FUJITSU

FUJITSU Software
ServerView Infrastructure Manager V2.2

ユーザーズマニュアル

CA92344-2044-01
2017年12月

まえがき

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。

ISM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 V2.2 ユーザーズマニュアル	ServerView Infrastructure Manager V2.2 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 V2.2 スタートガイド	ServerView Infrastructure Manager V2.2 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 V2.2 操作手順書	ServerView Infrastructure Manager V2.2 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 V2.2 REST API リファレンスマニュアル	ServerView Infrastructure Manager V2.2 REST API リファレンスマニュアル	お客様が作成したアプリケーションとISMを連携する際に必要なAPIの使用方法、サンプル、パラメータ情報などを説明したマニュアルです。
FUJITSU Software ServerView Infrastructure Manager V2.2 用語集	ServerView Infrastructure Manager V2.2 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、当社の本製品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。

ポイント

ポイントとなる内容について説明します。

注意

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	略称	
Microsoft® Windows Server® 2016 Datacenter	Windows Server 2016 Datacenter	Windows Server 2016
Microsoft® Windows Server® 2016 Standard	Windows Server 2016 Standard	
Microsoft® Windows Server® 2016 Essentials	Windows Server 2016 Essentials	
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 7.4 (for Intel64)	RHEL 7.4	Red Hat Enterprise Linux または Linux
Red Hat Enterprise Linux 7.3 (for Intel64)	RHEL 7.3	
Red Hat Enterprise Linux 7.2 (for Intel64)	RHEL 7.2	
Red Hat Enterprise Linux 7.1 (for Intel64)	RHEL 7.1	
Red Hat Enterprise Linux 6.9 (for Intel64)	RHEL 6.9(Intel64)	
Red Hat Enterprise Linux 6.9 (for x86)	RHEL 6.9(x86)	
Red Hat Enterprise Linux 6.8 (for Intel64)	RHEL 6.8(Intel64)	
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)	

正式名称	略称	
Red Hat Enterprise Linux 6.6 (for Intel64)	RHEL 6.6(Intel64)	
Red Hat Enterprise Linux 6.6 (for x86)	RHEL 6.6(x86)	
SUSE Linux Enterprise Server 12 SP3 (for AMD64 & Intel64)	SUSE 12 SP3(AMD64) SUSE 12 SP3(Intel64) または SLES 12 SP3(AMD64) SLES 12 SP3(Intel64)	SUSE Linux Enterprise Server または Linux
SUSE Linux Enterprise Server 12 SP2 (for AMD64 & Intel64)	SUSE 12 SP2(AMD64) SUSE 12 SP2(Intel64) または SLES 12 SP2(AMD64) SLES 12 SP2(Intel64)	
SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel64)	SUSE 12 SP1(AMD64) SUSE 12 SP1(Intel64) または SLES 12 SP1(AMD64) SLES 12 SP1(Intel64)	
SUSE Linux Enterprise Server 12 (for AMD64 & Intel64)	SUSE 12(AMD64) SUSE 12(Intel64) または SLES 12(AMD64) SLES 12(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel64)	SUSE 11 SP4(AMD64) SUSE 11 SP4(Intel64) または SLES 11 SP4(AMD64) SLES 11 SP4(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for x86)	SUSE 11 SP4(x86) または SLES 11 SP4(x86)	
VMware® vSphere™ ESXi 6.5	VMware ESXi 6.5	VMware ESXi
VMware® vSphere™ ESXi 6.0	VMware ESXi 6.0	
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 V2.2 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。

SUSEおよびSUSEロゴは、米国およびその他の国におけるSUSE LLC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。

Ciscoは、米国およびその他の国における Cisco Systems, Inc. およびその関連会社の商標です。

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

その他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 2017 All rights reserved

本書を無断で複載・転載することを禁止します。

改版履歴

版数	提供年月	章・節・項	変更箇所	変更内容
01	2017年12月	－	－	新規作成

目　次

第1章 ServerView Infrastructure Managerの概要 1
1.1 概要 1
1.2 機能概要 2
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 2
1.2.3 プロファイル管理機能の概要 2
1.2.4 ログ管理機能の概要 3
1.2.5 ファームウェア管理機能の概要 3
1.2.6 ネットワーク管理機能の概要 3
1.2.7 仮想リソース管理機能の概要 4
1.3 ISM機能とインフラ運用管理シーン 4
1.3.1 インフラ運用管理シーンごとのISM機能イメージ 4
1.4 構成 7
1.5 システム要件 9
1.5.1 ISM-VA（仮想マシン）のシステム要件 9
1.5.2 管理端末のシステム要件 9
1.5.3 ISMの運用に必要なサービス要件 10
1.5.4 仮想リソースの動作要件 12
1.6 留意事項 12

第2章 ISMの機能 14
2.1 ユーザーインターフェース 14
2.1.1 GUI 14
2.1.2 FTPアクセス 16
2.1.3 コンソールアクセス 18
2.1.4 REST API 18
2.2 ISMの機能説明 18
2.2.1 ノード管理機能 19
2.2.1.1 データセンター/フロア/ラック/ノードの登録 19
2.2.1.2 データセンター/フロア/ラック/ノードの確認 27
2.2.1.3 データセンター/フロア/ラック/ノードの編集 28
2.2.1.4 データセンター/フロア/ラック/ノードの削除 28
2.2.2 モニタリング機能 29
2.2.3 プロファイル管理機能 37
2.2.4 ファームウェア管理機能 46
2.2.4.1 ノードのファームウェア版数の確認 46
2.2.4.2 ファームウェアのアップデート 46
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 51
2.2.4.4 ジョブ管理 51
2.2.5 ログ管理機能 52
2.2.6 ネットワーク管理機能 63
2.2.7 電力制御機能 71
2.2.8 仮想リソース管理機能 72
2.2.8.1 サポート対象の仮想リソース 73
2.2.8.2 仮想リソース管理GUI 74
2.2.8.3 仮想リソース管理の操作 75
2.2.9 仮想IO管理機能 84
2.2.10 ハードウェア設定バックアップ機能 85
2.2.11 プール管理機能 87
2.3 ISM運用基盤の機能説明 89
2.3.1 ユーザー管理機能 89
2.3.1.1 ISMのユーザーの管理 94
2.3.1.2 ユーザーグループの管理 96
2.3.1.3 Microsoft Active DirectoryまたはLDAPとの連携 99
2.3.1.4 ノードグループの管理 101

2.3.2 リポジトリ管理機能 104
2.3.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの導入 111
2.3.4 タスク管理 111
2.3.5 ISM-VA管理機能 112
2.3.5.1 ISM-VA管理機能のコマンド一覧 112
2.3.6 仮想化管理ソフトウェア管理機能 115
2.3.7 共有ディレクトリ管理機能 117
2.3.8 ISM連携管理機能 120
2.3.8.1 他ISMのステータス情報のリンク表示機能 120
2.3.8.2 他ISMのリンク用の証明書管理機能 121
2.4 ノード削除時、グループ変更時の操作 122
2.4.1 ノード削除時 122
2.4.2 グループ変更/解除時 122
2.4.3 ユーザーグループ削除時 122
2.4.4 ユーザーグループ名の変更時 123

第3章 ISMの導入 124
3.1 ISM導入の流れ 124
3.2 ISMの導入設計 125
3.2.1 ディスク資源の見積り 125
3.2.1.1 ログ保存容量の見積り 126
3.2.1.2 リポジトリの必要容量の見積り 126
3.2.1.3 ノード管理データ容量の見積り 127
3.2.1.4 障害調査ログ容量の見積り 127
3.2.1.5 保守資料容量の見積り 128
3.2.2 リポジトリの設定 128
3.2.3 ネットワークの設計 128
3.2.4 ノード名の設定 129
3.2.5 ユーザーの設定 129
3.3 ISM-VAのインストール 129
3.3.1 Microsoft Windows Server Hyper-Vへのインストール 129
3.3.2 VMware vSphere Hypervisorへのインストール 132
3.3.2.1 VMware ESXi 5.5またはVMware ESXi 6.0へのインストール 133
3.3.2.2 VMware ESXi 6.5以降へのインストール 135
3.3.3 KVMへのインストール 138
3.4 ISM-VAの環境設定 140
3.4.1 ISM-VAの初回起動 140
3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（初回） 141
3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（初回） 142
3.4.1.3 KVMで動作するISM-VAの場合（初回） 143
3.4.2 ISM初期設定 144
3.4.2.1 基本設定メニューを使用した初期設定 144
3.4.2.2 ismadmコマンドを使用した初期設定 145
3.5 ライセンスの登録 148
3.6 ユーザーの登録 149
3.7 仮想ディスクの割当て 149
3.7.1 ISM-VA全体に対する仮想ディスク割当て 150
3.7.2 ユーザーグループに対する仮想ディスク割当て 152
3.8 仮想リソース管理機能の事前設定 155

第4章 ISMの操作 156
4.1 ISMの起動と終了 156
4.1.1 ISM-VAの起動 156
4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（2回目以降） 156
4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（2回目以降） 157
4.1.1.3 KVMで動作するISM-VAの場合（2回目以降） 160
4.1.2 ISM-VAの終了 160
4.1.3 ISM-VAの再起動 161

4.1.4 ISMのサービス起動と停止 161
4.2 ISM-VA基本設定メニュー 161
4.3 ISM公開サービスポートの変更 164
4.4 ISM-VAのバックアップとリストア 164
4.4.1 ISM-VAのバックアップ 164
4.4.2 ISM-VAのリストア 166
4.5 保守資料の採取 166
4.6 仮想ディスクの管理 167
4.6.1 仮想ディスクの割当て解除 167
4.6.2 ISM-VA全体に対する仮想ディスクの追加割当て 169
4.6.3 ユーザーグループに対する仮想ディスク追加割当て 169
4.7 証明書設定 170
4.7.1 SSLサーバ証明書配置 170
4.7.2 SSLサーバ証明書表示 170
4.7.3 SSLサーバ証明書出力 170
4.7.4 SSLサーバ自己署名証明書作成 171
4.7.5 CA証明書のダウンロード 171
4.8 ライセンス設定 171
4.9 ネットワーク設定 172
4.10 イベント通知設定 173
4.10.1 イベント通知メール用証明書登録 173
4.10.2 アクションスクリプト登録 173
4.10.3 イベント通知メール用証明書表示 173
4.10.4 アクションスクリプト表示 173
4.10.5 イベント通知メール用証明書削除 173
4.10.6 アクションスクリプト削除 173
4.11 ISM-VAサービス制御 174
4.12 システム情報の表示 175
4.13 ホスト名変更 175
4.14 修正適用 175
4.15 プラグイン操作 176
4.15.1 プラグイン適用 176
4.15.2 プラグイン表示 176
4.15.3 プラグイン削除 177
4.16 障害調査ログ切替え 177
4.17 障害調査ログレベル切替え 177
4.18 coreファイル採取ディレクトリの指定 178
4.19 ISM-VA内部のDHCPサーバ 179
4.19.1 ISM-VA内部のDHCPサーバの設定 179
4.19.2 ISM-VA内部のDHCPサービスの操作 180
4.19.3 ISM-VA内部のDHCPサーバ情報の確認 181
4.19.4 DHCPサーバの切替え 181
4.20 MIBファイル設定 182
4.20.1 MIBファイル登録 182
4.20.2 MIBファイル表示 182
4.20.3 MIBファイル削除 182
4.21 ISM-VAのアップグレード 182

第5章 ノードの保守 184
5.1 メンテナンスモード 184
5.2 エラー発生時の調査方法 185

付録A ISM-VAのアンインストール 186

付録B トラブルシューティング 189

付録C プロファイル設定項目 194
C.1 PRIMERGY・PRIMEQUEST3000Bサーバ用プロファイルのBIOS/iRMC設定項目 194

C.2 PRIMEQUEST 2000・PRIMEQUEST 3000Eシリーズ パーティション用プロファイルのMMB設定項目 202
C.3 サーバ用プロファイルのOS設定項目 203
C.3.1 Windows Server用プロファイル 203
C.3.2 VMware ESXi用プロファイル 207
C.3.3 Red Hat Enterprise Linux用プロファイル 210
C.3.4 SUSE Linux Enterprise Server 用プロファイル 214
C.4 PRIMERGYサーバ用プロファイルの仮想IO設定項目 218
C.4.1 カード設定 218
C.4.2 ポート設定 218
C.4.3 ブート設定 219
C.4.4 CNA設定 220
C.4.5 仮想アドレス設定 221
C.5 ストレージ用プロファイルの設定項目 222
C.6 スイッチ用プロファイルの設定項目 225
C.6.1 SRX用プロファイル 225
C.6.2 VDX用プロファイル 227
C.6.3 イーサネットスイッチ（10GBASE-T 48+6／10GBASE 48+6）用プロファイル 230
C.6.4 CFX用プロファイル 232

第1章 ServerView Infrastructure Managerの概要

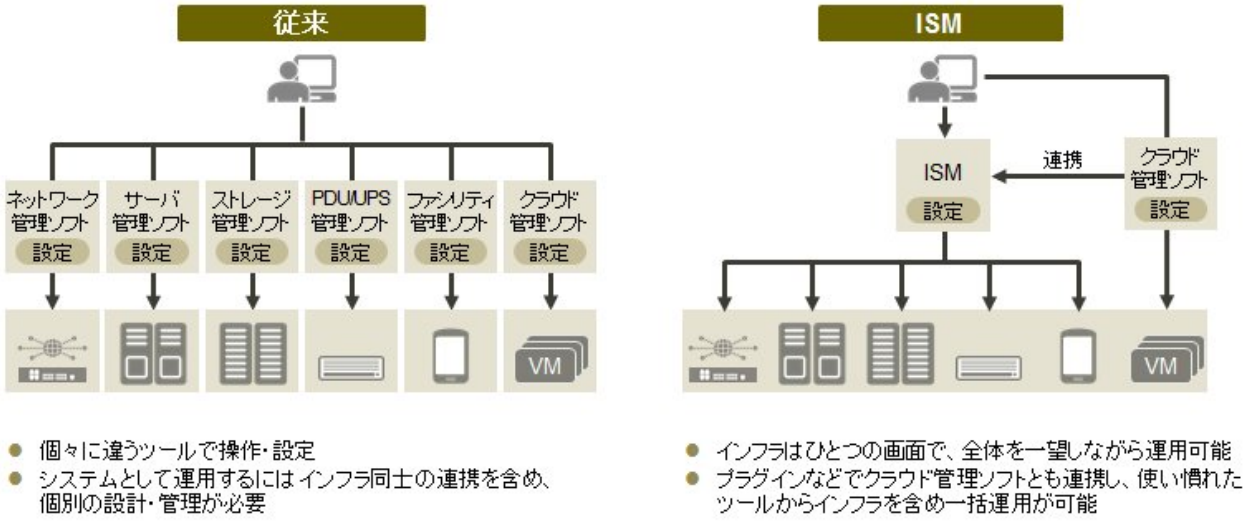
この章では、ServerView Infrastructure Managerの概要を説明します。

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

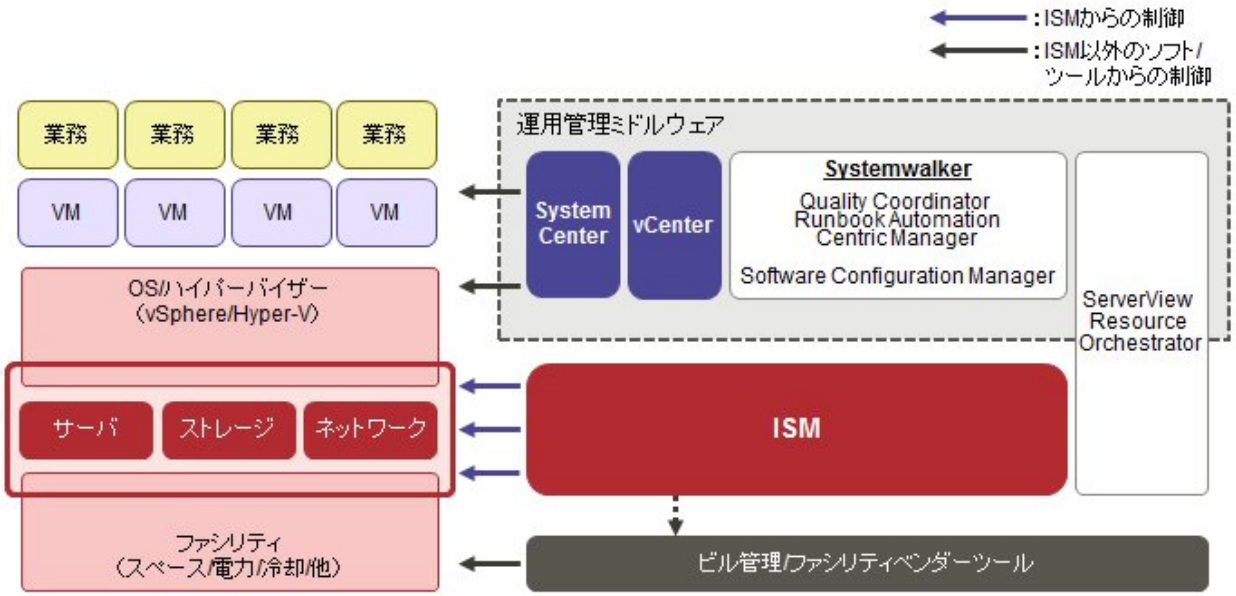
- インフラはひとつの画面で、全体を一望しながら運用可能
- プラグインなどでクラウド管理ソフトとも連携し、使い慣れたツールからインフラを含め一括運用が可能

- 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、当社の本製品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/

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・PRIMEQUEST 3000Bサーバに対する機能

  BIOS、iRMC、仮想IOの設定、およびOSインストールを、一括で実施します。

- PRIMEQUEST・PRIMEQUEST 3000Eサーバに対する機能

  BIOS、iRMC、MMBの設定、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。

- 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ネットワークマップで確認
- 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
- 管理対象ノードの物理的なポートとそのノード上の仮想マシンや仮想スイッチの仮想的なポートとの仮想的な接続関係をネットワークマップで確認
- ネットワークスイッチのVLAN、リンクアグリゲーション設定の確認、設定変更の実行

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。

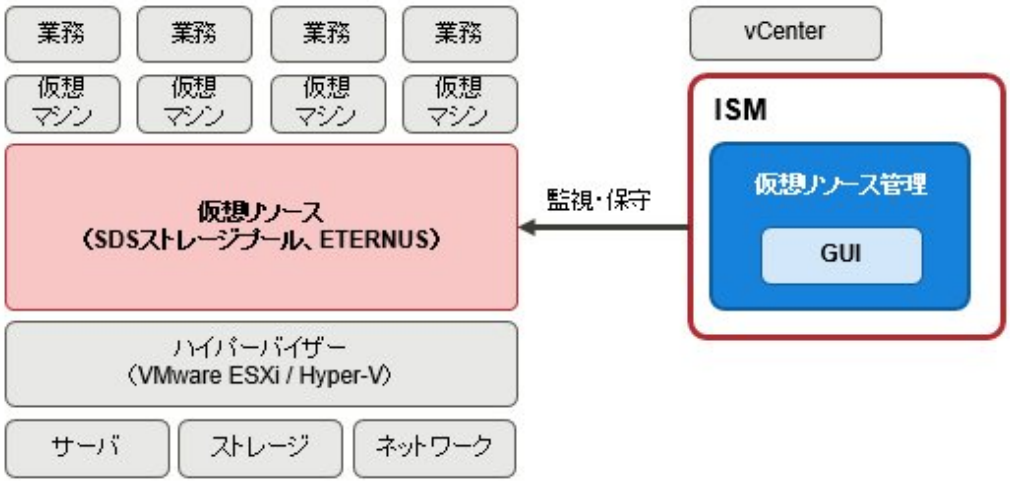
1.2.7 仮想リソース管理機能の概要

仮想リソース管理機能は、主に以下の用途で利用する機能です。

- 仮想リソースの使用状況や状態を、関係するハードウェア機器（ノード）の状態と連動して監視
- 仮想リソースを画面上で一元管理することで、スムーズな保守、リソースの再配置または追加（プロビジョニング）を支援

仮想リソース管理機能の詳細については、「2.2.8 仮想リソース管理機能」を参照してください。

図1.3 仮想リソース管理機能の概要



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。

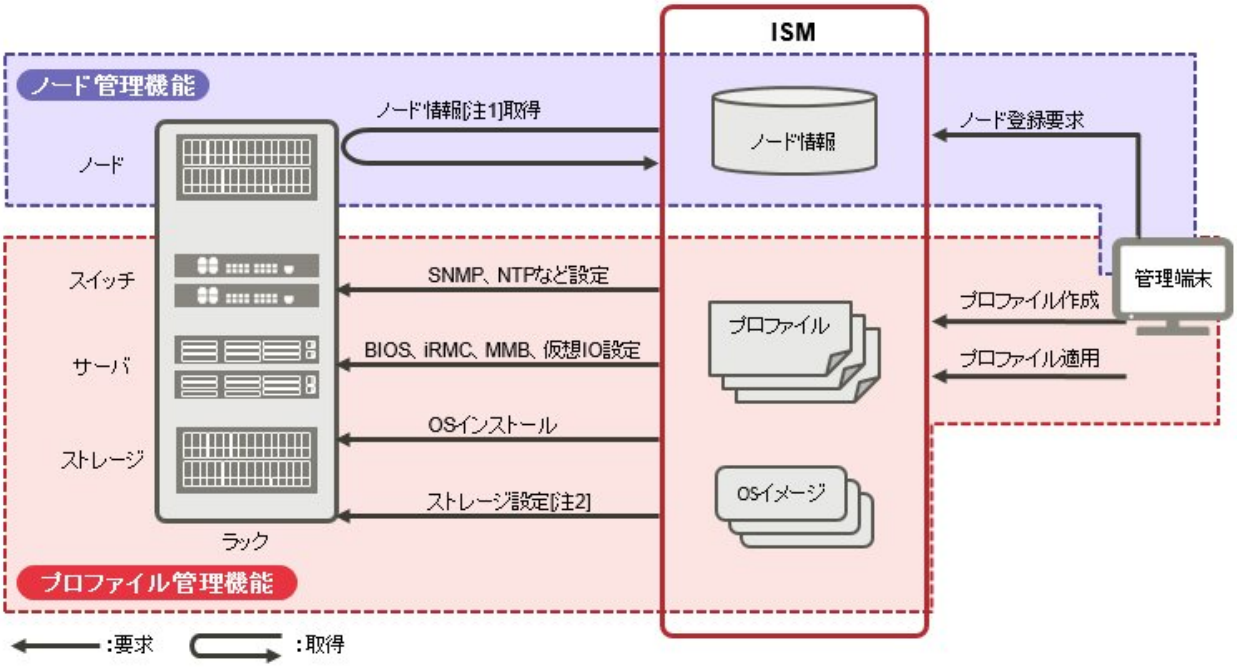
ISM機能	運用管理のシーン		
	システムの構築	管理対象ノードの監視運用	管理対象ノードの保守
ノード管理機能	○	○	－
モニタリング機能	－	○	－
プロファイル管理機能	○	－	－
ログ管理機能	－	○	○
ファームウェア管理機能	－	－	○
ネットワーク管理機能	－	－	○

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。

図1.4 機能イメージ（システムの構築）



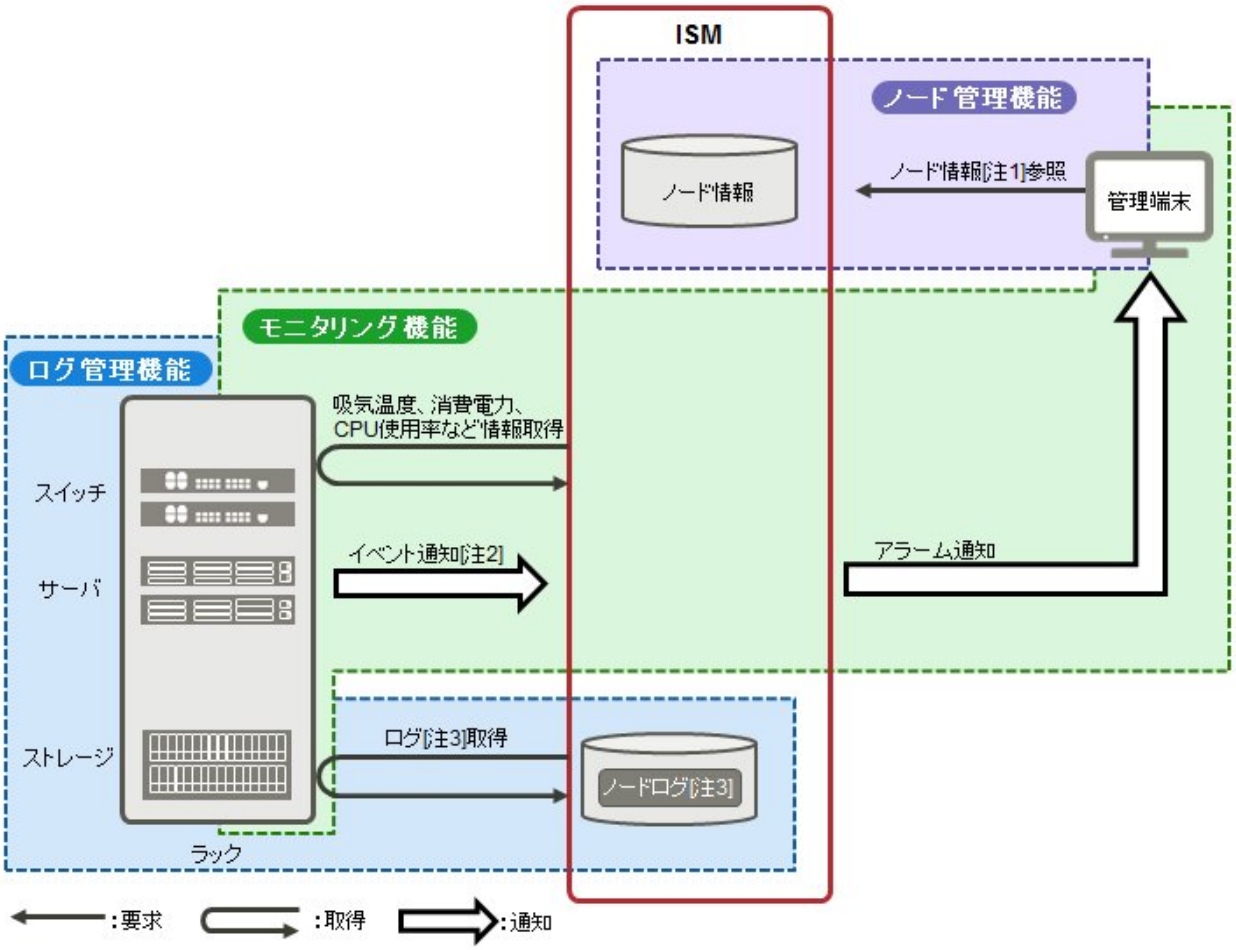
[注1]：ハードウェアのモデル名、シリアル番号、IPアドレスなど

[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1.5 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

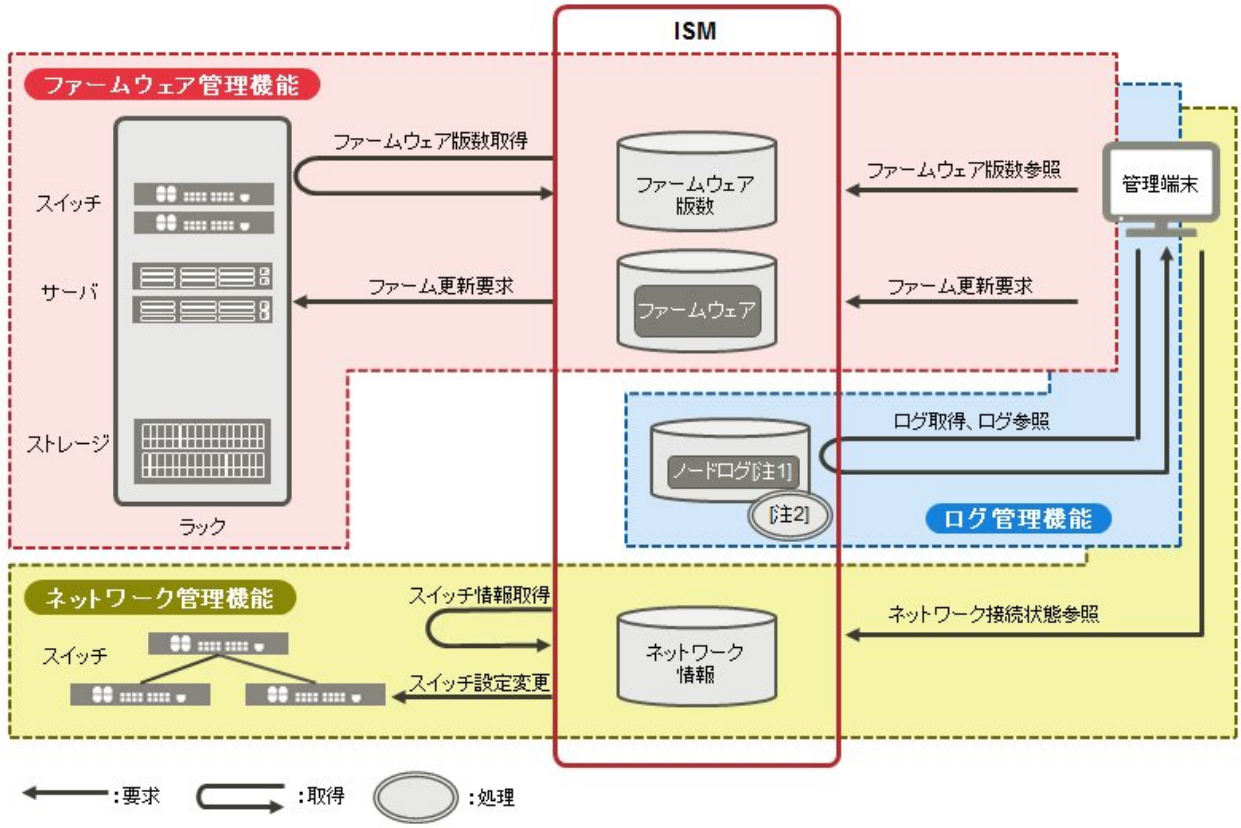
[注2]：SNMPトラップ

[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1.6 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

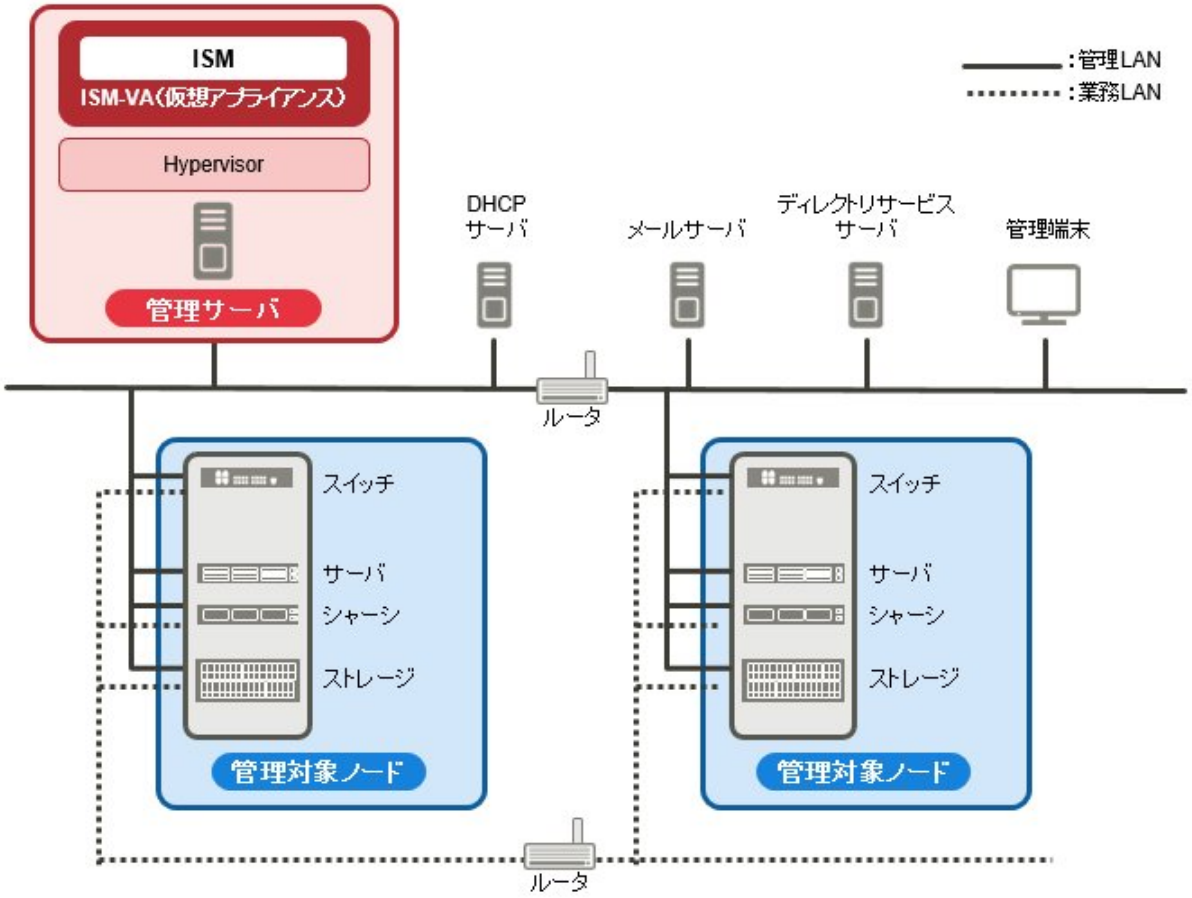
[注2]：ログ検索処理

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1.7 ネットワーク構成



注意

図1.6に記載しているISM外部で用意するサーバやサービスについての詳細は、「1.5.3 ISMの運用に必要なサービス要件」を参照してください。

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。
	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	ISMが状態監視、制御の対象とするノードです。
	ストレージ	

機器および機能		説明
	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)を管理LANに接続します。ISMのすべての機能を利用するためには、オンボードLANまたはLANカードも管理LANに接続します。

ネットワーク構成の設計および詳細情報については、当社の本製品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/「補足資料」

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。また、ISMの各種運用に必要な外部サービス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] [注4]
ネットワーク	1Gbps以上
ハイパーバイザー	Windows Server 2012/2012 R2/2016 VMware ESXi 5.5/6.0/6.5 Red Hat Enterprise Linux 7.2/7.3/7.4

[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。

[注4]:ISM-VA導入時に固定的に割り当てる必要があります。

サポートするハイパーバイザーの最新情報については、当社の本製品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/「補足資料」

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、当社の本製品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/「補足資料」

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

1.5.3 ISMの運用に必要なサービス要件

ISMの各種運用に必要な外部サービスは、以下のとおりです。

項目	説明
メールサーバ(SMTP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場合に、メールサーバが必要です。 [イベント]-[アラーム]-[SMTPサーバ]で設定します。 **注意** ISMに登録できるメールサーバは1つだけです。
ディレクトリサービスサーバ	以下の用途で使用する場合に、ディレクトリサービスが必要です。 1. ISMのユーザー管理で使用する場合 使用できるディレクトリサービスは、以下の2種類です。

項目	説明
	ー OpenLDAP ー Microsoft Active Directory [設定]-[ユーザー]-[LDAPサーバ設定]で、構築したサーバを登録します。 2. プロファイルのOSインストールで使用する場合 1.の設定は使用されません。 プロファイルのOSインストールの設定項目で指定されたディレクトリサービスが使用されます。詳細は、プロファイルのOSインストールを参照してください。 **注意** ・ ISMにはプライマリー、セカンダリの2つのLDAPサーバを登録できます。 ・ 監視対象ノードがディレクトリサービスを使用している場合、監視対象ノードが属しているディレクトリサービスとは連携していません。監視対象ノードにアクセスできるアカウントを個別に設定してください。
DHCPサーバ	以下の場合に、DHCPサーバが必要です。 ・ プロファイル管理機能でOSインストールを行う場合 ・ ファームウェア管理機能のOfflineアップデートを使用する場合 管理対象のノード(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。 **ポイント** DHCPサーバを別途準備する代わりに、ISM-VAに含まれているDHCPサーバ機能を利用することもできます。 ISM-VA内のDHCP機能の利用方法については、「4.19 ISM-VA内部のDHCPサーバ」を参照してください。
DNSサーバ	以下の用途で使用する場合に、DNSサーバが必要です。 ・ ISMにホスト名でアクセスしたい場合 ・ LDAP連携などISMの各種サーバ設定でFQDN を使う場合 DNSサーバをISMに設定する方法は、「4.9 ネットワーク設定」の「DNSサーバ追加」を参照してください。 **ポイント** ・ DNSサーバを使用せずにISMにホスト名でアクセスしたい場合は、ISM-VAに手動でホスト名を設定してください。手動でのホスト名設定方法は、「4.13 ホスト名変更」を参照してください。 ・ DNS サーバを使用しない場合、LDAP連携などISMの各種サーバ設定は、すべてIPアドレスで設定してください。
NTPサーバ	ISMと、監視対象ノードおよび管理クライアント間の時間がずれないよう同期させる場合に、NTPサーバが必要です。 NTPサーバをISMに設定する場合は、ismadmコマンドまたはismsetupコマンドを使用してください。 設定方法は、「3.4.2 ISM初期設定」の「NTP同期有効無効設定」、「NTPサーバ追加削除」を参照してください。

項目	説明
Proxyサーバ	管理クライアントからProxyサーバを経由してISMへアクセスする場合に、Proxyサーバが必要です。 注意 監視対象ノードとISM間は、Proxyサーバを経由して接続することはできません。
ルータ	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環境でISMを使用する場合に、各ネットワーク間で通信可能な状態にルータを設定しておく必要があります。 ゲートウェイをISMに設定する場合は、ismadmコマンドまたはismsetupコマンドを使用してください。 設定方法は、「4.9 ネットワーク設定」の「ネットワーク設定変更」を参照してください。

ネットワーク構成の設計および詳細情報については、当社の本製品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/「補足資料」

1.5.4 仮想リソースの動作要件

仮想リソース管理機能を使用するための要件については、以下を参照してください。

- 仮想リソース環境の要件:「2.2.8 仮想リソース管理機能」
- 事前設定要件:「3.8 仮想リソース管理機能の事前設定」

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
Windows	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
Linux(下記以外)	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
VMware ESXi (IP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)
VMware ESXi (IPアドレスがDHCP設定)	OSのインストールが完了し、再起動した状態	OSインストール途中(実行済み)

管理対象サーバにOSをインストールする際のRAID構成について

OSインストールには、ServerView Suite DVDが必要です。

ServerView Suite DVDのV11.16.04を使用してOSインストールを行う場合は、アレイコントローラーで構成するロジカルドライブは1個だけにしてください。

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[イベント]-[イベント]-[運用ログ]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。
- ログファイルの容量が、[設定]-[ユーザー]-[ユーザーグループ]でユーザーグループごとに設定した「保管ログ」および「ノードログ」それぞれの「警告しきい値」に達すると、ISMのイベントに警告イベントが登録されます。不要なログを削除してファイル量を削減してください。なお、同じく設定した「最大サイズ」に達した場合、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。

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 V2.2 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
- REST API

2.1.1 GUI

ISMではWebブラウザで動作するGUIを提供します。

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]を選択します。
  3. [証明書を表示]を選択します。
  4. [サーバ証明書]タブの[例外を追加]を選択します。
  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]を選択します。
  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]を選択します。
- 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]ボタンを選択し、以下の項目で[有効にする]を選択して[OK]ボタンを選択します。
     - [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]
     - [ActiveX コントロールとプラグイン]配下の[スクリプトを実行しても安全だとマークされているActiveXコントロールのスクリプトの実行]
     - [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]ボタンを選択します。
- 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]ボタンを選択します。

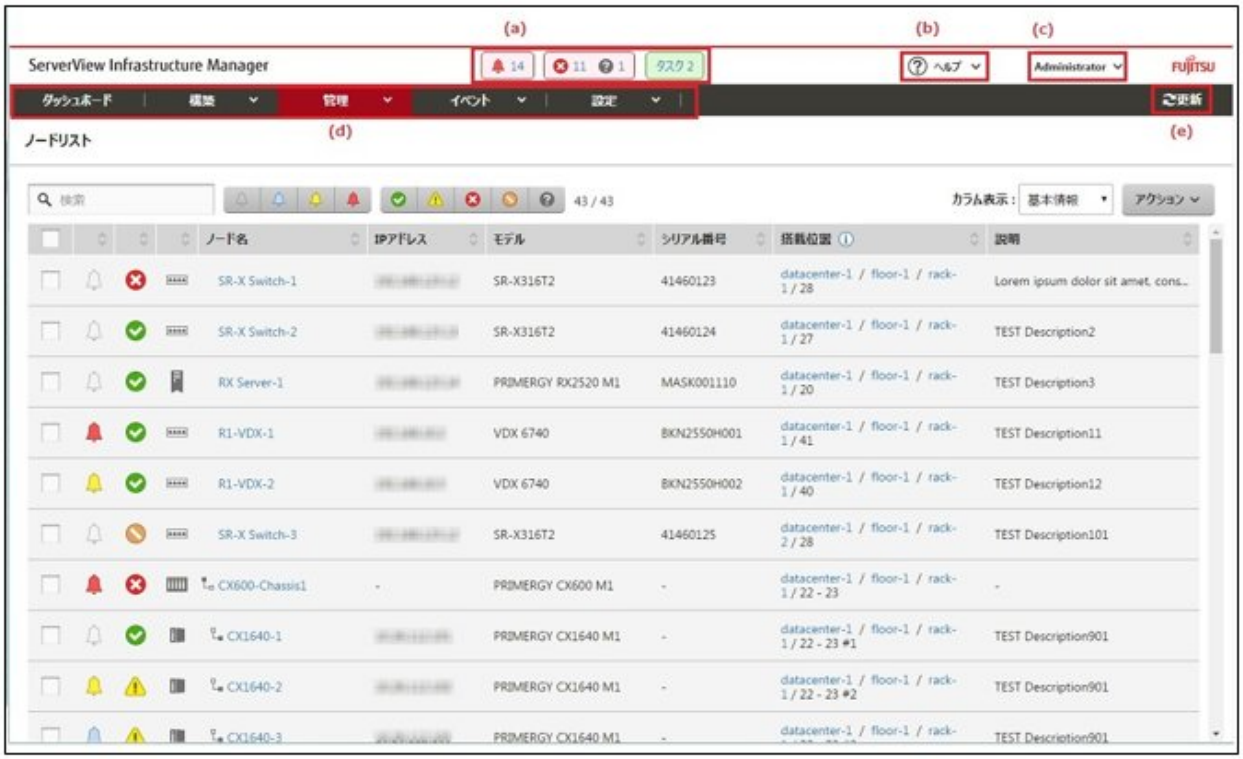
   セキュリティ証明書の警告が表示された場合は、「4.7 証明書設定」を参照して証明書の設定を行ってください。

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
- パスワード：admin

ISM GUIの画面構成は以下のとおりです。



(a) アラームステータス、ステータス、タスクアイコン

アラームステータス:

Errorアラームステータスのノード数が表示されます。Errorアラームステータスのノードがない場合には、Warningアラームステータスアイコンと Warningアラームステータスのノード数が表示されます。

ErrorまたはWarningアラームステータスのノードがない場合には表示されません。

ステータス:

Errorステータスのノード数、およびUnknownステータスアイコンとUnknownステータスのノード数が表示されます。

Errorステータスのノードがない場合には、Warningステータスアイコンと Warningステータスのノード数が表示されます。

ErrorまたはWarning、Unknownステータスのノードがない場合には表示されません。

タスク:

実行中のタスク数が表示されます。

(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]を選択します。

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する場合、[Language]を選択します。

(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

選択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、更新ボタンを選択して画面を更新してください。

以下の画面は、自動更新の設定を行うことで画面の自動更新が可能になります。

- 「ノード登録」画面
- 「タスク」画面

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。

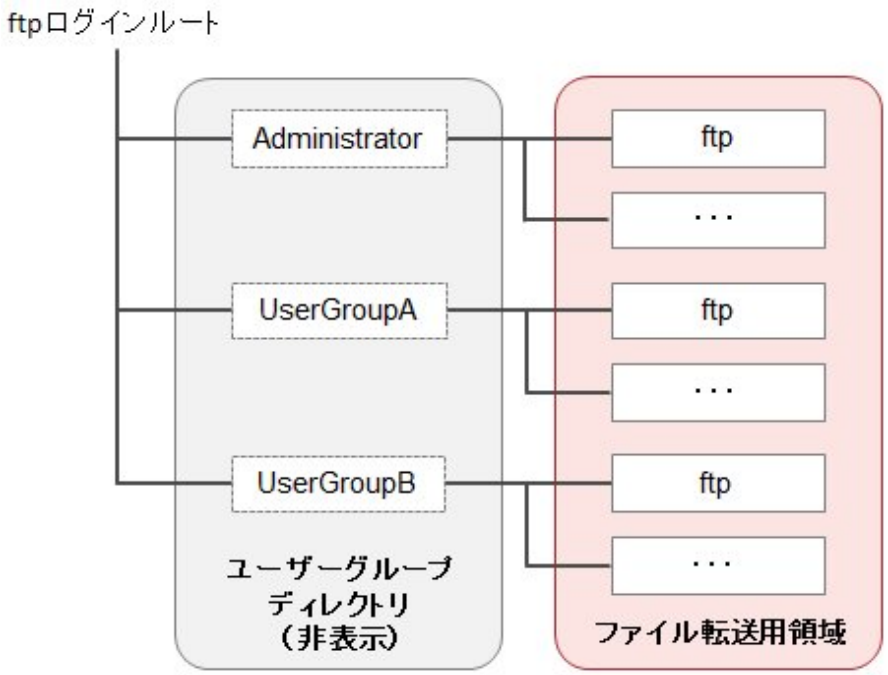
FTPで送受信するファイルの保存先は、下図のように「./<ユーザーグループ名>/ftp」となっています。

注意

- 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。
- パッチファイルなどのバイナリデータを転送する際は、バイナリモードで転送してください。

・ 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> ls
227 Entering Passive Mode (192,168,1,50,156,64).
150 Here comes the directory listing.
drwxr-sr-x    2 0        1001           33 Jun 16 20:36 bin
drwxrws---    3 992      989            26 Jun 16 21:54 elasticsearch
drwxrws---    3 0        1001           21 Jun 16 23:20 ftp
drwxrws---    2 0        0               6 Jun 16 20:36 imported-fw
drwxrws---    2 0        0               6 Jun 16 20:36 imported-os
drwxrws---    2 0        0               6 Jun 16 20:36 ismlog
```

```
drwxrws---    2 0        0               6 Jun 16 20:36 logarc
drwxrws---    8 0        0              75 Jun 17 14:03 profile
drwxrws---    2 0        0               6 Jun 16 20:36 tmp
drwxrws---    2 0        1001            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。

注意

[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。

2.1.4 REST API

ISMは、REST APIを備えています。これを使用して、ISMの機能を外部のプログラムから呼び出すことができます。詳細は、『ServerView Infrastructure Manager V2.2 REST API リファレンスマニュアル』を参照してください。

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
- 2.2.7 電力制御機能
- 2.2.8 仮想リソース管理機能
- 2.2.9 仮想IO管理機能
- 2.2.10 ハードウェア設定バックアップ機能
- 2.2.11 プール管理機能

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	実行可能	実行不可
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。

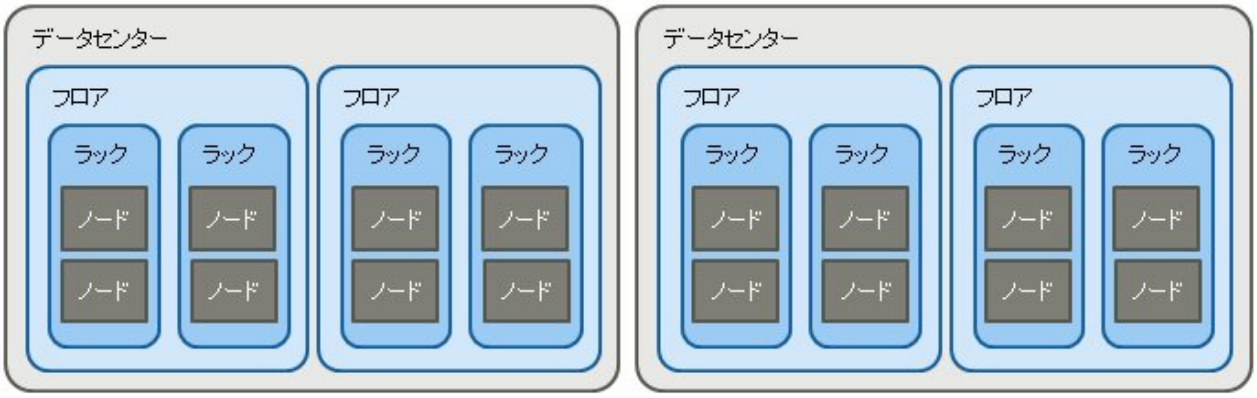
- 2.2.1.1 データセンター/フロア/ラック/ノードの登録
- 2.2.1.2 データセンター/フロア/ラック/ノードの確認
- 2.2.1.3 データセンター/フロア/ラック/ノードの編集
- 2.2.1.4 データセンター/フロア/ラック/ノードの削除

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 > ノードのラック内搭載位置番号（スロット番号/パーティション番号）」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
- ノードへのタグ付け

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、当社の本製品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/「補足資料」

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。ノードを登録するためには、事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。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ノード登録]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. [ノード手動登録]ウィザードに従い、設定項目を入力します。
   - ノード名

     ISM全体で、一意な名称を設定してください。
   - 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。
   - 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。
   - 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。
   - 説明

     ノードの説明(コメント)を自由に設定してください。
4. ノードのアカウント情報を入力します。
5. ノードのラック搭載位置情報を入力します。
6. 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。
7. ノードに設定するタグ情報を指定します。
8. 登録を実行します。

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ッション数があるため、正しく監視できません。
- ノードからSNMPv3でトラップ受信を行う場合、SNMPトラップ受信設定が必要になります。「2.2.2 モニタリング機能」の「トラップ受信設定」を参照してください。

ノード情報の管理

「ノードリスト」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、ノードの詳細画面を表示します。
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]-[イベント]-[運用ログ]にメッセージID「10020303」のログが出力されます。
4. 更新ボタンを選択して、ノードの詳細画面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。

ドメインユーザーIDを使用しサーバを監視する際には、ドメインID欄はActive Directoryのレルム名のFQDNを入力し、ユーザー名にはレルム名を除いたユーザー名を入力してください。

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、当社の本製品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/

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。

  アカウント情報にドメイン名、アカウントにドメインユーザーを登録した場合には、監視対象OSに別途ドメインユーザーで監視させるための設定を追加してください。

導入手順については、当社の本製品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/「補足資料」

- ドメインユーザーを使用してOSを監視する際には、DNSの設定およびドメイン環境の設定が必要になります。
  設定方法については、「3.4.2 ISM初期設定」を参照してください。
- 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。
- OS情報を登録する際にはドメイン名を大文字で記入してください。

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]タブを選択します。
3. [OS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]-[イベント]-[運用ログ]にメッセージID「10020303」のログが出力されます。
6. 更新ボタンを選択して、[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。

ノード検出機能には、以下の種類があります

- 手動検出
- 自動検出

手動検出

手動でノード検出を行います。以下の操作が行えます。

ー 手動検出設定を行い、実行する

ー 手動検出結果を確認する

ー 検出したノードを登録する

手動検出設定を行い、実行する

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。

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、当社の本製品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. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ノード登録]を選択し、「ノード登録」画面を表示します。
2. [アクション]ボタンから[検出]を選択します。
3. 検出に必要な情報を入力します。

4. 検出を実行します。

手動検出結果を確認する

「ノード登録」画面の画面更新を行い、[検出進捗]に表示されている検出処理の完了を待ちます。完了後、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検出に成功した場合、ステータスが成功となり、検出ノードを確認できます。

注意

- 検出ノード情報は、同じセッション内でのみ有効です。
- 検出結果には、サポート対象外の機器も表示される場合があります。サポート対象外の機器は登録しないでください。
- Brocade VDXスイッチの場合、ノード検出およびノード登録対象はBrocade VCS Fabricとなります。ファブリックに設定している仮想IPアドレスを指定してノード検出およびノード登録を実行してください。物理スイッチをノード検出した場合、検出結果は「自動登録のみ」となります。

検出したノードを登録する

手動検出によって検出され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]ボタンから[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。

   機器に設定されているIPアドレスを変更する場合、IPアドレス欄にある[編集]ボタンを選択して設定します。
   設定した場合、ノード登録時に機器に対してIPアドレス設定操作が実行されます。
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。登録されるアカウントは、「検出ノードリスト」画面の[成功した通信]カラムに表示されます。

注意

- 機器に設定されているIPアドレスを変更できるのは、以下の場合のみです。

  PRIMERGY M4シリーズ、PRIMEQUEST 3000B：機器がDHCP設定の場合のみ変更できます。機器に固定IPアドレスを設定している場合は、正しいIPアドレスを設定して検出し、IPアドレスを変更せずに登録を実行してください。
- IPアドレスを変更する場合、指定するIPアドレスがISMからアクセスできる範囲であることを確認してください。ISMからアクセスできないIPアドレスを指定した場合、機器に接続できなくなる可能性があります。
- Cisco CatalystスイッチおよびCisco Nexusスイッチの「ログ収集」や「ファームウェアアップデート」の機能を利用する場合は、ノード登録後、ノードの編集画面でSSH権限昇格パスワードを設定してください。

自動検出

自動でノード検出を行います。自動検出では、UPnP/Redfishによる自動検出が行われます。

また、自動検出タイプに応じた対象ノードは、以下のとおりです。

自動検出タイプ	対象ノード
UPnP	イーサネットスイッチ（10GBASE-T 48+6） イーサネットスイッチ（10GBASE 48+6）
Redfish	PRIMERGY M4シリーズ

