HITACHI
Inspire the Next

Hitachi IT Operations Analyzer

スターターガイド 機器構成編

解説書

3020-3-N87-10

■対象製品

P-242C-8614 Hitachi IT Operations Analyzer 02-51（適用 OS：Windows Server 2003，Windows Server 2003 R2，Windows Server 2008，Windows Server 2008 R2）

■輸出時の注意

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

■商標類

This software contains materials whose copyrights are reserved by Sun Microsystems, Inc.
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.
This product includes software developed by IAIK of Graz University of Technology.
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 the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).
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 contains materials developed with third party licenses.
All other trademarks, service marks, and company names are properties of their respective owners.

Hitachi IT Operations Analyzer は，RSA Security Inc. の RSA(R) BSAFE(TM) ソフトウェアを搭載しています。

■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。

製品名	表記		
Microsoft(R) Windows Server(R) 2003, Standard Edition	Windows Server 2003	Windows サーバ	Windows
Microsoft(R) Windows Server(R) 2003, Enterprise Edition			
Microsoft(R) Windows Server(R) 2003, Datacenter Edition			

製品名	表記		
Microsoft(R) Windows Server(R) 2003, Standard x64 Edition			
Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition			
Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition			
Microsoft(R) Windows Server(R) 2003 R2, Standard Edition	Windows Server 2003 R2		
Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition			
Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition			
Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition			
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition			
Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition			
Microsoft(R) Windows Server(R) 2008 Standard 32-bit	Windows Server 2008		
Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit			
Microsoft(R) Windows Server(R) 2008 Datacenter 32-bit			
Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) 32-bit			
Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) 32-bit			
Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) 32-bit			
Microsoft(R) Windows Server(R) 2008 Standard			
Microsoft(R) Windows Server(R) 2008 Enterprise			
Microsoft(R) Windows Server(R) 2008 Datacenter			
Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM)			
Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM)			
Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM)			

製品名	表記		
Microsoft(R) Windows Server(R)2008 R2 Standard	Windows Server 2008 R2		
Microsoft(R) Windows Server(R) 2008 R2 Enterprise			
Microsoft(R) Windows Server(R) 2008 R2 Datacenter			
Microsoft(R) Windows Server(R) 2008 R2 Standard without Hyper-V™			
Microsoft(R) Windows Server(R) 2008 R2 Enterprise Edition without Hyper-V™			
Microsoft(R) Windows Server(R) 2008 R2 Datacenter Edition without Hyper-V™			
Internet Explorer(R)	Internet Explorer		
Microsoft(R) Internet Explorer(R)			
Microsoft(R) Hyper-V™	Hyper-V		

■発行

2010 年 12 月　3020-3-N87-10

■著作権

変更内容

変更内容（3020-3-N87-10） Hitachi IT Operations Analyzer　02-51

追加・変更内容	変更個所
環境の準備に Dell サーバを追加した。	表 1-1
Dell サーバの準備に関する記述を追加した。	8 章

単なる誤字・脱字などはお断りなく訂正しました。

はじめに

このマニュアルは，「Hitachi IT Operations Analyzer スターターガイド」の補助資料です。管理対象のネットワーク構成要素の，インストール前のセットアップ作業について説明しています。また，このマニュアルでは，次に示す準備作業についても説明しています。

- Windows サーバ上の Hyper-V と WMI
- Linux/Solaris サーバ上の SSH
- VMware ESX サーバ
- IP スイッチの SNMP
- Hitachi AMS/WMS/SMS
- FC スイッチとストレージの SMI-S

■対象読者

- Hitachi IT Operations Analyzer を利用してサーバ，ストレージなど各種機器の情報を収集・管理する管理者の方
- Hitachi IT Operations Analyzer を使用する環境を構築するシステム管理者の方

また，このマニュアルは，次に示す知識があることを前提としています。

- Windows の操作に関する基本的な知識
- ネットワークに関する基本的な知識

■このマニュアルの構成

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

セットアップ手順，使用環境の設定，インストール中に必要となる情報の収集について説明しています。

第２章　Windows での Hyper-V と WMI の準備

Hyper-V と WMI 環境の準備について説明しています。

第３章　Linux/Solaris での SSH の準備

Linux と Solaris サーバの構成方法について説明しています。

第４章　VMware ESX サーバの準備

ESX サーバをどのようにして準備するかについて説明しています。

第５章　IP スイッチのための SNMP の準備

IP スイッチのための SNMP をどのように構成するかについて説明しています。

第６章　Hitachi ストレージの準備

Hitachi AMS/WMS/SMS ストレージ機器に接続するために収集しなければならない情報と，Hitachi ストレージを SMI-S 用にどのように構成すればよいかについて説明しています。

第 7 章　FC スイッチとストレージのための SMI-S の準備

SMI-S，および FC スイッチやストレージをセットアップするために必要なタスクについて説明しています。

第 8 章　Dell サーバの準備

Dell サーバをセットアップするのに必要な項目について説明しています。

付録 A　このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報について説明しています。

■このマニュアルで使用している記号

このマニュアルで使用する記号を次に示します。

記号	意味
斜体文字	ユーザーやシステムの設定値の代用となる可変値を示します。バージョン情報の記載個所で，斜体文字で *x* と記載してある場合は，すべてのバージョンを意味します。例を次に示します。 • *ソースファイル*と *ターゲットファイル*をコピーしてください。 • カーネルバージョン 2.6.*x* 注意：「<」，「>」も可変値を表す場合があります。
[ ]	メニュータイトル，メニュー項目，ボタン，キーなどの名称を示します。
< >	ユーザーやシステムの設定値の代用となる可変値を示します。 例：# pairdisplay -g <group> 注意：斜体文字も可変値を表す場合があります。

目次

1 概要

Hitachi IT Operations Analyzer をインストールする前，または探索ウィザードを使用する前に，管理用サーバや，管理対象のサーバ，ストレージなどの環境の確認と準備が必要です。この章では，セットアップ手順に加えて，使用環境の設定や，インストール中に必要となる情報の収集についても説明します。

1.1 環境の準備

1.1 環境の準備

Hitachi IT Operations Analyzer を使用する環境および管理目的に応じた必須作業，推奨作業，および任意の作業を表 1-1 ～ 3 に示します。

各作業の詳細を説明している章または節への参照文を記載しています。

表 1-1 環境の準備（必須作業）

作業		詳細	参照先
Hitachi IT Operations Analyzer がインストールされている管理用サーバで，WMI 用の DCOM の設定を確認する。		DCOM のリモート実行の不許可によって WMI リモート接続エラーが発生しないようにしてください。	「2. Windows での Hyper-V と WMI の準備」
使用している管理対象機器をセットアップする。	IP スイッチ	管理対象はサーバ，ストレージ，スイッチです。 IP スイッチの管理に SNMP を使用しています。 • IP アドレスの確認 • SNMP のコミュニティ名の取得 • SNMP トラップの有効化	「5. IP スイッチのための SNMP の準備」
	Hitachi 9500V および Hitachi USP VM	デバイスマネージャの SMI-S プロバイダを通して Hitachi 9500V および Hitachi USP VM を管理します。Hitachi 9500V の場合，パフォーマンスは管理されません。Hitachi 9500V の場合はデバイスマネージャ 5.9 かそれ以降，Hitachi USP VM の場合はデバイスマネージャ 6.2 かそれ以降をインストールして，SMI-S を有効化します。	「6.2 Hitachi 9500V および Hitachi USP VM ストレージ接続情報の取得」

作業		詳細	参照先
	Dell サーバ	標準添付される Dell Chassis plug-in を使用することで，Dell サーバの特性情報を収集できます。”Dell Chassis(Windows)”は Windows の Plug-in として，”Dell Chassis(Linux)”は Linux の Plug-in としてインストールされます。Hitachi IT Operations Analyzer で監視される Dell サーバに関するシステム要件については，次の項目を確認してください。 • 監視される Dell サーバにおいて Dell OpenManage Server Administrator(OMSA) バージョン 6.1.0 または 6.2.0 が実行されていること • 監視される Dell サーバにおいて SNMP Agent がインストールされて，実行されていること • ”Dell Chassis(Windows)”は Windows Server 上で，DSM SA Data Manager service が実行されていること • ”Dell Chassis(Linux)”は Red Hat Enterprise Linux Server 上で，dsm_sa_datamgrd または dsm_sa_datamgr32d プロセスが実行されていること Dell サーバに関する Linux と Windows の OS の要件は Linux サーバと Windows サーバの環境の準備について記載されている個所を参照してください。	「8. Dell サーバの準備」

作業		詳細	参照先
	その他のストレージや FC スイッチ	その他のストレージや FC スイッチの探索・管理に SMI-S を使用します。SMI-S プロバイダをインストールして，SMI-S プロバイダの次に示すものを確認してください。 • IP アドレス 組み込みモデル：FC スイッチと同じ IP アドレスを使用してください。 プロキシモデル：スイッチ用の SMI-S サーバの IP アドレスを使用してください。 • ユーザー ID とパスワード • ポート番号 • ネームスペース • SSL の状態 以下の条件の場合，Credential 入力において，「SSL:http」指定をすることを推奨します。 • NetApp FAS シリーズ • Linux 版 SMI-S Agent で管理。	「7. FC スイッチとストレージのための SMI-S の準備」

