

FUJITSU Software ServerView Infrastructure Manager V2.0



ユーザーズマニュアル

CA92344-1151-01 2016年9月

本書の目的

本書では、サーバやストレージなどのICT機器からファシリティ機器 (PDUなど)までを統合的に管理、運用する運用管理ソフトウェアであるFUJITSU Software ServerView Infrastructure Manager(以降、「ISM」と表記)の導入手順および機能全般を説明します。

関連マニュアル

マニュアル名称	本書での表記	説明
FUJITSU Software ServerView Infrastructure Manager V2.0 ユーザーズマニュアル	ServerView Infrastructure Manager V2.0 ユーザーズマニュアル	ISMの機能、導入手順、操作方法、トラブ ル対処方法を説明したマニュアルです。 ISMの全機能、全操作を把握できます。
FUJITSU Software ServerView Infrastructure Manager V2.0 スタートガイド	ServerView Infrastructure Manager V2.0 スタートガイド	ISMの機能概要、導入の流れを説明した マニュアルです。ISMの導入手順を把握で きます。
FUJITSU Software ServerView Infrastructure Manager V2.0 操作手順書	ServerView Infrastructure Manager V2.0 操作手順書	ISMの初期設定、運用(ノード監視、サー バ設定、サーバへのOSインストール、サー バのファームウェアアップデート)の操作手 順を説明したマニュアルです。
FUJITSU Software ServerView Infrastructure Manager V2.0 用語集	ServerView Infrastructure Manager V2.0 用語集	ISMを使用するうえで理解が必要な用語の 定義を説明した用語集です。

上記マニュアルと併せて、ISMに関する最新情報については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/

管理対象の各ハードウェアについては、各ハードウェアのマニュアルを参照してください。

PRIMERGYの場合は、「ServerView Suite ServerBooks」、またはPRIMERGYマニュアルページを参照してください。

http://jp.fujitsu.com/platform/server/primergy/manual/

本書の読者

このマニュアルは、ハードウェアとソフトウェアについて十分な知識を持っているシステム管理者、ネットワーク管理者、ファシリティ管理 者およびサービス専門家を対象とします。

本書の表記について

表記

キーボード

印字されない文字のキーストロークは、[Enter]や[F1]などのキーアイコンで表示されます。例えば、[Enter]はEnterというラベルの付いたキーを押すことを意味し、[Ctrl]+[B]は、CtrlまたはControlというラベルの付いたキーを押しながら[B]キーを押すことを意味します。

記号

特に注意すべき事項の前には、以下の記号が付いています。

믿 ポイント

ポイントとなる内容について説明します。



注意する項目について説明します。

変数:<xxx>

お使いの環境に応じた数値/文字列に置き換える必要のある変数を表します。

例:<IPアドレス>

略称

本書では、以下のとおり略称で記載することがあります。

正式名称	略和	东
Microsoft® Windows Server® 2012 R2 Datacenter	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2
Microsoft® Windows Server® 2012 R2 Standard	Windows Server 2012 R2 Standard	
Microsoft® Windows Server® 2012 R2 Essentials	Windows Server 2012 R2 Essentials	
Microsoft® Windows Server® 2012 Datacenter	Windows Server 2012 Datacenter	Windows Server 2012
Microsoft® Windows Server® 2012 Standard	Windows Server 2012 Standard	
Microsoft® Windows Server® 2012 Essentials	Windows Server 2012 Essentials	
Microsoft® Windows Server® 2008 R2 Datacenter	Windows Server 2008 R2 Datacenter	Windows Server 2008 R2
Microsoft® Windows Server® 2008 R2 Enterprise	Windows Server 2008 R2 Enterprise	
Microsoft® Windows Server® 2008 R2 Standard	Windows Server 2008 R2 Standard	
Red Hat Enterprise Linux 7.2 (for Intel64)	RHEL 7.2	Red Hat Enterprise Linux
Red Hat Enterprise Linux 7.1 (for Intel64)	RHEL 7.1	または
Red Hat Enterprise Linux 6.8 (for Intel64)	RHEL 6.8(Intel64)	Linux
Red Hat Enterprise Linux 6.8 (for x86)	RHEL 6.8(x86)	
Red Hat Enterprise Linux 6.7 (for Intel64)	RHEL 6.7(Intel64)	
Red Hat Enterprise Linux 6.7 (for x86)	RHEL 6.7(x86)	
VMware® vSphere™ ESXi 6.0	VMware ESXi 6.0	VMware ESXi
VMware® vSphere™ ESXi 5.5	VMware ESXi 5.5	

用語

本書で使用している主な略語および用語については、『ServerView Infrastructure Manager V2.0 用語集』を参照してください。

高度な安全性が要求される用途への使用について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業等の一般的用途を想定して開発・設計・製造されているものであり、原子 力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療 用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接 生命・身体に対する重大な危険性を伴う用途(以下「ハイセイフティ用途」という)に使用されるよう開発・設計・製造されたものではあり ません。お客様は本製品を必要な安全性を確保する措置を施すことなくハイセイフティ用途に使用しないでください。また、お客様が ハイセイフティ用途に本製品を使用したことにより発生する、お客様または第三者からのいかなる請求または損害賠償に対しても富士 通株式会社およびその関連会社は一切責任を負いかねます。

安全にお使いいただくために

本書には、本製品を安全に正しくお使いいただくための重要な情報が記載されています。本製品をお使いになる前に、本書を熟読してください。また、本製品を安全にお使いいただくためには、本製品のご使用にあたり各製品(ハードウェア、ソフトウェア)をご理解いただく必要があります。必ず各製品の注意事項に従ったうえで本製品をご使用ください。本書は本製品の使用中にいつでもご覧になれるよう大切に保管してください。

改造等

お客様は、本ソフトウェアを改造したり、あるいは、逆コンパイル、逆アセンブルをともなうリバースエンジニアリングを行うことはできません。

免責事項

本製品の運用を理由とする損失、免失利益等の請求につきましては、いかなる責任も負いかねます。本書の内容に関しては将来予告なしに変更することがあります。

登録商標について

Microsoft、Windows、Windows Vista、Windows Server、Hyper-V、Active Directory、またはその他のマイクロソフト製品の名称および 製品名は、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 氏の米国およびその他の国における登録商標あるいは商標です。

Red Hat およびRed Hat をベースとしたすべての商標とロゴは、米国およびその他の国におけるRed Hat, Inc.の商標または登録商標です。

VMware、VMwareロゴ、VMware ESXi、VMware SMPおよびVMotionはVMware,Inc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。

Intel、インテル、Xeonは、米国およびその他の国におけるIntel Corporationまたはその子会社の商標または登録商標です。

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

Zabbixはラトビア共和国にあるZabbix LLCの商標です。

PostgreSQLはPostgreSQLの米国およびその他の国における商標です。

Apacheは、Apache Software Foundationの商標または登録商標です。

その他の会社名と各製品名は、各社の商標、または登録商標です。

その他の各製品は、各社の著作物です。

著作権表示

© Copyright Fujitsu Limited 2016 All rights reserved

本書を無断で複載・転載することを禁止します。

目次

第1章 ServerView Infrastructure Managerの概要	1
1.1 概要	
1.2 機能概要	
1.2.1ノード管理機能の概要	2
1.2.2 モニタリング機能の概要	
1.2.3 プロファイル管理機能の概要	
1.2.4 ログ管理機能の概要	
1.2.5 ファームウェア管理機能の概要	
1.2.6 ネットワーク管理機能の概要	
1.3 ISM機能とインフラ運用管理シーン	
1.3.1 インフラ運用管理シーンごとのISM機能イメージ	
1.4 構成	
1.5 システム要件	
1.5.1 ISM-VA (仮想マシン)のシステム要件	
1.5.2 管理端末のシステム要件	
1.6 留意事項	
	,
第2章 ISMの機能	
2.1 ユーザーインターフェース	
2.1.1 GUI	
2.1.2 FTPアクセス	
2.1.3 コンソールアクセス	
2.2 ISMの機能説明	15
2.2.1 ノード管理機能	
2.2.1.1 データセンター/フロア/ラック/ノードの登録	
2.2.1.2 データセンター/フロア/ラック/ノードの確認	
2.2.1.3 データセンター/フロア/ラック/ノードの編集	
2.2.1.4 データセンター/フロア/ラック/ノードの削除	
2.2.2 モニタリング機能	
2.2.3 プロファイル管理機能	
2.2.4 ファームウェア管理機能	
2.2.4.1 ノードのファームウェア版数の確認	
2.2.4.2 ファームウェアのアップデート	
2.2.4.3 ファームウェアデータに添付されているドキュメントの確認	
2.2.5 ログ管理機能	
2.2.6 ネットワーク管理機能	
2.3 ISM運用基盤の機能説明	
2.3.1 ユーザー管理機能	
2.3.1.1 ISMのユーザーの管理	
2.3.1.2 ユーザーグループの管理	
2.3.1.3 Microsoft Active DirectoryまたはLDAPとの連携	
2.3.1.4 ノードグループの管理	61
2.3.2 リポジトリ管理機能	
2.3.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの導入	
2.3.4 タスク管理	
2.3.5 ISM-VA管理機能	
2.3.5.1 ISM-VA管理機能のコマンド一覧	
2.4.ノード登録解除時、グループ変更時の操作	
2.4.1 ノード登録解除時	
2.4.2 グループ変更/解除時	
2.4.3 ユーザーグループ削除時	73
2.4.4 ユーザーグループ名の変更時	73
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
第3章 ISMの導入	74
3.1 ISM導入の流れ	74

3.2 ISMの導入設計	74
3.2.1 ディスク資源の見積り	75
3.2.1.1 ログ保存容量の見積り	
3.2.1.2 リポジトリの必要容量の見積り	75
3.2.2 リポジトリの設定	
3.2.3 ネットワークの設計	
3.2.4 ノード名の設定	77
3.2.5 ユーザーの設定	
3.3 ISM-VAのインストール	
3.3.1 Microsoft Windows Server Hyper-Vへのインストール	77
3.3.2 VMware vSphere Hypervisorへのインストール	
3.3.3 KVMへのインストール	
3.4 ISM-VAの環境設定	
3.4.1 ISM-VAの初回起動	
3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(初回)	
3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(初回)	
3.4.1.3 KVMで動作するISM-VAの場合(初回)	
3.4.2 ISM初期設定	
3.5 ライセンスの登録	
3.6 ユーザーの登録	
3.7 仮想ディスクの割当て	
3.7.1 ISM-VA全体に対する仮想ディスク割当て	
3.7.2 ユーザーグループに対する仮想ディスク割当て	
第4章 ISMの操作	
4.1 ISMの起動と終了	96
4.1.1 ISM-VAの起動	
4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(2回目以降)	
4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(2回目以降)	
4.1.1.3 KVMで動作するISM-VAの場合(2回目以降)	
4.1.2 ISM-VAの終了	
4.1.3 ISM-VAの再起動	
4.1.4 ISMのサービス起動と停止	
4.2 ISM公開サービスホートの変更	
4.3 ISM-VA()/\\\/ \/ \/ Z) ZU/\\/	
4.3.1 ISM-VAのハックノッノ	
4.5.2 ISM-VA09ハト/	
4.4 保守資料の採取	
4.5 仮想デイベクの官理	
4.5.1 仮想アイスクの割当て解除	
4.5.2 ISM-VA主体に対する仮想アイベクの迫加割目 (
4.5.3 ユーザークルークに対する仮想デイベク道加割白(
4.0	
4.6.1 SSLサーハ証明書配直	
4.0.2 SSL7 一八証明音衣示	
4.0.3 SSL7 一个証明書田刀	
4.174ゼン人設定	
4.8 不ツトワーク設定	
4.7 1、2 1) 迎知設た	
4.9.1 イベンア連邦アール用祉労者登塚	
4.9.2 ノクンヨンヘクリノト全郷	
4.3.3 1 、 √	
4.9.4 ノクンヨンヘクリノ下衣小	
	100
4.9.5 イベント通知メール用証明書削除	
 4.9.5 イベント通知メール用証明書削除 4.9.6 アクションスクリプト削除	
 4.9.5 イベント通知メール用証明書削除 4.9.6 アクションスクリプト削除 4.10 ISM-VAサービス制御 4.11 システン 体知のまデー 	

4.12 ホスト名変更	
4.13 修正適用	
4.14 プラグイン適用	
4.15 障害調査ログ切替え	
4.16 障害調査ログレベル切替え	
第5章 ノードの保守	
5.1 メンテナンスモード	
5.2 エラー発生時の調査方法	
付録A ISM-VAのアンインストール	113
付録Bトラブルシューティング	

第1章 ServerView Infrastructure Managerの概要

この章では、ServerView Infrastructure Managerの概要を説明します。

1.1 概要

ServerView Infrastructure Manager(以降「ISM」と表記)は、データセンター/サーバルームで稼働する多数のICT機器およびファシリティ機器をよりシンプルで効率的に運用管理するソフトウェアです。

なお、ISM環境において、運用管理対象のICT機器およびファシリティ機器を「ノード」と呼びます。

図1.1 ISM導入による運用管理の統合



 個々に違うツールで操作・設定
 システムとして運用するにはインフラ同士の連携を含め、 個別の設計・管理が必要



 インフラはひとつの画面で、全体を一望しながら運用可能
 プラグインなどでクラウド管理ソフトとも連携し、使い慣れた ツールからインフラを含め一括運用が可能

- ・ サーバ/ストレージ/ネットワークにわたる物理レイヤーの大規模集約運用を最適化
 - ハードウェア資産、構成情報の収集/管理
 - 管理画面の統合
 - サーバ/ストレージ/スイッチに対するファームウェア/BIOSの更新操作を一元化

管理対象ノードおよび対応機能の最新情報については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/infrastructure-software/se

図1.2 他製品との連携



1.2 機能概要

ISMの機能の概要を説明します。

1.2.1 ノード管理機能の概要

ノード管理機能は、以下を行う機能です。

• 機器情報の管理

モデル名・シリアル番号・IPアドレスなどの機器情報を管理します。

機器の登録

```
ISMが管理対象として扱うノードを登録します。
```

ネットワークに接続されたノードを検出・登録でき、ノードの登録作業を効率的に行えます。また、データセンターのフロア上のラックの 配置、ラック内のノードの配置、ノードの構成および状態を管理できます。フロアやラックのノードを可視化する機能(フロアビュー、ラッ クビュー)を使用して、ノードの管理業務を直観的に行えます。

ノード管理機能の詳細については、「2.2.1ノード管理機能」を参照してください。

1.2.2 モニタリング機能の概要

モニタリング機能は、以下のイベントを監視する機能です。

- ・ ノードから発信されるSNMPトラップ
- ・ ノードが持つ正常/異常を示すステータスの変化
- ・ノードから取得した吸気温度、CPU使用率、消費電力がISMに設定した正常範囲内であるかどうか

これらのイベントに対して利用者が作成したスクリプトの実行やメール送信などのアクションを設定でき、利用者の運用方法に合わせてノードを監視できます。

モニタリング機能の詳細については、「2.2.2 モニタリング機能」を参照してください。

1.2.3 プロファイル管理機能の概要

プロファイル管理機能は、以下を行う機能です。

- PRIMERGYサーバに対する機能
 BIOS、iRMCに対する設定およびOSインストールを、一括で実施します。
- ・ネットワークスイッチに対する機能 スイッチの管理者パスワード、SNMP設定、NTP設定など、スイッチに対する設定を実施します。
- ・ ETERNUS (ストレージ)に対する機能

RAIDグループ、ボリューム、ホットスペアの構築およびAffinity設定を実施します。

ノードの設定やOSインストールは、以下の手順で行います。

1. ISM上で、「プロファイル」という設定定義ファイルを作成します。

2. ノードに対してプロファイルを適用します。

プロファイルを活用するために、「ポリシー機能」、「グループ管理」、「エクスポート/インポート」などの補助機能も用意されています。 プロファイル管理機能の詳細については、「2.2.3 プロファイル管理機能」を参照してください。

1.2.4 ログ管理機能の概要

ログ管理機能は、主に以下の用途で利用する機能です。

- あらかじめノードごとに設定したスケジューリングに従って定期的にログを収集
- ・ 任意のタイミングでノードのハードウェアログやオペレーティングシステムログを収集
- ・ 収集したログをダウンロードして利用
- ・ GUI画面上で参照やキーワード検索を実施

ログ管理機能の詳細については、「2.2.5 ログ管理機能」を参照してください。

1.2.5 ファームウェア管理機能の概要

ファームウェア管理機能は、主に以下の用途で利用する機能です。

- ・ ノードから取得した、現在適用されているファームウェア版数を画面上で確認
- ・ ノードのファームウェアを任意の版数にアップデート(複数ノードに対して同時並行で実施可能)
- ・ファームウェアデータに添付されているReadmeファイルや更新履歴などのファイルをISM画面から参照

これらにより、ファームウェアの版数を一元管理することができます。

なお、ファームウェアを更新する場合は、あらかじめ適用するファームウェアデータをWebなどからダウンロードしてISM-VAにインポートしておく操作が必要です。

ファームウェア管理機能の詳細については、「2.2.4 ファームウェア管理機能」を参照してください。

1.2.6 ネットワーク管理機能の概要

ネットワーク管理機能は、主に以下の用途で利用する機能です。

- ・ 複数ノード間のネットワーク接続状態を画面上の接続図(ネットワークマップ)で確認
- ・ ネットワーク接続状態に変化が発生した場合に、変更箇所を画面で確認
- ・ ネットワークスイッチのVLAN、リンクアグリゲーション(LAG)設定を確認

ネットワーク管理機能の詳細については、「2.2.6 ネットワーク管理機能」を参照してください。

1.3 ISM機能とインフラ運用管理シーン

ここでは、ISMの主な機能を利用シーン別に説明します。

ISM機能	運用管理のシーン		
	システムの構築	管理対象ノードの監視運用	管理対象ノードの保守
ノード管理機能	0	0	_
モニタリング機能	_	0	_
プロファイル管理機能	0	—	_
ログ管理機能	—	0	0
ファームウェア管理機能	_	_	0
ネットワーク管理機能	_	—	0

1.3.1 インフラ運用管理シーンごとのISM機能イメージ

(1)システムの構築

ICT機器の初期導入、増設を行うシーンでは、ノード管理機能、プロファイル管理機能を活用することにより、システム構築を行えます。





[注1]ハードウェアのモデル名、シリアル番号、IPアドレスなど

[注2]RAIDグループ、ボリューム、ホットスペアおよびAffinity設定

(2)管理対象ノードの監視運用

管理対象ノードの監視運用シーンでは、ノード管理機能、モニタリング機能、ログ管理機能を活用することにより、管理対象ノードの監 視運用を行えます。 図1.4 機能イメージ(管理対象ノードの監視運用)



[注1]ハードウェアのモデル名、シリアル番号、IPアドレス、ラック内搭載位置など

[注2]SNMPトラップ

[注3]ハードウェアログ、オペレーティングシステムログ

(3)管理対象ノードの保守

管理対象ノードの保守シーンでは、ログ管理機能、ファームウェア管理機能、ネットワーク管理機能を活用することにより、管理対象ノードの保守を行えます。

図1.5 機能イメージ(管理対象ノードの保守)



[注1]ハードウェアログ、オペレーティングシステムログ

[注2]ログ検索処理

1.4 構成

ISMは、原則的に管理対象となるサーバとは別に用意したサーバ上で動作します。本書では管理対象となる機器を「ノード」(または「管理対象ノード」)と呼び、ISMが動作しているサーバを「管理サーバ」と呼びます。管理サーバとノード間は、LANで接続します。

ISMのネットワークインターフェースは、1つだけ定義できます。複数のネットワークを構成する場合は、ルータを設定し、各ネットワーク間で通信可能な状態にしてください。

図1.6 ネットワーク構成



機器および機能		説明
ネットワーク	管理LAN	ISMが管理対象ノードの状態監視、制御、データ転送を行うために、管理対象ノードと通信するLANです。セキュリティ確保のため、閉じた接続環境にすることを推奨します。 ISMはIPv6非対応ですので、IPv4で使用してください。
	業務LAN	サーバとクライアント間で業務データを転送するLANです。管理サーバ は接続しません。
管理サーバ	ServerView Infrastructure Manager (ISM)	本ソフトウェアです。 ISMは動作基盤となるソフトウェアを仮想マシン向けにパッケージ化した仮想アプライアンスとして提供されます。仮想マシンにインストール後に、ハイパーバイザーのコンソール、またはSSHクライアント経由で操作できます。
管理端末		管理LANを経由して、ISMを操作するためのパソコン、タブレットなどです。
管理対象ノード	スイッチ ストレージ	ISMが状態監視、制御の対象とするノードです。
	サーバ (管理対象サーバ)	ISMが状態監視、制御の対象とするノードです。 BMC(iRMC)とオンボードLANインターフェースを管理LANに接続します。
関連サーバ	メールサーバ	管理対象ノードの異常や状態の変化をメール送信するためのサーバです。

機器表	および機能	説明
	ディレクトリサービス (OpenLDAP)サーバ	ディレクトリサービスを使用する環境の場合に接続します。
	DHCPサーバ	プロファイル管理機能でOSインストールを行う場合に必要です。 OSインストール先のノード(サーバ)でPXEブートを可能とするため、ノー ドに適切なIPv4アドレスをリースできるように設定してください。

ネットワーク構成の設計および詳細情報については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/

1.5 システム要件

ISMの動作環境となるISM-VA(仮想マシン)および管理端末のシステム要件について説明します。

1.5.1 ISM-VA(仮想マシン)のシステム要件

ISM-VAが動作する仮想マシンのシステム要件は以下のとおりです。

項目	説明
CPUコア数	2コア以上[注1]
メモリ容量	8GB以上[注1]
空きディスク容量	35GB以上[注2][注3]
ネットワーク	1Gbps以上
ハイパーバイザー	Windows Server 2012/2012R2 VMware ESXi 5.5/6.0 Red Hat Enterprise Linux KVM

[注1]管理するノード数に応じて、必要なコア数およびメモリ容量が異なります。

ノード数	CPUコア数	メモリ容量
1~100	2	8GB
101~400	4	8GB
401~1000	8	12GB

[注2]約100ノードを監視するのに必要最低限のディスク容量です。管理するノード数および使用するISM機能に応じて、ディスク容量 を見積もる必要があります。ディスク容量の見積りについては、「3.2.1 ディスク資源の見積り」を参照してください。

[注3]ISM-VAをバックアップする場合は、管理サーバにISM-VAと同等以上の空きディスク容量が必要です。

サポートするハイパーバイザーの最新情報については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

1.5.2 管理端末のシステム要件

GUI(ブラウザ)のシステム要件

ISMのGUIが動作する管理端末のシステム要件は以下のとおりです。

項目	説明
デバイス	パソコン、サーバ、iPad、Androidタブレット
ディスプレイ	・パソコン、サーバ:1280×768ピクセル以上

項目	説明	
	ISM GUIを表示するブラウザのウィンドウサイズを1280×768ピクセル以上にする必要があ ります。	
	・ タブレット:上記デバイスが搭載するディスプレイ	
ネットワーク	100Mbps以上	
Webブラウザ	 パソコン、サーバ: Internet Explorer 「3Dビュー」画面を表示するためには、更新バージョン:11.0.15以降が適用されている 必要があります。 Microsoft Edge Mozilla Firefox Google Chrome iPad:Safari8 Androidタブレット:Google Chrome 	
関連ソフトウェア	Acrobat Reader (マニュアル表示用)	

サポートするデバイスおよびWebブラウザの最新情報については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/infrastructure-software/infrastructure-software/serverviewism/environment/in

ファイル転送用管理端末のシステム要件

管理対象ノードのセットアップに必要なデータやISMのログなど、ISM-VAとファイル転送を行う管理端末のシステム要件は以下のとおりです。

項目	説明
デバイス	パソコン、サーバ
空きディスク容量	8GB以上(DVD 1枚分以上)
ネットワーク	100Mbps以上
必須ソフトウェア	FTPクライアントソフトウェア
関連ソフトウェア	SSHクライアントソフトウェア

1.6 留意事項

OSインストール完了のタイミング

OSの種類、OS設定によってプロファイル適用完了時の状態が異なります。また、プロファイルで指定する任意スクリプトが実行されるタイミングもOSの種類によって異なります。

	OS種類、設定	OSプロファイル適用完了時点の状態	任意スクリプトが実行されるタイミング						
Wir	ndows	OSインストール途中のEULA画面	EULA承諾、ライセンス入力などを完了し、最 初にログインした際						
Lin	ux	OS起動完了し、ログインプロンプトの状態	最初のログインプロンプトの状態(実行済み)						
	RHEL7でX Window有効	OSインストール途中の最終設定画面	最終設定が完了し、OSのログインプロンプト画 面になった時点						
VM (IP	ware ESXi アドレスが固定アドレス)	OS起動が完了し、ネットワーク通信可能と なった状態	OSインストール途中(実行済み)						

OS種類、設定	OSプロファイル適用完了時点の状態	任意スクリプトが実行されるタイミング
VMware ESXi	OSのインストールが完了し、再起動した状	OSインストール途中(実行済み)
(IPアドレスがDHCP設定)	態	

Red Hat Enterprise Linuxの有償サポートサービス(SupportDesk Standard)利用時の注意

有償サポートサービスを契約しサポートを受ける際は、システム構築に対する条件が存在します。

ISMのプロファイル機能を利用したRed Hat Enterprise Linuxの自動インストール時は、サポートに必要な「富士通Linuxサポートパッケージ(FJ-LSP)」の適用やメモリダンプ設定などは行われません。必要な設定はインストール後に手動で実施してください。

設定内容や設定方法などの詳細については、SupportDeskサービスご契約者様向けのLinuxユーザーズマニュアルを参照してください。

ログ管理機能の自動収集を利用する場合

事前に設定したスケジュールに従ってISMが定期的にログを収集できますが、利用する際は以下に注意してください。

- ・ ノードを登録しただけではログは収集されません。ノードごとに収集対象ログの種類とスケジュールを設定してください。
- ・ノード設定やISM上の設定に誤りがあると正しくログが収集できません。設定後は手動ログ収集を実施し、ログファイルが正しく蓄積されていること、またはISMイベントログにログ収集のエラーが記録されていないことを確認してください。
- ・ 収集可能なログファイルの総容量には上限が設定されています。ログの容量が上限の80%に達するとISMのイベントに警告イベントが登録されるので、不要なログを削除してファイル量を削減してください。上限に達するとそれ以上ログが保存されなくなります。
- ・収集したログの保有期間/保有回数はノードごとに設定されており、それを超えた古いログは自動的に削除されます。ログ収集機能の利用時に、適切な設定に変更してください。

ネットワークマップ([管理]-[ネットワークマップ])の表示について

ネットワークデバイスのタイプがCNAの場合、ポートを論理分割する機能が存在します。論理分割機能を有効にしたとき、ネットワーク マップでは、[論理分割元]であるポートの物理ステータスが「?」と表示されてしまいます。そのような場合、ポートのステータスは[論理 分割先]を参照してください。

第2章 ISMの機能

この章では、ISMの機能を説明します。

主要機能の操作手順については、『ServerView Infrastructure Manager V2.0 操作手順書』を参照してください。

2.1 ユーザーインターフェース

ISMのユーザーインターフェースについて説明します。

ISMは、ユーザーインターフェースとして以下を提供します。

- ・ GUI:ISMを操作するためのグラフィカルインターフェース
- ・FTP:FTPクライアントとISM-VA間のファイル転送インターフェース
- ・コンソール:ISM-VAを操作するためのコマンドラインインターフェース