自動検出タイプ	対象ノード
	PRIMEQUEST 3000B

自動検出機能では、以下の操作が行えます。

ー 自動検出を実行する

ー 自動検出結果を確認する

ー 検出したノードを登録する

自動検出を実行する

自動検出は自動的に実行されます。設定変更項目はありません。

注意

UPnP/Redfishによる自動検出を行うためには、以下の要件を満たす必要があります。

ー 対象機器側のAutoDiscovery機能がオンであること

ー 対象機器からのマルチキャスト送信パケットをISMが受信できるネットワーク構成であること

自動検出結果を確認する

機器が検出されると、「ノード登録」画面の[検出ノードリスト]にノードが表示されます。

検出したノードを登録する

自動検出によって検出され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]ボタンから[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。また、ISMに登録するIPアドレスを指定します。

   自動検出機能では、対象機器に設定されているIPv4とIPv6それぞれのIPアドレスが検出される場合があります。ISMに登録するIPアドレスを指定してください。

   機器のIPアドレスを変更する場合、設定するIPアドレス版数を選択し、[編集]ボタンを選択して設定します。
   設定した場合、ノード登録時に機器に対してIPアドレスが設定されます。
4. 通信方法を設定します。

   自動検出によって検出されたノードが表示されます。各ノードの通信方法を設定してください。機器のIPアドレスを変更する場合、通信方法の設定が必須です。
5. ノードのラック搭載位置情報を設定します。
6. ノードグループ情報およびタグ情報を設定します。
7. アカウント情報を設定します。
8. 登録を実行します。

注意

- IPv6リンクローカルアドレスで機器を管理することはできません。自動検出されたIPアドレスがIPv6リンクローカルアドレスのみの場合、IPアドレス設定が必要です。
- 機器に設定されているIPアドレスを変更できるのは、以下の場合のみです。

対象機器	変更できる場合
PRIMERGY M4シリーズ	機器がDHCP設定の場合のみ変更できます。

対象機器	変更できる場合
PRIMEQUEST 3000B	機器に固定IPアドレスを設定している場合は、正しいIPアドレスを設定し、IPアドレスを変更せずに登録を実行してください。
イーサネットスイッチ(10GBASE-T 48+6) イーサネットスイッチ(10GBASE 48+6)	機器が固定IPアドレス設定の場合のみ変更できます。機器に正しいIPアドレスを設定し、登録を実行してください。

- IPアドレスを変更する場合、指定するIPアドレスがISMからアクセスできる範囲であることを確認してください。ISMからアクセスできないIPアドレスを指定した場合、機器に接続できなくなる可能性があります。

ノードへのタグ付け

ISMではノードに対して自由にタグを設定できます。タグはユーザーが自由にノードをグルーピングするための情報を付与する機能です。ノードをグルーピングするための機能としてノードグループも存在しますが、ノードグループはユーザーのアクセス制御を行います。それに対して、タグはアクセス制御とは絡めずに設定できます。また、ノードに対して複数のタグを設定できます。

例えば、同じ目的を持つノード群に対してタグを設定することで、フィルタリングにより同じタグを持つノードリストを表示して管理できるようになります。

ノードへのタグ付けはノードの登録時に実行できます。また、ノードを登録したあとでも設定できます。

ノード登録後、タグを設定する

ノード登録後、タグを設定する際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]を選択します。
2. 対象ノード名を選択し、[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. タグ情報を編集します。
5. [適用]を実行し、編集内容を反映します。

複数のノードに対して一括でタグを編集する

複数のノードに対して一括でタグを編集できます。一括でタグを編集する際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]を選択します。
2. タグを編集するノードを選択し、[アクション]ボタンから[タグ編集]を選択します。
3. タグ情報を編集します。
   - タグを追加する場合

     [タグ一括追加]欄に新規タグを入力するか、既存のタグを選択して[追加]を選択します。
   - タグを一括で削除する場合

     [タグ一括削除]欄からタグを選択し、[削除]を選択します。
   - 個別のタグを削除する場合

     [対象ノード]の[タグ]欄に表示されているタグの[x]を選択します。
4. [適用]を実行し、編集内容を反映します。

タグによるフィルタリングを実行する

タグを指定してノードをフィルタリングする際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]を選択します。
2. [フィルター]ボタンを選択します。
3. フィルタリングしたいタグ名を入力して、[フィルター]を実行します。

   指定したタグが設定されているノードが[ノードリスト]画面に表示されます。

ポイント

フィルタリング結果のノードを選択し、[プロファイル適用]や[ファームウェアアップデート]を実行できます。プロファイル適用やファームウェアアップデートについては、「2.2.3 プロファイル管理機能」および「2.2.4 ファームウェア管理機能」を参照してください。

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。

ドメインユーザーIDを使用して仮想化管理ソフトウェアを監視する際には、ドメインID欄はActive Directoryのレルム名のFQDNを入力し、ユーザー名にはレルム名を除いたユーザー名を入力してください。

その場合、GUIの表示項目には、そのドメインユーザーの権限で取得できる情報だけが表示されます。

監視対象OSに関する設定方法については、当社の本製品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/「補足資料」

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

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

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

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

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。

注意

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

  更新ボタンを選択します。

- 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。

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。

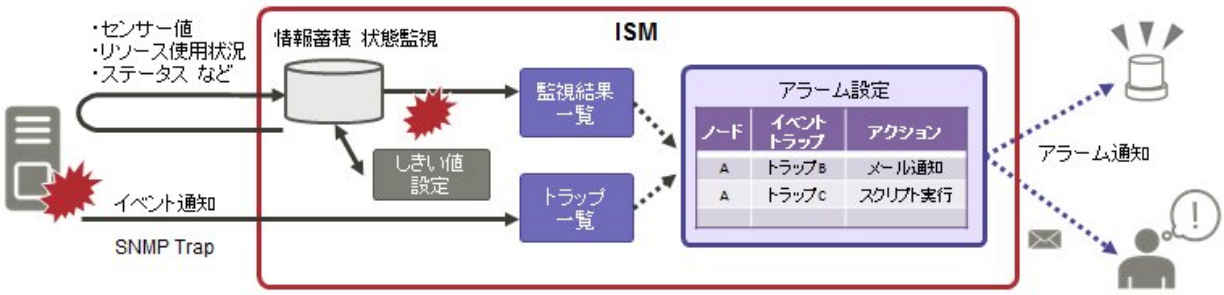
2.2.2 モニタリング機能

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4つがあります。

- 監視項目/しきい値の設定
- ネットワーク統計情報監視機能
- 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。 対象はPRIMERGYのみとなります。

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。
平均消費電力/平均吸気温度	消費電力、吸気温度の3分ごとの平均値を監視します。電力制御機能が有効で、電力制御設定の対象となっているノードのみ監視可能です。

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. [監視アクション]ボタンから[追加]を選択し、監視項目を追加します。

ネットワーク統計情報監視機能

ネットワークスイッチについて、ポート単位で各種統計情報（トラフィックなど）を取得し、しきい値監視を設定できます。

ネットワーク統計情報監視/しきい値監視の設定手順

1. ISMのGUI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. [ネットワーク統計]タブを選択します。

4. [ネットワーク統計アクション]ボタンから[編集]を選択し、ネットワーク統計情報監視を有効にします。

注意

ネットワーク統計情報監視を使用する場合、対象ノードのSNMPアカウントはv2cまたはv3を使用してください。

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。
トラップ転送/送信	受信したSNMPトラップを外部SNMPマネージャーに転送、またはISM内部で検出したイベントをSNMPトラップとして送信します。転送の場合、以下の転送タイプを選択できます。 ・ ISMを送信元として転送 転送されたSNMPトラップはISMから直接送信されたように処理されます。送信元情報以外は受信したトラップ情報をそのまま転送します。 ・ 受信したトラップをそのまま転送 受信したトラップがそのままSNMPマネージャーに転送されます。
Syslog転送	外部Syslogサーバに、イベント/トラップのメッセージを転送します。

ポイント

Syslog転送を使用する場合、外部Syslogサーバとして以下のOSをサポートしています。

- RHEL 6、RHEL 7
- CentOS 6、CentOS 7
- SLES 11、SLES 12

Syslogを受信できるようにするため、外部Syslogサーバにroot権限でログインし、以下の手順で設定を変更します。ここでは、受信のために最低限必要な設定について説明します。

[RHEL 6、RHEL 7／CentOS 6、CentOS 7／SLES 12の場合]

1. 以下のコマンドを実行し、/etc/rsyslog.confの編集を開始します。

```
# vi /etc/rsyslog.conf
```

2. 下記内容を追記します。

```
$ModLoad imtcp
$InputTCPServerRun 514
$AllowedSender TCP,  192.168.10.10/24      ※ISMのIPアドレス
```

3. 変更完了後、以下のコマンドを実行し、rsyslogデーモンを再起動します。

   ー RHEL 7／CentOS 7／SLES 12の場合

```
# systemctl restart rsyslog
```

   ー RHEL 6／CentOS 6の場合

```
# service rsyslog restart
```

[SLES 11の場合]

1. 以下のコマンドを実行し、/etc/syslog-ng/syslog-ng.confの編集を開始します。

```
# vi /etc/syslog-ng/syslog-ng.conf
```

2. 下記内容を追記します。

```
source src {

      ～略～

tcp(ip("0.0.0.0") port(514));          ※左行を追記、ISMのIPアドレスを使用
}
```

3. 変更完了後、以下のコマンドを実行し、syslogデーモンを再起動します。

```
# service syslog restart
```

マクロ

メール送信の件名や本文内、およびスクリプト実行時の引数指定に、以下に示すマクロ(自動変数)機能が使用できます。これらのマクロは、自動的にノード情報やイベント情報に置換されます。

また、アラーム設定を作成したときに指定した対象種別に応じて、使用できるマクロに差異があります。

各マクロの一覧と対象種別との対応関係は、以下のとおりです。

凡例:○＝使用できる、×＝使用できない

マクロ表記方法	概要	対象種別	
		ノード	システム
$_ISM	ISMホスト名	○	○
$_TRGTYPE	イベントの対象(SystemまたはNode)	○	○
$_TRG	イベントの対象名(ノード名)	○	×
$_IPA	ノードのIPアドレス	○	×
$_IDN	ノードのシリアル番号	○	×
$_MDL	ノードのモデル名	○	×
$_DC	ノードが設置されているデータセンター名	○	×
$_FLR	ノードが設置されているフロア名	○	×
$_RACK	ノードが設置されているラック名	○	×
$_POS	ノードのラック搭載位置 機器により表示形式が異なります。 ・ 1Uサーバが2Uに搭載されている場合 :2U	○	×

マクロ表記方法	概要	対象種別	
		ノード	システム
	・CX400シャーシ(2U)が2Uに搭載されており、そのスロット2に対象のサーバが存在する場合 :2-3U slot#2 ・BX900シャーシ(10U)が2Uに搭載されており、その背面スロット2に対象のコネクションブレードが存在する場合 :2-11U CB#2 ・PDUが搭載されている場合 :PDU2 ・RackCDUが搭載されている場合 :表示なし		
$_SEV	イベントの重要度	○	○
$_EVT	イベントのID	○	○
$_MSG	イベントのメッセージ	○	○
$_TIM	イベント発生時刻 UTC時刻をRFC3339形式で表示します。 (例:2017-01-01T00:00:00.000Z)	○	○

ポイント

マクロが使用できない場合(上記表で「×」のもの)や、置換するべき値が存在しない場合は、(none)と出力されます。

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[イベント]-[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、「4.10.2 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[イベント]-[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、「4.10.1 イベント通知メール用証明書登録」を参照してください。

トラップ転送/送信

SNMPトラップを転送/送信する場合、転送/送信先のSNMPマネージャーを登録する必要があります。

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[アラーム]を選択します。
2. 画面左側のメニューから[SNMPマネージャー]を選択し、「SNMPマネージャー設定」画面を表示します。
3. 画面右側の[アクション]ボタンから[追加]を選択し、SNMPマネージャー情報を登録します。

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[イベント]-[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。 アラームを発生させる対象となるイベントを重大度で指定するか、または個々のイベントを指定します(複数指定可)。
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。 アラームを発生させる対象となるトラップを重大度で指定するか、または個々のトラップを指定します。 「対象種別」で[システム]を選択した場合は表示されません。

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	ISM GUIでの アイコン表示	説明
Error	高	 赤色のベルマーク	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
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

アラームステータス	優先度	ISM GUIでの アイコン表示	説明
		黄色のベルマーク	・ MAJORまたはMINORレベルのSNMPトラップ
Info	低	 青色のベルマーク	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
None	-	 白色のベルマーク	何もイベントが検出されていない状態です。

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]-[イベント]を選択して、「イベントリスト」画面を表示し、各タブを選択して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。

ポイント

- アラームステータスは、自動的には解除されません。検出された、より優先度の高いステータスが表示されます。
- ノードの保守作業を行う際、計画的にノードを電源オフにすることがあります。保守作業による電源オフなどのアラームをISMが検出しないように、監視を一時的に停止する「メンテナンスモード」の機能があります。

  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の処理が抑止されるため、当該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。

トラップ受信設定

SNMPトラップを受信するための設定を変更する方法について説明します。受信プロトコルとしてv1、v2c、v3に対応しています。

SNMPトラップ受信設定の追加手順

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]を選択します。
2. 画面左側のメニューから[トラップ受信]を選択し、「トラップ受信設定リスト」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、トラップ受信設定を追加します。
4. 設定を行うSNMPバージョンを選択し、必要な情報を入力します。

   SNMPv3のトラップ受信設定を行う場合、受信対象ノードを選択して、「エンジンID」を設定してください。

注意

ー トラップ受信設定の追加/編集/削除を行った場合、変更は即時適用されます。リクエストを受け付けてから反映されるまで、一時的にすべてのSNMPトラップを受信しない状態となります。トラップ受信設定を変更する場合は、上記事象が問題とならないことを確認したうえで行ってください。

ー SNMPv3のトラップ受信を行う場合、ノードごとにSNMPトラップ受信設定が必要になります。ノード登録後、SNMPトラップ受信設定を行ってください。

MIBファイルの登録

ISMにMIBファイルを登録する方法と、登録されているMIBファイルの確認方法および削除方法について説明します。

MIBファイルについて

MIBとは、SNMPで管理されるネットワーク機器の状態の公開情報のことであり、RFC 1213で規定されているMIB2として標準化されています。MIBファイルは、この公開情報を定義したテキストベースのファイルを指します。SNMPトラップをやり取りするためには、受信側が機器側の提供するMIBファイルを保持しておく必要があります。

MIBファイルは、以下の場合に追加/更新します。

- 当社外装置からSNMPトラップを受信するために新規MIBファイルを追加したい場合
- ファームウェアアップデートに伴い、すでにISMに登録済みのMIBファイルを更新したい場合

注意

- 登録されているMIBファイルは削除できますが、削除したMIBファイルに定義されていたSNMPトラップを受信した場合、不明なトラップとして処理されます。
- 同一トラップが定義されたMIBファイルを複数登録しないでください。同一トラップが定義されたMIBファイルを複数登録した場合、同一トラップを複数受信したように扱われます。
- ISMがトラップの重要度などを扱うためには、取り込むMIBファイルが特定の書式で書かれている必要があります。指定外の書式で書かれたMIBファイルを取り込んだ場合、定義と異なる動作をする可能性があります。MIBファイルを取り込む前に書式に問題がないか確認してください。

  MIBファイルの書式に関する詳細は、当社の本製品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/「補足資料」

MIBファイルの登録方法

ISMに登録されていないMIBファイルを新たに追加します。

1. MIBファイルを用意します。このとき、MIBファイルに依存関係のあるすべてのファイルが必要になります。
2. ISM-VAにFTPで接続し、MIBファイルを転送します。
3. ISM-VA管理機能からMIBの登録コマンドを実行します。

詳細は、「4.20.1 MIBファイル登録」を参照してください。

ポイント

すでにISMに登録されているMIBファイルと同名のファイルを登録することで、MIBファイルをアップデートできます。

MIBファイルの確認

ISMに登録されているMIBファイル名の一覧を確認します。MIBファイル名の一覧を確認するには、ISM-VA管理機能のMIBファイル表示コマンドを実行します。

詳細は、「4.20.2 MIBファイル表示」を参照してください。

MIBファイルの削除

ISMに登録されているMIBファイルの登録を解除するためには、該当するMIBファイルを削除します。MIBファイルを削除するには、ISM-VA管理機能のMIBファイル削除コマンドを実行します。

詳細は、「4.20.3 MIBファイル削除」を参照してください。

ポイント

MIBファイルを削除する場合、依存関係に注意してください。依存関係のあるMIBファイルを削除した場合、トラップを受信できなくなる可能性があります。

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
- 管理対象ノードがサーバの場合に仮想IO設定を実施

  ISMのプロファイル管理機能では、仮想MACアドレス/仮想WWNの割当てのほか、サーバのブート設定も仮想IO設定に含みます。
- 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 ・ iRMC設定 ・ OSインストール ・ 仮想IO設定
	PRIMERGY BX PRIMERGY CX	・ BIOS設定 ・ iRMC設定 ・ OSインストール
	PRIMEQUEST 2000-Partition PRIMEQUEST3000E-Partition	・ MMB設定 ・ OSインストール
	PRIMEQUEST 3000B	・ BIOS設定 ・ 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 イーサネットスイッチ（10GBASE-T 48+6） イーサネットスイッチ（10GBASE 48+6）	・ 管理者パスワード設定 ・ SNMP、NTP設定
	CFX	・ 管理者パスワード、AAA設定 ・ SNMP、Interface、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

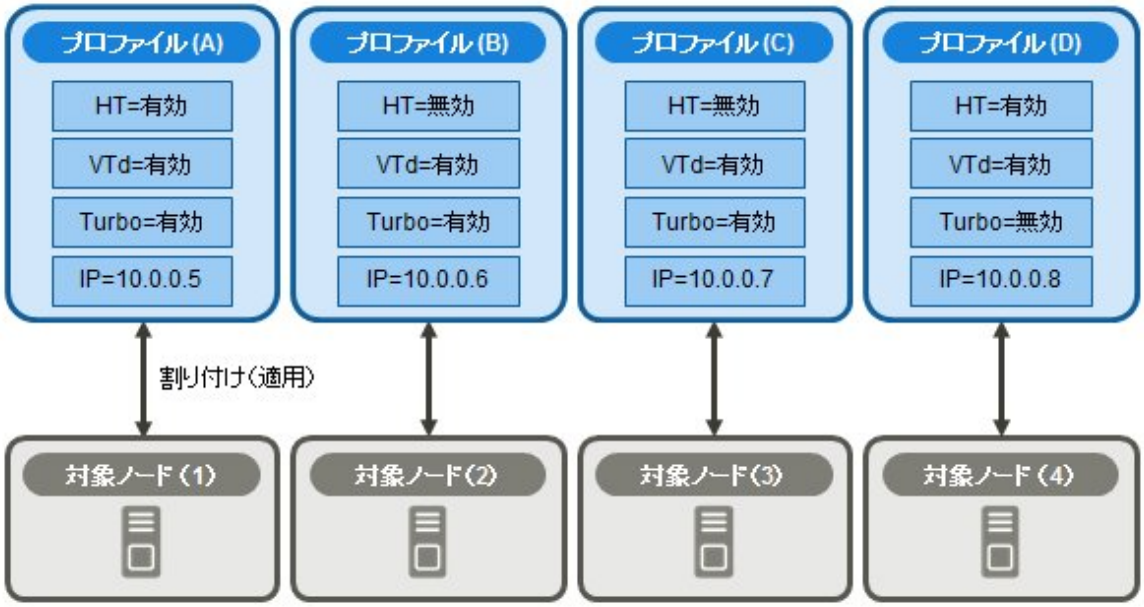
プロファイルの利用方法

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

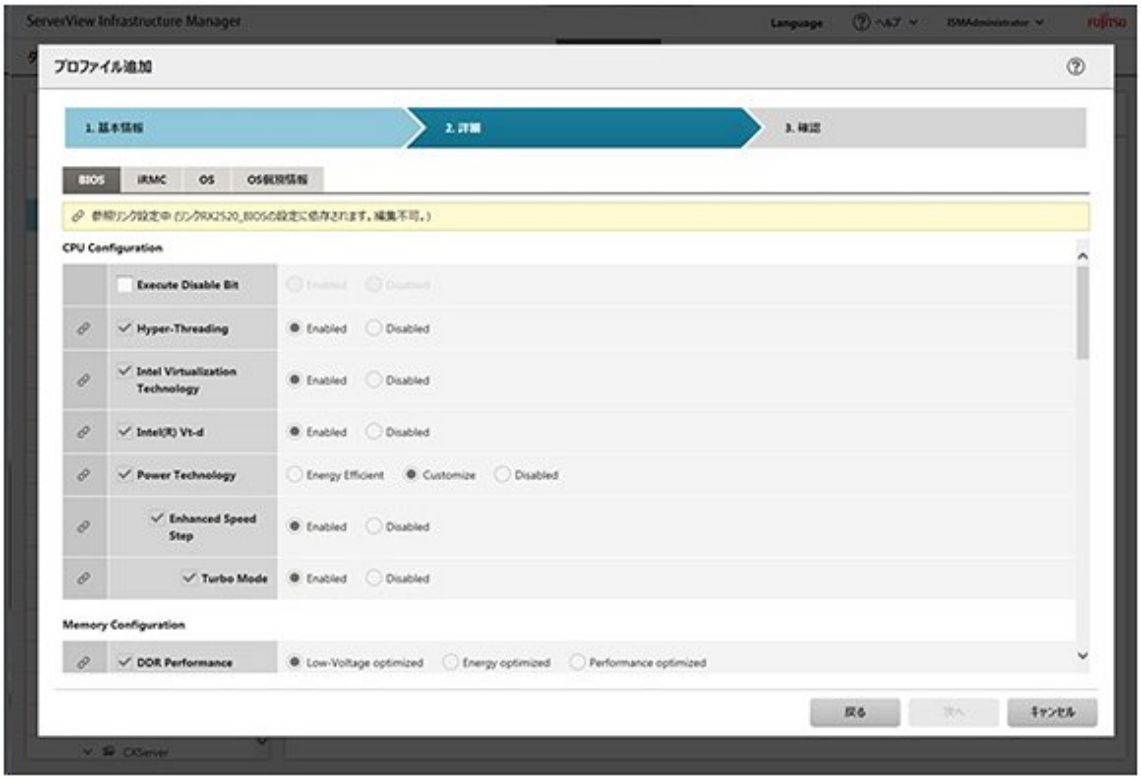


注意

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が新規にインストールされます。イン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）



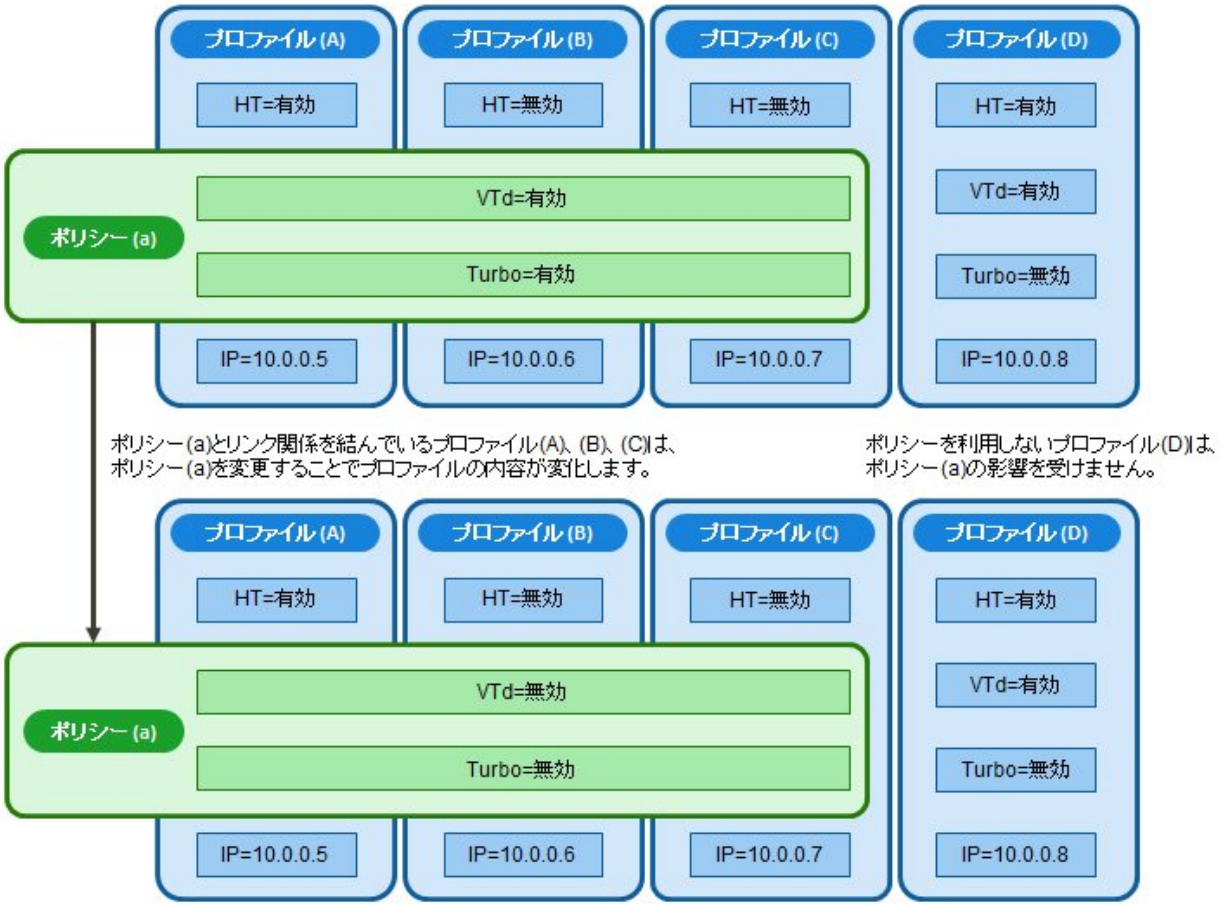
プロファイルとポリシー

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



注意

- 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。

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、iRMC設定、またはMMB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[構築]-[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[構築]-[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[構築]-[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[構築]-[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

注意

- 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。

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再編集し、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。

(ただし、ノードがサーバで、そのプロファイル内に「サーバのOSの設定」が記述されている場合、それらの項目は再編集できません。)

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再編集できます。そのとき、プロファイルを再編集してもノードの設定は連動して変化しません。ISM管理上、プロファイルの内容とノードの設定との不一致という状態となります。

任意のタイミングで再編集済みの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[構築]-[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。

注意

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。

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

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[構築]-[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。

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[構築]-[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[構築]-[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。

ポイント

- インポート完了後は、手順1でFTPサーバに転送したファイルは削除しても問題ありません。
- プロファイルにはパスワードなどのセキュリティ情報が含まれるため、エクスポートの際は、任意の暗号化キーを設定することが必須となっています。

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[構築]-[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[構築]-[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[構築]-[プロファイル]-[ポリシー設定]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[構築]-[プロファイル]-[ポリシー設定]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のインポートは、ISM管理者（Administratorグループのadministratorユーザー）で行ってください。全ユーザーグループで共有されるため、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。管理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、当社の本製品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/「補足資料」

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が起動することがあります。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（BIOS、iRMC、MMB、OS、仮想IO）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。
  ただし、OSは再適用できません。

- 電源オン状態でプロファイルを適用する

  サーバにプロファイルを適用する場合、通常は対象ノードの電源をオフにした状態で適用を行う必要がありますが、本動作を選択すると、対象ノードが電源オンの状態でもプロファイル適用が可能です。

  以下の点に注意してください。

  ー BIOS設定、iRMC設定、MMB設定の一部はサーバを再起動するまで変更が反映されません。

    プロファイル適用が完了したあと、任意のタイミングで再起動してください。

ー OSまたは仮想IO設定が適用対象の場合は、本モードは選択できません。

- 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、当社の本製品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
- 2.2.4.4 ジョブ管理

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。

1. 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。

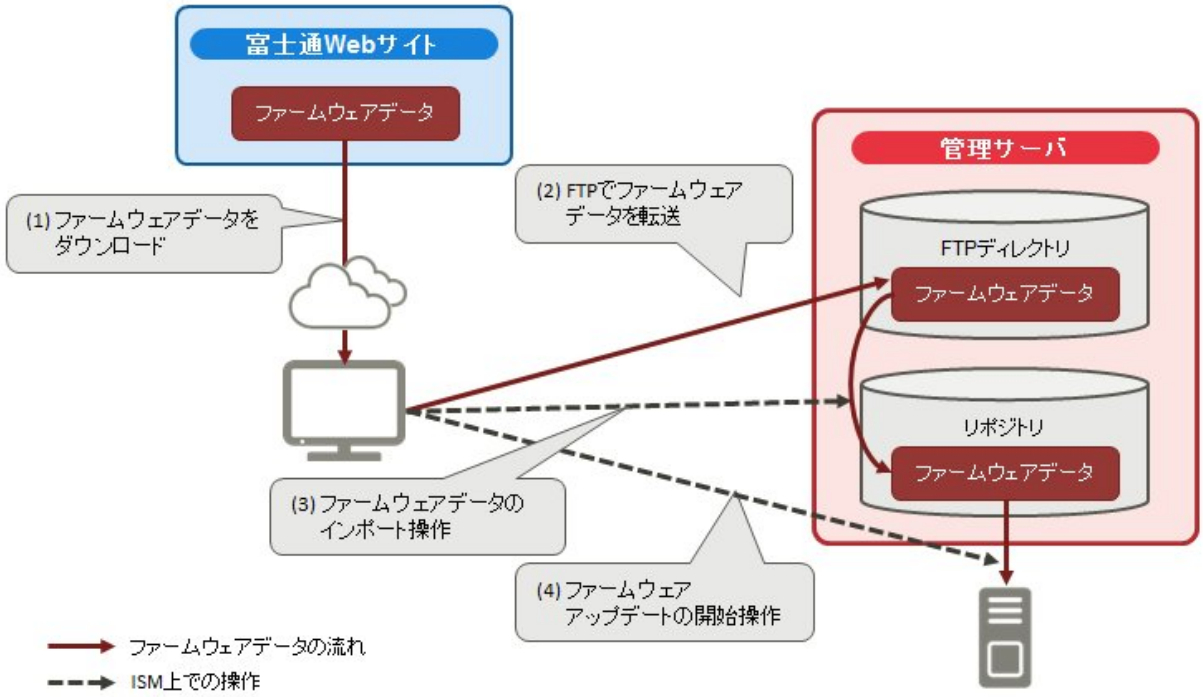
- ファームウェアアップデート方法
- アップデート時の動作
- ファームウェアアップデートの実施

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データをISMにインポートする作業が必要となります。

ファームウェアデータを富士通の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データ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データ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



ファームウェアアップデート方法

ファームウェア管理機能では、「Onlineアップデート」と「Offlineアップデート」の2種類のファームウェアアップデート方法が使用できます。

Onlineアップデート

ファームウェアアップデートを行う装置の電源がオンの状態で行うアップデート方法です。サーバ(BIOS/iRMC)の場合は、電源がオフの状態でもOnlineアップデートを実行できます。

ファームウェアアップデートの対象がサーバ(BIOS/iRMC/搭載PCIカード)、スイッチ、ストレージ、PRIMERGY BXシャーシMMBの場合に使用できます。

Offlineアップデート

ファームウェアアップデートを行う装置の電源がオフの状態で行うアップデート方法です。

ファームウェアアップデートの対象がサーバ(BIOS/iRMC/搭載PCIカード)の場合に使用できます。

Offlineアップデートを行う際は、事前にサーバの電源をオフにしてください。

Offlineアップデートに必要な準備作業

- 事前にServerView Suite DVDおよびServerView Suite Update 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。

  ServerView Suite Update DVD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のISOイメージをISM上に一度インポートしている場合、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ブート機能を使用します。

  PXEブートで使用する管理LANは、ノードの詳細画面の[ファームウェア]タブで設定できます。また、「ファームウェア」画面で対象のノードを選択した場合に表示される「ノード情報」画面からも設定できます。未設定の場合は、オンボードLANの先頭ポートが使用されます。

  管理LANからPXEブートが使用できるように、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。詳細は、当社の本製品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/「補足資料」

注意

「Onlineアップデート」と「Offlineアップデート」では、必要となるファームウェアデータが異なる場合があります。また、一部の搭載PCIカードにおいてサポート範囲が異なります。詳細は、当社の本製品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/

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。

表2.2 Onlineアップデートの場合

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のノードの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のノードの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(本体ファームウェア)	サーバの電源がオンの状態でアップデートが可能です。
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(CFX、PY CB Eth Switch 10/40Gb 18/8+2以外) 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アップデートを実施します。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。
スイッチ(CFX、PY CB Eth Switch 10/40Gb 18/8+2)	ノードの電源がオンの状態でファームウェアアップデートを実施します。新しいファームウェアに切り替えるためにノード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。再起動を行う際、システム構成によっては通信が遮断される場合があります。システム構成を考慮したうえで再起動を行ってください。
PRIMERGY BXシャーシMMB	ノードの電源がオンの状態でファームウェアアップデートを実施します。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。

表2.3 Offlineアップデートの場合

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)	サーバの電源がオフの状態でアップデートが可能です。
サーバ(BIOS)	ファームウェアアップデート中はサーバの電源投入および再起動が行われ、ファームウェアアップデート完了後は電源がオフになります。
サーバ(搭載PCIカード)	ファームウェアアップデート完了後に自動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の実施

注意

- アップデート中は以下の事項を遵守してください。
  - 対象ノードの電源操作を行わない。
  - 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。
  - リポジトリからインポートデータ、ファームウェアデータを削除しない。
- アップデート開始前に、ファームウェアデータ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データをインポートしておく必要があります。

  ファームウェアデータ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。
- CFX以外の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。
- Brocade VDXスイッチの場合、Brocade VCS Fabricを指定してファームウェアアップデートを行うことはできません。配下のVDXファブリックスイッチそれぞれに対して、ファームウェアアップデートを行ってください。
- ETERNUS DX/AF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したり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。
- Linux上のPCIカード(FC/CNA/LANカード)のファームウェアアップデートを行うためには、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ている必要があります。

  Emulex OneCommand Manager CLI、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。

- 一部のノードおよびPCIカードは、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が異なります。

  該当するノードおよびPCIカードと、表示状態については、当社の本製品Webサイトを参照してください。

  http://software.fujitsu.com/jp/serverviewism/environment/

- Ciscoスイッチ（Catalyst、Nexus）は、現行バージョンと最新バージョンの比較を行いません。

  現行バージョンと最新バージョンの値が異なる場合、アップデート対象となります。

- 一部のノードは、ファームウェアアップデートを段階的に適用する必要があります。各ファームウェアデータに添付されるドキュメントを参照してください。

- Onlineアップデートを使用したサーバ搭載の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。

  ー 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。

  ー 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のノードの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。

  ー 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のノードの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。

- 同時にファームウェアアップデート可能なノード数には上限があります。この上限数はISM-VA全体で50です。上限数より多いノードを指定してファームウェアアップデートを行った場合、はじめに上限数分のノードのファームウェアアップデートが実行され、残りのノードは先に実行しているファームウェアアップデートが終了してから実行されます。

  上限数のファームウェアアップデートを実行中にファームウェアアップデートを行った場合、先に実行しているファームウェアアップデートが終了してから実行されます。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア]を選択します。
2. アップデートを行うノードをメンテナンスモードに設定します。

   ノード名を選択し、[メンテナンスモード切替]ボタンで対象ノードをメンテナンスモードに設定します。
3. 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。
4. 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。
5. 画面表示に従い、操作を実行します。

   ー 時刻を指定してファームウェアアップデートする場合

   「ファームウェアアップデートを指定した時刻に開始する」を選択して実行する時間を指定してください。作業がISMのジョブとして登録されますので、作業の状態を「ジョブ」画面で確認してください。実行後の結果確認ダイアログボックスの「ジョブリスト:」欄にジョブIDが表示されます。ISMのGUIで[構築]欄の[ジョブ]を選択すると、ジョブ一覧が表示されます。ジョブIDを基に対象のジョブを識別してください。

   ー [アップデートをすぐに開始する]を選択して実行した場合

   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。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には、以下のタスクタイプが登録されます。

- Onlineアップデートの場合：Updating firmware
- Offlineアップデートの場合：Updating firmware（Offline mode）

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、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。

6. 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。

ポイント

- ファームウェアアップデートは、以下の手順で表示される画面でも同様の操作が行えます。
  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. 以下のどちらかを行います。
     - ノードリストの[カラム表示]から[ファームウェア]を選択します。
     - ノードリストで対象の[ノード名]を選択し、[ファームウェア]タブを選択します。
- 時刻を指定してファームウェアアップデートする場合は、事前にworkflowサービスを起動しておく必要があります。
  「2.3.5.1 ISM-VA管理機能のコマンド一覧」を参照して、ismadmコマンドでサービスを起動するように設定してください。

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[構築]-[ファームウェア]を選択します。
2. 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。
3. プルダウンメニューから更新バージョン、インポートデータを選択して、[次へ]ボタンを選択します。
4. [ドキュメント]欄で確認したいドキュメントを選択し、ドキュメントを確認します。

ポイント

- ファームウェアデータに添付されているドキュメントの確認操作は、以下の手順で表示される画面でも同様の操作が行えます。
  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. 以下のどちらかを行います。
     - ノードリストの[カラム表示]から[ファームウェア]を選択します。
     - ノードリストで対象の[ノード名]を選択し、[ファームウェア]タブを選択します。
  3. [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、インポートデータを選択して、[次へ]ボタンを選択します。
  5. [ドキュメント]欄で確認したいドキュメントを選択し、ドキュメントを確認します。
- ISMを使用したアップデートの方法は、ファームウェアデータ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、ファームウェアデータ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。ファームウェアデータは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。

2.2.4.4 ジョブ管理

時刻を指定してファームウェアアップデートを行う場合、その処理はジョブとして管理されます。

それぞれのジョブの状態は、操作した画面ではなく、「ジョブ」画面で一括表示されます。

実行中の処理を中止（キャンセル）する場合、実行前の処理を削除する場合、実行後の処理を削除する場合も「ジョブ」画面から操作します。

注意

ジョブの数には上限があります。ISM-VA全体で100を超えるジョブは登録できません。上限を超えないよう、不要なジョブは削除してください。

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。

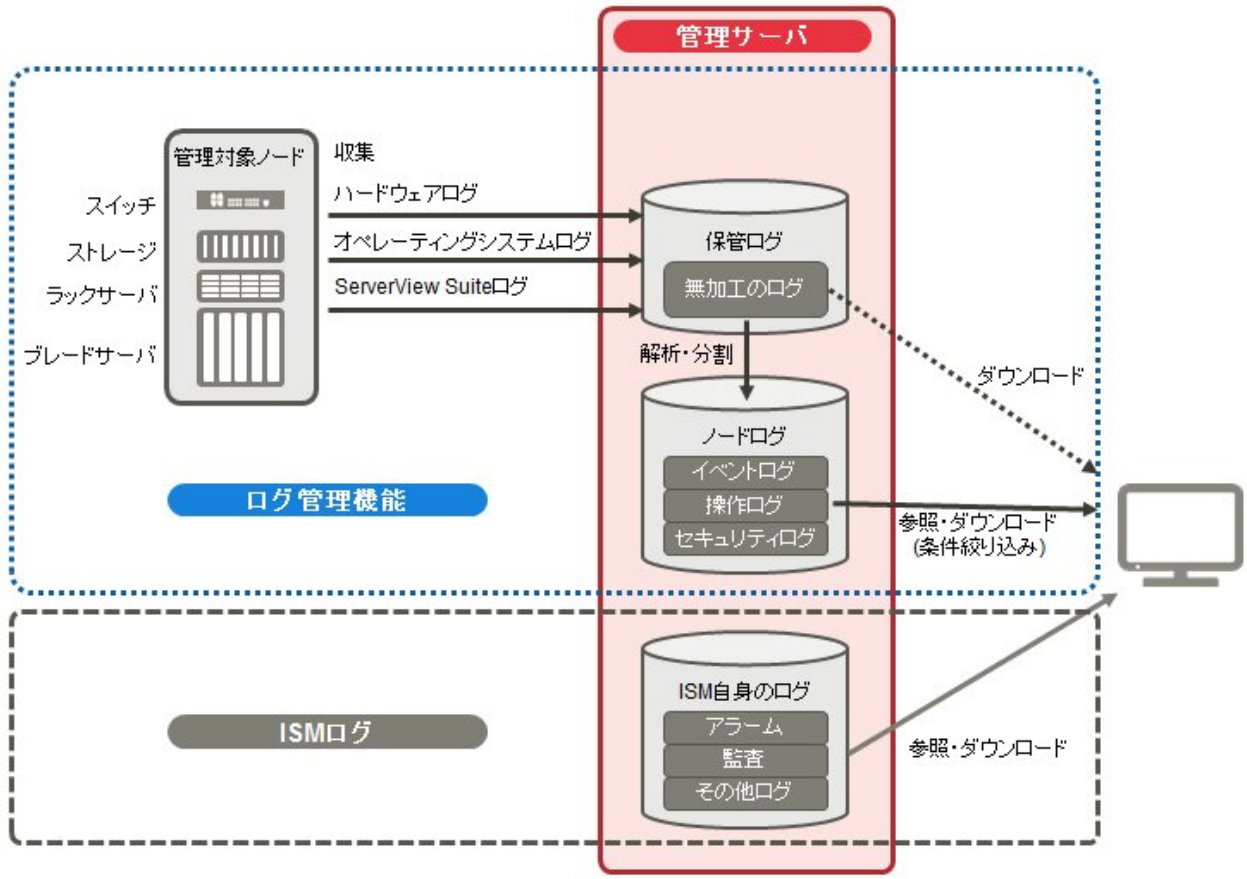
その設定に従ってノードから収集したログデータのひとかたまりを「保管ログ」と呼びます。

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



注意

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、当社の本製品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 System Report （iRMC S4以降を搭載したサーバ）	SEL
	PRIMEQUEST 3000B		
	IPCOM VX2		
シャーシ	PRIMERGY BX	show Log/MgmtBlade LogMgmtBladeAllコマンドの出力結果 set SystemInfo/Dump Started=trueコマンドの出力結果	show Log/MgmtBlade LogMgmtBladeAllコマンドの出力結果
	PRIMEQUEST 3000E	SEL	SEL
ストレージ	ETERNUS DX/AF	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
	ETERNUS NR（NetApp）	event log showコマンドの出力結果 /mroot/etc/logディレクトリ配下の各種ファイル	event log showコマンドの出力結果
コネクションブレード	Ethernet Switch	show tech-supportコマンドの出力結果	show logging buffered、または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）

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
	Fibre Channel Switch	supportshowコマンドの出力結果 supportsaveコマンドで作成される各種ファイル	supportshow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)
	CFX		
	イーサネットスイッチ(10GBASE-T 48+6) イーサネットスイッチ(10GBASE 48+6)	show tech-supportコマンドの出力結果	show logging persistent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)
	Cisco Catalyst	show tech-supportコマンドの出力結果	show logging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)
	Cisco Nexus		

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)
	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)
IPCOM OS	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)
	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)
	テクニカルサポート情報	―

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)

注意

- 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。

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さかのぼ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。

注意

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○曜日の○時○分」のように指定します。また、「毎月の第△○曜日の○時○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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ収集設定]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。

ポイント

ログ収集設定編集操作は、以下の手順で表示される画面でも同様の操作が行えます。

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. 以下のどちらかを行います。
   - ノードリストの[カラム表示]から[ログ設定]を選択します。
   - ノードリストで対象の[ノード名]を選択し、[ログ設定]タブを選択します。

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。

注意

- 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]-[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。
- 定期ログ収集開始後は、ログ収集を途中でキャンセルできません。そのため、対象ノードに対してファームウェアアップデート、プロファイル適用などのメンテナンスが予定され、定期ログ収集の実行時刻と重なる場合、メンテナンスが行えなくなる可能性があります。事前に定期ログ収集を無効にするか、スケジュール設定時刻の変更を推奨します。
- 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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ収集設定]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. ISMのGUIでグローバルナビゲーションメニュー上部の[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。

ポイント

手動ログ収集操作は、以下の手順で表示される画面でも同様の操作が行えます。

- ISMのGUIでグローバルナビゲーションメニューから[構築]-[ログ収集]を選択し、以下のどちらかを行います。
  - ログ収集メニューの[ログ管理]を選択します。
  - ログ収集メニューの[ノードログ検索]を選択します。
- 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、以下のどちらかを行います。
  - ノードリストの[カラム表示]から[ログ設定]を選択します。
  - ノードリストで対象の[ノード名]を選択し、[ログ設定]タブを選択します。

注意

- 手動ログ収集のキャンセルは、グローバルナビゲーションメニュー上部の[タスク]から行えますが、すでにログ収集が実行中の場合、ログ収集が完了するまでキャンセルは完了しません。
- 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。

ISMが保管する各種ログファイル(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))の総容量の上限(サイズ制限)とディスク容量監視(しきい値監視)の設定値はユーザーグループ設定に設定されています。ユーザーグループ設定については、「2.3.1.2 ユーザーグループの管理」を参照してください。

各種ログファイルの総容量が設定値に近づくと、グローバルナビゲーションメニューの[イベント]-[イベント]の[運用ログ]タブに警告/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、新たなログは保管されません。

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、新しいログが保管されるようになります。

条件	動作
ログファイルの総容量がディスク容量監視の設定値の容量を超えた場合 例) 上限設定値が10GB、ディスク容量監視の設定値が80%の場合、ログファイルの総容量が8GBを超えると右記動作を行います	• ログ収集は行う。 • [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 ノード(＜ノード名＞)のログ収集中に、ユーザーグループ(＜ユーザーグループ名＞)の保管ログ保存領域が(xxMB)となり、しきい値(xx%)(xxMB)を超過しました。

条件	動作
	「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(＜ノード名＞)のログ収集中に、ユーザーグループ(＜ユーザーグループ名＞)のノードログ(ダウンロード用データ)保存領域が(xxMB)となり、しきい値(xx%)(xxMB)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(＜ノード名＞)のログ収集中に、ノードログ(ログ検索用データ)保存領域が(xxMB)となり、しきい値(xx%)(xxMB)を超過しました。 「ノードログの削除」参照
ログファイルの総容量が上限設定値を超えた場合 例) 上限設定値が10GBの場合、ログファイルの総容量が10GBを超えると右記動作を行います	• ログ収集を行わない。 • [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。 ー 保管ログの場合 ノード(＜ノード名＞)のログ収集中に、ユーザーグループ(＜ユーザーグループ名＞)の保管ログ保存領域が設定容量(xxMB)に達しました。 「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(＜ノード名＞)のログ収集中に、ユーザーグループ(＜ユーザーグループ名＞)のノードログ(ダウンロード用データ)保存領域が設定容量(xxMB)に達しました。 「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(＜ノード名＞)のログ収集中に、ノードログ(ログ検索用データ)保存領域が設定容量(xxMB)に達しました。 「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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ノードログ検索]を選択します。
3. 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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ノードログ検索]を選択します。
3. [フィルター]ボタンを選択します。
4. フィルター画面で条件を入力し、[フィルター]ボタンを選択します。

   入力した条件に合致したログが表示されます。

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[CSVエクスポート]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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[ノードログ]タブを選択します。
3. 対象のノードにチェックを付けます。
4. [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、画面に従ってダウンロードファイル作成を実行します。

   「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。
5. ダウンロード用ファイルの作成完了を待ちます。

   作成状況は、画面上部に表示されるダウンロードファイル項目で確認します。
   または、グローバルナビゲーションメニュー上部の[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、「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。
6. ダウンロードファイルの作成が完了したら、[ダウンロード]ボタンを選択します。

ポイント

- ノードログのダウンロード操作は、以下の手順で表示される画面でも同様の操作が行えます。
  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. 以下のどちらかを行います。
     - ノードリストの[カラム表示]から[ログ設定]を選択します。
     - ノードリストで対象の[ノード名]を選択し、[ログ設定]タブを選択します。
- 複数のノードを選択した場合でも、ダウンロードファイルは1つのzipファイルにまとめられます。

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。
- ログ収集中のノードに対するダウンロードファイル作成は実行できません。ログ収集完了後にダウンロードファイル作成を実行してください。

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

```
NodeLog_＜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）2017年11月1日～2017年11月7日の期間を指定した場合

```
NodeLog_20171101-20171107.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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[保管ログ]タブを選択します。
3. ダウンロードする保管ログにチェックを付けます。
4. [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、画面に従ってダウンロードファイル作成を実行します。

   「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。

   また、[アクション]ボタンから[保管ログファイル確認]を選択し、表示された画面からでもダウンロード操作が行えます。
   この場合は、ダウンロードするファイルにチェックを付けます。
5. ダウンロードファイルの作成完了を待ちます。

   作成状況は、画面上部に表示されるダウンロードファイル項目で確認します。
   または、グローバルナビゲーションメニュー上部の[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。
6. ダウンロードファイルの作成が完了したら、[ダウンロード]ボタンを選択します。

ポイント

- 保管ログのダウンロード操作は、以下の手順で表示される画面でも同様の操作が行えます。
  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. 以下のどちらかを行います。
     - ノードリストの[カラム表示]から[ログ設定]を選択します。
     - ノードリストで対象の[ノード名]を選択し、[ログ設定]タブを選択します。
- 複数のノードを選択した場合や、複数の保管ログを選択した場合でも、ダウンロードファイルは1つのzipファイルにまとめられます。

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。
- ログ収集中のノードに対するダウンロードファイル作成は実行できません。ログ収集完了後にダウンロードファイル作成を実行してください。

