バックアップと復元

バックアップと復元について

災害から回復する能力は、システム保守計画の重要な部分を占めます。災害復旧計画の一環として、定期的なバックアップを実行することをお勧めします。このプロセスを自動化するには、スケジュール バックアップを参照してください。

（注） Firepower 展開のアップグレード前およびアップグレード後に、リモートロケーションにバックアップして、転送の成功を確認することを強くお勧めします。アプライアンスをアップグレードする際に、ローカルに保存されているバックアップは消去されます。アップグレード後、デバイスがアップグレードされたことを「識別」する新しい FMC バックアップファイルを作成する必要があります。リモートストレージの詳細については、リモートストレージ管理を参照してください。

Firepower のバックアップ機能

FMC を使用して、FMC 自体と FMC が管理するデバイスの多くをバックアップすることができます。 また、7000/8000 シリーズのローカル GUI を使用して、個々のデバイスをバックアッ

プすることもできます。FMC から Firepower Threat Defense デバイスをバックアップすることはできますが、復元は FTD CLI から行う必要があることに注意してください。

表 *1: Firepower* のバックアップ機能

プラットフォーム	バックアップされるデータ	バックアップの保存先	スケジューリング
FMC	次のいずれかです。 • コンフィギュレーション • イベント（キャプチャされたファイルデータは含まれません） • Cisco Threat Intelligence Director（TID）データ：次を参照してください。 TID データのバックアップおよび復元について マルチドメイン展開では、イベント/TIDデータのみをバックアップすることはできません。設定もバックアップする必要があります。	FMC または リモート ストレージ	可
FTD：物理デバイス FTDv：VMware	コンフィギュレーション	デバイス、および必要に応じて FMC または リモート ストレージ	可（FMC GUI から）。
7000/8000 シリーズ	コンフィギュレーションD	FMC GUI にバックアップされている場合は、デバイス（および必要に応じて FMC）に保存するか、リモートストレージに保存します。 デバイスの GUI にバックアップされている場合は、デバイスにのみ保存します。	可（FMC またはデバイス GUI から）。

プラットフォーム	バックアップされるデータ	バックアップの保存先	スケジューリング
FTDv：KVM、AWS、Azure FTD：クラスタ化されたデバイスとコンテナ インスタンス NGIPSv ASA FirePOWER	未サポート これらのデバイスのいずれかを交換する必要がある場合は、デバイス固有の設定を手動で再作成する必要があります。 ただし、FMC をバックアップすると、管理対象デバイスに展開するポリシーやその他の設定のほか、デバイスから FMC にすでに送信されているイベントはバックアップされます。		

バックアップと復元の注意事項と制限事項

以降の項では、デバイスおよび機能領域ごとにバックアップと復元のガイドラインについて詳しく説明します。

- バックアップと復元の注意事項と制限事項：FMC および 7000/8000 シリーズ （4 ページ）
- バックアップと復元の注意事項と制限事項：FTD （5 ページ）
- バックアップと復元の注意事項と制限事項：VPN 証明書を使用している FTD （6 ページ）
- Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン （6 ページ）

警告 Firepowerのバックアップへの不正アクセスがないことを確認する必要があります。バックアップファイルが何らかの方法で変更されている場合、そのファイルを使用してアプライアンスを復元することはできません。

（注） バックアップデータの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。

関連トピック

侵入イベントを確認済みとしてマーク
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

バックアップと復元の注意事項と制限事項：FMC および 7000/8000 シリーズ

Firepower Management Center および 7000/8000 シリーズデバイスのバックアップと復元に関する次の注意事項と制限事項に注意してください。

- 代替アプライアンスにバックアップを復元できるのは、2台が同じモデルであり、同じバージョンの Firepower ソフトウェアを実行している場合のみです。
- 管理対象デバイスをアップグレードした後、Firepower Management Center の新規バックアップを作成します。これは、復元後に、Firepower Management Center の管理対象デバイスの現在のバージョンがバックアップ ファイルのバージョンと同じであるようにするためです。
- Firepower Management Center では、バックアップ機能と復元機能はグローバル ドメインのみで使用できます。サブドメインの範囲内では、バックアップと復元の代わりにエクスポート機能とインポート機能を使用することができます。
- 証明書を含むバックアップ ファイルは、復元後に失敗としてマークされます。そのため、ユーザは Firepower Management Center に証明書を再インストールする必要があります。
- 代替アプライアンスでバックアップを復元すると、既存の設定がすべて削除され、復元された設定に完全に置き換えられます。
- シスコでは、特定のライセンスの予約または永続的なライセンスの予約に変更を加える場合は、Firepower Management Center をバックアップすることをお勧めします。
- アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップ ファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。
- Firepower Management Center を復元した後、最新の侵入ルールの更新を適用することを推奨します。
- PKI オブジェクトに関連付けられている秘密キーは、アプライアンスに保存されるときに、ランダムに生成されたキーで暗号化されます。PKI オブジェクトに関連付けられた秘密キーを含むバックアップを実行する場合、秘密キーは、暗号化されないバックアップ ファイルに組み込まれる前に復号化されます。バックアップ ファイルは安全な場所に保存してください。
- PKI オブジェクトに関連付けられている秘密キーを含むバックアップを復元すると、その秘密キーはランダムに生成されたキーで暗号化されてからアプライアンスに保存されます。
- クリーン リストとカスタム検出リストのいずれかを有効にしてファイル ポリシーを含むバックアップを復元すると、復元されるファイルのリストとあらゆる既存のファイル リストがマージされます。
- バックアップを実行してから、確認済みの侵入イベントを削除し、そのバックアップを使用して復元すると、削除された侵入イベントは復元されますが、それらの確認済みステー

