Cisco Secure Firewall Management Center 1700、2700、および4700スタートアップガイド

初版：2023 年 11 月 28 日

最終更新：2022 年 7 月 12 日

Cisco Secure Firewall Management Center 1700、2700、および 4700 について

Management Center は、Threat Defense デバイスの管理を一元化し、統合し、合理化します。さらに、アプリケーション制御、侵入防御システム（IPS）、URL フィルタリング、およびマルウェア保護機能も備えています。大規模なネットワークの導入では一般に、複数の管理対象 Threat Defense デバイスがネットワークセグメントにインストールされます。各デバイスは、トラフィックを制御、検査、監視、および分析して、Management Center に報告します。

Cisco Secure Firewall Management Center 1700、2700、および 4700 アプライアンスは、優れたパフォーマンスと高い効率性を実現します。

このドキュメントでは、Management Center のケーブル接続と初期設定の実施方法を説明します。

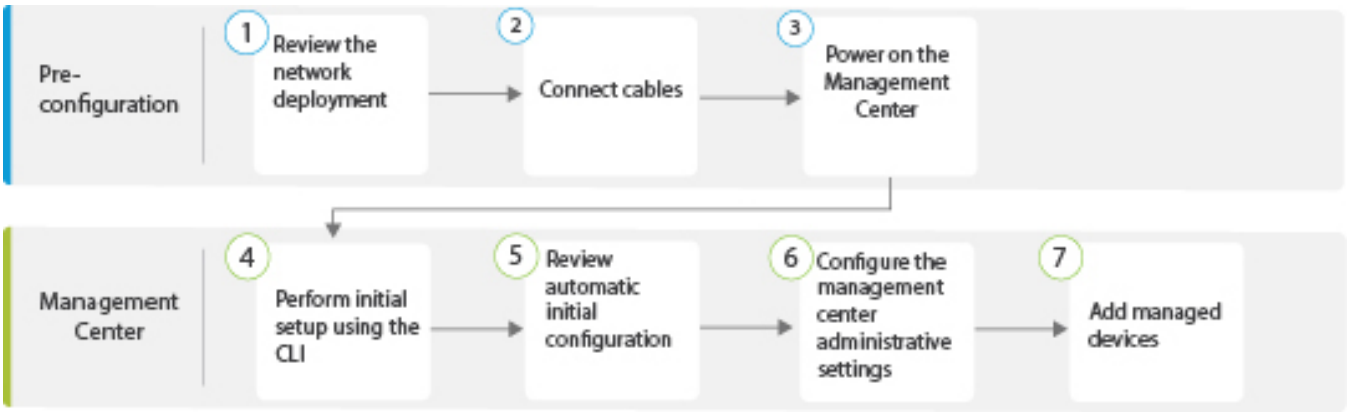
はじめる前に

Management Center をインストールします。詳細については、『*Cisco Secure Firewall Management Center 1700, 2700 and 4700 Hardware Installation Guide*』を参照してください。

