# Cisco Secure Firewall Threat Defense/Firepowerホットフィックス リリースノート

**最終更新**：2026 年 8 月 16 日

## Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリースノート

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。

このドキュメントには、公開されているホットフィックスのダウンロードページへのクイックリンクが記載されています。クイックリンクによっては特定のモデルのダウンロードページにアクセスできない場合があります。ただし、アプライアンスが同じファミリまたはシリーズである限り、ホットフィックスを安全にダウンロードして適用することができます。絶対に確実にしたい場合は、特定のモデルのページを参照してください。

## ホットフィックスの適用

### ホットフィックスのダウンロード

ほとんどの場合、システムはホットフィックスを直接ダウンロードできません。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、*Platform*_Hotfix_*letter-version-build*.sh.REL.tar という命名スキームが使用されます。署名付きの（.tar）パッケージは解凍しないでください。

### ホットフィックスのアップロード

オンプレミスの バージョン 7.2.6 以降/7.4.1 以降、クラウド提供型 Firewall Management Center、および Firewall Device Manager では、ホットフィックスを手動でアップロードしてください。

の展開では、デバイスがホットフィックスを取得できる内部 Web サーバーを設定することもできます。

（注） クラウド提供型 Firewall Management Center のインスタンスがアップグレードされると、ローカルに保存されているアップグレードパッケージは削除されます。これには、管理対象デバイスへの適用を待機していたホットフィックスが含まれます。デバイスのホットフィックスを再度アップロードしてください。クラウド提供型 Firewall Management Center のインスタンスがアップグレードされたかどうかを確認するには、『*Security Cloud Control* の新機能』をチェックしてください。

### 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。 の展開では、（Firewall Threat Defense ではなく）現在実行している のバージョンのガイドを使用します。Firewall Device Manager の展開では、通常 Security Cloud Control を使用する場合でも Firewall Device Manager のガイドを使用します。Security Cloud Control を使用して Firewall Threat Defense にホットフィックスを適用することはできません。

**表 *1:* のアップグレードガイド**

| 現在の 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 Management Center』：「Upgrade Management Center」 |
| 7.1 | 『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』：「Upgrade the FMC」 |
| 7.0 以前 | 『*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*』：「Upgrade Firepower Management Centers」 |

**表 *2: Firewall Threat Defense* を搭載した のアップグレードガイド**

| 現在の のバージョン | ガイド |
|---|---|
| クラウド提供型 Firewall Management Center | クラウド提供型 Firewall Management Center 向け Cisco Secure Firewall Threat Defense アップグレードガイド |
| 7.2 以降 | お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』：「Upgrade Threat Defense」 |
| 7.1 | 『Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1』：「Upgrade FTD」 |

| 現在の のバージョン | ガイド |
|---|---|
| 7.0 以前 | 『*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*』：「Upgrade Firepower Threat Defense」 |

表 *3 : Firewall Threat Defense* を搭載した *Firewall Device Manager* のアップグレードガイド

| 現在の **Firewall 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』：「Upgrade Threat Defense」 |
| 7.1 | 『Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1』：「Upgrade FTD」 |
| 7.0 以前 | お使いのバージョンの『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』：「System Management」 |

表 *4 : NGIPS* のアップグレードガイド

| プラットフォーム | 現在のマネージャバージョン | ガイド |
|---|---|---|
| を搭載した Firepower 7000/8000 シリーズ | 6.0.0 ～ 7.0.x | 『*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*』：「Upgrade Firepower 7000/8000 Series and NGIPSv」 |
| を搭載した NGIPSv | 6.0.0 ～ 7.1.x<br>7.2.0 ～ 7.2.5<br>7.3.x<br>7.4.0 | 『*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*』：「Upgrade Firepower 7000/8000 Series and NGIPSv」 |
| | 7.2.6 ～ 7.2.x<br>7.4.1 ～ 7.4.x | お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』：「Upgrade Older ASA FirePOWER and NGIPSv Devices」 |

| プラットフォーム | 現在のマネージャバージョン | ガイド |
|---|---|---|
| を搭載した ASA FirePOWER | 6.0.0 ～ 7.1.x<br>7.2.0 ～ 7.2.5<br>7.3.x<br>7.4.0 | 『*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*』：「Upgrade ASA with FirePOWER Services」 |
| | 7.2.6 ～ 7.2.x<br>7.4.1 ～ 7.4.x | お使いのバージョンの『Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center』：「Upgrade Older ASA FirePOWER and NGIPSv Devices」 |
| ASDM を使用した ASA FirePOWER | 任意（Any） | 『*Cisco Secure Firewall ASA アップグレードガイド*』：「Upgrade the ASA FirePOWER Module」 |

