Cisco Firepower Management Center 1000、2500、4500 向けスタートアップガイド

初版：2017 年 2 月 21 日

最終更新：2020 年 4 月 6 日

Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide

Firepower Management Center（*FMC*）*1000*、*2500*、および *4500* スタートアップガイドでは、FMC のインストール、ログイン、セットアップ、初期管理設定、およびセキュアなネットワークの設定について説明します。このドキュメントでは、FMC アクセスの代替手段の確立、FMC への管理対象デバイスの追加、FMC の工場出荷時状態へのリセット、設定の保存とロード、ハードドライブの消去、アプライアンスのシャットダウンまたは再起動の実行などのメンテナンスアクティビティについても説明しています。

大規模ネットワークの一般的な導入では、複数の管理対象デバイスがネットワークセグメントにインストールされます。各デバイスは、トラフィックを制御、検査、監視、および分析して、管理 FMC に報告します。FMC は、サービスの管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

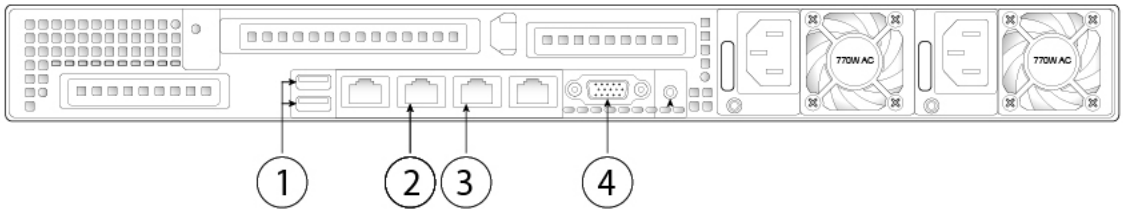
Firepower Management Center モデル 1000、2500、および 4500 について

ここでは、このドキュメントの指示に従う必要がある前面パネルと背面パネルの機能について説明します。

物理インターフェイス

次の図は、FMC 1000 の背面パネルを示し、このドキュメントの手順に従う必要があるポートを識別します。すべての背面パネルのポートについては、『Cisco Firepower Management Center 1000、2500、および 4500 ハードウェア設置ガイド』を参照してください。

図 *1 : FMC 1000* 背面パネル

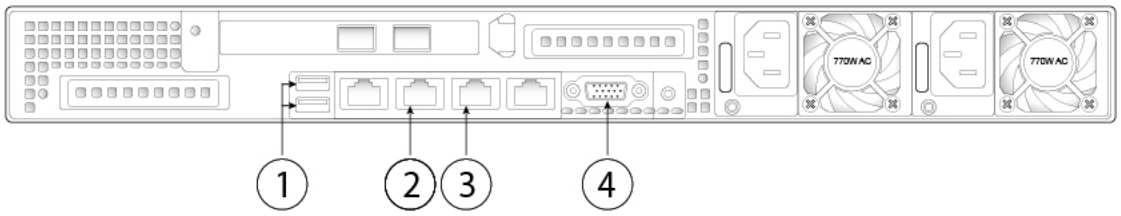


1	USB キーボードの 2 つのポート キーボードを接続して、VGA ポートのモニタとともに、コンソールにアクセスすることができます。	**2**	シリアル コンソール ポート
3	eth0 管理インターフェイス（ラベル「1」） ギガビット イーサネット 10/100/1000 Mbps インターフェイス、RJ-45 eth0 はデフォルトの管理インターフェイスです。	**4**	VGA インターフェイス コンソールメッセージは、デフォルトでこのポートに送信されます。

（注） FMC システムをリモートで監視または管理するには、Serial Over LAN（SOL）接続のデフォルト管理インターフェイス（eth0）で Lights-Out-Management（LOM）を使用できます。LOM および SOL の使用方法については、「Lights-Out Management のセットアップ （51 ページ）」を参照してください。

次の図は、FMC 2500 および 4500 の背面パネルを示し、このドキュメントの手順に従う必要があるポートを示しています。すべての背面パネルのポートについては、『Cisco Firepower Management Center 1000、2500、および 4500 ハードウェア設置ガイド』を参照してください。

図 *2 : FMC 2500* および *4500* の背面パネル



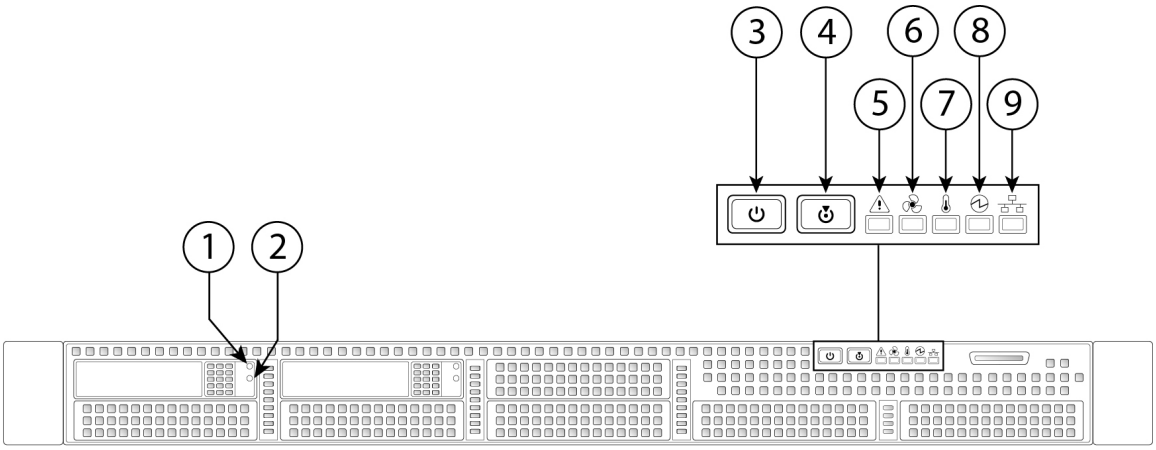
1	USB キーボードの 2 つのポート キーボードを接続して、VGA ポートのモニタとともに、コンソールにアクセスすることができます。	**2**	シリアル コンソール ポート

3	eth0 管理インターフェイス（ラベル「1」） ギガビットイーサネット 10/100/1000 Mbps インターフェイス、RJ-45 eth0 はデフォルトの管理インターフェイスです。	4	VGA インターフェイス コンソールメッセージは、デフォルトでこのポートに送信されます。

前面パネルの LED と LED の状態

次の図は、FMC 1000、2500、および 4500 の前面パネルを示します。LED ライトを識別し、LED に基づいてアプライアンスのステータスを判断するために必要な情報を提供します。FMC 2500 は 4 台の SAS ドライブを搭載し、FMC 4500 は 6 台の SAS ドライブを搭載します。図に示すように、同じドライブ障害 LED とドライブアクティビティ LED を備えています。前面パネルのすべての特徴については、『Cisco Firepower Management Center 1000、2500、および 4500 ハードウェア設置ガイド』を参照してください。

図 *3*：前面パネルの *LED*、ボタン、およびそれらの状態



1	ドライブ障害 LED • 消灯：ドライブは正常に動作中です。 • オレンジ：ドライブ障害が検出されました。 • オレンジの点滅：デバイスの再構成中です。 • 1 秒間隔のオレンジの点滅：ドライブ位置特定機能はアクティブです。	2	ドライブ アクティビティ LED • 消灯：ドライブトレイにドライブが存在しません（アクセスなし、障害なし）。 • 緑：ドライブの準備が完了しています。 • 緑の点滅：ドライブはデータの読み取り中または書き込み中です。

3	電源ボタン/電源ステータス LED • 消灯：シャーシに AC 電力が供給されていません。 • オレンジ：シャーシはスタンバイモードです。 • 緑：シャーシは主電源モードです。すべてのコンポーネントに電力が供給されています。	**4**	ユニット識別ボタン/LED • 消灯：ユニット識別機能は使用されていません。 • 青：ユニット識別機能はアクティブです。

5	システム ステータス LED
	• 緑：シャーシは正常動作状態で稼働しています。
	• 緑の点滅：シャーシはシステムの初期化とメモリチェックを行っています。
	• オレンジ：シャーシは機能が低下した動作状態にあります（軽度の障害）。次に例を示します。
	  • 電源装置の冗長性が失われています。
	  • CPU が一致しない。
	  • 少なくとも 1 個の CPU に障害が発生している。
	  • 少なくとも 1 個の DIMM に障害が発生している。
	  • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。
	• オレンジの点滅：サーバは重大な障害発生状態にあります。次に例を示します。
	  • ブートに失敗した。
	  • 修復不能な CPU またはバス エラーが検出された。
	  • シャーシは過熱状態である。
		6	ファンステータス LED
			• 緑：すべてのファンが正常に動作中です。
			• オレンジ：1 個以上のファンで重大なしきい値を超えました。
			• オレンジの点滅：1 個以上のファンで回復不能なしきい値を超えました。

7	温度ステータス LED • 緑：シャーシは正常温度で稼働中です。 • オレンジ：1 つ以上の温度センサーで重大なしきい値を超えました。 • オレンジの点滅：1 つ以上の温度センサーで回復不能なしきい値を超えました。	**8**	電源装置ステータス LED • 緑：すべての電源装置が正常に動作中です。 • オレンジ：1 つ以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置で重大な障害が発生しています。
9	ネットワーク リンク アクティビティ LED • 消灯：イーサネット リンクがアイドル状態です。 • 緑：1 個以上のイーサネット ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1 個以上のイーサネット ポートでリンクがアクティブになっていて、アクティビティが存在します。		

関連資料

ハードウェアの設置手順の詳細については、『Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide』を参照してください。

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、文書のロードマップを参照してください。

次での CLI または Linux シェルへのアクセス FMC

FMC CLI または Linux シェルにアクセスするには、FMC で実行している Firepower のバージョンに応じて、異なる手順が必要になります。

⚠

注意 Cisco TAC またはユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

始める前に

シリアルポート、キーボード、およびモニタを使用して FMC との物理的な直接接続を確立するか、FMC の管理インターフェイスを使用して SSH セッションを確立します。

手順

ステップ 1 CLI の **admin** ユーザのログイン情報を使用して FMC にログインします。

ステップ 2 使用している Firepower のバージョンに応じて、次に行う操作を決定します。

- FMC で Firepower バージョン 6.2 を実行している場合、このステップにより、Linux シェルに直接アクセスできます。
- FMC で Firepower バージョン 6.3 または 6.4 を実行しており、FMC CLI が有効になっていない場合、このステップにより、Linux シェルに直接アクセスできます。
- FMC で Firepower バージョン 6.3 または 6.4 を実行しており、FMC CLI が有効になっている場合、このステップにより、FMC CLI にアクセスできます。Linux シェルにアクセスするには、ステップ 3 に進みます。
- FMC で Firepower バージョン 6.5 以降を実行している場合、このステップにより、FMC CLI にアクセスできます。Linux シェルにアクセスするには、ステップ 3 に進みます。

ステップ 3 FMC CLI から Linux シェルにアクセスするには、**expert** コマンドを入力します。

FMC のシャットダウンまたは再起動

FMC を適切にシャットダウンまたは再起動するには、Web インターフェイスを使用します。

FMC CLI から **system shutdown** コマンドを使用して FMC をシャットダウンすることもできます（FMC CLI を使用できないバージョン 6.2 の場合は、アプライアンスシェルから **shutdown -h now** コマンドを使用できます）。

ヒント 仮想デバイスの場合は、ご使用の仮想プラットフォームのマニュアルを参照してください。特に VMware の場合、カスタム電源オプションは VMware ツールの一部です。

注意 電源ボタンを使用して FMC を停止しないでください。データが失われる可能性があります。Web インターフェイスまたは **shutdown** コマンドを使用すると、設定データを失うことなく、安全にシステムの電源を切って再起動する準備が整います。

手順

ステップ 1 **[System]** > **[Configuration]> [プロセス（Process）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [管理センターのシャットダウン（Shutdown Management Center）]：FMC のグレースフルシャットダウンを開始します。
- [管理センターの再起動（Reboot Management Center）]：FMC のグレースフルシャットダウンを実行し、再起動します。
- [管理センターコンソールの再起動（Restart Management Center Console）]：通信、データベース、HTTP サーバのプロセスを再起動します。これは、通常、トラブルシューティング時に使用されます。これにより、削除されたホストがネットワークマップに再表示される場合があります。

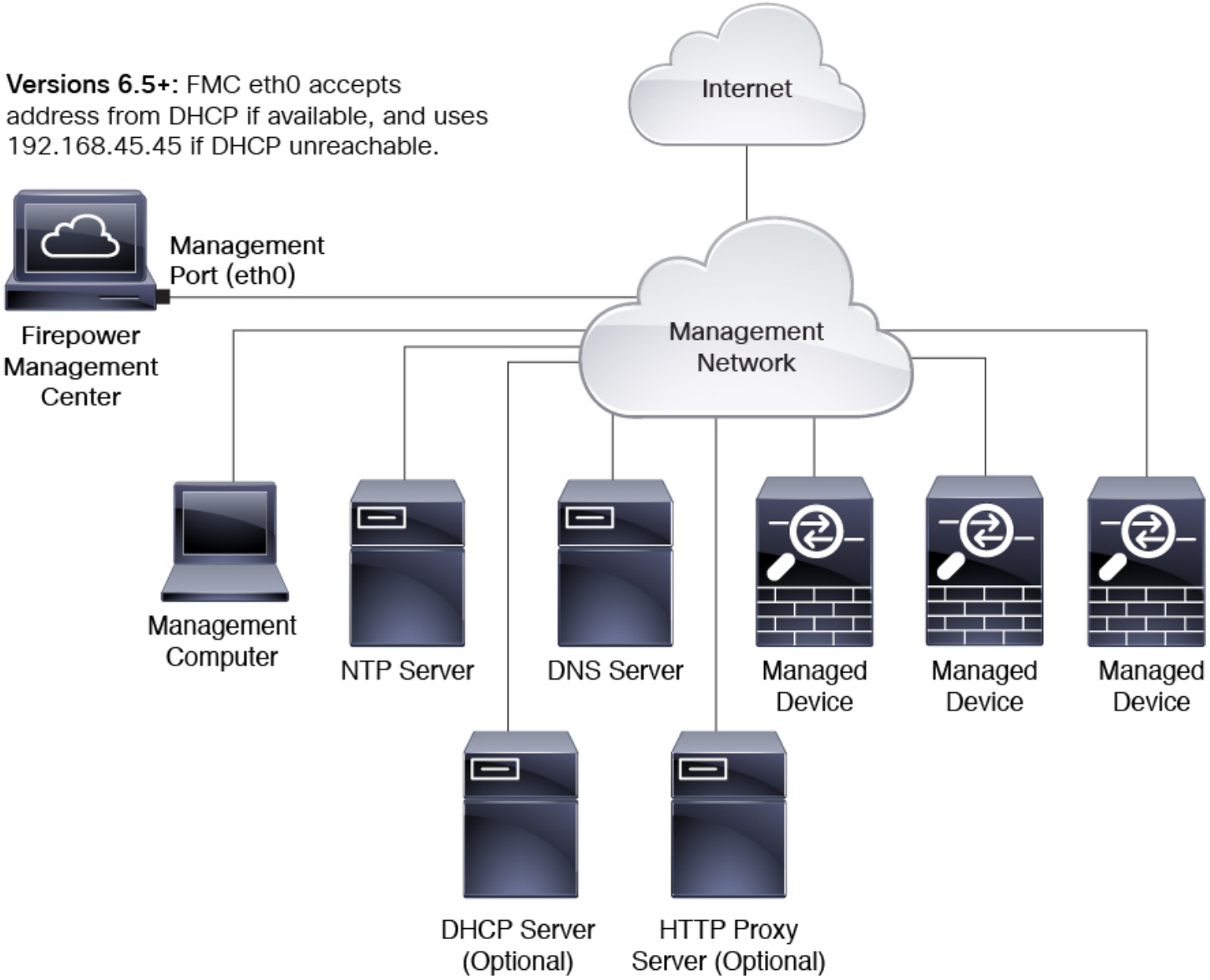
バージョン 6.5 以降の FMC のインストール

Firepower バージョン 6.5 以降を実行する FMC をインストールするには、次の手順に従います。

バージョン 6.5 以降のネットワーク展開の確認

FMC を展開するには、それが動作する環境に関する情報が必要です。次の図に、Firepower 展開のネットワーク設定の例を示します。

図 *4 :* ネットワーク導入例



デフォルトでは、FMC は管理インターフェイス（eth0）を介してローカル管理ネットワークに接続します。この接続を介して、FMC は、管理コンピュータ、管理対象デバイス、サービス（DHCP、DNS、NTP など）、およびインターネットと通信します。

スマートライセンス、AMP（Advanced Malware Protection）、および TID（Threat Intelligence Director）サービスをサポートするために FMC にはインターネットアクセスが必要です。ローカル管理ネットワークが提供するサービスによっては、NTP または DNS サーバにアクセスするためにも FMC にインターネットアクセスが必要になる場合があります。直接またはファイアウォールデバイスを介して FMC にインターネットアクセスを提供するようにネットワークを設定できます。

システムソフトウェアの更新や、脆弱性データベース（VDB）、地理位置情報データベース（GEoDB）、および侵入ルールを、インターネット接続から、または以前にインターネットからこれらの更新をダウンロードしたローカルコンピュータから、FMC に直接アップロードできます。

FMC といずれかの管理対象デバイスの間で接続を確立するには、少なくとも 1 つのデバイス（FMC または管理対象デバイス）の IP アドレスが必要です。可能であれば両方の IP アドレスを使用することをお勧めします。ただし、IP アドレスが 1 つしか分からない場合があります。たとえば、管理対象デバイスが NAT の背後にあるプライベートアドレスを使用している場合があります。この場合は、FMC アドレスしか分かりません。この場合は、管理対象デバイス上の FMC アドレスと、ユーザが選択した 1 回限り使用可能な一意のパスワード（NAT ID と呼ばれる）を指定できます。FMC では、管理対象デバイスを識別するために同じ NAT ID を指定します。

このドキュメントで説明する初期セットアップおよび設定プロセスでは、FMC がインターネットにアクセスできることを前提としています。エアギャップ環境に FMC を展開する場合、HTTP 通信用のプロキシの設定やスマートライセンス用の Smart Software Satellite Server の使用といった特定の機能をサポートするために使用できる代替方法については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。FMC がインターネットにアクセスできる展開では、システムソフトウェアの更新や、脆弱性データベース（VDB）、地理位置情報データベース（GEoDB）、および侵入ルールをインターネット接続から FMC に直接アップロードできます。ただし、FMC がインターネットにアクセスできない場合は、それらの更新が以前にインターネットからダウンロードされているローカルコンピュータから FMC にそれらをアップロードできます。さらに、エアギャップ展開では、FMC を使用して、展開内のデバイスに時間を提供することもできます。

Firepower バージョン 6.5 以降を使用した FMC の初期ネットワーク設定：

- 管理インターフェイス

  デフォルトでは、FMC は、管理インターフェイス（eth0）に使用する IP アドレス、ネットワークマスク、およびデフォルトゲートウェイについてローカル DHCP サーバを検索します。DHCP サーバに到達できない場合、FMC は、デフォルトの IPv4 アドレス（192.168.45.45）、ネットマスク（255.255.255.0）、およびゲートウェイ（192.168.45.1）を使用します。初期セットアップ時に、これらのデフォルトを受け入れるか、別の値を指定できます。

  管理インターフェイスに IPv6 アドレッシングを使用する場合は、初期セットアップの完了後に、Web インターフェイスを介してそれを設定する必要があります。

- DNS サーバ

  最大 2 つの DNS サーバの IP アドレスを指定します。評価ライセンスを使用している場合は、DNS を使用しないことを選択できます（初期設定時にホスト名とドメインを指定して、DNS を介した FMC と他のホストの通信を容易にすることもできます。初期セットアップの完了後に追加のドメインを設定できます）。

