute Systems Manager のラUNCHとは](#)
- [\(1\) Compute Systems Manager の URL を変更するタイミング](#)

## 3.5.4 JDK を変更する

管理サーバで使用する JDK を変更したい場合、Compute Systems Manager をインストールしたあとに、必要に応じて変更できます。

使用する JDK を変更する手順を次に示します。

1. Compute Systems Manager を停止します。
2. 次のコマンドを実行して、JDK を変更します。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64chgjdk
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64chgjdk
```

3. 表示された画面で、使用する JDK を選択します。
4. Compute Systems Manager を起動します。
5. セキュリティ通信している場合は、次の証明書を管理サーバにインポートし直します。
  - Hitachi Command Suite 共通コンポーネントのサーバ証明書および認証局の証明書
  - Compute Systems Manager サーバのサーバ証明書および認証局の証明書
  - LDAP ディレクトリサーバのサーバ証明書インポートし直すことで、証明書の格納場所が切り替わります。



#### 重要

- Oracle JDK を上書きまたはアップデートした場合は、hcmds64chgjdk コマンドを再実行して、設定し直してください。
- Oracle JDK をアンインストールする場合は、hcmds64chgjdk コマンドを実行して表示される画面で製品に同梱された JDK を選択してください。

#### 関連項目

- 5.1 セキュリティの設定とは
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 3.5.5 管理サーバの時刻設定の更新

### (1) Compute Systems Manager で適用される時刻について

Compute Systems Manager は、管理サーバの時刻を基準としてデータを管理します。

このため、管理クライアントの GUI または CLI で表示されるタスクやアラートに関する時刻なども、管理サーバの時刻を基準に表示されます。

#### 関連項目

- (2) 運用開始後に管理サーバの時刻を調整する

### (2) 運用開始後に管理サーバの時刻を調整する

NTP など、時刻を自動的に調整する機能を使用できない場合、または直ちに時刻を変更する必要がある場合、管理サーバの時刻を手動で変更します。



**重要** 米国およびカナダのタイムゾーンで Compute Systems Manager を使用する場合、2007 年から米国およびカナダで適用された新しい DST (サマータイム) に対応するよう、管理サーバの OS の設定を変更してください。OS が新しい DST に対応していない場合、Compute Systems Manager も対応しません。

管理サーバの時刻を手動で変更する手順を次に示します。

1. Compute Systems Manager を停止します。
2. 現在の管理サーバの時刻を控えたあとで、管理サーバの時刻を変更します。
3. 管理サーバの時刻を遅らせた場合、時刻を変更した時点の管理サーバの時刻になるまで待ちます。  
時刻を進めた場合、この手順はスキップして次の手順に移ってください。

4. OS を再起動します。

管理サーバに時刻が反映されます。

#### 関連項目

- (1) Compute Systems Manager で適用される時刻について

## 3.5.6 アラート発生時に実行するコマンドのタイムアウト時間を変更する

アラート発生時に実行するコマンドのタイムアウト時間を変更できます。処理に時間の掛かるコマンドを実行する場合は、タイムアウト時間を調整してください。

アラート発生時に実行するコマンドのタイムアウト時間を変更する手順を次に示します。

1. Compute Systems Manager を停止します。
  2. 次の場所に格納されている user.properties を開きます。  
Windows :  
< Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager¥conf¥user.properties  
Linux :  
< Compute Systems Manager のインストールディレクトリ >/ComputeSystemsManager/conf/user.properties
  3. server.process.timeout プロパティに、 コマンドのタイムアウト時間を設定します。
  4. Compute Systems Manager を起動します。
- コマンドのタイムアウト時間が変更されます。

#### 関連項目

- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

### 3.5.7 管理クライアントに表示される温度の単位を設定する

Compute Systems Manager でリソースの電力情報を取得している場合、管理クライアントに表示される温度の単位を、華氏または摂氏に変更できます。

管理クライアントに表示される温度の単位を設定する手順を次に示します。

1. Compute Systems Manager を停止します。
2. 次の場所に格納されている user.properties を開きます。  
Windows :  
< Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager¥conf¥user.properties  
Linux :  
< Compute Systems Manager のインストールディレクトリ >/ComputeSystemsManager/conf/user.properties
3. powermonitoring.temperature.unit プロパティに、温度の表示単位を設定します。  
powermonitoring.temperature.unit プロパティが設定されていない場合は追記します。
4. Compute Systems Manager を起動します。

管理クライアントに表示される温度の単位が変更されます。

#### 関連項目

- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

### 3.5.8 管理サーバのファイアウォールに例外登録をする (Windows)

Compute Systems Manager をインストールしたあとで Windows ファイアウォールを有効にした場合、Windows ファイアウォールの例外リストに Hitachi Command Suite 共通コンポーネントのサービスを登録する必要があります。

#### 事前に確認しておく情報

- Windows ファイアウォールのサービスが起動されている

管理サーバの Windows ファイアウォールに例外登録をする手順を次に示します。

1. 次のコマンドを実行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin%  
%hcmds64fwcancel
```

2. 次のコマンドを実行します。

```
netsh advfirewall firewall add rule name="HBase(trap)" dir=in  
action=allow program="<Hitachi Command Suite 共通コンポーネントのインストー  
ルディレクトリ>%uCP%server%bin%cjstartsv.exe" description="<  
Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%uCP%  
server%bin%cjstartsv.exe" enable=yes
```

3. Compute Systems Manager を再起動します。



参考 Windows ファイアウォールを有効にしてから Compute Systems Manager をインストールすれば、インストール時に自動的に Windows ファイアウォールの設定が変更されます。

#### 関連項目

- 4.3.2 Windows ファイアウォールを設定する (Windows ホスト)
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

### 3.5.9 管理サーバのファイアウォールに例外登録をする (Linux)

管理サーバの OS が Linux で、かつ次のどちらかに該当する場合は、ファイアウォールの例外リストに Compute Systems Manager で使用されるポート番号を登録する必要があります。

- ファイアウォールを有効にしている環境に Compute Systems Manager をインストールする場合
- Compute Systems Manager をインストールしたあとでファイアウォールを有効にした場合



重要 次に示す手順は、Red Hat Enterprise Linux 6.2 を使用した場合の例です。Red Hat Enterprise Linux 6.2 以外のファイアウォール設定の詳細については、各 OS のドキュメントを参照してください。

管理サーバのファイアウォールに例外登録をする手順を次に示します。

1. ターミナルウィンドウから setup コマンドを実行します。

テキストモードセットアップユーティリティの [ツール選択] 画面が表示されます。

2. [ファイアウォールの設定] を選択し、[Tab] キーで [実行ツール] ボタンへ移動し、[Enter] キーを押します。

[ファイアウォール設定] 画面が表示されます。

3. [セキュリティレベル] を [有効] に合わせ、スペースキーを押してチェックを入れ、[Tab] キーで [カスタマイズ] ボタンへ移動し、[Enter] キーを押します。

[ファイアウォール設定ーカスタマイズ] 画面が表示されます。

4. [その他のポート] に例外登録するポートを指定し、[Tab] キーで [OK] ボタンへ移動し、[Enter] キーを押します。

ポートを指定する例を次に示します。

その他のポート 162:udp 22015:tcp



**重要** すでにポートが指定されていた場合は、空白区切りで追加入力してください。

5. [ファイアウォール設定] 画面に戻ったら、[セキュリティレベル] が [有効] になっていることを確認し、[Tab] キーで [OK] ボタンへ移動し、[Enter] キーを押します。

#### 関連項目

- 3.5.10 管理サーバのファイアウォールに例外登録が必要なポート (Linux)

### 3.5.10 管理サーバのファイアウォールに例外登録が必要なポート (Linux)

管理サーバが Linux の場合に、ファイアウォールの例外リストに登録する必要があるポートの一覧を次の表に示します。

ポート番号をデフォルトから変更している場合は、例外登録するポート番号も変更してください。

表 3-1 管理サーバのファイアウォールに例外登録が必要なポート (Linux)

デフォルトのポート番号	説明
162/UDP	管理クライアントから SNMP トラップを受信する際に使用されます。 162/UDP がほかの製品で使用されていた場合、インストール時にポート番号を変更 (推奨値: 22601/UDP) しているため、例外リストには変更したポート番号を登録します。
22015/TCP	管理クライアント (GUI および CLI) と非 SSL で通信する際に、Hitachi Command Suite 共通コンポーネントのサービス (HBase 64 Storage Mgmt Web Service) へのアクセスで使用されます。
22016/TCP	管理クライアント (GUI) と SSL 通信する際に、Hitachi Command Suite 共通コンポーネントのサービス (HBase 64 Storage Mgmt Web Service) へのアクセスで使用されます。
22610/TCP	Device Manager と通信する際に使用されます。
22611/TCP	日立製のサーバからのアラートを受信する際に使用されます。

#### 関連項目

- 3.5.9 管理サーバのファイアウォールに例外登録をする (Linux)

### 3.5.11 WinRM の設定を反映する (Linux)

管理対象ホストで MaxEnvelopeSizekb に推奨値以外を指定して WinRM を有効にした場合、user.properties ファイルのプロパティを編集して、WinRM の設定を反映する必要があります。

#### 事前に確認しておく情報

- 管理対象ホストで設定した MaxEnvelopeSizekb の値  
複数の管理対象ホストで異なる値を設定している場合は、それらの値の中の最大値

#### 事前に完了しておく操作

- WinRM の有効化

WinRM の設定を反映する手順を次に示します。

1. Compute Systems Manager を停止します。
2. 次の場所に格納されている user.properties ファイルを開きます。  
    < *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/  
    conf/user.properties
3. winrm.maxEnvelopeSize プロパティに、事前に確認しておいた MaxEnvelopeSizekb の値を  
    指定します。
4. Compute Systems Manager を起動します。

#### 関連項目

- [4.3.4 WinRM を有効にする \(Windows ホスト\)](#)
- [8.1.2 Compute Systems Manager を起動する](#)
- [8.1.3 Compute Systems Manager を停止する](#)
- [B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ \(user.properties\)](#)





## 管理対象の設定

この章では、Compute Systems Manager の管理対象を設定するための前提条件および手順について説明します。

- 4.1 管理対象ホストの設定
- 4.2 管理対象サーバの設定
- 4.3 管理対象ホストの設定 (Windows ホスト)
- 4.4 管理対象ホストの設定 (Linux ホスト)
- 4.5 移行する管理対象ホストを探索するための設定を変更する
- 4.6 シャーシのマネジメントモジュールの IP アドレスを変更する

## 4.1 管理対象ホストの設定

### 4.1.1 WoL を有効にする

Compute Systems Manager では、ユーザーが設定した BMC の情報を基に、WoL を利用して管理対象ホストの電源を制御できます。WoL を有効にしておくことで、電源 ON 時に BMC の設定がない場合でも、WoL によって処理が試行されます。

#### 事前に確認しておく情報

- 管理対象ホストが WoL に対応している

ネットワークアダプターの WoL の設定を有効にします。設定の詳細については、サーバ（ハードウェア）の各ベンダーのドキュメントを参照してください。



**注意** ネットワークにスイッチまたはルーターが配置されている場合に WoL を使用するとき、管理対象ホストの電源管理ができなくなることがあります。次の場合に注意してください。

- マジックパケットが遮断された場合
- 電源が切れた結果、ARP テーブルから管理対象ホストの IP アドレス（マジックパケットの送信先）が消えた場合

#### 関連項目

- 4.3.1 ホストを管理対象にするための確認事項（Windows ホスト）
- 4.4.1 ホストを管理対象にするための確認事項（Linux ホスト）

### 4.1.2 BMC 監視を有効にする

Alive Monitor をインストールすると、BMC とホスト間で相互に監視できます。ホストに異常が発生した場合は、Compute Systems Manager にアラートが通知されます。BMC に異常が発生した場合は、ホストにログが出力されます。

管理対象ホストが Alive Monitor の適用 OS であることを確認の上、管理対象ホストに Alive Monitor をインストールします。

#### 関連項目

- 4.3.1 ホストを管理対象にするための確認事項（Windows ホスト）
- 4.4.1 ホストを管理対象にするための確認事項（Linux ホスト）

## 4.2 管理対象サーバの設定

### 4.2.1 日立製のブレードサーバを管理対象にするための確認事項

日立製のブレードサーバを管理対象として登録する前に、次の条件を満たしていることを確認してください。

- 日立製のブレードサーバとシャーシのマネジメントモジュールが最新のファームウェアの必要条件を満たしている  
詳細については、ソフトウェア添付資料を参照してください。
- シャーシのマネジメントモジュールが HTTPS のポートを使用する設定になっている

日立製のブレードサーバに付属している Web コンソールを使用して、HTTPS のポートの設定を確認してください。

## 4.2.2 日立製のラックマウントサーバを管理対象にするための確認事項

日立製のラックマウントサーバを管理対象として登録する前に、次の条件を満たしていることを確認してください。

- 日立製のラックマウントサーバの BMC が最新のファームウェアの必要条件を満たしている  
詳細については、ソフトウェア添付資料を参照してください。
- ラックマウントの BMC モジュールが HTTPS または SSH のポートを使用する設定になっている  
日立製のラックマウントサーバに付属している Web コンソールを使用して、HTTPS または SSH のポートの設定を確認してください。  
ラックマウントサーバの機種によって、使用するポートが異なります。ラックマウントサーバが使用するポートについては、ソフトウェア添付資料を参照してください。



**重要** ラックマウントサーバの一部機種の場合、電力情報を取得するには次の条件をすべて満たす必要があります。

- ラックマウントサーバ上のホストで Update Manager の snvpowermonitor サービスが稼働していること
- 電力情報を取得するラックマウントサーバ、および Update Manager が稼働しているホストが Compute Systems Manager の管理対象になっていること  
対象となるラックマウントサーバの機種については、ソフトウェア添付資料を参照してください。

## 4.3 管理対象ホストの設定（Windows ホスト）

### 4.3.1 ホストを管理対象にするための確認事項（Windows ホスト）

Windows ホストを管理対象に設定するため、ホストで事前に確認しておく情報と事前に完了しておく操作を、次に示します。

#### 事前に確認しておく情報

- ホストのハードウェアが Compute Systems Manager の前提ハードウェアである
- ホストの OS が Compute Systems Manager の適用 OS である
- リモート接続で使用するアカウントが、Administrators グループ所属でホストに登録されている

#### 事前に完了しておく操作

- 前提ソフトウェアのインストール
- Windows ファイアウォールの設定（管理サーバが Windows の場合）
- DCOM の有効化（管理サーバが Windows の場合）
- WinRM の有効化（管理サーバが Linux の場合）
- UAC を使用するためのリモート接続設定（任意）
- WoL の有効化（任意）

#### 関連項目

- [4.1.1 WoL を有効にする](#)

- 4.3.2 Windows ファイアウォールを設定する (Windows ホスト)
- 4.3.3 DCOM を有効にする (Windows ホスト)
- 4.3.4 WinRM を有効にする (Windows ホスト)
- 4.3.5 UAC を使用したリモート接続を設定する (Windows ホスト)

## 4.3.2 Windows ファイアウォールを設定する (Windows ホスト)

管理サーバの OS が Windows の場合、Windows ファイアウォールで WMI (DCOM) の通信を許可することで、管理対象ホストと通信できるようにします。

### 事前に確認しておく情報

- 管理対象ホストが Windows である
- Windows ファイアウォールが有効になっている

管理対象ホストが Windows の場合に、Windows ファイアウォールで WMI の通信を許可する手順を次に示します。

1. Windows ファイアウォールで [受信接続] が [すべての接続をブロック] の場合は [許可] または [ブロック (既定)] に変更します。  
[許可] に変更した場合は、次の手順以降は不要です。
2. 次のコマンドを実行して、Windows ファイアウォールで WMI の [規則] を有効にします。  

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

Windows ファイアウォールの設定で WMI の [規則] が有効になります。

### 関連項目

- 4.3.1 ホストを管理対象にするための確認事項 (Windows ホスト)

## 4.3.3 DCOM を有効にする (Windows ホスト)

管理サーバの OS が Windows の場合、管理対象ホストの DCOM を有効にすることで、WMI の通信が有効になり、管理対象ホストの情報が取得できるようになります。

DCOM を有効にする手順を次に示します。

1. dcomcnfg コマンドを実行します。
2. コンポーネントサービスのサブカテゴリの [コンピュータ] から [マイコンピュータ] を選択します。
3. 右クリックして [プロパティ] を選択します。
4. [既定のプロパティ] タブを選択し、[このコンピュータ上で分散 COM を有効にする] チェックボックスが選択されていることを確認します。
5. [COM セキュリティ] タブを選択し、次の項目を確認します。
  - [アクセス許可] の [制限の編集] ボタンをクリックし、Everyone グループに対して [リモートアクセス] の [許可] チェックボックスが選択されていること。
  - [起動とアクティブ化のアクセス許可] の [制限の編集] ボタンをクリックし、Administrators グループに対して [リモートからのアクティブ化] の [許可] チェックボックスが選択されていること。
6. 管理対象ホストを再起動します。

DCOM が有効になります。

#### 関連項目

- ・ 4.3.1 ホストを管理対象にするための確認事項 (Windows ホスト)

### 4.3.4 WinRM を有効にする (Windows ホスト)

管理サーバの OS が Linux の場合、管理対象ホストの Windows リモート管理 (WinRM) を有効にすることで、管理対象ホストの情報が取得できるようになります。

#### 事前に確認しておく情報

- ・ 管理対象ホストが Windows ホストである

WinRM を有効にする手順を次に示します。

1. 次のコマンドを実行して、WinRM を有効にします。

```
winrm qc
winrm set winrm/config/service @{AllowUnencrypted="true"}
winrm set winrm/config @{MaxEnvelopeSizekb="512"}
```

MaxEnvelopeSizekb の値は 512 (推奨値) を指定してください。ただし、ファイバーチャネル接続している管理対象ホストで、認識される LU 数が 25 を超える場合は LU 数×20 を指定します。

なお、ラックマウントサーバの一部機種の電力情報を Update Manager から取得する場合、MaxEnvelopeSizekb の値は 1500 (推奨値) を指定してください。ただし、ファイバーチャネル接続している管理対象ホストで、認識される LU 数が 75 を超える場合は LU 数×20 を指定します。

対象となるラックマウントサーバの機種については、ソフトウェア添付資料を参照してください。

2. WinRM が使用するポート番号を変更する場合、次のコマンドを実行します。

```
winrm delete winrm/config/Listener?Address=*&Transport=HTTP
winrm create winrm/config/Listener?Address=*&Transport=HTTP @{Port="<変更後のポート番号>"}
```

WinRM が使用するポート番号のデフォルト値は、80 または 5985 です。デフォルト値は、WinRM のバージョンによって異なります。

手順 1 で、MaxEnvelopeSizekb に推奨値以外を指定した場合、管理サーバでプロパティファイルを編集して、WinRM の設定を反映する必要があります。

WinRM が有効になります。

#### 関連項目

- ・ 3.5.11 WinRM の設定を反映する (Linux)
- ・ 4.3.1 ホストを管理対象にするための確認事項 (Windows ホスト)

### 4.3.5 UAC を使用したリモート接続を設定する (Windows ホスト)

Windows ホストと UAC を使用して接続するためには、管理サーバとホスト間のリモート接続が設定されている必要があります。

UAC が有効になっている状態で、Administrator (ビルトインアカウント) でないローカルユーザーを使用してリモート接続する場合、管理対象ホストでリモート接続を許可するよう設定します。



参考 Administrator (ビルトインアカウント) およびドメインユーザーは、標準で UAC を使用したリモート接続が許可されているため、このトピックで説明している設定は不要です。

#### 事前に確認しておく情報

- 管理対象ホストが Windows である

次に示すコマンドを実行して、UAC のリモート接続を許可します。コマンド実行後、OS の再起動は不要です。

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```



参考 UAC リモート接続の許可を解除する場合は次のコマンドを実行します。ただし、次のコマンドを実行した場合は、OS の再起動が必要です。

```
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /f
```

#### 関連項目

- 4.3.1 ホストを管理対象にするための確認事項 (Windows ホスト)

## 4.3.6 SNMP トラップを設定する (Windows ホスト)

Windows の管理対象ホストで発生したイベントのトラップを管理サーバで監視するには、管理対象ホストでの設定が必要です。

トラップを送信したい Windows の管理対象ホストにはすべて設定してください。



参考 日立製のサーバ上に作成したホストの場合、SNMP トラップの設定は不要です。

#### 関連項目

- 3.1.3 インバンド SNMP トラップの監視とは
- 3.1.4 インバンド SNMP トラップを監視する
- (3) ポートを変更する

## 4.4 管理対象ホストの設定 (Linux ホスト)

### 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)

Linux ホストを管理対象に設定するため、ホストで事前に確認しておく情報と事前に完了しておく操作を次に示します。

#### 事前に確認しておく情報

- ホストのハードウェアが Compute Systems Manager の前提ハードウェアである
- ホストの OS が Compute Systems Manager の適用 OS である
- 使用するアカウントがホストに登録されている
- OS のファイルおよびディレクトリ構成が登録可能な状態である

#### 事前に完了しておく操作

- 前提ソフトウェアのインストール
- 前提パッケージのインストール  
詳細については、ソフトウェア添付資料を参照してください。
- IP 接続の許可
- WoL の有効化（任意）

#### 関連項目

- 4.1.1 WoL を有効にする
- 4.4.2 OS のファイルおよびディレクトリ構成の確認項目（Linux ホスト）
- 4.4.3 Compute Systems Manager で使用するアカウントを設定する（Linux ホスト）
- 4.4.4 IP 接続を許可する（Linux ホスト）
- 4.4.5 管理対象ホストへのログインの許可とは
- 4.4.6 root ユーザーでのログインを許可する（Linux ホスト）
- 4.4.7 一般ユーザーでログインし、su コマンドを利用することを許可する（Linux ホスト）
- 4.4.8 一般ユーザーでログインし、sudo コマンドを利用することを許可する（Linux ホスト）

### 4.4.2 OS のファイルおよびディレクトリ構成の確認項目（Linux ホスト）

Linux ホストを管理対象として登録する場合に、ホストの OS のファイルおよびディレクトリ構成が次の状態になっているか確認してください。

- 次に示す OS 標準のコマンドのパスが変更されていない  
/sbin, /bin, /usr/sbin, /usr/bin
- /proc および/sys のディレクトリがある
- 次に示す Linux のディストリビューション情報ファイルが、存在していて、かつ変更されていない
  - Red Hat Enterprise Linux の場合 : /etc/redhat-release
  - SUSE Linux の場合 : /etc/SuSE-release
  - Oracle Linux の場合 : /etc/oracle-release または /etc/enterprise-release

### 4.4.3 Compute Systems Manager で使用するアカウントを設定する（Linux ホスト）

管理対象ホストが Linux の場合に、Compute Systems Manager で使用するアカウントの設定が必要です。

管理サーバから操作できるアカウントを割り当てる手順を次に示します。

1. ログインシェルを bash または tcsh に設定します。  
設定の例を次に示します。
  - 既存アカウントの場合 : usermod コマンドでログインシェルを変更します。
  - 新規アカウント作成の場合 : useradd コマンド実行時にログインシェルを指定します。
2. Compute Systems Manager で使用するアカウントの初期化スクリプトを変更している場合、次に示すファイルの内容を、OS をインストールした直後の状態に戻します。

- `bash` : /etc/profile, ~/.bash\_profile, ~/.bashrc
- `tcsh` : /etc/csh.login, /etc/csh.cshrc, ~/.login, ~/.cshrc



**重要** 初期化スクリプトを変更した内容によっては、ホストの探索に失敗するおそれがあります。

管理サーバから管理対象ホストにリモート接続できるようになります。

#### 関連項目

- 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)
- 4.4.5 管理対象ホストへのログインの許可とは

## 4.4.4 IP 接続を許可する (Linux ホスト)

管理対象ホストが Linux の場合に、管理サーバとの SSH プロトコルによる IP 接続の設定が必要です。

管理サーバからの SSH プロトコルによる接続を許可する手順を次に示します。

1. OS の TCP Wrapper 機能が有効になっている場合は、`/etc/hosts.allow` に管理サーバの IP アドレスを追記します。

```
sshd:<管理サーバの IP アドレス>
```

記述例を次に示します。

```
sshd:168.1.2.3
```

2. ほかのユーザーが SSH プロトコルによって接続していないことを確認します。
3. `/etc/ssh/sshd_config` を開き、次の項目の値を変更します。

```
PermitRootLogin yes
```

一般ユーザーだけをログインに利用する場合は、`PermitRootLogin no` に変更します。

```
PasswordAuthentication yes
```

```
Protocol 2,1 または Protocol 2
```

4. 次のコマンドを実行して、デーモンを再起動します。

```
Red Hat Enterprise Linux 6 以前または Oracle Linux 6 の場合 : /etc/rc.d/init.d/sshd restart
```

```
Red Hat Enterprise Linux 7 または Oracle Linux 7 の場合 : systemctl restart sshd
```

```
SUSE Linux の場合 : service sshd restart
```

5. 管理対象ホストでファイアウォールを設定した場合は、SSH プロトコルによる接続を許可するポートの設定を変更する必要があります。

ファイアウォール設定の詳細については、各 OS のドキュメントを参照してください。

SSH プロトコルによる接続が許可されます。

#### 関連項目

- 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)
- 4.4.5 管理対象ホストへのログインの許可とは

## 4.4.5 管理対象ホストへのログインの許可とは

Linux の管理対象ホストにアクセスする際、ホストに登録されているアカウントを使ってアクセスします。アカウントには `root` 権限が必要です。



次のどれかの方法で Linux の管理対象ホストにアクセスできます。運用に合わせて使い分けてください。

- 一般ユーザーでアクセスし、`sudo` コマンドで `root` 権限を持つユーザーで実行する  
ホストにアクセスする方法で最も安全な方法です。`root` 権限を持つユーザーで実行するためには、管理対象ホストで `sudo` コマンドの設定が必要です。
- 一般ユーザーでアクセスし、`su` コマンドで `root` 権限を持つユーザーに切り替える  
ユーザー ID やパスワードが漏えいしなければ、`root` ユーザーでアクセスするより安全です。ただし、`root` 権限を持つユーザーに切り替えるためには、`root` ユーザーのパスワードが必要です。
- `root` ユーザーでアクセスする  
`root` ユーザーでアクセスすることは容易ですが、`root` パスワードが漏えいして管理対象ホストの設定が偽造されるおそれがあります。`root` ユーザーでのアクセスは、権限のないアクセスを防止できる環境の場合に採用してください。

#### 関連項目

- [4.4.3 Compute Systems Manager で使用するアカウントを設定する \(Linux ホスト\)](#)
- [4.4.4 IP 接続を許可する \(Linux ホスト\)](#)
- [4.4.6 root ユーザーでのログインを許可する \(Linux ホスト\)](#)
- [4.4.7 一般ユーザーでログインし、su コマンドを利用することを許可する \(Linux ホスト\)](#)
- [4.4.8 一般ユーザーでログインし、sudo コマンドを利用することを許可する \(Linux ホスト\)](#)

### 4.4.6 root ユーザーでのログインを許可する (Linux ホスト)

Linux の管理対象ホストと管理サーバ間で SSH プロトコルを使用する場合は、ログインユーザーの設定が必要です。



**参考** 管理対象ホストに一般ユーザーでログインして `su` コマンドまたは `sudo` コマンドを利用する場合は、このトピックで説明している設定は不要です。

#### 事前に確認しておく情報

- 管理対象ホストが Linux である

#### 事前に完了しておく操作

- `root` ユーザーを使用した、SSH プロトコルによる IP 接続の設定

`root` ユーザーでログインできるようにする手順を次に示します。

管理対象ホストを探索するときに利用する認証情報として、次の情報を管理サーバに登録します。

- IP アドレス : <管理対象ホストの IP アドレス>
- ポート番号 : <管理対象ホストの SSH ポート番号>
- ユーザー名 : `root`
- パスワード : <`root` ユーザーのパスワード>
- `su` パスワード : 空白

管理クライアントを使用した管理対象ホストの設定については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

## 関連項目

- 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)
- 4.4.4 IP 接続を許可する (Linux ホスト)
- 4.4.5 管理対象ホストへのログインの許可とは

## 4.4.7 一般ユーザーでログインし、su コマンドを利用することを許可する (Linux ホスト)

Linux の管理対象ホストと管理サーバ間で SSH プロトコルを使用する場合は、ログインユーザーの設定が必要です。



参考 管理対象ホストに root ユーザーでログインする場合、または一般ユーザーでログインして sudo コマンドを利用する場合は、このトピックで説明している設定は不要です。

### 事前に確認しておく情報

- 管理対象ホストが Linux である

### 事前に完了しておく操作

- root 権限を持たない一般ユーザーを使用した、SSH プロトコルによる IP 接続の設定

管理対象ホストに一般ユーザーでログインし、su コマンドを利用できるようにする手順を次に示します。

1. 管理対象ホストを探索するときに利用する認証情報として、次の情報を管理サーバに登録します。
  - IP アドレス : <管理対象ホストの IP アドレス>
  - ポート番号 : <管理対象ホストの SSH ポート番号>
  - ユーザー名 : <ログイン時に使用する一般ユーザー名>
  - パスワード : <一般ユーザーのパスワード>
  - su パスワード : <root ユーザーのパスワード>

管理クライアントを使用した管理対象ホストの設定については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

2. root ユーザーでのアクセスを制限したい場合は、管理対象ホストで/etc/ssh/sshd\_config を開き、PermitRootLogin の値を次のように変更します。

```
PermitRootLogin no
```



### 重要

- ほかのプログラムで root ユーザーを使ってログインすることがない場合は、PermitRootLogin no に設定することをお勧めします。
- Device Manager と Compute Systems Manager を同じ管理サーバで使用する場合、Device Manager では sudo コマンドを実行できるように設定する必要があります。  
Device Manager での sudo コマンドの設定方法については、マニュアル「*Hitachi Command Suite システム構成ガイド*」を参照してください。

一般ユーザーでログインして su コマンドを利用できるようになります。

## 関連項目

- 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)

- ・ 4.4.4 IP 接続を許可する (Linux ホスト)
- ・ 4.4.5 管理対象ホストへのログインの許可とは

## 4.4.8 一般ユーザーでログインし、sudo コマンドを利用することを許可する (Linux ホスト)

Linux の管理対象ホストと管理サーバ間で SSH プロトコルを使用する場合は、ログインユーザーの設定が必要です。



**参考** 管理対象ホストに root ユーザーでログインする場合、または一般ユーザーでログインして su コマンドを利用する場合は、このトピックで説明している設定は不要です。

### 事前に確認しておく情報

- ・ 管理対象ホストが Linux である

### 事前に完了しておく操作

- ・ root 権限を持たない一般ユーザーを使用した、SSH プロトコルによる IP 接続の設定  
一般ユーザーでログインし、sudo コマンドを利用できるようにする手順を次に示します。

1. 次に示す定義を sudo コマンドの設定に追加します。

```
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /usr/sbin/dmidecode  
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /usr/sbin/smartctl  
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /sbin/ethtool  
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /sbin/shutdown
```

2. SUSE Linux の場合、次に示す定義も sudo コマンドの設定に追加します。

```
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /bin/cat  
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /bin/df
```

3. Red Hat Enterprise Linux 6 以降、Oracle Linux 6 以降、SUSE Linux 11 SP1 以降、および SUSE Linux 12 の場合、次に示す定義も sudo コマンドの設定に追加します。

```
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /usr/sbin/exportfs
```

4. ラックマウントサーバの一部機種の電力情報を Update Manager から取得する場合は、次に示す定義も sudo コマンドの設定に追加します。

```
<一般ユーザー名> <管理対象ホスト名>=NOPASSWD: /opt/hitachi/snv/bin/snvcli  
対象となるラックマウントサーバの機種については、ソフトウェア添付資料を参照してください。
```

5. root ユーザーでのアクセスを制限したい場合は、管理対象ホストで/etc/ssh/sshd\_config を開き、PermitRootLogin の値を次のように変更します。

```
PermitRootLogin no
```



**重要** ほかのプログラムで root ユーザーを使ってログインすることがない場合は、PermitRootLogin no に設定することをお勧めします。

6. 管理対象ホストを探索するときに利用する認証情報として、次の情報を管理サーバに登録します。
  - IP アドレス：<管理対象ホストの IP アドレス>
  - ポート番号：<管理対象ホストの SSH ポート番号>
  - ユーザー名：<ログイン時に使用する一般ユーザー名>
  - パスワード：<一般ユーザーのパスワード>
  - su パスワード：空白

管理クライアントを使用した管理対象ホストの設定については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

#### 関連項目

- 4.4.1 ホストを管理対象にするための確認事項 (Linux ホスト)
- 4.4.4 IP 接続を許可する (Linux ホスト)
- 4.4.5 管理対象ホストへのログインの許可とは

## 4.4.9 SNMP トラップを設定する (Linux ホスト)

Linux の管理対象ホストで発生したイベントのトラップを管理サーバで監視するには、管理対象ホストでの設定が必要です。

トラップを送信したい Linux の管理対象ホストにはすべて設定してください。



参考 日立製のサーバ上に作成したホストの場合、SNMP トラップの設定は不要です。

#### 関連項目

- 3.1.3 インバンド SNMP トラップの監視とは
- 3.1.4 インバンド SNMP トラップを監視する
- (3) ポートを変更する

## 4.5 移行する管理対象ホストを探索するための設定を変更する

管理対象ホストを移行する場合に、マザーボードの交換または IP アドレス割り当ての変更に伴って、ホストの探索やホスト情報の更新を実行する必要があります。

すべてのホストの更新情報をホストの探索で確実に取得するため、ホストの移行方法によって探索の設定を変更します。

ホストの移行方法と、対応する探索方法について次に示します。

- マザーボードを交換する場合、または *Compute Systems Manager* の [リソース] タブのホスト一覧に表示される IP アドレスを異なるホストに割り当てる場合  
GUI の [管理] タブから、情報を更新する管理対象ホストに対して、探索対象条件を指定しない ([リソース探索] 画面の詳細設定にある [探索対象条件] で [すべての IP アドレス] を選択) で、ホストの探索を実行します。
- ホストの詳細情報として [IP ネットワーク] タブにだけ表示される IP アドレスを新しいホストに割り当てる場合  
IP アドレスを変更した管理対象ホストの情報を更新したあと、新しいホストに対してホストの探索を実行します。

ホストの探索およびホスト情報の更新については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

#### 関連項目

- 2.5.8 管理対象リソースを登録する

## 4.6 シャーシのマネジメントモジュールの IP アドレスを変更する

シャーシのマネジメントモジュールの IP アドレスを変更した場合は、変更後の IP アドレスを指定してシャーシを再探索してください。

シャーシを探索してシャーシの情報を更新する場合の詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

### 関連項目

- [2.5.8 管理対象リソースを登録する](#)



## セキュリティ設定

この章では、SSL 通信などセキュリティ設定について説明します。

- 5.1 セキュリティの設定とは
- 5.2 管理クライアントとの通信のセキュリティ設定
- 5.3 SMTP サーバとの通信のセキュリティ設定
- 5.4 管理対象サーバとの通信のセキュリティ設定
- 5.5 Device Manager サーバとの通信のセキュリティ設定
- 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは
- 5.7 管理クライアントからの接続を制限する設定
- 5.8 サーバ証明書の有効期限を確認する
- 5.9 トラストストアーにインポートされたサーバ証明書を削除する

## 5.1 セキュリティの設定とは

Compute Systems Manager では、ネットワークの通信で TLS を使用してセキュリティ通信できます。セキュリティ通信を使用すると、通信路が暗号化されるため、情報の漏えいを防げます。また、通信相手を特定するための認証を強化したり、送受信するデータの改ざんを検出したりできます。

Compute Systems Manager では次の通信路でセキュリティ通信を使用できます。

- 管理サーバと管理クライアント間の通信路
- 管理サーバと SMTP サーバ間の通信路
- 管理サーバと管理対象サーバ間の通信路
- 管理サーバと Device Manager サーバ間の通信路
- 管理サーバと外部認証サーバ (LDAP ディレクトリサーバ) 間の通信路

また、特定の管理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よう、アクセス制限を設けることで管理サーバのセキュリティを強化できます。



**重要** セキュリティを有効にして Compute Systems Manager を運用する場合、サーバ証明書の有効期限が切れていないことを確認してください。サーバ証明書の有効期限が切れるとユーザーが Compute Systems Manager に接続できなくなることがあります。この場合、有効期限内の証明書を Compute Systems Manager に登録し直してください。

### 関連項目

- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.3.1 SMTP サーバとの通信のセキュリティ設定とは
- 5.4.1 管理対象サーバとの通信のセキュリティ設定とは
- 5.5.1 Device Manager サーバとの通信のセキュリティ設定とは
- 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは
- 5.7.1 管理クライアントからの接続の制限とは
- 5.8 サーバ証明書の有効期限を確認する

## 5.2 管理クライアントとの通信のセキュリティ設定

### 5.2.1 管理クライアントの通信のセキュリティ設定とは

管理サーバと管理クライアントの通信には、SSL 通信を利用できます。管理サーバと管理クライアント間で SSL 通信する場合、最初に管理サーバで設定したあと、管理クライアントで設定します。

管理クライアントでの SSL 通信の設定は、GUI と CLI で異なります。

### 関連項目

- 5.1 セキュリティの設定とは
- 5.2.2 管理サーバで SSL 通信するよう設定する (管理クライアントとの通信路)
- 5.2.3 管理クライアントで SSL 通信するよう設定する (GUI との通信路)
- 5.2.4 管理クライアントで SSL 通信するよう設定する (CLI との通信路)



## 5.2.2 管理サーバで SSL 通信するよう設定する (管理クライアントとの通信路)

管理サーバと管理クライアント間で SSL 通信するためには、管理サーバで次の手順を実行してください。

Compute Systems Manager では、暗号方式が RSA 暗号および楕円曲線暗号 (ECC) のサーバ証明書に対応しています。



**重要** ほかの Hitachi Command Suite 製品が Compute Systems Manager と同じマシンにインストールされている場合、この手順を実行すると、それらの製品の管理サーバと管理クライアント間の通信にも SSL 通信が適用されます。

### 事前に確認しておく情報

- 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。

次の情報については、使用する認証局に確認してください。

- 証明書発行要求の要件  
hcmds64ssltool コマンドで作成される証明書発行要求は PEM 形式です。秘密鍵のキーサイズは、RSA 暗号用のサーバ証明書の場合は 2,048 ビット、楕円曲線暗号用のサーバ証明書の場合は 256 ビットまたは 384 ビットです。
- 認証局が発行するサーバ証明書の要件  
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。  
また、サーバ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。
- サーバ証明書の発行申請方法

### 事前に完了しておく操作

- 既存の秘密鍵、証明書発行要求、自己署名証明書、および自己署名証明書の内容ファイルの退避または削除 (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、hcmds64ssltool コマンドを実行してもファイルは上書きされません。同じ名称のファイルを再作成する場合は、事前に既存のファイルを退避または削除する必要があります。

管理サーバで SSL 通信するよう設定する手順を次に示します。

- Compute Systems Manager を起動します。
- 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネントの秘密鍵、証明書発行要求、および自己署名証明書を作成します。

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。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%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  
<有効期限>] [/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>]
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/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 <有効期限>] [-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>]

#### key

出力される秘密鍵ファイル名を絶対パスで指定します。指定を省略した場合は、デフォルトの出力先パス※に httpsdkey.pem (RSA 暗号用) および ecc-httpsdkey.pem (楕円曲線暗号用) というファイル名で出力されます。

#### csr

出力される証明書発行要求ファイル名を絶対パスで指定します。指定を省略した場合は、デフォルトの出力先パス※に httpsd.csr (RSA 暗号用) および ecc-httpsd.csr (楕円曲線暗号用) というファイル名で出力されます。

#### cert

出力される自己署名証明書ファイル名を絶対パスで指定します。指定を省略した場合は、デフォルトの出力先パス※に httpsd.pem (RSA 暗号用) および ecc-httpsd.pem (楕円曲線暗号用) というファイル名で出力されます。

#### certtext

出力される自己署名証明書の内容ファイル名を絶対パスで指定します。指定を省略した場合は、デフォルトの出力先パス※に httpsd.txt (RSA 暗号用) および ecc-httpsd.txt (楕円曲線暗号用) というファイル名で出力されます。

#### validity

自己署名証明書の有効期間を日数で指定します。指定を省略した場合は、有効期間は 3650 日になります。

#### 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, SHA1withRSA または MD5withRSA を指定できます。指定を省略した場合は、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は、署名アルゴリズムは SHA384withECDSA になります。

#### ecckeysize

楕円曲線暗号用のサーバ証明書の秘密鍵のキーサイズ (ビット) を指定します。256 または 384 を指定できます。指定を省略した場合は、キーサイズは 384 になります。

コマンドを実行すると、指定した出力先パスに RSA 暗号用のファイルと楕円曲線暗号用のファイルが出力されます。RSA 暗号用のファイルは指定したファイル名で出力され、楕円曲線暗号用のファイルは指定したファイル名の先頭に「ecc-」が追加されて出力されます。

#### 注※

key, csr, cert または certtext オプションの指定を省略した場合の出力先パスは次のとおりです。

Windows :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \%u\CPSB  
\%httpsd%\conf%\ssl%\server

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/  
httpsd/conf/ssl/server

3. コマンド実行後に入力を求められたら、コロン (:) のあとに値を入力します。  
フィールドを空白にしておく場合は、ピリオド (.) を入力します。[]内に示されるデフォルト値を選択する場合は、[Enter] キーを押します。

```
Enter Server Name [default=<管理サーバのホスト名>]:<管理サーバのホスト名>  
Enter Organizational Unit:<組織の構成単位名>  
Enter Organization Name [default=<管理サーバのホスト名>]:<組織名>  
Enter your City or Locality:<市町村名または地域名>  
Enter your State or Province:<都道府県名>  
Enter your two-character country-code:<2文字の国コード>
```

4. 作成した証明書発行要求を認証局に送付し、サーバ証明書の発行を申請します。  
自己署名証明書を使用する場合、この手順は不要です。  
認証局で発行されたサーバ証明書は、通常、Eメールで送付されます。認証局からの返答、および発行されたサーバ証明書は保存しておいてください。
5. Compute Systems Manager を停止します。
6. 作成した秘密鍵と、サーバ証明書または自己署名証明書を次のディレクトリにコピーします。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB  
%httpsd%conf%ssl%server
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/  
httpsd/conf/ssl/server
```



参考 手順 2 で、hcnds64ssltool コマンドの key, csr, または cert オプションを省略して実行した場合、上記のディレクトリにファイルが出力されます。

7. 次に示す user\_httpsd.conf を開きます。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB  
%httpsd%conf%user_httpsd.conf
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/  
httpsd/conf/user_httpsd.conf
```

8. user\_httpsd.conf ファイルの次のプロパティから、#を削除します。
  - #Listen 22016
  - #<VirtualHost \*:22016>から#</VirtualHost>までの各行  
ただし、#SSLCertificateFile の#は削除しません。
  - #HWSLogSSLVerbose On
9. user\_httpsd.conf ファイルの次のプロパティを、必要に応じて編集します。
  - 先頭行の ServerName
  - <VirtualHost>タグ内の ServerName
  - SSLCertificateKeyFile
  - SSLCertificateFile
  - SSLECCertificateKeyFile
  - SSLECCertificateFile

- #SSLCACertificateFile  
チェーンした認証局で発行されたサーバ証明書を使用して運用する場合は、#SSLCACertificateFile の#を削除して、チェーンした認証局の証明書ファイルを絶対パスで指定します。

user\_httpsd.conf の編集例を次に示します。ここでは、デフォルトのポート番号を示しています。

```

ServerName <ホスト名>
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
    ServerName <ホスト名>
    SSLEnable
    SSLProtocol TLSv12
    SSLRequiredCiphers 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 "<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/server/<秘密鍵ファイル (RSA 暗号用)>"
    SSLCertificateFile "<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/server/<サーバ証明書または自己署名証明書ファイル (RSA 暗号用)>"
    SSLECCCertificateKeyFile "<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/server/<秘密鍵ファイル (楕円曲線暗号用)>"
    SSLECCCertificateFile "<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/server/<サーバ証明書または自己署名証明書ファイル (楕円曲線暗号用)>"
    # SSLCACertificateFile "<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/cacert/<認証局の証明書ファイル>"
</VirtualHost>
HWSLogSSLVerbose On

```



#### 重要

- 外部から管理サーバへの非 SSL 通信を遮断したい場合は、user\_httpsd.conf ファイルの「Listen 22015」と「Listen [::]:22015」の行に#を追記してコメント行にしたあと、「#Listen 127.0.0.1:22015」の行から#を削除してください。

この場合に、管理サーバに 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされているときは、これらの製品が提供する hcmdsprmset コマンドに print オプションを指定して実行し、表示されたホスト名から 127.0.0.1 への名前解決ができることを確認してください。

名前解決ができない場合は、OS 上でホスト名から 127.0.0.1 への名前解決ができるようにするか、hosts ファイルで任意のホスト名を 127.0.0.1 に定義したあと、hcmdsprmset コマンドの host オプションにそのホスト名を指定して実行してください。

- バージョン 8.2.1 より前の Compute Systems Manager からアップグレードした場合、楕円曲線暗号用のサーバ証明書を使用するときは、次のプロパティを編集および追加する必要があります。

- SSLRequiredCiphers (編集)
- SSLECCCertificateKeyFile (追加)
- SSLECCCertificateFile (追加)

上記の各プロパティの内容を、次に示すサンプルファイルからコピーして user\_httpsd.conf ファイルに反映してください。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%sample%httpsd
%conf%user_httpsd.conf
```

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/sample/httpsd/  
conf/user\_httpsd.conf

- サーバ証明書は、RSA 暗号用および楕円曲線暗号用の両方を使用することを推奨します。認証局が楕円曲線暗号用のサーバ証明書をサポートしていないなどの理由で、RSA 暗号用のサーバ証明書だけを使用する場合は、user\_httpsd.conf ファイルが次の条件をすべて満たすことを確認してください。
  - SSLRequiredCiphers プロパティに、「ECDHE-ECDSA-」で始まる記述が含まれていないこと。  
RSA 暗号のサーバ証明書だけを使用する場合の SSLRequiredCiphers プロパティの内容を次に示します。

```
SSLRequiredCiphers AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA:DES-CBC3-SHA
```
  - SSLECCertificateKeyFile プロパティ、および SSLECCertificateFile プロパティが記述されていないか、プロパティの行頭に#を追記してコメント行になっていること。

10. Compute Systems Manager を起動します。

11. hcmds64chgurl コマンドを実行して、Compute Systems Manager にアクセスする URL を次のように変更します。

- プロトコルを http: から https: に変更する。
- SSL 通信用のポート番号に変更する。

ほかの Hitachi Command Suite 製品が Compute Systems Manager と同じマシンにインストールされている場合は、それらの製品の URL も変更してください。

管理サーバに秘密鍵と、サーバ証明書または自己署名証明書が登録され、管理サーバの SSL 通信の設定が完了します。

#### 関連項目

- (2) Compute Systems Manager の URL を変更する
- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.2.3 管理クライアントで SSL 通信するよう設定する (GUI との通信路)
- 5.2.4 管理クライアントで SSL 通信するよう設定する (CLI との通信路)
- 5.8 サーバ証明書の有効期限を確認する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する
- B.2.3 Web サーバに関するプロパティ (user\_httpsd.conf)

## 5.2.3 管理クライアントで SSL 通信するよう設定する (GUI との通信路)

管理サーバと SSL 通信するすべての管理クライアント (GUI) で SSL 通信するよう設定する必要があります。管理クライアントで初めて SSL 通信する時だけ設定します。

#### 事前に確認しておく情報

- 署名アルゴリズムに SHA256withRSA を指定して GUI で SSL 通信する場合、使用する OS と Web ブラウザーの組み合わせが SHA256withRSA で署名されたサーバ証明書をサポートしている

#### 事前に完了しておく操作

- 管理サーバでの SSL 通信設定

GUI で SSL 通信するよう設定する手順を次に示します。

1. 管理クライアントから次の URL にアクセスします。  
`https://< Compute Systems Manager をインストールしたホスト名または IP アドレス > : < SSL 通信用のポート番号 > /ComputeSystemsManager/`
2. 管理クライアントに SSL 通信するための証明書をインストールします。

管理クライアントに証明書が登録され、管理サーバと SSL 通信できるようになります。

#### 関連項目

- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.2.2 管理サーバで SSL 通信するよう設定する（管理クライアントとの通信路）
- 5.2.4 管理クライアントで SSL 通信するよう設定する（CLI との通信路）

## 5.2.4 管理クライアントで SSL 通信するよう設定する（CLI との通信路）

管理サーバと SSL 通信するすべての管理クライアント（CLI）で SSL 通信するよう設定する必要があります。

#### 事前に完了しておく操作

- 管理サーバでの SSL 通信設定

CLI で SSL 通信するよう設定する手順を次に示します。

1. 次の場所に格納されている Compute Systems Manager のサーバ証明書を、任意のディレクトリに格納します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB  
%httpsd%conf%ssl%server
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /uCPSB/  
httpsd/conf/ssl/server
```

2. 次のコマンドを使って、Compute Systems Manager のサーバ証明書をトラストストア（cacerts）にインポートします。

Windows :

```
< JRE のインストールディレクトリ > %bin%keytool -importcert -trustcacerts -  
alias <トラストストア内のユニーク名> -file <サーバ証明書ファイル> -  
keystore <JRE のインストールディレクトリ> %lib%security%cacerts -storepass  
changeit
```

Linux :

```
< JRE のインストールディレクトリ > /bin/keytool -importcert -trustcacerts -  
alias <トラストストア内のユニーク名> -file <サーバ証明書ファイル> -keystore  
<JRE のインストールディレクトリ> /lib/security/cacerts -storepass changeit
```

file : 手順 1 で格納した証明書ファイルを指定します。

storepass : 「changeit」はトラストストア（cacerts）の初期パスワードです。パスワード不正でエラーになるときは入手元に確認してください。

3. 次のコマンドを実行します。

Windows :

```
< CLI のインストールディレクトリ > %csm configure
```

Linux :



< CLI インストール先ディレクトリ > /csm configure

4. コマンド実行時の応答に基づき、次の情報を入力します。

HCSM server host name: < Compute Systems Manager が稼働するホスト名 >  
Use SSL: y  
HCSM server port number: < SSL 通信用のポート番号 >

管理クライアントにサーバ証明書が登録され、管理サーバと SSL 通信できるようになります。

#### 関連項目

- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.2.2 管理サーバで SSL 通信するよう設定する（管理クライアントとの通信路）
- 5.2.3 管理クライアントで SSL 通信するよう設定する（GUI との通信路）

