HITACHI
Inspire the Next

# Hitachi Automation Director

## インストールガイド

4010-1J-011-20

**対象製品**
Hitachi Automation Director 8.6.5

**輸出管理に関する注意**
本マニュアル固有の技術データおよび技術は、米国輸出管理法、および関連の規制を含む米国の輸出管理法の対象となる場合があり、その他の国の輸出または輸入規制の対象となる場合もあります。読者は、かかるすべての規制を厳守することに同意し、マニュアルおよび該当製品の輸出、再輸出、または輸入許可を取得する責任があることを了解するものとします。

**商標類**
HITACHI 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。
Brocade は，米国またはその他の国における Brocade Communications Systems, Inc. の商標または登録商標です。
IBM，AIX は，世界の多くの国で登録された International Business Machines Corporation の商標です。
IBM，PowerPC は，世界の多くの国で登録された International Business Machines Corporation の商標です。
Citrix は，Citrix Systems, Inc.の米国あるいはその他の国における登録商標または商標です。
Citrix XenDesktop は，Citrix Systems, Inc.の米国あるいは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 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 Exchange 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。
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 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。
Microsoft および 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。
OpenStack®の文字表記と OpenStack のロゴは，米国とその他の国における OpenStack Foundation の登録商標/サービスマークまたは商標/サービスマークのいずれかであり，OpenStack Foundation の許諾を得て使用しています。日立製作所は，OpenStack Foundation や OpenStack コミュニティの関連企業ではなく、また支援や出資を受けていません。
Oracle と Java は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です。
Red Hat は，米国およびその他の国で Red Hat, Inc. の登録商標もしくは商標です。
RSA 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。
すべての SPARC 商標は, 米国 SPARC International, Inc. のライセンスを受けて使用している同社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。SPARC 商標がついた製品は，米国 Sun Microsystems, Inc. が開発したアーキテクチャに基づくものです。
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。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Hitachi Device Manager および Hitachi Tiered Storage Manager には，Oracle Corporation またはその子会社，関連会社が著作権 を有している部分が含まれています。
Hitachi Device Manager および Hitachi Tiered Storage Manager には，UNIX System Laboratories, Inc.が著作権を有している部 分が含まれています。
Hitachi Device Manager および Hitachi Tiered Storage Manager は，米国 EMC コーポレーションの RSA BSAFE ® ソフトウェア を搭載しています。

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。
This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.
Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.
This product includes software developed by the University of California, Berkeley and its contributors.
This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).
Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).
This product includes software developed by IAIK of Graz University of Technology.
This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).
This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).
This product includes software developed by Andy Clark.

本製品は，米国 EMC コーポレーションの RSA BSAFE®ソフトウェアを搭載しています。
Java is a registered trademark of Oracle and/or its affiliates.

**発行**
2019 年 9 月 4010-1J-011-20

# 目次

# はじめに

このマニュアルでは、Hitachi Automation Director（HAD）のインストールと構成の方法を説明します。

- 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
- 関連マニュアル
- このマニュアルで使用している記号
- KB（キロバイト）などの単位表記について

# 対象読者

このマニュアルは、ストレージ環境内のストレージ、サービス、およびアプリケーションを担当するストレージ管理者を対象としています。

# マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

**第 1 章　概要**

Automation Director の概要について説明しています。

**第 2 章　Hitachi Automation Director をインストールする**

クラスタと非クラスタ両方の環境における Microsoft® Windows®、または非クラスタ環境における Red Hat Enterprise Linux（RHEL）での、Hitachi Automation Director のインストール方法について説明しています。

**第 3 章　Automation Director を構成する**

Automation Director を構成する方法について説明しています。

**第 4 章　Hitachi Automation Director を削除する**

Hitachi Automation Director を削除する方法について説明しています。

**付録 A　Hitachi Automation Director のファイルの場所とポート**

Hitachi Automation Director のインストール時に作成されるファイルの場所およびポートについて説明しています。

**付録 B　hcmds64keytool ユーティリティを使用して証明書を管理する**

hcmds64keytool ユーティリティの使用方法について説明しています。

# マイクロソフト製品の表記について

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

| 表記 | 製品名 |
|---|---|
| Internet Explorer | 次の製品を区別する必要がない場合の表記です。<br>・Microsoft ® Internet Explorer ®<br>・Windows ® Internet Explorer ® |
| Windows | 次の製品を区別する必要がない場合の表記です。<br>・Microsoft ® Windows Server ® 2008 R2<br>・Microsoft ® Windows Server ® 2012<br>・Microsoft ® Windows Server ® 2012 R2<br>・Microsoft ® Windows Server ® 2016<br>・Microsoft ® Windows Server ® 2019 |
| Windows Server 2008 | 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。 |

| 表記 | 製品名 |
|---|---|
| | ・Microsoft ® Windows Server ® 2012<br>・Microsoft ® Windows Server ® 2012 R2 |
| Windows Server 2016 | Microsoft ® Windows Server ® 2016 |
| Windows Server 2019 | Microsoft ® Windows Server ® 2019 |

## 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 Automation Director ユーザーズガイド*, 4010-1J-010
- *Hitachi Automation Director Service Builder ユーザーズガイド*, 4010-1J-013
- *Hitachi Automation Director メッセージ*, 4010-1J-014
- Hitachi Command Suite ドキュメント
- Hitachi Tuning Manager ドキュメント

## 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、次のような表記規則を使用しています。

| 規則 | 説明 |
|---|---|
| **太字** | リスト項目の中で強調する語を示します。 |
| [] | ウィンドウのタイトル、メニュー、メニューオプション、ボタン、フィールド、ラベルなど、ウィンドウ内のテキストを示します。<br>例：[OK] をクリックします。 |
| *斜体* | ・ マニュアルのタイトルまたはテキスト内で強調する語を示します。<br>・ 変数を示します。これは、ユーザーが入力する実際のテキストのプレースホルダ、またはシステムから出力されるプレースホルダです。例：<br>`pairdisplay -g group`<br>（この変数の規則の例外については、山括弧の説明を参照してください。） |
| Monospace | 画面に表示されるテキスト、またはユーザーが入力するテキストを示します。例：<br>`pairdisplay -g oradb` |
| < >（山括弧） | 次のような場合に、変数を示します。<br>・ 変数は、周囲のテキストや他の変数から明確には区切られません。例：<br>`Status-<report-name><file-version>.csv`<br>・ 見出しに変数が含まれる場合。 |
| [ ]（角括弧） | オプションの値を示します。例：[ a \| b ]は、a または b を選択できる、あるいはどちらも省略できることを示します。 |
| { }（波括弧） | 必須の値または予期される値を示します。例：{ a \| b }は、a または b のどちらかを選択する必要があることを示します。 |
| \|（縦線） | 2 つ以上のオプションまたは引数から選択できることを示します。例：<br>[ a \| b ]は、a または b を選択できる、あるいはどちらも省略できることを示します。<br>{ a \| b }は、a または b のいずれかを選択する必要があることを示します。 |

# KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）は、それぞれ1KiB（キビバイト）、1MiB（メビバイト）、1GiB（ギビバイト）、1TiB（テビバイト）と読み替えてください。

1KiB、1MiB、1GiB、1TiB は、それぞれ 1,024 バイト、1,024KiB、1,024MiB、1,024GiB です。

# 1

# 概要

この章では、以下について説明します。

- 1.1 製品の概要
- 1.2 関連する Hitachi Command Suite 製品について
- 1.3 Hitachi Automation Director システム構成
- 1.4 Hitachi Automation Director のインストールと構成のワークフロー

## 1.1 製品の概要

Hitachi Automation Director は、ストレージおよびデータセンター管理者向けの、エンドツーエンドのストレージプロビジョニングプロセスを自動化および単純化するためのツールとなるソフトウェアソリューションです。この製品の基本要素は、サービステンプレートと呼ばれる、事前にパッケージ化されたオートメーションテンプレートです。これらの事前構成テンプレートは特定の環境とプロセスに合わせてカスタマイズされ、リソースプロビジョニングなどの複雑なタスクを自動化するサービスを作成します。構成が済むと、Automation Director は既存のアプリケーションと連携して、既存のインフラストラクチャサービスを利用することによって、共通のインフラストラクチャ管理タスクを自動化します。

Automation Director は、次のような機能を備えています。

- オートメーションサービスの作成を容易にする、事前構成されたサービステンプレート
- さまざまなストレージクラスのボリュームのインテリジェントなプロビジョニングのためのオートメーションサービス
- 定義されたサービスへのロールベースのアクセス
- インフラストラクチャーグループから最も性能の高いプールを選択し、プール情報を各タスクに提供してボリューム使用量の詳細を指定する、性能ベースのプール選択
- すべてのオートメーションサービスに割り当てて共有できる共通のサービス管理属性

## 1.2 関連する Hitachi Command Suite 製品について

Hitachi Automation Director は、以下のコンポーネントを含む Hitachi Command Suite の一部です。

- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Dynamic Link Manager
- Hitachi Replication Manager
- Hitachi Tuning Manager
- Hitachi Global Link Manager
- Hitachi Compute Systems Manager

Automation Director を他の Hitachi Command Suite 製品と同じサーバにインストールすると、共通の設定でユーザーとセキュリティを管理できます。また、Automation Director を Device Manager が稼働しているサーバにインストールすると、2 つの製品によって管理されるホスト情報が自動的に同期されるため、ホスト管理の作業効率が向上します。

**メモ**　Automation Director と Device Manager の両方を使用した場合に同期されるのはホスト情報のみで、他の種類のリソースの情報は同期されません。

## 1.3 Hitachi Automation Director システム構成

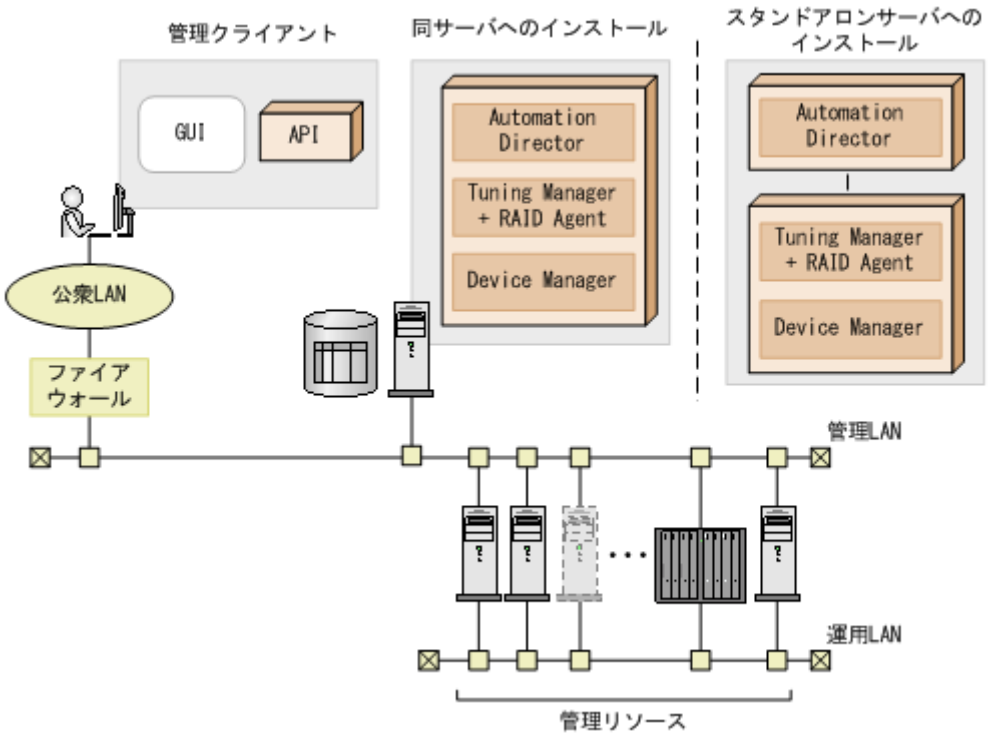
Automation Director 環境をセットアップするときのシステム構成について説明します。

### Hitachi Device Manager を前提製品とする場合

Device Manager を前提製品とする場合の基本的なシステム構成は，次のいずれかがあります。

- Automation Director と Device Manager を同じサーバにインストールします。
- Automation Director はスタンドアロンサーバへインストールし，その他の Hitachi Command Suite 製品は別のサーバへインストールします。

Device Manager を前提製品とする場合の基本的なシステム構成を次の図に示します。




メモ

**hcmds64prmset** コマンドを使用して、同一サーバ構成をスタンドアロンセットアップに変更することもできます。

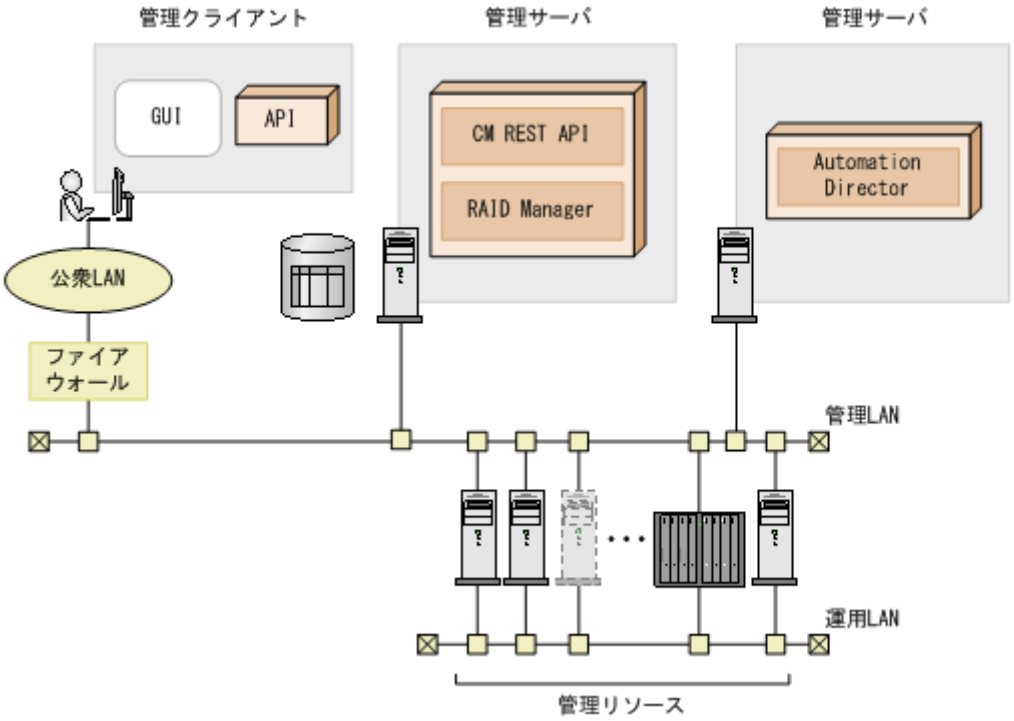
メモ

Automation Director がサポートできる Device Manager サーバの最大数は 50 です。追加情報については、Automation Director のリリースノートを参照してください。

### Configuration Manager REST API を前提製品とする場合

Configuration Manager REST API を前提製品とする場合は，Automation Director を管理サーバにインストールし，Configuration Manager REST API を別の管理サーバへインストールします。

Configuration Manager REST API を前提製品とする場合の基本的なシステム構成を次の図に示します。




## 1.4 Hitachi Automation Director のインストールと構成のワークフロー

次の図は、Automation Director のインストールと構成を含む、ワークフローの概要を示しています。


このマニュアルには、システムのインストール、セットアップ、管理、および保守に関する情報が含まれています。管理 GUI を使用したサービスの作成、管理、および自動化の詳細については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。

# 2

# Hitachi Automation Director をインストールする

この章では、クラスタと非クラスタ両方の環境における Microsoft® Windows®、および非クラスタ環境における Red Hat Enterprise Linux（RHEL）での、Hitachi Automation Director のインストール方法について説明します。

## 2.1 インストールの前提条件

Automation Director をインストールする前に、以下のタスクを完了してください。

- 環境と管理サーバがすべてのハードウェアおよびソフトウェア要件を満たしていることを確認します。システム要件の詳細については、Automation Director のリリースノートを参照してください。
- Automation Director によって使用されるポートが使用可能であることを確認します。管理サーバのポートが他の製品によって使用されておらず、競合していないことを確認します。ポートが別の製品によって使用されていた場合、どちらの製品も正しく動作しないことがあります。
- 関連マシンの名前を解決します。
- このマニュアルに含まれているインストールおよび構成タスクを完了するために、Windows 管理者権限が取得されていることを確認します。
- サーバ上のセキュリティ監視、ウイルス検出、プロセス監視ソフトウェアを無効にします。
- Windows のサービスまたは開いているコマンドプロンプトを閉じます。
- サーバが他の Hitachi Command Suite 製品を実行している場合は、それらの製品のサービスを停止します。
- サーバのシステム時刻が正しいことを確認します。Hitachi Command Suite が別のサーバにインストールされている場合は、Automation Director サーバの時刻を Hitachi Command Suite サーバに同期します。
- Red Hat Enterprise Linux の場合、必要に応じて Automation Director のファイアウォール例外を、手動で再追加します。これらの例外は、インストール時に自動的に再構成されません。

**関連参照**

- 2.1.2 名前解決設定を変更する
- 2.1.1 サーバ時刻を変更する
- 付録 A.2 ポート設定

### 2.1.1 サーバ時刻を変更する

Automation Director サーバの OS の時刻設定が Hitachi Command Suite 管理サーバと同期していることが重要です。

Automation Director のタスクおよびアラート発生時刻は、管理サーバの時刻設定に基づきます。したがって、サーバの OS の時刻設定が正確かどうかを確認することが重要です。必要に応じて、Automation Director をインストールする前にリセットしてください。Hitachi Command Suite 共通コンポーネントおよび Hitachi Command Suite 製品サービスが実行しているときに Automation Director サーバの時刻を変更した場合、Automation Director が正しく動作しないことがあります。

NTP など、サーバの時刻を自動的に調整するサービスを使用する場合は、次のようにサービスを構成する必要があります。

- サービスにより時刻の不一致が検出されたときに調整されるよう、設定を構成します。
- 特定の時刻差を超えない範囲内で時刻設定の調整が行われるようにします。最大範囲値に基づいて、時刻差が固定範囲を超えないように頻度を設定してください。

特定の時刻差の範囲内で時刻を調整できるサービスの例としては、Windows Time サービスがあります。

**メモ**　米国またはカナダのタイムゾーンで Automation Director を実行するときには、新しい夏時間（DST）ルールをサポートするように管理サーバの OS を構成する必要があります。サーバがサポートを提供しないかぎり、Automation Director は新しい DST ルールをサポートできません。

サーバの時刻を自動的に調整する機能を使用できない場合や、システム時刻を手動で変更する場合は、以下のステップを実行します。

1. Hitachi Command Suite 共通コンポーネントと、以下を含むすべての Hitachi Command Suite 製品のサービスを停止します。
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Common Service
   - HCS Device Manager Web Service
   - HiCommand Suite Tuning Manager
   - HiCommand Performance Reporter
   - HCS Tuning Manager REST Application Service
   - HAutomation Engine Web Service
   - HiCommand Server
   - HiCommand Tiered Storage Manager
2. 管理サーバの現在時刻を記録してから、時刻をリセットします。
3. サービスを再起動する時間を決めます。

- マシンの時刻を戻した場合（サーバの時刻が進んでいた場合）は、サーバのクロックが記録した時刻（変更を加えたときのサーバの時刻）を示すまで待ってから、マシンを再起動します。
- マシンの時刻を進めた場合は、すぐにマシンを再起動します。