### ホットフィックスの成功の確認

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

ホットフィックスとパッチは、インストールとまったく逆の順序（最後にインストールしたものを最初に削除）でアンインストールする必要があります。次に例を示します。

- インストール：パッチ A → ホットフィックス B → ホットフィックス C → パッチ D → ホットフィックス E

- アンインストール：ホットフィックスE→パッチD→ホットフィックスC→ホットフィックス B → パッチ A

以降のバージョンでは、 Web インターフェイスで正しい順序が適用されます。エキスパートモードを使用してアンインストールするFirewall Threat Defenseの場合は、自分で行う必要があります。アンインストール手順については、（上記のリンクが設定されている）該当するアップグレードガイドを参照してください。

（注） ホットフィックスおよびホットフィックスパッチのアンインストールは推奨されません。これを行う必要がある場合は、Cisco TAC にお問い合わせください。

### 通信フローと検査

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います。通信フローと検査の詳細については、（上記のリンクが設定されている）該当するアップグレードガイドを参照してください。

## ハードウェアの BIOS とファームウェアのホットフィックス

ハードウェアのBIOSおよびRAIDコントローラファームウェアのアップデートを提供します。が要件を満たしていない場合は、適切なホットフィックスを適用してください。使いの モデルとバージョンがリストになく、更新が必要だと思われる場合は、Cisco TAC までお問い合わせください。

**表 *5 : BIOS* とファームウェアの最小要件**

| プラットフォーム | バージョン | ホットフィックス | BIOS | RAIDコントローラファームウェア | CIMC ファームウェア |
|---|---|---|---|---|---|
| FMC 1700、2700、4700 | 10.x<br>7.7<br>7.6<br>7.4 | BIOS のアップデート ホットフィックス FX | C225M6.4.3.6a.0 | 52.30.0-5806 | 4.3(6.260017) |

| プラットフォーム | バージョン | ホットフィックス | BIOS | RAID コントローラファームウェア | CIMC ファームウェア |
|---|---|---|---|---|---|
| FMC 1600、2600、4600 | 10.x<br>7.7<br>7.6<br>7.4<br>7.3<br>7.2<br>7.1<br>7.0 | BIOS のアップデート ホットフィックス FX | C220M5.4.3.2g.0 | 51.23.0-5009 | 4.3(2.260007) |
| | 6.7<br>6.6<br>6.4 | BIOS のアップデート ホットフィックス EN | C220M5.4.2.3b.0 | 51.10.0-3612 | 4.2(3b) |
| FMC 1000、2500、4500 | 7.0<br>6.7<br>6.6<br>6.4 | BIOS のアップデート ホットフィックス EN | C220M5.4.2.3b.0 | 51.10.0-3612 | 4.2(3b) |

ホットフィックスの適用は、BIOS および RAID コントローラファームウェアを更新する唯一の方法です。ソフトウェアをアップグレードしても、このタスクは実行されず、新しいバージョンに再イメージ化されません。 がすでに最新の状態である場合、ホットフィックスは効果がありません。

**ヒント** これらのホットフィックスにより、CIMC ファームウェアも更新されます。解決された問題については、Cisco UCS ラックサーバソフトウェアのリリースノートを参照してください。一般に、CIMC の使用での設定の変更はサポートされていないことに注意してください。ただし、無効なCIMCユーザー名のロギングを有効にするには、最新のホットフィックスを適用してから、『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide』バージョン 4.0 以降（）の「*Viewing Faults and Logs*」の章に記載されている手順に従ってください。

