CA92276-8601-02

PRIMERGY

ファイバーチャネルスイッチブレード（8Gbps 18/8）(PG-FCS104)

Access Gateway 管理者ガイド

Fabric OS v6.2.0

FUJITSU

53-1001189-01
2008 年 11 月 24 日

アクセス・ゲートウェイ

管理者用ガイド

Fabric OS 6.2.0 サポート

ブロケード

注意: 本書は情報提供のみを目的としており、明示的・黙示的を問わず、ブロケード社が提供する装置、装置の機能、またはサービスについて保証を定めるものではありません。ブロケード社は事前予告無しに本書に随時変更を行う権利を保有し、その使用について免責されます。この情報文書は現在は利用不可の可能性がある機能を説明しています。 機能と製品の可用性に関する情報はブロケード営業所にお問い合わせください。
本書に含まれる技術データの輸出は米国政府による輸出許可を必要とする場合があります。

著者とブロケード・コミュニケーションズ・システムズ社はこの書籍またはこれに付随する計算機プログラムに含まれる情報を起因とするいかなる損失、費用、負債または損害に関していかなる人格または事業体からも債務または責務を免責されます。

本書に説明される製品は GNU 一般公有使用許諾またはその他のオープンソース使用許諾契約の対象となる"オープンソース"ソフトウェアを含むことがあります。どのオープンソース・ソフトウェアがブロケード製品に含まれるかを知るため、そのオープンソース・ソフトウェアに適用される使用許諾条件を読むため、当該プログラミング・ソースコードのコピーを得るためには、次のウェブサイトをご覧ください: *http://www.brocade.com/support/oscd*.

ブロケード・コミュニケーションズ・システムズ社

Corporate Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
Email: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Singapore Pte. Ltd.
30 Cecil Street
#19-01 Prudential Tower
Singapore 049712
Tel: +65-6538-4700
Fax: +65-6538-0302
Email:apac-info@brocade.com

European and Latin American Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
Email: emea-info@brocade.com

文書更新履歴

次表にアクセス・ゲートウェイ管理者用ガイドの全バージョンをまとめました。

文書の表題	出版番号	変更内容の要約	出版日
アクセス・ゲートウェイ管理者用ガイド	53-1000430-01	初版	2007.1
アクセス・ゲートウェイ管理者用ガイド	53-1000633-01	200Eサポートの追加	2007.06
アクセス・ゲートウェイ管理者用ガイド	53-1000605-01	新たなポリシーのサポート およびN_Portマッピング変更追加	2007.10
アクセス・ゲートウェイ管理者用ガイド	53-1000605-02	新プラットフォームの サポート追加 300 および 4424 新機能サポートの追加: マスターレス・トランキング ダイレクト・ターゲット接続 高度デバイス・セキュリティ・ポリシー 16 ビット・ルーティング	2008.03
アクセス・ゲートウェイ管理者用ガイド	53-1000605-03	次項目のサポート追加: カスケード型アクセス・ゲートウェイ	2008.07
アクセス・ゲートウェイ管理者用ガイド	53-1000605-04	目次修正による更新	2008.07
アクセス・ゲートウェイ管理者用ガイド	*53-1001189-01*	FOS6.2 のための更新	2008.11

目 次

図

表

本書について

本書の構成

本書は SAN 管理者がブロケード･アクセス･ゲートウェイを構成および管理するための手順書です。

この前書きには次の項目があります:

- 第 1 章 “はじめに” アクセス・ゲートウェイを使用してストレージ･エリア･ネットワーク(SAN)ファブリックへのシームレスな接続性を生成する方法を説明します。
- 第 2 章, “アクセス・ゲートウェイ・モードのスイッチ・ポリシーを有効化する”はアクセス・ゲートウェイ・モードにあるスイッチでのポリシーを説明します。
- 第 3 章, “アクセス・ゲートウェイを使用してデバイスを接続する”はアクセス・ゲートウェイを使用して複数のデバイスを接続する方法を説明します。
- 第 4 章, “アクセス・ゲートウェイ・モードにポートを構成する”はポートをアクセス・ゲートウェイ・モードに構成する方法を説明します。
- 付録 A, “問題解決法”は症状と問題を解決するためのヒントを提供します。

サポートされるハードウェアとソフトウェア

ブロケード・コミュニケーションズ・システムズ社では多種多様なソフトウェアとハードウェアの構成を試験しサポートしてはいますが、バージョン 6.2.0 についてすべての考えうる構成とシナリオを文書化するのは本書の範囲を超えます。Fabric OS はすべて v5.1 以降を実行していること、M-EOS スイッチはすべ
て M-EOSx 9.1 以降を実行していること、M-EOSn は 9.6.2 以降を実行していること、SAN OS による
Cisco・ベースのスイッチは 3.0(1)と 3.1(1)以降を実行していることが必要です。アクセス・ゲートウェイは 4Gbps と 8Gbps のブレード･サーバとブレードに対応します。

本書から新たに取上げられた項目

本書の直前のバージョンからの変更点を以下に一覧します:

追加された情報:

- サポートされるソフトウェア
  - M-EOSc製品: バージョン 9.1 以降とバージョン 9.6 以降
  - Cisco製品 :: SAN-OS 3.0(1) 以降と 3.1(1) 以降
- サポートされるプラットフォーム
  - Brocade 300 (24 ポート・バージョンのみ), 5100
  - ファイバーチャネル・スイッチブレード : 5410, 5424, 5480
- サポートされるカスケード型アクセス・ゲートウェイの構成

詳細はリリースノートを参照ください。

文書の表記規則

この節は本文のフォーマット規則と重要な注意事項のフォーマットを説明します。

本文のフォーマット

本書で使用される説明文フォーマットの表記規則は次に従います:

太字	コマンド名に使用します 使用者が操作するグラフィカル・ユーザー・インターフェイスの構成要素の名前に使用します 重要な単語とオペランドに使用します グラフィカル・ユーザー・インターフェイスまたはコマンドラインインターフェイスに入力する文字列に使用します
*斜体*文字	強調に使用します 変数に使用します パスとインターネット・アドレスに使用します 文書名に使用します
コード文	コマンドラインインターフェイスの出力に使用します シンタックスの例を識別します

読み易いように、このガイドの説明に使用するコマンド名には大文字・小文字を組合わせて使用します: たとえば、**switchShow。** 実例ではコマンドのケースはすべて 小文字を使用します。 それ以外の場合は、この説明書はコマンドが大文字と小文字の 区別を要する場合、それに応じて表記します。 **ficon CupSet** と **ficonCupShow** コマンドはこの規則の例外です。

コマンド構文の規則

この説明書で用いるコマンド構文の規則は次の内容です:

コマンド	コマンドは太字で記載されます。
--オプション，オプション	コマンド・オプションは太字で記載されます。
-引数，引数	引数.
[ ]	オプション要素。
変数	変数は斜体で表記されます。ヘルプページでは値は下線を付されるか、山括弧< >.で囲まれます。
...	直前の要素の繰り返し、たとえば“要素[;要素...]”
値	引数に続く固定値は普通のフォントで記載されています。 たとえ　ば、--**show** WWN
|	ブール論理。 要素は相互排他的です。例： --**show** -**mode**egress（出口モード）| ingress（入口モード）

Notes, cautions, and warnings

本書では以下の注意書きを用います。

NOTE

NOTE はヒント、ガイダンスまたはアドバイス、重要な情報の強調、また関連情報への参照を表示します。

ATTENTION

ATTENTION 文はハードウェアやデータへの潜在的な損害を示唆します

CAUTION

CAUTION 文は潜在的に危険な、もしくはハードウェア、ファームウェア、ソフトウェア、またデータへの損傷を引き起こす可能性がある状況を警告します。

DANGER

DANGER 文は生命を脅かす恐れがある、またはきわめて危険となる状態または状況を示唆します。安全ラベルも当該状態や状況を警告するために製品に直接貼られています。

重要な用語

ストレージ・エリア・ネットワークに固有の用語の定義については、次のウェブサイトでストレージ・ネットワーキング業界団体SNIAのオンライン辞書をご利用ください: *http://www.snia.org/education/dictionary*.

ブロケードとファイバーチャネルに固有の用語定義は*ブロケード用語集*を参照ください。

次の用語をこの説明書では使用してアクセス・ゲートウェイ・モードとそのコンポーネントを記述します。

アクセス・ゲートウェイ(AG)	
	NPIV(N_Port ID 仮想化機能)を利用することにより、SAN(ストレージ・エリア・ネットワーク)を展開する上での複雑性を軽減するスイッチのためのFabric OSのモード。
E_Port	ISL (インタースイッチ・リンク)ポート. スイッチをまとめて接続してファブリックを形 成するスイッチ・ポート。
エッジ・スイッチ	ホスト、ストレージ、または、ブロケード・アクセス・ゲートウェイ等の他のデバイスをファブリックに接続するファブリック・スイッチ。
F_Port	ファブリック・ポート。 SANにホスト、HBA(ホスト・バス・アダプタ)、またはストレージ・デバイスを接続するスイッチ・ポート。 ブロケード・アクセス・ゲートウェイでは、F_Portはホストまたはターゲットに接続します。
マッピング	ブロケード・アクセス・ゲートウェイでのF_PortからN_Portへのルートの構成。
N_Port	ノード・ポート。ファブリックまたは 2 点間接続におけるファイバーチャネル・ホストまたはストレージ・ポート。 ブロケード・アクセス・ゲートウェイでは、N_Portはエッジ・スイッチに接続します。
NPIV	N_Port IDの仮想化。. 1 個のファイバーチャネル・ポート を複数の区別されたポートのように見せて、ポートの識別とオペレーティング・システム・イメージ毎に専用の物理ポートを持つかの様にファブリック内のセキュリティ・ゾーニングをできるようにする。
優先セカンダリN_Port	ブロケード・アクセス・ゲートウェイでは、優先副N_Portとはプライマリ N_Portがオフライン になった場合F_Portがフェイル・オーバーするための予備チャネルを意味します。

読者への注記

本書は次の各企業の商標を参照する場合があります。 当該商標は各会社や企業の財産です。

これらの参照事項は情報提供のためにのみなされています。

企業	参照される商標と製品
Cisco Systems	Cisco
Emulex Corporation	Emulex
Qlogic Corporation	Qlogic

補足情報

この節はお役に立つと思われるブロケードおよび業界固有の追加資料を一覧しています。

ブロケードの情報源

最新情報を入手するにはブロケード･コネクトに登録してください。 登録無料です！ *http://www.brocade.com* から登録できます。ブロケード･コネクトをクリックして、無料登録し、ユーザー名とパスワードを取得できます。

SANの設計について実務的テーマは、アマゾンのウェブサイトから入手できる *ブロケード･ファブリック･スイッチによるSANの構築* で取上げられています。

http://www.amazon.com

ブロケードの追加資料については、Brocade SAN Info Center へ進み、Resource Library の場所をクリックします:

http://www.brocade.com

リリース･ノートはブロケード･コネクトのウェブサイトで取得できるほか、Fabric OS ファームウェア にも添付されます。

業界のその他情報源 .

- 次のブロケード･ウェブサイトから入手できる白書、オンライン･デモ、データシート。
  http://www.brocade.com/support/oscd
- ブロケードの提携各社ウェブサイトから入手できる成功例ガイド、白書、データシート、その他の資料。

追加的な情報源に関する情報は、技術委員会T11 のウェブサイトをご覧ください。 このウェブサイトはファイバーチャネル、ストレージ管理、その他のアプリケーションのために高性能大容量ストレージ･アプリケーションのインターフェイス規格を紹介しています:

http://www.t11.org

ファイバーチャネル業界についての情報は、ファイバーチャネル協議 会のウェブサイトをご覧ください:

http://www.fibrechannel.org

ブロケードのオプション機能

ブロケードのオプション機能リストやその説明は、*Fabric OS 管理者用ガイド*を参照ください。

技術的補助を受けるには

製品の修理や部品注文を含め、ハードウェア、ファームウェア、ソフトウェアのサポートについては担当スイッチのサポート納品業者までご連絡ください。電話受付処理の効率化のため、次の情報を準備してください:

1. 一般情報
   - 該当する場合はテクニカル･サポートの電話番号
   - スイッチの型式
   - スイッチのオペレーティング･システムの版
   - 受信されたエラー番号とエラー内容についての説明
   - **supportSave** コマンドの出力

- 問題発生直後のスイッチないしファブリックの動作を含め問題の詳細な記述と個別の質問内容
- すでに実施された問題解決法の手順とその結果の内容
- シリアル・コンソールと Telnet のセッション記録
- シスログ・メッセージの記録

2. スイッチのシリアルナンバー

   スイッチのシリアルナンバーとそれに対応するバーコードは次の図のようにシリアルナンバー・ラベルに記載されています。

   シリアルナンバー・ラベルの場所:

   - Brocade 200E—シャーシのポートが無い側
   - ブロケード 300、4100、4900、5100、 5300、 7500、ブロケード・エンクリプション・スイッチ—左側ポート側にあるシャーシ内部に位置するスイッチ ID 引き出しタブ
   - ブロケード 5000—スイッチのポート側の株に位置するスイッチ ID 引き出しタブ
   - ブロケード 7600—シャーシ底面
   - ブロケード 48000—シャーシ内部電源ベイの横
   - ブロケード DCX—シャーシのポート側の右底
   - ブロケード DCX-4S—シャーシの右底部のポート側、線管理アセンブリの真上

3. World Wide Name (WWN)

   wwn コマンドでスイッチの WWN を表示できます。

   wwn コマンドをスイッチ故障のために使用できない場合、WWN はブロケード DCX を除きシリアルナンバーと同じ場所にあります。ブロケード DCX では、シャーシのポートが無い側の上部にあるブロケードのロゴ板をはがすと番号が書かれた WWN カードがあります。

文書に関する意見

ブロケードでは品質に常に取組んでおり、本書は正確性と完璧性を維持するように最善の努力を払いました。しかし、誤記、省略を発見したり、さらに詳細な説明が必要と考えられるテーマについてご意見をお寄せください。

送り先:

documentation@brocade.com

文書の表題とバージョン、可及的に詳しいご意見、項目の表題とその該当ページ、改善のためのご意見を記載してください。

1章
はじめに

この章の内容

ブロケード・アクセス・ゲートウェイ

この章はアクセス・ゲートウェイ(AG)を使用してどのストレージ・エリア・ネットワーク(SAN)でもシームレスに接続する方法を説明します。安定的ファブリックを得るためにポート・タイプ、ポート・マッピング、そしてポリシーを設定する方法を説明します。

アクセス・ゲートウェイはFabric OS、M-EOSv9.1 またはv9.6 以降、Cisco・ベースのファブリックv3.0(1) 以降および v3.1(1)以降と互換性があります。 コマンド・ライン・インターフェイス(CLI)またはWeb Tools、Fabric ManagerまたはDCFMから、スイッチのアクセス・ゲートウェイ・モードを有効化/無効化できます。本書はCLIコマンドを使用する構成を説明します。 これらのツールのアクセス・ゲートウェイ・サポートについて詳細は、Web Tools管理者用ガイド、Fabric Manager管理者用ガイド、Data Center Fabric Manager取扱説明書をご覧ください。

ブロケード・アクセス・ゲートウェイはFabric OSの一機能であり、ドメインの代わりに追加的N_Portを操作することにより、エンタープライズ・ファブリックを 構成します。この構成はF_PortをN_Portとしてファブリックに接続するように構成して行います。これにより 1 つのファブリックに接続できるデバイス・ポート数を増加できます。複数のアクセス・ゲートウェイがDCXエンタープライズ・プラットフォーム、ダイレクタ、そしてスイッチに接続できます。

Fabric OSスイッチをアクセス・ゲートウェイ・モードに設定後は、F-PortはE_Portとしてではなく、N_Portとしてエンタープライズ・ファブリックに接続します。 Fabric OSスイッチがネイティブ・スイッチ・モードであればF_PortはE_portとして接続します。図 1 は 8 つのホストをファブリックに接続する構成のAGを使用した場合と、同じ構成のネイティブモードのFabric OSスイッチを使用した場合の比較です。

アクセス・ゲートウェイ・モードのスイッチはホストとファブリックに対して論理透過的です。スイッチを増やすことなく、ファブリックにアクセスできるホストの数を増加できます。このためドメインIDとポートの数が削減されるので大規模ファブリックでの構成と管理が簡素化されます。

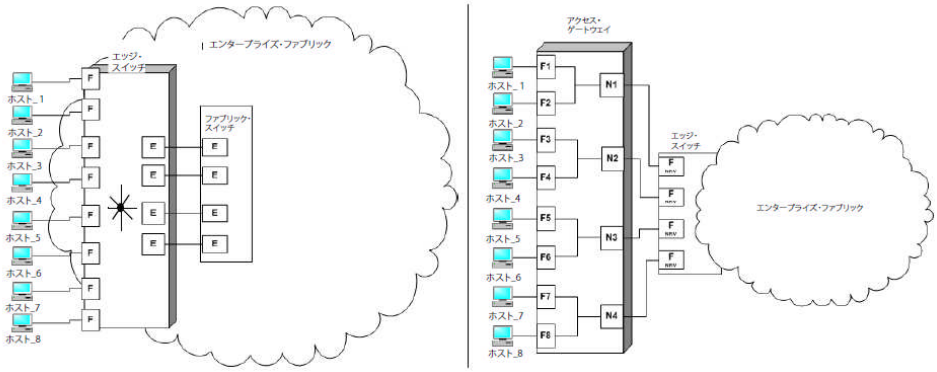

図 1 アクセス・ゲートウェイとファブリック・スイッチの比較

以下でネイティブ・モードのFabric OSスイッチとアクセス・ゲートウェイ・モードでのFabric OSスイッチの相違点をまとめました。

- ネイティブ・モードのFabric OSスイッチはファブリックの一部です。
  アクセス・ゲートウェイ・モードでのFabric OSスイッチより 2 倍から 4 倍多い物理ポートを必要とし、ファブリック資源をそれだけ消費するうえ、Fabric OSファブリックにしか接続できません。
- アクセス・ゲートウェイ・モードのスイッチはファブリックの外部にあります。このためファブリック内部のスイッチの数と必要な物理ポートの数を削減します。アクセス・ゲートウェイ・スイッチをどのFabric OS、M-EOSまたはCisco・ベースのファブリックにも接続できます。

アクセス・ゲートウェイモードでの Fabric OS の機能

スイッチがアクセス・ゲートウェイとして動作する場合、Fabric OSのRBAC機能は利用できますが、次の各機能は利用できないか、適用不可です：管理ドメイン、Advanced Performance Monitoring、SANターゲット・デバイスへの直接接続、ファイバーチャネル・アービトレイテド・ループ・サポート、FICON、IP over FC、拡張ファブリック、管理プラットフォーム・サービス、ネーム・サービス（SNS）、ポート・ミラーリング、SMI-S、ゾーニング。

図 1 はアクセス・ゲートウェイ・モードが有効化されているときにスイッチでサポートされるFabric OSのコンポーネントを示します。 "無" の意味は該当する機能がアクセス・ゲートウェイ・モードでは提供されないことです。"NA"の意味は該当する機能はアクセス・ゲートウェイ・モードに適用されないことです。星マーク 1 個（*）の意味は該当する機能はアクセス・ゲートウェイに透過的であること、すなわちアクセス・ゲートウェイが要求をエンタープライズ・ファブリックに転送することです。星マーク 2 個（**）の意味はエンタープライズ・ファブリックがブロケードのファブリックでない場合、当該機能は利用できないことです。

