Firepower 8000 シリーズ ハードウェア 設置ガイド

初版:2016 年 7 月 22 日
最終更新日:2018 年 7 月 12 日

Cisco Systems, Inc.
www.cisco.com
シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号は以下のシスコ Web サイトを
ご覧ください。
(www.cisco.com/go/offices) をご覧ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルについて

更新:2016 年 7 月 22 日

このマニュアルは、Cisco Firepower 8000 シリーズアプライアンスの設置と設定の方法について説明します。このガイドに記載されている情報は、Cisco 80xx ファミリ、81xx ファミリ、および 83xx ファミリモデルに適用されます。

この前書きは、次の項で構成されています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	役職（Title）	説明
第 1 章	Firepower 8000 シリーズについて	8000 シリーズに含まれているデバイスの概要について説明します。
第 2 章	ハードウェア仕様	Firepower 8000 シリーズモデルのハードウェア仕様について説明します。
第 3 章	Firepower 8000 シリーズデバイスの設置	ラックに Firepower 8000 シリーズデバイスを設置する方法、管理インターフェイスを接続する方法、およびシャーシの電源を入れる方法について説明します。
第 4 章	Firepower デバイス上の LCD パネルの使用	システムの Web インターフェイスの代わりに、デバイス前面の LCD パネルを使用して、デバイス情報を表示したり、特定の設定を構成したりする方法について説明します。

章	役職（Title）	説明
第 5 章	管理ネットワークでの展開	固有のネットワーク アーキテクチャのニーズに応じて使用可能な Firepower システムの展開オプションについて説明します。
第 6 章	Firepower 管理対象デバイスの展開	さまざまなセンシング インターフェイス（パッシブ、インライン、ルーテッド、スイッチド、ハイブリッドなど）が Firepower システムの機能に及ぼす影響について説明します。
付録 A	Firepower 8000 シリーズデバイスの電源要件	Firepower 8000 シリーズデバイスの AC 電源と DC 電源の要件について説明します。
付録 B	Firepower 8000 シリーズネットワーク モジュールの挿入と取り外し	Firepower 8000 シリーズデバイスにおける新しいモジュールの挿入方法または事前に装着されているモジュールの取り外しまたは交換方法について説明します。
付録 C	マルウェア ストレージ パックの取り付け	Firepower 8000 シリーズデバイスにおけるマルウェア ストレージ パックの取り付け方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字の文字	コマンド、キーワード、およびユーザが入力するテキストは、**太字**の文字で記載されます。
*イタリック*文字	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック*文字で記載されます。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	いずれか 1 つを選択しなければならない必須キーワードは波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは角カッコで囲み、縦棒で区切って示しています。
string	引用符のない一連の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
等幅文字	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
等幅の太字文字	コマンド、キーワード、およびユーザが入力するテキストは、**等幅の `courier`** 文字で記載されます。
*等幅のイタリック*文字	ユーザが値を指定する引数は、*等幅のイタリック*文字で記載されます。
< >	パスワードなどの出力されない文字は、山カッコで囲んで記載されます。

表記法	説明
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで記載されます。
!、#	コードの先頭にある感嘆符(!)またはポンド記号(#)は、コードのその行がコメント行であることを示します。

コメント 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

設置に関する警告

デバイスを設置する前に、『Regulatory Compliance and Safety Information』文書(http://www.cisco.com/c/en/us/td/docs/security/firesight/hw-docs/regulatory/compliance/firesight-firepower-rcsi.html)を必ずお読みください。

この項では、次の重要な安全上の警告について説明します。

電源の切断に関する警告

警告 シャーシの作業や電源モジュール周辺の作業を行う前に、AC 装置の電源コードを外し、DC 装置の回路ブレーカーの電源を切ってください。ステートメント 12

装飾品の取り外しに関する警告

警告 電源に接続された装置で作業する場合は、事前に、指輪、ネックレス、腕時計などの装身具を外してください。金属が電源やアースに接触すると、過熱して重度のやけどを引き起こしたり、金属類が端子に焼き付いたりすることがあります。ステートメント 43

リスト ストラップに関する警告

警告 作業中は、カードの静電破壊を防ぐため、必ず静電気防止用リスト ストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。ステートメント 94

雷の発生時の作業に関する警告

警告 雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

設置手順に関する警告

警告 システムを電源に接続する前に、すべての設置手順をお読みください。ステートメント 1004

ラック マウントおよびラックでの作業時のシャーシに関する警告

警告 ラックへのユニットの設置や、ラック内のユニットの保守作業を行う場合は、負傷事故を防ぐため、システムが安定した状態で置かれていることを十分に確認してください。次のガイドラインは、安全に作業を行ってもらうために用意してあります。この装置は、ラックに 1 つだけの場合は、一番下に搭載するようにしてください。ラックに複数の装置を取り付ける場合は、最も重い装置をラックの一番下にして、下から順番に取り付けます。ラックにスタビライザが付属している場合は、スタビライザを取り付けてから、装置の取り付けや保守を行ってください。ステートメント 1006

短絡保護に関する警告

警告 この製品は、設置する建物に回路短絡（過電流）保護機構が備わっていることを前提に設計されています。一般および地域の電気規格に準拠するように設置する必要があります。ステートメント 1045

SELV 回路に関する警告

感電を防ぐため、安全超低電圧（SELV）回路を電話網電圧（TNV）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートでは、共に RJ-45 コネクタが使用されています。ケーブルを接続する際は、注意してください。ステートメント 1021

アース線に関する警告

警告 この装置は、接地させる必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。接地が適正であるかどうかわからない場合は、電気検査機関または電気技術者に相談してください。Statement 1024

前面プレートとカバー パネルに関する警告

警告 ブランクの前面プレートおよびカバー パネルには、3 つの重要な機能があります。シャーシ内の危険な電圧および電流による感電を防ぐこと、他の装置への電磁干渉（EMI）の影響を防ぐこと、およびシャーシ内の冷気の流れを適切な状態に保つことです。システムは、必ずすべてのカード、前面プレート、前面カバー、および背面カバーを正しく取り付けた状態で運用してください。ステートメント 1029 および 142

製品の廃棄に関する警告

警告 本製品の最終処分は、各国のすべての法律および規制に従って行ってください。ステートメント 1040

地域および国の電気工事規定遵守に関する警告

警告 装置は地域および国の電気規則に従って設置する必要があります。ステートメント 1074

アース線機器に関する警告

警告 この機器は接地されることを前提にしています。通常の使用時にホストが接地されていることを確認してください。ステートメント 39

安全カバーの要件

警告 保護カバーは製品の重要な一部です。保護カバーを取り付けていない状態で装置を操作しないでください。カバーを所定の位置に取り付けていない状態での装置の操作は、安全規格に不適合になります。火災または感電事故が発生する危険性があります。ステートメント 117

安全性および警告に関する情報の入手先

安全性および警告については、次の URL にある『Regulatory Compliance and Safety Information』文書を参照してください。

http://www.cisco.com/c/en/us/td/docs/security/firesight/hw-docs/regulatory/compliance/firesight-firepower-rcsi.html

この RCSI 文書では、Cisco Firepower シリーズの国際機関への準拠および安全性の情報について説明しています。

関連資料

Cisco Firepower シリーズの文書とその入手先についての完全な一覧については、次の URL にある文書のロードマップを参照してください。

http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

Firepower 8000 シリーズについて

この章では、さまざまなスループットや機能で使用可能な専用の耐障害性ネットワーク アプライアンスである Cisco Firepower 8000 シリーズデバイスについて説明します。

組織内のネットワーク セグメントに展開されたデバイスは、分析対象のトラフィックを監視します。パッシブに展開されたデバイスは、ネットワーク トラフィックについて理解するうえで有用です。インラインで展開されている場合は、Firepower デバイスを使用し、複数の基準に基づいてトラフィックのフローに影響を及ぼすことができます。

Firepower 8000 シリーズデバイスは、Firepower Management Center で管理する**必要**があります。

警告 **この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。** ステートメント 49

Firepower システムに同梱されている Firepower 8000 シリーズ管理対象デバイス

次の表に、シスコが Firepower システムに同梱している Firepower 8000 シリーズ管理対象デバイスを示します。

表 1-1　Firepower 8000 シリーズアプライアンス

モデル/ファミリ	シリーズ/グループ	タイプ
80xx ファミリ： • AMP8050	8000 シリーズ	デバイス
81xx ファミリ： • 8120、8130、8140 • AMP8150	8000 シリーズ	デバイス

表 1-1　Firepower 8000 シリーズ [アプライアンス]（続き）

モデル/ファミリ	シリーズ/グループ	タイプ
82xx ファミリ： • 8250 • 8260、8270、8290	8000 シリーズ	デバイス
83xx ファミリ： • 8350 • 8360、8370、8390 • AMP8350 • AMP8360、AMP8370、AMP8390	8000 シリーズ	デバイス

Firepower 8000 シリーズデバイス シャーシの指定

次の表に、全世界で使用可能な Firepower 8000 シリーズモデルのシャーシ指定を示します。シャーシ コードはシャーシの外側の規制ラベルに記載されており、ハードウェア認定および安全性のための正式な参照コードです。

表 1-2　8000 シリーズシャーシ モデル

Firepower と AMP デバイス モデル	ハードウェアのシャーシ コード
AMP8050（AC または DC 電源）	CHAS-1U-AC/DC
8120、8130、8140、AMP8150 （AC または DC 電源）	CHAS-1U-AC/DC
8250、8260、8270、8290 （AC または DC 電源）	CHAS-2U-AC/DC
8350、8360、8370、8390 （AC または DC 電源）	PG35-2U-AC/DC
AMP830、AMP8360、AMP8370、AMP8390 （AC または DC 電源）	PG35-2U-AC/DC

ハードウェア仕様

Firepower 8000 シリーズデバイスは、組織のニーズを満たすさまざまなプラットフォーム上で提供されます。

ラックとキャビネットの取り付けオプション

Firepower デバイスはラックとサーバ キャビネットに設置することができます。アプライアンスにはラックマウント キットが付属しています。アプライアンスをラックに設置する方法については、ラックマウント キットに付属の取扱説明書を参照してください。

Firepower 8000 シリーズデバイス

Firepower 8000 シリーズデバイスは、銅線センシング インターフェイスとファイバ センシング インターフェイスのどちらかを含むネットワーク モジュール（NetMod）を使用します。デバイスは完全に組み立てられた状態で出荷することも、自分でモジュールを設置することもできます。Firepower システムを設置する前に、デバイスを組み立ててください。モジュールに付属の組立説明書を参照してください。

一部の 8000 シリーズデバイスは、スタッキングしてシステムの機能を強化することができます。スタッキング キットごとに、NetMod とスタッキング モジュールを交換し、8000 シリーズ スタッキング ケーブルを使用してデバイス同士をつなぎます。詳細については、「スタック構成でのデバイスの使用（3-11 ページ）」を参照してください。

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。

- AMP8050 は 1U シャーシであり、最大 3 つのモジュールを収容できます。
- 81xx ファミリとも呼ばれる Firepower 8120、8130、8140、および AMP8150 は、1U シャーシであり、最大 3 つのモジュールを収容することができます。Firepower 8140 だけは、スタッキング キットを追加して全部で 2U 構成にできます。
- 82xx ファミリに含まれる Firepower 8250 は、2U シャーシであり、最大 7 つのモジュールを収容することができます。合計 8 U の構成にするため最大 3 個のスタック構成キットを追加できます。
- 82xx ファミリに含まれる Firepower 8260 は、2 つの 2U シャーシからなる 4U 構成です。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 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。

- 82xx ファミリに含まれる Firepower 8270 は、3 つの 2U シャーシからなる 6U 構成です。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。各セカンダリ 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。
- 82xx ファミリに含まれる Firepower 8290 は、4 つの 2U シャーシからなる 8U 構成です。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。各セカンダリ 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。
- 83xx ファミリに含まれる Firepower 8350 および AMP8350 は、2U シャーシであり、最大 7 つのモジュールを収容することができます。合計 8 U の構成にするため最大 3 個のスタック構成キットを追加できます。
- 83xx ファミリに含まれる Firepower 8360 および AMP8360 は、2 つの 2U シャーシからなる 4U 構成です。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 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。
- 83xx ファミリに含まれる Firepower 8370 および AMP8370 は、3 つの 2U シャーシからなる 6U 構成です。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。各セカンダリ 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。
- 83xx ファミリに含まれる Firepower 8390 および AMP8390 は、4 つの 2U シャーシからなる 8U 構成です。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。各セカンダリ 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。

コメント　AMP モデルには Firepower の対応製品と共通のフォーム ファクタが少なからずありますが、Firepower システムのネットワークベースの高度なマルウェア防御（AMP）機能を利用するために最適化されています。

詳細については、次の項を参照してください。

- Firepower 8000 シリーズシャーシの前面図（2-2 ページ）
- Firepower 8000 シリーズシャーシの背面図（2-6 ページ）
- Firepower 8000 シリーズの物理パラメータと環境パラメータ（2-9 ページ）
- Firepower 8000 シリーズモジュール（2-13 ページ）

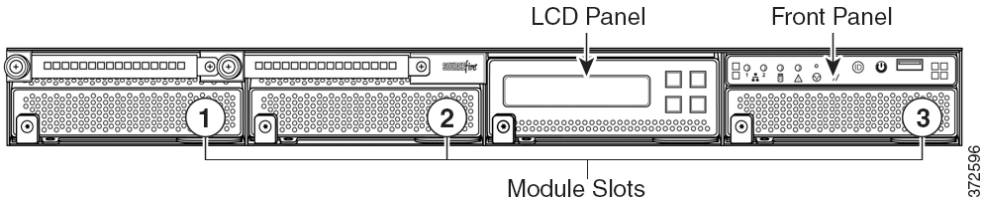
Firepower 8000 シリーズシャーシの前面図

Firepower 8000 シリーズシャーシは、AMP8x50、81xx ファミリ、82xx ファミリ、または 83xx ファミリに収容できます。AMP8x50、81xx ファミリ、82xx ファミリ、および 83xx ファミリ アプライアンスの安全上の考慮事項については、『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』を参照してください。

AMP8x50 および Firepower 81xx ファミリシャーシの前面図

シャーシの前面図には、ソリッドステート ディスク ドライブ、LCD パネル、前面パネル、および 3 つのモジュール スロットが示されています。

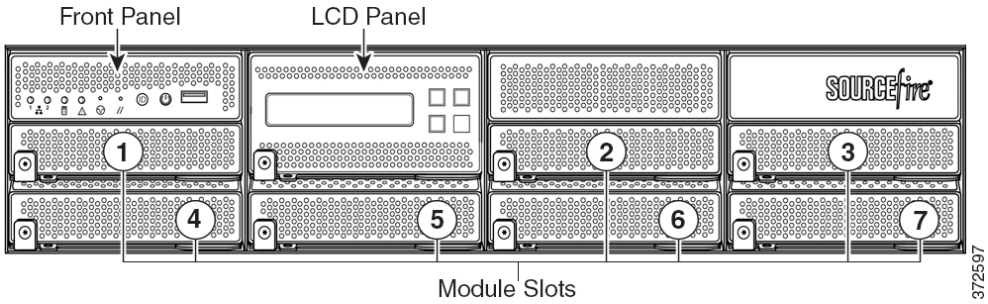
図 2-1　AMP8x50 および Firepower 81xx ファミリ（シャーシ：CHAS-1U-AC/DC）の前面図



Firepower 82xx ファミリと Firepower および AMP 83xx ファミリシャーシの正面図

シャーシの前面図には、LCD パネル、前面パネル、および 7 つのモジュール スロットが示されています。

図 2-2　Firepower 82xx ファミリ（シャーシ：CHAS-2U-AC/DC）と Firepower および AMP 83xx ファミリ（PG35-2U-AC/DC）の前面図



次の表に、アプライアンスの前面にある機能について示します。

表 2-1　Firepower 8000 シリーズシステム コンポーネント：前面図

機能	説明
ソリッドステート ディスク ドライブ（81xx ファミリ、AMP8x50）	オペレーティング システム、Firepower システム ソフトウェア、およびイベントと設定ファイルのローカル ファイル ストレージに使用されるプライマリ システムドライブとして機能するソリッドステート ドライブ（SSD）が付属しています。 疑わしいマルウェアのローカル ファイル ストレージを拡張する、オプションとなる 2 台目の SSD をインストールする方法については、マルウェア ストレージ パックの取り付け（C-1 ページ）を参照してください。
モジュール スロット	モジュールを収容します。使用可能なモジュールについては、Firepower 8000 シリーズモジュール（2-13 ページ）を参照してください。

表 2-1　Firepower 8000 シリーズシステム コンポーネント：前面図（続き）

機能	説明
LCD パネル	デバイスの設定、エラー メッセージの表示、およびシステム ステータスの確認を行うためにさまざまなモードで動作します。詳細については、Firepower デバイス上の LCD パネルの使用（4-1 ページ）を参照してください。
前面パネルのコントロール	システムの動作状態を表示する LED だけでなく、電源ボタンなどのさまざまなコントロールも配置されています。詳細については、図 2-4 Firepower 82xx ファミリと Firepower および AMP 83xx ファミリの前面パネル（2-4 ページ）を参照してください。
前面パネルの USB ポート	USB 2.0 ポートを使用すれば、デバイスにキーボードを接続できます。

詳細については、次の各項を参照してください。

- Firepower 8000 シリーズの前面パネル（2-4 ページ）
- Firepower 8000 シリーズシャーシの背面図（2-6 ページ）

Firepower 8000 シリーズの前面パネル

Firepower および AMP 81xx ファミリ、82xx ファミリ、および 83xx ファミリの前面パネルには、同じコンポーネントがあります。

図 2-3　Firepower 81xx ファミリの前面パネル

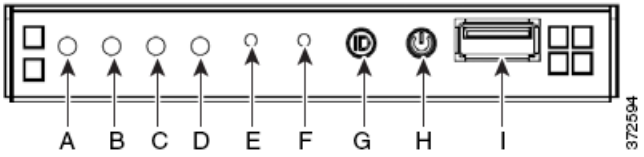


図 2-4　Firepower 82xx ファミリと Firepower および AMP 83xx ファミリの前面パネル

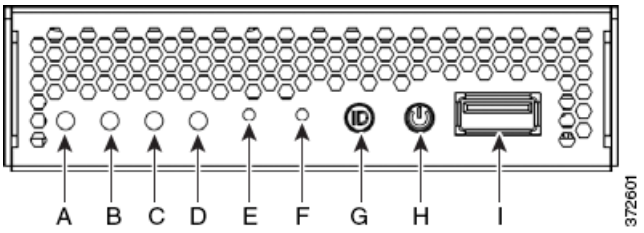


表 2-2　Firepower 8000 シリーズ前面パネルのコンポーネント

A	NIC アクティビティ LED	F	リセット ボタン
B	予約済み	G	ID ボタン
C	ソリッドステート ドライブ アクティビティ LED	H	電源ボタンおよび LED
D	システム ステータス LED	I	USB 2.0 コネクタ
E	マスク不能割り込みボタン		

シャーシの前面パネルには、システムの動作状態を表示する LED が付いています。次の表に、前面パネルの LED の説明を示します。

表 2-3　Firepower 8000 シリーズ前面パネル LED

LED	説明
NIC アクティビティ	ネットワーク アクティビティが存在するかどうかを示します。 • 緑色は、ネットワーク アクティビティが存在することを示します。 • ライトが消灯している場合は、ネットワーク アクティビティが存在しません。
ソリッドステート ドライブ アクティビティ	SSD ステータスを示します。 • 点滅する緑色は、固定ディスク ドライブがアクティブであることを示します。 • オレンジ色は、固定ディスク ドライブの障害を示します。 • ライトが消灯している場合は、ドライブ アクティビティが存在しないか、システムの電源がオフになっています。
システム ステータス	システム ステータスを示します。 • 緑色は、システムが正常に動作していることを示します。 • 点滅する緑色は、システムがデグレード状態で動作していることを示します。 • 点滅するオレンジ色は、システムが重大な状態にないことを示します。 • オレンジ色は、システムが重大なまたは回復不可能な状態にあるか、起動中であることを示します。 • ライトが消灯している場合は、システムが起動中か、オフになっています。 **コメント**　オレンジ色のステータス ライトは、緑色のステータス ライトより優先されます。オレンジ色のライトが点灯または点滅している場合は、緑色のライトが消灯しています。 詳細については、「表 2-4（2-6 ページ）」を参照してください。
システム ID	他の同様のシステムと一緒に高密度ラックに設置されているシステムを特定できるようにします。 • 青色のライトは ID ボタンが押されて、アプライアンスの背面で青色のライトが点灯していることを示します。 • 消灯は、ID ボタンが押されていないことを示します。
電源ボタンおよび LED	システムに電力が供給されているかどうかを示します。 • 緑色は、システムに電力が供給されていることを示します。 • ライトが消灯している場合は、システムに電力が供給されていません。

次の表に、システム ステータス LED が点灯する条件の説明を示します。

表 2-4　Firepower 8000 シリーズ システム ステータス

条件	説明
クリティカル	次のイベントに関連付けられた重大なまたは回復不可能なしきい値超過 • 温度、電圧、またはファンの重大なしきい値超過 • 電源サブシステムの障害 • 正しく取り付けられていないプロセッサまたは互換性のないプロセッサが原因でシステムの電源がオンにできない • 重大なイベント ロギング エラー、System Memory Uncorrectable ECC エラーと、PCI SERR や PERR などの致命的な/修正不可能なバス エラーを含む
重大でない	重大でない状態は、次のイベントに関連付けられたしきい値超過です。 • 温度、電圧、またはファンの重大でないしきい値超過 • シャーシ侵害 • システム BIOS からの Set Fault Indication コマンド。BIOS はこのコマンドを使用してシステム メモリや CPU の設定変更などの追加の、重大でないステータスを示す場合があります。
デグレード	デグレード状態は次のイベントに関連付けられます。 • 1 つ以上のプロセッサが Fault Resilient Boot（FRB）または BIOS によって無効になっている • 一部のシステム メモリが BIOS によって無効化またはマップアウトされている • いずれかの電源が、ケーブルが外れているか、機能していない **ヒント**　デグレード状態が表示された場合は、最初に電源の接続をチェックしてください。デバイスの電源をオフにして、両方の電源コードを外し、もう一度接続して元に戻してから、デバイスを再起動します。 ⚠ **注意**　電源を安全にオフにするには、『*Firepower Management Center Configuration Guide*』の「Managing Devices」の章に記載された手順または CLI から `system shutdown` コマンドを使用します。

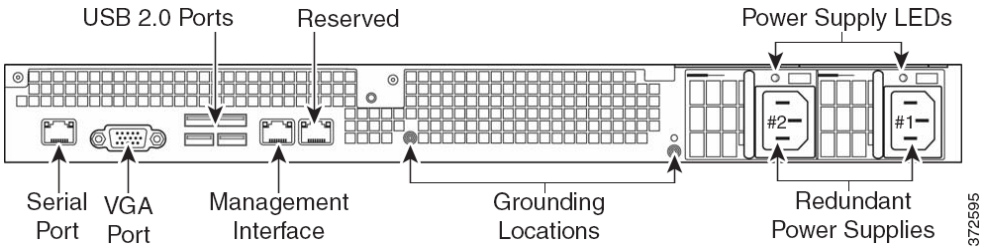
Firepower 8000 シリーズシャーシの背面図

Firepower 8000 シリーズシャーシは、81xx ファミリ、82xx ファミリ、または 83xx ファミリに収容できます。

AMP8x50 および Firepower 81xx ファミリシャーシの背面図

シャーシの背面図には、接続ポート、管理インターフェイス、および電源が示されています。

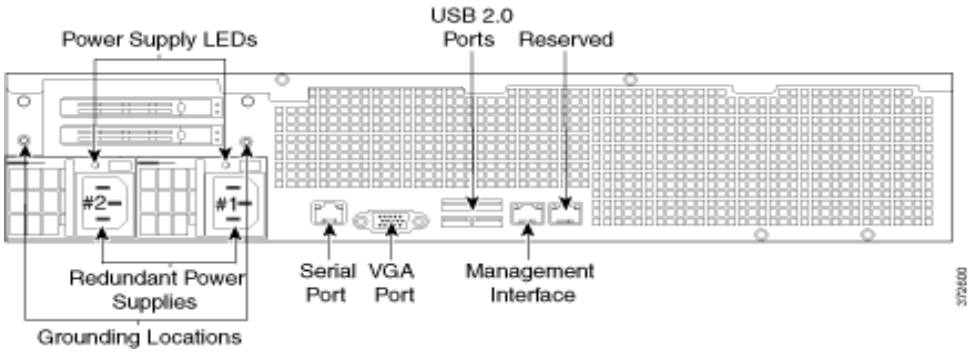
図 2-5　AMP8x50 および Firepower 81xx ファミリ（シャーシ：CHAS-1U-AC/DC）の背面図



Firepower 82xx ファミリシャーシの背面図

シャーシの背面図には、電源、ソリッドステート ディスク ドライブ、接続ポート、および管理インターフェイスが示されています。

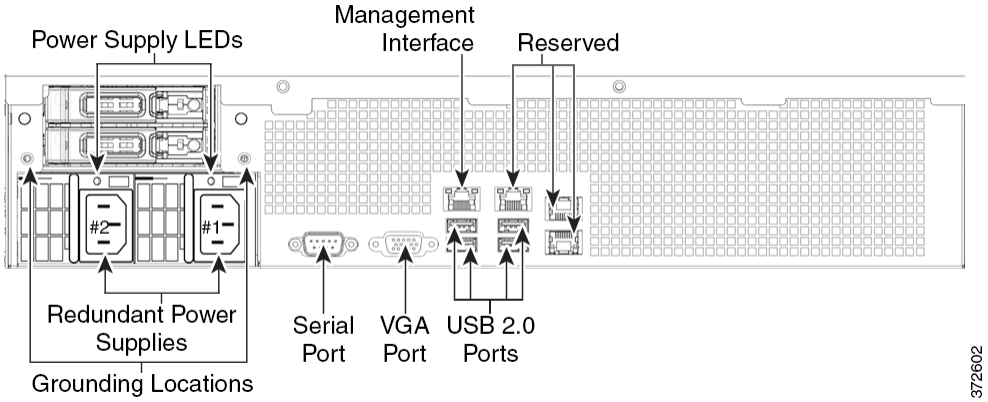
図 2-6　Firepower 82xx ファミリ（シャーシ：CHAS-2U-AC/DC）背面図



Firepower および AMP 83xx ファミリシャーシの背面図

シャーシの背面図には、電源、ソリッドステート ディスク ドライブ、接続ポート、および管理インターフェイスが示されています。

図 2-7　Firepower および AMP 83xx ファミリ（シャーシ：PG35-2U-AC/DC）の背面図



次の表に、アプライアンスの背面にある機能の説明を示します。

コメント　Firepower 83xx ファミリハードウェア プラットフォームには 6 つのファンがあり、FAN2 ～ FAN7 と表示されています。これは想定されている動作です。83xx ファミリプラットフォームに FAN1 はありません。

表 2-5　Firepower 8000 シリーズシステム コンポーネント：背面図

機能	説明
VGA ポート USB 2.0 ポート	シリアル ポートを使用する代わりに、デバイスにモニタ、キーボード、およびマウスを接続して、ワークステーション/アプライアンス間の直接接続を確立できるようにします。
RJ45 シリアル ポート（81xx ファミリと 82xx ファミリ）	デバイス上のすべての管理サービスに直接アクセスするためのワークステーション/アプライアンス間直接接続（RJ45 / DB-9 アダプタを使用）を確立できるようにします。RJ45 シリアル ポートは、メンテナンスと設定の目的に**のみ**使用され、サービス トラフィックを伝送するためのものではありません。
RS232 シリアル ポート（83xx ファミリ）	ワークステーション/アプライアンス間の直接接続を確立して、デバイス上のすべての管理サービスに直接アクセスできるようにします。RJ232 シリアル ポートは、メンテナンスと設定の目的に**のみ**使用され、サービス トラフィックを伝送するためのものではありません。
10/100/1000 イーサネット管理インターフェイス	アウトオブバンド管理ネットワーク接続を提供します。この管理インターフェイスは、メンテナンスと設定の目的に**のみ**使用され、サービス トラフィックを伝送するためのものではありません。
冗長電源	AC 電源を通してデバイスに電力を供給します。シャーシの背面から見て、電源 #1 は右側に、電源 #2 は左側にあります。
ソリッド ステート ディスク ドライブ（82xx ファミリおよび 83xx ファミリ）	オペレーティング システム、Firepower システム ソフトウェア、およびイベントと設定ファイルのローカル ファイル ストレージに使用されるプライマリ システム ドライブとして機能するソリッド ステート ドライブ（SSD）が付属しています。
アースの位置	アプライアンスを共通ボンディング網に接続できるようにします。詳細については、Firepower 8000 シリーズデバイスの電源要件（A-1 ページ）を参照してください。

10/100/1000 管理インターフェイスはアプライアンスの背面に配置されています。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 2-6　Firepower 8000 シリーズ管理インターフェイス LED

LED	説明
左（アクティビティ）	ポート上のアクティビティを示します。 • 点滅するライトはアクティビティを示します。 • 消灯は、アクティビティが存在しないことを示します。
右（リンク）	リンクが確立しているかどうかを示します。 • ライトはリンクが確立していることを示します。 • 消灯は、リンクが存在しないことを示します。

電源モジュールはアプライアンスの背面に配置されています。次の表に、管理インターフェイスに関連付けられた LED の説明を示します。

表 2-7　Firepower 8000 シリーズ電源 LED

LED	説明
オフ（Off）	電源が接続されていません。
オレンジ	このモジュールに電力が供給されていません。 または モジュール障害、飛んだヒューズ、ファン障害などの電源重大イベント。電源はシャット ダウンされます。
オレンジで点滅	高温やファン速度低下などの電源警告イベント。電源は動作を継続します。
緑の点滅	AC 入力が存在します。待機電圧。電源がオフになっています。
グリーン	電源が接続され、オンになっています。

次の表に、デバイスの RJ45 シリアル コネクタの一般的な DB-9 シリアル コネクタおよび該当するピン信号を示します。この表を使用して、アダプタをシリアル接続用に構成できます。

表 2-8　Firepower 8000 シリーズ RJ-45 / DB-9 アダプタ間のピン割り当て

DB-9 ピン	信号	説明	RJ45 ピン
1	DCD/DSR	データ キャリア検出/データ セット レディ	7
2	RD	受信データ	6
3	TD	伝送データ	3
4	DTR	データ ターミナル レディ	2
5	GND	地面	4 と 5
6		接続なし	
7	RTS	送信要求	1
8	CTS	送信可	8
9		接続なし	

Firepower 8000 シリーズの物理パラメータと環境パラメータ

次の表に、AMP8x50 デバイスと 81xx ファミリデバイスの物理属性と環境パラメータの説明を示します。

表 2-9　AMP8x50 および 81xx ファミリの物理パラメータと環境パラメータ

パラメータ	説明
フォーム ファクタ	1U
寸法 （D x W x H）	72.8 cm X 43.3 cm X 4.4 cm（28.7 インチ X 17.2 インチ X 1.73 インチ）
重量 最大設置	43.5 ポンド（19.8 kg）

表 2-9　AMP8x50 および 81xx ファミリの物理パラメータと環境パラメータ（続き）

パラメータ	説明
銅線 1000BASE-T 設定可能バイパス NetMod	ペア構成内のクアッドポート ギガビット銅線イーサネット設定可能バイパス インターフェイス ケーブルと距離：Cat5E、50 m
ファイバ 10GBASE 設定可能バイパス MMSR または SMLR NetMod	LC コネクタを使用したデュアルポート ファイバ設定可能バイパス インターフェイス ケーブルと距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）
ファイバ 1000BASE-SX 設定可能バイパス NetMod	LC コネクタを使用したクアッドポート ファイバ設定可能バイパス インターフェイス 1000BASE-SX ケーブルと距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）
銅線 1000BASE-T 非バイパス NetMod	ペア構成内のクアッドポート ギガビット銅線イーサネット非バイパス インターフェイス ケーブルと距離：Cat5E、50 m
ファイバ 10GBASE 非バイパス MMSR または SMLR NetMod	LC コネクタを使用したクアッドポート ファイバ非バイパス インターフェイス ケーブルと距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）
ファイバ 1000BASE-SX 非バイパス NetMod	LC コネクタを使用したクアッドポート ファイバ非バイパス インターフェイス 1000BASE-SX ケーブルと距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）
電源モジュール	AC または DC 用に設計されたデュアル 650 W 冗長電源 AC 電圧：公称 100 ～ 240 VAC（最大 85 ～ 264 VAC） AC 電流：電源あたりフルレンジで最大 5.2 A 電源あたり 187 ～ 264 VAC に対して最大 2.6 A AC 周波数範囲：47 ～ 63 Hz DC 電圧：RTN を基準に公称 -48 VDC 最大 -40 ～ -72 VDC DC 電流：電源あたり最大 11 A
ソリッドステート ドライブ（SSD）	200 GB 2.5 インチ SSD 疑わしいマルウェアのローカル ファイル ストレージを拡張する、オプションとなる 2 台目の SSD をインストールする方法については、マルウェア ストレージ パックの取り付け（C-1 ページ）を参照してください。
動作温度	50 ～ 95 °F（10 ～ 35 °C）
非動作時温度	-29 ～ 158 °F（-20 ～ 70 °C）
湿度（動作時）	5 ～ 85 %（結露しないこと）
非動作時湿度	5 ～ 90 %（77 ～ 95 °F（25 ～ 35 °C）の温度で 82 °F（28 °C）の最大湿球を使用して結露しないこと）
高度	0（海抜）～ 6000 フィート（0 ～ 1800 m）
冷却要件	1725 BTU/時 必要な動作温度範囲内でアプライアンスを維持するために十分な冷却を提供する必要があります。これができない場合は、アプライアンスの誤動作や損傷を引き起こす可能性があります。
音響ノイズ	最大正常作動音は 87.6 dB LWAd（高温）です。 標準正常作動音は 80 dB LWAd です。

表 2-9　AMP8x50 および 81xx ファミリの物理パラメータと環境パラメータ（続き）

パラメータ	説明
耐衝撃性	2G の半正弦波衝撃でエラーなし（作用時間 11 ms）
エアーフロー	160 フィート^3（4.5 m^3）/分 キャビネットのユニットの前後、または周囲を十分な空間を設けずに遮断するなどしてエアーフローを制限すると、周囲温度が動作範囲内であっても、ユニットが過熱状態になる可能性があります。 エアーフローはアプライアンスの前面から入って背面に抜けます。前後の空間の最小推奨値は 7.9 インチ（= 20 cm（3.50 インチ））である必要があります。この最小値は、アプライアンスの前面に低温の通気の供給が保証できる場合のみ使用できます。

次の表に、Firepower 82xx ファミリデバイスと Firepower および AMP 83xx ファミリデバイスの物理的特性と環境パラメータの説明を示します。

表 2-10　Firepower 82xx ファミリと Firepower および AMP 83xx ファミリの物理パラメータと環境パラメータ

パラメータ	説明	
フォーム ファクタ	2U	
寸法（D x W x H）	73.5 cm X 43.3 cm X 88.2 cm（29.0 インチ X 17.2 インチ X 3.48 インチ）	
最大設置重量	82xx ファミリ：	25.3 kg（58 ポンド）
	83xx ファミリ：	67 ポンド（30.5 kg）
銅線 1000BASE-T 設定可能バイパス NetMod	ペア構成内のクアッドポート ギガビット銅線イーサネット設定可能バイパス インターフェイス ケーブルと距離：Cat5E、50 m	
ファイバ 10GBASE MMSR または SMLR 設定可能バイパス NetMod	LC コネクタを使用したデュアルポート ファイバ設定可能バイパス インターフェイス ケーブルと距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）	
ファイバ 1000BASE-SX 設定可能バイパス NetMod	LC コネクタを使用したクアッドポート ファイバ設定可能バイパス インターフェイス 1000BASE-SX ケーブルと距離：SX はマルチモード ファイバ（850 nm）、550 m（標準）	
ファイバ 40GBASE-SR4 設定可能バイパス NetMod	OTP/MTP コネクタを使用したデュアルポート ファイバ設定可能バイパス インターフェイス ケーブルと距離： OM3：850 nm マルチモード、100 m OM4：850 nm マルチモード、150 m	
銅線 1000BASE-T 非バイパス NetMod	ペア構成内のクアッドポート ギガビット銅線イーサネット非バイパス インターフェイス ケーブルと距離：Cat5E、50 m	
ファイバ 10GBASE 非バイパス MMSR または SMLR NetMod	LC コネクタを使用したクアッドポート ファイバ非バイパス インターフェイス ケーブルと距離： LR はシングルモード、5000 m（使用可能） SR はマルチモード ファイバ（850 nm）、550 m（標準）	
ファイバ 1000BASE-SX 非バイパス NetMod	LC コネクタを使用したクアッドポート ファイバ非バイパス インターフェイス 1000BASE-SX ケーブルと距離： SX はマルチモード ファイバ（850 nm）、550 m（標準）	

表 2-10　Firepower 82xx ファミリと Firepower および AMP 83xx ファミリの物理パラメータと環境パラメータ(続き)

