P3AM-1862-36Z0

Brocade series, ETERNUS SN200 series
ユーザーズガイド 導入／運用（基本）編

このページは空白です。

はじめに

本システム構築手順書は、Brocade series, ETERNUS SN200 series を使用したシステム構築を行う際に、事前にお客様に行っていただきたい確認事項およびシステム構築時の各種設定方法について説明しています。

第 36 版
2024 年 4 月

安全にお使いいただくために

■ このマニュアルの取り扱いについて

このマニュアルには当製品を安全に使用していただくための重要な情報が記載されています。当製品を使用する前に、このマニュアルを熟読してください。特にこのマニュアルに記載されている「安全上の注意事項」をよく読み、理解した上で当製品を使用してください。また、このマニュアルは大切に保管してください。
富士通は、使用者および周囲の方の身体や財産に被害を及ぼすことなく安全に使っていただくために細心の注意を払っています。当製品を使用する際は、マニュアルの説明に従ってください。

本製品について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう設計・製造されたものではございません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途に使用される場合は、弊社の担当営業までご相談ください。

電波障害の防止について

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

コマンド名の表記について

コマンド名は読みやすくするために大文字と小文字で表記しています（例：switchShow）。
実際に入力するときは、ほとんどの場合すべて小文字で入力します。大文字小文字を区別して入力しなければならない場合は、区別して入力するよう注記しています。

商標について

- Brocade、B-wing シンボル、BigIron、DCX、Fabric OS、FastIron、IronView、NetIron、SAN Health, ServerIron、および TurboIron は、登録商標であり、Brocade Assurance,DCFM、Extraordinary Networks、および Brocade NET Health は、米国またはその他の国における Brocade Communications Systems Inc. の商標です。
- Windows 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。
- その他一般に、会社名、製品名、サービス名は、各社の商標または登録商標です。

Microsoft Corporation のガイドラインに従って画面写真を使用しています。

本書の読み方

本書の内容と構成

本書は、以下の構成になっています。

- 第 1 章　概要

  本書の目的、スイッチの接続対象、推奨構成について説明しています。

- 第 2 章　事前準備／セットアップ手順

  システム構築のために必要とされるスイッチの各種設定情報とセットアップ手順について説明しています。

- 第 3 章　スイッチの初期設定

  「図 2.1　システム構成図（例）」、「表 2.1　スイッチの設定パラメーター（例）」を参考に、スイッチを初期設定する手順について説明しています。

- 第 4 章　Zone 設定のセットアップ

  「図 2.1　システム構成図（例）」、「表 2.1　スイッチの設定パラメーター（例）」を参考に、ファブリックに Zone を設定する手順について説明しています。

付録として、以下を記載しています。

- 付録 A　装置パスワードの確認／変更
- 付録 B　管理 LAN ポート設定の確認／変更
- 付録 C　時刻設定の確認／変更
- 付録 D　ポート設定の確認／変更
- 付録 E　ポートの Offline / Online
- 付録 F　SNMP 設定
- 付録 G　追加ライセンスの発行／適用
- 付録 H　Virtual Fabrics 設定
- 付録 I　エクステンション設定
- 付録 J　FCoE 設定
- 付録 K　Zone 方式と設定変更
- 付録 L　設定情報の退避／復元
- 付録 M　ファームウェアの確認／適用
- 付録 N　装置ログ採取
- 付録 O　ダイレクタタイプのポートインデックス一覧
- 付録 P　リモート通報機能の設定／確認
- 付録 Q　アカウントの無効化

- 付録 R　Web Tools
- 付録 S　Secure Mode
- 付録 T　SFP 間欠故障監視

また用語集では、本書内で使用される用語の定義について説明しています。

関連マニュアル

本書の関連マニュアルとして以下のマニュアルが用意されています。

取扱説明書関連

- 『ETERNUS SN200 モデル 140, 600 ファイバチャネルスイッチ 取扱説明書』(P3AM-2242)
- 『Brocade 7800 取扱説明書』(P3AM-3982)
- 『Brocade 6505 ユーザーズガイド 設置編』(P3AM-6202)
- 『Brocade 6510 ユーザーズガイド 設置編』(P3AM-5442)
- 『Brocade 6520 ユーザーズガイド 設置編』(P3AM-7192)
- 『Brocade DCX 8510-8 ユーザーズガイド 設置編』(P3AM-5452)
- 『Brocade DCX 8510-4 ユーザーズガイド 設置編』(P3AM-5462)
- 『Brocade 7810 エクステンションスイッチ ユーザーズガイド 設置編』(P3AG-3882)
- 『Brocade 7840 エクステンションスイッチ ユーザーズガイド 設置編』(P3AG-1172)
- 『Brocade G610 ユーザーズガイド 設置編』(P3AG-2192)
- 『Brocade G620 ユーザーズガイド 設置編』(P3AG-1792)
- 『Brocade G630 ユーザーズガイド 設置編』(P3AG-3092)
- 『Brocade G730 ユーザーズガイド 設置編』(P3AG-6572)
- 『Brocade X6-4 ユーザーズガイド 設置編』(P3AG-1982)
- 『Brocade X6-8 ユーザーズガイド 設置編』(P3AG-1992)
- 『Brocade G720 ユーザーズガイド 設置編』(P3AG-5452)
- 『Brocade X7-4 ユーザーズガイド 設置編』(P3AG-5462)
- 『Brocade X7-8 ユーザーズガイド 設置編』(P3AG-5472)

システム構築関連

- 『Brocade series, ETERNUS SN200 series ユーザーズガイド 導入／運用（拡張）編』(P3AM-1852)

Fabric OS 関連

- Brocade Fabric OS 製品マニュアル 一式 （英語版）
  以下の URL からダウンロードできます。

  https://www.fujitsu.com/jp/products/computing/storage/manual/

■ REMCS 関連

- 『ファイバチャネルスイッチ リモートサポート監視エージェント インストールガイド Windows 用』（P3AM-2472）
- 『ファイバチャネルスイッチ リモートサポート監視エージェント インストールガイド Solaris Operating System, Linux 用』（P3AM-1272）

本書の規約

ここでは、テキスト書式の規約、本書で使われているマークについて説明しています。

テキスト書式

以下の表は、本書で使われている書式の規約について説明しています。

書式	目的
bold text	• コマンド名を識別します。 • GUI エレメントを識別します。 • キーワード／オペランドを識別します。 • GUI または CLI への入力テキストを識別します。
italic text	• 強調するのに用います。 • 変数を識別します。 • パス、またはインターネットアドレスを識別します。
`code` text	• CLI 出力を識別します。 • 構文例を識別します。

マーク

本書では以下のマークを使用しています。

注 意 お使いになるときに注意していただきたいことを記述しています。注意が守られない場合、当製品や利用者のデータ破壊などの損害が起こる危険性があります。必ずお読みください。

備 考 操作や設定を行ううえで、知っておくと便利な機能や使い方などが書いてあります。

安全上の注意事項

本マニュアル中に記載している重要な警告事項は以下のとおりです。

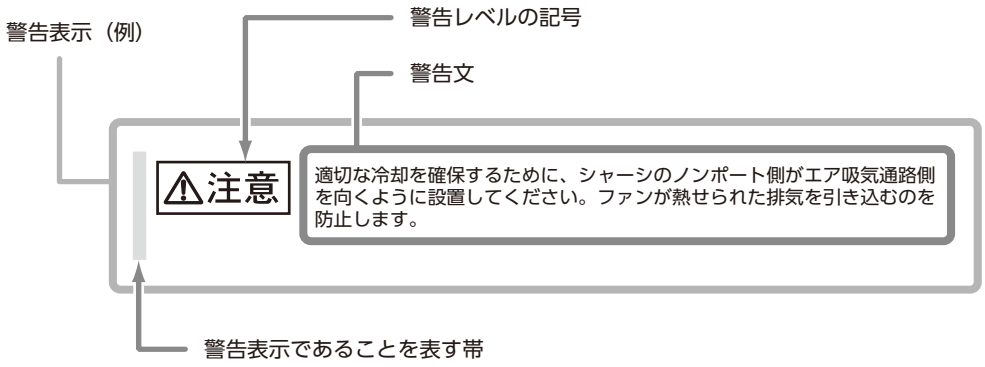
警告表示について

このマニュアルでは、使用者や周囲の方の身体や財産に損害を与えないために以下の警告表示をしています。

⚠注意	この記号は、正しく使用しない場合、軽傷、または中程度の傷害を負うことがあり得ることと、本装置自身またはその他の使用者などの財産に、損害が生じる危険性があることを示しています。
重　要	この記号は、お使いになる際の重要な注意点が書いてあります。

本文中の警告表示の仕方

警告レベルの記号の横に警告文が続きます。警告文は、通常の記述と区別するため、行の左側に帯を記述しています。表示例を以下に示します。



重要な警告事項の一覧

本マニュアル中に記載している重要な警告事項は以下のとおりです。

■ 作業区分：「3.4 ドメイン ID の設定」、「付録 H.5 論理スイッチのドメイン ID 設定（setcontext / configure）」

⚠注意

- スイッチ同士をカスケード接続する場合は、異なるドメイン ID を各スイッチに割り当ててください。また現時点でカスケードしない場合でも、将来のカスケード接続に備えて互いに異なる ID に設定しておくことを推奨します。
  同じドメイン ID のスイッチ同士をカスケード接続した場合、お客様が意図しないドメイン ID に自動的に変更されたり、設定情報の相互同期がとれなくなったりするなどの不具合が生じ、最悪の場合データが失われます。
- HP-UX 接続環境でスイッチを使用する場合は、ドメイン ID に「8」を使用しないでください。ドメイン ID を「8」に設定すると、デバイスが正常に認識できません（HP-UX 以外の OS では問題ありません）。

■ 作業区分：「第 4 章 Zone 設定のセットアップ」、「付録 K.2 Zone 設定の確認／変更」

⚠注意

- ファブリック内に異なるファームウェア版数のスイッチが併存する場合、最も新しいファームウェアを適用したスイッチから Zoning 設定を行ってください。
- Zone 設定の追加／削除を I/O アクセス中のデバイスへ行うと、I/O に影響があります。I/O アクセスを停止した状態で実施してください。
- WWN Zoning の場合、メンバーの指定方法として WWPN（World Wide Port Name）と WWNN（World Wide Node Name）の 2 種類がありますが、WWNN は使用しないでください。WWNN では同じアドレスに複数のポートが存在可能なため、Zoning が一意な組み合わせとならない場合があります。

改版履歴表

版数	日付	変更箇所（変更種別）（注）	変更内容
初版	2001 年 6 月	-	-
02	2002 年 2 月	全体（修正）	• SN200 モデル 240 新規追加 • SN200 モデル 10/30 のカスケード接続制限の解除 • その他誤記訂正など
03	2002 年 7 月	全体（追加）	SN200 モデル 210, 320 新規追加
		3.3.3（追加）	異なるファーム版数のカスケード接続に関する注意事項を追加
04	2004 年 7 月	全体（追加）	• SN200 モデル 220, 230, 340 新規追加 • SN200 モデル 280 新規追加 - 接続する HBA として “PW008FC2” を追加 - 誤記修正 • “ 関連マニュアル ” - 参考文書を追加 • “1.3 留意事項 ” の内容追加 - Zoning 関連 - カスケード接続関連 - 設定の退避／復元 • “2.3 SN200 の基本設定値 ” - HP-UX 接続環境での注意事項を追加 - その他の設定を追加 • “2.4 SN200 のゾーン構成 ” - 設定例の内容変更 • “3.6 Zoning セットアップ ” - 設定例の内容変更 • “3.6.5 設定情報の退避 ” を追加
05	2007 年 5 月	全体（修正）	マニュアルコードを変更
		全体（追加）	SN200 モデル 120, 430, 485, 490, 540 新規追加
		関連マニュアル（修正）	関連文書を変更
		1.3（追加）	注意事項を追加
06	2007 年 12 月	全体（修正）	QuickLoop 接続に関する記載を削除
		1.3.3（追加）	“Zoning 設定時の注意 ” を追加
		1.3.4（追加）	“ カスケード接続時の注意事項 ” を追加
		1.3.4 (4)（追加）	“ ポートスピード設定 ” を追加
		1.4（追加）	“FC ルーティング機能 ” の注意事項を追加

(2/5)

版数	日付	変更箇所（変更種別）（注）	変更内容
07	2008 年 8 月	全体（追加）	SN200 のモデル追加（140, 600, 630, 660）
		全体（修正）	コマンド実行結果を更新
		1.1（追加）	“ 冗長パス間のカスケード接続時の注意事項 ” の e 項の SN200 リング構成についての注意事項を修正
		2.3.4（追加）	“SFP タイプの決定 ” に 8G モデル用 SFP に関する注意事項を追加
		3.3.2.6（追加）	• “ その他の設定 ” を追加 • 「NTP サーバの設定（tsclockserver, tstimezone）」を追加
		3.6（修正）	SN200 の Zoning セットアップ「重要」の記載内容を修正
08	2008 年 9 月	関連マニュアル（修正）	SN200 関連マニュアルの更新
09	2009 年 4 月	全体（追加）	Zoning 設定を最新のファーム版数を適用した SN200 から実施するよう注意事項を追加
10	2009 年 9 月	全体（修正）	Brocade DCX-4S, DCX のモデル名の追記
		2.3.6、3.3.1（修正）	ファイバチャネルスイッチ 設定表（記入例）の Firm 版数の修正
		3.3.2.4（修正）	**ipaddrset** コマンド（実行例）の修正
		3.3.2.5（修正）	• **passwd** コマンドは、パスワードのみの修正 • 図 3.11 **passwd** コマンド（実行例）の修正
		3.6（新規追加）	Virtual Fabrics のセットアップの追加
11	2010 年 1 月	2.3.4（修正）	Brocade 7800 の追加
		3.3.2.4（修正）	
		2.5、3.7（追加）	FC ルーティング、FCIP トンネリングの設計、設定に関する記事を追加
12	2010 年 4 月	全体（修正）	Brocade 8000 の追加
		2.3.5（修正）	ポートタイプの決定「備考」を削除
		2.5.2（新規追加）	FCoE の追加
		3.7.2（新規追加）	FCoE のセットアップの追加
		3.8.5（追加）	**configUpload** コマンドに関する記事を追加
13	2011 年 1 月	2.3.4（追加）	“SFP タイプの決定 ” に mSFP に関する記載を追加
		3.3.2.6（追加）	“SNMP 設定 ” に SNMP のテスト trap の送信手順追加
		3.3.2.7（新規）	“ ポートの有効化 ” の記載を追加
14	2011 年 7 月	全体	全面改版（構成変更／記事見直し）

(3/5)

版数	日付	変更箇所（変更種別）(注)	変更内容
15	2012 年 1 月	全体	• Brocade 6505 の記述を追加 • FOS v7.0.1 の記述を追加
16	2012 年 8 月	全体	• 誤記修正 • Zoning に関する記述の修正
17	2013 年 2 月	関連マニュアル（追加）	関連文書を追加
		1.2（追加）	Brocade 6520 の記述を追加
18	2014 年 11 月	関連マニュアル（追加）	FOS v7.3.0 対応
		3.3（修正）	
		付録 M（修正）	
19	2015 年 10 月	マニュアルタイトル変更	本書のマニュアルタイトルを変更
		全体	• Brocade 7840 の記述を追加 • Brocade Network Advisor の記述を追加
		関連マニュアル（追加）	関連文書を追加
		A.1（追加）	" デフォルトパスワードの確認 " に「注意」を追加
		D.2（追加）	" ポート速度の変更（portcfgspeed）" に「注意」を追加
		H.6（新規追加）	" 論理スイッチの状態の確認（switchshow）" を追加
		I.1（追加）	タイトル、本文に IP エクステンショントンネリングの記述を追加
		L.2（追加）	" 設定情報の復元（configdownload）" に「注意」を追加
		付録 P（新規追加）	" リモート通報機能の設定／確認 " を追加
20	2016 年 9 月	全体	• Brocade G620 の記述を追加 • FOS v8.0.1a 対応
		D.2（修正）	注意事項を修正
		D.3 （修正）	portcfggport の実行例を修正
		F.1、F.2（追加）	snmpconfig の実行例を追加
21	2017 年 1 月	全体	Brocade X6 の記述を追加
		B.2（修正）	注意事項を修正
		D.1（修正）	switchshow の実行例を修正
		D.2（修正）	32Gbit/s の情報を追加
		L.2（追加）	注釈を追加
		付録 O（追加）	Brocade X6 ポートインデックス一覧を追加

(4/5)

版数	日付	変更箇所（変更種別）（注）	変更内容
22	2017 年 4 月	全体	Brocade G610 の記述を追加
		D.1（追加）	• " 事前確認（portcfgshow）" に注釈を追加 • " 事前確認（switchshow）" にポート状態を 1 項目追加
		F.2（追加）	FOS v8.1.x 以降の表示例を追加
		G.2（修正）	ライセンス発行手順の不要部分を削除
		G.4（新規追加）	"Dynamic POD（DPOD）ライセンスの開放（licenseport --release）" を追加
23	2017 年 7 月	関連マニュアル（修正）	関連文書を更新
		3.6（追加）	" ポリシーパラメーターの変更 " に「注意」を追加
		F.2（追加）	"SNMP の設定／確認（snmpconfig）" に「注意」を追加
		G.4（修正）	ポートのライセンス開放手順を修正
		L.2（追加）	" 設定情報の復元（configdownload）" に「注意」を追加
24	2017 年 10 月	付録 Q（新規追加）	" アカウントの無効化 " を追加
25	2018 年 5 月	全体	Brocade G630 の記述を追加
26	2018 年 7 月	L.2（追加）	" 設定情報の復元（configdownload）" に「注意」を追加
27	2018 年 12 月	関連マニュアル（修正）	Fabric OS 関連の記載を変更
28	2019 年 4 月	全体	Brocade 7810 の記述を追加
		G.2（修正）	ライセンス発行手順を削除
		L.1（修正）	" 設定情報の退避 " の Virtual Fabric 構成例を更新
		L.2（修正）	" 設定情報の復元 " の Virtual Fabric 構成例を更新
29	2019 年 10 月	2.1（追加）	管理者 (admin) パスワードに説明を追加
		2.2（修正）	作業フローの担当者を変更
		3.1（修正）	操作手順の「備考」を変更
		A.1（追加）	デフォルトパスワードに説明を追加
30	2020 年 10 月	全体	以下の新機種の記述を追加 • Brocade G720 • Brocade G620（switch type183） • Brocade G630（switch type184） • Brocade X7-4、X7-8
			Fabric OS9.0.0 以降対応のコマンドの仕様変更を追加
31	2021 年 4 月	付録 O（修正）	Brocade X7-4、X7-8 のポートインデックスを変更

(5/5)

版数	日付	変更箇所（変更種別）（注）	変更内容
32	2022 年 8 月	関連マニュアル（修正）	関連文書を更新
		1.2（修正）	モデルの追加と削除
		全体	Fabric OS のバージョンによる記述を追加
33	2023 年 1 月	1.2（追加）	冒頭の参照先、表 1.1 の switch type の追加、および表の備考を削除
34	2023 年 4 月	2.1（追加）	装置 ID 確認方法を追加
		第 4 章（追加）	TI ゾーンに関する注意事項を追加
		付録 C（追加）	タイムゾーン設定に関する注意事項を追加
		C.2（追加）	日付設定に関する注意事項を追加
		D.2、D.4（追加）	ボックスタイプの場合の指定方法を追加
		D.3（追加）	実行可能版数の情報を追加
		E.1、E.2（追加）	ボックスタイプの場合の指定方法を追加
		付録 R（追加）	Web Tools の項を追加
		付録 S（追加）	Secure Mode の項を追加
		付録 T（追加）	SFP 間欠故障監視の項を追加
		全体（追加）	Secure Mode の設定に関する注意事項を追加
35	2023 年 10 月	付録 P（追加）	センターとの接続確認に関する説明を追加
		付録 S（修正）	HTTP 無効コマンドのパラメーターを変更
36	2024 年 4 月	付録 S（修正、追加）	Telnet および HTTP の設定手順を変更 Secure syslog の設定手順を追加
		全体	FOS v9.2.0b の記述を追加

注） 変更箇所は最新版の項番を示しています。ただし、アスタリスク（*）の付いている項番は旧版の項番を示します。

目次

図目次

表目次

第1章

概要

本書は、お客様が要求されているサーバ／ストレージに対して、実際のシステム構築の際に必要となる情報の確認および各装置の設定方法・手順について説明しています。

1.1 サポートサーバ／ストレージ

以下の URL に記載されたサーバ／ストレージのファブリック接続をサポートします。

https://www.fujitsu.com/jp/products/computing/storage/switches/fc-switches/

1.2 サポートスイッチ

表 1.1 に、サポートするスイッチを示します。
相互接続する場合の詳細については、『Fabric OS ファームウェア版数組み合わせ表』の「カスケード時の推奨版数」シートを参照してください。

備 考

カスケード接続する際は、各スイッチに最新の FOS（Fabric OS）を適用することを推奨します。

表 1.1　サポートスイッチ

モデル
SN200 モデル 140, 600, Brocade 300
Brocade 6505, 6510, 6520
Brocade DCX 8510-8, 8510-4
Brocade G610（switch type170.0 ～ 170.3, 170.5）
Brocade G620（switch type162, 183, 183.5）
Brocade G630（switch type173, 184）
Brocade X6-4, X6-8
Brocade G720（switch type181, 181.5）
Brocade G730
Brocade X7-4, X7-8
Brocade 7800, 7810, 7840

1.3　サポート SFP

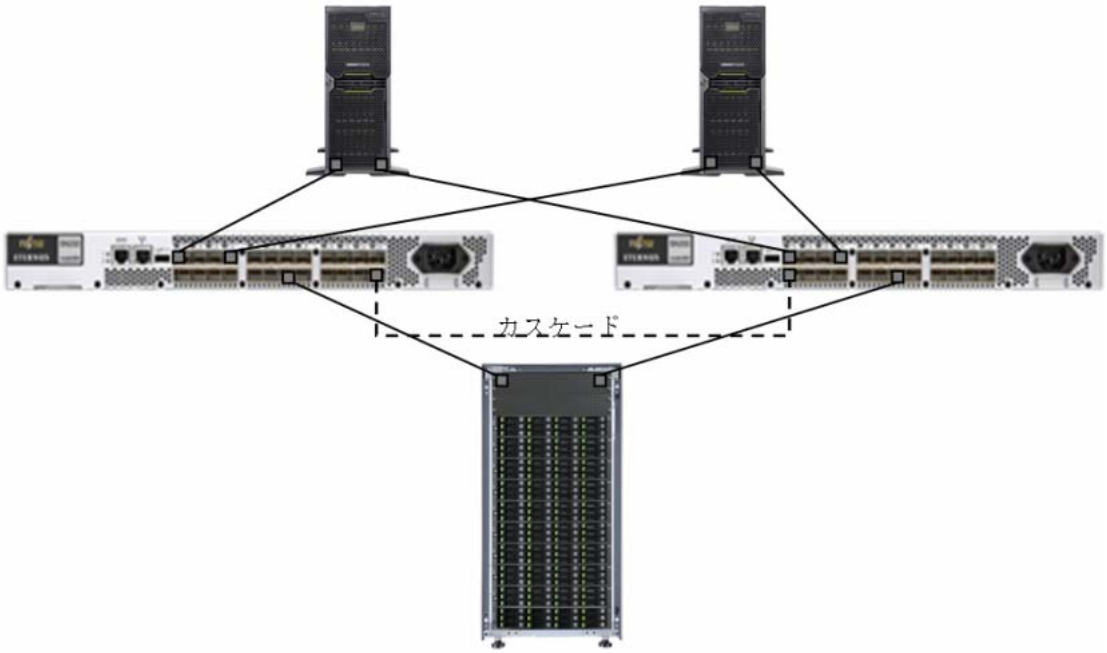
装置に搭載可能な SFP は、各装置の『ユーザーズガイド 設置編』または取扱説明書を確認してください。

備 考

SWL SFP と LWL SFP の組み合わせのように、波長の違う SFP 間を FC ケーブルで接続してもリンクは確立できません。

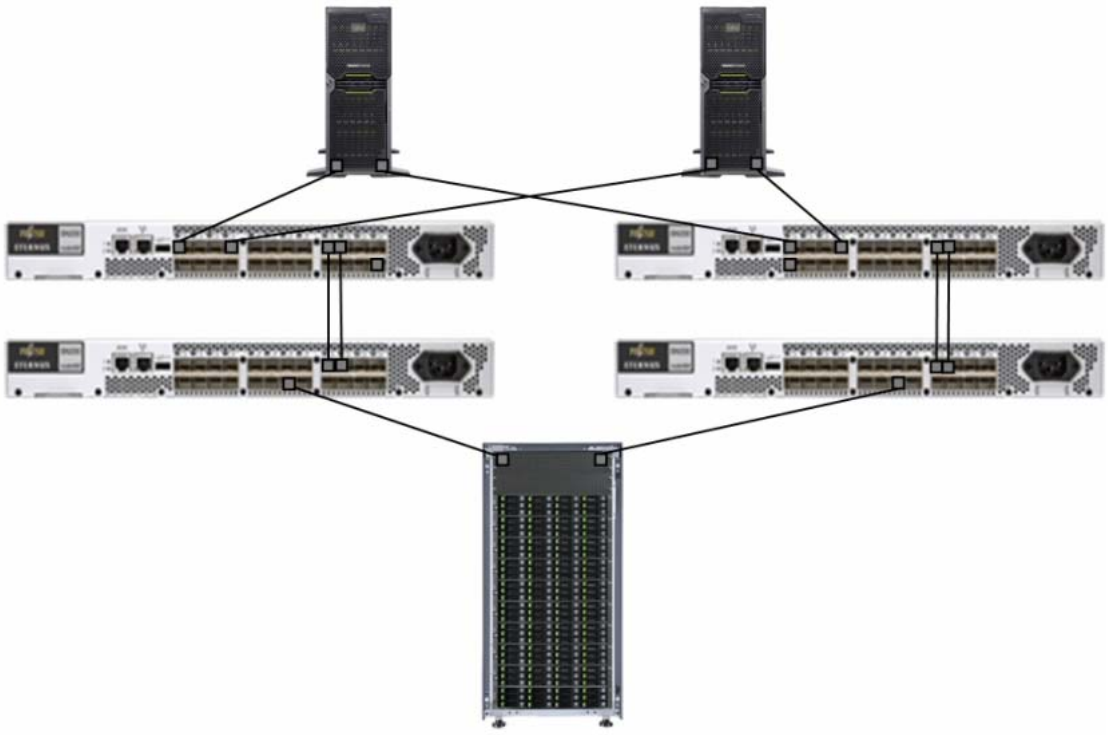
1.4　推奨構成

2 台以上のスイッチを用意し、マルチパスで構成された 2 つのホストバスアダプター（HBA）からそれぞれ異なるスイッチに接続することで、スイッチの本体故障やパス故障時のアクセス停止を回避し、システムの信頼性が向上します。



備 考

冗長構成のスイッチ間でカスケード（破線）を行う場合は、Zone 設定の共有のみを目的とし、常時接続しなくてもデータアクセスに影響がない Zone 構成としてください（FC ケーブルの接続先を間違えると、意図しない経路でデータアクセスが行われる場合があるため、ケーブルの接続確認を必ず行ってください）。



