Cisco Firepower 8000 シリーズ スタートアップ ガイド

81xx、82xx、および 83xx Firepower と AMP モデル用

更新日:2018 年 8 月 22 日

このマニュアルの構成は、次のとおりです。

パッケージの内容

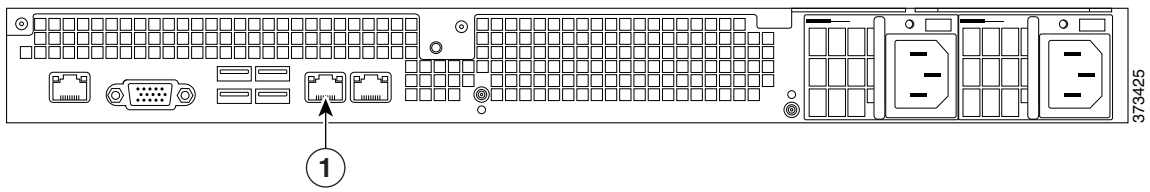
このセクションでは、各モデルに含まれる品目を示します。この内容は変更される場合があるため、実際に含まれているアイテムは多かったり、少なかったりする場合があることにご注意ください。

シャーシ モデル

FirePOWER 8000 シリーズ デバイスは、さまざまなシャーシで提供できます。

- FirePOWER 8120/8130/8140 および AMP8050/AMP8150 は 1 U アプライアンスとして使用可能で、3 つまでのセンシング モジュールを含めることができます。次のシャーシ背面図に、管理インターフェイスの位置を示します。

図 1 FirePOWER 81xx および AMP 8xxx シリーズのシャーシおよび管理インターフェイス



1	管理インターフェイス		

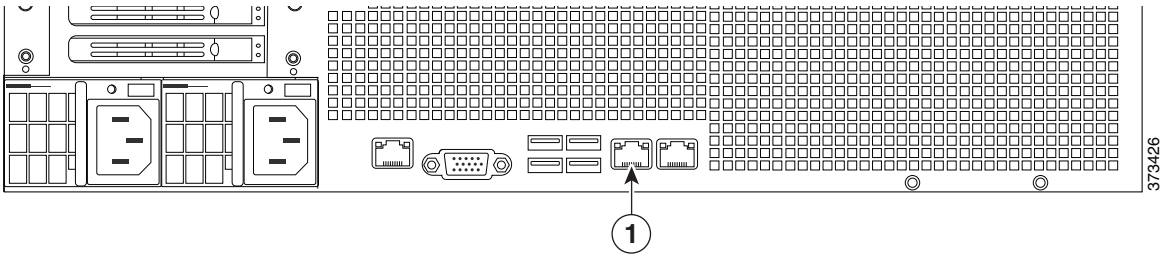
- Firepower 8130（1 U モデル）は、このシャーシに最大 3 つのセンシング モジュールを含めることができます。

  （注）FirePOWER 8120/8130/8140 および AMP8050/AMP8150 モデルには同一のシャーシがあります。どのモデルか不明な場合は、パッキング リストを確認してください。

  （注）FirePOWER 8140 にスタッキング キットを追加して全部で 2 U 構成にできます。

- FirePOWER 8250 は 2U アプライアンスとして提供されます。次のシャーシ背面図に、2U アプライアンスごとの管理インターフェイスの位置を示します。

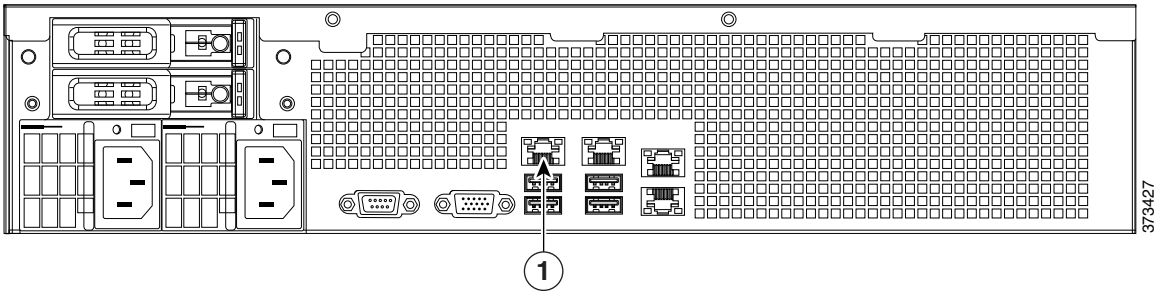
図 2　FirePOWER 82xx シリーズのシャーシおよび管理インターフェイス



1	管理インターフェイス		

- Firepower 8250（2 U モデル）のシャーシには、最大 7 つのモジュールを含めることができます。最大 3 つのスタッキング キットを追加して合計で 8 U 構成にできます。
  - Firepower 8260（4 U モデル）の 40 g プライマリ シャーシには、1 つのスタッキング モジュールと最大 6 つのセンシング モジュールが収容されます。セカンダリ シャーシには、1 つのスタッキング モジュールが収容されます。最大 2 つのスタッキング キットを追加して合計で 8U 構成にできます。
  - Firepower 8270（6 U スタック モデル）の 40 G プライマリ シャーシには、2 つのスタッキング モジュールと最大 5 つのセンシング モジュールが収容されます。2 つのセカンダリ シャーシには、1 つのスタッキング モジュールが収容されます。1 つのスタッキング キットを追加して合計で 8U 構成にできます。
  - Firepower 8290（8 U スタック モデル）の 40 G プライマリ シャーシには、3 つのスタッキング モジュールと最大 4 つのセンシング モジュールが収容されます。3 つのセカンダリ シャーシには、1 つのスタッキング モジュールが収容されます。このモデルはフル構成であり、スタッキング キットを収容できません。
- FirePOWER および AMP 8350 は 2 U アプライアンスとして提供されます。次のシャーシ背面図に、2U アプライアンスごとの管理インターフェイスの位置を示します。

図 3　FirePOWER および AMP 83xx シリーズのシャーシおよび管理インターフェイス



1	管理インターフェイス		

- FirePOWER 8350 および AMP8350（2 U モデル）のシャーシは最大 7 つのモジュールを含めることができます。最大 3 つのスタッキング キットを追加して合計で 8 U 構成にできます。
  - Firepower 8360 および AMP8360（4 U スタック モデル）の 40 G プライマリ シャーシには、1 つのスタッキング モジュールと最大 6 つのセンシング モジュールが収容されます。1 つのセカンダリ シャーシには、1 つのスタッキング モジュールが収容されます。最大 2 つのスタッキング キットを追加して合計で 8U 構成にできます。
  - Firepower 8370 と AMP8370（6 U スタック モデル）には、2 つのスタッキング モジュールと最大 5 つのセンシング モジュールを搭載した 40 G プライマリ シャーシが含まれています。2 つのセカンダリ シャーシには、1 つのスタッキング モジュールが収容されます。1 つのスタッキング キットを追加して合計で 8U 構成にできます。
  - Firepower 8390 および AMP8390（8 U スタック モデル）には、3 つのスタッキング モジュールと最大 4 つのセンシング モジュールを搭載した 40 G プライマリ シャーシが含まれています。3 つのセカンダリ シャーシには、1 つのスタッキング モジュールが収容されます。このモデルはフル構成であり、スタッキング キットを収容できません。

付属品

- シャーシごとに 2 本の電源コード。
- シャーシごとに 2 本ずつのストレート Cat 5e イーサネット ケーブル。
- シャーシごとに 1 つのラック設置キット。
- ネットワーク モジュール（NetMod）の組み合わせで、次のセクションで説明します。

ネットワーク モジュール

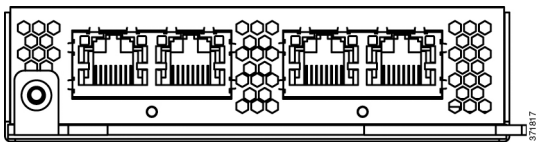
Firepower 8000 シリーズ アプライアンスのセンシング インターフェイスは、銅線インターフェイスまたはファイバ インターフェイスで提供できます。

注意：モジュールはホットスワップ可能ではありません。詳細については、『*Firepower 8000 Series Hardware Installation Guide*』を参照してください。

20180926 1010設定可能なバイパス

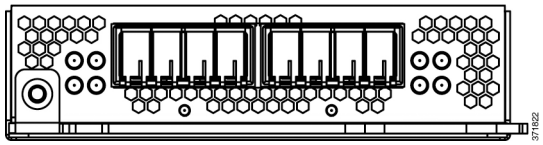
次のモジュールには、設定可能バイパス センシング インターフェイスが含まれています。

クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod



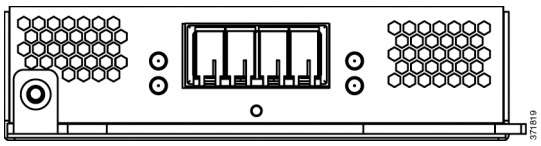
- ケーブル：標準銅ケーブル
- パッシブの設定：1、2、3、または 4
- インライン設定：1 または 2（左ペアまたは右ペア）

クアッドポート 1000BASE-SX ファイバ設定可能バイパス NetMod



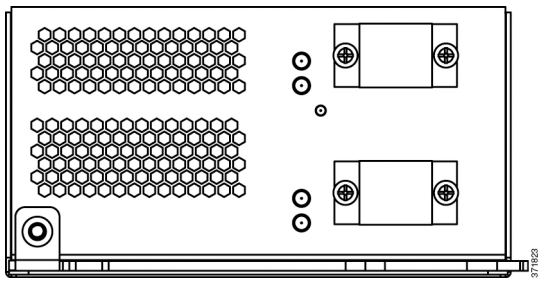
- ケーブル：ローカル コネクタ（LC）光トランシーバ
- パッシブの設定：1、2、3、または 4
- インライン設定：1 または 2（左ペアまたは右ペア）

デュアルポート 10GBASE ファイバ設定可能バイパス NetMod



- ケーブル:ローカル コネクタ(LC)光トランシーバ、MMSR または SMLR
- パッシブの設定:1 または 2
- インライン設定:1

デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod

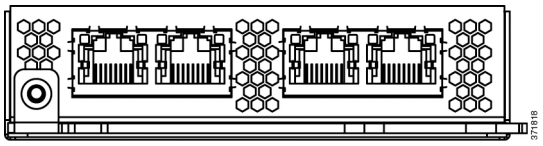


- Firepower 8270/8290、8370/8390、AMP8370/8390 または 40G 対応 Firepower 8250/8260、8350/8360 または AMP8350/8360 でのみ使用
- ケーブル:マルチファイバ プッシュ オン(MPO)コネクタの光トランシーバ
- パッシブの設定:1 または 2
- インライン設定:1

非バイパス

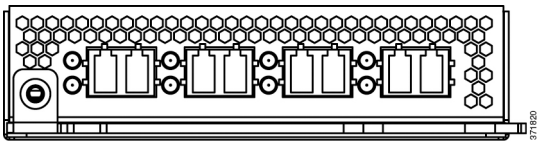
次のモジュールには、非バイパス センシング インターフェイスが含まれています。

クワッドポート 1000BASE-T 銅線非バイパス NetMod



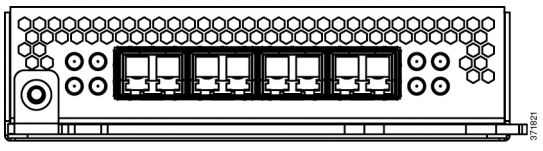
- ケーブル:標準銅ケーブル
- パッシブの設定:1、2、3、または 4
- インライン設定:1 または 2(左ペアまたは右ペア)

クワッドポート 1000BASE-SX ファイバ非バイパス NetMod



- ケーブル:ローカル コネクタ(LC)光トランシーバ
- パッシブの設定:1、2、3、または 4
- インライン設定:1 または 2(左ペアまたは右ペア)

クワッドポート 10GBASE-SR または LR ファイバ非バイパス NetMod



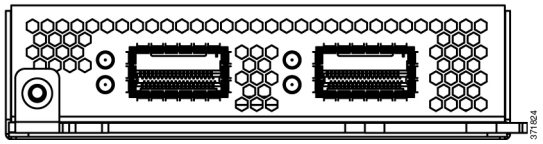
- ケーブル:ローカル コネクタ(LC)光トランシーバ
- パッシブの設定:1、2、3、または 4
- インライン設定:1 または 2(左ペアまたは右ペア)

スタック モジュール

スタッキング モジュールは 2 つの同様のデバイスに接続し、プライマリ デバイスの能力を向上させます。スタッキング モジュールは、Firepower 8140/8250/8350 および AMP8350 ではオプションです。Firepower 8260/8270/8290、Firepower 8360/8370/8390 および AMP8360/8370/8390 には含まれています。

