



Cisco Firepower Management Center 750、1500、2000、3500、4000 スタート アップガイド

更新日: 2020 年 4 月 6 日

このマニュアルの構成は、次のとおりです。

- パッケージの内容
- ライセンス要件
- バージョン 6.5 以降での設置と初期設定
- バージョン 5.4 ~ 6.4.x での設置と初期設定
- 管理に関する推奨事項
- コンソール出力のリダイレクト
- Lights-Out Management の設定
- 工場出荷時の初期状態への Firepower Management Center の復元
- Firepower Management Center の事前設定
- ハードドライブのスクラビング
- 関連資料

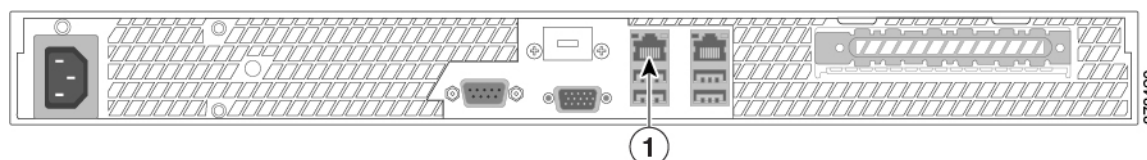
パッケージの内容

このセクションでは、各モデルに含まれる品目を示します。この内容は変更される場合があるため、実際に含まれている品目は前後する場合があります。

シャーシ モデル

- Firepower Management Center 750 (1U モデル)。次のシャーシ背面図に、MC750 の管理インターフェイスの位置を示します。

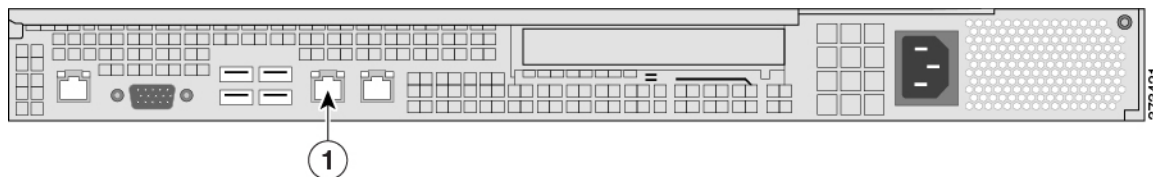
図 1 MC 750 のシャーシおよび管理インターフェイス



1	管理インターフェイス	
---	------------	--

- Firepower Management Center 1500 (1U モデル)。次のシャーシ背面図に、MC1500 の管理インターフェイスの位置を示します。

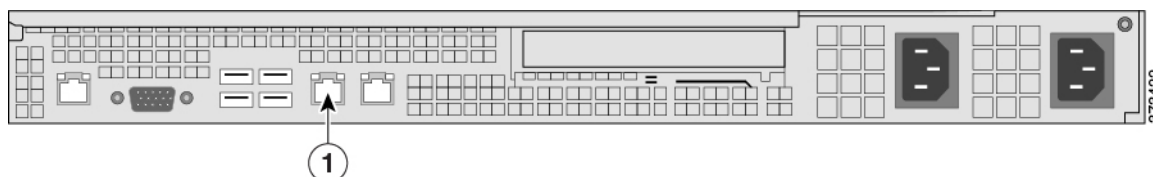
図 2 MC 1500 のシャーシおよび管理インターフェイス



1	管理インターフェイス		
---	------------	--	--

- Firepower Management Center 3500 (1U モデル)。次のシャーシ背面図に、MC3500 の管理インターフェイスの位置を示します。

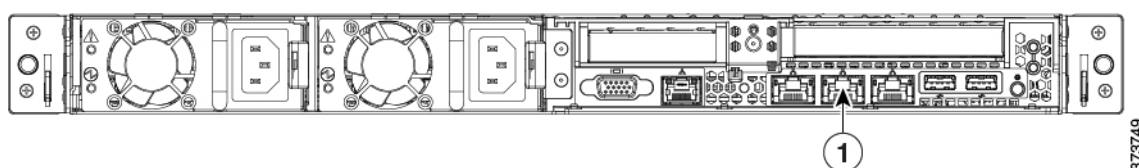
図 3 MC 3500 のシャーシおよび管理インターフェイス



1	管理インターフェイス		
---	------------	--	--

- Firepower Management Center 2000/4000 (1U モデル)。次のシャーシ背面図に、管理インターフェイスの位置を示します。

図 4 MC2000 および MC4000



1	管理インターフェイス		
---	------------	--	--

付属品

- 電源装置ごとに 1 本ずつの電源コード。
- シャーシごとに 1 本ずつのストレート Cat 5e イーサネット ケーブル。
- シャーシごとに 1 つずつのラック取り付けキット。

ライセンス要件

組織に対して Firepower System の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。Firepower Management Center を使用して、それ自身と管理対象デバイスのライセンスを管理できます。Firepower System で提供されるライセンス タイプは、管理するデバイスのタイプによって異なります。

クラシック ライセンス

7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv の各デバイスの場合、クラシック ライセンスを使用する必要があります。クラシック 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。

FMC で 6.5 よりも前のバージョンの Firepower を使用している場合: Cisco 初期設定ページを使用して、組織で購入したクラシック ライセンスを追加することを推奨します。「[ライセンス設定 \(16 ページ\)](#)」を参照してください。初期設定でクラシック ライセンスを追加しない場合、初期設定で登録するすべてのデバイスは、ライセンス未登録として Management Center に追加されるため、初期設定プロセスが終了した後で、個別にライセンスを付与する必要があります。再イメージ化されたアプライアンスをセットアップしており、復元プロセスの一部としてライセンス設定を維持している場合は、初期設定ページのこのセクションは事前に入力されていることがあります。

FMC で Firepower バージョン 6.5 以降を使用している場合: 初期設定ウィザードの完了後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。Firepower Management Center に管理対象デバイスを登録するとき、または Firepower Management Center に管理対象デバイスを登録した後に、それらのデバイスにライセンスを割り当てることができます。

スマート ライセンス

Firepower Threat Defense の物理デバイスとバーチャル 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 Smart Licensing によって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー (PAK) ライセンスとは異なり、スマート ライセンスは特定のシリアル番号またはライセンス キーに関連付けられません。スマート ライセンスを使用すると、ライセンスの使用状況と要件をひと目で確認できます。

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 タイプに関する情報、および展開全体でライセンスを管理する方法については、『*Firepower Management Center Configuration Guide*』を参照してください。

FMC での CLI または Linux シェルへのアクセス

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。FMC CLI または Linux シェルにログインするための手順が本書で示されている場合は、このトピックを参照してください。

注意: TAC またはユーザー 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。

はじめる前に:

キーボードとモニターを使用して 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との SSH セッションを確立します。

手順

1. CLI の **admin** ユーザーのログイン情報を使用して FMC にログインします。

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 5.4 ~ 6.2.x 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.x または 6.4.x 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.x または 6.4.x 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 2 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 にアクセスできません。Linux シェルにアクセスするには、ステップ 2 に進みます。

2. 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。

バージョン 6.5 以降での設置と初期設定

(注) Firepower バージョン 6.5 以降は、FMC モデル 750、1500、および 3500 ではサポートされていません。

バージョン 6.5 以降を実行している FMC に初めてログインすると、初期設定ウィザードに従って、信頼できる管理ネットワーク上で通信するように新しいアプライアンスを設定できます。ウィザードにより、効率的な初期設定プロセスが提供され、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ための週次メンテナンス作業が自動的に設定されます。

FMC 管理インターフェイスは、Dynamic Host Configuration Protocol (DHCP) によって割り当てられた IPv4 アドレスを受け入れるように事前に設定されています。FMC が DHCP リースの取得に失敗した場合、管理インターフェイスではフォールバック IPv4 アドレス 192.168.45.45 が使用されます。

(注) ライセンスとネットワークの設定を保持することを選択してシステムの復元を実行した後に、初めて FMC に接続した場合、管理インターフェイスの IP アドレスは、システムの復元を実行する前のアドレスと同じになります。「[Firepower Management Center の初期設定ウィザード \(7 ページ\)](#)」に直接進んでください。

バージョン 6.5 以降を実行している FMC を設置および設定するための手順

1. 「[アプライアンスの設置 \(4 ページ\)](#)」の説明に従って、アプライアンスを設置します。
2. 次の 2 つのうち適切な方法を選択して、初期設定を実行します。
 - ネットワークで DHCP を使用しておらず、PC からフォールバック アドレス (またはシステムの復元に保持されているアドレス) に到達できない場合は、「[管理インターフェイスを使用した Firepower Management Center へのアクセス \(5 ページ\)](#)」の説明に従って、コンピュータを FMC の物理管理インターフェイスに直接接続して初期設定を行うことをお勧めします。
 - ローカル DHCP によって FMC にアドレスが割り当てられる場合は、キーボードとモニターを使用してアプライアンスを設定します。「[キーボードおよびモニターを使用した Firepower Management Center へのアクセス \(6 ページ\)](#)」を参照してください。

アプライアンスの設置

次の手順は、アプライアンスを物理的に設置する手順の概要です。手順の詳細については、『*Cisco Firepower Management Center 750, 1500, 2000, 3500, and 4000 Hardware Installation Guide*』を参照してください。

手順

1. 取り付けキットと付属の手順を使用して、アプライアンスをラックに取り付けます。
2. 電源コードを両方の電源装置に接続し、別々の電源に差し込みます。

両方の電源装置を接続しないと、シャーシ前面パネルの警告インジケータがオレンジ色で点灯し、FMC Web インターフェイスにヘルス アラートが表示されます。
3. 前面パネルにある電源スイッチを押して、アプライアンスをオンにします。

電源スイッチを押すと、アプライアンスが一時的にオンになった後にシャーシ前面パネルの電源インジケータがオレンジ色で点灯している以外はシャットダウンしたように見ることがあります。これは正常な状態です。電源ボタンをもう一度押すと、アプライアンスの電源が入り、電源インジケータが緑色で点灯します。