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

エンドツーエンドの手順

次のフローチャートは、Management Center を展開して設定するタスクのフローを示しています。

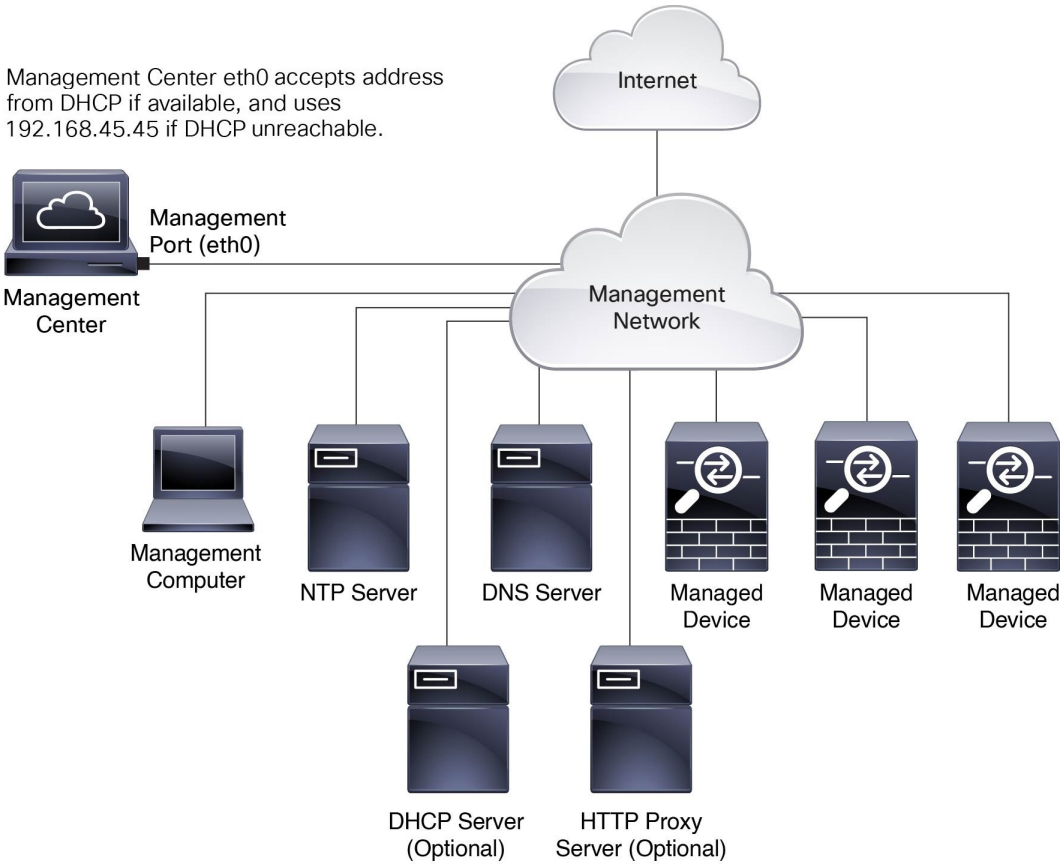


1	事前設定	ネットワーク展開の確認 （2 ページ）
2	事前設定	Management Center のケーブル接続 （5 ページ）
3	事前設定	Management Center の電源を入れる （7 ページ）
4	Management Center	CLI を使った Management Center の初期設定の実行 （9 ページ）
5	Management Center	自動初期設定の確認 （15 ページ）
6	Management Center	Management Center 管理設定の設定 （17 ページ）
7	Management Center	Management Center への管理対象デバイスの追加 （18 ページ）

ネットワーク展開の確認

Management Center を展開する前に、運用環境に関する情報が必要です。

次の図に、Management Center の一般的なネットワーク展開を示します。



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

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

システムソフトウェアの更新、脆弱性データベース（VDB）、地理位置情報データベース（GeoDB）、および侵入ルールを、インターネット接続を介して、またはインターネットからこれらの更新を取得したローカルコンピュータから、Management Center に直接アップロードできます。

Management Center といずれかの管理対象デバイスの間で接続を確立するには、少なくとも 1 つのデバイス（Management Center または管理対象デバイス）の IP アドレスが必要です。可能であれば両方の IP アドレスを使用することをお勧めします。ただし、知っている IP アドレスは 1 つだけです。たとえば、管理対象デバイスが NAT の背後にあるプライベートアドレスを使用している可能性があるため、ユーザーは Management Center アドレスしか知りません。こ

の場合は、管理対象デバイス上の Management Center アドレスと、ユーザーが選択した 1 回限り使用可能な一意のパスワード（NAT ID と呼ばれる）を指定できます。Management Center では、管理対象デバイスを識別するために同じ NAT ID を指定します。

このドキュメントで説明する初期セットアップおよび設定は、Management Center がインターネットにアクセスできることを前提としています。エアギャップ環境に Management Center を展開する場合、HTTP 通信用のプロキシ設定やスマートライセンス用の Smart Software Satellite Server の使用などの特定の機能をサポートするために使用できる別の方法については、ご使用のバージョンの『Cisco Secure Firewall Management Center アドミニストレーション ガイド』を参照してください。

Management Center の初期ネットワーク設定

- 管理インターフェイス

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

（注） DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、 Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更から回復するには、Management Center に接続し（ホスト名または新しい IP アドレスを使用）、**システム**（⚙）> **[構成（Configuration）]** > [管理インターフェイス（Management Interfaces）] の順に選択してネットワークをリセットします。

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

- DNS サーバ

  最大 2 つの DNS サーバーの IP アドレスを指定します。評価ライセンスを使用している場合は、DNS を使用しないことを選択できます。

（注） 初期設定時にホスト名とドメインを指定して、DNS を介した Management Center と他のホストの通信を容易にすることもできます。初期セットアップの完了後に追加のドメインを設定できます。

- NTP サーバ

初期設定時に、Management Center とその管理対象デバイスのシステム時刻を同期します。デフォルト（0.sourcefire.pool.ntp.org と 1.sourcefire.pool.ntp.org をそれぞれプライマリ NTP サーバーとセカンダリ NTP サーバーとして使用）を受け入れるか、ネットワークから到達可能な 1 つまたは 2 つの信頼できる NTP サーバーの FQDN または IP アドレスを指定することができます。DNS を使用しない場合、FQDN を使った NTP サーバーの指定はできません。

