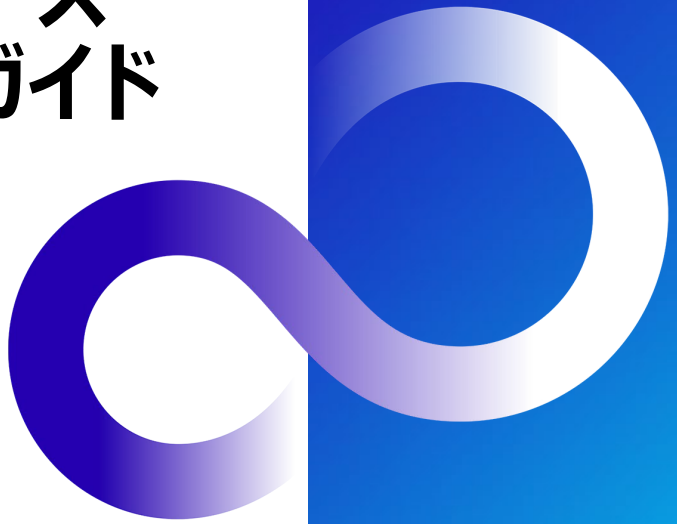
FUJITSU Server PRIMEQUEST 3000シリーズ Windowsネットワーク設計ガイド



CA92344-2153-03

目次

目次(続き)

目次(続き)

目次(続き)

- 本文中の略称

名称	略称	
Microsoft® Windows Server® 2022 Standard	Windows Server 2022	Windows
Microsoft® Windows Server® 2022 Datacenter		
Microsoft® Windows Server® 2019 Standard	Windows Server 2019	
Microsoft® Windows Server® 2019 Datacenter		
Microsoft® Windows Server® 2016 Standard	Windows Server 2016	
Microsoft® Windows Server® 2016 Datacenter		
Microsoft® Windows Server® 2012 R2 Standard	Windows Server 2012 R2	
Microsoft® Windows Server® 2012 R2 Datacenter		

はじめに

FUJITSU

- 本文中の略称

<table>
<tr><th>名称</th><th colspan="2">略称</th></tr>
<tr><td>PRIMEQUEST 3400S2 Lite</td><td rowspan="6">PRIMEQUEST 3400S2 Lite / 3400S2 / 3400E2 / 3400L2 / 3800E2 / 3800L2</td><td rowspan="12">PRIMEQUEST 3000シリーズ または PRIMEQUEST</td></tr>
<tr><td>PRIMEQUEST 3400S2</td></tr>
<tr><td>PRIMEQUEST 3400E2</td></tr>
<tr><td>PRIMEQUEST 3400L2</td></tr>
<tr><td>PRIMEQUEST 3800E2</td></tr>
<tr><td>PRIMEQUEST 3800L2</td></tr>
<tr><td>PRIMEQUEST 3400S Lite</td><td rowspan="6">PRIMEQUEST 3400S Lite / 3400S / 3400E / 3400L / 3800E / 3800L</td></tr>
<tr><td>PRIMEQUEST 3400S</td></tr>
<tr><td>PRIMEQUEST 3400E</td></tr>
<tr><td>PRIMEQUEST 3400L</td></tr>
<tr><td>PRIMEQUEST 3800E</td></tr>
<tr><td>PRIMEQUEST 3800L</td></tr>
</table>

- 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
integrated Remote Management Controller	iRMC
IOユニットE	IOUE
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

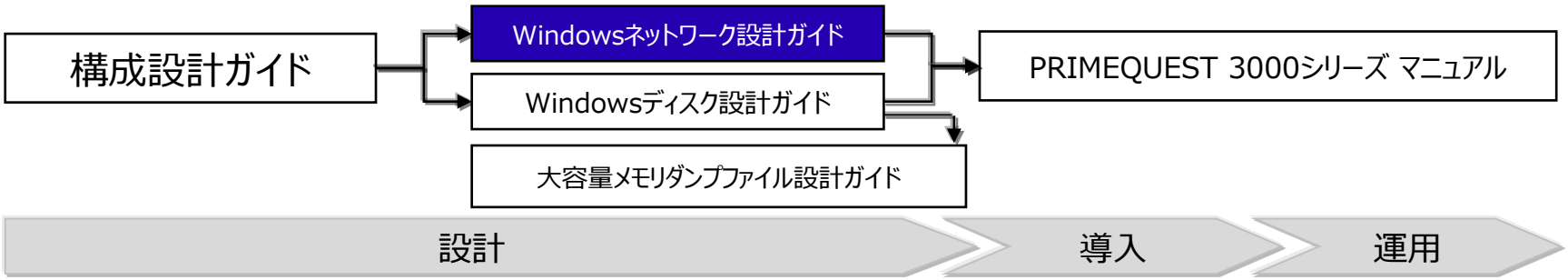
はじめに

- 本文中の略称

名称	略称
FUJITSU Server PRIMEQUEST 3000シリーズ 導入マニュアル	導入マニュアル
FUJITSU Server PRIMEQUEST 3000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 3000シリーズ 構成設計ガイド	構成設計ガイド
FUJITSU Server PRIMEQUEST 3000 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 3000シリーズシステム構成図 (PRIMEQUEST 3400S2 Lite / 3400S2 / 3400E2 / 3400L2 / 3800E2 / 3800L2)	システム構成図
FUJITSU Server PRIMEQUEST 3000シリーズシステム構成図 (PRIMEQUEST 3400S Lite / 3400S / 3400E / 3400L / 3800E / 3800L)	
FUJITSU Server PRIMEQUEST 3000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
Windows Server 2022 / 2019 / 2016 / 2012 R2 OS標準NICチーミング(LBFO)設定ガイド	LBFO設定ガイド
PRIMECLUSTER GL for Windows (PRIMEQUEST) 4.5 以降 および、PRIMECLUSTER GLS for Windows (PRIMEQUEST) 4.4 以前	PRIMECLUSTER GL for Windows (PRIMEQUEST)
PRIMECLUSTER GL for Windows ユーザーズガイド4.5 以降 および、PRIMECLUSTER GLS for Windows ユーザーズガイド 4.4 以前	PRIMECLUSTER GL for Windows ユーザーズガイド

- 本書の読み方
  - 本書の内容
    PRIMEQUEST 3000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 3000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 3000シリーズ Windows Server情報の
      サポート情報を参照してください
      https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/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 3000シリーズのシステム構成図を参照してください
      https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/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
      https://www.fujitsu.com/jp/products/software/resources/condition/configuration/

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。

はじめに

- 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、Broadcom Ltd.の登録商標です
- QLogicは、米国QLogic 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

はじめに

- Windows Server を導入するにあたって

  PRIMEQUESTにWindows Serverを導入するさいは、マイクロソフト社より公開されている最新の累積的な更新プログラムを適用してください。

  留意事項の詳細は下記を参照してください。

  - FUJITSU Server PRIMEQUEST 3000シリーズ Windows Server 2022 留意事項
    https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/os/windows/
  - FUJITSU Server PRIMEQUEST 3000シリーズ Windows Server 2019 留意事項
    https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/os/windows/support/2019/consideration/index.html
  - FUJITSU Server PRIMEQUEST 3000シリーズ Windows Server 2016 留意事項
    https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/os/windows/support/2016/consideration/index.html
  - FUJITSU Server PRIMEQUEST 3000シリーズ Windows Server 2012 R2 留意事項
    https://www.fujitsu.com/jp/products/computing/servers/primequest/products/2000/os/windows/support/2012/r2/consideration/index.html

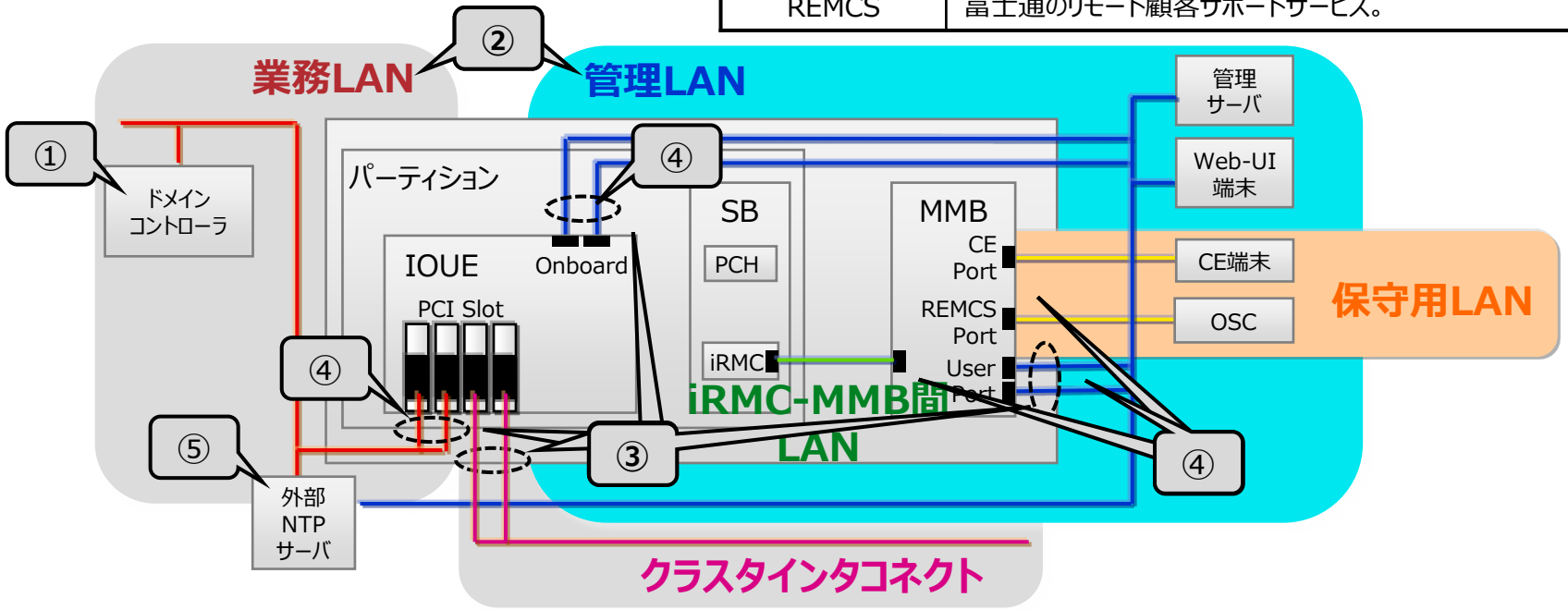
1. 前提知識

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フェースを持つ。
iRMC	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。
IOUE	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動させる単位。
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。