次の作業

- FMC 管理インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前に設定されていますが、DHCP リースの取得に失敗した場合、管理インターフェイスではフォールバック IPv4 アドレス 192.168.45.45 が使用されます。または、ライセンスとネットワークの設定を保持することを選択してシステムの復元を実行した後に、初めて FMC に接続した場合、IP アドレスは、システムの復元を実行する前のアドレスと同じになります。作業を進める前に、アプライアンスにアクセスするための次のいずれかの方法が確立していることを確認します。
 - ネットワークで DHCP を使用しておらず、PC からフォールバック アドレス(またはシステムの復元に保持されているアドレス)に到達できない場合は、「[管理インターフェイスを使用した Firepower Management Center へのアクセス\(5 ページ\)](#)」の説明に従って、コンピュータを FMC の物理管理インターフェイスに直接接続して初期設定を行うことをお勧めします。
 - ローカル DHCP によって FMC にアドレスが割り当てられる場合は、キーボードとモニターを使用してアプライアンスを設定します。「[キーボードおよびモニターを使用した Firepower Management Center へのアクセス\(6 ページ\)](#)」を参照してください。
- 初期設定プロセスを実行します。「[Firepower Management Center の初期設定ウィザード\(7 ページ\)](#)」を参照してください。
- 必要に応じて、[スマートライセンス(Smart License)] ポップアップ ダイアログを使用してスマート ライセンスを設定します。「[\[スマートライセンス\(Smart Licensing\)\] ダイアログ\(9 ページ\)](#)」を参照してください。
- 初期設定プロセスが完了した後、シリアル アクセスまたは Serial over LAN(SoL)アクセス用に FMC を設定できます。「[コンソール出力のリダイレクト\(19 ページ\)](#)」および「[Lights-Out Management の設定\(21 ページ\)](#)」を参照してください。

設定が完了したら、Firepower Management Center Web インターフェイスを使用して、展開用のほとんどの管理タスクと分析タスクを実行します。詳細については、「[管理に関する推奨事項\(18 ページ\)](#)」を参照してください。

管理インターフェイスを使用した Firepower Management Center へのアクセス

FMC 管理インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前に設定されていますが、DHCP が利用されないシナリオでは、管理インターフェイスでは IPv4 アドレス 192.168.45.45 が使用されます。または、ライセンスとネットワークの設定を保持することを選択してシステムの復元を実行した後に、初めて FMC に接続した場合、IP アドレスは、システムの復元を実行する前のアドレスと同じになります。

はじめる前に:

- 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
- FMC の管理インターフェイスに割り当てられる IP アドレスを特定します。
 - ライセンスとネットワークの設定を保持することを選択してシステムの復元(「[工場出荷時の初期状態への Firepower Management Center の復元\(23 ページ\)](#)」を参照)を実行した後に、初めて FMC に接続した場合、IP アドレスは、システムの復元を実行する前のアドレスと同じになります。
 - それ以外の場合、FMC 管理インターフェイスの IP アドレスは 192.168.45.45 になります。

手順

1. 付属のイーサネット ケーブルを使用して、事前設定した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直接接続します。

リンク LED がローカル コンピュータ上のネットワーク インターフェイスおよびアプライアンス上の管理インターフェイスの両方にあることを確認します。

2. Web ブラウザを使用して、次のように、アプライアンスの IP アドレスに移動します。

`https://<管理 IP アドレス>`

ログイン ページが表示されます。

3. ユーザー名に `admin` を、パスワードに `Admin123` を使用して、Web インターフェイスにログインします (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)。

次の作業

- 「[Firepower Management Center の初期設定ウィザード \(7 ページ\)](#)」の手順に従って設定プロセスを完了します。

キーボードおよびモニターを使用した Firepower Management Center へのアクセス

アプライアンスに USB キーボードと VGA モニターを接続できます。これはキーボード、ビデオ、マウスの (KVM) スイッチに接続しているラックマウント型アプライアンスで便利です。FMC 管理インターフェイスは、DHCP によって割り当てられた IPv4 アドレスを受け入れるように事前に設定されていますが、DHCP リースの取得に失敗した場合、管理インターフェイスではフォールバック IPv4 アドレス 192.168.45.45 が使用されます。ネットワークで DHCP を使用しておらず、PC からこのアドレスに到達できない場合は、「[管理インターフェイスを使用した Firepower Management Center へのアクセス \(5 ページ\)](#)」の説明に従って、FMC に直接接続して初期設定を行うことをお勧めします。

はじめる前に:

FMC の管理インターフェイスに割り当てられる IP アドレスを特定します。

- 新しい FMC を初めて設定する場合は、ネットワーク管理者に問い合わせ、ローカル ネットワークへの接続時に DHCP によって FMC の MAC アドレスに割り当てられる IP アドレスを確認してください (MAC アドレスはアプライアンスのラベルまたは引き出しカードに記載されています)。
- DHCP が存在しない場合、または DHCP のプールに空きアドレスがない場合、FMC 管理インターフェイスでは、IP アドレス 192.168.45.45 が使用されます。このケースで、PC からこのアドレスに到達できない場合は、「[管理インターフェイスを使用した Firepower Management Center へのアクセス \(5 ページ\)](#)」の説明に従って、FMC に直接接続して初期設定を行うことをお勧めします。
- ライセンスとネットワークの設定を保持することを選択してシステムの復元 ([「工場出荷時の初期状態への Firepower Management Center の復元 \(23 ページ\)」](#)を参照) を実行した後に、初めて FMC に接続した場合、IP アドレスは、システムの復元を実行する前のアドレスと同じになります。

手順

1. 付属のイーサネット ケーブルを使用して、FMC 背面の管理インターフェイスを保護された管理ネットワークに接続します。
2. Web ブラウザを使用して、次のように、FMC Web インターフェイスのログイン ページに移動します。

`https://<管理 IP アドレス>`

ログイン ページが表示されます。

3. ユーザー名に `admin` を、パスワードに `Admin123` を使用して、Web インターフェイスにログインします。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。

次の作業

- 「[Firepower Management Center の初期設定ウィザード \(7 ページ\)](#)」の手順に従って設定プロセスを完了します。

Firepower Management Center の初期設定ウィザード

新しいアプライアンス、またはシステムの復元を実行したアプライアンスで、初めて FMC Web インターフェイスにログインすると、初期設定ウィザードが表示され、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 ダイアログで構成されています。

- 最初の画面では、`admin` ユーザー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 ユーザー 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。
- 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 Configuration Guide*』の「Device Management Basics」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。

パスワードの変更

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。[パスワードの変更 (Change Password)] ウィザード画面が表示され、次の 2 つのオプションから選択できます。

- [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。
- [パスワードの生成 (Generate Password)] ボタンをクリックして、示された条件に準拠するパスワードを自動的に作成します (生成されるパスワードはニーモニックではありません。このオプションを選択した場合は、念のためにパスワードをメモしてください)。

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。このウィザードでは、新しいパスワードが満たす必要がある条件のリストが表示されます。満たされた各条件の横には緑色のチェックマークが表示されます。新しいパスワードがリストの条件を 1 つでも満たしていない場合、そのパスワードは拒否され、次のページに進むことはできません。

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。

(注) [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。

シスコ エンド ユーザー ライセンス契約 (EULA)

Firepower Management Center を使用するには、初期設定ウィザードの 2 番目の画面に表示される EULA に同意する必要があります。EULA を読み、[同意する (Accept)] をクリックして続行します。[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。

ネットワーク設定の変更

初期設定ウィザードの最後の画面では、管理インターフェイス(eth0)を介したネットワーク通信のために FMC で使用するネットワーク設定を、必要に応じて変更できます。ネットワークとライセンスの設定を保持することを選択してシステムの復元を実行した後に初めてログインした場合は、システムの復元前に FMC で使用されていた設定と同じ値があらかじめ入力されています。

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 サーバー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 サーバーおよび NTP サーバー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 の接続テストは必須条件ではないため、接続テストが完了する前に、[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 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。

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。

次のフィールドの値を設定できます。

完全修飾ドメイン名

FQDN を指定する必要があります。次のいずれかを実行できます。

- 表示されている値をそのまま使用します(値が表示されている場合)。
- 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。

IPv4 設定用のブート プロトコル

[IPv4の設定 (Configure IPv4)] というドロップダウンから、次の IP アドレス割り当て方式のいずれかを選択します。

- DHCP の使用
- スタティック/手動の使用

IPv4 アドレス

このフィールドは必須です。表示されている値をそのまま使用するか(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)。

ネットワーク マスク

このフィールドは必須です。表示されている値をそのまま使用するか(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(255.255.0.0 など)。

ゲートウェイ

表示されているゲートウェイ値をそのまま使用するか(値が表示されている場合)、新しいデフォルト ゲートウェイ値を入力できます。ドット付き 10 進法形式を使用します(192.168.0.1 など)。

DNS Group

FMC のオプションのドメイン ネーム サーバー グループを選択します。次の操作を実行できます。

- デフォルト値の DNS Cisco Umbrella をそのまま使用します。

- ドロップダウン リストから [カスタムDNSサーバー (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。
- ドロップダウン リストから [カスタムDNSサーバー (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 サーバーを設定しません。

NTPグループサーバー (NTP Group Servers)

FMC と管理対象デバイスとの間で適切な同期を維持するためには、NTP サーバーを使用する必要があります。ドロップダウン リストから、次のいずれかを選択します。

- [デフォルトNTPサーバー (Default NTP Servers)]: デフォルトでは、プライマリ NTP サーバーとして `0.sourcefire.pool.ntp.org` が使用され、セカンダリ NTP サーバーとして `1.sourcefire.pool.ntp.org` が使用されます。
- [カスタムNTPサーバー (Custom NTP Servers)]: ネットワークから到達可能な 1 つまたは 2 つの NTP サーバーの FQDN または IP アドレスを入力します。