2.1.1 GUI

ISMではWebブラウザで動作するGUIを提供します。

関 ポイント

- ・ 使用するブラウザでCookieおよびJavaScriptを有効にする必要があります。
- ・ Firefoxを使用する場合、サーバ証明書をブラウザに登録する必要があります。
 - 1. Firefoxを起動し、メニューから[オプション]を選択します。
 - 2. [詳細]を選択し、[証明書]をクリックします。
 - 3. [証明書を表示]をクリックします。
 - 4. [サーバ証明書]タブの[例外を追加]をクリックします。
 - 5. [URL]に「https://<ISMサーバIPアドレス>または<ISMサーバFQDN名>:25566/」を入力し、[証明書を取得]をクリックしま す。
 - 6. [次回以降にもこの例外を有効にする]にチェックが入っていることを確認し、[セキュリティ例外を承認]をクリックします。
- ・ Internet Explorerを使用する場合、以下の設定が必要です。
 - 1. Internet Explorerを起動し、メニューから[ツール]-[インターネットオプション]を選択します。
 - 2. [セキュリティ]タブで[レベルのカスタマイズ]ボタンをクリックし、以下の項目で[有効にする]を選択して[OK]ボタンをクリックします。
 - [ActiveX コントロールとプラグイン]配下の[ActiveX コントロールとプラグインの実行]
 - [ダウンロード]配下の[ファイルのダウンロード]
 - [ダウンロード]配下の[フォントのダウンロード]
 - 3. [詳細設定]タブで[マルチメディア]配下の[Webページのアニメーションを再生する]にチェックを付け、[OK]ボタンをクリック します。
- ・ Internet Explorer 11で「3Dビュー」画面を表示するには、Microsoftのサポート技術情報(以下「KB」)2991001が適用されている必要があります。「3Dビュー」画面とは、フロア、ラックの配置、ラック内の機器搭載位置を3次元画像で表示するGUIです。

https://support.microsoft.com/ja-jp/kb/2991001

「3Dビュー」画面でラックが表示されない場合、KB 2991001が含まれるマイクロソフトセキュリティ情報 MS14-051を適用してください。詳細については、以下のWebサイトを参照してください。

https://technet.microsoft.com/ja-jp/library/security/MS14-051

 Google Chromeを使用している場合、使用端末のハードウェア性能やグラフィックドライバなどによっては、WebGL機能(ブラウザ で3Dグラフィックスを表示するための機能)が無効化される場合があります。WebGL機能が無効化されている場合は、「3Dビュー」 画面を表示できません。

WebGL機能の有効/無効は、以下の手順で確認できます。

- 1. Google Chromeを起動し、アドレスバーにchrome://gpuと入力します。
- 2. [Graphics Feature Status] 配下の[WebGL]が[Hardware accelerated] と表示されていれば、WebGL機能は有効です。それ以外の場合は、WebGL機能は無効化されています。

ISM GUIを起動する方法は以下のとおりです。

1. ブラウザを起動し、以下のURLを入力します。

https://<ISMサーバIPアドレス>または<ISMサーバFQDN名>:25566/

2. ログイン画面が表示されますので、ユーザー名、パスワードを入力し、「ログイン」ボタンをクリックします。

セキュリティ証明書の警告が表示された場合は、「4.6 証明書設定」を参照して証明書の設定を行ってください。

🕑 ポイント

初回ログイン時のユーザー名、パスワードは以下を使用してください。このユーザー名でログイン後、デフォルトユーザーのパス ワード変更やユーザーの新規作成を行い運用してください。

- ユーザー名:administrator

ー パスワード:admin

ISM GUIの画面構成は以下のとおりです。

ServerView In	nfrastruct	ire Manager				Language (?)~67 ~	ISMAdministrator V
ダッシュボード	2	19 T	ille v	イベント/タスク ~	D7 ~	各種設定 >		(e)
ノードリスト								
Q 858		0	4 4 4	0 1	3 0 0 1	7 / 17	カラム表示:	基本情報 ・ アウション
•		J-F8 0	€7A 0	иррбия о	シリアル番号 〇	SRADE () 0	更新日 0	1994
۵ ت	0 =	rackswitch-	SR-X316T2	192.168.123.12	41460123	datacenter-1 / floor-1 / rack- 1 / 28	04/15/2015	Lorem ipsum dolor sit am
Π Φ	•	rackawitch- 2	SR-X316T2	192.168.123.13	41460124	datacenter-1 / floor-1 / rack- 1 / 27	04/15/2015	TEST Description2
Π Φ	•	linuxhost-1	PRIMERGY RX2520 M1	192.168.123.14	MASK001110	datacenter-1 / floor-1 / rack- 1/20	04/15/2015	TEST Description3
	•	blade- server1-	PRIMERGY BX900 S2		MA4J001725	datacenter-1 / floor-1 / rack-	04/15/2015	TEST Description4

(a) Language

GUIでの表示言語、日付フォーマット、タイムゾーンの設定を変更します。

(b) ヘルプ

ヘルプおよびガイダンスを表示します。

(c) ユーザー名

ログイン中のユーザー名が表示されます。

ISMからログアウトする場合、ユーザー名にマウスポインターを合わせ[ログアウト]をクリックします。

(d) グローバルナビゲーションメニュー

ISMの各画面に遷移するためのメニューです。

(e) 更新ボタン

クリックすると画面全体を更新します。

ISM GUIでは、同一画面を表示している場合、画面の自動更新は行われません(画面を遷移した場合は、サーバから情報の再取得が行われます)。

最新の情報を確認する場合、更新ボタンをクリックして画面を更新してください。

2.1.2 FTPアクセス

FTPクライアントを使用して、ISM-VA内のファイル転送用領域にFTPアクセスできます。

「3.4.2 ISM初期設定」で設定したIPアドレスを指定して接続します。

ログイン直後は、セキュリティ強化のためファイルおよびディレクトリは非表示になっていますので、ログインユーザーが所属するグループ名のディレクトリに移動し、ファイル転送用領域にアクセスします。

FTPで送受信するファイルの保存先は、下図のように「./<ユーザーグループ名>/ftp」となっています。



・ ユーザーグループ名として指定するディレクトリ名は、ISMのユーザーグループ管理機能で作成するユーザーグループ名または

- Administratorになります。詳しくは、「2.3.1.2 ユーザーグループの管理」を参照してください。
- ・ FTPでファイルを転送する際は、必ず<ユーザーグループ名>ディレクトリ配下の「ftp」ディレクトリ配下を使用してください。
- ・既存ディレクトリの変更・削除はしないでください。
- Microsoft Active DirectoryまたはLDAPと連携しているユーザーでFTPアクセスを行う場合、連携しているパスワードではなく、ISM に登録したパスワードを使用してください。

図2.1 ファイル転送用領域のディレクトリ構成

ftpログインルート



FTPアクセス実行例

Administratorグループに所属する、administratorユーザーでアクセスする場合

```
# ftp 192.168.1.50
Connected to 192.168.1.50 (192.168.1.50).
220 (vsFTPd 3.0.2)
Name (192.168.1.50:root): administrator
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (192, 168, 1, 50, 156, 64).
150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
         ※ログイン直後は何も表示されません
ftp> cd Administrator
250 Directory successfully changed.
         ※ログインユーザーの所属するグループ名のディレクトリへ移動
ftp> |s
227 Entering Passive Mode (192, 168, 1, 50, 156, 64).
150 Here comes the directory listing.
                       1001
                                     33 Jun 16 20:36 bin
drwxr-sr-x
             20
drwxrws---
             3 992
                       989
                                     26 Jun 16 21:54 elasticsearch
drwxrws---
             30
                       1001
                                     21 Jun 16 23:20 ftp
drwxrws---
             20
                       0
                                      6 Jun 16 20:36 imported-fw
                   0
0
0
0
                                      6 Jun 16 20:36 imported-os
drwxrws---
             20
                       0
drwxrws---
             20
                                      6 Jun 16 20:36 ismlog
drwxrws---
             20
                                      6 Jun 16 20:36 logarc
drwxrws---
           80
                                     75 Jun 17 14:03 profile
drwxrws---
             20
                                      6 Jun 16 20:36 tmp
                  1001
drwxrws---
             20
                                      6 Jun 16 20:36 transfer
```

226 Directory send OK. ※ファイル転送用領域にアクセス可能

2.1.3 コンソールアクセス

ハイパーバイザーのコンソール、またはSSHクライアント経由で、管理コマンドを実行できます。 SSHクライアント経由で接続する場合は、「3.4.2 ISM初期設定」で設定したIPアドレスを指定して接続します。 「2.2 ISMの機能説明」の「ポイント」で説明する、Administratorロールを持つユーザーのみ使用可能です。

使用可能なコマンドは、「2.3.5.1 ISM-VA管理機能のコマンド一覧」を参照してください。



[Tab]キーによるコマンドパラメーター補完には対応していません。コマンド入力中に[Tab]キーを押すと、「制限されています」というメッ セージが表示されます。

2.2 ISMの機能説明

管理対象ノードの構築/運用/保守を行うための機能について説明します。

以下の機能について説明します。

- ・ 2.2.1 ノード管理機能
- ・ 2.2.2 モニタリング機能
- ・ 2.2.3 プロファイル管理機能
- 2.2.4 ファームウェア管理機能
- ・ 2.2.5 ログ管理機能
- 2.2.6 ネットワーク管理機能

関 ポイント

ユーザーがISMの各機能を利用するためには、当該ユーザーが登録されたユーザーグループへの権限(ユーザーロール)の割当て が必要です。ユーザーと権限(ユーザーロール)については、「2.3.1 ユーザー管理機能」を参照してください。

以降、ユーザーグループとユーザーロールの組合せと操作実行可否を、以下の表に示すアイコンで表記します。

ユーザーが属するユーザーグループ	ユーザーが持つユーザーロール	実行できる	実行できない
Administratorグループ	Administratorロール	Admin	
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor
Administratorグループ以外	Administratorロール	Admin	Admin
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor

以降の説明では、操作を実行できるユーザーの属性を以下のように示します。

例)



- 上記の表示の場合、以下のユーザー属性を持つユーザーが操作を実行できます。
 - Administratorグループに属し、AdministratorまたはOperatorロールを持つユーザー
 - Administratorグループ以外のグループに属し、AdministratorまたはOperatorロールを持つユーザー
- グレーアイコンで示される、Monitorロールを持つユーザーは、機能を実行できません。

2.2.1 ノード管理機能

ノード管理機能は、データセンター/フロア/ラック/ノードの4階層でノードを管理します。データセンター/フロア/ラック/ノードは以下の意味を持ちます。

- ・ データセンター:データセンター施設の建屋
- ・フロア:データセンター施設内のマシンルーム
- ・ ラック:フロア内に設置されているラック
- ・ ノード: ラック内に搭載されている管理対象機器

以下の機能があります。

- ・2.2.1.1 データセンター/フロア/ラック/ノードの登録
- ・2.2.1.2 データセンター/フロア/ラック/ノードの確認
- ・ 2.2.1.3 データセンター/フロア/ラック/ノードの編集
- ・ 2.2.1.4 データセンター/フロア/ラック/ノードの削除

2.2.1.1 データセンター/フロア/ラック/ノードの登録

ISMでは、ノードの物理的な位置情報を管理できます。位置情報は、「データセンター > フロア > ラック > ユニット番号」という階層構造の中で一意に定められます。

ISMでは、データセンター、フロア、ラック、ノードの各個別情報と、相互の階層構造を設定管理します。

図2.2 データセンター、フロア、ラック、ノードの関係



以下の操作を行えます。

- ・ データセンター、フロア、ラックの登録
- ノードの登録
- ノード情報の管理

- ・ ノードのラック搭載位置情報の管理
- ・ノードのOS情報の登録
- ・ノード検出機能

データセンター、フロア、ラックの登録



ISMにデータセンター、フロア、およびラック情報を追加登録します。登録するデータセンター名、フロア名、ラック名にはISMで一意の 名前を設定する必要があります。

フロアが登録されている場合、GUIで「フロアビュー」画面および「3Dビュー」画面を表示できます。

ラックが登録されている場合、GUIで「ラックビュー」画面を表示できます。

ノードの登録



ISMでノードを管理するためには、ISMにノードを登録する必要があります。

登録の際には、必要な情報を入力します。登録する情報の条件は以下のとおりです。

・ノード名は、ISMで一意な名前を設定する。

すでにISMに登録されているノードと同じIPアドレスまたはシリアル番号を持つノードは登録できません。

ノード情報として、ノードにアクセスするために必要なアカウント情報を設定する。

ISMでは設定されたアカウント情報を使用してノードと通信を行い、ノードの情報取得や監視、プロファイル適用、ファームウェアアップ デート、ログ収集などの処理を行います。対象機種との通信に必要なアカウント情報や、ノードの登録を行う前に必要な設定について は、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/technical/

登録方法には以下の2種類があります。

- ・ 必要な情報を設定して、手動で登録する。
- ・ ISMの検出機能によってノードを検出後、登録する。

ISMに手動で登録する際の操作例を示します。検出機能を利用した登録方法は「ノード検出機能」を確認してください。

1. ノード登録に必要な機器情報を確認します。

ノード登録する前に、登録する機器のモデル名や設定されているIPアドレスなどの情報を確認しておく必要があります。

- 2. 登録に必要な情報を入力します。
 - ー ノード名

ISM全体で、一意な名称を設定してください。

ー ノードタイプ

登録するノードの種類を選択してください。

ー モデル

ノードのモデル名を選択してください。サポート外の機種を登録する場合は、モデル名を入力してください。

ー IPアドレス

ノードのIPアドレスを設定してください。

- Web i/f URL

ノードのWeb管理画面にアクセスするためのURLを設定してください。

一 説明

ノードの説明(コメント)を自由に設定してください。

- 3. ノードのアカウント情報を入力します。
- 4. ノードのラック搭載位置情報を入力します。
- 5. ノードが所属するノードグループを選択します。

ノードグループを設定しない場合、ノードはノードグループ未割当てとなります。未割当てのノードは、Administratorグループの ユーザーのみ管理できます。

6. 登録を実行します。

関 ポイント

複数のISMや監視ソフトウェアから同一のノードを監視することは推奨していません。ノードによって同時にアクセス可能なセション数 があるため、正しく監視できません。

ノード情報の管理



「管理」画面からノードを選択してノード情報を確認できます。

ISMではノードに設定されているアカウント情報を使用して、約24時間周期でノードからノード情報を収集します。最新のノード情報を 取得したい場合には、手動でノード情報取得を実行してください。

ノードの登録直後には、自動でノード情報取得が実行されます。

ノード情報取得の操作例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
- 2. 対象ノードのノード名を選択し、[プロパティ]タブを表示します。
- 3. [アクション]ボタンから[ノード情報取得]を選択します。

ノード情報取得が完了すると、イベントログにメッセージID「10020303」のログが出力されます。

4. 更新ボタンをクリックして、[プロパティ]タブの表示を更新します。

ノードのラック搭載位置情報の管理



ノードのラック搭載位置情報が設定されている場合、GUIの「ラックビュー」画面で確認できます。

ラック搭載位置情報が設定されていない場合、未搭載ノードとして表示されます。

・ ラック搭載位置情報の設定

ラック搭載位置情報はノードの登録時に設定できます。また、ノードの登録後に設定することもできます。

ノードの登録後、ラック搭載位置情報を設定する際の操作例を示します。

ラック搭載位置情報を設定する前に、ラックを登録しておく必要があります。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。

- 2. 対象ノードを選択し、[アクション]ボタンから[ノード位置設定]を選択します。
- 3. ノードを搭載するラックを選択します。
- 4. ノードの配置場所を選択して、適用します。

ノードのOS情報の登録



ISMに登録しているサーバにOSがインストールされている場合、OS情報を登録してください。

OS情報にはOSの種類、IPアドレス、およびOSに接続するためのアカウント情報などが含まれます。

ISMでは、登録されたOS情報を使用して、ノード上でOSの管理下に置かれている情報の取得が行われます。

サポート機器、OSに関する最新の情報は、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

G 注意

・サーバOSをISMから監視対象にするためには、OSごとに導入手順が必要になります。導入手順については、弊社の本製品Web サイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/technical/servervi

・ OS情報が登録されていない場合、またはOSがシャットダウンされている場合、ノード情報を一部取得できなくなります。また、ノード上でOSの管理下に置かれている情報が取得できなくなります。

操作例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
- 2. 対象ノードのノード名を選択し、[OS]タブを表示します。
- 3. [アクション]ボタンから[OS情報編集]を選択します。
- 4. 必要な情報を入力し、適用します。
- 5. [アクション]ボタンから[ノード情報取得]を選択します。

ノード情報取得が完了すると、イベントログにメッセージID「10020303」のログが出力されます。

6. 更新ボタンをクリックして、[OS]タブの表示を更新します。

ノード検出機能



ISMではネットワークに接続されているノードを検出できます。検出機能では、検出したノードから登録の際に必要な情報の一部を自動取得し、登録作業をサポートします。

検出は手動で行います。以下の操作が行えます。

- ・ 手動検出設定を作成し、検出を実行する
- ・ 手動検出結果を確認する
- ・ 検出したノードを登録する

手動検出設定を登録する

手動検出に必要な情報を設定します。指定したIPアドレス範囲に対して、ノードの検出が実行されます。また、設定したアカウント 情報を使用して、登録に必要なノード情報の一部が取得されます。

手動検出を行う前に、検出したいノードに対して、ノードと接続するために必要なアカウント設定を実行しておく必要があります。

対象ノードによって検出に使用されるプロトコルが異なります。

サポート機器、OSに関する最新の情報は、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

- 1. GUIで「登録」画面を表示します。
- 2. [アクション]ボタンから[手動検出]を選択します。
- 3. 手動検出に必要な情報を入力します。
- 4. 手動検出を実行します。

手動検出結果を確認する

「登録」画面の「検出進捗」画面で画面更新を行い、検出処理の完了を待ちます。完了後、「検出ノードリスト」画面で検出されたノードを確認します。

設定したアカウント情報でノード情報取得に成功した場合、ステータスがNormalとなり、取得したノード情報を確認できます。



検出されたノード情報は、同じセション内でのみ有効です。

検出したノードを登録する

手動検出によって検出したノードを登録する際の操作例を示します。

- 1. 検出されたノードを確認します。
- 2. 検出されたノードの中から登録するノードを選択し、[アクション]-[検出ノード登録]を選択します。
- 3. ノード名、シャーシ名、Web i/f URL、説明など、登録に必要な情報を入力します。
- 4. ノードのラック搭載位置情報を設定します。
- 5. ノードグループ情報を設定します。
- 6. 登録を実行します。

ノードのアカウント情報には、ノード検出時にノードへのアクセスに成功したアカウント情報が登録されます。

2.2.1.2 データセンター/フロア/ラック/ノードの確認

ISMに登録されている情報を確認します。

データセンター、フロア、ラックの確認



ISMのGUIでグローバルナビゲーションメニューから[管理]-[データセンター]を選択し、「データセンターリスト」画面を表示します。「データセンターリスト」画面で対象のデータセンターを選択し、画面右側の表示で確認します。

ノードの確認



ISMに登録されているノードを確認します。

ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。対象ノードのノード名を 選択し、[プロパティ]タブを表示することで確認します。

ノードのOS情報の確認



ノードにOSアカウント情報が登録されている場合には、OSからネットワーク、ディスク、カード情報を確認できます。

2.2.1.3 データセンター/フロア/ラック/ノードの編集

ISMに登録されている情報を編集します。

データセンター、フロア、ラックの編集



データセンター、フロア、ラック情報を編集する場合の操作方法を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[データセンター]を選択し、表示される「データセンターリスト」画面 で、対象のデータセンターまたはフロア、ラックを選択します。
- 2. [アクション]ボタンから[データセンター編集]または[フロア編集]、[ラック編集]を選択します。
- 3. 情報を編集します。
- 4. [適用]を実行し、情報の内容を反映します。

ノードの編集



ノード情報を編集する場合の操作方法を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
- 2. 対象ノードのノード名を選択し、[プロパティ]タブを表示します。
- 3. [アクション]ボタンから[編集]を選択します。
- 4. ノード情報を編集します。
- 5. [適用]を実行し、ノード情報の内容を反映します。

2.2.1.4 データセンター/フロア/ラック/ノードの削除

ISMに登録されている情報を削除します。

データセンターの削除



データセンターを削除する場合、データセンター内にフロアが登録されていると削除できません。フロアを削除または移動してからデー タセンターを削除してください。

フロアの削除



フロアを削除する場合、フロア内にラックが登録されていると削除できません。ラックを削除または移動してからフロアを削除してください。

ラックの削除



ラックを削除する場合、ラック内にノードが登録されていると削除できません。ノードを削除または移動してからラックを削除してください。

ノードの削除



ノードの監視情報やノード情報、ログ情報などが削除されます。



複数の端末からログインしている場合、データセンター、フロア、ラック、ノードを削除した際、削除していない端末で削除した対象に対 して操作すると、「存在しないか、既に削除されています」などのエラーが発生することがあります。この場合、以下の方法で画面を更 新してから操作を継続してください。

• ネットワークマップ以外の場合

更新ボタンをクリックします。

• ネットワークマップの場合

[アクション]ボタンから[ネットワーク管理情報の更新]を実行します。

関 ポイント

フロアが登録されているデータセンター、ラックが登録されているフロア、ノードが登録されているラックは削除できません。これと異なり、ノードが登録されているシャーシを削除すると、シャーシとノードが同時に削除されます。

2.2.2 モニタリング機能

モニタリング機能は、以下の用途で利用する機能です。

- ・ ノードの温度などのセンサーの値やCPU使用率などの資源使用状況、ステータスなどの状態をポーリングし、情報を蓄積
- ・ ポーリング結果から事前に指定したしきい値との比較やステータスの変化を基に、状態を監視
- ・ノードからのイベント通知(SNMPトラップ)を受信
- ・ 監視の結果およびノードからのイベント通知を、外部にアラームとして通知 通知方法はアクションとして事前に定義します。

図2.3 モニタリング機能イメージ



モニタリングに関係する設定は、以下の3つがあります。

- ・ 監視項目/しきい値の設定
- アクション設定
- アラーム設定の登録

監視項目/しきい値の設定



監視項目(値の取得対象の項目)としきい値を設定します。

以下の項目については、ノードの登録時にデフォルトで監視項目として登録されます(実際に管理可能な項目の詳細は機種によって 異なります)。

デフォルトの監視対象	説明
統合ステータス	管理対象ノード自身が持つ、システム全体としてのステータス値(overall status)を監視します。
消費電力	管理対象装置全体としての消費電力や部品ごとの消費電力を監視します。
温度情報	筐体内部の温度や、吸気口の温度などを監視します。
各種LEDステータス	Power LED, CSS LED, Identify LED, Error LEDを監視します。

以下の項目については、追加指定により監視できます。

追加の監視対象	説明
各種資源情報	CPU使用率、メモリ使用率などの資源状況を監視します。
FAN回転数	管理対象装置内にある各種FANの回転数を監視します。
Ethernet情報	ポートごとのネットワーク送受信量などを監視します。

監視項目/しきい値の追加手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
- 2. 対象ノードのノード名を選択します。
- 3. [監視]タブを選択します。
- 4. [アクション]ボタンから[追加]を選択し、監視項目を追加します。

アクション設定



通知方法(アクション)のタイプとして以下のものがあります。

通知方法のタイプ	説明
ユーザースクリプトの実行	ユーザーが定義した任意のスクリプトを実行します。
メール送信	ユーザーが定義した任意の内容のメールを送信します。

アクションの追加手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[アラーム]を選択します。
- 2. 画面左側のメニューから[アクション]を選択し、「アクションリスト」画面を表示します。
- 3. 画面右側の[アクション]ボタンから[追加]を選択し、アクションを追加します。

各アクションを使用するときに必要な準備作業

ユーザースクリプトの実行

実行するスクリプトファイルは、ISM-VA上にインポートしておく必要があります。

- 1. アクション設定に使用するユーザースクリプトを用意します。
- 2. ISM-VAにFTPで接続し、スクリプトファイルを転送します。
- 3. ISM-VA管理機能からスクリプトの登録コマンドを実行します。 詳細は、「4.9.2 アクションスクリプト登録」を参照してください。

メール送信

メール送信するためには、SMTPサーバの情報を登録しておく必要があります。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[アラーム]を選択します。
- 2. 画面左側のメニューから[SMTPサーバ]を選択し、「SMTPサーバ設定」画面を表示します。
- 3. 画面右側の[アクション]ボタンから[編集]を選択し、SMTPサーバ情報を登録します。

また、メール送信はS-MIMEによるメッセージの暗号化が可能です。その場合、暗号化に使用するユーザー証明書をISM-VA 上にインポートしておく必要があります。

- 1. アクション設定に使用する個人証明書を用意します。
- 2. ISM-VAにFTPで接続し、証明書ファイルを転送します。 この際、証明書はPEMエンコード形式である必要があります。
- 3. ISM-VA管理機能から証明書の登録コマンドを実行します。 詳細は、「4.9.1 イベント通知メール用証明書登録」を参照してください。

アラーム設定の登録



アラームの設定とは、どのノードで、何が発生した場合に、何を実行するかを事前に定義したものです。

アラームの追加手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[アラーム]を選択します。
- 2. 画面左側のメニューから[アラーム]を選択し、「アラームリスト」画面を表示します。

3. 画面右側の[アクション]ボタンから[追加]を選択し、アラームを追加します。

ISM自身のイベント(例:DVDのインポート完了)に関しては、「対象種別」でシステムを選択してください。

イベントタイプについて

イベントタイプには、以下の種類があります。

イベントタイプ	説明
イベント	ISM内部で検出した各種イベント。
トラップ	監視対象装置から送信されるSNMPトラップ。
	ISM-VA内に登録されているMIB情報を基に、受信可能なトラップの一覧が表示されます。

アラームステータスについて

アラームステータスは各ノードに1つ存在する値で、そのノードに関して何らかのISMイベントやSNMPトラップが検出された場合に変化します。アラームステータスは以下の値を取ります。

アラームステータス	優先度	説明
Error	高	以下のイベントが検出された場合に変化します。
		・ ErrorレベルのISMイベント
		・ CRITICALレベルのSNMPトラップ
		ISMのGUI上では、赤色のベルマーク(🌲)で表現されます。
Warning	中	以下のイベントが検出された場合に変化します。
		・ WarningレベルのISMイベント
		・ MAJORまたはMINORレベルのSNMPトラップ
		ISMのGUI上では、黄色のベルマーク()で表現されます。
Info	低	以下のイベントが検出された場合に変化します。
		・ InfoレベルのISMイベント
		・ INFORMATIONALレベルのSNMPトラップ
		ISMのGUI上では、青色のベルマーク()で表現されます。
None	-	何もイベントが検出されていない状態です。
		ISMのGUI上では、白色のベルマーク()で表現されます。

アラームステータスがInfo以上の値の場合、各レベルに対応したイベントを検出したことを意味します。[イベント/タスク]タブから「イ ベント」画面、または[ログ]タブから「受信トラップ」画面を表示し、検出したイベントの内容を確認してください。

検出したイベントに対して対処・確認が完了した場合は、以下の手順でアラームステータスを解除してください。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
- 2. 対象ノードのノード名を選択します。
- 3. [アクション]ボタンから[アラーム解除]を選択します。

関 ポイント

•••	•••	••	•••	•••	•••	•••	•••	•••	•••	•••	•••	••	••	•••	•••	•••	•••	•••	••	•••	••	•••	••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	••
ア	ラー	ムン	マテ・	ータ	スは	、自	動的	的に	は	解防)さ	れま	ミセ	\mathcal{h}_{c}	,検	出;	され	た	、よ	り優	先月	度の)高	いス	テー	ータ	スが	表表	示さえ	れま	き。					
••	•••	••	•••	• • •	•••	• • •	•••	•••	•••	•••	•••	••	••	••	•••	••	••	•••	••	•••	••	•••	••	•••	••	•••	••	•••	•••	•••	•••	•••	•••	• • •	•••	••

2.2.3 プロファイル管理機能

プロファイル管理機能は主に以下の用途で利用する機能です。

- ・ 管理対象ノードのハードウェア設定を実施
- ・ 管理対象ノードがサーバの場合にOSをインストール
- ・ 管理対象ノードがストレージの場合にRAID/ホットスペアを作成