## 5.3 SMTP サーバとの通信のセキュリティ設定

### 5.3.1 SMTP サーバとの通信のセキュリティ設定とは

SMTP サーバでサーバ証明書を使用している場合、管理サーバと SMTP サーバの通信に、SSL 通信を利用できます。

管理サーバに SMTP サーバの証明書を登録することで、管理サーバと SMTP サーバの通信に SSL 通信を利用できるようになります。

#### 関連項目

- 5.1 セキュリティの設定とは
- 5.3.2 管理サーバで SSL 通信するよう設定する（SMTP サーバとの通信路）

### 5.3.2 管理サーバで SSL 通信するよう設定する（SMTP サーバとの通信路）

管理サーバと SMTP サーバ間で SSL 通信するためには、管理サーバで次の手順を実行してください。

1. 次のコマンドを実行して、SMTP サーバの証明書を管理サーバに登録します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64keytool -import -alias < トラストストア内のユニーク名 > -file <  
SMTP サーバの証明書ファイル > -keystore < Hitachi Command Suite 共通コンポーネン  
トのインストールディレクトリ > %uCPsB%jdk%jre%lib%security%jssecacerts -  
storepass < トラストストアのパスワード >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPsB/jdk/bin/keytool -import -alias < トラストストア内のユニーク名 > -  
file < SMTP サーバの証明書ファイル > -keystore < Hitachi Command Suite 共通コ  
ンポーネントのインストールディレクトリ > /uCPsB/jdk/jre/lib/security/  
jssecacerts -storepass < トラストストアのパスワード >  
file: PEM 形式または DER 形式の証明書ファイルを指定します。
```

2. Compute Systems Manager を再起動します。
3. Compute Systems Manager にログインして、E メール通知の設定で、SMTP サーバで設定されている SSL 通信用のポート番号を設定します。

E メール通知の設定の詳細については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

管理サーバに SMTP サーバの証明書が登録され、管理サーバの SSL 通信の設定が完了します。

#### 関連項目

- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.3.1 SMTP サーバとの通信のセキュリティ設定とは
- 5.8 サーバ証明書の有効期限を確認する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 5.4 管理対象サーバとの通信のセキュリティ設定

### 5.4.1 管理対象サーバとの通信のセキュリティ設定とは

管理サーバと日立製のサーバ（ブレードサーバ上の HVM も含みます）との通信には、SSL 通信が適用されます。

デフォルトの設定で運用する場合、Compute Systems Manager に同梱されている自己署名証明書で SSL 通信が行われます。セキュリティを確保する場合は、ユーザーがキーストアを作成してサーバ証明書または自己署名証明書を登録する必要があります。

#### 関連項目

- 5.1 セキュリティの設定とは
- 5.4.2 管理サーバで SSL 通信するよう設定する（管理対象サーバとの通信路）

### 5.4.2 管理サーバで SSL 通信するよう設定する（管理対象サーバとの通信路）

日立製のサーバ（ブレードサーバ上の HVM も含みます）との通信でセキュリティを確保する場合は、次の手順を実行して、管理サーバの証明書または自己署名証明書と、日立製のサーバの証明書を管理サーバのキーストアにインポートします。

#### 事前に完了しておく操作

- 日立製のサーバの証明書の取得  
HVM を使用している場合は、HVM の証明書も取得してください。  
証明書の取得方法は、日立製のサーバのマニュアルを参照してください。

次の情報については、使用する認証局に確認してください。

- 証明書発行要求の要件  
hcms64keytool または keytool コマンドで作成される証明書発行要求は PEM 形式で、秘密鍵のキーサイズが 2,048 ビットです。
- 認証局が発行するサーバ証明書の要件  
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。  
また、サーバ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。



- サーバ証明書の発行申請方法

管理サーバと日立製のサーバの間で SSL 通信するためには、管理サーバで次の手順を実行してください。

1. **Compute Systems Manager** を停止します。
2. 次のコマンドを実行して、キーストアーを作成します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin
%hcmds64keytool -genkey -keystore < Compute Systems Manager のインストール
ディレクトリ > %ComputeSystemsManager%conf%ssl% < キーストアーファイル名 > -
storepass < キーストアーのパスワード > -keypass < 秘密鍵のパスワード > -keyalg
RSA -keysize 2048 -sigalg SHA256withRSA -validity < 証明書の有効期限日数 >
-alias < キーストアー内のユニーク名 >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /
uCP5B/jdk/bin/keytool -genkey -keystore < Compute Systems Manager のインス
トールディレクトリ > /ComputeSystemsManager/conf/ssl/< キーストアーファイル名 >
-storepass < キーストアーのパスワード > -keypass < 秘密鍵のパスワード > -keyalg
RSA -keysize 2048 -sigalg SHA256withRSA -validity < 証明書の有効期限日数 >
-alias < キーストアー内のユニーク名 >
```

3. サーバ証明書を使用する場合は、次のコマンドを実行して、証明書発行要求を作成します。  
自己署名証明書を使用する場合、手順 3～手順 6 は不要です。手順 7 に進んでください。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin
%hcmds64keytool -certreq -file < 出力する証明書発行要求ファイル > -keystore <
Compute Systems Manager のインストールディレクトリ > %ComputeSystemsManager
%conf%ssl% < キーストアーファイル名 > -storepass < キーストアーのパスワード > -
keypass < 秘密鍵のパスワード > -alias < キーストアー内のユニーク名 >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /
uCP5B/jdk/bin/keytool -certreq -file < 出力する証明書発行要求ファイル > -
keystore < Compute Systems Manager のインストールディレクトリ > /
ComputeSystemsManager/conf/ssl/< キーストアーファイル名 > -storepass < キー
ストアーのパスワード > -keypass < 秘密鍵のパスワード > -alias < キーストアー内の
ユニーク名 >
```

alias : 手順 2 で指定したエイリアス名を指定します。

4. 作成した証明書発行要求を認証局に送付し、サーバ証明書の発行を申請します。  
認証局で発行されたサーバ証明書は、通常、E メールで送付されます。認証局からの返答、および発行されたサーバ証明書は保存しておいてください。
5. 次のコマンドを実行して、認証局の証明書をキーストアーにインポートします。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin
%hcmds64keytool -import -file < 認証局の証明書ファイル > -keystore < Compute
Systems Manager のインストールディレクトリ > %ComputeSystemsManager%conf%ssl% <
キーストアーファイル名 > -storepass < キーストアーのパスワード > -alias < キースト
アー内のユニーク名 >
```

Linux :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > /  
uCPSB/jdk/bin/keytool -import -file <認証局の証明書ファイル> -keystore <  
*Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/  
conf/ssl/<キーストアーファイル名> -storepass <キーストアーのパスワード> -  
alias <キーストアー内のユニーク名>

alias : 手順 2 で指定した名称以外の任意のエイリアス名を指定します。

6. 次のコマンドを実行して、認証局で発行されたサーバ証明書をキーストアーにインポートします。

Windows :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64keytool -import -file <サーバ証明書ファイル> -keystore < *Compute  
Systems Manager* のインストールディレクトリ > %ComputeSystemsManager%conf%ssl%<  
キーストアーファイル名> -storepass <キーストアーのパスワード> -alias <キースト  
アー内のユニーク名>

Linux :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > /  
uCPSB/jdk/bin/keytool -import -file <サーバ証明書ファイル> -keystore <  
*Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/  
conf/ssl/<キーストアーファイル名> -storepass <キーストアーのパスワード> -  
alias <キーストアー内のユニーク名>

alias : 手順 2 で指定したエイリアス名を指定します。

7. 次のコマンドを実行して、日立製のサーバの証明書をキーストアーにインポートします。

HVM を使用している場合は、HVM の証明書も同様にインポートしてください。

Windows :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64keytool -import -file <日立製のサーバの証明書ファイル> -keystore <  
*Compute Systems Manager* のインストールディレクトリ > %ComputeSystemsManager  
%conf%ssl%<キーストアーファイル名> -storepass <キーストアーのパスワード> -  
alias <キーストアー内のユニーク名>

Linux :

< *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ > /  
uCPSB/jdk/bin/keytool -import -file <日立製のサーバの証明書ファイル> -  
keystore < *Compute Systems Manager* のインストールディレクトリ > /  
ComputeSystemsManager/conf/ssl/<キーストアーファイル名> -storepass <キ  
ーストアーのパスワード> -alias <キーストアー内のユニーク名>

file : PEM 形式または DER 形式の証明書ファイルを指定します。

alias : 手順 2 または手順 5 で指定した名称以外の任意のエイリアス名を指定します。

8. 次の場所に格納されている user.properties を開きます。

Windows :

< *Compute Systems Manager* のインストールディレクトリ > %ComputeSystemsManager  
%conf%user.properties

Linux :

< *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/  
conf/user.properties

9. hcsml.keystore.filename プロパティに、手順 2 で作成したキーストアーファイル名を設定します。

10. hcsml.certification.verify プロパティに Enable を設定します。

hcsml.certification.verify プロパティが設定されていない場合は追記します。

11. LPAR をマイグレーションする際に、管理サーバと HVM との間で暗号化された通信だけを許可したい場合は、`hvm.lpar.migration.allow.plaintext` プロパティに `Disable` を指定します。

`hvm.lpar.migration.allow.plaintext` プロパティが設定されていない場合は追記します。

12. Compute Systems Manager を起動します。
13. Compute Systems Manager にログインし、キーストアおよび秘密鍵のパスワードを設定します。

キーストアおよび秘密鍵のパスワード設定については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。



**参考** 日立製のサーバとの通信で使用する Compute Systems Manager のサーバ証明書をキーストアから取得する場合は、次のコマンドを実行します。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin%hcmds64keytool -exportcert -file <出力する証明書ファイル> -keystore <Compute Systems Manager のインストールディレクトリ>%ComputeSystemsManager%conf%ssl%<キーストアファイル名> -storepass <キーストアのパスワード> -alias <キーストア内のユニーク名>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/jdk/bin/keytool -exportcert -file <出力する証明書ファイル> -keystore <Compute Systems Manager のインストールディレクトリ>/ComputeSystemsManager/conf/ssl/<キーストアファイル名> -storepass <キーストアのパスワード> -alias <キーストア内のユニーク名>
```

alias : 手順 2 で指定したエイリアス名を指定します。

#### 関連項目

- 5.4.1 管理対象サーバとの通信のセキュリティ設定とは
- 5.8 サーバ証明書の有効期限を確認する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

## 5.5 Device Manager サーバとの通信のセキュリティ設定

### 5.5.1 Device Manager サーバとの通信のセキュリティ設定とは

Device Manager サーバでサーバ証明書を使用している場合、管理サーバと Device Manager サーバの通信に SSL 通信を利用できます。

管理サーバに Device Manager サーバの証明書を登録することで、管理サーバと Device Manager サーバの通信に SSL 通信を利用できるようになります。

#### 関連項目

- 5.1 セキュリティの設定とは
- 5.5.2 管理サーバで SSL 通信するよう設定する (Device Manager サーバとの通信路)

## 5.5.2 管理サーバで SSL 通信するよう設定する（Device Manager サーバとの通信路）

管理サーバと Device Manager サーバ間で SSL 通信するためには、管理サーバで次の手順を実行してください。

### 事前に完了しておく操作

- Device Manager サーバの証明書の取得  
証明書の取得方法については、マニュアル「*Hitachi Command Suite システム構成ガイド*」を参照してください。

管理サーバで SSL 通信するよう設定する手順を次に示します。

1. 次のコマンドを実行して、Device Manager サーバの証明書を管理サーバに登録します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64keytool -import -alias <トラストストア内のユニーク名> -file <  
Device Manager サーバの証明書ファイル> -keystore < Hitachi Command  
Suite 共通コンポーネントのインストールディレクトリ > %uCPSE%jdk%jre%lib%security  
%jssecacerts -storepass <トラストストアのパスワード>
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSE/jdk/bin/keytool -import -alias <トラストストア内のユニーク名> -  
file < Device Manager サーバの証明書ファイル > -keystore < Hitachi Command  
Suite 共通コンポーネントのインストールディレクトリ > /uCPSE/jdk/jre/lib/security/  
jssecacerts -storepass <トラストストアのパスワード>  
file : PEM 形式または DER 形式の証明書ファイルを指定します。
```

2. Compute Systems Manager を再起動します。
3. Compute Systems Manager にログインして、[管理] - [論理分割] - [マイグレーション WWPN の自動登録] を選択します。

通信に使用するプロトコルが HTTPS であることを確認します。

マイグレーション WWPN の自動登録については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

管理サーバに Device Manager サーバの証明書が登録され、管理サーバの SSL 通信の設定が完了します。

### 関連項目

- 5.2.1 管理クライアントの通信のセキュリティ設定とは
- 5.5.1 Device Manager サーバとの通信のセキュリティ設定とは
- 5.8 サーバ証明書の有効期限を確認する
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは

管理サーバと LDAP ディレクトリサーバの通信には、StartTLS 通信を利用できます。

管理サーバと LDAP ディレクトリサーバ間の通信を StartTLS で保護するためには次の作業が必要です。

- exauth.properties ファイルの設定
- LDAP ディレクトリサーバの証明書の入手
- トラストストアファイルへの証明書のインポート

#### 関連項目

- 1.6.7 LDAP ディレクトリサーバとの通信のセキュリティ設定の流れ
- 5.1 セキュリティの設定とは
- 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する

## 5.7 管理クライアントからの接続を制限する設定

### 5.7.1 管理クライアントからの接続の制限とは

Compute Systems Manager では、管理サーバに GUI または CLI 経由でアクセスする管理クライアントを制限できます。特定の管理クライアントだけをアクセスできるようにすることで、管理サーバのセキュリティを強化できます。

#### 関連項目

- 5.1 セキュリティの設定とは
- 5.7.2 管理クライアントからの接続を制限する

### 5.7.2 管理クライアントからの接続を制限する

管理クライアントからの接続を制限する手順を次に示します。

1. Compute Systems Manager を停止します。
2. 次の場所に格納されている user\_httpsd.conf ファイルを開きます。  
Windows :  
`<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%uCPSB%httpsd%conf%user_httpsd.conf`  
Linux :  
`<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/user_httpsd.conf`
3. user\_httpsd.conf ファイルの最終行に<Location /ComputeSystemsManager>タグを追加して、管理サーバに接続できる管理クライアントの情報を登録します。
4. Compute Systems Manager を起動します。



**重要** user\_httpsd.conf ファイルに登録していない管理クライアントで、Compute Systems Manager 以外の Hitachi Command Suite 製品にログインしている場合、ログインしている製品の GUI から Compute Systems Manager の GUI は起動できません。

管理サーバに接続できる管理クライアントが制限されるようになります。

#### 関連項目

- 5.7.1 管理クライアントからの接続の制限とは

- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する
- B.2.3 Web サーバに関するプロパティ (user\_httpsd.conf)

## 5.8 サーバ証明書の有効期限を確認する

管理サーバに登録されているサーバ証明書の有効期限を確認します。



**重要** 管理サーバと管理対象サーバ間の通信路で、SSL通信の設定をデフォルトから変更していない場合、有効期限の確認は不要です。

次のコマンドで、サーバ証明書の有効期限を確認できます。

### サーバ証明書ファイルの確認方法

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64keytool -printcert -v -file <サーバ証明書ファイル名>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/  
uCPSE/jdk/bin/keytool -printcert -v -file <サーバ証明書ファイル名>
```

file

サーバ証明書ファイル (X.509 PEM 形式) を指定します。

### キーストアまたはトラストストアファイルの確認方法

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64keytool -list -v -keystore <キーストアまたはトラストストアファイル名>  
> -storepass <キーストアまたはトラストストアのパスワード>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/  
uCPSE/jdk/bin/keytool -list -v -keystore <キーストアまたはトラストストア  
ファイル名> -storepass <キーストアまたはトラストストアのパスワード>
```

keystore

サーバ証明書がインポートされているキーストアまたはトラストストアファイルを指定します。

storepass

キーストアまたはトラストストアファイルにアクセスするためのパスワードを指定します。



**参考** サーバ証明書の有効期限は、上記のコマンドのほかに、OSの機能などを使用して確認することもできます。

サーバ証明書の内容が表示され、有効期限を確認できます。

## 関連項目

- 5.1 セキュリティの設定とは
- 5.2.2 管理サーバで SSL 通信するよう設定する（管理クライアントとの通信路）
- 5.3.2 管理サーバで SSL 通信するよう設定する（SMTP サーバとの通信路）
- 5.4.2 管理サーバで SSL 通信するよう設定する（管理対象サーバとの通信路）
- 5.5.2 管理サーバで SSL 通信するよう設定する（Device Manager サーバとの通信路）
- 5.9 トラストストアにインポートされたサーバ証明書を削除する
- 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する

# 5.9 トラストストアにインポートされたサーバ証明書を削除する

管理サーバのトラストストアにインポートされたサーバ証明書を削除します。

## 事前に確認しておく情報

- 削除するサーバ証明書のエイリアス名  
エイリアス名を確認する方法は、トラストストアファイルに登録されたサーバ証明書の有効期限を確認する方法と同じです。
- トラストストアファイルの格納先
- トラストストアのパスワード

次のコマンドで、サーバ証明書を削除できます。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64keytool -delete -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアのパスワード>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/  
uCPsB/jdk/bin/keytool -delete -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアのパスワード>
```

alias

削除するサーバ証明書のエイリアス名を指定します。

keystore

削除するサーバ証明書がインポートされているトラストストアファイルを指定します。

storepass

トラストストアファイルにアクセスするためのパスワードを指定します。

トラストストアからサーバ証明書が削除されます。

## 関連項目

- 5.8 サーバ証明書の有効期限を確認する





## 外部認証サーバとの連携

この章では、外部認証サーバと連携して認証する方法について説明します。

- 6.1 外部認証サーバとの連携の概要
- 6.2 外部認証サーバと連携するための操作フロー
- 6.3 複数の外部認証サーバと連携している場合の構成
- 6.4 LDAP ディレクトリサーバの構造モデル
- 6.5 LDAP ディレクトリサーバで認証する場合に必要な設定
- 6.6 LDAP ディレクトリサーバとの接続
- 6.7 Kerberos サーバとの接続
- 6.8 LDAP ディレクトリサーバと接続するための設定項目
- 6.9 Kerberos サーバと接続するための設定項目
- 6.10 外部認証サーバと接続するためのコマンド
- 6.11 情報検索用のユーザーアカウントを使用して LDAP ディレクトリサーバに接続する
- 6.12 LDAP ディレクトリサーバの証明書のインポート

## 6.1 外部認証サーバとの連携の概要

### 6.1.1 外部認証サーバとの連携とは

Hitachi Command Suite 製品では、外部認証サーバに登録されたユーザー ID を使って、ログインできます。

外部認証サーバに登録されているユーザー ID を Compute Systems Manager に登録しておくことで、外部認証サーバに登録されたユーザー ID を使って、Compute Systems Manager にログインできます。このため、Compute Systems Manager 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。

Compute Systems Manager 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
- Kerberos サーバ



**重要** 外部認証サーバと直接接続したり、DNS サーバに接続先の外部認証サーバを照会したりできます。外部認証サーバと直接接続する場合は、外部認証サーバと StartTLS 通信できます。DNS サーバに接続先の外部認証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。

#### 関連項目

- 1.6.8 外部認証サーバとの連携の流れ
- 6.1.2 外部認可サーバとの連携とは
- 6.3 複数の外部認証サーバと連携している場合の構成
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.7.2 Kerberos サーバと接続するよう設定する

### 6.1.2 外部認可サーバとの連携とは

外部認証サーバと外部認可サーバを併用することで、Compute Systems Manager に対するユーザーのアクセス権限を外部認可サーバで制御できます。

外部認可サーバとも連携する場合、Compute Systems Manager 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、Compute Systems Manager 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。

Compute Systems Manager 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。

#### 関連項目

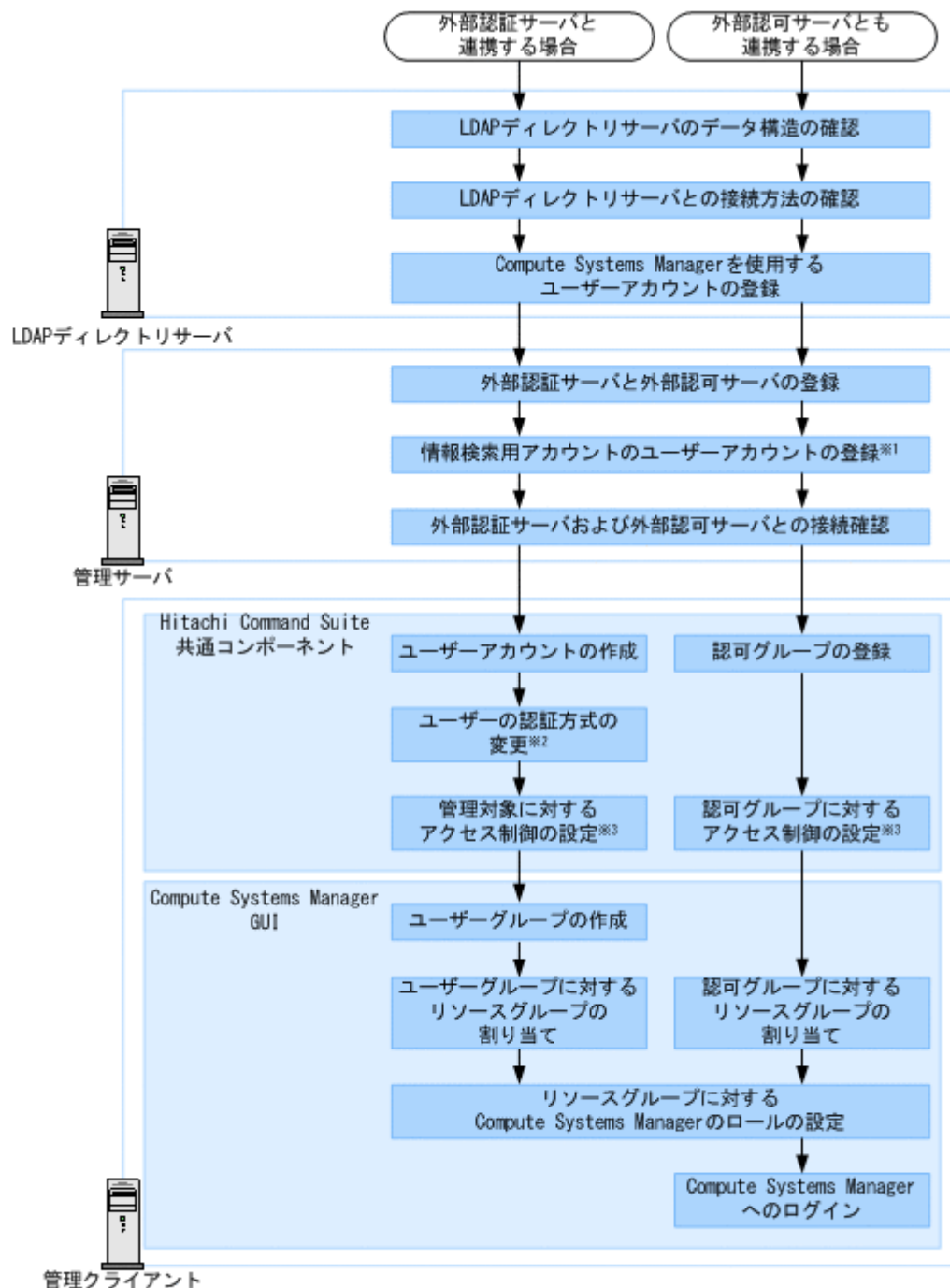
- 6.1.1 外部認証サーバとの連携とは
- 6.2.1 LDAP ディレクトリサーバと連携するための操作フロー
- 6.2.2 Kerberos サーバと連携するための操作フロー
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.7.2 Kerberos サーバと接続するよう設定する

## 6.2 外部認証サーバと連携するための操作フロー

### 6.2.1 LDAP ディレクトリサーバと連携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、Compute Systems Manager 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が必要です。

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を次に示します。



注※1 フラットモデルで外部認証サーバとだけ連携する場合、この操作は不要です。

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。



重要

- 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は同一サーバである必要があります。

- Compute Systems Manager 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、Compute Systems Manager 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 にドメイン名が含まれている場合（例：user1@example.com）も同様に、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 Compute Systems Manager にログインした際には、Hitachi Command Suite 共通コンポーネントで認証（内部認証）されます。
  - 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 Compute Systems Manager 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。
  - 外部認可サーバと連携している場合、外部認可サーバ側で認可グループにユーザーアカウントを登録したとき、またはユーザーの情報（所属する認可グループ、メールアドレス）を変更したときは、Compute Systems Manager にその情報を反映させるために、対象のユーザーは Compute Systems Manager にログインする必要があります。
- 

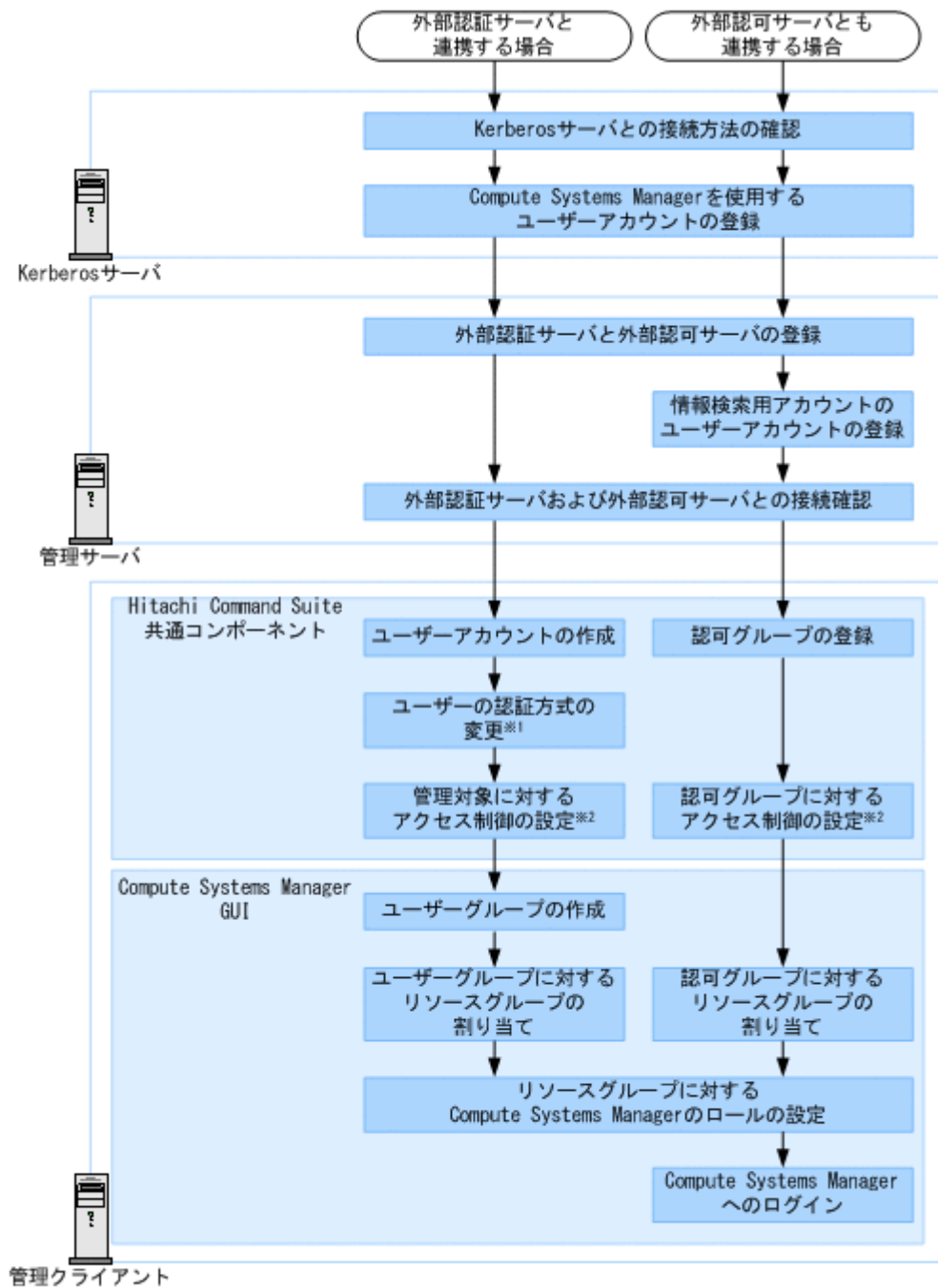
#### 関連項目

- [6.1.1 外部認証サーバとの連携とは](#)
- [6.1.2 外部認可サーバとの連携とは](#)
- [6.6.1 LDAP ディレクトリサーバと接続するよう設定する](#)
- [6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する](#)

## 6.2.2 Kerberos サーバと連携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、Compute Systems Manager 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。

Kerberos サーバでユーザー認証するための操作フローを次に示します。



注※1 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※2 ユーザーの作業範囲に応じて操作権限を設定します。



**重要**

- 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は同一サーバである必要があります。
- Compute Systems Manager 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、Compute Systems Manager 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 にレルム名が含まれている場合（例：user1@EXAMPLE.COM）も同様に、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 Compute Systems Manager にログインした際には、Hitachi Command Suite 共通コンポーネントで認証（内部認証）されます。
- 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 Compute Systems Manager を操作できるようになります。
- LDAP ディレクトリサーバ（外部認可サーバ）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。

- 外部認可サーバと連携している場合、外部認可サーバ側で認可グループにユーザーアカウントを登録したとき、またはユーザーの情報（所属する認可グループ、メールアドレス）を変更したときは、Compute Systems Manager にその情報を反映させるために、対象のユーザーは Compute Systems Manager にログインする必要があります。

#### 関連項目

- 6.1.1 外部認証サーバとの連携とは
- 6.1.2 外部認可サーバとの連携とは
- 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する
- 6.7.2 Kerberos サーバと接続するよう設定する

## 6.3 複数の外部認証サーバと連携している場合の構成

複数の外部認証サーバと連携している場合、冗長構成またはマルチドメイン構成でユーザー認証します。

それぞれの外部認証サーバで同一のユーザー情報を管理する構成を、冗長構成と呼びます。ある外部認証サーバに障害が発生しても、ほかの外部認証サーバでユーザー認証できます。

それぞれの外部認証サーバでドメイン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。

Compute Systems Manager がサポートする外部認証サーバの構成を次に示します。

外部認証サーバ	冗長構成	マルチドメイン構成
LDAP ディレクトリサーバ	○※1	○※1
Kerberos サーバ	○	○※2

(凡例)

○ : サポートしている

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。

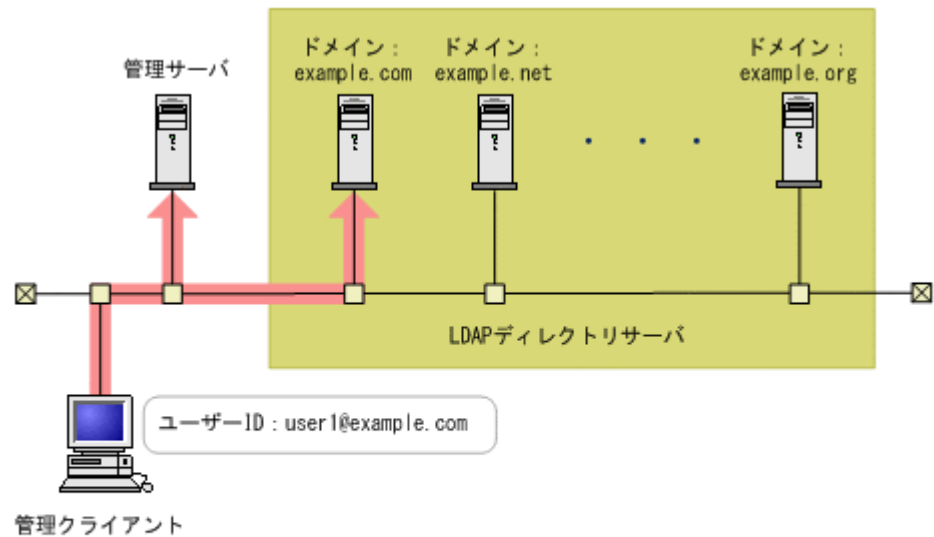
注※2


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。

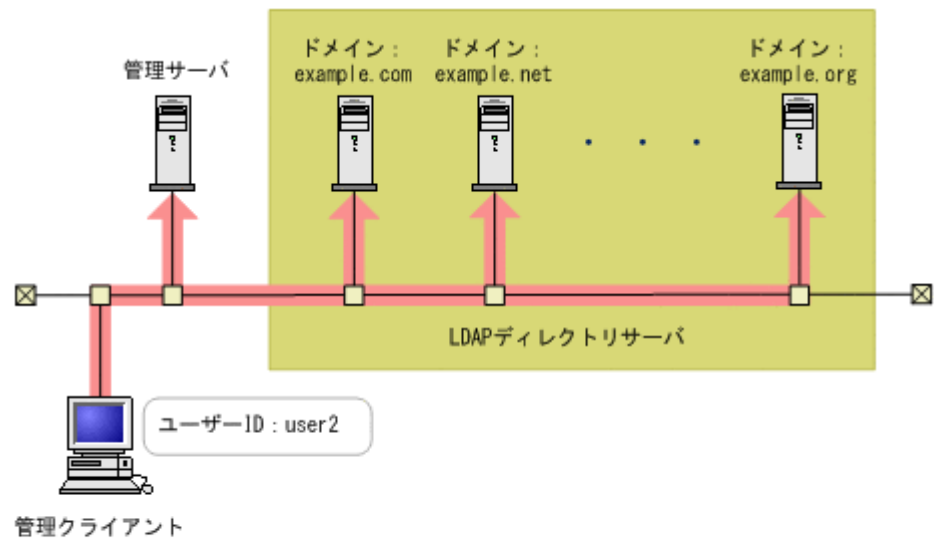
図 6-1 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいるユーザー ID の場合）




(凡例)  
 : ユーザー認証の処理

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推奨します。

図 6-2 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいないユーザー ID の場合）



(凡例)  
 : ユーザー認証の処理

**関連項目**

- ・ 6.1.1 外部認証サーバとの連携とは

## 6.4 LDAP ディレクトリサーバの構造モデル

### 6.4.1 BaseDN とは

BaseDN は、LDAP ディレクトリサーバを使用した認証の際にユーザーを検索する起点となるエンタリーです。

BaseDN は、Compute Systems Manager の管理サーバの `exauth.properties` ファイルのプロパティで設定します。

BaseDN より下の階層のユーザーエンタリーが認証の対象となります。Compute Systems Manager で認証したいユーザーをすべて含むエンタリーであることが必要です。

#### 関連項目

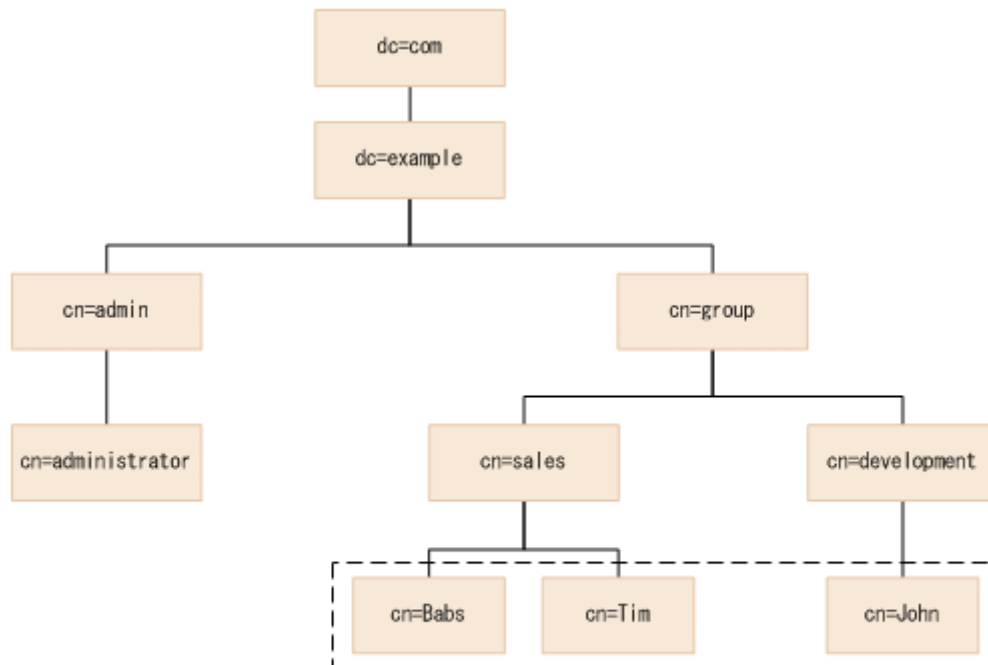
- 6.4.2 階層構造モデルとは
- 6.4.3 フラットモデルとは
- 6.5.1 LDAP ディレクトリサーバを接続するための前提条件

### 6.4.2 階層構造モデルとは

LDAP ディレクトリサーバを使用する前に、LDAP ディレクトリサーバのデータ構造を決定し、認証方式に合うよう設定する必要があります。

LDAP ディレクトリサーバが提供しているデータ構造の 1 つとして、階層構造モデルがあります。階層構造モデルは、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タリーが登録されているデータ構造です。この場合、BaseDN より下のエンタリーを対象に、ログイン ID とユーザー属性値が等しいエンタ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。



(凡例)          : 認証対象のユーザーエンタリー



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。

上記の例では、対象のユーザーエントリーが「cn=sales」および「cn=development」のエントリーにわたって属しているため、BaseDNは「cn=group,dc=example,dc=com」となります。

#### 関連項目

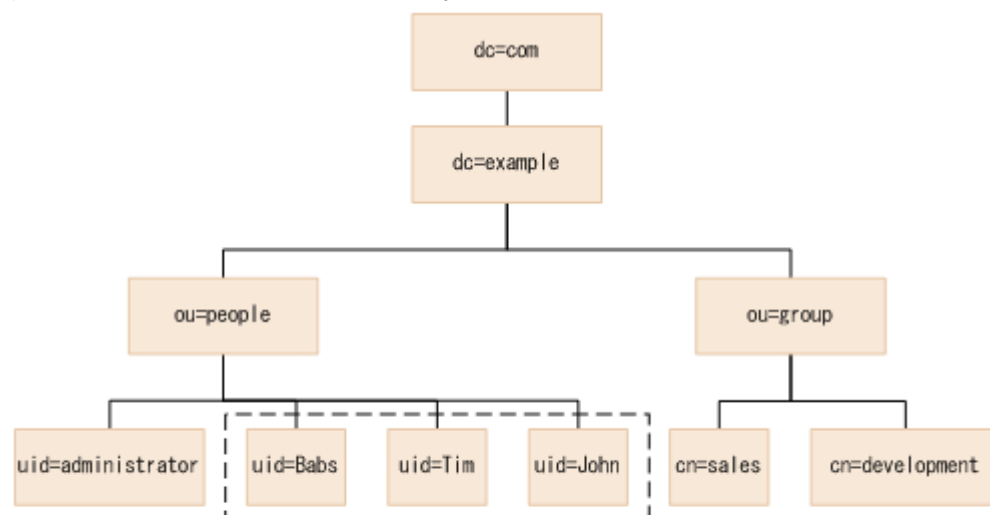
- 6.4.1 BaseDN とは
- 6.4.3 フラットモデルとは
- 6.5.1 LDAP ディレクトリサーバを接続するための前提条件

### 6.4.3 フラットモデルとは

LDAP ディレクトリサーバを使用する前に、LDAP ディレクトリサーバのデータ構造を決定し、認証方式に合うよう設定する必要があります。

LDAP ディレクトリサーバが提供しているデータ構造の1つとして、フラットモデルがあります。フラットモデルは、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です。この場合、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。



(凡例)  : 認証対象のユーザーエントリー

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ため、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、階層構造モデルとして設定してください。

- Compute Systems Manager 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、Compute Systems Manager 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 Compute Systems Manager のユーザー ID として使用します。そのため、Compute Systems Manager 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、フラットモデルで認証できません。使用できる RDN の例を次に示します。

```
uid=John123S
```

```
cn=John_Smith
```

使用できない RDN の例を次に示します。

```
uid=John:123S (コロン (:)) が使用されている)
```

```
cn=John Smith (半角スペースが使用されている)
```

#### 関連項目

- 6.4.1 BaseDN とは
- 6.4.2 階層構造モデルとは
- 6.5.1 LDAP ディレクトリサーバを接続するための前提条件

## 6.5 LDAP ディレクトリサーバで認証する場合に必要な設定

### 6.5.1 LDAP ディレクトリサーバを接続するための前提条件

Compute Systems Manager のログイン情報を、LDAP ディレクトリサーバで認証させる場合、LDAP ディレクトリサーバの次の情報を決定する必要があります。

- LDAP ディレクトリサーバのデータ構造  
LDAP ディレクトリサーバでは、次のどちらかのデータ構造が使用できます。
  - 階層構造モデル
  - フラットモデル
- BaseDN  
認証の際にユーザーを検索する起点となるエントリーです。

#### 関連項目

- 6.4.1 BaseDN とは
- 6.4.2 階層構造モデルとは
- 6.4.3 フラットモデルとは
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する

### 6.5.2 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の条件

LDAP ディレクトリサーバの情報を保持する DNS サーバに、LDAP ディレクトリサーバへの接続情報を照会する場合、次の操作を完了している必要があります。

- LDAP ディレクトリサーバの OS で、DNS サーバの環境設定が完了している
- DNS サーバの SRV レコードに、LDAP ディレクトリサーバのホスト名、ポート番号、ドメイン名など登録済みである



**重要** 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、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。

#### 関連項目

- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.8.2 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき)
- 6.8.4 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき)

## 6.6 LDAP ディレクトリサーバとの接続

### 6.6.1 LDAP ディレクトリサーバと接続するよう設定する

LDAP ディレクトリサーバと接続するためには、事前作業が必要です。必要な情報を確認したあと、LDAP ディレクトリサーバの情報を基に管理サーバで接続情報を設定したり、管理クライアントでユーザーアカウントの作成やアクセス制御の設定をしたりします。

#### 事前に確認しておく情報

- LDAP ディレクトリサーバのデータ構造  
階層構造モデルか、フラットモデルかによって、プロパティの設定が変わります。
- LDAP ディレクトリサーバとの接続方法  
LDAP ディレクトリサーバの情報を直接指定するか、DNS サーバに接続先の LDAP ディレクトリサーバの情報を照会するかによって、設定するプロパティが異なります。
- 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 (外部認可サーバとも連携する場合)
- 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 (外部認証サーバがマルチドメイン構成の場合)

#### 事前に完了しておく操作

- **Compute Systems Manager** で使用するための LDAP ディレクトリサーバでのユーザーアカウント登録  
登録されていない場合は、使用する LDAP ディレクトリサーバのマニュアルに従って、ユーザーアカウントを登録します。  
ユーザーアカウント登録時には次の内容に注意してください。
  - ユーザー ID およびパスワードは、**Compute Systems Manager** で使用できる次の文字で構成されている  
`A~Z a~z 0~9 ! # $ % & ' ( ) * + - . = @ ¥ ^ _ |`
  - 1 バイト以上 256 バイト以内の文字である
  - **Compute Systems Manager** では、ユーザー ID の大文字と小文字の違いが区別されない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。

LDAP ディレクトリサーバと接続するための設定手順を次に示します。

1. `exauth.properties` ファイルで、LDAP ディレクトリサーバと接続するよう設定します。

- 階層構造モデルの場合、またはフラットモデルでかつ外部認可サーバとも連携する場合は、`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登録します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64ldapuser /set /dn <情報検索用ユーザーの DN > [/pass <情報検索用ユーザーのパスワード>] /name <サーバ識別名 >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64ldapuser -set -dn <情報検索用ユーザーの DN > [-pass <情報検索用ユーザーのパスワード>] -name <サーバ識別名 >
```

フラットモデルで外部認証サーバとだけ連携する場合は、認証時にユーザー情報の検索が実行されないため、この作業は不要です。すでに登録されている場合は、情報検索用のユーザーアカウントを削除してください。

- `hcmds64checkauth` コマンドを実行して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64checkauth [/user <ユーザー ID >] [/pass <パスワード>] [/summary]
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64checkauth [-user <ユーザー ID >] [-pass <パスワード>] [-summary]
```

`user` または `pass` オプションを省略した場合は、ユーザー ID、パスワードの応答入力を求められます。メッセージの指示に従い入力してください。

- 外部認証サーバとだけ連携する場合は、管理クライアントで次の項目を設定します。

- ユーザーアカウントの作成
- ユーザーの認証方式の変更
- 管理対象に対するアクセス制御の設定
- ユーザーグループの作成
- ユーザーグループに対するリソースグループの割り当て
- リソースグループに対する **Compute Systems Manager** のロールの設定

管理クライアントでの設定方法については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

- 外部認可サーバとも連携する場合は、管理クライアントで次の項目を設定します。

- 認可グループの登録
- 認可グループに対するアクセス制御の設定
- 認可グループ (ユーザーグループ) に対するリソースグループの割り当て
- リソースグループに対する **Compute Systems Manager** のロールの設定

管理クライアントでの設定方法については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

- 外部認可サーバとも連携する場合は、LDAP ディレクトリサーバに登録したユーザーアカウントで、**Compute Systems Manager** にログインします。



**重要** 外部認可サーバに登録したユーザーアカウントの情報を **Compute Systems Manager** に反映させるために、ログインする必要があります。

---

外部認証サーバとして LDAP ディレクトリサーバと管理サーバが接続できるようになります。

## 関連項目

- 6.1.1 外部認証サーバとの連携とは
- 6.1.2 外部認可サーバとの連携とは
- 6.3 複数の外部認証サーバと連携している場合の構成
- 6.5.1 LDAP ディレクトリサーバを接続するための前提条件
- 6.5.2 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の条件
- 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する
- 6.8.1 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する場合で、外部認証サーバとだけ連携するとき)
- 6.8.2 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき)
- 6.8.3 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する場合で、外部認可サーバとも連携するとき)
- 6.8.4 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき)
- 6.10.1 外部認証サーバとの連携設定で使用するコマンドに関する注意事項
- 6.10.2 外部認証サーバとの接続を確認するコマンド (hcmds64checkauth) の書式
- 6.11.1 情報検索用のユーザーアカウントの条件
- 6.11.2 情報検索用のユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式
- 6.11.4 管理サーバから情報検索用のユーザーアカウントを削除する

## 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する

外部認証サーバとして LDAP ディレクトリサーバと管理サーバの接続を設定したあとで、StartTLS 通信するよう設定できます。

### 事前に完了しておく操作

- LDAP ディレクトリサーバとの接続設定

次の手順で、LDAP ディレクトリサーバと管理サーバ間の StartTLS 通信を設定します。

1. 管理サーバの exauth.properties ファイルで、次のプロパティを編集します。
  - auth.ocsp.enable (任意)
  - auth.ocsp.responderURL (任意)
  - auth.ldap.ServerName.protocol (必須)
2. exauth.properties ファイルの auth.ocsp.enable プロパティまたは auth.ocsp.responderURL プロパティを変更した場合には、Compute Systems Manager を再起動します。
3. 次のコマンドを実行して、証明書が Hitachi Command Suite 共通コンポーネントで利用するトラストストアに設定済みか確認します。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin%  
%hcmds64keytool -list -v -keystore <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%uCPSE%jdk%jre%lib%security%cacerts -storepass <トラストストアへのアクセスパスワード>
```

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSEB/jdk/bin/keytool -list -v -keystore < Hitachi Command Suite 共通コン  
ポーネントのインストールディレクトリ > /uCPSEB/jdk/jre/lib/security/cacerts -  
storepass < トラストストアへのアクセスパスワード >  
storepass : デフォルトのパスワードは「changeit」です。  
すでにトラストストアに設定されている場合は、以降の手順は不要です。

- LDAP ディレクトリサーバのサーバ証明書入手します。  
入手方法は、利用する LDAP ディレクトリサーバのマニュアルを参照してください。
- 入手した LDAP ディレクトリサーバの証明書が、Hitachi Command Suite 共通コンポーネント  
で利用するトラストストアにインポートする証明書の条件と合致することを確認します。
- 次のコマンドを実行して、証明書を Hitachi Command Suite 共通コンポーネントで利用するト  
ラストストアにインポートします。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64keytool -import -alias < トラストストア内のユニーク名 > -file < 証  
明書ファイル > -keystore < トラストストアファイル名 > -storepass < トラスト  
ストアへのアクセスパスワード >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSEB/jdk/bin/keytool -import -alias < トラストストア内のユニーク名 > -  
file < 証明書ファイル > -keystore < トラストストアファイル名 > -storepass <  
トラストストアへのアクセスパスワード >
```

証明書ファイルが複数ある場合は、トラストストア内で使用されていない任意のエイリアス名  
を指定して、インポートしてください。

- インポートしたトラストストアの内容を確認します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64keytool -list -v -keystore < トラストストアファイル名 > -storepass  
< トラストストアへのアクセスパスワード >
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSEB/jdk/bin/keytool -list -v -keystore < トラストストアファイル名 > -  
storepass < トラストストアへのアクセスパスワード >
```

- Compute Systems Manager を再起動します。

LDAP ディレクトリサーバと管理サーバが、StartTLS 通信で接続できるようになります。

## 関連項目

- 5.8 サーバ証明書の有効期限を確認する
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.8.1 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する  
場合で、外部認証サーバとだけ連携するとき)
- 6.8.2 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会  
する場合で、外部認証サーバとだけ連携するとき)
- 6.8.3 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する  
場合で、外部認可サーバとも連携するとき)

- 6.8.4 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認証サーバとも連携するとき)
- 6.10.2 外部認証サーバとの接続を確認するコマンド (`hcmds64checkauth`) の書式
- 6.12.1 LDAP ディレクトリサーバの証明書の条件
- 6.12.3 LDAP ディレクトリサーバの証明書をインポートするコマンド (`hcmds64keytool` または `keytool`) の書式

## 6.7 Kerberos サーバとの接続

### 6.7.1 Kerberos 認証に使用できる暗号タイプ

Hitachi 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 サーバを構築する必要があります。

Hitachi Command Suite 製品で、Kerberos 認証に使用できる暗号タイプ (encryption types) は次のとおりです。

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

#### 関連項目

- 6.9.1 `exauth.properties` ファイルの設定項目 (Kerberos サーバの情報を直接指定する場合で、外部認証サーバとだけ連携するとき)
- 6.9.2 `exauth.properties` ファイルの設定項目 (Kerberos サーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき)

### 6.7.2 Kerberos サーバと接続するよう設定する

Kerberos サーバと接続するためには、事前作業が必要です。必要な情報を確認したあと、Kerberos サーバの情報を基に管理サーバで接続情報を設定したり、管理クライアントでユーザーアカウントの作成やアクセス制御の設定をしたりします。

#### 事前に確認しておく情報

- Kerberos サーバとの接続方法  
Kerberos サーバの情報を直接指定するか、DNS サーバに接続先の Kerberos サーバの情報を照会するかによって、設定するプロパティが異なります。

#### 事前に完了しておく操作

- Compute Systems Manager で使用するための Kerberos サーバでのユーザーアカウント登録  
登録されていない場合は、使用する Kerberos サーバのマニュアルに従って、ユーザーアカウントを登録します。  
ユーザーアカウント登録時には次の内容に注意してください。



- ユーザー ID およびパスワードは、**Compute Systems Manager** で使用できる次の文字で構成されている  
A～Z a～z 0～9 ! # \$ % & ' ( ) \* + - . = @ ¥ ^ \_ |
- 1 バイト以上 256 バイト以内の文字である
- **Compute Systems Manager** では、ユーザー ID の大文字と小文字の違いが区別されない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。

**Kerberos** サーバと接続するための設定手順を次に示します。

1. `exauth.properties` ファイルで、**Kerberos** サーバと接続するよう設定します。
2. 外部認可サーバとも連携する場合は、`hcms64ldapuser` 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登録します。

**Windows :**

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin
¥hcms64ldapuser /set /dn <情報検索用ユーザーの DN > [/pass <情報検索用ユーザーのパスワード>] /name <サーバ識別名 >
```

**Linux :**

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
hcms64ldapuser -set -dn <情報検索用ユーザーの DN > [-pass <情報検索用ユーザーのパスワード>] -name <サーバ識別名 >
```

外部認証サーバとだけ連携する場合は、認証時にユーザー情報の検索が実行されないため、この作業は不要です。すでに登録されている場合は、情報検索用のユーザーアカウントを削除してください。

3. `hcms64checkauth` コマンドを実行して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

**Windows :**

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin
¥hcms64checkauth [/user <ユーザー ID >] [/pass <パスワード>] [/summary]
```

**Linux :**

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
hcms64checkauth [-user <ユーザー ID >] [-pass <パスワード>] [-summary]
```

`user` または `pass` オプションを省略した場合は、ユーザー ID、パスワードの応答入力を求められます。メッセージの指示に従い入力してください。

4. 外部認証サーバとだけ連携する場合は、管理クライアントで次の項目を設定します。

- ユーザーアカウントの作成
- ユーザーの認証方式の変更
- 管理対象に対するアクセス制御の設定
- ユーザーグループの作成
- ユーザーグループに対するリソースグループの割り当て
- リソースグループに対する **Compute Systems Manager** のロールの設定

