ユーザー ガイド

hp StorageWorks
iSCSI storage router 2122

製品バージョン： 1.0

初版 (2002 **年** 9 **月**)

製品番号： 304835-191

このユーザー ガイドでは、SR2122 iSCSI **ストレージ ルータのインストール手順と設定手順について説明します。**

HP StorageWorks iSCSI storage router 2122 ユーザーガイド
初版 (2002 年 9 月)
製品番号 : 304835-191

目次

このガイドについて

このユーザー ガイドでは、次の内容について説明します。

- SR2122 iSCSI ストレージ ルータの設置
- SR2122 iSCSI ストレージ ルータの設定

「このガイドについて」には、次の項目があります。

表記上の規則

表記上の規則には、次の項目があります。

- 表記上の規則
- 本文中の記号
- 装置の記号

表記上の規則

このガイドでは、ほとんどの場合、表1 に示す表記上の規則を採用しています。

表1: 表記上の規則

項目	表記法
クロス リファレンス リンク	**図**1
キー名とフィールド名、メニュー項目、ボタン名、ダイアログ ボックスのタイトル	**太字**
ファイル名、アプリケーション名、および強調するべき語句	**イタリック**
ユーザー入力、コマンドとディレクトリ名、およびシステム応答（出力とメッセージ）	Monospace**フォント** **コマンド名は、大文字・小文字の区別がない限り、すべて**monospace**フォントの大文字**
変数	<*monospace**フォント、イタリック体***>
Web**サイト アドレス**	**下線付きの**sans serif**フォント：** http: / / www.hp.com

本文中の記号

このガイドで使用されている記号はそれぞれ以下の意味を表します。

警告: **人体への傷害や生命の危険を引き起こす恐れがある警告事項を表します。**

注意: **装置の損傷やデータの消失を引き起こす恐れのある注意事項を表します。**

注記: **解説、補足、または役に立つ情報を示します。**

装置の記号

ハードウェアに貼付されている記号は、以下の意味を表しています。

これらの記号が貼付された装置の表面または内部部品に触れると、感電の危険があることを表します。修理はすべて、資格のある担当者に依頼してください。

警告 : **感電防止のため、カバーは開けないでください。**

これらの記号が貼付されたRJ-45**ソケットは、ネットワーク インタフェース接続を表します。**

警告: 感電、火災、または装置の損傷を防止するために、電話または電気通信用のコネクタをこのソケットに接続しないようにしてください。

これらの記号が貼付された装置の表面または内部部品の温度が非常に高くなる可能性があることを表します。この表面に手を触れるとやけどをする場合があります。

警告: 表面が熱くなっているため、やけどをしないように、システムの内部部品が十分に冷めてから手を触れてください。

電源やシステムにこれらの記号が貼付されている場合、装置の電源が複数あることを表します。

警告: 感電しないように、電源コードをすべて抜き取ってシステムの電源を完全に切ってください。

製品や機械にこの2つの記号が貼付されている場合、1人で安全に取り扱うことができる重量を超えていることを表します。

警告 : けがや装置の損傷を防ぐため使用する地域で定められている重量装置の安全な取り扱いに関する規定に従ってください。

ラックに関する注意

ラックを安定させて、人身傷害や装置の損傷を防止します。

警告: けがや装置の損傷を防止するために、次の点に注意してください。

- **ラックの水平脚を床まで伸ばしてください。**
- **ラックの全重量が水平脚にかかるようにしてください。**
- **1つのラックだけを設置する場合は、ラックに固定脚を取り付けてください。**
- **複数のラックを設置する場合は、ラックを連結してください。**
- **ラック コンポーネントは一度に1つずつ引き出してください。一度に複数のコンポーネントを引き出すと、ラックが不安定になる場合があります。**

製品概要

1

この章では、ストレージ ルータハードウェアの設置方法について説明します。ここでは、このマニュアルの他の章に進む前に理解しておくべき、非常に基本的な以下の内容について説明します。

ストレージ ルータを設置および設定するのに必要な作業は以下のとおりです。

- ストレージ ルータの設置
- ストレージ ルータ ソフトウェアの設定
- iSCSIドライバのインストールと設定

装置概要

ストレージ ルータは、1Uのラックマウント型ルータです（図1を参照）。ストレージ ルータにより、IPホストは、IPネットワーク経由でファイバ チャネル ストレージにアクセスできるようになります。

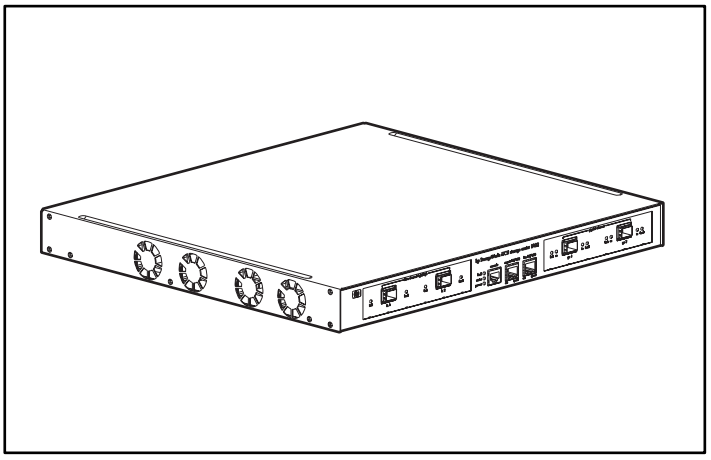

図1: ストレージ ルータのシャーシ

ストレージ ルータにより、IPホストは、ファイバ チャネル ストレージに直接接続されている場合と同じようにファイバ チャネル ストレージにアクセスできるようになります（図2を参照）。ストレージ ルータでアクセス可能なストレージのタイプについては、第4章「ソフトウェアの概要」および他の関連マニュアルを参照してください。

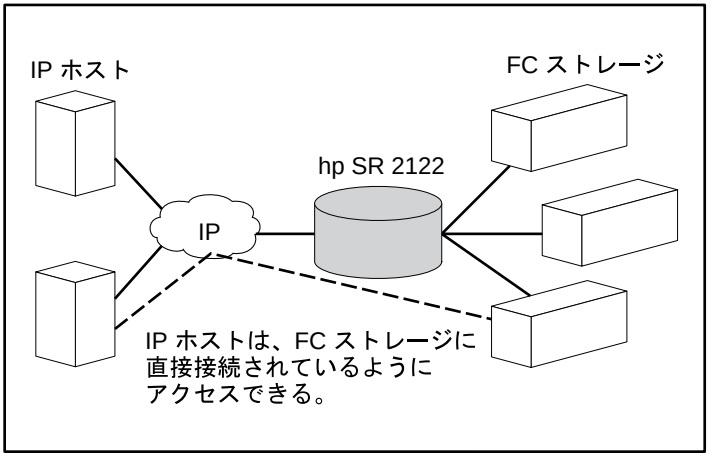

図2: ストレージ ルータを介してストレージにアクセスするIPホスト

ポート

ストレージ ルータには、2つの1 ギガビット イーサネット ポート、コンソール ポート、10/100 イーサネット管理ポート、10/100 イーサネット HA（High Availability：高可用性）ポート、2つの1 ギガビット/2 ギガビット ファイバ チャネル ポートがあります（図3を参照）。

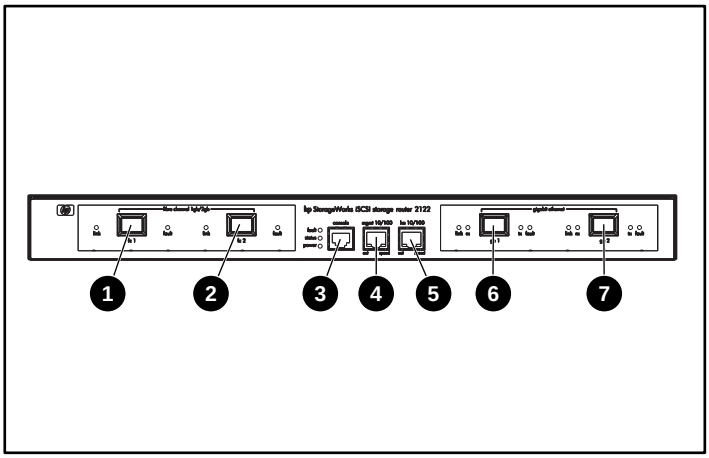

図3: ストレージ ルータのポート

❶ **ファイバ チャネル** 1G/2G、FC 1

❷ **ファイバ チャネル** 1G/2G、FC 2

❸ **コンソール ポート**、CONSOLE

❹ 10/100 **イーサネット管理ポート**、MGMT 10/100

❺ 10/100 **イーサネット** HA (High Availability) **ポート**、HA 10/100

❻ **ギガビット イーサネット**、GE 1

❼ **ギガビット イーサネット**、GE 2

各ポートについては以下の項で説明します。

- ギガビット イーサネット ポート（4ページ）
- コンソール ポート（4ページ）
- 10/100 イーサネット管理ポート（4ページ）
- 10/100 イーサネット HAポート（4ページ）
- ファイバ チャネル ポート（5ページ）

ギガビット イーサネット ポート

ギガビット イーサネット ポートには、GE 1およびGE 2というラベルが付いています（図3を参照）。各ポートは、ストレージにアクセスするIPホストに接続するための1 ギガビット イーサネット インタフェースを提供します。各ポートは、ポートの物理媒体への接続に、SFP（Small Form-Factor Pluggable）モジュールを使用します。SFPモジュールの仕様については、付録B「ケーブル/ポートのピンの配置」を参照してください。各ギガビット イーサネット ポートには、ステータスを示すLEDがあります。LEDの詳細については、5ページの「フロント パネル LED」を参照してください。

コンソール ポート

コンソール ポートにはCONSOLEというラベルが付いています（図3を参照）。このポートは、端末エミュレーション ソフトウェアを実行しているPCのシリアル ポートに接続するためのEIA/TIA-232インタフェースです。コンソール ポートにより、ストレージ ルータのコマンド ライン インタフェース（CLI）を使用してストレージ ルータを管理できます。コンソール ポートは8ピンのRJ-45コネクタで、LEDは付いていません。

10/100 イーサネット管理ポート

10/100 イーサネット管理ポートにはMGMT 10/100というラベルが付いています（ 図3を参照）。このポートは、管理ネットワークに接続するための10BaseT/100BaseT イーサネット インタフェースです。管理ネットワークを通じて、CLI、WebベースのGUI、またはSNMPを使用してストレージ　ルータを管理できます。10/100　イーサネット管理ポートは8ピンのRJ-45コネクタで、ステータスを示すLEDがあります。LEDの詳細については、5ページの「フロント パネル LED」を参照してください。

10/100 イーサネット HAポート

10/100 イーサネット HA（High-Availability）ポートには、HA 10/100というラベルが付いています（図3を参照）。このポートは、HAネットワークに接続するための10BaseT/100BaseT イーサネット インタフェースです。このポートにより、ストレージ ルータは、他のストレージ ルータとともにマルチノード クラスタ環境を構成して、フォールト トレランス機能を提供することができます。10/100 イーサネット HAポートは8ピンのRJ-45コネクタで、ステータスを示すLEDがあります。LEDの詳細については、5ページの「フロント パネル LED」を参照してください。

ファイバ チャネル ポート

ファイバ チャネルポートには、FC 1およびFC 2というラベルが付いています（図3を参照）。各ポートは、ストレージ システム、ファイバ チャネル スイッチ、ファイバ チャネル ホスト、または他のHPストレージ ネットワーク製品に接続するための1 ギガビット/2 ギガビット　ファイバ　チャネルインタフェースを提供します。各ファイバ　チャネルポートは、G_Port、GL_Port、F_Port、FL_Port、またはTL_Portのいずれかとして構成できます。各ポートは、ポートの物理媒体への接続に、SFP（Small Form-Factor Pluggable）モジュールを使用します。SFPモジュールの仕様については、付録B「ケーブル/ポートのピンの配置」を参照してください。各ファイバ チャネルポートには、ステータスを示すLEDがあります。LEDの詳細については、次の「フロント パネル LED」を参照してください。

フロント パネル LED

フロント パネル LEDは、ストレージ ルータのシャーシとポートのステータスを示します（図4を参照）。

- 各ギガビット イーサネット ポート（GE 1とGE 2）には4つのLEDがあり、それぞれLINK、RX、TX、FAULTというラベルが付いています。LEDは、各ギガビット イーサネット ポートの左右にあります。
- FAULT, STATUS, POWER LEDは、ストレージ ルータの全体ステータスを示します。LEDは、CONSOLEポートの左側にあります。
- 10/100 イーサネット管理ポート（MGMT 10/100）には2つのLEDがあり、それぞれACTおよびSPEEDというラベルが付いています。ACT　LEDは、ポートの左下隅にあり、SPEED LEDはポートの右下隅にあります。
- 10/100 イーサネット HAポート（HA 10/100）には2つのLEDがあり、それぞれACTおよびSPEEDというラベルが付いています。ACT LEDは、ポートの左下隅にあり、SPEED LEDはポートの右下隅にあります。
- 各ファイバ チャネル ポートには2つのLEDがあり、それぞれLINKおよびFAULTというラベルが付いています。LEDは、各ファイバ チャネル ポートの左右にあります。

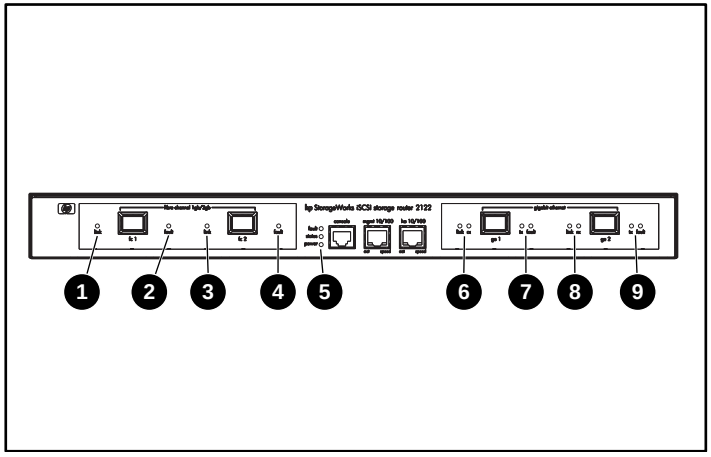

図4: フロント パネル LED

❶ FC 1 LINK

❷ FC 1 FAULT

❸ FC 2 LINK

❹ FC 2 FAULT

❺ FAULT、STATUS、POWER

❻ GE 1 LINK/RX

❼ GE 1 TX/FAULT

❽ GE 2 LINK/RX

❾ GE 2 TX/FAULT

表2: フロント パネル LEDの説明

LED		色	説明
GE 1、GE 2 LED	LINK	緑	ポート使用可
	TX	緑	パケット送信中
	RX	緑	パケット受信中
FAULT		赤	点灯 - ストレージ ルータでエラー発生
			点滅 - ストレージ ルータ コンポーネントでエラー発生
Status		緑	点灯 - 正常に起動
			点滅 - 起動中
POWER		緑	電源オン
MGMT 10/100 LED	ACT	緑	リンク：アクティブ
	SPEED	黄	ポート速度：100Mbps

LED		色	説明
HA 10/100 LED	ACT	緑	リンク：アクティブ
	SPEED	黄	ポート速度：100Mbps
FC 1、FC 2 LED	ACT	黄	フレーム送信中または受信中
	LOG	緑	点灯 - ポートは正常に接続
			点滅（1回/秒）- ポートはログイン中
			点滅（2回/秒）- ポート接続エラー

ファン アセンブリ

ファン アセンブリは、シャーシの内部コンポーネントを冷却します。ストレージ ルータのシャーシは 4 つの排気ファンを装備していて、これらはシャーシの左側に付いています。ファンは、シャーシの右側から吸気し、左側に向かって排気します（図5を参照）。

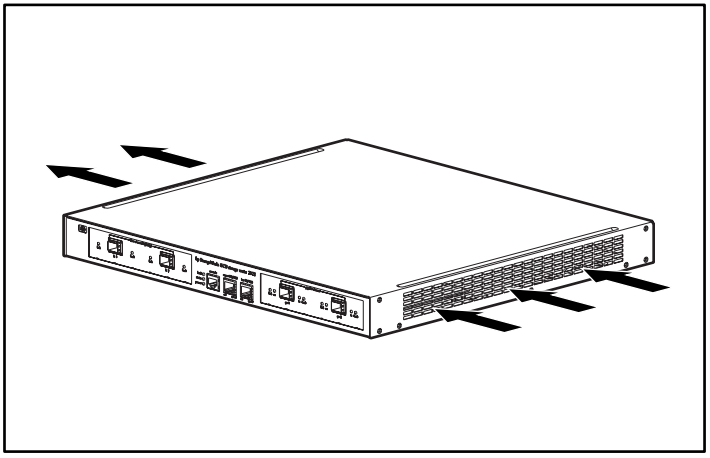

図5: シャーシの通気

電源装置

ストレージ ルータは、温度と出力電圧を監視する内蔵電源装置を装備しています。電源装置は、供給電源が115 VAC/60 Hzまたは230 VAC/50 Hzのどちらであるかを自動的に検知し、それに応じて切り替わります。

状態が危険値に達した場合、過度な熱や電流によってストレージ ルータが損傷しないように電源装置はシャットダウンします。電源装置は、電源コードとリアパネルにある電源コネクタを通じて設置場所の電源と接続されます（図6を参照）。電源装置の電源のオン/オフは、電源コネクタの横にあるロッカー スイッチで行います。スイッチには**I**と**O**というラベルが付いていて、**I**を押すと電源がオンになり、**O**を押すと電源がオフになります。

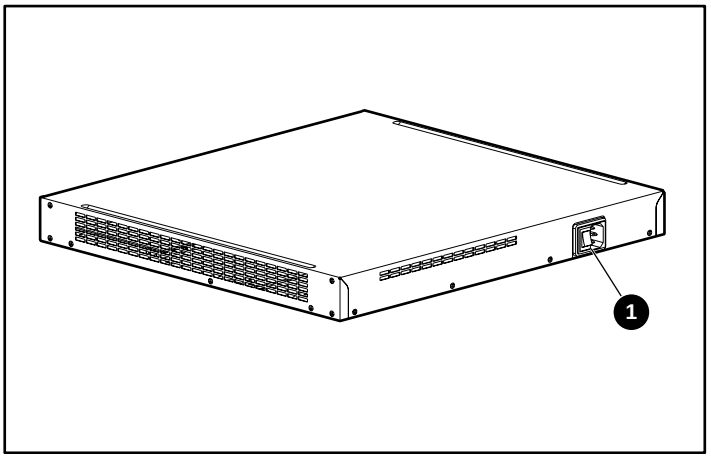

図6: リア パネル、電源コネクタ

❶ **電源コネクタ**

設置

2

この章では、設置場所の準備、ストレージ ルータの設置方法、ネットワークおよびファイバ チャネル ケーブルの接続方法、電源の接続方法、正しく設置されているかどうかの検証方法について説明します。初めて設置する場合は、以下の項の手順を以下の順序で実行してください。

設置場所の計画

ストレージ ルータ、装置用ラック（または配線クローゼット）を置く場所とレイアウトを計画することはストレージ ルータを運用していく上で重要です。装置の設置間隔が近すぎたり、装置を通気が悪い場所に設置すると、システムが過熱することがあります。また、適切な場所に設置しないと、システム パネルが開かなくなったり、メンテナンスが困難になります。

正しく動作することを保証し、メンテナンス作業を必要最低限に抑えるには、設置前に設置場所の計画と準備を行います。

付録Aの表19には、ストレージ ルータの動作時および保管時の環境条件が示されています。システムは指定されている環境条件で動作し続けますが、環境条件が上限または下限に近づくと問題が発生する可能性が高まります。上限値を超える前に環境条件を正すことで、通常の動作状態を維持できます。

設置場所の電源が、設置しているデバイスに適していることを確認してください。電源要件は、ストレージ ルータに必要な配電システムを計画する際に役立ちます。放熱効率は、設置場所の空調装置の容量を検討する際に重要です。ストレージ ルータの電源および放熱効率については、付録Aの表19を参照してください。

注意: 電源を安定して供給するためにも、電源装置に電源を供給している回路の合計最大負荷が、配線およびブレーカの電流容量以下になっていることを確認してください。

ストレージ ルータの設置

ストレージ ルータは、机上や棚、または装置ラックに設置できます。以下の項ではストレージ ルータの設置手順について説明します。

- 机上または棚への設置（10ページ）
- ラックへのストレージ ルータの設置（11ページ）
- SFPモジュールの取り付け（15ページ）

机上または棚への設置

ストレージ ルータは、机上や棚（あるいは安定した平らな場所）に設置することができます。

ストレージ ルータを装置ラックに設置する場合は、次の項「ラックへのストレージ ルータの設置」に進んでください。シャーシを机上または棚に設置する場合は、以下の手順に従ってください。

1. マジックテープ付きのゴム脚を用意します。ゴム脚は、ストレージ ルータに付属のアクセサリ キットに含まれています。
2. マジックテープのシールを剥がし、マジックテープが付いている面をシャーシの裏面の4つの丸いくぼみに貼り付けます。
3. ストレージ ルータをACコンセントが近くにある机上または棚に設置します。

ラックへのストレージ ルータの設置

ストレージ ルータは、19インチの装置ラックにフロント パネルを前面にして設置します。

ストレージ ルータに付属のアクセサリ キットには、2つのレール、2つの蝶ネジ、各種ネジが含まれています。

ストレージ ルータをラックに設置するには、以下の工具が必要です。

- プラス ドライバ
- メジャー

ストレージ ルータをラックに設置するには、以下の手順に従ってください。

1. 設置する準備を行います。
   a. ストレージ ルータを床または安定した机上に置きます。できるだけラックに近く、作業の邪魔にならない場所に置いてください。
   b. メジャーを使って、ラックの奥行きを測ります。フロント マウンティング ポストの外側からリア マウンティング ストリップの外側までの長さを測ります。奥行きは、48.26cm（19インチ）以上81.3cm（32インチ）以下でなければなりません。
   c. 左右のフロント マウンティング ポストの内側の寸法を測り、幅が45.72cm（17.75インチ）であることを確認します。
2. 付属のラック テンプレートを使用して、1Uのマウント位置の中央を示す印を左右のフロントおよびリア マウント用レールに付けます。

3. 手順2で印を付けた位置にケージ ナットを取り付けます（図7を参照）。

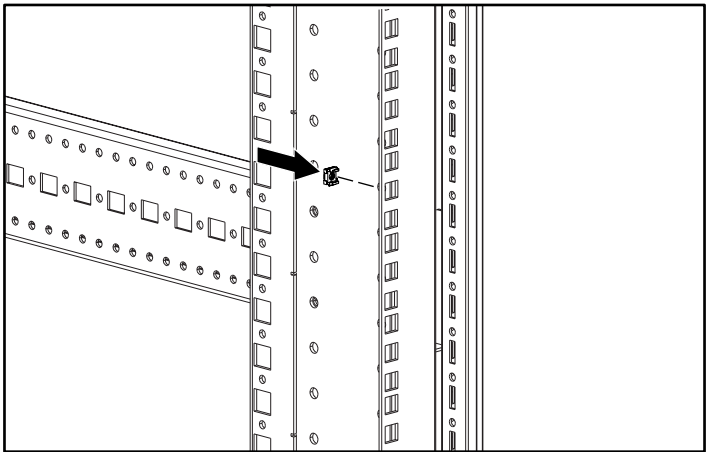

図7: ケージ ナットの取り付け

4. 付属の蝶ネジを使用してレールを取り付けます（図8を参照）。

注記: のちの設置手順にレールを調整する作業があります。蝶ネジは完全に締め付けないでください。

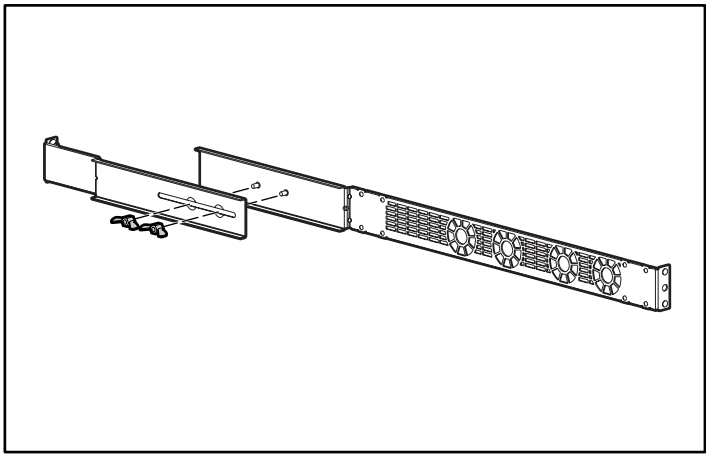

図8: レールの組み立て

5. シャーシの両側に付いているすべてのネジ（6個）を取り外します（図9を参照）。

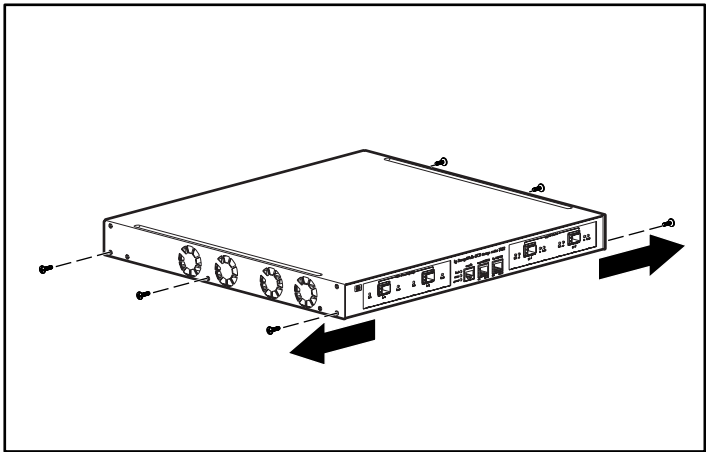

図9: ネジの取り外し

6. レールをシャーシに合わせ、付属の皿ネジを使用して取り付けます（図10を参照）。

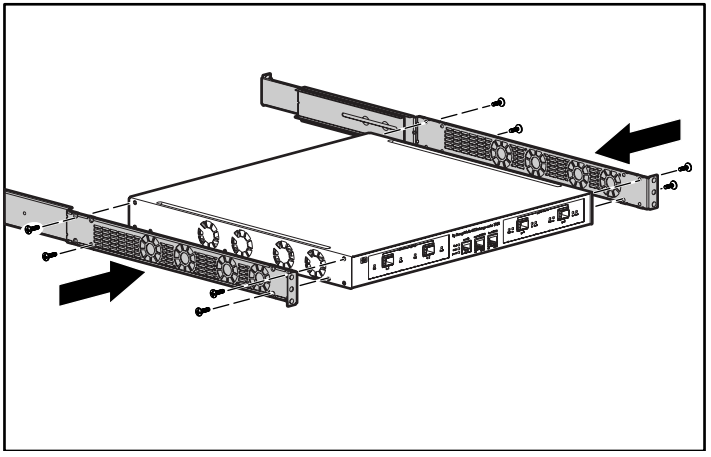

図10: レールの取り付け

7. ストレージ ルータをラックに差し込み、ラックのネジを使用してレールの前面を固定します（図11を参照）。

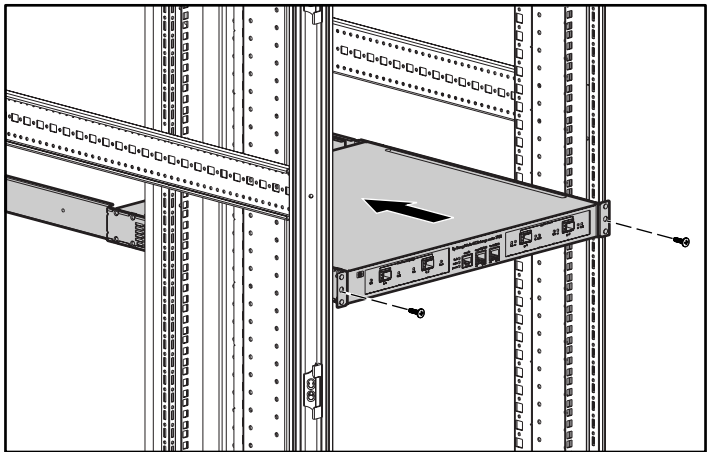

図11: ラックへのストレージ ルータの設置

8. ❶を調整し、ラック ネジ❷を使用してレールの背面を固定します（図12参照）。
9. 蝶ネジ❸を締めて前後のレールを固定します。

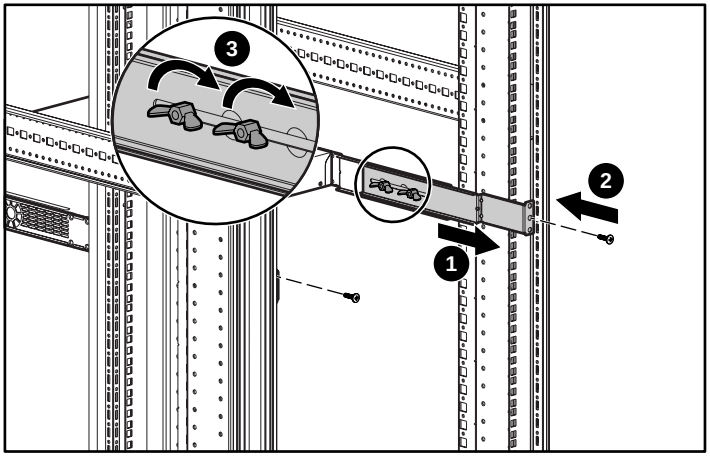

図12: レール背面の固定

SFPモジュールの取り付け

SFP（Small Form-Factor Pluggable）モジュールの取り付けまたは取り外しを行う前に、この項の説明を読んでください。ギガビット イーサネットおよびファイバ チャネルポートのSFP モジュールに接続する方法については、「ギガビット イーサネットおよびファイバ チャネル ポートへの接続」を参照してください。

注記: 相互運用性の問題により、HPではサード パーティから購入されたSFPはサポートしていません。SFPポートの仕様については、付録B「ケーブル/ポートのピンの配置」を参照してください。

注記: 光ファイバ ケーブルのプラグをSFPモジュールのコネクタから外した場合は、それぞれにダスト カバーを取り付けてください。

警告: 光ファイバ ケーブルが接続されていない場合、ポート開口部から不可視光線が放射されることがあります。光線にあたらないように注意し、開口部を覗き込まないでください。警告の各国語版については、デバイスに付属の『Regulatory Compliance and Safety』マニュアルを参照してください。

ギガビット イーサネット ポートには、MT-RJコネクタ（図13を参照）またはLCコネクタ（図14を参照）の光ファイバSFPモジュールを使用します。ファイバ チャネルポートには、LCコネクタ（ 図14を参照）の光ファイバSFPモジュールを使用します。ギガビット イーサネットおよびファイバ　チャネルポートに取り付け可能なSFPモジュールのタイプについては、表3を参照してください。モジュールの仕様については、付録B「ケーブル/ポートのピンの配置」を参照してください。

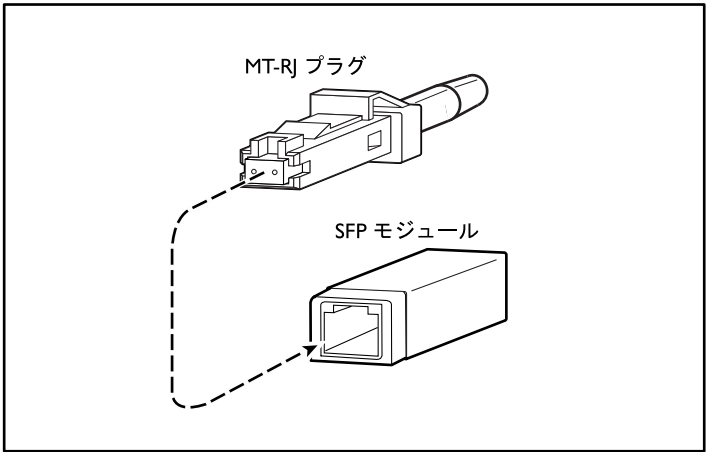

図13: MT-RJ光ファイバ コネクタとSFPモジュール

注意: 光ファイバSFPモジュールからケーブルを取り外した場合は、SFPにきれいなダストカバーを挿入して SFP モジュールを保護してください。光ファイバ ケーブルを別の SFP モジュールの光学開口部に差し込む場合は、必ず光ファイバ ケーブルの光学面を清掃してから差し込んでください。SFPモジュールの光学開口部に埃などが入らないようにしてください。埃などによって光が遮られると正しく動作しません。

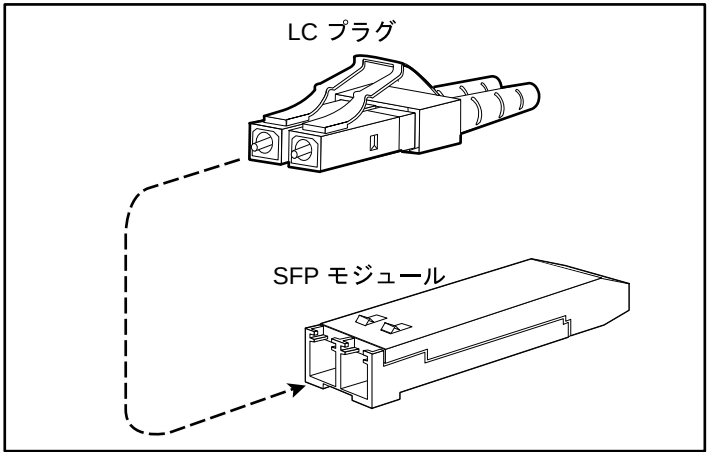

図14: LCコネクタとSFPモジュール

表3: ギガビット イーサネットおよびファイバ チャネル ポートのSFPモジュールのタイプ

SFP オプション キットの部品番号	コネクタのタイプ	ポート
221470-B21	LC	ギガビット イーサネットまたはファイバ チャネル

SFPモジュールは3種類あり、それぞれポートにSFPモジュールを固定したり取り外したりする際のラッチ デバイスが異なります。以下の項では、SFPモジュールのタイプについて説明します。

- Mylar Tab SFPモジュール（18ページ）
- Actuator/Button SFPモジュール（20ページ）
- Bale Clasp SFPモジュール（22ページ）

Mylar Tab SFPモジュール

Mylar Tab SFPモジュール（図15を参照）には、ポートからモジュールを取り外す際に引っ張るタブが付いています。

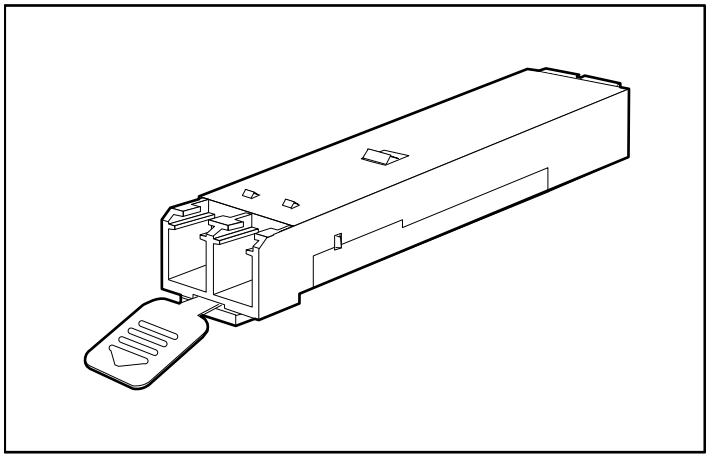

図15: Mylar Tab SFPモジュール

Mylar Tab SFPモジュールをポートに挿入するには、SFPモジュールをポートに揃えて所定の位置まで押し込みます（図16を参照）。

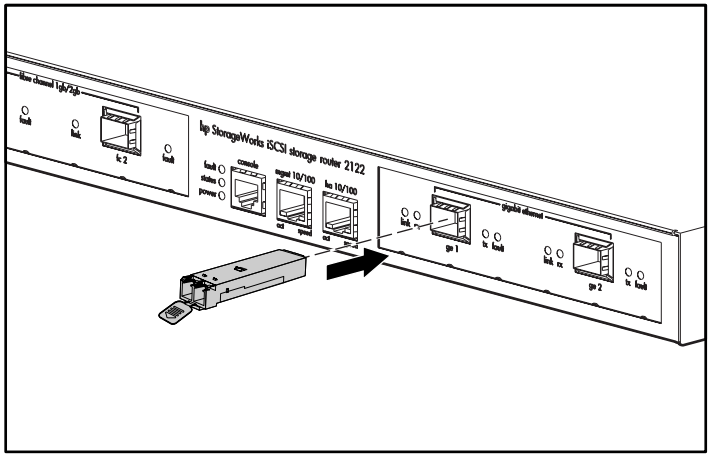

図16: Mylar Tab SFPモジュールの挿入

注意: SFPモジュールを取り外す場合は、SFPモジュールがポートからまっすぐ引き出されるようにタブをまっすぐに引っ張ってください。タブを斜めに引っ張ると、タブが SFP モジュールから取れてしまうことがあります。

ポートからSFPモジュールを取り外すには、SFPモジュールがポートから外れるまでタブをやや下向きにそっと引っ張り、SFPモジュールを引き出します（図17を参照）。

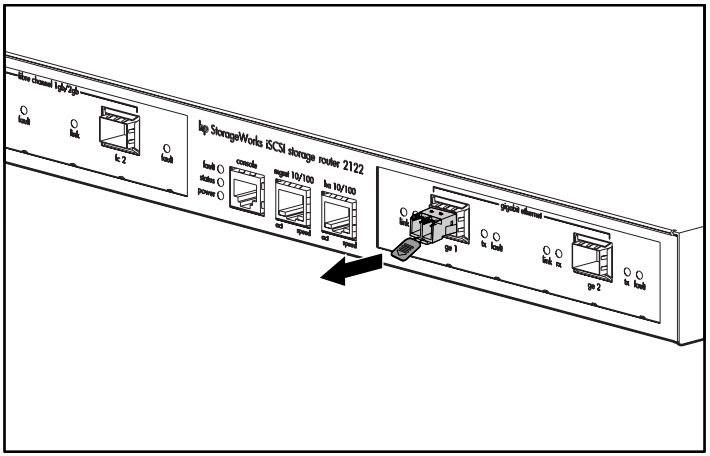

図17: Mylar Tab SFPモジュールの取り外し

Actuator/Button SFPモジュール

Actuator/Button SFPモジュール（図18を参照）には、SFPモジュールをポートから取り外すための押しボタンがあります。

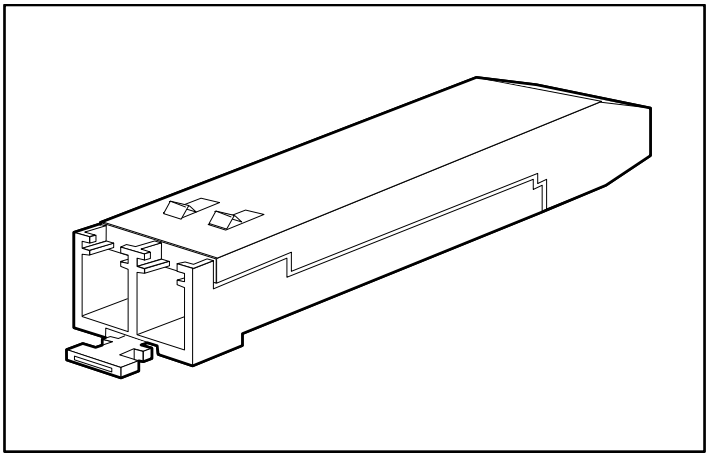

図18: Actuator/Button SFPモジュール

Actuator/Button SFPモジュールをポートに挿入するには、SFPモジュールをポートに揃え、カチッと音がして所定の位置に収まるまで押し込みます（図19を参照）。SFPモジュールを挿入するときにはアクチュエータ ボタンを押さないようにしてください。アクチュエータ ボタンを押すと、SFPモジュールがポートから外れます。