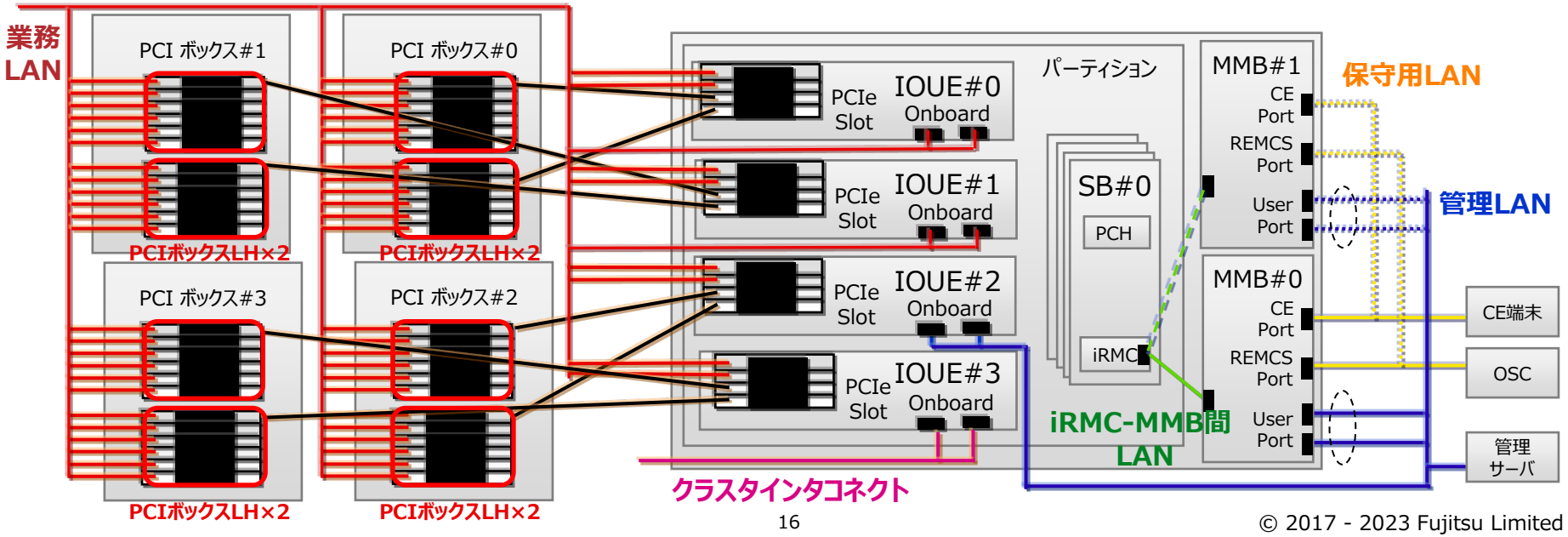
PRIMEQUESTの外部ネットワークについては
『運用管理マニュアル　第１章 ネットワーク環境の設定と管理ツールの導入』を参照

1.2 最大ネットワーク構成

- 最大ネットワーク構成(PRIMEQUEST 3800E3/4SB 4IOUE 1パーティションの場合)

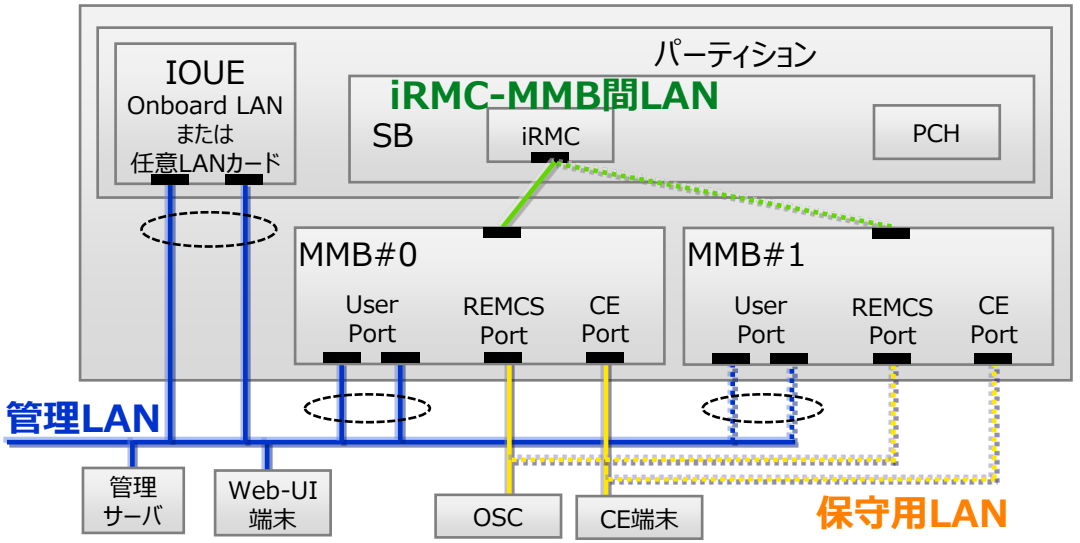
ポート名		接続コンポーネント	最大ポート数/搭載カード数	用途
管理LAN	Userポート	MMB(*1)	2ポート	MMB Web-UI操作用
	管理サーバ用LAN	業務LANと同一コンポーネント	–	監視や管理、バックアップ用
保守用LAN	CEポート	MMB(*1)	1ポート	保守専用の端末接続用
	REMCSポート		1ポート	REMCS 用
iRMC-MMB間LAN		iRMC	–	iRMC-MMB間通信用
業務LAN		IOUEのオンボードLAN	8ポート	お客様の業務用
		IOUEのPCIeスロットに挿すLANカード/CNA	8枚(*2)	
		PCIボックスのPCIeスロッ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

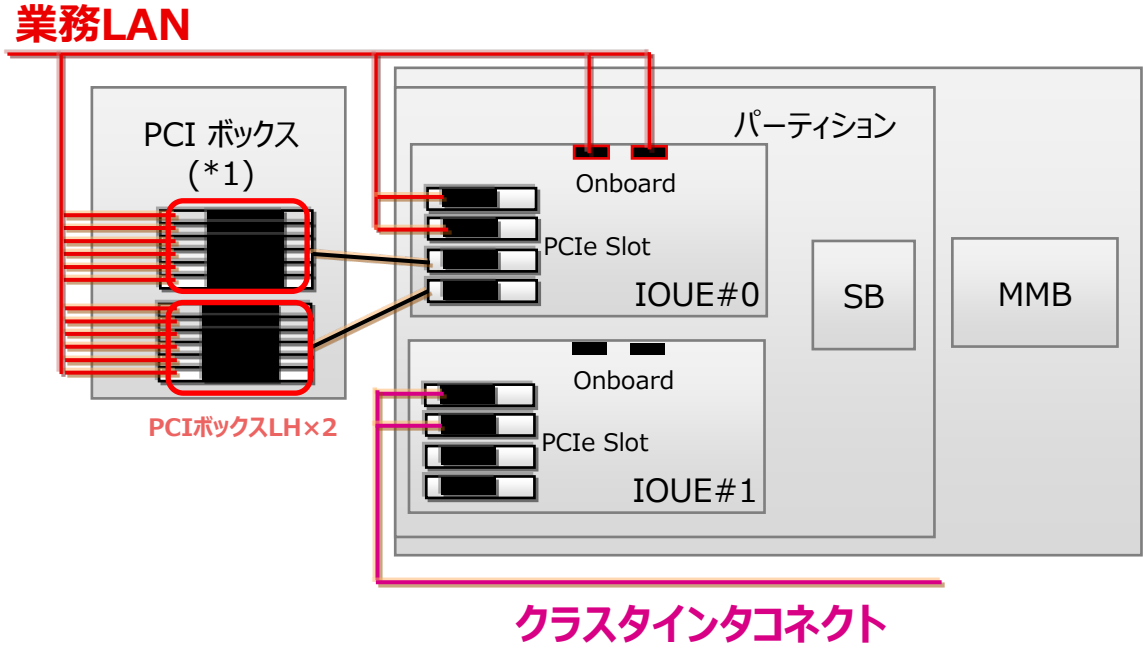
- 管理LAN
  - Web-UI端末や管理サーバとPRIMEQUEST内の各パーティションおよびパーティション同士を接続するLAN
- 保守用LAN
  - 保守作業のために CE端末やOSCと PRIMEQUESTを接続するLAN



- iRMC-MMB間LAN
  - iRMC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、PCIボックスLHとして別々にIOUEと接続されます。

FUJITSU

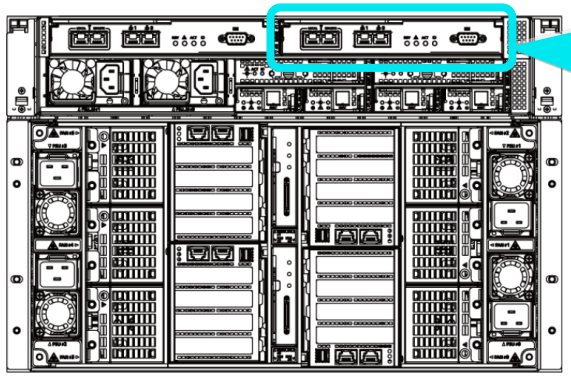
2. ネットワークコンポーネント

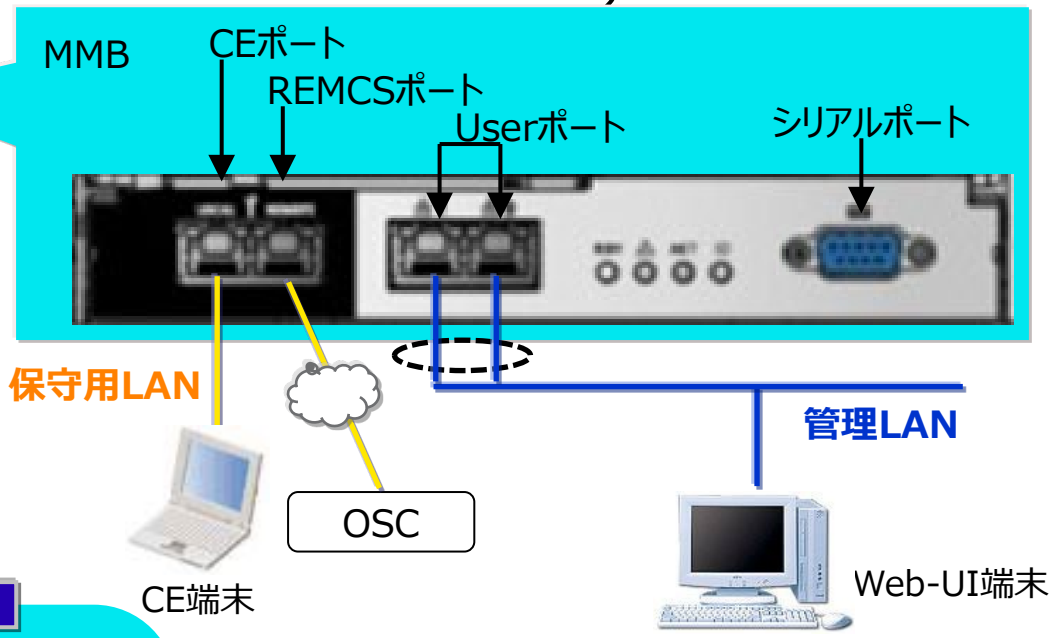
ネットワークを構成するコンポーネントについて説明します。

2.1 管理LAN/保守用LANを構成する主要コンポーネント

FUJITSU

- 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

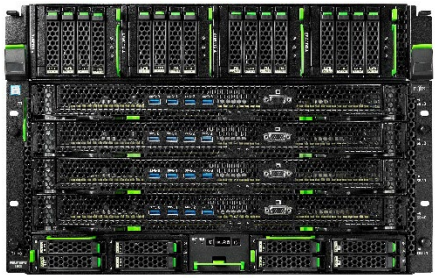
外部インタフェース	数	内容
シリアルポート	1	CEの装置セットアップ作業で使用
LAN	4	• Userポート 1Gbps×2ポート • CE用ポート 100Mbps×1ポート • REMCS用ポート 100Mbos×1ポート

