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

最終更新日： 2019 年 2 月 8 日

このマニュアルの構成は、次のとおりです。

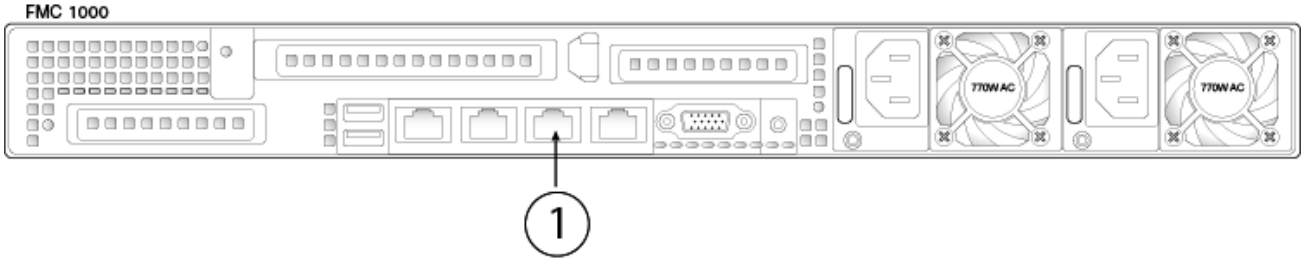
パッケージの内容

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

シャーシ モデル

- Firepower Management Center 1000（1U モデル）。次のシャーシ背面パネル図は、Firepower Management Center 1000 の管理インターフェイスの位置を示しています。

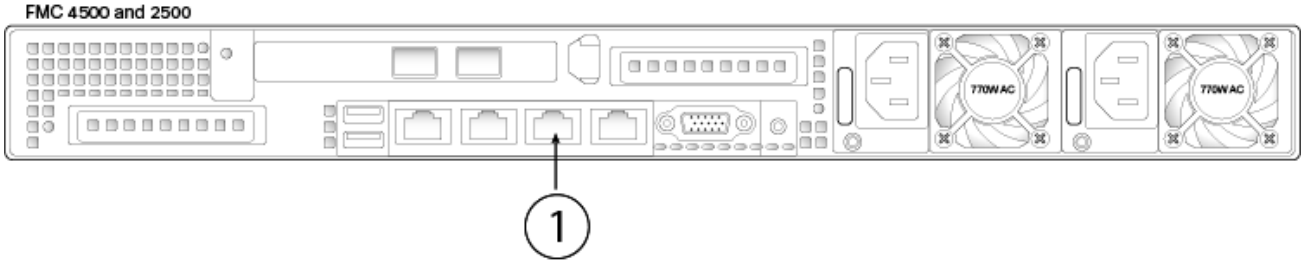
図 1　Firepower Management Center 1000 のシャーシおよび管理インターフェイス



1	管理インターフェイス		

- Firepower Management Center 2500/4500（1U モデル）。次のシャーシ背面パネル図は、管理インターフェイスの位置を示しています。