セキュリティの強制はDCCポリシーまたは高度デバイス・セキュリティ（ADS）ポリシーを使用するアクセス・ゲートウェイ・モジュールを使用するエンタープライズ・ファブリック内で行われます。ADSポリシーはSANへの仮想接続と物理接続を保護します。デフォルトでADSポリシーを有効化すると、すべてのF_Portはすべてのデバイスがログインできるまたはアクセス・リストの一部に許可するように構成されます。Allow Listは特定のF_Portにログインできるデバイスを限定します。WWNすべてがアクセス・リストの一部であるため、どのデバイスにF_Port毎のログインを許可するかは当該デバイスのポートWWN(PWWN)を指定すれば識別できます。"Allow List"をAll AccessまたはNo Accessに設定するため、ファブリック・コマンドライン・リファレンスを参照しag –adssetコマンドを使用してください。 またはエンタープライズ・ファブリックでセキュリティ・ポリシーを設定できます。ADSポリシーの詳細は、10 ページの"ADSポリシーが有効化されている場合にデバイス・ログイン許可を設定する"または 11 ページの"ADSポリシーが有効化されている場合にデバイス・ログイン拒否を設定する"を参照ください。

表 1 アクセス・ゲートウェイでサポートされる Fabric OS のコンポーネント

機能	サポート状況

アクセス制御	有（機能限定）
オーディット	有
ビーコン	有
構成のダウンロード/アップロード	有
DHCP（動的ホスト構成プロトコル）	有
環境監視	有
エラー・イベント管理	有
拡張ファブリック	無
ファブリック・デバイス管理インターフェイス（FDMI）	有*
Fabric Manager	有**
Fabric Watch	有（機能限定）
FICON（CUPを含む）	無
高可用性	ホット・コード・ロード
IPオーバー・ファイバー・チェネル	有*
ネイティブ相互運用モード	NA
ライセンス	有**
ログ追跡	有
管理サーバ	NA
ハードウェア診断	有
N_Port IDの仮想化(NPIV)	有
ネーム・サーバ	NA
ネットワーク・タイム・プロトコル(NTP)	無(ファブリックから見て関連性無し。ファイバーチャネル・スイッチブレードでは、時間はサーバ管理ユーティリティが更新しなければなりません。
開いたE_Port	NA
性能監視	有(PMのみ、APMはサポート無)
ポート・ミラーリング	無
QuickLoop、QuickLoop Fabric Assist	無
セキュリティ	部分的（ADSとDCCポリシー）
SNMP	有
速度のネゴシエーション	有
トランキング	有**
ValueLineオプション（静的POD, DPOD）	有
WebTools	有
ゾーニング、管理ドメイン	NA

アクセス・ゲートウェイのポート・タイプ

アクセス・ゲートウェイはアクセス・ゲートウェイ・コマンドを使用してスイッチに有効化するモードであり、スイッチではない点で典型的なファブリック・スイッチと異なります。スイッチをアクセス・ゲートウェイ・モードに設定後は、ノード・ポート(N_Port)を使用してファブリックに接続できます。 典型的なファブリック・スイッチはE_Port等のISL（インタースイッチ・リンク）ポートを使用してエンタープライズ・ファブリックに接続します。

以下はアクセス・ゲートウェイが使用するファイバーチャネル(FC)ポートです：

- **F_Port** – ホスト、HBA、またはストレージ・デバイスをアクセス・ゲートウェイ・モードにあるスイッチに接続するファブリック・ポート。
- **N_Port** – ファブリック・スイッチのF_Portにアクセス・ゲートウェイ・モードにあるスイッチを接続するノード・ポート。

アクセス・ゲートウェイ・ポートの標準スイッチ・ポートとの比較

アクセス・ゲートウェイはファブリックへのホスト接続を多重化します。アクセス・ゲートウェイはF_Portをホストに、N_Portをエッジ・ファブリック・スイッチに提供します。 N_Port IDの仮想化(NPIV)を使用して、アクセス・ゲートウェイは多数のファイバーチャネル・イニシエータが同じ物理ポートでSANにアクセスすることを可能にします。このためSAN接続のためにホストのハードウェア要件と管理オーバーヘッドを削減します。

ファブリック・スイッチはF_Port　(or FL_Ports)とストーレジ・デバイスをホストに提供し、ファブリック内の他のスイッチにはE_Ports, VE_Ports, or EX_Portを提供します。ファブリック・スイッチはドメインID等のSAN資源を消費し、ファブリック管理とゾーニングの配分に参加します。ファブリック・スイッチは同数のホストに接続するためにアクセス・ゲートウェイより多くの物理ポートを必要とします。

図 2 アクセス・ゲートウェイ・モードのポート・タイプと標準ファブリック・スイッチが使用するポート・タイプを比較します。

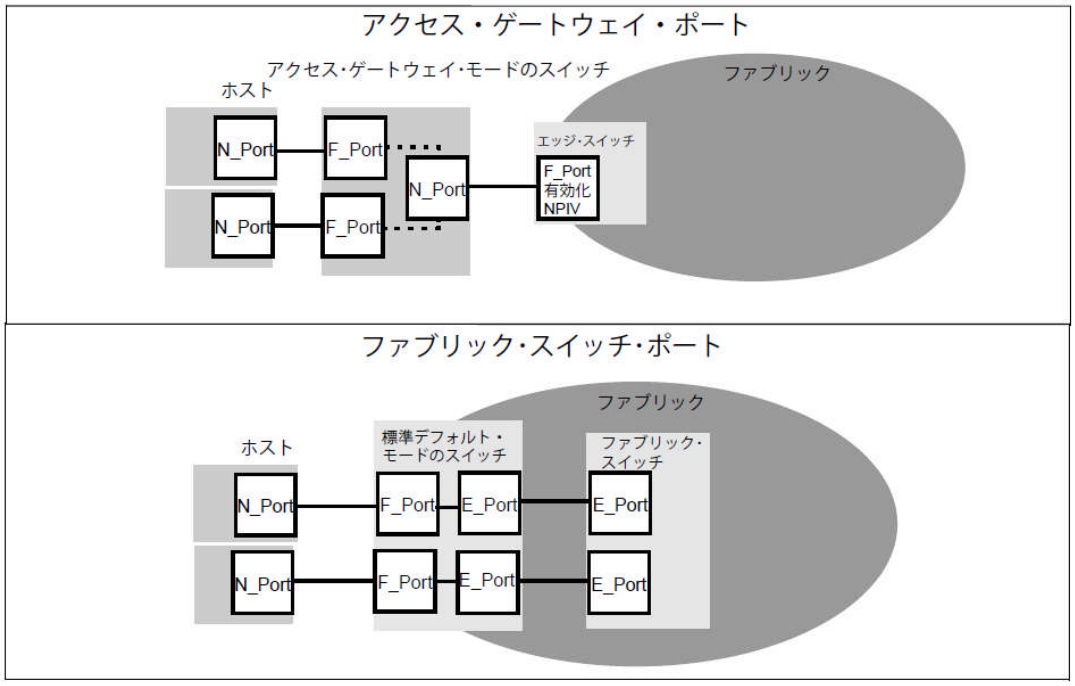

図 2　ポート使用状況の比較

表 2 はアクセス・ゲートウェイによるポート構成の標準ファブリック・スイッチとの比較を示します。

表 2 ポートの構成

ポート・タイプ	アクセス・ゲートウェイ		ファブリック・スイッチ	
F_Port	Yes	ホストとターゲットをアクセス・ゲートウェイに接続。	Yes	ホスト、HBA、ストレージ等デバイスをファブリックに接続。
N_Port	Yes	アクセス・ゲートウェイをファブリック・スイッチに接続。	NA	N_Portはサポートしない。
E_Port	NA	ISLはサポートされない。[1]	Yes	スイッチを他のスイッチと接続してファブリックを形成。

1. スイッチはファブリックに対して論理透過的なので、ファブリック・スイッチとしてSANには参加しません。

アクセス・ゲートウェイがポートをマップする方法

アクセス・ゲートウェイはマッピング －すなわち、プレ・プロビジョン・ルート－ を使用して、ホストからのトラフィックをファブリックに向かわせます。最初にアクセス・ゲートウェイ・モードにスイッチを有効化すると、デフォルトでは、F_Portは定義済みのN_Portセットにマップされます。デフォルトのF_PortからN_Portへのマッピングについては、53 ページの表 11 をご覧ください。必要に応じてデフォルト・マッピングを自分で変更できます。図 3 はアクセス・ゲートウェイ・モードのスイッチで 8 個のF_Portを等しく 4 個のN_Portにマップするマッピングを示します。N_Port は異なるエッジ・スイッチを通して同じファブリックに接続します。

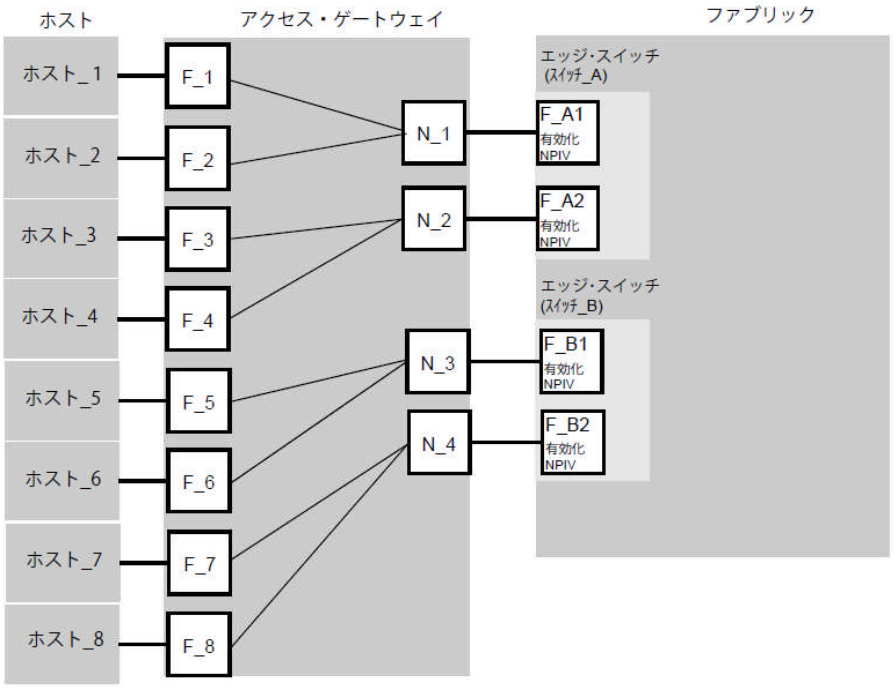

図 3 F_Port から N_Port へのマッピング例

表 3 F_Port から N_Port へのマッピング内容

アクセス・ゲートウェイのポート・タイプ

アクセス・ゲートウェイ		ファブリック・ウォッチ	
F_Port	N_Port	エッジ・スイッチ	F_Port
F_1, F_2	N_1	スイッチ_A	F_A1
F_3, F_4	N_2	スイッチ_A	F_A2
F_5, F_6	N_3	スイッチ_B	F_B1
F_7, F_8	N_4	スイッチ_B	F_B2

アクセス・ゲートウェイの制限

アクセス・ゲートウェイの制限は以下の内容です:

- xiiiページにリストされている“サポートされるハードウェアとソフトウェア” のスイッチ・プラットフォームとファイバーチャネル・スイッチ・プラットフォームに限定されます。
- エッジ・スイッチに最大 30 個のアクセス・ゲートウェイしか接続できません。
- Fabric OSスイッチにアクセス・ゲートウェイを通して接続できるデバイスの最大数は Fabric OSがサポートするローカル・デバイスの 最大数に依存します。
- アクセス・ゲートウェイはループ・デバイスをサポートしません。

アクセス・ゲートウェイ・モードのスイッチのアップグレードとダウングレードの検討

Fabric OS v6.1.0 以前のバージョンへのダウングレードはサポートされますが、アクセス・ゲートウェイ・モードを無効化してからでないとできません。Fabric OS v6.2.0 からFabric OS v6.1.0 以前のバージョンへダウングレードする際、次のことを考慮してください。

- Fabric OS v6.0.0 以前のバージョンへのダウングレードは、F_Portトランクがア クティブの場合許可されません。
- Fabric OS v6.0.0 以前のバージョンへダウングレードする前にトランキングを無効化する必要があります。
- スイッチがアクセス・ゲートウェイ・モードに設定されているときに、v6.0.0xバージョンへダウングレードすると、すべてのユーザー設定フェイルオーバーは消去されます。

次表はFabric OSバージョンへのアップグレード/ダウングレードのシナリオを示します。

表 4 ファームウェアのアップグレードとダウングレードのシナリオ

ポリシー	Fabric OS v6.2 -> 6.1	Fabric OS v6.1 -> 6.2	Fabric OS v6.2 -> 6.0
ポート自動構成	有	有	有
ポートのグループ化	有	有	無
ポート・トランキング (トランク・メンバーがオフライン)	有	有	無
ポート・トランキング (トランク・メンバーがオンライン)	有	有	無
高度デバイス・セキュリティ・ポリシー	有	有	無

ブロケード・ポリシーを有効化するときに次のアップグレード/ダウングレード配慮事項に注意してください。

高度デバイス・セキュリティ・ポリシー

v5.2.1/v5.3.xからv6.2.0 へのアップグレードでは, ADSポリシーは無効化されます。 v6.0 以前のバージョンへのダウングレードは許可されますが、ADSを無効化してください。v6.1 へのダウングレードは許可され、ADSはサポートされます。

ポート自動構成ポリシー（APS）

Fabric OS v6.0.x以前のバージョンからFabric OS 6.2.0 へアップグレードする場合、デフォルトではAPCポリシーは無効化されます。v6.2.0 からv5.2.1 または 5.3.xバージョンへダウングレードするには、APCを無効化してください。

ポート・グループ・ポリシー

v5.2.1 またはv5.3.xから 6.2.0 バージョンへアップグレードする場合、ポート･グループ化ポリシーは、すべてのN_Portを含むデフォルト・ポート・グループpg0 で有効化されます。ポート･グループポリシーが有効化されている場合、Fabric OS 6.2.0 からFabric OS v6.0.0 へのダウングレードはできます。 v6.0.0 以前のバージョンへダウングレードするには、最初にポート・グループ化を無効化してから行ってください。

1 アクセス･ゲートウェイ･モードのスイッチのアップグレードとダウングレードの検討

2 章
アクセス・ゲートウェイ・モードのスイッチでポリシーを有効化する

この章の内容

アクセス・ゲートウェイ・ポリシー

この章はアクセス・ゲートウェイ・モードのスイッチにポリシーを有効化するための情報と手順を説明します。

ブロケードのポリシーに基づく手法で標準Fabric OSスイッチとアクセス・ゲートウェイ・モードのスイッチでのトラフィックを制限したりフィルターできます。アクセス・ゲートウェイ・モードのスイッチに次のポリシーを有効化できます:

- 高度デバイス・セキュリティ・ポリシー (ADS)
- ポート自動構成ポリシー(APS)
- ポート・グループ・ポリシー

現在のポリシーを表示する

スイッチに有効化または無効化されているポリシーを見るには次のコマンドを使用します。

1. スイッチに接続してadminでログインします。
2. ag --policyshow コマンドを入力します。

```
switch:admin> ag --policyshow
AG Policy Policy Name State
------------------------------------------------------------------------
Port Grouping                   pg      Enabled
Auto Port Configuration         auto    Disabled
Advanced Device Security        ads     Enabled
```

デバイスの高度セキュリティ(ADS)ポリシー

高度デバイス・セキュリティ・ポリシー(ADS)はアクセス・ゲートウェイのF_Portでサポートされます。 Fabric OS v6.2.0 はDCCポリシーをアクセス・ゲートウェイ・モードのスイッチに拡張して、セキュリティのレベルを高めます。これは物理F_PortにDCCポリシーを物理F_PortとF_PortでのNPIVログインに拡張して行われます。物理サーバはどんどん仮想化し始め、仮想サーバが脆弱化しやすくなり、セキュリティがサーバI/Oの仮想化と切っても切り離せない部分になっています。このセキュリティ・ポリシーは、AGモードのスイッチを通して接続されるファブリックへのログインを指定、または許可できるデバイス・セットへのファブリック接続性を制限する仕組みです。デフォルトでは、ADSポリシーは無効化されています。スイッチをアクセス・ゲートウェイ・モードに設定後は、ADSポリシーを有効化でき、次にF_Port毎にどのデバイスにログインを許可するか指定できます。

セキュリティ強制もエンタープライズ・ファブリックで行うことができ、エンタープライズ・ファブリックでのDCCポリシーはADSポリシーより優先されます。ADSポリシーを有効化すると、スイッチにあるすべてのポートに適用されます。 デフォルトでは、すべてのデバイスがすべてのポートでファブリックにアクセスできます。

高度デバイス・セキュリティ・ポリシーを有効化する

1. スイッチに接続してadminでログインします。
2. ag ーpolicyenable adsコマンドを入力します。

   switch:admin> ag --policyenable ads
   ADSポリシーは有効化されます。

高度デバイス・セキュリティ・ポリシーを無効化する

1. スイッチに接続してadminでログインします。
2. ag ーpolicydisable adsコマンドを入力します。

   switch:admin> ag --policydisable ads
   ポリシーADSが無効化されています。

ADS ポリシーが有効化されている場合、どのデバイスがログインできいかを設定する

デバイスのポート WWN(PWWN)を指定することにより、F_Port 毎にどのデバイスがログインを許可されるかを定義できます。Ag – –adsset コマンドにより指定された F_Port セットにログインを許可されるデバイスを定義
できます。リストは二重引用符で囲みます。リストはセミコロンで区切ります。許可デバイス・リストの最大エントリ数はポート毎の最大ログイン回数の 2 倍です。WWN リストをアステリスク(*)で置換して、指定された F_Port リストのすべてのアクセスを指示します。F_Port リストをアステリスク(*)で置換して、指定した WWN をすべての F_PortAllow List に追加します。空白の WWN リスト(“”)はアクセス無しを意味します。ADS ポリシーはこのコマンドが機能するには有効化されていなければなりません。

注
“*”ー引用符で囲んだアステリスクーを使用して Allow List を全ての F_Port に対して”AllAccess”に設定し、“”ー二重引用符対を使用して Allow List を”No Access”に設定します。

Allow Listの次の特性に注意してください。

- Allow Listに許可される最大デバイス・エントリ数はポート毎の最大ログイン回数の2倍です。
- 各ポートは“not allow any device”または“to allow all the devices”のオールOrナッシングのログイン条件で構成できます。
- ADSポリシーが有効化されている場合、デフォルトでは、各ポートはすべてのデバイスのログインを許可する構成です。

- 同じAllow Listは1個以上のF_Portに指定できます。

この例はポート1、10、13の許可デバイスを全アクセス可に設定する方法を示します。

1. スイッチに接続してadminでログインします。
2. ag ーadsset “1;10;13”“*”コマンドを入力します。

   switch:admin> ag--adsset“1;10;13”“*”
   WWN list set successfully as the Allow Lists of the F_Port[s]。

ADS ポリシーが有効化されている場合、どのデバイスがログインできないかを設定する

この例はポート11と12に許可されたデバイスをアクセス無しに設定する方法を示します。

1. デバイスの高度セキュリティ(ADS)ポリシー
2. ag ーadsset “11;12” “” コマンドを入力します。

   switch:admin > ag --adsset “11;12” “”
   WWN list set successfully as the Allow Lists of the F_Port[s]。

ログインで許可されたデバイス・リストからデバイスを削除する

ag --adsdel コマンドを使用して特定のF_Portへのログインを許可されたデバイス・リストから特定のWWNを削除します。リストは必ず二重引用符(")で囲んでください。リストのメンバーは必ずセミコロン(;)で区切ります。F_Portリストをアステリスク(*)で置換し、F_Portのすべての Allow Listから特定のWWNを削除します。このコマンドが成功するためにはADSポリシーが有効化されていなければなりません。

例えば、3 と 9 のポートに許可されたデバイス・リストから 2 個のデバイスを削除するには、次の構文を使います:

ag--adsdel "F_Port [;F_Port2;...]" "WWN [;WWN2;...]"