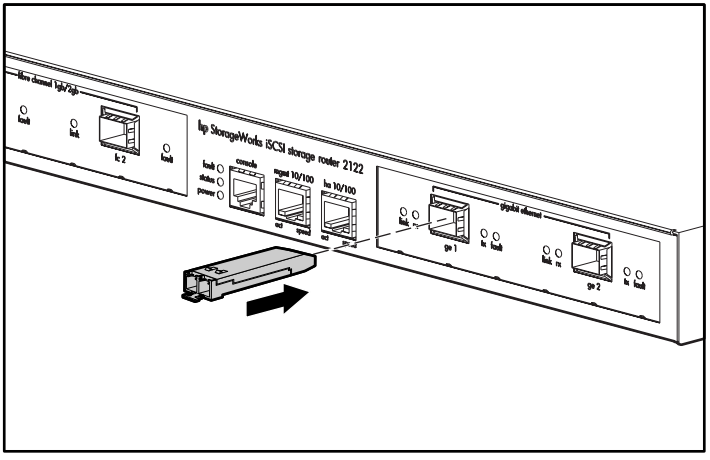

図19: Actuator/Button SFPモジュールの挿入

Actuator/Button SFPモジュールをポートから取り外すには、以下の手順を実行します。

1. カチッと音がしてラッチ機構が働いて SFP モジュールがポートから解放されるまで、SFP モジュールの前面にあるアクチュエータ ボタン ❶ をそっと押します（図 20 を参照）。
2. 親指と人差し指でアクチュエータ ボタンをつかみ、SFPモジュール❷をポートから引き出します（図20を参照）。

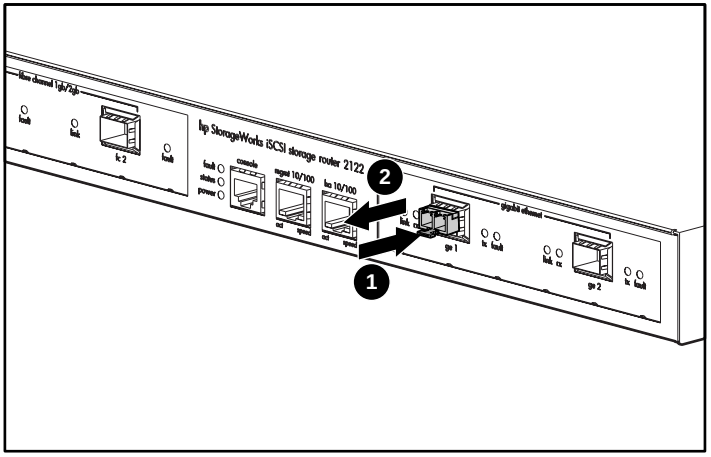

図20: ポートからのActuator/Button SFPモジュールの取り外し

Bale Clasp SFPモジュール

Bale Clasp SFPモジュール（図21を参照）には、SFPモジュールをポートに固定するための留め金具が付いています。

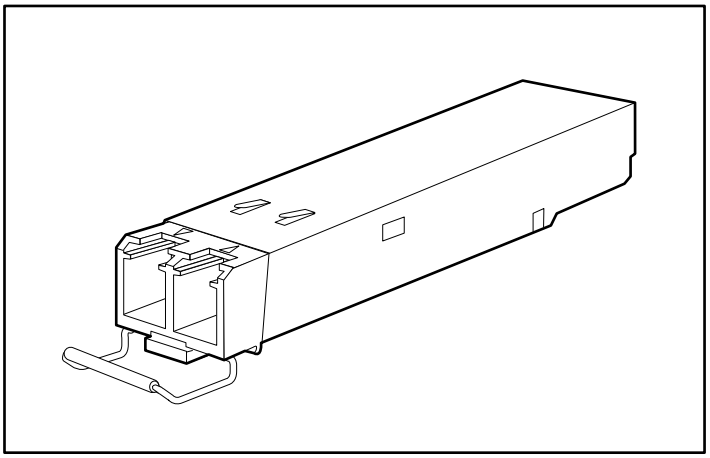

図21: Bale Clasp SFPモジュール

Bale Clasp SFPモジュールをポートに挿入するには、以下の手順に従います。

1. SFPモジュールを挿入する前に留め金具を閉じます。
2. SFPモジュールをポートに揃え、ポートに押し込みます（図22を参照）。

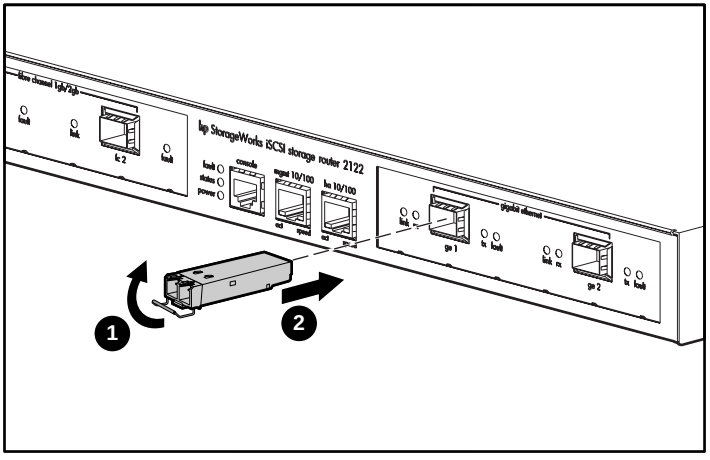

図22: ポートへのBale Clasp SFPモジュールの挿入

Bale Clasp SFPモジュールをポートから取り外すには、以下の手順に従います。

1. 人差し指でSFPモジュールの留め金具を下向きに回転させて開きます（図23を参照）。留め金具が人差し指で開かない場合は、小さなマイナス ドライバか先の尖ったものを使用して留め金具を開きます（図24を参照）。
2. 親指と人差し指でSFPモジュールをつかみ、ポートからそっと取り出します（図23を参照）。

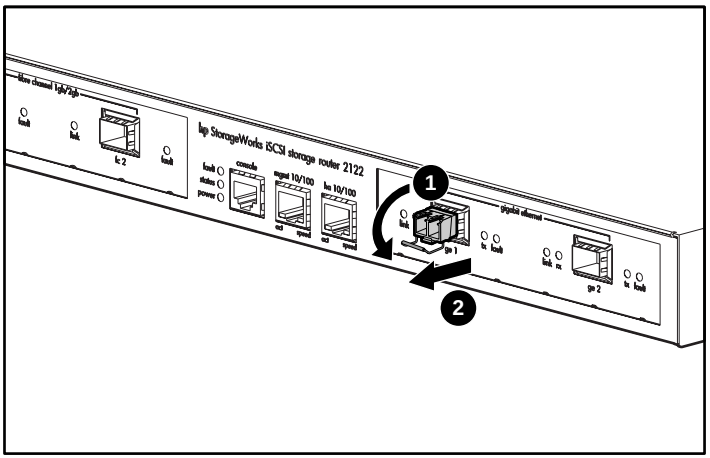

図23: 人差し指によるBale Clasp SFPモジュールの取り外し

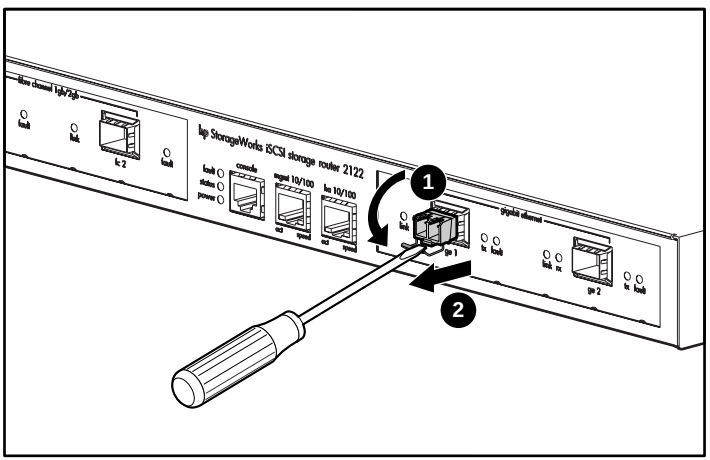

図24: マイナス ドライバによるBale Clasp SFPモジュールの取り外し

ギガビット イーサネットおよびファイバ チャネル ポートへの接続

ギガビット イーサネット ポート（GE 1およびGE 2）は、MT-RJまたはLCタイプの光ファイバSFPモジュールとケーブルを使用します。ファイバ チャネル ポート（FC 1およびFC 2）は、LC タイプの光ファイバ SFP モジュールとケーブルを使用します。光ファイバ SFP モジュールにケーブルを接続する際は、ケーブルのプラグをソケットにしっかりと差し込んでください。プラグの上端がソケットの手前上端にはまる必要があります。プラグがソケットに固定されるとカチッと音がします。プラグがソケットに固定されているかどうかを確認するには、プラグをそっと引いてみてください。

ソケットからプラグを取り外すには、プラグ上部のツメを押してラッチを解放します。カチッと音がして、ラッチが解放されます。プラグをソケットからそっと引き出します。

注記: モジュールから光ファイバ ケーブルを外す際は、コネクタのジャケットスリーブではなく、コネクタの本体部分を持って外してください。スリーブを持って取り外すと、長い間にコネクタ内の光ファイバ ケーブルのターミネーションの完全性が損なわれます。

MT-RJプラグのフェイス プレート（光ファイバ開口部の周り）に汚れや皮脂が付いていると減衰率が高まり、光学強度がしきい値以下に低下し、リンクが確立できなくなります。MT-RJプラグのフェイス プレートを清掃するには、以下の手順に従います。

1. 糸くずの出ない布を純度99%のイソプロピル アルコールに浸し、フェイス プレートをそっと拭きます。
2. ケーブルを取り付ける前に、フェイス プレートに残っている埃を圧縮空気で吹き飛ばします。

注記: 光ファイバ ケーブルのプラグをSFPモジュールのコネクタから外した場合は、それぞれにダスト カバーを取り付けてください。

以下の項では、ギガビット イーサネットおよびファイバ チャネル ポートにケーブルを接続する方法について説明します。

- ギガビット イーサネット ポートへの接続（24ページ）
- ファイバ チャネル ポートへの接続（25ページ）

ギガビット イーサネット ポートへの接続

ギガビット イーサネット ポートにケーブルを接続するには、以下の手順に従います。

1. ギガビット イーサネット ポートに挿入されているSFPモジュールからダスト カバーを取り外します。取り外したダスト カバーは保管しておいてください。
2. ケーブルのプラグからダスト カバーを取り外します。取り外したカバーは保管しておいてください。ギガビット イーサネットのSFPモジュールにケーブルを差し込みます。
3. ケーブルのもう一方の端を外部の終端システム、スイッチ、またはルータに接続します。

ファイバ チャネル ポートへの接続

ファイバ チャネル ポートにケーブルを接続するには、以下の手順に従います。

1. ファイバ チャネル SFPポートに挿入されているSFPモジュールからダスト カバーを取り外します。取り外したダスト カバーは保管しておいてください。
2. 光ファイバ ケーブルのプラグからダスト カバーを取り外します。取り外したダスト カバーは保管しておいてください。ファイバ チャネルのSFPモジュールにケーブルを差し込みます。
3. ケーブルのもう一方の端を他のシステム（ストレージ システム、スイッチ、ホスト、または他のストレージ ルータなど）のファイバ チャネル ポートに差し込みます。

10/100 イーサネット管理ポートとHAポートへの接続

10/100 管理ポートとHAポートに接続するには、以下の手順に従います。

1. 10/100 管理ポートとHAポートを終端システムに接続する場合は、モジュラ RJ-45 ストレートUTP ケーブルを使用します。外部スイッチやルータに接続する場合は、モジュラ RJ-45 クロスUTP ケーブルを使用します。
2. 適切なモジュラ ケーブルを10/100 管理ポートとHAポートに接続します（図25を参照）。

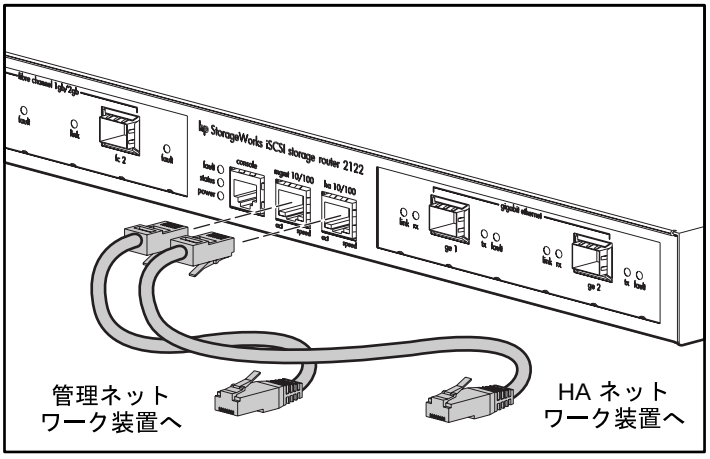

図25: 10/100 管理ポートとHAポートへの接続

3. ケーブルのもう一方の端を外部の終端システム、スイッチ、またはルータに接続します。

コンソール ポートへの接続

ストレージ ルータにローカル管理アクセスを行えるように、PCのシリアル ポートをコンソール ポートに接続します。PCは、VT100端末エミュレーションをサポートしている必要があります。端末エミュレーション ソフトウェア（HyperTerminalやProcomm PlusなどのPCアプリケーション）を使用して、セットアップや設定時にストレージ ルータとPC間で通信を行えるようになります。

コンソール ポートに接続するには、以下の手順に従います。

1. コンソール ポートのデフォルトの特性と一致するようにPC端末エミュレーション プログラムを設定します。

表4: コンソール ポートのデフォルトの特性

コンソール ポートのデフォルトの特性	
転送速度（bps：ビット/秒）	9600
データビット	8
パリティ	**なし**
ストップ ビット	1
フロー制御	**なし**

2. 付属のRJ-45/DB-9メス アダプタをPCのシリアル ポートに接続します。
3. 付属のコンソール ケーブルの一方の端（RJ-45/RJ-45ロールオーバ ケーブル）をコンソール ポートに接続します。もう一方の端をPCのシリアル ポートのRJ-45/DB-9アダプタに接続します（図26を参照）。

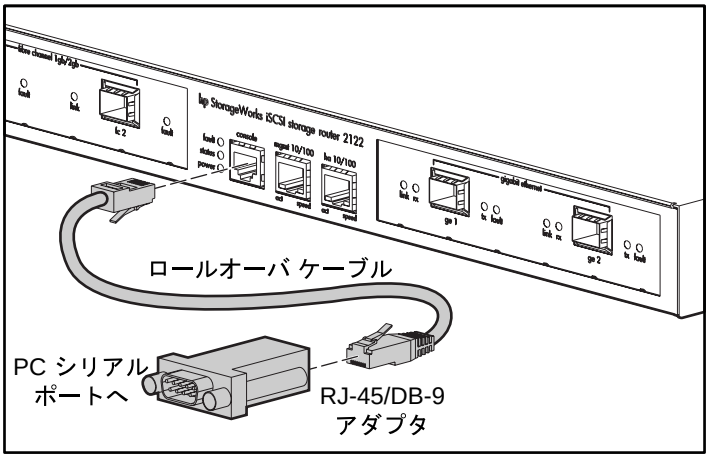

図26: コンソール ケーブルの接続

電源の接続

ストレージ ルータは、115～120 VAC/60 Hzまたは230～240 VAC/50 Hzのいずれかの電源に接続できます。電源装置は供給電源を自動的に検知し、それに応じて切り替わります。

ストレージ ルータに電源を接続するには、以下の手順に従います。

1. 電源スイッチがオフの位置になっていることを確認します（図27を参照）。

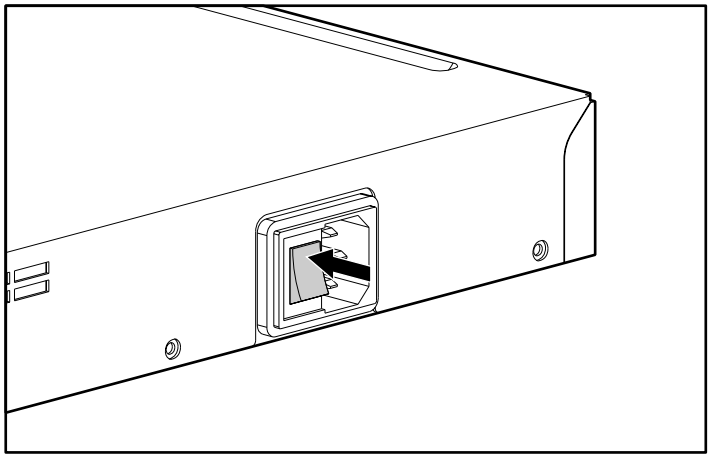

図27: 電源オフの状態

2. シャーシのリヤ パネルにある電源コネクタに電源コードを差し込みます（図 28 を参照）。

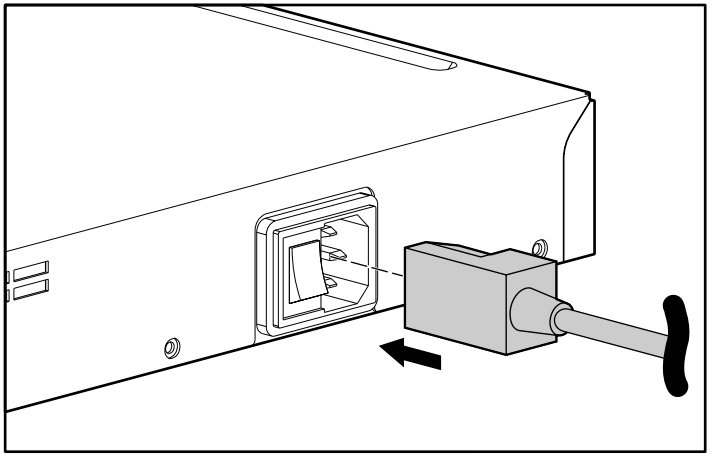

図28: 電源コネクタへの電源コードの接続

3. 電源コードのもう一方の端をストレージ ルータ用の電源に差し込みます。

正しく設置されているかどうかの確認

ストレージ ルータが正しく設置されていることを確認するには、ストレージ ルータが正常に起動し、ネットワークやファイバ チャネル接続が機能していることを確認します。

正しく起動するかどうかの確認

ストレージ ルータが正しく起動するかどうかを確認するには、以下の手順に従います。

1. ストレージ ルータのリヤ パネルにある電源スイッチをオンの位置にします。
2. ストレージ ルータのフロント パネルにあるPOWER LEDを見て、電源がオンになっていることを確認します。FAULT LEDが消灯していることを確認します。
3. ファンの回転音と通気の有無を調べて、ファン アセンブリが動作していることを確認します。
4. コンソールの出力を参照して、ストレージ ルータ ソフトウェアが正常に起動していることを確認します。起動プロセスが完了するまで3～5分かかり、その間起動情報とバナーが表示されます。正常に起動した場合は、ユーザー入力が可能なCLIプロンプトが表示されます。
5. このようにならない場合は、第3章「トラブルシューティング」を参照して問題を特定し、可能な場合は対処します。

ネットワーク接続が機能しているかどうかの確認

ネットワーク接続が機能しているかどうかを確認するには、ギガビット イーサネット ポート、10/100 イーサネット管理ポート、10/100 HAポートが機能していることを確かめます。

ネットワーク接続が機能しているかどうかを確認するには、以下の手順を実行します。

1. ポートのリンク ステータスLEDを調べて、ギガビット イーサネット ポート接続が機能していることを確認します。LEDの説明については、第1章の表2（6 ページ）を参照してください。
2. ポートのリンク ステータスLEDを調べて、10/100 イーサネット管理ポート接続が機能していることを確認します。LEDの説明については、第1章の表2を参照してください。
3. ポートのリンク ステータスLEDを調べて、10/100 HAポート接続が機能していることを確認します。LEDの説明については、第1章の表2を参照してください。
4. これらのポート接続が機能していない場合は、第3章「トラブルシューティング」を参照して問題を特定し、可能な場合は対処します。

ファイバ チャネル接続が機能しているかどうかの確認

接続が機能しているかどうかを確認するには、以下の手順を実行します。

1. ファイバ チャネルのLOG LEDを調べて、ファイバ チャネルポート接続が機能していることを確認します。LEDの説明については、第1章の表2を参照してください。

2. 接続されているポートのLOG LEDが点滅している場合は、第3章「トラブルシューティング」を参照して問題を特定し、可能な場合は対処します。

次の作業

ストレージ ルータ ハードウェアが正しく設置されたことを確認したら、ソフトウェアの設定を行います。ソフトウェアの設定方法については、第4章「ソフトウェアの概要」を参照してください。

トラブルシューティング

3

この章では、設置時に発生した問題の対処方法について説明します。以下の内容について説明します。

コンポーネント レベルでの問題の解決

ストレージ ルータのトラブルシューティングで重要なことは、問題の原因となっているストレージ ルータ コンポーネントを特定することです。まず、ストレージ ルータが本来実行すべきことを実行しているかどうかを確認します。起動時の問題は、通常、1つのコンポーネントが原因で発生するため、ストレージ　ルータの各コンポーネントをトラブルシューティングするのではなく、問題の原因となっているサブシステムを特定したほうが効率的です。

ストレージ ルータは、以下のサブシステムで構成されています。

- 電源装置。システムの電源がオンの状態で常に動作します（34 ページの「電源装置のトラブルシューティング」を参照）。
- シャーシのファン アセンブリ。システムの電源がオンの状態で常に動作します。高温状態または過電圧状態により、電源装置がストレージ ルータをシャットダウンした場合でもファンは動作し続けます（電源装置がシャットダウンした場合は、ストレージ ルータもシャットダウンします）。

  ファンに問題があるかどうかを判断するには、以下のことを確認します。

  — ファンの回転音の有無を調べて、ファン アセンブリが動作しているかどうかを確認します。

  — ストレージ ルータの通気が妨げられていないことを確認します。

  ファン アセンブリが正常に動作していないことがわかった場合は、カスタマ サービス担当者に連絡してください。

起動時の問題の特定

起動時の問題を特定するには、ストレージ ルータの動作とフロント パネルのLEDを確認します。LEDは、起動シーケンスでのストレージ ルータの状態を示します。LEDを確認することで、起動シーケンスのどの部分で障害が発生したかを判断できます。

ストレージ ルータの電源を入れるには、以下の手順に従います。

1. シャーシのファン アセンブリが動作していることを確認します。動作していない場合は、34 ページの「電源装置のトラブルシューティング」を参照してください。電源装置が正しく機能していて、ファン アセンブリが故障していることがわかった場合は、カスタマ サービス担当者に連絡してください。初めて起動したときにファン アセンブリが正しく動作しない場合（設置時の調整項目はありません）は、カスタマ サービス担当者に連絡してください。
2. フロント パネルのPOWER LEDを確認します。POWER LEDは、電源を入れた直後に点灯し、ストレージ ルータの通常の動作時には点灯したままになります。LEDが点灯していない場合は、34 ページの「電源装置のトラブルシューティング」を参照してください。
3. フロント パネルのSTATUSおよびFAULT LEDを確認します。LEDの説明については、第1章「フロント パネル LED」を参照してください。
4. フロント パネルのネットワークおよびファイバ チャネル ポートのLEDを確認します。LEDの説明については、第1章「フロント パネル LED」を参照してください。ネットワークまたはファイバ チャネル ポートのLEDがポート接続で問題があることを示している場合は、35 ページの「ネットワークまたはファイバ チャネル ポート接続に関するトラブルシューティング」を参照してください。
5. PC端末エミュレーション プログラムが正しく設定されていて、PCがコンソール ポートに正しく接続されていることを確認します。また、PC端末エミュレーション プログラムがストレージ ルータが正しく起動したことを示している（設定ウィザードを開始するためのプロンプトやCLIプロンプトが表示されている）ことを確認します。
6. ステータスLEDが障害が発生していることを示していたり、起動プロセスが不完全な状態で終了したことがコンソール ポートに接続されているPCに表示された場合は、カスタマ サービス担当者に連絡してください。

電源装置のトラブルシューティング

電源の問題の原因を特定するには、以下の手順に従います。

1. POWER LEDを確認します。
   - POWER LEDが点灯していない場合は、電源コードを差し込み直します。
   - POWER LEDが点灯しない場合は、電源が供給されていることと、電源コードに問題がないかどうかを確認してください。
2. 電源コードを別の電源に差し込みます。
   - POWER LEDが点灯した場合は、供給電源に問題があります。
   - 電源コードを別の電源に差し込んでも POWER LED が点灯しない場合は、電源コードを交換してください。
   - 新しい電源コードを別の電源に差し込んでも POWER LED が点灯しない場合は、電源装置が故障している可能性があります。
3. 問題を解決できない場合は、カスタマ サービス担当者に連絡してください。

ネットワークまたはファイバ チャネル ポート接続に関するトラブルシューティング

ネットワークまたはファイバ チャネル ポートのLEDが問題があることを示している場合は、以下の項の手順を実行して問題の原因を特定してください。

- ギガビット イーサネット ポートへの接続に関するトラブルシューティング（35ページ）
- 10/100 イーサネット管理ポートまたは10/100 イーサネット HAポートへの接続に関するトラブルシューティング（36ページ）
- ファイバ チャネル ポートへの接続に関するトラブルシューティング（37ページ）

ギガビット イーサネット ポートへの接続に関するトラブルシューティング

ギガビット イーサネット（GE 1またはGE 2）ポートへの接続が不良な場合は、LINK LEDが点灯しません。LINK LEDが点灯していない場合は、以下の手順を実行して問題の原因を特定してください。

1. ケーブルが正しく接続されていて、良好な動作状態になっていることを確認します。
   - ケーブルの両端を差し込み直します。LINK LEDが点灯した場合は、ケーブルが正しく接続されていなかったことが原因です。
   - LINK LEDが点灯しない場合は、ケーブルを交換してください。ケーブルを交換してLINK LEDが点灯したら、ケーブルが不良です。
   - ケーブルを交換してもLINK LEDが点灯しない場合、ケーブルが原因であることはほとんどありません。次の手順に進んでください。
2. ポートが接続されている外部の終端システム、スイッチ、またはルータを確認します。
   - 外部の終端システム、スイッチ、またはルータが正常に動作している場合は、次の手順に進んでください。
   - 外部の終端システム、スイッチ、またはルータが正常に動作していない場合は、それらの問題を解決してください。LINK LEDが点灯すれば、外部の終端システム、スイッチ、またはルータに問題があります。
   - LINK LEDが点灯しない場合は、次の手順に進んでください。
3. SFPモジュールを交換します。
   - LINK LEDが点灯すれば、SFPモジュールに問題があります。
   - LINK LEDが点灯しない場合は、カスタマ サービス担当者に連絡してください。

10/100 イーサネット管理ポートまたは10/100 イーサネット HAポートへの接続に関するトラブルシューティング

10/100 イーサネット管理ポートまたは10/100 イーサネット HAポート（MGMT 10/100またはHA 10/100）の接続が不良な場合は、ACT LEDが点灯しません。ACT LEDが点灯しない場合は、以下の手順を実行して問題の原因を特定してください。

1. ケーブルが正しく接続されていて、良好な動作状態になっていることを確認します。
   - ケーブルが正しいタイプのケーブルを使用していることを確認してください（付録B「ケーブル/ポートのピンの配置」を参照）。
   - ケーブルの両端を差し込み直します。ACT LEDが点灯した場合は、ケーブルが正しく接続されていなかったことが原因です。
   - ACT LEDが点灯しない場合は、ケーブルを交換してください。ケーブルを交換してACT LEDが点灯したら、ケーブルが不良です。
   - ケーブルを交換してもACT LEDが点灯しない場合、ケーブルが原因であることはほとんどありません。次の手順に進んでください。
2. ポートが接続されている外部の終端システム、スイッチ、またはルータを確認します。
   - 外部の終端システム、スイッチ、またはルータが正常に動作している場合は、次の手順に進んでください。
   - 外部の終端システム、スイッチ、またはルータが正常に動作していない場合は、それらの問題を解決してください。ACT LEDが点灯すれば、外部の終端システム、スイッチ、またはルータに問題があります。
   - ACT LEDが点灯しない場合は、カスタマ サービス担当者に連絡してください。

ファイバ チャネル ポートへの接続に関するトラブルシューティング

ファイバ チャネル ポート（FC 1またはFC 2）への接続が不良な場合は、LOG LEDが1秒間に2回点滅します。LOG LEDが1秒間に2回点滅している場合は、以下の手順を実行して問題の原因を特定してください。

1. ストレージ ルータのドメイン IDが正しく設定されていることを確認します。ドメイン IDが正しく設定されている場合は、次の手順に進んでください。

注記: 接続の問題が解決されると、LOG LEDは、1秒間に1回点滅するログイン状態がしばらく続いた後に点灯します。

---

2. ケーブルが正しく接続されていて、良好な動作状態になっていることを確認します。
   - ケーブルの両端を差し込み直します。LOG LEDが点灯した場合は、ケーブルが正しく接続されていなかったことが原因です。
   - LOG LEDが点灯しない場合は、ケーブルを交換してください。ケーブルを交換してLOG LEDが点灯したら、ケーブルが不良です。
   - ケーブルを交換してもLOG LEDが点灯しない場合、ケーブルが原因であることはほとんどありません。次の手順に進んでください。
3. ポートに接続しているデバイスまたはスイッチを確認します。
   - デバイスまたはスイッチが正常に動作している場合は、次の手順に進んでください。
   - デバイスまたはスイッチが正常に動作していない場合は、それらの問題を解決してください。LOG LEDが点灯すれば、デバイスまたはスイッチに問題があります。
   - LOG LEDが点灯しない場合は、次の手順に進んでください。
4. SFPモジュールを交換します。
   - LOG LEDが点灯すれば、SFPモジュールに問題があります。
   - LOG LEDが点灯しない場合は、カスタマ サービス担当者に連絡してください。

カスタマ サービスへの連絡方法

この章のトラブルシューティング手順を実行しても起動時の問題を解決できない場合は、カスタマ サービス担当者に連絡してサポートを要請してください。サービス担当者が迅速に問題を解決できるように、お問い合わせになる前に以下の情報を用意してください。

- ストレージ ルータの納入日
- シャーシのシリアル番号（シャーシのリヤ パネルの右上のラベルに記載されています）
- ソフトウェアの種類とリリース番号
- メンテナンス契約や保証に関する情報
- 問題となっている状況の簡単な説明
- 問題を特定および解決するために実行した手順の簡単な説明

ソフトウェアの概要

4

ストレージ ルータ の設置および設定に必要な手順は以下のとおりです。

- 第2章「設置」または『*hp StorageWorks iSCSI ストレージ ルータ 2122 インストール手順*』の指示に従ってストレージ ルータを設置する
- このガイドの説明に従ってストレージ ルータ ソフトウェアを設定する
- ストレージ　ルータに接続されているIPホストにiSCSIドライバをインストールして設定する。iSCSI ドライバは、内蔵 iSCSI プロトコルがインストールされている TCP/IP Offload Engine（TOE）を備えているIPホストでは必要ありません。

この章では、ストレージ ルータ ソフトウェアの設定方法について説明します。ここでは、ストレージ　ルータの機能とソフトウェア設定手順を理解するのに役立つ非常に基本的な以下の内容について説明します。

ストレージ ルータ ソフトウェアの概要

ストレージ ルータを使用することで、さまざまな場所からIPネットワーク経由でストレージにアクセスできるようになります。ストレージ ルータ ソフトウェアは、ストレージ ルータの動作を制御します。このソフトウェアにより、SCSIルーティングを使用してIPネットワーク経由でストレージにアクセスできます。

SCSIルーティングにより、IPホストは、iSCSIプロトコルを使用してファイバ チャネル（FC）ストレージ デバイスにアクセスすることができます。

注記: **iSCSIプロトコルは、IPストレージ（ips）用のIETF定義のプロトコルです。iSCSIプロトコルの詳細については、** http: / / www.ietf.org **に掲載されているIPストレージ用のIETF規格に関するページを参照してください。**

SCSI ルーティングを使用した場合、ストレージ デバイスへのアクセスは主にストレージ ルータで管理します（ 図29を参照）。

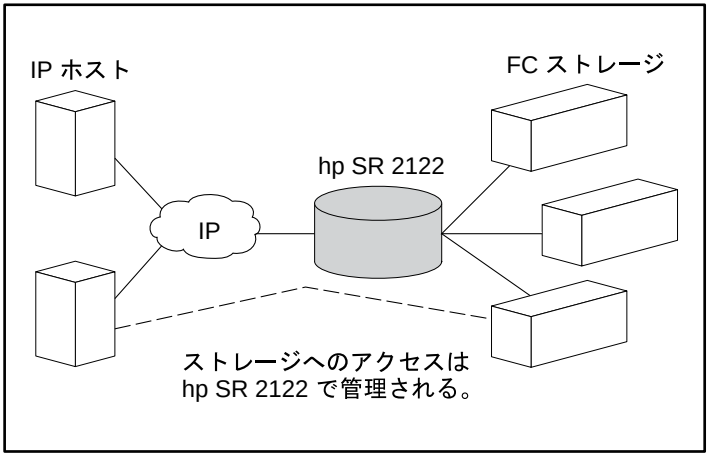

図29: SCSIルーティング

ストレージ ルータ ソフトウェアは、IPネットワーク経由でストレージにアクセスするためのサービスのほかに、以下のサービスを提供しています。

- **VLANアクセス制御：**VLAN ID（VID）番号に基づいた、ストレージへのIPアクセス制御を提供します（アクセス リストによるアクセス制御に加え）。
- **認証：**AAA認証方法を使用したiSCSI認証を提供します。
- **高可用性（HA）：**フェールオーバーや他のクラスタ関連の機能を実現できるようにストレージ ルータをクラスタにグループ化できます（SCSIルーティングのみ）。
- **SNMP/MIBサポート：**選択したMIBを使用したSNMPによるストレージ ルータのネットワーク管理を提供します。
- **コマンド ライン インタフェース（CLI）およびWebベースのGUI：**ストレージ ルータの設定およびメンテナンスを行うためのユーザー インタフェースを提供します。
- **SSL（Secure Sockets Layer）サポート：**WebベースのGUI経由での安全なアクセスを実現するためのHTTPS接続を提供します。

SCSIルーティングの概要

SCSIルーティングにより、IPホストは、ストレージ デバイスがホストに直接接続されている場合と同じようにFCストレージ デバイスや、ストレージ ルータで主に管理されているデバイスにアクセスできます。物理ストレージ デバイスのグループであるiSCSIターゲット（論理ターゲットとも言います）が作成され、ストレージ ルータに接続されている物理ストレージ デバイスにマップされます。ストレージ ルータは、物理ストレージ デバイスがホストに直接接続されているかのようにiSCSIターゲットをIPホスト（iSCSIイニシエータ）に提示します（図30を参照）。SCSIルーティングでは、ストレージ デバイスはそれぞれのIPホストではなくストレージ ルータを認識し、FCホスト上にあるかのようにそれに応答します。

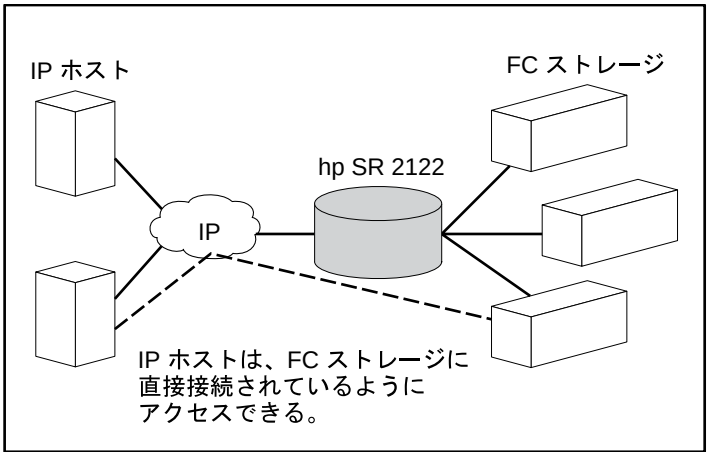

図30: SCSIルーティングの概要

ストレージ ルータをSCSIルーティング用に設定するには、以下の概念を理解している必要があります。

- iSCSIプロトコルを使用したSCSI要求と応答のルーティング（43ページ）
- SCSIルーティングの基本的なネットワーク構造（44ページ）
- SCSIルーティングのマッピングとアクセス制御（45ページ）
- 使用可能なSCSIルーティング インスタンス（49ページ）

注記: **FCストレージに加え、FCホスト接続およびFCスイッチ接続も可能です。ただし、このマニュアルではストレージ ルータの機能を説明することを目的としているため、ほとんどの場合ストレージ接続についてだけ説明しています。**

---

iSCSIプロトコルを使用したSCSI要求と応答のルーティング

SCSIルーティングは、IPネットワークとFCストレージ間でのSCSI要求と応答のルーティングで構成されます（図31を参照）。

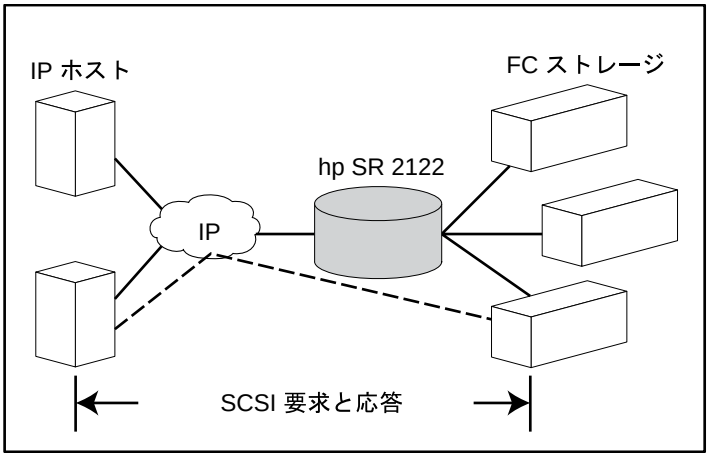

図31: SCSIルーティングのSCSI要求と応答のルーティング

ストレージ ルータを経由してストレージにIPアクセスする必要がある各ホストには、互換性のあるiSCSIドライバがインストールされている必要があります。iSCSIプロトコルを使用するiSCSIドライバにより、IPホストは、IPネットワーク経由でSCSI要求と応答を転送できます。ホストのオペレーティング システムにとって、iSCSIドライバはホスト内の周辺チャネル用のSCSIまたはファイバ チャネル ドライバとして映ります。