パラメータ	説明	
電源モジュール	82xx ファミリ：	AC または DC 用に設計されたデュアル 750 W 冗長電源 AC 電圧：公称 100 ～ 240 VAC(最大 85 ～ 264 VAC) AC 電流：電源あたりフルレンジで最大 8 A 電源あたり 187 ～ 264 VAC に対して最大 4 A AC 周波数範囲：47 ～ 63 Hz DC 電圧：RTN を基準に公称 -48 VDC 最大 -40 ～ -72 VDC DC 電流：電源あたり最大 18 A
	83xx ファミリ：	AC または DC 用に設計されたデュアル 1000 W 冗長電源。 AC 電圧：公称 100 ～ 240 VAC(最大 85 ～ 264 VAC) AC 電流：電源あたりフルレンジで最大 11 A 電源あたり 187 ～ 264 VAC に対して最大 5.5 A AC 周波数範囲：47 ～ 63 Hz DC 電圧：RTN を基準に公称 -48 VDC 最大 -40 ～ -72 VDC DC 電流：電源あたり最大 25 A
ソリッドステート ドライブ(SSD)	82xx ファミリ：	200 GB 2.5 インチ SSD
	83xx ファミリ：	800 GB 2.5 インチ SSD
	疑わしいマルウェアのローカル ファイル ストレージを拡張する、オプションとなる 2 台目の SSD をインストールする方法については、マルウェア ストレージ パックの取り付け (C-1 ページ)を参照してください。	
動作温度	82xx ファミリ：	50 °F ～ 95 °F(10 °C ～ 35 °C)
	83xx ファミリ：	41 ～ 104 °F(5 ～ 40 °C)
非動作時温度	-29 ～ 158 °F (- 20 ～ 70 °C)	
湿度(動作時)	5 ～ 85 %(結露しないこと)	
非動作時湿度	5 ～ 90 %(77 ～ 95 °F(25 ～ 35 °C)の温度で 82 °F(28 °C)の最大湿球を使用して結露しないこと)	
高度	0(海抜)～ 6000 フィート(0 ～ 1800 m)	
冷却要件	最大 2900 BTU/時 必要な動作温度範囲内でアプライアンスを維持するために十分な冷却を提供する必要があります。これができない場合は、アプライアンスの誤動作や損傷を引き起こす可能性があります。	
音響ノイズ	最大正常作動音は 81.6 dB LWAd(高温)です。 標準正常作動音は 81.4 dB LWAd です。	

表 2-10　Firepower 82xx ファミリと Firepower および AMP 83xx ファミリの物理パラメータと環境パラメータ（続き）

パラメータ	説明
耐衝撃性	2G の半正弦波衝撃でエラーなし（作用時間 11 ms）
エアーフロー	前から後ろへ、210 フィート^3（6 m^3）/分 キャビネットのユニットの前後、または周囲を十分な空間を設けずに遮断するなどしてエアーフローを制限すると、周囲温度が動作範囲内であっても、ユニットが過熱状態になる可能性があります。 エアーフローはアプライアンスの前面から入って背面に抜けます。前後の空間の最小推奨値は 7.9 インチ（20 cm）です。この最小値は、アプライアンスの前面に低温の通気の供給が保証できる場合のみ使用できます。

Firepower 8000 シリーズモジュール

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 シリーズ ネットワーク モジュールの挿入と取り外し（B-1 ページ）を参照してください。

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。

- バイパス機能を設定可能なクアッドポート 1000BASE-T 銅線インターフェイス。クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod（2-14 ページ）を参照してください。
- バイパス機能を設定可能なクアッドポート 1000BASE-SX ファイバ インターフェイス。詳細については、クアッドポート 1000BASE-SX ファイバ設定可能バイパス NetMod（2-15 ページ）を参照してください。
- バイパス機能を設定可能なデュアルポート 10GBASE（MMSR または SMLR）ファイバ インターフェイス。詳細については、デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod（2-16 ページ）を参照してください。
- バイパス機能を設定可能なデュアル ポート 40GBASE-SR4 ファイバ インターフェイス（2U デバイスのみ）。詳細については、デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod（2-18 ページ）を参照してください。

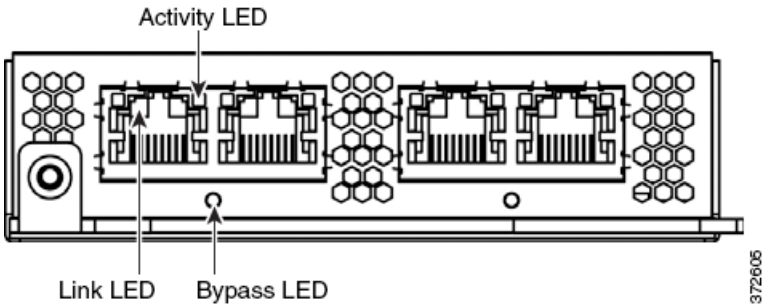
次のモジュールには、非バイパス センシング インターフェイスが含まれています。

- バイパス機能のないクアッドポート 1000BASE-T 銅線インターフェイス。詳細については、クアッドポート 1000BASE-T 銅線非バイパス NetMod（2-20 ページ）を参照してください。
- バイパス機能のないクアッドポート 1000BASE-SX ファイバ インターフェイス。詳細については、クアッドポート 1000BASE-SX ファイバ非バイパス NetMod（2-20 ページ）を参照してください。
- バイパス機能のないクアッドポート 10GBASE（MMSR または SMLR）ファイバ インターフェイス。詳細については、「クアッドポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod（2-21 ページ）」を参照してください。

加えて、スタック モジュールを使用して、2 つの Firepower 8140、最大 4 つの Firepower 8250、または最大 4 つの Firepower または AMP 8350 デバイスを接続し、それらの処理能力を組み合わせて、スループットを向上させることができます。詳細については、「スタッキング モジュール（2-23 ページ）」を参照してください。

クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod

クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod には、4 つの銅線ポート、およびリンク LED、アクティビティ LED、およびバイパス LED があります。



銅線インターフェイス上のリンク LED とアクティビティ LED については、次の表を参照してください。

表 2-11　銅線リンク/アクティビティ LED

Status（ステータス）	説明
両方の LED が消灯	インターフェイスは、リンクが存在せず、バイパス モードではありません。
リンク（オレンジ）	インターフェイス上のトラフィックの速度が 10 Mb または 100 Mb です。
リンク（緑）	インターフェイス上のトラフィックの速度が 1 Gb です。
アクティビティ（点滅する緑）	インターフェイス上にリンクが存在し、トラフィックが通過しています。

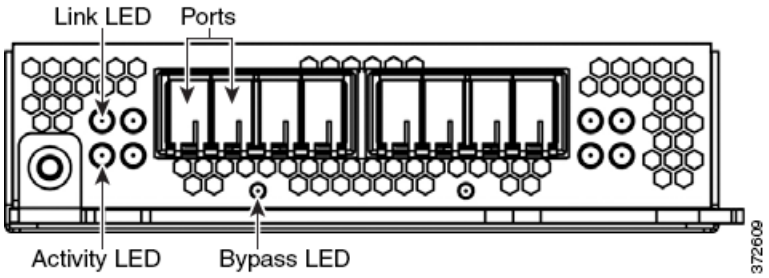
次の表に、銅線インターフェイスのバイパス LED の説明を示します。

表 2-12　銅線バイパス LED

Status（ステータス）	説明
消灯	インターフェイスは、リンクが存在せず、バイパス モードではありません。
緑色で点灯	インターフェイス上にリンクが存在し、トラフィックが通過しています。
黄色で点灯	インターフェイスは意図的に停止されています。
オレンジに点滅	インターフェイスがバイパス モードになっている、つまり、フェールオープンの状態になっています。

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

クアッドポート 1000BASE-AX ファイバ設定可能バイパス NetMod には、4 つのファイバ ポート、およびリンク LED、アクティビティ LED、およびバイパス LED があります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 2-13　ファイバ リンク/アクティビティ LED

Status（ステータス）	説明
上	インラインまたはパッシブ インターフェイスの場合: • 点滅するライトは、インターフェイス上にアクティビティが存在することを示します。 • 消灯は、アクティビティが存在しないことを示します。
下部	インライン インターフェイスの場合: • 点灯は、インターフェイス上にアクティビティが存在することを示します。 • 消灯は、アクティビティが存在しないことを示します。 パッシブ インターフェイスの場合は、ライトが常時点灯します。

次の表に、光ファイバ インターフェイスのバイパス LED の説明を示します。

表 2-14　ファイバ バイパス LED

Status（ステータス）	説明
消灯	インターフェイスは、リンクが存在せず、バイパス モードではありません。
緑色で点灯	インターフェイス上にリンクが存在し、トラフィックが通過しています。
黄色で点灯	インターフェイスは意図的に停止されています。
オレンジに点滅	インターフェイスがバイパス モードになっている、つまり、フェールオープンの状態になっています。

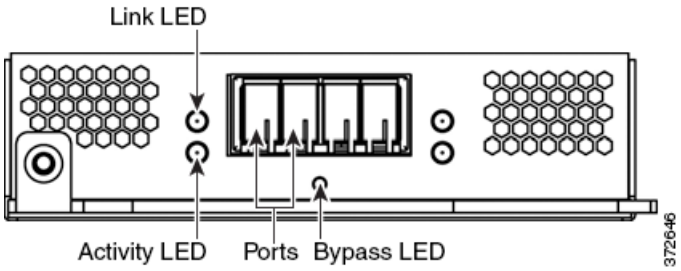
次の表に、光ファイバ インターフェイスの光仕様の説明を示します。

表 2-15　1000BASE-SX NetMod 光パラメータ

パラメータ	1000BASE-SX
光コネクタ	LC デュプレックス
ビット レート	1000 Mbps
ボー レート/符号化/許容値	1250 Mbps 8b/10b 符号化
光インターフェイス	マルチモード
動作距離	656 フィート（200 m）（62.5 µm/125 µm ファイバの場合） 1640 フィート（500 m）（50 µm/125 µm ファイバの場合）
トランスミッタ波長	770-860 nm（標準 850 nm）
最大平均出射パワー	0 dBm
最小平均出射パワー	-9.5 dBm
レシーバでの最大平均パワー	0 dBm
レシーバ感度	-17 dBm

デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod

デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod には、2 つのファイバ ポート、およびリンク LED、アクティビティ LED、およびバイパス LED があります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 2-16　ファイバ リンク/アクティビティ LED

Status（ステータス）	説明
上	インラインまたはパッシブ インターフェイスの場合： • 点滅するライトは、インターフェイス上にアクティビティが存在することを示します。 • 消灯は、アクティビティが存在しないことを示します。
下部	インライン インターフェイスの場合： • 点灯は、インターフェイス上にアクティビティが存在することを示します。 • 消灯は、アクティビティが存在しないことを示します。 パッシブ インターフェイスの場合は、ライトが常時点灯します。

次の表に、光ファイバ インターフェイスのバイパス LED の説明を示します。

表 2-17　ファイバ バイパス LED

Status（ステータス）	説明
消灯	インターフェイスは、リンクが存在せず、バイパス モードではありません。
緑色で点灯	インターフェイス上にリンクが存在し、トラフィックが通過しています。
黄色で点灯	インターフェイスは意図的に停止されています。
オレンジに点滅	インターフェイスがバイパス モードになっている、つまり、フェールオープンの状態になっています。

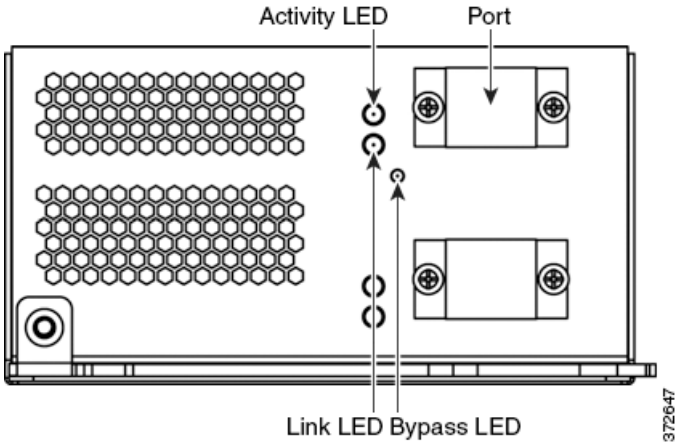
次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

表 2-18　10GBASE MMSR および SMLR NetMod の光パラメータ

パラメータ	10GBASE MMSR	10GBASE SMLR
光コネクタ	LC デュプレックス	LC デュプレックス
ビット レート	10.000 Gbps	10.000 Gbps
ボー レート/符号化/許容値	10.3125 Gbps 64/66b 符号化 +/- 100 ppm	10.3125 Gbps 64/166b 符号化 +/- 100 ppm
光インターフェイス	マルチモード	シングル モードのみ
動作距離	840-860 nm （標準 850 nm） 85 フィート（26 m）～ 108 フィート（33 m）（62.5 µm/125 µm ファイバ（それぞれモデル BW 160 ～ 200）の場合） 216 フィート（66 m）～ 269 フィート（82 m）（50 µm/125 µm ファイバ（それぞれモデル BW 400 ～ 500）の場合） 980 フィート（300 m）までの距離では高品質（OM3）ファイバを利用できます。 最短距離（すべて）: 6 フィート（2 m）	1270-1355 nm （標準 1310 nm） 6 フィート～ 6.2 マイル（2 m ～ 10 km） 9 µm / 125 µm ファイバの場合
トランスミッタ波長	840-860 nm （標準 850 nm）	1270-1355 nm （標準 1310 nm）
最大平均出射パワー	-1 dBm	-0.5 dBm
最小平均出射パワー	-7.3 dBm	-8.2 dBm
レシーバでの最大平均パワー	-1 dBm	-0.5 dBm
レシーバ感度	-9.9 dBm	-14.4 dBm

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

デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod には、2 つのファイバ ポート、リンク LED、アクティビティ LED、およびバイパス LED があります。



次の 8000 シリーズモデルで 40G NetMod を使用できます。

- Firepower 8270 および 8290
- Firepower および AMP 8360、8370、および 8390
- Firepower 8250 および 8260（40G 対応である必要があります）
- Firepower および AMP 8350（40G 対応である必要があります）

注意　40G 対応ではないデバイス上で 40G インターフェイスを作成しようとすると、それを管理する Firepower Management Center Web インターフェイスの 40G インターフェイス画面が赤く表示されます。40G 対応の 8250 の LCD パネルには「8250-40G」と表示され、40G 対応の 8350 の LCD パネルには「8350-40G」と表示されます。配置の詳細については、Firepower 8000 シリーズモジュール（3-5 ページ）を参照してください。

次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 2-19　ファイバ リンク/アクティビティ LED

Status（ステータス）	説明
上部（アクティビティ）	ライトは、インターフェイス上にアクティビティが存在する場合に点滅します。消灯している場合は、アクティビティが存在しません。
下部（リンク）	ライトは、インターフェイス上にリンクが存在する場合に点灯します。消灯している場合は、リンクが存在しません。

次の表に、光ファイバ インターフェイスのバイパス LED の説明を示します。

表 2-20　ファイバ バイパス LED

Status（ステータス）	説明
消灯	インターフェイス ペアは、リンクが存在せず、バイパス モードでないか、電力が供給されていません。
緑色で点灯	インターフェイス ペアは、リンクが存在し、トラフィックが通過しています。
黄色で点灯	インターフェイスは意図的に停止されています。
オレンジに点滅	インターフェイスがバイパス モードになっている、つまり、フェールオープンの状態になっています。

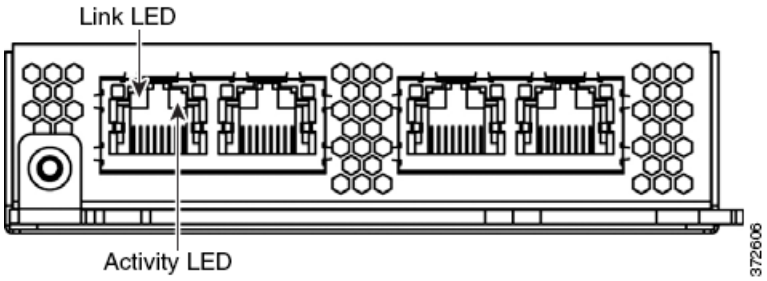
次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

表 2-21　40GBASE-SR4 NetMod 光パラメータ

パラメータ	40GBASE-SR4
光コネクタ	OTP/MTP 単一行 12 ファイバ位置。外側の 8 つのファイバだけが使用されます。
ビット レート	40.000 Gbps
ボー レート/符号化/許容値	10.3125 Gbps 64/66b 符号化 +/- 100 ppm
光インターフェイス	マルチモード
動作距離	320 フィート（100 m） 50 µm / 125 µm ファイバ（OM3）の場合 最小距離：2 フィート（0.5 m） 40G 光学素子は MPO コネクタ付きの 8 本のファイバ ケーブルで伝送されます。
トランスミッタ波長	840-860 nm（標準 850 nm）
最大平均出射パワー	2.4 dBm
最小平均出射パワー	-7.8 dBm
レシーバでの最大平均パワー	2.4 dBm
レシーバ感度	-9.5 dBm

クアッドポート 1000BASE-T 銅線非バイパス NetMod

クアッドポート 1000BASE-SX 銅線非バイパス NetMod には、4 つの銅線ポートと、リンク LED とアクティビティ LED があります。



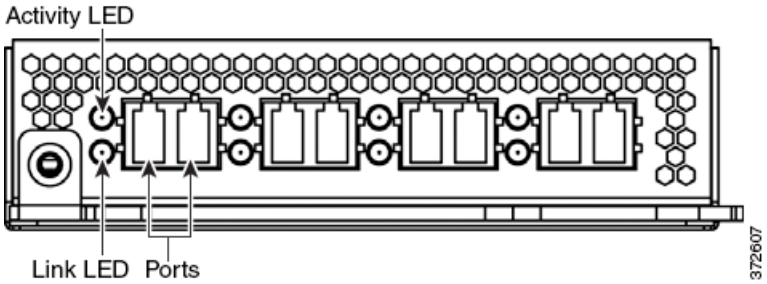
次の表に、銅線 LED の説明を示します。

表 2-22　非バイパス銅線リンク/アクティビティ LED

Status（ステータス）	説明
両方の LED が消灯	インターフェイス上にリンクが存在しません。
リンク（オレンジ）	インターフェイス上のトラフィックの速度が 10 Mb または 100 Mb です。
リンク（緑）	インターフェイス上のトラフィックの速度が 1 Gb です。
アクティビティ（点滅する緑）	インターフェイス上にリンクが存在し、トラフィックが通過しています。

クアッドポート 1000BASE-SX ファイバ非バイパス NetMod

クアッドポート 1000BASE-SX ファイバ非バイパス NetMod には、4 つのファイバ ポートと、リンク LED とアクティビティ LED があります。



ファイバ インターフェイス上のリンク LED とアクティビティ LED については、次の表を参照してください。

表 2-23　非バイパス ファイバ リンク/アクティビティ LED

Status（ステータス）	説明
上 （アクティビティ）	インラインまたはパッシブ インターフェイスの場合：インターフェイス上にアクティビティが存在する場合にライトが点滅します。消灯している場合は、アクティビティが存在しません。
下部 （リンク）	インライン インターフェイスの場合：インターフェイス上にリンクが存在する場合にライトが点灯します。消灯している場合は、リンクが存在しません。 パッシブ インターフェイスの場合：ライトが常時点灯します。

次の表に、光ファイバ インターフェイスの光パラメータの説明を示します。

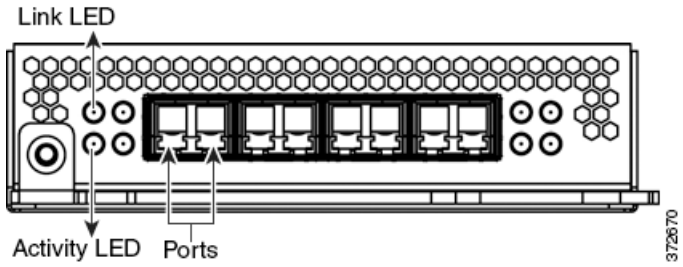
表 2-24　1000BASE-SX NetMod 光パラメータ

パラメータ	1000BASE-SX
光コネクタ	LC デュプレックス
ビット レート	1000 Mbps
ボー レート/符号化/許容値	1250 Mbps 8b/10b 符号化
光インターフェイス	マルチモード
動作距離	656 フィート（200 m）（62.5 µm/125 µm ファイバの場合） 1640 フィート（500 m）（50 µm/125 µm ファイバの場合）
トランスミッタ波長	770-860 nm（標準 850 nm）
最大平均出射パワー	0 dBm
最小平均出射パワー	-9.5 dBm
レシーバでの最大平均パワー	0 dBm
レシーバ感度	-17 dBm

クアッドポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod

クアッドポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod には、4 つのファイバ ポートと、リンク LED とアクティビティ LED があります。

注意　クアッドポート 10GBASE 非バイパス NetMod には、取り外し不可能な SFP が含まれています。SFP を取り外そうとすると、モジュールが破損することがあります。



次の表に、光ファイバ インターフェイスのリンク LED とアクティビティ LED の説明を示します。

表 2-25　ファイバ リンク/アクティビティ LED

Status（ステータス）	説明
上	インラインまたはパッシブ インターフェイスの場合: インターフェイス上にアクティビティが存在する場合にライトが点滅します。消灯している場合は、アクティビティが存在しません。
下部	インライン インターフェイスの場合: インターフェイス上にリンクが存在する場合にライトが点灯します。消灯している場合は、リンクが存在しません。 パッシブ インターフェイスの場合: ライトが常時点灯します。

次の表に、ファイバ インターフェイスの光パラメータの説明を示します。

表 2-26　10GBASE MMSR および SMLR NetMod の光パラメータ

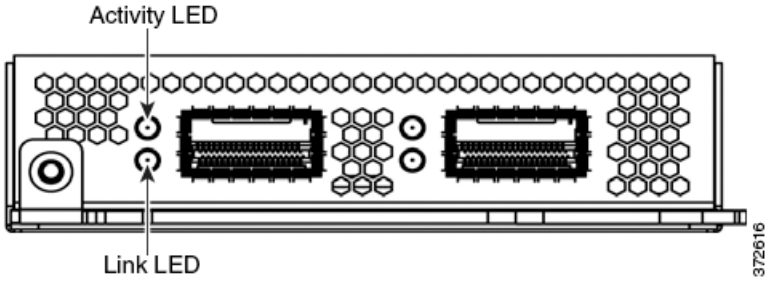
パラメータ	10GBASE MMSR	10GBASE SMLR
光コネクタ	LC デュプレックス	LC デュプレックス
ビット レート	10.000 Gbps	10.000 Gbps
ボー レート/ 符号化/許容値	10.3125 Gbps 64/66b 符号化 +/- 100 ppm	10.3125 Gbps 64/66b 符号化 +/- 100 ppm
光インターフェイス	マルチモード	シングル モードのみ
動作距離	840-860 nm （標準 850 nm） 85 フィート（26 m）～ 108 フィート（33 m）（62.5 µm/125 µm ファイバ（それぞれモデル BW 160 ～ 200）の場合） 216 フィート（66 m）～ 269 フィート（82 m）（50Hµm/125 µm ファイバ（それぞれモデル BW 400 ～ 500）の場合） 980 フィート（300 m）までの距離では高品質（OM3）ファイバを利用できます。 最短距離（すべて）: 6 フィート（2 m）	1270-1355 nm （標準 1310 nm） 6 フィート～ 6.2 マイル（2 m ～ 10 km）9 µm / 125 µm ファイバの場合
トランスミッタ波長	840-860 nm （標準 850 nm）	1270-1355 nm （標準 1310 nm）

表 2-26　10GBASE MMSR および SMLR NetMod の光パラメータ（続き）

パラメータ	10GBASE MMSR	10GBASE SMLR
最大平均出射パワー	-1 dBm	-0.5 dBm
最小平均出射パワー	-7.3 dBm	-8.2 dBm
レシーバでの最大平均パワー	-1 dBm	-0.5 dBm
レシーバ感度	-9.9 dBm	-14.4 dBm

スタッキング モジュール

スタッキング モジュールには、8000 シリーズスタッキング ケーブル用の 2 つの接続ポートと、アクティビティ LED とリンク LED が付属しています。



次の 8000 シリーズモデルではオプションとしてスタック モジュールを使用できます。

- Firepower 8140 および 8250
- Firepower および AMP 8350

スタック モジュールは次の 8000 シリーズスタック構成に含まれます。

- Firepower 8260、8270、および 8290
- Firepower および AMP 8360、8370、および 8390

次の表に、スタック構成 LED の説明を示します。

表 2-27　スタッキング LED

Status（ステータス）	説明
上	インターフェイス上のアクティビティを示します。 • 点滅するライトは、インターフェイス上にアクティビティが存在することを示します。 • 消灯は、アクティビティが存在しないことを示します。
下部	インターフェイス上にリンクが存在するかどうかを示します。 • 点灯は、インターフェイス上にリンクが存在することを示します。 • 消灯は、リンクが存在しないことを示します。

Firepower 8000 シリーズデバイスの設置

Firepower システムアプライアンスは、大規模な Firepower システム展開の一部としてネットワーク上に容易に設置できます。デバイスはネットワーク セグメントに設置され、それに適用された侵入ポリシーに基づいてトラフィックを検査し、侵入イベントを生成します。このデータは Firepower Management Center に送信されます。そこでは、データを展開全体で相互に関連付け、セキュリティに対する脅威を調整または処理するように 1 つ以上のデバイスが管理されます。

ヒント 複数の管理インターフェイスを使用することで、パフォーマンスを向上させたり、2 つの異なるネットワークのトラフィックを分離して管理することができます。初期設置中に、デフォルト管理インターフェイス（eth0）を設定します。設置した後、ユーザ インタフェースを介して追加の管理インターフェイスを設定できます。詳細については、*Firepower Management Center Configuration Guide* を参照してください。

複数のアプライアンスを別々の展開場所で使用するように 1 か所で事前設定できます。事前設定に関するガイダンスについては、『*FirePower 8000 シリーズ スタートアップ ガイド*』を参照してください。

アプライアンスの開梱と点検

ヒント サーバの輸送が必要となる場合に備えて、輸送用の箱は保管しておいてください。

コメント シャーシは厳密に検査したうえで出荷されています。輸送中の破損や内容品の不足がある場合には、ただちにカスタマー サービス担当者に連絡してください。

梱包内容を確認する手順は、次のとおりです。

ステップ 1 段ボール箱からシャーシを取り出します。梱包材はすべて保管しておいてください。

ステップ 2 次の Firepower 8000 シリーズデバイスに付属のコンポーネントのリストと梱包品を照合してください。システムと関連アクセサリを開梱するときに、次のようにパッケージの中身が完全であることを確認してください。

- アプライアンス × 1
- 電源コード（2 本の電源コードが冗長電源を含むアプライアンスに付属しています）

- カテゴリ 5e イーサネット ストレート ケーブル：Firepower デバイス用に 2 本
- 1 台のラックマウント キット

ステップ 3　破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。次の情報を用意しておきます。

- 発送元の請求書番号（梱包明細を参照）
- 破損している装置のモデルとシリアル番号
- 破損状態の説明
- 破損による設置への影響

セキュリティの考慮事項

Cisco では、アプライアンスを設置する前に、次の点を考慮することを推奨しています。

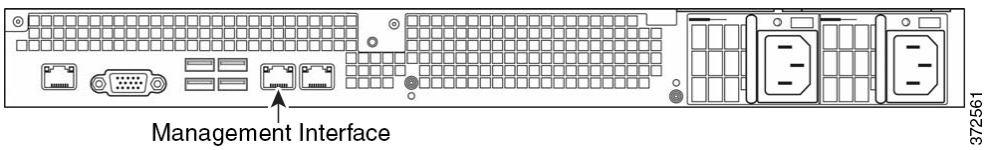
- 無許可ユーザによるアクセスから保護された安全な場所にあるロック付きラックにアプライアンスを配置します。
- アプライアンスの設置、交換、管理、または修理は、訓練を受け、資格要件を満たしている人物にのみ許可します。
- 管理インターフェイスは、必ず、不正アクセスから保護されたセキュアな内部管理ネットワークに接続します。
- アプライアンスへのアクセスを許可可能な特定のワークステーションの IP アドレスを特定します。アプライアンスのシステム ポリシー内のアクセス リストを使用している特定のホストにアプライアンスへのアクセスを限定します。詳細については、*Firepower Management Center Configuration Guide* を参照してください。

管理インターフェイスの識別

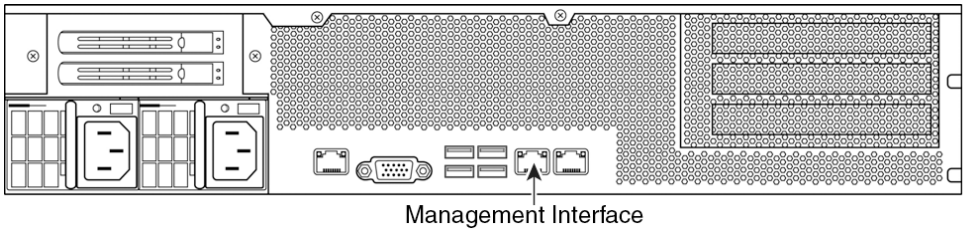
管理インターフェイスを使用して展開内の各アプライアンスをネットワークに接続します。これにより、Firepower Management Center は管理対象デバイスと通信して管理することができます。設置手順に従って作業する際、アプライアンスの正しい図を参照してください。

Firepower 8000 シリーズ

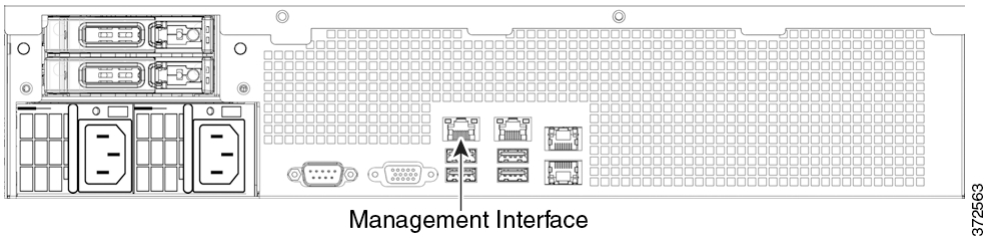
Firepower 8120、8130、8140、および AMP8150 は 1U アプライアンスとして提供されます。次のシャーシ背面図は、デフォルトの管理インターフェイスの位置を示しています。



Firepower 8250 は 2U アプライアンスとして提供されます。Firepower 8260、8270、および 8290 は 1 つ、2 つ、または 3 つのセカンダリ 2U アプライアンスが付属する 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は、各 2U アプライアンスのデフォルトの管理インターフェイスの位置を示しています。



Firepower および AMP 8350 は 2U アプライアンスとして提供されます。Firepower および AMP 8360、8370、8390 は 1 つ、2 つ、または 3 つのセカンダリ 2U アプライアンスが付属する 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は、各 2U アプライアンスのデフォルトの管理インターフェイスの位置を示しています。



センシング インターフェイスの識別

Firepower デバイスは、センシング インターフェイスを使用してネットワーク セグメントに接続します。1 つのデバイスで監視可能なセグメントの数は、デバイス上のセンシング インターフェイスの数とネットワーク セグメント上で使用する接続タイプ（パッシブ、インライン、ルーテッド、またはスイッチド）によって異なります。

以下の項では、各 Firepower デバイスのセンシング インターフェイスについて説明します。

- 8000 シリーズ上のセンシング インターフェイスを特定するには、Firepower 8000 シリーズ（3-3 ページ）を参照してください。
- 8000 シリーズ上のモジュール スロットを特定するには、Firepower 8000 シリーズ（3-3 ページ）を参照してください。
- 8000 シリーズ NetMod 上のセンシング インターフェイスを特定するには、Firepower 8000 シリーズモジュール（3-5 ページ）を参照してください。

接続タイプについては、センシング インターフェイスについて（6-2 ページ）を参照してください。

Firepower 8000 シリーズ

8000 シリーズは、10G ネットワーク スイッチを備えた 1 U デバイス、または 10G と 40G のどちらかのネットワーク スイッチを備えた 2 U デバイスとして使用可能です。このデバイスは、完全に組み立てた状態で出荷することも、センシング インターフェイスを含むネットワーク モジュール（NetMod）を取り付けることもできます。

コメント　デバイス上の互換性のないスロットに NetMod を取り付けた場合（Firepower 8250 または Firepower または AMP 8350 のスロット 1 と 4 に 40G NetMod を挿入した場合など）または NetMod がシステムと互換性がない場合は、NetMod を設定しようとすると、管理元の Firepower Management Center の Web インターフェイスにエラーまたは警告メッセージが表示されます。支援が必要な場合は、サポートに連絡してください。

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。

- バイパス機能を設定可能なクアッドポート 1000BASE-T 銅線インターフェイス
- バイパス機能を設定可能なクアッドポート 1000BASE-SX ファイバ インターフェイス
- バイパス機能を設定可能なデュアルポート 10GBASE（MMSR または SMLR）ファイバ インターフェイス
- バイパス機能を設定可能なデュアルポート 40GBASE-SR4 ファイバ インターフェイス（2U デバイスのみ）

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。

- バイパス機能のないクアッドポート 1000BASE-T 銅線インターフェイス
- バイパス機能のないクアッドポート 1000BASE-SX ファイバ インターフェイス
- バイパス機能のないデュアルポート 10GBASE（MMSR または SMLR）ファイバ インターフェイス

加えて、スタッキング モジュールは、同じ設定を持つ複数のアプライアンスのリソースを統合したものです。スタック モジュールは、Firepower 8140、8250、および 8350 上ではオプションであり、Firepower 8260、8270、8290 と Firepower および AMP 8360、8370、8390 のスタック構成では標準搭載です。

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 シリーズ ネットワーク モジュールの挿入と取り外し（B-1 ページ）を参照してください。

次のシャーシ前面図に、センシング インターフェイスを含むモジュール スロットの位置を示します。

図 3-1　Firepower 81xx ファミリのシャーシ前面図

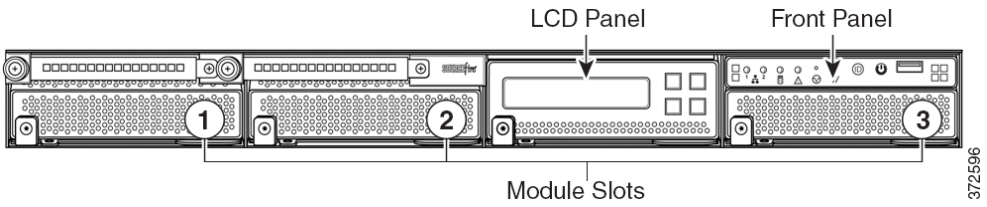
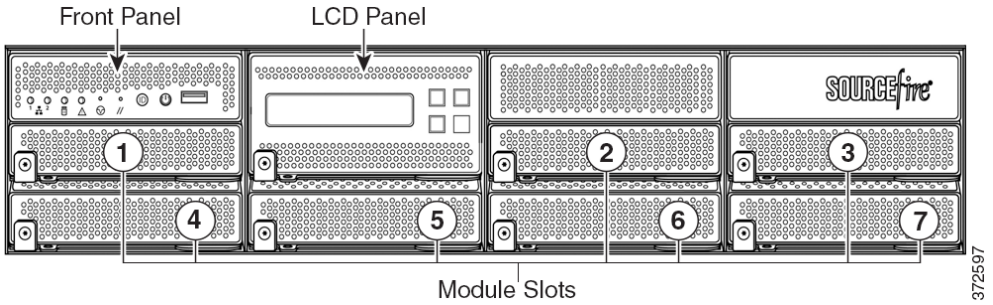


図 3-2　Firepower 82xx ファミリと Firepower および AMP 83xx ファミリシャーシの正面図



Firepower 8000 シリーズモジュール

Firepower 8000 シリーズは、バイパス機能が設定可能な次のモジュール付属で提供できます。

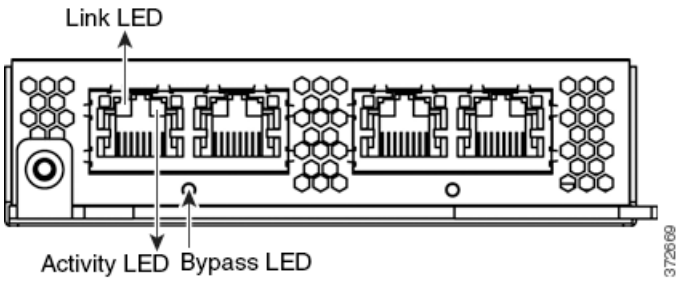
- バイパス機能を設定可能なクアッドポート 1000BASE-T 銅線インターフェイス。詳細については、図 3-3クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod（3-6 ページ）を参照してください。
- バイパス機能を設定可能なクアッドポート 1000BASE-SX ファイバ インターフェイス。詳細については、図 3-4クアッドポート 1000BASE-SX ファイバ設定可能バイパス NetMod（3-6 ページ）を参照してください。
- バイパス機能を設定可能なデュアルポート 10GBASE（MMSR または SMLR）ファイバ インターフェイス。詳細については、図 3-5デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod（3-7 ページ）を参照してください。
- バイパス機能を設定可能なデュアルポート 40GBASE-SR4 ファイバ インターフェイス。詳細については、「図 3-6デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod（3-7 ページ）」を参照してください。

Firepower 8000 シリーズは、バイパス機能が設定できない次のモジュール付属で提供できます。

- バイパス機能のないクアッドポート 1000BASE-T 銅線インターフェイス。詳細については、図 3-8クアッドポート 1000BASE-T 銅線非バイパス NetMod（3-8 ページ）を参照してください。
- バイパス機能のないクアッドポート 1000BASE-SX ファイバ インターフェイス。詳細については、図 3-9クアッドポート 1000BASE-SX ファイバ非バイパス NetMod（3-9 ページ）を参照してください。
- バイパス機能のないクアッドポート 10GBASE（MMSR または SMLR）ファイバ インターフェイス。詳細については、「図 3-10クアッドポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod（3-9 ページ）」を参照してください。

スタック モジュールは、Firepower 8140、8250、および 8350 上ではオプションであり、Firepower 8260、8270、8290 と Firepower 8360、8370、8390 のスタック構成では標準搭載です。詳細については、「Firepower 8000 シリーズスタック モジュール（3-10 ページ）」を参照してください。

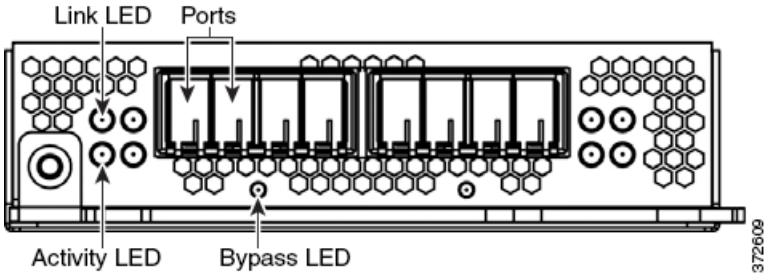
図 3-3　クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod



これらの接続を使用して、最大 4 つの異なるネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、デバイスを最大 2 つのネットワーク上に侵入防御システムとして展開することもできます。

デバイスの自動バイパス機能を利用する場合は、ネットワーク セグメントの左側にある 2 つのインターフェイスまたはネットワーク セグメントの右側にある 2 つのインターフェイスを接続する必要があります。これにより、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。また、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でバイパス モードを有効にすることもできます。

図 3-4　クアッドポート 1000BASE-SX ファイバ設定可能バイパス NetMod



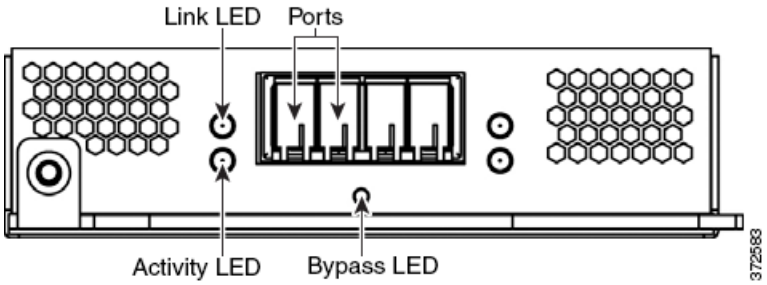
クアッドポート 1000BASE-SX ファイバ設定可能バイパス設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

この設定を使用して、最大 4 つの異なるネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、管理対象デバイスを最大 2 つのネットワーク上に侵入防御システムとして展開することもできます。

ヒント　最高のパフォーマンスを得るために、インターフェイス セットを連続的に使用します。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

デバイスの自動バイパス機能を利用する場合は、ネットワーク セグメントの左側にある 2 つのインターフェイスまたはネットワーク セグメントの右側にある 2 つのインターフェイスを接続する必要があります。これにより、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。また、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でバイパス モードを有効にすることもできます。

図 3-5　デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod



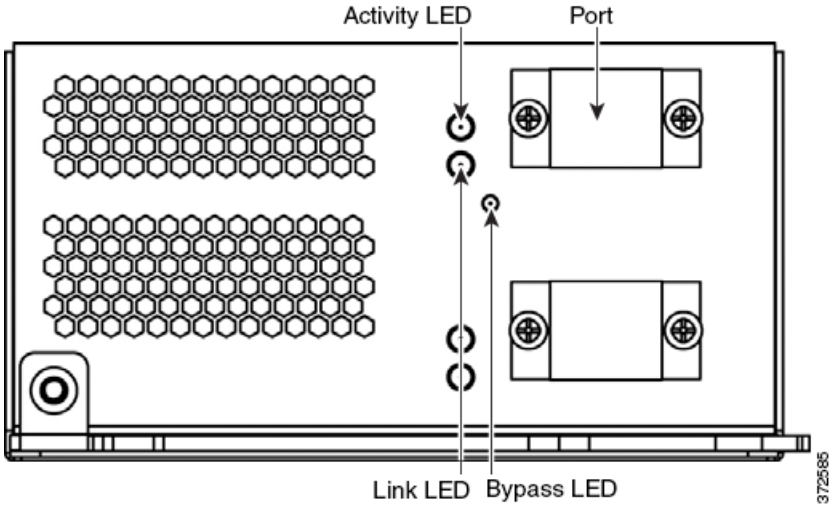
デュアルポート 10GBASE ファイバ設定可能バイパス設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。これらは MMSR インターフェイスまたは SMLR インターフェイスのいずれかであることに注意してください。

この設定を使用して、最大 2 つの異なるネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、管理対象デバイスを単一のネットワーク上に侵入防御システムとして展開することもできます。

ヒント　最高のパフォーマンスを得るために、インターフェイス セットを連続的に使用します。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

デバイスの自動バイパス機能を利用する場合は、2 つのインターフェイスをネットワーク セグメントに接続する必要があります。これにより、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。また、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でバイパス モードを有効にすることもできます。

図 3-6　デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod



デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス設定では、MPO（マルチファイバ プッシュ オン）コネク光トランシーバが使用されます。

次の 8000 シリーズモデルでのみ 40G NetMod を使用できます。

- Firepower 8270 および 8290
- Firepower および AMP 8360、8370、および 8390

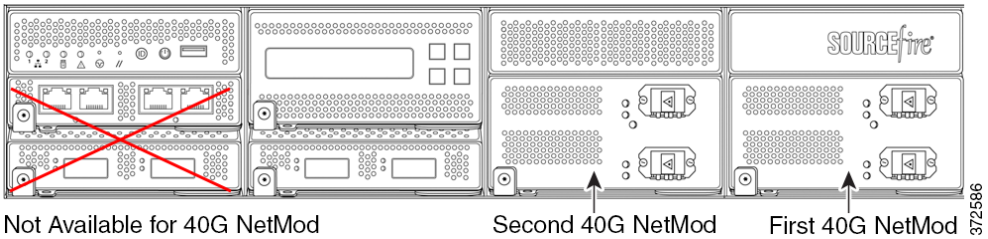
- Firepower 8250 および 8260（40G 対応である必要があります）
- Firepower および AMP 8350（40G 対応である必要があります）

注意　40G 対応ではないデバイス上で 40G インターフェイスを作成しようとすると、それを管理する Firepower Management Center Web インターフェイスの 40G インターフェイス画面が赤く表示されます。40G 対応の 8250 の LCD パネルには「8250-40G」と表示され、40G 対応の 8350 の LCD パネルには「8350-40G」と表示されます。

この設定を使用して、最大 2 つの異なるネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、デバイスを単一のネットワーク上に侵入防御システムとして展開することもできます。

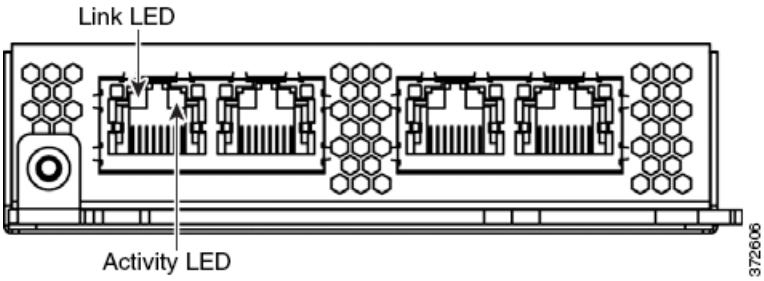
最大 2 つの 40G NetMod を使用できます。1 つ目の NetMod 40G をスロット 3 と 7 に、2 つ目の NetMod 40G をスロット 2 と 6 に取り付けます。スロット 1 と 4 で 40G NetMod を使用することはできません。

図 3-7　40G NetMod の配置



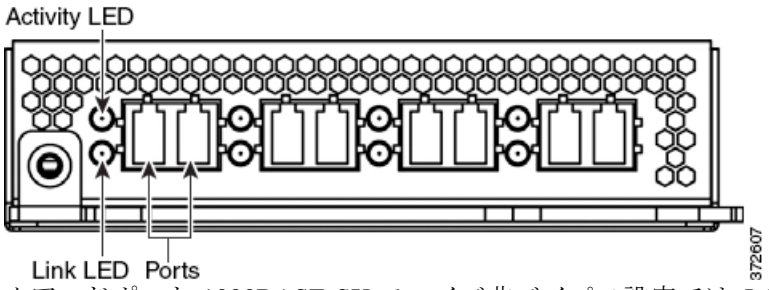
デバイスの自動バイパス機能を利用する場合は、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でバイパス モードを有効にする必要があります。

図 3-8　クアッドポート 1000BASE-T 銅線非バイパス NetMod



これらの接続を使用して、最大 4 つの異なるネットワーク セグメントを受動的に監視できます。また、最大 2 つのネットワーク セグメントのインライン設定でペア化されたインターフェイスを使用することもできます。

図 3-9　クアッドポート 1000BASE-SX ファイバ非バイパス NetMod

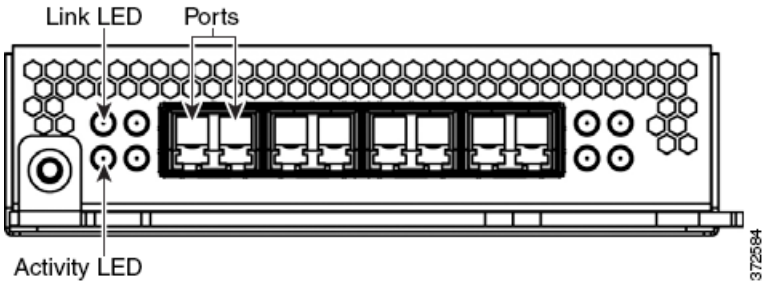


クアッドポート 1000BASE-SX ファイバ非バイパス設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

これらの接続を使用して、最大 4 つの異なるネットワーク セグメントを受動的に監視できます。また、最大 2 つのネットワーク セグメントのインライン設定でペア化されたインターフェイスを使用することもできます。

ヒント　最高のパフォーマンスを得るために、インターフェイス セットを連続的に使用します。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

図 3-10　クアッドポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod



クアッドポート 10GBASE ファイバ非バイパス設定では、MMSR インターフェイスまたは SMLR インターフェイスを備えた LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

注意　クアッドポート 10GBASE 非バイパス NetMod には、取り外し不可能な Small Form-Factor Pluggable（SFP）トランシーバが実装されています。SFP を取り外そうとすると、モジュールを破損する可能性があります。

これらの接続を使用して、最大 4 つの異なるネットワーク セグメントを受動的に監視できます。また、最大 2 つのネットワーク セグメントのインライン設定でペア化されたインターフェイスを使用することもできます。

ヒント　最高のパフォーマンスを得るために、インターフェイス セットを連続的に使用します。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

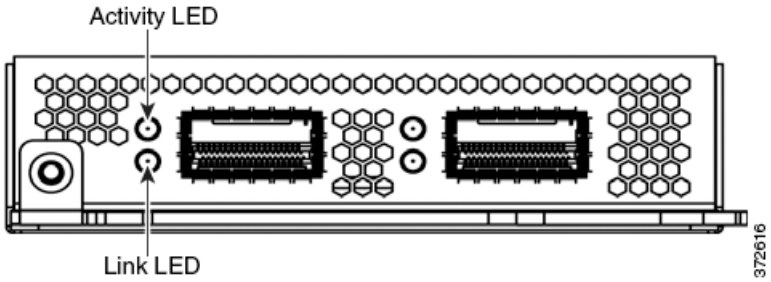
Firepower 8000 シリーズスタック モジュール

スタッキング モジュールは、同じ設定を持つ複数のアプライアンスのリソースを統合したものです。スタック モジュールは次の 8000 シリーズモデルでオプションです。

- Firepower 8140 および 8250
- Firepower および AMP 8350

スタック モジュールは次の 8000 シリーズスタック構成に含まれます。

- Firepower 8260、8270、および 8290
- Firepower および AMP 8360、8370、および 8390



スタッキング モジュールを使用すれば、2 つのデバイスのリソースをそれぞれプライマリ デバイスとセカンダリ デバイスとして統合することができます。プライマリ デバイスにのみセンシング インターフェイスがあります。次のデバイスでスタッキング モジュールを使用できます。

- Firepower 8140、8250、および 8350 はスタック モジュール付属で提供できます。
- Firepower 8260 のスタック構成には、プライマリ デバイスに 1 つのスタック モジュールが、セカンダリ デバイスに 1 つのスタック モジュールが付属しています。
- Firepower および AMP 8360 のスタック構成には、プライマリ デバイスに 1 つのスタック モジュールが、セカンダリ デバイスに 1 つのスタック モジュールが付属しています。
- Firepower 8270 のスタック構成には、プライマリ デバイスに 2 つのスタック モジュールが、2 台のセカンダリ デバイスそれぞれに 1 つのスタック モジュールが付属しています。
- Firepower および AMP 8370 のスタック構成には、プライマリ デバイスに 2 つのスタック モジュールが、2 台のセカンダリ デバイスそれぞれに 1 つのスタック モジュールが付属しています。
- Firepower 8290 のスタック構成には、プライマリ デバイスに 3 つのスタック モジュールが、3 台のセカンダリ デバイスそれぞれに 1 つのスタック モジュールが付属しています。
- Firepower および AMP 8390 のスタック構成には、プライマリ デバイスに 3 つのスタック モジュールが、3 台のセカンダリ デバイスそれぞれに 1 つのスタック モジュールが付属しています。

スタック構成デバイスの使用方法については、スタック構成でのデバイスの使用を参照してください。

スタック構成でのデバイスの使用

スタック構成内で同じ設定を持つデバイスのリソースを統合することによって、ネットワーク セグメントで検査するトラフィックの量を増やすことができます。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。Firepower Management Center がスタック構成を作成、編集、および管理します。

プライマリ デバイスには、センシング インターフェイスと、接続されているセカンダリ デバイスごとに 1 セットずつのスタッキング インターフェイスがあります。プライマリ デバイス上のセンシング インターフェイスを、非スタック構成デバイスと同じ方法で監視するネットワーク セグメントに接続します。スタッキング ケーブルを使用して、プライマリ デバイス上のスタッキング インターフェイスをセカンダリ デバイス上のスタッキング インターフェイスに接続します。それぞれのセカンダリ デバイスは、スタッキング インターフェイスを使用してプライマリ デバイスに直接接続されます。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、それらは使用されません。

次の設定でデバイスをスタックできます。

- 2 台の Firepower 8140
- 最大 4 台の Firepower 8250
- 1 つの Firepower 8260（1 つの 10G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの Firepower 8270（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの Firepower 8290（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）
- 最大 4 台の Firepower または AMP 8350
- 1 つの Firepower または AMP 8360（1 つの 40G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの Firepower または AMP 8370（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの Firepower または AMP 8390（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）

Firepower 8260 および 8270 デバイスと Firepower または AMP 8360 および 8370 デバイスの場合、デバイスを追加して合計 4 台までデバイスをスタックできます。

1 つのデバイスがプライマリ デバイスとして指定され、プライマリ ロールを持つ Firepower Management Center の Web インターフェイスに表示されます。スタック構成でのその他のすべてのデバイスはセカンダリであり、Web インターフェイスでセカンダリ ロールとして表示されます。スタック構成の個々のデバイスからの情報を表示する場合を除いて、組み合わせたリソースは 1 つのエンティティとして使用します。

単一の Firepower 8140、Firepower 8250、および Firepower または AMP 8350 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。

注意　すべてのデバイスのスタック メンバに対して管理インターフェイスが設定され、機能する**必要があります**。すべてのデバイスを単一のデバイスとして登録し、これらをスタックしてください。スタック構成のセカンダリ デバイスの管理インターフェイスを削除したり、無効化したりしないでください。これにより、スタック メンバはそれぞれヘルスをレポートし、設定情報を交換できます。

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。

ここでは、スタック構成デバイスを接続して管理する方法について詳しく説明します。

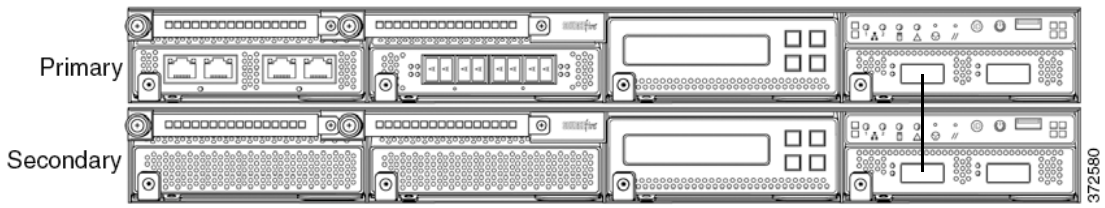
Firepower 8140 の接続

2 つの Firepower 8140 をスタック構成で接続できます。1 本の 8000 シリーズスタッキング ケーブルを使用して、プライマリ デバイスとセカンダリ デバイスの間の物理接続を確立する必要があります。スタッキング ケーブルの使用方法については、8000 シリーズスタッキング ケーブルの使用（3-17 ページ）を参照してください。

デバイスをラック内に設置して、スタッキング モジュール間をケーブルで容易に接続できるようにします。プライマリ デバイスの上または下にセカンダリ デバイスを設置できます。

単一の Firepower 8140 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。セカンダリ デバイスを直接プライマリ デバイスに接続します。

下の図に、プライマリ デバイスの下にセカンダリ デバイスを設置した状態を示します。



Firepower 8140 セカンダリ デバイスを接続するには：

ステップ 1　8000 シリーズスタッキング ケーブルを使用して、プライマリ デバイス上の左側のスタッキング インターフェイスをセカンダリ デバイス上の左側のスタッキング インターフェイスに接続してから、デバイスを管理する Firepower Management Center を使用して、システム内のスタック構成デバイスの関係を構築します。右側のスタッキング インターフェイスが接続されていないことに注意してください。スタック構成デバイスの管理（3-18 ページ）を参照してください。

注意　すべてのデバイスのスタック メンバに対して管理インターフェイスが設定され、機能する**必要があります**。すべてのデバイスを単一のデバイスとして登録し、これらをスタックしてください。スタック構成のセカンダリ デバイスの管理インターフェイスを削除したり、無効化したりしないでください。これにより、スタック メンバはそれぞれヘルスをレポートし、設定情報を交換できます。

Firepower 82xx ファミリと Firepower および AMP 83xx ファミリの接続

次の設定のいずれかを接続できます。

- 最大 4 台の 8250
- 最大 4 つの Firepower 8350 または AMP8350
- 1 つの Firepower 8260（1 つの 10G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの Firepower または AMP 8360（1 つの 40G 対応プライマリ デバイスと 1 つのセカンダリ デバイス）
- 1 つの Firepower 8270（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの Firepower または AMP 8370（1 つの 40G 対応プライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの Firepower 8290（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）
- 1 つの Firepower または AMP 8390（1 つの 40G 対応プライマリ デバイスと 3 つのセカンダリ デバイス）

次の構成では、デバイスを追加して合計 4 台までデバイスをスタックできます。

- Firepower 8260 および 8270
- Firepower または AMP 8360
- Firepower または AMP 8370

プライマリ デバイスに接続するセカンダリ デバイスごとに 2 本ずつの 8000 シリーズスタッキング ケーブルを使用する必要があります。スタッキング ケーブルの使用方法については、8000 シリーズ スタッキング ケーブルの使用（3-17 ページ）を参照してください。

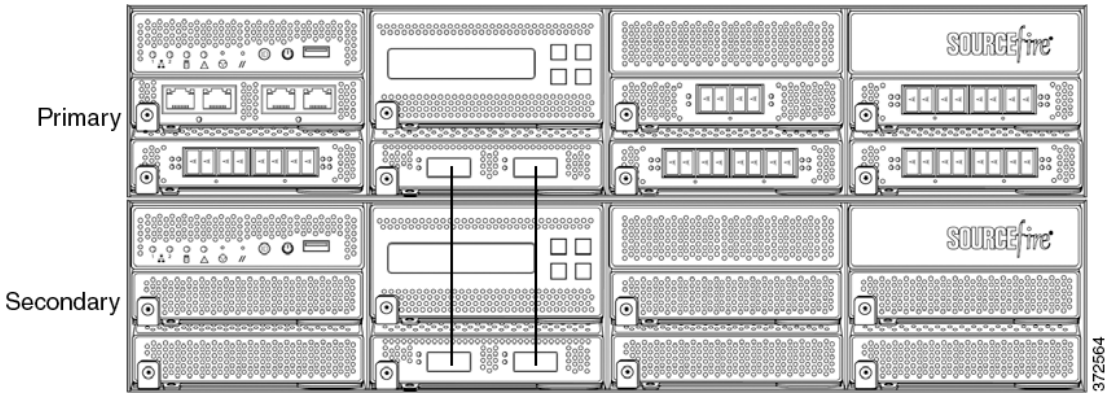
デバイスをラック内に設置して、スタッキング モジュール間をケーブルで容易に接続できるようにします。プライマリ デバイスの上または下にセカンダリ デバイスを設置できます。

単一の Firepower 8250 または 8350（Firepower または AMP）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。設定内のセカンダリ デバイスの数に必要な分だけ、各セカンダリ デバイスをプライマリ デバイスに直接接続します。

注意　すべてのデバイスのスタック メンバに対して管理インターフェイスが設定され、機能する**必要があります**。すべてのデバイスを単一のデバイスとして登録し、これらをスタックしてください。スタック構成のセカンダリ デバイスの管理インターフェイスを削除したり、無効化したりしないでください。これにより、スタック メンバはそれぞれヘルスをレポートし、設定情報を交換できます。

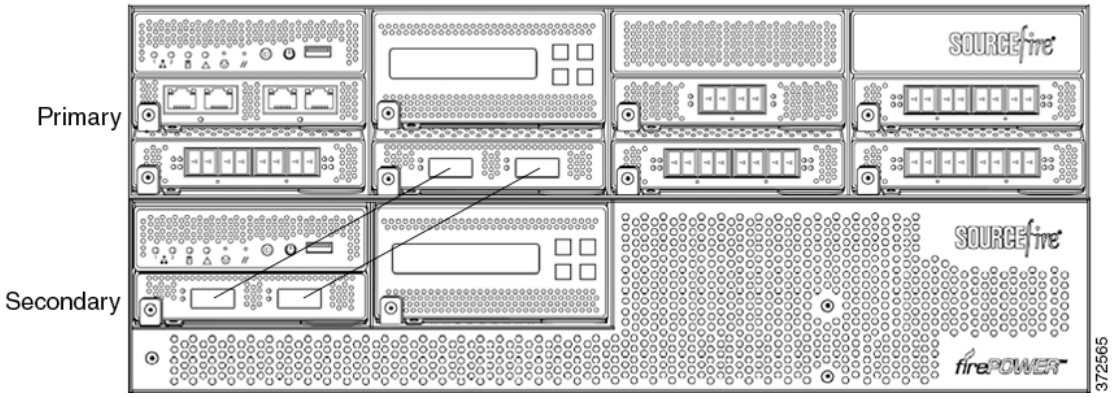
8250 または 8350 プライマリ デバイスと 1 つのセカンダリ デバイス

次に、Firepower 8250 または 8350（Firepower または AMP）プライマリ デバイスと 1 つのセカンダリ デバイスの例を示します。セカンダリ デバイスがプライマリ デバイスの下に設置されています。セカンダリ デバイスにはセンシング インターフェイスがないことに注意してください。



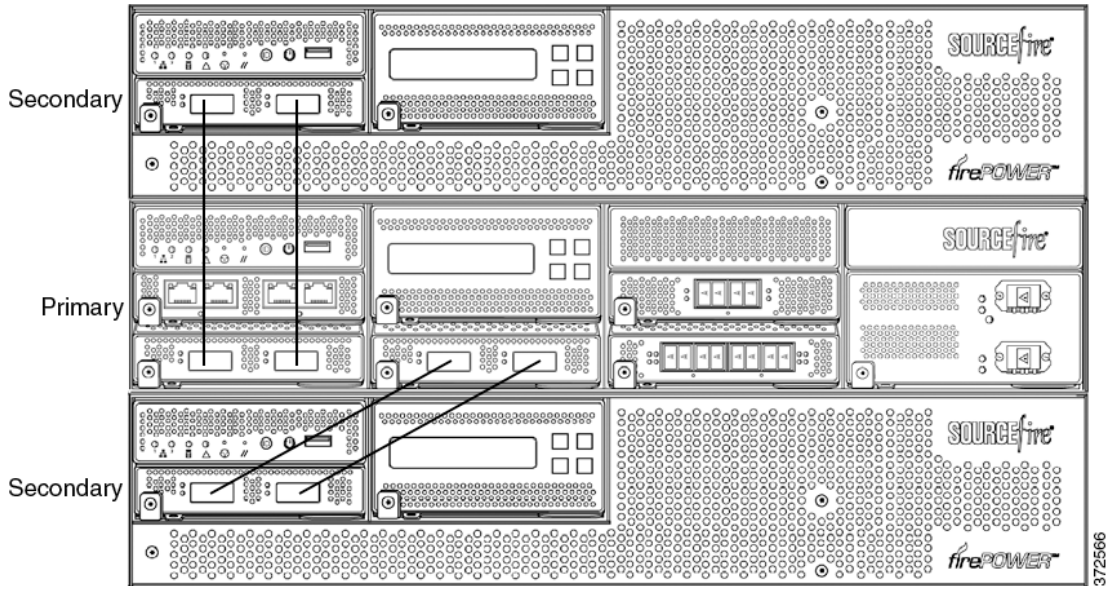
8260 または 8360 プライマリ デバイスと 1 つのセカンダリ デバイス

次に、Firepower 8260 または 8360（Firepower または AMP）の設定例を示します。Firepower 8260 には 10G 対応 8250 プライマリ デバイスと 1 つの専用セカンダリ デバイスが含まれています。Firepower または AMP 8360 には 40G 対応 8350 プライマリ デバイスと 1 つの専用セカンダリ デバイスが含まれています。各設定（8260 または 8360）で、セカンダリ デバイスがプライマリ デバイスの下に設置されます。



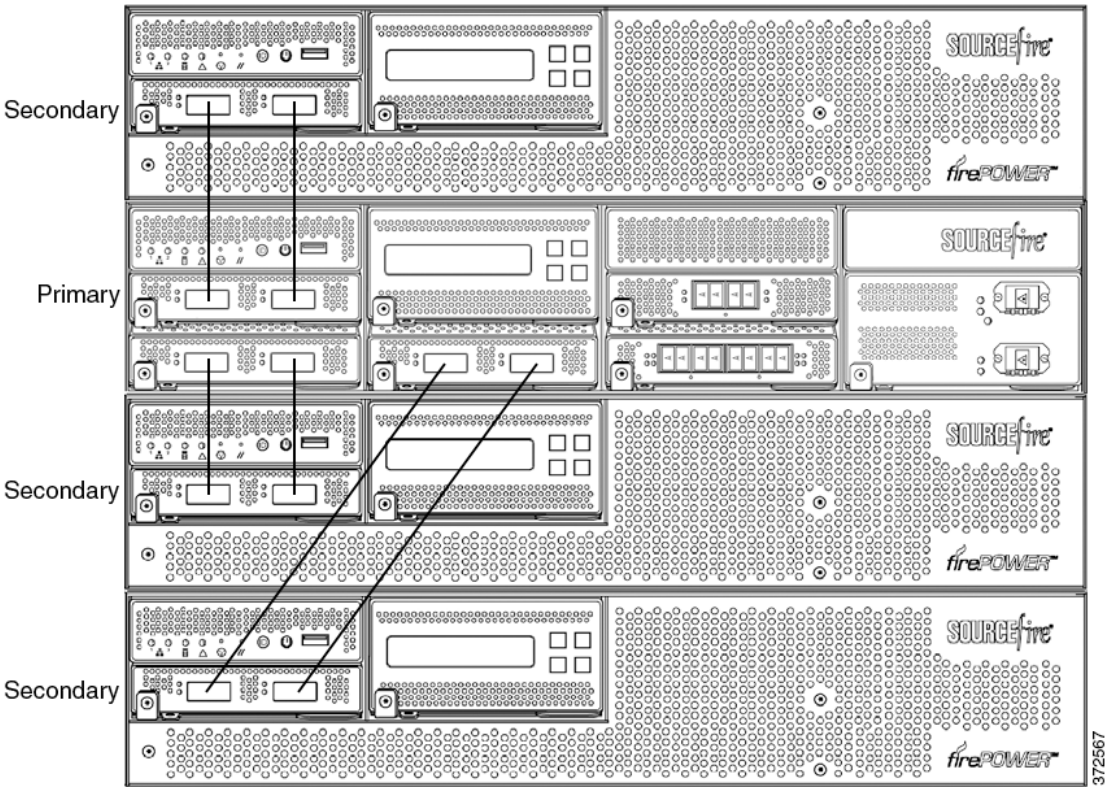
8270 または 8370 プライマリ デバイス（40G）と 2 つのセカンダリ デバイス

次に、Firepower 8270 または 8370（Firepower または AMP）の設定例を示します。Firepower 8270 には 40G 対応 8250 プライマリ デバイスと 2 つの専用セカンダリ デバイスが含まれています。Firepower または AMP 8370 には 40G 対応 8350 プライマリ デバイスと 2 つの専用セカンダリ デバイスが含まれています。各設定（8270 または 8370）で、1 つのセカンダリ デバイスがプライマリ デバイスの上に設置され、もう 1 つのセカンダリ デバイスがプライマリ デバイスの下に設置されます。



8290 または 8390 プライマリ デバイス（40G）と 3 つのセカンダリ デバイス

次に、Firepower 8290 または 8390（Firepower または AMP）の設定例を示します。Firepower 8290 には 40G 対応 8250 プライマリ デバイスと 3 つの専用セカンダリ デバイスが含まれています。Firepower または AMP 8370 には 40G 対応 8350 プライマリ デバイスと 2 つの専用セカンダリ デバイスが含まれています。各設定（8290 または 8390）で、1 つのセカンダリ デバイスがプライマリ デバイスの上に設置され、2 つのセカンダリ デバイスがプライマリ デバイスの下に設置されます。



8250 または 8350 セカンダリ デバイスを接続するには:

ステップ 1　8000 シリーズスタッキング ケーブルを使用して、プライマリ デバイス上のスタッキング モジュールの左側のインターフェイスをセカンダリ デバイス上のスタッキング モジュールの左側のインターフェイスに接続します。

ステップ 2　2 本目の 8000 シリーズスタッキング ケーブルを使用して、プライマリ デバイス上のスタッキング モジュールの右側のインターフェイスをセカンダリ デバイス上のスタッキング モジュールの右側のインターフェイスに接続します。

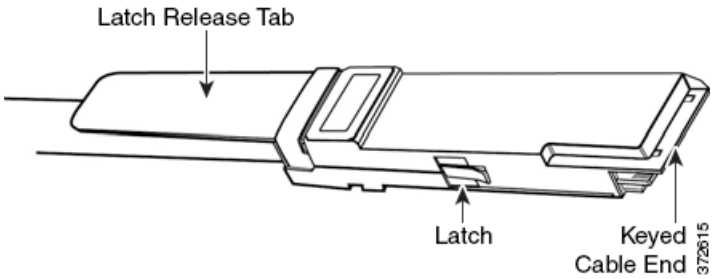
ステップ 3　接続するセカンダリ デバイスごとにステップ 1 と 2 を繰り返します。

ステップ 4　デバイスを管理する Firepower Management Center を使用して、スタック構成デバイスの関係を構築し、共有リソースを管理します。スタック構成デバイスの管理（3-18 ページ）を参照してください。

注意　すべてのデバイスのスタック メンバに対して管理インターフェイスが設定され、機能する**必要があります**。すべてのデバイスを単一のデバイスとして登録し、これらをスタックしてください。スタック構成のセカンダリ デバイスの管理インターフェイスを削除したり、無効化したりしないでください。これにより、スタック メンバはそれぞれヘルスをレポートし、設定情報を交換できます。

8000 シリーズスタッキング ケーブルの使用

8000 シリーズスタッキング ケーブルは先端が同様の鍵型になっており、デバイスにケーブルを固定するためのラッチとラッチ解放つまみが付いています。



8000 シリーズスタッキング ケーブルを使用して、デバイス設定ごとに必要なプライマリ デバイスと各セカンダリ デバイス間の物理接続を構築します。

- Firepower 8250、8260、8270、および 8290 には接続ごとに 2 本ずつのケーブルが必要
- Firepower または AMP 8350、8360、8370、および 8390 には接続ごとに 2 本ずつのケーブルが必要
- Firepower 8140 には 1 本のケーブルが必要

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。

注意　デバイスを配線する場合は、Cisco 8000 シリーズスタッキング ケーブルだけを使用してください。サポートされていないケーブルを使用すると予期せぬエラーが発生する可能性があります。

デバイスを物理的に接続したら、Firepower Management Center を使用して、スタック構成デバイスを管理します。

8000 シリーズスタッキング ケーブルを挿入するには:

ステップ 1　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。

8000 シリーズスタッキング ケーブルを取り外すには:

ステップ 1　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。

スタック構成デバイスの管理

Firepower Management Center は、デバイス同士のスタック関係を構築し、プライマリ デバイスのインターフェイス セットを制御し、スタック内の統合リソースを管理します。スタック構成デバイスのローカル Web インターフェイス上でインターフェイス セットを管理することはできません。

スタック構成関係が構築されると、すべてのデバイスで単一の共有検出設定を使用してトラフィックが個別に検査されます。プライマリ デバイスで障害が発生した場合は、プライマリ デバイスの設定に基づいてトラフィックが処理されます(つまり、スタック構成関係が存在しない場合と同様)。セカンダリ デバイスで障害が発生した場合は、プライマリ デバイスがトラフィックを検査して、アラートを生成し、トラフィックが破棄された故障中のセカンダリ デバイスにトラフィックを送信し続けます。

スタック構成デバイスを構築および管理する方法については、『*Firepower Management Center Configuration Guide*』の「Managing Stacked Devices」を参照してください。

ラックへの Firepower デバイスの設置

すべての Firepower デバイスをラックマウントできます。アプライアンスを設置するときに、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する必要もあります。初期設定でコンソールにアクセスするには、次のいずれかの方法で 1 つのアプライアンスに接続します。

キーボードとモニタ/KVM

USB キーボードと VGA モニタを 1 つの Firepower デバイスに接続できます。これは、キーボード、ビデオ、およびマウス(KVM)スイッチに接続される、ラックマウント アプライアンスで便利です。

注意　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。

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。

初期設定後に、次の追加の方法でコンソールにアクセスできます。

シリアル接続/ラップトップ

物理シリアル ポートを使用して、コンピュータを任意の Firepower デバイスに接続できます。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。

Firepower 8000 シリーズデバイスのシリアル ポートは RJ-45 接続を使用します。

適切なロールオーバー ケーブルをデバイスに接続した後、*FirePower 8000 シリーズ スタートアップ ガイド*に記載されているようにコンソール出力をリダイレクトします。各アプライアンスのシリアル ポートを特定するには、ハードウェア仕様（2-1 ページ）の図を使用してください。

Serial over LAN を使用した Lights-Out Management

LOM 機能を使用すると、SOL 接続を通して Firepower Management Center または Firepower デバイスに対して限定的なアクション セットを実行できます。LOM 対応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、この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。詳細については、*FirePower 8000 シリーズ スタートアップ ガイド*を参照してください。

コメント　Lights-Out Management は、デフォルト（`eth0`）管理インターフェイス上でのみ使用可能です。

LOM を使用してアプライアンスを工場出荷時設定に復元するには、ネットワーク設定を削除**しないでください**。ネットワーク設定を削除すると、LOM 接続もドロップされます。詳細については、*FirePower 8000 シリーズ スタートアップ ガイド*を参照してください。

アプライアンスを設置するには:

ステップ 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。

ステップ 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。

ステップ 3　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。

ステップ 4　Firepower デバイスの場合は、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。銅線インターフェイスでのインライン展開のケーブル配線（6-6 ページ）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 管理対象デバイスの展開（6-1 ページ）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。設置と遅延のテストについては、インライン バイパス インターフェイスの設置のテスト（3-20 ページ）を参照してください。

ステップ 5　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、別々の電源に差し込みます。

ステップ 6　アプライアンスの電源をオンにします。

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、銅線インターフェイスでのインライン展開のケーブル配線（6-6 ページ）を参照してください。

次の作業

- 新しいアプライアンスが信頼された管理ネットワークで通信できるようにするセットアップ プロセスを実行します。*FirePower 8000 シリーズ スタートアップ ガイド*を参照してください。
- バイパス インターフェイスを使用してデバイスを展開している場合は、それらのデバイスが正しく設置されているかどうかをテストします。インライン バイパス インターフェイスの設置のテスト（3-20 ページ）を参照してください。

インライン バイパス インターフェイスの設置のテスト

バイパス インターフェイスを備えた管理対象デバイスは、デバイスの電源がオフになっていても、デバイスが動作不能でもネットワーク接続を維持することができます。このようなデバイスが適切に設置され、それによる遅延が定量化されていることを確認することが重要です。

コメント　スイッチのスパニング ツリー ディスカバリ プロトコルは 30 秒のトラフィック遅延を引き起こす可能性があります。Cisco では、次の手順でスパニング ツリーを無効にすることを推奨しています。

銅線インターフェイスにのみ適用可能な次の手順では、インライン バイパス インターフェイスの設置と ping の遅延をテストする方法について説明します。ping テストを実行するネットワークに接続し、管理対象デバイスのコンソールに接続する必要があります。

はじめる前に

- Firepower デバイスのインターフェイス セット タイプがインライン バイパス モード用に設定されていることを確認します。
  インターフェイス セットをインライン バイパス モード用に設定する手順については、『*Firepower Management Center Configuration Guide*』の「Configuring Inline Sets」を参照してください。

インライン バイパス インターフェイスが設置されたデバイスをテストするには:

アクセス:Admin

ステップ 1　スイッチ上のすべてのインターフェイス、ファイアウォール、およびデバイスのセンシング インターフェイスを自動ネゴシエーションに設定します。

コメント　Firepower システムデバイスでは、自動 MDIX を使用する場合に自動ネゴシエーションが必要です。

ステップ 2　デバイスの電源をオフにして、すべてのネットワーク ケーブルを外します。

デバイスを再接続して、適切なネットワーク接続が存在することを確認します。デバイスからスイッチおよびファイアウォールへのクロス ケーブルとストレート ケーブルの配線手順を確認します。銅線インターフェイスでのインライン展開のケーブル配線（6-6 ページ）を参照してください。

ステップ 3　デバイスの電源をオフにして、デバイス経由でファイアウォールからスイッチに ping できることを確認します。

ping が失敗した場合は、ネットワーク配線を修正します。

ステップ 4　ステップ 9 が完了するまで継続的に ping を実行します。

ステップ 5　デバイスの電源をオンにします。

ステップ 6　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デバイスにログインします。パスワードは、デバイスの Web インターフェイスのパスワードと同じです。