表2.1 プロファイル管理機能の対象ノードおよび設定可能項目

ノード種別	対象ノード(例)	設定可能項目
サーバ	PRIMERGY RX	・ BIOS設定
	PRIMERGY CX	・ iRMC設定
		・ OSインストール
ネットワークスイッチ	SR-X	・ 管理者パスワード設定
		• SNMP、NTP、STP設定
	VDX	・ 管理者パスワード設定
		・ SNMP、NTP設定
ストレージ	ETERNUS DX	・ RAIDグループ/ボリューム作成
		• グローバルホットスペア作成
		・ Host Affinity設定

ここでは以下について説明します。

- プロファイルの利用方法
- プロファイルとポリシー
- プロファイルグループとポリシーグループ
- ・ ポリシーグループの作成手順
- ・ ポリシーの作成手順
- ・ プロファイルグループの作成手順
- ・ プロファイルの作成手順
- ・ プロファイルの適用手順
- ・ プロファイルの編集と再適用手順
- ・ プロファイルの適用の解除と削除手順
- ・ プロファイルのエクスポート/インポート
- ・ プロファイルグループの編集手順
- ・ プロファイルグループの削除手順
- ・ ポリシーグループの編集手順
- ・ ポリシーグループの削除手順
- ・ OSインストール時に必要な準備作業
- OSインストールの注意事項
- ・ OSインストール後に実行されるスクリプトの指定手順
- ・ プロファイル適用時の動作指定

プロファイルの利用方法

プロファイル管理機能でノード設定を行う際は、事前作業としてノードのハードウェア設定やOSインストール時設定を「プロファイル」と呼ぶ設定の集合体に記述しておきます。

そのプロファイルをノードに割り付ける(適用する)操作を行うことで、設定がノードに反映されます。

プロファイルは管理対象のノードと1対1で適用されます。プロファイルを使って管理するノード1台につき1つのプロファイルが必要です。

図2.4 プロファイルと管理対象のノードの関係



G 注意	
OS関連の設定が記述されたプロファイルをノードに適用すると、プロファイルの内容に従ってOSが新規にイストール済みの既存OSがある場合、設定が変更されるのではなく、既存OSおよびデータは消去されて新規	ンストールされます。イン インストールとなります。

プロファイル例

図2.5 「プロファイル作成」画面例(GUI)

1. 共通情		2.778	3.4815		
8805	IRMC OS OSERINIESE				
0 8932	2225年(RX2520_8005の設定に成存されます。編集不可。)				
CPUIDE					í
	Execute Disable Bit				I
ø	V Hyper-Threading	● #20 ○ #20			I
e	Intel Virtualization Technology	• #00 () #00			I
Ø	V Intel(R) Vt-d	● #30 ○ #30			ī
P	Power Technology	○ 有助 ④ 丸2971ズ ○ 無助			
P	Subhanced Speed Step	€ 400 ○ M00			
e	🗹 Turbo Mode	• #20 (#20			
メモリ設定					
P	DDR Performance	● 電圧単語化 ○ 174.5-単語化 ○ /Dx-マンス単語化			
P	V NUMA	● #30 ○ #30			

プロファイルとポリシー

ポリシーは複数のプロファイル間で同一の設定内容となる部分を抜き出して、一括設定するための仕組みです。ポリシーはプロファイ ルと同様に設定を記述したファイルですが、直接ノードに適用するのではなく、プロファイルがポリシーの内容を参照することで、間接 的にノードに対して設定が行われます。1つのポリシーは複数のプロファイルから参照させることができます。

プロファイルは、ノード1台につき1個必要です。例えば、多数のノードのハードウェア設定を同一内容で設定する場合は、ノード台数 分の同一設定のプロファイルを用意する必要があります。最初に1個のプロファイルを作成したあとに、プロファイルの参照作成機能で ノード台数分のプロファイルを作成できます。ただし、この方法では、全ノードの設定を同一内容で変更したい場合などに、すべての プロファイルに対して修正を繰り返す必要があります。

このような状況が想定される場合は、事前にポリシー機能を利用してプロファイルを作成しておくことで、簡単に設定の一括変更ができます。

図2.6 プロファイルとポリシーの関係

プロファイル (A) プロファイル (B) プロファイル (C) HT=有効 HT=無効 HT=無効	プロファイル (D) HT=有効
VTd=有効	VTd=有効
ポリシー (a) Turbo=有効	Turbo=無効
IP=10.0.0.5 IP=10.0.0.6 IP=10.0.0.7	IP=10.0.0.8
ポリシー(a)とリンク関係を結んでいるプロファイル(A)、(B)、(C)は、ポリポリシー(a)を変更することでプロファイルの内容が変化します。ポリ	リシーを利用しないプロファイル(D)は、 リシー(a)の影響を受けません。
プロファイル (A) プロファイル (B) プロファイル (C) HT=有効 HT=無効 HT=無効	プロファイル (D) HT=有効
VTd=無効	VTd=有効
ポリシー (a) Turbo=無効	Turbo=無効
IP=10.0.0.5 IP=10.0.0.6 IP=10.0.0.7	IP=10.0.0.8



 プロファイルとポリシーは、対象ノードでサポートされる一般的な設定項目を含みます。対象ノードのモデル種別やファームウェア 版数によってはサポートされない設定項目も存在します。適用するノードでサポートされない項目は、プロファイルおよびポリシー では設定しないでください。

・ OSインストールを実行する場合、対象ノードおよび使用するServerView Suite DVDでサポートされていないOSはインストールできません。

関 ポイント

- ・ ポリシーを利用する場合は、プロファイル作成前にポリシーを作成してください。
- ・ ポリシーは、サーバに対するBIOS設定またはiRMC設定に利用できます。

プロファイルグループとポリシーグループ

プロファイル、ポリシーは、グループ単位で管理できます。業務用途別や導入時期別などの任意のグループを作成してプロファイル、 ポリシーを所属させることで、管理が容易になります。

プロファイルはプロファイルグループ、ポリシーはポリシーグループに所属させることができます。
ポリシーグループの作成手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でポリシーグループ作成先を選択した状態で、[アクション]ボタンから[グループ追加]を選択します。

ポリシーの作成手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でポリシー作成先を選択した状態で、[アクション]ボタンから[ポリシー追加]を選択します。
- 3. [ポリシー追加]ウィザードに従い、設定項目を入力します。

ポリシーの設定項目のうち、プロファイルに反映する設定項目は、[ポリシー追加]ウィザードの[2.詳細]で、チェックボックスにチェッ クを付けたうえで設定値を選択します。チェックボックスにチェックを付けない設定項目は、ポリシーの設定がプロファイルに反映 されません。

プロファイルグループの作成手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でプロファイルグループ作成先を選択した状態で、[アクション]ボタンから[グループ追加]を選択します。

プロファイルの作成手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でプロファイル作成先を選択した状態で、[アクション]ボタンから[プロファイル追加]を選択します。
- 3. [プロファイル追加]ウィザードに従い、設定項目を入力します。

プロファイルの設定項目のうち、ノードに反映する設定項目は、[プロファイル追加]ウィザードの[2.詳細]で、チェックボックスに チェックを付けたうえで設定値を選択します。チェックボックスにチェックを付けない設定項目は、プロファイルをノードに適用し ても、プロファイルの設定がノードに反映されません。

プロファイルの適用手順



・対象ノードのWeb操作画面やSSHにログインした状態でプロファイル適用を行うと、プロファイル適用がエラーになる場合があります。

- ・ OSインストールを行う場合、事前に必要な設定とファイルの準備が必要です。以下を参照してください。 「OSインストール時に必要な準備作業」
- 1. プロファイル適用の対象ノードがサーバの場合は、プロファイル適用前にサーバの電源をオフにします。サーバ以外の場合は、 電源をオンにします。
- 2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 3. 「ノードリスト」画面の[カラム表示]欄で[プロファイル]を選択します。
- 4. プロファイル適用対象ノードにチェックを付け、[アクション]ボタンから[プロファイル適用/再適用]を選択します。

関 ポイント

プロファイルの内容によって、プロファイル適用完了までに長時間(例:1時間以上)必要な場合があります。プロファイル適用状況は 「タスク」画面で確認できます。詳細は、「2.3.4 タスク管理」を参照してください。

プロファイルの編集と再適用手順



ノードに適用したプロファイルを変更し、再度ノードに適用することにより、ノードの設定を変更できます。

プロファイルがノードに適用された状態でプロファイルの中身を変更できます。その場合、プロファイルを変更してもノードの設定は連動して変化しません。ISM管理上はプロファイルとノードの設定の不一致という状態となります。

任意のタイミングでプロファイルをノードに対して再適用してください。再適用が完了するとノードの設定が変更され、再びプロファイル とノードの設定が一致した正常状態になります。

プロファイル再適用手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でプロファイル編集先を選択して、右側の一覧からプロファイルを選択します。
- 3. [アクション]ボタンから[編集]を選択し、プロファイルを編集します。
- 4. プロファイル適用の対象ノードがサーバの場合は、プロファイル適用前にサーバの電源をオフにします。 サーバ以外の場合は、電源をオンにします。
- 5. グローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 6. 「ノードリスト」画面の[カラム表示]欄で[プロファイル]を選択します。
- 7. 対象のノードを選択し、[アクション]ボタンから[プロファイル適用/再適用]を選択します。

ノード設定とプロファイルの一致確認手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 2. 「ノードリスト」画面の[カラム表示]欄で[プロファイル]を選択します。

ノードの設定とプロファイルが不一致となっているノードは、[ステータス]に[要再適用]と表示されます。

ノードの設定とプロファイルが一致しているノードは、[ステータス]に[適用済]と表示されます。

プロファイル管理機能を使用せずに直接ノードの設定を変更した場合、ISM画面に表示される適用済みプロファイルの内容とノードの 状態が不一致となります。

- 31 -

プロファイルの適用の解除と削除手順



以下の場合は事前にプロファイルの適用を解除してください。

- ・ 適用済みのプロファイルを削除する場合
- ・ プロファイル適用済みのノードをISMから削除する場合
- ・ プロファイル適用済みのノードをノードグループから外す場合、ノードグループを変更する場合

몓 ポイント

ノードグループについては、「2.3.1 ユーザー管理機能」を参照してください。

プロファイルの適用の解除手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 2. 「ノードリスト」画面の[カラム表示]欄で[プロファイル]を選択します。
- 3. プロファイル適用済みノードにチェックを付け、[アクション]ボタンから[プロファイル解除]を選択します。

プロファイルの削除手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でプロファイル削除先を選択して、右側の一覧からプロファイルを選択します。
- 3. [アクション]ボタンから[削除]を選択します。

ステータスが[未適用]のプロファイルのみ削除できます。

プロファイルのエクスポート/インポート



プロファイルを別のISMで流用したい場合や、適用したプロファイルをISM外に保管しておきたい場合などは、プロファイルをJSON形式で記述されたテキストファイルとしてエクスポート/インポートできます。

関 ポイント

ポリシーについても同様にエクスポート/インポートができます。

プロファイルのエクスポート手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. エクスポート対象のプロファイルを選択します。
- 3. [アクション]ボタンから[エクスポート]を選択します。
- 4. パスワード暗号化キーを設定し(必須)、[エクスポート]ボタンでエクスポートを実行します。

プロファイルのインポート手順

- 1. ISM-VAにFTPで接続し、インポートするプロファイルを転送します。
- 2. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 3. 左側ツリー部でプロファイルの保存先を選択して、[アクション]ボタンから[インポート]を選択します。

4. エクスポート時に設定したパスワードの複合化キーを入力し(必須)、[インポート]ボタンでインポートを実行します。



プロファイルグループの編集手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でプロファイルグループ編集先を選択して、右側の一覧からプロファイルグループを選択します。
- 3. [アクション]ボタンから[編集]を選択し、プロファイルグループを編集します。

プロファイルグループの削除手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でプロファイルグループ削除先を選択して、右側の一覧からプロファイルグループを選択します。
- 3. [アクション]ボタンから[削除]を選択します。

ポリシーグループの編集手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でポリシーグループ編集先を選択して、右側の一覧からポリシーグループを選択します。
- 3. [アクション]ボタンから[編集]を選択し、ポリシーグループを編集します。

ポリシーグループの削除手順



- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[プロファイル]を選択します。
- 2. 左側ツリー部でポリシーグループ削除先を選択して、右側の一覧からポリシーグループを選択します。
- 3. [アクション]ボタンから[削除]を選択します。

OSインストール時に必要な準備作業

・ 事前にOSインストール媒体およびServerView Suite DVDをISM-VA上のリポジトリ領域にコピーしておく必要があります。この作業 を「インポート」と呼びます。

OSインストール媒体のISOイメージをインポートする場合は、ユーザーグループのLVMボリュームサイズを拡張してください。

ServerView Suite DVDのISOイメージをインポートする場合は、システムのLVMボリュームサイズを拡張してください。

ServerView Suite DVDは、ISM上に一度インポートされている場合、再度インポートする必要はありません(ユーザーグループごとのインポートは必要ありません)。

詳細は「2.3.2リポジトリ管理機能」を参照してください。

 対象ノードでPXEブート機能を利用します。オンボードLANからPXEブートが可能なように、ネットワーク接続および対象サーバの BIOS設定を事前に完了させてください。また、ネットワーク内に別途DHCPサーバが必要です。PXEブート時に適切なIPv4アドレ スを対象ノードにリースできるようにDHCPサーバを設定してください。

詳細については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/

OSインストールの注意事項

ネットワーク環境や対象サーバのBIOS設定などに問題がある場合はPXEブートに失敗して、対象サーバでインストール済みOSが起動する場合があります。この場合、OSインストール対象のサーバに対して、ISMによるシャットダウン操作は行われません。プロファイル 適用処理(タスク)はタイムアウト時間経過後にエラー終了します。

タイムアウトでエラー終了する前にプロファイル適用処理を強制的に中止する場合は、タスクをキャンセルしてください。

OSインストール後に実行されるスクリプトの指定手順

OSインストール後に、指定したスクリプトを実行させる場合は、事前にスクリプトファイルをISM-VAにFTPで転送しておく必要があります。

- 1. OSインストール後に実行させたいスクリプトを用意します。
- 2. ISM-VAにFTPで接続し、スクリプトファイルを転送します。

ftpディレクトリ配下にスクリプト用の任意のディレクトリを作成し、その下にスクリプトを転送してください。

FTP転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。

3. プロファイルの追加または編集で、[インストール後のスクリプト実行]の項目にスクリプトファイルを格納したディレクトリと実行する スクリプトファイル名を指定します。

プロファイル適用時の動作指定

通常、プロファイルは新規にノードに適用するか、適用済みの状態でプロファイルを変更したあとに再適用しますが、適用/再適用の GUI操作途中に、「プロファイル適用」画面で[高度な設定を有効にする]にチェックを付けることで、プロファイル適用時の動作条件を 変更できます。また、サーバの場合は、適用する範囲を機能グループ(iRMC、BIOS、OS)ごとに指定できます。

指定可能な動作条件は以下のとおりです。

- ・ 変更がない箇所にも適用を行う
- プロファイル適用状態で、ノードとプロファイル内容が一致している場合でも、ノードに対して設定を上書きします。
- ・ プロファイルをノードに適用せず、ISM上で適用したことにする

ISMの管理上はプロファイル適用を完了させますが、ノードに対する変更は行いません。そのため、適用後にノードの状態とISM 管理状態に差異が発生する場合があります。

2.2.4 ファームウェア管理機能

ファームウェア管理機能は主に以下の用途で利用する機能です。

・ 管理対象ノードで現在動作しているファームウェア版数をISMのGUI上に表示

- 管理対象ノードのファームウェアをアップデート
- ・ ファームウェアデータに添付されているドキュメントを確認

ファームウェア管理機能の対象ノードは以下のとおりです。

- ・ サーバおよび搭載されるPCIカード類
- ストレージ装置
- ・スイッチ

対象ノードの詳細については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/ ここでは以下について説明します。

- ・2.2.4.1 ノードのファームウェア版数の確認
- ・ 2.2.4.2 ファームウェアのアップデート
- ・2.2.4.3 ファームウェアデータに添付されているドキュメントの確認

2.2.4.1 ノードのファームウェア版数の確認



GUIを使った操作例を示します。

- 対象ノードの現在のノード情報を取得します。
 ノード情報取得の詳細は、「2.2.1.1 データセンター/フロア/ラック/ノードの登録」の「ノード情報の管理」を参照してください。
- 2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 3. [カラム表示]欄で[ファームウェア]を選択します。
- 4. 現行バージョン欄を確認します。

現行バージョン欄が現在動作中のファームウェア版数を表しています。

2.2.4.2 ファームウェアのアップデート

以下について説明します。

- アップデート時の動作
- ファームウェアアップデートの実施

ファームウェアをアップデートする場合は、事前にファームウェアをISMにインポートする作業が必要となります。

ファームウェアを富士通のWebサイトなどからダウンロードし(下図(1))、それをISM-VA上のリポジトリに転送します(下図(2)(3))。ISM はリポジトリに配置されたファームウェアを使用して対象ノードのアップデートを実行します(下図(4))。

リポジトリへファームウェアを転送する操作の詳細は、「2.3.2リポジトリ管理機能」を参照してください。

図2.7 ファームウェア管理機能のイメージ



アップデート時の動作

ファームウェアアップデートの対象ノードの種別に応じて、アップデート時およびアップデート後の動作が異なります。 以下に示す表に従ってアップデートを実施してください。

種別	アップデート時およびアップデート後の動作
サーバ(iRMC)	サーバの電源がオン・オフどちらの状態でもアップデートが可能です。
サーバ(BIOS)	サーバの電源がオン・オフどちらの状態でもアップデートが可能です。
	電源オンの状態でアップデートした場合は、新しいファームウェア(BIOS)に切り替えるためにサーバの再起動、および電源をオンにする操作が必要です。再起動は任意のタイミングで行ってください。再起動時に自動でファームウェアの適用が行われ、その後サーバの電源がオフになります。電源オフになったあとで、ISMの「ノード詳細」画面などで電源をオンにすることで新しいファームウェアに切り替わります。
	電源オフの状態でアップデートした場合は、新しいファームウェア(BIOS)に切り替えるためにサーバ の電源をオンにする操作が必要です。ファームウェアのアップデートが完了したタイミングで自動的に 電源がオン状態になり、その後サーバの電源がオフになります。電源オフになったあとで、ISMの「ノー ド詳細」画面などで電源をオンにすることで新しいファームウェアに切り替わります。
サーバ(搭載PCIカード)	サーバで、サポート対象OSが動作している場合にアップデートを実施できます。新しいファームウェア が動作するのは再起動後になります。再起動は任意のタイミングで行ってください。
スイッチ ストレージ	ノードの電源がオンの状態でファームウェアを実施します。ファームウェアアップデート後にノードの再 起動が実施される場合があります。

ファームウェアアップデートの実施





- アップデート中は以下の事項を遵守してください。
 - 対象ノードの電源をオフにしない。
 - 対象ノードの再起動、リセットを行わない。
 - ISMと対象ノードの間のネットワークを切断しない。
 - 管理サーバを再起動しない。管理サーバの電源をオフにしない。
 - リポジトリからファームウェアファイルを削除しない。
- アップデート開始前に、ファームウェア添付のドキュメントなどに記載されている注意事項を確認してください。
- アップデート操作の前に、対象ノードに対して適用可能なファームウェアをインポートしておく必要があります。
 ファームウェアのインポートについては、「2.3.2 リポジトリ管理機能」を参照してください。
- ファームウェアの版数を下げることはできません。
- ネットワークスイッチのアップデート後、スイッチはリセットされるため、通信が一時的に切断されます。ネットワークを冗長化している場合は冗長構成の片側ずつ順番にアップデートするなどしてください。
- ・ ETERNUS DXのファームウェアアップデートを行う際は、Maintainerのロールを持つアカウント情報がISMに登録されている必要 があります。
- PCIカードのファームウェアアップデートを行う際は、PCIカードが搭載されているサーバのOS情報がISMに登録されている必要があります。

ノードのOS情報の登録については、「2.2.1.1 データセンター/フロア/ラック/ノードの登録」の「ノードのOS情報の登録」を参照してください。また、PCIカードのファームウェアアップデートは、OSタイプが以下のもののみ対応しています。

- CentOS
- Red Hat Enterprise Linux
- ・ サーバに搭載されるPCIカードのファームウェアアップデートは、搭載されている同一種類のカードすべてに対して実行されます。

同一種類のカードが複数存在する場合、カードごとに異なるファームウェア版数を指示したり、一部のカードだけをアップデート対象とすることはできません。ISM画面上で一部のカードだけをアップデート対象に指定した場合や、それぞれ異なるファームウェア版数を指定した場合も、同一種類のカードはすべてファームウェアアップデートが実行され、アップデートされる版数は指示したファームウェア版数の中において、最も新しい版数となります。

 ・以下のPCIカードのファームウェアアップデートを行う際には、それらが搭載されているサーバにEmulex OneCommand Manager CLIが導入されている必要があります。

ファームウェア名:LPe1250、LPe12002、LPe16000、LPe16002、OCe10102、OCe14102

Emulex OneCommand Manager CLIの導入については、「2.3.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの導入」を参照してください。

 ・以下のPCIカードのファームウェアアップデートを行う際には、それらが搭載されているサーバにQlogic QConvergeConsole CLIが 導入されている必要があります。

ファームウェア名:QLE2560、QLE2562、QLE2670、QLE2672

Qlogic QConvergeConsole CLIの導入については、「2.3.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの 導入」を参照してください。

・以下のPCIカードの現行バージョン欄と最新バージョン欄に表示される版数のフォーマットは異なります。

ファームウェア名:QLE2560、QLE2562、QLE2670、QLE2672

現行バージョン欄には<ファームウェアバージョン>_<BIOSバージョン>が表示され、最新バージョン欄には<BIOSバージョン >が表示されます。

- ・サーバ搭載のPCIカードおよびサーバのBIOSのアップデートでは、ISM上でアップデート処理が完了しても古いファームウェアで 動作しています。新しいファームウェアに動作を切り替えるために、以下の手順を行ってください。
 - サーバ搭載のPCIカードをアップデートした場合は、新しいファームウェアに切り替えるためにサーバの再起動が必要です。再 起動は任意のタイミングで行ってください。
 - 電源オンの状態でサーバのBIOSをアップデートした場合は、新しいファームウェア(BIOS)に切り替えるためにサーバの再起動、および電源をオンにする操作が必要です。再起動は任意のタイミングで行ってください。再起動時に自動でファームウェアの適用が行われ、その後サーバの電源がオフになります。電源オフになったあとで、ISMの「ノード詳細」画面などで電源をオンにすることで新しいファームウェアに切り替わります。
 - 電源オフの状態でサーバのBIOSをアップデートした場合は、新しいファームウェア(BIOS)に切り替えるためにサーバの電源 をオンにする操作が必要です。ファームウェアのアップデートが完了したタイミングで自動的に電源がオン状態になり、その後 サーバの電源がオフになります。電源オフになったあとで、ISMの「ノード詳細」画面などで電源をオンにすることで新しいファー ムウェアに切り替わります。
- ・ファームウェアアップデート処理が正常に開始できない場合やアップデートに失敗した場合、通常はISMのアップデート処理はエ ラー終了します。しかし、アップデート途中で対象ノードが応答しなくなる場合などはタイムアウトエラーの検出は行いません。

想定される作業時間を大きく超えても処理が完了しない場合は、対象ノードの状態を直接確認してください。異常の場合は、ISM 上のファームウェアアップデートのタスクをキャンセルしてください。

目安となるファームウェアアップデートの処理時間については、Webに記載される情報を参照してください。

1. 対象ノードをメンテナンスモードに設定します。

メンテナンスモードの設定については、「5.1 メンテナンスモード」を参照してください。

- 2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 3. [カラム表示]欄で[ファームウェア]を選択します。
- 4. アップデートを行うノードの「現行バージョン」と「最新バージョン」を確認します。
- 5. アップデートを行うノードにチェックを付け、[アクション]ボタンから[ファームウェア更新]を選択します。
- 6. 画面表示に従い、操作を実行します。

[適用]実行後に結果確認ダイアログボックスが表示されただけでは適用そのものは完了していません。アップデート開始後、作業がISMのタスクとして登録されますので、作業の状況を「タスク」画面で確認してください。

[適用]実行後の結果確認ダイアログボックスの「タスク詳細:」欄にタスクIDが表示されます。

ファームウェアアップデートのタスクは、タスクタイプが「Updating Firmware」で登録されます。

ISMのGUIでグローバルナビゲーションメニューから[イベント/タスク]-[タスク]を選択すると、「タスク」画面にタスクの一覧が表示 されます。タスクID、タスクタイプを基に対象のタスクを識別してください。

7.「タスク」画面で該当タスクの完了を確認後、対象ノードのメンテナンスモードを解除します。

2.2.4.3 ファームウェアデータに添付されているドキュメントの確認

ファームウェアアップデートを実行する際、ファームウェアインポート時に取り込んだドキュメントを確認できます。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 2. [カラム表示]欄で[ファームウェア]を選択します。
- 3. アップデートを行うノードにチェックを付け、[アクション]ボタンから[ファームウェア更新]を選択します。
- 4. プルダウンメニューから更新バージョン、リポジトリを選択して、[次へ]ボタンをクリックします。
- 5. [ドキュメントURL]欄で確認したいドキュメントのURLを選択し、ドキュメントを確認します。

🕑 ポイント

・ ISMを使用したアップデートの方法は、ファームウェアに添付されているドキュメントに記載されている方法とは異なります。

サーバのiRMC/BIOSのOnlineアップデート方法は、ファームウェアに添付されているドキュメントの「オンラインアップデート」とは異なり、「リモートアップデート」に相当する処理が行われます。ファームウェアはISM-VA内のTFTPサーバから、対象サーバのiRMC Webインターフェースを利用して転送されます。

2.2.5 ログ管理機能

ログ管理機能は主に以下の用途で利用する機能です。

- ・ ノードのログを、指定したスケジュールで定期的に収集
- ・ ノードのログを、任意のタイミングで収集
- ・ GUI画面上での参照やファイルのダウンロードを実施

ISMでは、「取得するログの種類」や「収集スケジュール」をノードごとに設定できます。

その設定に従ってノードから収集したログデータのひとかたまりを「保管ログ」と呼びます。

保管ログは、各ノードから収集されたログファイルがそのままのデータ形式で管理サーバ内に保管されます。任意のタイミングでISMの GUIを操作して、保管ログをZIPファイルにして管理端末にダウンロードできます。

保管ログの任意のログファイルは、収集後直ちに、ISMの基準に従って「イベントログ」「操作ログ」「セキュリティログ」に分類されます。 管理サーバ内には、GUIに一覧(検索)表示するための「ログ検索用データ」と、ダウンロードするための「ダウンロード用データ」とし て、別々に蓄積されます。ISMでは、この状態のログをまとめて「ノードログ」と呼びます。

「ノードログ」はGUIに一覧表示され、さらに「イベントログ」「操作ログ」「セキュリティログ」での分類や発生日時などで表示内容をフィル タリングできます。また、フィルタリングされたログの一覧をCSVファイルやZIPファイルとして、管理端末にダウンロードできます。

図2.8 ログ管理機能のイメージ





ISMは保管ログのフォーマットを解析し、「イベントログ」「操作ログ」「セキュリティログ」に分類します。各ノードのログメッセージのフォーマットは、OSのデフォルト状態から変更しないでください。

例えばLinuxのオペレーティングシステムログの場合、OSのシステムログの設定でログメッセージのフォーマットが変更されると、ISMは そのログを認識できなくなり、正しいノードログを作成できなくなります。

以下について説明します。

- ・ 収集可能なログの種類
- ・ログ保有期間の設定
- ・ログ収集対象と収集日時の設定
- ・ログ収集の動作
- ノードログの検索
- ノードログのダウンロード
- 保管ログのダウンロード
- ノードログの削除
- ・ 保管ログの削除