表 1-2 環境の準備（推奨作業）

作業		詳細	参照先
管理対象を確認する。	Windows サーバ※	Windows サーバの管理に WMI を使用します。また，Hyper-V 仮想マシンを管理する場合は，仮想マシンに Integration Service をインストールしてください。	「2. Windows での Hyper-V と WMI の準備」
	Linux/Solaris サーバ	Linux/Solaris サーバの探索に SSH を使用します。また，証明書認証でなくパスワード認証を使用します。管理するためには，次について確認してください。 • SSH サービスがインストールされ，稼働しているか • SSH2 接続が有効か • パスワード認証が許可されているか	「3. Linux/Solaris での SSH の準備」

作業		詳細	参照先
	VMware ESX サーバ※	VMware Tools がインストールされていないと，仮想マシン上の Windows や Linux サーバを正確に管理できません。バージョンが次のとおりか確認してください。 • VMware ESX 3.0.1　またはそれ以降 • VMware ESX 3 • VMware ESX 3.5 • VMware ESX 3i • VMware ESX 3.5i • VMware ESX 4.0 • VMware ESX 4i 同様に，仮想マシンにも VMware Tools をインストールしてください。	「4.　VMware ESX サーバの準備」
	Hitachi AMS/ WMS/SMS	アカウント認証かパスワード保護が有効になっているか確認してください。有効になっている場合，Hitachi IT Operations Analyzer ではユーザー ID およびパスワードが必要となります。	「6.　Hitachi ストレージ装置の準備」

注※：ユーザーによるセットアップが必要な項目です。

表 1-3　環境の準備（任意の作業）

作業		詳細	参照先
管理対象を確認する。	Windows サーバ※	Windows サーバの管理に WMI を使用します。Windows Server 2003 の場合，FC HBA（Fiber Channel Host Bus Adapter）データを WMI を使って取得するためには，fcinfo をインストールする必要があります。	「2.　Windows での Hyper-V と WMI の準備」
	IP スイッチ	SNMP トラップの送信を有効にします。IP スイッチで SNMP トラップを受信できます。Hitachi IT Operations Analyzer はポーリングの使用によってトラップなしでも IP スイッチを管理できるため，この作業はオプションです。	「5.　IP スイッチ用のための SNMP の準備」

注※：ユーザーによるセットアップが必要な項目です。

2 Windows での Hyper-V と WMI の準備

Hitachi IT Operations Analyzer では，Hyper-V 仮想マシン上にインストールされた Windows サーバの管理に WMI を使用しています。WMI を使ってリモートアクセスする場合，Windows サーバと管理用サーバ上で DCOM が許可されている必要があります。DCOM が許可されていないと，Windows サーバの探索や管理ができません。この章では，Hyper-V と WMI 環境の準備について説明します。

2.1 Hyper-V の準備

Hyper-V 仮想マシン上にインストールされた Windows サーバの管理を計画する場合，仮想マシンの OS に Integration Service をインストールする必要があります。Integration Service がインストールされていないと，Hitachi IT Operations Analyzer では仮想マシンの状態もホストマシンとゲスト OS の関連も正しく表示されません。

注意事項

Hyper-V ホストマシンのセットアップは，Windows サーバの準備と類似しています。2.2 節を参照してください。

2.2 Windows サーバ用の WMI の準備

Hitachi IT Operations Analyzer は，WMI を利用して Windows サーバの探索と管理を実行します。ここでは，WMI へのリモートアクセスの許可に関連する作業と，FC HBA を使用する Windows Server 2003/2003 R2 の構成について説明します。

注意事項

Windows サーバおよび Microsoft Hyper-V 機器では，FC 接続，iSCSI 接続，およびローカル接続でのハードディスクに関するパフォーマンス情報を取得できます。CD-ROM や USB メモリのパフォーマンス情報は取得できません。パフォーマンス情報を取得できない場合は，モニタリング画面の［パフォーマンス］タブにある［監視項目］のアイコンは不明となります。

2.2.1 管理用サーバの準備

Windows コンピュータやストレージサーバを管理するには，管理用サーバ上で DCOM を許可している必要があります。詳細については，「2.2.2(3)　DCOM のリモート実行の許可」を参照してください。

2.2.2 Windows コンピュータと Windows サーバの準備

Windows サーバに接続するために必要な情報を次の表に示します。

表 2-1　Windows サーバに接続するために必要な情報

項目	詳細
IP アドレス	管理対象の Windows サーバの IP アドレスを指定する
ユーザー名	管理対象の Windows サーバに対する，Administrator 権限を持つユーザーアカウントを指定する
ドメイン名	［ユーザー名］で指定したユーザーアカウントがドメインユーザーである場合は，ユーザーのドメイン名を指定する
パスワード	［ユーザー名］に対応するパスワードを入力する

Windows サーバで DCOM を有効にして，ファイアウォールを通す通信許可を有効にしてください。FC HBA 情報を取得する Windows Server 2003，または Windows Server 2003 R2 を使用している場合，ファイバーチャネル情報（fcinfo）ツールをインストールしてください。Windows Server 2008 では追加設定が必要です。

(1) ファイバーチャネル情報（fcinfo）ツールのインストール

fcinfo ツールは，HBA を使用するときに必要です。HBA は，管理したいサーバがファイ

バーチャネル SAN ディスク機器へ接続する際に使用されます。fcinfo ツールは，Windows 上のファイバーチャネルの HBA の API をサポートし，WMI 対応機能を提供します。次に示す Microsoft のダウンロードセンターの Web サイトを参照してください。

http://www.microsoft.com/downloads/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

(2) Windows ファイアウォールへの WMI の例外登録

Windows コマンドプロンプトまたはグループポリシーエディタを使って権限を変更できます。Windows Server 2003 での手順を次に示します。Windows Server 2008 での手順については，「(4) Windows Server 2008 の構築設定の適用」を参照してください。

● Windows コマンドプロンプトを使う方法

1. サーバにログインしたあと，スタートメニューから［ファイル名を指定して実行］を選択する。
2. 「cmd」と入力し，［OK］ボタンをクリックする。
3. コマンドプロンプトで次のように指定し，［Enter］をクリックする。
   netsh firewall set service RemoteAdmin enable

● グループポリシーエディタを使う方法

1. サーバにログインしたあと，スタートメニューから［ファイル名を指定して実行］を選択する。
2. 「gpedit.msc」と入力して［OK］ボタンをクリックし，グループポリシーを起動する。
3. ［ローカル コンピュータ ポリシー］－［管理用テンプレート］フォルダを展開する。
4. ［ネットワーク］－［ネットワーク接続］－［Windows ファイアウォール］フォルダを展開し，［ドメインプロファイル］を選択する。
5. 設定リストの中から「Windows ファイアウォール：リモート デスクトップの例外を許可する」を右クリックし，「プロパティ」を選択する。
6. ［有効］を選択し，［OK］ボタンをクリックする。

! 注意事項

詳細については，次に示す Microsoft のデベロッパー センターの Web サイトを参照してください。
http://msdn2.microsoft.com/en-us/library/aa389286(VS.85).aspx

(3) DCOM のリモート実行の許可

Windows コマンドプロンプトで dcomcnfg.exe を実行すると，［コンポーネント サービス］画面を起動して DCOM の状態を確認できます。

1. サーバにログインしたあと，スタートメニューから［ファイル名を指定して実行］を

選ぶ。
2.「dcomcnfg.exe」と入力して［OK］ボタンをクリックし，［コンポーネント サービス］画面を起動する。
3.［コンポーネント サービス］ツリー下の［コンピュータ］－［マイ コンピュータ］を右クリックし，「プロパティ」をクリックする。
4.［規定のプロパティ］タブをクリックする。
5.「このコンピュータ上で分散 COM を有効にする」チェックボックスにチェックを入れて，「COM セキュリティ」タブを選択する。
6.「起動とアクティブ化のアクセス許可」の［制限の編集］ボタンをクリックし，［起動許可］ダイアログボックスを開く。「グループ名またはユーザー名」にユーザー名またはグループ名が表示されていない場合，次の手順を実行する。
1.［追加］ボタンをクリックする。
2.「ユーザー，コンピュータ または グループの選択」ダイアログボックスで，「選択するオブジェクト名を入力してください」にユーザー名とグループを追加し，［OK］ボタンをクリックする。
3.［起動許可］ダイアログボックスで「グループ名またはユーザー名」欄のユーザーまたはグループをクリックします。「ユーザーのアクセス権限」欄の「リモートからの起動」の「許可」のチェックボックスにチェックを入れて，［OK］ボタンをクリックする。

（4） Windows Server 2008 の構築設定の適用

Windows Server 2008 を使用する場合，次のどれかを設定する必要があります。

- ビルトイン管理者のアカウントを使用する
- ドメインユーザーアカウントを使用する
- 管理対象コンピュータの個々のレジストリキーを構築して，ローカル管理者アカウントを使って WMI リモート接続を許可する

