# Cisco Secure Firewall デバイスマネージャの新機能（リリース別）

**初版**：2021 年 1 月 19 日

**最終更新**：2022 年 9 月 7 日

## 各リリースの新機能

このドキュメントでは、各リリースの新機能と廃止された機能を示します。

## 推奨リリース

### 推奨リリース：バージョン 7.0.4

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを推奨リリース以上にアップグレードすることをお勧めします。シスコ サポートおよびダウンロードサイトでは、推奨リリースに金色の星が付いています。

### 古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。

## バージョン 7.2

### Device Manager バージョン 7.2 の新機能

| 機能 | 説明 |
|---|---|
| ファイアウォールと IPS の機能 | |

| 機能 | 説明 |
|---|---|
| オブジェクトグループ検索は、アクセス制御のためにデフォルトで有効になっています。 | CLI 構成コマンド **object-group-search access-control** は現在、デフォルトで有効になっています。FlexConfig を使用してコマンドを構成している場合は、FlexConfig オブジェクトを削除できます。この機能を無効にする必要がある場合は、FlexConfig を使用して **no object-group-search access-control** コマンドを実装します。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/I-R/asa-command-ref-I-R/o-commands.html#wp1852298285を参照してください。 |
| ルールのヒットカウントは再起動後も存続します。 | デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。<br><br>次の Threat Defense CLI コマンドを変更しました：**show rule hits**。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-access.html#id_92394を参照してください。 |
| **VPN 機能** | |
| IPsec フローがオフロードされます。 | Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。<br><br>FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-s2svpn.html#Cisco_Concept.dita_83d8d2c7-8a9c-4094-9649-91744c9fff06を参照してください。 |
| **インターフェイス機能** | |
| Cisco Secure Firewall 3130 および 3140 のブレークアウトポートのサポート。 | Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成できるようになりました。<br><br>新規/変更された画面：<br><br>• **[デバイス（Devices）] > [インターフェイス（Interfaces）]**<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-interfaces.html#Cisco_Concept.dita_14e59bb1-dd81-455d-bf70-f26fa2cc097eを参照してください。 |

| 機能 | 説明 |
|---|---|
| インターフェイスでの Cisco TrustSec の有効化または無効化。 | 名前付きか名前なしかにかかわらず、物理、サブインターフェイス、EtherChannel、VLAN、管理、または BVI インターフェイスで Cisco TrustSec を有効または無効にできます。デフォルトでは、インターフェイスに名前を付けると、Cisco TrustSec が自動的に有効になります。<br><br>インターフェイス構成ダイアログボックスに [Propagate Security Group Tag] 属性を追加し、さまざまなインターフェイス API に **ctsEnabled** 属性を追加しました。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-interfaces.html#task_D0C0FB15621B4F49B29CB010F7D6C2D1を参照してください。 |
| **ライセンシング機能** | |
| ISA 3000 の永久ライセンス予約のサポート。 | ISA 3000 は、承認されたお客様向けのユニバーサル永久ライセンスの予約をサポートするようになりました。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-license.html#id_123878を参照してください。 |
| **管理およびトラブルシューティングの機能** | |
| 完全な展開を強制する機能。 | 変更を展開すると、システムは通常、最後の正常な展開以降に加えられた変更のみを展開します。ただし、問題が発生した場合は、デバイスの構成を完全に更新するフル展開を強制するように選択できます。展開ダイアログボックスに [Apply Full Deployment] オプションを追加しました。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-get-started.html#task_BEE4E37389B64E518EE91FF3824476A9を参照してください。 |
| Threat Defense REST API バージョン 6.3（v6）。 | ソフトウェアバージョン 7.2 の Threat Defense REST API はバージョン 6.3 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.3 の URL バージョンパス要素は、6.0、6.1 および 6.2 と同じ v6 である点に注意してください。<br><br>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。<br><br>詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api.htmlを参照してください。 |

# バージョン 7.2 の新しいハードウェアと仮想プラットフォーム

表 *1 :* バージョン *7.2.0* の新しいハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| Firepower 4100 向けネットワークモジュール。 | Firewall 4100 向けに次のネットワークモジュールが導入されました。<br>• 2 ポート 100 ギガビットイーサネット QSFP28（FPR4K-NM-2X100G）<br>• 4 ポート 100 ギガビットイーサネット QSFP28（FPR4K-NM-4X100G） |
| デバイスマネージャが GCP 向け Threat Defense Virtual をサポート。 | デバイスネージャを使用して、GCP 対応 Threat Defense Virtual を構成できるようになりました。 |