備 考

サーバ／ストレージ間のパス経路が、スイッチを 8 台以上経由するシステム構成はサポートされません。データ経路が 7 段を超えないよう考慮してシステム設計を行ってください。

1.5　設定情報の退避／復元

スイッチの Zone や各種パラメーターの設定／変更前後は **configupload** コマンドを使用して、必ず設定情報ファイルを保存してください。スイッチの本体交換時に、**configdownload** コマンドを使用して、同じ設定情報を適用できます。
詳細は、「付録 L 設定情報の退避／復元」(P.103) を確認してください。

1.6　SAN 管理ソフトウェアのご使用について（推奨）

ETERNUS SF Storage Cruiser

ETERNUS の統合管理ソフトウェアである ETERNUS SF Storage Cruiser を導入すると、GUI を使用したわかりやすいインターフェースで実現しているため、複雑なストレージネットワークの構成設計および設定操作を、高度なスキルを必要とすることなく簡単に導入できます。
また、導入後もスイッチだけではなくサーバ／ストレージ環境を一元管理することでストレージシステムの安定稼働を支えます。SAN 管理ソフトウェアの詳細は、以下の URL を確認してください。

https://www.fujitsu.com/jp/products/computing/storage/software/sf-sc/

備 考

スイッチのファームウェア版数に応じて、SAN 管理ソフトウェアにパッチを適用する必要があります。ただし、Brocade 7810 は管理対象外です。

第 2 章

事前準備／セットアップ手順

2.1　システム構成図／設定パラメーターの作成

以下のようなシステム構成図／設定パラメーターを事前に設計してください。

図 2.1　システム構成図（例）

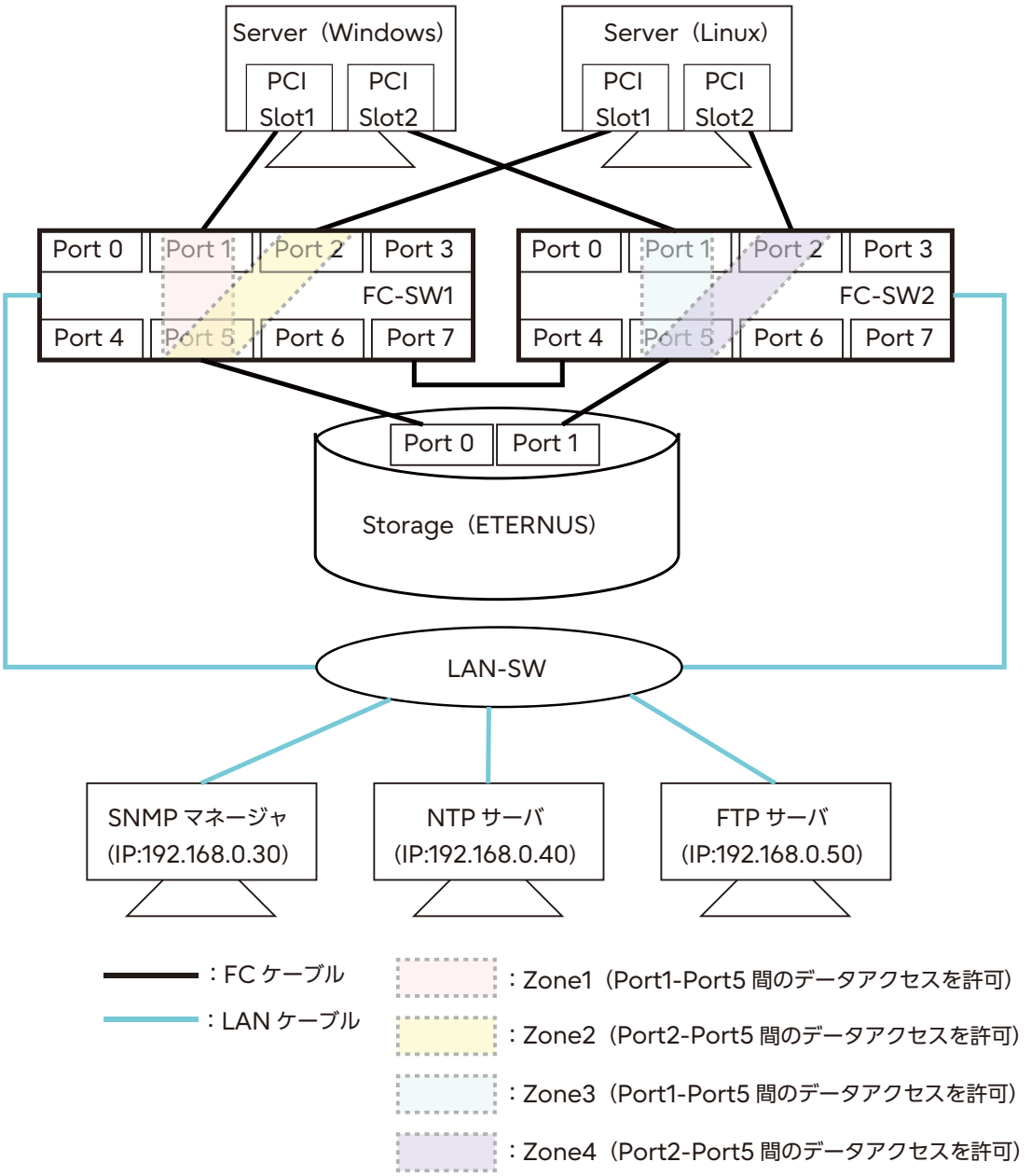
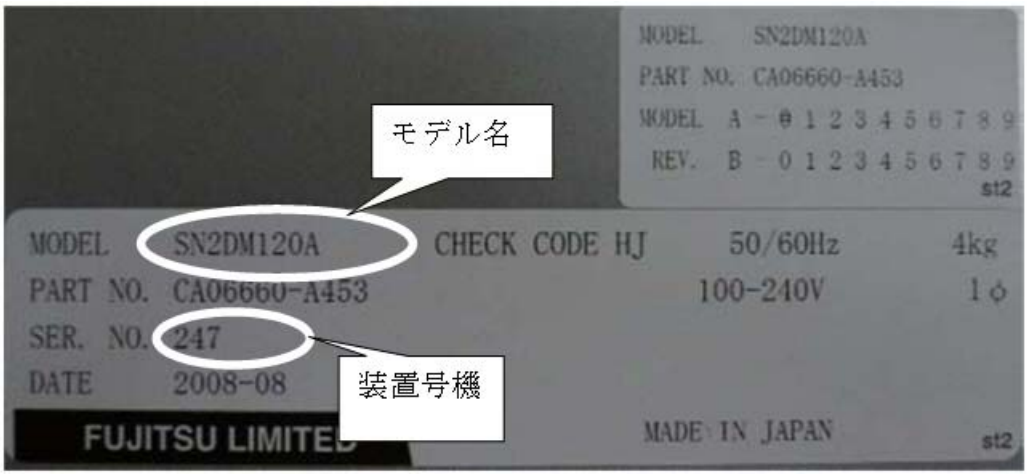


表 2.1　スイッチの設定パラメーター（例）

項目	FC-SW1	FC-SW2	初期値
スイッチ名	switch_1	switch_2	switch
ドメイン ID	10	20	1
管理 LAN:IP アドレス	192.168.0.10	192.168.0.20	192.168.30.70
管理 LAN: サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
管理 LAN: ゲートウェイアドレス	192.168.0.1	192.168.0.1	0.0.0.0
管理 LAN: 通信モード	AutoNego	AutoNego	AutoNego
SNMP:Community 名	public	public	public
SNMP: トラップ送信先 IP アドレス	192.168.0.30	192.168.0.30	0.0.0.0
SNMP: トラップ重大度レベル	3(warning)	3(warning)	0(none)
NTP サーバ IP アドレス	192.168.0.40	192.168.0.40	LOCL
タイムゾーン	JST(Asia/Tokyo)	JST(Asia/Tokyo)	UTC
管理者 (admin) パスワード（*1）	password	password	password
モデル名（*2）			
装置号機（*2）			
装置 ID NO（*3）			
装置 WWN（*4）			
ファームウェア版数	v7.3.0c	v7.3.0c	

*1:　パスワードは工場出荷時のものです。パスワードを変更した場合には、変更後のパスワードを入力してください。FOS v8.2.x 以降は必ず任意のパスワードに変更してください。

*2:　モデル名と装置号機は、装置本体の上面に貼られている製造銘板に記載されています。



*3:　装置 ID No.（シリアルナンバー）は、装置本体の底面に取り付けられたタグ、または引出式プレートのバーコードの下側にある 11 桁の文字列となります。

注 意

装置が起動している場合は、シリアルナンバーは chassisshow コマンドで確認することが可能です。コマンドの実施手順については、「G.1 事前確認（licenseshow, license --show / chassisshow）」(P.79) を参照してください。

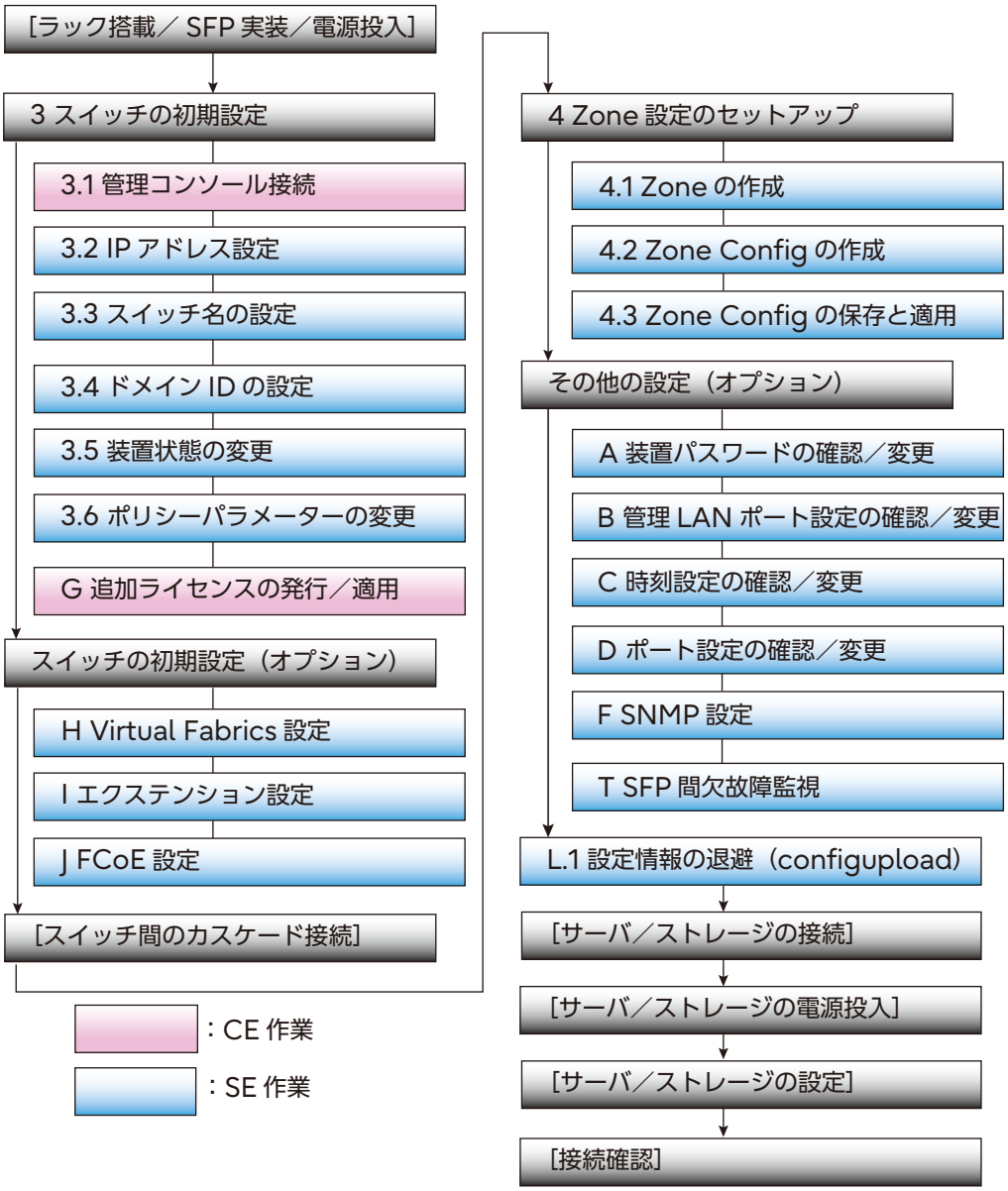
*4:　装置 WWN は、装置本体の上面に貼られている WWN ラベルに記載されている 16 桁の数字です。

2.2　セットアップ手順

本章では、「図2.1　システム構成図（例）」のFC-SW1の構成に従って、設定する手順を説明しています。スイッチのセットアップを行う際の手順は、以下のようなフローになっています。

備 考

各コマンドの出力結果は一例となります。詳細は「 関連マニュアル」(P.6) を参照してください。



第 3 章

スイッチの初期設定

3.1 管理コンソール接続

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。
セキュリティ強化のため、SSH での接続を推奨します。Telnet の使用が必要な場合は、Telnet を有効にしてください。設定確認方法の詳細については、「S.1 Telnet 有効／無効の設定手順」(P.132) を参照してください。

ターミナルソフトを使用し、以下の手順を実行します。

手 順

1 シリアルケーブルで接続して、ID およびパスワードを入力しログイン後、「S.1 Telnet 有効／無効の設定手順」(P.132) を参照して、Telnet を有効にします。
SSH 接続の場合、本手順は不要です。

2 スイッチに SSH 接続、Telnet 接続、またはシリアル接続後、ログイン画面でユーザー ID とパスワードを入力します（SSH 接続または Telnet 接続は、管理 LAN ポートを使用します）。

備 考

ログイン時にパスワードの変更を求められた場合は、パスワードを変更してください。変更した場合は忘れないよう管理してください。
Use Control-C to exit or press 'Enter' key to proceed. が表示された場合は、「Ctrl」+「C」キーを押すと操作をスキップできます。
FOS v8.2.2 以降、デフォルトパスワードでの運用はできない仕様です。

■ SSH 接続の場合

```
ssh admin@192.168.0.xxx

<<省略>>

admin@192.168.0.xxx's password:
Switch:admin>
```

■ Telnet 接続の場合

```
# telnet 192.168.30.70

<< 省略 >>

switch login: admin
Password:password

Please change your passwords now.
Use Control-C to exit or press 'Enter' key to proceed.  <Ctrl + C>

Password was not changed. Will prompt again at next login
until password is changed.
------------------------------------------------------------------
switch:admin>
```

3 Telnet を無効にします。手順については、「S.1 Telnet 有効／無効の設定手順」(P.132) を参照してください。

手順ここまで

3.2　IP アドレス設定

スイッチの IP アドレス／サブネットマスク／ゲートウェイ設定は、以下の手順を実行します。

手 順

1　以下のコマンドを使用して、ボックスタイプのスイッチは 1 個の IP アドレスを設定します。ダイレクタタイプのスイッチは、シャーシ内の 2 枚の CP ブレード用に各 1 個、シャーシの代表 IP に 1 個の計 3 個の IP アドレスを設定します。

備 考

IP アドレスが変更されると Telnet 接続が切断されるため、再度 Telnet 接続を行ってください。

■ ボックスタイプの場合

```
switch:admin> ipaddrset
DHCP [Off]: <Enter>
Ethernet IP Address [192.168.30.70]:192.168.0.10
Ethernet Subnet mask [255.255.255.0]:255.255.255.0
Gateway IP Address [none]:192.168.0.1
IP address is being changed...

switch:admin> ipaddrshow

SWITCH
Ethernet IP Address: 192.168.0.10
Ethernet Subnet mask: 255.255.255.0
Gateway IP Address: 192.168.0.1
DHCP: Off
IPv6 Autoconfiguration Enabled: No
Local IPv6 Addresses:
link local fe80::da1f:ccff:fefb:92e0/64
IPv6 Gateways:
DHCPv6: Off
IPv6 DDNS: Off
switch:admin>
```

■ ダイレクタタイプの場合（*1）

```
switch:admin> ipaddrset -chassis
DHCP [Off]:
Ethernet IP Address [192.168.0.195]:192.168.0.195
Ethernet Subnet mask [255.255.255.0]:255.255.255.0
x6-8DVT:admin> ipaddrset -cp 0
DHCP [Off]:
Host Name [cp0]:
Ethernet IP Address [192.168.0.196]:192.168.0.196
Ethernet Subnet mask [255.255.255.0]:255.255.255.0
Gateway IP Address [192.168.0.1]:192.168.0.1
x6-8DVT:admin> ipaddrset -cp 1
DHCP [Off]:
Host Name [cp1]:
Ethernet IP Address [192.168.0.197]:192.168.0.197
Ethernet Subnet mask [255.255.255.0]:255.255.255.0
Gateway IP Address [192.168.0.1]:192.168.0.1
switch:admin>


switch:admin> ipaddrshow

CHASSIS
Ethernet IP Address: 192.168.0.195
Ethernet Subnet mask: 255.255.255.0

CP0
Ethernet IP Address: 192.168.0.196
Ethernet Subnet mask: 255.255.255.0
Host Name: cp0
Gateway IP Address: 192.168.0.1

CP1
Ethernet IP Address: 192.168.0.197
Ethernet Subnet mask: 255.255.255.0
Host Name: cp1
Gateway IP Address: 192.168.0.1
DHCP: Off
IPv6 Autoconfiguration Enabled: Yes
Local IPv6 Addresses:
cp 0 link local fe80::c6f5:7cff:fe69:7f55/64
cp 1 link local fe80::c6f5:7cff:fea6:9add/64
IPv6 Gateways:
DHCPv6: Off
IPv6 DDNS: Off
switch:admin>
```

*1:　FOS v8.2.x 以降は、先に RON（Registered Organization Name）の設定をしないと、IP アドレス変更ができません。RON の設定手順は以下のとおりです。

- 以下のコマンドを入力します。

```
ron --set "XXX"     →"XXX"にRON（Registered Organization Name）を入力
```

- 実行例

```
swd77:FID128:admin> ipaddrset -chassis
Registered Organization Name is not set          →設定されていないと設定を促される
Please set the Registered Organization Name using: 'ron --set <org name>' command
before changing the ipaddress
swd77:FID128:admin>
swd77:FID128:admin>
swd77:FID128:admin> ron --set "xxxxxx"

Registered Organization Name will be set to: xxxxxx
Once changes are commited, it cannot be modified.
Are you sure you want to commit these changes? (Y/N)?y
Registered Organization Name is set successfully.→RON設定を確認後、IPアドレスを設定
swd77:FID128:admin>
swd77:FID128:admin>
swd77:FID128:admin> ipaddrset -chassis          →FOS v8.2.x以前の場合はここから設定可能
DHCP [Off]:
Ethernet IP Address [10.77.77.77]:192.168.0.124
Ethernet Subnet mask [255.255.255.0]:
IP address is being changed...
2020/06/25-09:26:30, [IPAD-1000], 90, SLOT 1 | CHASSIS, INFO, Brocade_X7-4, SW/0
Ether/0 IPv4 manual 192.168.0.124/24 DHCP Off.
Done.
swd77:FID128:admin>
swd77:FID128:admin> 2020/06/25-09:26:32, [IPAD-1000], 91, SLOT 2 | CHASSIS, INFO,
Brocade_X7-4, SW/0 Ether/0 IPv4 manual 192.168.0.124/24 DHCP Off.

swd77:FID128:admin> ipaddrset -cp 0
DHCP [Off]:
Host Name [cp0]:
Ethernet IP Address [10.77.77.75]:192.168.0.125
Ethernet Subnet mask [255.255.255.0]:
Gateway IP Address [none]:192.168.0.1
IP address is being changed...

2020/06/25-09:27:07, [IPAD-1000], 92, SLOT 1 | CHASSIS, INFO, Brocade_X7-4, CP/0
Ether/0 IPv4 manual 192.168.0.125/24 DHCP Off.
2020/06/25-09:27:07, [IPAD-1001], 93, SLOT 1 | CHASSIS, INFO, Brocade_X7-4, CP/0
IPv4 manual 192.168.0.1 DHCP Off.
2020/06/25-09:27:07, [IPAD-1001], 94, SLOT 1 | CHASSIS, INFO, Brocade_X7-4, CP/1
IPv4 manual 192.168.0.1 DHCP Off.
Done.
```

```
swd77:FID128:admin>
swd77:FID128:admin> 2020/06/25-09:27:09, [IPAD-1000], 95, SLOT 2 | CHASSIS, INFO,
Brocade_X7-4, CP/0 Ether/0 IPv4 manual 192.168.0.125/24 DHCP Off.
2020/06/25-09:27:09, [IPAD-1001], 96, SLOT 2 | CHASSIS, INFO, Brocade_X7-4, CP/0
IPv4 manual 192.168.0.1 DHCP Off.
2020/06/25-09:27:09, [IPAD-1001], 97, SLOT 2 | CHASSIS, INFO, Brocade_X7-4, CP/1
IPv4 manual 192.168.0.1 DHCP Off.

swd77:FID128:admin>
swd77:FID128:admin> ipaddrset -cp 1
DHCP [Off]:
Host Name [cp1]:
Ethernet IP Address [10.77.77.74]:192.168.0.126
Ethernet Subnet mask [255.255.255.0]:
Gateway IP Address [192.168.0.1]:
IP address is being changed...
2020/06/25-09:27:40, [IPAD-1000], 98, SLOT 1 | CHASSIS, INFO, Brocade_X7-4, CP/1
Ether/0 IPv4 manual 192.168.0.126/24 DHCP Off.
Done.
swd77:FID128:admin> 2020/06/25-09:27:42, [IPAD-1000], 99, SLOT 2 | CHASSIS, INFO,
Brocade_X7-4, CP/1 Ether/0 IPv4 manual 192.168.0.126/24 DHCP Off.
```

手順ここまで

3.3　スイッチ名の設定

スイッチ名の設定は、以下の手順を実行します。

手 順

1　以下のコマンドを使用して、スイッチの名称を設定します。

```
switch:admin> switchname "switch_1"                    (*1)
Committing configuration...
Done.
Switch name has been changed.Please re-login into the switch for the change to
be applied.
switch:admin>
```

*1:　スイッチ名として設定できる値は、以下の制限があります。
- 英字、数字、ハイフン、およびアンダースコアで構成されること（空白文字は使用不可）
- 30 文字以内であること

2　スイッチからいったんログアウトし、再度ログインしてから、以下のコマンドを使用してスイッチ名が修正されたことを確認します。

```
switch_1:admin> switchname
switch_1
switch_1:admin>
```

手順ここまで

3.4　ドメイン ID の設定

ドメイン ID とは、ファブリック内のスイッチを識別する一意な ID で、Zone はこの ID で指定が行われます。ドメイン ID の設定は、以下の手順を実行します。

手 順

1 以下のコマンドを使用して、ドメイン ID を設定します（ドメイン ID 以外のパラメーターは、通常特に変更する必要がないため、「Enter」キーを繰り返し押してコマンドを終了します）。

備 考

カスケードしたスイッチと同じドメイン ID を設定すると、相互に通信が行えないセグメンテーションと呼ばれる状態となります。

```
switch_1:admin> switchdisable
switch_1:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no] y
Domain: (1..239) [1] 10
WWN Based persistent PID (yes, y, no, n): [no] <Enter>

<< 省略 >>

switch_1:admin> switchenable
switch_1:admin> switchshow
switchName:     switch_1
switchType:     71.2
switchState:    Online
switchMode:     Native
switchRole:     Principal
switchDomain:   10
switchId:       fffc0a
switchWwn:      10:00:00:05:1e:07:c2:54
switchDomain:   10
zoning:         OFF
switchBeacon:   OFF

<< 省略 >>

switch_1:admin>
```

手順ここまで

3.5　装置状態の変更

SN200 モデル 140 の場合、以下の手順を実行します。

手 順

1　以下のコマンドを使用して、スイッチの状態を Online に変更します。

```
switch_1:admin> switchcfgpersistentenable
Switch' persistent state set to 'enabled'
switch_1:admin> switchshow
switchName:     switch_1
switchType:     71.2
switchState:    Online

<< 省略 >>

switch_1:admin>
```

手順ここまで

3.6　ポリシーパラメーターの変更

Brocade 6505 を使用し、スイッチ 1 台につき 2 個の電源装置を使用する場合、以下の手順を実行します。

注 意

本設定は Fabric Watch の設定です。FOS v7.4.0 以降では Fabric Watch はサポートされません。そのため、FOS v7.4.0 以降では本設定は不要です。検知については、Errdump に記録されるイベントを確認してください。

手 順

1 以下のコマンドを使用して、スイッチのポリシーパラメーターの「Bad PowerSupplies contributing to MARGINAL status」および「Bad Fans contributing to MARGINAL status」を変更します。

```
switch_1:admin> switchstatuspolicyset
To change the overall switch status policy parameters

<< 省略 >>

The minimum number of
  Bad PowerSupplies contributing to DOWN status: (0..2) [2]
  Bad PowerSupplies contributing to MARGINAL status: (0..2) [0] 1
  Bad Temperatures contributing to DOWN status: (0..1) [1]
  Bad Temperatures contributing to MARGINAL status: (0..1) [1]
  Bad Fans contributing to DOWN status: (0..2) [2]
  Bad Fans contributing to MARGINAL status: (0..2) [0] 1
  Out of range Flash contributing to DOWN status: (0..1) [0]
  Out of range Flash contributing to MARGINAL status: (0..1) [1]
  MarginalPorts contributing to DOWN status: (0..100) [25.00]
  MarginalPorts contributing to MARGINAL status: (0..100) [10.00]
  FaultyPorts contributing to DOWN status: (0..100) [25.00]
  FaultyPorts contributing to MARGINAL status: (0..100) [10.00]
  MissingSFPs contributing to DOWN status: (0..100) [0.00]
  MissingSFPs contributing to MARGINAL status: (0..100) [0.00]
  ErrorPorts contributing to DOWN status: (0..100) [0.00]
  ErrorPorts contributing to MARGINAL status: (0..100) [0.00]

Policy parameter set has been changedSwitch's persistent state set to
'enabled'
```

```
switch_1:admin> switchstatuspolicyshow
The current overall switch status policy parameters:
                   Down    Marginal
 ----------------------------------
     PowerSupplies    2           1
      Temperatures    1           1
              Fans    2           1
             Flash    0           1
     MarginalPorts  25.00%[6]          10.00%[2]
       FaultyPorts  25.00%[6]          10.00%[2]
       MissingSFPs   0.00%[0]           0.00%[0]
        ErrorPorts   0.00%[0]           0.00%[0]
Number of ports: 24
switch_1:admin>
```

手順ここまで

第 4 章

Zone 設定のセットアップ

本スイッチは Zone 設定を必須としています。Zone 設定を行うことにより、同じ Zone として定義されているサーバ／ストレージ間のみ互いにアクセスすることが可能です。以下に、Port Zoning による設定手順について説明します。