Management Center のケーブル接続

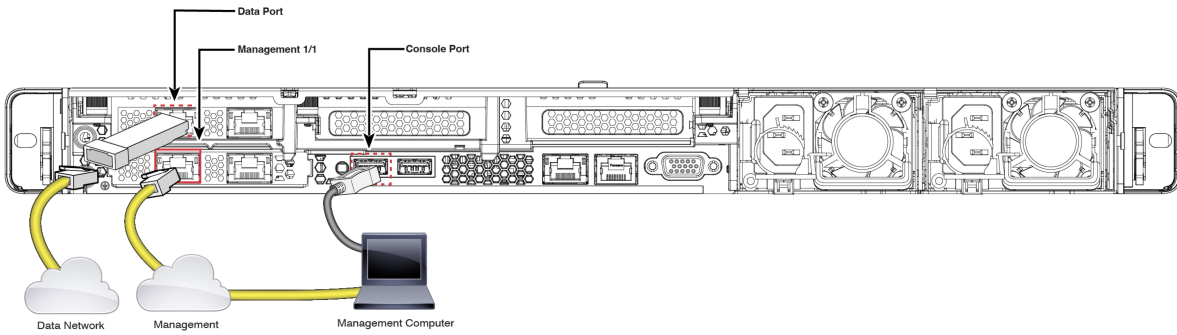
次に示す 3 つの接続のいずれか（または複数）を使用して、Management Center にケーブル接続できます。

- キーボードを USB ポートに、モニターを Management Center の VGA ポートに接続します。デフォルトでは、Management Center のコンソールメッセージは VGA ポートに送信されます。
- Management Center の **CIMC** ポートを Lights-Out Management の IPMI ユーティリティを実行できるローカルコンピュータから到達可能なローカルネットワークに接続します。この接続を使用するには、Light-Out Management の設定 （20 ページ）を参照してください。
- 下の手順に従って、ローカルコンピュータを Management Center のシリアルポートに接続します。

AC 電源装置は内部アースがあるため、サポート対象の AC 電源コードを使用する場合は、それ以上シャーシのアース接続は必要ありません。対応する電源コードの詳細については、『*Cisco Secure Firewall Management Center 1700, 2700 and 4700 Hardware Installation Guide*』を参照してください。

シャーシをラックに取り付けたら、次の手順に従ってケーブルを接続します。

図 *1*: アプライアンスと管理ネットワークのケーブル接続



始める前に

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

『*Cisco Secure Firewall Management Center 1700, 2700, and 4700 Hardware Installation Guide*』に記載されているように、アプライアンスをラックに設置します。

コンソールポートとローカルコンピュータを使用してアプライアンスをケーブル接続する場合は、コンソール出力をコンソールポートにリダイレクトします。詳細については、Web インターフェイスを使用したコンソール出力のリダイレクト （12 ページ）およびCLI を使用したコンソール出力のリダイレクト （13 ページ）を参照してください。

手順

ステップ 1 次のように管理ネットワークにケーブルを配線します。

- Management 1/1 インターフェイス
- 管理コンピュータ

ステップ 2 RJ-45/DB-9 コンソールケーブルを使用して、管理コンピュータをコンソールポートに接続します。コンソールポートを使用して CLI にアクセスし、初期設定を行います。

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

ステップ 4 （任意） サポートされている SFP+ トランシーバとケーブルを、Management Center 1700、2700、および 4700 の 10 ギガビットイーサネット SFP+ インターフェイス（データポート）、または Management Center 4700 の 25 ギガビットイーサネット SFP+ インターフェイスに取り付けます。ネットワーク要件に応じて、このインターフェイスを他の管理インターフェイスと同じか、または異なるネットワークに接続します。

（注） サポートされている SFP+ トランシーバのみを使用することを推奨します。1700、2700、および 4700 でサポートされる SFP の詳細については、『*Cisco Secure Firewall Management Center 1700, 2700 and 4700 Hardware Installation Guide*』を参照してください。

次のタスク

1. Management Center の電源を入れる （7 ページ）
2. CLI を使った Management Center の初期設定の実行 （9 ページ）

Management Center の電源を入れる

Management Center 1700、2700、および 4700 アプライアンスは、1050 W の AC 電源を使用します。電源および対応する電源コードの詳細については、『*Cisco Firepower Management Center 1700, 2700, and 4700 Hardware Installation Guide*』を参照してください。

始める前に

デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。シャーシをシャットダウンすることなく電源が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。

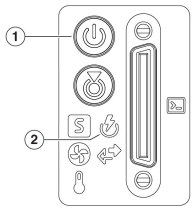
手順

ステップ 1 サポート対象の電源コードの 1 つを使用して、シャーシの電源装置を電源に接続します。

（注） Management Center の両方の電源装置を電源に接続することを推奨します。電源装置が 1 つだけ接続されている場合、アプライアンスはヘルスアラートを生成します。