# バージョン 7.1

## FDM バージョン 7.1 の新機能

表 *2 : FDM* バージョン *7.1.0* の新機能

| 機能 | 説明 |
|---|---|
| プラットフォーム機能 | |
| Cisco Secure Firewall 3100 | Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。<br>新しい/変更された画面：**[Devices]** > **[Interfaces]**<br>新しい/変更された Threat Defense コマンド： configure network speed、configure raid、show raid、show ssd |

| 機能 | 説明 |
| --- | --- |
| ASA 5508-X および 5516-X のサポートは終了します。サポートされる最後のリリースは Threat Defense 7.0 です。 | ASA 5508-X または 5516-X に Threat Defense Threat Defense 7.1 はインストールできません。これらのモデルで最後にサポートされるリリースは Threat Defense 7.0 です。 |
| **ファイアウォールと IPS の機能** | |
| Snort 3 のネットワーク分析ポリシー（NAP）設定。 | Snort 3 の実行時に、Device Manager を使用してネットワーク分析ポリシー（NAP）を設定できます。ネットワーク分析ポリシーはトラフィック前処理検査を制御します。インスペクタは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックがさらに検査されるように準備します。すべてのトラフィックに使用する NAP を選択し、ネットワークのトラフィックに最適な設定をカスタマイズできます。Snort 2 の実行中は NAP を設定できません。<br><br>[ポリシー（Policies）] > [侵入（Intrusion）] の設定ダイアログボックスにネットワーク分析ポリシーが追加されました。これには、直接の変更が可能な組み込み JSON エディタと、上書きをアップロードしたり、作成したものをダウンロードしたりするためのその他の機能があります。 > |
| 変換後の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの手動 NAT サポート。 | www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。 |
| 改善されたアクティブ認証アイデンティティルール。 | ID ポリシールールのアクティブ認証を設定して、ユーザーの接続をデバイスに入力するインターフェイスの IP アドレスではなく、完全修飾ドメイン名（FQDN）にユーザーの認証をリダイレクトできます。FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。<br><br>ID ポリシー設定に [ホスト名にリダイレクト（Redirect to Host Name）] オプションが追加されました。 |
| **VPN 機能** | |

| 機能 | 説明 |
| --- | --- |
| サイト間 VPN のバックアップリモートピア | リモートバックアップピアを含めるようにサイト間 VPN 接続を設定できます。プライマリリモートピアが使用できない場合、システムはバックアップピアの 1 つを使用して VPN 接続を再確立しようとします。バックアップピアごとに個別の事前共有キーまたは証明書を設定できます。バックアップピアは、ポリシーベースの接続でのみサポートされ、ルートベース（仮想トンネルインターフェイス）の接続では使用できません。<br>バックアップピア設定を含むように、サイト間 VPN ウィザードを更新しました。 |
| リモートアクセス VPN（MSCHAPv2）のパスワード管理。 | リモートアクセス VPN のパスワード管理を有効にできます。これにより、AnyConnect はユーザーに期限切れのパスワードの変更を求めることができます。パスワード管理がない場合、ユーザーは AAA サーバーを使用して期限切れのパスワードを直接変更する必要があります。AnyConnect はユーザーにパスワードの変更を要求しません。LDAP サーバーの場合は、パスワードの有効期限が近づいていることをユーザーに通知する警告期間を設定することもできます。<br>リモートアクセス VPN 接続プロファイルの認証設定に [パスワード管理を有効にする（Enable Password Management）] オプションが追加されました。 |
| AnyConnect VPN SAML 外部ブラウザ | リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。組み込みブラウザでは実行できない Web 認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。<br>リモートアクセス VPN 接続プロファイルウィザードが更新され、**SAML ログインエクスペリエンス**を設定できるようになりました。 |
| **管理およびトラブルシューティングの機能** | |