備 考

- Zone 設定は、ファブリック内のすべてのスイッチで共通の設定となります。「図 2.1　システム構成図（例）」の場合、FC-SW1 で Zone 設定を実施すると、FC-SW2 に同じ設定が伝搬します。
- FOS v9.1.x 以降では TI ゾーンはサポートされません。FOS v9.0.x で TI ゾーンが必要なシステムを新たに設定する場合は、FOS v8.x 以前の版数で TI ゾーンを作成してからファームウェアをアップグレードする必要があります。

4.1　Zone の作成

サーバ側ポートとストレージ側ポートが 1 対 1 となるようにサーバのポートごとに Zone を作り、サーバが使用するストレージを Zone の中へ含めます。

備 考

- ドメイン ID とポートインデックスの組み合わせや WWN に対して、**alias** コマンドでわかりやすい名前を付け、Zone を構成することも可能です。
- ポートインデックスは **switchShow** コマンドで確認します。ボックスタイプのポートインデックスは、ポート番号と同一です。ダイレクタタイプのポートインデックスは、「付録 O ダイレクタタイプのポートインデックス一覧」(P.110) を参照してください。

手 順

1　以下のコマンドを使用して、Zone を作成します。

alias 名は付けても付けなくても動作に違いはありません。

- Zone 設定例（alias 名なし）

```
switch_1:admin> zonecreate "Zone1","10,1;10,5"     (*1)
switch_1:admin> zonecreate "Zone2","10,2;10,5"     (*2)
switch_1:admin> zonecreate "Zone3","20,1;20,5"     (*3)
switch_1:admin> zonecreate "Zone4","20,2;20,5"     (*4)
switch_1:admin>
```

- Zone 設定例（alias 名あり）

```
switch_1:admin> alicreate "SV_Win_Slot1","10,1"
switch_1:admin> alicreate "SV_Lin_Slot1","10,2"
switch_1:admin> alicreate "Storage_Port0","10,5"
switch_1:admin> alicreate "SV_Win_Slot2","20,1"
switch_1:admin> alicreate "SV_Lin_Slot2","20,2"
switch_1:admin> alicreate "Storage_Port1","20,5"
switch_1:admin> zonecreate "Zone1","SV_Win_Slot1;Storage_Port0"  (*1)
switch_1:admin> zonecreate "Zone2","SV_Lin_Slot1;Storage_Port0"  (*2)
switch_1:admin> zonecreate "Zone3","SV_Win_Slot2;Storage_Port1"  (*3)
switch_1:admin> zonecreate "Zone4","SV_Lin_Slot2;Storage_Port1"  (*4)
switch_1:admin>
```

*1:　ドメイン ID:10 の Port1 - Port5 間のデータアクセスを許可する定義として「Zone1」を作成
*2:　ドメイン ID:10 の Port2 - Port5 間のデータアクセスを許可する定義として「Zone2」を作成
*3:　ドメイン ID:20 の Port1 - Port5 間のデータアクセスを許可する定義として「Zone3」を作成
*4:　ドメイン ID:20 の Port2 - Port5 間のデータアクセスを許可する定義として「Zone4」を作成

手順ここまで

4.2　Zone Config の作成

作成した Zone を装置に適用するには、適用対象の Zone を 1 つのコンフィグに束ねる必要があり、Zone Config の単位で使用する Zone を切り替えます。Zone Config の作成は、以下の手順を実行します。

手 順

1　以下のコマンドを使用して、Zone を作成します。

```
switch_1:admin> cfgcreate "CONFIG","Zone1;Zone2;Zone3;Zone4"      (*1)
switch_1:admin>
```

*1:　Zone1、Zone2、Zone3、Zone4 を 1 つのコンフィグとして定義する「CONFIG」を作成

手順ここまで

4.3　Zone Config の保存と適用

作成した Zone Config を適用することで、ファブリック内のすべてのスイッチに Zone が適用され、アクセス制御を開始します。Zone Config はファブリック内で 1 つのみ有効にすることができます。

手 順

1　以下のコマンドを使用して、Zone Config を適用します。

```
switch_1:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no, n): [no]
y
Updating flash ...
switch_1:admin> cfgenable "CONFIG"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'CONFIG' configuration  (yes, y, no, n): [no] y
zone config "CONFIG" is in effect
Updating flash ...
switch_1:admin>
```

手順ここまで

付録 A

装置パスワードの確認／変更

スイッチのパスワードを変更することで、セキュリティが向上します。ユーザー名「admin」は保守作業時にも使用します。パスワードを変更した場合は、担当保守員が保守作業を行う際にパスワードをお客様に入力していただく必要があります。admin のパスワードを忘れた場合は、本体交換になります。変更した場合は忘れないよう管理してください。

A.1 デフォルトパスワードの確認

デフォルトのユーザー名およびパスワードは以下となります。

ユーザー名	パスワード	備考
admin（*1）	password（*1）	スイッチ設定の変更および閲覧が可能
user	password	スイッチ設定の閲覧だけが可能

*1: ユーザー名とパスワードは工場出荷時のものです。ユーザー名とパスワードを変更した場合には、設定したユーザー名とパスワードを入力してください。

注 意

セキュリティの観点から、パスワードの変更および設定について以下の点に注意してください。

- 製品共通のユーザー ID およびパスワードは運用開始までに変更してください。
- パスワードは定期的に変更してください。
- パスワードは 8 文字以上を使用し、英文字、数字、および記号を組み合わせて設定してください。

A.2 パスワードの変更（passwd）

手 順

1 以下のコマンドを使用して、ログイン中のユーザーのパスワードを変更します。

```
switch_1:admin> passwd
Changing password for admin
Enter old password: password
Enter new password: xxxxxxxx                                    (*1)
Re-type new password: xxxxxxxx                                  (*1)
passwd: all authentication tokens updated successfully
Saving password to stable storage.
Password saved to stable storage successfully.
switch_1:admin>
```

*1: パスワードとして設定できる値には、以下の制限があります。

- 英字、数字、記号（コロンは対象外）で構成されること
- 8 ～ 40 文字以内であること
- 1 つ前に設定されたパスワードは再設定不可

FOS v9.0 以降では、admin およびユーザーアカウントのパスワードをデフォルトのパスワード文字列から変更する必要があります。

手順ここまで

付録 B

管理 LAN ポート設定の確認／変更

管理 LAN ポートの通信速度／通信モードは、接続先の LAN スイッチと設定を合わせる必要があります。

B.1　事前確認（ifmodeshow/ethif）

手 順

1　以下のコマンドを使用して、現在動作している通信速度／通信モードと MAC アドレスを確認します。

■ FOS v8.0.x 以降の場合（ethif コマンド）

```
switch_1:admin> ethif --show eth0
eth0 interface:
Link mode: negotiated 1000baseT-FD, link ok                    (*1)(*2)
MAC Address: C4:F5:7C:2A:84:48
eth0 Link encap:Ethernet HWaddr C4:F5:7C:2A:84:48
inet addr:192.168.0.57 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7725024 errors:0 dropped:0 overruns:0 frame:0
TX packets:226289 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
Memory:fe4e2000-fe4e2fff
switch_1:admin>
```

*1:　管理 LAN ポートが 1000M/FULL でリンクアップした際の出力例

*2:　管理インターフェースが 10Mbit/s で動作している場合、特定の FOS 操作（firmwaredownload など）が失敗することがあります。

■ FOS v7.4.x 以前の場合（ifmodeshow コマンド）

```
switch_1:admin> ifmodeshow eth0
Link mode: negotiated 100baseTx-FD, link ok                    (*1)
MAC Address: 00:05:1E:07:C2:54
switch_1:admin>
```

*1:　管理 LAN ポートが 100M/FULL でリンクアップした際の出力例

手順ここまで

B.2 通信速度／通信モードの変更（ifmodeset/ethif）

手 順

1 以下のコマンドを使用して、管理 LAN ポートの通信速度／通信モードを変更します。

備 考

ダイレクタタイプの装置は、両方の CP で変更を実施する必要があります。
G730 は通信速度／通信モードの初期値が自動設定のため、変更は不要です。

■ FOS v8.2.x 以降の場合（ethif コマンド）

```
switch_1:admin> ethif --set eth0                                          (*1)

Exercise care when using this command.  Forcing the link to
an operating mode not supported by the network equipment
to which it is attached, may result in an inability to
communicate with the system through its ethernet interface.

It is recommended that you only use this command from the
serial console port.

Are you sure you really want to do this? (yes, y, no, n): [no] y     (*2)
Proceed with caution.
Auto-negotiate (yes, y, no, n): [no] y
Advertise 1000 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 100 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 10 Mbps / Full Duplex (yes, y, no, n): [yes] y
Committing configuration...done.
switch_1:admin>
```

*1: すべての通信速度で「Auto-negotiate」を行う設定例です。
*2: コンソール接続している場合は表示されません。

■ FOS v8.0.x ～ FOS v8.1.x の場合（ethif コマンド）

```
switch_1:adminroot> ethif --set eth0 -an on -speed 1000 -duplex full  (*1)
an:on
speed:1000
cap:full
Exercise care when using this command. Forcing the link to
an operating mode not supported by the network equipment
to which it is attached, may result in an inability to
communicate with the system through its ethernet interface.
It is recommended that you only use this command from the
serial console port.
Are you sure you really want to do this? (yes, y, no, n): [no] y      (*2)
Proceed with caution.
MII_CMD:-A
ADVERTISE:Advertise
DEFMODE:yes
auto:1
MII_MODE:1000baseT-FD,
Committing configuration...done.
switch_1:admin>
```

*1: 1000M/FULL の通信速度で「Auto-negotiate」を行う設定例です。
複数の通信速度を指定することはできませんので、使用する回線に合わせた速度を指定してください。

*2: コンソール接続している場合は表示されません。

■ FOS v7.4.x 以前の場合（ifmodeset コマンド）

```
switch_1:admin> ifmodeset eth0                                        (*1)
Exercise care when using this command. Forcing the link to
an operating mode not supported by the network equipment to
which it is attached may result in an inability to
communicate with the system through its ethernet interface.
It is recommended that you only use this command from the
serial console port.
Are you sure you really want to do this? (yes, y, no, n): [no] y      (*2)
Proceed with caution.
Auto-negotiate (yes, y, no, n): [no] y
Advertise 1000 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 100 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 100 Mbps / Half Duplex (yes, y, no, n): [yes] y
Advertise 10 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 10 Mbps / Half Duplex (yes, y, no, n): [yes] y
Committing configuration...done.
switch_1:admin>
```

*1: すべての通信速度で「Auto-negotiate」を行う設定例です。

*2: コンソール接続している場合は表示されません。

手順ここまで

付録 C

時刻設定の確認／変更

スイッチのタイムゾーンはデフォルトで UTC となっており、NTP サーバとの時刻同期は行われていません。時刻同期を行う際の NTP サーバは、ネットワーク上で近いサーバを指定してください。

C.1　タイムゾーンの設定（tstimezone）

手 順

1　以下のコマンドを使用して、タイムゾーンを設定後、装置を再起動します。

```
switch_1:admin> tstimezone --interactive                          (*1)
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the POSIX TZ format.
Enter number or control-D to quit ? 5
Please select a country.
 1) Afghanistan           18) Israel                35) Palestine
 2) Armenia               19) Japan                 36) Philippines
 3) Azerbaijan            20) Jordan                37) Qatar
 4) Bahrain               21) Kazakhstan            38) Russia
 5) Bangladesh            22) Korea (North)         39) Saudi Arabia
 6) Bhutan                23) Korea (South)         40) Singapore
 7) Brunei                24) Kuwait                41) Sri Lanka
 8) Cambodia              25) Kyrgyzstan            42) Syria
 9) China                 26) Laos                  43) Taiwan
10) Cyprus                27) Lebanon               44) Tajikistan
11) East Timor            28) Macau                 45) Thailand
12) Georgia               29) Malaysia              46) Turkmenistan
```

```
13) Hong Kong             30) Mongolia              47) United Arab Emirates
14) India                 31) Myanmar (Burma)       48) Uzbekistan
15) Indonesia             32) Nepal                 49) Vietnam
16) Iran                  33) Oman                  50) Yemen
17) Iraq                  34) Pakistan
Enter number or control-D to quit ? 19

The following information has been given:

        Japan

Therefore TZ='Asia/Tokyo' will be used.
Local time is now:      Mon May 23 10:05:36 JST 2011.
Universal Time is now:  Mon May 23 01:05:36 UTC 2011.
Is the above information OK?
1) Yes
2) No
Enter number or control-D to quit ? 1
System Time Zone change will take effect at next reboot
switch_1:admin> tstimezone
Asia/Tokyo
switch_1:admin> fastboot                          (*2)
```

*1: タイムゾーンを「Asia/Tokyo」に設定

*2: タイムゾーンの変更後は、装置の再起動が必須

手順ここまで

C.2 時刻の設定（date）

注 意

- FOS v9.1.x 以降、前回の変更から 64 秒以内に日付を変更しようとすると、システムから「Date change within 64 seconds from previous change is not allowed（前回の変更から 64 秒以内の日付変更は許可されていません）」というメッセージが表示されます。再変更の場合は、64 秒経過後に実施してください。
- FOS v9.1.0 以降では、date コマンドを使用して前後 7 日を超えて日付を変更することはできません。

手 順

1 以下のコマンドを使用して、時刻を設定します。

```
switch_1:admin> date 0531012311                    (*1)
Tue May 31 01:23:00 JST 2011
switch_1:admin> date
Tue May 31 01:23:03 JST 2011
switch_1:admin>
```

*1: MMDDHHmmYY の形式で時刻を指定（MM は月、DD は日、HH は時、mm は分、YY は西暦の下 2 桁）
上記例は、スイッチの時刻を「2011 年 05 月 31 日 01 時 23 分」に設定

手順ここまで

C.3 NTP サーバとの時刻同期設定（tsclockserver）

注 意

FOS v9.1.0 以降では、tsclockserver コマンドを使用して前後 7 日を超えて日付を変更することはできません。

手 順

1 以下のコマンドを使用して、時刻同期先の NTP サーバを指定します。

備 考

本装置は NTP v3 をサポートします。また、NTP 設定はカスケード接続されたスイッチ間で伝搬され、共通の設定となります。

■ NTP サーバを 1 つ設定する場合

```
switch_1:admin> tsclockserver "192.168.0.40"                    (*1)
Updating Clock Server configuration...done.
Updated with the NTP servers
switch_1:admin> tsclockserver
Active NTP Server               192.168.0.40
Configured NTP Server List      192.168.0.40
switch_1:admin>
```

*1: 時刻同期先の NTP サーバを「192.168.0.40」に設定

■ NTP サーバを複数設定する場合

```
switch_1:admin> tsclockserver "192.168.0.40;192.168.0.140;192.168.0.240" (*1)
Updating Clock Server configuration...done.
Updated with the NTP servers
switch_1:admin> tsclockserver
Active NTP Server          192.168.0.40
Configured NTP Server List 192.168.0.40;192.168.0.140;192.168.0.240
switch_1:admin>
```

*1: 時刻同期先の NTP サーバを「192.168.0.40」に設定

■ NTP サーバを設定しない場合（デフォルト）

```
switch_1:admin> tsclockserver LOCL
Updating Clock Server configuration...done.
Updated with the NTP servers
switch_1:admin> tsclockserver
Active NTP Server               LOCL
Configured NTP Server List      LOCL
switch_1:admin>
```

手順ここまで

付録 D

ポート設定の確認／変更

ポートの設定変更は通常行う必要はありません。接続されるサーバ／ストレージで設定変更を指定された場合、変更してください。

備 考

本付録では、主要な設定項目について説明しています。
設定項目の詳細については、Brocade Fabric OS 製品マニュアルの該当するバージョンの『Command Reference Manual』を参照してください。

D.1 事前確認（portcfgshow/switchshow）

手 順

1 以下のコマンドを使用して、ポートの現行のコンフィグレーションを確認します。

■ FOS v8.0.0 以降の場合

```
switch_1:admin> portcfgshow
Ports of Slot 0          4   5   6   7     8   9  10  11    12  13  14  15
-----------------------+---+---+---+---+-----+---+---+---+-----+---+---+---
Octet Speed Combo        1   1   1   1     1   1   1   1     1   1   1   1
Speed                   AN  AN  AN  AN    AN  AN  AN  AN    AN  AN  AN  AN(*1)
AL_PA Offset 13          ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
Trunk Port               ON  ON  ON  ON    ON  ON  ON  ON    ON  ON  ON  ON
Long Distance            ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
VC Link Init             ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
Locked L_Port             -   -   -   -     -   -   -   -     -   -   -   -
Locked G_Port            ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
Disabled E_Port          ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
Locked E_Port            ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
ISL R_RDY Mode           ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
RSCN Suppressed          ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
Persistent Disable       ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
```

■ FOS v8.0.0 より前の場合

```
switch_1:admin> portcfgshow
Ports of Slot 0    0   1   2   3     4   5   6   7
-----------------+---+---+---+---+-----+---+---+---
Speed              AN  AN  AN  AN    AN  AN  AN  AN          (*1)
Fill Word          0   0   0   0     0   0   0   0           (*2)
AL_PA Offset 13    ..  ..  ..  ..    ..  ..  ..  ..
Trunk Port         ON  ON  ON  ON    ON  ON  ON  ON
Long Distance      ..  ..  ..  ..    ..  ..  ..  ..
VC Link Init       ..  ..  ..  ..    ..  ..  ..  ..
Locked L_Port      ..  ..  ..  ..    ..  ..  ..  ..
Locked G_Port      ..  ..  ..  ..    ..  ..  ..  ..
Disabled E_Port    ..  ..  ..  ..    ..  ..  ..  ..
Locked E_Port      ..  ..  ..  ..    ..  ..  ..  ..
ISL R_RDY Mode     ..  ..  ..  ..    ..  ..  ..  ..
RSCN Suppressed    ..  ..  ..  ..    ..  ..  ..  ..
Persistent Disable ..  ..  ..  ..    ..  ..  ..  ..
LOS TOV enable     ..  ..  ..  ..    ..  ..  ..  ..
NPIV capability    ON  ON  ON  ON    ON  ON  ON  ON
NPIV PP Limit     126 126 126 126   126 126 126 126
QOS E_Port         AE  AE  AE  AE    AE  AE  AE  AE
Mirror Port        ..  ..  ..  ..    ..  ..  ..  ..
Rate Limit         ..  ..  ..  ..    ..  ..  ..  ..
Credit Recovery    ON  ON  ON  ON    ON  ON  ON  ON
Fport Buffers      ..  ..  ..  ..    ..  ..  ..  ..
Port Auto Disable  ..  ..  ..  ..    ..  ..  ..  ..
CSCTL mode         ..  ..  ..  ..    ..  ..  ..  ..

Fault Delay        0   0   0   0     0   0   0   0

<< 省略 >>

switch_1:admin>
```

*1: 「D.2 ポート速度の変更 (portcfgspeed)」(P.58) で設定したポート速度（AN,1,2,4,8,16,32）を表示。設定値が 0 の場合は、「AN」が表示される。

*2: 転送速度が 16Gbit/s 以上のスイッチでは、「Fill Word」の項目は表示されません。

2 以下のコマンドを使用して、スイッチの動作状態を確認します。

■ FOS v8.0.0 以降の場合

```
switch:admin> switchshow
switchName:             switch                      (*1)
switchType:             165.0
switchState:            Online                      (*2)
switchMode:             Native
switchRole:             Principal
switchDomain:           1                           (*3)
switchId:               fffc01
switchWwn:              10:00:c4:f5:7c:2d:3c:48
zoning:                 OFF                         (*4)
switchBeacon:           OFF
FC Router:              OFF
FC Router BB Fabric ID: 1
Address Mode:           0
HIF Mode:               OFF

Index(*5) Slot Port(*6) Address Media Speed(*7) State(*8)    Proto
==========================================================================
 0         3    0       010000  --    N32       No_Module    FC
 1         3    1       010100  --    N32       No_Module    FC
 2         3    2       010200  --    N32       No_Module    FC
```

■ FOS v8.0.0 より前の場合

```
switch_1:admin> switchshow
switchshow
switchName:     switch_1                    (*1)
switchType:     71.2
switchState:    Online                      (*2)
switchMode:     Native
switchRole:     Subordinate
switchDomain:   10                          (*3)
switchId:       fffc1f
switchWwn:      10:00:00:05:1e:08:80:03
zoning:         ON (CONFIG)                 (*4)
switchBeacon:   OFF

Index(*5) Port(*6)Address Media Speed(*7)State(*8) Proto
==========================================================
 0         0      0a0000  id    N8       No_Light  FC
 1         1      0a0100  id    N8       Online    FC F-Port 10:00:00:00:c9:49:9f:76
 2         2      0a0200  id    N8       No_Light  FC

<< 省略 >>

switch_1:admin>
```

*1: 「3.3 スイッチ名の設定」(P.36) で設定したスイッチ名を表示
*2: 「E.3 スイッチ全体のオフライン設定（switchdisable)」(P.62)、「E.4 スイッチ全体のオンライン設定（switchenable)」(P.63) で設定したスイッチ状態を表示
*3: 「3.4 ドメイン ID の設定」(P.37) で設定したドメイン ID を表示
*4: 「4.3 Zone Config の保存と適用」(P.44) で適用した Zone Config を表示
*5: スイッチのポートインデックスを表示
*6: スイッチのポート番号を表示

*7: 「D.2 ポート速度の変更（portcfgspeed）」(P.58) で設定したポート速度を表示
（Autonegotiation 設定の場合、リンクを確立したポート速度を表示）

*8: 「E.1 ポートのオフライン設定（portdisable）」(P.61)、「E.2 ポートのオンライン設定（portenable）」(P.62) で設定したポート状態を表示します。ポートの主な状態表示パラメーターは以下となります。
No_Card: インターフェース カードがない
No_Module: モジュール（SFP など）がない
Mod_Val: モジュール適性チェック処理中
Mod_Inv: モジュール速度の不一致または互換性のない SFP
No_Light: モジュールが光を受信していない
No_SigDet: QSFP はインストールされているが、ケーブルに接続されていない
No_Sync: モジュールは光を受信しているが、同期していない
In_Sync: モジュールは光を受信し、同期している
Laser_Flt: モジュールがレーザー不良の信号を出している
Port_Flt: ポートが不良とマークされた
Diag_Flt: ポートの診断が失敗に終わった
Lock_Ref: 基準信号にロックしている
Testing: ポートが診断を実行中
Offline: ポート接続が確立されていない
Online: ポート接続が確立し、正常に動作している

手順ここまで

D.2 ポート速度の変更（portcfgspeed）

手 順

1 以下のコマンドを使用して、ポートの速度レベルの変更を行います。

```
switch_1:admin> portcfgspeed 0/7 0            (*1)(*2)
switch_1:admin>
```

*1: 速度レベルとして指定可能なパラメーターは以下となります（本設定例の場合、 [Slot0]/Port7 のポート速度を Autonegotiation に設定）。
0: Autonegotiation モードに設定
1: ポートを 1Gbit/s の固定速度に設定
2: ポートを 2Gbit/s の固定速度に設定
4: ポートを 4Gbit/s の固定速度に設定
8: ポートを 8Gbit/s の固定速度に設定
16: ポートを 16Gbit/s の固定速度に設定
32: ポートを 32Gbit/s の固定速度に設定
64: ポートを 64Gbit/s の固定速度に設定

*2: ダイレクタタイプの場合のみ、設定するポートのスロット番号を指定し、その後にスラッシュ（/）を付けてポートを指定します。ダイレクタタイプ以外の場合は、ポート番号のみを指定します。

注 意

以下の環境の場合、ドライブが接続されたファイバチャネルスイッチのポート速度を 4Gbit/s 固定設定としてください。
ただし、v7.3.0c 以降のファームウェアを適用しドライブが接続されたポートに対して、**portcfgnondfe** コマンドを使用して DFE（Decision Feedback Equalization）を無効に設定変更することで、通信速度 8Gbit/s での接続が可能です。

- ETERNUS LT250 テープライブラリ、ETERNUS LT270 テープライブラリ、ETERNUS LT270 S2 テープライブラリに搭載された LTO 5、LTO 6、および LTO 7 ドライブと接続する場合
- ETERNUS LT20 S2, LT40 S2, LT60 S2 テープライブラリ、ETERNUS LT260 テープライブラリに搭載された IBM 製 LTO 6 および LTO 7 ドライブ（*1）と接続する場合

*1: LTO 6 ドライブ（型名：LT20SFK1、LT40SFK1、LT60SFK1、LT26BFKE、LT26BFKL）、LTO 7 ドライブ（型名：LT20SFM1、LT40SFM1、LT60SFM1、LT26BFME、LT26BFML）

手順ここまで

D.3 ポートの固定設定（portcfggport）

注 意

本コマンドは FOS v9.0.x 以降ではサポートされません。

手 順

1 以下のコマンドを使用して、G ポート固定の設定をポートに行います。

```
switch_1:admin> portcfggport 2/3, 1          (*1)
switch_1:admin>
```

*1: Slot2/Port3 のポートを G ポート固定に設定

手順ここまで

D.4 ポートの初期化設定（portcfgdefault）

手 順

1 以下のコマンドを使用して、ポート設定の初期化を行います。

■ ダイレクタタイプの場合

```
switch_1:admin> portcfgdefault 2/3          (*1)
switch_1:admin>
```

*1: Slot2/Port3 のポートをデフォルト設定に変更

■ ボックスタイプの場合

```
switch_1:admin> portcfgdefault 7            (*1)
switch_1:admin>
```

*1: Port7 のポートをデフォルト設定に変更

手順ここまで

付録 E

ポートの Offline / Online

すべてのポートはデフォルトで「Online」となりますが、リンクが正常に確立されない場合はポート／スイッチ全体の「Offline/Online」を行うとリンクがリセットされます。

E.1 ポートのオフライン設定（portdisable）

手 順

1 以下のコマンドを使用して、単一のポートの Offline 設定を行います。

■ ダイレクタタイプの場合

```
switch_1:admin> portdisable 2/16                    (*1)
switch_1:admin>
```

*1: Slot2/Port16 のポートを Offline に設定

■ ボックスタイプの場合

```
switch_1:admin> portdisable 7                       (*1)
switch_1:admin>
```

*1: Port7 のポートを Offline に設定

手順ここまで

E.2 ポートのオンライン設定（portenable）

手 順

1 以下のコマンドを使用して、単一のポートの Online 設定を行います。

■ ダイレクタタイプの場合

```
switch_1:admin> portenable 2/16                    (*1)
switch_1:admin>
```

*1: Slot2/Port16 のポートを Online に設定

■ ボックスタイプの場合

```
switch_1:admin> portenable 7                       (*1)
switch_1:admin>
```

*1: Port7 のポートを Online に設定

手順ここまで

E.3 スイッチ全体のオフライン設定（switchdisable）

手 順

1 以下のコマンドを使用して、スイッチの全ポートの Offline 設定を行います。

```
switch_1:admin> switchdisable
switch_1:admin>
```

手順ここまで

E.4 スイッチ全体のオンライン設定（switchenable）

手 順

1 以下のコマンドを使用して、スイッチの全ポートの Online 設定を行います。

```
switch_1:admin> switchenable
switch_1:admin>
```

手順ここまで

付録 F

SNMP 設定

本スイッチは SNMP エージェント機能（SNMPv1, v3）を備えており、SNMP マネージャーと連携し管理 LAN ポートで管理情報ベース（MIB）の情報参照が行えます。また、スイッチの状態変化を Trap として SNMP マネージャーに通知します。

