CA92344-2515-02

FUJITSU Software Infrastructure Manager V2.3
Infrastructure Manager for PRIMEFLEX V2.3
ノードを管理・運用するための環境設定詳細

2018 年 10 月
富士通株式会社

改版履歴		
版数	提供年月	変更内容
01	2018 年 8 月	新規作成
02	2018 年 10 月	2.1　使用ポート番号一覧 2.2　ノード設定詳細 3.3.2　ログ容量の目安 ・Brocade VDX の名称を VDX に修正

本書では、FUJITSU Software Infrastructure Manager V2.3 および FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.3 の機能を利用するうえで必要な事前設定、環境設定の情報と、管理・運用の対象となるノードの設定や参考情報などを提供します。

以降、Infrastructure Manager を「ISM」、Infrastructure Manager for PRIMEFLEX を「ISM for PRIMEFLEX」と表記します。また、Infrastructure Manager と Infrastructure Manager for PRIMEFLEX を区別しないで説明する場合、両方を総称して「Infrastructure Manager」または「ISM」と表記します。

本書に記載の詳細や略語については、ISM または ISM for PRIMEFLEX の下記マニュアルを参照してください。

・ユーザーズマニュアル
・用語集
・補足情報『監視対象 OS、仮想化管理ソフトウェアに対する設定』

第 1 章　　ISM の動作環境設定

1.1　プロファイル管理機能・ファームウェア管理機能使用時の DHCP/PXE 設定

下記の機能を使用する場合は、PXE ブート機能を利用します。

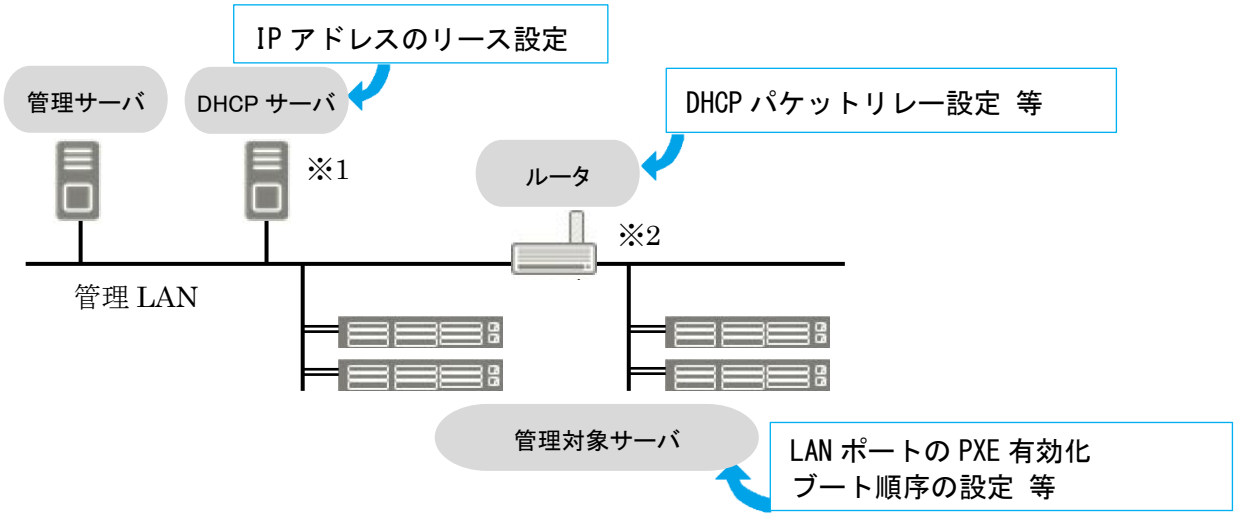
・プロファイル管理機能で、サーバへ OS をインストールする
・ファームウェア管理機能で、サーバまたは搭載 IO カードの Offline アップデートを実行する。

PXE ブートを正しく動作させるためには、事前に管理対象サーバ(ノード)およびネットワーク構成について適切な準備が必要です。ここでは PXE ブートに必要な作業について情報を提供します。

なお、OS インストール以外のプロファイル適用や、ファームウェアの Online アップデートの実行については、本作業は不要です。

1.1.1 ネットワーク構成例

以下に PXE ブート機能利用時のネットワーク構成例と主な事前準備作業を示します。



(※1)外部に DHCP サーバを用意する代わりに、ISM-VA(管理サーバ)内の DHCP サーバ機能の使用も可能です。
外部の DHCP サーバと管理サーバ内部の DHCP サーバ機能はどちらか一方を使用してください。
(※2)ネットワークセグメントを分割しない場合、ルータは不要です。

1.1.2 必要な準備作業

管理対象サーバ

PXE ブート機能は、オンボード LAN(*1)または LAN カードのポートを使用します。
必要に応じて BIOS 設定等を変更し、使用する LAN ポートからの PXE ブートを有効にします(*2)。

(※1) 管理対象サーバのモデルによっては、「Dynamic LoM」と記載される場合があります。
(※2) 使用する LAN ポートの指定は、各ノードの「PXE ブートポート」で設定します。

事前設定

・LAN ポートおよび PXE 機能を有効に設定してください。
オンボードの場合、これらの設定は工場出荷時に有効に設定されています。無効に変更した場合は有効に戻してください。LAN カードの場合は各カードのマニュアル等を参照してください。

