

# FUJITSU Server PRIMEQUEST 2000シリーズ Windowsネットワーク設計ガイド

C122-A019-10

- はじめに
- 1. 前提知識
  - 1.1 基本的なネットワーク構成と設計概要
  - 1.2 最大ネットワーク構成
  - 1.3 管理LAN/保守用LAN/Internal LAN/BMC-MMB間LANとは
  - 1.4 業務LAN/クラスタインタコネクトとは
- 2. ネットワークコンポーネント
  - 2.1 管理LAN/保守用LANを構成する主要コンポーネント
  - 2.2 業務LANを構成するコンポーネント

- 3. ネットワーク構成設計
  - 3.1 ネットワーク構成の考え方
  - 3.2 ネットワークの構成設計手順
  - 3.3 Active Directory環境での考慮
  - 3.4 管理LANと業務LANの構成設計
  - 3.5 ネットワークの信頼構成設計
  - 3.6 IPアドレスの割り当て
  - 3.7 Internal LANの設計
  - 3.8 時刻同期
- 4. 構成例
  - 4.1 ネットワーク構成例

- 5. iSCSI接続におけるネットワーク設計
  - 5.1 iSCSI接続の構成パターン
  - 5.2 iSCSI接続時の考慮
  - 5.3 iSCSIイニシエータの設計
  - 5.4 iSCSI接続におけるマルチパスドライバの考慮
- 6. FCoE接続におけるネットワーク設計
  - 6.1 FCoE接続の構成パターン
  - 6.2 FCoE接続時の考慮

- 付録A. LANポートの接続先確認方法
  - A.1 LANポートの接続先確認方法
- 付録B. チーミングソフトウェア
  - B.1 PRIMECLUSTER GLS for Windows(PRIMEQUEST)
- 付録C. ハードウェア監視のためのネットワーク設計
  - C.1 ハードウェア監視方法
  - C.2 MMB/BMC+SVASによるハードウェア監視
  - C.3 SV Agents/SV RAIDによるハードウェア監視
  - C.4 Windowsファイアウォールの設計

## ■ 本文中の略称

名称	略称	
Microsoft® Windows Server® 2008 R2 Standard	Windows Server 2008	Windows
Microsoft® Windows Server® 2008 R2 Enterprise		
Microsoft® Windows Server® 2008 R2 Datacenter		
Microsoft® Windows Server® 2012 Standard	Windows Server 2012	
Microsoft® Windows Server® 2012 Datacenter		
Microsoft® Windows Server® 2012 R2 Standard		
Microsoft® Windows Server® 2012 R2 Datacenter		
Microsoft® Windows Server® 2016 Standard	Windows Server 2016	
Microsoft® Windows Server® 2016 Datacenter		

## ■ 本文中の略称

名称	略称	
PRIMEQUEST 2400S Lite	PRIMEQUEST 2400S Lite / 2400S / 2400E / 2400L / 2800E / 2800L	PRIMEQUEST 2000シリー ズまたは PRIMEQUEST
PRIMEQUEST 2400S		
PRIMEQUEST 2400E		
PRIMEQUEST 2400L		
PRIMEQUEST 2800E		
PRIMEQUEST 2800L		
PRIMEQUEST 2400S2 Lite	PRIMEQUEST 2400S2 Lite / 2400S2 / 2400E2 / 2400L2 / 2800E2 / 2800L2	
PRIMEQUEST 2400S2		
PRIMEQUEST 2400E2		
PRIMEQUEST 2400L2		
PRIMEQUEST 2800E2		
PRIMEQUEST 2800L2		
PRIMEQUEST 2400S3 Lite	PRIMEQUEST 2400S3 Lite / 2400S3 / 2400E3 / 2400L3 / 2800E3 / 2800L3	
PRIMEQUEST 2400S3		
PRIMEQUEST 2400E3		
PRIMEQUEST 2400L3		
PRIMEQUEST 2800E3		
PRIMEQUEST 2800L3		

## ■ 本文中の略称

名称	略称
システムボード	SB
マネジメントボード	MMB
Baseboard Management Controller	BMC
I/Oユニット	IOU
Converged Network Adapter	CNA
Fiber Channel over Ethernet	FCoE
Web User Interface	Web-UI
Field Support Tool	FST
One-stop Solution Center	OSC
Remote Customer Support System	REMCS
ServerView Suite	SVS
ServerView Agentless Service	SVAS
ServerView Operations Manager	SVOM
ServerView Agents	SV Agents
ServerView RAID Manager	SV RAID
SMB	Server Message Block
STP	Spanning Tree Protocol



## ■ 本文中の略称

名称	略称
FUJITSU Server PRIMEQUEST 2000シリーズ 導入マニュアル	導入マニュアル
FUJITSU Server PRIMEQUEST 2000シリーズ 運用管理マニュアル	運用管理マニュアル
FUJITSU Server PRIMEQUEST 2000シリーズ 構成設計ガイド	構成設計ガイド
FUJITSU Server PRIMEQUEST 2000 シリーズ FCoE ブート環境構築マニュアル	FCoE Boot 環境構築マニュアル
FUJITSU Server PRIMEQUEST 2000シリーズシステム構成図 (PRIMEQUEST 2400S Lite / 2400S / 2400E / 2400L / 2800E / 2800L)	システム構成図
FUJITSU Server PRIMEQUEST 2000シリーズシステム構成図 (PRIMEQUEST 2400S2 Lite / 2400S2 / 2400E2 / 2400L2 / 2800E2 / 2800L2)	
FUJITSU Server PRIMEQUEST 2000シリーズシステム構成図 (PRIMEQUEST 2400S3 Lite / 2400S3 / 2400E3 / 2400L3 / 2800E3 / 2800L3)	
FUJITSU Server PRIMEQUEST 2000シリーズ Windowsディスク設計ガイド	Windowsディスク設計ガイド
Windows Server 2008/2008 R2/2012/2012 R2/2016 大容量メモリダンプ ファイル設計ガイド	大容量メモリダンプファイル設計ガイド
Windows Server 2008/2008 R2/2012/2012 R2 DHCP、DNS 構築・運用 ガイド	DHCP、DNS 構築・運用ガイド

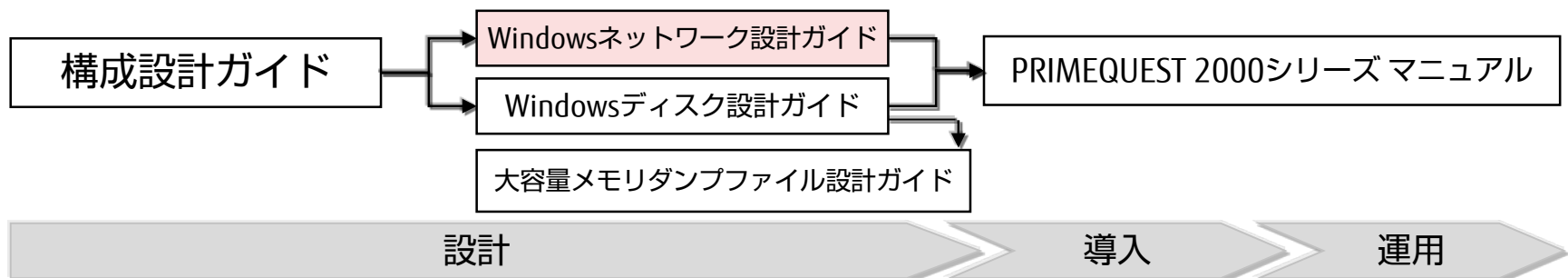
## ■ 本書の読み方

### ■ 本書の内容

PRIMEQUEST 2000シリーズでWindowsを使用される方を対象に、ネットワーク設計の考え方、留意事項などについて記載しています


- 具体的な操作などの情報については、PRIMEQUEST 2000シリーズ本体のマニュアルを参照してください
- 外部アレイディスク装置や各種スイッチの説明は、特筆がなければETERNUSなどの富士通製品を示しています
- サポートOSについてはFUJITSU Server PRIMEQUEST 2000シリーズ Windows Server情報のサポート情報を参照してください  
<http://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/os/windows/>
- サポートするシステム構成や周辺機器についてはFUJITSU Server PRIMEQUEST 2000シリーズのシステム構成図を参照してください  
<http://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/catalog/#material>
- 各ミドルウェアのサポートOS確認状況についてはOSへの対応状況および動作確認情報を参照してください  
<http://www.fujitsu.com/jp/products/software/resources/condition/syskou/>

### ガイド間の記事の流れ



## ■ 本文中の記号

本文中に記載されている記号には、次のような意味があります

記号	意味
	参照ページや参照ドキュメントを示しています。

- ・Microsoft、Windows、Windows Server、Active Directory、Hyper-Vは、米国 Microsoft Corporationの米国およびその他の国における登録商標または商標です
- ・Intelは、米国インテル社の登録商標および商標です
- ・Emulexは、米国Emulex Corporationの登録商標です
- ・その他、会社名と製品名は、それぞれ各社の商標または登録商標です
- ・本資料に記載されているシステム名、製品名等には、必ずしも商標表示（(R)、TM）を付記していません

## ■ Windows Server 2016を使用する場合

PRIMEQUEST2000シリーズでWindows Server 2016を使用する場合は、2017/3/21の累積的な更新プログラム（KB4015438）もしくはそれ以降の累積的な更新プログラムを適用してください。

- March 20, 2017-KB4015438 (OS Build 14393.969)

<https://support.microsoft.com/en-us/help/4015438/>

留意事項の詳細は『FUJITSU Server PRIMEQUEST 2000シリーズ Windows Server 2016 留意事項』を参照してください。

- FUJITSU Server PRIMEQUEST 2000シリーズ Windows Server 2016 留意事項  
<http://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/os/windows/support/2016/consideration/index.html>

# 1. 前提知識

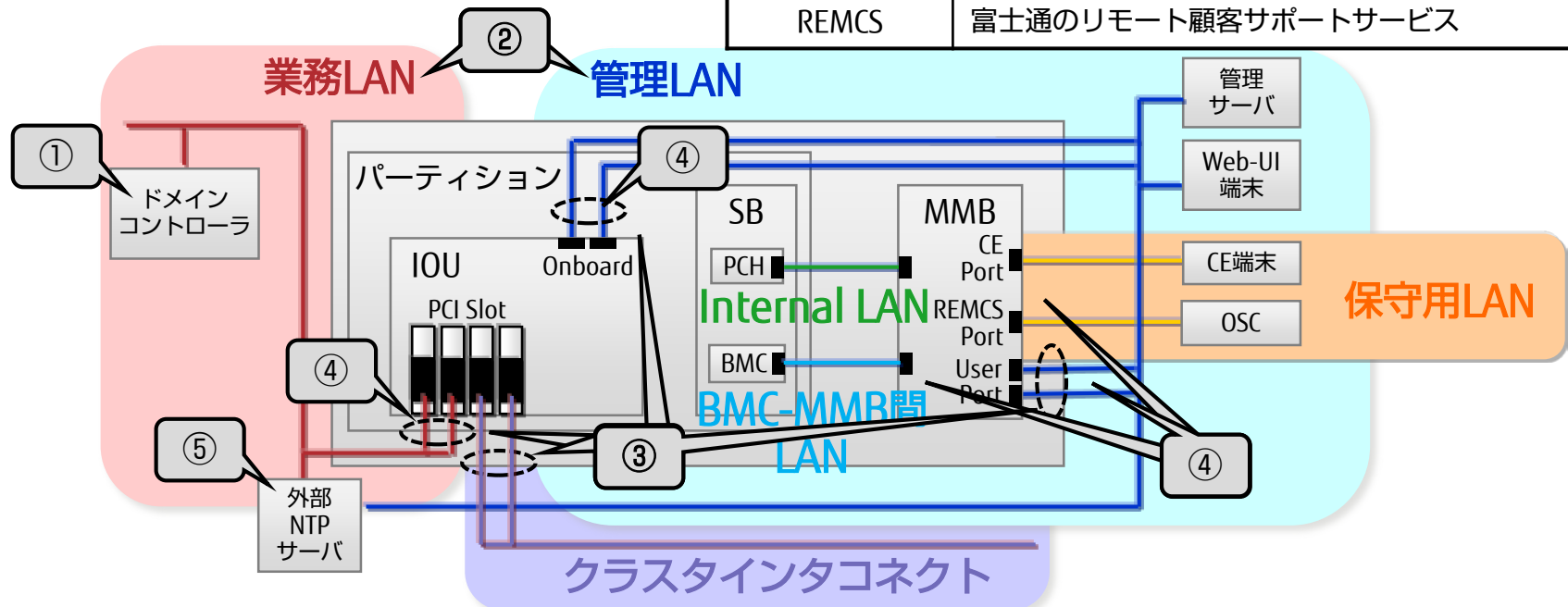
PRIMEQUESTにおけるネットワーク基礎技術を説明します

# 1.1 基本的なネットワーク構成と設計概要

## ■ 次の項目を設計する

- ① Active Directory環境の考慮
- ② 管理LANと業務LANの構成設計
- ③ ネットワークの信頼構成設計
- ④ IPアドレス割り当て
- ⑤ 時刻同期

用語	説明
PCH	チップセットの構成要素で、USBやPCIバスなど結びつけるインターフェースを持つ
BMC	システム管理用コントローラ。MMBと連携してハードウェアの制御/監視を行う
IOU	入出力制御ユニット、オンボードI/OとPCIカード搭載
パーティション	分割した独立したシステムを稼働させる単位
OSC	富士通のお客様総合サポートセンター
REMCS	富士通のリモート顧客サポートサービス



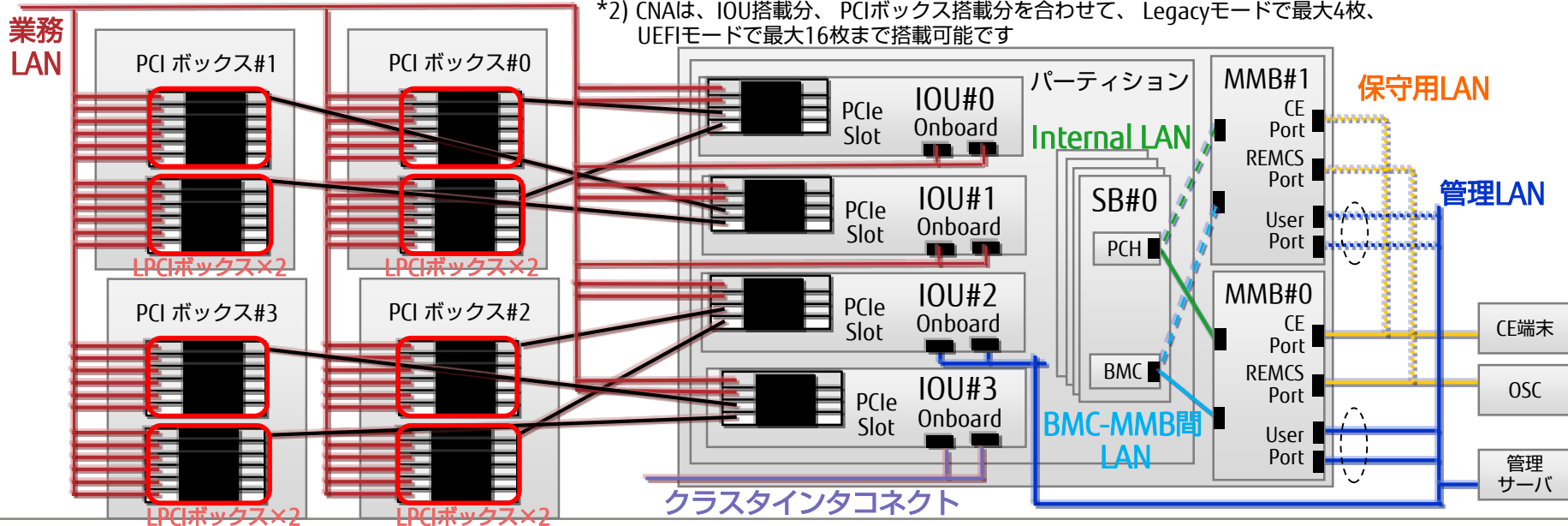
PRIMEQUESTの外部ネットワークについては『運用管理マニュアル 第1章 ネットワーク環境の設定と管理ツールの導入』を参照

