



## 利用可能なホットフィックス

これらのリリースノートでは、公開されているホットフィックスのページをダウンロードするクイックリンクを提供しています。



(注) 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ー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。

- [Management Center ハードウェアの BIOS およびファームウェアのホットフィックス \(2 ページ\)](#)
- [バージョン 7.4.x のホットフィックス \(3 ページ\)](#)
- [バージョン 7.3.x のホットフィックス \(3 ページ\)](#)
- [バージョン 7.2.x のホットフィックス \(3 ページ\)](#)
- [バージョン 7.1.x のホットフィックス \(5 ページ\)](#)
- [バージョン 7.0.x のホットフィックス \(6 ページ\)](#)
- [バージョン 6.7.x のホットフィックス \(8 ページ\)](#)
- [バージョン 6.6.x のホットフィックス \(12 ページ\)](#)
- [バージョン 6.5.0 のホットフィックス \(15 ページ\)](#)
- [バージョン 6.4.0 のホットフィックス \(18 ページ\)](#)
- [バージョン 6.3.0 のホットフィックス \(21 ページ\)](#)
- [バージョン 6.2.3 のホットフィックス \(24 ページ\)](#)
- [バージョン 6.2.2 のホットフィックス \(29 ページ\)](#)
- [バージョン 6.2.0 のホットフィックス \(31 ページ\)](#)
- [バージョン 6.1.0 のホットフィックス \(35 ページ\)](#)
- [バージョン 6.0.1 のホットフィックス \(38 ページ\)](#)
- [バージョン 6.0.0 のホットフィックス \(39 ページ\)](#)
- [バージョン 5.4.x のホットフィックス \(40 ページ\)](#)

# Management Center ハードウェアの BIOS およびファームウェアのホットフィックス

Management Center 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。Management Center 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 Management Center 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 1: BIOS および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	BIOS	RAID コントローラのファームウェア	CIMC ファームウェア	ホットフィックス
FMC 1600、2600、4600	6.3.0 ~ 7.0	C220M5.4.1.3i.0	51.10.0-3612	4.1 (3d)	BIOS のアップデート ホットフィックス EL
FMC 1000、2500、4500	6.2.3 ~ 7.0	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)	BIOS のアップデート ホットフィックス EL
FMC 2000、4000	6.2.3 ~ 6.6	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS のアップデート ホットフィックス EI
FMC 750、1500、3500	6.2.3 ~ 6.4	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS のアップデート ホットフィックス EI

ホットフィックスは、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。Management Center 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。Management Center に対し、無効な CIMC ユーザー名のログインを有効にするには、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*」の章の手順に従ってください。

シスコ サポートおよびダウンロード サイト へのクイックリンクについては、次の表を参照してください。



- (注) Management Center 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

Management Center 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7.4.xのホットフィックス

バージョン7.4.xには公開されているホットフィックスはありません。

## バージョン7.3.xのホットフィックス

バージョン7.3.xには公開されているホットフィックスはありません。

## バージョン7.2.xのホットフィックス

この表には、公開されているバージョン7.2.xのホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 2: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 BJ	7.2.5	FirePOWER 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_BJ-7.2.5.1-1</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_BJ-7.2.5.1-1</a> Secure Firewall 3100 シリーズ : <a href="#">Cisco_FTD_SSP_FP3K_Hotfix_BJ-7.2.5.1-1</a> Firepower 4100/9300 <a href="#">Cisco_FTD_SSP_Hotfix_BJ-7.2.5.1-1</a> ISA 3000 : <a href="#">Cisco_FTD_Hotfix_BJ-7.2.5.1-1</a> Threat Defense 仮想 : <a href="#">Cisco_FTD_Hotfix_BJ-7.2.5.1-1</a>	<b>CSCwh23100</b> : 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  <b>CSCwh45108</b> : 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 AW	7.2.4	FirePOWER 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1</a> Secure Firewall 3100 シリーズ : <a href="#">Cisco_FTD_SSP_FP3K_Hotfix_AW-7.2.4.1-1</a> Firepower 4100/9300 <a href="#">Cisco_FTD_SSP_Hotfix_AW-7.2.4.1-1</a> ISA 3000 : <a href="#">Cisco_FTD_Hotfix_AW-7.2.4.1-1</a> Threat Defense 仮想 : <a href="#">Cisco_FTD_Hotfix_AW-7.2.4.1-1</a>	<b>CSCwf71606</b> : 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 : <a href="#">Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2</a> (注) 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。	<b>CSCwf28592</b> : 一部の特定のシナリオでは、オブジェクトオブ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

この表には、公開されているバージョン 7.1.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 3: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 Q	7.1.0.2	Secure Firewall 3100 シリーズ : <a href="#">Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2</a>	<a href="#">CSCwb88651</a> : 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 <a href="#">CSCwb28334</a> : 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 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_P-7.1.0.2-2</a> Firepower 4100/9300 <a href="#">Cisco_FTD_SSP_Hotfix_P-7.1.0.2-2</a> ISA 3000 : <a href="#">Cisco_FTD_Hotfix_P-7.1.0.2-2</a> FTDv : <a href="#">Cisco_FTD_Hotfix_P-7.1.0.2-2</a>	<a href="#">CSCwb88651</a> : 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 <a href="#">CSCwb28334</a> : 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	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 A	7.1.0	<p>FDM を使用した Firepower 1000 シリーズ :  <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_A-7.1.0.1-7</a></p> <p>FDM を使用した Firepower 2100 シリーズ :  <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_A-7.1.0.1-7</a></p> <p>FDM を使用した Firepower 4100/9300 :  <a href="#">Cisco_FTD_SSP_Hotfix_A-7.1.0.1-7</a></p> <p>FDM を使用した ISA 3000 :  <a href="#">Cisco_FTD_Hotfix_A-7.1.0.1-7</a></p> <p>FDM を使用した FTDv :  <a href="#">Cisco_FTD_Hotfix_A-7.1.0.1-7</a></p> <p>(注) FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 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。</p>	<p><a href="#">CSCwa46963</a> : セキュリティ :            CVE-2021-44228 -&gt; Log4j 2 の脆弱性</p>