1. スイッチに接続してadminでログインします。
2. ag --adsdel “3;9“ ″22:03:08:00:88:35:a0:12;22:00:00:e0:8b:88:01:8b″コマンドを入力します。

   switch:admin> ag --adsdel ″3;9″

   ″22:03:08:00:88:35:a0:12;22:00:00:e0:8b:88:01:8b″

   WWNs removed successfully from Allow Lists of the F_Port[s]Viewing F_Ports allowed to login

ログインで許可されたデバイス・リストにデバイスを追加する

adsaddコマンドを使用して特定のF_Portへのログインを許可されたデバイス・リストに特定のWWNを追加します。リストは必ず二重引用符(")で囲んでください。リストのメンバーは必ずセミコロン(;)で区切ります。F_Portリストをアステリスク(*)で置換し、F_Portのすべての Allow Listに特定のWWNを追加します。このコマンドが成功するためにはADSポリシーが有効化されていなければなりません。

例えば、3 と 9 のポートに許可されたデバイス・リストに 2 個のデバイスを追加するには、次の構文を使います:

ag--adsadd ″F_Port [;F_Port2;...]″ ″WWN [;WWN2;...]″

1. スイッチに接続してadminでログインします。
2. ag --adsadd "3;9" "20:03:08:00:88:35:a0:12;21:00:00:e0:8b:88:01:8b" コマンドを入力します。

```
switch:admin> ag --adsadd "3;9"
"20:03:08:00:88:35:a0:12;21:00:00:e0:8b:88:01:8b"
WWNs added successfully to Allow Lists of the F_Port[s]
```

スイッチにデバイス・リストを表示する

1. スイッチに接続してadminでログインします。
2. ag --adsshowコマンドを入力します。

```
switch:admin> ag --adsshow
```

F_Port	WWNs Allowed
1	ALL ACCESS
3	20:03:08:00:88:35:a0:12 21:00:00:e0:8b:88:01:8b
9	20:03:08:00:88:35:a0:12 21:00:00:e0:8b:88:01:8b
10	ALL ACCESS
11	NO ACCESS
12	NO ACCESS
13	ALL ACCESS

ポート自動構成ポリシー（APC）

ポート自動構成ポリシー（APC）はアクセス・ゲートウェイのオプション・ポリシーで、デフォルトでは無効化されています。APCが有効化されると、アクセス・ゲートウェイ・モジュールは自動的にポート・タイプを発見します。 たとえば、アクセス・ゲートウェイ・モードのスイッチがポートに接続されると、アクセス・ゲートウェイはそのポートをN_Portとして構成します。ホストがアクセス・ゲートウェイのポートに接続されると、アクセス・ゲートウェイはその接続を検出して当該ポートをF_Portとして構成します。

すべてのポート・タイプが判断された後には、F_PortとN_portの動的マッピングが生成され、F_Portがすべての N_Portに均等に配分されます。APCが有効化されている間は、F_PortからN_Portのマッピングを手動で行うことはできません。

要注意

APCポリシーを有効化するとF_PortとN_Portの機能停止を伴います。APCポリシーを有効化する前に必ずモジュールを無効化してください。理由は、APCポリシーを有効化すると、現在のF_PortのN_Portマッピングが削除されるからです。APCポリシー強制によりスイッチの現在のポート・マッピングが消去されるので、APCポリシーを有効化する前にconfiguploadを実行することが推奨されます。APCポリシーの有効化後は、ポリシーは直ちに有効となり、再起動の必要はありません。APCポリシーを無効化する際は、N_Portの構成とF_PortからN_Portのマッピングは当該プラットフォームのデフォルト工場設定値に戻ります。

APCポリシーはポート・グループ化ポリシーと相互排他的です。APCポリシーが複数のファブリックに接続されたスイッチで有効化されると、N_Portが関連しないファブリックに接続されていてもフェールオーバー動作を制限する試行はアクセス・ゲートウェイにより行われません。アクセス・ゲートウェイが複数のファブリックに接続されているときはAPCポリシーを使用しないでください。

注

アクセス･ゲートウェイ･モードでは、MEOSスイッチに添付されている場合にはポート自動構成ポリシーは機能しないことがあります。 M-EOSポートはポート･タイプ発見の際の問題を防止するために、G_Portに設定する必要があります。FC8-48 ブレードの 16-47 ポートをアクセス･ゲートウェイF_Portトランキング接続に使用できません。

ポート自動構成ポリシーを有効化する

1. スイッチに接続してadminでログインします。
2. switchdisableコマンドを入力してスイッチを確実に無効化してください
3. ag --policyenable autoコマンドを入力してAPCポリシーを有効化します。

   switch:admin> **ag --policyenable auto**
   All Port related Access Gateway configurations will be lost.
   Please save the current configuration using configupload。
   Do you want to continue? (yes, y, no, n): [no] y
4. configuploadを入力してスイッチの現在の構成を保存します。
5. コマンドプロンプトでYをタイプしてポリシーを有効化します。

   スイッチの準備ができました。再起動は必要ありません。

ポート自動構成ポリシーを無効化する

1. スイッチに接続してログインします。
2. ag --policydisable autoコマンドを入力してAPCポリシーを無効化します。
3. コマンドプロンプトでYをタイプしてポリシーを無効化します。

   switch:admin> **ag --policydisable auto**
   Default factory settings will be restored.
   Default mappings will come into effect.
   Please save the current configuration using configupload.
   Do you want to continue? (yes, y, no, n): [no] y
   Access Gateway configuration has been restored to factory default.
4. switchenableコマンドを入力してスイッチを有効化します。

有効化された APC ポリシーで F_Port を再負荷分散する

APCポリシーが有効化されている場合、F_PortからN_Portの静的マッピングは無く、F_Portが特定のN_Portに結合することはありません。最初のマッピングの完了後にF_Portがオンラインになると、F_Portが全ての利用可能なN_Portにわたって、F_Portが均一に平衡を保たれるように、利用可能なN_Portの一つを通しての道順を自動的に決定します。同様に、最初のF_Port初期化後に新たなN_Portがオンラインになると、既存のN_Portを通して道順を作成中のF_Portの一部は再負荷分散が必要であれば新たなN_Portにフェールオーバーします。

注

F_Portの再分配による機能中断のため、モジュールに新たなN_Portを追加することが推奨されます。 N_Port の追加の詳細は、20 ページの “N_Portをポート･グループに追加する” を参照ください。

フェールオーバー・ポリシー

アクセス・ゲートウェイのフェールオーバーとフェールバック・ポリシーはサーバの稼働状態を最大限に確保できます。あるポートがN_Portとして構成されているとき、デフォルトでフェールオーバー・ポリシーが有効であれば、F_Port はN_Portがオフラインになっても無効化されません。任意のF_Portに優先セカンダリN_Portを指定した場合、
そのN_Portがオフラインになると、当該F_Portは優先副N_Portにフェールオーバーし、再有効化します。指定された優先副N_Portはオンラインでなければならず、オンラインでないとF_Portは無効化されます。

または、優先副N_PortがどのF_Portにも設定されていなければ、F_Portは同じN_Portグループに属する別のオンラインN_Portにフェールオーバーして、次に再有効化します。FLOGIとFDISCの要求はF_Portから新たなN_Portを通して転送されます。フェールオーバーの候補先として複数のN_Portが利用できる場合、アクセス･ゲートウェイは 1 個以上のN_Portを選ぶのでF_Portはすべてのに渡って均等に分散されます。

注

新たなN_PortへのF_Portフェールオーバーはメッセージを生成します。

フェールオーバー・ポリシーはプライマリN_Portがオフラインになるとホストが自動的にオンラインのN_Portに再マップすることを可能にします。フェールオーバー・ポリシーは起動中に有効化（または強制）されます。フェールオーバー・ポリシーは、オンラインのすべてのN_Portのなかからオフラインの N_Portにマップされる F_Portを均等に分散します。フェールオーバー・ポリシーは各N_Portのパラメータです。デフォルトでは、フェールオーバー・ポリシーはすべてのN_Portに有効化されています。

次にフェールオーバーが起きる様子を順に見ます。

- N_Portがオフラインになる。
- そのN_PortにマップされたF_Portはすべて無効化される。
- N_Portフェールオーバー・ポリシーが有効化されており、優先副N_PortがそのF_Portに指定され、このN_Portがオンラインであれば、このF_Portは対応する優先副N_Portにフェールオーバーして、再有効化される。

  注
  優先副 N_Port は F_Port 毎に定義されます。 たとえば、2 個の F_Port がプライマリ N_Port1 にマップされていれば、副 N_Port をこれらの F_Port の 1 個に定義して、もう 1 個の F_Port には副 N_Port を定義しないことができます。通常この操作はサーバ管理者が行います。優先セカンダリマップをサーバ毎にまたはサーバのサブセットのみに定義するかはサーバ管理者が決定しなければなりません。

- 優先副N_Portがオンライン状態でなければ、これらのF_Portは無効化されます。
- 優先副N_PortがどのF_Portにも設定されていなければ、F_Portは同じN_Portグループに属する別の利用可能なN_Portにフェールオーバーして、次に再有効化します。
- ホストはファブリックと新たに接続します。

例: フェールオーバー･ポリシー

この例は 2 個のファブリック･ポートが順にオフラインになるシナリオで、フェールオーバーが行われる様子を示します。 ここでは F_Port にはいずれも優先副 N_Port が設定されていないことを前提することに注意してください。

- エッジ･スイッチ F_A1 ポートが 15 ページ例 1（左）の図 4 に示すようにオフラインになり、対応するアクセス･ゲートウェイ・ポート N_1 が無効化されます。

  N_1 にマップされたポートがフェールオーバーします。F_1 は N_2 に、F_2 は N_3 にフェールオーバーします。

- 次にF_A2 ポートが 15 ページ例 2（右）の図 4 に示すようにオフラインし、対応するアクセス･ゲートウェイ･ポートN_2 が無効化されます。

  N_2 にマップされているポート（F_1、 F_3、F_4)は N_3 と N_4 にフェール･オーバーします。F_Port が 残りのオンライン N_Port に均等に配分され、ポート F_2 はフェール･オーバーには参加しなかったことに注意してください。

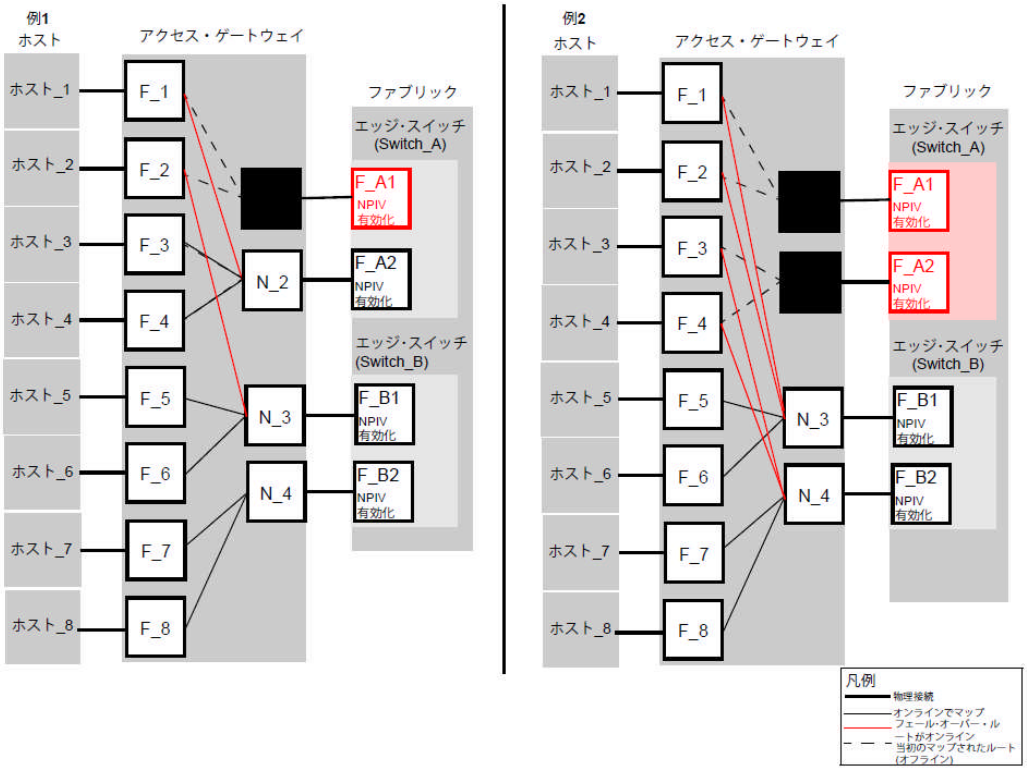

図 4 例 1 と 2 のフェール･オーバー･ポリシーの動作

フェール･オーバー･ポリシーを有効化する

1. スイッチに接続してadminでログインします。
2. agコマンドを --failovershow <n_portnumber> オペランド付きで入力し、フェール･オーバーの設定を表示します。

   switch:admin> ag --failovershow 13
   Failover on N_Port 13 is not supported

3. agコマンドを --failoverenable <n_portnumber> オペランド付きで入力し、フェール･オーバーを有効化します。

   switch:admin> ag --failoverenable 13
   Failover policy is enabled for port 13。

フェールオーバー・ポリシーを無効化する

1. スイッチに接続してadminでログインします。
2. agコマンドを --failovershow <n_portnumber> オペランド付きで入力してフェールオーバーの設定を表示します。

   switch:admin> **ag --failovershow 13**
   Failover on N_Port 13 is supported
3. ag --failoverdisable <n_portnumber> オペランドを入力してフェールオーバーを無効化します。

   switch:admin> **ag --failoverdisable 13**
   Failover policy is disabled for port 13。

フェールバック・ポリシー

フェールバック・ポリシーは、プライマリマップされたN_Portがオンラインに戻ると、N_Portへのフェールオーバー・ポリシーが有効化されていれば、F_PortをこれらのN_Portに自動的に再ルートします。

当初マップされたF_Portのみフェールバックします。複数のN_Portに障害が発生した場合、復活したN_Portにマップされた F_Portのみフェールバックします。残りのF_Portはフェールバックの際にオンラインのN_Portに再配分されません。APCポリシーが有効化されていれば、デフォルトではフェールバック･ポリシーは無効化されます。

注
フェールバック･ポリシーはN_Portのパラメータです。デフォルトでは、フェールバック･ポリシーは有効化されています。

次にフェールバックが起きる様子を順に見ます。

- N_Port がオンラインに復活すると、フェールバック･ポリシーが有効化されている場合、その N_Port に当初マップされた F_Port は無効化されます。
- この F_Port はマップされたプライマリ N_Port に再ルートされ、次に再有効化されます。
- ホストはファブリックと新たに接続します。

例: フェールバック・ポリシー

17 ページ図 5 例 3 では、アクセス･ゲートウェイ N_1 は、対応するポート F_A1 がオフラインなので無効化状態を維持します。しかし N_2 はオンラインに戻ります。15 ページ図 4 の当初のフェールオーバー・シナリオをご覧ください。

F_1 とF_2 ポートはN_1 にマップされ、N_3 へルーティングを続けます。N_2 に当初マップされたF_3 とF_4 ポートは無効化され、N_2 へ再ルートされてから有効化されます。

例 3

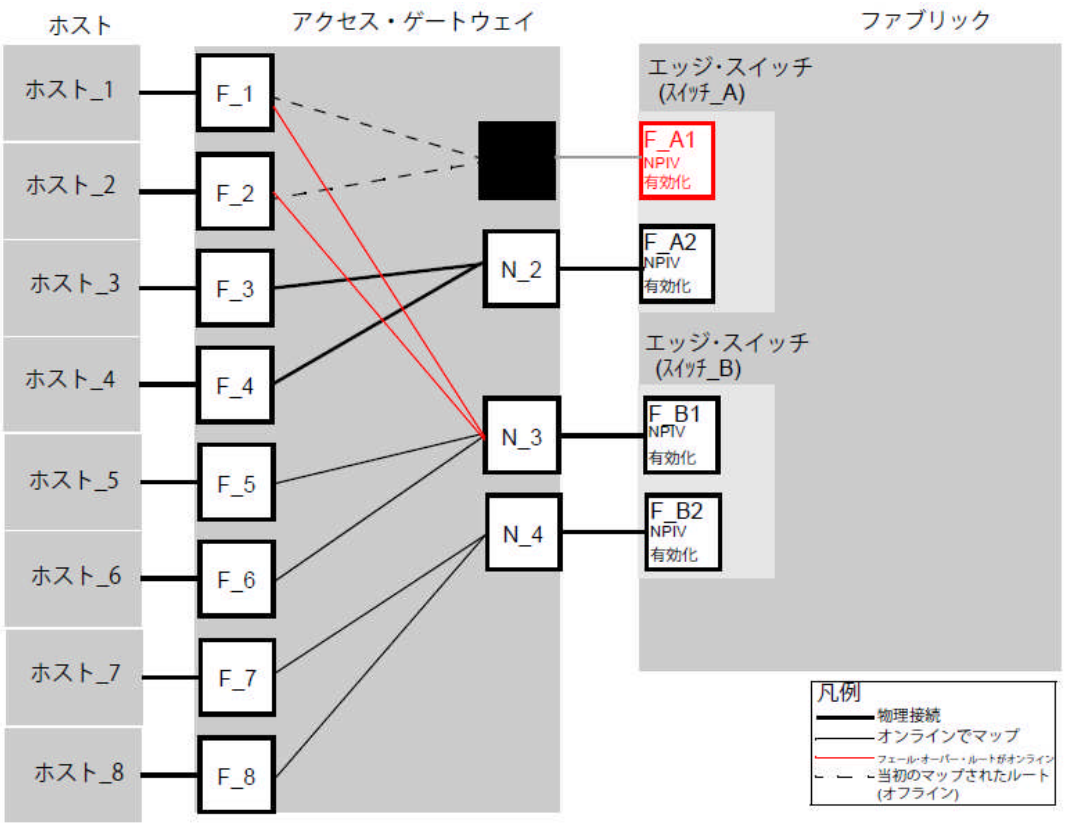

図 5 フェールバック・ポリシーの動作

フェールバック・ポリシーを有効化する

1. スイッチに接続してadminでログインします。
2. **ag —failbackshow**コマンドをn_portnumberオペランド付きで入力しフェールオーバー設定を表示します。
3. **ag —failbackenable**コマンドを<n_portnumber> オペランド付きで入力しフェールバックを有効化します。

   switch:admin> **ag —failbackenable 13**
   Failback policy is enabled for port 13。

フェールバック・ポリシーを無効化する

1. スイッチに接続してadminでログインします。
2. **ag —failbackshow**コマンドをn_portnumberオペランド付きで入力しフェールバック設定を表示します。

   switch:admin> **ag —failbackshow 13**
   Failback on N_Port 13 is supported

3. **ag —failbackdisable** コマンドに<n_portnumber> オペランドを付けて入力しフェールバックを無効化します。

   switch:admin> **ag —failbackdisable 13**

Failback policy is disabled for port 13。

コールド・フェールオーバー・ポリシー

オフラインになるN_Portにマップされているf_Portはすべて他のN_Portへフェールオーバーされます。しかし、スイッチがオンラインになった後でN_Portがオンラインにならない場合、当該F_Portにコールド・フェールオーバーさせます。F_Portのうちいずれかが優先セカンダリN_Portセットにマップされており、その優先副N_Portがオンラインの場合、コールド・フェールオーバーの際にF_Portは優先副N_Portにフェールオーバーします。優先副N_Portがオンライン状態でなければ、これらのF_Portは無効化されます。優先副N_Portがこれらのf_Portのいずれにも設定されていない場合、これらのF_Portはスイッチの任意のN_Portにフェールオーバーし、その結果F_Portは 同じN_Portグループに属するすべてのN_Portに均等に分散されます。