SCSIルーティングの主な動作は以下のとおりです（図32を参照）。

- ホストとストレージ ルータ間でIPネットワークを介してSCSI要求と応答を転送する
- IPネットワーク上のホストとFCストレージ間でSCSI要求と応答をルーティングする
- ストレージ ルータとFCストレージ間でSCSI要求と応答を転送する

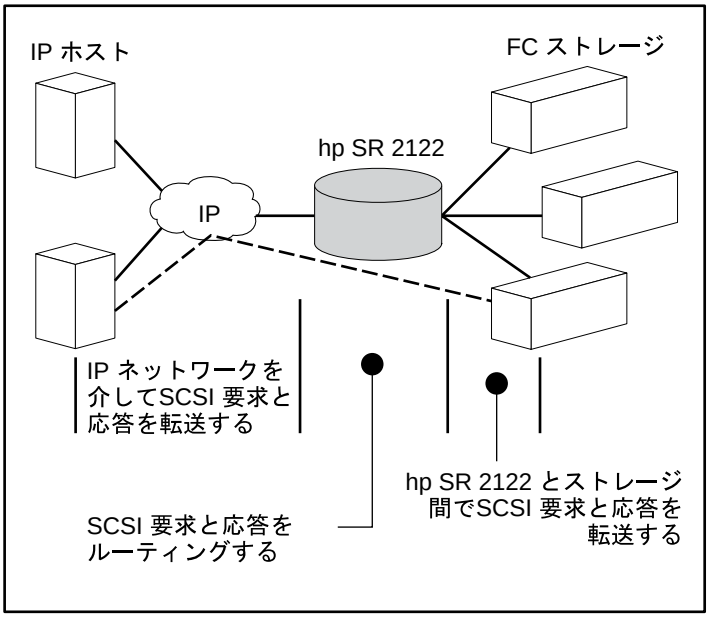

図32: SCSIルーティングの動作

SCSIルーティングの基本的なネットワーク構造

図33に、SCSIルーティング ネットワークの基本的な構造を示します。iSCSIドライバがインストールされているIPホストは、各ストレージ ルータのギガビット イーサネット インタフェースに接続されているIPネットワークを介してストレージ ルータにアクセスします。ストレージ ルータは、各ストレージ ルータのファイバ チャネル インタフェースに接続されているストレージ デバイスにアクセスします。管理ステーションは、各ストレージ ルータの管理インタフェースに接続されているIPネットワークを介してストレージ ルータを管理します。高可用性（HA）環境を実現できるように、ストレージ ルータは2つのネットワーク経由で通信します。一つは各ストレージ ルータのHAインタフェースに接続されているHAネットワークで、もう一つは各ストレージ ルータの管理インタフェースに接続されている管理ネットワークです。

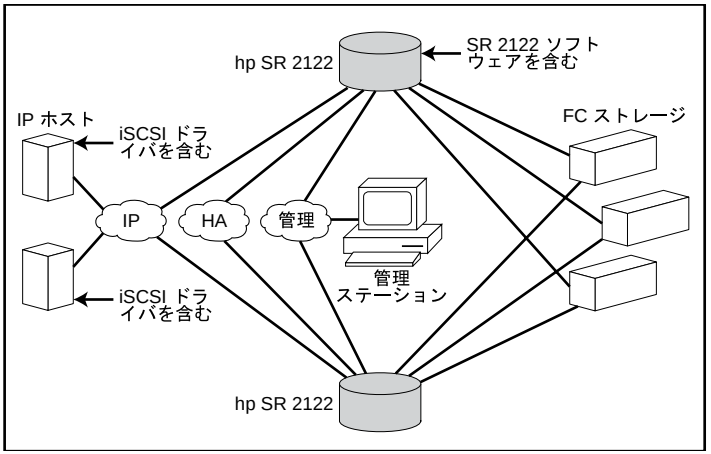

図33: SCSIルーティングの基本的なネットワーク構造

SCSIルーティングのマッピングとアクセス制御

SCSIルーティングは、物理ストレージ デバイスのiSCSIターゲットへのマッピングを介してストレージ ルータで行われます。物理ストレージ デバイスのグループであるiSCSIターゲット（論理ターゲットとも言います）は、複数の物理デバイスにマップできます。iSCSIターゲットには、少なくとも1つのLUN（Logical Unit Number）が含まれています。iSCSIターゲットの各LUNは、物理ストレージ ターゲットの1つのLUNにマップされています。

ターゲットとLUNのマッピング、またはターゲットのみのマッピングのいずれかのストレージ マッピングを選択できます。ターゲットとLUNのマッピングでは、iSCSIターゲットとLUNの組み合せが、物理ストレージ ターゲットとLUNの組み合せにマップされます。ターゲットのみのマッピングでは、iSCSIターゲットが物理ストレージ ターゲットとそのLUNにマップされます。

ターゲットとLUNのマッピングでは、指定したiSCSIターゲット名とiSCSI LUN番号が1つのLUNの物理ストレージ アドレスにマップされます。物理ストレージ アドレスは、WWPN + LUN（World Wide Port Name + LUN）の組み合せ、LUNWWN（LUN World Wide Name）、またはLUNシリアル番号で表します。LUNが使用可能な場合、iSCSI LUNとして使用できるようになり、指定したiSCSI LUN番号が付けられます。たとえば、*Database*、*LUN 9*として指定したiSCSIターゲットとiSCSI LUNを物理アドレス*WWPN ID*、*LUN 12*にマップした場合、*LUN 12*は1つのiSCSI LUNとして使用できます。iSCSIドライバは、*Database*という名前のiSCSIターゲットと、*LUN 9*として識別されている1つのiSCSI LUNを認識します。ホスト上に、1つのストレージ デバイスとしてiSCSI LUNが表示されます（表5を参照）。

表5: ターゲットとLUNマッピングの例

ホストが認識可能なディスク	iSCSI ターゲット	使用可能な iSCSI LUN	物理ストレージ アドレス	使用可能な物理 LUN
ローカル ディスク (D:)	Database	LUN 9	WWPN 070	LUN 12
ローカルに接続されている1つのストレージ デバイスとして認識される	Databaseは、1つのLUNが使用可能な1つのコントローラとして認識される	iSCSI LUNに指定した番号が付けられる。この番号は、物理LUN番号と異なっていてもかまわない	ストレージ コントローラのストレージ アドレスを指定する	マッピング可能な唯一のLUNとしてのLUN番号を指定

ターゲットのみのマッピングでは、iSCSIターゲット名を指定し、ストレージ コントローラの物理ストレージ アドレスであるWWPNにだけマップします。ストレージ コントローラで使用可能なLUNは、iSCSI LUNとして使用可能になり、ストレージ コントローラ内のLUNと同じ番号が付けられます。たとえば、*Webserver2000*として指定されているiSCSIターゲットが物理ストレージ アドレス*WWPN 050*にマップされていて、そのコントローラで*LUNs 0*～2が使用可能な場合、これらのLUNは3つのiSCSI LUNとして使用可能になります。iSCSIドライバは、*Webserver2000*という名前のiSCSIターゲットを、*LUN 0*、*LUN 1*、*LUN 2*という3つのiSCSI LUNのあるコントローラとして認識します。ホストにとって、各iSCSI LUNは、個別のストレージ デバイスとして認識されます（表6を参照）。

表6: ターゲットのみのマッピングの例

ホストが認識可能なディスク	iSCSI ターゲット	使用可能な iSCSI LUN	物理ストレージ アドレス	使用可能な物理 LUN
ローカル ディスク (D:)	Webserver2000	LUN 0	WWPN 050	LUN 0
ローカル ディスク (E:)	Webserver2000	LUN 1	WWPN 050	LUN 1
ローカル ディスク (F:)	Webserver2000	LUN 2	WWPN 050	LUN 2
ローカルに接続されている3つのストレージ デバイスとして認識される	Webserver2000は、LUN 0、1、2があるコントローラとして認識される	iSCSI LUNには物理LUNと同じ番号が付けられる	ストレージ コントローラのストレージ アドレスを指定する	LUN 0、1、および2はマッピング可能

SCSIルーティングのアクセスは、IPホストとストレージ ルータによって制御されます。IPホストでは、ストレージ ルータ内のSCSIルーティング インスタンスのギガビット イーサネット IPアドレスは、iSCSIドライバで設定されています。ホストは、このIPアドレスを使用してSCSI要求と応答を転送します。ストレージ ルータでは、アクセスは、ホストのアクセス リストとVLAN ID（VID）番号によって制御されます。また、ストレージ ルータで認証を使用して詳細にアクセス制御することもできます。認証の詳細については、50ページの「SCSI認証の概要」を参照してください。

アクセス リストにより、ホストIPアドレス、CHAPユーザー名、またはiSCSI名の任意の組み合せで、ストレージ ルータに接続されているストレージ デバイスにアクセスできます。アクセス リストには、これらの組み合せが含まれています。ホストVIDにより、各ホストのVIDに従ってストレージ デバイスにアクセスできます。VLANアクセスの詳細については、49ページの「VLANアクセスの概要」を参照してください。

アクセス リストとVIDの組み合せを使用して、ストレージ ルータでのアクセスを設定できます。つまり、VLANのIPアドレスに従った特定のホストが、ストレージ ルータに接続されているストレージ デバイスにアクセスできるように指定できます。

ホストとストレージ ルータでアクセスを設定し、ストレージ ルータでストレージ マッピングを設定すれば、ストレージ ルータは、マップされているストレージ デバイスとホスト間でSCSI要求と応答をルーティングします。

図34は、SCSIルーティング用のストレージ　マッピングとアクセス制御の概念を表しています。この図では、ストレージ ルータは、3つのIPホストに対して、4つのディスク コントローラのディスク ドライブへのIPアクセスを提供しています。ストレージ ルータには2つのSCSIルーティング インスタンスがあります。一方には、ギガビット イーサネット インタフェース用にIPアドレス10.1.2.3が設定されていて、もう一方にはIPアドレス10.1.2.4が設定されています。各IPホスト内のiSCSIドライバは、ギガビット イーサネット インタフェース経由でIPアドレスを使用して、これらのSCSIルーティング インスタンスにアクセスするように設定されています。ストレージ ルータ内のアクセス リストまたはVID（あるいはその両方）は、マップされているストレージ デバイスにホストA、B、Cがアクセスできることを指定しています。ホストにとって、マップされている各ディスク ドライバは、ローカルに接続されているディスク ドライブとして認識されます。表7は、アクセス リストとVID、SCSIルーティング インスタンスのギガビット イーサネット IPアドレス、およびストレージ デバイス マッピングの関係を示しています。

注記: 図34と表7は、ストレージ マッピングとアクセス制御の概念を示すことだけを目的としています。IPアドレスは、各サイトによって異なります。同様に、ストレージ アドレッシングの種類（LUNWWN、WWPN + LUN、またはLUNシリアル番号）は、ストレージの種類と各サイトに適したストレージ アドレッシングの種類によって異なります。また、この図と表では、高可用性を実現するための追加のストレージ ルータも示していません。

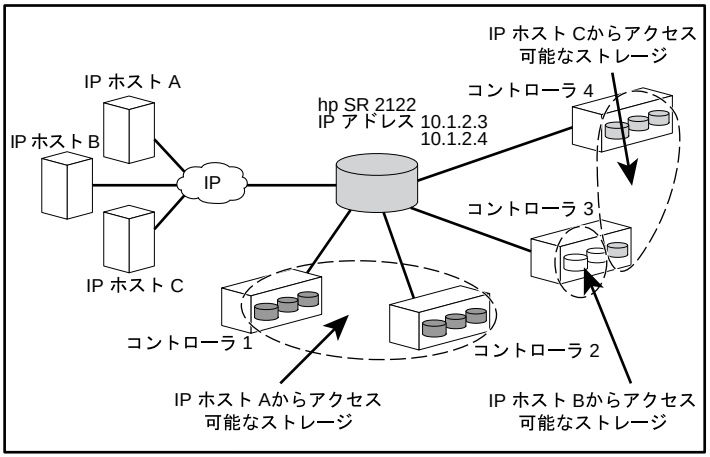

図34: SCSIルーティング ストレージ マッピングとアクセス制御の概念

表7: SCSIルーティング ストレージ マッピングとアクセス制御の概念

ストレージ ルータのアクセス リストと VID 経由でアクセスが許可されているホスト	ローカルに接続されているデバイスのようにホストに認識されるストレージ デバイス	経由する SCSI ルーティング インスタンスの GbE IP アドレス	マップされているコントローラ	マップされているドライブ
ホストA	ローカルディスク（D:）	10.1.2.3	1	1
	ローカルディスク（E:）	10.1.2.3	1	2
	ローカルディスク（F:）	10.1.2.3	1	3
	ローカルディスク（G:）	10.1.2.3	2	1
	ローカルディスク（H:）	10.1.2.3	2	2
	ローカルディスク（I:）	10.1.2.3	2	3
ホストB	ローカルディスク（D:）	10.1.2.3	3	1
	ローカルディスク（E:）	10.1.2.3	3	2
ホストC	ローカルディスク（D:）	10.1.2.4	4	1
	ローカルディスク（E:）	10.1.2.4	4	2
	ローカルディスク（F:）	10.1.2.4	4	3
	ローカルディスク（G:）	10.1.2.4	3	3

使用可能なSCSIルーティング インスタンス

ストレージ ルータでは、最大12個のSCSIルーティング サービスを設定できます。各サービスには、ギガビット イーサネット IPアドレス、iSCSIターゲット名と物理ストレージ アドレス間のマッピング、およびアクセス制御を設定する必要があります。

ストレージ ルータがクラスタの一部である場合、SCSIルーティング インスタンスは、一度に1つのストレージ ルータ（クラスタ内の）でのみ実行できます。クラスタ内のSCSIルーティングのインスタンスの詳細については、50ページの「ストレージ ルータ クラスタ管理の概要」を参照してください。ストレージ ルータの設定の詳細については、このドキュメントの設定に関する章を参照してください。

VLANアクセスの概要

ストレージ ルータ　VLANアクセスにより、IPホストは、各ホストが属しているVLANに従ってストレージ デバイスにアクセスできます。

図35に、ストレージ ルータ VLANアクセスを使用している単純なネットワークの例を示します。この図では、ストレージ ルータ ギガビット イーサネット インタフェースは、IEEE 802.1Qトランク経由でIPネットワークに接続されています。ストレージ ルータ ファイバチャネル インタフェースは、ストレージ1、2、および3に接続されています。ストレージ ルータには、*SR100*および*SR200*という名前の2つのSCSIルーティング インタフェースが設定されています。IPネットワークには、VLAN 100およびVLAN 200という2つのVLANが含まれています。SCSIルーティング インスタンスSR100は、VLAN 100内のホストがストレージ デバイス1および2にアクセスできるように設定されています。SCSIルーティング インスタンスSR200は、VLAN 200内のホストがデバイス3にアクセスできるように設定されています。

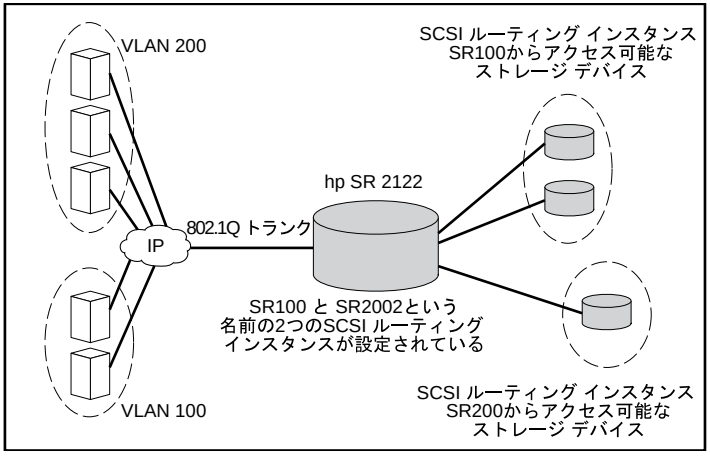

図35: VLANアクセスの概要

ストレージ ルータをスイッチ ネットワーク環境で使用する場合は、専用のVLAN Trunking Protocol（VTP）を使用してストレージ ルータを設定します。VTPを使用することで、ストレージ ルータは外部接続されたスイッチとVTPパケットを交換して、ネットワーク内でア

クセス可能なVLANに関する情報を動的に入手します。その後ストレージ ルータは、VTPを使用して、レイヤ 2マルチキャスト パケットを使用しているスイッチ ネットワークにVLAN情報を伝達します。

ストレージ ルータを非スイッチ ネットワーク環境で使用する場合は、VTPを使用せずにストレージ ルータをVLAN用に設定します。ストレージ ルータは、ネットワーク内のVLANに関する情報を入手するのにVTPパケットを交換しなくなります。その代わりに、ネットワーク内のVLANに、VLAN ID（VID）番号を手動で割り当てる必要があります。必要に応じて、各VLANに固有の名前を割り当てたり、MTUのサイズを手動で設定できます。

ストレージ ルータをクラスタに組み込む場合、ストレージ ルータ用に設定されたVLAN情報はクラスタ内のすべてのストレージ ルータに伝達されます。

ストレージ ルータは、VLANのカプセル化に関するIEEE 802.1Q規格を使用します。802.1Qのカプセル化規格により、VLAN情報は、ストレージ ルータのギガビット イーサネット インタフェース経由で送受信されるパケットで転送されます。これらのパケットには、VIDと、VLANメンバがVLANに加わるのに必要なその他のVLAN情報が含まれています。

VLANは、ストレージ ルータで設定されているSCSIルーティング インスタンスを介してストレージ デバイスにアクセスできます。SCSIルーティング インスタンスに割り当てられているiSCSIターゲットは、VLANがアクセス可能なストレージ デバイスを決定します。

iSCSI認証の概要

iSCSI認証は、各ストレージ ルータで使用可能なソフトウェア サービスです。これは、ストレージへのアクセスを要求するIPホストを認証します。iSCSI認証は、各ストレージ ルータで設定されているAAA（認証、認可、アカウンティング）サブシステムによって提供されます。AAAは、一貫性のあるモジュール的な方法で3つの独立したセキュリティ機能（認証、認可、アカウンティング）を設定するためのCiscoの体系的フレームワークです。ストレージ ルータ ソフトウェアは、認証機能を備えています。

認証は、要求したオブジェクト、機能、またはネットワーク サービスへのアクセスをユーザーに許可する前に、ユーザーを識別するための方法を提供します（ログインとパスワード ダイアログ、試行と応答、メッセージング サポートなど）。AAA認証は、認証サービスのリストを定義して設定します。AAA認証サービス リストを使用するiSCSI認証は、ストレージ ルータ内の特定のSCSIルーティング インスタンス用に有効にできます。

iSCSI認証を有効にした場合、iSCSIドライバがインストールされているIPホストは、iSCSI TCP　接続が確立されるたびにユーザー名とパスワード情報を提供する必要があります。iSCSI認証は、iSCSI CHAP（Challenge Handshake Authentication Protocol）認証方法を使用します。

ストレージ ルータ クラスタ管理の概要

障害発生時に備えて相互にバックアップできるように、クラスタ内のストレージ ルータを構成できます。

ストレージ ルータ クラスタは、2つのストレージ ルータで構成されており、以下のように接続されています。

■　同じホストに接続

- 同じストレージ システムに接続
- 管理および高可用性（HA）インタフェースを介して相互に接続

クラスタ環境の場合、ストレージ ルータは、設定データを相互に伝達したりクラスタ内の障害を検出できるようにHA情報を絶えず交換します。ストレージ ルータは、2つの独立したネットワーク経由でHA情報を交換します。一つは、各ストレージ ルータの管理インタフェースに接続されていて、もう一つは各ストレージ ルータのHAインタフェースに接続されています。ストレージ ルータ間でHA情報が信頼性の高い状態で交換されるように、ストレージ ルータは管理インタフェースとHAインタフェース間でHA情報の転送負荷のバランスをとります。

ストレージ ルータ クラスタは、アクティブなSCSIルーティング インスタンスを最大12個サポートします。SCSIルーティング インスタンスは、一度に1つのストレージ ルータ（クラスタ内の）でだけ実行できます。インスタンスは、以下のいずれかの状況になるまで、それが開始されたストレージ ルータ上で実行されます。

- インスタンスを明示的に停止またはクラスタ内の別のストレージ ルータにフェールオーバーした
- インタフェースが使用できない、または他のソフトウェア/ハードウェアの問題が発生したためにインスタンスが自動的に別のストレージ ルータにフェールオーバーした

クラスタ内の各ストレージ ルータは、SCSIルーティング インスタンスを最大12個実行できます。たとえば、1つのストレージ ルータが2つのインスタンスをすでに実行している場合、10個の追加インスタンスを実行できます。

インタフェースの名称付け

ストレージ ルータ ソフトウェアを設定する際には、ハードウェアのインタフェース名称付けを理解している必要があります。ここでは、ストレージ ルータ ハードウェアで使用するインタフェース名称付けシステムについて説明します。

各ストレージ ルータ インタフェースには、2つの英小文字と1つの数字で構成された3文字の名前が割り当てられます。英文字はインタフェースのタイプを表し、数字はインタフェースが装着されているシャーシ スロットを表します（図36を参照）。

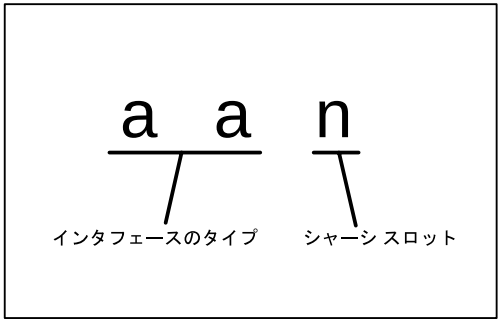

図36: ストレージ ルータ インタフェースの名称付けシステム

表8は、ストレージ ルータの有効なインタフェース タイプの表記名を示しています。図37は、ストレージ ルータの各インタフェースの場所と名前を示しています。

表8: インタフェース タイプの表記名

インタフェース タイプ	説明
FC	ファイバ チャネル
GE	ギガビット イーサネット

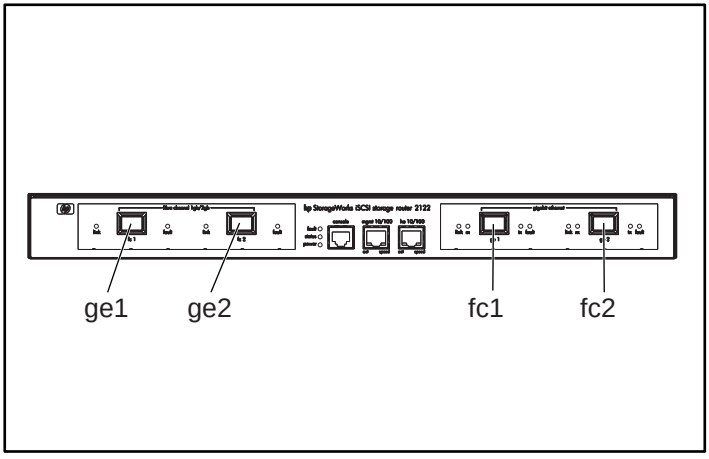

図37: ストレージ ルータ シャーシスロットの番号

次の作業

ストレージ ルータを設定する準備が整ったら、目的に応じてこのガイドの以下のいずれかの章に進んでください。

- 第5章「ストレージ ルータの設定」— 初めてセットアップする場合、または工場出荷時のデフォルト設定に戻した場合に必要となる手順について説明します。
- 第6章「システム パラメータの設定」— CLIを使用したシステム パラメータの設定および変更方法について説明します。
- 第7章「VLANの設定」— CLIを使用したVLAN設定の設定および変更方法について説明します。
- 第8章「SCSIルーティングの設定」— CLIを使用したSCSIルーティング設定の設定および変更方法について説明します。
- 第9章「認証の設定」— CLIを使用したSCSIルーティング設定の設定および変更方法について説明します。
- 第10章「高可用性クラスタの設定」— CLIを使用したクラスタ設定の設定および変更方法について説明します。
- 第11章「ストレージ ルータのメンテナンスと管理」— ソフトウェアのダウンロード、設定のバックアップと復元、関連するその他のメンテナンスおよび管理タスクについて説明します。

ストレージ ルータの設定

5

この章では、ストレージ ルータを初めて設定する際に収集する必要がある設定情報、初期システム コンフィギュレーション スクリプト、セットアップ コンフィギュレーション ウィザードについて説明します。また、その後設定タスクを実行するのに必要となるコマンド ライン インタフェース（CLI）とWebベースのGUIについても説明します。

この章では、以下の内容について説明します。

事前に必要な作業

ストレージ ルータを初めて設定する前に、第2章「設置」に従ってハードウェアの設置が完了していることを確認してください。

設定情報の収集

ストレージ ルータを初めて設定する際のチェックリスト（表10を参照）を使用して、ストレージ　ルータを初めて設定する際に必要となるシステムおよびネットワーク情報を収集してください。チェックリストの項目は、初期システム コンフィギュレーション スクリプトとセットアップ コンフィギュレーション ウィザードで必要となる情報に基づいています。初めて設定する際に必要となる設定項目については、表9を参照してください。

表9: 設定情報の収集

設定項目	説明	必須またはオプション
設定配備機能	SCSI**ルーティング**（ストレージ ルータにより、iSCSIホストはファイバ チャネル ストレージにアクセスできるようなる。ストレージ ルータは、ファイバ チャネル ストレージへのアクセスを管理する。）	必須
管理インタフェースのIPアドレスとサブネット マスク	ストレージ ルータの管理インタフェースのIPアドレスとサブネット マスク。 注記:　クラスタ内の各ストレージ ルータの管理インタフェースは、同じIPサブネット上になければなりません。	必須
管理インタフェース用の静的ルート	送信先IPアドレスとサブネット マスク、その後ゲートウェイIPアドレス。	物理的に接続されているサブネット以外のサブネットからストレージ ルータを管理する場合に必須
システム名	ストレージ ルータの名前。DNSのサービスを使用する場合は、管理インタフェースに入力および関連付けたのと同じシステム名を使用する。19文字以内で指定。	必須
GEインタフェース	IPネットワークとの通信で使用するギガビット イーサネット インタフェースで、ge1またはge2。デフォルトはge1。	SCSIルーティングでのみ必須
高可用性（HA）構成	ストレージ ルータは、スタンドアロンまたはクラスタ モードのいずれかで実行可能。デフォルトは**クラスタ モード**です。ストレージ ルータが他のストレージ ルータとともに高可用性機能を提供しない場合は、スタンドアロン モードに設定することを推奨。	SCSIルーティングでのみ必須
高可用性（HA）クラスタ名	ストレージ ルータを組み込むクラスタの名前。クラスタとは、ハードウェアまたはソフトウェアの障害が発生した場合に備えて相互にバックアップする複数のストレージ ルータ構成。1つのクラスタに組み込むすべてのストレージ ルータには、同じクラスタ名を付ける必要がある。	HA構成をクラスタ モードに指定した場合のみ必須

設定項目	説明	必須またはオプション
高可用性（HA）のIPアドレスとサブネット マスク	ストレージ ルータのHAインタフェースのIPアドレスとサブネット マスク。HAインタフェースと管理インタフェースは、固有のIPネットワーク上になければならない。ストレージ ルータをクラスタに組み込む場合には、HA IPアドレスは必須。スタンドアロン モードで使用する場合は、オプション。 注記: クラスタ内の各ストレージ ルータのHAインタフェースは、同じIPサブネット上になければなりません。	HA構成をクラスタ モードに指定した場合のみ必須
プライマリDNS IPアドレス	ストレージ ルータがアクセスするプライマリ ドメイン サーバのIPアドレス。他のサーバをIPアドレスではなく名前で参照する場合には必須。	オプション
セカンダリDNS IPアドレス	プライマリDNSが使用できない場合に、ストレージ ルータがサービスを要求することができるバックアップのDNS。	オプション
NTPサーバIPアドレス	ストレージ ルータが使用することができるNTPサーバのIPアドレス。これにより、ストレージ ルータはネットワーク上で日時を同期させることが可能。	オプション
タイム ゾーン、現在の日時	日付形式はmm/dd/yyyyで、時刻形式はhh:mm:ss。	オプション
すべてのインタフェースでTelnetを有効にする	すべてのインタフェースでTelnetアクセスを有効にする。デフォルトでは、Telnetアクセスは管理インタフェースでのみ有効。	オプション
SNMP読み取り専用コミュニティ名	ストレージ ルータ ネットワークに読み取り専用アクセス権を持っているコミュニティの名前。ストレージ ルータは、このコミュニティのGETコマンドに応答する。デフォルトはpublicです。	オプション
SNMP書き込みコミュニティ名	ストレージ ルータ ネットワークに書き込みアクセス権を持っているコミュニティの名前。ストレージ ルータは、このコミュニティのSETコマンドに応答する。デフォルトはprivateです。	オプション
最初のSNMPトラップ マネージャのIPアドレス	SNMP通知（トラップ）に使用する最初の送信先ホストのIPアドレス。SNMPトラップを使用する場合は必須。	オプション
最初のSNMP IPアドレスのトラップ バージョン	最初のSNMPトラップ マネージャのIPアドレスに送信するトラップのバージョン番号。デフォルトは1です。	オプション
2番目のSNMPトラップ マネージャのIPアドレス	SNMP通知（トラップ）に使用する2番目の送信先ホストのオプションのIPアドレス。	オプション
2番目のSNMP IPアドレスのトラップ バージョン	2番目のSNMPトラップ マネージャのIPアドレスに送信するトラップのバージョン番号。デフォルトは1です。	オプション
認証失敗トラップ送信オプション	ユーザーが正しくないコミュニティを指定した場合に認証失敗トラップを送信する。	オプション
リンク接続/切断トラップ送信オプション	管理インタフェース、HAインタフェース、ギガビット インタフェース、ファイバ チャネル インタフェースのリンクが接続/切断されたときにリンク接続/切断トラップを送信する。	オプション
Monitorレベルのパスワード	ストレージ ルータの動作をモニタするのみのユーザー用のパスワード。デフォルトのパスワードはhpです。	オプション

設定項目	説明	必須またはオプション
Administratorレベルのパスワード	ストレージ ルータを設定および管理するユーザー用のパスワード。デフォルトのパスワードはhpです。	オプション
EIA/TIA-232コンソール インタフェースへのパスワードの適用 (yes/no)	EIA/TIA-232コンソール インタフェース経由でストレージ ルータにアクセスする際に、ユーザーがMonitorパスワードおよびAdministratorパスワードを入力する必要があるかどうかを選択。デフォルトはnoです。	オプション
システム管理者の連絡先	ストレージ ルータのシステム管理者の名前、電子メール アドレス、電話番号、およびページャ番号。目的に応じて使用可。	オプション
SCSIルーティング インスタンスの名前	SCSIルーティング インスタンスの固有な名前。インスタンス名は32文字以内で指定可能。最大12個の固有なSCSIルーティング インスタンスを指定可能。**セットアップ コンフィギュレーション** ウィザードでは、1つのインスタンスのみの名称を付けることができる。 注記: ストレージ ルータをクラスタのメンバとして組み込む場合は、クラスタ内のすべてのストレージ ルータ全体に渡って12個を超えるSCSIルーティング インスタンスを定義しないでください。HA、クラスタ構成、およびフェールオーバーの詳細については、第10章「高可用性クラスタの設定」および第11章「ストレージ ルータのメンテナンスと管理」を参照してください。 注記: ストレージ ルータでVLANサービスを使用している場合は、セットアップ コンフィギュレーション ウィザードで SCSI ルーティング インスタンスの名称を付けないでください。SCSIルーティング インスタンスに名称を付けたり設定する前に、第7章「VLANの設定」を参照してください。	必須

初めて設定する際のチェックリストの記入が完了すれば、初期システム コンフィギュレーション スクリプトとセットアップ コンフィギュレーション ウィザードを使用してストレージ ルータを設定できます。

表10: ストレージ ルータを初めて設定する際のチェックリスト

設定項目	値
設定配備機能オプション（1または2）	
管理インタフェースのIPアドレスとサブネット マスク	
管理インタフェース用の静的ルート	
システム名	
GEインタフェース	
高可用性（HA）構成（スタンドアロン モードまたはクラスタ モード）	
HAクラスタ名	
HAインタフェースのIPアドレスとサブネット マスク	
プライマリDNS IPアドレス	
セカンダリDNS IPアドレス	
NTPサーバIPアドレス	
すべてのインタフェースでTelnetを有効にする（yes/no）	
SNMP読み取り専用コミュニティ名（デフォルト：public）	
SNMP書き込みコミュニティ名（デフォルト：private）	
最初のSNMPトラップ マネージャのIPアドレス	
最初のSNMP IPアドレスのトラップ バージョン	
2番目のSNMPトラップ マネージャのIPアドレス	
最初のSNMP IPアドレスのトラップ バージョン	
正しくないコミュニティを指定した場合の認証失敗トラップの送信（yes/no）	
1つまたは複数のインタフェースのリンク接続/切断トラップの変更（yes/no）	
管理インタフェースのリンク接続/切断トラップの送信（yes/no）	
HAインタフェースのリンク接続/切断トラップの送信（yes/no）	
ギガビット イーサネット インタフェースのリンク接続/切断トラップの送信（yes/no）	
ファイバ チャネル インタフェースのリンク接続/切断トラップの送信（yes/no）	
Monitorレベルのパスワード	
Administratorレベルのパスワード	
EIA/TIA-232コンソール インタフェースへのパスワードの適用（yes/no）	
システム管理者の名前	
システム管理者の電子メール アドレス	
システム管理者の電話番号	
システム管理者のページャ番号	

設定項目	値
SCSIルーティング インスタンスの名前（VLANサービスを使用している場合はセットアップ コンフィギュレーション ウィザードでSCSIルーティング インスタンスは設定しないでください）	
設定配備機能オプション（1または2）	
管理インタフェースのIPアドレスとサブネット マスク	

コンソールの接続

ストレージ ルータの設定を開始するには、『Storage Router Hardware Installation Guide』の指示に従って、端末エミュレーション プログラムがインストールされているPCをEIA/TIA-232コンソール インタフェースに接続します。そして、端末エミュレーション プログラムが表11の値に設定されていて、CLIセッションを実行できるようになっていることを確認します。

表11: 端末エミュレーションの設定

設定	値
端末モード	VT-100
ボーレート	9600
パリティ	パリティなし
ストップ ビット	1ストップ ビット

初期システム コンフィギュレーション スクリプト

初期システム コンフィギュレーション スクリプトはCLIで実行します。このスクリプトにより、ストレージ ルータを稼動させるのに必要ないくつかの必須の値が入力されます。初めてストレージ ルータの電源を入れて、初期起動処理が完了すると、スクリプトは、EIA/TIA-232コンソール接続経由で端末エミュレーション プログラム上で実行されているCLIセッションで自動的に実行されます。

初めての実行後、スクリプトは、ストレージ ルータに管理インタフェースのIPアドレスが設定されていない場合に自動的に実行されます。通常、システムの再設定が必要となる`clear conf`コマンドを実行した場合にこの状態になります。

初期システム コンフィギュレーション スクリプトでは、設定値の入力が要求される前に説明が表示されます。スクリプトには、2種類あります。スクリプトによって要求される値は、最初の問い合わせで入力する設定配備オプションの値によって決定されます。

表12に、設定項目を示します。これらはここに示している順にスクリプトで表示されます。

表12: 初期システム コンフィギュレーション スクリプトの設定項目

設定項目	設定配備
管理インタフェースのIPアドレスとサブネット マスク（CIDR形式）（例：10.1.10.244/24**）**	
送信先IPアドレスとサブネット マスク、その後ゲートウェイIPアドレス（例：1.0.1.0/24 10.0.1.2**）（オプション）**	
ストレージ ルータのシステム名（19文字以内）	
HA構成（スタンドアロン モードまたはクラスタ モード）	
クラスタ名（HA構成をクラスタ モードに設定した場合のみ要求される）	
HAインタフェースのIPアドレスとサブネット マスク（CIDR形式）（例：10.1.20.56/24**、HA構成をクラスタ モードに設定した場合のみ要求される）**	
IPネットワークとの通信で使用するギガビット イーサネット インタフェース、ge1**または**ge2**を選択**	
ギガビット イーサネット インタフェースのIPアドレスとサブネット マスク（CIDR形式）（例：10.1.0.45/24**）**	

スクリプトが完了すると、システムが自動的に再起動します。コマンド プロンプトが表示されたら、セットアップ コンフィギュレーション ウィザードを使用して設定を続けます。

セットアップ コンフィギュレーション ウィザードの実行

セットアップ コンフィギュレーション ウィザードは、CLIから実行可能なスクリプトで、ストレージ ルータの基本的なシステム設定値の入力を求める一連の問い合わせで構成されています。次の設定値を入力するように求められます。

- 管理インタフェース（プライマリ/セカンダリDNSサーバが含まれる）
- タイム ゾーン、NTPサーバ、現在の日時
- ネットワーク管理アクセス（SNMPを含む）
- Monitor用およびAdministrator用パスワード
- コンソール インタフェースのパスワード
- システム管理者の連絡先
- SCSIルーティング（ウィザードのこの部分は、初期システム コンフィギュレーション スクリプトで SCSI ルーティングを設定配備として選択した場合のみ表示されます。VLANサービスを使用している場合は、セットアップ コンフィギュレーション ウィザードでSCSIルーティングを設定しないでください）

セットアップ コンフィギュレーション ウィザードは、EIA/TIA-232 コンソール インタフェース接続経由で実行できます。ストレージ ルータでIPアドレスが設定されている場合は、管理インタフェースを使用して Telnet セッション経由でも実行できます。管理インタフェースを使用して設定を行う場合は、CLI セッションを確立するのにデフォルトのパスワードであるhpを使用してください。

セットアップ コンフィギュレーション ウィザードに入力した値は、ウィザードのスクリプトの最後に保存されます。**Ctrl-C** キーを押すことで、変更内容を保存せずにコンフィギュレーション ウィザードをいつでも終了できます。その後、ストレージ ルータを再起動すれば元の値に戻ります。

注記: **iSCSIトラフィック用のリスニング ポートの工場出荷時のデフォルト設定は3260です。このポート番号は、IANAによって割り当てられています。この値は、必要に応じてネットワーク構成に適した値に変更できます。**