## バージョン 7.0.x のホットフィックス

この表には、公開されているバージョン 7.0.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 4: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 EI	7.0.6	FirePOWER 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_EI-7.0.6.1-3</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3</a> FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_EI-7.0.6.1-3</a> FTDv : <a href="#">Cisco_FTD_Hotfix_EI-7.0.6.1-3</a>	<a href="#">CSCwh23100</a> : 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 <a href="#">CSCwh45108</a> : 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 DC	7.0.5	FMC : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_DC-7.0.5.1-5</a>	<a href="#">CSCwd88641</a> : 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 S	7.0.1	<p>FDM を使用した Firepower 1000 シリーズ：  <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10</a></p> <p>FDM を使用した Firepower 2100 シリーズ：  <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10</a></p> <p>FDM を使用した Firepower 4100/9300：  <a href="#">Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10</a></p> <p>FDM を使用した ASA 5500-X シリーズおよび ISA 3000：  <a href="#">Cisco_FTD_Hotfix_S-7.0.1.1-10</a></p> <p>FDM を使用した FTDv：  <a href="#">Cisco_FTD_Hotfix_S-7.0.1.1-10</a></p> <p>(注) 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。</p> <p>FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスポイトに対して脆弱ではありません。</p>	<p><a href="#">CSCwa46963</a>：セキュリティ：CVE-2021-44228 -&gt; Log4j 2 の脆弱性</p> <p><a href="#">CSCwa55039</a>：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</p>
ホットフィックス EL	7.0.0 7.0.x 7.0.x.x	<p>FMC (すべてのハードウェアモデル)：  <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EL-7</a></p> <p>(注) このホットフィックスにより、これらの Management Center 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。</p>	<p>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。</p> <p><a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。</p>

## バージョン 6.7.x のホットフィックス

この表には、公開されているバージョン 6.7.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。



表 5: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 AA	6.7.0.3	FirePOWER 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_AA-6.7.0.4-2</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_AA-6.7.0.4-2</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_AA-6.7.0.4-2</a> ASA 5500-X シリーズおよび ISA 3000 : <a href="#">Cisco_FTD_Hotfix_AA-6.7.0.4-2</a> FTDv : <a href="#">Cisco_FTD_Hotfix_AA-6.7.0.4-2</a>	

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
			<p><a href="#">CSCvw94160</a> : CIAM : OpenSSL CVE-2020-1971</p> <p><a href="#">CSCvx64478</a> : SAML トランザクション中に不要なコンソール出力がある</p> <p><a href="#">CSCvz70595</a> : 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</p> <p><a href="#">CSCvz76966</a> : 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</p> <p><a href="#">CSCvz81480</a> : 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</p> <p><a href="#">CSCvz84850</a> : 「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</p> <p><a href="#">CSCvz85683</a> : 414004 に関する間違った syslog メッセージ形式</p> <p><a href="#">CSCvz85913</a> : 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</p> <p><a href="#">CSCvz89545</a> : 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</p> <p><a href="#">CSCvz92016</a> : AD の有効なユーザーによる ASA 特権昇格</p> <p><a href="#">CSCwa04461</a> : 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</p> <p><a href="#">CSCwa14485</a> : Cisco Firepower</p>

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
			<p>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</p> <p><a href="#">CSCwa15185</a> : ASA/FTD : LUA から不要なプロセス呼び出しを削除</p> <p><a href="#">CSCwa33898</a> : 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</p> <p><a href="#">CSCwa36678</a> : 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</p> <p><a href="#">CSCwa65389</a> : 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</p>
<p>ホットフィックス Y</p>	<p>6.7.0.2</p>	<p>FDM を使用した Firepower 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_Y-6.7.0.3-7</a></p> <p>FDM を使用した Firepower 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_Y-6.7.0.3-7</a></p> <p>FDM を使用した Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_Y-6.7.0.3-7</a></p> <p>FDM を使用した ASA 5500-X シリーズおよび ISA 3000 : <a href="#">Cisco_FTD_Hotfix_Y-6.7.0.3-7</a></p> <p>FDM を使用した FTDv : <a href="#">Cisco_FTD_Hotfix_Y-6.7.0.3-7</a></p> <p>(注) FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 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。</p>	<p><a href="#">CSCwa46963</a> : セキュリティ : CVE-2021-44228 -&gt; Log4j 2 の脆弱性</p>

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 EL	6.7.0 6.7.x.x	FMC (すべてのハードウェアモデル) : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EL-7</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス C	6.7.0 6.7.x.x	FTD を使用した ISA 3000 : <a href="#">Cisco_FTD_Hotfix_C-6.7.0.999-2</a>	<a href="#">CSCvw53884</a> : 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

この表には、公開されているバージョン 6.6.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 6: 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 EB	6.6.7.1	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_EB-6.6.7.2-4</a>	<a href="#">CSCwd88641</a> : 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 6.6.5.1	<p>FMC/FMCv :</p> <p><a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8</a></p> <p>FDM を使用した Firepower 1000 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8</a></p> <p>FDM を使用した Firepower 2100 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8</a></p> <p>FDM を使用した Firepower 4100/9300 :</p> <p><a href="#">Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8</a></p> <p>FDM を使用した ASA 5500-X シリーズおよび ISA 3000 :</p> <p><a href="#">Cisco_FTD_Hotfix_DE-6.6.5.2-8</a></p> <p>FDM を使用した FTDv :</p> <p><a href="#">Cisco_FTD_Hotfix_DE-6.6.5.2-8</a></p> <p>ASDM を搭載した ASA FirePOWER :</p> <p><a href="#">Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8</a></p> <p>(注) FMC と、FDM、FDM/CDO、および ASDM 管理対象デバイスにのみこのホットフィックスを適用してください。FMC 管理対象デバイスには、FMC ホットフィックスによって対応します。</p>	<p><a href="#">CSCwa70008</a> : 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</p>

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	<p>FDM を使用した Firepower 1000 シリーズ :  <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4</a></p> <p>FDM を使用した Firepower 2100 シリーズ  <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4</a></p> <p>FDM を使用した Firepower 4100/9300 :  <a href="#">Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4</a></p> <p>FDM を使用した ASA 5500-X シリーズおよび ISA 3000 :  <a href="#">Cisco_FTD_Hotfix_DA-6.6.5.2-4</a></p> <p>FDM を使用した FTDv :  <a href="#">Cisco_FTD_Hotfix_DA-6.6.5.2-4</a></p> <p>(注) FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 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。</p>	CSCwa46963 : セキュリティ : CVE-2021-44228 -> Log4j 2 の脆弱性
ホットフィックス EL	6.6.0 6.6.x 6.6.x.x	<p>FMC 1000、1600、2500、2600、4500、4600 :  <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EL-7</a></p> <p>(注) このホットフィックスにより、これらの Management Center 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。</p>	<p>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。</p> <p><a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。</p>
ホットフィックス EI	6.6.0 6.6.x 6.6.x.x	<p>FMC 2000、4000 :  <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EI-15</a></p> <p>(注) このホットフィックスにより、これらの Management Center 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。</p>	<p>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。</p> <p><a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。</p>