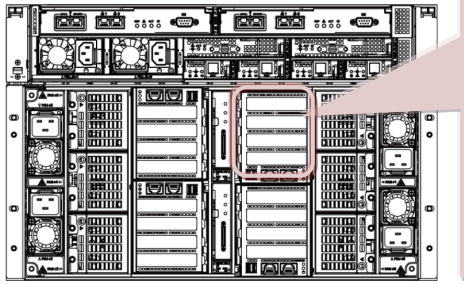
2.2 業務LANを構成する主要コンポーネント

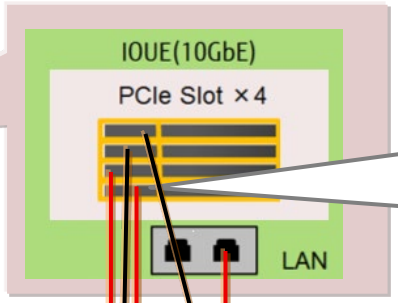
FUJITSU

- IOUE(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
IOUE(10GbE)	10GbE 2ポート	最大4枚	最大2枚







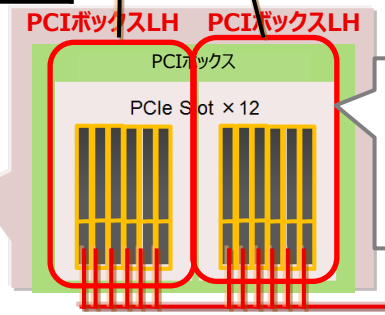
PCIボックス接続時はIOUEのPCIeスロットに最大2枚のPCIボックス接続カードを搭載する。

業務LAN

- 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	PCIボックス1台あたり12枚 (PCIボックスLH1つあたり6枚)

IOUEに対して、PCIボックスLHが1つ接続可能。



PCIボックスの内部にはカードを搭載するスロットが12本存在し、6スロットずつ分割されている(PCIボックスLH)。

*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です。

FUJITSU

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を設ける
  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 /CE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

FUJITSU

- 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	• 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	○	–	○
3.4	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 • 利用するLANポートの決定	○	–	○
3.5	ネットワークの信頼構成設計	• 接続するネットワークを二重化構成にする • PRIMEQUEST搭載のネットワーク コンポーネントを冗長化 • チーミングソフトウェアを選択	○	–	○
3.6	IPアドレスの割り当て	IPアドレスを決定	○	○	○
3.7	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

FUJITSU

- 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)

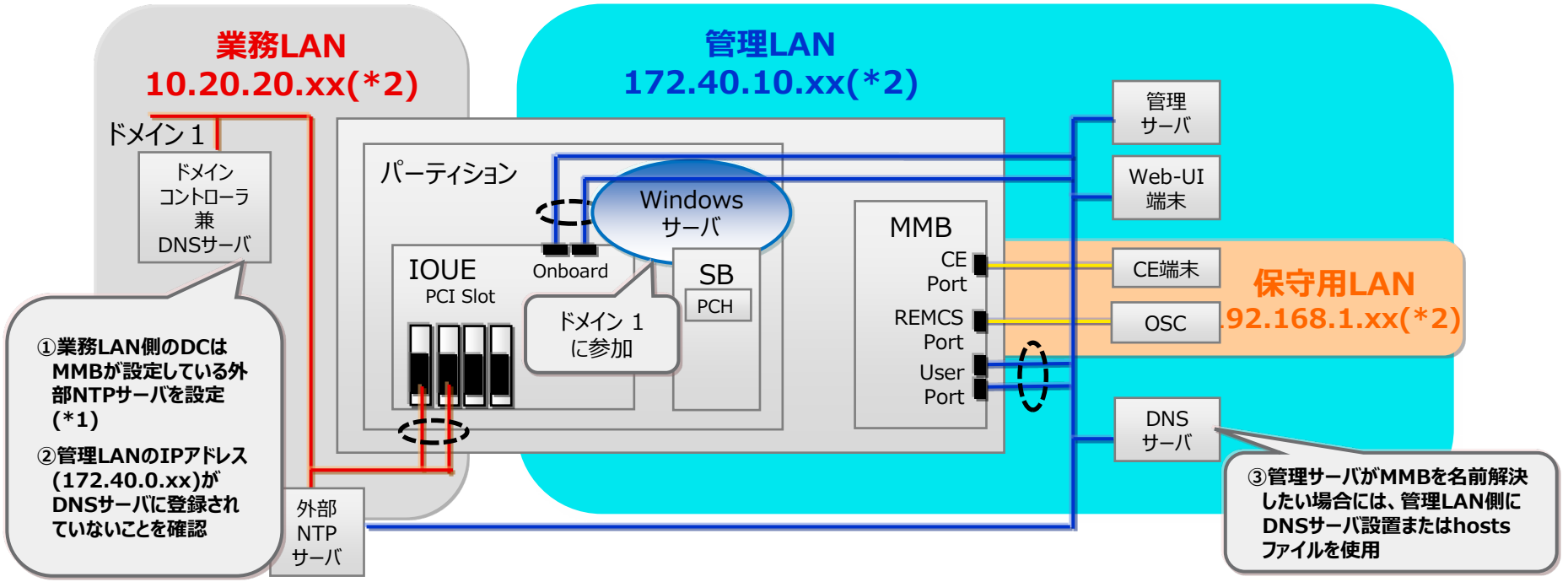
- 業務LAN側のみにドメインコントローラを配置する場合

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。
WS2022 / WS2019は外部PTPサーバによる時刻同期をサポートしていますが、MMBはサポートしていません。
*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)

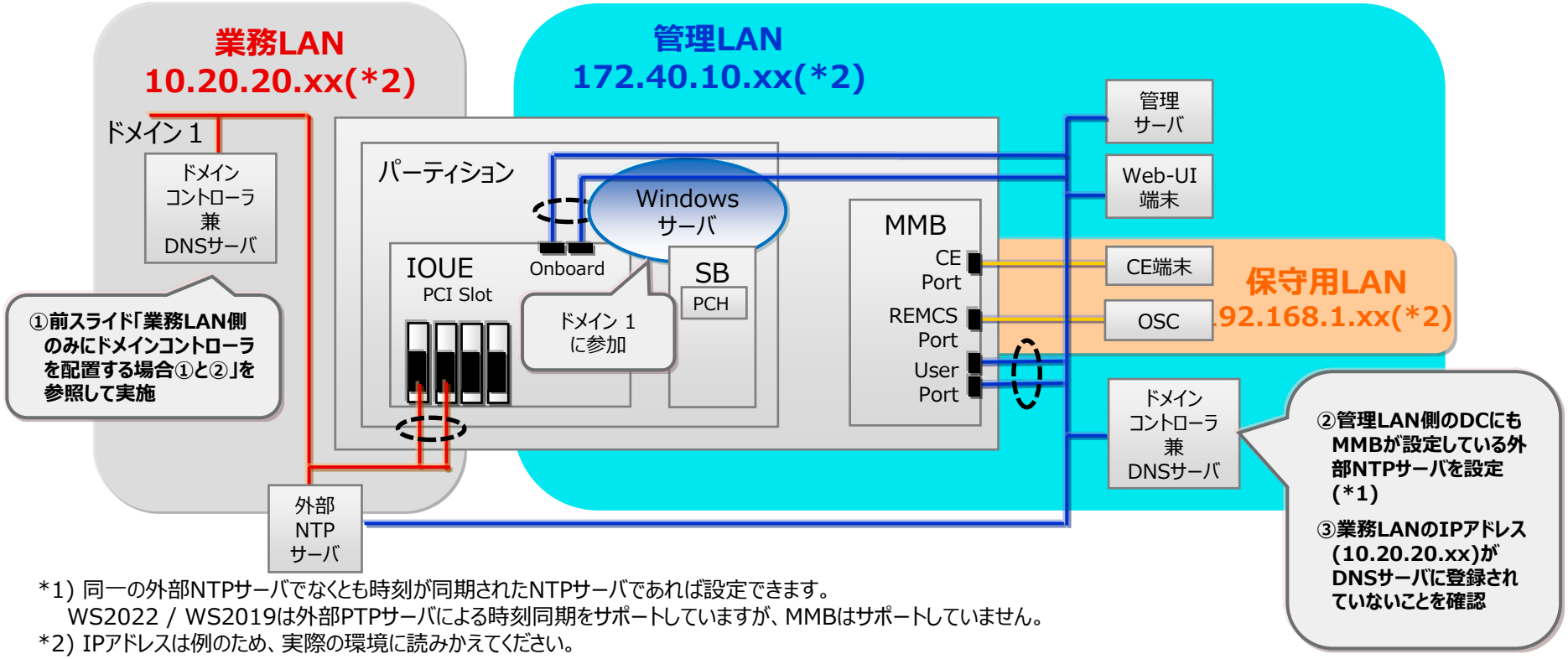
- 管理LAN側にもドメインコントローラを配置する場合

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側のみ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



*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。
WS2022 / WS2019は外部PTPサーバによる時刻同期をサポートしていますが、MMBはサポートしていません。
*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。

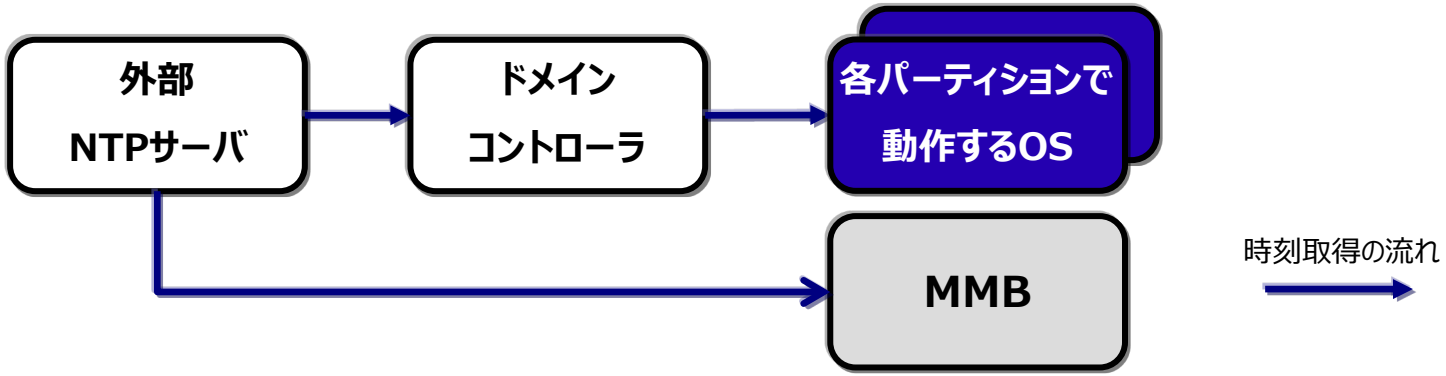
3.3.2 ドメイン メンバサーバの時刻同期の方法

FUJITSU

- 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『3.7 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「Windows Server で権限のあるタイム サーバーを構成する方法」を参照
https://docs.microsoft.com/ja-JP/troubleshoot/windows-server/identity/configure-authoritative-time-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® Ethernet Controller X540-AT2	IOUE (10GbE)	IOUEあたり 2ポート	• 故障時はIOUE単位で交換 • 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
LAN カード /CAN	IOUE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	IOUE(10GbE) 4スロット	• カード故障または拡張時はカード単位で交換 • IOUE故障時はIOUE単位で交換 • PCIホットプラグ機能は不可（ハード仕様）
	PCIボックスの PCI Express スロット			PCIボックス1台あたり12スロット	• カード故障または拡張時はカード単位で交換 • PCIボックス故障時はPCIボックス単位で交換 • PCIホットプラグ機能をサポート

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

3.5 ネットワークの信頼構成設計

- 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 チーミ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
  - 利用するチーミングソフトウェアに応じて、STPの設定を行う
    - PRIMECLUSTER GL for Windows(PRIMEQUEST)を利用する場合
      STPを有効化する。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。
      ＜STP有効時の留意点 (*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。