- NTP サーバ

Firepower システムを正常に動作させるには、FMC とその管理対象デバイスのシステム時刻を同期させることが不可欠です。初期設定時に FMC の時刻同期を設定する必要があります。デフォルト（0.sourcefire.pool.ntp.org と 1.sourcefire.pool.ntp.org をそれぞれプライマリ NTP サーバとセカンダリ NTP サーバとして使用）を受け入れるか、ネットワークから到達可能な 1 つまたは 2 つの信頼できる NTP サーバの FQDN または IP アドレスを指定することができます（DNS を使用していない場合は FQDN を使用して NTP サーバを指定できない）。

Firepower バージョン 6.2 ～ 6.4 を使用した FMC の初期ネットワーク設定：

- 管理インターフェイス

  FMC の管理インターフェイス（eth0）ではデフォルトの IPv4 アドレス（192.168.45.45）、ネットマスク（255.255.255.0）、およびゲートウェイ（192.168.45.1）が使用されます。初期セットアップ時に、これらのデフォルトを受け入れるか、別の値を指定できます。

  管理インターフェイスに IPv6 アドレッシングを使用する場合は、ルータの自動設定を使用するか、IPv6 アドレス、プレフィックス長、およびゲートウェイを指定する必要があります。ネットワークで DNS を使用している場合は、初期設定時にホスト名を指定して FMC を特定できます。

- DNS サーバ

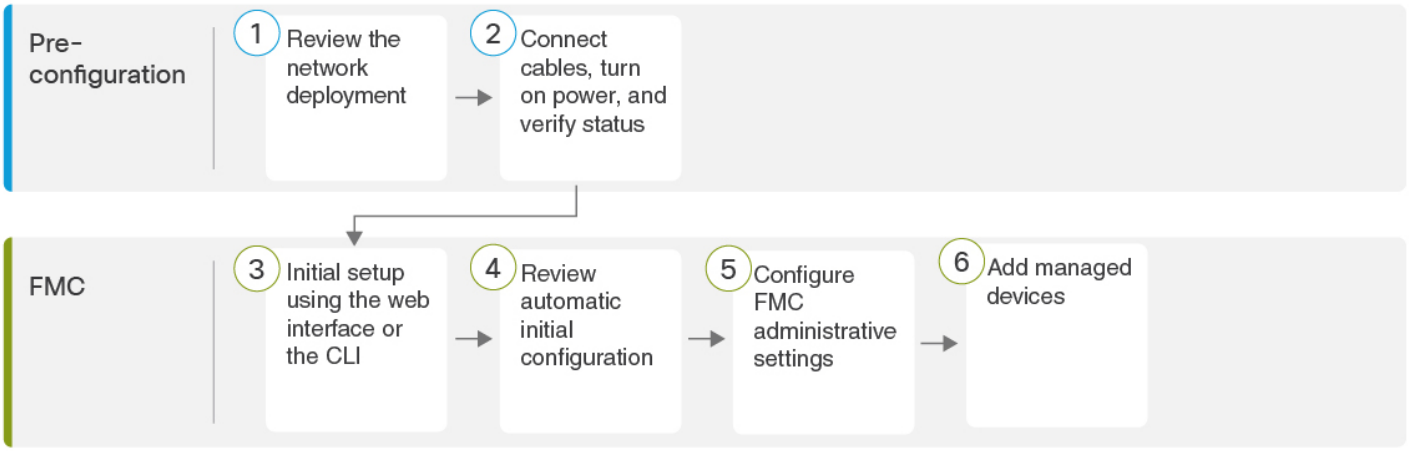
  ネットワークで DNS を使用している場合は、初期設定時に最大 3 つの DNS サーバの IP アドレスを指定できます。評価ライセンスを使用している場合は、DNS を使用しないことを選択できます（初期設定時にホスト名とドメインを指定して、DNS を介した FMC と他のホストの通信を容易にすることもできます。初期セットアップの完了後に追加のドメインを設定できます）。

- NTP サーバ

  FirePOWER システムを正常に動作させるには、FMC とその管理対象デバイスのシステム時刻を同期させることが不可欠です。初期設定では時刻同期を設定する必要はありませんが、信頼できる NTP サーバを使用するように FMC を設定することをお勧めします。初期セットアップ時に、これらの NTP サーバのホスト名または IP アドレスが必要になります。

バージョン 6.5 以降の FMC をインストールするための完全な手順

Firepower バージョン 6.5 以降を実行する FMC を展開して設定するには、次のタスクを参照してください。



1	事前設定	バージョン 6.5 以降のネットワーク展開の確認 （7 ページ）
2	事前設定	バージョン 6.2 ー 6.4 の接続ケーブル電源確認ステータス （27 ページ）
3	Firepower Management Center	次のいずれかを使用します。 • Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降） （14 ページ） • CLI（バージョン 6.5 以降）を使用した初期設定 （19 ページ）
4	Firepower Management Center	バージョン 6.5 以降の自動初期設定の確認 （22 ページ）
5	Firepower Management Center	FMC 管理設定の構成 （35 ページ）
6	Firepower Management Center	FMC への管理対象デバイスの追加 （47 ページ）

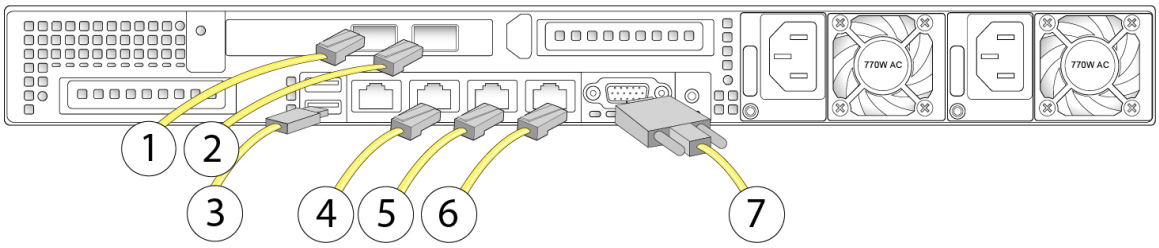
バージョン 6.5 以降のケーブルの接続、電源オン、ステータスの確認

この手順は、FMC 2500 および 4500 の背面パネルポートに関するものです。FMC 1000 は、イーサネットポートの上に 2 つの 10-G SFP+ ポートがないこと以外は同じです。

AC 電源装置は内部アースがあるため、サポート対象の AC 電源コードを使用する場合は、それ以上シャーシのアース接続は必要ありません。対応する電源コードの詳細については、『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』を参照してください。

シャーシをラックに取り付けたら、次の手順に従ってケーブルの接続、電源の投入、接続の確認を行います。背面パネルのポートを識別するには、次の図を使用します。

図 *5:* ケーブル接続



1	（モデル 2500 および 4500 のみ） eth2 管理インターフェイス 10 ギガビット イーサネット SFP+ のサポート シスコでサポートされている SFP のみを使用します。	**2**	（モデル 2500 および 4500 のみ） eth3 管理インターフェイス 10 ギガビット イーサネット SFP+ のサポート シスコでサポートされている SFP のみを使用します。
3	USB キーボード ポート	**4**	シリアル コンソール ポート コンソール ケーブル（RJ45 から DB9）を使用して、アプライアンスにコンピュータを接続します。
5	eth0 管理インターフェイス（ラベル「1」） ギガビット イーサネット 10/100/1000 Mbps インターフェイス、RJ-45 eth0 はデフォルトの管理インターフェイスです。	**6**	eth1 管理インターフェイス（ラベル「2」） ギガビット イーサネット 10/100/1000 Mbps インターフェイス、RJ-45
7	VGA ポート（DE-15 コネクタ） コンソールメッセージは、デフォルトでこのポートに送信されます。		

始める前に

重要 FMC シャーシを設置する前に、必ず『Regulatory Compliance and Safety Information』のドキュメントをお読みください。

- 『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』に記載されているようにアプライアンスをラックに設置します。

手順

ステップ 1 （モデル 2500 と 4500 のみが対象のオプション）eth2 管理インターフェイス：10 ギガビットイーサネット SFP+ インターフェイスがモデルに含まれている場合、FMC でサポートされる SFP+ トランシーバおよびケーブルを必要に応じて取り付けます。ネットワーク要件に応じて、このインターフェイスを他の管理インターフェイスと同じか、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

FMC 対応の各 SFP+ トランシーバ（FS2K-NIC-SFP/FS4K-NIC-SFP）には、セキュリティ情報が符号化された内部シリアル EEPROM が組み込まれています。このエンコーディングによって、SFP トランシーバが FMC シャーシの要件を満たしていることを識別して検証できます。

（注） シスコ認定の SFP+ トランシーバのみ、10-G インターフェイスと互換性があります。Cisco TAC は、テストされていないサードパーティ製の SFP トランシーバを使用したことに起因する相互運用性の問題についてはサポートを拒否することがあります。

ステップ 2 （モデル 2500 と 4500 のみが対象のオプション）eth3 管理インターフェイス：10 ギガビットイーサネット SFP+ インターフェイスがモデルに含まれている場合、FMC でサポートされる SFP+ トランシーバおよびケーブルを必要に応じて取り付けます。ネットワーク要件に応じて、このインターフェイスを他の管理インターフェイスと同じか、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

FMC 対応の各 SFP+ トランシーバ（FS2K-NIC-SFP/FS4K-NIC-SFP）には、セキュリティ情報が符号化された内部シリアル EEPROM が組み込まれています。このエンコーディングによって、SFP トランシーバが FMC シャーシの要件を満たしていることを識別して検証できます。

（注） シスコ認定の SFP+ トランシーバのみ、10-G インターフェイスと互換性があります。Cisco TAC は、テストされていないサードパーティ製の SFP トランシーバを使用したことに起因する相互運用性の問題についてはサポートを拒否することがあります。

ステップ 3 （オプション）USB ポート：USB ポートにキーボードを接続します。

この接続と VGA ポートに接続されたモニタを使用して、CLI で、ネットワーク設定を指定し、初期セットアップを実行することができます。

ステップ 4 （オプション）アプライアンスに付属の RJ-45 DP-9 コンソールケーブル（シスコ製品番号 72-3383-XX）を使用して、ローカルコンピュータを FMC のシリアルポートに接続します。この接続は FMC へのシリアルアクセスまたは Lights-Out 管理アクセスに使用できます。「FMC の代替アクセスのセットアップ （49 ページ）」を参照してください。

ステップ 5 eth0 管理インターフェイス（背面パネルに「1」というラベルが付いたインターフェイス）：イーサネットケーブルを使用して、管理 PC から到達可能なデフォルトの管理ネットワークに eth0 インターフェイスを接続します。このインターフェイスはデフォルトの管理インターフェイスで、デフォルトで有効になっています。ネットワーク インターフェイス（ローカルコンピュータ上）と FMC 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。

この接続を使用してネットワークを設定し、HTTPS を使用した初期設定を実行できます。この接続を使用して、ルーチン管理を実行したり、FMC Web インターフェイスからデバイスを管理したりできます。

ステップ 6 （オプション）eth1 管理インターフェイス（背面パネルのラベル「2」）：ネットワークの要件に応じて、この管理インターフェイスを他の管理インターフェイスと同じ、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、ご使用のバージョンの『Firepower Management Center Configuration Guide』を参照してください。

ステップ 7 （オプション）VGA ポート：モニタを VGA ポートに接続します。

この接続と USB ポートに接続されたキーボードを使用して、CLI で、ネットワーク設定を指定し、初期セットアップを実行することができます。

ステップ 8 電源：サポート対象の電源コードの 1 つを使用して、シャーシの電源装置を電源に接続します。対応する電源コードの詳細については、『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』を参照してください。

ステップ 9 電源：シャーシの前面にある電源ボタンを押し、前面パネルの電源ステータス LED がオンになっていることを確認します。

ステップ 10 確認：前面パネルの LED と LED の状態 （3 ページ） の図を使用して、前面パネルの LED が良好なステータスを示していることを確認します。

Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降）

FMC の IP アドレス（DHCP から取得したアドレスまたはデフォルトの 192.168.45.45）への HTTPS アクセスがある場合は、アプライアンスの Web インターフェイスで HTTPS を使用して初期設定を実行できます。手動で FMC の IP アドレスを設定する必要がある場合は、「CLI（バージョン 6.5 以降）を使用した初期設定 （19 ページ）」を参照してください。

FMC の Web インターフェイスへの初回ログイン時に、初期設定ウィザードが FMC に表示され、アプライアンスの基本設定をすばやく簡単に設定できます。このウィザードは、次の 3 つの画面と 1 つのポップアップ ダイアログ ボックスで構成されています。

- 最初の画面では、**admin** ユーザのパスワードをデフォルト値の **Admin123** から変更するよう求められます。
- 2 番目の画面では、シスコ エンドユーザ ライセンス契約（EULA）が表示されます。アプライアンスを使用するには、この内容に同意する必要があります。
- 3 番目の画面では、アプライアンス管理インターフェイスのネットワーク設定を変更できます。このページには現在の設定があらかじめ入力されており、必要に応じて変更できます。

  工場出荷時の初期状態に復元した後にアプライアンスを設定する場合（復元プロセスについて （61 ページ） を参照）に、アプライアンスのライセンスおよびネットワーク設定を削除しなかった場合、プロンプトには保持されている値が事前に入力されます。

- この画面で入力した値については、ウィザードによる検証が実行されて、次の点が確認されます。
  - 構文の正確性
  - 入力値の互換性（たとえば、IPアドレスやゲートウェイに互換性があるか、またFQDNを使用して NTP サーバが指定されている場合は設定された DNS に互換性があるか）
  - FMC と DNS サーバおよび NTP サーバとの間のネットワーク接続

  これらのテストの結果はリアルタイムで画面上に表示されます。したがって、必要な修正を行い、設定の妥当性をテストしてから、画面の下部にある [終了（Finish）] をクリックできます。NTP および DNS 接続テストは非ブロッキングです。ウィザードが接続テストを完了する前に [終了（Finish）] をクリックすることもできます。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に Web インターフェイスを使用してその接続を設定できます。

  FMC とブラウザとの間の既存の接続を切断することになる設定値を入力した場合、接続テストは実行されません。この場合、DNS または NTP の接続ステータス情報はウィザードに表示されません。
- 3 つのウィザード画面に続いて、ポップアップ ダイアログ ボックスが表示され、必要に応じてスマートライセンスをすばやく簡単に設定できます。

初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、お使いのバージョンの『Firepower Management Center コンフィギュレーションガイド ガイド』の「デバイス管理の基本」に記載されているように、デバイス管理ページが表示されます。

始める前に

- 「バージョン 6.2 ー 6.4 の接続ケーブル電源確認ステータス （27 ページ）」の説明に従って、FMC をインストールします。
- FMC が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    FMC 管理インターフェイスは、DHCP によって割り当てられた IP4 アドレスを受け入れるように事前設定されています。DHCP が FMC MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、FMC 管理インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。
- DHCP を使用している場合、次のネットワーク設定を使用して、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

このコンピュータの他のネットワーク接続をすべて無効にします。

手順

ステップ 1 Web ブラウザを使用して、FMC の IP アドレス：*https://<FMC-IP>* に移動します。

ログイン ページが表示されます。

ステップ 2 管理者アカウントのユーザ名に **admin** を、パスワードに **Admin123** を使用して FMC にログインします（パスワードでは大文字と小文字が区別されます）。

ステップ 3 [パスワードの変更（Change Password）] 画面で、次のようにします。

a) （オプション）この画面の使用中にパスワードが表示されるようにするには、[パスワードの表示（Show password）] チェックボックスをオンにします。

b) （オプション）[パスワードの生成（Generate Password）] ボタンをクリックして、表示されている条件に準拠するパスワードを自動的に作成します（生成されたパスワードは非ニーモニックです。このオプションを選択する場合は、パスワードをメモしてください）。

c) 任意のパスワードを設定するには、[新しいパスワード（New Password）] テキストボックスと [パスワードの確認（Confirm Password）] テキストボックスに新しいパスワードを入力します。

パスワードは、ダイアログに示された条件を満たす必要があります。

（注） FMC では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注） 初期設定プロセスが完了すると、システムは 2 つの **admin** アカウント（1 つは Web アクセス用、もう 1 つは CLI アクセス用）のパスワードを同じ値に設定します。パスワードは、ご使用のバージョンの『Firepower Management Center コンフィギュレーション ガイド』に記載されている強力なパスワード要件に準拠している必要があります。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

d) [次へ（Next）] をクリックします。

[パスワードの変更（Change Password）] 画面で [次へ（Next）] をクリックし、**admin** の新しいパスワードが承認されると、残りのウィザードの手順が完了していなくても、Web インターフェイスと CLI の両方の **admin** アカウントでそのパスワードが有効になります。

ステップ 4 [ユーザ契約（User Agreement）] 画面では、EULA を読み、[同意する（Accept）] をクリックし続行します。

[同意しない（Decline）] をクリックすると、FMC からログアウトされます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ネットワークの設定の変更（Change Network Settings）] 画面では次を実行します。

a) [完全修飾ドメイン名（Fully Qualified Domain Name）] を入力します。デフォルト値が表示される場合は、ネットワーク設定と互換性があればそれを使用できます。あるいは、完全修飾ドメイン名（構文は `<hostname>.<domain>`）またはホスト名を入力します。

b) [IPV4の設定（Configure IPV4）] オプションでブートプロトコルとして、[DHCPの使用（Using DHCP）] または [スタティック/手動の使用（Using Static/Manual）] を選択します。

c) [IPV4アドレス（IPV4 Address）] に表示されている値を使用するか（値が表示されている場合）、新しい値を入力できます。ドット付き 10 進法形式を使用します（192.168.45.45 など）。

（注） 初期設定中に IP アドレスを変更した場合は、新しいネットワーク情報を使用して FMC に再接続する必要があります。

d) [ネットワークマスク（Network Mask）] に表示されている値を使用するか（値が表示されている場合）、または新しい値を入力できます。ドット付き 10 進法形式を使用します（255.255.0.0 など）。

（注） 初期設定中にネットワークマスクを変更した場合は、新しいネットワーク情報を使用して FMC に再接続する必要があります。

e) [ゲートウェイ（Gateway）] に表示されている値を使用するか（値が表示されている場合）、または新しいデフォルトゲートウェイを入力できます。ドット付き 10 進法形式を使用します（192.168.0.1 など）。

（注） 初期設定中にゲートウェイを変更した場合は、新しいネットワーク情報を使用して、FMC への再接続が必要になる場合があります。

f) （オプション）[DNSグループ（DNS Group）] の場合は、デフォルト値の [Cisco Umbrella DNS] を使用します。

DNS 設定を変更するには、ドロップダウンリストから [カスタムDNSサーバ（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] と [セカンダリDNS（Secondary DNS）] の IPv4 アドレスを入力します。FMC にインターネットアクセスがない場合は、ローカルネットワークの外部では DNS を使用できません。ドロップダウンリストから [カスタムDNSサーバ（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] フィールドと [セカンダリDNS（Secondary DNS）] フィールドを空白のままにして、DNS サーバを設定しません。

（注） IP アドレスではなく FQDN を使用して NTP サーバを指定する場合は、この時点で DNS を指定する必要があります。評価ライセンスを使用している場合、DNS はオプションですが、展開の際に、DNS によって永続ライセンスの使用が求められます。

g) [NTPグループサーバ（NTP Group Servers）] の場合は、デフォルト値の [デフォルトNTPサーバ（Default NTP Servers）] を受け入れることができます。この場合は、システムでは **0.sourcefire.pool.ntp.org** がプライマリ NTP サーバとして使用され、**1.sourcefire.pool.ntp.org** がセカンダリ NTP サーバとして使用されます。