Automation Director 管理サーバが正しい時刻を反映していることを確認します。

## 2.1.2 名前解決設定を変更する

Automation Director と Hitachi Command Suite を 2 台の異なるマシンにインストールした場合は、クライアントに接続する Automation Director サーバの名前を解決する必要があります。

Automation Director がインストールされているマシンの名前も解決する必要があります。

Automation Director を Hitachi Command Suite と同じマシンにインストールした場合は、Automation Director にアクセスするためにブラウザを実行するマシンの名前を解決する必要があります。

`user_httpsd.conf` ファイルの最初の行で `ServerName` プロパティとして設定されている管理サーバのホスト名からシステムが IP アドレスを解決できるように、構成設定を更新します。次のコマンドを実行して、IP アドレスがホスト名に解決されることを確認します。

```
ping management-server-host-name
```

### 2.1.3 ポートの衝突を回避する

Automation Director を新しくインストールする前に、管理サーバ上で Automation Director が使用するポートが他の製品によって使用されていないことを確認してください。ポートが別の製品によって使用されていた場合、どちらの製品も正しく動作しないことがあります。

必要なポートが使用中でないことを確認するには、**netstat** コマンドを使用します。

ポート番号 22170～22173 が他の製品によって使用されていないことを確認する必要があります。使用されている場合、新規インストールまたはアップグレードインストールが失敗するためです。

**関連タスク**

- 3.1.1 管理サーバと管理クライアントとの通信に使用されるポート番号を変更する

**関連参照**

- 付録 A.2 ポート設定

## 2.2 Automation Director をインストールする（Windows）

このマニュアルでは、単体インストールメディアから製品インストーラを使用して Automation Director をインストールする方法を説明します。

ソフトウェアをアップグレードする場合は、**backupsystem** コマンドを使用して、既存のシステム構成とデータを必ずバックアップしてください。このコマンドの実行方法については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。

**メモ**　Automation Director を他の Hitachi Command Suite 製品とともにインストールする場合は、システムがすべての製品のインストール要件を満たしていることを確認してください。

**操作手順**

1. システムがインストール前のチェックリストに記載されているすべての管理サーバ前提条件を満たしていることを確認します。
2. サーバが Hitachi Command Suite 共通コンポーネントを使用する製品を実行している場合は、以下のサービスを停止します。
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Common Service
   - HCS Device Manager Web Service
   - HiCommand Suite Tuning Manager
   - HiCommand Performance Reporter
   - HCS Tuning Manager REST Application Service
   - HAutomation Engine Web Service
   - HiCommand Server
   - HiCommand Tiered Storage Manager
3. インストールメディアを DVD ドライブに挿入します。

4. インストールウィザードを起動します。
   ＜*Automation Director のインストールメディア*＞¥HAD_SERVER¥setup.exe を実行します。
5. 画面の指示に従って、必要な情報を指定します。
   ほとんどの場合、デフォルトのインストール選択項目を受け入れてください。
   ［インストール完了］ウィンドウが開きます。
6. ［完了］をクリックします。

**メモ**
SSL 通信が有効な環境、または Hitachi Command Suite 共通コンポーネントのポート番号が変更された環境に Automation Director をインストールする場合、［インストール完了］ウィンドウで［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グラフィカルユーザーインタフェースが起動しないことがあります。
この問題が発生した場合は、変更された管理サーバ情報をチェックしてから、Web ブラウザのアドレスバーに Automation Director の URL を入力して、インタフェースを起動します。

**操作結果**

これで、Automation Director がインストールされます。

**関連参照**

- 2.5 インストール後のタスク

# 2.3 クラスタ環境で Automation Director をインストールする（Windows）

Windows クラスタ環境に Automation Director をインストールします。

**メモ**　Automation Director は、Windows クラスタ環境だけをサポートします。Automation Director は、Linux 環境でのクラスタリングをサポートしていません。

## 2.3.1 クラスタ環境での Automation Director の使用について

Automation Director を使用するときには、Microsoft Windows Server Failover Clustering を使用してフェイルオーバー管理サーバをセットアップすることで信頼性を高めることができます。

**メモ**

クラスタ環境で Automation Director を使用するときには、次のように、1 台の Automation Director サーバをアクティブノードに、もう 1 台をスタンバイノードに指定します。

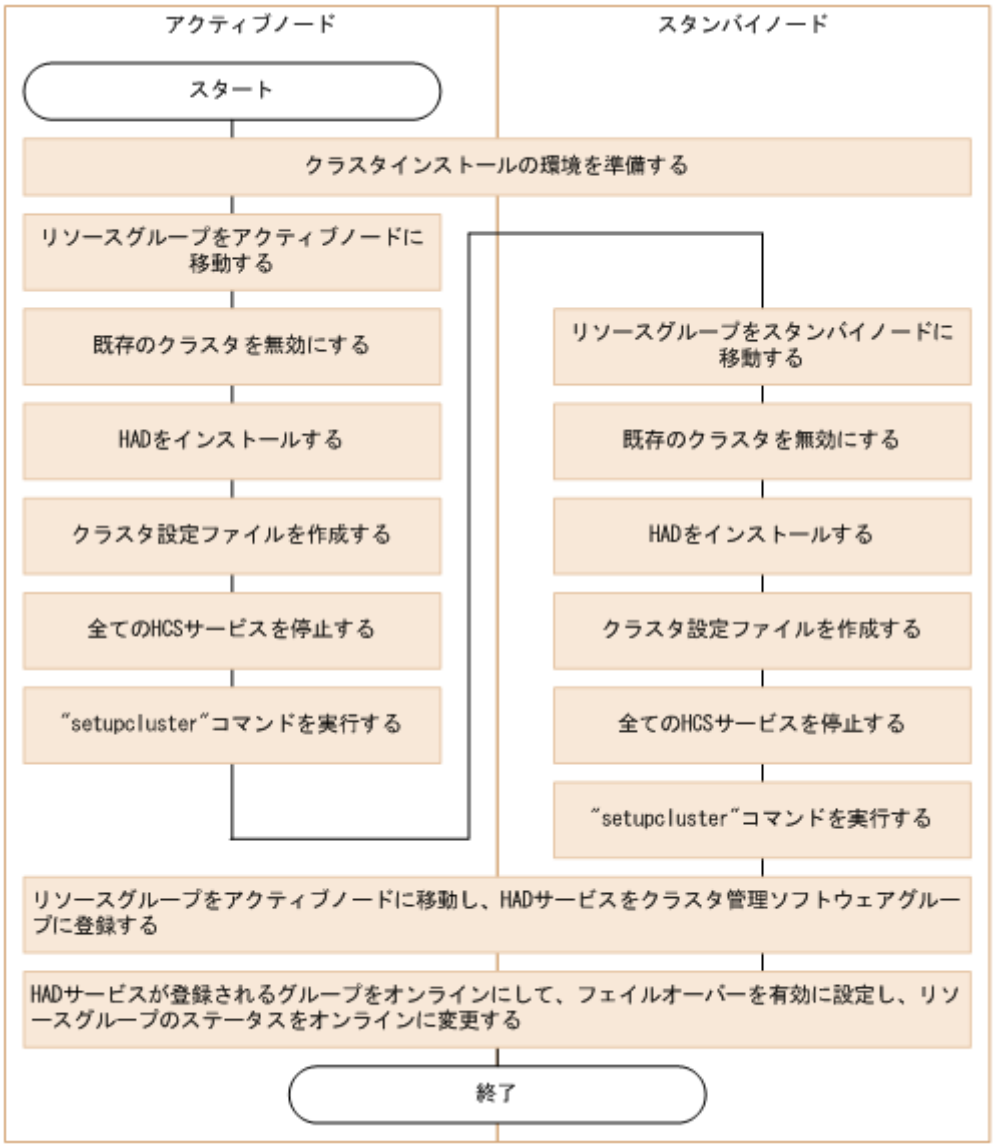
- アクティブノード
  アクティブノードは、クラスタを使用するシステムでサービスを実行しているホストです。
  障害が発生した場合、クラスタサービスがフェイルオーバーを実行し、スタンバイノードがシステムリソースの操作を引き継ぐため、サービスは中断されません。
- スタンバイノード
  スタンバイノードは、障害発生時にアクティブノードからシステムリソースの操作を引き継ぐホストです。

メモ　アクティブノードがスタンバイノードにフェイルオーバーした場合、実行中のタスクは失敗するので、スタンバイノード上でタスクを再び実行する必要があります。

## 2.3.2 クラスタインストールワークフロー

Automation Director をクラスタ構成でインストールするときには、一連のステップに従って、アクティブノードとスタンバイノードの両方を準備する必要があります。

以下に、クラスタ環境をセットアップするための一般的なワークフローを示します。




初めて Automation Director をクラスタ環境にインストールするとき、または非クラスタ環境からクラスタ環境に移行するときには、クラスタ内のすべてのノードが同じディスク構成を持つことと、すべての Hitachi Command Suite 製品が各ノードの同じ場所（ドライブ名、パスなどを含む）にインストールされていることを確認してください。

ソフトウェアをアップグレードする場合は、**backupsystem** コマンドを使用して、既存のシステム構成とデータを必ずバックアップしてください。このコマンドの実行方法については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。

メモ　既にクラスタ構成でインストールされている Automation Director のアップグレードを行うときには、アップグレードインストールを実行する前に、リソーススクリプトを無効にする必要があります。

**関連タスク**

- 2.3.4 アクティブノードで Automation Director クラスタ化をセットアップする
- 2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする

## 2.3.3 クラスタ管理ソフトウェアを使用してクラスタ構成をチェックする

クラスタ環境で Automation Director をセットアップするときには、クラスタ管理ソフトウェアを使用して現在の環境設定を確認し、追加の設定を構成する必要があります。

クラスタ環境で Automation Director をセットアップする前に、クラスタ環境ソフトウェアを使用して、以下の項目をチェックします。

- 他の Hitachi Command Suite 製品のサービスが登録されているグループが存在するかどうかをチェックします。
  Hitachi Command Suite のサービスが登録されているグループが既に存在する場合は、そのグループを使用します。グループが、Hitachi Command Suite 製品に関するリソースのみで構成されていることを確認します。
  Hitachi Command Suite のサービスが登録されているグループが存在しない場合は、クラスタ管理ソフトウェアを使用して、Automation Director のサービスを登録するグループを作成します。

  メモ　グループ名に次の文字を使用することはできません：!" % & ) * ^ | ; = , < >

- サービスを登録するグループに、アクティブノードとスタンバイノード間で継承できる共有ディスクとクライアントアクセスポイントが含まれていることを確認します。クライアントアクセスポイントは、クラスタ管理 IP アドレスと論理ホスト名です。
- クラスタ管理ソフトウェアを使用してリソースの割り当て、削除、および監視が問題なくできることを確認します。

クラスタ環境で使用されるサービスは、クラスタ管理ソフトウェアでグループとして登録することによってフェイルオーバーできます。これらのグループは、クラスタ管理ソフトウェアと OS のバージョンによって、「リソースグループ」や「ロール」など異なる名前で呼ばれることがあります。

## 2.3.4 アクティブノードで Automation Director クラスタ化をセットアップする

クラスタ構成のアクティブノード上の管理サーバで、Automation Director の新規インストールを完了することができます。

**操作手順**

1. 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。クラスタインストールのリソースグループがアクティブノードに移動されることを確認します。
2. 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、次のコマンドを使用して、Hitachi Command Suite 製品のサービスが登録されるクラスタグループをオフラインにして、フェイルオーバーを無効にします。

- バージョン 8.1.2 以降の Hitachi Command Suite 製品がインストールされていない場合：
  ＜*Automation Director のインストールメディア*＞¥HCS¥ClusterSetup
  ¥hcmds64clustersrvstate /soff /r ＜*グループ名*＞
- バージョン 8.1.2 以降の Hitachi Command Suite 製品がインストールされている場合：
  ＜*共通コンポーネントのインストールフォルダ*＞¥ClusterSetup
  ¥hcmds64clustersrvstate /soff /r ＜*グループ名*＞
  r オプションには、Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が HCS cluster の場合は、"HCS cluster"と指定します。

3. アクティブノード上の Automation Director の新規インストールを完了します。
   別の Hitachi Command Suite 製品がクラスタ環境に既に存在する場合は、Automation Director をインストールする前に、以下のことを確認してください。管理サーバの IP アドレスとして、論理ホストの IP アドレスを指定します。
   他の Hitachi Command Suite 製品がクラスタ環境に存在しない場合は、Automation Director をインストールする前に、以下のことを確認してください。管理サーバの IP アドレスとして、アクティブノードの IP アドレスを指定します。

   **メモ**　クラスタ構成で既にセットアップされた環境で Automation Director をアップグレードする場合は、アップグレードインストールを実行する前に、リソースグループに登録されるスクリプトのフェイルオーバーを防止する必要があります。クラスタ管理ソフトウェアで、リソースグループに登録されるスクリプトを右クリックして、［プロパティ］－［ポリシー］タブから、再起動しないようにリソースを設定します。

4. 使用する製品のライセンスを登録します。アクティブノードの IP アドレスにアクセスします。
5. クラスタ内で Hitachi Command Suite 製品を既に構成している場合、次のステップへスキップします。Automation Director がクラスタ内の最初の Hitachi Command Suite 製品である場合は、以下を実行します。
   a. 空白のテキストファイルに以下の情報を追加します。

```
mode=online
virtualhost=＜論理ホスト名＞
onlinehost=＜アクティブノードのホスト名＞
standbyhost=＜スタンバイノードのホスト名＞
```

   **メモ**　アクティブノードで、mode として online を指定する必要があります。

   ファイルを cluster.conf という名前で＜*共通コンポーネントのインストールフォルダ*＞¥conf に保存します。
6. 次のコマンドを使用して、Hitachi Command Suite 製品を確実に停止します。
   ＜*共通コンポーネントのインストールフォルダ*＞¥bin¥hcmds64srv /stop/server AutomationWebService
7. **setupcluster /exportpath** コマンドを実行します。exportpath には、絶対または相対ディレクトリパスを指定します。

**関連タスク**

- 2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする

## 2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする

アクティブノードでクラスタ化インストールを設定した後、クラスタ構成のスタンバイノード上の管理サーバで Automation Director のインストールを完了できます。

**操作手順**

1. クラスタ管理ソフトウェアで、Automation Director のリソースを含んでいるグループをスタンバイノードに移動します。グループを右クリックして［Move］を選択してから、［Select Node］または［Move this service or application to another node］を選択します。
2. 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、次のコマンドを使用して、Hitachi Command Suite 製品のサービスが登録されるクラスタグループをオフラインにして、フェイルオーバーを無効にします。
   - バージョン 8.1.2 以降の Hitachi Command Suite 製品がインストールされていない場合：
     *＜Automation Director のインストールメディア＞*¥HCS¥ClusterSetup
     ¥hcmds64clustersrvstate /soff /r *＜グループ名＞*
   - バージョン 8.1.2 以降の Hitachi Command Suite 製品がインストールされている場合：
     *＜共通コンポーネントのインストールフォルダ＞*¥ClusterSetup
     ¥hcmds64clustersrvstate /soff /r *＜グループ名＞*
     r オプションには、Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が HCS cluster の場合は、"HCS cluster"と指定します。
3. スタンバイノード上の Automation Director の新規インストールを完了します。
   スタンバイノードに Automation Director をインストールする前に、以下の要件に注意してください。
   - アクティブノードと同じ場所に Automation Director をインストールする必要があります。
   - 他の Hitachi Command Suite 製品が既に存在し、クラスタ環境でアクティブな場合、管理サーバの IP アドレスとして論理ホスト名（クラスタ管理 IP アドレスに割り当てられる仮想ホスト名）を指定します。クラスタ環境に他の Hitachi Command Suite 製品がない場合、スタンバイノードの IP アドレスまたはホスト名を指定します。

   **メモ**　クラスタ構成で既にセットアップされた環境で Automation Director をアップグレードする場合は、アップグレードインストールを実行する前に、リソースグループに登録されるスクリプトのフェイルオーバーを防止する必要があります。クラスタ管理ソフトウェアで、リソースグループに登録されるスクリプトを右クリックして、［プロパティ］ー［ポリシー］タブから、再起動しないようにリソースを設定します。

4. 使用する製品のライセンスを登録します。
5. クラスタ内で Hitachi Command Suite 製品を既に構成している場合、次のステップへスキップします。もし Automation Director がクラスタ内の最初の Hitachi Command Suite 製品である場合は、空白のテキストファイルに以下の情報を追加します。

```
mode=standby
virtualhost=＜論理ホスト名＞
onlinehost=＜アクティブノードのホスト名＞
standbyhost=＜スタンバイノードのホスト名＞
```

ファイルを cluster.conf という名前で<*共通コンポーネントのインストールフォルダ*>¥conf に保存します。

---

**メモ**　スタンバイノードで、mode として standby を指定する必要があります。

---

6. 次のコマンドを使用して、Hitachi Command Suite 製品を確実に停止します。
   hcmds64srv /stop /server AutomationWebService
7. **setupcluster /exportpath** コマンドを実行します。exportpath には、絶対または相対ディレクトリパスを指定します。

## 2.3.6 サービスを登録しクラスタインストールの初期設定を行う

Automation Director をクラスタ構成のアクティブノードおよびスタンバイノードにインストールした後、以下のステップの説明に従ってサービスとスクリプトを登録し、クラスタ化をオンラインにできます。

**操作手順**

1. クラスタ管理ソフトウェアで、Automation Director のリソースを含んでいるグループをアクティブノードに移動します。グループを右クリックして［Move］を選択してから、［Select Node］または［Move this service or application to another node］を選択します。
2. 次のコマンドを使用して、クラスタ管理ソフトウェアグループで Automation Director サービスを登録します。
   <*共通コンポーネントのインストールフォルダ*>¥ClusterSetup
   ¥hcmds64clustersrvupdate /sreg /r <*グループ名*> /sd <*共有ディスクのドライブレター名*> /ap <*クライアントアクセスポイント用リソース名*>

   - /r
     Automation Director を含む Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。
   - /sd
     クラスタ管理ソフトウェアに登録される共有ディスクのドライブ名を指定します。このオプションに対して複数のドライブ名を指定することはできません。Hitachi Command Suite 製品のデータベースが複数の共有ディスクに分割されている場合は、各共有ディスクについて hcmds64clustersrvupdate コマンドを実行します。
   - /ap
     クラスタ管理ソフトウェアに登録されるクライアントアクセスポイント用リソースの名前を指定します。
3. アクティブノードで、次のコマンドを使用して Automation Director を含む Hitachi Command Suite サービスが登録されるグループをオンラインにして、フェイルオーバーを有効にします。
   <*共通コンポーネントのインストールフォルダ*>¥ClusterSetup
   ¥hcmds64clustersrvstate /son /r <*グループ名*>
   r オプションには、Automation Director を含む Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。
4. クラスタソフトウェアで、リソースグループのステータスを［online］に変更します。

## 2.4 Hitachi Automation Director をインストールする（Linux）

このマニュアルでは、単体インストールメディアから製品インストーラを使用して Automation Director をインストールする方法を説明します。

ソフトウェアをアップグレードする場合は、**backupsystem** コマンドを使用して、既存のシステム構成とデータを必ずバックアップしてください。このコマンドの実行方法については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。

**メモ**　Automation Director を他の Hitachi Command Suite 製品とともにインストールする場合は、システムがすべての製品のインストール要件を満たしていることを確認してください。

**操作手順**

1. `install.sh` を実行して、Automation Director をインストールします。
   Linux での Automation Director のインストール先ディレクトリは、デフォルトでは`/opt/HiCommand/Automation` です。