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

```
ArchivedLog_＜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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[ノードログ]タブを選択します。
3. 対象のノードにチェックを付けます。

   複数のノードを選択できます。
4. [アクション]ボタンから[ノードログファイル削除]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。
5. グローバルナビゲーションメニュー上部の[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。

注意

- 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に削除対象としたノードログの情報が表示される場合があります。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[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[保管ログ]タブを選択します。
3. 対象のノードにチェックを付けます。

   複数のノードを選択できます。
4. [アクション]ボタンから[保管ログファイル削除]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。

   また、[アクション]ボタンから[保管ログファイル確認]を選択し、表示された画面からでも削除操作が行えます。
   この場合は、削除するファイルにチェックを付けます。複数のファイルにチェックを付けると、一度に削除できます。
5. グローバルナビゲーションメニュー上部の[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。

注意

- 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の情報が表示される場合があります。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。

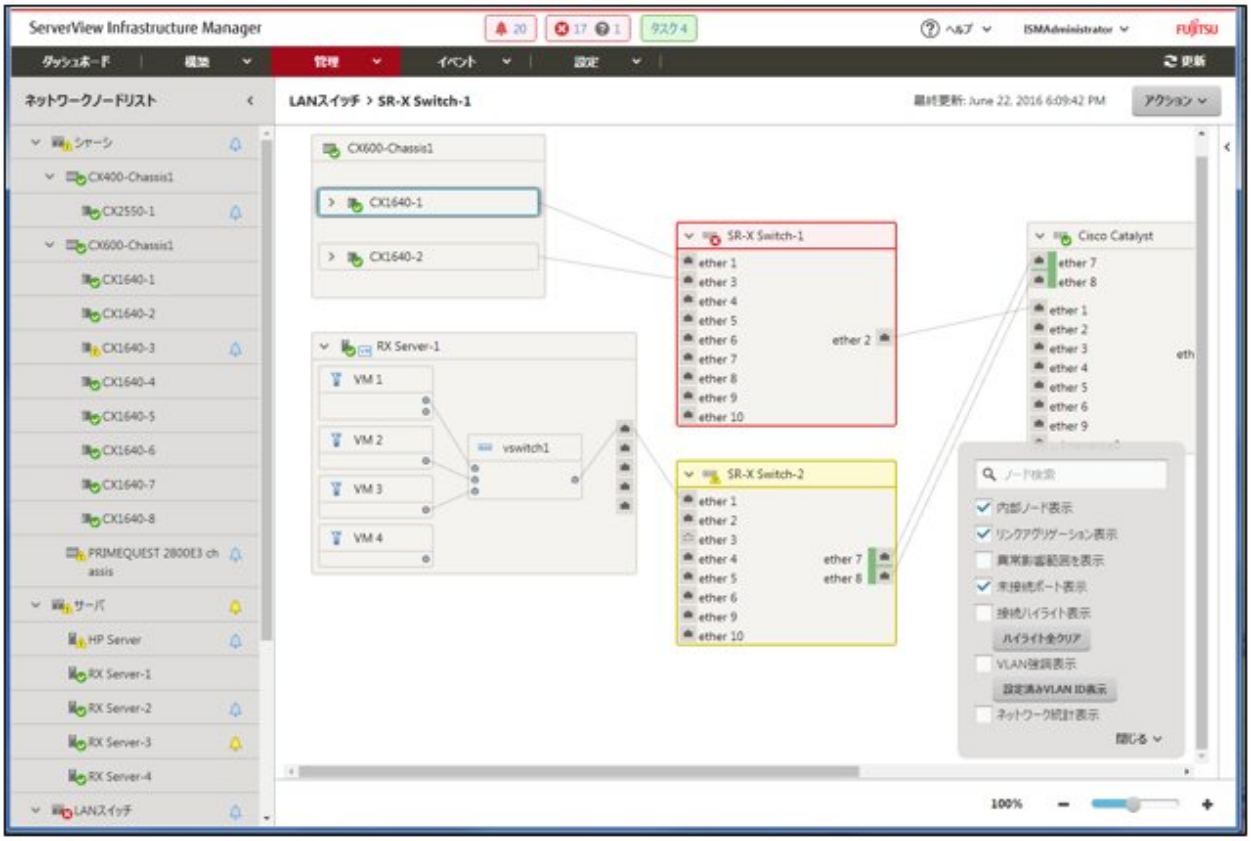
2.2.6 ネットワーク管理機能

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ネットワークマップで確認
- 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
- 管理対象ノードの物理的なポートとそのノード上の仮想マシンや仮想スイッチの仮想的なポートとの仮想的な接続関係をネットワークマップで確認
- 管理対象ノードのネットワーク統計情報をネットワークマップで確認

- ネットワークスイッチのVLAN、リンクアグリゲーション設定の確認、設定変更の実行

図2.9 ネットワークマップ



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
- ネットワーク統計情報の表示
- VLAN、リンクアグリゲーション設定の確認
- VLAN設定の変更
- リンクアグリゲーション設定の変更
- 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。
加えて、管理対象ノードの物理的なポートとそのノード上の仮想マシンや仮想スイッチの仮想的なポートとの仮想的な接続関係が確認できます。

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、[<]アイコンを選択することで左端に格納できます。

2. 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。

ネットワークマップの表示の切替え

表示設定パネルでネットワークマップに表示する情報を切り替えることができます。

表示設定名	説明
内部ノード表示	ネットワークマップ上での内部ノード(仮想ノード、ファブリック内部スイッチ)の表示・非表示を切り替えます。
リンクアグリゲーション表示	ネットワークマップ上でのリンクアグリゲーション設定の表示・非表示を切り替えます。
異常影響範囲を表示	ネットワークマップ上での異常の影響範囲の表示・非表示を切り替えます。エラーなど異常がある管理対象ノードが持つ接続、隣接する接続先ノードの外枠、および接続先ポートが黄色で表示されます。なお、接続先ノードに仮想ネットワークが構築されている場合、影響がある仮想ネットワークも黄色で表示されます。
未接続ポート表示	ネットワークマップ上でのリンクダウンポートの表示・非表示を切り替えます。
接続ハイライト表示	ネットワークマップ上でのハイライト表示機能のON/OFFを切り替えます。ハイライト表示機能がONの場合、管理対象ノードまたはそのポートを選択すると、それらが持つ接続がハイライト表示されます。また、[ハイライト全クリア]を選択すると、ハイライト表示がすべてクリアされます。
VLAN強調表示	ネットワークマップ上でのVLAN強調表示の表示・非表示を切り替えます。テキストボックスに入力したVLAN IDが設定されたノード、ポートが緑色で強調表示されます。また、[設定済みVLAN ID表示]ボタンにより、ネットワークマップに表示中のノードに設定されているVLAN IDの一覧が確認できます。
ネットワーク統計表示	ネットワークマップ上でのネットワーク統計表示の表示・非表示を切り替えます。しきい値を超えた値を検出したポートおよび接続が、オレンジ色(異常しきい値超過)または黄色(警告しきい値超過)で表示されます。 表示する監視項目を変更する場合は、本項目にチェックを付けたときに表示される選択ボックスのリストから変更できます。

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ノード名を選択すると、ノード内のポートが展開表示されます。

注意

- ネットワークの物理的な接続情報は、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。
- 表示されるネットワークマップは、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。

- 仮想スイッチ、仮想マシンの接続関係を表示するためには、管理対象ノードを管理している仮想化管理ソフトウェア、および管理対象ノードのOS情報をISMに登録しておく必要があります。仮想化管理ソフトウェアの登録については「2.3.6 仮想化管理ソフトウェア管理機能」、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」を参照してください。
- 管理対象ノードにおいて、チーミング(ボンディング)設定されているポートと仮想スイッチとの接続関係の表示には対応していません。直接ノードへアクセスして確認する必要があります。

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. [はい]ボタンを選択します。

注意

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。

ポイント

- ネットワーク管理情報の更新を実行する前に各管理対象ノードのノード情報を最新化してください。ノード情報の取得については、「2.2.1.1 データセンター/フロア/ラック/ノードの登録」の「ノード情報の管理」を参照してください。
- 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の最終更新時刻は、ネットワークマップの右上に表示されます。この最終更新時刻は、最後に情報の更新が完了した時刻を指します。
- 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

  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、ネットワークマップ上に太実線で表示されます。

・ 削除

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」された接続はネットワークマップ上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。

2. 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。

   「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。

ポイント

現在設定されている「基準時点」は、[接続情報変化の確認]の[最終更新]の日時で確認できます。

注意

[接続情報変化の確認]で[更新]ボタンを選択した場合、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

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。

2. 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。最終更新の日時が現在設定されている基準時点です。

4. [更新]ボタンを選択します。

   確認画面が表示されます。

5. 内容を確認し、[はい]ボタンを選択します。

   基準時点が更新操作を実行した時刻に更新されます。

ネットワーク統計情報の表示

ネットワークスイッチのポートの各種統計情報(トラフィックなど)をネットワークマップ上で視覚的に確認できます。

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。

2. 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. 表示設定パネルの[ネットワーク統計表示]にチェックを付けて、確認したいネットワーク統計情報監視項目を選択します。

   各ネットワーク統計情報監視項目に対してあらかじめ設定されたしきい値を超過したポートおよび接続が、オレンジ色(異常しきい値超過)または黄色(警告しきい値超過)で表示されます。

ポイント

過去の各種統計情報(トラフィックなど)を確認したい場合は、ネットワークスイッチのポートを選択した際に表示される「ポート情報」のトラフィック情報の[グラフ]で確認できます。

VLAN、リンクアグリゲーション設定の確認

ネットワークスイッチに設定されたVLAN、リンクアグリゲーションの設定状態をネットワークマップ上で視覚的に確認できます。

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。

2. 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. 確認する対象に応じて以下の操作をします。

   - VLANの場合

     表示設定パネルの[VLAN強調表示]にチェックを付けて、VLAN IDのテキストボックスに表示したいVLAN IDを入力します。

     指定したVLAN IDが設定されているポートおよび接続が、ネットワークマップ上に緑色で表示されます。

   - リンクアグリゲーションの場合

     ネットワークマップ上のノードのノード名を選択します。

     ノード内のポートが展開表示され、リンクアグリゲーションの設定が表示されます。

ポイント

- 表示設定パネルの[ID表示]を選択すると、設定済みVLAN情報を確認できます。
- 表示設定パネルの[リンクアグリゲーション表示]でネットワークマップ上のリンクアグリゲーション設定の表示・非表示を切り替えることができます。
- ネットワークスイッチによっては、リンクアグリゲーションではなく別の呼称（EtherChannelなど）で扱われる場合があります。ISMでは、総称してリンクアグリゲーションの名称で扱います。

VLAN設定の変更

ネットワークスイッチのVLAN設定を変更できます。

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。
2. ネットワークノードリストから、設定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一括設定]を選択します。
4. 同じVLAN IDを設定したいポートをそれぞれ選択してチェックを付け、右上の[設定]ボタンを選択します。
5. 設定するVLAN IDを入力、内容を編集し、[確認]ボタンを選択します。
6. 設定の変更内容を確認し、[登録]ボタンを選択します。

   VLAN設定が変更されます。

ポイント

VLAN設定は、ノード単位でも変更できます。[アクション]ボタンから[VLAN設定]を選択してください。

注意

- VLAN設定の内容によって、VLAN設定完了までに時間が必要な場合があります。VLAN設定完了後に画面を更新してください。VLAN設定状況は「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。
- VLAN設定は、ネットワークスイッチのモデルによって仕様が異なる場合があります。装置仕様を確認したあと、設定してください。
- 1つのポートに設定可能なVLAN IDの数は100個までとなります。
- ネットワークスイッチのモデルによって予約済みのVLAN IDが存在します。予約済みのVLAN IDは、設定変更できません。各ノードの仕様を確認してください。

リンクアグリゲーション設定の変更

ネットワークスイッチのリンクアグリゲーション設定を変更できます。

操作手順（追加の例）

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。
2. ネットワークノードリストから、設定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[リンクアグリゲーション設定]を選択します。
4. リンクアグリゲーションを設定する対象のノード名を選び、リンクアグリゲーション設定の[追加]ボタンを選択します。
5. LAG名、動作モードを入力し、リンクアグリゲーションの設定を行うポートにチェックを付け、[確認]ボタンを選択します。
6. リンクアグリゲーションの設定内容を確認し、[登録]ボタンを選択します。

注意

- リンクアグリゲーション設定は、ネットワークスイッチのモデルによって仕様が異なる場合があります。装置仕様を確認したあと、設定してください。
- ネットワークスイッチのモデルによって設定可能なLAG名や動作モードが異なります。設定可能なLAG名の範囲や動作モードについては、各ノードの仕様を確認してください。
- VLAN IDが異なるポート同士でリンクアグリゲーションを組むことはできません。ポート同士が同じVLAN設定となっていることを確認してリンクアグリゲーション設定を変更してください。
- 異なるノード間でマルチシャーシリンクアグリゲーションを設定する場合、各スイッチに対してリンクアグリゲーション設定を変更する必要があります。マルチシャーシリンクアグリゲーションを設定するためには、ノード間でピアリンク接続しておくなど、管理対象ノードの設定を事前に行ってください。
- マルチシャーシリンクアグリゲーションの呼称（MLAGやvPCなど）、および事前設定の内容は、ネットワークスイッチの種類によって異なります。装置仕様を確認したあと、設定してください。

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

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。
2. 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[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]ボタンを選択します。

   注意

   [追加]ボタンを選択したあとに、手動で行った設定をキャンセルしたい場合は、[クリア]ボタンを選択します。

5. 設定したいすべての接続情報を追加したあと、[保存]ボタンを選択します。
6. 編集内容が正しいことを確認し、[保存]ボタンを選択します。

2.2.7 電力制御機能

ラックに搭載した機器に対して、設定した消費電力の上限値に抑えるように電力制御を行います。

事前に、ラックに対して、ノードごとの制御情報と電力制御ポリシーの設定情報を登録し、電力制御ポリシーを有効化することで電力制御の運用を開始します。

ポイント

電力制御ポリシーは、以下の4種類があります。

- カスタム1、カスタム2

  通常運用の電力制御ポリシーです。2種類を切り替えて運用できます。

- スケジュール

  指定した曜日/時間帯だけ有効となるポリシーです。

- ミニマム

  消費電力が最小限となるように制御します。

電力制御設定の追加、編集

ノード電力設定

ノードごとの電力情報、業務の優先度を設定します。

設定した情報を元に、どの機器からどの程度の消費電力を抑えるかを調節します。

消費電力値が取得可能な機器の場合、電力制御ステータスが[電力制御停止中]または[電力制御中]の状態で、現在の消費電力値を確認できます。

電力制御ができないノードの場合、最大消費電力の値を固定値として換算します。

電力制御ポリシー

ポリシーごとの消費電力の上限値を設定します。

スケジュールポリシーについては、運用スケジュールを設定します。

電力制御の有効/無効

電力制御ポリシーの有効、無効を切り替えます。

ポイント

それぞれの電力制御ポリシーは、独立して有効化できますが、ミニマムが設定されている場合、ミニマムを最優先で実行します。ミニマム以外のポリシーが複数有効化された場合、消費電力の上限値が最も低いポリシーを実行します。

注意

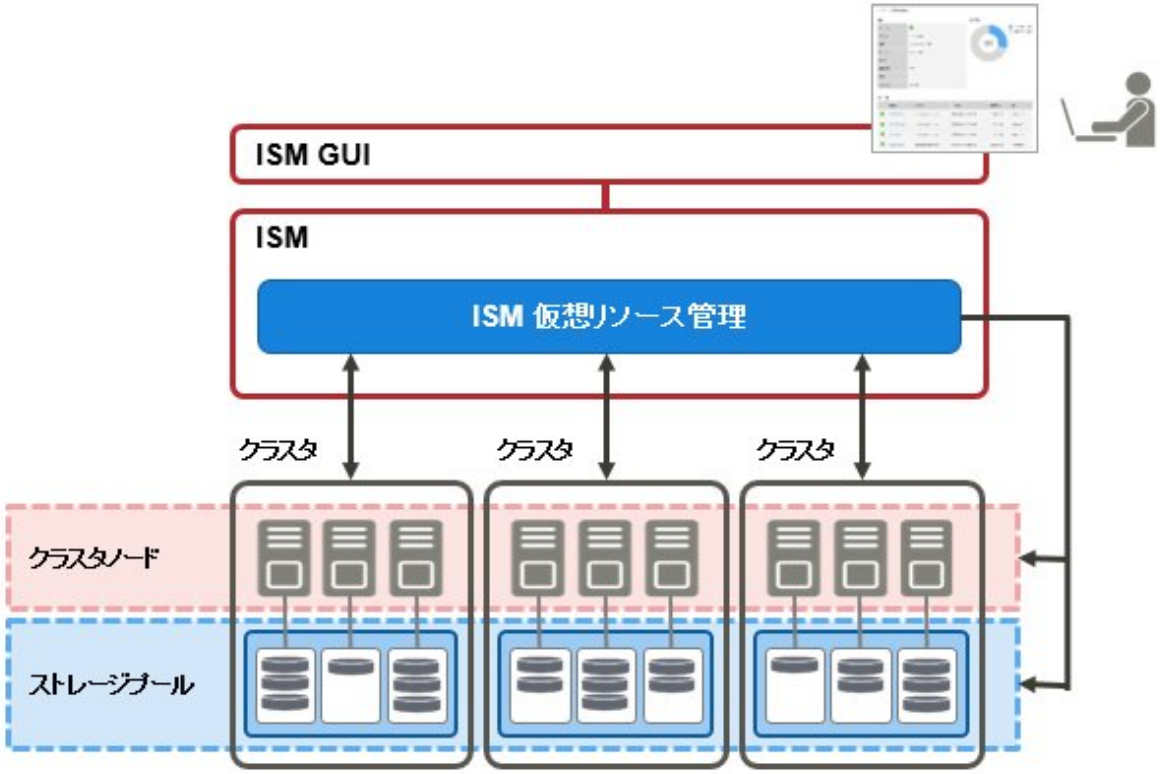
- 電力制御設定を実施済みのラックに対してノードを追加した場合、そのラックの電力制御設定を変更する必要があります。設定を変更しない場合、ラックあたりの消費電力が設定した上限値より大きくなります。
  ノードを削除した場合も、そのラックの電力制御設定の上限値を見直すことを推奨します。
  ノードを移動した場合は、移動前と移動後のラックそれぞれに対して対処を行う必要があります。
- 上限値は電力制御目標の値です。通常、上限値よりも消費電力が低くなるよう余裕をもって制御を実施しますが、上限値が低く設定されている場合は消費電力を超過することもあります。
- PRIMERGY CXのシャーシやDrive EnclosureがETERNUS DXを削除した場合や、別のラックに移動した場合は、搭載されているPRIMERGY CXのサーバノードや、接続されているDrive Enclosureの電力制御設定も同時に削除されます。
- PRIMERGY RX S7シリーズをご使用の場合は、ポリシーの上限値に対して、PRIMERGY RX S7シリーズの最小電力値を合計した値よりも大きい数値を指定してください。
  機器の最小電力値は、iRMC Webインターフェースの[電力制御]-[現在の消費電力]-[現在の全体消費電力]欄で確認できます。
- ISM-VAの日付・時間を過去の日時に変更すると、「ラック詳細」画面の[ラック情報]に表示される消費電力の値、およびノードの詳細画面の[監視]タブに表示される平均消費電力、平均吸気温度の値が正しく表示されなくなります。
  ISM-VAの日付・時間が変更した時刻を経過すると正しく表示されるようになります。

2.2.8 仮想リソース管理機能

仮想リソース管理機能は、ISM GUIで仮想リソースとして管理される要素の管理・監視を行う機能です。

本機能が動作する環境構成について、以下に示します。

図2.10 仮想リソース管理機能の動作環境の構成



注意

仮想リソース管理機能の事前設定については、当社の本製品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/「補足資料」

2.2.8.1 サポート対象の仮想リソース

本機能がサポートする仮想リソースは以下のとおりです。

VMware Virtual SAN

VMware Virtual SAN（以降、「VSAN」と表記）のVSANデータストアについて、ISM GUIに属性情報やステータスなどを表示します。

仮想リソース管理機能がサポートするVSAN環境の要件は、以下のとおりです。

項目	要件
ハイパーバイザー	・ VMware ESXi 6.0 Update 2 ・ VMware ESXi 6.5
VSANバージョン	・ 6.2 ・ 6.5
管理アプライアンス	・ vCenter Server Appliance v6.0 Update 2 ・ vCenter Server Appliance v6.5

Microsoft Storage Spaces Direct

Microsoft Storage Spaces Directの記憶域プールについて、ISM GUIに属性情報やステータスなどを表示します。

仮想リソース管理機能がサポートするMicrosoft Storage Spaces Direct環境の要件は、以下のとおりです。

項目	要件
OS	Windows Server 2016
役割と機能	以下の役割と機能がインストール済みであること ・ Hyper-V ・ Microsoft Failover Cluster

注意

事前にCredSSP認証を有効にする必要があります。仮想リソース管理機能の事前設定については、当社の本製品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/「補足資料」

ETERNUSストレージ

ETERNUSのストレージについて、ISM GUIに属性情報やステータスなどを表示します。

仮想リソース管理機能がサポートするETERNUSストレージの要件は、以下のとおりです。

項目	要件
ETERNUS機種とストレージの種類	以下のETERNUS DXシリーズのRAIDグループ ・ ETERNUS DX60 S3 ・ ETERNUS DX80 S2 ・ ETERNUS DX90 S2 ・ ETERNUS DX100 S3

項目	要件
	・ ETERNUS DX200 S3

注意

ETERNUSのシン・プロビジョニングプールの表示はサポートしていません。

RAIDグループがシン・プロビジョニングプールに組み込まれている場合でも、シン・プロビジョニングプールで使用されている容量は反映されません。

シン・プロビジョニングプールの参照および管理については、ETERNUS Web GUIを使用してください。

また、対象のETERNUS機種については、当社の本製品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/

2.2.8.2 仮想リソース管理GUI

仮想リソース管理機能は、管理GUIを備えています。

GUIの各画面の機能と、相互の表示関係について以下に示します。

なお、GUIの表示項目と説明については、ISMのオンラインヘルプを参照してください。また、ウィジェット追加方法については、『ServerView Infrastructure Manager V2.2 操作手順書』を参照してください。

図2.11 仮想リソース管理GUI

(a) 仮想リソースのウィジェット表示

ISMのダッシュボード上に、仮想リソースの状態がウィジェットで表示されます。

(b) 仮想リソースの一覧表示

仮想リソースの状態一覧が表示されます。

また、リソースの使用状況が矢印の向きおよび色で表示されます。

(c) 仮想リソースの詳細情報表示

仮想リソースの設定情報や使用容量など、詳細情報が表示されます。

仮想リソースを構成する物理ノードが表示され、関連画面を表示できます。

(d) ノード情報上の仮想リソース情報表示([SDS]タブ)

ノードの詳細画面に仮想リソースの情報を示す[SDS]タブが表示されます。

[SDS]タブを選択すると、VSANまたはMicrosoft Storage Spaces Directのノードと関連する仮想リソースの情報が表示されます。

2.2.8.3 仮想リソース管理の操作

仮想リソース管理の操作方法について説明します。

- ストレージプールの使用状況の監視
- ストレージプールの異常の特定
- 仮想リソース情報の更新

ポイント

ISMで監視を行う前に、仮想リソース環境をISMに登録する必要があります。以下の手順で実施します。

1. ストレージプール(クラスタ)を構成しているノードがISMに登録済みであることを確認します。

   ノードの登録方法および情報の確認方法については、「2.2.1 ノード管理機能」を参照してください。

2. 仮想化管理ソフトウェアがISMに登録済みであることを確認します。

   仮想化管理ソフトウェアの登録方法および情報の確認方法については、「2.3.6 仮想化管理ソフトウェア管理機能」を参照してください。

3. 仮想リソース情報の更新を行います。

   更新方法については、「仮想リソース情報の更新」を参照してください。

   仮想リソースのGUIにストレージプール情報が表示されます。

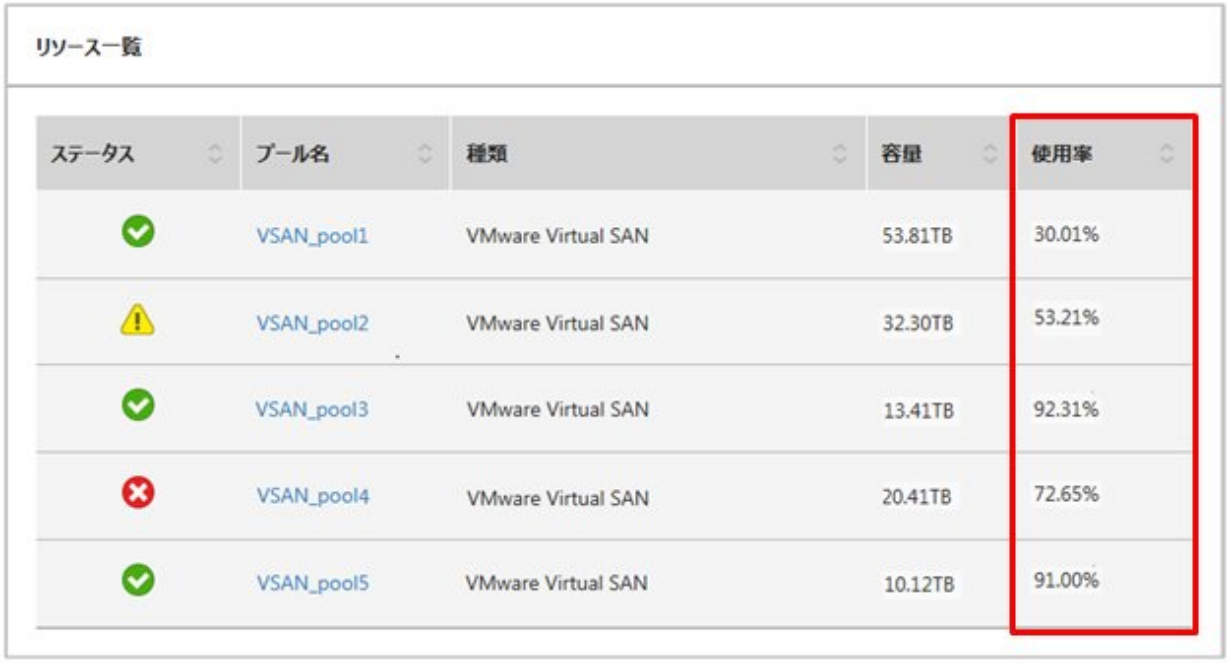
ストレージプールの使用状況の監視

ストレージプールの使用状況の監視方法について説明します。

1. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択し、仮想リソースのウィジェット「リソース一覧」を表示します。

   ウィジェット追加方法については、『ServerView Infrastructure Manager V2.2 操作手順書』を参照してください。

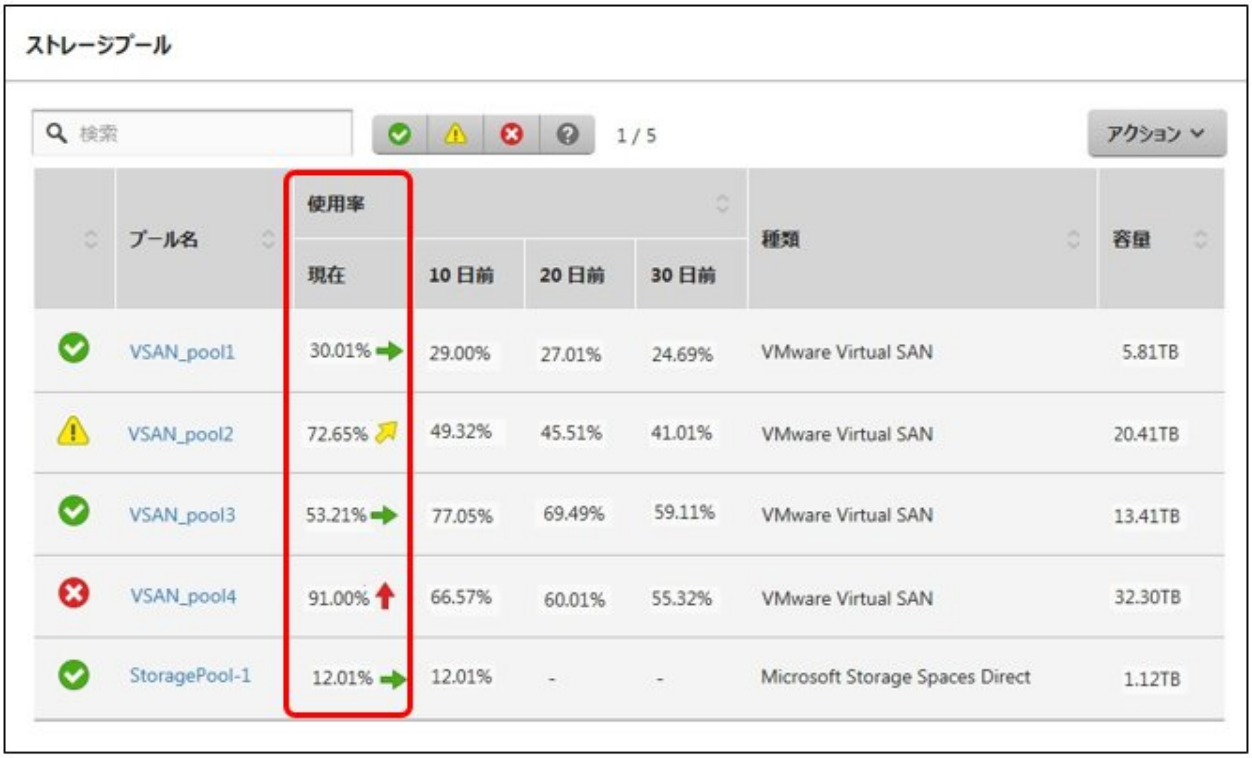
ー 「使用率」でストレージプールの現在の使用率を参照できます。



ー 仮想リソースの一覧表示画面で、より詳しい使用状況の確認ができます。

現在の使用率の状況を、矢印の向きおよび色から把握できます。

ISMのGUIでグローバルナビゲーションメニューから[管理]-[仮想リソース]を選択します。ISMにより管理できる仮想リソースの一覧が、リソースの種類別にツリー表示、およびリスト表示されます。



使用状況の見方は以下のとおりです。

- 矢印の色

  現在の全体の使用率を示します。

緑:使用率70%未満

黄:使用率70%以上～90%未満

赤:使用率90%以上

- 矢印の向き

使用率について、10日前と比較しての増加率を表現します。

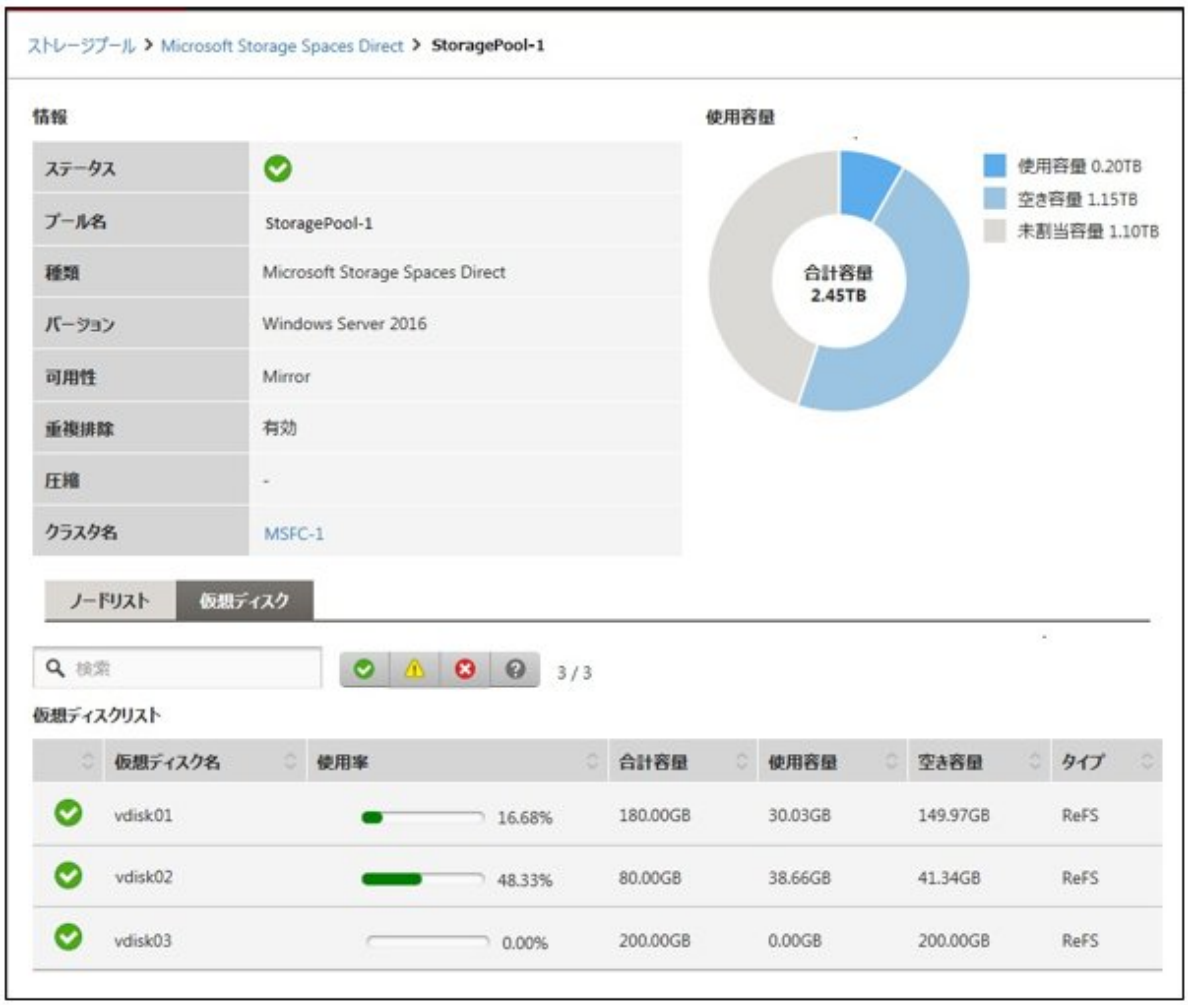
横向き:使用率が横ばい、微増(使用率が5%未満の増加)、または減少

斜め上向き:使用率が増加(使用率が5%以上～15%未満の増加)

上向き:使用率が大幅に増加(使用率が15%以上の増加)

2. 詳細な情報を確認したい場合は、対象のプール名を選択して詳細情報画面を表示し、「使用容量」で使用中の容量および空き容量を確認します。

Microsoft Storage Spaces Directの場合は、記憶域プールの容量情報に加え、記憶域プール上に作成されている仮想ディスクとその容量情報を確認できます。



Microsoft Storage Spaces Directの使用状況の円グラフに示される各容量情報の意味は、以下のとおりです。

ー 使用容量:記憶域プール上に存在する仮想ディスクの使用容量の合計を示します。

ー 空き容量:記憶域プール上に存在する仮想ディスクの空き容量の合計を示します。

ー 未割当容量:仮想ディスクが作られていない、記憶域プールの未割当ての容量を示します。

また、[仮想ディスク]タブを選択すると、記憶域プール上に存在する仮想ディスクの一覧と、使用容量などの情報が表示されます。

表示される内容の詳細については、ISMのオンラインヘルプを参照してください。

ポイント

[仮想ディスク]タブに表示される容量の情報は、仮想ディスクに設定された冗長性が反映されています。

「使用容量」の円グラフに表示される容量は、仮想ディスクの各容量に冗長性を考慮した値となります。

3. 空き容量が不足する場合は、以下の対処を実施します。

   ー ストレージを追加します。

   ノード一覧に、ストレージプールを構成しているノードが表示されています。空き容量が不足している場合は、これらのノードが保有するストレージの空きが少なくなっている可能性があります。

   ノードへディスクを増設するか、ノードを新たに追加して、空き容量の不足を解消します。

   ー ノードに異常が見られる場合は、必要な保守作業を実施します。

   ノード一覧に示されるステータスが異常を示している場合、そのノードのストレージが使用不可能であり、容量不足となっている可能性があります。

   対象のノードに関する事象をイベントログなどで確認し、適切な保守を実施します。

ストレージプールの異常の特定

ストレージプールの異常の検出、および原因を特定する手順を説明します。

ステップ1

仮想リソースの情報を更新します。

[アクション]ボタンから、[仮想リソース情報の更新]を選択します。詳細は、「仮想リソース情報の更新」を参照してください。

GUI上の仮想リソースの情報が最新に更新されます。異常が発生している場合は、ステータスの表示が変化します。

ステップ2

異常の検出・特定を行います。

リソースの異常は、仮想リソースの一覧表示画面から確認できます。また、ダッシュボードに「リソースステータス」ウィジェットを表示させている場合、そのウィジェット上に、リソースの異常が表示されます。

(1)仮想リソースの一覧表示画面から異常箇所を特定する場合

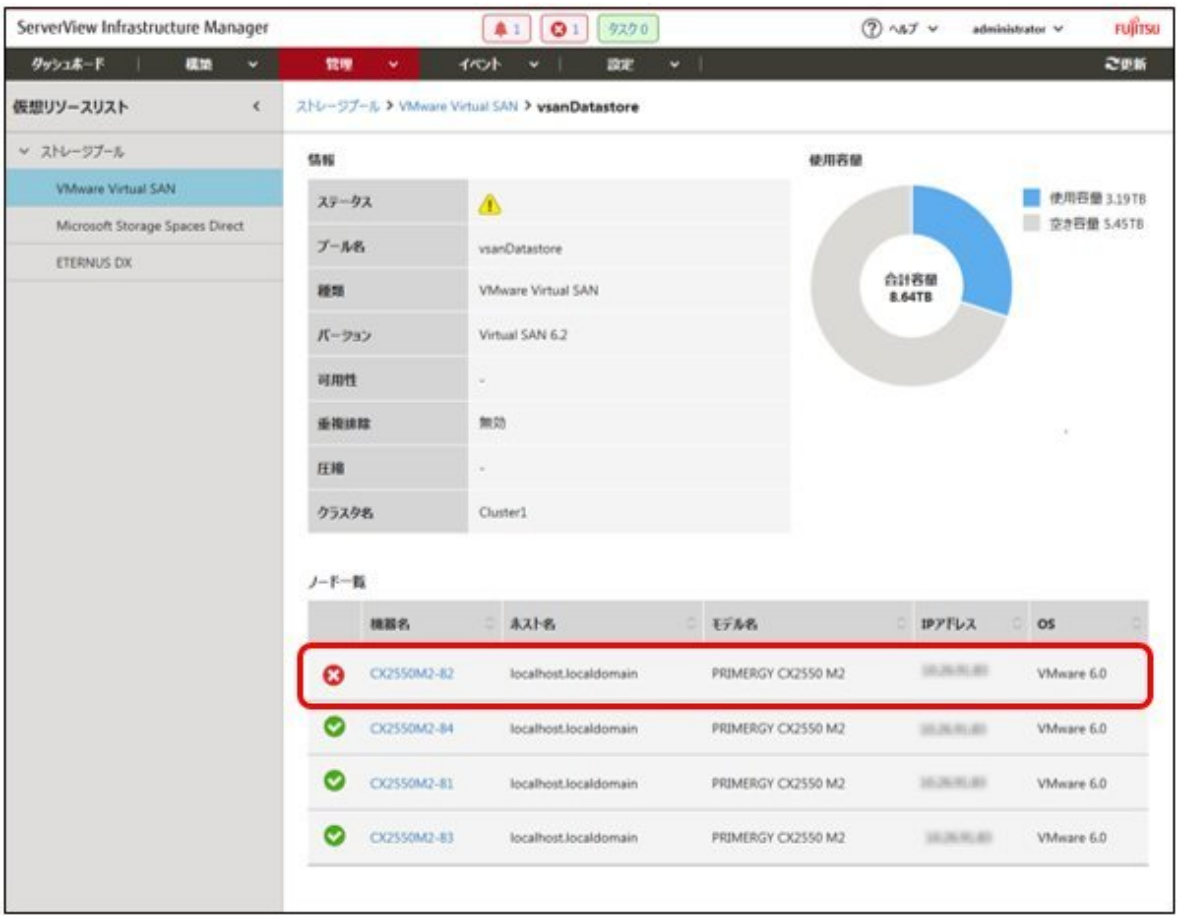
1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[仮想リソース]を選択します。

   仮想リソースの一覧表示画面が表示されます。

   画面上部のステータスの絞り込みアイコンで、指定したステータスの仮想リソースを絞り込めます。

2. プール名を選択します。

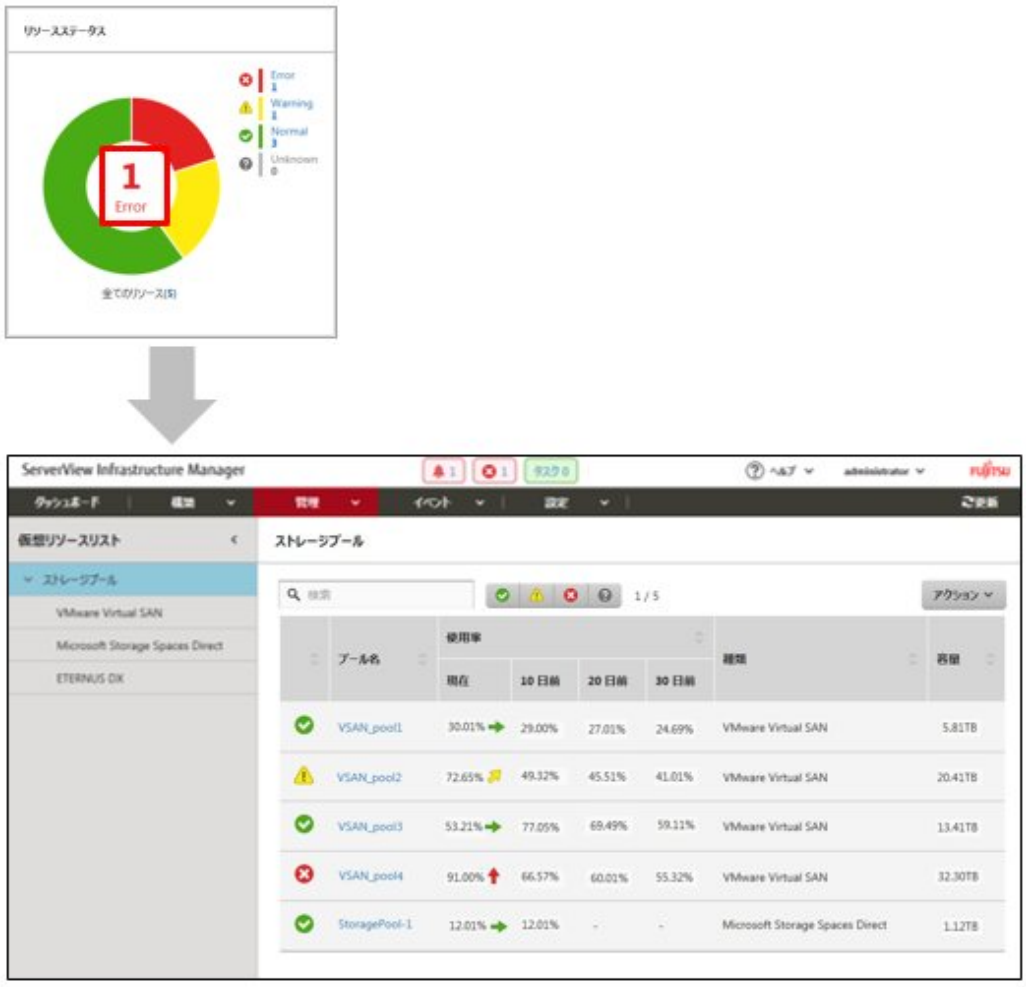
   仮想リソースの詳細情報画面が表示されるので、「ノード一覧」で、異常を示している機器名を確認します。



(2)ダッシュボードから異常箇所を特定する場合

1. ISMのダッシュボードで、「リソースステータス」ウィジェット中央に表示される数字を選択します。

   異常状態のリソース一覧が表示されます。



2. プール名を選択します。

   仮想リソースの詳細情報画面が表示されるので、「ノード一覧」で、異常を示している機器名を確認します。

ステップ3

発生している異常について、詳細を確認します。

(1)仮想リソースのステータスに異常が示されている場合

ストレージプールのステータスに異常が示されている場合、以下の状態が想定されます。

ステータス異常が発生した層	状態
物理的な層	物理的なコンポーネント(HDD、SSD、ノード)の問題により、ストレージプールに異常が発生している状態です。 SDSの種類によって、以下の状態となっています。 ・ VSANの場合、VSANの健全性に異常が発生している ・ Microsoft Storage Spaces Directの場合、記憶域プールを構成する物理ディスクまたはノードに異常が発生している

ステータス異常が発生した層	状態
	・ ETERNUSの場合、RAIDグループ、物理ディスク、またはETERNUS装置に異常が発生している
仮想的な層	仮想リソース(データストア)のレイヤーで異常が発生している状態です。

ステータス別のストレージプールの状態は、それぞれ以下のとおりです。

ステータス	ISM GUIでのアイコン表示	状態
異常		ストレージプールに問題が発生し、使用継続が不可能な状態です。
注意		ストレージプールに問題は発生していますが、使用継続は可能な状態です。
不明		ストレージプールに問題が発生し、状態が確認できない状態です。
正常		ストレージプールは正常な状態です。

ポイント

物理的または仮想的な層の異常によりストレージプールの容量が減少したときは、ストレージプールとして使用継続が不可能な「異常」のステータスと判断される場合があります。

異常の詳細および発生箇所については、以下のように確認します。

ポイント

詳細な異常箇所の特定や対処、または異常の復旧については、各ストレージプールのマニュアルなどに従って実施してください。

VSANの場合

ISM GUIおよびVMware vCenter Server Web Clientから、ストレージビューのVSANデータストアの状態、およびVSANの「健全性」を確認します。

1. ISM GUIの仮想リソースの一覧または詳細画面から、「プール名」と「クラスタ名」を確認します。
2. VMware vCenter Server Web Clientにサインインし、手順1で確認したプール名の状態の表示を[ストレージビュー]タブで確認します。

   正常ならば無印、異常ならば赤くマークされます。
3. 「ホストおよびクラスタ」で、手順1で確認したクラスタ名を選択します。
4. [監視]タブから[Virtual SAN]-[健全性]を選択します。

   VSANの健全性の「テスト結果」を参照し、異常の内容を特定してください。

異常を復旧したあとは、以下を実施してください。

1. VMware vCenter Server Web Clientにサインインし、「ホストおよびクラスタ」でクラスタ名を選択します。
2. [監視]タブから[Virtual SAN]-[健全性]を選択し、表示されるVirtual SANの健全性画面で[再テスト]を選択して、「失敗」となっていたテスト結果が「パス」に変わったことを確認します。
3. [ストレージビュー]タブを選択して表示されるデータストア一覧から、VSANデータストアの状態が正常であることを確認します。
4. ISM GUIの仮想リソース一覧画面で、[アクション]ボタンから[仮想リソース情報の更新]を選択し、ステータスが正常に戻ったことを確認します。

Microsoft Storage Spaces Directの場合

ISM GUIおよび管理サーバ上のサーバマネージャーから、記憶域プールの状態、および物理ディスクの状態を確認します。

1. ISM GUIの仮想リソースの一覧または詳細画面から、「プール名」を確認します。
2. 管理サーバ上でサーバマネージャーを開き、[ファイルサービスと記憶サービス]-[記憶域プール]を選択し、手順1で確認したプール名の状態を確認します。また、異常を示している物理ディスクを「物理ディスク」から確認します。

異常を復旧したあとは、以下を実施してください。

1. 管理サーバ上でサーバマネージャーを開き、[ファイルサービスと記憶サービス]-[記憶域プール]を選択し、記憶域プールおよび物理ディスクが正常であることを確認します。

   表示内容が古い場合があるため、画面上部の[更新]ボタンを選択し、最新の状態にしたうえで確認してください。
2. ISM GUIの仮想リソース一覧画面で、[アクション]ボタンから[仮想リソース情報の更新]を選択し、ステータスが正常に戻ったことを確認します。

ETERNUSストレージの場合

WebブラウザからETERNUS Web GUIを開き、RAIDグループおよび物理ディスクの状態を確認します。

ETERNUS Web GUIのURLは、仮想リソースの詳細画面の「ノード一覧」から、ETERNUSの機種名を選択して表示されるノード情報から確認できます。

異常を復旧したあとは、ISM GUIの仮想リソース一覧画面で、[アクション]ボタンから[仮想リソース情報の更新]を選択し、ステータスが正常に戻ったことを確認します。

(2)「ノード一覧」でノードの異常が示されている場合

ISMのイベントログで、異常の詳細を確認します。

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択します。

   「イベントリスト」画面が表示されます。
2. 検索ボックスに「ノード名」を入力して対象ノードのイベントを検索し、異常の内容を確認します。

仮想リソース情報の更新

仮想リソース一覧画面の[アクション]ボタンから[仮想リソース情報の更新]を実行します。

ポイント

- GUIに表示されている情報が古いままの場合がありますので、仮想リソースの状態を確認する際は必ず情報の更新を実行してください。

  なお、更新処理はISMのタスクに登録されます。

  表示情報が古いままの場合、ISM GUIの「タスク」画面からタスクタイプが「Refresh Virtual Resource」のタスクが「完了」になっているか確認してください。

- 仮想リソース情報は、以下のように定期的に自動更新されます(タスク表示はされません)。
  - すべての仮想リソース情報は、毎日午前0時に自動更新されます。
  - 仮想リソースのステータスは、3分おきに自動更新されます。

2.2.9 仮想IO管理機能

仮想IO管理機能は、LAN、FC(Fibre Channel)のI/Oパラメーター(MACとWWN)を仮想化する機能です。

- LANコントローラーのMACアドレスの代わりに仮想MACアドレスを使用できます。
- FCコントローラーのWWNアドレスの代わりに仮想WWNアドレスを使用できます。
- 仮想MACアドレス、仮想WWNアドレス、ネットワーク経路の割当て、およびネットワークブートのI/Oパラメーターをプロファイルとして保持できます。

ポイント

仮想MACアドレスや仮想WWNアドレスは、ISMで管理するノード全体またはノードグループ単位に一意である必要があります。このため、仮想MACアドレスや仮想WWNアドレスなどの仮想IOを設定したプロファイルは、複数のノードに適用できません。

注意

ServerView Virtual-IO Manager(VIOM)などの仮想IOを管理するソフトウェアが動作している場合、ISMとの競合に注意してください。

VIOMが動作している場合は、競合を避けるため、ISMとVIOMでは同じノードを管理しないようにしてください。

MACアドレス、WWNの仮想化

サーバの仮想IO(仮想MACアドレスや仮想WWNアドレスなど)の設定をプロファイルとして管理し、プロファイルを適用することによって仮想IO管理機能を使用可能にします。管理対象サーバやPCIカードを交換する際に周辺機器の設定変更作業の手間を軽減し、ネットワーク情報の再設定作業も容易に行えます。

仮想IO管理機能を使用した管理対象サーバ、およびPCIカードの交換は、以下の手順で行うことを想定します。

図2.12 仮想IO管理機能を使用した管理対象サーバの交換

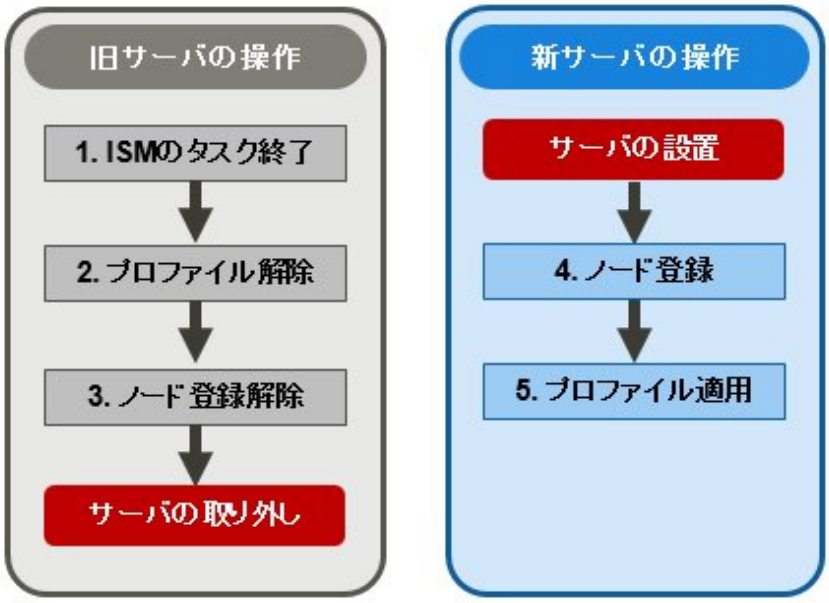
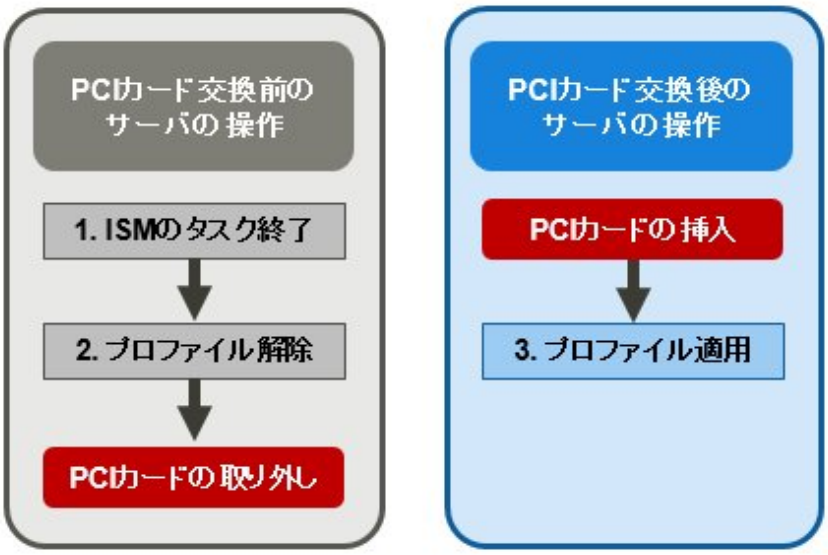


図2.13 仮想IO管理機能を使用したPCIカードの交換



2.2.10 ハードウェア設定バックアップ機能

ハードウェア設定バックアップ機能は、PRIMERGY・PRIMEQUEST3000BのBIOS/iRMC設定を吸い上げてファイルとして保存し、保存したファイルをエクスポートする機能です。

図2.14「ハードウェア設定バックアップ」画面例（GUI）

ポイント

- ハードウェア設定のファイルは、BIOSとiRMCで別々に保存されます。
- BIOSのハードウェア設定をバックアップする場合は、バックアップ前にサーバの電源をオフにする必要があります。

ハードウェア設定のバックアップ手順

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ハードウェア設定バックアップ]を選択します。
3. ノードを選択して、[アクション]ボタンから[ハードウェア設定バックアップ]を選択します。

   ウィザード画面が表示されます。
4. BIOSのハードウェア設定をバックアップする場合は、バックアップ前にサーバの電源をオフにし、[サーバ電源状態取得]ボタンを選択して、パワーステータスが「Off」になったことを確認します。
5. 設定をバックアップするBIOS、またはiRMCにチェックを付けて、[実行]を選択します。

ポイント

複数のノードとハードウェア設定を選択してバックアップすることが可能です。

ハードウェア設定の最新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[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ハードウェア設定バックアップ]を選択します。
3. ノードを選択して、[アクション]ボタンから[エクスポート(最新ファイル)]を選択します。
4. 任意の対象にチェックを付けて、[実行]を選択します。

ポイント

複数のノードとハードウェア設定を選択してエクスポートすることが可能です。

ハードウェア設定の過去分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[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ハードウェア設定バックアップ]を選択します。
3. ノードリスト画面上で過去分ファイルを取得する対象ノードの[バックアップ数]を選択します。
4. 取得対象のハードウェア設定を選択して、[アクション]ボタンから[エクスポート]を選択します。

ポイント

複数の過去分ハードウェア設定を選択してエクスポートすることが可能です。

ハードウェア設定の削除手順

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ハードウェア設定バックアップ]を選択します。
3. 削除対象ノードの[バックアップ数]欄を選択します。
4. 削除対象のハードウェア設定を選択して、[アクション]ボタンから[削除]を選択します。

ポイント

複数のハードウェア設定を選択して削除することが可能です。

2.2.11 プール管理機能

プール管理機能は、アドレスリソースをプール化して管理する機能です。主に以下の機能があります。

- ユーザーが使用可能なアドレス範囲をプールとして設定
- 要求に応じて、プールから値を払い出し
- 不要になった値をプールに返却

プールの対象リソース

プールの対象とするリソースは、以下の仮想アドレスです。

- 仮想MACアドレス
- 仮想WWNアドレス

プール管理機能は、仮想IO管理機能において、上記の仮想アドレスを設定する際に使用します。

プロファイル作成時に上記の仮想アドレスを設定する場合、使用する仮想アドレスの値を入力しなくても自動的にプール範囲から値の払い出しができます。また、設定されているプール範囲から払い出す値を選択することもできます。

上記の仮想アドレスが設定されているプロファイルを削除すると、不要になった値として仮想アドレスの値がプールに返却されます。

ここでは、以下の操作ついて説明します。

- プール設定の登録
- プール設定の確認
- プール設定の編集
- プール設定の削除

プール設定の登録

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定]を選択します。
2. [アクション]ボタンから[登録]を選択します。

3. 「プール登録」画面で必要な情報を設定し、[登録]を選択します。

   ー プールタイプ

     設定するプールの種類を選択します。

   ー 開始アドレスおよび終了アドレス

     設定するプール範囲の開始アドレスと終了アドレスを設定します。

   ー 使用可能ユーザーグループ

     設定するプール範囲から値を払い出すことができるユーザーグループを選択します。

     [全てのユーザーグループ]を選択した場合、どのユーザーもここで設定したプール範囲から値を払い出すことができます。

プール設定の確認

ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定]を選択して、「プールリスト」画面を表示します。

「プールリスト」画面には、ユーザーが使用可能なプール設定が表示されます。また、残っている使用可能なアドレス数および払い出し済みのアドレスを確認できます。

残っている使用可能なアドレス数が0の場合、そのプール範囲からの払い出しはできません。「プール設定の登録」または「プール設定の編集」を実行してプール範囲を追加してください。

プール設定の編集

プール設定の編集では、開始アドレスおよび終了アドレスのみ編集できます。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定] を選択します。
2. 編集するプール設定を選択し、[アクション]ボタンから[編集]を選択します。
3. 「プール編集」画面で必要な情報を設定し、[登録]を選択します。

注意

払い出し済みアドレスがある場合、払い出し済みアドレスがプール範囲外となる設定はできません。払い出し済みアドレスを確認して編集してください。

プール設定の削除

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定]を選択します。
2. 削除するプール設定を選択し、[アクション]ボタンから[削除]を選択します。
3. 削除対象を確認し、[削除]を選択します。

2.3 ISM運用基盤の機能説明

ISMの運用基盤となる各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
- 2.3.6 仮想化管理ソフトウェア管理機能
- 2.3.7 共有ディレクトリ管理機能
- 2.3.8 ISM連携管理機能

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2.15 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
- セキュリティポリシーの設定
- 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	管理対象ノード	アクセス範囲
Administratorグループ	全てのノードを管理	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	全てのノードを管理	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。

ユーザーグループ名	管理対象ノード	アクセス範囲
		ISMの全体管理用のユーザーグループです。
	指定ノードグループ内	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。
	管理ノードなし	すべてのノード、およびノードに関連する資源(ログなど)がありません。

ポイント

以降の説明では、管理対象ノードが「全てのノードを管理」と指定されているユーザーグループは、Administratorグループとみなしてください。

注意

管理対象ノードを「全てのノードを管理」から変更することも、「全てのノードを管理」へ変更することもできません。

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。

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。
- 以降の説明では、Administratorグループに属し、Administratorロールを持つユーザーのことを「ISM管理者」と表記します。

ユーザーがアクセス可能な権限の説明を行うため、以降ではユーザーが属するユーザーグループと、そのグループ内でユーザーが持つユーザーロールに分類して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	実行可能	実行不可
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

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）

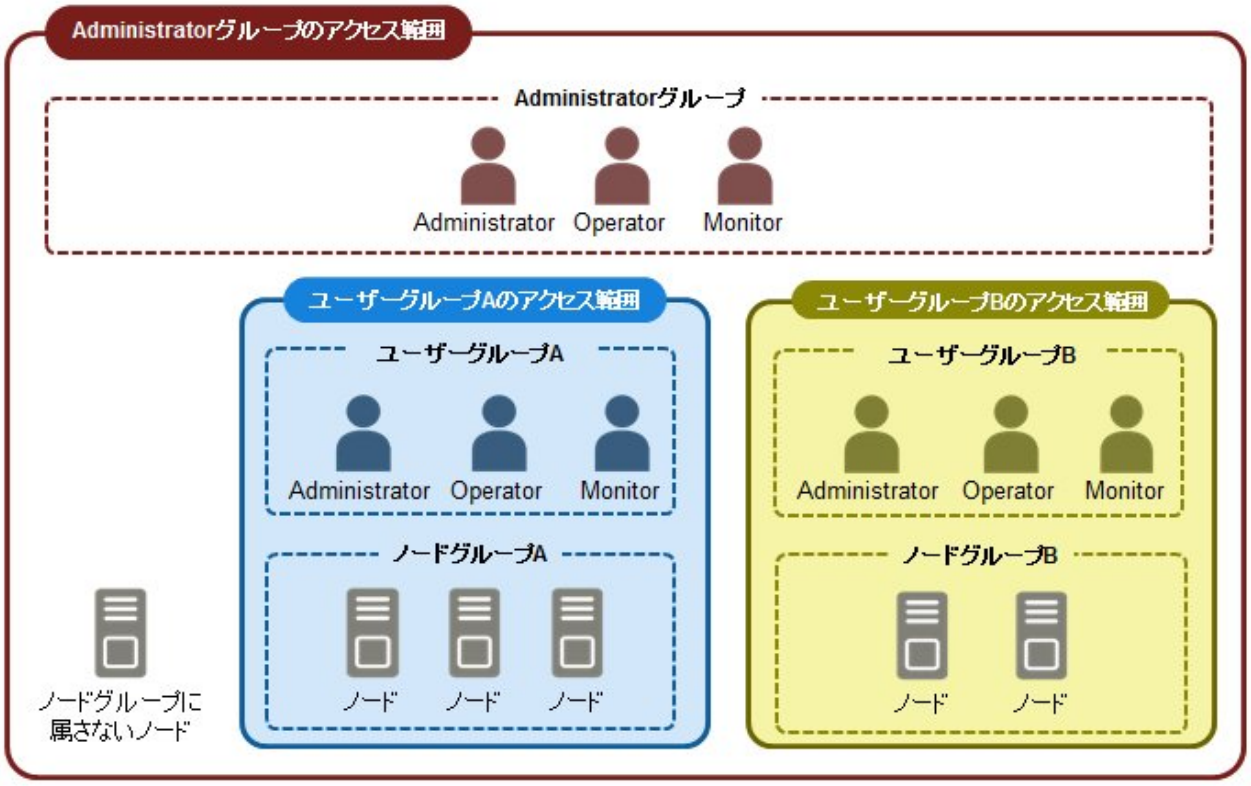
- 上記の表示の場合、以下のユーザー属性を持つユーザーが操作を実行できます。
  - Administratorグループに属し、AdministratorまたはOperatorロールを持つユーザー
  - Administratorグループ以外のグループに属し、AdministratorまたはOperatorロールを持つユーザー
- グレーアイコンで示される、Monitorロールを持つユーザーは、機能を実行できません。

注意

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（ISM管理者）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。

図2.15 ユーザーグループ、ノードグループ、ロールの関係



セキュリティポリシーの設定

ユーザー管理で扱うパスワードと、ログインの制限を設定できます。

セキュリティポリシーはISM全体で1つ設定できます。セキュリティポリシーを強固に設定することで、よりセキュアな運用が可能となります。設定項目は以下のとおりです。

ユーザーパスワードポリシー

項目	設定値	設定後の動作
以前のパスワードの使用	・使用可能(推奨値) ・過去n回のパスワードの使用禁止(1≦n≦24)	ユーザーの追加、およびユーザーの編集画面で、パスワードを設定時にチェックされます。
パスワードの長さ	1～32(バイト) (推奨値:8(バイト))	
使用文字種類	・限定しない(推奨値) ・数字、小文字、大文字、特殊文字のうち最低n種類使用する(2≦n≦4)	
ユーザー名と同じパスワード	・許容する ・禁止する(推奨値)	
使用禁止文字列[注1]	最大256個まで指定可能	
有効期限	・無期限 ・1～365(日) (推奨値:90(日))	「無期限」以外を設定してログインした場合、以下のように動作します。 ・有効期限に達した場合 期限超過後のアクションが実行されます。 ・有効期限が2週間に達した場合 警告メッセージが出力されます。 ・Administratorの場合 初期設定パスワードを変更していない場合、警告メッセージが出力されます。
期限超過後のアクション	・警告メッセージのみ出す ・ログインを無期限にロックする(推奨値)	

[注1]:使用できないパスワードを設定します。設定した文字列と完全一致するパスワードが使用禁止となります。

備考)[デフォルト]ボタンを選択すると、上記の表の推奨値に値が設定されます。

注意

- すでに作成されているユーザーについて、ISM V2.0.0.dパッチ以前のバージョンからISM V2.2へアップデートした場合の注意事項を以下に示します。
  - パスワードの有効期限は、パッチを適用したときから計算されます。
  - ユーザーパスワードポリシーは、以下のように設定されます。
    - パスワードの長さ:1(バイト)
    - 使用文字種類:限定しない
    - ユーザー名と同じパスワード:許容する
    - 有効期限:無期限
    - 期限超過後のアクション:警告メッセージのみ出す
- パスワード有効期限に「無期限」以外を設定し、期限超過後のアクションに「ログインを無期限にロックする」を設定した場合の注意事項を以下に示します。
  - ログインの制限は、ISMへのログインに限られます。FTPやISM-VAへのログインについては制限されないため、注意してください。

- パスワードの有効期限超過後、ISMへの初めてのログインは成功します。このときにパスワードを変更してください。パスワードを変更しなかった場合、ログインが無期限にロックされます。
- ログインが無期限にロックされた場合、ISM管理者にパスワードを再設定してもらうと、ロックが解除できます。
- ISM管理者は、ログインが無期限にロックされることはありません。警告メッセージのみ出力されます。

ログインポリシー

項目	設定値	説明
セッション有効時間	2～60(分) (初期値:30(分))	何の操作も行わなかった場合、セッションがタイムアウトとなるまでの時間です。
ロックしきい値	6～256(回) (初期値:6(回))	ログインを連続して失敗し、一定時間ログインが禁止される際のしきい値となる回数です。
ロック時間	1～1440(分) (初期値:30(分))	ログインを連続して失敗後、一定時間ログインが禁止される際の時間です。

注意

ー ログインを連続して失敗した回数は、以下の場合にリセットされます。
- ログインが成功した場合
- 最後にログインが失敗したときからロック時間経過した場合

ー ロック時間は、最初にロックしきい値となったときからの時間です。

ISM初期設定後の必要なユーザーの作成

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。