**（注）** Web インターフェイスは、現在のソフトウェアバージョンとは異なる（通常はそれ以降の）バージョンでこれらのホットフィックスを表示する場合があります。これは予想される動作であり、このホットフィックスは適用しても安全です。

### BIOS およびファームウェアバージョンの確認

での現在のバージョンを確認するには、Linux シェル/エキスパートモードで次のコマンドを実行します。

- BIOS: **sudo dmidecode -t bios -q**
- RAID コントローラファームウェア（FMC 4500）： **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID コントローラファームウェア（他のすべてのモデル）： **sudo storcli /c0 show | grep "FW Package"**

## バージョン 10.x のホットフィックス

表 *6 :* バージョン *10* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FX | 10.x | Management Center（1600、1700、2600、2700、4600、4700）：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_FX_BIOSUPDATE-10.0.99-3 | BIOS、CIMC ファームウェア、およびRAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |

# バージョン 7.7.x のホットフィックス

表 7: バージョン 7.7 のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス AE | 7.7.11 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_AE-7.7.11.1-4<br>Secure Firewall 1200：<br>Cisco_Secure_FW_TD_1200_Hotfix_AE-7.7.11.1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_AE-7.7.11.1-4<br>Secure Firewall 4200：<br>Cisco_Secure_FW_TD_4200_Hotfix_AE-7.7.11.1-4<br>Firepower 9300：<br>Cisco_FTD_SSP_Hotfix_AE-7.7.11.1-4 | CSCwt61597：Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense に対する永続性メカニズムの継続的な進化<br>「Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense」を参照 |
| ホットフィックス FX | 7.7.0<br>7.7.x<br>7.7.x.x | Management Center（すべてのハードウェアモデル）：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_X_BIOSUPDATE-7.7.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |

# バージョン 7.6.x のホットフィックス

表 *8* : バージョン *7.6.x* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス CC | 7.6.4 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_CC-7.6.4.1-1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_CC-7.6.4.1-1<br>Secure Firewall 4200：<br>Cisco_Secure_FW_TD_4200_Hotfix_CC-7.6.4.1-1<br>Firepower 9300：<br>Cisco_FTD_SSP_Hotfix_CC-7.6.4.1-1 | CSCwt61597：Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense に対する永続性メカニズムの継続的な進化<br>「Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense」を参照 |
| ホットフィックス FX | 7.6.0<br>7.6.x<br>7.6.x.x | Management Center（すべてのハードウェアモデル）：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_FX_BIOSUPDATE-7.6.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス B | 7.6.0 | Management Center：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_B-7.6.0.99-5 | CSCwd08098：FMC の cacert.pem が期限切れになり、すべてのデバイスが無効として表示されます。<br>「Firewall Management Center Certificate Expiration After 10 Years」を参照してください。 |

# バージョン 7.4.x のホットフィックス

**表 *9*: バージョン *7.4.x* のホットフィックス**

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FX | 7.4.0<br>7.4.x<br>7.4.x.x | Management Center（すべてのハードウェアモデル）：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_FX_BIOSUPDATE-7.4.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス BB | 7.4.2.1 | Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_BB-7.4.2.2-3<br>ISA 3000：<br>Cisco_FTD_Hotfix_BB-7.4.2.2-3<br>Threat Defense 仮想：<br>Cisco_FTD_Hotfix_BB-7.4.2.2-3<br>（注）<br>Firepower 4100/9300 の場合は、FXOS：fxos-k9.2.14.1.1900.SPA もアップグレードする必要があります。 | コモンクライテリア認定テスト中に見つかったギャップを解決します。 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス BR | 7.4.2.1 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_BR-7.4.2.2-1<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_BR-7.4.2.2-1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_BR-7.4.2.2-1<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_BR-7.4.2.2-1<br>ISA 3000：<br>Cisco_FTD_Hotfix_BR-7.4.2.2-1<br>Threat Defense 仮想：<br>Cisco_FTD_Hotfix_BR-7.4.2.2-1 | CSCwi84417：通信が期限切れ後に時間範囲オブジェクトを含むALLOWルールと誤って一致する |
| ホットフィックス AO | 7.4.0 ～ 7.4.2.1 | Management Center：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_AO-7.4.2.99-5 | CSCwd08098：FMC の cacert.pem が期限切れになり、すべてのデバイスが無効として表示されます。<br>「Firewall Management Center Certificate Expiration After 10 Years」を参照してください。 |