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 AB	6.6.1	FTD を使用した ISA 3000 : <a href="#">Cisco_FTD_Hotfix_AB-6.6.1.999-1</a>	<a href="#">CSCvw53884</a> : 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 6.6.0.x	FTD を使用した ISA 3000 : <a href="#">Cisco_FTD_Hotfix_N-6.6.0.999-1</a>	<a href="#">CSCvw53884</a> : 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 6.5.0 のホットフィックス

この表では、公開されているバージョン 6.5.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 7:バージョン 6.5.0 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 EL	6.5.0 6.5.0	FMC 1000、1600、2500、2600、4500、4600 : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_650_EL-7</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> 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 EI	6.5.0 6.5.0	FMC 2000、4000 : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_650_EI-15</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス T	6.5.0 6.5.0	FTD を使用した ISA 3000 : <a href="#">Cisco_FTD_Hotfix_T-6.5.0.999-1</a>	<a href="#">CSCvw53884</a> : 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 O	6.5.0.4	FirePOWER 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_O-6.5.0.5-3</a>  FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_O-6.5.0.5-3</a>  Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_O-6.5.0.5-3</a>  FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_O-6.5.0.5-3</a>  FTDv : <a href="#">Cisco_FTD_Hotfix_O-6.5.0.5-3</a>	<a href="#">CSCvt03598</a> : 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 H	6.5.0.4	<p>FirePOWER 1000 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP1K_Hotfix_H-6.5.0.5-2</a></p> <p>FirePOWER 2100 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP2K_Hotfix_H-6.5.0.5-2</a></p> <p>Firepower 4100/9300 :</p> <p><a href="#">Cisco_FTD_SSP_Hotfix_H-6.5.0.5-2</a></p> <p>FTD を搭載した ASA 5500-X シリーズおよび ISA 3000</p> <p><a href="#">Cisco_FTD_Hotfix_H-6.5.0.5-2</a></p> <p>FTDv :</p> <p><a href="#">Cisco_FTD_Hotfix_H-6.5.0.5-2</a></p>	<p><a href="#">CSCvp93468</a> : Cisco ASA ソフトウェアと 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</p> <p><a href="#">CSCvr92168</a> : 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</p> <p><a href="#">CSCvs10748</a> : Cisco 適応型アプリケーションおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性</p> <p><a href="#">CSCvs50459</a> : 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</p> <p><a href="#">CSCvt15163</a> : 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</p> <p><a href="#">CSCvu20521</a> : HF のインストール後に OSPF が構成されない</p>
ホットフィックス D	6.5.0.2	<p>FirePOWER 1000 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP1K_Hotfix_D-6.5.0.3-3</a></p> <p>FirePOWER 2100 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP2K_Hotfix_D-6.5.0.3-3</a></p> <p>Firepower 4100/9300 :</p> <p><a href="#">Cisco_FTD_SSP_Hotfix_D-6.5.0.3-3</a></p> <p>FTD を搭載した ASA 5500-X シリーズおよび ISA 3000</p> <p><a href="#">Cisco_FTD_Hotfix_D-6.5.0.3-3</a></p> <p>FTDv :</p> <p><a href="#">Cisco_FTD_Hotfix_D-6.5.0.3-3</a></p>	<p><a href="#">CSCvs55990</a> : ローカル/FDM で管理されている FTD 上に設定された SIDNS を使用した展開が失敗する</p>

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 B	6.5.0 6.5.0.1 および 6.5.0.2	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_B-6.5.0.3-3</a> (注) VDB 329+に更新し、設定の変更を展開する必要があります。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 C	6.5.0.1	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_C-6.5.0.2-2</a>	<a href="#">CSCvr52109</a> : 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

## バージョン 6.4.0 のホットフィックス

この表では、公開されているバージョン 6.4.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 8: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 EP	6.4.0.13	FDM を使用した Firepower 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_EP-6.4.0.14-9</a> FDM を使用した Firepower 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_EP-6.4.0.14-9</a> FDM を使用した ASA 5500-X シリーズおよび ISA 3000 : <a href="#">Cisco_FTD_Hotfix_EP-6.4.0.14-9</a> FDM を使用した FTDv : <a href="#">Cisco_FTD_Hotfix_EP-6.4.0.14-9</a> (注) FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 管理対象デバイスは、このエクスポloitに対して脆弱ではありません。	<a href="#">CSCwa46963</a> : 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 EL	6.4.0 6.4.0	FMC 1000、1600、2500、2600、4500、4600 : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EL-7</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス EI	6.4.0 6.4.0	FMC 750、1500、2000、3500、4000 : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EI-15</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス DV	6.4.0 6.4.0	FTD を使用した ISA 3000 : <a href="#">Cisco_FTD_Hotfix_DV-6.4.0.999-1</a>	<a href="#">CSCvw53884</a> : 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 BM	6.4.0.9	FirePOWER 1000 シリーズ : <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2</a> FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_BM-6.4.0.10-2</a> FTDv : <a href="#">Cisco_FTD_Hotfix_BM-6.4.0.10-2</a>	<a href="#">CSCvt03598</a> : 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	<p>FirePOWER 1000 シリーズ： <a href="#">Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3</a></p> <p>FirePOWER 2100 シリーズ： <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3</a></p> <p>Firepower 4100/9300： <a href="#">Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3</a></p> <p>FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_AY-6.4.0.9-3</a></p> <p>FTDv： <a href="#">Cisco_FTD_Hotfix_AY-6.4.0.9-3</a></p> <p>(注) 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。</p>	<p><a href="#">CSCvp49481</a>、<a href="#">CSCvp93468</a>：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</p> <p><a href="#">CSCvs10748</a>：Cisco 適応型アプリケーションおよび Firepower Threat Defense におけるサービス拒否攻撃に対する脆弱性</p> <p><a href="#">CSCvo80853</a>：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</p> <p><a href="#">CSCvs50459</a>：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</p> <p><a href="#">CSCvr86783</a>：HA の構成後にスタンバイ EDM の接続が失われる</p> <p><a href="#">CSCvr92168</a>：OSPF Hello 処理時に OSPF プロセスで ASA/FTD の低速メモリークが生じる</p> <p><a href="#">CSCvt15163</a>：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</p> <p><a href="#">CSCvq89361</a>：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</p> <p><a href="#">CSCvu20521</a>：HF のインストール後に OSPF が構成されない</p>
ホットフィックス U	6.4.0.5 および 6.4.0.6	<p>FMC/FMCv： <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_U-6.4.0.7-2</a></p>	<a href="#">CSCvr95287</a> ：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 6.4.0.1 ~ 6.4.0.4	<p>FMC/FMCv： <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_T-6.4.0.5-1</a></p>	<a href="#">CSCvr95287</a> ：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	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4</a>  (注) 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	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_X-6.4.0.7-2</a>	<a href="#">CSCvr52109</a> : 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	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_F-6.4.0.3-2</a> FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_F-6.4.0.3-2</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_F-6.4.0.3-2</a> FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_F-6.4.0.3-2</a> FTDv (VMware、FVM) : <a href="#">Cisco_FTD_Hotfix_F-6.4.0.3-2</a>	<a href="#">CSCvq34224</a> : 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。