(注) 別の設定でデバイスを接続することはできません。たとえば、Firepower 8350 に Firepower 8250 を接続しないでください。詳細については、『Firepower 8000 Series Hardware Installation Guide』を参照してください。

スタック モジュール



- ケーブル：8000 シリーズのスタッキング ケーブル
- Firepower 8140：接続ごとに 1 つ、最大 2 つの 8140 アプライアンス
- Firepower 8250/8260/8270/8290：接続ごとに 2 つ、最大 4 つの 8250 アプライアンス
- Firepower 8350/8360/8370/8390：接続ごとに 2 つ、最大 4 つの 8350 アプライアンス
- AMP8350/8360/8370/8390：接続ごとに 2 つ、最大 4 つの AMP8350 アプライアンス

デバイス スタック

次の設定でデバイスをスタックできます。

- 2 つの Firepower 8140（Firepower 8120/8130、AMP8050/AMP8150 ではできません）
- 最大 4 つの Firepower 8250、最大 4 つの Firepower 8350 または最大 4 つの AMP8350
- 1 つの FirePOWER 8260（1 台の 10 G 対応プライマリ デバイスと 1 台のセカンダリ デバイス）
- 1 つの FirePOWER 8360/AMP8360（1 台の 40 G 対応プライマリ デバイスと 1 台のセカンダリ デバイス）
- 1 つの FirePOWER 8270 または FirePOWER 8370/AMP8370（1 台の 40 G 対応プライマリ デバイスと 2 台のセカンダリ デバイス）
- 1 つの FirePOWER 8290 または FirePOWER 8390/AMP8390（1 台の 40 G 対応プライマリ デバイスと 3 台のセカンダリ デバイス）

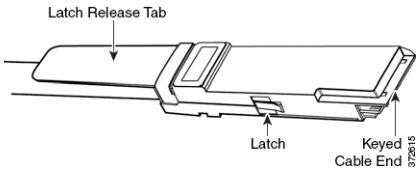
1 つのデバイスが、プライマリ デバイスとして指定され、ネットワーク セグメントに接続されます。その他のすべてのデバイスは、セカンダリ デバイスとして指定され、プライマリ デバイスに追加のリソースを提供するために使用されます。

単一の Firepower 8140、Firepower 8250、または Firepower 8350/AMP8350 を接続する場合と同様の方法で、プライマリ デバイスを分析対象のネットワーク セグメントに接続します。スタック配線図に示すように、セカンダリ デバイスをプライマリ デバイスに接続します。セカンダリ デバイスにセンシング インターフェイスがある場合、そのインターフェイスは使用されません。

デバイスがネットワーク セグメントと他のデバイスに物理的に接続されたら、Firepower Management Center を使用してスタックを設定して管理します。スタック構成でのデバイスの使用に関する詳細は、『Firepower 8000 Series Hardware Installation Guide 』を参照してください。

8000 シリーズのスタッキング ケーブルの使用

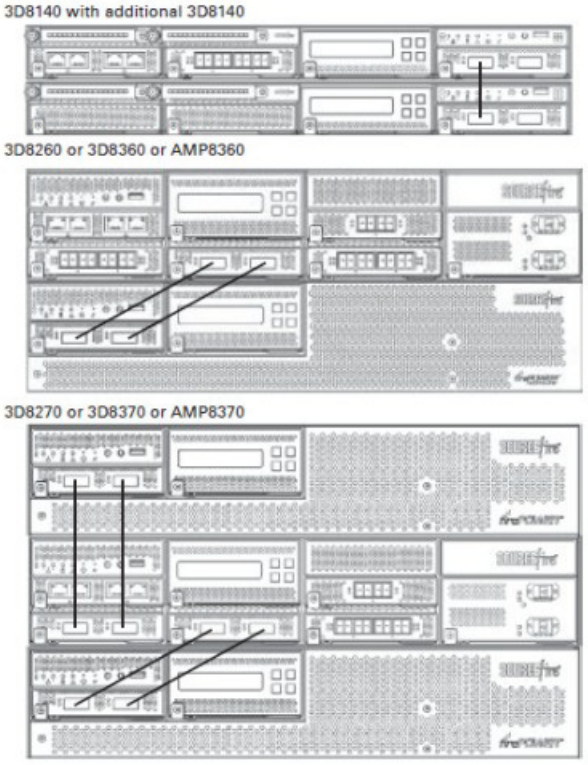
1 m（3 フィート）の 8000 シリーズ スタッキング ケーブルの範囲内にデバイスをインストールして、プライマリとセカンダリ デバイス間の物理的な接続を作成します。2 つの Firepower 8140 のスタック構成には、1 本のケーブルが必要です。Firepower 8250/8260/8270/8290、Firepower 8350/8360/8370/8390、または AMP8350/8360/8370/8390 のスタック構成には、接続あたり 2 本のケーブルが必要です。スタッキング ケーブルの取り付けまたは取り外し時にデバイスの電源をオフにする必要はありません。

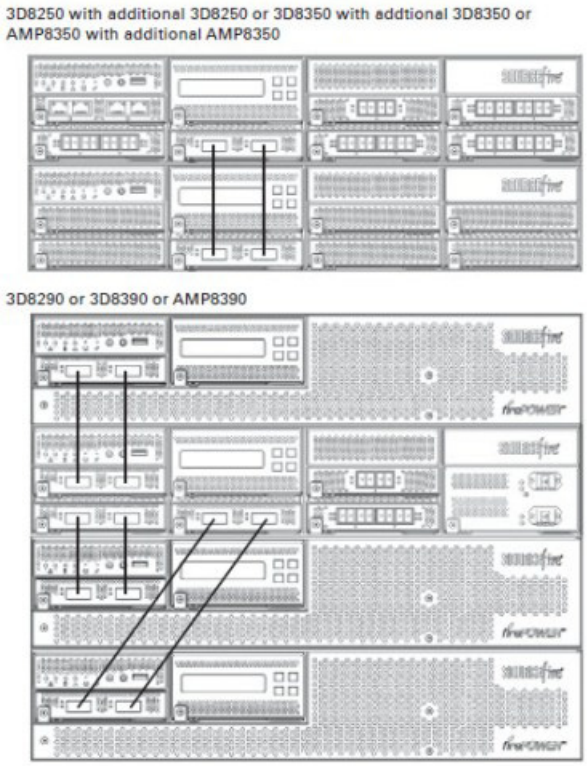


8000 シリーズのスタッキング ケーブルの使用方法

- ケーブルを挿入するには、ケーブルの先端を解放つまみを上にして持ち、鍵型の先端部分をスタッキング モジュールのポートに差し込んで、ラッチがカチッと鳴るまで押し込みます。
- ケーブルを取り外すには、ラッチを解放するための解放つまみを引っ張ってから、ケーブルの先端を引き抜きます。

ケーブル接続図



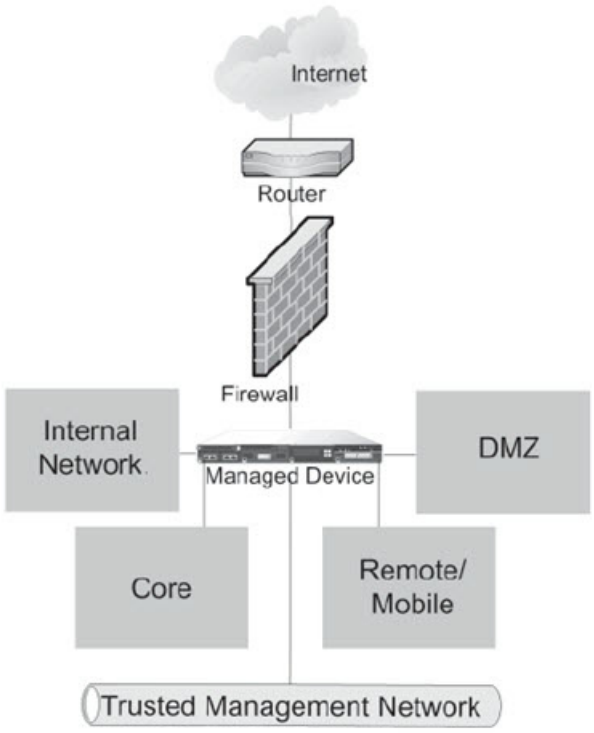


アプライアンスの展開

デバイスは通常ファイアウォール内に展開され、信頼できる管理ネットワークやモニタする各種のネットワーク セグメントに接続されます。

シンプルな展開シナリオとしては、イーサネット ケーブルを使用して、デバイスの管理インターフェイスを信頼できる管理ネットワークに接続し、適切なケーブル(銅またはファイバ)を使用して、センシング インターフェイスをパッシブまたはインライン ケーブル設定でモニタするネットワーク セグメントに接続します。

信頼できる管理ネットワーク(不正アクセスから保護されている制限されたネットワーク)は、セキュリティ アップデートや同様の機能のために単一のセキュアな接続を利用できますが、ネットワークの他の部分からは分離されており、日常のビジネス業務で使用するホストにはアクセスできません。



センシング インターフェイスは、個別のセグメントのニーズに基づく対象ポリシーに応じて異なるセキュリティ要件を持つ、特定のビジネス コンポーネント専用の異なるネットワーク セグメントに接続することができます。これらのセグメントには DMZ(メール、ftp、Web ホストなどの外部向けサーバ)、内部ネットワーク(日常業務や同様のアプリケーションで使用されているホスト)、およびコア(重要なビジネス資産のために確保されているホスト)が含まれており、リモート ロケーション、モバイル アクセス、またはその他の機能専用のセグメントを含めることもできます。

センシング インターフェイスのケーブルの配線方法によって、構成オプションが決まります。パッシブ配線を使用すると、パッシブ センシング インターフェイスを構成できます。インライン配線を使用すると、パッシブ、インライン、フェールオープンのインライン、仮想スイッチ、仮想ルータ、またはハイブリッド センシング インターフェイスをデバイスに作成できます。展開オプションやインターフェイス構成、および製品機能への影響についての詳細は、『*Firepower Firepower Management Center Configuration Guide*』および『*Firepower 8000 Series Hardware Installation Guide*』を参照してください。

デバイスの配線

デバイスにケーブルを配線して、展開の必要に応じてパッシブまたはインライン インターフェイスを設定できます。

次の場合、パッシブ配線を使用します。

- トラフィックをモニタする
- ホスト、オペレーティング システム、アプリケーション、ユーザ、ファイル、ネットワーク、および脆弱性についての情報を収集する

パッシブ展開と同じ機能に加えて、次のことが必要な場合にはインライン配線を使用します。

- 仮想スイッチ、仮想ルータ、またはハイブリッド インターフェイスを設定する
- ネットワーク アドレス変換(NAT)を実行する
- アプリケーション制御、ユーザ制御、セキュリティ インテリジェンス、URL 処理、ファイル制御、マルウェアの検出、または侵入防御などのアクセス制御機能に基づいてトラフィックをブロックするポリシーを使用する

設定するインターフェイスに適切なケーブル(インターフェイスにより指示される)と配線図を使用し、次に Firepower Management Center の Web インターフェイスを使用して、インターフェイスを設定します。センシング インターフェイスの接続(8 ページ)を参照してください。

センシング インターフェイスの接続

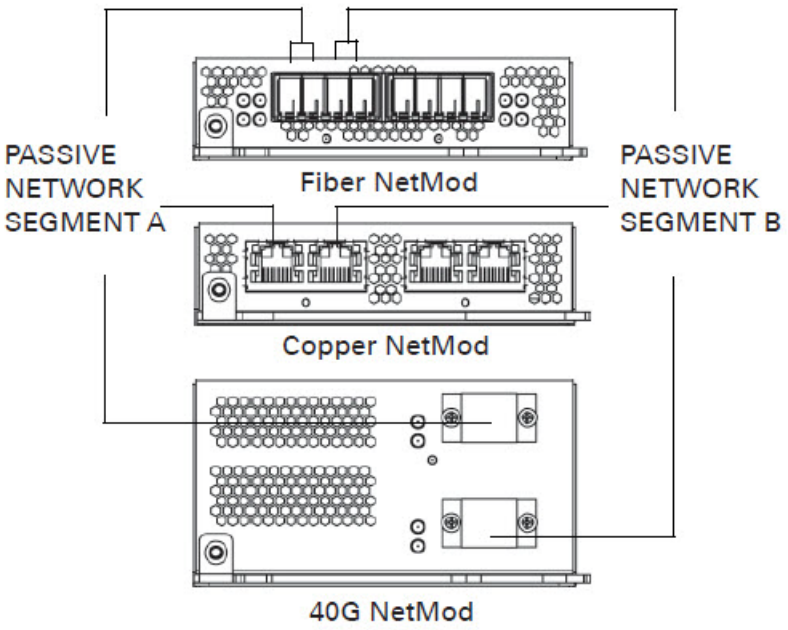
このセクションでは、センシング インターフェイスの物理的な接続について説明します。インターフェイスにケーブル配線した後、デバイスを管理する Firepower Management Center の Web インターフェイスを使用して、デバイスのセンシング インターフェイスをインライン、フェールオープンのインライン、スイッチド、ルーテッド、またはハイブリッドに設定します。センシング インターフェイスとして、デバイス前面のインターフェイスだけを使用します。