[スマートライセンス (Smart Licensing)] ダイアログ

初期設定ウィザードの [ネットワーク設定の変更 (Change Network Settings)] 画面で [終了 (Finish)] をクリックすると、スマート ライセンスをすばやく簡単に設定できるポップアップが表示されます。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。

自動初期設定

初期設定ウィザードの完了後、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ための週次メンテナンス作業が FMC によって自動的に設定されます。

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確認し、必要に応じて調整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 の更新を自動的にスケジュールします。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。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、お使いのソフトウェアバージョンの『*Firepower Management Center Configuration Guide*』の説明に従って、通常の GeoDB を更新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を自動的にスケジュールします。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。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、シスコの『*Firepower Management Center Upgrade Guide*』を参照してください。

■ FMC の週次設定バックアップ

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を自動的にスケジュールします。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となります。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。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

バージョン 6.6 以降では、FMC で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、お使いのバージョンの『*Firepower Management Center Configuration Guide*』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にかつ定期的に行われるように、タスクをスケジュールしておくことをお勧めします。

■ 侵入ルールの更新

バージョン 6.6 以降では、FMC で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。FMC では、次に影響を受けるポリシーを展開するときに、影響を受ける管理対象デバイスに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、この更新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、お使いのバージョンの『*Firepower Management Center Configuration Guide*』の説明に従って、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。

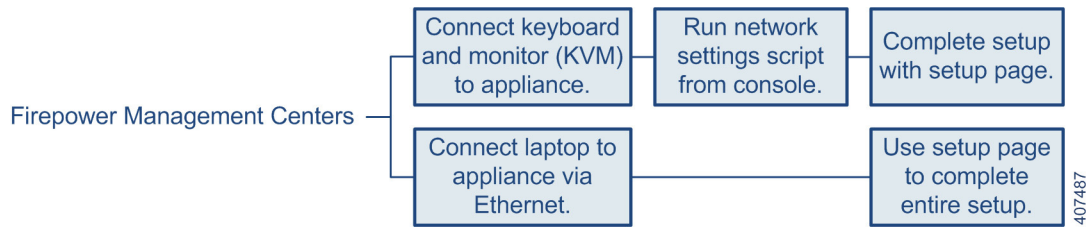
バージョン 5.4 ~ 6.4.x での設置と初期設定

Firepower バージョン 5.4 ~ 6.4.x は、本書に記載されているすべての FMC モデル (750、1500、2000、3500、および 4000) でサポートされています。

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

FMC Web インターフェイスに初めてログインすると、初期管理ページを使用して、信頼できる管理ネットワーク上で通信するように新しいアプライアンスを設定できます。また、管理者パスワードの変更、エンドユーザー ライセンス契約書 (EULA) への同意、時間の設定、および更新のスケジュールなどの初期管理レベル タスクも実行する必要があります。セットアップおよび登録時に選択されたオプションによって、システムで作成され、管理対象デバイスに適用されるデフォルト インターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

この初期設定プロセスを実行するために FMC にアクセスする際は、アプライアンスに直接接続されたラップトップを使用することも、信頼できるローカル管理ネットワークを介したイーサネット接続を使用することもできます。次の図に、Firepower バージョン 5.4 ~ 6.4.x を実行している FMC の設定時に選択可能な方法を示します。



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

(注) 工場出荷時設定に復元(「[工場出荷時の初期状態への Firepower Management Center の復元\(23 ページ\)](#)」を参照)後にアプライアンスを設定しており、アプライアンスのライセンスとネットワーク設定を削除していない場合は、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを直接閲覧しながら、設定を実行できます。「[初期設定ページ:Management Center\(13 ページ\)](#)」にスキップします。

バージョン 5.4 ~ 6.4.x を実行している FMC を設置および設定するための手順

1. 「[アプライアンスの設置\(4 ページ\)](#)」の説明に従って、アプライアンスを設置します。
2. FMC をネットワークに接続する前に、FMC の eth0 の IP アドレスをネットワークに合わせて変更してから、初期設定を実行する必要があります。次の 2 つの選択肢があります。
 - 初期設定を実行する前に、VGA/キーボード接続を使用して FMC にアクセスし、eth0 の IP アドレスを設定します。「[キーボードおよびモニターを使用した Firepower Management Center へのアクセス\(6 ページ\)](#)」を参照してください。
次に、Web ブラウザを使用して FMC にアクセスし、初期設定プロセスを実行します。「[初期設定ページ:Management Center\(13 ページ\)](#)」を参照してください。
 - eth0 インターフェイスからローカル コンピュータへの直接イーサネット接続を使用して、FMC にアクセスします。「[管理インターフェイスを使用した Firepower Management Center へのアクセス\(5 ページ\)](#)」を参照してください。
次に、Web ブラウザを使用して FMC にアクセスし、初期設定プロセスを実行して、そのプロセスの一部として eth0 の IP アドレスを設定します。「[初期設定ページ:Management Center\(13 ページ\)](#)」を参照してください。

アプライアンスの設置

次の手順は、アプライアンスを物理的に設置する手順の概要です。手順の詳細については、『*Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide*』を参照してください。

手順

1. 取り付けキットと付属の手順を使用して、アプライアンスをラックに取り付けます。
2. 電源コードをアプライアンスに接続し、電源に差し込みます。
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。
3. アプライアンスの電源をオンにします。

次の作業

- アプライアンスを設定するために、アプライアンスの物理管理インターフェイスにコンピュータを直接接続している場合は、「[管理インターフェイスを使用した Management Center のセットアップ\(12 ページ\)](#)」に移動します。

- アプライアンスを設定するために、キーボードとモニターを使用している場合は、「[キーボードおよびモニター \(KVM\) を使用した Management Center のセットアップ \(12 ページ\)](#)」に移動します。

管理インターフェイスを使用した Management Center のセットアップ

手順

1. 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(FMC 管理インターフェイスは、デフォルト IPv4 アドレスで事前に設定されています。ただし、設定プロセスの一部として、管理インターフェイスを IPv6 アドレスで再設定できます。)
2. 付属のイーサネット ケーブルを使用して、事前設定した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直接接続します。
リンク LED がローカル コンピュータ上のネットワーク インターフェイスおよびアプライアンス上の管理インターフェイスの両方にあることを確認します。
3. アプライアンスのデフォルトの IP アドレスに移動するには、Web ブラウザを使用します。
`https:// 192.168.45.45`
ログイン ページが表示されます。
4. ユーザー名として `admin` を、パスワードとして `Admin123` を使用してログインします。

次の作業

- 「[初期設定ページ: Management Center \(13 ページ\)](#)」の手順に従って設定プロセスを完了します。

キーボードおよびモニター (KVM) を使用した Management Center のセットアップ

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

はじめる前に

少なくとも、アプライアンスが管理ネットワーク上で通信するために必要な次の情報が手元にあることを確認してください。

- IPv4 または IPv6 管理 IP アドレス
- ネットマスクまたはプレフィックス長
- デフォルト ゲートウェイ

手順

1. 付属のイーサネット ケーブルを使用して、アプライアンス背面の管理インターフェイスを保護された管理ネットワークに接続します。
2. モニターを VGA ポートに、キーボードを USB ポートの 1 つに接続します。

3. ユーザー名として `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ることに注意してください)。お使いの Firepower バージョンに適した手順を使用します。「[FMC での CLI または Linux シェルへのアクセス \(3 ページ\)](#)」を参照してください。

4. 次のスクリプトを実行します。

```
sudo /usr/local/sf/bin/configure-network
```

次のプロンプト (現在値を伴う) が表示されます。

```
Management IP address?
```

5. 管理インターフェイスに割り当てる IP アドレスを入力するか、Enter キーを押して現在値を受け入れます。次に例を示します。

```
10.2.2.20
```

次のプロンプト (現在値を伴う) が表示されます。

```
Management netmask?
```

6. インターフェイスの IP アドレスのネットマスクを入力するか、Enter キーを押して現在値を受け入れます。次に例を示します。

```
255.255.255.0
```

次のプロンプト (現在値を伴う) が表示されます。

```
Management gateway?
```

7. インターフェイスの IP アドレスのゲートウェイを入力するか、Enter キーを押して現在値を受け入れます。次に例を示します。

```
10.2.1.1
```

次のプロンプトが表示されます。

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

8. 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` を入力して Enter を押します。情報を再度入力するように求められます。
9. 設定を承認した後、シェルからログアウトします。

次の作業

- 「[初期設定ページ: Management Center \(13 ページ\)](#)」の手順に従って設定プロセスを完了します。

初期設定ページ: Management Center

すべての Management Center に対して、Management Center の Web インターフェイスにログインして、設定ページで初期設定オプションを指定することによって、設定プロセスを完了する必要があります。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。

バージョン 5.4.x では、設定プロセスでデバイスの登録およびライセンス付与を行うこともできます。デバイスを登録する前に、Management Center をリモート マネージャとして追加するだけでなく、そのデバイス自体の設定プロセスを完了する必要があります。完了していない場合、デバイスの登録が失敗します。

手順

1. ブラウザで `https://mgmt_ip/` にアクセスします。ここで、`mgmt_ip` は Management Center 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 Management Center の場合は、そのコンピュータ上のブラウザでデフォルトの管理インターフェイスの IPv4 アドレス (`https://192.168.45.45/`) にアクセスします。

- ネットワーク設定がすでに構成されている Management Center の場合は、管理ネットワーク上のコンピュータを使用して、Management Center の管理インターフェイスの IP アドレスを閲覧します。