ここでは，WMI リモート接続でのローカル管理者アカウントの許可について説明します。

（a） WMI リモート接続でのローカル管理者アカウントの許可

管理対象のコンピュータ上のレジストリに，LocalAccountTokenFilterPolicy キーを登録して「1」を設定します。その後，WMI リモート接続でのローカル管理者権限を防ぐユーザーアカウント制御（UAC）によるフィルタリングを無効化します。ローカル管理者アカウントでは Windows Server 2003 と Windows Server 2008 のどちらも管理できます。レジストリを編集しないと，致命的なエラーが発生してシステム全体に深刻な影響を及ぼすおそれがあります。レジストリを編集する前に，バックアップを保存することをお勧めします。

注意事項

詳細については，次に示す URL を参照してください。ユーザーアカウント制御と Windows Vista でのリモート制限について説明しています。
http://support.microsoft.com/kb/951016/en-us

レジストリでの編集には，次の 2 とおりの方法があります。

- レジストリエディタ
- Windows の reg コマンド

それぞれの手順を次に示します。

● レジストリエディタの使用手順

1. スタートメニューから［ファイル名を指定して実行］を選択する。
2. コマンドプロンプトで「regedit」と入力し，［OK］ボタンをクリックする。
   レジストリエディタが表示されます。
3. 次に示すレジストリサブキーへ移動する。
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System
4. LocalAccountTokenFilterPolicy キーがない場合，次の手順で追加する。
   1.［編集］－［新規］－［DWORD 値］を選択する。
   2.「LocalAccountTokenFilterPolicy」と入力し，［Enter］ボタンをクリックする。
5. LocalAccountTokenFilterPolicy キーの値が 1 でない場合，次の手順で 1 へ変更する。
   1.LocalAccountTokenFilterPolicy キーを右クリックし，「修正」を選択する。
   2. ダイアログボックスで「1」を入力し，［OK］ボタンをクリックする。
6. レジストリエディタを閉じる。

● reg コマンドの使用手順

1. スタートメニューから［ファイル名を指定して実行］を選択する。
2. コマンドプロンプトで次のように入力する。
   reg add HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0x1 /f
3. ［OK］ボタンをクリックする。

3 Linux/Solaris での SSH の準備

Hitachi IT Operations Analyzer では，Linux サーバと Solaris サーバの探索に SSH を使用しています。管理には，証明書認証ではなくパスワード認証を使用しています。この章では，Linux サーバと Solaris サーバの設定方法について説明します。

3.1 ログイン方法に応じた接続設定

Linux サーバや Solaris サーバから情報を取得する SSH を使用する際のログイン方法には，次の種類があります。

- SSH 使用時に root ユーザーで直接ログインする
- SSH 使用時に通常ユーザーでログインしたあと，次のどちらかを実行する
  - root 権限の su コマンド
  - root 権限の sudo/pfexec コマンド

これらの方法でログインするには，確実な接続設定が必要です。以降の項では，設定方法について説明します。

注意事項

Linux サーバや Solaris サーバでは，マウントポイントに関するパフォーマンス情報が read/write 権限で取得できます。read 権限では，Windows パーティションと CD-ROM ドライブに関するパフォーマンス情報は取得できません。パフォーマンス情報が取得できない場合，モニタリング画面の中の［パフォーマンス］タブにある［監視項目］にあるアイコンは不明となります。

3.1.1 root ユーザーでの接続設定

次に示す設定が必要です。

- SSH2 を使った接続の許可
- SSH のパスワード認証の許可
- SSH を使った root ログインの許可

表 3-1 Linux/Solaris サーバの接続設定（root ユーザー）

設定	詳細
IP アドレス	管理対象の Linux/Solaris サーバの IP アドレスを指定してください
ポート番号	管理対象の Linux/Solaris サーバの SSH ポート番号を指定してください
ユーザー名	root を指定してください
パスワード	root パスワードを指定してください
root パスワード	空白にしてください

3.1.2 通常ユーザーの接続設定（ su コマンド）

次に示す設定が必要です。

- SSH2 を使った接続の許可
- SSH のパスワード認証の許可

表 3-2 Linux/Solaris サーバの接続設定（su コマンド）

設定	詳細
IP アドレス	管理対象の Linux/Solaris サーバの IP アドレスを指定してください
ポート番号	管理対象の Linux/Solaris サーバの SSH ポート番号を指定してください
ユーザー名	ログイン時のユーザー ID を指定してください
パスワード	ユーザー ID に対応するパスワードを指定してください
root パスワード	root パスワードを指定してください

3.1.3 通常ユーザーの接続設定（ sudo コマンド）

次に示す設定が必要です。

- SSH2 を使った接続の許可
- SSH のパスワード認証の許可
- 次に示す定義を sudo/pfexec コマンドの設定に追加します。定義内の「*user*」はユーザー ID,「*hostname*」は Linux サーバ名を示します。また,「/bin/cat」は SUSE Linux だけに必要です。

```
user hostname =NOPASSWD: /usr/sbin/dmidecode
user hostname =NOPASSWD: /usr/sbin/smartctl
user hostname =NOPASSWD: /bin/cat
```

- Solaris ではプロファイルに次の定義を追加します。「*Profile*」にはプロファイル名が入ります。

```
Profile:suser:cmd:::/sbin/ifconfig:euid=0
Profile:suser:cmd:::/usr/sbin/prtvtoc:euid=0
Profile:suser:cmd:::/usr/sbin/luxadm:euid=0
Profile:suser:cmd:::/usr/sbin/iscsiadm:euid=0
```

表 3-3 Linux/Solaris サーバの接続設定（sudo コマンド）

設定	詳細
IP アドレス	管理対象の Linux/Solaris サーバの IP アドレスを指定してください
ポート番号	管理対象の Linux/Solaris サーバの SSH ポート番号を指定してください
ユーザー名	ログイン時のユーザー ID を指定してください
パスワード	ユーザー ID に対応するパスワードを指定してください
root パスワード	空白にしてください

注意事項

SSH を使用する場合のセキュリティ項目を次に示します。

- 構築時に root ログインを許可することは容易ですが，root パスワードが漏洩してサーバ設定が偽造されるおそれがあります。この方法は，権限のないアクセスを防止できる環境の場合に採用してください。
- root ログインを抑止して，ユーザーに su root を許可することは，ユーザー ID やパスワードが漏洩しなければ，root ログインを許可するより安全です。
- SSH1 プロトコルは SSH2 プロトコルよりデータを傍受される危険が高いため，SSH2 プロトコルの使用をお勧めします。
- パスワード認証が許可されていると，パブリックキー認証（public key authentication）だけが許可されている場合よりも危険度が高くなります。Hitachi IT Operations Analyzer はパブリックキー認証を操作できないため，パスワード認証にはポート 22 以外のポートを使う方が安全です。

3.2 SSH サーバのセキュリティ設定の適用

この節では次に示す項目の概要を説明しています。

- SSH2 接続の許可
- SSH のパスワード認証の許可
- SSH 使用時の root ログインの許可
- Sudo コマンド設定の定義追加（Linux）
- pfexec コマンドのプロファイルの追加（Solaris）

3.2.1 始める前に

- SSH サービス（sshd デーモン）がインストールされていて，稼働していることを確認してください。
- 異なる SSH ソフトウェアを使用している場合は，そのソフトウェアのマニュアルを参照して同様の設定を実施してください。Linux は OpenSSH を同梱しています。
- 管理対象のサーバにログインできる環境を用意し，システムシェルを操作してください。
- サーバコンソールからログインするか，または SSH か telnet を使ってリモートでログインしてください。再接続の失敗を防ぐために，ローカルコンソールからログインすることをお勧めします（構成の設定誤りが存在する場合）。
- root パスワードを用意してください。
- root ユーザーや通常ユーザーでログインしたあと，su root コマンドを実行して root 権限を取得してください。

(1) SSH2 接続の許可

1. エディタで /etc/ssh/sshd_config を開く。
2. sshd_config 中で Protocol キーワードを使っているファイルを検索する。
   - 記述がない，または Protocol がコメントアウトされている場合は，SSH1 および SSH2 は利用できます。変更の必要はありません。
   - 「Protocol 1」がある場合は SSH1 だけが使用できます。「Protocol 1」を「Protocol 1, 2」へ変更してください。
   - 「Protocol 2」がある場合は SSH2 だけが使用できます。変更の必要はありません。
   - 「Protocol 1, 2」または「Protocol 2, 1」がある場合は，SSH1 および SSH2 を使用できます。変更の必要はありません。
3. ファイルを保存してエディタを閉じる。設定誤りがないことを確認するには，使用しているサーバに応じて，次のコマンドを実行する。

   ```
   Linuxの場合: /usr/sbin/sshd -t
   Solarisの場合: /usr/lib/ssh/sshd -t
   ```

   - エラーがなければ何も表示されません。
   - エラーがある場合はエラーメッセージが出力されます。

不正なプロトコル（Protocol 2, 3）を設定した場合の例を次に示します。

```
[root@linuxhost ssh]# /usr/sbin/sshd -t
ignoring bad proto spec: '3'.
```

4. SSH サービスを再起動するために，サーバ別に次のどれかのコマンドを実行する。
   - Linux の場合：service sshd restart
   - Solaris 9 の場合：/etc/init.d/sshd restart
   - Solaris 10 の場合：svcadm restart ssh
5.「Stopping」「Starting」に「OK」が表示されたら，サービスは正常に稼働している。例えば，「Stopping sshd: [OK]」のように表示されます。