他の NTP サーバを設定するには、ドロップダウンリストから [カスタムNTPグループサーバ（Custom NTP Group Servers）] を選択し、ネットワークから到達可能な 1 台または 2 台の NTP サーバの FQDN または IP アドレスを入力します。FMC からインターネットにアクセスできない場合は、ローカルネットワークの外部で NTP サーバを使用できません。

（注） 初期設定中にネットワーク設定を変更した場合は、新しいネットワーク情報を使用して FMC に再接続する必要があります。

ステップ 7 [終了（Finish）] をクリックします。

ウィザードでは、この画面で入力した値の検証を実行して、構文の正確性、入力した値の互換性、FMC と DNS および NTP サーバ間のネットワーク接続を確認します。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に FMC Web インターフェイスを使用してその接続を設定できます。

次のタスク

- 初期設定中にネットワーク設定を変更した場合は、新しいネットワーク情報を使用して FMC に再接続する必要があります。
- スマートライセンシングを迅速かつ簡単にセットアップできるポップアップ ダイアログ ボックスが表示されます。このダイアログの使用は任意です。スマートライセンスについて十分な知識があり、FMC で Firepower Threat Defense デバイスを管理する場合は、このダイアログを使用してください。それ以外の場合は、このダイアログを閉じて、お使いのバージョンの『Firepower Management Center Configuration Guide』の「Licensing the Firepower System」を参照してください。
- 初期設定プロセスの一環として、FMC で自動的に設定される週次メンテナンスアクティビティを確認します。これらのアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。バージョン 6.5 以降の自動初期設定の確認（22 ページ）を参照してください。
- 初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、お使いのバージョンの『*Firepower Management Center* コンフィギュレーションガイド』に記載されているように、デバイス管理ページが表示されます。「FMC 管理設定の構成 （35 ページ）」の説明に従って FMC の基本設定を行います。
- 使用しているバージョンの『Firepower Management Center Configuration Guide』で説明されているように、Webインターフェイスを使用して初期設定を完了した後で、IPv6アドレッシング用に FMC を設定できます。

- 「FMC の代替アクセスのセットアップ （49 ページ） 」で説明されているように、Serial Over LANまたは Lights-Out-Management アクセス用に FMC を任意で設定できます。

CLI（バージョン 6.5 以降）を使用した初期設定

Web インターフェイスを使用する代わりに、CLI を使用して初期設定を実行できます。初期構成ウィザードを完了させ、信頼できる管理ネットワークで通信するように新しいアプライアンスを設定する必要があります。ウィザードでは、エンドユーザーライセンス契約（EULA）に同意し、管理者パスワードを変更する必要があります。

始める前に

- 「バージョン 6.2 ー 6.4 の接続ケーブル電源確認ステータス （27 ページ） 」の説明に従って、FMC をインストールします。
- FMC が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    FMC 管理インターフェイスは、DHCP によって割り当てられた IP4 アドレスを受け入れるように事前設定されています。DHCP が FMC MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、FMC 管理インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。
- 次の 3 つの方法のいずれかで FMC に接続します。
  - IPv4 管理 IP アドレスを使用して、SSH 接続を確立します。
  - USB キーボードと VGA モニタを FMC に接続してコンソールにアクセスします。
  - RJ-45 DP-9 コンソールケーブルを使用して、ローカルコンピュータを FMC のシリアルポートに接続します。

IPv4 管理 IP アドレスを使用して、FMC に SSH 接続します。

手順

ステップ 1 **admin** アカウントのユーザ名に **admin** を、パスワードに **Admin123** を使用して、コンソールで FMC にログインします。パスワードでは、大文字と小文字が区別されることに注意してください。

ステップ 2 プロンプトが表示されたら、Enter を押してエンドユーザライセンス契約（EULA）を表示します。

ステップ 3 EULA を確認します。プロンプトが表示されたら、**yes**、**YES** を入力するか、Enter を押して EULA に同意します。

重要　EULA に同意せずに続行することはできません。**yes**、**YES**、または Enter 以外で応答すると、ログアウトされます。

ステップ 4　システムのセキュリティやプライバシーを確保するために、FMC に初めてログインするときは、**admin** のパスワードを変更する必要があります。新しいパスワードの入力を求めるプロンプトが表示されたら、表示された制限に従って新しいパスワードを入力し、確認のプロンプトが表示されたら同じパスワードを再度入力します。

（注）　FMC では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注）　初期設定プロセスの完了時に、2 つの **admin** アカウント（Web アクセス用と CLI アクセス用）のパスワードは同じ値に設定されます。これは、お使いのバージョンの『Firepower Management Center Configuration Guide』に記載されている強力なパスワードの要件に準拠しています。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

ステップ 5　プロンプトに応答して、ネットワーク設定を行います。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が **(y/n)** のように括弧で囲まれて示されます。デフォルト値は、**[y]** のように大カッコ内に列挙されます。プロンプトに応答する場合は、次の点に注意してください。

- 工場出荷時の初期状態に復元した後にアプライアンスを設定し（復元プロセスについて（61 ページ）を参照）、アプライアンスのライセンスおよびネットワーク設定を削除しなかった場合、プロンプトには保持されている値が事前に入力されます。
- Enter を押して、デフォルトを受け入れます。
- ホスト名に関しては、完全修飾ドメイン名（<hostname>.<domain>）またはホスト名を入力します。このフィールドは必須です。
- IPv4 を手動で設定することを選択した場合、IPv4 アドレス、ネットマスク、およびデフォルトゲートウェイの入力が求められます。[DHCP] を選択した場合、DHCP を使用してこれらの値が割り当てられます。DHCP を選択しない場合は、これらのフィールドの値を指定する必要があります。標準のドット付き 10 進表記を使用します。
- DNS サーバの設定はオプションです。DNS サーバを指定しない場合は **none** を入力します。それ以外の場合は、1 つまたは 2 つの DNS サーバに IPv4 アドレスを指定します。2 つのアドレスを指定する場合は、カンマで区切ります。（3 つ以上の DNS サーバを指定した場合、システムは追加のエントリを無視します）FMC にインターネットアクセスがない場合は、ローカルネットワークの外部では DNS を使用できません。

  （注）　評価ライセンスを使用している場合、この時点での DNS の指定はオプションですが、展開の際に永続ライセンスを使用するには DNS が必要です。

- ネットワークから到達可能な少なくとも 1 つの NTP サーバの完全修飾ドメイン名または IP アドレスを入力する必要があります。（DHCP を使用していない場合は、NTP サーバの FQDN を指定できません）2 つのサーバ（プライマリとセカンダリ）を指定できます。情報はカンマで区切ります。（3 つ以上の DNS サーバを指定した場合、システムは追加のエントリを無視します）FMC からインターネットにアクセスできない場合は、ローカルネットワークの外部で NTP サーバを使用できません。

例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]:
208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org,
1.sourcefire.pool.ntp.org]:
```

ステップ 6 システムによって、設定の選択内容の概要が表示されます。入力した設定を確認してください。

例：

```
Hostname:                            fmc
IPv4 configured via:                 manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                         208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

ステップ 7 最後のプロンプトで設定を確認することができます。

- 設定が正しい場合は、**y** を入力して **Enter** を押し、設定を承認して続行します。
- 設定が間違っている場合は、**n** を入力し **Enter** を押します。ホスト名で始まる情報を再入力するように求められます。

例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

ステップ 8 設定を承認したら、**exit** と入力して FMC CLI を終了します。

次のタスク

- 設定したネットワーク情報を使用して FMC の Web インターフェイスに接続できます。

- 初期設定プロセスの一環として、FMC で自動的に設定される週次メンテナンスアクティビティを確認します。これらのアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。バージョン 6.5 以降の自動初期設定の確認（22 ページ）を参照してください。
- 使用しているバージョンの『Firepower Management Center Configuration Guidehttps://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html』で説明されているように、Web インターフェイスを使用して初期設定を完了した後で、IPv6 アドレッシング用に FMC を設定できます。
- 「FMC」で説明されているように、Serial Over LAN や Lights-Out-Management を利用するために FMC の代替アクセスのセットアップ （49 ページ） を任意で設定できます。

バージョン 6.5 以降の自動初期設定の確認

初期設定の一環として（初期設定ウィザードまたはCLIのどちらで実行しても）、FMCによって、メンテナンスタスクが自動的に設定され、システムが最新の状態に保たれるとともに、データがバックアップされます。

タスクは UTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクは UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。

（注） 自動スケジュール設定を検証し、FMC がスケジュールを正しく確立し、必要に応じて調整しているかを確認することを強くお勧めします。

- 週次 GeoDB 更新

  FMC では、毎週、ランダムに選択された時刻に行われるように、GeoDB の更新が自動的にスケジュールされます。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。この自動更新の設定は、Web インターフェイスの **[システム（System）]** > **[更新（Updates）]** > **[地理位置情報の更新（Geolocation Updates）]** > [位置情報の定期的な更新（Recurring Geolocation Updates）] で確認できます。システムが更新プログラムを設定できず、FMC からインターネットに接続できる場合は、ご使用のバージョンの『Firepower Management Center Configuration Guide』で説明されているように、通常の GeoDB を設定することをお勧めします。

- FMC の週次ソフトウェアアップデート

  FMC では、FMC およびその管理対象デバイスの最新ソフトウェアをダウンロードするための週次タスクが自動的にスケジュールされます。このタスクは、UTC で日曜日の午前 2 ～ 3 時の間に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、土曜日の午後から日曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージ センターを使用して、このタスクの

ステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** で確認できます。FMC からインターネットにアクセスできるにもかかわらず、自動的にスケジュールされたタスクが失敗する場合は、お使いのバージョンの『Firepower Management Center Configuration Guide』の説明に従って、ソフトウェアの更新をダウンロードする定期タスクをスケジュールすることをお勧めします。

このタスクでは、アプライアンスで現在実行されているバージョンに対するソフトウェアパッチおよびホットフィックスをダウンロードするだけです。このタスクでダウンロードされた更新プログラムのインストールは、別に行う必要があります。詳細については、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

- 週次の FMC 設定バックアップ

  FMC では、ローカルに保存された設定のみのバックアップを実行するための週次タスクが自動的にスケジュールされます。このタスクは、UTC で月曜日の午前 2 時に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、日曜日の午後から月曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** で確認できます。自動的にスケジュールされたタスクが失敗する場合は、お使いのバージョンの『Firepower Management Center Configuration Guide』の説明に従って、バックアップを実行する定期タスクをスケジュールすることをお勧めします。

- 脆弱性データベースの更新

  FMC バージョン 6.6+ では、 シスコのサポートサイトから最新の脆弱性データベース（VDB）の更新ファイルがダウンロードおよびインストールされます。これは 1 回限りの操作です。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。システムを最新の状態に保つため、FMC がインターネットにアクセスできる場合は、ご使用のバージョンの『Firepower Management Center コンフィギュレーション ガイド』の説明に従って、VDB 更新ファイルのダウンロードとインストールが自動的かつ定期的に実行されるように、タスクをスケジュールしておくことを推奨します。

- 侵入ルールの更新

  FMC のバージョン 6.6+ では、 侵入ルールがシスコのサポートサイトから自動的に日次更新されるように設定されます。影響を受けるポリシーが FMC で次に展開される際、該当する管理対象デバイスに対して自動侵入ルールの更新が展開されます。Web インターフェイスのメッセージセンターを使用して、このタスクのステータスを確認できます。このタスクの設定は、Web インターフェイスの **[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]** で確認できます。更新プログラムの設定に失敗した場合、FMC からインターネットに接続できるのであれば、ご使用のバージョンの『Firepower Management Center コンフィギュレーション ガイド』で説明されているように、通常の侵入ルールの更新を設定することをお勧めします。

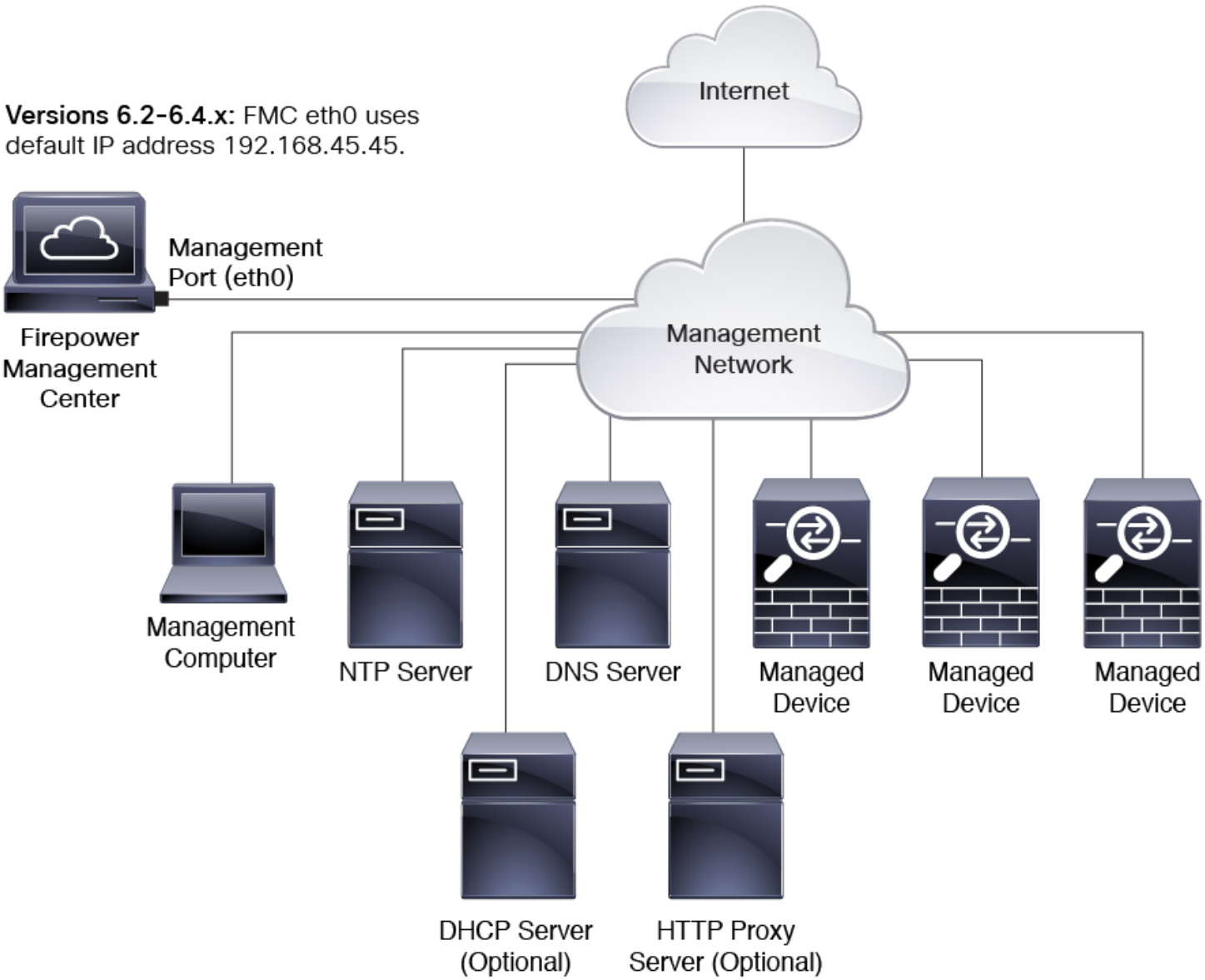
ソフトウェアバージョン 6.2 ～ 6.4 の FMC のインストール

Firepower バージョン 6.2 ー 6.4 を実行する FMC をインストールするには、次の手順に従います。

バージョン 6.2-6.4 のネットワーク導入の確認

FMC を展開するには、それが動作する環境に関する情報が必要です。次の図に、Firepower 展開のネットワーク設定の例を示します。

図 *6*: ネットワーク導入例



デフォルトでは、FMCは管理インターフェイス（eth0）を介してローカル管理ネットワークに接続します。この接続を介して、FMC は、管理コンピュータ、管理対象デバイス、サービス（DHCP、DNS、NTP など）、およびインターネットと通信します。

スマートライセンス、AMP（Advanced Malware Protection）、および TID（Threat Intelligence Director）サービスをサポートするためにFMC にはインターネットアクセスが必要です。ローカル管理ネットワークが提供するサービスによっては、NTP または DNS サーバにアクセスするためにも FMC にインターネットアクセスが必要になる場合があります。直接またはファイアウォールデバイスを介して FMC にインターネットアクセスを提供するようにネットワークを設定できます。

システムソフトウェアの更新や、脆弱性データベース（VDB）、地理位置情報データベース（GEoDB）、および侵入ルールを、インターネット接続から、または以前にインターネットからこれらの更新をダウンロードしたローカルコンピュータから、FMC に直接アップロードできます。

FMC といずれかの管理対象デバイスの間で接続を確立するには、少なくとも 1 つのデバイス（FMC または管理対象デバイス）の IP アドレスが必要です。可能であれば両方の IP アドレスを使用することをお勧めします。ただし、知っている IP アドレスは 1 つだけです。たとえば、管理対象デバイスが NAT の背後にあるプライベートアドレスを使用している可能性があるため、ユーザはFMC アドレスしか知りません。この場合は、管理対象デバイス上の FMC アドレスと、ユーザが選択した 1 回限り使用可能な一意のパスワード（NAT ID と呼ばれる）を指定できます。FMC では、管理対象デバイスを識別するために同じ NAT ID を指定します。

このドキュメントで説明する初期セットアップおよび設定プロセスでは、FMCがインターネットにアクセスできることを前提としています。エアギャップ環境に FMC を展開する場合、HTTP 通信用のプロキシの設定やスマートライセンス用の Smart Software Satellite Server の使用といった特定の機能をサポートするために使用できる代替方法については、ご使用のバージョンの『Firepower Management Center のコンフィギュレーション ガイド』を参照してください。FMC がインターネットにアクセスできる展開では、システムソフトウェアの更新や、脆弱性データベース（VDB）、地理位置情報データベース（GEoDB）、および侵入ルールをインターネット接続から FMC に直接アップロードできます。ただし、FMC がインターネットにアクセスできない場合は、それらの更新が以前にインターネットからダウンロードされているローカルコンピュータからFMCにそれらをアップロードできます。さらに、エアギャップ展開では、FMC を使用して、展開内のデバイスに時間を提供することもできます。

Firepower バージョン 6.5 以降を使用した FMC の初期ネットワーク設定：

- 管理インターフェイス

  デフォルトでは、FMC は、管理インターフェイス（eth0）に使用する IP アドレス、ネットワークマスク、およびデフォルトゲートウェイについてローカルDHCPサーバを検索します。DHCP サーバに到達できない場合、FMC は、デフォルトの IPv4 アドレス（192.168.45.45）、ネットマスク（255.255.255.0）、およびゲートウェイ（192.168.45.1）を使用します。初期セットアップ時に、これらのデフォルトを受け入れるか、別の値を指定できます。

  管理インターフェイスに IPv6 アドレッシングを使用する場合は、初期セットアップの完了後に、Web インターフェイスを介してそれを設定する必要があります。

- DNS サーバ

  最大 2 つの DNS サーバの IP アドレスを指定します。評価ライセンスを使用している場合は、DNS を使用しないことを選択できます（初期設定時にホスト名とドメインを指定して、DNS を介した FMC と他のホストの通信を容易にすることもできます。初期セットアップの完了後に追加のドメインを設定できます）。

- NTP サーバ

  Firepower システムを正常に動作させるには、FMC とその管理対象デバイスのシステム時刻を同期させることが不可欠です。初期設定時に FMC の時刻同期を設定する必要があります。デフォルト（0.sourcefire.pool.ntp.org と 1.sourcefire.pool.ntp.org をそれぞれプライマリ NTP サーバとセカンダリ NTP サーバとして使用）を受け入れるか、ネットワークから到達可能な 1 つまたは 2 つの信頼できる NTP サーバの FQDN または IP アドレスを指定することができます（DNS を使用していない場合は FQDN を使用して NTP サーバを指定できない）。