・複数のネットワークポートで PXE ブートを有効にしている場合は、BIOS のブート順設定を確認し、ISM が PXE ブートに使用する LAN ポートがネットワークポートの中で最も高い優先度になるように設定してください。

DHCP サーバ／ルータ

ISM-VA 内の DHCP 機能を有効にするか、管理サーバと同じネットワークセグメント内で DHCP サーバを動作させ、PXE ブート用の LAN ポートに対して適切な IPv4 アドレスがリースできるよう設定してください。その際、リース期間は 60 分以上に設定してください。

例）ISM-VA が 192.168.1.100/24 に接続している場合のスコープ設定例

リース範囲：192.168.1.128～192.168.1.159

リース期間：8 日間

管理対象サーバが別セグメントのネットワークに接続されている場合は、PXE ブートに必要な DHCP パケット等がセグメント間で相互に通信可能になるようルータを設定してください。

その他、ISM が使用する各種ポートも通信可能に設定してください。

ISM（管理サーバ）

PXE ブート以外に必要な主な作業を記載します。「ユーザーズマニュアル」に従って実施してください。

－ISM-VA 全体に対する仮想ディスク割当て／ユーザーグループに対する仮想ディスク割当て

－OS インストール DVD のインポート (OS インストールの場合)

－ServerView Suite Update DVD のインポート (Offline アップデートの場合)

－ServerView Suite DVD のインポート

－管理対象サーバの ISM への登録

※ISM に登録する際は「OEM」または「Administrator」権限を持つ iRMC ユーザーを登録してください。

注意

・ROR（ServerView Resource Orchestrator）が ISM と同じ管理 LAN 上に構築されている場合、ROR の PXE サービスを停止する必要があります。下記のマニュアルサイトから該当の ROR バージョンを選択し、PXE サービス停止のコマンドを確認してください。

http://software.fujitsu.com/cgi-bin/manualps.cgi?langtype=ja&viewtype=icon&keyword=ServerView+Resource+Orchestrator&ostype=all

・ServerView Resource Orchestrator Cloud Edition の『リファレンスガイド（コマンド/XML 編）』

・ServerView Resource Orchestrator Express/Virtual Edition の『リファレンスガイド（コマンド編）』

上記マニュアルの“rcxadm pxectl”コマンドを参照してください。

1.2　仮想リソース管理機能の事前設定

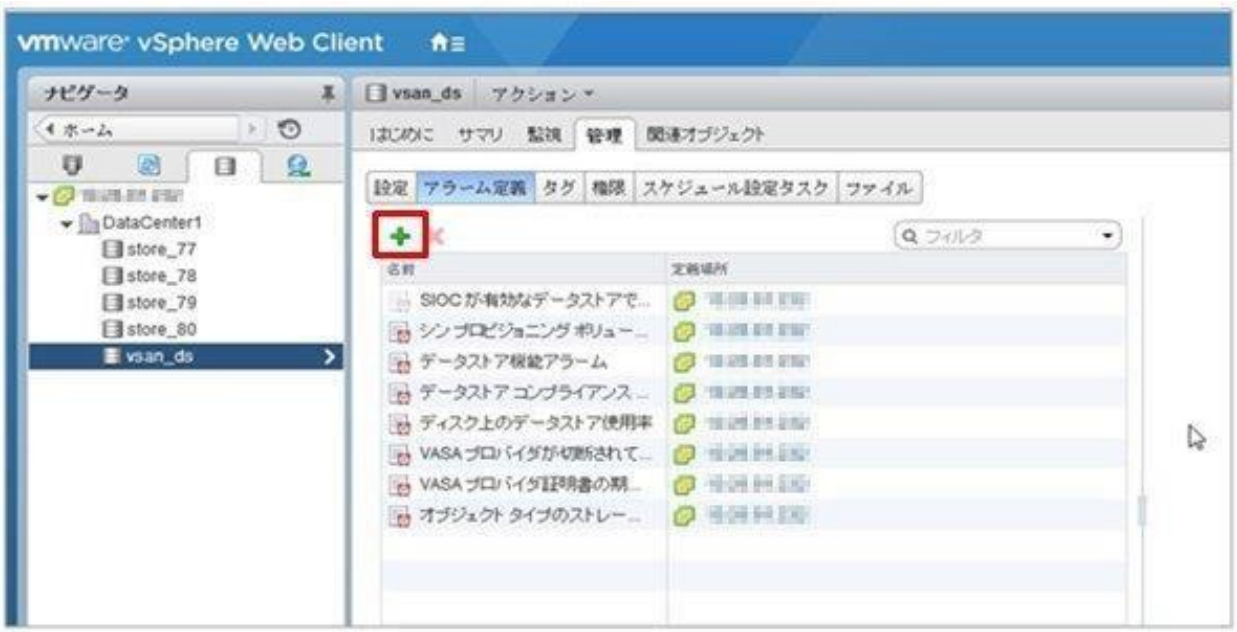
仮想リソース管理機能を使用することで、仮想化基盤の運用監視ができます。ここでは仮想リソース管理機能に必要な事前設定の情報を提供します。

1.2.1 VMware VSAN の事前設定

VMware VSAN のホスト間のネットワーク断線による VSAN データストアの異常を検出できるようにするため、アラーム定義を行います。VSAN のアラーム定義の追加方法について説明します。

(1) vSphere Web Client画面を表示します。[ホーム]からストレージビュータブを選択し、表示されたデータストアからVSANデータストアを選択します（以下はVSANデータストア名が「vsan_ds」の例）。