ステップ 2 シャーシ前面にある電源ボタン（図中の「**1**」）を押し、電源ステータス LED（図中の「**2**」）がオンになっていることを確認します。

図 *2:* 電源ボタンと電源ステータス *LED*



Management Centerでの CLI または Linux シェルへのアクセス

⚠

注意 Cisco 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。

始める前に

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

手順

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

この方法でログインすることで、Management Center CLI にアクセスできます。

ステップ 2 **show version** コマンドを使用して Management Center のソフトウェアバージョンを検証します。

例：

```
> show version
-----------[ firepower ]------------
Model                 : Cisco Firewall Management Center 4700 (66) Version 7.4.0 (Build
 1482)
UUID                   : a10ed34e-d127-11e8-b440-728439d95305
Rules update version   : 2023-11-15-001-vrt
LSP version            : lsp-rel-20231115-1600
VDB version            : 375
----------------------------------------------------
```

ステップ 3 Management Center 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。

Management Center のシャットダウンまたは再起動

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

Management Center CLI から **system shutdown** コマンドを使用して Management Center をシャットダウンすることもできます

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

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

手順

ステップ 1 Management Center にログインし、**システム**（⚙）>[設定（Configuration）]>[プロセス（Process）] を選択します。

ステップ 2 次のいずれかを実行します。

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

CLI を使った Management Center の初期設定の実行

CLI を使用して初期設定を実行することもできます。初期構成ウィザードを完了させ、信頼できる管理ネットワークで通信するように新しいアプライアンスを設定する必要があります。

始める前に

- Management Center のケーブル接続 （5 ページ）の説明に従って、Management Center にケーブルを接続します。
- Management Center が管理ネットワーク上で通信するための、次の情報がそろっていることを確認してください。
  - IPv4 管理 IP アドレス
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）
- 次の 3 つの方法のいずれかで Management Center に接続します。
  - USB キーボードと VGA モニターを Management Center に接続してコンソールにアクセスします。
  - RJ-45 DP-9 コンソールケーブルを使用して、ローカルコンピュータを Management Center のシリアルポートに接続します。
  - 上記の 2 つの方法で IP を設定した後、セキュアシェル（SSH）を使用してデバイスにアクセスし、IPv4 管理 IP アドレスを使用して Management Center に接続します。

手順

ステップ 1 **admin** アカウントのユーザー名に **admin** を、パスワードに **Admin123** を使用して、コンソールで Management Center にログインします。パスワードでは大文字と小文字が区別されます。

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

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

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

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

（注） Management Center 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、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』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、2 つのパスワードは同じではなくなります。すると、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の要件を削除できます。

ステップ 5 ネットワークの設定を行います。

プロンプトに従って進めると、（**y/n**）のようにオプションがカッコ内に表示されます。デフォルト値は、**[y]** のように角カッコ内に列挙されます。プロンプトに入力する際は、次の点に注意してください。

- 工場出荷時の初期状態に復元した後にアプライアンスを設定し、アプライアンスのライセンスおよびネットワーク設定を削除しなかった場合、プロンプトには保持されている値が事前に入力されます。
- Enter を押して、デフォルトを受け入れます。
- ホスト名に関しては、完全修飾ドメイン名（<hostname>.<domain>）またはホスト名を入力します。このフィールドは必須です。
- DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Management Center ネットワー

ク設定が同期しなくなるため、デバイスの登録は失敗します。DHCPアドレスの変更から回復するには、Management Centerに接続し（ホスト名または新しいIPアドレスを使用）、**システム**（⚙）>**[構成（Configuration）]**>[管理インターフェイス（Management Interfaces）] の順に選択してネットワークをリセットします。

- IPv4を手動で設定することを選択した場合、IPv4アドレス、ネットマスク、およびデフォルトゲートウェイの入力が求められます。
- DNS サーバーの設定はオプションです。DNS サーバーを指定しない場合は **none** を入力します。それ以外の場合は、1 つまたは 2 つの DNS サーバーに IPv4 アドレスを指定します。2 つのアドレスを指定する場合は、カンマで区切ります。3 つ以上の DNS サーバーを指定した場合、システムは追加のエントリを無視します。Management Center にインターネットアクセスがない場合は、ローカルネットワークを出て DNS を使用できません。