# 1.2 最大ネットワーク構成

## ■ 最大ネットワーク構成(PRIMEQUEST 2800E3/4SB 4IOU 1パーティションの場合)

ポート名		接続コンポーネント	最大ポート数/搭載カード数	用途
管理 LAN	Userポート	MMB(*1)	2ポート	MMB Web-UI操作用
	管理サーバ用LAN	業務LANと同一コンポーネント	-	監視や管理、バックアップ用
保守用 LAN	CEポート	MMB(*1)	1ポート	保守専用の端末接続用
	REMCSポート		1ポート	REMCS 用
Internal LAN		MMB(*1)	-	パーティション-MMB 間通信用
BMC-MMB間LAN		BMC	-	BMC-MMB間通信用
業務LAN		IOUのオンボードLAN	8ポート	お客様の業務用
		IOUのPCIeスロットに挿すLANカード/CNA	8枚(*2)	
		PCIボックスのPCIeスロットに挿すLANカード/CNA	48枚(*2)	
クラスタインタコネク		業務LANと同一コンポーネント	-	クラスタノード間の監視用

\*1) MMB#1はオプション搭載となります。MMB#1を追加搭載して二重化した場合は、Active側のMMBでのみ通信します  
 \*2) CNAは、IOU搭載分、PCIボックス搭載分を合わせて、Legacyモードで最大4枚、UEFIモードで最大16枚まで搭載可能です





# 1.3 管理LAN/保守用LAN/Internal LAN/BMC-MMB間LANとは

## ■ 管理LAN

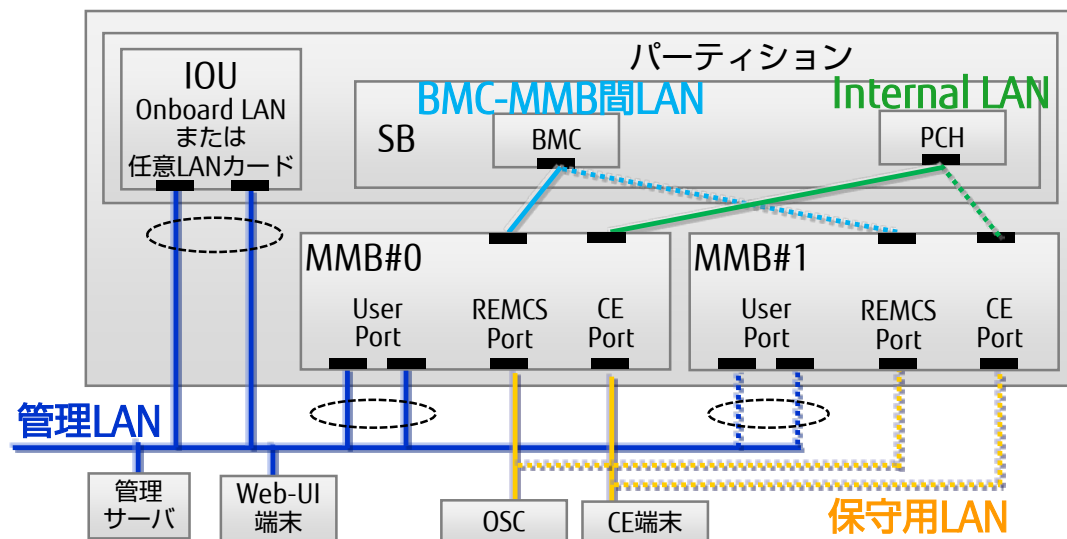
- Web-UI端末や管理サーバとPRIMEQUEST内の各パーティションおよびパーティション同士を接続するLAN

## ■ 保守用LAN

- 保守作業のために、CE端末やOSCとPRIMEQUESTを接続するLAN

## ■ Internal LAN(\*1)

- パーティション側に導入したREMCS OptionがMMBと通信するための、パーティションとMMB間の内部通信用LAN



\*1) 統合ファームウェアBB15074版以降、UEFIメニュー[PCI Subsystem Configuration]でInternal LANを有効/無効に設定できますが、Windowsでは既定値：有効(Enabled)のまま利用してください。

## ■ BMC-MMB間LAN

- BMCの遠隔操作機能で利用する、パーティションとMMB間の内部通信用LAN

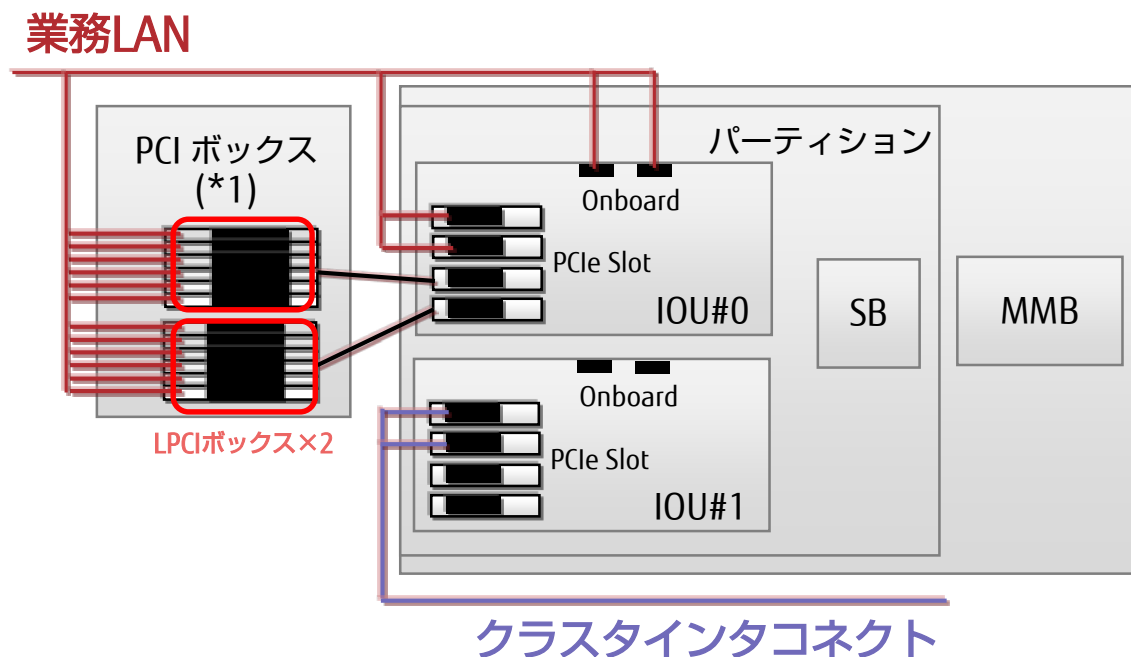
# 1.4 業務LAN/クラスタインタコネクトとは

## ■ 業務LAN

- お客様業務で利用するLAN

## ■ クラスタインタコネクト

- クラスタ構成時に、クラスタノード間の監視などに利用するLAN



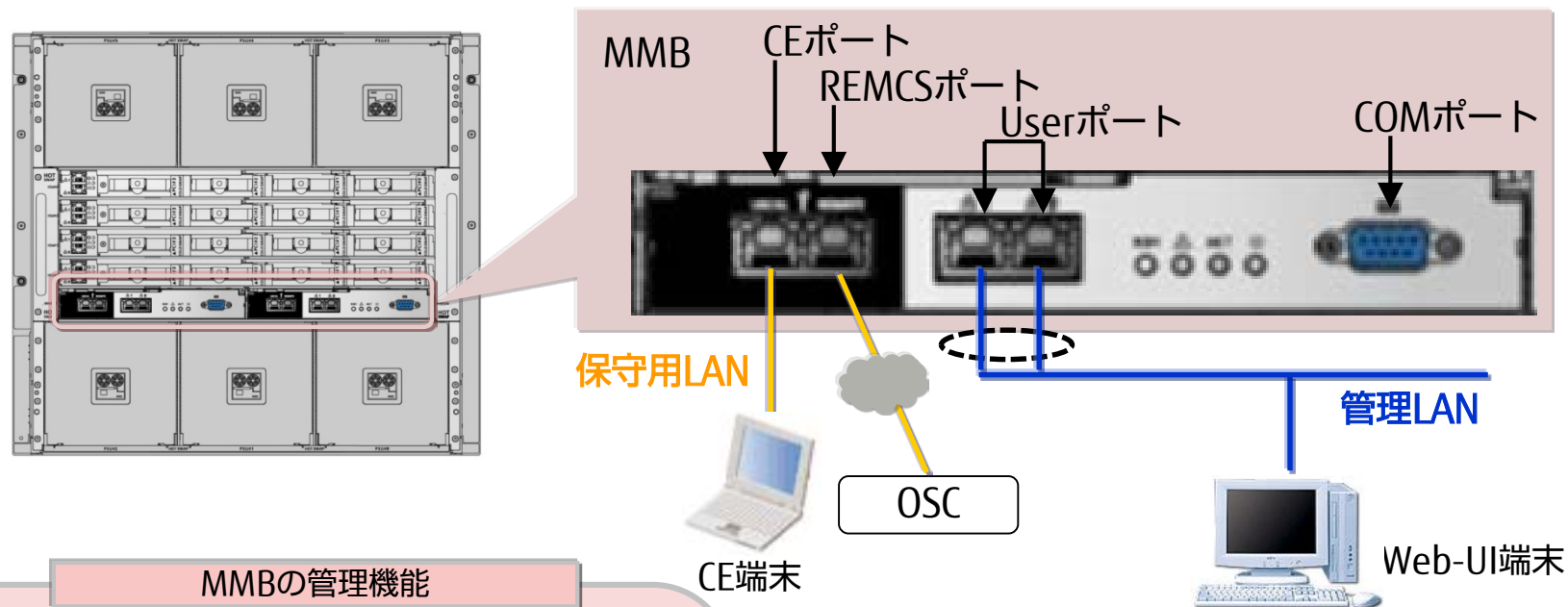
\*1) PCIボックスの内部は6スロットずつ2分割されており、LPCIボックスとして別々にIOUと接続されます

## 2. ネットワークコンポーネント

ネットワークを構成するコンポーネントについて説明します

## 2.1 管理LAN/保守用LANを構成する主要コンポーネント

### ■ MMB(筐体内のハードウェア全体を管理するためのユニット)



#### MMBの管理機能

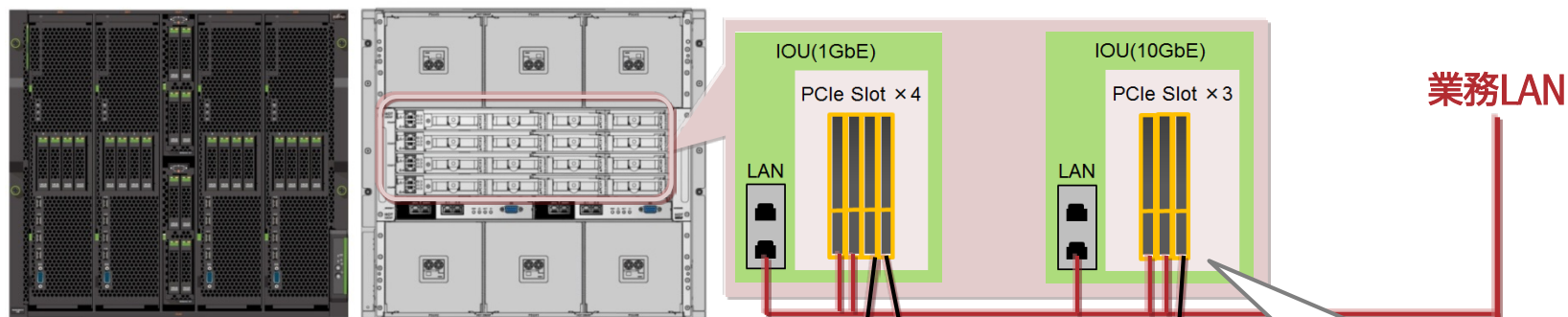
システム管理機能、ハードウェア監視、  
電源制御、システム管理のためのWeb-UI機能、  
ビデオリダイレクション機能、  
テキストコンソールリダイレクション機能、  
パーティション制御、システム初期化  
ユーザー権限管理、電源スケジュール運転、  
各種ファームウェアの保守、  
設定情報のセーブ・リストア など

外部インターフェース	数	内容
シリアルインターフェース COMポート	1	CEの装置セットアップ作業で使用
LAN	4	<ul style="list-style-type: none"> <li>• Userポート 1Gbps×2ポート</li> <li>• CE用ポート 100Mbps×1ポート</li> <li>• REMCS用ポート 100Mbps×1ポート</li> </ul>

# 2.2 業務LANを構成する主要コンポーネント

## ■ IOU(SBと他のコンポーネントや外部装置を接続するためのユニット)

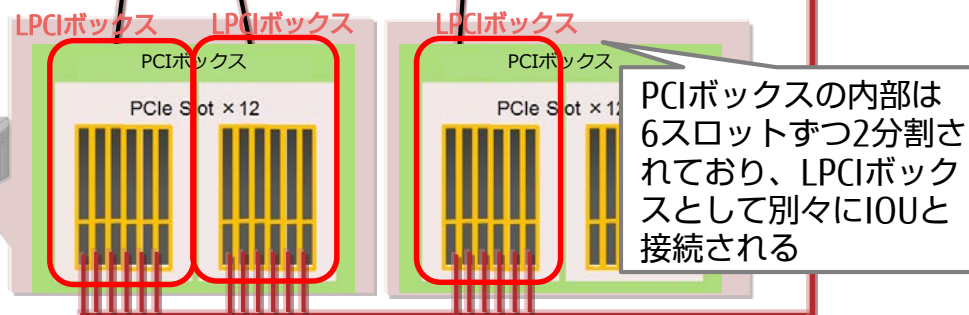
コンポーネント	オンボードLAN	LANカード /CNA(*1)	PCIボックス 接続カード
IOU(1GbE)	1GbE 2ポート	最大4枚	最大2枚
IOU(10GbE)	10GbE 2ポート	最大3枚	最大1枚



## ■ PCIボックス (拡張I/O筐体)

コンポーネント	LANカード/CNA(*1)
PCIボックス	最大6枚 (PCIボックス接続カード1枚あたり)

\*1) Legacyモードの場合  
CNAは1パーティションあたり最大4枚まで搭載可能です。  
UEFIモードの場合  
CNAは1パーティションあたり最大16枚まで搭載可能です。



これらのコンポーネントはパーティション側の管理LAN/クラスタインタコネクトを構成することも可能

# 3. ネットワーク構成設計

Windowsにおけるネットワーク構成設計の考え方を説明します

# 3.1 ネットワーク構成の考え方

- 管理LAN、保守用LAN、および業務LANのネットワークは必ず用途別に分離する

- 保守用端末接続時には顧客ネットワークに接続しない

- iSCSI利用の場合は専用LANを設け、管理LAN、保守用LAN、および業務LANとの分離を推奨する

iSCSI接続の詳細は『[5. iSCSI接続におけるネットワーク設計](#)』を参照

## ■ ネットワーク接続形態

セグメント		構成の考え方
管理LAN	管理サーバ用LAN	分離必須
	Userポート	
保守用LAN	REMCS用ポート /ICE用ポート	分離必須
業務LAN		分離必須
iSCSI LAN		分離推奨