展開計画の詳細については、『*Firepower 8000 Series Hardware Installation Guide*』を参照してください。展開モデルを選択した後、設定に応じてセンシング インターフェイスにケーブル配線します。

パッシブ インターフェイスのケーブル配線

受動的にモニタする各ネットワーク セグメントに対して、適切なケーブル(ファイバまたは銅線のいずれか)を 1 つのセンシング インターフェイスに接続します。

パッシブ インターフェイスを設定する場合、このケーブル配線を使用します。

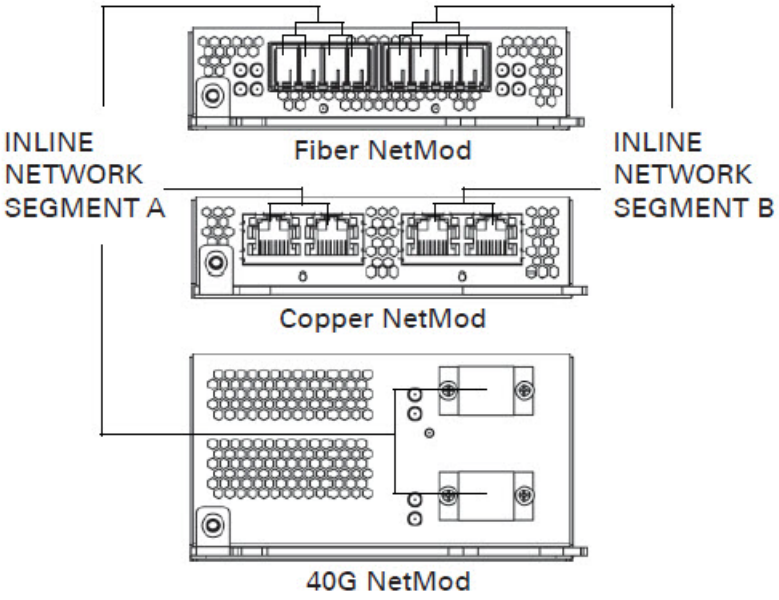


インライン インターフェイスのケーブル配線

インラインでモニタする各ネットワーク セグメントに対して、適切なケーブル(ファイバまたは銅線のいずれか)をセンシング インターフェイスのペアに順番に接続します。

インライン、フェールオープンのインライン、スイッチド、ルーテッド、またはハイブリッドに設定する場合、このケーブル配線を行います。

デバイスの設定可能なフェールオープン機能を利用する場合は、インターフェイスをケーブル配線し、デバイスを管理する Firepower Management Center の Web インターフェイスを使用して、フェールオープンでインラインとしてインターフェイスを設定します。



FirePOWER 8000 シリーズ デバイスの取り付け

アプライアンスを設置するときには、初期設定のためにアプライアンスのコンソールにアクセスできることを確認してください。KVM でキーボードとモニタを使用するか、シリアル接続、または管理インターフェイスへのイーサネット接続を使用して、初期設定のためにコンソールにアクセスできます。

(注) 管理インターフェイスは、デフォルト IPv4 アドレスで事前に設定されています。ただし、設定プロセスの一部として、管理インターフェイスを IPv6 アドレスで再設定できます。

キーボードとモニタ/KVM

アプライアンスに USB キーボードと VGA モニタを接続できます。これはキーボード、ビデオ、マウスの(KVM)スイッチに接続しているラックマウント型アプライアンスで便利です。

シリアル接続

物理シリアル ポートを使用して、コンピュータを任意の 8000 シリーズ アプライアンスに接続できます。適切なロールオーバー シリアル ケーブル(ヌル モデム ケーブルまたはシスコ コンソール ケーブルとも呼ばれる)を常に接続した状態で、デフォルト VGA 出力をシリアル ポートにリダイレクトするようリモート管理コンソールを設定してください。アプライアンスと通信するには、HyperTerminal や Xmodem などの端末エミュレーション ソフトウェアを使用します。このソフトウェアの設定は、9600 ボー、8 データ ビット、パリティ チェックなし、1 ストップ ビット、およびフロー制御なしです。FirePOWER8000 シリーズ および AMP8000 シリーズ デバイスは RJ-45 接続を使用します。

管理インターフェイスへのイーサネット接続

次のネットワーク設定を使用して、インターネットに接続してはならないローカル コンピュータを設定します。

- IP アドレス:192.168.45.2
- ネットマスク:255.255.255.0
- デフォルト ゲートウェイ:192.168.45.1

イーサネット ケーブルを使用して、ローカル コンピュータ上のネットワーク インターフェイスをアプライアンス上の管理インターフェイスに接続します。管理インターフェイスは、デフォルト IPv4 アドレスで事前に設定されていることに注意してください。ただし、設定プロセスの一部として、管理インターフェイスを IPv6 アドレスで再設定できます。

アプライアンスを設置するには:

1. 取り付けキットと付属の手順を使用して、アプライアンスをラックに取り付けます。
2. キーボードとモニタまたはイーサネット接続を使用してアプライアンスに接続します。
   - キーボードとモニタを使用してアプライアンスを設定している場合は、ここでイーサネット ケーブルを使用して管理インターフェイスを保護されたネットワーク セグメントに接続します。
   - コンピュータを直接アプライアンスの物理管理インターフェイスに接続することによって初期設定プロセスを実行する予定の場合は、設定の完了時に、管理インターフェイスを保護されたネットワークに接続します。
3. インターフェイスに対して適切なケーブルを使用して、センシング インターフェイスを分析対象のネットワーク セグメントに接続します。
   - 銅線センシング インターフェイス:デバイスに銅線センシング インターフェイスがある場合は、適切なケーブルを使用してデバイスがネットワークに接続されていることを確認します。『Firepower 8000 Series Hardware Installation Guide』の「Cabling Inline Deployments on Copper Interfaces」を参照してください。
   - ファイバ アダプタ カード:ファイバ アダプタ カードを備えたデバイスの場合は、オプションのマルチモード ファイバ ケーブルの LC コネクタを、任意の順序でアダプタ カード上の 2 つのポートに接続します。SC プラグを分析対象のネットワーク セグメントに接続します。
   - ファイバ タップ:オプションの光ファイバ タップを備えたデバイスを展開している場合は、オプションのマルチモード ファイバ ケーブルの SC プラグをタップ上の「アナライザ」ポートに接続します。タップを分析対象のネットワーク セグメントに接続します。
   - 銅線タップ:オプションの銅線タップを備えたデバイスを展開している場合は、タップの左側にある A ポートと B ポートを分析対象のネットワーク セグメントに接続します。タップの右側にある A ポートと B ポート(「アナライザ」ポート)をアダプタ カード上の 2 つの銅線ポートに接続します。

   管理対象デバイスを展開するためのオプションについては、『Firepower 8000 Series Hardware Installation Guide』の「Deploying Managed Devices」を参照してください。

   バイパス インターフェイスを備えたデバイスを展開している場合は、デバイスで障害が発生してもネットワーク接続を維持できるデバイスの能力を活用できることに注意してください。取り付けと遅延のテストの詳細については、『Firepower 8000 Series Hardware Installation Guide』の「Testing an Inline Bypass Interface Installation」を参照してください。
4. 電源コードをアプライアンスに接続し、電力源に差し込みます。

   アプライアンスに冗長電源がある場合は、電源コードを両方の電源に接続し、別々の電力源に差し込みます。
5. アプライアンスの電源をオンにします。
6. 直接イーサネット接続を使用してアプライアンスを設定する場合は、ローカル コンピュータ上のネットワーク インターフェイスとアプライアンス上の管理インターフェイスの両方のリンク LED が点灯していることを確認してください。

   管理インターフェイスとネットワーク インターフェイスの LED が点灯していない場合は、クロス ケーブルを使用してみてください。詳細については、『Firepower 8000 Series Hardware Installation Guide』の「Cabling Inline Deployments on Copper Interfaces」を参照してください。

次の作業

- デバイスの初期設定(11 ページ)の手順に従って設定プロセスを完了します。

デバイスの初期設定

新しい FirePOWER デバイスを展開して設置したら、設定プロセスを完了する必要があります。設定プロセスにより、時間の設定、デバイスの登録とライセンシング、スケジュールの更新など、管理レベルの多数の初期タスクを実行することもできます。設定および登録時に選択したオプションにより、システムが作成および適用するデフォルトのインターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

設定を開始する前に、次の要件を満たしているかどうかを確認してください。

アクセス

新しいアプライアンスを設定するには、キーボードとモニタ/KVM またはアプライアンスの管理インターフェイスへの直接イーサネット接続を使用して接続する必要があります。初期設定後は、アプライアンスをシリアル アクセス用に設定できます。詳細については、『*Firepower 8000 Series Hardware Installation Guide*』の「Rack-Mounting a Firepower Device」を参照してください。

(注) アプライアンスは大容量ストレージ デバイスをブート デバイスとして使用する可能性があるため、初期セットアップのためにアプライアンスにアクセスするときには、KVM コンソールと一緒に USB 大容量ストレージを**使用しない**でください。

ネットワークと展開の情報

少なくとも、アプライアンスが管理ネットワーク上で通信できるようにするために必要な情報(IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイ)は入手しておきます。

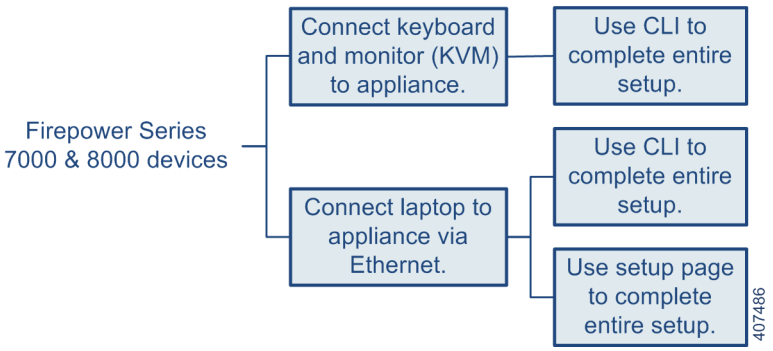
アプライアンスの展開方法がわかっている場合は、設定プロセスが登録とライセンス認証を含むさまざまな初期管理レベル タスクを実行する良い機会になります。

(注) 複数のアプライアンスを展開している場合は、先にデバイスを設定してから、管理元の FirePOWER Management Center を設定します。デバイスの初期設定プロセスを使用すれば、デバイスを FirePOWER Management Center に事前登録できます。FirePOWER Management Center の設定プロセスを使用すれば、事前登録した管理対象デバイスを追加してライセンス認証できます。

設定が完了したら、FirePOWER Management Center Web インターフェイスを使用して、展開用のほとんどの管理タスクと分析タスクを実行します。FirePOWER デバイスは、基本的な管理を実行するためにしか使用できないように Web インターフェイスが制限されています。詳細については、次の手順(17 ページ)を参照してください。

(注) 工場出荷時設定に復元(デバイスの工場出荷時の初期状態への復元(19 ページ)を参照)後にアプライアンスを設定しており、アプライアンスのライセンスとネットワーク設定を削除していない場合は、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを直接閲覧しながら、設定を実行できます。Web インターフェイスを使用した初期設定(12 ページ)にスキップします。

次の図に、FirePOWER デバイスの設定時に選択可能な設定を示します。



FirePOWER デバイスへのアクセスによって、その設定方法が決まります。次の選択肢があります。

- 直接イーサネット接続経由でアプライアンスにアクセスしている場合は、ローカル コンピュータからアプライアンスの Web インターフェイスを閲覧できます。Web インターフェイスを使用した初期設定（12 ページ）を参照してください。
- デバイスへの接続方法に関係なく、CLI を使用してデバイスを設定できます。CLI を使用した初期設定（15 ページ）を参照してください。

再イメージ化されたデバイスを設定しており、復元プロセスの一部としてネットワーク設定を維持している場合は、SSH または Lights-Out Management（LOM）接続経由で CLI にアクセスできます。また、管理ネットワーク上のコンピュータからデバイスの Web インターフェイスを閲覧することもできます。