## バージョン 7.3.x のホットフィックス

表 *10*：バージョン *7.3.x* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FX | 7.3.0<br>7.3.x<br>7.3.x.x | Management Center（すべてのハードウェアモデル）：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_FX_BIOSUPDATE-7.3.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他のBIOSおよびファームウェアホットフィックスがすべて置き換えられます。以前のBIOSおよびファームウェアホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、およびRAIDコントローラファームウェアが更新されます。<br>ハードウェアのBIOSとファームウェアのホットフィックス（5ページ）を参照してください。 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス AE | 7.3.0 ～ 7.3.1.2 | Management Center：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_AE-7.3.1.99-5 | CSCwd08098：FMC の cacert.pem が期限切れになり、すべてのデバイスが無効として表示されます。<br>「Firewall Management Center Certificate Expiration After 10 Years」を参照してください。 |

## バージョン 7.2.x のホットフィックス

**表 *11* : バージョン *7.2.x* のホットフィックス**

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス HI | 7.2.11 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_HI-7.2.11.1-1<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_HI-7.2.11.1-1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_HI-7.2.11.1-1<br>Firepower 4100：<br>Cisco_FTD_SSP_Hotfix_HI-7.2.11.1-1<br>Firepower 9300：<br>Cisco_FTD_SSP_Hotfix_HI-7.2.11.1-1 | CSCwt61597：Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense に対する永続性メカニズムの継続的な進化<br>「Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense」を参照 |
| ホットフィックス FX | 7.2.0<br>7.2.x<br>7.2.x.x | Management Center（すべてのハードウェアモデル）：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_FX_BIOSUPDATE-7.2.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FA | 7.2.10.2 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_HA-7.2.10.3-1<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_HA-7.2.10.3-1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_HA-7.2.10.3-1<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_HA-7.2.10.3-1<br>FTD を使用した ISA 3000：<br>Cisco_FTD_Hotfix_HA-7.2.10.3-1<br>FTDv：<br>Cisco_FTD_Hotfix_HA-7.2.10.3-1 | CSCwq75339：複数のシスコ製品における Snort 3 DCERPC の脆弱性<br>CSCwq75359：複数のシスコ製品における Snort 3 DCERPC の脆弱性 |
| ホットフィックス FZ | 7.2.0 ～ 7.2.9 | Management Center：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_FZ-7.2.9.99-4 | CSCwd08098：FMC の cacert.pem が期限切れになり、すべてのデバイスが無効として表示されます。<br>「Firewall Management Center Certificate Expiration After 10 Years」を参照してください。 |
| ホットフィックス BJ | 7.2.5 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_BJ-7.2.5.1-1<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_BJ-7.2.5.1-1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_BJ-7.2.5.1-1<br>Firepower 4100/9300<br>Cisco_FTD_SSP_Hotfix_BJ-7.2.5.1-1<br>ISA 3000：<br>Cisco_FTD_Hotfix_BJ-7.2.5.1-1<br>Threat Defense 仮想：<br>Cisco_FTD_Hotfix_BJ-7.2.5.1-1 | CSCwh23100：Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性<br>CSCwh45108：Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス AW | 7.2.4 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1<br>Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_AW-7.2.4.1-1<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_AW-7.2.4.1-1<br>ISA 3000：<br>Cisco_FTD_Hotfix_AW-7.2.4.1-1<br>Threat Defense 仮想：<br>Cisco_FTD_Hotfix_AW-7.2.4.1-1 | CSCwf71606：リロード時に Cisco ASA および FTD ACL がインストールされない |
| ホットフィックス AN | 7.2.4-165 | Management Center：<br>Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2<br>（注）<br>このホットフィックスは、バージョン 7.2.4-165 にのみ適用します。この問題を修正するバージョン 7.2.4-169 には適用しないでください。 | CSCwf28592：一部の特定のシナリオでは、オブジェクトオプティマイザによって、デバイスに不適切なルールが展開される可能性がある |