| 機能 | 説明 |
| --- | --- |
| システムインターフェイスの完全修飾ドメイン名（FQDN）から IP アドレスへのマッピングを更新するためのダイナミック ドメイン ネーム システム（DDNS）のサポート。 | ダイナミックアップデートを DNS サーバーに送信するように、システムのインターフェイスに DDNS を設定できます。これにより、インターフェイスに定義された FQDN が正しいアドレスに解決され、ユーザーが IP アドレスではなくホスト名を使用して簡単にシステムにアクセスできるようになります。これは、DHCP を使用してアドレスを取得するインターフェイスに特に役立ちますが、静的にアドレス指定されたインターフェイスにも役立ちます。<br><br>アップグレード後に FlexConfig を使用して DDNS を設定した場合は、変更を再度展開する前に、Device Manager または Threat Defense API を使用して設定をやり直し、FlexConfig ポリシーから DDNS FlexConfig オブジェクトを削除する必要があります。<br><br>Device Manager を使用して DDNS を設定し、Management Center 管理に切り替えると、DDNS 構成が保持され、Management Center が DNS 名を使用してシステムを検索できるようになります。<br><br>Device Manager で、**[System Settings]** > **[DDNS Service]**ページが追加されました。Threat Defense API で、DDNSService および DDNSInterfaceSettings リソースが追加されました。 |
| デバイス CLI で、**dig** コマンドが **nslookup** コマンドに置き換わります。 | デバイス CLI で完全修飾ドメイン名（FQDN）の IP アドレスを検索するには、**dig** コマンドを使用します。**nslookup** コマンドは削除されます。 |
| Device Manager を使用した DHCP リレー構成。 | Device Manager を使用して DHCP リレーを構成できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。<br><br>[システム設定（System Settings）] > [DHCP] > [DHCPリレー（DHCP Relay）] ページを追加し、DHCP サーバーを新しい DHCP 見出しの下に移動しました。 > > |

| 機能 | 説明 |
|---|---|
| Device Manager の自己署名証明書のキータイプとサイズ。 | Device Manager で新しい自己署名内部および内部 CA 証明書を生成するときに、キータイプとサイズを指定できます。キータイプには、RSA、ECDSA、および EDDSA があります。許可されるサイズはキータイプによって異なります。推奨される最小長よりも小さいキーサイズの証明書をアップロードすると、警告が表示されるようになりました。また、可能な場合は置き換える必要がある脆弱な証明書を見つけるために役立つ、事前定義された脆弱キー検索フィルタもあります。 |
| 信頼できる CA 証明書の使用検証の制限。 | 信頼できる CA 証明書を使用して特定のタイプの接続を検証できるかどうかを指定できます。SSL サーバー（ダイナミック DNS で使用）、SSL クライアント（リモートアクセス VPN で使用）、IPsec クライアント（サイト間 VPN で使用）、または LDAPS などの Snort 検査エンジンによって管理されていないその他の機能の検証を許可または阻止できます。これらのオプションの主な目的は、特定の証明書に対して検証できるため、VPN 接続が確立されないようにすることです。<br>信頼できる CA 証明書のプロパティとして [検証の使用（Validation Usage）] が追加されました。 |
| Device Manager での**管理者**パスワードの生成。 | Device Manager での初期システム設定時、または Device Manager で**管理者**パスワードを変更するときに、ボタンをクリックしてランダムな 16 文字のパスワードを生成できるようになりました。 |
| 起動時間と tmatch コンパイルステータス。 | **show version** コマンドには、システムの起動（ブート）にかかった時間に関する情報が含まれるようになりました。設定が大きいほど、システムの起動に時間がかかることに注意してください。<br>新しい **show asp rule-engine** コマンドは、tmatch コンパイルのステータスを表示します。Tmatch コンパイルは、アクセスグループ、NAT テーブル、およびその他のいくつかの項目として使用されるアクセスリストに使用されます。これは、非常に大きな ACL と NAT テーブルがある場合には、CPU リソースを消費し、進行中のパフォーマンスに影響を与える可能性がある内部プロセスです。コンパイル時間は、アクセスリスト、NAT テーブルなどのサイズによって異なります。 |

| 機能 | 説明 |
| --- | --- |
| **show access-list element-count** 出力の拡張。 | **show access-list element-count** コマンドの出力が拡張されました。オブジェクトグループ検索を有効にして使用すると、出力には要素数のオブジェクトグループの数に関する詳細が含まれます。<br><br>さらに、**show tech-support** 出力には **show access-list element-count** と **show asp rule-engine** からの出力が含まれます。 |
| Device Manager を使用した Management Center による管理のための Threat Defense の構成 | Device Manager を使用して初期設定を実行すると、管理および Management Center アクセス設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。Threat Defense CLI を使用すると、管理と Management Center のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。<br><br>Management Center に切り替えると、Device Manager を使用して Threat Defense を管理できなくなります。<br><br>新規/変更された画面：[システム設定（System Settings）]、[管理センター（Management Center）] > |
| Threat Defense REST API バージョン 6.2（v6）。 | ソフトウェアバージョン 7.1 用の Threat Defense REST API はバージョン 6.2 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.2 の URL バージョンパス要素は、6.0/1 と同じ v6 である点に注意してください。<br><br>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。 |