Firepower バージョン 6.2 ～ 6.4 を使用した FMC の初期ネットワーク設定：

- 管理インターフェイス

  FMC の管理インターフェイス（eth0）ではデフォルトの IPv4 アドレス（192.168.45.45）、ネットマスク（255.255.255.0）、およびゲートウェイ（192.168.45.1）が使用されます。初期セットアップ時に、これらのデフォルトを受け入れるか、別の値を指定できます。

  管理インターフェイスに IPv6 アドレッシングを使用する場合は、ルータの自動設定を使用するか、IPv6 アドレス、プレフィックス長、およびゲートウェイを指定する必要があります。ネットワークで DNS を使用している場合は、初期設定時にホスト名を指定して FMC を特定できます。

- DNS サーバ

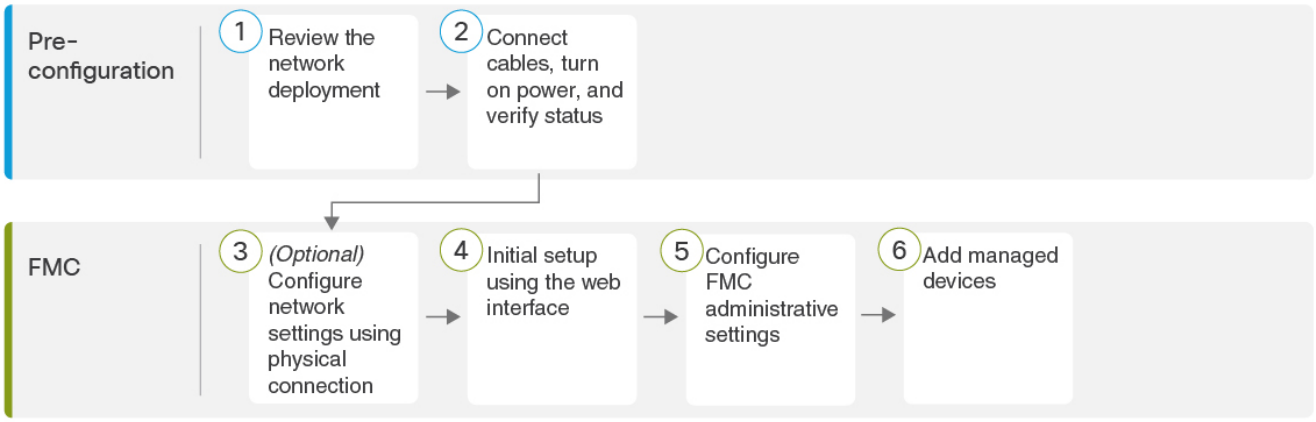
  ネットワークで DNS を使用している場合は、初期設定時に最大 3 つの DNS サーバの IP アドレスを指定できます。評価ライセンスを使用している場合は、DNS を使用しないことを選択できます（初期設定時にホスト名とドメインを指定して、DNS を介した FMC と他のホストの通信を容易にすることもできます。初期セットアップの完了後に追加のドメインを設定できます）。

- NTP サーバ

  FirePOWER システムを正常に動作させるには、FMC とその管理対象デバイスのシステム時刻を同期させることが不可欠です。初期設定では時刻同期を設定する必要はありませんが、信頼できる NTP サーバを使用するように FMC を設定することをお勧めします。初期セットアップ時に、これらの NTP サーバのホスト名または IP アドレスが必要になります。

FMC をインストールしてソフトウェアバージョン 6.2 ～ 6.4 を実行するための完全な手順

Firepower バージョン 6.2 ～ 6.4 を実行する FMC を展開して設定するには、次のタスクを参照してください。



1	事前設定	バージョン 6.2-6.4 のネットワーク導入の確認 （24 ページ）
2	事前設定	バージョン 6.2 ～ 6.4 の接続ケーブル電源確認ステータス （27 ページ）
3	Firepower Management Center	（任意）ソフトウェアバージョン 6.2 ～ 6.4 用の物理接続を使用したネットワーク設定の指定 （30 ページ）
4	Firepower Management Center	ソフトウェアバージョン 6.2 ～ 6.4 の Web インターフェイスを使用した FMC 初期セットアップ （31 ページ）
5	Firepower Management Center	FMC 管理設定の構成 （35 ページ）
6	Firepower Management Center	FMC への管理対象デバイスの追加 （47 ページ）

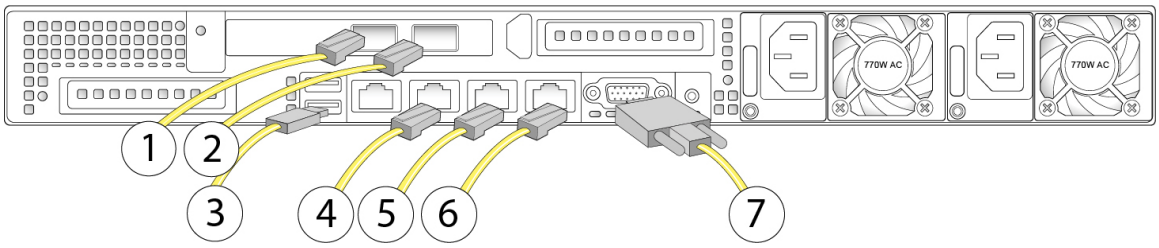
バージョン 6.2 ～ 6.4 の接続ケーブル電源確認ステータス

この手順は、FMC 2500 および 4500 の背面パネルポートに関するものです。FMC 1000 は、イーサネットポートの上に 2 つの 10-G SFP+ ポートがないこと以外は同じです。

AC 電源装置は内部アースがあるため、サポート対象の AC 電源コードを使用する場合は、それ以上シャーシのアース接続は必要ありません。対応する電源コードの詳細については、『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』を参照してください。

シャーシをラックに取り付けたら、次の手順に従ってケーブルの接続、電源の投入、接続の確認を行います。背面パネルのポートを識別するには、次の図を使用します。

図 7: ケーブル接続



1	（モデル 2500 および 4500 のみ） eth2 管理インターフェイス 10 ギガビット イーサネット SFP+ のサポート シスコでサポートされている SFP のみを使用します。	**2**	（モデル 2500 および 4500 のみ） eth3 管理インターフェイス 10 ギガビット イーサネット SFP+ のサポート シスコでサポートされている SFP のみを使用します。
3	USB キーボード ポート	**4**	シリアル コンソール ポート コンソール ケーブル（RJ45 から DB9）を使用して、アプライアンスにコンピュータを接続します。
5	eth0 管理インターフェイス（ラベル「1」） ギガビット イーサネット 10/100/1000 Mbps インターフェイス、RJ-45 eth0 はデフォルトの管理インターフェイスです。	**6**	eth1 管理インターフェイス（ラベル「2」） ギガビット イーサネット 10/100/1000 Mbps インターフェイス、RJ-45
7	VGA ポート（DE-15 コネクタ） コンソールメッセージは、デフォルトでこのポートに送信されます。		

始める前に

重要 FMC シャーシを設置する前に、必ず『Regulatory Compliance and Safety Information』のドキュメントをお読みください。

- 『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』に記載されているようにアプライアンスをラックに設置します。

手順

ステップ 1 （モデル 2500 と 4500 のみが対象のオプション）eth2 管理インターフェイス：10 ギガビットイーサネット SFP+ インターフェイスがモデルに含まれている場合、FMC でサポートされる SFP+ トランシーバおよびケーブルを必要に応じて取り付けます。ネットワーク要件に応じて、このインターフェイスを他の管理インターフェイスと同じか、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

FMC 対応の各 SFP+ トランシーバ（FS2K-NIC-SFP/FS4K-NIC-SFP）には、セキュリティ情報が符号化された内部シリアル EEPROM が組み込まれています。このエンコーディングによって、SFP トランシーバが FMC シャーシの要件を満たしていることを識別して検証できます。

（注） シスコ認定の SFP+ トランシーバのみ、10-G インターフェイスと互換性があります。Cisco TAC は、テストされていないサードパーティ製の SFP トランシーバを使用したことに起因する相互運用性の問題についてはサポートを拒否することがあります。

ステップ 2 （モデル 2500 と 4500 のみが対象のオプション）eth3 管理インターフェイス：10 ギガビットイーサネット SFP+ インターフェイスがモデルに含まれている場合、FMC でサポートされる SFP+ トランシーバおよびケーブルを必要に応じて取り付けます。ネットワーク要件に応じて、このインターフェイスを他の管理インターフェイスと同じか、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

FMC 対応の各 SFP+ トランシーバ（FS2K-NIC-SFP/FS4K-NIC-SFP）には、セキュリティ情報が符号化された内部シリアル EEPROM が組み込まれています。このエンコーディングによって、SFP トランシーバが FMC シャーシの要件を満たしていることを識別して検証できます。

（注） シスコ認定の SFP+ トランシーバのみ、10-G インターフェイスと互換性があります。Cisco TAC は、テストされていないサードパーティ製の SFP トランシーバを使用したことに起因する相互運用性の問題についてはサポートを拒否することがあります。

ステップ 3 （オプション）USB ポート：USB ポートにキーボードを接続します。

Web インターフェイスを使用して初期設定を実行する前に、この接続と VGA ポートに接続されたモニタを利用して、FMC のネットワークを設定できます。

ステップ 4 （オプション）アプライアンスに付属の RJ-45 DP-9 コンソールケーブル（シスコ製品番号 72-3383-XX）を使用して、ローカルコンピュータを FMC のシリアルポートに接続します。この接続は FMC へのシリアルアクセスまたは Lights-Out 管理アクセスに使用できます。「FMC の代替アクセスのセットアップ （49 ページ）」を参照してください。

ステップ 5 eth0 管理インターフェイス（背面パネルに「1」というラベルが付いたインターフェイス）：イーサネットケーブルを使用して、管理 PC から到達可能なデフォルトの管理ネットワークに eth0 インターフェイスを接続します。このインターフェイスはデフォルトの管理インターフェイスで、デフォルトで有効になっています。ネットワーク インターフェイス（ローカルコンピュータ上）と FMC 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。

この接続を使用してネットワークを設定し、HTTPS を使用した初期設定を実行できます。この接続を使用して、ルーチン管理を実行したり、FMC Web インターフェイスからデバイスを管理したりできます。

ステップ 6 （オプション）eth1 管理インターフェイス（背面パネルのラベル「2」）：ネットワークの要件に応じて、この管理インターフェイスを他の管理インターフェイスと同じ、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、ご使用のバージョンの『Firepower Management Center Configuration Guide』を参照してください。

ステップ 7 （オプション）VGA ポート：モニタを VGA ポートに接続します。

Web インターフェイスを使用して初期設定を実行する前に、この接続と USB ポートに接続されたキーボードを利用して、FMC のネットワークを設定できます。

ステップ 8 電源：サポート対象の電源コードの 1 つを使用して、シャーシの電源装置を電源に接続します。対応する電源コードの詳細については、『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』を参照してください。

ステップ 9 電源：シャーシの前面にある電源ボタンを押し、前面パネルの電源ステータス LED がオンになっていることを確認します。

ステップ 10 確認：前面パネルの LED と LED の状態 （3 ページ） の図を使用して、前面パネルの LED が良好なステータスを示していることを確認します。

（任意）ソフトウェアバージョン 6.2 ～ 6.4 用の物理接続を使用したネットワーク設定の指定

アプライアンスに直接接続された USB キーボードと VGA モニタを使用して Linux シェルにアクセスし、スクリプトを実行してアプライアンスのネットワーク設定を確立することができます。このタスクを実行する際は、物理インターフェイス （1 ページ） の図を参照して背面パネルのポートを識別してください。

手順

ステップ 1 モニタを VGA ポートに、キーボードをシャーシ背面の USB ポートの一つに接続します（まだ接続していない場合）。

ステップ 2 ユーザ名として **admin** を、パスワードとして **Admin123** を使用して、FMC 上の Linux シェルにアクセスします（パスワードでは大文字と小文字が区別されます）。お使いの Firepower バージョンに適した手順を使用します。「次での CLI または Linux シェルへのアクセス FMC （5 ページ）」を参照してください。

ステップ 3 次のスクリプトを実行して、FMC のネットワーク設定を指定します：**sudo /usr/local/sf/bin/configure-network**

ステップ 4 アプライアンスに IPv4 および IPv6（オプション）の設定情報を提供するためにプロンプトに応答します。

ステップ 5 最後のプロンプトで設定を確認することができます。

```
Are these settings correct? (y or n)
```

入力した設定を確認してください。

- 設定が正しい場合は、**y** を入力して **Enter** を押し、設定を承認して続行します。
- 設定が間違っている場合は、 **n** を入力し **Enter** を押します。情報を再度入力するように求められます。

ステップ 6 設定を承認した後、**exit** と入力してシェルからログアウトします。

次のタスク

ソフトウェアバージョン 6.2 ～ 6.4 の Web インターフェイスを使用した FMC 初期セットアップ （31 ページ）の説明に従ってセットアップ プロセスを完了します。

ソフトウェアバージョン 6.2 ～ 6.4 の Web インターフェイスを使用した FMC 初期セットアップ

すべての FMC に対して、FMC の Web インターフェイスにログインして、セットアップページで初期設定オプションを選択することによって、セットアッププロセスを完了する必要があります。少なくとも、管理者のパスワード変更と、ネットワーク設定の指定をまだ行っていない場合はこれらの 2 つを実行し、EULA に同意する必要があります。

手順

ステップ 1 ブラウザで https://*mgmt_ip*/ にアクセスします。ここで、*mgmt_ip* は FMC の管理インターフェイスの IP アドレスです。

- イーサネット ケーブルを使用してコンピュータに接続された FMC の場合は、そのコンピュータ上のブラウザでデフォルトの管理インターフェイスの IPv4 アドレス（https://192.168.45.45/）にアクセスします。
- 物理接続を介して FMC の IP アドレスを設定（（任意）ソフトウェアバージョン 6.2 ～ 6.4 用の物理接続を使用したネットワーク設定の指定 （30 ページ） を参照）した場合は、管理ネットワーク上のコンピュータを使用して FMC 管理インターフェイスの IP アドレスを参照します。

ステップ 2 ユーザ名として **admin** を、パスワードとして **Admin123** を使用してログインします。（パスワードでは大文字と小文字が区別されます）。

ステップ 3 [セットアップ（Setup）] ページの [パスワードの変更（Change Password）] セクションで、管理者アカウントのパスワードを変更します。Web インターフェイスの admin アカウントには管理者権限があり、アカウントを削除することはできません。大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することをお勧めします。辞書に掲載されている単語の使用は避けてください。

（注） シェルによる FMC へのアクセスと Web インターフェイスによる FMC へのアクセスのための admin アカウントは同じではないため、異なるパスワードを使用できます。この設定により、両方の管理者パスワードが同じ値に変更されます。

ステップ 4 FMC のネットワーク設定によって、管理ネットワーク上で通信できるようになります。[セットアップ（Setup）] ページの [ネットワーク設定（Network Settings）] セクションでこれらの設定を構成します。

- キーボードとモニタを使用してアプライアンスにアクセスするためのネットワーク設定がすでに完了している場合は、[セットアップ（Setup）]ページの[ネットワーク設定（Network Settings）] セクションが事前に入力されている可能性があります。
- [ネットワーク設定（Network Settings）] の値が事前に入力されていない場合、または事前に入力された値を変更する場合は、管理ネットワークプロトコルを選択する必要があります。Firepower システムは、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。IPv4、IPv6、または両方を指定できます。

  プロトコルの選択に応じて[セットアップ（Setup）]ページにフィールドが表示されます。ここで FMC の IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィックスの長さ、およびデフォルトのゲートウェイを入力する必要があります。また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。

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

ステップ 5 （任意）[セットアップ（Setup）] ページの [時刻設定（Time Settings）] セクションで、2つの方法（手動または NTP サーバからの Network Time Protocol（NTP）を使用）のいずれかで FMC の時間を設定できます。

- Network Time Protocol（NTP）を使用して時間を設定するには、[次からNTPで（Via NTP from）] をオンにして、FMC がアクセスできる 1 つ以上の NTP サーバを指定します。
- 手動で時間を設定するには、[手動（Manually）] をオンにして、表示されているフィールドに現在の時間を入力します。

ローカル Web インターフェイスで admin アカウントに対して使用されるタイム ゾーンを選択し、現在のタイム ゾーンをクリックして、ポップアップ ウィンドウからタイム ゾーンを選択します。

（注） FMC とその管理対象デバイスの間で適切な時間同期を維持するには、NTP サーバの使用が重要です。初期セットアッププロセス中に NTP サーバを設定しない場合は、できるだけ早く設定することを強くお勧めします。詳細については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドで「Time and Time Synchronization」の項を参照してください。

ステップ 6 （任意）展開で侵入検知および防御を実行するよう計画している場合、[セットアップ（Setup）] ページの [定期的なルール更新のインポート（Recurring Rule Update Imports）] セクションで [サポート サイトからのルール更新の定期インポートを有効にする] チェックボックスをオンにすることをお勧めします。

それぞれのルール更新の後で、システムが侵入についての [ポリシーの展開（Policy Deploy）] を実行するよう設定するだけでなく、[インポート頻度（Import Frequency）] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[今すぐインストール（Install Now）] チェックボックスをオンにします。

新しい脆弱性が判明すると、Cisco Talos Intelligence Group は侵入ルールの更新をリリースします。ルールの更新では、新規および更新された侵入ルールおよびプリプロセッサルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が提供されます。ルールの更新では、ルールを削除して、新しいルール カテゴリおよびシステム変数を提供する場合もあります。

ルールの更新には、新しいバイナリが含まれている場合があります。ルール更新のダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認します。加えて、ルール更新のサイズが大きい場合があるため、ネットワーク使用率の低い時間帯にルールをインポートするようにしてください。

ステップ 7 （任意）展開で位置情報関連の分析を実行する予定の場合、[セットアップ（Setup）] ページの [定期的な位置情報の更新（Recurring Geolocation Updates）] セクションで [サポート サイトからの定期的な週次更新を有効にする（Enable Recurring Weekly Updates from the Support Site）] をオンにして、表示されるフィールドを使用して [開始時間の更新（Update Start Time）] を指定することをお勧めします。初期設定プロセスの一部として GeoDB の更新を実行するには、[今すぐインストール（Install Now）] チェックボックスをオンにします。

GeoDB の更新はサイズが大きくなることがあるため、ダウンロードの後のインストールに最大で 45 分かかることがあります。GeoDB は、ネットワークの使用量が少ないときに更新してください。

ほとんどの FMC を使用して、ダッシュボードおよび Context Explorer の地理情報統計を監視するだけでなく、システムで生成されたイベントに関連付けられているルーテッド IP アドレスの地理情報を表示することができます。FMC の地理情報データベース（GeoDB）には、この機能をサポートするための情報（IP アドレスに関連する ISP、接続タイプ、プロキシ情報、正確な位置情報など）が含まれています。定期的な GeoDB の更新を有効にすることで、システムが常に最新の地理情報を使用するようにすることができます。

ステップ 8 （任意）[セットアップ（Setup）] ページの [自動バックアップ（Automatic Backups）] セクションで、[自動バックアップを有効にする（Enable Automatic Backups）] をオンにして、失敗した場合に復元できる FMC の設定の週次バックアップを作成するスケジュール タスクを作成できます。

ステップ 9 FMC を使用して、管理対象のデバイスのライセンスを管理します。FMC は、デバイスに必要なライセンスのタイプに関係なく、デバイスを管理できます。

- 7000 および 8000 シリーズ、ASA with FirePOWER Services、および NGIPSv デバイスの場合は、従来のライセンスを使用する必要があります。従来のライセンスを使用するデバイスは、クラシック デバイスと呼ばれることもあります。