以下のコマンドを入力して、セットアップ コンフィギュレーション ウィザードを開始します。

1. `enable` — Administratorモードに入ります。Administrator用のパスワードの入力が求められたら、デフォルトのパスワード**hp**を入力します。
2. `setup` — セットアップ コンフィギュレーション ウィザードを開始します。ウィザードは、**novice**（初心者）または**expert**（熟練者）のいずれかのモードで実行できます。novice レベルでは、プロンプトが表示される前に要求されている情報の説明が表示されます。expertレベルでは、説明は表示されません。ウィザードは、いずれかのレベルを選択するように求めてきます。59ページの「ストレージ ルータを初めて設定する際のチェックリスト」を参照して、プロンプトに応答してください。複数の選択肢がある質問では、選択肢が角かっこ内に表示されます。特殊な形式で入力する必要がある場合には、その形式が角かっこ内に表示されます。値がすでに入力済み（たとえば、初期システム コンフィギュレーション スクリプトで入力済み）の場合には、システムに保存されている現在の値が角かっこ内に表示されます。デフォルト値は、角かっこ内に丸かっこで囲まれて表示されるので現在の値またはデフォルト値を使用する場合は、**Enter**キーを押します。デフォルト値が存在せず、その問い合わせを省略したい場合（つまり、値を変更したり指定しない場合）は、**Enter**キーを押します。

ストレージ ルータの管理サブネット外にあるインタフェースを設定したり、サーバをストレージ ルータに提示した場合は、それらのインタフェースやサーバへアクセスするための適切なゲートウェイを指定して、ストレージ ルータのルート テーブルを更新する必要があります（`ip route`コマンドを使用します）。

`setup`コマンドを使用して、これらの基本設定パラメータを変更できます。また、コマンドライン インタフェース（CLI）またはWebベースのGUIを使用して、ストレージ ルータの基本設定を変更したり、ストレージ ルータをより詳細に設定できます。WebベースのGUIにアクセスするには、ブラウザのURLフィールドにストレージ ルータの管理インタフェースのIPアドレスを入力します。

CLIの概要

CLIは、管理インタフェースへのTelnetセッション経由で使用できます。また、EIA/TIA-232コンソール インタフェース接続経由でも使用できます。CLIは、ソフトウェアのアップグレードとメンテナンスを含む、必要なすべてのストレージ ルータ管理機能を実行するためのコマンドを備えています。

すべてのCLIコマンドで、入力中のコマンドの詳細情報を問い合わせることができます。たとえば、入力途中のコマンドが固有になった時点でTabキーを押すと、そのコマンドの残りの文字が自動的に表示されます。また、疑問符（?）キーを押すと、コマンド構文のその時点で使用可能なすべてのオプションが表示されます。コマンド内の各単語は、固有になった時点で入力する必要はありません。

CLIでの大文字と小文字の区別

CLIコマンド、キーワード、および予約語では大文字と小文字の区別はありません。コマンド、キーワード、および予約語は、大文字と小文字のどちらで入力してもかまいません。ユーザー定義のテキスト文字列は、大文字と小文字の両方で定義でき（大文字と小文字の組み合わせも可）、設定に保存できます。

コマンド モード

ストレージ ルータの管理インタフェースはパスワード保護されています。Telnet（CLIの場合）またはWebベースのGUI経由でストレージ ルータにアクセスする際にはパスワードを入力する必要があります。

以下の2種の許可があります。

- **Monitor モード：**ストレージ ルータのステータスとシステム設定情報の表示のみが可能
- **Administratorモード：**ストレージ ルータ、ストレージ ルータのアクセス リストとSCSIルーティング インスタンス、ストレージ ルータクラスタの設定や管理が可能

MonitorおよびAdministratorモードのパスワードは、セットアップ コンフィギュレーション ウィザードで設定できます（61ページの「セットアップ コンフィギュレーション ウィザードの実行」を参照）。これらのモードの工場出荷時のデフォルトのパスワードはどちらもhpです。

コマンド プロンプト

CLIコマンド プロンプトには、ストレージ ルータ システム名が含まれています。変更されているが保存されていないシステム設定の先頭には、アスタリスク（*）が表示されます。

予約語

予約語は、CLIコマンドで値または名前として使用することはできません。コマンドまたはコマンドのキーワードとして使用する単語は予約語です。CLI でのその他の予約語は以下のとおりです。

- `acl`
- `canonical`
- `iprouter`
- `iptan`
- `loglevel`

show CLIコマンド

`show cli`コマンドは、CLIコマンド構文ツリー全体とコマンド パラメータや引数に関する情報を表示するのに使用します。使用しているストレージ ルータの現在のコマンド モードで有効なコマンドのみが表示されます。

`show cli`に目的のコマンドを指定することで、特定のコマンドのみを表示できます。たとえば、`show cli aaa debug scsirouter` と入力した場合、すべての aaa、debug、scsirouterコマンドの構文ツリーが表示されます。

特殊キー

CLIでは、キーボードの特殊キーを使用できます。表13に、特殊キーとその機能を示します。

表13: 特殊キー

キー	機能
?	指定可能なオプションを表示
Backspace	カーソルの前にある1文字を削除
Tab	コマンド語句の補足入力
Ctrl-A	カーソルを行頭に移動
Ctrl-Bまたは左矢印	カーソルを1文字後ろに移動
Ctrl-D	カーソル位置の文字を削除
Ctrl-E	カーソルを行末に移動
Ctrl-Fまたは右矢印	カーソルを1文字前に移動
Ctrl-K	カーソル位置から行末までを削除
Ctrl-Nまたは下矢印	履歴バッファ内の次の行に移動
Ctrl-Pまたは上矢印	履歴バッファ内の前の行に移動
Ctrl-T	カーソル位置の文字とその前の文字を置換
Ctrl-U	行を削除
Ctrl-W	前にある単語を削除

CLI管理セッションの開始

ストレージ ルータへのTelnet接続経由でCLI管理セッションを開始するには、以下の手順に従います。

1. ストレージ ルータへのTelnetセッションを確立します。
2. ログイン プロンプトに対して適切なパスワードを入力します。
3. `enable`と入力して、Administratorモードに変更します（オプション）。

注記: ストレージ ルータの設定を変更する必要がある場合は、Administratorモードを有効にする必要があります。

4. プロンプトに対して、Administrator用のパスワードを入力します（オプション）。
5. 適切なCLIコマンドを入力して、目的のタスクを実行します。

WebベースのGUIの概要

CLIの代わりにWebベースのGUIを使用してストレージ ルータを設定することができます。GUIを使用して設定を行うには、まず初期システム コンフィギュレーション スクリプトを実行します。これにより、ストレージ ルータの管理インタフェースにIPアドレスが設定されます。

GUIにアクセスするには、ブラウザのURLフィールドに、HTTPプロトコルとストレージ ルータの管理インタフェースのIPアドレスを入力します（たとえば、「`http://10.1.10.244`」と入力します）。

ログイン

ストレージ ルータのURLを入力すると、ログイン ページが表示されます。MonitorまたはAdministratorとしてログインできます。ユーザー名とパスワードの入力が求められます。2つのログイン オプションを使用するためのユーザー名と工場出荷時のデフォルトのパスワードについては、表14を参照してください。Monitor モードまたはAdministratorモードの新しいパスワードを設定した場合は、ログイン時にそれらを使用してください。

表14: WebベースのGUIへのログイン

ログイン オプション	ユーザー名	工場出荷時のデフォルトのパスワード
Monitor	monitor	hp
Administrator	admin	hp

Monitor モード

WebベースのGUIのMonitor モードでは、ストレージ ルータのモニタリングのみを行うことができます。Monitor モードでは、ストレージ ルータの設定、メンテナンス、またはトラブルシューティングは行えません。GUIで [Configuration]、[Maintenance]、[Troubleshooting] メニュー項目をクリックすると、Administrator モードのユーザー名とパスワードを求めるログイン ダイアログ ボックスが表示されます。

Administratorモード

Administratorモードでは、ストレージ ルータの設定、メンテナンス、またはトラブルシューティングを行えます。[Monitor] メニュー項目をクリックすると、Monitor モードのユーザー名とパスワードを求めるログイン ダイアログ ボックスが表示されます。

メニュー項目とリンク

GUIのメニュー項目とリンクは、ブラウザ ページの上端に水平に表示されます。表15にメニュー項目とリンク、それらをクリックしたときに実行されるアクション、選択可能なログイン モードを示します。

表15: メニュー項目とリンク

メニュー項目とリンク	アクション	ログイン モード
[Monitor]	左側のフレームに表示されているメニュー オプションがメインのフレームに表示されます	Monitor モードのみ
[Configuration]	左側のフレームに表示されているメニュー オプションがメインのフレームに表示されます	Administratorモードのみ
[Maintenance]	左側のフレームに表示されているメニュー オプションがメインのフレームに表示されます	Administratorモードのみ
[Troubleshooting]	左側のフレームに表示されているメニュー オプションがメインのフレームに表示されます	Administratorモードのみ
[Support]	HP.comの「サービス & サポート」ページを新しいブラウザ ウィンドウで表示する	Monitor / Administrator モード
[Home]	Monitor モードまたはAdministratorモードのどちらでログインするかを指定したログイン ページに戻る	Monitor / Administrator モード
[Help]	GUIのオンライン ヘルプを新しいブラウザ ウィンドウで表示する	Monitor / Administrator モード

iSCSIドライバのインストール

ここでは、LinuxおよびCiscoイニシエータ用のiSCSIドライバのインストール手順について説明しますので、いずれかの適切なインストール手順に従ってください。

Linux用のiSCSIドライバのインストール

ここでは、Linux用のiSCSIドライバをインストールするための手順と以下の内容について説明します。

事前に必要な作業（66ページ）
ドライバのインストール（67ページ）
ドライバのアンインストール（68ページ）

事前に必要な作業

iSCSIドライバを正常にコンパイルするためには、カーネル ソースをインストールする必要があります。

以前のバージョンのiSCSIドライバからアップグレードする場合は、新しいドライバをインストールする前に */etc/initiatorname.iscsi*を削除することをお勧めします。

ドライバのインストール

1. tar（1）を使用して、ソース アーカイブを目的のディレクトリに展開します。アーカイブには、アーカイブ名と同じサブディレクトリが含まれています。

   ```
   cd /usr/src
   tar xvzf /path/to/linux-iscsi-<version>.tgz
   cd linux-iscsi-<version>
   ```

2. iSCSI ドライバをコンパイルします。カーネル ソースが通常の場所にない場合は、「TOPDIR=/path/to/kernel」を追加するか、MakefileのTOPDIRの定義を変更します。

   ```
   make
   ```

3. rootアカウントでログインし、ドライバをインストールします。iSCSI ドライバをすでに使用している場合は、すべてのiSCSIデバイスをアンマウントして、古いiSCSIドライバをアンロードします。Linuxディストリビューションに iSCSI ドライバが含まれている場合は、まずそのパッケージをアンインストールする必要があります。

   ```
   make install
   ```

4. iSCSIターゲットのIPアドレスが含まれるように*/etc/iscsi.conf* を更新します。サンプルの設定ファイルには、以下のようなエントリが含まれています。

   ```
   DiscoveryAddress=192.168.10.94
   ```

   *iscsi.conf*の man ページには、設定ファイルの形式に関する詳細な説明が記述されています。man ページを表示するには、以下のように入力します。

   ```
   man iscsi.conf
   ```

5. iSCSIサービスを手動で起動して、設定をテストします。Red Hatシステムの場合は、以下のコマンドを実行します。

   ```
   /etc/rc.d/init.d/iscsi start
   ```

   iSCSIカーネル モジュールのロードで問題が発生した場合は、*/var/log/iscsi.log*に診断情報が書き込まれます。

   iSCSIの初期化処理では、検出した各デバイスの情報がコンソールまたは dmesg（8）に出力されます。

   ```
   Vendor: SEAGATE Model: ST39103FC Rev: 0002
   Type: Direct-Access                ANSI SCSI revision: 02
   Detected scsi disk sda at scsi0, channel 0, id 0, lun 0
   SCSI device sda: hdwr sector= 512 bytes.
                    Sectors= 17783240 [8683 MB] [8.7 GB]
   sda: sda1
   scsi singledevice 0 0 0 1
   ```

   fdisk、mkfs、fsckなどの一般的なディスク操作コマンドは、iSCSIデバイス上でローカル ドライブの場合と同様に機能します。

   */proc/scsi/iscsi*に、iSCSIデバイスに関する情報が含まれているファイル（コントローラ番号）が配置されます。

   iSCSIドライブを手動で停止するには、以下のコマンドを入力します。

```
/etc/rc.d/init.d/iscsi stop
```

6. iSCSIに対応するようにinitスクリプトを変更します。Red Hat以外のLinuxディストリビューションを使用している場合は、iSCSIセットアップ スクリプトが正しく実行されるように起動スクリプトを編集しなければならないことがあります。また、ネットワークが初期化されたあとで iSCSI サービスが開始されるように起動スクリプトの順序を変更しなければならないこともあります。
7. */etc/fstab.iscsi*内のiSCSIパーティションを表示します。*/etc/fstab*と同じ形式になっています。initスクリプトは、これらのパーティションを自動的にマウントおよびアンマウントします。この手順の詳細については、iSCSIドライバのソース アーカイブに付属の readme ファイルを参照してください。

ドライバのアンインストール

1. インストール手順1で指定したドライバのソース ディレクトリに移動します。
2. rootアカウントでログインし、以下のコマンドを実行します。

   ```
   make remove
   ```

   これにより、適切なファイルが */lib/modules*および*/usr/local/sbin*から削除されます。*/etc*にある設定ファイルは、あとで別のドライバ バージョンをインストールするときに必要となるため削除されません。
3. 1つのディレクトリをバックアップし、ソース コードを削除します。

   ```
   cd ..
   rm -fr linux-iscsi-<ver>
   ```

Microsoft Windows 2000環境でのCiscoイニシエータ ソフトウェアのインストール手順

1. イニシエータ ソフトウェアのインストール ディレクトリに移動して、*Setup.exe*を実行します。

   ```
   C:\SR2122\Initiator\Setup.exe
   ```
2. 画面の指示に従って、使用許諾契約に同意します。
3. 適切な画面でターゲットIPアドレスを入力します
4. ファイル サーバを再起動するように指示されたら、再起動します。
5. システムが再起動したらテスト ドメインにログインし、コントロール パネルの*iSCSI Config*に移動します。[コントロール パネル] でアイコンをダブルクリックします。
6. ネットワークの接続を確認するには、[Rescan] または [Re-Login] ボタンを押します。手順3で追加したIPアドレスが表示されます。
7. [iSCSI Config] 画面を終了します。
8. インターネット ブラウザを起動して、SR2122 GUIをAdministratorとして開きます。
9. 「Configuring SCSI Targets and Access List Entries」に進み、ストレージの設定を行います。

次の作業

ストレージ ルータのセットアップ コンフィギュレーション ウィザードを完全に実行しなかった場合、またはシステム構成を追加、変更、または訂正する場合は、第6章「システムパラメータの設定」に進んでください。

ストレージ ルータでVLANサービスを使用していて、SCSIルーティング以外のすべてのパラメータをセットアップ コンフィギュレーション ウィザードで入力した場合(詳細については、61ページの「セットアップ コンフィギュレーション ウィザードの実行」を参照)、第7章「VLANの設定」に従ってVLANの設定を行ってください。

VLANまたはゾーニングの設定を行う必要がない場合は、第8章「SCSIルーティングの設定」に進んでSCSIルーティングの詳細設定を行ってください。

注記: ストレージ ルータを既存のストレージ ルータ クラスタに追加する場合は、SCSIルーティングを設定する前に、第10章「高可用性クラスタの設定」の情報と手順を参照してください。

システム パラメータの設定

6

この章では、ストレージ ルータのシステム パラメータの設定方法と以下の内容について説明します。

システム パラメータは、CLIコマンドかWebベースのGUIを使用して設定または変更できます。この章では、CLIコマンドによる設定方法を説明します。WebベースのGUIを使用する場合は、Webブラウザでストレージ ルータの管理インタフェースのIPアドレスを指定し、ログオン後、［Help］をクリックしてGUIのオンライン ヘルプを参照してください。

事前に必要な作業

システム パラメータを設定する前に、以下のタスクを実行したことを確認してください。

- 『Storage Router Hardware Installation Guide』の指示に従ってハードウェアを設置した
- 初期システム コンフィギュレーション スクリプトで求められた値を入力した(詳細については、第5章の「初期システム コンフィギュレーション スクリプト」60ページを参照)

注記: ストレージ ルータ セットアップ コンフィギュレーション ウィザードを完全に実行した場合(キーワードなしのsetup CLIコマンドを使用して)、または setup scsiを除くすべてのsetup CLI コマンドを使用してウィザードを個別に実行した場合は、この章で説明している設定作業を実行する必要はありません。

設定作業

ストレージ ルータのシステム パラメータを設定するには、以下の手順を実行します。

1. 管理インタフェースを設定します。
2. 日時を設定します。
3. ネットワーク管理アクセスを設定します(オプション)。
4. パスワードを設定します。
5. 管理者の連絡先を設定します。
6. HAインタフェースを設定します(オプション)。
7. 設定を確認して保存します。

注記: 設定作業を実行しているときには、save system bootconfig または save all bootconfigコマンドを使用して、いつでも設定を確認および保存できます。

図38に、この章で使用している設定例を示します。

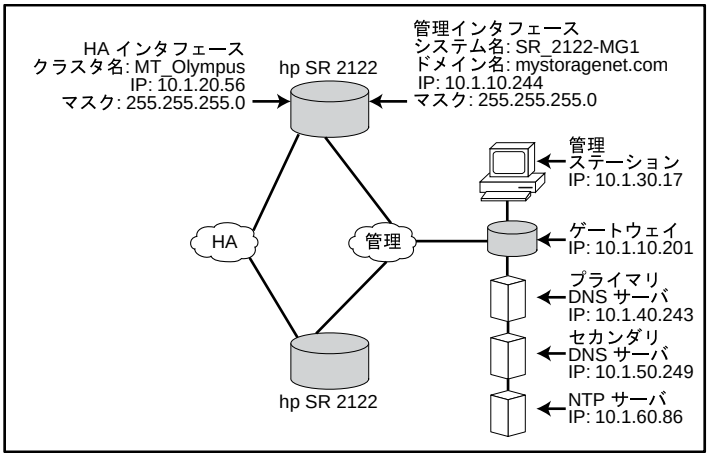

図38: システム パラメータの設定例

管理インタフェースの設定

管理インタフェースの設定作業は、システム名、IPアドレスとマスク、ゲートウェイ、DNSサーバの設定で構成されています。管理インタフェースを設定するには、以下の手順に従います。

注記: 図38のシステム構成は一つの例として示しています。また、以下の手順のIPアドレスや名前も同様です。

---

1. `enable` — Administratorモードに入ります。
2. `hostname` *`SR_2122-MG1`* — システム名を指定または変更します。システム名は、管理インタフェース全体を通してストレージ ルータを識別し、入力直後に表示されます。
3. `interface mgmt ip-address` *`10.1.10.244/24`* — 管理インタフェースのIPアドレスとサブネット マスクを指定または変更します。

注記: このストレージ ルータをクラスタに組み込む場合は、クラスタ内のすべてのストレージ ルータの管理インタフェースは同じIPサブネット上になければなりません。

---

4. `ip route` *`10.1.30.0/24 10.1.10.201`* — ストレージ ルータの管理サブネット外にある管理ステーションからストレージ ルータを管理する場合は、ゲートウェイIPアドレスを設定します。2番目のIPアドレスには、管理ステーションへのアクセスを提供するストレージ ルータ管理ネットワーク上のゲートウェイを指定します（オプション）。

注記: この設定例では、サブネット10.1.30.0上の任意のホストが管理ステーションとして機能できるようにマスクは24 255.255.255.0に設定されています。

5. `ip name-server` *`10.1.40.243 10.1.50.249`* — プライマリおよびセカンダリDNS IPアドレスを設定します。管理インタフェースのIPアドレスをDNSホスト名と相関させる場合は、プライマリDNSサーバのIPアドレスを指定します。セカンダリDNSが存在する場合は、2番目のIPアドレスにセカンダリDNSサーバのIPアドレスを指定します（オプション）。
6. `ip domain-name` *`mystoragenet.com`* — ストレージ ルータのドメイン名を指定します。このコマンドは、`ip name-server`コマンドとともに使用してください（オプション）。
7. `ip route` *`10.1.40.243/32 10.1.10.201`* — プライマリDNSサーバがストレージ ルータの管理サブネット外にある場合は、ゲートウェイIPアドレスを設定します。2番目の IP アドレスには、プライマリ DNS サーバへのアクセスを提供するストレージ ルータ管理ネットワーク上のゲートウェイを指定します（オプション）。

注記: この設定例では、ホストにIPアドレス10.1.40.243（プライマリDNSサーバ）を指定するために、マスクは32 255.255.255.255に設定されています。

8. `ip route` *`10.1.50.249/32 10.1.10.201`* — セカンダリDNSサーバがストレージ ルータの管理サブネット外にある場合は、ゲートウェイIPアドレスを設定します。2番目の IP アドレスには、セカンダリ DNS サーバへのアクセスを提供するストレージ ルータ管理ネットワーク上のゲートウェイを指定します（オプション）。

注記: この設定例では、ホストにIPアドレス10.1.50.249（セカンダリDNSサーバ）を指定するために、マスクは32 255.255.255.255に設定されています。

日時の設定

日時パラメータの設定作業は、時刻、日付、タイムゾーン、およびタイム サーバの設定で構成されています。日時パラメータを設定するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `Clock set` *`08:20:00 04 15 2002`* — 時刻と日付を設定します（例：時刻 **8:20 A.M.**、日付 **April 15, 2002**）。
3. `Clock set` *`08:20:00 04 15 2002`* —ストレージ ルータが設置されている場所のタイム ゾーンを指定します。タイム ゾーンを指定しなかった場合、デフォルトでGMTが使用されます。

`clock timezone`コマンドを使用するには、有効なタイムゾーン文字列を使用する必要があります。有効なタイムゾーン文字列を表示するには、`clock timezone ?`コマンドを使用します。

4. `NTP peer 10.1.60.86` — ストレージ ルータが日付と時刻を同期させるNTPサーバの名前またはIPアドレスを指定します（オプション）。
5. `IP route 10.1.60.86/32 10.1.10.201` — タイム サーバがストレージ ルータの管理サブネット外にある場合は、ゲートウェイIPアドレスを設定します。2番目のIPアドレスには、タイム サーバへのアクセスを提供するストレージ ルータ管理ネットワーク上のゲートウェイを指定します（オプション）。

注記: この設定例では、ホストにIPアドレス10.1.60.86を指定するために、マスクは32 255.255.255.255に設定されています。

ネットワーク管理アクセスの設定

ネットワーク管理アクセスの設定作業では、SNMPを設定します。ネットワーク管理アクセス用にSNMPを設定するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `no restrict all telnet` — すべてのインタフェースでTelnetアクセスを有効にします。デフォルトでは、Telnetアクセスは管理インタフェースでのみ有効になっています（オプション）。
3. `snmp-server community world ro` — ストレージ ルータ ネットワークへの読み取り専用アクセス権を持っているコミュニティ（つまり、ストレージ ルータが応答するGETコマンド発行元のコミュニティ）の名前を指定します。デフォルトの読み取り専用コミュニティは**public**です（オプション）。
4. `snmp-server community mynetmanagers rw` — ストレージ ルータ ネットワークへの書き込みアクセス権を持っているコミュニティ（つまり、ストレージ ルータが応答するSETコマンド発行元のコミュニティ）の名前を指定します。デフォルトの書き込みコミュニティは**private**です（オプション）。
5. `snmp-server host 10.1.30.17 version 2 traps` — 指定したバージョンの通知（トラップ）に使用する最初の送信先ホストのIPアドレスを指定します。デフォルトのバージョンは、バージョン1トラップです。

注記: この構成例では、トラップ ホストのIPアドレスはストレージ ルータ管理サブネット外になっています。「管理インタフェースの設定」の手順で、10.1.30.0サブネット上のホストへのアクセスを提供するゲートウェイがすでに指定されています。

---

6. `snmp-server host 10.1.30.18 traps` — 通知（トラップ）に使用する2番目の送信先ホストの IP アドレスを指定します。デフォルトのバージョンは、バージョン 1 トラップです（オプション）。

7. `snmp-server sendauthtraps` — 認証失敗トラップの送信を有効にします（オプション）。
8. `no snmp-server linkupdown all` — デフォルトでは、SNMPエージェントは、すべてのインタフェース用のリンク接続/切断トラップを生成することができます。この構成例では、コマンドによりすべてのインタフェースのこの設定が無効になっています（オプション）。

パスワードの設定

パスワードの設定では、10/100 イーサネット管理インタフェースへアクセスするためのMonitorモードおよびAdministratorモードのパスワードを設定します。（Telnet経由のCLIとHTTP経由のWebベースのGUIで使用）。これらのパスワードを有効にして、EIA/TIA-232 コンソール インタフェースへのアクセスを制限できます。パスワードを設定するには、以下の手順に従います。

注記: Monitor**および**Administrator**モードの工場出荷時のデフォルトのパスワードはどちらもhpです。**

---

1. `enable` — Administrator モードに入ります。
2. `Monitor password janu$01` — Monitor パスワードを設定します。
3. `Admin password electr@50` — Administratorパスワードを設定します（システム管理者が設定を変更できるようになります）。
4. `Restrict console` — EIA/TIA-232コンソール インタフェースに接続されているコンソール経由でストレージ ルータにアクセスする際に、MonitorモードおよびAdministratorモードのパスワードが要求されるようになります（オプション）。

管理者の連絡先の設定

管理者の連絡先では、ストレージ ルータのシステム管理者の名前、電子メール アドレス、電話番号、およびページャ番号を指定します。管理者の連絡先を設定するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `Admin contactinfo name Pat J. Smith, email pjsmith@mystoragenet.com phone 763-555-1117, and pager 763-555-7766` — 担当者名、電子メール アドレス、電話番号、およびページャ番号を指定します。スペースが含まれている各文字列は、単一引用符または二重引用符で囲みます。

注記: `admin contactinfo`**コマンドでは、いずれか1つのパラメータ、または4つすべてのパラメータを指定する必要があります。**

HAインタフェースの設定

ストレージ ルータがストレージ ルータ クラスタの一部である場合、HA（High-Availability）インタフェースを設定する必要があります。HAインタフェースのパラメータを設定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `Show cluster` — クラスタ情報を表示し、HA構成フィールドを参照して、ストレージ ルータがスタンドアロンまたはクラスタのどちらで実行されているかを確認します。また、HAインタフェースが正しいIPアドレスで構成されているかどうかを確認します。
3. `setup cluster` — セットアップ クラスタ ウィザードを実行します。ウィザードでは、以下のことが求められます。
   - 適切なHA構成モード（スタンドアロンまたはクラスタ）の選択
   - HAインタフェースのIPアドレスとサブネット マスクの指定（HAインタフェースおよび管理インタフェースは、同じネットワーク上にあってはいけません。各インタフェースは、固有なIPネットワーク上になければなりません。クラスタ モードの場合、すべてのストレージ ルータのHAインタフェースが同じIPサブネット上になければなりません）
   - クラスタ名の変更（必要に応じて）
   - ストレージ ルータの現在の設定を保持する（retain）か削除する（delete）かどうか
     - 保持することを選択した場合は、このストレージ ルータの設定（SCSI ルーティング インスタンスを含む）が、同じクラスタ内の他のストレージ ルータに伝達される
     - 削除することを選択した場合は、既存の設定（SCSI ルーティング インスタンスを含む）がストレージ ルータから削除される

   既存のクラスタを結合すると、クラスタが使用可能なアクセス リストで以前に定義したアクセス リストが上書きされます。設定情報を保持または削除するかどうかに関わらず、このようになります。現在のアクセス リストをクラスタで使用するためには、クラスタを結合する前にそれをファイルに保存して、結合してからそれを復元します。詳細については、第10章「高可用性クラスタの設定」を参照してください。

   表示された指示に従って`yes`と入力し、ストレージ ルータの現在の設定を保持または削除することを了承します。システムは自動的に再起動します。

設定の確認と保存

以下の手順に従って、システム パラメータを確認します。`save system bootconfig`または`save all bootconfig`コマンドを使用して、設定をいつでも保存できます。実行中の設定がストレージ ルータの再起動時に使用されるようにするには、実行中の設定を起動時の設定に保存する必要があります。

設定情報を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `Show system` — システム名、ソフトウェア バージョン、日時(タイム ゾーンを含む)、NTPサーバ、DNS（ネーム サーバ)、および管理インタフェースとHAインタフェースのIPアドレスなどのシステム情報を表示します。
3. `Show IP route` — ルーティング情報を追加した場合に、システム ルート テーブルを表示します（オプション)。
4. `Show SNMP` — ストレージ ルータのSNMP管理設定情報が設定されている場合にそれを表示します（オプション)。
5. `Show admin` — ストレージ ルータのシステム管理者の連絡先が設定されている場合にそれを表示します（オプション)。
6. `Show cluster` — ストレージ ルータをクラスタのメンバとして構成した場合に、クラスタ名と他のクラスタ情報を表示します（オプション)。
7. `Show bootconfig` — ストレージ ルータの現在の起動設定を表示します（オプション)。
8. `Show runningconfig` — ストレージ ルータの現在の実行設定を表示します（オプション)。

VLANの設定

7

この章では、ストレージ ルータをVLAN用に設定する方法と以下の内容について説明します。

VLANは、CLIコマンドまたはWebベースのGUIを使用して設定または変更できます。この章では、CLIコマンドによる設定方法を説明します。WebベースのGUIを使用する場合は、Webブラウザでストレージ ルータの管理インタフェースのIPアドレスを指定し、ログオン後、［Help］をクリックしてGUIのオンライン ヘルプを参照してください。

事前に必要な作業

VLANを設定する前に、第5章「ストレージ ルータの設定」と第6章「システム パラメータの設定」の指示に従ってすべてのシステム パラメータを設定したことを確認してください。

VLANカプセル化

ストレージ ルータは、VLANカプセル化に関するIEEE 802.1Q規格を使用します。

注記: ストレージ ルータをスイッチに接続する場合は、スイッチ ポートをトランク ポートとして設定し、カプセル化をトランク ポートのデフォルト設定であるInter-Switch Link（ISL）ではなく802.1Qに設定する必要があります。

設定作業

ストレージ ルータでVLANを設定するには、以下の手順に従います。

1. VTP（VLAN Trunking Protocol）を使用してVLANを設定するか、VTPを使用せずにVLANを設定します。
2. IPルートを設定します。
3. 設定を確認して保存します。

注記: 設定作業を実行しているときには、いつでも設定を確認および保存できます。
`save all bootconfig` **CLIコマンドを使用して設定を保存します。このコマンドを実行すると、すべての設定データが起動設定に保存され、ストレージ ルータの再起動時に使用されます。**

---

4. SCSIルーティングを設定して、SCSIルーティング インスタンスにVLANを割り当てる場合は、第8章「SCSIルーティングの設定」に進みます。

図39に、VLAN用にストレージ ルータを設定するのにVTPを使用した場合と使用しない場合の違いを示します。

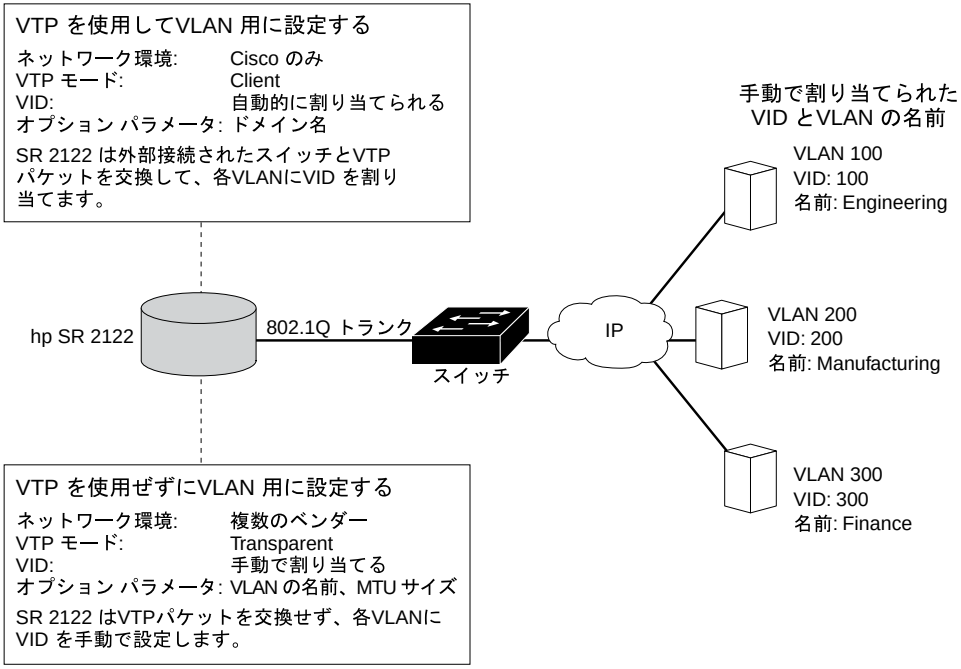

図39: VLAN用に設定するのにVTPを使用した場合と使用しない場合の違い

VTPを使用してストレージ ルータをVLAN用に設定する

VTP（VLAN Trunking Protocol）を使用してストレージ ルータをVLAN用に設定するには、VTPドメイン名を割り当て、VTPモードをクライアントに設定します。Cisco Systemsのプロトコルであ るVTPは、VLAN情報をスイッチ ネットワーク全体に伝達するのに使用します。

VTPを使用してVLANを設定するには、以下の手順に従います。

注記: VTP**は、Cisco**ネットワーク環境でのみ使用できます。

---

1. `enable` — Administratorモードに入ります。
2. `vtp domain` *`opus`* — ストレージ ルータが属しているドメインにVTPドメイン名opusを割り当てます。ドメイン名を指定しないと、ストレージ ルータは最初にVTPメッセージを受信したドメインに自分自身を割り当てます。デフォルトの設定は**none**です。
3. `vtp mode` *`client`* — VTPモードのデフォルト設定は**client**です。現在の設定が**transparent**である場合は、VTPモードを**client**に設定してください。

   clientモードの場合、ストレージ ルータは外部接続されたスイッチとVTPパケットを交換して、ネットワーク内でアクセス可能なVLANに関する情報を入手します。

注記: VTP**モードは、クラスタ全体に影響する設定項目です。設定して保存すると、クラスタ内のすべてのストレージ ルータ上でモード設定がアクティブになります。**

VTPを使用せずにストレージ ルータをVLAN用に設定する

VTPを使用せずにストレージ ルータをVLAN用に設定するには、VTPモードをtransparentに設定し、VIDを割り当て、必要に応じてVLANに名前とMTU（maximum transmission unit）を割り当てます。

VTPを使用せずにVLANを設定するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `vtp mode` *`transparent`* — ストレージ ルータのVTPモードを**transparent**に設定します。transparentモードの場合、ストレージ ルータはVTPパケットを交換しないため、VLANを手動で設定する必要があります。デフォルト設定は**client**です。

注記: **VTPモードは、クラスタ全体に影響する設定項目です。設定して保存すると、クラスタ内のすべてのストレージ ルータ上でモード設定がアクティブになります。**

---

3. `vlan` *`100`* `or vlan` *`100`* `name` *`Engineering`* `and mtusize` *`9000`* — VLANを固有に識別するVLAN ID（VID）番号を割り当てます。VIDには、1～4095の任意の整数値を指定できます。

   また、VLANに**Engineering**のような32文字以内の固有の名前を割り当てることもできます。名前を指定しなかった場合、デフォルトの名前が**自動的に割り当てられます**。デフォルト名は、VLANの後ろに4バイトのVID番号（4桁未満の場合は、左側に0が付けられる）が付いた名前になります（例：**VLAN0100**）。

   また、MTUサイズのサイズに1500～9000の値を指定することもできます。デフォルト値は**1500**です。

注記: **VLANは、クラスタ全体に影響する設定項目です。設定して保存すると、クラスタ内のすべてのストレージ ルータにVLAN情報が伝達されます。**

IPルートの設定

VLANにアクセスするためにIPルートを設定するには、目的のVLANに接続されているゲートウェイを使用する静的ルートを指定します。IPルートを設定するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `ip route 10.2.90.285/32 10.2.10.233, interface ge2, and VLAN 100` — 送信先のIPアドレスとサブネット マスク10.2.90.285/32を指定します。サブネット マスクを255.255.255.255に設定します。この例では、サブネット マスクはCIDR 形式/32を使用して設定されています。

   また、ゲートウェイIPアドレス10.2.10.233、インタフェース名ge2、およびVID 100を指定します。

注記: **目的のVID番号を検索するには、`show vlan`コマンドを使用します。VIDがVLAN列に表示されます。**

設定の確認と保存

以下の手順に従って、VTPとVLANの動作情報と設定情報を確認します。
`save all bootconfig`コマンドを使用して設定を保存することができます。実行中の設定がストレージ ルータの再起動時に使用されるようにするには、実行中の設定を起動時の設定に保存する必要があります。設定を保存すれば、ストレージ ルータが再起動時に使用する設定が現在実行されている設定と同じであるかどうかを確認できます。

VTPの動作情報を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `show vtp` — VTPの動作情報を表示します（例1）。

例 1: VTP の動作情報の確認

```
[Storage Router]# show vtp
Configuration Revision   : 8
Number of existing VLANs : 4
VTP Operating Mode       : Client
VTP Domain Name          : opus
```

VTPの設定を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `show vtp config` — VTPの設定を表示します（例2）。

例 2: VTP の設定の確認

```
➔ [Storage Router]# show vtp config
  vtp mode client
  vtp domain opus
```

すべてのVLAN（clientモードでVTPを使用してネットワークから設定を入手した、またはtransparentモードでローカルに設定した）の現在の動作情報を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `show vlan` — VLANの現在の動作情報を表示します（例3）。

例 3: VLAN の動作情報の確認

```
➔ [Storage Router]# show vlan
  VLAN Name                            Status    Ports
  ---- ------------------------------- --------- -----
  100  Engineering                     active    ge2
  200  Manufacturing                   active    ge2

  VLAN Type  MTU   Interfaces
  ---- ----- ----- ------------------------------
  100  enet  1500  ge2VLAN100
  200  enet  1500  ge2VLAN200
```

設定済みのVLAN情報を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `show vlan config` — VTPの設定済み情報を表示します（例4）。

例 4: VLAN の設定情報の確認

```
➔ [Storage Router]# show vlan config
  vlan 100 name Engineering mtu 1500
  vlan 200 name Manufacturing mtu 1500
```

SCSIルーティング インスタンスへのVLANの割り当て

VLANをSCSIルーティング インスタンスに割り当てるには、`scsirouter serverif vlan`コマンドを使用します。この手順は、第8章「SCSIルーティングの設定」の「サーバ インタフェースの設定」で説明しています。SCSIルーティングを設定する場合は、ここで説明している手順に従って設定することをお勧めします。

SCSIルーティングの設定

8

この章では、ストレージ ルータをSCSIルーティング用に設定する方法と以下の内容について説明します。

SCSIルーティングは、CLIコマンドまたはWebベースのGUIを使用して設定できます。この章では、CLIコマンドによる設定方法を説明します。WebベースのGUIを使用する場合は、Webブラウザでストレージ ルータの管理インタフェースのIPアドレスを指定し、ログイン後、［Help］をクリックしてGUIのオンライン ヘルプを参照してください。