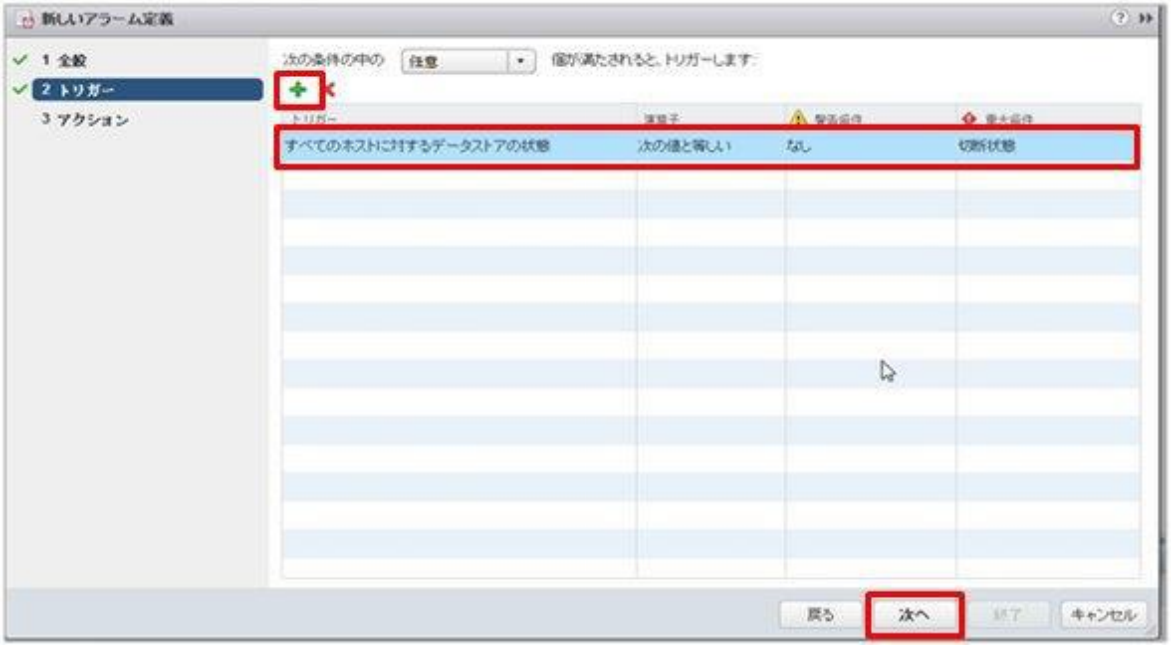
表示された画面右側の[管理]タブ（vCenter Server Appliance 6.5の場合は[監視]タブから[問題]を選択）から[アラーム定義]を選択して[＋]を選択します。



(2) ウィザード画面で「アラーム名」と「説明」に下表のように入力し[次へ]ボタンを選択します。

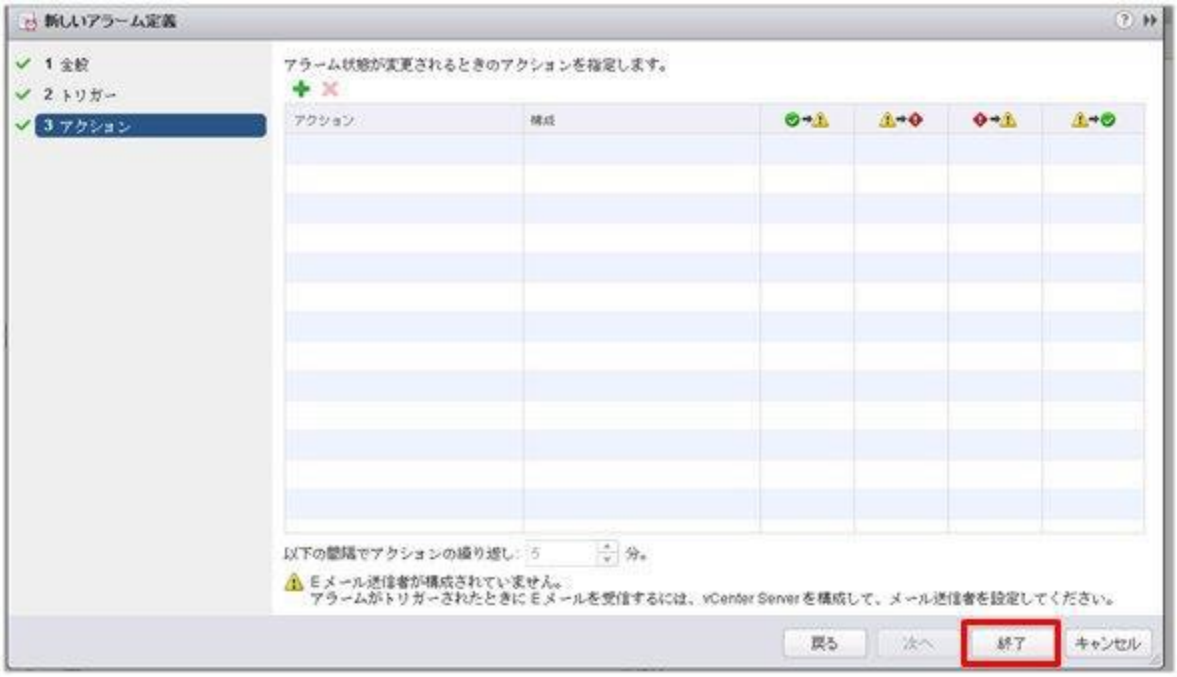
項目	入力内容
アラーム名	ホスト間ネットワークの断線
説明	ホスト間のネットワークが断線した場合のアラーム