図 2　Firepower Management Center 2500 および Firepower Management Center 4500



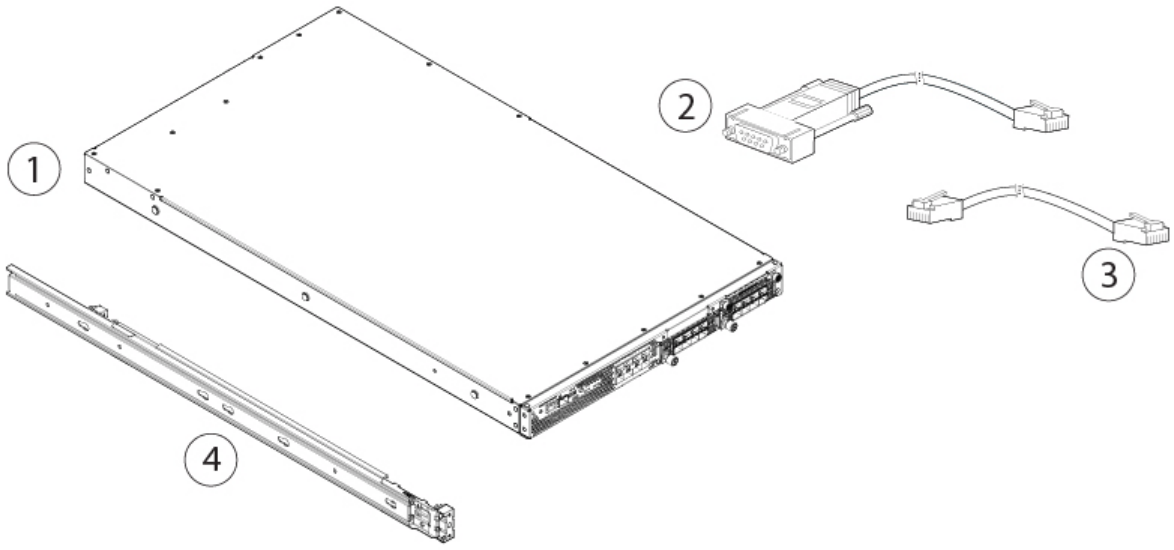
1	管理インターフェイス		

付属品

次の一覧と図は、Cisco Firepower Management Center モデル 1000、2500、および 4500 のパッケージの内容を示しています。この内容は変更される場合があるため、実際に含まれているアイテムは多かったり、少なかったりする場合があることにご注意ください。

1. Cisco Firepower Management Center シャーシ
2. RJ45 to DP9-RS232 コンソール ケーブル（Cisco製品番号 72-3383-XX）
3. RJ45 to RJ45 Cat 5 イーサネット ケーブル、黄色、長さ 6 フィート（Cisco製品番号 72-1482-XX）
4. Cisco 1RU レール キット（Cisco製品番号 800-43376-XX）

図 3　Cisco Firepower Management Center モデル 1000、2500、および 4500 のパッケージの内容



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。

Cisco では、初期設定ページを使用して、組織で購入したライセンスを追加することを推奨しています。ライセンス設定（8 ページ）を参照してください。ライセンスをここで追加しない場合は、初期設定プロセスが終了するまで管理対象デバイスのライセンスを追加する必要があります。初期設定プロセス中またはその後にライセンスを追加するかどうかで、Firepower Management Center にこれらを登録するとき、または Firepower Management Center にこれらを登録した後に、管理対象デバイスにライセンスを割り当てることができます。再イメージ化されたアプライアンスを設定しており、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、このセクションが事前生成されていることがあることに注意してください。

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。

シスコ スマート ライセンスによって、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。

Firepower Management Center への接続

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

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

キーボードとモニタ/KVM

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

管理インターフェイスへのイーサネット接続

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

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

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

Firepower Management Center の初期セットアップ

Firepower Management Center を展開して設置したら、その新しいアプライアンスが信頼できる管理ネットワーク上で通信できるように設定プロセスを完了する必要があります。また、管理者パスワードを変更し、エンドユーザ ライセンス契約書(EULA)に同意する必要もあります。

設定プロセスを使用すると、時間の設定および更新のスケジューリングなどのさまざまな管理レベル タスクを実行することもできます。設定と登録中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。

設定を開始する前に、次の要件を満たしているかどうかを確認してください。

アクセス

新しいアプライアンスを設定するには、キーボードとモニタ/KVM(キーボード、ビデオ、およびマウス)またはアプライアンスの管理インターフェイスへの直接イーサネット接続を使用して接続する必要があります。初期設定後は、アプライアンスをシリアル アクセス用に設定できます。詳細については、*Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide*を参照してください。

ネットワークと展開の情報

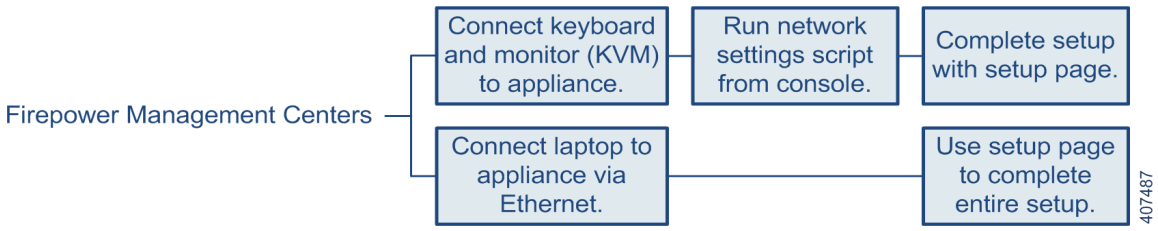
少なくとも、アプライアンスが管理ネットワーク上で通信できるようにするために必要な情報(IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイ)は入手しておきます。