事前に必要な作業

SCSIルーティングを設定する前に、第5章「ストレージ ルータの設定」と第6章「システム パラメータの設定」の指示に従ってすべてのシステム パラメータを設定したことを確認してください。

ストレージ ルータでVLANサービスを使用する場合は、まず第7章の「VLANの設定」の説明に従ってVLANを設定してください。

設定作業

ストレージ ルータでSCSIルーティングを設定するには、以下の手順に従います。

1. SCSIルーティング インスタンスを作成します。インスタンスを作成したら、サーバ インタフェース、iSCSIターゲット、およびIPホストによるアクセス用のパラメータを指定してインスタンスを設定します。
2. VLANを使用するように、またはVLANを使用しないようにサーバ インタフェースを設定します。
3. iSCSIターゲットを設定します。
4. SCSIルーティング インスタンスの一部として設定されているiSCSIターゲットにアクセスできるIPホストを識別するアクセス リストを設定します。アクセス リストは、iSCSIターゲットへのアクセスを、IPホストごとに指定する場合に必要です。SCSIルーティング インスタンスに設定されているiSCSIターゲットに、すべてのIPホストがアクセスできるようにする場合は、アクセス リストは必要ありません。（オプション）
5. アクセスを設定します。SCSIルーティング インスタンスの一部として設定されているiSCSIターゲットにアクセスできるIPホストが識別されます。
6. 設定を確認して保存します。

注記: **設定作業を実行しているときは、いつでも設定を確認および保存できます。**
`save all bootconfig` CLI**コマンドを使用して設定を保存します。このコマンドを実行すると、すべての設定データが起動設定に保存され、ストレージ ルータの再起動時に使用されます。**

注意: SCSIルーティング インスタンスを変更する（ターゲットを追加/削除したり、アクセスを変更する）場合は、SCSIルーティング インスタンスを使用してストレージ リソースにアクセスするIPホストのiSCSIドライバの設定も変更してください。詳細については、第5章の「iSCSIドライバのインストール」を参照するか、適切なiSCSIドライバのreadmeファイルを参照してください（最新の iSCSI ドライバ、readme ファイル、設定ファイルのサンプルを http://www.hp.com/supportから入手できます）。

図40に、SCSIルーティング設定要素を示します。図41に、この章で使用している設定例を示します。図42に、SCSIルーティング インスタンスの設定によって決定されるストレージデバイスへのVLANアクセスを示します。

注記: SCSIルーティング インスタンスの設定では、FCインタフェースの設定は行いません。SCSIルーティング インスタンスを設定すれば、すべてのFCインタフェースが使用可能になります。FCインタフェースのデフォルトの特性については、102ページの「FCインタフェースのデフォルト値」を参照してください。

SCSI ルーティングの設定をしたSR 2122

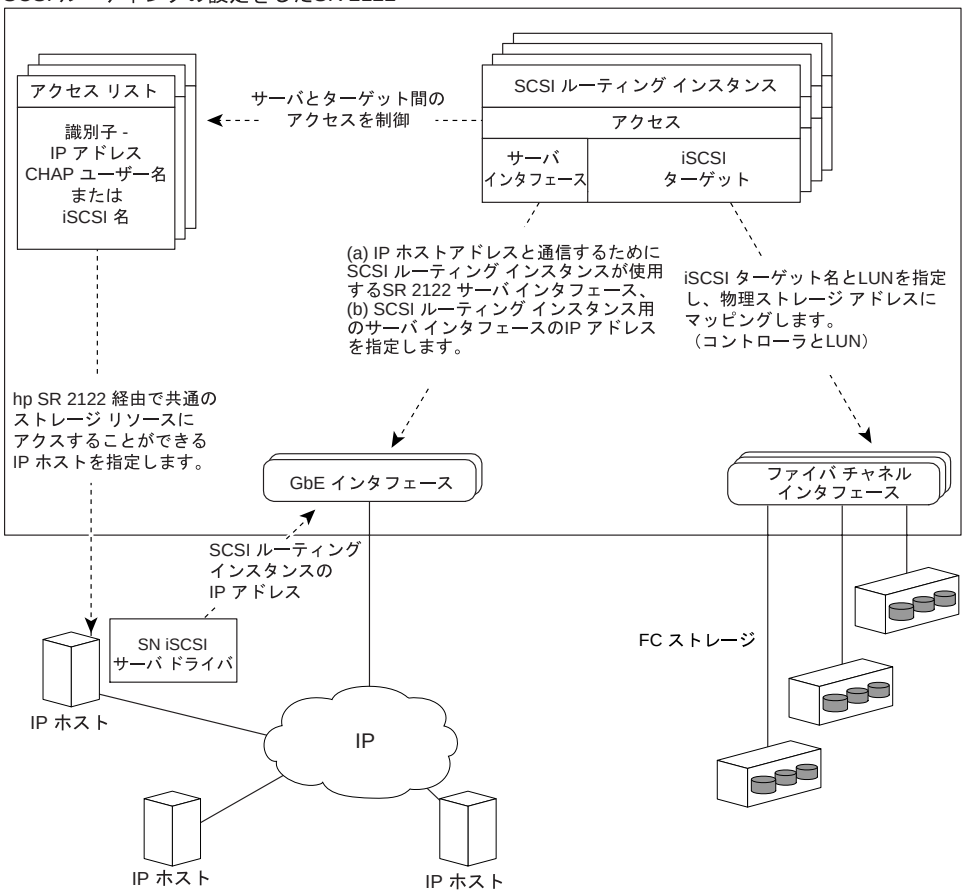

図40: SCSIルーティングの設定要素

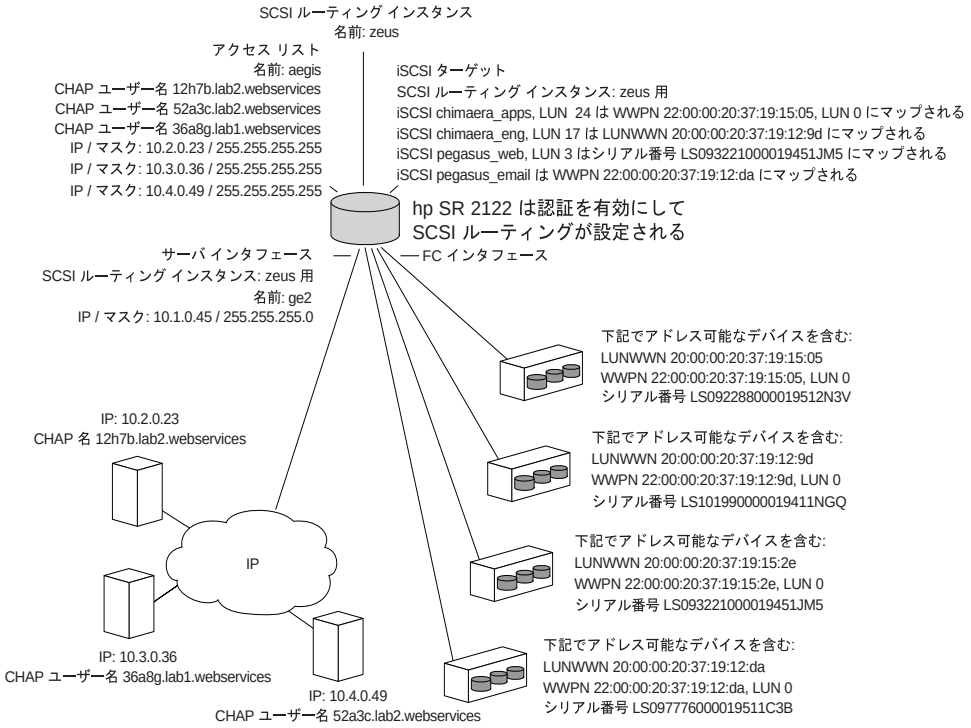

図41: SCSIルーティングのパラメータの設定例

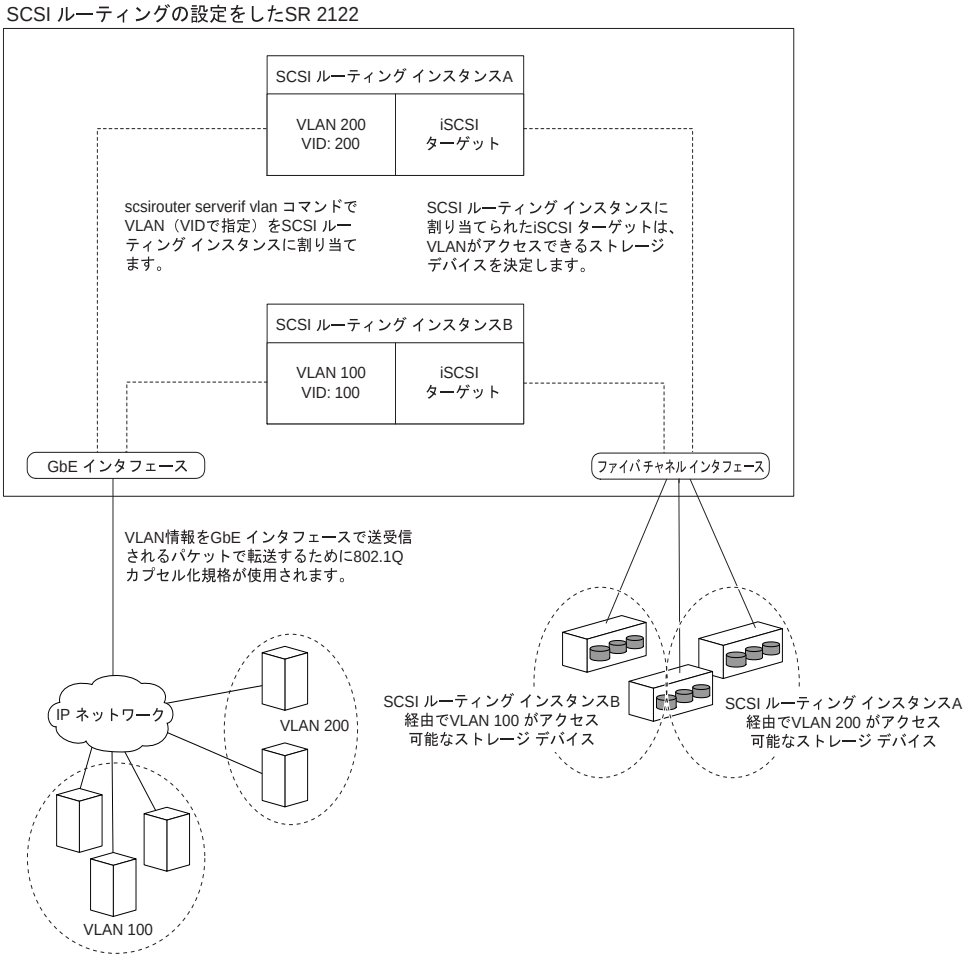

図42: SCSIルーティングの設定によって決定されるストレージ デバイスへのVLANアクセス

SCSIルーティング インスタンスの作成

SCSIルーティング インスタンスの作成では、新しいインスタンスの名前を付けます。SCSIルーティング インスタンスを作成するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* — 新しいインスタンス名**zeus**を指定してSCSIルーティング インスタンスを作成します。

注記: **1つのストレージ ルータまたはクラスタ全体で最大12個のインスタンスを定義できます。高可用性を実現できるようにストレージ ルータ クラスタを構成する方法については、第10章「高可用性クラスタの設定」を参照してください。**

サーバ インタフェースの設定

サーバ インタフェースの設定では、サーバ インタフェースとともに、目的のSCSIルーティング インスタンスへのIPアドレスとサブネット マスクを割り当てます。ストレージ ルータをVLANとともに使用する場合は、VIDでVLANを指定します。

VLANを使用しない場合

SCSIルーティング インスタンスのサーバ インタフェースを設定するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `serverif` *`ge2`* `VLAN` *`100 10.1.0.45/24`* — サーバ インタフェースge2を、目的のSCSIルーティング インスタンス**zeus**に割り当てます。IPホストがSCSIルーティング インスタンスにアクセスするのに使用するIPアドレスとサブネットマスク**10.1.0.45/24**を指定します。この例では、サブネット マスク**255.255.255.0**はCIDR 形式 **/24**を使用して設定されています。

VLANを使用する場合

サーバ インタフェースとVLANをSCSIルーティング インスタンスに割り当てるには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `serverif` *`ge2`* `VLAN` *`100 10.1.0.45/24`* — VID **100**のVLANを目的のSCSIルーティング インスタンス**zeus**に割り当てます。サーバ インタフェース**ge2**と、VLANがSCSIルーティング インスタンスにアクセスするのに使用するIPアドレスとサブネット マスク**10.1.0.45/24**を指定します。この例では、サブネットマスク**255.255.255.0** はCIDR 形式 **/24**を使用して設定されています。

注記: **VIDを検索するには、`show vlan`コマンドを使用します。VIDがVLAN列に表示されます。**

---

iSCSIターゲットの設定

iSCSIターゲットの設定では、iSCSIターゲットが割り当てられるSCSIルーティング インスタンスを指定し、iSCSIターゲットを指定し、iSCSIターゲットを物理ストレージ デバイスにマッピングします。iSCSIターゲットを割り当てる際には、物理ストレージ アドレス、シリアル番号、またはデバイスに割り当てられているインデックス番号によって物理ストレージ デバイスを指定できます。

注記: 新しいiSCSIターゲットを設定した場合、IPホストはそれにアクセスできません。この章の「アクセスの設定」の説明に従って、新しく作成したiSCSIターゲットへのアクセスを設定する必要があります。

マッピングのタイプとストレージ アドレッシングのタイプに応じて、以下のいずれかの手順に従ってください。

- WWPNアドレッシングを使用したターゲットとLUNのマッピング（94ページ）
- LUNWWNアドレッシングを使用したターゲットとLUNのマッピング（95ページ）
- シリアル番号アドレッシングを使用したターゲットとLUNのマッピング（95ページ）
- WWPNアドレッシングを使用したターゲットのみのマッピング（96ページ）

例 5: ストレージ デバイスのインデックス リスト

```
id interface lunwwn           wwpn             tgtid lun vendor  product    serial number
1  fc4       20000020371912d5 22000020371912d5 n/a   0   DEC     HSG80      LS099969000019511C2H
2  fc4       20000020371912da 22000020371912da n/a   0   DEC     HSG80      LS097776000019511C3B
3  fc4       200000203719129d 220000203719129d n/a   0   DEC     HSG80CCL   LS101990000019411NGQ
4  fc4       2000002037191505 2200002037191505 n/a   0   COMPAQ  MSA1000    LS101990000019451JM5
5  fc4       20000020371912b2 22000020371912b2 n/a   0   COMPAQ  MSA1000    LS099843000019430RC7
6  fc4       200000203719152e 220000203719152e n/a   0   COMPAQ  MSA1000    LS093221000019451JM5
```

WWPNアドレッシングを使用したターゲットとLUNのマッピング

物理ストレージ アドレスを使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`24`* `WWPN` *`22:00:00:20:37:19:15:05`* `LUN` *`0`* — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**chimaera_apps**とLUN **24**を指定し、それを目的の物理アドレスWWPN **22:00:00:20:37:19:15:05** LUN **0**にマップします。

インデックス番号を使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`31`* `WWPN` *`#?`* — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**chimaera_apps**とLUN **31**を指定し、シャープ記号と疑問符（#?）を使用して使用可能なストレージ アドレスのインデックス リストを問い合わせます。

3. `SCSIRouter zeus target chimaera_apps LUN 31 WWPN #4` — インデックス番号で示されている物理アドレスを選択して（例5の4を参照）、iSCSIターゲット**chimaera_apps**とLUN **31**の組み合せを目的の物理アドレス WWPN **22:00:00:20:37:19:15:05**, LUN **0**にマップします。

LUNWWNアドレッシングを使用したターゲットとLUNのマッピング

物理ストレージ アドレスを使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target chimaera_apps LUN 17 LUNWWN 22:00:00:20:37:19:12:9d` — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**chimaera_apps**とLUN **17**を指定し、それを目的の物理アドレスLUNWWN **22:00:00:20:37:19:12:9d**にマップします。

インデックス番号を使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target chimaera_apps LUN 17 WWPN #?` — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**chimaera_apps**とLUN **17**を指定し、シャープ記号と疑問符（#?）を使用して使用可能なストレージ アドレスのインデックス リストを問い合わせます。
3. `SCSIRouter zeus target chimaera_apps LUN 17 LUNWWN #3` — インデックス番号で示されている物理アドレスを選択して（例5の3を参照）、iSCSIターゲット**chimaera_apps**とLUN **17**の組み合せを目的の物理アドレスLUNWWN **22:00:00:20:37:19:12:9d**にマップします。

シリアル番号アドレッシングを使用したターゲットとLUNのマッピング

シリアル番号を使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target pegasus_web LUN 3 serial number LS093221000019451JM5` — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**pegasus_web**とLUN **3**を指定し、それを目的のシリアル番号 **LS093221000019451JM5**にマップします。

インデックス番号を使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target pegasus_web LUN 3 serial number #?` — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**pegasus_web**とLUN **3**を指定し、シャープ記号と疑問符（#?）を使用して使用可能なストレージ アドレスのインデックス リストを問い合わせます。

3. `SCSIRouter zeus target pegasus_web LUN 3 serial number #6` — インデックス番号で示されている物理アドレスを選択して（例5の6を参照）、iSCSIターゲット**pegasus_web**とLUN **3**の組み合せを目的の物理アドレス**LS093221000019451JM5**にマップします。

WWPNアドレッシングを使用したターゲットのみのマッピング

物理ストレージ アドレスを使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target pegasus_email WWPN 22:00:00:20:37:19:12:da` — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**pegasus_email**を指定し、それを目的の物理アドレスWWPN **22:00:00:20:37:19:12:da**とそのWWPNの一部として使用可能なすべてのLUNにマップします。

インデックス番号を使用してiSCSIターゲットをストレージ デバイスにマップするには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target pegasus_email WWPN #?` — 目的のSCSIルーティング インスタンス**zeus**を指定します。iSCSIターゲット**pegasus_email**を指定し、シャープ記号と疑問符（#?）を使用して使用可能なストレージ アドレスのインデックス リストを問い合わせます。
3. `SCSIRouter zeus target pegasus_email WWPN #2` — インデックス番号で示されている物理アドレスを選択して（例5の2を参照）iSCSIターゲット**pegasus_email**を目的の物理アドレスWWPN **22:00:00:20:37:19:12:da**にマップします。

アクセス リストの設定

アクセス リストの設定では、名前を指定してアクセス リストを作成し、iSCSIターゲット名を使ってストレージ デバイスにアクセスすることができるIPホストを指定します。IPホストは、以下の方法で指定できます。

- IPアドレス
- CHAPユーザー名（iSCSI認証で使用）
- IPホストのiSCSI名 - iSCSI名は、iSCSIの機能要件に基づいてUTF-8文字列で表されます。これは、場所に依存しない永久的なiSCSIノードIDで、ターゲットの作成時に生成されます。

アクセス リストには、1つまたは複数のタイプの識別エントリを含めることができます。あるタイプの識別エントリがアクセス リストに存在する場合、関連付けられているストレージ ターゲットにアクセスしようとしているIPホストは、アクセス リストに定義されているのと同じタイプのエントリを持っている必要があります。たとえば、アクセス リストにIP

アドレスとiSCSI名の両方の識別エントリ タイプが含まれている場合、関連付けられている一連のストレージ リソースにアクセスする必要があるIPホストは、アクセス リストに含まれているのと同じIPアドレスとiSCSI名エントリを持っている必要があります。

アクセス リストは、iSCSIターゲットへのアクセスを、IPホストごとに指定する場合に必要です。SCSIルーティング インスタンスに設定されているiSCSIターゲットに、すべてのIPホストがアクセスできるようにする場合は、アクセス リストは必要ありません。

注記: アクセス リストにCHAPユーザー名エントリが含まれている場合、ストレージ ターゲットにアクセスするのに使用するSCSIルーティング インスタンスのiSCSI認証も有効にする必要があります。AAAおよびiSCSI認証の詳細については、第9章「認証の設定」を参照してください。

アクセス リストを作成するには、以下の手順に従います。この手順では、アクセス リストの名前は**aegis**で、IPホストIDには3つのIPアドレス（**10.2.0.23**、**10.3.0.36**、**10.4.0.49**）とCHAPユーザー名（**12h7b.lab2.webservices**）が含まれています。

1. `enable` — Administrator モードに入ります。
2. `accesslist` *`aegis`* — 名前**aegis**を指定してアクセス リストを作成します。31文字以内で指定します。
3. `accesslist` *`aegis`* `description` *`“Access to zeus SCSI routing service”`* — アクセス リストの説明を追加します。単一引用符または二重引用符で文字列を囲みます（オプション）。
4. `accesslist` *`aegis 10.2.0.23/32 10.3.0.36/32 10.4.0.49/32`* — IPホストのIPアドレスをアクセス リストに追加します。複数のIPアドレスは、スペースで区切ります。各IPアドレスへのアクセスを制限するには、サブネット マスクを**255.255.255.255**に設定します。この例では、サブネット マスクはCIDR 形式 **/32**を使用して設定されています。
5. `accesslist` *`aegis`* `CHAP-username` *`12h7b.lab2.webservices`* — CHAP ユーザー名をアクセス リストに追加します。各CHAP ユーザー名へのアクセスを制限するには、提供されるパスワードは、AAA認証方法で正しく許可される必要があります。

注記: アクセス リストでCHAP ユーザー名を使用した場合は、認証を有効にする必要があります。

注記: クラスタ環境の場合、クラスタを結合するには、すべてのアクセス リストが最初のストレージ ルータで作成および管理される必要があります。クラスタ内の別のストレージ ルータから `accesslist`コマンドを実行すると、情報メッセージと現在アクセス リストのすべての機能を処理しているストレージ ルータのIPアドレスが表示されます。クラスタ内のストレージ ルータの操作方法については、第11章「ストレージ ルータのメンテナンスと管理」を参照してください。

アクセスの設定

アクセスの設定では、IP ホストがアクセスすることができる iSCSI ターゲットを指定します。アクセスを設定する場合は、iSCSIターゲットを1つずつ指定するか、すべてのiSCSIターゲットを指定できます。同様に、アクセス リストを1つずつ指定するか、SCSIルーティング インスタンスを使用しているすべてのIPホストを指定できます。また、アクセスを拒否するiSCSIターゲットを1つずつ指定するか、すべてのiSCSIターゲットを指定できます。

新しく設定したiSCSIターゲットへのアクセスはデフォルトでは設定されていません。ここで説明している手順に従ってアクセスを設定する必要があります。

アクセスのタイプに応じて、以下のいずれかの手順に従ってください。

- アクセス リストに含まれているIPホストによる、1つのiSCSIターゲットへのアクセスの許可（98ページ）
- すべてのIPホストによる、1つのiSCSIターゲットへのアクセスの許可（98ページ）
- アクセス　リストに含まれているIPホストによる、すべてのiSCSIターゲットへのアクセスの許可（99ページ）
- すべてのIPホストによる、すべてのiSCSIターゲットへのアクセスの許可（99ページ）
- 1つのiSCSIターゲットへのアクセスの拒否（99ページ）
- すべてのiSCSIターゲットへのアクセスの拒否（99ページ）

アクセス リストに含まれているIPホストによる、1つのiSCSIターゲットへのアクセスの許可

アクセス リストに含まれているIPホストがアクセス可能なiSCSIターゲットを1つずつ指定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` ***`zeus`*** `target` ***`chimaera_email`*** `accesslist` ***`aegis`*** — SCSIルーティング インスタンス**zeus**の一部として設定されているiSCSIターゲット**chimaera_email**が、アクセス リスト**aegis**に含まれているIPホストによってアクセスできるように指定します。

すべてのIPホストによる、1つのiSCSIターゲットへのアクセスの許可

すべてのIPホストがアクセス可能なiSCSIターゲットを1つずつ指定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` ***`zeus`*** `target` ***`chimaera_apps`*** `accesslist` ***`all`*** — SCSIルーティング インスタンス**zeus**の一部として設定されているiSCSIターゲット**chimaera_apps**が、すべてのIPホストによってアクセスできるように指定します。

アクセス リストに含まれているIPホストによる、すべてのiSCSIターゲットへのアクセスの許可

アクセス　リストに含まれているIPホストがすべてのiSCSIターゲットにアクセスできるように指定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`aegis`* — SCSIルーティング インスタンス**zeus**の一部として設定されているすべてのiSCSIターゲットが、アクセス リスト**aegis**に含まれているIPホストによってアクセスできるように指定します。

すべてのIPホストによる、すべてのiSCSIターゲットへのアクセスの許可

すべてのIPホストがすべてのiSCSIターゲットにアクセスできるように指定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`all`* — SCSIルーティング インスタンス**zeus**の一部として設定されているすべてのiSCSIターゲットが、すべてのIPホストによってアクセスできるように指定します。

1つのiSCSIターゲットへのアクセスの拒否

IPホストのアクセスを拒否するiSCSIターゲットを1つずつ指定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter zeus target` *`chimaera_apps`* `accesslist` *`none`* — SCSIルーティング インスタンス**zeus**の一部として設定されているiSCSIターゲット**chimaera_apps**に、どのIPホストもアクセスできないことを指定します。

すべてのiSCSIターゲットへのアクセスの拒否

すべての iSCSI ターゲットがすべての IP ホストのアクセスを拒否するように指定する場合は、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`none`* — SCSIルーティング インスタンス**zeus**の一部として設定されているすべてのiSCSIターゲットに、どのIPホストもアクセスできないことを指定します。

設定の確認と保存

以下の手順に従って、アクセス リストの設定とSCSIルーティング設定を確認します。`save all bootconfig`コマンドを使用していつでも設定を保存することができます。実行中の設定がストレージ ルータの再起動に使用されるようにするには、実行中の設定を起動時の設定に保存する必要があります。設定を保存すれば、ストレージ ルータが再起動時に使用する設定が現在実行されている設定と同じであるかどうかを確認できます。

アクセス リストの設定を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `Show accesslist` — 既存のすべてのアクセス リストの一覧を表示します（例6）。
3. `Show accesslist` *`aegis`* — アクセス リストに指定されているIPホストを表示します（例7）。

例 6: 既存のアクセス リストの確認

```
➔ [SR2122]# show accesslist
aegis
hris-mgmt
```

例 7: アクセス リスト aegis に含まれている IP アドレスの確認

```
➔ [SR2122]# show accesslist aegis
accesslist aegis description "Access to zeus SCSI routing service"
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis chap-username 12h7b.lab2.webservices
```

SCSIルーティング インスタンスの設定を確認するには、以下の手順に従います。

1. `enable` — Administrator モードに入ります。
2. `Show scsirouter` *`zeus`* — 指定したSCSIルーティング インスタンス用に設定されているパラメータを表示します（例8）。

例 8: SCSI ルーティング インスタンスの設定の確認

```
➔ [SR2122]# show scsirouter zeus
zeus description "(not set)"
zeus authenticate "none"
zeus primary "none"
zeus proxy server disabled
zeus failover primary "none"
zeus failover secondary "none"
zeus target naming authority "none"
zeus target log level is not available
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps Name "iqn.1987-05.com.hp.00.d3f8a650c7deacecd97e1812d.chimaera_"
zeus target chimaera_apps enabled "TRUE"
```

```
zeus target chimaera_apps accesslist "all"
zeus target chimaera_apps lun 24 wwpn "22:00:00:20:37:19:15:05" lun "0" I/F fci1
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "all"
zeus target chimaera_eng lun 17 lunwwn "22:00:00:20:37:19:12:9d" I/F fci1
zeus target pegasus_web description "(not set)"
zeus target pegasus_web Name
"iqn.1987-05.com.hp.00.d6bf2b11ed9c88ce9299ea3f0961ad94.pegasus_web"
zeus target pegasus_web enabled "TRUE"
zeus target pegasus_web accesslist "all"
zeus target pegasus_web lun 3 serial "LS0932210000019451JM5" I/F fci1
```

FCインタフェースのデフォルト値

ファイバ チャネル インタフェース1および2の デフォルトの動作特性を以下に示します。

- 公平性：無効（スイッチが優先される）
- Fabric Address Notification（FAN）：無効
- オート ネゴシエーション転送速度（回線速度：自動）
- マルチフレーム シーケンス バンドル：有効
- ポート タイプの自動選択：
  - auto - ポート タイプ：gl-port
  - e-port - ポート タイプ：スイッチ/スイッチ
  - f-port - ポート タイプ：Fabric
  - fl-port - ポート タイプ：Fabric Loop（Public Loop）
  - g-port - ポート タイプ：Generic（f-portまたはe-port）
  - gl-port - ポート タイプ：Generic Loop（fl-port、e-port、またはg-port）
  - tl-port - ポート タイプ：Translated Loop

認証の設定

9

この章では、HPの認証、認可、アカウンティング（authentication, authorization and accounting：AAA）方式の認証機能をストレージ ルータに設定する方法について、およびAAA認証方式を使用するiSCSI認証を有効にする方法について説明します。

作業内容は以下のとおりです。

このストレージ ルータでは、AAA認証機能が常に有効になっています。AAA認証機能を無効にすることはできません。

認証パラメータは、CLIコマンドかWebベースのGUIを使用して設定できます。この章では、CLIコマンドによる設定方法を説明します。WebベースのGUIを使用する場合は、Webブラウザでストレージ ルータの管理インタフェースのIPアドレスを指定し、ログイン後、［Help］をクリックしてGUIのオンライン ヘルプを参照してください。

事前に必要な作業

ストレージ ルータのAAA認証およびiSCSI認証の設定作業に入る前に、第5章「ストレージ ルータの設定」または第6章「システム パラメータの設定」を参照して、システム パラメータの設定を済ませておいてください。また、ストレージ ルータでSCSIルーティングを行う場合は、第8章「SCSIルーティングの設定」を参照して、SCSIルーティング インスタンスの設定も済ませておいてください。

注記: **AAA認証およびiSCSI認証の設定パラメータはクラスタ全体で共有されるのではなく、システムごとに保存されます。ただし、クラスタ内のすべてのストレージ ルータに同じ認証パラメータを設定したほうが好都合な場合もあります。**

---

iSCSI認証の使用

iSCSI認証は、SCSIルーティング インスタンス経由でストレージにアクセスするIPホストの認証メカニズムです。iSCSI認証を有効にした場合、iSCSI TCP接続が確立されるたびに、ユーザー名とパスワードが iSCSI ドライバによって提供されます。iSCSI 認証では、iSCSI CHAP（Challenge Handshake Authentication Protocol）認証方式を使用しています。認証サービスは、各ストレージ ルータに設定されたAAAサブシステムによって提供されます。

AAA（Authentication, Authorization and Accounting）はセキュリティ機能の設定に関するCiscoの体系的フレームワークであり、認証、認可、アカウンティングという3つの独立した機能を、モジュール化された整合的な方法で設定する仕組みです。このストレージ ルータには、この中の認証機能が実装されています。

認証機能によって、ユーザー確認に関する各種機能（ログイン/パスワード ダイアログ ボックスの表示、認証の試行と応答、メッセージングのサポートなど）が提供されます。ユーザーは、認証を経てから、要求したオブジェクト、機能、ネットワーク サービスにアクセス可能になります。AAA 認証機能を設定するには、認証サービスのリストを定義します。iSCSI認証機能では、このAAA認証サービス リストが使用されます。iSCSI認証機能は、個々のSCSIルーティング インスタンスごとに有効にできます。

AAAセキュリティ サービス

iSCSI認証では、AAAセキュリティ サービスを使用してセキュリティ機能を管理します。リモートのセキュリティ サーバを使用する場合、AAAによって、ストレージ ルータとリモートRADIUS/TACACS+セキュリティ サーバの間の通信が確立されます。

この章では、以下のAAAセキュリティ サービスの設定方法について説明します。

- RADIUS：不正アクセスからネットワークを保護する分散型クライアント/サーバ システムです。RADIUSは、AAAに基づいて実装されています。RADIUSでは、ストレージ ルータから中央の RADIUS サーバに認証要求が送信されます。RADIUS サーバには、ユーザー認証とネットワーク サービス アクセスに関するあらゆる情報が格納されています。
- TACACS+：指定されたSCSIルーティング インスタンス経由でストレージ ターゲットにアクセスするユーザーを集中的に検証する、セキュリティ アプリケーションです。TACACS+は、AAAに基づいて実装されています。TACACS+サービスは、TACACS+デーモン上のデータベースで管理されます。TACACS+デーモンは、通常、UNIXワークステーションやWindows NTワークステーションで実行されます。TACACS+では、認証、認可、アカウンティングの各機能が、個別にモジュール化された形で提供されています。
- localまたはlocal-case：ストレージ ルータ上のローカル ユーザー名データベースを使用して認証を行います。local-caseの場合、ユーザー名の認証で大文字/小文字が区別されます。なお、パスワードの認証では、常に大文字/小文字が区別されます。

設定作業

以下の手順に従って、ストレージ ルータのiSCSI認証、および対応するAAA認証サービスを設定します。

1. RADIUS、TACACS+、ローカル　ユーザー名データベースなどの必要なセキュリティ サービスを設定します。
2. AAA認証リストを作成します。
3. iSCSI認証サービスをテストします。
4. 個々のSCSIルーティング インスタンスに対して、iSCSI認証を有効にします。
5. AAA認証とiSCSI認証の設定を確認して保存します。

図43に、AAA認証設定の構成要素を示します。また、図44に、この章の説明で使用する、iSCSI認証とAAA認証サービスの設定例を示します。

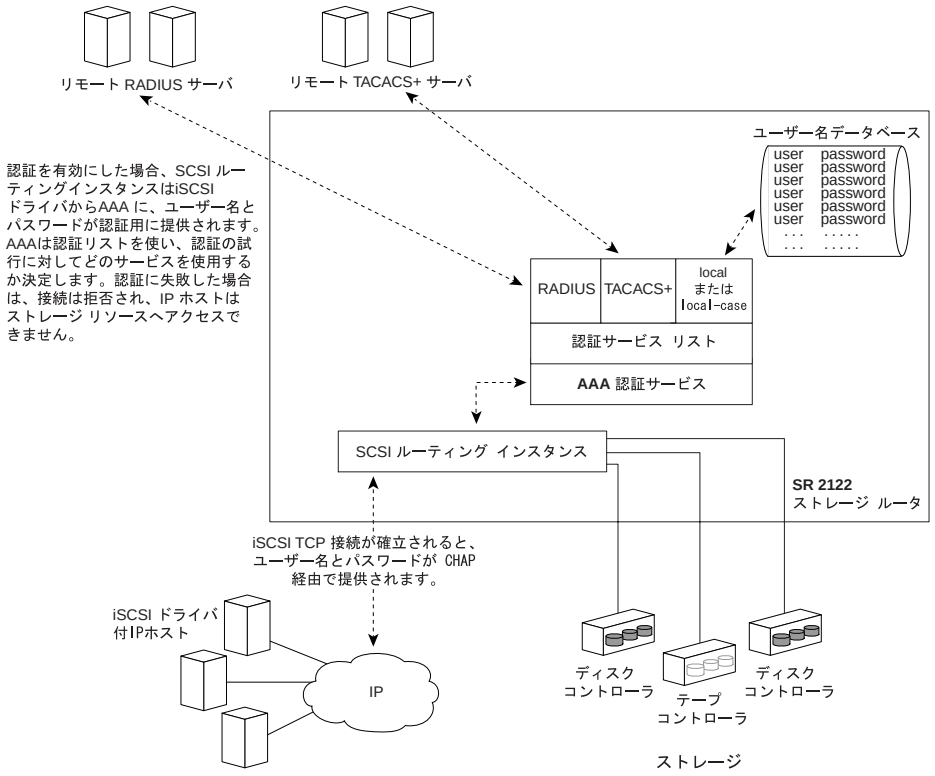

図43: iSCSI認証設定の構成要素

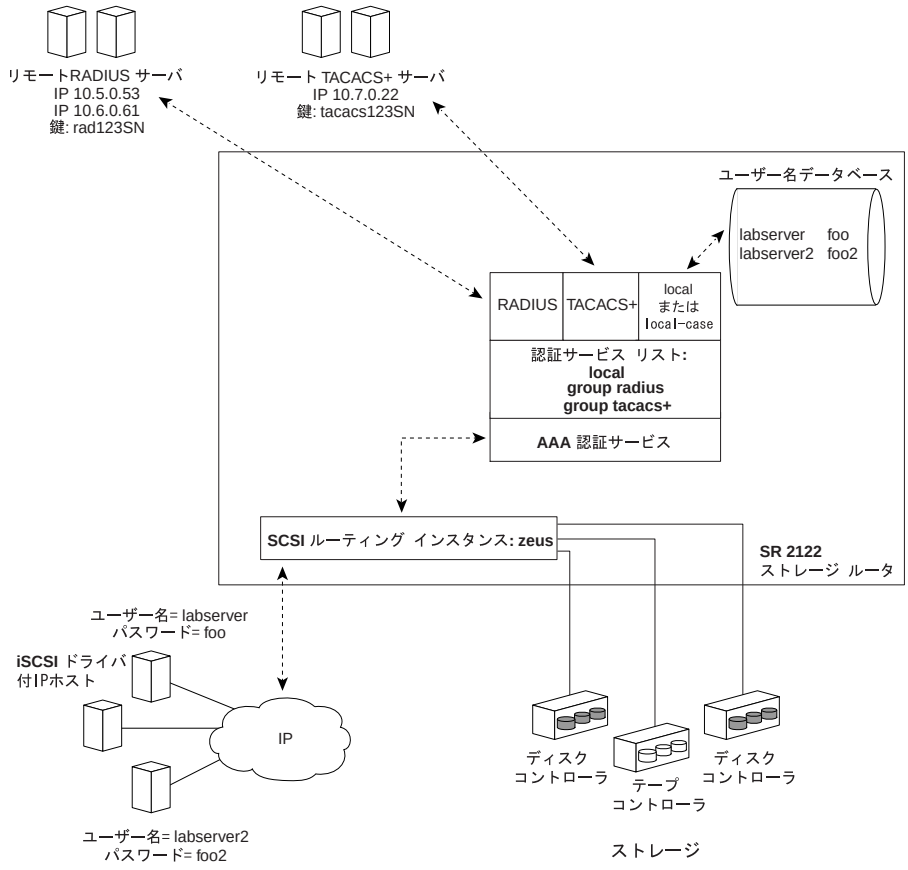

図44: iSCSI認証の設定例

セキュリティ サービスの設定

セキュリティ サービスを設定するには、ストレージ ルータで使用可能な各種サービス オプションのパラメータを適切に設定します。ストレージ ルータでは、サポートされているセキュリティ サービスの一部またはすべてを使用できます。