# 3.2 ネットワークの構成設計手順

## ■ 次の順にネットワークを設計する

項番	手順	説明	設計の対象		
			管理LAN	保守用LAN	業務LAN
3.3	Active Directory環境での考慮	<ul style="list-style-type: none"><li>• NTPサーバとDNSサーバの考慮</li><li>• ドメイン メンバサーバの時刻同期の方法</li></ul>	○	—	○
3.4	管理LANと業務LANの構成設計	<ul style="list-style-type: none"><li>• 管理LANと業務LANのネットワークを分離する</li><li>• 利用するLANポートの決定</li></ul>	○	—	○
3.5	ネットワークの信頼構成設計	<ul style="list-style-type: none"><li>• 接続するネットワークを二重化構成にする</li><li>• PRIMEQUEST搭載のネットワークコンポーネントを冗長化</li><li>• チューニングソフトウェアを選択</li></ul>	○	—	○
3.6	IPアドレスの割り当て	IPアドレスを決定	○	○	○
3.7	Internal LANの設計	Internal LANのIPアドレスを設計	○	—	—
3.8	時刻同期	外部NTPサーバを決定	○	—	○

## ■ 必要に応じてiSCSI接続用のネットワークを設計する



# 3.3 Active Directory環境での考慮

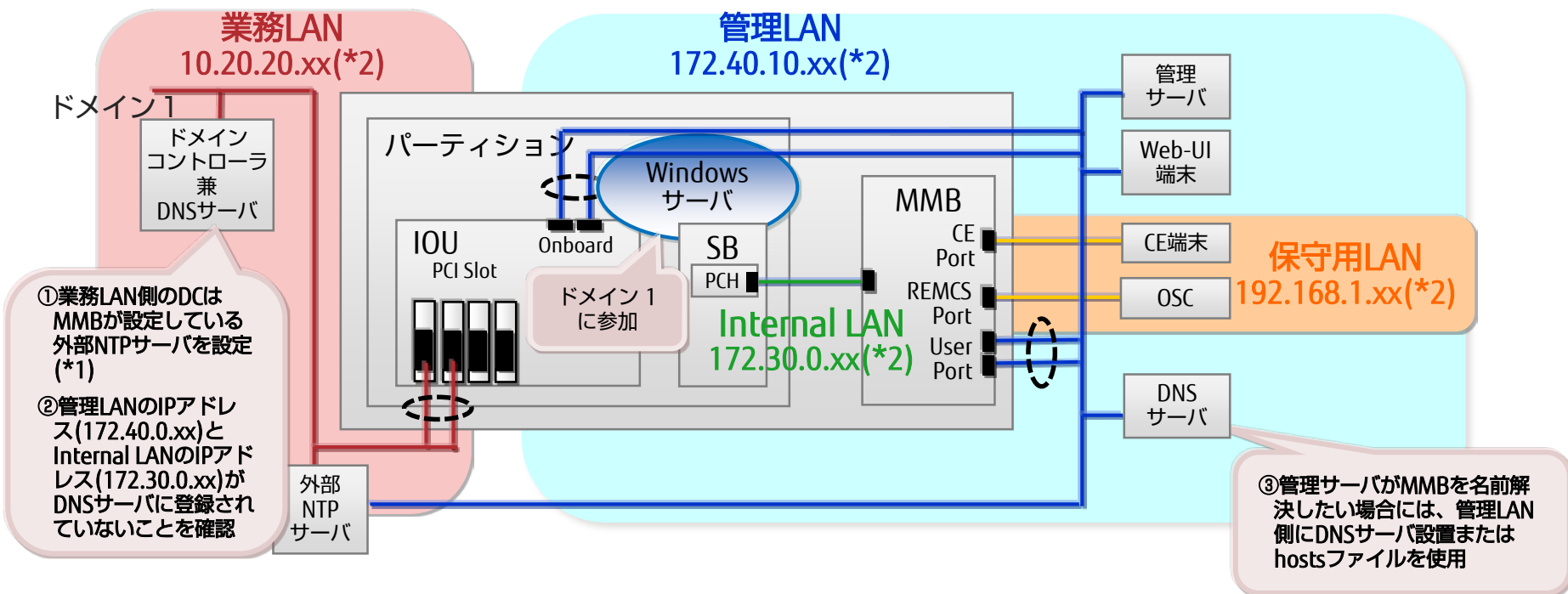
- NTPサーバとDNSサーバの考慮
- ドメイン メンバサーバの時刻同期の方法

## 3.3.1 NTPサーバとDNSサーバの考慮(1/2)

### ■ 業務LAN側のみドメインコントローラを配置する場合

- ① 業務LAN側のドメインコントローラはMMBが設定している外部NTPサーバを設定する(\*1)
- ② 管理LANとInternal LANのIPアドレス(Aレコード)が、業務LAN上のDNSサーバ(DC)に登録されていないことを確認する
- ③ 管理サーバがMMBを名前解決したい場合には、管理LAN側にDNSサーバ設置または、hostsファイルを使用する

☞ 複数のネットワークを設定したマルチホームコンピュータにおけるDNS動的登録については『DHCP、DNS 構築・運用ガイド』を参照



\*1) 同一の外部NTPサーバでなくとも時刻が同期されたNTPサーバであれば設定できます

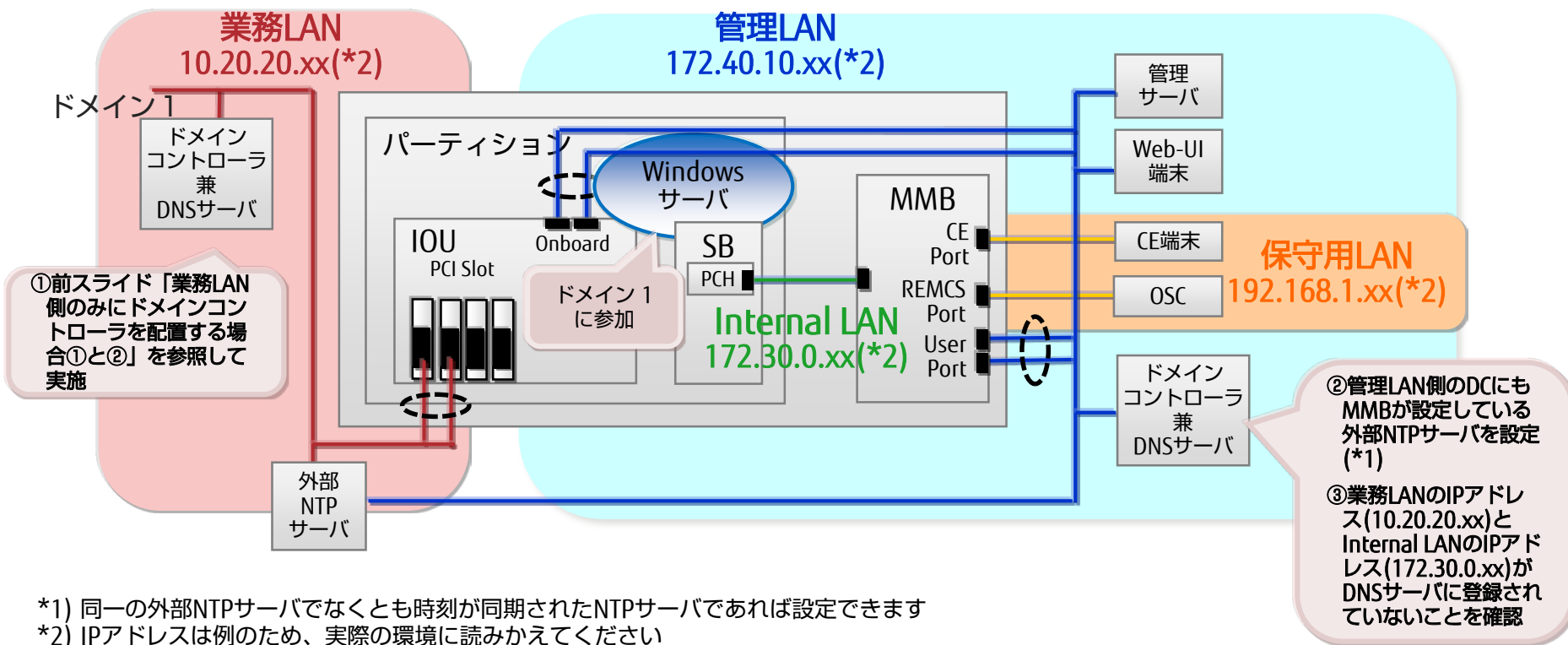
\*2) IPアドレスは例のため、実際の環境に読みかえてください

## 3.3.1 NTPサーバとDNSサーバの考慮(2/2)

### ■ 管理LAN側にもドメインコントローラを配置する場合

利用シーン：複数台のPRIMEQUESTを設置するさいに、管理LAN側ドメイン(業務LAN側とは異なるドメイン)でシステム管理者アカウントを一括管理する

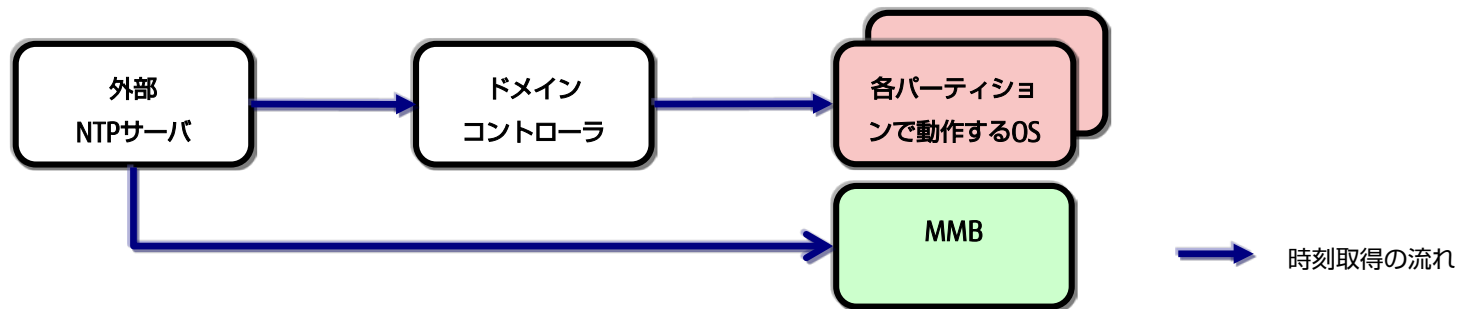
- ① 前スライド「業務LAN側だけにドメインコントローラを配置する場合①と②」を実施する
- ② 管理LAN側のドメインコントローラにもMMBが設定している外部NTPサーバを設定する(\*1)
- ③ 業務LANとInternal LANのIPアドレス(Aレコード)が、管理LAN上のDNSサーバ(DC)に登録されていないことを確認する



### ■ 時刻同期について次の考慮が必要

MMBと各パーティションで動作するOSの時刻が同期されるように設計する

- ドメインに参加しているメンバサーバは、自動的にドメインコントローラと時刻同期を行う。ドメインコントローラとMMBは同じ外部NTPサーバを参照させるなど、時刻を同期させる



👉 MMBを時刻同期させる方法は『[3.8 時刻同期](#)』を参照

👉 ドメインコントローラを外部NTPサーバと時刻同期させる方法は、以下のマイクロソフトページにある、「外部のタイムソースを使用するようにWindowsタイムサービスを構成する」を参照  
<https://support.microsoft.com/ja-jp/help/816042/how-to-configure-an-authoritative-time-server-in-windows-server>

# 3.4 管理LANと業務LANの構成設計

## ■ 管理LANと業務LANのネットワークを分離する

- セキュリティレベルが高い
- 管理LANと業務LAN間のネットワーク干渉、負荷過多を回避
- ネットワーク管理しやすい

## ■ 管理LANと業務LANが利用するLANポートを決める

- 必要とされるネットワーク性能
- システム保守と拡張性
- PCI Express スロット（FCカードやSASカードなど）の利用状況

コンポーネント		デバイスの説明	通信速度	搭載数	保守性/拡張性
オンボードLAN		Intel® I350 Gigabit Network Connection	IOU(1GbE) 最大1Gbps	IOUあたり 2ポート	<ul style="list-style-type: none"> <li>• 故障時はIOU単位で交換</li> <li>• 活性保守にはDynamic Reconfiguration機能が必要だが、Windowsは未サポートのため活性保守不可</li> </ul>
		Intel® Ethernet Controller X540-AT2	IOU(10GbE) 最大10Gbps		
LAN カード /CNA	IOUのPCI Express スロット	カードの 種類に依存	カードの 種類に依存	IOU(1GbE) 4スロット	<ul style="list-style-type: none"> <li>• カード故障または拡張時はカード単位で交換</li> <li>• ポート拡張時はカード種類を選択可能</li> <li>• IOU故障時はIOU単位で交換</li> <li>• PCIホットプラグ機能は不可（ハード仕様）</li> </ul>
	PCIボックスの PCI Express スロット			IOU(10GbE) 3スロット	
				PCIボックス接続 カード1枚あたり 6スロット	<ul style="list-style-type: none"> <li>• カード故障または拡張時はカード単位で交換</li> <li>• ポート拡張時はカード種類を選択可能</li> <li>• PCIボックス故障時はPCIボックス単位で交換</li> <li>• PCIホットプラグ機能をサポート</li> </ul>

コンポーネント交換の詳細は『運用管理マニュアル 第3章 コンポーネントの構成と交換（増設、削除）』を参照

## ■ ネットワークを高信頼化する3つのポイント

- ① ネットワークの二重化構成
- ② ネットワークコンポーネントの冗長化
- ③ チューニングソフトウェアの選択

# 3.5.1 ネットワークの二重化構成

## ■ PRIMEQUESTを接続するネットワークを二重化構成にする

以下を考慮してネットワークを設計する

- ルーターをホットスタンバイ構成にする場合はルーター故障時のフェールオーバー時間を考慮する
- PRIMEQUESTで動作するアプリケーションの通信タイムアウト時間以内にネットワークが復旧するように設計する
- STPを有効にした場合(\*1)
  - LANカードがリンクアップしてからSTPタイマーが満了するまで通信できない状態となり、監視エラーや意図しない切替えが発生する場合がある
  - ネットワーク冗長機能の切替え時間に比べてSTPの切替え時間が短い場合、不要な切替えが発生する場合がある

\*1)管理LANを設計する場合、必ずSTPをOFFにする

[PRIMECLUSTER GLS for Windows(PRIMEQUEST)の設計]

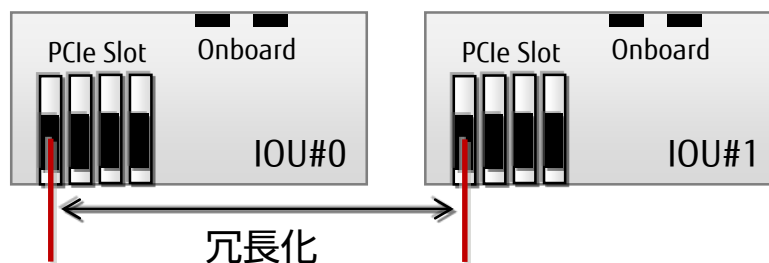
hanetpollコマンドを使用して、ping監視開始から監視先へのチェックを行うまでの待ち時間をSTPタイマー以上に設計する