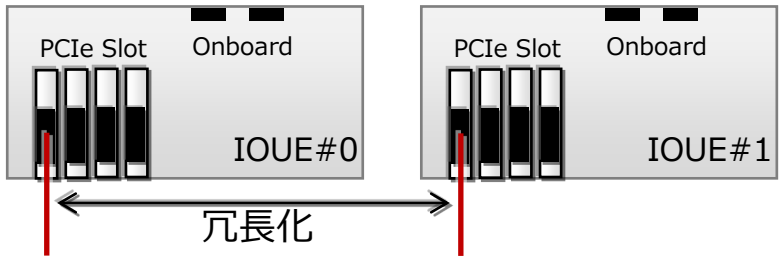
詳細は『PRIMECLUSTER GL for Windows ユーザーズガイド』を参照

3.5.2 ネットワークコンポーネントの冗長化

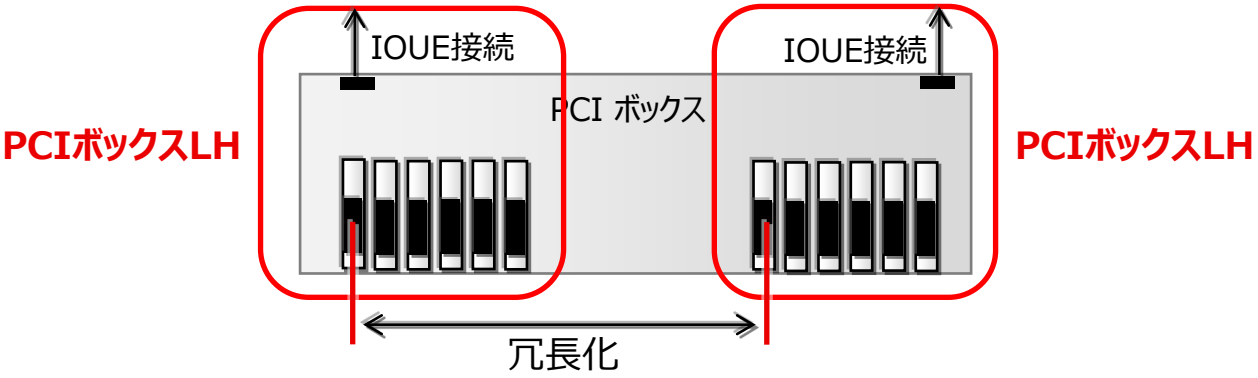
- PRIMEQUEST搭載のネットワークコンポーネントを選択する

  以下を考慮して冗長化するLANポートを選択する。

  - 複数のIOUE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IOUE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PCIボックスLH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

3.5.3 チーミングソフトウェアの選択(1/3)

FUJITSU

- 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間で負荷分散や異常発生時のトラフィックの引継ぎをおこなう。
  業務LANまたは管理LANのポートを組み合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3種類
  機能/要件を踏まえて選択する。

  - PRIMECLUSTER GL for Windows (PRIMEQUEST)
  - OSのNICチーミング機能
  - Intel PROSet(*1)

  *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。

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 GL for Windows (PRIMEQUEST)
    - 有償ソフトウェア
    - 最も高信頼性を実現する場合に推奨
    - 業務の即時再開と継続、故障箇所の特定と復旧が可能
    - Windows Server 2022は非対応
  - OSのNIC チーミング機能
    - Windows Server 2012以降の標準機能
    - PRIMECLUSTER GL for Windows (PRIMEQUEST)を利用しない場合に推奨
    - SMBマルチチャネルとの併用が可能
  - Intel PROSet
    - 標準添付ソフトウェア
    - Windows Server 2012 R2を使用している場合にチーミング機能が利用可能
    - 次の条件を満たす場合に推奨
      - Intel製コントローラを使用している
      - SMBマルチチャネルと併用しない

*1)　同種カード間またはIOUE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

3.5.3 チーミングソフトウェアの選択(3/3)

FUJITSU

- チーミングソフトウェアの機能比較

チーミングソフトウェア / 機能/使用可能なOS	PRIMECLUSTER GL for Windows (PRIMEQUEST)	Intel PROSet	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	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	Windows Server 2012 以降の標準機能
使用可能なOS	Windows Server 2012 R2 ～ Windows Server 2019	Windows Server 2012 R2	Windows Server 2012 R2 ～ Windows Server 2022

○：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 2012 R2のみ)。
*2) PRIMECLUSTER GL for Windows(PRIMEQUEST)と組み合わせることで可能。
*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 GL for Windows(PRIMEQUEST)の詳細は『付録Ｂ チーミングソフトウェア』を参照
OSのNICチーミングは『Windows Server 2022 / 2019 / 2016 / 2012 R2 OS標準NICチーミング(LBFO)設定ガイド』を参照

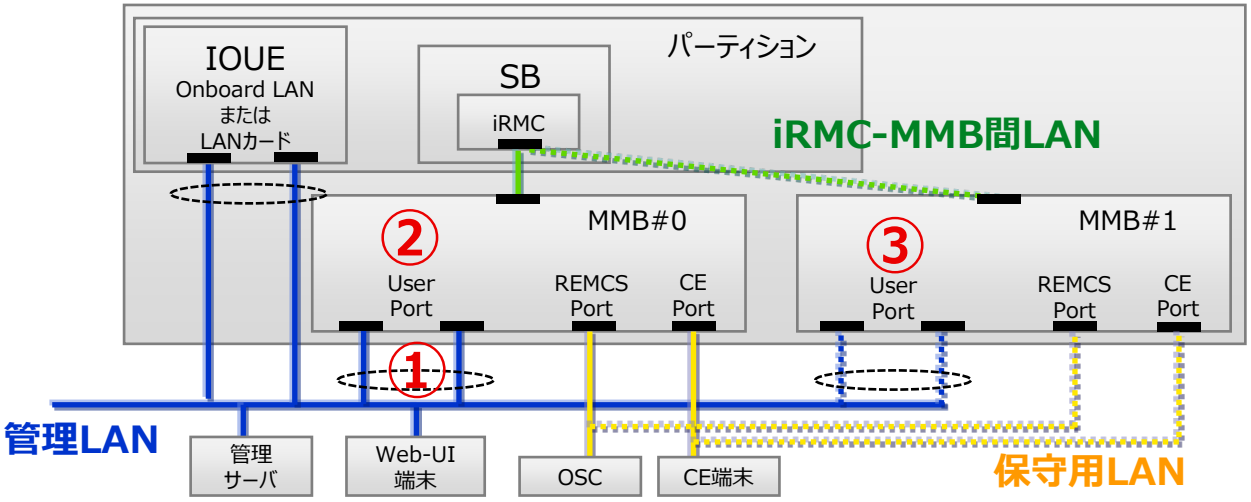
3.6 IPアドレスの割り当て(1/4)

- 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。

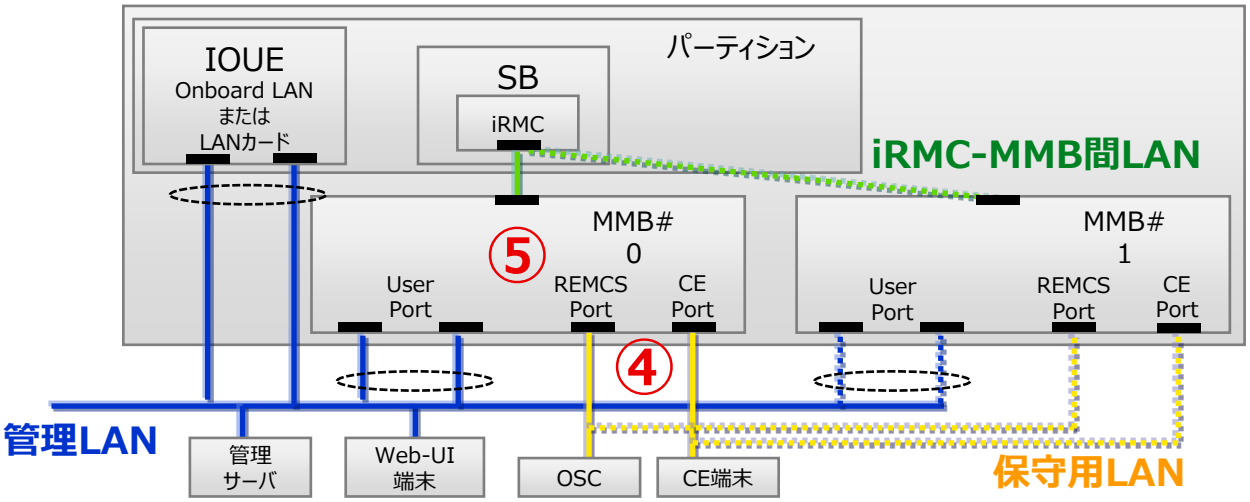


3.6 IPアドレスの割り当て(2/4)

- 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

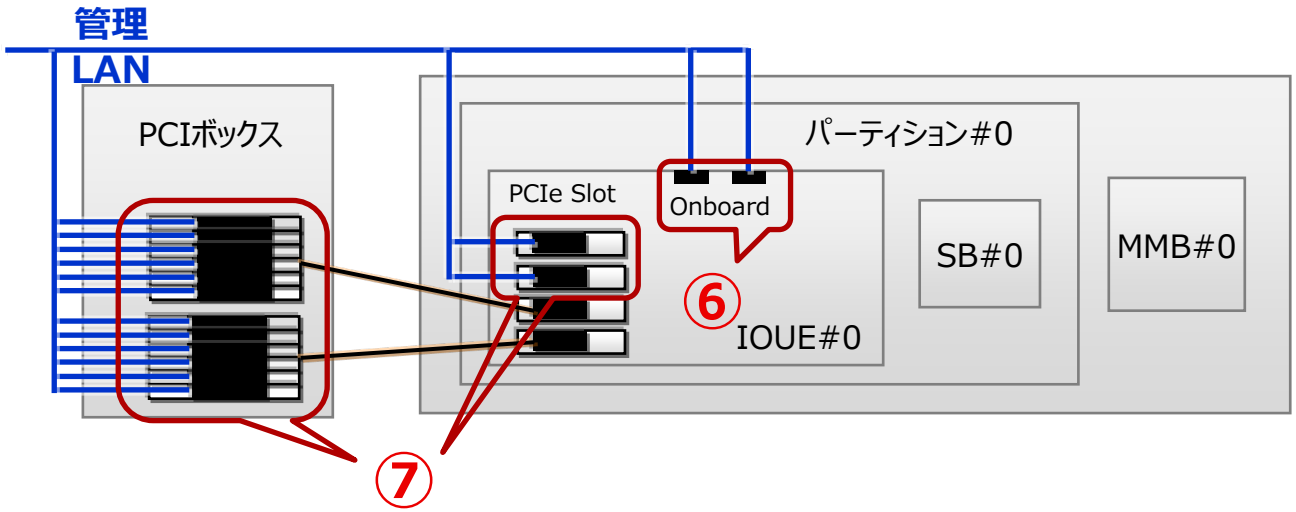
設定項目		NIC	IPアドレス数	設定方法	説明
④	Maintenance IP Address	REMCS/CE Port	1	MMB Web-UI または MMB CLI	REMCSで通信する場合に使用。CE ポートに接続した保守用端末と通信する場合にも使用。 MMBを二重化した場合は、Active側のMMBのみ通信し、MMBが切り替わるとStandby側に同じIPアドレスが割り当てられる。
⑤	Console Redirection Setup	iRMC-MMB間 LAN用のポート (MMB)	パーティション数分	MMB Web-UI	管理LAN上のPCからiRMCの遠隔操作機能を利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