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。

F.1 事前確認（snmpconfig）

手 順

1 以下のコマンドを使用して、SNMP 設定を確認します。

- SNMPv1 の場合（FOS v9.0.0 未満）

```
switch_1:admin> snmpconfig --show snmpv1

SNMPv1 community and trap recipient configuration:
Community 1: Secret C0de (rw)
No trap recipient configured yet
Community 2: OrigEquipMfr (rw)
No trap recipient configured yet
Community 3: private (rw)
No trap recipient configured yet
Community 4: public (ro)
No trap recipient configured yet
Community 5: common (ro)
No trap recipient configured yet
Community 6: FibreChannel (ro)
No trap recipient configured yet
switch_1:admin>
```

- SNMPv1 の場合（FOS v9.0.x 以降 v9.2.0 未満）

```
switch_1:admin> snmpconfig --show snmpv1
  Community 1:
    No trap recipient configured yet
  Community 2:
    No trap recipient configured yet
  Community 3:
    No trap recipient configured yet
  Community 4:
    No trap recipient configured yet
  Community 5:
    No trap recipient configured yet
  Community 6:
    No trap recipient configured yet
SNMPv1:Enabled
```

- SNMPv1 の場合（FOS v9.2.0 以降）

```
switch:admin> snmpconfig --show snmpv1

SNMPv1 community and trap recipient configuration:
  Community 1:
    No trap recipient configured yet
  Community 2:
    No trap recipient configured yet
  Community 3:
    No trap recipient configured yet
  Community 4:
    No trap recipient configured yet
  Community 5:
    No trap recipient configured yet
  Community 6:
    No trap recipient configured yet
SNMPv1:Disabled
```

- SNMPv3 の場合（FOS v9.0.0 未満）

```
switch_1:admin> snmpconfig --show snmpv3

SNMP Informs = 0 (OFF)

SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 2 (rw): snmpadmin2
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 3 (rw): snmpadmin3
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 4 (ro): snmpuser1
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 5 (ro): snmpuser2
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 6 (ro): snmpuser3
        Auth Protocol: noAuth
        Priv Protocol: noPriv

SNMPv3 Trap/Informs configuration:
Trap Entry 1:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 2:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 3:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 4:     No trap recipient configured yet
   Notify Type: TRAP(1)
Trap Entry 5:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 6:     No trap recipient configured yet
    Notify Type: TRAP(1)
switch_1:admin>
```

- SNMPv3 の場合（FOS v9.0.x 以降 v9.2.0 未満）

```
switch_1:admin> snmpconfig --show snmpv3

SNMP Informs = 0 (OFF)

SNMPV3 user password encrypted  = 0 (OFF)

SNMPv3 USM configuration:
User 1:
User 2:
User 3:
User 4:
User 5:
User 6:
User 7:
User 8:
User 9:
User 10:
User 11:
User 12:

SNMPv3 Trap/Informs configuration:
Trap Entry 1:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 2:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 3:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 4:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 5:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 6:     No trap recipient configured yet
    Notify Type: TRAP(1)
```

- SNMPv3 の場合（FOS v9.2.0 以降）

```
switch:admin> snmpconfig --show snmpv3

SNMP Informs = 0 (OFF)

SNMPV3 user password encrypted  = 1 (ON)

SNMPv3 USM configuration:
User 1:
User 2:
User 3:
User 4:
User 5:
User 6:
User 7:
User 8:
User 9:
User 10:
User 11:
User 12:

SNMPv3 Trap/Informs configuration:
Trap Entry 1:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 2:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 3:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 4:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 5:     No trap recipient configured yet
    Notify Type: TRAP(1)
Trap Entry 6:     No trap recipient configured yet
    Notify Type: TRAP(1)
```

手順ここまで

F.2 SNMP の設定／確認（snmpconfig）

SNMP の設定は、以下の手順を実行します。

手 順

1 以下のコマンドを使用して、SNMP 設定を実施します。

■ SNMPv1、FOS v8.2.x まで

```
switch_1:admin> snmpconfig --set snmpv1

SNMP community and trap recipient configuration:
Community (rw): [Secret C0de] <Enter>
Trap Recipient's IP address : [0.0.0.0] <Enter>
Community (rw): [OrigEquipMfr] <Enter>
Trap Recipient's IP address : [0.0.0.0] <Enter>
Community (rw): [private] <Enter>
Trap Recipient's IP address : [0.0.0.0] <Enter>
Community (ro): [public] storage-nw                          (*1)
Trap Recipient's IP address : [0.0.0.0] 192.168.0.30         (*2)
Trap recipient Severity level : (0..5) [0] 3                 (*3)
Trap recipient Port : (0..65535) [162] 162                   (*2)
Community (ro): [common] <Enter>
Trap Recipient's IP address : [0.0.0.0] <Enter>
Community (ro): [FibreChannel] <Enter>
Trap Recipient's IP address : [0.0.0.0] <Enter>
Committing configuration.....done.
switch_1:admin>
```

*1: SNMP マネージャーがスイッチの MIB 値要求時（情報参照／情報設定）に使用する Community 名
（本設定例の場合、SNMP マネージャーから Community 名 :storage-nw でスイッチの情報参照が可能）

*2: Trap 送信先となる SNMP マネージャーの IP アドレス／送信先ポート番号
（本設定例の場合、SNMP マネージャー [IP:192.168.0.30, Port162] 宛てに Trap を送信）

*3: スイッチでイベントが発生した際、指定された重大度レベル以上のメッセージが Trap として通知されます。重大度レベルで指定可能なパラメーターは以下となります（本設定例の場合、イベントログから Critical/Error/Warning メッセージが Trap 通知）。
0: None（デフォルト）
1: Critical
2: Error
3: Warning
4: Informational
5: Debug

■ SNMPv1、FOS v9.0.x 以降

1 SNMPv1 を有効にします（FOS v9.1.x より前のバージョンでは実施不要です）。

```
switch:admin> snmpconfig --enable snmpv1
```

2 以下のコマンドを使用して、Secure Mode が無効になっていることを確認します。最終行が Enabled と表示されている場合、SNMPv1 が有効となります。

```
admin> snmpconfig --show snmpv1

SNMPv1 community and trap recipient configuration:
  Community 1: public (ro)
    No trap recipient configured yet
  Community 2:
    No trap recipient configured yet
  Community 3:
    No trap recipient configured yet
  Community 4:
    No trap recipient configured yet
  Community 5:
    No trap recipient configured yet
  Community 6:
    No trap recipient configured yet
SNMPv1:Enabled                                          (*1)
```

*1: Enabled は SNMPv1 が有効、Disabled は SNMPv1 が無効になっていることを示しています。

3 SNMPv1 設定を実施します。

備 考

環境変更に応じて snmp の設定を snmpv1 から snmpv3 へ変更する場合は、セキュリティ強化のため snmpv1 を無効にする手順を実施してください。

```
                                          (*1)                (*2)
switch:admin> snmpconfig --add snmpv1 -index 1 -community storage-nw -host
(*3)                              (*4)
192.168.0.30 -groupname ro -severity 3
Committing configuration.....done.
switch:admin>
```

*1: 設定を保存するインデックスとして 1~6 のいずれかの数値を指定します。

*2: SNMP マネージャーがスイッチの MIB 値要求時（情報参照／情報設定）に使用する Community 名
（本設定例の場合、SNMP マネージャーから Community 名：storage-nw でスイッチの情報参照が可能）

*3: Trap 送信先となる SNMP マネージャーの IP アドレス／送信先ポート番号
（本設定例の場合、SNMP マネージャー [IP:192.168.0.30, Port162] 宛てに Trap を送信）

*4: スイッチでイベントが発生した際、指定された重大度レベル以上のメッセージが Trap として通知されます。重大度レベルで指定可能なパラメーターは以下となります（本設定例の場合、イベントログから Critical/Error/Warning メッセージが Trap 通知）。

0: None（デフォルト）
1: Critical
2: Error
3: Warning
4: Informational
5: Debug

■ SNMPv3、FOS v8.0.x 以前の場合

注 意

Virtual Fabric を構成するスイッチを Brocade Network Advisor で監視する場合は、スイッチのユーザーを、SNMPv3 ユーザーとして構成してください。

```
switch_1:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false]                    (*1)

SNMPv3 user configuration(snmp user not configured in FOS user database will
have physical AD and admin role as the default):
User (rw): [snmpadmin1]                                              (*2)
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1                (*3)
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (1..4) [2] 4   (*4)
New Priv Passwd:
Verify Priv Passwd:
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]

SNMPv3 trap/inform recipient configuration:
Trap Recipient's IP address : [0.0.0.0] 192.168.0.30                 (*5)

Notify Type [TRAP(1)/INFORM(2)]: (1..1) [1]                          (*6)
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [0] 3                         (*7)
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
switch_1:admin>
```

*1: SNMPv3 で Inform（Recipient へ受領確認要求）を使用する場合は、true を選択します。
*2: SNMPv3 用のユーザーを選択します。
*3: (*2) で選択したユーザーで使用する認証プロトコルを選択します。noAuth 以外を選択するとパスワードの入力を求められます。
*4: (*2) で選択したユーザーで使用する暗号方法を選択します。noPriv 以外を選択するとパスワードの入力を求められます。
*5: 通知の送信先となるサーバの IP アドレスを指定します。
*6: 通知の形式が INFORM か TRAP かを選択します。(*1) で false を選択した場合は、TRAP を選択してください。
*7: スイッチでイベントが発生した場合、指定された重大度レベル以上のメッセージが Trap として通知されます。重大度レベルで指定可能なパラメーターは以下となります（本設定例の場合、イベントログから Critical/Error/Warning メッセージが Trap 通知）。
0: None（デフォルト）
1: Critical
2: Error
3: Warning
4: Informational
5: Debug

■ SNMPv3、FOS v8.1.x ~FOS v8.2.x の場合

```
switch_1:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false]

SNMPV3 Password Encryption Enabled (true, t, false, f): [false]      (*1)

SNMPv3 user configuration(snmp user not configured in FOS user database
will have default VF context and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [1]
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (1..4) [4]
New Priv Passwd:
Verify Priv Passwd:
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (1..4) [2] 4
New Priv Passwd:
Verify Priv Passwd:
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]

SNMPv3 trap/inform recipient configuration:
Trap Recipient's IP address : [0.0.0.0] 192.168.0.30

Notify Type [TRAP(1)/INFORM(2)]: (1..1) [1]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
```

*1: パスワードの暗号化を、有効または無効にします。

■ SNMPv3、FOS v9.0.x 以降 v9.2.0 未満

```
                                        (*1)        (*2)          (*3)
switch:admin> snmpconfig --add snmpv3 -index 1 -user user -groupname ro
Committing configuration.....done.
G620:FID128:admin>
G620:FID128:admin>
G620:FID128:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false]                      (*4)

SNMPV3 Password Encryption Enabled (true, t, false, f): [false]        (*5)

SNMPv3 user configuration(snmp user not configured in FOS user database will
have default VF context and admin role as the default):
User (ro): [esfuser]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1                  (*5)
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (1..4) [2] 1    (*6)
New Priv Passwd:
Verify Priv Passwd:

SNMPv3 trap/inform recipient configuration:
Trap Recipient's IP address : [0.0.0.0] 192.168.0.30                   (*7)

Notify Type [TRAP(1)/INFORM(2)]: (1..1) [1]                            (*8)
UserIndex: (1..12) [1]
Trap recipient Severity level : (0..5) [0] 3                           (*9)
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
switch:admin>
```

*1: 設定を保存するインデックスとして 1~12 のいずれかの数値を指定します。

*2: SNMPv3 用のユーザー名を指定します。

*3: コミュニティーまたはユーザーに与えられるアクセス権を設定します。読み取り専用の場合は "ro" を、読み書き可能な場合は "rw" を指定します。

*4: SNMPv3 で Inform (Recipient へ受領確認要求) を使用する場合は、true を選択します。

*5: (*2) で入力したユーザーで使用する認証プロトコルを選択します。noAuth 以外を選択するとパスワードの入力を求められます。

*6: (*2) で選択したユーザーで使用する暗号方法を選択します。noPriv 以外を選択するとパスワードの入力を求められます。

*7: 通知の送信先となるサーバの IP アドレスを指定します。

*8: 通知の形式が INFORM か TRAP かを選択します。(*1) で false を選択した場合は、TRAP を選択してください。

*9: スイッチでイベントが発生した場合、指定された重大度レベル以上のメッセージが Trap として通知されます。重大度レベルで指定可能なパラメーターは以下となります（本設定例の場合、イベントログから Critical/Error/Warning メッセージが Trap 通知）。
0: None（デフォルト）
1: Critical

2: Error
3: Warning
4: Informational
5: Debug

■ FOS v9.2.0 以降

```
switch:admin> snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname ro
Committing configuration.....done.
switch:admin>
switch:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false]

SNMPV3 Password Encryption Enabled (true, t, false, f): [true]            (*1)

SNMPv3 user configuration(snmp user not configured in FOS user database will
have default VF context and admin role as the default):
User (ro): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)/SHA512(4)]: (1..4) [3]             (*2)
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]         (*3)

SNMPv3 trap/inform recipient configuration:
Trap Recipient's IP address : [0.0.0.0] 192.168.0.114

Notify Type [TRAP(1)/INFORM(2)]: (1..1) [1]
UserIndex: (1..12) [1]
Trap recipient Severity level : (0..5) [0] 3
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
```

*1: FOS v9.0 以降では、SNMP パスワード暗号化はデフォルトで有効です。

*2: SNMP v3 認証プロトコルである MD5 および SHA は非推奨です。そのため、設定中に以下のような警告メッセージが表示されます。
Warning: The authentication protocols MD5 and SHA are deprecated. Using SHA512 is recommended and required to upgrade to the next release.

*3: SNMP v3 プライバシープロトコル DES は非推奨です。そのため、設定中に以下のような警告メッセージが表示されます。
Warning: The Privacy protocol DES is deprecated.It is recommended to use AES.

2 以下のコマンドを使用して、SNMP マネージャーにテスト用 Trap を送信することが可能です。本コマンドは Trap 到達確認の目的でのみ使用してください。

```
switch_1:admin> snmptraps --send
Number of traps sent : 25
switch_1:admin>
```

以下、SNMP マネージャーに通知される Trap メッセージの例となります（本メッセージはテスト用のため、正しく表示されない場合があります）。

```
Info 2010/11/29 11:00:37 switch_1 SSC - Warm Start Trap
Info 2010/11/29 11:00:42 switch_1 SSC - Cold Start Trap
Info 2010/11/29 11:00:43 switch_1 SSC - Link Up Trap
Info 2010/11/29 11:00:43 switch_1 SSC - Link Down Trap
Info 2010/11/29 11:00:43 switch_1 SSC - Authentication Failure Trap
```

手順ここまで

F.3 拡張 MIB ファイルの登録

本装置の拡張 MIB は Fabric OS の版数ごとに用意されています。SNMP マネージャーに拡張 MIB を登録すると、対応したメッセージを参照しやすい形式で表示できます（ETERNUS SF Storage Cruiser は最新のパッチを適用することで、拡張 MIB が自動適用されます）。

備 考

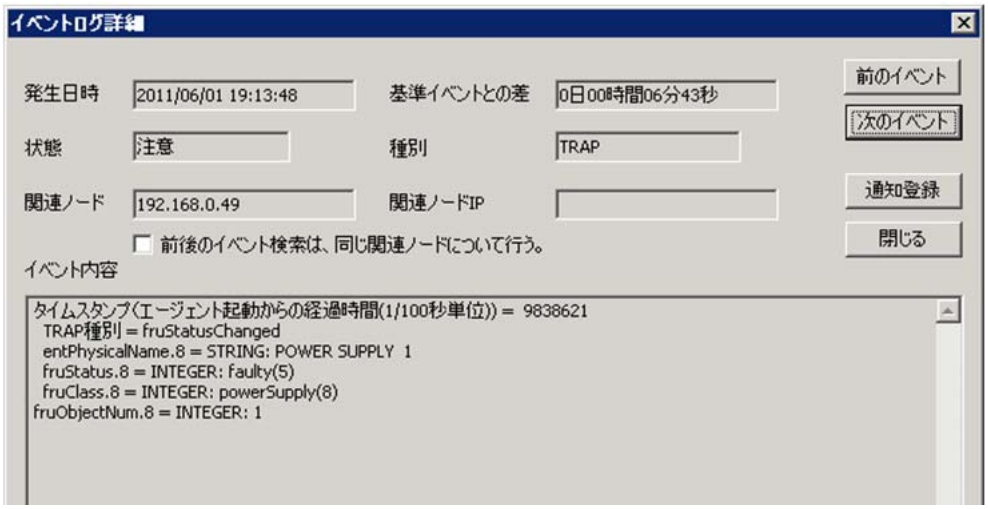
- MIB は、相互依存関係の順序で登録する必要があります。例えば SW.mib を登録する場合、事前に [Brocade-REG-MIB(BRCD_REG.mib)]、[Brocade-TC(BRCD_TC.mib)]、[FCMGMT-MIB(FA.mib)] の順序で登録する必要があります。詳細は、Fabric OS MIB Reference の MIB loading order の項、または各 MIB ファイル内の IMPORTS 文の指定を確認してください。
- SNMP マネージャーによっては、拡張 MIB の登録時にエラーとなるケースがあります。
  エラー原因／対処については、SNMP マネージャー側に確認してください。以下は、過去事例です。
  - 拡張 MIB 内で宣言されているオブジェクトの SYNTAX（データ型など）が、SNMP マネージャーで未サポートだった。
  - すでに SNMP マネージャーに同じ MIB が登録されており、重複登録を許可しない仕様だった。

F.4 Trap メッセージ

ハードウェア故障（電源／ FAN）やポートの Online / Offline などのイベント、重大度レベルに応じて通知されるイベントログのメッセージが Trap として送信されます。
以下に主な Trap を示します。詳細は、Fabric OS MIB Reference を確認してください。
ETERNUS SF Storage Cruiser の場合は、『ETERNUS SF Storage Cruiser イベント説明書』を参照してください。

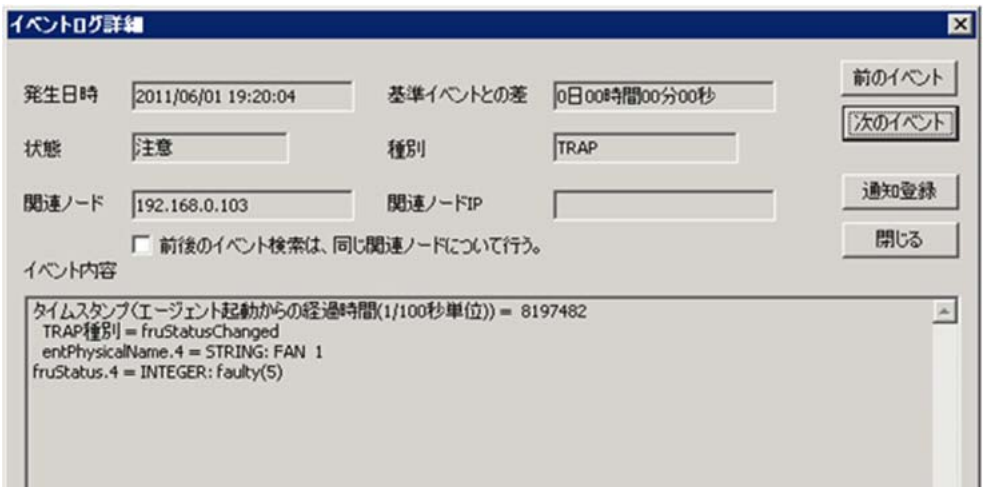
ハードウェア故障（電源 1）の Trap 例

対応 MIB ファイル：HA.mib



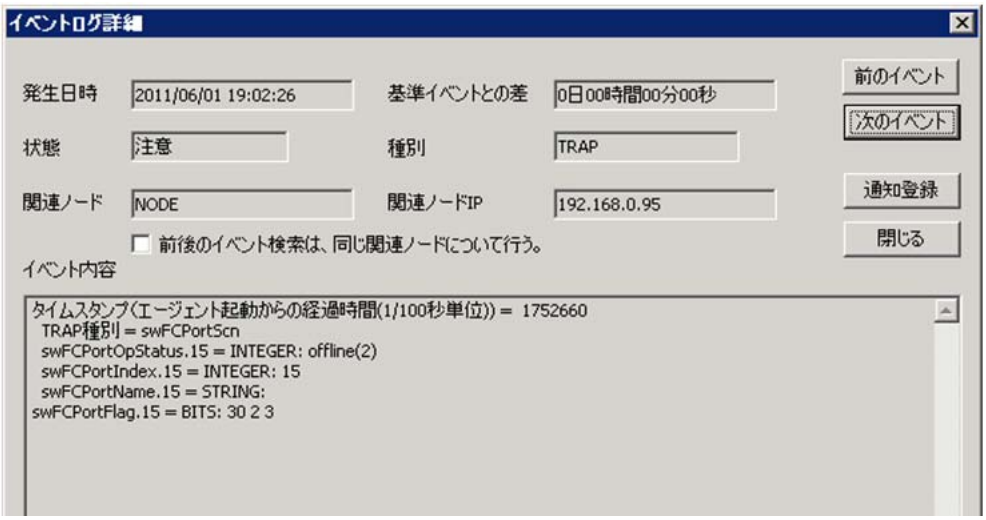
ハードウェア故障（FAN1）の Trap 例

対応 MIB ファイル：HA.mib



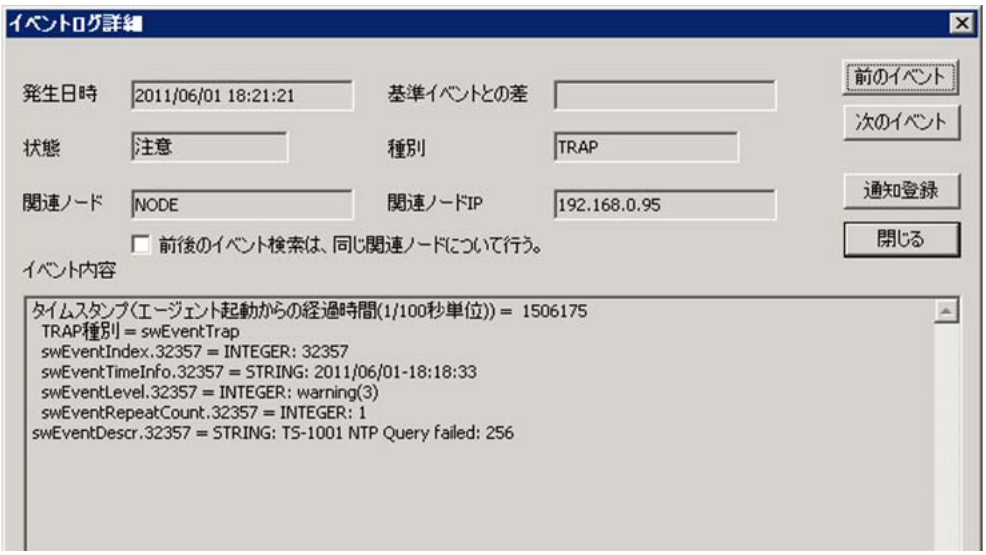
FC ポート（Port14）オフラインの Trap 例

対応 MIB ファイル：SW.mib



イベントログの Trap 例

該当 MIB ファイル：SW.mib



付録 G

追加ライセンスの発行／適用

スイッチにオプションライセンスを適用することで、様々な機能拡張を行うことが可能です。

G.1 事前確認（licenseshow, license --show / chassisshow）

手 順

1 以下のコマンドを使用して、装置情報（適用済みライセンス／ Serial No）を確認します。

■ FOS v9.0.0 未満（licenseshow コマンド）

```
switch_1:admin> licenseshow

<< 省略 >>

switch_1:admin> chassisshow

<< 省略 >>
Factory Serial Num:       ALJ0000G000
<< 省略 >>

switch_1:admin>
```

■ FOS v9.0.0 以降で G610（switch type170.5 以上）、G620（switch type 183）、G630（switch type 184）、G720、G730、X7-4、X7-8 の場合（license --show コマンド）

```
switch_1:admin> license --show
  License Id : 10:00:d8:1f:cc:18:de:f4
  License 1 :
  ----------------------------------------------------------------
    License serial number   : FOS-86-0-03-11365747
    License features        : Trusted FOS (TruFOS) Certificate
    Generation date         : 08/11/2023
    Expiry date             : 08/10/2024
  License 2 :
  ----------------------------------------------------------------
    License serial number   : FOS-19-0-04-10000756
    License features        : Extended Fabric
                              Trunking
                              FICON_CUP
                              Integrated Routing
                              Fabric Vision and IO Insight
    Generation date         : 05/15/2020
  License 3 :
  ----------------------------------------------------------------
    License serial number   : FOS-19-0-02-10000757
    License features        : Ports on Demand
    License Capacity        : 32
    Generation date         : 05/15/2020
```

■ FOS v9.0.0 以降で上記以外の機種の場合（license --show コマンド）

```
switch_1:admin> license --show
  License Id : 10:00:c4:f5:7c:9f:88:68
  License 1 :
  ----------------------------------------------------------------
    License serial number   : FOS-86-0-03-11365749
    License features        : Trusted FOS (TruFOS) Certificate
    Generation date         : 08/11/2023
    Expiry date             : 08/10/2024
  License 2 :
  ----------------------------------------------------------------
    License key             : M4S3JLYJHfBmS4AS4FD4tRFgJBSHFD9RYFFCZPEAEDKB
    License features        : Ports on Demand
    License Capacity        : 8
  License 3 :
  ----------------------------------------------------------------
    License key             : KBFCtEMCYYAWAJHftLKPSf7gfTSKFZ9ABS37R
    License features        : Extended Fabric
                              Trunking
                              Fabric Vision
```

手順ここまで

G.2 ライセンス発行

オプションライセンスを購入すると、トランザクションキーと呼ばれる 16 進数の ID が記載されたライセンス証書が届きます。本トランザクションキーとスイッチの WWN とともに Broadcom 社の Web
サイトから申請を行うと、専用のライセンスキーまたはファイルが発行されます。

備 考

ライセンス発行作業は、担当保守員が実施してください。

G.3 ライセンス適用（licenseadd / license --install）

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。

発行された専用のライセンスキーまたはファイルを装置に適用します。

手 順

1 以下のコマンドを使用して、スイッチにライセンスを適用します。

■ FOS v9.0.0 未満（ licenseadd コマンド）

```
licenseadd "XXXXXXXXXXXXXXXX"
```

コマンドの後に半角空白を入力し発行されたライセンスキーをコピー & ペーストしてください。
余計な空白や文字列、ライセンスオプションのライセンスシートに記載されているトランザクションキーなどを誤入力するとインストールに失敗します。

```
switch_1:admin> licenseadd "XXXXXXXXXXXXXXXX"
adding license-key [XXXXXXXXXXXXXXXX]          (*1)
switch_1:admin>
```

*1: インストールしたライセンスキーが表示されます。

■ FOS v9.0.0 以降で G610（switch type 170.5 以上）、G620（switch type 183）、G630（switch type 184）、G720、G730、X7-4、X7-8 の場合（license --install コマンド）