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

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、次の手順(9 ページ)を参照してください。

(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(12 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。Firepower Management Center の初期設定ページ(6 ページ) にスキップします。

次の図に、Firepower Management Center の設定時に選択可能な設定を示します。



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 Firepower Management Center の設定(5 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を使用している場合は、キーボードおよびモニタを使用した Firepower Management Center の設定(5 ページ)に移動します。

管理インターフェイスを使用した Firepower Management Center の設定

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. 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。

3. 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。

次の作業

- Firepower Management Center の初期設定ページ（6 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を使用した Firepower Management Center の設定

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. ユーザ名に `admin` を、パスワードに `Admin123` を使用してコマンドライン 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。
4. 次のスクリプトを実行します。

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

5. 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。
6. 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)?
   ```

   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。

7. 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

- Firepower Management Center の初期設定ページ（6 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 の初期設定ページ

すべての Firepower Management Center に対して、Firepower 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。

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 Firepower 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 Firepower 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 Firepower 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、Firepower 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（7 ページ）
   - ネットワーク設定（7 ページ）
   - 時刻設定（7 ページ）
   - ルール更新の定期インポート（7 ページ）
   - 地理情報の定期的な更新（8 ページ）
   - 自動バックアップ（8 ページ）
   - ライセンス設定（8 ページ）
   - エンド ユーザ ライセンス契約（9 ページ）
3. 完了したら、[適用（Apply）] をクリックします。

   Firepower Management Center は、選択の内容に従って設定を適用してサマリ ダッシュボード ページを表示し、`admin` ユーザ（管理者ロールがあります）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、Firepower 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 Firepower 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. タスクのステータスをモニタすることによって、初期設定が成功したことを確認します。
   - バージョンが 6.0 より前の場合、[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。
   - バージョンが 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。

   Firepower 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

- 次の手順（9 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 アカウントのパスワードを変更する必要があります。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。

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。

ネットワーク設定

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

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

時刻設定

Firepower 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

新しい脆弱性が発見されると、脆弱性調査チーム(VRT)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。

Firepower 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（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することができます。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 Firepower 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 の初期設定中、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）] ページから [ライセンスの新規追加（Add New License）] ボタンをクリックするときに、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。

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。

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。

エンド ユーザ 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。

Firepower Management Center は設定を適用して、[サマリ ダッシュボード(Summary Dashboard)] ページを表示します。管理者ロールを持つ admin ユーザとして Web インターフェイスにログインします。Firepower Management Center の初期設定を完了するには、Firepower Management Center の初期設定ページ(6 ページ) の手順 3. に進みます。

次の手順

アプライアンスの初期設定プロセスが完了し、正常に終了したことが確認できたら、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、ライセンスの取得など、初期設定で省略したタスクも完了する必要があります。以降のセクションで説明するタスクの詳細について、および展開の設定を始める方法については、『*Firepower Management Center Configuration Guide*』を参照してください。

個別のユーザ アカウント

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、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 Firepower 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、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。また、特別なアクセス権限を持つカスタム ユーザ ロールを作成することもできます。

デバイス登録

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。

- 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 高速パス 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、『*Firepower Management Center Configuration Guide*』のデバイスの管理情報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、Firepower Management Center を使用して、それ自身およびその管理対象デバイスすべてに同じシステム ポリシーを適用することを推奨しています。

デフォルトで、Firepower Management Center にはヘルス ポリシーも適用されます。ヘルス ポリシーは、ヘルス モニタリング機能の一部として、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、Firepower Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェア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。

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、Firepower 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。
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 ポートに転送するには:

     ```
     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 ポートに転送するには:

     ```
     sudo /usr/local/sf/bin/configure_console.sh serial
     ```
   - コンソール メッセージを SOL に転送するには(LOM 使用時):

     ```
     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 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 人のユーザに対してそれを有効にする必要があります。LOM および LOM ユーザの有効化(24 ページ)を参照してください。

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

Cisco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

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

設定とイベント 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設定を復元すると、アプライアンスのほぼ**すべての**設定とイベント データが失われます。復元ユーティリティはアプライアンスのライセンス、ネットワーク、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、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。

注意: LOM を使用して FMC をバージョン 6.3 以降に復元しているときに、アプライアンスへの物理的なアクセス権がない状態でライセンス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。

復元プロセスについて

Firepower Management Center 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。

メンテナンス ウィンドウの間でのみアプライアンスを再イメージ化します。

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

キーボードとモニタ/KVM

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

シリアル接続/ラップトップ

アプライアンスにコンピュータを接続するためにアプライアンス（Cisco製品番号 72-3383-XX）によって提供される RJ45 to DP9-RS232 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 Firepower Management Center 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（23 ページ）を参照してください。

（注）Lights-Out Management を使用して Firepower Management Center 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。

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（14 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 Management Center を復元するには：

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（14 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（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、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 Management Center 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。

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実行することを推奨します。アプライアンスをサポートされる最新メジャー バージョンに復元した後で、システム ソフトウェア、侵入ルール、脆弱性データベース（VDB）を更新する必要があります。詳細については、適用する更新のリリース ノートと『*Firepower Management Center 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 6.2 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 6.2.0.1 に更新できます。ルール更新は Firepower Management Center だけで必要であることに注意してください。