デバイスのプロンプトが表示されます。

ステップ 7　「`system shutdown`」と入力して、デバイスをシャットダウンします。

また、Web インターフェイスを使用してデバイスをシャットダウンすることもできます。『*Firepower Management Center Configuration Guide*』の「Managing Devices」の章を参照してください。ほとんどのデバイスで電源をオフにすると、カチッという音がします。この音は、リレーが切り替わって、デバイスがハードウェア バイパスに移行した音です。

ステップ 8　30 秒間待機します。

ping トラフィックが再開したことを確認します。

ステップ 9　デバイスの電源をオンにして、ping トラフィックが継続的に通過していることを確認します。

ステップ 10　タップ モードをサポートする Firepower デバイスの場合は、次の条件下で ping 遅延結果をテストして記録できます。

- デバイスの電源がオフ
- デバイスの電源がオン、ポリシーにルールが適用されていない、インライン侵入ポリシー保護モード

- デバイスの電源がオン、ポリシーにルールが適用されていない、インライン侵入ポリシー保護タップ モード
- デバイスの電源がオン、ポリシーに調整済みのルールが適用されている、インライン侵入ポリシー保護モード

設置の遅延期間が容認できる範囲であることを確認します。過剰な遅延の問題の解決方法については、『*Firepower Management Center Configuration Guide*』の「Configuring Packet Latency Thresholding and Understanding Rule Latency Thresholding」を参照してください。

Firepower デバイス上の LCD パネルの使用

システムの Web インターフェイスの代わりに、Firepower デバイス前面の LCD パネルを使用して、デバイス情報を表示したり、特定の設定を構成したりすることができます。

LCD パネルにはディスプレイと 4 つの Multi-Function キーがあり、複数の異なる動作モードが用意されています。モードによって異なる情報が表示され、デバイスの状態に応じて異なる設定を構成できるようになっています。

詳細については、次の項を参照してください。

- LCD パネルのコンポーネントについて (4-2 ページ) では、LCD パネルのコンポーネントを識別する方法、およびパネルのメイン メニューを表示する方法を説明しています。
- LCD パネルの Multi-Function キーの使用 (4-3 ページ) では、LCD パネルの Multi-Function キーを使用する方法を説明しています。
- アイドル ディスプレイ モード (4-4 ページ) では、デバイスがアイドル状態のときに LCD パネルに表示される各種のシステム情報について説明しています。
- ネットワーク コンフィギュレーション モード (4-4 ページ) は、LCD パネルを使用してデバイスの管理インターフェイスのネットワーク構成 (IPv4 または IPv6 アドレス、サブネット マスクまたはプレフィックス、およびデフォルト ゲートウェイ) を設定する方法について説明します。

注意 LCD パネルを使用して再設定できるようにすると、セキュリティ リスクが生じる可能性があります。LCD パネルを使用して設定を行うために必要なのは、物理的なアクセスだけであり、認証は必要ありません。

- システム ステータス モード (4-7 ページ) では、モニタ対象システムの情報 (リンク状態の伝搬、バイパス ステータス、システム リソースなど) を表示する方法、および LCD パネルの輝度とコントラストを変更する方法を説明しています。
- 情報モード (4-8 ページ) では、システムの識別情報 (デバイスのシャーシ シリアル番号、IP アドレス、モデル、ソフトウェアおよびファームウェアのバージョンなど) を表示する方法を説明しています。
- エラー アラート モード (4-9 ページ) では、LCD パネルでのエラーまたは障害状態 (バイパス、ファン ステータス、ハードウェア アラートなど) の通知について説明します。

コメント LCD パネルを使用するには、デバイスの電源が投入されている必要があります。デバイスの安全な電源投入またはシャットダウン方法については、『*Firepower Management Center Configuration Guide*』の「*Managing Devices*」の章を参照してください。

LCD パネルのコンポーネントについて

デバイスFirepower 前面の LCD パネルには、ディスプレイと 4 つの Multi-Function キーがあります。

- ディスプレイには 2 行のテキスト（各行につき最大 17 文字）と、Multi-Function キー マップが表示されます。マップには、対応する Multi-Function キーで実行できる操作が記号で示されます。
- Multi-Function キーを使用して、システム情報を表示したり、基本的な設定タスクを実行したりすることができます。表示される情報と実行可能なタスクは、LCD パネルのモードに応じて異なります。詳細については、LCD パネルの Multi-Function キーの使用（4-3 ページ）を参照してください。

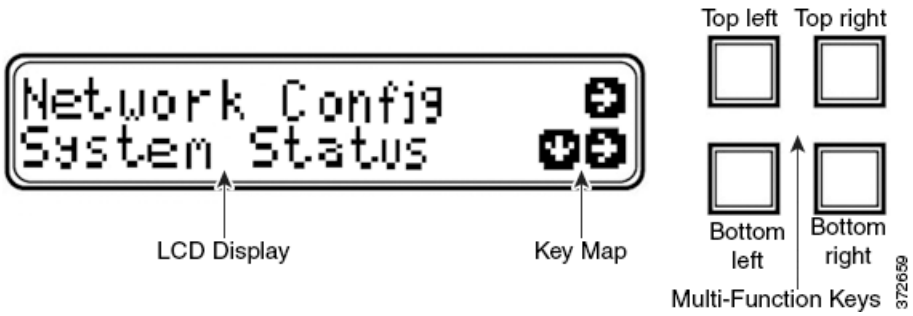
以下の図に、パネルの [Idle Display] モード（デフォルトのモード）を示します。このモードでは、キー マップは表示されません。

図 4-1　　アイドル ディスプレイ モードの LCD パネル

アイドル ディスプレイ モードでは、パネルに CPU 使用率および使用可能な空きメモリ容量と、シャーシ シリアル番号が交互に表示されます。任意のキーを押すと [Idle Display] モードは中断し、[Network Configuration]、[System Status]、および [Information] モードにアクセスできる LCD パネルのメイン メニューが表示されます。

以下の図に、メイン メニューを示します。メイン メニューには、4 つの Multi-Function キー（左上、右上、左下、右下）のそれぞれに対応するキー マップが表示されます。

図 4-2　　LCD パネルのメイン メニュー



メイン メニューにアクセスするには:

ステップ 1　アイドル ディスプレイ モードで、任意の Multi-Function キーを押します。

メイン メニューが表示されます。

- デバイスのネットワーク コンフィギュレーションを変更する場合は、ネットワーク コンフィギュレーション モード（4-4 ページ）を参照してください。

- モニタ対象システムの情報を表示する場合、または LCD パネルの輝度とコントラストを調整する場合は、システム ステータス モード (4-7 ページ)を参照してください。
- システムの識別情報を表示する場合は、情報モード (4-8 ページ)を参照してください。

コメント　LCD パネルがアイドル ディスプレイ モードに切り替わるときに Multi-Function キーを押すと、予期しないメニューが表示されることがあります。

LCD パネルの Multi-Function キーの使用

LCD パネルでは、4 つの多機能キーを使用してメニューとオプションに移動できます。これらの Multi-Function キーを使用できるのは、ディスプレイにキー マップが表示されている場合です。マップ上の記号の位置は、各機能およびその機能を実行するために使用するキーの位置に対応します。記号が表示されていない場合、対応するキーで実行できる機能はありません。

ヒント　LCD パネルのモードによって、記号の機能は異なります(したがって、表示されるキー マップも異なります)。期待する結果を得られない場合は、LCD パネルのモードを確認してください。

以下の表に、Multi-Function キーの機能を記載します。

表 4-1　LCD パネルの Multi-Function キー

記号	説明	機能
↑	上矢印	現在のメニュー オプションのリストをスクロールアップします。
↓	下矢印	現在のメニュー オプションのリストをスクロールダウンします。
←	左矢印	以下のいずれかの操作を実行します。 • 操作を実行せずに、LCD パネル メニューを表示します。 • カーソルを左に移動します。 • 再び編集可能にします。
→	→	以下のいずれかの操作を実行します。 • その行に示されているメニュー オプションに移動します。 • カーソルを右に移動します。 • 以降に続くテキストにスクロールします。
X	キャンセル	操作をキャンセルします。
+	追加	選択された数値を 1 つ増やします。
-	減算	選択された数値を 1 つ減らします。
✓	チェックマーク	操作を受け入れます。

アイドル ディスプレイ モード

エラーが検出されない状態で、60 秒間操作が行われないと（Multi-Function キーが押されないと）、LCD パネルはアイドル ディスプレイ モードに切り替わります。システムがエラーを検出すると、そのエラーが解決されるまで、パネルはエラー アラート モードになります（エラー アラート モード（4-9 ページ）を参照）。ネットワーク設定の編集中や診断の実行中も、[Idle Display] モードが無効になります。

[Idle Display] モードでは、パネルに CPU 使用率および使用可能な空きメモリ容量と、シャーシ シリアル番号が（5 秒間隔で）交互に表示されます。

以下に、それぞれの表示例を示します。

```
CPU: 50%
FREE MEM: 1024 MB
```

または

```
Serial Number:
3D99-101089108-BA0Z
```

アイドル ディスプレイ モードの状態で Multi-Function キーを押すと、メイン メニューが表示されます。LCD パネルのコンポーネントについて（4-2 ページ）を参照してください。

コメント　LCD パネルがアイドル ディスプレイ モードに切り替わるときに Multi-Function キーを押すと、予期しないメニューが表示されることがあります。

ネットワーク コンフィギュレーション モード

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。[Network Configuration] モードでは、LCD パネルを使用して、Firepower デバイスの管理インターフェイスのネットワーク設定（IP アドレス、サブネット マスクまたはプレフィックス、デフォルト ゲートウェイ）を設定できます。

LCD パネルを使用して Firepower デバイスの IP アドレスを編集する場合、管理元の Management Center に変更が反映されることを確認してください。場合によっては、デバイス管理設定を手動で編集する必要があります。詳細については、『』を参照してください。

デフォルトでは、LCD パネルを使用してネットワーク設定を変更する機能は無効になっています。このオプションは、初期設定プロセス中、あるいはデバイスの Web インターフェイスを使用して有効にすることができます。詳細については、LCD パネルを使用したネットワーク再設定の許可（4-6 ページ）を参照してください。

注意　このオプションを有効にすると、セキュリティ リスクが生じ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。

[Network Configuration] モードを使用してネットワーク設定を行うには、以下を行います。

ステップ 1　アイドル ディスプレイ モードで、Multi-Function キーを押してメイン メニューを表示します。

メイン メニューが表示されます。

```
Network Config        →
System Status         ↓ →
```

ステップ 2　上の行の右矢印キーを押して、ネットワーク コンフィギュレーション モードにアクセスします。

LCD パネルに以下のオプションが表示されます。

```
IPv4                ↓ →
IPv6                  →
```

ステップ 3　設定する IP アドレスを選択するには、該当する右矢印キーを押します。

- IPv4 の場合、LCD パネルには次のオプションが表示されます。

```
IPv4 set to DHCP.     ←
Enable Manual?        →
```

- IPv6 の場合、LCD パネルには次のオプションが表示されます。

```
IPv6 Disabled.        ←
Enable Manual?        →
```

ステップ 4　手動でネットワークを設定するには、右矢印キーを押します。

- IPv4 の場合、LCD パネルに IPv4 アドレスが表示されます。次に例を示します。

```
IPv4 Address:      - +
194.170.001.001    X →
```

- IPv6 の場合、LCD パネルに空白の IPv6 アドレスが表示されます。次に例を示します。

```
IPv6 Address:      - +
0000:0000:0000:00 X →
```

IPv4 アドレスと IPv6 アドレスのどちらを編集しているかは、パネルの最初の行に示されます。2 番目の行に、編集中の IP アドレスが示されます。カーソルは最初の桁の下に配置され、編集中の桁を示します。各行の右側にある 2 つの記号は、Multi-Function キーに対応します。

IPv6 アドレスは、ディスプレイに収まりきらないことに注意してください。各桁の編集を進めていくとカーソルが右に移動し、IPv6 アドレスが右にスクロールしていきます。

ステップ 5　必要に応じて、カーソルが下に配置されていない桁を編集し、IP アドレスの次の桁に移動します。

- 桁を編集するには、上の行のマイナス(-)キーまたはプラス(+)キーを押して、その桁の数値を 1 つずつ増減します。
- IP アドレスの次の桁に移動するには、下の行にある右矢印キーを押して、カーソルを右隣の桁に移動します。

カーソルが最初の桁に配置されているときには、LCD パネル上の IP アドレスの末尾にキャンセル記号と右矢印記号が表示されます。カーソルが最初の桁以外の桁に配置されているときには、LCD パネルに左矢印と右矢印の記号が表示されます。

ステップ 6　IPv4 または IPv6 アドレスの編集が完了したら、右矢印キーを再度押してチェックマーク(✓)キーを表示し、変更を受け入れます。

右矢印キーを押す前は、ディスプレイ上の機能記号は以下のように表示されます。

```
IPv4 Address:      - +
194.170.001.001    X →
```

右矢印キーを押した後は、ディスプレイ上の機能記号は以下のように表示されます。

```
IPv4 Address:      X ✓
194.170.001.001    ←
```

ステップ 7　IP アドレスに対する変更を受け入れるには、チェックマーク キーを押します。

IPv4 の場合、LCD パネルに以下が表示されます。

```
Subnet Mask:       - +
000.000.000.000    X →
```

IPv6 の場合、LCD パネルに以下が表示されます。

```
Prefix:          - +
000.000.000.000  X →
```

ステップ 8　IP アドレスを編集する場合と同じ方法で、サブネット マスクまたはプレフィックスを編集し、チェックマーク キーを押して変更を受け入れます。

LCD パネルに以下のオプションが表示されます。

```
Default Gateway  - +
000.000.000.000  X →
```

ステップ 9　IP アドレスを編集する場合と同じ方法で、デフォルト ゲートウェイを編集し、チェックマーク キーを押して変更を受け入れます。

LCD パネルに以下のオプションが表示されます。

```
Save?            ✓
                 X
```

ステップ 10　変更を保存するには、チェックマーク キーを押します。

LCD パネルを使用したネットワーク再設定の許可

セキュリティ リスクが生じるため、LCD パネルを使用してネットワーク設定を変更する機能は、デフォルトでは無効になっています。このオプションは、初期設定プロセス中に有効にすることができます（*FirePower 8000 シリーズ スタートアップ ガイド*を参照）。または、以下の手順に従って、デバイスの Web インターフェイスで有効にすることもできます。

デバイスの LCD パネルでのネットワーク再設定を許可するには:

アクセス:Admin

ステップ 1　デバイスの初期設定を完了したら、管理者特権が割り当てられたアカウントを使用して、デバイスの Web インターフェイスにログインします。

ステップ 2　[System] > [Local] > [Configuration] の順に選択します。

[Information] ページが表示されます。

ステップ 3　[ネットワーク（Network）] をクリックします。

[Network Settings] ページが表示されます。

ステップ 4　[LCD Panel] の下にある [Allow reconfiguration of network configuration] チェック ボックスを選択します。セキュリティ警告が表示されたら、このオプションを有効にすることを確認します。

ヒント　このページで示される他のオプションの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

ステップ 5　[Save] をクリックします。

ネットワーク設定が変更されます。

システム ステータス モード

LCD パネルのシステム ステータス モードでは、モニタ対象システムの情報として、リンク状態の伝搬、バイパス ステータス、システム リソースなどが表示されます。システム ステータス モードでも、LCD パネルの輝度とコントラストを変更できます。

次の表に、このモードで使用できる情報およびオプションを記載します。

表 4-2　システム ステータス モードのオプション

オプション	説明
Resources	CPU 使用率と使用可能な空きメモリが表示されます。この情報は、[Idle Display] モードでも表示されます。

Link State	現在使用中のインライン セットと、そのセットのリンク状態ステータスのリストが表示されます。最初の行はインライン セットを識別し、2 番目の行は、そのセットのステータス（正常またはトリップ）を表示します。次に例を示します。
	`eth2-eth3:`
	`normal`

Fail Open	使用中のバイパス インライン セットと、それらのペアのステータス（正常またはバイパス）のリストが表示されます。
Fan Status	デバイスのファンとそのステータスのリストが表示されます。
Diagnostics	サポートから使用可能な特定のキー シーケンスを押した後にアクセス可能になります。 **注意**　サポートの指示がない限り、診断メニューにアクセス**しないでください**。サポートからの特定の指示なしで診断メニューにアクセスすると、システムが破損することがあります。
LCD Brightness	LCD ディスプレイの輝度を調整する場合に使用します。
LCD Contrast	LCD ディスプレイのコントラストを調整する場合に使用します。

システム ステータス モードに切り替えてモニタ対象システムの情報を表示するには：

ステップ 1　アイドル ディスプレイ モードで、Multi-Function キーを押してメイン メニューを表示します。

メイン メニューが表示されます。

```
Network Config          →
System Status       ↓   →
```

ステップ 2　下の行にある右矢印（→）キーを押して、システム ステータス モードにアクセスします。

LCD パネルに以下のオプションが表示されます。

```
Resources           ↓   →
Link State          ↓   →
```

ステップ 3　下矢印（â）キーを押して、オプションをスクロールします。表示するステータスの行で横に表示された右矢印キーを押します。

選択したオプションに応じて、LCD パネルに表 4-2（4-7 ページ）にリストされている情報が表示されます。LCD パネルの輝度またはコントラストを変更するには、次の手順を参照してください。

LCD パネルの輝度またはコントラストを調整するには:

ステップ 1　システム ステータス モードで、LCD パネルに [LCD Brightness] および [LCD Contrast] オプションが表示されるまで、下矢印(â)キーを押してオプションをスクロールします。

```
LCD Brightness      ↓ →
LCD Contrast        ↓ →
```

ステップ 2　調整する LCD ディスプレイ機能(輝度またはコントラスト)の行で横に表示された右矢印キーを押します。

LCD パネルに以下のオプションが表示されます。

```
Increase            →
Decrease            ↓ →
```

ステップ 3　右矢印キーを押して、選択したディスプレイ機能の値を増減します。

キーを押すごとに LCD ディスプレイが変化します。

ステップ 4　下矢印を押して、[Exit] オプションを表示します。

```
Decrease            ↓ →
Exit                →
```

ステップ 5　[Exit] 行で右矢印キーを押して設定を保存し、メイン メニューに戻ります。

情報モード

LCD パネルの情報モードでは、システムの識別情報として、デバイスのシャーシ シリアル番号、IP アドレス、モデル、およびソフトウェアとファームウェア バージョンが表示されます。サポートに支援を要請する場合に、この情報が必要になることがあります。

次の表に、このモードで使用できる情報を記載します。

表 4-3　情報モードのオプション

オプション	説明
IP address	デバイスの管理インターフェイスの IP アドレスが示されます。
Model	デバイスのモデルが示されます。
Serial number	デバイスのシャーシ シリアル番号が示されます。
Versions	デバイスのシステム ソフトウェアおよびファームウェアのバージョンが示されます。以下の情報をスクロールするには、Multi-Function キーを使用します。 • 製品バージョン • NFE のバージョン • マイクロ エンジンのバージョン • Flash のバージョン • GerChr のバージョン

情報モードに切り替えてシステムの識別情報を表示するには:

ステップ 1　アイドル ディスプレイ モードで、Multi-Function キーを押してメイン メニューを表示します。

メイン メニューが表示されます。

```
Network Config          →
System Status        ↓  →
```

ステップ 2　LCD パネルに [Information] モードが表示されるまで、下矢印(â)キーを押してモードをスクロールします。

```
System Status        ↓  →
Information          ↓  →
```

ステップ 3　下の行にある右矢印(→)キーを押して、情報モードにアクセスします。

ステップ 4　下矢印(â)キーを押して、オプションをスクロールします。表示する情報の横の行にある右矢印キーを押します。

選択したオプションに応じて、LCD パネルに表 4-3(4-8 ページ)にリストされている情報が表示されます。

エラー アラート モード

ハードウェア エラーや障害状態が発生した場合、[Idle Display] モードは中断されて [Error Alert] モードになります。エラー アラート モードでは、LCD ディスプレイが点滅し、次の表にリストするエラーのうち、1 つ以上のエラーが表示されます。

表 4-4　　LCD パネルのエラー アラート

エラー	説明
Hardware alarm	ハードウェア アラームに関するアラート
Link state propagation	ペアになっているインターフェイスのリンク状態が表示されます。
Bypass	バイパス モードで設定されたインライン セットのステータスが表示されます。
Fan status	ファンがクリティカル条件に達した時点でアラートが出されます。

ハードウェア エラーのアラートが発生すると、LCD ディスプレイにハードウェア アラートのメイン メニューが次のように表示されます。

```
HARDWARE ERROR!         →
Exit                    →
```

多機能キーを使用して、エラー アラートのリストをスクロールしたり、[Error Alert] モードを終了したりできます。注意すべき点として、すべてのエラー状態が解決されるまで LCD ディスプレイは点滅し、アラート メッセージを表示します。

LCD パネルでは、常にプラットフォーム デーモン エラー メッセージが最初に表示され、それに続いて他のハードウェア エラー メッセージのリストが表示されます。次の表には、Firepower デバイスのエラー メッセージに関する基本情報が示されています。ここで、*x* はアラートを生成する NFE アクセラレータ カート(0 または 1)を示します。

表 4-5　ハードウェア アラームのエラー メッセージ

エラー メッセージ	監視対象条件	説明
NFE_platformd*X*	プラットフォーム デーモン	プラットフォーム デーモンが失敗したときにアラートを出します。
NFE_temp*X*	温度ステータス	アクセラレータ カードの温度が許容範囲を超えたときにアラートを出します。 • WARNING:97°C/206°F を超えた • CRITICAL:102°C/215°F を超えた
HeartBeat*X*	ハートビート	システムがハートビートを検出できないときにアラートを出します。
frag*X*	nfe_ipfragd(ホスト フラグ)デーモン	ipfragd デーモンが失敗したときにアラートを出します。
rules*X*	Rulesd(ホストのルール)デーモン	Rulesd デーモンが失敗したときにアラートを出します。
TCAM*X*	TCAM デーモン	TCAM デーモンが失敗したときにアラートを出します。
NFEMessD*X*	メッセージ デーモン	メッセージ デーモンが失敗したときにアラートを出します。
NFEHardware	ハードウェア ステータス	1 つ以上のアクセラレータ カードが通信していないときにアラートを出します。
NFEcount	検出されたカード	デバイスで検出されたアクセラレータ カード数がプラットフォームの予想アクセラレータ カード数に一致しないときにアラートを表示します。
NMSB_comm	通信	メディア アセンブリが存在しない場合や通信していない場合にアラートを出します。
scmd	scmd デーモン ステータス	scmd デーモンが失敗したときにアラートを出します。
psls	psls デーモン ステータス	psls デーモンが失敗したときにアラートを出します。
ftwo	ftwo デーモン ステータス	ftwo デーモンが失敗したときにアラートを出します。
NFE_port18 NFE_port19 NFE_port20 NFE_port21	内部リンクのステータス	ネットワーク モジュールのスイッチ ボードとアクセラレータ カードの間のリンクが失敗したときにアラートを出します。 • 81xx ファミリ:NFE_port18 および NFE_port19 のみ 82xx ファミリおよび 83xx ファミリ:NFE_port18、NFE_port19、NFE_port20、および NFE_port21

LCD ディスプレイにハードウェア アラートのエラー メッセージを表示するには、次の手順に従います。

ハードウェア アラートのエラー メッセージを確認するには、以下のようにします。

ステップ 1　[Error Alert] モードで、[HARDWARE ERROR!] 行にある右矢印(→)キーを押して、[Error Alert] モードをトリガーしたハードウェア エラーを表示させます。

LCD パネルに、NFE platform デーモンの障害から始まるエラー アラート メッセージがリストされ、それに続いてエラー メッセージのリストが表示されます。

```
NFEplatformd X
NFEtemp X                ↓
```

ここで、*x* はアラートを生成したアクセラレータ カード(0 または 1)です。

ステップ 2　エラーをさらに表示するには、エラー メッセージの行にある下矢印(â)キーを押します。その他のエラーがない場合、[Exit] 行が表示されます。

```
Exit                    →
```

ステップ 3　[Error Alert] モードを終了するには、右矢印(→)キーを押します。

アラートをトリガーしたエラーを解決する前にエラー アラート モードを終了すると、LCD パネルはエラー アラート モードに戻ります。支援が必要な場合は、サポートに連絡してください。

管理ネットワークでの展開

Firepower システムは、それぞれ固有のネットワーク アーキテクチャのニーズに応じて展開することができます。Management Center が、Firepower システムの集中管理コンソールおよびデータベース リポジトリとなります。トラフィック接続を収集して分析するために、複数のネットワーク セグメントにデバイスを設置します。

Management Center は管理インターフェイスを使用して、*信頼できる管理ネットワーク*(つまり、公開されている外部トラフィックではない安全な内部ネットワーク)に接続します。デバイスは、管理インターフェイスを使用して Management Center に接続します。

そして、デバイスはセンシング インターフェイスを使用して外部ネットワークに接続して、トラフィックをモニタします。展開におけるセンシング インターフェイスの使用方法の詳細については、Firepower 管理対象デバイスの展開(6-1 ページ)を参照してください。

管理展開に関する考慮事項

管理展開の決定は、さまざまな要因に基づいて行われます。以下の質問に答えることは、最も効率的かつ効果的なシステムを構成するための展開オプションの理解に役立ちます。

- デフォルトの単一の管理インターフェイスを使用してデバイスを Management Center に接続しますか? パフォーマンスを向上したり、Management Center で受信した別のネットワークからのトラフィックを分離するために、追加の管理インターフェイスを有効化しますか? 詳細については、管理インターフェイスについて(5-2 ページ)を参照してください。
- パフォーマンスを向上するために、トラフィック チャネルを有効化して Management Center と管理対象デバイスの間に 2 つの接続を作成しますか?Management Center と管理対象デバイスの間のスループット容量をさらに増加するために、複数の管理インターフェイスを使用しますか? 詳細については、複数のトラフィック チャネルを持つ場合の展開(5-3 ページ)を参照してください。
- 単一の Management Center を使用して、別のネットワーク デバイスからのトラフィックを管理および分離しますか? 詳細については、ネットワーク ルートを持つ場合の展開(5-5 ページ)を参照してください。
- 保護された環境に管理インターフェイスを展開しますか? アプライアンスのアクセスは、特定のワークステーション IP アドレスに制限されますか?セキュリティの考慮事項(5-5 ページ)には、管理インターフェイスを安全に展開するための考慮事項が説明されています。
- 8000 シリーズデバイスを展開しますか? 詳細については、特殊なケース:8000 シリーズデバイスの接続(5-6 ページ)を参照してください。

管理インターフェイスについて

管理インターフェイスは、防御センターが管理するすべてのデバイスと Management Center の間の通信手段を提供します。アプライアンス間のトラフィック制御を正常に維持することが、展開の成功に不可欠です。

Management Center および Firepower デバイス上では、Management Center またはデバイス上、あるいは両方の管理インターフェイスを使用して、アプライアンス間のトラフィックを 2 種類のトラフィック チャネルに分類できます。*管理トラフィック チャネル*は、すべての内部トラフィック（アプライアンスおよびシステムの管理専用のデバイス間トラフィックなど）を伝送し、*イベント トラフィック チャネル*は、すべてのイベント トラフィック（すなわち、侵入イベントやマルウェア イベントなどの大容量イベント トラフィック）を伝送します。トラフィックを 2 つのチャネルに分割することにより、アプライアンス間に 2 つの接続ポイントが作成されてスループットが増大するために、パフォーマンスが向上します。また、*複数の管理インターフェイス*を有効化して、アプライアンス間のスループットをさらに向上させたり、異なるネットワーク上のデバイス間のトラフィックの管理と分離を行うこともできます。

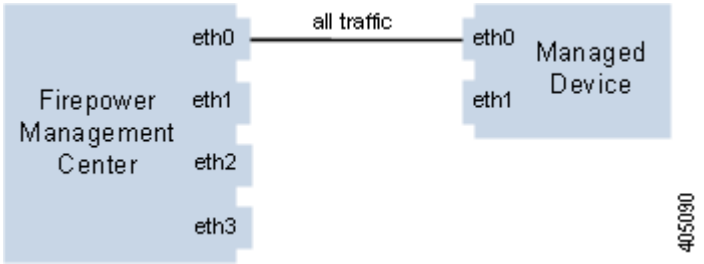
デバイスを Management Center に登録した後、各アプライアンスの Web ブラウザを使用してデフォルト設定を変更し、トラフィック チャネルや複数の管理インターフェイスの有効化ができます。設定については、*Firepower Management Center Configuration Guide* の「Configuring Appliance Settings」を参照してください。

通常、管理インターフェイスは、アプライアンスの背面に配置されています。詳細については、管理インターフェイスの識別（3-2 ページ）を参照してください。

単一の管理インターフェイス

デバイスを Management Center に登録すると、Management Center 上の管理インターフェイスとデバイス上の管理インターフェイスとの間のすべてのトラフィックを伝送する単一通信チャネルが確立されます。

以下の図に、デフォルトの単一通信チャネルを示します。1 つのインターフェイスにより、管理トラフィックとイベント トラフィックの両方が 1 つの通信チャネルで伝送されます。



複数の管理インターフェイス

複数の管理インターフェイスを有効化および設定して、それぞれに固有の IPv4 または IPv6 アドレス（および必要に応じてホスト名）を割り当て、各トラフィック チャネルを異なる管理インターフェイスに送信することによって、トラフィック スループットを大幅に向上できます。負荷が軽い管理トラフィックの搬送用には小さなインターフェイスを構成し、負荷が大きいイベント トラフィックの搬送用には大きなインターフェイスを構成します。デバイスを別々の管理インターフェイスに登録し、同一のインターフェイスに対して両方のトラフィック チャネルを構成したり、Management Center によって管理されるすべてのデバイスのイベント トラフィック チャネルを専用の管理インターフェイスで伝送することができます。

また、Management Center 上の特定の管理インターフェイスから別のネットワークまでのルートを作成することにより、あるネットワーク上のデバイスからのトラフィックと別のネットワーク上のデバイスからのトラフィックを、Management Center で別々に管理することもできます。

追加の管理インターフェイスは、以下の例外を使用して、デフォルト管理インターフェイスと同じように機能します。

- DHCP は、デフォルト（`eth0`）管理インターフェイスにのみ設定できます。追加のインターフェイス（`eth1` など）には、固有の静的 IP アドレスとホスト名が必要です。Cisco では、追加の管理インターフェイスの DNS エントリを設定する代わりに、これらのインターフェイスに対する IP アドレスのみを使用して Management Center およびデバイスを登録することを推奨しています。
- デフォルト以外の管理インターフェイスを使用して Management Center と管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。
- Lights-Out Management は、デフォルトの管理インターフェイスでのみ使用できます。
- 70xx ファミリでは、トラフィックを 2 つのチャネルに分離して、Management Center 上の 1 つ以上の管理インターフェイスにトラフィックを送信するようにそれらのチャネルを設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上で Management Center から送信されたトラフィックを受信します。

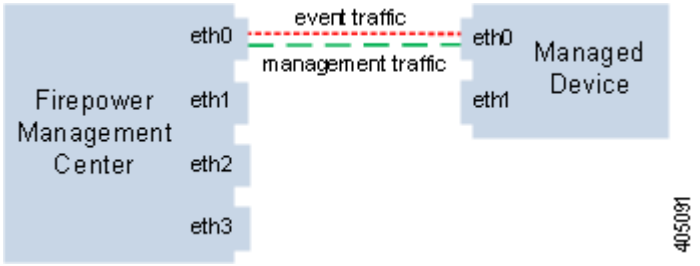
展開オプション

トラフィック チャネルを使用してトラフィック フローを管理することで、1 つ以上の管理インターフェイスを使用してシステムのパフォーマンスを向上させることができます。さらに、Management Center およびその管理対象デバイス上の専用の管理インターフェイスを使用して別のネットワークまでのルートを作成することにより、異なるネットワーク上のデバイス間のトラフィックを分離することもできます。詳細については、次の項を参照してください。

複数のトラフィック チャネルを持つ場合の展開

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、Management Center と管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。

次の例は、同じインターフェイス上に 2 つの独立したトラフィック チャネルを持つ通信チャネルを示しています。

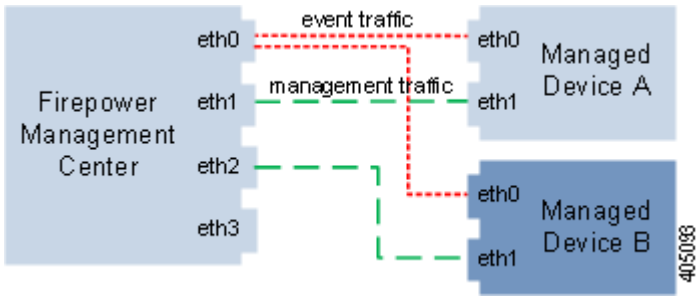


複数の管理インターフェイスを使用する場合、トラフィック チャネルを 2 つの管理インターフェイスに分割することによりパフォーマンスを向上できます。それによって両方のインターフェイス容量が増し、トラフィック フローが増加します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

次の図は、2 つの管理インターフェイス上にある管理トラフィック チャネルとイベント トラフィック チャネルを示しています。

専用の管理インターフェイスを使用して、複数のデバイスからのイベント トラフィックのみを伝送することができます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、Management Center 上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

以下の図では、2 台のデバイスが別々の管理チャネル トラフィック インターフェイスを使用し、イベント トラフィック チャネルに対しては同じ専用インターフェイスを共有しています。



ネットワーク ルートを持つ場合の展開

Management Center 上の特定の管理インターフェイスから別のネットワークまでのルートを作成できます。そのネットワークのデバイスを Management Center 上の指定された管理インターフェイスに登録すると、別のネットワーク上のデバイスと Management Center の間で独立した接続が実現されます。両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定することで、そのデバイスからのトラフィックが他のネットワーク上のデバイス トラフィックから確実に分離された状態を維持できます。ルーテッド インターフェイスは Management Center 上の他のすべてのインターフェイスから分離されているため、ルーテッド管理インターフェイスに障害が発生した場合、接続が失われます。

ヒント　デバイスを、デフォルト（eth0）の管理インターフェイス以外の管理インターフェイスの静的 IP アドレスに登録する必要があります。DHCP は、デフォルト管理インターフェイスだけでサポートされています。

Management Center をインストールした後に、Web インターフェイスを使用して、複数の管理インターフェイスを設定します。詳しくは、*Firepower Management Center Configuration Guide* の「Configuring Appliance Settings」を参照してください。

次の図では、2 つのデバイスですべてのトラフィックに対して別々の管理インターフェイスを使用することにより、ネットワーク トラフィックを分離しています。さらに管理インターフェイスを追加して、デバイスごとに独立した管理トラフィック チャネル インターフェイスとイベント トラフィック チャネル インターフェイスを構成できます。

セキュリティの考慮事項

管理インターフェイスを安全な環境に展開するために、Cisco では次の事項を考慮することを推奨しています。

- 管理インターフェイスは、必ず、不正アクセスから保護された信頼できる内部管理ネットワークに接続します。
- アプライアンスへのアクセスを許可可能な特定のワークステーションの IP アドレスを特定します。アプライアンスのシステム ポリシー内のアクセス リストを使用している特定のホストにアプライアンスへのアクセスを限定します。詳細については、*Firepower Management Center Configuration Guide* を参照してください。

特殊なケース:8000 シリーズデバイスの接続

サポートされるデバイス:8000 シリーズ

Management Center に 8000 シリーズのデバイスを登録するときは、接続の両側で自動ネゴシエーションするか、または両側を同じ固定速度に設定して安定したネットワーク リンクを確保する必要があります。8000 シリーズのデバイスは、半二重のネットワーク リンクをサポートしません。また、接続の反対側の速度構成やデュプレックス構成の違いもサポートしません。

Firepower 管理対象デバイスの展開

Firepower Management Center にデバイスを登録したら、侵入検知システムを使用してトラフィックを監視するため、または侵入防御システムを使用してネットワークを脅威から保護するために、デバイスのセンシング インターフェイスをネットワーク セグメントに展開します。

センシングの展開に関する考慮事項

センシングの展開に関する決定は、さまざまな要素に基づいて行います。以下の質問に答えることで、自分のネットワークの脆弱な領域を理解し、侵入検知と侵入防御のニーズを明確にすることができます。

- パッシブ インターフェイスまたはインライン インターフェイスを使用して管理対象デバイスを展開するのか。デバイスはインターフェイスの混在（一部がパッシブで、その他はインライン）をサポートするのか。詳細については、「センシング インターフェイスについて（6-2 ページ）」を参照してください。
- 管理対象デバイスをネットワークに接続する手段は何か。ハブ、タップ、スイッチ上のスパニング ポート、または仮想スイッチを使用するのか。詳細については、「ネットワークへのデバイスの接続（6-5 ページ）」を参照してください。
- ネットワーク上のすべての攻撃を検出する必要があるのか、またはファイアウォールを通過する攻撃についてのみ知りたいのか。特殊なセキュリティ ポリシーを必要とする、財務、会計、人事記録、生産コード、その他の機密性の高い保護された情報など、特定の資産がネットワーク上に存在しますか。詳細については、「展開オプション（6-7 ページ）」を参照してください。
- 管理対象デバイスの複数のセンシング インターフェイスを、ネットワーク タップからのさまざまな接続を再結合するために使用しますか、またはさまざまなネットワークからのトラフィックをキャプチャして評価するために使用しますか。複数のセンシング インターフェイスを、仮想ルータまたは仮想スイッチのどちらとして機能するように使用しますか。詳細については、「管理対象デバイスでの複数のセンシング インターフェイスの使用（6-18 ページ）」を参照してください。
- リモートの作業者が VPN またはモデムでアクセスできるようにするのか。侵入防御の展開を必要とするリモート オフィスがありますか。契約社員やその他の臨時スタッフを雇用しているか。それらのスタッフを特定のネットワーク セグメントに制限しているか。自社のネットワークを、顧客、サプライヤ、ビジネス パートナーなどの他の組織のネットワークと統合するか。詳細については、「複雑なネットワーク展開（6-20 ページ）」を参照してください。