# バージョン 7.1 の新しいハードウェアと仮想プラットフォーム

表 *3:* バージョン *7.1.0* の新しいハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| Cisco Secure Firewall 3100 | Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。<br><br>ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。<br><br>（注） バージョン 7.1.0 リリースには、これらのデバイスのオンラインヘルプが含まれていません。FDM の場合は、Cisco.com に掲載されているドキュメントを参照してください。将来のリリースに新しいオンラインヘルプを含める予定です。<br><br>これらのモデルに関連する画面と CLI コマンドについては、FDM バージョン 7.1 の新機能 （4 ページ）を参照してください。 |
| AWS 用 FMCv300<br><br>OCI 用 FMCv300 | AWS と OCI の両方に対応する FMCv300 が導入されました。FMCv300 は、最大 300 台のデバイスを管理できます。 |

| 機能 | 説明 |
| --- | --- |
| AWS 用 FTDv のインスタンス。 | AWS 用 FTDv により、次のインスタンスのサポートが追加されています。<br>• c5a.xlarge、c5a.2xlarge、c5a.4xlarge<br>• c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge<br>• c5d.xlarge、c5d.2xlarge、m c5d.4xlarge<br>• i3en.xlarge、i3en.2xlarge、i3en.3xlarge<br>• inf1.xlarge、inf1.2xlarge<br>• m5.xlarge、m5.2xlarge、m5.4xlarge<br>• m5a.xlarge、m5a.2xlarge、m5a.4xlarge<br>• m5ad.xlarge、m5ad.2xlarge、m5ad.4xlarge<br>• m5d.xlarge、m5d.2xlarge、m5d.4xlarge<br>• m5dn.xlarge、m5dn.2xlarge、m5dn.4xlarge<br>• m5n.xlarge、m5n.2xlarge、m5n.4xlarge<br>• m5zn.xlarge、m5zn.2xlarge、m5zn.3xlarge<br>• r5.xlarge、r5.2xlarge、r5.4xlarge<br>• r5a.xlarge、r5a.2xlarge、r5a.4xlarge<br>• r5ad.xlarge、r5ad.2xlarge、r5ad.4xlarge<br>• r5b.xlarge、r5b.2xlarge、r5b.4xlarge<br>• r5d.xlarge、r5d.2xlarge、r5d.4xlarge<br>• r5dn.xlarge、r5dn.2xlarge、r5dn.4xlarge<br>• r5n.xlarge、r5n.2xlarge、r5n.4xlarge<br>• z1d.xlarge、z1d.2xlarge、z1d.3xlarge |
| Azure 用 FTDv のインスタンス。 | Azure 用 FTDv により、次のインスタンスのサポートが追加されています。<br>• Standard_D8s_v3<br>• Standard_D16s_v3<br>• Standard_F8s_v2<br>• Standard_F16s_v2 |

## バージョン 7.1 で廃止されたハードウェアと仮想プラットフォーム

表 *4 :* バージョン *7.1.0* で廃止されたハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| ASA 5508-X および 5516-X | ASA 5508-X または 5516-X ではバージョン 7.1 以降を実行できません。 |

# バージョン 7.0

## FDM バージョン 7.0 の新機能

表 *5 : FDM* バージョン *7.0.0* の新機能

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| ISA 3000 の仮想ルータサポート。 | ISA 3000 デバイスには最大 10 の仮想ルータを設定できます。 |
| AWS における Threat Defense Virtual の新しいデフォルトパスワード | AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[Advanced Details]** > **[User Data]**）していなければ、Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。 |
| **ファイアウォールと IPS の機能** | |
| システム定義の NAT ルールの新しいセクション 0。 | 新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。 |