以下の手順に従って、ストレージ ルータで使用する適切なセキュリティ サービスを設定します。

- RADIUSサーバ（108ページ）
- TACACS+ホスト（108ページ）
- ローカル ユーザー名データベース（109ページ）

RADIUSサーバ

RADIUSセキュリティ サービスを設定するには、以下の手順でコマンドを実行します。

1. `enable` — Administratorモードに入ります。
2. `radius-server host 10.5.0.53` — AAA認証サービスに使用するRADIUSサーバを指定します。この例では、IPアドレス**10.5.0.53**のRADIUSサーバをストレージ ルータで使用するよう指定しています。ポート番号を指定していないので、デフォルトのUDPポート1645が認証要求に使用されます。グローバル タイムアウト値と再送信回数が使用されます。
3. `radius-server host 10.6.0.61` — セカンダリRADIUSサーバを指定します。RADIUSサーバは、定義した順にアクセスされます。この例では、AAA認証サービスに使用する2番目のRADIUSサーバとして、IPアドレス**10.6.0.61**のRADIUSサーバを指定しています。
4. `radius-server key rad123SN` — ストレージ ルータとRADIUSデーモン間のあらゆるRADIUS通信に使用する、グローバル認証と暗号化の鍵を指定します。この例では、**rad123SN**という鍵を指定しています。この鍵は、RADIUSデーモンで使用する鍵と一致させる必要があります。

TACACS+ホスト

TACACS+セキュリティ サービスを設定するには、以下の手順でコマンドを実行します。

1. `enable` — Administratorモードに入ります。
2. `tacacs-server host 10.7.0.22` — AAA認証サービスに使用するTACACS+サーバを指定します。この例では、IPアドレス**10.7.0.22**のTACACS+サーバをストレージ ルータで使用するよう指定しています。ポート番号を指定していないので、デフォルトのポート**49**が認証要求に使用されます。グローバル タイムアウト値が使用できます。
3. `tacacs-server key tacacs123SN` — ストレージ ルータとTACACS+デーモン間のあらゆるTACACS+通信に使用する、グローバル認証と暗号化の鍵を指定します。この例では、**tacacs123SN**という鍵を指定しています。この鍵は、TACACS+デーモンで使用する鍵と一致させる必要があります。

ローカル ユーザー名データベース

ローカル ユーザー名データベースを設定するには、以下の手順でコマンドを実行します。

注記: パスワードはクリア テキストで入力しますが、CLIコマンド履歴キャッシュには「XXXX」に変更されて格納されます。またローカル ユーザー名データベースには、暗号化された形式で格納されます。

1. `enable` — Administratorモードに入ります。
2. `username labserver password foo username labserver2 password foo2` — ストレージへのアクセスに認証が必要な各デバイスごとに、ユーザー名とパスワードを指定します。たとえば、次のユーザー名とパスワードの組み合わせを指定します。
   - `labserver`と`foo`
   - `labserver2`と`foo2`

   ここで指定するユーザー名とパスワードは、iSCSIドライバ（iSCSI認証が有効になっているSCSIルーティング インスタンス経由でストレージにアクセスする必要のあるiSCSIドライバ）で設定されているユーザー名とパスワードと一致させる必要があります。他の認証サービス（RADIUSやTACACS+）も使用する場合は、それらのサービスが認証時に使用するデータベースにも、同じユーザー名とパスワードを設定しておく必要があります。

パスワードには、以下の規則が適用されます。

- パスワードはクリア テキストで入力します。ただし、データベースには暗号化された形式で格納されます。
- スペース文字を含む文字列をパスワードに指定する場合は、全体をシングル クォーテーションかダブル クォーテーションで囲みます。
- 最初に入力するとき以外、パスワードは暗号化された形式で表示されます。ローカル ユーザー名データベースのエントリは、`show aaa`コマンドを使用して表示できます。以下にこのコマンドの出力例を示します。

  ```
  username "foo" password "9 ea9bb0c57ca4806d3555f3f78a4204177a"
  ```

注記: 上の出力例のパスワードの先頭にある「9」は、パスワードが暗号化されていることを示しています。

- 通常の`username password`コマンドを使用して、暗号化されたパスワードを再設定することができます。暗号化されたパスワードには、先頭に「**9**」とスペース文字が付くので、全体をシングル クォーテーションかダブル クォーテーションで囲みます。たとえば、上の例の「`"9 ea9bb0c57ca4806d3555f3f78a4204177a"`」をコピーし、それを`username pat`コマンドに貼り付けて実行すると、ユーザー `foo`と同じパスワードがユーザー `pat`に設定されます。この機能を使用して、保存済みの設定ファイルからユーザー名とパスワードを復元することができます。
- 暗号化されていないパスワードを指定する場合は、パスワードの先頭に「0（ゼロ）」とスペース文字を付けます。暗号化されているパスワードを指定する場合は、「9」とスペース文字を付けます。「0」や「9」自体で始まり、その後にいくつかのスペース文字が続くパスワードを指定する場合は、まず「0」とスペース文字を入力し、その後にパスワードを入力します。たとえば、「0 123」というパスワードをユーザー `pat`に設定するには、次のコマンドを実行します。

  ```
  username pat password “0 0 123”
  ```

  「`9 73Zjm 5`」というパスワードをユーザー `lab1`に設定するには、次のコマンドを実行します。

  ```
  username lab1 password “0 9 73Zjm 5”
  ```

AAA認証リストの作成

iSCSI認証では、セキュリティ機能の管理に、定義済みAAA認証サービスのリストを使用します。この認証サービス リストは、*default*という名前で作成する必要があります。

iSCSI認証に使用するAAA認証サービス リストを作成するには、以下の手順でコマンドを実行します。

1. `enable` — Administratorモードに入ります。
2. `aaa authentication iscsi default local group radius group tacacs+` — 認証サービス リストを**default**という名前で作成します。この例では、認証時にAAAがまずローカル ユーザー名データベースを使用するように、認証リストを作成しています。該当するユーザー名がローカル ユーザー名データベースに見つからなかった場合、AAAはRADIUSサーバの使用を試みます。RADIUSサーバが見つからなかった場合はRADIUSからエラーが返され、AAAは次にTACACS+サーバの使用を試みます。TACACS+サーバが見つからなかった場合はTACACS+からエラーが返され、AAA認証はエラーになります。RADIUSサーバやTACACS+サーバが、該当するユーザー名とパスワードのペアを見つけられなかった場合は、その時点で認証エラーになり、それ以外の認証方式は試行されません。

注記: **localまたはlocal-caseが認証リストの1番目のサービスとして指定されているときに、該当するユーザー名が見つからなかった場合、認証リストの2番目のサービスが試行されます。1番目のサービスがlocalまたはlocal-caseでなかった場合は、該当するユーザー名が見つからないと認証エラーになります。**RADIUS**サーバや**TACACS+**サーバがユーザー名を見つけられなかった場合は、常に認証エラーになります。**

---

iSCSI認証のテスト

SCSIルーティング インスタンスに対してiSCSI認証を有効にする前に、ストレージ ルータからiSCSI認証をテストできます。テストでは、指定したユーザー名とパスワードがAAA認証機能に渡され、AAA認証機能がiSCSIのdefault認証リストを使用して認証を行います。テストの合否（passまたはfail）は、コマンドの出力結果に示されます。

iSCSI認証をテストするには、以下の手順でコマンドを実行します。

1. `enable` — Administratorモードに入ります。
2. `aaa test authentication iscsi default labserver foo`および`aaa test authentication iscsi default labserver2 foo2` — ユーザー名データベースに登録されているユーザー名とパスワードをテストします。AAA認証機能は、default認証リストのサービスを使用して認証を行います（例9）。

例 9: 認証のテスト

```
→ *[SR2122-MG1]# aaa test authentication iscsi default labserver foo

  Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being queued

  Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete, status = pass
```

iSCSI認証の有効化

iSCSI認証は、個々のSCSIルーティング インスタンスごとに有効にします。デフォルトでは、iSCSI認証は無効になっています。

default AAA認証リストに定義されているAAA認証方式を使用してiSCSI認証を有効にするには、以下の手順でコマンドを実行します。

1. `enable` — Administratorモードに入ります。
2. `scsirouter zeus authenticate yes` — 指定したSCSIルーティング インスタンスに対して、認証を有効にします。この例では、**zeus**というSCSIルーティング インスタンスに対して、認証を有効にしています。

設定の確認と保存

認証設定は、`save aaa bootconfig`コマンドまたは`save all bootconfig`コマンドを使用して、いつでも保存できます。ストレージ ルータの再起動時に常に設定が復元されるようにするには、認証設定を保存しておく必要があります。

認証設定の確認と保存を行うには、以下の手順でコマンドを実行します。

1. `enable` — Administratorモードに入ります。
2. `show aaa` – AAA認証設定を表示します（例10）。
3. `show scsirouter zeus` — SCSIルーティング インスタンス**zeus**でiSCSI認証が有効になっていることを確認します（例11）。
4. `save aaa bootconfig` – 認証設定を保存します。
5. `save scsirouter zeus bootconfig` – SCSIルーティング インスタンスを保存します。
6. `save all bootconfig` – 一度にすべての設定を保存します。手順4の`save aaa bootconfig`コマンドと手順5の`save scsirouter bootconfig`コマンドを個々に実行する代わりに、このコマンドを実行してもかまいません。（オプション）

例 10: AAA 認証設定の表示

```
➔ [SR2122-MG1]# show aaa
aaa new-model
aaa authentication iscsi default local gro up radius group tacacs+
username "LabServer" password "9 3b7e1560943b2c3df73ae16dd8c21406ad"
username "LabServer2" password "9
5a034dba7085f7628852db4637787b3f9e"
radius-server key "9 4f5e3deda858731566fa8c7fa23d8a5b4d"
radius-server timeout 100
radius-server retransmit 3
radius-server host 10.5.0.53 auth-port 1645
radius-server host 10.6.0.61 auth-port 1645
tacacs-server key "9 10d2a453d607e75f36ca96dfc5d36b4495"
tacacs-server host 10.7.0.22 auth-port 49
```

例 11: SCSI ルーティング インスタンスに対する iSCSI 認証の確認

```
[SR2122-MG1]# show scsirouter zeus
zeus description "(not set)"
zeus authentication "yes"
zeus primary "none"
zeus target naming authority "none"
zeus serverif ge2 10.1.0.45/24
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps WWUI
"iqn.1987-05.com.hp.00.0b1aaa415a4146aa2d899c47070c3c06.chimaera_apps"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "none"
zeus target chimaera_apps lun 24 wwpn "22:00:00:20:37:19:15:05" lun "0"
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng WWUI
"iqn.1987-05.com.hp.00.0b1aaa415a4146ab2d799c45070c3d06.chimaera_eng"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "aegis"
zeus target chimaera_eng lun 17 wwnn "22:00:00:20:37:19:12:9d"
zeus target pegasus_email description "(not set)"
zeus target pegasus_email WWUI
"iqn.1987-05.com.hp.00.0b1aca415a6146ea2d809c44070c2c06.pegasus_email"
zeus target pegasus_email enabled "TRUE"
zeus target pegasus_email accesslist "all"
zeus target pegasus_email wwpn "22:00:00:20:37:19:12:da"
```

高可用性クラスタの設定

10

この章では、ストレージ ルータのクラスタ構成の設定方法について説明します。クラスタを構成すると、一方のストレージ　ルータに障害が発生した場合でも、他方のストレージ ルータがバックアップ機として動作します。作業内容は以下のとおりです。

高可用性クラスタの設定は、CLIコマンドかWebベースのGUIを使用して行えます。この章では、CLIコマンドによる設定方法を説明します。WebベースのGUIを使用する場合は、Web ブラウザでストレージ　ルータの管理インタフェースのIPアドレスを指定し、ログイン後、［Help］をクリックしてGUIのオンライン ヘルプを参照してください。

事前に必要な作業

高可用性クラスタの設定作業に入る前に、第5章「ストレージ ルータの設定」または第6章「システム パラメータの設定」を参照して、HAインタフェースの設定を含む、すべてのシステム パラメータの設定を済ませておいてください。

高可用性クラスタ環境で使用するSCSIルーティング インスタンスを設定する場合は、以下のガイドラインに従ってください。

- WWPNを使用してターゲットをマップする場合は、必ずプライマリWWPN（クラスタ内のプライマリストレージ ルータが認識するストレージ リソースに対応付けられたWWPN）とセカンダリWWPN（クラスタ内のセカンダリストレージ ルータが認識するストレージ リソースに対応づけられたWWPN）の両方を指定してください。
- SCSIルーティング インスタンスの自動フェールオーバは、ギガビット イーサネット インタフェースが利用できない場合、またはマップされたターゲットのいずれもが利用できない場合に行われます。一部のターゲットが利用できない場合でも、利用可能なターゲットが存在すれば、そのSCSIルーティング インスタンスで自動フェールオーバは行われません。SCSIルーティング インスタンスを実行するストレージ ルータが高可用性クラスタ内でハートビートを交換できない場合は、すべてのSCSIルーティング インスタンスのフェールオーバが行われます。

  ターゲットが利用不可能になったときに自動フェールオーバが最大限行われるようにするには、1つのSCSIルーティング インスタンスに対応付けられたターゲットを、1つのファイバ チャネル インタフェース経由で利用可能なストレージにマップしてください。複数のファイバ チャネ ルインタフェース経由で利用可能なストレージには、1つのSCSIルーティング インスタンスに対応づけられたターゲットはマップしないでください。

  このようにマッピングすることによって、利用可能なターゲットと利用不可能なターゲットが混在して存在する可能性を最小限に抑えることができます。利用可能なターゲットが混在している状態では、IP ホストからアクセスできないストレージが存在するにもかかわらず、SCSIルーティング インスタンスの自動フェールオーバが行われません。

クラスタへのストレージ ルータの追加

通常は、基本的に使用する一方のストレージ ルータを、（クラスタ レベルで共有されるすべての設定を含め）完全に設定してから、もう一方の未設定のストレージ ルータ、または最小限設定のストレージ ルータをクラスタに追加します。高可用性クラスタは、2台のストレージ ルータで構成します。

ストレージ ルータの以下の設定は、クラスタ全体で共有されます。これらの設定は、クラスタ内の最初のストレージ ルータに設定しておくと、クラスタに追加したもう一方のストレージ ルータにも適用されます

- アクセス リスト
- クラスタ名
- SCSIルーティング インスタンス
- VLAN情報（VID、VTPモード、ドメイン名など）

注記: **「最小限設定のストレージ ルータ」とは、管理インタフェースのIPアドレス、システム名、および必要に応じてネットワーク管理インタフェースを設定したストレージ ルータのことです。最小限設定のストレージ ルータには、これ以外に、HAインタフェースのIPアドレス、Administrator / Monitorモードのパスワードなどのシステム情報を設定しておいてもかまいませんが、クラスタ全体で共有される設定項目は設定しないでください。**

未設定のストレージ ルータの追加

以下の手順に従って、新しい未設定のストレージ ルータを既存のクラスタに追加します。

1. ストレージ ルータの初期システム コンフィギュレーション スクリプトのプロンプトで、次の項目を設定します。
   - 管理インタフェースのIPアドレス
   - システム名
   - HA構成モード
   - クラスタ名
   - HAインタフェースのIPアドレス

   HA設定モードを選択するプロンプトでは、［clusterd］を選択します。クラスタ名を指定するプロンプトでは、既存のクラスタの名前を入力します。初期システム設定スクリプトが終了すると、ストレージ ルータが自動的に再起動します。
2. ストレージ ルータは再起動時に、クラスタ内のもう一方のストレージ ルータと通信し、現在のクラスタ設定情報を取得します。ストレージ ルータの再起動が完了したら、新しいクラスタ設定を確認してください。`show cluster`コマンドを実行して、クラスタ名を確認し、ストレージ ルータがクラスタ内のもう一方のストレージ ルータとハートビートを交換していることを確認します。

3. 両方のストレージ ルータに同じ設定が適用されていることを確認します。まず、クラスタ内に元からあったストレージ ルータで、次のコマンドを実行します。
   - `show accesslist all from bootconfig`
   - `show scsirouter all from bootconfig`
   - `show vlan`
   - `show vtp`

   次に、クラスタに追加したストレージ ルータで同じコマンドを実行し、同じ情報が表示されることを確認します。
4. セットアップ コンフィギュレーション ウィザード、CLIコマンド、またはGUIを使用して、ストレージ ルータの設定を完了します。詳しくは、第5章「ストレージ ルータの設定」または第6章 「システム パラメータの設定」を参照してください。
5. **bootconfig**キーワードとともに`save`コマンドを実行して、設定の変更を保存します。このコマンドによって、ストレージ ルータの起動設定が更新され、クラスタ内のすべてのストレージ ルータに設定の変更が通知されます。（オプション）
6. クラスタ内のストレージ ルータ間で負荷を分散させるために、`failover scsirouter`コマンドを使用して、指定したSCSIルーティング インスタンスを手動でフェールオーバできます。SCSIルーティング インスタンスのフェールオーバについて詳しくは、第11章「ストレージ ルータのメンテナンスと管理」の「クラスタ構成でのSCSIルーティング インスタンスの制御」を参照してください。（オプション）

最小限設定のストレージ ルータの設定

以下の手順に従って、最小限設定のストレージ ルータを既存のクラスタに追加します。

1. セットアップ クラスタ ウィザードを実行します。
   - HA設定モードを選択するプロンプトでは、［clusterd］を選択します。
   - クラスタ名を指定するプロンプトでは、既存のクラスタの名前を入力します。
   - scsirouterインスタンスを維持（retain）するか削除（delete）するかを指定するプロンプトでは、［delete］を指定します。［delete］を指定すると、このストレージ ルータの既存のSCSIルーティング インスタンスが削除されます。
   - 変更内容を確認するメッセージが表示されたら、「yes」と入力します。ストレージ ルータが自動的に再起動します。
2. ストレージ ルータは再起動時に、クラスタ内のもう一方のストレージ ルータと通信し、現在のクラスタ設定情報を取得します。ストレージ ルータの再起動が完了したら、新しいクラスタ設定を確認してください。`show cluster`コマンドを実行して、クラスタ名を確認し、ストレージ ルータがクラスタ内のもう一方のストレージ ルータとハートビートを交換していることを確認します。

3. 両方のストレージ ルータに同じ設定が適用されていることを確認します。まず、クラスタ内に元からあったストレージ ルータで、以下のコマンドを実行します。
   - `show accesslist all from bootconfig`
   - `show scsirouter all from bootconfig`
   - `show vlan`
   - `show vtp`

   次に、クラスタに追加したストレージ ルータで同じコマンドを実行し、同じ情報が表示されることを確認します。
4. 必要に応じて、追加したストレージ ルータのその他の設定を行います。たとえば、次の設定を行います。
   - セットアップ アクセス コンフィギュレーション ウィザードを使用して、ストレージ ルータのパスワードを設定します。
   - セットアップ マネジメント コンフィギュレーション ウィザードを使用して、SNMP経由のネットワーク管理機能を設定します。
   - セットアップ タイム コンフィギュレーション ウィザードを使用して、ストレージ ルータの日時、およびNTPサーバを使用する場合はその情報を設定します。
   - CLIまたはGUIを使用して、AAA認証機能を設定します。詳しくは第9章「認証の設定」を参照してください。
5. **bootconfig**キーワードとともに`save`コマンドを実行して、設定の変更を保存します。このコマンドによって、ストレージ ルータの起動設定が更新され、クラスタ内のすべてのストレージ ルータに設定の変更が通知されます。
6. クラスタ内のストレージ ルータ間で負荷を分散させるために、`failover scsirouter`コマンドを使用して、指定したSCSIルーティング インスタンスを手動でフェールオーバできます。SCSIルーティング インスタンスのフェールオーバについて詳しくは、第11章 「ストレージ ルータのメンテナンスと管理」の「クラスタ構成でのSCSIルーティング インスタンスの制御」を参照してください。（オプション）

設定済みのストレージ ルータの追加

場合によっては、すでにスタンドアロン システムとして（SCSIルーティング インスタンスやアクセス リストなどを）設定済みのストレージ ルータ 2台から、クラスタを構成したいことがあります。

以下の例では、*StorageRouterSys1*と*StorageRouterSys2*という2つのStorageRouterから、*Cluster1*というクラスタを構成する手順を説明します。これらの2台のストレージ ルータでは、すでにSCSIルーティング インスタンスとアクセス リストが適切に設定されているとします（これらの設定について詳しくは、第8章「SCSIルーティングの設定」を参照してください）。必要に応じて、`scsirouter primary`コマンドを使用して、優先的に使用するストレージ ルータに、一部またはすべてのSCSIルーティング インスタンスを割り当てておいてください。

注記: **1つのクラスタにつき最大12個のSCSIルーティング インスタンスをアクティブにできます。**

以下の手順に従って、設定済みのストレージ ルータからクラスタを構成します。

1. セットアップ クラスタ コンフィギュレーション ウィザードを使用して、*StorageRouterSys1*を*Cluster1*のメンバーとして定義します。アクセス リストおよびSCSIルーティング インスタンスの既存の設定を維持するかどうか指定するプロンプトでは、［retain］を指定します。
2. *StorageRouterSys1*の再起動後、`show cluster`コマンドを実行してクラスタ名を確認します。また、`show scsirouter`コマンドおよび`show accesslist`コマンドを実行して、SCSIルーティング インスタンスとアクセス リストの設定が維持されていることを確認します。
3. *StorageRouterSys2*上で`save accesslist`コマンドを実行して、クラスタで使用するアクセス リスト情報をファイルに保存します。（オプション）

   たとえば、すべてのアクセス リストを*StorageRouterSys2_AccessLists.xml*というファイルに保存するには、次のコマンドを実行します。

   ```
   save accesslist all SR2122Sys2_AccessLists.xml
   ```

4. アクセス リストはクラスタ内の最初のストレージ ルータでのみ操作可能なので、*StorageRouterSys2*で保存した設定ファイルを*StorageRouterSys1*で利用できるようにする必要があります。この作業は、`copy savedconfig`コマンドまたは`FTP`を使用して行うことができます。ストレージ ルータの保存済み設定ファイルの管理について詳しくは、第11章 「ストレージ ルータのメンテナンスと管理」を参照してください。
5. セットアップ クラスタ コンフィギュレーション ウィザードを使用して、*StorageRouterSys2*を新しいクラスタ*Cluster1*に追加します。SCSIルーティング インスタンスの既存の設定をクラスタ内で維持するかどうか指定するプロンプトでは、［retain］を指定します。
6. *StorageRouterSys2*の再起動後、`show cluster`コマンドを実行してクラスタ名を確認します。また、`show scsirouter`コマンドを実行して、SCSIルーティング インスタンスの設定が維持されていることを確認します。
7. `restore accesslist from`コマンドを使用して、手順3で保存したアクセス リストを復元します。アクセス リストはクラスタ内の最初のストレージ ルータでのみ操作可能なので、このコマンドは*StorageRouterSys1*で実行する必要があります。（オプション）
8. `save all bootconfig`コマンドを実行して、*StorageRouterSys1*上の設定情報を保存します。このコマンドによって、クラスタ内のすべてのストレージ ルータの起動設定が更新されます。（オプション）
9. 各ストレージ ルータ上で`show scsirouter stats`コマンドを実行して、すべてのSCSIルーティング インスタンスがアクティブになっていることを確認します。

クラスタの変更

場合によっては、あるクラスタから他のクラスタにストレージ ルータを移動したいことがあります。単にストレージ ルータをクラスタに追加する場合に比べ、設定済みのストレージ ルータを他のクラスタに移動する場合は設定手順が複雑になり、高度なプランニングが必要とされます。

以下の手順に従って、ストレージ ルータをあるクラスタから他のクラスタに移動します。

1. 移動するストレージ　ルータのハードウェア構成が、移動先クラスタ内の他方のストレージ ルータと同じであることを確認します。クラスタ内の各ストレージ ルータは、同じIPホストおよびファイバ チャネル ストレージに接続可能である必要があります。クラスタ内のストレージ ルータの管理インタフェースにはすべて、同一IPサブネット上のIPアドレスを割り当てる必要があります。また、クラスタ内の各ストレージ ルータのHAインタフェースにはすべて、同一IPサブネット上のIPアドレスを割り当てる必要があります。ただし、管理インタフェースとHAインタフェースは、異なるIPネットワーク上にある必要があります。
2. 移動するストレージ ルータ上の設定済みSCSIルーティング インスタンスを維持する必要があるかどうかを判断します。設定済みデータを維持すると、そのストレージ ルータ上のすべてのSCSIルーティング インスタンスが、移動先クラスタの定義済みインスタンスに追加されます。既存のインスタンスを維持しない場合は、それらを削除します。
3. 設定済みデータを維持する場合は、SCSIルーティング インスタンス名に重複がないかどうかを調べます。重複がある場合、ストレージ ルータをクラスタに追加すると、ストレージ ルータの設定済みデータは、クラスタのデータで上書きされます。このような場合は、必要に応じてストレージ ルータの設定を変更してから、クラスタに追加してください。
4. また、設定済みデータを維持する場合は、既存のアクセス リスト情報を保存しておく必要があるかどうかも判断します。他のクラスタにストレージ　ルータを移動する場合、ストレージ ルータのアクセス リストは維持されず、新しいクラスタに追加された時点で破棄されます。既存のアクセス リスト情報を保存しておけば、新しいクラスタでそれを復元することができます。アクセス リスト情報を復元するには、保存済みの設定ファイルをクラスタ内の最初のストレージ ルータに転送してから、restoreコマンドを実行します。この作業は、ストレージ ルータをクラスタに追加する前でも後でも行えます。
5. セットアップ クラスタ コンフィギュレーション ウィザードを使用して、新しいクラスタにストレージ ルータを追加します。必要に応じて、表示されるプロンプトで、設定を維持するか削除するかを指定します。セットアップ クラスタ コンフィギュレーション ウィザードが終了すると、ストレージ ルータが自動的に再起動します。
6. 必要に応じて、その他の設定を行います。たとえば、クラスタ内のストレージ ルータ間で負荷を分散するために、新しく追加したストレージ　ルータにSCSIルーティング インスタンスがフェールオーバされるように設定できます。
7. **bootconfig**キーワードとともに`save all`コマンドを実行してストレージ　ルータの設定のコピーと保存を行い、クラスタを更新します

ストレージ ルータのメンテナンスと管理

11

この章では、ストレージ　ルータの標準的なメンテナンスと管理の作業について説明します。説明する内容は以下のとおりです。

ストレージ ルータのメンテナンスと管理の作業は、CLIコマンドかWebベースのGUIを使用して行えます。この章では、CLIコマンドによる設定方法を説明します。WebベースのGUIを使用する場合は、Webブラウザでストレージ ルータの管理インタフェースのIPアドレスを指定し、ログイン後、［Help］をクリックしてGUIのオンライン ヘルプを参照してください。

注記: **この章で説明する作業がすべてのストレージ ルータで必要なわけではありません。たとえば、スタンドアロン システムとして使用しているストレージ ルータでは、高可用性クラスタ関連の作業（SCSIルーティング インスタンスのフェールオーバなど）は不要です。**

事前に必要な作業

ストレージ ルータのメンテナンス作業に入る前に、第5章 「ストレージ ルータの設定」または第6章 「システム パラメータの設定」を参照して、システム パラメータの設定を済ませておいてください。

注記: **ソフトウェアのダウンロード元の設定など一部の作業は、初期設定時には省略してもかまいません。これらの作業は、**CLI**や**GUI**を使用していつでも行うことができます。この章では、必要に応じてその都度、関連する作業とコマンドを説明します。**

アップデート ソフトウェアのインストール

このストレージ ルータは、多くのメンテナンス作業を行わなくても連続稼動できるように設計されています。ただし、必要に応じて定期的にソフトウェアをアップデートする必要があります。ストレージ ルータは、ローカル ファイル システム上に、ソフトウェア ファイルを（コンフィギュレーション ファイル、ログ ファイル、その他の情報とともに）格納しています。このファイルシステムは、内蔵の不揮発性フラッシュ ディスクに格納されています。`show software version all`コマンドを実行すると、ストレージ ルータに格納されているすべてのソフトウェア バージョンのリスト、およびソフトウェアの追加に利用可能なディスク容量が表示されます。

登録ユーザーは、http://www.hp.comでストレージ ルータのアップデート ソフトウェアを入手できます。アップデート ソフトウェアは、HP.comから、標準のHTTPまたはプロキシ経由のHTTPを使用してストレージ ルータに直接ダウンロードできます。また、標準的なWebブラウザを使用して、http://www.hp.comから、アップデート ソフトウェアおよび付随するreadmeファイルを指定した場所にダウンロードすることもできます。ダウンロード後、CLIまたはWebベースのGUIを使用して、この場所（「ダウンロード場所」と呼ばれます）から、HTTP、プロキシ経由のHTTP、またはTFTP（Trivial File Transport Protocol）経由で、ストレージ ルータがアップデート ソフトウェアを利用できるようにします。

注記: **ストレージ ルータでアップデート ソフトウェアを使用する前に、必ず**readme**ファイルに目を通しておいてください。**

CLIの`download software http`コマンドまたは`download software proxy`コマンドを使用してストレージ ルータでアップデート ソフトウェアを利用可能にする場合、ダウンロード場所となるマシンでは Web サーバが稼動している必要があります。CLI の`download software tftp`コマンドを使用する場合、ダウンロード場所となるマシンはTFTP（Trivial File Transport Protocol）経由でアクセス可能である必要があります。ダウンロード場所のマシンでWebサーバが稼働していない場合や、ダウンロード場所のマシンにTFTP経由でアクセスできない場合は、ストレージ ルータのWebベースGUIを使用して、ストレージ ルータでアップデート ソフトウェアを利用可能にする必要があります（詳しくはオンライン ヘルプを参照してください）。

アップデート ソフトウェアの取得に使用するダウンロード場所は、`software http url`コマンド、`software proxy url`コマンド、または`software tftp`コマンドを使用して設定します。現在指定されているダウンロード場所を確認するには、`show software version all`コマンドを実行します（例12）。`show software version all`コマンドを実行すると、HTTPのURL、プロキシのURL、TFTPのホスト名などダウンロード場所の識別に使用される情報、ストレージ ルータで稼働中のソフトウェアのバージョン、およびシステム再起動後に使用されるようになるソフトウェアのバージョンが表示されます。以下の例では、デフォルトのダウンロード場所、および関連するユーザー名とパスワードが設定されています。

注記: HP.com**の登録ユーザーの方は、**Microsoft Windows 95**、**98**、**NT**対応の**TFTP**サーバ ツールを、**HP.com**の**Service & Support **(**http: / / www.hp.com / support**) にある**Software Center**からダウンロードできます。**

例 12: show software version all コマンドの実行結果

```
[SR2122_A01]# show software version all
Version    Boot  Hash  Sign  Crash  Size     Date
---------  ----  ----  ----  -----  -----    ----------
2.3.0.49   OK    OK    N/A   0      18585600 Mar 21 18:08 CST 2002
2.3.1      OK    OK    N/A   0      18616320 Mar 22 16:35 CST 2002

Http Url: http://www.HP.com
Http Username: SWAdmin01
Http Password: *********

Proxy Address: 10.1.12.32
Proxy Port: 3122
Proxy Url: http://www.hp.com
Proxy Username: SWAdmin01
Proxy Password: *********

Tftp Hostname: 10.1.1.122
Tftp Directory: SR2122/v2.3/

Disk Space Available: 13357.0 KB
Current Version: 2.3.1
Boot Version: 2.3.1
```

以下の手順に従って、ストレージ ルータのソフトウェアをアップデートします。

1. ストレージ ルータのアップデート ソフトウェアの取得場所（http: / / www.hp.comまたは指定したその他のダウンロード場所）を指定します。（オプション）
2. 指定したバージョンのソフトウェアを、ストレージ ルータのローカル ファイル システム上で利用できるようにします。
3. 新しいバージョンを次回のシステム再起動時に起動するバージョンとして設定し、ストレージ ルータを再起動します。（オプション）

アップデート ソフトウェアの取得場所の指定

アップデート ソフトウェアの取得場所を指定する必要があります。また、現在設定されているダウンロード場所が適切でない場合は、指定し直すことができます。以下の手順で、適切なダウンロード場所を指定します。

- HTTPを使用する場合（126ページ）
- プロキシ サーバを使用する場合（127ページ）
- TFTPを使用する場合（127ページ）

作業後、`show software version all`コマンドを実行して新しい設定を確認し、`save system bootconfig`コマンドまたは`save all bootconfig`コマンドを使用して設定を保存します。

HTTPを使用する場合

以下の手順に従って、HTTP経由のダウンロード場所を指定します。

1. `enable` — Administratorモードに入ります。
2. `show software version` ***`all`*** — 現在起動時に使用されるよう設定されているソフトウェアのバージョン、および現在設定されているダウンロード場所を表示します。必要なソフトウェア バージョンがまだ利用可能になっていないことを確認します。また、HTTP経由のダウンロード場所が正しく設定されているかどうかを確認します。
3. `software http url` ***`http://10.1.11.32/~software/SR2122`*** — 現在のダウンロード場所がアップデート ソフトウェアの標準的な取得元でない場合、ダウンロード場所を設定し直します。この例では、ダウンロード場所を**http://10.1.11.32/~software/SR2122**に設定しています。（オプション）
4. `software http username` ***`webadmin`*** `password` ***`webword`*** — 指定した場所にアクセスするために必要なユーザー名とパスワードを指定します。この例では、ユーザー名**webadmin**、パスワード**webword**を指定しています。ユーザー名とパスワードが不要な場合は、キーワード**none**を指定します（たとえば、`software http username none`を実行します）。（オプション）

注記: **デフォルトの**URL http: / / www.hp.com**を使用する場合は、**hp.com**のログイン**ID**とパスワードを指定します。**

プロキシ サーバを使用する場合

以下の手順に従って、プロキシ サーバ経由のダウンロード場所を指定します。

1. `enable` — Administratorモードに入ります。
2. `show software version all` — 現在起動時に使用されるよう設定されているソフトウェアのバージョン、および現在設定されているダウンロード場所を表示します。必要なソフトウェア バージョンがまだ利用可能になっていないことを確認します。また、プロキシ経由HTTPのダウンロード場所が正しく設定されているかどうかを確認します。
3. `software proxy url default` — 現在のダウンロード場所がアップデート ソフトウェアの標準的な取得元でない場合、ダウンロード場所を設定し直します。この例では、ダウンロード場所を**default**（http://www.hp.com）に設定しています。（オプション）
4. `software proxy address http://10.1.10.126 port 32` — 手順3で指定したプロキシ サーバのアドレスとポート番号を指定します（この例では、**http://10.1.10.126**および ポート番号**32**を指定しています）。（オプション）
5. `software proxy username HPuser password HPpswd` — 指定した場所にアクセスするために必要なユーザー名とパスワードを指定します。この例では、ユーザー名**HPuser**、パスワード**HPpswd**を指定しています。ユーザー名とパスワードが不要な場合は、キーワードnoneを指定します（たとえば、`software proxy username none`を実行します）。（オプション）

注記: **デフォルトの**URL http://www.hp.com**を使用する場合は、**hp.com**のログイン**ID**とパスワードを指定します。**

TFTPを使用する場合

以下の手順に従って、TFTP経由のダウンロード場所を指定します。

1. `enable` — Administratorモードに入ります。
2. `show software version all` — 現在起動時に使用されるよう設定されているソフトウェアのバージョン、および現在設定されているダウンロード場所を表示します。必要なソフトウェア バージョンがまだ利用可能になっていないことを確認します。また、TFTP経由のダウンロード場所が正しく設定されているかどうかを確認します。
3. `software tftp hostname TFTPHost1 directory /tftpboot` — 現在設定されているホスト名とベース ディレクトリがアップデート ソフトウェアの標準的な取得元でない場合、必要に応じてホスト名とベース ディレクトリ（省略可能）を設定し直します。この例では、ホスト名を**TFTPHost1default**、ベース ディレクトリを`/tftpboot`に設定しています。なお、ストレージ ルータでDNSが設定されていない場合は、TFTPホストのIPアドレスを指定します。

アップデート ソフトウェアのダウンロード

ストレージ ルータで新バージョンのソフトウェアを利用可能にするには、`download software`コマンドを実行します。ストレージ ルータには2つのソフトウェア バージョンを格納できます。アップデート ソフトウェアをダウンロードする前に、現在1つのソフトウェア バージョンだけがストレージ ルータに格納されていることを確認してください。

以下の手順に従って、新バージョンのソフトウェアをストレージ ルータで利用できるようにします。

- HTTPを使用する場合（128ページ）
- プロキシ サーバを使用する場合（128ページ）
- TFTPを使用する場合（129ページ）

HTTPを使用する場合

HTTPを使用してストレージ ルータで新バージョンのソフトウェアを利用可能にするには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show software version` *`all`* — ストレージ ルータ上に現在1つのソフトウェア バージョンだけが格納されていることを確認します。2 つのバージョンが格納されている場合は、`delete software version` コマンドを実行して古いほうのバージョンを削除し、新バージョン用のスペースを確保します。
3. `download software http version` *`2.3.1`* — ストレージ ルータに新バージョン（この例では**2.3.1**）のソフトウェアをダウンロードします。

注記: **HPテクニカル サポートから指示があった場合など、特別なソフトウェアをストレージ ルータにダウンロードすることが必要になることもあります。標準のアップデート ソフトウェアとは別の（デフォルトのダウンロード場所以外の）場所に特別なソフトウェアを格納する場合は、デフォルトのダウンロード場所をいったん変更し、ソフトウェアのダウンロード後にデフォルトのダウンロード場所を元に戻します。または、より簡単な方法として、**`download software http`**コマンドの** URL**パラメータを使用する方法もあります。たとえば、**
`http://your.website.com/StorageRouter`**から、バージョン**2.3.1**のソフトウェア ファイル**
231.tar**をダウンロードするには、次のコマンドを実行します。**
```
download software http url http://your.website.com/
StorageRouter/231.tar.
```

プロキシ サーバを使用する場合

プロキシ サーバを使用してストレージ ルータで新バージョンのソフトウェアを利用可能にするには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。

2. `show software version all` — ストレージ ルータ上に現在1つのソフトウェア バージョンだけが格納されていることを確認します。2つのバージョンが格納されている場合は、`delete software version`コマンドを実行して古いほうのバージョンを削除し、新バージョン用のスペースを確保します。
3. `download software proxy version 2.3.1` — ストレージ ルータに新バージョン（この例では**2.3.1**）のソフトウェアをダウンロードします。

注記: **HPテクニカル サポートから指示があった場合など、特別なソフトウェアをストレージ ルータにダウンロードすることが必要になることもあります。標準のアップデート ソフトウェアとは別の（デフォルトのダウンロード場所以外の）場所に特別なソフトウェアを格納する場合は、デフォルトのダウンロード場所をいったん変更し、ソフトウェアのダウンロード後にデフォルトのダウンロード場所を元に戻します。または、より簡単な方法として、**`download software proxy`**コマンドの** URL**パラメータを使用する方法もあります。たとえば、**
`http://your.website.com/StorageRouter`**から、バージョン**2.3.1**のソフトウェア ファイル**
231.tar**をプロキシ サーバ経由でダウンロードするには、次のコマンドを実行します。**
`download software proxy url http://your.website.com/StorageRouter/231.tar`.