4. 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[設定]-[ユーザー]-左側ツリー部で[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。
- ISM連携

  以下のどちらかを選択できます。

  ー 連携用のユーザーとして設定しない

  ー 連携用のユーザーとして設定する

- 認証方式

  以下のどちらかを選択できます。

  ー ユーザーグループの設定に従う

  ー ServerView Infrastructure Manager(ISM)

- 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。

- 言語

  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[設定]-[ユーザー]-左側ツリー部で[ユーザー]を選択します。
2. 以下のどちらかを行います。

   ー 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。

   ー 編集したいユーザー名を選択し、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	○	○	○	○
パスワード	○	○	○	○
ユーザーロール	○	×	○	×
ISM連携	○	×	×	×
認証方式	○	×	○	×
説明	○	×	○	×
言語	○	○	○	○
日付フォーマット	○	○	○	○
タイムゾーン	○	○	○	○
ユーザーグループ	○	×	×	×

○:変更可能、×:変更不可能

注意

- 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。

・ ISM連携で[連携用のユーザーとして設定する]を選択した場合、パスワードも同時に編集してください。

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[設定]-[ユーザー]-左側ツリー部で[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選択し、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

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[設定]-[ユーザー]-左側ツリー部で[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。

  - ServerView Infrastructure Manager(ISM)
  - Open LDAP / Microsoft Active Directory(LDAP)

- 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。

- ディレクトリサイズ

  ユーザーグループで使用するファイルの総容量の上限と警告の通知しきい値を指定できます。

用途	サイズ制限	しきい値監視
ユーザーグループ全体	ユーザーグループで使用するファイルの総容量を[最大サイズ]にMB単位で指定します。 ファイルの総容量とは、以下のデータの合計を意味します。	警告メッセージを出力するしきい値を[警告しきい値]に%単位で指定します。 警告メッセージは運用ログに出力されます。

用途	サイズ制限	しきい値監視
	• リポジトリ • 保管ログ • ノードログ • FTPでISM-VAに取り込むファイル 実際の使用量が[最大サイズ]で指定した値を超えた場合、運用ログにエラーメッセージが出力されます。ただし、[最大サイズ]の値を超えても、リポジトリ、保管ログ、ノードログの動作には影響しません。	
リポジトリ	リポジトリにインポートするファイルの総容量を[最大サイズ]にMB単位で指定します。 インポートしたファイルの総使用量が[最大サイズ]で指定した値を超えた場合、実行中のリポジトリへのインポートはエラーになり、運用ログにエラーメッセージが出力されます。	指定できません。
保管ログ	保管ログの総容量を[最大サイズ]にMB単位で指定します。 保管ログの総容量が[最大サイズ]で指定した値を超えた場合、新たに発生したログは保管されなくなり、運用ログにエラーメッセージが出力されます。 なお、[最大サイズ]をデフォルトの「0」のままにしておくと、発生したログは保管されず、そのたびに運用ログにエラーメッセージが出力されます。 [最大サイズ]の値を超える前に保管されたログは、そのまま保管されます。	警告メッセージを出力するしきい値を[警告しきい値]に%単位で指定します。 警告メッセージは運用ログに出力されます。
ノードログ	ダウンロード用データとログ検索用データの総データ容量を[最大サイズ]にMB単位で指定します。 ログ検索用データは、Administratorユーザーグループにのみ指定できます。 ダウンロード用データ、またはログ検索用データの総データ容量のどちらかが[最大サイズ]で指定した値を超えた場合、ダウンロード用データとログ検索用データの両方が出力されなくなり、運用ログにエラーメッセージが出力されます。 なお、ダウンロード用データ、ログ検索用データのどちらか、または両方の[最大サイズ]をデフォルトの「0」のままにしておくと、どちらのデータも出力されず、運用ログにエラーメッセージが出力されます。	ダウンロード用データの容量とログ検索用データの容量に対して、警告メッセージを出力するしきい値を[警告しきい値]に%単位で指定します。 警告メッセージは運用ログに出力されます。

リポジトリにインポートするファイルの総容量、保管ログの容量、ノードログ(ダウンロード用データ、ログ検索用データ)の容量の見積り方法については、「3.2.1 ディスク資源の見積り」を参照してください。

- 管理対象ノード

  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。
- ユーザーグループ作成後は、すぐに「3.7.2 ユーザーグループに対する仮想ディスク割当て」手順を行ってください。

- 「全てのノードを管理」を選択した場合、Administratorグループと同様に、すべてのノードグループおよびユーザーグループにアクセスできます。ただし、リポジトリがAdministratorグループと共有されます。

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[設定]-[ユーザー]-左側ツリー部で[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選択し、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
- ディレクトリサイズ

  編集内容は、「ユーザーグループの追加」の「ディレクトリサイズ」を参照してください。
- 管理対象ノード

  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。
- 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、既存の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[設定]-[ユーザー]-左側ツリー部で[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選択し、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。

注意

- 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。

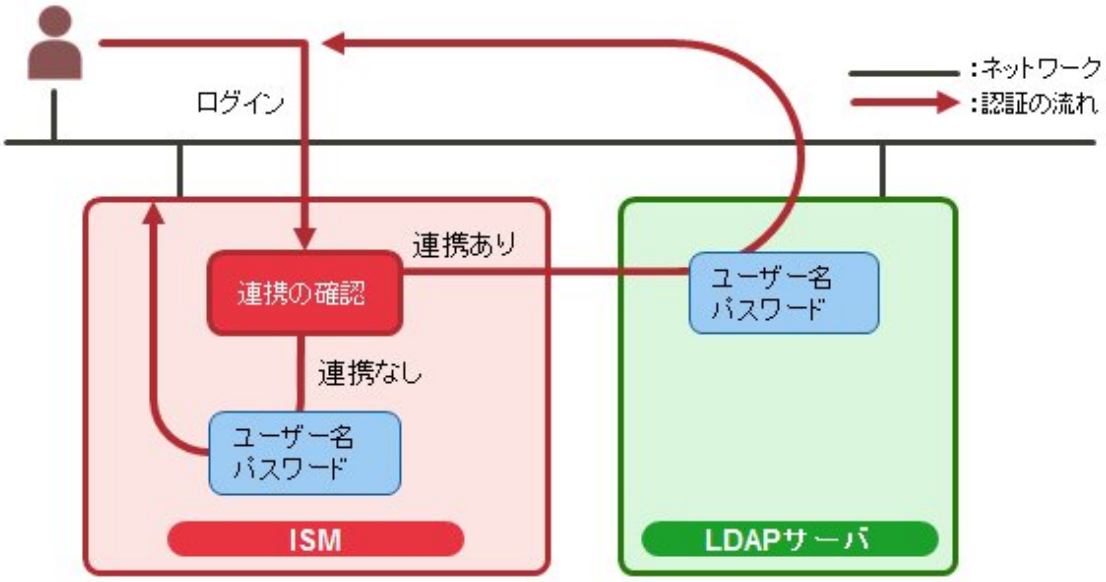
  ユーザーグループを削除する場合は、事前にユーザーを削除するか、ユーザーの所属をほかのユーザーグループへ変更してください。
- ノードグループに関連付けられた状態のままユーザーグループを削除しても、ノードグループは削除されません。
- ユーザーグループを削除すると、元には戻せません。
- ユーザーグループに関連したデータ(リポジトリ)はすべて削除されます。

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2.16 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>

項目	設定内容
	・ 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 ・ 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。
SSL証明書	ディレクトリサーバとの接続にSSLを使用したい場合、SSL証明書を設定します。

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[設定]-[ユーザー]-左側ツリー部で[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。
認証方法	「ユーザーグループの設定に従う」を指定します。
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。

注意

- administratorユーザーは、Microsoft Active DirectoryまたはLDAPと連携できません。
- ユーザーの認証方法が「ServerView Infrastructure Manager(ISM)」であるユーザーは、Microsoft Active DirectoryまたはLDAPと連携できません。

- LDAPサーバ名にFQDN名を指定する場合、事前にDNSサーバをISMに設定する必要があります。
- [設定]-[ユーザー]-[LDAPサーバ設定]で指定した内容で、ディレクトリサーバと接続できない場合、ディレクトリサーバ情報はエラーとなって設定できません。
- ディレクトリサーバは、プライマリーとセカンダリの2つ指定できます。2つ指定した場合、現在使用中のサーバと応答できなくなったときは、もう一方のサーバを使用します。
- SSL証明書の設定についての注意事項を以下に示します。
  - SSL証明書は、事前にFTPでAdministrator/ftpディレクトリにアップロード後、指定してください。
  - 設定後、アップロードしたSSL証明書は不要ですので削除してください。
  - SSL証明書に記載されたURLをLDAPサーバ名に指定してください。
- ディレクトリサーバとの接続にSSLを使用したい場合の注意事項を以下に示します。
  - LDAPサーバ名は、ldaps://から指定してください。
  - ポート番号をSSL通信用のポート番号(例:636)を指定してください。
  - SSL証明書を設定してください。
- ディレクトリサーバで、バインドDNで指定したユーザーのパスワードを変更した場合、ISMの設定には反映されません。ISMのLDAPサーバの設定で、パスワードを変更してください。

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

  以下のどちらかを行ってください。

  - 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。
  - ユーザーの認証方法を「ServerView Infrastructure Manager(ISM)」に変更します。
- 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「ServerView Infrastructure Manager(ISM)」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[設定]-[ユーザー]-左側ツリー部で[ノードグループ]を選択します。
2. [アクション]ボタンから[ノードグループ追加]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[＋]ボタンを選択します。

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[設定]-[ユーザー]-左側ツリー部で[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[ノードグループ編集]を選択します。
   - 編集したいノードグループ名を選択し、表示された情報画面で[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。

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、[ノードアクション]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]ボタンを選択します。
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]ボタンを選択します。
   - 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]ボタンを選択します。

注意

ノード間で親子の繋がりがあるノードの場合、親ノードのみ[ノードグループへ割り当て]を実行できます。
子ノードは自動的に親ノードと同じノードグループに設定されます。

繋がりがあるノードは、ノードリスト画面でノード名の横にアイコンが表示されます。親子の繋がりが設定される機種については、「表2.4 ノード間で親子の繋がりが設定される機種」のとおりです。

表2.4 ノード間で親子の繋がりが設定される機種

モデル	親ノード	子ノード	アイコン
PRIMERGY BXシャーシ	-	PRIMERGY BX サーバ BXコネクションブレード	
PRIMERGY BXサーバ	PRIMERGY BXシャーシ	-	
BXコネクションブレード	PRIMERGY BXシャーシ	-	
PRIMERGY CXシャーシ	-	PRIMERGY CXサーバ	
PRIMERGY CXサーバ	PRIMERGY CXシャーシ		
PRIMEQUEST 2000シリーズ/3000Eシリーズ	-	PRIMEQUESTパーティション	
PRIMEQUESTパーティション	PRIMEQUEST 2000シリーズ/3000Eシリーズ	PRIMEQUEST拡張パーティション	
PRIMEQUEST拡張パーティション	PRIMEQUESTパーティション	-	
ETERNUS DX	-	ドライブエンクロージャ	
ドライブエンクロージャ	ETERNUS DX	-	
ETERNUS NR（NetApp）クラスタ	-	ETERNUS NR（NetApp）シャーシ	
ETERNUS NR（NetApp）シャーシ	ETERNUS NR（NetApp）クラスタ	外付けディスクシェルフ	
外付けディスクシェルフ	ETERNUS NR（NetApp）シャーシ	-	
VCSファブリック	-	VDXスイッチ	
VDXスイッチ	VCSファブリック	-	
C-Fabric	-	CFX2000シリーズ/ PY CB Eth Switch 10/40Gb 18/8+2 (ファブリックモード)	
CFX2000シリーズ	C-Fabric	-	
PY CB Eth Switch 10/40Gb 18/8+2 (ファブリックモード)	C-Fabric	-	

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[設定]-[ユーザー]-左側ツリー部で[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[ノードグループ削除]を選択します。
   - 削除したいノードグループ名を選択し、表示された情報画面で[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。

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。

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ファームウェアデータ、およびServerView Suite Update DVDを保管

  「ファームウェア管理機能」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インストールおよびOfflineアップデートに使用するServerView Suite DVDを保管

  「プロファイル管理機能」、「ファームウェア管理機能」で利用されます。

注意

リポジトリのディスク領域が不足している場合、リポジトリ管理機能の各種データの保存に失敗します。以下を参照してリポジトリに対して十分なディスク領域を割り当ててください。

- 3.2.1.2 リポジトリの必要容量の見積り
- 3.7 仮想ディスクの割当て
- 2.3.1.2 ユーザーグループの管理

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 PRIMERGY本体 iRMC	ServerView Suite Update DVD（11.15.09版以降） または 富士通のPRIMERGY Webサイトに公開されたファームウェアデータ
	PRIMERGY搭載カード類	
	PRIMEQUEST本体ファームウェア	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
PRIMERGY BXシャーシMMB	MMB	
スイッチブレード	基本ソフトウェア	
ネットワークスイッチ（Cisco Systems Nexusシリーズ、Cisco Systems Catalystシリーズ以外）	基本ソフトウェア	
ネットワークスイッチ（Cisco Systems Nexusシリーズ）	NX-OS	富士通の担当営業・SE、もしくはサポートから入手したファームウェアデータ
ネットワークスイッチ（Cisco Systems Catalystシリーズ）	IOS	

ファームウェアデータ入手先

下記のWebサイトから対象モデルのファームウェアデータ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://azby.fmworld.net/app/customer/driversearch/ia/drviaindex http://support.ts.fujitsu.com/globalflash/ManagementController/
PRIMERGY本体 BIOS	BIOS	http://azby.fmworld.net/app/customer/driversearch/ia/drviaindex http://support.ts.fujitsu.com/globalflash/SystemBoard/
PRIMERGY搭載カード類	FC	http://support.ts.fujitsu.com/globalflash/FibreChannelController/
	CNA	http://support.ts.fujitsu.com/globalflash/LanController/
PRIMEQUEST本体	本体ファームウェア	http://www.fujitsu.com/jp/products/computing/servers/primequest/download/
PRIMERGY BX シャーシMMB	MMB	http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ http://support.ts.fujitsu.com/globalflash/BladeSystem/
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/

対象ファームウェア	ファームウェアタイプ（種類）	入手先
	LAN Switch（VDXモデル）	http://eservice.fujitsu.com/supportdesk/ [注1]
	LAN Switch（CFXモデル）	http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/
	LAN Switch（PY CB Eth Switchモデル）	http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ http://support.ts.fujitsu.com/globalflash/BladeSystem/
	LAN Switch（Cisco Systems Nexusシリーズ、Cisco Systems Catalystシリーズ）	富士通の担当営業・SE、もしくはサポートに連絡して入手してください。
	FC Switch	http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/
ストレージコントローラー	ETERNUS DX/AF	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。

ISMは11.15.09版以降のServerView Suite Update DVDに対応しています。

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

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[構築]-[ファームウェア]を選択します。
3. 画面左側のメニューから[インポート]を選択します。
4. 以下のどちらかを行います。

   ー 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

   [インポートデータリスト]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。

   ー 富士通のWebサイトからダウンロードしたファームウェアデータをリポジトリに保存する場合

   [インポートデータリスト]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。

5. 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上部の[タスク]を選択すると、タスクの一覧が表示されます。

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。

- [DVDインポート]実施時に「インポート成功後、インポート元のファイルを削除する。」の項目にチェックを付けると、インポートが完了したあとFTPサーバ上にあるインポート元のファイルが削除されます。
- [DVDインポート]実施時に共有ディレクトリに配置しているファイルをインポートすることができます。共有ディレクトリを利用したDVDインポートを行う場合は、「2.3.7 共有ディレクトリ管理機能」を参照して共有ディレクトリの設定を行い、共有ディレクトリのマウントを実施してください。
- [DVDインポート]実施時に「共有ディレクトリのマウントを解除する」の項目にチェックを付けると、インポートが完了したあと共有ディレクトリとのマウントを解除します。

リポジトリからのファームウェアデータの削除

GUIを使用した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[構築]-[ファームウェア]を選択します。
2. 画面左側のメニューから[インポート]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していた場合
     a. [インポートデータリスト]タブを選択します。
     b. 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。
     c. 画面表示に従い、操作を実行します。
   - 富士通のWebサイトからダウンロードしたファームウェアデータをリポジトリに保存していた場合
     a. [ファームウェアデータ]タブを選択します。
     b. 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。
     c. 画面表示に従い、操作を実行します。

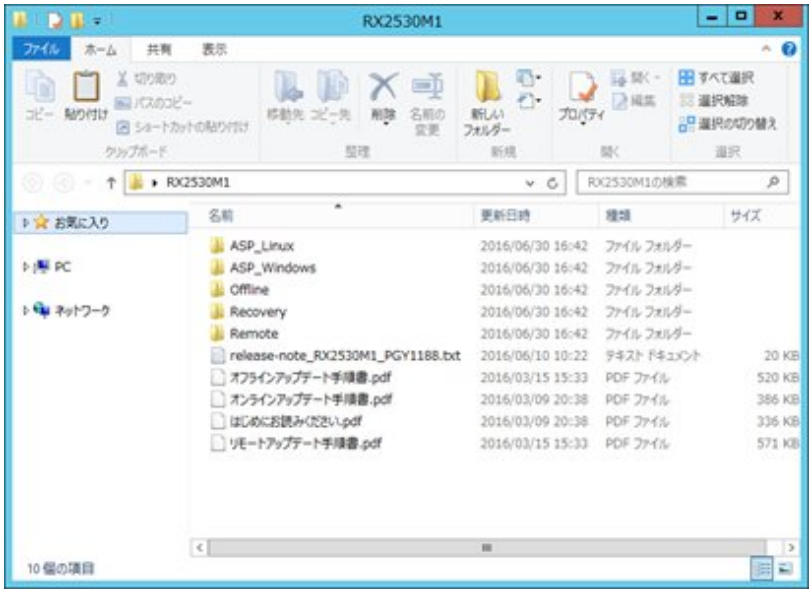
ファームウェアデータのインポート

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

1. ファームウェアデータ入手先から、ファームウェアデータを入手します。

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。

   ー 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。

   ー 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。

   ー 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. ファームウェアデータ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[構築]-[ファームウェア]を選択します。

   b. 画面左側のメニューから[インポート]を選択します。

   c. 以下のどれかを行います。

      - 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、[インポートデータリスト]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。

        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。

      - 富士通のWebサイトからダウンロードしたファームウェアデータをインポートする場合は、[インポートデータリスト]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。

        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、BX920 S4、PRIMEQUEST 3800Bなど	iRMCとSDRのバージョン[注1]
BIOS	RX100 S8、CX2550 M1、BX920 S4、PRIMEQUEST 3800Bなど	BIOSのバージョン[注1]
MMB	BX900 S2	ファームウェアのバージョン[注1]
PRIMEQUEST	PRIMEQUEST 2400S3など	本体ファームウェアのバージョン[注1]
FC	LPe1250、LPe12002、MC-FC82E	BIOSとFWのバージョン[注2]

種類	モデル	バージョン
	LPe1250、LPe12002以外のLPeXXX、MC-FC162E	ファームウェアのバージョン[注2]
	QLEXXX	BIOSのバージョン[注2]
CNA	OCe10102、OCe14102、MC-CNA112E	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]
	CFXモデル	ファームウェアのバージョン[注1]
	PY CB Eth Switch/IBP 1Gb 36/12	ファームウェアのバージョン[注1]
	PY CB Eth Switch/IBP 10Gb 18/8	ファームウェアのバージョン[注1]
	PY CB Eth Switch 10/40Gb 18/8+2	ファームウェアのバージョン[注1]
	Cisco Systems Nexusシリーズ	NX-OSのバージョン[注1]
	Cisco Systems Catalystシリーズ	IOSのバージョン[注1]
FC Switch	Brocade FC Switch	基本ソフトウェアのバージョン[注2]
ETERNUS DX/AF	ETERNUS DX/AF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上部の[タスク]を選択すると、タスクの一覧が表示されます。

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。
- 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データおよび、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[構築]-[プロファイル]を選択します。

4. 画面左側のメニューから[DVDインポート]を選択します。
5. [アクション]ボタンから[DVDインポート]を選択します。
6. [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。

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

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[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[DVDインポート]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[構築]-[プロファイル]を選択します。
4. 画面左側のメニューから[DVDインポート]を選択します。
5. [アクション]ボタンから[DVDインポート]を選択します。
6. [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[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[DVDインポート]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

注意

- 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、QLogic QConvergeConsole CLIのインストールが必要になるPCIカードは、当社の本製品Webサイトを参照してください。

  http://software.fujitsu.com/jp/serverviewism/environment/

- 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
ネットワーク管理機能	VLAN設定の変更
仮想リソース管理機能	仮想リソース情報の更新

「タスク」画面の表示方法

1. ISMのGUIでグローバルナビゲーションメニュー上部の[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。

コンソール管理メニュー

機能	コマンド
ISM-VA基本設定メニュー	ismsetup

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
SSLサーバ自己署名証明書作成	ismadm sslcert self-create

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
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
ISM-VAのアップグレード	ismadm system upgrade
ホスト名変更	ismadm system modify
障害調査ログ切替え	ismadm system set-debug-flag

coreファイルの採取ディレクトリ設定

機能	コマンド
採取ディレクトリ表示	ismadm system core-dir-show
採取ディレクトリ設定	ismadm system core-dir-set
採取ディレクトリ解除	ismadm system core-dir-reset

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

MIBファイル設定

機能	コマンド
MIBファイル登録	ismadm mib import
MIBファイル表示	ismadm mib show
MIBファイル削除	ismadm mib delete

注意

時刻設定により過去の時刻に戻した場合、ISM-VAを再起動する必要があります。

2.3.6 仮想化管理ソフトウェア管理機能

仮想化管理ソフトウェアとの連携機能を利用する場合は、ISMに仮想化管理ソフトウェアを登録します。

仮想化管理ソフトウェア管理機能でサポートする仮想化管理ソフトウェアの最新情報については、当社の本製品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/「補足資料」

仮想化管理ソフトウェアの登録

新しく仮想化管理ソフトウェアを登録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[設定]-[全般]-[仮想化管理ソフトウェア]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 登録に必要な情報を入力します。
   - 仮想化管理ソフトウェア名

     ISM 全体で、一意な名称を設定してください。
   - IPアドレス

     仮想化管理ソフトウェアのIPアドレスを設定してください。

     Microsoft Failover Clusterの場合には、クラスタ仮想IPを登録してください。
   - タイプ

     登録する仮想化管理ソフトの種類を選択してください。

     Microsoft Failover Clusterの場合には、Windows Serverのバージョンも指定してください。

注意

Microsoft Failover Clusterを指定した場合は、[アカウント情報]にドメイン名を必ず設定してください。

- アカウント情報

  仮想化管理ソフトウェアのドメイン名、アカウント名、パスワードを設定してください。

  ドメイン名は大文字で記入してください。

- URL

  仮想化管理ソフトウェアの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。

  [タイプ]にWeb管理機能を提供する仮想化管理ソフトウェアを指定した場合は、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。

- ユーザーグループ

  管理するユーザーグループ名を選択してください。

4. [登録]ボタンを選択します。

   仮想化管理ソフトウェアリスト画面に登録した仮想化管理ソフトウェアが表示されます。

仮想化管理ソフトウェアからの情報取得

ISMでは、ノード上で動作している仮想マシンおよび仮想スイッチの情報を取得して確認できます。

- 仮想マシン情報

  仮想化管理ソフトウェアから取得した仮想マシン情報を、ノードの詳細画面の[仮想マシン]タブで確認できます。

- 仮想スイッチ情報

  仮想化管理ソフトウェアから取得した仮想スイッチ情報は、「ネットワークマップ」画面で確認できます。

  仮想化管理ソフトウェアの種類がVMware vCenter Server、System Center、またはMicrosoft Failover Clusterの場合に取得できます。KVMの場合はサポート外となります。

注意

ISMは、登録されている仮想化管理ソフトウェア情報と、ノードのOS情報を紐づけて仮想マシンおよび仮想スイッチ情報を管理します。仮想マシンおよび仮想スイッチ情報を取得するにはそれぞれを設定してください。

ISMは、仮想マシンおよび仮想スイッチ情報を24時間周期で取得します。任意の時点で情報を取得するには以下の手順を実行してください。

1. 仮想化管理ソフトウェアで管理されているノードのノード情報取得を実行します。

   ノード情報取得完了後、手順2を実行してください。

2. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択します。

3. 以下のどちらかの方法で情報取得を実行してください。

   - すべての仮想化管理ソフトウェアから情報を取得する場合は、[仮想化管理ソフトウェア情報取得]を選択し、[実行]を選択します。
   - 取得対象を限定する場合は、対象の仮想化管理ソフトウェアを選択し、[アクション]ボタンから[情報取得]-[実行]を選択します。

   情報取得が完了すると、[イベント]-[イベント]-[運用ログ]にメッセージID「10021503」のログが出力されます。情報取得に失敗した仮想化管理ソフトウェアが存在する場合、追加で[イベント]-[イベント]-[運用ログ]にログが出力されます。エラーが出力されていないかを確認し、仮想マシンおよび仮想スイッチ情報を確認してください。

注意

- System Centerと、そのSystem Centerに登録されているMicrosoft Failover Clusterの両方をISMに登録している場合、ISMではSystem Centerから情報取得を行い、Microsoft Failover Clusterからは情報取得を行いません。
- Microsoft Failover Clusterをご使用の環境で、仮想マシンをHyper-Vマネージャーから削除した場合は、その仮想マシンをフェイルオーバクラスタマネージャーの役割からも削除してください。

仮想化管理ソフトウェアの編集

ISMに登録されている仮想化管理ソフトウェア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[設定]-[全般]-[仮想化管理ソフトウェア]を選択し、表示される「仮想化管理ソフトウェアリスト」画面で、対象の仮想管理ソフトウェアを選択します。
2. [アクション]ボタンから[編集]を選択します。
3. 情報を編集します。
4. [登録]を実行し、情報の内容を反映します。

仮想化管理ソフトウェアの削除

ISMに登録されている仮想化管理ソフトウェアを削除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[設定]-[全般]-[仮想化管理ソフトウェア]を選択し、表示される「仮想化管理ソフトウェアリスト」画面で、対象の仮想管理ソフトウェアを選択します。
2. [アクション]ボタンから[削除]を選択します。
3. [削除]を実行し、仮想化管理ソフトウェアを削除します。

2.3.7 共有ディレクトリ管理機能

DVDインポートで使用する共有ディレクトリを追加します。

共有ディレクトリの追加

新しく共有ディレクトリを追加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[設定]-[全般]-[共有ディレクトリ]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 必要な情報を入力します。

   ー ホスト名/IPアドレス

   共有ディレクトリのIPアドレスまたはホスト名を設定します。

- ドメイン

  共有ディレクトリのドメイン名を設定します。ドメイン名は大文字で設定します。

- 共有ディレクトリパス

  共有ディレクトリのパスを設定します。

- 種類

  共有ディレクトリタイプをSMB/CIFS、NFSから選択します。

- アカウント名

  共有ディレクトリのアカウント名を設定します。

- パスワード

  共有ディレクトリのパスワードを設定します。

- ユーザーグループ

  共有ディレクトリ情報が所属するユーザーグループを選択します。

4. [登録]ボタンを選択します。

   「共有ディレクトリリスト」画面に追加した共有ディレクトリが表示されます。

注意

- ユーザーグループごとに5つまで共有ディレクトリ情報を追加できます。
- 指定した共有ディレクトリ情報で、共有ディレクトリをマウントできない場合はエラーとなります。

共有ディレクトリの編集

ISMに登録されている共有ディレクトリ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[設定]-[全般]-[共有ディレクトリ]を選択します。
2. 以下のどちらかを行います。
   - 編集したい共有ディレクトリにチェックを付け、[アクション]ボタンから[編集]を選択します。
   - 編集したい共有ディレクトリを選択し、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。
3. 情報を編集します。
4. [登録]を実行し、情報の内容を反映します。

注意

共有ディレクトリがマウント中の場合は、編集できません。

共有ディレクトリの削除

ISMに登録されている共有ディレクトリを削除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[設定]-[全般]-[共有ディレクトリ]を選択します。
2. 以下のどちらかを行います。
   - 削除したい共有ディレクトリにチェックを付け、[アクション]ボタンから[削除]を選択します。
   - 削除したい共有ディレクトリを選択し、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。
3. [削除]を選択します。

注意

共有ディレクトリがマウント中の場合は、削除できません。

共有ディレクトリのマウント

ISMに登録されている共有ディレクトリ情報にマウント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[設定]-[全般]-[共有ディレクトリ]を選択します。
2. 以下のどちらかを行います。
   - マウントしたい共有ディレクトリにチェックを付け、[アクション]ボタンから[マウント]を選択します。
   - マウントしたい共有ディレクトリを選択し、表示された情報画面で[アクション]ボタンから[マウント]を選択します。

注意

- マウントしたディレクトリの権限について、以下に示します。
  - 読み込み専用でマウントします。
  - SMB/CIFSの場合

    共有ディレクトリ情報を作成したユーザーグループの権限と同じユーザー権限でマウントします。
  - NFSの場合

    root権限でマウントします。
- 以下の場合、マウントは解除されます。
  - ISM-VAを再起動、または停止した場合
  - ISMのサービスを停止した場合
- マウントした共有ディレクトリ情報を持つユーザーグループは、以下の操作ができません。
  - ユーザーグループ名の変更
  - ユーザーグループの削除

共有ディレクトリのマウント解除

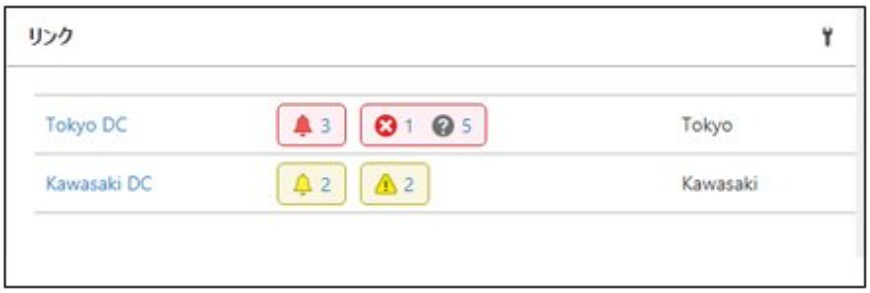
マウントされた共有ディレクトリ情報をマウント解除する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[共有ディレクトリ]を選択します。
2. 以下のどちらかを行います。
   - マウント解除したい共有ディレクトリにチェックを付け、[アクション]ボタンから[マウント解除]を選択します。
   - マウント解除したい共有ディレクトリを選択し、表示された情報画面で[アクション]ボタンから[マウント解除]を選択します。

2.3.8 ISM連携管理機能

2.3.8.1 他ISMのステータス情報のリンク表示機能

ISMで、他ISMのステータス情報（ステータス/アラームステータス）を、ダッシュボードに表示できます。



ステータス（ステータス/アラームステータス）の詳細は、「2.1.1 GUI」を参照してください。

他ISMのステータスをダッシュボードに表示する場合の操作方法を示します。

1. 他ISMのステータスをダッシュボードに表示したいユーザーを設定します。

   なお、このユーザーは、他ISMにも同じユーザー名、パスワードで登録されている必要があります。

   a. 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。
   b. 他ISMのステータスをダッシュボードに表示したいユーザーの編集を行って、以下を設定します。
      - [ISM連携]で[連携用のユーザーとして設定する]を選択
      - パスワード
2. 表示したい他ISMのCA証明書を登録します。
3. GUIのダッシュボードに[リンク]を追加します。
   a. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択します。

      [リンク]が表示されている場合、手順fへ進みます。

      [リンク]が表示されていない場合、以下の手順でリンクを追加してください。
   b. [レイアウト設定]を選択します。
   c. [+追加]を選択します。
   d. 表示される[ウィジェット追加]から[リンク]を選択し、追加します。
   e. [レイアウト変更中]の[保存]を選択します。
   f. ダッシュボードに表示される[リンク]の[ ]を選択します。
   g. 「ウィジェット設定:リンク」画面で、以下を設定します。
      - 名前:ウィジェットで表示したい名前を指定します。
      - URL:他ISMへのURLを以下のように指定します。

        https://＜対象ISMのIPアドレス、またはFQDN名＞:＜ポート番号＞

- 説明:説明(コメント)を自由に指定してください。

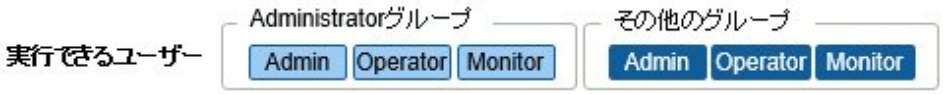
ウィジェット追加方法は、『ServerView Infrastructure Manager V2.2 操作手順書』を参照してください。

ウィジェットの内容の詳細については、ISMのオンラインヘルプを参照してください。

2.3.8.2 他ISMのリンク用の証明書管理機能

ウィジェットのリンク機能で、他ISMにアクセスする場合のCA証明書を追加します。

証明書の登録



新しく証明書を追加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[設定]-[全般]-[CA証明書]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 必要な情報を入力します。
   - インポート完了後の動作

     元のファイルを削除するかどうかを選択します。
   - ファイル

     アクセスしたい他ISMのCA証明書をFTPでアップロードし、アップロードしたファイルを設定してください。
   - ホスト名/IPアドレス

     アクセスしたい他ISMのホスト名、またはIPアドレスを設定してください。
4. [登録]ボタンを選択します。

   結果画面が表示され、「CA証明書リスト」画面に登録した証明書が表示されます。

注意

- 登録する証明書は、CA証明書です。CA証明書は、「4.7.5 CA証明書のダウンロード」を参照してください。
- 登録した証明書で、実際に他ISMにアクセスできるかはチェックされません。

証明書の削除

ISMに登録されている証明書を削除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[設定]-[全般]-[CA証明書]を選択します。
2. 以下のどちらかを行います。
   - 削除したい証明書にチェックを付け、[アクション]ボタンから[削除]を選択します。
   - 削除したい証明書を選択し、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。
3. [削除]を実行し、証明書を削除します。

注意

ウィジェットのリンク機能を使用中の場合でも、証明書は削除できます。

2.4 ノード削除時、グループ変更時の操作

ノードを削除する場合や、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 ノード削除時

ノードを削除する場合は、事前に以下の操作を完了させてください。

- 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。

ポイント

プロファイルが適用された状態でノードを削除すると、当該ノードは削除されません(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。
- 当該ノードに関するアラーム設定は、削除してください。

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。

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。

- ファームウェアデータのインポート操作
- 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
- ネットワークの設計
- ノード名の設定
- ユーザーの設定

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。

「3.7 仮想ディスクの割当て」を参照して、ISM-VA全体とAdministratorユーザーグループに対して仮想ディスクを割り当ててください。

注意

ISM-VA導入後は、すぐに「3.7.2 ユーザーグループに対する仮想ディスク割当て」手順でAdministratorグループ用の仮想ディスク割当てを行ってください。

(7)仮想化管理ソフトウェアの登録

管理対象ノードに構築された仮想マシンや仮想スイッチを管理する場合、仮想化管理ソフトウェアを登録します。

仮想化管理ソフトウェアの登録作業については、「2.3.6 仮想化管理ソフトウェア管理機能」を参照してください。また、仮想化管理ソフトウェア管理機能を使用するために必要な事前設定については、当社の本製品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/「補足資料」

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

ISMの利用にあたっては、下表のディスク領域の使用量見積りと事前の追加割当てを行ってください。

用途	保管されるデータ	容量算出方法	種別	
			システム領域	ユーザー領域
ログ保存	ログ管理機能で取得したログ、およびアーカイブしてダウンロードする際のファイル 「2.2.5 ログ管理機能」	ログを採取するノード数、採取するログの種類、採取頻度、保管期間に応じて算出 「3.2.1.1 ログ保存容量の見積り」	○[注1]	○
リポジトリ（ServerView Suite DVDを除く）	DVDイメージやファームウェアデータ 「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」	インポートするDVD数、ファームウェアデータ量に応じて算出 「3.2.1.2 リポジトリの必要容量の見積り」	○[注1]	○
リポジトリ（ServerView Suite DVDのみ）	DVDイメージ 「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」	インポートするDVD数に応じて算出 「3.2.1.2 リポジトリの必要容量の見積り」	○	－
ノード管理データ	ISMが内部動作に使用するデータ	管理するノード数に応じて算出 「3.2.1.3 ノード管理データ容量の見積り」	○	－
障害調査ログ	トラブル発生時の調査などに使用するログ	管理するノード数に応じて算出 「3.2.1.4 障害調査ログ容量の見積り」	○	－
保守資料	障害調査ログをアーカイブして取り出す際のファイル 「4.5 保守資料の採取」	管理するノード数および資料を保管する世代に応じて算出 「3.2.1.5 保守資料容量の見積り」	○[注1]	○[注2]

[注1]:ユーザーグループに領域が割り当てられている場合、そのユーザーグループでは割り当てられた領域が使用されます。領域が割り当てられていないユーザーグループではシステム領域が使用されます。

[注2]:Administratorユーザーグループのリポジトリ領域に出力されます。

注意

- 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。

  システム領域に対する仮想ディスクの作成、割当て方法については、「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。

  ユーザーグループに対する仮想ディスクの作成、割当て方法については、「3.7.2 ユーザーグループに対する仮想ディスク割当て」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。

現在使用中のディスク容量は、以下の手順で確認できます。

1. コンソールからadministratorでISM-VAにログインします。
2. ディスクの使用状況を確認します。

   ```
   ismadm volume show -disk -r
   ```

   /dev/mapper/centos-rootを確認します。

   例)