管理クライアントでの設定方法については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。

5. 外部認可サーバとも連携する場合は、管理クライアントで次の項目を設定します。

- 認可グループの登録
- 認可グループに対するアクセス制御の設定
- 認可グループ (ユーザーグループ) に対するリソースグループの割り当て



- 。 リソースグループに対する Compute Systems Manager のロールの設定  
管理クライアントでの設定方法については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。
6. 外部認可サーバとも連携する場合は、Kerberos サーバに登録したユーザーアカウントで、Compute Systems Manager にログインします。



**重要** 外部認可サーバに登録したユーザーアカウントの情報を Compute Systems Manager に反映させるために、ログインする必要があります。

外部認証サーバとして Kerberos サーバと管理サーバが接続できるようになります。

### 関連項目

- ・ 6.1.1 外部認証サーバとの連携とは
- ・ 6.1.2 外部認可サーバとの連携とは
- ・ 6.3 複数の外部認証サーバと連携している場合の構成
- ・ 6.5.1 LDAP ディレクトリサーバを接続するための前提条件
- ・ 6.5.2 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の条件
- ・ 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する
- ・ 6.9.1 `exauth.properties` ファイルの設定項目 (Kerberos 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)
- ・ 6.9.2 `exauth.properties` ファイルの設定項目 (Kerberos 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)
- ・ 6.9.3 `exauth.properties` ファイルの設定項目 (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)
- ・ 6.9.4 `exauth.properties` ファイルの設定項目 (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)
- ・ 6.10.1 外部認証サーバとの連携設定で使用するコマンドに関する注意事項
- ・ 6.10.2 外部認証サーバとの接続を確認するコマンド (`hcmds64checkauth`) の書式
- ・ 6.11.1 情報検索用のユーザーアカウントの条件
- ・ 6.11.2 情報検索用のユーザーアカウントを登録するコマンド (`hcmds64ldapuser`) の書式
- ・ 6.11.4 管理サーバから情報検索用のユーザーアカウントを削除する

## 6.8 LDAP ディレクトリサーバと接続するための設定項目

### 6.8.1 `exauth.properties` ファイルの設定項目 (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)

`exauth.properties` ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
<code>auth.server.type</code>	<code>ldap</code>
<code>auth.server.name</code>	LDAP ディレクトリサーバのサーバ識別名
<code>auth.ldap.multi_domain</code> <sup>※1</sup>	<code>true</code> (マルチドメイン構成の場合) <code>false</code> (冗長構成の場合)

プロパティ名	設定値
auth.group.mapping	false
auth.ocsp.enable	false※2
auth.ocsp.responderURL	(空白) ※2
auth.ldap.< auth.server.name の指定値 >.protocol	ldap※3
auth.ldap.< auth.server.name の指定値 >.host	LDAP ディレクトリサーバのホスト名または IP アドレス
auth.ldap.< auth.server.name の指定値 >.port	LDAP ディレクトリサーバのポート番号
auth.ldap.< auth.server.name の指定値 >.timeout	LDAP ディレクトリサーバとの接続待ち時間
auth.ldap.< auth.server.name の指定値 >.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
auth.ldap.< auth.server.name の指定値 >.basedn	DN (BaseDN)
auth.ldap.< auth.server.name の指定値 >.retry.interval	LDAP ディレクトリサーバとの通信失敗時のリトライ間隔
auth.ldap.< auth.server.name の指定値 >.retry.times	LDAP ディレクトリサーバとの通信失敗時のリトライ回数
auth.ldap.< auth.server.name の指定値 >.domain※4	マルチドメイン構成のドメイン名
auth.ldap.< auth.server.name の指定値 >.dns_lookup	false

注※1

接続先の LDAP ディレクトリサーバがマルチドメイン構成または冗長構成の場合に指定しません。

注※2

StartTLS 通信する場合は、必要に応じて設定を変更します。

注※3

StartTLS 通信する場合は、tls に変更します。

注※4

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に指定します。

**関連項目**

- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)
- B.2.14 LDAP ディレクトリサーバとの連携に関するプロパティの設定例

## 6.8.2 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	ldap
auth.server.name	LDAP ディレクトリサーバのサーバ識別名
auth.group.mapping	false
auth.ldap.< auth.server.name の指定値 >.protocol	ldap
auth.ldap.< auth.server.name の指定値 >.timeout	LDAP ディレクトリサーバとの接続待ち時間
auth.ldap.< auth.server.name の指定値 >.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
auth.ldap.< auth.server.name の指定値 >.basedn	DN (BaseDN)
auth.ldap.< auth.server.name の指定値 >.retry.interval	LDAP ディレクトリサーバとの通信失敗時のリトライ間隔
auth.ldap.< auth.server.name の指定値 >.retry.times	LDAP ディレクトリサーバとの通信失敗時のリトライ回数
auth.ldap.< auth.server.name の指定値 >.domain.name	ドメイン名
auth.ldap.< auth.server.name の指定値 >.dns_lookup	true

#### 関連項目

- 6.5.2 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の条件
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)
- B.2.14 LDAP ディレクトリサーバとの連携に関するプロパティの設定例

### 6.8.3 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する場合で、外部認可サーバとも連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	ldap
auth.server.name	LDAP ディレクトリサーバのサーバ識別名
auth.ldap.multi_domain <sup>※1</sup>	true (マルチドメイン構成の場合) false (冗長構成の場合)
auth.group.mapping	true
auth.ocsp.enable	false <sup>※2</sup>
auth.ocsp.responderURL	(空白) <sup>※2</sup>
auth.ldap.< auth.server.name の指定値 >.protocol	ldap <sup>※3</sup>
auth.ldap.< auth.server.name の指定値 >.host	LDAP ディレクトリサーバのホスト名または IP アドレス
auth.ldap.< auth.server.name の指定値 >.port	LDAP ディレクトリサーバのポート番号

プロパティ名	設定値
auth.ldap.< auth.server.name の指定値 >.timeout	LDAP ディレクトリサーバとの接続待ち時間
auth.ldap.< auth.server.name の指定値 >.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
auth.ldap.< auth.server.name の指定値 >.basedn	DN (BaseDN)
auth.ldap.< auth.server.name の指定値 >.retry.interval	LDAP ディレクトリサーバとの通信失敗時のリトライ間隔
auth.ldap.< auth.server.name の指定値 >.retry.times	LDAP ディレクトリサーバとの通信失敗時のリトライ回数
auth.ldap.< auth.server.name の指定値 >.domain.name	外部認可サーバのドメイン名
auth.ldap.< auth.server.name の指定値 >.domain <sup>※4</sup>	マルチドメイン構成のドメイン名
auth.ldap.< auth.server.name の指定値 >.dns_lookup	false

注※1

接続先の LDAP ディレクトリサーバがマルチドメイン構成または冗長構成の場合に指定します。

注※2

StartTLS 通信する場合は、必要に応じて設定を変更します。

注※3

StartTLS 通信する場合は、tls に変更します。

注※4

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に指定します。

**関連項目**

- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)
- B.2.14 LDAP ディレクトリサーバとの連携に関するプロパティの設定例

## 6.8.4 exauth.properties ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	ldap
auth.server.name	LDAP ディレクトリサーバのサーバ識別名
auth.group.mapping	true
auth.ldap.< auth.server.name の指定値 >.protocol	ldap

プロパティ名	設定値
auth.ldap.< auth.server.name の指定値 >.timeout	LDAP ディレクトリサーバとの接続待ち時間
auth.ldap.< auth.server.name の指定値 >.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
auth.ldap.< auth.server.name の指定値 >.basedn	DN (BaseDN)
auth.ldap.< auth.server.name の指定値 >.retry.interval	LDAP ディレクトリサーバとの通信失敗時のリトライ間隔
auth.ldap.< auth.server.name の指定値 >.retry.times	LDAP ディレクトリサーバとの通信失敗時のリトライ回数
auth.ldap.< auth.server.name の指定値 >.domain.name	ドメイン名
auth.ldap.< auth.server.name の指定値 >.dns_lookup	true

#### 関連項目

- ・ 6.5.2 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の条件
- ・ 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- ・ B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)
- ・ B.2.14 LDAP ディレクトリサーバとの連携に関するプロパティの設定例

## 6.9 Kerberos サーバと接続するための設定項目

### 6.9.1 exauth.properties ファイルの設定項目 (Kerberos サーバの情報を直接指定する場合で、外部認証サーバとだけ連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	kerberos
auth.group.mapping	false
auth.ocsp.enable	false※
auth.ocsp.responderURL	(空白) ※
auth.kerberos.default_realm	レルム名
auth.kerberos.dns_lookup_kdc	false
auth.kerberos.default_tkt_encypes	Kerberos 認証に使用する暗号タイプ
auth.kerberos.clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲
auth.kerberos.timeout	Kerberos サーバと接続するときの接続待ち時間
auth.kerberos.realm_name	レルム識別名
auth.kerberos.< auth.kerberos.realm_name の指定値 >.realm	レルム名
auth.kerberos.< auth.kerberos.realm_name の指定値 >.kdc	<ホスト名または IP アドレス>[:<ポート番号>]

注※

StartTLS 通信する場合は、必要に応じて設定を変更します。

#### 関連項目

- 6.7.1 Kerberos 認証に使用できる暗号タイプ
- 6.7.2 Kerberos サーバと接続するよう設定する
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)
- B.2.16 Kerberos サーバとの連携に関するプロパティの設定例

## 6.9.2 exauth.properties ファイルの設定項目 (Kerberos サーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	kerberos
auth.group.mapping	false
auth.kerberos.default_realm	レルム名
auth.kerberos.dns_lookup_kdc	true
auth.kerberos.default_tkt_enctypes	Kerberos 認証に使用する暗号タイプ
auth.kerberos.clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲
auth.kerberos.timeout	Kerberos サーバと接続するときの接続待ち時間

#### 関連項目

- 6.7.1 Kerberos 認証に使用できる暗号タイプ
- 6.7.2 Kerberos サーバと接続するよう設定する
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)
- B.2.16 Kerberos サーバとの連携に関するプロパティの設定例

## 6.9.3 exauth.properties ファイルの設定項目 (Kerberos サーバの情報を直接指定する場合で、外部認可サーバとも連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	kerberos
auth.group.mapping	true
auth.ocsp.enable	false <sup>※1</sup>
auth.ocsp.responderURL	(空白) <sup>※1</sup>
auth.kerberos.default_realm	レルム名
auth.kerberos.dns_lookup_kdc	false

プロパティ名	設定値
auth.kerberos.clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲
auth.kerberos.timeout	Kerberos サーバと接続するときの接続待ち時間
auth.kerberos.realm_name	レルム識別名
auth.kerberos.<auth.kerberos.realm_nameの指定値>.realm	レルム名
auth.kerberos.<auth.kerberos.realm_nameの指定値>.kdc	<ホスト名または IP アドレス>[:<ポート番号>]
auth.group.<レルム名>.protocol	ldap※2
auth.group.<レルム名>.port	Kerberos サーバのポート番号
auth.group.<レルム名>.basedn	DN (BaseDN)
auth.group.<レルム名>.timeout	LDAP ディレクトリサーバとの接続待ち時間
auth.group.<レルム名>.retry.interval	LDAP ディレクトリサーバとの通信失敗時のリトライ間隔
auth.group.<レルム名>.retry.times	LDAP ディレクトリサーバとの通信失敗時のリトライ回数

注※1

StartTLS 通信する場合は、必要に応じて設定を変更します。

注※2

StartTLS 通信する場合は、「tls」に変更します。

関連項目

- 6.7.2 Kerberos サーバと接続するよう設定する
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)
- B.2.16 Kerberos サーバとの連携に関するプロパティの設定例

## 6.9.4 exauth.properties ファイルの設定項目 (Kerberos サーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき)

exauth.properties ファイルを編集します。編集するプロパティとその設定値を次の表に示します。

プロパティ名	設定値
auth.server.type	kerberos
auth.group.mapping	true
auth.kerberos.default_realm	レルム名
auth.kerberos.dns_lookup_kdc	true
auth.kerberos.clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲
auth.kerberos.timeout	Kerberos サーバと接続するときの接続待ち時間

関連項目

- 6.7.2 Kerberos サーバと接続するよう設定する
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)

## 6.10 外部認証サーバと接続するためのコマンド

### 6.10.1 外部認証サーバとの連携設定で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コマンドを実行する場合、コマンドの引数を指定する規則に従っている必要があります。

コマンドラインの引数に制御文字が含まれる場合は、次の規則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。

Windows の場合 :

次の文字が引数に含まれる場合、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。

半角スペース & | ^ < > ( )

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。

Linux の場合 :

次の文字が引数に含まれる場合は、引数を引用符 (") で囲むか、1文字ごとに円記号 (¥) でエスケープしてください。

半角スペース # & ' ( ) ~ ¥ ` < > ; |

ただし、円記号 (¥) は、引用符 (") で囲われていてもエスケープ文字として扱われます。引数に円記号 (¥) が含まれる場合には、必ず円記号 (¥) でエスケープしてください。

#### 関連項目

- ・ 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- ・ 6.10.2 外部認証サーバとの接続を確認するコマンド (hcmds64checkauth) の書式

### 6.10.2 外部認証サーバとの接続を確認するコマンド (hcmds64checkauth) の書式

管理サーバと、外部認証サーバまたは外部認可サーバが接続できているかを確認するコマンド (hcmds64checkauth) の書式を次に示します。

#### 書式

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \bin  
¥hcmds64checkauth [/user <ユーザー ID >] [/pass <パスワード >] [/summary]
```



Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/  
hcmds64checkauth [-user <ユーザー ID >] [-pass <パスワード>] [-summary]
```

## オプション

user および pass

接続を確認する外部認証サーバまたは外部認可サーバに登録されているユーザーアカウントのユーザー ID およびパスワードを指定します。<ユーザー ID >および<パスワード>の先頭に、Windows の場合はスラント (/)、Linux の場合はハイフン (-) を指定できません。

- 認証方式が LDAP の場合

<ユーザー ID >に、exauth.properties ファイルの auth.ldap.<auth.server.name の指定値>.attr の値を指定してください。

- 認証方式が Kerberos の場合

外部認証サーバとだけ連携するときは、Hitachi Command Suite 製品に登録されていて、かつ認証方式が Kerberos のユーザーアカウントを指定してください。

外部認可サーバとも連携するときは、Hitachi Command Suite 製品に登録されていないユーザーアカウントを指定してください。

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。

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、レルムごとに接続できるかを確認してください。この場合、接続を確認するユーザーアカウントがデフォルトのレルム (exauth.properties ファイルの auth.kerberos.default\_realm プロパティで指定した値) に所属しているかどうかで、<ユーザー ID >の指定方法が異なります。

- デフォルトのレルムと異なるレルムに所属するユーザーアカウントを指定する場合  
「<ユーザー ID >@<レルム名>」の形式で指定してください。
- デフォルトのレルムに所属するユーザーアカウントを指定する場合  
レルム名を省略して<ユーザー ID >を指定できます。

summary

summary オプションを指定すると、コマンド実行時に表示される確認メッセージが簡略化されます。

user または pass オプションを省略した場合は、ユーザー ID またはパスワードの応答入力を求められます。メッセージの指示に従い入力してください。

hcmds64checkauth コマンドを実行すると、次の 4 フェーズに分けてチェックされ、結果が表示されます。

- ・ フェーズ 1 : exauth.properties ファイルの共通のプロパティが正しく設定されているか
- ・ 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
- ・ フェーズ 3 : 外部認証サーバに接続できるか

- ・ 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

#### 関連項目

- ・ 6.8.1 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する場合で、外部認証サーバとだけ連携するとき)
- ・ 6.8.2 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認証サーバとだけ連携するとき)
- ・ 6.8.3 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバの情報を直接指定する場合で、外部認可サーバとも連携するとき)
- ・ 6.8.4 `exauth.properties` ファイルの設定項目 (LDAP ディレクトリサーバを DNS サーバに照会する場合で、外部認可サーバとも連携するとき)
- ・ 6.10.1 外部認証サーバとの連携設定で使用するコマンドに関する注意事項

## 6.11 情報検索用のユーザーアカウントを使用して LDAP ディレクトリサーバに接続する

### 6.11.1 情報検索用のユーザーアカウントの条件

LDAP ディレクトリサーバの接続を設定するためには、LDAP 情報の検索のためのユーザーアカウントを LDAP ディレクトリサーバに用意しておく必要があります。

ユーザーアカウントの条件を示します。条件に記載している「DN」は、認証方式によって指定するプロパティが異なります。

認証方式が LDAP の場合

```
exauth.properties ファイルの auth.ldap.<auth.server.nameの指定値>.  
>.basedn で指定した DN
```

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
```

LDAP 情報を検索するためのユーザーアカウントは、次の条件をすべて満たしている必要があります。

- ・ DN にバインドできる
- ・ DN に参照できる
- ・ 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
- ・ DN 下にある認可グループを参照できる (外部認可サーバとも連携するとき)
- ・ 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 (外部認可サーバとも連携するとき)



**重要** 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、管理サーバに登録するユーザーアカウントの DN およびパスワードには引用符 (") を使用しないでください。



**参考** Active Directory を使用している場合、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。

ユーザーを「administrator」とした場合、次のコマンドを実行して DN を確認します。

```
dsquery user -name administrator
```

---

## 関連項目

- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.11.2 情報検索用のユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式
- 6.11.3 管理サーバで情報検索用のユーザーアカウントの登録状況を確認する
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)

## 6.11.2 情報検索用のユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式

LDAP ディレクトリサーバのユーザー情報を検索するためのユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式を次に示します。

### 書式

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64ldapuser /set /dn <情報検索用ユーザーの DN> [/pass <情報検索用ユーザー  
のパスワード>] /name <サーバ識別名>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64ldapuser -set -dn <情報検索用ユーザーの DN> [-pass <情報検索用ユーザー  
のパスワード>] -name <サーバ識別名>
```

### オプション

dn

情報検索用ユーザーの DN を指定します。RFC4514 の規約に従って指定してください。

pass

情報検索用ユーザーのパスワードを指定します。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。

name

認証方式によって指定内容が異なります。

- 認証方式が LDAP の場合 : LDAP ディレクトリサーバのサーバ識別名、またはドメイン名 exauth.properties ファイルの auth.server.name プロパティの値、または auth.ldap.< auth.server.name の指定値>.domain.name プロパティの値を指定します。
- 認証方式が Kerberos の場合 : Kerberos サーバのレルム名  
Kerberos サーバの情報を直接指定するよう設定した場合は、auth.kerberos.default\_realm の値、または auth.kerberos.< auth.kerberos.realm\_name の指定値>.realm の値を指定します。  
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。

データ構造が階層構造モデルで、情報検索用のユーザーアカウント (BaseDN 以下のすべてのユーザーの属性を検索する権限を持つ) を「administrator」、administrator の DN を

「cn=administrator,cn=admin,dc=example,dc=com」、administrator のパスワードを「administrator\_pass」とした場合のコマンドの実行例を、次に示します。

Windows :

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example,dc=com" /  
pass administrator_pass /name < auth.server.name の指定値 >
```

Linux :

```
hcmds64ldapuser -set -dn "cn=administrator,cn=admin,dc=example,dc=com" -  
pass administrator_pass -name < auth.server.name の指定値 >
```

また、DN に「cn=administrator,cn=admin,dc=example,com」のように、コンマ (,) が含まれる場合は、次のように指定します。

Windows :

```
hcmds64ldapuser /set /dn "cn=administrator,cn=admin,dc=example¥,com" /  
pass administrator_pass /name < auth.server.name の指定値 >
```

Linux :

```
hcmds64ldapuser -set -dn "cn=administrator,cn=admin,dc=example¥¥,com" -  
pass administrator_pass -name < auth.server.name の指定値 >
```

#### 関連項目

- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.11.1 情報検索用のユーザーアカウントの条件
- 6.11.3 管理サーバで情報検索用のユーザーアカウントの登録状況を確認する
- 6.11.4 管理サーバから情報検索用のユーザーアカウントを削除する
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)

## 6.11.3 管理サーバで情報検索用のユーザーアカウントの登録状況を確認する

管理サーバに登録されている、LDAP ディレクトリサーバの情報検索用ユーザーアカウントを確認する場合は、次のコマンドを実行します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin  
¥hcmds64ldapuser /list
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64ldapuser -list
```

#### 関連項目

- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- 6.11.1 情報検索用のユーザーアカウントの条件
- 6.11.2 情報検索用のユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式

- ・ 6.11.4 管理サーバから情報検索用のユーザーアカウントを削除する

## 6.11.4 管理サーバから情報検索用のユーザーアカウントを削除する

管理サーバから情報検索用のユーザーアカウントを削除するには、次のコマンドを実行します。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64ldapuser /delete /name <サーバ識別名>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64ldapuser -delete -name <サーバ識別名>
```

### 関連項目

- ・ 6.11.2 情報検索用のユーザーアカウントを登録するコマンド (hcmds64ldapuser) の書式

## 6.12 LDAP ディレクトリサーバの証明書のインポート

### 6.12.1 LDAP ディレクトリサーバの証明書の条件

管理サーバと LDAP ディレクトリサーバ間をセキュリティ通信する場合には、入手した LDAP ディレクトリサーバのサーバ証明書が特定の条件を満たしている必要があります。

LDAP ディレクトリサーバのサーバ証明書の CN (Subject 欄の CS) が、exauth.properties ファイルの次のプロパティに値が設定されていることを確認してください。

- ・ 認証方式が LDAP の場合  
auth.ldap.< auth.server.name の指定値 >.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 の指定値 >.kdc

### 関連項目

- ・ 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- ・ 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する

### 6.12.2 LDAP ディレクトリサーバの証明書をインポートする場合の注意事項

LDAP ディレクトリサーバの証明書を管理サーバにインポートする場合、次の規則に従うようにしてください。

- ・ トラストストア cacerts は、Hitachi Command Suite 共通コンポーネントをバージョンアップすると更新されるため、cacerts に独自の証明書をインポートして運用しないでください。
- ・ hcmds64keytool コマンド (Windows の場合) または keytool コマンド (Linux の場合) で、トラストストア内のユニーク名、トラストストアのファイル名、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。

- ファイル名は 255 バイト以内の文字列にしてください。
- ファイル名には次の記号を使用しないでください。  
: , ; \* ? " < > |
- トラストストア内のユニーク名、およびパスワードには引用符 (") を含めないでください。

#### 関連項目

- 6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する
- 6.12.1 LDAP ディレクトリサーバの証明書の条件
- 6.12.3 LDAP ディレクトリサーバの証明書をインポートするコマンド (hcmds64keytool または keytool) の書式

## 6.12.3 LDAP ディレクトリサーバの証明書をインポートするコマンド (hcmds64keytool または keytool) の書式

セキュリティ通信するため、LDAP ディレクトリサーバの証明書を管理サーバにインポートするコマンド (hcmds64keytool または keytool) の書式を説明します。

#### 書式

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin
%hcmds64keytool -import -alias <トラストストア内のユニーク名> -file <証明書ファイル> -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/
uCPSB/jdk/bin/keytool -import -alias <トラストストア内のユニーク名> -file
<証明書ファイル> -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

#### オプション

alias

トラストストア内で証明書を識別するための名称を指定します。

file

証明書ファイルを指定します。

keystore

LDAP ディレクトリサーバの証明書をインポートするために作成するトラストストアファイル名、または既存のトラストストアファイル名を指定します。

次のどちらかを指定してください。

- Hitachi Command Suite 製品以外と証明書を共有しない場合 :

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%conf
%sec%ldapcerts
```

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
conf/sec/ldapcacerts

- Hitachi Command Suite 製品以外と証明書を共有する場合：

Windows :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > \u005CuCPSB  
\jdk\jre\lib\security\jssecacerts

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSB/jdk/jre/lib/security/jssecacerts

セキュリティリスクを低減するために、LDAP ディレクトリサーバの証明書は ldapcacerts  
ファイルを指定することを推奨します。Hitachi Command Suite 製品以外と証明書を共有す  
る場合は、jssecacerts ファイルを指定します。

#### 関連項目

- [6.6.2 LDAP ディレクトリサーバと StartTLS 通信するよう設定する](#)
- [6.12.1 LDAP ディレクトリサーバの証明書の条件](#)
- [6.12.2 LDAP ディレクトリサーバの証明書をインポートする場合の注意事項](#)





## デプロイメントマネージャーの環境設定

この章では、デプロイメントマネージャーの前提ソフトウェアおよびデプロイメントマネージャーのインストール手順、デプロイメントマネージャーで使用されるポートおよび管理対象リソースの設定などについて説明します。

- 7.1 デプロイメントマネージャーの環境設定とは
- 7.2 デプロイメントマネージャーをインストールするための前提条件
- 7.3 IIS をインストールする
- 7.4 .NET Framework をインストールする（デプロイメントマネージャーを使用する場合）
- 7.5 デプロイメントマネージャーをインストールする
- 7.6 デプロイメントマネージャーを運用するための前提条件
- 7.7 管理対象リソースのポートの設定を変更する
- 7.8 デプロイメントマネージャーが使用するポート番号を変更する
- 7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル

## 7.1 デプロイメントマネージャーの環境設定とは

デプロイメントマネージャーは、ディスクの障害や破損が発生した場合に、管理対象リソースのディスクデータを過去の状態に戻したり、同じ環境の管理対象リソースを複数構築したりする機能です。

デプロイメントマネージャーは、管理サーバの OS が Windows の場合に運用できます。

デプロイメントマネージャーを環境設定するには、管理サーバに IIS、および .NET Framework をインストールしたあとに、Compute Systems Manager のインストールウィザードからデプロイメントマネージャーをインストールします。

必要に応じて、デプロイメントマネージャーが使用するポートを変更します。また、管理対象リソースのブートの設定を変更します。

すでにデプロイメントマネージャーがインストールされている場合、Compute Systems Manager のインストールウィザードからデプロイメントマネージャーをアップグレードインストール、上書きインストール、およびアンインストールできます。

### 関連項目

- 2.2.2 システム要件を確認する
- 7.5 デプロイメントマネージャーをインストールする
- 7.6 デプロイメントマネージャーを運用するための前提条件
- 7.7 管理対象リソースのブートの設定を変更する
- 7.8 デプロイメントマネージャーが使用するポート番号を変更する

## 7.2 デプロイメントマネージャーをインストールするための前提条件

デプロイメントマネージャーをインストールするための前提条件を次に示します。

- 管理サーバがネットワークに接続されている  
ネットワークに接続されていない場合、デプロイメントマネージャーのインストールに失敗します。
- 管理サーバに次の前提ソフトウェアがインストールされている
  - IIS 7.5 以降
  - .NET Framework 3.5 SP1 または 3.5.1
  - .NET Framework 4.5.2, 4.6.0 または 4.6.1
- デプロイメントマネージャーが使用するポートが、ほかの製品で使用されているポートと競合していない  
デプロイメントマネージャーが使用するポートには変更できないものがあり、そのポートがほかの製品によって使用されている場合は、デプロイメントマネージャーとその製品が正常に動作しなくなるおそれがあります。
- 異なる言語対応の SQL Server が混在していない  
デプロイメントマネージャーをインストールすると、SQL Server が自動でインストールされます。このとき、異なる言語対応の SQL Server がインストールされていると、デプロイメントマネージャーのインストールに失敗します。



注意 デプロイメントマネージャー以外で使用している SQL Server のインスタンスをアンインストールする場合は、DPMDBI インスタンスを削除しないでください。

#### 関連項目

- 2.2.3 ポート番号が競合していないことを確認する
- 7.1 デプロイメントマネージャーの環境設定とは
- 7.3 IIS をインストールする
- 7.4 .NET Framework をインストールする (デプロイメントマネージャーを使用する場合)
- 7.5 デプロイメントマネージャーをインストールする
- A.1 Compute Systems Manager サーバで使用されるポート
- A.3 デプロイメントマネージャーで使用されるポート

## 7.3 IIS をインストールする

デプロイメントマネージャーをインストールする前に、IIS をインストールします。

#### 事前に確認しておく情報

- 管理サーバに IIS 7.5 以降がインストールされているかどうか

IIS をインストールする手順を次に示します。

1. OS に添付されている IIS をインストールします。このとき、用途に応じた役割サービスを有効にする必要があります。

IIS のバージョンに応じて、次に示す役割サービスを指定してインストールしてください。

IIS 7.x の場合

- 静的なコンテンツ
- ASP.NET
- IIS 6 メタベース互換
- IIS 管理コンソール

IIS 8.0 以降の場合

- 静的なコンテンツ
- ASP.NET 4.5
- IIS 6 メタベース互換
- IIS 管理コンソール

2. IIS 7.x の場合、IIS の既定の Web サイトを設定します。

- a. 既定の Web サイトがなければ新規に作成します。
- b. 既定の Web サイトへ HTTP 通信でループバックアドレス 127.0.0.1 からアクセスできるよう設定します。既定の Web サイトのポート番号は、デプロイメントマネージャーと通信する場合に使用されます。

#### 関連項目

- 7.1 デプロイメントマネージャーの環境設定とは
- 7.2 デプロイメントマネージャーをインストールするための前提条件

## 7.4 .NET Framework をインストールする（デプロイメントマネージャーを使用する場合）

デプロイメントマネージャーをインストールする前に、.NET Framework をインストールします。

### 事前に確認しておく情報

- 管理サーバに次の.NET Framework がインストールされているかどうか
  - .NET Framework 3.5 SP1 または 3.5.1
  - .NET Framework 4.5.2, 4.6.0 または 4.6.1

### 事前に完了しておく操作

- 前提となる IIS のインストール

.NET Framework をインストールする手順を次に示します。

- .NET Framework 3.5 SP1 または 3.5.1 がインストールされていない場合、次の手順でインストールします。

#### Windows Server 2008 R2 の場合

Windows の [サーバーマネージャー] - [機能] - [機能の追加] を選択します。ウィザードに従って、追加する機能として [.NET Framework 3.5.1 の機能] を選択します。

#### Windows Server 2012 の場合

Windows の [サーバーマネージャー] - [管理] - [役割と機能の追加] を選択します。ウィザードに従って、.NET Framework をインストールするサーバを選択し、追加する機能として [.NET Framework 3.5 Features] を選択します。

- .NET Framework 4.5.2, 4.6.0, または 4.6.1 がインストールされていない場合、次のコマンドを実行してインストールします。

```
< Compute Systems Manager のインストールメディア > %HCSM_SERVER%\HCSM\%DPMEDIA  
%dotNet Framework452%\NDP452-KB2901907-x86-x64-AllOS-ENU.exe
```

```
< Compute Systems Manager のインストールメディア > %HCSM_SERVER%\HCSM\%DPMEDIA  
%dotNet Framework452%\ja%\NDP452-KB2901907-x86-x64-AllOS-JPN.exe
```



**参考** このコマンドを実行すると、.NET Framework 4.5.2 が管理サーバにインストールされます。.NET Framework 4.6.0 または 4.6.1 を使用する場合は、コマンドを実行する代わりに、Microsoft のホームページから .NET Framework をダウンロードしてインストールしてください。

### 関連項目

- [7.1 デプロイメントマネージャーの環境設定とは](#)
- [7.2 デプロイメントマネージャーをインストールするための前提条件](#)
- [7.3 IIS をインストールする](#)

## 7.5 デプロイメントマネージャーをインストールする

### 事前に完了しておく操作

- 前提ソフトウェアのインストール

デプロイメントマネージャーをインストールする手順を次に示します。

1. **Compute Systems Manager** のインストールウィザードで、デプロイメントマネージャーのインストールを選択します。すでにデプロイメントマネージャーがインストールされている場合は、アンインストールが選択できます。
2. インストールウィザードの指示に従って、それぞれの画面で必要な情報を指定します。
3. [インストール完了] 画面で、[完了] ボタンをクリックします。

デプロイメントマネージャーが IIS との内部通信に使用するポート番号は、デプロイメントマネージャーをインストールしたあと、[管理] タブからデプロイメントマネージャーの設定を選択して変更できます。



#### 重要

- デプロイメントマネージャーのインストール中に OS の再起動を要求されることがあります。OS を再起動した場合は、再度 **Compute Systems Manager** のインストールウィザードからインストールしてください。
- デプロイメントマネージャーを上書きインストール、アップグレードインストール、およびアンインストールするには、新規インストールしたときのユーザーでログインする必要があります。デプロイメントマネージャーを新規インストールしたときにログインしたユーザー名を控えておいてください。



**参考**すでに **Compute Systems Manager** がインストールされている場合、デプロイメントマネージャーをインストールすると、**Compute Systems Manager** は上書きインストールされます。

#### 関連項目

- [7.1 デプロイメントマネージャーの環境設定とは](#)
- [7.2 デプロイメントマネージャーをインストールするための前提条件](#)
- [7.3 IIS をインストールする](#)
- [7.4 .NET Framework をインストールする \(デプロイメントマネージャーを使用する場合\)](#)
- [7.8 デプロイメントマネージャーが使用するポート番号を変更する](#)

## 7.6 デプロイメントマネージャーを運用するための前提条件

デプロイメントマネージャーを運用するための前提条件を次に示します。

- 管理対象リソースがシステム要件を満たしている
- 複製元と複製先の管理対象リソースはハードウェアのモデルが同じである  
ハードウェア条件については、該当するリソースのドキュメントを参照してください。
- 管理対象リソースの環境を複製する場合、LAN の二重化が解除されている  
ただし、**bonding** ドライバーまたは **hbonding** ドライバーによって LAN が二重化されている場合は、デプロイメントマネージャーを運用できません。
- DHCP サーバの構築状態が次の条件を満たしている
  - DHCP サーバを管理サーバに構築する場合：同一ネットワーク内に DHCP サーバは 1 つだけである
  - DHCP サーバを管理サーバ以外に構築する場合：DHCP サーバが同一ネットワーク内に構築されている  
この場合は、複数の DHCP サーバを構築できます。

## 関連項目

- ・ 7.1 デプロイメントマネージャーの環境設定とは

## 7.7 管理対象リソースのブートの設定を変更する

デプロイメントマネージャーを使用して管理サーバから管理対象リソースを操作するには、管理対象リソースのブートの設定を変更する必要があります。

### 事前に確認しておく情報

- ・ デプロイメントマネージャーを運用するための前提条件を満たしている

管理サーバから管理対象リソースを PXE ブート（ネットワークブート）するために、管理対象リソースの BIOS の起動順位の設定を次のように変更します。

- ・ ハードディスクドライブよりネットワークを上位に設定してください。
- ・ LAN ボードが複数ある場合は、デプロイメントマネージャーで管理する LAN ボードをハードディスクドライブより上位に設定し、それ以外の LAN ボードは PXE ブートの設定を無効にしてください。

無効にできない場合はハードディスクドライブより下位に設定してください。

## 関連項目

- ・ 7.1 デプロイメントマネージャーの環境設定とは
- ・ 7.6 デプロイメントマネージャーを運用するための前提条件

## 7.8 デプロイメントマネージャーが使用するポート番号を変更する

デプロイメントマネージャーが使用するポートがほかの製品が使用するポートと競合している場合は、デプロイメントマネージャーが使用するポートを変更する必要があります。

ただし、デプロイメントマネージャーで使用するポートには変更できないものがあります。

### 事前に確認しておく情報

- ・ デプロイメントマネージャーがインストールされている

デプロイメントマネージャーが使用するポート番号を変更する手順を次に示します。

変更するポート番号によって、手順が次のとおり異なります。

#### IIS との内部通信で使用されるポート番号（デフォルト 80/tcp）を変更する場合

1. IIS の設定で、既定の Web サイトのポート番号を変更します。
2. Compute Systems Manager にログインし、[管理] タブから [デプロイメント] - [設定] を選択します。
3. 手順 1 で設定したポート番号と同じ値に変更します。

#### 上記以外のポート番号を変更する場合

1. Compute Systems Manager を停止します。

2. プロパティファイルを編集し、デプロイメントマネージャーが使用するポート番号を変更します。
3. Compute Systems Manager を起動します。

#### 関連項目

- 2.2.3 ポート番号が競合していないことを確認する
- 7.1 デプロイメントマネージャーの環境設定とは
- 7.5 デプロイメントマネージャーをインストールする
- 7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル
- 8.1.2 Compute Systems Manager を起動する
- 8.1.3 Compute Systems Manager を停止する

## 7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル

ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイルについて説明します。

表 7-1 ポート変更時の編集箇所 (Port.ini)

デフォルトのポート番号	プロパティファイルの格納パス	プロパティ
26501/tcp または 56020/tcp	< Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager ¥DeploymentManager¥PXE¥Images¥Port.ini	BackupRestoreUnicast
26502/tcp または 56022/tcp		BOOTNIC
26503/tcp または 56030/tcp		FSC
26508/tcp または 56023/tcp		FTUnicast
26504/tcp		ReceiveClientInfo
26505/tcp		DHCPless
26506/tcp		AUUpdate
26507/tcp		ReceiveClientResult

表 7-2 ポート変更時の編集箇所 (MgrServerList.xml)

デフォルトのポート番号	設定ファイルの格納パス	編集箇所	編集例
26500/tcp	< Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager ¥DeploymentManager¥WebServer¥App_Data ¥Config¥MgrServerList.xml	<Port><変更するポート番号></Port>	<Port>26500</Port>

#### 関連項目

- 7.1 デプロイメントマネージャーの環境設定とは
- 7.8 デプロイメントマネージャーが使用するポート番号を変更する
- A.3 デプロイメントマネージャーで使用されるポート
- B.3 デプロイメントマネージャーで使用されるポートに関するプロパティ (Port.ini)





## 管理サーバの運用

この章では、Compute Systems Manager の起動と停止、データベースの管理など、管理サーバの運用について説明します。

- [8.1 Compute Systems Manager の起動と停止](#)
- [8.2 データベースの管理](#)

# 8.1 Compute Systems Manager の起動と停止

## 8.1.1 Compute Systems Manager の起動と停止とは

Compute Systems Manager がインストールされているマシンの OS を起動すると、Compute Systems Manager は自動で起動されます。このとき、ほかの Hitachi Command Suite 製品も起動されます。

Compute Systems Manager の設定を変更するときは、ユーザーが手動で Compute Systems Manager を起動または停止します。

### 関連項目

- [8.1.2 Compute Systems Manager を起動する](#)
- [8.1.3 Compute Systems Manager を停止する](#)
- [8.1.4 Compute Systems Manager の常駐プロセス](#)
- [8.1.5 Compute Systems Manager の稼働状況を確認する](#)

## 8.1.2 Compute Systems Manager を起動する

Compute Systems Manager は次の方法で起動できます。

Windows :

次のどちらかの方法で起動します。

- Windows のメニューから起動する。
  - Windows Server 2008 R2 の場合 :  
[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Compute Systems Manager] - [Start - HCSM] を選択します。
  - Windows Server 2012 の場合 :  
[スタート] - [すべてのアプリ] - [Hitachi Command Suite] - [Compute Systems Manager] - [Start - HCSM] を選択します。
- コマンドを実行して起動する。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin  
%hcmds64srv /start

Linux :

次のコマンドを実行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/  
hcmds64srv -start
```

Compute Systems Manager が起動します。同じマシンにインストールされた Hitachi Command Suite 共通コンポーネントを含むほかの Hitachi Command Suite 製品も起動します。

### 関連項目

- [8.1.1 Compute Systems Manager の起動と停止とは](#)
- [8.1.4 Compute Systems Manager の常駐プロセス](#)
- [8.1.5 Compute Systems Manager の稼働状況を確認する](#)

## 8.1.3 Compute Systems Manager を停止する

Compute Systems Manager は次の方法で停止できます。



**重要** 構成を変更する前には、すべての Hitachi Command Suite 製品を停止してください。障害対処など特別な理由がないかぎり、Compute Systems Manager だけを停止しないでください。

Windows :

次のどちらかの方法で停止します。

- Windows のメニューから停止する。
  - Windows Server 2008 R2 の場合 :  
[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Compute Systems Manager] - [Stop - HCSM] を選択します。
  - Windows Server 2012 の場合 :  
[スタート] - [すべてのアプリ] - [Hitachi Command Suite] - [Compute Systems Manager] - [Stop - HCSM] を選択します。
- コマンドを実行して停止する。
  - すべての Hitachi Command Suite 製品を停止するには、次のコマンドを実行します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin%\hcmds64srv /stop
  - ほかの Hitachi Command Suite 製品を停止しないで、Compute Systems Manager だけを停止するには、次のコマンドを実行します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin%\hcmds64srv /stop /server ComputeSystemsManagerWebService

Linux :

- すべての Hitachi Command Suite 製品を停止するには、次のコマンドを実行します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -stop
- ほかの Hitachi Command Suite 製品を停止しないで、Compute Systems Manager だけを停止するには、次のコマンドを実行します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -stop -server ComputeSystemsManagerWebService

Compute Systems Manager が停止します。同じマシンにインストールされた Hitachi Command Suite 共通コンポーネントを含むほかの Hitachi Command Suite 製品も停止します。

### 関連項目

- [8.1.1 Compute Systems Manager の起動と停止とは](#)
- [8.1.4 Compute Systems Manager の常駐プロセス](#)
- [8.1.5 Compute Systems Manager の稼働状況を確認する](#)

## 8.1.4 Compute Systems Manager の常駐プロセス

Compute Systems Manager の常駐プロセス、およびデプロイメントマネージャーの常駐プロセスを、それぞれ次の表に示します。

表 8-1 Compute Systems Manager の常駐プロセス一覧 (Windows)

プロセス名	プロセス数	サービス名	説明
cjstartsv.exe	1	HCS Compute Systems Manager Web Service	Compute Systems Manager の J2EE サービス ほかの Hitachi Command Suite 製品が同じマシンにインストールされている場合、その製品のプロセスが、cjstartsv.exe および hcmdssvctl.exe という名称で起動されることがあります。
hcmdssvctl.exe	1		
cjstartsv.exe	1	HBase 64 Storage Mgmt SSO Service	シングルサインオン用の Hitachi Command Suite の J2EE サービス ほかの Hitachi Command Suite 製品が同じマシンにインストールされている場合、その製品のプロセスが、cjstartsv.exe および hcmdssvctl.exe という名称で起動されることがあります。
hcmdssvctl.exe	1		
httpsd.exe	1~2	HBase 64 Storage Mgmt Web Service	Hitachi Command Suite 共通 Web サービス
rotatelog.exe	2~4		
httpsd.exe	1~2	HBase 64 Storage Mgmt Web SSO Service	シングルサインオン用の Hitachi Command Suite 共通 Web サービス
rotatelog.exe	2~4		
hntr2mon.exe	1	Hitachi Network Objectplaza Trace Monitor 2	Hitachi Command Suite 共通トレースログ採取 (統合トレースログ情報の採取)
hntr2srv.exe	1		Hitachi Command Suite 共通トレースサービス ([サービス] ダイアログからのイベントの処理)
hntr2mon.exe	1	Hitachi Network Objectplaza Trace Monitor 2 (x64)	Hitachi Command Suite 共通トレースログ採取 (統合トレースログ情報の採取)
hntr2srv.exe	1		Hitachi Command Suite 共通トレースサービス ([サービス] ダイアログからのイベントの処理)
pdservice.exe	1	HiRDB/ EmbeddedEdition_HD1	データベースの関連プロセスの管理
pdprcd.exe	1		

表 8-2 デプロイメントマネージャーの常駐プロセス一覧

プロセス名	プロセス数	サービス名	説明
apiserv.exe	1	DeploymentManager API Service	デプロイメントマネージャー共通コンポーネントサービス
bkressvc.exe	1	DeploymentManager Backup/Restore Management	バックアップやリストアのタスク実行サービス
depssvc.exe	1	DeploymentManager Get Client Information	デプロイメントマネージャーターゲットサーバからの情報取得サービス

プロセス名	プロセス数	サービス名	説明
pxesvc.exe	1	DeploymentManager PXE Management	ネットワーク (PXE) ブートの制御サービス
pxemtftp.exe	1	DeploymentManager PXE Mtftp	tftp サーバ機能
rupdssvc.exe	1	DeploymentManager Remote Update Service	デプロイメントマネージャターゲットサーバのリモートアップデート実行サービス
schwatch.exe	1	DeploymentManager Schedule Management	スケジュール管理サービス
ftsvc.exe	1	DeploymentManager Transfer Management	ファイル転送サービス
sqlservr.exe	1	SQL Server (DPMDBI)	データベースサービス
sqlagent.exe	0	SQL Server Agent (DPMDBI)※	データベースジョブ管理サービス

注※

デプロイメントマネージャのインストール時に登録されますが、常駐プロセスとしては動作しません。

表 8-3 Compute Systems Manager の常駐プロセス一覧 (Linux)

プロセス名	説明
cjstartsv	Compute System Manager の J2EE サービス
hcs_csm	
cjstartsv	シングルサインオン用の Hitachi Command Suite の J2EE サービス
hcs_hssso	
httpsd	Hitachi Command Suite 共通 Web サービス このプロセスは複数起動されていることがあります。
httpsd	シングルサインオン用の Hitachi Command Suite 共通 Web サービス このプロセスは複数起動されていることがあります。
rotatelog	Web サービス用のログ分割ユーティリティ このプロセスは複数起動されていることがあります。
hntr2mon	Hitachi Command Suite 共通トレースログ採取 (統合トレースログ情報の採取)
pdprcd	データベースのプロセスサーバプロセス

#### 関連項目

- 8.1.1 Compute Systems Manager の起動と停止とは
- 8.1.5 Compute Systems Manager の稼働状況を確認する

## 8.1.5 Compute Systems Manager の稼働状況を確認する

Compute Systems Manager は次の方法で稼働状況を確認できます。

Windows :

次のどちらかの方法で確認します。

- Windows のメニューから確認する。

- Windows Server 2008 R2 の場合 :  
[スタート] – [すべてのプログラム] – [Hitachi Command Suite] – [Compute Systems Manager] – [Status - HCSM] を選択します。
- Windows Server 2012 の場合 :  
[スタート] – [すべてのアプリ] – [Hitachi Command Suite] – [Compute Systems Manager] – [Status - HCSM] を選択します。
- コマンドを実行して確認する。  

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin%
%hcmds64srv /statusall
```

Linux :

次のコマンドを実行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
hcmds64srv -statusall
```

Compute Systems Manager の稼働状況が表示されます。

#### 関連項目

- [8.1.1 Compute Systems Manager の起動と停止とは](#)
- [8.1.4 Compute Systems Manager の常駐プロセス](#)

## 8.2 データベースの管理

### 8.2.1 データベースの管理とは

Compute Systems Manager では、障害が発生したときにデータベースをリストアできます。また、Compute Systems Manager をアップグレードしたり、新しいマシンへ管理サーバを移行したりする場合などに、データベースを移行できます。

データベースをバックアップおよびリストアする方法を次に示します。

- hcmds64backups コマンドを使ってバックアップしたデータベースを、hcmds64db コマンドを使ってリストアする  
このバックアップおよびリストア方法を推奨しています。
- hcmds64dbtrans コマンドを使ってエクスポートしたデータベースを、hcmds64dbtrans コマンドを使ってインポートする  
リストアしたい環境が、hcmds64db コマンドでリストアするときの条件に合わない場合に、この方法で実行します。



**重要** 障害が発生したときに備えて、hcmds64backups コマンドで取得するバックアップと hcmds64dbtrans コマンドで取得するエクスポートを、定期的に両方実行しておくことを推奨します。

データベースを移行するには、hcmds64dbtrans コマンドを使って移行元のデータベースをエクスポートしたあと、hcmds64dbtrans コマンドで移行先へインポートします。

次に示すような、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 (例 : Windows Server 2008 R2 から Windows Server 2012 への移行)

- Compute Systems Manager のインストール先が異なるマシンへの移行
- Compute Systems Manager 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

Compute Systems Manager 以外の Hitachi Command Suite 製品が稼働しているマシンでは、すべての Hitachi Command Suite 製品について一括でデータベースのバックアップ、リストア、および移行を実行できます。



#### 重要

- バックアップソフトウェアを使用して、Compute Systems Manager のインストールディレクトリ、およびデータベースの格納先ディレクトリを含むディスク領域をバックアップする場合は、すべての Hitachi Command Suite 製品のサービスを停止してから実施してください。

サービスを停止しないでバックアップを実施すると、I/O 遅延やファイル排他などによって障害が発生するおそれがあります。

- コマンドを実行するときに指定するパスおよびファイル名には、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。

¥ / : , ; \* ? " < > | \$ % & ' `

ただし、パスの区切り文字として、Windows の場合は円記号 (¥)、コロンの (: ) およびスラント (/), Linux の場合はスラント (/) 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。

Windows の場合、パス中に半角スペースを指定するときは、パスを引用符 (") で囲んで指定してください。Linux の場合は、パス中に半角スペースは指定できません。

#### 関連項目

- 8.1.3 Compute Systems Manager を停止する
- 8.2.2 データベースをバックアップするための確認事項
- 8.2.3 データベースをバックアップする
- 8.2.4 データベースをリストアするための確認事項
- 8.2.5 データベースをリストアする
- 8.2.6 データベースを移行するための確認事項
- 8.2.7 移行元サーバからデータベースをエクスポートする
- 8.2.8 移行先サーバにデータベースをインポートする
- 10.2.3 トラブルシューティング事例 (データベースをリストアできない)

## 8.2.2 データベースをバックアップするための確認事項

データベースをバックアップするためには、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。

バックアップファイルを格納するディレクトリに必要な空き容量 : ( $<$ バックアップ対象となる Hitachi Command Suite 製品のデータベースサイズの総和<sup>※</sup>  $>$  + 4.6 GB)  $\times$  2

#### 注※

Compute Systems Manager、および Hitachi Command Suite 共通コンポーネントのデータベースの容量については、データベースファイルの格納先ディレクトリの容量をデータベースのサイズとしてください。ほかの Hitachi Command Suite 製品のデータベースの容量については、各製品のマニュアルを参照してください。

## 関連項目

- 2.3.3 インストールに使用するディレクトリの内容を確認する
- 8.2.1 データベースの管理とは
- 8.2.3 データベースをバックアップする

## 8.2.3 データベースをバックアップする

障害が発生した場合に、管理サーバでデータベースをリストアできるようにデータベースをバックアップしておく必要があります。

### 事前に完了しておく操作

- データベースをバックアップするための確認作業

データベースをバックアップする手順を次に示します。

1. バックアップファイルを格納するディレクトリの下に、ファイルおよびサブディレクトリがないことを確認します。
2. `hcms64backups` 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。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >\bin  
hcms64backups /dir <ローカルディスク上のバックアップファイル格納先ディレクトリ  
> /auto
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/  
hcms64backups -dir <ローカルディスク上のバックアップファイル格納先ディレクトリ  
> -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。

`auto`

Hitachi Command Suite 製品およびデータベースのサービスを、適切な状態に変更するためのオプションです。コマンド実行後には、Hitachi Command Suite 製品およびデータベースのサービスが起動した状態になります。

`hcms64backups` 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の下に `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。



参考 `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た `database` 以外のディレクトリには、Hitachi Command Suite 製品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 Hitachi 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。

## 関連項目

- 8.2.1 データベースの管理とは
- 8.2.2 データベースをバックアップするための確認事項
- 8.2.5 データベースをリストアする



## 8.2.4 データベースをリストアするための確認事項

データベースをリストアする前に、バックアップを取得した時点の管理サーバと、データベースをリストアする時点の管理サーバとで、次の項目が同じであることを確認してください。

- ・ インストールされている Compute Systems Manager を含む Hitachi Command Suite 製品の、バージョンおよびリビジョン
- ・ Compute Systems Manager を含む Hitachi Command Suite 製品および Hitachi Command Suite 共通コンポーネントのインストール先
- ・ Compute Systems Manager を含む Hitachi Command Suite 製品および Hitachi 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

リストアの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

### 関連項目

- ・ [8.2.1 データベースの管理とは](#)
- ・ [8.2.3 データベースをバックアップする](#)
- ・ [8.2.5 データベースをリストアする](#)

## 8.2.5 データベースをリストアする

障害が発生した場合に、あらかじめ取得しておいたバックアップを使用して、データベースをリストアできます。

### 事前に完了しておく操作

- ・ データベースをリストアするための確認作業

データベースをリストアする手順を次に示します。

1. hcmds64db コマンドを実行してデータベースをリストアします。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64db /restore <バックアップファイル> /type ALL /auto
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64db -restore <バックアップファイル> -type ALL -auto
```

restore

バックアップファイル (backup.hdb) の名称を絶対パスで指定します。

auto

Hitachi Command Suite 製品およびデータベースのサービスを、適切な状態に変更するためのオプションです。コマンド実行後には、Hitachi Command Suite 製品およびデータベースのサービスが停止した状態になります。