 詳細は『PRIMECLUSTER GLS for Windows ユーザーズガイド』を参照

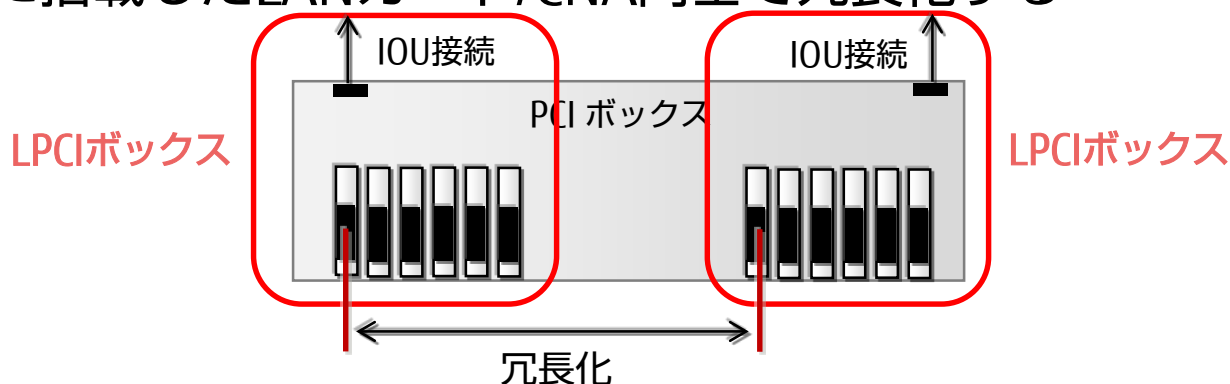
[Intel PROSet / OneCommand NIC Teaming and VLAN Manager/ OSのNICチーミング機能 (Windows Server 2012/2016の標準機能)の設計]  
STPを無効化する

- PRIMEQUEST搭載のネットワークコンポーネントを選択する  
以下を考慮して冗長化するLANポートを選択する

- 複数のIOUやPCIボックスを使用してパーティションを構成する場合は、別々のIOUやPCIボックスに搭載したLANカード/CNA同士で冗長化する



- 同一のPCIボックスを使用して二重化を行なう場合は、別々のLPCIボックスに搭載したLANカード/CNA同士で冗長化する



👉 詳細は『構成設計ガイド 3.3 I/O構成設計のポイント』を参照



## ■ LANカード/CNAを二重化(チーミング)するためのソフトウェアを選択して設定する

### チーミングとは

LANカード/CNA複数枚をチームとして構成し、チームを構成するメンバー間で負荷分散や異常発生時のトラフィックの引継ぎを行なう  
業務LANまたは管理LANのポートを組み合わせてチームを構成する

PRIMEQUESTが対応しているチーミングソフトウェアは以下の4種類  
機能/要件を踏まえて選択する

- PRIMECLUSTER GLS for Windows (PRIMEQUEST)
- Intel PROSet(\*1)
- Emulex OneCommand NIC Teaming and VLAN Manager
- OSのNICチーミング機能

\*1) Intel 製LANカード搭載時は、チーミング機能を使用する・しないに関わらずインストールが必要

 PRIMECLUSTER GLS for Windows(PRIMEQUEST)、Intel PROSetのOS対応状況は『FUJITSU Server PRIMEQUEST 2000シリーズ Windows Server情報』を参照

# 3.5.3 チーミングソフトウェアの選択(2/3)

## ■ チーミングソフトウェアの選択ポイント(\*1)

それぞれの特徴は以下のとおり、要件に応じてソフトウェアを選択する

### ■ PRIMECLUSTER GLS for Windows (PRIMEQUEST)

- 最も高信頼性を実現する場合に選択
- 業務の即時再開と継続、故障箇所の特定と復旧が可能

### ■ Intel PROSet

- Windows Server 2008/2012を使用しており、Intel製コントローラの場合でSMBマルチチャネルと併用しない場合に選択
- 標準添付ソフトウェア


### ■ OneCommand NIC Teaming and VLAN Manager

- Windows Server 2008 を使用しており、Emulex 製CNA コントローラの場合に選択
- 標準添付ソフトウェア

### ■ OSのNIC チーミング機能

- Windows Server 2016を使用している場合、もしくは、上記3つのチーミングソフトウェアの使用条件に合致しない場合に選択
- Windows Server 2012/2016の標準機能

\*1) 同種カード間またはIOUのオンボードLAN内でチーム構成することを推奨

 詳細は『運用管理マニュアル G.8 NIC(ネットワークインターフェースカード)』を参照

## ■ チーミングソフトウェアの機能比較

機能	PRIMECLUSTER GLS for Windows (PRIMEQUEST)	Intel PROSet	Emulex OneCommand	OSのNIC チーミング
LANカード/CNAの故障検出	○	○	○	○
ネットワークの故障検出	○	×	×	×
帯域を拡張したネットワーク同士の二重化	△(*1)	△(*2)	×	△(*3)
SMBマルチチャネルとの併用	×	×	×	○
SMBダイレクトとの併用	×	×	×	×
サポート(*4)	富士通	Intel社	Emulex社	Microsoft社
マルチプラットフォーム	○(*5)	—	—	—
提供形態	有償製品(*4)	標準添付ソフトウェア	標準添付ソフトウェア	Windows Server 2012以降の標準機能

○：可能 △：条件付き可能 ×：不可 —：該当せず

\*1) Intel PROSet と組み合わせることで可能(Windows Server 2016は除く)

\*2) PRIMECLUSTER GLS for Windows(PRIMEQUEST) と組み合わせることで可能(Windows Server 2016は除く)

\*3) SMBマルチチャネルと組み合わせることで可能

\*4) サポートにはSupportDesk契約が必須

\*5) Windows環境/Linux環境にも同じ機能および操作性を提供

PRIMECLUSTER GLS for Windows(PRIMEQUEST)の詳細は『[付録B チーミングソフトウェア](#)』を参照

# 3.6 IPアドレスの割り当て(1/4)

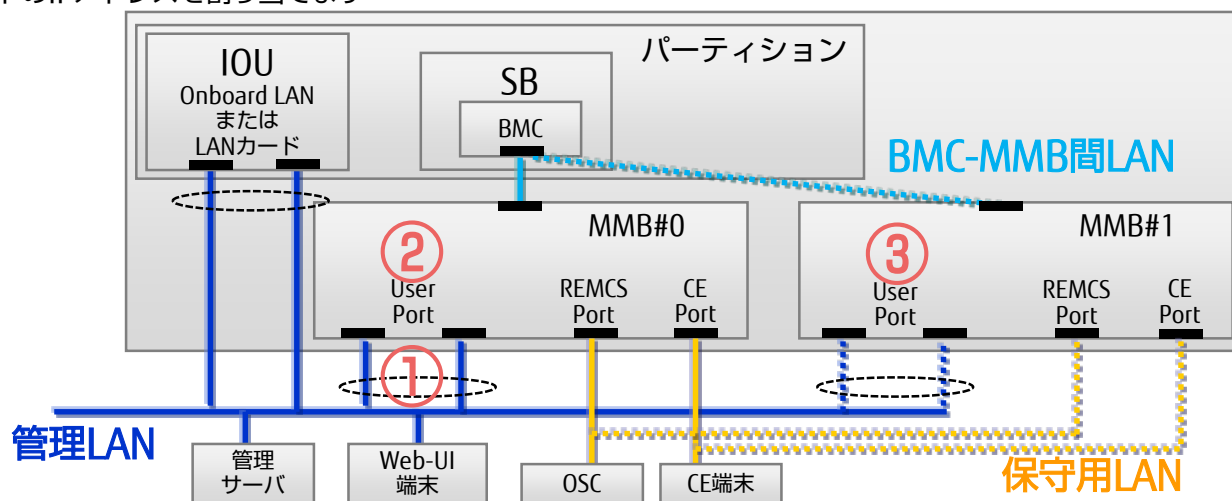
## ■ 管理LANと保守用LANの構成に必要なIPアドレスを決める

### ■ MMBから設定するIPアドレス

詳細は『運用管理マニュアル 第1章 ネットワーク環境の設定と管理ツールの導入』を参照

設定項目	NIC	IPアドレス数	設定方法	説明
① Virtual IP Address(*1)	MMB User Port	1	MMB Web-UI または MMB CLI	MMBを二重化した場合において、MMB(Active)と通信(Web、telnet など)する際に使用する仮想IPアドレス
② MMB#0 IP Address(*1)	MMB#0 User Port	1	MMB Web-UI または MMB CLI	管理LAN上のPCがMMB#0と通信する際に使用する物理IPアドレス
③ MMB#1 IP Address(*1)	MMB#1 User Port	1	MMB Web-UI または MMB CLI	管理LAN上のPCがMMB#1と通信する際に使用する物理IPアドレス

(\*1) 同一サブネットのIPアドレスを割り当てます



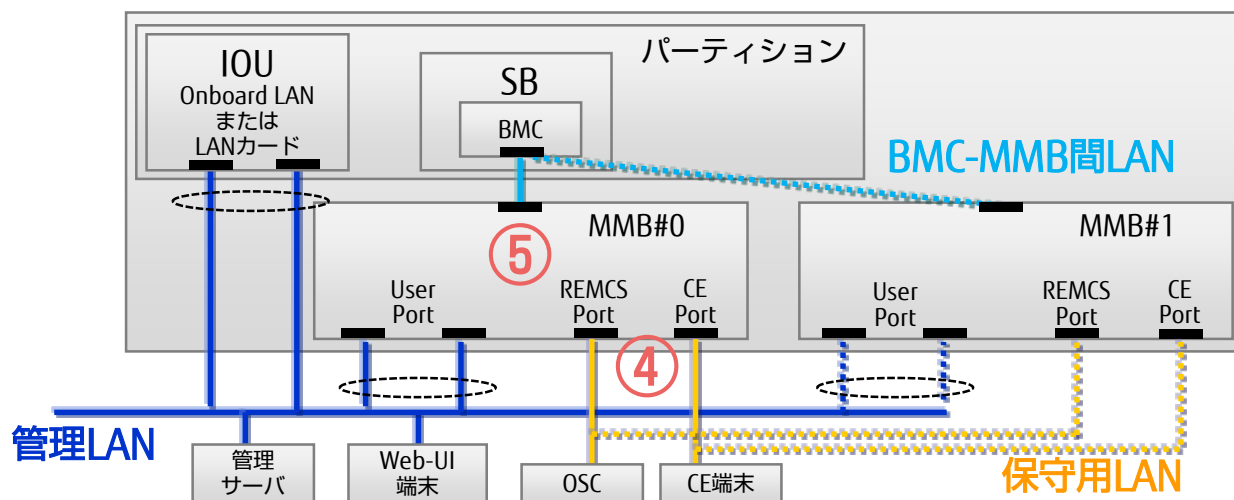
# 3.6 IPアドレスの割り当て(2/4)

## ■ 管理LANと保守用LANの構成に必要なIPアドレスを決める

### ■ MMBから設定するIPアドレス

詳細は『運用管理マニュアル 第1章 ネットワーク環境の設定と管理ツールの導入』を参照

設定項目	NIC	IPアドレス数	設定方法	説明
④ Maintenance IP Address	REMCS/CE Port	1	MMB Web-UI または MMB CLI	REMCSで通信する場合に使用。CEポートに接続した保守用端末と通信する場合にも使用 MMBを二重化した場合は、Active側のMMBのみ通信し、MMBが切り替わるとStandby側に同じIPアドレスが割り当てられる
⑤ Console Redirection Setup	BMC-MMB間LAN用のポート(MMB)	パーティション数分	MMB Web-UI	管理LAN上のPCからBMCの遠隔操作機能を利用するためのIPアドレス。管理LAN上のIPアドレスを指定する

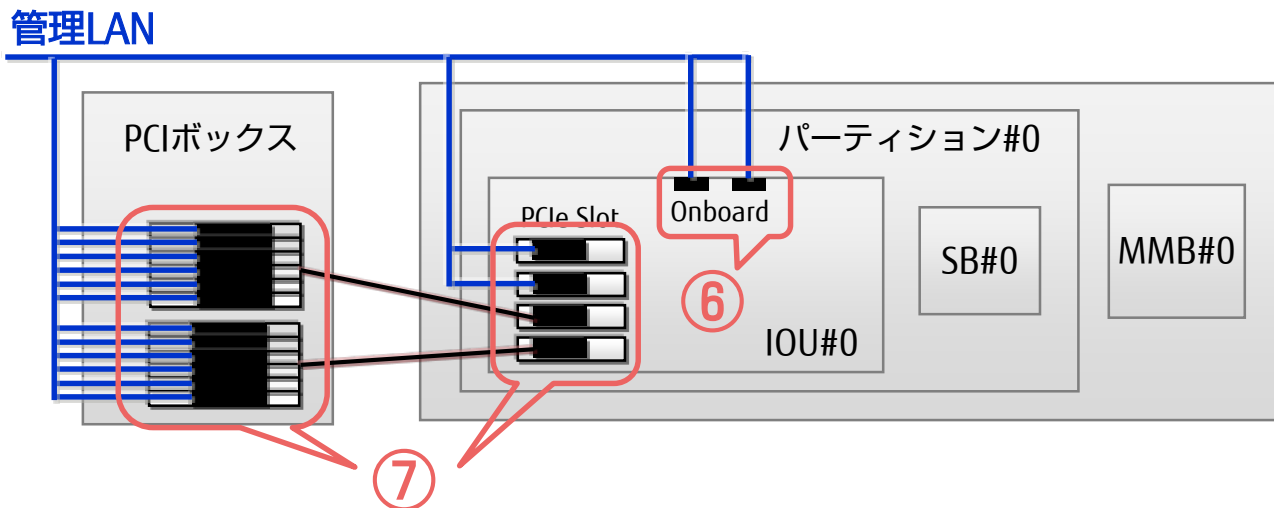


# 3.6 IPアドレスの割り当て(3/4)

## ■ 管理LANの構成に必要なIPアドレスを決める

### ■ パーティション内のOSから設定するIPアドレス

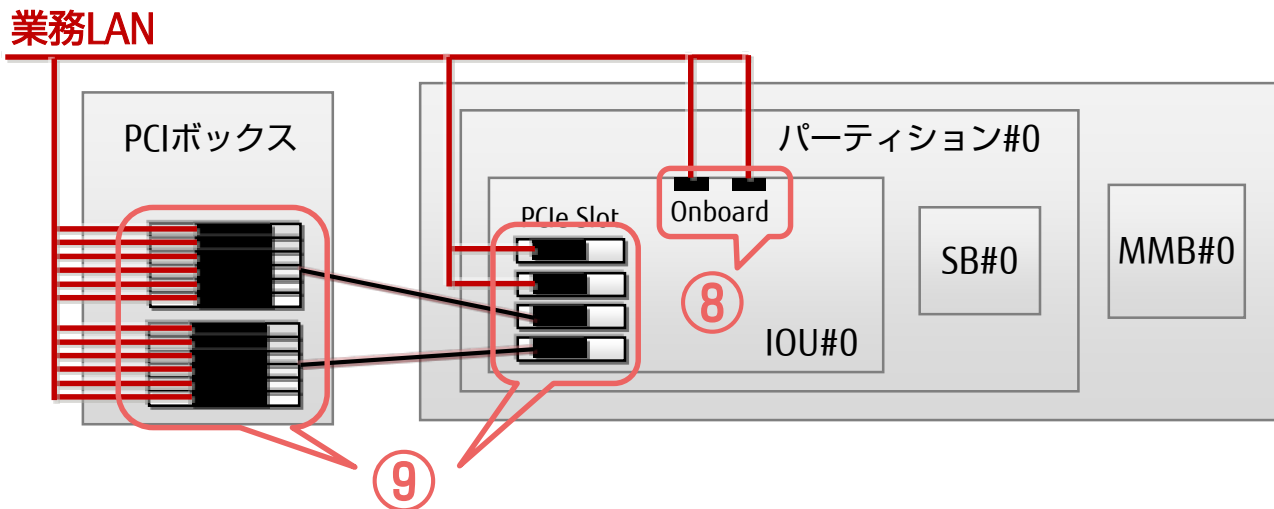
	NIC	IPアドレス数	設定方法	説明
⑥	IOUのオンボードLAN	ネットワークへ接続する数分	Windowsの[ネットワーク接続]のプロパティで設定	各ポートから筐体外のネットワークに接続する管理サーバ用の管理LANとして使用 当該パーティション内のネットワークへ接続する数分のIPアドレスが必要 (実際に使用するポートにIPアドレスを割り当てる)
⑦	IOUまたはPCIボックス搭載のLANカード/CNA	ネットワークへ接続する数分	Windowsの[ネットワーク接続]のプロパティで設定	