タスは復元されません。それらの復元された侵入イベントは、[確認済みイベント（Reviewed Events）] ではなく [侵入イベント（Intrusion Events）] に表示されます。

- 侵入イベントのデータを含むバックアップを、そのデータがすでに含まれているアプライアンスに復元すると、重複したイベントが作成されることになります。そのようなことが起こらないようにするため、侵入イベントのバックアップは、以前の侵入イベントデータが含まれていないアプライアンスにのみ復元してください。
- 登録された Firepower デバイスの管理 IP アドレスをデバイスの CLI および Firepower Management Center から変更した場合、HA 同期後も、セカンダリ Firepower Management Center には変更が反映されません。セカンダリ Firepower Management Center も更新されるようにするには、2 つの Firepower Management Center の間でロールを切り替えて、セカンダリ Firepower Management Center をアクティブ ユニットにします。現在アクティブな Firepower Management Center のデバイス管理のページで、登録されている Firepower デバイスの管理 IP アドレスを変更します。

バックアップと復元の注意事項と制限事項：FTD

Firepower Threat Defense でのバックアップと復元については、次の注意事項と制限事項に注意してください。

- 代替 Firepower Threat Defense デバイスにバックアップを復元できるのは、2 台のデバイスが同じモデルであり、同じ Firepower バージョンを実行している場合のみです。
- 高可用性ペアの Firepower Threat Defense デバイスのバックアップ ファイルを Firepower Management Center から作成および復元できます。高可用性展開の場合、代替 Firepower Threat Defense デバイスは、交換されるデバイスと同数のネットワーク モジュールと、同タイプおよび同数の物理インターフェイスを備えている必要があります。
- FTD CLI を使用して、代替 Firepower Threat Defense デバイスにバックアップを復元する必要があります。Web インターフェイスから復元操作を実行することはできません。
- Firepower Threat Defense デバイスを Firepower Management Center から登録解除するか管理対象外にすると、復元操作は一部しか実行されません。

  Firepower Threat Defense デバイスを再登録すると、Firepower Management Center のマッピングとインターフェイスを取る以前のセキュリティーゾーンが失われる食べ、機能を予想どおりに再割当てする必要があります。
- Firepower 4100 シリーズや Firepower 9300 デバイスの場合、バックアップおよび復元操作を実行する前に、設定のエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスおよびプラットフォーム構成時の設定が含まれている XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」にあるガイドラインと制約事項を参照してください。
- 代替 Firepower Threat Defense デバイスにバックアップを復元すると、デバイスが実行中の構成に関する既存の設定は削除され、復元された設定に置き換えられます。

- 復元操作の一環として、代替 Firepower Threat Defense デバイスの管理 IP は、置き換えられる Firepower Threat Defense デバイスと同じものになります。IP の競合を避けるため、古い Firepower Threat Defense デバイスがネットワークに接続されていないことを確認してください。

関連トピック

侵入イベントを確認済みとしてマーク
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

バックアップと復元の注意事項と制限事項：VPN 証明書を使用している FTD

VPN 証明書を使用している Firepower Threat Defense デバイスのバックアップと復元を実行する場合、次のガイドラインに注意してください。

ヒント　Firepower Threat Defense デバイスで VPN 証明書を登録または削除する手順については、FTD 証明書の管理 を参照してください。

- Firepower Threat Defense デバイスがバックアップされた後、新しい VPN 証明書が Firepower Management Center に追加されると、Firepower Management Center には新しい証明書がありますが、Firepower Threat Defense デバイスにはありません。Firepower Threat Defense デバイスに新しい証明書を再登録する必要があります。詳細については、FTD 証明書の管理を参照してください。
- 復元操作時にすべての VPN 設定と証明書が Firepower Threat Defense デバイスから削除されます。復元操作後は、すべての証明書の登録が失敗したと Firepower Management Center に表示されます。そのため、Firepower Management Center から設定を展開する前に各証明書を再登録する必要があります。

関連トピック

侵入イベントを確認済みとしてマーク
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン

Firepower 4100/9300 シャーシの論理デバイスとプラットフォームのコンフィギュレーション設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートするコンフィギュレーションのエクスポート機能を使用できます。そのコンフィギュレーション ファイルを後でインポートして Firepower 4100/9300 シャーシに迅速にコンフィギュレーション設定を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。