ライセンス付与された機能を使用する前に管理対象デバイスのクラシックライセンスを追加する必要があります。FMC の初期セットアップ中、FMC にデバイスを追加するとき、またはデバイスの追加後デバイスの一般的なプロパティを編集するときに、ライセンスを追加することができます。

FMC の初期セットアップ時にクラシックライセンスを追加するには、（任意）初期セットアップ時のクラシックライセンスの追加（バージョン 6.2 ～ 6.4）（35 ページ）の手順に従ってください。初期セットアップの完了後にクラシックライセンスを追加することもできます（クラシックライセンスの設定（41 ページ）を参照）。

- FTD の物理デバイスと仮想デバイスの場合、スマート ライセンスを使用する必要があります。

  Cisco スマート ソフトウェア ライセンシングを使用するデバイスを管理する予定がある場合は、初期セットアップの完了後にスマートライセンスを追加する必要があります（スマート ライセンスの設定（38 ページ）を参照）。

『Firepower Management Center 構成ガイド』は、クラシック ライセンスおよびスマート ライセンス、各クラスのライセンス タイプ、および展開全体でのライセンスの管理方法についての情報を提供します。

ステップ 10 **エンドユーザライセンス契約**をよくお読みください。条件を遵守することに同意する場合は、[エンドユーザライセンス契約を読んだうえで同意する（I have read and agree to the End User License Agreement）] チェックボックスをオンにします。

ステップ 11 指定した情報がすべて正しいことを確認して、[適用（Apply）] をクリックします。

FMC は、選択の内容に従って設定を適用し、ユーザを admin ユーザ（管理者ロールを持つ）として Web インターフェイスにログインさせ、サマリダッシュボードページを表示します。

（注） ネットワーク環境で NAT が使用されていると、ブラウザでの、初期セットアップページで設定されているアドレスによる FMC への到達の試みがタイムアウトする場合があります。この場合は、ブラウザのアドレス ウィンドウに正しいアドレスを入力して、再試行してください。

ステップ 12 イーサネットケーブルを使用してアプライアンスの管理インターフェイスに直接接続している場合は、[適用（Apply）] をクリックすると、IP アドレスが変更されているため、FMC から切断されます。コンピュータの接続を切断し、FMC の管理インターフェイスを管理ネットワークに接続してください。このガイドの残りの手順を完了するには、管理ネットワーク上のコンピュータのブラウザを使用して、先ほど設定した IP アドレスまたはホスト名で FMC GUI にアクセスします。

ステップ 13 Message Center の [タスク（Tasks）] タブのステータスをモニタすることによって、初期セットアップが成功したことを確認します。

次のタスク

- FMC 管理設定の構成（35 ページ）で説明されているアクティビティを実行します。

- 必要に応じて、シリアル アクセスまたは Lights-Out Management（LOM）アクセス用に FMC を設定します。FMC の代替アクセスのセットアップ （49 ページ）を参照してください。

（任意）初期セットアップ時のクラシックライセンスの追加（バージョン 6.2 ～ 6.4）

FMC を使用して 7000 および 8000 シリーズ、ASA with FirePOWER Services、および NGIPSv のクラシック ライセンスを管理します。

（注） ライセンス付与された機能を使用する前に管理対象デバイスのクラシック ライセンスを有効にする必要があります。FMC の初期セットアップ時の、FMC にデバイスを追加するとき、またはデバイスを追加した後にデバイスの一般的なプロパティを編集するときに、ライセンスを有効にすることができます（以下の手順を使用します）。

始める前に

クラシック ライセンスを FMC に追加する前に、ライセンスの購入時にシスコから製品認証キー（PAK）が提供されていることを確認してください。レガシーの、以前のシスコのライセンスの場合は、Cisco TAC に問い合わせてください。

手順

ステップ 1 初期セットアップ ページの [ライセンス設定（License Settings）] セクションから、シャーシのライセンス キーを取得します。

ライセンス キーは明確にラベル付けされます（たとえば、66:18:E7:6E:D9:93:35）。

ステップ 2 ライセンスを取得するには https://www.cisco.com/go/license/ に移動します。そこで、ライセンス キー（たとえば、66:18:E7:6E:D9:93:35）と PAK の入力が求められます。

（注） 追加のライセンスを発注したら、そのライセンスに対してカンマで区切った PAK を同時に入力することができます。

ステップ 3 画面の指示に従ってライセンスを生成します。ライセンスは電子メールで送信されます。

ステップ 4 検証ボックスのライセンスを貼り付けて、[追加/確認（Add/Verify）] をクリックします。

FMC 管理設定の構成

FMC の初期セットアップ手順が完了し、正常にセットアップされたことを確認したら、展開の管理を容易にするためのさまざまな管理タスクを実行することをお勧めします。また、ライセンスの取得など、初期セットアップで省略したタスクも完了する必要があります。デフォル

トの**管理者**アカウントまたは管理者アクセス権を持つ別のアカウントを使用して、これらの設定を確立します。

以下のセクションで説明するタスクの詳細、および展開の設定を開始する方法の詳細については、ご使用のソフトウェアバージョンに対応する『Firepower Management Center コンフィギュレーションガイド』を参照してください。

FMC の Web インターフェイスへの管理者としてのログイン

初期設定を実行するためにまだ FMC の Web インターフェイスにログインしていない場合は、FMC の管理設定を指定するためにログインする必要があります。デフォルトの **admin** アカウントを使用するか、管理者アクセス権を持つアカウントを使用します（すでに追加のユーザアカウントを作成している場合）。

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

複数の FMC が同じ IP アドレスを共有し、ポート番号によって区別される NAT 環境では、次のようになります。

- 各 FMC が一度にサポートできるログイン セッションは 1 つだけです。
- 異なる FMC にアクセスするには、ログインごとに別のブラウザ（Firefox や Chrome など）を使用するか、ブラウザをシークレットモードまたはプライベートモードに設定します。

手順

ステップ 1 ブラウザで **https://***ipaddress_or_hostname/* に移動します。ここで、*ipaddress* または *hostname* は使用している FMC に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックします。

個別のユーザアカウントの作成

初期設定が完了した時点で、システム上の唯一の Web インターフェイスのユーザは、管理者ロールとアクセス権を持つ **admin** ユーザです。その役割を持つユーザはシステムへのすべてのメニューと設定にアクセスできます。セキュリティおよび監査上の理由から、**admin** アカウント（および Administrator ロール）の使用を制限することをお勧めします。

（注） シェルによる FMC へのアクセスと Web インターフェイスによる FMC へのアクセスのための **admin** アカウントは同じではないため、異なるパスワードを使用できます。

システムには、Webインターフェイスを使用してさまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。システムを使用する各ユーザに対して個別のアカウントを作成すると、各ユーザによって行われたアクションと変更を組織で監査できるほか、各ユーザに関連付けられたユーザアクセスロールを制限することができます。これは、ほとんどの設定および分析タスクを実行する FMC で特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベントデータにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。ユーザロールの説明については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

外部認証されたユーザアカウントまたはマルチドメイン展開のユーザアカウントについては、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

手順

ステップ 1 **[System]** > **[Users]**を選択します。

ステップ 2 [ユーザ（Users）] タブで、[ユーザの作成（Create User）] をクリックします。

ステップ 3 [ユーザ名（User Name）] を入力し、ユーザアカウントの特性に関する値を入力または選択します。

ステップ 4 [**保存（Save**）] をクリックします。

時刻設定値の設定

FirePOWER システムを正常に動作させるには、FMC とその管理対象デバイスのシステム時刻を同期させることが不可欠です。FMC の初期設定時にネットワーク内で NTP サーバを指定することをお勧めしますが、指定しなかった場合は、初期設定の完了後に NTP サーバを追加できます。

FMC が NTP サーバに到達できない場合は、Firepower 展開の時間を設定する別の方法について、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

手順

ステップ 1 **[System]** > **[Configuration]** > **[Time Synchronization]**を選択します。

ステップ 2 [NTPを使用して時間を提供（Serve Time via NTP）] オプションを無効にします。

ステップ 3 [マイクロックの設定（Set My Clock）] オプションの場合、[NTP経由（Via NTP）] を選択します。

ステップ 4 バージョン 6.2 ー 6.4 の場合：[追加（Add）] をクリックし、FMC からアクセス可能な NTP サーバのホスト名または IP アドレスを入力します。次に、[保存（Save）] をクリックします。

バージョン 6.5 以降の場合：[追加（Add）] をクリックし、FMC からアクセス可能な NTP サーバのホスト名または IP アドレスを入力します。その後、[追加（Add）]、[保存（Save）] の順にクリックします。

スマート ライセンスの設定

FMC 自体にはライセンスは必要ありませんが、Firepower Threat Defense デバイスを管理する予定である場合は、スマートアカウントを作成し（まだ持っていない場合）、脅威とマルウェアの検出および URL フィルタリング機能をサポートするために必要なスマートライセンスを購入する必要があります。参考 Web サイト https://software.cisco.com/smartaccounts/setup#accountcreation-account。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts.html を参照してください。

FTD デバイスには、次のことを可能にする基本ライセンスが付属しています。

- スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するように FTD デバイスを設定する
- FTD デバイスをハイアベイラビリティペアとして設定する
- Firepower 9300 シャーシ内のクラスタとしてセキュリティ モジュールを設定する（シャーシ内クラスタリング）
- Firepower Threat Defense を実行している Firepower 9300 または Firepower 4100 シリーズ デバイスをクラスタとして設定する（シャーシ間クラスタリング）
- アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装する

脅威とマルウェアの検出および URL のフィルタリング機能には追加のオプション ライセンスが必要です。展開を計画する際は、FMC が管理する FTD デバイスの数と、それぞれでライセンスが必要な機能を決定してください。

（注） このドキュメントでは、スマートライセンスの効率化された設定手順を示します。これは、このプロセスにすでに慣れている場合に役立ちます。Firepower およびスマートライセンスを使用し慣れていない場合や、エアギャップ展開、ハイアベイラビリティを使用するデバイス、クラスタ化されたデバイス、マルチテナント、またはエクスポート制御機能のためにスマートライセンスを設定する必要がある場合は、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

Firepower バージョン 6.5 以降の場合：すでにスマートアカウントを持っており、ライセンスを購入済みで、スマートライセンスに精通している場合は、初期設定ウィザードの完了後にシステムによって表示されるダイアログボックスを使用できます。または、ウィザードの完了後に、バージョン 6.2 ー 6.4 と同じライセンス設定プロセスを使用できます。

Firepower バージョン 6.2 ～ 6.4 の場合：初期セットアップの完了後にスマートライセンスを追加します。ライセンスごとに、次の手順を実行してください。

- Cisco Smart Software Manager（CSSM）からスマートライセンス用の製品ライセンス登録トークンを取得します。デバイスで使用可能なライセンス PID を確認するには、そのデバイスのスタートアップガイドを参照してください。
- トークンを使用して FMC を CSSM に登録します。
- 管理対象の FTD を FMC に追加する場合、デバイスにライセンスを割り当てます。

スマート ライセンス用の製品ライセンス登録トークンの取得

始める前に

- スマートアカウントを作成し、必要なタイプのライセンスを必要な数購入します。参考 Web サイト https://software.cisco.com/smartaccounts/setup#accountcreation-account。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts.html を参照してください。
- ライセンスがスマートアカウントに表示されていることを確認します。
- Cisco Smart Software Manager にサインインするためのクレデンシャルがあることを確認します。

手順

ステップ 1 https://software.cisco.comに進みます。

ステップ 2 （[ライセンス（License）] セクションで）[スマート ソフトウェア ライセンシング（Smart Software Licensing）] をクリックします。

ステップ 3 Cisco Smart Software Manager にサインインします。

ステップ 4 [インベントリ（Inventory）] をクリックします。

ステップ 5 [General] をクリックします。

ステップ 6 [新規トークン（New Token）] をクリックします。

ステップ 7 [説明（Description）] に、このトークンを使用する Firepower Management Center を一意かつ明確に特定する名前を入力します。

ステップ 8 365 日以内の期限を入力します。この期限により、トークンを Firepower Management Center に登録しておく必要がある期間が決まります

ステップ 9 [トークンの作成（Create Token）] をクリックします。

ステップ 10 リストで新しいトークンを見つけて、[アクション（Actions）] をクリックして、[コピー（Copy）] または [ダウンロード（Download）] を選択します。

ステップ 11 Firepower Management Center にトークンを入力する準備ができるまで、トークンを安全な場所に保存します。

次のタスク

「スマート ライセンスの登録 （40 ページ）」に進みます。

スマート ライセンスの登録

始める前に

- FMC が tools.cisco.com:443 で Cisco Smart Software Manager（CSSM）サーバにアクセスできることを確認します。
- FMC が NTP サーバとの接続を確立していることを確認します。登録時に、NTP サーバと Cisco Smart Software Manager の間でキー交換が実行されるため、適切な登録には時刻の同期が必要です。

  Firepower 4100/9300 シャーシに FTD を展開する場合は、FMC と同じ NTP サーバをシャーシに使用して Firepower シャーシに NTP を設定する必要があります。
- CSSMから必要な製品ライセンス登録トークンを生成します。「スマート ライセンス用の製品ライセンス登録トークンの取得 （39 ページ）」を参照してください（すべての前提条件を含む）。FMC にアクセスするマシンからトークンにアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** > [登録（Registration）] を選択します。

ステップ 2 CSSM から生成されたトークンを [製品インスタンス登録トークン（Product Instance Registration Token）] フィールドに貼り付けます。テキストの前後にスペースや空白の行がないことを確認します。

ステップ 3 **バージョン 6.2.3 以降の場合**：使用状況データをシスコに送信するかどうかを決定します。

- [Cisco Success Networkの有効化（Enable Cisco Success Network）] は、デフォルトで有効です。シスコによって収集されるデータの種類を表示するには、[サンプルデータ（sample data）] をクリックします。Cisco Success Network の情報ブロックを読むと、判断に役立ちます。
- **バージョン 6.5 以降の場合**：[Cisco Proactive Support の有効化（Enable Cisco Proactive Support）] は、デフォルトで有効になっています。シスコが収集するデータの種類は、このチェック ボックスの上に表示されているリンクで確認できます。[Cisco Support Diagnostics] 情報ブロックを読むと、判断に役立ちます。

  （注）
  - 有効にすると、Cisco Support Diagnostics は、次の同期サイクルで FTD デバイスで有効になります。FMC と FTD との同期は、30 分ごとに 1 回実行されます。
  - 有効にすると、今後この FMC に登録される新しい FTD では、Cisco Support Diagnostics が自動的に有効になります。

ステップ 4 [Apply Changes] をクリックします。

次のタスク

FTD 管理対象デバイスを FMC に追加する場合、適切なライセンスを選択してデバイスに適用します。FMC への管理対象デバイスの追加 （47 ページ） を参照してください。

クラシックライセンスの設定

FMC 自体にはライセンスは必要ありませんが、7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスについては、これらのデバイスでライセンス付与された機能を使用するために、クラシックライセンスを購入して有効にする必要があります。従来のライセンスを使用するデバイスは、クラシック デバイスと呼ばれることもあります。

クラシックライセンスは、シスコの製品ライセンス登録ポータル（https://cisco.com/go/license）を使用して管理します。ポータルの使用方法については、https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart を参照してください。これらのリンクにアクセスするには、アカウントのクレデンシャルが必要です。

（注） このドキュメントでは、クラシックライセンスの効率化された設定手順を示します。これは、このプロセスにすでに慣れている場合に役立ちます。Firepower およびクラシックライセンスを使用し慣れていない場合や、エアギャップ展開またはマルチテナントを使用した展開のためにクラシックライセンスを設定する必要がある場合は、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

システムで Firepower バージョン 6.5 以降を使用している場合、FMC の初期設定ウィザードの完了後に管理対象のクラシックデバイスのライセンスを FMC に追加する必要があります。これについては、クラシックライセンスの生成と Firepower Management Center への追加 （42 ページ）またはご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

システムが 6.2 ～ 6.4 を実行している場合、FMC の初期セットアッププロセスを開始する前にクラシックライセンスを購入し、ライセンスを FMC に追加（（任意）初期セットアップ時のクラシックライセンスの追加（バージョン 6.2 ～ 6.4） （35 ページ）を参照）することをお勧めします。初期セットアップの完了後にライセンスを追加する場合は、クラシックライセンスの生成と Firepower Management Center への追加 （42 ページ）またはご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドに記載されている手順に従ってください。

FMC の初期セットアップ時にクラシックライセンスを追加しない場合は、FMC の初期セットアップの完了後に管理対象のクラシックデバイスのライセンスを追加する必要があります。ライセンスを追加するのが FMC の初期セットアッププロセス中かその後であるかに関係なく、管理対象のクラシックデバイスを FMC に登録するときに、またはデバイスの全般プロパティを編集してそれらを FMC に登録した後に、それらにライセンスを割り当てることができます。

詳細については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

初期セットアップの完了後にクラシックライセンスを追加するには、ライセンスごとに次の手順を実行します。

- ライセンスを生成し、それを FMC に追加します。
- ライセンスを管理対象のクラシックデバイスに割り当てます。

クラシックライセンスの生成と Firepower Management Center への追加

始める前に

- シスコの製品ライセンス登録ポータル（https://cisco.com/go/license）にアクセスできることを確認してください。
- ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドでクラシックライセンスのタイプに関する情報を確認して、必要なクラシックライセンスのタイプと、使用する予定の機能のサービスサブスクリプションを購入する必要もあるかどうかを判断してください。
- ライセンスごとに製品認証キー（PAK）を購入し、必要に応じてサービスサブスクリプションを購入します。

手順

ステップ 1 **[System]** > **[Licenses]** > **[Classic Licenses]** > [新しいライセンスの追加（Add New License）] を選択します。

ステップ 2 [機能ライセンスの追加（Add Feature License）] ダイアログの上部にある [ライセンス キー（License Key）] フィールドの値をメモします。

ステップ 3 [ライセンス取得（Get License）] をクリックして、Cisco ライセンス登録ポータルを開きます。

ステップ 4 ライセンス登録ポータルで、PAK からライセンスを生成します。詳細については、https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Home を参照してください。この手順では、ライセンスの購入時に入手した PAK と、FMC からのライセンスキーが必要です。

ステップ 5 ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。

重要 ポータルまたは電子メール メッセージ内のライセンス テキスト ブロックには、複数のライセンスを含めることができます。各ライセンスは、BEGIN LICENSE 行と END LICENSE 行で囲まれます。一度に 1 つのライセンスしかコピーして貼り付けることができません。

ステップ 6 FMC の Web インターフェイスの [機能ライセンスの追加（Add Feature License）] ページに戻ります。

ステップ 7 [ライセンス（License）] フィールドにライセンス テキストを貼り付けます。

ステップ 8 [ライセンスの検証（Verify License）] をクリックします。

ステップ 9 [ライセンスの提出（Submit License）] をクリックします。

次のタスク

Firepower クラシック管理対象デバイスを FMC に追加する場合、適切なライセンスを選択してデバイスに適用します。FMC への管理対象デバイスの追加 （47 ページ） を参照してください。

システム更新とバックアップのスケジュール

Firepower バージョン 6.5 以降の場合：

初期設定プロセスの一環として、FMC によって次の自動更新が確立されます。

- GeoDB の週次の更新
- FMC ソフトウェア更新の週次のダウンロード（これらの更新のインストールはユーザが行う。詳細については、『Cisco Firepower Management Center Upgrade Guide』を参照）
- FMC 設定の週次のバックアップ