2. Compute Systems Manager を起動します。

同じホストにほかの Hitachi Command Suite 製品がインストールされていた場合は、Compute Systems Manager と合わせてリストアされます。ほかの Hitachi Command Suite 製品もリストアされた場合は、リストア後に作業が必要なことがあります。リストア後に必要な作業については、各 Hitachi Command Suite 製品のマニュアルを参照してください。

#### 関連項目

- 8.2.1 データベースの管理とは
- 8.2.3 データベースをバックアップする
- 8.2.4 データベースをリストアするための確認事項
- 10.2.3 トラブルシューティング事例（データベースをリストアできない）

## 8.2.6 データベースを移行するための確認事項

データベースを異なる管理サーバに移行するために、移行元サーバでエクスポートしたあと、移行先サーバでインポートする必要があります。

データベースの移行を開始する前に、次の条件がすべて満たされていることを確認してください。

- 移行先サーバにインストールする Hitachi Command Suite 製品のバージョンが、すべて移行元サーバの Hitachi Command Suite 製品と同じか、それ以降であること
- Compute Systems Manager のデータベースをエクスポートする場合、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に、十分な容量が確保されていること  
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 Hitachi Command Suite 製品の各データベースの格納先ディレクトリ
  - Hitachi 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（SYS ディレクトリとその下を除く）



**重要** 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を格納するディレクトリの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、十分な容量を確保したあとに再度エクスポートしてください。

#### 関連項目

- 8.2.1 データベースの管理とは
- 8.2.7 移行元サーバからデータベースをエクスポートする
- 8.2.8 移行先サーバにデータベースをインポートする

## 8.2.7 移行元サーバからデータベースをエクスポートする

異なるマシンへデータベースを移行するために、現在使用中のマシンのデータベースをエクスポートします。また、障害に備えてデータベースをエクスポートしておけば、障害が発生したときにデータベースをインポート（リストア）できます。

#### 事前に完了しておく操作

- データベースを移行するための確認作業

データベースをエクスポートする手順を次に示します。

1. エクスポートに使用する作業用ディレクトリの下に、ファイルおよびサブディレクトリがないことを確認します。
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。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64dbtrans /export /workpath <作業用ディレクトリ> /file <アーカイブ  
ファイル> /auto
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64dbtrans -export -workpath <作業用ディレクトリ> -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`

Hitachi Command Suite 製品およびデータベースのサービスを、適切な状態に変更するためのオプションです。コマンド実行後には、Hitachi Command Suite 製品およびデータベースのサービスが起動した状態になります。

3. データベースを移行するためにエクスポートした場合、アーカイブファイルを移行先サーバに転送します。

## 関連項目

- [8.2.1 データベースの管理とは](#)
- [8.2.6 データベースを移行するための確認事項](#)
- [8.2.8 移行先サーバにデータベースをインポートする](#)

## 8.2.8 移行先サーバにデータベースをインポートする

移行元のマシンでエクスポートしたデータベースを、異なるマシンへインポートします。また、エクスポートで取得したデータを使って、障害が発生したときにデータベースをインポート（リストア）できます。

### 事前に完了しておく操作

- データベースを移行するための確認作業

データベースをインポートする手順を次に示します。

1. 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。
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。



**参考** 通常は、アーカイブファイルを使用する方法でインポートしてください。

アーカイブファイルを使用しないでインポートする方法は、バージョン 8.1.0 以前の Compute Systems Manager からデータベースを移行する場合に、移行元のデータベースの全体容量が 2GB を超えているなどの理由で、アーカイブファイルが作成されなかったときに実行します。

アーカイブファイルを使用してインポートする場合：

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcms64dbtrans /import /workpath <作業用ディレクトリ> /file <アーカイブファイル> /type {ALL|< Hitachi Command Suite 製品名 >} /auto
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64dbtrans -import -workpath <作業用ディレクトリ> -file <アーカイブファイル> -type {ALL|< Hitachi Command Suite 製品名 >} -auto
```

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：

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcms64dbtrans /import /workpath <作業用ディレクトリ> /type {ALL|< Hitachi Command Suite 製品名 >} /auto
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64dbtrans -import -workpath <作業用ディレクトリ> -type {ALL|< Hitachi Command Suite 製品名 >} -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：**

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。

**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ます。転送したディレクトリの下ファイル構成は変更しないでください。

file

アーカイブファイルを使用してインポートする場合、移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。アーカイブファイルを使用しないでインポートする場合は、このオプションを指定しないでください。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。Compute Systems Manager のデータベースだけインポートする場合は、type オプションで「HCSM」と指定します。ほかの Hitachi Command Suite 製品のデータベースを個別にインポートする場合は、各 Hitachi Command Suite 製品のマニュアルを参照してください。

auto

Hitachi Command Suite 製品およびデータベースのサービスを、適切な状態に変更するためのオプションです。コマンド実行後には、Hitachi Command Suite 製品およびデータベースのサービスが停止した状態になります。

3. 移行先の Compute Systems Manager を起動します。

4. 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。

#### 関連項目

- 8.2.1 データベースの管理とは
- 8.2.3 データベースをバックアップする
- 8.2.6 データベースを移行するための確認事項
- 8.2.7 移行元サーバからデータベースをエクスポートする



# クラスタを使用するための環境設定と運用

この章では、クラスタを使用して運用するための Compute Systems Manager のインストールと環境設定、起動と停止、データベースの管理などについて説明します。

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス
- 9.3 クラスタ運用を開始する前の確認事項
- 9.4 クラスタ環境へのインストール
- 9.5 クラスタ環境への移行
- 9.6 クラスタ管理アプリケーションへのサービスの登録と削除
- 9.7 新規インストールまたはクラスタ環境に移行した後の環境設定
- 9.8 クラスタ環境での Compute Systems Manager の起動と停止
- 9.9 クラスタ環境でのデータベースの管理
- 9.10 クラスタ環境からのアンインストール

## 9.1 クラスタを使用するための環境設定と運用とは

Compute Systems Manager では、クラスタ環境で管理サーバのフェールオーバーを設定することで、管理サーバの信頼性を高められます。

クラスタを使用して Compute Systems Manager の運用を開始するためには、Compute Systems Manager のインストールまたは非クラスタ環境からクラスタ環境への移行、ならびにクラスタ構成に関する環境の設定が必要です。

また、データベースの操作や Compute Systems Manager の起動または停止など、クラスタ環境で運用する場合の手順があります。

クラスタ環境では、2 台の管理サーバを、それぞれ実行系ノード、待機系ノードとして運用します。

障害発生時は、フェールオーバーすることで、実行系ノードで使用していたシステムリソースを待機系ノードに引き継いで運用の停止を防ぎます。

- 実行系ノード  
クラスタ運用しているシステムで、実際に稼働しているホストです。
- 待機系ノード  
クラスタ運用しているシステムで、障害発生時に、実行系ノードで使用していたシステムリソースを引き継げるように待機しているホストです。

このマニュアルでは、次のクラスタ管理アプリケーションを対象としています。

- Windows  
Windows Server Failover Clustering
- Red Hat Enterprise Linux  
Red Hat High Availability

マニュアルでは、Red Hat High Availability が提供する Conga を使用した手順を説明します。Conga を使用する場合は、パッケージ (luci) をインストールする必要があります。

マニュアルに記載している操作例は、次に示すバージョンの luci パッケージがインストールされていることを前提にしています。

Version : 0.26.0

Release : 48.el6

luci パッケージの詳細については、Red Hat High Availability のマニュアルを参照してください。



### 重要

- 障害が発生し、実行系ノードから待機系ノードにフェールオーバーした場合、実行中のタスクは失敗します。必要に応じて、失敗したタスクを再実行してください。
- ストレージシステムの一部機種の SVP と、Compute Systems Manager を同一ホストで運用する場合、SVP はクラスタ構成をサポートしていないため、Compute Systems Manager を非クラスタ構成にしてください。  
対象となるストレージシステムの機種については、ソフトウェア添付資料を参照してください。

### 関連項目

- [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)
- [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)
- [9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認](#)
- [9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認](#)



- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.5.1 クラスタ環境に移行する (Windows)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)
- 9.10.2 クラスタ環境から Compute Systems Manager をアンインストールする (Windows)
- 9.10.3 クラスタ環境から Compute Systems Manager をアンインストールする (Red Hat Enterprise Linux)
- D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)

## 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス

クラスタ環境で使用する、Compute Systems Manager および Hitachi Command Suite 共通コンポーネントのサービスを次に示します。

- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- HCS Compute Systems Manager Web Service
- HiRDB/ClusterService\_HD1 (Windows の場合)
- HiRDB (Red Hat Enterprise Linux の場合)

Windows の管理サーバでデプロイメントマネージャーを使用する場合は、次のサービスも使用します。

- DeploymentManager PXE Management
- DeploymentManager PXE Mtftp
- DeploymentManager Transfer Management

### 関連項目

- 8.1.4 Compute Systems Manager の常駐プロセス
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.6.1 クラスタ管理アプリケーションにサービスを登録する (Windows)
- 9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux)
- 9.6.3 クラスタ管理アプリケーションからサービスを削除する (Windows)
- 9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux)
- 9.8.1 Compute Systems Manager のクラスタ運用を一時停止する (Windows)
- 9.8.2 Compute Systems Manager のクラスタ運用を一時停止する (Red Hat Enterprise Linux)
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)

## 9.3 クラスタ運用を開始する前の確認事項

### 9.3.1 クラスタ運用を開始する環境設定手順の確認

クラスタ環境で Compute Systems Manager を運用する場合、環境設定手順は管理サーバの状態によって異なります。

運用する管理サーバの状態を確認し、実施する環境設定手順を決定してください。

管理サーバの状態ごとに、クラスタ環境を設定する手順を次に示します。

図 9-1 管理サーバがクラスタ環境の場合のクラスタ環境設定手順 (Windows)

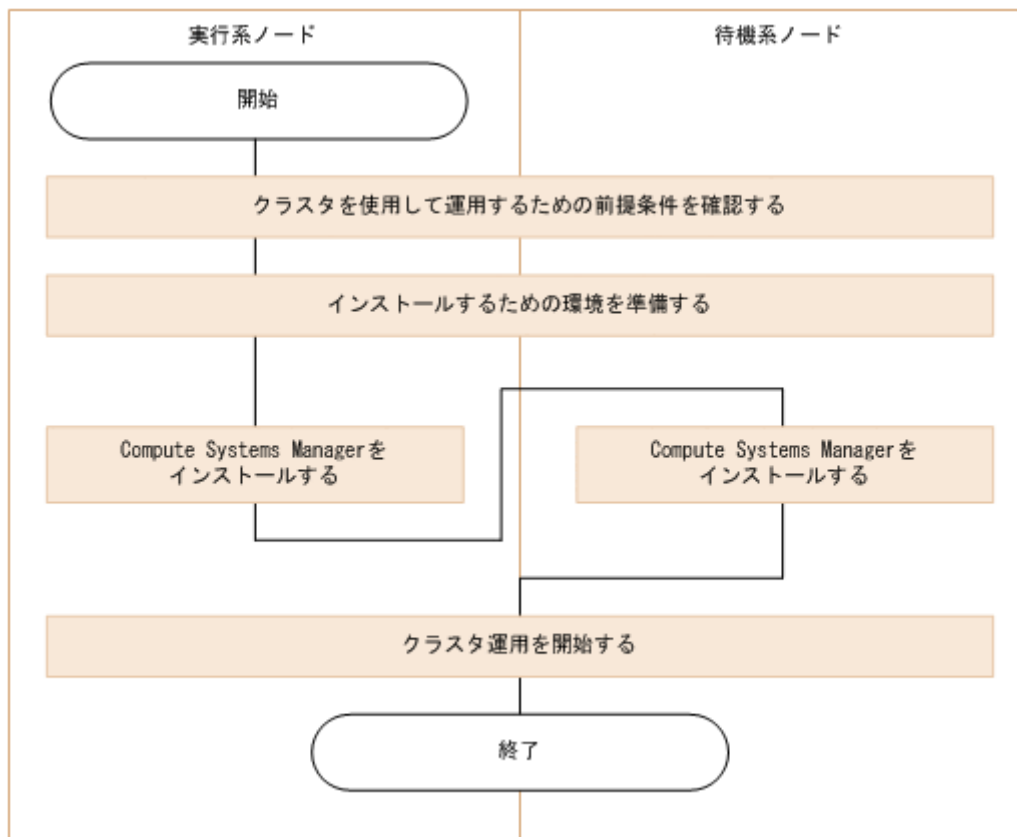


図 9-2 管理サーバがクラスタ環境で、Compute Systems Manager がインストールされていない場合のクラスタ環境設定手順 (Red Hat Enterprise Linux)

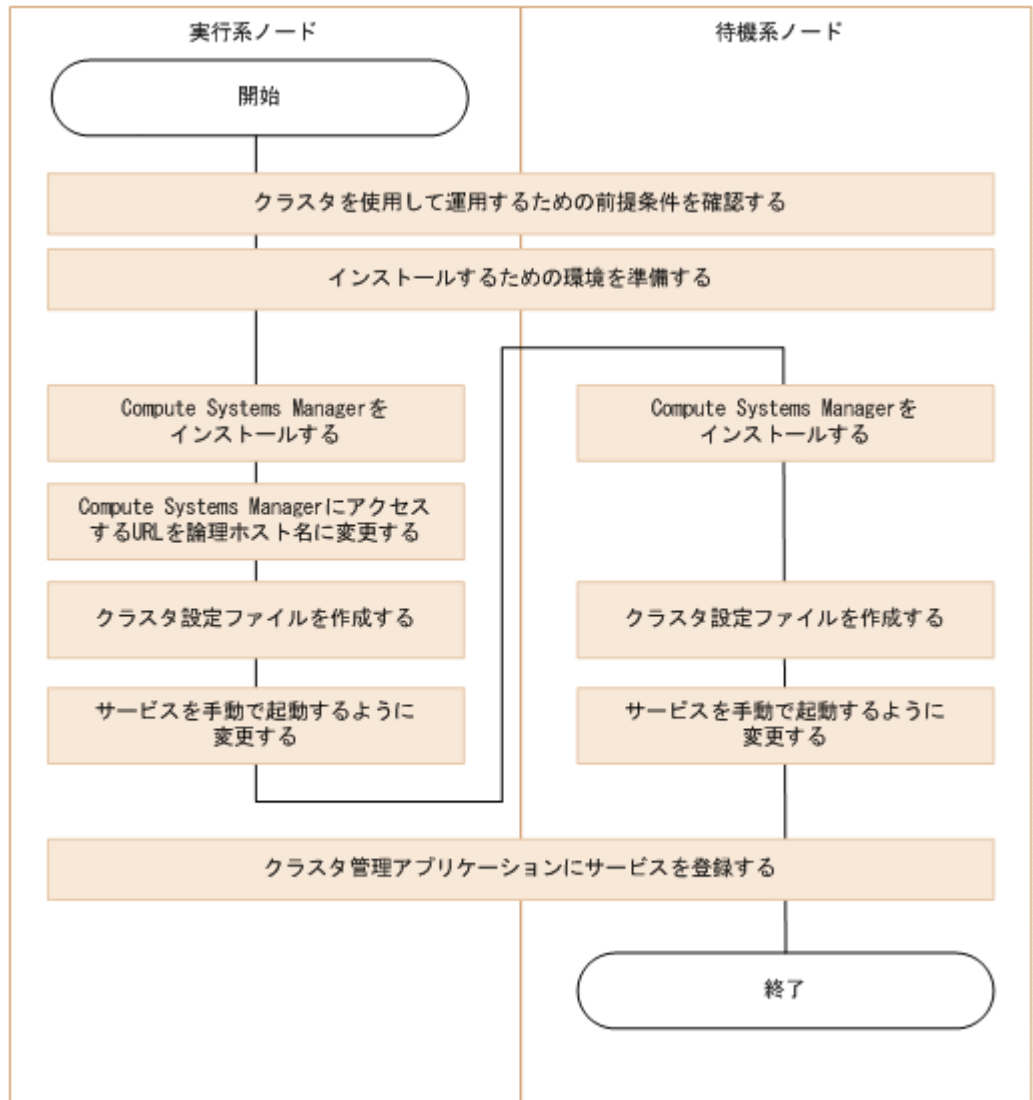


図 9-3 管理サーバがクラスタ環境で、Compute Systems Manager がインストールされている場合のクラスタ環境設定手順 (Red Hat Enterprise Linux)

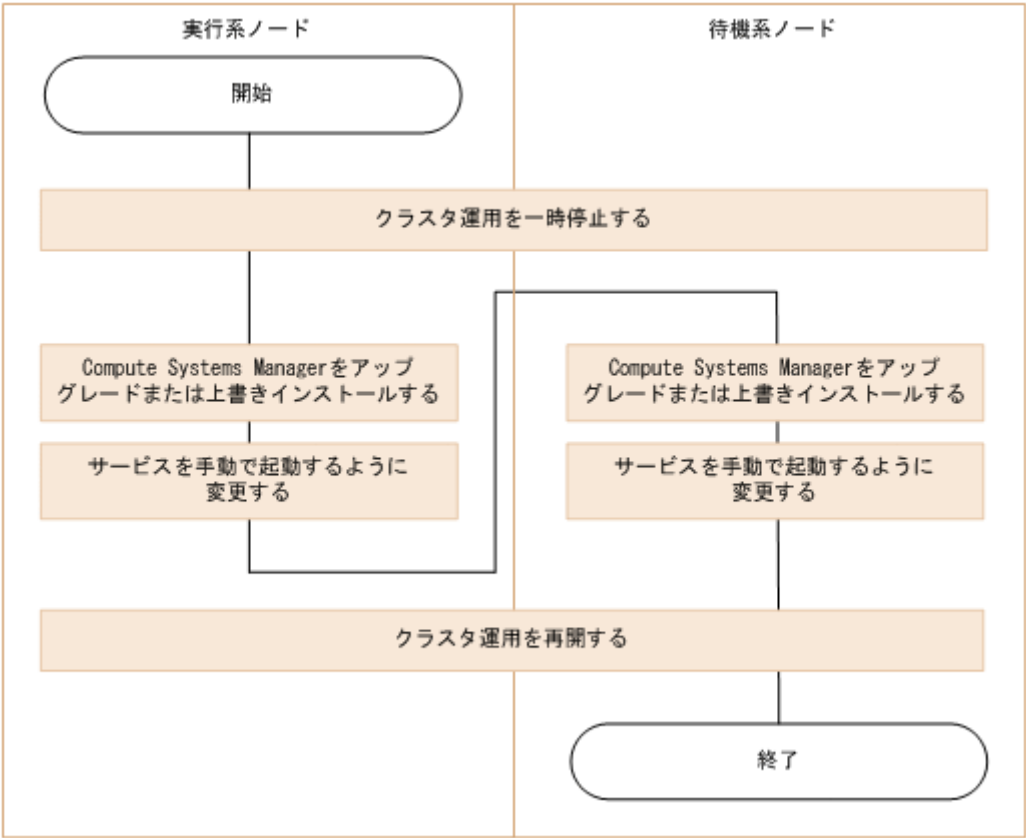


図 9-4 管理サーバが非クラスタ環境の場合のクラスタ環境設定手順 (Windows)

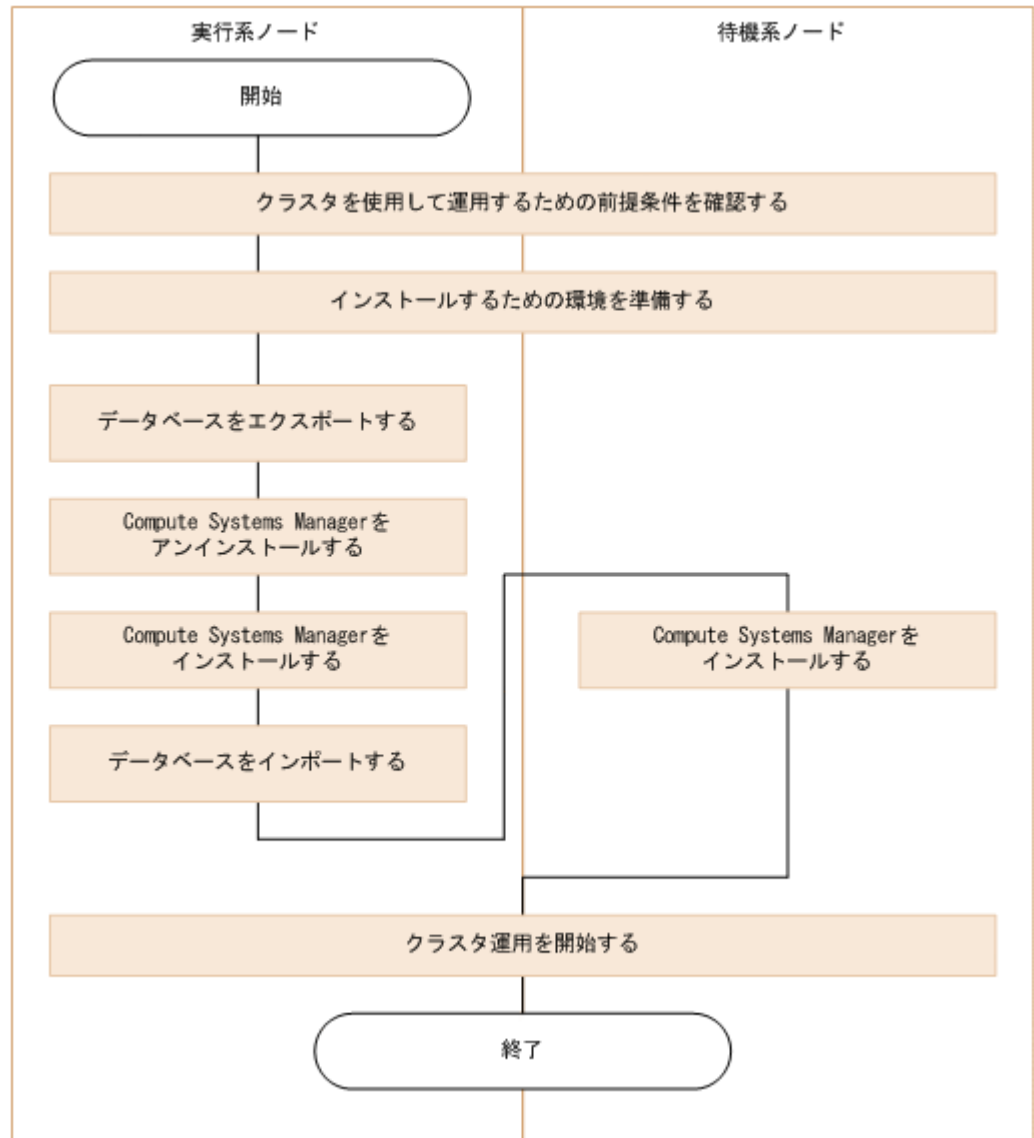
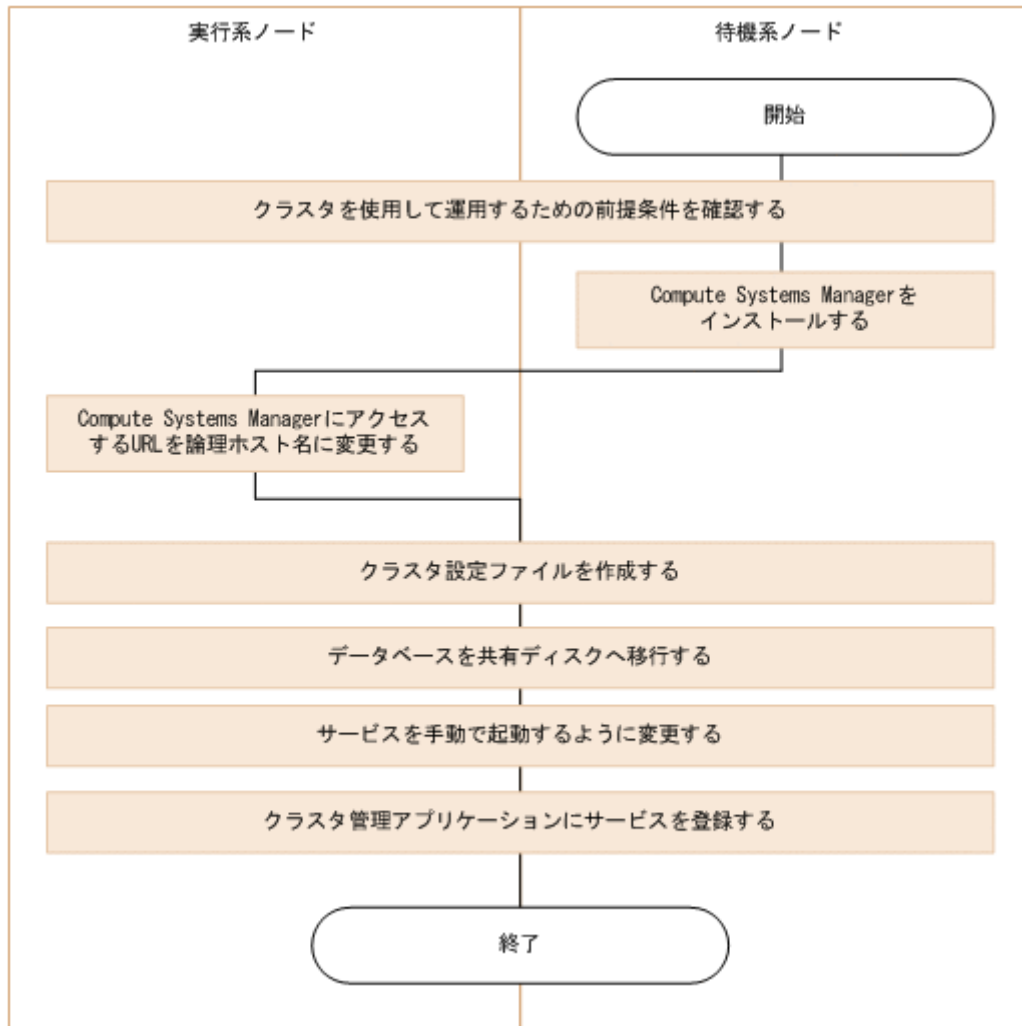


図 9-5 管理サーバが非クラスタ環境の場合のクラスタ環境設定手順 (Red Hat Enterprise Linux)



**重要**

- Compute Systems Manager を新たにクラスタ環境へインストールする場合、または、非クラスタ環境からクラスタ環境に移行する場合は、クラスタを構成するすべてのノードが、同じディスク構成で、かつ、Hitachi Command Suite 製品のインストール先（ドライブ文字やパス名など）も同じになるようにしてください。
- Windows の場合、クラスタ環境へのインストールにはドメインの Administrator 権限を持つユーザーでのログインが必要です。

**関連項目**

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認
- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認
- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.4.4 実行系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux)
- 9.4.5 待機系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux)

- 9.5.1 クラスタ環境に移行する (Windows)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)
- 9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux)
- 9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux)
- 9.8.2 Compute Systems Manager のクラスタ運用を一時停止する (Red Hat Enterprise Linux)
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)

## 9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認

クラスタを使用して、Compute Systems Manager の運用を開始するための環境設定では、データベースをバックアップしたり、必要なデータを共有ディスクへ移行したりします。

管理サーバに次の空き容量があることを確認してください。

- データベースのバックアップに必要な空き容量：  
データベースをバックアップするための確認事項を参照して、空き容量を確認します。
- 共有ディスクに必要な空き容量：
  - データベースを移行するために指定する再作成先に必要な容量  
 $\langle \text{Hitachi Command Suite 共通コンポーネントのデータベース容量} \rangle +$   
 $\langle \text{Compute Systems Manager と同一ホストにインストールされている Compute Systems Manager を含むすべての Hitachi Command Suite 製品のデータベース容量} \rangle$
  - Windows の管理サーバでデプロイメントマネージャーを使用する場合、イメージファイルを移行するために必要な容量
  - Compute Systems Manager が使用する作業ディレクトリを格納するために必要な容量  
 Compute Systems Manager が使用する作業ディレクトリについては、次のファイルに定義する `hcsml.shared.directory` プロパティの説明を参照してください。

Windows :

$\langle \text{Compute Systems Manager のインストールディレクトリ} \rangle$   
`¥ComputeSystemsManager¥conf¥user.properties`

Red Hat Enterprise Linux :

$\langle \text{Compute Systems Manager のインストールディレクトリ} \rangle /$   
`ComputeSystemsManager/conf/user.properties`

注※

Compute Systems Manager, および Hitachi Command Suite 共通コンポーネントのデータベースの容量については、データベースファイルの格納先ディレクトリの容量をデータベースのサイズとしてください。ほかの Hitachi Command Suite 製品のデータベースの容量については、各製品のマニュアルを参照してください。

### 関連項目

- 8.2.2 データベースをバックアップするための確認事項
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux)

- 9.4.4 実行系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux)
- 9.5.1 クラスタ環境に移行する (Windows)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)
- D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)

### 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認

クラスタを使用して運用を開始するための環境設定では、クラスタ管理アプリケーションでの操作が必要です。

クラスタ環境を設定する前に、クラスタ管理アプリケーションで次の項目を確認してください。



**重要** Windows の場合、クラスタ管理アプリケーションを操作するには、ドメインの Administrator 権限を持つユーザーでログインする必要があります。

- すでに、ほかの Hitachi Command Suite 製品のサービスが登録されているグループがあるか  
すでに登録されているグループがあれば、そのグループを使用してください。サービスを登録するグループは、Hitachi Command Suite 製品に関連するリソースだけで構成してください。  
すでに登録されているグループがなければ、Compute Systems Manager のサービスを登録する予定のグループを、クラスタ管理アプリケーションに用意してください。

Windows の管理サーバの場合、グループ名に次の文字は使用できません。

! " & ) \* ^ | < >

- 実行系ノードと待機系ノードで引き継ぎ可能な共有ディスクならびにクライアントアクセスポイント (クラスタ管理 IP アドレスおよび論理ホスト名) を含めてグループが構成されているか
- クラスタ管理アプリケーションによって、リソースの割り当て、削除および動作監視が、正常に制御できるか

クラスタ環境で使用するサービスは、クラスタ管理アプリケーションで登録するグループ単位でフェールオーバーできます。クラスタ管理アプリケーションや OS のバージョンによっては、「リソースグループ」、「役割」など、グループを示す名称が、異なる名称で呼ばれることがあります。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.4.4 実行系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux)
- 9.5.1 クラスタ環境に移行する (Windows)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)
- D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)



## 9.4 クラスタ環境へのインストール

### 9.4.1 クラスタ環境にインストールする (Windows)

クラスタ構成である Windows の管理サーバに、Compute Systems Manager をインストールします。

ここで説明する手順は、新規インストール、上書きインストール、およびバージョン 8.0.0 以降からのアップグレードインストールを対象にしています。

バージョン 7.x.x からアップグレードする場合は手順が異なります。詳細については、バージョン 7.x.x からのアップグレードについての説明を参照してください。

#### 事前に完了しておく操作

- ・ インストールする前の確認作業
- ・ クラスタ環境で運用する管理サーバの空き容量の確認
- ・ クラスタ管理アプリケーションを使用して設定する前の確認
- ・ データベースが使用するポート番号の確認 (ほかの Hitachi Command Suite 製品でクラスタが構築されている環境に新規インストールする場合)

Compute Systems Manager を新規インストールすると、データベースが使用するポート番号がデフォルト (22032/tcp) に設定されます。

ポート番号をデフォルト以外の番号に変更して運用している場合は、ポート番号を控えておいてください。



#### 重要

- ・ デプロイメントマネージャーをバージョン 8.1.4 以前からアップグレードする場合、アップグレードを実行するユーザーが前回のインストールと異なるときは、事前にデプロイメントマネージャーをアンインストールする必要があります。

前回インストールを実行したユーザーでログインしたあと、デプロイメントマネージャーをアンインストールしてください。

そのあと、アップグレードを実行するユーザーでログインし直して、デプロイメントマネージャーを選択してアップグレードしてください。

- ・ インストールウィザードで指定するクラスタ管理アプリケーションのグループに、すでに Hitachi Command Suite 製品のサービスが登録されている場合は、次の点に注意してください。

登録されているサービスは、実行系ノードでのインストール時にすべて削除され、待機系ノードでのインストール時にデフォルトの設定で再登録されます。サービスのリソース名を変更している場合は、必要に応じて事前にリソース名を控えておき、インストール後に手動で変更してください。

ただし、Hitachi File Services Manager のサービスは削除されないため、上記の対処は不要です。

クラスタ環境に Compute Systems Manager をインストールする手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を実行系ノードに移動し、クラスタ管理 IP アドレスと共有ディスクをオンラインにします。
2. 実行系ノードに Compute Systems Manager をインストールします。  
インストールウィザードでは、クラスタ構成でのインストールを選択して、それぞれの画面で必要な情報を指定します。ほかの Hitachi Command Suite 製品ですでにクラスタ環境が構築されている場合は、その設定が適用されるため、再度指定する必要はありません。
3. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を待機系ノードに移動します。
4. 待機系ノードに Compute Systems Manager をインストールします。

インストールの際には、次の条件に従ってください。

- インストール先を実行系ノードと同じにしてください。
- 実行系ノードでデプロイメントマネージャーをインストールした場合は、待機系ノードでもインストールしてください。



**重要** 待機系ノードで複数の Hitachi Command Suite 製品を新規インストールする場合は、実行系ノードでインストールした順番で製品をインストールしてください。

5. データベースが使用するポート番号をデフォルト以外の番号に変更して運用する場合は、控えておいたポート番号を実行系および待機系の各ノードで設定します。



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている場合は、その製品が使用するポート番号と競合しないことを確認してください。

6. 日立製のサーバを管理対象にする場合は、必要に応じて、日立製のサーバに登録される管理サーバの IP アドレスがクラスタ管理 IP アドレスになるように設定を変更します。

実行系および待機系の各ノードで、次のファイルの `svp.bind.address` プロパティに、クラスタ管理 IP アドレスを指定します。

```
< Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager  
¥conf¥user.properties
```



#### 参考

- `svp.bind.address` プロパティを指定しない場合、日立製のサーバには実行系および待機系の各ノードの IP アドレスが登録されます。
- すでに運用中の日立製のサーバには、通信先の管理サーバの IP アドレスが登録されています。  
`svp.bind.address` プロパティを指定すると、プロパティに指定した IP アドレスも新しく登録されます。日立製のサーバに登録されている管理サーバの IP アドレスは、Web コンソールで確認できます。使用していない管理サーバの IP アドレスが残っている場合は削除してください。

7. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcnds64clustersrvstate /son /r <グループ名 >
```
8. プラグインライセンスを登録する場合は、待機系ノードでライセンスキーを入力します。
9. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を実行系ノードに移動します。
10. 待機系ノードでプラグインライセンスを登録した場合は、実行系ノードでも同様にライセンスキーを入力します。
11. デプロイメントマネージャーをインストールした場合は、デプロイメントマネージャーを使用するためのクラスタ環境を設定します。

#### 関連項目

- [2.4.2 インストールする前の確認事項](#)
- [2.4.3 Compute Systems Manager をインストールする \(Windows\)](#)
- [\(1\) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [\(3\) ポートを変更する](#)
- [7.2 デプロイメントマネージャーをインストールするための前提条件](#)
- [7.5 デプロイメントマネージャーをインストールする](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)

- 9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認
- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認
- 9.7.1 クラスタ環境でウイルス検出プログラムを使用する場合に必要な設定
- 9.7.2 クラスタ環境で同期が必要な設定
- 9.7.3 デプロイメントマネージャーを使用する場合のクラスタ環境を設定する
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)
- D.1 バージョン 7.x.x からのアップグレードとは

## 9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux)

クラスタ構成の実行系ノードである Red Hat Enterprise Linux の管理サーバに、Compute Systems Manager を新規インストールします。

### 事前に完了しておく操作

- インストールする前の確認作業
- クラスタ環境で運用する管理サーバの空き容量の確認
- クラスタ管理アプリケーションを使用して設定する前の確認
- ほかの Hitachi Command Suite 製品がインストールされている場合は、データベースが使用するポート番号の確認  
 インストールの手順で hcmds64dbclustersetup コマンドを実行すると、データベースが使用するポート番号がデフォルト (22032/tcp) に設定されます。  
 ポート番号をデフォルト以外の番号に変更して運用している場合は、ポート番号を控えておいてください。
- ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、各製品のサービスの削除  
 クラスタ管理アプリケーションのグループに登録されている Hitachi Command Suite 製品のサービスをすべて削除します。  
 ただし、共有ディスクおよびクラスタ管理 IP アドレスはグループから削除しないでください。  
 削除する手順については、各製品のマニュアルを参照してください。

実行系ノードで Compute Systems Manager を新規インストールする手順を次に示します。

1. クラスタ管理アプリケーションで、実行系ノードを選択してグループを起動します。  
 実行系ノードにグループが移動し、共有ディスクおよびクラスタ管理 IP アドレスだけが有効になっていることを確認してください。
2. 実行系ノードに Compute Systems Manager を新規インストールします。  
 ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、次の条件に従ってください。
  - 共有ディスクをアクセスできる状態にしたあとで、データベースの格納先に共有ディスク上のパスを指定する。
  - 管理サーバの IP アドレスに論理ホスト名 (クラスタ管理 IP アドレスに割り当てられた仮想のホスト名) を指定する。
 ほかの Hitachi Command Suite 製品でクラスタ環境が構築されていない場合は、次の条件に従ってください。

- データベースの格納先に、ローカルディスク上のパスを指定する。
  - 管理サーバの IP アドレスに、実行系ノードの IP アドレスを指定する。
3. プラグインライセンスが必要な場合は、ライセンスキーを入力してください。
  4. 次のコマンドを実行して、論理ホスト名になっているかを確認します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64chgurl -list`
  5. 手順 4 で論理ホスト名が指定されていなかった場合、Compute Systems Manager にアクセスする URL を論理ホスト名に変更します。  
 次のコマンドを実行して URL を変更します。ホスト名には、インストール時に入力した値を指定します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64chgurl -change http://<実行系ノードの IP アドレスまたはホスト名>:<ポート番号> http://<論理ホスト名>:<ポート番号>`
  6. クラスタ設定ファイルを作成します。ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、この手順は不要です。  
 クラスタ設定ファイルは、テキストファイルで次の場所に格納します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/conf/cluster.conf`  
 クラスタ設定ファイルには、次の内容を記述してください。実行系ノードの場合、mode には online を指定する必要があります。  

```
mode=online
virtualhost=<論理ホスト名>
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```
  7. データベースを共有ディスクに移行します。  
 その方法を手順 8～手順 10 で説明します。  
 ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、データベースを共有ディスクに移行する手順は不要です。手順 11 に進んでください。
  8. 次のコマンドを実行して、新規インストール後の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、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。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64backups -dir <ローカルディスク上のバックアップファイル格納先ディレクトリ > -auto`
  9. 次のコマンドを実行して、データベースを共有ディスクに移行します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64dbclustersetup -createcluster -databasepath <共有ディスク上のデータベース再作成先ディレクトリ > -exportpath <ローカルディスク上の退避データ格納先ディレクトリ > -auto`



#### 注意

- hcmds64dbclustersetup コマンドを実行すると、Device Manager と Tuning Manager の間のリモート接続の設定が初期化されます。必要に応じて再設定してください。
- 共有ディスク上に、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品 (Hitachi File Services Manager および Hitachi Storage Navigator Modular 2) のデータベースが作成されている場合、databasepath オプションには別のディレクトリを指定する必要があります。

10. データベースが使用するポート番号をデフォルト以外の番号に変更して運用する場合は、控えておいたポート番号を設定します。



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品 (Hitachi File Services Manager および Hitachi Storage Navigator Modular 2) がインストールされている場合は、その製品が使用するポート番号と競合しないことを確認してください。

11. 次のコマンドを実行して、Hitachi Command Suite 製品が停止していることを確認します。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞/bin/  
hcnds64srv -status
12. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始されないようにします。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞/bin/  
hcnds64srv -starttype manual -all
13. Compute Systems Manager がマシンの起動時に自動的に開始されないようにします。  
次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S を使用しないでください。
  - /etc/rc3.d/S99hicommand64-hcs\_csm
  - /etc/rc5.d/S99hicommand64-hcs\_csmほかの Hitachi Command Suite 製品がインストールされている場合は、その製品も自動的に開始されないようにします。操作の対象となるファイルについては、各製品のマニュアルを参照してください。
14. Compute Systems Manager が使用する作業ディレクトリとして、共有ディスクに任意のディレクトリを作成したあと、そのディレクトリへのパスを次のファイルの hscsm.shared.directory プロパティに指定します。  
＜Compute Systems Manager のインストールディレクトリ＞/ComputeSystemsManager/  
conf/user.properties
15. 日立製のサーバを管理対象にする場合は、必要に応じて、日立製のサーバに登録される管理サーバの IP アドレスがクラスタ管理 IP アドレスになるように設定を変更します。  
次のファイルの svp.bind.address プロパティに、クラスタ管理 IP アドレスを指定します。  
＜Compute Systems Manager のインストールディレクトリ＞/ComputeSystemsManager/  
conf/user.properties



#### 参考

- svp.bind.address プロパティを指定しない場合、日立製のサーバには実行系および待機系の各ノードの IP アドレスが登録されます。
- すでに運用中の日立製のサーバには、通信先の管理サーバの IP アドレスが登録されています。svp.bind.address プロパティを指定すると、プロパティに指定した IP アドレスも新しく登録されます。日立製のサーバに登録されている管理サーバの IP アドレスは、Web コンソールで確認できます。使用していない管理サーバの IP アドレスが残っている場合は削除してください。

16. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループを待機系ノードに移動します。

#### 関連項目

- [2.4.2 インストールする前の確認事項](#)
- [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)
- [\(1\) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [\(3\) ポートを変更する](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)
- [9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認](#)

- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認
- 9.9.2 クラスタ環境でデータベースをバックアップする (Red Hat Enterprise Linux)
- 9.9.9 データベースを移行するコマンド (hcmds64dbclustersetup) の書式 (Red Hat Enterprise Linux)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)
- B.2.18 管理サーバをクラスタ構成にする場合に設定が必要なプロパティ (cluster.conf)

### 9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux)

クラスタ構成の待機系ノードである Red Hat Enterprise Linux の管理サーバに、Compute Systems Manager を新規インストールします。

#### 事前に完了しておく操作

- インストールする前の確認作業
- 実行系ノードへの Compute Systems Manager のインストール

待機系ノードで Compute Systems Manager を新規インストールする手順を次に示します。

1. 待機系ノードに Compute Systems Manager を新規インストールします。  
インストールの際には、次の条件に従ってください。
  - インストール先を実行系ノードと同じにしてください。
  - ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、管理サーバの IP アドレスに論理ホスト名 (クラスタ管理 IP アドレスに割り当てられた仮想のホスト名) を指定してください。ほかの Hitachi Command Suite 製品でクラスタ環境が構築されていない場合は、待機系ノードの IP アドレスまたはホスト名を指定してください。
2. プラグインライセンスが必要な場合は、ライセンスキーを入力してください。
3. クラスタ設定ファイルを作成します。ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、この手順は不要です。  
クラスタ設定ファイルは、テキストファイルで次の場所に格納します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf/  
cluster.conf  
クラスタ設定ファイルには、次の内容を記述してください。待機系ノードの場合、mode には standby を指定する必要があります。  
mode=standby  
virtualhost=<論理ホスト名>  
onlinehost=<実行系ノードのホスト名>  
standbyhost=<待機系ノードのホスト名>
4. 共有ディスク上のデータベースを使用するように設定を変更します。  
その方法を手順 5～手順 6 で説明します。  
ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、共有ディスク上のデータベースを使用するように設定を変更する手順は不要です。手順 7 に進んでください。
5. 次のコマンドを実行して、データベースを共有ディスクに移行します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64dbclustersetup -createcluster -databasepath <共有ディスク上のデータベース再作成先ディレクトリ> -exportpath <ローカルディスク上の退避データ格納先ディレクトリ> -auto



databasepath には、実行系ノードで指定した<共有ディスク上のデータベース再作成先ディレクトリ>と同じディレクトリを指定してください。



**注意** hcmds64dbclustersetup コマンドを実行すると、Device Manager と Tuning Manager の間のリモート接続の設定が初期化されます。必要に応じて再設定してください。

6. データベースが使用するポート番号を実行系ノードで変更した場合は、待機系ノードでも同じポート番号を設定します。
7. 次のコマンドを実行して、Hitachi Command Suite 製品が停止していることを確認します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmd64srv -status
8. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始されないようにします。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmd64srv -starttype manual -all
9. Compute Systems Manager がマシンの起動時に自動的に開始されないようにします。  
次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S を使用しないでください。
  - /etc/rc3.d/S99hicommand64-hcs\_csm
  - /etc/rc5.d/S99hicommand64-hcs\_csmほかの Hitachi Command Suite 製品がインストールされている場合は、その製品も自動的に開始されないようにします。操作の対象となるファイルについては、各製品のマニュアルを参照してください。
10. 次のファイルの hcsm.shared.directory プロパティに、実行系ノードで指定した、Compute Systems Manager が使用する作業ディレクトリへのパスを指定します。  
<Compute Systems Manager のインストールディレクトリ>/ComputeSystemsManager/conf/user.properties
11. 実行系ノードで、次のファイルの svp.bind.address プロパティにクラスタ管理 IP アドレスを指定した場合は、待機系ノードでも同様に指定します。  
<Compute Systems Manager のインストールディレクトリ>/ComputeSystemsManager/conf/user.properties
12. Compute Systems Manager のサービスを、クラスタ管理アプリケーションのグループに登録します。  
Compute Systems Manager をインストールする前に、ほかの Hitachi Command Suite 製品のサービスを削除した場合は、それらの製品が使用するサービスも登録します。
13. クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。

## 関連項目

- [2.4.2 インストールする前の確認事項](#)
- [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)
- [\(3\) ポートを変更する](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)
- [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)
- [9.6.2 クラスタ管理アプリケーションにサービスを登録する \(Red Hat Enterprise Linux\)](#)
- [9.7.1 クラスタ環境でウィルス検出プログラムを使用する場合に必要な設定](#)

- 9.7.2 クラスタ環境で同期が必要な設定
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)
- 9.9.9 データベースを移行するコマンド (hcmds64dbclustersetup) の書式 (Red Hat Enterprise Linux)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)
- B.2.18 管理サーバをクラスタ構成にする場合に設定が必要なプロパティ (cluster.conf)

## 9.4.4 実行系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux)

クラスタ環境の実行系ノードで、Red Hat Enterprise Linux の管理サーバの Compute Systems Manager をアップグレードまたは上書きインストールします。

### 事前に完了しておく操作

- インストールする前の確認作業
- クラスタ環境で運用する管理サーバの空き容量の確認
- クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスの削除

実行系ノードで Compute Systems Manager をアップグレードまたは上書きインストールする手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されているグループを待機系ノードから実行系ノードに移動します。
2. Hitachi Command Suite 製品が起動中の場合は、次のコマンドを実行して停止します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -stop`
3. Compute Systems Manager をアップグレードまたは上書きインストールします。  
 インストーラーの指示に従って、上書きまたはアップグレードインストール前のデータベースをバックアップしてください。
4. Hitachi Command Suite 製品が起動中の場合は、次のコマンドを実行して停止します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -stop`
5. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始されないようにします。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -starttype manual -all`
6. Compute Systems Manager がマシンの起動時に自動的に開始されないようにします。  
 次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S を使用しないでください。
  - /etc/rc3.d/S99hicommand64-hcs\_csm
  - /etc/rc5.d/S99hicommand64-hcs\_csm
 ほかの Hitachi Command Suite 製品がインストールされている場合は、その製品も自動的に開始されないようにします。操作の対象となるファイルについては、各製品のマニュアルを参照してください。



7. 次のファイルの `hcsm.shared.directory` プロパティに、**Compute Systems Manager** が使用する作業ディレクトリへのパスが指定されていることを確認します。

< *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/conf/user.properties

指定されていない場合は、共有ディスクに任意のディレクトリを作成したあと、そのディレクトリへのパスを指定します。

8. 日立製のサーバを管理対象にしている場合は、必要に応じて、日立製のサーバに登録される管理サーバの IP アドレスがクラスタ管理 IP アドレスになるように設定を変更します。

次のファイルの `svp.bind.address` プロパティに、クラスタ管理 IP アドレスを指定します。

< *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/conf/user.properties



#### 参考

- `svp.bind.address` プロパティを指定しない場合、日立製のサーバには実行系および待機系の各ノードの IP アドレスが登録されます。
- すでに運用中の日立製のサーバには、通信先の管理サーバの IP アドレスが登録されています。  
`svp.bind.address` プロパティを指定すると、プロパティに指定した IP アドレスも新しく登録されます。日立製のサーバに登録されている管理サーバの IP アドレスは、Web コンソールで確認できます。使用していない管理サーバの IP アドレスが残っている場合は削除してください。

9. クラスタ管理アプリケーションで、**Compute Systems Manager** のサービスが登録されているグループを待機系ノードに移動します。

#### 関連項目

- [2.4.2 インストールする前の確認事項](#)
- [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)
- [8.1.3 Compute Systems Manager を停止する](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)
- [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)
- [9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認](#)
- [9.6.4 クラスタ管理アプリケーションからサービスを削除する \(Red Hat Enterprise Linux\)](#)
- [B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ \(user.properties\)](#)

## 9.4.5 待機系ノードでアップグレードまたは上書きインストールする (Red Hat Enterprise Linux)

クラスタ環境の待機系ノードで、Red Hat Enterprise Linux の管理サーバの **Compute Systems Manager** をアップグレードまたは上書きインストールします。

#### 事前に確認しておく情報

- 新規インストール時に、クラスタ管理アプリケーションへのサービス登録に使用したスクリプトのファイルパス  
インストール後、クラスタ管理アプリケーションにサービスを登録するときに使用する情報です。

## 事前に完了しておく操作

- ・ インストールする前の確認作業
- ・ 実行系ノードへの Compute Systems Manager のインストール

待機系ノードで Compute Systems Manager をアップグレードまたは上書きインストールする手順を次に示します。

1. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -stop`
2. Compute Systems Manager をアップグレードまたは上書きインストールします。
3. Hitachi Command Suite 製品が起動中の場合は、次のコマンドを実行して停止します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -stop`
4. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始されないようにします。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/hcmds64srv -starttype manual -all`
5. Compute Systems Manager がマシンの起動時に自動的に開始されないようにします。  
次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S を使用しないでください。
  - /etc/rc3.d/S99hicommand64-hcs\_csm
  - /etc/rc5.d/S99hicommand64-hcs\_csmほかの Hitachi Command Suite 製品がインストールされている場合は、その製品も自動的に開始されないようにします。操作の対象となるファイルについては、各製品のマニュアルを参照してください。
6. 次のファイルの `hcsm.shared.directory` プロパティに、実行系ノードで指定した、Compute Systems Manager が使用する作業ディレクトリへのパスが指定されていることを確認します。  
`< Compute Systems Manager のインストールディレクトリ >/ComputeSystemsManager/conf/user.properties`  
指定されていない場合は、実行系ノードで `hcsm.shared.directory` プロパティに指定したパスに変更します。
7. 実行系ノードで、次のファイルの `svp.bind.address` プロパティにクラスタ管理 IP アドレスを指定している場合は、待機系ノードでも同様に指定します。  
`< Compute Systems Manager のインストールディレクトリ >/ComputeSystemsManager/conf/user.properties`
8. クラスタ管理アプリケーションのグループから削除したサービスを再登録します。
9. クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。

## 関連項目

- ・ [2.4.2 インストールする前の確認事項](#)
- ・ [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)
- ・ [8.1.3 Compute Systems Manager を停止する](#)
- ・ [9.1 クラスタを使用するための環境設定と運用とは](#)
- ・ [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)
- ・ [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)

- 9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux)
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

## 9.5 クラスタ環境への移行

### 9.5.1 クラスタ環境に移行する (Windows)

非クラスタ環境で運用していた Windows の管理サーバを、クラスタ環境に移行します。

#### 事前に完了しておく操作

- インストールする前の確認作業
- クラスタ環境で運用する管理サーバの空き容量の確認
- クラスタ管理アプリケーションを使用して設定する前の確認
- デプロイメントマネージャーを使用している場合は、既存のイメージファイルの共有ディスクへの移動
- Compute Systems Manager が使用する作業ディレクトリの、共有ディスクへの移動  
 Compute Systems Manager が使用する作業ディレクトリの下に、すでにサブディレクトリやファイルなどが格納されているか確認してください。すでにサブディレクトリやファイルなどが格納されている場合は、共有ディスクに Compute Systems Manager が使用する作業ディレクトリを移動してください。  
 Compute Systems Manager が使用する作業ディレクトリについては、次のファイルに定義する hcsml.shared.directory プロパティの説明を参照してください。  
`< Compute Systems Manager のインストールディレクトリ >%ComputeSystemsManager%conf\user.properties`
- データベースが使用するポート番号の確認  
 クラスタ環境に移行すると、データベースが使用するポート番号がデフォルト (22032/tcp) に設定されます。  
 ポート番号をデフォルト以外の番号に変更して運用している場合は、ポート番号を控えておいてください。
- アンインストール前の確認作業  
 クラスタ環境に移行するには、Compute Systems Manager を含む Hitachi Command Suite 製品をいったんアンインストールする必要があります。  
 クラスタ環境に移行すると、設定がすべて初期化されます。設定をデフォルトから変更している場合は、設定内容を控えておいてください。

非クラスタ環境で運用していた Compute Systems Manager を、クラスタ環境に移行する手順を次に示します。

1. 次のコマンドを実行して、データベースをエクスポートします。  
 ほかの Hitachi Command Suite 製品がインストールされている場合は、その製品のデータベースもエクスポートされます。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin%hcmds64dbtrans /export /workpath <作業用ディレクトリ> /file <アーカイブファイル> /auto`
2. Compute Systems Manager をアンインストールします。

ほかの Hitachi Command Suite 製品がインストールされている場合は、その製品もアンインストールしてください。

3. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を実行系ノードに移動し、クラスタ管理 IP アドレスと共有ディスクをオンラインにします。
4. 実行系ノードに Compute Systems Manager をインストールします。  
インストールウィザードでは、クラスタ構成でのインストールを選択して、それぞれの画面で必要な情報を指定します。ほかの Hitachi Command Suite 製品ですでにクラスタ環境が構築されている場合は、その設定が適用されるため、再度指定する必要はありません。
5. 次のコマンドを実行して、エクスポートしたデータベースをインポートします。  

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin  
%hcmts64dbtrans /import /workpath <作業用ディレクトリ> /file <アーカイブ  
ファイル> /type ALL /auto
```
6. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を待機系ノードに移動します。
7. 待機系ノードに Compute Systems Manager をインストールします。  
インストールの際には、次の条件に従ってください。
  - インストール先を実行系ノードと同じにしてください。
  - 実行系ノードでデプロイメントマネージャーをインストールした場合は、待機系ノードでもインストールしてください。
8. データベースが使用するポート番号をデフォルト以外の番号に変更して運用する場合は、控えておいたポート番号を実行系および待機系の各ノードで設定します。