(3) 以下の画面で[＋]を選択し、各項目を下表のように設定して、[次へ]ボタンを選択します。

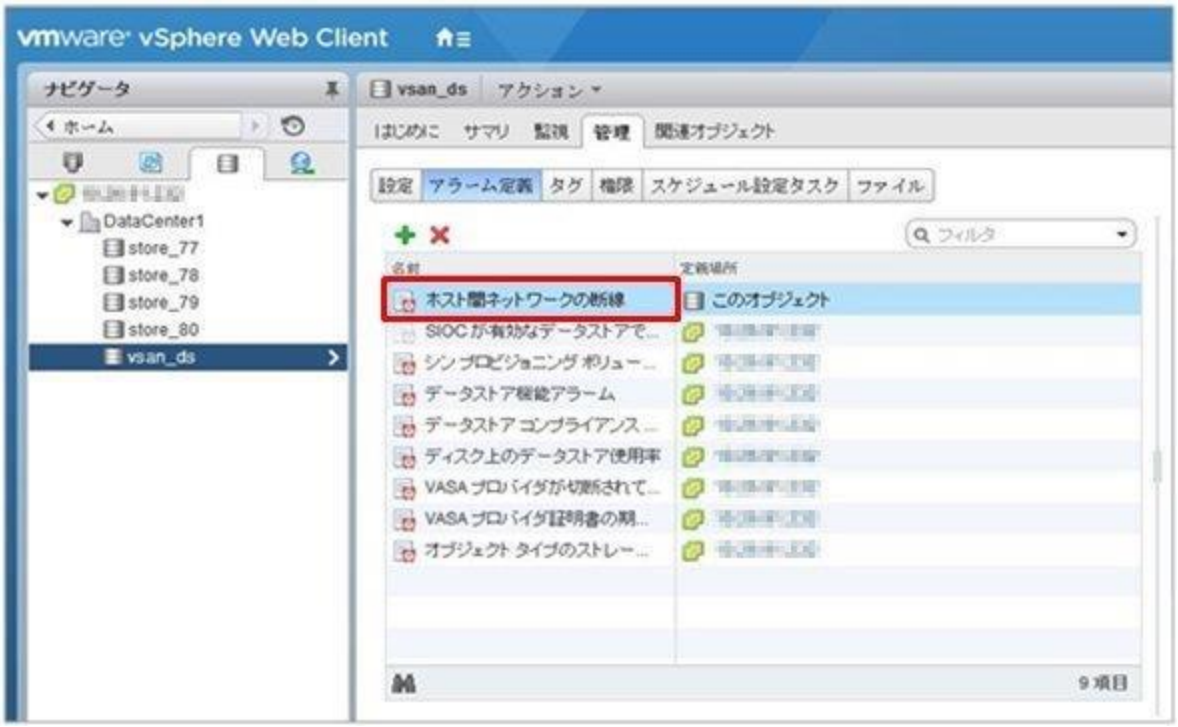


項目	設定値
トリガー	すべてのホストに対するデータストアの状態
演算子	次の値と等しい
警告条件	なし
重大条件	切断状態

(4) アクションは設定不要です。[終了]ボタン（または[完了]ボタン）を選択します。



(5) 完了すると、アラーム定義に新しい定義が追加されます。



1.2.2 Storage Spaces Direct の事前設定

Microsoft Storage Spaces Direct の運用管理を行うために、ISM-VA に対して OS 監視の設定、および記憶域プールを構成するすべてのノードに対して、CredSSP 認証の有効化が必要です。以下の手順で実施してください。

ISM-VA への設定

ISM から OS を監視するための設定を行います。設定方法については、「監視対象 OS、仮想化管理ソフトウェアに対する設定」の（2.1 Windows への設定手順）を参照してください。

ノードへの設定

記憶域プールを構成するすべてのノードに対して CredSSP 認証の有効化を設定します。

注意

本設定を行わない場合、Storage Spaces Direct に対して仮想リソース管理機能が利用できません。
また、記憶域プールを構成するノードは、サーバマネージャーまたはフェイルオーバクラスタマネージャーから確認できます。

---

(1) ノードにドメイン管理者権限のユーザーでログインし、PowerShellを起動します。

(2)以下のコマンドを実行します。

```
Enable-WSManCredSSP -Role client -DelegateComputer ＜対象ノード（コンピューター）名＞
```

ドメイン内のすべてのコンピューター名の指定には、ワイルドカード（*）を使用できます。
例：

```
Enable-WSManCredSSP -Role client -DelegateComputer *.fujitsu.local
```

(3)続いて以下のコマンドを実行します。

```
Enable-WSManCredSSP -Role server
```

1.3　MIB ファイルのインポートに関する注意

ISM での MIB のインポートに関する注意事項について説明します。

1.3.1 MIB の記述形式について

MIB のトラップ定義に特定形式の注釈を記述することにより重要度等を取り扱うことが可能ですが、内容によっては定義どおりに処理されない場合があります。ここではインポートする MIB の記述形式について説明します。