**関連参照**

- 2.5 インストール後のタスク

## 2.5 インストール後のタスク

Automation Director のインストール後は、以下のインストール後のタスクを完了してください。

1. ユーザーアカウントを管理するサーバが SSL 通信を使用する場合、**hcmds64prmset** コマンドを実行して、サーバのポート番号を設定します（必要に応じて）。
2. 登録済み URL を確認します（推奨）。
3. Automation Director 管理サーバへのアクセスを確認します。
4. ライセンスを登録します。
5. System アカウントのパスワードを変更します（推奨）。
6. System アカウントのメールアドレスを設定します。
7. RMI 通信を有効にします。

   **メモ**　このステップは、Device Manager v8.1.4 を使用する場合のみ必要です。

8. Hitachi Command Suite および Automation Director サービスを停止し、再開します（必要に応じて）。

### 2.5.1 登録済み URL を確認する（Windows）

Automation Director のインストール後に、登録済み URL を確認します。

**操作手順**

1. 次のコマンドを使用して、登録済み URL を確認します。

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

2. URL 内のホスト名をチェックします。非クラスタ環境では、ホスト名は物理ホスト名でなければなりません。クラスタ環境では、ホスト名は論理ホスト名でなければなりません。登録済み URL が正しくなかった場合には、次のコマンドを使用して URL を変更します。

   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64chgurl /change http://*<変更前の IP アドレスまたはホスト名>*:*<ポート番号>* http://*<変更後の IP アドレスまたはホスト名>*:*<ポート番号>*

## 2.5.2 登録済み URL を確認する（Linux）

Automation Director のインストール後に、登録済み URL を確認します。

**操作手順**

1. 次のコマンドを使用して、登録済み URL を確認します。

   *<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

2. URL 内のホスト名をチェックします。非クラスタ環境では、ホスト名は物理ホスト名でなければなりません。クラスタ環境では、ホスト名は論理ホスト名でなければなりません。登録済み URL が正しくなかった場合には、次のコマンドを使用して URL を変更します。

   *<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://*<変更前の IP アドレスまたはホスト名>*:*<ポート番号>* http://*<変更後の IP アドレスまたはホスト名>*:*<ポート番号>*

## 2.5.3 インストールを確認する

インストールが完了したら、インストールが成功したことを Web ブラウザから確認してください。

**操作手順**

1. Automation Director によってサポートされている Web ブラウザを開きます。
2. アドレスバーに、Automation Director の URL を次の形式で指定します。

   http://*<Automation Director 管理サーバの IP アドレスまたはホスト名>*:22015/Automation/

**操作結果**

管理サーバにアクセスできることを確認するログインウィンドウが開きます。

## 2.5.4 ライセンスを登録する

最初にログオンするときには、有効なライセンスキーを指定する必要があります。

**メモ**　Automation Director のライセンスについては、サポートサービスにお問い合わせください。

**操作手順**

1. ログオンウィンドウの［ライセンス］をクリックします。
2. ライセンスキーを入力するか、ライセンスファイルの場所を参照して、［保存］をクリックします。

## 2.5.5 System アカウントのパスワードを変更する

System アカウントは、すべての Hitachi Command Suite 製品のユーザー管理および実行権限を持つデフォルトのアカウントです。Automation Director を初めてインストールするときには、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。

**操作手順**

1. 管理クライアントから、次の認証情報を使用してログオンします。
   ユーザー ID：system
   パスワード（デフォルト）：manager
2. ［管理］タブで、［プロファイル］をクリックします。
3. ［パスワード変更］をクリックし、必要なパスワードを入力して［OK］をクリックします。

## 2.5.6 System アカウントのメールアドレスを設定する

Automation Director のシステム操作に関するメール通知を Automation Director からシステムへ送信できるようにするには、System アカウントのメールアカウントを設定する必要があります。

**操作手順**

1. ［管理］タブで［プロファイル］をクリックします。
2. ［プロファイル］画面で［プロファイル編集］をクリックし、フルネームとメールアドレスを入力して、［OK］をクリックします。

**操作結果**

System アカウントのメールアドレスが設定されます。

メール通知を受信するには、システム設定を実施してメールの SMTP サーバ接続情報を設定し（IP アドレスまたはホスト名、ユーザー ID、パスワードおよびポートはすべて必須です）、システム・パラメータ設定でメール通知を有効にする必要があります。詳細については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。

## 2.5.7 Hitachi Command Suite および Automation Director のサービスを停止および開始する

Hitachi Command Suite および Automation Director はコマンドプロンプトからサービスを実行します。Hitachi Command Suite は、［スタート］メニューからでも停止および開始できます。

**メモ**　Automation Director サービスは、［スタート］メニューからは開始できません。

### (1) 「スタート」メニューからすべてのサービスを停止および開始する

次の手順により、すべての Hitachi Command Suite サービスを停止および開始します。

**操作手順**

1. ［スタート］ －［すべてのプログラム］ －［Hitachi Command Suite］ －［Manage Services］を選択します。
2. ［Start - HCS］または［Stop - HCS］をクリックします。

### (2)　コマンドプロンプトからすべてのサービスを停止および開始する（Windows）

次の手順により、すべての Hitachi Command Suite および Automation Director のサービスを停止および開始します。

**操作手順**

1. コマンドプロンプトで、`C:¥Program Files¥HiCommand¥Base64¥bin` に移動します。
2. サービスを停止するには、次のコマンドを入力します。

hcmds64srv.exe /stop
サービスを開始するには、次のコマンドを入力します。
hcmds64srv.exe /start

### (3) コマンドプロンプトからすべてのサービスを停止および開始する（Linux）

次の手順により、すべての Hitachi Command Suite および Automation Director のサービスを停止および開始します。

**操作手順**

1. コマンドプロンプトで、/opt/HiCommand/Base64/bin に移動します。
2. サービスを停止するには、次のコマンドを入力します。
   hcmds64srv -stop
   サービスを開始するには、次のコマンドを入力します。
   hcmds64srv -start

### (4) コマンドプロンプトから Automation Director サービスのみ停止および開始する（Windows）

**操作手順**

1. C:¥Program Files¥HiCommand¥Base64¥bin に移動します。
2. サービスを停止または開始します。
   - サービスを停止するには、次のコマンドを入力します。
     hcmds64srv.exe /stop /server AutomationWebService
   - サービスを開始するには、次のコマンドを入力します。
     hcmds64srv.exe /start /server AutomationWebService

### (5) コマンドプロンプトから Automation Director サービスのみ停止および開始する（Linux）

**操作手順**

1. /opt/HiCommand/Base64/bin に移動します。
2. サービスを停止または開始します。
   - サービスを停止するには、次のコマンドを入力します。
     hcmds64srv -stop -server AutomationWebService
   - サービスを開始するには、次のコマンドを入力します。
     hcmds64srv -start -server AutomationWebService

## 2.5.8 RMI 通信を有効にする（Windows）

Automation Director サービスを使用する前に、Replication Manager の RMI 通信を構成する必要があります。このステップは、Replication Manager を使用するかどうかにかかわらず必要です。Replication Manager の RMI 通信を有効にしなかった場合、Device Manager 接続は正しく機能せず、［管理］タブにリストされる接続ステータスはエラーを示します。

**前提条件**

Administrator 権限を持つユーザーとして、Device Manager サーバにログオンします。

**操作手順**

1. Hitachi Command Suite 製品のサービスを停止します。
2. Replication Manager の base.properties ファイルの base.rmi.enabled プロパティとして、true を指定します。base.properties ファイルは、次の場所に格納されています。

   ＜*Hitachi Command Suite のインストールフォルダ*＞¥ReplicationManager¥conf

   Replication Manager の base.properties ファイルと base.rmi.enabled プロパティの詳細については、『*Hitachi Command Suite Replication Manager システム構成ガイド*』を参照してください。
3. Device Manager サーバの rpmlib.properties ファイルの rpmlib.rpm.port プロパティを設定します。

   Replication Manager の base.properties ファイルの base.rmi.port プロパティに対して設定されているポート番号を入力します。base.rmi.port プロパティの値（デフォルト：25200）を変更していない場合は、この操作は不要です。

   base.properties ファイルは、次の場所に格納されています。

   ＜*Hitachi Command Suite のインストールフォルダ*＞¥ReplicationManager¥conf
4. Hitachi Command Suite 製品のサービスを開始します。

## 2.5.9 RMI 通信を有効にする（Linux）

Automation Director サービスを使用する前に、Replication Manager の RMI 通信を構成する必要があります。このステップは、Replication Manager を使用するかどうかにかかわらず必要です。Replication Manager の RMI 通信を有効にしなかった場合、Device Manager 接続は正しく機能せず、［管理］タブの接続ステータスにエラーが表示されます。

**前提条件**

root ユーザーとして、Device Manager サーバにログオンします。

**操作手順**

1. Hitachi Command Suite 製品のサービスを停止します。
2. Replication Manager の base.properties ファイルの base.rmi.enabled プロパティとして、true を指定します。base.properties ファイルは、次の場所に格納されています。

   ＜*Hitachi Command Suite のインストールディレクトリ*＞/ReplicationManager/conf

   Replication Manager の base.properties ファイルと base.rmi.enabled プロパティの詳細については、『*Hitachi Command Suite Replication Manager システム構成ガイド*』を参照してください。
3. Device Manager サーバの rpmlib.properties ファイルの rpmlib.rpm.port プロパティを設定します。

   Replication Manager の base.properties ファイルの base.rmi.port プロパティに対して設定されているポート番号を入力します。base.rmi.port プロパティの値（デフォルト：25200）を変更していない場合は、この操作は不要です。

   base.properties ファイルは、次の場所に格納されています。

   ＜*Hitachi Command Suite のインストールディレクトリ*＞/ReplicationManager/conf

   Replication Manager の base.properties ファイルと base.rmi.port プロパティの詳細については、『*Hitachi Command Suite Replication Manager システム構成ガイド*』を参照してください。
4. Hitachi Command Suite 製品のサービスを開始します。

# 3

# Automation Director を構成する

この章では、Automation Director を構成する方法について説明します。

# 3.1 管理サーバのシステム設定を変更する

ここでは、Automation Director 管理サーバのシステム設定の変更に関して説明します。

## 3.1.1 管理サーバと管理クライアントとの通信に使用されるポート番号を変更する

Automation Director 管理サーバと管理クライアント（Web ブラウザ）間の通信に使用されるポート番号を変更するには、定義ファイルの編集と、ファイアウォールの例外登録が必要になります。クラスタシステムの場合、実行系サーバと待機系サーバで同じ手順を実施してください。

**メモ**　Automation Director に使用される他のポートの情報については、ポート設定の参考トピックを参照してください。

Automation Director 管理サーバと管理クライアント間のポート番号を変更するには：

**操作手順**

1. Automation Director を停止します。
2. 定義ファイルのキーを編集してポート番号の設定を変更します。
   - HTTPS の場合、手順 3 に進みます。
   - HTTP の場合、次のように定義ファイルのキーを編集してポート番号の設定を変更します。

   a. `user_httpsd.conf` ファイルの `Listen` キーの行を変更します。

   Windows の場合：
   *<共通コンポーネントのインストールフォルダ>*¥uCPSB¥httpsd¥conf¥user_httpsd.conf
   Linux の場合：
   /opt/HiCommand/Base64/uCPSB/httpsd/conf/user_httpsd.conf
   次の行で、22015 に替わる新しいポート番号を指定します。

   ```
   Listen 22015

   Listen [::]:22015

   #Listen 127.0.0.1:22015
   ```

   b. `command_user.properties` ファイルの `command.http.port` の行を変更します。
   クラスタシステムの場合、この定義ファイルは別のフォルダに含まれています。
   Windows（非クラスタ環境）の場合：
   *<Automation Director のインストールフォルダ>*¥conf
   Windows（クラスタ環境）の場合：
   *<共有フォルダ名>*¥Automation¥conf
   Linux の場合：
   /opt/HiCommand/Automation/conf

   c. `config_user.properties` ファイルの `server.http.port` の行を変更します。
   クラスタシステムの場合、この定義ファイルは別のフォルダに含まれています。
   Windows（非クラスタ環境）の場合：
   *<Automation Director のインストールフォルダ>*¥conf
   Windows（クラスタ環境）の場合：
   *<共有フォルダ名>*¥Automation¥conf
   Linux の場合：
   /opt/HiCommand/Automation/conf

   d. 手順 4 に進みます。

3. HTTPS の場合、次のように定義ファイルのキーを編集してポート番号の設定を変更します。

   a. user_httpsd.conf ファイルを開きます。

      Windows の場合：
      *<共通コンポーネントのインストールフォルダ>*¥uCPSB¥httpsd¥conf¥user_httpsd.conf
      Linux の場合：
      /opt/HiCommand/Base64/uCPSB/httpsd/conf/user_httpsd.conf

   b. 次の行で 22016 に替わる新しいポート番号を指定して、Listen キーの行を変更します。

      ```
      Listen 22016
      ```

      ```
      Listen [::]:22016
      ```

      ```
      VirtualHost *22016
      ```

4. ファイアウォールの例外登録をします。
   - OS が Windows の場合は、**hcmds64fwcancel** コマンドを実行してファイアウォールの例外登録をします。
   - OS が Linux の場合は、OS の仕様に従って例外登録をします。手順については、OS のマニュアルを参照してください。
5. Automation Director を開始します。
6. **hcmds64chgurl** コマンドを実行して、Automation Director にアクセスするための URL を更新します。

**関連概念**

- 2.5.7 Hitachi Command Suite および Automation Director のサービスを停止および開始する

**関連参照**

- 3.1.2 ポート番号を変更した場合の Hitachi Command Suite のプロパティ更新
- 付録 A.2 ポート設定

## 3.1.2 ポート番号を変更した場合の Hitachi Command Suite のプロパティ更新

Automation Director のポート番号を変更する場合は、次の表に示されている Hitachi Command Suite 共通プロパティを更新する必要があります。

| ポート番号（デフォルト） | プロパティファイルのパス（HCS 共通コンポーネントインストール先ディレクトリ） | 更新場所 |
|---|---|---|
| 22015/TCP | ¥uCPSB¥httpsd¥conf¥user_httpsd.conf | Listen |
| | | Listen [::]: |
| | | #Listen 127.0.0.1: |
| 22016/TCP | ¥uCPSB¥httpsd¥conf¥user_httpsd.conf | VirtualHost タグの *host-name*:*port-number* |
| | | Listen |
| | | Listen [::]: |
| 22031/TCP | ¥uCPSB¥httpsd¥conf¥user_hsso_httpsd.conf | Listen |
| 22032/TCP | ¥HDB¥CONF¥emb¥HiRDB.ini | PDNAMEPORT |
| | ¥HDB¥CONF¥pdsys | pd_name_port |

| ポート番号（デフォルト） | プロパティファイルのパス（HCS 共通コンポーネントインストール先ディレクトリ） | 更新場所 |
|---|---|---|
| | ¥database¥work¥def_pdsys | pd_name_port |
| 22035/TCP | ¥uCPSB¥CC¥web¥redirector¥workers.properties | worker.HBase64StgMgmtSSOService.port |
| | ¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties | webserver.connector.ajp13.port |
| 22036/TCP | ¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties | ejbserver.rmi.naming.port |
| 22037/TCP | ¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties | ejbserver.http.port |
| 22038/TCP | ¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties | ejbserver.rmi.remote.listener.port |
| 22170/TCP | ¥uCPSB¥CC¥server¥userconf¥ejb¥AutomationWebService¥usrconf.properties | webserver.connector.ajp13.port |
| 22170/TCP | ¥uCPSB¥CC¥web¥redirector¥workers.properties | worker.Automation.port |
| 22171/TCP | ¥uCPSB¥CC¥server¥userconf¥ejb¥AutomationWebService¥usrconf.properties | ejbserver.rmi.naming.port |
| 22172/TCP | ¥uCPSB¥CC¥server¥userconf¥ejb¥AutomationWebService¥usrconf.properties | ejbserver.http.port |
| 22173/TCP | ¥uCPSB¥CC¥server¥userconf¥ejb¥AutomationWebService¥usrconf.properties | ejbserver.rmi.remote.listener.port |

## 3.1.3 ユーザーアカウントを管理するサーバの情報を変更する

必要に応じて、ユーザーアカウントを管理するサーバの情報を変更できます。

**メモ**　ユーザーアカウントは、接続先の Device Manager がインストールされているホスト上の共通コンポーネントによって管理されます。

**操作手順**

1. Device Manager の HBase 64 Storage Mgmt Web Service に対して SSL が設定されていない場合は、このコマンドを実行します。

   Windows：
   *＜共通コンポーネントのインストールフォルダ＞*¥bin¥hcmds64prmset /host *＜Device Manager サーバの IP アドレスまたはホスト名＞* /port *＜Device Manager の HBase 64 Storage Mgmt Web Service のポート番号（非 SSL）＞*
   Linux:

*<共通コンポーネントのインストールディレクトリ>*/bin/hcmds64prmset -host *<Device Manager サーバの IP アドレスまたはホスト名>* -port *<Device Manager の HBase 64 Storage Mgmt Web Service のポート番号（非 SSL）>*

2. Device Manager の HBase 64 Storage Mgmt Web Service に対して SSL が設定されている場合は、このコマンドを実行します。

   Windows：
   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64prmset /host *<Device Manager の IP アドレスまたはホスト名>* /sslport *<Device Manager の HBase 64 Storage Mgmt Web Service のポート番号（SSL）>*
   Linux:
   *<共通コンポーネントのインストールディレクトリ>*/bin/hcmds64prmset -host *<Device Manager の IP アドレスまたはホスト名>* -sslport *<Device Manager の HBase 64 Storage Mgmt Web Service のポート番号（SSL）>*

## 3.1.4 管理サーバのホスト名または IP アドレスを変更する

管理サーバのホスト名は、Automation Director のインストール後に変更できます。

管理サーバのホスト名は最大 128 文字で、大文字と小文字が区別されます。

### 操作手順

1. 新しい管理サーバのホスト名と IP アドレスをメモしておいてください。

   Windows マシンでホスト名を確認する必要がある場合は、ipconfig /ALL コマンドを使用してホスト名を表示します。
2. hcmds64srv /stop コマンドを実行して、すべての Hitachi Command Suite サービスを停止します。
3. Hitachi Command Suite の共通コンポーネントのプロパティを編集します。
4. 他の Hitachi Command Suite 製品を実行している場合は、必要に応じてそれらの設定を変更します。
5. 管理サーバのホスト名または IP アドレスを変更します。変更後、サーバを再起動します。
6. 元のホスト名または IP アドレスを使用してブラウザから管理サーバにアクセスする場合は、Hitachi Command Suite の URL を更新します。

### 関連概念

- 2.5.7 Hitachi Command Suite および Automation Director のサービスを停止および開始する

## 3.1.5 管理サーバの URL を変更する

管理サーバのホスト名または IP アドレス、Automation Director のポート、または SSL 設定を変更した場合は、Automation Director 管理サーバの URL を変更する必要があります。Automation Director が他の Hitachi Command Suite 製品と同じ管理サーバで実行している場合は、Hitachi Command Suite のすべての URL を 1 つのコマンドで変更できます。

**メモ**　プロトコルとポート番号を含んだ完全な URL を使用する必要があります（たとえば、http://HostA:22015）。

### 操作手順

1. 次のコマンドを使用して、現在の URL を確認します。

   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64chgurl /list
2. Automation Director がスタンドアロンのサーバにインストールされている場合は、次のコマンドで Automation Director の URL だけを変更します。

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

3. Automation Director が同じサーバにインストールされている場合は、次のコマンドを使用して、この管理サーバ上で実行している Hitachi Command Suite のすべての URL を変更します。
   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64chgurl /change *<変更前のURL>* *<変更後のURL>*
4. 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］ －［Automation Director］を選択して、［HAD Login］を右クリックします。［プロパティ］を選択して、［Web ドキュメント］タブで URL を変更します。
   - Windows Server 2012 および Windows Server 2012 R2 の場合：
     ［スタート］ －［すべてのアプリ］ －［Hitachi Command Suite］ －［Automation Director］を選択して、［HAD Login］を右クリックします。［プロパティ］を選択して、［Web ドキュメント］タブで URL を変更します。