(2) SSH パスワード認証の許可

注意事項

/etc/ssh/sshd_config の編集や SSH サービスの再起動に関する情報については，「(1) SSH2 接続の許可」を参照してください。

/etc/ssh/sshd_config 中でキーワード「PasswordAuthentication」を指定してファイルを検索してください。

- PasswordAuthentication の記述がない，またはコメントアウトされている場合は，パスワード認証は有効です。変更の必要はありません。
- 「PasswordAuthentication no」がある場合，パスワード認証は抑止されています（パブリックキー認証だけが有効）。「PasswordAuthentication yes」へ変更してください。
- 「PasswordAuthentication yes」がある場合，パスワード認証は有効です。変更の必要はありません。

(3) SSH 使用時の root ログインの許可

注意事項

/etc/ssh/sshd_config の編集や SSH サービスの再起動に関する情報については，「(1) SSH2 接続の許可」を参照してください。

/etc/ssh/sshd_config 中で，キーワード「PermitRootLogin」を指定してファイルを検索します。

- 「PermitRootLogin」がないかコメントアウトされている場合は，デフォルトでは root ログインは有効です。変更の必要はありません。
- 「PermitRootLogin no」がある場合は root ログインは抑止されています（通常ユーザーだけが有効）。「PermitRootLogin yes」へ変更してください。
- 「PermitRootLogin yes」がある場合は root ログインは有効です。変更の必要はありま

せん。

(4) sudo コマンド設定の定義（Linux）

sudo の設定は /etc/sudoers ファイルに記載します。ファイルの編集は，排他制御と文法チェックの機能を備えている visudo コマンドで実行してください。

1. visudo コマンドを実行する。
   正常に起動するとエディタが開きます。

注意事項

visudo コマンドが異なる場所で同時に実行された場合，次のエラーメッセージが表示され，エディタは起動しません。

[root@linuxhost ssh]# visudo
visudo: sudoers file busy, try again later

コマンドを同時実行していないのにこのエラーメッセージが表示された場合，前回のコマンド実行で接続が終了しているのに，プロセスがまだ実行中の可能性があります。この場合は，visudo プロセスを強制終了してください。

2. ユーザーが次の 3 コマンドをパスワードなしで実行できるように，行を追加する。ただし，「/bin/cat」は SUSE Linux の場合だけ必要なので注意する。

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
```

例えば，接続に使用されるユーザー名が「sshconn」，サーバ名が「linuxhost」の場合，次のように記述してください。

```
sshconn linuxhost=NOPASSWD: /usr/sbin/dmidecode
sshconn linuxhost=NOPASSWD: /usr/sbin/smartctl
sshconn linuxhost=NOPASSWD: /bin/cat
```

3. ファイルを保存し，エディタを閉じる。
   文法エラーがある場合，エラーメッセージが表示されて保存されません。
   - 「e」を入力するとエディタは再起動します。修正して，保存してください。
   - 「x」を入力すると変更は無視され，visudo コマンドを実行する前の状態に復帰できます。
   - 「Q」を入力すると，誤りがあっても強制的に変更内容が保存されます。
     例えば，「NOPASSWD」の入力を誤ると次のエラーメッセージが表示されます。
     Warning: undeclared Cmnd_Alias `NOPASSWD referenced near line 92
     >>> sudoers file: syntax error? line 91 <<<
     What now?

注意事項

変更内容を強制保存すると，予期しない結果になる場合があるので注意してください。実行結果に自信がない場合は，変更内容の強制保存を実施しないでください。

(5) pfexec コマンドのプロファイルの追加（Solaris）

pfexec を使用して root 権限を付与するには，/etc/security/prof_attr と /etc/security/exec_attr にプロファイルを追加し，プロファイルにユーザーを割り当ててください。

1. 「vi /etc/security/prof_attr」を実行する。
   - 正常に起動した場合，エディタが開きます。
   - コマンドが同時実行されていないのにエラーメッセージが表示された場合，以前コマンドを実行した際のプロセスの残留によって接続が縮小（curtail）していると考えられます。この場合は vi プロセスを強制終了してください。
2. プロファイルを登録する。
   例えば，プロファイル名が「HITOA」に設定された場合，「HITOA::::」のように表示されます。
3. ファイルを保存し，エディタを終了する。
4. 「vi /etc/security/exec_attr」を実行する。
   正常に起動するとエディタが開きます。
5. コマンドをパスワードなしで実行できるように，次の 4 行を追加する。

   ```
   /sbin/ifconfig
   /usr/sbin/prtvtoc
   /usr/sbin/luxadm
   /usr/sbin/iscsiadm
   ```

   例えば，プロファイル名が「HITOA」に設定された場合，次のように記述してください。

   ```
   HITOA:suser:cmd:::/sbin/ifconfig:euid=0
   HITOA:suser:cmd:::/usr/sbin/prtvtoc:euid=0
   HITOA:suser:cmd:::/usr/sbin/luxadm:euid=0
   HITOA:suser:cmd:::/usr/sbin/iscsiadm:euid=0
   ```

6. ファイルを保存し，エディタを終了する。
7. ユーザーに対してプロファイルを割り当てる。
   例えば，ユーザー名が「sshconn」に設定された場合，次に示すようにコマンドを実行してください。

   ```
   usermod -P HITOA sshconn
   ```

4 VMware ESX サーバの準備

Hitachi IT Operations Analyzer は，VMware Tools がインストールされていないと，仮想マシン上の Windows サーバ，または Linux サーバを正しく管理できません。この章では，VMware ESX サーバをどのようにして準備するかについて説明します。

4.1 ESX サーバ接続情報の取得

管理したいサーバが仮想マシンの場合，VMware ESX サーバが稼働しているかどうか確認してください。次の表で，ESX サーバに接続するときに必要な情報について説明します。探索処理では，追加の認証情報は必要ありません。探索処理の場合，ユーザー名とパスワードの情報だけが必要です。

表 4-1 VMware ESX サーバに接続するために必要な情報

項目	詳細
IP アドレス	ESX サーバの IP アドレスを使用してください
ポート番号	ESX サーバで使用するポート番号を指定してください
プロトコル	ESX サーバの構成に基づいて，http または https を使用してください
ユーザー名	ESX サーバの管理者ユーザー名を使用してください
パスワード	ESX サーバのパスワードを使用してください

4.2 仮想マシンへの VMware Tools のインストール

Windows サーバまたは Linux サーバの仮想マシンを管理しようとする場合，ESX サーバの情報を取得するために，各仮想マシンのゲスト OS に，VMware Tools をインストールする必要があります。

VMware Tools がインストールされていない場合，仮想マシンの状態や，ホストマシンとゲスト OS の間の関係を正しく表示できません。

ゲスト OS は，個別の機器として管理されますのでご注意ください。

VMware Tools のインストールについては，ESX サーバの「Basic System Administration」というマニュアルを参照してください。次に示すサイトで参照できます。

http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_admin_guide.pdf

5 IP スイッチのための SNMP の準備

Hitachi IT Operations Analyzer は，IP スイッチから SNMP トラップを受信できます。この章では，IP スイッチのための SNMP をどのように構成するかについて説明します。

5.1 IP スイッチの概要

Hitachi IT Operations Analyzer は，次の条件を満たしていれば，ご使用の環境内の IP スイッチを管理できます。

- SNMP バージョン 1 がインストールされて，稼働している。
- MIB-II が読める状態になっている。