| 機能 | 説明 |
| --- | --- |
| Snort 3 のカスタム侵入ルール。 | オフラインツールを使用して、Snort 3 で使用するカスタム侵入ルールを作成し、侵入ポリシーにアップロードできます。独自のカスタムルールグループにカスタムルールを編成して、必要に応じて簡単に更新できます。Device Manager で直接ルールを作成することもできますが、ルールの形式はアップロードされたルールと同じです。Device Manager には、ルール作成のガイダンスはありません。新しい侵入ルールの基礎として、システム定義のルールを含む既存のルールを複製できます。<br>侵入ポリシーの編集時に、**[Policies]** > **[Intrusion]**ページにカスタムグループとルールのサポートが追加されました。 |
| Device Manager 管理対象システムの Snort 3 の新機能 | Device Manager 管理対象システムで Snort 3 を検査エンジンとして使用する場合、次の追加機能を設定できるようになりました。<br>• 時間ベースのアクセス制御ルール（Threat Defense API のみ）。<br>• 複数の仮想ルータ。<br>• SSL 復号ポリシーを使用した TLS 1.1 以下の接続の復号化。<br>• SSL 復号ポリシーを使用したプロトコル FTPS、SMTPS、IMAPS、POP3S の復号化。 |
| URL カテゴリとレピュテーションに基づく DNS 要求のフィルタリング。 | URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用できます。ルックアップ要求の完全修飾ドメイン名（FQDN）にブロックしているカテゴリやレピュテーションがある場合、システムは DNS 応答をブロックします。ユーザーは DNS 解決を受信しないため、ユーザーは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーション フィルタリングを適用するには、このオプションを使用します。この機能を使用するには、URL フィルタリングライセンスが必要です。<br>アクセス コントロール ポリシーの設定に [Reputation Enforcement on DNS Traffic] オプションが追加されました。 |
| **VPN 機能** | |

| 機能 | 説明 |
|---|---|
| リモートアクセス VPN の Device Manager SSL 暗号設定 | Device Manager でリモートアクセス VPN 接続に使用する TLS バージョンと暗号化の暗号を定義できます。以前は、Threat Defense API を使用して SSL を設定する必要がありました。<br>次のページが追加されました：**[Objects]** > **[SSL Ciphers]**、**[Device]** > **[System Settings]** > **[SSL Settings]**。 |
| Diffie-Hellman グループ 31 のサポート。 | IKEv2 プロポーザルおよびポリシーで Diffie-Hellman（DH）グループ 31 を使用できるようになりました。 |
| デバイス上の仮想トンネルインターフェイスの最大数は 1024 です。 | 作成できる仮想トンネルインターフェイス（VTI）の最大数は 1024 です。以前のバージョンでは、送信元インターフェイスあたりの最大数は 100 でした。 |
| サイト間 VPN セキュリティアソシエーションの IPsec ライフタイム設定。 | セキュリティ アソシエーションが再ネゴシエートされるまでに維持する期間のデフォルト設定を変更できます。<br>サイト間 VPN ウィザードに [Lifetime Duration] オプションと [Lifetime Size] オプションが追加されました。 |
| **ルーティング機能** | |
| 等コストマルチパス（ECMP）ルーティング。 | 複数のインターフェイスを含むように ECMP トラフィックゾーンを設定できます。これにより、ゾーン内の任意のインターフェイスで、既存の接続のトラフィックが Threat Defense デバイスに出入りできるようになります。この機能により、Threat Defense デバイス上での等コストマルチパス（ECMP）のルーティングや、Threat Defense デバイスへのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。<br>ECMP トラフィックゾーンはルーティングにのみ使用されます。これらはセキュリティゾーンとは異なります。<br>[Routing] ページに [ECMP Traffic Zones] タブが追加されました。Threat Defense API に ECMPZones リソースが追加されました。 |
| **インターフェイス機能** | |
| 新しいデフォルトの内部 IP アドレス | 192.168.1.0/24 のアドレスが DHCP を使用して外部インターフェイスに割り当てられている場合、IP アドレスの競合を避けるために、内部インターフェイスのデフォルト IP アドレスが 192.168.1.1 から **192.168.95.1** に変更されています。 |