収集可能なログの種類

ログ管理機能は、ハードウェアログ、オペレーティングシステムログ、ServerView Suiteログの3種類のログが収集可能です。サポートするハードウェアやOSなどの詳細は、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

ハードウェアログ

各種管理対象ノードの装置ログを収集します。

種別	収集対象ノード	収集する保管ログ種類	解析および蓄積されるノードログ種類
サーバ	PRIMERGY	SEL	SEL
ストレージ	ETERNUS DX	export logコマンドの出力結果 show eventsコマンドの出力結果	show eventsコマンドの出力結果
スイッチ	SR-X	show tech-supportコマンドの出力結果	show logging syslogコマンドの出力結果 (show tech-supportコマンドの出力結果に含 まれている)
	VDX	copy supportコマンドで作成される各種ファ イル	show logging raslogコマンドの出力結果 show logging auditコマンドの出力結果 (copy supportコマンドで作成される<任意 の文字列>.INFRA_USER.txt.gzファイルに 含まれている)

オペレーティングシステムログ

管理対象サーバ上で動作しているOSのログを取得します。

取得対象のOS	収集するログ種類		
	OS上での名称 ISM上での分類		
Windows	イベントログ(システムログ/アプリケーションログ)	オペレーティングシステムログ(イベントログ)	
	イベントログ(セキュリティログ)	オペレーティングシステムログ(セキュリティログ)	
Linux	システムログ (/var/log/messages)	オペレーティングシステムログ(イベントログ)	

取得対象のOS	収集するログ種類		
	OS上での名称	ISM上での分類	
	システムログ (/var/log/secure)	オペレーティングシステムログ(セキュリティログ)	
VMware ESXi	システムログ (syslog.log)	オペレーティングシステムログ(イベントログ)	

G 注意

仮想マシン上で動作しているOSは取得対象外です。

ServerView Suiteログ

管理対象サーバ上で動作しているソフトウェア(ServerView Suite製品)のログを取得します。

取得対象のソフトウェア	収集するノードログ種類
ServerView Agents	PrimeCollectコマンドの出力結果
ServerView Agentless Service	PrimeCollectコマンドの出力結果
ServerView RAID Manager	動作ログ(RAIDLog.xml、snapshot.xml)



- 仮想マシン上で動作しているServerView Suiteログは取得対象外です。

- ServerView Suiteログは、ノードログ作成対象外です。

ログ保有期間の設定



ログの保有期間は、分類された「イベントログ」「操作ログ」「セキュリティログ」のそれぞれに対して別々に設定できます。また、分類前の「保管ログ」についても別途保有世代数を設定できます。

ログの保有期間は任意の値に設定できます。

「イベントログ」「操作ログ」「セキュリティログ」は、それぞれの保有期間を日数で設定します。指定した日数より古いタイムスタンプのログは削除されます。デフォルトでは過去30日分が保有される設定になっています。設定可能な範囲は1日~1830日(約5年分)です。

「保管ログ」はスケジュール動作または任意タイミングの収集を一回とカウントしたときに、過去何世代分を保有しておくかを設定します。設定した世代数より古い「保管ログ」は削除されます。デフォルトでは過去7世代分が保有される設定になっています。設定可能な範囲は1~366世代です。

関 ポイント

「イベントログ」「操作ログ」「セキュリティログ」「保管ログ」のそれぞれの保有期間、保有世代数は互いに影響しません。

例えば、「イベントログ」「操作ログ」「セキュリティログ」のそれぞれの保有期間が30日に設定されている状態で、対象ノードには過 去1年分のログが蓄積されている場合、ログ収集を実行すると、「保管ログ」には1年分すべてが保存されます。「イベントログ」「操 作ログ」「セキュリティログ」は過去30日より古いログは保存されません。

・最初のログ収集を実行する前に、保有期間の設定が運用に最適な値となっていることを確認してください。

デフォルトでは、「イベントログ」「操作ログ」「セキュリティログ」のそれぞれの保有期間は30日に設定されています。

最初のログ収集でノードから「保管ログ」を取得したとき、30日分より古いログは「イベントログ」「操作ログ」「セキュリティログ」のそれ ぞれには蓄積されません。 2回目以降のログ収集の前に保有期間を30日より大きな値に変更しても、30日以前のノードログは遡って蓄積されることはありません。

過去30日より前のログを蓄積したい場合は、最初のログ収集を実行する前に、ログ保有期間の設定を30日より大きな任意の値に 変更してください。

ログ収集対象と収集日時の設定



ISMにノードを登録しただけでは、ノードからのログ収集を適切に行うことはできません。

ノードからログ収集を行うとき、各ノードで以下の内容を設定しておく必要があります。

ログ収集ターゲット

収集対象とするログの種類を「ハードウェア」「オペレーティングシステム」「ServerView Suite」の中から任意に組み合わせて指定します。

収集対象ノードがサーバ以外の場合は、「ハードウェア」だけが指定できます。

1つも選択しなければログの収集は行われません。

・保有期間(すべて必須)

イベントログ:保有しておく最大日数を設定します。

操作ログ:保有しておく最大日数を設定します。

セキュリティログ:保有しておく最大日数を設定します。

保管ログ:保有しておく最大世代数を設定します。

ノードからのログ収集は、以下の2通りの実行方法があります。

- ・ 任意のタイミングで手動実行する
- ・ スケジュールに従って自動実行する

ログの取得をスケジュールに従って定期的に自動実行したい場合は、それぞれのノードで実行スケジュールを設定します。



ISMは、ノードからの情報を取得し確認したうえで、そのノードが「ハードウェアログ」「オペレーティングシステムログ」「ServerView Suite ログ」の各種ログの収集対象として有効であるかどうかを判定します。

ログ収集ターゲットの設定において、本来は設定可能であるべき「ハードウェアログ」「オペレーティングシステムログ」「ServerView Suite ログ」が設定不可能な状態になっている場合は、そのノードからの情報取得が正常に完了していない可能性があります。

- ・「ハードウェアログ」が設定不可能な場合は、管理サーバとノードとのネットワーク接続や、ノードプロパティの設定(特にネットワーク関連項目)を再度確認したあと、[ノード情報取得]を再実行してください。
- ・「オペレーティングシステムログ」「ServerView Suiteログ」が設定不可能な場合は、ノードのOS情報の内容が正しく登録されている かを確認したあと、[ノード情報取得]を再実行してください。
- ・「ServerView Suiteログ」は、ログ収集に対応したServerView Suite製品 (ServerView Agents、ServerView Agentless Service、 ServerView RAID Manager) がインストールできるOSである場合のみ設定可能な状態となります。

定期ログ収集を行う場合は、スケジュールを設定します。

ノード1台ごとに設定したスケジュールで、指定した種類のログを収集し、ISM-VAの定められた領域に保管しておくことができます。 収集スケジュールの指定は以下の2種類が可能です。 • 曜日指定

曜日ごとにログ取得の時刻を指定します。ログを取得する曜日と時刻を「毎週〇曜日の〇時〇分」のように指定します。また、「毎月の第△〇曜日の〇時〇分」といった指定も可能です。

例1)毎週日曜日23:00にログ取得

例2)毎月の第一月曜日の12:10にログ取得

例3)毎週水曜日の11:00と金曜日の18:00にログ取得

• 日付指定

毎月の決まった日、または最終日ごとにログ取得の時刻を指定します。

例1)毎月10日の11:00と20日の18:00にログ取得

例2)毎月最終日の23:50にログ取得

GUIを使った設定操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 2. [カラム表示]欄で[ログ設定]を選択します。
- 3. 設定対象のノードにチェックを付けます。複数のノードにチェックすると、同様の内容を一度に設定できます。
- 4. [アクション]ボタンから[ログ収集設定編集]を選択します。

ログ収集の動作



定期ログ収集

定期ログ収集は、ノードのログを指定したスケジュールで定期的に収集して蓄積します。

定期ログ収集を行うためには、ログ収集のスケジュール設定を行う必要があります。

スケジュール設定時刻になると、自動的にログ収集が開始されます。



 定期ログ収集では収集開始時刻にログ収集できない状態だった場合は、収集がスキップされて次回のスケジュール日時で取得されます。

ログ収集できない状態の例を示します。

- ノードからのログ収集が正常に実施できない(電源がオフになっている、ネットワーク通信できないなど)
- ノードに対してISMで別の操作を実施している
- ノードがメンテナンスモードになっている(手動での取得は可能)
- ISMが停止している

ログ収集できなかった場合は、ISMの[イベント/タスク]-[イベント]-[運用ログ]にエラーイベント(メッセージIDが「5014」で始まる ログ)が登録されます。

- ノードの種類によっては、ログ収集に時間がかかることがあります。そのため、ログ収集のスケジュール時刻と保有しているログのタイムスタンプに大きな差が生じる場合があります。
- 一同時にログ収集可能なノード数には上限があります。上限数のログ収集が実行中の場合、あとから開始するログ収集はすぐに 実行されず、先に実行しているログ収集が終了してから実行されます。
- ログ収集中は、ログ削除処理は保留されます。

手動ログ収集

ノードのログを任意のタイミングで収集して蓄積します。

GUIを使ったログ収集操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
- 2. [カラム表示]欄で[ログ設定]を選択します。
- 3. ログ収集対象のノードにチェックを付けます。複数のノードにチェックすると、同様の内容を一度に設定できます。
- 4. [アクション]ボタンから[ログ収集実行]を選択します。

「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。

5. [イベント/タスク]-[タスク]を選択し、処理状況を確認します。

タスクタイプは、[Collecting Node Log]と表示されます。

タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。



- 手動ログ収集を1回実行するたびに、保管ログの保有世代数が加算されます。連続して何度も実行すると、保有最大世代数の
- 設定を超えた過去のログが削除されますので注意してください。なお、手動ログ収集がエラーとなった場合は世代数にカウント されません。

- ログ収集中の場合、ログ収集が完了するまで、ログ削除処理は保留されます。

ログ保管先のディスク容量監視機能

ログファイルは、ノードが所属しているユーザーグループのログ保存領域に保管されます。

本機能はユーザーグループのログ保存領域の容量を監視します。

保管されるログファイルの最大容量は、保管ログ、ノードログ(ダウンロード用データ)、ノードログ(ログ検索用データ)それぞれ10GB で設定されています。この設定値は変更できません。それぞれのログファイル容量が設定値に近づくと、ISMの[イベント/タスク]-[イ ベント]-[運用ログ]に警告/エラーイベントが登録されます。設定値を超えた(エラーイベントが登録された)場合は、新たなログは取 得されません。

警告/エラーイベントが登録された場合、イベントが発生したノード、または、同じユーザーグループに所属している別ノードに対して、手作業で不要なログを削除するか、保管期限を超えたログが自動削除されて空き領域が増えると、新しいログが取得されるようになります。

条件	動作
ログのデータ量が設定した容量の80%を超	・ログ収集は行う。
えた場合	・ [イベント]-[運用ログ]に警告イベントが出力される。
	表示されるメッセージは以下のような内容になります。
	ー 保管ログの場合
	保管ログ保存領域のデータ量がしきい値を超過しました。
	「保管ログの削除」参照
	ー ノードログ(ダウンロード用データ)の場合
	ノードログ(ダウンロード用データ)保存領域のデータ量がしきい値 を超過しました。
	「ノードログの削除」参照
	- ノードログ(ログ検索用データ)の場合
	ノードログ(ログ検索用データ)保存領域のデータ量がしきい値を超 過しました。

条件	動作	
	「ノードログの削除」参照	
ログのデータ量が設定した容量を超えた場	・ログ収集を行わない。	
合	・ [イベント]-[運用ログ]にエラーイベントが出力される。	
	表示されるメッセージは以下のような内容になります。	
	- 保管ログの場合	
	保管ログ保存領域の設定容量を超過しました。	
	「保管ログの削除」参照	
	ー ノードログ(ダウンロード用データ)の場合	
	ノードログ(ダウンロード用データ)保存領域の設定容量を超過しま した。	
	「ノードログの削除」参照	
	ー ノードログ(ログ検索用データ)の場合	
	ノードログ(ログ検索用データ)保存領域の設定容量を超過しました。	
	「ノードログの削除」参照	

ノードログの検索



蓄積された「ノードログ」から、指定したキーワードを含むログを検索して表示できます。

「ノードログ」画面を開いた初期状態では、ノードごとに蓄積された「ノードログ」がひとまとめに一覧表示されます。

GUIを使ったログの検索操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[ログ]-[ノードログ]を選択します。
- 2. GUI上の検索用テキストボックスにキーワードを入力します。

入力したキーワードを含むログが表示されます。

次にGUIを使ったログのフィルタリング操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[ログ]-[ノードログ]を選択します。
- 2. [フィルター]ボタンをクリックします。
- フィルター画面で条件を入力し、[フィルター]ボタンをクリックします。
 入力した条件に合致したログが表示されます。

믿 ポイント

ログの簡易的なダウンロード機能として、GUI画面の現在の表示内容をCSVファイルとして出力できます。CSV出力は、[アクション]ボ タンから[表示内容ダウンロード(CSV)]を選択することで実行できます。

ノードログのダウンロード



蓄積しているノードログを期間、種別を指定してダウンロードできます。

また、複数のノードのログをまとめてダウンロードできます。

ダウンロードファイルは、1つのzipファイルに圧縮されます。

また、zipファイルにパスワードを設定することもできます。

GUIを使ったログのダウンロード操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[ログ]-[ノードログ]を選択します。
- [アクション]ボタンから[ダウンロードファイル作成]を選択します。
 「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。
- 3. ダウンロード用ファイルの作成完了を待ちます。

[イベント/タスク]-[タスク]を選択し、処理状況を確認します。

タスクタイプは、[Creating Node Log download file]と表示されます。

タスクIDは、[ダウンロードファイル作成]実行後に表示される「結果」画面のタスク詳細の番号を確認してください。

4. ダウンロード用ファイルの作成が完了したら、[アクション]ボタンから[ダウンロードファイル確認]を選択します。

注意

ISMでは、ダウンロードファイルは常に1つしか保持できません。そのため、ログのダウンロード操作を連続で実行した場合、以前に作成されたダウンロードファイルは削除されます。

ダウンロードしたログは、以下のファイル名になります。

ダウンロードファイル名

Log_<ダウンロード指定期間>.zip

<ダウンロード指定期間>のフォーマットは<指定開始日>-<指定終了日>となり、それぞれYYYYMMDD(年月日)で表示されます。

例)2016年6月1日~2016年6月7日の期間を指定した場合

Log_20160601-20160607.zip

zipファイルの展開後のフォルダー構成は以下のとおりです。

• フォルダー構成

<ノード名>_<ノードID>¥<カテゴリー>¥<ログ種別>

<カテゴリー>のフォーマットは、「hardware/os」です。

<ログ種別>のフォーマットは、「event/operation/security」です。

保管ログのダウンロード



保管ログをダウンロードできます。また、同一ノードの複数の世代のログや複数ノードのログをまとめてダウンロードできます。ダウンロードファイルは、1つのzipファイルに圧縮されます。また、zipファイルにパスワードを設定することもできます。

GUIを使ったログのダウンロード操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[ログ]-[保管ログ]を選択します。
- 2. ダウンロードする保管ログにチェックを付けます。

複数の保管ログにチェックを付けると、それらは1つのzipファイルにまとめられた状態でダウンロードされます。

3. [アクション]ボタンから[ダウンロードファイル作成]を選択します。

「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。

4. ダウンロード用ファイルの作成完了を待ちます。

[イベント/タスク]-[タスク]を選択し、処理状況を確認します。

タスクタイプは、[Creating Archive Log download file]と表示されます。

タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。

5. ダウンロード用ファイルの作成が完了したら、[アクション]ボタンから[ダウンロードファイル確認]を選択します。



ISMでは、ダウンロードファイルは常に1つしか保持できません。そのため、ログのダウンロード操作を連続で実行した場合、以前に作成されたダウンロードファイルは削除されます。

ダウンロードしたログは、以下のファイル名になります。

ダウンロードファイル名

Material_<ダウンロードファイル作成日時>.zip

zipファイルの展開後のフォルダー構成は以下のとおりです。

• フォルダー構成

<ノード名>_<ノードID>¥<日時>_<ノード名>_<ノードID>¥<カテゴリー>

<日時>のフォーマットは、「YYYYMMDDhhmmss(年月日時分秒)」です。

<カテゴリー>のフォーマットは、「hardware/software」です。

ノードログの削除



設定した保有期間を経過したノードログ(ダウンロード用データ、およびログ検索用データ)は自動的に削除されますが、手動で任意のノードログを個別に削除することもできます。その場合、ノード名や期間、ログの種類を条件として、対象を絞り込んだうえで削除を実行します。

ダウンロード用データ、およびログ検索用データは、同じ対象のデータが同時に削除されます。

GUIを使ったノードログの削除操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[ログ]-[ノードログ]を選択します。
- [アクション]ボタンから[ログ削除]を選択し、画面に従ってログの削除を実行します。
 「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。
- 3. [イベント/タスク]-[タスク]を選択し、処理状況を確認します。

タスクタイプは、[Deleting Log files]と表示されます。

タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。



- ノードログの削除には時間がかかることがあります。このため、削除処理が完了するまで、GUIに削除対象とした保管ログが表示されてしまう場合があります。この場合、「タスク」画面の該当タスクでノードログの削除処理完了を確認し、本画面を再表示してください。
- 大量のノードログを一度に削除するときは、削除に数分から数時間かかる場合があります。なお、選択したノードのすべてのログを 削除してもよい場合は、削除条件の[種類]にすべてのログ種類を選択し、[期間]に削除当日の日付を指定することで、短時間で 削除できます。
- ・ノードログの削除が完了するまで、ログ収集処理は保留されます。

保管ログの削除



設定した保有回数を超えた保管ログは自動的に削除されますが、手動で任意の保管ログや保有世代を指定して蓄積された保管ログ を個別に削除することもできます。

GUIを使った保管ログの削除操作の例を示します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[ログ]-[保管ログ]を選択します。
- 2. 削除するファイル名にチェックを付けます。複数のファイル名にチェックすると、一度に削除できます。
- 3. [アクション]ボタンから[削除]を選択し、画面に従って削除を実行します。

「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。

4. [イベント/タスク]-[タスク]を選択し、処理状況を確認します。

タスクタイプは、[Deleting Log files]と表示されます。

タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。



保管ログの削除には時間がかかることがあります。このため、削除処理が完了するまで、GUIに削除対象とした保管ログが表示されてしまう場合があります。この場合、「タスク」画面の該当タスクで保管ログの削除処理完了を確認し、本画面を再表示してください。

保管ログの削除が完了するまで、ログ収集処理は保留されます。

2.2.6 ネットワーク管理機能

ネットワーク管理機能は主に以下の用途で利用する機能です。

- ・ 管理対象ノード間の物理のネットワーク接続情報やポートの情報を確認
- ・ 管理対象ノード間のネットワーク接続情報の変化を確認
- VLAN、LAG設定を確認

ServerView Infrastructure Manager			© م¢۲ ۲ المطالب ۲۵۲۲ ۲۰	รบตัวร
ダッシュホード ノード登録 ノード	140 × 140h/920 × 7-	-カイブ * 各種設定 *		2
₽»トワークノーFUスト <	1407- VFAB-B			
₩ ₩ ±-/(-	blade-server1-mmb1	- ON/OFF	8.8E-11 M02- ▼ 7	95a> ~
G blade-server1-mmb1			· · · · · · · · · · · · · · · · ·	
Bo blade-server1-mmb2	blade-server1-chassis			1
By blade-server1-server1				
inuxhost-1	> biade-server1-server1			
 ・コンパージドファブルク 	> A blade-server1-mmb1	v 📷 rada	sitch-1 > "@ blade-server1-s	witch1
110 C-Fabric		ether 1 ether 3	ether 2 m	
✓ ₩0122.49F			/	
blade-server1-switch1	> 🔥 inuhost-1	> % rada	shch-2	
Tackswitch-1				
*** rackswitch-2				
Tackswitch-3	<			>
			100% -	

以下について説明します。

- ネットワーク接続情報の表示
- ・ ネットワーク管理情報の更新
- ネットワーク接続の変化情報の確認
- ・ ネットワーク接続の変化情報の基準設定
- ・ VLAN、LAG設定の確認
- 手動でのネットワーク接続情報の設定

ネットワーク接続情報の表示



管理対象ノード間のネットワーク接続情報をネットワークの接続図(ネットワークマップ)としてグラフィカルに確認できます。簡単な操作 で各管理対象ノードやそのポートの状態を含む詳細な情報が表示されます。サーバ、ネットワークスイッチの接続関係を1つの画面で 確認できます。

操作手順

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

ネットワークノードリストは、[<]アイコンをクリックすることで左端に格納できます。

ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。
 ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。
 画面中央にネットワークマップが表示されます。

🕑 ポイント

ネットワークマップでは、ネットワークノードリストから選択したノードと接続関係にあるノードが表示されます。ネットワークマップ上のノー ドの[>]アイコンをクリックすると、ノード内のポートが展開表示されます。



- ネットワークの接続情報はLLDP(Link Layer Discovery Protocol)を利用して取得されます。LLDPに対応していないノードやLLDP が無効になっている場合、実際に接続が存在していても接続情報は取得できません。ノードのLLDP対応の有無、ノードのLLDP 設定の有効・無効の確認方法については、各ノードの仕様を確認してください。
- 表示される接続図は、前回の[ネットワーク管理情報の更新]操作時に取得した状態、またはISMによる1日1回の定期的なネット ワーク管理情報の更新時の状態になります。ノード登録後、接続変更後または異常発生時などに最新状態を確認する場合は[ア クション]ボタンから[ネットワーク管理情報の更新]を実行してください。
 また、ノードのハードウェア構成変更後は、対象ノードの「ノード詳細」画面で[ノード情報取得]を実行後に、[ネットワーク管理情報の更新]を実行してください。定期的なネットワーク管理情報の更新は、AM4:00に実行が開始されます。

ネットワーク管理情報の更新



ネットワーク接続情報は定期的に最新情報に更新されます。また、ユーザーの任意のタイミングで手動更新することもできます。以下 はネットワーク管理情報の更新の操作手順です。

操作手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
- 2. [アクション]ボタンから[ネットワーク管理情報の更新]を選択します。
- 3. [更新]ボタンをクリックします。



ネットワーク管理情報の更新中に、ネットワーク接続情報の取得および、各ノードへの設定はできません。情報更新の完了後に操作し てください。

関 ポイント

 ネットワーク管理情報の更新は管理対象ノードの数に応じて時間がかかります。情報更新の完了は、イベント/タスクの運用ログで 更新の完了を示すイベントを確認してください。

- ・ ネットワーク管理情報は、1日に1度、AM4:00に定期的に更新されます。
- ネットワーク管理情報の更新は、各ノードの情報の更新後に実行することで最新化できます。

ネットワーク接続の変化情報の確認



ネットワークマップでは、設定された基準時点からのネットワーク接続の状態変化を確認できます。状態変化の種類には「追加」と「削除」があります。

「追加」は接続の追加などの新規の接続が検出された場合です。「追加」された接続は、接続図中に太実線で表示されます。

「削除」は接続断や接続の撤去によりこれまで検出していた接続が存在しなくなった場合です。「削除」された接続は接続図中に太破線で表示されます。

本機能を使用してネットワーク接続の変化を捉え、ネットワークの接続断を検出し、その箇所を特定できます。

また、以下の操作手順により、ネットワーク接続の変化情報をリスト形式で確認できます。

操作手順

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。 画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。
- ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。
 ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。
 画面中央にネットワークマップが表示されます。
- [アクション]ボタンから[接続変化情報の確認]を選択します。
 「削除」された接続情報、「追加」された接続情報をそれぞれ確認できます。



[接続情報変化の確認]で[更新]ボタンをクリックした場合、基準時点が更新されて、変化情報が削除されます。

ネットワーク接続の変化情報の基準設定



ネットワーク接続の変化情報は、ある基準時点からの変化(追加、削除)を表示したものです。この基準時点を更新できます。基準時 点はネットワーク接続の構成を変更した場合などに設定します。基準時点を更新すると、その時点から「追加」または「削除」によって 変化したネットワーク接続情報が表示されます。

.