- ブリッジ MIB が読める状態になっている。

IP スイッチに接続するためには，次の情報が必要です。

表 5-1 IP スイッチに接続するために必要な情報

項目	詳細
IP アドレス	SNMP IP スイッチ機器の IP アドレスです
ポート番号	SNMP IP スイッチが通信を待機するポートです（ポート 161）
コミュニティ名	SNMP IP スイッチのために使用するコミュニティ名です

次の条件を満たしていれば，データをさらに正確に収集できます。

- Virtual Bridge MIB が読める状態になっている。
- Cisco VTP MIB が読める状態になっている。
- Extreme FDB MIB が読める状態になっている。
- SNMPv2c がインストールされて，稼働している。
- Interfaces Group MIB が読める状態になっている。

注意事項

IP スイッチを管理する際に必要な事項について確認してください。
IP スイッチが次の両方の状態にあることを確認してください。

- RFC1213：SNMP v1 MIB-II がサポートされている
- RFC1493：SNMP v1 Bridge MIB がサポートされている

RCA 機能とトポロジー閲覧機能を確実に使用するために，次のものがサポートされていることを確認してください。

- RFC2674（Virtual Bridge MIB）または RFC4363（Virtual Bridge MIB）
- Cisco VTP MIB

Extreme Network 社 (R) の IP スイッチを管理している場合は，ExtremeXOS（バージョン 12.1.2 以上）を使用してください。

5.2 SNMP トラップの有効化

Hitachi IT Operations Analyzer は，IP スイッチのコミュニケーションリンクに関する SNMP トラップ（リンクダウンまたはリンクアップ）を受信できます。トラップ受信に関する追加の設定をする場合は，次に示す設定を適用してください。

- 「Send trap」を有効にしてください。バージョンは SNMP v1 限定です。
- 「Send Trap Destination Address」を，Hitachi IT Operations Analyzer 管理用サーバの IP アドレスにして，セットアップしてください。さらに，「Send Trap Destination Port」を，Hitachi IT Operations Analyzer 管理用サーバの Trapping Port（ポート番号 162）に設定してください。

注意事項

Hitachi IT Operations Analyzer が使用しているデフォルトのポート番号については，マニュアル「Hitachi IT Operations Analyzer スターターガイド」の 2 章を参照してください。

5.2.1 Cisco IP スイッチ（IOS）の構成手順例

1. telnet を使って IP スイッチに接続して，次の内容を入力する。
   a.「enable」と入力して，パスワードの入力を求められたら，入力する。
   b.「configure terminal」と入力する。
   c.「snmp-server enable traps」と入力する。
   d.「snmp-server host 192.168.1.1 version 1 public」と入力する。「192.168.1.1」はトラップの送信先，「public」はコミュニティ名。両方とも，必要に応じて変更する。
   e.「end」と入力する。
   f.「show running-config」と入力して，設定を確認する。
2. telnet を切断する。

5.2.2 Juniper IP スイッチ（EX シリーズ）の構成手順例

1. Web ブラウザを使用して，Juniper Web デバイスマネージャに接続する。
   a. ログインする。
   b.「Configure」をクリックする。
   c.「Service」をクリックして，「SNMP」を選択する。
   d.「Trap Groups」の中から，「Add」をクリックする。
   e.「Trap Group Name」を指定する。
   f. カテゴリーエリアから，「Link」または「None」を選択する。
   g.「Targets」に，監視用サーバの IP アドレスを追加する。
   h.「OK」をクリックする。

2. Web ブラウザを閉じる。

5.2.3 Enterasys IP スイッチの構成手順例

1. telnet を使用して IP スイッチに接続する。管理者モードでログインして，次のコマンドを実行する。
   a.「set snmp targetparams testParams user public securitymodel v1 message-processing v1」と入力する。
   「testParams」は必要に応じて変更できる。
   b.「set snmp notify testNotify tag testTag trap」と入力する。
   「testNotify」および「testTag」は必要に応じて変更できる。
   c.「set snmp targetaddr testTargetAddr 192.168.55.11 param testParams udpport 162 mask 255.255.255.0 taglist testTag」と入力する。
   「testTargetAddr」は任意で入力する名前。「192.168.55.11」はトラップ送信先の IP アドレス。「162」はトラップ送信先のポート番号。そして，「255.255.255.0」はトラップ送信先のサブネットマスク。この情報は必要に応じて変更できる。
   d.「show running-config」と入力して，設定を確認する。
2. telnet を切断する。

5.2.4 Extreme IP スイッチの構成手順例

1. telnet を使用して IP スイッチに接続する。管理者モードでログインして，次のコマンドを実行する。
   a.「configure snmpv3 add target-params testTargetParam user v1v2c_ro mp-model snmpv1 sec-model snmpv1 sec-level noauth」と入力する。
   「testTargetParam」は任意で入力する名前。「v1v2c_ro」はセキュリティ名。どちらも，必要に応じて変更できる。セキュリティ名は「show snmpv3 community」を使って確認する。
   b.「configure snmpv3 add target-addr 192.168.55.11 param testTargetParam ipaddress 192.168.55.11/FFFFFF00 transport-port 162 from 192.168.55.7」と入力する。
   「191.168.55.11」はトラップ送信先の IP アドレス。「FFFFFF00」はトラップ送信先のサブネットマスク。「162」はトラップ送信先のポート番号。そして，
   「192.168.55.7」はトラップソースの IP アドレス。IP アドレスは必要に応じて変更できる。
   c.「show running-config」と入力して，設定を確認する。
2. telnet を切断する。

6 Hitachi ストレージの準備

Hitachi IT Operations Analyzer は，デバイスマネージャの SMI-S プロバイダを使って，Hitachi 9500V と，Hitachi USP VM を管理できます。この章では，Hitachi AMS/WMS/SMS ストレージ機器に接続するために収集しなければならない情報と，Hitachi ストレージを SMI-S 用にどのように構成すればよいかについて説明します。

6.1 Hitachi AMS/WMS/SMS 接続情報の取得

Hitachi IT Operations Analyzer は，Hitachi AMS/WMS/SMS を管理できます。Hitachi AMS/WMS/SMS に接続する場合は，次の表に示す情報が必要になります。

表 6-1 Hitachi AMS/WMS/SMS に接続するのに必要な情報

項目	詳細
IP アドレス	ストレージに接続するのに使用される IP アドレスです
ユーザー ID	アカウント認証またはパスワード保護が有効な場合は，ストレージにログオンするユーザーの ID を指定してください
パスワード	ユーザー ID に対応するパスワードを指定してください。アカウント認証またはパスワード保護が有効な場合は，この情報が必要になります

注意事項

パスワード保護が有効になっている場合，エラーが発生するおそれがあります。例えば，複数の管理用サーバでパスワード保護が有効になっている Hitachi ストレージに同時にアクセスしようとしている場合などに，エラーが発生するおそれがあります。エラーを回避するために，パスワード保護を無効にすることをお勧めします。

ポート番号の変更方法

Hitachi ストレージの管理ポート番号を変更している場合は，services ファイルにポート番号を登録する必要があります。

services ファイルのパス：

<Windows ディレクトリ >¥system32¥drivers¥etc¥services

通常ポート番号のサービス名：

df-damp-snm

セキュアポート番号のサービス名：

df-damp-snm-ssl

設定例（通常ポートを 2300，セキュアポートを 25000 に設定）：