MIB のトラップ定義(TRAP-TYPE/NOTIFICATION-TYPE)の注釈の形式は、Novell NMS で提唱の形式に準じています。

例：

```
sniScVoltageTooHigh TRAP-TYPE
ENTERPRISE sniServerMgmt
VARIABLES {
trapServerName,
trapTime,
trapCabinetNumber,
trapObjectNumber,
trapString
}
DESCRIPTION
      "Power supply voltage is too high."
--#TYPE        "Voltage too high"
--#SUMMARY    "Power supply voltage %d (%s) in cabinet %d at server %s is too high."
--#SEVERITY        CRITICAL
::= 652
```

コメントフィールドの記述

--#TYPE	トラップのショートネーム。この名前には、最大 40 文字を使用できます。ISM 上ではトラップメッセージの一部として使用します。
--#SUMMARY	プレースホルダを含むトラップの説明、およびトラップで渡される実際のパラメーターの書式情報。ISM 上ではトラップメッセージの一部として使用します。
--#ARGUMENTS	SUMMARY 文字列に代入するパラメーターのリスト。パラメーターは、リストに表示された順序で代入されます。リストの各要素は、VARIABLES 句のパラメーターのインデックス(ゼロベース)です。
--#SEVERITY	トラップに割り当てられるデフォルトの重要度。次のいずれかになります。 情報（INFORMATIONAL） 軽度（MINOR） 重度（MAJOR） 危険（CRITICAL）

注意

・--#TYPE の記載がない場合、オブジェクト名が代用されます。
・--#SUMMARY の記載がない場合、DESCRIPTION の内容が代用されます。
・--#SEVERITY の記載がない場合、あるいは INFOMATIONAL/MINOR/MAJOR/CRITICAL のいずれにも該当しない重要度が定義されている場合、トラップの重要度は INFORMATIONAL として扱われます。

1.3.2 Unknown トラップを受信した場合の対処

トラップを受信した場合、対応する MIB が登録されていないと重要度が Unknown となりメッセージが正しく表示されません。Unknown トラップを受信した場合最新の MIB を取得し更新してください。更新後も Unknown トラップを受信する場合、対象の装置に異常がないか確認してください。

第 2 章　　管理対象ノードの設定詳細

2.1　使用ポート番号一覧

ISM は装置と通信する必要があります。ここでは通信に必要な使用ポート番号の情報を提供します。機器や環境に合わせて設定する必要があります。

ISM の使用ポート番号(ポート番号のデフォルト設定を記載)

対象機器	機能	プロトコル	使用ポート
PRIMERGY (RX/BX/CX/TX) PRIMEQUEST 3000B IPCOM VX2 (PRIMERGY CX1430 M1 を除く)	ノード情報取得	IPMI / HTTPS	623 / 443
	モニタリング	IPMI	623
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	IPMI / TFTP	623 / 69
	ログ収集	IPMI / SSH / HTTPS	623 / 22 / 443
	プロファイル適用(全般)	IPMI	623
		HTTP	80
		HTTPS	443
	プロファイル適用（OS インストール時のみ)	FTP	21
		DHCP	67
		TFTP	69
		SMB	445
		PXE	4011
		独自	9213
PRIMERGY CX1430 M1	ノード情報取得	IPMI / HTTPS	623 / 443
	モニタリング ファームウェアアップデート	IPMI	623
PRIMERGY BX シャーシ (MMB)	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP / SSH	161 / 22
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	SNMP / SSH / TFTP	161 / 22 69
	ログ収集	SSH	22
PRIMEQUEST 2000Type3 PRIMEQUEST 3000E	ノード情報取得	SNMP / IPMI	161 / 623
	モニタリング	SNMP / IPMI	161 / 623
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	IPMI	623
ETERNUS DX/AF	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	FTP / SSH	21 / 22
	プロファイル適用	SSH	22
ETERNUS NR (NetApp)	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP / HTTPS	161 / 443
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	-	-
	ログ収集	SSH / HTTPS	22 / 443
	プロファイル適用	-	-

SR-X	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6)	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
ExtremeSwitching VDX (Brocade VDX) (以降、「VDX」と表記)	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
Catalyst 3750-X Nexus 5000 Series	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
CFX2000F/R PRIMERGY スイッチブレード/ コンバージドファブリックスイッチブレード(10Gbps 18/8+2)	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
PRIMERGY BX スイッチブレード(1Gbps/10Gbps)	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / TFTP SSH	21 / 69 22
	ログ収集	SSH	22
PRIMERGY BX LAN パススルーブレード	ノード情報取得 モニタリング	SNMP	161 (通信先はMMB)
	トラップ受信	SNMP (Trap)	162
Brocade FC スイッチ	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
PRIMERGY BX FC スイッチブレード	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	SSH	22
	ログ収集	SSH	22
Asetek Rack CDU / Schneider Electric Metered Rack Mount PDU / Schneider Electric Smart-UPS	ノード情報取得	SNMP	161
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162

対象 OS	機能	プロトコル	使用ポート
Windows	OS 情報取得	WSMAN	5986
	モニタリング	WSMAN	5986
	ファームウェアアップデート	-	-
	ログ収集	WSMAN	5986
Linux	OS 情報取得	SSH	22
	モニタリング	SSH	22
	ファームウェアアップデート	SSH	22
	ログ収集	SSH	22
VMware ESXi	OS 情報取得	vSphere API / CIM	443 / 5989
	モニタリング	vSphere API	443
	ファームウェアアップデート	-	-
	ログ収集	REST	443