2. ユーザー名として `admin` を、パスワードとして `Admin123` を使用してログインします。

設定の完了方法については、次の項を参照してください。

- [パスワードの変更\(14 ページ\)](#)
- [ネットワーク設定\(15 ページ\)](#)
- [時刻設定\(15 ページ\)](#)
- [ルール更新の定期インポート\(15 ページ\)](#)
- [地理情報の定期的な更新\(15 ページ\)](#)
- [自動バックアップ\(16 ページ\)](#)
- [ライセンス設定\(16 ページ\)](#)
- [デバイスの登録\(17 ページ\)](#)
- [エンド ユーザー ライセンス契約\(18 ページ\)](#)

3. 完了したら、[適用(Apply)] をクリックします。

Management Center が選択内容に従って設定されます。管理者ロールを持つ `admin` ユーザーとして Web インターフェイスにログインします。

(注) イーサネット ケーブルを使用してデバイスに直接接続している場合は、コンピュータの接続を切断して、Management Center の管理インターフェイスを管理ネットワークに接続します。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 Management Center にアクセスし、このガイドの残りの手順を完了します。

4. 初期設定が正常に終了したことを確認します。

- 6.0 よりも前のバージョンでは、初期設定が正常に終了したことを確認するには、[タスクのステータス(Task Status)] ページ([システム(System)]>[モニタリング(Monitoring)]>[タスクのステータス(Task Status)])を使用します。ページは 10 秒ごとに自動的に更新されます。最初のデバイス登録およびポリシーの適用のタスクについて、[完了(Completed)] ステータスが表示されるまでページを監視します。設定の一部として、侵入ルールまたは位置情報の更新を設定した場合は、これらのタスクも監視することができます。
- バージョン 6.0 以降の場合、システム ステータスのアイコンをクリックして、メッセージセンターのタスク タブを表示します。

Management Center を使用する準備が整いました。展開の設定の詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

次の作業

- [「管理に関する推奨事項\(18 ページ\)」](#)に進みます。

セットアップ オプション

パスワードの変更

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

Cisco では、大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することを推奨しています。辞書に掲載されている単語の使用は避けてください。

(注) シェルによる Firepower Management Center へのアクセスと Web インターフェイスによる Firepower Management Center へのアクセスのための `admin` アカун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。

ネットワーク設定

Management Center 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。ネットワーク設定が完了している場合、このページのこのセクションは事前設定されていることがあります。

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

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

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

時刻設定

Management Center の時刻は、手動で設定することも、ネットワーク タイム プロトコル(NTP)サーバーから NTP 経由で設定することもできます。

また、admin アカウント用のローカル Web インターフェイスで使用されるタイムゾーンを指定することもできます。現在のタイムゾーンをクリックして、ポップアップ ウィンドウを使用してそれを変更します。

ルール更新の定期インポート

新たな脆弱性が発見されると、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。

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、Ciscoでは、[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 (Enable Recurring Rule Update Imports from the Support Site)] を選択することを推奨しています。

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 [ポリシーの再適用 (Policy Reapply)] 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)] を選択します。

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。

地理情報の定期的な更新

ほとんどの Firepower Management Center 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。

Management Center の地理情報データベース (GeoDB) には、IP アドレスに関連するインターネット サービス プロバイダー (ISP)、接続タイプ、プロキシ情報、正確な位置情報などの情報が含まれています。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なります。展開で地理情報システムに関連する分析の実行を計画する場合、Ciscoは [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)] を選択することを推奨しています。

GeoDB について、週次の更新頻度を指定できます。ポップアップ ウィンドウを使用してタイムゾーンを変更するには、そのタイムゾーンをクリックします。初期設定プロセスの一部としてデータベースをダウンロードするには、[今すぐインストール(Install Now)] を選択します。

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。

自動バックアップ

Firepower Management Center には、障害時に設定を復元できるように、データをアーカイブするためのしくみが用意されています。初期設定の一部として、**自動バックアップを有効にすることが**できます。

この設定を有効にすると、スケジュールされたタスクが作成され、このタスクによって Management Center の設定のバックアップが週次に作成されます。

ライセンス設定

Firepower Management Center を使用して、それ自身と管理対象デバイスのライセンスを管理できます。Firepower System で提供されるライセンスタイプは、管理するデバイスのタイプによって異なります。

- 7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv の各デバイスの場合は、クラシック ライセンスを使用する必要があります。クラシック 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。
- Firepower Threat Defense の物理デバイスとバーチャル 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。

クラシック ライセンスを Firepower Management Center に追加する前に、ライセンスの購入時にシスコから 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、サポートに問い合わせてください。

(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。Firepower Management Center の初期セットアップ中に、Firepower Management Center 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、ライセンスを有効にすることができます。

手順

1. 初期設定ページの [ライセンス設定(License Settings)] セクションからの初期設定中に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 です。

(注) [システム(System)] > [ライセンス(Licenses)] > [クラシック ライセンス(Classic Licenses)] ページで [ライセンスの新規追加(Add New License)] ボタンをクリックすると、いつでも Firepower Management Center でライセンス キーを検索できます。

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 (66:18:E7:6E:D9:93:35) と製品認証キー (PAK) の入力求められます。

(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。

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。
4. 検証ボックスに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。

次の作業

- 初期設定を続行します。

(注) Cisco Smart Licensing を使用するデバイスがある場合、[システム (System)] > [ライセンス (Licenses)] > [スマート ライセンス (Smart Licenses)] ページを使用してライセンスを追加および確認することができます。Firepower Management Center にスマート ライセンスを追加する方法の詳細については、そのデバイスの製品マニュアルを参照してください。『*Firepower Management Center Configuration Guide*』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。

デバイスの登録

Firepower Management Center は、現在 Firepower システム でサポートされているすべてのデバイス (物理または仮想) を管理できます。デバイスを Management Center に登録するには、デバイス上でリモート管理を設定する必要があります。

Firepower システム バージョン 6.0 以降を使用している場合は、『*Firepower Management Center Configuration Guide*』のデバイス管理情報でデバイスの登録手順を参照してください。

6.0 より前の Firepower システム バージョンを使用している場合は、初期設定プロセス中に、7000 および 8000 シリーズ デバイスを Management Center に追加できます。ただし、デバイスと Management Center が NAT デバイスによって分離されている場合は、設定プロセスが完了した後で、デバイスを追加する必要があります。『*Firepower 7000 and 8000 Series Installation Guide*』を参照してください。

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、同じ管理インターフェイスを使用するよう両方のトラフィック チャンネルを設定する必要があります。詳細については、『*Firepower 7000 and 8000 Series Installation Guide*』の「Deploying on a Management Network」を参照してください。

Management Center に管理対象デバイスを登録する際、登録時にアクセス制御ポリシーを自動的にデバイスに適用する場合は、[デフォルトのアクセスコントロールポリシーを適用する (Apply Default Access Control Policies)] チェックボックスをオンのままにしておきます。Management Center が各デバイスに対してどのポリシーを適用するかは、選択できません。選択できるのはポリシーを適用するかどうかのみであることに注意してください。次の表に示すように、それぞれのデバイスに適用されるポリシーは、デバイスの設定時に選択した検出モード (『*Firepower 7000 and 8000 Series Installation Guide*』の「Setting Up Firepower Managed Devices」を参照) によって異なります。

表 1 検出モードごとに適用されるデフォルトのアクセス コントロール ポリシー

検出モード	デフォルトのアクセス コントロール ポリシー
インライン	[デフォルト侵入防御 (Default Intrusion Prevention)]
パッシブ	[デフォルト侵入防御 (Default Intrusion Prevention)]
アクセス制御	[デフォルト アクセス制御 (Default Access Control)]
ネットワーク ディスカバリ	[デフォルト ネットワーク ディスカバリ (Default Network Discovery)]

Management Center を使用して以前にデバイスを管理しており、そのデバイスの最初のインターフェイス設定を変更すると、例外が発生します。このような場合、新しい Management Center のページによって適用されるポリシーは、変更した (現在の) デバイスの設定によって異なります。インターフェイスが設定されている場合、Management Center はデフォルト侵入防御ポリシーを適用します。そうでない場合は、Management Center が Default Access Control ポリシーを適用します。

デバイスがアクセス制御ポリシーに適合していない場合は、ポリシーの適用に失敗します。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。最初のアクセス コントロール ポリシーの適用が失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス コントロール ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

デバイスを追加するには、デバイスの登録時に指定した登録キーのほかに、ホスト名または IP アドレスを入力します。このキーは、長さが 37 文字以下で、ライセンス キーとは異なるシンプルなキーであることに注意してください。

次に、チェックボックスを使用して、ライセンスが付与された機能をデバイスに追加します。事前に Management Center に追加したライセンスしか選択できません。「[ライセンス設定\(16 ページ\)](#)」を参照してください。

すべてのライセンスがすべての管理対象デバイスでサポートされるわけではありません。ただし、設定 ページで、管理対象デバイス上でサポートされていないライセンスを有効にしたり、モデル固有のライセンスが付与されていない機能を有効にしたりすることは可能です。これは、Management Center はこの時点ではデバイス モデルを決定していないためです。システムは無効なライセンスを有効にすることはできません。また、無効なライセンスを有効にしようとしても、ユーザーが使用できるライセンス数は減少しません。

ライセンスを有効にした後で [追加(Add)] をクリックしてデバイスの登録設定を保存します。必要に応じてデバイスを追加します。間違ったオプションを選択した場合、またはデバイス名を誤って入力した場合は、[削除(Delete)] をクリックして削除します。その後で、デバイスをもう一度追加できます。

エンド ユーザー ライセンス契約

EULA をよく読んで、規定に従う場合はチェックボックスをオンにします。指定した情報がすべて正しいことを確認して、[適用(Apply)] をクリックします。

Management Center が選択内容に従って設定されます。管理者ロールを持つ admin ユーザーとして Web インターフェイスにログインします。Management Center の初期設定を完了するには、「[初期設定ページ: Management Center\(13 ページ\)](#)」の手順 3. に進みます。