```
df-damp-snm      2300/tcp    #normal port
df-damp-snm-ssl 25000/tcp    #secure port - SSL
```

注意事項

The IT Operations Analyzer で監視する Hitachi ストレージのポート番号は，すべて同一である必要があります。
また，services ファイルを変更すると，同一サーバ上で動作する「HSNM2-API」を使用する製品にも設定の影響を受けます。
HSNM2-API を使用する製品：

- Hitachi Storage Navigator Modular 2，HiCommand シリーズなど

6.1.1 Hitachi AMS/WMS/SMS のパフォーマンス情報の取得

パフォーマンスを管理するためには，次に示すように，パフォーマンス情報を取得する機能を有効にする必要があります。

1. Hitachi Storage Navigator Modular 2 でパフォーマンスを管理しているストレージの，［Performance Statistics］画面を開く。
2. ［RAID グループ / ロジカルユニット情報］，［キャッシュ情報］，［プロセッサ情報］，および［ドライブ操作情報］を確認して，［OK］ボタンをクリックする。

注意事項

Hitachi 9500V および Hitachi USP VM ストレージの構成についての情報は，「6.2 Hitachi 9500V および Hitachi USP VM ストレージ接続情報の取得」を参照してください。

6.2 Hitachi 9500V および Hitachi USP VM ストレージ接続情報の取得

SMI-S プロバイダを，次の手順に従って構成してください。詳細については，Hitachi デバイスマネージャのマニュアルを参照してください。

1. 任意のサーバに，デバイスマネージャをインストールする。インストール中に SMI-S プロバイダが存在するかどうか選択してから，SMI-S プロバイダを有効にする。
2. デバイスマネージャにログインして，［サブシステム］をクリックする。そして，［サブシステムの追加］をクリックして，ストレージ機器を登録する。
   機器を登録するときに，IP アドレス，ユーザー ID，およびストレージコントローラのパスワードが必要です。表 6-2 に，Hitachi 9500V および Hitachi USP VM ストレージに接続するときに必要な情報を示します。
3. SMI-S プロバイダを使用している場合，デバイスマネージャサーバのメモリヒープサイズを拡張する必要がある。次に，Microsoft Windows で作業する場合の手順を例として示す。
   a. メモリヒープサイズを計算する。
   b. テキストエディタを使って Server.ini ファイルを開く。
   ＜デバイスマネージャのインストール場所 >¥HiCommandServer¥Server.ini
   c. ステップ a で計算した結果を基に，JVM_XOPT_HEAP_MAX. の値を変更する。記述形式を示します。
   JVM_XOPT_HEAP_MAX=Xmx< 設定する値 >m
   d. デバイスマネージャサーバを再起動する。

表 6-2 Hitachi 9500V および Hitachi USP VM ストレージに接続するために必要な情報

項目	詳細
IP アドレス	デバイスマネージャがインストールされているサーバの IP アドレスを入力する
ネームスペース	デバイスマネージャ 5.9 以上の場合は，次を指定する root/smis/smis12 デバイスマネージャ 6.2 以上の場合は，次を指定する root/smis/smis13
SSL の存在	デバイスマネージャのインストール時に適用した設定を使用する
ポート番号	デバイスマネージャのインストール時に適用した設定を使用する デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	デバイスマネージャのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを使用する

注意事項

Hitachi デバイスマネージャを使用して Hitachi 9500V および Hitachi USP VM ストレージを管理している場合，モニタリング画面で，次のコンポーネントが常に通常運用の状態でレポートされます。

- ストレージコントローラ
- ストレージ FC ポート
- ストレージディスクドライブ
- ストレージボリューム
- LUN

それによって，何かエラーが発生するということは，ありません。

6.3 Hitachi ストレージ USP VM のパフォーマンス情報の取得

Hitachi USP VM のパフォーマンス情報を取得するための一般的な手順を示します。詳細については，Hitachi デバイスマネージャのマニュアルを参照してください。

1. ストレージサブシステムを準備する。
   パフォーマンス情報を取得したいストレージサブシステムのコマンドデバイスを準備します。コマンドデバイスとは，大容量ディスクアレイユニットに対してコントロールコマンドを発行するコントロールデバイスです。そして，パフォーマンス情報を収集するホストにパスを割り当てて，ホストがコマンドデバイスを認識できるように構成します。
2. パフォーマンス情報を収集するホストを準備する。
   デバイスマネージャエージェントをインストールして，コマンドデバイスを構成します。
3. デバイスマネージャサーバを準備する。
   パフォーマンス情報を収集するホストのホスト名を，デバイスマネージャサーバのプロパティファイルで設定します。

6.4 一つのストレージ当たりの最大ボリューム数に関する注意事項

一つのストレージについて，管理できるボリュームの数は，最大で 2,000 です。最大数を超えた場合，モニタリング画面の［コンポーネント］タブに次のような情報を持つ，管理できないストレージボリュームが表示されます。

- コンポーネント名：ボリューム（ボリューム数）
- 状態：ボリュームは，2000 を超えているため，監視できません。
- 種別：ストレージボリューム

さらに，ボリュームに関連する情報は取得されません。モニタリング画面には次のように表示されます。

［コンポーネント］タブ：2,000 個を超えるストレージボリュームを新たに監視対象にした場合，「LUN」，「ストレージファイル共有」，「ストレージファイル共有ポート」および「ストレージボリューム」には何も表示されません。ストレージボリューム数が途中で増えて 2,000 個を超えた場合は，監視対象外に状態変更されます。

［パフォーマンス］タブ：書き込み処理のキャッシュヒット率については，状態が不明なため，パフォーマンスが取得できません。

注意事項

この最大ボリューム数の注意事項は，日立ストレージに限らず，そのほかのストレージについても当てはまります。

7 FC スイッチとストレージのための SMI-S の準備

Hitachi IT Operations Analyzer は，FC スイッチやその他のストレージの探索と管理のために SMI-S を使用しています。この章では，SMI-S およびご使用の環境の FC スイッチやストレージをセットアップするために必要な準備について説明します。

7.1 SMI-S の準備について

SMI-S は，SNIA が規定した基準で，open management application programming interface（API）を提供しています。これは，バーチャルストレージ，スイッチ，ホストといったストレージネットワークやストレージ機器の相互管理をサポートしています。

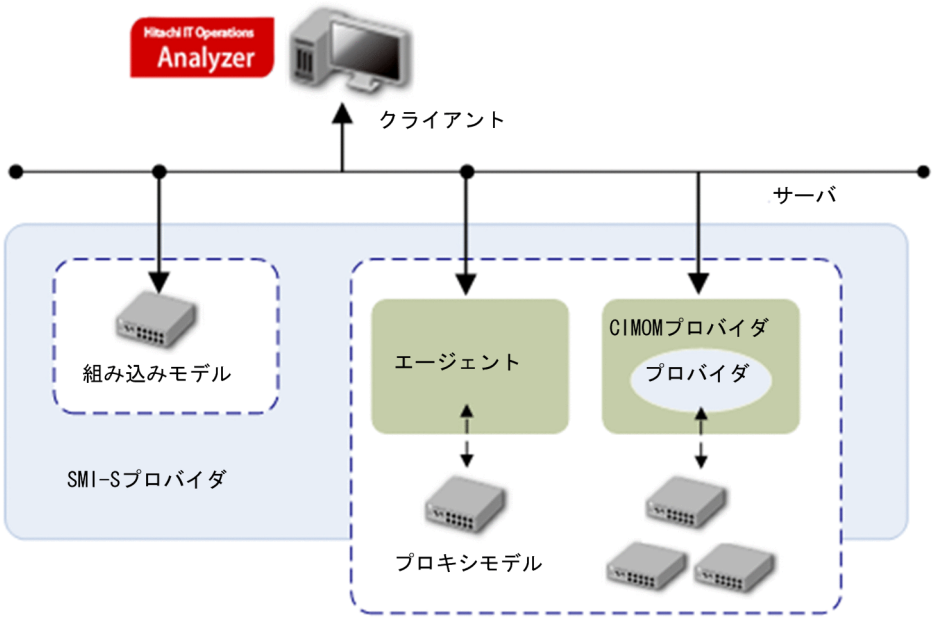
ご使用の環境でサードパーティー製のストレージ（FC スイッチや Hitachi ストレージ以外のストレージ）を使用している場合，Hitachi IT Operations Analyzer は，SMI-S プロバイダを使用することでサードパーティー製のストレージを探索，管理できます。

SMI-S プロバイダと併せてサードパーティー製のストレージを使用している環境で使用されているのは，組み込みモデル，またはプロキシモデルのどちらかです。

- 組み込みモデルの場合，SMI-S プロバイダは機器上で稼働しています。
- プロキシモデルの場合，SMI-S プロバイダはコンピュータにインストールされています。

次の図に，SMI-S 環境の例を示します。これは，サーバ（SMI-S サーバと呼びます）とクライアントで構成されます。Hitachi IT Operations Analyzer は，クライアントとして操作します。この例では，ファイバーチャネル（FC）についての情報を収集しています。図の中の影を付けた部分が，組み込みモデルおよびプロキシモデルを包含しています。そして，この部分については，初期探索前に準備する必要があります。

図 7-1 SMI-S 環境の例



次の節で，ご使用の環境内での FC スイッチやストレージで必要な準備について説明します。

7.2 ファイバーチャネル（FC）スイッチ用の SMI-S の準備

機器を管理対象に指定するためには，管理対象となる機器が SMI-S バージョン 1.0 から 1.3 までをサポートしている必要があります。また，これらの機器を管理するデバイスが稼働していることが必要です。この節では，次に示す SMI-S プロバイダ設定について説明します。

- Brocade(R) FC スイッチ
- Brocade Sphereon シリーズ FC スイッチ
- QLogic(R) FC スイッチ
- Cisco(R) FC スイッチ

7.2.1 Brocade FC スイッチ（Sphereon シリーズを除く）の構成

SMI-S プロバイダ設定を，次の手順に従って構成します。詳細については，Brocade SMI エージェントのドキュメントを参照してください。

1. Brocade SMI エージェントを，次の Web サイトからダウンロードする。
   http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. Brocade SMI エージェントを任意のサーバにインストールする。インストール中に，［Proxy Connection Configuration］ウィンドウの中の，［Add］をクリックして，IP アドレス，ユーザー ID，および FC スイッチのパスワードを登録する。

次の表に，Brocade FC スイッチに接続するために必要な情報を示します。

表 7-1 Brocade FC スイッチに接続するために必要な情報

項目	詳細
IP アドレス	Brocade SMI エージェントがインストールされているサーバの IP アドレスを指定する
ネームスペース	固定で，［root/brocade1］と指定する
SSL 有無	インストール中に構成された SMI エージェント設定を適用する
ポート番号	インストール中に構成された Brocade SMI エージェントの設定を適用する。デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	Brocade SMI エージェントのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.2.2 Brocade Sphereon シリーズ FC スイッチの構成

SMI-S プロバイダ設定を，次の手順に従って構成します。詳細については，Brocade SMI エージェント（EOS 用）のドキュメントを参照してください。

1. Brocade SMI エージェント（EOS 用）を，次の Web サイトからダウンロードする。
   http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. Brocade SMI エージェント（EOS 用）を任意のサーバにインストールする。そして，Brocade のドキュメントを参照してエージェントを構成する。

次の表に，Brocade Sphereon シリーズ FC スイッチに接続するために必要な情報を示します。

表 7-2 Brocade Sphereon シリーズ FC スイッチに接続するために必要な情報

項目	詳細
IP アドレス	Brocade SMI エージェント（EOS 用）がインストールされているサーバの IP アドレスを指定する
ネームスペース	固定で，［root/mcdata］と指定する
SSL 有無	インストール中に構成された SMI エージェント設定を適用する
ポート番号	インストール中に構成された Brocade SMI エージェント（EOS 用）の設定を適用する
ユーザー ID	Brocade SMI エージェント（EOS 用）のユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.2.3 QLogic FC スイッチの構成

SMI-S は，すでにこのデバイスに組み込まれています。次の手順に従うか，または CLI を使用して，SMI-S プロバイダ設定を構成してください。詳細については，QLogic FC スイッチのドキュメントを参照してください。

1. Web ブラウザから，QLogic FC スイッチの管理ポートに接続する（例：http://10.208.113.46）。［Switch Manager］ウィンドウが表示される。