# 3.6 IPアドレスの割り当て(4/4)

## ■ 業務LANの構成に必要なIPアドレスを決める

NIC	IPアドレス数	設定方法	説明
⑧ IOUのオンボードLAN	ネットワークへ接続する数分	Windowsの[ネットワーク接続]のプロパティで設定	各ポートから筐体外のネットワークに接続する業務LANとして使用 当該パーティション内のネットワークへ接続する数分のIPアドレスが必要 (実際に使用するポートにIPアドレスを割り当てる)
⑨ IOUまたはPCIボックス搭載のLANカード/CNA	ネットワークへ接続する数分	Windowsの[ネットワーク接続]のプロパティで設定	



## ■ Internal LANのIPアドレスを決める

設計指針		MMB側のIPアドレスとパーティション側のIPアドレスを同じサブネットで設計
設定方法	MMB側	MMB Web-UIのNetwork Configurationメニューから設定変更
	パーティション側	Windows上から設定変更 [注意点] <ul style="list-style-type: none"><li>• デフォルトゲートウェイを設定しない</li><li>• MMB側でIPアドレスを設定変更してもパーティション側では連動して変更されないため、変更時にはパーティション側でも設定する</li><li>• DNSサーバのAレコードにInternal LANを設定しない</li></ul>

## ■ 留意事項

- Internal LANのMMB側ネットワークは、REMCS Optionインストール時に、IPアドレス 172.30.0.1/24が自動的に割り当てられる  
既存環境のIPアドレスと重複するなど問題がある場合は変更する
  - 問題がなければ、パーティション側に同じサブネットのIPを設定するだけでよい



## ■ MMBと各パーティションで動作するOSの時刻を同期する

MMBと各パーティションは直接同期されないため個別に指定する

### ■ MMB：NTPサーバを最大3つ指定可能

MMB Web-UIの[Network Configuration]-[Date/Time]で指定

### ■ パーティション

MMBが時刻同期先として指定しているNTPサーバを  
[日付と時刻のプロパティ]に指定

<WindowsでNTPサーバを複数台指定する方法>

w32tmコマンドを使用して複数台のNTPサーバを指定する

- w32timeサービスによりNTPプロトコルを利用して時刻同期を行なう
- NTPを利用しているため、Windows以外とも時刻同期可能

指定例) w32tm /config /manualpeerlist:<時刻同期先>,0x9

詳細はw32tm /? でヘルプ表示してください

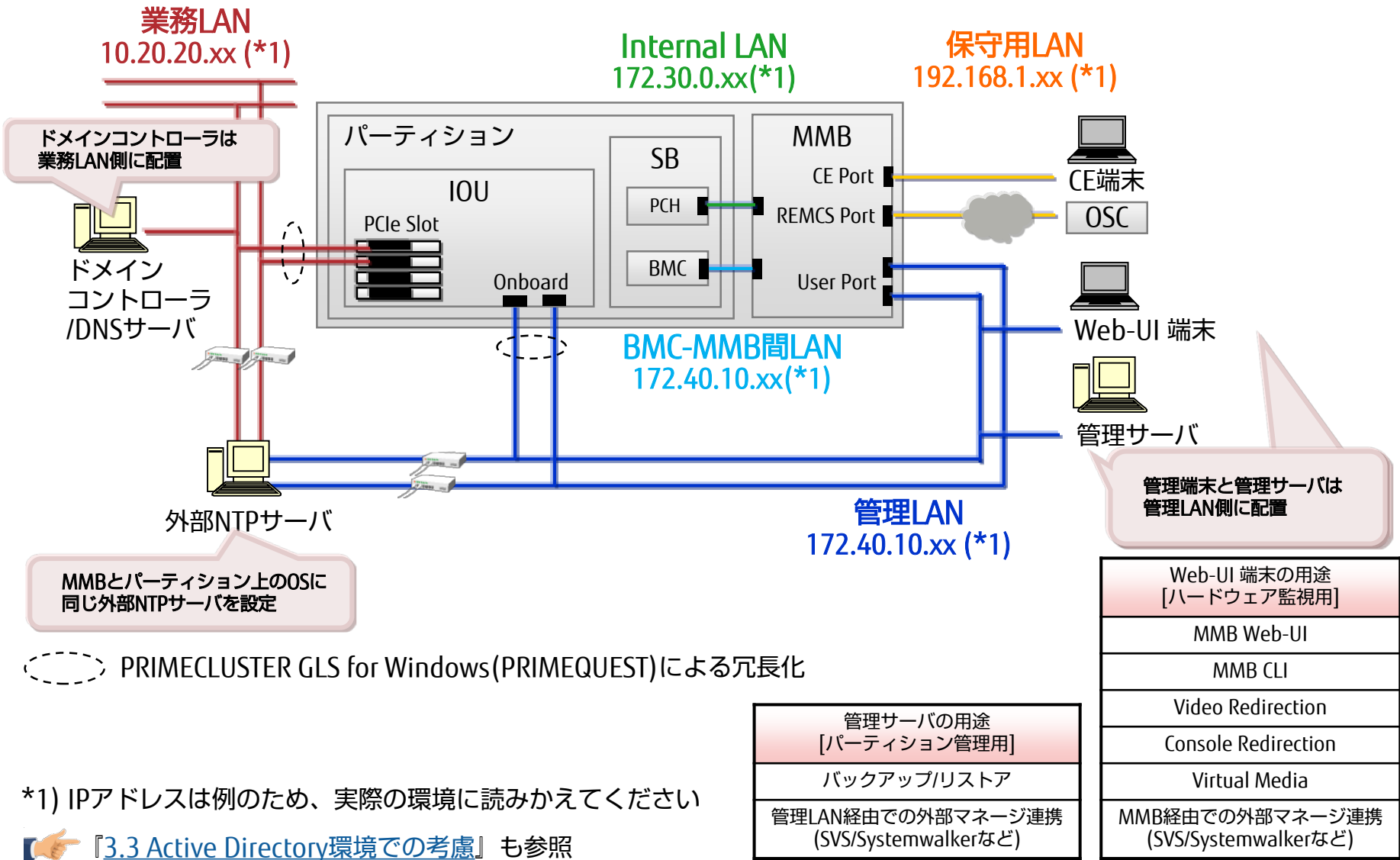
 パーティションがドメインに参加している場合の時刻同期については  
『[3.3.2 ドメイン メンバサーバの時刻同期の方法](#)』を参照

※ Windows環境としてNTPサーバを複数台必要という条件はありませんが、例えば、NTPサーバの耐障害性を考慮したい場合は複数台のNTPサーバを準備してください

## 4. 構成例

Windowsにおけるネットワーク構成例を紹介します

# 4.1 ネットワーク構成例



\*1) IPアドレスは例のため、実際の環境に読みかえてください

👉 『3.3 Active Directory環境での考慮』も参照

## 5. iSCSI接続におけるネットワーク設計

iSCSI接続する場合の設計項目を説明します

# 5.1 iSCSI接続の構成パターン

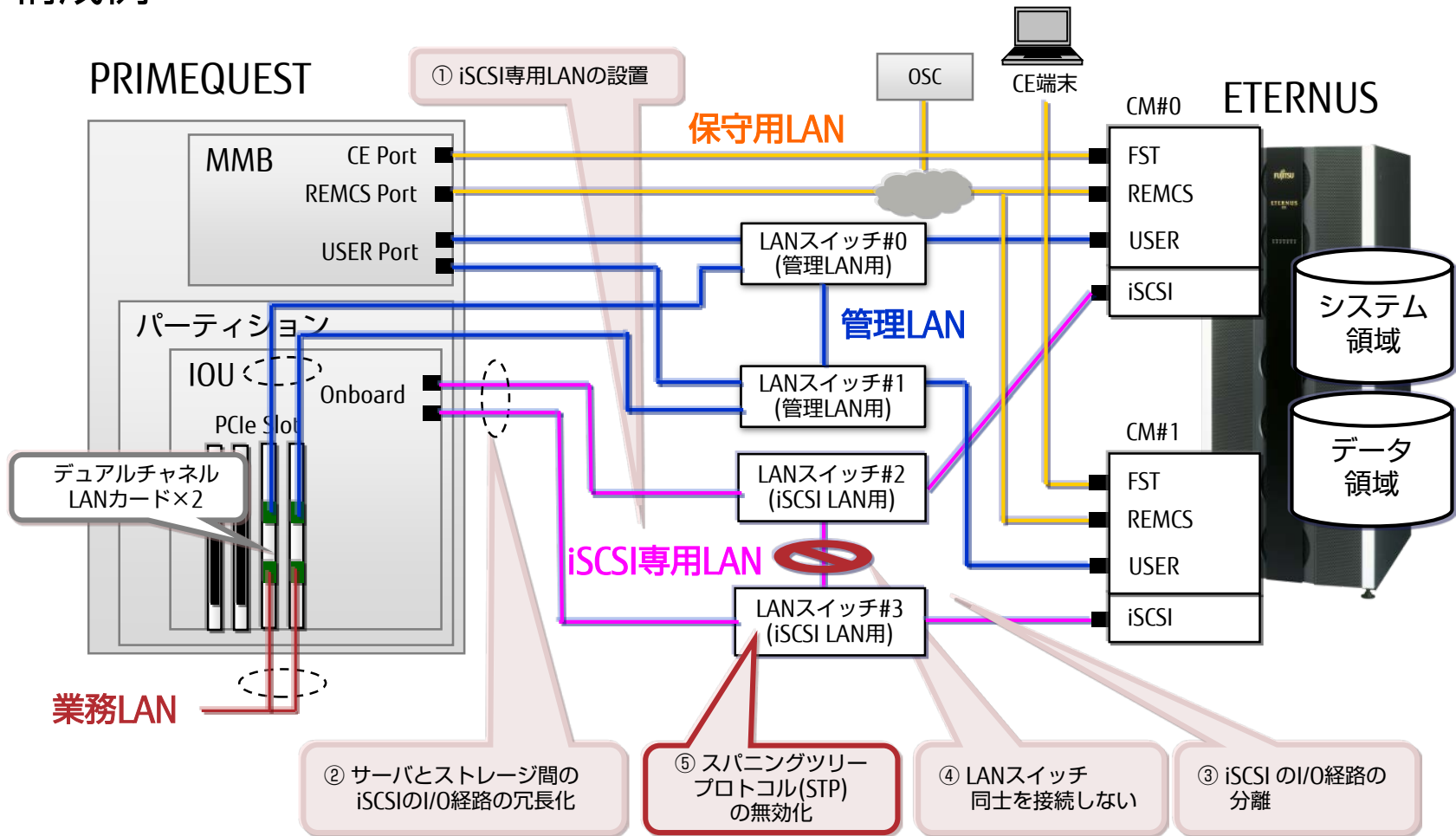
- iSCSI接続のアクセスパス構成のパターンは以下のとおり
  - データ領域を格納した外部アレイドisks装置へiSCSI接続するアクセスパス構成
  - システム領域とデータ領域を格納した外部アレイドisksへiSCSI接続するアクセスパス構成(\*1)
  
- IOU搭載のオンボードLANとCNAを使用したiSCSIブート/接続の設計ポイントは同じ
  - FCoEスイッチを利用する場合は本章記載のLANスイッチをFCoEスイッチとして読み替えてください
  
- iSCSI専用LANの設置
  - 管理LAN、業務LAN、保守用LANとは物理的に異なるスイッチ、ケーブルでiSCSI専用LANの設置を推奨する

\*1) iSCSIブートはWindows Server 2012 R2のみサポート

 アクセスパス構成の詳細は『Windowsディスク設計ガイド』を参照

# 5.2 iSCSI接続時の考慮(1/3)

- システム領域とデータ領域を格納した外部アレイディスクへiSCSI接続する構成例



☁ インターネット  
⋯ ソフトウェアでの冗長化

# 5.2 iSCSI接続時の考慮(2/3)

## 考慮ポイント

- ① iSCSI専用LANの設置  
管理LAN、業務LAN、保守用LANとは物理的に異なるスイッチ、ケーブルでLANを設置する
- ② サーバとストレージ間のiSCSIのI/O経路の冗長化  
チーミングソフトウェアではなく、以下のマルチパスソフトウェアを使用する  
(管理/業務LANはチーミングソフトウェアを使用する)  
ETERNUSマルチパスドライバ  
OS標準のマルチパスドライバ(\*1)  
物理的に異なるスイッチを使用して、スイッチ間でマルチパスを構成する
- ③ iSCSIのI/O経路の分離  
ストレージ側のI/Oポート毎に、スイッチ上では異なるポートVLAN IDでセグメントを分離する
- ④ LANスイッチ同士を接続しない  
マルチパスにより冗長化を行うことから、LANスイッチ同士を接続しない
- ⑤ スパニングツリープロトコル(STP)の無効化  
スイッチがSTPの処理を行う間はリンクダウンした状態が続き、ブートディスクが見つからずタイムアウトしてしまう可能性がある  
そのため、システム領域とデータ領域をiSCSI接続する場合は、STPを無効化する

\*1) 「機能」の選択画面で「マルチパスI/O」のチェックボックスをチェックし、MPIO機能をインストールします

## 5.2 iSCSI接続時の考慮(3/3)

- 複数接続セッション(MCS)の構成不可
  - ETERNUSをターゲットとする場合は、複数接続セッション(MCS)を構成できない
- iSCSIブートする際の考慮
  - Windows Server 2016 において、iSCSIブートは未サポート
  - Windows Server 2012 R2において、一部機能が未サポート
    - 仮想スイッチ：詳細はKB2969306を参照  
(<https://support.microsoft.com/en-us/help/2969306/a-newly-created-virtual-switch-disappears-after-you-restart>)
    - NICチームング：詳細はKB2969300を参照  
(<https://support.microsoft.com/en-us/help/2969300/-faulted-not-found-status-for-nic-team-after-you-restart-windows-from-an-iscsi-boot-disk>)
  - IOU搭載のオンボードLANまたはCNAを使用



# 5.3 iSCSIイニシエータの設計

## ■ 利用可能なイニシエータ

接続デバイスおよびブート/接続により利用可能なイニシエータが異なる

接続デバイス		PRIMEQUEST対応 イニシエータ	ソフトウェアイニシエータ	ハードウェアイニシエータ
iSCSIブート	IOUのオンボードLAN		○	×
	CNA		×	○
iSCSI 接続	IOUのオンボードLAN		○	×
	CNA		×	○

## ■ iSCSIイニシエータ設定ツール

○：可能 ×：不可

ソフトウェアイニシエータ： WindowsのiSCSI Initiatorアプリケーションを使用する

ハードウェアイニシエータ： LegacyモードではEmulex iSCSISelect Utilityを使用する  
UEFIモードではEmulex iSCSI Utility を使用する