   URL には次の形式を使用します。
   *<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>*/Automation/login.htm

   - *<プロトコル>*は、非 SSL 通信の場合は http、SSL 通信の場合は https です。
   - *<管理サーバのIPアドレスまたはホスト名>*は、Automation Director がインストールされている管理サーバの IP アドレスまたはホスト名です。
   - *<ポート番号>*は、user_httpsd.conf ファイルの Listen 行で設定されたポート番号です。
     SSL 以外の通信の場合は、SSL 以外の通信用のポート番号を指定します（デフォルト：22015）。
     SSL 通信の場合は、SSL 通信用のポート番号を指定します（デフォルト：22016）。
     user_httpsd.conf ファイルは、*<共通コンポーネントのインストールフォルダ>*¥uCPSB¥httpsd¥conf にあります。
5. 新しい URL を使用して Automation Director にアクセスできることを確認します。

# 3.2 セキュア通信を構成する

ここでは、Automation Director のセキュア通信を構成する方法について説明します。

## 3.2.1 Automation Director のセキュリティ設定について

Automation Director に対してセキュア通信を使用することによって、セキュリティを高めることができます。セキュア通信では、Automation Director は Automation Director ネットワーク通信に Secure Sockets Layer（SSL）または Transport Layer Security（TLS）を使用することによって、セキュリティを高めることができます。SSL または TLS により、Automation Director での通信パートナー確認、パートナー識別のための認証強化、送受信される情報内の改ざんデータ検出を実現します。また、通信チャンネルが暗号化されるため、データが盗聴から保護されます。

Automation Director は、以下のタイプの通信について、SSL または TLS を使用したセキュア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
- 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

- 管理サーバと管理対象間の通信

また、特定の管理クライアントだけが管理サーバにアクセスできるように、アクセスを制限できます。

**メモ** セキュリティを有効にして Automation Director を使用するときには、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ている場合は、有効な証明書を Automation Director に登録しないとサーバに接続できません。

## 3.2.2 管理クライアントのセキュリティを構成する

ここでは、管理サーバと管理クライアント間のセキュア通信の設定について説明します。

### (1) 管理クライアントのセキュア通信について

SSL を使用して Automation Director 管理サーバと管理クライアント間のセキュア通信を実現します。SSL を実装するには、まず管理サーバに SSL をセットアップし、次に管理クライアントに SSL をセットアップします。Web ベースのクライアントに SSL をセットアップするプロセスは、CLI クライアントの場合とは異なります。

### (2) VMware vCenter を使用する場合にサーバ上で SSL をセットアップする

「Allocate Volumes and Create Datastore on VMware vSphere」または「Allocate Like Volumes and Create Datastore on VMware vSphere」サービステンプレートを使用しようとする場合で、VMware vCenter Server のバージョンが v5.5u3 未満の場合は、Hitachi Command Suite 共通コンポーネントの設定を次のように更新することで、SSL 経由で TLSv1.0 を検証する必要があります。

**操作手順**

1. 編集のため、次のファイルを開きます。
   Windows の場合：
   *<共通コンポーネントのインストールフォルダ>*¥conf¥init.conf
   Linux の場合：
   *<共通コンポーネントのインストールディレクトリ>*/conf/init.conf
2. SSL プロパティを更新します。
   a. ssl.protocol プロパティに移動して TLSv1 を追加します。
   b. ssl.ClientCipherSuites プロパティに移動して TLS_RSA_WITH_AES_256_CBC_SHA および TLS_RSA_WITH_AES_128_CBC_SHA を追加します。
   c. ファイルを保存して閉じます。
3. Hitachi Command Suite を再起動します。

### (3) セキュアなクライアント通信のためにサーバ上で SSL をセットアップする（Windows）

管理サーバと管理クライアント間のセキュア通信を実装するには、管理サーバで SSL をセットアップする必要があります。

詳細については、『*Hitachi Command Suite システム構成ガイド*』の「SSL サーバの構築（Hitachi Command Suite 共通コンポーネ ント）」を参照してください。

hcmds64ssltool コマンドは、2 種類の秘密鍵、RSA 暗号と ECC（楕円曲線暗号）に対応する証明書署名要求および自己署名証明書を作成します。証明書署名要求は、PEM 形式で作成されます。

このコマンドは自己署名証明書の作成にも使用できますが、自己署名証明書は、テスト目的にだけ使用することをお勧めします。

**前提条件**

Administrator 権限を持つユーザーとしてログインします。

次の情報を収集します。

- 認証局が指定する証明書署名要求の要件
- 管理クライアントで実行している Web ブラウザのバージョン
  Web ブラウザは、X.509 PEM 形式を使用しており、管理クライアント（GUI）で使用されているサーバ証明書の署名アルゴリズムをサポートしている必要があります。
- 既存の秘密鍵、証明書署名要求、および自己署名証明書の保存先フォルダ（再作成する場合）
  出力先パスに同じ名前のファイルが既に存在する場合、ファイルを上書きしません。したがって、秘密鍵、証明書署名要求、および自己署名証明書を再作成する場合、既存の保存先フォルダ以外のフォルダに出力するか、既存のファイルを削除する必要があります。

**操作手順**

1. Hitachi Command Suite 共通コンポーネントの秘密鍵（`httpsdkey.pem`）、証明書署名要求（`httpsd.csr`）、および自己署名証明書（`httpsd.pem`）を作成するには、次のコマンドを使用します。
   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64ssltool [/key *<秘密鍵ファイル>*] [/csr *<証明書発行要求ファイル>*] [/cert *<自己署名証明書ファイル>*] [/certtext *<自己署名証明書の内容ファイル>*] [/validity *<有効日数>*] [/sigalg *<RSA 暗号用のサーバ証明書の署名アルゴリズム>*] [/eccsigalg *<ECC 用のサーバ証明書の署名アルゴリズム>*] [/ecckeysize *<ECC 用の秘密鍵のキーサイズ>*]

   - /key
     作成された秘密鍵ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsdkey.pem、ECC の場合は ecc-httpsdkey.pem というファイル名で、デフォルトの出力先パス※に出力されます。
   - /csr
     作成された証明書発行要求ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.csr、ECC の場合は ecc-httpsd.csr というファイル名で、デフォルトの出力先パス※に出力されます。
   - /cert
     作成された自己署名証明書の出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.pem、ECC の場合は ecc-httpsd.pem というファイル名で、デフォルトの出力先パス※に出力されます。
   - /certtext
     作成された自己署名証明書の内容ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.txt、ECC の場合は ecc-httpsd.txt というファイル名で、デフォルトの出力先パス※に出力されます。
   - /validity
     日数で自己署名証明書の有効期限を指定します。このオプションを省略すると、デフォルトの 3,650 日が使用されます。
   - /sigalg

RSA 暗号用のサーバ証明書の署名アルゴリズムを SHA256withRSA または SHA1withRSA で指定します。このオプションを省略すると、デフォルトの SHA256withRSA が使用されます。

- /eccsigalg
  ECC 用のサーバ証明書の署名アルゴリズムを SHA512withECDSA、SHA384withECDSA、SHA256withECDSA、または SHA1withECDSA で指定します。このオプションを省略すると、デフォルトの SHA384withECDSA が使用されます。
- /ecckeysize
  ECC 用のサーバ証明書の秘密鍵のサイズを 256 または 384 ビットで指定します。このオプションを省略すると、デフォルトの 384 が使用されます。

このコマンドは、RSA ファイルおよび ECC ファイルを指定した出力先パスに出力します。
RSA ファイルは、指定したファイル名で、ECC ファイルは、指定したファイル名の先頭に「ecc-」が付いて出力されます。
注※　key、csr、cert、または certtext オプションを省略した場合のデフォルトの出力先は、次のとおりです。
*<共通コンポーネントのインストールフォルダ>*¥uCPSB¥httpsd¥conf¥ssl¥server

2. プロンプトが表示されたら、コロン（:）の後に以下の情報を入力します。
   - サーバ名（管理サーバのホスト名） - 例：Automation_Director_SC1
   - 組織単位（セクション） - 例：Automation Director
   - 組織名（会社） - 例：Hitachi
   - 都市または地区名 - 例：Santa Clara
   - 州または県名（フルネーム） - 例：California
   - 国名（2 文字のコード） - 例：US

   フィールドを空白のままにしておくには、ピリオド（.）を入力します。角括弧（[]）内に表示されるデフォルト値を選択するには、［Enter］を押します。
3. 証明書署名要求（httpsd.csr）を認証局に送信して、サーバ証明書を申請します。

**メモ**　自己署名証明書を使用する場合、このステップは不要ですが、本番環境では署名付きサーバ証明書を使用することを推奨します。

認証局によって発行されたサーバ証明書は、通常、メールで送信されます。認証局によって送信されたメールとサーバ証明書を必ず保存してください。

4. Automation Director を停止します。
5. 秘密鍵（httpsdkey.pem）とサーバ証明書または自己署名証明書（httpsd.pem）を、次のディレクトリにコピーします。
   *<共通コンポーネントのインストールフォルダ>*¥uCPSB¥httpsd¥conf¥ssl¥server
6. 次の場所から user_httpsd.conf ファイルを開きます。
   *<共通コンポーネントのインストールフォルダ>*¥uCPSB¥httpsd¥conf
   ¥user_httpsd.conf
7. user_httpsd.conf ファイル内で、以下のようにします。
   a. ハッシュ[#]記号を削除することによって、以下の行を非コメント化します。
      ```
      #Listen 22016
      #<VirtualHost *:22016>
      ```
      から
      ```
      #</VirtualHost>
      ```

ただし、#SSLCACertificateFile はコメントアウトしたままにしておく必要があります。
以下に、user_httpsd.conf ファイルの編集例を示します。SSL ECC を使用している場合は、以下の行も非コメント化します。
#SSLECCCertificateKeyFile
#SSLECCCertificateFile

```
ServerName ＜管理サーバのホスト名＞
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName ＜管理サーバのホスト名＞
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-GCM-
SHA384:AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA
SSLRequireSSL
SSLCertificateKeyFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
httpsd.pem"
#SSLECCCertificateKeyFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
ecc-httpsdkey.pem"
#SSLECCCertificateFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
ecc-httpsd.pem"
# SSLCACertificateFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/cacert/
anycert.pem"
</VirtualHost>
#HWSLogSSLVerbose On
```

b. 必要に応じて、以下の行を編集します。
最初の行の ServerName
<VirtualHost>タグの ServerName
SSLCertificateKeyFile
SSLCertificateFile
SSLECCCertificateKeyFile（ECC を使用する場合）
SSLECCCertificateFile（ECC を使用する場合）
#SSLCACertificateFile
認証局から発行されたチェーンサーバ証明書を使用するときには、"#
SSLCACertificateFile"行から番号記号（#）を削除し、（認証局によって作成された）チェーン証明書ファイルを絶対パスで指定します。

**メモ**
外部サーバから管理サーバへの非 SSL 通信をブロックするには、Listen 22015 行と Listen [::]:22015 行の先頭に番号記号（#）を追加してコメントアウトします。これらの行をコメントアウトした後、#Listen 127.0.0.1:22015 行の番号記号を削除します。
IPv6 環境の場合、#Listen [::]:22016 行の先頭の番号記号（#）を削除します。

以下に、user_httpsd.conf ファイルの編集例を示します。番号は、デフォルトのポート番号を示しています。

```
ServerName ＜管理サーバのホスト名＞
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName ＜管理サーバのホスト名＞
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-GCM-SHA384:AES256-
SHA256:AES256-SHA:AES128-SHA256:AES128-SHA
SSLRequireSSL
SSLCertificateKeyFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
server-certificate-or-self-signed-certificate-file"
#SSLECCCertificateKeyFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
ecc-httpsdkey.pem"
#SSLECCCertificateFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/server/
ecc-httpsd.pem"
SSLCACertificateFile
"＜共通コンポーネントのインストールフォルダ＞/uCPSB/httpsd/conf/ssl/cacert/
certificate-file-from-certificate-authority"
</VirtualHost>
#HWSLogSSLVerbose On
```

8. Automation Director を開始します。
9. 次のように hcmds64chgurl コマンドを使用して、Automation Director の URL を更新します。
   - プロトコルを http:から https:に変更します。
   - セキュア通信に使用されるポート番号を変更します。

**操作結果**

これで、Automation Director サーバ上で SSL が実装されます。

## (4) セキュアなクライアント通信のためにサーバ上で SSL をセットアップする（Linux）

管理サーバと管理クライアント間のセキュア通信を実装するには、管理サーバで SSL をセットアップする必要があります。

詳細については、『*Hitachi Command Suite システム構成ガイド*』の「SSL サーバの構築（Hitachi Command Suite 共通コンポーネ ント）」を参照してください。

hcmds64ssltool コマンドは、2 種類の秘密鍵、RSA 暗号と ECC（楕円曲線暗号）に対応する証明書署名要求および自己署名証明書を作成します。証明書署名要求は、PEM 形式で作成されます。このコマンドは自己署名証明書の作成にも使用できますが、自己署名証明書は、テスト目的にだけ使用することをお勧めします。

**前提条件**

root ユーザーとしてログインします。

次の情報を収集します。

- 認証局が指定する証明書署名要求の要件
- 管理クライアントで実行している Web ブラウザのバージョン
  Web ブラウザは、X.509 PEM 形式を使用しており、管理クライアント（GUI）で使用されているサーバ証明書の署名アルゴリズムをサポートしている必要があります。
- 既存の秘密鍵、証明書署名要求、および自己署名証明書の保存先ディレクトリ（再作成する場合）
  出力先パスに同じ名前のファイルが既に存在する場合、ファイルを上書きしません。したがって、秘密鍵、証明書署名要求、および自己署名証明書を再作成する場合、既存の保存先ディレクトリ以外のディレクトリに出力するか、既存のファイルを削除する必要があります。

**操作手順**

1. Hitachi Command Suite 共通コンポーネントの秘密鍵（`httpsdkey.pem`）、証明書署名要求（`httpsd.csr`）、および自己署名証明書（`httpsd.pem`）を作成するには、次のコマンドを使用します。
   *＜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 ＜`*有効日数*`＞] [-sigalg ＜`*RSA 暗号用のサーバ証明書の署名アルゴリズム*`＞] [-eccsigalg ＜`*ECC 用のサーバ証明書の署名アルゴリズム*`＞] [-ecckeysize ＜`*ECC 用の秘密鍵のキーサイズ*`＞]`

   - `-key`
     作成された秘密鍵ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsdkey.pem、ECC の場合は ecc-httpsdkey.pem というファイル名で、デフォルトの出力先パス※に出力されます。
   - `-csr`
     作成された証明書発行要求ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.csr、ECC の場合は ecc-httpsd.csr というファイル名で、デフォルトの出力先パス※に出力されます。
   - `-cert`
     作成された自己署名証明書の出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.pem、ECC の場合は ecc-httpsd.pem というファイル名で、デフォルトの出力先パス※に出力されます。
   - `-certtext`
     作成された自己署名証明書の内容ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.txt、ECC の場合は ecc-httpsd.txt というファイル名で、デフォルトの出力先パス※に出力されます。
   - `-validity`
     日数で自己署名証明書の有効期限を指定します。このオプションを省略すると、デフォルトの 3,650 日が使用されます。
   - `-sigalg`
     RSA 暗号用のサーバ証明書の署名アルゴリズムを SHA256withRSA または SHA1withRSA で指定します。このオプションを省略すると、デフォルトの SHA256withRSA が使用されます。

- -eccsigalg
  ECC 用のサーバ証明書の署名アルゴリズムを SHA512withECDSA、SHA384withECDSA、SHA256withECDSA、または SHA1withECDSA で指定します。このオプションを省略すると、デフォルトの SHA384withECDSA が使用されます。
- -ecckeysize
  ECC 用のサーバ証明書の秘密鍵のサイズを 256 または 384 ビットで指定します。このオプションを省略すると、デフォルトの 384 が使用されます。

このコマンドは、RSA ファイルおよび ECC ファイルを指定した出力先パスに出力します。
RSA ファイルは、指定したファイル名で、ECC ファイルは、指定したファイル名の先頭に「ecc-」が付いて出力されます。
注※　key、csr、cert、または certtext オプションを省略した場合のデフォルトの出力先は、次のとおりです。
*<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. プロンプトが表示されたら、コロン（:）の後に以下の情報を入力します。
   - サーバ名（管理サーバのホスト名）- 例：Automation_Director_SC1
   - 組織単位（セクション）- 例：Automation Director
   - 組織名（会社）- 例：Hitachi
   - 都市または地区名 - 例：Santa Clara
   - 州または県名（フルネーム）- 例：California
   - 国名（2 文字のコード）- 例：US

   フィールドを空白のままにしておくには、ピリオド（.）を入力します。角括弧（[]）内に表示されるデフォルト値を選択するには、［Enter］を押します。
3. 証明書署名要求（httpsd.csr）を認証局に送信して、サーバ証明書を申請します。

メモ　自己署名証明書を使用する場合、このステップは不要ですが、本番環境では署名付きサーバ証明書を使用することを推奨します。

認証局によって発行されたサーバ証明書は、通常、メールで送信されます。認証局によって送信されたメールとサーバ証明書を必ず保存してください。

4. Automation Director を停止します。
5. 秘密鍵（httpsdkey.pem）とサーバ証明書または自己署名証明書（httpsd.pem）を、次のディレクトリにコピーします。
   *<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
6. 次の場所から user_httpsd.conf ファイルを開きます。
   *<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
7. user_httpsd.conf ファイル内で、以下のようにします。
   a. ハッシュ[#]記号を削除することによって、以下の行を非コメント化します。
      #Listen 22016
      #<VirtualHost *:22016>
      から
      #</VirtualHost>
      ただし、#SSLCACertificateFile はコメントアウトしたままにしておく必要があります。
      以下に、user_httpsd.conf ファイルの編集例を示します。SSL ECC を使用している場合は、以下の行も非コメント化します。

#SSLECCCertificateKeyFile
#SSLECCCertificateFile

```
ServerName ＜管理サーバのホスト名＞
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName ＜管理サーバのホスト名＞
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-GCM-
SHA384:AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA
SSLRequireSSL
SSLCertificateKeyFile
"＜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/httpsdkey.pem"
SSLCertificateFile
"＜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/httpsd.pem"
#SSLECCCertificateKeyFile
"＜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/ecc-httpsdkey.pem"
#SSLECCCertificateFile
"＜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/ecc-httpsd.pem"
# SSLCACertificateFile
"＜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/anycert.pem"
</VirtualHost>
#HWSLogSSLVerbose On
```

b. 必要に応じて、以下の行を編集します。
最初の行の ServerName
<VirtualHost>タグの ServerName
SSLCertificateKeyFile
SSLCertificateFile
SSLECCCertificateKeyFile（ECC を使用する場合）
SSLECCCertificateFile（ECC を使用する場合）
#SSLCACertificateFile
認証局から発行されたチェーンサーバ証明書を使用するときには、"#
SSLCACertificateFile"行から番号記号（#）を削除し、（認証局によって作成された）チェーン証明書ファイルを絶対パスで指定します。

**メモ**
外部サーバから管理サーバへの非 SSL 通信をブロックするには、Listen 22015 行と Listen [::]:22015 行の先頭に番号記号（#）を追加してコメントアウトします。これらの行をコメントアウトした後、#Listen 127.0.0.1:22015 行の番号記号を削除します。
IPv6 環境の場合、#Listen [::]:22016 行の先頭の番号記号（#）を削除します。