管理に関する推奨事項

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

個別のユーザー アカウント

初期セットアップが完了した時点で、システム上の唯一のユーザーは、管理者ロールとアクセス権を持つ admin ユーザーです。このロールを所有しているユーザーは、シェルまたは CLI を介したアクセスを含め、システムのすべてのメニューおよび設定にアクセスできます。セキュリティおよび監査上の理由から、Cisco では、admin アカウント（および Administrator ロール）の使用を制限することを推奨しています。

(注) シェルによる Firepower Management Center へのアクセスと Web インターフェイスによる Firepower Management Center 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。

システムを使用する各ユーザーに対して個別のアカウントを作成すると、各ユーザー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、各ユーザーに関連付けられたユーザー 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 Management Center 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。

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

デバイス登録

すべての Firepower バージョンで、FMC の初期設定が完了した後に、デバイスを FMC に登録できます。

(注) 6.0 より前の Firepower システム バージョンを使用している場合は、初期設定プロセス中に、7000 および 8000 シリーズ デバイスを Management Center に追加できます。詳細については、「[デバイスの登録\(17 ページ\)](#)」を参照してください。

Firepower Management Center は、お使いのバージョンの Firepower システムで現在サポートされているすべてのデバイス(物理または仮想)を管理できます。お使いの Firepower のバージョンに応じて、これには以下が含まれます。

- Firepower 7000 および 8000 シリーズ アプライアンス: Firepower システム用に特別に設計された物理デバイス。Firepower 7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多数の同じ機能を共有します。一般に、8000 シリーズ デバイスは 7000 シリーズ デバイスよりも高性能で、8000 シリーズ 高速バス ルール、リンク集約、およびスタックなどの追加機能もサポートします。デバイスを Firepower Management Center に登録するには、デバイス上でリモート管理を設定する必要があります。
- NGIPSv: VMware vSphere 環境で展開する 64 ビットのバーチャル デバイス。NGIPSv のデバイスは、冗長性とリソースの共有、スイッチ、およびルーティングのようなシステムのハードウェアベースの機能のどちらもサポートしていません。
- Cisco ASA with FirePOWER Services (または ASA FirePOWER モジュール): 第一線システム ポリシーを提供し、検出とアクセス制御のために Firepower システムにトラフィックをパスします。ただし、Firepower Management Center の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Cisco ASA with FirePOWER Services には、ASA プラットフォームに一意なソフトウェアと CLI (コマンド ライン インターフェイス) があり、システムをインストールし、他のプラットフォーム固有の管理タスクを実行します。
- Firepower Threat Defense: 統合した次世代ファイアウォールと次世代 IPS デバイスを提供します。
- 仮想 Firepower Threat Defense: 複数のハイパーバイザ環境で作業し、管理オーバーヘッドを削減し、運用効率を向上させるために設計された 64 ビットのバーチャル デバイス。

Firepower Management Center に管理対象デバイスを登録するには、お使いのソフトウェア バージョンの『*Firepower Management Center Configuration Guide*』のデバイス管理情報を参照してください。Firepower デバイスとソフトウェア バージョンの互換性の詳細については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ヘルス ポリシーとシステム ポリシー

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

デフォルトで、Management Center にはヘルス ポリシーも適用されます。ヘルス ポリシーは、ヘルス モニタリング機能の一部として、システムが展開環境内でアプライアンスのパフォーマンスを継続して監視するための基準を提供します。Cisco では、Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアとデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。Cisco では、展開環境内のすべてのアプライアンスが Firepower システム の最新のバージョンを実行することを推奨しています。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。バージョン 6.5 以降では、これらの更新作業の一部は初期設定ウィザードによって自動的に設定されます。詳細については、「[自動初期設定\(9 ページ\)](#)」を参照してください。

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 ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

コンソール出力のリダイレクト

デフォルトで、Management Center 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 Cisco では推奨しています。

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

コンソール出力をリダイレクトするシェルの使用

手順

1. キーボード/モニターまたはシリアル接続を使用し、管理者特権を持つアカウントでアプライアンスのシェルにログインします。お使いの Firepower バージョンに適した手順を使用します。「[FMC での CLI または Linux シェルへのアクセス\(3 ページ\)](#)」を参照してください。

アプライアンスのプロンプトが表示されます。

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。

- VGA を使用してアプライアンスにアクセスする場合は、次のコマンドを入力します。

```
sudo /usr/local/sf/bin/configure_console.sh vga
```

- 物理シリアル ポートを使用してアプライアンスにアクセスする場合は、次のコマンドを入力します。

```
sudo /usr/local/sf/bin/configure_console.sh serial
```

- SOL 経由で LOM を使用してアプライアンスにアクセスする場合は、次のコマンドを入力します。

```
sudo /usr/local/sf/bin/configure_console.sh sol
```

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。

アプライアンスが再起動します。

コンソール出力をリダイレクトする Web インターフェイスの使用

手順

1. [管理(Administration)] > [設定(Configuration)] を選択します。

2. [コンソールの設定(Console Configuration)] を選択します。

3. リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。これがデフォルトのオプションです。
- アプライアンスのシリアル ポートを使用するか、または Management Center デバイス上で 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。

[物理シリアルポート (Physical Serial Port)] を選択した場合は、LOM の設定が表示されます。

4. SOL 経由で LOM を設定するには、次の該当する設定値を入力します。

- アプライアンスの DHCP 設定 ([DHCP] または [スタティック (Static)])
- LOM に使用する [IP アドレス (IP Address)]。LOM IP アドレスは、アプライアンスの管理インターフェイスの IP アドレスとは異なる必要があります。
- アプライアンスの [ネットマスク (Netmask)]
- アプライアンスの [デフォルトゲートウェイ (Default Gateway)]

5. [保存(Save)] をクリックします。

アプライアンスのリモート コンソール構成が保存されます。Lights-Out 管理を構成した場合は、少なくとも 1 人のユーザーに対してそれを有効にする必要があります。「[LOM および LOM ユーザーの有効化\(38 ページ\)](#)」を参照してください。

Lights-Out Management の設定

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

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

注意: Firepower Management Center 2000 および 4000 は、シスコのユニファイド コンピューティング システム (UCS) プラットフォームを Firepower System に導入しました。これらのモデルは、ベースボード管理コントローラ (BMC) 上で UCS Manager や Cisco Integrated Management Controller (CIMC) などのツールを使用して設定を変更したり、ファームウェアを更新したりするシスコの機能をサポートしていません。

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 2 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。
-U username	-U username	承認済み LOM アカウントのユーザー名を指定します。
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。 <ul style="list-style-type: none"> ■ IPMItool の場合、コマンドは最後に入力します。 ■ ipmiutil の場合、コマンドは最初に入力します。

IPMItool の場合:

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

ipmiutil の場合:

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

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

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

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

詳細については、次の項を参照してください。

- [LOM および LOM ユーザーの有効化\(38 ページ\)](#)
- [IPMI ユーティリティのインストール\(39 ページ\)](#)

LOM および LOM ユーザーの有効化

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

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

LOM ユーザーには、次のような制約もあります。

- ユーザーに Administrator ロールを割り当てる必要があります。
- ユーザー名には最大で 16 文字の英数字を使用できます。LOM ユーザーに対し、ハイフンやそれより長いユーザー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 ユーザーに対し、これよりも長いパスワードはサポートされていません。ユーザーの LOM パスワードは、そのユーザーのシステム パスワードと同じです。
- Management Center には、最大 13 人の LOM ユーザーを設定できます。

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

LOM を有効にするには:

1. [システム(System)] > [設定(Configuration)] を選択し、[コンソールの設定(Console Configuration)] をクリックします。
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。
3. LOM IP アドレス、ネットマスク、デフォルト ゲートウェイを指定します(または DHCP を使用してこれらの値を自動的に割り当てるようにします)。

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

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

1. [システム(System)] > [ユーザー管理(User Management)] を選択し、既存のユーザーを編集して 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ーを作成します。
2. [ユーザー設定(User Configuration)] ページで、[管理者(Administrator)] ロールがまだ有効になっていない場合は、このロールを有効にします。
3. [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。

IPMI ユーティリティのインストール

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

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

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

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

<http://ipmiutil.sourceforge.net/>

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

Cisco は、そのサポート サイトで、Firepower Management Center の工場出荷時設定の復元と再イメージ化のための ISO イメージを提供しています。

詳細については、次の項を参照してください。

- [はじめる前に \(23 ページ\)](#)
- [復元プロセスについて \(24 ページ\)](#)
- [復元 ISO と更新ファイルの入手 \(25 ページ\)](#)
- [復元プロセスの開始 \(26 ページ\)](#)
- [対話型メニューを使用したアプライアンスの復元 \(29 ページ\)](#)
- [次の手順 \(36 ページ\)](#)
- [Lights-Out Management の設定 \(37 ページ\)](#)

はじめる前に

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

バージョン 6.3 以降へのバージョン 5.x ハードウェアの再イメージ化

ISO イメージ名の変更により、バージョン 5.x を現在実行している Firepower 物理アプライアンスにバージョン 6.3 以降を新規インストールすることはできません。これには、このガイドに記載されている次の Firepower Management Center モデルが含まれます。

- 750、1500、1500
- 2000、4000

バージョン 6.3 以降への最短パスは次のとおりです。

1. バージョン 6.2.3 を新規インストールします。

2. バージョン 6.3+ を新規インストール(または バージョン 6.3+ にアップグレード)します。

(注) バージョン 5.x の Defense Center/Management Center をバージョン 6.2.3 の Firepower Management Center に再イメージ化した後、古いデバイスを管理することはできません。また、これらのデバイスを再イメージ化してから、Management Center に再度追加する必要があります。

ISO イメージ名の変更の詳細については、[Firepower リリース ノート](#)を参照してください。

設定とイベント バックアップのガイドライン

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

アプライアンスの工場出荷時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とイベント データが失われます。復元ユーティリティはアプライアンスのライセンス、ネットワーク、および一部の Lights-Out 管理 (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、モデルや Firepower のバージョンによって異なります。