復元 ISO とその他の更新ファイルを入手するには：

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

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

   ページの左側にあるリンクの 1 つをクリックして、ページの該当するセクションを表示します。たとえば、Firepower システム バージョン 6.2.0 のイメージとリリース ノートを表示するには、[6.2.0. イメージ（6.2.0 Images）] をクリックします。
5. ダウンロードする ISO イメージをクリックします。

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

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（15 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（16 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 Management Center では、Ciscoは内部フラッシュ ドライブに復元ユーティリティを組み込んで提供しています。

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（16 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。デフォルトでは、これによってシェルへのアクセス権が付与されます。Firepower Management Center の CLI が有効になっている場合（6.3 以降のバージョンでサポートされます）、これによって CLI へのアクセス権が付与されます。
2. CLI が有効になっている Firepower Management Center では（6.3 以降のバージョンでサポートされます）、`expert` コマンドを入力してシェルにアクセスします。
3. 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。
4. 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。
5. 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。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。

   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（17 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 FMC をバージョン 6.3 以降に復元しているときに、アプライアンスへの物理的なアクセス権がない状態でライセンス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 を使用してリンクを Firepower Management Center を復元する前に、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。Lights-Out Management の設定（23 ページ）を参照してください。

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

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

   IPMItool では次のように入力します。

   ```
   sudo ipmitool -I lanplus -H IP_address -U admin 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 admin -P password
   ```

   ここで、*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、*password* 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。

2. CLI が有効になっている Firepower Management Center では（6.3 以降のバージョンでサポートされます）、`expert` コマンドを入力してシェルにアクセスします。
3. 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。
4. 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。
5. 復元ユーティリティの対話型メニューの表示モードに入力するように求められます。2 と入力して Enter を押し、アプライアンスのシリアル接続で対話型復元メニューをロードします。

   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。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。

   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（17 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 Management Center 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) メンテナンス ウィンドウの間でのみアプライアンスを再イメージ化します。

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 1 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(18 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(19 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(20 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(20 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(21 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。	復元設定の保存とロード(22 ページ)
[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(28 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 回目のパスで復元イメージを更新し、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(20 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(22 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(20 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(18 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(19 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(20 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(20 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(21 ページ)を参照してください。

アプライアンスの管理インターフェイスの指定

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

アプライアンスの管理インターフェイスを指定するには:

1. 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

復元プロセスで必要なファイルをダウンロードするために使用される管理 IP アドレスを設定したら、次にアプライアンスの復元に使用する ISO イメージを指定する必要があります。これは、サポート サイト（復元 ISO と更新ファイルの入手（14 ページ）を参照）からダウンロードし、Web サーバ、FTP サーバ、または SCP 対応ホストに保存した ISO イメージです。

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

表 2 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
SCP	■ SCP サーバの IP アドレス ■ SCP サーバの認証ユーザ名 ■ ISO イメージ ディレクトリのフル パス ■ 先に入力したユーザ名のパスワード パスワードを入力する前に、アプライアンスから、信頼できるホストのリストに SCP サーバを追加するよう求められることがある点に注意してください。続行するには、同意する必要があります。

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

復元ファイルの場所および転送方式を指定するには：

1. 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 2（-19 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. 復元プロセスの一部としてシステムのソフトウェアまたは侵入ルールの更新を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」を続行します。インストールしている場合は、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（20 ページ）に進んでください。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 Firepower 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（14 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（19 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（22 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 回目のパスで復元イメージを更新し、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 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(21 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:

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. 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、一連のページで設定を確認します。
4. Enter キーを押して著作権情報を確認します。

次の作業

- 次の項で記載されている、プロセスの 2 番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(20 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、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。詳細については、次の手順(23 ページ)を参照してください。

注意: LOM を使用して FMC をバージョン 6.3 以降に復元しているときに、アプライアンスへの物理的なアクセス権がない状態でライセンス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）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。

次の作業

- 次の手順（23 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 Management Center を再び復元する必要が生じた場合に使用します。復元ユーティリティは最後に使用された設定を自動的に保存しますが、次のような複数の設定を保存することもできます。

- アプライアンスの管理インターフェイスに関するネットワーク情報。アプライアンスの管理インターフェイスの指定（18 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（19 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（20 ページ）を参照してください。

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

復元設定を保存するのに最適なタイミングは、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（20 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（20 ページ）に進みます。

次の手順

Firepower Management Center の工場出荷時設定を復元すると、アプライアンスのほぼ**すべての**設定とイベント データが失われます。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、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。

注意: LOM を使用して FMC をバージョン 6.3 以降に復元しているときに、アプライアンスへの物理的なアクセス権がない状態でライセンス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、Firepower Management Center の初期設定ページ（6 ページ）を参照してください。
- ライセンスとネットワーク設定を削除している場合は、アプライアンスを新品の場合と同様に設定する必要があります。最初に、管理ネットワークと通信するように設定します。Firepower Management Center への接続（3 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」（10 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 ユーザを有効にする必要があります。LOM および LOM ユーザの有効化（24 ページ）を参照してください。

Lights-Out Management の設定

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。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、アウトオブバンド管理接続でコマンド ライン インターフェイスを使用して、シャーシ シリアル番号の確認や、ファン速度や温度などの状況の監視といった作業を行うことができます。

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

表 3　　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、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
```