## <参考>

- iSCSIイニシエータとは  
通信の送信元サーバのこと  
通信の送信先のストレージシステムは「iSCSIターゲット」と呼ぶ
- iSCSIイニシエータの役割  
1台または複数のiSCSIターゲットと通信して、ターゲットから提示されたiSCSIデバイスをサーバに  
対してローカルなSCSIデバイスとして見せる

# 5.3.1 ソフトウェアイニシエータの設計

## ■ パラメーターの値を設計する

Windowsの iSCSI Initiatorアプリケーションでは以下を設計する

項目	説明
イニシエーター名	iSCSIノード(iSCSI接続するサーバやETERNUS)を一意に識別するためのiSCSI Qualified Name (IQN)名 最大223バイト文字 ETERNUSマニュアルではiSCSIネームと呼ばれている
IPアドレスまたはDNS名	ETERNUS側のiSCSIポートのTCP/IP 設定に入力したアドレス
ポート番号	ETERNUSへiSCSI接続する場合は3260
イニシエーターIP	イニシエーターサーバ側のiSCSIポートのIPアドレス
認証方式	セキュリティ要件により「認証なし, CHAP認証, Bidirectional CHAP認証」のいずれかを選択する ■CHAP認証 ETERNUSがサーバ側を認証する。シークレット(パスワード)はターゲット(ETERNUS)にのみ設定され、そのターゲットにアクセスしようとする全てのサーバは、同じシークレットを使用してターゲットとのログオンセッションを開始する ■Bidirectional CHAP認証 ETERNUS側とサーバ側が互いに認証する。SAN内の各ターゲットと各サーバ側に、別のシークレットが設定される
CHAPユーザ名	CHAP認証で使用するユーザ名。ETERNUS側での設定値と同じ値
CHAPパスワード	CHAP認証で使用するパスワード。12バイト以上、16バイト以下 ETERNUS側での設定値と同じ値
CHAPシークレット	Bidirectional CHAPで使用するパスワード。12バイト以上、16バイト以下 ETERNUS側での設定値と同じ値

## 5.3.2 ハードウェアイニシエータの設計

### ■ パラメーターの値を設計する

Emulex iSCSISelect Utility / Emulex iSCSI Utilityでは以下を設計する

項目	説明
iSCSI Initiator Name	iSCSIノード(iSCSI接続するサーバやETERNUS)を一意に識別するためのiSCSI Qualified Name (IQN)名 最大223バイト文字。ETERNUSマニュアルではiSCSIネームと呼ばれている
iSCSI Target IP Address	ETERNUS側のiSCSIポートのTCP/IP 設定に入力したアドレスを設定する ここで設定したターゲットをBoot TargetのPrimaryとして設定する
TCP Port Number	ETERNUSへiSCSI接続する場合は3260
IP Address	コントローラのiSCSIポートのIPアドレスを静的IPアドレスとして設定する DHCPを利用する場合はDHCP を有効に設定する
IP Version	ターゲットのIP Address設定時にIPv4またはIPv6を選択する CNAによるiSCSIブート時はIPv4のみサポートする
Authentication Method	セキュリティ要件により「None, One-Way Chap, Mutual Chap」のいずれかを選択する ■One-Way Chap ETERNUSがサーバ側を認証する。シークレット(パスワード)はターゲット(ETERNUS)にのみ設定され、そのターゲットにアクセスしようとする全てのサーバは、同じシークレットを使用してターゲットとのログオンセッションを開始する ■Mutual Chap ETERNUS側とサーバ側が互いに認証する。SAN内の各ターゲットと各サーバ側に、別のシークレットが設定される
Target CHAP Name	CHAP認証で使用するターゲットCHAP名。ETERNUS側での設定値と同じ値
Target Secret	CHAP認証で使用するターゲット秘密鍵。12バイト以上、16バイト未満 ETERNUS側での設定値と同じ値
Initiator CHAP Name	Mutual CHAPで使用するターゲットCHAP名。ETERNUS側での設定値と同じ値
Initiator Secret	Mutual CHAPで使用するイニシエータ秘密鍵。12バイト以上、16バイト未満 ETERNUS側での設定値と同じ値

# 5.4 iSCSI接続におけるマルチパスドライバの考慮

## ■ ETERNUSマルチパスドライバ

### ■ FCパスと同様に利用可能、ただし以下を考慮する

- I/O応答時間監視の初期設定  
iSCSIは無効、iSCSI以外は有効。iSCSIを利用する場合は無効の設定のままにしておく
- WindowsのiSCSI Initiatorアプリケーションに対する設定  
ターゲットへの接続設定において、「複数パスを有効にする」のチェックボックスは必ずオフにする
- MPIOの制御対象デバイス設定  
ETERNUSマルチパスドライバをインストールすると、MPIOのプロパティに制御対象デバイスの一覧が表示されるが、この一覧の情報は編集しない

## ■ ETERNUSマルチパスドライバ/OS標準のマルチパスドライバ共通

- 負荷分散ポリシーや再実行回数などの各種設定が可能だが  
これら設定は変更せずに、デフォルトで使用する

画面の名前	変更してはいけないパラメーター
Multi-Path Disk DeviceプロパティのMPIOタブ	負荷分散ポリシー、詳細ボタン、編集ボタン
DSMの詳細	タイマーカウンタ（パス確認期間、パス確認を有効化、再実行回数、再実行間隔、PDO削除期間）
MPIOパスの詳細	パスの状態

## 6. FCoE接続におけるネットワーク設計

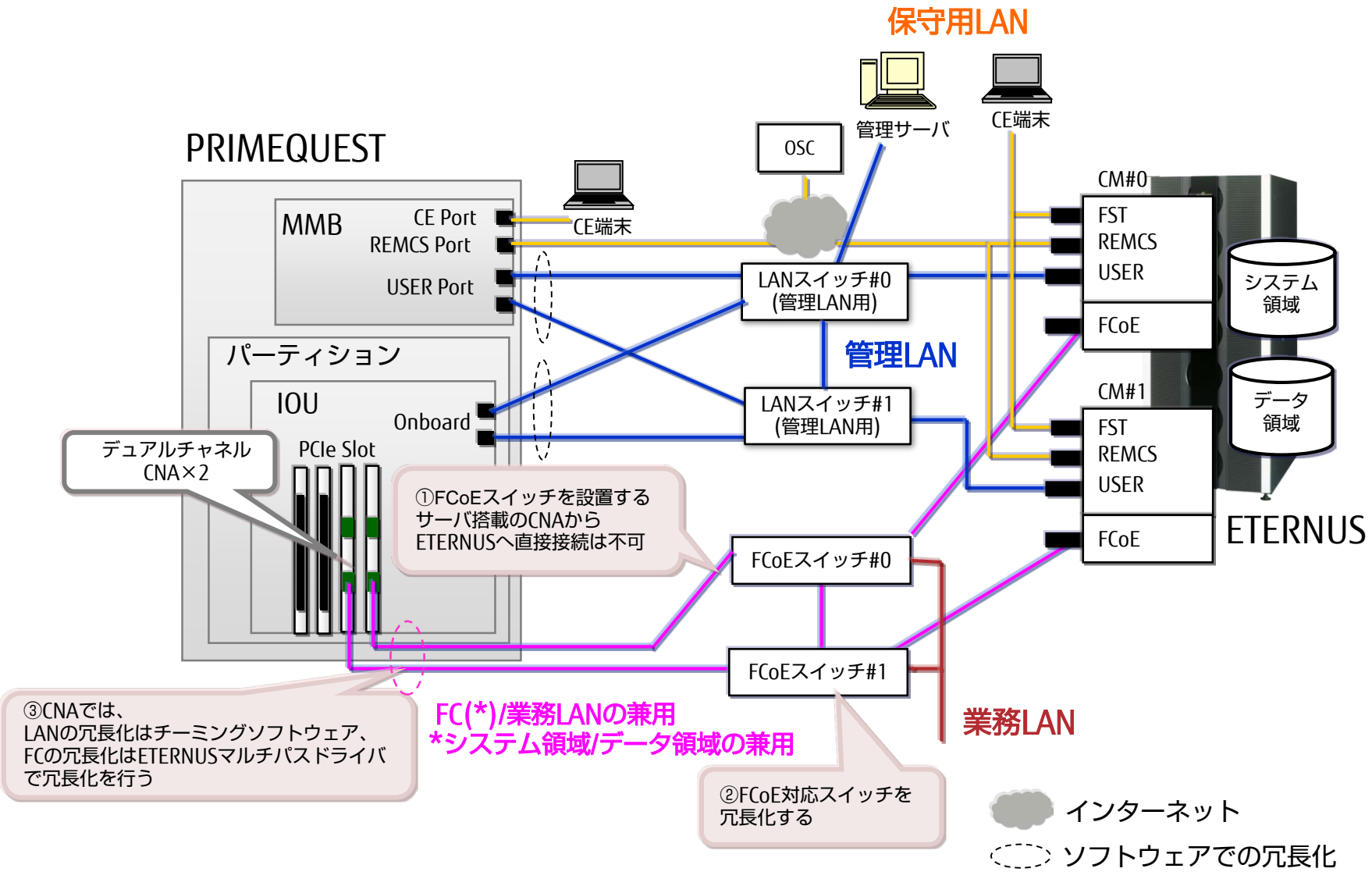
# 6.1 FCoE接続の構成パターン

- FCoE接続の構成パターンは以下のとおり
  - データ領域のみを外部アレイドISK装置へFCoE接続する構成
  - システム領域とデータ領域を外部アレイドISK装置へFCoE接続する構成(FCoEブート)

 詳細は『Windowsディスク設計ガイド』を参照

- FCoE対応スイッチの設置
  - サーバから外部アレイドISK装置へ直接接続は不可

# 6.2 FCoE接続時の考慮(1/2)



## 6.2 FCoE接続時の考慮(2/2)

- ① FCoE使用時にはFCoEスイッチを設置する  
サーバ搭載のCNAからETERNUSへ直接接続不可
  - ② FCoEスイッチは冗長化する
  - ③ 経路の冗長化には以下を使用する
    - LAN ⇒ チーミングソフトウェア
    - FC ⇒ ETERNUSマルチパスドライバ
- OneCommand Managerユーティリティにより、CNAのPersonalityの設定値が“FCoE”であることを確認する
- FCoEブート構築時はPXESelectユーティリティによる設定も必要
- 👉 OneCommand Managerユーティリティの詳細はドライバ添付の『ソフトウェアガイド コンバージド・ネットワーク・アダプタ』を参照
- 👉 PXESelectユーティリティの詳細は『FCoE Boot 環境構築マニュアル』を参照



# 付録A. LANポートの接続先確認方法

PRIMEQUESTは多数のLANポートを利用可能なため、Windowsの[ネットワーク接続]画面にも多数のLANポートが表示されます。

物理的な搭載位置と[ネットワーク接続]画面に表示されるLANポートを関連づけて特定する方法を紹介します

# A.1 LANポートの接続先確認方法(1/4)

## ■ 2通りの確認方法がある

### a. OS標準の機能を利用して確認する

- Windows Server 2012/2016では、OS標準機能で確認することが可能  
Windows Server 2008 R2では、  
b.のSVOM/SV Agentsを利用した方法で確認することが可能

### b. SVOMおよびSV Agentsを利用し、次の3つを比較して確認する

#### 1. SVOM画面

[システムステータス]-[ドライバモニタ]で  
搭載位置と物理アドレスを確認する

#### 2. ipconfig /all コマンド

物理アドレスと名前を確認する

#### 3. Windowsの[ネットワーク接続]画面

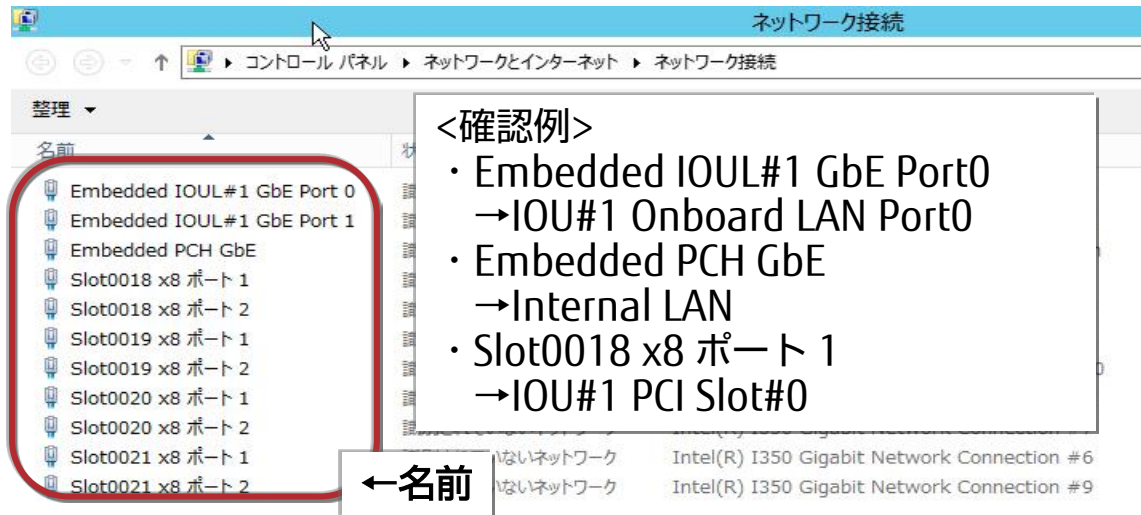
[コントロールパネル]-[ネットワークとインターネット]  
-[ネットワーク接続]で表示

SVOM画面で確認した物理アドレスとipconfig /allで表示した物理アドレスを比較し、名前を割り出す。Windowsのネットワーク画面での名前を比較して搭載位置とLANポートを特定する

# A.1 LANポートの接続先確認方法(2/4)

## a. OS標準の機能を利用して確認する

- Windowsの[ネットワーク接続]画面で、NICに対応した名前（スロット番号など）が自動的に表示される



- スロット番号と実装位置の対応関係は、  
『運用管理マニュアル 付録B 物理実装位置、ポート番号』 または  
『運用管理マニュアル 付録D I/Oの物理位置・BUS番号およびPCI Expressス  
ロット実装位置・スロット番号』 を参照して特定できる

# A.1 LANポートの接続先確認方法(3/4)

## b. SVOMおよびSV Agentsを利用し、次の3つを比較して確認する

### 1. SVOM画面

[システムステータス]-[ドライバモニタ]で  
LANポートの搭載位置と物理アドレスを確認する(\*1)

ServerView  
ユーザー: Administrator ログアウト

シングルシステムビュー  
WS2012

PRIMEQUEST 2800E

表示データ: オンライン: 2014-01-29 10:02:18 更新 アーカイブ取得 識別灯

ID	タイプ	識別番号	筐体ステータス
0	PRIMEQUEST 2800E	1541326007	N/A

監視コンポーネント

チェック	タイプ	名前	搭載位置
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#0-FUNC#0
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#0-FUNC#1
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#2-FUNC#0
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#2-FUNC#1
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#1-FUNC#0
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#1-FUNC#1
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#3-FUNC#0
✓	network	pci FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035	-PCIC#3-FUNC#1

← 搭載位置

詳細

Seg/Bus/Dev/Func: 0/140/0/0  
ベンダ: 0x8086 INTEL CORPORATION  
デバイス: 0x1521 FUJITSU Eth Ctrl 2x1Gb Cu PCIe x4 D3035  
ハードウェアアドレス: 001999D5BE63  
← 物理アドレス