注意事項および制約事項

- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。
- 用途別のコンフィギュレーション設定は、コンフィギュレーションファイルに含まれていません。用途別の設定やコンフィギュレーションを管理するには、アプリケーションが提供するコンフィギュレーション バックアップ ツールを使用する必要があります。
- Firepower 4100/9300 シャーシへのコンフィギュレーションのインポート時、Firepower 4100/9300 シャーシのすべての既存のコンフィギュレーション（論理デバイスを含む）は削除され、インポート ファイルに含まれるコンフィギュレーションに完全に置き換えられます。
- コンフィギュレーション ファイルのエクスポート元と同じ Firepower 4100/9300 シャーシだけにコンフィギュレーション ファイルをインポートすることをお勧めします。
- インポート先の Firepower 4100/9300 シャーシのプラットフォーム ソフトウェア バージョンは、エクスポートしたときと同じバージョンになるはずです。異なる場合は、インポート操作の成功は保証されません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。
- インポート先の Firepower 4100/9300 シャーシでは、エクスポートしたときと同じスロットに同じネットワーク モジュールがインストールされている必要があります。
- インポート先の Firepower 4100/9300 シャーシでは、インポートするエクスポート ファイルに定義されているすべての論理デバイスに、正しいソフトウェア アプリケーション イメージがインストールされている必要があります。
- 既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作時にファイル名を変更するか、既存のファイルを別の場所にコピーしてください。

関連トピック

侵入イベントを確認済みとしてマーク
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

のバックアップ Firepower Management Center

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC	グローバルのみ	管理者/メンテナンス

Firepower Management Center をバックアップするには、次の手順を使用します。

始める前に

FMC に十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90% 超を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送するか、リモート ストレージを使用してください。リモート ストレージ管理を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [Firepower 管理バックアップ（Firepower Management Backup）] をクリックします。

ステップ 3 [名前（Name）] を入力します。

ステップ 4 バックアップするものを選択します。

- 設定をアーカイブするには、[設定をバックアップ（Back Up Configuration）] を選択します。マルチドメイン展開では、このオプションを無効にできません。
- イベント データベース全体をアーカイブするには、[イベントをバックアップ（Back Up Events）] を選択します。
- TID 設定と TID データベース全体をアーカイブするには、[TID をバックアップ（Back Up Threat Intelligence Director）] を選択します。

ステップ 5 バックアップの完了時に通知を受けるためには、[電子メール（Email）]チェックボックスを選択して、用意されているテキスト ボックスに電子メール アドレスを入力します。

電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定 で説明されているように、リレー ホストを設定する必要があります。

ステップ 6 セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [Host] フィールド：バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールド：バックアップのコピー先となるディレクトリへのパス
- User] フィールド：リモート マシンへのログインに使用するユーザ名
- [パスワード（Password）] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 7 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。バックアップ ファイルは/var/sf/backup ディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存（Save As New）] をクリックします。

次のタスク

バックアップファイルにPKIオブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

デバイスのリモートバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FTD：物理プラットフォーム FTDv VMware 上 7000 & 8000 シリーズ	グローバルのみ	管理者/メンテナンス

Firepower Management Center でリモート デバイスのバックアップを実行するには、次の手順を使用します。

デバイスのバックアップファイルは、デバイスの /var/sf/backup ディレクトリに保存されます。Firepower Management Center にバックアップのコピーを保存することを選択した場合、コピーは FMC の /var/sf/remote-backup ディレクトリに格納されます。

FTD デバイについては、バックアップファイルは、スタンドアロンデバイスの場合は <Displayname/IP>-<Timestamp>.tar の形式に従い、ハイアベイラビリティペアのデバイスの場合は <Displayname/IP>-<Role>-<Timestamp>.tar の形式に従います。

始める前に

十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90% 超を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除または転送するか、リモート ストレージを使用してください。リモート ストレージ管理を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [管理対象デバイスのバックアップ（Managed Device Backup）] をクリックします。

ステップ 3 1 つまたは複数の管理対象デバイスを選択します。

ステップ 4 [管理センターで取得する（Retrieve to Management Center）] を有効または無効にすることによって、バックアップ ファイルを保存する場所を指定します。

- 有効（デフォルト）：デバイスのバックアップをデバイスに保存し、そのファイルを FMC にもコピーします。
- 無効：デバイスのバックアップをデバイスのみに保存します。

リモート バックアップ ストレージを設定している場合、バックアップ ファイルはリモートに保存され、このオプションは無効になります。

ステップ 5 [バックアップ開始（Start Backup）] をクリックします。

次のタスク

バックアップに PKI オブジェクトのデータが含まれている場合、バックアップ内に暗号化されていない秘密キーが保存されるため、安全な場所にバックアップを保存します。

7000/8000 シリーズデバイスのローカルバックアップ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	7000 & 8000 シリーズ	該当なし	管理者/メンテナンス

7000 または 8000 シリーズ デバイスのローカル Web インターフェイスを使用して、次の手順を実行する必要があります。

始める前に

アプライアンスに十分なディスク領域があることを確認してください。バックアップの処理で使用可能なディスク領域の 90%以上を使用すると、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [デバイス バックアップ（Device Backup）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、バックアップ ファイルの名前を入力します。

ステップ 4 バックアップの完了時に通知を受けるためには、[電子メール（Email）]チェックボックスを選択して、用意されているテキスト ボックスに電子メール アドレスを入力します。