## バージョン 6.3.0 のホットフィックス

この表では、公開されているバージョン 6.3.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 9:バージョン 6.3.0 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 EL	6.3.0 6.3.0.x	FMC 1000、1600、2500、2600、4500、4600 : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_630_EL-7</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス EI	6.3.0 6.3.0.x	FMC 750、1500、2000、3500、4000 : <a href="#">Cisco_Firepower_Mgmt_Center_BIOSUPDATE_630_EI-15</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス AZ	6.3.0 6.3.0.x	FTD を使用した ISA 3000 : <a href="#">Cisco_FTD_Hotfix_AZ-6.3.0.999-1</a>	<a href="#">CSCvw53884</a> : 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 AV	6.3.0.5	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_AV-6.3.0.6-3</a>  Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_AV-6.3.0.6-3</a>  FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_AV-6.3.0.6-3</a>  FTDv : <a href="#">Cisco_FTD_Hotfix_AV-6.3.0.6-3</a>	<a href="#">CSCvt03598</a> : 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 AO	6.3.0.5	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_AO-6.3.0.6-2</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_AO-6.3.0.6-2</a> FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_AO-6.3.0.6-2</a> FTDv : <a href="#">Cisco_FTD_Hotfix_AO-6.3.0.6-2</a>	<a href="#">CSCvp93468</a> : Cisco ASA ソフトウェアと 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 <a href="#">CSCvo80853</a> : 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 <a href="#">CSCvr07419</a> <a href="#">CSCvs50459</a> : 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 <a href="#">CSCvs10748</a> : 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 <a href="#">CSCvp49481</a> : Cisco ASA ソフトウェアと 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 <a href="#">CSCvt15163</a> : 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 <a href="#">CSCvr55825</a> : Cisco ASA および FTD ソフトウェアのストラバースルの脆弱性
ホットフィックス AI	6.3.0 6.3.0.1 ~ 6.3.0.5	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_AI-6.3.0.6-2</a>	<a href="#">CSCvr95287</a> : Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
ホットフィックス AK	6.3.0.5	FMC/FMCv : <a href="#">Cisco_Firepower_Mgmt_Center_Hotfix_AK-6.3.0.6-2</a> (注) VDB 329+ に更新し、設定の変更を展開する必要があります。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	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	6.3.0.3	ASA 5508-X および FTD 搭載の ASA 5516-X : <a href="#">Cisco_FTD_Hotfix_AA-6.3.0.4-2</a>	<a href="#">CSCvp36425</a> : Cisco ASA & FTD ソフトウェアの暗号化 TLS および SSL ドライバにおけるサービス拒否攻撃に対する脆弱性
ホットフィックス W	6.3.0.3	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_W-6.3.0.4-4</a>	<a href="#">CSCvn77248</a> : シスコ セキュアブート ハードウェアにおける改ざんの脆弱性
ホットフィックス B	6.3.0	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_B-6.3.0.1-1</a>  (注) 複数のインスタンス (1つのセキュリティモジュールに複数の論理デバイス) を設定している場合は、このホットフィックスを適用しないでください。	<a href="#">CSCvo02577</a> : SSL HW 復号化によるバッファ枯渇

## バージョン 6.2.3 のホットフィックス

この表では、公開されているバージョン 6.2.3 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 10: バージョン 6.2.3 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 EM	6.2.3.17	FDM を使用した Firepower 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_EM-6.2.3.18-13</a>  FDM を使用した ASA 5500-X シリーズおよび ISA 3000 : <a href="#">Cisco_FTD_Hotfix_EM-6.2.3.18-13</a>  FDM を使用した FTDv : <a href="#">Cisco_FTD_Hotfix_EM-6.2.3.18-13</a>  (注) FDM および FDM/CDO 管理対象デバイスにこのホットフィックスを適用してください。FMC 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。	<a href="#">CSCwa46963</a> : 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 EL	6.2.3 6.2.3.x	FMC 1000、2500、4500 : <a href="#">Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス EI	6.2.3 6.2.3.x	FMC 750、1500、2000、3500、4000 : <a href="#">Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EI-15</a>  (注) このホットフィックスにより、これらの Management Center 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。  <a href="#">Management Center ハードウェアの BIOS およびファームウェアのホットフィックス (2 ページ)</a> を参照してください。
ホットフィックス EH	6.2.3 6.2.3.x	FTD を搭載した ASA 5506-X シリーズ : <a href="#">Cisco_FTD_Hotfix_EH-6.2.3.999-6</a>	<a href="#">CSCvw53884</a> : 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 DT	6.2.3.15	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_DT-6.2.3.16-3</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_DT-6.2.3.16-3</a> FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_DT-6.2.3.16-3</a> FTDv : <a href="#">Cisco_FTD_Hotfix_DT-6.2.3.16-3</a>	<a href="#">CSCvr55825</a> : Cisco ASA および FTD ソフトウェアのパストラバーサル脆弱性 <a href="#">CSCvp49481</a> 、 <a href="#">CSCvp93468</a> : 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 <a href="#">CSCvp16945</a> 、 <a href="#">CSCvp16949</a> : Cisco ASA ソフトウェアおよび Cisco FTD ソフトウェアの MGCP におけるサービス拒否攻撃に対する脆弱性 <a href="#">CSCvo62077</a> : Cisco Firepower Threat Defense ソフトウェアの VPN システムロギングにおけるサービス拒否攻撃に対する脆弱性 <a href="#">CSCvs10748</a> : 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 <a href="#">CSCvs50459</a> : 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 <a href="#">CSCvo80853</a> : 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 <a href="#">CSCvr07419</a> : Cisco ASA および FTD ソフトウェアの IPv6 DNS におけるサービス拒否攻撃に対する脆弱性 <a href="#">CSCvt15163</a> : 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