ポート・グループ・ポリシー

アクセス・ゲートウェイ・モードのスイッチを複数のファブリックに接続する、または、他のサーバからサーバのサブセットを隔離させる場合、サーバと、対応するファブリック・ポートをグループ化できます。このグループ化はポートグループ化ポリシーを有効化して行いますが、これはN_Portでのみ実行できます。ポート・グループは重複できません。それは 1 個のN_Portは 2 つの異なるグループには属さないことを意味します。

ポート・グループ毎にフェールオーバーとフェールバックの各ポリシーは同じになり、優先副N_Portは同じポート・グループのN_Portのみ指定できます。このため優先副パスを定義する前にグループ化することが推奨されます。この動作はFabric OS v6.0.0 でのみ行われます。Fabric OS v6.0.0 からFabric OS v6.2.0 へアップグレードすると、Fabric OS v6.0.0 で強制されたポート・グループ化ポリシー
とポート・グループは保持されます。

たとえば図 6 はpg0 の一例を示します。N_Port1 と 2 がpg0 にあり、F_Port 1 と 2 がN_Port1 にマップされているとき、N_Port1 がオフラインになると、N_Port2 が同じポート・グループpg0 のメンバーなので、F_Port 1 と 2 はN_Port2 を通してルーティングが行われます。

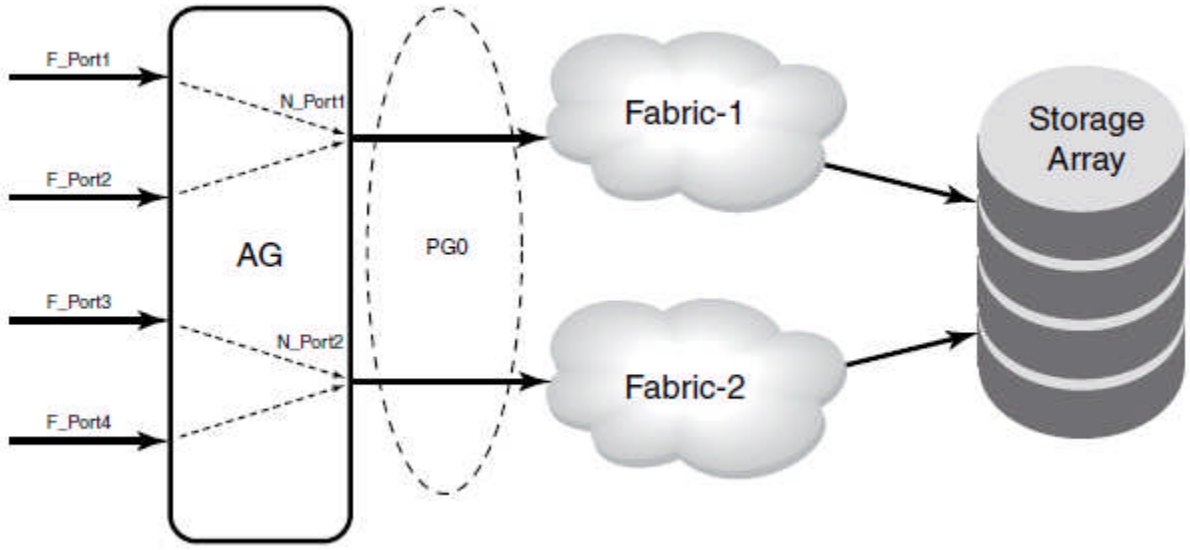

図 6 ポート・グループ 0(pg0)の構造例

図 7 はポート･グループを生成して N_Port がオフラインになると、このポートを通してルーティングされている F_Port はこのポート･グループのメンバーで現在アクティブな任意の N_Port にフェールオーバーします。たとえば、N_Port4 がオフラインになると、F_Port 7 と 8 は N_Port 3 がオンラインである限り N_Port 3 にルーティングされますが、その理由は、N_Port 3 と 4 が同じポート･グループ PG2 のメンバーであるためです。 アクティブな N_Port がない場合、F_Port は無効化されます。ポート･グループのメンバーである F_Port は別のポート･グループに属する N_Port にはフェールオーバーしません。

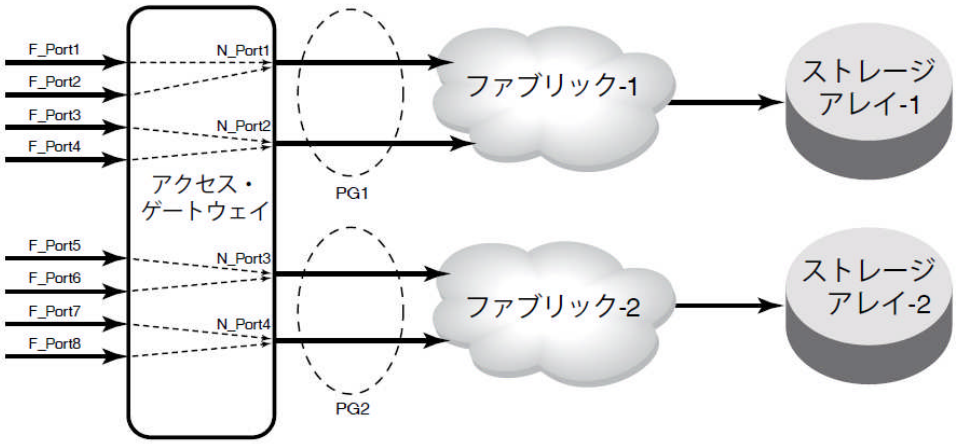

図 7 ポート･グループ化の動作

2 つの冗長ファブリックからなる構成が使用されている場合、アクセス･ゲートウェイ･モードのスイッチに接続されたF_Portは両方のファブリックから同じターゲットにアクセスできます。この場合、冗長ファブリックに接続されたN_Portを 1 つのポート･グループにグループ化しなければなりません。メインのファブリックが落ちた場合に冗長ファブリックにパスをフェールオーバーさせることが推奨されます。

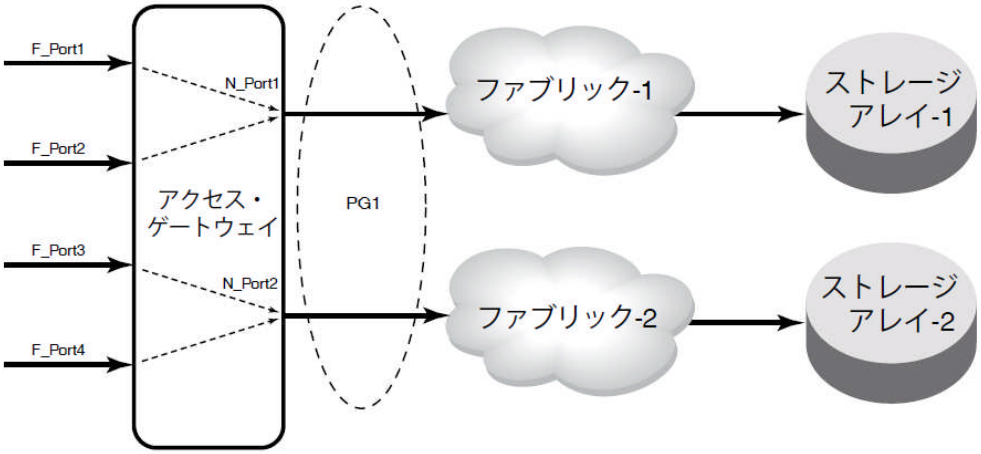

図 8 ポート･グループ 1(pg1)の構造

要注意

関連しないファブリックに接続されたN_Portがグループ化されると、ポート･グループ内でのN_Portフェールオーバーにより F_Portは別のファブリックに接続し、このF_Portはフェールオーバーの前に接続されていたターゲットへの接続を失い、図 8 に示す入出力破壊を伴うことがあります。

新たなポート･グループを生成してN_Portをこれらのグループに追加できます。 しかし、ユーザー定義のポート･グループのメンバーではないN_Portはすべてデフォルトのポート･グループpg0 のメンバーです。

ポート･グループは重複不可なので、N_Portを優先副N_Portに指定して、このN_Portが別のポート･グループのメンバーであると、ポート･グループ化は失敗します。

注

アクセス･ゲートウェイ･モードのスイッチがオンラインの間にポート･グループ化ポリシーが無効化されると、すべてのユーザー定義ポート･グループは削除されますが、F_PortからN_Portのマッピングは変らず維持されます。

ポート･グループを生成する

1. スイッチに接続してadminでログインします。
2. **ag ―pgcreate**コマンドに<PG_ID> “<N_Port1;N_Port2;…> [-n <PG_Name>] オペランドを付けて入力します。たとえば、N_Port　1 と 3 を含む“FirstFabric”名のポート･グループを生成するには:

   switch:admin> **ag ―pgcreate 3 "1;3" -n FirstFabric1**
   Port Group 3 created successfully

3. **ag ―pgshow**コマンドを入力してポート･グループが生成されたことを検証します。

   switch:admin> ag --pgshow
   Port Group ID Port Group Name
   ---
   0 None pg0
   2 0;2 SecondFabric
   3 1;3 FirstFabric

N_Port をポート･グループに追加する

1. スイッチに接続してadminでログインします。
2. **ag ―pgadd**コマンドに<PG_ID> “<N_Port1;N_Port2;…> オペランド付け入力します。

   1 個以上のN_Portを追加するには、セミコロンで分離してください。

   switch:admin> **ag ―pgadd 3 14**
   N_Port[s] are added to the port group 3

3. **ag ―pgshow**コマンドを入力して指定されたポート･グループにN_Portが追加されたか検証します。

   switch:admin> ag --pgshow
   PG_ID N_Port PG_Name
   ---
   0 15 pg0
   3 2;13;14 Test

N_Port をポート･グループから削除する

1. スイッチに接続してadminでログインします。
2. **ag ―pgdel**コマンドに<PG_ID> “<N_Port1;N_Port2;…> オペランドを付けて入力します。

   switch:admin> **ag ―pgdel 3 13**
   N_Port[s] are added to the port group 3

3. **ag ―pgshow**コマンドを入力して指定されたポート･グループからN_Portが削除されたか検証します。

   switch:admin> **ag ―pgshow**
   PG_ID N_Port PG_Name

0	13;15	pg0
3	12;14	Test

ポート･グループを削除する

1. スイッチに接続してadminでログインします。
2. **ag --pgremove**コマンドに<PG_ID>オペランドを付けて入力します。

   switch:admin> **ag --pgremove 3**
   Port Group 3 has been removed successfully。
3. ag --pgshowコマンドを入力して、ポート･グループが削除されたことを検証します。

   switch:admin> **ag --pgshow**

PG_ID	N_Port	PG_Name
0	12;13;14;15	pg0

ポート･グループの名前を変更する

1. スイッチに接続してadminでログインします。
2. ag --pgrenameコマンドに<PG_ID> <newname> オペランドを付けて入力します。
   たとえばポート･グループpgid2 の名前を "My EvenFabric"に変更するには:

   switch:admin> ag --pgrename 2 MyEvenFabric
   Port Group 2 has been renamed as MyEvenFabric successfully。
3. ag --pgshowコマンドを入力してポート･グループの名前が変更されたことを検証します。

   switch:admin> ag --pgshow

PG_ID	N_Port	PG_Name
0	None	pg0
2	0;2	MyEvenFabric
3	1;3	FirstFabric

ポート･グループ･ポリシーを無効化する

1. スイッチに接続してadminでログインします。
2. ag --policydisableコマンドにpg オペランドを付けて入力します。

   switch:admin> **ag --policydisable pg**
3. ag --pgshowコマンドを入力して、ポート･グループ･ポリシーが無効化されたことを検証します。

   switch:admin> **ag --policyshow**

AGﾎﾟﾘｼｰ	ﾎﾟﾘｼｰ名	ｽﾃｰﾄ
ﾎﾟｰﾄのｸﾞﾙｰﾌﾟ化	pg	無効

APC	自動	無効
高度デバイス・セキュリティ・ポリシー	(ADS)	無効

アクセス・ゲートウェイ・ポリシー強制マトリックス

この表はポリシーの組合わせが同時に存在できることを示しています。

表 5 ポリシー強制マトリックス

ポリシー	ポート自動構成	ポートのグループ化	N_Portトランキング	ADSポリシー
ポート自動構成	N/A	相互排他的	共存可能	共存可能
N_Portのグループ化	相互排他的	N/A	共存可能	共存可能
N_Portトランキング	共存可能	共存可能	N/A	共存可能
ADSポリシー	共存可能	共存可能	共存可能	N/A

アクセス・ゲートウェイ・トランキング

アクセス・ゲートウェイ・モードのスイッチでは、マスターレス・トランキング機能は、N_Portのみエンタープライズ・ファブリックに接続するので、N_Portをトランクします。F_PortをN_Portにマップまたは割当した後、N_Portはモジュールで利用可能なパス・リンクのセット全体にフレームを配分します。これは利用可能なパス・リンクポートのみエンタープライズ・ファブリックを隣接エッジ・スイッチに接続できるからです。アクセス・ゲートウェイのマスターレス・トランキングを使用するには、すべてのトランキングがエッジ・スイッチに構成されていることが必要です。アクセス・ゲートウェイ・モジュールに設定は不要です。以下にアクセス・ゲートウェイ・トランキングの利点をまとめました:

- トランク・グループの 1 個以上のN_Portがオフラインになると、トランク・グループの少なくとも 1 個のN_Portがアクティブである限り、N_PortにマップされていたF_PortのPIDは変化しません。このためトランク・グループ内では透過的なフェールオーバーとフェールバックが可能です。
- トランク・グループ上のすべてのリンクにより均等に入出力を分散するスイッチングASICに実装されたトランキング・アルゴリズムにより、トランクされたリンクはより効率的になります。
- トランク・グループはAGモードのAGモジュール内にある複数のN_Portグループ全体に渡っては展開できません。
- 複数のトランク・グループは同じN_Portグループ内で許可されます。

注

エッジ・スイッチではこの機能はF_Portトランキングまたはマスターレス F_Portトランキングと呼ばれます。アクセス・ゲートウェイ・トランキングの構成すべてがエッジ・スイッチで行われるので、この説明はアクセス・ゲートウェイ・モジュールではなくエッジ・スイッチ・モジュールを対象にしています。アクセス・ゲートウェイ・モジュールの 1 つのみの要件は、ISLトランキングライセンスがインストールされていることです。

エッジ・スイッチにトランキングを構成しなければならないので、F_Portトランキングはアクセス・ゲートウェイ・モジュールのN_Portとエッジ・スイッチ・モジュールの間のトランク・グループを形成します。この機能によりアクセス・ゲートウェイのF_Portは、トランク・グループ内にあるN_Portに障害がおきても、無効化されません。トランク・グループに少なくとも 1 個のアクティブなリンクがある限り、フェールオーバーは起きません。トランキングによりトランク内のリンクはオフラインになるまたは無効化されますが、トランクは機能性を保持するので、再構成は不要です。

N_Portがオフラインになった場合、トランキングはポート番号の再割当(26 ページ表 7 に記載されているようにアドレス識別子とも言われる) を防止します。

エッジ・スイッチとアクセス・ゲートウェイ・モードのスイッチともにブロケードISLライセンスをインストールする必要があり、さらに、これらのモジュールがFabric OS v6.1.0 以降のバージョンを実行するようにしてください。

トランク・グループ内のすべてのポートは同じポート・グループのメンバーでなければならず、ポート・グループに属さないポートはトランク・グループを形成できません。 ポート・グループの詳細は、18 ページの“ポート・グループ化ポリシー” を参照ください。

注

スイッチに ISLトランキング使用許諾があれば、アクセス・ゲートウェイのN_Portマスターレス・トランキングで使用するための新たなライセンスは不要です。さらに、アクセス・ゲートウェイ・モードのスイッチにトランキング使用許諾がインストールされていて、スイッチを標準モードに変更する場合にも、同じ使用許諾で行うことができます。アクセス・ゲートウェイはM-EOSまたはブロケード以外のスイッチでは機能しません。

エッジ・スイッチにF_Portのマスターレス・トランキングを実装するには、最初にF_Portトランク・グループを構成して、トランク・グループ内にArea_IDを静的に割当てなければなりません。ポート・グループまたはトランク・グループにトランク・エリアを割当てると、そのポート・グループまたはトランク・グループでF_Portのマスターレス・トランキングが有効化されます。トランク・エリアがポート・グループまたはトランク・グループに割当てられると、そのポートはプロセスID(PID)のエリアとしてトランク・エリアをただちに取得します。さらにトランク・エリアがポート・グループまたはトランク・グループから削除されると、ポートはそのPIDとしてデフォルト・エリアに戻ります。

エッジ・スイッチのためのアクセス・ゲートウェイ・トランキングの検討

表 6 エッジ・スイッチのためのアクセス・ゲートウェイ・トランキングの検討

カテゴリ	内容
エリアの割当	エッジ・スイッチでトランク・グループ内部にエリアを静的 に割当てます。 このグループはF_Portのマスターレス・トランクです。 割当てる静的トランク・エリアはエッジ・スイッチまたはブレード上のポート 0 から始まるF_Portトランク・グループ内部になければなりません。 割当てる静的トランク・エリアはトランク・グループにあるポートのデフォルト・エリアであることが必要です。
認証	認証はF_Portトランク・マスターでのみ行われ、トランク全体で一回のみです。 この動作はE_Portトランク・マスター認証と同じです。その理由はトランク内の 1 個のポートのみがスイッチへのFLOGIを行い、認証はそのポートでのFLOGIに従い、そのポートのみがportshowコマンドを実行したときに認証の詳細を表示します。 **注**: アクセス・ゲートウェイ・モードのスイッチは認証を行いません。
管理サーバ	F_Portトランクでは、登録ノード番号(RNID)、リンク・インシデント・レコード登録(LIRR)、クエリ・セキュリティ属性(QSA)ELSはサポートされません。
トランク・エリア	エッジ・スイッチにあるトランク・エリアをポートに割当てるまたはトトランク・グループからトランク・エリアを削除する前に、ポートは無効化されていることが必要です。 スタンドバイCPがFabric OS v6.2.0 以前のバージョンのファームウェアを実行している場合、トランク・エリアをポートに割当てられません。
PWWN	トランク・エリア全体にあるトランク・グループがトランク・グループ内部の同じポートWWNを共有します。 PWWNはその最初のバイトが 0x2fまたは 0x25 であるF_Portトランクに共通します。トランク・エリアは 26 ページ表 7 のリストにあるフォーマットのPWWNの一部です。