2. ［Switch Manager］メニューバーから，［Switch］を選択して，［Services］をクリックする。［System Services］ダイアログボックスが表示されます。
3. SMI-S プロバイダサービスが有効であることを確認する。
   ・［CIM Service］が選択されている場合は，SMI-S プロバイダサービスは有効になっています。［Close］をクリックしてください。
   ・［CIM Service］が選択されていない場合は，選択して，［OK］をクリックしてください。
4. ［System Services］ダイアログボックス内に，［SSL Service］を指定するオプション

が存在する場合は，SSL ポート 5989 を使用できる。

次の表に，QLogic FC スイッチに接続するために必要な情報を示します。

表 7-3 QLogic FC スイッチに接続するために必要な情報

項目	詳細
IP アドレス	QLogic FC スイッチの IP アドレスを指定する
ネームスペース	固定で，［root/switch］と指定する
SSL 有無	QLogic FC スイッチの設定を適用する
ポート番号	インストール中に構成された QLogic FC スイッチの設定を適用する。デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	QLogic FC スイッチのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.2.4 Cisco FC スイッチの構成

SMI-S サーバを，CLI を使ってセットアップできます。次に示す手順に従うと，HTTP プロトコル（ポート 5988）を使ってサーバを有効にして，CLI に接続できます。
HTTPS プロトコル（ポート 5989）を使用することを選択した場合は，SSL 認証を適用して，ログイン情報を暗号化してください。そして，HTTPS と SMI-S サーバを有効にしてください。

1. FC スイッチに telnet で接続して，ログインする。
2. ［config t］と入力して，構成モードを開始する。
3. デフォルトでは，HTTP が有効になっています。有効になっていない場合は，［cimserver enableHttp］と入力して，有効にする。
4. ［cimserver enable］と入力して，SMI-S サーバを有効にする。
5. ［show cimserver］と入力して，設定を確認する。
   ・CIM サーバが有効であるか
   ・CIM サーバの HTTP が有効であるか
6. FC スイッチをログアウトして，telnet を切断する。

次の表に，Cisco FC スイッチに接続するために必要な情報を示します。

表 7-4 Cisco FC スイッチに接続するために必要な情報

項目	詳細
IP アドレス	Cisco FC スイッチの IP アドレスを指定する
ネームスペース	固定で，［root/cimv2］と指定する

項目	詳細
SSL 有無	Cisco FC スイッチの設定を適用する。詳細については，「Cisco MDS 9000 Family SMI-S Programming Reference」を参照すること http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html
ポート番号	インストール中に構成された Cisco FC スイッチの設定を適用する。デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	Cisco FC スイッチのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.3 ストレージ用の SMI-S の準備

ストレージを管理対象として指定するためには，管理対象とするストレージが SMI-S バージョン 1.0 から 1.3 までをサポートしている必要があります。そして，ストレージを管理するサービスが稼働していることが必要です。この節では，次に示すストレージについて SMI-S プロバイダの設定を説明します。

- EMC ストレージ
- HP EVA シリーズストレージ
- HP MSA シリーズストレージ
- Engenio OEM Sun ストレージおよび IBM ストレージ
- NetApp ストレージ

注意事項

Hitachi ストレージの設定と，Hitachi USP VM のパフォーマンス情報の取得については，「6. Hitachi ストレージ装置の準備」を参照してください。

7.3.1 EMC ストレージの構成

EMC ストレージで SMI-S プロバイダを構成する場合は，次の手順を参照してください。詳細については，EMC SMI-S プロバイダのドキュメントを参照してください。

1. EMC SMI-S プロバイダを，次の Web サイトからダウンロードする。http://Powerlink.EMC.com
2. EMC SMI-S プロバイダを，EMC ストレージボリュームが適用されているサーバにインストールする。
3. symcfg コマンドを使用して，ストレージ機器の認証情報を登録する。入力例を次に示す。
   symcfg authorization add -host **<***Storage IP address***>** -Username **<***Storage User ID***>** -Password **<***Storage Password***>**

7.3.2 EMC ストレージのパフォーマンス情報の取得

次の手順に従って，EMC ストレージのパフォーマンス情報を取得してください。

1. EMC ストレージ管理ソフトを使用して，パフォーマンスデータを取得する。例として，EMC Navisphere Management Suite を使用したときの手順について説明する。
   a. EMC Navisphere Management Suite のメニューバーから，［Data Logging］ウィンドウを開く。
   b. ［Target］エリアで，パフォーマンスを取得したいストレージを選択する。そして，［Logging］から，［Status］フィールドを確認する。

［Status］が，［Stopped］になっている場合は，［Start］をクリックしてください。［Status］が，［Running］になっている場合は，［Started on date time］を選択して，［Cancel］をクリックしてください。SMI-S プロバイダを再起動する必要はありません。

2. SMI-S プロバイダを再起動する。CLI を使用している場合は，次に示すように cimserver コマンドを実行して，SMI-S プロバイダを停止・開始する。
C:¥Program Files¥EMC¥SYMCLI¥strobin> cimserver -stop EMC_SMI_Provider
Pegasus stopped as a Windows service
C:¥Program Files¥EMC¥SYMCLI¥strobin> cimserver -start EMC_SMI_Provider
Pegasus started as a Windows service

次の表に，EMC ストレージに接続するために必要な情報を示します。

表 7-5 EMC ストレージに接続するために必要な情報

項目	詳細
IP アドレス	EMC SMI-S プロバイダのインストールされているサーバの IP アドレスを指定する
ネームスペース	固定で，［root/emc］と指定する
SSL 有無	EMC SMI-S プロバイダの設定を適用する
ポート番号	EMC SMI-S プロバイダの設定を適用する。デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	EMC SMI-S プロバイダのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.3.3 HP EVA シリーズストレージの構成

SMI-S プロバイダ設定を，次の手順に従って構成してください。詳細については，Command View EVA のマニュアルを参照してください。

注意事項

HP EVA シリーズ SMI-S プロバイダは，パフォーマンス情報取得機能を持っていません。

1. HP EVA シリーズストレージボリュームが適用されているサーバに，Command View EVA をインストールする。
2. Command View EVA を開始する。そして，ストレージが探索されていることを確認する。探索されていない場合は，［Discover］をクリックする。

次の表に，HP EVA ストレージに接続するために必要な情報を示します。

表 7-6 HP EVA ストレージに接続するために必要な情報

項目	詳細
IP アドレス	Command View EVA のインストールされているサーバの IP アドレスを指定する
ネームスペース	固定で，［root/eva］と指定する
SSL 有無	Command View EVA の設定を適用する
ポート番号	Command View EVA の設定を適用する。デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	Command View EVA のユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.3.4 HP MSA シリーズストレージの構成

SMI-S プロバイダ設定を，次の手順に従って構成してください。詳細については，MSA SMI-S プロバイダのドキュメントを参照してください。

注意事項

HP EVA シリーズ SMI-S プロバイダは，パフォーマンス情報取得機能を持っていません。

1. MSA SMI-S プロバイダを，次の Web サイトからダウンロードする。http://h18006.www1.hp.com/storage/smis.html
2. MSA SMI-S プロバイダを，任意のサーバにインストールする。

次の表に，HP MSA ストレージに接続するために必要な情報を示します。

表 7-7 HP MSA ストレージに接続するために必要な情報

項目	詳細
IP アドレス	MSA SMI-S プロバイダのインストールされているサーバの IP アドレスを指定する
ネームスペース	固定で，［root/hpmsa］と指定する
SSL 有無	MSA SMI-S プロバイダの設定を適用する
ポート番号	MSA SMI-S プロバイダの設定を適用する
ユーザー ID	MSA SMI-S プロバイダのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.3.5 Engenio OEM Sun ストレージおよび IBM ストレージの構成

SMI-S プロバイダ設定を，次の手順に従って構成してください。詳細については，Engenio SMI-S プロバイダのドキュメントを参照してください。

1. Engenio SMI プロバイダを，次の Web サイトからダウンロードする。http://www.lsi.com/storage_home/products_home/external_raid/management_software/smis_provider/index.html
2. ProviderUtil コマンドを実行する。そして，ストレージ機器を登録する。
   C:¥Program Files¥EngenioProvider¥SMI_SProvider¥bin>ProviderUtil
   Input CIMOM Username: < プロバイダユーザー ID。デフォルトユーザー ID は，空欄です。>
   Input CIMOM Password: < デフォルトパスワードは空欄です。>
   Input Port [5988]: < プロバイダのポート番号 >
   Input Operation
   1)addDevice
   2)removeDevice
   3)Add credentials for an array
   Please Input 1, 2, or 3: <Enter 1>
   Input device DNS - resolvable hostname or IP address: < ストレージのホスト名または IP アドレス >
   Input Array Password: < ストレージパスワード。デフォルトは空欄です >

次の表に，Engenio OEM Sun ストレージおよび IBM ストレージに接続するために必要な情報を示します。

表 7-8 Engenio OEM Sun ストレージおよび IBM ストレージに接続するために必要な情報

項目	詳細
IP アドレス	Engenio SMI-S プロバイダのインストールされているサーバの IP アドレスを指定する
ネームスペース	固定で，［root/lsissi11］と指定する
SSL 有無	Engenio SMI-S プロバイダの設定を適用する
ポート番号	Engenio SMI-S プロバイダの設定を適用する。デフォルトでは，次のとおり • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	Engenio SMI-S プロバイダのユーザー ID を使用する
パスワード	ユーザー ID に対応するパスワードを入力する

7.3.6 NettApp ストレージの構成