- 750、1500、または 3500 の FMC モデルを工場出荷時の初期状態に復元する場合、ライセンスとネットワーク設定を削除すると LOM 設定もリセットされます。

注意: LOM を使用して 750、1500、または 3500 の FMC モデル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 FMC にアクセスできなくなります。

- 2000 または 4000 の FMC モデルを工場出荷時の初期状態に復元する場合
 - 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。

注意: LOM を使用して 2000 または 4000 の FMC モデルをバージョン 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、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 FMC にアクセスできなくなります。

復元プロセスにおけるトラフィック フロー

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

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

復元プロセスについて

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

アプライアンスの再イメージ化は、必ず保守期間中に行ってください。再イメージ化により、バイパス モードのアプリケーションは非バイパス設定にリセットされ、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、「[復元プロセスにおけるトラフィック フロー \(24 ページ\)](#)」を参照してください。

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

キーボードとモニター/KVM

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

シリアル接続/ラップトップ

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

Serial over LAN を使用した Lights-Out Management

Serial over LAN (SOL)接続による Lights-Out Management (LOM)を使用して、限定されたアクションのセットを Management Center と Firepower デバイス上で実行できます。アプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。LOM を使用してアプライアンスに接続した後で、物理シリアル接続を使用する場合と同様の方法で、復元ユーティリティに対してコマンドを発行します。Lights-Out Management は、デフォルト (`eth0`)の管理インターフェイスでのみ使用できることに注意してください。詳細については、[Lights-Out Management の設定\(37 ページ\)](#)を参照してください。

はじめる前に

- サポート サイトからアプライアンスの復元 ISO イメージを入手します。「[復元 ISO と更新ファイルの入手\(25 ページ\)](#)」を参照してください。
- Firepower Management Center を再イメージ化すると、シスコのライセンス認証局とのコンプライアンス違反 (OOC)状態になることがあります。ベスト プラクティスとして、Firepower Management Center を再イメージ化するときに、まず Cisco Smart Software Manager から Firepower Management Center の登録を取り消します。[システム (System)] > [ライセンス (Licenses)] > [スマート ライセンス (Smart Licenses)] を選択して、登録削除アイコンをクリックします。

Firepower デバイスを復元する方法:

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

次の作業

- 「[復元プロセスの開始\(26 ページ\)](#)」の手順に従って、ISO イメージをインストールします。

復元 ISO と更新ファイルの入手

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

アプライアンス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 Cisco 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(5.2、5.3 など)に関連付けられています。互換性のないバージョンのシステムをインストールしないようにするため、Cisco では、アプライアンスの最新 ISO イメージを常に使用することを推奨しています。

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

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

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

復元 ISO とその他の更新ファイルを手に入れるには:

1. サポート アカウントのユーザー名とパスワードを使用して、サポート サイト (<https://sso.cisco.com/auth/forms/CDClogin.html>) にログインします。
2. ソフトウェア ダウンロード セクション (<https://software.cisco.com/download/navigator.html>) を参照します。
3. ダウンロードしてインストールするシステム ソフトウェアで表示されるページの [検索 (Find)] 領域に検索文字列を入力します。
たとえば、Firepower のソフトウェア ダウンロードを検索するには、Firepower と入力します。
4. ダウンロードするイメージ (ISO イメージ) を見つけます。
ページの左側にあるリンクの 1 つをクリックして、ページの該当するセクションを表示します。たとえば、Firepower システム バージョン 6.0 のイメージとリリース ノートを表示するには、[6.0 Images] をクリックします。
5. ダウンロードする ISO イメージをクリックします。
ファイルのダウンロードが開始されます。
6. 管理ネットワーク上でアプライアンスがアクセスできる HTTP (Web) サーバー、FTP サーバー、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 または更新ファイルを転送しないでください。このように転送すると、ファイルが破損することがあります。また、ファイルの名前を変更しないでください。復元ユーティリティでは、ファイル名がサポート サイトでの名前と同一であることが必要です。

復元プロセスの開始

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

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

- **KVM または物理シリアル ポートを使用する復元ユーティリティの起動 (26 ページ)** では、LOM にアクセスできないアプライアンスでの復元プロセスの開始方法を説明します。
- **Lights-Out Management を使用した復元ユーティリティの開始 (28 ページ)** では、LOM を使用して SOL 接続経由で復元プロセスを開始する方法を説明します。

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

KVM または物理シリアル ポートを使用する復元ユーティリティの起動

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

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

アプライアンスを工場出荷時設定に復元する必要があるが、物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。「[Lights-Out Management を使用した復元ユーティリティの開始\(28 ページ\)](#)」を参照してください。

復元ユーティリティを開始するには:

1. キーボード/モニター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。「[FMC での CLI または Linux シェルへのアクセス\(3 ページ\)](#)」を参照してください。
2. 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。
3. 再起動の状況を監視します。
 - システムがデータベースの検査を実行している場合、次のメッセージが表示されることがあります。
The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.
 - キーボードとモニター接続を使用する場合は、矢印キーの 1 つを素早く繰り返し押します (アプライアンスが現在インストールされているバージョンのシステムを起動することを防ぐため)。
 - シリアル接続を使用する場合は、BIOS 起動オプションが表示されたら、Tab をゆっくりと繰り返し押します (アプライアンスが現在インストールされているバージョンのシステムを起動することを防ぐため)。
4. システムの応答は、ハードウェアモデルと接続のタイプによって次のように異なります。

モデル 750、1500、または 3500 の場合:

- キーボードとモニターの接続の場合:

赤色の LILO メニューに、現在のバージョンのシステムを起動する、標準コンソールを使用してシステムの復元を実行する ([System_Restore])、またはシリアル接続を使用してシステムの復元を実行する ([Restore_Serial]) ための 3 つのオプションが表示されます。矢印キーを使用して [System_Restore] を選択し、Enter を押します。

- シリアル接続の場合:

LILO boot プロンプトが表示されます。次に例を示します。

```
LILO 24.2 boot:
6.4.0          System_Restore      Restore_Serial
boot:
```

Restore_Serial と入力し、Enter を押します。

モデル 2000 および 4000 の場合:

- キーボードとモニターの接続の場合:

赤色の LILO メニューに、現在のバージョンのシステムを復元する、またはシステムの復元を実行する ([System_Restore]) ための 2 つのオプションが表示されます。矢印キーを使用して [System_Restore] を選択し、Enter を押します。

以下の選択項目の後に boot: プロンプトが表示されます。

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

0 と入力して Enter を押します。

- シリアル接続の場合:

LILO boot プロンプトが表示されます。次に例を示します。

```
LILO 24.2 boot:
```

```
6.4.0      System_Restore
boot:
```

System_Restore と入力し、Enter を押します。

以下の選択項目の後に boot: プロンプトが表示されます。

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

1 と入力して Enter を押します。

5. Enter キーを押して著作権情報を確認します。

6. 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、[Cisco Firepower アプライアンス<バージョン>設定メニュー (Cisco Firepower Appliance <Version> Configuration Menu)] が表示されるまでの一連のページで設定を確認します。

次の作業

- 「[対話型メニューを使用したアプライアンスの復元\(29 ページ\)](#)」に進みます。

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

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

注意: LOM を使用して 750、1500、または 3500 の FMC モデル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 FMC にアクセスできなくなります。

注意: LOM を使用して 2000 または 4000 の FMC モデルをバージョン 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、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 FMC にアクセスできなくなります。

(注) LOM を使用してアプライアンスを復元する前に、LOM を有効にする必要があります。「[Lights-Out Management の設定\(37 ページ\)](#)」を参照してください。

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

1. admin アカウントを使用して Linux シェルにアクセスします。お使いの Firepower バージョンに適した手順を使用します。「[FMC での CLI または Linux シェルへのアクセス\(3 ページ\)](#)」を参照してください。
2. コンピュータのコマンド プロンプトで、IPMI コマンドを入力して SoL セッションを開始します。

IPMItool では次のように入力します。

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

ipmiutil では次のように入力します。

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

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

3. 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。

4. 再起動状況の監視

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

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

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

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

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

以下の選択項目の後に boot プロンプトが表示されます。

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

6. 1 と入力して Enter キーを押します。アプライアンスのシリアル接続を介して対話型の復元メニューが読み込まれます。

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

7. Enter キーを押して著作権情報を確認します。

8. 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、[Cisco Firepowerアプライアンス<バージョン>設定メニュー (Cisco Firepower Appliance <Version> Configuration Menu)] が表示されるまでの一連のページで設定を確認します。

次の作業

- 「[対話型メニューを使用したアプライアンスの復元\(29 ページ\)](#)」に進みます。

対話型メニューを使用したアプライアンスの復元

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

(注) アプライアンスの再イメージ化は、必ず保守期間中に行ってください。再イメージ化により、バイパス モードのアプリケーションは非バイパス設定にリセットされ、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、「[復元プロセスにおけるトラフィック フロー\(24 ページ\)](#)」を参照してください。

メニューに表示されるオプションを次の表に示します。

表 3 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ー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 (31 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(31 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侵入ルールの更新(32 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(33 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。	復元プロセスの開始(33 ページ)
[6 設定の保存(6 Save Configuration)]	後で使用できるように復元設定のセットを保存するか、または保存されているセットを読み込みます。	復元設定の保存とロード(35 ページ)
7 設定の読み込み(7 Load Configuration)		
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 ドライブのスクラビング(42 ページ)

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

メニューには、2 種類のオプションが表示されます。

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

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

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

これが 2 回目のパスであるか、または使用する復元設定が復元ユーティリティにより自動的に読み込まれる場合は、メニュー オプション 4:「ISO および更新ファイルのダウンロードとイメージのマウント(33 ページ)」から開始できます。ただし Cisco は、操作を続行する前に復元設定の内容をダブルチェックすることを推奨しています。