表 6　エッジ・スイッチのためのアクセス・ゲートウェイ・トランキングの検討

カテゴリ	内容
ダウングレード	トランキングはオンを維持できますが、ファームウェアをダウングレードする前にトランク・ポートを無効化しなければなりません。 **注**:トラフィックを実行中のポートでトランク・エリアを削除するのは破壊的です。 Fabric OS v6.1.0 以前のバージョンのファームウェアにダウングレードする必要がある場合、トランク・エリアを割当てる前によく注意してください。
アップグレード	F_PortがスイッチにあればFabric Osv6.1.0 へのアップグレードに制約はありません。 アップグレードは破壊的ではないです。
HA同期化	Fabric OS v6.1.0 以前のバージョンのファームウェアでスタンドバイCPをプラグインし、トランク・エリアがスイッチに存在する場合、CPブレードは同期化されなくなります。
ポート・タイプ	Fabric OS v6.1.0 ではF_Portトランク・ポートのみトランク・エリア・ポートに許可されます。 F/FL/E/EXを含むその他すべてのポート・タイプはFabric OS v6.1.0 では持続的に無効化されます。
デフォルト・エリア	Port Xはトランク・エリアと同じデフォルト・エリアがあるポートです。トランク・グループからポートXを削除できる時は、ランク・グループ全体でトランク・エリアが無効化されている場合のみです。
portCfgTrunkPort <*port*>, 0	**portCfgTrunkPort** <port>, 0 は、ランク・エリアがポートで有効化されていると失敗します。 ポートでトランク・エリアをまず無効化してください。
switchCfgTrunk *0*	switchCfgTrunk *0* はポートでトランク・エリアを有効化されていると失敗します。スイッチ上のすべてのポートでトランク・エリアをまず無効化してください。
ポート・スワップ	トランク・エリアをトランク・グループに割当てる際、トランク・エリアはポート・スワップ不可です。ポート・スワップが行われると、トランク・エリアをそのポートに割当てることはできません。
トランク・マスター	トランク・グループで有効なトランク・マスターは 1 つです。2 個目のトランク・マスターは”エリアは取得済みです”という理由により、持続的に無効化されます。
FastWrite	トランク・エリアをトランク・グループに割当てる際、トランク・グループはこれらのポートでFastWriteを有効化できません。ポートでFastWriteが有効化されると、ポートはトランク・エリアに割当てられません。
FICON	FICONはF_portトランク・ポートではサポートでされません。しかし同じスイッチの中でF_Portトランクされていないポートでは、FICONは実行可能です。
FC8-48 とFC4-48Cブレード	F_Portマスターレス・トランキングは、FC8-48 ブレードの 16-43 ポートではサポートされます。 FC8-48/FC4-48Cブレードでは、F_Portトランキングは 0 – 15 ポートでのみサポートされます。
FC4-32 ブレード	FC4-32 (Electron)の 16 – 31 ポートでトランク・エリアが有効化されており、ブレードをFC4-48CとFC8-48 とスワップすると、ランク・エリア・ポートは持続的に無効化されます。これらのポートにトランク・エリアを割当てるには**porttrunkarea**コマンドを実行します。
トランキング	ポートにトランク・エリアを割当てる前に、ポートでのトランキングを最初に有効化してください。
プロセスID(PID)のフォーマット	F_Portマスターレス・トランキングはCORE PIDフォーマットでのみサポートされます。.
長距離	F_Portトランクで長距離は許可されません、すなわち、トランク・エリアは長距離ポートで許可されず、トランク・エリアが割当てられたポートに長距離を有効化することはできません。

表 6　エッジ・スイッチのためのアクセス・ゲートウェイ・トランキングの検討

カテゴリ	内容
ポート・ミラーリング	ポート・ミラーリングはトランク・エリア・ポートまたはF_Portトランク・ポートのPIDではサポートされません。
Configdownload	F_Portトランキングと互換性が無いポート構成に**configdownload**コマンドを発行して、ポートがトランク・エリアを有効化されている場合、ポートは持続的に無効化されます。 **注**:F_Portトランキングと互換性が無い構成は長距離、ポート・ミラーリング、non-CORE_PID、Fastwriteです。
ICLポート	F_Portトランクは ICLポートでは許可されません。**porttrunkarea**コマンドは許可しません。
管理ドメイン（AD）	異なる管理ドメイン にあるポートにトランク・エリアを生成することはできません。 管理ドメイン 255 にトランク・エリアを生成することはできません。
DCCポリシー	F_Portトランクへの DCCポリシー強制はトランク・エリアに基づきます。トランク・ポートへのFDISC要求は、接続されているデバイスのWWNがトランク・エリアに対するDCCポリシーの一部をなす場合のみ、許可されます。 アクセス・ゲートウェイから送信されたFLOGIのPWWNはF_Portトランク・マスターに対して動的です。アクセス・ゲートウェイが使用するPWWNは予め知ることはできず、FLOGIのPWWNは、F_Portトランク・マスターでのDCCポリシー・チェックに合格しません。しかしFDISCのPWWNはDCCポリシー・チェックに合格し続けます。
D.I. ゾーニング (D,I) 管理ドメイン (D, I) DCCと(PWWN, I) DCC	トランク・エリアを生成するとこのトランク・エリアにグループ化されるスイッチからインデックス（"I"）が削除されることがあります。トランク・エリアにあるすべてのポートは同じ"I"を共有します。この意味は、"I"を参照する、削除された可能性があるドメイン/インデックス (D,I)はスイッチにはもはや含まれなくなることです。 **注**:トランク・エリアを生成する際は、管理ドメイン、ゾーニング、DCCを必ず含めてください。 トランク・エリアからポートを削除して"I"を復元できます。 D,I は普通に動作しますが、単一の"I"へのポート・グループ化の影響が理解できます。 さらに、D,Iはトランク・エリア・グループで動作し続けます。 "I"は、これがトランク・エリア・グループのためのものであれば、D,Iで使用できます。 **注**:"I"はインデックス、D,Iはドメイン/インデックスを意味します。
2 個のマスター	2 個のマスターは、同じF_Portトランク・グループではサポートされません。
QoS	現在はサポートされていません。

この表はF_PortとN_Portのトランク・ポートでのPWWNフォーマットを記載しています。

表 7 F_Port と N_Port トランク・ポートのための PWWN フォーマット

NAA = 2	2f:xx:nn:nn:nn:nn:nn:nn (1)	ポートWWN: スイッチのFX_Port用。	xxの有効範囲は、最大 256 で、 [0 – FF]です。
NAA = 2	2f:xx:nn:nn:nn:nn:nn:nn (1)	ポートWWN: スイッチのFX_Port用。	xxの有効範囲は、最大 256 で、 [0 – FF]です。

トランク・グループの生成

ポート・トランキングは、トランクキングをサポートする 2 個の分離されたFabric OSスイッチの間で、
各スイッチのすべてのポートが同じクァッドに常駐し、同速度で実行中であれば、有効化されます。 トランク・グループは、1 つのFabric OSスイッチに接続されている 2 本またはそれ以上のケーブルを、
同じポート・グループまたはクァッドのポートがある別のFabric OSスイッチに接続すると形成されます。
ポート・グループまたはクァッドは、例えば 0～3 ポートのように連続したポート・セットです。ブロケード 300 スイッチは8個のポートまでのトランク・グループをサポートします。トランク・グループは 0–7、8–15、16–23 等、スイッチのポート数まで連続した 8 つのポートを一つのグループとしたユーザー・ポート番号に基づきます。

F_Port トランキングをセットアップする

ポート・トランキングは、トランクキングをサポートする 2 個の分離されたFabric OSスイッチの間で、各スイッチのすべてのポートが同じクァッドに常駐し、同速度で実行中であれば、有効化されます。 トランク・グループは、1 つのFabric OSスイッチに接続されている 2 本またはそれ以上のケーブルを、同じポート・グループまたはクァッドのポートがある別の Fabric OS スイッチに接続すると形成されます。ポート・グループまたはクァッドは、例えばこの図に示すように 0–3 ポートと連続したポート・セットです。ブロケード 300 プラットフォームは8個のポートまでのトランク・グループをサポートします。トランク・グループは、0 – 7、8–15、16–23 等さらにスイッチにあるポート数までを 1 つのグループとして連続8個のポートを持つ、ユーザー・ポート番号に基づきます。

1. スイッチに接続してadminでログインします。
2. エッジ・スイッチとアクセス・ゲートウェイ・モードのスイッチの両方ともにトランキングライセンスが有効であることを確認してください。
3. portcfgshowコマンドでポートがトランキング有効であることを確認します。トランキング有効化されていない場合、portcfgtrunkport *〈port〉, 1* コマンドを発行します。
4. ポートがトランク内では同速度になるようにしてください。
5. エッジ・スイッチのF_Portトランク・ポートがアクセス・ゲートウェイ・スイッチでのASICサポートされたトランク・グループ内で接続されていることを確認してください。
6. モジュールが両方とも同じバージョンのFabric OSを実行することを確認してください。
7. “トランク・エリアを割当てる” 手順でトランク・エリア(TA)を割当て、エッジスイッチでトランクを構成します。
8. F_Portトランキングを有効化します。

トランク・エリアを割当てる

トランク・エリアを生成する前に、トランク・エリアに含まれるすべてのポートでのトランキングをまず有効化してください。**portCfgTrunkPort**または**switchCfgTrunk**コマンドでスイッチの１個またはすべてのポートでトランキングを有効化します。

porttrunkareaコマンドを発行すると、１個のポートまたはポート・トランク・グループに静的トランク・エリアを割当てること、１個のポートまたはトランク内のポート・グループからトランク・エリアを削除すること、マスターレス・トランキングの情報を表示することができます。

porttrunkarea --disableコマンドでトランク・エリアから特定ポートを削除できますが、トランク・グループのすべてのポートを割当て解除指定しない限り、直前に割当てられたArea_IDがトランク・エリアの同じアドレス識別子（Area_ID）であれば、このコマンドはトランク・エリアの割当を解除しません。**porttrunkarea**コマンドの詳細については、**help porttrunkarea**コマンドを入力するか、*Fabric OS コマンド・リファレンス*を参照ください。 F_Port trunkingはブロケードFC8-48 とFC4-48Cブレードの共有エリア 16-47 のポートはサポートしません。

この表はアドレス識別子の例を示しています。

表 8　アドレス識別子

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
ドメインID								エリア_ID								ポートID							
アドレス識別子																							

1. スイッチに接続してadminでログインします。
2. トランク・エリアに含めるポートを無効化します。
3. ポート・インデックス 125 のスロット 10 にある 13 と 14 ポートのトランク・エリアを有効化します：:

   ```
   switch:admin> porttrunkarea --enable 10/13-14 -index 125
   Trunk index 125 enabled for ports 10/13 and 10/14
   ```

4. トランク・エリア・ポート構成を表示します（ポートはまだ無効):

   ```
   switch:admin> porttrunkarea --show enabled
   Slot Port Type State Master TI DI
   ------------------------------------------------
   10  13      --      --      --      125     125
   10  14      --      --      --      125     126
   ------------------------------------------------
   ```

5. 13 と 14 ポートを有効化します:

   ```
   switch:admin> portenable 10/13
   switch:admin> portenable 10/14
   ```

6. ポート有効化後にトランク・エリア・ポート構成を表示します：:

   ```
   switch:admin> porttrunkarea --show enabled
   Slot Port Type State Master TI DI
   ------------------------------------------------
   10  13  F-port  Master  10/13  125  125
   10  14  F-port  Slave   10/13  125  126
   ```

トランクの DCC ポリシーを有効化する

1. トランク・エリアの割当て後にporttrunkarea CLIコマンドがインデックスTAのポートのアクティブなDCCポリシーがないか調べ、TAインデックスのある既存DCCポリシーにすべてのデバイスWWNを追加するよう警告を発します。

   存在しなくなったインデックスを参照するすべてのDCCポリシーは無効です。

2. トランク・エリアに対するDCCポリシーにすべてのデバイスのWWNを追加します。

3. secpolicyactivateコマンドを発行してDCCポリシーをアクティブにします。

   セキュリティのためにトランク・ポートにDCCポリシーを施行できるように、**secpolicyactivate**コマンドを発行する前にトランク・エリアを必ず有効化してください。

4. トランク・ポートをオンにします。

   DCCセキュリティ・ポリシー違反の際ポートが無効化されないように、**secpolicyactivate**コマンドを発行後にはトランク・ポートをオンにする必要がああります。

トランク・エリアの構成管理

異なる管理ドメインにあるポートは同じトランク・エリア・グループに参加できません。 porttrunkareaコマンドは異なる管理ドメインがトランク・エリア・グループに参加するのを防止します。

トランク・エリアを割当てる際、トランク・エリア・グループ内のポートは同じインデックスを持つようになります。ポートに割当てられたインデックスはスイッチの部分ではありません。ドメインに属したはずのドメイン/インデックス(D,I)管理ドメインは、スイッチから削除されたのでそのドメインにはもはや存在することができません。

例: どうトランク・エリアの割当てがポートのドメイン/インデックスに影響するのか

AD1: 3,7; 3,8; 4,13; 4,14 さらにAD2: 3,9; 3,1 があるとして、それからインデックス 7、8、9、10 があるポートでインデックス 8 のトランク・エリアを生成します。そうすると、インデックス 7、9、10 はドメイン 3 にはもう含まれません。これはAD2 は、インデックス 9 と 10 がドメイン 3 にもう存在しないため、どのポートにもアクセスできないということを意味します。さらにドメイン 3 にはもうインデックス 7 がないので、AD1 にはもう有効な 3,7 がないということを意味します。トランク・エリア・グループである AD1 の 3,8 は、4,13 と 4,14 とともにAD1 からまだ見えます。

トランク・エリア内のポートは削除できますが、再びインデックスがスイッチに追加されます。たとえば、トランク・エリア 8 をもつ同じ管理ドメインAD1 とAD2 は当てはまります。トランク・エリアから 7 ポートを削除すると、スイッチにはインデックス 7 を再度追加します。 その意味はAD1 の 3,7 は 3,8、4,13、4,14 ともAD1 から見えることです。

アクセス・ゲートウェイ・トランキングを有効化する

1. portdisable port コマンドをトランク・エリアに含むポートすべてに対して実行して、36-39 ポートを無効化します。

2. エリア番号 37 の 36-39 ポートにトランク・エリアを有効化します::

   switch:admin> porttrunkarea --enable 36-39 -index 37

   Trunk area 37 enabled for ports 36, 37, 38 and 39。

3. portenable port コマンドをトランク・エリアのポートすべてに対して実行して、36-39 ポートを再有効化します。

4. スイッチとポート情報を表示します:

5. ```
   switch:admin> switchshow
   switchName: switch
   switchType: 43.2
   switchState: Online
   switchMode: Native
   switchRole: Principal
   switchDomain: 1
   switchId: fffc01
   ```
   ```

```
switchWwn: 10:00:00:05:1e:03:4b:e7
zoning: OFF
switchBeacon: OFF
Area Port Media Speed State Proto
==================================
0 0 -- N4 No_Module
1 1 cu N4 Online F-Port 50:06:0b:00:00:3c:b7:32
2 2 cu N4 Online F-Port 10:00:00:00:c9:35:43:f5
3 3 cu AN No_Sync
4 4 cu AN No_Sync Disabled (Persistent)
5 5 cu N4 Online F-Port 50:06:0b:00:00:3c:b4:3e
6 6 cu N4 Online F-Port 10:00:00:00:c9:35:43:f3
7 7 cu AN No_Sync Disabled (Persistent)
8 8 cu AN No_Sync
9 9 cu AN No_Sync Disabled (Persistent)
10 10 cu AN No_Sync Disabled (Persistent)
11 11 cu AN No_Sync Disabled (Persistent)
12 12 cu AN No_Sync Disabled (Persistent)
13 13 cu AN No_Sync Disabled (Persistent)
14 14 cu AN No_Sync Disabled (Persistent)
15 15 cu AN No_Sync Disabled (Persistent)
16 16 cu AN No_Sync Disabled (Persistent)
17 17 -- N4 No_Module
18 18 -- N4 No_Module
19 19 -- N4 No_Module
20 20 -- N4 No_Module
21 21 id N4 Online E-Port segmented,(zone conflict)(Trunk
master)
22 22 id N4 Online E-Port (Trunk port, master is Port 21 )
23 23 id N4 Online E-Port (Trunk port, master is Port 21 )
```

6. トランク・エリアが有効化されたポート構成を表示します:

   switch:admin> **porttrunkarea --show enabled**

ポート・	タイプ	ステート	マスター	TA	DA
36	--	--	--	37	36
37	--	--	--	37	37
38	--	--	--	37	38
39	--	--	--	37	39

F_Port トランキングを無効化する

1. スイッチに接続してadminでログインします。
2. **porttrunkarea --disable**コマンドを入力します。

   switch:admin> **porttrunkarea --disable 36-39**
   エラー: 36 ポートは無効化される必要があります

トランク・エリアからポートを削除する前にポートをすべて無効化します。 その後コマンドを再発行します:

switch:admin> porttrunkarea --disable 36-39
36、37、38、39 のポートにトランク・エリア 37 が無効化されました。

F_Port トランキング監視

F_Portマスターレス・トランキングには、 F_Portトランク・ポートにFilter、EE またはTTモニターをインストールすることが必要です。マスター・ポートが変る度に、モニターを新たなマスター・ポートに移動することが必要です。たとえば、あるマスター・ポートが停止すれば、残りのスレーブ・ポートから新たなマスターが選択されます。APMは古いマスターからモニターを削除して、新たなマスター・ポートにそのモニターをインストールしなければなりません。スレーブ・ポートにモニターを追加しようとすると自動的にマスター・ポートに追加されます。

アクセス・ゲートウェイ・カスケード化

アクセス・ゲートウェイ・カスケード化は、2 個のアクセス・ゲートウェイ・スイッチを一端ではN_Port、他端ではF_Portとしてリンクさせて接続することをいいます。ファブリックに直接接続されるアクセス・ゲートウェイ・スイッチをコア・アクセス・ゲートウェイと呼びます。デバイスに直接接続されるアクセス・ゲートウェイ・スイッチをエッジ・アクセス・ゲートウェイと呼びます。この図はアクセス・ゲートウェイ・カスケード化を説明しています。

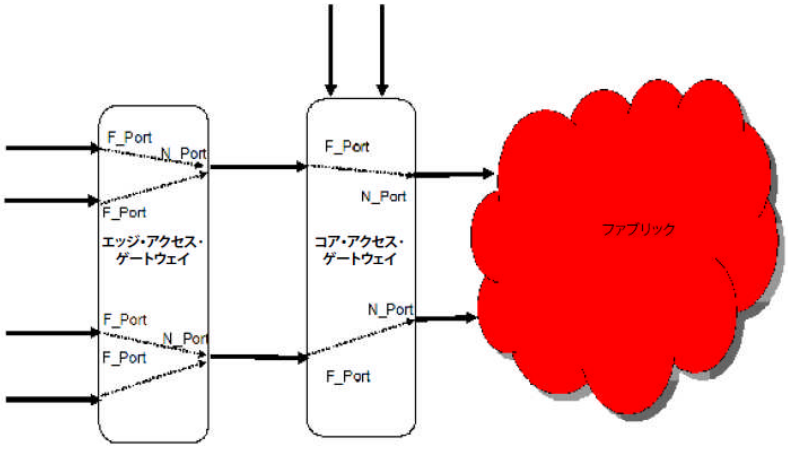

図 9　アクセス・ゲートウェイ・カスケード化

ポートは 2 個の相互接続されたアクセス・ゲートウェイ・スイッチ間で接続されます。デバイス間のアクセス・ゲートウェイ・カスケード接続は、メイン・ファブリックにつながるポート数を統合できる一方、カスケード化が超過予約を提供するので、ネットワーク使用度を増大させます。 使用許諾無しにこの機能を利用できます。

アクセス・ゲートウェイ・モジュール/スイッチをカスケード化する際の構成検討項目：

- エッジ・スイッチとコア・アクセス・ゲートウェイ・スイッチでポート・グループ化(PG)ポリシーを有効化できます。
- カスケード化は 1 段のみサポートされます。数個のエッジ・アクセス・ゲートウェイが単一アクセス・ゲートウェイに接続でき、より高い統合比率をサポートできることを銘記してください。
- エッジ・スイッチとコア・アクセス・ゲートウェイ・スイッチ間でのアクセス・ゲートウェイ・トランキングはサポートされません。コア・アクセス・ゲートウェイ・スイッチとファブリックとのトランキングはサポートされます。
- サーバに直接接続されているアクセス・ゲートウェイF_Portに高度セキュリティ・ポリシー(ADS)を有効化することが推奨されます。
- カスケード化の際はAPCポリシーはサポートされません。
- ループバック(コア・アクセス・ゲートウェイN_portからエッジ・アクセス・ゲートウェイF_Port)は禁止です。
- ファブリックに対して発行される**agshow**コマンドがコア・アクセス・ゲートウェイ・スイッチのみを発見します。**agshow ―name** <AGName>コマンドを発行すると、エッジ・アクセス・ゲートウェイ・スイッチとコア・アクセス・ゲートウェイ・スイッチのF_portがコア・アクセス・ゲートウェイ・スイッチについて表示されます。