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

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

例：

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

ステップ 6 設定を確認します。システムによって、設定の概要が表示されます。

例：

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

ステップ 7 正しく設定されているか確認します。

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

例：

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

Updated network configuration.
```

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

次のタスク

- 設定したネットワーク情報を使用して Management Center の Web インターフェイスに接続します。
- 初期設定プロセスの一環として、Management Center で自動的に設定される週次メンテナンスアクティビティを確認します。このアクティビティは、システムを最新の状態に保ち、データをバックアップする目的で設計されています。詳細については、自動初期設定の確認 （15 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初期セットアップを完了した後で、Management Center の IPv6 アドレッシングを設定します。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイドを参照してください。
- （オプション）Light-Out Management の設定 （20 ページ）の説明に従って、Management Center の SOL または LOM アクセスを設定します。

Web インターフェイスを使用したコンソール出力のリダイレクト

この手順を実行するには、管理者ユーザーである必要があります。

始める前に

- アプライアンスの初期設定プロセスを完了します。
- デバイスの管理インターフェイスに接続されたサードパーティスイッチング装置で、スパニングツリープロトコル（STP）を無効にします。

手順

ステップ 1 **システム**（⚙） > [設定（Configuration）] の順に設定します。

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

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- （デフォルト）アプライアンスの VGA ポートを使用するには、[VGA] を選択します。

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

ステップ 4 [保存（Save）] をクリックします。

CLI を使用したコンソール出力のリダイレクト

始める前に

Management Center の初期セットアッププロセスを完了します。

手順

ステップ 1 Management Center CLI **admin** ログイン情報を使用して、Management Center の Linux シェルにアクセスします。詳細については、Management Centerでの CLI または Linux シェルへのアクセス （7 ページ）を参照してください。

ステップ 2 プロンプトで、以下のいずれかのコマンドを使って、コンソール出力を設定します。

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

ステップ 3 変更を反映させるには、**sudo reboot** コマンドを使ってアプライアンスを再起動します。

CLI 管理者パスワードのリセット

Management Center CLI にアクセスするための管理者アカウントのパスワードを変更できます。

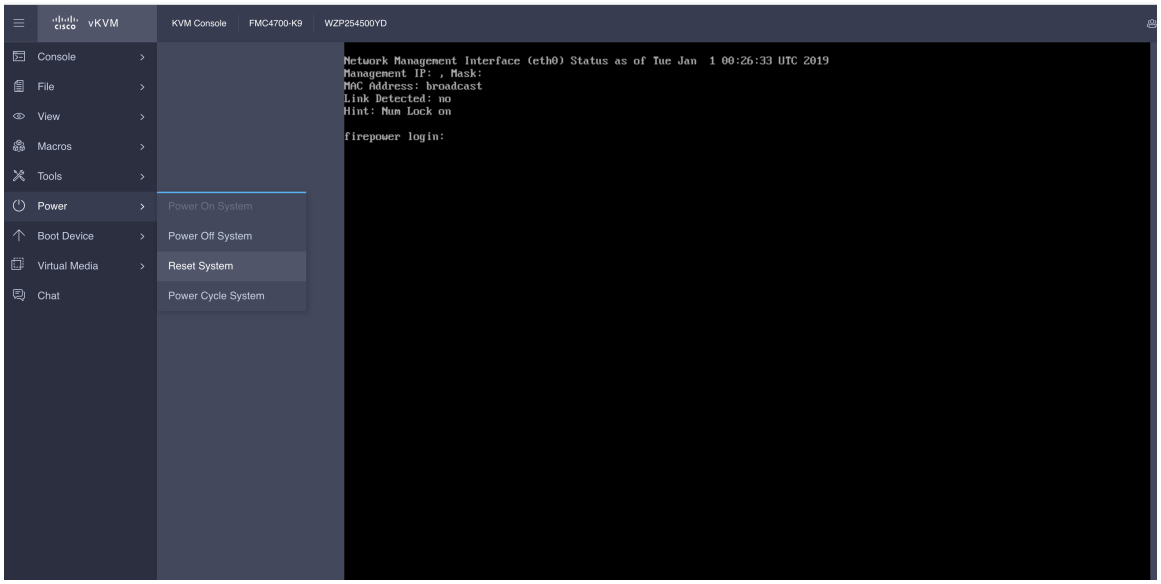
始める前に

管理者パスワードをリセットするには、アプライアンスとのコンソール接続を確立する必要があります。

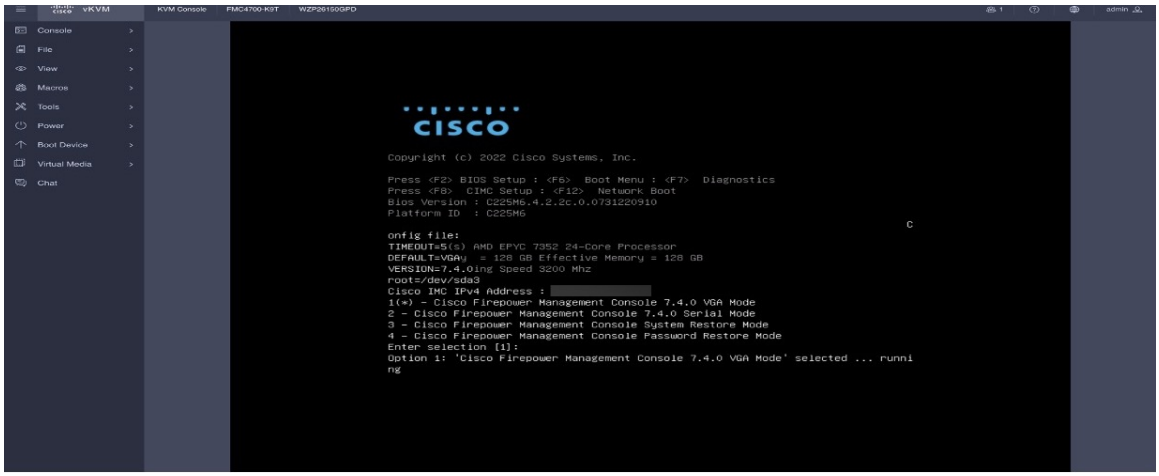
手順

ステップ 1 Management Center CLI 管理者ユーザーとしてログインします。

ステップ 2 コンソールで、[電源（Power）] > [システムのリセット（Reset System）] の順に選択します。



次のメッセージがコンソールに表示されます。



ステップ 3 オプション 4 を入力して、パスワードをリセットします。

ステップ 4 # プロンプトで、**passwd admin** コマンドを入力します。

ステップ 5 新しい管理者パスワードを入力します。

（注） 複雑なパスワードの使用を推奨します。

ステップ 6 **reboot** コマンドを入力します。再起動プロセスが完了するまで待ちます。

Web インターフェイス管理者パスワードのリセット

Management Center Web インターフェイスにアクセスするための管理者アカウントのパスワードを変更できます。

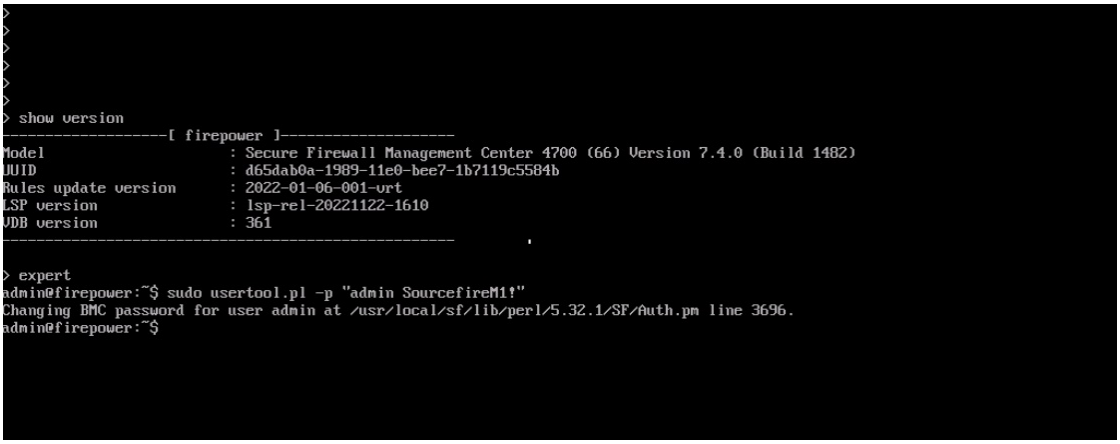
手順

ステップ 1 Management Center の Web インターフェイスに管理者ユーザーとしてログインします。管理者パスワードをリセットするには、アプライアンスとのコンソール接続を確立する必要があります。

ステップ 2 Linux シェルにアクセスするには、**expert** コマンドを入力します。

ステップ 3 シェルプロンプトで、**sudo usertool.pl -p "admin password"** コマンドを入力します。このとき、*password* は Web インターフェイス管理者ユーザーの新しいパスワードです。

次の例では、パスワードは **SourcefireM1!** です。



ステップ 4 パスワード入力画面で、新しいパスワードを入力します。