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 DW	6.2.3.15	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_DW-6.2.3.16-6</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_DW-6.2.3.16-6</a> FTD を搭載した ASA 5500-X シリーズおよび ISA 3000 <a href="#">Cisco_FTD_Hotfix_DW-6.2.3.16-6</a> FTDv : <a href="#">Cisco_FTD_Hotfix_DW-6.2.3.16-6</a>	<a href="#">CSCvs84578</a> : 4100/9300 プラットフォーム上の FTD を 6.2.3.15 にアップグレードすると、SSHD が破損し、FTD インスタンスの起動が妨げられる <a href="#">CSCvs84713</a> : ASA55XX/ISA 3000/FTDv 上の FTD を 6.2.3.15 ビルド 38 にアップグレードした後、デバイスに SSH 接続できない <a href="#">CSCvs95725</a> : 6.2.3.15 で実行されている仮想 FTD が SSH 要求をブロックし、FMC との接続を失う
ホットフィックス DO	6.2.3 6.2.3.1 ~ 6.2.3.15	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_DO-6.2.3.16-3</a>	<a href="#">CSCvr95287</a> : Cisco Firepower Management Center LDAP 認証バypass の脆弱性
ホットフィックス DQ	6.2.3.15	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.2.3.16-2</a>  (注) VDB 329+ に更新し、設定の変更を展開する必要があります。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 CY	6.2.3.14	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_CY-6.2.3.15-2</a>	<a href="#">CSCvq34224</a> : 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。
ホットフィックス CK	6.2.3.12	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_CK-6.2.3.13-1</a>	<a href="#">CSCvn77248</a> : シスコセキュアブートハードウェアにおける改ざんの脆弱性
ローカルマルウェア証明書のホットフィックス	6.2.3 6.2.3.x	FMC/FMCv : <a href="#">Hotfix_Local_Malware_Cert-6.2.3.999-4</a>	<a href="#">CSCvm81052</a> : 証明書チェーンが無効であるため、ローカルマルウェア検出の更新が FMC にダウンロードされない。

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 H	6.2.3 6.2.3.1 ~ 6.2.3.3	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_H-6.2.3.999-5</a> Firepower 7000/8000 シリーズ : <a href="#">Sourcefire_3D_Device_S3_Hotfix_H-6.2.3.999-5</a> ASA FirePOWER : <a href="#">Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5</a> NGIPSv : <a href="#">Sourcefire_3D_Device_VMware_Hotfix_H-6.2.3.999-5</a>	<a href="#">CSCvj07038</a> : Firepower デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス G	6.2.3 6.2.3.1 ~ 6.2.3.3	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_G-6.2.3.999-6</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_G-6.2.3.999-6</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_G-6.2.3.999-6</a> FTDv (VMware、KVM、AWS) : <a href="#">Cisco_FTD_Hotfix_G-6.2.3.999-6</a>	<a href="#">CSCvj07038</a> : Firepower デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス T	6.2.3.1 ~ 6.2.3.3	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_T-6.2.3.4-4</a>	<a href="#">CSCvk06176</a> : 実行ファイルが誤っているため SSEConnector が起動しない。
ホットフィックス A	6.2.3	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_A-6.2.3.1-10</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_A-6.2.3.1-10</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_A-6.2.3.1-10</a> FTDv (VMware、KVM、AWS) : <a href="#">Cisco_FTD_Hotfix_A-6.2.3.1-10</a>	<a href="#">CSCvg65072</a> : ASA、Threat Defense、および AnyConnect セキュリティ モビリティ クライアントの SAML 認証セッションの固定における脆弱性。 <a href="#">CSCvi16029</a> : ASA Web インターフェイス認証のバイパス。

## バージョン 6.2.2 のホットフィックス

この表では、公開されているバージョン 6.2.2 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 11:バージョン 6.2.2 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 CB	6.2.2.5	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_CB-6.2.2.6-2</a>	<a href="#">CSCvn77248</a> : シスコ セキュアブート ハードウェアにおける改ざんの脆弱性
ホットフィックス BY	6.2.2 6.2.2.x	FMC (すべてのハードウェアモデル) : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1</a>	RAID コントローラのファームウェアを更新します。
ローカルマルウェア証明書のホットフィックス	6.2.2 6.2.2.x	FMC/FMCv : <a href="#">Hotfix_Local_Malware_Cert-6.2.2.999-4</a>  (注) バージョン 6.2.3 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	<a href="#">CSCvm81052</a> : 証明書チェーンが無効であるため、ローカルマルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス BZ	6.2.2.4	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_BZ-6.2.2.5-4</a>  Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_BZ-6.2.2.5-4</a>  FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_BZ-6.2.2.5-4</a>  FTDv (VMware、KVM、AWS) : <a href="#">Cisco_FTD_Hotfix_BZ-6.2.2.5-4</a>	<a href="#">CSCvm43975</a> : SIP インспекションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU。

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 BN	6.2.2 6.2.2.1 ~ 6.2.2.4	<p>FMC/FMCv :</p> <p><a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_BN-6.2.2.999-5</a></p> <p>FirePOWER 2100 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP2K_Hotfix_BN-6.2.2.999-5</a></p> <p>Firepower 4100/9300 :</p> <p><a href="#">Cisco_FTD_SSP_Hotfix_BN-6.2.2.999-5</a></p> <p>FTD を搭載した ASA 5500-X シリーズ :</p> <p><a href="#">Cisco_FTD_Hotfix_BN-6.2.2.999-5</a></p> <p>FTDv (VMware、KVM、AWS) :</p> <p><a href="#">Cisco_FTD_Hotfix_BN-6.2.2.999-5</a></p> <p>Firepower 7000/8000 シリーズ :</p> <p><a href="#">Sourcefire_3D_Device_S3_Hotfix_BN-6.2.2.999-5</a></p> <p>ASA FirePOWER :</p> <p><a href="#">Cisco_Network_Sensor_Hotfix_BN-6.2.2.999-5</a></p> <p>NGIPSv :</p> <p><a href="#">Sourcefire_3D_Device_VMware_Hotfix_BN-6.2.2.999-5</a></p>	<p><a href="#">CSCvj07038</a> : Firepower デバイスは Threat Grid 証明書を信頼する必要があります。</p>
ホットフィックス BS	6.2.2.4	<p>FMC/FMCv :</p> <p><a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_BS-6.2.2.5-3</a></p>	<p><a href="#">CSCvk17382</a> : ルールの評価の処理中に Snort が予期せず終了する</p>
ホットフィックス BD	6.2.2.2	<p>FirePOWER 2100 シリーズ :</p> <p><a href="#">Cisco_FTD_SSP_FP2K_Hotfix_BD-6.2.2.3-4</a></p> <p>Firepower 4100/9300 :</p> <p><a href="#">Cisco_FTD_SSP_Hotfix_BD-6.2.2.3-4</a></p> <p>FTD を搭載した ASA 5500-X シリーズ :</p> <p><a href="#">Cisco_FTD_Hotfix_BD-6.2.2.3-4</a></p> <p>FTDv (VMware、KVM、AWS) :</p> <p><a href="#">Cisco_FTD_Hotfix_BD-6.2.2.3-4</a></p>	<p><a href="#">CSCvi16029</a>、<a href="#">CSCvg65072</a> : ASA、Threat Defense、および AnyConnect セキュリティ モビリティ クライアントの SAML 認証セッションの固定における脆弱性。</p> <p><a href="#">CSCvi16029</a>: ASA Web インターフェイス認証のバイパス。</p>