以下に、user_httpsd.conf ファイルの編集例を示します。番号は、デフォルトのポート番号を示しています。

```
ServerName ＜管理サーバのホスト名＞
Listen 22015
```

```
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName ＜管理サーバのホスト名＞
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-GCM-SHA384:AES256-
SHA256:AES256-SHA:AES128-SHA256:AES128-SHA
SSLRequireSSL
SSLCertificateKeyFile
"＜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/httpsdkey.pem"
SSLCertificateFile
"＜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/server-certificate-or-self-signed-certificate-file"
#SSLECCCertificateKeyFile
"＜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/ecc-httpsdkey.pem"
#SSLECCCertificateFile
"＜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/ecc-httpsd.pem"
SSLCACertificateFile
"＜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/certificate-file-from-certificate-authority"
</VirtualHost>
#HWSLogSSLVerbose On
```

8. Automation Director を開始します。
9. 次のように hcmds64chgurl コマンドを使用して、Automation Director の URL を更新します。
   - プロトコルを http:から https:に変更します。
   - セキュア通信に使用されるポート番号を変更します。

**操作結果**

これで、Automation Director サーバ上で SSL が実装されます。

## (5) Web ベースの管理クライアントで SSL をセットアップする

管理サーバと管理クライアント間のセキュア通信を実装するには、Automation Director の Web ベースのユーザーインタフェースにアクセスするすべての Automation Director 管理クライアント上で SSL をセットアップする必要があります。まず、管理サーバに SSL をセットアップし、次に管理クライアントに SSL をセットアップします。このクライアントから管理サーバに最初にアクセスするときのみ、この手順に従う必要があります。

**前提条件**

使用される署名アルゴリズムが SHA256 と RSA の場合、使用される Web ブラウザは SHA256 と RSA 署名を持つサーバ証明書をサポートする必要があります。

**操作手順**

1. 管理 Web クライアントから、次の URL を使用して、SSL 接続で管理サーバにアクセスします。
   https://＜*Automation Director 管理サーバの IP アドレスまたはホスト名*＞:＜*ポート番号（SSL）*＞/Automation/
2. SSL 証明書をインストールします。

**操作結果**

SSL 証明書が管理クライアントに登録され、SSL を使用して管理サーバと通信できるようになります。

## 3.2.3 外部認証サーバのセキュア通信を設定する

Windows 環境で Automation Director 管理サーバと LDAP ディレクトリサーバ間のセキュア通信を実装するには、StartTLS プロトコルを使用します。StartTLS を実装するには、`exauth.properties` ファイルでプロパティを更新し、LDAP ディレクトリサーバ証明書を管理サーバにインポートする必要があります。

詳細については、『*Hitachi Command Suite システム構成ガイド*』の「Hitachi Command Suite 共通コンポーネントのトラストストアーへの証明書のインポート」を参照してください。

---

メモ　Linux 環境で IPV6 アドレスを指定する場合は、アドレスを角括弧[ ]で囲む必要があります。

---

### (1)　プライマリ Hitachi Command Suite サーバへの認証接続のポート番号を変更する（Windows）

外部認証サーバとのセキュア通信を設定後、認証接続のポート番号を変更する必要があります。

認証接続のポート番号を変更するには、次のように **hcmds64prmset** コマンドを実行します。

```
＜共通コンポーネントのインストールフォルダ＞¥bin¥hcmds64prmset /host ＜プライマリサーバのホスト名＞ /sslport ＜ポート番号（SSL）＞
```

方法：

- `host` オプションには、サーバ証明書の Common Name（CN）と同じ名前を指定します。
- `sslport` オプションには、共通コンポーネントの SSL ポート番号を指定します。デフォルトは 22016 です。

### (2)　プライマリ Hitachi Command Suite サーバへの認証接続のポート番号を変更する（Linux）

外部認証サーバとのセキュア通信を設定後、認証接続のポート番号を変更する必要があります。

認証接続のポート番号を変更するには、次のように **hcmds64prmset** コマンドを実行します。

```
＜共通コンポーネントのインストールディレクトリ＞/bin/hcmds64prmset -host ＜プライマリサーバのホスト名＞ -sslport ＜ポート番号（SSL）＞
```

方法：

- `host` オプションには、サーバ証明書の Common Name（CN）と同じ名前を指定します。
- `sslport` オプションには、共通コンポーネントの SSL ポート番号を指定します。デフォルトは 22016 です。

## 3.2.4 Web サービス接続の証明書をインポートする

Hitachi Command Suite 共通コンポーネントのトラストストアに Web サービス接続の証明書をインポートする必要があります。

次のような Web サービス接続にサーバ証明書を使用するときに、Hitachi Command Suite 共通コンポーネントのトラストストアに証明書をインポートする必要があります。

- Device Manager
  Device Manager を使用する場合、共通コンポーネントで使用されるポート（22016）の証明書をインポートします。
- Configuration Manager
- VMware vCenter
- BNA
- その他の Web サービス接続

次の証明書もインポートする必要があります。

- 認証局
- 中間認証局
- ルート認証局

場合によっては、認証局の証明書が既にインポートされている可能性があります。この場合、この手順は不要です。

Windows の場合、**hcmds64keytool** コマンドを使用します。Unix の場合、標準 **keytool** を使用します。Java で証明書をインポートするには、トラストストアのパスワードが 6 文字以上であることを確認してください。また、新しいエイリアス名が既存のエイリアス名と衝突しないことを確認してください。

Windows の場合：

```
＜共通コンポーネントのインストールフォルダ＞¥bin¥hcmds64keytool -import -alias ＜エイリアス名＞ -keystore ＜共通コンポーネントのインストールフォルダ＞¥uCPSB¥jdk¥jre¥lib¥security¥jssecacerts -storepass ＜トラストストアへのアクセスパスワード＞ -file ＜サーバ証明書のパス＞
```

**hcmds64srv** コマンドを実行して、サービスを再開します。

Unix の場合：

```
＜共通コンポーネントのインストールディレクトリ＞/uCPSB/jre/jdk/bin/keytool -import -alias ＜エイリアス名＞ -keystore ＜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 ＜トラストストアへのアクセスパスワード＞ -file ＜サーバ証明書のパス＞
```

**hcmds64srv** コマンドを実行して、サービスを再開します。

**追加のガイドライン**

- サードパーティ接続のセキュリティ設定の方法については、各製品のマニュアルを参照してください。たとえば、VMware vCenter の場合は、VMware のマニュアルを参照してください。
- サードパーティのサーバ証明書を取得するには、関連する製品のマニュアルでサーバ証明書へのアクセスについて参照してください。

## 3.2.5 ESX クラスタサービスの VMware サーバ証明書をインストールする（Windows）

セキュア通信を使用するすべての Web サービス接続と同様に、Automation Director が参照する Automation Director 共通コンポーネントのトラストストアに、VMware サーバ証明書をインポートする必要があります。ただし、ESX クラスタサービステンプレートを使用する場合、VMware は一部の機能に独自（自己署名）のルート証明書を使用するため、VMware ルート証明書もインストールする必要があります。

**メモ**　ESX クラスタサービステンプレートを使用しない場合は、この手順を完了する必要はありません。

Windows サーバに VMware サーバ証明書をインストールするには、次の手順に従う必要があります。

**操作手順**

1. VMware サーバ証明書を次のようにダウンロードします。
   a. Web ブラウザを使用して vCenter ユーザーインタフェースにアクセスします。
   b. 右側のパネルで、［信頼されたルート CA 証明書をダウンロード］を選択します。
   c. Automation Director 共通コンポーネントのトラストストアが存在するサーバ上でダウンロードする場所を選択し、ダウンロードを確認します。
2. 共通コンポーネントのトラストストアが存在するサーバで、zip ファイルをダウンロードした場所に移動し、そのファイルを解凍します。

   **メモ**　ダウンロードしたファイルの拡張子が.zip でない場合は、拡張子を.zip に変更します。

   両方の証明書ファイルが含まれる、.certs フォルダが解凍されます。
3. 証明書をインストールします。
   a. 拡張子.crt のファイルの上で右クリックし、［証明書のインストール］を選択します。
   証明書のインポート ウィザードが開きます。
   b. ［ローカル コンピューター］を選択し、［次へ］をクリックします。
   c. ［証明書をすべて次のストアに配置する］を選択します。
   d. ［参照］をクリックし、［信頼されたルート証明機関］を選択して、［完了］をクリックします。

   証明書がトラストストアにインストールされます。

   **メモ**　ESX クラスタサービステンプレートを使用する場合は、『*Hitachi Automation Director ユーザーズガイド*』に説明されているように、Python もインストールする必要があります。

## 3.2.6 ESX クラスタサービスの VMware サーバ証明書をインストールする（Linux）

セキュア通信を使用するすべての Web サービス接続と同様に、Automation Director が参照する Automation Director 共通コンポーネントのトラストストアに、VMware サーバ証明書をインポートする必要があります。ただし、ESX クラスタサービステンプレートを使用する場合、VMware は一部の機能に独自（自己署名）のルート証明書を使用するため、VMware ルート証明書もインストールする必要があります。

メモ　ESX クラスタサービステンプレートを使用しない場合は、この手順を完了する必要はありません。

Linux サーバに VMware サーバ証明書をインストールするには、次の手順に従う必要があります。

**操作手順**

1. VMware サーバ証明書を次のようにダウンロードします。
   a. Web ブラウザを使用して vCenter ユーザーインタフェースにアクセスします。
   b. 右側のパネルで、［信頼されたルート CA 証明書をダウンロード］を選択します。
   c. Automation Director 共通コンポーネントのトラストストアが存在するサーバ上でダウンロードする場所を選択し、ダウンロードを確認します。
2. 共通コンポーネントのトラストストアが存在するサーバで、zip ファイルをダウンロードした場所に移動し、そのファイルを解凍します。

   メモ　ダウンロードしたファイルの拡張子が.zip でない場合は、拡張子を.zip に変更します。

   拡張子が.0（xxx.0）のファイルが含まれる「lin」という名前のフォルダが解凍されます。
3. 「xxx.0」ファイルを次のディレクトリにコピーします。
   `/etc/pki/tls/certs`
   証明書がトラストストアにインストールされます。

   メモ　ESX クラスタサービステンプレートを使用する場合は、『*Hitachi Automation Director ユーザーズガイド*』に説明されているように、Python もインストールする必要があります。

## 3.2.7 Device Manager サーバ証明書をインポートする

セキュア通信を使用する 1 つまたは複数の Device Manager サーバを接続する場合、Device Manager の証明書をインポートする必要があります。使用を計画している Device Manager サーバおよびサービスの数によって、複数の証明書のインストールが必要になる場合があります。

- Clone（ShadowImage）、Snapshot（Thin Image）、および Copy Topology サービスを使用する場合は、Device Manager サーバ証明書を Device Manager エージェントのトラストストアにインポートする必要があります。
- 複数の Device Manager サーバに接続する場合は、各サーバに証明書をインストールする必要があります。

### (1)　Device Manager Agent のトラストストアにサーバ証明書をインポートする

Clone（ShadowImage）、Snapshot（Thin Image）、および Copy Topology サービスを使用するときには、Device Manager サーバ証明書を Device Manager Agent のトラストストアにインポートする必要があります。

詳細については、『*Hitachi Command Suite システム構成ガイド*』の「Device Manager エージェントのトラストストアへのサーバ証明書のインポート」を参照してください。

## (2) Device Manager サーバの証明書をインポートする

Add Host 機能が有効になっている場合、各 Device Manager のサーバ証明書を取得し、自己署名証明書または認証局の証明書を Automation Director が参照する共通コンポーネントのトラストストアにインポートする必要があります。

Device Manager 証明書をインポートするには、次の手順に従う必要があります。

1. Device Manager のサーバ証明書を取得します。
   詳細については、『*Hitachi Command Suite システム構成ガイド*』の「SSL サーバの構築（Device Manager サーバ）」を参照してください。

   
   **メモ** Allocate Volumes for Symmetric Cluster Server from 2-Storage Systems サービスを使用する場合、Add Host 機能が有効かどうかにかかわらず、この手順が必要です。

2. 自己署名証明書または認証局の証明書をインポートします。
   認証局の証明書を使用するときには、中間認証局およびルート認証局の証明書もインポートする必要があります。場合によっては、認証局の証明書が既にインポートされている可能性があります。この場合、この手順は不要です。


**メモ** Automation Director サーバ上の Hitachi Command Suite 共通コンポーネントのトラストストアは、`jssecacerts` です。

Device Manager 証明書をインポートするときには、次のガイドラインに従ってください。

- 複数の Device Manager 構成を実行している場合は、各 Device Manager 用のサーバ証明書を取得する必要があります。
- 自己署名証明書を使用するときには、各 Device Manager サーバ用の自己署名証明書をトラストストアにインポートします。
- 認証局の証明書を使用するときには、サーバ証明書を発行する各認証局の証明書をトラストストアにインポートします。

**関連参照**

- (3) Hitachi Command Suite 共通コンポーネントのトラストストアに各 Device Manager のサーバ証明書をインポートする

## (3) Hitachi Command Suite 共通コンポーネントのトラストストアに各 Device Manager のサーバ証明書をインポートする

サーバ証明書は、各 Device Manager サーバから入手した後、Automation Director が参照する共通コンポーネントのトラストストアにインポートする必要があります。

1. Device Manager のトラストストアファイルをダウンロードします。

   
   **メモ** Device Manager サーバが認証局の証明書を既に使用している場合、このステップは不要です。

   Device Manager サーバが自己署名証明書を使用している場合は、Web ブラウザからトラストストアをダウンロードします。

詳細については、『*Hitachi Command Suite システム構成ガイド*』の「SSL クライアントの構築」を参照してください。
次の URL のどちらかを使用してトラストストアをダウンロードします。SSL の場合はポート番号を 2443 に、非 SSL の場合は 2001（デフォルト）に設定します。
SSL の場合：
`https://＜Device Manager サーバの IP アドレスまたはホスト名＞:＜Device Manager サーバのポート番号（SSL）＞/service/HiCommandCerts`
非 SSL の場合：
`http://＜Device Manager サーバの IP アドレスまたはホスト名＞:＜Device Manager サーバのポート番号（非 SSL）＞/service/HiCommandCerts`

2. 各 Device Manager の証明書をエクスポートします。

---

**メモ** Device Manager サーバが認証局の証明書を既に使用している場合、このステップは不要です。

---

Device Manager が自己署名証明書を使用している場合は、**hcmds64keytool** を使用して、Device Manager サーバ証明書を、ダウンロードしたトラストストアからエクスポートします。詳細については、『*Hitachi Command Suite システム構成ガイド*』の「SSL クライアントの構築」を参照してください。
ダウンロードしたトラストストアをトラストストアファイルとして指定します。
Windows の場合：
`＜共通コンポーネントのインストールフォルダ＞¥bin¥hcmds64keytool -export -keystore ＜トラストストアファイル名＞ -alias ＜エイリアス名＞ -file ＜サーバ証明書のパス＞`
Linux の場合：
`＜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 -export -keystore ＜トラストストアファイル名＞ -alias ＜エイリアス名＞ -file ＜サーバ証明書のパス＞`

3. 各 Device Manager の証明書を Hitachi Command Suite 共通コンポーネントのトラストストアにインポートします。
エクスポートした自己署名証明書のサーバ証明書、または認証局の証明書をトラストストアにインポートします。
Windows の場合、**hcmds64keytool** を使用します。Unix の場合、Java の標準 **keytool** を使用して、証明書をインポートします。Java で証明書をインポートするには、トラストストアのパスワードが 6 文字以上であることを確認してください。また、新しいエイリアス名が既存のエイリアス名と衝突しないことを確認してください。
Device Manager が認証局の証明書、中間認証局および（他の認証局もルートする）ルート認証局の証明書を使用している場合、認証局をインポートする必要があります。場合によっては、認証局の証明書が既にインポートされている可能性があります。この場合、この手順は不要です。
Windows の場合：
`＜共通コンポーネントのインストールフォルダ＞¥bin¥hcmds64keytool -import -alias ＜エイリアス名＞ -keystore ＜共通コンポーネントのインストールフォルダ＞¥uCPSB¥jdk¥jre¥lib¥security¥jssecacerts -storepass ＜トラストストアへのアクセスパスワード＞ -file ＜サーバ証明書のパス＞`
Unix の場合：
`＜共通コンポーネントのインストールディレクトリ＞/jdk/bin/hcmds64keytool -import -alias ＜エイリアス名＞ -keystore ＜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 <*トラストストアへのアクセスパスワード*> -file <*サーバ証明書のパス*>

4. **hcmds64srv** コマンドを実行して、サービスを再開します。

### 3.2.8 REST API クライアントと REST API サーバの間で SSL 通信を使用するための設定を指定する（認証局によるサーバ証明書を使っている場合）

自己署名証明書または認証局の証明書を使用することで、REST API クライアントと REST API サーバの間で使用する SSL 通信を設定することが可能です。

詳細については、『*Hitachi Command Suite Configuration Manager REST API リファレンスガイド*』の「REST API クライアントと REST API サーバ間で SSL 通信するよう設定する（自己署名証明書を使用する場合）」または「REST API クライアントと REST API サーバ間で SSL 通信するよう設定する（認証局が発行したサーバ証明書を使用する場合）」 を参照してください。

### 3.2.9 サーバ証明書の有効期限を確認する

SSL 証明書の有効期限をチェックすることで、証明書の有効期限が切れていないかどうかを確認できます。管理サーバ証明書の有効期限が切れておらず、管理対象サーバとのセキュア通信を維持できることを確認する必要があります。

Hitachi Command Suite 共通コンポーネントのサーバ証明書の有効期限をチェックするには、次のコマンドを実行します。

Windows の場合：

<*共通コンポーネントのインストールフォルダ*>¥uCPSB¥jdk¥jre¥bin¥keytool -printcert -v -file <*サーバ証明書のパス*>

Linux の場合：

<*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 -printcert -v -file <*サーバ証明書のパス*>

**メモ**　自己署名証明書の有効期限は、サーバ間の接続時にはチェックされません。Automation Director サーバと Device Manager サーバの接続時に証明書の有効期限をチェックする必要がある場合は、認証局によって発行された証明書を使用してください。その場合、サーバの証明書だけでなく、認証局と中間認証局の証明書もインポートします。

## 3.3 別のホストへ Automation Director を移動する

必要に応じて、Automation Director を別のホストに移動できます。

**メモ**　移動元のホスト名または IP アドレスと移動先のホスト名または IP アドレスが異なる場合は、管理サーバのホスト名を変更する必要があります。

**前提条件**

以下の設定が移動元のホストと移動先のホストで同じであることを確認します。

- ホスト名と IP アドレス。
- Automation Director によって使用される OS ユーザーのアカウント。

- Hitachi Command Suite 製品環境（構成、バージョン、およびリビジョン）。
- Automation Director のインストールパス。

Automation Director の［**タスク**］タブの「状態」列が実行中、応答待ち中、異常検出、長期実行中、または停止中を示す処理中のタスクがないことも確認する必要があります。

**操作手順**

1. Administrator 権限を使用して管理サーバにログインします。
2. 移動元ホストで Automation Director のバックアップを完了します。
   a. **hcmds64srv /stop** コマンドを実行して、現在のサービスを停止します。
   b. **backupsystem** コマンドを実行して、バックアップを実行します。
3. アーカイブされたバックアップファイルを移動先のホストに移動します。
4. 移動先のホストの管理サーバにログオンします。
5. 移動先のホストで、Automation Director のリストアを実行します。
   a. **hcmds64srv /stop** コマンドを実行して、サービスを停止します。
   b. **restoresystem** コマンドを実行して、バックアップをリストアします。
   c. リストア先の環境に合わせて、以下の構成ファイルの設定を変更します。
      - 外部認証サーバ統合構成ファイル（exauth.properties）
      - セキュリティ定義ファイル（security.conf）
      - 監査ログ定義ファイル（auditlog.conf）
      - ポート番号変更設定（user_httpsd.conf）
      - SSL 環境構築手順（user_httpsd.conf）