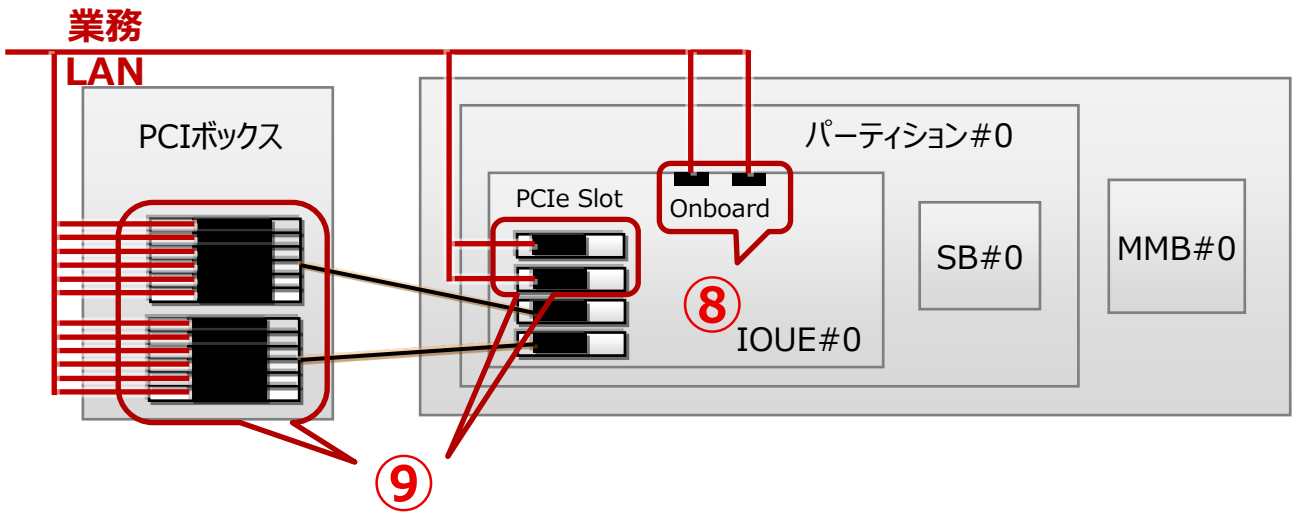
NIC		IPアドレス数	設定方法	説明
⑥	IOUEのオンボードLAN	ネットワークへ接続する数分	Windowsの[ネットワーク接続]のプロパティで設定	各ポートから筐体外のネットワークに接続する管理サーバ用の管理LANとして使用。当該パーティション内のネットワークへ接続する数分のIP アドレスが必要 (実際に使用するポートにIP アドレスを割り当てる)。
⑦	IOUEまたはPCIボックス搭載のLANカード/CNA	ネットワークへ接続する数分	Windowsの[ネットワーク接続]のプロパティで設定	



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
  - 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
⑧	IOUE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	IOUE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	



3.7 時刻同期

- 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]に指定する。

    ☞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。

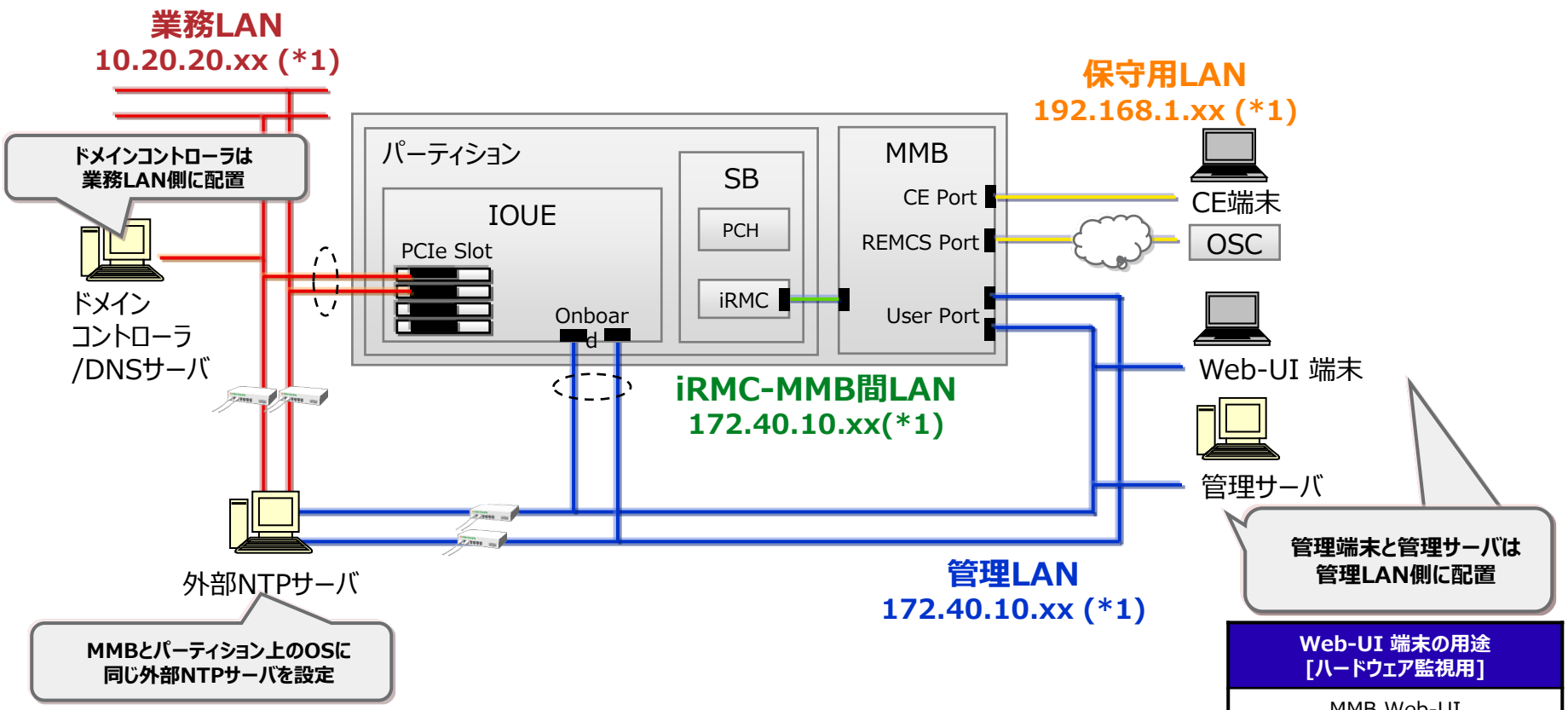
※ Windows環境としてNTPサーバを複数台必要という条件はありませんが、例えば、NTPサーバの耐障害性を考慮したい場合は複数台のNTPサーバを準備してください。

FUJITSU

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



PRIMECLUSTER GL for Windows(PRIMEQUEST)による冗長化

管理サーバの用途 [パーティション管理用]
バックアップ/リストア
管理LAN経由での外部マネージ連携 (SVS/Systemwalkerなど)

Web-UI 端末の用途 [ハードウェア監視用]
MMB Web-UI
MMB CLI
Video Redirection
Console Redirection
Virtual Media
MMB経由での外部マネージ連携 (SVS/Systemwalkerなど)

*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

FUJITSU

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ディスク装置へ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ディスクへ
    iSCSI接続するアクセスパス構成

    
    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

- IOUE搭載のオンボードLANやCNAを使用したiSCSI接続/
  CNAを使用したiSCSIブートの設計ポイントは同じ

  iSCSI専用LANにおいてFCoEスイッチを利用する場合は本章記載のネットワークスイッチを
  FCoEスイッチとして 読み替えてください。

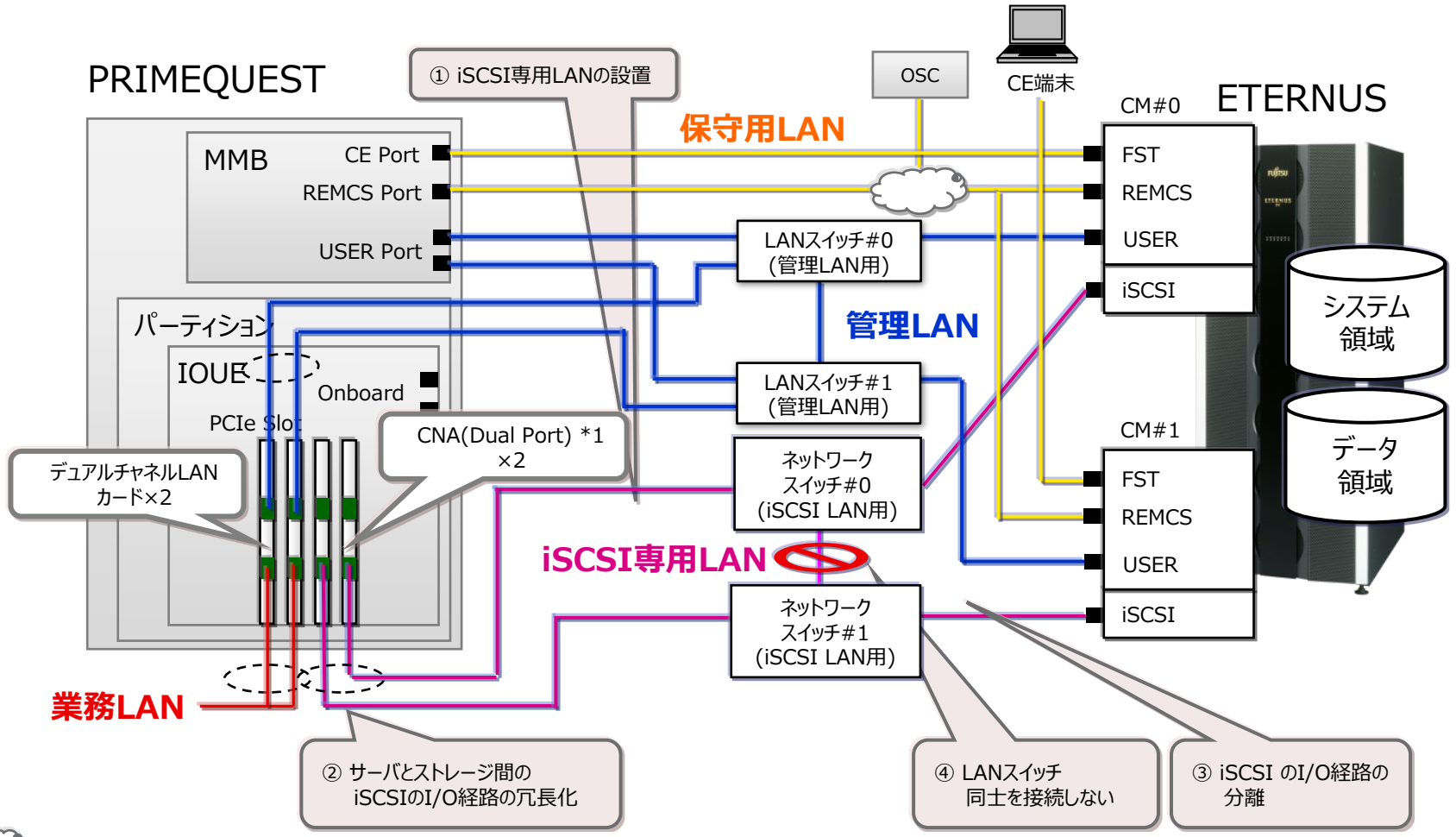
- iSCSI専用LANの設置

  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。

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



*1)iSCSIブートはCNAのみサポート。
iSCSI接続はオンボード、CNA、LANのいずれもサポート。

5.2 iSCSI接続時の考慮(2/3)

