ソフトウェアのインストール

アップグレードできない場合、またはアップグレードしない場合は、メジャーリリースおよびメンテナンスリリースを新規インストールできます。

パッチ用のインストールパッケージは提供していません。特定のパッチを実行するには、適切なメジャーリリースまたはメンテナンスリリースをインストールしてからパッチを適用してください。

インストールにおけるチェックリストおよびガイドライン

再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。このチェックリストは、一般的な再イメージ化の問題を回避できるアクションを示しています。ただし、このチェックリストは包括的なものではありません。詳細な手順については、該当する設置ガイド『取り付け手順 （5 ページ）』を参照してください。

表 *1:*

✓	アクション/チェック
	アプライアンスへのアクセスを確認します。 アプライアンスに物理的にアクセスできない場合、再イメージ化プロセスによって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設定を削除する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。 （注） 以前のバージョンに再イメージ化すると、ネットワーク設定が自動的に削除されます。このようなまれなケースでは、物理的アクセスが必要です。 デバイスに関して、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	バックアップを実行します。 サポートされている場合、再イメージ化の前にバックアップします。 再イメージ化してアップグレードする必要がない場合、バージョンの制約により、バックアップを使用して古い設定をインポートできないことに注意してください。設定は手動で再作成する必要があります。 **注意** 安全なリモートロケーションにバックアップし、正常に転送が行われることを確認することを強くお勧めします。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。 バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

✓	アクション/チェック
	FMC 管理からデバイスを削除する必要があるか判断します。 再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、リモート管理からデバイスを削除します。 • FMC を再イメージ化する場合は、すべてのデバイスを管理から削除します。 • 単一のデバイスを再イメージ化するか、またはリモートからローカルでの管理に切り替える場合は、その単一のデバイスを削除します。 再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。
	ライセンスの問題に対処します。 アプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager（CSSM）から登録解除することが必要になる場合があります。これで、再登録を防ぐことができます。または、新しいライセンスについてセールス部門に連絡する必要がある場合があります。 詳細については、以下を参照してください。 • ご使用の製品の設定ガイド。 • スマート ライセンスの登録解除 （3 ページ） • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

以前のメジャー バージョンへの Firepower 1000/2100 シリーズ デバイスの再イメージ化

Firepower 1000/2100 シリーズデバイスの完全な再イメージ化を実行することを推奨します。消去設定方式を使用すると、Firepower Threat Defense ソフトウェアに加えて、FXOS が復元しない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。

詳細については、『Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）』に記載されている再イメージ化の手順を参照してください。

スマート ライセンスの登録解除

Firepower Threat Defense は Cisco Smart Licensing を使用します。ライセンス供与された機能を使用するには、Cisco Smart Software Manager（CSSM）で登録します。後で再イメージ化または管理の切り替えを行うことにした場合は、孤立した権限付与を発生させないように登録を解除する必要があります。これらが生じると再登録できない場合があります。

（注） FMC または FTD デバイスをバックアップから復元する必要がある場合は、再イメージ化の前に登録を解除しないでください。また、FMC からデバイスを削除しないでください。代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

登録を解除すると、仮想アカウントからアプライアンスが削除され、クラウドおよびクラウドサービスからアプライアンスが登録解除され、関連付けられたライセンスが解放されるため、ライセンスを再割り当てできるようになります。アプライアンスを登録解除すると、適用モードになります。アプライアンスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

次の操作を行う前に、CSSM から手動で登録解除します。

- FTD デバイスを管理する Firepower Management Center を再イメージ化する。
- モデルの移行中にソース Firepower Management Center をシャットダウンする。
- FDM によってローカルで管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FDM から FMC 管理に切り替える。

FMC からデバイスを削除すると、CSSM から自動的に登録解除されます。これにより、次のことが可能になります。

- FMC によって管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FMC から FDM 管理に切り替える。

上記の 2 つのケースでは、FMC からデバイスを削除すると、デバイスが自動的に登録解除されます。FMC からデバイスを削除すれば、手動で登録解除する必要はありません。

ヒント NGIPS デバイスのクラシック ライセンスは、特定のマネージャ（ASDM/FMC）に関連付けられており、CSSM を使用して制御されません。クラシック デバイスの管理を切り替える場合、または NGIPS 展開から FTD 展開に移行する場合は、セールス担当者にお問い合わせください。

取り付け手順

表 *2 : Firepower Management Center* 取り付け手順

FMC	ガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual Getting Started Guide

表 *3 : Firepower Threat Defense* 取り付け手順

FTDプラットフォーム	ガイド
Firepower 1000/2100 シリーズ	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 スタートアップガイド Cisco Firepower 9300 スタートアップ ガイド
ASA 5500-X シリーズ	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド
ISA 3000	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド
FTDv：AWS	AWS クラウド向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：Azure	Microsoft Azure クラウド向け Cisco Secure Firewall Threat Defense Virtual クイックスタートガイド
FTDv：GCP	Google クラウドプラットフォーム向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：KVM	KVM 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

FTDプラットフォーム	ガイド
FTDv：OCI	Oracle クラウド インフラストラクチャ向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
FTDv：VMware	VMware 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

表 *4 : NGIPSv* および *ASA FirePOWER* のインストール手順

NGIPS プラットフォーム	ガイド
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA FirePOWER	Cisco Secure Firewall ASA および Threat Defense 再イメージ化ガイド ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide：Managing the ASA FirePOWER Module