電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定 で説明されているように、リレー ホストを設定する必要があります。

ステップ 5 セキュアなコピー（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[完了時にコピー（Copy when complete）] チェックボックスを選択してから、用意されているテキストボックスに以下の情報を入力します。

- [ホスト（Host）] フィールドに、バックアップのコピー先となるマシンのホスト名または IP アドレス。
- [パス（Path）] フィールドに、バックアップのコピー先となるディレクトリへのパス。
- [ユーザ（User）] フィールドに、リモート マシンへのログインに使用するユーザ名。
- [パスワード（Password）] フィールドに、そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモート マシンにアクセスする場合は、そのマシンの指定ユーザの `authorized_keys` ファイルに、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存さ**れません**。Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。バックアップ ファイルは `/var/sf/backup` ディレクトリに保存されます。
- この設定を後で使用できるバックアップ プロファイルとして保存するには、[新規として保存（Save As New）] をクリックします。

次のタスク

バックアップファイルに PKI オブジェクトデータが含まれる場合は、バックアップ内に暗号化されていない秘密キーが含まれています。このため、バックアップはセキュアな場所に保存してください。

バックアップ プロファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	FMC 7000 & 8000 シリーズ	グローバルのみ	管理者/メンテナンス

次の手順は、デバイスの Web ユーザ インターフェイス、または Firepower Management Center Web インターフェイス（該当する場合）を使用して実行する必要があります。

さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。バックアップを実行またはスケジュールするときに、これらのプロファイルのいずれかを選択できます。

ヒント　新規ファイル名を使用してバックアップ ファイルを作成する場合、システムにより自動的に、その名前でバックアップ プロファイルが作成されます。

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

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

ステップ 3　バックアップ ファイルの名前を入力します。

ステップ 4　バックアップ プロファイルを設定します。

オプションの詳細は、のバックアップ Firepower Management Center （7 ページ）を参照してください。

ステップ 5　[新規として保存（Save As New）] をクリックします。

バックアップ ファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

デバイスに応じて、Firepower Management Center Web インターフェイスまたはデバイスのローカル Web インターフェイスを使用して、ローカル ホストから Firepower Management Center、7000 シリーズデバイス、または 8000 シリーズデバイスにバックアップ ファイルをアップロードできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

始める前に

- [バックアップ管理（Backup Management）] ページ （13 ページ）の説明に従って、ダウンロード機能を使用し、バックアップ ファイルをローカル ホストにダウンロードします。

- SCP を介してローカル ホストからリモート ホストに 4GB より大きいバックアップをコピーし、そこから Firepower Management Center に取り出します（Web ブラウザではその大きさのファイルのアップロードがサポートされていないため）。詳細については、リモート ストレージ管理を参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 [バックアップのアップロード（Upload Backup）] をクリックします。

ステップ 3 [参照（Browse）] をクリックし、アップロードするバックアップ ファイルまで移動して選択します。

ステップ 4 [バックアップのアップロード（Upload Backup）] をクリックします。

ステップ 5 [バックアップ管理（Backup Management）] をクリックして、[バックアップ管理（Backup Management）] ページに戻ります。

次のタスク

アプライアンスによってファイルの整合性が確認された後、[バックアップ管理（Backup Management）] ページを更新し、詳細なファイル システム情報を表示します。

[バックアップ管理（Backup Management）] ページ

[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [バックアップ管理（Backup Management）] で、Firepower Management Center Web インターフェイスの [バックアップ管理（Backup Management）] ページにアクセスできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、アップロード時に、システムはランダム生成されたキーを使用して、内部 CA および内部証明書オブジェクトに関連付けられた秘密キーを再暗号化します。

ローカル ストレージを使用する場合、バックアップ ファイルは `/var/sf/backup` に保存されて、`/var` パーティションで使用されているディスク領域量と共に [バックアップ管理（Backup Management）] ページの下部にリストされます。Firepower Management Center で、[バックアップ管理（Backup Management）] ページの上部にある [リモート ストレージ（Remote Storage）] を選択して、リモート ストレージ オプションを設定します。その後、リモート ストレージを有効にするには[バックアップ管理（Backup Management）]ページの[バックアップ用にリモート ストレージを有効にする（Enable Remote Storage for Backups）] チェック ボックスをオンにします。 リモート ストレージを使用している場合は、プロトコル、バックアップ システム、およびバックアップ ディレクトリがページの下部に表示されます。

次の表では、[バックアップ管理（Backup Management）] ページの各列およびボタンについて説明します。

表 *2 :* バックアップ管理（*Backup Management*）

機能	説明
System Information	元のアプライアンスの名前、タイプ、バージョン （注） バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してのみです。
Date Created	バックアップ ファイルが作成された日時
File Name	バックアップ ファイルのフルネーム
VDB Version	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
Location	バックアップ ファイルの場所
Size (MB)	バックアップ ファイルのサイズ（メガバイト）
Events?	[Yes] は、バックアップにイベント データが含まれていることを示します
View	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
Restore	バックアップファイルが選択された状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。詳細については、バックアップからの復元：FMC および 7000/8000 シリーズ （15 ページ）を参照してください。
Download	バックアップファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
Delete	バックアップファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
Move	Firepower Management Center で、以前に作成したローカル バックアップが選択された状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップからの復元：FMC および 7000/8000 シリーズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	FMC 7000 & 8000 シリーズ	グローバルだけ	Admin/Maint