FUJITSU

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 ネットワーク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、ネットワークスイッチ同士を接続しない。

*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)

FUJITSU

- 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
  - IOUE搭載のCNAを使用
  - Windows Server 2012 R2において、一部機能が未サポート
    - 仮想スイッチ：「外部ネットワーク」として作成した仮想スイッチが「内部ネットワーク」として表示され、外部ネットワークアダプターを使用することができません。また、作成した仮想スイッチの削除が失敗します。
      外部ネットワークアダプター(外部仮想スイッチ)を使用しないか、Hyper-V役割の削除で回避する必要があります。
    - NICチーミング：詳細はKB2969300を参照
      (https://learn.microsoft.com/en-US/troubleshoot/windows-server/networking/faulted-not-found-status-nic-team-restart-iscsi-boot-disk)

5.3 iSCSIイニシエータの設計

FUJITSU

- 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	IOUEのオンボードLAN	×	×
	オプションLANカード	×	×
	CNA	×	○
iSCSI接続	IOUEのオンボードLAN	○	×
	オプションLANカード	○	×
	CNA	×	○

○：可能　×：不可

- iSCSIイニシエータ設定ツール

  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

FUJITSU

- 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

FUJITSU

- 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

FUJITSU

- 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以外は有効になっている。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施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、再施行回数、再施行間隔、PDO削除期間）
MPIOパスの詳細	パスの状態

FUJITSU

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

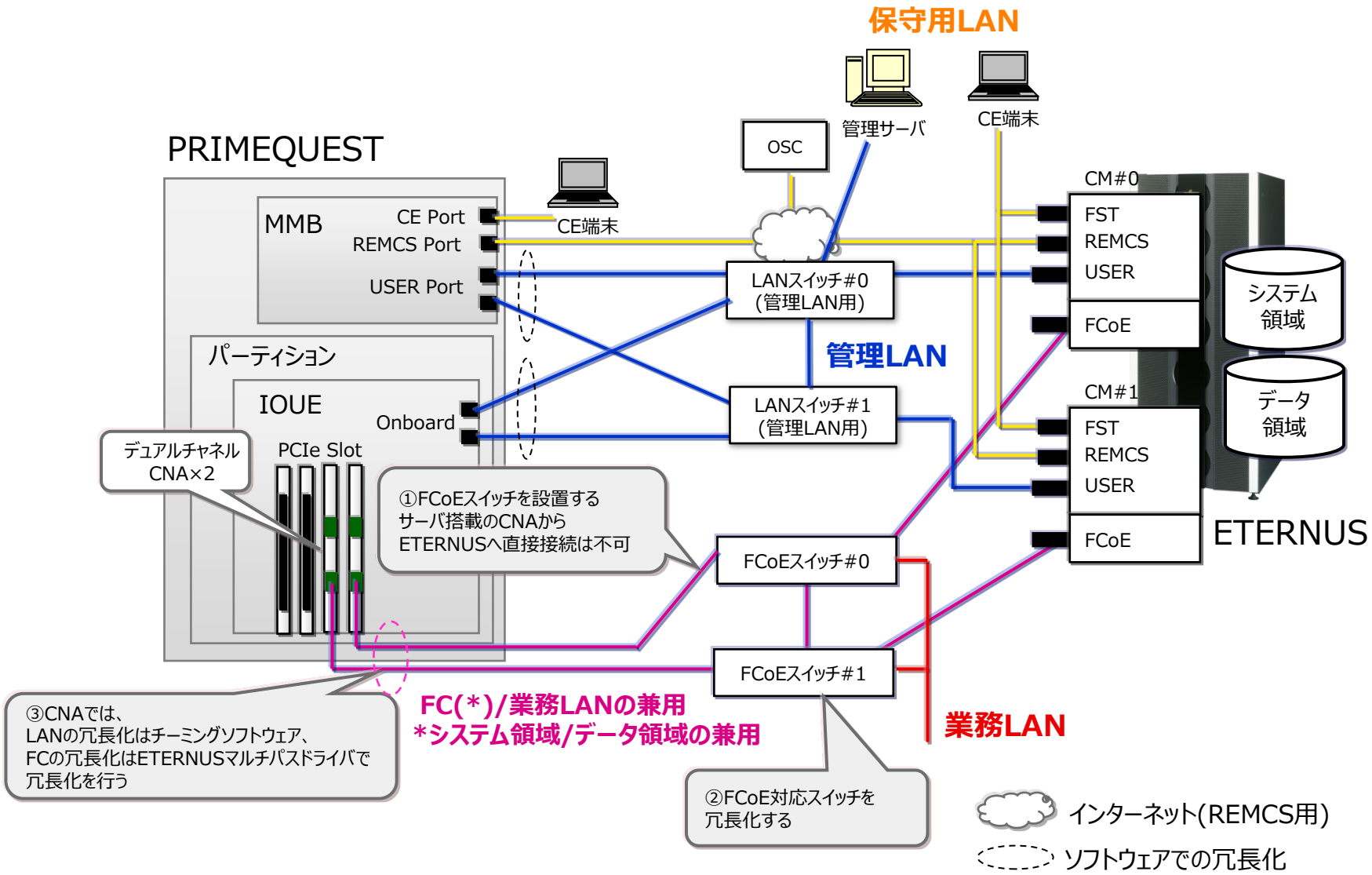
FUJITSU

- 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ディスク装置へ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ディスク装置へ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ディスク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)

FUJITSU

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)

FUJITSU

- 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
  - OS標準機能([ネットワーク接続]画面)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

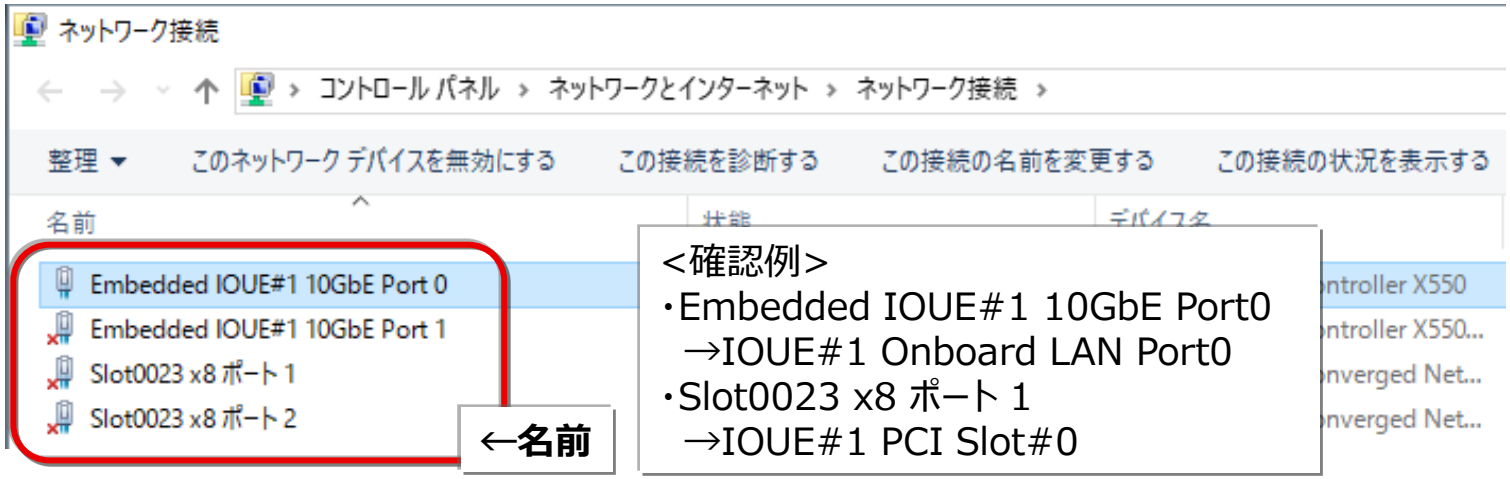
  SVOM画面で確認した物理アドレスとipconfig /allで表示した物理アドレスを比較し、名前を割り出す。Windowsのネットワーク画面での名前を比較して搭載位置とLANポートを特定する。

A.1 LANポートの接続先確認方法(2/4)

FUJITSU

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

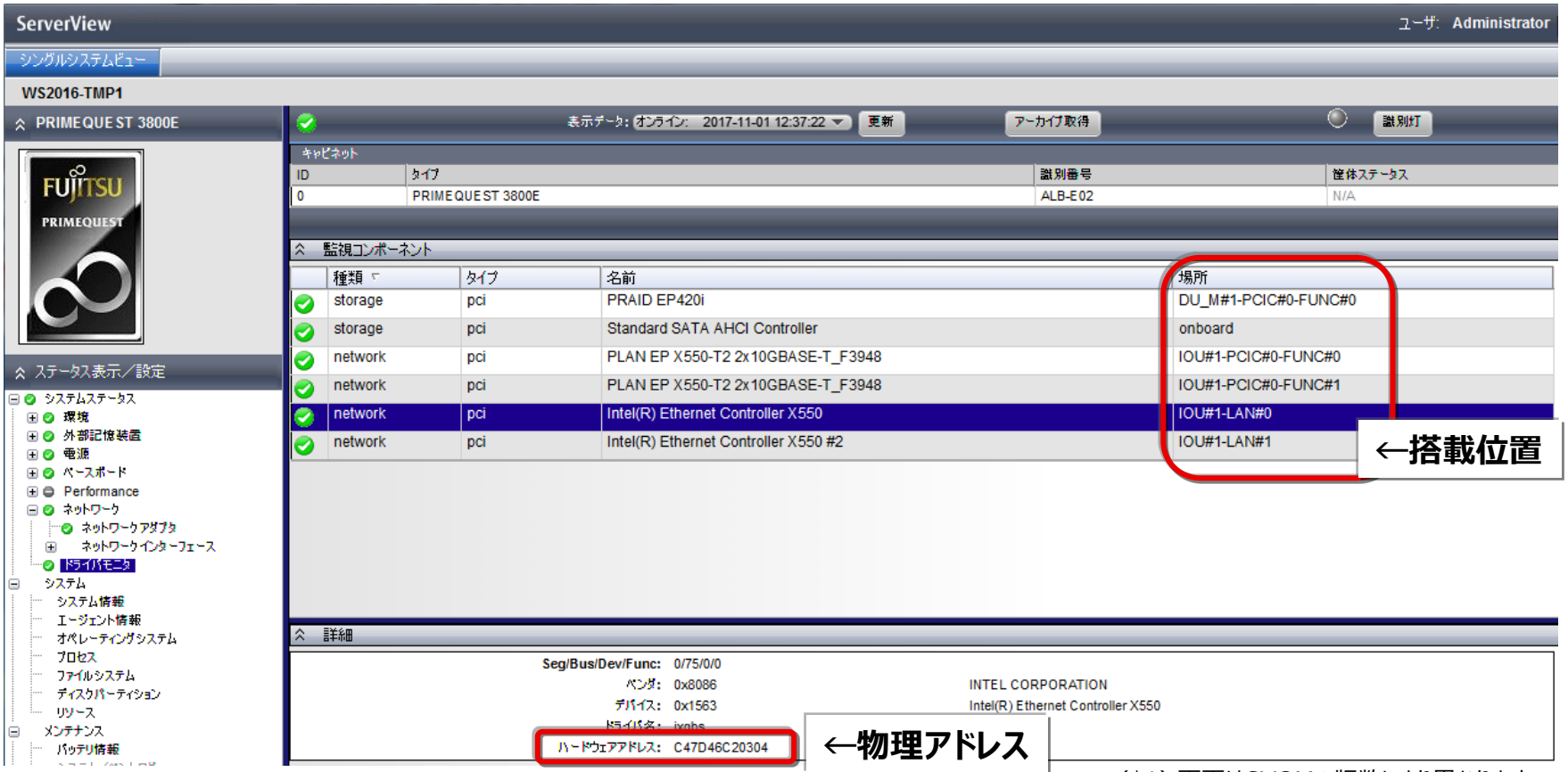


- スロット番号と実装位置の対応関係は、
  『運用管理マニュアル 付録B 物理実装位置、ポート番号』または
  『運用管理マニュアル 付録D I/Oの物理位置・BUS番号およびPCI Expressスロット実装位置・スロット番号』を参照して特定できる