注意：このガイドの手順では、電源をオンにしたままアプライアンスを設定する方法について説明します。ただし、何らかの理由で電源をオフにする必要がある場合は、『*Firepower Management Center 設定ガイド*』の「Device Management Basics」の章にある手順を使用するか、FirePOWER デバイスの CLI から `system shutdown` コマンドを使用するか、またはアプライアンスのシェル（エキスパート モードとも呼ばれます）から `shutdown -h now` コマンドを使用します。

Web インターフェイスを使用した初期設定

ほとんどの場合、デバイスの Web インターフェイスにログインし、設定ページで初期設定オプションを指定することによって、設定プロセスを完了する必要があります。

手順

1. ブラウザで `https://mgmt_ip/` にアクセスします。ここで、*mgmt_ip* はデバイスの管理インターフェイスの IP アドレスです。
   - イーサネット ケーブルを使用してコンピュータに接続されたデバイスの場合は、そのコンピュータ上のブラウザでデフォルトの管理インターフェイスの IPv4 アドレス（`https://192.168.45.45/`）にアクセスします。
   - ネットワーク設定がすでに構成されているデバイスの場合は、管理ネットワーク上のコンピュータを使用して、デバイスの管理インターフェイスの IP アドレスを閲覧します。
2. ユーザ名として `admin` を、パスワードとして `Admin123` を使用してログインします。

   初期設定のオプションについては、次の項を参照してください。
   - パスワードの変更（13 ページ）
   - ネットワーク設定（13 ページ）
   - FirePOWER デバイスの LCD パネルの設定（13 ページ）
   - リモート管理（13 ページ）
   - 時刻の設定（14 ページ）
   - 検出モード（14 ページ）
   - 自動バックアップ（15 ページ）
   - End User License Agreement（15 ページ）
3. 完了したら、[Apply] をクリックします。

   デバイスが選択内容に従って設定されます。管理者ロールを持つ `admin` ユーザとして Web インターフェイスにログインします。
4. デバイスからログアウトします。

   デバイスを FirePOWER Management Center に追加する準備が整いました。

(注) イーサネット ケーブルを使用してデバイスに直接接続している場合は、コンピュータの接続を切断して、デバイスの管理インターフェイスを管理ネットワークに接続します。デバイスの Web インターフェイスに常時アクセスする必要がある場合は、管理ネットワーク上のコンピュータのブラウザで、設定中に設定した IP アドレスまたはホスト名にアクセスします。

パスワードの変更

admin アカウントのパスワードを変更する必要があります。このアカウントは管理者特権が付与されているため、削除できません。

このパスワードを使用すると、admin ユーザはデバイスの Web インターフェイスとその CLI にログインできます。admin ユーザにはコンフィギュレーション CLI アクセス権が付与されます。Web インターフェイス用のいずれかのユーザ パスワードを変更すると、CLI のパスワードも変更されます(その逆も同様です)。

ネットワーク設定

デバイスのネットワーク設定によって、それが管理ネットワーク上で通信できるようになります。デバイスのネットワーク設定が完了している場合、このページのこのセクションは事前設定されていることがあります。

Firepower システム は、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。管理ネットワーク プロトコル([IPv4] 、[IPv6] 、または [Both])を指定する必要があります。選択した内容に応じて、設定のページにはさまざまなフィールドが表示されます。ここで IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィックスの長さ、およびデフォルトのゲートウェイを設定する必要があります。

- IPv4 の場合は、アドレスとネットマスクをドット付き 10 進法の形式(255.255.0.0 のネットマスクなど)で設定する必要があります。
- IPv6 ネットワークの場合は、[Assign the IPv6 address using router autoconfiguration] チェックボックスをオンにして IPv6 のネットワーク設定を自動的に割り当てることができます。このチェックボックスをオンにしない場合は、コロンで区切った 16 進形式のアドレスと、プレフィックスのビット数を設定する必要があります(プレフィックスの長さ 112 など)。

また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。

FirePOWER デバイスの LCD パネルの設定

LCD パネルを使用した FirePOWER デバイスのネットワーク設定の変更を許可するかどうかを選択します。

(注) このオプションを有効にすると、セキュリティ リスクが高まる可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。詳細については、『*Firepower 8000 Series Hardware Installation Guide*』の「Using the LCD Panel on a Firepower Device」を参照してください。

リモート管理

シスコ デバイスは FirePOWER Management Center を使用して管理する必要があります。この 2 段階プロセスでは、最初にデバイス上のリモート管理を設定してから、デバイスを FirePOWER Management Center に追加します。操作が簡単になるよう、設定ページでは、デバイスを管理元の FirePOWER Management Center に事前登録することができます。

[Register This Device Now] チェックボックスをオンにしたまま、管理元の FirePOWER Management Center の IP アドレスまたは完全修飾ドメイン名を [Management Host] として指定します。また、後でデバイスを FirePOWER Management Center に登録するときに使用する英数字の [Registration Key] を入力します。このキーは、長さが 37 文字以下で、ライセンス キーとは異なるシンプルなキーであることに注意してください。

デバイスと FirePOWER Management Center がネットワーク アドレス変換(NAT)デバイスによって分離されている場合は、初期設定が完了するまでデバイス登録を延期します。詳細については、『*Firepower Management Center 設定ガイド*』の「Managing Devices」の章を参照してください。

時刻の設定

デバイスの時刻は、手動で設定することも、FirePOWER Management Center を含むネットワーク タイム プロトコル（NTP）サーバから NTP 経由で設定することもできます。シスコ では、FirePOWER Management Center を管理対象デバイス用の NTP サーバとして使用することを推奨しています。

admin アカウントのローカル Web インターフェイスで使用するタイム ゾーンも指定できます。現在のタイム ゾーンをクリックして、ポップアップ ウィンドウを使用してそれを変更します。

検出モード

デバイスに対して検出モードを選択すると、システムが最初にデバイス インターフェイスをどのように設定するか、およびこれらのインターフェイスがインライン セットとセキュリティ ゾーンのどちらに属するかが決定されます。

検出モードはユーザが後から変更できない設定で、設定時にユーザが選択するだけのオプションです。このオプションの選択により、システムはデバイスの初期設定を調整して行うことができます。一般的には、デバイスがどのように展開されているかに基づいて検出モードを選択する必要があります。

- [パッシブ（Passive）]：デバイスが侵入検知システム（IDS）としてパッシブに展開されている場合、このモードを選択します。パッシブ展開では、ファイルとマルウェアの検出、セキュリティ インテリジェンスの監視、およびネットワーク ディスカバリ実行できます。
- [インライン（Inline）]：デバイスが侵入防御システムとしてインラインで展開されている場合、このモードを選択します。通常、侵入防御システムは *Fail Open* 型であり、一致しないトラフィックが*許可* されます。

  インライン展開では、ネットワーク向け AMP、ファイル制御、セキュリティ インテリジェンス フィルタリング、およびネットワーク検出も実行できます。

  すべてのデバイスに対してインライン モードを選択できますが、8000 シリーズ デバイスで非バイパス NetMod を使用したインライン セットはバイパス機能が欠如していることに留意してください。

(注) 再イメージ化はインライン展開内のデバイスを非バイパス設定にリセットします。これにより、バイパス モードを再設定するまで、ネットワーク上のトラフィックが中断されます。詳細については、復元プロセスにおけるトラフィック フロー（20 ページ）を参照してください。

- [アクセス制御（Access Control）]：デバイスがアクセス制御展開の一部としてインライン展開されている場合、つまり、アプリケーション、ユーザ、および URL 制御を実行する場合に、このモードを選択します。アクセス制御を実行するように設定されているデバイスは、通常、*フェールクローズ*であり、一致しないトラフィックを*ブロック*します。ルールで、通過させるトラフィックが明示的に指定されます。

  デバイスの特定のハードウェアベースの機能（（モデルによって異なる）高可用性、厳密な TCP の適用、ファストパス ルール、スイッチング、ルーティング、DHCP、NAT、VPN など）を使用する場合は、このモードも選択する必要があります

  アクセス制御展開では、ネットワーク向け AMP、ファイル制御、セキュリティ インテリジェンス フィルタリング、およびネットワーク検出も実行できます。

- [ネットワーク検出（Network Discovery）]：デバイスがパッシブ展開され、ホスト、アプリケーション、およびユーザ ディスカバリのみを実行する場合、このモードを選択します。

次の表は、選択した検出モードごとに、システムが作成するインターフェイス、インライン セット、およびゾーンを示しています。

表 1 検出モードに基づいた初期設定

検出モード	セキュリティ ゾーン	インライン セット	インターフェイス
インライン	内部と外部	デフォルトの インライン セット	最初のペアはデフォルト インライン セットへ追加される（1 つは内部ゾーン、もう 1 つは外部ゾーンへ追加される）
パッシブ	パッシブ	なし	パッシブ ゾーンに割り当てられた最初のペア
アクセス コントロール	なし	なし	なし
ネットワーク ディスカバリ	パッシブ	なし	最初のペアはパッシブ ゾーンへ割り当てられる

（注） セキュリティ ゾーンは、実際にデバイスが FirePOWER Management Center に登録されるまでシステムで作成されない FirePOWER Management Center レベルの設定です。登録時に、適切なゾーン（内部、外部、またはパッシブ）がすでに FirePOWER Management Center 上に存在していた場合は、登録プロセスによって、列挙されたインターフェイスが既存のゾーンに追加されます。ゾーンが存在しない場合は、システムがそれを作成してインターフェイスを追加します。インターフェイス、インライン セット、およびセキュリティ ゾーンの詳細については、『*Firepower Management Center 設定ガイド*』を参照してください。

自動バックアップ

デバイスはデータのアーカイブ メカニズムを備えているため、障害発生時に設定とイベント データを復元できます。初期設定の一部として、**自動バックアップを有効にする**ことができます。

この設定を有効にすると、デバイス上で設定の週次バックアップを作成する予定タスクが作成されます。

End User License Agreement

EULA をよく読んで、規定に従う場合はチェックボックスをオンにします。指定した情報がすべて正しいことを確認して、[Apply] をクリックします。デバイスが選択内容に応じて設定され、管理元の FirePOWER Management Center に追加する準備が整います。

CLI を使用した初期設定

オプションで、デバイスの Web インターフェイスを使用する代わりに、CLI を使用して FirePOWER デバイスを設定できます。

CLI からはデバイスの設定 Web ページと同じ設定情報の大部分が要求されることに注意してください。これらのオプションの詳細については、Web インターフェイスを使用した初期設定（12 ページ）を参照してください。

手順

1. デバイスにログインします。ユーザ名として `admin` を、パスワードとして `Admin123` を使用します。
   - モニタとキーボードが取り付けられたデバイスの場合は、コンソールからログインします。
   - イーサネット ケーブルを使用して、コンピュータをデバイスの管理インターフェイスに接続している場合は、インターフェイスのデフォルト IPv4 アドレス（192.168.45.45）に SSH を使用して接続します。

   直後に、デバイスから EULA を読むように要求されます。
2. EULA を読んで同意します。

3. admin アカウントのパスワードを変更します。このアカウントは管理者特権が付与されているため、削除できません。

   このパスワードを使用すると、admin ユーザはデバイスの Web インターフェイスとその CLI にログインできます。admin ユーザにはコンフィギュレーション CLI アクセス権が付与されます。Web インターフェイス用のいずれかのユーザ パスワードを変更すると、CLI のパスワードも変更されます(その逆も同様です)。

   シスコ では、大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することを推奨しています。辞書に掲載されている単語の使用は避けてください。詳細については、パスワードの変更(13 ページ)を参照してください。

4. デバイスのネットワーク設定を構成します。

   最初に IPv4 の管理設定を行い(または無効にして)、次に IPv6 を設定します。手動でネットワークの設定を指定する場合は、次のようにする必要があります。

   - IPv4 のアドレスを、ドット付き 10 進法形式でネットマスクを含めて入力します。たとえば、255.255.0.0 のネットマスクを指定できます。
   - IPv6 のアドレスを、コロンで区切った 16 進数の形式で入力します。IPv6 プレフィックスに対して、ビット数を指定します。たとえば、112 のプレフィックス長を指定します。

   詳細については、ネットワーク設定(13 ページ)を参照してください。設定が実装されたときに、コンソールにメッセージが表示される場合があります。

5. LCD パネルを使用したデバイスのネットワーク設定の変更を許可するかどうかを選択します。

注意:このオプションを有効にすると、セキュリティ リスクが高まる可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。詳細については、『*Firepower 8000 Series Hardware Installation Guide*』を参照してください。

6. デバイスの展開方法に基づいて検出モードを指定します。

   詳細については、検出モード(14 ページ)を参照してください。設定が実装されたときに、コンソールにメッセージが表示される場合があります。完了したら、このデバイスを FirePOWER Management Center に登録するよう要求され、CLI プロンプトが表示されます。