Firepower Management Center Web インターフェイスまたはデバイスの Web インターフェイスの [バックアップ管理（Backup Management）] ページを使用して、バックアップ ファイルから Firepower Management Center、7000 シリーズ デバイス、または 8000 シリーズ デバイスを復元できます。

注意 この操作により、すべてのコンフィギュレーション ファイルが上書きされ、管理対象デバイスでは、すべてのイベント データが上書きされます。

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。バックアップの完了後に Cisco Smart Software Manager から Firepower Management Center を登録解除し、このバックアップを復元する場合、Firepower Management Center を登録解除し Firepower Management Center を再度登録する必要があります。

（注） Firepower Management Center の登録解除の詳細については、Cisco Smart Software Manager から Firepower Management Center の登録解除を参照してください。Firepower Management Center を登録するには、スマート ライセンスの登録を参照してください。

始める前に

- バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致していることを確認します。詳細については、ダッシュボードの表示を参照してください。
- バックアップの完了後にアプライアンスに追加したライセンスは、リストア時の競合を避けるために、バックアップの復元前に削除します。詳細については、Firepower ライセンスについてを参照してください。

- バックアップに保管されているものと同じ侵入イベントデータがアプライアンスに存在しないことを確認します。これは、そのような状況下でバックアップを復元すると、重複するイベントが作成されるためです。詳細については、侵入イベントについてを参照してください。

ステップ 1 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択します。

ステップ 2 バックアップ ファイルをクリックして、そのコンテンツを表示します。詳細には、ファイルの所有者、ファイルの権限、ファイル サイズ、および日付が含まれています。

ステップ 3 **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** を選択して、[バックアップ管理（Backup Management）] ページに戻ります。

ステップ 4 復元するバックアップ ファイルを選択します。

ステップ 5 [復元（Restore）] をクリックします。

（注） バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[復元（Restore）] ボタンはグレー表示されます。

ステップ 6 ファイルを復元するには、次のいずれかまたは両方のオプションを選択します。

- **設定データの復元（Restore Configuration Data）**

  （注） 管理対象デバイスの設定をバックアップ ファイルから復元すると、デバイスの管理用の Firepower Management Center から行われたデバイス設定の変更も復元されます。バックアップ ファイルを復元することで、バックアップ ファイルの作成後に行った変更は上書きされます。

- イベント データの復元（Restore Event Data）（FMC のみ）
- Threat Intelligence Director データの復元（Restore Threat Intelligence Director Data）（FMC のみ）

ステップ 7 [復元（Restore）] をクリックします。

ステップ 8 （オプション）システムが自動的に再起動するまで待ちます。

バックアップに設定データが含まれている場合にのみ、システムは自動的に再起動します。

次のタスク

- 最新のシスコ ルール アップデートをインポートします。侵入ルールのワンタイム手動更新を参照してください。インポートの一環としてポリシーを再展開する場合、設定の変更を展開する必要はありません（後述）。
- 設定変更を展開します。設定変更の展開を参照してください。
- バックアップの復元前に、アプライアンスから削除したライセンスを追加して再設定します。

- 復元時にアプライアンスがライセンスの競合を示した場合は、サポートまでお問い合わせください。

バックアップからの復元： Firepower Threat Defense

問題または障害のある Firepower Threat Defense デバイスを交換する必要がある場合、次に示すバックアップおよび復元手順のいずれかを実行します。

- バックアップからの FTD の復元：Firepower 1000/2100 シリーズ （17 ページ）
- バックアップからの FTD の復元：Firepower 4100/9300 シャーシ （19 ページ）
- バックアップからの FTD の復元： ASA 5500-X シリーズ （22 ページ）
- バックアップからの FTD の復元： FTDv （24 ページ）
- バックアップからの FTD の復元：高可用性 （25 ページ）

バックアップからの FTD の復元：Firepower 1000/2100 シリーズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 1000 シリーズ Firepower 2100 シリーズ	グローバルだけ	Admin/Maint

問題または障害のある Firepower 1000 シリーズ または Firepower 2100 シリーズ デバイスを交換するには、次の手順を実行します。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （3 ページ）を確認してください。
- 環境内に展開された Firepower 1000 シリーズ または Firepower 2100 シリーズ デバイスのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （9 ページ）を参照してください。

  バックアップ ファイルは、Firepower 1000 シリーズ または Firepower 2100 シリーズ デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバッ

クアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。

- Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスだけを接続して、デバイスの電源を投入します。詳細については、『*Cisco Firepower 1000 Series Using Firepower Management Center Quick Start Guide*』または『*Cisco Firepower 2100 Series Using Firepower Management Center Quick Start Guide*』を参照してください。

ステップ 3 交換用デバイスで実行している Firepower のバージョンが、交換されるデバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 `restore` コマンドを使用して、デバイス上のバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開を参照してください。