以下の操作手順で更新できます。

操作手順

- ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
 画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。
- ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。
 ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。
 画面中央にネットワークマップが表示されます。
- 3. [アクション]ボタンから[接続変化情報の確認]を選択します。
- (更新)ボタンをクリックします。
 確認画面が表示されます。
- 内容を確認し、[はい]ボタンをクリックします。
 基準時点が更新操作を実行した時刻に更新されます。

関 ポイント

ネットワーク接続の変化情報の基準設定は、ISMのサービス起動時に自動的に更新されます。

VLAN、LAG設定の確認



ネットワークスイッチに設定されたVLAN、LAGの設定状態を専用のGUI画面で確認できます。 ネットワーク接続図上で、設定を視覚的に確認できます。

操作手順(VLANの例)

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。 画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。
- ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。
 ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。
 画面中央にネットワークマップが表示されます。
- 3. [アクション]ボタンから[VLAN表示]-[表示設定]を選択します。
- 4. 表示したいVLAN IDを入力し、[表示]ボタンをクリックします。

操作手順(LAGの例)

- ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
 画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。
- ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。
 ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。
 画面中央にネットワークマップが表示されます。
- 3. ネットワークマップ左上に表示されているプルダウンメニューから[リンクアグリゲーション]を選択します。

手動でのネットワーク接続情報の設定



自動的に物理ネットワークの接続情報が取得できない場合は、手動でネットワーク接続情報を設定できます。以下は手動での接続情報設定の操作手順です。

操作手順

- ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
 画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。
- ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。
 ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。
 画面中央にネットワークマップが表示されます。
- 3. ネットワークマップ左上に表示されているプルダウンメニューから[手動接続編集]を選択します。
- 4. 設定を行う両端のポートを選択し、[追加]ボタンをクリックします。

🔓 注意

[追加]ボタンをクリックしたあとに、手動で行った設定をキャンセルしたい場合は、[アクション]ボタンから[編集内容取消]を実行 します。

- 5. 設定したいすべての接続情報を追加したあと、[アクション]ボタンから[編集内容保存]を選択します。
- 6. 編集内容が正しいことを確認し、[保存]ボタンをクリックします。

2.3 ISM運用基盤の機能説明

ISMのユーザー管理機能、リポジトリ管理機能、タスク管理機能、ISM-VA管理機能について説明します。

以下の機能について説明します。

- 2.3.1 ユーザー管理機能
- ・ 2.3.2 リポジトリ管理機能
- ・ 2.3.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの導入
- ・ 2.3.4 タスク管理
- 2.3.5 ISM-VA管理機能

2.3.1 ユーザー管理機能

ISMのユーザーは、以下のように管理されています。

- ・ユーザーごとにユニークなログイン名とパスワードが割り当てられます。
- ・ ユーザーロールという権限によって、ノードに対するアクセス方法や、各機能の実行が制限されます。
- ユーザーをグループ化(以降、ユーザーグループと表記)することによって、ユーザーグループ単位で、各機能のアクセス範囲が 制限されます。
- ノードをグループ化(以降、ノードグループと表記)し、ユーザーグループと対応付けることによって、ユーザーのアクセスできるノードの範囲が制限されます。

ユーザーグループとノードグループの関係を、「図2.9 ユーザーグループ、ノードグループ、ロールの関係」で示します。

ここでは、以下について説明します。

- ・ ユーザーグループの種別と、そのユーザーグループに属するユーザーのアクセスできる範囲
- ・ ユーザーロールの種別と、そのロールを持つユーザーが実行できる操作
- ・ ISM初期設定後の必要なユーザーの作成
- ・ ユーザー管理機能の操作
- 2.3.1.1 ISMのユーザーの管理
- 2.3.1.2 ユーザーグループの管理
- 2.3.1.3 Microsoft Active DirectoryまたはLDAPとの連携
- 2.3.1.4 ノードグループの管理

ユーザーグループの種別と、そのユーザーグループに属するユーザーのアクセスできる範囲

ユーザーグループをノードグループに対応付けることで、ユーザーグループに属するユーザーのアクセス範囲を定義します。

ユーザーグループ名	アクセス範囲
Administratorグループ	すべてのノード、およびノードに関連する資源(ログなど)にアクセスできます。
	ISMの全体管理用のユーザーグループです。
Administratorグループ以外	ユーザーグループと対応付けたノードグループ内のノードおよびノードに関連する資源(ロ グなど)にアクセスできます。

ユーザーロールの種別と、そのロールを持つユーザーが実行できる操作

アクセス範囲内のノードに対してユーザーが実行できる操作は、ユーザーロールによって以下のように定義されます。

ユーザーロール	アクセスの種類		
Administrator	ノード、ユーザー、および各種設定の追加、変更、削除、および閲覧ができます。		
Operator	ノード、各種設定の変更、および閲覧ができます。 ユーザー管理はできません。		
Monitor	ノード、各種設定の閲覧ができます。 ユーザー管理、ノードの追加、変更、削除はできません。		

関 ポイント

Operatorによる設定の変更の可否は、本マニュアルでの各種機能の記載内容(アイコン表記)を参照してください。アイコン表記については、以下の説明を参照してください。

ユーザーができるアクセスの説明を行うため、以降ではユーザーが属するユーザーグループと、ユーザーが持つユーザーロールによるユーザーの種類を、以下のアイコンで示します。

ユーザーが属するユーザーグループ	ユーザーが持つユーザーロール	実行できる	実行できない
Administratorグループ	Administratorロール	Admin	
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor
Administratorグループ以外	Administratorロール	Admin	Admin
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor

以降の説明では、操作を実行できるユーザーの属性を以下のように示します。

例)

- 上記の表示の場合、以下のユーザー属性を持つユーザーが操作を実行できます。

- Administratorグループに属し、AdministratorまたはOperatorロールを持つユーザー
- Administratorグループ以外のグループに属し、AdministratorまたはOperatorロールを持つユーザー
- グレーアイコンで示される、Monitorロールを持つユーザーは、機能を実行できません。



Administratorグループに属し、Administratorロールを持つユーザーは、ISMの全体管理を行う特別なユーザーです。

Administratorグループに属し、OperatorロールまたはMonitorロールを持つユーザーは、Administrator以外のグループに属し、Operator ロールまたはMonitorロールを持つユーザーとはアクセス範囲が異なるだけで、実行できる操作は同じです。





ISM初期設定後の必要なユーザーの作成

関 ポイント

ISMの初期状態では、[Administratorグループ]の[Administratorロール]のユーザーだけが登録されています。

ユーザー名	パスワード	所属ユーザーグループ	ユーザーロール	用途
administrator	admin[注]	Administratorグループ	Administrator	ISM全体管理

[注]パスワード変更を行ったあと、運用を行ってください。

上記のadministratorユーザーを使用して、必要なユーザーを作成してください。

以下の手順で行います。

- 1. Administratorグループに属し、Administratorロールを持つユーザーでISMにログインします。
- 2. ノードグループを作成します。

詳細は「2.3.1.4 ノードグループの管理」の「ノードグループの追加」を参照してください。

- 3. ノードグループに所属するノードを登録します(ノードはあとからでも登録できます)。 詳細は「2.3.1.4 ノードグループの管理」の「ノードグループの編集」を参照してください。
- ユーザーグループを作成します。
 詳細は、「2.3.1.2 ユーザーグループの管理」の「ユーザーグループの追加」を参照してください。
- 5. ユーザーグループとノードグループの関連付けを行います。 詳細は、「2.3.1.2 ユーザーグループの管理」の「ユーザーグループの編集」を参照してください。

6. ユーザーグループに所属するユーザーを登録します。

詳細は、「2.3.1.1 ISMのユーザーの管理」の「ユーザーの追加」を参照してください。

ユーザー管理機能の操作

ユーザー管理機能は、主に以下の用途で利用する機能です。

- ISMのユーザーを管理
- ユーザーグループを管理
- ・ISMのユーザー認証を実施
- Microsoft Active DirectoryまたはLDAPと連携
- ノードグループを管理

ユーザー管理機能では、操作ユーザーにより操作対象が異なります。

操作ユーザー	操作対象
Administratorグループに属し、Administratorロールを持つ ユーザー	存在するユーザーグループのすべてが操作対象です。
Administrator以外のグループに属し、Administratorロールを 持つユーザー	操作ユーザーが所属するユーザーグループが操作対象で す。

2.3.1.1 ISMのユーザーの管理

ユーザーの管理には、以下の3種類あります。

- ユーザーの追加
- ユーザーの編集
- ユーザーの削除

ユーザーの追加



以下の方法で新しくユーザーを追加します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ユーザー]を選択します。
- 2. [アクション]ボタンから[追加]を選択します。

ユーザーを登録する場合に設定する情報は、以下のとおりです。

• ユーザー名

ISM全体で、ユニークな名称を指定してください。

- ・ パスワード
- ・ ユーザーロール

ユーザーロールについては、「ユーザーロールの種別と、そのロールを持つユーザーが実行できる操作」を参照してください。

説明

ユーザーの説明(コメント)を自由に指定してください。

日本語または英語を指定してください。指定しない場合は、英語となります。

• 日付フォーマット

- ・タイムゾーン
- ユーザーグループを選択してください

ユーザーの編集



以下の方法でユーザーの情報を変更します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ユーザー]を選択します。
- 2. 以下のどちらかを行います。
 - 編集したいユーザーにチェックを付け、[アクション]ボタンから[編集]を選択します。
 - 編集したいユーザー名をクリックし、表示された情報画面で[アクション]ボタンから[編集]を選択します。

変更できる情報は、以下のとおりです。

ユーザー情報	Administratorグループ		Administratorグループ以外のグループ	
	Administratorロール	Operatorロール Monitorロール	Administratorロール	Operatorロール Monitorロール
ユーザー名	0	0	0	0
パスワード	0	0	0	0
ユーザーロール	0	×	0	×
説明	0	×	0	×
· 語 日	0	0	0	0
日付フォーマット	0	0	0	0
タイムゾーン	0	0	0	0
ユーザーグループ	0	×	×	×

○:変更可能、×:変更不可能



```
LDAPなどと連携している場合、パスワードを変更しても、LDAPサーバのパスワードは変更されません。
```

ユーザーの削除



以下の方法でユーザーを削除できます。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ユーザー]を選択します。
- 2. 以下のどちらかを行います。
 - 削除したいユーザーにチェックを付け、[アクション]ボタンから[削除]を選択します。
 - 削除したいユーザー名をクリックし、表示された情報画面で[アクション]ボタンから[削除]を選択します。

2.3.1.2 ユーザーグループの管理

ユーザーグループの管理には、以下の種類があります。

- ユーザーグループの追加
- ユーザーグループの編集
- ユーザーグループの削除

ユーザーグループの追加

Administratorグループ その他のグループ 実行できるユーザー Admin Operator Monitor Admin Operator Monitor

ISM管理者が、以下の方法で新しくユーザーグループを追加します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ユーザーグループ]を選択します。
- 2. [アクション]ボタンから[追加]を選択します。

ユーザーグループを追加する場合に設定する情報は、以下のとおりです。

ユーザーグループ名

ISM全体で、ユニークな名称を指定してください。

• 認証方法

ユーザーグループに属するユーザーの認証方法は、以下のどちらかを指定します。

- ISM認証
- Microsoft Active DirectoryまたはLDAP連携認証
- 説明

ユーザーグループの説明(コメント)を入力してください。入力内容は任意です。

ノードグループを選択してください
 ノードグループを選択することで、ユーザーグループとノードグループの関連付けを行います。

注意

- ・ ユーザーグループに関連付けられるノードグループは1つだけです。
- ユーザーグループに所属する各ユーザーは、そのユーザーグループに関連付けられたノードグループに所属するノードだけを操 作対象にできます。ユーザーグループに関連付けられていないノードグループのノードにはアクセスできません。

ユーザーグループの編集



以下の方法で、ユーザーグループの情報を編集します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ユーザーグループ]を選択します。
- 2. 以下のどちらかを行います。
 - 編集したいユーザーグループにチェックを付け、[アクション]ボタンから[編集]を選択します。
- 編集したいユーザーグループ名をクリックし、表示された情報画面で[アクション]ボタンから[編集]を選択します。

編集できる情報は、以下のとおりです。

- ユーザーグループ名
- 認証方法
- 説明
- ノードグループを選択してください

ノードグループを選択することで、ユーザーグループとノードグループの関連付けを行います。

🌀 注意

- Administratorグループのグループ名は、変更できません。
- ・ Administratorグループの認証方法には、「ISM」のみ指定できます。
- ・ ユーザーグループに関連付けられるノードグループは1つだけです。

ノードグループに関連付けられた状態のユーザーグループに、新たに別のノードグループとの関連付けを行った場合、関連付け られていたノードグループとの関連付けは解除されます。

ユーザーグループの削除



以下の方法でユーザーグループを削除できます。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ユーザーグループ]を選択します。
- 2. 以下のどちらかを行います。
 - 削除したいユーザーグループにチェックを付け、[アクション]ボタンから[削除]を選択します。
 - 削除したいユーザーグループ名をクリックし、表示された情報画面で[アクション]ボタンから[削除]を選択します。



- Administratorグループは削除できません。
- ユーザーが存在するユーザーグループは、削除できません。
 ユーザーグループを削除する場合は、事前にユーザーを削除するか、ユーザーの所属をほかのユーザーグループへ変更してください。
- ・ ノードグループに関連付けられた状態のままユーザーグループを削除しても、ノードグループは削除されません。
- ・ ユーザーグループを削除すると、元には戻せません。
- ユーザーグループに関連したデータ(リポジトリ)はすべて削除されます。

2.3.1.3 Microsoft Active DirectoryまたはLDAPとの連携

Microsoft Active Directoryまたは、LDAPと連携することで、複数サービスのユーザーとパスワードを一元的に管理できます。 連携した場合の概要を以下に示します。

図2.10 ISMとLDAPとの連携イメージ



- 1. ユーザーがログインします。
 - ユーザーが連携対象であった場合

LDAP(Microsoft Active Directory)で認証を行います。

- ユーザーが連携対象でない場合
 - ISMで認証を行います。

Microsoft Active Directoryまたは、LDAPと連携するには、以下の手順で設定を行います。

設定手順

- 1. Microsoft Active DirectoryまたはLDAP(以降、「ディレクトリサーバ」と表記)と連携するユーザーを、ディレクトリサーバに登録します。
- 2. Administratorグループに属し、Administratorロールを持つユーザーでISMにログインします。
- 3. ディレクトリサーバ情報が設定されていない場合、ISMのLDAPサーバの設定で、以下の情報を設定します。 設定内容については、ディレクトリサーバの管理者に、手順1で登録した設定内容を問い合わせてください。

項目	設定内容
LDAPサーバ名	ディレクトリサーバ名を指定します。以下のどれかを指定します。
	・URLまたはIPアドレス
	・ ldap://url または ldap://IPアドレス
	・ ldaps://url または ldaps://IPアドレス
ポート番号	ディレクトリサーバのポート番号を指定します。
ベースDN	アカウント検索用のベースDNを指定します。ディレクトリサーバの登録内容に依存します。
	例)
	・ LDAPの場合:ou=Users,ou=system
	・ Microsoft Active Directoryの場合:DC=company,DC=com
検索属性	アカウント検索用のアカウント属性を指定します。以下のどちらかの固定文字列を指定します。
	・ LDAPの場合:uid

項目	設定内容
	 Microsoft Active Directoryの場合:sAMAccountName
バインドDN	ディレクトリサーバ上で、検索できるアカウントを指定します。ディレクトリサーバの登録内容に依存します。
	例)
	・ LDAPの場合:uid=ldap_search,ou=system
	・ Microsoft Active Directoryの場合: CN=ldap_search, OU=user_group, DC=company, DC=com
	anonymousはサポートしていません。
パスワード	バインドDNで指定したアカウントのパスワードを指定します。

- 4. 認証方法にMicrosoft Active DirectoryまたはLDAPを設定したユーザーグループを用意します。
- 5. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本情報]を選択し、[ユーザー]を選択して、手順1で登録した ユーザーを追加します。

登録する情報は以下のとおりです。

項目	設定内容
ユーザー名	手順1で登録したユーザー名を指定します。
パスワード	手順1のパスワードとは異なり、連携を解除した場合のパスワードを指定します。
	なお、ここで指定したパスワードが、FTPでログイン時に使用するパスワードとなります。
ユーザーロール	ISMでのユーザーロールを指定します。
説明	自由な値を指定します。
言語	追加するユーザーで使用する言語を指定します。
日付フォーマット	追加するユーザーで使用する日付フォーマットを指定します。
タイムゾーン	追加するユーザーで使用するタイムゾーンを指定します。
ユーザーグループ名	手順4で用意したユーザーグループを指定します。

6. 手順5で登録したユーザーがログインできることを確認します。

ログインできない場合、手順3に戻ってください。

設定解除手順

連携対象のユーザーグループやユーザーの連携を解除する方法は、以下のとおりです。

• ユーザーの変更

ユーザーが属するユーザーグループを、連携していないユーザーグループに変更します。ユーザーの編集で変更してください。

ユーザーグループの変更

ユーザーグループの編集で、認証方法を「ISM認証」に変更します。

上記のどちらの場合も、パスワードはユーザーの登録、変更操作で設定したパスワードが有効となります。

2.3.1.4 ノードグループの管理

ノードグループの管理には、以下の種類があります。

- ノードグループの追加
- ノードグループの編集
- ノードグループの削除

ノードグループの追加



ISM管理者が、以下の方法で新しくノードグループを追加します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ノードグループ]を選択します。
- 2. [アクション]ボタンから[追加]を選択します。
- または
 - 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノードグループ]を選択します。
 - 2. ノードグループリスト画面の[+]ボタンをクリックします。

ノードグループを追加する場合に設定する情報は、以下のとおりです。

ノードグループ名

ISM全体で、ユニークな名称を指定してください。

・ 割り当てるノードを選択

所属ノードグループが[未割り当て]のノードを複数選択します。

なお、ここで割り当てなくても、あとでノードグループの編集により割り当てることができます。

🌀 注意

ノードが所属できるノードグループは1つだけです。

ノードグループの編集



ISM管理者が、以下の方法で、ノードグループを編集します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ノードグループ]を選択します。
- 2. 以下のどちらかを行います。
 - 編集したいノードグループにチェックを付け、[アクション]ボタンから[編集]を選択します。

- 編集したいノードグループ名をクリックし、表示された情報画面で[アクション]ボタンから[編集]を選択します。

または

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノードグループ]を選択します。

2. 画面左側のノードグループリストからノードグループを選択し、[アクション]ボタンから[ノードグループ編集]を選択します。 ノードグループを編集する場合に設定する情報は、以下のとおりです。

ノードグループ名

ISM全体で、ユニークな名称を指定してください。

• 新たに割り当てるノードを選択

所属ノードグループが[未割り当て]のノードを複数選択します。

- ノードの割当てを解除または変更するには、以下の手順で行います。
 - 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノードグループ]を選択します。

- 2. 画面左側のノードグループリストからノードグループを選択します。
- 3. 画面右側でノードを選択し、[アクション]ボタン(画面右上に2つある[アクション]ボタンのうち、下のボタン)から[ノードグループへ 割り当て]を選択します。
- 4. 「ノードグループへの割り当て」画面で、[選択]ボタンをクリックします。
- 5.「ノードグループ選択」画面で以下のどちらかを選択し、[選択]ボタンをクリックします。
 - ノード割当てを解除する場合:[未割り当て]
 - ノード割当てを変更する場合:[<新たに割り当てるノードグループ>]
- 6. 「ノードグループへの割り当て」画面で[適用]ボタンをクリックします。

ノードグループの削除



ISM管理者が、以下の方法で、ノードグループを削除します。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[基本設定]-[ノードグループ]を選択します。
- 2. 以下のどちらかを行います。
 - 削除したいノードグループにチェックを付け、[アクション]ボタンから[削除]を選択します。
 - 削除したいノードグループ名をクリックし、表示された情報画面で[アクション]ボタンから[削除]を選択します。

または

- 1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノードグループ]を選択します。
- 2. 画面左側のノードグループリストからノードグループを選択し、[アクション]ボタンから[ノードグループ削除]を選択します。

7 注意

ノードが存在するノードグループは、削除できません。ノードグループを削除する場合は、以下のどれかを行ってください。

- 事前にノードを削除する
- ノードの割当てを解除する
- ほかのノードグループに割り当てる

2.3.2 リポジトリ管理機能

リポジトリは、ISMが利用する各種リソースを保管する場所です。各種リソースは、ユーザーグループに関連しています。主に以下の用途で利用します。

- ファームウェアアップデート用のデータを保管
 「ファームウェア管理機能」、「プロファイル管理機能」で利用されます。
- ・ OSインストール用のOSインストール媒体を保管
 - 「プロファイル管理機能」で利用されます。
- OSインストールに使用するServerView Suite DVDを保管
 「プロファイル管理機能」で利用されます。

関 ポイント

リポジトリのディスク領域には、ISM-VAに仮想ディスクを割り当てます。仮想ディスクの割当て方法については、「3.2.1.2 リポジトリの必要容量の見積り」および「3.7 仮想ディスクの割当て」を参照してください。

ファームウェアデータの保存



管理対象ノードに適用するファームウェアデータをリポジトリに保存する方法としては、2種類あります。

- ・DVDで提供されるファームウェアデータのISOイメージファイルをリポジトリに取り込みます。
- ・ 富士通のWebサイトに公開された各ノードのファームウェアデータをリポジトリに取り込みます。

管理対象ノードによって使用するファームウェアデータが異なります。下表のデータを準備します。データがDVD形式の場合はISOイ メージファイルを準備してください。

管理対象ノード	対象ファームウェア	使用するファームウェアデータ
サーバ	PRIMERGY本体 BIOS	富士通のPRIMERGY Webサイトに公開されたBIOS/iRMC データ
	PRIMERGY本体 iRMC	富士通のPRIMERGY Webサイトに公開されたBIOS/iRMC データ
	PRIMERGY搭載力一ド類	ServerView Suite Update DVD または 富士通のWebサイトに公開されたファームウェアデータ
ネットワークスイッチ	基本ソフトウェア	富士通のWebサイトに公開されたファームウェアデータ
ストレージ	コントローラー	富士通のWebサイトに公開されたファームウェアデータ

操作例を示します。

1. 準備したファームウェアデータを、FTPを使ってISM-VAへ転送します。ISOイメージまたはZIP圧縮されたファームウェアデータ を展開したフォルダーを管理サーバへ転送します。

転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。

- 2. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。
- 3. 以下のどちらかを行います。
 - ファームウェアデータをDVDからリポジトリに保存する場合は、[リポジトリ]タブの[アクション]ボタンから[DVDインポート]を選択します。
 - ファームウェアデータを富士通のWebサイトからリポジトリに保存する場合は、[ファームウェア]タブの[アクション]ボタンから [ファームウェアインポート]を選択します。
- 4. 画面表示に従い、操作を実行します。

リポジトリのインポートには時間がかかることがあります。インポートの開始後、作業がISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニューから[イベント/タスク]-[タスク]を選択すると、「タスク」画面にタスクの一覧が表示されます。

몓 ポイント

ISMのFTPサーバに配置したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。
•••••••••••••••••••••••••••••••••••••••

リポジトリからのファームウェアデータの削除



操作例を示します。

ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。

- ・ ファームウェアデータをDVDからリポジトリに保存していた場合
 - 1. [カラム表示]欄で[リポジトリ]を選択します。
 - 2. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
 - 3. 画面表示に従い、操作を実行します。
- ・ファームウェアデータを富士通のWebサイトからリポジトリに保存していた場合
 - 1. [カラム表示]欄で[ファームウェア]を選択します。
 - 2. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
 - 3. 画面表示に従い、操作を実行します。

ファームウェアデータのインポート



管理対象ノードによって使用するファームウェアイメージが異なります。下表のデータを準備してください。データがDVD形式の場合は、ISOイメージファイルを準備してください。

ファームウェアイメージ入手先

下記のWebサイトから対象モデルのファームウェアをダウンロードしてください。

対象ファームウェア	ファームウェア タイプ(種類)	入手先	
PRIMERGY本体 iRMC	iRMC	http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/	
PRIMERGY本体 BIOS	BIOS		
PRIMERGY 搭載カー ド類	FC	http://support.ts.fujitsu.com/globalflash/FibreChannelController/	
	CNA	http://support.ts.fujitsu.com/globalflash/LanController/	
ネットワークスイッチ 基本ソフトウェア	LAN Switch (SR-Xモデル)	http://www.fujitsu.com/jp/products/network/download/sr-x/firm/	
	LAN Switch (VDXモデル)	http://eservice.fujitsu.com/supportdesk/ [注1]	
ストレージ コントローラー	ETERNUS DX	http://eservice.fujitsu.com/supportdesk/ [注1] http://www.fujitsu.com/jp/products/computing/storage/download/ [注2]	

[注1]ご利用にはSupportDesk契約が必要です。

[注2]ご利用には「富士通ID(登録無料)」が必要です。
ServerView Suite Update DVDイメージ入手先

以下のPRIMERGYダウンロード検索画面で、「製品名」欄でご利用の製品名を選択し、「添付ソフト/ドライバ名称(部分一致可)」 欄に「Update DVD」と入力して検索してください。

http://azby.fmworld.net/app/customer/driversearch/ia/drviaindex



Administratorグループに所属するadministratorユーザーでファームウェアをインポートする場合の操作例を示します。

- 1. ファームウェアイメージ入手先から、ファームウェアイメージを入手します。
- 2. ISOイメージファイルを利用しない場合は、任意のフォルダーにダウンロードしたファイルを格納します。

ダウンロードしたファイルが圧縮ファイルの場合は、フォルダー内で展開してください。



- 3. FTPを使ってISM-VAへ転送します。
 - FTPコマンドまたはFTPクライアントソフトウェア(FFFTP、WinSCPなど)を使って転送してください。その際、文字コードがUTF-8 で変換されるように設定してください。Windows Explorerを使用すると文字コードが正しく扱われないため、使用しないでく ださい。
 - FTPクライアントソフトウェアからISM-VAへログイン後、ルートディレクトリから「<ユーザーグループ名>/ftp」ディレクトリへ移動し、そのディレクトリに転送を行います。
 - ISOイメージファイルを利用しない場合は、必ずフォルダー構造を変更せずに転送してください。
- 4. ファームウェアをインポートします。
 - a. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。
 - b. 以下のどちらかを行います。
 - ISOイメージファイルをリポジトリにインポートする場合は、[リポジトリ]の[アクション]ボタンから[DVDインポート]を選択 します。

画面表示に従い、ファイルの配置場所、メディアの種類を選択して、[適用]を選択します。

- ISOイメージファイルを利用せずにリポジトリにインポートする場合は、[ファームウェア]の[アクション]ボタンから[ファームウェアインポート]を選択します。

画面表示に従い、ファイルの配置場所、種類、モデル、バージョンを入力して、[適用]を選択します。

入力するバージョンは、下記の表に従って入力してください。

種類	モデル	バージョン
iRMC	RX100 S8、CX2550 M1など	iRMCとSDRのバージョン[注1]
BIOS	RX100 S8、CX2550 M1など	BIOSのバージョン[注1]
FC	LPe1250、LPe12002	BIOSとFWのバージョン[注2]
	LPe1600、LPe16002	ファームウェアのバージョン[注2]
	QLE2560、QLE2562、 QLE2600、QLE2602	BIOSのバージョン[注2]
CNA	Oce10102など	ファームウェアのバージョン[注1]
LAN Switch	SR-Xモデル	基本ソフトウェアのバージョン[注1]
	VDXモデル	ファームウェアのバージョン[注1]
ETERNUS DX	ETERNUS DXモデル	ファームウェアのバージョン[注1]

[注1]バージョンについては、リリースノートを参照してください。

[注2]バージョンについては、リリースノートまたはファイル名を参照してください。

リポジトリのインポートには時間がかかることがあります。インポートの開始後、作業がISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニューから[イベント/タスク]-[タスク]を選択すると、「タスク」画面にタスクの一覧が表示されます。

関 ポイント

- ISMのFTPサーバに配置したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。
- FTPクライアントソフトウェアを使ってファイル転送を行う際、文字コードがUTF-8で変換されるように設定してください。文字コードの 変換が正常に行われないと、ISM-VA上でファイルが文字化けを起こすことがあり、正しくインポートが実行できない場合がありま す。インポートが正しく行われない、インポートしたドキュメントが表示されないなどの場合は、インポート済みのファームウェアおよ び、ISM-VA上へFTP転送したファイルを削除し、文字コード変換の設定を見直したうえで、再度インポートを行ってください。

OSインストールファイルの保存



プロファイル管理機能は、リポジトリにインポートしたOSインストール媒体を使用してインストール作業を行うため、インポート後は、OSインストール媒体を直接使用しません。

インポートは以下の手順で実施します。

- 1. OSインストール媒体のISOイメージを用意します。ESXiの場合は富士通カスタムイメージを用意してください。
- 2. ISM-VAにFTPでログイン後、「./<ユーザーグループ名>/ftp」のディレクトリ配下に準備したISOイメージを転送します。 FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。
- 3. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。
- 4. 左のメニューで[オペレーティングシステム]を選択し、[アクション]ボタンから[OSインポート]を選択します。
- 5. [メディアタイプ]で適切なOS種類を選択し、FTPで転送したISOファイルを指定して、インポートを実行します。

ピポイント ISMのFTPサーバに配置したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。

リポジトリからのOSインストールファイルの削除

Administratorグループ その他のグループ その他のグループ 案行できるユーザー Admin Operator Monitor Admin Operator Monitor

削除は以下の手順で行います。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。
- 2. 左のメニューで[オペレーティングシステム]を選択します。
- 3. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
- 4. 画面表示に従い、操作を実行します。

ServerView Suite DVDの保存



プロファイル管理機能がOSのインストールを行う際、対象ノードを制御するプログラム、および対象ノードにインストールするドライバ、 アプリケーションなどのファイルは、ServerView Suite DVDから取得します。

対象ノードおよびインストールするOSをサポートするServerView Suite DVDを事前にインポートしてください。

インポートは以下の手順で行います。

- 1. ServerView Suite DVD Installation (DVD 1)のISOイメージを用意します。
- 2. ISM-VAにFTPでログイン後、「./<ユーザーグループ名>/ftp」のディレクトリ配下に準備したISOイメージを転送します。 FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。
- 3. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。
- 4. 左のメニューで[オペレーティングシステム]を選択し、[アクション]ボタンから[OSインポート]を選択します。
- 5. [メディアタイプ]で[ServerView Suite DVD]を選択し、FTPで転送したISOファイルを指定して、インポートを実行します。

🕑 ポイント

ISMのFTPサーバに配置したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。

リポジトリからのServerView Suite DVDの削除



削除は以下の手順で行います。

- 1. ISMのGUIでグローバルナビゲーションメニューから[各種設定]-[リポジトリ]を選択します。
- 2. 左のメニューで[オペレーティングシステム]を選択します。
- 3. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
- 4. 画面表示に従い、操作を実行します。

2.3.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの 導入



 Linux上の富士通PCIカードのファームウェアアップデートをするためには、対象サーバのOS上にEmulex OneCommand Manager CLI、または、QLogic QConvergeConsole CLIがインストールされ、対象のPCIカード情報が取得できる状態である必要があります。 インストール、操作方法は、Emulex One Command Manager CLIのマニュアル、QLogic QConvergeConsole CLIのマニュアルを参照してください。Emulex OneCommand Manager CLIのインストールが必要になる型番は、以下のとおりです。

.