7. CLI を使用して、デバイスを管理元の FirePOWER Management Center に登録するには、次の項(CLI を使用した Management Center への FirePOWER デバイスの登録)に進みます。

   デバイスは FirePOWER Management Center で管理する必要があります。今すぐデバイスを登録しない場合は、後でデバイスにログインしてそれを登録するまで FirePOWER Management Center に追加できません。

8. デバイスからログアウトします。

CLI を使用した Management Center への FirePOWER デバイスの登録

シスコ では、CLI を使用して FirePOWER デバイスを設定した場合は、設定スクリプトの完了時点で、CLI を使用してデバイスを FirePOWER Management Center に登録することを推奨しています。初期設定プロセス中にデバイスを FirePOWER Management Center に登録する方が簡単です。これは、すでにデバイスの CLI にログインしているためです。

デバイスを登録するには、configure manager add コマンドを使用します。デバイスを FirePOWER Management Center に登録する場合は、一意の英数字登録キーが必須です。このキーは、長さが 37 文字以下で、ライセンス キーとは異なるシンプルなキーです。

ほとんどの場合、次のように、登録キーと一緒に FirePOWER Management Center のホスト名または IP アドレスを指定する必要があります。

```
configure manager add MC.example.com my_reg_key
```

ただし、デバイスと FirePOWER Management Center が NAT デバイスによって分離されている場合は、次のように、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに DONTRESOLVE を指定します。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

手順:

1. CLI Configuration アクセス レベルを持つユーザとしてデバイスにログインします。
   - コンソールから初期設定を実行している場合は、必要なアクセス レベルを持つ admin ユーザとしてすでにログインしています。
   - そうでない場合は、デバイスの管理 IP アドレスまたはホスト名に SSH を使用して接続します。
2. プロンプトで、次のような構文の configure manager add コマンドを使用してデバイスを FirePOWER Management Center に登録します。

   `configure manager add {`*`hostname`* `|` *`IPv4_address`* `|` *`IPv6_address`* `| DONTRESOLVE} `*`reg_key`* `[`*`nat_id`*`]`

   値は次のとおりです。

   {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE} は、FirePOWER Management Center の完全修飾ホスト名と IP アドレスのどちらかを指定します。FirePOWER Management Center が直接アドレス指定できない場合は、DONTRESOLVE を使用します。

   reg_key は、デバイスを FirePOWER Management Center に登録するために必要な、長さが 37 文字以下の一意の英数字登録キーです。

   nat_id は、FirePOWER Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。ホスト名が DONTRESOLVE に設定されている場合に必須です。
3. デバイスからログアウトします。

   デバイスを FirePOWER Management Center に追加する準備が整いました。

次の手順

アプライアンスの初期設定プロセスが完了し、正常に終了したことが確認できたら、シスコ では、展開での管理を容易にするためのさまざまな管理タスクを完了することを推奨しています。また、デバイスの登録やライセンスの取得など、初期設定で省略したタスクも完了する必要があります。以降のセクションで説明するタスクの詳細について、および展開の設定を始める方法については、『*Firepower Management Center 設定ガイド*』を参照してください。

(注) シリアル接続または LOM/SOL 接続を使用してアプライアンスのコンソールにアクセスする場合は、コンソール出力をリダイレクトする必要があります。『*Firepower 7000 Series Hardware Installation Guide*』の「Testing an Inline Bypass Interface Installation」を参照してください。特に LOM を使用する場合は、その機能を有効にするだけでなく、1 人以上の LOM ユーザも有効にする必要があります。LOM および LOM ユーザの有効化 (33 ページ) を参照してください。

個別のユーザ アカウント

初期セットアップを完了した時点で、システム上には管理者ロールおよびアクセス権を持つ admin ユーザしか存在しません。このロールを所有しているユーザは、シェルまたは CLI を介したアクセスを含め、システムのすべてのメニューおよび設定にアクセスできます。セキュリティおよび監査上の理由から、シスコ では、admin アカウント (および Administrator ロール) の使用を制限することを推奨しています。

システムを使用する各ユーザに対して個別のアカウントを作成すると、各ユーザによって行われたアクションと変更を組織で監査できるほか、各ユーザに関連付けられたユーザ アクセス ロールを制限することができます。これは、設定と分析タスクのほとんどを実行する FirePOWER Management Center では特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベント データにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。

システムには、さまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。また、特別なアクセス権限を持つカスタム ユーザ ロールを作成することもできます。

ヘルスとシステム ポリシー

デフォルトでは、すべてのアプライアンスにシステムの初期ポリシーが適用されます。システム ポリシーは、メール リレー ホストのプリファレンスや時間同期の設定など、展開内の複数のアプライアンスで共通している可能性が高い設定を管理します。シスコ では、FirePOWER Management Center を使用して、それ自身およびその管理対象デバイスすべてに同じシステム ポリシーを適用することを推奨しています。

デフォルトで、FirePOWER Management Center にはヘルス ポリシーも適用されます。ヘルス ポリシーは、ヘルス モニタリング機能の一部として、展開内のアプライアンスのパフォーマンスを継続的に監視するシステムの条件を提供します。シスコでは、FirePOWER Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアおよびデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。シスコでは、展開環境内のすべてのアプライアンスが Firepower システム の最新のバージョンを実行することを推奨しています。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。

注意：Firepower システムのいずれかの部分を更新する前に、更新に付属のリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。リリース ノートには、サポートされるプラットフォーム、互換性、前提条件、警告、および特定のインストールとアンインストールの手順などの重要な情報が記載されています。

コンソール出力のリダイレクト

デフォルトで、FirePOWER デバイスは、初期化ステータスまたは *init* メッセージを VGA ポートに出力します。物理シリアル ポートまたは SOL を使用してコンソールにアクセスする必要がある場合、初期セットアップの完了後にコンソール出力をシリアル ポートにリダイレクトすることをシスコでは推奨しています。

シェルを使用してコンソール出力をリダイレクトするには、アプライアンスのシェルからスクリプトを実行します。

コンソール出力をリダイレクトするシェルの使用

手順

1. キーボード/モニタまたはシリアル接続を使用し、管理者特権を持つアカウントでアプライアンスのシェルにログインします。パスワードは、アプライアンスの Web インターフェイスのパスワードと同じです。
2. `expert` と入力してシェル プロンプトを表示します。

   アプライアンスのプロンプトが表示されます。
3. プロンプトで、以下のコマンドのいずれかを入力して、コンソール出力を設定してください。
   - VGA を使用してアプライアンスにアクセスする場合は、次のコマンドを入力します。

     ```
     sudo /usr/local/sf/bin/configure_console.sh vga
     ```
   - 物理シリアル ポートを使用してアプライアンスにアクセスする場合は、次のコマンドを入力します。

     ```
     sudo /usr/local/sf/bin/configure_console.sh serial
     ```
   - SOL 経由で LOM を使用してアプライアンスにアクセスする場合は、次のコマンドを入力します。

     ```
     sudo /usr/local/sf/bin/configure_console.sh sol
     ```
4. 変更を反映させるには、「`sudo reboot`」と入力してアプライアンスをリブートします。

   アプライアンスがリブートします。

コンソール出力をリダイレクトする Web インターフェイスの使用

手順

1. [System] > [Configuration] を選択します。
2. [Console Configuration] を選択します。
3. リモート コンソール アクセスのオプションを選択します。
   - アプライアンスの VGA ポートを使用するには、[VGA] を選択します。これがデフォルトのオプションです。
   - アプライアンスのシリアル ポートを使用するか、8000 シリーズ デバイス上で LOM/SOL を使用する場合には、[Physical Serial Port] を選択します。

     LOM 設定が表示されます。
4. SOL 経由で LOM を設定するには、次の該当する設定値を入力します。
   - アプライアンスの DHCP 設定([DHCP] または [Static])
   - LOM に使用する [IP Address] LOM IP アドレスは、アプライアンスの管理インターフェイスの IP アドレスとは異なる必要があります。
   - アプライアンスの [Netmask]
   - アプライアンスのデフォルト ゲートウェイ
5. [Save(保存)] をクリックします。

アプライアンスのリモート コンソール構成が保存されます。Lights-Out 管理を構成した場合は、少なくとも 1 人のユーザに対してそれを有効にする必要があります。LOM および LOM ユーザの有効化(33 ページ)を参照してください。

デバイスの工場出荷時の初期状態への復元

シスコ のサポート サイトで、FirePOWER 管理対象デバイスの工場出荷時設定の復元と再イメージ化のための ISO イメージを提供しています。

詳細については、次の項を参照してください。

はじめる前に

アプライアンスの工場出荷時設定を復元する前に、復元プロセス中に予期されるシステムの動作を理解しておく必要があります。

設定およびイベントのバックアップのガイドライン

シスコ は、復元プロセスを開始する前に、アプライアンスに存在するバックアップ ファイルをすべて削除または移動してから、最新のイベントおよび設定データを外部ロケーションにバックアップすることを推奨します。

アプライアンスの工場出荷時設定を復元すると、アプライアンスのほぼ**すべての**設定とイベント データが失われます。復元ユーティリティはアプライアンスのライセンス、ネットワーク、コンソール、Lights-Out Management（LOM）の設定を保持できますが、復元プロセス完了後にその他のすべての設定タスクを実行する必要があります。

復元プロセスにおけるトラフィック フロー

ネットワークのトラフィック フローが中断されないようにするため、シスコ は、アプライアンスの復元を、保守期間中または中断により展開環境に及ぶ影響が最も少ない時間帯に行うことを推奨します。

インライン展開された FirePOWER デバイスを復元すると、デバイスは非バイパス（フェール クローズ）設定にリセットされ、ネットワーク上のトラフィックが中断します。デバイスでバイパス対応インライン セットを設定するまで、トラフィックはブロックされます。デバイス設定を編集してバイパスを設定する方法については、『*Firepower Management Center 設定ガイド*』の「Managing Devices」の章を参照してください。

復元プロセスについて

FirePOWER デバイスを復元するには、アプライアンスの内部フラッシュ ドライブから起動し、対話型メニューを使用して ISO イメージをアプライアンスにダウンロードしてインストールします。便宜上、復元プロセスの一環としてシステム ソフトウェアと侵入ルールの更新をインストールできます。

アプライアンスの再イメージ化は、必ず保守期間に実行してください。再イメージ化により、バイパス モードのアプリケーションは非バイパス設定にリセットされ、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、復元プロセスにおけるトラフィック フロー（20 ページ）を参照してください。

Web インターフェイスを使用してアプライアンスを復元することは**できない**ことに注意してください。アプライアンスを復元するには、次のいずれかの方法でアプライアンスに接続する必要があります。

キーボードとモニタ/KVM

アプライアンスに USB キーボードと VGA モニタを接続できます。これは、KVM（キーボード、ビデオ、マウス）スイッチに接続しているラックマウント型アプライアンスで便利です。リモートアクセス可能な KVM がある場合、物理的にアクセスできない状態でもアプライアンスを復元できます。

シリアル接続/ラップトップ

アプライアンスにコンピュータを接続するために、ロールオーバー シリアル ケーブル（別名ヌル モデム ケーブルまたは シスコ コンソール ケーブル）を使用できます。シリアル ポートの場所は、アプライアンスのハードウェア仕様を参照してください。アプライアンスと通信するには、HyperTerminal や Xmodem などの端末エミュレーション ソフトウェアを使用します。

Serial over LAN を使用した Lights-Out Management

Serial over LAN（SOL）接続による Lights-Out Management（LOM）を使用して、限定されたアクションのセットを Management Center と FirePOWER デバイス上で実行できます。アプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。LOM を使用してアプライアンスに接続した後で、物理シリアル接続を使用する場合と同様の方法で、復元ユーティリティに対してコマンドを発行します。Lights-Out Management は、デフォルト（`eth0`）の管理インターフェイスでのみ使用できることに注意してください。詳細については、Lights-Out Management の設定（31 ページ）を参照してください。

はじめる前に

- サポート サイトからアプライアンスの復元 ISO イメージを取得します。復元 ISO と更新ファイルの入手（21 ページ）を参照してください。

FirePOWER デバイスを復元する方法:

1. 適切なストレージ メディアにイメージをコピーします。
2. アプライアンスに接続します。
3. アプライアンスを再起動して、復元ユーティリティを起動します。

次の作業

- 復元プロセスの開始(22 ページ)の手順を使用して ISO イメージをインストールします。

復元 ISO と更新ファイルの入手

シスコ は、アプライアンスを元の工場出荷時設定に復元するための ISO イメージを提供しています。アプライアンスを復元する前に、サポート サイトから正しい ISO イメージを取得してください。

アプライアンスの復元に使用する ISO イメージは、そのアプライアンス モデルのサポートをシスコがいつ導入したかによって異なります。新しいアプライアンス モデルに対応するためにマイナー バージョンで ISO イメージがリリースされる場合を除き、ISO イメージは通常、システム ソフトウェアのメジャー バージョン(5.2、5.3 など)に関連付けられています。互換性のないバージョンのシステムをインストールしないようにするため、シスコ では、アプライアンスの最新 ISO イメージを常に使用することを推奨しています。