センシング インターフェイスについて

以下の項では、さまざまなセンシング インターフェイスが Firepower システムの機能に与える影響について説明します。パッシブ インターフェイスとインライン インターフェイスに加え、ルーテッド インターフェイス、スイッチド インターフェイス、ハイブリッド インターフェイスを使用することもできます。

センシング インターフェイスはデバイスの前面にあります。センシング インターフェイスを識別するには、センシング インターフェイスの識別（3-3 ページ）を参照してください。

パッシブ インターフェイス

スイッチの SPAN、仮想スイッチ、またはミラー ポートを使用して、ネットワークで送られるトラフィックを監視するパッシブ展開を設定し、スイッチ上の他のポートからトラフィックをコピーできるようにすることができます。パッシブ インターフェイスでは、ネットワーク内のトラフィックを、そのネットワーク トラフィック フローの外部から検査できます。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブ インターフェイスは、すべてのトラフィックを無条件で受信し、受信したトラフィックを再送信しません。

インライン インターフェイス

2 つのポートを一緒にバインドすることで、インライン構成をネットワーク セグメントにトランスペアレントに設定します。インライン インターフェイスを使用すれば、隣接するネットワーク デバイスを設定することなく、任意のネットワーク コンフィギュレーションでデバイスを設置できます。インライン インターフェイスは、すべてのトラフィックを無条件に受信し、明示的にドロップされたトラフィックを除くすべての受信トラフィックを再送信します。インライン インターフェイスがインライン展開環境のトラフィックを処理するには、その前に、インライン インターフェイスのペアをインライン セットに割り当てる必要があります。

コメント　インターフェイスをインライン インターフェイスとして設定すると、そのインターフェイスの NetMod 上の隣接ポートも自動的にインライン インターフェイスとなり、インライン インターフェイスのペアが完成します。

設定可能なバイパス インライン セットを使用して、ハードウェアが完全に故障した場合（たとえば、デバイスが電力を失った場合など）にトラフィックを処理する方法を選択できます。たとえば、あるネットワーク セグメントでは接続が不可欠であり、別のネットワーク セグメントでは未検査のトラフィックを許可できないと指定することができます。設定可能なバイパス インライン セットを使用することで、次のいずれかの方法でネットワークのトラフィック フローを管理できます。

- *バイパス*：バイパスとして設定したインターフェイスのペアを使用して、デバイスで故障が発生した場合でも、すべてのトラフィックのフローを維持します。トラフィックは、デバイスをバイパスし、そのデバイスによる検査や他の処理をバイパスします。バイパスでは、検査が行われないトラフィックがネットワーク セグメント間を通過する可能性がありますが、ネットワークの接続性は保持されます。

- *非バイパス*:非バイパスに設定されているインターフェイス ペアは、デバイスに障害が発生した場合、すべてのトラフィックを停止させます。障害が発生したデバイスに到達したトラフィックは、そのデバイスに入りません。非バイパスでは、未検査のトラフィックがネットワーク セグメントを通過することを許可しませんが、デバイスに障害が発生すると、ネットワーク セグメントは接続を失います。ネットワーク セキュリティの重要性がトラフィックの損失よりも優先される展開環境では、非バイパス インターフェースを使用します。

デバイスに障害が発生しても、トラフィック フローが維持されるようにする場合は、インライン セットをバイパスとして設定します。デバイスに障害が発生した場合にトラフィックを停止するには、インライン セットを非バイパスとして設定します。再イメージ化によって、バイパス モードの Firepower デバイスが非バイパスの設定にリセットされて、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ることに注意してください。詳細については、*FirePower 8000 シリーズ スタートアップ ガイド*を参照してください。

設定可能なバイパス インターフェイスは、すべての Firepower デバイスに含めることができます。8000 シリーズデバイスには、バイパスに設定できないインターフェイスを持つ NetMods を含めることもできます。NetMods の詳細については、Firepower 8000 シリーズモジュール（2-13 ページ）を参照してください。他の拡張インターフェイス オプションには、タップ モード、リンク ステート伝搬、トランスペアレント インライン モード、ストリクト TCP モードが含まれます。インライン インターフェイス セットを設定する方法については、『*Firepower Management Center Configuration Guide*』の「Configuring Inline Sets」を参照してください。インライン インターフェイスの使用方法について詳しくは、ネットワークへのデバイスの接続（6-5 ページ）を参照してください。

Firepower Management Center を使用して ASA FirePOWER デバイスのバイパス インターフェイスを設定することはできません。インライン モードの ASA FirePOWER デバイスを設定する方法について詳しくは、ASA のドキュメントを参照してください。

スイッチド インターフェイス

レイヤ 2 展開環境の Firepower デバイスにスイッチド インターフェイスを設定することで、複数のネットワーク間でのパケット スイッチングに対応できます。また、Firepower デバイスにスタンドアロン ブロードキャスト ドメインとして機能する仮想スイッチを設定して、ネットワークを論理セグメントに分割することもできます。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判別します。

スイッチド インターフェイスには、物理構成または論理構成を使用できます。

- *物理スイッチド インターフェイス*は、スイッチングが設定された物理インターフェイスです。タグなし VLAN トラフィックを処理するには、物理スイッチド インターフェイスを使用します。
- *論理スイッチド インターフェイス*は、物理インターフェイスと VLAN タグとの間のアソシエーションです。VLAN タグが指定されたトラフィックを処理するには、論理インターフェイスを使用します。

仮想スイッチはスタンドアロン ブロードキャスト ドメインとして機能し、ネットワークを論理セグメントに分割します。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判別します。仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。その後は、タグ付きのリターン トラフィックを使用して、各ポートに接続されたネットワーク上にどのホストが存在するのかを学習していきます。

デバイスを仮想スイッチとして設定し、残りのインターフェイスを使用して、モニタ対象のネットワーク セグメントに接続できます。デバイス上で仮想スイッチを使用するには、物理スイッチド インターフェイスを作成した後、『*Firepower Management Center Configuration Guide*』の「Setting Up Virtual Switches」に記載されている手順に従ってください。

ルーテッド インターフェイス

レイヤ 3 展開の Firepower デバイスにルーテッド インターフェイスを設定し、複数のインターフェイス間でトラフィックをルーティングすることができます。各インターフェイスに IP アドレスを割り当て、これらのインターフェイスを、トラフィックをルーティングする仮想ルータに割り当てる必要があります。

ゲートウェイのバーチャル プライベート ネットワーク（ゲートウェイ VPN）または Network Address Translation（NAT）と併用するための、ルーテッド インターフェイスを設定できます。詳細については、ゲートウェイ VPN の展開（6-11 ページ）およびポリシー ベースの NAT を使用した展開（6-12 ページ）を参照してください。

また、宛先アドレスに応じてパケットの転送決定を行って、パケットをルーティングするようにシステムを設定することもできます。ルーテッド インターフェイスとして設定されたインターフェイスは、レイヤ 3 トラフィックを受信し、転送します。ルータは、転送基準に基づく発信インターフェイスからの宛先を取得します。適用するセキュリティ ポリシーは、アクセス制御ルールによって指定されます。

ルーテッド インターフェイスには、物理構成または論理構成を使用できます。

- *物理ルーテッド インターフェイス*は、ルーティングが設定された物理インターフェイスです。タグなし VLAN トラフィックを処理するには、物理ルーテッド インターフェイスを使用します。
- *論理スイッチド インターフェイス*は、物理インターフェイスと VLAN タグとの間のアソシエーションです。VLAN タグが指定されたトラフィックを処理するには、論理インターフェイスを使用します。

レイヤ 3 展開でルーテッド インターフェイスを使用するには、仮想ルータを設定し、それらの仮想ルータにルーテッド インターフェイスを割り当てる必要があります。仮想ルータは、レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループです。

デバイスを仮想ルータとして設定し、残りのインターフェイスを使用して、モニタ対象のネットワーク セグメントに接続できます。また、厳密な TCP 適用を有効にして、TCP セキュリティを最大限に強化することもできます。デバイス上で仮想ルータを使用するには、デバイスに物理ルーテッド インターフェイスを作成した後、『*Firepower Management Center Configuration Guide*』の「Setting Up Virtual Routers」に記載されている手順に従ってください。

ハイブリッド インターフェイス

Firepower デバイス上に論理ハイブリッド インターフェイスを設定することで、Firepower システムが仮想ルータと仮想スイッチの間でトラフィックをブリッジできるようになります。仮想スイッチのインターフェイスで受信した IP トラフィックの宛先が、そのスイッチに関連付けられたハイブリッド論理インターフェイスの MAC アドレスとなっている場合、システムは、そのトラフィックをレイヤ 3 トラフィックとして処理し、宛先 IP アドレスに応じてトラフィックをルーティング（またはトラフィックに応答）します。それ以外の宛先が設定されたトラフィックを受信した場合、システムはそのトラフィックをレイヤ 2 トラフィックとして処理し、適切なスイッチングを行います。

ハイブリッド インターフェイスを作成するには、まず、仮想スイッチと仮想ルータを設定し、それらの仮想スイッチと仮想ルータをハイブリッド インターフェイスに追加します。仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティングに使用できません。したがって、トラフィックを生成することも、トラフィックに応答することもしません。

ネットワーク アドレス変換（NAT）を使用するハイブリッド インターフェイスを設定すると、ネットワーク間でのトラフィックの受け渡しが可能になります。詳細については、ポリシー ベースの NAT を使用した展開（6-12 ページ）を参照してください。

デバイス上でハイブリッド インターフェイスを使用するには、デバイスにハイブリッド インターフェイスを定義した後、『*Firepower Management Center Configuration Guide*』の「Setting Up Hybrid Interfaces」に記載されている手順に従ってください。

ネットワークへのデバイスの接続

管理対象デバイスのセンシング インターフェイスは複数の方法でネットワークに接続できます。パッシブまたはインライン インターフェイスを使用してハブまたはネットワーク タップを設定するか、またはパッシブ インターフェイスを使用して Span ポートを設定します。

ハブの使用

管理対象デバイスがネットワーク セグメントのすべてのトラフィックを認識できるようにするには、イーサネット ハブが簡単な手段となります。このタイプのほとんどのハブは、セグメント上のいずれかのホストを目的とする IP トラフィックを取得し、そのトラフィックをハブに接続されているすべてのデバイスにブロードキャストします。設定したインターフェイスをハブに接続して、セグメントのすべての着信および発信トラフィックをモニタします。トラフィック量が大きいネットワークでは、パケット衝突の可能性があるため、ハブを使用しても検出エンジンがすべてのパケットを認識するとは限りません。この問題は、低トラフィックの単純なネットワークではほとんど発生しません。トラフィック量の大きいネットワークでは、ハブ以外のオプションのほうが良い結果を得られる場合があります。ハブに障害が発生した場合、またはハブが電源を失った場合は、ネットワーク接続が切断されることに注意してください。その場合、単純なネットワークでは、ネットワークがダウンします。

一部のデバイスはハブとして販売されていますが、実際にはスイッチとして機能し、各パケットをすべてのポートにブロードキャストするわけではありません。管理対象デバイスをハブに接続してもすべてのトラフィックが表示されない場合は、別のハブを購入するか、SPAN ポートを備えたスイッチを使用してください。

SPAN ポートの使用

多くのネットワーク スイッチには、1 つ以上のポートのトラフィックをミラーリングする SPAN ポートが組み込まれています。設定したインターフェイスを SPAN ポートに接続することで、すべてのポートのトラフィック（通常は着信トラフィックと発信トラフィックの両方）をまとめてモニタできます。この機能を備えたスイッチをすでにネットワーク上の適切な場所で使用している場合、管理対象デバイスのコストの他にはほとんど機器にコストをかけることなく、複数のセグメントで検出機能を展開できます。トラフィックの多いネットワークの場合、このソリューションには制限があります。SPAN ポートが 200Mbps を処理することができ、3 つのミラー対象ポートのそれぞれが 100Mbps まで処理できる場合、SPAN ポートはオーバーサブスクライブされてパケットをドロップするようになり、管理対象デバイスの効率が減少する可能性があります。

ネットワーク タップの使用

ネットワーク タップを使用すると、ネットワーク フローを中断したり、ネットワー トポロジーを変更したりすることなく、トラフィックをパッシブにモニタできます。タップはさまざまな帯域幅ですぐに使用できます。タップを使用することで、ネットワーク セグメントの着信パケットと発信パケットの両方を分析できます。通常、タップでモニタできるネットワーク セグメントは 1 つに限られるため、スイッチ上の 8 個のポートのうち、2 個のポートでトラフィックをモニタする必要がある場合には、タップは有効なソリューションになりません。その場合は、ルータとスイッチの間にタップを設置し、スイッチへの IP ストリーム全体にアクセスします。

仕様上、ネットワーク タップは着信トラフィックと発信トラフィックを 2 つの異なるケーブルで 2 つのストリームに分割します。管理対象デバイスは、通信の 2 つの部分を再結合する複数センシング インターフェイスのオプションを提供し、トラフィック ストリーム全体がデコーダ、プリプロセッサ、および検出エンジンによって評価されるようにします。

銅線インターフェイスでのインライン展開のケーブル配線

ネットワークでデバイスをインライン展開する場合、デバイスのパイパス機能を使用して、デバイスに障害が発生してもネットワーク接続を維持できるようにするには、ケーブル配線に特に注意する必要があります。

ファイバ バイパス対応インターフェイスを備えたデバイスを展開する場合は、接続がしっかり固定されていて、ケーブルがよじれていないことを確認する以外に、ケーブル配線に関する特別な懸念事項はありません。一方、ファイバ ネットワーク インターフェイスではなく銅線インターフェイスを使用したデバイスを展開する場合、デバイスのモデルによって使用するネットワーク カードが異なるため、使用するデバイス モデルに注意する必要があります。一部の 8000 シリーズ NetMods ではバイパス設定が許可されないことに注意してください。

デバイスのネットワーク インターフェイス カード（NIC）でサポートしている Auto-Medium Dependent Interface Crossover（Auto-MDI-X）と呼ばれる機能を使用すると、ネットワーク インターフェイスは、ストレート イーサネット ケーブルまたはクロス イーサネット ケーブルのどちらを使用して別のネットワーク デバイスに接続するかを自動的に設定します。Firepower デバイスは、クロスオーバー接続としてバイパスされます。

デバイスを展開することなく通常どおりにデバイスを配線します。デバイスへの電源供給が失われても、リンクは機能する必要があります。通常は、2 本のストレート ケーブルを使用して、2 つのエンドポイントにデバイスを接続します。

図 6-1　　クロス接続でバイパスする場合のケーブル配線

次の表は、ハードウェア バイパス設定で、クロス ケーブルまたはストレート ケーブルを使用するケースを示しています。展開環境では、レイヤ 2 ポートがストレート（MDI）エンドポイントとして機能し、レイヤ 3 ポートがクロス（MDIX）エンドポイントとして機能することに注意してください。バイパスが正常に機能するには、クロス（ケーブルおよびアプライアンス）の合計が奇数でなければなりません。

表 6-1　ハードウェア バイパスの有効な設定

エンドポイント 1	ケーブル	管理対象デバイス	ケーブル	エンドポイント 2
MDIX	ストレート	ストレート	ストレート	MDI
MDI	クロス	ストレート	ストレート	MDI
MDI	ストレート	ストレート	クロス	MDI
MDI	ストレート	ストレート	ストレート	MDIX
MDIX	ストレート	クロス	ストレート	MDIX
MDI	ストレート	クロス	ストレート	MDI
MDI	クロス	クロス	クロス	MDI
MDIX	クロス	クロス	ストレート	MDI

すべてのネットワーク環境が一意であり、エンドポイントの Auto-MDI-X のサポートの組み合わせが異なっていることに注意してください。デバイスが正しいケーブル配線で設置されていることを確認する最も簡単な方法は、まずデバイスの電源をオフにした上で、1 本のクロス ケーブルと 1 本のストレート ケーブルを使用してデバイスを 2 つのエンドポイントに接続することです。この 2 つのエンドポイントが通信できることを確認します。通信できない場合は、一方のケーブルのタイプが誤っています。その場合は、ケーブルの一方だけを別のタイプ（ストレート ケーブルまたはクロス ケーブル）と交換します。

インライン デバイスの電源が入っていない状態で、2 つのエンドポイントが正常に通信できるようになったら、デバイスの電源を投入します。Auto-MDI-X 機能により、2 つのエンドポイント間の通信は維持されます。インライン デバイスを交換する必要がある場合は、元のデバイスと交換デバイスのバイパス特性が異なっている場合に備え、新しいデバイスの電源が入っていない状態で、エンドポイントが通信できることを確認するプロセスを再度実行してください。

Auto-MDI-X 設定は、ネットワーク インターフェイスの自動ネゴシエーションを許可している場合にのみ、正常に機能します。[Network Interface] ページの [Auto Negotiate] オプションを無効にする必要があるネットワーク環境の場合は、インライン ネットワーク インターフェイスに適切な MDI/MDIX オプションを指定する必要があります。詳細については、『*Firepower Management Center Configuration Guide*』の「Configuring Inline Interfaces」を参照してください。

特殊なケース：Firepower 8000 シリーズデバイスの接続

Firepower 8000 シリーズの管理対象デバイスを Firepower Management Center に登録するときは、接続の両側で自動ネゴシエーションを使用するか、またはその両側を同じ固定速度に設定して、ネットワーク リンクが安定したものとなるようにする必要があります。8000 シリーズの管理対象デバイスは、半二重のネットワーク リンクをサポートしません。また、接続の反対側の速度構成やデュプレックス構成の違いもサポートしません。

展開オプション

ネットワーク セグメントに管理対象デバイスを配置すると、侵入検知システムを使用してトラフィックをモニタすることや、侵入防御システムを使用してネットワークを脅威から保護することが可能になります。

また、仮想スイッチ、仮想ルータ、またはゲートウェイ VPN として機能する管理対象デバイスを展開することもできます。さらに、ポリシーを使用してトラフィックをルーティングしたり、ネットワークでのトラフィックへのアクセスを制御したりすることもできます。

仮想スイッチを使用した展開

インライン インターフェイスをスイッチド インターフェイスとして設定することで、管理対象デバイス上に*仮想スイッチ*を作成できます。仮想スイッチは、展開環境でレイヤ 2 パケット スイッチングを行います。拡張オプションには、スタティック MAC アドレスの設定、スパニング ツリー プロトコルの有効化、厳密な TCP 適用の有効化、ドメイン レベルでのブリッジ プロトコル データ ユニット（BPDU）のドロップが含まれます。スイッチド インターフェイスの詳細については、スイッチド インターフェイス（6-3 ページ）を参照してください。

仮想スイッチがトラフィックを処理するには、仮想スイッチに複数のスイッチド インターフェイスがなければなりません。仮想スイッチごとに、システムはスイッチド インターフェイスとして設定されたポートのセットにのみトラフィックをスイッチングします。たとえば、4 つのスイッチド インターフェイスを使用して仮想スイッチを設定した場合、システムは 1 つのポートからトラフィック パケットを受信すると、それらのパケットをスイッチ上の残りの 3 つのポートにブロードキャストします。

トラフィックを許可するように仮想スイッチを設定するには、まず、物理ポートに複数のスイッチド インターフェイスを設定します。そして、仮想スイッチを追加して設定した後、その仮想スイッチを、物理ポートに設定したスイッチド インターフェイスに割り当てます。システムは、スイッチド インターフェイスが待機していない、外部物理インターフェイスで受信したすべてのトラフィックをドロップします。システムが VLAN タグなしのパケットを受信した場合、該当するポートに物理スイッチド インターフェイスが設定されていなければ、パケットはドロップされます。システムが VLAN タグ付きのパケットを受信した場合、論理スイッチド インターフェイスが設定されていなければ、同じくパケットはドロップされます。

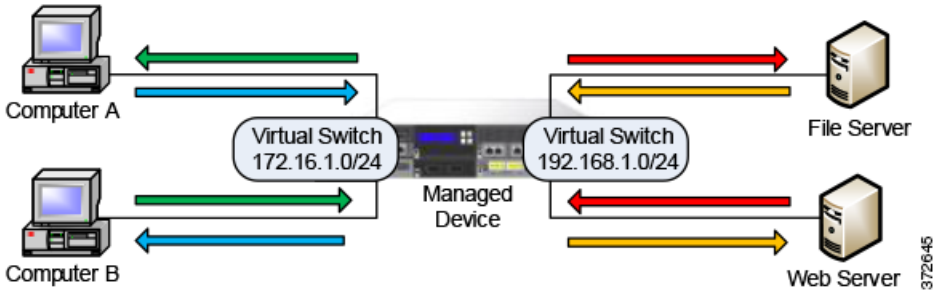
物理ポートには、必要に応じて追加の論理スイッチド インターフェイスを定義できます。ただし、論理スイッチド インターフェイスを仮想スイッチに割り当てなければ、トラフィックは処理されません。

仮想スイッチには、スケーラビリティに関する利点があります。物理スイッチを使用する場合、スイッチ上の使用可能なポートの数が制限されています。物理スイッチを仮想スイッチに置き換えると、帯域幅と展開環境に導入する複雑さのレベルのみによって制限されます。

ワークグループの接続やネットワークのセグメント化など、レイヤ 2 スイッチを使用する場合は、仮想スイッチを使用してください。レイヤ 2 スイッチは、作業者が時間の大半をローカル セグメントで費やす場合には特に有効です。大規模な展開環境（たとえば、ブロードキャスト トラフィック、VoIP、または複数のネットワークが含まれる環境）では、展開環境を複数のネットワーク セグメントに分割して、それぞれのセグメントで仮想スイッチを使用できます。

同じ管理対象デバイスに複数の仮想スイッチを展開すると、各ネットワークのニーズに応じた異なるレベルのセキュリティ レベルを維持できます。

図 6-2　　管理対象デバイス上の仮想スイッチ



この例では、管理対象デバイスが、2 つの異なるネットワーク（172.16.1.0/20 および 192.168.1.0/24）からのトラフィックをモニタしています。両方のネットワークを同じ管理対象デバイスでモニタしていますが、仮想スイッチは、同じネットワーク上にあるコンピュータまたはサーバにのみトラフィックを渡します。トラフィックは、172.16.1.0/24 仮想スイッチを介してコンピュータ A からコンピュータ B に（青色の線で示されているように）渡し、同じ仮想スイッチを介してコンピュータ B からコンピュータ A に（緑色の線で示されているように）渡すことができます。同様に、192.168.1.0/24 仮想スイッチを介してファイル サーバおよび Web サーバ間でトラフィックが受け渡されます（赤色の線とオレンジ色の線）。ただし、コンピュータと Web サーバまたはファイル サーバとの間でトラフィックを受け渡すことはできません。これらのコンピュータとサーバは、それぞれ異なる仮想スイッチ上にあるためです。

スイッチド インターフェイスおよび仮想スイッチの設定の詳細については、『*Firepower Management Center Configuration Guide*』の「*Setting Up Virtual Switches*」を参照してください。

仮想ルータを使用した展開

管理対象デバイス上に*仮想ルータ*を作成すると、複数のネットワーク間でトラフィックをルーティングすることや、プライベート ネットワークをパブリック ネットワーク（インターネットなど）に接続することが可能になります。仮想ルータは、2 つのルーテッド インターフェイスを接続し、宛先アドレスに応じて、展開環境でのレイヤ 3 パケット転送を決定します。オプションで、仮想ルータの厳密な TCP 適用を有効にすることができます。ルーテッド インターフェイスの詳細については、ルーテッド インターフェイス（6-4 ページ）を参照してください。仮想ルータは、ゲートウェイ VPN と併せて使用する必要があります。詳細については、ゲートウェイ VPN の展開（6-11 ページ）を参照してください。

仮想ルータには、同じブロードキャスト ドメイン内の 1 つ以上の個々のデバイスの物理インターフェイスまたは論理ルーテッド インターフェイス設定を含めることができます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックをルーティングするには、論理ルーテッド インターフェイスを仮想ルータに割り当てる必要があります。

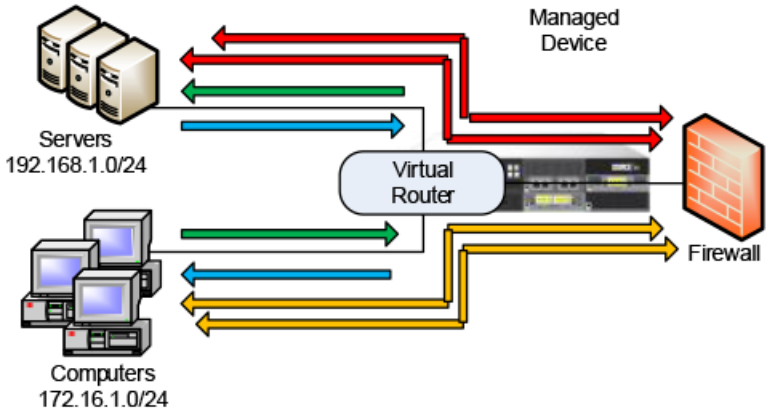
仮想ルータを設定するには、物理または論理設定のいずれかを使用したルーテッド インターフェイスを設定します。タグなし VLAN トラフィックを処理する、物理ルーテッド インターフェイスを設定できます。指定の VLAN タグ付きトラフィックを処理する、論理ルーテッド インターフェイスを作成することもできます。システムは、ルーテッド インターフェイスが待機していない、外部物理インターフェイスで受信したすべてのトラフィックをドロップします。システムが VLAN タグなしのパケットを受信した場合、該当するポートに物理ルーテッド インターフェイスが設定されていなければ、パケットはドロップされます。システムが VLAN タグ付きのパケットを受信した場合、論理ルーテッド インターフェイスが設定されていなければ、同じくパケットはドロップされます。

仮想ルータには、スケーラビリティに関する利点があります。物理ルータによって、接続可能なネットワークの数が制限される場合、同じ管理対象デバイスに複数の仮想ルータを設定できます。同じデバイスに複数のルータを配置すると、展開環境の物理的な複雑さが軽減され、1 台のデバイスから複数のルータをモニタおよび管理することが可能になります。

展開環境内の複数のネットワーク間でトラフィックを転送する場合、あるいはプライベート ネットワークをパブリック ネットワークに接続する場合は、レイヤ 3 物理ルータを使用する代わりに仮想ルータを使用してください。多数のネットワークまたはネットワーク セグメントにそれぞれ異なるセキュリティ要件が伴う大規模な展開環境では、仮想ルータが特に有効です。

管理対象デバイスに仮想ルータを展開すると、1 台のアプライアンスで複数のネットワークを相互接続することや、複数のネットワークをインターネットに接続することが可能になります。

図 6-3　　管理対象デバイスの仮想ルータ



この例では、管理対象デバイスに含まれる仮想ルータによって、ネットワーク 172.16.1.0/20 上のコンピュータ間、およびネットワーク 192.168.1.0/24 上のサーバ間でトラフィックを受け渡すことができます（青色と緑色の線）。仮想ルータの 3 番目のインターフェイスでは、各ネットワークとファイアウォールとの間でトラフィックを受け渡すことができます（赤色とオレンジ色の線）。

詳細については、『*Firepower Management Center Configuration Guide*』の「Setting Up Virtual Routers」を参照してください。

ハイブリッド インターフェイスを使用した展開

管理対象デバイス上に*ハイブリッド インターフェイス*を作成すると、仮想スイッチと仮想ルータを使用して、レイヤ 2 ネットワークとレイヤ 3 ネットワークの間でトラフィックをルーティングできます。これにより、1 つのインターフェイスで、スイッチ上のローカル トラフィックのルーティングと、外部ネットワークとの間でのトラフィックのルーティングの両方に対応できます。最適な結果を得るためには、インターフェイスにポリシー ベースの NAT を設定して、ハイブリッド インターフェイスでネットワーク アドレス変換を行えるようにしてください。ポリシー ベースの NAT を使用した展開（6-12 ページ）を参照してください。

ハイブリッド インターフェイスには、1 つ以上のスイッチド インターフェイスと 1 つ以上のルーテッド インターフェイスを含める必要があります。一般的な展開環境は、ローカル ネットワーク上でトラフィックを渡す仮想スイッチとして設定されたスイッチド インターフェイスと、プライベート ネットワークまたはパブリック ネットワークにトラフィックをルーティングする仮想ルータとして設定されたルーテッド インターフェイスの 2 つで構成されます。

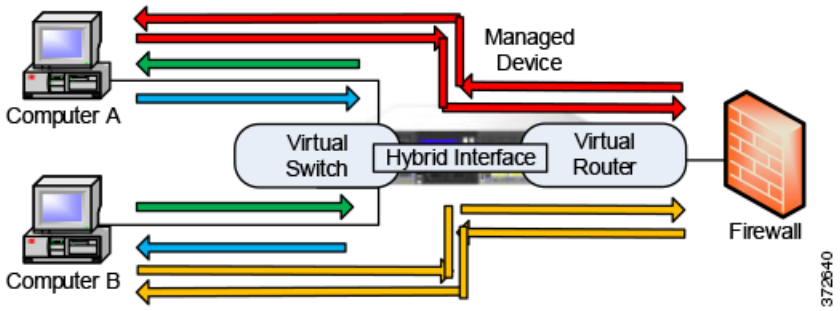
ハイブリッド インターフェイスを作成するには、まず、仮想スイッチと仮想ルータを設定し、それらの仮想スイッチと仮想ルータをハイブリッド インターフェイスに追加します。仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティングに使用できません。したがって、トラフィックを生成することも、トラフィックに応答することもしません。

ハイブリッド インターフェイスには、簡潔さとスケーラビリティに関する利点があります。レイヤ 2 とレイヤ 3 両方のトラフィック ルーティング機能が結合された単一のハイブリッド インターフェイスを使用することで、展開環境内の物理アプライアンスの数が減り、トラフィックを 1 つの管理インターフェイスで管理できます。

レイヤ 2 とレイヤ 3 の両方のルーティング機能が必要な場合は、ハイブリッド インターフェイスを使用してください。この展開は、スペースやリソースが限られた小規模な展開環境の小さなセグメントに最適です。

ハイブリッド インターフェイスを展開すると、トラフィックをローカル ネットワークから外部またはパブリック ネットワーク（インターネットなど）に渡すことができると共に、ハイブリッド インターフェイスでの仮想スイッチと仮想ルータに関する個別のセキュリティ上の考慮事項に対応することができます。

図 6-4　　管理対象デバイス上のハイブリッド インターフェイス



この例では、コンピュータ A とコンピュータ B が同じネットワーク上にあり、管理対象デバイス上に設定されたレイヤ 2 仮想スイッチを使用して通信しています（青色と緑色の線）。管理対象デバイス上に設定された仮想ルータは、ファイアウォールへのレイヤ 3 アクセスを提供します。ハイブリッド インターフェイスには仮想スイッチと仮想ルータのレイヤ 2 およびレイヤ 3 機能が統合されているため、各コンピュータからのトラフィックをハイブリッド インターフェイスを介してファイアウォールに渡すことができます（赤色とオレンジ色の線）。

詳細については、『*Firepower Management Center Configuration Guide*』の「Setting Up Hybrid Interfaces」を参照してください。

ゲートウェイ VPN の展開

ライセンス：VPN

ローカル ゲートウェイとリモート ゲートウェイの間のセキュア トンネルを確立するには、*ゲートウェイ バーチャル プライベート ネットワーク*（ゲートウェイ VPN）接続を作成します。ゲートウェイ間のセキュア トンネルにより、ゲートウェイの間での通信が保護されます。

Cisco 管理対象デバイスの仮想ルータからリモート デバイスや他のサードパーティ VPN エンドポイントへのセキュア VPN トンネルを作成するには、インターネット プロトコル セキュリティ（IPSec）プロトコル スイートを使用して Firepower システムを設定します。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストは、セキュア VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続できるようになります。VPN エンドポイントは、Internet Key Exchange（IKE）バージョン 1 またはバージョン 2 のプロトコルを使用して相互認証することで、トンネルのセキュリティ アソシエーションを確立します。システムは、IPsec 認証ヘッダー（AH）モードまたは IPsec Encapsulating Security Payload（ESP）モードのいずれかで稼動します。AH と ESP は両方とも認証を提供します。ESP は、さらに暗号化も提供します。

ゲートウェイ VPN は、ポイントツーポイント展開、スター型展開、またはメッシュ型展開で使用できます。

- ポイントツーポイント展開では、2 つのエンドポイントを直接 1 対 1 の関係で相互接続します。両方のエンドポイントがピア デバイスとして設定され、いずれのデバイスもセキュア接続を開始できます。少なくともどちらかのデバイスが、VPN 対応の管理対象デバイスである必要があります。

  リモートに位置するホストがパブリック ネットワークを使用してネットワーク内のホストに接続する場合は、ポイントツーポイント展開を使用してネットワークのセキュリティを確保してください。

- スター型展開では、ハブと複数のリモート エンドポイント（リーフ ノード）間のセキュア接続を確立します。ハブ ノードと個々のリーフ ノードとの間の接続が、それぞれ別個の VPN トンネルとなります。通常、ハブ ノードとなるのは、本社に配置される VPN 対応の管理対象デバイスです。リーフ ノードは支社に配置します。トラフィックの大部分は、これらのリーフ ノードから開始されます。

  インターネットまたは他のサードパーティ ネットワークでセキュア接続を使用して組織の本社と各支社を接続するには、スター型展開を使用して、従業員全員が、組織のネットワークに管理された形でアクセスするようにしてください。

- メッシュ型展開では、VPN トンネルを使用してすべてのエンドポイントを同時に接続します。これにより、あるエンドポイントで障害が発生しても、残りのエンドポイントの相互通信は維持されるという冗長性が提供されます。

  1 つ以上の VPN トンネルで障害が発生しても、トラフィック フローが維持されるようにするには、メッシュ型展開を使用して、分散された場所に位置する一連の支社を接続してください、冗長性のレベルは、この設定で展開する VPN 対応の管理対象デバイスの数によって決まります。

ゲートウェイ VPN の設定の詳細については、『*Firepower Management Center Configuration Guide*』の「Gateway VPN」を参照してください。

ポリシー ベースの NAT を使用した展開

ポリシー ベースのネットワーク アドレス変換（NAT）を使用してポリシーを定義し、NAT の実行方法を指定できます。ポリシーのターゲットは、単一のインターフェイス、1 つ以上のデバイス、またはネットワーク全体に設定できます。

静的（1 対 1）変換または動的（1 対多）変換を設定できます。動的変換は順序に依存することに注意してください、つまり、最初に一致するルールが適用されるまで、ルールが順に検索されます。

一般に、ポリシー ベースの NAT は以下の展開で機能します。

- プライベート ネットワーク アドレスを非公開にする展開。

  プライベート ネットワークからパブリック ネットワークにアクセスする際に、NAT がプライベート ネットワーク アドレスをパブリック ネットワーク アドレスに変換します。特定のプライベート ネットワーク アドレスは、パブリック ネットワークから隠されます。

- プライベート ネットワーク サービスへのアクセスを許可する展開。

  パブリック ネットワークがプライベート ネットワークにアクセスする際に、NAT がパブリック アドレスをプライベート ネットワーク アドレスに変換します。これにより、パブリック ネットワークは、特定のプライベート ネットワーク アドレスにアクセスできます。

- 複数のプライベート ネットワーク間でトラフィックをリダイレクトする展開。

  プライベート ネットワーク上のサーバが接続先のプライベート ネットワーク上のサーバにアクセスする際に、プライベート アドレスの重複がなく、これらのプライベート ネットワーク間でのトラフィック フローが可能になるように、NAT が 2 つのプライベート ネットワーク間でプライベート アドレスを変換します。

ポリシー ベースの NAT を使用すると、ハードウェアを追加する必要がなくなり、侵入検知または防御システムの設定と NAT が 1 つのユーザ インターフェイスに統合されます。詳細については、『*Firepower Management Center Configuration Guide*』の「Using NAT Policies」を参照してください。

アクセス制御による展開

アクセス制御は、ネットワークへの出入りあるいはネットワーク内での移動を許可するトラフィックを指定、検査、および記録するために使用できる、ポリシー ベースの機能です。ここでは、アクセス制御が展開でどのように機能するのかを説明します。この機能の詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

アクセス制御ポリシーは、ネットワーク上のトラフィックをシステムがどのように処理するかを決定します。ポリシーにアクセス制御ルールを追加することで、ネットワーク トラフィックの処理方法やロギング方法をよりきめ細かく制御できます。

アクセス制御ルールが含まれないアクセス制御ポリシーは、以下のいずれかのデフォルト アクションを使用してトラフィックを処理します。

- すべてのトラフィックをブロックして、ネットワークに入れない
- すべてのトラフィックを信頼してネットワークに入ることを許可し、検査は行わない
- すべてのトラフィックがネットワークに入ることを許可し、ネットワーク ディスカバリ ポリシーのみを使用してトラフィックを検査する
- すべてのトラフィックがネットワークに入ることを許可し、侵入ポリシーとネットワーク ディスカバリ ポリシーを使用してトラフィックを検査する

アクセス制御ルールはさらに、ターゲット デバイスでのトラフィックの処理方法を定義します。その方法には、単純な IP アドレスのマッチングから、異なる複数のユーザ、アプリケーション、ポート、URL が関与する複雑なシナリオまでがあります。それぞれのルールについて、ユーザはルールのアクション、つまり侵入またはファイル ポリシーと一致するトラフィックを信頼、監視、ブロック、または検査するかどうかを指定します。

アクセス制御では、セキュリティ インテリジェンスのデータに基づいてトラフィックをフィルタリングできます。セキュリティ インテリジェンスとは、アクセス制御ポリシーごとに、送信元 IP アドレスまたは宛先 IP アドレスに基づいて、ネットワークを移動できるトラフィックを指定するための機能です。この機能では、許可されない IP アドレスのブラックリストを作成できます。ブラックリストに含まれる IP アドレスからのトラフィックはブロックされ、検査されません。