PG-FC203, PGBFC203, PG-FC203L, PGBFC203L, PG-FC204, PGBFC204, PG-FC204L, PGBFC204L, PY-FC201, PYBFC201, PY-FC201L, PYBFC201L, PY-FC202, PYBFC202, PY-FC202L, PYBFC202L, PY-FC202L, PYBFC221L, PY-FC222, PYBFC222L, PYBFC222L, PY-CN302, PYBCN302, PYBCN302L, PY-CN202, PYBCN202, PY-CN202L, PYBCN202L, PY-LA3A2, PYBLA3A2, PYBLA3A2L, PY-LA3B2, PYBLA3B2, PYBLA3B2L

QLogic QConvergeConsole CLIのインストールが必要になる型番は、以下のとおりです。

PG-FC205, PGBFC205, PG-FC205L, PGBFC205L, PG-FC206, PGBFC206, PG-FC206L, PGBFC206L, PY-FC211, PYBFC211, PY-FC211L, PY-FC212, PYBFC212, PYBFC212L, PYBFC212L, PYBFC311, PYBFC311, PYBFC311L, PY-FC312, PYBFC312, PYBFC312L

・ Linux上のPCIカードのファームウェアアップデートをするためには、対象サーバ上のLinuxでlspciコマンドが実行できる必要があります。

Emulex OneCommand Manager CLI、またはQLogic QConvergeConsole CLIは、最新のものを利用してください。

以下のPRIMERGYダウンロード検索画面で製品名の欄にご利用の製品名を選択し、添付ソフト/ドライバ名称(部分一致可)の欄に「OCManager」または「QConvergeConsole」と入力して検索し、最新のものをダウンロードしてください。

http://jp.fujitsu.com/platform/server/primergy/downloads/

2.3.4 タスク管理

ISMでは時間がかかる処理を行う場合、その処理はタスクとして管理されます。それぞれのタスクの状態は操作した画面ではなく、「タスク」画面で一括参照します。

実行中の処理を中止(キャンセル)する場合も「タスク」画面から操作します。

「タスク」画面では、下表の処理がタスクとして参照できます。

機能	処理
ファームウェア管理機能	ファームウェアデータのインポート ファームウェアのアップデート
プロファイル管理機能	OS インストールメディアのインポート プロファイルの適用 プロファイルの再適用 プロファイルの適用の解除
ログ管理機能	ログ収集 ログ削除 ダウンロードファイルの作成

「タスク」画面の表示方法



1. [イベント/タスク]-[タスク]を選択します。

2.3.5 ISM-VA管理機能

ISM-VA管理機能は、ISMの導入・サービス運用およびメンテナンス時に使用する機能です。

以下について説明します。

- ISM導入時に使用する機能
- メンテナンス時に使用する機能

また、ISM-VA管理機能で使用できるコマンドについては、「2.3.5.1 ISM-VA管理機能のコマンド一覧」で説明します。

ISM導入時に使用する機能

機能名	機能概要
初期設定機能	ISM-VAをインストール後、最初に起動した際にハイパーバイザーのコンソール上で基本的な設定を行う機能を提供します。
	・ ネットワーク設定
	 ・時刻設定
	• 初期ロケール設定
ライセンス設定機能	ISMのライセンスキーを設定する機能を提供します。
証明書設定機能	Webブラウザでアクセスする際の証明書管理機能を提供します。

メンテナンス時に使用する機能

機能名	機能概要	
ISM-VAサービス制御機能	ISM-VAの停止/再起動や、内部で動作しているサービスの制御を行えます。	
基本設定機能	導入後にISM-VAの設定変更を行う機能を提供します。	
	・ ネットワーク設定	
	• 時刻設定	
	 ロケール設定 	
	・ 仮想ディスク設定	
	• ホスト名変更	
保守機能	ISM-VAの各種保守機能を提供します。	
	 版数確認 	
	・修正適用	
	 保守ログ採取 	
	・ デバッグフラグ切替え	

2.3.5.1 ISM-VA管理機能のコマンド一覧

ISM-VA管理機能のコマンド一覧を以下に示します。

ネットワーク設定

機能	コマンド
ネットワークデバイス表示	ismadm network device
ネットワーク設定変更	ismadm network modify
ネットワーク設定表示	ismadm network show

時刻設定

機能	コマンド
時刻設定表示	ismadm time show
設定可能タイムゾーン表示	ismadm time list-timezones
タイムゾーン設定	ismadm time set-timezone
日時/時刻設定	ismadm time set-time
NTP同期有効/無効設定	ismadm time set-ntp
NTPサーバ追加	ismadm time add-ntpserver
NTPサーバ削除	ismadm time del-ntpserver

ロケール/キーマップ設定

機能	コマンド
ロケール/キーマップ表示	ismadm locale show
設定可能ロケール表示	ismadm locale list-locales
ロケール設定	ismadm locale set-locale
設定可能キーマップ表示	ismadm locale list-keymaps
キーマップ設定	ismadm locale set-keymap

ライセンス設定

機能	コマンド
ライセンス一覧表示	ismadm license show
ライセンス設定	ismadm license set
ライセンス削除	ismadm license delete

証明書設定

機能	コマンド
SSLサーバ証明書配置	ismadm sslcert set
SSLサーバ証明書表示	ismadm sslcert show
SSLサーバ証明書出力	ismadm sslcert export

ISM-VAサービス制御

機能	コマンド
ISM-VA再起動	ismadm power restart
ISM-VA停止	ismadm power stop
ISM公開サービスポート変更	ismadm service modify
内部サービス一覧表示	ismadm service show
内部サービス個別起動	ismadm service start
内部サービス個別停止	ismadm service stop
内部サービス個別再起動	ismadm service restart
内部サービス個別ステータス表示	ismadm service status

機能	コマンド
内部サービス個別有効化設定	ismadm service enable
内部サービス個別無効化設定	ismadm service disable

仮想ディスク設定

機能	コマンド
LVMボリューム追加	ismadm volume add
ユーザーグループにLVMボリューム割当て	ismadm volume mount
ユーザーグループのLVMボリューム割当て解除	ismadm volume umount
ボリューム設定表示	ismadm volume show
LVMボリュームサイズ拡張	ismadm volume extend
システムのLVMボリュームサイズを拡張	ismadm volume sysvol-extend
LVMボリューム削除	ismadm volume delete

保守機能

機能	コマンド
保守ログ採取	ismadm system snap
システム情報の表示	ismadm system show
修正適用	ismadm system patch-add
プラグイン適用	ismadm system plugin-add
ホスト名変更	ismadm system modify
障害調査ログ切替え	ismadm system set-debug-flag

イベント通知設定

機能	コマンド
イベント通知メール用証明書/ アクションスクリプト登録	ismadm event import
イベント通知メール用証明書/ アクションスクリプト表示	ismadm event show
イベント通知メール用証明書/ アクションスクリプト削除	ismadm event delete

2.4 ノード登録解除時、グループ変更時の操作

ノード登録を解除する場合や、グループを変更する場合は、以下の操作を実行してください。

2.4.1 ノード登録解除時

ノード登録を解除する場合は、事前に以下の操作を完了させてください。

- ・ 実行中のタスクがある場合は、完了を待ってください。
- ・ 適用済みプロファイルは適用を解除してください。

関 ポイント

プロファイルが適用された状態でノード登録を解除すると、当該ノードは登録解除されません(プロファイルが適用済みの状態のまま 残ります)。個別にプロファイルを適用解除してください。

2.4.2 グループ変更/解除時

ノードグループに所属するノードを、別のノードグループに所属させる場合や、ノードグループから解除する場合は、事前に以下の操 作を完了させてください。

- ・ 当該ノード上で実行中のタスクがある場合は、完了を待ってください。
- ・ 当該ノードに適用済みのプロファイルがある場合は、適用を解除してください。
- ・ 当該ノードのログ収集スケジュールは、削除してください。
- ・ 当該ノードから取得し保存しているログは、削除してください。

믿 ポイント

۳

- ・ ユーザーグループに所属するユーザーがプロファイルを設定していた場合、そのユーザーからプロファイルの設定を参照・変更で きなくなります。その場合、Administratorグループのユーザーでプロファイルを削除してください。
- ・ 保存したログを削除し忘れた場合は、一度ノードを元のユーザーグループに戻してから削除してください。

2.4.3 ユーザーグループ削除時

ユーザーグループを削除する場合は、事前に以下の操作を完了させてください。

- ・ 適用済みプロファイルは適用を解除してください。
- ユーザーグループに含まれるプロファイル、プロファイルグループ、ポリシー、ポリシーグループは削除してください。
- ・ インポートしたOSメディア、SVS DVD、ファームウェアデータはリポジトリから削除してください。
- ・ ログ収集スケジュールは削除してください。
- ・保存したログは削除してください。

関 ポイント

ユーザーグループに所属するユーザーがプロファイル、ログ関連操作を設定していた場合、そのユーザーからプロファイル、ログ関連 操作の設定を参照・変更できなくなります。その場合は、Administratorグループのユーザーで修正してください。

2.4.4 ユーザーグループ名の変更時

ユーザーグループ名を変更する場合は、事前に以下のタスクが実行中で存在していないことを確認してください。

- ファームウェアのインポート操作
- ファームウェアのアップデート操作

第3章 ISMの導入

この章では、ISMの導入方法を説明します。

3.1 ISM導入の流れ

ISM (本体)の動作環境を構築します。

(1)導入設計

ISMを導入するにあたって事前に準備しておくべき作業は以下のとおりです。

- ・ ディスク資源の見積り
- ・リポジトリの設定
- ネットワークの構成
- ・ ノード名/プロファイル名の設定

作業内容については、「3.2 ISMの導入設計」を参照してください。

(2) ISM-VAのインストール

ISM-VAを管理サーバにインストールします。

インストール手順については、「3.3 ISM-VAのインストール」を参照してください。

(3) ISM-VAの環境設定

インストールしたISM-VAの動作環境を設定します。

環境設定手順の内容については、「3.4 ISM-VAの環境設定」を参照してください。

(4)ライセンスの登録

ISMの使用に必要なライセンスを登録します。 ライセンスの登録作業については、「3.5 ライセンスの登録」を参照してください。

(5)ユーザーの登録

ISMの利用者をユーザーとして登録します。 ユーザーを登録する作業については、「3.6 ユーザーの登録」を参照してください。

(6)仮想ディスクの割当て

ISM-VAのディスク容量を拡張するため、仮想ディスクを割り当てます。 ISM-VAのディスク容量を拡張する作業については、「3.7 仮想ディスクの割当て」を参照してください。

3.2 ISMの導入設計

ISMを円滑に運用するには、事前の導入設計が重要です。以下を設計してください。

- ・ 3.2.1 ディスク資源の見積り
- ・ 3.2.2 リポジトリの設定
- 3.2.3 ネットワークの設計
- ・ 3.2.4 ノード名の設定
- 3.2.5 ユーザーの設定

3.2.1 ディスク資源の見積り

以下の運用においてディスク容量の見積りが必要です。

- ・ ログ
- リポジトリ
- ・ バックアップ

ISM-VAの運用中は、ディスク容量を動的に拡張できません。このため、運用中にディスク容量が不足すると、ログ管理機能のログ収 集やリポジトリ、バックアップの運用に影響します。ディスクの容量が不足しないように、事前に見積もっておくことが重要です。

見積もったディスク容量は、仮想ディスクとして作成し、ISM-VAに割り当てます。仮想ディスクの作成、割当て方法については、「3.7 仮想ディスクの割当て」を参照してください。

ディスクの容量不足を回避するため、不要になったリポジトリのデータやバックアップデータなどを定期的に削除するといった運用も併せて設計してください。

3.2.1.1 ログ保存容量の見積り

ISMは、以下の機能でログを出力します。

ログ管理機能

ログ管理機能で出力するログのディスク容量は、管理対象のノード数とログの保有期間または保有回数に依存します。将来的に 増設するノード数を考慮して見積もってください。

ログ管理機能で出力するログのディスク容量の見積り方法については、弊社の本製品Webサイトを参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

・ 障害調査ログ

ISM-VAで管理するノード数に応じ、ログ領域の拡張を行う必要があります。

以下は、管理対象ノード数とログ領域に必要なディスク容量の目安です。

管理対象ノード数	ログ領域に必要なディスク容量
100ノード	10GB (デフォルト)
400ノード	40GB
1000ノード	100GB

ログ領域拡張は、以下の手順で行います。

1. 追加の仮想ディスクを割り当てます。

詳細は、「3.7.1 ISM-VA全体に対する仮想ディスク割当て」を参照してください。

2. ログレベルの切替えを行います。

詳細は、「4.16障害調査ログレベル切替え」を参照してください。

3.2.1.2 リポジトリの必要容量の見積り

プロファイル管理機能やファームウェア管理機能の運用には、ISM-VAにリポジトリの準備が必要です。リポジトリには、以下のデータが格納されます。

- ファームウェアのデータ
- OSのイメージファイル
- 作業ファイル

リポジトリに必要なディスク容量は、管理対象ノードにインストールするOSの種類やインポートするUpdateDVDの数に応じて必要な容量は異なりますが、通常は10GB以上が使用されます。下表を参照して必要な容量を見積もってください。

用途	操作	必要容量
ファームウェアデータの格	UpdateDVDのインポート	UpdateDVD1枚あたり7GB程度
游内	その他のファームウェアデータのインポー ト	インポートデータに依存
OSインストールメディアの	Windowsインストールメディアのインポー	OS1種あたり3~8GB程度
ファイル格納	F	プロファイル管理機能でインストールするOS種 のみインポートが必要
	VMware ESXiインストールメディアのイン	OS1種あたり0.5GB程度
	ポート	プロファイル管理機能でインストールするOS種 のみインポートが必要
	Linuxインストールメディアのインポート	OS1種あたり4GB程度
ServerView Suite DVDの 格納	ServerView Suite DVDのインポート	ServerView Suite DVD1枚あたり8GB程度
作業用ファイルの作成・保 管	特になし	0.5GB程度

関 ポイント

・ ユーザーグループとノードグループを関連付けることで、ノードグループごとに分離してISMを運用できます。この場合、ユーザー グループごとにリポジトリを準備します。ユーザーグループ数の分だけ、リポジトリに必要なディスク容量を見積もる必要があります。

 ServerView Suite DVDは、システム領域に格納されます。使用するServerView Suite DVDの数に応じて、システム領域のLVMボ リュームに必要なディスク容量を見積もる必要があります。

3.2.2 リポジトリの設定

リポジトリには、大容量のデータを格納します。ユーザーグループごとにリポジトリを分離して運用する場合には、さらに大容量のデー タを格納することになります。このため、ディスク容量を拡張する仮想ディスクにリポジトリを作成してください。仮想ディスクの作成、割 当て方法については、「3.7 仮想ディスクの割当て」を参照してください。

3.2.3 ネットワークの設計

ISMがサーバを管理するには、以下の2種類の管理LANを使用します。

・ iRMC Management LANに接続するネットワーク

主にサーバの制御やBIOS・iRMCの設定などに使用します。

・ オンボードLANに接続するネットワーク

主にOSのインストールやOSをインストールしたあとの接続などに使用します。

また、スイッチやストレージの管理にもネットワークの接続が必要です。それらは物理的・論理的に分解することも、1つに統合することも可能です。

関 ポイント

・業務に利用するネットワーク(業務LAN)は、これらの管理LANとは別に用意することを推奨します。

- ユーザーグループとノードグループを関連付けることで、ノードグループごとに分離してISMを運用できます。この場合、ノードグループごとにネットワークを分けて設計してください。ノードグループ間のネットワークにファイアーウォールを設けてグループ間の 通信を分離することで、ほかのノードグループに属するノードの参照や操作を抑止できます。
- ISMのネットワークインターフェースは、1つだけ定義できます。複数のネットワークを構成する場合は、ルータを設定し、各ネット ワーク間で通信可能な状態にしてください。

3.2.4 ノード名の設定

ノードを登録する際に、必要になるノード名およびプロファイル名のルールを決定します。

ノードを登録するときは、1台ごとに固有のノード名を設定します。

ノード名には最大64文字の英数字またはハイフン(-)、アンダースコア(_)が使用できます。

3.2.5 ユーザーの設定

各ユーザーの業務や職務に応じて、適切なユーザーロールやユーザーグループを設定してください。ノードの増設や監視、保守などの業務に合わせてユーザーロールを設定したり、ノードの資源を実際に使用する利用者を組織単位にユーザーグループを設定したりして、ユーザーの役割や体制に合わせたユーザーの設定を推奨します。

ユーザーグループごとにノードの運用を分離する場合には、ユーザーグループが運用・管理するノードをノードグループとして定義し、 ユーザーグループとノードグループを関連付けてください。このとき、ユーザーグループには、Administratorロールを持つユーザーを 作成してください。

ノード管理のセキュリティを堅持するため、不要になったユーザーの削除やパスワードを定期的に変更するなどの運用も併せて設計 することを推奨します。

ユーザーロール、ユーザーグループの設定方法およびパスワードの変更方法などについては、ISMのオンラインヘルプを参照してください。

3.3 ISM-VAのインストール

ISMソフトウェアは、「FUJITSU Software ServerView Infrastructure Manager 2.0.0 メディアパック」に同梱されています。

インストール先に応じてインストールします。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMへのインストール手順を説明します。

- 3.3.1 Microsoft Windows Server Hyper-Vへのインストール
- 3.3.2 VMware vSphere Hypervisor へのインストール
- ・ 3.3.3 KVMへのインストール

3.3.1 Microsoft Windows Server Hyper-Vへのインストール

DVDメディアに含まれるzipファイルを使用してインストールします。インストールの途中で指定するインストール先やネットワークアダプ ターの選択の詳細は、Hyper-Vのマニュアルを参照してください。 1. DVDメディアに含まれるzipファイルを、Hyper-VホストであるWindowsサーバの一時展開場所に展開します。

🗜 i 🕞 🚯 = i		圧縮フォルダー ツール	デスクトップ	i.		*
77-1% 东-山 共有	表示	展開		1.1		~ 0
🕞 💿 = 🕆 🗽 PC	 デスクト 	ップ・	Ý C	デスクトップの検索		P
☆ お気に入り	名明	. * s	更新日時	8:1	サイズ	
😹 Ø0>0-F	E Fujit	suServerViewISM2.0.zip	2016/02/17 13:12	圧線 (zip 形式) フ	997,055 KB	
■ デスクトップ 131 最近表示した場所	🌲 Fujit	suServerViewISM2.0	2016/02/17 22:37	774% 7x%9-		
PC						
デスクトップ						
10×14×1						
ビクチャ						
2 CTA						
■ ローカル ディスク (C:)						
🎭 ネットワーク						
2 個の項目 1 個の項目を	副択 973 N	18				1

2. Hyper-Vマネージャーを起動し、Hyper-VホストであるWindowsサーバを右クリックして[仮想マシンのインポート]を選択します。

iii ファイル(F) 操作(A) ◆ 吟 🖄 🗊 🛙	表示(V)	へルプ(H)	
Hyper-V マネージャ WIN-HE9BQF1	- NEVIP1 新規(1	仮想マシン(I)	,
	Hyper 仮想ス 仮想 S	マンクロファート(2) r-V の設定(S) イッチ マネージャー(T) SAN マネージャー(A)	6
	ディスク	の編集(E)	

3.「フォルダーの選択」画面で、手順1で展開したディレクトリを選択します。

選択するディレクトリは、「Snapshots」、「Virtual Hard Disks」、「Virtual Machines」というディレクトリの親ディレクトリです。



4.「インポートの種類の選択」画面で、[仮想マシンをコピーする(新しい一意なIDを作成する)]を選択し、[次へ]をクリックします。

	仮想マシンのインボート
	の種類の選択
開始する前に フォルダーの検索 仮想マシンの選択 インポートの推測的選択 要約	 実行するインボートの種類を選択する: 仮想マシンをインブレースで登録する (既存の一意な ID を使用する)(8) 仮想マシンを設定する (既存の一意な ID を作成する)(5) 仮想マシンをコピーする (新しい一意な ID を作成する)(0)
	<前へ(B) 次へ(N)> 売了(E) キャンセル

- 5. 「移動先の選択」画面と「保存するフォルダーの選択」画面では、ISM-VAのインポート先を選択します。デフォルトの場所が表示 されていますので、必要に応じて変更してください。
- 6.「ネットワークへの接続」画面で、ISM-VAで使用する仮想スイッチを選択し、[次へ]をクリックします。

	仮想マシンのインボート	×
*7トワーカへ	の接続	
間始する前に フォルダーの検索 仮想マシンの違択 インボートの種類の違択 移動先の違訳 (学作するフォルダーを違択しま す ホットワークへの 接続 要約	このページでは、宛先コンピューターで使用可能な仮想スイッチに接続できます。 仮想マシン FugitsuServerViewISM2.0 について、次の構成エラーが見つかりました。 ③ イーサネット スイッチ TSM Switch が見つかりませんでした。 コンピューター TWDN+#ESBQENEVP1*で使用する仮想スイッチを指定してください。 接続(<u>C</u>): Intel(R) 1210 Gigabit Network Connection - Virtual Switch v	
	<約へ(P) 次へ(N)> 売7(5) キャン	U

- 7. [完了]をクリックし、インポートウィザードを完了させます。
- 8. ISM-VAのインポート完了後、ハードディスクを固定容量に変換します。変換方法の詳細は、Hyper-Vのマニュアルを参照してください。

3.3.2 VMware vSphere Hypervisorへのインストール

DVDメディアに含まれるovaファイルを使用してインストールします。

1. vSphere Clientを起動し、[ファイル]メニューから[OVFテンプレートのデプロイ]を選択します。

✓ VSphere	Client
ファイル (F) 編集 (E) 表示 (W)	インペントリ (N) 管理 (A) ブラグイン (P) ヘルプ (H)
新規 (N)	 ・ トラ 日 インペンド
OVF テンプレートのデブロイ	(D)
エクスポート (E)	16
レポート (R)	alhost.localdomain VMware ESXi, 6.0.0, 2615704
マップのED場(P)	▶ 30に サマリ 仮想マシン リソース割り当て パフォーマンス
終了 (20	
	*ZFICOUT
	ホストは、ESX や ESXIなどの仮想化ソフトウェアを使う 想マシンを実行するコンピュータです。ホストは、仮想マ 使用する CPU およびメモリ リソースを提供し、さらに低 ンからストレージ1こアクセスしたり、ネットワーク接続した ことができるようにします。
	仮想マシンを新規作成するか、仮想アプライアンスをデ することによって、ホストに仮想マシンを追加できます。
	仮想マシンのもっとも簡単な追加方法は、仮想アブライ をデブロイする方法です。仮想アブライアンスは、オペレ ング システムおよびソフトウェアがすでにインストールで る事前構築済みの仮想マシンです。新規仮想マシンに Windows、Linux などのオペレーティング システムをイ ルする必要があります。

2. ソースの選択画面で、DVDメディアに含まれるovaファイルを選択し、[次へ]をクリックします。

OVF ランプレートのデプロイ ソース ソースの場所を選択します。		LOX
ソース の# テンプレートの原知細 名紙ジ環閉 ストレージ ディスクのフォーマット 終了準備の完了	ファイルまたは URL からのデブロイ 「>:WuglsuServerVervISM2.0.ova URL も入力してインターネットから OVF パッケージを行つ つードしてインストール する か または使用しているエンピューかからアクセス可能な場所 (ローカル・ハード ドライ フ、ネットワーク共有、CD/DVD ドライブなど) を確定します。	
		##>\th

3. 「ストレージ」画面で、仮想マシンの保存場所を指定し、[次へ]をクリックします。

ALL A REPORT	仮想マシン	ファイルのター	-ゲットストレージを	選択します。				
アレートの道動機	名前		15170-	容量	プロビジョー	堂き容量	タイプ	This P
5	dat dat	astorel	JF SSD	129.25 GB	181.65 GB	95.41 GB	VMPSS	サポー
フォーマット クロマッピング 幼売?	U ost	astons2	30 250	136.30 GB	100.72 GB	80.90 GB	VMP30	78-
	-							
	E rest			101				
	C 2005	注意マシンの7 Pの変捩:	いしージ DRS の通さ	thrib.				
	「 この形 データスト) 名約	i想マシンの? Pの選択:	(F)-9 0KS 0111	新化 容量【ブ	089x2>-[285£	917	This Pro
	■ この成 データスト 名前	注目マシンの7 PRO選択:	(H)5 Des 0/#3	551C 容量【力	089az>=	空8容量 [917	Thin Pr

4. 「ディスクのフォーマット」画面で、[シックプロビジョニング(Lazy Zeroed)]または[シックプロビジョニング(Eager Zeroed)]を選択し、[次へ]をクリックします。

🚱 OVF テンプレートのデフロイ			
ディスクのフォーマット 仮想ディスクはどのフォーマ	ットで保存しますか?		
2二2 <u>ロボテングレートの副類類</u> 名前と地理 ストレーラ ディスクのフォーマット ネットワークのマッピング 終了準備の完了	データストア: (使用可能な容量 (G8): (* シック プロビジョニング 0 (* シック プロビジョニング 0 (* Thin Provision	Jatastore 1 95.4 azy Zeroed) iager Zeroed)	

5.「ネットワークのマッピング」画面で、ISMで使用するネットワークを選択し、[次へ]をクリックします。

WF テンプレートのデプロイ			_10
キットワークのマッピング デプロイされたテンプレード	で使用するネットワークを指定してください。		
2-2	-	UTALIN MADE UNDER UNDER UNDER	
20月テンフレートの詳細 名前と場所	COUNT FUTURATION	いゆキラドノークをインヘンドがイロネラドノークへくラフレ	æ9.
21-1-2	ソースネットワーク	ターゲット ネットワーク	
2+12-10-10-10-10-10-10-10-10-10-10-10-10-10-	VM Network	VM Network	
*7F9-9049C99	LocalLan	LocalLan	
	leen-		
	The VM Network network		
	TO BE THE THE STORE CHESTING &		-
			-
			2
			2
			ž
			<u>*</u>
			*
			<u>*</u>
		must france	

6. [完了]をクリックし、OVFテンプレートのデプロイを完了させます。

3.3.3 KVMへのインストール

Г

DVDメディアに含まれるtar.gzファイルを使用してインストールします。

1. KVMホストの任意のディレクトリにtar.gzファイルを転送し展開します。

tar xzvf ISMV200si421_kvm.tar.gz
ISMV200si421_kvm/
ISMV200si421_kvm/ISMV200si421_kvm.qcow2
ISMV200si421_kvm/ISMV200si421.xml

- 2. 展開されたディレクトリに含まれるファイルをそれぞれ所定の場所にコピーします。
 - a. qcow2ファイルを/var/lib/libvirt/imagesにコピーします。

cp ISMV200si421_kvm.qcow2 /var/lib/libvirt/images

b. xmlファイルを/etc/libvirt/qemuにコピーします。

cp ISMV200si421.xml /etc/libvirt/qemu

3. xmlファイルを指定してISM-VAを登録します。

virsh define /etc/libvirt/qemu/ISMV200si421.xml

4. [仮想マシンマネージャー]をクリックし、仮想マシンマネージャーを開きます。



5. 仮想マシンマネージャー上でISM-VAを選択し、[開く]をクリックします。

	仮想マシンマネージャー		. a x
ファイル(F) 編集(E) 表示(V)	ヘルプ(H)		
📓 🔳 🖩 K k 🗈 🛛 🖉	-		
名前		*	CPU 使用率
▼ GEMU/KVM			
ISMV200si421 伊止中			

6. ISM-VA仮想マシン画面の[表示]メニューから[詳細]を選択します。

ファイル(F) 仮想マシン(M) 	表示(V) キーの送信(K)	
🖷 💡 🕨 🔟	Q 73 4 4 (d)	
	() J J J J – //(C)	
-	○詳細(D)	
	○スナップショット(P)	
	ロフルスクリーン(F)	
	仮想マシンの画面サイズに合わせる(R)	
	画面の縮小拡大(S)	
	テキストコンソール(T)	•
	仮想マシン	が稼働していません