(注) 以前に保存した設定を使用するには、メニュー オプション 6:「復元設定の保存とロード(35 ページ)」から開始します。設定を読み込んだら、メニュー オプション 4:「ISO および更新ファイルのダウンロードとイメージのマウント(33 ページ)」に進みます。

対話型メニューを使用してアプライアンスを復元するには:

1. [1 IPの設定(1 IP Configuration)]:「[アプライアンスの管理インターフェイスの指定\(31 ページ\)](#)」を参照してください。
2. [2 トランスポート プロトコルの選択(2 Choose the transport protocol)]:「[ISO イメージの場所および転送方式の指定\(31 ページ\)](#)」を参照してください。
3. [3 パッチ/ルール更新の選択(3 Select Patches/Rule Updates)](オプション):「[復元時のシステム ソフトウェアおよび侵入ルールの更新\(32 ページ\)](#)」を参照してください。
4. [4 ISOのダウンロードとマウント(4 Download and Mount ISO)]:「[ISO および更新ファイルのダウンロードとイメージのマウント\(33 ページ\)](#)」を参照してください。
5. [5 インストールの実行(5 Run the Install)]:「[復元プロセスの開始\(33 ページ\)](#)」を参照してください。

アプライアンスの管理インターフェイスの指定

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

アプライアンスの管理インターフェイスを指定するには:

1. 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。
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。
3. 管理ネットワークに使用するプロトコル([IPv4] または [IPv6]) を選択します。
管理インターフェイスに IP アドレスを割り当てるためのオプションが表示されます。
4. 管理インターフェイスに IP アドレスを割り当てる方法([スタティック (Static)] または [DHCP]) を選択します。
 - [スタティック (Static)] を選択した場合は、一連のページで、管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイを手動で入力するよう促されます。
 - [DHCP] を選択した場合は、管理インターフェイスの IP アドレス、ネットワーク マスクまたはプレフィックス長、およびデフォルト ゲートウェイがアプライアンスにより自動的に検出され、IP アドレスが表示されます。
5. プロンプトが表示されたら、設定を確認します。
プロンプトが表示されたら、アプライアンスの管理インターフェイスに割り当てられている IP アドレスを確認します。

次の作業

- 次の項([ISO イメージの場所および転送方式の指定](#))に進みます。

ISO イメージの場所および転送方式の指定

復元プロセスに必要なファイルをダウンロードするために使用される管理 IP アドレスを設定したら、次にアプライアンスの復元に使用する ISO イメージを指定する必要があります。これは、サポート サイト(「[復元 ISO と更新ファイルの入手\(25 ページ\)](#)」を参照)からダウンロードし、Web サーバー、FTP サーバー、または SCP 対応ホストに保存した ISO イメージです。

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

表 4 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	<ul style="list-style-type: none"> ■ Web サーバーの 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	<ul style="list-style-type: none"> ■ FTP サーバーの IP アドレス ■ 資格情報が使用されるユーザーのホーム 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 サーバーの認証ユーザー名とパスワード
SCP	<ul style="list-style-type: none"> ■ SCP サーバーの IP アドレス ■ SCP サーバーの認証ユーザー名 ■ 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ー名のパスワード <p>パスワードを入力する前に、アプライアンスから、信頼できるホストのリストに SCP サーバーを追加するよう求められることがある点に注意してください。続行するには、同意する必要があります。</p>

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

復元ファイルの場所および転送方式を指定するには:

1. 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。
2. 表示されるページで、[HTTP]、[FTP]、または [SCP] を選択します。
3. 復元ユーティリティにより表示される一連のページで、「表 4 (32 ページ)」の説明に従い選択したプロトコルに必要な情報を入力します。
情報が正しければ、アプライアンスはサーバーに接続し、指定された場所の Cisco ISO イメージのリストを表示します。
4. 使用する ISO イメージを選択します。
5. プロンプトが表示されたら、設定を確認します。
6. 復元プロセス中にシステム ソフトウェアまたは侵入ルールの更新をインストールしますか？
 - インストールする場合は、次の項 ([復元時のシステム ソフトウェアおよび侵入ルールの更新](#)) に進みます。
 - インストールしない場合は、「[ISO および更新ファイルのダウンロードとイメージのマウント \(33 ページ\)](#)」に進みます。復元プロセスが完了したら、システムの Web インターフェイスを使用して手動で更新をインストールできることに注意してください。

復元時のシステム ソフトウェアおよび侵入ルールの更新

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

復元ユーティリティは、1 つのシステム ソフトウェア更新と 1 つのルール更新だけを使用できます。ただしシステム更新は直前のメジャー バージョンに対して累積されます。ルール更新も累積されます。Cisco では、ご使用のアプライアンスに対して使用可能な最新の更新を入手することを推奨します。「[復元 ISO と更新ファイルの入手 \(25 ページ\)](#)」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。

復元プロセスの一環として更新をインストールするには:

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 (31 ページ)」を参照)で指定した場所とプロトコルを使用して、その場所にあるすべてのシステム ソフトウェア更新ファイルのリストを取得して表示します。SCP を使用する場合、更新ファイル リストを表示するためのプロンプトが表示されたらパスワードを入力します。

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

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

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

3. 使用するルール更新がわかっている場合は、それを選択します。

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

次の作業

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

ISO および更新ファイルのダウンロードとイメージのマウント

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

はじめる前に

- この手順を開始する前に、復元設定を後で使用できるように保存しておくことをお勧めします。詳細については、「復元設定の保存とロード (35 ページ)」を参照してください。

ISO イメージをダウンロードしてマウントするには:

1. 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。
2. プロンプトが表示されたら、選択項目を確認します。SCP サーバーからダウンロードする場合は、プロンプトが表示されたらパスワードを入力します。
該当するファイルがダウンロードされ、マウントされます。

次の作業

- 次の項(復元プロセスの開始)に進みます。

復元プロセスの開始

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

2つのパスのうちの1回目のパス(メジャーバージョンの変更のみ)

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

(注) アプライアンスを同じメジャーバージョンに復元する場合、またはこれがこのプロセスの2回目のパスの場合は、次の手順(「[2回目のパス、および1つのパスのみ\(34ページ\)](#)」)に進みます。

2パス復元プロセスの1回目のパスを実行するには、次の手順を実行します。

1. 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。
2. プロンプトが表示されたら(2回)、アプライアンスを再起動することを確認します。
3. 再起動を監視し、復元プロセスを再度開始します。

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

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

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

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

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

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

いずれの場合でも、以下の選択項目の後に boot プロンプトが表示されます。

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

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

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

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

6. Enter キーを押して著作権情報を確認します。

次の作業

- 「[対話型メニューを使用したアプライアンスの復元\(29ページ\)](#)」を参照してプロセスの2回目のパスを開始します。

2回目のパス、および1つのパスのみ

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

復元プロセスの 2 回目のパスまたは 1 つだけのパスを実行するには:

1. 2 パス復元プロセスの 2 回目のパスを実行している場合、「[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 \(33 ページ\)](#)」の説明に従い、ISO イメージを再度ダウンロードしてマウントします。
2. 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。
3. アプライアンスを復元することを確認し、次のステップに進みます。
4. 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、初期設定プロセスが短くなる可能性があるため、これらの設定は削除しないでください。復元とそれに続く初期設定の後に設定を変更する場合、通常は、これらの設定を今リセットするよりも時間がかかりません。詳細については、「[次の手順 \(36 ページ\)](#)」を参照してください。

注意: LOM を使用して 750、1500、または 3500 の FMC モデル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 FMC にアクセスできなくなります。

注意: LOM を使用して 2000 または 4000 の FMC モデルをバージョン 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、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 FMC にアクセスできなくなります。

5. アプライアンス復元の最終確認を入力します。

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

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

(注) 再イメージ化により、バイパス モードのアプリケーションは非バイパス設定にリセットされ、バイパス モードを再設定するまではネットワーク上のトラフィックが中断されます。詳細については、「[復元プロセスにおけるトラフィック フロー \(24 ページ\)](#)」を参照してください。

次の作業

- 「[次の手順 \(36 ページ\)](#)」に進みます。

復元設定の保存とロード

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

- アプライアンスの管理インターフェイスに関するネットワーク情報。「[アプライアンスの管理インターフェイスの指定 \(31 ページ\)](#)」を参照してください。
- 復元 ISO イメージの場所と、アプライアンスがファイルをダウンロードするために必要とする転送プロトコルおよび資格情報。「[ISO イメージの場所および転送方式の指定 \(31 ページ\)](#)」を参照してください。
- アプライアンスを ISO イメージのベース バージョンに復元した後で適用するシステム ソフトウェアと侵入ルールの更新 (存在する場合)。「[復元時のシステム ソフトウェアおよび侵入ルールの更新 \(32 ページ\)](#)」を参照してください。

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

復元設定を保存するのに最適なタイミングは、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。

復元設定を保存するには:

1. 復元ユーティリティのメイン メニューから、[6 設定の保存 (6 Save Configuration)] を選択します。
ユーティリティにより、保存する設定の設定内容の設定が表示されます。
2. プロンプトが表示されたら、設定を保存することを確認します。
3. プロンプトが表示されたら、設定の名前を入力します。

次の作業

- 保存された設定を使用してアプライアンスを復元する場合は、「[ISO および更新ファイルのダウンロードとイメージのマウント \(33 ページ\)](#)」に進みます。

保存された復元設定を読み込むには:

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。
2. 使用する設定を選択します。
ユーティリティにより、読み込む設定の設定内容が表示されます。
3. プロンプトが表示されたら、設定を読み込むことを確認します。
設定が読み込まれます。プロンプトが表示されたら、アプライアンスの管理インターフェイスに割り当てられている IP アドレスを確認します。

次の作業

- 読み込まれた設定を使用してアプライアンスを復元する場合は、「[ISO および更新ファイルのダウンロードとイメージのマウント \(33 ページ\)](#)」に進みます。