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている場合は、その製品が使用するポート番号と競合しないことを確認してください。

9. 日立製のサーバを管理対象にする場合は、必要に応じて、日立製のサーバに登録される管理サーバの IP アドレスがクラスタ管理 IP アドレスになるように設定を変更します。  
実行系および待機系の各ノードで、次のファイルの `svp.bind.address` プロパティに、クラスタ管理 IP アドレスを指定します。  

```
< Compute Systems Manager のインストールディレクトリ >%ComputeSystemsManager  
%conf%user.properties
```



#### 参考

- `svp.bind.address` プロパティを指定しない場合、日立製のサーバには実行系および待機系の各ノードの IP アドレスが登録されます。
- すでに運用中の日立製のサーバには、通信先の管理サーバの IP アドレスが登録されています。  
`svp.bind.address` プロパティを指定すると、プロパティに指定した IP アドレスも新しく登録されます。日立製のサーバに登録されている管理サーバの IP アドレスは、Web コンソールで確認できます。  
使用していない管理サーバの IP アドレスが残っている場合は削除してください。

10. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
%ClusterSetup%hcmts64clustersrvstate /son /r <グループ名>
```
11. プラグインライセンスを登録する場合は、待機系ノードでライセンスキーを入力します。
12. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を実行系ノードに移動します。
13. 待機系ノードでプラグインライセンスを登録した場合は、実行系ノードでも同様にライセンスキーを入力します。

14. デプロイメントマネージャーをインストールした場合は、デプロイメントマネージャーを使用するためのクラスタ環境を設定します。
15. デプロイメントマネージャーのイメージファイルを共有ディスクに移動した場合は、イメージファイルをインポートします。  
イメージファイルのインポートなど、デプロイメントマネージャーのイメージファイルの管理については、マニュアル「*Hitachi Command Suite Compute Systems Manager ユーザーズガイド*」を参照してください。
16. 非クラスタ環境で運用していた時に、Device Manager が Tuning Manager とリモート接続していた場合は、必要に応じて、Tuning Manager のサービスを起動したあと、Tuning Manager と連携するための設定を再度実施します。

#### 関連項目

- 2.4.2 インストールする前の確認事項
- 2.4.3 Compute Systems Manager をインストールする (Windows)
- 2.6.2 アンインストールするための確認事項
- 2.6.3 アンインストールする (Windows)
- (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (3) ポートを変更する
- 7.2 デプロイメントマネージャーをインストールするための前提条件
- 7.5 デプロイメントマネージャーをインストールする
- 8.2.6 データベースを移行するための確認事項
- 8.2.7 移行元サーバからデータベースをエクスポートする
- 8.2.8 移行先サーバにデータベースをインポートする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.3.1 クラスタ運用を開始する環境設定手順の確認
- 9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認
- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認
- 9.7.1 クラスタ環境でウイルス検出プログラムを使用する場合に必要な設定
- 9.7.2 クラスタ環境で同期が必要な設定
- 9.7.3 デプロイメントマネージャーを使用する場合のクラスタ環境を設定する
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

## 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)

非クラスタ環境で運用していた Red Hat Enterprise Linux の管理サーバを、クラスタ環境に移行します。

#### 事前に完了しておく操作

- インストールする前の確認作業
- クラスタ環境で運用する管理サーバの空き容量の確認
- クラスタ管理アプリケーションを使用して設定する前の確認

- **Compute Systems Manager** が使用する作業ディレクトリの、共有ディスクへの移動  
**Compute Systems Manager** が使用する作業ディレクトリの下に、すでにサブディレクトリやファイルなどが格納されているか確認してください。すでにサブディレクトリやファイルなどが格納されている場合は、共有ディスクに **Compute Systems Manager** が使用する作業ディレクトリを移動してください。  
**Compute Systems Manager** が使用する作業ディレクトリについては、次のファイルに定義する `hcsm.shared.directory` プロパティの説明を参照してください。  
 < *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/conf/user.properties
- データベースが使用するポート番号の確認  
 移行の手順で `hcmds64dbclustersetup` コマンドを実行すると、データベースが使用するポート番号がデフォルト (`22032/tcp`) に設定されます。  
 ポート番号をデフォルト以外の番号に変更して運用している場合は、ポート番号を控えておいてください。

非クラスタ環境で運用していた **Compute Systems Manager** を、クラスタ環境に移行する手順を次に示します。

ここでは、すでに運用中の **Compute Systems Manager** がインストールされたマシンを実行系ノードとする場合を想定して説明します。

1. 待機系ノードとなるマシンに **Compute Systems Manager** をインストールします。
2. プラグインライセンスが必要な場合は、待機系ノードの IP アドレスでログイン画面にアクセスして、ライセンスキーを入力してください。
3. 実行系ノードで次のコマンドを実行して、**Compute Systems Manager** にアクセスする URL を論理ホスト名に変更します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64chgurl -change http://<実行系ノードの IP アドレスまたはホスト名>:<  
ポート番号> http://<論理ホスト名>:<ポート番号>
```

4. 実行系および待機系の各ノードで、クラスタ設定ファイルを作成します。ほかの **Hitachi Command Suite** 製品でクラスタ環境が構築されている場合、この手順は不要です。

クラスタ設定ファイルは、テキストファイルで次の場所に格納します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /conf/  
cluster.conf
```

実行系ノードのクラスタ設定ファイルの内容を次に示します。mode には online を指定する必要があります。

```
mode=online
```

```
virtualhost=<論理ホスト名>
```

```
onlinehost=<実行系ノードのホスト名>
```

```
standbyhost=<待機系ノードのホスト名>
```

待機系ノードの場合は、次の内容をクラスタ設定ファイルに記述してください。mode には standby を指定する必要があります。

```
mode=standby
```

```
virtualhost=<論理ホスト名>
```

```
onlinehost=<実行系ノードのホスト名>
```

```
standbyhost=<待機系ノードのホスト名>
```

5. 実行系ノードで次のコマンドを実行して、データベースをバックアップします。



```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64backups -dir <ローカルディスク上のバックアップファイル格納先ディレクトリ  
> -auto
```

6. 実行系ノードで次のコマンドを実行して、データベースを共有ディスクに移行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64dbclustersetup -createcluster -databasepath <共有ディスク上のデー  
タベース再作成先ディレクトリ > -exportpath <ローカルディスク上の退避データ格納先  
ディレクトリ > -auto
```

7. 待機系ノードで次のコマンドを実行して、共有ディスク上のデータベースを使用するように設定を変更します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64dbclustersetup -createcluster -databasepath <共有ディスク上のデー  
タベース再作成先ディレクトリ > -exportpath <ローカルディスク上の退避データ格納先  
ディレクトリ > -auto
```

databasepath には、実行系ノードで指定した <共有ディスク上のデータベース再作成先ディ  
レクトリ > と同じディレクトリを指定してください。



#### 注意

- hcms64dbclustersetup コマンドを実行すると、Device Manager と Tuning Manager の間のリ  
モート接続の設定が初期化されます。必要に応じて、実行系および待機系の各ノードで再設定してく  
ださい。
- 共有ディスク上に、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品 (Hitachi  
File Services Manager および Hitachi Storage Navigator Modular 2) のデータベースが作成されてい  
る場合、databasepath オプションには別のディレクトリを指定する必要があります。

8. データベースが使用するポート番号をデフォルト以外の番号に変更して運用する場合は、控えて  
おいたポート番号を実行系および待機系の各ノードで設定します。



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品 (Hitachi File Services  
Manager および Hitachi Storage Navigator Modular 2) がインストールされている場合は、その製品が  
使用するポート番号と競合しないことを確認してください。

9. 実行系および待機系の各ノードで次のコマンドを実行して、Hitachi Command Suite 製品が停  
止していることを確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64srv -status
```

10. 実行系および待機系の各ノードで次のコマンドを実行して、Hitachi Command Suite 製品の  
サービスがマシンの起動時に自動的に開始されないようにします。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64srv -starttype manual -all
```

11. 実行系および待機系の各ノードで、Compute Systems Manager がマシンの起動時に自動的  
に開始されないようにします。

次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する  
場合は、変更後のファイル名の先頭文字に **k** と **s** を使用しないでください。

- /etc/rc3.d/S99hicommand64-hcs\_csm

- /etc/rc5.d/S99hicommand64-hcs\_csm

ほかの Hitachi Command Suite 製品がインストールされている場合は、その製品も自動的に開  
始されないようにします。操作の対象となるファイルについては、各製品のマニュアルを参照し  
てください。

12. 実行系および待機系の各ノードで、次のファイルの hcsm.shared.directory プロパティに、  
Compute Systems Manager が使用する作業ディレクトリへのパスを指定します。

あらかじめ **Compute Systems Manager** が使用する作業ディレクトリを共有ディスクに移動してあれば、そのディレクトリへのパスを指定します。移動していなければ、共有ディスクに任意のディレクトリを作成したあと、そのディレクトリへのパスを指定します。

< *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/conf/user.properties

- 日立製のサーバを管理対象にしている場合は、必要に応じて、日立製のサーバに登録される管理サーバの IP アドレスがクラスタ管理 IP アドレスになるように設定を変更します。

実行系および待機系の各ノードで、次のファイルの `svp.bind.address` プロパティに、クラスタ管理 IP アドレスを指定します。

< *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/conf/user.properties



#### 参考

- `svp.bind.address` プロパティを指定しない場合、日立製のサーバには実行系および待機系の各ノードの IP アドレスが登録されます。
- すでに運用中の日立製のサーバには、通信先の管理サーバの IP アドレスが登録されています。  
`svp.bind.address` プロパティを指定すると、プロパティに指定した IP アドレスも新しく登録されます。日立製のサーバに登録されている管理サーバの IP アドレスは、Web コンソールで確認できます。  
使用していない管理サーバの IP アドレスが残っている場合は削除してください。

- Compute Systems Manager** のサービスを、クラスタ管理アプリケーションのグループに登録します。

- クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。

#### 関連項目

- [2.4.2 インストールする前の確認事項](#)
- [2.4.4 Compute Systems Manager をインストールする \(Linux\)](#)
- [\(1\) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [\(3\) ポートを変更する](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)
- [9.3.1 クラスタ運用を開始する環境設定手順の確認](#)
- [9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認](#)
- [9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認](#)
- [9.6.2 クラスタ管理アプリケーションにサービスを登録する \(Red Hat Enterprise Linux\)](#)
- [9.7.1 クラスタ環境でウイルス検出プログラムを使用する場合に必要な設定](#)
- [9.7.2 クラスタ環境で同期が必要な設定](#)
- [9.8.4 Compute Systems Manager のクラスタ運用を開始する \(Red Hat Enterprise Linux\)](#)
- [9.9.2 クラスタ環境でデータベースをバックアップする \(Red Hat Enterprise Linux\)](#)
- [9.9.9 データベースを移行するコマンド \(hcmds64dbclustersetup\) の書式 \(Red Hat Enterprise Linux\)](#)
- [B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ \(user.properties\)](#)
- [B.2.18 管理サーバをクラスタ構成にする場合に設定が必要なプロパティ \(cluster.conf\)](#)



## 9.6 クラスタ管理アプリケーションへのサービスの登録と削除

### 9.6.1 クラスタ管理アプリケーションにサービスを登録する (Windows)

Windows のクラスタ管理アプリケーションのグループに、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスを登録します。

サービスの登録には、Hitachi Command Suite 共通コンポーネントのコマンドを使用します。



**重要** Hitachi Command Suite 製品のサービスは、インストール時に自動的に登録されるため、通常はこのコマンドを実行する必要はありません。誤ってサービスを削除したなどの理由で、サービスを登録し直す必要がある場合にだけ実行してください。

#### 事前に完了しておく操作

- ・ ドメインの Administrator 権限を持つユーザーでのログイン
- ・ クラスタ管理アプリケーションでの、サービスを登録するグループの作成

クラスタ管理アプリケーションのグループにサービスを登録するには、次のコマンドを実行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%ClusterSetup  
%hcnds64clustersrvupdate /sreg /r <グループ名> /sd <共有ディスクのドライブ文字  
> /ap <クライアントアクセスポイントのリソース名>
```

#### sreg

クラスタ管理アプリケーションのグループに、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスを登録するためのオプションです。

#### r

Compute Systems Manager を含む Hitachi Command Suite 製品のサービスを登録するグループ名を指定します。グループ名に次の文字が含まれる場合は、グループ名を引用符 (") で囲んで指定してください。

半角スペース, ; =

#### sd

クラスタ管理アプリケーションに登録されている共有ディスクのドライブ文字を指定します。このオプションには複数のドライブ文字を指定できません。Hitachi Command Suite 製品のデータベースを複数の共有ディスクに分割している場合は、共有ディスクごとに hcnds64clustersrvupdate コマンドを実行してください。

#### ap

クラスタ管理アプリケーションに登録されているクライアントアクセスポイントのリソース名を指定します。



#### 参考

- ・ デプロイメントマネージャーがインストールされている場合は、デプロイメントマネージャーのサービスも登録されます。
  - ・ 管理サーバにほかの Hitachi Command Suite 製品がインストールされている場合は、その製品のサービスも登録されます。
- ほかの Hitachi Command Suite 製品のサービスについては、各製品のマニュアルを参照してください。

## 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス
- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認

## 9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux)

Red Hat Enterprise Linux のクラスタ管理アプリケーションのグループに、Compute Systems Manager のサービスを登録します。

はじめに、クラスタ環境でサービスを制御するためのスクリプトを作成します。そのあと、クラスタ管理アプリケーションで、作成したスクリプトを指定してサービスを登録します。

### 事前に完了しておく操作

- クラスタ管理アプリケーションでの、サービスを登録するグループの作成

クラスタ管理アプリケーションのグループにサービスを登録する手順を次に示します。

1. インストールメディアから、スクリプトのサンプルファイルを任意の場所にコピーします。  
サンプルファイルの格納先：<DVD ドライブ>/SAMPLE/CLUSTER\_TOOL  
次に示す zip ファイルをコピーします。
  - HCS\_LinuxCluster\_SampleScripts\_Common.zip  
Hitachi Command Suite 共通コンポーネントのサービスを制御するスクリプトが格納されています。
  - HCS\_LinuxCluster\_SampleScripts\_HCSM.zip  
Compute Systems Manager のサービスを制御するスクリプトが格納されています。
2. コピーした zip ファイルを任意の場所に解凍します。  
解凍先に作成されるスクリプトを次に示します。
  - sc\_hbase64\_hirdb
  - sc\_hbase64\_hssso
  - sc\_hbase64\_hweb
  - sc\_hbase64\_web
  - sc\_hbase64\_csm
3. 各スクリプトに定義されているプロパティを、次のとおり編集します。
  - HCMDS\_HOME  
Hitachi Command Suite 共通コンポーネントのインストールディレクトリのパスを指定します。  
sc\_hbase64\_hirdb ファイルの場合は、次のプロパティも編集します。
  - PDHOST  
論理ホスト名を指定します。
4. 実行系および待機系の各ノードの/etc/init.dディレクトリに、編集したスクリプトを格納します。
5. 実行系および待機系の各ノードで次のコマンドを実行して、スクリプトに実行権限を割り当てます。

chmod u+x <スクリプトのファイル名>

- クラスタ管理アプリケーションで、Compute Systems Manager のクラスタ運用を一時停止します。
- クラスタ管理アプリケーションで、[Add Resource] ボタンをクリックしたあと、[Add Resource to Service] から [Script] を選択し、サービスを登録します。  
サービスを登録する順番、および各項目に指定する値を次に示します。

表 9-1 クラスタ管理アプリケーションでサービスを登録する順番および各項目に指定する値

順番	サービス名	スクリプト名 (任意)	スクリプトのファイルパス
1	HiRDB	sc_hbase64_hirdb	/etc/init.d/ sc_hbase64_hirdb
2	HBase 64 Storage Mgmt SSO Service	sc_hbase64_hssso	/etc/init.d/ sc_hbase64_hssso
3	HBase 64 Storage Mgmt Web SSO Service	sc_hbase64_hweb	/etc/init.d/ sc_hbase64_hweb
4	HBase 64 Storage Mgmt Web Service	sc_hbase64_web	/etc/init.d/ sc_hbase64_web
5	HCS Compute Systems Manager Web Service	sc_hbase64_csm	/etc/init.d/ sc_hbase64_csm

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、その製品のサービスも登録します。

登録する手順については、各製品のマニュアルを参照してください。

- [Submit] ボタンをクリックします。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス
- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認
- 9.8.2 Compute Systems Manager のクラスタ運用を一時停止する (Red Hat Enterprise Linux)

### 9.6.3 クラスタ管理アプリケーションからサービスを削除する (Windows)

Windows のクラスタ管理アプリケーションのグループから、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスを削除します。

サービスの削除には、Hitachi Command Suite 共通コンポーネントのコマンドを使用します。



**重要** Hitachi Command Suite 製品のサービスは、アンインストール時に自動的に削除されるため、通常はこのコマンドを実行する必要はありません。  
誤ってサービスの設定を変更したなどの理由で、サービスをいったん削除する必要がある場合にだけ実行してください。

#### 事前に完了しておく操作

- ドメインの Administrator 権限を持つユーザーでのログイン

クラスタ管理アプリケーションのグループからサービスを削除するには、次のコマンドを実行します。

コマンドは、次のどちらかの方法で実行できます。

- インストールメディアから実行する  
    < *Compute Systems Manager* のインストールメディア > ¥HCS¥ClusterSetup  
    ¥hcmds64clustersrvupdate /sdel /r <グループ名 >
- Hitachi Command Suite 製品のインストールディレクトリから実行する  
    < *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ >  
    ¥ClusterSetup¥hcmds64clustersrvupdate /sdel /r <グループ名 >

sdel

クラスタ管理アプリケーションのグループから、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスを削除するためのオプションです。

r

Compute Systems Manager を含む Hitachi Command Suite 製品のサービスが登録されているグループ名を指定します。グループ名に次の文字が含まれる場合は、グループ名を引用符 (" ) で囲んで指定してください。

半角スペース , ; =



#### 重要

- r オプションで指定したグループに登録されている、Compute Systems Manager および Hitachi Command Suite 製品のサービスがすべて削除されます。ただし、Hitachi File Services Manager のサービスは削除されません。  
ほかの Hitachi Command Suite 製品のサービスについては、各製品のマニュアルを参照してください。
- サービスのリソース名を変更している場合、サービスを削除したあとに再登録すると、リソース名がすべて初期化されます。必要に応じて、サービスを削除する前のリソース名を控えておき、再登録後に変更してください。

#### 関連項目

- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)

## 9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux)

Red Hat Enterprise Linux のクラスタ管理アプリケーションのグループから、Compute Systems Manager のサービスを削除します。

クラスタ管理アプリケーションのグループからサービスを削除する手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のクラスタ運用を一時停止します。
2. クラスタ管理アプリケーションで、次のサービスの [Remove] をクリックしてサービスを削除します。
  - HiRDB
  - HBase 64 Storage Mgmt SSO Service
  - HBase 64 Storage Mgmt Web SSO Service
  - HBase 64 Storage Mgmt Web Service
  - HCS Compute Systems Manager Web Service

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、必要に応じてその製品のサービスも削除します。

削除する手順については、各製品のマニュアルを参照してください。

3. [Submit] ボタンをクリックします。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス
- 9.8.2 Compute Systems Manager のクラスタ運用を一時停止する (Red Hat Enterprise Linux)

## 9.7 新規インストールまたはクラスタ環境に移行した後の環境設定

### 9.7.1 クラスタ環境でウイルス検出プログラムを使用する場合に必要な設定

共有ディスクを管理するマシン上でウイルス検出プログラムを使用する場合は、データベースを移行したときに指定した共有ディスク上のディレクトリを、スキャン対象から外してください。

ウイルス検出プログラムが、共有ディスクにあるデータベース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によって障害が発生するおそれがあります。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.5.1 クラスタ環境に移行する (Windows)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)
- D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)

### 9.7.2 クラスタ環境で同期が必要な設定

実行系ノードと待機系ノードで同期が必要な設定項目を示します。

- 警告バナーのメッセージ設定
- パスワードポリシーの設定
- 自動アカウントロックまでのログイン連続失敗回数

また、クラスタ環境で、Compute Systems Manager をインストールしたあとに Hitachi Command Suite 製品の設定を変更する場合は、すべてのノードで設定内容が同じになるよう設定してください。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux)

- 9.5.1 クラスタ環境に移行する (Windows)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)

## 9.7.3 デプロイメントマネージャーを使用する場合のクラスタ環境を設定する

デプロイメントマネージャーを使用する場合のクラスタ環境を設定します。

### 事前に完了しておく操作

- デプロイメントマネージャーのクラスタ環境へのインストール

デプロイメントマネージャーを使用する場合のクラスタ環境を設定する手順を次に示します。

1. **Compute Systems Manager** にログインし、[管理] タブからデプロイメントマネージャーの設定を選択して、次のように指定します。  
 [イメージファイル格納デフォルトパス]: 共有ディスク上のディレクトリを指定します。  
 [デプロイメントマネージャーが使用する IP アドレス]: [クラスタ IP アドレスまたは指定の IP アドレス] を選択して、クラスタ管理 IP アドレスを指定します。  
 [DHCP サーバはデプロイメントマネージャーと同じ IP アドレスを使用する]: 環境に合わせて選択します。  
 設定変更のタスクが完了したら、手順 2~手順 3 を実行してサービスを再起動します。
2. 次のコマンドを実行して、**Compute Systems Manager** のクラスタ運用を一時停止します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
 %ClusterSetup%hcmds64clustersrvstate /soff /r <グループ名 >`
3. 次のコマンドを実行して、**Compute Systems Manager** のクラスタ運用を開始します。  
`< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
 %ClusterSetup%hcmds64clustersrvstate /son /r <グループ名 >`

### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.4.1 クラスタ環境にインストールする (Windows)
- 9.5.1 クラスタ環境に移行する (Windows)
- 9.8.1 **Compute Systems Manager** のクラスタ運用を一時停止する (Windows)
- 9.8.3 **Compute Systems Manager** のクラスタ運用を開始する (Windows)
- D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)

## 9.8 クラスタ環境での Compute Systems Manager の起動と停止

### 9.8.1 Compute Systems Manager のクラスタ運用を一時停止する (Windows)

クラスタ構成となっている Windows の管理サーバで、クラスタ環境を設定するために **Compute Systems Manager** のクラスタ運用を一時停止します。

クラスタでの運用を一時停止するには、次のコマンドを実行します。

コマンドは、次のどちらかの方法で実行できます。

- インストールメディアから実行する  
    < *Compute Systems Manager* のインストールメディア > ¥HCS¥ClusterSetup  
    ¥hcnds64clustersrvstate /soff /r <グループ名>
- Hitachi Command Suite 製品のインストールディレクトリから実行する  
    < *Hitachi Command Suite* 共通コンポーネントのインストールディレクトリ >  
    ¥ClusterSetup¥hcnds64clustersrvstate /soff /r <グループ名>

soff

クラスタ管理アプリケーションのグループに登録されている、*Compute Systems Manager* を含む *Hitachi Command Suite* 製品のサービスをオフラインにし、フェールオーバーを抑制するためのオプションです。

r

*Compute Systems Manager* を含む *Hitachi Command Suite* 製品のサービスが登録されているグループ名を指定します。グループ名に次の文字が含まれる場合は、グループ名を引用符 (") で囲んで指定してください。

半角スペース, ; =

*Compute Systems Manager* を含む *Hitachi Command Suite* 製品のサービスが登録されているグループがオフラインになり、フェールオーバーが抑止されます。

#### 関連項目

- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する \*Compute Systems Manager\* のサービス](#)

## 9.8.2 *Compute Systems Manager* のクラスタ運用を一時停止する (Red Hat Enterprise Linux)

クラスタ構成となっている Red Hat Enterprise Linux の管理サーバで、クラスタ環境を設定するために *Compute Systems Manager* のクラスタ運用を一時停止します。

クラスタでの運用を一時停止する手順を次に示します。

1. クラスタ管理アプリケーションで [Service Groups] ウィンドウを開き、*Compute Systems Manager* を含む *Hitachi Command Suite* 製品のサービスが登録されているグループを選択します。
2. [stop (disable)] アイコンをクリックして、グループを停止し、無効にします。

*Compute Systems Manager* を含む *Hitachi Command Suite* 製品のサービスが登録されているグループがオフラインになり、フェールオーバーが抑止されます。

#### 関連項目

- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する \*Compute Systems Manager\* のサービス](#)

## 9.8.3 *Compute Systems Manager* のクラスタ運用を開始する (Windows)

クラスタ構成となっている Windows の管理サーバで、*Compute Systems Manager* のクラスタ運用を開始します。



クラスタでの運用を開始するには、次のコマンドを実行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%ClusterSetup  
%hcmds64clustersrvstate /son /r <グループ名>
```

son

クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスをオンラインにし、フェールオーバーを有効にするためのオプションです。

r

Compute Systems Manager を含む Hitachi Command Suite 製品のサービスが登録されているグループ名を指定します。グループ名に次の文字が含まれる場合は、グループ名を引用符 (") で囲んで指定してください。

半角スペース , ; =

Compute Systems Manager を含む Hitachi Command Suite 製品のサービスが登録されているグループがオンラインになり、フェールオーバーが有効になります。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス

## 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)

クラスタ構成となっている Red Hat Enterprise Linux の管理サーバで、Compute Systems Manager のクラスタ運用を開始します。

クラスタでの運用を開始する手順を次に示します。

1. クラスタ管理アプリケーションで [Service Groups] ウィンドウを開き、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスが登録されているグループを選択します。
2. ドロップダウンリストから実行系または待機系ノードを選択して、[start] アイコンをクリックします。

Compute Systems Manager を含む Hitachi Command Suite 製品のサービスが登録されているグループがオンラインになり、フェールオーバーが有効になります。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.2 クラスタを運用するために使用する Compute Systems Manager のサービス

## 9.9 クラスタ環境でのデータベースの管理

### 9.9.1 クラスタ環境でデータベースをバックアップする (Windows)

クラスタ構成となっている Windows の管理サーバで、データベースをバックアップします。

データベースのバックアップは、実行系ノードで操作します。



## 事前に完了しておく操作

- データベースをバックアップするための確認作業

クラスタ環境でデータベースをバックアップする手順を次に示します。



**注意** Compute Systems Manager と同じ管理サーバにインストールされている Device Manager が Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager をいったん停止しておく必要があります。

データベースのバックアップが完了したあと、Tuning Manager を再開させてください。

Tuning Manager を停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。

1. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を一時停止します。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞  
¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
2. 次のコマンドを実行して、データベースをバックアップします。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞¥bin  
¥hcmds64backups /dir <ローカルディスク上のバックアップファイル格納先ディレクトリ>  
> /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。
3. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞¥bin  
¥hcmds64srv /stop
4. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスが停止していること、またはコマンドの戻り値が 0 であることを確認します。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞¥bin  
¥hcmds64srv /statusall
5. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  
＜Hitachi Command Suite 共通コンポーネントのインストールディレクトリ＞  
¥ClusterSetup¥hcmds64clustersrvstate /son /r <グループ名>

## 関連項目

- [8.1.3 Compute Systems Manager を停止する](#)
- [8.2.2 データベースをバックアップするための確認事項](#)
- [8.2.3 データベースをバックアップする](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.8.1 Compute Systems Manager のクラスタ運用を一時停止する \(Windows\)](#)
- [9.8.3 Compute Systems Manager のクラスタ運用を開始する \(Windows\)](#)

## 9.9.2 クラスタ環境でデータベースをバックアップする (Red Hat Enterprise Linux)

クラスタ構成となっている Red Hat Enterprise Linux の管理サーバで、データベースをバックアップします。

データベースのバックアップは、実行系ノードで操作します。

## 事前に確認しておく情報

- 新規インストール時に、クラスタ管理アプリケーションへのサービス登録に使用したスクリプトのファイルパス  
データベースのバックアップ後、クラスタ管理アプリケーションにサービスを登録するときに使用する情報です。

## 事前に完了しておく操作

- データベースをバックアップするための確認作業
- クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスの削除

クラスタ環境でデータベースをバックアップする手順を次に示します。

- クラスタ管理アプリケーションのグループが、実行系ノードに移動していることを確認します。  
グループが待機系ノードに移動している場合は、実行系ノードに移動します。
- 次のコマンドを実行して、Hitachi Command Suite 製品のサービスが停止していること、またはコマンドの戻り値が 0 であることを確認します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64srv -statusall
- 次のコマンドを実行して、データベースをバックアップします。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64backups -dir <ローカルディスク上のバックアップファイル格納先ディレクトリ > -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。
- 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64srv -stop
- 次のコマンドを実行して、Hitachi Command Suite 製品のサービスが停止していること、またはコマンドの戻り値が 0 であることを確認します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcms64srv -statusall
- クラスタ管理アプリケーションのグループから削除したサービスを再登録します。
- クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。

## 関連項目

- [8.1.3 Compute Systems Manager を停止する](#)
- [8.2.2 データベースをバックアップするための確認事項](#)
- [8.2.3 データベースをバックアップする](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.6.2 クラスタ管理アプリケーションにサービスを登録する \(Red Hat Enterprise Linux\)](#)
- [9.6.4 クラスタ管理アプリケーションからサービスを削除する \(Red Hat Enterprise Linux\)](#)
- [9.8.4 Compute Systems Manager のクラスタ運用を開始する \(Red Hat Enterprise Linux\)](#)

### 9.9.3 クラスタ環境でデータベースをリストアする (Windows)

クラスタ構成となっている Windows の管理サーバで、データベースをリストアします。

データベースのリストアは、実行系ノードで操作します。

#### 事前に完了しておく操作

- データベースをリストアするための確認作業

クラスタ環境でデータベースをリストアする手順を次に示します。



**注意** Compute Systems Manager と同じ管理サーバにインストールされている Device Manager が Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager をいったん停止しておく必要があります。データベースのリストアが完了したあと、Tuning Manager を再開させてください。

Tuning Manager を停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。

1. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を一時停止します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
%ClusterSetup%hcmds64clustersrvstate /soff /r <グループ名 >
2. 次のコマンドを実行して、データベースをリストアします。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%bin  
%hcmds64db /restore <バックアップファイル > /type ALL  
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。
3. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
%ClusterSetup%hcmds64clustersrvstate /son /r <グループ名 >
4. GUI で Compute Systems 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。
5. Device Manager が Tuning Manager とリモート接続していた場合は、データベースのリストアによって設定が初期化されるため、再設定します。

#### 関連項目

- 8.2.4 データベースをリストアするための確認事項
- 8.2.5 データベースをリストアする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.8.1 Compute Systems Manager のクラスタ運用を一時停止する (Windows)
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)

### 9.9.4 クラスタ環境でデータベースをリストアする (Red Hat Enterprise Linux)

クラスタ構成となっている Red Hat Enterprise Linux の管理サーバで、データベースをリストアします。

データベースのリストアは、実行系ノードで操作します。

### 事前に確認しておく情報

- 新規インストール時に、クラスタ管理アプリケーションへのサービス登録に使用したスクリプトのファイルパス  
データベースのリストア後、クラスタ管理アプリケーションにサービスを登録するときに使用する情報です。

### 事前に完了しておく操作

- データベースをリストアするための確認作業
- クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスの削除

クラスタ環境でデータベースをリストアする手順を次に示します。

- クラスタ管理アプリケーションのグループが、実行系ノードに移動していることを確認します。  
グループが待機系ノードに移動している場合は、実行系ノードに移動します。
- 次のコマンドを実行して、データベースをリストアします。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcms64db -restore <バックアップファイル> -type ALL  
  
restore  
hcms64backups 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。
- 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcms64srv -stop
- クラスタ管理アプリケーションのグループから削除したサービスを再登録します。
- クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。
- GUI で、Compute Systems 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。

### 関連項目

- [8.1.3 Compute Systems Manager を停止する](#)
- [8.2.4 データベースをリストアするための確認事項](#)
- [8.2.5 データベースをリストアする](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.6.2 クラスタ管理アプリケーションにサービスを登録する \(Red Hat Enterprise Linux\)](#)
- [9.6.4 クラスタ管理アプリケーションからサービスを削除する \(Red Hat Enterprise Linux\)](#)
- [9.8.4 Compute Systems Manager のクラスタ運用を開始する \(Red Hat Enterprise Linux\)](#)

## 9.9.5 クラスタ環境でデータベースをエクスポートする (Windows)

クラスタ構成となっている Windows の管理サーバで、データベースをエクスポートします。

データベースのエクスポートは、実行系ノードで操作します。

## 事前に完了しておく操作

- データベースを移行するための確認作業

クラスタ環境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。



**注意** Compute Systems Manager と同じ管理サーバにインストールされている Device Manager が Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager をいったん停止しておく必要があります。

データベースのエクスポートが完了したあと、Tuning Manager を再開させてください。

Tuning Manager を停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。

1. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を一時停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名 >
```

2. 次のコマンドを実行して、データベースをエクスポートします。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin  
¥hcmds64dbtrans /export /workpath <作業用ディレクトリ > /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。

アーカイブファイルを作成できなかった場合、十分な容量を確保したあとに再度エクスポートしてください。

3. アーカイブファイルを移行先サーバに転送します。
4. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin  
¥hcmds64srv /stop
5. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcmds64clustersrvstate /son /r <グループ名 >

## 関連項目

- 8.1.3 Compute Systems Manager を停止する
- 8.2.6 データベースを移行するための確認事項
- 8.2.7 移行元サーバからデータベースをエクスポートする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.8.1 Compute Systems Manager のクラスタ運用を一時停止する (Windows)
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)

## 9.9.6 クラスタ環境でデータベースをエクスポートする (Red Hat Enterprise Linux)

クラスタ構成となっている Red Hat Enterprise Linux の管理サーバで、データベースをエクスポートします。

データベースのエクスポートは、実行系ノードで操作します。

### 事前に確認しておく情報

- 新規インストール時に、クラスタ管理アプリケーションへのサービス登録に使用したスクリプトのファイルパス  
データベースのエクスポート後、クラスタ管理アプリケーションにサービスを登録するときに使用する情報です。

### 事前に完了しておく操作

- データベースを移行するための確認作業
- クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスの削除

クラスタ環境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。

1. クラスタ管理アプリケーションのグループが、実行系ノードに移動していることを確認します。グループが待機系ノードに移動している場合は、実行系ノードに移動します。

2. 次のコマンドを実行して、データベースをエクスポートします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64dbtrans -export -workpath <作業用ディレクトリ> -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。

アーカイブファイルを作成できなかった場合、十分な容量を確保したあとに再度エクスポートしてください。

3. アーカイブファイルを移行先サーバに転送します。
4. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64srv -stop
```
5. クラスタ管理アプリケーションのグループから削除したサービスを再登録します。
6. クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。

### 関連項目

- [8.1.3 Compute Systems Manager を停止する](#)
- [8.2.6 データベースを移行するための確認事項](#)



- 8.2.7 移行元サーバからデータベースをエクスポートする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux)
- 9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux)
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)

## 9.9.7 クラスタ環境でデータベースをインポートする (Windows)

クラスタ構成となっている Windows の管理サーバで、データベースをインポートします。

データベースのインポートは、実行系ノードで操作します。

### 事前に完了しておく操作

- データベースを移行するための確認作業
- プロパティファイルの設定値の見直し  
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、移行先の実行系ノードおよび待機系ノードでプロパティファイルの設定値を見直してください。

クラスタ環境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** Compute Systems Manager と同じ管理サーバにインストールされている Device Manager が Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager をいったん停止しておく必要があります。

データベースのインポートが完了したあと、Tuning Manager を再開させてください。

Tuning Manager を停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。

1. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を一時停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>
¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
```

2. 次のコマンドを実行して、データベースをインポートします。



**参考** 通常は、アーカイブファイルを使用する方法でインポートしてください。

アーカイブファイルを使用しないでインポートする方法は、バージョン 8.1.0 以前の Compute Systems Manager からデータベースを移行する場合に、移行元のデータベースの全体容量が 2GB を超えているなどの理由で、アーカイブファイルが作成されなかったときに実行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>¥bin
¥hcmds64dbtrans /import /workpath <作業用ディレクトリ> /file <アーカイブ
ファイル> /type {ALL|<Hitachi Command Suite 製品名>} /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：

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。

#### 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ます。転送したディレクトリの下にファイル構成は変更しないでください。

file

アーカイブファイルを使用してインポートする場合、移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。アーカイブファイルを使用しないでインポートする場合は、このオプションを指定しないでください。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。Compute Systems Manager のデータベースだけインポートする場合は、type オプションで「HCSM」と指定します。ほかの Hitachi Command Suite 製品のデータベースを個別にインポートする場合は、各 Hitachi Command Suite 製品のマニュアルを参照してください。

3. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcmds64clustersrvstate /son /r <グループ名 >
```

4. 次のコマンドを実行して、データベースをバックアップします。

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。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin  
¥hcmds64backups /dir <ローカルディスク上のバックアップファイル格納先ディレクトリ >  
> /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。

5. Device Manager が Tuning Manager とリモート接続していた場合は、データベースのインポートによって設定が初期化されるため、再設定します。

#### 関連項目

- 8.1.2 Compute Systems Manager を起動する
- 8.2.6 データベースを移行するための確認事項
- 8.2.8 移行先サーバにデータベースをインポートする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.8.1 Compute Systems Manager のクラスタ運用を一時停止する (Windows)
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)
- 9.9.1 クラスタ環境でデータベースをバックアップする (Windows)

## 9.9.8 クラスタ環境でデータベースをインポートする (Red Hat Enterprise Linux)

クラスタ構成となっている Red Hat Enterprise Linux の管理サーバで、データベースをインポートします。

データベースのインポートは、実行系ノードで操作します。

#### 事前に確認しておく情報

- 新規インストール時に、クラスタ管理アプリケーションへのサービス登録に使用したスクリプトのファイルパス



データベースのインポート後、クラスタ管理アプリケーションにサービスを登録するときに使用する情報です。

### 事前に完了しておく操作

- データベースを移行するための確認作業
- クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスの削除
- プロパティファイルの設定値の見直し

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、移行先の実行系ノードおよび待機系ノードでプロパティファイルの設定値を見直してください。

クラスタ環境でデータベースをインポートする手順を次に示します。

1. クラスタ管理アプリケーションのグループが、実行系ノードに移動していることを確認します。グループが待機系ノードに移動している場合は、実行系ノードに移動します。
2. 次のコマンドを実行して、データベースをインポートします。



**参考** 通常は、アーカイブファイルを使用する方法でインポートしてください。

アーカイブファイルを使用しないでインポートする方法は、バージョン 8.1.0 以前の Compute Systems Manager からデータベースを移行する場合に、移行元のデータベースの全体容量が 2GB を超えているなどの理由で、アーカイブファイルが作成されなかったときに実行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcnds64dbtrans -import -workpath <作業用ディレクトリ> -file <アーカイブ  
ファイル> -type {ALL|<Hitachi Command Suite 製品名>} -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：

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。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ます。転送したディレクトリの下にファイル構成は変更しないでください。

file

アーカイブファイルを使用してインポートする場合、移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。アーカイブファイルを使用しないでインポートする場合は、このオプションを指定しないでください。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。

Compute Systems Manager のデータベースだけインポートする場合は、「HCSM」と指定します。ほかの Hitachi Command Suite 製品のデータベースを個別にインポートする場合は、各 Hitachi Command Suite 製品のマニュアルを参照してください。

3. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcnds64srv -stop
```

4. クラスタ管理アプリケーションのグループから削除したサービスを再登録します。

5. クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。
6. 次のコマンドを実行して、データベースをバックアップします。  
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。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64backups -dir <ローカルディスク上のバックアップファイル格納先ディレクトリ  
> -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。

#### 関連項目

- 8.1.3 Compute Systems Manager を停止する
- 8.2.6 データベースを移行するための確認事項
- 8.2.8 移行先サーバにデータベースをインポートする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.6.2 クラスタ管理アプリケーションにサービスを登録する (Red Hat Enterprise Linux)
- 9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux)
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)
- 9.9.1 クラスタ環境でデータベースをバックアップする (Windows)

### 9.9.9 データベースを移行するコマンド (hcmds64dbclustersetup) の書式 (Red Hat Enterprise Linux)

データベースを移行するコマンド (hcmds64dbclustersetup) の書式を説明します。

このコマンドを実行すると、移行する前のデータベースをローカルディスクに退避したあと、クラスタ環境で使用するデータベースを共有ディスクに再作成します。

なお、Windows の場合は、Compute Systems Manager のインストール時に自動的にデータベースを移行するため、このコマンドを実行する必要はありません。

#### 書式

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64dbclustersetup -createcluster -databasepath <共有ディスク上のデータ  
ベース再作成先ディレクトリ > -exportpath <ローカルディスク上の退避データ格納先ディレ  
クトリ > -auto
```

#### オプション

createcluster

非クラスタ構成の Hitachi Command Suite 製品をクラスタ構成へ移行するためのオプションです。

databasepath

クラスタ環境で使用するデータベースの再作成先ディレクトリを指定します。共有ディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。パスに使用できる文字を次に示します。

A~Z a~z 0~9 . \_

ただし、パスの区切り文字として、スラント (/) を使用できます。

#### exportpath

移行する前のデータベースを退避するディレクトリを指定します。ローカルディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepath に指定できる文字と同じです。

#### auto

Hitachi Command Suite 製品およびデータベースのサービスを、適切な状態に変更するためのオプションです。コマンド実行後には、Hitachi Command Suite 製品およびデータベースのサービスが停止した状態になります。



#### 注意

- hcmds64dbclustersetup コマンドを実行すると、データベースが使用するポート番号および Device Manager と Tuning Manager の間のリモート接続の設定が初期化されます。  
データベースが使用するポート番号が初期化されると、デフォルト値 (22032/tcp) に戻ります。
- <ローカルディスク上の退避データ格納先ディレクトリ>がすでにある場合は、ディレクトリの中を空にするか、ディレクトリを削除してください。
- hcmds64dbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmds64dbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。
- 共有ディスク上に、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品 (Hitachi File Services Manager, Hitachi Storage Navigator Modular 2) のデータベースが作成されている場合、databasepath オプションには別のディレクトリを指定する必要があります。

#### 関連項目

- 9.1 クラスタを使用するための環境設定と運用とは
- 9.4.2 実行系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.4.3 待機系ノードで新規インストールする (Red Hat Enterprise Linux)
- 9.5.2 クラスタ環境に移行する (Red Hat Enterprise Linux)

## 9.10 クラスタ環境からのアンインストール

### 9.10.1 クラスタ環境からデプロイメントマネージャーをアンインストールする

クラスタ環境からデプロイメントマネージャーをアンインストールします。

デプロイメントマネージャーだけをクラスタ環境からアンインストールし、Compute Systems Manager は引き続きクラスタ環境で運用する手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されているグループの所有者を実行系ノードに移動します。
2. 実行系ノードでデプロイメントマネージャーをアンインストールします。
3. 実行系ノードで、不要になったファイルやディレクトリをすべて削除します。
4. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されていたグループの所有者を待機系ノードに移動します。

5. 待機系ノードでデプロイメントマネージャーをアンインストールします。
6. 待機系ノードで、不要になったファイルやディレクトリをすべて削除します。
7. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcmds64clustersrvstate /son /r <グループ名 >
8. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されているグループの所有者を実行系ノードに移動します。

#### 関連項目

- 2.6.3 アンインストールする (Windows)
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)

## 9.10.2 クラスタ環境から Compute Systems Manager をアンインストールする (Windows)

クラスタ環境の管理サーバ (Windows) から、Compute Systems Manager をアンインストールします。

#### 事前に完了しておく操作

- アンインストール前の確認作業



**重要** ほかの Hitachi Command Suite 製品を引き続き使用する場合は、次の点に注意してください。クラスタ管理アプリケーションのグループに登録されている Hitachi Command Suite 製品のサービスは、実行系ノードでのアンインストール時にすべて削除され、待機系ノードでのアンインストール時にデフォルトの設定で再登録されます。サービスのリソース名を変更している場合は、必要に応じて事前にリソース名を控えておき、アンインストール後に手動で変更してください。ただし、Hitachi File Services Manager のサービスは削除されないため、上記の対処は不要です。

クラスタ環境から Compute Systems Manager をアンインストールする手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されているグループの所有者を実行系ノードに移動します。
2. 実行系ノードで Compute Systems Manager をアンインストールします。
3. 実行系ノードで、不要になったファイルやディレクトリ (クラスタ環境内でのインストール中に作成されたファイルやディレクトリなど) をすべて削除します。
4. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されていたグループの所有者を待機系ノードに移動します。
5. 待機系ノードで Compute Systems Manager をアンインストールします。
6. 待機系ノードで、不要になったファイルやディレクトリ (クラスタ環境内でのインストール中に作成されたファイルやディレクトリなど) をすべて削除します。
7. 次のリソースがほかのアプリケーションによって使用されていない場合は、クラスタ管理アプリケーションで、そのリソースをオフラインにしてから削除します。
  - クラスタ管理 IP アドレス
  - 共有ディスク
8. Compute Systems Manager のサービスが登録されていたグループが不要になった場合は、そのグループも削除します。

- ほかの Hitachi Command Suite 製品を引き続き使用する場合は、次のコマンドを実行して、クラスタ運用を開始します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>  
%ClusterSetup%hcmds64clustersrvstate /son /r <グループ名>
```

- ほかの Hitachi Command Suite 製品を引き続き使用する場合は、クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスが登録されているグループの所有者を実行系ノードに移動します。

#### 関連項目

- 2.6.2 アンインストールするための確認事項
- 2.6.3 アンインストールする (Windows)
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)

### 9.10.3 クラスタ環境から Compute Systems Manager をアンインストールする (Red Hat Enterprise Linux)

クラスタ環境の管理サーバ (Red Hat Enterprise Linux) から、Compute Systems Manager をアンインストールします。

#### 事前に完了しておく操作

- アンインストール前の確認作業
- クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスの削除

クラスタ環境から Compute Systems Manager をアンインストールする手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されていたグループを待機系ノードから実行系ノードに移動します。
2. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmds64srv -stop
3. 次のコマンドを実行して、データベースをバックアップします。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmds64backups -dir <ローカルディスク上のバックアップファイル格納先ディレクトリ> -auto
4. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmds64srv -stop
5. 実行系ノードで Compute Systems Manager をアンインストールします。
6. 実行系ノードで、不要になったファイルやディレクトリ (クラスタ環境内でのインストール中に作成されたファイルやディレクトリなど) をすべて削除します。
7. クラスタ管理アプリケーションで、Compute Systems Manager のサービスが登録されていたグループを待機系ノードに移動します。
8. 待機系ノードで Compute Systems Manager をアンインストールします。
9. 待機系ノードで、不要になったファイルやディレクトリ (クラスタ環境内でのインストール中に作成されたファイルやディレクトリなど) をすべて削除します。

10. 次のリソースがほかのアプリケーションによって使用されていない場合は、クラスタ管理アプリケーションでそのリソースを削除します。
  - クラスタ管理 IP アドレス
  - 共有ディスク
11. **Compute Systems Manager** のサービスが登録されていたグループが不要になった場合は、そのグループも削除します。
12. ほかの **Hitachi Command Suite** 製品を引き続き使用する場合は、そのサービスをクラスタ管理アプリケーションのグループに登録します。  
登録する手順については、各製品のマニュアルを参照してください。
13. ほかの **Hitachi Command Suite** 製品を引き続き使用する場合は、クラスタ管理アプリケーションで実行系ノードを選択してクラスタ運用を開始します。

#### 関連項目

- [2.6.2 アンインストールするための確認事項](#)
- [2.6.3 アンインストールする \(Windows\)](#)
- [8.1.3 Compute Systems Manager を停止する](#)
- [9.1 クラスタを使用するための環境設定と運用とは](#)
- [9.2 クラスタを運用するために使用する Compute Systems Manager のサービス](#)
- [9.6.4 クラスタ管理アプリケーションからサービスを削除する \(Red Hat Enterprise Linux\)](#)
- [9.8.4 Compute Systems Manager のクラスタ運用を開始する \(Red Hat Enterprise Linux\)](#)
- [9.9.1 クラスタ環境でデータベースをバックアップする \(Windows\)](#)

# トラブルシューティング

この章では、Compute Systems Manager 運用中に障害が発生した場合に必要な保守情報の採取方法、ログの設定について説明します。

- 10.1 トラブルシューティングについて
- 10.2 トラブルシューティング事例
- 10.3 保守情報の採取
- 10.4 監査ログの確認
- 10.5 ログの設定

## 10.1 トラブルシューティングについて

Compute Systems Manager でシステムを運用している場合にトラブルが発生したときは、表示されたメッセージに従って対処します。

メッセージが表示されない場合や、メッセージに従っても解決できない場合は、システム管理者に連絡してください。また、必要に応じて障害調査のための資料（保守情報）を採取してください。