7. ISM-VA仮想マシンの詳細画面で[NIC]を選択し、ISM-VAを接続する仮想ネットワークまたはホストデバイスを選択して、[適用] をクリックします。

	15	MV200si421 仮想マシン	
ファイル(F) 仮想マシン(M) 表示(V) キーの送信(K)		
	6		\$
 ● 構要 ● Performance ● Processor ● Memory ● Boot Options ● VirtIO Disk 1 ● NIC:dc:bd:0b ② タブレット ○ マウス = キーボード ● ディスプレイ Spice ● サウンド: ich6 ● Serial 1 ○ Channel gemu-ga ○ Channel spice ● ビデオ QXL ● コントローラー USB ● コントローラー VirtIO Serial 	仮想ネットワークインター ネットワークソース(N): デバイスのモデル(L): MAC アドレス:	仮想ネットワーク 'default': NAT 仮想ネットワーク 'local': 隔離されたネットワーク、内部とホス ホストデバイス enp6s0f0: macvtap ホストデバイス enp6s0f1: macvtap 共有デバイス名を指定 面除(R) キャンセルの	(C) 初期(A)

3.4 ISM-VAの環境設定

ISMインストール後の初期設定を行います。

3.4.1 ISM-VAの初回起動

インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMでの起動手順を説明します。

- ・ 3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(初回)
- ・ 3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(初回)
- 3.4.1.3 KVMで動作するISM-VAの場合(初回)

3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(初回)

1. Hyper-Vマネージャーで、インストールしたISM-VAを右クリックし、[接続]を選択します。

às.		Hy	per-V マネージヤ	-		
77イル(F) 操作(A) 表示(V)	ヘルプ(H)					
 •• • •						
WIN-HE9BQFNEVPJ	仮想マシン(I)					
	名前	状態	CPU 使用率	メモリの割り当て	移住	
	FujitsuServerViewISM2.0	接続(C) N			
		19定(8	J)			
		起動(5	5)			
		チェックス	ポイント(C)			
	1	###8(V	ŋ			
		エクスポート(X)				
	チェックホイント(C)	名駒の	変更(N)			
		MIR(L	.)			
		レプリケ	ーションを有効にする(/	A)		
		へルブ(H)			

2.「仮想マシン接続」画面の[操作]メニューから[起動]を選択し、ISM-VAを起動します。

🐏 WI	N-HE9BQFNEVPJ	の FujitsuServe	rViewISM2	2.0 - 仮想マシン接続	- • ×
77-116(F)	操作(A) メディア(M) ま	表示(V) ヘルプ(H)		Ĩ	
S 0 (Ctrl+Alt+Del(C)	Ctrl	+ Alt+ End		
	起動(T)	N	Ctrl+S		
	シャットダウン(D)	ME	Ctrl+D		
	保存(A)		Ctrl+A		
	一时停止(E)		Ctrl+P		
	リセット(R)		Ctrl+R		
	チェックポイント(P)		Ctrl+N		
	元に戻す(V)		Ctrl+E	Y はオフになってい	±₫
	統合サービス セットアッフ	「ディスクの挿入(1)	Ctrl+I		0. 7
	仮想マシンを	活動するには、日常に	FJX_1-01	起動]をクリックします	
状態: オフ					0

3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(初回)

1. vSphere Clientで、インストールしたISM-VAを右クリックし、[コンソールを開く]を選択します。



2.「コンソール」画面の[仮想マシン]メニューから[電源]-[パワーオン]を選択し、ISM-VAを起動します。



3.4.1.3 KVMで動作するISM-VAの場合(初回)

1. 仮想マシンマネージャーで、インストールしたISM-VAを右クリックし、[開く]を選択します。



2. ISM-VA仮想マシン画面の[仮想マシン]メニューから[実行]を選択し、ISM-VAを起動します。

7ァイル(F)	仮想マシン(M) 表示(V) キーの送 実行(R)	雲(K)
8	実行(R)	
	—肠停止(P)	
	シャットダウン(S) クローン 移行 削除(D)	>
	スクリーンショットの取得(T) USB デバイスのリダイレクト(R)	

3.4.2 ISM初期設定

ISM-VA起動後、コンソールのコマンドを使用して、ISMの基本的な設定を行います。

- 1. 管理者アカウントと初期パスワードを使用し、コンソールにログインします。
 - 管理者アカウント:administrator
 - 初期パスワード:admin
- 2. コンソールで、ネットワークを設定します。
 - LANデバイス名を確認

ismadm network device デバイス タイプ 状態 接続

eth0	ethernet	接続済み	eth0
lo	loopback	管理無し	

ー ネットワークを設定

ismadm network modify <LANデバイス名> ipv4.method manual ipv4.addresses <IPアドレス>/<マスクビット> ipv4.gateway <ゲートウェイIPアドレス>

実行例

ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway 192.168.1.1

You need to reboot the system to enable the new settings. Immediately reboots the system. [y/n]:

コマンド終了後に、システムを再起動するかどうかを確認するメッセージが表示されますので、「y」を入力してシステムを再起動してください。

ネットワーク設定後の操作は、ハイパーバイザーのコンソールでも、SSH経由のコンソールでも同じように実行できますので、 操作性のよいSSH経由でのアクセスを推奨します。

3. コンソールで、System LocaleとKeymapを設定します。

現在の設定の確認方法は以下のとおりです。

ismadm locale show
 System Locale: LANG=ja_JP.UTF-8
 VC Keymap: jp
 X11 Layout: jp

現在の設定を変更するには、以下のコマンドを使用します。

- System Localeの設定

ismadm locale set-locale LANG=<ロケール名>

実行例

ismadm locale set-locale LANG=en_US.utf8

- 設定可能な<ロケール名>の表示

ismadm locale list-locales

- Keymapの設定

ismadm locale set-keymap <キーマップ名>

実行例

ismadm locale set-keymap us

- 設定可能な<キーマップ名>の表示

ismadm locale list-keymaps

System Localeの変更は、ISM-VAの再起動後に有効になります。

4. コンソールで、日付・時間の設定をします。

現在の設定の確認方法は以下のとおりです。

ismadm time show Local time: 木 2016-06-09 16:57:40 JST Universal time: 木 2016-06-09 07:57:40 UTC RTC time: 木 2016-06-09 16:57:40 Time zone: Asia/Tokyo (JST, +0900) NTP enabled: no NTP synchronized: no RTC in local TZ: no DST active: n/a

現在の設定を変更するには、以下のコマンドを使用します。

- タイムゾーンの設定

ismadm time set-timezone <タイムゾーン>

実行例

ismadm time set-timezone <code>America/New_York</code>

- 設定可能なタイムゾーンの表示

ismadm time list-timezones

- 日付・時間の設定

ismadm time set-time <日付> <時間>

実行例

ismadm time set-time 2016-06-09 17:10:00

- NTP同期有効無効設定

有効設定

ismadm time set-ntp 1

無効設定

ismadm time set-ntp 0

- NTPサーバ追加削除

サーバ追加

ismadm time add-ntpserver $\langle NTP + -i \rangle$

サーバ削除

ismadm time del-ntpserver <NTPサーバ>

3.5 ライセンスの登録

ライセンスには、以下の2種類があります。ISMでは、サーバライセンスとノードライセンスの両方の登録が必要です。

ライセンスは、ISM-VAのインストール後、ISM-VA管理機能で登録します。

・ サーバライセンス

ISMを使用するために必要なライセンスです。

・ ノードライセンス

ISMに登録可能なノード数に関するライセンスです。ISM-VA管理機能で登録したノードライセンスのライセンス数を超える数のノードは登録できません。ノードライセンスを追加登録してから、追加するノードをISMに登録してください。

ライセンスの登録は、コンソールからadministratorでISM-VAにログインして行います。

1. サーバライセンスを登録します。

ismadm license set -key <ライセンスキー>

2. ノードライセンスを登録します。

ismadm license set -key <ライセンスキー>

3. ライセンスの登録結果を確認します。

ismadm license show

4. ISM-VAを再起動します。

ismadm power restart

3.6 ユーザーの登録

ISMの運用で登録が必要なユーザーを登録します。

ユーザーの登録方法については、「2.3.1 ユーザー管理機能」を参照してください。

3.7 仮想ディスクの割当て

仮想ディスクは、ISM-VAのディスク容量を増設するための資源です。ログやリポジトリ、バックアップの格納には大容量のディスク資源 が必要になります。また、それらの運用方法や管理対象ノードの規模などによって容量が異なります。大容量の資源を仮想ディスクに 割り当てることによって、ISM-VAのディスク容量や負荷の影響を回避します。仮想ディスクには必要十分な容量を確保しておくことで、 ログやリポジトリ、バックアップの運用を円滑に行えます。

仮想ディスクの割当ては、ISM-VA全体またはユーザーグループに対して行えます。

3.7.1 ISM-VA全体に対する仮想ディスク割当て

1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA(仮想マシン)に接続します。

ISMV200si40	- + • G
	ヘードドライブ

Microsoft Windows Server Hyper-Vの場合

仮想ディスクは、SCSIコントローラーの配下に作成してください。

VMware vSphere Hypervisorの場合

バイスタイプ ィスクの選択	追加するデバイスタイプを選択し	t7.
< <2001年65 洋總オブション えて 準備の完 了	 シリアルポート パラレルポート コッピードライブ ロシッピードライブ USB コントローラ USB ゴントローラ USB デバイス (使用不可) PCI デバイス (使用不可) マイーサネット アダプタ ハードディスク SCSI デバイス (使用不可) 	- 「詳細情報 このデバイスは、この仮想マシンイご自知できます。

作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

KVMの場合

Storage	ストレージ
Controller	・ コンピューターのハードディフクトにディフクノメージをを成する(A)
Network	
🖇 Input	10.0 - + GB
Graphics	793.6 GIB available in the default location
Sound	□ 今すぐディスク全体を割り当てる(A)
Serial	管理しているストレージか、他の既存のストレージを選択する(M)
Parallel	●聲聲(W)
Console	
Channel	デバイスの種類(D): 🖃 ディスクデバイス 🔹
8 USB Host Device	
8 PCI Host Device	/(ズの細期(B): SCSI *
🛡 Video	▶ 詳細なオプション(V)
Watchdog	
Filesystem	
Smartcard	
USB Redirection	
Э трм	
8 RNG	
A Panic Notifier	

バスの種類は、SCSIを選択してください。

- 2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
- 3. 仮想ディスク割当てのため、一時的にISMサービスを停止させます。

ismadm service stop ism

- 4. 手順1で追加した仮想ディスクが認識されているか確認します。
 - 例)

<pre># ismadm volume show -d</pre>	isk			
ファイルシステム	サイズ	使用	残り	使用% マウント位置
$/{\rm dev}/{\rm mapper}/{\rm centos}{\rm -root}$	16G	2. 6G	13G	17% /
devtmpfs	1.9G	0	1.9G	0% /dev
tmpfs	1.9G	4. OK	1.9G	1% /dev/shm
tmpfs	1.9G	8.5M	1.9G	1% /run
tmpfs	1.9G	0	1.9G	0% /sys/fs/cgroup
/dev/sda1	497M	170M	328M	35% /boot
tmpfs	380M	0	380M	0% /run/user/1001
/dev/sdb				(Free)
PV VG Fmt	∆ttr P	Size	PFree	
/dev/sda2_centos_lvm/	2 a 1	9 51g	0	

この例では、/dev/sdbが追加され未使用領域と認識されています。

5. 追加した仮想ディスクをISM-VA全体のシステムボリュームに割り当てます。

ismadm volume sysvol-extend -disk /dev/sdb

6. 仮想ディスク設定を確認します。

新規追加したボリューム(/dev/sdb)が、システムボリューム用(centos)として設定されていることを確認してください。

# ismadm volu	ume show -a	disk					
ファイルシス・	テム	サ	イズ	使用	残り	使用%	マウント位置
/dev/mapper/d	centos-root	t	26G	2. 5G	23G	10%	/
devtmpfs			1.9G	0	1.9G	0%	/dev
tmpfs			1.9G	4. OK	1.9G	1%	/dev/shm
tmpfs			1.9G	8.5M	1.9G	1%	/run
tmpfs			1.9G	0	1.9G	0%	/sys/fs/cgroup
/dev/sda1		4	497M	170M	328M	35%	/boot
tmpfs		:	380M	0	380M	0%	/run/user/1001
tmpfs		ć	380M	0	380M	0%	/run/user/0
PV	VG F	mt	Attr	PSize	PFre	e	
/dev/sda2	centos	l vm2	а	19. 51g	g ()	
/dev/sdb1	centos	l vm2	а	10.00§	g ()	

7. ISM-VAを再起動します。

ismadm power restart

3.7.2 ユーザーグループに対する仮想ディスク割当て

Administratorユーザーグループを例として、仮想ディスク割当ての手順を示します。

1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA(仮想マシン)に接続します。

Microsoft Windows Server Hyper-Vの場合

ISMV200si40	4 1 0
★ ハードウェア 1/1-ドウェアの対応加 ● BIOS コロミやらブート ラジビッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の反型プロセッサ 20回の下ライフ 2000 ドライブ 2000 ビーディスク ドライブ 200 ジーディスク ドライブ 次し フロッピーディスク ドライブ 次し 200 ジーディスク ドライブ 次し 200 ジーディスク ドライブ 次し 200 ジーディスク ドライブ 200 ジーデスク モジンドローラー 200 ジーディスク ドライブ 200 ジーデスク ドランボージン ドローシー 200 ジージスの 単の ジン ドローシー 200 ジージスの 小田 ジージン 小田	ヘードドライブ

仮想ディスクは、SCSIコントローラーの配下に作成してください。

VMware vSphere Hypervisorの場合

バイスタイプ イスクの選択 イスクの作成 細サブション で準備の死了	 追加するデバイスタイナを選択し、 シリアルボート パラレルボート フロッピードライブ CD,DVDドライブ GUSB コントローラ USB デバイス (使用不可) PCI デバイス (使用不可) イーサネット アダプタ ハードディスク SCSI デバイス (使用不可) 	ます。 ・ このデバイスは、この仮想マシンに3歳加できます。
--	--	--------------------------------------

作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

KVMの場合

	新しい仮想ハードウェアを追加
🖬 Storage	ストレージ
Controller	 コンピューターのハードディスク上にディスクイメージを作成する(R) 10.0 – + GiB 793.6 GiB available in the default location 今すぐディスク全体を割り当てる(A) 管理しているストレージか、他の既存のストレージを選択する(M) 参照(W)
Console Channel Channel USB Host Device PCI Host Device Video Filesystem Smartcard USB Redirection TPM RNG RNG Panic Notifier	デパイスの種類(D): □ ディスクデパイス ▼ パスの種類(B): SCSI ▼ ・詳細なオプション(V)
	キャンセル(C) 完了(F)

バスの種類は、SCSIを選択してください。

- 2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
- 3. 仮想ディスク割当てのため、一時的にISMサービスを停止させます。

```
# ismadm service stop ism
```

4. 手順1で追加した仮想ディスクが認識されているか確認します。

```
例)
```

```
# ismadm volume show -disk
                  サイズ 使用 残り 使用% マウント位置
ファイルシステム
/dev/mapper/centos-root 16G 2.6G 13G 17% /
devtmpfs
                     1.9G 0 1.9G
                                      0% /dev
                     1.9G 4.0K 1.9G
tmpfs
                                      1% /dev/shm
                     1.9G 8.5M 1.9G
tmpfs
                                      1% /run
tmpfs
                      1.9G
                           0 1.9G
                                      0% /sys/fs/cgroup
/dev/sda1
                      497M 170M 328M
                                      35% /boot
tmpfs
                      380M
                           0 380M
                                      0% /run/user/1001
/dev/sdb
                                        (Free)
 ΡV
           VG
                Fmt Attr PSize PFree
 /dev/sda2 centos lvm2 a-- 19.51g 0
```

この例では、/dev/sdbが追加され未使用領域と認識されています。

5. Administratorグループ用の追加ボリューム名を「adminvol」として作成し、新規追加した仮想ディスク(/dev/sdb)に関連付けます。

ismadm volume add -vol adminvol -disk /dev/sdb Logical volume "/dev/mapper/adminvol-lv" created.

6. 手順5で作成した追加ボリューム(adminvol)を、実際にAdministratorグループ用として使用できるように有効化します。

ismadm volume mount -vol adminvol -gdir /Administrator

7. 仮想ディスク設定を確認します。

新規追加したボリューム(/dev/sdb)が、Administratorグループ用として設定されていることを確認してください。

# ismadm volume show -d	isk			
ファイルシステム	サイズ	使用	残り	使用% マウント位置
/dev/mapper/centos-root	16G	2.6G	13G	17% /
devtmpfs	1.9G	0	1.9G	0% /dev
tmpfs	1.9G	4. OK	1.9G	1% /dev/shm
tmpfs	1.9G	8.6M	1.9G	1% /run
tmpfs	1.9G	0	1.9G	0% /sys/fs/cgroup
/dev/sda1	497M	170M	328M	35% /boot
tmpfs	380M	0	380M	0% /run/user/1001
tmpfs	380M	0	380M	0% /run/user/0
/dev/mapper/adminvol-lv	8. OG	39M	8. OG	1% 'RepositoryRoot'/Administrator
		D0:	סרייי	_
PV VG Fr	nt Attr	PSize	PFre	e
/dev/sda2 centos l	vm2 a	19.51	g 0	
/dev/sdb1 adminvol l	vm2 a	8.00	g 0	

8. ISM-VAを再起動します。

ismadm power restart

第4章 ISMの操作

この章では、ISMの操作を説明します。

4.1 ISMの起動と終了

保守などのため、ISMの起動/終了操作が必要になることがあります。

4.1.1 ISM-VAの起動

インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMでの起動手順を説明します。

- ・ 4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(2回目以降)
- ・ 4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(2回目以降)
- 4.1.1.3 KVMで動作するISM-VAの場合(2回目以降)

4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(2回目以降)

1. Hyper-Vマネージャーで、インストールしたISM-VAを右クリックし、[接続]を選択します。

23 2		Hy	per-V マネージャ	_	
77イル(F) 操作(A) 表示(V)	へルプ(H)				
Hyper-V マネージャー a WIN-HE9BQFNEVPJ	仮想マシン(I)				
In the second second second second second second	名前	状態	CPU 使用率	メモリの割り当て	移
	FujitsuServerViewISM2	接続(0	o) N		
		19定(8	B)		
		起動(5	5)		
		チェック	ポイント(C)		
	<	移動()	<i>ı</i>)	-	
	Saube () L(C)	エクスオ	(-+(x)		-
	7199/11 JF(C)	名駒の	/変更(N)		
		Mineric			
		レブリケ	ーションを有効にする(/	A)	
		~JL7((H)		

2.「仮想マシン接続」画面の[操作]メニューから[起動]を選択し、ISM-VAを起動します。



- 4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(2回目以降)
 - 1. vSphere Clientで、インストールしたISM-VAを右クリックし、[コンソールを開く]を選択します。



2.「コンソール」画面の[仮想マシン]メニューから[電源]-[パワーオン]を選択し、ISM-VAを起動します。

localhost localdomain ファイル (F) 表示 (W) 仮想	上の FujitsuServerViewISM2.0 マシン(V)			
	電源 (0)		パワーオン(P)	Ctrl+B
	ゲスト (G) スナップショット (S)	;	パワーオフ (0) サスペンド (S)	Ctrl+E Ctrl+Z
3	設定の編集 (E)		リセット (T)	Ctrl+T
	権限の這加 (P) Ctrl+P		ゲストのシャットダウン	(D) Ctrl+D
	パフォーマンスのレポート (F)_		ゲストの再起動(E)	Ctrl+R
	名前の変更 (N)			
	インペントリカら和除(Y) ディスクから和除(K)			

4.1.1.3 KVMで動作するISM-VAの場合(2回目以降)

1. 仮想マシンマネージャーで、インストールしたISM-VAを右クリックし、[開く]を選択します。



2.「ISM-VA仮想マシン」画面の[仮想マシン]メニューから[実行]を選択し、ISM-VAを起動します。



```
Pポイント
ISM-VAの起動には数分かかることがあります。しばらく待ってからGUIにログインできることを確認してください。
```

4.1.2 ISM-VAの終了

ISM-VAのコマンドを使用して、ISM-VAを終了します。

1. GUIを起動します。

GUIには、ISM管理者でログインしてください。

2. 運用を終了します。

「タスク」画面を参照して、タスクが終了していることを確認します。

- a. [イベント/タスク]-[タスク]を選択します。
- b.「タスク」画面で、ステータスが「Complete」または「Cancel-Complete」になっていることを確認します。
- c.「Complete」または「Cancel-Complete」でないタスクは、終了を待ち合わせるか、タスクをキャンセルします。

タスクをキャンセルする場合、実行中のタスクを選択して、[アクション]-[キャンセル]を選択します。実行中のすべてのタス クに対してキャンセルします。

タスクタイプが「Firmware Update」(ファームウェアのアップデート処理)のタスクは、キャンセルしても処理を中止できない 場合があります。この場合、処理の終了を待ち合わせます。



タスクが終了していない状態でISM-VAを終了すると、タスクの処理が異常な状態で中断され、以降の運用で正しく動作しないことがあります。

必ずタスクの終了を待ち合わせるか、タスクをキャンセルして処理が終了してからISM-VAを終了してください。

- 3. ISMのGUIをログアウトして、GUIを終了します。
- 4. コンソールを起動し、ISM管理者のユーザーでログインします。

5. ISM-VAの終了コマンドを実行し、ISM-VAを終了します。

ismadm power stop

4.1.3 ISM-VAの再起動

ISM-VAの再起動は、主にISM-VAへの修正適用時に行います。

- 1. ISMのタスクとGUIを終了し、コンソールにログインします。 ISMのタスクとGUIの終了方法については、「4.1.2 ISM-VAの終了」を参照してください。
- 2. 以下のコマンドを実行し、ISM-VAを再起動します。

ismadm power restart

4.1.4 ISMのサービス起動と停止

ISM-VAを起動すると、ISMのサービスは自動的に起動されます。

ISMのサービス起動/停止は、コンソールからadministratorでISM-VAにログインし、ISM-VAのコマンドを使用して行います。

ISMのサービス起動

1. 以下のコマンドを実行し、ISMのサービスを起動します。

ismadm service start ism

ISMのサービス停止

1. ISMのタスクとGUIを終了します。

ISMのタスクとGUIの終了方法については、「4.1.2 ISM-VAの終了」を参照してください。

2. 以下のコマンドを実行し、ISMのサービスを停止します。

ismadm service stop ism

4.2 ISM公開サービスポートの変更

WebブラウザでGUIへ接続する際のデフォルトポート番号(25566)を変更できます。

- 1. administratorユーザーでコンソールにログインします。
- 2. 以下のコマンドを実行し、ISMのサービスを停止します。

ismadm service stop ism

3. 以下のコマンドを実行し、ISM公開サービスポートを変更します。

ismadm service modify -port <サービスポート番号>

実行例

ismadm service modify -port 35566 You need to reboot the system to enable the new settings. Immediately reboots the system. [y/n]:

コマンド終了後に、再起動するかどうかを確認するメッセージが表示されますので、「y」を入力してISM-VAを再起動してください。

再起動完了後に新しいサービスポート番号でGUIが接続できるようになります。

4.3 ISM-VAのバックアップとリストア

ISM-VAのバックアップとリストアの手順を説明します。



4.3.1 ISM-VAのバックアップ

ISM-VAのバックアップは、ハイパーバイザーのエクスポート機能を使用して行います。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMでのバックアップ手順を説明します。

Microsoft Windows Server Hyper-Vで動作するISM-VAのバックアップ

```
Hyper-Vマネージャーで、インストールしたISM-VAを右クリックし、[エクスポート]を選択します。
```



VMware vSphere Hypervisorで動作するISM-VAのバックアップ

vSphere Clientで、インストールしたISM-VAを右クリックし、[ファイル]メニューから[エクスポート]-[OVFテンプレートのエクスポート]を選択します。

新規 (N)	•	N ▶ 🗊 インベントリ
OVF テンプレートのデプロイ (D)		
エクスポート (E)	•	▶ OVF テンプレートのエクスポート (O)
レポート (R)	•	リストのエクスポート(L)…
マップの印刷 (P)	Þ	ー マップのエクスポート (M)…
		システム ログのエクスポート (X)
KVMで動作するISM-VAのバックアップ

以下の場所に格納されているKVMファイルを任意の場所にバックアップします。

- /etc/libvirt/qemu
- /var/lib/libvirt/images

4.3.2 ISM-VAのリストア

バックアップしたファイルを使用して、「3.3 ISM-VAのインストール」の手順でISM-VAをリストアします。

4.4 保守資料の採取

ISMで運用するシステムにおいて、トラブル発生時の調査に必要な保守資料を採取できます。

調査の目的に応じて保守資料を採取します。

調査目的	調査担当者	保守資料
ISMやISM-VAの誤動作を調査	サポート要員	ISM RASログ ISM-VA オペレーティングシステムログ 保管ログ

これらの保守資料を調査の目的に応じて採取したり、一括して採取したりできます。

保守資料の採取はISM管理者が行います。ISM管理者は、採取した保守資料を調査目的ごとの調査担当者に提供します。



・保管ログの採取には、数時間かかることがあります。また、ISM-VAに大容量の空きディスク容量が必要です。これらを採取する場

- 合、または保守資料を一括して採取する場合、サポート要員の指示に従ってください。
- ・ コマンド実行時、ハイパーバイザーのコンソールに以下のメッセージが表示される場合がありますが、問題はありません。

blk_update_request : I/O error, dev fdO, sector O

.