TFTPを使用する場合

TFTPを使用してストレージ ルータで新バージョンのソフトウェアを利用可能にするには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show software version all` — ストレージ ルータ上に現在1つのソフトウェア バージョンだけが格納されていることを確認します。2つのバージョンが格納されている場合は、`delete software version`コマンドを実行して古いほうのバージョンを削除し、新バージョン用のスペースを確保します。
3. `download software tftp version 2.3.1` — ストレージ ルータに新バージョン（この例では**2.3.1**）のソフトウェアをダウンロードします。

注記: **HPテクニカル サポートから指示があった場合など、特別なソフトウェアをストレージ ルータにダウンロードすることが必要になることもあります。標準のアップデート ソフトウェアとは別の（デフォルトのダウンロード場所以外の）場所に特別なソフトウェアを格納する場合は、デフォルトのダウンロード場所をいったん変更し、ソフトウェアのダウンロード後にデフォルトのダウンロード場所を元に戻します。または、より簡単な方法として、**`download software tftp`**コマンドのホスト名とファイル名のパラメータを使用する方法もあります。たとえば、**my_tftpHost**から、バージョン**2.3.1**のソフトウェア ファイル**231.tar**を**TFTP**でダウンロードするには、**
`download software tftp hostname my_tftp Host filename 231.tar`**を実行します。**231.tar**ファイルは、**TFTP**ホストのデフォルト ベース ディレクトリ内にある必要があります。**

アップデート ソフトウェアを起動バージョンに設定する

アップデート ソフトウェアをストレージ ルータにダウンロードしても、それだけでは稼働中のソフトウェア バージョンは変更されません。また、次回のシステム起動時に起動されるバージョンも自動的には設定されません。新バージョンのソフトウェアが起動されるようにするには、そのための作業を行う必要があります。

ソフトウェアを起動バージョンとして設定すると、ソフトウェアの整合性チェック、および指定したソフトウェアのバージョンが起動可能かどうかを確認する内部チェックが行われます。

以下の手順に従って、新しいソフトウェアを起動バージョンに設定します。

1. `enable` — Administratorモードに入ります。
2. `software version 2.3.1` — 次回のシステム起動時に起動するソフトウェアを指定します（この例では、**2.3.1**を指定しています）。システムによって、指定したソフトウェア バージョンの整合性チェックが行われ、起動可能かどうかが確認されます。
3. `show software version boot` — 正しいバージョンが起動バージョン（Boot Version）として表示されることを確認します。
4. `reboot` — 新しいソフトウェアを起動するために、ストレージ ルータを再起動します。（オプション）

新バージョンのソフトウェアを起動バージョンとして設定すると、内部チェックが行われ、新しいソフトウェアが実行可能かどうかが確認されます。

クラスタ環境に関する注意事項

クラスタ環境では、`software version`コマンドを実行すると、新しいソフトウェアが実行可能かどうかを確認する内部チェックの実行中に、通常のHA通信が一時的に中断されることがあります。この場合、HA通信の中断によって、ストレージ ルータ上でアクティブなSCSIルーティング インスタンスのフェールオーバが発生します。

プライマリ属性がストレージ ルータの名前に設定されているインスタンスは、再起動後ストレージ ルータで実行を再開します。ストレージ ルータをすぐに再起動しない場合は、`failover scsirouter`コマンドを実行して所定のSCSIルーティング インスタンスをストレージ ルータに戻します。

ストレージ ルータがクラスタ環境で稼動している場合、`reboot`コマンドが実行されると、ストレージ ルータは、クラスタ内の別のストレージ ルータにすべてのSCSIルーティング インスタンスをフェールオーバしようとします。iSCSIドライバは、該当するストレージ リソースへのユーザーの再接続を行い、これらのユーザーに対する再起動シーケンスの影響を最小限に抑えます。

システム コンフィギュレーションのバックアップ

ストレージ ルータのコンフィギュレーション情報は、XMLファイルにバックアップしておくことができます。このXMLファイルは、ローカル システムとリモート システムのどちらにも保存できます。問題が発生した場合、このファイルからAAA認証情報、SCSI ルーティング インスタンス、アクセス リスト、VLAN、およびストレージ ルータのその他のシステム コンフィギュレーション情報を復元できます。

`save`コマンドはCLIコマンド セッション中であればいつでも実行できますが、定期的にストレージ ルータのシステム コンフィギュレーションをファイルにバックアップしておくようにしてください。

コンフィギュレーション ファイルは、通常ストレージ ルータの`savedconfig`ディレクトリに格納されています。`copy`コマンドを使用して、TFTPが稼働しているサーバにコンフィギュレーション ファイルをコピーすれば、ストレージ ルータソフトウェアのバックアップを他のソフトウェア アーカイブと一緒に保管しておくことができます。また、リモート サーバからWebベースのGUIにアクセスすることによって、ストレージ ルータのバックアップ ファイルをそのサーバ上で直接作成することができます。詳しくは、GUIのオンライン ヘルプを参照してください。

ローカル バックアップの作成

XML形式のコンフィギュレーション ファイルは、ストレージ ルータのローカルの`savedconfig`ディレクトリに、直接バックアップすることができます。

すべてのSCSIルーティング インスタンスに関する現在のコンフィギュレーションを、ローカルの`savedconfig`ディレクトリのファイル*backup1*に保存するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `save scsirouter all` ***`backup1`*** — ファイル*backup1*に、設定済みのすべてのSCSIルーティング インスタンスを保存します。

リモートTFTPサーバへのバックアップ

*backup1*という名前のバックアップコンフィギュレーション ファイルを作成し、それをTFTPホストtserver1上のデフォルト ディレクトリ/tftpbootに*back1.xml*という名前で保存するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `save all backup1` — savedconfigディレクトリの*backup1*というファイルに、現在のコンフィギュレーションを保存します。
3. `copy savedconfig: backup1 tftp://tserver1/back1.xml` — 保存したコンフィギュレーション ファイル*backup1*を、TFTPサーバtserver1上のデフォルト ディレクトリにある*back1.xml*というファイルにコピーします。

注記: **このback1.xmlファイルは、デフォルト ディレクトリ内にすでに存在し、上書き可能に設定されている必要があります。**TFTP**では、新規ファイルは作成できません。**

バックアップからの復元

AAA認証情報、SCSIルーティング インスタンス、アクセス リスト、VLAN、および指定したシステム コンフィギュレーション データを、保存済みのコンフィギュレーション ファイルから復元することができます。restoreコマンドのfromキーワードを使用して、特定のSCSIルーティング インスタンスなど選択したデータのみを復元するのか、すべてのデータを復元するのかを指定できます。

コンフィギュレーションの復元に使用するファイルは、savedconfigディレクトリ（/ata3/savedconfig）に格納されている必要があります。ネットワーク上のその他の場所にあるバックアップ ファイルからコンフィギュレーション データを復元する場合は、copyコマンドを使用して、そのファイルをsavedconfigディレクトリにコピーしておいてください。

コンフィギュレーション データを復元すると、指定したファイルの一部またはすべての内容が実行用メモリにコピーされますが、ストレージ ルータで実行中のコンフィギュレーションに常に変更が反映されるとは限りません。たとえば、インスタンスが再起動されるまでは、from bootconfigキーワードを指定してshow scsirouterコマンドを実行しても、復元したSCSIルーティング インスタンスのコンフィギュレーションが完全には表示されないことがあります。

削除したSCSIルーティング インスタンスの復元

たとえば、SCSIルーティング インスタンス**scsi1**を誤って削除した場合に、ある場所に保管してあったコンフィギュレーション ファイルから**scsi1**を復元するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `copy` *`http://10.1.1.44/~s1/back1.xml`* `savedconfig:` *`scsi1_restore.xml`* — 指定したURL上のコンフィギュレーション ファイルを、*scsi1_restore.xml*という名前で`savedconfig`ディレクトリにコピーします。
3. `show savedconfig` — インポートファイルが`savedconfig`ディレクトリにあることを確認します。
4. `show scsirouter all from` *`scsi1_restore.xml`* — 指定したファイルから、SCSIルーティング インスタンス**scsi1**を復元します。
5. `show scsirouter` *`scsi1`* `from` *`bootconfig`* — 復元されたSCSIルーティング インスタンス**scsi1**を表示して、コンフィギュレーションが希望どおりであることを確認します。
6. `scsirouter` *`scsi1`* `enable` — 復元されたSCSIルーティング インスタンスを起動し、ストレージ ルータの使用中のコンフィギュレーションを更新します。インスタンスが復元されて再起動した後、コンフィギュレーションを変更することもできます。
7. `save scsirouter` *`scsi1`* `bootconfig` — SCSIルーティング インスタンスのコンフィギュレーションを変更した場合は、そのSCSIルーティング インスタンスをストレージ ルータの起動コンフィギュレーションに保存します。（オプション）

既存のSCSIルーティング インスタンスの復元

ストレージ ルータで現在アクティブなSCSIルーティング インスタンスのコンフィギュレーションを復元する場合は、そのインスタンスをいったん停止し、指定したファイルからコンフィギュレーションを復元してから、インスタンスを再起動する必要があります。たとえば、ファイル*scsi2_backup*からSCSIルーティング インスタンス**scsi2**を復元するには、次の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show scsirouter` *`scsi2`* `stats` — SCSIルーティング インスタンスscsi2の現在のステータスを表示します。ステータスがアクティブの場合は、手順3の `no scsirouter enable`コマンドを実行してインスタンスを停止します。
3. `no scsirouter` *`scsi2`* `enable` — アクティブなSCSIルーティング インスタンスを無効にします。アクティブなインスタンスは復元できません。
4. `show savedconfig` — 必要なバックアップ ファイルが、`savedconfig`ディレクトリに格納されていることを確認します。
5. `show scsirouter` *`all`* `from` *`scsi2_backup`* — 復元するインスタンスがコンフィギュレーション ファイルに保存されていることを確認します。
6. `restore scsirouter` *`scsi2`* `from` *`scsi2_backup`* — SCSIルーティング インスタンスを復元します。
7. `show scsirouter` *`scsi2`* `from` *`bootconfig`* — SCSIルーティング インスタンスのコンフィギュレーションが正しく設定されたことを確認します。
8. `scsirouter` *`scsi2`* `enable` — SCSIルーティング インスタンスを再起動します。
9. `show scsirouter` *`scsi2`* — SCSIルーティング インスタンスのコンフィギュレーションを確認します。使用中のコンフィギュレーションと、復元したコンフィギュレーションが一致しているはずです。インスタンスが復元されて再起動した後、コンフィギュレーションを変更することもできます。
10. `save scsirouter` *`scsi2`* `bootconfig` — SCSIルーティング インスタンスのコンフィギュレーションを変更した場合は、そのSCSIルーティング インスタンスをストレージ ルータの起動コンフィギュレーションに保存します。

アクセス リストの復元

アクセス リストを復元しても、既存のエントリは削除されません。復元することによって、削除されたエントリが追加され、同名のエントリが上書きされますが、既存のエントリが削除されることはありません。必要に応じて、アクセス リスト全体を削除してから、保存しておいたコンフィギュレーション ファイルからアクセス リストを復元することもできます。

ファイル*accesslist_backup.xml*からアクセス リスト**mylist1**を復元するには、以下の手順に従います。この例では、使用中のコンフィギュレーション**mylist1**に以下のエントリが含まれているとします。

- 10.1.1.30/32
- 172.16.255.220/32
- chap-username 12h7b.lab2.webservices
- chap-username 12784.lab1.webservices

また、コンフィギュレーション ファイル*accesslist_backup.xml*に保存されているアクセス リストには、以下のエントリが含まれているとします。

- 209.165.200.225/32
- 10.1.1.30/32
- chap-username 12h7b.lab2.webservices
- chap-username test2.sys3

注記: クラスタ環境では、アクセス リストの管理は、特定の1つのストレージ ルータによって行われます。アクセス リスト管理を行っていないストレージ ルータで`access list`コマンドを実行すると、現在アクセス リスト管理を行っているストレージ ルータの名前が通知メッセージに表示されます。

---

1. `enable` — Administratorモードに入ります。
2. `show accesslist mylist1` — アクセス リスト**mylist1**に現在定義されているエントリを表示します。
3. `show accesslist mylist1 from accesslist_backup.xml` — コンフィギュレーション ファイル*accesslist_backup.xml*に保存されている、アクセス リストmylist1に対応するエントリを表示します。このコンフィギュレーション ファイルは、`savedconfig`ディレクトリに格納されている必要があります。
4. `restore accesslist mylist1 from accesslist backup.xml` — 保存してあったコンフィギュレーション ファイル*accesslist_backup.xml*から、mylist1のアクセス リスト エントリを復元します。
5. `show accesslist mylist1` — 復元されたアクセス リスト**mylist1**のエントリを表示します。以下のエントリが表示されます。
   - 10.1.1.30/32
   - 172.16.255.220/32
   - 209.165.200.225/32
   - chap-username 12h7b.lab2.webservices
   - chap-username 12784.lab1.webservices
   - chap-username test2.sys3
6. `save accesslist mylist1 bootconfig` — 復元前のエントリの中に保存されていないものがある場合は、`copy`コマンドを実行して現在のアクセス リストの設定をストレージ ルータの起動コンフィギュレーションに保存します。（オプション）

AAA認証情報の復元

AAA認証情報を復元すると、次のコンフィギュレーションが更新されます。

- AAA認証リスト
- ローカル ユーザー名データベース内のユーザー名とパスワード
- RADIUSサーバ、関連するサーバ、グローバル認証ポート、再送信、タイムアウト、および鍵の設定
- TACACS+サーバ、関連するサーバ、グローバル認証ポート、タイムアウト、および鍵の設定

保存してあったコンフィギュレーション ファイル*aaa_backup.xml*からAAA認証のコンフィギュレーションを復元するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show savedconfig` *`aaa_backup.xml`* — バックアップ ファイルの内容を表示し、復元しようとしているAAA認証コンフィギュレーションがこのバックアップ ファイルに含まれていることを確認します。このファイルは、`savedconfig`ディレクトリに格納されている必要があります。
3. `restore aaa from` *`aaa_backup.xml`* — 保存してあったコンフィギュレーション ファイル*aaa_backup.xml*から、AAA認証情報を復元します。
4. `show aaa` — AAA認証情報を表示し、正しく復元されたことを確認します。
5. `save aaa bootconfig` — 復元後にAAA認証コンフィグレーションを変更した場合は、変更後のコンフィギュレーションをストレージ ルータの起動用コンフィギュレーションに保存します。（オプション）

VLANの復元

VLANの復元は、一部のVLANに対して行うことも、すべてのVLANに対して行うこともできます。VLANを復元すると、VTPモードも復元されます。

以下の手順に従って、VLANを復元します。この例では、保存してあったコンフィギュレーション ファイル*VLAN_backup.xml*から、**TestLab**という名前のVLAN 10を復元しています。

注記: **クラスタ環境では、最初にクラスタに追加したストレージ ルータで、VLANを設定する必要があります。クラスタ内の別のストレージ ルータでVLANコマンドを実行すると、VLAN機能を現在実行しているストレージ ルータのシステム名とIPアドレスが通知メッセージに表示されます。**

---

1. `enable` — Administratorモードに入ります。
2. `show savedconfig` *`VLAN_backup.xml`* — 保存してあったコンフィギュレーション ファイル*VLAN_backup.xml*の内容を表示します。復元するVLANとVTPのコンフィギュレーションがファイルに格納されていることを確認します（例13）。
3. `restore vlan 10 from` *`VLAN_backup.xml`* — 保存してあったコンフィギュレーション ファイル*VLAN_backup.xml*からVLAN 10を復元します。
4. `show vlan` — VLANのコンフィギュレーションが正しく復元されたことを確認します。
5. `show vtp` — VTPのコンフィギュレーションが正しいことを確認します。
6. `save vlan` *`10`* `bootconfig` — 復元後にVLAN設定を変更した場合は、変更後のコンフィギュレーションをストレージ ルータの起動コンフィギュレーションに保存します。（オプション）

例 13: コンフィギュレーション ファイルに保存されている VLAN 情報の表示

```
!
! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode transparent
!
! VLAN
!
vlan 10 name TestLab mtusize 1500
```

システム コンフィギュレーションの復元

`restore system`コマンドを使用して、指定したシステム情報を復元することができます。復元可能な情報は以下のとおりです。

- 管理者の連絡先設定
- SNMPネットワーク管理のコンフィギュレーション
- NTPサーバ、日付、時刻、およびタイムゾーンの設定
- DNSのコンフィギュレーション
- リモートsyslogホストのIPアドレス
- ソフトウェアのデフォルトのダウンロード場所、および対応するユーザー名とパスワード
- CDPのコンフィギュレーション
- すべてのインタフェースのサービス設定の制限
- ストレージ ルータのルーティング テーブル
- ストレージ ルータのイベント メッセージ ログ テーブル
- すべてのファイバ チャネルインタフェースのコンフィギュレーション

以下の手順に従って、システム コンフィギュレーションを復元します。この例では、保存してあったコンフィギュレーション ファイル*system_backup.xml*から、SNMPネットワーク管理コンフィギュレーションおよび管理者の連絡先設定を復元しています。

1. `enable` — Administratorモードに入ります。
2. `show savedconfig` *`system_backup.xml`* — 保存してあったコンフィギュレーション ファイル*system_backup.xml*の内容を表示します。復元するSNMPネットワーク管理コンフィギュレーションおよび管理者の連絡先設定がファイルに格納されていることを確認します。
3. `restore system snmp from` *`system_backup.xml`* — SNMPネットワーク管理コンフィギュレーションを復元します。
4. `show snmp` — SNMPネットワーク管理情報が正しく復元されたことを確認します(例14)。
5. `restore system contactinfo from` *`system_backup.xml`* — 管理者の連絡先設定を復元します。
6. `show admin` — 管理者の連絡先設定が正しく復元されたことを確認します（例15)。
7. `save system bootconfig` — 復元後にSNMPコンフィギュレーションや管理者の連絡先を変更した場合は、変更後のコンフィギュレーションをストレージ ルータの起動コンフィギュレーションに保存します。(オプション)

例 14: SNMP コンフィギュレーションの確認

```
➔ [SR2122_PR1]# show snmp
  First Trap Host: 10.1.32.200
  Second Trap Host: 10.2.12.242
  Get Community String: public
  Set Community String: private
  Send Authentication Traps: enabled
  Link Up/Down Enable for mgmt: enabled
```

```
Link Up/Down Enable for fc1: enabled
Link Up/Down Enable for fc2: enabled
Link Up/Down Enable for fc3: enabled
Link Up/Down Enable for fc4: enabled
Link Up/Down Enable for fc5: enabled
Link Up/Down Enable for fc6: enabled
Link Up/Down Enable for fc7: enabled
Link Up/Down Enable for fc8: enabled
Link Up/Down Enable for ge1: enabled
Link Up/Down Enable for ge2: enabled
```

例 15: 管理者の連絡先設定の確認

```
[SR2122_PR1]# show admin
Administrator Contact Information
   Name: Pat Hurley
   Email: phurley@abc123z.com
   Phone: 123.456.7890
   Pager: 123.456.3444 pin 2234
```

ストレージ ルータの電源切断

ストレージ ルータの設置場所やケーブル配線を変更する場合は、ストレージ ルータの電源を切断する時間帯について、あらかじめ予定を立てておきます。ストレージ ルータの電源を切断するには、以下の手順に従ってください。この手順に従うと、シャットダウン前にファイル システムが適切な状態になります。

1. `enable` — Administratorモードに入ります。
2. `halt` — すべてのコンフィギュレーションを保存します。プロンプトに従って、必要な情報を保存してください。`[HALTED]#`コマンド プロンプトが表示されたら、ストレージ ルータの電源を安全に切断できます。

システムのリセット

ストレージ ルータの設定の一部またはすべてを、工場出荷時のデフォルト設定に戻すことが必要になることがあります。たとえば、システムをさまざまな環境間（テスト環境と本番環境など）で移動する場合や、トラブルシューティングを行う場合などです。

以下の手順に従って、ストレージ ルータの設定をリセットします。

1. 既存のコンフィギュレーションをファイルに保存します。（オプション）
2. `clear conf`コマンドを実行して現在のコンフィギュレーションを消去し、工場出荷時のデフォルト設定の一部またはすべてを復元します。

注記: クラスタ環境でストレージ ルータを使用している場合、ストレージ ルータ上で稼働しているSCSIルーティング インスタンスは、クラスタ内の別のストレージ ルータにフェールオーバされます。クラスタ環境で使用しているときに、SCSIルーティング インスタンスを別のストレージ ルータにフェールオーバさせたくない場合は、すべてのインスタンス（またはフェールオーバさせない特定のインスタンス）に対して`scsirouter enable`コマンドを実行してから、`clear conf`コマンドを実行します（これによって、それらのSCSIルーティング インスタンスはクラスタから永久に削除されます）。クラスタ環境でのストレージ ルータの操作について詳しくは、143ページの「クラスタ構成でのSCSIルーティング インスタンスの制御」を参照してください。

3. 初期コンフィギュレーション スクリプトを実行して、EIA/TIA-232コンソール接続経由の管理インタフェースを設定します。（オプション）
4. 特定のコンフィギュレーションを復元するか、CLIコマンドまたはWebベースのGUIを使用してストレージ ルータを再設定します。

全設定を工場出荷時のデフォルト設定にリセットする場合

現在のコンフィギュレーションを維持せずに、ストレージ ルータをまったく別の環境（システム設定が異なる環境）に物理的に移動する場合は、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `clear conf or clear conf all` *HP* — 現在のシステム コンフィギュレーションをすべて消去します。ネットワーク管理情報も消去されます。

   ストレージ ルータでSCSIルーティングを行っている場合は、**クリア コンフィギュレーション** ウィザードを使用できます。プロンプトにAdministratorモードのパスワードを入力します。「all」と入力して、システム コンフィギュレーションと管理ポート設定、および保存済みコンフィギュレーションとSCSIルーティング インスタンスをすべて消去します（例16）。または、Administratorモードのパスワード（**hp**など）を指定してCLIの`clear conf all`コマンドを実行しても、システム コンフィギュレーションと管理ポート設定を消去できます。

   どちらの場合も、コマンドの完了後にストレージ ルータが再起動します。

   例 16: ストレージ ルータのコンフィギュレーションのリセット

```
Enter admin password: *****

This process can restore factory default settings for the SR2122.
* Select "apps" to remove active applications and retain system
  configuration settings.
* Select "system" to remove active applications and system
  configuration settings.
* Select "saved" to remove all backup configurations from disk.
* Select "all" to remove active applications, system   configuration,
  and saved configurations.

The system configuration includes the management port, dns, admin and
monitor login, ntp, and snmp. You will need to use the console
```

```
to reconfigure the management port if you erase the system
configuration.

The system will reboot if you select "apps", "system", or "all".

Erase what? [apps/system/saved/all/cancel (cancel)]
```

注記: 移動後は、まずEIA / TIA-232コンソール接続を使用して、管理インタフェースのIPアドレスおよびその他の必要なシステム情報を設定します（詳しくは、「第5章 ストレージ ルータの設定」の「初期システム コンフィギュレーション スクリプト」を参照してください）。その後、セットアップ コンフィギュレーション ウィザード、その他のCLIコマンド、またはWebベースのGUIを使用して、ストレージ ルータを設定します。

システム設定を保持しながらリセットする場合

ストレージ ルータをテストに使用し、テスト後に現在のコンフィギュレーションを復元するというケースで、テスト時にはストレージ ルータのシステム コンフィギュレーションを変更しない場合は、以下の手順に従ってください。以下の手順に従うと、システム コンフィギュレーションおよび保存されたコンフィギュレーション ファイルが、システムのリセット後まで維持されます。

1. `enable` — Administratorモードに入ります。
2. `save all` ***`myfile`*** — すべてのコンフィギュレーションをファイル***myfile***に保存します。このファイルは、`savedconfig`ディレクトリに格納されます。
3. `clear conf` — 現在のコンフィギュレーションを消去します。ただし、システム情報（管理インタフェース、HAインタフェース、ログ テーブル、DNS、Administratorモードと Monitorモードのパスワード、NTPサーバ、SNMP情報など）および保存されたコンフィギュレーション ファイルは維持されます。

   プロンプトで、Administratorモードのパスワードを入力します。「apps」と入力してシステム コンフィギュレーションを維持します。

   ストレージ ルータが再起動します。

   必要なユーザー テストを実行します。テスト終了後、手順4に進み、元のコンフィギュレーションを復元します。
4. `restore all from` ***`myfile`*** — 元のコンフィギュレーションを復元します。このコンフィギュレーション ファイルは、`clear conf`コマンドの実行後も維持されています。
5. `reboot` — ストレージ ルータを再起動します。再起動後、元のアプリケーション コンフィギュレーションが実行用メモリに復元されます。

リセット時に保存済みコンフィギュレーションを削除する場合

スタンドアロンのストレージ ルータをクラスタに追加し、新しいクラスタ設定が適用されている場合は、以下の手順に従ってください。この手順では、スタンドアロンで使用していたときに保存したコンフィギュレーション ファイルは削除されますが、ストレージ ルータのシステム コンフィギュレーション、管理情報、およびSCSIルーティング インスタンスはそのまま維持されます。

1. `enable` — Administratorモードに入ります。
2. `clear conf` — `savedconfig`ディレクトリに保存されているコンフィギュレーション ファイルをすべて削除します。

   プロンプトでAdministratorモードのパスワードを入力します。「saved」と入力して、システム コンフィギュレーションを維持します。

   `savedconfig`ディレクトリからすべてのファイルが削除されますが、ストレージ ルータは再起動しません。
3. `show savedconfig` — `savedconfig`ディレクトリからすべてのファイルが削除されたことを確認します。

注記: `delete savedconfig`**コマンドを使用して、**`savedconfig`**ディレクトリから、指定した保存済みコンフィギュレーション ファイルを削除することもできます。**

パスワードの復旧

ストレージ ルータの管理インタフェースは、パスワードで保護されています。Telnet（CLIの場合）やWebベースのGUIを使用してストレージ ルータにアクセスするときは、パスワードを入力する必要があります。また、ストレージ ルータのコンソール インタフェースに対して、パスワード保護を有効にすることもできます。その場合は、管理インタフェースで設定したパスワードと同じAdministratorモードおよびMonitorモードのパスワードが、コンソール インタフェースに適用されます。

コンソール インタフェースでパスワードが有効になっているときにパスワードを忘れてしまった場合は、パスワード復旧の手順に従って、ストレージ ルータへの管理アクセスを復旧できます。パスワードの復旧を行う際は、ストレージ ルータのコンソールに物理的にアクセスする必要があります。詳しくは、http://www.hp.comを参照してください。

クラスタ構成でのSCSIルーティング インスタンスの制御

SCSIルーティング インスタンスがどこで稼働しているかを把握しておくことは、非常に重要です。自動フェールオーバ機能によって、システムに問題が発生した場合でもストレージ ルータ クラスタの動作は維持されますが、手動HA制御機能を使用すれば、独自のネットワーク要件を満たすように、クラスタ内のストレージ ルータ間でSCSIルーティング インスタンスを分散させることができます。

以下に、クラスタ環境でのSCSIルーティング インスタンスの制御に関する一般的な作業を示します。これらの作業の大半は頻繁には行いませんが、一部、定期的に行う作業（動作に関する統計情報の表示など）もあります。

インスタンスのコンフィギュレーションの変更

注記: クラスタ内のすべてのストレージ ルータに正しく変更が反映されるように、SCSIルーティング インスタンスの設定を変更するときは、必ず、そのインスタンスが現在アクティブになっているストレージ ルータで作業してください。

SCSIルーティング インスタンスのコンフィギュレーションは、随時、変更する必要が生じます。変更には、ターゲットの追加/削除、LUNの追加/削除、ターゲットの再マッピング、アクセスの変更などがあります。コンフィギュレーションを変更する際は、対応するストレージ リソースにアクセスする IP ホストに変更がどのように影響するかを把握しておくことが重要です。たとえば、インスタンスの設定を変更すると、IPホストに表示されるデバイスが変更され、その結果、ホストのオペレーティング システムがデバイスに割り当てる名前や番号が変更される可能性があります。ターゲットの追加/削除、特定ターゲット内のLUNの追加/削除、インスタンス全体の追加/削除など、インスタンスの特定のコンフィギュレーションを変更すると、ホストに表示されるデバイスの順序が変更される場合もあります。ホストに1つのSCSIルーティング インスタンスだけが対応付けられている場合でも、デバイスの順序の変更によって相違が生じる場合があります。

一般的に、IPホストのオペレーティング システムは、一定の条件に基づいて、受け取り順にドライブIDを割り当てます。たとえば、Linuxシステムは、ホスト、バス、ターゲット、およびLUN情報に基づいて、受け取り順にドライブIDを割り当てます。このため、ストレージの検出順序が変更されると、ドライブIDも変更される可能性があります。このような場合、ホスト上で稼動するアプリケーションがドライブに正しくアクセスできるように、アプリケーション設定を変更することが必要になることがあります。

SCSIルーティング インスタンス全体を削除した場合や、ホスト上に利用可能なターゲットがない場合は、ホストのiSCSIドライバのコンフィギュレーション ファイルを更新して、該当する参照を削除してからiSCSIドライバを再起動する必要があります。存在しないインスタンスや、そのホストで利用可能なターゲットのないインスタンスに対する参照がホストのiSCSIコンフィギュレーション ファイルに含まれている場合、iSCSIドライバはログインを実行せず、またSCSIルーティング インスタンスに対応付けられたターゲットを一切検出しません。

iSCSI ドライバのコンフィギュレーションの変更に関する詳細および推奨手順については、第5章の「iSCSI ドライバのインストール」、またはiSCSIドライバのreadmeファイルを参照してください。最新のiSCSIドライバおよびreadmeファイルは、http://www.hp.comから入手できます。

接続の有効化と無効化

デフォルトでは、SCSIルーティング インスタンスは、IPホストのギガビット イーサネット インタフェースと対応付けられた時点で有効になります。インスタンスに追加された個々のターゲットも、デフォルトで有効になります。ただし、アクセス リストをターゲットに対応付けられていないため、IPホストからそのターゲットに接続したりログインしたりすることはできません。アクセス リストがターゲットに対応付けられると、そのアクセス リストが自動的に有効になり、アクセス リスト内のエントリによって指定されたIPホストから、ターゲットに接続したりログインしたりできるようになります。

アクセス リストの対応付けを変更せずに、またはSCSIルーティング インスタンス全体を停止させずにターゲットへのアクセスを制御するには、`scsirouter target disabled`コマンドを実行します。このコマンドを実行した場合、既存の接続とログインは影響を受けませんが、以後の接続およびログインは禁止されます。

再び接続とログインを許可できるようになったら、`scsirouter target enabled`コマンドを実行します。

たとえば、アクセス リストwebserver2内のあるエントリに問題があるとします。また、このアクセス リストはターゲット**webstorage2**に対応付けられており、そのターゲットはSCSIルーティング インスタンス**foo**に対応付けられているとします。

問題のあるアクセス　リストと対応付けられたターゲットへのアクセスを一時的に禁止するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show scsirouter` *`foo`* `stats` — ステータスを表示し、SCSIルーティング インスタンスfooがこのストレージ ルータ上でアクティブになっていることを確認します。
3. `show scsirouter` *`foo`* — ターゲットの名前と現在のステータス、およびアクセス リストを確認します。この例では、ターゲット**webstorage2**はアクセス リスト**webserver2**に対応付けられ、ターゲットは有効になっています（例17）。
4. `scsirouter` *`foo`* `target` *`webstorage2`* `disabled` — ターゲットwebstorage2へのアクセスを無効にします（例18）。

例 17: ターゲット、アクセス リスト、ターゲット ステータスの確認

```
[SR2122_PR1]# show scsirouter foo
foo description “test SCSI routing instance”
foo authenticate “none”
foo primary "none"
foo proxy server disabled
foo failover primary “none”
foo failover secondary “none”
foo lun reset no
foo cdb retry counter 30
foo serverif ge2 10.1.0.45/24, TCP port:3260
foo target webstorage2 description “Web Storage”
foo target webstorage2 Name
“ign.1987-05.com.hp.00.0b1aaa415.....webstorage2”
➔ foo target webstorage2 enabled "TRUE"
➔ foo target webstorage2 accesslist "webserver2"
   foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

例 18: 新しいターゲット ステータスの確認

```
[SR2122_PR1]# show scsirouter foo
foo description “test SCSI routing instance”
foo authenticate “none”
foo primary "none"
foo proxy server disabled
foo failover primary “none”
foo failover secondary “none”
foo lun reset no
foo cdb retry counter 30
foo serverif ge2 10.1.0.45/24,TCP port:3260
foo target webstorage2 description “Web Storage”
foo target webstorage2 Name
“ign.1987-05.com.hp.00.0b1aaa415.....webstorage2”
➔ foo target webstorage2 enabled "FALSE"
   foo target webstorage2 accesslist "webserver2"
   foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

インスタンスの停止と起動

いくつかのIPホストやストレージ リソースで問題が発生した場合、クラスタ内で実行中の対応するSCSIルーティング インスタンスをすべて停止したいことがあります。このような場合、`no scsirouter enable`コマンドを使用すれば、クラスタ内の別のストレージ ルータへのフェールオーバは行わずに、指定したSCSIルーティング インスタンスを停止できます。このコマンドを使用すると、クラスタ内のどこで稼動している場合でも、指定したインスタンスを停止できます。

SCSIルーティング インスタンスが停止された場合、`scsirouter enable`コマンドにより再実行することができます。`scsirouter enable`コマンドは`no scsirouter enable`コマンドを実行した同じストレージ ルータから実行します。

このコマンドについて詳しくは、『コマンド ライン インタフェース リファレンス ガイド』を参照してください。

動作に関する統計情報の表示

show scsirouter statsコマンドを実行すると、SCSIルーティング インスタンスのステータスが表示され、アクティブな接続の数、ストレージ ルータが最後に再起動されてから（または最後に統計情報が消去されてから）発生したログインの数を確認できます。

たとえば例19のshow scsirouter statsの実行例は、SCSIルーティング インスタンス**foo**が現在アクティブであることを示しています。

例 19: show scsirouter stats の実行結果

```
[SR2122_PR1]# show scsirouter foo stats

router status    started           iSCSI ver (Min/Max) logins active
foo    ACTIVE    Jan 11 23:06:08         2/2           10     7
```

フェールオーバ処理

クラスタ環境では、ストレージ ルータは継続的にハートビートを交換し合い、クラスタ内の障害を検出します。HAメッセージはIP上のUDPを使用して送信され、メッセージ タイプや状況によってはユニキャスト メッセージまたはマルチキャスト メッセージとして送信されます。ストレージ ルータ間で確実にHA情報が交換されるように、ストレージ ルータは管理インタフェースとHAインタフェースの間で交互にハートビートを送信します。

SCSIルーティング インスタンスのフェールオーバは、クラスタ内の一方のストレージ ルータが、他方のストレージ ルータがハートビートに応答していないことを検出したときに、自動的に行われます。また、対応するギガビット イーサネット インタフェースが利用できない場合や、いずれのターゲットも利用できない場合も、SCSIルーティング インスタンスのフェールオーバが行われます。

注記: 一部のターゲットが利用できない場合でも、利用可能なターゲットがあれば、SCSIルーティング インスタンスのフェールオーバは行われません。

各クラスタでは最大12のアクティブなSCSIルーティング インスタンスがサポートされます。各ストレージ ルータでも最大12のSCSIルーティング インスタンスがサポートされるため、（ストレージ ルータ間でのインスタンスの振り分けとは無関係に）クラスタ内の各インスタンスの高可用性が保証されます。

手動フェールオーバ

SCSIルーティング インスタンスのフェールオーバは自動的に行われますが、一方のストレージ ルータから他方のストレージ ルータに手動でSCSIルーティング インスタンスを移動したい場合もあります。このような場合、インスタンスの移動は一時的に行うだけで、後で元のストレージ ルータにインスタンスを戻すこともあります。または、SCSIルーティング インスタンスを別のストレージ ルータに完全に移動し、可能なかぎりインスタンスが特定のストレージ ルータ上で動作を続けるようにする場合もあります。

以下のクラスタ環境の例では、**StorageRouterSys1**と**StorageRouterSys2**という2台のストレージ ルータでクラスタが構成されています。**StorageRouterSys1**はインスタンス**scsi1**と**scsi2**を実行中であり、両方のインスタンスのプライマリストレージ ルータになっています。**StorageRouterSys2**はインスタンス**scsi3**と**scsi4**を実行中であり、**scsi3**と**scsi4**のプライマリ属性は、デフォルト値の**none**に設定されています。つまり、どちらのインスタンスにも、フェールオーバ時に優先するストレージ ルータが設定されていません。

インスタンスを一時的に移動する場合

上に説明したクラスタ環境で、SCSIルーティング インスタンス**scsi1**をプライマリ（優先する）ストレージ ルータの**StorageRouterSys1**から**StorageRouterSys2**に一時的に移動するには、以下の手順に従います。この手順のコマンドは、**StorageRouterSys1**のCLIセッションで実行します。

1. `enable` — Administratorモードに入ります。
2. `show cluster or show scsirouter` *`scsi1`* `stats` — 移動するインスタンス**scsi1**が、実際に**StorageRouterSys1**上で稼働していることを確認します。
3. `failover scsirouter` *`scsi1`* — SCSIルーティング インスタンス**scsi1**をフェールオーバします。

注記: **クラスタ内にストレージ ルータは2台しかないので、フェールオーバ先の指定は不要です。**

---

4. `show cluster or show scsirouter` *`scsi1`* `stats` — 指定したSCSIルーティング インスタンス**scsi1**が、**StorageRouterSys1**上で稼働していないことを確認します。

フェールオーバの完了後、**StorageRouterSys2**にTelnet接続し、手順1および手順2のCLIコマンドを実行して、SCSIルーティング インスタンス**scsi1**が**StorageRouterSys2**上で稼働していることを確認します。

この場合、**StorageRouterSys1**がSCSIルーティング インスタンス**scsi1**のプライマリストレージ ルータに指定されたままなので、一時的な移動と見なされます。たとえば、**StorageRouterSys1**を再起動すると、**scsi1**は**StorageRouterSys2**での稼働を停止し、**StorageRouterSys1**で起動します。

注記: **プライマリストレージ ルータとして設定されていないストレージ ルータ上で稼働しているSCSIルーティング インスタンスのコンフィギュレーションを変更する場合は、注意が必要です。あるインスタンスのコンフィギュレーションを、そのインスタンスのプライマリストレージ ルータの非稼動中に（またはそのストレージ ルータがクラスタから削除された後に）変更した場合、そのプライマリストレージ ルータには変更が通知されません。このため、そのストレージ ルータは、再起動時（またはクラスタに戻されたとき）に、自身がプライマリストレージ ルータであると見なし、クラスタから離れる前の最後の設定に基づいて、そのインスタンスの実行を開始します。**

インスタンスを完全に移動する場合

上に説明したクラスタ環境で、SCSIルーティング インスタンス**scsi2**をプライマリ（優先する）ストレージ ルータの**StorageRouterSys1**から**StorageRouterSys2**に完全に移動するには、以下の手順に従います。この手順のコマンドは、**StorageRouterSys1**のCLIセッションで実行します。