```
# ismadm volume show -disk -r
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/centos-root   31G  4.2G   27G  14% /
devtmpfs                 3.9G     0  3.9G   0% /dev
tmpfs                    3.9G  4.0K  3.9G   1% /dev/shm
tmpfs                    3.9G  225M  3.7G   6% /run
tmpfs                    3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/sda1                497M  172M  326M  35% /boot
tmpfs                    783M     0  783M   0% /run/user/1005
tmpfs                    783M     0  783M   0% /run/user/0
tmpfs                    783M     0  783M   0% /run/user/1001

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g    0
  /dev/sda3  centos lvm2 a--  15.00g    0
#
```

3.2.1.1 ログ保存容量の見積り

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。
また、ログをダウンロードする際に使用するディスク容量も同様に見積ってください。

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、当社の本製品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/「補足資料」

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納	UpdateDVDのインポート	UpdateDVD1枚あたり7GB程度
	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ファイル格納	Windowsインストールメディアのインポート	OS1種あたり3～8GB程度 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ポート	OS1種あたり0.5GB程度 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
coreファイル採取・保管	ismadm system core-dirでの設定	1GB程度

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ServerView Suite DVD以外の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。

3.2.1.3 ノード管理データ容量の見積り

ISM-VAで管理するノード数に応じて、ノード管理データ領域のためのディスク容量を見積もってください。

以下は、管理対象ノード数とノード管理データ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	必要なディスク容量	
	ネットワーク統計情報を監視しない場合	ネットワーク統計情報を監視する場合
100ノード	20GB	25GB
400ノード	80GB	100GB
1000ノード	200GB	250GB

ネットワーク統計情報については、「2.2.6 ネットワーク管理機能」を参照してください。

3.2.1.4 障害調査ログ容量の見積り

ISM-VAで管理するノード数に応じて、障害調査ログレベルの設定を変更し、ディスク容量を見積もってください。

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	障害調査ログレベル	必要なディスク容量
100ノード以下	small（デフォルト）	10GB

管理対象ノード数	障害調査ログレベル	必要なディスク容量
400ノード以下	medium	40GB
1000ノード以下	large	100GB

ログレベルの切替え方法については、「4.17 障害調査ログレベル切替え」を参照してください。

3.2.1.5 保守資料容量の見積り

ISM-VAで管理するノード数に応じて、障害調査ログレベルの設定を変更し、ディスク容量を見積もってください。

以下は、管理対象ノード数と保守資料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	障害調査ログレベル	必要なディスク容量
100ノード以下	small(デフォルト)	15GB
400ノード以下	Medium	50GB
1000ノード以下	Large	120GB

ログレベルの切替え方法については、「4.17 障害調査ログレベル切替え」を参照してください。

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、MMB、仮想IOの設定などに使用します。

- オンボードLANまたはLANカード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。

注意

ISM-VAは、デフォルトで「192.168.1.101」のIPアドレスが有効になった状態で起動します。ネットワーク内のほかの装置との競合に注意してください。

IPアドレスが競合する場合は、以下のような手順でIPアドレスを変更することにより、競合を解消できます。

1. 本番環境以外のハイパーバイザーにISM-VAをインストール
2. ISM-VAのIPアドレスを変更
3. 「4.4.1 ISM-VAのバックアップ」手順に従いバックアップ
4. バックアップしたISM-VAを、「4.4.2 ISM-VAのリストア」手順に従い本番環境のハイパーバイザーにリストア

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文字の文字列が設定できます。

ただし以下の文字は使用できません。

スラッシュ(/)、バックスラッシュ(¥)、コロン(:)、アスタリスク(*)、クエスチョンマーク(?)、ダブルクォーテーション(“)、山括弧(<>)、パイプライン(|)

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 2.2 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。

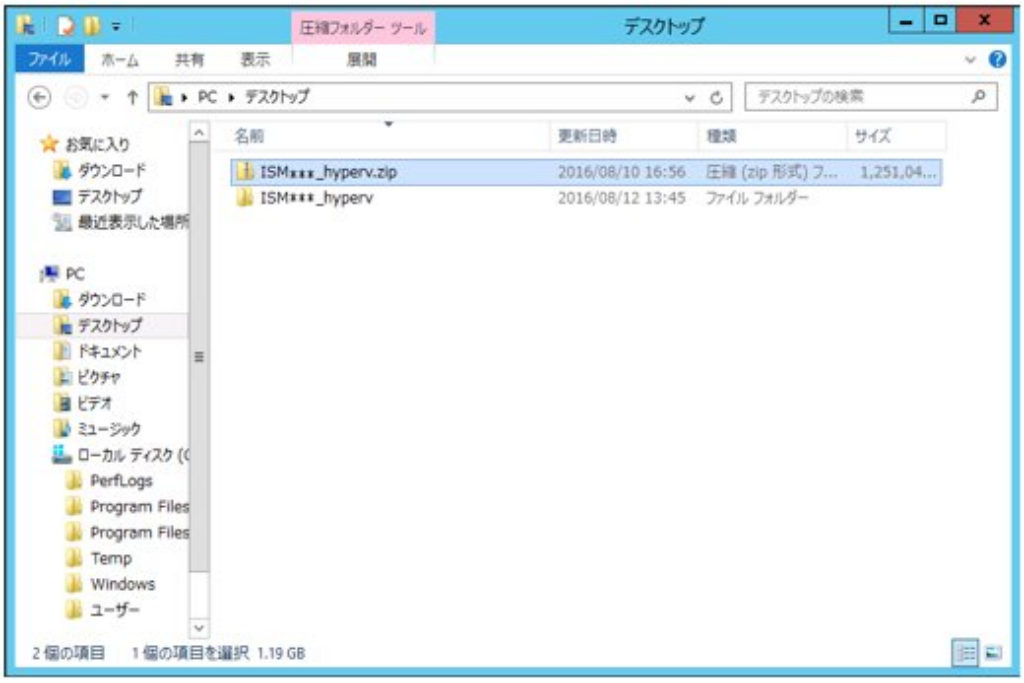
以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMへのインストール手順を説明します。

- 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

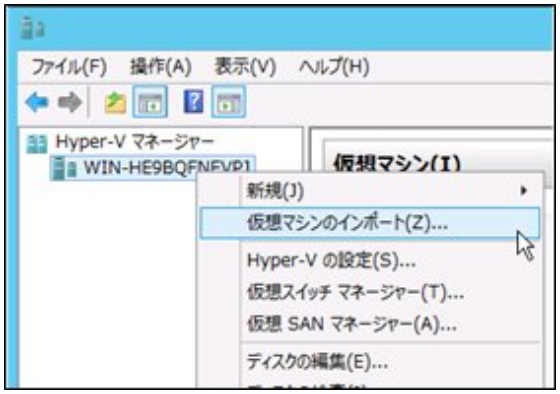
3.3.1 Microsoft Windows Server Hyper-Vへのインストール

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。

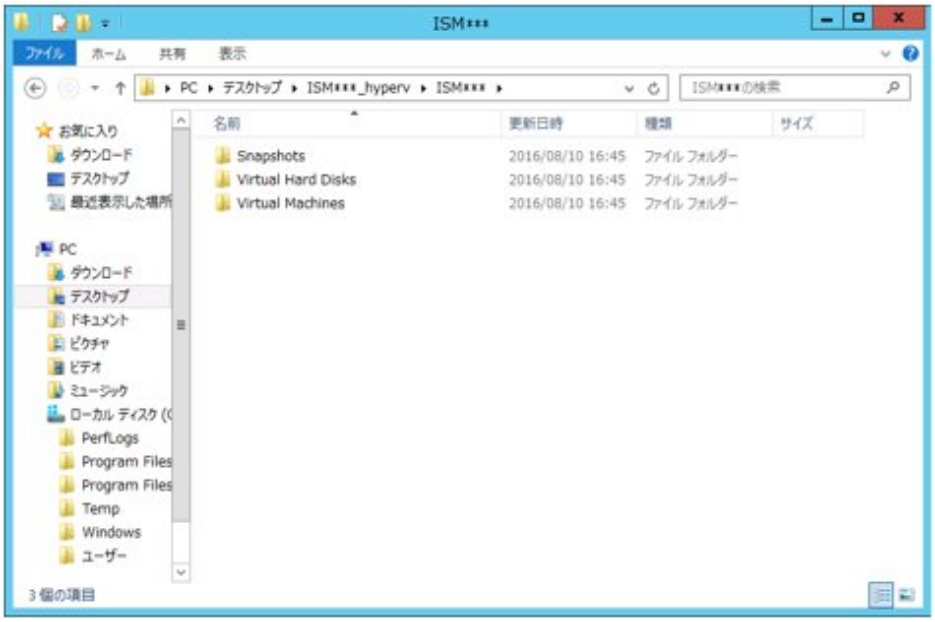


2. Hyper-Vマネージャーを起動し、Hyper-Vホストであるwindowsサーバを右クリックして[仮想マシンのインポート]を選択します。

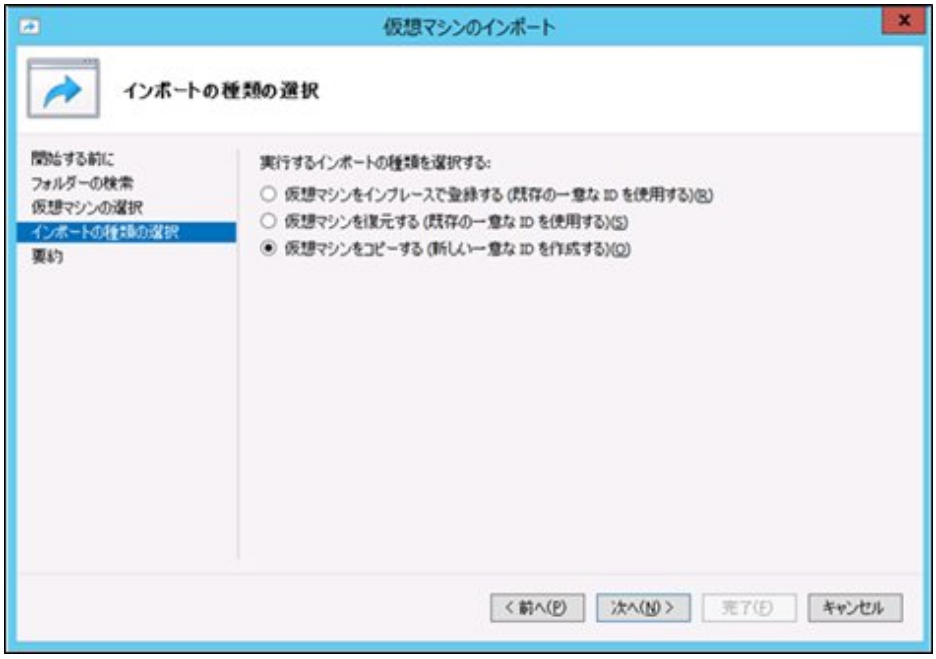


3. 「フォルダーの選択」画面で、手順1で展開したディレクトリを選択します。

   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。

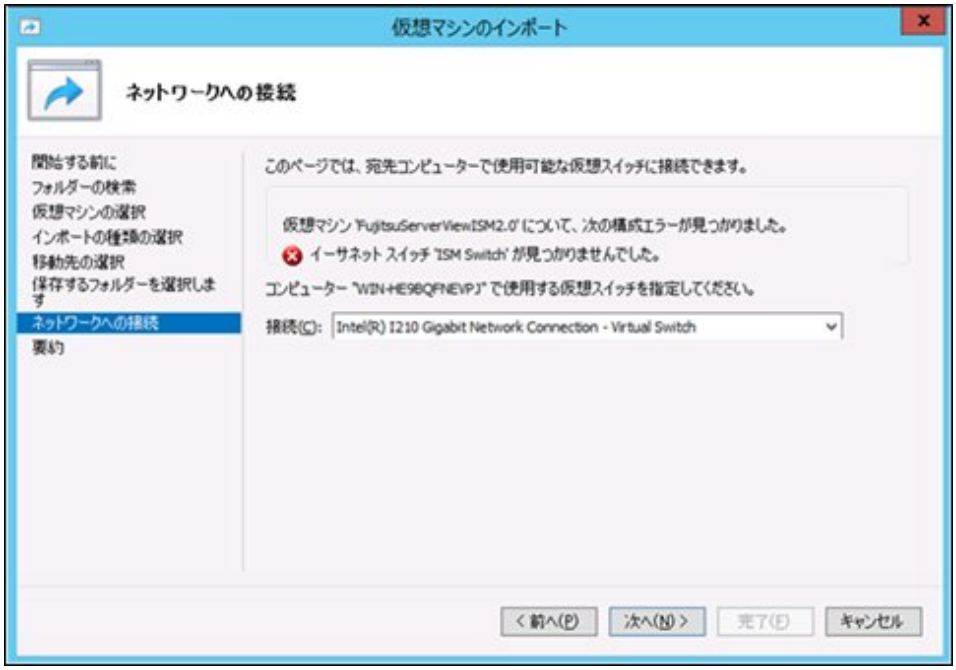


4. 「インポートの種類の選択」画面で、[仮想マシンをコピーする（新しい一意なIDを作成する）]を選択し、[次へ]を選択します。



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]を選択します。



7. [完了]を選択し、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。

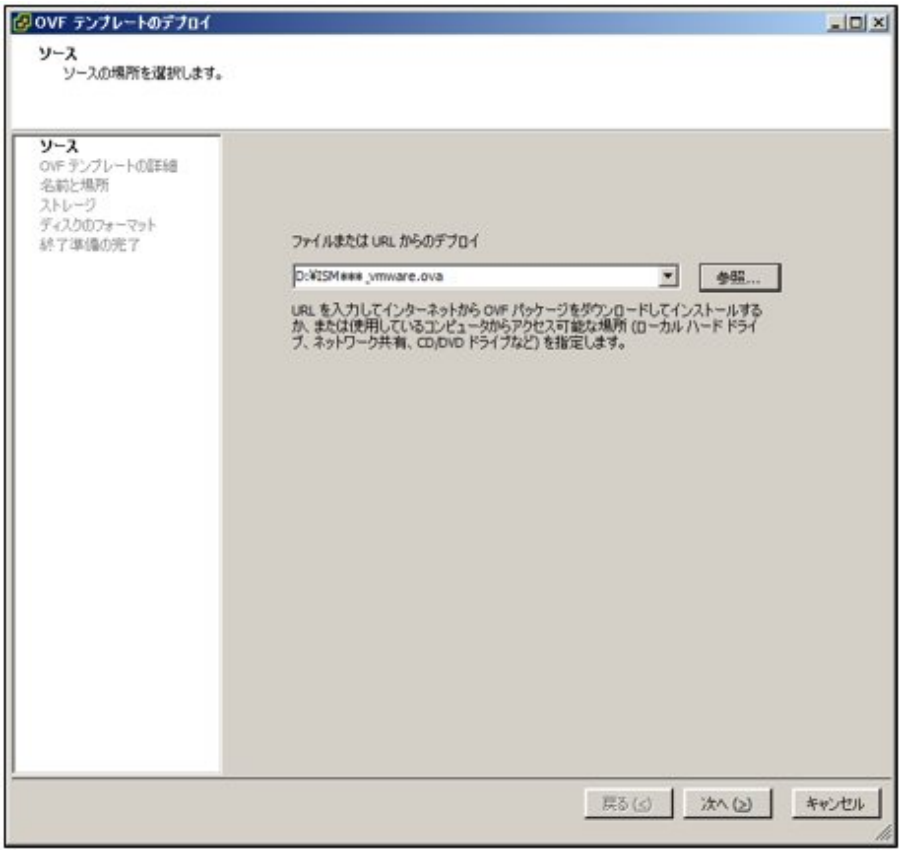
VMware ESXiのバージョンによって操作が異なります。該当するバージョンの参照先をご覧ください。

- 3.3.2.1 VMware ESXi 5.5またはVMware ESXi 6.0へのインストール
- 3.3.2.2 VMware ESXi 6.5以降へのインストール

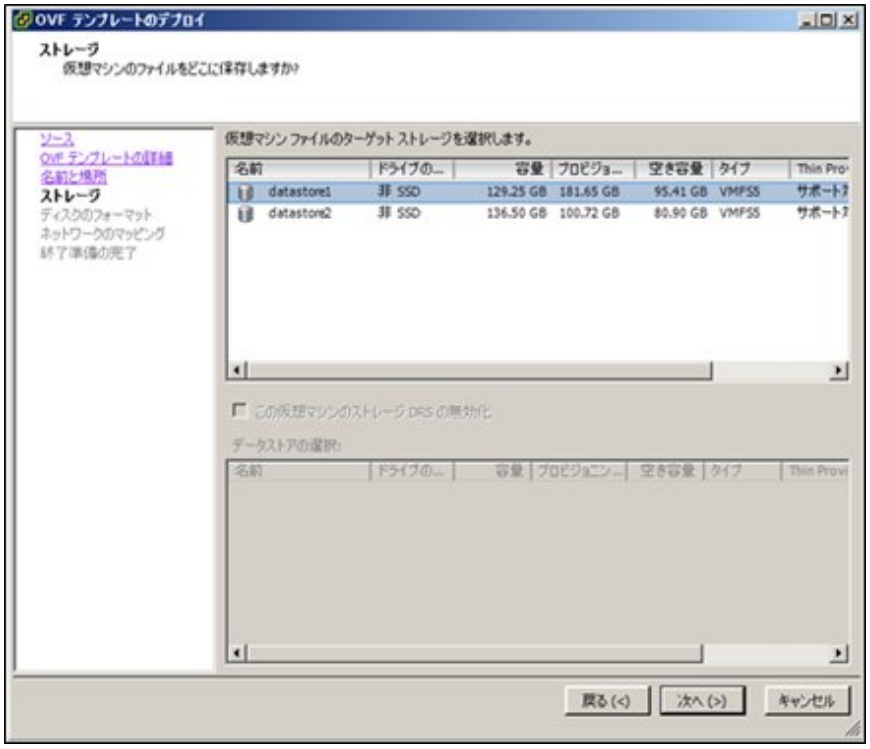
3.3.2.1 VMware ESXi 5.5またはVMware ESXi 6.0へのインストール

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。

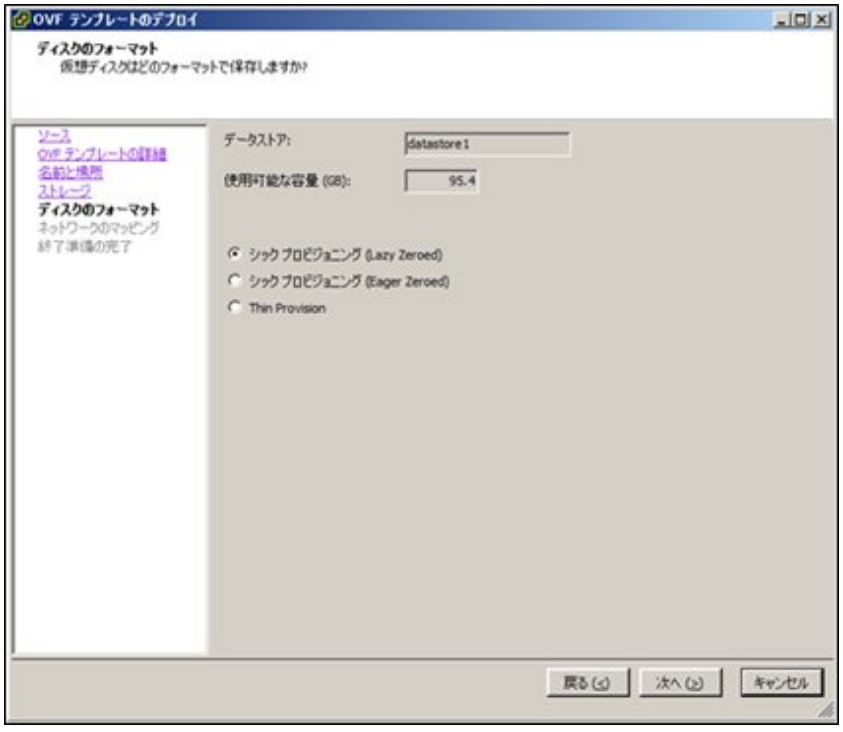
2. ソースの選択画面で、DVDメディアに含まれるovaファイルを選択し、[次へ]を選択します。



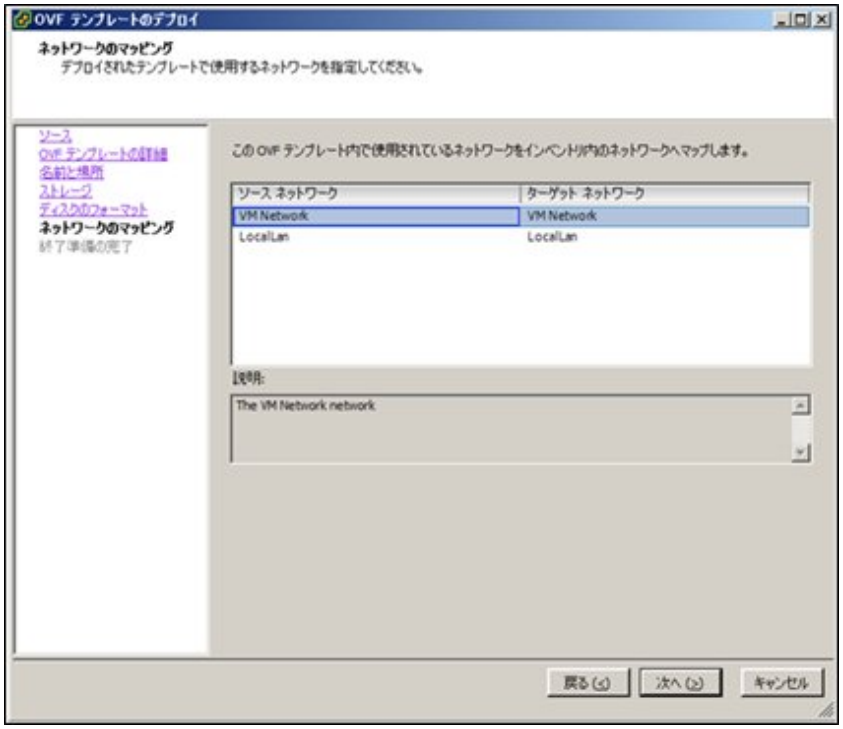
3. 「ストレージ」画面で、仮想マシンの保存場所を指定し、[次へ]を選択します。



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]を選択します。



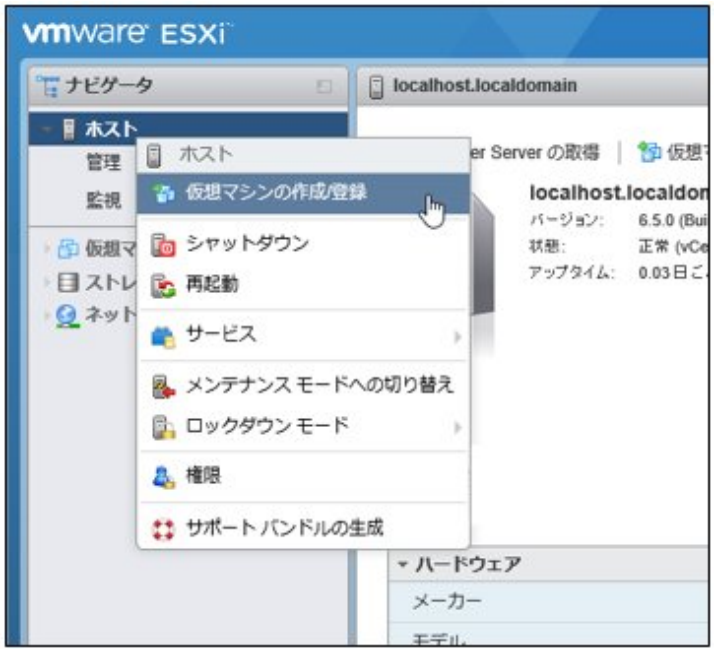
5. 「ネットワークのマッピング」画面で、ISMで使用するネットワークを選択し、[次へ]を選択します。



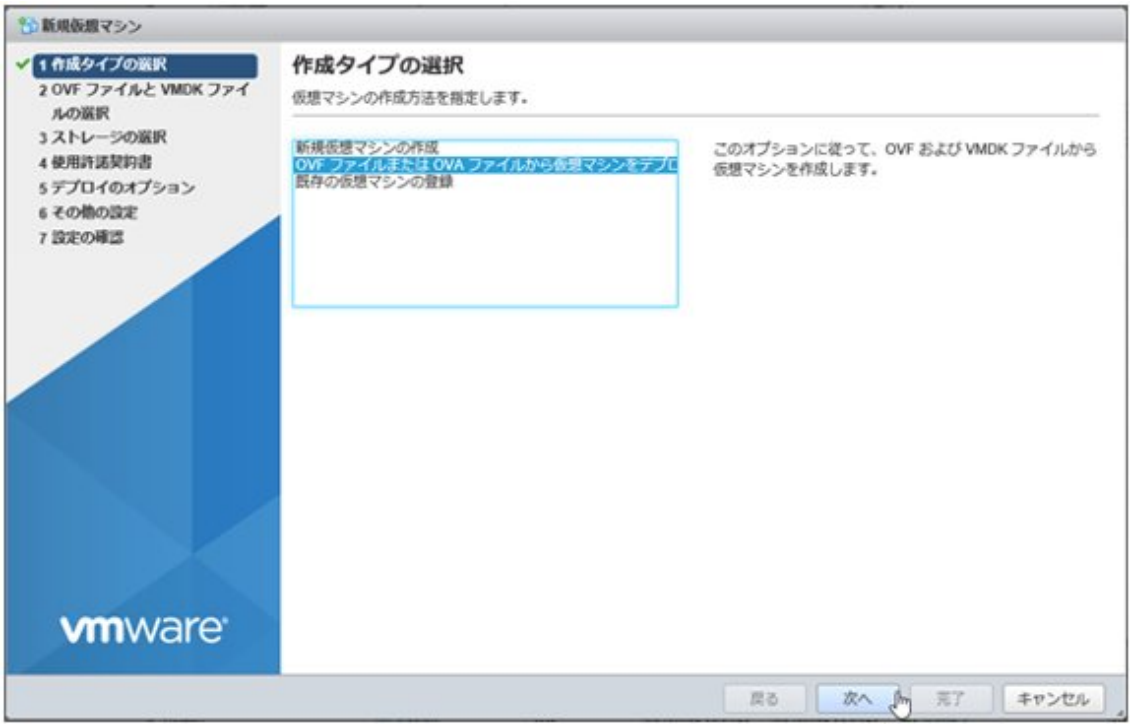
6. [完了]を選択し、OVFテンプレートのデプロイを完了させます。

3.3.2.2 VMware ESXi 6.5以降へのインストール

1. vSphere Client（HTML5）を起動し、ナビゲータの[ホスト]を右クリックして、[仮想マシンの作成/登録]を選択します。

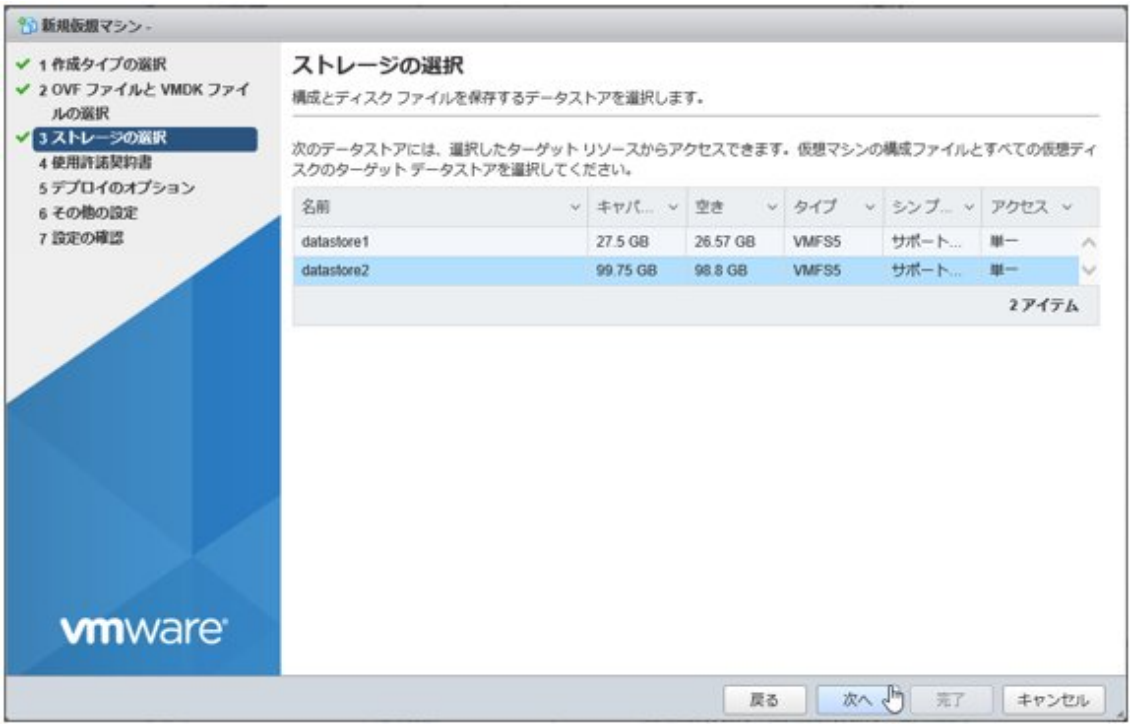


2. 「作成タイプの選択」画面で[OVFファイルまたはOVAファイルから仮想マシンをデプロイ]を選択し、[次へ]を選択します。

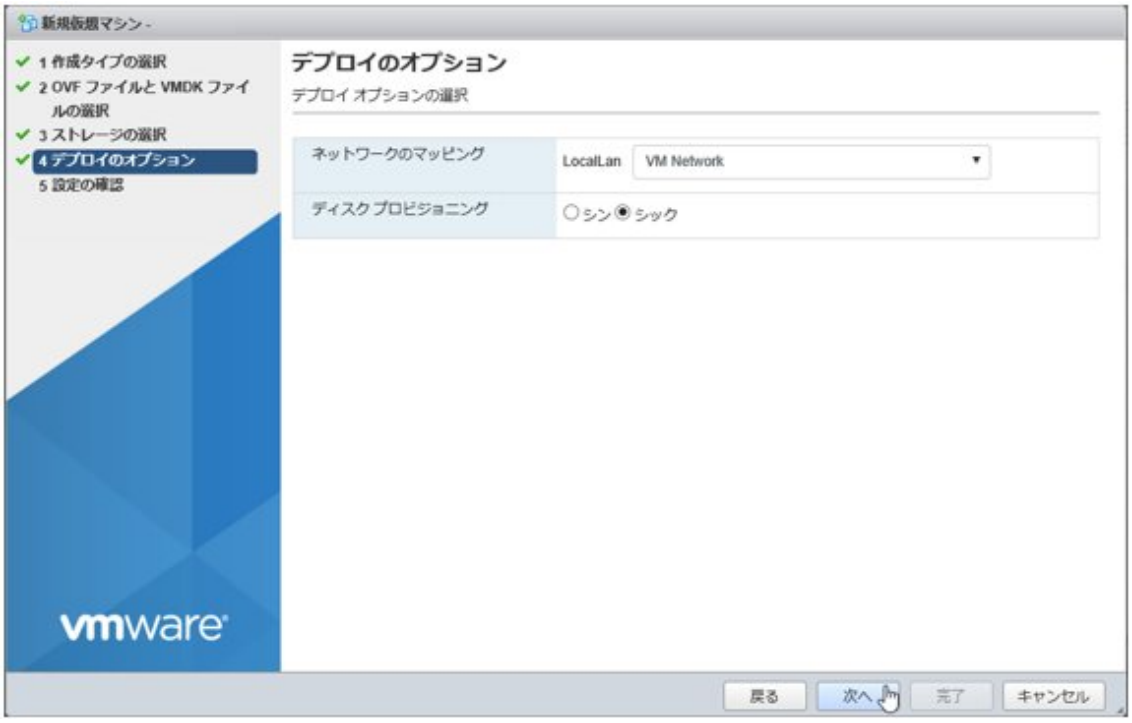


3. 「OVFファイルとVMDKファイルの選択」画面で仮想マシンに任意の名称を指定し、DVDメディアに含まれるovaファイルをデプロイ設定して、[次へ]を選択します。

4. 「ストレージの選択」画面でデプロイ先のデータストアを選択し、[次へ]を選択します。



5. 「デプロイのオプション」画面で使用するネットワークを選択し、ディスクプロビジョニングは「シック」を選択して、[次へ]を選択します。



6. 「設定の確認」画面で設定内容を確認し、[完了]を選択してデプロイを完了させます。

3.3.3 KVMへのインストール

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 ISM＜Version＞_kvm.tar.gz
ISM＜Version＞_kvm/
ISM＜Version＞_kvm/ISM＜Version＞_kvm.qcow2
ISM＜Version＞_kvm/ISM＜Version＞.xml
```

＜Version＞部分は、ISM-VAの版数に応じた表記になります。

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 ISM＜Version＞_kvm.qcow2 /var/lib/libvirt/images
   ```

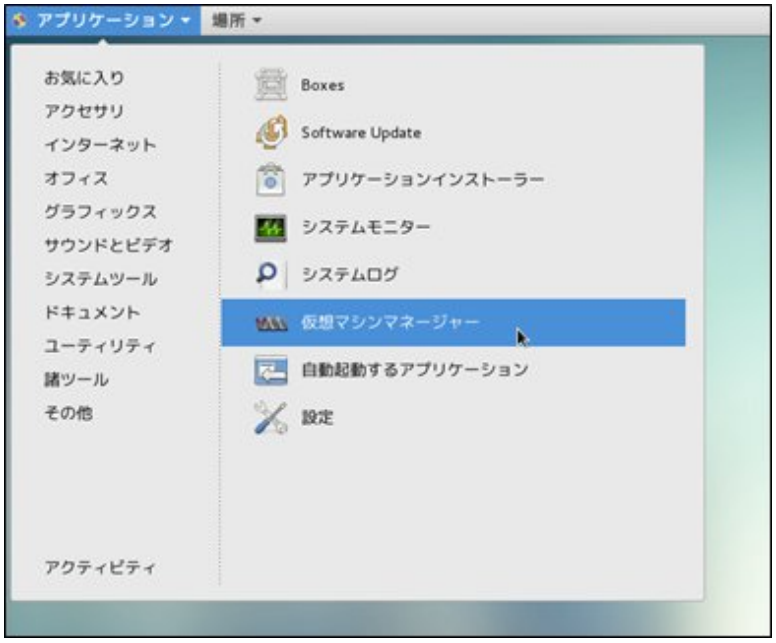
   b. xmlファイルを/etc/libvirt/qemuにコピーします。

   ```
   # cp ISM＜Version＞.xml /etc/libvirt/qemu
   ```

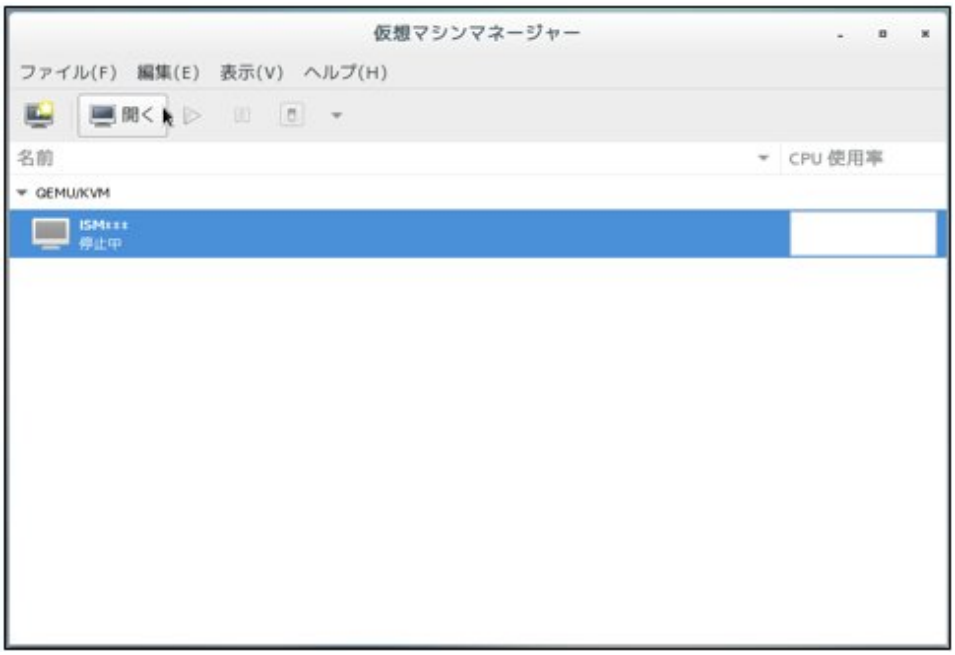
3. xmlファイルを指定してISM-VAを登録します。

```
# virsh define /etc/libvirt/qemu/ISM＜Version＞.xml
```

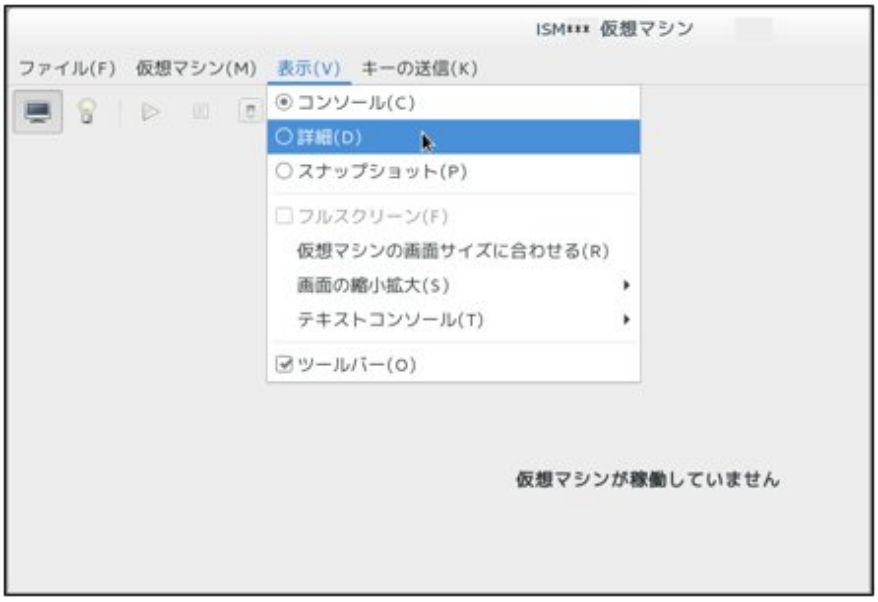
4. [仮想マシンマネージャー]を選択し、仮想マシンマネージャーを開きます。



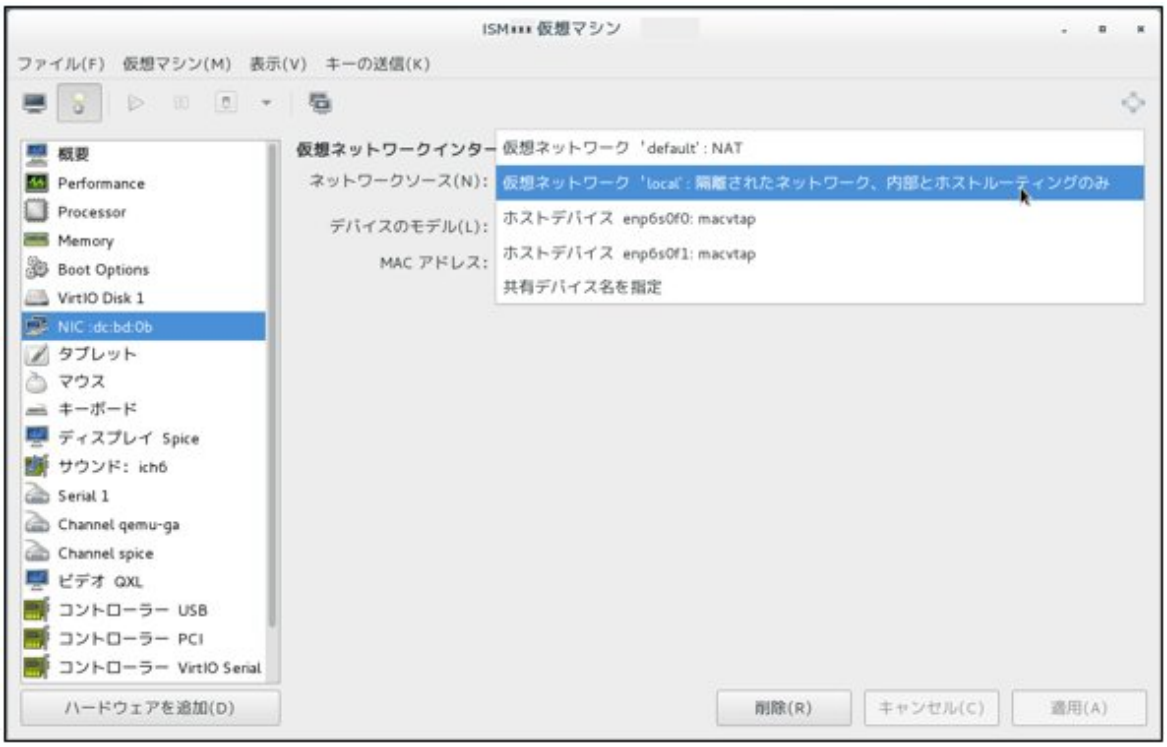
5. 仮想マシンマネージャー上でISM-VAを選択し、[開く]を選択します。



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。



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]を選択します。



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

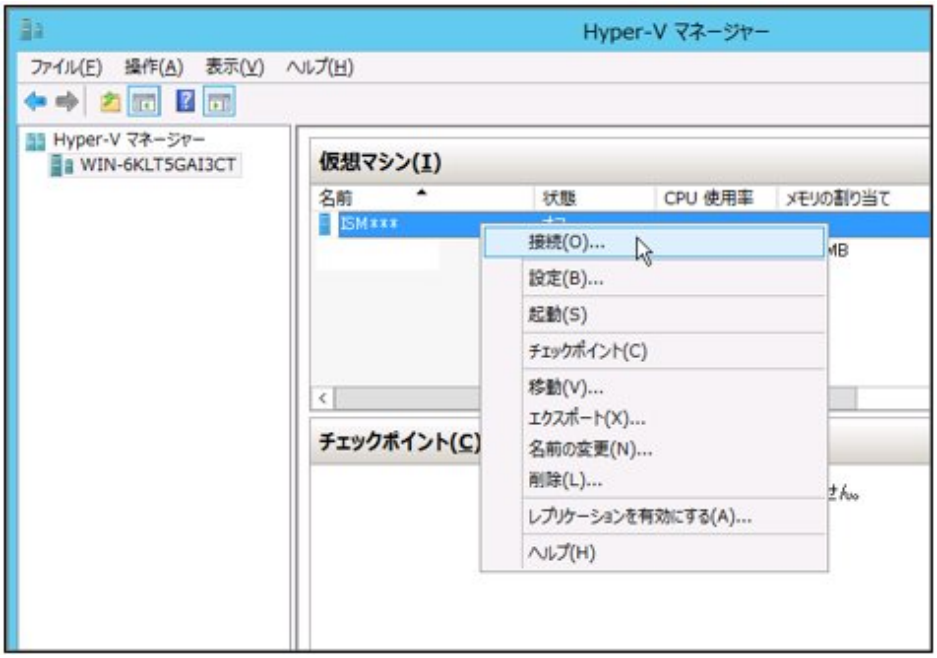
インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

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。

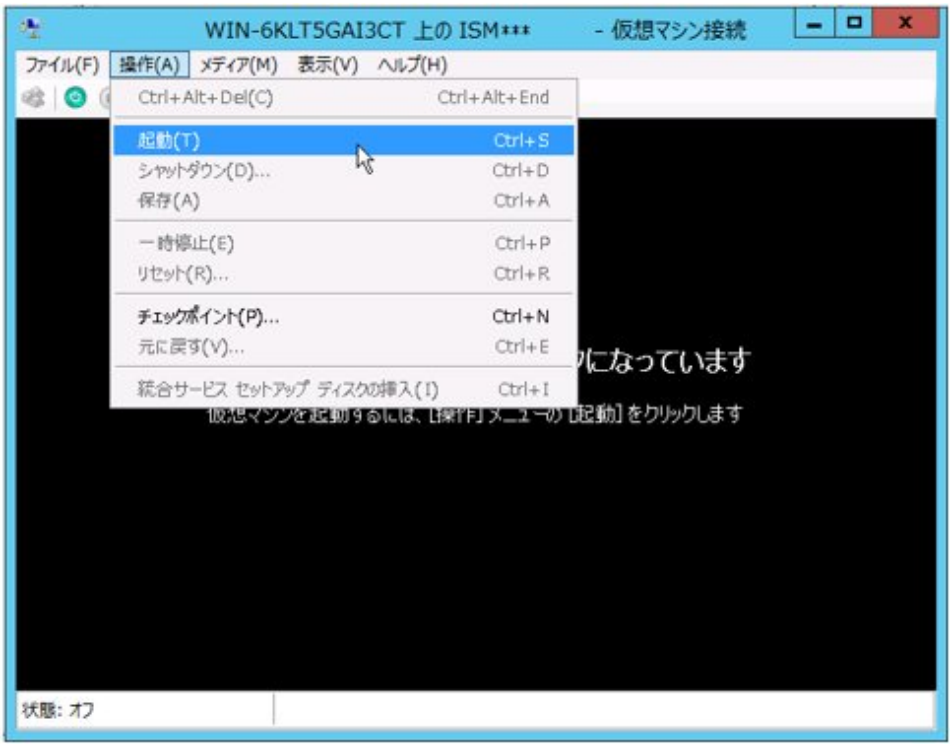
- 3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（初回）
- 3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（初回）
- 3.4.1.3 KVMで動作するISM-VAの場合（初回）

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。



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。



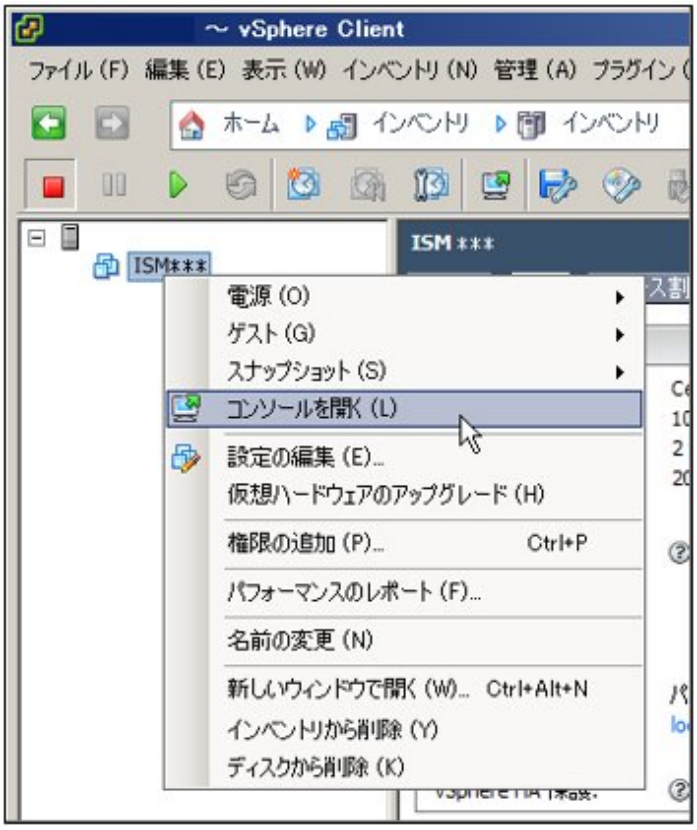
3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（初回）

VMware ESXiのバージョンによって操作が異なります。該当するバージョンの参照先をご覧ください。

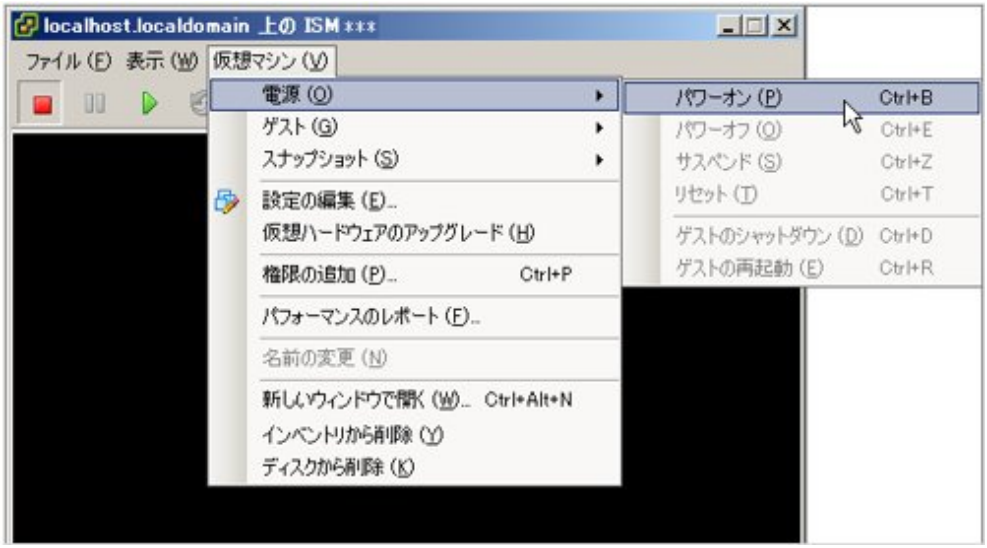
- VMware ESXi 5.5またはVMware ESXi 6.0の場合
- VMware ESXi 6.5以降の場合

VMware ESXi 5.5またはVMware ESXi 6.0の場合

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。

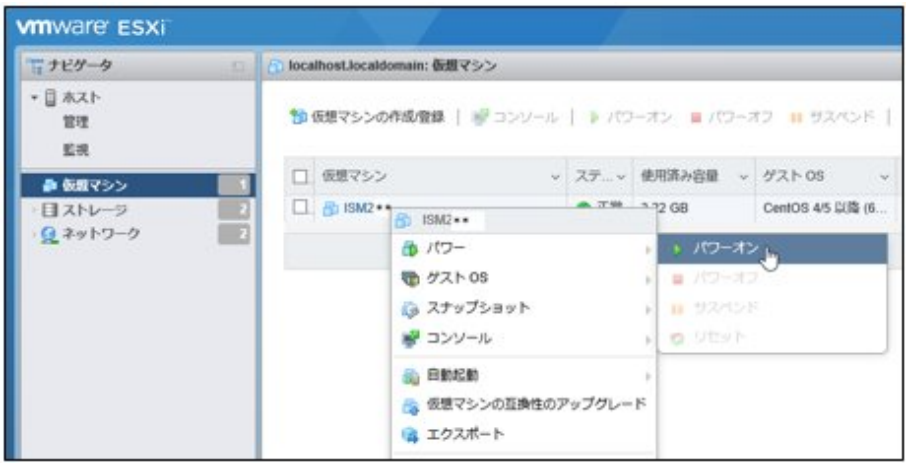


2. 「コンソール」画面の[仮想マシン]メニューから[電源]-[パワーオン]を選択し、ISM-VAを起動します。

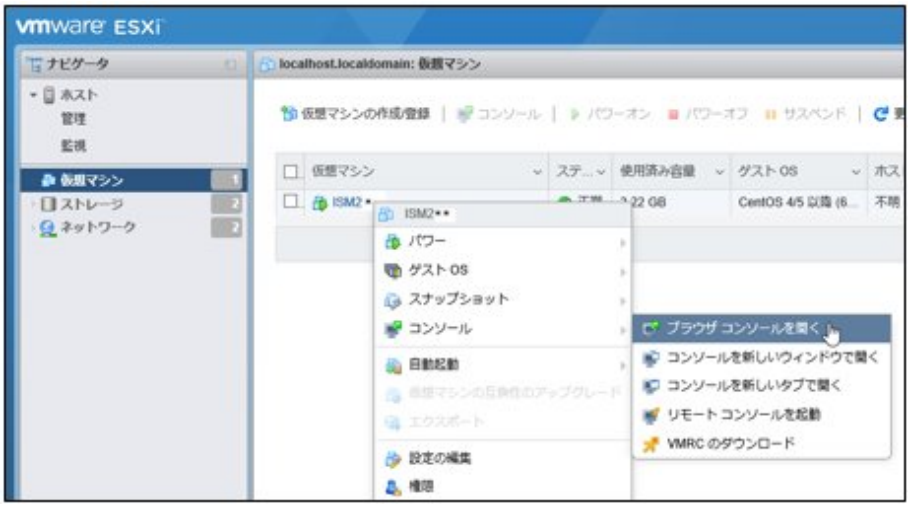


VMware ESXi 6.5以降の場合

1. vSphere Client（HTML5）で、インストールしたISM-VAを右クリックし、[パワーオン]を選択します。



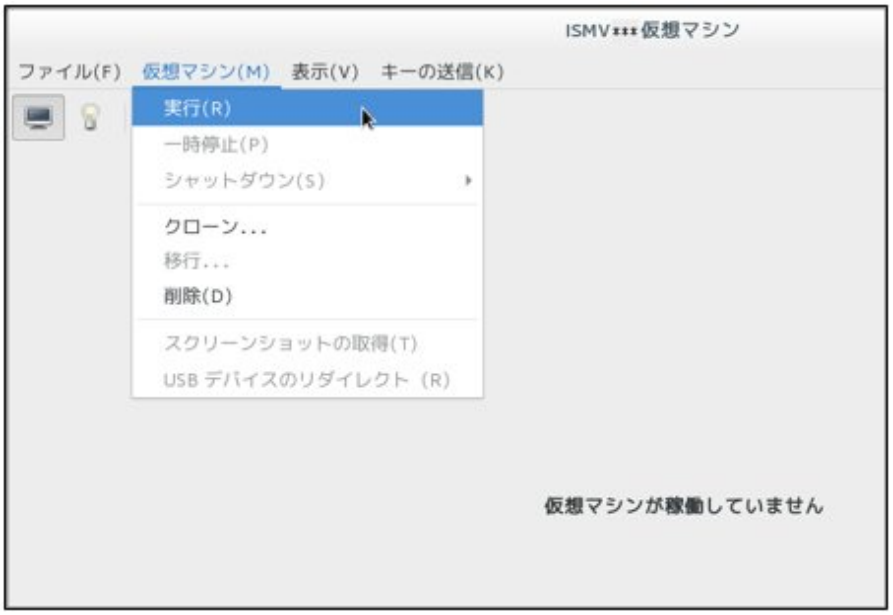
2. インストールしたISM-VAを右クリックし、[ブラウザコンソールを開く]またはほかのコンソールを選択します。



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。



3.4.2 ISM初期設定

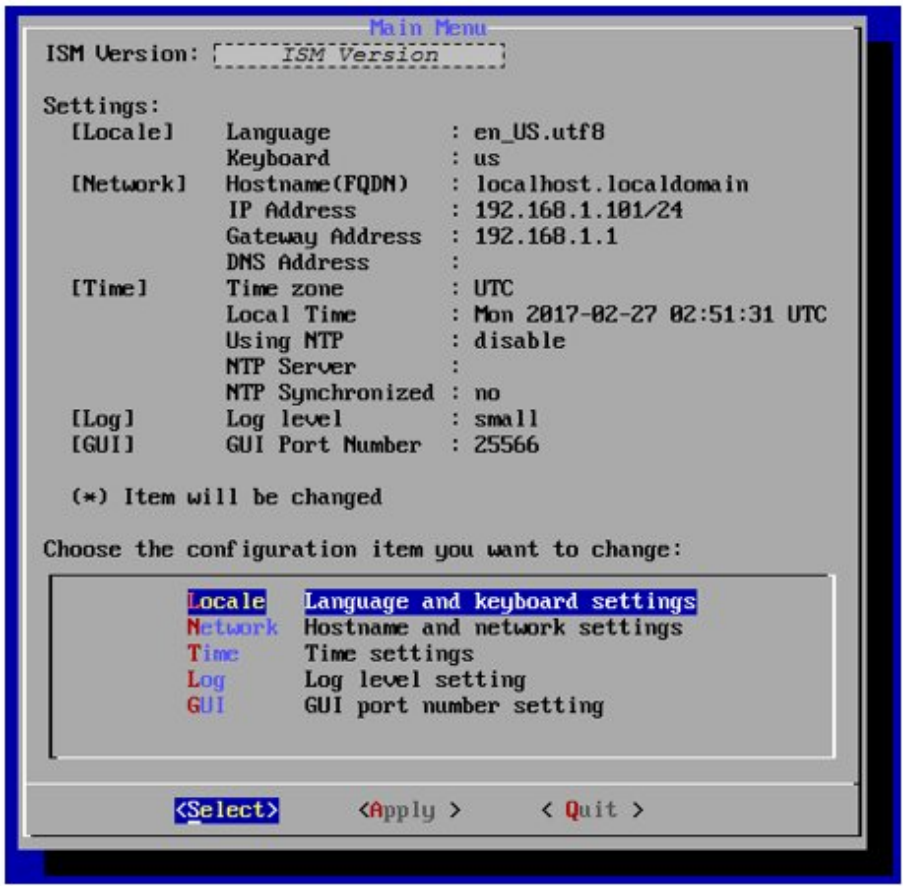
ISM-VA起動後、コンソールの基本設定メニューまたはismadmコマンドを使用して、ISMの基本的な設定を行います。

3.4.2.1 基本設定メニューを使用した初期設定

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. 以下のコマンドを実行し、基本設定メニューを起動します。

```
# ismsetup
```

以下の画面が表示されます。



3. ISMの設定を行います。

   基本設定メニューでは、以下の項目を設定できます。

   - ロケール
   - ネットワーク
   - NTPサーバ
   - ログレベル
   - Web GUIポート番号

   基本設定メニューの詳細は、「4.2 ISM-VA基本設定メニュー」を参照してください。

   ドメイン環境の設定が必要な場合は、「3.4.2.2 ismadmコマンドを使用した初期設定」の手順5を実行してください。

3.4.2.2 ismadmコマンドを使用した初期設定

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。

ー 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
```

ー 設定可能な＜ロケール名＞の表示

```
# ismadm locale list-locales
```

ー Keymapの設定

```
# ismadm locale set-keymap ＜キーマップ名＞
```

実行例

```
# ismadm locale set-keymap us
```

ー 設定可能な＜キーマップ名＞の表示

```
# ismadm locale list-keymaps
```

表3.1 キーマップ一覧

言語名	キーマップ名
日本語	jp
英語	us
ドイツ語	de-nodeadkeys
中国語	cn
韓国語	kr
フィリピン語	ph

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
          Time zone: Asia/Tokyo (JST, +0900)
       NTP enabled: no
  NTP synchronized: no
   RTC in local TZ: no
        DST active: n/a

NTP Servers:
506 Cannot talk to daemon
```

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。

ー 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 America/New_York
```

ー 設定可能なタイムゾーンの表示

```
# ismadm time list-timezones
```

ー 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
```

ー 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
```

ー NTPサーバ追加削除

サーバ追加

```
# ismadm time add-ntpserver ＜NTPサーバ＞
```

サーバ削除

```
# ismadm time del-ntpserver ＜NTPサーバ＞
```

5. コンソールで、ドメイン環境の設定をします。

ドメイン環境を使用しない場合には本設定は不要です。

ー ドメイン設定情報を追加する

```
# ismadm kerberos add -d ＜Domain Name＞ -r ＜Realm＞ -n ＜Controller Name＞
```

実行例

```
# ismadm kerberos add -d sample.local -r SAMPLE.LOCAL -n adsvr.sample.local
```

－ ドメイン設定情報を表示する

```
# ismadm kerberos show
```

－ ドメイン設定情報を1つ前の状態に戻す

```
# ismadm kerberos restore
```

2つ以上前の状態に戻すことはできません。

－ ドメイン設定情報を初期化する

```
# ismadm kerberos init
```

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、コンソールから登録する方法と、Webブラウザで動作するGUIから登録する方法の2通りあります。