2.2 ノード設定詳細

ISM でノードを管理するためには、ノード側で接続情報を設定する必要があります。ここでは設定に必要な接続情報を提供します。

2.2.1 接続情報

ノードと接続するには、ノード登録を行う前にノード側で以下の設定が必要です。設定方法については、それぞれの装置のマニュアルを参照してください。　　○：必須、-：不要

ノード	接続情報			
	IPMI のアカウント(※1)/パスワード	SSH のアカウント/パスワード	SNMP の必須入力情報(※2)	HTTPS のアカウント/パスワード
PRIMERGY(RX/CX/TX) (CX1430 M1 を除く)	○	-	-	-(※4)
PRIMERGY CX1430 M1	○	-	-	○
PRIMEQUEST 2000Type3	○	○	○	-
PRIMEQUEST 3000E	○	○	○	-
PRIMEQUEST 3000B	○	-	-	-(※4)
ETERNUS DX/AF	-	○	○	-
ETERNUS NR	-	○	○	-
SR-X	-	○	○	-
イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6)	-	○	○	-
VDX(Brocade VDX)	-	○	○	-
Brocade FC スイッチ	-	○	○	-
Cisco Catalyst	-	○	○	-
Cisco Nexus	-	○	○	-
PRIMERGY BX シャーシ (MMB)	-	○	○	-
PRIMERGY BX サーバブレード	○	-	-	-
PRIMERGY BX スイッチブレード (1Gbps/10Gbps)	-	○	○	-
PRIMERGY BX LAN パススルーブレード	-	-	-(※3)	-
PRIMERGY BX FC スイッチブレード	-	○	○	-
PRIMERGY スイッチブレード / コンバージドファブリックスイッチブレード (10Gbps 18/8+2)	-	○	○	-
CFX2000F/R	-	○	○	-
AsetekRackCDU	-	-	○	-
SchneiderElectric Metered RackMountPDU	-	-	○	-
SchneiderElectric Smart-UPS	-	-	○	-

動作確認済みのモデルについては、当社の本製品 Web サイトで「管理対象機器一覧」を参照してください。

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

rviewism/environment/

（※1）アクセス権限が Administrator、または OEM を持つアカウントをご使用ください。

（※2）SNMP v1 または v2 の場合は、コミュニティー名の入力が必須です。SNMP v3 の場合は、ユーザー名、セキュリティレベル、認証プロトコル(認証使用時)、認証パスワード(認証使用時)、暗号化プロトコル(暗号化使用時)、暗号化パスワード(暗号化使用時) の入力が必須です。

（※3）シャーシ(MMB)の接続情報設定が必要となります。

（※4）アカウント/パスワードは IPMI と同じものが使用されます。HTTPS のポート番号のみ指定することができます。

2.2.2 管理のために必要な設定

接続情報の設定に加えて、以下の設定を行ってください。

【PRIMERGY】

・PRIMERGY S8/M1/M2/M3 世代のサーバ にて iRMC S4 ファームウェアの版数が 9.00 以上をご使用の場合、ISM のノード詳細の SAS カードについての情報を取得するためには、iRMC の Web UI の IPMI 権限/許可 の変更が必要です。変更は以下のように行います。

[ユーザ管理] - [iRMC S4 ユーザ管理] - [IPMI 権限/許可] - [Redfish Enabled] をチェック。

[ユーザ管理] - [iRMC S4 ユーザ管理] - [IPMI 権限/許可] - [Redfish Role] を Administrator に変更。

【SR-X】

・LLDP 設定を有効にしてください。

【VDX(Brocade VDX)】

・LLDP 設定を有効にしてください。

・スイッチごとに管理 LAN ポートの IP アドレスを設定してください。

【ETERNUS DX/AF】

・ISM と接続するためのポートは、Control Module のメンテナンスポートをご使用ください。
（リモートポートに接続した場合、ファームウェアアップデート機能、ログ収集機能、および プロファイル適用機能が動作しない場合があります。）

【PRIMEQUEST 2000 Type3、PRIMEQUEST 3000E】

・ISM の MMB のアカウント設定(IPMI 接続のアカウント設定)では、PRIMEQUEST の Web UI の［Network Configuration］-［Remote Server Management］ に登録したアカウントをご使用ください。

・ISM の SSH のアカウント設定では、PRIMEQUEST の Web UI の［User Administration］-［User List］に登録したアカウントをご使用ください。その際 Privilege は Admin または CE である必要があります。

【PRIMERGY BX】

・スイッチブレード:　LLDP 設定を有効にしてください。

・ファイバーチャネルスイッチブレード:　SW-MIB を有効にしてください。

実行例）

```
snmpconfig --enable mibCapability -mib_name SW-MIB
```

・シャーシの電源が OFF の場合、MMB から情報が取得できません。それにより、サーバブレード、コネクションブレードとの関係性が一時的に解除されて見えます。電源が ON 状態になってからシャーシを選択し、[アクション] - [ノード情報取得]の操作を実施してください。