### 関連項目

- 10.2.1 トラブルシューティング事例（ログイン画面が表示されない）
- 10.2.2 トラブルシューティング事例（Compute Systems Manager が起動しない）
- 10.2.3 トラブルシューティング事例（データベースをリストアできない）
- 10.2.4 トラブルシューティング事例（Windows のクラスタ環境でデータベースをリストアできない）
- 10.2.5 トラブルシューティング事例（Red Hat Enterprise Linux のクラスタ環境でデータベースをリストアできない）

## 10.2 トラブルシューティング事例

### 10.2.1 トラブルシューティング事例（ログイン画面が表示されない）

正しい URL を指定したのに Compute Systems Manager のログイン画面が表示されない場合のトラブルシューティング事例を示します。

#### 考えられる要因

Compute Systems Manager が起動していないか、起動処理中です。

#### 対処方法

Compute Systems Manager が起動していない場合は、起動してください。

#### 関連項目

- 10.1 トラブルシューティングについて

### 10.2.2 トラブルシューティング事例（Compute Systems Manager が起動しない）

Compute Systems Manager または Hitachi Command Suite 共通コンポーネントが起動しない場合のトラブルシューティング事例を示します。

#### 考えられる要因

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。詳細は Microsoft 社のホームページを参照してください。



## 関連項目

- 10.1 [トラブルシューティングについて](#)

### 10.2.3 [トラブルシューティング事例（データベースをリストアできない）](#)

hcms64db コマンドと hcms64dbtrans コマンドのどちらを使っても、データベースをリストアできない場合のトラブルシューティング事例を示します。ここでは、hcms64dbtrans コマンドでエクスポートしたデータベースを、hcms64dbrepair コマンドを使用してリストアする手順について説明します。

#### 考えられる要因

データベースが破損しています。

#### 対処方法

1. エクスポートしたデータベースのサイズに応じて、次のディレクトリに空き領域を確保します。

Windows :

<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%tmp

Linux :

<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/tmp

リストア時、エクスポートで取得したアーカイブファイルはこのディレクトリに展開されます。

2. Compute Systems Manager を停止します。

3. hcms64dbrepair コマンドを実行してデータベースをリストアします。

Windows :

<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin

%hcms64dbrepair /trans <エクスポートで取得したアーカイブファイルまたはエクスポート先ディレクトリ>

Linux :

<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/

hcms64dbrepair -trans <エクスポートで取得したアーカイブファイルまたはエクスポート先ディレクトリ>

trans : <エクスポートで取得したアーカイブファイルまたはエクスポート先ディレクトリ>は、フルパスで指定してください。

4. Compute Systems Manager を起動します。

5. Compute Systems Manager の System アカウントのパスワードを変更します。

hcms64dbrepair コマンドを実行すると、System アカウントのパスワードが初期化されるためです。

#### 関連項目

- 2.5.4 [System アカウントのパスワードを変更する](#)
- 8.1.2 [Compute Systems Manager を起動する](#)
- 8.1.3 [Compute Systems Manager を停止する](#)
- 8.2.4 [データベースをリストアするための確認事項](#)
- 10.1 [トラブルシューティングについて](#)

## 10.2.4 トラブルシューティング事例（Windows のクラスタ環境でデータベースをリストアできない）

Windows のクラスタ環境で、hcmds64db コマンドと hcmds64dbtrans コマンドのどちらを使っても、データベースをリストアできない場合のトラブルシューティング事例を示します。ここでは、hcmds64dbtrans コマンドでエクスポートしたデータベースを、hcmds64dbrepair コマンドを使用してリストアする手順について説明します。

データベースのリストアは、実行系ノードで操作します。

### 考えられる要因

クラスタ環境で、データベースが破損しています。

### 対処方法

1. エクスポートしたデータベースのサイズに応じて、次のディレクトリに空き領域を確保します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥tmp  
リストア時、エクスポートで取得したアーカイブファイルはこのディレクトリに展開されます。
2. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を一時停止します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名 >
3. 次のコマンドを実行して、データベースをリストアします。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin  
¥hcmds64dbrepair /trans <エクスポートで取得したアーカイブファイル >  
  
trans  
    <エクスポートで取得したアーカイブファイル >には、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. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >¥bin  
¥hcmds64srv /stop
5. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >  
¥ClusterSetup¥hcmds64clustersrvstate /son /r <グループ名 >
6. GUI で Compute Systems 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。
7. Device Manager が Tuning Manager とリモート接続していた場合は、データベースのリストアによって設定が初期化されるため、再設定します。
8. Compute Systems Manager の System アカウントのパスワードを変更します。  
hcmds64dbrepair コマンドを実行すると、System アカウントのパスワードが初期化されるためです。

### 関連項目

- [8.2.4 データベースをリストアするための確認事項](#)
- [9.8.1 Compute Systems Manager のクラスタ運用を一時停止する（Windows）](#)
- [9.8.3 Compute Systems Manager のクラスタ運用を開始する（Windows）](#)
- [10.1 トラブルシューティングについて](#)

## 10.2.5 トラブルシューティング事例（Red Hat Enterprise Linux のクラスタ環境でデータベースをリストアできない）

Red Hat Enterprise Linux のクラスタ環境で、`hcmds64db` コマンドと `hcmds64dbtrans` コマンドのどちらを使っても、データベースをリストアできない場合のトラブルシューティング事例を示します。ここでは、`hcmds64dbtrans` コマンドでエクスポートしたデータベースを、`hcmds64dbrepair` コマンドを使用してリストアする手順について説明します。

データベースのリストアは、実行系ノードで操作します。

### 考えられる要因

クラスタ環境で、データベースが破損しています。

### 対処方法

1. エクスポートしたデータベースのサイズに応じて、次のディレクトリに空き領域を確保します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/tmp  
リストア時、エクスポートで取得したアーカイブファイルはこのディレクトリに展開されます。
2. クラスタ管理アプリケーションのグループに登録されている、Compute Systems Manager を含む Hitachi Command Suite 製品のサービスを削除します。
3. クラスタ管理アプリケーションのグループが、実行系ノードに移動していることを確認します。グループが待機系ノードに移動している場合は、実行系ノードに移動します。
4. 次のコマンドを実行して、データベースをリストアします。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
`hcmds64dbrepair -trans <エクスポートで取得したアーカイブファイル>`  
  
`trans`  
  
<エクスポートで取得したアーカイブファイル>には、`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。
5. 次のコマンドを実行して、Hitachi Command Suite 製品を停止します。  
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
`hcmds64srv -stop`
6. クラスタ管理アプリケーションのグループから削除したサービスを再登録します。
7. クラスタ管理アプリケーションで、実行系ノードを選択してクラスタ運用を開始します。
8. GUI で Compute Systems 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. Device Manager が Tuning Manager とリモート接続していた場合は、データベースのリストアによって設定が初期化されるため、再設定します。
10. Compute Systems Manager の System アカウントのパスワードを変更します。  
`hcmds64dbrepair` コマンドを実行すると、System ユーザーのパスワードが初期化されるためです。

### 関連項目

- [8.1.2 Compute Systems Manager を起動する](#)
- [8.2.4 データベースをリストアするための確認事項](#)
- [9.6.2 クラスタ管理アプリケーションにサービスを登録する \(Red Hat Enterprise Linux\)](#)

- 9.6.4 クラスタ管理アプリケーションからサービスを削除する (Red Hat Enterprise Linux)
- 9.8.4 Compute Systems Manager のクラスタ運用を開始する (Red Hat Enterprise Linux)
- 10.1 トラブルシューティングについて

## 10.3 保守情報の採取

### 10.3.1 保守情報の採取とは

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、障害に関する次の情報を用意して、障害対応窓口にご連絡してください。

- 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
- 管理サーバや管理対象リソースのネットワーク構成
- 管理サーバや管理対象ホストの OS
- 障害が発生したマシン（管理サーバまたは管理対象リソース）の保守情報

管理サーバで採取する必要がある保守情報を次に示します。

- ログファイルおよびデータベースファイル  
hcmds64getlogs コマンドを実行して採取します。
- Java VM スレッドダンプ  
Java VM スレッドダンプは、次に示す問題が発生した場合、原因を見つけるために採取します。
  - GUI を起動しても Compute Systems Manager のログインウィンドウが表示されない
  - Compute Systems Manager へのログイン後、Compute Systems Manager のメインウィンドウが表示されない

管理対象リソースで採取する必要がある保守情報を次に示します。

- 管理対象ホスト
  - システム情報
  - Windows ホストの場合：イベントログ情報（アプリケーションログおよびシステムログ）
  - Linux ホストの場合：システムログ情報
- 管理対象ハイパーバイザー
  - Hyper-V の場合：net start コマンドの実行結果
  - VMware ESXi の場合：システムログ情報

保守情報を採取する方法については、ハイパーバイザーのマニュアルを参照してください。

- 管理対象シャーシ、サーバ、および LPAR
  - 通知されたアラート
  - ランプ情報
  - シャーシのエラー情報や構成情報（管理対象ブレードサーバがある場合）
  - HVM のエラー情報や構成情報（管理対象 LPAR がある場合）

保守情報を採取する方法については、管理対象シャーシおよびサーバのマニュアルを参照してください。

## 関連項目

- 10.1 トラブルシューティングについて
- 10.3.2 管理サーバの保守情報を採取する (hcmds64getlogs)
- 10.3.3 管理サーバの Java VM スレッドダンプを採取する (Windows)
- 10.3.4 管理サーバの Java VM スレッドダンプを採取する (Linux)
- 10.3.5 管理対象ホストの保守情報を採取する (Windows ホスト)
- 10.3.6 管理対象ホストの保守情報を採取する (Linux ホスト)

## 10.3.2 管理サーバの保守情報を採取する (hcmds64getlogs)

hcmds64getlogs コマンドを実行すると、ログファイルとデータベースファイルの保守情報を採取できます。

管理サーバの保守情報を採取する hcmd64getlogs コマンドの書式を次に示します。

### 書式

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%bin  
%hcmds64getlogs /dir <ディレクトリ名> [/types <Hitachi Command Suite 製品の名称  
> [<Hitachi Command Suite 製品の名称>...] [/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>...]]
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmds64getlogs -dir <ディレクトリ名> [-types <Hitachi Command Suite 製品の名称  
> [<Hitachi Command Suite 製品の名称>...] [-arc <アーカイブファイル名>] [-logtypes <ログファイル種別> [<ログファイル種別>...]]
```

### オプション

dir

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の名前を指定します。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。type オプションに **Compute Systems Manager** 以外のアプリケーション名を指定した場合の最大長については、各製品のマニュアルを参照してください。
- 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。

```
¥ / : , ; * ? " < > | $ % & ' `
```

パスの区切り文字として、Windows の場合は円記号 (¥)、コロン (:) およびスラント (/)、Linux の場合はスラント (/) 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。

- Windows の場合、パス中に半角スペースを指定するときは、パスを引用符 (") で囲んで指定してください。Linux の場合は、パス中に半角スペースは指定できません。

types

障害などの理由によって、特定の Hitachi Command Suite 製品の保守情報だけしか採取できない場合に、採取対象の製品の名称を指定します。

- Compute Systems Manager 以外の Hitachi Command Suite 製品の名称については、それぞれの Hitachi Command Suite 製品のマニュアルを参照してください。
- Compute Systems Manager の保守情報だけを採取する場合には、「HCSM」と指定します。
- 複数の製品名を指定する場合は、半角スペースで区切ってください。
- types オプションと logtypes オプションの両方を指定する場合、logtypes オプションの引数には「log」を指定してください。
- types オプションを省略した場合、管理サーバにインストールされているすべての Hitachi Command Suite 製品の保守情報が採取されます。管理サーバに 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている場合は、その製品の保守情報も採取されます。

#### arc

作成されるアーカイブファイルの名前を指定します。通常は、指定不要です。

- arc 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。
- アーカイブファイルは、dir オプションで指定したディレクトリの下に出力されます。
- アーカイブファイルが出力されるときに、各アーカイブファイルの種類に応じた拡張子（.jar, .hdb.jar, .db.jar または.csv.jar）が付けられます。
- 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。  
¥ / : , ; \* ? " < > | \$ % & ' `
- Linux の場合、ファイル名に半角スペースは指定できません。

#### logtypes

障害などの理由によって、特定のログファイルしか採取できない場合に、採取対象のログファイルの種別を指定します。

指定できるログファイルの種別を次に示します。

「log」: .jar ファイルと.hdb.jar ファイルだけを採取する場合に指定します。

「db」: .db.jar ファイルだけを採取する場合に指定します。

「csv」: .csv.jar ファイルだけを採取する場合に指定します。

- 複数の種別を指定する場合は、半角スペースで区切ってください。
- logtypes オプションを省略した場合、すべてのログファイル（.jar, .hdb.jar, .db.jar および.csv.jar）が採取されます。

#### 戻り値

0: 正常終了

1: パラメーターエラー

2: 異常終了



#### 重要

- hcnds64getlogs コマンドを複数同時に実行しないでください。
- hcnds64getlogs コマンド終了時に、メッセージ KAPM05318-I または KAPM05319-E が出力されない場合は、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 hcnds64getlogs コマンドが途中で終了している状態です。  
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 hcnds64getlogs コマンドを実行してください。

Compute Systems Manager を含むすべての Hitachi Command Suite 製品の保守情報を採取する hcmds64getlogs コマンドの実行例を次に示します。

実行例 1 : Windows の管理サーバで保守情報を c:\logs ディレクトリに格納する場合

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64getlogs /dir c:\logs
```

実行例 2 : Linux の管理サーバで保守情報を /var/tmp/logs ディレクトリに格納する場合

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64getlogs -dir /var/tmp/logs
```

実行例どおりにコマンドを実行すると、Compute Systems Manager 以外の Hitachi Command Suite 製品の保守情報も採取されます。Compute Systems Manager だけに限定して保守情報を採取する hcmds64getlogs コマンドの実行例を次に示します。

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %bin  
%hcmds64getlogs /dir c:\logs /types HCSM
```

Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmds64getlogs -dir /var/tmp/logs -types HCSM
```

#### 関連項目

- 10.3.1 保守情報の採取とは

### 10.3.3 管理サーバの Java VM スレッドダンプを採取する (Windows)

保守情報として、管理サーバで次の Java VM スレッドダンプを採取します。

- HBase 64 Storage Mgmt SSO Service
- HCS Compute Systems Manager Web Service



**重要** Oracle JDK を使用している場合、Java VM スレッドダンプは出力するたびに上書きされます。出力後は別名で保存してください。

管理サーバで Java VM スレッドダンプを採取する手順を次に示します。

1. < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPsB%CC %server%public%ejb%HBase64StgMgmtSSOService に、dump という名前のファイルを作成します。
2. < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPsB%CC %server%public%ejb%ComputeSystemsManagerWebService に、dump という名前のファイルを作成します。
3. Windows の [サービス] ダイアログにアクセスします。
4. HBase 64 Storage Mgmt SSO Service を停止します。
5. HBase 64 Storage Mgmt SSO Service を開始します。
6. HCS Compute Systems Manager Web Service を停止します。
7. HCS Compute Systems Manager Web Service を開始します。



次のディレクトリに Java VM スレッドダンプが出力されます。Java VM スレッドダンプのファイル名称は、使用している JDK によって異なります。dump という名前のファイルは、Java VM スレッドダンプ出力時に削除されます。

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCP SB %CC %server %public %ejb %HBase64StgMgmtSSOService

- Compute Systems Manager に同梱されている JDK を使用している場合：  
javacorexxx .xxxx .txt
- Oracle JDK を使用している場合：HBase64StgMgmtSSOService.log

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCP SB %CC %server %public %ejb %ComputeSystemsManagerWebService

- Compute Systems Manager に同梱されている JDK を使用している場合：  
javacorexxx .xxxx .txt
- Oracle JDK を使用している場合：ComputeSystemsManagerWebService.log

#### 関連項目

- 10.3.1 保守情報の採取とは

### 10.3.4 管理サーバの Java VM スレッドダンプを採取する (Linux)

保守情報として、管理サーバで次の Java VM スレッドダンプを採取します。

- HBase 64 Storage Mgmt SSO Service
- HCS Compute Systems Manager Web Service



**重要** Oracle JDK を使用している場合、Java VM スレッドダンプは出力するたびに上書きされます。出力後は別名で保存してください。

管理サーバで Java VM スレッドダンプを採取する手順を次に示します。

1. 次のコマンドを実行して、HBase 64 Storage Mgmt SSO Service を停止します。

```
kill -3 <PID >
```

<PID >は、< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > / uCP SB / CC / server / public / ejb / HBase64StgMgmtSSOService / logs / CC / maintenance / cjstdout.log ファイルの最後に書き込まれている Process ID を指定します。

2. 次のコマンドを実行して、HCS Compute Systems Manager Web Service を停止します。

```
kill -3 <PID >
```

<PID >は、< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > / uCP SB / CC / server / public / ejb / ComputeSystemsManagerWebService / logs / CC / maintenance / cjstdout.log ファイルの最後に書き込まれている Process ID を指定します。

3. Compute Systems Manager を再起動します。

次のディレクトリに Java VM スレッドダンプが出力されます。Java VM スレッドダンプの出力先およびファイル名称は、使用している JDK によって異なります。

Compute Systems Manager に同梱されている JDK を使用している場合：



- < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSB/CC/server/public/ejb/HBase64StgMgmtSSOService/  
javacorexxx .xxxx .txt
- < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSB/CC/server/public/ejb/ComputeSystemsManagerWebService/  
javacorexxx .xxxx .txt

Oracle JDK を使用している場合 :

- < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSB/CC/server/repository/HBase64StgMgmtSSOService/  
HBase64StgMgmtSSOService.log
- < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /  
uCPSB/CC/server/repository/ComputeSystemsManagerWebService/  
ComputeSystemsManagerWebService.log

#### 関連項目

- [8.1.2 Compute Systems Manager を起動する](#)
- [8.1.3 Compute Systems Manager を停止する](#)
- [10.3.1 保守情報の採取とは](#)

## 10.3.5 管理対象ホストの保守情報を採取する (Windows ホスト)

Windows の管理対象ホストで保守情報を採取する手順を次に示します。

1. イベントログ情報を採取します。
  - a. Windows の [イベント ビューアー] ダイアログを開く
  - b. 左ペインの [Windows ログ] のツリーを展開する
  - c. 左ペインの次の項目を選択し、ログファイルを保存する
    - [アプリケーション] または [Application]
    - [システム]

それぞれの項目で、テキストまたは CSV 形式、およびイベントログまたはイベントファイル形式の 2 つのログファイルを採取する必要があるため、計 4 つのファイルを保存します。

ログファイルは、[ログファイルの名前を付けて保存]、[イベントに名前を付けて保存]、または [すべてのイベントに名前を付けて保存] を選択し、[ファイルの種類] を指定して保存します。

[表示情報] ダイアログボックス (設定はデフォルトのまま) が表示された場合は、[OK] ボタンをクリックします。
2. システム情報を採取します。
  - a. msinfo32 コマンドを実行する
  - b. 左ペインから [システムの概要] または [システムの要約] を選択する
  - c. [ファイル] メニューから [エクスポート] を選択し、システム情報をテキストファイルで保存する

#### 関連項目

- [10.3.1 保守情報の採取とは](#)

## 10.3.6 管理対象ホストの保守情報を採取する (Linux ホスト)

Linux の管理対象ホストで保守情報を採取する手順を次に示します。

1. システムログ情報を採取します。
  - a. /etc/syslog.conf ファイルまたは/etc/rsyslog.conf ファイルをコピーする
  - b. 次のコマンド実行結果をファイルに出力する

```
ls -l /var/log/messages*
```
  - c. /var/log/messages\* ファイルをコピーする
2. システム情報を採取します。
  - a. 次に示すファイルをコピーする

```
/etc/hosts
/etc/services
```

Red Hat Enterprise Linux の場合 : /etc/redhat-release  
SUSE Linux の場合 : /etc/SuSE-release  
Oracle Linux の場合 : /etc/oracle-release または /etc/enterprise-release
  - b. 次のコマンドの実行結果をそれぞれファイルに出力する

```
uname -a
rpm -qa
dmesg
ps -elf
```

### 関連項目

- 10.3.1 保守情報の採取とは

## 10.4 監査ログの確認

### 10.4.1 監査ログとは

Compute Systems Manager 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。

### 関連項目

- 10.4.2 監査ログの環境設定ファイルを設定する
- 10.4.3 監査ログを確認する
- 10.4.4 監査ログの種別
- 10.4.5 監査ログのメッセージ部の出力形式
- 10.4.6 タスクの操作で出力される情報
- 10.4.7 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
- 10.4.8 リクエスト受理時に監査ログの詳細メッセージに出力される情報

### 10.4.2 監査ログの環境設定ファイルを設定する

監査ログは大量に出力されるおそれがあるため、環境設定ファイルを設定して、出力される監査ログの量を制御できます。

採取した監査ログは、必要に応じて、退避または保管などを実施してください。

Compute Systems Manager での操作を監査ログに出力する手順を次に示します。

1. Compute Systems Manager を停止します。
2. 次に示す監査ログに関するプロパティファイルを設定します。

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%conf%\sec  
%auditlog.conf
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf/sec/  
auditlog.conf
```

3. Compute Systems Manager を起動します。

Compute Systems Manager での操作が監査ログに出力されるようになります。

#### 関連項目

- [8.1.2 Compute Systems Manager を起動する](#)
- [8.1.3 Compute Systems Manager を停止する](#)
- [10.4.1 監査ログとは](#)
- [10.4.3 監査ログを確認する](#)
- [B.2.17 監査ログに関するプロパティ \(auditlog.conf\)](#)

## 10.4.3 監査ログを確認する

Compute Systems Manager でのユーザー操作が出力された監査ログを次に示す画面で確認できます。

Windows :

監査ログは、次に示すイベントログに出力されます。

Windows の [イベントビューアー] - [Windows ログ] - [アプリケーション] または [Application] で、イベントを開いたときに表示される [イベントプロパティ] の [全般] タブの内容

監査ログは次の形式で出力されます。

```
<プログラム名> [<プロセス ID >]: <メッセージ部>
```

Linux :

監査ログは、syslog に次の形式で出力されます。

```
<syslog ヘッダ部> <メッセージ部>
```

syslog ヘッダ部のフォーマットは、OS の環境設定に依存します。

例えば、rsyslog を使用している場合、/etc/rsyslog.conf の設定で \$ActionFileDefaultTemplate RSYSLOG\_SyslogProtocol23Format を指定すると、RFC5424 対応の形式で出力されます。

#### 関連項目

- [10.4.1 監査ログとは](#)

- 10.4.4 監査ログの種別
- 10.4.5 監査ログのメッセージ部の出力形式

## 10.4.4 監査ログの種別

監査ログは種別で分類され、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。

次の表に、監査ログの種別とその詳細の説明を示します。

**表 10-1 監査ログの種別**

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 <ul style="list-style-type: none"> <li>• OS の起動と終了</li> <li>• ハードウェアコンポーネントの起動と終了</li> <li>• Hitachi Command Suite 製品の起動と終了</li> </ul>
Authentication	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 <ul style="list-style-type: none"> <li>• ユーザーの認証</li> <li>• アカウントの自動ロック</li> </ul>
ExternalService	外部サービスとの通信結果を示す事象 <ul style="list-style-type: none"> <li>• NTP サーバや DNS サーバなどとの通信</li> <li>• 管理サーバとの通信（SNMP）</li> </ul>
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 <ul style="list-style-type: none"> <li>• 構成情報の参照または更新</li> <li>• アカウントの追加、削除などのアカウント設定の更新</li> <li>• セキュリティの設定</li> <li>• 監査ログ設定の参照または更新</li> </ul>

次に示す 4 つの表に、監査ログに出力される監査事象を、種別ごとに分けて説明します。

表の「詳細種別」は、監査ログの種別を詳細に分類した説明です。

**表 10-2 監査ログに出力される監査事象（種別が StartStop の場合）**

詳細種別	監査事象	Severity	メッセージ ID
ソフトウェアの起動と終了	SSO サーバの起動成功	6	KAPM00090-I
	SSO サーバの起動失敗	3	KAPM00091-E
	SSO サーバの停止	6	KAPM00092-I

**表 10-3 監査ログに出力される監査事象（種別が Authentication の場合）**

詳細種別	監査事象	Severity	メッセージ ID
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

詳細種別	監査事象	Severity	メッセージ ID
	ログインの失敗（権限なし）	4	KAPM01095-E
	ログインの失敗（認証失敗）	4	KAPM01125-E
	ログインの失敗（外部認証サーバ認証失敗）	4	KAPM02451-W
	ログアウトの成功	6	KAPM08009-I
	ログアウトの失敗	4	KAPM01126-W
アカウントの自動ロック	アカウントの自動ロック（認証の連続失敗またはアカウントの有効期限切れ）	4	KAPM02292-W

表 10-4 監査ログに出力される監査事象（種別が ExternalService の場合）

詳細種別	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
	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
	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

表 10-5 監査ログに出力される監査事象（種別が ConfigurationAccess の場合）

詳細種別	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
(管理者によるほかのユーザーの) パスワードの変更	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
(ログインユーザーによる自分の) パスワードの変更	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
	ログインユーザーによる自分のパスワード変更成功	6	KAPM07232-I
	ログインユーザーによる自分のパスワード変更失敗	3	KAPM07240-E
プロフィールの変更	プロフィールの変更成功	6	KAPM07233-I
	プロフィールの変更失敗	3	KAPM07240-E
権限の変更	権限の変更成功	6	KAPM02280-I
	権限の変更失敗	3	KAPM07240-E
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
	hcnds64unlockaccount コマンドによるアカウントのロック解除成功	6	KAPM07236-I
	hcnds64unlockaccount 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 および CLI)	ユーザーの登録成功	6	KAPM07241-I
	ユーザーの登録失敗	3	KAPM07242-E
ユーザー情報の更新 (GUI および CLI)	ユーザー情報の更新成功	6	KAPM07243-I
	ユーザー情報の更新失敗	3	KAPM07244-E

詳細種別	監査事象	Severity	メッセージID
ユーザーの削除 (GUI および CLI)	ユーザーの削除成功	6	KAPM07245-I
	ユーザーの削除失敗	3	KAPM07246-E
認可グループの登録 (GUI および CLI)	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 および CLI)	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 および CLI)	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 hcmdsb64db 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 hcmdsb64db コマンドによるバックアップ失敗	3	KAPM05562-E
	hcmds64db コマンドによる全体リストアの成功	6	KAPM05563-I
	hcmds64db コマンドによる全体リストアの失敗	3	KAPM05564-E
	hcmds64db コマンドによる部分リストアの成功	6	KAPM05565-I
	hcmds64db コマンドによる部分リストアの失敗	3	KAPM05566-E
データベースの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成功	6	KAPM05834-I
	hcmds64authmove コマンドによるデータ入力失敗	3	KAPM05835-E
リソースグループの作成	リソースグループの作成成功	6	KAPM07257-I
	リソースグループの作成失敗	3	KAPM07258-E
リソースグループの削除	リソースグループの削除成功	6	KAPM07259-I
	リソースグループの削除失敗	3	KAPM07260-E

詳細種別	監査事象	Severity	メッセージID
リソースグループのプロパティ編集	リソースグループのプロパティ編集成功	6	KAPM07261-I
	リソースグループのプロパティ編集失敗	3	KAPM07262-E
ユーザーグループの登録	ユーザーグループの登録成功	6	KAPM07263-I
	ユーザーグループの登録失敗	3	KAPM07264-E
ユーザーグループの削除	ユーザーグループの削除成功	6	KAPM07265-I
	ユーザーグループの削除失敗	3	KAPM07266-E
ユーザーグループの更新	ユーザーグループの更新成功	6	KAPM07267-I
	ユーザーグループの更新失敗	3	KAPM07268-E
ロールの登録	ロールの登録成功	6	KAPM07269-I
	ロールの登録失敗	3	KAPM07270-E
ロールの削除	ロールの削除成功	6	KAPM07271-I
	ロールの削除失敗	3	KAPM07272-E
ロールの更新	ロールの更新成功	6	KAPM07273-I
	ロールの更新失敗	3	KAPM07274-E
ユーザーグループへのユーザーアカウントの割り当て	ユーザーグループへのユーザーアカウントの割り当て成功	6	KAPM07275-I
	ユーザーグループへのユーザーアカウントの割り当て失敗	3	KAPM07276-E
ロールへのパーミッションの割り当て	ロールへのパーミッションの割り当て成功	6	KAPM07277-I
	ロールへのパーミッションの割り当て失敗	3	KAPM07278-E
次の3項目の割り当て ・ ユーザーグループおよび外部認証グループ ・ リソースグループ ・ ロール	次の3項目の割り当ての成功 ・ ユーザーグループおよび外部認証グループ ・ リソースグループ ・ ロール	6	KAPM07279-I
	次の3項目の割り当ての失敗 ・ ユーザーグループおよび外部認証グループ ・ リソースグループ ・ ロール	3	KAPM07280-E
Compute Systems Manager サーバの処理	リクエスト受理	6	KASV27000-I
	レスポンス送信 (正常時)	6	KASV27002-I
	レスポンス送信 (異常時)	3	KASV27003-I
タスクに対する操作	タスクのキャンセル成功	6	KASV27004-I
	タスクのキャンセル失敗	4	KASV27005-W
	タスクの登録成功	6	KASV27006-I
	タスクの登録失敗	4	KASV27007-W
	タスクの削除成功	6	KASV27008-I
	タスクの削除失敗	4	KASV27009-W
	タスクの実行成功	6	KASV27010-I
	タスクの実行失敗	4	KASV27011-W
	タスクのリスケジュール成功	6	KASV27012-I



詳細種別	監査事象	Severity	メッセージID
	タスクのリスケジュール失敗	4	KASV27013-W
	タスクの履歴に移動成功	6	KASV27014-I
	タスクの履歴に移動失敗	4	KASV27015-W

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は、監査ログに記録されません。

関連項目

- 10.4.3 監査ログを確認する
- 10.4.5 監査ログのメッセージ部の出力形式

## 10.4.5 監査ログのメッセージ部の出力形式

監査ログは次の形式で出力されます。

```
<プログラム名> [<プロセスID>]: <メッセージ部>
```

<メッセージ部>には、半角で 953 文字まで表示されます。

次に、<メッセージ部>の出力形式と出力される項目の内容を示します。監査事象によっては、<メッセージ部>に出力されない項目もあります。

```
<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>
```

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
<日付・時刻>	メッセージが出力された日付と時刻
<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

項目	内容
<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。

注※

Hitachi 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。

ログイン時の例: "The login was successful. (session ID = <セッションID>)"

監査事象「ログインの成功」で出力されるメッセージ部の例を次に示します。

```
CELFS,1.1,0,KAPM01124-I,2014-07-22T14:08:23.1+09:00,HBBase-SSO,management-host,Authentication,Success,uid=system,,,,,,,,,,,,BasicLog,,, "The login was successful. (session ID = <セッションID>)"
```

関連項目

- 10.4.3 監査ログを確認する
- 10.4.4 監査ログの種別
- 10.4.6 タスクの操作で出力される情報
- 10.4.7 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
- 10.4.8 リクエスト受理時に監査ログの詳細メッセージに出力される情報

## 10.4.6 タスクの操作で出力される情報

監査ログの<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、タスクでの操作の場合に出力される監査ログの<メッセージテキスト>の形式と内容を説明します。

```
uk=<ユニークキー> [taskname=<タスク名>]
```

項目	内容
<ユニークキー>	タスクに対する一意なキー値です。
<タスク名>	操作したタスク名を表示します。この項目は出力されないことがあります。

#### 関連項目

- 10.4.3 監査ログを確認する
- 10.4.4 監査ログの種別
- 10.4.5 監査ログのメッセージ部の出力形式
- 10.4.8 リクエスト受理時に監査ログの詳細メッセージに出力される情報

### 10.4.7 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

監査ログの<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、構成変更、情報取得など、Compute Systems Manager サーバの処理に関する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監査ログの<メッセージテキスト>の形式と内容を説明します。

#### リクエスト受理時

<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 >

#### 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 >

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。
<エラーメッセージ ID >	エラーメッセージ ID です。

#### 関連項目

- 10.4.3 監査ログを確認する
- 10.4.4 監査ログの種別
- 10.4.5 監査ログのメッセージ部の出力形式
- 10.4.8 リクエスト受理時に監査ログの詳細メッセージに出力される情報

### 10.4.8 リクエスト受理時に監査ログの詳細メッセージに出力される情報

Compute Systems Manager サーバが、リクエストを受理したときに出力される<詳細メッセージ>の出力形式と内容を次に示します。

<コマンド> <ターゲット> [<パラメーター>]

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。
<ターゲット>	操作内容を特定する情報です。

項目	内容
<パラメーター>	<p>操作内容, 対象リソースを特定する情報です。この項目は、リクエストで指定された場合だけ出力されます。</p> <p>&lt;パラメーター&gt;は、次に示すとおりタグ形式で出力されます。</p> <p>&lt;&lt;エレメント&gt; &lt;属性&gt;/&gt; &lt;エレメント&gt;</p> <p>エレメント名を示す文字列です。</p> <p>&lt;属性&gt;</p> <p>エレメントに対して指定された属性値が、info='...'の形式で出力されます。複数個出力される場合は、コンマ(,)で区切られます。属性値は、文字列または数値で出力されます。</p> <p>対応する属性が未指定、または属性値に何も指定されていなかった場合、値は出力されません。すべての属性が未指定、または属性値に何も指定されていなかった場合、この項目は出力されません。</p> <p>属性値にアポストロフィ(')またはコンマ(,)が含まれる場合、疑問符(?)で置換されます。</p>

次の3つの表に、項目ごとに出力される内容の詳細について説明します。

表 10-6 詳細メッセージの<コマンド>に出力される文字列と内容

出力文字列	正式名	操作内容
Add	Add	追加
Del	Delete	削除
Get	Get	取得
Mod	Modify	変更
Set	Set	設定

表 10-7 詳細メッセージの<ターゲット>に出力される文字列と内容

出力文字列	正式名	操作内容
Alerts	Alerts	アラート情報の参照・削除
Chassis	Chassis	シャーシの設定・参照
Server	Server	サーバの設定・参照
Host	Host	ホストの設定・参照
LGrp	LogicalGroup	論理グループの設定・参照
SrvI	ServerInfo	Compute Systems Manager サーバの情報取得
User	User	ユーザーの設定・参照

表 10-8 詳細メッセージの<パラメーター>に出力される<エレメント>と<属性値>の出力内容

<エレメント>の出力文字列	内容	<属性値>の出力内容
Alert	Compute Systems Manager または管理対象リソースで発生したエラー情報	アラート番号
Chassis	シャーシ情報	シャーシ名, シャーシの IP アドレス
Server	サーバ情報	サーバ名, サーバの IP アドレス
Host	ホスト情報	ホスト名, ホストの IP アドレス

<エレメント>の出力文字列	内容	<属性値>の出力内容
User	Compute Systems Manager の 1 ユーザーアカウント情報	ユーザー ID

#### 関連項目

- 10.4.3 監査ログを確認する
- 10.4.4 監査ログの種別
- 10.4.5 監査ログのメッセージ部の出力形式
- 10.4.7 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

## 10.5 ログの設定

### 10.5.1 ログの設定とは

Compute Systems Manager で出力するログの設定について説明します。

障害発生後の再現テスト、障害調査など、詳細なログ情報の採取が必要な場合、Compute Systems Manager のメッセージログの設定を変更できます。通常の運用の際にはログの設定変更は不要です。

変更できる設定は次のとおりです。

- ログファイルの最大サイズ
- ログの最大ファイル数
- ログ出力情報の詳細度



参考 メッセージログファイルは、次の場所に格納されています。

Windows :

< Compute Systems Manager のインストールディレクトリ >%logs%WebServiceMessageN.log

Linux :

/var/< Compute Systems Manager のインストールディレクトリ >/logs/WebServiceMessageN.log

WebServiceMessageN.log の N は、ログファイルの数を表す整数です。

#### 関連項目

- 10.5.2 Compute Systems Manager のログの設定を変更する

### 10.5.2 Compute Systems Manager のログの設定を変更する

Compute Systems Manager のログのファイルサイズ、ファイル数、および出力情報の詳細度を変更する手順を、次に示します。

1. Compute Systems Manager を停止します。
2. 次の場所に格納されている logger.properties を開きます。

Windows :

< Compute Systems Manager のインストールディレクトリ >%ComputeSystemsManager%conf%logger.properties

Linux :

< *Compute Systems Manager* のインストールディレクトリ > /ComputeSystemsManager/  
conf/logger.properties

3. 次のプロパティを設定します。

- message.maxFileSizeInMB  
ファイルサイズを設定します。ファイルサイズを超えた場合、古いメッセージから上書きされます。
- message.maxBackupIndex  
ログファイル数を設定します。
- message.logLevel  
ログ出力情報の詳細度を設定します。

4. *Compute Systems Manager* を起動します。

*Compute Systems Manager* のログの設定が変更されます。

#### 関連項目

- [8.1.2 \*Compute Systems Manager\* を起動する](#)
- [8.1.3 \*Compute Systems Manager\* を停止する](#)
- [10.5.1 ログの設定とは](#)
- [B.1.4 ログ出力に関するプロパティ \(logger.properties\)](#)

# ポートの設定

ここでは、Compute Systems Manager で使用されるポートについて説明します。

- [A.1 Compute Systems Manager サーバで使用されるポート](#)
- [A.2 Hitachi Command Suite 共通コンポーネントで使用されるポート](#)
- [A.3 デプロイメントマネージャーで使用されるポート](#)
- [A.4 用途ごとのポートの詳細](#)

## A.1 Compute Systems Manager サーバで使用されるポート

Compute Systems Manager サーバで使用されるポートの一覧を次の表に示します。

Compute Systems 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製品と重複しないようにしてください。重複する場合は、その製品の設定を変更するか、Compute Systems Manager サーバの設定を変更してください。

次の表のポート番号は、すべて変更できます。

ポート番号	説明
162/UDP または 22601/UDP	SNMP トラップを受信する際に使用されます。デフォルトは 162/UDP です。 162/UDP がほかの製品で使用されていた場合の推奨値は 22601/UDP です。
22610/TCP	Device Manager と通信する際に使用されます。
22611/TCP	日立製のサーバからのアラートを受信する際に使用されます。

### 関連項目

- 2.2.3 ポート番号が競合していないことを確認する
- (2) ポート変更時に編集する Compute Systems Manager サーバのプロパティ
- (3) ポートを変更する

## A.2 Hitachi Command Suite 共通コンポーネントで使用されるポート

Hitachi Command Suite 共通コンポーネントで使用されるポートの一覧を次の表に示します。

Hitachi 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製品と重複しないようにしてください。重複する場合は、その製品の設定を変更するか、Hitachi Command Suite 共通コンポーネントの設定を変更してください。

デフォルトのポート番号	説明
22015/TCP	管理クライアント (GUI および CLI) と非 SSL で通信する際に、Hitachi Command Suite 共通コンポーネントのサービス (HBase 64 Storage Mgmt Web Service) へのアクセスで使用されます。 ポート番号は変更できます。 SSL 通信している場合に、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 ファイルの編集が必要です。
22016/TCP	管理クライアント (GUI) と SSL 通信する際に、Hitachi Command Suite 共通コンポーネントのサービス (HBase 64 Storage Mgmt Web Service) へのアクセスで使用されます。 ポート番号は変更できます。
22017/TCP~22026/TCP	予約済みのポートです。
22027/TCP 22035/TCP 22037/TCP 22038/TCP 22613/TCP 22614/TCP	Hitachi Command Suite 共通コンポーネントの内部通信 (Web サーバとの通信) で使用されます。 ポート番号は変更できます。



デフォルトのポート番号	説明
22028/TCP 22036/TCP	Hitachi Command Suite 共通コンポーネントの内部通信（ネーミングサービス）で使用されます。 ポート番号は変更できます。
22029/TCP～22030/TCP	予約済みのポートです。
22031/TCP	Hitachi Command Suite 共通コンポーネントの内部通信（シングルサインオン用 Web サーバとの通信）で使用されます。 ポート番号は変更できます。
22032/TCP	Hitachi Command Suite 共通コンポーネントの内部通信（データベースとの通信）で使用されます。 ポート番号は変更できます。

#### 関連項目

- ・ 2.2.3 ポート番号が競合していないことを確認する
- ・ (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ (3) ポートを変更する

## A.3 デプロイメントマネージャーで使用されるポート

デプロイメントマネージャーで使用されるポートの一覧を次の表に示します。

デプロイメントマネージャー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製品と重複しないようにしてください。重複する場合は、デプロイメントマネージャーの設定を変更してください。

ただし、デプロイメントマネージャーで変更できないポート番号については、ほかの製品の設定を変更してください。

ポート番号	説明
67/UDP 69/UDP	管理対象リソースを PXE ブートする際に使用されます。 ポート番号は変更できません。
80/TCP	IIS 上のサービスプロセスとの内部通信で使用されます。 ポート番号は変更できます。
4011/UDP	管理対象リソースを PXE ブートする際に使用されます。 ポート番号は変更できません。
26500/TCP	IIS に配置するサービスプロセスとデプロイメントマネージャーとの内部通信で使用されます。 ポート番号は変更できます。
26501/TCP または 56020/TCP	管理対象リソースのディスクをリストアしたり、バックアップしたりする際に使用されます。デフォルトは 26501/TCP です。 ポート番号は変更できます。ポート番号の変更に失敗した場合は、56020/TCP が使用されます。
26502/TCP または 56022/TCP	管理対象リソースを PXE ブートする際に使用されます。デフォルトは 26502/TCP です。 ポート番号は変更できます。ポート番号の変更に失敗した場合は、56022/TCP が使用されます。
26503/TCP または 56030/TCP	管理対象リソースを PXE ブートする際に使用されます。デフォルトは 26503/TCP です。 ポート番号は変更できます。ポート番号の変更に失敗した場合は、56030/TCP が使用されます。

ポート番号	説明
26504/TCP~26507/TCP	デプロイメントマネージャーの内部処理で使用するポートです。ポート番号は変更できます。
26508/TCP または 56023/TCP	管理対象リソースのディスクを操作する際に使用されます。デフォルトは26508/TCPです。ポート番号は変更できます。ポート番号の変更に失敗した場合は、56023/TCPが使用されます。
56011/TCP 56024/TCP 56028/TCP 56060/TCP	デプロイメントマネージャーの内部処理で使用するポートです。ポート番号は変更できません。

#### 関連項目

- ・ 2.2.3 ポート番号が競合していないことを確認する
- ・ 7.8 デプロイメントマネージャーが使用するポート番号を変更する
- ・ 7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル

## A.4 用途ごとのポートの詳細

Compute Systems Manager がネットワーク通信時に、通信を実行するプロセス、使用されるポート、プロトコルなどの詳細情報を用途ごとに示します。

使用するポートを限定したい場合や、ファイアウォールを設定する場合に参照してください。

次に示す表に通信路ごとに分けてポート情報を記載します。

表中の「管理サーバ」は「Compute Systems Manager サーバ」を指します。

表中の「cjstartsv.exe」は Windows の場合のプロセス名です。Linux の場合は「cjstartsv」に読み替えてください。

「●」が付いているコンポーネント名は、データの送信元となるコンポーネントを表します。

表 A-1 管理サーバと管理クライアントの通信に使用されるポート

用途	コンポーネント (通信プロセス)	ポート 番号	プロトコル	宛先 指定	データ の 向き	ポート 番号	コンポーネント
管理クライアントから管理サーバへの通信	管理サーバ (cjstartsv.exe)	22015 (変更可)	TCP (HTTP)	U	<-	自動割り当て	●管理クライアント (GUI/CLI)
		22016 (変更可)	TCP (HTTPS)	U	<-	自動割り当て	

(凡例)

U : Unicast

表 A-2 管理サーバと管理対象の通信に使用されるポート

用途	コンポーネント (通信プロセス)	ポート 番号	プロトコル	宛先 指定	デー タの 向き	ポート 番号	コンポーネント (通信プロセス)
稼働監視, 電源管理, および 構成情報 取得	●管理サーバ (cjstartsv.e xe)	自動割り 当て	TCP,UDP (WMI/ DCOM)	U	->	135, エフェメ ラルポー ト※1	Windows Hyper-V
			TCP (WinRM/ HTTP)	U	->	5985 (変更可)	
			TCP (SSH)	U	->	22 (変更可)	Linux (sshd)
			TCP	U	->	443	VMware ESXi
			TCP(SSL)	U	->	443 (変更可)	SVP BMC※2
			TCP (SSH)	U	->	22 (変更可)	BMC※2
電源管理 (BMC)※3	管理サーバ (cjstartsv.e xe)	自動割り 当て	UDP (RMCP)	U	<-	623	●BMC
	●管理サーバ (cjstartsv.e xe)		UDP (RMCP)	U	->	623	BMC
電源管理 (WoL)※3	●管理サーバ (cjstartsv.e xe)	自動割り 当て	UDP (WoL)	B※4	->	0	管理対象サーバ
			UDP (WoL)	U	->	0	
	●管理サーバ (magicsend.e xe)		UDP (WoL)	B※5	->	5561	
SNMP トラップ 受信	管理サーバ (cjstartsv.e xe)	162 また は 22601※6 (変更可)	UDP	U	<-	自動割り 当て	●Windows ●Linux ●Hyper-V
アラート 受信	管理サーバ (cjstartsv.e xe)	22611 (変更可)	TCP	U	<-	自動割り 当て	●SVP ●BMC ●HVM
LPAR の マイグ レーショ ン	●管理サーバ (cjstartsv.e xe)	自動割り 当て	TCP	U	->	23401	HVM

(凡例)

U : Unicast

B : Broadcast

注※1

最初に 135 で接続したあと、管理対象ホストのエフェメラルポートが自動的に割り当てられます。

エフェメラルポートのデフォルトの範囲は、49152~65535 です。

管理対象ホストでエフェメラルポートの範囲を変更した場合は、変更後の範囲がこの通信で自動的に割り当てられるポートの範囲になります。

注※2

BMC との通信プロトコルは、ラックマウントサーバの機種によって異なります。

ラックマウントサーバの通信プロトコル、およびポート番号については、ソフトウェア添付資料を参照してください。

注※3

日立製でないサーバの電源管理で使用されます。

注※4

リミテッドブロードキャスト (255.255.255.255 宛て)

注※5

同セグメントのマシンにはリミテッドブロードキャスト (255.255.255.255 宛て) で、別セグメントのマシンにはディレクティッドブロードキャストで通信します。

注※6

ポート 162 がほかの製品で使用されている場合は、22601 がデフォルトになります。

表 A-3 Windows の管理サーバと管理対象の通信に使用されるポート (デプロイメントマネージャ)

用途	コンポーネント (通信プロセス)	ポート番号	プロトコル	宛先指定	データの向き	ポート番号	コンポーネント
PXE ブート	管理サーバ (pxesvc.exe)	67	UDP (DHCP)*1	B**2	<-	68	●管理対象サーバ
		4011	UDP	U	<-	68	
		4011	UDP	U	<-	4011	
	管理サーバ (pxemtftp.exe)	69	UDP (TFTP)	U	<-	自動割り当て	
	管理サーバ (bkressvc.exe)	26503 または 56030 (変更可)	TCP	U	<-	自動割り当て	
		26502 または 56022 (変更可)	TCP	U	<-	自動割り当て	
	●管理サーバ (pxesvc.exe)	67	UDP (DHCP)*1	B**2	->	68	管理対象サーバ
67		UDP	U	->	68		
67		UDP	U	->	4011		
●管理サーバ (pxemtftp.exe)	69	UDP (TFTP)	U	->	自動割り当て		
ディスク構成チェック	管理サーバ (ftsvc.exe)	26508 または 56023 (変更可)	TCP	U	<-	自動割り当て	●管理対象サーバ

用途	コンポーネント (通信プロセス)	ポート 番号	プロトコル	宛先 指定	データ の 向き	ポート 番号	コンポーネント
スナップ ショット の取得	管理サーバ (ftsvc.exe)	26508 または 56023 (変更可)	TCP	U	<-	自動割り 当て	
マスター イメージ のデプロ イ	管理サーバ (ftsvc.exe)	26508 または 56023 (変更可)	TCP	U	<-	自動割り 当て	
	管理サーバ (pxesvc.exe)	4011※3	UDP (DHCP)	B	<-	68	
	管理サーバ (pxemtftp.ex e)	69※3	UDP (TFTP)	U	<-	自動割り 当て	
	●管理サーバ (pxesvc.exe)	67※3	UDP (DHCP)	B	->	68	管理対象サーバ
	●管理サーバ (pxemtftp.ex e)	69※4	UDP (TFTP)	U	->	自動割り 当て	
ディスク データの リストア	管理サーバ (ftsvc.exe)	26508 または 56023 (変更可)	TCP	U	<-	自動割り 当て	●管理対象サー バ
	管理サーバ (bkressvc.ex e)	26501 または 56020 (変更可)	TCP	U	<-	自動割り 当て	
ディスク データの バック アップ	管理サーバ (ftsvc.exe)	26508 または 56023 (変更可)	TCP	U	<-	自動割り 当て	
	管理サーバ (bkressvc.ex e)	26501 または 56020 (変更可)	TCP	U	<-	自動割り 当て	

(凡例)

U : Unicast

B : Broadcast

n または m : デフォルトポート番号は n です。ポート番号の変更に失敗した場合にポート番号 m が使用されます。

注※1

DHCP サーバと管理サーバが別装置の場合だけ発生する通信です。

注※2

DHCP リレーによってリレーされたパケットの宛先は Unicast になる場合があります。

注※3

マスターイメージのデプロイ実行時、管理対象が管理サーバと通信できない場合に使用されま  
す。

注※4

マスターイメージのデプロイ実行時、デプロイ対象が管理サーバと通信できない場合に使用されます。

表 A-4 管理サーバと外部連携サーバの通信に使用されるポート

用途	コンポーネント (通信プロセス)	ポート 番号	プロトコル	宛先 指定	データ の 向き	ポート 番号	コンポーネント
Eメール 通知 (SMTP)	●管理サーバ (cjstartsv.exe)	自動割 り当て	TCP (SMTP)	U	->	25 (変更可)	SMTPサーバ
Device Manager との接続		自動割 り当て	TCP (HTTP)	U	->	2001 (変更可)	Device Managerサーバ
			TCP (HTTPS)	U	->	2443 (変更可)	
外部認証 サーバと の連携 (Kerberos サーバ)		自動割 り当て	TCP/UDP	U	->	88 (変更可)	認証サーバ
外部認証 サーバと の連携 (LDAP ディレク トリサーバ/ StartTLS 通信)	自動割 り当て	TCP/UDP	U	->	389 (変更可)		

(凡例)

U : Unicast

表 A-5 管理クライアントと管理対象の通信に使用されるポート

用途	コンポーネント	ポート 番号	プロトコル	宛先 指定	データ の 向き	ポート 番号	コンポーネント
Webコン ソール起 動 (シャージ)	●管理クライ アント	自動割 り当て	TCP (HTTP)	U	->	80	SVP
		自動割 り当て	TCP (HTTPS)	U	->	443	
Webコン ソール起 動 (サーバ)		自動割 り当て	TCP (HTTP)	U	->	80	BMC
		自動割 り当て	TCP (HTTPS)	U	->	443	
Webリ モート KVM通信		自動割 り当て	TCP	U	->	5001 (変更可)	

(凡例)

U : Unicast

表 A-6 管理対象と外部連携サーバの通信に使用されるポート

用途	コンポーネント	ポート番号	プロトコル	宛先指定	データの向き	ポート番号	コンポーネント
デプロイメントマネージャー (PXE ブート)	管理対象サーバ	68	UDP (DHCP)	B※	<-	67	●DHCP サーバ
	●管理対象サーバ	68	UDP (DHCP)	B※	->	67	DHCP サーバ

(凡例)