コンソールから登録する方法

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
   ```

Webブラウザで動作するGUIから登録する方法

ライセンスを初めて登録する場合

1. 「3.4.2 ISM初期設定」を実施します。
2. ISM-VAを再起動します。
3. Webブラウザで動作するGUIを起動します。
4. GUIからadministratorでログインします。

5. ライセンスキーを以下の方法で登録します。

    a. 入力フィールドに、ライセンスキーを指定します。

    b. [適用]ボタンを選択します。

    c. ほかに登録するライセンスキーがある場合、[追加]ボタンを選択して入力フィールドを追加します。

    d. 手順a～cを繰り返し、すべてのライセンスを登録後、[閉じる]ボタンを選択します。

    ポイント

    [登録済ライセンス]ボタンを選択すると、登録済みのライセンスが一覧表示されます。

6. [ISM-VA再起動]ボタンを選択して、ISM-VAを再起動します。

ノードライセンスを追加で登録する場合

GUIからadministratorでログインし、以下の方法で新しくライセンスを登録します。

1. [設定]-[全般]-[ライセンス]で、ライセンス画面を表示します。
2. [登録]ボタンを選択します。
3. 入力フィールドに、ライセンスキーを指定します。
4. ほかに登録するライセンスキーがある場合、[追加]ボタンを選択して入力フィールドを追加します。
5. 手順3～4を繰り返し、すべてのライセンスを指定後、[適用]ボタンを選択します。

注意

GUIからはライセンスの削除はできません。ライセンスの削除は、コンソールから行ってください。詳細は、「4.8 ライセンス設定」のライセンス削除を参照してください。

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

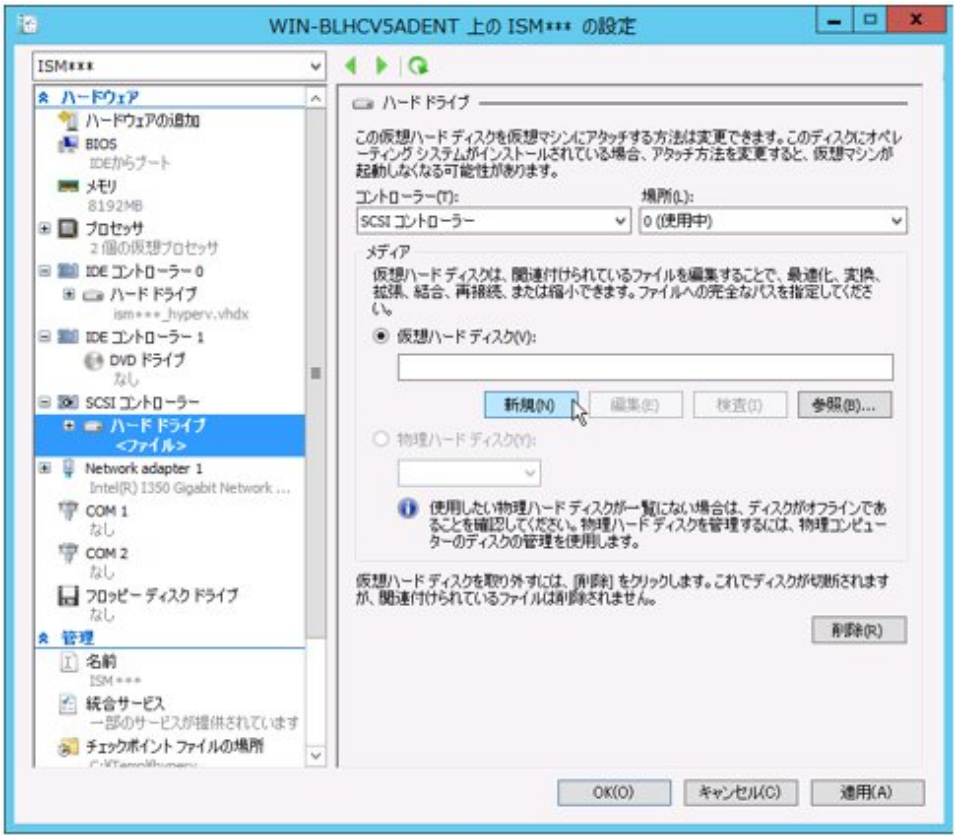
仮想ディスクは、ISM-VAのディスク容量を増設するための資源です。ログやリポジトリ、バックアップの格納には大容量のディスク資源が必要になります。また、それらの運用方法や管理対象ノードの規模などによって容量が異なります。大容量の資源を仮想ディスクに割り当てることによって、ISM-VAのディスク容量や負荷の影響を回避します。仮想ディスクには必要十分な容量を確保しておくことで、ログやリポジトリ、バックアップの運用を円滑に行えます。

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

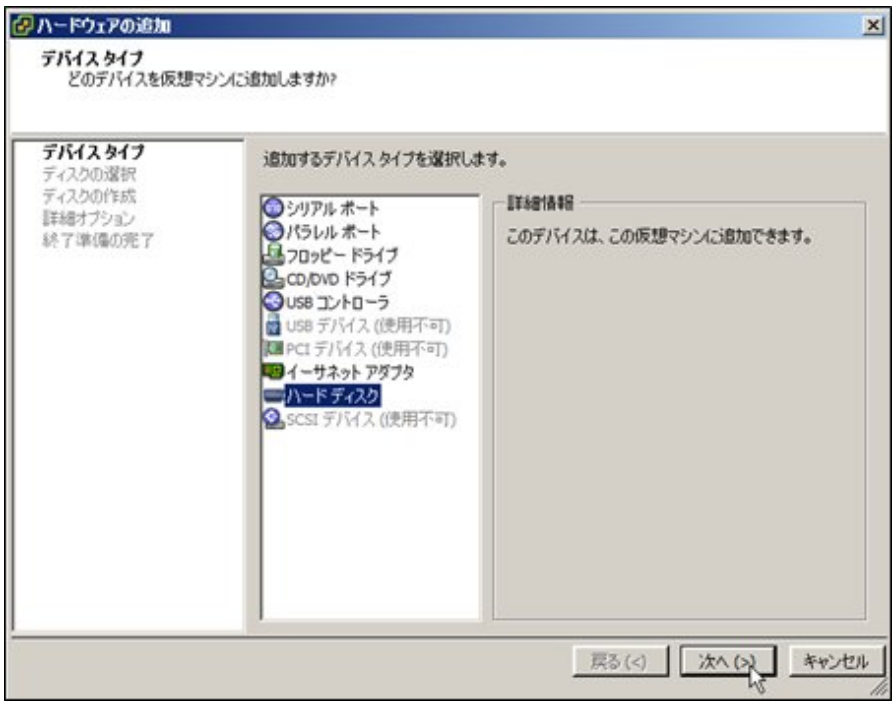
1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA（仮想マシン）に接続します。

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 5.5またはVMware vSphere Hypervisor 6.0の場合

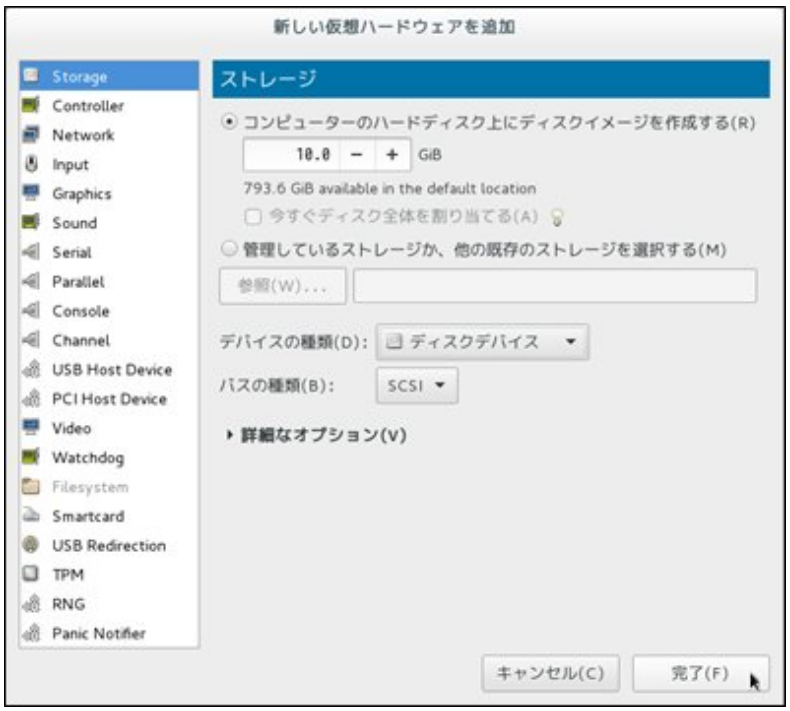


作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

VMware vSphere Hypervisor 6.5の場合

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



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
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  4.0K  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  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. 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 volume show -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/centos-root    26G  2.5G   23G   10% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  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
tmpfs                     380M     0  380M    0% /run/user/0

  PV         VG       Fmt  Attr PSize  PFree
  /dev/sda2  centos   lvm2 a--  19.51g    0
  /dev/sdb1  centos   lvm2 a--  10.00g    0
```

7. ISM-VAを再起動します。

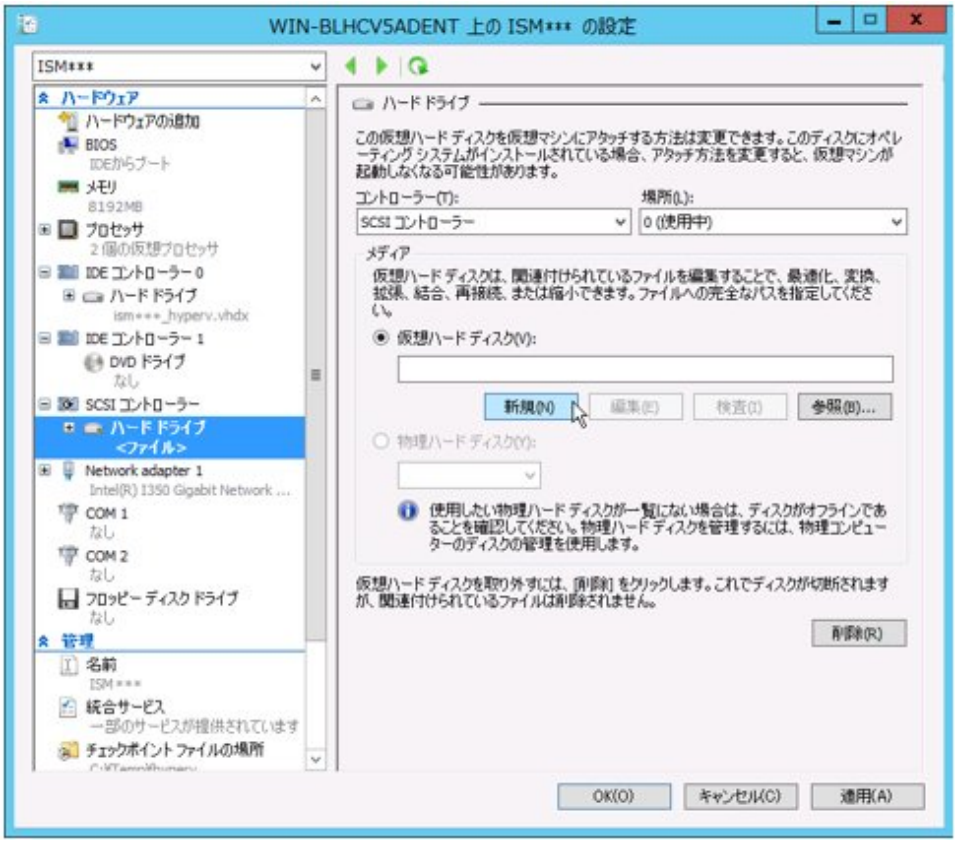
```
# ismadm power restart
```

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。

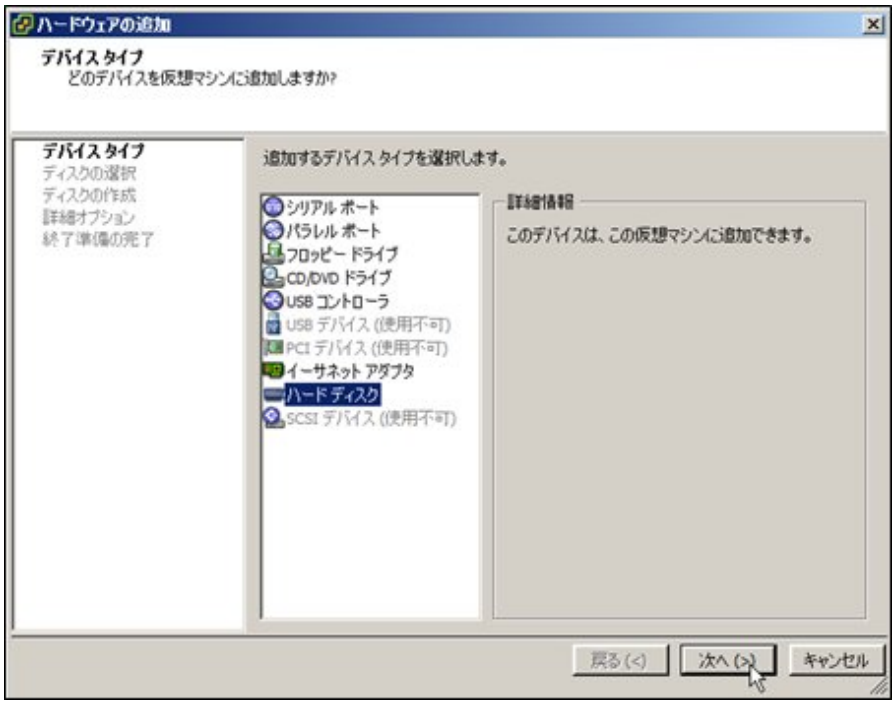
1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA（仮想マシン）に接続します。

Microsoft Windows Server Hyper-Vの場合



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 5.5またはVMware vSphere Hypervisor 6.0の場合



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。

VMware vSphere Hypervisor 6.5の場合

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

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
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  4.0K  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  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任意の名称(例:「adminvol」など)で作成し、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(以下例では「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 -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/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  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   8.0G   39M  8.0G    1% 'RepositoryRoot'/Administrator

  PV         VG       Fmt  Attr PSize  PFree
  /dev/sda2  centos   lvm2 a--  19.51g    0
  /dev/sdb1  adminvol lvm2 a--   8.00g    0
```

8. ISM-VAを再起動します。

```
# ismadm power restart
```

3.8 仮想リソース管理機能の事前設定

仮想化基盤の運用監視は、仮想リソース管理機能を使用して行えます。

仮想リソースの管理・監視は、ISM GUIの仮想リソースの各管理画面から行えます。

なお、仮想リソース管理GUIの内容および表示項目の説明などについては、ISMのオンラインヘルプを参照してください。

注意

仮想リソース管理機能の事前設定については、当社の本製品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/「補足資料」

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

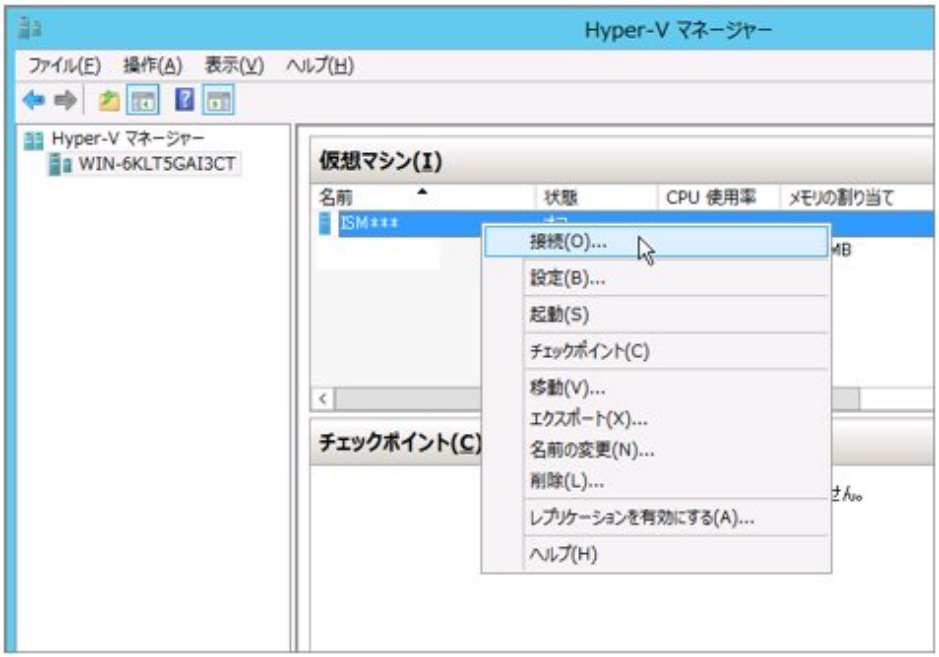
インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

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。

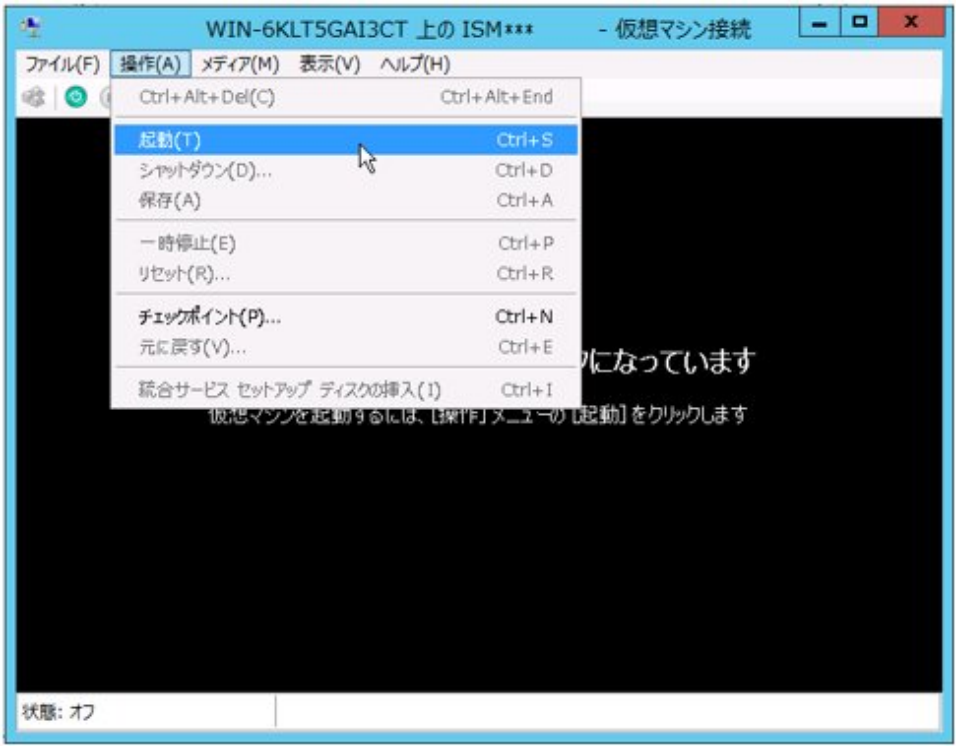
- 4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（2回目以降）
- 4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（2回目以降）
- 4.1.1.3 KVMで動作するISM-VAの場合（2回目以降）

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。



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。



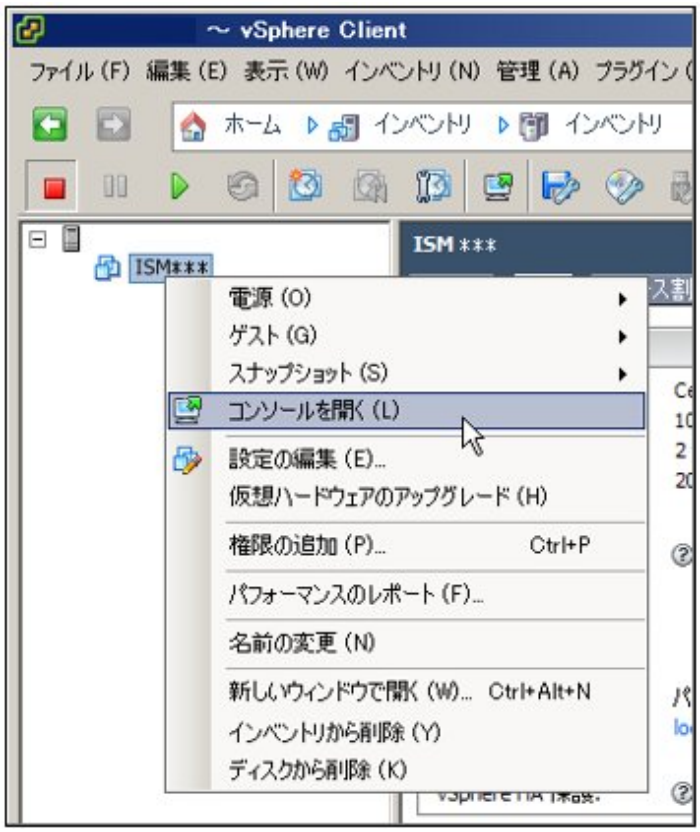
4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（2回目以降）

VMware ESXiのバージョンによって操作が異なります。該当するバージョンの参照先をご覧ください。

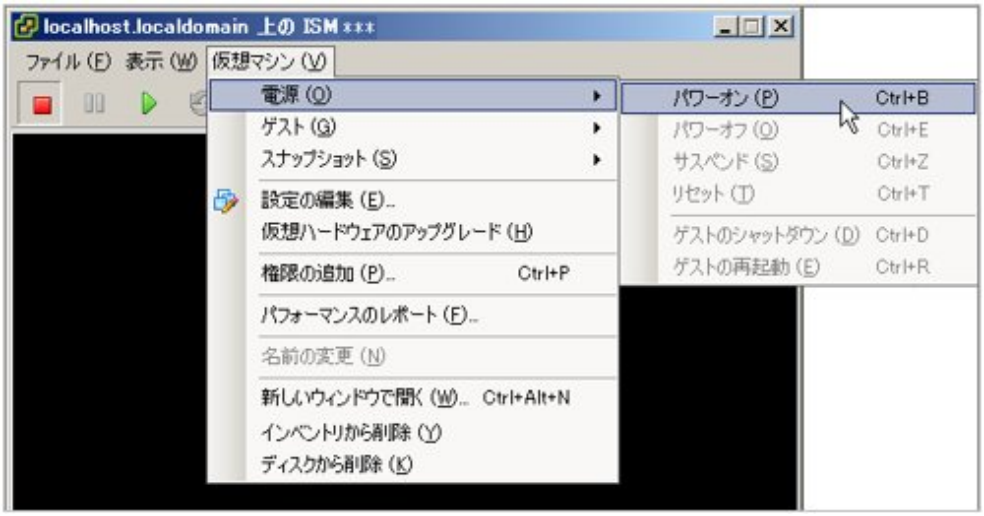
- VMware ESXi 5.5またはVMware ESXi 6.0の場合
- VMware ESXi 6.5以降の場合

VMware ESXi 5.5またはVMware ESXi 6.0の場合

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。

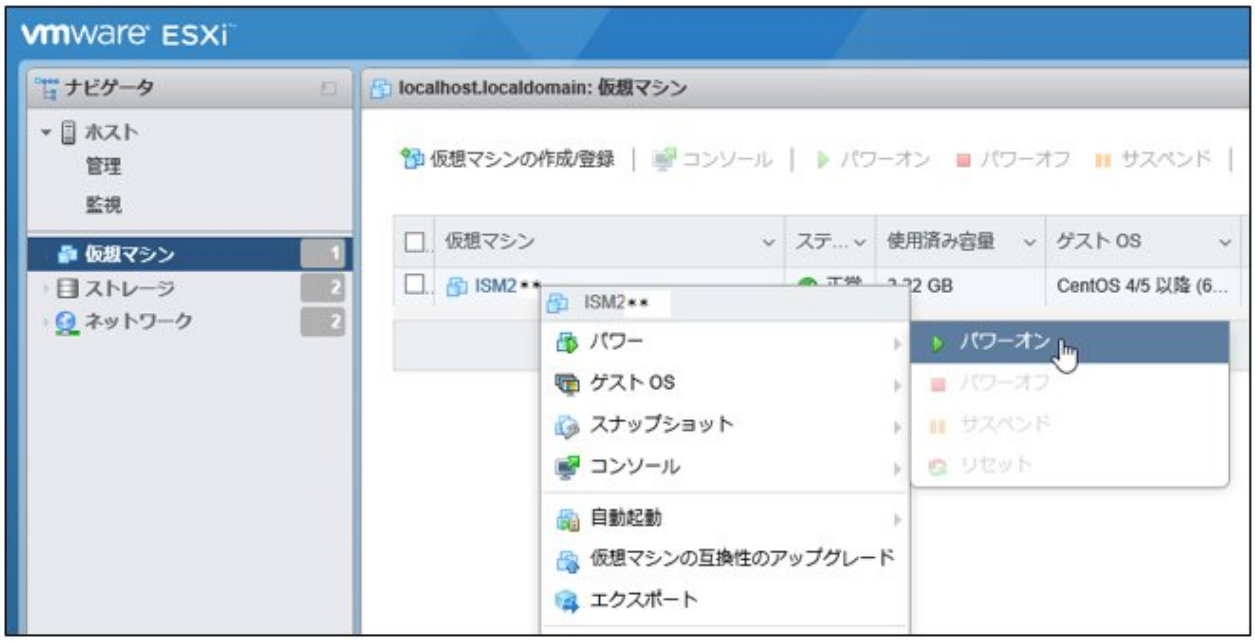


2. 「コンソール」画面の[仮想マシン]メニューから[電源]-[パワーオン]を選択し、ISM-VAを起動します。

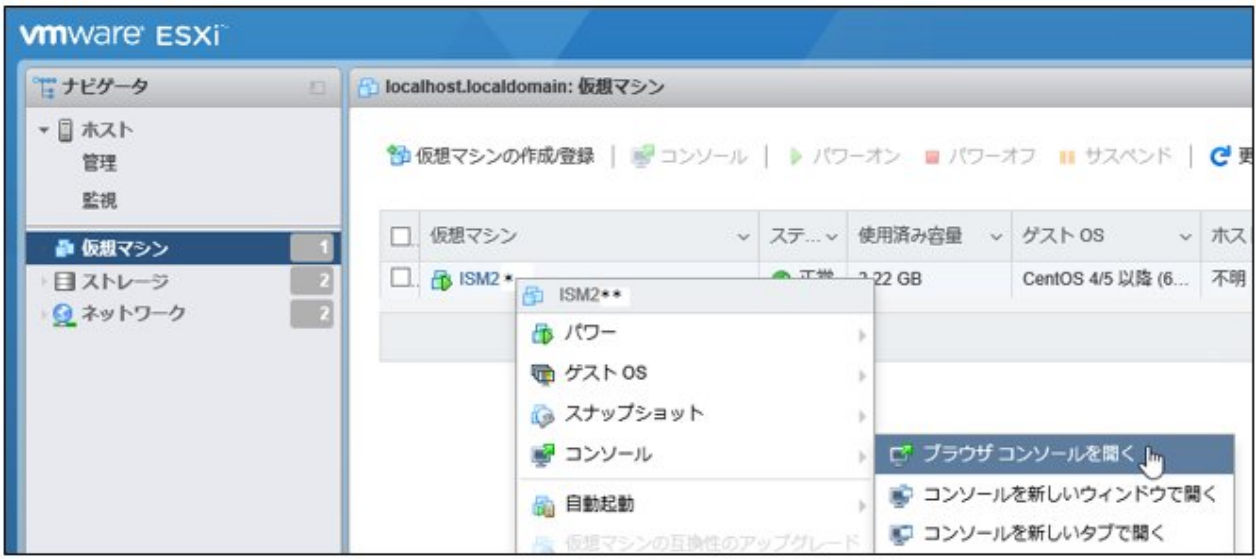


VMware ESXi 6.5以降の場合

1. vSphere Client（HTML5）で、インストールしたISM-VAを右クリックし、[パワーオン]を選択します。



2. インストールしたISM-VAを右クリックし、[ブラウザコンソールを開く]またはほかのコンソールを選択します。



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。

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. ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択します。

b. 「タスク」画面で、ステータスが「完了」または「キャンセル完了」になっていることを確認します。

c. 「完了」または「キャンセル完了」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]ボタンから[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「Updating firmware」(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。

注意

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-VA基本設定メニュー

ISM-VAの基本的な設定を、メニュー選択および項目選択方式で簡単に実行できます。

ISM-VA基本設定メニューで設定できる項目を以下に示します。

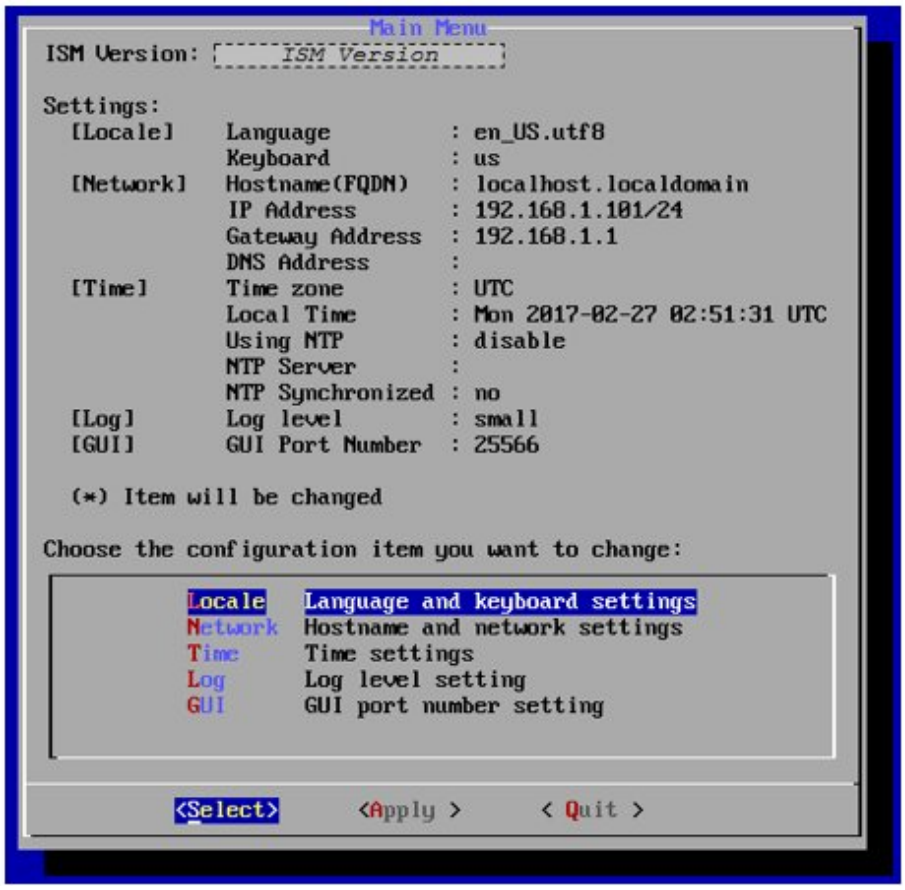
項目		設定/表示内容	対応するismadmコマンド
Locale	Language	内部言語設定	ismadm locale set-locale
	Keyboard	キーボードキーマップ設定	ismadm locale set-keymap
Network	Hostname(FQDN)	ホスト名設定	ismadm network modify
	IP Address	IPアドレス設定	
	Gateway Address	ゲートウェイ設定	
	DNS Address	DNSサーバ設定	
Time	Timezone	タイムゾーン設定	ismadm time set-timezone
	Local Time	ローカル時間表示	ismadm time show
	Using NTP	NTP有効・無効設定	ismadm set-ntp
	NTP Server	NTPサーバ設定	ismadm add-ntpserver ismadm del-ntpserver
	NTP Synchronized	NTP同期表示	ismadm time show
Log	Log level	障害調査ログサイズ設定	ismadm system change-log-level
GUI	GUI port number	Web GUI接続ポート設定	ismadm service modify -port

ISM-VA基本設定メニューの実行方法を以下に示します。

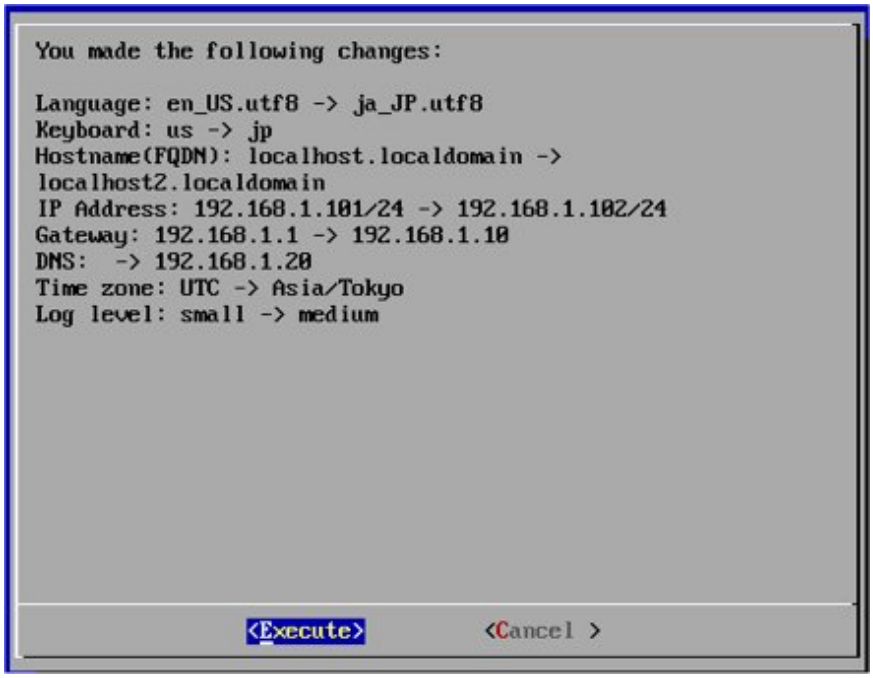
1. コンソールからadministratorでISM-VAにログインします。
2. ISM-VA基本設定メニューコマンドを実行します。

```
# ismsetup
```

以下の画面が表示されます。



3. 設定項目を選択し、設定値の入力または選択を行います。
4. 設定項目を入力後、[Apply]を選択します。
5. 変更内容を確認し、[Execute]を選択します。



変更処理終了後、変更結果が表示されます。

6. [Reboot ISM-VA]を選択してISM-VAを再起動し、変更を反映させます。

4.3 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。

4.4 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。

注意

ISM-VAをバックアップ/リストアする前に、ISM-VAを終了してください。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。

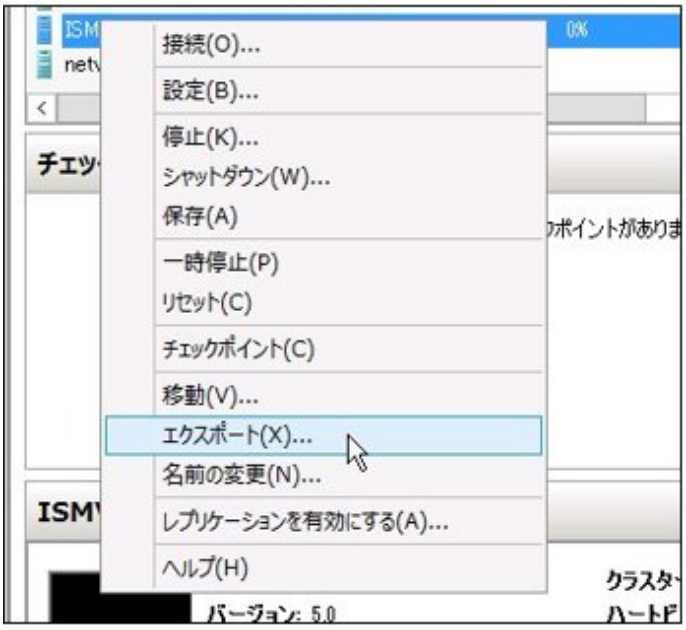
4.4.1 ISM-VAのバックアップ

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。

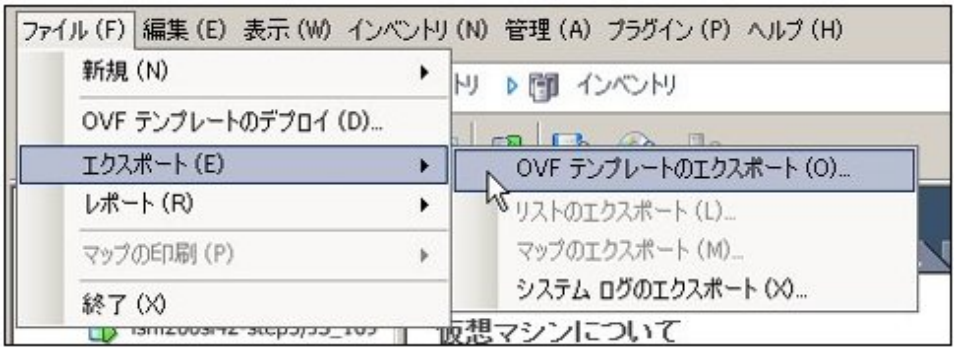
Microsoft Windows Server Hyper-Vで動作するISM-VAのバックアップ

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。



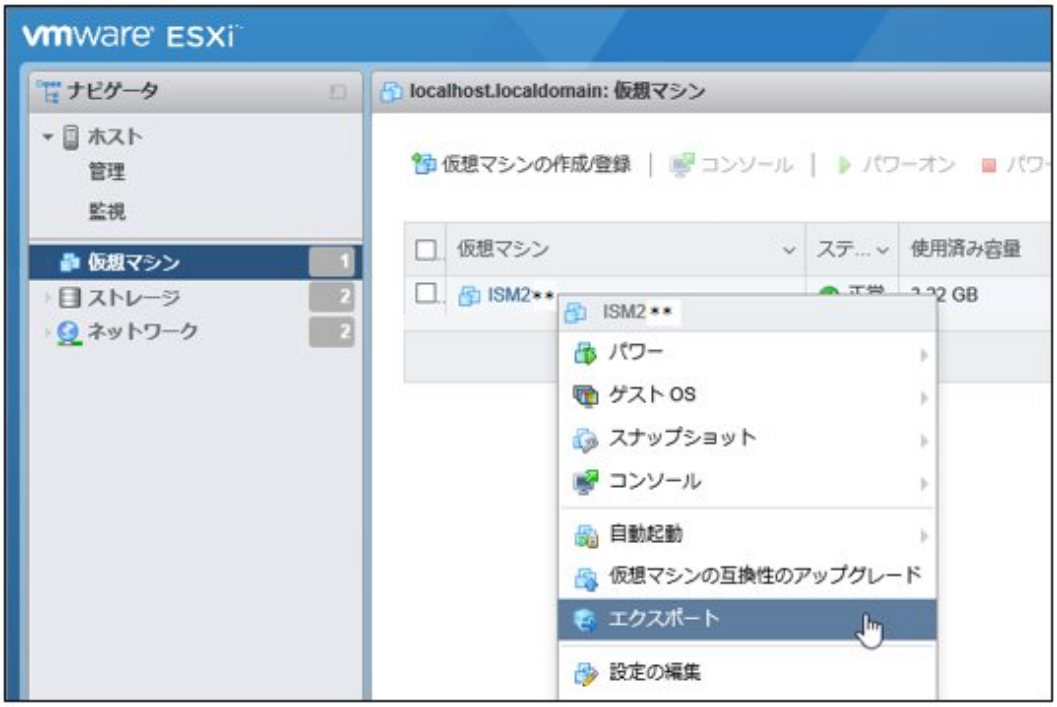
VMware vSphere Hypervisor 5.5またはVMware vSphere Hypervisor 6.0で動作するISM-VAのバックアップ

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。



VMware vSphere Hypervisor 6.5で動作するISM-VAのバックアップ

vSphere Client (HTML5)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。



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

4.4.2 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。

4.5 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。

注意

- 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 fd0, sector 0
```

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

   ー 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
```

   ー 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
```

ポイント

-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。

注意

- 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。
- 仮想リソース管理機能の保守資料としてvCenterからvc-supportログを採取します。詳細は、以下のURL(英語ページ)の「To collect ESX/ESXi and vCenter Server diagnostic data」の手順を参照してください。

  https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2032892

  上記URLに記載されたログ収集の手順6で、ログ収集対象のESXiホストとして、問題が発生しているVSANクラスタのESXiホストをすべて選択してください。

4.6 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。

4.6.1 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。

注意

- 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 -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/centos-root    16G  2.5G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  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-lv  10G   33M   10G    1% 'RepositoryRoot'/usrgrp1

  PV         VG          Fmt  Attr PSize  PFree
  /dev/sda2  centos      lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol  lvm2 a--  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。

```
# ismadm volume show -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/centos-root    16G  2.5G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  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/sdb1                                       (Free)

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g     0
  /dev/sdb1         lvm2 ---  10.00g 10.00g
```

7. ISM-VAを再起動します。

```
# ismadm power restart
```

4.6.2 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。

4.6.3 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。

```
# ismadm volume show -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/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  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-lv  10G   33M   10G    1% 'RepositoryRoot'/usrgrp1
tmpfs                     380M     0  380M    0% /run/user/0
/dev/sdc                                       (Free)

  PV         VG      Fmt  Attr PSize  PFree
  /dev/sda2  centos  lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol  lvm2 a--  10.00g    0
```

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 volume show -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/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  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/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 PSize  PFree
  /dev/sda2  centos  lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol lvm2 a--  10.00g    0
  /dev/sdc1  usrgrp1vol lvm2 a--   5.00g    0
```

7. ISM-VAを再起動します。

```
# ismadm power restart
```

4.7 証明書設定

4.7.1 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. ISM-VAを再起動します。

```
# ismadm power restart
```

ポイント

ローカルネットワーク内で使用する独自のホスト名に対応した独自SSLサーバ証明書は、opensslコマンドがインストールされたLinuxサーバ上で、以下のコマンドで作成できます。

```
# openssl genrsa -rand /proc/uptime 2048 > server.key
# openssl req -new -key server.key -x509 -sha256 -days 365 -set_serial $RANDOM -extensions v3_req -out server.crt
```

- 証明書のファイル名(server.key/server.crt)は任意のファイル名を指定。
- daysオプションは証明書の有効日数を指定
- ホスト名は、openssl reqコマンド実行後の「Common Name」入力時に指定。

4.7.2 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
```

4.7.3 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。

4.7.4 SSLサーバ自己署名証明書作成

ISM-VAで設定済みのIPアドレスまたはFQDNを元に、SSLサーバ自己署名証明書を作成します。

1. コンソールからadministratorでISM-VAにログインします。
2. SSLサーバ自己署名証明書作成コマンドを実行します。

   ー IPアドレスでSSLアクセスする場合

   ```
   # ismadm sslcert self-create -cnset ip
   ```

   ー FQDNでSSLアクセスする場合

   ```
   # ismadm sslcert self-create -cnset fqdn
   ```

3. ISM-VAを再起動します。

```
# ismadm power restart
```

4.7.5 CA証明書のダウンロード

SSLサーバ自己署名証明書を作成した場合、CA証明書を以下のURLからダウンロードできます。

https://＜ISM-VAのIPアドレス＞:25566/ca.crt

Internet ExplorerやGoogle Chromeを使用する場合、表示された内容に対して、[名前を付けて保存]を実施し、ファイル名を"ca.crt"に変更します。
保存時のファイルの種類は、ブラウザに応じて以下を選択してください。

- Internet Explorerの場合:[テキスト ファイル(*.txt)]
- Google Chromeの場合:[すべてのファイル]

実行例)curlコマンドがインストールされたLinuxサーバ上でダウンロードする場合

```
# curl -Ok https://192.168.10.20:25566/ca.crt
```

4.8 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。

   ー ライセンス登録

   ```
   # ismadm license set -key ＜ライセンスキー＞
   ```

   ー ライセンス一覧表示

   ```
   # ismadm license show
   ```

   ー ライセンス削除

   ```
   # ismadm license delete -key ＜ライセンスキー＞
   ```

注意

ライセンスの登録/削除後は、ISM-VAの再起動が必要です。

ポイント

ライセンスの登録/表示は、ISMのGUIでグローバルナビゲーションメニューの[設定]-[全般]-[ライセンス]からも行えます。

4.9 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。

   ー ネットワークデバイス表示

   ```
   # ismadm network device
   ```

   ー 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 DNSサーバ追加

   ```
   # ismadm network modify ＜LANデバイス名＞ +ipv4.dns ＜DNSサーバ＞
   ```

   実行例）

   ```
   # ismadm network modify eth0 +ipv4.dns 192.168.1.2
   ```

   ー DNSサーバ削除

   ```
   # ismadm network modify ＜LANデバイス名＞ -ipv4.dns ＜DNSサーバ＞
   ```

   実行例）

   ```
   # ismadm network modify eth0 -ipv4.dns 192.168.1.2
   ```

   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
   ```

ポイント

ネットワーク設定は、「4.2 ISM-VA基本設定メニュー」で行うこともできます。

4.10 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。

4.10.1 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
```

4.10.2 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
```

4.10.3 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
```

4.10.4 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
```

4.10.5 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＞
```

4.10.6 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＞
```

4.11 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。

   ー ISM-VA再起動

   ```
   ismadm power restart
   ```

   ー ISM-VA停止

   ```
   ismadm power stop
   ```

   ー 内部サービス一覧表示

   ```
   ismadm service show
   ```

   ー 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
   ```

   ー 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
   ```

   ー 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
   ```

   ー 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
   ```

   ー 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
   ```

   ー 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
```

4.12 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     : <Version>
GUI Port Number : 25566
Hostname        : localhost
Log Level       : small
```

＜Version＞部分は、ISM-VAの版数が表示されます。

4.13 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]:
```

注意

- 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、「4.7 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。

ポイント

ホスト名変更は、「4.2 ISM-VA基本設定メニュー」で行うこともできます。

4.14 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。

   修正ファイルはバイナリモードで転送してください。
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
```

4.15 プラグイン操作

ISM-VAにプラグインの適用、削除および、適用しているプラグインの表示を行うことができます。

4.15.1 プラグイン適用

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。

   プラグインファイルはバイナリモードで転送してください。

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）

```
# ismadm system plugin-add -file /Administrator/ftp/FJSVsvism-ext-1.0.0-10.tar.gz
```

5. プラグイン適用後、ISM-VAを再起動します。

```
# ismadm power restart
```

4.15.2 プラグイン表示

適用されているプラグインの版数を表示します。

```
# ismadm system plugin-show
  FJSVsvism-ext 1.0.0
```

「プラグイン名 版数」の形式で表示されます。

ポイント

「4.12 システム情報の表示」の「ismadm system show」コマンドでもプラグインの情報が表示されます。

```
# ismadm system show
ISM Version     : ＜Version＞
GUI Port Number : 25566
Hostname        : localhost
```

```
Log Level       : small
Plugin          : FJSVsvism-ext 1.0.0
```

＜Version＞部分は、ISM-VAの版数が表示されます。

Pluginには、適用されているプラグイン名と版数が表示されます。

4.15.3 プラグイン削除

適用したプラグインをアンインストールします。

1. プラグイン削除コマンドを実行します。

   ```
   # ismadm system plugin-del -name ＜プラグイン名＞
   ```

   プラグイン名は、「4.15.2 プラグイン表示」で記述されているコマンドの出力で表示されます。

   実行例）

   ```
   # ismadm system plugin-del -name FJSVsvism-ext
   Uninstall plugin <FJSVsvism-ext 1.0.0> ?
   [y/n]:
   ```

   コマンド実行後に、プラグインのアンインストールの確認画面が表示されます。

2. [y]を入力して、アンインストールを確定させます。
3. プラグイン削除後、ISM-VAを再起動します。

   ```
   # ismadm power restart
   ```

4.16 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。

   ー ログ出力有効化

   ```
   # ismadm system set-debug-flag 1
   ```

   ー ログ出力無効化

   ```
   # ismadm system set-debug-flag 0
   ```

4.17 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	管理対象ノード数
small（デフォルト）	10GB	100ノード
medium	40GB	400ノード
large	100GB	1000ノード

注意

- 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。

   ー mediumへの切替え

   ```
   # ismadm system change-log-level medium
   ```

   ー 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 system show
   ISM Version      : <Version>
   GUI Port Number : 25566
   Hostname         : localhost
   Log Level        : medium
   ```

   ＜Version＞部分は、ISM-VAの版数が表示されます。
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。

ポイント

障害調査ログレベル切替えは、「4.2 ISM-VA基本設定メニュー」で行うこともできます。

4.18 coreファイル採取ディレクトリの指定

調査資料としてcoreファイルが出力される際の採取・保管先のディレクトリを設定できます。未設定の場合は、ISM-VA内部のシステム領域のディレクトリが使用されます。

出力されたcoreファイルは、「4.5 保守資料の採取」の対象として採取されます。

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。

   ー 採取ディレクトリ表示

   ```
   ismadm system core-dir-show
   Core Directory: Default Internal Directory
   Store Size: 713596
   ```

   現在設定されているcoreファイル採取ディレクトリの場所と、使用されているディレクトリサイズが表示されます。

   採取ディレクトリの場所が未設定の場合は、「Default Internal Directory」と表示されます。

ー 採取ディレクトリ設定

```
ismadm system core-dir-set -dir <ディレクトリ>
```

ftpクライアントを使用して、事前に/Administrator/ftp/などの配下にディレクトリを作成し、そのディレクトリを指定してください。

例:

```
ismadm system core-dir-set -dir /Administrator/ftp/coredump/
```

注意

作成した採取ディレクトリは、coreファイル出力専用として使用し、ほかにファイルを配置しないでください。

ー 採取ディレクトリ解除

```
ismadm system core-dir-reset
```

採取ディレクトリを未設定状態に戻します。

4.19 ISM-VA内部のDHCPサーバ

ISM-VA内部のDHCPサービスを起動することで、ISM-VAをDHCPサーバとして使用できます。

DHCPサーバは、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。外部のDHCPサーバを使用することも、以下の手順で設定したISM-VAをDHCPサーバとして使用することも、どちらでも可能です。(その場合、「4.19.4 DHCPサーバの切替え」で示されている手順により、どちらのDHCPサーバを使用するかを指定します。)

外部のDHCPサーバのみを使用する場合は、以下の設定は不要です。

4.19.1 ISM-VA内部のDHCPサーバの設定

ISM-VA内部のDHCPサーバの設定をします。設定後、DHCPサービスを停止、起動することにより設定が反映されます。

注意

DHCPサーバの設定変更を行った場合は、DHCPサービスの停止と起動を行ってください。

サービスの停止、起動の方法は、「4.19.2 ISM-VA内部のDHCPサービスの操作」を参照してください。

DHCPサーバの設定には、2つの方法があります。運用に合わせてどちらかの方法で設定してください。

- ismadm dhcpsrv コマンドのパラメーター指定による設定

  ISM-VAのプロファイル適用に必要なDHCPサーバの設定を行います。

- confファイルによる設定

  ISM-VAのプロファイル適用で使用する設定に限らず、一般的なDHCPサーバの設定を行います。

ismadm dhcpsrv コマンドのパラメーター指定による設定

```
# ismadm dhcpsrv set-simple -subnet <サブネット>
                            -netmask <サブネットマスク>
                            -start <割当て開始アドレス>
                            -end <割当て終了アドレス>
                            -broadcast <ブロードキャストアドレス>
                            [-dns <DNSサーバのIPアドレス>]
                            [-gw <ゲートウェイのIPアドレス>]
```

コマンドは1行で入力してください。

以下のパラメーターは指定が必須です。指定を省略できません。

-subnet

-netmask

-start

-end

-broadcast

実行例）

```
# ismadm dhcpsrv set-simple -subnet 192.168.1.0 -netmask 255.255.255.0 -start 192.168.1.150 -end 192.168.1.160 -
broadcast 192.168.1.255 -dns 192.168.1.200 -gw 192.168.1.250

---------------- New Configuration ----------------
ddns-update-style none;
default-lease-time 86400;
max-lease-time 259200;

shared-network LOCAL-NET {
  subnet 192.168.1.0 netmask 255.255.255.0 {
     range 192.168.1.150 192.168.1.160;
     option subnet-mask 255.255.255.0;
     option broadcast-address 192.168.1.255;
     option vendor-class-identifier "PXEClient";
     option domain-name-servers 192.168.1.200;
     option routers 192.168.1.250;
          }
    }
-------------------------------------------------
Update DHCP configureation ? (Current settings are discarded)
[y/n]:
```

コマンド終了後に、設定した値を確認するメッセージが表示されるので、「y」を入力して設定を確定させてください。

confファイルによる設定

記述済みのconfファイルをISM-VAのftp機能でアップロードし、コマンドで取り込みます。

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。

```
# ismadm dhcpsrv set -file ＜confファイル＞
```

実行例）

```
# ismadm dhcpsrv set -file /Administrator/ftp/dhcpd.conf.new
```

4.19.2 ISM-VA内部のDHCPサービスの操作

ISM-VA内部のDHCPサービスの状態の表示、起動、停止を行います。

・ DHCPサービスの状態を確認

```
# ismadm service status dhcpd
```

コマンド出力

```
Active：active(running)  ：DHCPサービス起動状態
Active：inactive(dead)   ：DHCPサービス未起動状態
/usr/lib/systemd/system/dhcpd.service; enable;    ：ISM-VAブート時起動設定
/usr/lib/systemd/system/dhcpd.service; disabled;  ：ISM-VAブート時未起動設定
```

・ DHCPサービスの手動起動

```
# ismadm service start dhcpd
```

注意

- ISM-VA内部のDHCPサービスを起動する前に、DHCPサーバの設定を行ってください。

  DHCPサーバの設定方法は、「4.19.1 ISM-VA内部のDHCPサーバの設定」を参照してください。

- DHCPサーバが起動状態設定で「(dead)」状態になっている場合は、「4.19.3 ISM-VA内部のDHCPサーバ情報の確認」の「DHCPサーバメッセージ表示」でエラーが出ていないかどうか確認してください。

- DHCPサービスの手動停止

```
# ismadm service stop dhcpd
```

- ISM-VA起動時にDHCPサービスを起動するように設定

```
# ismadm service enable dhcpd
```

- ISM-VA起動時にDHCPサービスを起動しないように設定

```
# ismadm service disable dhcpd
```

4.19.3 ISM-VA内部のDHCPサーバ情報の確認

ISM-VA内部のDHCPサーバの情報を表示します。

現在設定されているDHCPサーバの内容の表示、DHCPサーバのメッセージの表示、現在の設定内容(confファイル)をftpアクセス可能な場所へエクスポート、サンプルconfファイルをftpアクセス可能な場所へエクスポートすることができます。

- 現在設定されているDHCPサーバの内容を表示

```
# ismadm dhcpsrv show-conf
```

- DHCPサーバのメッセージ表示

```
# ismadm dhcpsrv show-msg [-line]
```

オプションなしで実行した場合、20行表示します。

オプション[-line] を指定した場合、表示行数を指定できます。

実行例)

```
# ismadm dhcpsrv show-msg -line 50
```

- 現在の設定内容(confファイル)をftpアクセス可能な場所へエクスポート

```
# ismadm dhcpsrv export-conf -dir /Administrator/ftp
```

- 設定内容(confファイル)のサンプルをftpアクセス可能な場所へエクスポート

```
# ismadm dhcpsrv export-sample -dir /Administrator/ftp
```

4.19.4 DHCPサーバの切替え

プロファイル機能でDHCPサーバを使用する場合に、ISM-VA内部のDHCPサーバを使用するか、外部のDHCPサーバを使用するかを切り替えることができます。

- 現在の設定の表示

```
# ismadm dhcpsrv show-mode
```

コマンド出力

```
DHCP mode: local    : Profile機能はISM内部のDHCPサーバを使用します。
DHCP mode: remote   : Profile機能は外部のDHCPサーバを使用します。
```

・ 設定の切替え

ー ISM-VA内部のDHCPサーバを使用してプロファイル適用を行うように設定

```
# ismadm dhcpsrv set-mode local
```

ー 外部のDHCPサーバを使用してプロファイル適用を行うように設定

```
# ismadm dhcpsrv set-mode remote
```

4.20 MIBファイル設定

任意のトラップ受信を可能にするMIBファイルを、ISM-VA内に取り込むことができます。

4.20.1 MIBファイル登録

1. FTPでMIBファイルを転送します。

   転送先:/Administrator/ftp/mibs

   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. MIBファイル登録コマンドを実行します。