次の手順

アプライアンスの工場出荷時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とイベント データが失われます。ライセンスおよびネットワーク設定を削除すると、LOM 設定もリセットされる場合があることに注意してください。

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

- 750、1500、または 3500 の FMC モデルを工場出荷時の初期状態に復元する場合、ライセンスとネットワーク設定を削除すると LOM 設定もリセットされます。

注意: LOM を使用して 750、1500、または 3500 の FMC モデル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 FMC にアクセスできなくなります。

- 2000 または 4000 の FMC モデルを工場出荷時の初期状態に復元する場合
 - アプライアンスをバージョン 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。
 - アプライアンスをバージョン 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。

注意: LOM を使用して 2000 または 4000 の FMC モデルをバージョン 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、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 FMC にアクセスできなくなります。

アプライアンスの復元後に、初期設定プロセスを実行する必要があります。

- アプライアンスのライセンスおよびネットワーク設定を削除していない場合は、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを直接参照し、設定を実行できます。詳細については、次を参照してください。
 - バージョン 5.4.x ~ 6.4.x の場合は、「[初期設定ページ: Management Center \(13 ページ\)](#)」を参照してください。
 - バージョン 6.5 以降の場合は、「[Firepower Management Center の初期設定ウィザード \(7 ページ\)](#)」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、次を参照してください。
 - バージョン 5.4.x ~ 6.4.x の場合は、「[バージョン 5.4 ~ 6.4.x での設置と初期設定 \(10 ページ\)](#)」を参照してください。
 - バージョン 6.5 以降の場合は、「[バージョン 6.5 以降での設置と初期設定 \(4 ページ\)](#)」を参照してください。
- Cisco Smart Software Manager から Firepower Management Center の登録を取り消したら、Cisco Smart Software Manager にアプライアンスを登録します。[システム(System)], [ライセンス(Licenses)], [スマート ライセンス(Smart Licenses)] の順に選択して、登録アイコンをクリックします。

初期設定プロセスの完了後:

- シリアル接続または SOL/LOM 接続を使用してアプライアンスのコンソールにアクセスする場合は、コンソール出力をリダイレクトする必要があります。「[コンソール出力のリダイレクト \(19 ページ\)](#)」を参照してください。
- 復元中に LOM がリセットされ、LOM を使用する場合は、機能を再度有効にし、1 つ以上の LOM ユーザーを有効にする必要があります。「[LOM および LOM ユーザーの有効化 \(38 ページ\)](#)」を参照してください。

Lights-Out Management の設定

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

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

注意: Firepower Management Center 2000 および 4000 は、シスコのユニファイド コンピューティング システム (UCS) プラットフォームを Firepower System に導入しました。これらのモデルは、ベースボード管理コントローラ (BMC) 上で UCS Manager や Cisco Integrated Management Controller (CIMC) などのツールを使用して設定を変更したり、ファームウェアを更新したりするシスコの機能をサポートしていません。

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 5 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。
-l lanplus	-J3	LOM セッションの暗号化を有効にします。

表 5 LOM コマンド構文 (続き)

IPMItool(Linux/Mac)	ipmiutil(Windows)	説明
-H <i>IP_address</i>	-N <i>IP_address</i>	アプライアンスの管理インターフェイスの IP アドレスを指定します。
-U <i>username</i>	-U <i>username</i>	承認済み LOM アカウントのユーザー名を指定します。
適用対象外(ログオン時に求められます)	-P <i>password</i>	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。 <ul style="list-style-type: none"> ■ IPMItool の場合、コマンドは最後に入力します。 ■ ipmiutil の場合、コマンドは最初に入力します。

IPMItool の場合:

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

ipmiutil の場合:

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

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

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

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

詳細については、次の項を参照してください。

- [LOM および LOM ユーザーの有効化\(38 ページ\)](#)
- [IPMI ユーティリティのインストール\(39 ページ\)](#)

LOM および LOM ユーザーの有効化

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

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

LOM ユーザーには、次のような制約もあります。

- ユーザーに Administrator ロールを割り当てる必要があります。
- ユーザー名には最大で 16 文字の英数字を使用できます。LOM ユーザーに対し、ハイフンやそれより長いユーザー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 ユーザーに対し、これよりも長いパスワードはサポートされていません。ユーザーの LOM パスワードは、そのユーザーのシステム パスワードと同じです。
- Management Center には、最大 13 人の LOM ユーザーを設定できます。

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

LOM を有効にするには:

1. [システム(System)] > [設定(Configuration)] を選択し、[コンソールの設定(Console Configuration)] をクリックします。
2. LOM IP アドレス、ネットマスク、およびデフォルト ゲートウェイを指定する(または DHCP を使用してこれらの値を自動的に割り当てる)前に、[物理シリアル ポート(Physical Serial Port)] を使用してリモート アクセスを有効にします。

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

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

1. [システム(System)] > [ユーザー管理(User Management)] を選択し、既存のユーザーを編集して 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ーを作成します。
2. [ユーザー設定(User Configuration)] ページで、[管理者(Administrator)] ロールがまだ有効になっていない場合は、このロールを有効にします。
3. [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。

IPMI ユーティリティのインストール

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

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

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

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

<http://ipmiutil.sourceforge.net/>

Firepower Management Center 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 Management Center 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。

- 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。
- 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。

- 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。

はじめる前に

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。

必須の事前設定の情報

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 サーバーの 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 サーバーの IP アドレス

オプションの事前設定情報

次のようないくつかのデフォルト設定を変更できます。

- アプライアンスの時間を手動で設定する場合は、時間帯を設定します。
- 自動バックアップに使用するリモート ストレージ ロケーションを設定します。
- Lights-Out 管理 (LOM) を有効にするための LOM IP アドレスを設定します。

(注) 電源の再投入のシナリオによっては、管理インターフェイス経由でネットワークに接続された 3D7050 のベースボード管理コントローラ (BMC) は、DHCP サーバーによって割り当てられた IP アドレスを消失する可能性があります。このため、Cisco では 3D7050 BMC をスタティック IP アドレスで設定することを推奨しています。ネットワークケーブルの切断と再接続やデバイスの電力遮断と再投入により、リンクの再ネゴシエーションを強制的に行うことができます。

時間管理の事前設定

次の考慮事項に注意します。

- Cisco では、物理的 NTP サーバーと時間を同期することを推奨します。
- 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 サーバーおよび NTP サーバーにアクセスできる場合は、ターゲット ロケーションの DNS サーバーおよび NTP サーバーの IP アドレスを使用します。それ以外の場合は、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。

- 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、『*Firepower Management Center Configuration Guide*』を参照してください。

システムのインストール

「バージョン 5.4 ~ 6.4.x での設置と初期設定 (10 ページ)」および「アプライアンスの設置 (11 ページ)」で説明するインストール手順を使用してください。詳細については、『*Cisco Firepower Management Center 750, 1500, 2000, 3500, および 4000 ハードウェア インストールガイド*』を参照してください。

システムを事前設定する際には、以下に注意してください。

- 管理対象デバイスのライセンスは、初期設定時に追加します。この時点でライセンスを追加しない場合は、初期設定時に登録したデバイスが Management Center にライセンスなしとして追加されます。初期設定プロセスの完了後に、各デバイスに個別にライセンスを付与する必要があります。「[ライセンス設定 \(16 ページ\)](#)」を参照してください。

アプライアンスの移送の準備


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、アプライアンスを再梱包します。

- アプライアンスの電源を安全にオフにするには、『*Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide*』を参照してください。
- アプライアンスの移送の準備が完了したことを確認するには、「[移送に関する考慮事項 \(41 ページ\)](#)」を参照してください。

Management Center からのライセンスの削除

何らかの理由でライセンスを削除する必要がある場合は、次の手順を使用します。Cisco は、各 Management Center 固有のライセンス キーに基づいてライセンスを生成するため、ある Management Center でライセンスを削除し、そのライセンスを別の Management Center で再利用することはできない点に注意してください。詳しくは、『*Firepower Management Center Configuration Guide*』の「Firepower システム」を参照してください。

ライセンスを削除するには:

1. [システム (Systems)] > [ライセンス (Licenses)] を選択します。
2. 削除するライセンスの横にある削除アイコン () をクリックします。
ライセンスを削除すると、そのライセンスを使用するすべてのデバイスから、ライセンスされている機能が削除されます。たとえば、Protection ライセンスが有効であり、100 台の管理対象デバイスに対して有効化されている場合は、このライセンスを削除すると、この 100 台のデバイスすべてから保護機能が削除されます。
3. ライセンスを削除することを確認します。
ライセンスが削除されます。

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、そのアプライアンス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。「[初期設定ページ: Management Center \(13 ページ\)](#)」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 ポートの管理については、ご使用のファイアウォールのマニュアルを参照してください。必要なオープン ポートについては、『*Firepower Management Center Configuration Guide*』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。

ハードドライブのスクラビング

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

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

標準規格

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

注意: ハードドライブのスクラビング処理では、アプライアンスのすべてのデータが失われ、動作不能であると示されます。

ハードドライブのスクラビングは、「[対話型メニューを使用したアプライアンスの復元 \(29 ページ\)](#)」で説明されているインタラクティブ メニューのオプションを使用して行います。

ハードドライブのスクラビング処理を行うには:

1. 以下のいずれかの項の説明に従い、復元ユーティリティの対話型メニューを表示します。これは、アプライアンスへのアクセス方法に応じて異なります。
 - [KVM または物理シリアル ポートを使用する復元ユーティリティの起動 \(26 ページ\)](#)
 - [Lights-Out Management を使用した復元ユーティリティの開始 \(28 ページ\)](#)
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。
3. プロンプトが表示されたら、ハードドライブをスクラビング処理することを確認します。

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

関連資料

Cisco Firepower Management Center シリーズの文書とその入手先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。

<https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>

このドキュメントは、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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016-2020 Cisco Systems, Inc. All rights reserved.

翻訳について

このドキュメントは、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。