## バージョン 7.1.x のホットフィックス

表 *12 :* バージョン *7.1.x* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FX | 7.1.0<br>7.1.x<br>7.1.x.x | FMC（すべてのハードウェアモデル）：<br>Cisco_Firepower_Mgmt_Center_Hotfix_FX_BIOSUPDATE-7.1.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス Q | 7.1.0.2 | Secure Firewall 3100：<br>Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2 | CSCwb88651 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性<br>CSCwb28334 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性 |
| ホットフィックス P | 7.1.0.1 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_P-7.1.0.2-2<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_P-7.1.0.2-2<br>ISA 3000：<br>Cisco_FTD_Hotfix_P-7.1.0.2-2<br>FTDv：<br>Cisco_FTD_Hotfix_P-7.1.0.2-2 | CSCwb88651 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性<br>CSCwb28334 : Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性 |
| ホットフィックス A | 7.1.0 | Device Manager 搭載 Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_A-7.1.0.1-7<br>Device Manager 搭載 Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_A-7.1.0.1-7<br>Device Manager 搭載 Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_A-7.1.0.1-7<br>Device Manager 搭載 ISA 3000：<br>Cisco_FTD_Hotfix_A-7.1.0.1-7<br>Device Manager 搭載 FTDv：<br>Cisco_FTD_Hotfix_A-7.1.0.1-7<br>（注）<br>このホットフィックスは Device Manager と Device Manager/CDO 管理対象デバイスに適用してください。Management Center 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。 | CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性 |

# バージョン 7.0.x のホットフィックス

表 *13* : バージョン *7.0.x* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FZ | 7.0.9 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_FZ-7.0.9.1-3<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_FZ-7.0.9.1-3<br>Firepower 4100：<br>Cisco_FTD_SSP_Hotfix_FZ-7.0.9.1-3<br>Firepower 9300：<br>Cisco_FTD_SSP_Hotfix_FZ-7.0.9.1-3 | CSCwt61597：Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense に対する永続性メカニズムの継続的な進化<br>「Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense」を参照 |
| ホットフィックス FX | 7.0.0<br>7.0.x<br>7.0.x.x | Management Center（1600、2600、4600）：<br>Cisco_Firepower_Mgmt_Center_Hotfix_FX_BIOSUPDATE-7.0.99.99-3<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス FT | 7.0.8.1 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_FT-7.0.8.2-2<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_FT-7.0.8.2-2<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_FT-7.0.8.2-2<br>FTD 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_FT-7.0.8.2-2<br>FTDv：<br>Cisco_FTD_Hotfix_FT-7.0.8.2-2 | CSCwq75339：複数のシスコ製品における Snort 3 DCERPC の脆弱性<br>CSCwq75359：複数のシスコ製品における Snort 3 DCERPC の脆弱性 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス FK | 7.0 ～ 7.0.6.3 | Management Center：<br>Cisco_Firepower_Mgmt_Center_Hotfix_FK-7.0.6.99-9 | CSCwd08098：FMC の cacert.pem が期限切れになり、すべてのデバイスが無効として表示されます。<br>「Firewall Management Center Certificate Expiration After 10 Years」を参照してください。 |
| ホットフィックス FJ | 7.0.6.3 | Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_FJ-7.0.6.4-1 | CSCwk48488：Cisco Firepower 2100 シリーズ向け Cisco FTD の TCP/UDP Snort 2 および Snort 3 における DoS の脆弱性 |
| ホットフィックス FI | 7.0.6.3 | Management Center：<br>Cisco_Firepower_Mgmt_Center_Hotfix_FI-7.0.6.4-1 | CSCwj01321：AnyConnect カスタム属性の編集による FMC での XSS の保存 |
| ホットフィックス EN | 7.0.0<br>7.0.x<br>7.0.x.x | F（1000、2500、4500）：<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EN-11<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス EI | 7.0.6 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_EI-7.0.6.1-3<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3<br>FTD 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_EI-7.0.6.1-3<br>FTDv：<br>Cisco_FTD_Hotfix_EI-7.0.6.1-3 | CSCwh23100：Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性<br>CSCwh45108：Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス DC | 7.0.5 | Management Center：<br>Cisco_Firepower_Mgmt_Center_Hotfix_DC-7.0.5.1-5 | CSCwd88641：デバイスモデルと snort エンジンに基づいて VDB パッケージをプッシュするための展開の変更 |
| ホットフィックス S | 7.0.1 | Device Manager 搭載 Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10<br>Device Manager 搭載 Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10<br>Device Manager 搭載 Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10<br>Device Manager 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_S-7.0.1.1-10<br>Device Manager 搭載 FTDv：<br>Cisco_FTD_Hotfix_S-7.0.1.1-10<br>（注）<br>このホットフィックスは、2021 年 12 月 19 日にビルド 9 として最初にリリースされました。2021 年 12 月 21 日にビルド 10 として再リリースされました。前のビルドをインストールした場合は、後のビルドをインストールする必要はありません。<br>このホットフィックスは Device Manager と Device Manager/CDO 管理対象デバイスに適用してください。Management Center 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。 | CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性<br>CSCwa55039 : 7.0.1 用の Firepower Threat Defense ホットフィックス S を 2 回実行するとシステムが失敗する |