自動初期設定の確認

初期設定の一環として、Management Center によって、メンテナンスタスクが自動的に設定され、システムが最新の状態に保たれるとともに、データがバックアップされます。

タスクは UTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクは UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受

ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間遅れて実行されることになります。

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

表 *1 : Management Center* のメンテナンスタスク

タスク	説明	GUI パス	詳細
週次 GeoDB 更新	GeoDB は、地理的な位置に基づいてトラフィックを表示およびフィルタ処理するためのデータベースです。	**[システム（System）] > [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）]** > [地理位置情報の定期更新（Recurring Geolocation Updates）]	*Cisco Secure Firewall Management Center アドミニストレーションガイド*
Management Center の週次ソフトウェアアップデート	Management Center では、Management Center およびその管理対象デバイスの最新ソフトウェアをダウンロードするための週次タスクが自動的にスケジュールされます。	**[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]**	
週次の Management Center 設定バックアップ	Management Center により、毎週ローカルに保存された構成のみをバックアップするタスクが自動的にスケジュールされます。	**[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]**	*Cisco Secure Firewall Management Center アドミニストレーションガイド*

タスク	説明	GUI パス	詳細
脆弱性データベースの更新	Management Center では、シスコのサポートサイトから最新の脆弱性データベース（VDB）の更新ファイルがダウンロードおよびインストールされます。これは 1 回限りの操作です。	**[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]**	*Cisco Secure Firewall Management Center アドミニストレーションガイド*
毎日の侵入ルールの更新	Management Center では、侵入ルールがシスコのサポートサイトから毎日自動更新されるように設定されます。（Management Center 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侵入ルールの自動更新が展開されます。）	**[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]**	

Management Center 管理設定の設定

Management Center の初期セットアップが完了し、正常にセットアップされたことを確認したら、いくつかの管理タスクを実行することを推奨します。ライセンスの取得など、初期セットアップで省略したタスクがあれば実施する必要があります。デフォルトの**管理者**アカウントまたは管理者アクセス権を持つ別のアカウントを使用して、これらのタスクを設定します。

複数の Management Center が同じ IP アドレスを共有し、ポート番号によって区別される NAT 環境では、次のようになります。次の条件に注意してください。

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

手順

ステップ 1 Management Center にログインします。

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

ステップ 3 [ログイン（Login）] をクリックします。

ステップ 4 次の管理タスクを設定します。

タスク	GUI パス	詳細
ユーザーアカウントの作成	**[システム（System）] > [ユーザ（Users）]**	*Cisco Secure Firewall Management Center* アドミニストレーション ガイド
時刻の設定	**[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]**	
スマートライセンスの設定	**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]**	

Management Center への管理対象デバイスの追加

マルチテナント、クラスタ、または高可用性を含まない単純な展開を確立するには、管理対象デバイスごとに、次の手順を実行します。これらの機能のいずれかを使用して展開を設定するには、ご使用のバージョンの Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド を参照してください。

始める前に

- デバイス固有のセットアップアクティビティを実行し、遠隔管理用にデバイスを設定します。

重要 このとき、デバイスに使用する登録キーをメモしておいてください。

- NAT を使用する環境の場合は、デバイスのセットアップ時に使用した NAT ID をメモしておいてください。
- DNS を使用する環境の場合は、デバイスの有効な IP アドレスに解決されるホスト名をメモしておいてください。DHCP を使用して IP アドレスを割り当てる環境の場合は、IP アドレスではなくホスト名を使用してデバイスを識別してください。
- DNS を使用しない環境の場合は、デバイスの IP アドレスが必要です。

- 管理対象デバイスに必要なライセンスを特定し、それらを Management Center に追加します。これらのライセンスは、管理対象デバイスを Management Center に追加するプロセスにおいて、管理対象デバイスに追加できます。