FTP サイトにアップロードされた xml ファイルをダウンロードし、ライセンスを適用します。FOS v9.1.1 以降の版数では、本手順の実施前に FTP を有効にし、実施後は FTP を無効に戻してください。有効／無効の方法については、「S.2 FTP・Non-secure syslog 有効／無効の設定手順」(P.139) を参照してください。

```
license --install -h XX.XXX.XX.XX -t XXX -u XXX -p XXXXXX -f /XXX/XXX/XXXX.xml
```

switch type は、switchshow コマンドで表示される switchType で確認できます。
ライセンスがファイル形式で発行されるため、必ず .xml の拡張子で格納場所を指定します。
パラメータ間の空白はすべて半角です。コマンド構文に余計な空白や文字列などを誤入力するとインストールに失敗します。

```
switch:admin> license --install -h 192.168.0.100 -t ftp -u xenon -p xenon -f /XML/
20200713165436714SW-CHASICLPODQ16-1.xml      (*1)
License Installed [FOS-19-0-01-10000690]     (*2)
```

*1: switch:admin> license --install -h 10.20.30.40 -t scp -u user -p testpwd -f /test/test1/test.xml
太字の文字列は環境によって異なります。

-h **10.20.30.40**：	サーバの IP アドレス
-t **scp**：	プロトコル（scp/ftp など）を指定します。
-u **user**：	サーバのユーザー名
-p **testpwd**：	サーバのパスワード
-f **/test/test1/text.xml**：	サーバのパスとファイルネーム。 ファイル名はダウンロードし格納した xml ファイルの名称です。ライセンスキー、ライセンス SN、トランザクションキーではありません。

*2: インストールされた xml ファイル形式のライセンス SN が表示されます。

■ FOS v9.0.0 以降で上記以外の機種の場合（license --install コマンド）

```
license --install -key XXXXXXXXXXXXXXXX
```

発行されたライセンスキーをコピー & ペーストしてください。ライセンスオプションのライセンスシートに記載されているトランザクションキーなどを誤入力するとインストールに失敗します。
必ず「-key」を入力してから、ライセンスキーをコピー & ペーストしてください。
パラメータ間の空白はすべて半角です。コマンド構文に余計な空白や文字列などを誤入力するとインストールに失敗します。

```
switch:admin> license --install -key abcxxxxxxxxxx
License Installed [abcxxxxxxxxxx] ]                (*1)
```

*1: インストールしたライセンスキーが表示されます。

手順ここまで

G.4 Dynamic Ports on Demand（DPOD）ライセンスの開放（licenseport --release / license --release -port）

Dynamic Ports on Demand では、ポートがオンラインになると reserve されるため、開放するには release の操作が必要です。

手 順

1 reserve されているポートを確認します。
以下の例では、Port 5 が開放されておらず、「(POD license not assigned or reserved yet)」が表示されません。

```
Switch:admin> switchshow
switchName: Switch
switchType: 170.0
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 1
switchId: fffc01
switchWwn: 10:00:c4:f5:7c:9f:78:28
zoning:  ON (cfg)
switchBeacon: OFF
HIF Mode: OFF

Index Port Address  Media Speed   State       Proto
==================================================
       .
       .
       .

   5   5   010500   --    N32   No_Module   FC
   6   6   010600   --    N32   No_Module   FC  (POD license not assigned or
reserved yet)
```

2 開放するポートを disable にします。

```
Switch:admin> portdisable 5
```

3 reserve されている Port 5 を開放します。

■ FOS v8.2.x まで

```
Switch:admin> licenseport --release 5     (*1)
```

*1: 連続する複数のポートを開放する場合は、以下のようにポート範囲を指定します。

```
Switch:admin> licenseport --release 0-23
```

■ FOS v9.0.x 以降

注 意

FOS v9.0.x 以降は licenseport --release コマンドは使用できません。license --release -port コマンドを使用してください。

```
switch:admin> license --release -port 5    (*2)
```

*2: 連続する複数のポートを開放する場合は、以下のようにポート範囲を指定します。

```
switch:admin> license --release -port 0-23
```

4 Port 5 が開放されていることを確認します。

```
G610_1_v810DVT:admin> switchshow
switchName: Switch
switchType: 170.0
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 1
switchId: fffc01
switchWwn: 10:00:c4:f5:7c:9f:78:28
zoning:  ON (cfg)
switchBeacon: OFF
HIF Mode: OFF

Index Port Address  Media Speed   State     Proto
==================================================
       .
       .
       .

   5  5    010500   --    N32   No_Module   FC  (POD license not assigned or
 reserved yet)
   6  6    010600   --    N32   No_Module   FC  (POD license not assigned or
 reserved yet)
```

5 開放したポートを使用する場合は、ポートを enable にします。

```
Switch:admin> portenable 5
```

手順ここまで

付録 H

Virtual Fabrics 設定

Virtual Fabrics とは、物理スイッチを複数のファブリック要素へと論理的に分割を行う機能です。分割されたファブリックは論理スイッチと呼ばれ、各論理スイッチは独立したスイッチとして機能します。

H.1 事前確認（fosconfig）

手 順

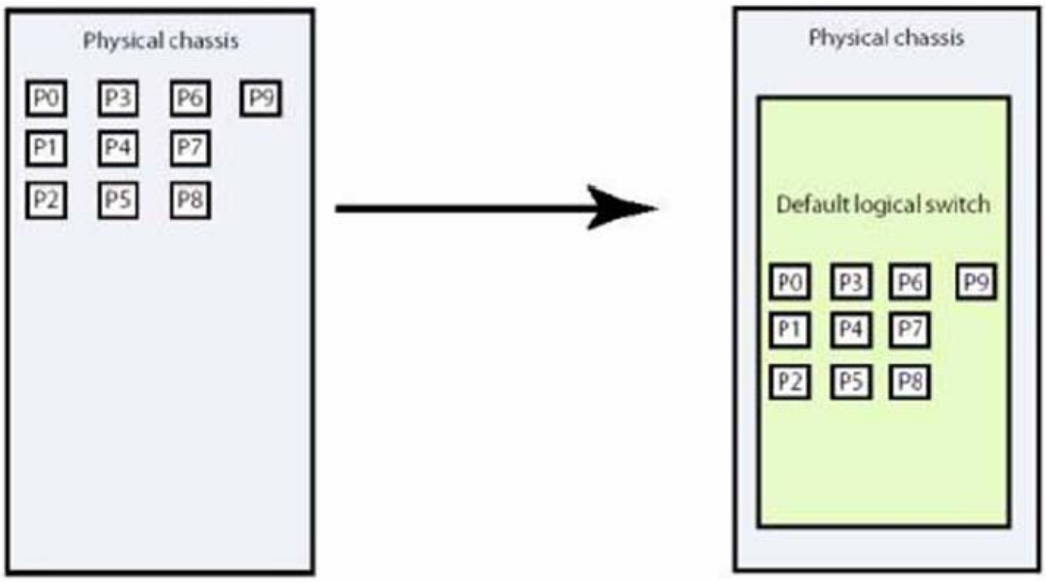
1 以下のコマンドを使用して、Virtual Fabrics の設定を確認します。

```
switch_1:admin> fosconfig --show
FC Routing service: disabled
iSCSI service: Service not supported on this Platform
iSNS client service: Service not supported on this Platform
Virtual Fabric: disable
switch_1:admin>
```

手順ここまで

H.2 Virtual Fabrics の有効化（fosconfig）

Virtual Fabrics 機能を有効にすると、単一の論理スイッチが作成されます。この論理スイッチは Default logical switch と呼ばれ、すべてのポートが割り当てられ、カスケード接続（E-port 接続）／装置直接接続（F-port 接続）は共にサポートされます。



Virtual Fabrics 無効時　　Virtual Fabrics 有効時

手 順

1 以下のコマンドを使用して、Virtual Fabrics を有効にします。
装置が再起動します。

```
switch:admin> fosconfig --enable vf
WARNING: This is a disruptive operation that requires a reboot to take effect.
All EX ports will be disabled upon reboot.
Enabling VF will cause other non-default admin accounts to gain chassis admin
role permissions if default admin account is disabled.
Would you like to continue [Y/N]: Y
VF has been enabled.  Your system is being rebooted.
Rebooting! Thu Dec 28 19:11:32 JST 2023

Broadcast message from admin@switch_1 (pts/1) (Thu Dec 28 19:11:32 2023):

The system is going down for reboot NOW!
```

注 意

FOS v9.2.0 以降では、デフォルトの管理者アカウントが無効な場合に Virtual Fabrics を有効にすると、管理者権限を持つデフォルト以外のすべてのアカウントに自動的にシャーシ管理者権限が割り当てられます。
シャーシ管理者権限を継続して使用しない場合は、権限を無効にしてください。デフォルトの管理者アカウントが有効な場合は、対処の必要はありません。

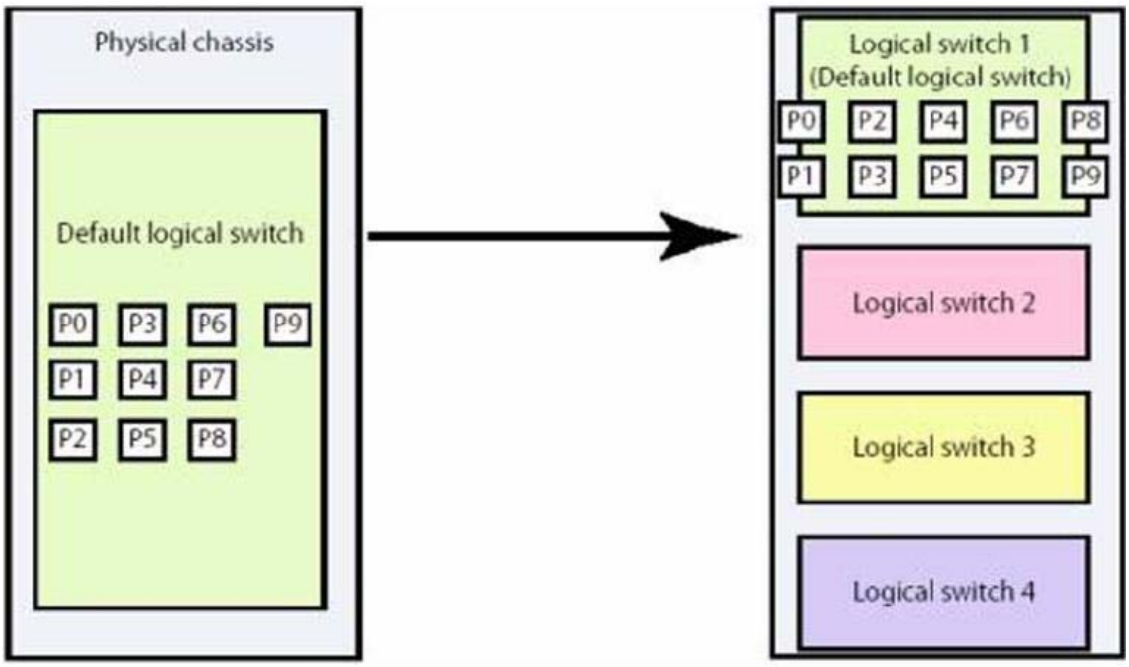
2 以下のコマンドを使用して、Virtual Fabrics の設定を確認します。

```
Switch:FID128:admin> fosconfig --show
FC Routing service:             disabled
Virtual Fabric:                 enabled
```

手順ここまで

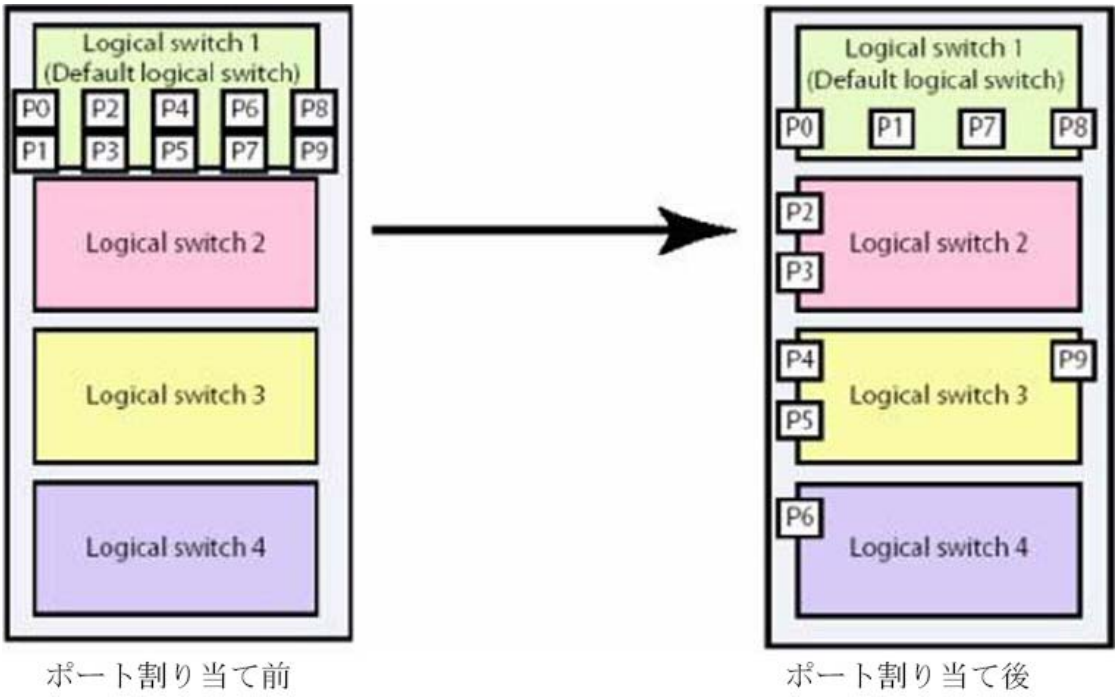
H.3 論理スイッチの作成とポート割り当て（lscfg）

論理スイッチを新たに作成する際、物理スイッチ内で固有となるファブリック ID（FID）を割り当てます。作成された論理スイッチはポート未割り当ての論理スイッチとして作成され、最大 8 つまでの論理スイッチを作成できます。また、Logical switch として作成された論理スイッチでカスケード接続（E-port 接続）／装置直接接続（F-port 接続）は共にサポートされます。



論理スイッチの作成前　　論理スイッチの作成後

また、各ポートは 1 つの論理スイッチに属するように割り当てることができます。複数の論理スイッチで 1 つのポートを共用して割り当てることはできません。



ポート割り当て前　　ポート割り当て後

手 順

1 以下のコマンドを使用して、論理スイッチの作成とポート割り当てを行います。

- 例：Logical switch（ファブリック ID：10）に slot7 に属するすべてのポートを割り当て

```
switch:FID128:admin> lscfg --create 10
A Logical switch with FID 10 will be created with default configuration.
Would you like to continue [y/n]?: y
About to create switch with fid=10. Please wait...
Logical Switch with FID (10) has been successfully created.

Logical Switch has been created with default configurations.
Please configure the Logical Switch with appropriate switch
and protocol settings before activating the Logical Switch.
switch_1:FID128:admin> lscfg --config 10 -slot 7
This operation requires that the affected ports be disabled.
Would you like to continue [y/n]?: y
Making this configuration change. Please wait...
Configuration change successful.
Please enable your ports/switch when you are ready to continue.
switch_1:FID128:admin>
```

- 例：Base switch（ファブリック ID：127）に slot1 のポート 0 ～ 7、slot2 のポート 20 を割り当て

```
switch_1:FID128:admin> lscfg --create 127 -base
Creation of a base switch requires that the proposed new base switch on
this system be disabled.
Would you like to continue [y/n]?: y
About to create switch with fid=127. Please wait...
Logical Switch with FID (127) has been successfully created.
Logical Switch has been created with default configurations.
Please configure the Logical Switch with appropriate switch
and protocol settings before activating the Logical Switch.
switch_1:FID128:admin> lscfg --config 127 -slot 1 -port 0-7
This operation requires that the affected ports be disabled.
Would you like to continue [y/n]?: y
Making this configuration change. Please wait...
Configuration change successful.
Please enable your ports/switch when you are ready to continue.
switch_1:FID128:admin> lscfg --config 127 -slot 2 -port 20
This operation requires that the affected ports be disabled.
Would you like to continue [y/n]?: y
Making this configuration change. Please wait...
Configuration change successful.
Please enable your ports/switch when you are ready to continue.
switch_1:FID128:admin>
```

- 例：作成済み論理スイッチ／割り当てポート一覧の確認

```
switch_1:FID128:admin> lscfg --show
Created switches: 128(ds) 127(bs) 10
Slot 1 2 3 4 5 6 7 8
-----------------------------------------------------
Port
0 | 127 | 128 | 128 | | | 128 | 10 | 128 |
1 | 127 | 128 | 128 | | | 128 | 10 | 128 |
2 | 127 | 128 | 128 | | | 128 | 10 | 128 |
3 | 127 | 128 | 128 | | | 128 | 10 | 128 |
4 | 127 | 128 | 128 | | | 128 | 10 | 128 |
5 | 127 | 128 | 128 | | | 128 | 10 | 128 |

<< 省略 >>
```

手順ここまで

H.4 論理スイッチ名の設定（setcontext / switchname）

手 順

1 以下のコマンドを使用して、論理スイッチにログイン後、スイッチ名を設定します。

```
switch_1:FID128:admin> setcontext 10
switch_1_10:FID10:admin> switchname sw_01_10
sw_01_10:FID10:admin> setcontext 128
switch_1:FID128:admin>
```

手順ここまで

H.5 論理スイッチのドメイン ID 設定（setcontext / configure）

手 順

1 以下のコマンドを使用して、論理スイッチにログイン後、ドメイン ID を設定します。

```
switch_1:FID128:admin> setcontext 10
sw_01_10:FID10:admin> switchdisable
sw_01_10:FID10:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no] yes
Domain: (1..239) [1] 2

<< 省略 >>

sw_01_10:FID10:admin> switchenable
sw_01_10:FID10:admin> setcontext 128
switch_1:FID128:admin>
```

手順ここまで

H.6 論理スイッチの状態の確認（switchshow）

手 順

1 以下のコマンドを使用して、論理スイッチにログイン後、スイッチの状態を確認します。

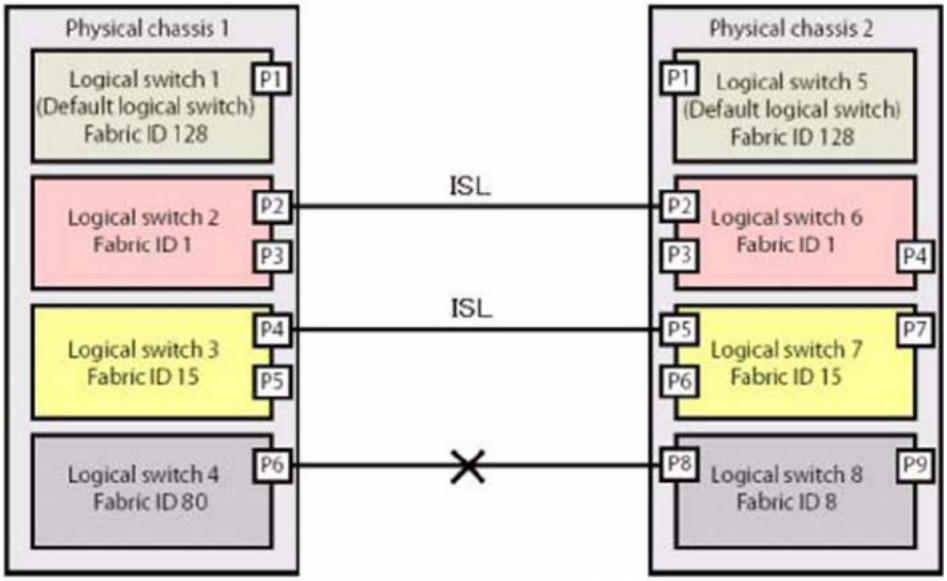
- 例：論理スイッチ 100 に 0-3 ポートを割り当て（FOS v7.4.0b）

```
switch:admin> setcontext 100

switch_100:FID100:admin> switchshow
switchName:     switch
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Principal
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:50:eb:1a:7a:6f:45
zoning:         OFF
switchBeacon:   OFF
FC Router:      OFF
HIF Mode:       OFF
Allow XISL Use: ON
LS Attributes:  [FID: 100, Base Switch: No, Default Switch: No, Address
Mode 0]

Index Port Address Media Speed       State    Proto
==================================================
   0    0   010000   id    N16      No_Light    FC  Disabled
   1    1   010100   id    N16      No_Light    FC  Disabled
   2    2   010200   id    N16      No_Light    FC  Disabled
```

手順ここまで

H.7 論理スイッチの接続

論理スイッチは、同じファブリック ID の Logical switch/Default Logical switch を ISL（DISL）で接続できます。異なるファブリック ID を持つ論理スイッチ間での接続はできません。



H.8 その他の設定

システム要件に応じて、各種設定（Zone、ポート設定など）を行ってください。

付録 I

エクステンション設定

I.1 FCIP トンネリング・IP エクステンショントンネリングおよび FC ルーティングのセットアップ

FCIP トンネリング・IP エクステンショントンネリングおよび FC ルーティング機能を使用する際は、『Brocade series, ETERNUS SN200 series ユーザーズガイド 導入／運用（拡張）編』を参照してください。

付録 J
FCoE 設定

J.1 FCoE のセットアップ

FCoE 機能を使用する際は、『ファイバチャネルスイッチ FCoE Fabric OS 管理者ガイド Fabric OS v6.3.x 用』を参照してください。

付録 K

Zone 方式と設定変更

Zone とは接続されたデバイス間でアクセス制御を行う機能で、多数のサーバ／ストレージを接続した場合でもセキュリティを高く保つことができます。また、装置の再起動時などに発生する RSCN を局所化することができ、システム影響を Zone 設定された範囲内にとどめることができます。

K.1 Zone 方式

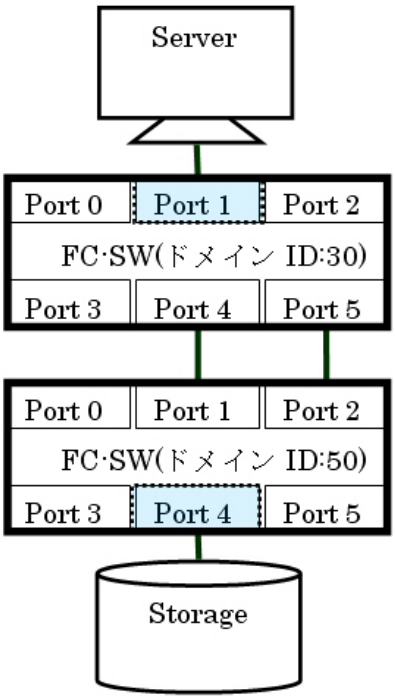
Zone 方式として、スイッチのドメイン ID とポートインデックスの組み合わせで指定する Port Zoning と、デバイスの WWN で指定する WWN Zoning の 2 種類があります。

備 考

ポートインデックスは **switchShow** コマンドで確認します。ボックスタイプのポートインデックスは、ポート番号と同一です。ダイレクタタイプのポートインデックスは、「付録 O ダイレクタタイプのポートインデックス一覧」(P.110) を参照してください。

K.1.1 Port Zoning

スイッチのドメイン ID とポートインデックスの組み合わせで Zone を作成します。なお、ポートの指定はサーバ／ストレージが接続されたポートのみで行い、カスケード接続されたポートに対して行う必要はありません。



設定例

```
switch:admin> zonecreate "pz1","30,1;50,4"
switch:admin> cfgcreate "portzone","pz1"
switch:admin> cfgsave
switch:admin> cfgenable "portzone"
```

- メリット

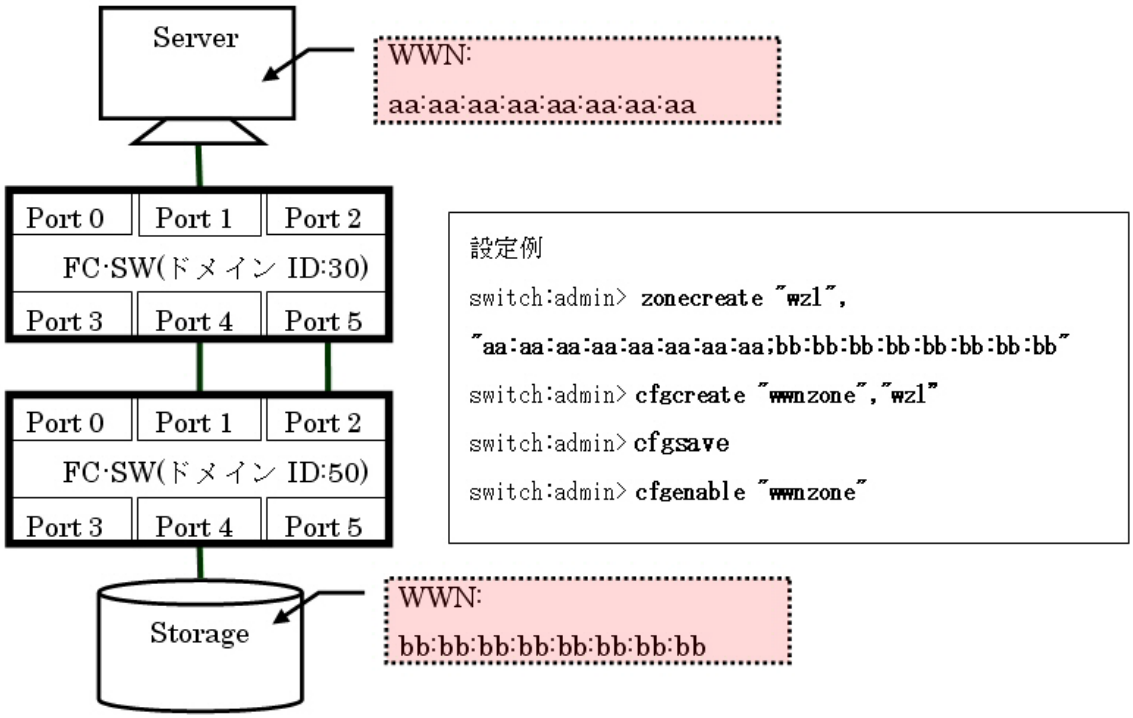
  サーバの HBA やストレージを交換しても Zone を再設定する必要がない。

- デメリット

  ポート障害や障害の切り分け時にポートを差し替えができない（新たに Zone 設定が必要）。

K.1.2 WWN Zoning

サーバ／ストレージの WWN の組み合わせで、Zone を作成します。



- メリット

  WWN の組み合わせで Zone を行っているため、ポート障害や障害の切り分けなどの際、既存の Zone 設定のままポートを差し替えることができる。

- デメリット

  サーバの HBA やストレージの交換を行うと WWN が変わるため、その都度 Zone を修正する必要がある。

K.2 Zone 設定の確認／変更

Zone 設定の追加／削除を I/O アクセス中のデバイスへ行うと、I/O に影響があります。I/O アクセスが一時的に中断した場合でも、通常はサーバ側のリトライ処理により I/O アクセスが停止することはありません。ただし、テープバックアップ処理中などリトライ処理に対応しない状況では、業務を停止した状態で実施してください。