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 AO	6.2.2.1	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_AO-6.2.2.2-1</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_AO-6.2.2.2-1</a> FTDv : <a href="#">Cisco_FTD_Hotfix_AO-6.2.2.2-1</a> (注) ホットフィックス AB はホットフィックス AO に置換されます。ホットフィックス AB をインストールしている場合は、ホットフィックス AO をインストールする必要があります。	<a href="#">CSCvg35618</a> : Cisco 適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 <a href="#">CSCvh79732</a> 、 <a href="#">CSCvh81737</a> 、 <a href="#">CSCvh81870</a> : Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ホットフィックス AN	6.2.2.1	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_AN-6.2.2.2-4</a> (注) ホットフィックス AC はホットフィックス AN に置換されます。ホットフィックス AC をインストールしている場合は、ホットフィックス AN をインストールする必要があります。	<a href="#">CSCvg35618</a> : Cisco 適応型セキュリティ アプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 <a href="#">CSCvh79732</a> 、 <a href="#">CSCvh81737</a> 、 <a href="#">CSCvh81870</a> : Cisco 適応型セキュリティ アプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ホットフィックス Z	6.2.2 6.2.2.1	FTDv : <a href="#">Cisco_FTD_Hotfix_Z-6.2.2.2-7</a>	<a href="#">CSCvg68914</a> : TCP トラフィック処理中 (StreamQueue) のセグメンテーション違反。
ホットフィックス D	6.2.2	FirePOWER 2100 シリーズ : <a href="#">Cisco_FTD_SSP_FP2K_Hotfix_D-6.2.2.1-4</a>	<a href="#">CSCvg06695</a> : 検出サービス モジュールの障害により FP2100 Threat Defense ペアがステータスのレポートに失敗する。

## バージョン 6.2.0 のホットフィックス

この表では、公開されているバージョン 6.2.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 12: バージョン 6.2.0 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
ローカルマルウェア証明書のホットフィックス	6.2.0 6.2.0.x	FMC/FMCv : <a href="#">Hotfix_Local_Malware_Cert-6.2.0.999-1</a>  (注) バージョン 6.2.2 または 6.2.3 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	<a href="#">CSCvm81052</a> : 証明書チェーンが無効であるため、ローカルマルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス CE	6.2.0.6	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_CE-6.2.0.7-1</a>  FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_CE-6.2.0.7-1</a>  FTDv : <a href="#">Cisco_FTD_Hotfix_CE-6.2.0.7-1</a>	<a href="#">CSCvm43975</a> : SIP インспекションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU。
ホットフィックス BX	6.2.0 6.2.0.1 ~ 6.2.0.5	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_BX-6.2.0.999-5</a>  FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_BX-6.2.0.999-5</a>  FTDv : <a href="#">Cisco_FTD_Hotfix_BX-6.2.0.999-5</a>	<a href="#">CSCvj07038</a> : Firepower デバイスは Threat Grid 証明書を信頼する必要があります。
ホットフィックス BW	6.2.0 6.2.0.1 ~ 6.2.0.5	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_BW-6.2.0.999-6</a>  Firepower 7000/8000 シリーズ : <a href="#">Sourcefire_3D_Device_S3_Hotfix_BW-6.2.0.999-6</a>  ASA FirePOWER : <a href="#">Cisco_Network_Sensor_Hotfix_BW-6.2.0.999-6</a>  NGIPSv : <a href="#">Sourcefire_3D_Device_Virtual64_VMware_Hotfix_BW-6.2.0.999-6</a>	<a href="#">CSCvj07038</a> : Firepower デバイスは Threat Grid 証明書を信頼する必要があります。



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 BN	6.2.0.4	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_BN-6.2.0.5-3</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_BN-6.2.0.5-3</a> FTDv : <a href="#">Cisco_FTD_Hotfix_BN-6.2.0.5-3</a>	<a href="#">CSCvg35618</a> : Cisco 適応型セキュリティ アプライアンスの Remote Code Execution と サービス拒否攻撃に対する脆弱性。 <a href="#">CSCvh79732</a> 、 <a href="#">CSCvh81737</a> 、 <a href="#">CSCvh81870</a> : Cisco 適応型セキュリティ アプライアンスにおける サービス拒否攻撃に対する脆弱性。
ホットフィックス BH	6.2.0.3	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_BH-6.2.0.4-1</a>	<a href="#">CSCvg32885</a> : 6.2.0.3 にアップグレードした後、一部のアクセスコントロール ルールの欠落で編集または展開ができない。
ホットフィックス AQ	6.2.0.2	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_AQ-6.2.0.3-3</a>	<a href="#">CSCve82386</a> : Threat Defense クラスタでの診断ポート チャネルインターフェイスの IP プールの設定に失敗する。
ホットフィックス U	6.2.0.1	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_U-6.2.0.2-1</a>	<a href="#">CSCve44987</a> : eStreamer サービスが破損したメッセージと、接続されていない状態のスパム ログ ファイルを送信する。
ホットフィックス S	6.2.0.1	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_S-6.2.0.2-1</a>	<a href="#">CSCve35816</a> : <code>handle_host_address_changes()</code> の null ポインタの逆参照による <code>SFDataCorrelator segfault</code> 。
ホットフィックス N	6.2.0	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_N-6.2.0.1-1</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_N-6.2.0.1-1</a> FTDv : <a href="#">Cisco_FTD_Hotfix_N-6.2.0.1-1</a>	<a href="#">CSCve02069</a> : Cisco FirePOWER の検出エンジンの SSL 復号時のメモリ使用による Denial of Service (DoS) の脆弱性。
ホットフィックス G	6.2.0	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_G-6.2.0.1-4</a>	<a href="#">CSCvd27278</a> : インポートリスト内のユーザーのいずれかが削除されていると、UIMP はすべてのユーザーのインポートに失敗する。