B : Broadcast

注※

DHCP リレーによってリレーされたパケットの宛先は Unicast になる場合があります。

#### 関連項目

- ・ 2.2.3 ポート番号が競合していないことを確認する
- ・ (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ (2) ポート変更時に編集する Compute Systems Manager サーバのプロパティ
- ・ (3) ポートを変更する
- ・ 7.8 デプロイメントマネージャーが使用するポート番号を変更する
- ・ 7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル
- ・ 8.1.4 Compute Systems Manager の常駐プロセス





## プロパティ

ここでは、Compute Systems Manager のプロパティについて説明します。

- [B.1 Compute Systems Manager サーバのプロパティ](#)
- [B.2 Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [B.3 デプロイメントマネージャーで使用されるポートに関するプロパティ \(Port.ini\)](#)

## B.1 Compute Systems Manager サーバのプロパティ

### B.1.1 Compute Systems Manager サーバのプロパティとは

Compute Systems Manager のポートやログに関する設定を変更するには、Compute Systems Manager サーバのプロパティを変更します。プロパティを変更したあと、Compute Systems Manager を再起動すると、設定が反映されます。

#### 関連項目

- B.1.2 Compute Systems Manager サーバのプロパティの一覧

### B.1.2 Compute Systems Manager サーバのプロパティの一覧

Compute Systems Manager サーバのプロパティファイルと格納先ディレクトリの一覧を次の表に示します。

説明	プロパティファイル	格納先ディレクトリ
Compute Systems Manager サーバで使用されるポートや機能に関するプロパティ	user.properties	Windows : < Compute Systems Manager のインストールディレクトリ >¥ComputeSystemsManager¥conf Linux : < Compute Systems Manager のインストールディレクトリ > /ComputeSystemsManager /conf
ログ出力に関するプロパティ	logger.properties	

#### 関連項目

- B.1.1 Compute Systems Manager サーバのプロパティとは
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)
- B.1.4 ログ出力に関するプロパティ (logger.properties)

### B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)

user.properties を使って Compute Systems Manager サーバのポートを変更したり、コマンドのタイムアウト時間や温度表示などの Compute Systems Manager サーバの機能に関する設定を変更したりできます。

user.properties で指定できるプロパティの一覧を次の表に示します。

プロパティ	説明
snmp.trap.receive.port	SNMP トラップを受信するポートを指定します。 <ul style="list-style-type: none"><li>• 指定できる値 : 1~65535 の整数</li><li>• デフォルト値 : 162 または 22601</li></ul>
server.rmi.port	Device Manager からの RMI リクエストの受付ポートを指定します。 <ul style="list-style-type: none"><li>• 指定できる値 : 1~65535 の整数</li><li>• デフォルト値 : 22610</li></ul>
server.process.timeout	アラート発生時に実行するコマンドのタイムアウト時間を秒単位で指定します。 <ul style="list-style-type: none"><li>• 指定できる値 : 0~100000 の整数</li></ul>

プロパティ	説明
	<ul style="list-style-type: none"> <li>デフォルト値：1800</li> </ul> コマンドの処理が完了するまでタイムアウトを発生させたくない場合は、「0」を指定します。
svp.alert.receive.port	日立製のサーバからのアラートを受信するポートを指定します。 <ul style="list-style-type: none"> <li>指定できる値：1～65535の整数</li> <li>デフォルト値：22611</li> </ul>
hcsn.keystore.filename	管理サーバと日立製のサーバ（ブレードサーバ上のHVMも含みます）との間のSSL通信で、Compute Systems Managerが使用するキーストアのファイル名を文字列で指定します。 デフォルト値は、「hcsn_default.keystore」です。 指定できる値は文字列です。
powermonitoring.temperature.unit	管理クライアントに表示される温度の表示単位を指定します。 <ul style="list-style-type: none"> <li>「F」：華氏（Fahrenheit）で表示する場合に指定します。</li> <li>「C」：摂氏（Celsius）で表示する場合に指定します。</li> </ul> デフォルトは「C」です。
hcsn.shared.directory	Compute Systems Managerが使用する作業ディレクトリのパスを指定します。 クラスタ環境で運用する場合は、共有ディスク上のディレクトリのパスを指定します。 指定したディレクトリがない場合は、デフォルトのパスが使用されます。 デフォルトは次のとおりです。 <b>Windows：</b> < Compute Systems Manager のインストールディレクトリ > ¥shared パスに円記号（¥）を指定する場合は「¥¥」と指定してください。プロパティファイル内で円記号（¥）はエスケープシーケンスを示す文字として使用されます。 <b>Linux：</b> < Compute Systems Manager のインストールディレクトリ >/ shared
winrm.maxEnvelopeSize	管理対象ホストでMaxEnvelopeSizekbに推奨値（512）以外を指定してWinRMを有効にした場合、その値を指定します。複数の管理対象ホストで異なる値を設定しているときは、それらの値の中の最大値を指定します。 <ul style="list-style-type: none"> <li>指定できる値：512～4194304の整数</li> <li>デフォルト値：512</li> </ul>
hcsn.certification.verify	管理サーバと日立製のサーバ（ブレードサーバ上のHVMも含みます）との間のSSL通信で、日立製のサーバからの証明書を、管理サーバで確認するかどうかを指定します。 <ul style="list-style-type: none"> <li>「Enable」：証明書を確認します。管理サーバのキーストアに登録されている日立製のサーバの証明書と一致した場合に通信が許可されます。</li> <li>「Disable」：証明書を確認しません。</li> </ul> デフォルトは「Disable」です。 「Enable」を指定する場合は、日立製のサーバの証明書を管理サーバのキーストアに登録してください。
hvm.lpar.migration.allow.plaintext	LPARをマイグレーションする場合に、管理サーバとHVMとの間で暗号化されていない通信を許可するかどうかを指定します。 <ul style="list-style-type: none"> <li>「Enable」：許可します。</li> <li>「Disable」：許可しません。</li> </ul> デフォルトは「Enable」です。
svp.bind.address	管理サーバと日立製のサーバとの間のSSL通信で、日立製のサーバに登録される管理サーバのIPアドレスを指定します。 デフォルト値は空白です。

プロパティ	説明
	デフォルトの場合、管理サーバの OS の仕様に基づいた IP アドレスが登録されます。クラスタ環境では、実行系および待機系の各ノードの IP アドレスが登録されます。 このプロパティは、SSH プロトコルで BMC と通信するラックマウントサーバに対しては無効です。ラックマウントサーバの通信プロトコルについては、ソフトウェア添付資料を参照してください。
hcsmdisplay.storage.systems.list	[リソース] タブに、ストレージシステムの一覧を表示するかどうかを指定します。 <ul style="list-style-type: none"> <li>「Enable」: 表示します。</li> <li>「Disable」: 表示しません。</li> </ul> デフォルトは「Disable」です。

#### 関連項目

- [B.1.1 Compute Systems Manager サーバのプロパティとは](#)
- [B.1.2 Compute Systems Manager サーバのプロパティの一覧](#)

## B.1.4 ログ出力に関するプロパティ (logger.properties)

logger.properties を使ってログ出力の設定を変更できます。

logger.properties で指定できるプロパティの一覧を次の表に示します。

プロパティ	説明
message.maxFileSizeInMB	メッセージログのファイルサイズ (単位: MB) を指定します。 <ul style="list-style-type: none"> <li>指定できる値: 1~2047 の整数</li> <li>デフォルト値: 1</li> </ul>
message.maxBackupIndex	メッセージログのファイル面数を指定します。 <ul style="list-style-type: none"> <li>指定できる値: 1~16 の整数</li> <li>デフォルト値: 10</li> </ul>
message.logLevel	ログに出力する情報の詳細度を指定します。 <ul style="list-style-type: none"> <li>指定できる値: -1~1000 の整数</li> <li>デフォルト値: 20</li> </ul> 障害の再現テスト時は、「30」の利用をお勧めします。「-1」を指定した場合は、ログの出力が行われません。

#### 関連項目

- [B.1.1 Compute Systems Manager サーバのプロパティとは](#)
- [B.1.2 Compute Systems Manager サーバのプロパティの一覧](#)

## B.2 Hitachi Command Suite 共通コンポーネントのプロパティ

### B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは

Hitachi Command Suite 共通コンポーネントの機能に関する設定を変更するには、Hitachi Command Suite 共通コンポーネントのプロパティを変更します。プロパティを変更したあと、Compute Systems Manager を再起動すると、設定が反映されます。



重要 Hitachi Command Suite 共通コンポーネントのプロパティを変更すると、同じ環境で使用するすべての Hitachi Command Suite 製品に変更が反映されます。

## 関連項目

- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

Hitachi Command Suite 共通コンポーネントのプロパティファイルと格納先ディレクトリの一覧を次の表に示します。

説明	プロパティファイル	格納先ディレクトリ
Web サーバに関するプロパティファイル	user_httpsd.conf	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB%\httpsd\%conf Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/ uCPSB/httpsd/conf
	user_hssso_httpsd.conf	
	usrconf.properties (Hitachi Command Suite 共通コンポーネントのシングルサインオン用)	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB%\CC%\server%\usrconf%\ejb %HBase64StgMgmtSSOService Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/ uCPSB/CC/server/usrconf/ejb/ HBase64StgMgmtSSOService
usrconf.properties (Compute Systems Manager 用)	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB%\CC%\server%\usrconf%\ejb %ComputeSystemsManagerWebService Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/ uCPSB/CC/server/usrconf/ejb/ ComputeSystemsManagerWebService	
workers.properties	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %uCPSB%\CC%\web%\redirector Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/ uCPSB/CC/web/redirector	
データベースに関するプロパティファイル	HiRDB.ini	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > %HDB%\CONF%\emb Linux :

説明	プロパティファイル	格納先ディレクトリ
		< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/HDB/CONF/emb
	pdsys	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ> ¥HDB¥CONF Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/HDB/CONF
	pdutysys	
	def_pdsys	Windows : < Hitachi Command Suite 共通コンポーネントのディレクトリ>¥database¥work Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/ database/work
	def_pdutysys	
ユーザーアカウントに関するプロパティファイル	user.conf	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ> ¥conf Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/ conf
外部認証サーバとの連携に関するプロパティファイル	exauth.properties	
クラスタに関するプロパティファイル	cluster.conf	
監査ログに関するプロパティファイル	auditlog.conf	Windows : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ> ¥conf¥sec Linux : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/ conf/sec

## 関連項目

- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.3 Web サーバに関するプロパティ (user\_httpsd.conf)
- B.2.4 Web コンテナサーバに関するプロパティ (usrconf.properties)
- B.2.5 Web コンテナサーバに関するプロパティ (workers.properties)
- B.2.6 シングルサインオン用 Web サーバに関するプロパティ (user\_hssso\_httpsd.conf)
- B.2.7 データベースに関するプロパティ (HiRDB.ini)
- B.2.8 データベースに関するプロパティ (pdsys)
- B.2.9 データベースに関するプロパティ (def\_pdsys)
- B.2.10 データベースに関するプロパティ (pdutysys)
- B.2.11 データベースに関するプロパティ (def\_pdutysys)
- B.2.12 ユーザーアカウントに関するプロパティ (user.conf)
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)

- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)
- B.2.17 監査ログに関するプロパティ (auditlog.conf)
- B.2.18 管理サーバをクラスタ構成にする場合に設定が必要なプロパティ (cluster.conf)

## B.2.3 Web サーバに関するプロパティ (user\_httpsd.conf)

user\_httpsd.conf ファイルに記載する Hitachi Command Suite 共通コンポーネントの Web サーバ通信に関するプロパティの一覧を次の表に示します。

プロパティ	説明
ServerName <ホスト名>	管理サーバのホスト名または IP アドレスを指定します。 デフォルト値は、OS に設定されているホスト名です。 管理サーバのホスト名、または IP アドレスが変更になるときに 見直しが必要です。 変更する場合は、ホスト名を指定することを推奨します。 SSL 通信する場合は、証明書発行要求の作成時に指定したホスト 名と同じにしてください。大文字と小文字は区別されます。
Listen <ポート番号>	HBase 64 Storage Mgmt Web Service にアクセスするための ポート番号を指定します。 デフォルト値は、「22015」です。 変更する場合は、Listen [::]:プロパティおよび#Listen 127.0.0.1:プロパティでも同じポート番号を指定してくださ い。
Listen [::]: <ポート番号>	HBase 64 Storage Mgmt Web Service にアクセスするための ポート番号を指定します。 デフォルト値は、「22015」です。 変更する場合は、Listen プロパティおよび#Listen 127.0.0.1:プロパティと同じポート番号を指定してください。
#Listen 127.0.0.1:<ポート番号>	SSL 通信用のパラメーター。SSL 通信する場合で、かつ外部か ら管理サーバへの非 SSL 通信を遮断したい場合は、Listen プロ パティと Listen [::]:プロパティの行頭に#を追記してコメ ント行にしたあと、このプロパティの行頭にある#を削除してく ださい。 HBase 64 Storage Mgmt Web Service にアクセスするための ポート番号を指定します。 デフォルト値は、「22015」です。 変更する場合は、Listen プロパティおよび Listen [::]:プ ロパティと同じポート番号を指定してください。
#Listen <ポート番号>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削 除してください。 SSL 通信で HBase 64 Storage Mgmt Web Service にアクセス するためのポート番号を指定します。 デフォルト値は、「22016」です。 変更する場合は、#Listen [::]:プロパティでも同じポート番 号を指定してください。
#Listen [::]: <ポート番号>	SSL 通信用のパラメーター。SSL 通信する場合も行頭の#は削 除しないでください。 SSL 通信で HBase 64 Storage Mgmt Web Service にアクセス するためのポート番号を指定します。 デフォルト値は、「22016」です。 変更する場合は、#Listen プロパティと同じポート番号を指定 してください。
#<VirtualHost <ホスト名>:<ポート 番号>>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削 除してください。 <ホスト名>には、「*」を指定します。

プロパティ	説明
	<ポート番号>には、SSL 通信で HBase 64 Storage Mgmt Web Service にアクセスするためのポート番号を指定します。デフォルト値は、「22016」です。
# ServerName <ホスト名>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。 管理サーバのホスト名を指定します。デフォルトは OS に設定されているホスト名です。 管理サーバのホスト名が変更になるときに見直しが必要です。証明書発行要求の作成時に指定したホスト名と同じにしてください。大文字と小文字は区別されます。
# SSLEnable	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。
# SSLProtocol	
# SSLRequiredCiphers	
# SSLRequireSSL	
# SSLCertificateKeyFile <秘密鍵ファイルパス>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。 RSA 暗号用の秘密鍵ファイルを絶対パスで指定します。 パスに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。
# SSLCertificateFile <証明書ファイルパス>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。 RSA 暗号用のサーバ証明書（認証局から返送された署名済みのサーバ証明書、または自己署名証明書）のファイルを絶対パスで指定します。 パスに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。
# SSLECCCertificateKeyFile <秘密鍵ファイルパス>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。 楕円曲線暗号用の秘密鍵ファイルを絶対パスで指定します。 パスに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。
# SSLECCCertificateFile <証明書ファイルパス>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。 楕円曲線暗号用のサーバ証明書（認証局から返送された署名済みのサーバ証明書、または自己署名証明書）のファイルを絶対パスで指定します。 パスに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。
# SSLCACertificateFile <認証局の証明書ファイルパス>	SSL 通信用のパラメーター。通常は行頭の#を削除する必要はありません。 チェインした認証局で発行されたサーバ証明書を使用して運用する場合に、行頭の#を削除して、チェインした認証局の証明書ファイルを絶対パスで指定します。複数の証明書（PEM 形式）をテキストエディターで連結させることで、1つのファイルに複数の証明書を混在させることができます。ただし、パスに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。
# </VirtualHost>	SSL 通信用のパラメーター。SSL 通信する場合は、行頭の#を削除してください。
#HWSLogSSLVerbose On	
<Location / ComputeSystemsManager>	管理サーバに接続でき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。



プロパティ	説明
	このプロパティで、管理サーバに接続できる管理クライアントの情報を設定する詳細については、表の下に示す「<Location / ComputeSystemsManager>の指定方法」を参照してください。

### <Location /ComputeSystemsManager>の指定方法

次の書式で記述します。

```
<Location /ComputeSystemsManager>
order allow,deny
allow from <管理クライアント> [<管理クライアント>...]
</Location>
```

order

必ず形式どおりに指定してください。余分な半角スペースやタブなどを挿入すると動作しません。

```
allow from <管理クライアント> [<管理クライアント>...]
```

次のどれかの形式で<管理クライアント>を指定できます。

- ドメイン名、またはドメイン名の一部
- 完全な IPv4 アドレス、または IPv4 アドレスの一部
- 「IPv4 のネットワーク/ネットマスク」の形式
- 「IPv4 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 進の整数です。

複数の管理クライアントのアクセスを許可するには、次のように指定します。

- 1 つの allow from で、複数の<管理クライアント>を指定する場合は、半角スペースで区切る
- allow from の指定を複数行で記述する

管理サーバで Hitachi Command Suite 製品の GUI または CLI 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。

hitachi.com ドメイン内のすべてのコンピュータの管理クライアントからはアクセスできるようにし、かつ、そのほかのドメイン内にある管理クライアントはアクセスさせないようにするための指定例を、次に示します。

```
<Location /ComputeSystemsManager>
order allow,deny
allow from hitachi.com
</Location>
```

上記の例の場合、<管理クライアント>は次のどれかの形式で記述できます。

- ドメイン名 (例: hitachi.datasystem.com)
- ドメイン名の一部 (例: hitachi)
- 完全な IPv4 アドレス (例: 10.1.2.3 127.0.0.1)
- 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 のネットワーク/c」の CIDR 形式 (例: 10.1.0.0/16)

### 関連項目

- (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ

- (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- 5.2.2 管理サーバで SSL 通信するよう設定する (管理クライアントとの通信路)
- 5.7.2 管理クライアントからの接続を制限する
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## B.2.4 Web コンテナサーバに関するプロパティ (usrconf.properties)

usrconf.properties ファイルに記載する Web コンテナサーバとの通信に関するプロパティの一覧を次の表に示します。

usrconf.properties ファイルは、Web コンテナサーバごとにあります。

Hitachi Command Suite 共通コンポーネントのシングルサインオン用 Web コンテナサーバに関するプロパティの一覧を次に示します。

**表 B-1 Hitachi Command Suite 共通コンポーネントのシングルサインオン用 Web コンテナサーバに関するプロパティ (usrconf.properties)**

プロパティ	説明
webserver.connector.ajp13.port	HBase 64 Storage Mgmt SSO Service で使用されるポート番号です。デフォルト値は、「22035」です。変更する場合は、workers.properties の worker.HBase64StgMgmtSSOService.port プロパティに同じポート番号を指定してください。
ejbserver.rmi.naming.port	HBase 64 Storage Mgmt SSO Service で使用されるポート番号です。デフォルト値は、「22036」です。
ejbserver.http.port	HBase 64 Storage Mgmt SSO Service で使用されるポート番号です。デフォルト値は、「22037」です。
ejbserver.rmi.remote.lister.port	HBase 64 Storage Mgmt SSO Service で使用されるポート番号です。デフォルト値は、「22038」です。

Compute Systems Manager 用 Web コンテナサーバに関するプロパティの一覧を次に示します。

**表 B-2 Compute Systems Manager 用 Web コンテナサーバに関するプロパティ (usrconf.properties)**

プロパティ	説明
webserver.connector.ajp13.port	HCS Compute Systems Manager Web Service で使用されるポート番号です。デフォルト値は、「22027」です。変更する場合は、workers.properties の worker.ComputeSystemsManagerWebService.port プロパティに同じポート番号を指定してください。
ejbserver.rmi.naming.port	HCS Compute Systems Manager Web Service で使用されるポート番号です。デフォルト値は、「22028」です。
ejbserver.http.port	HCS Compute Systems Manager Web Service で使用されるポート番号です。デフォルト値は、「22613」です。

プロパティ	説明
<code>ejbserver.rmi.remote.lister.port</code>	HCS Compute Systems Manager Web Service で使用されるポート番号です。 デフォルト値は、「22614」です。

#### 関連項目

- ・ (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- ・ B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- ・ B.2.5 Web コンテナサーバに関するプロパティ (`workers.properties`)

## B.2.5 Web コンテナサーバに関するプロパティ (`workers.properties`)

`workers.properties` ファイルに記載する Hitachi Command Suite 共通コンポーネントの Web コンテナサーバとの通信に関するプロパティの一覧を次の表に示します。

プロパティ	説明
<code>worker.ComputeSystemsManagerWebService.port</code>	Web サーバにアクセスするためのポート番号を指定します。 デフォルト値は、「22027」です。 変更する場合は、Compute Systems Manager 用の <code>usrconf.properties</code> にある <code>webserver.connector.ajp13.port</code> プロパティに同じポート番号を指定してください。
<code>worker.HBase64StgMgmtSSOService.port</code>	Web サーバにアクセスするためのポート番号を指定します。 デフォルト値は、「22035」です。 変更する場合は、Hitachi Command Suite 共通コンポーネントのシングルサインオン用の <code>usrconf.properties</code> にある <code>webserver.connector.ajp13.port</code> プロパティに同じポート番号を指定してください。

#### 関連項目

- ・ (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- ・ B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- ・ B.2.4 Web コンテナサーバに関するプロパティ (`usrconf.properties`)

## B.2.6 シングルサインオン用 Web サーバに関するプロパティ (`user_hssso_httpsd.conf`)

`user_hssso_httpsd.conf` ファイルに記載する Hitachi Command Suite 共通コンポーネントのシングルサインオン用 Web サーバとの通信に関するプロパティの一覧を次の表に示します。

プロパティ	説明
<code>Listen</code>	HBase 64 Storage Mgmt Web SSO Service にアクセスするためのポート番号を指定します。 デフォルト値は、「22031」です。

#### 関連項目

- ・ (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ

- [B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは](#)
- [B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧](#)

## B.2.7 データベースに関するプロパティ (HiRDB.ini)

Hitachi Command Suite 共通コンポーネントの HiRDB.ini ファイルに記載するデータベースに関するプロパティの一覧を次の表に示します。

プロパティ	説明
PDNAMEPORT	データベースが使用するポート番号を指定します。 デフォルト値は、「22032」です。 変更する場合は、pdsys の pd_name_port プロパティ、および def_pdsys の pd_name_port プロパティに同じポート番号を指定してください。
PDHOST	IP アドレスを指定します。通常は変更する必要はありません。 管理サーバのホスト名、または IP アドレスが変更になるときに見直しが必要です。 変更前の IP アドレスが指定されている場合は、ループバックアドレス 127.0.0.1 に変更してください。

### 関連項目

- [\(1\) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [\(1\) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [\(2\) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)
- [B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは](#)
- [B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧](#)
- [B.2.8 データベースに関するプロパティ \(pdsys\)](#)
- [B.2.9 データベースに関するプロパティ \(def\\_pdsys\)](#)

## B.2.8 データベースに関するプロパティ (pdsys)

Hitachi Command Suite 共通コンポーネントの pdsys ファイルに記載するデータベースに関するプロパティの一覧を次の表に示します。

プロパティ	説明
pd_name_port	データベースが使用するポート番号を指定します。 デフォルト値は、「22032」です。 変更する場合は、HiRDB.ini の PDNAMEPORT プロパティ、および def_pdsys の pd_name_port プロパティに同じポート番号を指定してください。
pdunit -x	IP アドレスを指定します。通常は変更する必要はありません。 管理サーバのホスト名、または IP アドレスが変更になるときに見直しが必要です。 変更前の IP アドレスが指定されている場合は、ループバックアドレス 127.0.0.1 に変更してください。

### 関連項目

- [\(1\) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ](#)

- ・ (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- ・ B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- ・ B.2.7 データベースに関するプロパティ (HiRDB.ini)
- ・ B.2.9 データベースに関するプロパティ (def\_pdsys)

## B.2.9 データベースに関するプロパティ (def\_pdsys)

Hitachi Command Suite 共通コンポーネントの def\_pdsys ファイルに記載するデータベースに関するプロパティの一覧を次の表に示します。

プロパティ	説明
pd_name_port	データベースが使用するポート番号を指定します。 デフォルト値は、「22032」です。 変更する場合は、HiRDB.ini の PDNAMEPORT プロパティ、および pdsys の pd_name_port プロパティに同じポート番号を指定してください。
pdunit -x	IP アドレスを指定します。通常は変更する必要はありません。 管理サーバのホスト名、または IP アドレスが変更になるときに直視が必要ですが、変更前の IP アドレスが指定されている場合は、ループバックアドレス 127.0.0.1 に変更してください。

### 関連項目

- ・ (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- ・ B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- ・ B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- ・ B.2.7 データベースに関するプロパティ (HiRDB.ini)
- ・ B.2.8 データベースに関するプロパティ (pdsys)

## B.2.10 データベースに関するプロパティ (pdutsys)

Hitachi Command Suite 共通コンポーネントの pdutdsys ファイルに記載するデータベースに関するプロパティの一覧を次の表に示します。

プロパティ	説明
pd_hostname	IP アドレスを指定します。通常は変更する必要はありません。 管理サーバのホスト名、または IP アドレスが変更になるときに直視が必要ですが、変更前の IP アドレスが指定されている場合は、ループバックアドレス 127.0.0.1 に変更してください。

## 関連項目

- (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- B.2.7 データベースに関するプロパティ (HiRDB.ini)
- B.2.11 データベースに関するプロパティ (def\_pdutsys)

## B.2.11 データベースに関するプロパティ (def\_pdutsys)

Hitachi Command Suite 共通コンポーネントの def\_pdutsys ファイルに記載するデータベースに関するプロパティの一覧を次の表に示します。

プロパティ	説明
pd_hostname	IP アドレスを指定します。通常は変更する必要はありません。 管理サーバのホスト名、または IP アドレスが変更になるときに見直しが必要です。 変更前の IP アドレスが指定されている場合は、ループバックアドレス 127.0.0.1 に変更してください。

## 関連項目

- (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (2) 管理サーバの IP アドレス変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- B.2.7 データベースに関するプロパティ (HiRDB.ini)
- B.2.10 データベースに関するプロパティ (pdutsys)

## B.2.12 ユーザーアカウントに関するプロパティ (user.conf)

Hitachi Command Suite 共通コンポーネントの user.conf ファイルに記載するユーザーアカウントに関するプロパティの一覧を次の表に示します。

プロパティ	説明
account.lock.system	System アカウントを自動ロックおよび手動ロックの対象にするかどうかを指定します。 <ul style="list-style-type: none"><li>• 「true」: System アカウントもロックの対象になります。</li><li>• 「false」: System アカウントはロックの対象から外れます。</li></ul>

## 関連項目

- 3.2.2 System アカウントをロックの対象にする
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)

exauth.properties ファイルには、外部の LDAP ディレクトリサーバと連携して通信するためのプロパティを記載します。

LDAP ディレクトリサーバの情報を直接指定するか、DNS サーバに接続先の LDAP ディレクトリサーバの情報を照会するかによって、設定するプロパティが異なります。

次に示すファイルを exauth.properties ファイルのサンプルとして使用できます。

サンプルファイル格納先：

Windows：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%sample%conf%exauth.properties
```

Linux：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/sample/conf/exauth.properties
```

サンプルファイルは、次の場所にコピーして使用してください。

ファイル格納先：

Windows：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%conf%exauth.properties
```

Linux：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf/exauth.properties
```



**重要** プロパティを編集するときは、次の点に注意してください。

- 設定値は、大文字と小文字を区別してください。
- 設定値の先頭および末尾には半角スペースを入力しないでください。また、設定値は引用符 (") で囲まないでください。  
設定値にこれらの文字が含まれる場合、値は無視され、デフォルト値が採用されます。
- サンプルファイルをコピーして使用する場合、プロパティの設定値を変更したときは、プロパティの行頭にある#を削除してください。#を削除しない場合、変更した値は無視され、デフォルト値が採用されます。

LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルのプロパティ一覧を次の表に示します。

プロパティ	詳細
auth.server.type	外部認証サーバの種類を指定します。 <ul style="list-style-type: none"><li>「ldap」：LDAP ディレクトリサーバと連携する場合に指定します。</li><li>「internal」：LDAP ディレクトリサーバと連携しない場合に指定します。</li></ul> デフォルト値は、「internal」です。
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。



プロパティ	詳細
	<p>必ず1つ以上のサーバ識別名を指定してください。LDAP ディレクトリサーバを複数指定する場合は、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。同じサーバ識別名は重複して登録しないでください。</p> <ul style="list-style-type: none"> <li>指定できる値: 64 バイト以内の次の文字列 0~9 A~Z a~z ! # ( ) + - . = @ [ ] ^ _ { } ~</li> <li>デフォルト値: なし 初期値として「ServerName」が設定されています。</li> </ul>
auth.ldap.multi_domain	<p>auth.server.name プロパティで 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。</p> <ul style="list-style-type: none"> <li>「true」: マルチドメイン構成である場合に指定します。</li> <li>「false」: 冗長構成である場合に指定します。</li> </ul> <p>デフォルト値は、「false」です。</p>
auth.group.mapping	<p>外部認可サーバとも連携するかどうかを指定します。</p> <ul style="list-style-type: none"> <li>「true」: 外部認可サーバとも連携する場合に指定します。</li> <li>「false」: 外部認可サーバと連携しない場合に指定します。</li> </ul> <p>デフォルト値は、「false」です。</p>
auth.ocsp.enable	<p>LDAP ディレクトリサーバと StartTLS 通信する場合に、OCSP レスポンダーまたは CRL 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。</p> <ul style="list-style-type: none"> <li>「true」: 証明書の有効性を検証する場合に指定します。</li> <li>「false」: 証明書の有効性を検証しない場合に指定します。</li> </ul> <p>デフォルト値は、「false」です。</p>
auth.ocsp.responderURL	<p>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。</p>
auth.ldap.< auth.server.name の指定値 >.protocol	<p>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。</p> <ul style="list-style-type: none"> <li>「ldap」: 平文で通信する場合に指定します。</li> <li>「tls」: StartTLS 通信する場合に指定します。</li> </ul> <p>「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。</p> <ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_256_GCM_SHA384</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul>
auth.ldap.< auth.server.name の指定値 >.host <sup>*1</sup>	<p>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。この項目は必須です。</p> <p>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 アドレスを使用できます。</p>
auth.ldap.< auth.server.name の指定値 >.port	<p>LDAP ディレクトリサーバのポート番号を指定します。</p> <p>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。</p> <ul style="list-style-type: none"> <li>指定できる値: 1~65535</li> <li>デフォルト値: 389</li> </ul>
auth.ldap.< auth.server.name の指定値 >.timeout	<p>LDAP ディレクトリサーバと接続するときの接続待ち時間を秒単位で指定します。</p>



プロパティ	詳細
	<ul style="list-style-type: none"> <li>指定できる値：0～120</li> <li>デフォルト値：15</li> </ul> <p>「0」を指定した場合、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。</p>
<p>auth.ldap.&lt; auth.server.name の指定値&gt;.attr</p>	<p>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 (AttributeType) を指定します。この項目は必須です。</p> <ul style="list-style-type: none"> <li>階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を Hitachi Command Suite 製品のユーザー ID として使用します。※2 例：ActiveDirectory を使用している場合で、Windows のログオン ID をユーザー ID として使用したいときは、Windows のログオン ID が値として定義されている属性名「sAMAccountName」を指定します。</li> <li>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。 デフォルト値は、「sAMAccountName」です。</li> </ul>
<p>auth.ldap.&lt; auth.server.name の指定値&gt;.basedn</p>	<p>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) を指定します。この項目は必須です。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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p>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。 半角スペース # + ; , &lt; = &gt; ¥</p>
<p>auth.ldap.&lt; auth.server.name の指定値&gt;.retry.interval</p>	<p>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を指定します。</p> <ul style="list-style-type: none"> <li>指定できる値：1～60</li> <li>デフォルト値：1</li> </ul>
<p>auth.ldap.&lt; auth.server.name の指定値&gt;.retry.times</p>	<p>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を指定します。</p> <ul style="list-style-type: none"> <li>指定できる値：0～50</li> <li>デフォルト値：20</li> </ul> <p>「0」を指定した場合、リトライされません。</p>
<p>auth.ldap.&lt; auth.server.name の指定値&gt;.domain.name</p>	<p>LDAP ディレクトリサーバが管理するドメインの名称を指定します。 次に示す構成の場合、この項目は必須です。</p> <ul style="list-style-type: none"> <li>DNS サーバに LDAP ディレクトリサーバの情報を照会する場合</li> <li>LDAP ディレクトリサーバの情報を直接指定、かつ、外部認可サーバと連携する場合</li> </ul>
<p>auth.ldap.&lt; auth.server.name の指定値&gt;.domain</p>	<p>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を指定します。 ログイン時に、ユーザー ID を「&lt;ユーザー ID &gt;@&lt;このプロパティで指定したドメイン名 &gt;」の形式で入力すると、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。</p>

プロパティ	詳細
	LDAP ディレクトリサーバのサーバ識別子ごとにドメイン名を指定する際は、ドメイン名が重複しないようにしてください。ドメイン名の大文字と小文字は区別されません。 LDAP ディレクトリサーバがマルチドメイン構成の場合、この項目は必須です。
auth.ldap.< auth.server.name の指定値 >.dns_lookup	DNS サーバに LDAP ディレクトリサーバの情報を照会するかどうかを指定します。 <ul style="list-style-type: none"> <li>「true」: DNS サーバに照会する場合に指定します。</li> <li>「false」: DNS サーバに照会しないで、直接指定する場合に指定します。</li> </ul> デフォルト値は、「false」です。 「true」を指定した場合でも、次の属性に値が設定されている場合は、DNS サーバに照会しないで、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します。 <ul style="list-style-type: none"> <li>auth.ldap.&lt; auth.server.name の指定値 &gt;.host</li> <li>auth.ldap.&lt; auth.server.name の指定値 &gt;.port</li> </ul> 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の情報を照会できません。そのため、このプロパティに「true」は指定しないでください。

#### 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

Compute Systems Manager 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。

#### 関連項目

- 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧
- B.2.14 LDAP ディレクトリサーバとの連携に関するプロパティの設定例

## B.2.14 LDAP ディレクトリサーバとの連携に関するプロパティの設定例

LDAP ディレクトリサーバと連携するためのプロパティの設定例を次に示します。接続の種類によっては、指定値が異なります。

LDAP ディレクトリサーバの情報を直接指定する場合（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
```

LDAP ディレクトリサーバが冗長構成の場合：

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
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.dns_lookup=false
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.dns_lookup=false
```

LDAP ディレクトリサーバが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.ocsp.enable=false
auth.ocsp.responderURL=
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.ServerName1.dns_lookup=false
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
auth.ldap.ServerName2.dns_lookup=false
```

#### 関連項目

- 5.1 セキュリティの設定とは
- 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは
- 6.6.1 LDAP ディレクトリサーバと接続するよう設定する
- B.2.13 LDAP ディレクトリサーバとの連携に関するプロパティ (exauth.properties)

## B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)

exauth.properties ファイルには、外部の Kerberos サーバと連携して通信するためのプロパティを記載します。

Kerberos サーバの情報を直接指定するか、DNS サーバに接続先の Kerberos サーバの情報を照会するかによって、設定するプロパティが異なります。

次に示すファイルを exauth.properties ファイルのサンプルとして使用できます。

サンプルファイル格納先 :

Windows :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>%sample%conf
%exauth.properties
```

Linux :

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/sample/conf/
exauth.properties
```

サンプルファイルは、次の場所にコピーして使用してください。

ファイル格納先 :

Windows :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >%conf  
%exauth.properties

Linux :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/conf/  
exauth.properties



**重要** プロパティを編集するときは、次の点に注意してください。

- ・ 設定値は、大文字と小文字を区別してください。
- ・ 設定値の先頭および末尾には半角スペースを入力しないでください。また、設定値は引用符 (") で囲まないでください。  
設定値にこれらの文字が含まれる場合、値は無視され、デフォルト値が採用されます。
- ・ サンプルファイルをコピーして使用する場合、プロパティの設定値を変更したときは、プロパティの行頭に  
ある#を削除してください。#を削除しない場合、変更した値は無視され、デフォルト値が採用されます。

Kerberos サーバで認証する場合の exauth.properties ファイルのプロパティ一覧を次の表に示します。

プロパティ	詳細
auth.server.type	外部認証サーバの種類を指定します。 <ul style="list-style-type: none"><li>・ 「kerberos」: Kerberos サーバと連携する場合に指定します。</li><li>・ 「internal」: Kerberos サーバと連携しない場合に指定します。</li></ul> デフォルト値は、「internal」です。
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。 <ul style="list-style-type: none"><li>・ 「true」: 外部認可サーバと連携する場合に指定します。</li><li>・ 「false」: 外部認可サーバと連携しない場合に指定します。</li></ul> デフォルト値は、「false」です。
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS 通信する場合に、OCSP レスポンダーまたは CRL 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。 <ul style="list-style-type: none"><li>・ 「true」: 証明書の有効性を検証する場合に指定します。</li><li>・ 「false」: 証明書の有効性を検証しない場合に指定します。</li></ul> デフォルト値は、「false」です。
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。
auth.kerberos.default_realm	デフォルトのレルム名を指定します。この項目は必須です。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。
auth.kerberos.dns_lookup_kdc	DNS サーバに Kerberos サーバの情報を照会するかどうかを指定します。 <ul style="list-style-type: none"><li>・ 「true」: DNS サーバに照会する場合に指定します。</li><li>・ 「false」: DNS サーバに照会しないで、直接指定する場合に指定します。</li></ul> デフォルト値は、「false」です。「true」を指定した場合でも、次のすべてのプロパティに値を設定しているときは、DNS サーバに照会されません。 <ul style="list-style-type: none"><li>・ auth.kerberos.realm_name</li></ul>

プロパティ	詳細
	<ul style="list-style-type: none"> <li>auth.kerberos.&lt; auth.kerberos.realm_name の指定値 &gt;.realm</li> <li>auth.kerberos.&lt; auth.kerberos.realm_name の指定値 &gt;.kdc</li> </ul>
auth.kerberos.default_tkt_enc_types	<p>Kerberos 認証に使用する暗号タイプを指定します。</p> <ul style="list-style-type: none"> <li>指定できる値： <ul style="list-style-type: none"> <li>aes256-cts</li> <li>aes128-cts</li> <li>rc4-hmac</li> <li>des3-cbc-sha1</li> <li>des-cbc-md5</li> <li>des-cbc-crc</li> </ul> </li> <li>デフォルト値：なし (DES-CBC-MD5 での認証)</li> </ul> <p>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。</p>
auth.kerberos.clockskew	<p>管理サーバと Kerberos サーバ間の時刻の差の許容範囲を秒数で指定します。</p> <ul style="list-style-type: none"> <li>指定できる値：0~300</li> <li>デフォルト値：300</li> </ul> <p>指定した値よりも時刻に差がある場合、認証エラーになります。</p>
auth.kerberos.timeout	<p>Kerberos サーバと接続するときの接続待ち時間を秒数で指定します。</p> <ul style="list-style-type: none"> <li>指定できる値：0~120</li> <li>デフォルト値：3</li> </ul> <p>「0」を指定した場合、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。</p>
auth.kerberos.realm_name	<p>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。</p> <p>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、各サーバの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。</p>
auth.kerberos.< auth.kerberos.realm_name の指定値 >.realm	<p>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。</p> <p>プロパティの名称で、&lt;レルム名&gt;としている部分は、このプロパティの指定値で指定してください。</p>
auth.kerberos.< auth.kerberos.realm_name の指定値 >.kdc <sup>※1</sup>	<p>Kerberos サーバの情報を次の形式で指定します。この項目は必須です。</p> <p>&lt;ホスト名または IP アドレス&gt;[:&lt;ポート番号&gt;]</p> <ul style="list-style-type: none"> <li>&lt;ホスト名または IP アドレス&gt; 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。</li> <li>&lt;ポート番号&gt; 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。</li> </ul> <p>Kerberos サーバを複数指定する場合は、次のようにコンマ (,) で区切って指定します。</p> <p>&lt;ホスト名または IP アドレス&gt;[:&lt;ポート番号&gt;], &lt;ホスト名または IP アドレス&gt;[:&lt;ポート番号&gt;], ...</p>

プロパティ	詳細
auth.group.<レルム名>.protocol <sup>※2</sup>	LDAP ディレクトリサーバ接続のプロトコルです。 <ul style="list-style-type: none"> <li>「ldap」：平文による通信の場合に指定します。</li> <li>「tls」：StartTLS による通信の場合に指定します。</li> </ul> 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。 <ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_256_GCM_SHA384</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul> デフォルト値は、「ldap」です。
auth.group.<レルム名>.port	LDAP ディレクトリサーバのポート番号を指定します。 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。 <ul style="list-style-type: none"> <li>指定できる値：1～65535</li> <li>デフォルト値：389</li> </ul>
auth.group.<レルム名>.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の DN (BaseDN) を指定します。 この DN より下の階層のユーザーエントリが認可の対象となります。検索対象のユーザーエントリ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。 半角スペース # + ; , < = > ¥ 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。
auth.group.<レルム名>.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を秒単位で指定します。 <ul style="list-style-type: none"> <li>指定できる値：0～120</li> <li>デフォルト値：15</li> </ul> 「0」を指定した場合、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。
auth.group.<レルム名>.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を指定します。 <ul style="list-style-type: none"> <li>指定できる値：1～60</li> <li>デフォルト値：1</li> </ul>
auth.group.<レルム名>.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を指定します。 <ul style="list-style-type: none"> <li>指定できる値：0～50</li> <li>デフォルト値：20</li> </ul> 「0」を指定した場合、リトライされません。

注※1

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 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



LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。

#### 関連項目

- [5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは](#)
- [6.7.2 Kerberos サーバと接続するよう設定する](#)
- [B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは](#)
- [B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧](#)
- [B.2.16 Kerberos サーバとの連携に関するプロパティの設定例](#)

## B.2.16 Kerberos サーバとの連携に関するプロパティの設定例

Kerberos サーバと連携するためのプロパティの設定例を次に示します。接続の種類によっては、指定値が異なります。

Kerberos 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=kerberos
auth.group.mapping=false
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
```

Kerberos 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=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
```



Kerberos サーバが冗長構成の場合：

```
auth.server.type=kerberos
auth.group.mapping=false
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,kerberos.example.com:88
```

Kerberos サーバのレルム識別名を複数指定する場合：

```
auth.server.type=kerberos
auth.group.mapping=false
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=RealmName1,RealmName2
auth.kerberos.RealmName1.realm=EXAMPLE.COM
auth.kerberos.RealmName1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.RealmName2.realm=EXAMPLE.NET
auth.kerberos.RealmName2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

#### 関連項目

- 5.1 セキュリティの設定とは
- 5.6 LDAP ディレクトリサーバとの通信のセキュリティ設定とは
- 6.7.2 Kerberos サーバと接続するよう設定する
- B.2.15 Kerberos サーバとの連携に関するプロパティ (exauth.properties)

## B.2.17 監査ログに関するプロパティ (auditlog.conf)

Hitachi Command Suite 共通コンポーネントの auditlog.conf ファイルに記載する監査ログに関するプロパティの一覧を次の表に示します。

プロパティ	説明
Log.Facility	未使用 (指定しても無視されます)
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半角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。 大文字、小文字は区別されません。 次に示す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。 <ul style="list-style-type: none"><li>• 指定できる種別: 「StartStop」、「Authentication」、「ExternalService」、または「ConfigurationAccess」</li><li>• デフォルト値: 指定なし</li></ul>
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、イベントログに出力されます。 次に示す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。 <ul style="list-style-type: none"><li>• 指定できる値: 0~7</li><li>• デフォルト値: 6</li></ul>

監査事象の重要度とイベントログの種類への対応は、次の表のとおりです。

監査事象の重要度	イベントログの種類
0～3	エラー
4	警告
5～7	情報

auditlog.conf ファイルの例を次に示します。

```
# 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, 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。Windows の場合、「エラー」、「警告」および「情報」の重要度を持つ監査ログが出力されます。Linux の場合、分類が user として syslog.conf ファイルに定義された syslog ファイルに、監査ログが出力されます。

#### 関連項目

- 10.4.1 監査ログとは
- 10.4.2 監査ログの環境設定ファイルを設定する
- 10.4.4 監査ログの種類
- B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧

## B.2.18 管理サーバをクラスタ構成にする場合に設定が必要なプロパティ (cluster.conf)

Hitachi Command Suite 共通コンポーネントの cluster.conf ファイルに記載するクラスタ構成の設定に関するプロパティの一覧を次の表に示します。

プロパティ	説明
mode	実行系ノードの場合は、「online」を指定します。 待機系ノードの場合は、「standby」を指定します。
virtualhost	有効でアクセスできる IP アドレスが割り当てられている論理ホスト名※を指定します。 IP アドレスは指定できません。
onlinehost	実行系ノードのホスト名※を指定します。 IP アドレスは指定できません。
standbyhost	待機系ノードのホスト名※を指定します。 IP アドレスは指定できません。

注※

指定するホスト名から IP アドレスの名前解決ができることを確認してください。

#### 関連項目

- (1) 管理サーバのホスト名変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ

- [9.4.2 実行系ノードで新規インストールする \(Red Hat Enterprise Linux\)](#)
- [9.4.3 待機系ノードで新規インストールする \(Red Hat Enterprise Linux\)](#)
- [9.5.2 クラスタ環境に移行する \(Red Hat Enterprise Linux\)](#)
- [B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは](#)
- [B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧](#)

## B.3 デプロイメントマネージャーで使用されるポートに関するプロパティ (Port.ini)

Port.ini を使ってデプロイメントマネージャーで使用するポートを変更できます。

Port.ini ファイルの格納先を次に示します。