K.2.1 事前確認（cfgshow）

手 順

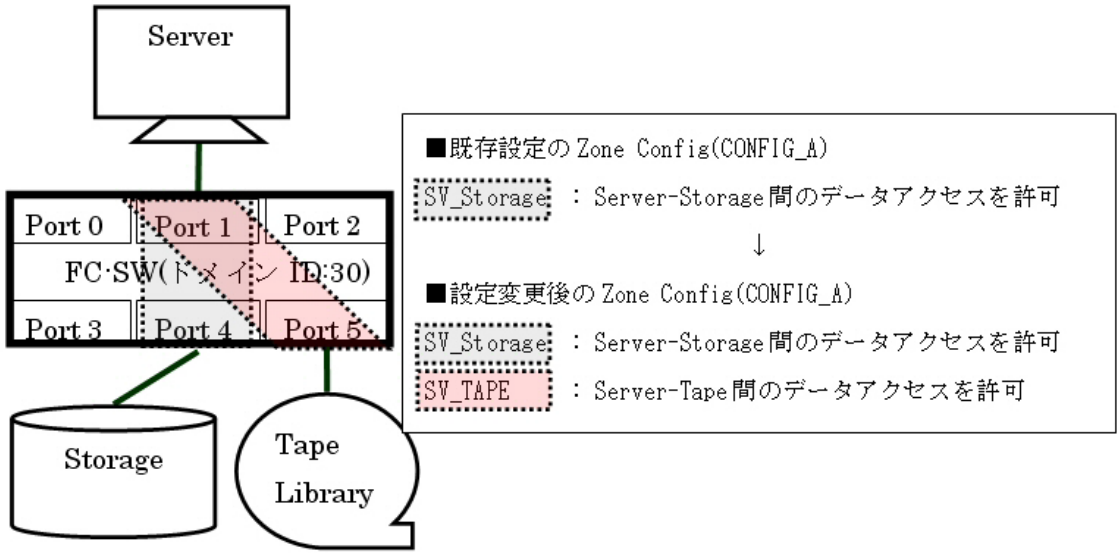
1 以下のコマンドを使用して、定義されている Zone 情報と有効な Zone 情報を確認します。

```
switch_1:admin> cfgshow
Defined configuration:
 cfg:    CONFIG_A
                 SV_Storage
 zone:   SV_Storage
                 30,1; 30,4

Effective configuration:
 cfg:    CONFIG_A
 zone:   SV_Storage
                 30,1
                 30,4
switch_1:admin>
```

手順ここまで

K.2.2 Zone 設定の追加（zonecreate / cfgadd）

Server-Storage 間で Zone 設定済みの環境に、新たに Tape Library を追加した際の Zone 設定の追加手順を示します。



手 順

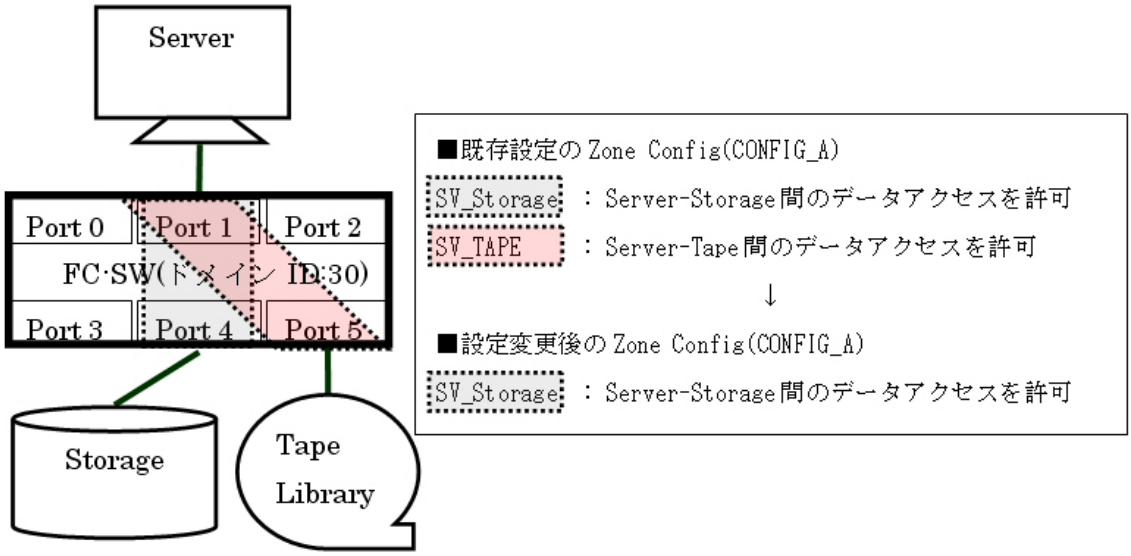
1 以下のコマンドを使用して、既存の Zone Config に Zone を追加します。

```
switch:admin> zonecreate "SV_TAPE","30,1;30,5"
switch:admin> cfgadd "CONFIG_A","SV_TAPE"
switch:admin> cfgsave
switch:admin> cfgenable "CONFIG_A"
```

手順ここまで

K.2.3 Zone 設定の一部削除（zonedelete / cfgremove）

Server-Tape 間に設定した Zone 設定を削除し、Server-Storage 間の Zone 設定のみを適用する手順を示します。



手 順

1 以下のコマンドを使用して、既存の Zone Config から Zone を削除します。

```
switch:admin> cfgremove "CONFIG_A","SV_TAPE"
switch:admin> zonedelete "SV_TAPE"
switch:admin> cfgsave
switch:admin> cfgenable "CONFIG_A"
```

手順ここまで

K.2.4 Zone 設定の初期化（cfgdisable / cfgclear）

本設定を行うと既存の Zone Config がすべて削除されます。新規に Zone 設定を行いたい場合に設定してください。

手 順

1 以下のコマンドを使用して、適用している Zone Config を無効にします。

```
switch:admin> cfgdisable
You are about to disable zoning configuration. This
action will disable any previous zoning configuration enabled.
Do you want to disable zoning configuration? (yes, y, no, n): [no] y
switch:admin>
```

2 以下のコマンドを使用して、設定済みの Zone Config をすべて削除します。

```
switch:admin> cfgclear
The Clear All action will clear all Aliases, Zones, FA Zones
and configurations in the Defined configuration.
cfgSave may be run to close the transaction or cfgTransAbort
may be run to cancel the transaction.
Do you really want to clear all configurations?  (yes, y, no, n): [no] y
switch:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only?  (yes, y, no, n): [no]
y
Updating flash ...
switch:admin>
```

3 以下のコマンドを使用して、設定済みの Zone Config がすべて削除されたことを確認します（装置環境に応じて、以下のように出力結果が異なる場合があります）。

```
switch:admin> cfgshow
Defined configuration:
 no configuration defined

Effective configuration:
 no configuration in effect

switch:admin>
```

```
switch:admin> cfgshow
Defined configuration:

Effective configuration:
No Effective configuration: (No Access)

switch:admin>
```

手順ここまで

付録 L

設定情報の退避／復元

設定情報の退避は、設定変更を行ったすべてのスイッチで実施してください。

備 考

ほかのスイッチとカスケード接続を行っている場合は、設定情報ファイルを保存していなくても Zone 設定のみ伝搬できます。

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。FOS v9.1.1 以降の版数では、本手順の実施前に FTP を有効にし、実施後は無効に戻してください。有効／無効の方法については、「S.2 FTP・Non-secure syslog 有効／無効の設定手順」(P.139) を参照してください。

L.1 設定情報の退避（configupload）

手 順

1 以下のコマンドを使用して、スイッチの設定情報を FTP サーバに保存します。

```
switch_1:admin> configupload                                    (*1)
Protocol (scp, ftp, local) [ftp]: ftp
Server Name or IP Address [host]: 192.168.0.50
User Name [user]: ftpuser
File Name [config.txt]: /switch/20110523_switch_1_config.txt
Section (all|chassis [all]): all
Password:xxxxxxxxxx                                             (*2)

configUpload complete: All config parameters are uploaded
switch_1:admin>
```

*1: FTP サーバの IP アドレス／ FTP ユーザー名／ FTP パスワード／転送ファイル名は、接続環境に応じて指定してください。

*2: パスワードは実際には表示されません。

2 Virtual Fabric 構成を設定している場合は、別途「-vf」オプションを指定して、スイッチの設定情報を FTP サーバに保存を行います。保存するファイル名は、手順 1 で保存したファイル名と重複しないように注意してください。

```
Switch:admin> configupload -vf                                    (*1)
Protocol (scp, ftp, sftp, local) [ftp]: ftp
Server Name or IP Address [host]: 192.168.0.XX
User Name [user]: ftpuser
Path/Filename [<home dir>/config.txt]: CONFIG/configupload/vf-conf_BR7840.txt
Password:

configUpload complete: VF config parameters uploaded
```

*1: FTP サーバの IP アドレス／ FTP ユーザー名／ FTP パスワード／転送ファイル名は、接続環境に応じて指定してください。

手順ここまで

L.2 設定情報の復元（configdownload）

手 順

1 以下のコマンドを使用して、FTP サーバに保存した設定情報ファイルをスイッチに適用します。

注 意

- Virtual Fabric 構成を設定している場合は、設定情報ファイルをスイッチに適用する前に「-vf」オプションを指定して、Virtual Fabric の設定情報を適用します。
  本コマンドを実行した場合、スイッチは自動で再起動されます。

```
Switch:admin> configdownload -vf
Protocol (scp, ftp, sftp, local) [ftp]: ftp
Server Name or IP Address [host]: 192.168.0.XX
User Name [user]: ftpuser
Path/Filename [<home dir>/config.txt]: CONFIG/configupload/
vf-conf_BR7840.txt

<<省略>>

  Do you want to continue [y/n]: y
Password:
configDownload complete : VF config parameters are downloaded
Connection closed by foreign host.
```

- **configdownload** コマンドでは、以下の設定情報は FOS の版数によって引き継がれない場合があります。引き継がれる設定は版数によって異なるため、確認が必要です。
  - スイッチ名の設定
  - 装置パスワード
  - IP アドレス設定
  - 管理 LAN ポート設定
  - NTP サーバとの時刻同期設定
  - 時刻の設定

```
switch_1:admin> switchdisable                                          (*1)
switch_1:admin> configdownload                                         (*2)
Protocol (scp, ftp, sftp, local) [ftp]: ftp
Server Name or IP Address [host]: 192.168.0.50
User Name [user]: ftpuser
Path/Filename [<home dir>/config.txt]: /switch/20110523_switch_1_config.txt
Section (all|chassis|switch [all]): all

<< 省略 >>

  Do you want to continue [y/n]: y
Password:ftppassword

<< 省略 >>

configDownload complete: All selected config parameters are downloaded
switch_1:admin> switchenable
switch_1:admin> reboot                                                 (*3)
```

*1: 論理スイッチが存在する場合は、**chassisdisable** コマンドを使用してください。**switchdisable** コマンドを使用する場合は、各論理スイッチに対して **switchdisable** コマンドを実施してください。

*2: FTP サーバの IP アドレス／ FTP ユーザー名／ FTP パスワード／転送ファイル名は、接続環境に応じて指定してください。

*3: 設定情報の復元後は、装置の再起動が必須です。

手順ここまで

付録 M

ファームウェアの確認／適用

最新のファームウェアをFTPサーバに格納したうえでファイバチャネルスイッチにダウンロードすると、最新のファームウェアを適用できます。
通常は、担当保守員がファームウェアを適用します。

M.1 事前確認（firmwareshow）

手 順

1 以下のコマンドを使用して、スイッチのファームウェア版数を確認します。

```
switch_1:admin> firmwareshow
Appl Primary/Secondary Versions
------------------------------------------
FOS v7.3.0c
    v7.3.0c
switch_1:admin>
```

手順ここまで

M.2 ファームウェアの適用（firmwaredownload / firmwaredownloadstatus）

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。FOS v9.1.1 以降の版数では、本手順の実施前に FTP を有効にし、実施後は無効に戻してください。有効／無効の方法については、「S.2 FTP・Non-secure syslog 有効／無効の設定手順」(P.139) を参照してください。
FOS を v9.1.1 以降にアップデートする場合は、ファームウェアアップデート後に「付録 S Secure Mode」(P.132) を参考に、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP を無効にしてください。

手 順

1 以下のコマンドを使用して、スイッチにファームウェアを適用します。

備 考

本コマンドは、FTP サーバ配備したファームウェアをスイッチにダウンロードします。

```
switch_1:admin> firmwaredownload                                    (*1)
Server Name or IP Address: 192.168.0.50
User Name: ftpuser
File Name: /work/v7.3.0c/release.plist
Network Protocol(1-auto-select, 2-FTP, 3-SCP) [1]: 2
Password: ftppassword

<< 省略 >>

Do you want to continue (Y/N) [Y]: Y

<< 省略 >>

switch_1:admin>
```

*1: FTP サーバの IP アドレス／ FTP ユーザー名／ FTP パスワード／転送ファイル名は、接続環境に応じて指定してください。また、版数によって転送ファイル名であるファームウェア名称に装置クラスが付くため注意が必要です。

2 以下のコマンドを使用して、ファームウェアダウンロードのステータスを確認し、正常に終了したことを確認します。

```
switch_1:admin> firmwaredownloadstatus
[1]: Mon Jun  6 14:54:26 2011
Firmware is being downloaded to the switch. This step may take up to 30 minutes.

[2]: Mon Jun  6 14:58:45 2011
Firmware has been downloaded to the secondary partition of the switch.

[3]: Mon Jun  6 15:01:12 2011
The firmware commit operation has started. This may take up to 10 minutes.

[4]: Mon Jun  6 15:03:59 2011
The commit operation has completed successfully.

[5]: Mon Jun  6 15:03:59 2011
Firmwaredownload command has completed successfully. Use firmwareshow to
verify the firmware versions.

switch_1:admin>
```

手順ここまで

付録 N

装置ログ採取

装置トラブルが発生した場合、**supportshow / supportsave** コマンドでスイッチが保持するシステム情報／ログ／トレースなどのテクニカルサポート情報を一括採取してください。障害調査の際は、**supportsave** コマンドで収集したスイッチのログが必要です。

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。FOS v9.1.1 以降の版数では、本手順の実施前に FTP を有効にし、実施後は無効に戻してください。有効／無効の方法については、「S.2 FTP・Non-secure syslog 有効／無効の設定手順」(P.139) を参照してください。

N.1 装置ログ一括採取（supportsave）

手 順

1 以下のコマンドを使用して、装置の情報を一括採取します。

備 考

本コマンドは、一括収集したスイッチのログを FTP サーバにアップロードします。

```
switch_1:admin> supportsave                                    (*1)

<< 省略 >>

OK to proceed? (yes, y, no, n): [no] y

Host IP or Host Name: 192.168.0.50
User Name: ftpuser
Password:ftppassword
Protocol (ftp or scp): ftp
Remote Directory: /work/

<< 省略 >>

switch_1:admin>
```

*1: FTP サーバの IP アドレス／ FTP ユーザー名／ FTP パスワード／転送ファイル名は接続環境に応じて指定してください。

手順ここまで

N.2 装置イベントログ採取（errdump）

手 順

1 以下のコマンドを使用して、装置のイベントログを出力します。

```
switch_1:admin> errdump -a

<< 省略 >>

switch_1:admin>
```

手順ここまで

N.3 装置センサー情報（sensorshow）

手 順

1 以下のコマンドを使用して、装置の温度／ FAN ／電源の状態を出力します。

```
switch_1:admin> sensorshow
sensor  1: (Temperature) is Ok, value is 32 C
sensor  2: (Temperature) is Ok, value is 31 C
sensor  3: (Temperature) is Ok, value is 33 C
sensor  4: (Fan         ) is Ok,speed is 5869 RPM
sensor  5: (Fan         ) is Ok,speed is 5921 RPM
sensor  6: (Fan         ) is Ok,speed is 6081 RPM
sensor  7: (Power Supply) is Ok
switch_1:admin>
```

手順ここまで

付録 O

ダイレクタタイプのポートインデックス一覧

ボックスタイプのポートインデックスはポート番号と同一ですが、ダイレクタタイプのポートインデックスはポート番号と同一とは限りません。ポートインデックスは **switchShow** コマンドで確認できます。

表 O.1　DCX 8510-8 ポートインデックス一覧

ポートインデックスは、すべてのタイプのブレードで共通です。

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	63	783	799	815	831					847	863	879	895
	62	782	798	814	830					846	862	878	894
	61	781	797	813	829					845	861	877	893
	60	780	796	812	828					844	860	876	892
	59	779	795	811	827					843	859	875	891
	58	778	794	810	826					842	858	874	890
	57	777	793	809	825					841	857	873	889
	56	776	792	808	824					840	856	872	888
	55	775	791	807	823					839	855	871	887
	54	774	790	806	822					838	854	870	886
	53	773	789	805	821					837	853	869	885
	52	772	788	804	820					836	852	868	884
	51	771	787	803	819					835	851	867	883
	50	770	786	802	818					834	850	866	882
	49	769	785	801	817					833	849	865	881
	48	768	784	800	816					832	848	864	880
	47	271	287	303	319					335	351	367	383
	46	270	286	302	318					334	350	366	382
	45	269	285	301	317					333	349	365	381
	44	268	284	300	316					332	348	364	380
	43	267	283	299	315					331	347	363	379
	42	266	282	298	314					330	346	362	378
	41	265	281	297	313					329	345	361	377
	40	264	280	296	312					328	344	360	376

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	39	263	279	295	311					327	343	359	375
	38	262	278	294	310					326	342	358	374
	37	261	277	293	309					325	341	357	373
	36	260	276	292	308					324	340	356	372
	35	259	275	291	307					323	339	355	371
	34	258	274	290	306					322	338	354	370
	33	257	273	289	305					321	337	353	369
	32	256	272	288	304					320	336	352	368
	31	143	159	175	191					207	223	239	255
	30	142	158	174	190					206	222	238	254
	29	141	157	173	189					205	221	237	253
	28	140	156	172	188					204	220	236	252
	27	139	155	171	187					203	219	235	251
	26	138	154	170	186					202	218	234	250
	25	137	153	169	185					201	217	233	249
	24	136	152	168	184					200	216	232	248
	23	135	151	167	183					199	215	231	247
	22	134	150	166	182					198	214	230	246
	21	133	149	165	181					197	213	229	245
	20	132	148	164	180					196	212	228	244
	19	131	147	163	179					195	211	227	243
	18	130	146	162	178					194	210	226	242
	17	129	145	161	177					193	209	225	241
	16	128	144	160	176					192	208	224	240
	15	15	31	47	63					79	95	111	127
	14	14	30	46	62					78	94	110	126
	13	13	29	45	61					77	93	109	125
	12	12	28	44	60					76	92	108	124
	11	11	27	43	59					75	91	107	123
	10	10	26	42	58					74	90	106	122
	9	9	25	41	57					73	89	105	121
	8	8	24	40	56					72	88	104	120
	7	7	23	39	55					71	87	103	119
	6	6	22	38	54					70	86	102	118

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	5	5	21	37	53					69	85	101	117
	4	4	20	36	52					68	84	100	116
	3	3	19	35	51					67	83	99	115
	2	2	18	34	50					66	82	98	114
	1	1	17	33	49					65	81	97	113
	0	0	16	32	48					64	80	96	112

表 O.2　DCX 8510-4 ポートインデックス一覧

ポートインデックスは、すべてのタイプのブレードで共通です。

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	63	63	127					191	255
	62	62	126					190	254
	61	61	125					189	253
	60	60	124					188	252
	59	59	123					187	251
	58	58	122					186	250
	57	57	121					185	249
	56	56	120					184	248
	55	55	119					183	247
	54	54	118					182	246
	53	53	117					181	245
	52	52	116					180	244
	51	51	115					179	243
	50	50	114					178	242
	49	49	113					177	241
	48	48	112					176	240
	47	47	111					175	239
	46	46	110					174	238
	45	45	109					173	237
	44	44	108					172	236
	43	43	107					171	235
	42	42	106					170	234
	41	41	105					169	233
	40	40	104					168	232
	39	39	103					167	231
	38	38	102					166	230
	37	37	101					165	229
	36	36	100					164	228
	35	35	99					163	227
	34	34	98					162	226
	33	33	97					161	225
	32	32	96					160	224

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	31	31	95					159	223
	30	30	94					158	222
	29	29	93					157	221
	28	28	92					156	220
	27	27	91					155	219
	26	26	90					154	218
	25	25	89					153	217
	24	24	88					152	216
	23	23	87					151	215
	22	22	86					150	214
	21	21	85					149	213
	20	20	84					148	212
	19	19	83					147	211
	18	18	82					146	210
	17	17	81					145	209
	16	16	80					144	208
	15	15	79					143	207
	14	14	78					142	206
	13	13	77					141	205
	12	12	76					140	204
	11	11	75					139	203
	10	10	74					138	202
	9	9	73					137	201
	8	8	72					136	200
	7	7	71					135	199
	6	6	70					134	198
	5	5	69					133	197
	4	4	68					132	196
	3	3	67					131	195
	2	2	66					130	194
	1	1	65					129	193
	0	0	64					128	192

表 O.3　Brocade X6-8 ポートインデックス一覧

ポートインデックスは、すべてのタイプのブレードで共通です。

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	47			271	287	303	319			335	351	367	383
	46			270	286	302	318			334	350	366	382
	45			269	285	301	317			333	349	365	381
	44			268	284	300	316			332	348	364	380
	43			267	283	299	315			331	347	363	379
	42			266	282	298	314			330	346	362	378
	41			265	281	297	313			329	345	361	377
	40			264	280	296	312			328	344	360	376
	39			263	279	295	311			327	343	359	375
	38			262	278	294	310			326	342	358	374
	37			261	277	293	309			325	341	357	373
	36			260	276	292	308			324	340	356	372
	35			259	275	291	307			323	339	355	371
	34			258	274	290	306			322	338	354	370
	33			257	273	289	305			321	337	353	369
	32			256	272	288	304			320	336	352	368
	31			143	159	175	191			207	223	239	255
	30			142	158	174	190			206	222	238	254
	29			141	157	173	189			205	221	237	253
	28			140	156	172	188			204	220	236	252
	27			139	155	171	187			203	219	235	251
	26			138	154	170	186			202	218	234	250
	25			137	153	169	185			201	217	233	249
	24			136	152	168	184			200	216	232	248
	23			135	151	167	183			199	215	231	247
	22			134	150	166	182			198	214	230	246
	21			133	149	165	181			197	213	229	245
	20			132	148	164	180			196	212	228	244
	19			131	147	163	179			195	211	227	243
	18			130	146	162	178			194	210	226	242
	17			129	145	161	177			193	209	225	241
	16			128	144	160	176			192	208	224	240

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	15			15	31	47	63			79	95	111	127
	14			14	30	46	62			78	94	110	126
	13			13	29	45	61			77	93	109	125
	12			12	28	44	60			76	92	108	124
	11			11	27	43	59			75	91	107	123
	10			10	26	42	58			74	90	106	122
	9			9	25	41	57			73	89	105	121
	8			8	24	40	56			72	88	104	120
	7			7	23	39	55			71	87	103	119
	6			6	22	38	54			70	86	102	118
	5			5	21	37	53			69	85	101	117
	4			4	20	36	52			68	84	100	116
	3			3	19	35	51			67	83	99	115
	2			2	18	34	50			66	82	98	114
	1			1	17	33	49			65	81	97	113
	0			0	16	32	48			64	80	96	112

表 O.4　Brocade X6-4 ポートインデックス一覧

ポートインデックスは、すべてのタイプのブレードで共通です。

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	47			47	111			175	239
	46			46	110			174	238
	45			45	109			173	237
	44			44	108			172	236
	43			43	107			171	235
	42			42	106			170	234
	41			41	105			169	233
	40			40	104			168	232
	39			39	103			167	231
	38			38	102			166	230
	37			37	101			165	229
	36			36	100			164	228
	35			35	99			163	227
	34			34	98			162	226
	33			33	97			161	225
	32			32	96			160	224
	31			31	95			159	223
	30			30	94			158	222
	29			29	93			157	221
	28			28	92			156	220
	27			27	91			155	219
	26			26	90			154	218
	25			25	89			153	217
	24			24	88			152	216
	23			23	87			151	215
	22			22	86			150	214
	21			21	85			149	213
	20			20	84			148	212
	19			19	83			147	211
	18			18	82			146	210
	17			17	81			145	209
	16			16	80			144	208

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	15			15	79			143	207
	14			14	78			142	206
	13			13	77			141	205
	12			12	76			140	204
	11			11	75			139	203
	10			10	74			138	202
	9			9	73			137	201
	8			8	72			136	200
	7			7	71			135	199
	6			6	70			134	198
	5			5	69			133	197
	4			4	68			132	196
	3			3	67			131	195
	2			2	66			130	194
	1			1	65			129	193
	0			0	64			128	192

表 O.5　Brocade X7-8 ポートインデックス一覧

ポートインデックスは、すべてのタイプのブレードで共通です。

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	95			95	191	287	383			479	575	671	767
	94			94	190	286	382			478	574	670	766
	93			93	189	285	381			477	573	669	765
	92			92	188	284	380			476	572	668	764
	91			91	187	283	379			475	571	667	763
	90			90	186	282	378			474	570	666	762
	89			89	185	281	377			473	569	665	761
	88			88	184	280	376			472	568	664	760
	87			87	183	279	375			471	567	663	759
	86			86	182	278	374			470	566	662	758
	85			85	181	277	373			469	565	661	757
	84			84	180	276	372			468	564	660	756
	83			83	179	275	371			467	563	659	755
	82			82	178	274	370			466	562	658	754
	81			81	177	273	369			465	561	657	753
	80			80	176	272	368			464	560	656	752
	79			79	175	271	367			463	559	655	751
	78			78	174	270	366			462	558	654	750
	77			77	173	269	365			461	557	653	749
	76			76	172	268	364			460	556	652	748
	75			75	171	267	363			459	555	651	747
	74			74	170	266	362			458	554	650	746
	73			73	169	265	361			457	553	649	745
	72			72	168	264	360			456	552	648	744
	71			71	167	263	359			455	551	647	743
	70			70	166	262	358			454	550	646	742
	69			69	165	261	357			453	549	645	741
	68			68	164	260	356			452	548	644	740
	67			67	163	259	355			451	547	643	739
	66			66	162	258	354			450	546	642	738
	65			65	161	257	353			449	545	641	737
	64			64	160	256	352			448	544	640	736
	63			63	159	255	351	831	895	447	543	639	735
	62			62	158	254	350	830	894	446	542	638	734