| 機能 | 説明 |
| --- | --- |
| デフォルトの外部 IP アドレスで IPv6 自動設定が有効になりました。管理用の新しいデフォルト IPv6 DNS サーバー | 外部インターフェイスのデフォルト設定には、IPv4 DHCP クライアントに加えて、IPv6 自動設定が含まれています。デフォルトの管理 DNS サーバーには、IPv6 サーバー：2620:119:35::35 も含まれるようになりました。 |
| ISA 3000 の EtherChannel サポート | Device Manager を使用して ISA 3000 で EtherChannel を設定できるようになりました。<br>新規/変更された画面：**[Devices]** > **[Interfaces]** > **[EtherChannels]** |
| **ライセンシング機能** | |
| Threat Defense Virtual のパフォーマンス階層型ライセンス | Threat Defense Virtual は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマートライセンスをサポートするようになりました。使用可能なパフォーマンスライセンスのいずれかで Threat Defense Virtual のライセンスを取得すると、2 つのことが発生します。まず、デバイスのスループットを指定されたレベルに制限するレートリミッタがインストールされます。次に、VPN セッションの数は、ライセンスで指定されたレベルに制限されます。 |
| **管理およびトラブルシューティングの機能** | |
| Threat Defense API を使用した DHCP リレー設定。 | Threat Defense API を使用して DHCP リレーを設定できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。<br>以前のリリースで FlexConfig を使用して DHCP リレーを設定した場合は（**dhcprelay** コマンド）、アップグレード後に API を使用して設定を再実行し、FlexConfig オブジェクトを削除する必要があります。<br>Threat Defense API に次のモデルを追加しました：dhcprelayservices |
| ブートストラップ処理の高速化と Device Manager への早期ログイン | Device Manager 管理対象システムを最初にブートストラップするプロセスが改善され、より高速になりました。したがって、デバイスを起動してから Device Manager にログインするまで待機する必要はありません。また、ブートストラップの進行中にログインできるようになりました。ブートストラップが完了していない場合は、プロセスのステータス情報が表示されるため、デバイスで何が発生しているかがわかります。 |

| 機能 | 説明 |
| --- | --- |
| 多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。 | ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。<br><br>次のコマンドが変更されました：**clear local-host**（廃止）、**show local-host** |
| Device Manager 管理対象デバイスのアップグレード準備状況チェック。 | アップロードした Threat Defense ソフトウェア アップグレード パッケージをインストールする前に、アップグレード準備状況チェックを実行できます。準備状況チェックでは、システムに対してアップグレードが有効であり、システムがパッケージのインストールに必要な他の要件を満たしていることを確認します。アップグレードの準備状況チェックを実行すると、インストールの失敗を回避できます。<br><br>**[Device]** > **[Updates]**ページの **[System Upgrade]** セクションに、アップグレードの準備状況チェックを実行するリンクが追加されました。 |
| Threat Defense REST API バージョン 6.1（v6）。 | ソフトウェアバージョン 7.0 の Threat Defense REST API はバージョン 6.1 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.1 の URL バージョンパス要素は、6.0：v6 と同じであることに注意してください。<br><br>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。 |

# バージョン 7.0 の新しいハードウェアと仮想プラットフォーム

表 *6 :* バージョン *7.0.0* の新しいハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| VMware vSphere/VMware ESXi 7.0 のサポート。 | VMware vSphere/VMware ESXi 7.0 に FTDv 仮想アプライアンスを展開できるようになりました。<br>バージョン 7.0 でも VMware 6.0 のサポートは終了します。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。 |
| 新しい仮想環境。 | 次の環境に FMCv および FTDv が導入されました。<br>• Cisco HyperFlex<br>• Nutanix エンタープライズクラウド |

# FDM バージョン 7.0 で廃止された機能

表 *7 : FDM* バージョン *7.0.0* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| dhcprelay FlexConfig コマンド。 | アップグレード後に展開ができないようにします。<br>アップグレード後に設定をやり直す必要があります。 | バージョン 7.0 では、FDM を使用する FTD の次の FlexConfig CLI コマンドは廃止されます。<br>• **dhcprelay**FTD API を使用して DHCP リレーを設定できるようになりました。インターフェイスで DHCP リレーを使用すると、デバイス上の別のインターフェイスで実行されている DHCP サーバー、または他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。<br>関連付けられている FlexConfig オブジェクトを削除するまで、アップグレード後に展開することはできません。 |

## バージョン 7.0 で廃止されたハードウェアと仮想プラットフォーム

表 *8 :* バージョン *7.0.0* で廃止されたハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| VMware vSphere/VMware ESXi 6.0 のサポート。 | バージョン 7.0 では、VMware vSphere/VMware ESXi 6.0 での仮想展開のサポートが廃止されています。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。 |

# バージョン 6.7

## FDM バージョン 6.7 の新機能

表 *9 : FDM* バージョン *6.7.0* の新機能

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| ASA 5525-X、5545-X、5555-X でのサポートが終了します。最後にサポートされていたリリースは Threat Defense 6.6 です。 | Threat Defense 6.7 を ASA 5525-X、5545-X、5555-X にインストールすることはできません。これらのモデルで最後にサポートされていたリリースは Threat Defense 6.6 です。 |
| **ファイアウォールと IPS の機能** | |
| アクセス制御ルールの照合のための TLS サーバーアイデンティティ検出。 | TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたはURLフィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するため、[TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] を有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。<br><br>[アクセス制御の設定（Access Control Settings）]（⚙）ボタンとダイアログボックスが **[ポリシー（Policy）]** > **[アクセス制御（Access Control）]**ページに追加されました。 |