   これらの構成ファイルは、次のディレクトリにあります。
   - *<バックアップ先のディレクトリ>¥HBase¥base¥conf*
   - *<バックアップ先のディレクトリ>¥HBase¥base¥httpsd.conf*
6. ポート番号が変更された場合、新しいポート番号を反映するように、必要な設定を変更します。
7. **hcmds64srv /start** コマンドを実行して、サービスを再開します。

**関連タスク**

- 3.1.4 管理サーバのホスト名または IP アドレスを変更する

## 3.4 システム構成を変更する

config_user.properties ファイルを編集すると、ログやタスクなど、Automation Director のさまざまな設定を構成できます。ファイルを変更して保存した後で、Automation Director エンジン Web サービスは再起動する必要があることに注意してください。

このファイルを編集することで、以下の設定を変更できます。

- ログファイル構成（保存するログの数を指定します）
- タスクおよび履歴構成（保存するタスクとタスク履歴の数を指定します）
- リモートコマンド実行に関する構成（SSH/telnet ポート番号）
- メール通知の構成情報
- Service Builder に関する構成情報
- 接続タイムアウト値の設定

ファイルは、次のディレクトリにあります。
＜*Automation Director のインストールフォルダ*＞¥conf

ファイルは、次の形式を使用します。

*specification-key-name*=*setting*

プロパティファイルを編集するときには、次のことに注意してください。

- #で始まる行は、コメントとして扱われます。
- 空白行は無視されます。
- エンコードは ISO 8859-1 です。
- 内容は大文字と小文字が区別されます。
- 文字列の中で¥を指定するには、¥¥と入力する必要があります。
- 設定として無効な値を入力した場合はデフォルト値に設定され、メッセージ KNAE02022-W が統合トレースログとパブリックログに送信されます。
- 1 つのファイル内で同じ指定キーが複数回入力された場合は、最後に指定したキーが有効になります。

**表 1 config_user.properties ファイルの設定**

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| HTTP 接続ポート番号 | server.http.port | Automation Director サーバと Hitachi Command Suite 共通コンポーネント間の HTTP 通信に使用されるポート番号を指定します。 | 0～65535 | 22015 |
| ログ[1] | logger.message.server.MaxBackupIndex | サーバのログバックアップファイルの最大数を指定します。 | 1～16 | 7 |
| | logger.message.server.MaxFileSize | サーバの最大ログファイルサイズ（KB 単位）を指定します。 | 4～2097151 | 1024 |
| | logger.message.command.MaxBackupIndex | コマンドのログバックアップファイルの最大数を指定します。 | 1～16 | 7 |
| | logger.message.command.MaxFileSize | コマンドの最大ログファイルサイズ（KB 単位）を指定します。 | 4～2097151 | 1024 |
| | logger.TA.MaxFileSize | タスクの最大ログファイルサイズ（KB 単位）を指定します。 | 4～2097151 | 10240 |
| タスク管理 | tasklist.autoarchive.taskRemainingPeriod | 終了したタスクをタスクリストに残しておく期間（日数）を指定します。 | 1～90 | 7 |
| | tasklist.autoarchive.executeTime | 自動アーカイブタスクを実行する時刻を指定します。 | 00:00:00～23:59:59 | 04:00:00 |
| | tasklist.autoarchive.maxTasks | タスクリストに表示するタスクの最大数を指定します。 | 100～5000 | 5000 |

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| | tasklist.autodelete.maxHistories | 保持する履歴エントリの最大数を指定します。 | 100～30000 | 30000 |
| 繰り返し | foreach.max_value | 繰り返し実行部品によって実行できる同時タスクの最大数を指定します。 | 1～99 | 3 |
| リモート接続ポート番号 | ssh.port.number | 操作対象機器の SSH ポート番号を指定します。 | 0～65535 | 22 |
| | telnet.port.number | 操作対象機器の Telnet ポート番号を指定します。 | 0～65535 | 23 |
| 一般的なコマンド<br>リモートコマンド<br>ファイル転送<br>ターミナル接続 | plugin.stdoutSize.wmi | 標準出力および標準エラーの合計サイズがプロパティ値を超えると、部品エラーが発生します。<br>注:プロパティ値の単位はキロバイト（KB）です。<br>次の条件が当てはまる場合、部品操作時にこのプロパティが適用されます。<br>- 接続先のホストが Windows<br>- 実行対象の部品が汎用コマンド実行部品またはコンテンツ部品<br>Windows では、改行数が 65535 以上でも、部品は実行を続けることができます。この機能の特徴を生かすには、プロパティ値を適切に設定する必要があります。たとえば、このプロパティが 100 KB に設定（デフォルト値）されている場合は、部品は改行の最大数 65535 以上を処理できません。部品は、最大 100 KB に達すると実行を停止します。 | 1～1024 | 100 |
| | plugin.stdoutSize.ssh | 標準出力および標準エラーの合計サイズがプロパティ値を超えると、部品エラーが発生します。<br>注:プロパティ値の単位はキロバイト（KB）です。<br>次の 2 つの主要な条件が当てはまる場合、部品操作時にこのプロパティが適用されます。<br>[条件（1）（注：次の対象の条件を満たす必要があります。）]<br>- 接続先のホストが Linux または UNIX。<br>- 実行対象の部品が汎用コマンド実行部品またはコンテンツ部品。 | 1～1024 | 100 |

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| | | [条件（2）（注：次のプロトコル条件と部品の条件を満たす必要があります。）]<br>- 接続プロトコルが SSH。<br>- 実行対象の部品がターミナル接続部品またはターミナルコマンド実行部品。 | | |
| | plugin.stdoutSize.telnet | 標準出力および標準エラーの合計サイズがプロパティ値を超えると、部品エラーが発生します。<br>注:プロパティ値の単位はキロバイト（KB）です。<br>次の条件が当てはまる場合、部品操作時にこのプロパティが適用されます。<br>- 接続プロトコルが SSH。<br>- 対象の部品がターミナル接続部品またはターミナルコマンド実行部品。 | 1～1024 | 100 |
| | plugin.remoteFileAccess.retry.times | コンテンツ部品またはファイル転送部品によって内部実行されるファイル操作コマンドの再試行回数を指定します。<br>再試行間隔は 100ms に固定されています。<br>一時的なファイルアクセスエラーが発生した場合、コマンドを再試行すると操作が成功することがあります。ただし、ファイルアクセスエラーが回復しなかった場合、部品が終了するまで、再試行に余分な時間がかかります。ディスクに問題がない場合でもファイルアクセスエラーが発生する環境では、このプロパティを指定してください。 | 0～100 | 0 |
| | ssh.privateKeyFile | SSH 接続に公開鍵認証が使用される場合、秘密鍵ファイルの絶対パスを指定します。 | 0～255 文字 | ""（null 文字） |
| | plugin.localMode | ローカル実行モードを有効にするか無効にするかを指定します。<br>true：有効<br>false：無効 | true/false | true |
| リモートファイル操作の再試行 | plugin.remoteFileAccess.retry.times | コンテンツ部品およびファイル転送部品によって内部実行されるファイルを操作するコマンドの再試行回数を指定します。再試行間隔は 100ms に固定されています。 | 0～100 | 0 |

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| | | 一時的なファイルアクセスエラーが発生した場合でも、再試行によって成功することがあります。ただし、ファイルアクセスエラーが回復しなかった場合、部品が終了するまで、再試行に余分な時間がかかります。ディスクなどに問題がない場合でもファイルアクセスエラーが発生する環境では、このプロパティを設定してください。 | | |
| ターミナル接続 | plugin.terminal.prompt.account | ユーザー ID 待機状態の検出に使用される正規表現を指定します。(1～1,024 文字)<br>標準出力および標準エラー出力が指定された正規表現に一致した場合、ターミナル接続部品（プロトコルとして Telnet が指定される）は、ユーザー ID が入力されなければならないと判断して、ユーザー ID を入力します。 | 正規表現パターンで使用できる文字列。 | login\|Login Name\|Username\|UserName |
| | plugin.terminal.prompt.password | パスワード待機状態の検出に使用される正規表現を指定します。(1～1,024 文字)<br>標準出力および標準エラー出力が指定された正規表現に一致した場合、ターミナル接続部品（プロトコルとして Telnet が指定される）は、パスワードが入力されなければならないと判断して、パスワードを入力します。 | 正規表現パターンで使用できる文字列。 | password\|Password\|PassWord |
| | telnet.connect.wait | 操作対象機器との Telnet 接続が確立された後、標準出力が戻るまでの待ち時間（秒数）を指定します。 | 1～600 | 60 |
| リモートコマンド | plugin.remoteCommand.executionDirectory.wmi | 対象ホストが Windows を実行している場合に実行するコンテンツ部品を含む、実行ディレクトリのパスを指定します。実行ディレクトリは、事前に作成しておく必要があります。コンテンツ部品の［実行モード］が［スクリプト］の場合、指定された値とスクリプトファイル名の合計文字列長は最大 140 文字です。長さが 140 文字を超えた場合、スクリプトの転送は失敗します。さらに、スクリプトファイル名は 90 文字以内で指定しなければな | 0～128 文字の文字列 | ""（null 文字） |

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| | | らないため、この指定値は 50 文字以内でなければなりません。 | | |
| | plugin.remoteCommand.executionDirectory.ssh | 操作対象ホストの OS が UNIX の場合にコンテンツ部品を実行する実行ディレクトリのパスを指定します。実行ディレクトリは、事前に作成しておく必要があります。 | 0～128 文字の文字列 | ""（null 文字） |
| | plugin.remoteCommand.workDirectory.ssh | 操作対象ホストの OS が UNIX の場合、ファイル転送部品またはコンテンツ部品の実行時に使用される作業フォルダを指定します。フォルダまたはシンボリックリンクを絶対パスとして入力します（1～128 文字）。さらに、シンボリックリンクはパスのレイヤとして含めることができます。 | 1～128 | /tmp/Hitachi_AO |
| リモートホスト接続の再試行 | ssh.connect.retry.times | 操作対象機器への SSH 接続が失敗した場合の再試行回数を指定します。 | 0～100 | 3 |
| | ssh.connect.retry.interval | 操作対象機器への SSH 接続が失敗した場合の再試行間隔（秒数）を指定します。 | 1～600 | 10 |
| | wmi.connect.retry.times | 操作対象機器への WMI 接続が失敗した場合の再試行回数を指定します。 | 0～100 | 3 |
| | wmi.connect.retry.interval | 操作対象機器への WMI 接続が失敗した場合の再試行間隔（秒数）を指定します。 | 1～600 | 10 |
| | telnet.connect.retry.times | 操作対象機器への Telnet 接続が失敗した場合の再試行回数を指定します。 | 0～100 | 3 |
| | telnet.connect.retry.interval | 操作対象機器への Telnet 接続が失敗した場合の再試行間隔（秒数）を指定します。 | 1～600 | 10 |
| メール通知の再試行 | mail.notify.retry.times | メールを送信する通知機能が失敗した場合の再試行回数を指定します。 | 0～100 | 3 |
| | mail.notify.retry.interval | メールを送信する通知機能が失敗した場合の再試行間隔（秒数）を指定します。 | 1～600 | 10 |
| | mail.plugin.retry.times | メール通知部品でのメール送信が失敗した場合の再試行回数を指定します。 | 0～100 | 3 |
| | mail.plugin.retry.interval | メール通知部品でのメール送信が失敗した場合の再試行間隔（秒数）を指定します。 | 1～600 | 10 |

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| 監査ログ | logger.Audit.command.useLoginUserID | コマンドが実行されるときの監査ログのサブジェクト識別情報に、ユーザー ID として Automation Director のログインユーザー ID を出力するかどうかを指定します。 | true/false | false |
| ウィンドウの更新 | client.events.refreshinterval | イベントの更新間隔（秒数）を指定します。 | 0～65535 | 5 |
| Service Builder | client.editor.upload.maxfilesize | [Service Builder Edit] ウィンドウで、Automation Director の操作に使用される端末からサーバにアップロードできる最大ファイルサイズ（MB 単位）を指定します。 | 1～10 | 3 |
| | client.editor.canvas.maxwidth | [フロー] ビューの幅の最大サイズ（px 単位）を指定します。 | 3600～10000 | 3600 |
| | client.editor.canvas.maxhigh | [フロー] ビューの高さの最大サイズ（px 単位）を指定します。 | 2400～30000 | 2400 |
| | server.editor.step.perTemplate.maxnum | サービステンプレートあたりの最大ステップ数を指定します。 | 320～40000 | 320 |
| | server.editor.step.perLayer.maxnum | レイヤあたりの最大ステップ数を指定します。 | 80～10000 | 80 |
| | server.editor.publicProperty.perTemplate.maxnum | サービステンプレートあたりのサービスプロパティの最大数を指定します。 | 100～2000 | 1000 |
| | server.editor.propertyGroup.perTemplate.maxnum | サービステンプレートあたりのプロパティグループの最大数を指定します。 | 5～1000 | 500 |
| デバッガ | tasklist.debugger.autodelete.taskRemainingPeriod | サービステンプレートあたりのプロパティグループの最大数を指定します。 | 1～90 | 7 |
| | client.debugger.tasklog.maxfilesize | [タスクログ] タブに表示されるタスクログのサイズ（KB）を指定します。 | 4～10240 | 1024 |
| | logger.debugger.TA.MaxFileSize | デバッグタスクの最大ログファイルサイズ（KB）を指定します。 | 4～2097151 | 10240 |
| 長期実行中のタスクのチェック間隔しきい値 | server.longRunning.check.interval | 長期実行中のタスクのチェック間隔しきい値（分数） | 0～20160 | 2880 |
| 長期実行中の監視間隔 | server.longRunning.monitor.interval | 長期実行中の監視間隔（秒数） | 1～3600 | 60 |

| カテゴリ | キー名 | 設定 | 値 | デフォルト値 |
|---|---|---|---|---|
| Web クライアント | plugin.http.connect.timeout | HTTP/HTTPS 接続が確立されるときのタイムアウト値(秒数) を指定します。0 を指定した場合、タイムアウトは発生しません。 | 0～3600 | 60 |
| | plugin.http.read.timeout | HTTP/HTTPS 接続の確立後、データが読み込まれるときのタイムアウト値 (秒数) を指定します。0 を指定した場合、タイムアウトは発生しません。 | 0～86400 | 600 |

[1] タスクのログ出力しきい値は、サービス共有プロパティで設定します。

［例］

logger.message.server.MaxBackupIndex = 7

logger.message.server.MaxFileSize = 1024

logger.message.command.MaxBackupIndex = 7

logger.message.command.MaxFileSize = 1024

logger.TA.MaxFileSize = 1024

tasklist.autoarchive.taskRemainingPeriod = 7

tasklist.autoarchive.executeTime = 04:00:00

tasklist.autoarchive.maxTasks = 5000

tasklist.autodelete.maxHistories = 30000

mail.notify.retry.times = 3

mail.notify.retry.interval = 10

mail.plugin.retry.times = 3

mail.plugin.retry.interval = 10

client.events.refreshinterval = 5

## 3.5 メール通知を構成する

メール通知設定を構成し、障害発生時またはタスクに問題が発生した場合に、メール通知を受信するようにします。メールアドレス、件名、障害や問題について受信する情報のタイプを構成できます。

**メモ**　システムのメール通知を有効にするには、［管理］タブでシステム・パラメータを設定する必要があります。詳細については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。

メール定義ファイル、mailDefinition は XML 形式です。次のディレクトリにあります。

＜*Automation Director のインストールフォルダ*＞¥conf

定義ファイルは、次の形式を使用します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<mail xmlns="http://www.example.com/products/it/software/xml/
automation/">
<title>＜メールタイトル＞</title>
<body>＜メール本文＞</body> </mail>
```

ファイルを編集するときには、次のことに注意してください。

- メール通知の定義ファイルがない場合や整形式 XML でない場合、読み取りエラーが発生します。この場合、メールはデフォルトの件名と本文で送信されます。
- <mail>、<title>、および<body>の外部でタグを指定した場合、タグが整形式 XML であっても、タグとその内容は無視されます。
- <title>または<body>タグの値が省略された場合には、空の文字列が指定されます。
- <mail>タグを省略することはできません。省略した場合、形式は無効であり、読み取りエラーが発生します。
- すべてのエントリで大文字と小文字が区別されます。

設定を変更するには、mailDefinition ファイルのメールの件名およびメール本文のセクションを編集します。

**表 2 メール通知設定**

| 設定 | XML 要素 | 文字列長 | デフォルト値 |
|---|---|---|---|
| メール通知に使用されるメールの件名 | <title> | 0～9,999 バイトの文字列 | [Automation Director] $TASK_NAME$が $TASK_STATUS$に変更されました。 |
| メール通知に使用されるメールの本文 | <body> | 0～9,999 バイトの文字列 | サービスグループ名：$SERVICE_GROUP_NAME$ タスク名：$TASK_NAME$ 実行者:$USER_NAME$ タスク詳細：$TASK_DETAIL_ URL$ |

**XML エンティティ参照**

| メールに表示する文字 | 入力する文字 |
|---|---|
| & | &amp; |
| < | &lt; |
| > | &gt; |
| " | &quot; |
| ' | &apos; |

**表 3 メール通知に埋め込まれる文字**

| 埋め込まれる文字 | 項目 | 備考 |
|---|---|---|
| $SERVICE_GROUP_NAME$ | サービスグループ名 | サービスグループ名を表す文字列が設定されます。 |
| $TASK_NAME$ | タスク名 | タスクのプロパティの形式に従ってタスク名が設定されます。 |
| $TASK_ID$ | タスク ID | |
| $TASK_KIND$ | タスク種別 | |
| $SERVICE_NAME$ | サービス名 | |
| $TASK_TAGS$ | タスクのタグ | |
| $TASK_STATUS$ | タスクの状態 | |
| $EXECUTION_DATE$ | 実行操作日時 | |
| $PLANNED_START_DATE$ | 開始予定日時 | |
| $START_DATE$ | 開始日時 | |
| $END_DATE$ | 終了日時 | |
| $SCHEDULE_PERIOD$ | 定期実行周期 | |
| $SCHEDULE_TIME$ | 定期実行時刻 | |
| $SCHEDULE_ START_DATE$ | 定期実行適用開始日 | |
| $USER_NAME$ | 実行者 | |
| $TASK_DETAIL_URL$ | ［タスク詳細］ウィンドウの URL | http で始まる URL が設定されます。 |

## 3.6 パスワードポリシーを変更する

security.conf ファイルを編集すると、ユーザーパスワードの条件とロックに関連する Automation Director のさまざまな設定を構成できます。これにより、ユーザーの特定のパスワードポリシーに適したセキュリティ設定にカスタマイズできます。

ファイルは、次のディレクトリにあります。

*<共通コンポーネントのインストールフォルダ>*¥conf¥sec

ファイルは、次の形式を使用します。

*specification-key-name=setting*

ファイルを編集する場合は、1 行に 1 つの指定キーと設定を指定します。以下に、セキュリティ定義ファイルのデフォルトの状態を示します。

```
# This is the minimum length of the password
# (minimum:1 -256 characters)
password.min.length=4

# This is the minimum number of uppercase characters included in the
password
```

```
# (minimum:0-256 characters, character type:A-Z)
password.min.uppercase=0

# This is the minimum number of lowercase characters included in the
password
# (minimum:0-256 characters, character type: a-z)
password.min.lowercase=0