2.2.3 通知のために必要な設定

接続情報 および、管理のために必要な情報の設定に加えて、SNMP トラップの設定を行ってください。詳細については各機器のマニュアルを参照してください。

なお、以下の機器では ISM のトラップ通知受信設定で対象ノードを選択した際に、エンジン ID が自動的に入力されます。

対応機器　　○：対応、−：非対応

ノード	エンジン ID の自動入力
PRIMERGY(RX/CX/TX)	○
PRIMEQUEST 2000Type3	−
PRIMEQUEST 3000E	○
PRIMEQUEST 3000B	○
ETERNUS DX/AF	○
ETERNUS NR	−
SR-X	○ （※1）
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)	○
VDX(Brocade VDX)	○
Brocade FC スイッチ	○
Cisco Catalyst	○
Cisco Nexus	○
PRIMERGY BX シャーシ (MMB)	−
PRIMERGY BX サーバブレード	○
PRIMERGY BX スイッチブレード(1Gbps/10Gbps)	○ （※1）
PRIMERGY BX LAN パススルーブレード	−
PRIMERGY BX FC スイッチブレード	○
PRIMERGY スイッチブレード / コンバージドファブリック スイッチブレード(10Gbps 18/8+2)	○ （※1）（※2）
CFX2000F/R	○ （※1）（※2）
AsetekRackCDU	−
SchneiderElectricMetered RackMountPDU	−
SchneiderElectricSmart-UPS	−

（※1）以下の機器に対して SNMP v3 engine ID を設定しない場合、ISM のトラップ通知受信設定で対象ノードを選択した際に、エンジン ID が自動的に入力されません。

自動的に入力されるようにするには､機器に対して事前に snmpv3 engine ID を設定してください。

- PRIMERGY BX スイッチブレード(10Gbps)
- PRIMERGY スイッチブレード / コンバージドファブリックスイッチブレード(10Gbps 18/8+2)
- CFX2000F/R
- SR-X

(※2) ファブリックを組み、かつ、機器に対して SNMP v3 engine ID を設定している場合、ファブリック全体で engine ID を同じ値に設定してください。

第 3 章　　その他の設定詳細

3.1　ETERNUS DX/AF ドライブエンクロージャの表示

ISM は、ETERNUS DX/AF のコントローラーエンクロージャに接続されているドライブエンクロージャをノードとして管理します。

ここではドライブエンクロージャの管理をするために必要な設定にてついて情報を提供します。

3.1.1 ドライブエンクロージャの登録

ドライブエンクロージャは、以下の手順によって自動的に ISM にノード登録されます。

(1) ドライブエンクロージャが接続されている ETERNUS DX/AF のコントローラーエンクロージャを ISM にノード登録します。

(2) コントローラーエンクロージャのノード情報取得が完了すると、ドライブエンクロージャがノードリストに表示されます。

3.1.2 ドライブエンクロージャのノード詳細情報

ISM では、ドライブエンクロージャのノード詳細情報はコントローラーエンクロージャのノード詳細情報に表示します。

3.1.3 ドライブエンクロージャのステータス

ドライブエンクロージャのステータスは常に Unknown が表示されます。ドライブエンクロージャはコントローラーエンクロージャによって集約管理されているため、コントローラーエンクロージャのステータスを参照してください。

3.1.4 ドライブエンクロージャの削除

ドライブエンクロージャは、以下の場合にノードリストから削除されます。

・ドライブエンクロージャがコントローラーエンクロージャから切断された後に、コントローラーエンクロージャのノード情報取得が実行された場合

・ISM からコントローラーエンクロージャのノードを削除した場合

3.2　ファームウェアアップデート時間の目安

ISM のファームウェア管理機能を使用したファームウェアのアップデートには、長時間を要する場合があります。ここではファームウェアアップデートに要する時間の目安を提示します。

ファームウェアアップデートの作業計画を立てる際は以下の時間を参考にしてください。また、ファームウェアアップデート完了前に中断しないでください。

注意

以下に記載された時間は現行ファームウェアを標準的な構成でアップデートした際の時間です。ファームウェア版数や、ネットワーク構成、ネットワーク負荷状態などで変動する場合がありますので、作業計画を立てる際には万一のトラブル発生時の対応時間も含め、十分な余裕を持った設計を推奨します。

ファームウェアアップデート時間の目安

アップデート対象	1 台当たりの目安	備考
PRIMERGY の iRMC ファームウェアアップデート	Online アップデート 10～20 分	
	Offline アップデート 15～30 分	ファームウェアを適用後、サーバの電源がオンになる設定にしている場合、さらに 15 分必要。
PRIMERGY の BIOS ファームウェアアップデート	Online アップデート 1～2 分	ファームウェアを適用するためにサーバの電源オフ・オン操作の時間が別途必要。
	Offline アップデート 15～30 分	ファームウェアを適用後、サーバの電源がオンになる設定にしている場合、さらに 15 分必要。
PRIMEQUEST 3800B の iRMC ファームウェアアップデート	Online アップデート 10～20 分	
PRIMEQUEST 3800B の BIOS ファームウェアアップデート	Online アップデート 5～15 分	ファームウェア適用にはサーバの電源オフ・オン操作の時間が別途必要。
PRIMEQUEST 2000 シリーズ、3000 シリーズの本体ファームウェアアップデート	70～130 分	
PRIMERGY BX900S2 MMB	10～20 分	左記は MMB 1 枚当たりの時間。
ネットワークスイッチ SR-X のファームウェアアップデート	2～10 分	
ファブリックスイッチ CFX2000R/F、コンバージドファブリックスイッチブレードのファームウェアアップデート	10～20 分	
コンバージドスイッチ VDX のファームウェアアップデート	15～30 分	
イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6) のファームウェアアップデート	20～30 分	
LAN スイッチブレードのファームウェアアップデート	10～20 分	
Cisco Systems Nexus シリーズのファームウェアアップデート	30～50 分	
Cisco Systems Catalyst シリーズのファームウェアアップデート	10～20 分	
FC スイッチブレードのファームウェアアップデート	10～20 分	
PCI カードのファームウェアアップデート	Online アップデート 5～15 分	ファームウェア適用でサーバの電源オフ・オン操作の時間が別途必要。左記はカード 1 枚当たりの時間。
	Offline アップデート 15～20 分	左記はカード 1 枚当たりの時間。
ETERNUS DX/AF シリーズのファームウェアアップデート	10～60 分	ユニファイド機構有り、またコントローラーエンクロージャ多数搭載の場合、アップデート時間が長くなる。