FirePOWER デバイスでは内部フラッシュ ドライブを使用してアプライアンスを起動します。これにより、復元ユーティリティを実行できます。

シスコ はまた、アプライアンスでサポートされる最新バージョンのシステム ソフトウェアを常に実行することを推奨します。アプライアンスをサポートされる最新メジャー バージョンに復元した後で、システム ソフトウェア、侵入ルール、脆弱性データベース(VDB)を更新する必要があります。詳細については、適用する更新のリリース ノートと『*Firepower Management Center 設定ガイド*』を参照してください。

便宜上、復元プロセスの一環としてシステム ソフトウェアと侵入ルールの更新をインストールできます。たとえば、デバイスをバージョン 6.0 に復元してから、この復元プロセスの一部としてさらにバージョン 6.0.0.1 に更新できます。ルール更新は Management Center だけで必要であることに注意してください。

復元 ISO とその他の更新ファイルを入手する方法:

1. サポート アカウントのユーザ名とパスワードを使用して、サポート サイト(https://sso.cisco.com/autho/forms/CDClogin.html)にログインします。
2. ソフトウェア ダウンロード セクション(https://software.cisco.com/download/navigator.html)を参照します。
3. ダウンロードしてインストールするシステム ソフトウェアで表示されるページの [Find] 領域に検索文字列を入力します。

   たとえば、FirePOWER のソフトウェア ダウンロードを検索するには、**Firepower** と入力します。
4. ダウンロードするイメージ(ISO イメージ)を見つけます。

   ページの左側にあるリンクの 1 つをクリックして、ページの該当するセクションを表示します。たとえば、Firepower システム バージョン 6.0 のイメージとリリース ノートを表示するには、[6.0 Images] をクリックします。
5. ダウンロードする ISO イメージをクリックします。

   ファイルのダウンロードが開始されます。
6. 管理ネットワーク上でアプライアンスがアクセスできる HTTP(Web)サーバ、FTP サーバ、または SCP 対応ホストにファイルをコピーします。

   FTP を使用する場合、ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、ユーザからの FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。詳細については、ご使用の FTP サーバのマニュアルを参照してください。

注意：電子メールを使用して ISO または更新ファイルを転送しないでください。このように転送すると、ファイルが破損することがあります。また、ファイルの名前を変更しないでください。復元ユーティリティでは、ファイル名がサポート サイトでの名前と同一であることが必要です。

復元プロセスの開始

内部フラッシュ ドライブからアプライアンスを起動して、復元プロセスを開始します。

アプライアンスへのアクセスと接続のレベルが適切であり、ISO イメージが正しいことを確認したら、次のいずれかの手順でアプライアンスを復元します。

- KVM または物理シリアル ポートを使用する復元ユーティリティの起動（22 ページ）では、LOM にアクセスできないアプライアンスでの復元プロセスの開始方法を説明します。
- Lights-Out Management を使用した復元ユーティリティの開始（23 ページ）では、SOL 接続を介し、LOM を使用して復元プロセスを開始する方法を説明します。

注意：この章の手順では、アプライアンスの電源をオフにせずにアプライアンスを復元する方法を説明します。ただし、何らかの理由で電源をオフにする必要がある場合は、アプライアンスの Web インターフェイス、FirePOWER デバイスの CLI の `system shutdown` コマンド、またはアプライアンスのシェル（エキスパート モードとも呼ばれます）の `shutdown -h now` コマンドを使用します。

KVM または物理シリアル ポートを使用する復元ユーティリティの起動

FirePOWER デバイスの場合、シスコ は内部フラッシュ ドライブに復元ユーティリティを提供します。

（注）アプライアンスは大容量ストレージ デバイスをブート デバイスとして使用する可能性があるため、初期セットアップのためにアプライアンスにアクセスするときには、KVM コンソールと一緒に USB 大容量ストレージを**使用しない**でください。

アプライアンスを工場出荷時設定に復元する必要があるが、物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。Lights-Out Management を使用した復元ユーティリティの開始（23 ページ）を参照してください。

復元ユーティリティを開始するには、次の手順を実行します。

1. キーボード/モニタまたはシリアル接続を使用し、管理者特権を持つアカウントでアプライアンスにログインします。パスワードは、アプライアンスの Web インターフェイスのパスワードと同じです。
2. アプライアンスをリブートします。FirePOWER デバイスで、次のように入力します。

   ```
   system reboot
   ```

   アプライアンスがリブートします。
3. 再起動の状況を監視します。
   - システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。

     ```
     The system is not operational yet. Checking and repairing database are in progress.
     This may take a long time to finish.
     ```
   - キーボードとモニタ接続の場合、アプライアンスが現在インストールされているバージョンのシステムを起動することを防ぐため、矢印キーの 1 つを素早く押します。
   - シリアル接続の場合、BIOS 起動オプションが表示されたら、Tab キーをゆっくりと繰り返し押します（アプライアンスが現在インストールされているバージョンのシステムを起動することを防ぐため）。LILO boot プロンプトが表示されます。次に例を示します。

     ```
     GNU/Linux - LILO 24 - Boot Menu
     6.1.0
     System_Restore
     Restore_Serial
     ```

4. システムを復元することを指定します。
   - キーボード/モニタ接続の場合、矢印キーを使用して [System_Restore] を選択し、Enter キーを押します。
   - シリアル接続の場合、プロンプトで **Restore_Serial** と入力し、Enter キーを押します。

   以下の選択項目の後に boot プロンプトが表示されます。

   ```
   0. Load with standard console
   1. Load with serial console
   ```

5. 復元ユーティリティの対話型メニューの表示モードを選択します。
   - キーボード/モニタ接続の場合、`0` と入力して Enter キーを押します。
   - シリアル接続の場合、`1` と入力して Enter キーを押します。

   表示モードを選ばない場合、復元ユーティリティは 30 秒後にデフォルトの標準コンソールを表示します。

   アプライアンスをこのメジャー バージョンに初めて復元する場合以外は、最後に使用した復元設定がユーティリティにより自動的に読み込まれます。続行するには、一連のページで設定を確認します。

6. Enter キーを押して、著作権表示を確認します。

次の作業

- 対話型メニューを使用したアプライアンスの復元（24 ページ）に進みます。

Lights-Out Management を使用した復元ユーティリティの開始

アプライアンスを工場出荷時設定に復元する必要があるが、アプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。初期設定を行うために LOM を使用する場合は、初期設定時にネットワーク設定を保持する**必要がある**ことに注意してください。また、Lights-Out Management は、デフォルト（`eth0`）の管理インターフェイスでのみ使用できることにも注意してください。

（注）LOM を使用してアプライアンスを復元する前に、LOM を有効にする必要があります。Lights-Out Management の設定（31 ページ）を参照してください。

Lights-Out Management を使用して復元ユーティリティを開始するには、次の手順を実行します。

1. コンピュータのコマンド プロンプトで、IPMI コマンドを入力して SoL セッションを開始します。

   IPMItool では次のように入力します。

   ```
   sudo ipmitool -I lanplus -H IP_address -U username sol activate
   ```

   ipmiutil では次のように入力します。

   ```
   sudo ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password
   ```

   IP_address はアプライアンスの管理インターフェイスの IP アドレス、*username* は承認済み LOM アカウントのユーザ名、*password* はそのアカウントのパスワードです。IPMItool では、**sol activate** コマンドの発行後にパスワードの入力が求められることに注意してください。

   FirePOWER デバイスを使用している場合は、**expert** と入力して、シェル プロンプトを表示します。

2. root ユーザとしてアプライアンスをリブートします。FirePOWER デバイスで、次のように入力します。

   ```
   system reboot
   ```

   アプライアンスがリブートします。

3. 再起動状況の監視

   システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。

   ```
   The system is not operational yet. Checking and repairing database are in progress.
   This may take a long time to finish.
   ```

   BIOS 起動オプションが表示されたら、LILO boot プロンプトが表示されるまで Tab キーをゆっくりと繰り返し押します(アプライアンスが現在インストールされているバージョンのシステムを起動することを防ぐため)。次に例を示します。

   ```
   GNU/Linux - LILO 24 - Boot Menu
   6.1.0
   System_Restore
   Restore_Serial
   ```

4. boot プロンプトで **Restore_Serial** と入力して、復元ユーティリティを開始します。

   以下の選択項目の後に boot プロンプトが表示されます。

   ```
   0. Load with standard console
   1. Load with serial console
   ```

5. 1 と入力して Enter キーを押します。アプライアンスのシリアル接続を介して対話型の復元メニューが読み込まれます。

(注) 表示モードを選ばない場合、復元ユーティリティは 30 秒後にデフォルトの標準コンソールを表示します。

アプライアンスをこのメジャー バージョンに初めて復元する場合以外は、最後に使用した復元設定がユーティリティにより自動的に読み込まれます。続行するには、一連のページで設定を確認します。

6. Enter キーを押して、著作権表示を確認します。

次の作業

- 対話型メニューを使用したアプライアンスの復元(24 ページ)に進みます。

対話型メニューを使用したアプライアンスの復元

FirePOWER デバイスの復元ユーティリティでは、対話型メニューによって復元処理を進められます。

(注) アプライアンスの再イメージ化は、必ず保守期間中に行ってください。再イメージ化により、バイパス モードのアプリケーションは非バイパス設定にリセットされ、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、復元プロセスにおけるトラフィック フロー(20 ページ)を参照してください。

メニューに表示されるオプションを次の表に示します。

表 2 復元メニューのオプション

オプション	説明	詳細情報の参照先
1 IP Configuration	復元するアプライアンスの管理インターフェイスに関するネットワーク情報を指定します。これにより、ISO および更新ファイルを格納したサーバとアプライアンスが通信できるようになります。	アプライアンスの管理インターフェイスの指定(26 ページ)
2 Choose the transport protocol	アプライアンスを復元するために使用する ISO イメージの場所と、アプライアンスでファイルのダウンロードに必要なすべての資格情報を指定します。	ISO イメージの場所および転送方式の指定(26 ページ)
3 Select Patches/Rule Updates	アプライアンスを ISO イメージのベース バージョンに復元した後で適用するシステム ソフトウェアおよび侵入ルールの更新を指定します。	復元時のシステム ソフトウェアおよび侵入ルールの更新(27 ページ)

表 2　復元メニューのオプション(続き)

オプション	説明	詳細情報の参照先
4 Download and Mount ISO	適切な ISO イメージと、システム ソフトウェアまたは侵入ルールの更新をダウンロードします。ISO イメージをマウントします。	ISO および更新ファイルのダウンロードとイメージのマウント(28 ページ)
5 Run the Install	復元プロセスを開始します。	復元プロセスの開始(28 ページ)
6 Save Configuration 7 Load Configuration	後で使用できるように復元設定のセットを保存するか、または保存されているセットを読み込みます。	復元設定の保存とロード(30 ページ)
8 Wipe Contents of Disk	ハード ドライブの内容に今後アクセスできないようにするため、ハード ドライブのスクラビング処理を確実に実行します。	ハード ドライブのスクラビング(34 ページ)

メニュー内の移動には矢印キーを使用します。メニュー オプションを選択するには、上下矢印キーを使用します。ページ下部にある [OK] ボタンと [Cancel] ボタンの切り替えには、左右矢印キーを使用します。

メニューには、2 種類のオプションが表示されます。

- 番号付きオプションを選択するには、最初に上下矢印キーを使用して正しいオプションを強調表示してから、ページ下部で [OK] ボタンが強調表示されている状態で Enter キーを押します。
- 複数項目オプション(オプション ボタン)を選択する場合は、最初に上下矢印キーを使用して正しいオプションを強調表示してから、スペース バーを押して、そのオプションに [X] のマークを付けます。選択内容を受け入れるには、[OK] ボタンが強調表示されている状態で Enter キーを押します。

ほとんどの場合、メニュー オプション **1**、**2**、**4**、および **5** をこの順序で実行します。オプションで、メニュー オプション **3** を追加して、復元プロセスでシステム ソフトウェアおよび侵入ルールの更新をインストールします。

アプライアンスに現在インストールされているバージョンとは異なるメジャー バージョンにアプライアンスを復元する場合は、2 パス復元プロセスが必要です。1 回目のパスでオペレーティング システムを更新し、2 回目のパスでシステム ソフトウェアの新しいバージョンをインストールします。

これが 2 回目のパスであるか、または使用する復元設定が復元ユーティリティにより自動的に読み込まれる場合は、メニュー オプション **4**:ISO および更新ファイルのダウンロードとイメージのマウント(28 ページ)から開始できます。ただし シスコ は、操作を続行する前に復元設定の内容をダブルチェックすることを推奨しています。