# This is the minimum number of numeric characters included in the
password
# (minimum:0-256 characters, character type:0-9)
password.min.numeric=0

# This is the minimum number of symbolic characters included in the
password
# (minimum:0-256 characters, character type:!# $ % & ' ( ) * + - .= @ ¥ ^
_ |)
password.min.symbol=0

# This specifies whether the user ID can be used for the password
# (true = cannot use the user ID, false = can use the user ID)
password.check.userID=false

# This is the minimum number of login failures before an account is
locked
# (minimum:0-10 times)
account.lock.num=0
```

**表 4 security.conf ファイルの設定**

| キー名 | 設定 | 設定可能な値 | デフォルト値 |
|---|---|---|---|
| password.min.length | パスワードの最小文字数を指定します。 | 1～256 | 4 |
| password.min.uppercase | パスワードに含むべき大文字の最小数を指定します。0 を指定した場合、大文字の数に関する制約はありません。 | 0～256 | 0 |
| password.min.lowercase | パスワードに含むべき小文字の最小数を指定します。0 を指定した場合、小文字の数に関する制約はありません。 | 0～256 | 0 |
| password.min.numeric | パスワードに含むべき数字の最小数を指定します。0 を指定した場合、文字の数に関する制約はありません。 | 0～256 | 0 |
| password.min.symbol | パスワードに含むべき記号の最小数を指定します。0 を指定した場合、記号の | 0～256 | 0 |

| キー名 | 設定 | 設定可能な値 | デフォルト値 |
|---|---|---|---|
| | 数に関する制約はありません。 | | |
| password.check.userID | ユーザー ID と同じパスワードの設定を禁止するかどうかを指定します。 | • true：禁止します<br>• false：禁止しません | false |
| account.lock.num | アカウントが自動的にロックされるまでのログインの連続失敗回数を指定します。0 を指定した場合、ログインの試みが失敗してもアカウントは自動的にロックされません。 | 0～10 | 0 |

## 3.7 操作対象機器との接続に使用される情報を構成する

Automation Director の部品およびサービスが、部品によるタスクが実行され、アクションが実施されるリモートマシンと通信できるようになる前に、リモートマシン接続情報を構成する必要があります。

開始する前に、以下のことを確認してください。

- 次のパスにあるすべてのファイルは、接続先プロパティファイルとみなされます。
  ＜*Automation Director のインストールフォルダ*＞¥Automation¥conf¥plugin¥destinations
- ファイル名は、次の形式を使用します。
  ＜*ホスト名*＞.properties, ＜*IPv4 アドレス*＞.properties, ＜*IPv6 アドレス*＞.properties

> **メモ** IPv6 アドレス内のコロン「:」はファイル名には使用できないため、ダッシュ（-）に置き換えます。例：2001::234:abcd -> 2001--234-abcd.properties.

サンプルファイルは、次の場所にあります。

＜*Automation Director のインストールフォルダ*＞¥Automation¥conf¥plugin¥destinations¥#sample.properties

プロパティファイルを編集するときには、次のことに注意してください。

- #で始まる行は、コメントとして扱われます。
- 空白行は無視されます。
- エンコードは ISO 8859-1 です。
- 内容は大文字と小文字が区別されます。
- 文字列の中で¥を指定するには、¥¥と入力する必要があります。
- 接続先プロパティファイルで無効な値を指定した場合、接続先プロパティファイルを参照する部品で実行エラーが発生します。

- 1 つのファイル内で同じ指定キーを複数回入力した場合は、最後に指定したキーが有効になります。

対象機器に接続するには、以下の構成情報を使用してください。

**対象機器がクラスタ環境の一部である場合のガイドライン**

クラスタの対象機器に情報を入力する場合：

- クラスタ環境で対象機器が Windows Server 2012 または Windows Server 2012 R2 を実行している場合、作業ディレクトリ（wmi.workDirectory.sharedName および wmi.workDirectory.sharedPath）を設定する必要があります。設定しないと、部品が接続エラーの原因となります。
- コンテンツ部品でスクリプトを実行する場合は、実行ディレクトリ（common.executionDirectory）を指定する必要があります。指定しないと、スクリプトは転送されません。

| キー名 | 設定 | 有効値 | 最小値 | 最大値 |
|---|---|---|---|---|
| terminal.charset | 通信に使用される文字セットを指定します。 | EUC-JP<br>eucjp<br>ibm-943C<br>ISO-8859-1<br>MS932<br>PCK<br>Shift_JIS<br>UTF-8<br>windows-31j | 1 | 64 |
| telnet.port | ターミナル接続部品での Telnet 接続に使用されるポート番号を指定します。この設定は、プロパティファイル（config_user.properties）の telnet.port.number 設定に優先します。 | 0～65535 | 0 | 65535 |
| ssh.port | 次のどれかの部品を使用して、SSH 接続に使用されるポート番号を指定します：<br>• 汎用コマンド実行部品<br>• ファイル転送部品<br>• ターミナル接続部品<br>• コンテンツ部品<br>この設定は、プロパティファイル（config_user.properties）の ssh.port.number 設定に優先します。 | 0～65535 | 0 | 65535 |
| telnet.prompt.account | ターミナル接続部品を使用して対象機器との接続を確立する際に出力され | 正規表現パターンで使用される文字列 | 1 文字 | 1024 文字 |

| キー名 | 設定 | 有効値 | 最小値 | 最大値 |
|---|---|---|---|---|
| | るユーザー ID の入力を求める文字列の検出に使用する、正規表現パターンを指定します。1～1,024 文字を使用できます。たとえば、「Username:」と指定します。 | | | |
| telnet.prompt.password | ターミナル接続部品を使用して対象機器との接続を確立する際に出力されるパスワードの入力を求める文字列の検出に使用する、正規表現パターンを指定します。1～1,024 文字を使用できます。たとえば、「Password:」と指定します。 | 正規表現パターンで使用される文字列 | 1 文字 | 1024 文字 |
| telnet.noStdout.port.list | ターミナル接続部品を使用して接続が確立された後に標準出力を返さないサービスのポート番号を指定します。1～1,024 文字を使用できます。複数のポート番号を指定するには、区切り文字としてコンマを使用します。 | 0～65535 とコンマ（,） | 1 文字 | 1024 文字 |
| wmi.workDirectory.sharedName | Windows 対象機器のプロパティです。操作対象でのコマンド実行時にファイルが送信される共有フォルダの共有フォルダ名を指定します。フォルダは wmi.workDirectory.sharedPath と同じである必要があります。このプロパティを使用する場合、操作対象の管理共有設定は不要です。0～80 文字の文字列を指定します。 | 1 バイトの英数字、「-」、「_」、および「.」。 | 0 文字 | 80 文字 |
| wmi.workDirectory.sharedPath | Windows 対象機器のプロパティです。操作対象でのコマンド実行時にファイルが送信される共有フォルダの絶対パスを指定します。汎用コマンド実行部品を使用している場合、実行ディレクトリは、このプロパティにリストされるパスの下の ¥Hitachi¥CMALib¥HAD¥home になります。フォルダは wmi.workDirectory.share | 1 バイトの英数字、「:」、「¥」、「-」、「_」、および「.」。 | 0 文字 | 80 文字 |

| キー名 | 設定 | 有効値 | 最小値 | 最大値 |
|---|---|---|---|---|
| | dName と同じである必要があります。このプロパティを使用する場合、操作対象の管理共有設定は不要です。0～80 文字の文字列を指定します。 | | | |
| ssh.workDirectory | Linux/Unix 対象機器のプロパティです。ファイル転送部品またはコンテンツ部品で転送用ファイルが置かれるディレクトリの絶対パスを指定します。このプロパティで指定されたパスも、親ディレクトリのパスも、ファイル転送部品の接続先および受信先として指定することはできません。作業フォルダには、接続するユーザーの読み取り権限、書き込み権限、および実行権限が必要です。ファイル転送部品またはコンテンツ部品が使用されるときに、このプロパティで指定されたパスが存在しなかった場合、部品の実行時に作成されます。ディレクトリを作成できない場合、部品の実行は異常終了します。新しいディレクトリのアクセス権限は、必ず 777 であることを確認してください。優先されるのは、config_user.properties ファイルで定義された plugin.remoteCommand.workDirectory.ssh の値です。0～128 文字の文字列を指定します。 | 1 バイトの英数字、「/」、「-」、「_」、および「.」。 | 0 文字 | 128 文字 |
| common.executionDirectory | 操作対象に対してコンテンツ部品を実行するときの実行ディレクトリを指定します。部品定義で定義された実行ディレクトリの値が設定されていなかった場合、このプロパティの値が適用されます。優先されるのは、config_user.properties ファイルで定義された plugin.remoteCommand. | | 0 文字 | 128 文字 |

| キー名 | 設定 | 有効値 | 最小値 | 最大値 |
|---|---|---|---|---|
| | executionDirectory.wmi と plugin.remoteCommand.executionDirectory.ssh の値です。0～128 文字の文字列を指定します。 | | | |

## 3.8 エージェントレス接続の Windows 前提条件

エージェントレス接続を使用するには、次のセクションに記載されている Windows の前提条件が必要です。

**サポートされるユーザー**

エージェントレス接続では、次のユーザーを使用できます。

- ビルトイン Administrator
- Active Directory のビルトイン Administrator
- administrators グループに属するユーザー
- Active Directory の Domain Admin グループに属するユーザー

administrator グループに属するユーザーを使用する場合は、コマンド実行時に UAC（ユーザーアクセス制御）昇格が適用されないことに注意してください。また、リモート接続 OS が次のいずれかの条件を満たす場合は、レジストリも編集する必要があります。

- Windows Server 2008 で UAC 機能が有効である
- Windows Server 2008 R2 で UAC 機能が有効である
- OS は Windows Server 2012 である
- OS は Windows Server 2012 R2 である

レジストリエディタを使用して、次のレジストリのキーのエントリを設定します。

**メモ**　OS を再起動する必要はありません。

| 項目 | 値 |
|---|---|
| レジストリキー | HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System |
| レジストリエントリ | LocalAccountTokenFilterPolicy |
| レジストリエントリとして設定される値 | 1 (DWORD) |

必要に応じて、コマンドプロンプトで次のコマンドを入力できます。

```
reg add HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion
¥Policies¥System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0x1 /f
```

**管理共有設定**

管理共有を使用して、レジストリエディタで次のレジストリのキーの下にエントリを設定し、OS を再起動します。

| 項目 | 値 |
|---|---|
| レジストリキー | HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Lanmanserver¥parameters |
| レジストリエントリ | AutoShareServer |
| レジストリエントリとして設定される値 | 1 (DWORD) |

コマンドプロンプトで次のコマンドを入力します。

```
reg add HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Lanmanserver
¥parameters /v AutoShareServer /t REG_DWORD /d 1
```

## 3.9 エージェントレス接続の SSH 前提条件

エージェントレス接続を使用するには、次のセクションに記載されている SSH プロトコル前提条件が必要です。

SSH 前提条件は次の部品で必要です。

- コンテンツ部品
- 汎用コマンド実行部品
- ファイル転送部品
- ターミナル接続部品
- ターミナルコマンド実行部品
- ターミナル切断部品

**メモ**　SSH はバージョン 2 をサポートする必要があります。

### 3.9.1 パスワード認証

SSH サーバに対するパスワード認証を、次のように設定する必要があります。

1. リモート操作対象ホストに root としてログインします。
2. sshd_config ファイルを開きます。
   HP-UX の場合：/opt/ssh/etc/sshd_config
   他の OS の場合：/etc/ssh/sshd_config
3. PubkeyAuthentication の値を yes に設定します。PubkeyAuthentication の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。
4. 次のコマンドを実行して、sshd サービスを再開します。
   RHEL/CentOS/SUSE Linux/Oracle Linux（RHEL 6.4 など）の場合：/etc/rc.d/init.d/sshd restart

Solaris（Solaris 10 など）の場合：/usr/sbin/svcadm restart ssh
AIX（AIX 6.1 など）の場合：kill -HUP [**Process ID of sshd**]
HP-UX（HP-UX 11i V3 など）の場合：/sbin/init.d/secsh stop; /sbin/init.d/secsh start

**メモ**　これらのコマンドは、OS のバージョンによって変わることがあります。追加情報については、OS のマニュアルを参照してください。

## 3.9.2 公開鍵認証

ここでは、SSH サーバに接続する公開鍵を認証する方法について説明します。

**SSH サーバのセットアップ**

公開鍵認証を使用するには、SSH サーバに対する公開鍵認証を設定する必要があります。

1. リモート操作対象ホストに root としてログインします。
2. sshd_config を開きます。
   HP-UX：/opt/ssh/etc/sshd_config
   HP-UX 以外：/etc/ssh/sshd_config
3. PubkeyAuthentication の値を yes に設定します。PubkeyAuthentication の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。
4. 次のコマンドを実行して、sshd サービスを再開します。
   RHEL/CentOS/SUSE Linux/Oracle Linux（RHEL 6.4 など）の場合：/etc/rc.d/init.d/sshd restart
   Solaris（Solaris 10 など）の場合：/usr/sbin/svcadm restart ssh
   AIX（AIX 6.1 など）の場合：kill -HUP [**Process ID of sshd**]
   HP-UX（HP-UX 11i V3 など）の場合：/sbin/init.d/secsh stop; /sbin/init.d/secsh start

**メモ**　これらのコマンドは、OS のバージョンによって変わることがあります。追加情報については、OS のマニュアルを参照してください。

**鍵の作成（初回）**

公開鍵と秘密鍵を作成します。鍵は、Automation Director がインストールされる OS 上で作成することを強く推奨します。

**メモ**　秘密鍵を別の OS に移動すると、秘密鍵が漏えいしてセキュリティリスクを負う恐れがあります。ただし、別の OS 上で作成された鍵を使用することは可能です。

参考として、以下の手順では RHEL6.4（Linux）上で鍵を作成します。

1. **ssh-keygen** コマンドを実行します。
   RSA 鍵を作成する場合：ssh-keygen -t rsa
   DSA 鍵を作成する場合：ssh-keygen -t dsa
2. 秘密鍵の場所と名前を決めます。

マルチバイト文字を含まないパスとファイル名を指定します。デフォルトでは、~/.ssh/id_rsa が設定されます（RSA 鍵を作成する場合）。秘密鍵は、選択されたパスに対して指定されたファイル名として設定されます。公開鍵は、秘密鍵と同じディレクトリに、秘密鍵の名前に「.pub」ファイル拡張子を付けたファイルとして設定されます。

3. パスフレーズを入力します。
   パスフレーズを入力して、Return キーを押すように求められます。次に、パスフレーズの再入力を求められます。秘密鍵のパスフレーズを設定しない場合は、パスフレーズを入力せずに Return キーを押します。

**Automation Director への秘密鍵の配置**

Automation Director がインストールされる OS 上に秘密鍵を配置します。任意の場所に配置し、パスをプロパティファイル（config_user.properties）の ssh.privateKeyFile に設定します。

**リモート操作対象ホストへの公開鍵の配置**

1. **cat** コマンドの出力をリダイレクトし、生成された公開鍵ファイルの内容を、認証に使用される公開鍵ファイル（authorized_keys）に追加します。（例：cat id_rsa.pub >> authorized_keys）
2. **chmod** コマンドを実行して、authorized_keys の属性を 600 に変更します（書き込みおよび読み取り権限を所有者にのみ与えます）。属性が 600 でない場合、部品実行時に認証が失敗することがあります。
   デフォルトでは、authorized_keys の配置場所は、~/.ssh の直下になっています。~/.ssh に関しては、属性を 700 に変更します（書き込み、読み取り、および実行権限を所有者にのみ与えます）。

**shared property の構成**

1. Automation Director アプリケーションにログインします。
2. [管理] > [サービス共有プロパティ]を選択します。
3. 秘密鍵のパスフレーズを開きます（SSH 公開鍵認証の場合）。
4. 値としてパスフレーズを入力します。
   値は、秘密鍵のパスフレーズです（SSH 公開鍵認証の場合）。

## 3.9.3 キーボードインタラクティブ認証

キーボードインタラクティブ認証を使用するには、認証を SSH サーバに設定する必要があります。

1. リモート操作対象ホストに root としてログインします。
2. sshd_config を開きます。
   HP-UX：/opt/ssh/etc/sshd_config
   HP-UX 以外：/etc/ssh/sshd_config
3. 次のようにキーボードインタラクティブ認証を設定します。
   RHEL/CentOS/SUSE、Linux/Oracle Linux、Linux/AIX/HP-UX の場合：

   - ChallengeResponseAuthentication の値を yes に設定します。
     （ChallengeResponseAuthentication の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。）

- UsePAM の値を yes に設定します。（UsePAM の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。）

Solaris10 の場合：
PAMAuthenticationViaKBDInt の値を yes に設定します。
（PAMAuthenticationViaKBDInt の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。）
Solaris11 の場合：
KbdInteractiveAuthentication の値を yes に設定します。
（KbdInteractiveAuthentication の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。）

4. AIX の場合、以下の設定を行います。

---

メモ　AIX OS 以外の場合は、設定を変更する必要はありません。

---

- /etc/pam.conf を開き、以下を追加します。
  - # Authentication ブロックの内側
    sshd auth required /usr/lib/security/pam_aix を追加します。
  - # Account Management ブロックの内側
    sshd account required /usr/lib/security/pam_aix を追加します。
  - # Password Management ブロックの内側
    sshd auth required /usr/lib/security/pam_aix を追加します。
  - # Password Management ブロックの内側
    sshd password required /usr/lib/security/pam_aix を追加します。
  - # Session Management ブロックの内側
    sshd session required /usr/lib/security/pam_aix を追加します。
- /etc/ssh/sshd_config を開いて、次の行を変更します。
  UsePAM = no を UsePAM = yes に変更します。（UsePAM の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。）
- /etc/security/login.cfg を開いて、次の行を変更します。
  auth_type = STD_AUTH を auth_type = PAM_AUTH に変更します。（auth_type の行がコメントアウトされている場合は、コメントアウトのハッシュ記号（#）を削除します。）

5. 次のコマンドを実行して、sshd サービスを再開します。サポートされる各 OS についてコマンド例を示します。
   - RHEL/CentOS/SUSE Linux/Oracle Linux（RHEL 6.4 など）の場合：