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(*1)
   [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) 画面はSVOMの版数により異なります

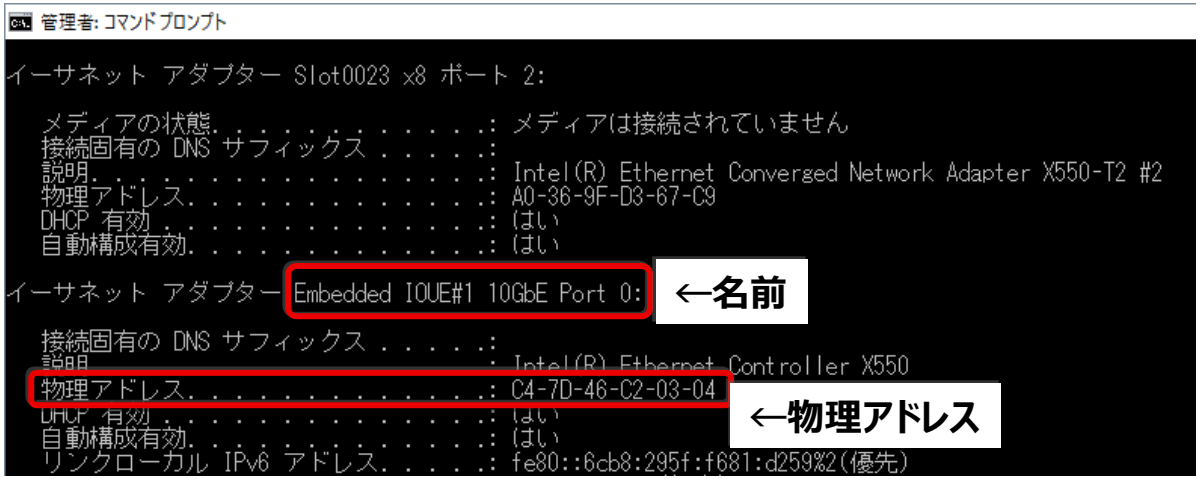
A.1 LANポートの接続先確認方法(4/4)

FUJITSU

b. SVOMおよびSV Agentsを利用し、次の3つを比較して確認する

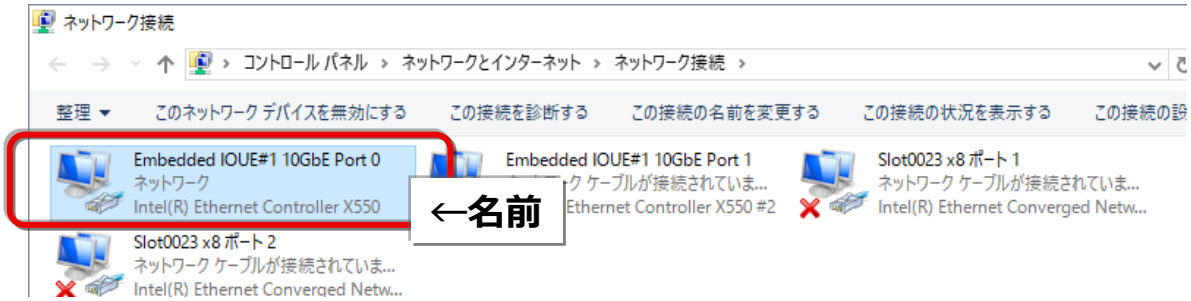
2. ipconfig /all画面

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 GL for Windows(PRIMEQUEST)について説明します。
なお、本製品および本付録の記載内容は、Windows Server 2019までを対象としています。
Windows Server 2022には対応していません。

B.1 PRIMECLUSTER GL for Windows (PRIMEQUEST)

- PRIMECLUSTER GL for Windows(PRIMEQUEST)の優位性(1/3)

○：適　×：不適

お客様要件		PRIMECLUSTER GL 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。

B.1 PRIMECLUSTER GL for Windows (PRIMEQUEST)

FUJITSU

- PRIMECLUSTER GL for Windows(PRIMEQUEST)の優位性(2/3)

○：適　×：不適

お客様要件		PRIMECLUSTER GL 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。

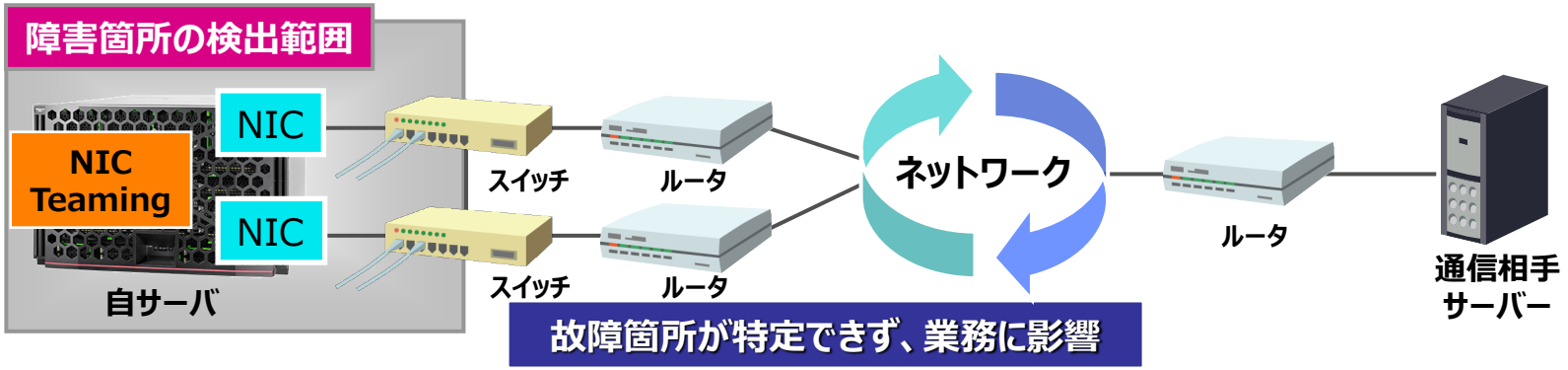
- PRIMECLUSTER GL for Windows(PRIMEQUEST)の優位性(3/3)

○：適　×：不適

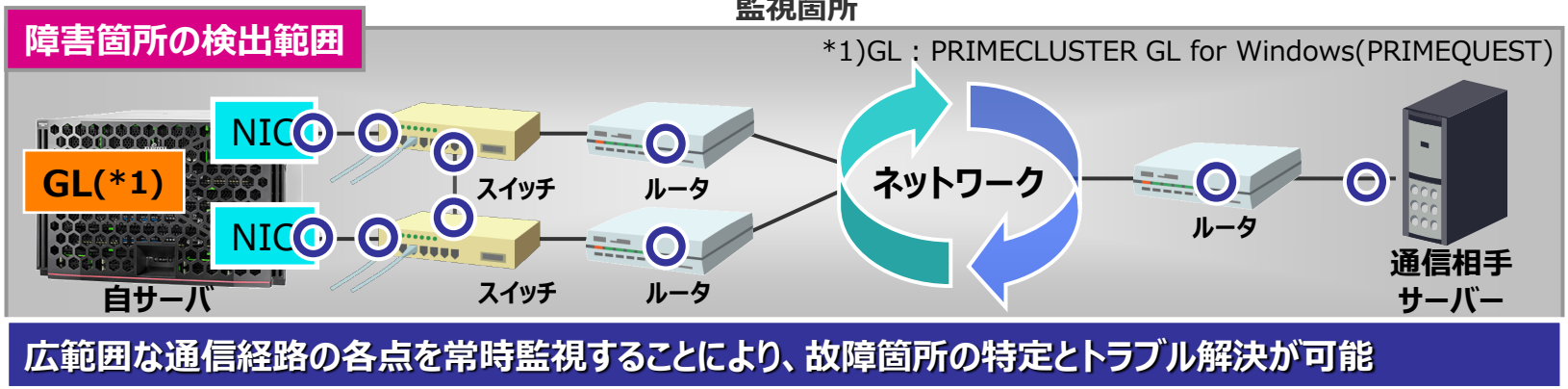
お客様要件		PRIMECLUSTER GL for Windows (PRIMEQUEST)	Intel PROSet	OSの NIC チーミング
マルチプラットフォームでの運用	運用・保守方法の統一	○	×	×
		Windows/Linux/Solarisで運用・保守方法が同じであり、設定や故障箇所の確認方法が統一可能。	Windows上でのみ運用可能。	Windows上でのみ運用可能。
	ネットワーク管理者の負担軽減	○	×	×
		Windows/Linux/Solarisで運用形態が統一しており、管理者の負担を軽減。	Windows上でのみ運用可能であるため、管理者は複数の運用スキ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



B.1.2 ネットワークの状態に応じたアプリケーション連携

FUJITSU

- 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
	ping監視でネットワーク機器の通信異常を検出した場合
通信相手システムの異常検出時	ping監視で通信相手システムの通信異常を検出した場合

B.1.3 マルチプラットフォームでの運用

FUJITSU

- 統一された障害検出タイミングと設定・確認方法

  PRIMECLUSTER GL 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 GL 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

B.1.4 PRIMECLUSTER GL for Windows(PRIMEQUEST)の設定(1/2)

- チーミングの設定

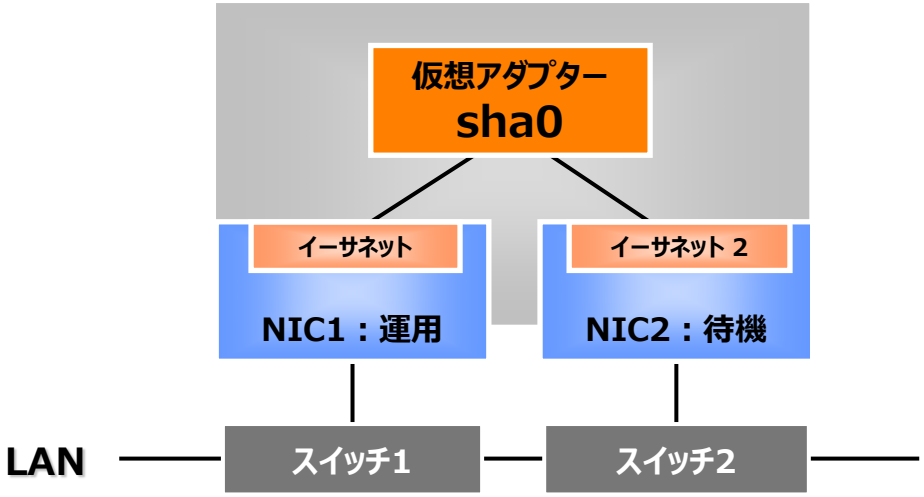
  hanetconfigコマンドを使用して、仮想アダプターを作成する

  （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 GL for Windows ユーザーズガイド』を参照



B.1.4 PRIMECLUSTER GL for Windows(PRIMEQUEST)の設定(2/2)