(注) 以前に保存した設定を使用するには、メニュー オプション **6**:復元設定の保存とロード(30 ページ)から開始します。設定を読み込んだら、メニュー オプション **4**:ISO および更新ファイルのダウンロードとイメージのマウント(28 ページ)に進みます。

対話型メニューを使用してアプライアンスを復元するには、次の手順を使用してください。

1. **1 IP Configuration**:アプライアンスの管理インターフェイスの指定(26 ページ)を参照してください。
2. **2 Choose the transport protocol**:ISO イメージの場所および転送方式の指定(26 ページ)を参照してください。
3. **3 Select Patches/Rule Updates**(オプション):復元時のシステム ソフトウェアおよび侵入ルールの更新(27 ページ)を参照してください。
4. **4 Download and Mount ISO**:ISO および更新ファイルのダウンロードとイメージのマウント(28 ページ)を参照してください。
5. **5 Run the Install**:復元プロセスの開始(28 ページ)を参照してください。

アプライアンスの管理インターフェイスの指定

復元ユーティリティを実行する際には、最初に復元するアプライアンスの管理インターフェイスを指定します。これにより、ISO および更新ファイルをコピーしたサーバとアプライアンスが通信できるようになります。LOM を使用する場合は、アプライアンスの管理 IP アドレスが LOM IP アドレス**ではない**ことに注意してください。

アプライアンスの管理インターフェイスを指定するには:

1. メイン メニューで、[1 IP Configuration] を選択します。
2. アプライアンスの管理インターフェイス（通常は [th0]）を選択します。
3. 管理ネットワークに使用するプロトコル（[IPv4] または [IPv6]）を選択します。

   管理インターフェイスに IP アドレスを割り当てるためのオプションが表示されます。
4. 管理インターフェイスに IP アドレスを割り当てる方法（[Static] または [DHCP]）を選択します。
   - [Static] を選択した場合は、一連のページで、管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイを手動で入力するよう促されます。
   - [DHCP] を選択した場合は、管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイがアプライアンスにより自動的に検出され、IP アドレスが表示されます。
5. プロンプトが表示されたら、設定を確認します。

   プロンプトが表示されたら、アプライアンスの管理インターフェイスに割り当てられている IP アドレスを確認します。

次の作業

- 次の項（ISO イメージの場所および転送方式の指定）に進みます。

ISO イメージの場所および転送方式の指定

復元プロセスで必要なファイルをダウンロードするために使用される管理 IP アドレスを設定したら、次にアプライアンスの復元に使用する ISO イメージを指定する必要があります。これは、サポート サイト（復元 ISO と更新ファイルの入手（21 ページ）を参照）からダウンロードし、Web サーバ、FTP サーバ、または SCP 対応ホストに保存した ISO イメージです。

対話型メニューで、ダウンロードを実行するために必要な情報の入力が求められます。これらの情報を次の表に示します。

表 3 復元ファイルのダウンロードに必要な情報

使用する方式	指定する必要がある情報
HTTP	■ Web サーバの IP アドレス ■ ISO イメージ ディレクトリのフル パス（例：`/downloads/ISOs/`）
FTP	■ FTP サーバの IP アドレス ■ 資格情報が使用されるユーザのホーム ディレクトリを基準にした ISO イメージ ディレクトリの相対パス（例：`mydownloads/ISOs/`） ■ FTP サーバの認証ユーザ名とパスワード **（注）** FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、ユーザからの FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。詳細については、ご使用の FTP サーバのマニュアルを参照してください。

表 3 復元ファイルのダウンロードに必要な情報

使用する方式	指定する必要がある情報
SCP	■ SCP サーバの IP アドレス ■ SCP サーバの認証ユーザ名 ■ ISO イメージ ディレクトリのフル パス ■ 先に入力したユーザ名のパスワード パスワードを入力する前に、アプライアンスから、信頼できるホストのリストに SCP サーバを追加するよう求められることがある点に注意してください。続行するには、同意する必要があります。

復元ユーティリティは、ISO イメージ ディレクトリ内でも更新ファイルを検索することに注意してください。

復元ファイルの場所および転送方式を指定するには:

1. メイン メニューで、[2 トランスポート プロトコルの選択(2 Choose the transport protocol)] を選択します。
2. 表示されるページで、[HTTP]、[FTP]、または [SCP] を選択します。

   FTP を使用する場合、ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、ユーザからの FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。詳細については、ご使用の FTP サーバのマニュアルを参照してください。
3. 復元ユーティリティにより表示される一連のページで、表 3 の説明に従い選択したプロトコルに必要な情報を入力します。

   情報が正しければ、アプライアンスはサーバに接続し、指定された場所の シスコ ISO イメージのリストを表示します。
4. 使用する ISO イメージを選択します。
5. プロンプトが表示されたら、設定を確認します。
6. 復元プロセス中にシステム ソフトウェアまたは侵入ルールの更新をインストールしますか?
   - インストールする場合は、次の項(復元時のシステム ソフトウェアおよび侵入ルールの更新)に進みます。
   - インストールしない場合は、ISO および更新ファイルのダウンロードとイメージのマウント(28 ページ)に進みます。復元プロセスが完了したら、システムの Web インターフェイスを使用して手動で更新をインストールできることに注意してください。

復元時のシステム ソフトウェアおよび侵入ルールの更新

オプションで、アプライアンスを ISO イメージのベース バージョンに復元した後で、復元ユーティリティを使用してシステム ソフトウェアおよび侵入ルールを更新できます。ルール更新は Management Center だけで必要となることに注意してください。

復元ユーティリティは、1 つのシステム ソフトウェア更新と 1 つのルール更新だけを使用できます。ただしシステム更新は直前のメジャー バージョンに対して累積されます。ルール更新も累積されます。シスコ では、ご使用のアプライアンスに対して使用可能な最新の更新を入手することを推奨します。復元 ISO と更新ファイルの入手(21 ページ)を参照してください。

復元プロセスでアプライアンスを更新しないことを選択した場合、後でシステムの Web インターフェイスを使用して更新できます。詳細については、インストールする更新のリリース ノート、および『*Firepower Management Center 設定ガイド*』の「Updating System Software」の章を参照してください。

復元プロセスの一環として更新をインストールするには、次の手順を実行します。

1. メイン メニューで [3 パッチ/ルール更新の選択（3 Select Patches/Rule Updates）] を選択します。

   復元ユーティリティは、前の手順（ISO イメージの場所および転送方式の指定（26 ページ）を参照）で指定した場所とプロトコルを使用して、その場所にあるすべてのシステム ソフトウェア更新ファイルのリストを取得して表示します。SCP を使用する場合、更新ファイル リストを表示するためのプロンプトが表示されたらパスワードを入力します。

2. 使用するシステム ソフトウェア更新がわかっている場合は、それを選択します。

   更新を選択しなくてもかまいません。続行するには、更新を選択せずに Enter キーを押します。適切な場所にシステム ソフトウェア更新がない場合は、Enter キーを押して続行するよう求められます。

   復元ユーティリティは、ルール更新ファイルのリストを取得して表示します。SCP を使用する場合、リストを表示するためのプロンプトが表示されたらパスワードを入力します。

3. 使用するルール更新がわかっている場合は、それを選択します。

   更新を選択しなくてもかまいません。続行するには、更新を選択せずに Enter キーを押します。適切な場所にルール更新がない場合は、Enter キーを押して続行するよう求められます。

次の作業

- 次の項（ISO および更新ファイルのダウンロードとイメージのマウント）に進みます。

ISO および更新ファイルのダウンロードとイメージのマウント

復元プロセスを呼び出す前の最後の手順として、必要なファイルをダウンロードして ISO イメージをマウントします。

はじめる前に

- この手順を開始する前に、復元設定を後で使用できるように保存しておくことをお勧めします。詳細については、復元設定の保存とロード（30 ページ）を参照してください。

ISO イメージをダウンロードしてマウントするには：

1. メイン メニューで [4 ISO のダウンロードとマウント（4 Download and Mount ISO）] を選択します。
2. プロンプトが表示されたら、選択項目を確認します。SCP サーバからダウンロードする場合は、プロンプトが表示されたらパスワードを入力します。

   該当するファイルがダウンロードされ、マウントされます。

次の作業

- 次の項（復元プロセスの開始）に進みます。

復元プロセスの開始

ISO イメージをダウンロードしてマウントしたら、復元プロセスを開始できます。アプライアンスに現在インストールされているバージョンとは異なるメジャー バージョンにアプライアンスを復元する場合は、2 パス復元プロセスが必要です。1 回目のパスでオペレーティング システムを更新し、2 回目のパスでシステム ソフトウェアの新しいバージョンをインストールします。

2 つのパスのうちの 1 回目のパス（メジャー バージョンの変更のみ）

アプライアンスを異なるメジャー バージョンに復元する場合は、復元ユーティリティによる 1 回目のパスではアプライアンスのオペレーティング システムと、必要に応じて復元ユーティリティ自体が更新されます。

(注) アプライアンスを同じメジャー バージョンに復元する場合、またはこれがこのプロセスの 2 回目のパスの場合は、次の手順(2 回目のパス、および 1 つのパスのみ(29 ページ))に進みます。

2 パス復元プロセスの 1 回目のパスを実行するには、次の手順を実行します。

1. メイン メニューで [5 Run the Install] を選択します。
2. プロンプトが表示されたら(2 回)、アプライアンスを再起動することを確認します。
3. 再起動を監視し、復元プロセスを再度開始します。

   システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。

   ```
   The system is not operational yet. Checking and repairing database are in progress.
   This may take a long time to finish.
   ```

   キーボードとモニタ接続の場合、アプライアンスが現在インストールされているバージョンのシステムを起動することを防ぐため、矢印キーの 1 つを素早く押します。

   シリアル接続または SOL/LOM 接続の場合、BIOS ブート オプションが表示されたら、LILO boot プロンプトが表示されるまで、Tab キーをゆっくりと繰り返し押します。次に例を示します。

   ```
   GNU/Linux - LILO 24 - Boot Menu
   6.1.0
   System_Restore
   Restore_Serial
   ```

4. システムを復元することを指定します。
   - キーボード/モニタ接続の場合、矢印キーを使用して [System_Restore] を選択し、Enter キーを押します。
   - シリアル接続の場合、プロンプトで **Restore_Serial** と入力し、Enter キーを押します。

   ```
   0. Load with standard console
   1. Load with serial console
   ```

5. 復元ユーティリティの対話型メニューの表示モードを選択します。
   - キーボード/モニタ接続の場合、0 と入力して Enter キーを押します。
   - シリアル接続または SOL/LOM 接続の場合、1 と入力して Enter キーを押します。

   表示モードを選ばない場合、復元ユーティリティは 30 秒後にデフォルトの標準コンソールを表示します。

   アプライアンスをこのメジャー バージョンに初めて復元する場合以外は、最後に使用した復元設定がユーティリティにより自動的に読み込まれます。続行するには、一連のページで設定を確認します。

6. Enter キーを押して、著作権表示を確認します。

次の作業

- 対話型メニューを使用したアプライアンスの復元(24 ページ)から開始して、プロセスの 2 回目のパスを開始します。

2 回目のパス、および 1 つのパスのみ

復元プロセスの 2 回目のパスまたは 1 つだけのパスを実行するには、次の手順を使用します。

復元プロセスの 2 回目のパスまたは 1 つだけのパスを実行するには:

1. メイン メニューで [5 インストールの実行(5 Run the Install)] を選択します。
2. アプライアンスを復元することを確認し、次のステップに進みます。

3. アプライアンスのライセンスおよびネットワーク設定を削除するかどうかを選択します。これらの設定を削除すると、表示(コンソール)および LOM の設定もリセットされます。

   ほとんどの場合、初期設定プロセスが短くなる可能性があるため、これらの設定は削除しないでください。復元とそれに続く初期設定の後に設定を変更する場合、通常は、それらの設定を今リセットするよりも時間がかかりません。詳細については、次の手順(31 ページ)を参照してください。

注意:LOM 接続を使用してアプライアンスを復元する場合には、ネットワーク設定を削除しないでください。アプライアンスをリブートした後は、LOM 経由で再接続できません。

4. アプライアンス復元の最終確認を入力します。

   復元プロセスの最終段階が開始されます。完了し、プロンプトが表示されたら、アプライアンスを再起動することを確認します。

注意:復元プロセスが完了するまで十分な時間をおいてください。内部フラッシュ ドライブを備えたアプライアンスでは、ユーティリティは最初にフラッシュ ドライブを更新し、その後このフラッシュ ドライブを使用して他の復元タスクが実行されます。フラッシュ更新中に(Ctrl + C を押す操作などにより)終了すると、回復不能なエラーが発生する可能性があります。復元にかかる時間が長すぎる場合、または復元プロセスに関連する他の問題が発生している場合は、終了しないでください。代わりに、サポートに連絡してください。