3 章

アクセス・ゲートウェイを使用してデバイスを接続する

この章の内容

複数デバイスの接続性概要

この章はアクセス・ゲートウェイ・モードのスイッチに複数のデバイスを接続する方法を説明し、エッジ・スイッチの互換性、ポート要件、NPIV HBA、相互運用性について説明します。 アクセス・ゲートウェイはターゲットの直接接続をサポートするので、アクセス・ゲートウェイ・スイッチが外部ファブリックに接続されていれば、アクセス・ゲートウェイ・モードのスイッチにターゲット・デバイスを直接接続することができます。アクセス・ゲートウェイは、2 個のアクセス・ゲートウェイはデバイスが相互接続されていると、デイジーチェーンをサポートしません。アクセス・ゲートウェイ・モードのスイッチは次のファームウェア・バージョンではエッジ・スイッチ上の他の種類のファブリックに接続できます:

- M-EOSc v9.6.2 以降とM-EOSn v9.6
- Cisco v3.0(1)以降、v3.1(1)以降、v3.2(1)以降。
- Only FCP イニシエータ・ポートの みF_Portとしてアクセス・ゲートウェイ・モードのスイッチに接続できます。FCPターゲット・ポートは、アクセス・ゲートウェイ・モードのスイッチが外部スイッチに接続されていればサポートされます。ループ・デバイスとFICONチャネル/コントロール・ユニットの接続はサポートされません。
- アクセス・ゲートウェイ・モードのスイッチはNPIVが有効化されたHBAまたは、NPIV可能なF_Portに接続できます。 アクセス・ゲートウェイはFC-LS-2 v1.4 によるNPIV業界規格をサポートします。

ファブリックとエッジ・スイッチの構成

アクセス・ゲートウェイを使用してホストをファブリックに接続するには、次のパラメータをしようしてファブリックを構成します。次のパラメータはFabric OS、M-EOS、Cisco・ベースのファブリックに該当します:

- 以下の手順へ進む前に、*ハードウェア参照説明書*に従いスイッチをインストールして構成します。
- *インタロップ・モード・パラメータが 0 に、ブロケード・ネイティブ・モード、またはスイッチ・モードがネイティブ・モードに設定されていることを検証します。*
- *アクセス・ゲートウェイが次のように接続されるようにエッジ・スイッチのF_Portを構成します:*
  - NPIVを有効化する。
  - 長距離モードを無効化する。

- マルチ・ログインを許可します。推奨されるファブリック・ログイン設定はポート、スイッチ毎に最大可能な数を許可することです。

- ファブリックを通してWWNゾーニングを使用します。アクセス・ゲートウェイはドメインIDその他の種類のゾーニングはサポートしません。
- アクセス・ゲートウェイのWWN またはN_PortのポートWWNおよびアクセス・ゲートウェイF_Portに接続されるHBA WWNもACLポリシーのACLリストに含めます。
- 転送されたファブリック管理を目的とするインバンド・クエリのホストからの要求を許可します。 インバンド・クエリが制限されている場合、アクセス・リストにアクセス・ゲートウェイ・スイッチのWWNを追加します。

注
アクセス・ゲートウェイをFabric OSファブリックに接続する前に、Fabric OS管理サーバ・プラットフォーム・サービスを無効化します。

スイッチ・モードを検証する

1. スイッチに接続してadminでログインします。
2. **switchShow**コマンドを入力して現在のスイッチ構成を表示します。

   次例はswitchModeがNativeとして表示されるFabric OS Native状態にあるスイッチを示します。

```
switch:admin>          switchshow
ｽｲｯﾁ名 :               ｽｲｯﾁ
ｽｲｯﾁﾀｲﾌﾟ:              43.2
ｽｲｯﾁｽﾃｰﾄ:              ｵﾝﾗｲﾝ
switchMode:            Native
ｽｲｯﾁﾛｰﾙ:               主
ｽｲｯﾁﾄﾞﾒｲﾝ:             1
ｽｲｯﾁID:                fffc01
ｽｲｯﾁWWN::              10:00:00:05:1e:03:4b:e7
ｿﾞｰﾆﾝｸﾞ:               OFF
ｽｲｯﾁﾋﾞｰｺﾝ:             OFF
```

エリア	ポート	媒体	速度	ステート	ﾌﾟﾛﾄ	
0	0	--	N4	No_Module		
1	1	cu	N4	ｵﾝﾗｲﾝ	F-Port	50:06:0b:00:00:3c:b7:32
2	2	cu	N4	ｵﾝﾗｲﾝ	F-Port	10:00:00:00:c9:35:43:f5
3	3	cu	AN	No_Sync		
4	4	cu	AN	No_Sync	無効化（持続的）	
5	5	cu	N4	ｵﾝﾗｲﾝ	F-Port	50:06:0b:00:00:3c:b4:3e
6	6	cu	N4	ｵﾝﾗｲﾝ	F-Port	10:00:00:00:c9:35:43:f3
7	7	cu	AN	No_Sync	無効化（持続的）	
8	8	cu	AN	No_Sync		
9	9	cu	AN	No_Sync	無効化（持続的）	
10	10	cu	AN	No_Sync	無効化（持続的）	
11	11	cu	AN	No_Sync	無効化（持続的）	
12	12	cu	AN	No_Sync	無効化（持続的）	
13	13	cu	AN	No_Sync	無効化（持続的）	
14	14	cu	AN	No_Sync	無効化（持続的）	
15	15	cu	AN	No_Sync	無効化（持続的）	
16	16	cu	AN	No_Sync	無効化（持続的）	
17	17	--	N4	No_Module		
18	18	--	N4	No_Module		
19	19	--	N4	No_Module		

20	20	--	N4	No_Module		
21	21	id	N4	ｵﾝﾗｲﾝ		E-Port セグメント化,(ｿﾞｰﾝ競合)(ﾄﾗﾝｸﾏｽﾀｰ)
22	22	id	N4	ｵﾝﾗｲﾝ		E-Port (ﾄﾗﾝｸﾎﾟｰﾄ, ﾏｽﾀｰは 21 ﾎﾟｰﾄ)
23	23	id	N4	Online	E-Port	(ﾄﾗﾝｸﾎﾟｰﾄ, ﾏｽﾀｰは 21 ﾎﾟｰﾄ)

ポート状態の説明は 41 ページ表 10 をご覧ください。

スイッチがネイティブ・モードにある場合、アクセス･ゲートウェイ・モードを有効化できます。それ以外の場合、スイッチをネイティブ・モードに設定して、スイッチを再起動します。

Fabric OS スイッチをネイティブ・モードに設定する

1. スイッチに接続してadminでログインします
2. **switchDisable**コマンドを入力してスイッチを無効化します。

   switch:admin> **switchdisable**
3. **configUpload**コマンドを使用してスイッチ構成を保存します。
   a. FTP サービスがホスト・コンピュータで実行中であることを確認してください。
   b. **configUpload**コマンドを入力します。

      コマンドは対話型で、必要な情報の入力を促されます。
4. **configure**コマンドを入力してインターロップ・モードが 0 に設定されていることを確認します。

M-EOS スイッチで NPIV を有効化する

1. スイッチに接続してM-EOSスイッチにadminでログインします。
2. 次のコマンドを入力してMSサービスを有効化します:

   config OpenSysMs setState
3. エッジ･ファブリックにNPIV機能を有効化し、ポート毎の複数ログインを許可します。 M-EOSスイッチに次のコマンドを入力して指定したポートにNPIVを有効化します。

   config NPIV

   M-EOSスイッチはこれで接続準備ができました。

注

agshowコマンドを実行して、ファブリックに登録されたアクセス･ゲートウェイの情報を表示できます。 アクセス･ゲートウェイが非FOSスイッチのみに接続される場合、ファブリック内の他のブロケード・スイッチには**agshow**コマンドの出力を表示しません。

Cisco･ファブリックへの接続性

アクセス･ゲートウェイ･モードのスイッチを、QLogicベースのデバイスがあるCisco・ファブリックに接続する際、一部のQLogicファイバーチャネルASICベースのホスト・バス・アダプタ(HBA)は、アクセス･ゲートウェイ･モードのスイッチが使用するルーティング機構と互換性がありません。

この場合には、アクセス・ゲートウェイとの相互運用性を確保するため、Ciscoから提供された手順でCisco・スイッチを構成しなければなりません。

QLogic FC ASICテクノロジーには基づいていないEmulex HBAやその他のHBAを使用する場合、Cisco・スイッチ上でN_Port ID仮想化(NPIV)が有効化されること、そのスイッチがSAN-OS 3.0 (1)またはSAN-OS 3.1 (1)以降のバージョンを実行しているようにしてください。デフォルトでは、NPIVはポート毎にではなく、スイッチ毎に有効化されます。

Cisco・ファブリックでのアクセス・ゲートウェイのルーティング要件

AGモードのスイッチのルーティングの仕組みや,AGスイッチの後ろでQlogicベースのデバイスとCisco MDSスイッチが相互運用できるようにする回避方法は、Ciscoの企業IDリストに基づいています。

AGで、8-bit ALPAルーティングをAreaとALPAフィールドの両方を使用する 16-bitルーティングに拡張すると、下位 8-bitでもPIDを処理できるようになります。ALPAルーティング・モードでは、CiscoスイッチはNPIVデバイスに下位 16bitの点で異なる、ddXXXXというフォーマットでNPIVログインの為のPIDを割り振ります。

AGモードのスイッチはF_Port(サーバに接続)とN_Port(ファブリックに接続)の間でフレームをルーティングするために、FCID(ALPA/Port_IDフィールド)の下位 8bitを使用しているので、アクセス・ゲートウェイは次の 2 点を受諾できません:

- 同じN_Portでの同じ下位 8 ビット(たとえば、0xaabb02 と 0xccdd02)がある 2 個のFCID
- F_Portログイン(AGを通してのサーバHBAログイン、FDISCログインとして知られている)のため返されるFCIDのALPA/Port_IDフィールドが"00"。これら二つの状況のどちらかが検出されると、AGモードのスイッチは、原因コード"Duplicate ALPA detected."でサーバ・ポートを持続的に無効化します。

Cisco・スイッチで NPIV を有効化する

1. CiscoMDSスイッチにadminとしてログインします。
2. show versionコマンドを入力して正しいSAN-OSバージョンを使用中であるか、 NPIVがスイッチで有効化されているかを判断します。
3. 次の手順でNPIVを有効化します:

   ```
   conf  t
   enable  npiv
   ```

4. **Ctrl-Z**を押して終了します。
5. 次のコマンドを入力してMDSスイッチ接続を保存します:

   ```
   copy  run  start
   ```

   Cisco・スイッチはこれでアクセス・ゲートウェイ・モードのスイッチに接続する準備ができました。

QLogic ベースのデバイス用手順

AGモードのスイッチにQLogicベースのデバイスがある場合、Ciscoから提供されている手順でAGモードのFabric OSスイッチからCiscoファブリックに接続しなければなりません。Ciscoのソフトウェアには QLogicベースのHBAリストがあります。ファブリック・ログインの際、PWWNに使用される企業ID（Organizational Unit Identifier、またはOUIとしても知られます）により、HBA毎に識別されます。CLIからCisco企業IDエントリを変更できます。

注
fcinterop FC IDの割当方式をautoに設定し て、FC IDデバイス割当てを操作するため企業IDリストと持続的FC ID設定を使用する必要があります。

表 9 はCiscoの企業IDリストです。ここにはOUI IDがWorld Wide Name (WWN)の中央 3 バイトとして表示されています。このOUI IDフォーマットはイニシエータ・デバイスに使用されます。

表 9　特別な処置を要する OUI ID リスト

OUI ID		
00:E0:8B	00:02:6B	
00:09:6B	00:06:2B	WWN: 00:00:11:22:33:00:00:00
00:11:25	00:14:5E	OUI
00:50:8B	00:A0:B8	
00:60:B0	00:D0:60	
00:90:A5	00:E0:69	
00:50:2E	00:D0:B2	

HBAへのFCID割当てについて詳しい資料は次のサイトをご覧ください：

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_2_x/san-os/configuration/guide/adv.html#wp1127676

スイッチにファイバーチャネル・ターゲット・デバイスが無い場合に企業 ID リストを編集する

Cisco・スイッチにストレージ・アレイ等ファイバーチャネルのターゲット・デバイスが無い場合、CiscoMDSスイッチをアクセス・ゲートウェイ・モードのスイッチに接続できます。これは企業IDリストを編集、またはCiscoスイッチのFCID割当モードをFLATモードに置換するとできます。

1. スイッチに接続してCiscoMDSスイッチにadminでログインします。
2. 企業IDリストから、アクセス・ゲートウェイ・モードのスイッチを通して接続されたすべてのHBAのOUI IDを削除します。
3. OUI IDは企業IDリストにOUI IDが含まれる場合のみ、削除してください。
4. 次のコマンドを入力して企業IDリストにあるOUIを判断します：

```
switch#_show　fcid-allocation　area
FCID　area　allocation　company　id　info:（FCIDエリア割当企業ID情報）
00:50:2E　<- Default entry（デフォルト入力値）
00:50:8B
00:60:B0
00:E0:79
00:0D:60　+　<- User added entry
```

00:E0:8B ＊ <- Explicitly deleted entry（元のデフォルト・リストから明示的に削除された値）
Total company ids 6（合計企業ID数）
+ - Additional user configured company ids（ユーザー定義による追加企業ID数）
＊ -Explicitly deleted company ids from default list.
（デフォルト・リストから明示的に削除された企業ID）

企業 ID リストから OUI を追加または削除する

次例は企業IDリストからOUI(0x112233) を追加または削除する方法を示しています。

1. 次のコマンドを入力します:

   config t

2. 次のコマンドを入力してOUI ID 0x112233 をリストに追加します:

   fcid-allocation area company-id 0x112233

3. 次のコマンドを入力してOUI ID 0x445566 をリストから削除します:

   no fcid-allocation area company-id 0x445566

4. 次のコマンドを入力してリストを表示します:

   do show fcid-allocation area

5. **Ctrl-Z**を押して終了します。

6. 次のコマンドを発行してMDSスイッチ構成を保存します。

   copy run start

接続されたターゲット・デバイスのOUI IDが更新された企業IDリストにリストされることを確認してください。
リストの更新後は、アクセス・ゲートウェイ・デバイスを接続できます。原因コード"Duplicate ALPA detected（複製ALPAが検出されました）"でポートが無効化されたことをアクセス・ゲートウェイ・サーバ・ポート(F_Port)が通知すれば、次の手順に従います:

- デバッグFLOGIモードが有効化されていないことを確認してください。CiscoはFLOGIデバッグが設定されているときはNPIVをサポートしません。**show debug flogi**コマンドを実行してFLOGIモードが有効化されていないことを確認してください。FLOGIモードが有効化されている場合、次のFLOGIデバッグ・コマンドで無効化してください:

  config t
  no flogi debug
  Press Ctrl-Z to exit。
  copy run start Saves MDS switch configuration

- デフォルトでは、アクセス・ゲートウェイ・モードのスイッチで使用する新たなまたは既存のVSANであれば、デフォルトのアクセス・ポリシーは"deny"（拒否）です。"permit"（許可）に設定するか、デバイスのゾーニングをアクセスのために行います。

- アクセス・ゲートウェイはCiscoのVSAN、Dynamic Port VSAN (DVPM)、Inter-VSAN Routing (IVR)機能と互換ですが、これらのMDS機能をフル活用するにはアクセス・ゲートウェイ・ポート・グループポリシーを使用することが必要になります。ポート・グループ化ポリシーの詳細については、18 ページの“ポート・グループ化ポリシー” を参照ください。

スイッチにファイバーチャネル・ターゲット・デバイスが無い場合に FLAT FCID モードを有効化する

1. もう一つの手段として、次のコマンドを入力して、CiscoスイッチFCID割当モードをFLATモードに変えることができます:

   config t
   fcinterop fcid-allocation flat

2. 次のコマンドを入力してVSANモードを有効化します:

   vsan database

3. 次のコマンドを入力してFlat FCIDモードを有効化します:

   vsan 〈vsan#〉 suspend
   no vsan 〈vsan#〉 suspend

4. **Ctrl-Z**を押して終了します。

5. 次のコマンドを入力してMDSスイッチ構成を保存します:

   copy run start

注
停止するVSANにデバイスがある場合、そのデバイスはVSANを再開するまではオフラインになります。

スイッチにファイバーチャネル・ターゲット・デバイスがある場合に企業 ID リストを編集する

スイッチにターゲット・デバイスがある場合、スイッチにあるすべてのターゲット・スイッチのOUIを企業IDリストに追加してから、アクセス・ゲートウェイ・モードのスイッチを通して接続されたすべてのHBAのOUIIDを企業IDリストから削除しなければなりません。 OUI IDは企業IDリストにOUI IDが含まれる場合のみ、削除してください。 次のコマンドを入力して企業IDリストにあるOUIを判断します:

```
switch#_show fcid-allocation area
FCID area allocation company id info:(FCIDエリア割当企業ID情報)
00:50:2E <- Default entry(デフォルト入力値)
00:50:8B
00:60:B0
00:E0:79
00:0D:60 + <- User -added entry(追加した値)
00:09:6B + <- User -added entry(追加した値)
00:E0:8B * <- Explicitly deleted entry (元のデフォルト・リストから明示的に削除された値)
Total company ids 6(合計企業ID数)
+ - Additional user configured company ids(ユーザー定義による追加企業ID数)
* - Explicitly deleted company ids from default list.
    (デフォルト・リストから明示的に削除された企業ID)
```

注
CiscoのGUIツールにあるPersistent FCIDフィールドを使用しても、アクセス・ゲートウェイ・モジュールのQLogicベースのデバイスにFCIDを自分で割当てることができます。この方法を採用する場合、正しいFCIDが割当てられていることを確認してください。このIDは同じMDSスイッチに接続されたターゲット・デバイスとは異なるエリア・フィールドを持ちます。36 ページの“Ciscoファブリックでのアクセス・ゲートウェイのルーティング要件”を参照のうえ、スイッチがAGルーティング要件に合致するか確認してください。

アクセス・ゲートウェイ・モード

AGモード有効化後はｿﾞｰﾝやセキュリティ・データベース等、一部のファブリック情報が消去されるので、スイッチをAGモードに有効化する前にスイッチ構成を保存してください。構成ファイルのバックアップと復元について詳細は、*Fabric OS 管理者用ガイド*を参照ください。

AGモードの有効化はスイッチが無効化され、再起動されるので、機能停止を伴います。スイッチがネイティブ・モードまたはインターロップモード 0 に設定されていることを確認してください。switchshowコマンドを実行してスイッチ・モードを検証します。スイッチ・モードが 0 以外の場合、interopmode 0 コマンドを実行してスイッチをネイティブ・モードにしてください。スイッチをネイティブ・モードにする詳細については、35 ページの"Fabric OSスイッチを ネイティブ・モードに設定する" を参照ください。アクセス･ゲートウェイについての詳細は、*Fabric OS コマンド・リファレンス*を参照ください。

ブロケード 300 と 200E スイッチをアクセス･ゲートウェイ･モードに設定する場合、アクセス･ゲートウェイ･モードを有効化する前にポートを使用するすべてのPODライセンスを有効化しなければなりません。

注

エッジ・スイッチに接続できるアクセス･ゲートウェイの最大数は 30 です。アクセス･ゲートウェイを通してFabric OSに接続できるデバイスの最大数はFabric OSがサポートするローカル・デバイスの最大数により変ります。

アクセス・ゲートウェイ・モードを有効化する

ゾーニングまたは管理ドメインのトランザクション・バッファがアクティブではないようにしてください。トランザクション・バッファがアクティブな場合、アクセス・ゲートウェイ・モードを有効化はエラー・メッセージ"Failed to clear Zoning/Admin Domain configuration"で失敗します。

1. **ag ―modeenable**コマンドを入力します。

   switch:admin> ag –modeenable

   スイッチが自動再起動して、出荷時初期設定であるF_PortのN_Portマッピングを使用してアクセス・ゲートウェイモードでオンラインに戻ります。アクセス・ゲートウェイのデフォルトF_PortからN_Portマッピングについて詳細は、53 ページ表 11 を参照ください。

2. **ag ―modeshow**コマンドを入力してアクセス・ゲートウェイモードが有効化されていることを検証します。

   switch:admin> **ag –modeshow**
   Access Gateway mode is enabled.