3.3　ログ管理機能利用時のディスク消費量の目安

ログ管理機能を利用し、ノードからログを定期的に収集して ISM-VA 上に蓄積できます。ここでは収集したログの蓄積場所、および蓄積されるデータ量の目安に関する情報を提供します。

収集したログはユーザーグループに割り当てられている仮想ディスク上のログ保存領域に蓄積されます。ISM-VA の各ユーザーグループへの仮想ディスク割り当ての参考にしてください。

注意

・ログ保有期間、世代数はデフォルトで以下が設定されています。

必要に応じてログ保有期間、世代数を変更してください。

保管ログ	ノードログ（ダウンロード用データ / ログ検索用データ）
7 世代	30 日

・本書に記載された容量は特定の構成・運用を行った場合の参考値です。実際の使用状況により大きく異なる場合があります。

3.3.1 管理するログの種別および蓄積場所について

ログ管理機能はログを収集した際、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）を作成します。

各ログは、それぞれ以下のログ保存領域に蓄積されます。

ログ種別	保存領域
保管ログ	ノードが所属するノードグループが関連付けられているユーザーグループのログ保存領域（※1）
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）	Administrator グループのログ保存領域（※2）

（※1）ノードグループがユーザーグループに関連付けられていない場合は、Administrator グループのログ保存領域に蓄積されます。

（※2）全てのノードのノードログ（ログ検索用データ）が Administrator グループのログ保存領域に蓄積されます。ノードグループが Administrator グループ以外のユーザーグループに関連付けられている場合も Administrator グループのログ保存領域に蓄積されます。

3.3.2 ログ容量の目安

【保管ログの容量】

1 ノードあたりの 1 世代の目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY	1KB
		PRIMEQUEST 3000B	1KB
		IPCOM VX2	1KB
	Chassis	PRIMERGY BX	100KB
		PRIMEQUEST 3000E	50KB
	Connection Blade	Ethernet Switch	100KB
		Fibre Channel Switch	10MB
	Switch	SR-X	50KB
		CFX	100KB
		イーサネットスイッチ 10GBASE-T 48+6 / 10GBASE 48+6)	350KB
		VDX(Brocade VDX)	50MB
		Cisco Catalyst	1MB
		Cisco Nexus	1MB
	Storage	ETERNUS DX/AF	10MB
		ETERNUS NR (NetApp) Cluster	100KB
		ETERNUS NR (NetApp) Chassis	500MB
オペレーティングシステム	Windows		5MB
	Linux		5MB
	VMware ESXi		3MB
	IPCOM OS		50MB
ServerView Suite	ServerView Agents		Windows：10MB Linux：80MB
	ServerView Agentless Service		
	ServerView RAID Manager		

【ノードログ(ダウンロード用データ)の容量】

1 ノードあたりの 30 日間分の目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY	50KB
		PRIMEQUEST 3000B	50KB
		IPCOM VX2	50KB
	Chassis	PRIMERGY BX	50KB
		PRIMEQUEST 3000E	50KB
	Connection Blade	Ethernet Switch	100KB
		Fibre Channel Switch	50KB
	Switch	SR-X	100KB
		CFX	100KB
		イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6)	150KB
		VDX(Brocade VDX)	100KB
		Cisco Catalyst	50KB
		Cisco Nexus	50KB
	Storage	ETERNUS DX/AF	100KB
		ETERNUS NR (NetApp) Cluster	200KB
オペレーティングシステム	Windows		1MB
	Linux		1MB
	VMware ESXi		4MB
	IPCOM OS		1MB

【ノードログ(検索用データ)の容量】

1 ノードあたりの 30 日間分の目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY	500KB
		PRIMEQUEST 3000B	500KB
		IPCOM VX2	500KB
	Chassis	PRIMERGY BX	500KB
		PRIMEQUEST 3000E	500KB
	Connection Blade	Ethernet Switch	1MB
		Fibre Channel Switch	500KB
	Switch	SR-X	1MB
		CFX	1MB
		イーサネットスイッチ 10GBASE-T 48+6 / 10GBASE 48+6)	1MB
		VDX(Brocade VDX)	1MB
		Cisco Catalyst	500KB
		Cisco Nexus	500KB
	Storage	ETERNUS DX/AF	1MB
		ETERNUS NR (NetApp) Cluster	2MB
オペレーティングシステム	Windows		15MB
	Linux		15MB
	VMware ESXi		50MB
	IPCOM OS		15MB