- 管理対象デバイスを Management Center に追加した後で、管理対象デバイスにアクセス コントロール ポリシーを割り当てます。次の手順には、この目的のための基本的なアクセス コントロール ポリシーを確立する手順が含まれています。

手順

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

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

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

NAT 環境では、Management Center の管理対象としてデバイスを設定するときに Management Center の IP アドレスまたはホスト名をすでに指定した場合、デバイスの IP アドレスまたはホスト名を指定する必要はありません。

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

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

ステップ 5 [アクセス コントロール ポリシー（Access Control Policy）] で初期ポリシーを選択します。カスタマイズ済みのポリシーがある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。

デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイドを参照してください。この問題を解消してから、デバイスに手動で設定を展開します。

ステップ 6 デバイスに適用するライセンスを選択します。

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

ステップ 8 [登録（Register）] をクリックします。

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

Light-Out Management の設定

LOM 機能では、Serial over LAN（SOL）接続を使用して、Management Center の一部のアクションを実行できます。LOM では、帯域外管理接続で CLI を使用して、シャーシのシリアル番号の表示などのタスクを実行したり、ファンの速度や温度などの状態を監視したりします。

（注） LOM は CIMC インターフェイスでのみ使用できます。

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、LOM を使用して復元プロセスを実行できます。

注意 この復元プロセスによってデバイスの LOM 設定がリセットされます。新しく復元されたアプライアンスに LOM を使用してアクセスすることはできません。LOM を使用してデバイスを工場出荷時設定に復元しているときに、アプライアンスに物理的にアクセスできない場合、ライセンス設定とネットワーク設定を削除すると、復元後にアプライアンスにアクセスできなくなります。

（注） ファイアウォール アプライアンスも LOM をサポートしています。各アプライアンスのローカル Web インターフェイスを使用して、アプライアンスごとに LOM と LOM ユーザーを設定できます。Management Center を使用してファイアウォールデバイスで 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、ファイアウォールデバイスのユーザーにはその機能が伝達されません。

前提条件

- インテリジェントプラットフォーム管理インターフェイス（IMPI）ユーティリティをローカル コンピュータにインストールします。詳細については、IPMI ユーティリティのインストール （21 ページ）を参照してください。
- IPMI ツールを使用してアプライアンスにアクセスするために必要なコマンドを確認します。詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

LOM を設定するには、次の手順を実行します。

ステップ	タスク	GUI パス	詳細
1	LOM を有効にする	**[システム（System）]** > **[ユーザ（Users）]** > **[ユーザ（Users）]**	Cisco Secure Firewall Management Center アドミニストレーションガイド
2	LOM ユーザーアクセスを有効にする	**[システム（System）]** > **[設定（Configuration）]** > [コンソール設定（Console Configuration）] > [Lights-Out Management]	Cisco Secure Firewall Management Center アドミニストレーションガイド
3	アプライアンスへの SOL 接続を作成するには、サードパーティ IPMI ユーティリティを使用します。	-	IPMI ユーティリティのインストール （21 ページ）

IPMI ユーティリティのインストール

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

Mac OS が稼働しているコンピュータでは、IPMItool をインストールします。最初に、Mac に Apple 社の Xcode デベロッパー ツール パッケージがインストールされていることを確認します。コマンドライン開発のためのオプションコンポーネント（新しいバージョンでは UNIX Development および System Tools、古いバージョンではCommand Line Support）がインストールされていることを確認します。最後に、MacPorts および IPMItool をインストールします。詳細については、https://developer.apple.com/technologies/tools/およびhttp://www.macports.org/を参照してください。

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、http://ipmiutil.sourceforge.net/を参照してください。