- 通信経路の監視設定
  - リンク状態監視

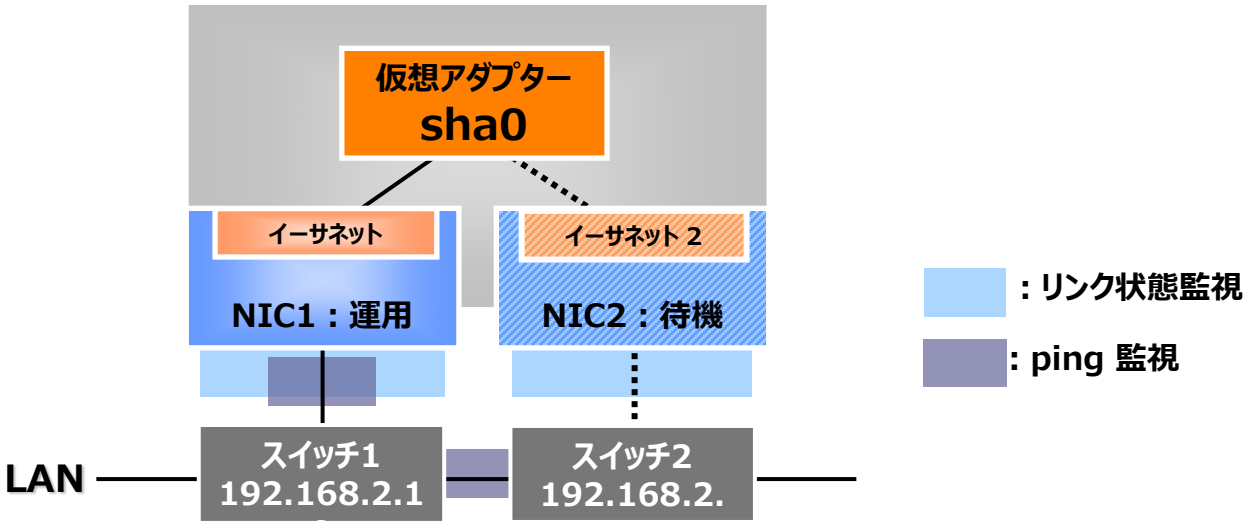
    設定は不要。自動的に監視を開始する
  - ping監視

    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 GL for Windows ユーザーズガイド』を参照



FUJITSU

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/iRMC+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/iRMC	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	×	○	○
	Partition Status	×	○	○
ミドルウェア	GL(*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)GL：PRIMECLUSTER GL for Windows(PRIMEQUEST)

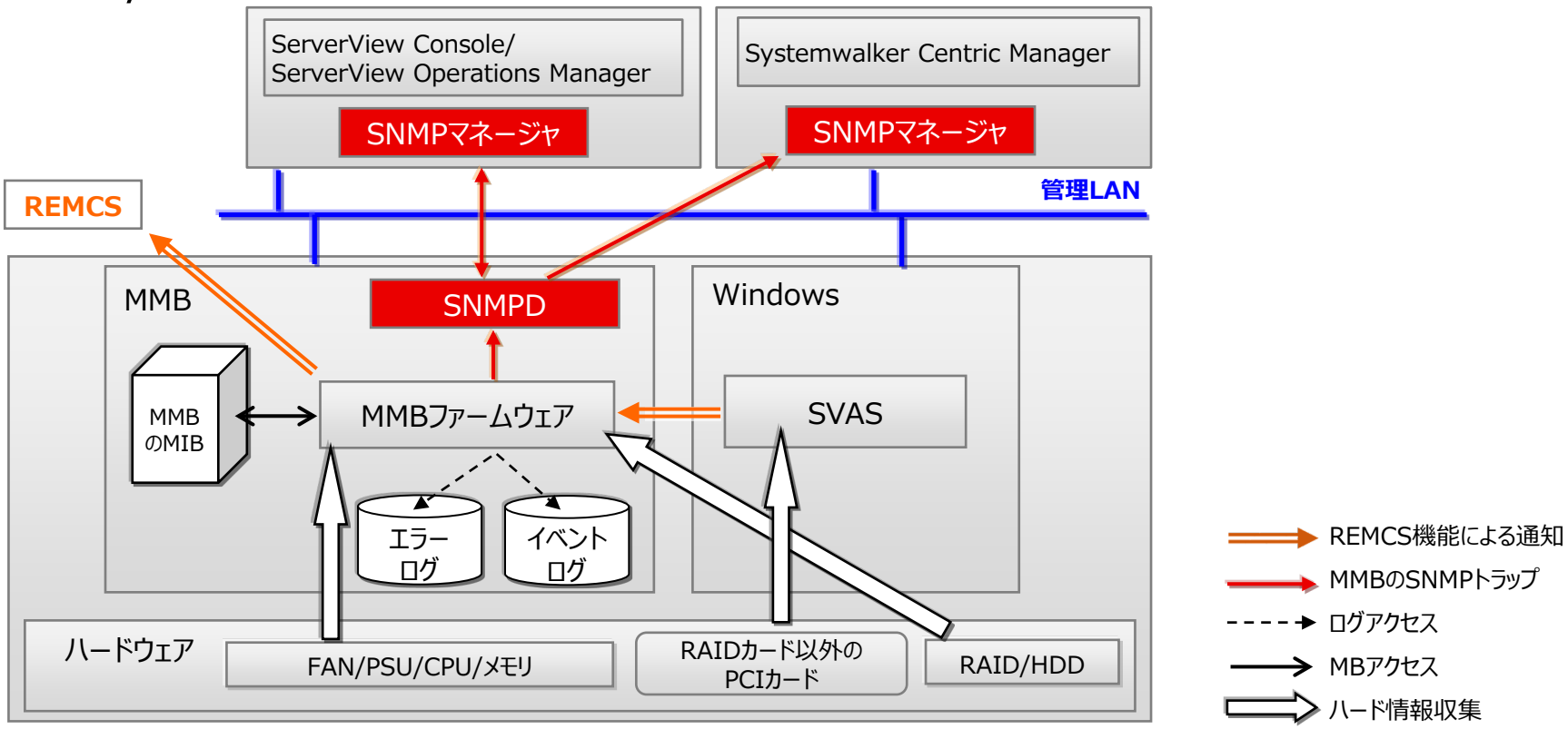
- 運用管理ソフトウェアと連携する場合はSNMPトラップ設定が必要

SVSの詳細はマニュアル
https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/catalog/#tab-d-07 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』

C.2 MMB/iRMC+SVASによるハードウェア監視(1/2)

FUJITSU

- MMB/iRMC+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

C.2 MMB/iRMC+SVASによるハードウェア監視(2/2)

FUJITSU

- 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。
• 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 • 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） • 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）	
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。

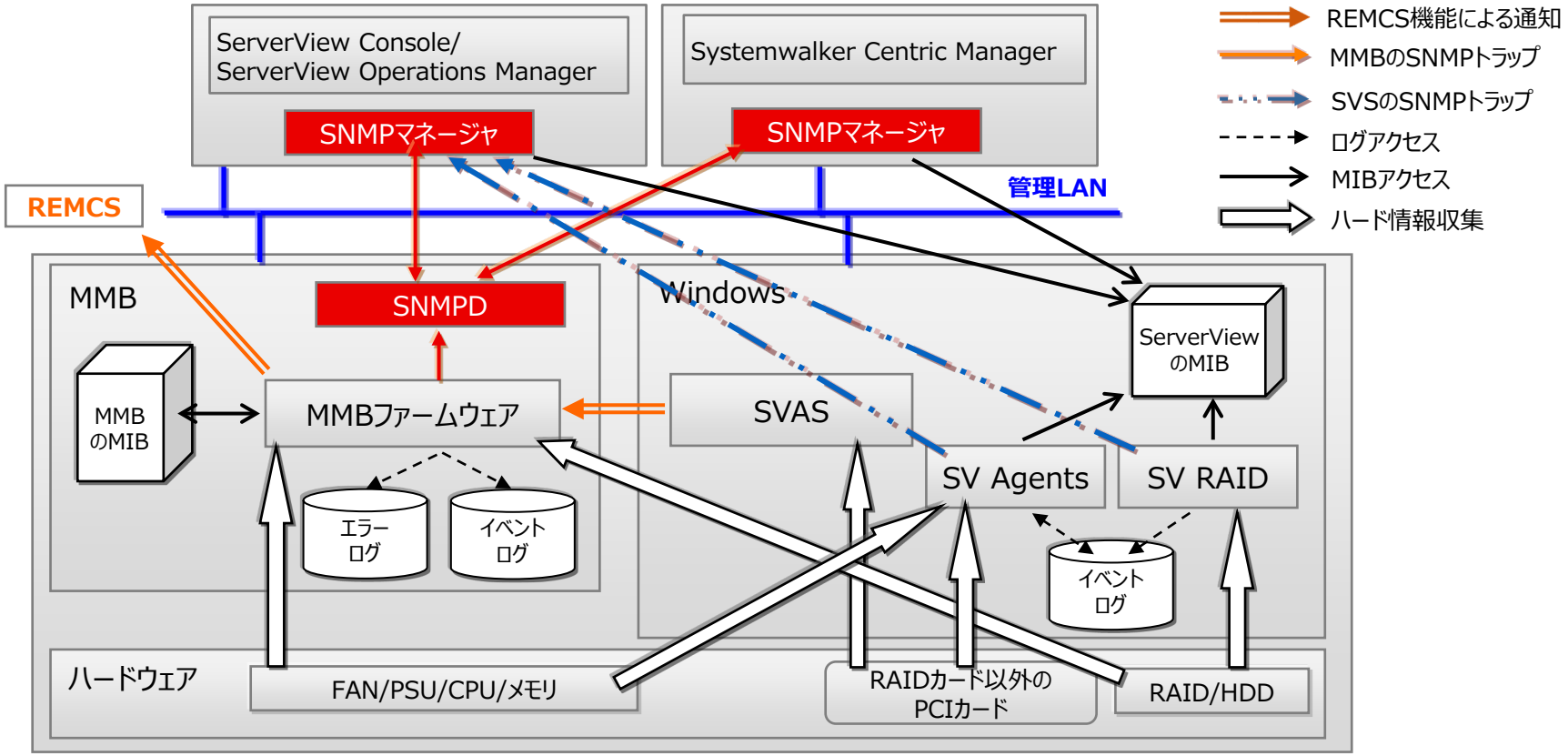
*1) SVSおよびSystemwalker Centric Managerを意味します。

Systemwalker Centric Managerの詳細は『Systemwalker Centric Manager 技術情報 https://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

C.3 SV Agents/SV RAIDによるハードウェア監視(1/2)

- 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

C.3 SV Agents/SV RAIDによるハードウェア監視(2/2)

- 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。

C.4 Windowsファイアウォールの設計

FUJITSU

- 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
    https://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/catalog/#tab-d-07
    『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
    https://www.fujitsu.com/jp/products/software/resources/technical/systemwalker/centricmgr/
    『Systemwalker Centric 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。

改版履歴

版数	日付	変更箇所	変更内容
01	2017-11-08	• 新規作成	–
02	2019-04-03	• 全体	• PRIMEQUEST 3400S2 Lite / 3400S2 / 3400E2 / 3400L2 / 3800E2 / 3800L2に対応 • WS2019情報の追加 • PRIMECLUSTER GL for Windows (PRIMEQUEST)の名称変更に対応
03	2023-02-28	• 全体	• WS2022情報の追加 • Intel PROSet / OSのNICチーミング機能を利用する場合のSTP無効化の制限解除

使用条件

■ 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、「PRIMEQUESTのお問い合わせ」
(https://www.fujitsu.com/jp/products/computing/servers/primequest/contact/)
よりお尋ねください。

CA92344-2153-03
2023.2

FUJITSU