Firepower バージョン 6.6 以降の場合：

初期設定プロセスの一環として、FMC によって次の自動更新が追加的に確立されます。

- 脆弱性データベースの 1 回限りの更新
- 侵入ルールの日次の更新

これらの自動更新については、バージョン 6.5 以降の自動初期設定の確認 （22 ページ）で説明しています。これらの設定のステータスは、Web インターフェイスのメッセージセンターを使用して確認できます。これらの更新のいずれかの設定が失敗する場合は、システムを最新の状態に保つために、それらの更新を自分で設定する（以降の項を参照）ことを強くお勧めします。VDB 更新の場合は、最新の VDB 更新だけがシステムによって自動的にインストールされます。定期的な自動 VDB 更新をスケジュールすることをお勧めします。

Firepower バージョン 6.2 ～ 6.4 の場合：

FMC の初期設定が完了したら、システムを最新の状態に保つために、更新アクティビティを設定する（以降の項を参照）ことを強くお勧めします。

GeoDB の週次更新のスケジュール

シスコ地理位置情報データベース（GeoDB）は、ルーティング可能な IP アドレスと関連付けられた地理的データ（国、都市、座標など）および接続関連のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。

国や大陸以外の位置情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。シスコでは、GeoDB の定期的な更新を提供しています。GeoDB ルックアップの精度を最適化するために、常にシステムで最新の GeoDB 更新を使用することをお勧めします。

始める前に

FMC でインターネットにアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）]** を選択します。

ステップ 2 [位置情報の定期更新（Recurring Geolocation Updates）] で、[サポートサイトからの定期的な週次更新を有効にする（Enable Recurring Weekly Updates from the Support Site）] をオンにします。

ステップ 3 [開始時刻の更新（Update Start Time）] を指定します。

ステップ 4 **[保存（Save）]** をクリックします。

ソフトウェアアップデートの週次スケジュール

これらの手順を使用して、スケジュールされた毎週のタスクを作成し、シスコから最新の FMC ソフトウェアアップデートを自動的にダウンロードします。FMC ソフトウェアを最新の状態に保つことで、最適なパフォーマンスが保証されます。ダウンロードしたアップデートのインストールはお客様の責任で行います。インストールの手順については、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

始める前に

FMC でインターネットにアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択し、[タスクの追加（Add Task）] をクリックします。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 3 定期タスクをスケジュールすることを指定し、[Start On]、[Repeat Every]、[Run At]、および [Repeat On]フィールドに適切な値を選択して、週次スケジュールを設定します。

ステップ 4 [ジョブ名（Job Name）] にジョブ名を入力し、[アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

FMC 設定の週次バックアップのスケジュール

破滅的なシステム障害が発生した場合に FMC の設定を簡単に復元できるように、定期的なシステムバックアップをスケジュールすることをお勧めします。

始める前に

FMC でインターネットにアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択し、[バックアッププロファイル（Backup Profiles）] をクリックします。

ステップ 2 [プロファイルの作成（Create Profile）] をクリックします。

ステップ 3 [名前（Name）] を入力し、[バックアップ設定（Back Up Configuration）] を選択して、[新規保存（Save As New）] をクリックします。

ステップ 4 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択し、[タスクの追加（Add Task）] をクリックします。

ステップ 5 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 6 定期タスクをスケジュールすることを指定し、[開始日（Start On）]、[繰り返し設定（Repeat Every）]、[実行時刻（Run At）]、および [繰り返し間隔（Repeat On）] フィールドに適切な値を選択して、週次スケジュールを確立します。

ステップ 7 ジョブ名を入力し、[バックアップのタイプ（Backup Type）] の横にある [管理センター（Management Center）] を選択します。

ステップ 8 [バックアッププロファイル（Backup Profile）] で、ステップ 3 で作成したプロファイルを選択します。

ステップ 9 **[保存（Save）]** をクリックします。

定期的な侵入ルール更新の設定

新しい脆弱性が明らかになるのに伴い、Cisco Talos Intelligence Group（Talos）は侵入ルールの更新をリリースします。これらの更新を FMC にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装できます。それらの更新は、侵入ルール、プリプロセッサルール、およびルールを使用するポリシーに影響を及ぼします。侵入ルール更新は更新を累積されていくものなので、常に最新の更新をインポートすることをお勧めします。

始める前に

FMC でインターネットにアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]**を選択します。

ステップ 2 [サポートサイトからの定期的なルール更新のインポートを有効化（Enable Recurring Rule Update Imports from the Support Site）] チェックボックスをオンにします。

ステップ 3 [インポート頻度（Import Frequency）] で、インポート頻度を決定する値を選択します。

ステップ 4 [ルール更新の完了後、更新されたポリシーを管理対象デバイスに展開する（Deploy updated policies to targeted devices after rule update completes）] チェックボックスをオンにします。

ステップ 5 [**保存（Save）**] をクリックします。

VDB のダウンロードと更新のスケジュール

シスコ脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

最新の VDB 更新の定期的な自動ダウンロードとインストールをスケジュールするには、以下の手順を使用します。Cisco Talos Intelligence Group（Talos） は、VDB の定期的な更新を 1 日に 1 回以上発行することはありません。常に FMC で最新の VDB 更新を維持することを強くお勧めします。

VDB 更新を自動化する場合、次に示す 2 つの別個の手順を自動化する必要があります。

- VDB 更新をダウンロードします。
- VDB 更新をインストールします。

プロセスを完了させるには、タスクとタスクの間に十分な時間を確保してください。たとえば、更新のインストール タスクをスケジュールした場合、更新がまだ完全にダウンロードされていないと、インストール タスクは正しく実行されません。ただし、スケジュール済みインストール タスクが毎日繰り返される場合は、翌日のタスク実行時に、ダウンロード済みの VDB 更新がインストールされます。

（注） 初期設定の一環として、FMCはシスコのサポートサイトから最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。これは 1 回限りの操作です。Web インターフェイスのメッセージセンターを使用して、この更新のステータスを確認できます。システムを最新の状態に保つために、 FMCがインターネットにアクセスできる場合は、

このセクション。

注意 VDB 更新に管理対象デバイスに適用される変更が含まれている場合、新しい VBD 更新をインストールした後の最初の手動またはスケジュール済み展開により、検査なしに少数のパケットがドロップする可能性があります。また、一部の設定を展開すると Snort プロセスが再起動され、トラフィックの検査が中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

始める前に

FMC でインターネットにアクセスできることを確認します。

手順

ステップ 1 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択し、[タスクの追加（Add Task）] をクリックします。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 3 定期タスクをスケジュールすることを指定し、[Start On]、[Repeat Every]、[Run At]、および [Repeat On]フィールドに適切な値を選択して、週次スケジュールを設定します。

ステップ 4 [ジョブ名（Job Name）] にジョブ名を入力し、[アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** を選択し、[タスクの追加（Add Task）] をクリックします。

ステップ 7 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 8 定期タスクをスケジュールすることを指定し、[開始日（Start On）]、[繰り返し設定（Repeat Every）]、[実行時刻（Run At）]、および [繰り返し間隔（Repeat On）] フィールドに適切な値を選択して、週次スケジュールを確立します。

ステップ 9 [ジョブ名（Job Name）] にジョブ名を入力し、[アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 10 **[保存（Save）]** をクリックします。

FMC への管理対象デバイスの追加

マルチテナント、クラスタ、またはハイアベイラビリティを含まない単純な展開を確立するには、管理対象デバイスごとに、次の手順を実行します。これらの機能のいずれかを使用して展

開を設定するには、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

始める前に

- デバイス固有のセットアップアクティビティを実行し、リモート管理用にデバイスを設定します（デバイスのスタートアップガイドを参照）。

  重要 必ず、デバイスに使用する登録キーをメモしておいてください。

- NAT を使用する環境の場合は、デバイスのセットアップ時に使用した NAT ID をメモしておいてください。
- DNS を使用する環境の場合は、デバイスの有効な IP アドレスに解決されるホスト名をメモしておいてください。DHCP を使用して IP アドレスを割り当てる環境の場合は、IP アドレスではなくホスト名を使用してデバイスを識別してください。
- DNS を使用しない環境の場合は、デバイスの IP アドレスが必要です。
- 管理対象デバイスに必要なライセンスを特定し、それらを FMC に追加します。これらのライセンスは、管理対象デバイスを FMC に追加するプロセスにおいて、管理対象デバイスに追加します。スマート ライセンスの設定 （38 ページ）およびクラシックライセンスの設定 （41 ページ）を参照してください。
- 管理対象デバイスを FMC に追加する際に、管理対象デバイスにアクセス コントロール ポリシーを割り当てる必要があります。次の手順には、この目的のための基本的なアクセス コントロール ポリシーを確立する手順が含まれています。

手順

ステップ 1 **[Devices]** > **[Device Management]** > [追加（Add）] > [デバイスの追加（Add Device）] を選択します。

ステップ 2 [ホスト（Host）] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。

デバイスのホスト名は、完全修飾名またはローカル DNS で有効な IP アドレスに解決される名前です。ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、FMC の管理対象としてデバイスを設定するときに FMC の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要がない場合があります。

ステップ 3 [表示名（Display Name）] フィールドに、FMC の Web インターフェイスでのデバイスの表示名を入力します。

ステップ 4 [登録キー（Registration Key）] フィールドに、FMC の管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します（この登録キーは、この FMC をデバイスで最初に識別したときに作成した 1 限り使用可能な共有シークレット）。

ステップ 5 [アクセス コントロール ポリシー（Access Control Policy）] で初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。これは、後で、トラフィックを許可するように変更できます。詳細については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。詳細については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。この障害の原因を解決した後、デバイスに手作業で設定を行います。

ステップ 6 デバイスに適用するライセンスを選択します。

クラシックデバイスの場合は、制御、マルウェア、URL フィルタリングライセンスに保護ライセンスが必要であることに注意してください。

ステップ 7 デバイスの設定時に、NAT ID を使用した場合、[詳細（Advanced）] セクションを展開し、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

ステップ 8 [登録（Register）] をクリックします。

FMC がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

FMC の代替アクセスのセットアップ

初期セットアッププロセスが完了したら、次のいずれかを実行して、FMC への別のアクセス方法を確立できます。

- ローカル コンピュータからシリアル ポートへの直接アクセス用に FMC をセットアップできます。
- デフォルト（eth0）の管理インターフェイスでの Serial over LAN（SoL）接続による Lights Out Management（LOM）アクセス用に FMC をセットアップできます。これにより、アプライアンスへの物理的なアクセスがなくても、限られた数のメンテナンス タスクを実行できます。

シリアル アクセスまたは LOM/SoL アクセス用に FMC を設定する前に、コンソール出力をシリアル ポートにリダイレクトすることを推奨します。

シリアル アクセスのセットアップ

始める前に

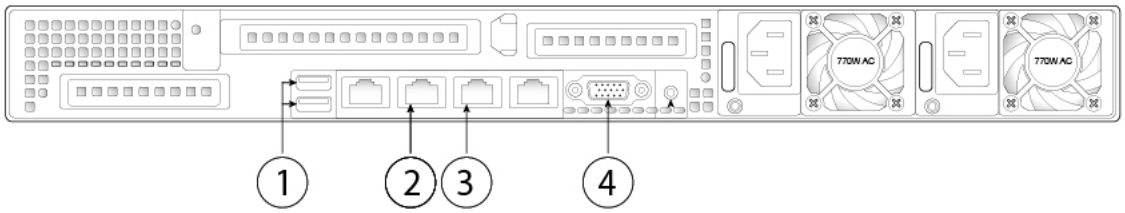
- ご使用のバージョンの Firepower に適した初期セットアッププロセスを完了します。
  - Firepower バージョン 6.5 以降については、バージョン 6.5 以降の FMC のインストール （7 ページ）を参照してください。
  - Firepowerバージョン 6.2 ー 6.4 については、ソフトウェアバージョン 6.2 ～ 6.4 の FMC のインストール （24 ページ）を参照してください。
- 端末エミュレーション ソフトウェア（HyperTerminal や XModem など）を入手し、FMC と通信するローカル コンピュータにインストールします。
- コンソール出力をシリアルポートにリダイレクトします。「コンソール出力のリダイレクト （54 ページ）」を参照してください。

手順

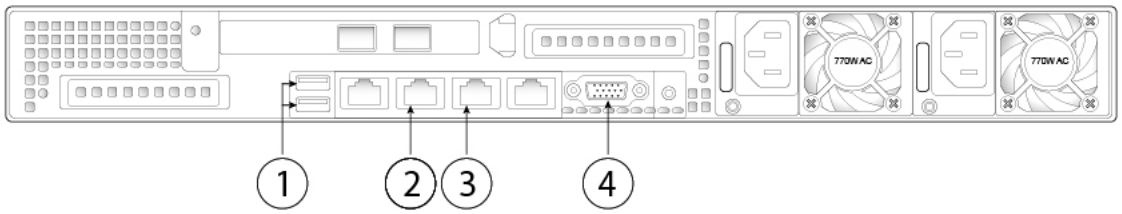
ステップ 1 FMC 背面パネルのシリアルポートを見つけます。

以下のモデルについては、図の項目 4 を使用してください。

- FMC 1000 背面パネル：



- FMC 2500 および FMC 4500 背面パネル：



ステップ 2 アプライアンスに付属の RJ-45 to DP9 コンソール ケーブル（シスコ製品番号 72-3383-XX）を使用して、ローカル コンピュータを FMC のシリアル ポートに接続します。

ステップ 3 ローカル コンピュータ上の端末エミュレーション ソフトウェア（HyperTerminal や XModem など）を使用して FMC と通信します。端末エミュレータを 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定します。

Lights-Out Management のセットアップ

Lights-Out Management（LOM）機能では、Serial over LAN（SoL）接続を使用して、Firepower Management Center で限られたアクションを実行できます。LOM では、帯域外管理接続で CLI を使用して、シャーシのシリアル番号の表示などのタスクを実行したり、ファンの速度や温度などの状態を監視したりします。Lights-Out Management は、デフォルト（`eth0`）の管理インターフェイスでのみ使用できることに注意してください。

Firepower Management Center を工場出荷時設定に復元する必要があるが、アプライアンスに物理的にアクセスできない場合は、Lights-Out Management（LOM）を使用して復元プロセスを実行できます。

注意 バージョン 6.3 以降の場合は、復元プロセスによってデバイスの LOM 設定がリセットされます。LOM を使用して、6.3 以降のバージョンに新しく復元されたアプライアンスにアクセスすることはできません。LOM を使用して、デバイスをバージョン 6.3 以降の工場出荷時設定に復元する場合、アプライアンスに物理的にアクセスできない場合は、ライセンス設定とネットワーク設定を削除すると、復元後にアプライアンスにアクセスできなくなります。

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

照明の管理の詳細については、ご使用のバージョンのの『Firepower Management Center Configuration Guide』の「Remote Console Access management」を参照してください。

始める前に

- インテリジェントプラットフォーム管理インターフェイス（IMPI）ユーティリティをローカル コンピュータにインストールします。詳細については、IPMI ユーティリティのインストール （52 ページ）を参照してください。
- IPMI ツールを使用してアプライアンスにアクセスするために必要なコマンドを確認します。詳細については、LOM コマンド （52 ページ）を参照してください。
- コンソール出力をシリアルポートにリダイレクトします。「コンソール出力のリダイレクト （54 ページ）」を参照してください。

手順

ステップ 1 アプライアンスの LOM を有効にします。Lights-Out Management の有効化 （53 ページ）を参照してください。

ステップ 2 この機能を使用するユーザの LOM を有効にします。Lights-Out Management ユーザの有効化 （54 ページ）を参照してください。

ステップ 3 アプライアンスにアクセスするには、サードパーティ製の IPMI ユーティリティを使用します。

IPMI ユーティリティのインストール

コンピュータ上のサードパーティの IPMI ユーティリティを使用して、アプライアンスへの SoL 接続を作成できます。IPMItool は多くの Linux ディストリビューションの標準ツールですが、Mac システムと Windows システムではユーティリティをインストールする必要があります。

Mac OS が稼働しているコンピュータでは、IPMItool をインストールします。最初に、Apple の xCode 開発ツール パッケージが Mac にインストールされていることを確認します。コマンドライン開発のためのオプション コンポーネント（新しいバージョンでは「UNIX Development」および「System Tools」、古いバージョンでは「Command Line Support」）がインストールされていることを確認します。最後に、MacPorts および IPMItool をインストールします。詳細については、検索エンジンを使用するか、次のサイトを参照してください：https://developer.apple.com/technologies/tools/ および http://www.macports.org/。

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

LOM コマンド

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

表 *1: LOM* コマンド構文

IPMItool（Linux/Mac）	**ipmiutil（Windows）**	**説明**
ipmitool	**ipmiutil**	IPMI ユーティリティを起動します。
適用対象外	**-V4**	ipmiutil のみ。LOM セッションで管理特権を有効にします。
-I lanplus	**-J3**	LOM セッションの暗号化を有効にします。
-H *IP_address*	**-N** *IP_address*	アプライアンスの管理インターフェイスの IP アドレスを指定します。

IPMItool（Linux/Mac）	ipmiutil（Windows）	説明
-U *username*	**-U *username***	承認済みLOMアカウントのユーザ名を指定します。
適用対象外（ログオン時に求められます）	**-P *password***	ipmiutil のみ。承認済み LOM アカウントのパスワードを指定します。
command	**command**	アプライアンスに対して発行するコマンド。コマンドを発行する場所は、ユーティリティによって異なります。 • IPMItool の場合は、最後に次のコマンドを入力します：**ipmitool -I lanplus -H** *IP_address* -U *username command* • ipmiutil の場合は、最初に次のコマンドを入力します：**ipmiutil** *command* **-V4 -J3 -N** *IP_address* **-U** *username* **-P** *password*

Firepowerシステムでサポートされている LOM コマンドの完全なリストについては、『Firepower Management Center Configuration Guide』の「 LOM Commands」を参照してください。

Lights-Out Management の有効化

手順

ステップ 1 FMC の Web インターフェイスで、**[System]** > **[Configuration]** を選択し、[コンソール設定（Console Configuration）] をクリックします。

ステップ 2 [コンソール（Console）] で、[物理シリアルポート（Physical Serial Port）] を選択します。

ステップ 3 必要な IPv4 設定を入力します。

- システムのアドレス構成（[DHCP] または [Manual（手動）]）を選択します。
- LOM に使用する IP アドレスを入力します。

  （注） LOM IP アドレスは、システムの管理インターフェイスの IP アドレスとは異なる必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

この機能を使用するユーザに対してLOM権限を明示的に付与する必要があります。Lights-Out Management ユーザの有効化 （54 ページ） を参照してください。

Lights-Out Management ユーザの有効化

始める前に

LOM ユーザは次の制限を満たしている必要があります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名に使用できるのは英数字 16 文字までです。LOM ユーザに対し、ハイフンやそれより長いユーザ名はサポートされていません。
- パスワードには、最大で 20 文字の英数字を使用できます。LOM ユーザに対し、これよりも長いパスワードはサポートされていません。ユーザの LOM パスワードは、そのユーザのシステム パスワードと同じです。
- FMC には、最大 13 人の LOM ユーザを設定できます。

手順

ステップ 1 FMC の Web インターフェイスで、**[System]** > **[Users]** を選択し、[ユーザ（Users）] タブで、既存のユーザを編集して LOM 許可を追加するか、またはアプライアンスへの LOM アクセスに使用する新規ユーザを作成します。

ステップ 2 [ユーザロールの設定（User Role Configuration）] で、まだオンになっていない場合は、[管理者（Administrator）] チェックボックスをオンにします。

ステップ 3 [Lights-Out Management へのアクセスを許可する（Allow Lights-Out Management Access）] チェックボックスをオンにし、変更を保存します。

コンソール出力のリダイレクト

デフォルトで、FMC は、初期化ステータスまたは *init* メッセージを VGA ポートに出力します。物理シリアル ポートまたは SOL を使用してコンソールにアクセスする必要がある場合、初期セットアップの完了後にコンソール出力をシリアルポートにリダイレクトすることを推奨します。これは、Web インターフェイスまたはシェルから実行できます。