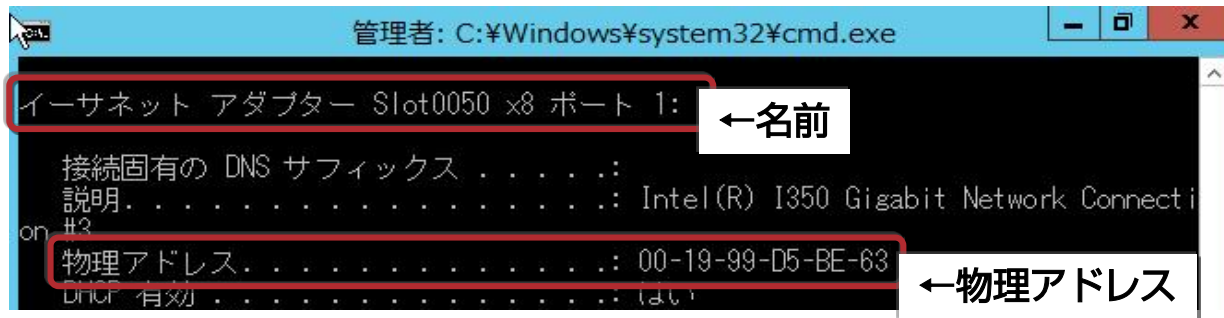
\*1) IOUのオンボードLANは搭載位置が表示されないため確認できません

# A.1 LANポートの接続先確認方法(4/4)

## b. SVOMおよびSV Agentsを利用し、次の3つを比較して確認する

### 2. ipconfig /all画面

コマンドプロンプトで ipconfig /all を実行し、SVOM画面で確認した物理アドレスをもとに名前を確認する



### 3. Windowsの[ネットワーク接続]画面(表示例)

ipconfigコマンドで確認した名前をもとにLANポートを特定する



# 付録B. チーミングソフトウェア

PRIMECLUSTER GLS for Windows(PRIMEQUEST)  
について説明します

## ■ PRIMECLUSTER GLS for Windows (PRIMEQUEST)の優位性(1/3)

○：適    ×：不適

お客様要件		PRIMECLUSTER GLS for Windows (PRIMEQUEST)	Intel PROSet	OSの NIC チーミング
通信の 高信頼化	業務の 即時再開と 継続	○	×	×
		ルーターの故障を検出し、必要に応じて切替え可能	ルーター故障の検出不可 ネットワーク構成によっ て、切替わらない可能性 あり	ルーター故障の検出不可 ネットワーク構成によっ て、切替わらない可能性 あり
	故障箇所の 特定と復旧	○	×	×
		ネットワーク機器ごとに 監視可能なため、故障箇 所の特定と復旧が容易	物理アダプターの状態 (リンク状態やパケット の送受信状態) のみの監 視のため故障箇所の特定 が不可	物理アダプターの状態 (リンク状態やパケット の送受信状態) のみの監 視のため故障箇所の特定 が不可

## PRIMECLUSTER GLS for Windows (PRIMEQUEST)の優位性(2/3)

○：適    ×：不適

お客様要件		PRIMECLUSTER GLS for Windows (PRIMEQUEST)	Intel PROSet	OSの NIC チーミング
ネットワークの状態に応じたアプリケーション連携	伝送路異常検出時	○	×	×
		物理アダプターのリンクダウンや無効化、ネットワーク機器の通信異常を検出した場合に、事前に用意したスクリプトを実行して通信異常の通知等が可能	連携不可	連携不可
	通信相手システムの異常検出時	○	×	×
		通信相手システムの通信異常を検出した場合に、事前に用意したスクリプトを実行して通信異常の通知等が可能	連携不可	連携不可



## ■ PRIMECLUSTER GLS for Windows(PRIMEQUEST)の優位性(3/3)

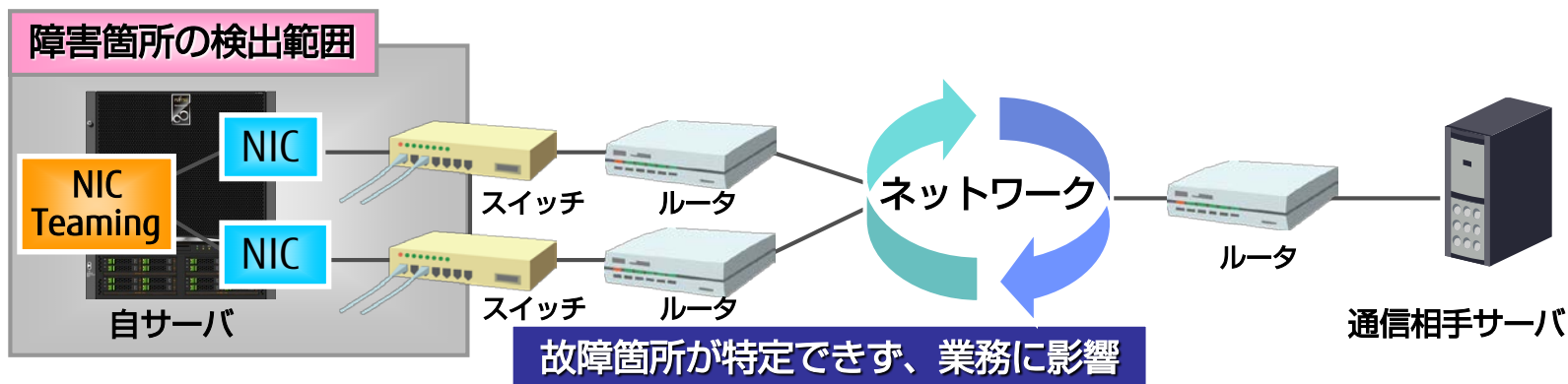
○：適    ×：不適

お客様要件		PRIMECLUSTER GLS for Windows (PRIMEQUEST)	Intel PROSet	OSの NIC チューニング
マルチプラットフォームでの運用	運用・保守方法の統一	○	×	×
		Windows/Linux/Solarisで運用・保守方法が同じであり、設定や故障箇所の確認方法が統一可能	Windows上でのみ運用可能	Windows上でのみ運用可能
	ネットワーク管理者の負担軽減	○	×	×
		Windows/Linux/Solarisで運用形態が統一しており、管理者の負担を軽減	Windows上でのみ運用可能であるため、管理者は複数の運用スキルが必要	Windows上でのみ運用可能であるため、管理者は複数の運用スキルが必要

## B.1.1 通信の高信頼化

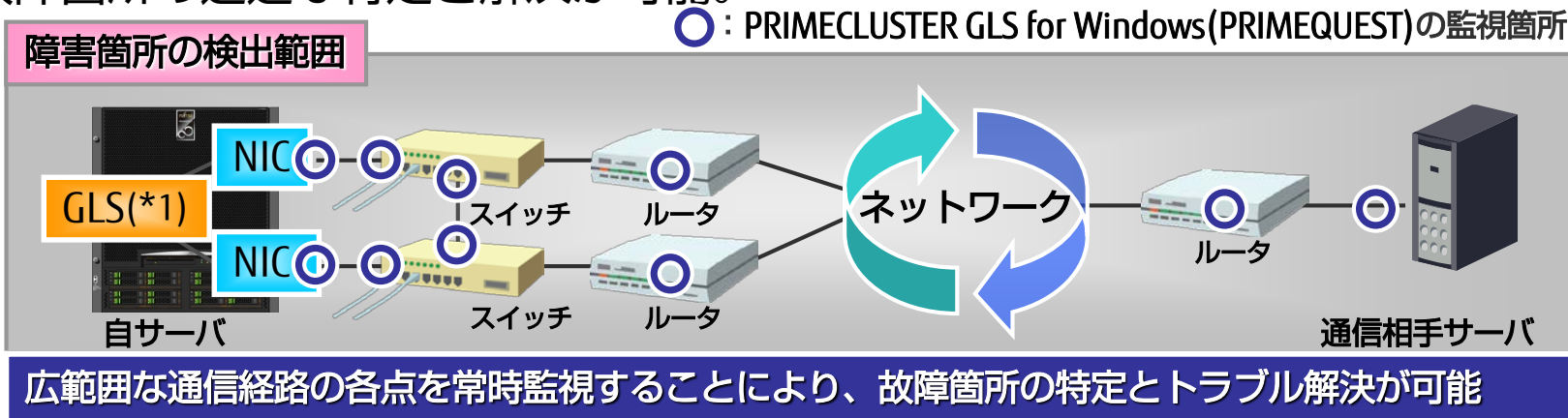
### ■ OSのNICチームングの監視範囲

自サーバからサーバ直結LANポートまでであり、隣接スイッチのハングアップを検出できない。また、通信経路の各点を監視することはできない。



### ■ PRIMECLUSTER GLS for Windows (PRIMEQUEST)の監視範囲

自サーバから通信相手機器までの通信経路において、各点を監視することができ、故障箇所の迅速な特定と解決が可能。



\*1) GLS : PRIMECLUSTER GLS for Windows (PRIMEQUEST)

### ■ 異常検出時のスクリプト実行

物理アダプターの異常や通信異常を検出した場合、ユーザーが事前に用意したスクリプトを実行することにより、システム管理者やアプリケーションへの異常通知等が可能。

スクリプト種別	実行タイミング
伝送路異常検出時	物理アダプターのリンクダウンを検出した場合
	物理アダプターが無効化された場合
通信相手システムの異常検出時	ping監視でネットワーク機器の通信異常を検出した場合
	ping監視で通信相手システムの通信異常を検出した場合

### ■ 統一された障害検出タイミングと設定・確認方法

PRIMECLUSTER GLS for Windows(PRIMEQUEST)は、Linux版、およびSolaris版と運用・保守方法が同じため、Windows/Linux/Solarisが混在したシステムで運用する場合、設定、障害検出タイミング、トラブル時の確認方法を統一できる。

また、ネットワーク管理者に多くのスキルを必要とせず、ネットワーク運用の負担を軽減する。

	Windows	Linux	Solaris
使用ソフト名	PRIMECLUSTER GLS for Windows (PRIMEQUEST)	PRIMECLUSTER GL または、PRIMECLUSTER GLS	
監視方法	Ping		
タイミング	3秒×5回 = 15秒 (Windowsのデフォルト) (*1)		
操作方法	OS設定、専用コマンド		
確認方法	詳細ログ、専用コマンド		

\*1) 監視間隔と回数のチューニングが可能。

**障害検出タイミングの統一が可能。設定やトラブル時の確認方法も同じ**

## ■ チーミングの設定

hanetconfig コマンドを使用して、仮想アダプターを作成する

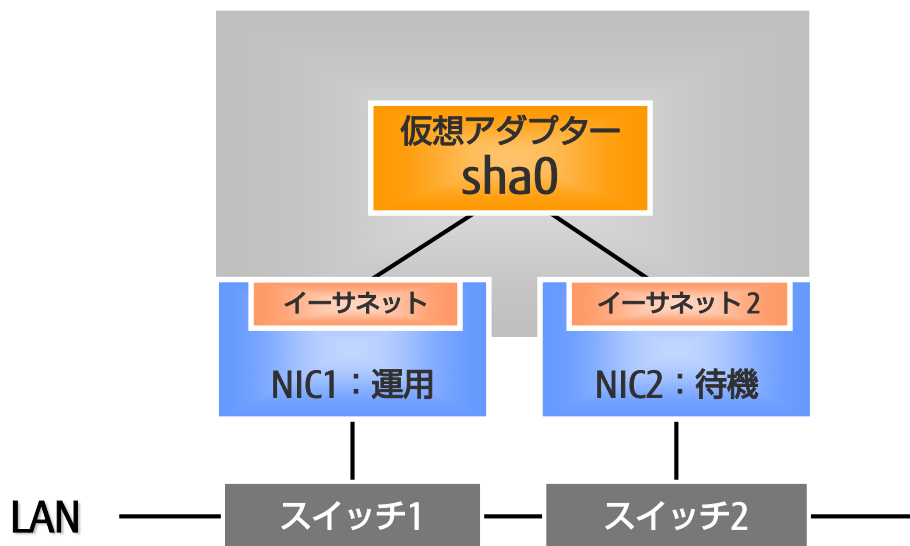
(既存の仮想アダプターを使用したまま、新たに仮想アダプターを追加できるため、業務を継続しつつネットワーク増強に柔軟に対応可能)

実行例：

```
> hanetconfig create -n sha0 -t "イーサネット","イーサネット 2"  
FJSVhanet: INFO: 00000: The command ended normally.
```



詳細は『PRIMECLUSTER GLS for Windows ユーザーズガイド』を参照



## ■ 通信経路の監視設定

### ■ リンク状態監視

設定は不要。自動的に監視を開始する

### ■ ping監視

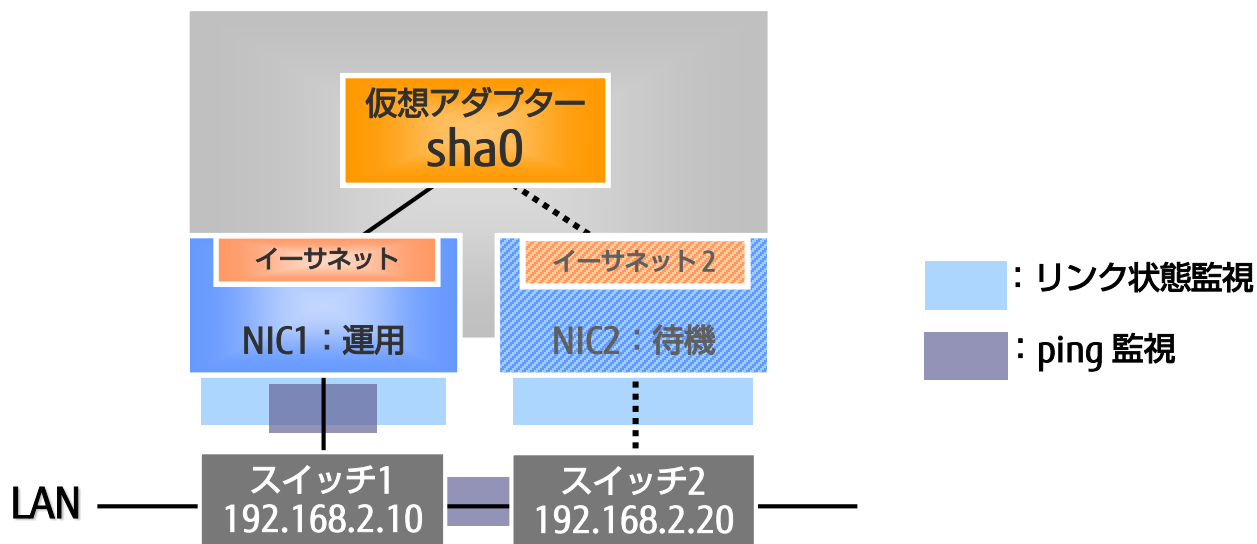
設定高信頼化する通信範囲を拡大する場合、hanetpollコマンドで本機能を設定する

実行例：

```
> hanetpoll create -t "イーサネット" -p 192.168.2.10,192.168.2.20
FJSVhanet: INFO: 00000: The command ended normally.
> hanetpoll create -t "イーサネット 2" -p 192.168.2.10,192.168.2.20
FJSVhanet: INFO: 00000: The command ended normally.
```



詳細は『PRIMECLUSTER GLS for Windows ユーザーズガイド』を参照



## 付録C. ハードウェア監視のためのネットワーク設計

# C.1 ハードウェア監視方法

## ■ ハードウェア/ミドルウェアを監視する方法

### ■ MMB/BMC+SVASによる監視

- PRIMEQUEST筐体を1つの管理単位として監視

### ■ SV Agents/SV RAIDによる監視

- 各パーティションを1つの管理単位として監視

○：監視可  
 ×：監視不可  
 ←：左記の手段により監視している

監視対象		デフォルト		任意インストール
		MMB/BMC	SVAS	SV Agents/SV RAID
ハードウェア	CPU,DIMM,Chipset	○	←	○
	Temp,Voltage,FAN	○	←	○
	SAS RAID Card	○	←	○
	RAID Card以外のPCIe Card	×	○	○
	Boot/Software Watchdog	×	○	○
	Partiotion Status	×	○	○
ミドルウェア	GLS(*1)/EMPD(REMCS通知)	×	○	×
	ROR/Systemwalker	○ MMBのMIBに アクセスする	×	○ ServerViewのMIBに アクセスする