| 機能 | 説明 |
| --- | --- |
| 外部の信頼できる CA 証明書のグループ。 | SSL 復号ポリシーで使用される信頼できる CA 証明書のリストをカスタマイズできるようになりました。デフォルトでは、ポリシーはすべてのシステム定義の信頼できる CA 証明書を使用しますが、カスタムグループを作成して証明書を追加したり、デフォルトグループを独自のより制限されたグループに置き換えることができます。<br>**[オブジェクト（Objects）]** > **[証明書（Certificates）]** ページに証明書グループが追加され、SSL 復号ポリシー設定を変更して証明書グループを選択できるようにしました。 |
| パッシブ ID ルールの Active Directory レルムシーケンス。 | Active Directory（AD）サーバーとそのドメインの番号付きリストであるレルムシーケンスを作成し、パッシブ認証 ID ルールで使用できます。レルムシーケンスは、複数の AD ドメインをサポートしている状況で、ユーザーベースのアクセス制御を実行するときに役立ちます。各 AD ドメインの個別のルールを記述する代わりに、すべてのドメインを対象とする単一のルールを作成できます。シーケンス内の AD レルムの順序は、ID の競合が発生した場合に、その競合を解決するために使用されます。<br>**[オブジェクト（Objects）]** > **[アイデンティティ ソース（Identity Sources）]** ページに AD レルム シーケンス オブジェクトが追加され、そのオブジェクトをパッシブ認証アイデンティティルールのレルムとして選択できるようになりました。Threat Defense API に **RealmSequence** リソースが追加されました。また **IdentityRule** リソースには、アクションとしてパッシブ認証を使用するルールのレルムとしてレルム シーケンス オブジェクトを選択する機能が追加されました。 |
| TrustSec セキュリティグループタグ（SGT）グループオブジェクトの FDM サポートと、アクセス制御ルールでのそれらの使用 | Threat Defense 6.5 では、SGT グループオブジェクトを設定し、それらをアクセス制御ルールの一致基準として使用するためのサポートが Threat Defense API に追加されました。さらに、ISE によってパブリッシュされた SXP トピックをリッスンするように ISE アイデンティティ オブジェクトを変更できます。これらの機能を FDM で直接設定できるようになりました。<br>新しいオブジェクトである SGT グループが追加され、それらを選択および表示できるようにアクセス制御ポリシーが更新されました。また、サブスクライブするトピックの明示的な選択を含むように ISE オブジェクトを変更しました。 |

| 機能 | 説明 |
| --- | --- |
| Snort 3.0 のサポート。 | 新しいシステムでは、Snort 3.0 がデフォルトの検査エンジンです。古いリリースから 6.7 にアップグレードした場合、アクティブな検査エンジンは Snort 2.0 のままですが、Snort 3.0 に切り替えることができます。このリリースでは、Snort 3.0 は、仮想ルータ、時間ベースのアクセス制御ルール、または TLS 1.1 以下の接続の復号化をサポートしていません。これらの機能が必要ない場合にのみ Snort 3.0 を有効にしてください。Snort 2.0 と Snort 3.0 の間を自由に切り替えることができるため、必要に応じて、変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。<br><br>**[デバイス（Device）] > [更新（Updates）]**ページの [侵入ルール（Intrusion Rules）] グループに Snort のバージョンを切り替える機能が追加されました。Threat Defense API では、IntrusionPolicy リソースアクション/toggleinspectionengine が追加されました。<br><br>さらに、Snort 3 ルールパッケージの更新で追加、削除、または変更された侵入ルールを示す新しい監査イベント、ルール更新イベントがあります。 |
| Snort 3 のカスタム侵入ポリシー。 | Snort 3 を検査エンジンとして使用している場合は、カスタム侵入ポリシーを作成できます。これに対し、Snort 2 を使用する場合にのみ、事前定義されたポリシーを使用できます。カスタム侵入ポリシーを使用すると、ルールのグループを追加または削除し、グループレベルでセキュリティレベルを変更して、グループ内のルールのデフォルトアクション（無効化、アラート、またはドロップ）を効率的に変更できます。Snort 3 の侵入ポリシーを使用すると、Cisco Talos 提供の基本ポリシーを編集することなく、IPS/IDS システムの動作をより詳細に制御できます。<br><br>侵入ポリシーを一覧表示するように **[ポリシー（Policies）] > [侵入（Intrusion）]**ページが変更されました。新しいポリシーを作成したり、既存のポリシーを表示または編集（グループの追加/削除、セキュリティレベルの割り当て、ルールのアクションの変更など）することができます。複数のルールを選択し、それらのアクションを変更することもできます。さらに、アクセス制御ルールでカスタム侵入ポリシーを選択できます。 |
| 侵入イベント用の複数の syslog サーバー。 | 侵入ポリシー用に複数の syslog サーバーを設定できます。侵入イベントは各 syslog サーバーに送信されます。<br><br>侵入ポリシー設定ダイアログボックスに、複数の syslog サーバーオブジェクトを選択する機能が追加されました。 |