Web インターフェイスによるコンソール出力のリダイレクト

始める前に

ご使用のバージョンの Firepower に適した初期セットアッププロセスを完了します。

- Firepower バージョン 6.5 以降については、バージョン 6.5 以降の FMC のインストール （7 ページ）を参照してください。
- Firepower バージョン 6.2 ～ 6.4 については、ソフトウェアバージョン 6.2 ～ 6.4 の FMC のインストール （24 ページ）を参照してください。

手順

ステップ 1 **[System]** > **[Configuration]**を選択します。

ステップ 2 [コンソール設定（Console Configuration）] を選択します。

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。
- アプライアンスのシリアルポートを使用するかLOM/SoL を使用する場合には、[物理シリアル ポート（Physical Serial Port）] を選択します。

ステップ 4 SoL を使用して LOM を設定するには、次の適切な IPv4 設定を入力します。

- アプライアンスのアドレス設定（[DHCP] または [Manual（手動）]）を選択します。
- LOM に使用する IP アドレスを入力します。

  （注） LOM IP アドレスは、システムの管理インターフェイスの IP アドレスとは異なる必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

ステップ 5 [保存（**Save**）] をクリックします。

シェルによるコンソール出力のリダイレクト

始める前に

ご使用のバージョンの Firepower に適した初期セットアッププロセスを完了します。

- Firepower バージョン 6.5 以降については、バージョン 6.5 以降の FMC のインストール （7 ページ）を参照してください。
- Firepowerバージョン 6.2 ～ 6.4 については、ソフトウェアバージョン 6.2 ～ 6.4 の FMC のインストール （24 ページ）を参照してください。

手順

ステップ 1 FMC CLI **管理者**認証情報を使用して、Firepower バージョンに適切なメソッドを使用して FMC の Linux シェルにアクセスします。「次での CLI または Linux シェルへのアクセス FMC （5 ページ）」を参照してください。

ステップ 2 プロンプトで、以下のコマンドのいずれかを入力して、コンソール出力を設定してください。

- コンソール メッセージを VGA ポートにダイレクトする場合：**sudo /usr/local/sf/bin/configure_console.sh vga**
- コンソール メッセージを物理シリアル ポートにダイレクトする場合：**sudo /usr/local/sf/bin/configure_console.sh serial**
- コンソール メッセージを SoL にダイレクトする場合（LOM 使用時）：**sudo /usr/local/sf/bin/configure_console.sh sol**

ステップ 3 変更を反映させるには、「**sudo reboot**」と入力してアプライアンスを再起動します。

FMC の事前設定

ステージングロケーション（複数のアプライアンスを事前設定またはステージングするための中央の場所）で、ターゲットロケーション（ステージングロケーション以外の任意のロケーション）に展開する FMC を事前設定することができます。

アプライアンスを事前設定してターゲット ロケーションに展開するには、以下の手順に従います。

1. ステージング ロケーションでデバイスにシステムをインストールします。
2. アプライアンスをシャットダウンし、ターゲット ロケーションに移送します。
3. アプライアンスをターゲットロケーションに展開します。

（注） すべての梱包材を保管し、アプライアンスを再梱包するときにはすべての参考資料と電源コードを同梱します。

必須の事前設定の情報

アプライアンスを事前設定する前に、ステージング ロケーションとターゲット ロケーションのネットワーク設定情報、ライセンス情報、その他の関連情報を収集します。

（注） ステージング ロケーションとターゲット ロケーションでこの情報を管理するためのスプレッドシートを作成すると便利です。

初期設定時に、アプライアンスをネットワークに接続してシステムをインストールするための十分な情報を使用してアプライアンスを設定します。

アプライアンスを事前設定するには、最低でも以下の情報が必要です。

- 新しいパスワード（初期設定時にパスワードを変更する必要があります）
- アプライアンスのホスト名
- アプライアンスのドメイン名
- アプライアンスの IP 管理アドレス
- ターゲット ロケーションのアプライアンスのネットワーク マスク
- ターゲット ロケーションのアプライアンスのデフォルト ゲートウェイ
- ステージング ロケーション（またはターゲット ロケーションにアクセス可能な場合はターゲット ロケーション）の DNS サーバの IP アドレス
- ステージング ロケーション（またはターゲット ロケーションにアクセス可能な場合はターゲット ロケーション）の NTP サーバの IP アドレス

オプションの事前設定の情報

次を含むいくつかのデフォルト設定を変更できます。

- 時間帯（アプライアンスの時間を手動で設定する場合）
- 自動バックアップに使用するリモート ストレージ ロケーション
- LOM を有効にする LOM IP アドレス

時間管理の事前設定

手順

ステップ 1 物理的 NTP サーバと時間を同期させます。

ステップ 2 次のいずれかの方法を使用して、DNS サーバと NTP サーバの IP アドレスを設定します。

- ステージング ロケーションのネットワークからターゲット ロケーションの DNS サーバおよび NTP サーバにアクセスできる場合は、ターゲット ロケーションの DNS サーバおよび NTP サーバの IP アドレスを使用します。
- ステージング ロケーションのネットワークからターゲット ロケーションの DNS サーバおよび NTP サーバにアクセスできない場合は、ステージング ロケーションの情報を使用し、ターゲット ロケーションでリセットします。

ステップ 3 NTP を使用する代わりに、アプライアンスの時間を手動で設定する場合は、ターゲット展開環境の時間帯を使用します。詳細については、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

システムのインストール

手順

ステップ 1 ご使用のバージョンに適したインストール手順を使用します。

- Firepower バージョン 6.5 以降については、次を参照してください：バージョン 6.5 以降の FMC のインストール （7 ページ）
- Firepowerバージョン 6.2 ー 6.4 については、ソフトウェアバージョン 6.2 ～ 6.4 の FMC のインストール （24 ページ）を参照してください。

ステップ 2 シャーシのインストールに関する詳細については、『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』を参照してください。

Firepower Management Center の移送の準備

手順

ステップ 1 FMC の電源を安全に切ります。詳細については、『Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide』を参照してください。

ステップ 2 アプライアンスの移送の準備が完了したことを確認します。詳細については、移送に関する考慮事項 （58 ページ）を参照してください。

移送に関する考慮事項

ターゲット ロケーションへの移送に向けてアプライアンスを準備するには、アプライアンスの電源を安全にオフにし、再梱包する必要があります。次の考慮事項に注意します。

- アプライアンスの再梱包には元の梱包材を使用します。
- アプライアンスに付属のすべての参考資料および電源コードを同梱します。
- 新しいパスワードや検出モードを含むすべての設定情報をターゲット ロケーションに提供します。

アプライアンスの事前設定のトラブルシューティング

アプライアンスがターゲットでの配布用に適切に設定されている場合、その FMC は追加の設定なしでインストールして配布できます。

アプライアンスへのログインに問題がある場合、事前設定にエラーがある可能性があります。次のトラブルシューティング手順を試行してください。

- すべての電源コードおよび通信ケーブルがアプライアンスに正しく接続されていることを確認します。
- アプライアンスの現行パスワードがわかっていることを確認します。ステージングロケーションでの初期設定時に、パスワードの変更が求められます。新しいパスワードについては、ステージング ロケーションで提供される設定情報を参照してください。
- ネットワーク設定が正しいことを確認します。詳細については、ご使用のバージョンに適した初期セットアップ手順を参照してください。
  - Firepower バージョン 6.5 以降については、Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降）（14 ページ）またはCLI（バージョン 6.5 以降）を使用した初期設定（19 ページ）を参照してください。
  - Firepowerバージョン 6.2 ー 6.4 については、（任意）ソフトウェアバージョン 6.2 ー 6.4 用の物理接続を使用したネットワーク設定の指定（30 ページ）またはソフトウェアバージョン 6.2 ー 6.4 の Web インターフェイスを使用した FMC 初期セットアップ（31 ページ）を参照してください。
- 正しい通信ポートが正しく動作していることを確認します。ファイアウォールポートの管理と必要なオープンポートについては、ご使用のバージョンの Firepower Management Center のコンフィギュレーション ガイドを参照してください。

それでも問題が解決しない場合は、IT 部門に連絡してください。

システム復元ユーティリティを使用した Firepower Management Center の管理

FMC には、次のようないくつかのメンテナンス機能を実行するために使用できるシステム復元ユーティリティがあります。

- シスコがサポートサイトで提供している ISO イメージを使用して FMC を工場出荷時の設定に復元します。復元プロセスについて（61 ページ）を参照してください。
- FMC の一連の設定を保存するか、以前に保存した FMC の設定をロードします。Firepower Management Center の設定の保存および読み込み（74 ページ）を参照してください

- FMC のハードドライブの内容に今後アクセスできないようにするため、ハードドライブのスクラビング処理を確実に実行します。ハード ドライブの消去 （76 ページ） を参照してください。

復元ユーティリティのメニュー

FMC の復元ユーティリティでは、対話型メニューによって復元プロセスを進められます。

メニューに表示されるオプションを次の表に示します。

表 *2:* 復元メニューのオプション

オプション	説明	詳細
1 IPの設定（1 IP Configuration）	復元するアプライアンスの管理インターフェイスに関するネットワーク情報を指定します。これにより、ISO および更新ファイルを格納したサーバとアプライアンスが通信できるようになります。	アプライアンスの管理インターフェイスの指定 （69 ページ）
2 トランスポート プロトコルの選択（2 Choose the transport protocol）	アプライアンスを復元するために使用する ISO イメージの場所と、アプライアンスでファイルのダウンロードに必要なすべての資格情報を指定します。	ISO イメージの場所および転送方式の指定 （69 ページ）
3 パッチ/ルール更新の選択（3 Select Patches/Rule Updates）	アプライアンスを ISO イメージのベース バージョンに復元した後で適用するシステム ソフトウェアおよび侵入ルールの更新を指定します。	復元時のシステム ソフトウェアおよびルールの更新の選択 （71 ページ）
4 ISOのダウンロードとマウント（4 Download and Mount ISO）	適切な ISO イメージと、システム ソフトウェアまたは侵入ルールの更新をダウンロードします。ISO イメージをマウントします。	ISO および更新ファイルのダウンロードとイメージのマウント （72 ページ）
5 インストールの実行（5 Run the Install）	復元プロセスを開始します。	Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）
6 設定の保存（6 Save Configuration） 7 設定の読み込み（7 Load Configuration）	後で使用できるように復元設定のセットを保存するか、または保存されているセットを読み込みます。	Firepower Management Center の設定の保存および読み込み （74 ページ）

オプション	説明	詳細
8 ディスクの内容を消去（8 Wipe Contents of Disk）	ハードドライブの内容に今後アクセスできないようにするため、ハードドライブのスクラビング処理を確実に実行します。	ハード ドライブの消去 （76 ページ）

矢印キーを使用してメニューを移動します。メニューオプションを選択するには、[上（Up）] および [下（Down）] 矢印キーを使用します。ページ下部にある [OK] ボタンと [キャンセル（Cancel）] ボタンの切り替えには、[右（Right）] および [左（Left）] 矢印キーを使用します。

メニューには、2 つのオプションが表示されます。

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

復元プロセスについて

アプライアンスを復元するために使用する ISO イメージは、そのアプライアンスモデルに対してシスコがサポートを提供する時点によって異なります。新しいアプライアンス モデルに対応するためにマイナー バージョンで ISO イメージがリリースされる場合を除き、ISO イメージは通常、システム ソフトウェアのメジャー バージョン（6.1、6.2 など）に関連付けられています。互換性のないバージョンのシステムをインストールしないようにするため、アプライアンスの最新 ISO イメージを常に使用することを推奨します。便宜上、復元プロセスの一環としてシステム ソフトウェアと侵入ルールの更新をインストールできます。ルール更新は FMC だけで必要であることに注意してください。

FMC は、内部フラッシュ ドライブを使用してアプライアンスを起動するため、復元ユーティリティを実行できます。

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

アプライアンスを工場出荷時のデフォルトに復元する前に、復元プロセス中の次の推奨事項とシステムの予想される動作に注意してください。

- ネットワーク上のトラフィックフローの中断を回避するために、メンテナンスウィンドウ中、または中断による展開への影響が最も少ないときにアプライアンスを復元することをお勧めします。

- アプライアンスに存在するバックアップファイルをすべて削除または移動してから、最新のイベントおよび設定データを外部ロケーションにバックアップすることを推奨します。
- アプライアンスの工場出荷時の初期状態に復元すると、アプライアンスのほぼすべての設定およびイベントデータ（コンソール表示設定を含む）が失われます。復元ユーティリティはアプライアンスのライセンス、ネットワーク、および（場合によっては）LOM の設定を保持できますが、復元プロセス完了後にその他のすべての設定タスクを実行する必要があります。

  復元プロセス完了後の LOM 設定の保存期間は、Firepower のバージョンによって異なります。

  - FMC をバージョン 6.2.3 以前に復元する場合、ライセンスおよびネットワーク設定の削除を選択するかどうかに関係なく、システムで LOM 設定はリセットされません。
  - FMC をバージョン 6.3 以降に復元する場合、ライセンスおよびネットワーク設定の削除を選択するかどうかに関係なく、システムで LOM 設定がリセットされます。

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

  （注） Web インターフェイスを使用してアプライアンスを復元することはできません。

- FMC を復元するには、次のいずれかの方法でそれに接続する必要があります。
  - キーボードとモニタ/KVM：アプライアンスに USB キーボードと VGA モニタを接続できます。これは、KVM（キーボード、ビデオ、マウス）スイッチに接続しているラックマウント型アプライアンスで便利です。物理インターフェイス （1 ページ）の図を参照して、USB ポートと VGA ポートを識別してください。リモートアクセス可能な KVM がある場合、物理的にアクセスできない状態でもアプライアンスを復元できます。
  - シリアル接続/ラップトップ：アプライアンスに付属の RJ-45 to DP9 コンソール ケーブル（シスコ製品番号 72-3383-XX）を使用して、コンピュータをアプライアンスに接続できます。物理インターフェイス （1 ページ） の図を参照して、シリアルポートを識別してください。アプライアンスと通信するには、HyperTerminal や Xmodem などの端末エミュレーション ソフトウェアを使用します。
  - Serial over LAN（SoL）接続による Lights-Out Management（LOM）：SoL 接続による LOM を使用して、限定されたアクションのセットを FMC 上で実行できます。アプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。LOM を使用してアプライアンスに接続した後で、物理シリアル接続を使用する場合と同様の方法で、復元ユーティリティに対してコマンドを発行します。

（注） LOM はデフォルト（eth0）の管理インターフェイスでのみ使用できます（物理インターフェイス （1 ページ） の図を参照）。LOM を使用して FMC を復元するには、**admin** ユーザに LOM 権限を付与する必要があります。詳細については、Lights-Out Management のセットアップ （51 ページ）を参照してください。

注意 バージョン 6.3 以降では、LOM を使用してデバイスを工場出荷時の設定に復元しているときに、アプライアンスに物理的にアクセスできない場合、復元後にアプライアンスを利用できなくなります。

（注） この章の手順では、アプライアンスの電源をオフにせずにアプライアンスを復元する方法を説明します。ただし、何らかの理由で電源をオフにする必要がある場合は、アプライアンスの Web インターフェイス、（バージョン 6.3 以降でサポートされている）FMC CLI からの **system shutdown** コマンド、またはアプライアンスシェルからの **shutdown-h now** コマンドを使用します。

Firepower Management Center の工場出荷時の初期状態への復元

ここでは、FMC を工場出荷時の初期状態に復元するために必要なタスクの概要と、それらを実行する順序について説明します。

始める前に

FMC の対話型の復元メニューをよく理解しておいてください。詳細については、復元ユーティリティのメニュー （60 ページ）を参照してください。

手順

ステップ 1 復元ファイルと ISO 更新ファイルを入手します。復元 ISO ファイルと更新ファイルの入手 （65 ページ）を参照してください。

ステップ 2 次の 2 つの方法のいずれかを使用して、復元プロセスを開始します。

- KVM または物理シリアル ポートを使用した復元ユーティリティの開始 （66 ページ）
- Lights-Out Management を使用した復元ユーティリティの開始 （67 ページ） （これは、アプライアンスに物理的にアクセスできない場合に役立ちます）

注意 LOM を使用して、デバイスをバージョン 6.3 以降の工場出荷時設定に復元する場合、アプライアンスに物理的にアクセスできない場合は、ライセンス設定とネットワーク設定を削除すると、復元後にアプライアンスにアクセスできなくなります。

ステップ 3 対話型の復元メニューを使用して、アプライアンスの管理インターフェイスを指定します。アプライアンスの管理インターフェイスの指定 （69 ページ）を参照してください。

ステップ 4 対話型の復元メニューを使用して、ISO イメージの場所と転送方法を指定します。ISO イメージの場所および転送方式の指定 （69 ページ）を参照してください。

ステップ 5 （任意）対話型の復元メニューを使用して、復元プロセスに含めるシステム ソフトウェアやルールの更新を選択します。復元時のシステム ソフトウェアおよびルールの更新の選択 （71 ページ）を参照してください。

ステップ 6 （任意）将来の復元アクティビティで使用できるように、選択したシステム設定を保存します。Firepower Management Center の設定の保存 （75 ページ）を参照してください。

ステップ 7 対話型の復元メニューを使用して、ISO ファイルと更新ファイルをダウンロードし、そのイメージをアプライアンスにマウントします。ISO および更新ファイルのダウンロードとイメージのマウント （72 ページ）を参照してください。

ステップ 8 ソフトウェア バージョンに基づいて、次の 2 つのアプライアンス復元先を選択できます。

- システムを別のメジャーバージョンに復元する場合は、2 パス復元プロセスを実行します。
  1. 最初のパスで復元イメージを更新します。復元イメージの更新 （72 ページ）を参照してください。
  2. 2 番目のパスでシステム ソフトウェアの新しいバージョンをインストールします。新しいシステム ソフトウェア バージョンのインストール （73 ページ）を参照してください。
- システムを同じメジャーバージョンに復元する場合は、システム ソフトウェアの新しいバージョンをインストールするだけです。新しいシステム ソフトウェア バージョンのインストール （73 ページ）を参照してください。

次のタスク

FMC を工場出荷時設定に復元すると、アプライアンスのほぼすべての設定およびイベントデータ（コンソール表示設定を含む）が失われます。

- アプライアンスのライセンスおよびネットワーク設定を削除していない場合は、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを直接参照し、設定を実行できます。

  詳細については、ご使用のバージョンの Firepower に適したセットアッププロセスを参照してください。

  - Firepower バージョン 6.5 以降については、Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降） （14 ページ）を参照してください。

- Firepowerバージョン 6.2 ー 6.4x については、ソフトウェアバージョン 6.2 ー 6.4 の Web インターフェイスを使用した FMC 初期セットアップ （31 ページ）を参照してください。

- ライセンスとネットワーク設定を削除している場合は、アプライアンスを新品の場合と同様に設定する必要があります。最初に、管理ネットワークと通信するように設定します。

  詳細については、ご使用のバージョンの Firepower に適したセットアッププロセスを参照してください。

  - Firepower バージョン 6.5 以降については、Web インターフェイスを使用したプラットフォームの初期設定（バージョン 6.5 以降） （14 ページ）を参照してください。
  - Firepowerバージョン 6.2 ー 6.4x については、ソフトウェアバージョン 6.2 ー 6.4 の Web インターフェイスを使用した FMC 初期セットアップ （31 ページ）を参照してください。

- Cisco Smart Software Manager から FMC の登録を解除した場合は、アプライアンスを Cisco Smart Software Manager に登録します。**[システム（System）]**>**[ライセンス（Licenses）]**>**[スマートライセンス（Smart Licenses）]** を選択し、登録アイコンをクリックします。