NetApp の SMI-S プロバイダは，「Data ONTAP SMI-S Agent」という名前を，Windows と Linux の両方で使用します。

次に，Linux で Data ONTAP SMI-S Agent をどのように設定するかについて説明します。さらに詳しい情報については，SMI-S プロバイダに付属の，「Data ONTAP SMI-S Agent README」を参照してください。

1. SMI-S プロバイダ（Linux バージョン）を，次の Web サイトからダウンロードする。
   http://www.netapp.com/us/company/leadership/industry-standards/smi-s-agent.html
2. インストールのために，Linux サーバを準備する。
   a.SMI-S プロバイダが OS をサポートしているか確認する。
   b. SMI-S プロバイダには，前提条件として JRE（バージョン 1.5 以降）が必要。Linux サーバに JRE がインストールされているかどうか，確認する。
   c. 環境変数 JAVA_HOME を，次のように設定する。
   JRE をインストールしている場合：JAVA_HOME="/usr/java"
   JDK をインストールしている場合（例：jdk1.5.0_19）：
   JAVA_HOME="/usr/java/jdk1.5.0_19"
3. 手順 1 でダウンロードしたインストールパッケージを，Linux サーバに移動させる（例で示すインストールパッケージは，smisagent-3-0-1.tar）。
4. ルートアカウントで Linux サーバにログインする。
5. tar コマンドを使って，任意のディレクトリにインストールパッケージを展開する。
6. 次に示すように，展開された install_smisproxy スクリプトを実行する。そして，SMI-S Agent をインストールする。
   # tar xvf ./smisagent-3-0.tar
   # ./install_smisproxy /usr
7. デフォルトでは，SMI-S プロバイダに接続するためには，ポート番号 5989 と，HTTPS プロトコルを使用する。HTTP プロトコルを使うためにポート番号を変更するためには，WEBSconfig.ini を編集する。このファイルは，次のディレクトリに格納されている。
   /usr/ws/server/cserver/bin
   デフォルトの設定を次に示します。
   enableOverride=False （この先の設定を変更する場合は，True に変更してください）
   HTTPPort=5988
   HTTPSPort=5989
   enableSSL=True
   enableHTTP=False
   Linux 版の場合は，HTTP を推奨します。HTTP を利用する場合 enableHTTP を True に変更してください。
8. 次のスクリプトを実行する。ps コマンドを使用すると，サービスが開始しているかど

うか確認できる。
cd /usr/ws/server/cserver/bin
./start_server
ps -C cwbemserver

9. 次に示すとおり，smis スクリプトを実行する。そして，ストレージ機器を，SMI-S プロバイダのリポジトリに登録する。
/usr/ws/bin/smis < ユーザー ID: ルート > < パスワード > add
< ストレージの IP アドレス > < ストレージのユーザー ID> < ストレージのパスワード >
10. smis スクリプトを実行して，結果を確認する。
例：# /usr/ws/bin/smis < ユーザー ID> < パスワード > list
11. natest スクリプトを実行する。そして，SMI-S プロバイダがストレージ情報を取得できたか確認する。次の例では，ストレージのディスク情報を出力する。
/usr/ws/bin/natest < ユーザー ID: ルート > < パスワード > disks

次の表に，Nett App ストレージに接続するために必要な情報を示します。

表 7-9 Net App ストレージに接続するために必要な情報

項目	詳細
IP アドレス	Data ONTAP SMI-S Agent のインストールされているサーバの IP アドレスを指定する。
ネームスペース	固定で，［root/ontap］と指定する。
SSL 有無	Data ONTAP SMI-S Agent の設定を適用する。 Linux 版の場合は，Non-SSL を推奨します。
ポート番号	Data ONTAP SMI-S Agent の設定を適用する。デフォルトでは，次のとおり。 • 非 SSL 通信：5988 • SSL 通信：5989
ユーザー ID	Data ONTAP SMI-S Agent のユーザー ID を使用する。
パスワード	ユーザー ID に対応するパスワードを入力する。

8 Dell サーバの準備

この章では，Dell サーバをセットアップするのに必要な項目について説明します。

8.1 Dell サーバの概要

次の二つの各項目がセットアップされていることが必要です。

- Dell サーバに関する Windows の WMI/SNMP（認証情報）
- Dell サーバに関する Linux の SSH/SNMP（認証情報）

Dell サーバに接続する場合，次の表に示す情報が必要です。

表 8-1 Dell サーバに接続するために必要な情報

項目	詳細
IP アドレス	Dell サーバの IP アドレスです。
ポート番号	Dell サーバが通信を待機する SNMP ポートです（ポート 161）。
コミュニティ名	SNMP Dell サーバのために使用するコミュニティ名です。

8.2 SNMP トラップ接続の有効化

監視される Dell サーバ上の SNMP エージェントは，Hitachi IT Operations 管理用サーバに SNMP トラップを送ることで設定されます。

Dell OMSA（Open Manage Server Administrator）トラップをサーバから受け取ったとき，Hitachi IT Operations Analyzer はトラップの重要性に基づいて，Dell OMSA トラップ構成要素のステータスを更新します。

8.2.1 Windows 環境での SNMP エージェントの構成

次の手順にしたがって，Microsoft Windows 環境で Dell サーバの SNMP エージェントを設定してください。

1. **［スタート］メニューから［コントロールパネル］を選択する。**
2. **［管理ツール］を開く。**
3. **［サービス］を開く。**
4. **［SNMP Service］を右クリックして，［プロパティ］を選択する。**
5. **［トラップ］タブをクリックして，［トラップ］ダイアログボックスを開く。**
6. **［コミュニティ名］ドロップダウンリストから該当の SNMP コミュニティ名を選択する。そのあと，［トラップ送信先］リストボックスの下にある［追加］をクリックする。**
   ［SNMP サービスの構成］ボックスが表示されます。
7. **Hitachi IT Operations Analyzer 管理用サーバのホスト名または IP アドレスを入力したあと，［追加］をクリックする。**

8.2.2 Linux 環境での SNMP エージェントの構成

Linux 環境で Dell サーバの SNMP エージェントを構成するための手順は次のとおりです。

1. **/etc/snmp/snmpd.conf 構成ファイルに，次の行を追加する。**
   trapsink IP_address community_name
   IP_address 変数の値は Hitachi IT Operations Analyzer 管理サーバの IP アドレスです。
   community_name 変数の値は SNMP コミュニティ名です。
2. **次のコマンドを使って，SNMP エージェントをリスタートする。**
   /sbin/service snmpd restart

付録

付録 A　このマニュアルの参考情報

付録 A　このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

付録 A.1　関連マニュアル

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 IT Operations Analyzer スターターガイド（3020-3-N86）

マニュアルの本文中で，「デバイスマネージャのマニュアル」と記載されている場合，次の 3 冊のマニュアルを指します。

Hitachi Device Manager，Provisioning Manager and Tiered Storage Manager Software インストールガイド（3020-3-P29）

Hitachi Device Manager and Provisioning Manager Software システム構成ガイド（3020-3-P13）

Hitachi Device Manager Software Web Client ユーザーズガイド（3020-3-P11）

付録 A.2　このマニュアルでの表記

このマニュアルでは，製品名を次のように表記しています。

製品名	このマニュアルでの表記	
AMD Athlon™	AMD	
Hitachi 9500V	Hitachi ストレージ	
Hitachi AMS/WMS/SMS		
Hitachi USP		
Java™	Java	
Red Hat Enterprise Linux(R) 5 (AMD/Intel 64)	Linux 5 (AMD/Intel 64)	Linux
Red Hat Enterprise Linux(R) 5 (IPF)	Linux 5 (IPF)	
Red Hat Enterprise Linux(R) 5 (x86)	Linux 5 (x86)	
Red Hat Enterprise Linux(R) 5 Advanced Platform (AMD/Intel 64)	Linux 5 Advanced Platform (AMD/Intel 64)	
Red Hat Enterprise Linux(R) 5 Advanced Platform (IPF)	Linux 5 Advanced Platform (IPF)	

製品名	このマニュアルでの表記	
Red Hat Enterprise Linux(R) 5 Advanced Platform (x86)	Linux 5 Advanced Platform (x86)	
Solaris 9	Solaris	
Solaris 10		

このマニュアルでは VMware(R) について次のように表記しています。

- 製品のタイプやバージョンが一定の場合は，「VMware ESX 3，VMware ESX 3i，VMware ESX 4.0」などのように表記しています。
- サーバのタイプやバージョンが一定ではない場合は，「ESX サーバ」のように表記しています。

付録 A.3　英略語

このマニュアルで使用する英略語を次に示します。

英略語	英字での表記
API	Application Programming Interface
CD-ROM	Compact Disc Read Only Memory
CIM	Common Information Model
CIMOM	Common Information Model Object Manager
DCOM	Distributed Component Object Model
FC	Fiber Channel
FC HBA	Fiber Channel Host Bus Adapter
fcinfo	Fiber Channel Information tool
HBA	Host Bus Adapter
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IPF	Itanium(R) Processor Family
iSCSI	Internet Small Computer System Interface
LAN	Local Area Network
MIB	Management Information Base
RCA	Root Cause Analysis
SAN	Storage Area Network
SMI-S	Storage Management Initiative Specification
SNIA	Storage Networking Industry Association
SNMP	Simple Network Management Protocol

英略語	英字での表記
SSH	Secure SHell
SSL	Secure Socket Layers
UDP	User Datagram Protocol
USB	Universal Serial Bus
USP	Universal Storage Platform
WBEM	Web-Based Enterprise Management
WMI	Windows Management Instrumentation
WWW	World Wide Web

付録 A.4　KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイトです。

索引

V

W

か

く

す

ひ

ふ