\*1)GLS : PRIMECLUSTER GLS for Windows(PRIMEQUEST)

## ■ 運用管理ソフトウェアと連携する場合はSNMPトラップ設定が必要

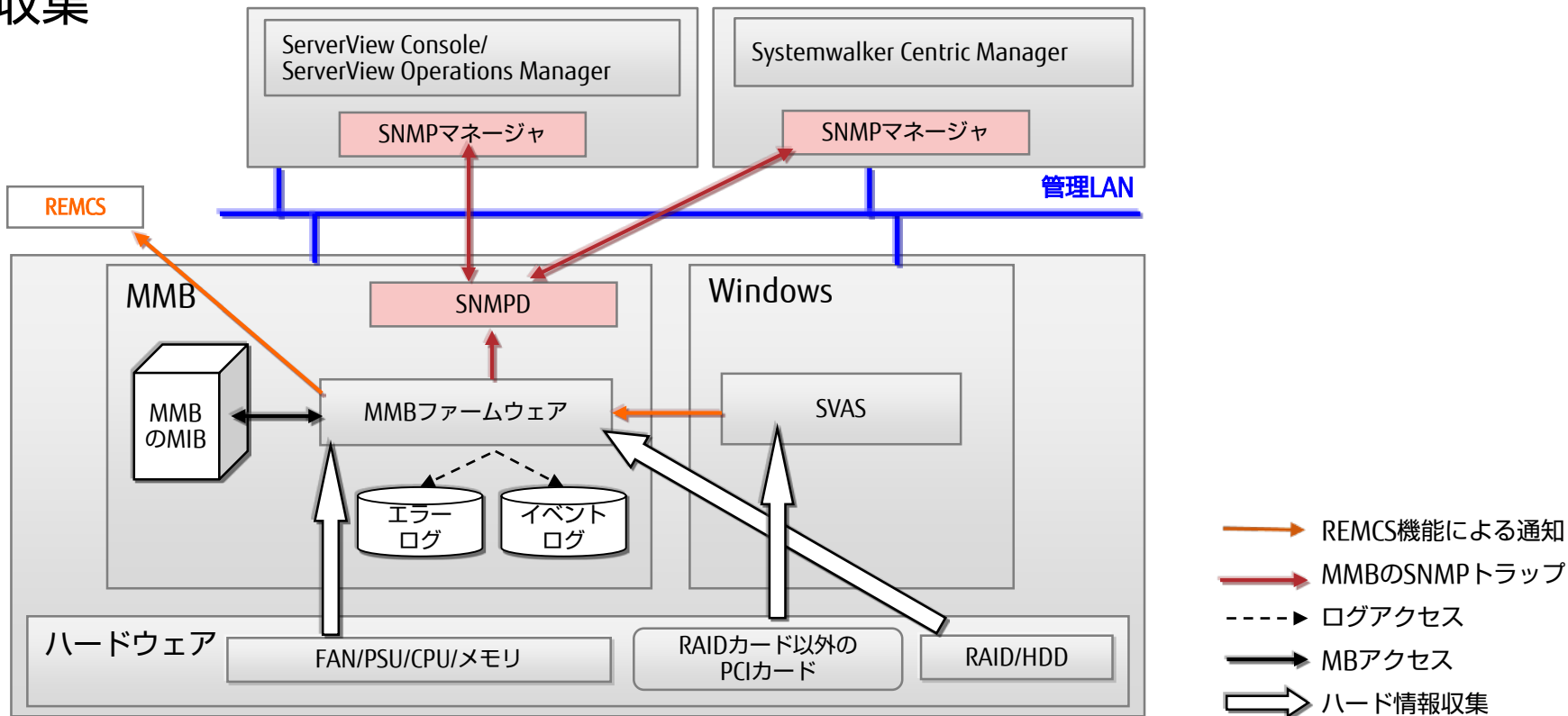
SVSの詳細はマニュアル

<http://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/catalog/manual/svs/> を参照

- 『ServerView Suite Basic Concepts』
- 『ServerView Suite ServerView Operations Manger』の『取扱説明書』
- 『ServerView Suite ServerView RAID Management』の『取扱説明書』



## ■ MMB/BMC+SVASから監視対象コンポーネントへのアクセスルートとログ収集



### ■ SNMPアクセスルート（運用管理ソフトと連携する場合のみ）

- MMBのトラップルート  
トラップ情報の発生元は、PRIMEQUESTシステム全体として表示される

### ■ SNMPが流れるLAN

- 管理LAN  
PRIMEQUESTからSNMPマネージャへのSNMPトラップ送信に使われる

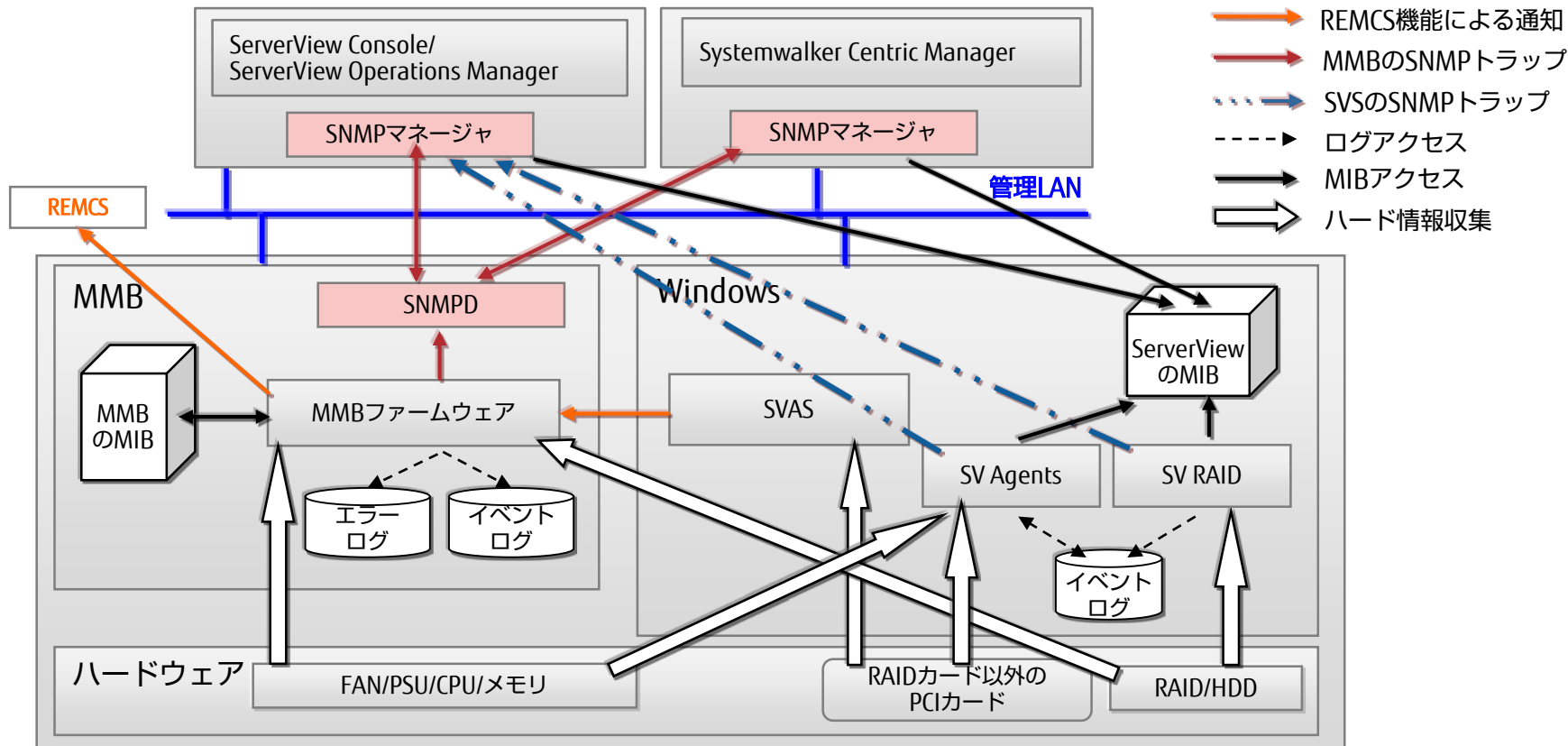
- SVASのネットワーク設計は不要
- 運用管理ソフトウェア(\*1)がSNMPを使ってPRIMEQUEST管理する場合に、MMBからのSNMPトラップを利用する

MMBからのSNMPトラップ監視	
要件	運用管理ソフトからPRIMEQUEST全体を1つの管理単位として監視する
	<ul style="list-style-type: none"><li>• SNMPマネージャーはMMBへのアクセスのみで、MMBおよび全パーティションの情報収集が出来る</li><li>• SNMPマネージャーはMMBへのSNMP設定のみ必要（各パーティションへの設定不要）</li><li>• 運用管理ソフトが受信するトラップ情報は、全て発生元としてPRIMEQUESTと表示される（トラップ内容によりどのパーティションで発生したかは判別可能）</li></ul>
設計点	MMB Web-UIのNetwork ConfigurationメニューのSNMPに設定するMMBのトラップ送信先と、メール送信先を決める

\*1) SVSおよびSystemwalker Centric Managerを意味します。

- 👉 Systemwalker Centric Managerの詳細は『Systemwalker Centric Manager 技術情報一覧 <http://www.fujitsu.com/jp/products/software/resources/technical/systemwalker/centricmgr/>』を参照
- 👉 SNMPの設定方法については、『導入マニュアル 第6章 導入後の作業』を参照

## ■ SV Agents/SV RAIDから監視対象へのアクセスルートとログ



### ■ SNMPアクセスルート

- MMBのトラップルート  
トラップ情報の発生元はPRIMEQUESTシステム全体として表示される
- SVSによるパーティション直接のトラップルート  
トラップ情報の発生元はパーティションごとに表示される

### ■ SNMPが流れるLAN

- 管理LAN  
PRIMEQUESTからSNMPマネージャへのSNMPトラップ送信に使われる

- 運用管理ソフトウェア(\*1)がSNMPを使ってPRIMEQUEST管理する場合に、SVSのSNMPトラップを利用する

ServerViewからのSNMPトラップ監視	
要件	運用管理ソフトから各パーティションを1つの管理単位として監視する
	• 運用管理ソフトは受信したトラップ情報の発生元をパーティション毎に表示できる
設計点	Windowsのサービスマネージャにある[SNMP Service]に設定するコミュニティ名とトラップ送信先(サーバのホスト名またはIPアドレス)を決める ・ トラップ送信先では、トラップ受信用のアプリケーションや管理マネージャが動作していて、SNMPサービスの標準トラップが受信できる必要がある

\*1) SVSおよびSystemwalker Centric Managerを意味します。

- 上位ソフトウェアと連携する場合はファイアウォールの設計が必要
  - 管理LANのファイアウォール設計
    - SNMP Serviceが使用するUDP:161ポート(MMBからの受信)
    - 管理コンソール画面へのアクセスなど、環境によっては他のポートの開放も必要（詳細は以下を参照）
  - ☞ SVOMが使用するポートは、以下のマニュアルデータベースから参照  
<http://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/catalog/manual/svs/>  
『ServerView Operations Manager』の  
『Installing ServerView Operations Manager Software under Windows』
  - ☞ Systemwalker Centric Managerが使用するポートは、以下のマニュアルを参照  
<http://www.fujitsu.com/jp/products/software/resources/technical/systemwalker/centricmgr/>  
『Systemwalker Cenric Manager 導入手引書』
- 業務LANのファイアウォール設計  
PRIMEQUEST独自の設計ポイントはない

版数	日付	変更箇所	変更内容
01	2014-04-10	•新規作成	—
02	2014-07-22	•全体	<ul style="list-style-type: none"> <li>•iSCSIブートに対応</li> <li>•情報の最新化</li> </ul>
03	2015-02-10	•全体	<ul style="list-style-type: none"> <li>•FCoEブートに対応</li> <li>•情報の最新化</li> </ul>
04	2015-05-08	•はじめに	<ul style="list-style-type: none"> <li>•PRIMEQUEST 2400S2 Lite/2400S2/ 2400E2/ 2400L2/2800E2/2800L2対応の略称を追加</li> <li>•システム構成図の略称を追加</li> </ul>
		•1章・2章	•PRIMEQUEST 2400S2 Lite/2400S2/ 2400E2/ 2400L2/ 2800E2/ 2800L2対応のため注釈を変更
		•5章	<ul style="list-style-type: none"> <li>•ハードウェアイニシエータ情報を追加</li> <li>•iSCSI接続時の考慮を変更</li> </ul>
		•6章	•FCoE接続時の結線図を変更
		•付録A	•LANポートの接続先確認方法(4/4)を変更
05	2015-06-16	•はじめに	•使用していない本文中の略称などを削除
		•1章・2章	•CNAの「1パーティションあたり最大4枚」の制限解除により、注釈変更
		•5章	<ul style="list-style-type: none"> <li>•iSCSIブートはWS2012R2のみ可能につき、注釈変更</li> <li>•表のCNAの項目を変更</li> </ul>
		•6章	•参照先ガイド名を変更
06	2015-07-14	•5章	•利用可能なiSCSIイニシエータの状況を7月時点に変更
		•改版履歴	•改版履歴（04版、05版）の変更内容を記載

版数	日付	変更箇所	変更内容
07	2015-09-08	• 1章	• Internal LANの説明に注釈を追加
		• 全体	• 用語「PCIスロット拡張ボックス」を「PCIボックス」に変更
08	2015-10-06	• 3章	• 「Active Directory環境での考慮」にスライドを追加
09	2016-06-07	• はじめに	• PRIMEQUEST 2400S3 Lite/2400S3/ 2400E3/ 2400L3/2800E3/2800L3対応の略称を追加 • システム構成図の略称を追加
		• 5章	• 利用可能なiSCSIイニシエータの状況を最新化 • iSCSI接続の構成パターンに説明を追加
		• 6章	• FCoE接続の構成パターンに説明を追加
		• 付録B	• 用語「ローカル エリア接続」を「イーサネット」に変更
		• 全体	• ページ構成変更に伴うURLの変更
10	2017-06-09	• 全体	• Windows Server 2016に対応 • 情報の最新化

## ■ 著作権・商標権・その他の知的財産権について

コンテンツ（文書・画像・音声等）は、著作権・商標権・そのほかの知的財産権で保護されています。本コンテンツは、個人的に使用する範囲でプリントアウトまたはダウンロードできます。ただし、これ以外の利用（御自分のページへの再利用やほかのサーバへのアップロードなど）については、当社または権利者の許諾が必要となります

## ■ 保証の制限

本コンテンツについて、当社は、その正確性、商品性、御利用目的への適合性などに関して保証するものではなく、その御利用により生じた損害について、当社は法律上のいかなる責任も負いかねます。本コンテンツは、予告なく変更・廃止されることがあります  
不明な点は、「本製品のお問い合わせ」


(<http://www.fujitsu.com/jp/products/computing/servers/primequest/contact/>)よりお尋ねください。

無断転載を禁じます。

C122-A019-10

2017.06





**FUJITSU**

shaping tomorrow with you