# バージョン 6.7.x のホットフィックス

表 *14 :* バージョン *6.7.x* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス EN | 6.7.0<br>6.7.x<br>6.7.x.x | Management Center（すべてのハードウェアモデル）：<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EN-11<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス AA | 6.7.0.3 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_AA-6.7.0.4-2<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_AA-6.7.0.4-2<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_AA-6.7.0.4-2<br>FTD 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_AA-6.7.0.4-2<br>FTDv：<br>Cisco_FTD_Hotfix_AA-6.7.0.4-2 | |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| | | | CSCvw94160：CIAM：OpenSSL CVE-2020-1971<br><br>CSCvx64478：SAML トランザクション中に不要なコンソール出力がある<br><br>CSCvz70595：SAML ハンドラの処理中に ASA でトレースバックが観察される<br><br>CSCvz76966：Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアのドメインネームシステム（DNS）DoS の脆弱性<br><br>CSCvz81480：IPsec で GCM が使用されている場合、アウトバウンドパケットの IV が Nitrox V プラットフォームで更新されない<br><br>CSCvz84850：「タイマーサービス」機能により、ASA および FTD のトレースバックとリロードが発生する<br><br>CSCvz85683：414004 に関する間違った syslog メッセージ形式<br><br>CSCvz85913：ASN.1 文字列が、CISCO-SSL-1.0.2 の ASN1_STR として OpenSSL 内で内部的に表される<br><br>CSCvz89545：アップグレード後の SSL VPN のパフォーマンスの低下と重大な安定性に関する問題<br><br>CSCvz92016：AD の有効なユーザーによる ASA 特権昇格<br><br>CSCwa04461：Cisco ASA ソフトウェアおよび FTD ソフトウェア リモート アクセスの SSL VPN サービス拒否<br><br>CSCwa14485：Cisco Firepower |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| | | | Threat Defense ソフトウェアで確認されたサービス拒否攻撃に対する脆弱性<br><br>CSCwa15185：ASA/FTD：LUA から不要なプロセス呼び出しを削除<br><br>CSCwa33898：Cisco 適応型セキュリティアプライアンスのソフトウェア クライアントレス SSL VPN ヒープオーバーフローの脆弱性<br><br>CSCwa36678：FMC からの展開中にトレースバックを使用してランダム FTD がリロードされる<br><br>CSCwa65389：ASDM を介してインターフェイス構成を変更する場合は、Unicorn Admin Handler で ASA トレースバックおよびリロードが発生 |
| ホットフィックス Y | 6.7.0.2 | Device Manager 搭載 Firepower 1000：<br><br>Cisco_FTD_SSP_FP1K_Hotfix_Y-6.7.0.3-7<br><br>Device Manager 搭載 Firepower 2100：<br><br>Cisco_FTD_SSP_FP2K_Hotfix_Y-6.7.0.3-7<br><br>Device Manager 搭載 Firepower 4100/9300：<br><br>Cisco_FTD_SSP_Hotfix_Y-6.7.0.3-7<br><br>Device Manager 搭載 ASA 5500-X および ISA 3000：<br><br>Cisco_FTD_Hotfix_Y-6.7.0.3-7<br><br>Device Manager 搭載 FTDv：<br><br>Cisco_FTD_Hotfix_Y-6.7.0.3-7<br><br>（注）<br>このホットフィックスは Device Manager と Device Manager/CDO 管理対象デバイスに適用してください。Management Center 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。 | CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス C | 6.7.0<br>6.7.x.x | FTD を使用した ISA 3000：<br>Cisco_FTD_Hotfix_C-6.7.0.999-2 | CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある |

## バージョン 6.6.x のホットフィックス

表 *15*：バージョン *6.6.x* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス EN | 6.6.0<br>6.6.x<br>6.6.x.x | Management Center（1000、1600、2500、2600、4500、4600）：<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EN-11<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス EB | 6.6.7.1 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_EB-6.6.7.2-4 | CSCwd88641：デバイスモデルと snort エンジンに基づいて VDB パッケージをプッシュするための展開の変更 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス DE | 6.6.5<br>6.6.5.1 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8<br>Device Manager 搭載 Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8<br>Device Manager 搭載 Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8<br>Device Manager 搭載 Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8<br>Device Manager 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_DE-6.6.5.2-8<br>Device Manager 搭載 FTDv：<br>Cisco_FTD_Hotfix_DE-6.6.5.2-8<br>ASDM を搭載した ASA FirePOWER：<br>Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8<br>（注）<br>このホットフィックスは、Management Center と Device Manager、Device Manager/CDO、および ASDM 管理対象デバイスにのみ適用してください。Management Center 管理対象デバイスは、Management Center ホットフィックスの対象です。 | CSCwa70008：期限切れの証明書がセキュリティ Intel を引き起こし、マルウェアファイルの事前分類署名の更新が失敗する |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス DA | 6.6.5.1 | Device Manager 搭載 Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4<br>Device Manager 搭載 Firepower 2100<br>Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4<br>Device Manager 搭載 Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4<br>Device Manager 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_DA-6.6.5.2-4<br>Device Manager 搭載 FTDv：<br>Cisco_FTD_Hotfix_DA-6.6.5.2-4<br>（注）<br>このホットフィックスは Device Manager と Device Manager/CDO 管理対象デバイスに適用してください。Management Center 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。 | CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性 |
| ホットフィックス EI | 6.6.0<br>6.6.x<br>6.6.x.x | Management Center 2000、4000：<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EI-15<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス AB | 6.6.1 | FTD を使用した ISA 3000：<br>Cisco_FTD_Hotfix_AB-6.6.1.999-1 | CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある |
| ホットフィックス N | 6.6.0<br>6.6.0.x | FTD を使用した ISA 3000：<br>Cisco_FTD_Hotfix_N-6.6.0.999-1 | CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある |

# バージョン 6.4.0 のホットフィックス

表 *16* : バージョン *6.4.0* のホットフィックス

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス EN | 6.4.0<br>6.4.x<br>6.4.x.x | Management Center（1000、1600、2500、2600、4500、4600）：<br>Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EN-11<br>（注）<br>このホットフィックスにより、これらのモデルの他の BIOS およびファームウェア ホットフィックスがすべて置き換えられます。以前の BIOS およびファームウェア ホットフィックスを適用済みの場合でも、このホットフィックスを適用してください。 | BIOS、CIMC ファームウェア、および RAID コントローラファームウェアが更新されます。<br>ハードウェアの BIOS とファームウェアのホットフィックス （5 ページ）を参照してください。 |
| ホットフィックス EP | 6.4.0.13 | Device Manager 搭載 Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_EP-6.4.0.14-9<br>Device Manager 搭載 Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_EP-6.4.0.14-9<br>Device Manager 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_EP-6.4.0.14-9<br>Device Manager 搭載 FTDv：<br>Cisco_FTD_Hotfix_EP-6.4.0.14-9<br>（注）<br>このホットフィックスは Device Manager と Device Manager/CDO 管理対象デバイスに適用してください。Management Center 管理対象デバイスは、このエクスプロイトに対して脆弱ではありません。 | CSCwa46963：セキュリティ：CVE-2021-44228 -> Log4j 2 の脆弱性 |
| ホットフィックス DV | 6.4.0<br>6.4.0 | FTD を使用した ISA 3000：<br>Cisco_FTD_Hotfix_DV-6.4.0.999-1 | CSCvw53884：ASA5506 の M500IT モデル ソリッド ステート ドライブが 3.2 年のサービス期間後に応答しなくなることがある |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス BM | 6.4.0.9 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2<br>FTD 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_BM-6.4.0.10-2<br>FTDv：<br>Cisco_FTD_Hotfix_BM-6.4.0.10-2 | CSCvt03598：Cisco ASA ソフトウェアおよび FTD ソフトウェア Web サービスの読み取り専用パストラバーサルの脆弱性 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックス AY | 6.4.0.8 | Firepower 1000：<br>Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3<br>FTD 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_AY-6.4.0.9-3<br>FTDv：<br>Cisco_FTD_Hotfix_AY-6.4.0.9-3<br>（注）<br>このホットフィックスを適用する代わりに、バージョン 6.4.0.9 以上にパッチを適用することを推奨します。パッチを適用できない場合は、このホットフィックスは最初にビルド 2 として 2020 年 5 月 6 日にリリースされ、2020 年 5 月 15 日にビルド 3 として再リリースされたことに注意してください。以前のビルドをインストールしている場合は、新しいビルドもインストールしてください。アンインストールする必要はありません。 | CSCvp49481、CSCvp93468：Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアの SSL VPN におけるサービス拒否攻撃に対する脆弱性<br>CSCvs10748：Cisco 適応型アプライアンスおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性<br>CSCvo80853：Cisco Firepower Threat Defense ソフトウェアのパケットにおけるサービス拒否攻撃に対する脆弱性<br>CSCvs50459：Cisco ASA および Cisco FTD の不正な OSPF パケット処理によるサービス拒否攻撃に対する脆弱性<br>CSCvr86783：HA の構成後にスタンバイ FDM の接続が失われる<br>CSCvr92168：OSPF Hello 処理時に OSPF プロセスで ASA/FTD の低速メモリリークが生じる<br>CSCvt15163：Cisco ASA および FTD ソフトウェアの Web サービスに関する情報漏洩の脆弱性<br>CSCvq89361：Cisco Firepower 1000 シリーズの SSL/TLS におけるサービス拒否攻撃に対する脆弱性<br>CSCvu20521：HF のインストール後に OSPF が構成されない |
| ホットフィックス U | 6.4.0.5 および 6.4.0.6 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_U-6.4.0.7-2 | CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性 |
| ホットフィックス T | 6.4.0<br>6.4.0.1 ～ 6.4.0.4 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_T-6.4.0.5-1 | CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性 |

| ホットフィックス | バージョン | プラットフォーム | 解決済み |
|---|---|---|---|
| ホットフィックスAA | 6.4.0.4 ～ 6.4.0.7 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4<br>（注）<br>VDB 329+ に更新し、設定の変更を展開する必要もあります。この操作は、ホットフィックスを適用する前または後に実行できます。 | アプリケーション ID に関する問題を解決します。 |
| ホットフィックスX | 6.4.0.6 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_X-6.4.0.7-2 | CSCvr52109：FTD のアクセスリストにはヒットカウントがあるが、トラフィックがアクセスポリシールールにヒットしていない |
| ホットフィックスF | 6.4.0.2 | Management Center/Management Center Virtual：<br>Cisco_Firepower_Mgmt_Center_Hotfix_F-6.4.0.3-2<br>Firepower 2100：<br>Cisco_FTD_SSP_FP2K_Hotfix_F-6.4.0.3-2<br>Firepower 4100/9300：<br>Cisco_FTD_SSP_Hotfix_F-6.4.0.3-2<br>FTD 搭載 ASA 5500-X および ISA 3000：<br>Cisco_FTD_Hotfix_F-6.4.0.3-2<br>FTDv（VMware、FVM）：<br>Cisco_FTD_Hotfix_F-6.4.0.3-2 | CSCvq34224：マネージャをアップグレードすると、Firepower プライマリ検出エンジン プロセスが終了する。 |

# 支援が必要な場合

### 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：https://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://cisco.com/c/ja_jp/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/

- シスコ通知サービス：https://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

【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。