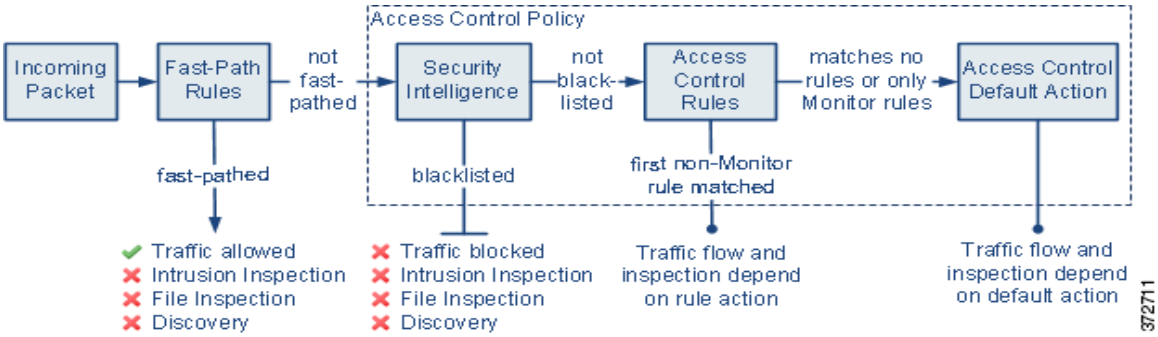
展開の例に、共通のネットワーク セグメントが示されています。各場所に展開された管理対象デバイスは、それぞれに異なる目的を果たします。ここでは、配置場所に関する一般的な推奨事項を説明します。

- ファイアウォールの内側（6-14 ページ）では、ファイアウォールを通過するトラフィックに対してアクセス制御がどのように機能するかを説明しています。
- DMZ（6-15 ページ）では、DMZ 内のアクセス制御がネットワーク外部と接触するサーバを保護する仕組みについて説明しています。
- 内部ネットワーク（6-16 ページ）では、アクセス制御が内部ネットワークを侵入や不測の攻撃から保護する仕組みについて説明しています。
- コア ネットワーク（6-16 ページ）では、厳密なルールを使用したアクセス制御ポリシーで重要な資産を保護する方法を説明しています。
- リモート ネットワークまたはモバイル ネットワーク（6-17 ページ）では、アクセス制御ポリシーでトラフィックをモニタし、リモートの場所やモバイル デバイスでのトラフィックからネットワークを保護する方法を説明しています。

ファイアウォールの内側

ファイアウォールの内側に配置された管理対象デバイスは、ファイアウォールによって許可された着信トラフィック、あるいは誤った設定が原因でファイアウォールを通過したトラフィックをモニタします。共通のネットワーク セグメントには、DMZ、内部ネットワーク、コア ネットワーク、モバイル アクセス ネットワーク、リモート ネットワークがあります。

以下の図に、Firepower システムを介したトラフィック フローと、トラフィックに対して行われるタイプのインスペクションの詳細を示します。高速パスで処理されたトラフィックやブラックリストに登録されたトラフィックに対しては、インスペクションが行われないことに注意してください。アクセス制御ルールまたはデフォルト アクションで処理されたトラフィックの場合、そのフローとインスペクションは、ルール アクションによって異なります。簡潔にするために、この図にはルール アクションを示していませんが、信頼されたトラフィックまたはブロックされたトラフィックに対しては、インスペクションは一切行われません。また、ファイル インスペクションは、デフォルト アクションでサポートされていません。



着信パケットは、最初に高速パス ルールについてチェックされます。一致が見つかった場合、トラフィックは高速パスで処理されます。一致しない場合、セキュリティ インテリジェンス ベースのフィルタリングにより、パケットがブラックリストに登録されているかどうかが判別されます。登録されていない場合、アクセス制御ルールが適用されます。パケットがルールの条件を満たす場合、そのトラフィック フローとインスペクションは、ルール アクションによって異なります。パケットに一致するルールがない場合、そのトラフィック フローとインスペクションは、デフォルトのポリシー アクションによって異なります。(モニタ ルールの場合は例外です。この場合は、トラフィックが引き続き評価されます)。各アクセス コントロール ポリシーのデフォルト アクションは、高速パス処理またはブラックリスト登録が行われなかったトラフィック、あるいはモニタ ルール以外のルールと一致したトラフィックを管理します。高速パスが使用できるのは、8000 シリーズデバイスのみです。

アクセス制御ルールを作成することで、ネットワーク トラフィックの処理方法やロギング方法をよりきめ細かく制御できます。ルールごとに、特定の基準を満たすトラフィックに適用するアクション(信頼、モニタ、ブロック、またはインスペクション)を指定します。

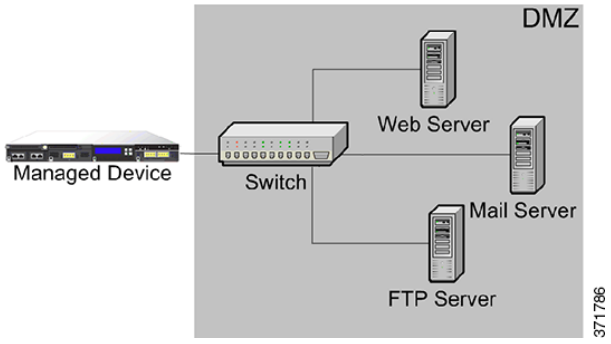
DMZ

DMZ 内には、ネットワーク外部と接触するサーバ(Web、FTP、DNS、メールなど)があり、DMZ が内部ネットワークでメール中継や Web プロキシなどのサービスをユーザに提供する場合もあります。

DMZ に保管されるコンテンツは静的であり、変更の計画および実行は、明確なコミュニケーションと事前予告によって行われます。このセグメント内での攻撃は、一般に着信トラフィックによって行われますが、DMZ 内のサーバーでは計画された変更しか行われないことから、すぐに明らかになります。このセグメントに効果的なアクセス制御ポリシーは、サービスに対するアクセスを厳密に制御し、あらゆる新規ネットワーク イベントを検索するポリシーです。

DMZ 内のサーバには、DMZ がネットワークを介して問い合わせできるデータベースを含めることができます。DMZ と同じく、データベースに対しても予定外の変更は行われないはずですが、データベースのコンテンツはより機密性が高いため、Web サイトや他の DMZ サービスより保護を強化する必要があります。DMZ のアクセス制御ポリシーに加え、強力な侵入防御ポリシーを使用することが、効果的な戦略となります。

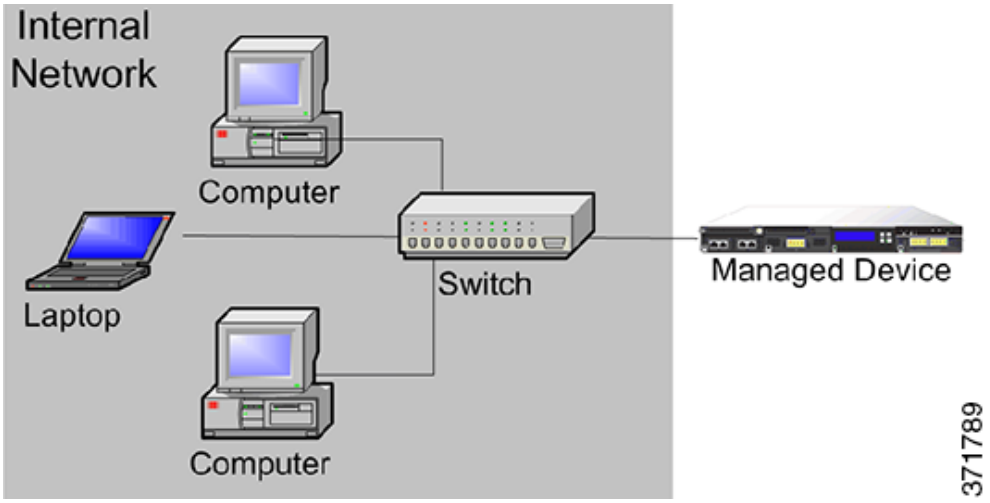
このセグメントに展開された管理対象デバイスでは、DMZ 内のセキュリティが侵害されたサーバから開始されてインターネットに送信された攻撃を検出できます。ネットワーク ディスカバリを使用してネットワーク トラフィックをモニタすることで、DMZ 内のサーバのセキュリティ侵害の兆候として、これらの公開されたサーバの変更(たとえば、予期しないサービスが突然出現したことなど)をモニタすることができます。



内部ネットワーク

不正な攻撃が、内部ネットワーク上のコンピュータから開始される可能性もあります。これらの攻撃は、作為的であることも（たとえば、不明なコンピュータがネットワーク上に突然現れるなど）、予想外の感染であることもあります（たとえば、オフサイトで感染した職場のラップトップがネットワークに接続されて、ウイルスが拡散するなど）。内部ネットワークでのリスクは、発信トラフィックで生じる場合もあります（たとえば、コンピュータが疑わしい外部 IP アドレスに情報を送信するなど）。

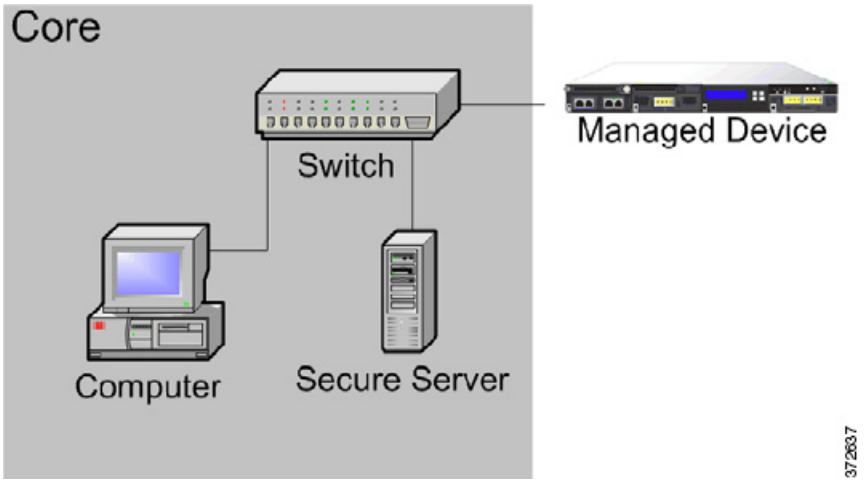
この動的なネットワークには、発信トラフィックに加え、すべての内部トラフィックに対して厳密なアクセス制御ポリシーが必要になります。ユーザとアプリケーションの間のトラフィックを厳密に制御するアクセス制御ルールを追加してください。



コア ネットワーク

コア資産とは、ビジネスの成功に不可欠な資産であり、いかなる代償を払っても保護しなければなりません。コア資産はビジネスの特性によって異なりますが、一般的なコア資産としては、財務管理センターや知的財産のリポジトリが挙げられます。コア資産のセキュリティが侵害されると、ビジネスが壊滅的損害を被る恐れがあります。

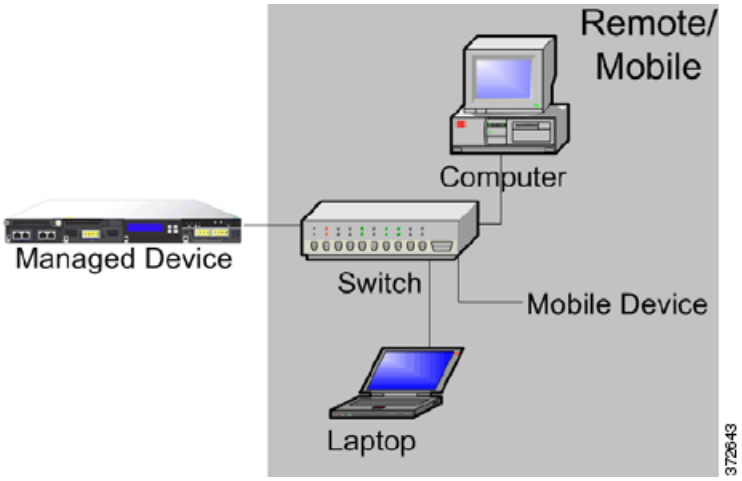
ビジネスが機能するためには、このセグメントをすぐに利用できるようにする必要がありますが、それと同時に厳重に制限および制御しなければなりません。アクセス制御によって、リスクの高いネットワーク セグメント（リモート ネットワークやモバイル デバイスなど）からはコア資産にアクセスできないようにする必要があります。このセグメントには常に、ユーザとアプリケーションによるアクセスに対する厳密なルールを含む、最も積極的なアクセス制御ルールを適用してください。



リモート ネットワークまたはモバイル ネットワーク

オフサイトに位置するリモート ネットワークでは、多くの場合、仮想プライベート ネットワーク（VPN）を使用してプライマリ ネットワークへのアクセスを提供します。モバイル デバイスやパーソナル デバイスをビジネスで使用することが次第に一般的になってきています（たとえば、「スマートフォン」を使用して会社の電子メールにアクセスするなど）。

これらのネットワークは、急速かつ継続的に変化する、極めて動的な環境です。専用のモバイル ネットワークまたはリモート ネットワークに管理対象デバイスを展開すると、不明な外部ソースとの間で送受信されるトラフィックをモニタおよび管理する、厳密なアクセス制御ポリシーを作成できます。コア リソースに対するユーザ、ネットワーク、アプリケーションのアクセスをポリシーによって厳しく制限することで、リスクを軽減できます。



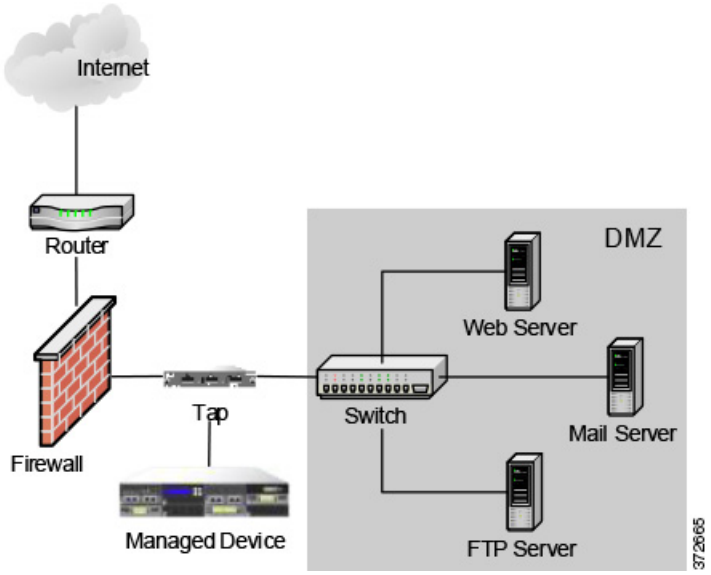
管理対象デバイスでの複数のセンシング インターフェイスの使用

管理対象デバイスのネットワーク モジュールには、複数のセンシング インターフェイスが用意されています。以下の目的で、管理対象デバイスにおいて複数のセンシング インターフェイスを使用できます。

- ネットワーク タップからの個別の接続を再結合する
- 複数の異なるネットワークからトラフィックを捕捉して評価する
- 仮想ルータとして機能させる
- 仮想スイッチとして機能させる

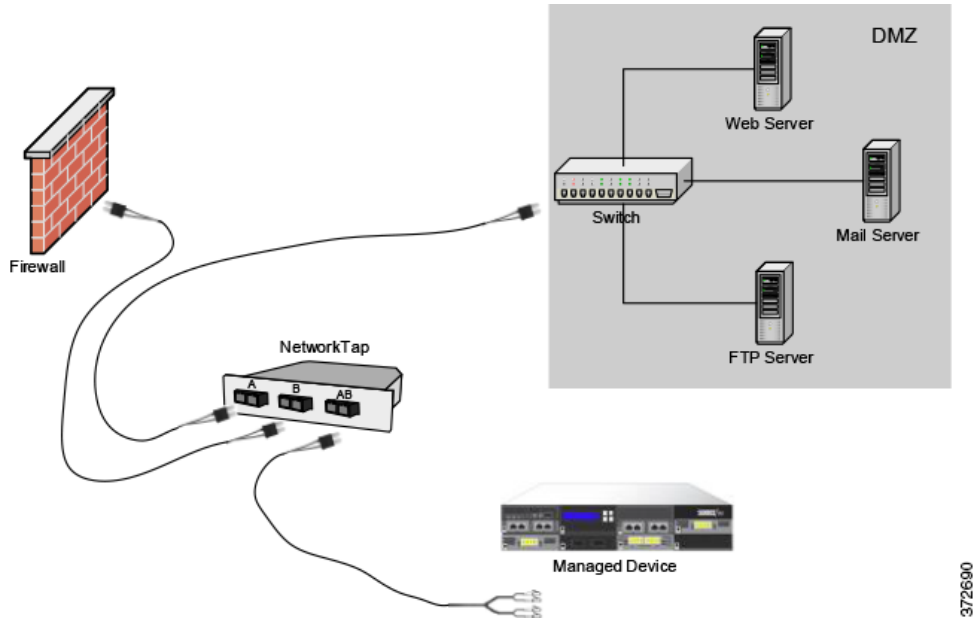
コメント　各センシング インターフェイスは、デバイスの評価対象となる完全なスループットを受信できますが、管理対象デバイスでの合計トラフィックが帯域幅の評価を超えるとパケットの消失が発生します。

ネットワーク タップのある管理対象デバイス上に複数のセンシング インターフェイスを展開することは、簡単なプロセスです。以下の図に、トラフィック量の多いネットワーク セグメントに設置されたネットワーク タップを示します。

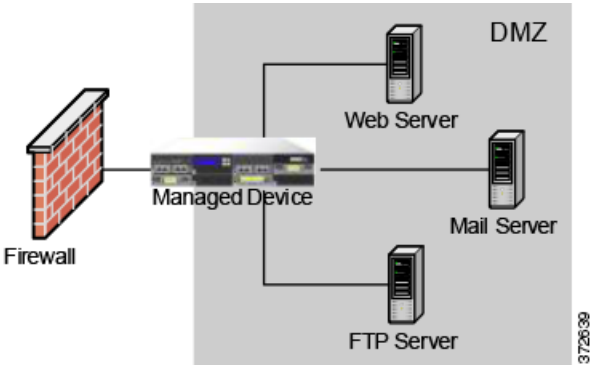


このシナリオでは、タップが別個のセンシング インターフェイスを介して着信および発信トラフィックを伝送します。管理対象デバイス上で複数のセンシング インターフェイス アダプタ カードをタップに接続すると、管理対象デバイスはトラフィックを単一のデータ ストリームに組み合わせます。これにより、トラフィックが分析可能になります。

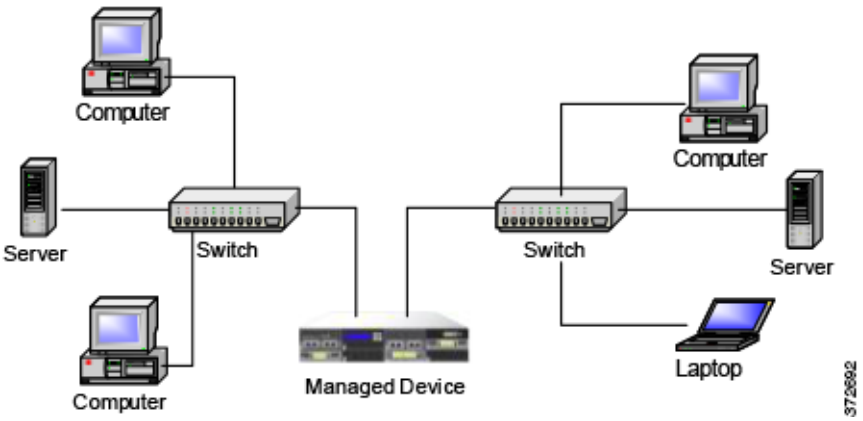
以下の図に示すようなギガビット光タップでは、管理対象デバイス上にある 2 組のセンシング インターフェイスは、どちらもタップのコネクタによって使用されることに注意してください。



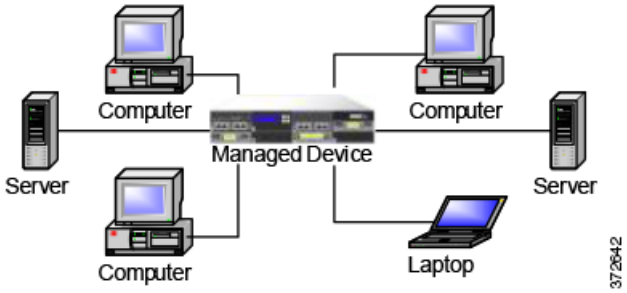
展開環境のタップとスイッチの両方を、仮想スイッチで置き換えることができます。タップを仮想スイッチに置き換えると、タップ パケット配信が保証されなくなることに注意してください。



個別のネットワークからデータを捕捉するインターフェイスを作成することもできます。次の図は、デュアル センシング インターフェイスのアダプタがある単一のデバイスと、2 つのネットワークに接続された 2 つのインターフェイスを示しています。



1 台のデバイスで両方のネットワーク セグメントをモニタできるだけでなく、デバイスの仮想スイッチ機能を使用して、展開環境内の両方のスイッチを置き換えることもできます。



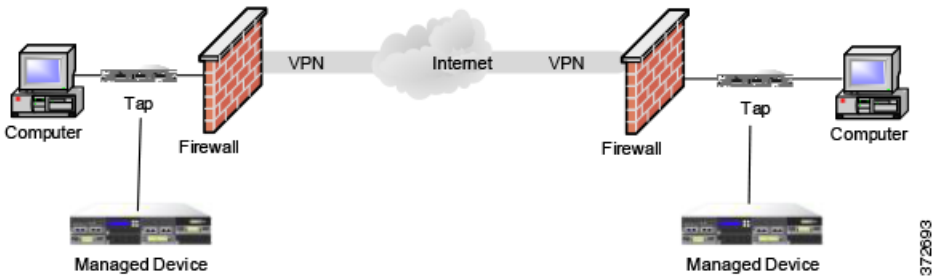
複雑なネットワーク展開

企業のネットワークには、例えば VPN を使用したリモート アクセスが必要になったり、ビジネス パートナーやバンキング接続などの複数のエントリ ポイントを使用したりする場合があります。

VPN の統合

バーチャル プライベート ネットワーク（VPN）では、IP トンネリング手法を使用して、インターネットを介したローカル ネットワークとリモート ユーザ間のセキュリティを提供します。一般に、VPN ソリューションでは IP パケットのデータ ペイロードを暗号化します。他のパケットと同様に、パブリック ネットワークでパケットを送信できるようにするために、IP ヘッダーは暗号化されません。パケットが宛先ネットワークに到達すると、ペイロードが暗号解除されて、パケットが適切なホストに送信されます。

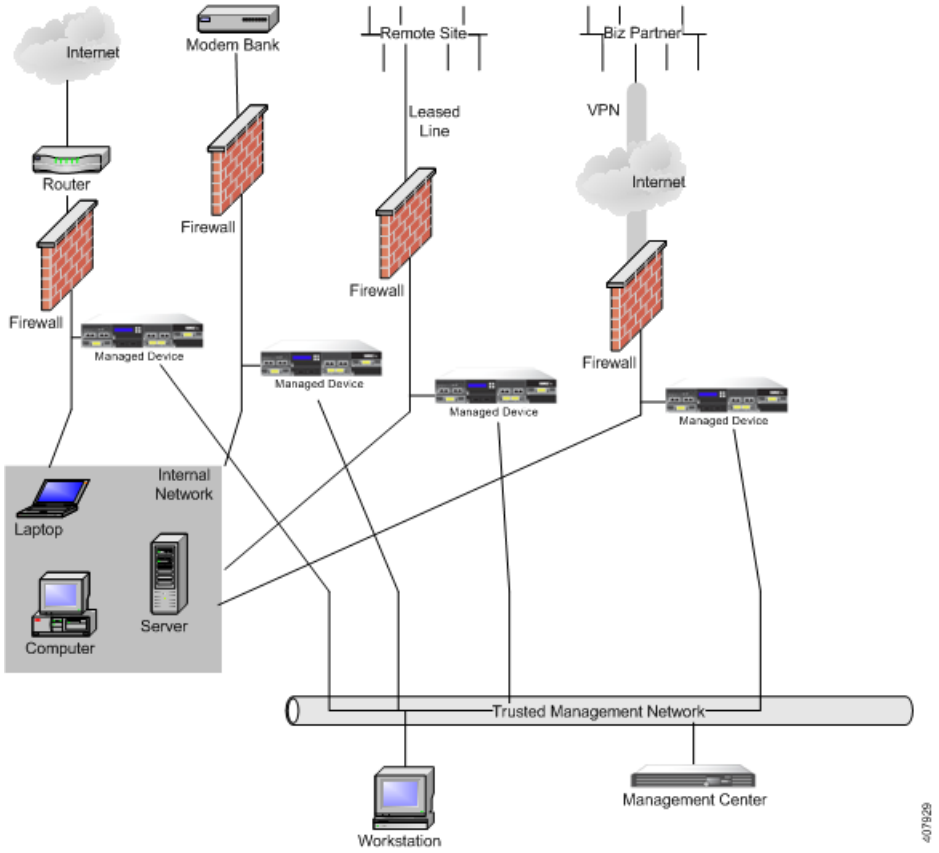
ネットワーク アプライアンスでは VPN パケットの暗号化されたペイロードを分析できないため、すべてのパケット情報にアクセスできるように、管理対象デバイスは VPN 接続の終端エンドポイント外部に配置します。以下の図に、管理対象デバイスを VPN に展開する方法を示します。



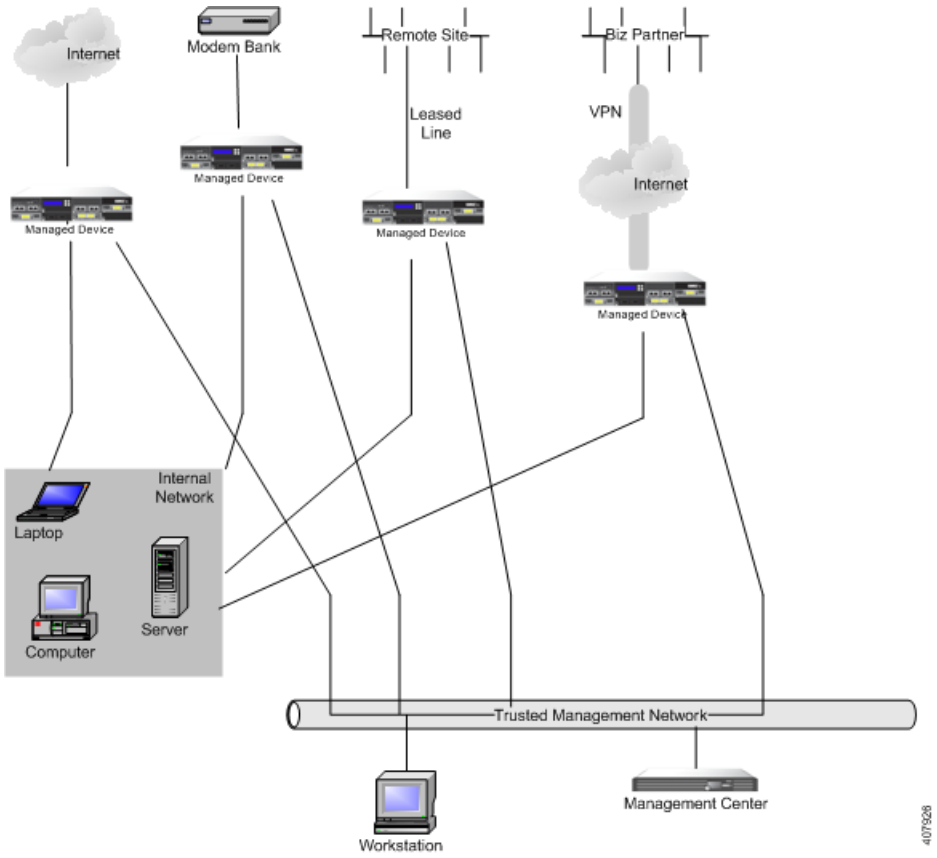
VPN 接続の一方の終端で、ファイアウォールまたはタップを管理対象デバイスに置き換えることができます。タップを管理対象デバイスに置き換えると、タップ パケット配信が保証されなくなることに注意してください。

他のエントリ ポイントでの侵入検知

多くのネットワークには、複数のアクセス ポイントが含まれます。単一の境界ルータでインターネットに接続する代わりに、一部の企業では、インターネット、モデム バンク、およびビジネス パートナー ネットワークへの直接リンクを組み合わせて使用しています。通常、管理対象デバイスを展開する場所は、ファイアウォールの近く（ファイアウォール内部または外部、あるいはその両方）の、ビジネス データの整合性および機密性にとって重要なネットワーク セグメント上でなければなりません。以下の図に、複数のエントリ ポイントがある複雑なネットワーク上の重要な場所に管理対象デバイスを設置する方法を示します。

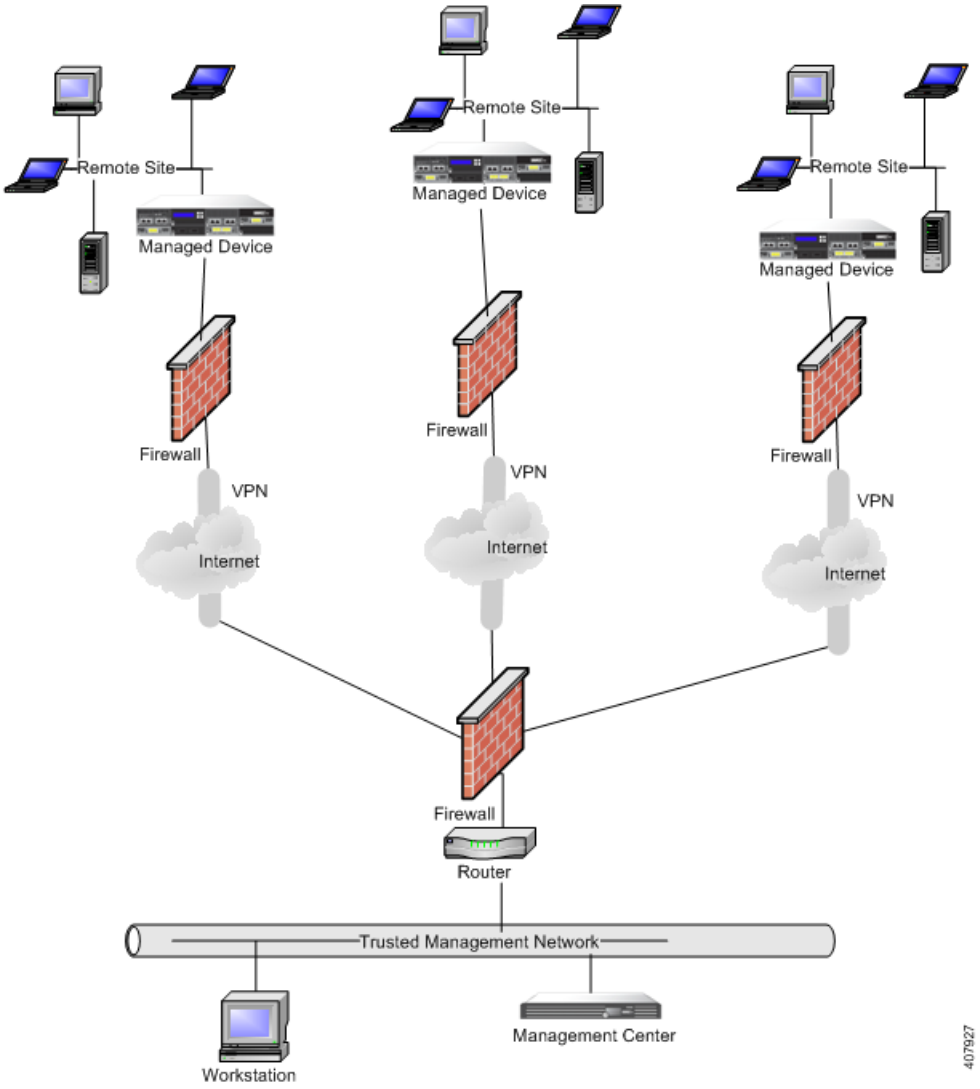


ファイアウォールとルータは、そのネットワーク セグメント上に展開された管理対象デバイスに置き換えることができます。

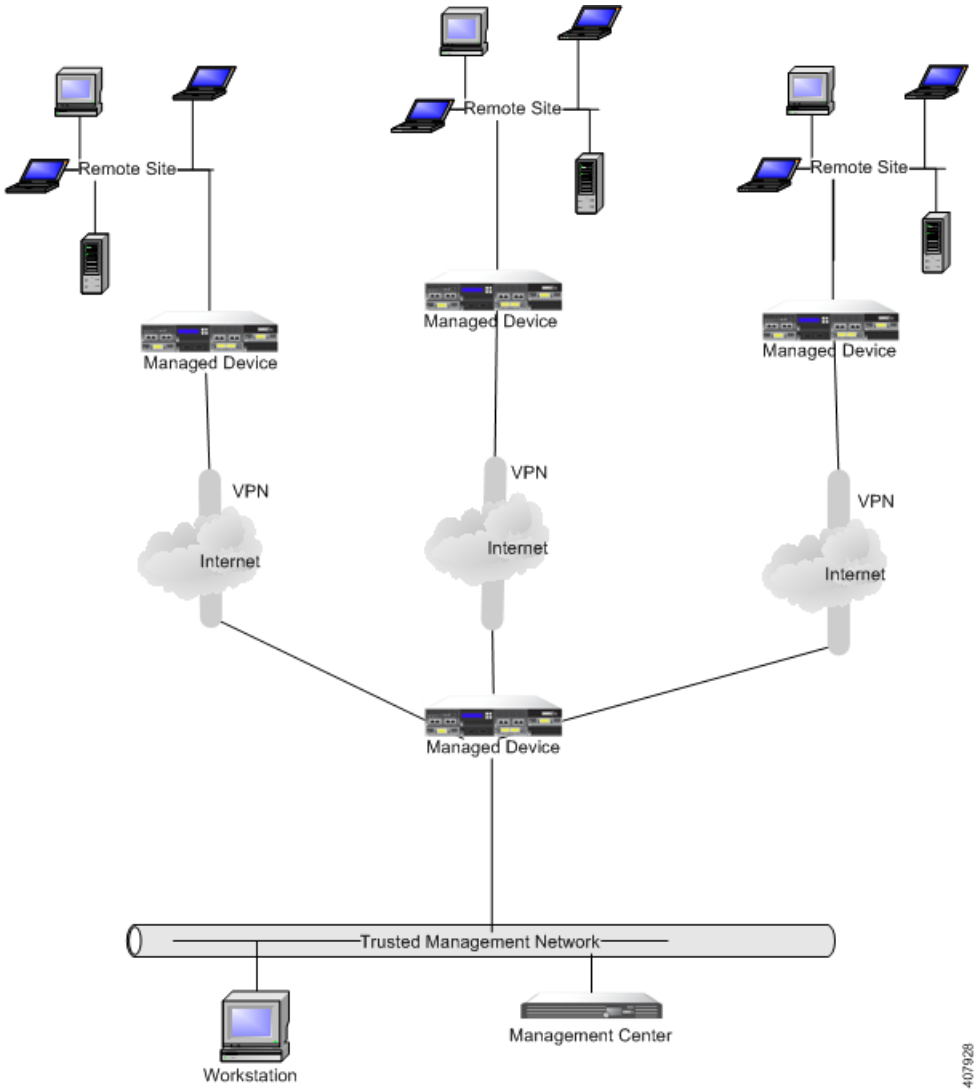


マルチサイト環境での展開

多くの組織では、地理的に分散している企業全体で侵入検知を展開し、1 か所からすべてのデータを分析することを望んでいます。この形態をサポートするために、Firepower システムで提供している Firepower Management Center は、組織のさまざまな場所に展開されている管理対象デバイスからのイベントを集約して相互に関連付けます。同じ地理的な場所で同じネットワークに複数の管理対象デバイスと Firepower Management Center を展開する場合とは異なり、分散した地理的な場所に管理対象デバイスを展開する場合には、管理対象デバイスおよびデータ ストリームのセキュリティが確保されるように注意しなければなりません。データを保護するには、管理対象デバイスと Firepower Management Center を、保護されていないネットワークから隔離する必要があります。これは、VPN を介した管理対象デバイスからのデータ ストリームを送信することによって、または次の図のように他のセキュアなトンネリング プロトコルによって実行できます。



ファイアウォールとルータは、各ネットワーク セグメントに展開された管理対象デバイスに置き換えることができます。



複雑なネットワーク内にある複数の管理インターフェイスの統合

任意の展開内の複数の管理インターフェイスを設定して、さまざまなネットワークを監視しており、同じ Firepower Management Center によって管理されるデバイスからトラフィックを分離できます。複数の管理インターフェイスを使用して、固有の IP アドレス（IPv4 または IPv6）を持つ管理インターフェイスを Firepower Management Center に追加し、その管理インターフェイスから管理対象のデバイスを含むネットワークへのルートを作成できます。新しい管理インターフェイスにデバイスを登録すると、そのデバイスのトラフィックは、Firepower Management Center のデフォルト管理インターフェイスに登録されたデバイスのトラフィックから分離されます。

ヒント　デバイスを、デフォルト（eth0）の管理インターフェイス以外の管理インターフェイスの静的 IP アドレスに登録する必要があります。DHCP は、デフォルトの管理インターフェイスだけでサポートされています。

トラフィック チャネルのために別個の管理インターフェイスを使用する場合を除いて、複数の管理インターフェイスが NAT 環境でサポートされます。詳細については、「管理ネットワークでの展開（5-1 ページ）」を参照してください。Lights-Out Management は、追加の管理インターフェイスではなく、デフォルトの管理インターフェイスでのみサポートされることに注意してください。

Firepower Management Center をインストールした後に、Web インターフェイスを使用して、複数の管理インターフェイスを設定します。詳細については、『*Firepower Management Center Configuration Guide*』の「Configuring Appliance Settings」を参照してください。

複雑なネットワーク内での管理対象デバイスの統合

単純な複数セクタからなるネットワークよりも複雑なネットワーク トポロジに管理対象デバイスを展開できます。ここでは、プロキシ サーバ、NAT デバイス、および VPN が存在する環境に管理対象デバイスを展開する場合に、ネットワーク ディスカバリおよび脆弱性の分析に伴う問題に加え、Firepower Management Center を使用して複数の管理対象デバイスを管理する方法、およびマルチサイト環境での管理対象デバイスの展開と管理について説明します。