```
/etc/rc.d/init.d/sshd restart
```

   - Solaris（Solaris 10 など）の場合：

```
/usr/sbin/svcadm restart ssh
```

   - AIX（AIX 6.1 など）の場合：

```
kill -HUP [Process ID of sshd]
```

- HP-UX（HP-UX 11i V3 など）の場合：

```
/sbin/init.d/secsh stop; /sbin/init.d/secsh start
```

**メモ**　これらのコマンドは、OS のバージョンによって変わる場合があります。詳細については、該当する OS のマニュアルを参照してください。

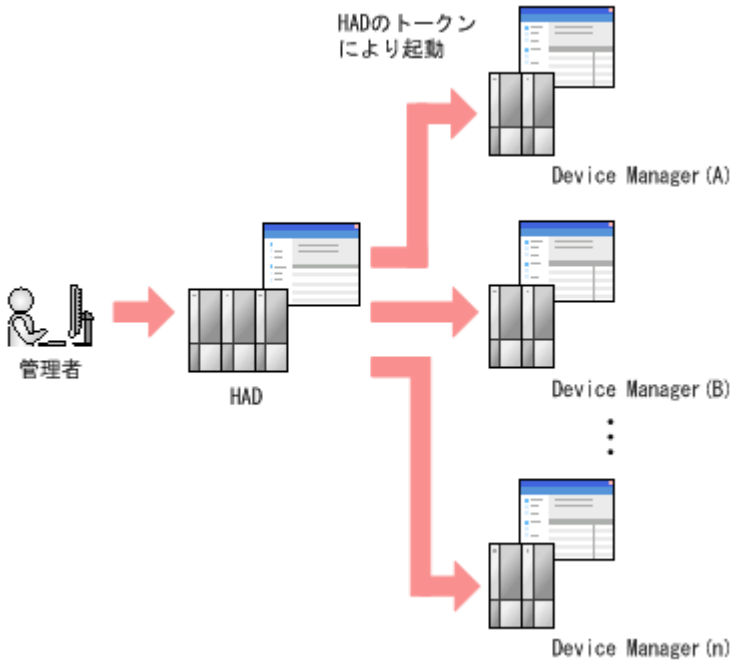
## 3.10 1 つの Automation Director サーバから複数の Device Manager インスタンスを使用する

Automation Director では、1 つの Automation Director サーバから複数の Device Manager インスタンスを使用することができます。この機能は、1 つのトークンだけを（主に）使用する複数の共通コンポーネント認証サーバ間の相互認証を使用することによって可能になります。

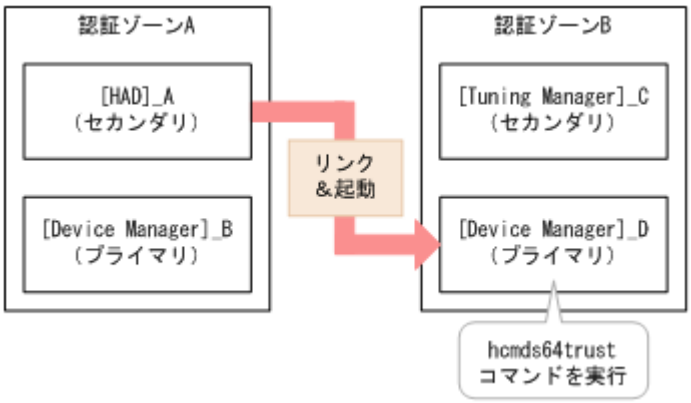
相互認証とは、クライアント／サーバ接続経由でアプリケーショントラフィックを送信する前にクライアントがサーバに身元を証明しなければならず、サーバがクライアントに身元を証明しなければならないセキュリティ機能です。

**メモ**　相互認証は、システムアカウントや共通コンポーネントの内部アカウント（セットアップやその他の内部機能に使用される）などのビルトインアカウントでは行うことができません。

次の図は、1 つの Automation Director サーバから複数の Device Manager インスタンスを使用する例を示しています。




次の図は、2 つの認証ゾーンの相互認証を示しています。図のあとで、このシナリオをセットアップするプロセスについて説明しています。




**相互認証構成プロセス**

1. サーバ ID を変更するには、**hcmds64chgtsid** コマンドを使用します。サーバ ID がデフォルトのホスト名の場合、このステップは不要です。
2. [Device Manager]_D で **hcmds64trust** コマンドを実行し、[Device Manager]_B の接続先情報を登録します。
3. 認証ゾーン A と認証ゾーン B で相互認証を行うユーザーの設定を、次のように選択します。

- 共通ユーザー管理に登録されたユーザーを使用する場合は、認証ゾーン A と認証ゾーン B の共通ユーザー管理に同じユーザーを登録し、権限を付与します。
- 共通ユーザー管理に登録されていない外部認証グループのユーザーを使用する場合は、グループ DN（そのユーザーが含まれる認証サーバ上の外部ユーザーグループ）を認証ゾーン A と認証ゾーン B の共通ユーザー管理に登録し、必要な権限を付与します。

## 3.11 外部認証サーバでのユーザー管理

外部認証サーバに登録したユーザーアカウントを使用して Automation Director にログインできます。外部認証サーバと連携すると、Automation Director のため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。Automation Director は、次の外部認証サーバと連携させることができます。

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

外部認証サーバの設定の方法については、『*Hitachi Command Suite システム構成ガイド*』の「外部認証サーバでのユーザー管理」を参照してください。

# 4

# Automation Director を削除する

この章では、Automation Director を削除する方法について説明します。

# 4.1 Automation Director を削除する（Windows）

Windows 環境で Automation Director を削除するには、次のセクションに記載されている手順に従います。

**前提条件**

- Automation Director のタスクタブの「状態」列が待機中、応答待ち中、実行中、長期実行中、異常検出のいずれかの状態になっているタスクがある場合には、タスクが停止または終了するまで待ちます。
- すべてのサービスダイアログボックスを閉じます。
- Windows のサービスまたは開いているコマンドプロンプトを閉じます。
- サーバ上のセキュリティ監視、ウイルス検出、またはプロセス監視ソフトウェアを無効にします。

**注意**　他の Hitachi Command Suite 製品が同じホストにインストールされている場合は、共有フォルダ（¥Base64¥database）を削除しないでください。このフォルダを削除すると、他の Hitachi Command Suite 製品が停止します。

**操作手順**

1. Windows に管理者としてログオンします。
2. 次のコマンドを実行して、すべてのサービスを停止します。
   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64srv /stop
3. ［Control Panel］を開き、［Programs and Features］または［Add or Remove Programs］を選択します。
4. ［Automation Director］を選択して［Remove］をクリックするか、プログラムを選択し、右クリックして［Uninstall］を選択します。
5. ［Setup］ウィンドウで［Uninstallation］をクリックして、ソフトウェア削除プロセスを開始します。
   削除プロセスによって、*<Automation Director のインストールフォルダ>*¥Automation フォルダが削除されます。

**操作結果**

Automation Director がホストから削除されます。

# 4.2 クラスタ環境で Automation Director を削除する

Automation Director を別のサーバに移行するか、運用を中止する場合には、クラスタ環境のサーバから Automation Director ソフトウェアを削除できます。

**メモ**　Automation Director を削除した場合、プロパティファイル、ログファイル、その他の製品関連のファイルが削除されます。

**操作手順**

1. クラスタ管理ソフトウェアで、Automation Director サービスが登録されているグループをスタンバイノードからアクティブノードに移動します。グループを右クリックして［Move］を選択し、［Select Node］または［Move this service or application to another node］を選択します。

2. 次のコマンドを使用して、Automation Director を含む Hitachi Command Suite サービスが登録されているグループをオフラインにして、フェイルオーバーを無効にします。

   *<共通コンポーネントのインストールフォルダ>*¥ClusterSetup

   ¥hcmds64clustersrvstate /soff /r *<グループ名>*

   r オプションには、Automation Director を含む Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。

3. 次のコマンドを使用して、Automation Director を含む Hitachi Command Suite サービスを削除します。

   **メモ**　サービスを削除する前に、クラスタ管理ソフトウェアから customer script を削除します。

   *<共通コンポーネントのインストールフォルダ>*¥ClusterSetup

   ¥hcmds64clustersrvupdate /sdel /r *<グループ名>*

   r オプションには、Automation Director を含む Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。

   **メモ**

   - r オプションで指定されたグループに登録されているすべての Automation Director と Hitachi Command Suite 製品のサービスが削除されます。ただし、Hitachi File Services Manager のサービスは削除されません。
   - Hitachi Command Suite 製品を引き続き使用する場合は、Automation Director を削除した後で再登録できます。Automation Director サービスを削除しても、問題はありません。サービスリソース名を変更していた場合、サービスが再登録されるときに、すべてのリソース名が再初期化されます。したがって、削除するサービスのリソース名を記録しておき、それらのサービスの再登録後に名前を変更する必要があります。

4. 次のコマンドを使用して、Hitachi Command Suite 製品を停止します。

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

5. アクティブノードから Automation Director を削除します。
6. アクティブノードで、不要になったファイルとフォルダ（クラスタ環境でのインストール時に作成されたファイルとフォルダなど）を削除します。
7. クラスタ管理ソフトウェアで、Automation Director services group をスタンバイノードに移動します。グループを右クリックして［Move］を選択してから、［Select Node］または［Move this service or application to another node］を選択します。
8. スタンバイノードから Automation Director を削除します。
9. クラスタインストールの削除を実行した後、Automation Director フォルダを削除して、他の Hitachi Command Suite サービスを使用しない場合は、スタンバイノードから Base64 フォルダも削除します。
10. 以下のリソースが他のアプリケーションによって使用されていない場合は、クラスタ管理ソフトウェアを使用して、それらをオフラインにしてから削除します。
    - IP アドレス
    - 共有ディスク
11. スタンバイノードで、不要になったファイルとフォルダ（クラスタ環境でのインストール時に作成されたファイルとフォルダなど）を削除します。

12. 他の Hitachi Command Suite 製品を引き続き使用する場合は、次のコマンドを使用して、Hitachi Command Suite サービスをクラスタ管理ソフトウェアグループに登録します。

    *<共通コンポーネントのインストールフォルダ>*¥ClusterSetup¥hcmds64clustersrvupdate /sreg /r *<グループ名>* /sd *<共有ディスクのドライブレター名>* /ap *<クライアントアクセスポイント用リソース名>*

    - /r

      Hitachi Command Suite 製品のサービスを登録するグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster" と指定します。

    - /sd

      クラスタ管理ソフトウェアに登録される共有ディスクのドライブ名を指定します。このオプションに対して複数のドライブ名を指定することはできません。Hitachi Command Suite 製品のデータベースが複数の共有ディスクに分割されている場合は、各共有ディスクについて hcmds64clustersrvupdate コマンドを実行します。

    - /ap

      クラスタ管理ソフトウェアに登録されるクライアントアクセスポイント用リソースの名前を指定します。

13. 他の Hitachi Command Suite 製品を引き続き使用する場合は、次のコマンドを使用して、Hitachi Command Suite サービスが登録されるグループをオンラインにして、フェイルオーバーを有効にします。

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

    r オプションには、Hitachi Command Suite 製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。

14. クラスタ管理ソフトウェアで、Hitachi Command Suite のリソースを含んでいるグループをアクティブノードに移動します。グループを右クリックして［Move］を選択してから、［Select Node］または［Move this service or application to another node］を選択します。

## 4.3 認証データを削除する（Windows）

Automation Director の削除が正常に完了したにもかかわらず KNAE04574-E 警告ダイアログボックスが表示された場合、認証データの削除は失敗しています。データを削除するには、ユーザーアカウントを管理するサーバ（Device Manager がインストールされている接続先のホスト）上で **hcmds64intg** コマンドを実行します。

**hcmds64intg** コマンドを実行して、Windows ホストから認証データを削除するには：

### 操作手順

1. 次のコマンドを実行して、インストールされている Hitachi Command Suite 製品のすべてのサービスを開始します。
   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64srv /start
2. 次のコマンドを実行して、認証データを削除します。
   *<共通コンポーネントのインストールフォルダ>*¥bin¥hcmds64intg /delete /type *<コンポーネント名>* /user *<ユーザー ID>* /pass *<パスワード>*

    - /type

削除するコンポーネントの名前を指定します。Automation を指定できます。

- /user
  Admin（ユーザー管理）権限を持つユーザーのユーザー ID を指定します。user オプションを指定せずにコマンドを実行した場合、ユーザー ID の指定を求められます。
- /pass
  Admin（ユーザー管理）権限を持つユーザーのパスワードを指定します。pass オプションを指定せずにコマンドを実行した場合、パスワードの指定を求められます。

**メモ**　認証データを削除せずに、別の Hitachi Command Suite 製品の GUI ウィンドウを表示した場合、Automation Director サーバを削除した後でも、次のような問題が発生することがあります。

- Automation Director サーバのユーザー管理情報が表示される。
- ダッシュボードにある Automation Director サーバを起動するためのボタンが有効になる。ボタンをクリックすると、リンクエラーが表示される。

## 4.4 Automation Director を削除する（Linux）

Linux 環境で Automation Director を削除するには、次の手順に従います。

**操作手順**

1. root ディレクトリ（/root など）に移動します。
2. 次のコマンドを実行します。
   ＜*Automation Director のインストールディレクトリ*＞/ADUninstall/uninstall.sh

## 4.5 認証データを削除する（Linux）

Automation Director の削除が正常に完了したにもかかわらず KNAE04574-E 警告ダイアログボックスが表示された場合、認証データの削除は失敗しています。データを削除するには、ユーザーアカウントを管理するサーバ（Device Manager を実行する、サーバに接続されたホスト）上で、**hcmds64intg** コマンドを実行します。

**操作手順**

1. 次のコマンドを実行して、インストールされている Hitachi Command Suite 製品のすべてのサービスを開始します。
   ＜*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
2. 次のコマンドを実行して、認証データを削除します。
   ＜*共通コンポーネントのインストールディレクトリ*＞/bin/hcmds64intg -delete -type ＜*コンポーネント名*＞ -user ＜*ユーザー ID*＞ -pass ＜*パスワード*＞

   - -type
     削除するコンポーネントの名前を指定します。Automation を指定できます。
   - -user
     Admin（ユーザー管理）権限を持つユーザーのユーザー ID を指定します。user オプションを指定せずにコマンドを実行した場合、ユーザー ID の指定を求められます。
   - -pass

Admin（ユーザー管理）権限を持つユーザーのパスワードを指定します。pass オプションを指定せずにコマンドを実行した場合、パスワードの指定を求められます。

**メモ**　認証データを削除せずに、別の Hitachi Command Suite 製品の GUI ウィンドウを表示した場合、Automation Director サーバを削除した後でも、次のような問題が発生することがあります。

- Automation Director サーバのユーザー管理情報が表示される。
- ダッシュボードにある Automation Director サーバを起動するためのボタンが有効になる。ボタンをクリックすると、リンクエラーが表示される。

# A

# Automation Director のファイルの場所とポート

この付録には、Automation Director のインストール時に作成されるすべてのフォルダの一覧が含まれています。またポートの一覧も含まれています。

# A.1 Automation Director のファイルの場所

### インストール先フォルダ

次の表は、Automation Director をインストールしたときに作成されるフォルダを示しています。「Windows フォルダの場所」列、または「Linux ディレクトリの場所」列にはデフォルトのパスが示されていますが、インストール時に変更できます。

| Windows フォルダの詳細 | Windows フォルダの場所 |
|---|---|
| インストール先フォルダ | *system-drive*¥Program Files¥HiCommand¥Automation |
| コマンドファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥bin |
| 構成ファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥conf |
| サービステンプレートのフォルダ | *system-drive*¥Program Files¥HiCommand¥Automation¥contents |
| データファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥data |
| ヘルプファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥docroot |
| 事前設定プロパティ定義ファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥extra_presets |
| インストールおよびアンインストール時の一時作業フォルダ | *system-drive*¥Program Files¥HiCommand¥Automation¥inst |
| ライブラリファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥lib |
| ログファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥logs |
| オープンソースソフトウェアのソースファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥ossSource |
| システムファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥system |
| 内部コマンドによって使用される作業用ファイル | *system-drive*¥Program Files¥HiCommand¥Automation¥webapps |
| 作業用フォルダ | *system-drive*¥Program Files¥HiCommand¥Automation¥work |
| 共通コンポーネント | *system-drive*¥Program Files¥HiCommand¥Base64 |

| Linux ディレクトリの詳細 | Linux ディレクトリの場所 |
|---|---|
| インストール先ディレクトリ | /opt/HiCommand/Automation |
| コマンドファイル | /opt/HiCommand/Automation/bin |
| 構成ファイル | /opt/HiCommand/Automation/conf |
| サービステンプレートのディレクトリ | /var/opt/HiCommand/Automation/contents |

| Linux ディレクトリの詳細 | Linux ディレクトリの場所 |
|---|---|
| データファイル | /var/opt/HiCommand/Automation/data |
| ヘルプファイル | /opt/HiCommand/Automation/docroot |
| 事前設定プロパティ定義ファイル | /var/opt/HiCommand/Automation/extra_presets |
| インストールおよびアンインストール時の一時作業ディレクトリ | /opt/HiCommand/Automation/inst |
| ライブラリファイル | /opt/HiCommand/Automation/lib |
| ログファイル | /var/opt/HiCommand/Automation/logs |
| オープンソースソフトウェアのソースファイル | /opt/HiCommand/Automation/ossSource |
| システムファイル | /opt/HiCommand/Automation/system |
| 内部コマンドによって使用される作業用ファイル | /var/opt/HiCommand/Automation/work |
| 共通コンポーネント | /opt/HiCommand/Base64 |

## A.2 ポート設定

Automation Director は、以下のポートを使用します。

**外部接続ポート**

| ポート番号 | ファイアウォール | 説明 |
|---|---|---|
| 22/tcp | Automation Director ←→ 操作対象 | SSH に使用されます。<br>cjstartsv は、このポートを使用します。 |
| 23/tcp | Automation Director ←→ 操作対象 | Telnet に使用されます。<br>cjstartsv は、このポートを使用します。 |
| 445/tcp または udp | Automation Director ←→ 操作対象 | 共有管理に使用されます。<br>cjstartsv は、このポートを使用します。 |
| 135/tcp および 139/tcp | Automation Director ←→ 操作対象 | 共有管理に使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22015/tcp | ブラウザ → Automation Director | HBase 64 Storage Mgmt Web Service へのアクセスに使用。非 SSL（非セキュア）通信では、初期設定が必要です。<br>このポート番号は変更できます。<br>httpsd は、このポートを使用します。 |
| 22016/tcp | ブラウザ → Automation Director | HBase 64 Storage Mgmt Web Service へのアクセスに使用。SSL（セキュア）通信では、設定が必要です。<br>このポート番号は変更できます。 |

| ポート番号 | ファイアウォール | 説明 |
|---|---|---|
| | | httpsd は、このポートを使用します。 |
| 25/tcp | Automation Director → SMTP サーバ | メール送信に使用されます。<br>このポート番号は変更できます。<br>cjstartsv は、このポートを使用します。 |
| 88/tcp または udp | Automation Director → Kerberos サーバ | cjstartsv は、このポートを使用します。 |
| 359/tcp | Automation Director → LDAP ディレクトリサーバ | ldap/tls に使用されます。<br>cjstartsv は、このポートを使用します。 |
| 636/tcp | Automation Director → LDAP ディレクトリサーバ | LDAP に使用されます。<br>このポート番号は変更できます。<br>cjstartsv は、このポートを使用します。 |
| 1812/udp | Automation Director → Radius サーバ | Radius サーバに使用されます。<br>cjstartsv は、このポートを使用します。 |

**内部接続ポート**

| ポート番号 | ファイアウォール | 説明 |
|---|---|---|
| 22017/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22018/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22025/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22026tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22031/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22032/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22035/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22036/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |

| ポート番号 | ファイアウォール | 説明 |
|---|---|---|
| 22037/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22038/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22170/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22171/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22172/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22173/tcp | Automation Director → Automation Director | 共通コンポーネントへのアクセスに使用されます。<br>cjstartsv は、このポートを使用します。 |
| 22220/tcp | Automation Director → Automation Director | 組み込みデータベースで使用されます。 |

**メモ**　このポートは予約済みであり、内部ポート接続にのみ使用されます。

# B

# hcmds64keytool ユーティリティを使用して証明書を管理する

hcmds64keytool ユーティリティは、次のようにさまざまな方法で使用できます。

- 証明書をトラストストアにインポートする。
- トラストストアから証明書を削除する。
- Device Manager サーバの自己署名証明書をエクスポートする。
- トラストストアの一意の名前、トラストストアファイル名、およびパスワードを指定する。
- トラストストアに証明書が正しくインポートされたことを確認する。

詳細については、『*Hitachi Command Suite システム構成ガイド*』を参照してください。

# 索引

## く



## こ



## さ



## し



## せ



## そ



## て



## な



## は



## ふ



## ほ



## ま



## め



## ら

## り



## わ