```
< Compute Systems Manager のインストールディレクトリ >%ComputeSystemsManager%DeploymentManager%PXE%Images%Port.ini
```

Port.ini ファイルで指定できるプロパティの一覧を次の表に示します。

プロパティ	説明
BackupRestoreUnicast	管理対象リソースのディスクをリストアしたり、バックアップしたりする際に使用されます。 デフォルトは「26501」です。 ポート番号の変更に失敗した場合は、「56020」が使用されます。
BOOTNIC	管理対象リソースを PXE ブートする際に使用されます。 デフォルトは「26502」です。 ポート番号の変更に失敗した場合は、「56022」が使用されます。
FSC	管理対象リソースを PXE ブートする際に使用されます。 デフォルトは「26503」です。 ポート番号の変更に失敗した場合は、「56030」が使用されます。
FTUnicast	管理対象リソースのディスクを操作する際に使用されます。 デフォルトは「26508」です。 ポート番号の変更に失敗した場合は、「56023」が使用されます。

### 関連項目

- [7.9 ポート変更時に編集するデプロイメントマネージャーのプロパティと設定ファイル](#)
- [B.2.1 Hitachi Command Suite 共通コンポーネントのプロパティとは](#)
- [B.2.2 Hitachi Command Suite 共通コンポーネントのプロパティの一覧](#)



# Compute Systems Manager が発行する JP1 イベント

ここでは、Compute Systems Manager で発行される JP1 イベントの内容について説明します。

- C.1 Compute Systems Manager が発行する JP1 イベントの属性
- C.2 事象種別ごとの JP1 イベント拡張属性

## C.1 Compute Systems Manager が発行する JP1 イベントの属性

Compute Systems Manager が発行する JP1 イベントの属性を説明します。

JP1 イベントの属性には、基本属性と拡張属性があります。

- 基本属性：すべての JP1 イベントが持っている属性  
次の通知情報を含みます。
  - イベント ID：重大度に応じて次の ID を示します。  
0x00012410：情報  
0x00012411：警告  
0x00012412：エラー
  - メッセージ：アラートの内容を示します。
- 拡張属性：Compute Systems Manager が独自に割り当てる属性  
共通情報と固有情報があります。事象種別によって通知される内容が異なります。  
拡張属性は、[アラート詳細情報] 画面など、Compute Systems Manager の GUI に表示されるアラート情報と同等の内容です。

### 関連項目

- 3.3.1 JP1/IM でのアラート監視とは
- 3.3.2 JP1/IM でアラート監視できるように設定する
- C.2 事象種別ごとの JP1 イベント拡張属性

## C.2 事象種別ごとの JP1 イベント拡張属性

Compute Systems Manager が発行する JP1 イベントの拡張属性は、事象種別によって通知される内容が異なります。

JP1 イベントとして通知される Compute Systems Manager のアラートに対応する事象種別を次に示します。

- SNMP：SNMP トラップに関するアラートです。
- PERFORMANCE：性能監視に関するアラートです。
- SVP：SVP に関するアラートです。
- N+M：N+M コールドスタンバイの構成変更に関するアラートです。
- HVM：HVM に関するアラートです。

事象種別ごとに、JP1 イベントの拡張属性として通知される内容を次の表に示します。

表 C-1 SNMP トラップに関するアラートで通知される JP1 イベントの拡張属性

拡張属性種別	属性名	通知情報	内容
共通情報	SEVERITY	重大度	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"><li>• 情報</li><li>• 警告</li><li>• エラー</li></ul>

拡張属性種別	属性名	通知情報	内容
			Compute Systems Manager のアラートレベル「障害」に対応します。
	PRODUCT_NAME	プロダクト名	/HITACHI/HCSM
	ROOT_OBJECT_TYPE	登録名タイプ	HOST
	OBJECT_TYPE	オブジェクトタイプ	SNMP_TRAP
	ROOT_OBJECT_NAME	登録名	アラートを通知したサーバ名を示します。
	OBJECT_NAME	オブジェクト名	アラートの発生部位を示します。
	OCCURRENCE	事象種別	SNMP
固有情報	HCSM_ALERT_LEVEL	アラートレベル	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>Information</li> <li>Warning</li> <li>Error</li> </ul>
	HCSM_RESOURCE_NAME	リソース名	ホスト名を示します。
	HCSM_ALERT_ID	アラート ID	アラート ID を示します。 先頭に「0x」が付かない 16 進数です。
	HCSM_RECEIVE_TIME	受信日時	アラートの受信日時を示します。
	HCSM_ALERT_NO	アラート番号	アラートのシーケンス番号を示します。
	HCSM_LOCATION	発生個所	アラートの発生個所を示します。
	SNMP_TRAP_OID	SNMP トラップ OID	SNMP トラップの OID を示します。
	SNMP_TRAP_OBJECT_NAME	SNMP トラップオブジェクト名	SNMP トラップの発生部位を示します。
	HCSM_THRESHOLD	しきい値	—
	HCSM_OCCURRENCE_S	回数	—
	HCSM_OCCURRENCE_TIME	発生日時	—
	HCSM_RELATED_ALERT_ID	関連アラート ID	—
	HCSM_NM_GROUP	N+M グループ	—

(凡例)

— : 通知されません。

表 C-2 性能監視に関するアラートで通知される JP1 イベントの拡張属性

拡張属性種別	属性名	通知情報	内容
共通情報	SEVERITY	重大度	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>情報</li> <li>警告</li> <li>エラー</li> </ul> Compute Systems Manager のアラートレベル「障害」に対応します。
	PRODUCT_NAME	プロダクト名	/HITACHI/HCSM

拡張属性種別	属性名	通知情報	内容
	ROOT_OBJECT_TYPE	登録名タイプ	HOST
	OBJECT_TYPE	オブジェクトタイプ	SERVER
	ROOT_OBJECT_NAME	登録名	アラートを通知したサーバ名を示します。
	OBJECT_NAME	オブジェクト名	アラートの発生部位を示します。
	OCCURRENCE	事象種別	PERFORMANCE
固有情報	HCSM_ALERT_LEVEL	アラートレベル	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul>
	HCSM_RESOURCE_NAME	リソース名	ホスト名を示します。
	HCSM_ALERT_ID	アラート ID	アラート ID を示します。 先頭に「0x」が付かない 16 進数です。
	HCSM_RECEIVE_TIME	受信日時	アラートの受信日時を示します。
	HCSM_ALERT_NO	アラート番号	アラートのシーケンス番号を示します。
	HCSM_LOCATION	発生個所	アラートの発生個所を示します。
	SNMP_TRAP_OID	SNMP トラップ OID	—
	SNMP_TRAP_OBJECT_NAME	SNMP トラップオブジェクト名	—
	HCSM_THRESHOLD	しきい値	アラートに設定されている性能しきい値を示します。
	HCSM_OCCURRENCE_S	回数	アラートに設定されている性能しきい値の超過回数を示します。
	HCSM_OCCURRENCE_TIME	発生日時	—
	HCSM_RELATED_ALERT_ID	関連アラート ID	—
	HCSM_NM_GROUP	N+M グループ	—

(凡例)

—：通知されません。

表 C-3 SVP に関するアラートで通知される JP1 イベントの拡張属性

拡張属性種別	属性名	通知情報	内容
共通情報	SEVERITY	重大度	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>• 情報</li> <li>• 警告</li> <li>• エラー</li> </ul> Compute Systems Manager のアラートレベル「障害」に対応します。
	PRODUCT_NAME	プロダクト名	/HITACHI/HCSM
	ROOT_OBJECT_TYPE	登録名タイプ	CHASSIS
	OBJECT_TYPE	オブジェクトタイプ	HARDWARE



拡張属性種別	属性名	通知情報	内容
	ROOT_OBJECT_NAME	登録名	アラートを通知したサーバ名を示します。
	OBJECT_NAME	オブジェクト名	アラートの発生部位を示します。
	OCCURRENCE	事象種別	SVP
固有情報	HCSM_ALERT_LEVEL	アラートレベル	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>Information</li> <li>Warning</li> <li>Error</li> </ul>
	HCSM_RESOURCE_NAME	リソース名	<ul style="list-style-type: none"> <li>シャーシまたはブレードサーバの場合シャーシ名を示します。</li> <li>ラックマウントサーバの場合サーバ名を示します。</li> </ul> 「<サーバ名> BMC (<BMC の IP アドレス>)」の形式で通知されます。
	HCSM_ALERT_ID	アラート ID	アラート ID を示します。 先頭に「0x」が付かない 16 進数です。
	HCSM_RECEIVE_TIME	受信日時	アラートの受信日時を示します。
	HCSM_ALERT_NO	アラート番号	アラートのシーケンス番号を示します。
	HCSM_LOCATION	発生個所	アラートの発生個所を示します。
	SNMP_TRAP_OID	SNMP トラップ OID	—
	SNMP_TRAP_OBJECT_NAME	SNMP トラップオブジェクト名	—
	HCSM_THRESHOLD	しきい値	—
	HCSM_OCCURRENCE_S	回数	—
	HCSM_OCCURRENCE_TIME	発生日時	アラートの発生日時を示します。
	HCSM_RELATED_ALERT_ID	関連アラート ID	関連するアラート ID を示します。
	HCSM_NM_GROUP	N+M グループ	—

(凡例)

— : 通知されません。

表 C-4 N+M コールドスタンバイの構成変更に関するアラートで通知される JP1 イベントの拡張属性

拡張属性種別	属性名	通知情報	内容
共通情報	SEVERITY	重大度	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>情報</li> <li>警告</li> <li>エラー</li> </ul> Compute Systems Manager のアラートレベル「障害」に対応します。
	PRODUCT_NAME	プロダクト名	/HITACHI/HCSM
	ROOT_OBJECT_TYPE	登録名タイプ	CHASSIS

拡張属性種別	属性名	通知情報	内容
	OBJECT_TYPE	オブジェクトタイプ	HARDWARE
	ROOT_OBJECT_NAME	登録名	アラートを通知したサーバ名を示します。
	OBJECT_NAME	オブジェクト名	アラートの発生部位を示します。
	OCCURRENCE	事象種別	N+M
固有情報	HCSM_ALERT_LEVEL	アラートレベル	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul>
	HCSM_RESOURCE_NAME	リソース名	シャージ名を示します。
	HCSM_ALERT_ID	アラート ID	アラート ID を示します。 先頭に「0x」が付かない 16 進数です。
	HCSM_RECEIVE_TIME	受信日時	アラートの受信日時を示します。
	HCSM_ALERT_NO	アラート番号	アラートのシーケンス番号を示します。
	HCSM_LOCATION	発生個所	アラートの発生個所を示します。
	SNMP_TRAP_OID	SNMP トラップ OID	—
	SNMP_TRAP_OBJECT_NAME	SNMP トラップオブジェクト名	—
	HCSM_THRESHOLD	しきい値	—
	HCSM_OCCURRENCES	回数	—
	HCSM_OCCURRENCE_TIME	発生日時	—
	HCSM_RELATED_ALERT_ID	関連アラート ID	—
	HCSM_NM_GROUP	N+M グループ	N+M グループ名を示します。

(凡例)

— : 通知されません。

表 C-5 HVM に関するアラートで通知される JP1 イベントの拡張属性

拡張属性種別	属性名	通知情報	内容
共通情報	SEVERITY	重大度	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>• 情報</li> <li>• 警告</li> <li>• エラー</li> </ul> Compute Systems Manager のアラートレベル「障害」に対応します。
	PRODUCT_NAME	プロダクト名	/HITACHI/HCSM
	ROOT_OBJECT_TYPE	登録名タイプ	SERVER
	OBJECT_TYPE	オブジェクトタイプ	HARDWARE
	ROOT_OBJECT_NAME	登録名	アラートを通知したサーバ名を示します。

拡張属性種別	属性名	通知情報	内容
	OBJECT_NAME	オブジェクト名	アラートの発生部位を示します。
	OCCURRENCE	事象種別	HVM
固有情報	HCSM_ALERT_LEVEL	アラートレベル	Compute Systems Manager のアラートレベルに対応した、次のどれかを示します。 <ul style="list-style-type: none"> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul>
	HCSM_RESOURCE_NAME	リソース名	サーバ名を示します。
	HCSM_ALERT_ID	アラート ID	アラート ID を示します。 先頭に「0x」が付かない 16 進数です。
	HCSM_RECEIVE_TIME	受信日時	アラートの受信日時を示します。
	HCSM_ALERT_NO	アラート番号	アラートのシーケンス番号を示します。
	HCSM_LOCATION	発生個所	アラートの発生個所を示します。
	SNMP_TRAP_OID	SNMP トラップ OID	—
	SNMP_TRAP_OBJECT_NAME	SNMP トラップオブジェクト名	—
	HCSM_THRESHOLD	しきい値	—
	HCSM_OCCURRENCE_S	回数	—
	HCSM_OCCURRENCE_TIME	発生日時	アラートの発生日時を示します。
	HCSM_RELATED_ALERT_ID	関連アラート ID	関連するアラート ID を示します。
	HCSM_NM_GROUP	N+M グループ	—

(凡例)

— : 通知されません。

#### 関連項目

- [3.3.1 JP1/IM でのアラート監視とは](#)
- [3.3.2 JP1/IM でアラート監視できるよう設定する](#)
- [C.1 Compute Systems Manager が発行する JP1 イベントの属性](#)



# バージョン 7.x.x からのアップグレード

ここでは、Compute Systems Manager をバージョン 7.x.x からアップグレードする手順について説明します。

- D.1 バージョン 7.x.x からのアップグレードとは
- D.2 アップグレードする前の確認事項
- D.3 バージョン 7.x.x からアップグレードする（非クラスタ環境の場合）
- D.4 バージョン 7.x.x からアップグレードする（クラスタ環境の場合）

## D.1 バージョン 7.x.x からのアップグレードとは

Compute Systems Manager をバージョン 7.x.x からアップグレードして運用するには、Compute Systems Manager のアップグレードインストールに加えて、幾つかの操作が必要です。

管理サーバにインストールされた Compute Systems Manager をバージョン 7.x.x からアップグレードする上で必要な操作は、管理サーバにクラスタ環境を設定しているかどうかによって異なります。操作手順の詳細については、それぞれの説明を参照してください。

### 関連項目

- D.2 アップグレードする前の確認事項
- D.3 バージョン 7.x.x からアップグレードする（非クラスタ環境の場合）
- D.4 バージョン 7.x.x からアップグレードする（クラスタ環境の場合）

## D.2 アップグレードする前の確認事項

バージョン 7.x.x からのアップグレードを開始する前に、次の項目を確認してください。

- バージョン 7.x.x の Compute Systems Manager は、アップグレード時にアンインストールされます。Compute Systems Manager のインストール先ディレクトリに追加したファイルまたはディレクトリは、アンインストール時に削除されます。再利用したい場合は、アップグレード前に退避してください。
- バージョン 8.0.0 以前の Hitachi Command Suite 製品がインストールされている場合は、アップグレードした Compute Systems Manager の運用を開始する前に、すべての Hitachi Command Suite 製品をバージョン 8.0.1 以降にアップグレードしてください。
- アップグレード後の管理サーバに、バージョン 7.x.x 以前の Hitachi Command Suite 製品をインストールしないでください。
- アップグレード後の Compute Systems Manager では、非 SSL 通信で使用するデフォルトのポート番号が次のとおり変更されます。

バージョン 7.x.x : 23015

バージョン 8.0.0 以降 : 22015

Web ブラウザーに登録している管理サーバの URL や、ファイアウォールの例外登録に非 SSL 通信用のポート番号を設定している場合は、これらの設定を見直してください。

- アップグレード後の管理サーバでは、コマンド名およびデフォルトのインストール先が次のとおり変更されます。

- コマンド名

「hcmdsxxxx」から「hcmds64xxxx」に変更されます。

- Compute Systems Manager のデフォルトのインストール先

バージョン 7.x.x :

32 ビット版 Windows : %ProgramFiles%¥HiCommand

64 ビット版 Windows : %ProgramFiles(x86)%¥HiCommand

バージョン 8.0.0 以降 :

%ProgramFiles%¥HiCommand

ただし、デプロイメントマネージャーは、%ProgramFiles(x86)%に設定されているディレクトリの配下にインストールされます。

%ProgramFiles%、および%ProgramFiles(x86)%は Windows の環境変数です。

- Hitachi Command Suite 共通コンポーネントのデフォルトのインストール先

バージョン 7.x.x :

< Compute Systems Manager のインストールディレクトリ >%Base

バージョン 8.0.0 以降 :

< Compute Systems Manager のインストールディレクトリ >%Base64

アップグレード前の管理サーバで、上記のコマンド名またはファイルパスを記述したスクリプトを使用していて、アップグレード後の管理サーバでも引き続き使用する場合は、スクリプトに記述しているコマンド名およびファイルパスを見直してください。

- 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている場合、Compute Systems Manager をアップグレードすると、これらの製品のユーザーアカウントは引き続き共有されます。

ユーザーアカウントの共有については、32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定についての説明を参照してください。

#### 関連項目

- 2.2.9 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とユーザーアカウントを共有する場合の設定を確認する
- D.1 バージョン 7.x.x からのアップグレードとは
- D.3 バージョン 7.x.x からアップグレードする (非クラスタ環境の場合)
- D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)

## D.3 バージョン 7.x.x からアップグレードする (非クラスタ環境の場合)

非クラスタ環境の管理サーバにインストールされている Compute Systems Manager を、バージョン 7.x.x からアップグレードします。

#### 事前に完了しておく操作

- インストールする前の確認作業
- 管理サーバの設定の確認  
アップグレード時に、バージョン 7.x.x の Compute Systems Manager から次の設定を引き継ぐことができます。
  - データベース
  - Compute Systems Manager を含む Hitachi Command Suite 製品のデータベースの認証情報
  - SNMP トラップ定義を含む MIB ファイル  
アップグレード後のインストール先ディレクトリに移動されます。
  - Compute Systems Manager サーバのプロパティファイル (user.properties ファイル、および logger.properties ファイル)  
バージョン 7.x.x のプロパティファイルの内容は、アップグレード後のプロパティファイルにマージされます。上記以外のファイルおよび設定内容は、アップグレードすると初期化されます。上記以外の設定を変更している場合は、必要に応じて設定内容を控えておいてください。
- デプロイメントマネージャーのアンインストール (デプロイメントマネージャーを使用している場合)

デプロイメントマネージャーは、アップグレード前にアンインストールする必要があります。アンインストールには、バージョン 7x.x のインストールメディアが必要です。

Compute Systems Manager のインストールウィザードで、デプロイメントマネージャーを選択してアンインストールしてください。

Compute Systems Manager をアップグレードする手順を次に示します。

1. インストールメディアを管理サーバにセットします。  
統合インストールメディアでウィンドウが自動で表示されない場合は、<統合インストールメディア>%index.html をダブルクリックしてウィンドウを開いてください。
2. インストールウィザードを起動します。
  - 単体インストールメディアの場合  
<Compute Systems Manager のインストールメディア>%HCSM\_SERVER%setup.exe を実行します。
  - 統合インストールメディアの場合  
表示された画面の [HCSM] を選択して、[Install] ボタンをクリックします。
3. インストールウィザードの指示に従って、それぞれの画面で必要な情報を指定します。
4. [インストール完了] 画面で、[完了] ボタンをクリックします。
5. アップグレード前に管理サーバの設定を変更していた場合は、必要に応じて再設定します。
6. Compute Systems Manager を再起動します。
7. Web ブラウザーで Compute Systems Manager にアクセスできることを確認します。



#### 重要

- SSL 通信をしている場合、または Hitachi Command Suite 共通コンポーネントのポート番号を変更している場合、[インストール完了] 画面で [インストール完了時に Hitachi Command Suite GUI を起動する。] チェックボックスを選択しても、GUI を起動できないことがあります。

その場合は、変更後の管理サーバの情報を確認して、Web ブラウザーのアドレスバーに Compute Systems Manager の URL を入力して GUI を起動してください。

また、次のショートカットの URL も変更してください。

Windows Server 2008 R2 の場合：

[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Compute Systems Manager] - [Login - HCSM] を右クリックすると表示される、[プロパティ] - [Web ドキュメント] タブの [URL]

Windows Server 2012 の場合：

[スタート] - [すべてのアプリ] - [Hitachi Command Suite] - [Compute Systems Manager] - [Login - HCSM] を右クリックすると表示される、[プロパティ] - [Web ドキュメント] タブの [URL]

- Web ブラウザーが Internet Explorer 11 の場合、Compute Systems Manager にログインしたあと、空白や遷移途中のウィンドウが表示されることがあります。

その場合は、再度 Web ブラウザーを起動し、アドレスバーに Compute Systems Manager の URL を入力してください。

新しいバージョンの Compute Systems Manager が使用できるようになります。

#### 関連項目

- [2.4.2 インストールする前の確認事項](#)
- [2.5.2 管理サーバにアクセスできるか確認する](#)
- [7.2 デプロイメントマネージャーをインストールするための前提条件](#)
- [7.5 デプロイメントマネージャーをインストールする](#)
- [8.1.2 Compute Systems Manager を起動する](#)



- 8.1.3 Compute Systems Manager を停止する
- D.1 バージョン 7.x.x からのアップグレードとは
- D.2 アップグレードする前の確認事項

## D.4 バージョン 7.x.x からアップグレードする (クラスタ環境の場合)

クラスタ環境の管理サーバにインストールされている Compute Systems Manager を、バージョン 7.x.x からアップグレードします。

### 事前に完了しておく操作

- インストールする前の確認作業
- クラスタ環境で運用する管理サーバの空き容量の確認
- クラスタ管理アプリケーションを使用して設定する前の確認
- 管理サーバの設定の確認  
アップグレード時に、バージョン 7.x.x の Compute Systems Manager から次の設定を引き継ぐことができます。
  - データベース
  - Compute Systems Manager を含む Hitachi Command Suite 製品のデータベースの認証情報
  - SNMP トラップ定義を含む MIB ファイル  
アップグレード後のインストール先ディレクトリに移動されます。
  - Compute Systems Manager サーバのプロパティファイル (user.properties ファイル、および logger.properties ファイル)  
バージョン 7.x.x のプロパティファイルの内容は、アップグレード後のプロパティファイルにマージされます。  
上記以外のファイルおよび設定内容は、アップグレードすると初期化されます。上記以外の設定を変更している場合は、必要に応じて設定内容を控えておいてください。
- データベースが使用するポート番号の確認  
Compute Systems Manager をアップグレードすると、データベースが使用するポート番号がデフォルト (22032/tcp) に設定されます。  
ポート番号をデフォルト以外の番号に変更して運用している場合は、ポート番号を控えておいてください。
- デプロイメントマネージャーのアンインストール (デプロイメントマネージャーを使用している場合)  
アップグレード前に、実行系および待機系の各ノードからアンインストールする必要があります。  
アンインストールには、バージョン 7.x.x のインストールメディアが必要です。Compute Systems Manager のインストールウィザードで、デプロイメントマネージャーを選択してアンインストールしてください。



**重要** インストールウィザードで指定するクラスタ管理アプリケーションのグループに、すでに Hitachi Command Suite 製品のサービスが登録されている場合は、次の点に注意してください。  
登録されているサービスは、実行系ノードでのインストール時にすべて削除され、待機系ノードでのインストール時にデフォルトの設定で再登録されます。サービスのリソース名を変更している場合は、必要に応じて事前にリソース名を控えておき、インストール後に手動で変更してください。

クラスタ環境で Compute Systems Manager をアップグレードする手順を次に示します。

1. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を実行系ノードに移動し、クラスタ管理 IP アドレスと共有ディスクをオンラインにします。
2. 実行系ノードで Compute Systems Manager をアップグレードインストールします。  
インストールウィザードでは、クラスタ構成でのインストールを選択して、それぞれの画面で必要な情報を指定します。ほかの Hitachi Command Suite 製品ですでにクラスタ環境が構築されている場合は、その設定が適用されるため、再度指定する必要はありません。
3. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を待機系ノードに移動します。
4. 待機系ノードで Compute Systems Manager をアップグレードインストールします。  
インストールの際には、次の条件に従ってください。
  - インストール先を実行系ノードと同じにしてください。
  - 実行系ノードでデプロイメントマネージャーをインストールした場合は、待機系ノードでもインストールしてください。



**重要** 待機系ノードで複数の Hitachi Command Suite 製品を新規インストールする場合は、実行系ノードでインストールした順番で製品をインストールしてください。

5. データベースが使用するポート番号をデフォルト以外の番号に変更して運用する場合は、控えておいたポート番号を実行系および待機系の各ノードで設定します。



**重要** 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品がインストールされている場合は、その製品が使用するポート番号と競合しないことを確認してください。

6. 次のコマンドを実行して、Compute Systems Manager のクラスタ運用を開始します。  
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ (バージョン 8 以降) > %ClusterSetup%hcmds64clustersrvstate /son /r <グループ名 >
7. プラグインライセンスを登録する場合は、待機系ノードでライセンスキーを入力します。
8. 日立製のサーバを管理対象にしている場合は、必要に応じて、日立製のサーバに登録される管理サーバの IP アドレスがクラスタ管理 IP アドレスになるように設定を変更します。  
実行系および待機系の各ノードで、次のファイルの `svp.bind.address` プロパティに、クラスタ管理 IP アドレスを指定します。  
< Compute Systems Manager のインストールディレクトリ > %ComputeSystemsManager%conf%user.properties



#### 参考

- `svp.bind.address` プロパティを指定しない場合、日立製のサーバには実行系および待機系の各ノードの IP アドレスが登録されます。
  - すでに運用中の日立製のサーバには、通信先の管理サーバの IP アドレスが登録されています。  
`svp.bind.address` プロパティを指定すると、プロパティに指定した IP アドレスも新しく登録されます。日立製のサーバに登録されている管理サーバの IP アドレスは、Web コンソールで確認できます。  
使用していない管理サーバの IP アドレスが残っている場合は削除してください。
9. クラスタ管理アプリケーションで、Compute Systems Manager のサービスを登録するグループの所有者を実行系ノードに移動します。
  10. 待機系ノードでプラグインライセンスを登録した場合は、実行系ノードでも同様にライセンスキーを入力します。

11. デプロイメントマネージャーをインストールした場合は、デプロイメントマネージャーを使用するためのクラスタ環境を設定します。

新しいバージョンの Compute Systems Manager が使用できるようになります。

#### 関連項目

- 2.4.2 インストールする前の確認事項
- 2.4.3 Compute Systems Manager をインストールする (Windows)
- (1) ポート変更時に編集する Hitachi Command Suite 共通コンポーネントのプロパティ
- (3) ポートを変更する
- 7.2 デプロイメントマネージャーをインストールするための前提条件
- 7.5 デプロイメントマネージャーをインストールする
- 9.1 クラスタを使用するための環境設定と運用とは
- 9.3.1 クラスタ運用を開始する環境設定手順の確認
- 9.3.2 クラスタ環境で運用する管理サーバの空き容量の確認
- 9.3.3 クラスタ管理アプリケーションを使用して設定する前の確認
- 9.7.1 クラスタ環境でウィルス検出プログラムを使用する場合に必要な設定
- 9.7.2 クラスタ環境で同期が必要な設定
- 9.7.3 デプロイメントマネージャーを使用する場合のクラスタ環境を設定する
- 9.8.3 Compute Systems Manager のクラスタ運用を開始する (Windows)
- B.1.3 Compute Systems Manager サーバのポートや機能に関するプロパティ (user.properties)
- D.2 アップグレードする前の確認事項



## このマニュアルの参考情報

ここでは、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ます。

- E.1 関連マニュアル
- E.2 このマニュアルでの表記
- E.3 英略語
- E.4 KB（キロバイト）などの単位表記について
- E.5 ディレクトリとフォルダの表記について

## E.1 関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- *Hitachi Command Suite Compute Systems Manager ユーザーズガイド* (3021-9-096)
- *Hitachi Command Suite Compute Systems Manager CLI リファレンスガイド* (3021-9-099)
- *Hitachi Command Suite Compute Systems Manager メッセージ* (3021-9-100)
- *Hitachi Command Suite Compute Systems Manager REST API リファレンスガイド* (3021-9-101)
- *Hitachi Command Suite システム構成ガイド* (3021-9-008)
- *Hitachi Command Suite メッセージ* (3021-9-011)
- *Hitachi Command Suite 仮想アプライアンス インストールガイド* (3021-9-017)

## E.2 このマニュアルでの表記

このマニュアルでは、製品名を次のように表記しています。

表記	製品名
32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Hitachi File Services Manager</li><li>• Hitachi Storage Navigator Modular 2</li><li>• JP1/Automatic Operation</li></ul>
Alive Monitor	Hitachi Server Navigator - Alive Monitor
Device Manager	Hitachi Device Manager
Dynamic Link Manager	Hitachi Dynamic Link Manager
Global Link Manager	Hitachi Global Link Manager
J2EE	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• J2EE</li><li>• Java 2 Platform, Enterprise Edition</li></ul>
Java VM	Java Virtual Machine
JDK	Java Development Kit
JP1/IM	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• JP1/Integrated Management - Manager</li><li>• JP1/Integrated Management - View</li></ul>
JP1/IM - Manager	JP1/Integrated Management - Manager
JP1/IM - View	JP1/Integrated Management - View
JRE	Java Runtime Environment
Linux	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Oracle Enterprise Linux<sup>®</sup></li><li>• Oracle Linux<sup>®</sup></li><li>• Red Hat Enterprise Linux<sup>®</sup></li><li>• SUSE Linux<sup>®</sup> Enterprise Server</li></ul>
Oracle Linux	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"><li>• Oracle Enterprise Linux<sup>®</sup></li><li>• Oracle Linux<sup>®</sup></li></ul>
Red Hat Enterprise Linux	Red Hat Enterprise Linux <sup>®</sup>
Replication Manager	Hitachi Replication Manager
SUSE Linux	SUSE Linux <sup>®</sup> Enterprise Server

表記	製品名
Tiered Storage Manager	Hitachi Tiered Storage Manager
Tuning Manager	Hitachi Tuning Manager
Update Manager	Hitachi Server Navigator - Update Manager
VMware ESXi	VMware vSphere® ESXi™

## E.3 英略語

このマニュアルで使用する英略語を次に示します。

英略語	英字での表記
ARP	Address Resolution Protocol
BMC	Baseboard Management Controller
CDP	CRL Distribution Point
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CN	Common Name
CRL	Certificate Revocation List
CSV	Comma-Separated Values
DCOM	Distributed Component Object Model
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
DST	Daylight Saving Time
ECC	Elliptic Curve Cryptography
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PEM	Privacy Enhanced Mail
PXE	Preboot eXecution Environment
RFC	Request For Comments
RMI	Remote Method Invocation
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRV	SeRVice
SSH	Secure SHell
SSL	Secure Sockets Layer
SSO	Single Sign-On
SVP	SerVice Processor

英略語	英字での表記
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UAC	User Access Control
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WoL	Wake-on-Lan
WWPN	World Wide Port Name

## E.4 KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）はそれぞれ 1,024 バイト、1,024<sup>2</sup> バイト、1,024<sup>3</sup> バイト、1,024<sup>4</sup> バイトです。

## E.5 ディレクトリとフォルダの表記について

このマニュアルでは、Linux のディレクトリと Windows のフォルダを総称して「ディレクトリ」と表記しています。Windows 環境では、「ディレクトリ」を「フォルダ」に置き換えてお読みください。



# 用語解説

Compute Systems Manager を使用するために理解しておきたい用語の意味について解説します。

## (英字)

### Hitachi Command Suite 共通コンポーネント

Hitachi 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。ログイン、Web サービスなどの機能を提供します。

### HVM (Hitachi Virtualization Manager)

論理分割の機能で、LPAR を管理するブレードサーバ上のコンポーネントです。

### LID (Location IDentifier lamp)

シャーシや各モジュールを識別するためのランプです。Compute Systems Manager を使用して、ブレードまたはシャーシ上の LID を遠隔制御することで、データセンター内で管理対象リソースを特定しやすくします。

### LPAR (Logical PARtition)

論理分割の機能を使用している場合に、それぞれに独立したサーバ環境を作成して利用できる論理区画です。

### N+M コールドスタンバイ

障害に備えて、予備ブレードを電源オフ状態で待機させておくことです。稼働中の現用ブレードで障害が発生した場合、自動的に予備ブレードに切り替わります。

### VMM (Virtual Machine Manager)

ハイパーバイザーと関連する仮想マシンを管理するソフトウェアです（基本的な概念については、仮想マシンを参照してください）。複数のハイパーバイザーとそのハイパーバイザー上で起動しているすべての仮想マシンを管理対象にできます。VMM を使用して、仮想マシンの作成、仮想マシンの構成の変更、異なるハイパーバイザーへの仮想マシンの移動ができます。

### Web コンソール

日立製のサーバに付属しているソフトウェアです。シャーシやサーバのハードウェア情報を参照したり、遠隔操作したりできます。

### Web リモート KVM (Keyboard, Video and Mouse)

日立製のサーバに付属しているソフトウェアです。ホスト、サーバ、または LPAR を遠隔操作できます。

## (カ行)

### 外部認可ユーザー

外部認可サーバと連携する場合に、Compute Systems Manager に登録した認可グループに属するユーザーです。

### 仮想マシン (Virtual Machine)

コンピュータ内の独立したパーティションで、1つまたは複数のアプリケーションを実行している OS のインスタンスです。仮想マシンを使用すると、同一のコンピュータ上で複数の OS を同時に実行できるようになります。

### 管理クライアント

GUI または CLI クライアントの操作に使用するコンピュータです。

### 管理サーバ

Compute Systems Manager をインストールしたサーバです。管理対象リソースを一元管理します。

### 管理対象リソース

ホストや日立製のサーバなど、Compute Systems Manager で管理する対象となるリソースです。管理対象となる日立製のサーバは、ブレードサーバおよびラックマウントサーバです。

### 現用ブレード

N+M コールドスタンバイ機能を使用している場合、障害が発生したときに、予備ブレードと切り替わるブレードです。

## (サ行)

### 実行系ノード

クラスタ運用しているシステムで、実際に稼働しているホストです。

### 性能プロファイル

ユーザー定義による一連の性能情報とデータ取得間隔の設定です。管理対象ホストの性能情報の取得や分析に使用します。

## (タ行)

### 待機系ノード

クラスタ運用しているシステムで、障害が発生した場合に、実行系ノードで使用していたシステムリソースを引き継げるように待機しているホストです。

### 探索

Compute Systems Manager で管理対象となるリソースを発見する操作です。

### デプロイメントマネージャー

複数の管理対象リソースのディスクデータをイメージファイルとしてバックアップしたり、リストアしたりできる機能です。また、バックアップしたイメージファイルを使用して、管理対象リソースの環境をほかの管理対象リソースに複製もできます。

### 電力プロファイル

ユーザー定義による一連の電力情報とデータ取得間隔の設定です。シャーシの電力消費量の取得や分析に使用します。

## (ハ行)

### ハイパーバイザー

1 台の物理ホストコンピュータ上で複数のゲスト OS（仮想マシン）を同時に起動するためのソフトウェアです。各 OS は独立して起動しますが、ハイパーバイザーがホストプロセッサとリソースを制御します。

## (マ行)

### マネジメントモジュール

シャーシにインストールされたコンポーネントで、ブレードやその他のさまざまな共有電子部品を制御します。

## (ヤ行)

### ユーザーグループ

ユーザーアカウントをグルーピングしたものです。外部認可サーバと連携する場合は、認可グループをユーザーグループとしても利用できます。ユーザーグループにリソースグループおよびロールを割り当てることで、管理対象に対するアクセスを制御できます。

### 予備ブレード

N+M コールドスタンバイ機能を使用している場合、障害が発生した現用ブレードと切り替わるまで、電源オフの状態で待機するブレードです。

## (ウ行)

### リソースグループ

管理対象リソースをグルーピングしたものです。

### ロール

ユーザーグループ内のユーザーが、リソースグループ内のリソースに対して持つ操作権限です。

### 論理グループ

管理対象リソースをユーザー定義によってグルーピングしたものです。

### 論理分割

日立サーバ論理分割機構を使用して、1 台または複数台のブレードで構成されているブレードサーバを論理的に分割し、それぞれに独立したサーバ環境を作成して利用できる機能です。



# 索引

## 記号

- .NET Framework  
インストール [デプロイメントマネージャー] 156

## 数字

- 32 ビットの Hitachi Command Suite 共通コンポーネントを使用する製品とのユーザーアカウントの共有  
設定確認 45  
無効にする手順 55  
有効にする手順 54

## A

- auditlog.conf 281
- Authentication 236

## B

- BaseDN 128
- BMC 監視  
有効 90

## C

- cluster.conf 282
- Compute Systems Manager 22
  - 稼働状況確認 165
  - 起動 162
  - 起動 [概要] 162
  - サービス [クラスタ] 177
  - 常駐プロセス [Linux] 165
  - 常駐プロセス [Windows] 164
  - 停止 163
  - 停止 [概要] 162
- Compute Systems Manager サーバ

- プロパティ 258
- プロパティの一覧 258
- ポート 248

- Compute Systems Manager のログ  
設定変更 245
- ConfigurationAccess 236

## D

- DCOM  
有効 [Windows ホスト] 92
- WinRM  
有効 [Windows ホスト] 93
- def\_pdsys 269
- def\_pdsutys 270
- DeploymentManager API Service 164
- DeploymentManager Backup/Restore Management 164
- DeploymentManager Get Client Information 164
- DeploymentManager PXE Management 165
- DeploymentManager PXE Mtftp 165
- DeploymentManager Remote Update Service 165
- DeploymentManager Schedule Management 165
- DeploymentManager Transfer Management 165
- Device Manager サーバ  
セキュリティ設定 [概要] 115
- DNS サーバ照会条件  
LDAP ディレクトリサーバ 130
- DNS サーバに照会  
exauth.properties ファイルの設定項目 [Kerberos サーバ] 142, 143  
exauth.properties ファイルの設定項目 [LDAP ディレクトリサーバ] 138, 140

## E

- exauth.properties  
Kerberos サーバとの連携 276

LDAP ディレクトリサーバとの連携 271  
exauth.properties ファイルの設定項目  
DNS サーバに照会 [Kerberos サーバ] 142, 143  
DNS サーバに照会 [LDAP ディレクトリサーバ]  
138, 140  
Kerberos サーバ情報を直接指定 141, 142  
LDAP ディレクトリサーバ情報を直接指定 137, 139  
外部認可サーバ連携 [Kerberos サーバ] 142, 143  
外部認可サーバ連携 [LDAP ディレクトリサーバ]  
139, 140  
ExternalService 236  
E メール通知  
アラートレベル設定 59  
設定 59

## H

HBase 64 Storage Mgmt SSO Service 164  
HBase 64 Storage Mgmt Web Service 164  
HBase 64 Storage Mgmt Web SSO Service 164  
hcnds64checkauth 144  
hcnds64dbclustersetup 218  
hcnds64getlogs 229  
hcnds64keytool 150  
hcnds64ldapuser 147  
HCS Compute Systems Manager Web Service 164  
HiRDB.ini 268  
HiRDB/EmbeddedEdition\_HD1 164  
Hitachi Command Suite 共通コンポーネント  
ポート 248  
Hitachi Network Objectplaza Trace Monitor 2 164  
Hitachi Network Objectplaza Trace Monitor 2 (x64)  
164  
HVM  
JP1 イベント拡張属性 290

## I

IIS  
インストール 155  
IPv6 を使用する場合の設定 45  
IP アドレス  
変更 79  
IP アドレス変更  
マネジメントモジュール 101  
IP アドレス変更時に編集  
プロパティ [Hitachi Command Suite 共通コンポー  
ネント] 78  
IP 接続  
許可 [Linux ホスト] 96

## J

JDK  
変更 82  
JP1/IM  
アラート監視設定 70  
ラUNCH 71  
ラUNCHの設定 71  
JP1/IM でのアラート監視 70  
JP1 イベント拡張属性 286  
HVM 290  
N+M コールドスタンバイの構成変更 289  
SNMP トラップ 286  
SVP 288  
性能監視 287  
JP1 イベントの属性 286

## K

Kerberos サーバ  
接続設定 135  
プロパティの設定例 280  
Kerberos サーバ情報を直接指定  
exauth.properties ファイルの設定項目 141, 142  
Kerberos サーバとの連携  
exauth.properties 276  
作業フロー 35  
Kerberos 認証  
暗号タイプ 135  
keytool 150

## L

LDAP ディレクトリサーバ  
DNS サーバ照会条件 130  
StartTLS 通信設定 133  
証明書 149  
セキュリティ設定 116  
接続条件 130  
接続設定 131  
プロパティの設定例 274  
LDAP ディレクトリサーバ情報を直接指定  
exauth.properties ファイルの設定項目 137, 139  
LDAP ディレクトリサーバとの連携  
exauth.properties 271  
作業フロー 34  
Linux ホスト  
確認項目 95  
管理対象にするための確認事項 94  
logger.properties 260

## M

MIB ファイル  
登録 66

## N

N+M コールドスタンバイの構成変更  
JP1 イベント拡張属性 289

## P

pdsys 268  
pdutsys 269  
Port.ini 283

## R

root  
ログインの許可 [Linux ホスト] 97

## S

Severity 281  
SMTP サーバ  
セキュリティ設定 111  
SNMP トラップ 66  
JP1 イベント拡張属性 286  
監視 67  
設定 [Linux ホスト] 100  
設定 [Windows ホスト] 94  
SNMP トラップの設定  
作業フロー 29  
SQL Server (DPMDBI) 165  
SQL Server Agent (DPMDBI) 165  
SSL 通信  
設定 [CLI] 110  
設定 [GUI] 109  
SSL 通信設定  
管理サーバと Device Manager サーバ 116  
管理サーバと SMTP サーバ 111  
管理サーバと管理クライアント 105  
管理サーバと管理対象サーバ 112  
StartStop 236  
StartTLS 通信設定  
LDAP ディレクトリサーバ 133  
su  
利用許可 [Linux ホスト] 98  
sudo  
利用許可 [Linux ホスト] 99  
SVP  
JP1 イベント拡張属性 288

System アカウント  
パスワード変更 58  
メールアドレス設定 58  
ロック対象 68

## U

URL  
変更 81  
変更するタイミング 80  
user.conf 270  
user.properties 258  
user\_hssd\_httpsd.conf 267  
user\_httpsd.conf 263  
usrconf.properties  
Compute Systems Manager 266  
Hitachi Command Suite 共通コンポーネント [シン  
グルサインオン] 266

## W

Windows ホスト  
管理対象にするための確認事項 91  
WinRM  
設定 [Linux 管理サーバ] 86  
WoL  
有効 90  
workers.properties 267

## あ

アカウント  
設定 [Linux ホスト] 95  
ロック解除 69  
空き容量確認  
クラスタ 183  
アクセス確認  
管理サーバ 56  
アップグレード [バージョン 7.x.x からの場合]  
概要 294  
確認事項 294  
アップグレードインストール [バージョン 7.x.x からの  
場合]  
クラスタ環境 297  
非クラスタ環境 295  
アラート監視設定  
JP1/IM 70  
アラートレベル設定  
Eメール通知 59  
アンインストール  
Linux 63  
Windows 62

概要	61
確認事項	62
クラスタ [Red Hat Enterprise Linux]	221
クラスタ [Windows]	220
クラスタ [デプロイメントマネージャー]	219
暗号タイプ	
Kerberos 認証	135

## い

### 移行

確認事項 [データベース]	170
クラスタ [Red Hat Enterprise Linux]	197
クラスタ [Windows]	195

### 一時停止

クラスタ [Red Hat Enterprise Linux]	207
クラスタ [Windows]	206

### インストール

.NET Framework [デプロイメントマネージャー]	156
IIS	155
Linux	52
Windows	51
アップグレードまたは上書きインストール [Red Hat Enterprise Linux のクラスタ環境]	192, 193
インストール [Windows のクラスタ環境]	185

概要	49
確認事項	50
仮想アプライアンス	42
作業フロー	27
新規インストール [Red Hat Enterprise Linux のクラスタ環境]	187, 190
デプロイメントマネージャー	156

### インストール環境

確認	42
----	----

### インストール時の入力項目

検討	46
----	----

### インストールするための前提条件

デプロイメントマネージャー	154
---------------	-----

### インストールディレクトリ

確認	48
----	----

### インバンド SNMP トラップの監視

### インポート

データベース	171
データベース [Red Hat Enterprise Linux のクラスタ環境]	216
データベース [Windows のクラスタ環境]	215

## う

### ウイルス検出プログラムの設定

### 運用開始

クラスタ [Red Hat Enterprise Linux]	208
クラスタ [Windows]	207
運用するための前提条件	
デプロイメントマネージャー	157

## え

### エクスポート

データベース	170
データベース [Red Hat Enterprise Linux のクラスタ環境]	214
データベース [Windows のクラスタ環境]	212

## お

### 温度の単位

設定	84
----	----

## か

### カーネルパラメーター [Linux 管理サーバ]

設定	44
----	----

### 階層構造モデル

### 外部認可サーバ

### 外部認可サーバ連携

exauth.properties ファイルの設定項目 [Kerberos サーバ]	142, 143
exauth.properties ファイルの設定項目 [LDAP ディレクトリサーバ]	139, 140

### 外部認証サーバ

### 外部認証サーバとの連携

作業フロー	34
作業フロー [Kerberos サーバ]	124
作業フロー [LDAP ディレクトリサーバ]	123

### 外部認証サーバ連携で使用するコマンド

注意事項	144
------	-----

### 確認

インストール環境	42
インストールディレクトリ	48
監査ログ	235
管理サーバ情報	49
管理サーバのシステム環境 [Linux]	43
システム要件	43
ポート番号	43

### 確認項目

Linux ホスト	95
-----------	----

### 確認事項

アップグレード [バージョン 7.x.x からの場合]	294
アンインストール	62
移行 [データベース]	170
バックアップ [データベース]	167
リストア [データベース]	169



仮想アプライアンス 42

環境設定ファイル設定

  監査ログ 234

監査ログ 234

  確認 235

  環境設定ファイル設定 234

  メッセージ部 241

監査ログの種別 236

監視

  SNMP トラップ 67

管理クライアント

  セキュリティ設定 104

  接続制限 117

  接続制限〔概要〕 117

管理サーバ

  SSL 通信設定〔Device Manager サーバ〕 116

  SSL 通信設定〔SMTP サーバ〕 111

  SSL 通信設定〔管理クライアント〕 105

  SSL 通信設定〔管理対象サーバ〕 112

  アクセス確認 56

  システム環境の確認〔Linux〕 43

管理サーバ移行

  作業フロー 36

管理サーバ情報

  確認 49

管理対象

  Compute Systems Manager 22

管理対象サーバ

  セキュリティ設定 112

管理対象にするための確認事項

  Linux ホスト 94

  Windows ホスト 91

  日立製ブレードサーバ 90

  日立製ラックマウントサーバ 91

管理対象ホスト

  ログインの許可 96

管理対象ホスト設定

  作業フロー〔Linux〕 31

  作業フロー〔Windows〕 30

管理対象ホストの移行 100

管理対象ホストの設定

  作業フロー 29

管理対象リソース

  登録 59

  ブートの設定変更 158

完了

  初期設定作業 61

関連製品 25

## き

許可

IP 接続〔Linux ホスト〕 96

## く

クラスタ

  空き容量確認 183

  アンインストール〔Red Hat Enterprise Linux〕 221

  アンインストール〔Windows〕 220

  アンインストール〔デプロイメントマネージャー〕 219

  移行〔Red Hat Enterprise Linux〕 197

  移行〔Windows〕 195

  一時停止〔Red Hat Enterprise Linux〕 207

  一時停止〔Windows〕 206

  インストール〔Windows〕 185

  ウイルス検出プログラムの設定 205

  運用開始〔Red Hat Enterprise Linux〕 208

  運用開始〔Windows〕 207

  環境設定と運用 176

  実行系ノードでアップグレードまたは上書きインス

  トール〔Red Hat Enterprise Linux〕 192

  実行系ノードで新規インストール〔Red Hat

  Enterprise Linux〕 187

  設定手順確認 178

  待機系ノードでアップグレードまたは上書きインス

  トール〔Red Hat Enterprise Linux〕 193

  待機系ノードで新規インストール〔Red Hat

  Enterprise Linux〕 190

  デプロイメントマネージャーの環境設定 206

  同期が必要な設定 205

クラスタ管理アプリケーション

  サービスの削除〔Red Hat Enterprise Linux〕 204

  サービスの削除〔Windows〕 203

  サービスの登録〔Red Hat Enterprise Linux〕 202

  サービスの登録〔Windows〕 201

  設定前の確認 184

## け

検討

  インストール時の入力項目 46

## さ

サーバ管理者

  ユーザーアカウント作成 60

サーバ証明書

  削除 119

  有効期限確認 118

サービス

  Compute Systems Manager〔クラスタ〕 177

  サービスの削除

クラスタ管理アプリケーション [Red Hat Enterprise Linux]	204
クラスタ管理アプリケーション [Windows]	203
サービスの登録	
クラスタ管理アプリケーション [Red Hat Enterprise Linux]	202
クラスタ管理アプリケーション [Windows]	201
採取	
スレッドダンプ [Linux 管理サーバ]	232
スレッドダンプ [Windows 管理サーバ]	231
保守情報 [Linux ホスト]	234
保守情報 [Windows ホスト]	233
保守情報 [管理サーバ]	229
作業フロー	25
Kerberos サーバとの連携	35, 124
LDAP ディレクトリサーバとの連携	34, 123
SNMP トラップの設定	29
インストール	27
外部認証サーバとの連携	34
管理サーバ移行	36
管理対象ホスト設定 [Linux]	31
管理対象ホスト設定 [Windows]	30
管理対象ホストの設定	29
新規インストール	27
通信のセキュリティ設定 [Device Manager サーバ]	33
通信のセキュリティ設定 [LDAP ディレクトリサーバ]	33
通信のセキュリティ設定 [SMTP サーバ]	32
通信のセキュリティ設定 [管理クライアント]	31
通信のセキュリティ設定 [管理対象サーバ]	32
データベースの管理	37
デプロイメントマネージャーの環境設定	35
トラブルシューティング	38
ネットワーク構成変更	37
削除	
サーバ証明書	119
情報検索用ユーザーアカウント	149
サマータイム	45, 83
<b>し</b>	
シェル制限 [Linux 管理サーバ]	
設定	44
時刻	
調整	44
調整 [運用開始後]	83
システム構成	23
システム構成要素	23
システム要件	
確認	43
出力情報	
タスク操作	242
リクエスト受理時	243
リクエスト受理時 [詳細メッセージ]	243
レスポンス送信時	243
常駐プロセス	
Linux	165
Windows	164
デプロイメントマネージャー	164
冗長構成 [外部認証サーバ]	126
情報検索用ユーザーアカウント	146
削除	149
登録状況確認	148
証明書	
LDAP ディレクトリサーバ	149
証明書インポート	
注意事項 [LDAP ディレクトリサーバ]	149
初期設定作業	
完了	61
新規インストール	
作業フロー	27
新規インストール後に必要な作業	56
<b>す</b>	
スレッドダンプ	
採取 [Linux 管理サーバ]	232
採取 [Windows 管理サーバ]	231
<b>せ</b>	
性能監視	
JP1 イベント拡張属性	287
セキュリティ設定	104
Device Manager サーバ [概要]	115
LDAP ディレクトリサーバ	116
SMTP サーバ	111
管理クライアント	104
管理対象サーバ	112
接続条件	
LDAP ディレクトリサーバ	130
接続制限	
管理クライアント	117
管理クライアント [概要]	117
接続設定	
Kerberos サーバ	135
LDAP ディレクトリサーバ	131
設定	
E メール通知	59
IPv6	45
SNMP トラップ [Linux ホスト]	100
SNMP トラップ [Windows ホスト]	94
SSL 通信 [CLI]	110

SSL 通信 [GUI]	109
WinRM [Linux 管理サーバ]	86
アカウント [Linux ホスト]	95
温度の単位	84
カーネルパラメーターとシェル制限 [Linux 管理サーバ]	44
ファイアウォール [Windows ホスト]	92
ファイアウォールの例外登録 [Linux 管理サーバ]	85
ファイアウォールの例外登録 [Windows 管理サーバ]	85
ユーザーグループ	60
リソースグループ	60
リモート接続 [Windows ホスト]	93
設定手順確認	
クラスタ	178
設定変更	
Compute Systems Manager のログ	245
設定前の確認	
クラスタ管理アプリケーション	184
<b>た</b>	
タイムアウト時間	
変更	83
タスク操作	
出力情報	242
<b>ち</b>	
注意事項	
外部認証サーバ連携で使用するコマンド	144
証明書インポート [LDAP ディレクトリサーバ]	149
調整	
時刻	44
時刻 [運用開始後]	83
<b>つ</b>	
通信のセキュリティ設定	
作業フロー [Device Manager サーバ]	33
作業フロー [LDAP ディレクトリサーバ]	33
作業フロー [SMTP サーバ]	32
作業フロー [管理クライアント]	31
作業フロー [管理対象サーバ]	32
<b>て</b>	
データベース	
インポート	171
インポート [Red Hat Enterprise Linux のクラスタ環境]	216
インポート [Windows のクラスタ環境]	215
エクスポート	170
エクスポート [Red Hat Enterprise Linux のクラスタ環境]	214
エクスポート [Windows のクラスタ環境]	212
バックアップ	168
バックアップ [Red Hat Enterprise Linux のクラスタ環境]	209
バックアップ [Windows のクラスタ環境]	208
リストア	169
リストア [Red Hat Enterprise Linux のクラスタ環境]	211
リストア [Windows のクラスタ環境]	211
データベースの管理	166
作業フロー	37
適用時刻	83
デプロイメントマネージャー	
インストール	156
インストールするための前提条件	154
運用するための前提条件	157
環境設定 [クラスタ]	206
常駐プロセス	164
ポート	249
ポート番号変更	158
デプロイメントマネージャーの環境設定	154
作業フロー	35
<b>と</b>	
同期が必要な設定	
クラスタ	205
登録	
MIB ファイル	66
管理対象リソース	59
プラグインライセンス	57
登録状況確認	
情報検索用ユーザーアカウント	148
トラブルシューティング	224
作業フロー	38
トラブルシューティング事例	
Compute Systems Manager が起動しない	224
データベースをリストアできない	225
データベースをリストアできない [Red Hat Enterprise Linux のクラスタ環境]	227
データベースをリストアできない [Windows のクラスタ環境]	226
ログイン画面が表示されない	224
<b>ね</b>	
ネットワーク構成	25
ネットワーク構成変更	

**は**

- パス指定規則 47
- パスワード変更
  - System アカウント 58
- バックアップ
  - 確認事項 [データベース] 167
  - データベース 168
  - データベース [Red Hat Enterprise Linux のクラスタ環境] 209
  - データベース [Windows のクラスタ環境] 208

**ひ**

- 日立製ブレードサーバ
  - 管理対象にするための確認事項 90
- 日立製ラックマウントサーバ
  - 管理対象にするための確認事項 91

**ふ**

- ファイアウォール
  - 設定 [Windows ホスト] 92
  - 例外登録 [Linux 管理サーバ] 44, 85
  - 例外登録 [Windows 管理サーバ] 85
  - 例外登録が必要なポート [Linux 管理サーバ] 86
- ブートの設定変更
  - 管理対象リソース 158
- プラグインライセンス
  - 登録 57
- フラットモデル 129
- プロパティ
  - Compute Systems Manager サーバ 258
  - Hitachi Command Suite 共通コンポーネント 260
  - IP アドレス変更時に編集 [Hitachi Command Suite 共通コンポーネント] 78
  - ポート変更時に編集 [Compute Systems Manager サーバ] 75
  - ポート変更時に編集 [Hitachi Command Suite 共通コンポーネント] 72
  - ホスト名変更時に編集 [Hitachi Command Suite 共通コンポーネント] 76
- プロパティと設定ファイル
  - ポート変更時に編集 [デプロイメントマネージャー] 159
- プロパティの一覧
  - Compute Systems Manager サーバ 258
  - Hitachi Command Suite 共通コンポーネント 261
- プロパティの設定例
  - Kerberos サーバ 280

**へ**

- 変更
  - IP アドレス 79
  - JDK 82
  - URL 81
  - タイムアウト時間 83
  - ポート 76
  - ホスト名 79
- 変更するタイミング
  - URL 80
- 編集
  - ポート変更時 [デプロイメントマネージャー] 159

**ほ**

- ポート
  - Compute Systems Manager サーバ 248
  - Hitachi Command Suite 共通コンポーネント 248
  - デプロイメントマネージャー 249
  - 変更 76
- ポートの詳細 250
- ポート番号
  - 確認 43
  - 例外登録 [Linux 管理サーバ] 86
- ポート番号変更
  - デプロイメントマネージャー 158
- ポート変更時に編集
  - プロパティ [Compute Systems Manager サーバ] 75
  - プロパティ [Hitachi Command Suite 共通コンポーネント] 72
- 保守情報
  - 採取 [Linux 管理サーバの Java VM スレッドダンプ] 232
  - 採取 [Linux ホスト] 234
  - 採取 [Windows 管理サーバの Java VM スレッドダンプ] 231
  - 採取 [Windows ホスト] 233
  - 採取 [管理サーバ] 229
- 保守情報の採取 228
- ホスト名
  - 変更 79
- ホスト名変更時に編集
  - プロパティ [Hitachi Command Suite 共通コンポーネント] 76
- ポリシー設定 68

**ま**

- マネジメントモジュール

IP アドレス変更 101  
マルチドメイン構成 [外部認証サーバ] 126

## め

メールアドレス設定  
System アカウント 58  
メッセージ部  
監査ログ 241

## ゆ

有効  
BMC 監視 90  
DCOM [Windows ホスト] 92  
WinRM [Windows ホスト] 93  
WoL 90  
有効期限確認  
サーバ証明書 118  
ユーザーアカウント作成  
サーバ管理者 60  
ユーザーグループ  
設定 60

## ら

ラウンチ 71

## り

リクエスト受理時  
出力情報 243  
出力情報 [詳細メッセージ] 243  
リストア  
確認事項 [データベース] 169  
データベース 169  
データベース [Red Hat Enterprise Linux のクラスタ環境] 211  
データベース [Windows のクラスタ環境] 211  
リソースグループ  
設定 60  
リモート接続  
設定 [Windows ホスト] 93  
利用許可  
sudo [Linux ホスト] 99  
su [Linux ホスト] 98

## れ

レスポンス送信時  
出力情報 243

## ろ

ログインの許可  
root [Linux ホスト] 97  
管理対象ホスト 96  
ログの設定 245  
ロック解除  
アカウント 69  
ロック対象  
System アカウント 68