（注） 復元プロセス完了後の LOM 設定の保存期間は、Firepower のバージョンによって異なります。

- FMC をバージョン 6.2.3 以前に復元する場合、ライセンスおよびネットワーク設定の削除を選択するかどうかに関係なく、システムで LOM 設定はリセットされません。
- FMC をバージョン 6.3 以降に復元する場合、ライセンスおよびネットワーク設定の削除を選択するかどうかに関係なく、システムでLOM設定がリセットされます。初期セットアップ プロセスを完了した後に、次のいずれかを実行してください。
  - シリアル接続または SoL/LOM 接続を使用してアプライアンスのコンソールにアクセスする場合は、コンソール出力をリダイレクトします。コンソール出力のリダイレクト （54 ページ）を参照してください。
  - LOM を使用する場合は、機能を再度有効にし、1 つ以上の LOM ユーザを有効にします。詳細については、「Lights-Out Management のセットアップ （51 ページ）」を参照してください。

復元 ISO ファイルと更新ファイルの入手

始める前に

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

手順

ステップ 1 サポートアカウントのユーザ名とパスワードを使用して、サポートサイト（https://sso.cisco.com/autho/forms/CDClogin.html）にログインします。

ステップ 2 ソフトウェア ダウンロード セクション（https://software.cisco.com/download/navigator.html）を参照します。

ステップ 3 表示されるページの[検索（Find）]エリアに、ダウンロードしてインストールするシステム ソフトウェアの検索文字列を入力します。

例：

Firepower のソフトウェア ダウンロードを検索するには、**Firepower** と入力します。

ステップ 4 ダウンロードするイメージ（ISO イメージ）を見つけます。ページの左側にあるリンクの 1 つをクリックして、ページの該当するセクションを表示します。

例：

[6.3.0] をクリックして、Firepower システムのバージョン 6.3.0 のイメージとリリース ノートを表示します。

ステップ 5 ダウンロードする ISO イメージをクリックします。
ファイルのダウンロードが開始されます。

ステップ 6 管理ネットワーク上でアプライアンスがアクセスできる HTTP（Web）サーバ、FTP サーバ、または SCP 対応ホストにファイルをコピーします。

注意 電子メールを使用して ISO ファイルまたは更新ファイルを転送しないでください。ファイルが破損する可能性があります。また、ファイルの名前を変更しないでください。復元ユーティリティでは、ファイル名がサポートサイトでの名前と同じである必要があります。

KVM または物理シリアル ポートを使用した復元ユーティリティの開始

FMC では、内部フラッシュ ドライブに復元ユーティリティが組み込まれています。

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ） で説明している復元プロセスの適切な前の手順を完了していることを確認してください。

手順

ステップ 1 キーボード/モニタまたはシリアル接続を使用し、**admin** アカウントを使用したアプライアンスのシェルにログインします。お使いの Firepower バージョンに適した手順を使用します。「次での CLI または Linux シェルへのアクセス FMC （5 ページ）」を参照してください。

ステップ 2 アプライアンスを起動します。**sudo reboot** と入力します。プロンプトが表示されたら、admin パスワードを指定します。

ステップ 3 再起動状況の監視ブート メニューが表示されたら、すぐに [オプション 3（Option 3）] を選択してシステムを復元します。

（注） ブートメニューでは、タイムアウトするまでに選択できる時間は秒数です。そのウィンドウで失敗すると、アプライアンスはリブートプロセスに進みます。リブートが完了するまで待ち、再試行します。

ステップ 4 復元ユーティリティの対話型メニューに表示モードの入力を求められます。

- キーボードとモニタ接続の場合、**1** と入力して **Enter** キーを押します。
- シリアル接続の場合、**2** と入力して **Enter** キーを押します。

表示モードを選ばない場合、復元ユーティリティはデフォルトのアスタリスク（*****）の印が付いたオプションを表示します。

（注） 表示モードメニューでは、タイムアウトするまでに選択できる時間は秒数です。機会を逃し、誤ったコンソール選択でアプライアンスを誤ってシステム復元モードに再起動した場合は、再起動が完了するまで待ってから、アプライアンスの電源を切ってください。（FMC ソフトウェアが実行されていないため、この時点では電源ボタンを使用してアプライアンスをシャットダウンする必要があります。) その後、FMC の電源を入れ、このタスクからやり直します。

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

ステップ 5 **Enter** キーを押して著作権情報を確認します。

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

アプライアンスを工場出荷時設定に復元する必要があるが、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。

（注） バージョン 6.3 以降の場合は、復元プロセスによってデバイスの LOM 設定がリセットされます。新しく復元されたアプライアンスに LOM を使用してアクセスすることはできません。

注意 バージョン 6.3 以降の場合は、LOM を使用してデバイスを工場出荷時設定に復元しているときに、アプライアンスに物理的にアクセスできない場合、ライセンス設定とネットワーク設定を削除すると、復元後にアプライアンスにアクセスできなくなります。

始める前に

- Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）で説明している復元プロセスの適切な前の手順を完了していることを確認してください。
- LOM 機能を有効にし、admin ユーザに LOM 権限を付与する必要があります。詳細については、Lights-Out Management のセットアップ （51 ページ）を参照してください。

手順

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

- IPMItool の場合は次を入力します：**sudo ipmitool -I lanplus -H *IP_address* -U admin sol activate**
- ipmiutil の場合は次を入力します：**sudo ipmiutil sol -a -V4 -J3 -N *IP_address* -U admin -P *password***

IP_address は、アプライアンスの管理インターフェイスの IP アドレスで、パスワードは admin アカウントのパスワードです。IPMItool では、**sol activate** コマンドの発行後にパスワードの入力が求められることに注意してください。

ステップ 2 ルート ユーザとしてのアプライアンスを再起動します。**sudo reboot** と入力します。プロンプトが表示されたら、admin パスワードを指定します。

ステップ 3 再起動状況の監視ブート メニューが表示されたら、すぐに [オプション 3（Option 3）] を選択してシステムを復元します。

（注） ブート メニューでは、タイムアウトするまでに選択できる時間は秒数です。そのウィンドウで失敗すると、アプライアンスはリブート プロセスに進みます。リブートが完了するまで待ち、再試行します。

ステップ 4 復元ユーティリティの対話型メニューに表示モードの入力を求められます。**2** と入力して **Enter** キーを押します。アプライアンスのシリアル接続を使用して対話型の復元メニューが読み込まれます。

表示モードを選ばない場合、復元ユーティリティはデフォルトのアスタリスク（*****）の印が付いたオプションを表示します。

重要 表示モードメニューでは、タイムアウトするまでに選択できる時間は秒数です。（キーボードとモニタ接続の場合）オプション 1 を使用してアプライアンスをシステム復元モードに誤って再起動した場合に、その機会のウィンドウを見逃した場合は、アプライアンスへの物理的なアクセスを取得し、リブートが完了するまで待機してから、アプライアンスの電源を切ってください。（FMC ソフトウェアが実行されていないため、この時点では電源ボタンを使用してアプライアンスをシャットダウンする必要があります。) その後、FMC の電源を入れ、このタスクからやり直します。

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

ステップ 5 **Enter** キーを押して著作権情報を確認します。

アプライアンスの管理インターフェイスの指定

復元ユーティリティを実行する際には、最初に復元するアプライアンスの管理インターフェイスを指定します。これにより、ISO および更新ファイルをコピーしたサーバとアプライアンスが通信できるようになります。

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）で説明している復元プロセスの適切な前の手順を完了していることを確認してください。

手順

ステップ 1 復元ユーティリティのメイン メニューから、[1 IP の設定（1 IP Configuration）] を選択します。

ステップ 2 アプライアンスの管理インターフェイス（通常は eth0）を選択します。

ステップ 3 管理ネットワークに使用しているプロトコル（**IPv4** または **IPv6**）を選択します。
管理インターフェイスに IP アドレスを割り当てるためのオプションが表示されます。

ステップ 4 管理インターフェイスに IP アドレスを割り当てる方法を選択します。

- [スタティック（Static）]：一連のページで、管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイを手動で入力するよう促されます。
- [DHCP]：管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイがアプライアンスにより自動的に検出され、IP アドレスが表示されます。

ステップ 5 プロンプトが表示されたら、設定を確認します。

プロンプトが表示されたら、アプライアンスの管理インターフェイスに割り当てられている IP アドレスを確認します。LOM を使用する場合は、アプライアンスの管理 IP アドレスが LOM IP アドレスではないことに注意してください。

ISO イメージの場所および転送方式の指定

復元プロセスで必要なファイルをダウンロードするために使用される管理 IP アドレスを設定したら、次にアプライアンスの復元に使用する ISO イメージを指定する必要があります。これは、サポート サイト（復元 ISO ファイルと更新ファイルの入手 （65 ページ）を参照）からダ

ウンロードし、Web サーバ、FTP サーバ、または SCP 対応ホストに保存した ISO イメージです。

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）で説明している復元プロセスの適切な前の手順を完了していることを確認してください。

手順

ステップ 1 復元ユーティリティのメイン メニューで、[2 トランスポート プロトコルの選択（2 Choose the transport protocol）] を選択します。

ステップ 2 表示されるページで、[HTTP]、[FTP]、または [SCP] を選択します。

ステップ 3 復元ユーティリティにより表示される一連のページで、選択したプロトコルに必要な情報を入力します。復元ファイルのダウンロード設定 （70 ページ）を参照してください。

情報が正しければ、アプライアンスはサーバに接続し、指定された場所の Cisco ISO イメージのリストを表示します。

ステップ 4 使用する ISO イメージを選択します。

ステップ 5 プロンプトが表示されたら、設定を確認します。

復元ファイルのダウンロード設定

アプライアンスの復元に使用する ISO イメージを指定するには、復元プロセスで必要なファイルをダウンロードするために使用される管理 IP アドレスを設定する必要があります。FMC の対話型メニューで、ダウンロードを実行するための情報の入力が求められます。これらの情報を次の表に示します。

表 *3:* 復元ファイルのダウンロードに必要な情報

使用する方式	指定する必要がある情報
HTTP	• Web サーバの IP アドレス • ISO イメージ ディレクトリのフル パス（例：`/downloads/ISOs/`）
FTP	• FTP サーバの IP アドレス • 資格情報が使用されるユーザのホーム ディレクトリを基準にした ISO イメージ ディレクトリの相対パス（例：`mydownloads/ISOs/`） • FTP サーバの認証ユーザ名とパスワード

使用する方式	指定する必要がある情報
SCP	• SCP サーバの IP アドレス • SCP サーバの認証ユーザ名 • ISO イメージ ディレクトリのフル パス • 先に入力したユーザ名のパスワード （注） パスワードを入力する前に、信頼できるホストのリストにSCPサーバを追加するよう求められる場合があります。続行するには、同意する必要があります。

復元時のシステム ソフトウェアおよびルールの更新の選択

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

復元ユーティリティは、1 つのシステム ソフトウェア更新と 1 つのルール更新だけを使用できます。ただしシステム更新は直前のメジャーバージョンに対して累積されます。ルール更新も累積されます。ご使用のアプライアンスに対して使用可能な最新の更新を入手することを推奨します。復元 ISO ファイルと更新ファイルの入手 （65 ページ） を参照してください。

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

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ） で説明している復元プロセスの適切な前の手順を完了していることを確認してください。

手順

ステップ 1 復元ユーティリティのメイン メニューで [3 パッチ/ルール更新の選択（3 Select Patches/Rule Updates）] を選択します。

復元ユーティリティは、前の手順（「ISO イメージの場所および転送方式の指定 （69 ページ）」を参照）で指定した場所とプロトコルを使用して、その場所にあるすべてのシステム ソフトウェア更新ファイルのリストを取得して表示します。SCP を使用する場合、更新ファイルリストを表示するためのプロンプトが表示されたらパスワードを入力します。

ステップ 2 使用するシステム ソフトウェア更新がある場合は、それを選択します。更新を選択しなくてもかまいません。続行するには、更新を選択せずに **Enter** キーを押します。適切な場所にシステム ソフトウェア更新がない場合は、**Enter** キーを押して続行するよう求められます。

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

ステップ 3 使用するルール更新がわかっている場合は、それを選択します。更新を選択しなくてもかまいません。続行するには、更新を選択せずに **Enter** キーを押します。適切な場所にルール更新がない場合は、**Enter** キーを押して続行するよう求められます。

ISO および更新ファイルのダウンロードとイメージのマウント

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）で説明している復元プロセスの適切な前の手順を完了していることを確認してください。

手順

ステップ 1 復元ユーティリティのメイン メニューで [4 ISO のダウンロードとマウント（4 Download and Mount ISO）] を選択します。

ステップ 2 プロンプトが表示されたら、選択項目を確認します。SCP サーバからダウンロードする場合は、プロンプトが表示されたらパスワードを入力します。該当するファイルがダウンロードされ、マウントされます。

復元イメージの更新

アプライアンスを異なるメジャーバージョンに復元する場合、復元ユーティリティによるこの最初のパスでは、アプライアンスの復元イメージと、必要に応じて復元ユーティリティ自体が更新されます。

（注） アプライアンスを同じメジャーバージョンに復元する場合、またはこれがこのプロセスの 2 番目のパスの場合は、この手順を使用しないでください。新しいシステム ソフトウェア バージョンのインストール （73 ページ）を参照してください。

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）で説明している復元プロセスの適切な前の手順を完了していることを確認してください。

手順

ステップ 1 復元ユーティリティのメイン メニューで [5 インストールの実行（5 Run the Install）] を選択します。

ステップ 2 プロンプトが表示されたら（2 回）、アプライアンスを再起動することを確認します。

ステップ 3 復元ユーティリティの対話型メニューに表示モードの入力を求められます。

- キーボードとモニタ接続の場合、**1** と入力して Enter キーを押します。
- シリアル接続の場合、**2** と入力して **Enter** キーを押します。

表示モードを選ばない場合、復元ユーティリティはデフォルトのアスタリスク（*****）の印が付いたオプションを表示します。

アプライアンスをこのメジャーバージョンに初めて復元する場合以外は、最後に使用した復元設定がユーティリティにより自動的に読み込まれます。続行するには、以降の一連のページで設定を確認します。

ステップ 4 **Enter** キーを押して著作権情報を確認します。

次のタスク

復元プロセスの 2 番目のパスのタスクを実行します。新しいシステム ソフトウェア バージョンのインストール （73 ページ） を参照してください。

新しいシステム ソフトウェア バージョンのインストール

アプライアンスを同じメジャーバージョンに復元する場合、またはこれが2パス復元プロセスの 2 番目のパスの場合は、以下のタスクを実行します。

（注） 復元プロセスにより、コンソールの表示設定を VGA ポートを使用するデフォルトモードにリセットされます。

始める前に

- Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）で説明している復元プロセスの適切な前の手順を完了していることを確認してください。
- このタスクを 2 パス復元プロセスの 2 番目のパスを実行している場合は、まず ISO イメージをダウンロードしてマウントする必要があります。ISO および更新ファイルのダウンロードとイメージのマウント （72 ページ）を参照してください。（2 パス復元プロセスを実行している場合は、これは 2 回目の ISO イメージのダウンロードとマウントになります）

手順

ステップ 1 復元ユーティリティのメイン メニューで [5 インストールの実行（5 Run the Install）] を選択します。

ステップ 2 アプライアンスを復元することを確認します。

ステップ 3 アプライアンスのライセンスおよびネットワーク設定を削除するかどうかを選択します。

ほとんどの場合、これらの設定は削除しないでください。設定を保持することで初期設定プロセスを短くすることができます。復元とそれに続く初期設定の後に設定を変更する場合、通常は、それらの設定を今リセットするよりも時間がかかりません。

注意 バージョン 6.3 以降の場合は、復元プロセスによってデバイスの LOM 設定がリセットされます。新しく復元されたアプライアンスに LOM を使用してアクセスすることはできません。LOM を使用してデバイスをバージョン 6.3 以降に復元しているときに、アプライアンスに物理的にアクセスできない場合、復元後にアプライアンスにアクセスできなくなります。

ステップ 4 アプライアンス復元の最終確認を入力します。

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

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

（注） アプライアンスの再イメージ化は、必ず保守期間中に行ってください。

Firepower Management Center の設定の保存および読み込み

FMC を復元する必要がある場合は、復元ユーティリティを使用して設定を保存できます。復元ユーティリティは最後に使用された設定を自動的に保存しますが、次のような複数の設定を保存することもできます。

- アプライアンスの管理インターフェイスに関するネットワーク情報。詳細については、アプライアンスの管理インターフェイスの指定 （69 ページ）を参照してください。
- ISO イメージの場所と、アプライアンスがファイルをダウンロードするために必要とする転送プロトコルおよび資格情報。詳細については、ISO イメージの場所および転送方式の指定 （69 ページ）を参照してください。

- アプライアンスを ISO イメージのベース バージョンに復元した後で適用するシステム ソフトウェアと侵入ルールの更新（存在する場合）。詳細については、復元時のシステム ソフトウェアおよびルールの更新の選択 （71 ページ）を参照してください。

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

設定を保存するのに最適なタイミングは、上記の情報の指定後、ISO イメージをダウンロードしてマウントする前です。

Firepower Management Center の設定の保存

始める前に

Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）のステップ 1 ～ 5 を完了します。

手順

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

ユーティリティにより、保存する設定の設定内容の設定が表示されます。

ステップ 2 プロンプトが表示されたら、設定を保存することを確認します。

ステップ 3 プロンプトが表示されたら、設定の名前を入力します。

次のタスク

保存された設定を使用してシステムの復元する場合は、Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ）のステップ 7 に進みます。

保存されている Firepower Management Center の設定の読み込み

以前に保存した設定を読み込んで、FMC を復元できます。

手順

ステップ 1 復元ユーティリティのメイン メニューから、[7 設定の読み込み（7 Load Configuration）] を選択します。

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

ステップ 2 使用する設定を選択します。

ユーティリティにより、読み込む設定の設定内容が表示されます。

ステップ 3 プロンプトが表示されたら、設定を読み込むことを確認します。

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

次のタスク

読み込まれた設定を使用してシステムを復元する場合は、Firepower Management Center の工場出荷時の初期状態への復元 （63 ページ） のステップ 7 に進みます。

ハード ドライブの消去

FMC のハードドライブを安全に消去して、その内容にアクセスできないようにすることができます。たとえば、機密データが含まれている故障したアプライアンスを返却する必要がある場合は、この機能を使用してそのアプライアンス上のデータを上書きできます。

ハードドライブ消去シーケンスは、着脱可能または着脱不可能なリジッドディスクのサニタイズに関する DoD 5220.22-M 手順に準拠しています。この手順では、すべてのアドレス可能な場所を 1 つの文字で上書きし、その補数の文字で上書きし、さらにランダムな文字コードで上書き処理を行ってから、検証する必要があります。追加の制約については、DoD ドキュメントを参照してください。

注意 ハードドライブの消去処理では、アプライアンスのすべてのデータが失われ、動作不能であると示されます。

アプライアンスの対話型メニューのオプションを使用して、ハードドライブを消去できます。詳細については、復元ユーティリティのメニュー （60 ページ）を参照してください。

手順

ステップ 1 以下のいずれかの項の説明に従い、復元ユーティリティの対話型メニューを表示します。これは、アプライアンスへのアクセス方法に応じて異なります。

- KVM または物理シリアル ポートを使用した復元ユーティリティの開始 （66 ページ）
- Lights-Out Management を使用した復元ユーティリティの開始 （67 ページ）

ステップ 2 復元ユーティリティのメインメニューで、[8 ディスクの内容を消去（8 Wipe Contents of Disk）] を選択します。

ステップ 3 プロンプトが表示されたら、ハードドライブを消去することを確認します。プロセスが完了するまでに数時間かかることがあります。ドライブの容量が大きいほど、時間がかかります。

【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。