```
# ismadm mib import
```

4.20.2 MIBファイル表示

ISM-VAに登録されたMIBファイルを表示できます。

```
# ismadm mib show
```

4.20.3 MIBファイル削除

ISM-VAに登録されたMIBファイルを削除できます。

```
# ismadm mib delete -file <MIBファイル名>
```

4.21 ISM-VAのアップグレード

ISM-VAをアップグレードできます。

1. FTPでアップグレードファイルを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. アップグレードのため、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. アップグレードコマンドを実行します。

   アップグレードファイルを指定してコマンドを実行してください。

```
# ismadm system upgrade -file <アップグレードファイル>
```

実行例）

```
# ismadm system upgrade -file /Administrator/ftp/ISM220_S2017xxxx-01.tar.gz
```

5. アップグレード後、ISM-VAを再起動します。

```
# ismadm power restart
```

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。

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
- 手動ノード情報取得
- 手動ノードログ収集

メンテナンスモード設定手順

1. ノードの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]を選択します。

メンテナンスモード解除手順

1. ノードの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。

注意

- PRIMEQUESTをメンテナンスモード設定/解除すると、配下のパーティションおよび拡張パーティションもメンテナンスモード設定/解除されます。パーティションおよび拡張パーティションを指定してメンテナンスモード設定/解除することはできません。
- Brocade VCS Fabricをメンテナンスモード設定/解除すると、配下のVDXファブリックスイッチもメンテナンスモード設定/解除されます。VDXファブリックスイッチを指定してメンテナンスモード設定/解除することはできません。

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。

[イベント]-[イベント]-[運用ログ]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 5.5、またはVMware vSphere Hypervisor 6.0からのアンインストール
- VMware vSphere Hypervisor 6.5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

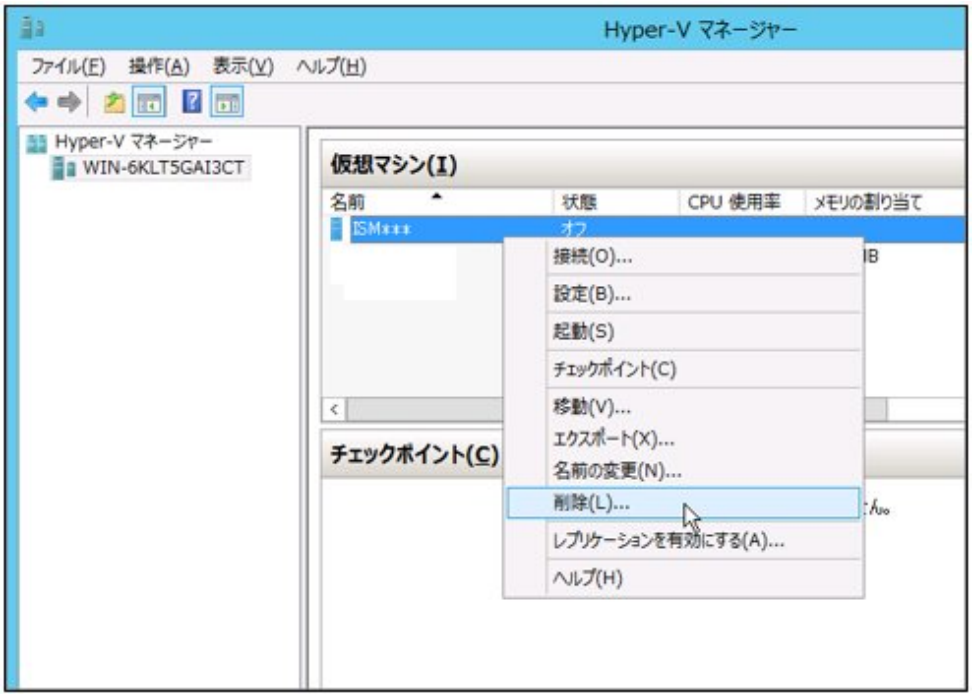
1. ISM-VAを停止します。

   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。



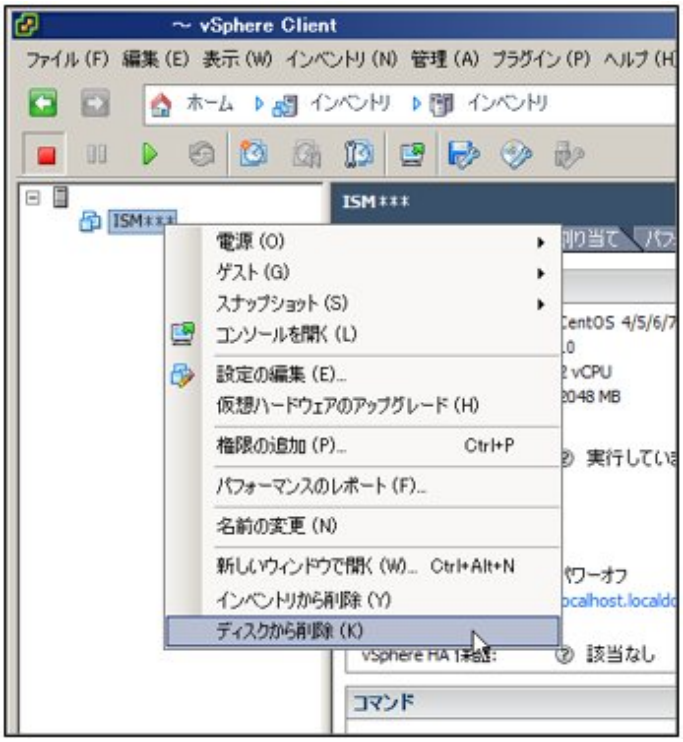
4. 手順2で記録した仮想ハードディスクを、エクスプローラーで削除します。

VMware vSphere Hypervisor 5.5、またはVMware vSphere Hypervisor 6.0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。

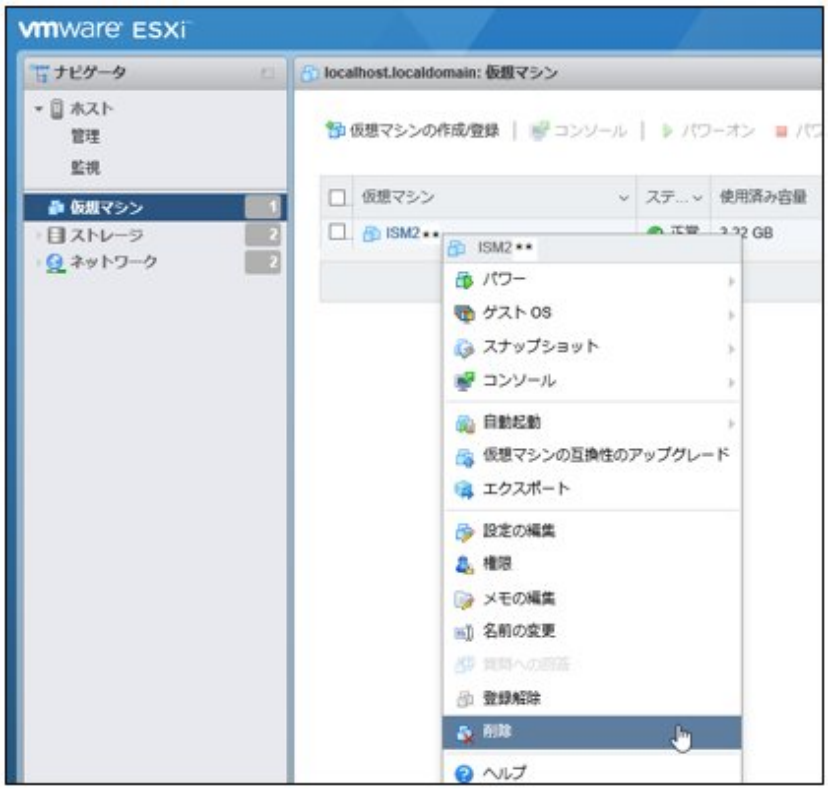


VMware vSphere Hypervisor 6.5からのアンインストール

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（HTML5）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。



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。

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。

現象：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：IPアドレスの編集を行ってノード登録を行った場合、登録時に「手動検出したノードの登録に失敗しました。IPアドレスが変更できません。指定されたIPアドレスは既に存在します。」のエラーが表示される。

原因・対処

IPアドレスの編集を行ってノード登録を行う場合、変更後のIPアドレスにpingを行い、応答がないことを確認してから実施してください。

iRMC S3世代のPRIMERGYは、IPアドレス変更後の数分間、変更前と変更後の両方のIPアドレスに対してpingが成功する場合があります。

現象：正常に使用できていたISMでGUIへのログインに「セッションタイムアウト」で失敗し、ISM-VAを再起動しても現象が変わらない。
ハイパーバイザのコンソール画面には、以下のようなメッセージが出力されている。