（注） Firepower Threat Defense デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （3 ページ） の VPN 証明書管理のセクションを参照してください。

- デバイスのデータ インターフェイスをネットワークに接続します。手順については、『*Cisco Firepower 1000 Series Using Firepower Management Center Quick Start Guide*』または『*Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide*』を参照してください。

バックアップからの FTD の復元：Firepower 4100/9300 シャーシ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	Firepower 4100/9300	グローバルだけ	Admin/Maint

Firepower 4100/9300 シャーシで実行中の Firepower Threat Defense でハードウェア障害が発生した場合は、次の手順を実行して交換してください。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （3 ページ）を確認してください。
- Firepower Chassis Manager から FXOS の設定をエクスポートします。詳細については、FXOS コンフィギュレーション ファイルのエクスポート （20 ページ）を参照してください。
- 環境内に展開された Firepower 4100/9300 シャーシで実行中の論理 Firepower Threat Defense デバイスのバックアップがあることを確認します。詳細については、デバイスのリモート バックアップ （9 ページ）を参照してください。

  バックアップ ファイルは、Firepower 4100/9300 シャーシの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。
- Firepower 4100/9300 で実行中の Firepower Threat Defense デバイスに障害が発生した場合は、Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のある Firepower 4100/9300 シャーシをネットワークから取り外します。

ステップ 2 交換用 Firepower 4100/9300 シャーシをネットワーク上に設置し、管理インターフェイスだけを接続して、デバイスの電源を投入します。詳細については、*Cisco Firepower Threat Defense for Firepower 4100* クイック スタート ガイド [英語] または *Cisco Firepower Threat Defense for Firepower 9300* クイック スタート ガイド [英語] を参照してください（該当する場合）。

ステップ 3 Firepower Threat Defense が、交換用デバイスで実行されている FXOS バージョンと互換性があることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』を参照してください。

ステップ 4 Firepower Chassis Manager から以前エクスポートした FXOS の構成時の設定をインポートします。詳細については、コンフィギュレーション ファイルのインポート （21 ページ）を参照してください。

ステップ 5 `restore` コマンドを使用して、交換用 Firepower Threat Defense デバイスのバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、Firepower Threat Defense の `/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開を参照してください。

（注） 論理 Firepower Threat Defense デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （3 ページ）の VPN 証明書管理のセクションを参照してください。

- Firepower 4100/9300 シャーシ デバイスのデータ インターフェイスをネットワークに接続します。手順については、*Cisco Firepower Threat Defense for Firepower 4100* クイック スタート ガイド [英語] または *Cisco Firepower Threat Defense for Firepower 9300* クイック スタート ガイド [英語] を参照してください。

FXOS コンフィギュレーション ファイルのエクスポート

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含むXMLファイルをリモート サーバまたはローカル コンピュータにエクスポートします。

エクスポート機能の使用に関する重要な情報については、「Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン」を参照してください。

ステップ 1 **[System]** > **[Configuration]** > **[Export]** の順に選択します。

ステップ 2 コンフィギュレーション ファイルをローカル コンピュータにエクスポートするには、次の操作を行います。

a) [Local] オプション ボタンをクリックします。

b) [Export] をクリックします。
コンフィギュレーション ファイルが作成され、ブラウザによって、ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するようプロンプトが表示されます。

ステップ 3 コンフィギュレーション ファイルをリモート サーバにエクスポートするには、次の操作を行います。

a) [Remote] オプション ボタンをクリックします。
b) リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

   IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。

d) デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。
e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
g) [Location] フィールドに、ファイル名を含むコンフィギュレーション ファイルをエクスポートする場所のフル パスを入力します。ファイル名を省略すると、エクスポート手順によって、ファイルに名前が割り当てられます。
h) [Export] をクリックします。
   コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

コンフィギュレーション ファイルのインポート

設定のインポート機能を使用して、Firepower 4100/9300 シャーシからエクスポートした構成設定を適用できます。この機能を使用して、既知の良好な構成に戻したり、システム障害を解決したりできます。インポート機能の使用に関する重要な情報については、「Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポート ガイドライン」を参照してください。

ステップ 1 **[System]** > **[Configuration]** > **[Import]** の順に選択します。
ステップ 2 ローカルのコンフィギュレーション ファイルからインポートする場合は、次の操作を行います。

a) [Local] オプション ボタンをクリックします。
b) [Choose File] をクリックし、インポートするコンフィギュレーション ファイルを選択します。
c) [Import] をクリックします。
   操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
d) [Yes] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
   既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

ステップ 3 リモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

a) [Remote] オプション ボタンをクリックします。
b) リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。

d) バックアップ ファイルが格納されている場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。

e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

g) [File Path] フィールドに、コンフィギュレーション ファイルのフル パスをファイル名を含めて入力します。

h) [Import] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。

i) [Yes] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

バックアップからの FTD の復元： ASA 5500-X シリーズ

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	ASA 5500-X シリーズ with FTD	グローバルだけ	Admin/Maint

問題または障害のある ASA 5500-X シリーズ デバイスを交換するには、次の手順を実行します。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （3 ページ）を確認してください。
- 環境内に展開された ASA 5500-X シリーズ デバイスのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （9 ページ）を参照してください。