3. **ag ―mapshow**コマンドをオプション無しで入力してすべてのマップされたポートを表示します。

   ag ―mapshowコマンドは、N_Portが接続されていない場合でも、N_Port（**portcfgnport** の値が 1 で）を表示します。

   switch:admin> **ag –mapshow**

N_Port	Configured_F_Ports	Current_F_Ports	Failover	Failback	PG_ID	PG_Name
0	4;5;6	4;5;6	1	0	2	SecondFabric
1	7;8;9	7;8;9	0	1	0	pg0
2	10;11	10;11	1	0	2	SecondFabric
3	12;13	12;13	0	1	0	pg0

4. **switchShow**コマンドをオプション無しで入力してすべてのポートの状態を表示します。

5.
```
switch:admin> switchshow
switchName: switch
switchType: 43.2
switchState: Online
switchMode: Access Gateway Mode
switchWwn: 10:00:00:05:1e:03:4b:e7
switchBeacon: OFF
Area Port Media Speed State                                Proto
==============================================================================
0     0   --     N4   No_Module
1     1   cu     N4    Online       F-Port 50:06:0b:00:00:3c:b7:32 0x5a0101
2     2   cu     N4    Online       F-Port 10:00:00:00:c9:35:43:f5 0x5a0003
3     3   cu     N4    Online       F-Port 50:06:0b:00:00:3c:b6:1e 0x5a0102
4     4   cu     N4    Online       F-Port 10:00:00:00:c9:35:43:9b 0x5a0002
5     5   cu     N4    Online       F-Port 50:06:0b:00:00:3c:b4:3e 0x5a0201
6     6   cu     N4    Online       F-Port 10:00:00:00:c9:35:43:f3 0x5a0202
7     7   cu     AN    No_Sync      Disabled (Persistent)
8     8   cu     N4    Online       F-Port 10:00:00:00:c9:35:43:a1 0x5a0001
9     9   cu     AN    No_Sync      Disabled (Persistent)
10    10   cu     AN    No_Sync      Disabled (Persistent)
11    11   cu     AN    No_Sync      Disabled (Persistent)
12    12   cu     AN    No_Sync      Disabled (Persistent)
13    13   cu     AN    No_Sync      Disabled (Persistent)
14    14   cu     AN    No_Sync      Disabled (Persistent)
15    15   cu     AN    No_Sync      Disabled (Persistent)
16    16   cu     AN    No_Sync      Disabled (Persistent)
17    17   --     N4    No_Module
18    18   --     N4    No_Module
19    19   id     N4    No_Light
20    20   --     N4    No_Module
21    21   id     N4    Online       N-Port 10:00:00:05:1e:35:10:1e 0x5a0200
22    22   id     N4    Online       N-Port 10:00:00:05:1e:35:10:1e 0x5a0100
23    23   id     N4    Online       N-Port 10:00:00:05:1e:35:10:1e 0x5a0000
```

ポート状態

次表は可能なポート状態を記載します。

表 10 ポート状態の内容

ステート	内容
No _Card	インターフェイス・カードはありません
No _Module	モジュール（GBICまたはその他）はありません
Mod_Val	モジュールの動作検証中
Mod_Inv	無効なモジュール
No_Light	モジュールに光が来ていません
No_Sync	光は来ていますが同期されていません
In_Sync	光を受信中で同期されています
Laser_Flt	モジュールはレーザ障害を報知しています
Port_Flt	ポートは障害ありとマークされています
Diag_Flt	ポート障害診断失敗
Lock_Ref	参照信号にロック中です
Testing	診断の実行中

表 10 ポート状態の内容

ステート	内容
Offline	接続は確立されていません（仮想ポートのみ該当）
Online	ポートは稼働しています

AG・モードを無効化する

アクセス・ゲートウェイ・モードのスイッチを無効化する前に、現在の構成を必ずバックアップしてください。アクセス・ゲートウェイ・モードを無効化するとF_PortからN_Portのマッピングが消去されます。

AGモードの無効化はスイッチが無効化され、再起動されるので、機能停止を伴います。アクセス・ゲートウェイ・モードの無効化後は、スイッチはFabric OSネイティブ・モードで始動します。 スイッチは再起動と同時にファブリックから分割します。スイッチをコアファブリックに再び参加させるには、43 ページの“スイッチをファブリックに再び参加させる”を参照ください。

スイッチの再構成とそれをファブリックに参加させる補足情報は、*Fabric OS 管理者用ガイドを参照ください*。

1. スイッチに接続してadminでログインします。
2. **ag ―modeshow**コマンドを入力してスイッチがアクセス・ゲートウェイモードであることを検証します。

   switch:admin> **ag –modeshow**
   Access Gateway mode is enabled.
3. switchDisableコマンドを入力してスイッチを無効化します。

   switch:admin> switchdisable

   注

   アクセス・ゲートウェイの構成を保存するため、configUpload コマンドを入力してから、 次の手順へ進みます。

4. **ag**コマンドを**―modedisable**オペランド付きで入力し、アクセス・ゲートウェイ・モードを無効化します。

   switch:admin> **ag –modedisable**

   スイッチは自動的に再起動し、ファブリック・スイッチ構成を使用してオンラインに戻ります。F_PortのN_Portマッピングやフェールオーバーとフェールバックのポリシー等のアクセス・ゲートウェイ・パラメータは自動的に削除されます。
5. **ag ―modeshow**コマンドを入力してアクセス・ゲートウェイモードが無効化されていることを検証します。

   switch:admin> **ag –modeshow**
   Access Gateway mode is NOT enabled.

アクセス・ゲートウェイの構成を保存する

1. スイッチに接続してadminでログインします。
2. **configUpload**コマンドを入力します。

スイッチをファブリックに再び参加させる

スイッチが再起動してアクセス・ゲートウェイ・モードが無効化されてから、デフォルト・ゾーンはアクセス無しに設定されます。このためスイッチは接続先ファブリックには直ちに参加しません。 次の方法のいずれかを
使用してスイッチをファブリックに再び参加させます:

- アクセス・ゲートウェイ・モード有効化する前にFabric OSの構成を保存した場合、**configDownload**コマンドを使用して構成をダウンロードします。
- ファブリック構成を使用してファブリックにスイッチを再び参加させるには、次の手順を用います。

1. スイッチに接続してadminでログインします。
2. **switchDisable**コマンドを入力してスイッチを無効化します。
3. **defZone ―allAccess**コマンドを入力してスイッチがファブリックに結合できるようにします。
4. **cfgSave**コマンドを入力してdefzoneの変更を実行します。
5. **switchEnable**コマンドを入力してスイッチを有効化し、ファブリックと結合できるようにします。

   スイッチは自動的にファブリックに再び参加します。

直前の構成に戻す

1. スイッチに接続してadminでログインします。
2. **switchDisable**コマンドを入力してスイッチを無効化します。
3. **configDownload** コマンドを入力して直前の構成に戻ります。
4. **switchEnable** コマンドを入力してスイッチをオンラインに戻します。
   スイッチは自動的にファブリックに参加します。

4 章
アクセス・ゲートウェイ・モードのポートを構成する

この章の内容

アクセス・ゲートウェイ・モードでのポート初期化

この章はポートをアクセス・ゲートウェイ・モードに構成し、アクセス・ゲートウェイ・マスターレス・トランキングを実装する方法を説明します。アクセス・ゲートウェイの構成はsecurityadmin、adminまたはuserの権限がないとできません。

アクセス・ゲートウェイ・モードのスイッチが機動するとすべてのホストがオンラインになるように、ポートは次のように初期化されます;

1. スイッチをアクセス・ゲートウェイ・モードで有効化すると、N_Portはｽｲｯﾁの初期工場設定に属する場合のみ初期化されます。N_Portの初期化中はF_Portは無効化されています(オフライン状態を保ちます).

   ポートは次のようにして有効化/無効化されます:

   - ポートは、ファブリック・ログイン・イベントを受信して、NPIV(N_Port ID仮想化)をサポートするエッジ・スイッチのF_Portに接続されると**有効化**(オンライン)されます。
   - ポートはファブリックに接続されていない、または、NPIVをサポートしないファブリック・ポートに接続されていると**無効化**(オフライン)されます。
2. オンラインのN_PortにマップされたF_Portはすべて有効化されます。
3. フェールオーバー・ポリシーが有効化されたオフラインのN_PortにマップされたF_PortはオンラインのN_Portにフェールオーバーします。
4. ホストはファブリックに次のようにログインします:
   a. ホストはFLOGI(ファブリック・ログイン)要求を送る。
   b. AGはFLOGI要求をホストと同じパラメータでファブリックへのFDISC要求に変換する。
   c. ファブリックは要求を処理してFDISC応答を返す。
   d. アクセス・ゲートウェイは、ホストへのFDISCの許可リンク・サービス(ACC)応答をファブリックと同じパラメータを使用してFLOGI ACCとして変換する。
   e. ホストがファブリックからの応答を受ける。

   図 10 はポート初期化後にホストとファブリックに対して論理透過的なアクセス・ゲートウェイを示しています。

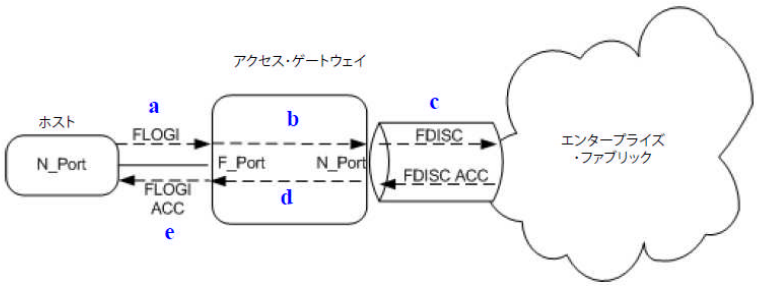

図 10　アクセス・ゲートウェイの初期化されたポート

F_PortをN_Portとしてファブリックに接続するように構成してファブリックを拡張できます。これにより 1 つのファブリック・ポートに接続できるデバイス・ポート数を増加できます。アクセス・ゲートウェイは 1 つ以上のファブリックに接続できます。

アクセス・ゲートウェイがファブリック内の少なくとも 1 個のエッジ・スイッチに接続されているときは、FCP埋め込みはターゲットまたはイニシエータとして動作します。ファイバーチャネル・ポートのターゲット・ポートはF_Portとしてアクセス・ゲートウェイにも接続できます。

次のイニシエータとターゲットの組合わせが可能です:

- すべてのF_Portがファイバーチャネル・ポートのイニシエータ・ポートに接続。
- すべてのF_Portがファイバーチャネル・ポートのターゲット・ポートに接続。
- あるF_Portはファイバーチャネル・ポートのイニシエータ・ポートに、あるF_Portはファイバーチャネル・ポートのターゲット・ポートに接続。
- 同じアクセス・ゲートウェイに接続されたターゲットとホストはサポートされません。

N_Port

エンタープライズ・ファブリックに接続されたアクセス・ゲートウェイ・ポートは、**portcfgnport** *mode* コマンドを使用してN_Portとして構成されなければなりません。デフォルトでは、ブレードスイッチでアクセス・ゲートウェイの内部ポートのみF_Portとして構成されます。すべての外部ポートはN_Portとして構成（ロック）されます。どのポートがデフォルトではマップされるかについて詳細は、53 ページ表 11 を参照ください。内部ポートはブレード・サーバ上のホストに接続し、外部ポートはファブリックに接続します。

有効化されたN_Portは、NPIVをサポートするエンタープライズ・ファブリック・スイッチに接続されると自動的にオンラインします。NPIV機能はアクセス・ゲートウェイに接続されたポートでは有効化されることが必要です。特定のポートのNPIV機能を有効化するには**portcfgnpivport**コマンドを使用します。デフォルトでは、NPIVは 8Gbpsスイッチでは有効化されています。

注
NPIVは、アクセス・ゲートウェイのN_portへのログイン後はブロケード・エッジ・スイッチでは無効化されますから、NPIVデバイスがそのN_portを使用してログインしなかった場合、アクセス・ゲートウェイのN_portからはログアウトされることはありません。この場合はアクセス・ゲートウェイのN_portを自分で無効化してください。 *Fabric OS 管理者用ガイド*でその詳細情報を参照ください。

注
アクセス・ゲートウェイ・モードのスイッチは少なくとも 1 個のポートがN_Portとして構成されていなければなりません。従って、N_PortにマップされうるF_Portの最大数はスイッチのポート数 – 1 です。

図 11 はアクセス・ゲートウェイが有効化されているときにブレードスイッチの外部に接続されたホストを示します。 構成されたF_PortはN_Portにマップされます。

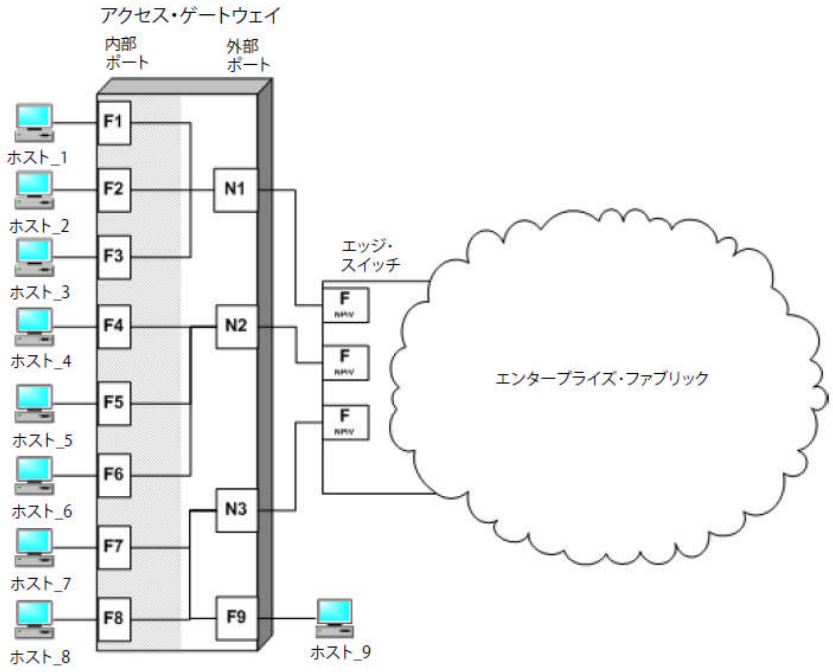

図 11　埋め込みスイッチで外部 F_Port (F9)を追加する例

N_Port をアンロックする

N_Port構成をアンロックすると自動的にポートはF_Portに変ります。N_Portをアンロックすると、F_Portではマッピングが自動的に解除されて無効化されます。

1. スイッチに接続してadminでログインします。
2. **portcfgnport**コマンドを入力します。

注
portcfgnportコマンドは、ポート・グループ・ポリシーが有効化されているときのみ機能します。

```
switch:admin>  portcfgnport

ポート .                  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
--------------------+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--
Locked N_Port             .. .. .. .. .. .. .. .. .. .. ON ON ON ON ON ON
```

3. portcfgnportコマンドに<portnumber> 0 オペランドをつけて入力し、N_Portモードをアンロックします。

   switch:admin> **portcfgnport 10 0**

   逆に、N_Portモードのポートをロックするには、 **portcfgnport** <*portnumber*> 1 コマンドを入力します。

   switch:admin> **portcfgnport 10 1**

デフォルトでは、ブレードスイッチでは、アクセス・ゲートウェイを有効化するとすべての外部ポートはN_Portロック・モードとして構成されます。アクセス・ゲートウェイはFCPイニシエータとターゲットのみファブリックに接続します。ISL(インタースイッチ・リンク)ポート等他の種類のポートはサポートしません。

ファブリック・スイッチのポート・タイプはロックされません。 Fabric OSネイティブモードは接続
されたデバイスに基づいて動的にポート・タイプを割当てます：ホスト、HBA、ストレージ・デバイスにはF_PortとFL_Port、他のスイッチへの接続にはE_Port、EX_Port、VE_Portを割当てます。

N_Port の構成を表示する

1. スイッチに接続してadminでログインします。
2. **portcfgnport**コマンドを入力します。

   switch:admin> **portcfgnport**

```
ポート .                  0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
--------------------+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--
Locked N_Port       .. .. .. .. .. .. .. .. .. .. ON ON ON ON ON ON
```

ポート・マッピングとポート状態を確認する

アクセス・ゲートウ ェイでのポート・マッピングとファブリックへのホスト接続の状態はag --mapshowコマンドを使用して表示できます。*Fabric OS コマンド・リファレンス*に**ag**コマンドの詳細が説明されています。

1. スイッチに接続してadminでログインします。
2. **ag ―mapshow**コマンドを入力します。

   switch:admin> ag –mapshow

   N_Port Configured_F_Ports Current_F_Ports Failover Failback PG_ID PG_Name

0	4;5;6	4;5;6	1	0	2	SecondFabric
1	7;8;9	7;8;9	0	1	0	pg0
2	10;11	10;11	1	0	2	SecondFabric
3	12;13	12;13	0	1	0	pg0

次のパラメータを使用します：

N_Port	N_Portモードにロックされたポートの数
Configured F_Ports	対応するN_PortにマップされたF_Port
Current F_Ports	対応するN_PortでファブリックにF_Portを示す。 フェイルオーバの場合、Current F_PortとConfigured F_Portは違う。
Failover and Failback	N_Portポリシーが有効化されている(1)か無効化されている(0)かを示します。
PG_ID and PG_Name	ポート・グループ・ポリシーが有効化されているか(1)無効化されているか(0)を示します。

N_Portマッピングを表示する

1. スイッチに接続してadminでログインします。
2. **ag —mapshow**コマンドを入力して、ポート番号を指定します。

   N_Portフェールオーバーとフェールバック・ポリシーとマップされたF_Portが表示されます。

```
switch:admin>  ag –mapshow
N_Port Configured_F_Ports Current_F_Ports Failover Failback PG_ID PG_Name
-----------------------------------------------------------------------
   0        4;6              4;6            1        0        2     SecondFabric
   1        7;8;9            7;8;9          0        1        0     pg0
   2        5;10;11  5;10;11  1        0     2        SecondFabric
   3        12;13            12;13          0        1        0     pg0
```