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 Management Center の事前設定をしてから、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）に展開できます。

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

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

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

事前設定の前提条件

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。

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

アプライアンスを事前設定するには、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の情報

次を含むいくつかのデフォルト設定を変更できます。

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

時間管理の事前設定

手順

ステップ 1 物理的 NTP サーバーと時間を同期させます。

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

- ステージング ロケーションのネットワークからターゲット ロケーションの DNS サーバーおよび 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。
- 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ない場合は、ステージングロケーションの情報を使用し、ターゲットロケーションでアプライアンスをリセットします。

ステップ 3 NTP を使用する代わりに、アプライアンスの時間を手動で設定する場合は、ターゲット展開環境の時間帯を使用します。詳細については、そのバージョンの『Cisco Secure Firewall Management Center アドミニストレーション ガイド』を参照してください。

Management Center の出荷の準備

手順

ステップ 1 『*Cisco Secure Firewall Management Center 1700, 2700, and 4700 Hardware Installation Guide*』の手順に従ってシャーシを設置します。

ステップ 2 アプライアンスにケーブルを接続し、電源をオンにします。

ステップ 3 CLI を使ってアプライアンスの初期セットアップを実施します。

ステップ 4 Management Center の電源を安全に切ります。

ステップ 5 アプライアンスの移送の準備が完了したことを確認します。詳細については、移送に関する考慮事項 （23 ページ）を参照してください。

移送に関する考慮事項

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

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

アプライアンスの事前設定のトラブルシューティング

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

アプライアンスにログインできない場合、事前設定にエラーがある可能性があります。次のトラブルシューティング手順を試行してください。

- すべての電源コードおよび通信ケーブルがアプライアンスに正しく接続されていることを確認します。
- アプライアンスの現行パスワードがわかっていることを確認します。ステージング ロケーションでの初期設定時に、パスワードの変更が求められます。新しいパスワードについては、ステージング ロケーションで提供される設定情報を参照してください。
- ネットワーク設定が正しいことを確認します。詳細については、CLI を使った Management Center の初期設定の実行 （9 ページ）を参照してください。
- 正しい通信ポートが正しく動作していることを確認します。ファイアウォールポートの管理と必要なオープンポートについては、ご使用のバージョンの『Cisco Secure Firewall Management Center アドミニストレーション ガイド』を参照してください。

アプライアンスにログインできない状態が続く場合は、シスコ テクニカル アシスタンス センター（TAC）にお問い合わせください。

Management Center の電源を切る

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。常に多数のバックグラウンドプロセスが実行されているため、電源プラグを抜いたり、電源を切断したりすると、アプライアンスをグレースフルシャットダウンできません。

次のいずれかの方法で、デバイスの電源をオフにできます。

- Management Center デバイス管理ページの Web インターフェイス。**[システム（System）]** > **[設定（Configuration）]** > [プロセス（Process）] > [Management Centerのシャットダウン（Shutdown Management Center）] を選択します。
- Management Center CLI からの **shutdown** コマンド。

仮想デバイスの場合は、ホストの電源をオフにできます。詳細については、ご使用の仮想プラットフォームのマニュアルを参照してください。特に VMware の場合、カスタム電源オプションは VMware ツールの一部です。

次のステップ

続けて Management Center を設定するには、『*Cisco Secure Firewall Management Center Administration Guide*』および『*Cisco Secure Firewall Management Center Configuration Guide*』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。