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	61			61	157	253	349	829	893	445	541	637	733
	60			60	156	252	348	828	892	444	540	636	732
	59			59	155	251	347	827	891	443	539	635	731
	58			58	154	250	346	826	890	442	538	634	730
	57			57	153	249	345	825	889	441	537	633	729
	56			56	152	248	344	824	888	440	536	632	728
	55			55	151	247	343	823	887	439	535	631	727
	54			54	150	246	342	822	886	438	534	630	726
	53			53	149	245	341	821	885	437	533	629	725
	52			52	148	244	340	820	884	436	532	628	724
	51			51	147	243	339	819	883	435	531	627	723
	50			50	146	242	338	818	882	434	530	626	722
	49			49	145	241	337	817	881	433	529	625	721
	48			48	144	240	336	816	880	432	528	624	720
	47			47	143	239	335	815	879	431	527	623	719
	46			46	142	238	334	814	878	430	526	622	718
	45			45	141	237	333	813	877	429	525	621	717
	44			44	140	236	332	812	876	428	524	620	716
	43			43	139	235	331	811	875	427	523	619	715
	42			42	138	234	330	810	874	426	522	618	714
	41			41	137	233	329	809	873	425	521	617	713
	40			40	136	232	328	808	872	424	520	616	712
	39			39	135	231	327	807	871	423	519	615	711
	38			38	134	230	326	806	870	422	518	614	710
	37			37	133	229	325	805	869	421	517	613	709
	36			36	132	228	324	804	868	420	516	612	708
	35			35	131	227	323	803	867	419	515	611	707
	34			34	130	226	322	802	866	418	514	610	706
	33			33	129	225	321	801	865	417	513	609	705
	32			32	128	224	320	800	864	416	512	608	704
	31			31	127	223	319	799	863	415	511	607	703
	30			30	126	222	318	798	862	414	510	606	702
	29			29	125	221	317	797	861	413	509	605	701
	28			28	124	220	316	796	860	412	508	604	700

		Slot 番号											
		1	2	3	4	5	6	7	8	9	10	11	12
Port 番号	27			27	123	219	315	795	859	411	507	603	699
	26			26	122	218	314	794	858	410	506	602	698
	25			25	121	217	313	793	857	409	505	601	697
	24			24	120	216	312	792	856	408	504	600	696
	23			23	119	215	311	791	855	407	503	599	695
	22			22	118	214	310	790	854	406	502	598	694
	21			21	117	213	309	789	853	405	501	597	693
	20			20	116	212	308	788	852	404	500	596	692
	19			19	115	211	307	787	851	403	499	595	691
	18			18	114	210	306	786	850	402	498	594	690
	17			17	113	209	305	785	849	401	497	593	689
	16			16	112	208	304	784	848	400	496	592	688
	15			15	111	207	303	783	847	399	495	591	687
	14			14	110	206	302	782	846	398	494	590	686
	13			13	109	205	301	781	845	397	493	589	685
	12			12	108	204	300	780	844	396	492	588	684
	11			11	107	203	299	779	843	395	491	587	683
	10			10	106	202	298	778	842	394	490	586	682
	9			9	105	201	297	777	841	393	489	585	681
	8			8	104	200	296	776	840	392	488	584	680
	7			7	103	199	295	775	839	391	487	583	679
	6			6	102	198	294	774	838	390	486	582	678
	5			5	101	197	293	773	837	389	485	581	677
	4			4	100	196	292	772	836	388	484	580	676
	3			3	99	195	291	771	835	387	483	579	675
	2			2	98	194	290	770	834	386	482	578	674
	1			1	97	193	289	769	833	385	481	577	673
	0			0	96	192	288	768	832	384	480	576	672

表 O.6　Brocade X7-4 ポートインデックス一覧

ポートインデックスは、すべてのタイプのブレードで共通です。

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	95			95	191			287	383
	94			94	190			286	382
	93			93	189			285	381
	92			92	188			284	380
	91			91	187			283	379
	90			90	186			282	378
	89			89	185			281	377
	88			88	184			280	376
	87			87	183			279	375
	86			86	182			278	374
	85			85	181			277	373
	84			84	180			276	372
	83			83	179			275	371
	82			82	178			274	370
	81			81	177			273	369
	80			80	176			272	368
	79			79	175			271	367
	78			78	174			270	366
	77			77	173			269	365
	76			76	172			268	364
	75			75	171			267	363
	74			74	170			266	362
	73			73	169			265	361
	72			72	168			264	360
	71			71	167			263	359
	70			70	166			262	358
	69			69	165			261	357
	68			68	164			260	356
	67			67	163			259	355
	66			66	162			258	354
	65			65	161			257	353
	64			64	160			256	352
	63			63	159	447	511	255	351
	62			62	158	446	510	254	350

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	61			61	157	445	509	253	349
	60			60	156	444	508	252	348
	59			59	155	443	507	251	347
	58			58	154	442	506	250	346
	57			57	153	441	505	249	345
	56			56	152	440	504	248	344
	55			55	151	439	503	247	343
	54			54	150	438	502	246	342
	53			53	149	437	501	245	341
	52			52	148	436	500	244	340
	51			51	147	435	499	243	339
	50			50	146	434	498	242	338
	49			49	145	433	497	241	337
	48			48	144	432	496	240	336
	47			47	143	431	495	239	335
	46			46	142	430	494	238	334
	45			45	141	429	493	237	333
	44			44	140	428	492	236	332
	43			43	139	427	491	235	331
	42			42	138	426	490	234	330
	41			41	137	425	489	233	329
	40			40	136	424	488	232	328
	39			39	135	423	487	231	327
	38			38	134	422	486	230	326
	37			37	133	421	485	229	325
	36			36	132	420	484	228	324
	35			35	131	419	483	227	323
	34			34	130	418	482	226	322
	33			33	129	417	481	225	321
	32			32	128	416	480	224	320
	31			31	127	415	479	223	319
	30			30	126	414	478	222	318
	29			29	125	413	477	221	317
	28			28	124	412	476	220	316

		Slot 番号							
		1	2	3	4	5	6	7	8
Port 番号	27			27	123	411	475	219	315
	26			26	122	410	474	218	314
	25			25	121	409	473	217	313
	24			24	120	408	472	216	312
	23			23	119	407	471	215	311
	22			22	118	406	470	214	310
	21			21	117	405	469	213	309
	20			20	116	404	468	212	308
	19			19	115	403	467	211	307
	18			18	114	402	466	210	306
	17			17	113	401	465	209	305
	16			16	112	400	464	208	304
	15			15	111	399	463	207	303
	14			14	110	398	462	206	302
	13			13	109	397	461	205	301
	12			12	108	396	460	204	300
	11			11	107	395	459	203	299
	10			10	106	394	458	202	298
	9			9	105	393	457	201	297
	8			8	104	392	456	200	296
	7			7	103	391	455	199	295
	6			6	102	390	454	198	294
	5			5	101	389	453	197	293
	4			4	100	388	452	196	292
	3			3	99	387	451	195	291
	2			2	98	386	450	194	290
	1			1	97	385	449	193	289
	0			0	96	384	448	192	288

付録 P

リモート通報機能の設定／確認

リモート通報機能とは、本装置からの SNMP トラップを ETERNUS SF Storage Cruiser で受信した契機でリモート通報メールを送信し、遠隔地（リモート）にある富士通サポートセンター（集中監視センター：OSC）の支援または管理の下で、リモート保守をサポートする機能です。本装置は、ETERNUS SF Storage Cruiser のメール通報機能を利用してリモート通報機能を実現しています。

P.1 設定手順

リモート通報機能を設定するには、以下の手順を実行します。

手 順

1 ETERNUS SF Storage Cruiser が動作しているサーバで、以下の階層に remcs フォルダを作成します。

■ Oracle Solaris 版または Linux 版マネージャーの場合

```
# mkdir /etc/opt/FJSVssmgr/current/eventmail/remcs
```

■ Windows 版マネージャーの場合

```
C:¥> mkdir $ENV_DIR¥ESC¥Manager¥etc¥opt¥FJSVssmgr¥current¥eventmail¥remcs
```

2 作成した remcs フォルダに、以下の内容のメール情報設定ファイル（remcsmail.conf）を作成します。

備 考

このファイルは ASCII 文字列だけ使用できます。また、不要な空白や既定の項目以外を記載しないでください。

- メール情報設定ファイル作成例（remcsmail.conf）

```
eventmail.smtp.host=10.23.4.3                          (*1)
eventmail.smtp.port=25                                 (*2)
eventmail.smtp.from=esc@example.com                    (*3)
eventmail.message.to=acommon@remcsworld.ne.jp          (*4)
remcs.polling.week=Sunday                              (*5)
remcs.polling.hour=23                                  (*6)
```

*1: リモート通報のメールの送信元となる顧客所有のメールサーバを、IP アドレスで指定します。
*2: 上記メールサーバのポート番号を指定します。
*3: メール送信する際に「From」ヘッダーに記載される発信元メールアドレスを 1 つ指定します。「P.2 設定確認手順」(P.128) でセンターとの接続確認が正常に行われた場合、ここに指定したメールアドレスにセンター側から返信メールが送信されます。
*4: 送信先メールアドレスには、この設定値を指定します。
*5: 定期ポーリングを行う曜日を、以下のいずれか 1 つで指定します（定期ポーリングは装置の状態確認のため、定期的にセンターと接続を行います）。この例では、日曜日に定期ポーリングが行われます。
設定値 ：Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday
*6: 定期ポーリングを行う時間を、24 時間表記で指定します。指定できる値は 1 時間単位で 0 ～ 23 までの値です（定期ポーリングは、装置の状態確認のため、定期的にセンターと接続を行います）。この例では、日曜日の 23 時に定期ポーリングが行われます。

3 作成した remcs フォルダに、以下の内容の製品情報設定ファイル（remcsproduct.conf）を作成します。

備 考

- リモート通報対象の装置の情報（IP アドレス、モデル名、装置号機）だけを記載してください。
- このファイルは ASCII 文字列だけ使用できます。また、不要な空白や既定の項目以外を記載しないでください。

- 製品情報設定ファイル作成例（remcsproduct.conf）

```
192.168.0.10:EBR6733F,100                    (*1)
192.168.0.20:EBR6733F,101                    (*2)
192.168.0.30:EBR6715F,200                    (*3)
```

*1: この設定の場合、管理 LAN の IP アドレス :192.168.0.10/ モデル名 :EBR6733F/ 装置号機 :100 の装置が REMCS センターの通報対象となります。
*2: この設定の場合、管理 LAN の IP アドレス :192.168.0.20/ モデル名 :EBR6733F/ 装置号機 :101 の装置が REMCS センターの通報対象となります。
*3: この設定の場合、管理 LAN の IP アドレス :192.168.0.30/ モデル名 :EBR6751F/ 装置号機 :200 の装置が REMCS センターの通報対象となります。

4 すべての設定を完了後、以下のコマンドで設定反映を行います。

備 考

メール情報設定ファイル、または製品情報リストファイルの設定に誤りがある場合、「ERROR:ssmgr9200:Failed to configure mail information: 」が出力されます。このエラー以外が出力された場合は、『ETERNUS SF メッセージ説明書』を参照してください。

■ Oracle Solaris 版または Linux 版マネージャーの場合

```
# /opt/FJSVssmgr/sbin/storageadm remcs load
eventmail.smtp.host=10.23.4.3
eventmail.smtp.port=25
eventmail.smtp.from=esc@example.com
eventmail.message.to=acommon@remcsworld.ne.jp
remcs.polling.week=Sunday
remcs.polling.hour=23
192.168.0.10:EBR6733F,100
192.168.0.20:EBR6733F,101
192.168.0.30:EBR6715F,200
#
```

■ Windows 版マネージャーの場合

```
C:¥> "C:¥ETERNUS_SF¥ESC¥Manager¥opt¥FJSVssmgr¥sbin¥storageadm" remcs load
eventmail.smtp.host=10.23.4.3
eventmail.smtp.port=25
eventmail.smtp.from=esc@example.com
eventmail.message.to=acommon@remcsworld.ne.jp
remcs.polling.week=Sunday
remcs.polling.hour=23
192.168.0.10:EBR6733F,100
192.168.0.20:EBR6733F,101
192.168.0.30:EBR6715F,200
C:¥>
```

手順ここまで

P.2 設定確認手順

手 順

1 以下のコマンドを使用してテストメールを送信し、センターとの接続確認が正常に行われることを確認します。
接続確認が正常に行われた場合、「P.1 設定手順」(P.125) の eventmail.smtp.from に指定したメールアドレスにセンター側から返信メールが送信されます。

備 考

- メール情報設定ファイル、または製品情報リストファイルの設定に誤りがある場合、「ERROR:ssmgr9201:Failed to send mail:」が出力されます。このエラー以外が出力された場合は、『ETERNUS SF メッセージ説明書』を参照してください。
- ETERNUS SF Storage Cruiser の SNMP トラップ設定確認テストでもリモート通報メールが送信されますが、この場合はセンターとの接続確認ではなく、装置異常のアラーム通知として送信されます。アラーム通知や、定期ポーリングの状況についてはセンター側にお問い合わせください。SNMP トラップ設定確認テストの詳細は『ETERNUS SF Storage Cruiser 運用ガイド』を参照してください。

■ Oracle Solaris 版または Linux 版マネージャーの場合

```
# /opt/FJSVssmgr/sbin/storageadm remcs send -ipaddr 192.168.0.10  (*1)
INFO:swsag0001:Command terminated normally
#
```

*1: この例の場合、192.168.0.10 の装置からのテスト用リモート通報メールを送信します。

■ Windows 版マネージャーの場合

```
C:¥> "C:¥ETERNUS_SF¥ESC¥Manager¥opt¥FJSVssmgr¥sbin¥storageadm"
 remcs send -ipaddr 192.168.0.10                                (*1)
INFO:swsag0001:Command terminated normally
C:¥>
```

*1: この例の場合、192.168.0.10 の装置からのテスト用リモート通報メールを送信します。

手順ここまで

付録 Q

アカウントの無効化

スイッチに使用しない以下のアカウントを無効化することで、オープンソースの脆弱性などに対するセキュリティが向上します。

- root
- factory

注 意

- この方法によるセキュリティ向上はファームウェアが FOS v7.3 以前の場合にのみ有効です。FOS v7.4 以降では「factory」アカウントは使用できず、「root」アカウントは出荷時に無効になっていますので、無効化の作業は必要はありません。
- ユーザー名「admin」のアカウントは保守作業時に使用します。無効化しないよう注意してください。

Q.1 事前確認（userconfig）

手 順

1 以下のコマンドを使用して現在のアカウントの状態を確認します。

■ root アカウントの確認

```
switch:admin> userconfig --show root

Account name: root*
Description: root
Enabled: Yes     ← 「Yes」であることを確認する。
```

■ factory アカウントの確認

```
switch:admin> userconfig --show factory

Account name: factory*
Description: Diagnostics
Enabled: Yes     ← 「Yes」であることを確認する。
```

「Enabled」が「No」の場合、およびアカウントの情報が表示されない場合は、アカウントがすでに無効になっているか使用不可の状態となっているので、これ以降の手順は実施する必要はありません。

手順ここまで

Q.2 アカウントの無効化（userconfig）

手 順

1 以下のコマンドを使用してアカウントを無効化します。

■ root アカウントの無効化

```
switch:admin> userconfig --change root -e no
```

■ factory アカウントの無効化

```
switch:admin> userconfig --change factory -e no
```

2 アカウントが無効に変更されたことを確認します。

■ root アカウントの確認

```
switch:admin> userconfig --show root

Account name: root*
Description: root
Enabled: No     ←「No」であることを確認する。
```

■ factory アカウントの確認

```
switch:admin> userconfig --show factory

Account name: factory
Description: Diagnostics
Enabled: No     ←「No」であることを確認する。
```

手順ここまで

付録 R

Web Tools

重　要

HTTPS 証明書には有効期限が設定されています。お客様のセキュリティ運用ポリシーに従って、有効期限の更新作業を行ってください。

HTTPS または HTTP を使用して、ブラウザから Web Tools を起動しスイッチ情報を確認します。

注 意

FOS v9.1.1 以降をサポートする装置では、セキュリティ強化のため、SNMPv1、Telnet、FTP、および HTTP はデフォルトで無効になっています。使用する場合は、各プロトコルの設定変更が必要です。
セキュリティ強化のため、HTTPS での接続を推奨します。HTTP 有効／無効の方法については「S.4 SNMPv1 有効／無効の設定手順」(P.149) を参照してください。
HTTPS を使用するには、HTTPS 証明書が必要です。確認方法およびインストール方法については、「S.3.3 HTTPS 証明書の確認／登録／削除手順」(P.147) を参照してください。

FOS v9.0.x より前の FOS では、Web Tools を使用する場合、Web Tools を使用する端末にファームウェア版数に対応した Java-Plugin を適用する必要があります。FOS v9.0.x 以降の場合は Java-Plugin は不要です。
FOS v9.x のスイッチに HTTPS 証明書がインストールされている場合、HTTP でのアクセスが拒否されるおそれがあります。その場合は、HTTPS を使用してアクセスしてください。HTTPS 証明書の確認方法については、「S.3.3 HTTPS 証明書の確認／登録／削除手順」(P.147) を参照してください。

FOS v9.2.0 以降、HTTPS 証明書に DSA アルゴリズム（SHA1 または SHA2）が使用されている場合、Web Tools はスイッチを検出できません。

手 順

1　ブラウザを開き、アドレスバーへ HTTP または HTTPS に続いてスイッチの IP アドレスを入力し、Web Tools を起動します。

```
https://192.168.0.xx
```

手順ここまで

付録 S
Secure Mode

FOS v9.1.1 以降で出荷される装置については、セキュリティ強化のため、Telnet、FTP、HTTP、および SNMPv1 はデフォルトで無効になっています（Secure Mode 有効設定）。
また、FOS v9.1.1 以降で使用する装置は、これらの機能を無効とした（Secure Mode 有効設定）運用を推奨します。
そのため、以下の機能を使用する場合は、各機能の設定変更が必要です（Secure Mode 無効設定）。

- Telnet
- FTP
- HTTP
- SNMPv1

さらに、FOS v9.2.0 以降で出荷された装置では、より強化されたデフォルトセキュアの設定が有効となります。
以前のバージョンよりアップグレードされた FOS v9.2.0 は以前の環境が引き継がれます。

- 以前のバージョンよりアップグレードされた FOS で動作する装置、およびデフォルトセキュア環境の装置の両方で、SNMP パスワード暗号化はデフォルトで有効です。
- デフォルトセキュアの環境では、非セキュア Syslog は無効です。

各機能で推奨する運用は、以下のとおりです。

機能	推奨運用
Telnet	SSH を推奨
FTP	必要に応じて機能を有効にし、作業後は機能を無効（Secure Mode 有効）に戻す
HTTP	HTTPS を推奨
SNMPv1	SNMPv1 が必要な環境では有効化して運用
Syslog	セキュア syslog を使用（デフォルトセキュアの設定時）

S.1 Telnet 有効／無効の設定手順

Telnet を有効／無効にする手順について説明します。

S.1.1 Telnet 設定確認

Telnet の有効／無効の設定を確認する手順について説明します。

手 順

1 スイッチにログインします。

2 以下のコマンドを入力し、設定を確認します。

```
switch:admin> ipfilter --show

Name: default_ipv4, Type: ipv4, State: defined                          (*1)
Rule    Source IP                       Protocol    Dest Port    Action
1       any                                    tcp         22    permit
2       any                                    tcp         23    permit
3       any                                    tcp         80    permit
4       any                                    tcp        443    permit
5       any                                    udp        161    permit
6       any                                    udp        123    permit
7       any                                    tcp  600 - 1023    permit
8       any                                    udp  600 - 1023    permit
          (*2)                                                        (*3)
Name: default_ipv6, Type: ipv6, State: active                           (*4)
Rule    Source IP                       Protocol    Dest Port    Action
1       any                                    tcp         22    permit
2       any                                    tcp         23    permit    (*5)
3       any                                    tcp         80    permit
4       any                                    tcp        443    permit
5       any                                    udp        161    permit
6       any                                    udp        123    permit
7       any                                    tcp  600 - 1023    permit
8       any                                    udp  600 - 1023    permit

Name: DS_ipv4, Type: ipv4, State: active                                (*4)
Rule    Source IP                       Protocol    Dest Port    Action
1       any                                    tcp         22    permit
2       any                                    tcp         23    deny      (*5)
3       any                                    tcp         80    deny
4       any                                    tcp        443    permit
5       any                                    udp        161    permit
6       any                                    udp        123    permit
7       any                                    tcp  600 - 1023    permit
8       any                                    udp  600 - 1023    permit
```

*1: Name: ポリシー名。装置に定義されているポリシーが表示されます。

Type: ipv4およびipv6があり、各1つのポリシーがアクティブになります。

State: ポリシーの状態を示します。有効なポリシーがactiveとなり、無効なポリシーはdefinedになります。**ipfilter --activate**コマンドによりアクティブ化されます。

*2: ルール番号。**ipfilter --addrule/delrule** コマンドでこの番号を指定してポリシーを編集します。

*3: プロトコルのポート番号。Telnet では 23 を使用します。

*4: 「State: active」となっているポリシーを確認します。
この例では、ipv4 は「DS_ipv4」、ipv6 は「default_ipv6」というポリシーがアクティブになっています。

*5: アクティブなポリシーの Dest Port「23」の Action を確認します。
「permit」の状態であれば Telnet 使用可能、「deny」の状態であれば Telnet 使用不可です。
この例では、ipv4 は Telnet 使用不可、ipv6 は Telnet 使用可能となります。

手順ここまで

備 考

デフォルトポリシー「default_ipv4/default_ipv6」の内容は、configdefault 実行時のファームウェア版数により異なります。出荷時の状態は以下のとおりです。

- FOS v9.0.x 以前
  default_ipv4/default_ipv6 で Telnet は許可（permit）されている。
- FOS v9.1.x
  default_ipv4/default_ipv6 で Telnet は許可（permit）となっているが、ポリシーは非アクティブ。DS_ipv4/DS_ipv6 ポリシーがアクティブになり、Telnet は拒否（deny）されている。
- FOS v9.2.x 以降
  default_ipv4/default_ipv6 で Telnet は拒否（deny）されている。

S.1.2 Telnet 有効／無効化手順

アクティブなポリシーが default_ipv4/default_ipv6 の場合

ポリシー「default_ipv4/default_ipv6」の内容は、configdefault 実行時のファームウェア版数により異なり、書き換えることができません。

default_ipv4 により Telnet が無効化されている場合を例に、新たなポリシーを作成し、アクティブなポリシーを変更する手順について説明します。

手 順

1 default_ipv4 ポリシーをもとに、新規ポリシー「New_Filter」を作成します。

```
switch:admin> ipfilter --clone New_Filter -from default_ipv4
```

2 新規ポリシーが作成されたことを確認します。

```
switch:admin> ipfilter --show
 : <<省略>>
Name: New_Filter, Type: ipv4, State: defined (modified)
Rule   Source IP                                  Protocol   Dest Port   Action
1      any                                              tcp        22     permit
2      any                                              tcp        23       deny
3      any                                              tcp        80       deny
4      any                                              tcp       443     permit
5      any                                              udp       161     permit
6      any                                              udp       123     permit
7      any                                              tcp  600 - 1023  permit
8      any                                              udp  600 - 1023  permit
```

3 New_Filter ポリシーに Telnet を有効または無効にするルールを追加します。

```
switch:admin> ipfilter --addrule New_Filter -rule 3 -sip any -dp 23 -prot tcp -act permit
```

-rule	ルール番号を指定します。この例では3番目にルールを追加しており、既存の3番以降のルールは番号が繰り下がります。
-sip	送信元IPアドレスを指定します。
-dp	宛先ポート番号、ポート番号の範囲、またはサービス名を指定します。Telnetのポート番号は23です。
-prot	プロトコルタイプ（tcpやudpなど）を指定します。
-act {permit | deny}	このルールに関連付けられたアクションを指定します。有効化する場合はpermit、無効化する場合はdenyを指定してください。

この時点での設定は以下のようになります。

```
switch:admin> ipfilter --show
: <<省略>>
Name: New_Filter, Type: ipv4, State: defined (modified)
Rule    Source IP               Protocol     Dest Port   Action
1      any                            tcp        22      permit
2      any                            tcp        23      deny      既存のルール
3      any                            tcp        23      permit    追加したルール
4      any                            tcp        80      deny
5      any                            tcp       443      permit
6      any                            udp       161      permit
7      any                            udp       123      permit
8      any                            tcp   600 - 1023   permit
9      any                            udp   600 - 1023   permit
```

4 New_Filter ポリシーから、Telnet について定義された既存のルールを削除します。

```
switch:admin> ipfilter --delrule New_Filter -rule 2
```

5 New_Filter ポリシーが更新されたことを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: New_Filter, Type: ipv4, State: defined (modified)
Rule    Source IP                                Protocol    Dest Port   Action
1       any                                             tcp         22      permit
2       any                                             tcp         23      permit
3       any                                             tcp         80        deny
4       any                                             tcp        443      permit
5       any                                             udp        161      permit
6       any                                             udp        123      permit
7       any                                             tcp   600 - 1023    permit
8       any                                             udp   600 - 1023    permit
```

6 作成した New_Filter ポリシーをアクティブにします。

```
switch:admin> ipfilter --activate New_Filter
```

7 New_Filter ポリシーがアクティブになっていることを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: New_Filter, Type: ipv4, State: active
Rule    Source IP                               Protocol    Dest Port   Action
1       any                                             tcp         22      permit
2       any                                             tcp         23      permit
3       any                                             tcp         80        deny
4       any                                             tcp        443      permit
5       any                                             udp        161      permit
6       any                                             udp        123      permit
7       any                                             tcp   600 - 1023    permit
8       any                                             udp   600 - 1023    permit
```

手順ここまで

Telnet を使い続ける必要がない場合、Telnet の使用が終了したら、「■ アクティブなポリシーが default_ipv4/default_ipv6 以外の場合」(P.136) と同様の手順で、作成したポリシーを編集し、Telnet を無効化してください。

```
switch:admin> ipfilter --addrule New_Filter -rule 3 -sip any -dp 23 -prot tcp -act deny
switch:admin> ipfilter --delrule New_Filter -rule 2
switch:admin> ipfilter --activate New_Filter
```

■ アクティブなポリシーが default_ipv4/default_ipv6 以外の場合

アクティブなポリシーのルールを変更し、Telnet 有効／無効を変更する手順を説明します。

「S.1.1 Telnet 設定確認」(P.132) の例のとおり、DS_ipv4 ポリシーで Telnet（ポート 23）が無効になっている状態から、Telnet を有効にする場合を例に説明します。

有効になっているポリシー名が DS_ipv4 と異なる場合は、読み換えて実施してください。

手 順

1 アクティブなポリシーに Telnet を有効または無効にするルールを追加します。

```
switch:admin> ipfilter --addrule DS_ipv4 -rule 3 -sip any -dp 23 -prot tcp -act permit
```

-rule	ルール番号を指定します。この例では3番目にルールを追加しており、既存の3番以降のルールは番号が繰り下がります。
-sip	送信元IPアドレスを指定します。
-dp	宛先ポート番号、ポート番号の範囲、またはサービス名を指定します。Telnetのポート番号は23です。
-prot	プロトコルタイプ (tcpやudpなど) を指定します。
-act {permit | deny}	このルールに関連付けられたアクションを指定します。有効化する場合はpermit、無効化する場合はdenyを指定してください。

この時点での設定は以下のようになります。

```
switch:admin> ipfilter --show
: <<省略>>
Name: DS_ipv4, Type: ipv4, State: active (modified)
Rule    Source IP                Protocol    Dest Port   Action
1       any                             tcp        22     permit
2       any                             tcp        23       deny  既存のルール
3       any                             tcp        23     permit  追加したルール
4       any                             tcp        80       deny
5       any                             tcp       443     permit
6       any                             udp       161     permit
7       any                             udp       123     permit
8       any                             tcp  600 - 1023   permit
```