(注) 再イメージ化により、バイパス モードのアプリケーションは非バイパス設定にリセットされ、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、復元プロセスにおけるトラフィック フロー(20 ページ)を参照してください。

次の作業

- 次の手順(31 ページ)に進みます。

復元設定の保存とロード

復元ユーティリティを使用して復元設定を保存できます。復元設定は、FirePOWER デバイスを再び復元する必要が生じた場合に使用します。復元ユーティリティは最後に使用された設定を自動的に保存しますが、次のような複数の設定を保存することもできます。

- アプライアンスの管理インターフェイスに関するネットワーク情報。アプライアンスの管理インターフェイスの指定(26 ページ)を参照してください。
- 復元 ISO イメージの場所と、アプライアンスがファイルをダウンロードするために必要とする転送プロトコルおよび資格情報。ISO イメージの場所および転送方式の指定(26 ページ)を参照してください。
- アプライアンスを ISO イメージのベース バージョンに復元した後で適用するシステム ソフトウェアと侵入ルールの更新(存在する場合)。復元時のシステム ソフトウェアおよび侵入ルールの更新(27 ページ)を参照してください。

SCP パスワードは保存されません。ユーティリティがアプライアンスに ISO やその他のファイルを転送するときに SCP を使用する必要があることが設定で指定されている場合は、復元プロセスを実行するためにサーバに対して再度認証を行う必要があります。

復元設定を保存するのに最適な時点は、上記の情報の指定後、ISO イメージをダウンロードしてマウントする前です。

復元設定を保存するには、次の手順を実行します。

1. 復元ユーティリティのメイン メニューから、[6 設定の保存(6 Save Configuration)] を選択します。

   ユーティリティにより、保存する設定の設定内容の設定が表示されます。
2. プロンプトが表示されたら、設定を保存することを確認します。
3. プロンプトが表示されたら、設定の名前を入力します。

次の作業

- 保存された設定を使用してアプライアンスを復元する場合は、ISO および更新ファイルのダウンロードとイメージのマウント（28 ページ）に進みます。

復元設定を読み込むには、次の手順を実行します。

1. メイン メニューで、[7 設定の読み込み（7 Load Configuration）] を選択します。

   ユーティリティにより、保存されている復元設定のリストが表示されます。1 番目のオプション [default_config] は、最後にアプライアンスを復元する際に使用した設定です。その他のオプションは、これまでに保存した復元設定です。

2. 使用する設定を選択します。

   ユーティリティにより、読み込む設定の設定内容が表示されます。

3. プロンプトが表示されたら、設定を読み込むことを確認します。

   設定が読み込まれます。プロンプトが表示されたら、アプライアンスの管理インターフェイスに割り当てられている IP アドレスを確認します。

次の作業

- 読み込まれた設定を使用してアプライアンスを復元する場合は、ISO および更新ファイルのダウンロードとイメージのマウント（28 ページ）に進みます。

次の手順

アプライアンスの工場出荷時設定を復元すると、アプライアンスのほぼ**すべての**設定とイベント データ（インライン展開されたデバイスのバイパス設定を含む）が失われます。詳細については、復元プロセスにおけるトラフィック フロー（20 ページ）を参照してください。

アプライアンスの復元後に、初期設定プロセスを実行する必要があります。

- アプライアンスのライセンスおよびネットワーク設定を削除していない場合は、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを直接参照し、設定を実行できます。詳細については、Web インターフェイスを使用した初期設定（12 ページ）を参照してください。
- ライセンスとネットワーク設定を削除している場合は、アプライアンスを新品の場合と同様に設定する必要があります。最初に、管理ネットワークと通信するように設定します。FirePOWER 8000 シリーズ デバイスの取り付け（9 ページ）を参照してください。

ライセンスおよびネットワーク設定を削除すると、表示（コンソール）設定と LOM 設定もリセットされることに注意してください。初期設定プロセスの完了後：

- シリアル接続または SOL/LOM 接続を使用してアプライアンスのコンソールにアクセスする場合は、コンソール出力をリダイレクトする必要があります。『*Firepower 8000 Series Hardware Installation Guide*』の「Testing an Inline Bypass Interface Installation」を参照してください。
- LOM を使用する場合は、機能を再度有効にし、1 つ以上の LOM ユーザを有効にします。LOM および LOM ユーザの有効化（33 ページ）を参照してください。

Lights-Out Management の設定

FirePOWER デバイスを工場出荷時設定に復元する必要があるが、アプライアンスに物理的にアクセスできない場合は、Lights-Out Management（LOM）を使用して復元プロセスを実行できます。Lights-Out Management は、デフォルト（`eth0`）の管理インターフェイスでのみ使用できることに注意してください。

(注) FirePOWER 71xx、FirePOWER 82xx、または FirePOWER または AMP 83xx デバイスのベースボード管理コントローラ(BMC)は、ホストの電源がオンのときにのみ 1Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

LOM 機能により、Serial over LAN(SOL)の接続を使用して、FirePOWER デバイスに対して限定されたアクションのセットを実行できます。LOM では、アウトオブバンド管理接続でコマンド ライン インターフェイスを使用して、シャーシ シリアル番号の確認や、ファン速度や温度などの状況の監視といった作業を行うことができます。

LOM コマンドの構文は、使用しているユーティリティにより異なりますが、通常 LOM コマンドには、次の表に示す要素が含まれています。

表 4 LOM コマンド構文

IPMItool (Linux/Mac)	ipmiutil (Windows)	説明
ipmitool	ipmiutil	IPMI ユーティリティを起動します。
n/a	v4	ipmiutil のみ。LOM セッションで管理特権を有効にします。
-I lanplus	-J3	LOM セッションの暗号化を有効にします。
-H *IP_address*	-N *IP_address*	アプライアンスの管理インターフェイスの IP アドレスを指定します。
-U *username*	-U *username*	承認済み LOM アカウントのユーザ名を指定します。
n/a(ログオン時に求められます)	-P *password*	ipmiutil のみ。承認済み LOM アカウントのパスワードを指定します。
command	command	アプライアンスに対して発行するコマンド。コマンドを発行する場所は、ユーティリティによって異なります。 ■ IPMItool の場合、コマンドは最後に入力します。 ■ ipmiutil の場合、コマンドは最初に入力します。

IPMItool の場合:

```
ipmitool -I lanplus -H IP_address -U username command
```

ipmiutil の場合:

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

`chassis power off` コマンドと `chassis power cycle` コマンドは 70xx ファミリ アプライアンスでは無効であることに注意してください。Firepower システムでサポートされる LOM コマンドの完全なリストについては、『*Firepower Management Center 設定ガイド*』の「Configuring Appliance Settings」の章を参照してください。

(注) 電源の再投入のシナリオによっては、管理インターフェイス経由でネットワークに接続された FirePOWER 7050 のベースボード管理コントローラ(BMC)は、DHCP サーバによって割り当てられた IP アドレスを消失する可能性があります。このため、シスコ では FirePOWER 7050 BMC を静的 IP アドレスで設定することを推奨しています。ネットワーク ケーブルの切断と再接続やデバイスの電力遮断と再投入により、リンクの再ネゴシエーションを強制的に行うことができます。

LOM を使用してアプライアンスを復元するには、その前に、アプライアンスと復元を実行するユーザの両方に対して LOM を有効にする必要があります。次に、サードパーティの Intelligent Platform Management Interface(IPMI)ユーティリティを使用して、アプライアンスにアクセスします。また、アプライアンスのコンソール出力をシリアル ポートにリダイレクトしていることも確認する必要があります。

詳細については、次の項を参照してください。

- LOM および LOM ユーザの有効化（33 ページ）
- IPMI ユーティリティのインストール（33 ページ）

LOM および LOM ユーザの有効化

LOM を使用してアプライアンスを復元するには、その前に、この機能を有効にして設定する必要があります。この機能を使用するユーザに対して LOM 権限を明示的に付与する必要もあります。

各アプライアンスのローカル Web インターフェイスを使用して、アプライアンスごとに LOM と LOM ユーザを設定します。つまり、Management Center を使用して FirePOWER デバイスで LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、Management Center で LOM 対応ユーザを有効化または作成しても、FirePOWER デバイスのユーザにはその機能が伝達されません。

LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名には最大で 16 文字の英数字を使用できます。LOM ユーザに対し、ハイフンとこれよりも長いユーザ名はサポートされていません。
- パスワードには、最大で 20 文字の英数字を使用できます。LOM ユーザに対し、これよりも長いパスワードはサポートされていません。ユーザの LOM パスワードは、そのユーザのシステム パスワードと同じです。
- 8000 シリーズ デバイスには、最大 13 人の LOM ユーザを設定できます。

  （注）以下の作業の詳細については、『*Firepower Management Center 設定ガイド*』の「Configuring Appliance Settings」の章を参照してください。

LOM を有効にするには、次の手順を実行します。

1. [System] > [Configuration] を選択し、[Console Configuration] をクリックします。
2. [Physical Serial Port] を使用してリモート アクセスを有効にしてから、LOM IP アドレス、ネットマスク、およびデフォルト ゲートウェイを指定します（または DHCP を使用してこれらの値を自動的に割り当てます）。

   （注）LOM IP アドレスは、アプライアンスの管理インターフェイスの IP アドレスとは異なる必要があります。

Firepower システム ユーザに対して LOM 機能を有効にするには：

1. [System] > [User Management] を選択し、既存のユーザを編集して LOM 許可を追加するか、またはアプライアンスへの LOM アクセスに使用する新規ユーザを作成します。
2. [ユーザ設定（User Configuration）] ページで、[管理者（Administrator）] ロールがまだ有効になっていない場合は、このロールを有効にします。
3. [Allow Lights-Out Management Access] チェックボックスをオンにし、変更を保存します。

IPMI ユーティリティのインストール

アプライアンスへの SOL 接続を作成するには、コンピュータでサードパーティ IPMI ユーティリティを使用します。

Linux または Mac OS が稼働しているコンピュータでは、IPMItool を使用します。IPMItool は多くの Linux ディストリビューションで標準ですが、Mac には IPMItool をインストールする必要があります。最初に、Apple の xCode 開発ツール パッケージが Mac にインストールされていることを確認します。コマンドライン開発のためのオプション コンポーネント（新しいバージョンでは「UNIX Development」および「System Tools」、古いバージョンでは「Command Line Support」）がインストールされていることも確認します。最後に、MacPorts および IPMItool をインストールします。詳細については、検索エンジンを使用するか、または次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows 環境では ipmiutil を使用します。このツールは各自でコンパイルする必要があります。コンパイラにアクセスできない場合は、ipmiutil 自体を使用してコンパイルできます。詳細については、検索エンジンを使用するか、または次のサイトを参照してください。

`http://ipmiutil.sourceforge.net/`

ハード ドライブのスクラビング

Management Center および FirePower デバイスのハード ドライブを安全にスクラビングして、その内容にアクセスできないようにすることができます。たとえば、機密データが含まれている故障したアプライアンスを返却する必要がある場合は、この機能を使用してデータを上書きできます。

ディスクのスクラビング処理を行うこのモードは、次の軍用標準規格に準拠しています。

標準規格

DoD スクラブ シーケンスは、着脱可能または着脱不可能なリジッド ディスクのサニタイズに関する DoD 5220.22-M 手順に準拠しています。この手順では、すべてのアドレス可能な場所を 1 つの文字で上書きし、その補数の文字で上書きし、さらにランダムな文字コードで上書き処理を行う必要があります。その他の制約については、DoD の資料を参照してください。

注意:ハード ドライブのスクラビング処理では、アプライアンスのすべてのデータが失われ、動作不能になります。

ハード ドライブのスクラビングは、対話型メニューを使用したアプライアンスの復元（24 ページ）で説明されているインタラクティブ メニューのオプションを使用して行います。

ハード ドライブのスクラビング処理を行うには、次の手順を実行します。

1. 以下のいずれかの項の説明に従い、復元ユーティリティの対話型メニューを表示します。これは、アプライアンスへのアクセス方法に応じて異なります。
   - KVM または物理シリアル ポートを使用する復元ユーティリティの起動（22 ページ）
   - Lights-Out Management を使用した復元ユーティリティの開始（23 ページ）
2. メイン メニューで、[8 ディスクの内容を消去（8 Wipe Contents of Disk）] を選択します。
3. プロンプトが表示されたら、ハード ドライブをスクラビング処理することを確認します。

ハード ドライブがスクラビング処理されます。スクラビング処理プロセスが完了するまでに数時間かかることがあります。ドライブの容量が大きいほど、時間がかかります。

関連資料