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。

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

詳細については、次の項を参照してください。

- LOM および LOM ユーザの有効化（24 ページ）
- IPMI ユーティリティのインストール（25 ページ）

LOM および LOM ユーザの有効化

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

各アプライアンスのローカル Web インターフェイスを使用して、アプライアンスごとに LOM と LOM ユーザを設定します。つまり、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。

LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名には最大で 16 文字の英数字を使用できます。LOM ユーザに対し、ハイフン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。
- Firepower Management Center には、最大 13 人の LOM ユーザを設定できます。

  (注) 以下の作業の詳細については、『*Firepower Management Center 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 ユーザに対して LOM 機能を有効にするには:

1. [システム(System)] > [ユーザ管理(User Management)] を選択し、既存のユーザを編集して LOM 許可を追加するか、またはアプライアンスへの LOM アクセスに使用する新規ユーザを作成します。
2. [ユーザ設定(User Configuration)] ページで、[管理者(Administrator)] ロールがまだ有効になっていない場合は、このロールを有効にします。
3. [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 Firepower 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。

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。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

Firepower Management Center の初期セットアップ（4 ページ）およびFirepower Management Center への接続（3 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 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

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、アプライアンスの電源オフ（28 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が完了したことを確認するには、移送に関する考慮事項（28 ページ）を参照してください。

Firepower 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 Firepower 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 Firepower Management Center でライセンスを削除し、そのライセンスを別の Firepower 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「Licensing the 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）]、[クラシック ライセンス（Classic Licenses）] の順に選択します。
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。

アプライアンスの電源オフ

電源を取り外す前に、次の手順に従ってアプライアンスの電源を安全にオフにします。

Firepower Management Center の電源を切るには:

1. Firepower Management Center で、コマンド ラインに次のように入力します。

```
sudo shutdown -h now
```

Firepower Management Center が安全にシャット ダウンします。

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。Firepower Management Center の初期設定ページ(6 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

Firepower Management Center 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（17 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（15 ページ）
   - Lights-Out Management を使用した復元ユーティリティの開始（16 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 シリーズの文書とその入手先についての完全な一覧については、次の URL にある文書のロードマップを参照してください。

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