```
[55490.269659] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.272852] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.275983] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 00 7a 2e fc  BMAP.........z..
[55490.277488] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00  .............. .
[55490.278907] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00  .............. .
[55490.280367] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00  .......0........
[55490.281844] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.284837] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.286288] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 00 7a 2e fc  BMAP.........z..
[55490.287727] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00  .............. .
[55490.289073] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00  .............. .
[55490.290441] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00  .......0........
[55490.291716] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.294744] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.296176] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 00 7a 2e fc  BMAP.........z..
[55490.297620] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00  .............. .
[55490.299035] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00  .............. .
[55490.300401] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00  .......0........
[55490.301766] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
```

原因・対処

- ISM-VAの仮想ディスクが破損しているためISMが正常に動作していません。

  仮想ディスクの破損は、物理的なハードの異常や、ISM-VAを動作させているサーバまたはISM-VAが強制的に停止された場合に起こることがあります。

- バックアップ済みのISM-VAがある場合は、バックアップ済みのISM-VAをリストアして使用してください。
  バックアップしていない場合は、新規にインストールしてください。

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。

- [構築]-[プロファイル]-[アクション]-[インポート]-[選択]ボタン

- [構築]-[ファームウェア]-画面左側のメニューから[インポート]を選択し、[ファームウェア]-[インポートデータリスト]-[アクション]-[DVDインポート]-[選択]ボタン
- [構築]-[ファームウェア]-画面左側のメニューから[インポート]を選択し、[ファームウェア]-[インポートデータリスト]-[アクション]-[ファームウェアインポート]-[選択]ボタン
- [構築]-[ファームウェア]-画面左側のメニューから[インポート]を選択し、[SeverView Suite]タブ-[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]ボタンを選択し、[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。

現象：Microsoft Active DirectoryをLDAPサーバ設定で登録すると失敗する。

原因・対処

大量のユーザー情報（例えば1000件以上）を登録しているActive Directoryを登録する場合、Active Directoryの「MaxPageSize」という環境変数が、登録ユーザー情報数に応じた値になっているか確認してください。

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Onlineアップデートに失敗する。

原因・対処

Onlineアップデートの場合、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。

ファームウェアがサーバのOSに対応していない場合は、Offlineアップデートを使用してください。

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/AF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。

ファームウェアデータ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。

現象:Offlineアップデートが失敗する。

原因・対処

- Offlineアップデートを使用するには、ServerView Suite DVDおよびServerView Suite Update DVDがインポートされている必要があります。ServerView Suite DVDおよびServerView Suite Update DVDがインポートされているか確認してください。
- 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またはLANカードとISM-VAが接続されているか、など

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またはLANカードと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。

現象：ネットワークマップに仮想スイッチ、仮想マシンの接続関係が表示されない、または表示内容に誤りがある。

原因・対処

仮想スイッチ、仮想マシンの接続関係を表示するためには、管理対象ノードを管理している仮想化管理ソフトウェア、および管理対象ノードのOS情報をISMに登録しておく必要があります。

仮想化管理ソフトウェア情報、および管理対象ノードのOS情報が正しく登録されているかを確認してください。

現象：VLAN設定の変更に失敗する。

原因・対処

- 設定対象のネットワークスイッチがISMからアクセス可能である必要があります。ネットワークスイッチが正常に動作し、ISMからアクセス可能になっていることを確認してください。
- ネットワークスイッチの機種によっては予約済みのVLAN IDがあります。変更するVLAN IDが設定対象のネットワークスイッチの予約済みVLAN IDでないことを確認してください。

現象：リンクアグリゲーション設定の変更に失敗する。

原因・対処

- 設定対象のネットワークスイッチがISMからアクセス可能である必要があります。ネットワークスイッチが正常に動作し、ISMからアクセス可能になっていることを確認してください。
- ネットワークスイッチの機種によって設定可能なLAG名や動作モードが異なります。LAG名や動作モードについて設定可能であることを装置仕様で確認してください。

ログ管理機能

現象：ノードのログが収集されない、ノードのログ収集に失敗する。

原因・対処

- 通信状態などによる影響でログ収集に失敗した場合、時間をおいて再度実行してください。

- 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。
- ノードの詳細画面の[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。
- ログファイルの総容量がユーザーグループ設定に設定された上限（サイズ制限）設定値を超えると、新たなログは保管されません。グローバルナビゲーションメニューの[イベント]-[イベント]の[運用ログ]タブを確認し、ログ収集のタイミングで以下のどれか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。
  - 「ノード(<ノード名>)のログ収集中に、ユーザーグループ(<ユーザーグループ名>)の保管ログ保存領域が設定容量(xxMB)に達しました。」
  - 「ノード(<ノード名>)のログ収集中に、ユーザーグループ(<ユーザーグループ名>)のノードログ(ダウンロード用データ)保存領域が設定容量(xxMB)に達しました。」
  - 「ノード(<ノード名>)のログ収集中に、ノードログ（ログ検索用データ）保存領域が設定容量(xxMB)に達しました。」

現象：ノードの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：ノードのログ収集で、「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。

付録C　プロファイル設定項目

C.1 PRIMERGY・PRIMEQUEST3000Bサーバ用プロファイルのBIOS/iRMC設定項目

プロファイル中のBIOS/iRMCタブで設定可能な項目を記載します。サーバ種類に応じて一部設定できない項目や設定内容が異なる項目があります。対象サーバがサポートしている範囲で設定してください。

プロファイル内の設定項目は、個別に有効／無効を選択できます。無効にした場合、プロファイルを適用しても、無効に設定した項目は変更されません。

プロファイルと実際の機種の設定項目が異なる場合があります。各項目の詳細は、対象サーバのマニュアルを参照し、プロファイルの該当する設定項目に対して設定してください。

BIOSタブ

項目名	説明	設定値
CPU Configuration		
Execute Disable Bit （Enabled / Disabled）	CPUのExecute Disable Bit動作を指定します。本機能は、マニュアルによって、「XD（eXecute Disable）ビット」、または「NX（NoeXecute）ビット」として説明されている場合があります。	Enabled＝機能を使用可能にする Disabled＝機能を無効にする
Hyper-Threading （Enabled / Disabled）	CPUのHyper Threading Technology動作を指定します。 本機能を持たないCPUを搭載している場合、本設定は無視されます。	Enabled＝機能を使用可能にする Disabled＝機能を無効にする
Intel Virtualization Technology （Enabled / Disabled）	CPUの仮想化支援機能の動作を指定します。	Enabled＝機能を有効にする Disabled＝機能を無効にする
Intel (R) VT-d （Enabled / Disabled）	CPUのVirtualization Technology for Directed I/O機能動作を指定します。	Enabled＝機能を有効にする Disabled＝機能を無効にする
Power Technology （Energy Efficient / Customize / Disabled）	CPUの電源管理動作を設定します。	Energy Efficient＝省電力に最適化された動作をする Custom＝追加設定項目により詳細動作を設定する Disabled＝電源管理機能を無効にする
Enhanced SpeedStep （Enabled / Disabled）	Power TechnologyがCustomの場合のみ設定可能な項目です。 CPUのEIST（Enhanced Intel SpeedStep Technology）動作を指定します。	Enabled＝機能を有効にする Disabled＝機能を無効にする
Turbo Mode （Enabled / Disabled）	Enhanced SpeedStepがEnabledの場合のみ設定可能な項目です。 CPUのTurbo Boost Technology動作を指定します。 本機能を持たないCPUを搭載している場合、本設定に関わらず無効（Disabled）と設定されます。	Enabled＝機能を有効にする Disabled＝機能を無効にする
Memory Configuration		

項目名	説明	設定値
DDR Performance （Low-Voltage optimized / Energy optimized / Performance optimize）	メモリモジュールは異なる速度（周波数）で動作します。高速になるほどパフォーマンスが向上し、低速になるほど省電力になります。使用可能なメモリ速度は、取り付けられているメモリモジュールの構成に応じて異なります。	Low-Voltage optimized＝低電圧で可能な最も高速な設定 Energy optimized＝省電力で可能な最も低速な設定 Performance optimized＝最高のパフォーマンスを得るために可能な最も高速な設定
Numa （Enabled / Disabled）	NUMA(Non-Uniform Memory Access)機能の利用有無を指定します。 マルチプロセッサ構成ではない場合は意味を持ちません。 BX920、BX924、RX200、RX300、RX2520の場合、本設定は、BX920 S4、BX924 S4、RX200 S8、RX300 S8、RX2520 M1のBIOS 1.3.0、iRMCファーム7.19F以降が適用された装置でのみサポートされます。それ以外の装置では、本設定自体を無効化しておく必要があります。	Enabled=NUMA機能を有効にする Disabled=NUMA機能を無効にする
Onboard Device Configuration		
Onboard SAS/SATA (SCU) （Enabled / Disabled）	オンボードSAS/SATAストレージコントローラーユニット（SCU）の動作を指定します。	Enabled＝SCUを有効にする Disabled＝SCUを無効にする
SAS/SATA OpROM （Enabled / Disabled）	Onboard SAS/SATA（SCU）がEnabledの場合のみ設定可能な項目です。 SAS/SATAコントローラーのOption ROM動作を指定します。	Enabled＝Option ROMを有効にする Disabled＝Option ROMを無効にする
SAS/SATA Driver （LSI MegaRAID / Intel RSTe）	SAS/SATA OpROMがEnabledの場合のみ設定可能な項目です。 SAS/SATAコントローラーのOption ROMの種類を指定します。	LSI MegaRAID＝Embedded MegaRAID用Option ROMを使用する Intel RSTe＝Intel RSTe用Option ROMを使用する
Option ROM Configuration		
Launch Slot X OpROM （Enabled / Disabled）	各PCIスロットに搭載されたオプションカードの拡張ROM実行を指定します。 プロファイルでは多くのスロットに対して指定できますが、実機上に存在しないスロットに対しては設定しないでください。	Enabled＝拡張ROMを実行する Disabled＝拡張ROMを実行しない
CSM Configuration		
Launch CSM （Enabled / Disabled）	CSM（Compatibility Support Module）を実行するかどうかを指定します。 CSM がロードされている場合のみ、レガシーオペレーティングシステムを起動できます。	Enabled＝CSMを実行する Disabled＝CSMを実行しない
Boot Option Filter （UEFI and Legacy / UEFI only / Legacy only）	どちらのドライブからブートできるかを指定します。	UEFI and Legacy＝UEFI OSドライブおよびLegacy OSドライブからブート可能 UEFI only＝UEFI OSドライブからのみブート可能

項目名	説明	設定値
		Legacy only＝Legacy OS ドライブからのみブート可能
Launch Pxe OpRomPolicy （UEFI only / Legacy only / Do not launch）	起動する PXE Option ROM を指定します。 PXE ブートの場合は、使用可能な通常の（Legacy）PXE ブートおよび UEFI PXE ブートがあります。	UEFI only=UEFI Option ROM のみ起動する Legacy only=Legacy Option ROM のみ起動する Do not launch=Option ROM を起動しない
Launch Storage OpRomPolicy （UEFI only / Legacy only / Do not launch）	起動する Storage Option ROM を指定します。	UEFI only=UEFI Storage Option ROM のみ起動する Legacy only=Legacy Storage Option ROM のみ起動する Do not launch=Storage Option ROM を起動しない
Other PCI Device Rom Priority （UEFI only / Legacy only）	ネットワーク、マスストレージデバイス、ビデオ以外のデバイスで起動する Option ROM を指定します。	UEFI only＝UEFI Option ROM のみ起動する Legacy only＝Legacy Option ROM のみ起動する
Network Stack		
Network Stack （Enabled / Disabled）	UEFI Network Stack を UEFI でネットワークアクセスに使用できるかどうかを設定します。	Disabled＝UEFI ネットワークスタックの使用を許可しない Enabled＝UEFI ネットワークスタックの使用を許可する
IPv4 PXE Support （Enabled / Disabled）	IPv4 による PXE UEFI Boot を UEFI モードで使用できるかどうかを指定します。	Disabled＝IPv4 による PXE UEFI Boot の使用を許可しない Enabled＝IPv4 による PXE UEFI Boot の使用を許可する
IPv6 PXE Support （Enabled / Disabled）	IPv6 による PXE UEFI Boot を UEFI モードで使用できるかどうかを指定します。	Disabled＝IPv6 による PXE UEFI Boot の使用を許可しない Enabled＝IPv6 による PXE UEFI Boot の使用を許可する
Server Mgmt		
Sync RTC with MMB （PRIMERGY BXシリーズのみ）	Real Time Clockをマネジメントブレードと同期させるかどうかを指定します。	Disabled＝同期しない Enabled＝同期する
Adjust Date Time	プロファイル適用時に、サーバの時刻を管理サーバの時刻を基準にして変更します。 Sync RTC with MMBがDisabledの場合のみ設定できます。 **注意** 本項目はサーバのBIOSセットアップユーティリティの設定項目ではありません。 BIOS設定を変更するのではなく、対象サーバの時刻（RTC）をプロファイル適用時	Local Time＝管理サーバのタイムゾーン設定に応じた時刻を指定する UTC＝管理サーバのタイムゾーン設定からUTCに変換した時刻を指定する

項目名	説明	設定値
	に一度だけ変更する機能であり、すべてのPRIMERGY BXシリーズで使用可能です。	

iRMCタブ

項目名	説明	設定値
iRMC GUI		
デフォルト言語 （英語 / ドイツ語 / 日本語）	言語の初期設定を行います。 次回 iRMC Web インターフェースを呼び出す際に有効になります。	英語＝デフォルト言語を英語にする ドイツ語＝デフォルト言語をドイツ語にする 日本語＝デフォルト言語を日本語にする
電源制御		
POSTエラー時の動作 （起動継続 / 起動停止）	サーバ起動時にエラーが発生した場合の対応動作を設定します。	起動継続＝エラーが発生しても、起動処理を続ける 起動停止＝エラーが発生すると、キー入力があるまで起動を停止する
電源復旧時動作設定 （電源断前の状態に戻す / 電源投入しない / 電源投入する）	AC電源入力が切断されたあと、電源復旧した際の電源動作を設定します。	電源断前の状態に戻す＝電源切断発生時の状態を保持する（切断時にサーバが電源オン中だった場合は電源投入する。電源オフ中だった場合は電源投入しない） 電源投入しない＝常に電源オフになる 電源投入する＝常に電源オンになる
電力制御 （OSによるコントロール / 省電力動作）	サーバの省電力動作や静音動作に関する設定を行います。 **注意** BIOS設定で、Enhanced SpeedStepを無効に設定した場合、本制御も無効となります。	OSによるコントロール＝OSの制御に従う 省電力動作＝消費電力を抑えることを優先した動作となる （スケジュール）＝プロファイル管理では設定できない （電力制限）＝プロファイル管理では設定できない
ファンテスト		
ファン確認時刻	ファンテストを実行する場合に有効になります。	ファンテストの開始時刻を入力する。
ファンテスト無効化	定期的なファンの診断を行うかどうかを設定します。	（チェックあり）＝ファンテストを行わない （チェックなし）＝毎日指定した時刻にテストを行う
ソフトウェアウォッチドッグ		
ソフトウェアウォッチドッグ	ソフトウェアウォッチドッグで、OS動作中に定期的な通信チェックをするかどうかを指定します。 **注意** 設定はサーバ再起動後に有効となります。	（チェックあり）＝通信監視を行う （チェックなし）＝通信監視を行わない
動作	通信が行えない場合の動作を指定します。	プルダウンから以下を選択する。 継続稼働＝特に何も行わない リセット＝サーバの再起動を行う

項目名	説明	設定値
	注意 設定はサーバ再起動後に有効となります。	パワーサイクル＝一度サーバを電源オフにしたあと、電源オンを行う
タイムアウト時間	通信できないと判断する時間を指定します。 注意 設定はサーバ再起動後に有効となります。	1～100分までの数値を指定する。
Bootウォッチドッグ		
Bootウォッチドッグ	Bootウォッチドッグで、POST終了後からOS起動までの時間を監視するかどうかを指定します。 注意 設定はサーバ再起動後に有効となります。	(チェックあり)＝時間監視を行う (チェックなし)＝時間監視を行わない
動作	指定した時間内にOSが起動しない場合の動作を指定します。 注意 設定はサーバ再起動後に有効となります。	プルダウンから以下を選択する。 継続稼働＝特に何も行わない リセット＝サーバの再起動を行う パワーサイクル＝一度サーバを電源オフにしたあと、電源オンを行う
タイムアウト時間	OSが起動しないと判断する時間を指定します。 注意 設定はサーバ再起動後に有効となります。	1～100分までの数値を指定する。
時刻		
タイムモード (システムRTC / NTPサーバ)	iRMC の時刻設定を管理対象サーバから取得する、またはNTPサーバから取得するかどうかを指定します。	System RTC＝管理対象サーバのシステムクロックからiRMCの時刻を取得する NTP Server＝ネットワークタイムプロトコル(NTP)を使用して独自の時刻を参照時刻ソースとして動作する NTP サーバとiRMCの時刻を同期する
RTCモード (ローカルタイム / UTC)	iRMC の時刻を UTC(協定世界時)形式で表示する、またはローカルタイム形式で表示するかを選択できます。	ローカルタイム＝iRMCの時刻をローカルタイム形式で表示する UTC＝iRMC の時刻を UTC(協定世界時)形式で表示する
NTPサーバ 0	プライマリー NTP サーバの IP アドレスまたは DNS 名を指定します。	IPアドレスまたはDNS文字列を入力する。
NTPサーバ 1	セカンダリ NTP サーバの IP アドレスまたは DNS 名を指定します。	IPアドレスまたはDNS文字列を入力する。
タイムゾーン	サーバのある場所に対応するタイムゾーンを設定できます。	プルダウンから選択する。
ポート番号とネットワークサービス設定		

項目名	説明	設定値
Telnet 有効	Telnet接続を有効にするかどうかを指定します。	(チェックあり)＝Telnet接続を有効にする (チェックなし)＝Telnet接続を無効にする
Telnet ポート (初期値: 3172)	iRMCのTelnetポート番号を指定します。	ポート番号を入力する。 初期値は3172
SSH 有効	ssh接続を有効にするかどうかを指定します。	(チェックあり)＝ssh接続を有効にする (チェックなし)＝ssh接続を無効にする
SSH ポート (初期値: 22)	sshのTelnetポート番号を指定します。	ポート番号を入力する。 初期値は22
SNMP 一般設定		
SNMP 有効	SNMPを有効にするかどうかを指定します。 **注意** iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	有効＝SNMPを有効にする 無効＝SNMPを無効にする
SNMPポート(初期値: 161)	SNMP サービスが待機しているポートを指定します。 **注意** iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	ポート番号を入力する。 初期値は UDP 161
SNMPサービスプロトコル (全て(SNMPv1/v2c/v3) / SNMPv3のみ)	SNMPサービスプロトコルを指定します。 **注意** iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	全て(SNMPv1/v2c/v3)＝全プロトコルサポート (SNMPv1/v2c/v3) SNMPv3のみ＝SNMPv3のみサポート
SNMPv1/v2cコミュニティー名	SNMP v1/v2c の場合のコミュニティー文字列を指定します。 **注意** iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定	

項目名	説明	設定値
	項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	
SNMPv3 ユーザー設定		
SNMPv3 有効 （有効 / 無効）	ユーザーに対して SNMPv3 サポートを有効にするかどうかを指定します。 **注意** ・ SNMPv3ユーザーを作成/変更するには、[ネットワーク設定] -> [SNMP]でSNMPを有効にする必要があります。 ・ SNMPv3を使用するには最低8文字のパスワードを設定する必要があります。 ・ iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	有効＝SNMPv3サポートを有効にする 無効＝SNMPv3サポートを無効にする
SNMPv3 アクセス権	ユーザーのアクセス権限を指定します。 **注意** ・ SNMPv3ユーザーを作成/変更するには、[ネットワーク設定] -> [SNMP]でSNMPを有効にする必要があります。 ・ SNMPv3を使用するには最低8文字のパスワードを設定する必要があります。 ・ iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	常に読み取りのみとなる。
認証 （SHA / MD5 / 無効）	SNMPv3 が認証に使用する認証プロトコルを選択します。 **注意** ・ SNMPv3ユーザーを作成/変更するには、[ネットワーク設定] -> [SNMP]でSNMPを有効にする必要があります。 ・ SNMPv3を使用するには最低8文字のパスワードを設定する必要があります。 ・ iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一	SHA＝SHAを使用する MD5＝MD5を使用する 無効＝認証を無効にする

項目名	説明	設定値
	部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	
暗号化 （DES / AES / 無効）	SNMPv3がSNMPv3トラフィックの暗号化に使用する暗号化プロトコルを指定します。 **注意** ・ SNMPv3ユーザーを作成/変更するには、[ネットワーク設定] -> [SNMP]でSNMPを有効にする必要があります。 ・ SNMPv3を使用するには最低8文字のパスワードを設定する必要があります。 ・ iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	DES＝DESを使用する AES＝AESを使用する 無効＝暗号化を無効にする
SNMPトラップ送信先		
SNMPトラップコミュニティー	SNMPトラップコミュニティーを指定します。	SNMPトラップコミュニティー文字列を入力する。
SNMPユーザー	SNMPv3トラップ送信先に定義済みのSNMPv3ユーザーを指定します。 **注意** iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	SNMPユーザー文字列を入力する。
送信先SNMPサーバ 1-7	「トラップ送信先」として設定するコミュニティーに属するサーバのDNS名またはIPアドレスを指定します。	SNMPサーバのIPアドレス、またはDNS文字列を入力する。
プロトコル	トラップの受信に使用するSNMPプロトコルバージョンを指定します。 **注意** iRMCのWebUI画面にない設定項目は設定できません。ファーム版数により、一部の設定項目はiRMCのWebUI画面に設定項目があっても設定できません。プロファイルの適用に失敗する場合は、設定項目を無効化してください。	プルダウンから以下を選択する。 SNMPv1、SNMPv2c、SNMPv3

C.2 PRIMEQUEST 2000・PRIMEQUEST 3000Eシリーズ パーティション用プロファイルのMMB設定項目

プロファイル中のMMBタブで設定可能な項目を記載します。

MMBタブ

項目名	説明	設定値
Automatic Server Restart		
対象とする	ASR (Automatic Server Restart) を設定するかどうかを指定します。	(チェックあり)＝設定を行う (チェックなし)＝設定を行わない
Number of Restart Tries	ウォッチドッグやハードウェアエラーでOSがシャットダウンした場合に、OSをリスタートするリトライ回数を設定します。	再起動の有無の選択、および回数(1～10)を指定する。
Action after exceeding Restart tries	上記リトライ回数を超えた場合の動作を設定します。	電源OFF＝リブート処理を止め、パーティションの電源をOFFにする(Stop rebooting and Power off) 停止＝リブート処理を止め、パーティションを停止する(Stop rebooting) NMI割込み＝リブート処理を止め、パーティションに対してNMI割り込みを指示する(Diagnostic Interrupt assert)
Boot Watchdog		
対象とする	ブートウォッチドッグを設定するかどうかを指定します。	(チェックあり)＝設定を行う (チェックなし)＝設定を行わない
Boot Watchdog	ブートウォッチドッグの有効/無効化のことです。 OS起動までの時間を監視するかどうかを指定します。	(チェックあり)＝時間監視を行う (チェックなし)＝時間監視を行わない
Timeout time(seconds)	ここで指定した時間を超えてOSが起動しない場合に異常と判断されます。	1～6000秒までの数値を指定する。
Action when watchdog expires	指定した時間を超えてOSが起動しない場合の動作を指定します。	Continue(継続稼働)＝処理を継続する Reset(リセット)＝再起動を行う Power Cycle(パワーサイクル)＝一度電源OFFしたあと、電源ONを行う
Software Watchdog		
対象とする	ソフトウェアウォッチドッグを設定するかどうかを指定します。	(チェックあり)＝設定を行う (チェックなし)＝設定を行わない
Software Watchdog	ソフトウェアウォッチドッグの有効/無効化のことです。 OS動作中に定期的な通信チェックをするかどうかを指定します。	(チェックあり)＝通信チェックを行う (チェックなし)＝通信チェックを行わない
Timeout time(seconds)	ここで指定した時間を超えて通信ができない場合に異常と判断されます。	1～6000秒までの数値を指定する。

項目名	説明	設定値
Action when watchdog expires	指定した時間を超えて通信ができない場合の動作を指定します。	Continue(継続稼働)＝処理を継続する Reset(リセット)＝再起動を行う Power Cycle(パワーサイクル)＝一度電源OFFしたあと、電源ONを行う NMI＝NMIを発生させる

C.3 サーバ用プロファイルのOS設定項目

プロファイル中のOS/OS個別情報タブで設定可能な項目を記載します。省略可の記載がある項目はプロファイル上で設定をしなくてもOSのインストールは可能です。省略した場合は設定されないか、OSのデフォルトの設定が適用されます。

C.3.1 Windows Server用プロファイル

対象OSは以下のとおりです。

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

OSタブ

項目名	説明	設定値
インストール指定		
インストールのタイプ	OSをコアインストール、フルインストールのどちらでインストールするかを指定します。	画面から選択する。
インストールメディア	インストールに使用するメディアの種類を選択します。	プルダウンから選択する。 Microsoft社メディアを選択した場合は、さらにプロダクトキーの入力が必要。
ServerView Suite DVD （最新版数でインストール/版数を指定する）	インストールに使用するServerView Suite DVDの版数を指定します。	最新版数でインストール＝リポジトリに登録されている中で、最も新しいバージョンのServerView Suiteを使用する 版数を指定する＝指定した版数のServerView Suiteを使用する
管理LAN ネットワークポート設定		
ネットワークポート指定	管理LANに使用するネットワークのポートを指定します。	（チェックあり）＝管理LANのネットワークポートを指定する
指定方法	管理LANのネットワークポートの指定方法を選択します。[注1]	プルダウンから選択する。
ネットワークカード	指定方法で、「ポート番号」を指定した場合に設定します。 使用するネットワークカードの種類を選択します。	画面から選択する。 PCIカードを選択した場合には、PCIスロット番号を入力する。
ポート番号	指定方法で、「ポート番号」を指定した場合に入力します。	使用するポート番号を入力する。

項目名	説明	設定値
MACアドレス	指定方法で、「MACアドレス」を指定した場合に入力します。	使用するネットワークのMACアドレスを入力する。
ブートモード指定	ブートモードを指定します。	(チェックあり)＝ブート種別を指定する
ブート種別	サーバのブートモードを変更した場合、または明示的に指定する場合に選択します。	使用するブートの種別を画面から選択する。
RAIDとディスクの構成		
アレイコントローラーを使用する	サーバ内蔵のアレイコントローラーをOSインストール先として使用する場合に選択します。	(選択時)＝アレイコントローラーを使用する[注2]
既存アレイ構成を使用する	すでにアレイコントローラー上に作成済みのボリュームを使用します。	(選択時)＝既存のアレイ構成を使用する
アレイを新規に構築する	新しくアレイを構築し、その中にボリュームを作成して使用します。	(選択時)＝アレイを新規に構築する 加えて、アレイコントローラーの種類、RAIDレベル、RAIDに組み込むディスクの台数をプルダウンから選択する。
アレイコントローラーを使用しない	アレイコントローラー以外のドライブをOSインストール先として使用する場合に選択します。	(選択時)＝アレイコントローラー以外を使用する 加えて、使用するドライブの種類を画面から選択する。[注3]
ボリューム1		
ボリュームラベル	ボリューム名を指定します。	ボリューム名 文字列を入力する。[注4]
ファイルシステム	ファイルシステムの種類を選択します。	常にNTFSとなる。
パーティションサイズ(自動／指定)	パーティションのサイズを指定します。	自動＝自動的に適切なサイズでパーティションを作成する 指定＝入力したサイズでパーティションを作成する
クイックフォーマット	パーティションのフォーマット時にクイックフォーマットを利用するかどうかを指定します。	する＝クイックフォーマットを行う しない＝通常のフォーマットを行う (作業時間は長くなる)
利用形態	パーティションの用途を指定します。	常にBoot、OSとなる。
基本設定		
タイムゾーン	タイムゾーンを指定します。	プルダウンから選択する。
地域と言語	地域と言語を指定します。	プルダウンから選択する。
キーボード	キーボードの言語や種類を指定します。	プルダウンから選択する。
システム設定		
画面解像度 [px]	OSインストール直後の画面解像度を指定します。	プルダウンから選択する。[注5] 例: 600×480、800×600、1024×768、1280×1024
リフレッシュレート [Hz]	OSインストール直後のディスプレイのリフレッシュレートを指定します。	プルダウンから選択する。[注5]
画面の色数 [bit]	OSインストール直後の画面の表示色数をビット数で指定します。	プルダウンから選択する。[注5]
役割と機能の追加		
SNMPサービスのインストール	SNMPサービスをインストールするかどうかを指定します。	(チェックあり)＝SNMPサービスをインストールする

項目名	説明	設定値
SNMPトラップ設定	SNMPトラップ送信時のコミュニティー名とトラップ送信先を指定します。	追加ボタンを選択して任意の数の設定を行う。 【省略可】
コミュニティー名	SNMPトラップ送信時のコミュニティー名を指定します。	送信時のコミュニティー名文字列を入力する。
トラップ送信先	SNMPトラップの送信先を指定します。	送信先のIPアドレス文字列を入力する。
SNMPセキュリティサービス	受け付けるSNMPコミュニティー名とその権利を指定します。	追加ボタンを選択して任意の数の設定を行う。 【省略可】
受け付けるコミュニティー名	受け付けるSNMPコミュニティー名を指定します。	受け付けるコミュニティー名文字列を入力する。
コミュニティーの権利	受け付けるSNMPコミュニティーの権利を指定します。	プルダウンから選択する。 None＝なし Read Create＝読み取り、作成 Read Write＝読み取り、書き込み Read Only＝読み取りのみ Notify＝通知
認証トラップの送信	未知のホストまたはコミュニティーからのSNMP要求があった場合に認証トラップを送信するかどうかを指定します。	(チェックあり)＝認証トラップを送信する (チェックなし)＝認証トラップを送信しない
SNMPパケットの受付 (デフォルトのホストからSNMPパケットを受け付ける(LocalHost)/これらのホストからSNMPパケットを受け付ける)	LocalhostからのSNMPパケットを受け付けるかどうかを指定します。	(デフォルトのホストからSNMPパケットを受け付ける(LocalHost))＝Localhostからの SNMPパケットを受け付ける (これらのホストからSNMPパケットを受け付ける)＝次に指定したホスト名からの SNMPパケットを受け付ける。加えて、ホスト名を記載する
SNMP設定エージェント	連絡先と物理的な位置を入力する。	日本語を含む文字列が使用可能。 【省略可】
サービス	SNMPホストに関する情報を5つのオプションから指定します。	任意のサービスをチェックする。
リモートデスクトップ	リモートデスクトップの利用可否を指定します。	(チェックあり)＝リモートデスクトップを有効にする (チェックなし)＝リモートデスクトップを無効にする
リモートアシスタンス(インストールのタイプがフルの場合のみ)	リモートアシスタンスの利用可否を指定します。	許可する範囲を画面で指定する。 必要に応じて招待の有効時間も指定する。
ファイアーウォール設定	対象サーバをSCVMMへ登録する際に必要となるファイアーウォールの例外を作成します。 以下のアプリケーションからのアクセスが有効になります。 ・ Windows Management Instrumentation(WMI) ・ ファイルとプリンターの共有	(チェックあり)＝ファイアーウォール例外を作成する (チェックなし)＝ファイアーウォール例外を作成しない

項目名			説明	設定値
追加アプリケーション				
	Java Runtime Environment		Java Runtime Environmentをインストールするかどうかを指定します。 ServerView RAID Managerをインストールする場合には必ず指定してください。	(チェックあり)＝アプリケーションをインストールする[注6]
	ServerViewエージェント		ServerViewエージェントをインストールするかどうかを指定します。 SNMPサービスをインストールする場合に指定できます。	(チェックあり)＝アプリケーションをインストールする [注7]
	ServerViewアップデートエージェント		ServerViewアップデートエージェントをインストールするかどうかを指定します。 ServerViewエージェントをインストールする場合に指定できます。	(チェックあり)＝アプリケーションをインストールする [注7]
	DSNAP		DSNAPをインストールするかどうかを指定します。	(チェックあり)＝アプリケーションをインストールする [注8]
	ソフトウェアサポートガイド		ソフトウェアサポートガイドをインストールするかどうかを指定します。	(チェックあり)＝アプリケーションをインストールする [注8]
	ServerView RAID Manager		ServerView RAID Managerをインストールするかどうかを指定します。	(チェックあり)＝アプリケーションをインストールする
インストール後のスクリプト実行				
	インストール後のスクリプト実行		インストール後にスクリプトを実行するかどうかを指定します。	(チェックあり)＝インストール後にスクリプトを実行する
		OSに転送するディレクトリ	インストール後、OSに転送するディレクトリを指定します。	インストール後、OSに転送するディレクトリを指定する。
		実行するスクリプト	実行するスクリプトを指定します。[注9]	実行するスクリプトを指定する。

[注1]:CNAカードのUniversal Multi-Channel(UMC)機能が有効になっている場合は、ポート番号ではなく、MACアドレスを設定してください。

[注2]:アレイコントローラーを使用する場合、BIOSの「Onboard Device Configuration」設定と矛盾がないように設定してください。

[注3]:PRIMEQUEST 2000・PRIMEQUEST 3000Eシリーズでは、iSCSIに対応していません。対応状況は、サーバとServerView Suite DVDのマニュアルを参照してください。

[注4]:Windows Server 2016の場合、ボリューム名は半角の英数字・記号で設定してください。

[注5]:OSでサポートしていない値を設定した場合、デフォルト設定でインストールされます。

[注6]:「インストールのタイプ」設定でフルインストールを選択している場合のみインストール可能です。

[注7]:「地域と言語」設定で日本語を選択している場合は、アプリケーションが日本語でインストールされます。その他の場合は英語でインストールされます。

[注8]:「地域と言語」設定で日本語を選択している場合のみインストール可能です。

[注9]:Windowsの"cmd /c"コマンドにより、指定したスクリプトを実行します。

OS個別情報タブ

項目名	説明	設定値
インストールメディアタイプ	インストールに使用するメディアの種類を選択します。	常に[OS]タブで指定したインストールメディアとなる。
ユーザー名	ユーザーの名前を入力します。	ユーザー名の文字列を入力する。
組織	ユーザーが属する組織を入力します。	組織の文字列を入力する。

項目名	説明	設定値
コンピュータ名	ネットワーク上で識別するためのコンピュータ名を入力します。	コンピュータ名 文字列を入力する。
Administratorパスワード	パスワードを入力します。	パスワード文字列を入力する。
ワークグループ/ドメイン		
ワークグループ/ドメイン	ワークグループまたはドメインのどちらに参加するかを選択します。	ワークグループ＝ワークグループに参加する ドメイン＝ドメインに参加する [注1]
ワークグループ/ドメイン名	ワークグループまたはドメインの名前を指定します。	文字列を入力する。 [注2]
ドメインユーザー名	ドメインの場合、ドメインユーザー名を入力します。	文字列を入力する。
ドメインパスワード	ドメインの場合、パスワードを入力します。	文字列を入力する。
ネットワーク		
DHCP	管理LANのIPアドレスに関して固定IPアドレスを指定するか、DHCPを使用するかを選択します。	（チェックあり）＝DHCPを利用する （チェックなし）＝固定IPを指定する
IPアドレス	DHCPを利用しない場合、固定IPアドレスを指定します。	IPアドレスをIPv4形式で入力する。
サブネットマスク	DHCPを利用しない場合、サブネットマスクを指定します。	サブネットマスクをIPv4形式で入力する。
デフォルトゲートウェイ	DHCPを利用しない場合、ゲートウェイを指定します。	ゲートウェイのIPアドレスをIPv4形式で入力する。
DNSサーバ	DHCPを利用しない場合、DNSサーバのIPアドレスを指定します。	DNSサーバのIPアドレスをIPv4形式で入力する。
DNSドメイン名	DHCPを利用しない場合、ドメイン名を指定します。	ドメイン名 文字列を入力する。

[注1]:ドメインサーバに接続できない場合、ワークグループに設定されます。

[注2]:ワークグループ名は、15文字以下で設定してください。全角は2文字、半角は1文字としてカウントします。

C.3.2 VMware ESXi用プロファイル

対象OSは以下のとおりです。

- VMware ESXi 5.5 update3
- VMware ESXi 6.0 update1, update2, update3
- VMware ESXi 6.5 update1

OSタブ

項目名	説明	設定値
インストール設定		
インストールメディア	インストールに使用するメディアの種類を選択します。	プルダウンから選択する。

項目名	説明	設定値
ServerView Suite DVD （最新版数でインストール/版数を指定する）	インストールに使用するServerView Suite DVDの版数を指定します。	最新版数でインストール＝リポジトリに登録されている中で、最も新しいバージョンのServerView Suiteを使用する 版数を指定する＝指定した版数のServerView Suiteを使用する
管理LAN ネットワークポート設定		
ネットワークポート指定	管理LANに使用するネットワークのポートを指定します。	（チェックあり）＝管理LANのネットワークポートを指定する
指定方法	管理LANのネットワークポートの指定方法を選択します。[注1]	プルダウンから選択する。
ネットワークカード	指定方法で、「ポート番号」を指定した場合に設定します。 使用するネットワークカードの種類を選択します。	画面から選択する。 PCIカードを選択した場合には、PCIスロット番号を入力する。
ポート番号	指定方法で、「ポート番号」を指定した場合に入力します。	使用するポート番号を入力する。
MACアドレス	指定方法で、「MACアドレス」を指定した場合に入力します。	使用するネットワークのMACアドレスを入力する。
ブートモード指定	ブートモードを指定します。	（チェックあり）＝ブート種別を指定する
ブート種別	サーバのブートモードを変更した場合、または明示的に指定する場合に選択します。	使用するブートの種別を画面から選択する。
RAIDとディスクの構成		
アレイコントローラーを使用する	サーバ内蔵のアレイコントローラーをOSインストール先として使用する場合に選択します。	（選択時）＝アレイコントローラーを使用する[注2] [注3]
既存アレイ構成を使用する	すでにアレイコントローラー上に作成済みのボリュームを使用します。	（選択時）＝既存のアレイ構成を使用する
アレイを新規に構築する	新しくアレイを構築し、その中にボリュームを作成して使用します。	（選択時）＝アレイを新規に構築する 加えて、アレイコントローラーの種類、RAIDレベル、RAIDに組み込むディスクの台数をプルダウンから選択する。
アレイコントローラーを使用しない	アレイコントローラー以外のドライブをOSインストール先として使用する場合に選択します。	（選択時）＝アレイコントローラー以外を使用する 加えて、使用するドライブの種類を画面から選択する。[注4]
基本設定		
キーボード	キーボードの言語や種類を指定します。	プルダウンから選択する。
ネットワーク		
セットアップ	VM標準ネットワークでセットアップするかどうかを指定します。	（チェックあり）＝標準ネットワークを作成する
使用するVLAN ID	VLAN IDを入力します。VLANを使用しない場合は「0」を入力します。	VLAN IDを入力する。
仮想化管理ソフトへの登録		
仮想化管理ソフトへの登録	ESXiのインストールが完了したあと、続けてvCenterへ自動的に登録するかどうかを指定します。	（チェックあり）＝ 登録する （チェックなし）＝ 登録しない

項目名	説明	設定値
	自動登録を行う場合、[OS個別情報]タブで設定するIPアドレスは固定IPアドレスを設定してください。また、[OS]タブではVLAN IDに「0」を指定してください。	
登録先仮想化管理ソフト名	登録先のvCenterを指定します。	事前に[設定]-[全般]-左側ツリー部で[仮想化管理ソフトウェア]を選択し、画面に登録した登録先から選択する。
ホスト登録先のフォルダー名またはクラスタ名	登録先のフォルダー名またはクラスタ名を指定します。	登録先のフォルダー名またはクラスタ名を指定する。
インストール後のスクリプト実行		
インストール後のスクリプト実行	インストール後にスクリプトを実行するかどうかを指定します。	(チェックあり)＝インストール後にスクリプトを実行する
スクリプト格納ディレクトリ	インストール後に実行するスクリプトが格納されているディレクトリを指定します。	インストール後に実行するスクリプトが格納されているディレクトリを指定する。
実行するスクリプト	インストール後に実行するスクリプトを指定します。[注5]	インストール後に実行するスクリプトを指定する。

[注1]:CNAカードのUniversal Multi-Channel(UMC)機能が有効になっている場合は、ポート番号ではなく、MACアドレスを設定してください。

[注2]:アレイコントローラーを使用する場合、BIOSの「Onboard Device Configuration」設定と矛盾がないように設定してください。

[注3]:VMware ESXiでは、「オンボードSATAアレイコントローラー」は使用できません。

[注4]:PRIMEQUEST 2000・PRIMEQUEST 3000Eシリーズでは、iSCSIに対応していません。対応状況は、サーバとServerView Suite DVDのマニュアルを参照してください。

[注5]:ファイル中にプレーンテキスト形式でスクリプトを記述してください。自動インストール(kickStart)中の%post処理として実行されます。%firstboot --interpreter=busyboxの記述を行うと、%firstboot --interpreter=busybox処理として実行されます。

OS個別情報タブ

項目名	説明	設定値
ライセンス合意	VMware社のライセンスに合意するか選択します。 必ずチェックを付け、合意したことを示してください。	(チェックあり)＝ライセンスに合意する (チェックなし)＝ライセンスに合意しない
インストールメディアタイプ	インストールに使用するメディアの種類を選択します。	常にOSタブで指定したインストールメディアとなる。
Rootパスワード	パスワードを入力します。	パスワード文字列を入力する。
ネットワーク		
DHCP	管理LANのIPアドレスに関して固定IPアドレスを指定するか、DHCPを使用するかを選択します。	(チェックあり)＝DHCPを利用する (チェックなし)＝固定IPを指定する
IPアドレス	DHCPを利用しない場合、固定IPアドレスを指定します。	IPアドレスをIPv4形式で入力する。
サブネットマスク	DHCPを利用しない場合、サブネットマスクを指定します。	サブネットマスクをIPv4形式で入力する。
デフォルトゲートウェイ	DHCPを利用しない場合、ゲートウェイを指定します。	ゲートウェイのIPアドレスをIPv4形式で入力する。
DNSサーバ	DHCPを利用しない場合、DNSサーバをIPアドレスで指定します。	DNSサーバのIPアドレスをIPv4形式で入力する。

項目名	説明	設定値
コンピュータ名をDNSサーバから取得	DNSから取得したコンピュータ名を利用するかどうかを指定します。 DHCPを無効にした場合、チェックあり/なしを選択できます。	(チェックあり)＝DNSから取得する (チェックなし)＝任意のコンピュータ名を指定する
コンピュータ名	DNSからコンピュータ名(ホスト名)を取得しない場合に任意のコンピュータ名(ホスト名)を指定します。	ホスト名を入力する。

C.3.3 Red Hat Enterprise Linux用プロファイル

対象OSは以下のとおりです。

- Red Hat Enterprise Linux 6.6 (for x86)
- Red Hat Enterprise Linux 6.6 (for Intel64)
- Red Hat Enterprise Linux 6.7 (for x86)
- Red Hat Enterprise Linux 6.7 (for Intel64)
- Red Hat Enterprise Linux 6.8 (for x86)
- Red Hat Enterprise Linux 6.8 (for Intel64)
- Red Hat Enterprise Linux 6.9 (for x86)
- Red Hat Enterprise Linux 6.9 (for Intel64)
- Red Hat Enterprise Linux 7.1 (for Intel64)
- Red Hat Enterprise Linux 7.2 (for Intel64)
- Red Hat Enterprise Linux 7.3 (for Intel64)
- Red Hat Enterprise Linux 7.4 (for Intel64)

OSタブ

項目名	説明	設定値
インストール設定		
インストールメディア	インストールに使用するメディアの種類を選択します。	プルダウンから選択する。
ServerView Suite DVD (最新版数でインストール/版数を指定する)	インストールに使用するServerView Suite DVDの版数を指定します。	最新版数でインストール＝リポジトリに登録されている中で、最も新しいバージョンのServerView Suiteを使用する 版数を指定する＝指定した版数のServerView Suiteを使用する
管理LAN ネットワークポート設定		
ネットワークポート指定	管理LANに使用するネットワークのポートを指定します。	(チェックあり)＝管理LANのネットワークポートを指定する
指定方法	管理LANのネットワークポートの指定方法を選択します。[注1]	プルダウンから選択する。
ネットワークカード	指定方法で、「ポート番号」を指定した場合に設定します。 使用するネットワークカードの種類を選択します。	画面から選択する。 PCIカードを選択した場合には、PCIスロット番号を入力する。

項目名	説明	設定値
ポート番号	指定方法で、「ポート番号」を指定した場合に入力します。	使用するポート番号を入力する。
MACアドレス	指定方法で、「MACアドレス」を指定した場合に入力します。	使用するネットワークのMACアドレスを入力する。
ブートモード指定	ブートモードを指定します。	(チェックあり)＝ブート種別を指定する
ブート種別	サーバのブートモードを変更した場合、または明示的に指定する場合に選択します。	使用するブートの種別を画面から選択する。
基本設定		
地域と言語	言語を指定します。	プルダウンから選択する。
キーボード	キーボード種類を指定します。	プルダウンから選択する。
タイムゾーン	タイムゾーンを指定します。	プルダウンから選択する。
システムクロックでUTCを使用	システムクロックとして使用する時刻の種類を指定します。	(チェックあり)＝UTCを使用 (チェックなし)＝ローカルタイムを使用
RAIDとディスクの構成		
アレイコントローラーを使用する	サーバ内蔵のアレイコントローラーをOSインストール先として使用する場合に選択します。	(選択時)＝アレイコントローラーを使用する
既存アレイ構成を使用する	すでにアレイコントローラー上に作成済みのボリュームを使用します。	(選択時)＝既存のアレイ構成を使用する
アレイを新規に構築する	新しくアレイを構築し、その中にボリュームを作成して使用します。	(選択時)＝アレイを新規に構築する 加えて、アレイコントローラーの種類、RAIDレベル、RAIDに組み込むディスクの台数を画面から選択する。
アレイコントローラーを使用しない	アレイコントローラー以外のドライブをOSインストール先として使用する場合に選択します。	(選択時)＝アレイコントローラー以外を使用する 加えて、使用するドライブの種類を画面から選択する。[注2]
パーティション	下記の項目を「プロファイル」画面に表示された/boot、/varなどの各マウントポイントに対して指定します。	
(各マウントポイント左のチェックボックス)	マウントポイントに対して独立したパーティションを作成するかどうかを指定します。	(チェックあり)＝パーティションを作成する (チェックなし)＝パーティションを作成しない
ファイルシステムタイプ	ファイルシステムの種類を指定します。	プルダウンから選択する。 例 : ext2, ext3, ext4
サイズ	パーティションの容量を指定します。	数値を10進数で入力する。
最大許容量まで使用	余ったディスク容量を指定したパーティションに割り当てるかどうかを指定します。 Linuxインストール後に空き領域に別途パーティションを作成する場合は、本指定は行いません。	(チェックあり)＝指定のパーティションに余った容量を割り当てて容量を拡大 (チェックなし)＝指定した容量でパーティションを作成
パッケージ選択		
パッケージ選択の初期値	インストールするパッケージとして画面に表示されるパッケージグループと個別パッケージの初期選択を変更します。	最小＝必要最小限のパッケージ 全て＝すべてのパッケージ[注3] デフォルト＝推奨パッケージ[注3]

項目名			説明	設定値
	パッケージグループ		インストールするパッケージグループを指定します。	(チェックあり)＝インストールする (チェックなし)＝インストールしない
	個別パッケージ		インストールするパッケージ名を個別に指定します。	パッケージ名を文字列で入力する。 1行あたり1パッケージで複数行の記述が可能。
ブートローダーオプション				
	ブートローダをインストール		ブートローダをインストールするかどうかを設定します。	(チェックあり)＝ブートローダをインストールする 本項目は常にチェック状態となる。
	ブートローダのインストール場所		ブートローダのインストール先を指定します。	MBR＝マスタブートレコードにインストールする 本項目は常に「MBR」に設定される。
	カーネルパラメーター		カーネルパラメーターを指定します。	カーネルパラメーターとして指定する文字列を入力する。 【省略可】
Security-Enhanced Linux				
	SE Linux		SE Linuxの使用有無を指定します。	プルダウンで以下から選択する。 Enforcing, Disabled, Permissive
認証				
	シャドウパスワードの使用		シャドウパスワードを使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない[注4]
	MD5の使用		パスワード暗号化にMD5を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
	nscdの有効		Name Switch Cacheを使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
アプリケーション			OSインストール後に自動的にインストールするアプリケーションを指定します。	
	アプリケーション選択 (各種アプリケーション)		インストールするアプリケーションを指定します。 アプリケーションの種類はディストリビューションによって異なります。[注5]	(チェックあり)＝アプリケーションをインストールする
インストール後のスクリプト実行				
	インストール後のスクリプト実行		インストール後にスクリプトを実行するかどうかを指定します。	(チェックあり)＝インストール後にスクリプトを実行する
		OSに転送するディレクトリ	インストール後、OSに転送するディレクトリを指定します。	インストール後、OSに転送するディレクトリを指定する。
		実行するスクリプト	実行するスクリプトを指定します。[注6] [注7]	実行するスクリプトを指定する。

[注1]:CNAカードのUniversal Multi-Channel(UMC)機能が有効になっている場合は、ポート番号ではなく、MACアドレスを設定してください。

[注2]:PRIMEQUEST 2000・PRIMEQUEST 3000Eシリーズでは、iSCSIに対応していません。対応状況は、サーバとServerView Suite DVDのマニュアルを参照してください。

[注3]:ServerView Suite DVD V11.16.04以降を使用した場合、インストールされないパッケージグループがあります。その場合、手動でインストールしてください。

[注4]:「シャドウパスワード」は、プロファイル設定に関わらず常に有効になります。

[注5]:下表のアプリケーションはServerView Suite DVD V11.16.04、V12.16.10を使用した場合です。将来的にServerView Suite DVDの改版によって変更されることがあります。

凡例:○=ISMで指定可、×=ISMで指定不可

アプリケーション	RHEL 6.x(x86)	RHEL 6.x(Intel64)	RHEL 7.x
ServerView Agentless Service	×	○	○
ServerView SNMP Agents	○	○	○
ServerView CIM Providers	×	○	○
ServerView Update Agent (online flash)	○	○	○
ServerView Operations Manager (注:インストール時には、SELinuxをDisabledに設定)	○	○	○
ServerView RAID Manager	○	○	○
AIS Connect (注:ServerView Suite DVD V12.16.10以降では設定不可)	○	○	×
Java Runtime Environment	○	○	○
Dynamic Reconfiguration utility PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	○	○
PRIMEQUEST REMCS Option PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	○	○
HBA blockage function PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	○	○
SIRMSエージェント PRIMEQUEST 2000・PRIMEQUEST 3000E用	○	○	○
ServerView Mission Critical Option PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	○	○

[注6]:スクリプトから、ほかのスクリプトを実行する場合、実行権限を付与し、呼び出してください。

[注7]:shコマンドにより、指定したスクリプトを実行します。

OS個別情報タブ

項目名	説明	設定値
インストールメディアタイプ	インストールに使用するメディアの種類を選択します。	常にOSタブで指定したインストールメディアとなる。
Rootパスワード	パスワードを入力します。	パスワード文字列を入力する。
ネットワーク		
コンピュータ名をDNSサーバから取得	DNSから取得したコンピュータ名を利用するかどうかを指定します。	(チェックあり)=DNSから取得する (チェックなし)=任意のコンピュータ名を指定する
コンピュータ名	DNSからコンピュータ名(ホスト名)を取得しない場合に、任意のホスト名を指定します。	ホスト名を入力する。
DHCP	管理LANのIPアドレスに対して固定IPアドレスを指定するか、DHCPを使用するかを選択します。	(チェックあり)=DHCPを利用する (チェックなし)=固定IPを指定する
IPアドレス	DHCPを利用しない場合、固定IPアドレスを指定します。	IPアドレスをIPv4形式で入力する。

項目名	説明	設定値
サブネットマスク	DHCPを利用しない場合、サブネットマスクを指定します。	サブネットマスクをIPv4形式で入力する。
デフォルトゲートウェイ	DHCPを利用しない場合、デフォルトゲートウェイを指定します。	ゲートウェイのIPアドレスをIPv4形式で入力する。
DNSサーバ	DHCPを利用しない場合、DNSサーバをIPアドレスで指定します。	DNSサーバのIPアドレスをIPv4形式で指定する。

C.3.4 SUSE Linux Enterprise Server 用プロファイル

対象OSは以下のとおりです。

- SUSE Linux Enterprise Server 11 SP4 (for x86)
- SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel64)
- SUSE Linux Enterprise Server 12 (for AMD64 & Intel64)
- SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel64)
- SUSE Linux Enterprise Server 12 SP2 (for AMD64 & Intel64)
- SUSE Linux Enterprise Server 12 SP3 (for AMD64 & Intel64)

OSタブ

項目名	説明	設定値
インストール設定		
インストールメディア	インストールに使用するメディアの種類を選択します。	プルダウンから選択する。
ServerView Suite DVD （最新版数でインストール/版数を指定する）	インストールに使用するServerView Suite DVDの版数を指定します。	最新版数でインストール＝リポジトリに登録されている中で、最も新しいバージョンのServerView Suiteを使用する 版数を指定する＝指定した版数のServerView Suiteを使用する
管理LAN ネットワークポート設定		
ネットワークポート指定	管理LANに使用するネットワークのポートを指定します。	（チェックあり）＝管理LANのネットワークポートを指定する
指定方法	管理LANのネットワークポートの指定方法を選択します。[注1]	プルダウンから選択する。
ネットワークカード	指定方法で、「ポート番号」を指定した場合に設定します。 使用するネットワークカードの種類を選択します。	画面から選択する。 PCIカードを選択した場合には、PCIスロット番号を入力する。
ポート番号	指定方法で、「ポート番号」を指定した場合に入力します。	使用するポート番号を入力する。
MACアドレス	指定方法で、「MACアドレス」を指定した場合に入力します。	使用するネットワークのMACアドレスを入力する。
ブートモード指定	ブートモードを指定します。	（チェックあり）＝ブート種別を指定する
ブート種別	サーバのブートモードを変更した場合、または明示的に指定する場合に選択します。	使用するブートの種別を画面から選択する。
基本設定		

項目名	説明	設定値
地域と言語	言語を指定します。	プルダウンから選択する。
キーボード	キーボード種類を指定します。	プルダウンから選択する。
タイムゾーン	タイムゾーンを指定します。	プルダウンから選択する。
システムクロックでUTCを使用	システムクロックとして使用する時刻の種類を指定します。	(チェックあり)＝UTCを使用 (チェックなし)＝ローカルタイムを使用
RAIDとディスクの構成		
アレイコントローラーを使用する	サーバ内蔵のアレイコントローラーをOSインストール先として使用する場合に選択します。	(選択時)＝アレイコントローラーを使用する[注2]
既存アレイ構成を使用する	すでにアレイコントローラー上に作成済みのボリュームを使用します。	(選択時)＝既存のアレイ構成を使用する
アレイを新規に構築する	新しくアレイを構築し、その中にボリュームを作成して使用します。	(選択時)＝アレイを新規に構築する 加えて、アレイコントローラーの種類、RAIDレベル、RAIDに組み込むディスクの台数を画面から選択する。
アレイコントローラーを使用しない	アレイコントローラー以外のドライブをOSインストール先として使用する場合に選択します。	(選択時)＝アレイコントローラー以外を使用する 加えて、使用するドライブの種類を画面から選択する。[注3]
パーティション	下記の項目を「プロファイル」画面に表示された/boot、/varなどの各マウントポイントに対して指定します。	
(各マウントポイント左のチェックボックス)	マウントポイントに対して独立したパーティションを作成するかどうかを指定します。	(チェックあり)＝パーティションを作成する (チェックなし)＝パーティションを作成しない
ファイルシステムタイプ	ファイルシステムの種類を指定します。	プルダウンから選択する。 例 : ext2, ext3, ext4 [注4]
サイズ	パーティションの容量を指定します。	数値を10進数で入力する。
最大許容量まで使用	余ったディスク容量を指定したパーティションに割り当てるかどうかを指定します。 Linuxインストール後に空き領域に別途パーティションを作成する場合は、本指定は行いません。	(チェックあり)＝指定のパーティションに余った容量を割り当てて容量を拡大 (チェックなし)＝指定した容量でパーティションを作成
パッケージ選択		
パッケージ選択の初期値	インストールするパッケージとして画面に表示されるパッケージグループと個別パッケージの初期選択を変更します。	最小＝必要最小限のパッケージ 全て＝すべてのパッケージ デフォルト＝推奨パッケージ
パッケージグループ [注5]	インストールするパッケージグループを指定します。	(チェックあり)＝インストールする (チェックなし)＝インストールしない
個別パッケージ	インストールするパッケージ名を個別に指定します。	パッケージ名を文字列で入力する。 1行あたり1パッケージで複数行の記述が可能。
ブートローダーオプション		

項目名	説明	設定値
ブートローダをインストール	ブートローダをインストールするかどうかを設定します。	(チェックあり)＝ブートローダをインストールする 本項目は常にチェック状態となる。
ブートローダのインストール場所	ブートローダのインストール先を指定します。	MBR＝マスタブートレコードにインストールする 本項目は常に「MBR」に設定される。
カーネルパラメーター	カーネルパラメーターを指定します。	カーネルパラメーターとして指定する文字列を入力する。 【省略可】
Security-Enhanced Linux		
SE Linux	SE Linuxの使用有無を指定します。	本項は常に「Disabled」に設定される。
認証		
シャドウパスワードの使用	シャドウパスワードを使用するかどうかを指定します。	本項は常に「チェックあり(使用する)」に設定される。
MD5の使用	パスワード暗号化にMD5を使用するかどうかを指定します。	本項は常に「チェックなし(使用しない)」に設定される。
nscdの有効	Name Switch Cacheを使用するかどうかを指定します。	本項は常に「チェックあり(使用する)」に設定される。
アプリケーション	OSインストール後に自動的にインストールするアプリケーションを指定します。	
アプリケーション選択 (各種アプリケーション)	インストールするアプリケーションを指定します。 アプリケーションの種類はディストリビューションによって異なります。[注6]	(チェックあり)＝アプリケーションをインストールする
インストール後のスクリプト実行 [注7]		
インストール後のスクリプト実行	インストール後にスクリプトを実行するかどうかを指定します。	(チェックあり)＝インストール後にスクリプトを実行する
OSに転送するディレクトリ	インストール後、OSに転送するディレクトリを指定します。	インストール後、OSに転送するディレクトリを指定する。
実行するスクリプト	実行するスクリプトを指定します。[注8] [注9]	実行するスクリプトを指定する。

[注1]:CNAカードのUniversal Multi-Channel(UMC)機能が有効になっている場合は、ポート番号ではなく、MACアドレスを設定してください。

[注2]:アレイコントローラーを使用する場合、BIOSの「Onboard Device Configuration」設定と矛盾がないように設定してください。

[注3]:PRIMEQUEST 2000・PRIMEQUEST 3000Eシリーズでは、iSCSIに対応していません。対応状況は、サーバとServerView Suite DVDのマニュアルを参照してください。

[注4]:SLES 11 SP4では、ext4はReadのみ対応しています。SLES 12では、ext4がRead/Write両方可能ですが、SLESとして正式サポートの対象ではありません。

[注5]:SLES 12では、パッケージグループに「X Windows System」が指定されていない場合も、コンソールで起動しません。[Ctrl]+[Alt]+[F1]を押すと、コンソールからログインできます。

[注6]:下表のアプリケーションはServerView Suite DVD V11.16.04、V12.16.10を使用した場合です。将来的にServerView Suite DVDの改版によって変更される場合があります。

凡例:○＝ISMで指定可、×＝ISMで指定不可

アプリケーション(SLESの場合)	SLES 11 SP4(x86)	SLES 11 SP4(Intel64)	SLES 12系
ServerView Agentless Service	×	○	○

アプリケーション(SLESの場合)	SLES 11 SP4(x86)	SLES 11 SP4(Intel64)	SLES 12系
ServerView SNMP Agents	○	○	○
ServerView CIM Providers	×	×	×
ServerView Update Agent (online flash)	○	○	○
ServerView Operations Manager	×	×	×
ServerView RAID Manager	○	○	○
AIS Connect （注：ServerView Suite DVD V12.16.10以降では設定不可）	×	×	×
Java Runtime Environment	○	○	○
Dynamic Reconfiguration utility PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	×	○
PRIMEQUEST REMCS Option PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	×	×
HBA blockage function PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	×	×
SIRMSエージェント PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	×	×
ServerView Mission Critical Option PRIMEQUEST 2000・PRIMEQUEST 3000E用	×	×	×

[注7]：SLES 12では、インストール後のスクリプト実行に対応していません。

[注8]：スクリプトから、ほかのスクリプトを実行する場合、実行権限を付与し、呼び出してください。

[注9]：shコマンドにより、指定したスクリプトを実行します。

OS個別情報タブ

項目名	説明	設定値
インストールメディアタイプ	インストールに使用するメディアの種類を選択します。	常にOSタブで指定したインストールメディアとなる。
Rootパスワード	パスワードを入力します。	パスワード文字列を入力する。
ネットワーク		
コンピュータ名をDNSサーバから取得	DNSから取得したコンピュータ名を利用するかどうかを指定します。	（チェックあり）＝DNSから取得する （チェックなし）＝任意のコンピュータ名を指定する
コンピュータ名	DNSからコンピュータ名（ホスト名）を取得しない場合に、任意のホスト名を指定します。	ホスト名を入力する。
DHCP	管理LANのIPアドレスに対して固定IPアドレスを指定するか、DHCPを使用するかを選択します。	（チェックあり）＝DHCPを利用する （チェックなし）＝固定IPを指定する
IPアドレス	DHCPを利用しない場合、固定IPアドレスを指定します。	IPアドレスをIPv4形式で入力する。
サブネットマスク	DHCPを利用しない場合、サブネットマスクを指定します。	サブネットマスクをIPv4形式で入力する。
デフォルトゲートウェイ	DHCPを利用しない場合、デフォルトゲートウェイを指定します。	ゲートウェイのIPアドレスをIPv4形式で入力する。
DNSサーバ	DHCPを利用しない場合、DNSサーバをIPアドレスで指定します。	DNSサーバのIPアドレスをIPv4形式で指定する。

C.4 PRIMERGYサーバ用プロファイルの仮想IO設定項目

C.4.1 カード設定

使用したいカード数分設定します。

項目名	説明	設定値
オンボードカードスロット数	オンボード数を選択します。	プルダウンから選択する。
PCIカードスロット数	使用するカード数を選択します。	プルダウンから選択する。
カードスロット		
オンボードスロット		
カードタイプ	使用する種別を選択します。	画面から選択する。
ポート数	使用するポート数を選択します。	プルダウンから選択する。
PCIカード		
カードタイプ	使用する種別を選択します。	画面から選択する。
ポート数	使用するポート数を選択します。	プルダウンから選択する。

注意

- 仮想IOの設定は、サーバに搭載されているLAN、FC、CNA のカード/ボードすべてに仮想アドレスを割り当てて使用してください。一部のカード/ボードや一部のポートだけに仮想アドレスを割り当てるといった部分的な割当て運用はサポートしていません。
- 仮想IOの設定は、プロファイル編集で設定から除外したカード/ボード(カード/ボード数を0に設定したものを含む)は使用できない状態になります。基本的にOSから認識されなくなります(OSやドライバによっては認識表示される場合があります)。
- 仮想IOの設定はiRMCに保存されるため、iRMCの電源がオンの場合に有効です。iRMCの電力が喪失した場合、iRMCの仮想IOの設定もなくなります。再度仮想IOの設定を有効にするには、プロファイルを再適用してください。

C.4.2 ポート設定

「C.4.1 カード設定」で設定したカード数分の設定が必要です。

以下のカードごとの設定では、カードタイプ別の設定値について説明します。

項目名	説明	設定値
ポート情報		
仮想アドレスを使用する	仮想アドレスを使用する場合に選択します。	(チェックあり)＝仮想アドレスを使用する
SR-IOVを使用する	SR-IOVを使用する場合に選択します。	(チェックあり)＝SR-IOVを使用する
ブートメニュー非表示 (F12)	ブートメニューを非表示にする場合に選択します。	(チェックあり)＝ブートメニューを非表示にする
UEFIブートモード	使用するブートモードを選択します。	画面から選択する。
カードタイプがCNAの場合		
機能タイプ	CNAのFunctionを選択します。	プルダウンから選択する。
Boot	ブート方法を選択します。	プルダウンから選択する。
SR-IOV	SR-IOVを有効にする場合に選択します。	(チェックあり)＝SR-IOVを有効にする
カードタイプがLANの場合		
機能タイプ	LANのFunctionを選択します。	常にLANとなる。
Boot	ブート方法を選択します。	プルダウンから選択する。

項目名	説明	設定値
SR-IOV	SR-IOVを有効にする場合に選択します。	(チェックあり)＝SR-IOVを有効にする
カードタイプがFCの場合		
機能タイプ	FCのFunctionを選択します。	常にFCとなる。
Boot	ブート方法を設定します。	プルダウンから選択する。
SR-IOV	SR-IOVを有効にする場合に選択します。	(チェックあり)＝SR-IOVを有効にする

注意

ローカルディスク(SATA、またはSAS)へOSインストールを行う場合、仮想IOでBoot設定は利用できません。プロファイル適用前に手動でサーバのPXEブートが優先となるようにサーバのブート順を変更してください。

C.4.3 ブート設定

ブート優先順を変更する場合は、各項目の右側にある矢印ボタンを使用してください。

オンボードのポート数、およびPCIカード数・ポート数は、「C.4.1 カード設定」および「C.4.2 ポート設定」で設定した数分、設定してください。

以下では、オンボード・PCIカード問わず、機能タイプ別の設定値について説明します。

項目名	説明	設定値
機能タイプがLANの場合		
IPプロトコル	IPプロトコルについて選択します。	画面から選択する。
機能タイプがFCoEの場合		
接続速度	接続速度を選択します。	プルダウンから以下を選択する。 自動、1 Gbit/s、2 Gbit/s、4 Gbit/s、8 Gbit/s、16 Gbit/s
接続タイプ	接続形態を選択します。	画面から選択する。
第1ターゲット		
ポート名(WWPN)	SANブートで起動するストレージのWWPNを入力します。	WWPNを入力する。
LUN	SANブートで起動するストレージのLUNを入力します。	LUNを入力する。
第2ターゲット		
ポート名(WWPN)	SANブートで起動するストレージのWWPNを入力します。	WWPNを入力する。
LUN	SANブートで起動するストレージのLUNを入力します。	LUNを入力する。
機能タイプがiSCSIの場合		
イニシエータパラメーター		
アドレス設定	イニシエータのアドレス取得方法を選択します。	画面から選択する
イニシエータ名	イニシエータのIQNを入力します。	IQNを入力する。 入力する文字列は、先頭および、末尾が英数字、それ以外は、英数字および記号(ピリオド"."、コロン":"およびハイフン"-")で構成された223文字以内とする。

項目名	説明	設定値
VLAN ID	HBAが要求を送信するために使用されるVLAN IDを入力します。	VLAN IDを入力する。
IPv4	アドレス設定で「固定」を選択した場合、イニシエータで使用するIPアドレスを入力します。	IPアドレスを入力する。
サブネットマスク	アドレス設定で「固定」を選択した場合、サブネットマスクを入力します。	サブネットマスクを入力する。
ゲートウェイアドレス	アドレス設定で「固定」を選択した場合、ゲートウェイのアドレスを入力します。	ゲートウェイのアドレスを入力する。
ターゲットパラメーター		
IPアドレス	ターゲットのアドレス取得方法を選択します。	画面から選択する。
ターゲット名	ターゲットのIQNを入力します。	IQNを入力する。 入力する文字列は、先頭および、末尾が英数字、それ以外は、英数字および記号(ピリオド"."、コロン":"およびハイフン"-")で構成された223文字以内とする。
IPv4	IPアドレスで「固定」を選択した場合、ターゲットで使用するIPアドレスを入力します。	IPアドレスを入力する。
ポート(opt)	IPアドレスで「固定」を選択した場合、ターゲットのポート番号を入力します。	ポート番号を入力する。
LUN	IPアドレスで「固定」を選択した場合、ターゲットのLUN番号を入力します。	LUN番号を入力する。
認証方式	認証方式を選択します。	画面から選択する。
CHAPユーザー名	認証方式で、「CHAP」または「Mutual CHAP」を選択した場合、認証ユーザー名を入力します。	認証ユーザー名を入力する。 文字列は、半角英数字および記号で構成された127文字以内とする[注1]。
CHAPパスワード	認証方式で、「CHAP」または「Mutual CHAP」を選択した場合、CHAP認証に使用するパスワードを入力します。	パスワードを入力する。 文字列は、半角英数字および記号で構成された12以上16文字以内とする[注1]。
Mutual CHAPパスワード	認証方式で、「Mutual CHAP」を選択した場合、Mutual CHAP認証に使用するパスワードを入力します。	パスワードを入力する。 文字列は、半角英数字および記号で構成された12以上16文字以内とする[注1]。

[注1]:ハードウェアのモデルによっては記号が使用できない場合があります。半角英数字のみを使用することを推奨します。

C.4.4 CNA設定

「C.4.1 カード設定」でオンボードまたはPCIカードのカードタイプに、「CNA」を指定した場合に設定します。

「C.4.2 ポート設定」で設定した、CNAの機能タイプ数分設定します。

機能タイプ別の設定値について説明します。

項目名	説明	設定値
機能タイプがFCoEの場合		
最少帯域幅[%]	帯域幅の最小値を入力します。	帯域幅の最小値を入力する。[注1]
最大帯域幅[%]	帯域幅の最大値を入力します。	帯域幅の最大値を入力する。[注1]
機能タイプがLAN または iSCSIの場合		

項目名	説明	設定値
最少帯域幅[%]	帯域幅の最小値を入力します。	帯域幅の最小値を入力する。[注1]
最大帯域幅[%]	帯域幅の最大値を入力します。	帯域幅の最大値を入力する。[注1]
VLAN ID	VLAN IDを入力します。	VLAN IDを入力する。

[注1]:1つのIOチャネルのすべての合計が100になるように設定します。

1つのIOチャネルのすべての帯域幅の合計が100 でない場合、帯域幅の値はそれに応じて内部で調整されます。

C.4.5 仮想アドレス設定

「C.4.1 カード設定」で入力したカード情報数分設定します。

カードタイプ別の設定値について説明します。

項目名	説明	設定値
カードタイプがLANの場合		
仮想アドレス割り当て	仮想アドレス割り当てを行う場合に選択します。	(チェックあり)＝仮想アドレスを割り当てる
仮想アドレス[注1]		
自動割り当て	プール管理からの自動割り当てを有効にする場合に選択します。	(チェックあり)＝自動割り当てを有効にする
MAC[注2]	仮想MACアドレスを入力します。	仮想MACアドレスを入力する。 2桁ずつの半角英数字をコロン(:)またはハイフン(-)で区切る。
カードタイプがFCの場合		
仮想アドレス割り当て	仮想アドレス割り当てを行う場合に選択します。	(チェックあり)＝仮想アドレスを割り当てる
仮想アドレス[注1]		
自動割り当て	プール管理からの自動割り当てを有効にする場合に選択します。	(チェックあり)＝自動割り当てを有効にする
WWNN[注2]	仮想WWNNを入力します。	仮想WWNNを入力する。 2桁ずつの半角英数字をコロン(:)で区切る。
WWPN[注2]	仮想WWPNを入力します。	仮想WWPNを入力する。 2桁ずつの半角英数字をコロン(:)で区切る。
カードタイプがCNAの場合		
仮想アドレス割り当て	仮想アドレス割り当てを行う場合に選択します。	(チェックあり)＝仮想アドレスを割り当てる
仮想アドレス[注1]		
自動割り当て	プール管理からの自動割り当てを有効にする場合に選択します。	(チェックあり)＝自動割り当てを有効にする
WWNN[注2]	機能タイプが「FCoE」の場合、仮想WWNNを入力します。	仮想WWNNを入力する。 2桁ずつの半角英数字をコロン(:)で区切る。
WWPN[注2]	機能タイプが「FCoE」の場合、仮想WWPNを入力します。	仮想WWPNを入力する。 2桁ずつの半角英数字をコロン(:)で区切る。

項目名			説明	設定値
		E-MAC[注2]	機能タイプが「FCoE」の場合、仮想E-MACアドレスを入力します。	仮想E-MACアドレスを入力する。 2桁ずつの半角英数字をコロン(:)またはハイフン(-)で区切る。
		MAC[注2]	機能タイプが「iSCSI」または「LAN」の場合、仮想MACアドレスを入力します。	仮想MACアドレスを入力する。 2桁ずつの半角英数字をコロン(:)またはハイフン(-)で区切る。

[注1]:「仮想アドレス割り当て」にチェックを付けた場合のみ設定します。

[注2]:「自動割り当て」にチェックを付けない場合のみ設定します。

注意

- IQN、WWPN、仮想MACアドレスは、全体で一意である必要があります。

  WWNNは、同一カードを除き、全体で一意である必要があります。

  IQN、WWPN、WWNNが重複し、同一ボリュームに同時にアクセスするとボリュームを破壊する可能性があります。

  仮想MACアドレスが重複すると、ネットワーク通信ができなくなります。

- マルチキャストMACアドレスは仮想MACアドレスとして使用できません。

  任意に仮想アドレスを設定すると、他カードの工場出荷値と重複する可能性があります。

  次の範囲で仮想アドレスを設定することを推奨します。

  ー MACアドレス(00:19:99:3E:D2:A1～00:19:99:3F:CC:A1)

  ー WWN(50:01:99:93:ED:2A:10:00～50:01:99:93:FC:C9:FF:FF)

C.5 ストレージ用プロファイルの設定項目

ETERNUS DXシリーズ用のプロファイル中で設定する項目を記載します。対象とするストレージ種類に応じて選択可能な項目が異なる場合があります。

各項目の詳細は、対象ストレージのマニュアルを参照してください。

RAID&ディスク構成タブ

項目名		説明	設定値
RAID構成			
	RAIDグループ名	RAIDグループ名を指定します。 **注意** 装置に設定済みのRAIDグループ名は指定できません。	RAIDグループ名文字列を入力する。 1～16文字が入力可能。
	RAIDレベル	構築するディスクアレイのRAIDレベルを指定します。	プルダウンから以下を選択する。 RAID1、RAID5、RAID6、RAID1+0
	ディスク本数	ディスクアレイに組み込むディスク本数を指定します。	ディスク数を指定する。 選択したRAIDレベルに応じて選択可能な台数は異なる。

項目名	説明	設定値
ディスクインチ	ディスクドライブの種類(ドライブ外形サイズ)を指定します。	プルダウンから以下を選択する。 2.5 Inch、3.5 Inch
ディスク種別	ディスクアレイに組み込むディスクドライブの種類(インターフェース種類)を指定します。	プルダウンから以下を選択する。 ETERNUSのモデル、選択したディスクインチに応じて選択可能な種別は異なる。 SAS、NL-SAS、SED、SSD
ディスク容量	ディスクアレイに組み込むディスクドライブの種類(ディスク容量)を指定します。	プルダウンから以下を選択する。 選択したディスクインチ、ディスク種別に応じて選択可能な容量は異なる。 300GB、450GB、1TBほか
ボリューム		
ボリューム名	RAIDグループに作成するボリューム名を指定します。 注意 装置に設定済みのボリューム名は指定できません。	RAIDグループに作成するボリューム名文字列を指定する。 1～16文字が入力可能。
ボリュームサイズ	RAIDグループに作成するボリュームサイズを指定します。	テキストボックスにボリュームサイズを指定し、プルダウンから以下を選択する。 最後のボリュームサイズに対しては"max"を指定するとRAIDグループの残り全容量が割り当てられる。 ETERNUS DX60 S2では"max"は指定できない。 MB、GB、TB
グローバルホットスペア		
ディスクインチ	ホットスペアとして定義するディスクドライブの種類(ドライブ外形サイズ)を指定します。	プルダウンから以下を選択する。 2.5 Inch、3.5 Inch
ディスク種別	ホットスペアとして定義するディスクドライブの種類(インターフェース種類)を指定します。	プルダウンから以下を選択する。 ETERNUSのモデル、選択したディスクインチに応じて選択可能な種別は異なる。 SAS、NL-SAS、SED、SSD
ディスク容量	ホットスペアとして定義するディスクドライブの種類(ディスク容量)を指定します。	プルダウンから以下を選択する。 選択したディスクインチ、ディスク種別に応じて選択可能な容量は異なる。 300GB、450GB、1TBほか
ホストアフィニティ		
LUNグループ		
LUNグループ名	LUNグループ名を指定します。	LUNグループ名文字列を指定する。

項目名	説明	設定値
	注意 装置に設定済みのLUNグループ名は指定できません。	
ボリューム		
ボリューム名	LUNグループに属するボリューム名を指定します。	LUNグループに属するボリューム名 文字列を入力する。 プロファイルで作成するボリュームか、すでに装置に作成されているボリュームを指定する。
ポートグループ		
ポートグループ名	ポートグループ名を指定します。 注意 装置に設定済みのポートグループ名は指定できません。	ポートグループ名 文字列を指定する。 1～16文字が入力可能。
ポート		
ポート番号	ポートグループに属するポート番号を指定します。	ポートグループに属するポート番号を三桁の数字で指定する。
ホストグループ		
ホストグループ名	ホストグループ名を指定します。 注意 装置に設定済みのホストグループ名は指定できません。	ホストグループ名 文字列を指定する。 1～16文字が入力可能。
ホストタイプ	ホストグループのタイプを指定します。	プルダウンから以下を選択する。 iSCSI、FC
ホスト		
ホスト名	ホストグループに属するホスト名を指定します。 注意 装置に設定済みのホスト名は指定できません。	ホストグループに属するホスト名 文字列を指定する。 1～16文字が入力可能。
ホストiSCSI	ホスト名を定義するiSCSI名を指定します。 ホストグループのホストタイプがiSCSI名のときに入力可能です。	iSCSI名 文字列を入力する。 先頭に"iqn."または"eui."を入力する。
ホストWWN	ホスト名を定義するホストWWNを指定します。 ホストグループのホストタイプがFCのときに入力可能です。	ホストWWN文字列を入力する。 16文字の16進数が入力可能。
詳細設定		
Pre実行コマンド	プロファイルの適用動作（RAID/ホットスペア/ホストアフィニティ設定）の実行前に	記述内容については対象装置の『CLIユーザーガイド』を参照してください。

項目名	説明	設定値
	ETERNUSに対して実施したい制御コマンドを記述します。 特別な要求がない場合はチェックボックスを無効にしておきます。	
Post実行コマンド	プロファイルの適用動作(RAID/ホットスペア/ホストアフィニティ設定)の完了後にETERNUSに対して実施したい制御コマンドを記述します。 特別な要求がない場合はチェックボックスを無効にしておきます。	記述内容については対象装置の『CLIユーザーガイド』を参照してください。

ポイント

- アレイ構成に使用するディスクドライブの搭載スロット位置は指定できません。
- ホットスペア構築に使用するディスクドライブの搭載スロット位置は指定できません。

C.6 スイッチ用プロファイルの設定項目

スイッチ用のプロファイル中で設定する項目を記載します。

各項目の詳細は、対象スイッチのマニュアルを参照してください。

C.6.1 SRX用プロファイル

SNMPタブ

項目名	説明	設定値
SNMPサービス		
SNMPサービス設定	SNMPサービス設定を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
SNMPエージェントとトラップ(ON/OFF)	SNMPエージェントとトラップの有効、無効を指定します。	ON＝機能を有効にする OFF＝機能を無効にする
SNMPエージェント設定	SNMPエージェント設定を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
エージェントアドレス	エージェントアドレスを有効にするかどうかを指定します。	(チェックあり)＝エージェントアドレスを有効にする 加えて、エージェントアドレスをIPv4形式で入力する
SNMPエンジンID	SNMPエンジンIDを有効にするかどうかを指定します。	(チェックあり)＝SNMPエンジンIDを有効にする 加えて、SNMPエンジンIDを入力する。
SNMPホスト (SNMPv1 or v2c)		
番号	SNMPホスト定義番号を指定します。	プルダウンから選択する。
アドレス	SNMPホストのIPアドレスを指定します。	SNMPホストのIPアドレスをIPv4形式で指定する。

項目名	説明	設定値
コミュニティー名	SNMPホストのコミュニティー名を指定します。	SNMPホストのコミュニティー名 文字列を入力する。
トラップ	SNMPトラップの送信有無を指定します。	プルダウンから以下を選択する。 Off、v1、v2c
書き込み	SNMPマネージャーからの書込みを許可するかどうかを指定します。	(チェックあり)＝許可する (チェックなし)＝許可しない
SNMPユーザー (SNMPv3)		
番号	SNMPユーザー定義番号を指定します。	プルダウンから選択する。
ユーザー名	SNMPユーザー名を指定します。	SNMPユーザー名 文字列を入力する。
アドレス設定	SNMPのホストアドレスを有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
ホスト番号	SNMPホスト定義番号を指定します。	プルダウンから選択する。
ホストアドレス	SNMPホストのIPアドレスを指定します。	SNMPホストのIPアドレス文字列を入力する。
トラップ設定	SNMPトラップ設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
ホスト番号	SNMPホスト定義番号を指定します。	プルダウンから選択する。
ホストアドレス	SNMPホストのIPアドレスを指定します。	SNMPホストのIPアドレス文字列を入力する。
認証設定	SNMP認証プロトコルを有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
認証プロトコル	SNMP認証プロトコルを指定します。	プルダウンから以下を選択する。 None、MD5、SHA
認証パスワード	SNMP認証パスワードを指定します。	SNMP認証パスワード文字列を入力する。
暗号化設定	SNMP暗号化設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
暗号化プロトコル	SNMP暗号プロトコルを指定します。	プルダウンから以下を選択する。 None、DES
暗号化パスワード	SNMP暗号パスワードを指定します。	SNMP暗号パスワード文字列を入力する。
読み取り	SNMP MIB読取りを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none：読取りを許可しない all：読取りを許可する
書き込み	SNMP MIB書込みを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none：書込みを許可しない all：書込みを許可する
通知	SNMP MIBトラップ通知を有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none：読出しを許可しない

項目名	説明	設定値
		all：読出しを許可する

認証タブ

項目名	説明	設定値
アカウント		
管理者のパスワードの変更	管理者パスワードを変更するかどうかを指定します。	（チェックあり）＝管理者パスワードを変更する
パスワード	新たな管理者パスワードを指定します。	パスワード文字列を入力する。

NTPタブ

項目名	説明	設定値
時刻の自動調整		
時刻の自動調整	時刻の自動調整を有効にするかどうかを指定します。	（チェックあり）＝有効にする
サーバ設定	時刻提供サーバの設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
プロトコル （Time/SNTP）	使用するプロトコルを指定します。	Time＝TCPを使用する SNTP＝UDPを使用する
アドレス	時刻提供サーバのIPアドレスを指定します。	時刻提供サーバのIPアドレス文字列を入力する。
間隔設定	自動時刻設定する間隔を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
間隔時間 （起動時/期間指定）	自動時刻設定の間隔を指定します。	起動時＝起動時に行う 期間指定＝任意の期間に行う。加えて、画面に期間を入力する
タイムゾーン設定	タイムゾーン設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
グリニッジ標準時刻からの時間差	装置が使用するグリニッジ標準時刻からの時間差を指定します。	プルダウンから選択する。

STPタブ

項目名	説明	設定値
STP (スパニングツリープロトコル) 設定		
STP	STP設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから選択する。

C.6.2 VDX用プロファイル

SNMPタブ

項目名	説明	設定値
SNMPサービス		

項目名	説明	設定値
SNMPサービス設定	SNMPサービス設定を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
SNMPエージェントとトラップ(ON/OFF)	SNMPエージェントとトラップの有効、無効を指定します。	ON＝機能を有効にする OFF＝機能を無効にする
グループ(コミュニティーとユーザー用)		
グループ名	グループ名を指定します。	グループ名文字列を入力する。
SNMPバージョン	SNMPバージョンを指定します。	プルダウンから以下を選択する。 v1、v2c、v3
v3セキュリティレベル	SNMPv3用セキュリティレベルを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を選択する。 auth、noauth、priv
読み取り	SNMP MIB読取りを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none:読取りを許可しない all:読取りを許可する
書き込み	SNMP MIB書込みを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none:書込みを許可しない all:書込みを許可する
通知	SNMP MIBトラップ通知を有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none:読出しを許可しない all:読出しを許可する
コミュニティー(ホスト用)		
コミュニティー名	SNMPコミュニティー名を指定します。	コミュニティー名文字列を入力する。
グループ	コミュニティーが所属するグループを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから選択済みのグループを選択する。
書き込み	SNMPコミュニティーの書込みを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を選択する。 Enabled、Disabled
ホスト		
アドレス	SNMPホストのIPアドレスを指定します。	ホストのIPアドレスをIPv4またはIPv6のアドレス表記に従った文字列を入力する。
コミュニティー名	SNMPコミュニティー名を指定します。	プルダウンから設定済みのコミュニティー名を選択する。
重大度レベル	SNMPトラップレベルを指定します。	プルダウンから選択する。
トラップバージョン	SNMPトラップバージョンを指定します。	プルダウンから以下を選択する。 v1、v2c

項目名	説明	設定値
UDPポート	SNMPトラップ送信ポートを指定します。	SNMPトラップ送信ポート文字列を入力する。 「0」～「65535」が指定可能。
ユーザー (v3ホスト用)		
ユーザー名	SNMPユーザー名を指定します。	ユーザー名1～16文字の文字列を入力する。
グループ	SNMPグループ名を指定します。	プルダウンから設定済みのグループを選択する。
認証設定	SNMP認証設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする
認証プロトコル	SNMP認証プロトコルを指定します。	プルダウンから以下を選択する。 MD5、SHA、NoAuth
認証パスワード	SNMP認証パスワードを入力します。	認証パスワード1～32文字の文字列を入力する。
暗号化設定	SNMP暗号化設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする
暗号化プロトコル	SNMP暗号化プロトコルを指定します。	プルダウンから以下を選択する。 DES、AES128、NoPriv
暗号化パスワード	SNMP暗号パスワードを指定します。	暗号化パスワード1～32文字の文字列を入力する。
v3ホスト		
アドレス	SNMPホストのIPアドレスを指定します。	ホストのIPアドレスをIPv4またはIPv6のアドレス表記に従った文字列を入力する。
ユーザー名	SNMPユーザー名を指定します。	プルダウンから設定済みのユーザーを選択する。
重大度レベル	SNMPトラップレベルを指定します。	プルダウンから選択する。
通知タイプ	SNMP通知タイプを指定します。	プルダウンから以下を選択する。 traps、informs
エンジンID	SNMPエンジンIDを指定します。	エンジンID「0:0:0:0:0:0:0:0:0:0」～「FF:FF:FF:FF:FF:FF:FF:FF:FF:FF」を文字列で指定する。 文字パターンは、MACアドレスと同様。
UDPポート	SNMPトラップ送信ポートを指定します。	SNMPトラップ送信ポート文字列を入力する。 「0」～「65535」が指定可能。

認証タブ

項目名	説明	設定値
アカウント		
管理者のパスワードの変更	管理者パスワードを変更するかどうかを指定します。	(チェックあり)＝管理者パスワードを変更する
パスワード	新たな管理者パスワードを指定します。	パスワード8～32文字の文字列を入力する。

NTPタブ

項目名	説明	設定値
時刻の自動調整		
時刻の自動調整	時刻の自動調整を有効にするかどうかを指定します。	(チェックあり)＝有効にする
サーバ設定	時刻提供サーバの設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
アドレス	時刻提供サーバのIPアドレスを指定します。	時刻提供サーバのIPアドレスをIPv4またはIPv6のアドレス表記に従った文字列を入力する。
タイムゾーン設定	タイムゾーン設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
地域	地域情報を指定します。	地域情報を(地域)/(都市)形式で入力する。

C.6.3 イーサネットスイッチ(10GBASE-T 48+6／10GBASE 48+6)用プロファイル

SNMPタブ

項目名	説明	設定値
SNMPサービス		
SNMPサービス設定	SNMPサービス設定を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
SNMPエージェントとトラップ (ON/OFF)	SNMPエージェントとトラップの有効、無効を指定します。	ON＝機能を有効にする OFF＝機能を無効にする
グループ(コミュニティーとユーザー用)		
グループ名	グループ名を指定します。	グループ名文字列を入力する。
SNMPバージョン	SNMPバージョンを指定します。	プルダウンから以下を選択する。 v1、v2c、v3
v3セキュリティレベル	SNMPv3用セキュリティレベルを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を選択する。 auth、noauth、priv
読み取り	SNMP MIB読取りを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none:読取りを許可しない Default:読取りを許可する
書き込み	SNMP MIB書込みを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。 none:書込みを許可しない Default:書込みを許可する
通知	SNMP MIBトラップ通知を有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、プルダウンから以下を指定する。

項目名		説明	設定値
			none：読出しを許可しない Default：読出しを許可する
コミュニティー（ホスト用）			
	コミュニティー名	SNMPコミュニティー名を指定します。	コミュニティー名 文字列を入力する。
	グループ	コミュニティーが所属するグループを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから選択済みのグループを選択する。
	書き込み	SNMPコミュニティーの書込みを有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから以下を選択する。 Enabled、Disabled
ホスト			
	アドレス	SNMPホストのIPアドレスを指定します。	ホストのIPアドレスをIPv4またはIPv6のアドレス表記に従った文字列を入力する。
	コミュニティー名	SNMPコミュニティー名を指定します。	プルダウンから設定済みのコミュニティー名を選択する。
	トラップバージョン	SNMPトラップバージョンを指定します。	プルダウンから以下を選択する。 v1、v2c
	UDPポート	SNMPトラップ送信ポートを指定します。	SNMPトラップ送信ポート文字列を入力する。 「1」～「65535」が指定可能。
ユーザー (v3ホスト用)			
	ユーザー名	SNMPユーザー名を指定します。	ユーザー名1～30文字の文字列を入力する。
	グループ	SNMPグループ名を指定します。	プルダウンから設定済みのグループを選択する。
	認証設定	SNMP認証設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする
	認証プロトコル	SNMP認証プロトコルを指定します。	プルダウンから以下を選択する。 MD5、SHA、NoAuth
	認証パスワード	SNMP認証パスワードを入力します。	認証パスワード1～32文字の文字列を入力する。
	暗号化設定	SNMP暗号化設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする
	暗号化プロトコル	SNMP暗号化プロトコルを指定します。	プルダウンから以下を選択する。 DES、NoPriv
	暗号化パスワード	SNMP暗号パスワードを指定します。	暗号化パスワード1～32文字の文字列を入力する。
v3ホスト			
	アドレス	SNMPホストのIPアドレスを指定します。	ホストのIPアドレスをIPv4またはIPv6のアドレス表記に従った文字列を入力する。
	ユーザー名	SNMPユーザー名を指定します。	プルダウンから設定済みのユーザーを選択する。
	通知タイプ	SNMP通知タイプを指定します。	プルダウンから以下を選択する。

項目名	説明	設定値
		traps、informs
UDPポート	SNMPトラップ送信ポートを指定します。	SNMPトラップ送信ポート文字列を入力する。 「1」～「65535」が指定可能。

認証タブ

項目名	説明	設定値
アカウント		
管理者のパスワードの変更	管理者パスワードを変更するかどうかを指定します。	(チェックあり)＝管理者パスワードを変更する
パスワード	新たな管理者パスワードを指定します。	パスワード8～64文字の文字列を入力する。

NTPタブ

項目名	説明	設定値
時刻の自動調整		
時刻の自動調整	時刻の自動調整を有効にするかどうかを指定します。	(チェックあり)＝有効にする
サーバ設定	時刻提供サーバの設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
アドレス	時刻提供サーバのIPアドレスを指定します。	時刻提供サーバのIPアドレスをIPv4またはIPv6のアドレス表記に従った文字列を入力する。
モード	モードを指定します。	Broadcast＝SNTPサーバにブロードキャスト情報を問い合わせして時刻を同期する Unicast＝SNTPクライアントはSNTPサーバとポイント・ツー・ポイントの関係で動作する
間隔設定	自動時刻設定する間隔を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
間隔時間[s]	自動時刻設定の間隔[秒]を指定します。	画面に期間を入力する
タイムゾーン設定	タイムゾーン設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
グリニッジ標準時刻からの時間差	装置が使用するグリニッジ標準時刻からの時間差を指定します。	プルダウンから選択する。

C.6.4 CFX用プロファイル

SNMPタブ

項目名	説明	設定値
SNMPサービス		

項目名	説明	設定値
SNMPサービス設定	SNMPサービス設定を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
SNMPエージェントとトラップ(ON/OFF)	SNMPエージェントとトラップの有効、無効を指定します。	ON＝機能を有効にする OFF＝機能を無効にする
SNMPエージェント設定	SNMPエージェント設定を使用するかどうかを指定します。	(チェックあり)＝使用する (チェックなし)＝使用しない
ドメインID	ドメインIDを指定します。	ドメインIDを入力する
エージェントアドレス	エージェントアドレスを有効にするかどうかを指定します。	(チェックあり)＝エージェントアドレスを有効にする 加えて、エージェントアドレスのIPアドレス文字列を入力する。
SNMPエンジンID	SNMPエンジンIDを有効にするかどうかを指定します。	(チェックあり)＝SNMPエンジンIDを有効にする 加えて、SNMPエンジンIDを入力する。
SNMPホスト (SNMPv1 or v2c)		
番号	SNMPホスト定義番号を指定します。	プルダウンから選択する。
アドレス	SNMPホストのIPアドレスを指定します。	SNMPホストのIPアドレスを入力する。
コミュニティー名	SNMPホストのコミュニティー名を指定します。	SNMPホストのコミュニティー名 文字列を入力する。
トラップタイプ	SNMPトラップの送信有無を指定します。	プルダウンから以下を選択する。 off、v1、v2c
書き込み	SNMPマネージャーからの書込みを許可するかどうかを指定します。	(チェックあり)＝許可する (チェックなし)＝許可しない
SNMPユーザー (SNMPv3)		
番号	SNMPユーザー定義番号を指定します。	プルダウンから選択する。
ユーザー名	SNMPユーザー名を指定します。	(チェックあり)＝指定する 加えて、SNMPユーザー名 文字列を入力する。
アドレス設定	SNMPのホストアドレスを有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
ホスト番号	SNMPホスト定義番号を指定します。	プルダウンから選択する。
ホストアドレス	SNMPホストのIPアドレスを指定します。	SNMPホストのIPアドレス文字列を入力する。
トラップ設定	SNMPトラップ設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
ホスト番号	SNMPホスト定義番号を指定します。	プルダウンから選択する。
ホストアドレス	SNMPホストのIPアドレスを指定します。	SNMPホストのIPアドレス文字列を入力する。
認証設定	SNMP認証プロトコルを有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
認証プロトコル	SNMP認証プロトコルを指定します。	プルダウンから以下を選択する。

項目名	説明	設定値
		None、MD5、SHA
認証パスワード	SNMP認証パスワードを指定します。	SNMP認証パスワード文字列を入力する。
暗号化設定	SNMP暗号化設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
暗号化プロトコル	SNMP暗号プロトコルを指定します。	プルダウンから以下を選択する。 None、DES
暗号化パスワード	SNMP暗号パスワードを指定します。	SNMP暗号パスワード文字列を入力する。
読み取り	SNMP MIB読取りを有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから以下を指定する。 none：読取りを許可しない all：読取りを許可する
書き込み	SNMP MIB書込みを有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから以下を指定する。 none：書込みを許可しない all：書込みを許可する
通知	SNMP MIBトラップ通知を有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから以下を指定する。 none：通知を許可しない all：通知を許可する

Interfaceタブ

項目名	説明	設定値
インターフェース設定		
ターゲット	etherポートを指定します。	「シャーシID/etherポート番号」または「ドメインID/スイッチID/シャーシID/etherポート番号」で指定します。
ポートタイプ	Endpointにするかどうかを指定します。	（チェックあり）＝Endpointにする
LLDP	LLDPを有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから以下を選択する。 Disable＝LLDP機能は動作しない Enable＝LLDP情報の送受信を行う Send＝LLDP情報の送信だけを行う Receive＝LLDP情報の受信だけを行う
Cfabポートモード	Cfabポートモードを有効にするかどうかを指定します。	（チェックあり）＝有効にする 加えて、プルダウンから以下を選択する。 Auto＝自動的に検知したポート種別で動作する External＝強制的に外部ポートとして動作する

認証タブ

項目名	説明	設定値
アカウント		
管理者のパスワードの変更	管理者パスワードを変更するかどうかを指定します。	(チェックあり)＝管理者パスワードを変更する
パスワード	新たな管理者パスワードを指定します。	パスワード文字列を入力する。
AAA設定		
AAAグループID	AAAグループIDを指定します。	プルダウンから以下を選択する。 0～9
LDAP機能	LDAPサービス機能の有効、無効を指定します。	有効＝機能を有効にする 無効＝機能を無効にする
LDAP設定	LDAPクライアント設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
クライアント		
番号	クライアント番号を指定します。	プルダウンから以下を選択する。 0～3
サーバ情報設定	サーバ情報設定を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
LDAPサーバアドレス	LDAPサーバのIPアドレスを指定します。	LDAPサーバのIPアドレス文字列を入力する。
送信元	送信元情報を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
ドメインID	送信元ドメインIDを指定します。	プルダウンから以下を選択する。 1～32
アドレス	送信元IPアドレスを指定します。	送信元のIPアドレス文字列を入力する。
RDN	RDNを有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、RDNを入力する。 例:CN
バインド名(RDN以外)	RDNを除くバインド名を有効にするかどうかを指定します。	(チェックあり)＝有効にする 加えて、RDNを除くバインド名を入力する。 例:CN=user,DC=local
管理者	管理者クラス情報を有効にするかどうかを指定します。	(チェックあり)＝有効にする (チェックなし)＝無効にする
クラスID	クラスIDを指定します。	プルダウンから以下を選択する。 0～3
クラス値	管理者クラス値を指定します。	管理者クラス値の文字列を入力する。 例:user

NTPタブ

項目名	説明	設定値
時刻の自動調整		

項目名	説明	設定値
時刻の自動調整	時刻の自動調整を有効にするかどうかを指定します。	（チェックあり）＝有効にする
サーバ設定	時刻提供サーバの設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
プロトコル （Time/SNTP）	使用するプロトコルを指定します。	Time＝TCPを使用する SNTP＝UDPを使用する
アドレス	時刻提供サーバのIPアドレスを指定します。	時刻提供サーバのIPアドレス文字列を入力する。
間隔設定	自動時刻設定する間隔を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
間隔時間 （起動時/期間指定）	自動時刻設定の間隔を指定します。	起動時＝起動時に行う 期間指定＝任意の期間に行う。加えて、画面に期間を入力する
タイムゾーン設定	タイムゾーン設定を有効にするかどうかを指定します。	（チェックあり）＝有効にする （チェックなし）＝無効にする
グリニッジ標準時刻からの時間差	装置が使用するグリニッジ標準時刻からの時間差を指定します。	プルダウンから選択する。