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 F	6.2.0	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_F-6.2.0.1-3</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_F-6.2.0.1-3</a> FTDv : <a href="#">Cisco_FTD_Hotfix_F-6.2.0.1-3</a>	<a href="#">CSCve96586</a> : 9K ブロック カウンタには Snort ヘパンとされたトラフィックを停止し、Snort をビジー状態にする問題がある。
ホットフィックス B	6.2.0	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_B-6.2.0.1-2</a>	<a href="#">CSCve57533</a> : デルタ スプリットの論理障害によりポリシーの展開が失敗する場合がある。
ホットフィックス AM	6.2.0.2	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_AM-6.2.0.3-3</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_AM-6.2.0.3-3</a> FTDv : <a href="#">Cisco_FTD_Hotfix_AM-6.2.0.3-3</a>	<a href="#">CSCve04326</a> : スタンバイは出力インターフェイスがダウンしているときのトラフィックの転送にブラックホールではなく CCL を使用する必要があります。
ホットフィックス AG	6.2.0 6.2.0.1	FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_AG-6.2.0.2-3</a>	<a href="#">CSCve95026</a> : UUID が EOAttributes にないと、Threat Defense デバイスで <code>ids_event_alertercauses</code> により CPU 使用率が高くなる。
ホットフィックス AC	6.2.0.2	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_AC-6.2.0.3-2</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_AC-6.2.0.3-2</a> FTDv : <a href="#">Cisco_FTD_Hotfix_AC-6.2.0.3-2</a>	<a href="#">CSCve71661</a> : Firepower Threat Defense : マルチキャストと BPDU トラフィックが <code>dst-l2_lookup-fail</code> によりドロップされる。
ホットフィックス AU	6.2.0 6.2.0.1 ~ 6.2.0.3	FMC 1000、2500、4500 : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_AU-6.2.0.4-1</a>	<a href="#">CSCvf77493</a> : Firepower Management Center 4500、2500、または 1000 上で管理インターフェイスが見つからない。

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 A	6.2.0	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_A-6.2.0.1-10</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_A-6.2.0.1-10</a> ASDM を搭載した ASA FirePOWER : <a href="#">Cisco_Network_Sensor_Hotfix_A-6.2.0.1-10</a>	CSCvc88603 : 地理位置情報を使用しているすべてのポリシーがトラフィックをブロックしている。

## バージョン 6.1.0 のホットフィックス

この表では、公開されているバージョン 6.1.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 13:バージョン 6.1.0 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 ES	6.1.0 6.1.0.1 ~ 6.1.0.7	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_ES-6.1.0.8-2</a>	CSCvr95287 : Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
ローカルマルウェア証明書のホットフィックス	6.1.0 6.1.0.x	FMC/FMCv : <a href="#">Hotfix_Local_Malware_Cert-6.1.0.999-1.sh</a> (注) バージョン 6.2.0 または 6.2.3 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	CSCvm81052 : 証明書チェーンが無効であるため、ローカルマルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス EM	6.1.0 6.1.0.1 ~ 6.1.0.5	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_EM-6.1.0.999-49</a> Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_EM-6.1.0.999-51</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_EM-6.1.0.999-51</a> FTDv : <a href="#">Cisco_FTD_Hotfix_EM-6.1.0.999-51</a>	CSCvj07038 : Firepower デバイスは Threat Grid 証明書を信頼する必要があります。

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 ER	6.1.0.7	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_ER-6.1.0.8-1.sh</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_ER-6.1.0.8-1.sh</a> FTDv : <a href="#">Cisco_FTD_Hotfix_ER-6.1.0.8-1.sh</a>	<a href="#">CSCvm43975</a> : SIP インスペクションの脆弱性による Cisco ASA および FTD のサービス拒否または高 CPU。
ホットフィックス EI	6.1.0.6	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_EI-6.1.0.7-2</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_EI-6.1.0.7-2</a> FTDv : <a href="#">Cisco_FTD_Hotfix_EI-6.1.0.7-2</a>  (注) ホットフィックス DZ はホットフィックス EI に置換されます。ホットフィックス DZ をインストールしている場合は、ホットフィックス EI もインストールする必要があります。	<a href="#">CSCvg35618</a> : Cisco 適応型セキュリティアプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。  <a href="#">CSCvh95456</a> 、 <a href="#">CSCvh23085</a> : Cisco 適応型セキュリティアプライアンスのアプリケーションレイヤプロトコルのインスペクションにおける DoS に対する脆弱性。  <a href="#">CSCvh79732</a> : Cisco 適応型セキュリティアプライアンスにおけるサービス拒否攻撃に対する脆弱性。  <a href="#">CSCvi16029</a> : Cisco 適応型セキュリティアプライアンスの WebVPN におけるサービス拒否攻撃に対する脆弱性。
ホットフィックス CF	6.1.0.1 6.1.0.2	Firepower 4100/9300 <a href="#">Cisco_FTD_SSP_Hotfix_CF-6.1.0.3-3</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_CF-6.1.0.3-3</a> FTDv : <a href="#">Cisco_FTD_Hotfix_CF-6.1.0.3-3</a>	<a href="#">CSCvd78303</a> : バージョン 6.1.0.1 またはバージョン 6.1.0.2 を実行している Firepower Threat Defense デバイスが、稼働時間が 213 日後にトラフィックの受け渡しを停止し、接続の制限からトラフィックの停止に至るまでの問題が発生した。
ホットフィックス DH	6.1.0.5	FirePOWER 8000 シリーズ : <a href="#">Sourcefire_3D_Device_S3_Hotfix_DH-6.1.0.6-48</a>	<a href="#">CSCvf66660</a> : ハイアベイラビリティ環境で設定されたクラスタ化 Firepower 8000 シリーズスタックをバージョン 6.1.0.5 に更新すると、ピアに継続的なフェールオーバーが発生する。