1. `enable` — Administratorモードに入ります。
2. `show cluster or show scsirouter` *`scsi2`* `stats` — 移動するインスタンス**scsi2**が、実際に**StorageRouterSys1**上で稼働していることを確認します。
3. `scsirouter` *`scsi2`* `primary` *`StorageRouterSys2`* — **StorageRouterSys2**を、SCSIルーティング インスタンス**scsi2**のプライマリストレージ ルータに設定します。
4. `save scsirouter` *`scsi2`* `bootconfig` — SCSIルーティング インスタンスのプライマリ設定およびその他の設定を保存し、変更をクラスタ全体に通知します。
5. `failover scsirouter` *`scsi2`* — SCSIルーティング インスタンス**scsi2**をフェールオーバします。

フェールオーバの完了後、**StorageRouterSys2**にTelnet接続し、`show scsirouter scsi2`コマンドを実行して、SCSIルーティング インスタンス**scsi2**が**StorageRouterSys2**上で稼働していること、および**scsi2**のプライマリストレージ ルータが**StorageRouterSys2**に設定されていることを確認します。

インスタンスを分散させる場合

上に説明したクラスタ環境で、SCSIルーティング インスタンス**scsi4**のトラフィックが増加したことにより、他のインスタンス（**scsi1**、**scsi2**、**scsi3**）をすべて**StorageRouterSys1**上で実行して負荷を分散させるとします。**StorageRouterSys1**では、すでに**scsi1**と**scsi2**が稼働しているとします。

以下の手順では、SCSIルーティング インスタンス**scsi3**を**StorageRouterSys1**に移動します。この手順のコマンドは、**StorageRouterSys2**のCLIセッションで実行します。

1. `enable` — Administratorモードに入ります。
2. `show cluster or show scsirouter` *`scsi3`* `stats` — 移動するインスタンス**scsi3**が、実際に**StorageRouterSys2**上で稼働していることを確認します。
3. `failover scsirouter` *`scsi3`* `to` *`StorageRouterSys1`* — 指定したSCSIルーティン インスタンス**scsi3**を、**StorageRouterSys1**に移動します。

フェールオーバの完了後、**StorageRouterSys1**にTelnet接続し、`show scsirouter`コマンドを実行して、SCSIルーティング インスタンス**scsi1**、**scsi2**、**scsi3**が**StorageRouterSys1**上で稼働していることを確認します。

注記: **scsi3にはプライマリストレージ ルータが設定されていないため、StorageRouterSys1を明示的に停止/フェールオーバするか、またはインタフェースが利用不可能になるなどのソフトウェア/ハードウェア障害によりStorageRouterSys1が自動的にフェールオーバされない限り、StorageRouterSys1で稼動を続けます。**

ストレージ ルータのCDPの管理

CDP（Cisco Discovery Protocol）は、主に、隣接するデバイスのプロトコル アドレスの取得、およびそれらのデバイスのプラットフォーム検出に使用されます。CDPはメディアおよびプロトコルに非依存であり、ルータ、ブリッジ、アクセス サーバ、スイッチなどCisco製のあらゆる機器で利用できます。

CDP対応デバイスは、定期的に「advertisement」と呼ばれるメッセージをマルチキャスト アドレス宛てに送信します。各デバイスは、SNMPメッセージを受信可能なアドレスを、最低1つ通知します。通知には、TTL（Time-To-Live）、つまり受信側デバイスがCDP情報を破棄するまでの保持時間も含まれます。各デバイスは、他のデバイスから定期的に送信されるCDPメッセージを受信することによって、近隣デバイスの情報を取得し、それらのデバイスでメディアとのインタフェースがいつアップし、いつダウンしたかを判断します。

このストレージ ルータでは、デフォルトで、ネットワーク上の他のCDP対応デバイスとCDP情報を交換するよう設定されています。CDPは、ストレージ ルータのインタフェースごとに、有効または無効にすることができます。また、受信側デバイスでの保持時間、およびストレージ ルータからCDP情報を送信する頻度は、変更することができます。

個々のインタフェースのCDPの無効化

CDPは、ストレージ ルータの管理インタフェース、HAインタフェース、およびギガビット イーサネット インタフェースに対して、個々に有効または無効にすることができます。デフォルトでは、すべてのインタフェースでCDPが有効になっています。各インタフェースでCDPを無効にするには、次の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `no cdp interface` *`ge2`* `enable` — 指定したインタフェース**ge2**でCDPを無効にします。
3. `show cdp interface` — 指定したインタフェースでCDPが無効になったことを確認します。
4. `save system bootconfig` — ストレージ ルータの起動コンフィギュレーションにCDP設定の変更を保存します。（オプション）

CDPの保持時間とタイムアウト値の変更

保持時間とは、ストレージ ルータからCDPパケットを受信したデバイスが、そのパケットを破棄するまでの時間（秒数）です。CDP保持時間は、CDPタイマー値（ストレージ ルータがCDP情報を送信する間隔）より大きい値に設定する必要があります。たとえば、デフォルトでは、CDP保持時間は**180**秒、CDPタイマー値は**60**秒に設定されています。

CDP保持時間とCDPタイマー値を変更するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show cdp` — 現在のCDP設定を確認します。
3. `cdp holdtime` ***`300`*** — 受信側デバイスがストレージ ルータからのCDPパケットを保持する秒数を設定します（この例では**300**）。
4. `cdp timer` ***`120`*** — ストレージ ルータからのCDPパケットの送信間隔を秒数で設定します（この例では**120**）。
5. `show cdp` — CDPの新しいコンフィギュレーションを確認します。（オプション）
6. `save system bootconfig` — ストレージ ルータの起動コンフィギュレーションにCDP設定の変更を保存します。（オプション）

スクリプトによる作業の自動化

一連のCLIコマンドを頻繁に使用する場合は、それらのコマンドをスクリプトとして記述しておくと、時間を節約できます。コマンド スクリプトはCLIコマンドを記述したASCIIテキスト ファイルであり、`script`ディレクトリに格納されます。

コマンド スクリプトを作成するときは、以下のルールに従ってください。

- コマンドは、行内のどこから記述し始めてもかまいません。コメント文字が先頭に付けられていない限り、行内の最初の単語がコマンド文字列の先頭とみなされます。
- コメントを記述するには、行頭または行の任意の位置で、感嘆符（!）またはシャープ記号（#）を記述します。たとえば、ファイルの内容や想定される実行結果をコメントとして記述しておくことができます。また、コマンドの前にコメント文字を挿入することで、ファイルからコマンドの記述を削除せずに、そのコマンドが実行されないようにすることができます。
- 1 つのコマンドを複数行にわたって記述する場合は、行末に継続文字としてバックスラッシュ（\）を記述します（例20）。継続文字を使用することで、コマンドを複数行に分割して、読みやすく記述することができます。継続文字が記述されていない行までが、ひとつのコマンド シーケンスとみなされます。継続行の並びの後にコメント行を記述する場合は、コメント行の後に空行を追加する必要があります。

  例 20: 複数行にわたるコマンドの記述

  ```
  radius-server host 10.5.0.53 \
  auth-port 1644 \
  timeout 60 \
  retransmit 5
  ! Configure 1st RADIUS server

  radius-server host 10.6.0.61
  . . .
  ```

- スクリプトから他のスクリプトを呼び出すことができます。

スクリプトを実行すると、コマンドと応答がストレージ ルータのコンソールにエコー表示されます。

スクリプトは、好みのテキスト エディタを使用して、どのシステム上でも作成できます。作成したスクリプトは、FTPを使用して、ストレージ ルータの`script`ディレクトリ（`/ata3/script`）にコピーします。FTPの使用方法については、157ページの「ストレージ ルータでのFTPの利用」を参照してください。また、`copy`コマンドを使用して、HTTP経由やFTP経由でスクリプト ファイルをストレージ ルータにコピーすることもできます。

コマンド スクリプトの実行

スクリプト ファイルに記述されている一連のCLIコマンドを実行するには、以下の手順に従います。この例では、*CreateSc*というスクリプトファイルを実行しています。このファイルは`script`ディレクトリに格納されている必要があります。

1. `enable` — Administratorモードに入ります。
2. `show script` ***`CreateSc`*** — スクリプト**CreateSc**が`script`ディレクトリにあること、および再作成したいコンフィギュレーションがそのファイルに記述されていることを確認します。

3. `read script CreateSc` or `read script CreateSc force` — スクリプト ファイル内のCLIコマンドを読み取り、実行します。プロンプトが表示されたら、処理の続行を確認し、スクリプト コマンドを実行します。

   プロンプトを表示せずに直ちにスクリプトを実行するには、**force**キーワードを指定します。（オプション）

スクリプトの完了後、適切な`show`コマンドを実行し、スクリプトが希望どおりに実行されたかどうかを確認します。

ログ ファイルの管理

このストレージ ルータでは、ストレージ ルータ上のログ テーブルに設定されたルーティング ルールに基づいて、一連のログ ファイルにイベント情報を記録できます。デフォルトでは、通知レベルinfo以下のすべてのストレージ ルータ イベント メッセージがログ ファイルに記録されます。また、`show logging`コマンドを使用して、ログ ファイルのエントリを表示し、指定した文字列や正規表現にマッチするエントリを検索できます。

ログ ファイルは、ストレージ ルータの`log`ディレクトリ（`/ata4/log`）に作成され、最大4 MBのメモリを消費します。この限界に達すると、古いファイルから順に削除され、新しいファイルが作成されます。既存のログ ファイルのサイズを表示するには、`show logging size`コマンドを実行します。ログ ファイルに現在割り当てられているサイズと現在使用可能なログ ファイルのサイズを表示するには、`show system`コマンドを実行します。

ログ ファイルには、*messages*の後に番号を付けた名前が付けられます（*messages3*、*messages12*など）。最初のログ ファイルには*messages0*、次のログ ファイルには*messages1*というように、順次名前が付けられます。

ログ ファイルは、要件に応じて、リモート サーバにアーカイブとして保管したり、定期的に削除したりできます。ストレージ ルータからリモート サーバにファイルを転送するには、FTPを使用できます（詳しくは、157ページの「ストレージ ルータでのFTPの利用」を参照してください）。または、WebベースのGUIを使用してログ ファイルの内容を表示し、カット アンド ペースト機能を使用して、内容をローカル ファイルに保存することもできます。また、`show logging all`コマンドを実行し、特定のコンソール インタフェースのログ機能を使用して、コンソールの出力をリダイレクトすることもできます。

注記: **ストレージ ルータのログ テーブルへのルーティング ルールの追加について詳しくは、159ページの「ログについて」を参照してください**

ログ ファイルの削除

ストレージ ルータのログ ファイルを定期的に削除するには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show logging size` — ストレージ ルータのログ ファイルの現在のサイズを調べます（例21）。
3. `show logging all`または`show logging last` ***50*** — 現在のログ ファイル エントリをすべて表示します（1つ目のコマンド）。または、ファイルの末尾から、指定した数のエントリ（この例では**50**）を表示します（2つ目のコマンド）。
4. `clear log` — 既存のログ ファイルを削除します。既存のログ ファイルが削除され、新しいログ ファイルが作成されます。

例 21: show logging size コマンドの実行結果

```
[SR2122_PRA]# show logging size
5120 messages (342797 bytes) logged
```

トラブルシューティング時の情報収集

ストレージ ルータで問題が発生した場合は、トラブルシューティングに必要な情報を収集して、HPテクニカル サポートの担当者にご連絡ください。ストレージ ルータには、必要な情報を収集するためのさまざまな機能があります。

ストレージ ルータのトラブルシューティング時には、通常、以下の作業を行います。

- クラッシュ時のログの利用（156ページ）
- ストレージ ルータでのFTPの利用（157ページ）
- 診断機能について（159ページ）
- 起動時のシステム メッセージの収集（159ページ）
- ログについて（159ページ）
- ストレージ ルータのコンフィギュレーションのキャプチャ（163ページ）
- デバッグ機能の利用（163ページ）

クラッシュ時のログの利用

ストレージ ルータで予期しない問題が発生し、自動的に再起動した場合、特別なログ ファイルが作成されます。このログ ファイルは、*crash.txt*という名前で`log`ディレクトリ（`/ata4/log`）に格納されます。このログ ファイルの内容は、`show crash`コマンドを実行してコンソールに表示できます。

`show crash`コマンドの出力を保存するには、特定のコンソール インタフェースのログ機能を使用して、コンソールの出力をリダイレクトします。一部のコンソール インタフェースでは、スクロール バッファ サイズが十分な値に設定されていれば、コンソールの表示内容をASCIIテキスト ファイルにコピー アンド ペーストすることもできます。

クラッシュ時のログから、次の情報が得られます。

- 例外情報
- カーネル バージョン、作成日などの起動情報
- ソフトウェア情報
- すべてのタスクのリスト（エントリ ポイント、タスクID、各タスクの優先度を含む）
- タスク レジスタ、およびタスク リスト内の各タスクのスタック トレース
- ネット ジョブ リング
- すべてのモジュールのリスト （モジュールID、データ開始アドレスなどを含む）
- すべてのデバイスおよび対応するドライバのリスト
- すべてのドライバのリスト（作成、削除、オープン、クローズ、読み取り、書き込み、および入出力制御の実行回数を含む）
- 空きメモリ アドレスのリスト、およびメモリ使用率の概要
- 開いているファイル ディスクリプタのリスト
- ネットワーク インタフェースの情報（ストレージ ルータの全インタフェースに関する、フラグ、インタフェース タイプ、アドレス、MTU情報など）
- ストレージ ルータのルーティング テーブル
- ARPテーブル
- ストレージ ルータのホスト テーブル
- アクティブなインターネット接続の情報（PCB、接続タイプ（TCPまたはUDP）、受信/送信キュー、ローカル/外部アドレス、各接続の状態など）
- ルーティングの統計情報
- IPの統計情報
- ICMPの統計情報
- TCPの統計情報
- UDPの統計情報
- ネットワーク スタック データ プール（Mbuf）およびクラスタ プールのテーブル情報
- NFS認証

- マウント済みNFSファイル システムの情報
- IDEディスクまたはフラッシュ ディスクの情報（デバイス タイプ、パラメータなど）
- 登録済みクラッシュ ダンプ機能
- サンプルの登録済みダンプ機能
- 例外発生時のCPC710レジスタ

*crash.txt*ファイルの作成時に使用される情報は、`log`ディレクトリの*tmpcrash.txt*ファイルに定期的に書き込まれます。クラッシュ発生時に`show crash current`コマンドを実行すると、クラッシュ ログに書き込まれる情報が表示されます。

ストレージ ルータでのFTPの利用

ストレージ ルータのログ ファイルを解析のためにネットワーク上の別のサーバにコピーしたり、コンフィギュレーションファイルやスクリプトファイルを別のサーバにコピーし、他のストレージ ルータで利用できるようにしたい場合があります。ストレージ ルータにはFTPデーモンが組み込まれています。ただし、デフォルトでは、FTPポート（**port 21**）は制限状態（**restricted**）になっています。

FTPを有効にし、ストレージ ルータからネットワーク上の別のサーバに現在のメッセージ ログ ファイルをコピーするには、以下の手順に従います。

1. `enable` — Administratorモードに入ります。
2. `show restrict` — インタフェースの制限を表示します。管理インタフェース（**fei0**）のポート21が閉じられている場合は、手順3のコマンドを実行してそれを開きます。
3. `no restrict mgmt ftp` — 管理インタフェース上のFTP機能を使用可能にします。（オプション）

FTP機能を有効にした後、サーバからストレージ ルータへのFTPセッションを開始します。ユーザー名およびパスワードの入力を求められます。ユーザー名として*`admin`*、パスワードとしてストレージ ルータのAdministratorモードのパスワードを入力します。デフォルトのAdministratorパスワードは**hp**です。

注記: **ユーザー名とパスワードは、大文字/小文字が区別されます。**

ストレージ ルータのログ ファイルとクラッシュトレース ファイルは`/ata4/log`ディレクトリに、コンフィギュレーションファイルは`/ata3/savedconfig`ディレクトリに、スクリプトファイルは`/ata3/script`ディレクトリにそれぞれ格納されています。

FTPを使用してストレージ ルータのログ ファイルを取得するには、まず、`FTP cd`コマンドを実行して`/ata4/log`ディレクトリに移動します。ファイル リストを表示し、取得するファイルを決めます（この例では、ログ ファイル*messages0*を取得します）。必要に応じて、`FTP binary`コマンドを実行して、binaryフラグを指定します。`FTP get`コマンドを実行して、ログ ファイルを、サーバ上の指定したファイルにコピーします。作業が終わったら、`FTP bye`コマンドを実行してFTP接続を閉じます。

上に説明したFTPセッションの実行例を例22に示します。この例では、ストレージ ルータ管理インタフェースのIPアドレスは**10.1.11.210**になっています。

例 22: FTP セッション

```
Server1> ftp 10.1.11.210
Connected to 10.1.11.210.
220 VxWorks (5.4.1) FTP server ready
Name: admin
331 Password required
Password:********
230 User logged in
ftp> cd /ata4/log
250 Changed directory to "/ata4/log"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size           date       time      name
--------       ------     ------    --------
     512    Apr-09-2002  20:46:18   .        <DIR>
     512    Apr-09-2002  20:46:18   ..       <DIR>
   13803    May-16-2002  15:13:56   messages0
   92167    Apr-10-2002  19:14:06   tmpcrash.txt

226 Transfer complete
ftp: 374 bytes received in 0.02Seconds 23.38Kbytes/sec.
ftp> binary
200 Type set to I, binary mode
ftp> get
(remote-file) messages0
(local-file) SR2122Sys1_Messages
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
40863 bytes received in 0.049 seconds (8.1e+02 Kbytes/s)
ftp> bye
221 Bye...see you later
```

FTPセッションの開始前に管理インタフェースに対する制限を解除する必要があった場合は、ストレージ ルータのCLIセッションに戻り、以下の手順で制限を再度有効にします。

1. `show restrict` — 管理インタフェース上のポート21が現在開いていることを確認します。
2. `restrict mgmt ftp` — 管理インタフェース上のFTP機能を閉じます。FTP機能は使用できなくなります

診断機能について

ストレージ ルータでは、ユニット起動時にハードウェア診断が実行されます。ハードウェア診断は省略できません。ハードウェア診断でエラーが発生した場合、ストレージ ルータは停止します。この場合、起動プロセスを再開することはできません。

ハードウェア診断でエラーが発生した場合は、HPテクニカル サポートにご連絡ください。

ストレージ ルータでは、起動時のハードウェア診断の完了後、およびシステム再起動後に、さらにソフト診断が実行されます。ソフト診断は、不要な場合は省略することもできます。

ソフト診断でエラーが発生した場合は、HPテクニカル サポートにご連絡ください。

起動時のシステム メッセージの収集

ストレージ ルータでは、システム起動プロセス中に、さまざまなメッセージがコンソールに表示されます。このメッセージを収集しておくと、ストレージ ルータで問題が発生したときに役立つ場合があります。コンソール インタフェースを使用して起動プロセスを実行し、一般的な外部手段を使用してコンソール ログを収集してください。

ログについて

ストレージ ルータでは、さまざまなシステム イベント メッセージが生成されます。ストレージ ルータのイベント メッセージとデバッグ メッセージは、すべて次の形式で出力されます。

例 23: イベント メッセージ

```
Mar 18 11:48:05: %SNMP-5-SASAS: SnmpApp starting...
<timestamp>: %<facility>-<level_number>-<mnemonic>: <message text>
```

すべてのメッセージに、システムでのメッセージの優先度を示す通知レベルが割り当てられます。優先度が最も高いメッセージには、emergencyという通知レベルが割り当てられます。このレベルのメッセージは、システムが使用不可であることを示しています。優先度が最も低いメッセージには、debugという通知レベルが割り当てられます。このレベルのメッセージはトラブルシューティングに使用されます。例23では、メッセージ レベル番号**5**が示されています。これは、noticeという通知レベルを表します。

表16に、各通知レベルのレベル番号と意味を示します。

表16: イベント メッセージの通知レベル

通知レベル	レベル番号	意味
emergency	0	システム使用不可
alert	1	緊急な対処が必要
critical	2	危険な状態
error	3	エラー状態
warning	4	致命的ではない警告状態
notice	5	正常だが注意を要する状態
info	6	情報メッセージのみ
debug	7	トラブルシューティング用の情報

イベント メッセージ、トレース メッセージ、およびデバッグ メッセージは、メッセージの通知レベルおよびメッセージを生成したアプリケーション領域（ファシリティ）に応じて、さまざまな宛先にルーティングすることができます。表17に、ログ宛先とその意味を示します。また、表18に、ログのファシリティとその意味を示します。

表17: イベント メッセージのログ宛先

送信先	意味
all	すべての宛先にメッセージのログを残します。
none	メッセージのログを残さずに破棄します。
console	シリアル コンソールCLIセッションにメッセージのログを残します。
logfile	ストレージ ルータのログ ファイルにメッセージのログを残します。
rslog	リモートのsyslogサーバにメッセージのログを残します。リモートsyslogサーバのIPアドレスを指定するには、`logging syslog`コマンドを使用します。
vty	すべてのTelnetセッションまたはその他の仮想端末CLIセッションに、メッセージのログを残します。

表18: イベント メッセージのファシリティ

ファシリティ	意味
AUTH	AAA認証
CDP	CDP(Cisco Discovery Protocol)
CONF	コンフィギュレーション機能
FC	ストレージ ルータのファイバ チャネル インタフェース
GE	ストレージ ルータのギガビット イーサネット インタフェース
HA	ストレージ ルータの高可用性クラスタ
IF	インタフェース マネージャ
INVALID	一般機能
IPROUTER	ストレージ ルータのIP機能
ISCSI	iSCSI機能
MON	ハードウェア モニタ
SNMP	SNMP（Simple Network Management Protocol）
SNMP	SNMP（Simple Network Management Protocol）
SYSLOG	syslog機能
UI	ストレージ ルータのユーザー インタフェース

メッセージのルーティング用に、ルーティング ルールのリストが作成されます。イベント メッセージまたはデバッグ メッセージを受信すると、このリストで、ファシリティと通知レベルが一致するルールが検索されます。このルーティング ルールのリストは、ストレージ ルータのログ テーブルと呼ばれています。

デフォルトでは、通知レベル`notice`（またはそれ以下のレベル）のすべてのメッセージが、すべての宛先に送信されます。また、通知レベル`info`のメッセージはストレージ ルータのログ ファイルに送信されます。一致するルールのないメッセージはどの宛先にも送信されません。

現在のログ テーブルのルーティング ルールおよびその他のログ情報を表示するには、`show logging`コマンドを実行します。

イベント メッセージのフィルタとルーティング

ストレージ ルータのログ テーブルによって、メッセージはファシリティと通知レベルからフィルタされ、指定の宛先にルーティングされます。イベント メッセージが着信すると、ファシリティ名とレベルが一致するルールが見つかるまでログ テーブルのルールが検索され、一致したルールに指定されているすべての宛先に、そのメッセージが送信されます。一致するルールがない場合、そのイベント メッセージは破棄されます。

新しく追加したルーティング ルールは、既存のテーブルに追加されます。新しいルーティング ルールをログ テーブルに追加するには、`logging level`コマンドを使用します。ログ テーブルの特定のエントリの前にルーティング ルールを挿入するには、`logging #?`コマンドを使用します。

各ファシリティには8つの通知レベルを設定できます。ファシリティと通知レベルの各組み合わせには、最大7つの宛先を設定できます。

例24では、ファシリティはSNMP、通知レベルは5（notice）です。ログ テーブルに例14のエントリがある場合、例24 のイベント メッセージは最初のルーティング ルールと一致するので、有効なすべての宛先に送信されます。SNMPファシリティからの通知レベルinfoのメッセージ、および別のファシリティからの通知レベルinfo（またはそれ以下）のメッセージは2番目のルールと一致するので、ストレージ ルータのコンソールとログ ファイルに送信されます。通知レベル**debug**のメッセージはファシリティの場所に関係なく、すべて破棄されます。

例 24: ログ ルート エントリ リストの例

```
Index  Level    Priority  Facility  Route
1      notice   5         SNMP      all
2      info     6         all       console log file
```

ログ テーブルは保存することができ、いったん保存すればストレージ ルータの再起動後も維持されます。また、エントリが削除されても、ログ テーブルのルールの順番は維持されます。

ログの有効化と無効化

ログはデフォルトで有効になっています。また、デフォルトでは、ストレージ ルータのログ テーブルに、次のルーティング ルールが指定されています。

- 通知レベルnotice以下のメッセージは、有効なすべての宛先に送信される。
- 通知レベルinfoのメッセージは、ストレージ ルータのログ ファイルに送信される。
- debugメッセージはすべて破棄される。

no logging onコマンドを使用すると、ストレージ ルータのログ テーブルを変更せずに、すべての宛先に対するログを簡単に無効にできます。この場合、logging onコマンドでログを再び有効にするまでログが無効になります。

工場出荷時の設定に戻さずにログ テーブルを消去すると、ログ テーブルからすべてのルールが削除されます。この場合、一致するルールがログ テーブルに存在しないため、すべてのメッセージが破棄されることになります。再度ログが行われるようにするには、新しいルーティング ルールを追加するか、以前保存したログ テーブルを復元するか、ログ テーブルを工場出荷時設定に戻します。

ログ ファイルの表示と保存

show loggingコマンドを実行すると、ストレージ ルータのログ ファイル全体の内容、または選択した一部の内容を表示できます。WebベースのGUIでログ ファイルを表示することもできます。また、ログ ファイルを詳細に分析したり検索したりする場合は、FTPでログ ファイルのコピーを取得できます。詳しくは、157ページの「ストレージ ルータでのFTPの利用」を参照してください。

ストレージ ルータのログ ファイルの管理について詳しくは、154ページの「ログ ファイルの管理」を参照してください。

ストレージ ルータのコンフィギュレーションのキャプチャ

show runningconfigコマンドまたはshow bootconfigコマンドを実行すると、ストレージ ルータで現在使用中のコンフィギュレーションまたは起動コンフィギュレーションを表示できます。さらに、この表示結果をリダイレクトして、ストレージ ルータのscriptディレクトリにスクリプト ファイルを作成することができます。このように作成したファイルを土台にして、一般的な作業を自動化するコマンド スクリプトを作成できます。詳しくは、152ページの「スクリプトによる作業の自動化」を参照してください。

デバッグ機能の利用

ストレージ ルータには、SCSIルーティング インスタンス用のデバッグ機能が組み込まれています。ただし、デバッグ トレースを実行すると、ストレージ ルータの動作に影響を与える場合があります。SCSIルーティング インスタンスに関して解決できない問題が発生した場合、HPテクニカル サポートの担当者がデバッグ トレースのキャプチャを依頼することがあります。その場合は、この作業を行うために必要な設定について、担当者がご説明いたします。デフォルトでは、デバッグ機能は、すべてのSCSIルーティング インスタンスに対して無効になっています。

技術仕様

この付録では、ストレージ ルータの技術仕様の詳細を示します。

仕様

表19に技術仕様を示します。

表19: ストレージ ルータの仕様

仕様	
周囲環境	
温度（動作時）	10～35ºC（50～95ºF）
温度（非動作時および保管時）	-30～60ºC（-20～140ºF）
相対湿度（結露なし、動作時）	10～70%（結露なし）
相対湿度（結露なし、非動作時および保管時	5～95%（結露なし）
高度（動作時および非動作時）	-152.4～3048 m（-500～10000 ft）
物理特性	
寸法（H×W×D）	4.45×44.3×40.97 cm（1.75×17.44×16.13 in.）1 RU[1]
重量	5.1 kg（11.25 lb）
AC電源	
電源出力	70W
システム電力損失	50W
AC電流	最大1.0A（100～240 VAC）
AC周波数	50～60 Hz
通気	右側面から吸気、左側面から排気
ヒューズ（F1）定格	3.15A、250 VAC、タイムディレイ、現場での保守サービスなし

1. RU = ラック ユニット

ケーブル/ポートのピンの配置

B

この付録では、ストレージ ルータのケーブル/ポートのピンの配置を示します。内容は以下のとおりです。

ギガビット ポートおよびファイバ チャネル ポート

表20に、ストレージ ルータのギガビット イーサネット ポートおよびファイバ チャネル ポートで使用する、SFPモジュールとコネクタのタイプを示します。SFPモジュールとコネクタについては、SFPモジュールとコネクタの規格書を参照してください。

表20: SFPモジュールとコネクタ

ポート	準拠規格	コネクタ	媒体
ギガビット イーサネット（GE 1およびGE 2）	1000 Base-SX	MT-RJ	**光ファイバ**
		LC	**光ファイバ**
ファイバ チャネル（FC 1およびFC 2）	FC-PI 100/200-M5-SN-I **および** FC-PI 100/200-M6-SN-I	LC	**光ファイバ**

10/100イーサネット管理ポートおよびHAポート

10/100イーサネット ポートに終端システムを接続するには、モジュラRJ-45ストレートUTPケーブルを使用します。10/100イーサネット ポートに外部のスイッチやルータを接続するには、モジュラRJ-45クロス ケーブルを使用します。図45にストレート ケーブルの結線図、図46にクロス ケーブルの結線図を示します。

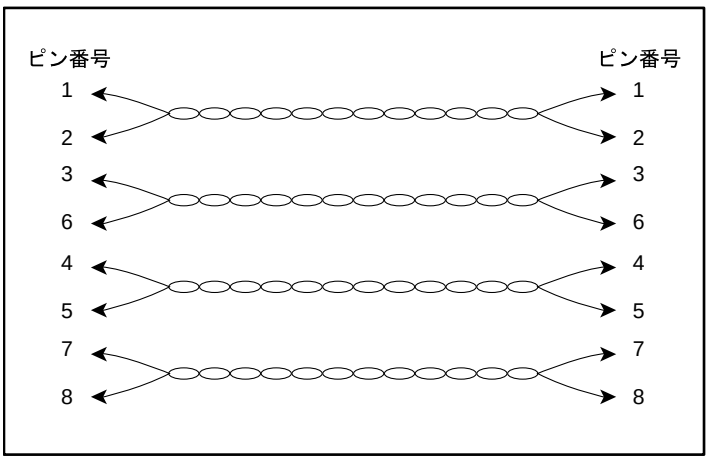

図45: ストレート ケーブル

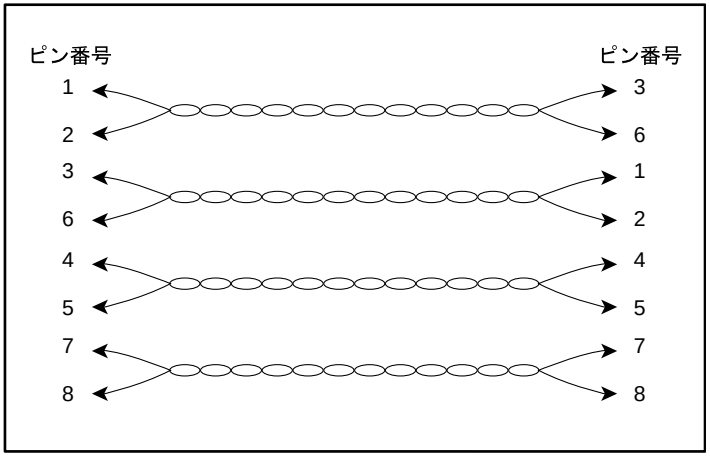

図46: クロス ケーブル

10/100イーサネット ポートではRJ-45コネクタをサポートします。表21に、RJ-45コネクタの各ピンの信号を示します。

表21: 10/100イーサネット管理ポートおよびHAポートのピン配置

ピン	信号	方向	説明
1	TD_P	出力	データ送信+
2	TD_N	出力	データ送信-
3	RD_P	入力	データ受信+
4			終端
5			終端
6	RD_N	入力	データ受信-
7			終端
8			終端

コンソール ポート

コンソール　ポートは、メス型8ピンRJ-45コネクタを備えたEIA/TIA-232ポートです。コンソール ポートへの接続には、ストレージ ルータに付属のロールオーバ ケーブルを使用します（図47参照）。表22にコンソール ポートのピン配置を示します。

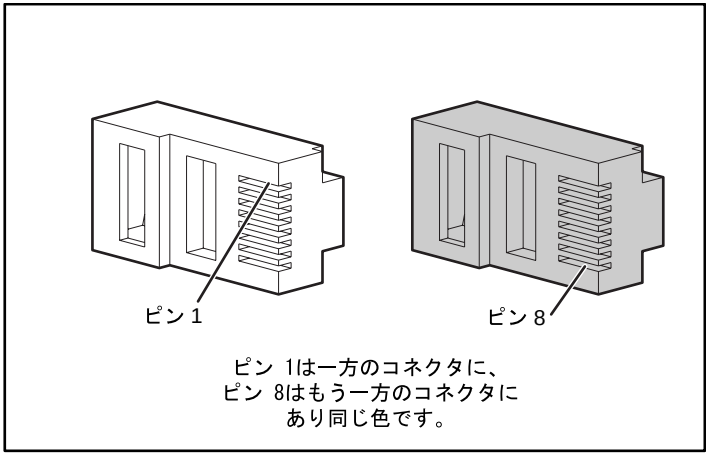

図47: コンソールポート接続用ロールオーバ ケーブル

表22: コンソール ポートのピン配置

ピン	信号	方向	説明
1	RTS	出力	送信要求
2	—	—	非接続
3	TxD_N	出力	送信データ
4	GND	—	信号接地
5	GND	—	信号接地
6	RxD_N	入力	受信データ-
7	—	—	非接続
8	CTS	入力	送信可

このコンソール　　ポートでは、EIA/TIA-232信号の一部だけを使用しています。TxD_N、RxD_N、CTS、およびRTSだけが接続されています。

注記: モデム制御信号は接続されていません。コンソール ポート経由でストレージ ルータにリモート アクセスする場合は、端末サーバを使用してください。

規定に関するご注意

C

規定準拠識別番号

規定に準拠していることの証明と識別のために、ご使用の製品には、HP固有のシリーズ番号が割り当てられています。このシリーズ番号は、必要な認可マークおよび情報とともに、製品ラベルに印刷されています。この製品の認可情報を請求する場合は、必ず、このシリーズ番号を参照してください。このシリーズ番号を、製品の製品名またはモデル番号と混同しないでください。

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. After the Class of the device is determined, refer to the corresponding statement in the following sections.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected
- Consult the dealer or an experienced radio or television technician for help

Declaration of Conformity for Products Marked with the FCC Logo, United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
  P. O. Box 692000, Mail Stop 530113
  Houston, Texas 77269-2000
- 1-800-652-6672 (1-800-OK COMPAQ) (For continuous quality improvement, calls may be recorded or monitored.)

For questions regarding this FCC declaration, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
  P. O. Box 692000, Mail Stop 510101
  Houston, Texas 77269-2000
- 1-281-514-3333

To identify this product, refer to the part, series, or model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Computer Corporation may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Power Cords

The power cord set included in your server meets the requirements for use in the country where you purchased your server. If you need to use this server in another country, you should purchase a power cord that is approved for use in that country.

The power cord must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product. In addition, the cross sectional area of the wire must be a minimum of 1.00 mm² or 18AWG, and the length of the cord must be between 6 feet (1.8 m) and 12 feet (3.6 m). If you have questions about the type of power cord to use, contact your HP authorized service provider.

A power cord should be routed so that it is not likely to be walked on or pinched by items placed upon it or against it. Particular attention should be paid to the plug, electrical outlet, and the point where the cord exits from the product.

Mouse Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parenthesis):

- EN55022 (CISPR 22) – Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) – Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) – Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) – Power Line Flicker
- EN60950 (IEC950) – Product Safety

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス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。

Taiwanese Notice

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

レーザー装置

レーザー装置を搭載したHPのシステム製品はすべて、IEC 825等の安全基準に適合しています。またこれらの装置は、米国政府の定めるClass 1のレーザー装置基準に適合しており、通常の使用では人体に有害なレーザー光線を装置外部に放射することはありません。

レーザーの安全に関するご注意

警告: 火災や人体への傷害、装置の損傷を防ぐために、次の注意事項に従ってください。

- **レーザー装置のカバーを開けないでください。お客様が直接修理することはできません。**
- **レーザー装置に対してこのガイドに記載された以外の修理、調整等は絶対にしないでください。**
- **内蔵レーザー装置の保守や修理は、必ず、HPのサービス窓口にご依頼ください。**

CDRH規定

米国食品医薬局CDRH（Center for Devices and Radiological Health）のレーザー製品に関する規定（1976年8月2日施行）は1976年8月1日以降に製造されたレーザー製品に適用されます。米国内で販売されるすべての製品がこの規定に適合しなければなりません。

国際規定

レーザー装置を搭載したHPのシステム製品はすべて、IEC 825等の安全基準に適合しています。

レーザー製品ラベル

以下のラベルまたはそれに類似するものが、HPの提供するレーザー装置に貼付されています。

このラベルを貼付した製品は、Class1レーザー装置として分類されます。左のラベルが製品の外側と内蔵レーザー製品の外側に貼付されています。

レーザー部

表23: レーザー部

機能	説明
種別	**半導体（GaAlAs）レーザー**
波長	780nm±35 nm
ビーム分散角	53.5±0.5 °
出力	0.2mW / 10,869W m-2 sr-1**未満**
偏光	**環状**0.25
レンズ口径	11.43±1.02mm（0.45±0.04**インチ**）

静電気対策

D

システムのセットアップ時、また部品を取り扱ったりする場合には、システムの損傷を防止するために守らなければならないことがあるので注意してください。人間の指など、導電体からの静電気によって、システム ボードなどの静電気に弱いデバイスが損傷して、耐用年数が短くなることがあります。

静電気による損傷を防止するには、以下のことを守ってください。

- 運搬や保管の際は、静電気防止用のケースに入れ、手で直接触れることは避けます。
- 静電気に弱い部品は、静電気防止措置のなされている作業台に置くまでは、専用のケースに入れたままにしておきます。
- 部品をケースから取り出す前に、まずアースされている面にケースごと置きます。
- ピン、リード線、回路には触れないようにします。
- 静電気に弱い部品および機材に触れるときには、つねに自分の身体に対して適切なアース対策を行います。

アースの方法

アースにはいくつかの方法があります。静電気に弱い部品を取り扱うときには、以下のうち1つ以上の方法でアースを行ってください。

- すでにアースされている作業台またはコンピュータ本体にリスト ストラップをつなぎます。リスト ストラップは柔軟な帯状のもので、アース コード内の抵抗は、1MΩ ±10%です。アースを正しく行うために、リスト ストラップを肌に密着させてください。
- 立って作業する場合、かかとやつま先または足全体にリスト ストラップをつけます。導電性または静電気が伝わる恐れのある床の場合、両足にリスト ストラップをつけます。
- 作業用具は導電性のものを使用します。
- 折りたたみ式の静電気防止マットがついた、携帯式の作業用具もあります。

上記のような、適切にアースを行うための器具がないときは、HP販売店またはHPのサービス窓口にお問い合わせください。

注記: 静電気に関する詳細や製品のインストールについては、HP販売店またはHPのサービス窓口にお問い合わせください。

索引

す

せ

そ