  バックアップ ファイルは、ASA 5500-X シリーズ デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。

- Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスだけを接続して、デバイスの電源を投入します。詳細については、該当する *Firepower Management Center* を使用した *Cisco Firepower Threat Defense*（*ASA 5500-X* シリーズ用）クイック スタート ガイド [英語] を参照してください。

ステップ 3 交換用デバイスで実行している Firepower システム ソフトウェアのバージョンが、交換対象デバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 `restore` コマンドを使用して、ASA 5500-X シリーズ デバイス上のバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開を参照してください。

（注） Firepower Threat Defense デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （3 ページ）の VPN 証明書管理のセクションを参照してください。

- ASA 5500-X シリーズ デバイスのデータ インターフェイスをネットワークに接続します。手順については、*Firepower Management Center* を使用した *Cisco Firepower Threat Defense*（*ASA 5500-X* シリーズ用）クイック スタート ガイド [英語] を参照してください。

バックアップからの FTD の復元： FTDv

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTDv VMware の場合	グローバルだけ	Admin/Maint

VMware で実行中の問題または障害のある Firepower Threat Defense Virtual デバイスを交換するには、次の手順を実行します。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （3 ページ）を確認してください。
- 環境内に展開された Firepower Threat Defense Virtual デバイスのバックアップがあることを確認します。デバイスのリモートバックアップ （9 ページ）を参照してください。

  バックアップ ファイルは、Firepower Threat Defense Virtual デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。
- Cisco Technical Assistance Center（TAC） に連絡して壊れた Firepower Threat Defense Virtual の交換を依頼してください。

ステップ 1 VMware vSphere Web クライアントまたは vSphere Hypervisor を使用して Firepower Threat Defense Virtual を展開します。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

ステップ 2 CLI を使用して Firepower Threat Defense Virtual デバイスを設定します。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

ステップ 3 （オプション）交換用デバイスを再イメージ化して、実行している Firepower システム ソフトウェアのバージョンを、交換対象デバイスのバージョンと同じにします。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

警告 `/var/sf/backup` から SCP 対応のリモート ロケーションまたは Firepower Management Center にバックアップ ファイルをコピーしてから、バックアップを作成した Firepower Threat Defense Virtual デバイスを再イメージ化します。

ステップ 4 `restore` コマンドを使用して、Firepower Threat Defense Virtual のバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。

- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元操作の進捗状況は、`/var/log/restore.log` ログを表示することでモニタできます。

次のタスク

- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開を参照してください。

（注） Firepower Threat Defense Virtual デバイスで VPN 構成を使用している場合は、バックアップと復元の注意事項と制限事項 （3 ページ）の VPN 証明書管理のセクションを参照してください。

- VMware インターフェイスを追加して設定します。詳細については、*VMware* 展開向け *Cisco Firepower Threat Defense Virtual* クイック スタート ガイドを参照してください。

バックアップからの FTD の復元：高可用性

高可用性ペアの 1 つ以上の障害または問題が発生した Firepower Threat Defense デバイスを交換する必要がある場合は、次に示すいずれかの手順に従う必要があります。

- バックアップからの FTD の復元：HA ペア（1 つのピアの交換） （25 ページ）
- バックアップからの FTD の復元：HA ペア（両方のピアの交換） （27 ページ）

バックアップからの FTD の復元：HA ペア（1 つのピアの交換）

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD：物理プラットフォーム	グローバルだけ	Admin/Maint

高可用性構成の Firepower Threat Defense デバイスでハードウェア障害が発生した場合は、次の手順を実行して交換してください。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （3 ページ）を確認してください。

（注） Firepower Threat Defense で稼働している Firepower 4100/9300 シャーシ デバイスを交換する場合、FXOS の設定を Firepower Chassis Manager からエクスポートしてから Firepower Threat Defense のバックアップと復元操作を進めてください。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

- Firepower Threat Defense 高可用性ペアのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （9 ページ）を参照してください。

  バックアップ ファイルは、Firepower Threat Defense デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。Firepower Management Center は、プライマリとセカンダリの Firepower Threat Defense デバイスに対してバックアップ ファイルを個別に作成します。高可用性ペアの Firepower Threat Defense デバイスの場合、バックアップ tar ファイルの形式は `<Hostname/IP>-<Role>-<Timestamp>.tar` です。

- 高可用性ペアの Firepower Threat Defense デバイスに障害が発生した場合は、Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスと高可用性リンクを接続して、デバイスの電源を投入します。詳細については、該当する *Firepower* クイック スタート ガイドを参照してください。

（注） トラフィックの中断を回避するため、交換用デバイスにデータ インターフェイスが接続されていないことを確認します。

ステップ 3 交換用デバイスで実行している Firepower システム ソフトウェアのバージョンが、交換対象デバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 コマンド ライン インターフェイスで `restore` コマンドを使用して Firepower Threat Defense デバイスにバックアップを復元します。

- ローカルの Firepower Threat Defense からバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

交換している Firepower Threat Defense デバイスがプライマリか、セカンダリかに応じて、適切なバックアップ ファイルを選択します。復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