プロキシ サーバと NAT の統合

ネットワーク アドレス変換（NAT）デバイスまたはソフトウェアをファイアウォールの境界に導入することで、内部ホストの IP アドレスを効果的にファイアウォールの背後に隠すことができます。管理対象デバイスがこれらのデバイスまたはソフトウェアとモニタ対象のホストの間に位置していると、システムがプロキシまたは NAT デバイスの背後にあるデバイスを正しく識別できない可能性があります。この場合、Cisco では、ホストが正しく検出されるように、管理対象デバイスをプロキシまたは NAT で保護されたネットワーク セグメントの内部に配置することを推奨しています。

ロード バランシング方式の統合

一部のネットワーク環境では、「サーバ ファーム」構成を使用して、Web ホスティング、FTP ストレージ サイトといったサービスに対するネットワーク ロード バランシングを実行します。ロード バランシング環境では、それぞれに固有のオペレーティング システムを使用した複数のホストの間で IP アドレスが共有されます。この場合、システムはオペレーティング システムの変更を検出しても、信頼度の高い静的オペレーティング システム ID を提供できません。影響を受けるホストで使用している異なる種類のオペレーティング システムの数によっては、システムが大量のオペレーティング システム変更イベントを生成したり、信頼度の低い静的オペレーティング システム ID を提示したりすることがあります。

検出に関するその他の考慮事項

識別対象のホストの TCP/IP スタックが変更されている場合、システムはホスト オペレーティング システムを正確に識別できない可能性があります。TCP/IP スタックの変更は、パフォーマンスを向上するために行われる場合があります。たとえば、Internet Information Services（IIS）Web サーバを実行する Windows ホストの管理者には、パフォーマンスを向上させる方法として、大量のデータを受信できるように TCP ウィンドウ サイズを大きくすることが推奨されています。また、実際のオペレーティング システムを曖昧にして正確な識別を不可能にし、攻撃の対象にならないようにするために TCP/IP スタックが変更されることもあります。TCP/IP スタックの変更によって対処する同様のシナリオには、攻撃者がネットワークの予備調査スキャンを実行して、特定のオペレーティイング システムを使用するホストを識別した後、それらのホストを対象に、そのオペレーティング システムに固有の攻撃を仕掛けるというシナリオもあります。

Firepower 8000 シリーズデバイスの電源要件

警告と注意

このマニュアルには警告と注意の両方が含まれています。警告は、安全性に関連するものです。警告に従わないと、けがや機器の損傷を引き起こす可能性があります。注意は、正常に機能するための要件です。注意に従わないと、操作が正しく行われない結果となることがあります。

注意 機器またはサブアセンブリの屋内ポートは、建物内配線や露出配線、またはケーブル配線のみの接続に適しています。機器またはサブアセンブリの屋内ポートは、局外設備（OSP）あるいはその配線に接続されるインターフェイスに金属で接続**してはなりません**。これらのインターフェイスは、屋内インターフェイス専用（GR-1089-CORE Issue 4 に記載されたタイプ 2 ポートまたはタイプ 4 ポート）に設計されており、屋外用の OSP ケーブルと区別する必要があります。これらのインターフェイスを金属で OSP 配線と接続する場合、プライマリ プロテクタを追加するだけでは、十分に保護されません。

静電気対策

注意 アプライアンスの開梱、設置、移動の前に、静電気放電対策手順（接地リスト ストラップや静電気防止用の作業台の使用など）を実施してください。過剰な静電気放電は、アプライアンスを損傷し、意図しない操作が行われる可能性があります。

Firepower 81xx ファミリアプライアンス

ここでは、次の所要電力について説明します。

- Firepower 8120、8130、および 8140（CHAS-1U-AC、CHAS-1U-DC、または CHAS-1U-AC/DC）

これらのアプライアンスは、National Electric Code が適用される場所やネットワーク通信施設で、認定を受けた担当者により設置されるものです。

シスコでは、返品に備えて梱包材を保管しておくことを推奨します。

詳細については、次の項を参照してください。

- 回路の配置、電圧、電流、周波数範囲、および電源コードの詳細については AC 電源の設置（A-2 ページ）を参照してください。

- 回路の配置、電圧、電流、接地基準、端子、ブレーカーの要件、および最小ワイヤ サイズについては、DC 電源の設置（A-3 ページ）を参照してください。
- ボンディング位置、推奨される端子、アース線の要件、および DC 電源については接地要件（A-5 ページ）を参照してください。

AC 電源の設置

Firepower システムは、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

注意　AC 電源に DC 電源を接続**しないでください**。

冗長電源を作成するためには個別の回路が必要です。入力線での電力グリッチによる電源状態の問題や電力損失を防ぐため、無停電電源またはバッテリ バックアップの電源を使用します。

アプライアンス全体を稼働できる十分な電力を各電源に供給します。各電源の定格電圧と定格電流は、アプライアンスのラベルに記載されています。

Firepower システムを装着するネットワーク機器の入力部に外部電力サージ保護装置を使用します。

専用回路の設置

専用回路を使用する場合、各回路の定格はアプライアンスのフル定格に基づいている必要があります。この設定は、回路の故障や電源の故障に備えたものです。

例：各電源はそれぞれ異なる 220V 回路に接続しています。各回路は、ラベルに記載されているように 5A を供給できる必要があります。

共有回路の設置

1 つの回路で両方の電源に電力を供給する場合は、1 つの電源の定格電力がボックス全体に適用されます。この設定は、電源の故障に対する保護のみを提供します。

例：両方の電源が同じ 220V 回路に接続されています。この回路の最大引き込み電流量は、ラベルに記載されているように 5A です。

AC 電圧

電源は公称 100VAC ～ 240VAC（最大 85VAC ～ 264 VAC）で動作します。この範囲を超える電圧を使用すると、アプライアンスが損傷する恐れがあります。

AC 電流

各電源のラベルに記載されている定格電流：電源あたりフルレンジで最大 5.2A、電源あたり 187VAC ～ 264VAC で最大 2.6A。火災発生の可能性を抑えるため、適切なワイヤおよびブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz ～ 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、または正しく動作しない可能性があります。

電源コード

電源の電源接続部は IEC C14 コネクタです。IEC C13 コネクタも使用可能です。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG、UL 認定コード（NEMA 515P プラグ付き）です。ほかの電源コードについては、工場にお問い合わせください。

DC 電源の設置

冗長電源を作成するためには個別の回路が必要です。入力線での電力グリッチによる電源状態の問題や電力損失を防ぐため、無停電電源またはバッテリ バックアップの電源を使用します。

注意　DC 電源に AC 電源を接続**しないでください**。

アプライアンス全体を稼働できる十分な電力を各電源に供給します。各電源の定格電圧と定格電流は、アプライアンスのラベルに記載されています。

Firepower システムを装着するネットワーク機器の入力部に外部電力サージ保護装置を使用します。

専用回路の設置

専用回路を使用する場合、各回路の定格はアプライアンスのフル定格に基づいている必要があります。この設定は、回路の故障や電源の故障に備えたものです。

例：各電源はそれぞれ異なる -48VDC 回路に接続しています。各回路は、ラベルに記載されているように 20A を供給できる必要があります。

共有回路の設置

1 つの回路で両方の電源に電力を供給する場合は、1 つの電源の定格電力がボックス全体に適用されます。この設定は、電源の故障に対する保護のみを提供します。

例：両方の電源が同じ –48VDC 回路に接続されています。この回路の最大引き込み電流量は、ラベルに記載されているように 20A です。

注意　この最適化を利用するには、電源コードの定格が各電源のフル定格に基づいている必要があります。

DC 電圧

電源の作動電圧は次のとおりです。

- 公称 -48VDC（RTN を基準）
- 最大 -40VDC ～ -72VDC

この範囲を超える電圧を使用すると、アプライアンスが損傷する恐れがあります。

DC 電流

電源あたり最大 11A

接地基準

DC 電源は、接地基準から完全に隔離されます。

推奨される端子

電源はネジ端子を介して DC 電源に接続します。端子は UL 認定品である必要があります。端子には、M4 または #8 ネジに対応した穴が付いている必要があります。端子の最大幅は 8.1mm（0.320 インチ）です。10 ～ 12 ゲージのワイヤ用の代表的な Y 字型端子は Tyco 325197 です。

ブレーカーの要件

定格電圧で定格電流を伝送できる十分な規模のブレーカーを用意する必要があります。回路ブレーカーは次の要件を満たしている必要があります。

- UL 認定
- CSA 認定（推奨）
- VDE 認定（推奨）
- 最大負荷電流（20A）に対応
- 導入電圧（電源での必要に応じて -40V ～ -72VDC）に対応
- DC 使用に適した定格

推奨されるブレーカーは Airpax IELK1-1-72-20.0-01-V です。使用する端末のオプションは、インストールによって異なります。このブレーカーは単極、定格 DC 80V の 20A ブレーカーです。このブレーカーは*長期遅延型*であると示されています。このブレーカーに関する情報は http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf にあります。

最小ワイヤ サイズ要件

レースウェイあたり 3 本のワイヤ（1 回路）を使用した給電部では、12 AWG 線を使用できます。レースウェイあたり複数の回路を使用した給電部では、10 AWG 線を使用する必要があります。冗長電源用の 2 つの個別の給電部が 2 つの回路であり、10 AWG 線を使用する必要があることに注意してください。

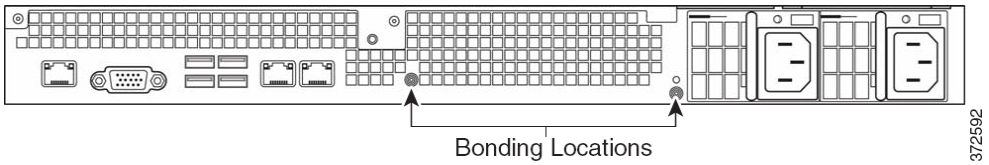
接地要件

Firepower システムは共通ボンディング網に接地する必要があります。

ボンディング位置

接地ボンディング位置は、シャーシの背面です。M4 スタッドが提供されます。リング端子を接続するための外歯ロック ワッシャが提供されます。標準接地記号を各スタッドに使用できます。

次の図は、1U シャーシのボンディング位置を示します。



推奨される端子

接地接続には、UL 認定端子を使用する必要があります。4mm または #8 スタッド用の隙間穴付きリング端子を使用できます。10 ～ 12 AWG ワイヤには Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

単一故障の場合に回路の電流を処理できる十分なサイズのアース線を使用する必要があります。アース線のサイズは、回路保護のために使用されるブレーカーの電流と同等である必要があります。AC 回路については、AC 電流（A-2 ページ）を参照してください。DC 電流については、DC 電流（A-4 ページ）を参照してください。

圧着接続を行う前に、裸導線に腐食防止剤が塗布されている必要があります。接地には銅線ケーブルだけを使用できます。

DC 電源

各 DC 電源には追加のアース接続があります。これにより、ホットスワップ可能な電源をパワー、リターン、アースに接続でき、電源を安全に挿入できます。このアース ラグを接続する必要があります。

これは M4 ネジと外歯ロック ワッシャです。

アース線のサイズは、回路のブレーカーに対応するように調整する必要があります。

Firepower 82xx ファミリアプライアンス

ここでは、次の所要電力について説明します。

- Firepower 8250、8260、8270、および 8290（CHAS-2U-AC、CHAS-2U-DC、または CHAS-2U-AC/DC）

これらのアプライアンスは、National Electric Code が適用される場所やネットワーク通信施設で、認定を受けた担当者により設置されるものです。

シスコでは、返品に備えて梱包材を保管しておくことを推奨します。

詳細については、次の項を参照してください。

- 回路の配置、電圧、電流、周波数範囲、および電源コードの詳細については AC 電源の設置（A-6 ページ）を参照してください。
- 回路の配置、電圧、電流、接地基準、端子、ブレーカーの要件、および最小ワイヤ サイズについては、DC 電源の設置（A-7 ページ）を参照してください。
- ボンディング位置、推奨される端子、アース線の要件、および DC 電源については接地要件（A-9 ページ）を参照してください。

AC 電源の設置

Firepower システムは、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

注意　AC 電源に DC 電源を接続**しないでください**。

冗長電源を作成するためには個別の回路が必要です。入力線での電力グリッチによる電源状態の問題や電力損失を防ぐため、無停電電源またはバッテリ バックアップの電源を使用します。

アプライアンス全体を稼働できる十分な電力を各電源に供給します。各電源の定格電圧と定格電流は、アプライアンスのラベルに記載されています。

Firepower システムを装着するネットワーク機器の入力部に外部電力サージ保護装置を使用します。

専用回路の設置

専用回路を使用する場合、各回路の定格はアプライアンスのフル定格に基づいている必要があります。この設定は、回路の故障や電源の故障に備えたものです。

例：各電源はそれぞれ異なる 220V 回路に接続しています。各回路は、ラベルに記載されているように 5A を供給できる必要があります。

共有回路の設置

1 つの回路で両方の電源に電力を供給する場合は、1 つの電源の定格電力がボックス全体に適用されます。この設定は、電源の故障に対する保護のみを提供します。

例：両方の電源が同じ 220V 回路に接続されています。この回路の最大引き込み電流量は、ラベルに記載されているように 5A です。

AC 電圧

電源は公称 100VAC ～ 240VAC（最大 85VAC ～ 264 VAC）で動作します。この範囲を超える電圧を使用すると、アプライアンスが損傷する恐れがあります。

AC 電流

各電源のラベルに記載されている定格電流：電源あたりフルレンジで最大 8A、電源あたり 187VAC ～ 264VAC で最大 4A。火災発生の可能性を抑えるため、適切なワイヤおよびブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz ～ 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、または正しく動作しない可能性があります。

電源コード

電源の電源接続部は IEC C14 コネクタです。IEC C13 コネクタも使用可能です。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG、UL 認定コード（NEMA 515P プラグ付き）です。ほかの電源コードについては、工場にお問い合わせください。

DC 電源の設置

冗長電源を作成するためには個別の回路が必要です。入力線での電力グリッチによる電源状態の問題や電力損失を防ぐため、無停電電源またはバッテリ バックアップの電源を使用します。

注意　DC 電源に AC 電源を接続**しないでください**。

アプライアンス全体を稼働できる十分な電力を各電源に供給します。各電源の定格電圧と定格電流は、アプライアンスのラベルに記載されています。

Firepower システムを装着するネットワーク機器の入力部に外部電力サージ保護装置を使用します。

専用回路の設置

専用回路を使用する場合、各回路の定格はアプライアンスのフル定格に基づいている必要があります。この設定は、回路の故障や電源の故障に備えたものです。

例：各電源はそれぞれ異なる -48VDC 回路に接続しています。各回路は、ラベルに記載されているように 20A を供給できる必要があります。

共有回路の設置

1 つの回路で両方の電源に電力を供給する場合は、1 つの電源の定格電力がボックス全体に適用されます。この設定は、電源の故障に対する保護のみを提供します。

例：両方の電源が同じ –48VDC 回路に接続されています。この回路の最大引き込み電流量は、ラベルに記載されているように 20A です。

注意　この最適化を利用するには、電源コードの定格が各電源のフル定格に基づいている必要があります。

DC 電圧

電源の作動電圧は次のとおりです。

- 公称 -48VDC（RTN を基準）
- 最大 -40VDC ～ -72VDC

この範囲を超える電圧を使用すると、アプライアンスが損傷する恐れがあります。

DC 電流

電源あたり最大 18A

接地基準

DC 電源は、接地基準から完全に隔離されます。

推奨される端子

電源はネジ端子を介して DC 電源に接続します。端子は UL 認定品である必要があります。端子には、M4 または #8 ネジに対応した穴が付いている必要があります。端子の最大幅は 8.1mm（0.320 インチ）です。10 ～ 12 ゲージのワイヤ用の代表的な Y 字型端子は Tyco 325197 です。

ブレーカーの要件

定格電圧で定格電流を伝送できる十分な規模のブレーカーを用意する必要があります。回路ブレーカーは次の要件を満たしている必要があります。

- UL 認定
- CSA 認定（推奨）
- VDE 認定（推奨）
- 最大負荷電流（20A）に対応
- 導入電圧（電源での必要に応じて -40V ～ -72VDC）に対応
- DC 使用に適した定格

推奨されるブレーカーは Airpax IELK1-1-72-20.0-01-V です。使用する端末のオプションは、インストールによって異なります。このブレーカーは単極、定格 DC 80V の 20A ブレーカーです。このブレーカーは*長期遅延型*であると示されています。このブレーカーについて詳しくは、http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf を参照してください。

最小ワイヤ サイズ要件

レースウェイあたり 3 本のワイヤ（1 回路）を使用した給電部では、12 AWG 線を使用できます。レースウェイあたり複数の回路を使用した給電部では、10 AWG 線を使用する必要があります。冗長電源用の 2 つの個別の給電部が 2 つの回路であり、10 AWG 線を使用する必要があることに注意してください。

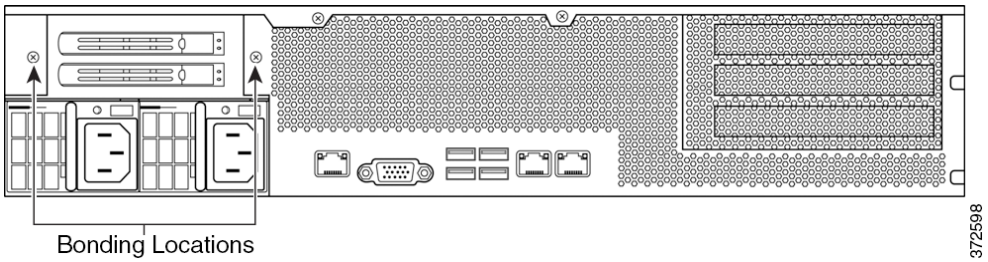
接地要件

Firepower システムは共通ボンディング網に接地する必要があります。

ボンディング位置

接地ボンディング位置は、シャーシの背面です。M4 スタッドが提供されます。リング端子を接続するための外歯ロック ワッシャが提供されます。標準接地記号を各スタッドに使用できます。

次の図は、2U シャーシのボンディング位置を示します。



推奨される端子

接地接続には、UL 認定端子を使用する必要があります。4mm または #8 スタッド用の隙間穴付きリング端子を使用できます。10 ～ 12 AWG ワイヤには Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

単一故障の場合に回路の電流を処理できる十分なサイズのアース線を使用する必要があります。アース線のサイズは、回路保護のために使用されるブレーカーの電流と同等である必要があります。AC 回路については、AC 電流（A-2 ページ）を参照してください。DC 電流については、DC 電流（A-4 ページ）を参照してください。

圧着接続を行う前に、裸導線に腐食防止剤が塗布されている必要があります。接地には銅線ケーブルだけを使用できます。

DC 電源

各 DC 電源には追加のアース接続があります。これにより、ホットスワップ可能な電源をパワー、リターン、アースに接続でき、電源を安全に挿入できます。このアース ラグを接続する必要があります。

これは M4 ネジと外歯ロック ワッシャです。

アース線のサイズは、回路のブレーカーに対応するように調整する必要があります。

Firepower および AMP 83xx ファミリアプライアンス

ここでは、次の所要電力について説明します。

- Firepower および AMP 8350、8360、8370、および 8390（PG35-2U-AC/DC）

これらのアプライアンスは、National Electric Code が適用される場所やネットワーク通信施設で、認定を受けた担当者により設置されるものです。

シスコでは、返品に備えて梱包材を保管しておくことを推奨します。

詳細については、次の項を参照してください。

- 回路の配置、電圧、電流、周波数範囲、および電源コードの詳細については AC 電源の設置（A-10 ページ）を参照してください。
- 回路の配置、電圧、電流、接地基準、端子、ブレーカーの要件、および最小ワイヤ サイズについては、DC 電源の設置（A-11 ページ）を参照してください。
- ボンディング位置、推奨される端子、アース線の要件、および DC 電源については接地要件（A-13 ページ）を参照してください。

AC 電源の設置

Firepower システムは、NFPA 70 の 250 条、National Electric Code（NEC）ハンドブック、および地域の電気規格の要件に従って設置する必要があります。

注意　AC 電源に DC 電源を接続**しないでください**。

冗長電源を作成するためには個別の回路が必要です。入力線での電力グリッチによる電源状態の問題や電力損失を防ぐため、無停電電源またはバッテリ バックアップの電源を使用します。

アプライアンス全体を稼働できる十分な電力を各電源に供給します。各電源の定格電圧と定格電流は、アプライアンスのラベルに記載されています。

Firepower システムを装着するネットワーク機器の入力部に外部電力サージ保護装置を使用します。

専用回路の設置

専用回路を使用する場合、各回路の定格はアプライアンスのフル定格に基づいている必要があります。この設定は、回路の故障や電源の故障に備えたものです。

例：各電源はそれぞれ異なる 220V 回路に接続しています。各回路は、ラベルに記載されているように 10A を供給できる必要があります。

共有回路の設置

1 つの回路で両方の電源に電力を供給する場合は、1 つの電源の定格電力がボックス全体に適用されます。この設定は、電源の故障に対する保護のみを提供します。

例：両方の電源が同じ 220V 回路に接続されています。この回路の最大引き込み電流量は、ラベルに記載されているように 10A です。

AC 電圧

電源は公称 100VAC ～ 240VAC（最大 85VAC ～ 264 VAC）で動作します。この範囲を超える電圧を使用すると、アプライアンスが損傷する恐れがあります。

AC 電流

各電源のラベルに記載されている定格電流：電源あたりフルレンジで最大 11A、電源あたり 187VAC ～ 264VAC で最大 5.5A。火災発生の可能性を抑えるため、適切なワイヤおよびブレーカーを使用する必要があります。

周波数範囲

AC 電源の周波数範囲は 47 Hz ～ 63 Hz です。この範囲外の周波数では、アプライアンスが動作しないか、または正しく動作しない可能性があります。

電源コード

電源の電源接続部は IEC C14 コネクタです。IEC C13 コネクタも使用可能です。UL 認定電源コードを使用する必要があります。最小ワイヤ ゲージは 16 AWG です。アプライアンスに付属のコードは 16 AWG、UL 認定コード（NEMA 515P プラグ付き）です。ほかの電源コードについては、工場にお問い合わせください。

DC 電源の設置

冗長電源を作成するためには個別の回路が必要です。入力線での電力グリッチによる電源状態の問題や電力損失を防ぐため、無停電電源またはバッテリ バックアップの電源を使用します。

注意　DC 電源に AC 電源を接続**しないでください**。

アプライアンス全体を稼働できる十分な電力を各電源に供給します。各電源の定格電圧と定格電流は、アプライアンスのラベルに記載されています。

Firepower システムを装着するネットワーク機器の入力部に外部電力サージ保護装置を使用します。

専用回路の設置

専用回路を使用する場合、各回路の定格はアプライアンスのフル定格に基づいている必要があります。この設定は、回路の故障や電源の故障に備えたものです。

例：各電源はそれぞれ異なる -48VDC 回路に接続しています。各回路は、ラベルに記載されているように 25A を供給できる必要があります。

共有回路の設置

1 つの回路で両方の電源に電力を供給する場合は、1 つの電源の定格電力がボックス全体に適用されます。この設定は、電源の故障に対する保護のみを提供します。

例：両方の電源が同じ –48VDC 回路に接続されています。この回路の最大引き込み電流量は、ラベルに記載されているように 25A です。

注意　この最適化を利用するには、電源コードの定格が各電源のフル定格に基づいている必要があります。

DC 電圧

電源の作動電圧は次のとおりです。

- 公称 -48VDC（RTN を基準）
- 最大 -40VDC ～ -72VDC

この範囲を超える電圧を使用すると、アプライアンスが損傷する恐れがあります。

DC 電流

電源あたり最大 25A

接地基準

DC 電源は、接地基準から完全に隔離されます。

推奨される端子

電源はネジ端子を介して DC 電源に接続します。端子は UL 認定品である必要があります。端子には、M4 または #8 ネジに対応した穴が付いている必要があります。端子の最大幅は 8.1mm（0.320 インチ）です。10 ～ 12 ゲージのワイヤ用の代表的な Y 字型端子は Tyco 325197 です。

ブレーカーの要件

定格電圧で定格電流を伝送できる十分な規模のブレーカーを用意する必要があります。回路ブレーカーは次の要件を満たしている必要があります。

- UL 認定
- CSA 認定（推奨）
- VDE 認定（推奨）
- 最大負荷電流（20A）に対応
- 導入電圧（電源での必要に応じて - 40V ～ -72VDC）に対応
- DC 使用に適した定格

推奨されるブレーカーは Airpax IELK1-1-72-20.0-01-V です。使用する端末のオプションは、インストールによって異なります。このブレーカーは単極、定格 DC 80V の 20A ブレーカーです。このブレーカーは*長期遅延型*であると示されています。このブレーカーについて詳しくは、http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf を参照してください。

最小ワイヤ サイズ要件

レースウェイあたり 3 本のワイヤ（1 回路）を使用した給電部では、12 AWG 線を使用できます。レースウェイあたり複数の回路を使用した給電部では、10 AWG 線を使用する必要があります。冗長電源用の 2 つの個別の給電部が 2 つの回路であり、10 AWG 線を使用する必要があることに注意してください。

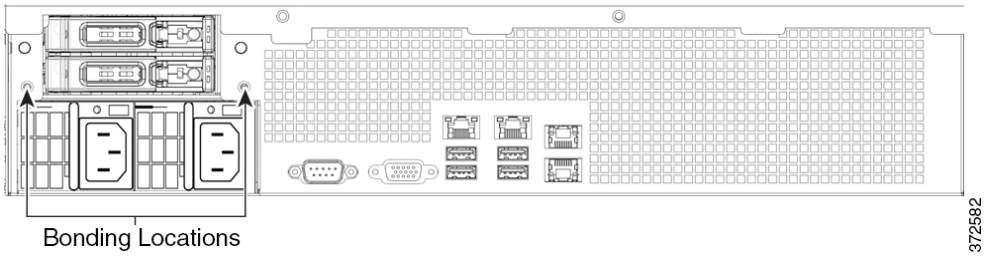
接地要件

Firepower システムは共通ボンディング網に接地する必要があります。

ボンディング位置

接地ボンディング位置は、シャーシの背面です。M4 スタッドが提供されます。リング端子を接続するための外歯ロック ワッシャが提供されます。標準接地記号を各スタッドに使用できます。

次の図は、83xx ファミリ 2U シャーシのボンディング位置を示します。



推奨される端子

接地接続には、UL 認定端子を使用する必要があります。4mm または #8 スタッド用の隙間穴付きリング端子を使用できます。10 ～ 12 AWG ワイヤには Tyco 34853 が推奨されます。これは、#8 スタッド用の穴付き UL 認定リング端子です。

アース線の要件

単一故障の場合に回路の電流を処理できる十分なサイズのアース線を使用する必要があります。アース線のサイズは、回路保護のために使用されるブレーカーの電流と同等である必要があります。AC 回路については、AC 電流（A-11 ページ）を参照してください。DC 電流については、DC 電流（A-12 ページ）を参照してください。

圧着接続を行う前に、裸導線に腐食防止剤が塗布されている必要があります。接地には銅線ケーブルだけを使用できます。

DC 電源

各 DC 電源には追加のアース接続があります。これにより、ホットスワップ可能な電源をパワー、リターン、アースに接続でき、電源を安全に挿入できます。このアース ラグを接続する必要があります。

これは M4 ネジと外歯ロック ワッシャです。

アース線のサイズは、回路のブレーカーに対応するように調整する必要があります。

Firepower 8000 シリーズネットワーク モジュールの挿入と取り外し

Firepower 8000 シリーズデバイスは、銅線センシング インターフェイスまたはファイバ センシング インターフェイスのどちらかを含むネットワーク モジュール（NetMod）を使用して、導入時のモジュールの柔軟性を強化します。デバイスは完全に組み立てられた状態で出荷することも、自分でモジュールを設置することもできます。モジュールの交換や変更が必要な場合もあります。

このセクションで説明するいくつかの手順を使用して、新しい NetMod の挿入や、インストール済み NetMod の削除または交換を実行します。

注意 NetMod のホットスワップは**できません**。モジュールを挿入または取り外す前に、電源をオフにし、アプライアンスから**両方の**電源コードを抜きます。

コメント スタック構成で NetMod を交換するときは、最初にセカンダリ ユニットですべての手順を完了してから、プライマリ ユニットで交換を実行します。

FirePOWER 8000 シリーズモジュールについて

Firepower システムを設置する前に、新しいアプライアンスのデバイスを組み立ててください。NetMod に付属の組立説明書を参照してください。

コメント 韓国の認証（KCC マーク）を受けているフル構成された Firepower デバイスの場合、NetMod を交換するとその構成が変更される可能性があります。詳しくは、アプライアンスの元のコンフィギュレーション マニュアル、および『*Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances*』マニュアルを参照してください。

モジュール部品の確認

Firepower 8000 シリーズアプライアンスのセンシング インターフェイスには、銅線インターフェイスまたはファイバ インターフェイスが付属しています。設定可能バイパス センシング インターフェイスまたは非バイパス センシング インターフェイスを指定できます。モジュールのセンシング インターフェイス、速度、寸法に関係なく、NetMod の付属部品はすべて同一です。

図 B-1　NetMod またはスロット カバーの例（開いた状態）

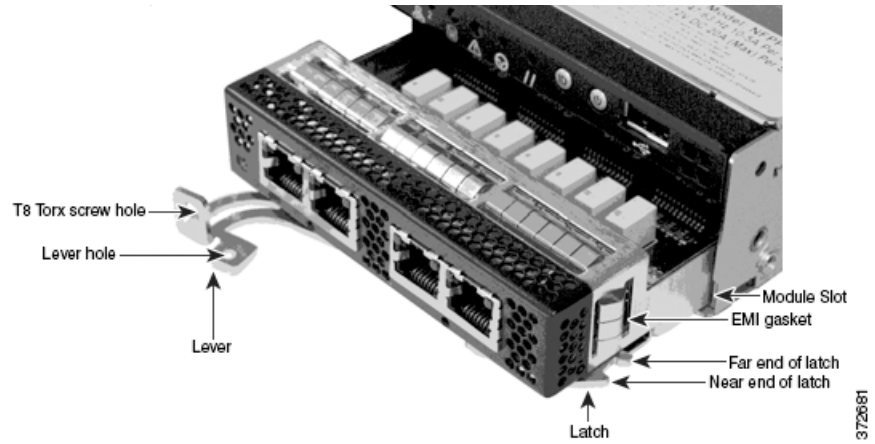
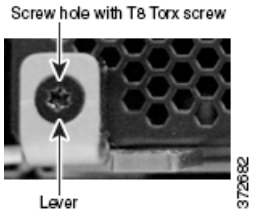


図 B-2　NetMod レバーの例（ネジを穴に取り付け、閉じた状態）



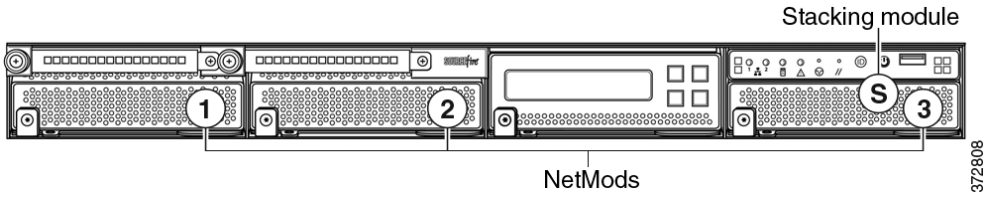
Firepower 8000 シリーズモジュールの詳細については、Firepower 8000 シリーズモジュール（2-13 ページ）を参照してください。

Firepower 8000 シリーズデバイスのモジュール スロット

次のシャーシ前面図に、センシング インターフェイスの NetMod が含まれるモジュール スロットの位置を示します。

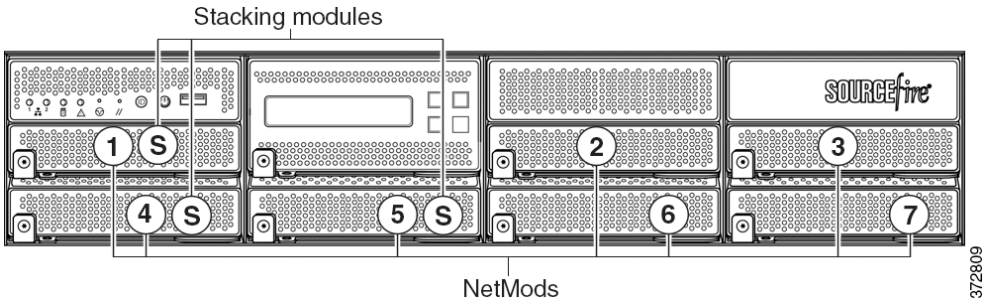
- Firepower 81xx ファミリデバイスの次のスロットでモジュールを使用できます。

図 B-3　Firepower 81xx ファミリのプライマリ デバイス



- Firepower 82xx ファミリおよび 83xx ファミリデバイスの次のスロットでモジュールを使用できます。

図 B-4　Firepower 82xx ファミリおよび 83xx ファミリプライマリ デバイス



スタック設定に関する考慮事項

スタッキング モジュールは、同じ設定を持つ複数のアプライアンスのリソースを統合したものです。どの Firepower 8000 シリーズモデルがスタックをサポートするかの詳細については、Firepower 8000 シリーズスタック モジュール（3-10 ページ）を参照してください。スタック構成デバイスの場合、モジュールを次のように設定します。

- デバイス スタックは展開内で単一のデバイスと同じように使用できますが、いくつかの例外があります。ハイ アベイラビリティ ペアに Firepower 8000 シリーズデバイスがある場合は、デバイスのハイ アベイラビリティ ペアまたはハイ アベイラビリティ ペアのデバイスをスタックできません。
- スタック構成で NetMod を交換するときは、最初にセカンダリ ユニットですべての手順を完了してから、プライマリ ユニットで交換を実行します。
- NetMod はプライマリ デバイスのみに装着します。
- プライマリ デバイスに、スタック構成のセカンダリ デバイスごとに 1 つのスタック モジュールを装着し、もう 1 つのスタック モジュールを各セカンダリ デバイスに装着します。

スタックの詳細については、スタック構成でのデバイスの使用（3-11 ページ）を参照してください。Firepower Management Center でデバイス スタックを管理する方法については、『*Firepower Management Center Configuration Guide*』の「8000 Series Device Stacking」の章を参照してください。

付属品

モジュール アセンブリ キットには T8 トルクス ドライバと、次の 1 つ以上のモジュールが含まれています。

- クワッド ポート 1000BASE-T 銅線設定可能バイパス NetMod。詳細については、クアッドポート 1000BASE-T 銅線設定可能バイパス NetMod（2-14 ページ）を参照してください。
- クワッド ポート 1000BASE-SX ファイバ設定可能バイパス NetMod。詳細については、クアッドポート 1000BASE-SX ファイバ設定可能バイパス NetMod（2-15 ページ）を参照してください。
- デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod。詳細については、デュアルポート 10GBASE（MMSR または SMLR）ファイバ設定可能バイパス NetMod（2-16 ページ）を参照してください。
- デュアル ポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod。詳細については、デュアルポート 40GBASE-SR4 ファイバ設定可能バイパス NetMod（2-18 ページ）を参照してください。

コメント　このデュアルスロット NetMod は、容量が 40G の Firepower 8250 か、Firepower または AMP 8350 でのみ使用します。デバイスをアップグレードする必要がある場合は、『*Cisco* 8000 シリーズ *Device 40G Capacity Upgrade Guide*』を参照してください。

- クワッド ポート 1000BASE-T 銅線非バイパス NetMod。詳細については、クアッドポート 1000BASE-T 銅線非バイパス NetMod（2-20 ページ）を参照してください。
- クアッド ポート 1000BASE-SX ファイバ非バイパス NetMod。詳細については、クアッド ポート 1000BASE-SX ファイバ非バイパス NetMod（2-20 ページ）を参照してください。
- クアッド ポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod。詳細については、クアッドポート 10GBASE（MMSR または SMLR）ファイバ非バイパス NetMod（2-21 ページ）を参照してください。

注意　クアッド ポート 10GBASE ファイバ非バイパス NetMod は、取り外し不可能な着脱可能小型フォーム ファクタ（SFP）トランシーバを内蔵しています。SFP を取り外そうとすると、モジュールを破損する可能性があります。

- スタック モジュール。詳細については、スタッキング モジュール（2-23 ページ）を参照してください。

コメント　NetMod を Firepower デバイス上の互換性がないスロットに装着する場合、または NetMod にご使用のシステムとの互換性がない場合は、NetMod を設定しようとすると管理元の Management Center Web インターフェイスにエラー メッセージまたは警告メッセージが表示されます。支援が必要な場合は、サポートに連絡してください。

アプライアンスの電源オフ

注意　NetMod のホットスワップは**できません**。モジュールを挿入または取り外す前に、電源をオフにし、アプライアンスから**両方の**電源コードを抜きます。

はじめる前に

次のガイドラインを使用してモジュールの挿入または取り外しの準備をしてください。

- すべてのアプライアンスおよびモジュールの部品を確認します。
- NetMod を装着するスロットを確認します。

ヒント　NetMod は、使用可能な互換性のあるスロットに挿入できます。

- EMI ガスケットが正しい位置にあることを確認します。
- アプライアンスがデバイス スタックまたはハイアベイラビリティ ペアに含まれている場合は、Firepower Management Center のメンテナンス モードでデバイスを配置します。
  - [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

- メンテナンス モードを開始するスタック メンバまたはピアの横にある、メンテナンス モード切り替えアイコン( )をクリックします。
- [はい(Yes)] をクリックして、メンテナンス モードを確定します。

手順

ステップ 1　アプライアンスをシャットダウンするには、[システム(System)] > [設定(Configuration)] を選択します。

ステップ 2　[プロセス(Process)] を選択します。

ステップ 3　[アプライアンスのシャットダウン(Shutdown Appliance)] の横にある [コマンドの実行(Run Command)] をクリックします。