採取方法

ISM-VAのコマンドを使用して、ISMの保守資料を採取します。

- 1. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
- 2. ISMの保守資料を採取します。

ISMやISM-VAの誤動作を調査するときの実施例

- ISM RASログのみの採取

```
# ismadm system snap -dir /Administrator/ftp
snap start
Your snap has been generated and saved in:
    /Administrator/ftp/ismsnap-20160618175323.tar.gz
```

- ISM RASログ/ISM-VA オペレーティングシステムログ/保管ログの一括採取

```
# ismadm system snap -dir /Administrator/ftp -full
snap start
Your snap has been generated and saved in:
/Administrator/ftp/ismsnap-20160618175808.tar.gz
```



-dirは出力先の指定です。「2.1.2 FTPアクセス」に記述されているファイル転送領域を指定することにより、FTPアクセスで採取した保守資料を取り出せます。

🌀 注意

保守資料の一括採取には数時間かかり、大容量の空きディスク容量が必要です。

3. 採取した保守資料をダウンロードします。

採取コマンド実行時に出力先とファイル名が表示されますので、管理端末からadministratorでFTPアクセスし、ダウンロードします。



保守資料格納ディレクトリに作成された保守資料は、自動的には削除されません。FTPクライアントソフトウェアなどを使用して、不要になった保守資料を手動で削除してください。保守資料は採取するたびに作成されますので、削除しないとISM-VAの空きディスク容量を圧迫するため、ほかの機能や運用に影響することがあります。

4.5 仮想ディスクの管理

仮想ディスクの割当て解除や、仮想ディスクの追加割当てができます。

4.5.1 仮想ディスクの割当て解除

「3.7.2 ユーザーグループに対する仮想ディスク割当て」で割り当てた仮想ディスクの割当て解除ができます。



• 割当て解除を行うと、ユーザーグループに保存されていたデータはすべて失われます。

- ・ Administratorグループに割り当てた仮想ディスク割当ては解除できません。
- ・「3.7.1 ISM-VA全体に対する仮想ディスク割当て」で割り当てたISM-VA全体に対する仮想ディスク割当ては解除できません。

以下、usrgrp1というユーザーグループに割り当てた仮想ディスクの割当て解除操作例を示します。

- 1. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
- 2. 仮想ディスク割当て解除のため、一時的にISMサービスを停止させます。

ismadm service stop ism

3. usrgrp1へ仮想ディスクが割り当てられていることを確認します。

# ismadm volume show -di	sk				
ファイルシステム	サイズ	使用	残り	使用%	マウント位置
/dev/mapper/centos-root	16G	2. 5G	13G	17%	/
devtmpfs	1.9G	0	1.9G	0%	/dev
tmpfs	1.9G	4. OK	1.9G	1%	/dev/shm
tmpfs	1.9G	8.6M	1.9G	1%	/run
tmpfs	1.9G	0	1.9G	0%	/sys/fs/cgroup
/dev/sda1	497M	170M	328M	35%	/boot
tmpfs	380M	0	380M	0%	/run/user/0
tmpfs	380M	0	380M	0%	/run/user/1001
/dev/mapper/usrgrp1vol-l	v 1	0G 3	3M 1	10G	1% 'RepositoryRoot'/usrgrp1

PV	VG	Fmt	Attr	PSize	PFree
/dev/sda2	centos	l vm2	а	19.51g	0
/dev/sdb1	usrgrp1vol	l vm2	а	10.00g	0

この例では、usrgrp1volというVGが、usergrp1に割り当てられています。

4. ユーザーグループ名を指定し、仮想ディスクをアンマウントします。

ismadm volume umount -gdir usrgrp1

5. usrgrp1用のボリューム名 (usrgrp1vol)を指定し、仮想ディスクを削除します。

```
# ismadm volume delete -vol usrgrp1vol
Logical volume "usrgrp1vol" successfully removed.
```

6. 仮想ディスク設定を確認します。

usrgrp1用の仮想ディスクが設定されておらず、使用されていた/dev/sdbが未使用状態(Free)であることを確認してください。

<pre># ismadm volume show</pre>	-dis	k				
ファイルシステム	÷	ナイズ	、 使用	残り	使用%	マウント位置
/dev/mapper/centos-ro	oot	160	G 2.5G	13G	17%	/
devtmpfs		1.90	G O	1.9G	0%	/dev
tmpfs		1.90	3 4.OK	1.9G	1%	/dev/shm
tmpfs		1.90	G 8.6M	1.9G	1%	/run
tmpfs		1.90	G O	1.9G	0%	/sys/fs/cgroup
/dev/sda1		497N	/ 170M	328M	35%	/boot
tmpfs		380	/ 0	380M	0%	/run/user/0
tmpfs		380	/ 0	380M	0%	/run/user/1001
/dev/sdb1					(F	Free)
PV VG F	Fmt	Attr	PSize	PFree		
/dev/sda2 centos	l vm2	a	19.51g	0		
/dev/sdb1	l vm2		10.00g	10.00§	g	

7. ISM-VAを再起動します。

ismadm power restart

4.5.2 ISM-VA全体に対する仮想ディスクの追加割当て

「3.7.1 ISM-VA全体に対する仮想ディスク割当て」と同様の方法で、複数の仮想ディスクをISM-VA全体に追加割当てすることができます。

4.5.3 ユーザーグループに対する仮想ディスク追加割当て

「3.7.2 ユーザーグループに対する仮想ディスク割当て」で割り当てた仮想ディスクに対し、追加の仮想ディスクを割り当てることができます。

以下、usrgrp1というユーザーグループに割り当てた仮想ディスクの追加割当ての操作例を示します。

1. 仮想ディスクに接続します。

「3.7.2 ユーザーグループに対する仮想ディスク割当て」の手順1の操作を行ってください。

- 2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
- 3. 仮想ディスク追加割当てのため、一時的にISMサービスを停止させます。

ismadm service stop ism

4. 手順1で追加した仮想ディスクが認識されているか確認します。

ファイルシステム /dev/mapper/centos-root	サイズ 16G	使用 2.6G	残り 13G	使用% マウント位置 17% /
devtmpfs	1.9G	0	1.9G	0% /dev
tmpfs	1.9G	4. OK	1.9G	1% /dev/shm
tmpfs	1.9G	8.5M	1.9G	1% /run
tmpfs	1.9G	0	1.9G	0% /sys/fs/cgroup
/dev/sda1	497M	169M	329M	34% /boot
/dev/mapper/usrgrp1vol-l	v 10G	33M	10G	1% 'RepositoryRoot'/usrgrp1
tmpfs	380M	0	380M	0% /run/user/0
/dev/sdc				(Free)
PV VG Fmt /dev/sda2 centos lvm /dev/sdb1 vergen1vc	Attr 2 a	PSize 19.51g	PFree 0	
/dev/sdb1_usrgrp1vol	ivm2 a	a 10	. 00g	U

この例では、/dev/sdcが追加され、未使用領域と認識されています。

5. 仮想ディスク追加割当てコマンドを実行し、追加した仮想ディスクをusrgrp1volに割り当てます。

ismadm volume extend -vol usrgrp1vol -disk /dev/sdc Logical volume "/dev/mapper/usrgrp1vol-lv" resized.

6. 仮想ディスク設定を確認します。

新規追加したボリューム(/dev/sdc)が、usrgrp1用(usrgrp1vol)として設定されていることを確認してください。

# ismadm volu	ume show -dis	sk			
ファイルシス	テム	サイズ	使用	残り	使用% マウント位置
/dev/mapper/d	centos-root	16G	2.6G	13G	17% /
devtmpfs		1.9G	0	1.9G	0% /dev
tmpfs		1.9G	4. OK	1.9G	1% /dev/shm
tmpfs		1.9G	8.6M	1.9G	1% /run
tmpfs		1.9G	0	1.9G	0% /sys/fs/cgroup
/dev/sda1		497M	170M	328M	35% /boot
/dev/mapper/u	usrgrp1vol-lv	/ 15G	33M	15G	1% 'RepositoryRoot'/usrgrp1
tmpfs		380M	0	380M	0% /run/user/0
tmpfs		380M	0	380M	0% /run/user/1001
PV	VG Fmt	Attr I	PSize	PFree	
/dev/sda2	centos lvm2	2 a	19.51g	0	
/dev/sdb1	usrgrp1vol	vm2 a-	- 10.0	00g	0
/dev/sdc1	usrgrp1vol	vm2 a-	- 5.0	00g	0

7. ISM-VAを再起動します。

ismadm power restart

4.6 証明書設定

4.6.1 SSLサーバ証明書配置

認証機関などで発行されたSSLサーバ証明書をISM-VAへ設定します。

1. FTPでSSLサーバ証明書をISM-VAへ転送します。

転送先:/Administrator/ftp

FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. コンソールからadministratorでISM-VAにログインします。

3. SSLサーバ証明書を配置します。

FTP転送した「key」ファイルと「crt」ファイルを指定し、コマンドを実行してください。

ismadm sslcert set -key /Administrator/ftp/server.key -crt /Administrator/ftp/server.crt

4.6.2 SSLサーバ証明書表示

ISM-VAに設定されているSSLサーバ証明書を表示します。

- 1. コンソールからadministratorでISM-VAにログインします。
- 2. SSLサーバ証明書表示コマンドを実行します。

ismadm sslcert show

4.6.3 SSLサーバ証明書出力

ISM-VAに設定されているSSLサーバ証明書を出力します。

- 1. コンソールからadministratorでISM-VAにログインします。
- 2. SSLサーバ証明書出力コマンドを実行します。

ismadm sslcert export -dir /Administrator/ftp

出力されたファイルは、FTPでダウンロードできます。

4.7 ライセンス設定

ISM-VAのサーバライセンスおよびノードライセンスの登録/表示/削除が行えます。

- 1. コンソールからadministratorでISM-VAにログインします。
- 2. ライセンス設定コマンドを実行します。
 - ライセンス登録

ismadm license set -key <ライセンスキー>

- ライセンス一覧表示

ismadm license show

- ライセンス削除

ismadm license delete -key <ライセンスキー>



ライセンスの登録/削除後は、ISM-VAの再起動が必要です。

4.8 ネットワーク設定

ネットワークの設定/表示を行います。

1. コンソールからadministratorでISM-VAにログインします。

- 2. ネットワーク設定コマンドを実行します。
 - ネットワークデバイス表示

ismadm network device

- ネットワーク設定変更

ismadm network modify <LANデバイス名> ipv4.method manual ipv4.addresses <IPアドレス>/<マスクビット> ipv4.gateway <ゲートウェイIPアドレス>

.

🌀 注意

ネットワーク設定変更後は、ISM-VAの再起動が必要です。

実行例)

ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway 192.168.1.1

ー ネットワーク設定表示

ismadm network show <LANデバイス名>

実行例)

ismadm network show eth0

4.9 イベント通知設定

モニタリング機能のイベント通知で使用する証明書とアクションスクリプトを登録できます。

4.9.1 イベント通知メール用証明書登録

1. FTPで証明書を転送します。

転送先:/<ユーザーグループ名>/ftp/cert

FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

- 2. コンソールからadministratorでISM-VAにログインします。
- 3. イベント通知メール用証明書登録コマンドを実行します。

ismadm event import -type cert

4.9.2 アクションスクリプト登録

1. FTPでスクリプトを転送します。

転送先:/<ユーザーグループ名>/ftp/actionscript

FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

- 2. コンソールからadministratorでISM-VAにログインします。
- 3. アクションスクリプト登録コマンドを実行します。

ismadm event import -type script

4.9.3 イベント通知メール用証明書表示

ISM-VAに登録されたイベント通知メール用証明書を表示できます。

ismadm event show -type cert

4.9.4 アクションスクリプト表示

ISM-VAに登録されたアクションスクリプトを表示できます。

ismadm event show -type script

4.9.5 イベント通知メール用証明書削除

ISM-VAに登録されたイベント通知メール用証明書を削除できます。

ismadm event delete -type cert -file <証明書ファイル> -gid <ユーザーグループ名>

4.9.6 アクションスクリプト削除

ISM-VAに登録されたアクションスクリプトを削除できます。

ismadm event delete -type script -file <スクリプトファイル> -gid <ユーザーグループ名>

4.10 ISM-VAサービス制御

ISM-VAの停止/再起動や、内部で動作しているサービスの制御を行えます。

- 1. コンソールからadministratorでISM-VAにログインします。
- 2. ISM-VAサービス制御コマンドを実行します。
 - ISM-VA再起動

ismadm power restart

- ISM-VA停止

ismadm power stop

- 内部サービス一覧表示

ismadm service show

- 内部サービス個別起動

ismadm service start <サービス名>

実行例)FTPサーバの個別起動

ismadm service start vsftpd

- 内部サービス個別停止

ismadm service stop <サービス名>

実行例)FTPサーバの個別停止

ismadm service stop vsftpd

- 内部サービス個別再起動

ismadm service restart <サービス名>

実行例)FTPサーバの個別再起動

ismadm service restart vsftpd

- 内部サービス個別ステータス表示

ismadm service status <サービス名>

実行例)FTPサーバの個別ステータス表示

ismadm service status vsftpd

- 内部サービス個別有効化設定

ismadm service enable <サービス名>

実行例)FTPサーバの個別有効化設定

ismadm service enable vsftpd

- 内部サービス個別無効化設定

ismadm service disable <サービス名>

実行例)FTPサーバの個別無効化設定

ismadm service disable vsftpd

4.11 システム情報の表示

コンソールからISM-VAの内部システム情報を表示できます。

1. コンソールからadministratorでISM-VAにログインします。

2. システム情報の表示コマンドを実行します。

# ismadm system	show
ISM Version	: 2.0.0
GUI Port Number	: 25566
Hostname	: localhost
Log Level	: small

4.12 ホスト名変更

ISM-VAのホスト名を変更できます。

- 1. コンソールからadministratorでISM-VAにログインします。
- 2. ホスト名変更コマンドを実行します。

```
\# ismadm system modify -hostname ismva2 You need to reboot the system to enable the new settings. Immediately reboots the system. [y/n]:
```



- ホスト名は小文字で入力してください。
- コマンド実行後に再起動が必要です。
- デフォルトのホスト名「localhost」を変更する場合は、「4.6 証明書設定」に記載された手順に従い、変更するホスト名に対応した証明書をISM-VAに配置する必要があります。

4.13 修正適用

ISM-VAに修正を適用できます。

- 1. FTPで修正ファイルをISM-VAへ転送します。
 - 転送先:/Administrator/ftp

FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

- 2. コンソールからadministratorでISM-VAにログインします。
- 3. 修正適用のため、一時的にISMサービスを停止させます。 「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。
- 4. 修正適用コマンドを実行します。

修正ファイルを指定してコマンドを実行してください。

ismadm system patch-add -file <修正ファイル>

実行例)

ismadm system patch-add -file /Administrator/ftp/SVISM_V200S20160606-02.tar.gz

5. 修正適用後、ISM-VAを再起動します。

ismadm power restart

4.14 プラグイン適用

ISM-VAにプラグインを適用できます。

- 1. FTPでプラグインファイルをISM-VAへ転送します。
 - 転送先:/Administrator/ftp

FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

- 2. コンソールからadministratorでISM-VAにログインします。
- 3. プラグイン適用のため、一時的にISMサービスを停止させます。

「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。

4. プラグイン適用コマンドを実行します。

プラグインファイルを指定してコマンドを実行してください。

ismadm system plugin-add -file <プラグインファイル>

実行例)

 $\label{eq:limit} \mbox{ $\#$ ismadm system plugin-add -file /Administrator/ftp/SVISM_V200_plugin-02.tar.gz}$

5. プラグイン適用後、ISM-VAを再起動します。

ismadm power restart

4.15 障害調査ログ切替え

障害調査で使用するログ出力の有効/無効を切り替えることができます。

1. コンソールからadministratorでISM-VAにログインします。

- 2. 障害調査ログ出力切替えコマンドを実行します。
 - ログ出力有効化

ismadm system set-debug-flag 1

- ログ出力無効化

ismadm system set-debug-flag 0

4.16 障害調査ログレベル切替え

障害調査で使用するログの出力レベルを切り替えることができます。

出力レベルを切り替えることにより、出力されるログの容量を制限できます。

ログレベル	出力されるログ容量の目安
small(デフォルト)	10GB
medium	40GB
large	100GB



- 下位から上位のレベルへの切替えのみ有効です。
- ・ ログレベルの切替え後は、ISM-VAの再起動が必要です。
- 1. コンソールからadministratorでISM-VAにログインします。
- 2. ISMサービスを停止させます。

「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。

3. 障害調査ログレベル切替えコマンドを実行します。

- mediumへの切替え

ismadm system change-log-level medium

- largeへの切替え

ismadm system change-log-level large

4. 障害調査ログレベルの設定を確認します。

システム情報の表示コマンドで確認できます。

```
# ismadm systemshowISM Version: 2.0.0GUI Port Number: 25566Hostname: localhostLog Level: medium
```

5. 以下のコマンドを実行し、ISM-VAを再起動します。

ismadm power restart

ISM-VA起動後に、新しい障害調査ログレベルが有効になります。

第5章 ノードの保守

この章では、ノードの保守を説明します。

5.1 メンテナンスモード

ノードの故障が検出されてノードの保守作業を行う場合、ISM上で対象ノードをメンテナンスモードに変更することをお勧めします。

メンテナンスモードに変更されたノードに対しては、ISMのアラーム検出およびバックグラウンドでの処理が抑止されるため、故障した ノードで何度もアラームが発生することを防止できます。

メンテナンスモード中のISMの動作は以下のとおりです。

影響を受ける機能	メンテナンスモード中の動作
センサーしきい値監視	センサー状態の取得が停止します。
SNMPトラップの監視	トラップは受信され、トラップログに入りますが、アラームは発生しません。
ノード情報取得	ISMが定期的に実行するノード情報取得は停止します。 必要に応じて、ノード情報取得を手動で実行してください。
ノードログ収集	スケジュール設定されたログ収集はスキップされます。 必要に応じて、ノードログ収集を手動で実行してください。

関 ポイント

メンテナンスモード中でも、上記以外の機能は利用可能です。例えば、メンテナンスモードになっているノードに対しても、以下の操作 は実行できます。

- ・ プロファイルの適用、再適用、適用解除
- ファームウェアアップデート
- 手動ノードログ収集

.

メンテナンスモード設定手順

- 1. 「ノード詳細」画面を表示します。
- 2. [アクション]ボタンから[メンテナンスモード設定]を選択します。

確認画面が表示されるので、ノード名を確認して[はい]をクリックします。

メンテナンスモード解除手順

- 1. 「ノード詳細」画面を表示します。
- 2. [アクション]ボタンから[メンテナンスモード解除]を選択します。

5.2 エラー発生時の調査方法

ISMでは、ノード単位での障害検出を行っています。

ISMログに記載されているものよりも詳細な情報については、各機器にアクセスして調べる必要があります。

付録A ISM-VAのアンインストール

ISM-VAのインストール先に応じてアンインストールします。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMからのアンインストール手順を説明します。

- Microsoft Windows Server Hyper-Vからのアンインストール
- VMware vSphere Hypervisorからのアンインストール
- KVMからのアンインストール

Microsoft Windows Server Hyper-Vからのアンインストール

1. ISM-VAを停止します。

詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

2. Hyper-Vマネージャーを起動し、インストールしたISM-VAを右クリックして[設定]を選択します。

ISM-VAに割り当てられている仮想ハードディスクの格納場所とファイル名が表示されるので、メモしてください。

3. Hyper-Vマネージャー上で、インストールしたISM-VAを右クリックして[削除]を選択します。

ā.			Hy	per-V マネージャ	-	
ファイル(E) 操作(A) 表示(V)	∧ルプ(圧)					
Hyper-V マネージャー WIN-HE9BQFNEVPJ	仮想マシン(1)					
	名前	뀫	ER .	CPU 使用率	メモリの割り当て	1
	FujitsuServerViewISM2.0	*	7 报続(0)		
			設定(設定(B)		
			起動(S)		
			チェック	ポイント(C)		
	<		移動(v)		
	チェックポイント(<u>C</u>)		エクスパ 名前の	ポート(X) D変更(N)		
		3	削除(L) 🗟		
			レプリク	ァーションを有効にする(A)	
			NIJ	(H)		

4. 手順2で記録した仮想ハードディスクを、エクスプローラーで削除します。

VMware vSphere Hypervisorからのアンインストール

1. ISM-VAを停止します。

詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

2. vSphere Clientを起動し、インストールしたISM-VAを右クリックして[ディスクから削除]を選択します。

	8 1 1	HOVCH B I HOVC	
🔳 II 🕨 🙆 🙆	Ch	19 😫 🔛 🧼 🕪	
Euliter Convertional St	12.0	FujitsuServerViewISM2.0	5.
C. Province of Province		電源(O) ・ ゲスト(G) ・ スナップショット(S) ・ コンソールを開く(L)	テマンス イベ
	8	設定の編集 (E)_	するソフトウェ
		権限の追加 (P)_ Ctrl+P	ラシステム (
		パフォーマンスのレポート(F)_	
		名前の麦更 (N)	レビュータ環!
		新しんウィンドウで開く(W)_ Ctrl+Alt+N インベンドリから削除(Y)	って使用した
		ディスクから利用除(K)	ーのホストで

KVMからのアンインストール

1. ISM-VAを停止します。

詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

2. 仮想マシンマネージャーを起動し、インストールしたISM-VAを右クリックして[削除]を選択します。

	仮想マシンマネージャー	. 0 X
ファイル(F) 編集(E)	表示(V) ヘルプ(H)	
🔛 🔳 🕅 < 🕞	10 · ·	
名前		▼ CPU 使用率
▼ GEMU/KVM		
ISMV200si421 存止中	実行(B) 一時停止(P) シャットダウン(S) → クローン 移行 削除(D)	
	問<(Q)	

付録B トラブルシューティング

ISMの動作がエラーになる場合や、期待した動作にならない場合の主な原因と対処について説明します。

ここに記載されない項目や詳細な原因と対処については、以下のURLのトラブルシューティング情報を参照してください。

http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/

現象:手動検出したノードの登録に失敗する

原因·対処

検出したノードのシリアル番号を確認してください。すでにノード登録されている場合にはノードを削除してから登録してください。

現象:以下の機能において、ファイルのインポート操作の実施時に、ファイル選択画面で「サーバとの通信に失敗しました。」のエラーが表示される。

- ・ [各種設定]-[プロファイル]-[アクション]-[インポート]-[選択]ボタン
- ・ [各種設定]-[リポジトリ]-[ファームウェア]-[リポジトリ]-[アクション]-[DVDインポート]-[選択]ボタン
- ・ [各種設定]-[リポジトリ]-[ファームウェア]-[ファームウェア]-[アクション]-[ファームウェアインポート]-[選択]ボタン
- ・ [各種設定]-[リポジトリ]-[OS / SVS]-[アクション]-[DVDインポート]-[選択]ボタン

原因·対処

- ・使用者が所属しているユーザーグループのFTPフォルダー配下のファイルについて、ファイル名にUTF-8でない文字コードが 含まれていないか確認してください。
- ・ ISMとクライアントの通信状態を確認してください。

現象:ノードの状態確認、制御に失敗する。

原因·対処

- ・対象ノードとISM間のネットワークが正しく動作していることを確認してください。
- ・ 電源ケーブルが対象装置に接続されているか、電源が供給されているかを確認してください。
- ・ ISMに登録されているIPアドレスと、対象装置(またはOS)のIPアドレスが一致しているか確認してください。特にIPアドレスを変更した場合は、ISMの登録情報の変更忘れがないか確認してください。
- ・ ISMに登録されているユーザーアカウントと、対象装置(またはOS)のユーザーアカウントが一致しているか確認してください。 特にパスワードを変更した場合は、ISMの登録情報の変更忘れがないか確認してください。
- ・ ISMで操作対象ノードに対して、ISMの別の機能を利用中でないことを確認してください(ファームウェアアップデート中にプロファイル適用を開始するなど)。

現象: Internet Explorer 11を使用している場合に、ファイルのダウンロードが失敗する。

原因·対処

Internet Explorerの設定によりファイルのダウンロードが失敗します。以下の設定を変更してください。

[インターネットオプション]-[セキュリティ]タブで[レベルのカスタマイズ]ボタンをクリックし、[ダウンロード]-[ファイルのダウンロード]を [有効にする]に変更。

ファームウェア管理機能

現象:ファームウェアのアップデート操作を行う際に、アップデートするファームウェアが指定できない。

原因·対処

 ファームウェアデータは、事前にインポートして取り込んでおく必要があります。インポートしていない場合は、最初にインポート を実行してください。

- ・ 個別ファームウェアのインポートの際、指定したファームウェア種別、モデル名などが間違っていると、指定したノードに対応するファームウェアとして表示されません。リポジトリ画面で情報を確認してください。間違いがある場合は、一度リポジトリから削除したあとに、正しい情報でインポートを実行してください。
- ファームウェアの版数を下げることができないため、ノードの現行バージョンより古いファームウェアは、最新バージョン欄に表示されません。ノードの現行バージョンと、インポートしたファームウェアの版数を確認してください。

現象:PCIカードのファームウェアアップデートに失敗する。

原因·対処

PCIカードのファームウェアの動作は、PCIカードが搭載されているサーバのOSに依存します。ファームウェアデータ添付のドキュメント、または入手元を参照しファームウェアがサーバのOSに対応しているか確認してください。

現象:リリースノート内の文字が正常に表示されない

原因·対処

ご利用のブラウザのエンコードの設定によって、リリースノートの表示が正常に行われない場合があります。エンコードの設定を確認してください。

現象:ETERNUS DXモデルのファームウェアアップデートに失敗する。

原因·対処

「Update モード実施可能」な条件を満たしていない可能性があります。

ファームウェアと共に提供されている、留意事項のpdfファイルの「ファームウェアアップデート実行可否版数マトリクス」を参照して、 ご利用の環境が「Update モード実施可能」な条件を満たしているか確認してください。

プロファイル管理機能

現象:PRIMERGYサーバに対するプロファイル適用・再適用・適用解除がエラーになる。

原因·対処

プロファイル適用操作時に、対象ノードの電源がオンになっています。PRIMERGYへのプロファイル適用操作は、電源をオフにした状態で実行してください。

現象:スイッチ、ストレージに対するプロファイル適用・再適用・適用解除がエラーになる。

原因·対処

ISM以外からSSHやWeb経由で対象ノードに接続している状態のときは、ISMから設定を実行するとエラーになる場合があります。 ISMからノードを操作する際は、外部からの接続をログアウトしてください。

現象:プロファイル機能でOSインストールがエラーになる。

原因·対処

- ・ インストール対象のOSインストールメディアがインポートされていません。インストールするOSのインストールメディアをインポートしてからプロファイル適用を実行してください。
- インストール対象ノードとOS種別に対応したServerView Suite DVDがインポートされていません。インストール対象ノードとOS 種別をサポートしたServerView Suite DVDをインポートしてからプロファイル適用を実行してください。プロファイル内で使用す るServerView Suite DVD版数の指定がない場合は、インポートされた最新のDVDが使用されます。旧機種、旧OSの場合に は、使用するDVD版数をプロファイル内で設定してください。
- ・ PXE bootを動作させるための環境設定に問題がある可能性があります。以下を確認してください。
 - DHCPサーバが適切なIPアドレスをリースできるか
 - ノードのBIOS設定でPXE機能が無効になっていないか
 - ノードのオンボードLANとISM-VAが接続されているか、など

現象:エクスポートしたプロファイル/ポリシーをインポートするとエラーになる。

原因·対処

エクスポート元のISMに、そのままインポートすると、同一名の既存プロファイル/ポリシーが存在するためエラーとなります。インポートするファイル内の「ProfileName」を編集して、プロファイル名/ポリシー名を変更してください。

ネットワーク管理機能

現象:ネットワークマップに接続情報が表示されない。

原因·対処

ISMが接続情報を自動的に取得して表示するためには、各ノードのLLDP機能を有効にする必要があります。ノードの取扱説明書などを参照して、LLDPを有効にしてください。LLDP機能を持たないノードの場合は、ISM画面の手動接続定義で接続情報を入力してください。

現象:ネットワークマップの表示情報が古い、また正しい情報が表示されない。

原因·対処

- ・ ネットワークマップに表示される内容は、GUI画面上で[ネットワーク管理情報の更新]を最後に実行した時点の情報となります。 [ネットワーク管理情報の更新]を実行してください。
- ノードのポート状態などが変更された場合は、[ノード情報取得]を実行後に、[ネットワーク管理情報の更新]を実行してください。

ログ管理機能

現象:ノードログが収集されない、ノードログの収集に失敗する。

原因·対処

- ノードを新規に登録した時点では、ログ収集は行われない状態になっています。[ログ設定]でログ収集スケジュールを設定して ください。
- 「ノード詳細」画面の[ログ設定]タブ内で、ステータスが「対象外」となっていて、ログ収集用のアクションボタンが表示されない 場合は、ノードがログ収集対象外の機器か、ノード登録直後で機器情報が未取得の状態です。ログ収集対象ノードの場合は、 数分待ったあとに画面を更新してください。
- ログ収集時に指定するログ種類の[対象]を確認してください。スケジュール設定の場合は、[スケジュール実行有効化]にチェックが付いていることを確認してください。
- ・ GUI画面から[ログ収集実行]を実行するとログが収集できるが、スケジュール設定してもログが収集できていない場合は、スケジュール実行のタイミングでノードの電源がオフになっているなどが考えられます。スケジュールの内容を確認してください。
- ノードログのファイルサイズが10GBを超えると、ログの収集は実行されません。[イベント/タスク]-[イベント]を確認し、ログ収集の タイミングで「保管ログ保存領域の設定容量を超過しました。」または「ノードログ保存領域の設定容量を超過しました。」が記録 されている場合は、収集済みのログを一部削除してファイル容量を減らしてください。

現象:ノードログ収集の設定ができない。

原因·対処

ノードのステータスが「対象外」となっている場合は、ノードがログ収集のサポート対象であるか確認してください。サポート対象で 「対象外」となっている場合は、ISMがノード情報を取得できていないことがあるので、ノードとのネットワーク接続やノードプロパティ の設定を確認したあと、[ノード情報取得]を実行してください。

現象:ノードログ収集で、「オペレーティングシステム」、「ServerView Suite」が指定できない。

原因·対処

- ・対象ノードのOS情報が登録されていないか、ISMがノードのOS情報を未取得の場合は指定できません。OS情報を登録後に [ノード情報取得]を実行してください。
- ・ OSの種類によっては、「ServerView Suite」は取得対象外のため指定できません。