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 DQ	6.1.0.5	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_DQ-6.1.0.6-1</a>	<a href="#">CSCve82410</a> : TCP、UDP、ICMP、または IP スキャンをブロックするように設定された侵入ポリシーを展開すると、Firepower Management Center はポート スキャンを検出しても、ブロックが必要な場合にブロックしない。
ホットフィックス AJ	6.1.0 6.1.0.1	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.1.0.2-1</a>	<a href="#">CSCvb96776</a> : Firepower Management Center ハイアベイラビリティ ペアをバージョン 6.1.0 以降からバージョン 6.2.0 への正常な更新に失敗した後、ハイアベイラビリティの同期の再確立に失敗した。
ホットフィックス AZ	6.1.0.2	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_AZ-6.1.0.3-1</a>	<a href="#">CSCvd10943</a> : 同じ侵入ポリシーを参照する 2 つ以上のアクセスコントロールルールを含んでいるアクセスコントロールポリシーを展開したが、バージョン 6.1.0.2 を実行している Firepower Management Center とは異なる変数セットを使用している場合、展開に失敗した。
ホットフィックス AI	6.1.0	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_AI-6.1.0.2-3</a>	<a href="#">CSCvc49789</a> : 最適化コンポーネントが誤ったデータベースに接続しようとする CPU 使用率の上昇や全般的なパフォーマンスの低下などのシステムの問題が発生した。

## バージョン 6.0.1 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 AF	6.1.0	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_AF-6.1.0.2-1</a> Firepower 7000/8000 シリーズ <a href="#">Sourcefire_3D_Device_S3_Hotfix_AF-6.1.0.2-1</a> ASA FirePOWER : <a href="#">Cisco_Network_Sensor_Hotfix_AF-6.1.0.2-1</a> NGIPSv : <a href="#">Sourcefire_3D_Device_Virtual64_VMware_Hotfix_AF-6.1.0.2-1</a>	<a href="#">CSCvc26880</a> : Firepower 8350 デバイスまたは AMP8350 デバイスがシリアルポートコンソール、または、有効にしていた場合は Lights-out 管理 (LOM) コンソールで異常に大きなメッセージのストリームを生成した場合にデバイスが応答しなくなった。

## バージョン 6.0.1 のホットフィックス

この表では、公開されているバージョン 6.0.1 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 14: バージョン 6.01 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 BH	6.0.1.4	Firepower 4100/9300 : <a href="#">Cisco_FTD_SSP_Hotfix_BH-6.0.1.5-1</a> FTD を搭載した ASA 5500-X シリーズ : <a href="#">Cisco_FTD_Hotfix_BH-6.0.1.5-1</a> FTDv : <a href="#">Cisco_FTD_Hotfix_BH-6.0.1.5-1</a>	<a href="#">CSCvg35618</a> : Cisco 適応型セキュリティアプライアンスの Remote Code Execution とサービス拒否攻撃に対する脆弱性。 <a href="#">CSCvh79732</a> 、 <a href="#">CSCvh81870</a> : Cisco 適応型セキュリティアプライアンスにおけるサービス拒否攻撃に対する脆弱性。
ローカルマルウェア証明書のホットフィックス	6.0.1 6.0.1.x	FMC/FMCv : <a href="#">Hotfix_Local_Malware_Cert-6.0.1.999-1</a> (注) バージョン 6.1 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	<a href="#">CSCvm81052</a> : 証明書チェーンが無効であるため、ローカルマルウェア検出の更新が FMC にダウンロードされない。

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 AU	6.0.1.1	Firepower 7000/8000 シリーズ : <a href="#">Sourcefire_3D_Device_S3_Hotfix_AU-6.0.1.3-1</a>	<a href="#">CSCvc26880</a> : 場合によっては、シリーズ 3 デバイスがシリアルポート コンソール、または、有効にしていた場合は Lights-out 管理 (LOM) コンソールで異常に大きなメッセージのストリームを生成した場合にデバイスが応答しなくなる。

## バージョン 6.0.0 のホットフィックス

この表では、公開されているバージョン 6.0.0 のホットフィックスのページをダウンロードするためのクイックリンクを提供しています。

表 15: バージョン 6.0.0 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
ローカルマルウェア証明書のホットフィックス	6.0.0 6.0.0.1	FMC/FMCv : <a href="#">Hotfix_Local_Malware_Cert-6.0.0.999-1</a>  (注) バージョン 6.0.1 にアップグレードした後、新しいローカルマルウェア証明書のホットフィックスを適用する必要があります。	<a href="#">CSCvm81052</a> : 証明書チェーンが無効であるため、ローカルマルウェア検出の更新が FMC にダウンロードされない。
ホットフィックス O	6.0.0.1	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_O-6.0.0.999-1</a> ASDM を搭載した ASA FirePOWER : <a href="#">Cisco_Network_Sensor_Hotfix_O-6.0.0.999-1</a>	<a href="#">CSCuy99274</a> : Firepower Management Center またはローカル管理のいずれかからセキュリティゾーンで設定された ASA Firepower モジュールにアクセスコントロールルールを展開した場合、システムは誤った順序で制御ルールを展開し、必要な設定でトリガーされることがないルールを着信トラフィックがトリガーされる。
ホットフィックス K	6.0.0.1	FMC/FMCv : <a href="#">Sourcefire_3D_Defense_Center_S3_Hotfix_K-6.0.0.2-3</a>	<a href="#">CSCuy60529</a> : SRU の更新後、新しい共有オブジェクトルールがセンサーにプッシュされない。

## バージョン 5.4.x のホットフィックス

この表には、公開されているバージョン 5.4.x のホットフィックスのページをダウンロードするためのクイックリンクが提供されています。

表 16: バージョン 5.4.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 CX	5.4.1.8	ASA FirePOWER (ASA 5506-X シリーズ、5508-X、5516-X、ISA 3000) : <a href="#">Cisco_Network_Sensor_Hotfix_CX-5.4.1.9-1</a>	<b>CSCuv11738</b> : リモート NTP サーバーを使用して、バージョン 5.4 よりも前のバージョンを実行している登録済みの ASA FirePower モジュールとシステムの時刻を同期するように設定している場合にうるう秒が発生すると、システムが CPU を大量に使用する可能性がある。
ホットフィックス DK	5.4.0.9	Firepower 7000/8000 シリーズ : <a href="#">Sourcefire_3D_Device_S3_Hotfix_DK-5.4.0.10-1</a> ASA FirePOWER (ASA 5515-X、5525-X、5545-X、5555-X) : <a href="#">Cisco_Network_Sensor_Hotfix-5.4.0.10-1</a> NGIPSv : <a href="#">Sourcefire_3D_Device_Virtual64_VMware_Hotfix-5.4.0.10-1</a>	<b>CSCvb26230</b> : 過剰なロギングによって、ディスク領域の問題、パフォーマンスの低下、およびストレージの制限が発生する。



## 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。