ホットフィックスについて

ホットフィックスは、特定の緊急の問題に対処するマイナーな更新プログラムです。

ホットフィックスのダウンロード

シスコ サポートおよびダウンロードサイト（https://software.cisco.com/download/home）からホットフィックスをダウンロードします。

ホットフィックスを見つけるには、モデルを選択または検索し、現在のバージョンに対するソフトウェアのダウンロードページを参照します。使用可能なホットフィックスがアップグレードおよびインストール パッケージとともに一覧表示されます。パッチレベルのダウンロードページでホットフィックスが見つからない場合（特に同じホットフィックスが他のパッチに適用される場合）は、ホットフィックスが適用される他のダウンロードページ（特に最初のバージョンと最新のバージョン）を参照してください。

ファミリまたはシリーズのすべてのモデルに同じホットフィックスパッケージを使用します。ほとんどのホットフィックスパッケージでは、次の命名スキームが使用されます。

- *Platform*_Hotfix_*letter-version-build*.sh.REL.tar（バージョン 6.2.2+）
- *Platform*_Hotfix_*letter-version-build*.sh（バージョン 5.4 ～ 6.2.0）

署名付きの（.tar）パッケージは解凍しないでください。

ヒント　使用中のアプライアンスでインターネットにアクセス可能な Management Center 展開および ASDM 展開では、シスコから直接ホットフィックスを簡単に取得できます。Management Center で、**[System]** > **[Updates]**を選択して [Download Update] をクリックします。ASDM で、**[Configuration]** > **[ASA FirePOWER Configuration]** > **[Updates]** を選択し、[Download Updates] をクリックします。

ホットフィックスのインストール

ホットフィックスは、パッチをインストールするのと同じ方法でインストールします。手順については、次のいずれかのガイドを参照してください。

（注）　CDO と Device Manager の展開では、Device Manager を使用して Threat Defense ホットフィックスをインストールしてください。CDO は使用できません。

Management Center

表 *1 : Management Center* のホットフィックス

現在の Management Center のバージョン	ガイド
クラウド提供型の管理センター（バージョンなし）	なし。更新はシスコが行います。
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』内の「Upgrade the Management Center」。
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』内の「Upgrade the FMC」。
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0内の「Upgrade Firepower Management Centers」。

Threat Defense

表 *2 : Management Center* を使用した *Threat Defense* のホットフィックス

現在の Management Center のバージョン	ガイド
クラウド提供型の管理センター（バージョンなし）	最新のリリースバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』内の「Upgrade Threat Defense」。
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』内の「Upgrade Threat Defense」。
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』内の「Upgrade FTD」。
7.0 以前	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0の「Upgrade Firepower Threat Defense」。

表 *3 : Device Manager* を使用した *Threat Defense* のホットフィックス

現在の Threat Defense のバージョン	ガイド
7.2 以降	お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager』内の「Upgrade Threat Defense」。
7.1	『Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1』内の「Upgrade FTD」。
7.0 以前	『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』内の「System Management」。
バージョン 6.4 以降、CDO 使用	Device Manager を使用して Threat Defense ホットフィックスをインストールします。CDO は使用できません。

NGIPS

表 *4 : NGIPS* デバイスのホットフィックス

現在のマネージャバージョン	プラットフォーム	ガイド
任意	Firepower 7000/8000 シリーズ	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0の「Upgrade Firepower 7000/8000 Series and NGIPSv」。

現在のマネージャバージョン	プラットフォーム	ガイド
任意	FMC を搭載した ASA FirePOWER	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0の「Upgrade ASA with FirePOWER Services」。
任意	ASDM を使用した ASA FirePOWER	Cisco Secure Firewall ASA Upgrade Guideの「Upgrade the ASA FirePOWER Module」。

ホットフィックス成功の確認

ホットフィックスを適用しても、ソフトウェアのバージョンまたはビルドは更新されません。ホットフィックスが正常にインストールされたことを確認するには、Linux シェル（エキスパートモードとも呼ばれる）にアクセスして、次のコマンドを実行します。

```
cat/etc/sf/patch_history
```

ソフトウェアが新規にインストールされると、システムは、正常なアップグレード、パッチ、ホットフィックス、およびインストール前のパッケージをすべて一覧表示します。

無応答または失敗したホットフィックス

ホットフィックスのインストール中は、構成の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のホットフィックスを手動でリブート、シャットダウン、または再起動しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。1 つのアプライアンスに対して同じホットフィックスを複数回インストールしないでください。ホットフィックスに失敗する、アプライアンスが応答しないなど、ホットフィックスで問題が発生した場合には Cisco TAC にお問い合わせください。

ホットフィックスのアンインストール

ホットフィックスをアンインストールしようとしないでください。代わりに、Cisco TAC にお問い合わせください。

トラフィック フローとインスペクション

デバイスのホットフィックスは、トラフィックフローとインスペクションに影響を与える可能性があります。ホットフィックスによってデバイスが再起動された場合、または構成の変更を展開する必要がある場合は特に注意が必要です。

デバイスのタイプ、展開のタイプ（スタンドアロン、高可用性、クラスタ化）、およびインターフェイスの構成によって中断の性質が決まります。ホットフィックスのインストールは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強くお勧めします。

トラフィックフローとインスペクションの詳細については、お使いのバージョンの『Cisco Secure Firewall Threat Defense リリースノート』を参照してください。

サポートが必要な場合

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービスリクエストをオープンしたりするための次のオンラインリソースを提供しています。これらのリソースは、Cisco ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- マニュアル：http://www.cisco.com/go/ftd-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

シスコ サポートおよびダウンロード サイトの大部分のツールにアクセスする際は、Cisco.com のユーザー ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンライン リソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先

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。