ステップ 4　アプライアンスからすべての電源コードを抜きます。

関連項目

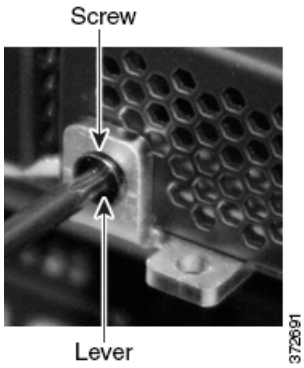
- 『*Firepower Management Center Configuration Guide*』の「Placing a High-Availability Peer into Maintenance Mode」の章。
- 『*Firepower Management Center Configuration Guide*』の「Replacing a Device in a Stack in a High-Availability Pair」の章。

モジュールまたはスロット カバーの取り外し

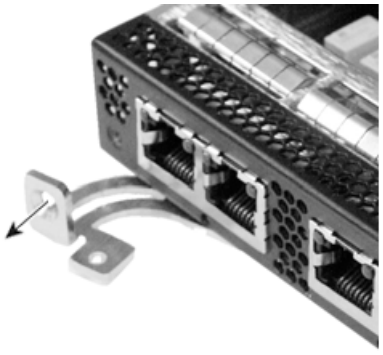
モジュールを扱うときには、リスト ストラップの装着や静電気防止作業台の使用など、適切な静電気防止(ESD)対策に従ってください。損傷を防ぐため、未使用のモジュールは静電気防止用の袋または箱に入れて保存します。

手順

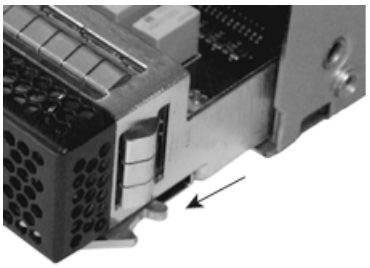
ステップ 1　付属のドライバを使用して、モジュールのレバーから T8 トルクス ネジを取り外して保管します。



ステップ 2　ラッチが解除されるまでレバーをモジュールから引き出します。



ステップ 3　モジュールを滑らせながらスロットから取り出します。

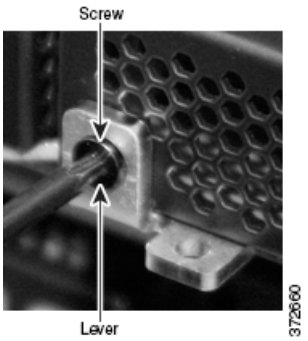


モジュールまたはスロット カバーの挿入

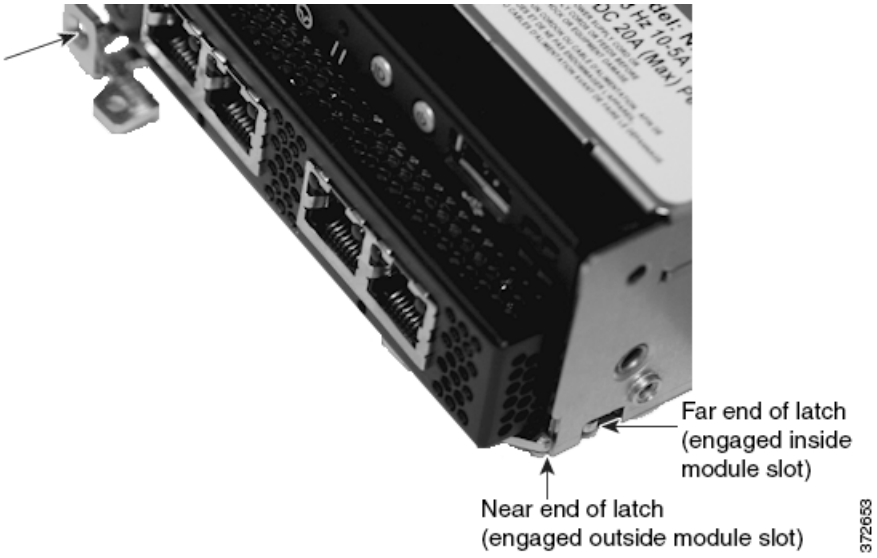
モジュールを扱うときには、リスト ストラップの装着や静電気防止作業台の使用など、適切な静電気防止（ESD）対策に従ってください。損傷を防ぐため、未使用のモジュールは静電気防止用の袋または箱に入れて保存します。

手順

ステップ 1　付属のドライバを使用して、モジュールのレバーから T8 トルクス ネジを取り外して保管します。

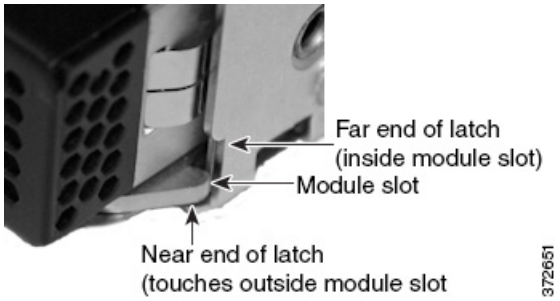


ステップ 2　ラッチが開くまで、レバーをモジュールから引き出します。ラッチの近端が目で確認できます。ラッチの遠端はモジュール内側にあります。

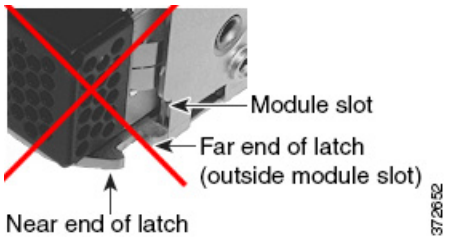


ステップ 3　ラッチの遠端がスロットの内側に入り、ラッチの近端がモジュール スロットの外側に接触するまで、モジュールをスロットに挿入します。

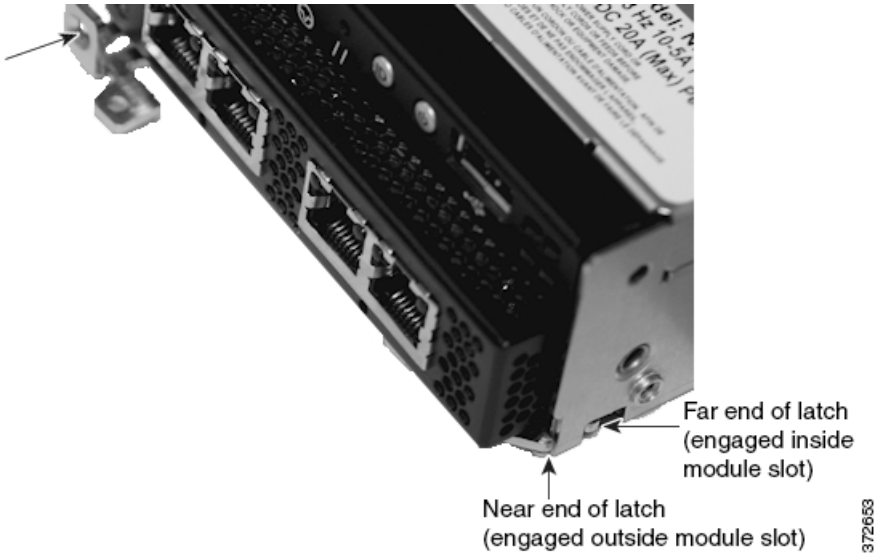
正しいモジュールの配置



正しくないモジュールの配置



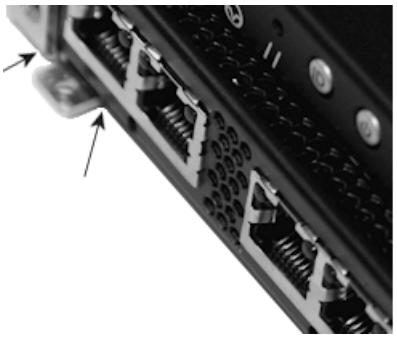
ステップ 4　ラッチがはまり、モジュールをスロットに引き込むまで、レバーをモジュールの方へ押します。



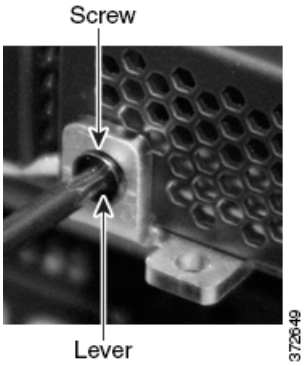
注意　力を**入れすぎないでください**。ラッチがはまらない場合は、モジュールを取り外して位置を整え直してから、もう一度試してください。

ステップ 5　ネジ穴部分をしっかり押し、ラッチが確実にはまるまでモジュールに対してレバーを押し込みます。

レバーがモジュールにしっかりと押し込まれると、モジュールがシャーシとぴったりと揃います。



ステップ 6　保管しておいた T8 トルクス ネジをレバーに差し込んで締めます。



アプライアンスの再起動

はじめる前に

- アプライアンスにすべての電源コードを接続します。
- アプライアンスの電源が完全に入るまで待ちます。これには数分かかる場合があります。

手順

ステップ 1　[システム（System）] > [設定（Configuration）] を選択します。

ステップ 2　[プロセス（Process）] を選択します。

ステップ 3　[アプライアンスコンソールの再起動（Restart Appliance Console）] の横にある [コマンドの実行（Run Command）] をクリックします。

Firepower Management Center での NetMod の検証

手順

ステップ 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2　インターフェイスを表示するデバイスの横にある編集アイコン（  ）をクリックします。

ステップ 3　[インターフェイス（Interfaces）] タブでインターフェイスを確認します。

ステップ 4　アプライアンスがデバイス スタックまたはハイアベイラビリティ ペアに含まれている場合は、Firepower Management Center からデバイスのメンテナンス モードを終了します。

- [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
- スタック メンバまたはピアの横にあるメンテナンス モード切り替えアイコン（）をクリックすると、デバイスのメンテナンス モードが終了します。

次の作業

- 新しいインターフェイスを設定します。『*Firepower Management Center Configuration Guide*』の「Interface Configuration Settings」の章を参照してください。
- 設定の変更を適用します。

アプライアンスへの変更の適用

デバイス、デバイス クラスタ、またはデバイス スタックの設定に変更を加えた後、それらの変更を適用するまでは、システム全体に変更が反映されません。デバイスが変更適用前の状態でなければ、このオプションは無効になります。

インターフェイスを編集してデバイス ポリシーを再適用すると、編集したインターフェイス インスタンスだけでなく、デバイス上のすべてのインターフェイス インスタンスで Snort が再起動することに注意してください。

ヒント　デバイスの変更を適用するには、[Device Management] ページまたはアプライアンス エディタの [Interfaces] タブを使用します。

手順

ステップ 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2　変更を適用するデバイスの横にある適用アイコン（  ）をクリックします。

ステップ 3　プロンプトが出されたら、[Apply] をクリックします。

マルウェア ストレージ パックの取り付け

マルウェア ストレージ パックは、Firepower 8000 シリーズデバイスに取り付けることができます。マルウェア ストレージ パックは、疑わしいマルウェアにオプションで使用する、拡張ローカル ファイル ストレージ用の第 2 ソリッド ステート ドライブ（SSD）です。

シスコから購入可能なマルウェア ストレージ パック キットには、マルウェア ストレージ パックをデバイスに取り付けるために必要な部品がすべて含まれています。各キットには、シャーシ互換 SSD トレイに取り付けるマルウェア ストレージ パックと取り付け工具が含まれています。空の第 2 SSD トレイを取り外して、互換性のあるマルウェア ストレージ パックと交換します。

注意 シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**しか**購入することができません。このキットを使用できるのは、Firepower システムのバージョン 5.3 以降**のみ**です。マルウェア ストレージ パックのサポートが必要な場合は、シスコサポートにお問い合わせください。

この手順は、Firepower システムのバージョン 5.3 以降を実行している Firepower 8000 シリーズ デバイスで使用するためのものであり、次のセクションで構成されています。

マルウェア ストレージ パックの概要

Firepower 8000 シリーズデバイスには、オペレーティング システム、Firepower システムソフトウェア、およびイベントと設定ファイルのローカル ファイル ストレージに使用されるプライマリ システム ドライブとして機能するソリッド ステート ドライブ（SSD）が付属しています。*高度なマルウェア防御*機能の一部として、ネットワーク上を伝送されているマルウェア ファイルを検出、保存、追跡、分析、および（オプションで）ブロックするように Firepower システムを設定できます。検出時は、*ファイル ストレージ*機能を使用して、デバイスが対象ファイルをハード ドライブに保存することができます。

ファイルを保存するようにデバイスを設定した場合は、プライマリ ハード ドライブのスペースの特定の部分だけがキャプチャ ファイル ストレージに割り当てられます。ファイル ポリシー設定によっては、デバイスが大量のファイルをハード ドライブに保存する可能性があります。

マルウェア ストレージ パックは、疑わしいマルウェアの拡張ローカル ファイル ストレージを提供し、8000 シリーズデバイスのオプション機能として購入できます。デバイスにマルウェア ストレージ パックを取り付けて、ファイルを保存するようにデバイスを設定すると、デバイスは、マルウェア ストレージ パック全体をキャプチャしたファイルの保存用として割り当て、プライマリ ハード ドライブ上のより広い空間をイベントと設定ファイルの保存用として割り当てます。

コメント　高度なマルウェア防御とファイル制御の特定の局面では、ターゲット デバイス上で特定のライセンスされた機能を有効にする必要があります。詳細については、*Firepower Management Center Configuration Guide* を参照してください。

本書では、次の概念と手順について説明します。:

- マルウェア ストレージ パックをサポートしているデバイス
- マルウェア ストレージ パックを取り付けるために必要なもの
- 特定のデバイス タイプへのマルウェア ストレージ パックの取り付け方法
- マルウェア ストレージ パックの取り付け後の通常運用の再開方法

サポートされるデバイス

マルウェア ストレージ パックは、Firepower システムのバージョン 5.3 以降を実行している 8000 シリーズデバイスに取り付けることができます。次の 8000 シリーズデバイスは、マルウェア ストレージ パックをサポートしています。

- 81xx ファミリデバイス（Firepower 8120、8130、8140、ただし、AMP8150 は**除く**）
- 82xx ファミリデバイス（Firepower 8250、8260、8270、8290）
- 83xx ファミリデバイス（Firepower 8350、8360、8370、8390）

マルウェア ストレージ パックを取り付ける前に、Firepower システムソフトウェアのバージョン 5.3 以降を実行している必要があります。その他のガイダンスについては、シスコサポートにお問い合わせください。

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。

はじめる前に

マルウェア ストレージ パックを Firepower 8000 シリーズデバイスに取り付ける前に、マルウェア ストレージ パック取り付けキットの内容とマルウェア ストレージ パックを取り付けるデバイスを検査する必要があります。マルウェア ストレージ パック取り付けキットには、次のアイテムが含まれています。

- シャーシ互換 SSD トレイに取り付けるマルウェア ストレージ パック
- 取り付け工具
- 手順書（本書）

2 種類の取り付けキットがあります。1U シャーシ キットは 81xx ファミリのデバイスに適合し、2U シャーシ キットは 82xx ファミリと 83xx ファミリの両方のデバイスに適合します。

キットとデバイスの両方を検査して、デバイスに適切なマルウェア ストレージ パック キットが揃っていることを確認します。キットに関する質問や不明点がある場合は、シスコサポートにお問い合わせください。詳細については、次の項を参照してください。

- 1U デバイス用のマルウェア ストレージ パック キット（C-3 ページ）
- 2U デバイス用のマルウェア ストレージ パック キット（C-3 ページ）

1U デバイス用のマルウェア ストレージ パック キット

81xx ファミリのデバイスには、以下で構成される 1U シャーシ用のマルウェア ストレージ パック キットが必要です。

- シャーシ互換 SSD トレイに取り付けられるマルウェア ストレージ パック
- T8 Torx ドライバ
- 手順書（本書）

2U デバイス用のマルウェア ストレージ パック キット

82xx ファミリと 83xx ファミリのデバイスには、以下で構成される 2U シャーシ用のマルウェア ストレージ パック キットが必要です。

- シャーシ互換 SSD トレイに取り付けられるマルウェア ストレージ パック
- 3 mm 六角レンチ

インストール

マルウェア ストレージ パックは、すでに現場に展開されている 8000 シリーズデバイスに取り付けることができます。この手順は、次のシナリオに対処するために使用します。

- お客様のアップグレード中にマルウェア ストレージ パックを取り付ける、マルウェア ストレージ パックを取り付けて、Firepower システムを再イメージ化する
- お客様のアップグレード後にマルウェア ストレージ パックを取り付ける、Firepower システムを再イメージ化してから、マルウェア ストレージ パックを取り付ける

コメント　デバイスを安全にシャットダウンまたは再起動する方法については、『*Firepower Management Center Configuration Guide*』の「*Managing Devices*」の章を参照してください。

アップグレード中のマルウェア ストレージ パックの取り付け

次の手順を使用して、マルウェア ストレージ パックを現場のデバイスに取り付け、Firepower システムを再イメージ化します。

お客様のアップグレード中にマルウェア ストレージ パックを取り付けるには:

ステップ 1　システムをシャットダウンします。

ステップ 2　デバイスの電源をオフにします。

ステップ 3　マルウェア ストレージ パックを取り付ける:

- 81xx ファミリデバイスの場合は、81xx ファミリデバイスに関する手順（C-5 ページ）を参照してください。
- 82xx ファミリデバイスと 83xx ファミリデバイスの場合は、82xx ファミリデバイスと 83xx ファミリデバイスに関する手順（C-8 ページ）を参照してください。

ステップ 4　デバイスを再イメージ化します。『*Cisco Firepower 8000 Series Getting Started Guide*』と、ソフトウェア アップデートに付属のリリース ノートまたはアドバイザリ テキスト内の手順に従います。

ステップ 5　システムの電源をオンにします。

マルウェア ストレージ パックの取り付け後のデバイスの再起動方法については、取り付け後（C-12 ページ）を参照してください。

バージョン 6.0.1 デバイスへのマルウェア ストレージ パックの取り付け

次の手順を使用して、すでに設定され、Firepower システムバージョン 5.3 以降を実行しているデバイスにマルウェア ストレージ パックを取り付けます。

バージョン 5.3 以降を実行しているデバイスにマルウェア ストレージ パックを取り付けるには：

ステップ 1　システムをシャットダウンします。

ステップ 2　デバイスの電源をオフにします。

ステップ 3　マルウェア ストレージ パックを取り付ける：

- 81xx ファミリデバイスの場合は、81xx ファミリデバイスに関する手順（C-5 ページ）を参照してください。
- 82xx ファミリデバイスと 83xx ファミリデバイスの場合は、82xx ファミリデバイスと 83xx ファミリデバイスに関する手順（C-8 ページ）を参照してください。

ステップ 4　システムの電源をオンにします。

- 第 2 SSD の取り付け後のデバイスの再起動方法については、取り付け後（C-12 ページ）を参照してください。

81xx ファミリデバイスに関する手順

ここでは、Firepower 8120、8130、および 8140 デバイスを含む、81xx ファミリデバイスにマルウェア ストレージ パックを取り付ける方法について説明します。マルウェア ストレージ パックは、AMP8150 デバイスでサポート**されない**ことに注意してください。

81xx ファミリシャーシの前面図

SSD トレイは 81xx ファミリシャーシの前面にあります。

図 C-1　　81xx ファミリ（シャーシ：CHAS-1U-AC/DC）前面図

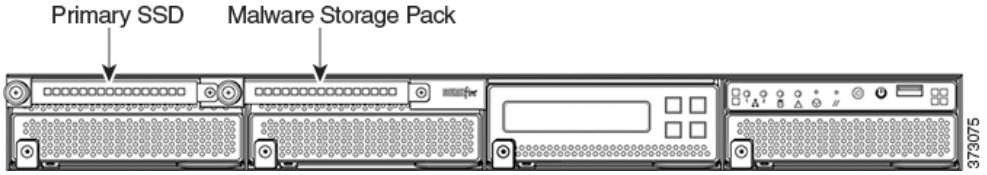
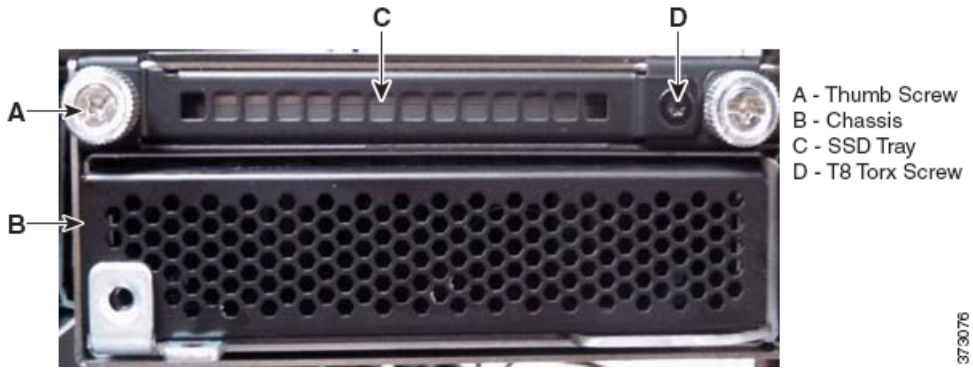


図 C-2　　SSD の詳細



次の手順では、81xx ファミリのデバイスにマルウェア ストレージ パックを取り付ける方法について説明します。*マルウェア ストレージ パック*というラベルの付いた SSD ベイにマルウェア ストレージ パックを取り付けます。空の SSD トレイを取り外して、それを該当するマルウェア ストレージ パックと交換します。

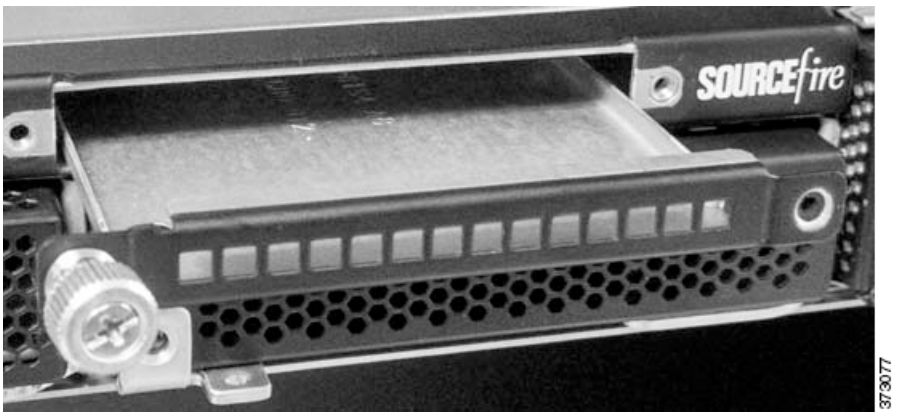
コメント　適切な静電気防止（ESD）対策（リスト ストラップや ESD 作業台など）を施します。

ステップ 1　マルウェア ストレージ パックの取り付けまたは取り外しを行う前に、デバイスの電源がオフになっていることを確認します。

ステップ 2　T8 Torx ドライバを使用して、第 2 SSD トレイの右側の Torx ネジを外します。ネジは保存しておきます。

ステップ 3　取り付けネジを緩めて外し、デバイスから空の SSD トレイを取り外します。

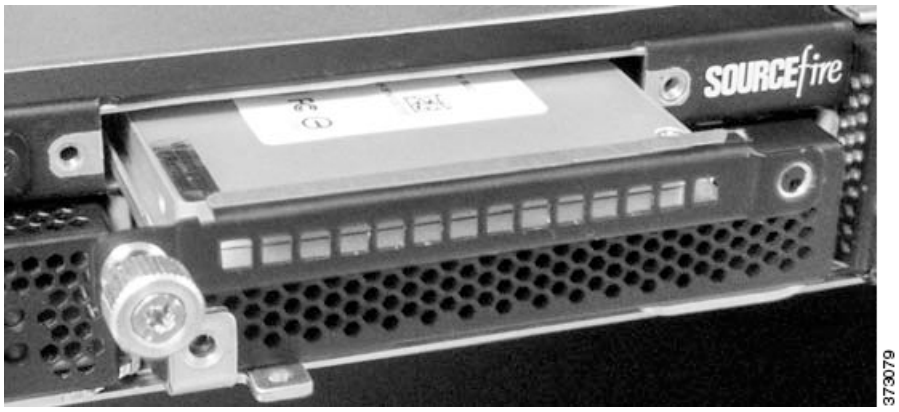
コメント　空の SSD トレイは保存しておきます。マルウェア ストレージ パックをいつでも取り外せるようにしておく必要がある場合は、デバイスに空のトレイを取り付け直します。



ステップ 4　マルウェア ストレージ パックを開梱します。

373078

ステップ 5　マルウェア ストレージ パックを SSD ベイに揃えてデバイス内に挿入します。



373079

ステップ 6　マルウェア ストレージ パックの取り付けネジを締めて、ストレージ パックをデバイスに固定します。

ステップ 7　T8 Torx ドライバを使用して、ステップ 1 で取り外したネジを元に戻します。

ステップ 8　システムの電源をオンにします。

マルウェア ストレージ パックの取り付け後のデバイスの再起動方法については、取り付け後（C-12 ページ）を参照してください。

82xx ファミリデバイスと 83xx ファミリデバイスに関する手順

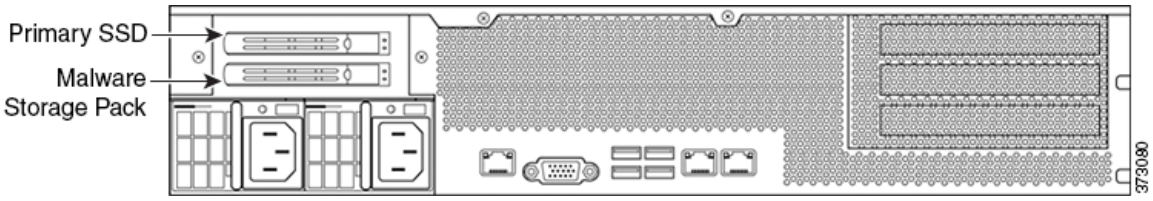
ここでは、2U シャーシ付きの次の 8000 シリーズデバイスにマルウェア ストレージ パック SSD を取り付ける方法について説明します。

- 82xx ファミリデバイス（Firepower 8250、8260、8270、8290）
- 83xx ファミリデバイス（Firepower 8350、8360、8370、8390）

82xx ファミリシャーシの背面図

SSD トレイは 82xx ファミリシャーシの背面にあります。

図 C-3　82xx ファミリ背面図



83xx ファミリシャーシの背面図

SSD トレイは 83xx ファミリシャーシの背面にあります。

図 C-4　83xx ファミリ背面図

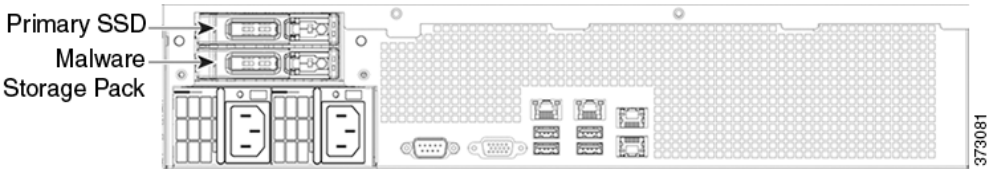
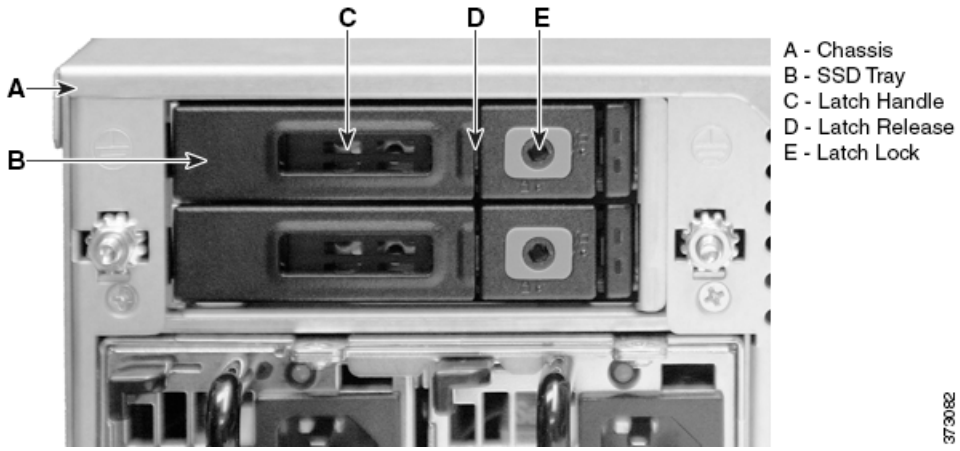


図 C-5　　SSD の詳細

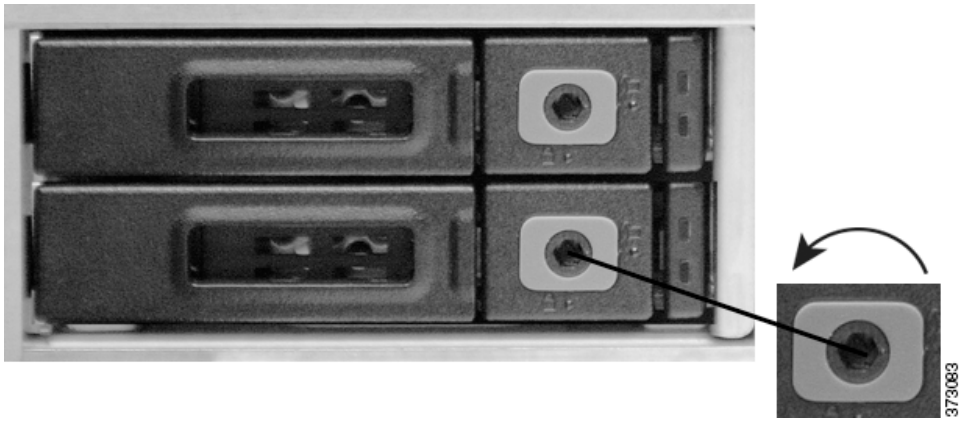


次の手順では、82xx ファミリと 83xx ファミリのデバイスにマルウェア ストレージ パックを取り付ける方法について説明します。*マルウェア ストレージ パック*というラベルの付いた SSD ベイにマルウェア ストレージ パックを取り付けます。空の SSD トレイを取り外して、それを該当するマルウェア ストレージ パックと交換します。

コメント　適切な静電気防止（ESD）対策（リスト ストラップや ESD 作業台など）を施します。

ステップ 1　マルウェア ストレージ パックの取り付けまたは取り外しを行う前に、デバイスの電源がオフになっていることを確認します。

ステップ 2　3 mm 六角レンチを使用して、一番下の SSD トレイで六角ネジをロック解除アイコン（ ）の方向に反時計回りに 1/4 だけ回すことにより、ラッチ リリースをロック解除します。

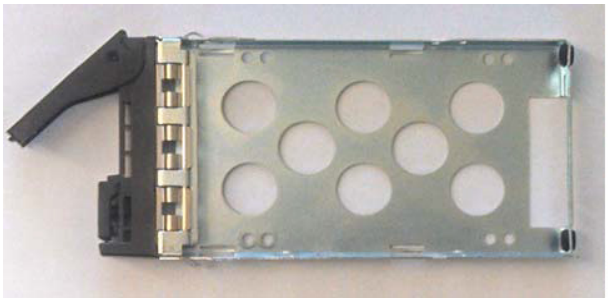


ステップ 3　ラッチ ロックを押して、ラッチ ハンドルを解放します。

ラッチ ハンドルが作業者の方に開きます。

ステップ 4　ラッチ ハンドルを引っ張って、デバイスから SSD トレイを取り外します。

コメント　空の SSD トレイは保存しておきます。マルウェア ストレージ パックをいつでも取り外せるようにしておく必要がある場合は、デバイスに空のトレイを取り付け直します。



ステップ 5　マルウェア ストレージ パックを開梱します。

ステップ 6　ラッチ ロックを押して、ラッチ ハンドルを解放します。

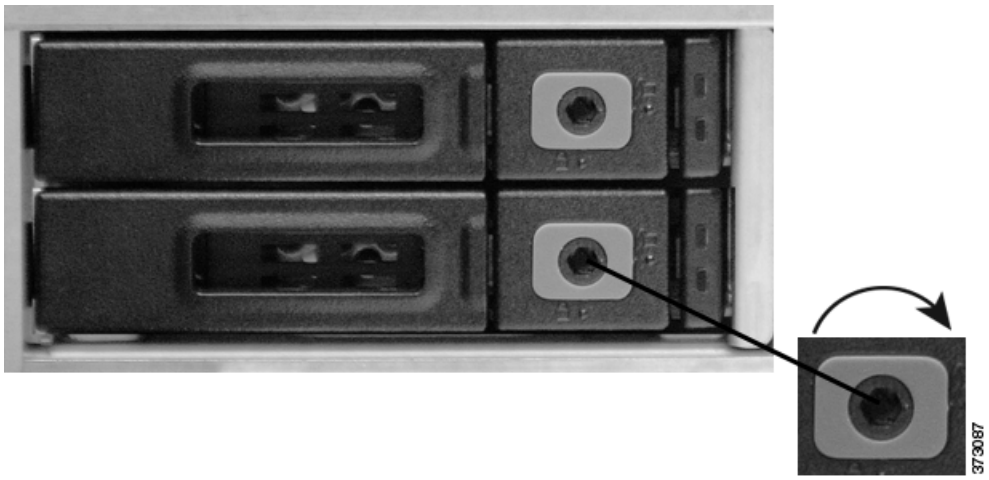
ラッチ ハンドルが作業者の方に開きます。

コメント　ラッチ リリースがロックされている場合は、3 mm 六角レンチを使用して、マルウェア ストレージ パックで六角ネジをロック解除アイコン( )の方向に反時計回りに 1/4 だけ回すことにより、ラッチ リリースをロック解除します。

ステップ 7　マルウェア ストレージ パックを SSD ベイに揃えてアプライアンス内に挿入します。

ステップ 8　SSD トレイのラッチ ハンドルを押し込んで、マルウェア ストレージ パックをアプライアンスに固定します。

ステップ 9　3 mm 六角レンチを使用して、マルウェア ストレージ パックで六角ネジをロック アイコン（  ）の方向に時計回りに 1/4 だけ回すことにより、ラッチ リリースをロックします。



ステップ 10　システムの電源をオンにします。

マルウェア ストレージ パックの取り付け後のデバイスの再起動方法については、取り付け後（C-12 ページ）を参照してください。

取り付け後

マルウェア ストレージ パックの取り付けが完了したら、デバイスを再起動して通常の運用を再開することができます。

コメント デバイスを安全に再起動またはシャットダウンする方法については、『*Firepower Management Center Configuration Guide*』の「*Managing Devices*」の章を参照してください。

デバイスを再起動すると、Firepower システムが自動的に新しいストレージ パックの追加を確認します。デバイスを再起動する前に、次の状態を確認します。

- 新しい（未フォーマット/未使用の）マルウェア ストレージ パックが検出されたら、Firepower システムが疑わしいマルウェア ファイルの保存用のディスクをフォーマットしてマウントし、ファイル ストレージ用のドライブ スペース全体を使用する 1 つのパーティションでマルウェア ストレージ パックを設定します。

コメント Firepower システムは、ストレージ パックがフォーマット中であることをコンソール メッセージ経由で作業者に通知します。マルウェア ストレージ パックのストレージ容量によっては、そのフォーマットと設定に 5 分以上かかる場合があります。リブートしたり、その他の方法でこのプロセスを中断したりしないでください。

- マルウェア ストレージ パックを、すでにプライマリ SSD 上でファイルをキャプチャするために使用されている 8000 シリーズデバイスに追加すると、Firepower システムが、ファイルを保存し、プライマリ SSD 上でこれまで使用されていたスペースを回復するための取り組みの中で、プライマリ SSD 上に保存されたファイルを新しいマルウェア ストレージ パックに移動します。

コメント Firepower システムは、ファイル キャプチャ データがプライマリ SSD から転送中であることをコンソール警告メッセージ経由で作業者に通知します。ファイル転送プロセスは 5 分以上かかる場合があります。リブートしたり、その他の方法でこのプロセスを中断したりしないでください。

マルウェア ストレージ パックはいつでもデバイスから取り除くことができることに注意してください。ファイル キャプチャ データを含むマルウェア ストレージ パックは、Firepower システムを実行している別の互換性のあるデバイスに再配置することができます。プライマリ ドライブ上のファイル キャプチャ データが再配置先のマルウェア ストレージ パックに転送され、以前のデバイスからのマルウェア ストレージ パック上の既存のデータは元のディレクトリ構造内にそのまま残されます。また、Firepower システムを使用して、マルウェア ストレージ パックの使用状況と動作状態をモニタすることができます。

詳細については、以下を参照してください。

- マルウェア ストレージ パックの取り外し（C-13 ページ）
- マルウェア ストレージ パックのモニタリング（C-13 ページ）

マルウェア ストレージ パックの取り外し

あるデバイスからマルウェア ストレージ パックを取り外して、別のデバイスに再配置することができます。

デバイスからマルウェア ストレージ パックを取り外すには:

ステップ 1　システムをシャットダウンします。

ステップ 2　デバイスの電源をオフにします。

ステップ 3　マルウェア ストレージ パックを取り外す:

- 81xx ファミリデバイスの場合は、81xx ファミリデバイスに関する手順（C-5 ページ）を参照してください（逆の順序で）。
- 82xx ファミリ デバイスと 83xx ファミリ デバイスの場合は、82xx ファミリデバイスと 83xx ファミリデバイスに関する手順（C-8 ページ）を参照してください（逆の順序で）。

ステップ 4　システムの電源をオンにします。

マルウェア ストレージ パックを取り外すと、動作状態アラートがトリガーされます。詳細については、『*Firepower Management Center Configuration Guide*』の「Using Health Monitoring」の章を参照してください。

マルウェア ストレージ パックのモニタリング

Firepower システムを使用して、マルウェア ストレージ パックをモニタします。Firepower システムは使用状況に関する情報を提供します。これには、マルウェア ストレージ パック上で使用されているスペースの割合とマルウェア ストレージ パックの容量が含まれます。Firepower システムは、システムの日常管理を支援するさまざまな便利なモニタリング機能（ヘルス モジュールなど）も提供します。詳細については、*Firepower Management Center Configuration Guide* を参照してください。