ポート状態を表示する

1. スイッチに接続してadminでログインします。
2. switchshowコマンドをオペランドを付けずに入力します。

```
switch:admin>          switchshow
ｽｲｯﾁ名 :               ｽｲｯﾁ
ｽｲｯﾁﾀｲﾌﾟ:              43.2
ｽｲｯﾁｽﾃｰﾄ:              ｵﾝﾗｲﾝ
switchMode:            AGﾓｰﾄﾞ
ｽｲｯﾁWWN::              10:00:00:05:1e:03:4b:e7
ｽｲｯﾁﾋﾞｰｺﾝ:             OFF

Area  Port  Media  Speed  State       Proto
=============================================
0     0     --     N4     No_Module
1     1     cu     N4     Online      F-Port  50:06:0b:00:00:3c:b7:32  0x5a0101
2     2     cu     N4     Online      F-Port 10:00:00:00:c9:35:43:f5 0x5a0003
3     3     cu     N4     Online      F-Port 50:06:0b:00:00:3c:b6:1e 0x5a0102
4     4     cu     N4     Online      F-Port 10:00:00:00:c9:35:43:9b 0x5a0002
5     5     cu     N4     Online      F-Port 50:06:0b:00:00:3c:b4:3e 0x5a0201
6     6     cu     N4     Online      F-Port 10:00:00:00:c9:35:43:f3 0x5a0202
7     7     cu     AN     No_Sync                Disabled (Persistent)
8     8     cu     N4     Online      F-Port  10:00:00:00:c9:35:43:a1  0x5a0001
9     9     cu     AN     No_Sync        Disabled (Persistent)
10    10    cu     AN     No_Sync        Disabled (Persistent)
11    11    cu     AN     No_Sync        Disabled (Persistent)
12    12    cu     AN     No_Sync        Disabled (Persistent)
13    13    cu     AN     No_Sync        Disabled (Persistent)
14    14    cu     AN     No_Sync        Disabled (Persistent)
15    15    cu     AN     No_Sync        Disabled (Persistent)
16    16    cu     AN     No_Sync        Disabled (Persistent)
17    17    --     N4     No_Module
18    18    --     N4     No_Module
19    19    id     N4     No_Light
20    20    --     N4     No_Module
21    21    id     N4     Online      N-Port  10:00:00:05:1e:35:10:1e  0x5a0200
22    22    id     N4     Online      N-Port 10:00:00:05:1e:35:10:1e 0x5a0100
23    23    id     N4     Online      N-Port 10:00:00:05:1e:35:10:1e 0x5a0000
```

注

ポート状態の説明は 41 ページ表 10 をご覧ください。

ポートの構成

以下のポート・マッピングの更新、ポートの追加と削除はポート・グループ・ポリシーのみに適用できます。

F_Port を N_Port に追加する

マッピングを更新する際は、追加または削除されたF_Portのみに該当します。F_PortをN_Portに追加すると、指定したN_Portを通るファブリックとのトラフィックのルーティングを行います。フェールオーバー・ポリシーを有効化する際、N_Portがオフラインになるか障害を起こすと、F_Portは同じファブリックに接続された別のN_Portにルーティングします。

一度にF_Portを 1 個のみのプライマリN_Portに割当てできます。F_PortがN_Portにすでに割当てられている場合、追加する前にN_Portから削除してください。 次の手順でF_PortをN_Portに追加します。

注
ブレード・サーバではHBAは内部ポートに接続します。内部ポートはF_Portです。デフォルトでは、外部ポートのみN_Portとして構成されます。

1. スイッチに接続してadminでログインします。
2. ag—mapdel コマンドに*〈n_portnumber〉 〈F_Port1;...;F_Port2〉* オペランドを付けて入力して、F_PortをN_Portから削除します。この*f_portlist*にはたとえば“17;18”のようにセミコロンで区切られたF_Port 番号を複数含めることができます。

   switch:admin〉 **ag --mapdel 10 6**
   F-Port to N-Port mapping has been updated successfully。
3. **switchshow** コマンドを入力して F_Port がフリーであること(未割当て)を確認します。

   未割当て F_Port 状態は Disabled (無効、F_Port にマッピング無し)です。 次例で 6 のポートを見てください。

```
switch:admin>          switchshow
switchName:            fsw534_4016
switchType:            45.0
switchState:           Online
switchMode:            Access Gateway Mode
switchWwn: 10:         00:00:05:1e:02:1d:b0
switchBeacon:          OFF
```

Area	Port	Media	Speed	State	Proto
0	0	cu	AN	No_Sync	
1	1	cu	AN	No_Sync	Disabled (N-Port Offline for F-Port)
2	2	cu	AN	No_Sync	Disabled (N-Port Offline for F-Port)
3	3	cu	AN	No_Sync	Disabled (N-Port Offline for F-Port)
4	4	cu	AN	No_Sync	Disabled (N-Port Offline for F-Port)
5	5	cu	AN	No_Sync	Disabled (N-Port Offline for F-Port)
6	6	cu	AN	No_Sync	Disabled (No mapping for F-Port)
7	7	cu	AN	No_Sync	
8	8	cu	AN	No_Sync	
9	9	cu	AN	No_Sync	
10	10	--	N4	No_Module	
11	11	--	N4	No_Module	
12	12	--	N4	No_Module	

13	13	id	N4	オンライン	N-Port 10:00:00:05:1e:35:10:1e 0x5a0a00
14	14	id	N4	オンライン	N-Port 10:00:00:05:1e:35:10:1e 0x5a0900
15	15	id	N4	オンライン	N-Port 10:00:00:05:1e:35:10:1e 0x5a0800

4. **ag --mapaddコマンドを**<n_portnumber> "<f_port1;f_port2;...>オペランドを付けて入力し、F_Portのリストをn_Portに追加します。

   この*f_portlist* にはたとえば"17;18"のようにセミコロンで区切られたF_Port番号を複数含めることができます。

   switch:admin> **ag --mapadd 13 "6;7"**

   F-Port to N-Port mapping has been updated successfully。

5. Enter the **ag --mapshow**コマンドにn_portnumber オペランドを付けて入力し、マップされたF_Portのリストを表示します。追加されたF_Portがリストに現れます。

   switch:admin> **ag --mapshow 13**

   N_Port : 13
   Failover(1=enabled/0=disabled) : 1
   Failback(1=enabled/0=disabled) : 1
   Current F_Port : None
   Configured F_Port : 6;7
   PG_ID : 0
   PG_Name : pg0

N_Port から F_Port を削除する

N_PortからF_Portを削除するとF_Portの割当てが解除されます。F_Portの状態は無効に変ります（F_Portにマッピング無し)。

1. スイッチに接続してadminでログインします。
2. **ag --mapdel**コマンドに*<n_portnumber> <f_port1;f_port2;...>* オペランドを付けて入力し、F_Portのリストをn_Portから削除します。

   switch:admin> **ag --mapdel 13 "5;6"**

   F-Port to N-Port mapping has been updated successfully。

3. Enter the **ag --mapshow**コマンドに*n_portnumber*オペランドを付けて入力し、マップされたF_Portのリストを 表示します。削除したF_Portがリストに無いことを検証します。

   switch:admin> **ag --mapshow 13**

   N_Port : 13
   Failover(1=enabled/0=disabled) : 1
   Failback(1=enabled/0=disabled) : 1
   Current F_Port : None
   Configured F_Port : 7
   PG_ID : 0
   PG_Name : pg0

優先セカンダリポートを追加する

優先マッピングはオプションです。優先N_Portを追加するとF_Portがフェールオーバーできる代替N_Portを提供します。F_Portはセカンダリ N_Portが構成される前にプライマリN_Portにマップされていなければなりません。

prefsetコマンドでF_Portを優先セカンダリN_Portに追加します。このコマンドで優先N_Portを 1 個以上のF_Portに設定できます。prefdelコマンドで優先N_PortからF_Portを削除できます。次の手順では、3 と 9 のF_Portを 4 の優先副N_Portに追加します。

1. スイッチに接続してadminでログインします。
2. ag ―prefsetコマンドに*〈F_Port1;F_Port2; ...〉 〈N_Port〉* オペランドを付けて入力し、優先副F_Portを指定したN_Portに追加します。

   マップするF_Portは必ず引用符で囲み、ポート番号はセミコロンで区切ります。たとえば:

   switch:admin> **ag ―prefset "3;9" 4**
   Preferred N_Port is set successfully for the F_Port[s]

優先副 N_Port から F_Port を削除する

この例では 4 の優先副N_Portから 3 と 9 のF_Portを削除します。

1. スイッチに接続してadminでログインします。
2. ag ―prefdelコマンドに〈F_Port1;F_Port2; ...〉 〈N_Port〉 オペランドを付けて入力し、優先F_Portを指定したN_Portから削除します。

   セカンダリ・マッピングから削除するF_Portのリストは必ず引用符で囲み、ポート番号はセミコロンで区切ります。たとえば:

   switch:admin> **ag ―prefdel "3;9" 4**
   Preferred N_Port is deleted successfully for the F_Port[s]

次表は、アクセス・ゲートウェイ・モードが有効化されると自動的に構成されるデフォルトのF_PortからN_Portへのマッピングを示しています。すべてのN_Portでフェイルオーバーとフェイルバックが有効化されています。ブロケード 300 と 200Eでアクセス・ゲートウェイを使用するには、すべてのポートにアクティブなPODライセンスが必要です。

表 11　アクセス・ゲートウェイのF_PortからN_Portへのデフォルト・マッピング

ﾌﾞﾛｹｰﾄﾞ ﾓﾃﾞﾙ	ﾎﾟｰﾄ合計数	F_Port	N_Port	F_PortからN_Portへのデフォルト・マッピング
300	24	0–15	16–23	0 と 1 は 16 にマップします。 2 と 3 は 17 にマップします。 4 と 5 は 18 にマップします。 6 と 7 は 19 にマップします。 8 と 9 は 20 にマップします。 10 と 11 は 21 にマップします。 12 と 13 は 22 にマップします。 14 と 15 は 23 にマップします。
200E	16	0–11	12–15	0, 1 と 2 は 12 にマップします。 3, 4 と 5 は 13 にマップします。 6, 7 と 8 は 14 にマップします。 9, 10 と 11 は 15 にマップします。
4012	12	0–7	8–11	0 と 1 は 8 にマップします。 2 と 3 は 9 にマップします。 4 と 5 は 10 にマップします。 6 と 7 は 11 にマップします。
4016	16	0–9	10–15	0 と 1 は 10 にマップします。 2 と 3 は 11 にマップします。 4 と 5 は 12 にマップします。 6 と 7 は 13 にマップします。 8 は 14 にマップします。 9 は 15 にマップします。
4018	18	4–11	0–3	4, 5, と 12 は 0 にマップします。 6, 7, と 13 は 1 にマップします。 8, 9, 14 と 16 は 2 にマップします。 10, 11, 15 と 17 は 3 にマップします。
4020	20	1–14	0,15–19	1 と 2 は 0 にマップします。 3 と 4 は 15 にマップします。 5, 6 と 7 は 16 にマップします。 8 と 9 は 17 にマップします。 10 と 11 は 18 にマップします。 12, 13 と 14 は 19 にマップします。
4024	24	1–16	0, 17–23	1 と 2 は 17 にマップします。 9 と 10 は 18 にマップします。 3 と 4 は 19 にマップします。 11 と 12 は 20 にマップします。 5 と 6 は 21 にマップします。 13 と 14 は 22 にマップします。 7 と 8 は 23 にマップします。 15 と 16 は 0 にマップします。

表 11　アクセス・ゲートウェイのF_PortからN_Portへのデフォルト・マッピング

ﾌﾞﾛｹｰﾄﾞ ﾓﾃﾞﾙ	ﾎﾟｰﾄ合計数	F_Port	N_Port	F_PortからN_Portへのデフォルト・マッピング
4424	24	17–20	18	0、17–23 はフェールオーバーとフェールバックが有効化されたN_Port 1と2 は17にマップします。 3と 4 は18にマップします。 5と6 は19にマップします。 7と8 は20にマップします。 9と10 は21にマップします。 11と12 は22にマップします。 13と 14 は23にマップします。 15 と 16 は 0 にマップします。
5424	24	0, 17–23	1–16	0 、17–23 はフェールオーバーとフェールバックが有効化され、ポート・グループ化ポリシーがあるN_Port 1と2 は17にマップします。 3と 4 は18にマップします。 5と6 は19にマップします。 7と8 は20にマップします。 9と10 は21にマップします。 11と12 は22にマップします。 13と 14 は23にマップします。 15 と 16 は 0 にマップします。
5470	20	0, 15–19	1–14	0 、15–19 はフェールオーバーとフェールバックが有効化され、ポート・グループ化ポリシーがあるN_Port 1と 2 は0にマップします。 3と 4 は15にマップします。 5, 6と 7 は16にマップします。 8と 9 は17にマップします。 10と 11 は18にマップします。 12, 13 と 14 は 19 にマップします。
5480	24	0, 17–23	1–16	有効化され、ポート・グループ化ポリシーがあるN_Port 1と 2 は17にマップします。 9と10 は18にマップします。 3と 4 は19にマップします。 11と 12 は20にマップします。 15と 16 は0にマップします。 5と 6 は21にマップします。 13と14 は22にマップします。 7 と 8 は 23 にマップします。

表 11　アクセス・ゲートウェイのF_PortからN_Portへのデフォルト・マッピング

ﾌﾞﾛｹｰﾄﾞ モﾃﾞﾙ	ﾎﾟｰﾄ合計数	F_Port	N_Port	F_PortからN_Portへのデフォルト・マッピング
5100	40	32–39	0–31	32–39 はフェールオーバーとフェールバックが有効化されたN_Port 0, 1, 2と 3 は32にマップします。 4, 5, 6と 7 は33にマップします。 8, 9, 10と 11 は34にマップします。 12, 13, 14と 15 は35にマップします。 16, 17, 18と 19 は36にマップします。 20, 21, 22と 23 は37にマップします。 24, 25, 26と 27 は38にマップします。 28, 29, 30 と 31 は 39 にマップします。

問題解決法

この付録は問題解決法を指示します。

表 12　問題解決法

問題	原因	解決法
スイッチがアクセス・ゲートウェイ・モードではない	スイッチがネイティブ・スイッチ・モード	スイッチを**switchDisable**コマンドで無効化します。 アクセス・ゲートウェイ・モードを ag --modeenableコマンドを使用して有効化します。 プロンプトでyesと答えます。スイッチが再起動します。 スイッチにログインします。 スイッチの設定を**switchShow**コマンドで表示します。アクセス・switchModeのフィールドがAccess Gateway Modeと表示されることを確認します。
エッジ・スイッチ・ポートでNPIVは無効	不慮の電源オフ	エッジ・スイッチで**portCfgShow**コマンドを入力します。 ブロケード・アクセス・ゲートウェイが接続されているポートのNPIV状態がオンであることを確認します。 その状態が"--"で表示されていれば、NPIVは無効です。 NPIVを有効化するには**portCfgNpivPort** *〈port_number〉* コマンドをオペランド 1 を付けて入力します。 必要に応じてstepをポート毎に反復します。
N_PortとF_Port を再構成する必要がある	顧客環境にデフォルト・ポート設定が適格ではない	ブロケード・アクセス・ゲートウェイで**portCfgShow**コマンドを入力します。 N_Portとしてアクティブにするポート毎に**portCfgNport** *〈port_number〉* コマンドをオペランド 1 を付けて入力します。 他のすべてのポートはF_Portとしてとどまります。 ポートをF_Portにリセットするには、**portCfgNpivPort** *〈port_number〉* コマンドをオペランド **0** を付けて入力します。
LUNが見えない	ファブリック・スイッチでのゾーニングが不正。 アクセス・ゲートウェイ・モードのスイッチでポート・マッピングが不正。 配線接続が不正。	エッジ・スイッチでのゾーニングを検証します。 オンラインのN_PortにF_Portがマップされているか検証します。 これについては 53 ページの"アクセス・ゲートウェイのF_PortからN_Portへのデフォルト・マッピング" を参照ください。目視による配線の点検を行い、ポートを間違っていないか、ケーブルのねじれや折れを検査します。 ケーブルを交換して再度試みます。

表 13 問題解決法(続き)

問題	原因	解決法
フィールオーバーが機能しない	N_Portでフェールオーバーが無効化されている。	フェールオーバーとフェールバックのポリシーが次に示すように有効化されているか検証します: **ag ―failoverShow**コマンドに <**port_number**> オペランドを付けて入力します。 **ag ―failbackShow**コマンドに <**port_number**>オペランドを付けて入力します。 コマンドは"Failback (or Failover) on N_Port <port_number> is supported."を返します。 コマンドが""Failback (or Failover) on N_Port <port_number> is not supported."を返した場合、52 ページの。
アクセス・ゲートウェイ・モードにしたくない	アクセス・ゲートウェイを無効化しなければなりません。	スイッチを**switchDisable**コマンドで無効化します。 アクセス･ゲートウェイ･モードを **ag ―modeDisable**コマンドを使用して無効化します。 プロンプトでyesと答えます。スイッチが再起動します。 スイッチにログインします。 スイッチの設定を**switchShow**コマンドで表示します。switchModeフィールドがFabric OS native modeと表示することを確認します。

注
Fabric OSスイッチがアクセス･ゲートウェイ･モードであり、このスイッチがM-EOSスイッチに接続されたときにMcDATAファブリック・モードにも設定されている場合、Fabric OSスイッチは、agshowコマンドに対して出力表示しません。

索引

A

B

C

D

E

F

H

Q

R

S

T

U

Z

本書をお読みになる前に

外国為替及び外国貿易法に基づく特定技術について

当社のドキュメントには「外国為替および外国貿易管理法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

本書の内容について

このたびは、弊社の PRIMERGY ファイバーチャネルスイッチブレード(8Gbps 18/8)をお買い上げいただき、誠にありがとうございます。
本書は、本製品を Access Gateway モードとして使用した場合の使用方法を示した、Access Gateway 管理者ガイドです。
なお、本文は英語で記載しています。
本書をよくお読みになり、正しい取り扱いをされますようお願いいたします。

■ 関連マニュアル

- PRIMERGY ファイバーチャネルスイッチブレード(8Gbps 18/8) (PG-FCS104)取扱説明書
- PRIMERGY ファイバーチャネルスイッチブレード(8Gbps 18/8) (PG-FCS104)
  Fabric OS リファレンスガイド V6.2.0
- PRIMERGY ファイバーチャネルスイッチブレード(8Gbps 18/8) (PG-FCS104)
  Web Tools リファレンスガイド V6.2.0

上記マニュアルは「PRIMERGY」ページの「マニュアル」(http://primeserver.fujitsu.com/primergy/manual.html)からご覧ください。

本書の補足説明

本製品を使用するにあたり、本書における補足説明について記載します。

・本書 「Port Configurations」Table11 (ページ 53, 54) において、Access Geteway モードを有効にした場合の各モデルにおけるデフォルトの F_Port と N_Port のマッピングが記載されていますが、本ファイバーチャネルスイッチブレードについて記載がありません。本ファイバーチャネルスイッチでのデフォルトのマッピングは次のとおりです。

TABLE 1 (補足) Access Gateway default F_Port-to-N_Port mapping

Brocade Model	Total Ports	F_Ports	N_Ports	Default F_ to N_Port Mapping
5450	26	1-18	0,19-25	0,19-25 are N_ports with failover enabled, failback enabled and PG policy 1, 2, 17 mapped to 19 3, 4, 18 mapped to 20 5, 6 mapped to 21 7, 8 mapped to 22 9, 10 mapped to 23 11, 12 mapped to 24 13, 14 mapped to 25 15, 16 mapped to 0

※本製品は、Brocade Model 5450 と表記します。

PRIMERGY

ファイバーチャネルスイッチブレード（8Gbps 18/8）
（PG-FCS104）
Access Gateway 管理者ガイド（v6.2.0）

CA92276-8601-02

発行日　2009年7月
改版日　2010年11月
発行責任　富士通株式会社