2 DS_ipv4 ポリシーから、Telnet について定義された既存のルールを削除します。

```
switch:admin> ipfilter --delrule DS_ipv4 -rule 2
```

3 DS_ipv4 ポリシーが更新されたことを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: DS_ipv4, Type: ipv4, State: active (modified)
Rule    Source IP                          Protocol    Dest Port   Action
1       any                                     tcp        22     permit
2       any                                     tcp        23     permit
3       any                                     tcp        80       deny
4       any                                     tcp       443     permit
5       any                                     udp       161     permit
6       any                                     udp       123     permit
7       any                                     tcp  600 - 1023   permit
8       any                                     udp  600 - 1023   permit
```

4 DS_ipv4 ポリシーの activate を実行し、変更を反映します。

```
switch:admin> ipfilter --activate DS_ipv4
```

5 DS_ipv4 ポリシーへの変更が反映されたことを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: DS_ipv4, Type: ipv4, State: active
Rule    Source IP                                Protocol    Dest Port   Action
1       any                                             tcp        22     permit
2       any                                             tcp        23     permit
3       any                                             tcp        80       deny
4       any                                             tcp       443     permit
5       any                                             udp       161     permit
6       any                                             udp       123     permit
7       any                                             tcp   600 - 1023  permit
8       any                                             udp   600 - 1023  permit
```

手順ここまで

Telnet を使い続ける必要がない場合、Telnet の使用が終了したら、同様の手順で Telnet を無効化してください。

```
switch:admin> ipfilter --addrule DS_ipv4 -rule 3 -sip any -dp 23 -prot tcp -act deny
switch:admin> ipfilter --delrule DS_ipv4 -rule 2
switch:admin> ipfilter --activate DS_ipv4
```

注 意

設定後に **configdefault -all** コマンドを実行した場合、デフォルトポリシー「default_ipv4/default_ipv6」の内容が **configdefault** 実行時のファームウェア版数により異なるため、Telnet が有効になることがあります。
継続して Telnet 接続が必要でない場合は、確認コマンドを実施のうえ、再度 Telnet を無効に設定してください。

S.2 FTP・Non-secure syslog 有効／無効の設定手順

FTP・Non-secure syslog を有効／無効にする手順について説明します。

手 順

1 スイッチにログインし、以下のコマンドを入力して FTP・Non-secure syslog の状態を確認します。

```
switch_1:admin> configure --show -module CHS -key cfgload.secure
Key Name                                                Value
Enable secure switch mode(cfgload.secure)               1
```

2 以下のコマンドを入力し、FTP・Non-secure syslog を有効にします。

```
switch:admin> configure --set -module CHS -key cfgload.secure -value 0
```

注 意

この手順を実施すると、FTP・Non-secure syslog の両方が有効になります。

3 以下のコマンドで設定を確認します。

```
switch:admin> configure --show -module CHS -key cfgload.secure
Key Name                                                Value
Enforce secure config Upload/Download(cfgload.secure)   0           (*1)
```

*1: Value が「0（有効）」になっていることを確認します。FTP・Non-secure syslog は有効のため、使用できます。

4 FTP の使用が終了したら、以下のコマンドで FTP・Non-secure syslog を無効にします。

```
switch:admin> configure --set -module CHS -key cfgload.secure -value 1
```

注 意

この手順を実施すると、FTP・Non-secure syslog の両方が無効になります。

5 以下のコマンドで設定を確認します。

```
switch:admin> configure --show -module CHS -key cfgload.secure
Key Name                                                Value
Enforce secure config Upload/Download(cfgload.secure)   1           (*1)
```

*1: Value が「1（無効）」になっていることを確認します。FTP・Non-secure syslog は無効のため、使用できません。

注 意

設定後に **configdefault –all** コマンドを実行すると、ファームウェア版数により FTP・Non-secure syslog が有効になる場合があります。手順 1 の確認作業を実施し、継続して FTP 接続・Non-secure syslog が必要でない場合は、再度無効設定をしてください。

手順ここまで

S.3 HTTP 有効／無効の設定手順

HTTP を有効／無効にする手順について説明します。

S.3.1 HTTP 設定確認

HTTP の有効／無効の設定を確認する手順について説明します。

手 順

1 スイッチにログインします。

2 以下のコマンドを入力し、設定を確認します。

```
switch:admin> ipfilter --show

Name: default_ipv4, Type: ipv4, State: defined                          (*1)
Rule    Source IP                       Protocol    Dest Port    Action
1       any                                    tcp         22    permit
2       any                                    tcp         23    permit
3       any                                    tcp         80    permit
4       any                                    tcp        443    permit
5       any                                    udp        161    permit
6       any                                    udp        123    permit
7       any                                    tcp  600 - 1023    permit
8       any                                    udp  600 - 1023    permit
                (*2)                                                (*3)
Name: default_ipv6, Type: ipv6, State: active                           (*4)
Rule    Source IP                       Protocol    Dest Port    Action
1       any                                    tcp         22    permit
2       any                                    tcp         23    permit
3       any                                    tcp         80    permit    (*5)
4       any                                    tcp        443    permit
5       any                                    udp        161    permit
6       any                                    udp        123    permit
7       any                                    tcp  600 - 1023    permit
8       any                                    udp  600 - 1023    permit

Name: DS_ipv4, Type: ipv4, State: active                                (*4)
Rule    Source IP                       Protocol    Dest Port    Action
1       any                                    tcp         22    permit
2       any                                    tcp         23    deny
3       any                                    tcp         80    deny      (*5)
4       any                                    tcp        443    permit
5       any                                    udp        161    permit
6       any                                    udp        123    permit
7       any                                    tcp  600 - 1023    permit
8       any                                    udp  600 - 1023    permit
```

*1: Name: ポリシー名。装置に定義されているポリシーが表示されます。

Type: ipv4およびipv6があり、各1つのポリシーがアクティブになります。

State: ポリシーの状態を示します。有効なポリシーがactiveとなり、無効なポリシーはdefinedになります。**ipfilter --activate**コマンドによりアクティブ化されます。

*2: ルール番号。**ipfilter --addrule/delrule** コマンドでこの番号を指定してポリシーを編集します。

*3: プロトコルのポート番号。HTTP では 80 を使用します。

*4: 「State: active」となっているポリシーを確認します。
この例では、ipv4 は「DS_ipv4」、ipv6 は「default_ipv6」というポリシーがアクティブになっています。

*5: アクティブなポリシーの Dest Port「80」の Action を確認します。
「permit」の状態であれば HTTP 使用可能、「deny」の状態であれば HTTP 使用不可です。
この例では、ipv4 は HTTP 使用不可、ipv6 は HTTP 使用可能となります。

手順ここまで

備 考

デフォルトポリシー「default_ipv4/default_ipv6」の内容は、configdefault 実行時のファームウェア版数により異なります。出荷時の状態は以下のとおりです。

- FOS v9.0.x 以前
  default_ipv4/default_ipv6 で HTTP は許可（permit）されている。
- FOS v9.1.x
  default_ipv4/default_ipv6 で HTTP は許可（permit）となっているが、ポリシーは非アクティブ。DS_ipv4/DS_ipv6 ポリシーがアクティブになり、HTTP は拒否（deny）されている。
- FOS v9.2.x 以降
  default_ipv4/default_ipv6 で HTTP は拒否（deny）されている。

S.3.2 HTTP 有効／無効化手順

アクティブなポリシーが default_ipv4/default_ipv6 の場合

ポリシー「default_ipv4/default_ipv6」の内容は configdefault 実行時のファームウェア版数により異なり、書き換えることができません。

default_ipv4 により HTTP が無効化されている場合を例に、新たなポリシーを作成し、アクティブなポリシーを変更する手順に説明します。

手 順

1 default_ipv4 ポリシーをもとに、新規ポリシー「New_Filter」を作成します。

```
switch:admin> ipfilter --clone New_Filter -from default_ipv4
```

2 新規ポリシーが作成されたことを確認します。

```
switch:admin> ipfilter --show
 : <<省略>>
Name: New_Filter, Type: ipv4, State: defined (modified)
Rule   Source IP                                  Protocol   Dest Port   Action
1      any                                              tcp        22     permit
2      any                                              tcp        23       deny
3      any                                              tcp        80       deny
4      any                                              tcp       443     permit
5      any                                              udp       161     permit
6      any                                              udp       123     permit
7      any                                              tcp  600 - 1023  permit
8      any                                              udp  600 - 1023  permit
```

3 New_Filter ポリシーに HTTP を有効または無効にするルールを追加します。

```
switch:admin> ipfilter --addrule New_Filter -rule 4 -sip any -dp 80 -prot tcp -act permit
```

-rule	ルール番号を指定します。この例では4番目にルールを追加しており、既存の4番以降のルールは番号が繰り下がります。
-sip	送信元IPアドレスを指定します。
-dp	宛先ポート番号、ポート番号の範囲、またはサービス名を指定します。HTTPのポート番号は80です。
-prot	プロトコルタイプ（tcpやudpなど）を指定します。
-act {permit | deny}	このルールに関連付けられたアクションを指定します。有効化する場合はpermit、無効化する場合はdenyを指定してください。

この時点での設定は以下のようになります。

```
switch:admin> ipfilter --show
: <<省略>>
Name: New_Filter, Type: ipv4, State: defined (modified)
Rule    Source IP               Protocol     Dest Port   Action
1       any                            tcp        22       permit
2       any                            tcp        23         deny
3       any                            tcp        80         deny  既存のルール
4       any                            tcp        80       permit  追加したルール
5       any                            tcp       443       permit
6       any                            udp       161       permit
7       any                            udp       123       permit
8       any                            tcp   600 - 1023    permit
9       any                            udp   600 - 1023    permit
```

4 New_Filter ポリシーから、HTTP について定義された既存のルールを削除します。

```
switch:admin> ipfilter --delrule New_Filter -rule 3
```

5 New_Filter ポリシーが更新されたことを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: New_Filter, Type: ipv4, State: defined (modified)
Rule    Source IP                              Protocol     Dest Port   Action
1       any                                           tcp        22       permit
2       any                                           tcp        23         deny
3       any                                           tcp        80       permit
4       any                                           tcp       443       permit
5       any                                           udp       161       permit
6       any                                           udp       123       permit
7       any                                           tcp   600 - 1023    permit
8       any                                           udp   600 - 1023    permit
```

6 作成した New_Filter ポリシーをアクティブにします。

```
switch:admin> ipfilter --activate New_Filter
```

7 New_Filter ポリシーがアクティブになっていることを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: New_Filter, Type: ipv4, State: active
Rule    Source IP                                Protocol    Dest Port   Action
1       any                                             tcp        22     permit
2       any                                             tcp        23       deny
3       any                                             tcp        80     permit
4       any                                             tcp       443     permit
5       any                                             udp       161     permit
6       any                                             udp       123     permit
7       any                                             tcp   600 - 1023  permit
8       any                                             udp   600 - 1023  permit
```

手順ここまで

HTTP を使い続ける必要がない場合、HTTP の使用が終了したら、「■ アクティブなポリシーが default_ipv4/default_ipv6 以外の場合」(P.144) と同様の手順で、作成したポリシーを編集し、HTTP を無効化してください。

```
switch:admin> ipfilter --addrule New_Filter -rule 4 -sip any -dp 80 -prot tcp -act deny
switch:admin> ipfilter --delrule New_Filter -rule 3
switch:admin> ipfilter --activate New_Filter
```

■ アクティブなポリシーが default_ipv4/default_ipv6 以外の場合

アクティブなポリシーのルールを変更し、HTTP 有効／無効を変更する手順を説明します。

「S.3.1 HTTP 設定確認」(P.140) の例のとおり DS_ipv4 ポリシーで HTTP（ポート 80）が無効になっている状態から、HTTP を有効にする場合を例に説明します。

有効になっているポリシー名が DS_ipv4 と異なる場合は、置き換えて実施してください。

手 順

1 アクティブなポリシーに HTTP を有効または無効にするルールを追加します。

```
switch:admin> ipfilter --addrule DS_ipv4 -rule 4 -sip any -dp 80 -prot tcp -act permit
```

-rule	ルール番号を指定します。この例では4番目にルールを追加しており、既存の4番以降のルールは番号が繰り下がります。
-sip	送信元IPアドレスを指定します。
-dp	宛先ポート番号、ポート番号の範囲、またはサービス名を指定します。HTTPのポート番号は80です。

-prot	プロトコルタイプ（tcpやudpなど）を指定します。
-act {permit | deny}	このルールに関連付けられたアクションを指定します。有効化する場合はpermit、無効化する場合はdenyを指定してください。

この時点での設定は以下のようになります。

```
switch:admin> ipfilter --show
: <<省略>>
Name: DS_ipv4, Type: ipv4, State: active (modified)
Rule    Source IP               Protocol     Dest Port   Action
1       any                             tcp        22      permit
2       any                             tcp        23        deny
3       any                             tcp        80        deny  既存のルール
4       any                             tcp        80      permit  追加したルール
5       any                             tcp       443      permit
6       any                             udp       161      permit
7       any                             udp       123      permit
8       any                             tcp   600 - 1023   permit
```

2 DS_ipv4 ポリシーから、HTTP について定義された既存のルールを削除します。

```
switch:admin> ipfilter --delrule DS_ipv4 -rule 3
```

3 DS_ipv4 ポリシーが更新されたことを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: DS_ipv4, Type: ipv4, State: active (modified)
Rule    Source IP                               Protocol    Dest Port   Action
1       any                                            tcp        22     permit
2       any                                            tcp        23       deny
3       any                                            tcp        80     permit
4       any                                            tcp       443     permit
5       any                                            udp       161     permit
6       any                                            udp       123     permit
7       any                                            tcp   600 - 1023  permit
8       any                                            udp   600 - 1023  permit
```

4 DS_ipv4 ポリシーの activate を実行し、変更を反映します。

```
switch:admin> ipfilter --activate DS_ipv4
```

5 DS_ipv4 ポリシーへの変更が反映されたことを確認します。

```
switch:admin> ipfilter --show
: <<省略>>
Name: DS_ipv4, Type: ipv4, State: active
Rule    Source IP                                  Protocol    Dest Port   Action
1       any                                               tcp        22     permit
2       any                                               tcp        23       deny
3       any                                               tcp        80     permit
4       any                                               tcp       443     permit
5       any                                               udp       161     permit
6       any                                               udp       123     permit
7       any                                               tcp   600 - 1023  permit
8       any                                               udp   600 - 1023  permit
```

手順ここまで

HTTP を使い続ける必要がない場合、HTTP の使用が終了したら、同様の手順で HTTP を無効化してください。

```
switch:admin> ipfilter --addrule DS_ipv4 -rule 4 -sip any -dp 80 -prot tcp -act deny
switch:admin> ipfilter --delrule DS_ipv4 -rule 3
switch:admin> ipfilter --activate DS_ipv4
```

注 意

設定後に **configdefault -all** コマンドを実行した場合、デフォルトポリシー「default_ipv4/default_ipv6」の内容が **configdefault** 実行時のファームウェア版数により異なるため、HTTP が有効になることがあります。
継続して HTTP 接続が必要でない場合は、確認コマンドを実施のうえ、再度 HTTP を無効に設定してください。

S.3.3 HTTPS 証明書の確認／登録／削除手順

セキュリティ強化のため、推奨する HTTPS の使用に必要な証明書を確認および登録する手順について説明します。
証明書を登録済みの場合は本手順は不要です。
HTTP を使用する必要がある場合は、「HTTPS 証明書削除」が必要です。

重　要

HTTPS 証明書には有効期限が設定されています。お客様のセキュリティ運用ポリシーに従って、有効期限の更新作業を行ってください。

S.3.3.1 HTTPS 証明書の確認／登録手順

HTTPS 証明書の確認および登録する手順について説明します。

手 順

1 HTTPS 証明書の登録状況を確認します。

```
switch:admin> seccertmgmt show -cert https

No https switch certificate found                (*1)
```

*1: 証明書がないことを示しています。

2 HTTPS 証明書を登録します。

```
switch:admin> seccertmgmt generate -cert https    (*1)
Generating a new certificate will automatically do the following
1. Delete existing switch certificate(s).
2. Disable secure protocol HTTPS

Warning: Certificate generation is CPU intensive and can cause high CPU usage

Continue (yes, y, no, n): [no] y                  (*2)
Generating ... ...Generated self-signed https certificate successfully.
switch:admin>
```

*1: 「-years」オプションで有効期限（年数）を指定できます。
例：-years オプションで有効期限（3 年）を指定する場合
switch:admin> seccertmgmt generate -cert https -years 3
*2: 「y」を入力します。

3 HTTPS 証明書の登録状況を確認します。

「Period Of Validity」に期限が表示されます。

注 意

「Period Of Validity」が期限切れとなった場合、セキュリティ保護のため [MAPS-1021] および [MAPS-1020] のメッセージが記録され、mapsdb --show の「2 Switch Health Report」のステータスが HEALTHY から MARGINAL に変更されます。その場合は、HTTPS 証明書を再作成してください。
HTTPS 証明書の再作成後、HEALTHY へのステータス変更に最大 24 時間かかる場合があります。

```
switch:admin> seccertmgmt show -cert https

Issued To
    countryName               = US
    stateOrProvinceName       = California
    localityName              = San Jose
    organizationName          = org
    organizationalUnitName    = unit
    commonName                = 10.xxx.xxx.xxx
Issued By
    countryName               = US
    stateOrProvinceName       = California
    localityName              = San Jose
    organizationName          = org
    organizationalUnitName    = unit
    commonName                = 10.xxx.xxx.xxx
Period Of Validity
    Begins On                 Mar  7 06:00:22 2023 GMT
    Expires On                Mar  6 06:00:22 2025 GMT
Fingerprints
    SHA1 Fingerprint  A5:5C:84:29:90:4A:E0:50:34:F8:EF:D7:FF:19:F8:42:05:91:3E:9D
    SHA256 Fingerprint  28:D5:7C:32:68:4E:48:18:B3:28:CD:BD:83:00:19:C9:E0:CC:01:
66:BD:DA:F9:76:2A:3A:49:D1:22:4F:3A:69
Crypto Algorithm
    Signature Algorithm       sha256WithRSAEncryption
    Public Key Algorithm      rsaEncryption
    Public-Key                2048 bit
```

手順ここまで

S.3.3.2 HTTPS 証明書の削除手順

HTTPS 証明書を削除する手順について説明します。

手 順

1. HTTPS 証明書を削除（HTTP 使用可能）状態に戻す場合、以下のコマンドを実行します。

```
switch:admin> seccertmgmt delete -cert https
WARNING!!!

About to delete https switch certificate file(s)
This will disable secure protocol HTTPS

Continue (yes, y, no, n): [no] y                    (*1)
switch:admin>
```

*1: 「y」を入力します。

2. 証明書の登録状況を確認します。

```
switch:admin> seccertmgmt show -cert https

No https switch certificate found                   (*1)
```

*1: 証明書がないことを示しています。

手順ここまで

S.4 SNMPv1 有効／無効の設定手順

SNMPv1 を有効／無効にする手順について説明します。

手 順

1. スイッチにログインします。
2. 以下のコマンドを入力し、SNMPv1 を有効にします。

```
switch:admin> snmpconfig --enable snmpv1
```

3 以下のコマンドで設定を確認します。

```
admin> snmpconfig --show snmpv1
SNMPv1 community and trap recipient configuration:
  Community 1: public (ro)
    No trap recipient configured yet
  Community 2:
    No trap recipient configured yet
  Community 3:
    No trap recipient configured yet
  Community 4:
    No trap recipient configured yet
  Community 5:
    No trap recipient configured yet
  Community 6:
    No trap recipient configured yet
SNMPv1:Enabled                                          (*1)
```

*1: 「Enabled（有効）」になっていることを確認したら、SNMPv1 は使用できます。

4 SNMPv1 の使用が終了したら、以下のコマンドで SNMPv1 を無効にします。

```
switch:admin> snmpconfig --disable snmpv1
```

5 以下のコマンドで設定を確認します。

```
admin> snmpconfig --show snmpv1
SNMPv1 community and trap recipient configuration:
  Community 1: public (ro)
    No trap recipient configured yet
  Community 2:
    No trap recipient configured yet
  Community 3:
    No trap recipient configured yet
  Community 4:
    No trap recipient configured yet
  Community 5:
    No trap recipient configured yet
  Community 6:
    No trap recipient configured yet
SNMPv1:Disabled                                         (*1)
```

*1: 「Disabled（無効）」になっていることを確認したら、SNMPv1 は使用できません。

備 考

設定後に **configdefault –all** コマンドを実行した場合も、有効／無効の設定に影響はありません。

手順ここまで

付録 T

SFP 間欠故障監視

FC の経路が間欠故障状態になった場合、経路を冗長化しても切り替わりが正常に機能せず、システムダウンになる場合があります。そのため、間欠故障が発生した場合を想定し、その際のシステム全体の動作や業務影響の回避策を検討しておく必要があります。間欠故障の予兆監視を目的に、以下の方法で監視することが可能です。

注 意

この監視方法は、Fabric Vision 機能で行います。本機能のライセンスがない場合は、オプションライセンス（エンタープライズライセンスオプション：有料）を適用してください。

T.1 事前確認

以下に、事前確認の手順について説明します。

手 順

1 「G.1 事前確認（licenseshow, license --show / chassisshow）」(P.79) を参照して、Fabric Vision のライセンスがインストールされていることを確認します。

2 デフォルトポリシーの 1 つを使用してスイッチをモニタするように MAPS を簡単に設定できます。
監視 policy は、以下の 5 つがあります。上から 3 つの内どの Policy を使用するかをシステム管理者に確認します。
FOS v9.2.0 未満の場合は、dflt_always_active_policy は表示されません。
dflt_moderate_policy の使用を推奨します。
- dflt_aggressive_policy：最も厳しいしきい値が設定されている
- dflt_conservative_policy：最も余裕のあるしきい値が設定されている
- dflt_moderate_policy：上記 2 つの中間の厳しさのしきい値が設定されている
- dflt_base_policy：Fabric Vision ライセンスなしで監視できる機能に基づくルールが含まれている
- dflt_always_active_policy：重要なシステムリソースを管理するためのすべての既定のシステム規則が含まれている
このシステムポリシーは常にアクティブであり、カスタマイズまたは非アクティブ化することはできません。

手順ここまで

T.2 監視条件の設定

以下に、監視条件の設定手順について説明します。

手 順

1 以下のコマンドを使用して policy 設定を確認します。

```
switch:admin> mapspolicy --show -summary
        Policy Name                       Number of Rules
-------------------------------------------------------------
dflt_aggressive_policy            :               384
dflt_moderate_policy              :               388
dflt_conservative_policy          :               388
dflt_base_policy                  :                44
dflt_always_active_policy         :                 6

Active Policy is 'dflt_conservative_policy'. The policy 'dflt_always_
active_policy' always monitors the system.                              (*1)
```

*1: 現在設定されている policy 設定が表示されます。

2 以下のコマンドを使用して、しきい値に達した場合の設定を実施します。

```
switch:admin> mapsconfig --actions <actions_list>
```

通知のみの場合は以下を設定します。

```
switch:admin> mapsconfig --actions raslog,snmp,email
```

詳細は、『MAPS ユーザーズガイド』を参照してください。

3 以下のコマンドを使用して policy 設定を実施します。

```
switch:admin> mapspolicy --enable <policy>
```

dflt_moderate_policy の場合は以下を設定します。

```
switch:admin> mapspolicy --enable dflt_moderate_policy
```

4 以下のコマンドを使用して policy 設定を確認します。

```
switch_1:admin> mapspolicy --show -summary
      Policy Name                       Number of Rules
-------------------------------------------------------------
dflt_aggressive_policy            :               384
dflt_moderate_policy              :               388
dflt_conservative_policy          :               388
dflt_base_policy                  :                44
dflt_always_active_policy         :                 6

Active Policy is 'dflt_moderate_policy'. The policy 'dflt_always_active_
policy' always monitors the system.                                     (*1)
```

*1: 現在設定されている policy 設定が表示されます。

手順ここまで

Fabric Vision が未適用の場合

システム管理者が手動で監視して、発生条件により間欠故障を判断します。
監視項目は、CRC エラー発生回数および WARNING メッセージ発生回数です。
判断情報の取得、判断方法については以下のとおりです。

判断情報の取得について

監視項目について説明します。

- CRC エラー発生回数
  porterrshow 実行時の出力表示を記録します。
  スイッチの負荷が高くならないように記録間隔は 1 時間以上空けてください。
  本回数は累計回数となっています。
  - 確認例

```
porterrshow
         frames      enc    crc    ...
       tx     rx      in    err    ...
 0:     1.0g  1.6g    0      0(*1) ...
```

  *1: CRC エラーの値です。

- WARNING メッセージ発生回数
  errdump の確認、または通報されるメッセージで、以下のエラーコードの発生回数を監視します。

  [C4-1014], 3973, CHASSIS, WARNING, swd77,
  　Link Reset on Port S0,P4(35) vc_no=0 crd(s)lost=12 auto trigger.
  [XTUN-1997], 804, CHASSIS, WARNING, swd77,
  　FTRACE buffer 7 on slot 0 dp 0 has been triggered. (*1)

  *1: Brocade 78x0（エクステンションスイッチ）のみ監視対象です。

判断方法について

以下のいずれかに該当した場合、間欠故障と判断します。

- CRC エラー発生回数
  121 回／時間を超えた場合
- WARNING メッセージ発生回数
  1 回／時間を超えた場合

用語集

ストレージの基本用語について、本書で使用されている用語を中心に解説します。その他の用語は以下のリンクを参照してください。

https://www.fujitsu.com/jp/products/computing/storage/eternus/glossary/

E

E ポート

スイッチが接続されたポートです。

EX ポート

FC ルーティング機能が設定されたポートです。

F

F ポート

サーバ／ストレージが接続されたポートです。

FOS（Fabric OS）

スイッチのファームウェアの名称です。

G

G ポート

E ポート、F ポートの機能のいずれかをサポートするジェネリックポートです（例：G ポート固定設定されたポートは、L ポートとならない）。

I

ISL（Inter-Switch Link）

スイッチ間接続のカスケードのことです。

R

RSCN（Remote State Change Notification）

デバイスの追加／削除など、ファブリックのトポロジに変更があった際、状態変更通知（RSCN）と呼ばれるフレームを、同じ Zone メンバーのデバイスに対して送信します。RSCN を受け取ったデバイスは、ネーム・サーバに問い合わせることによって、どのデバイスに変更が生じたのかを知ることができます。

V

VE ポート（Storage Area Network）

FCIP 機能が設定されたポートです。

セ

セグメンテーション

設定に問題があるためにスイッチ同士を接続できない現象のことです。ドメイン ID が同じスイッチがあるファブリック同士を接続した場合や有効なゾーン設定が異なるスイッチ同士を接続した場合など、設定情報にコンフリクトがある場合に発生します。

タ

ダイレクタタイプ

複数のブレードスロットを備えたシャーシ型のスイッチのことです（例：Brocade DCX）。

フ

ファブリック

ISL により接続されたスイッチで構成されるエンティティのことです（Zone 設定はファブリック単位で動作します）。

ホ

ボックスタイプ

筐体とポートが一体になったボックス型のスイッチのことです（例：SN200 Model 140/600）。

Brocade series, ETERNUS SN200 series
ユーザーズガイド 導入／運用（基本）編

P3AM-1862-36Z0

発行日　2024 年 4 月
発行責任　富士通株式会社

FUJITSU