復元が正常に完了すると、デバイスが再起動します。

次のタスク

- コマンド ライン インターフェイスで `configure high-availability resume` コマンドを使用して高可用性ピア間で高可用性設定を再開します。
- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開を参照してください。
- Firepower Threat Defense デバイスのデータ インターフェイスをネットワークに接続します。手順については、該当する *Cisco Firepower Threat Defense* の *Firepower Management Center* の使用に関するクイック スタート ガイド を参照してください。

バックアップからの FTD の復元：HA ペア（両方のピアの交換）

高可用性構成の両方の Firepower Threat Defense デバイスでハードウェア障害が発生した場合は、次の手順を実行して交換してください。

警告 Firepower Management Center とのすべての通信が停止するため、障害のある Firepower Threat Defense デバイスを登録解除したり、または管理対象外にしないでください。

始める前に

- バックアップと復元の注意事項と制限事項 （3 ページ）を確認してください。

（注） Firepower Threat Defense で稼働している Firepower 4100/9300 シャーシ デバイスを交換する場合、FXOS の設定を Firepower Chassis Manager からエクスポートしてから Firepower Threat Defense のバックアップと復元操作を進めてください。詳細については、『*Cisco FXOS Firepower Chassis Manager* コンフィギュレーション ガイド』の「コンフィギュレーションのインポート/エクスポート」を参照してください。

- Firepower Threat Defense 高可用性ペアのバックアップがあることを確認します。詳細については、デバイスのリモートバックアップ （9 ページ）を参照してください。

バックアップ ファイルは、Firepower Threat Defense デバイスの `/var/sf/backup` でローカルに保持されます。Firepower Management Center 上にバックアップを保持することを選択した場合、バックアップは `/var/sf/remote-backup` ディレクトリに格納されます。Firepower Management Center は、プライマリとセカンダリの Firepower Threat Defense デバイスに対してバックアップ ファイルを個別に作成します。高可用性ペアの Firepower Threat Defense デバイスの場合、バックアップ tar ファイルの形式は `<Hostname/IP>-<Role>-<Timestamp>.tar` です。

- 高可用性ペアの Firepower Threat Defense デバイスに障害が発生した場合は、Cisco Technical Assistance Center（TAC） に連絡して交換を依頼してください。

ステップ 1 障害のあるデバイスをネットワークから取り外します。

ステップ 2 交換用デバイスをネットワーク上に展開し、管理インターフェイスと高可用性リンクを接続して、デバイスの電源を投入します。詳細については、該当する *Firepower* クイック スタート ガイドを参照してください。

（注） トラフィックの中断を回避するため、交換用デバイスにデータ インターフェイスが接続されていないことを確認します。

ステップ 3 交換用デバイスで実行している Firepower システム ソフトウェアのバージョンが、交換対象デバイスで実行しているバージョンと同じであることを確認します。必要に応じて、交換用デバイスを再イメージ化します。詳細については、*Cisco ASA* および *Firepower Threat Defense* デバイスの再イメージ化ガイドを参照してください。

ステップ 4 `restore` コマンドを使用して、両方の Firepower Threat Defense デバイス上のバックアップを連続して復元します。

- ローカルの Firepower Threat Defense デバイスからバックアップを復元するには、`restore remote-manager-backup <backup tar-file>` コマンドを使用します。
- SCP 対応リモート ネットワークからバックアップを復元するには、`restore remote-manager-backup location <scp-hostname> <username> <filepath> <backup tar-file>` コマンドを使用します。

復元されている該当 Firepower Threat Defense デバイスに対応するバックアップ ファイルを選択します。復元操作の進捗状況は、Firepower Threat Defense デバイスの `/var/log/restore.log` ログを表示することでモニタできます。

復元が正常に完了すると、デバイスが再起動します。

次のタスク

- コマンド ライン インターフェイスで `configure high-availability resume` コマンドを使用して高可用性ピア間で高可用性設定を再開します。
- 復元に成功すると、Firepower Threat Defense デバイスは Firepower Management Center に接続して使用可能になります。復元された Firepower Threat Defense デバイス上のポリシーは期限切れになります。設定の変更を Firepower Management Center から展開して、ポリシーを更新します。詳細については、設定変更の展開を参照してください。

- Firepower Threat Defense デバイスのデータ インターフェイスをネットワークに接続します。手順については、該当する *Cisco Firepower Threat Defense* の *Firepower Management Center* の使用に関するクイック スタート ガイド を参照してください。

バックアップと復元の履歴

機能	バージョン	詳細
管理対象デバイスのオンデマンドでのリモート バックアップ	6.3	FMC を使用して、特定の管理対象デバイスのリモートバックアップをオンデマンドで実行できるようになりました。 以前、バックアップをサポートしていたのは 7000 および 8000 シリーズのデバイスのみで、デバイスのローカル GUI を使用する必要がありました。 新規/変更された画面：[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）] 新規/変更された FTD CLI コマンド： **restore** サポートされるプラットフォーム：FTD の物理プラットフォーム、FTDv for VMware、7000/8000 シリーズ 例外：FTD のクラスタ化されたデバイスまたはコンテナ インスタンスはサポートされていません。