| 機能 | 説明 |
| --- | --- |
| URL レピュテーション照合にレピュテーションが不明なサイトを含めることが可能です。 | URL カテゴリのトラフィック一致基準を設定し、レピュテーション範囲を選択する場合に、レピュテーションが不明な URL をレピュテーション照合に含めることができます。<br>アクセス制御ルールと SSL 復号ルールの URL レピュテーション基準に [レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] チェックボックスが追加されました。 |
| **VPN 機能** | |
| 仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN。 | VPN 接続プロファイルのローカルインターフェイスとして仮想トンネルインターフェイスを使用して、ルートベースのサイト間 VPN を作成できるようになりました。ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウド サービス プロバイダーや大企業の VPN 管理が簡素化されます。<br>インターフェイスのリストのページに [仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] タブが追加され、VTI をローカルインターフェイスとして使用できるように、サイト間 VPN ウィザードが更新されました。 |
| Threat Defense リモート アクセス VPN 接続を行うための Hostscan およびダイナミック アクセス ポリシー（DAP）の API サポート。 | Hostscan パッケージとダイナミック アクセス ポリシー（DAP）ルール XML ファイルをアップロードし、XML ファイルを作成するよう DAP ルールを設定することで、接続中のエンドポイントのステータスに関連する属性に基づいてグループポリシーをリモートユーザーに割り当てる方法を制御することができます。Cisco Identity Services Engine（ISE）がない場合は、これらの機能を使用して認可変更を実行できます。Hostscan のアップロードと DAP の設定は Threat Defense API を使用してのみ行えます。FDM を使用して設定することはできません。Hostscan および DAP の使用方法の詳細については、AnyConnect のマニュアルを参照してください。<br>dapxml、hostscanpackagefiles、hostscanxmlconfigs、ravpns の各 Threat Defense API オブジェクトモデルを追加または変更しました。 |

| 機能 | 説明 |
|---|---|
| 外部 CA 証明書の証明書失効チェックの有効化。 | Threat Defense API を使用して、特定の外部 CA 証明書の証明書失効チェックを有効にすることができます。失効チェックは、リモートアクセス VPN で使用される証明書に特に役立ちます。FDM を使用して証明書の失効チェックを設定することはできません。Threat Defense API を使用する必要があります。<br><br>ExternalCACertificate リソースに revocationCheck、crlCacheTime、および oscpDisableNonce 属性が追加されました。 |
| 安全性の低い Diffie-Hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートがなくなりました。 | 6.6 で廃止されていた以下の機能が削除されました。それらを IKE プロポーザルまたは IPsec ポリシーで引き続き使用している場合は、アップグレード後にそれらを置き換えないと、設定変更を展開できません。VPN が正しく機能するように、サポートされる DH および暗号化アルゴリズムにアップグレードする前に VPN 設定を変更することをお勧めします。<br><br>• Diffie-Hellman グループ：2、5、および 24。<br><br>• 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。<br><br>• ハッシュアルゴリズム：MD5。 |
| リモートアクセス VPN 用のカスタムポート。 | リモートアクセス VPN（RA VPN）接続に使用するポートを設定できます。RA VPN に使用されているインターフェイスで FDM に接続する必要がある場合は、RA VPN 接続のポート番号を変更できます。FDM が使用するポート 443 は、デフォルトの RA VPN ポートでもあります。<br><br>RA VPN ウィザードのグローバル設定ステップが更新され、ポート設定が追加されました。 |
| リモートアクセス VPN を認証するための SAML サーバーのサポート。 | SAML 2.0 サーバーをリモートアクセス VPN の認証ソースとして設定できます。サポートされている SAML サーバーは次のとおりです：Duo。<br><br>**[オブジェクト（Objects）] > [アイデンティティソース（Identity Sources）]** ページでのアイデンティティソースとして SAML サーバーが追加され、それを使用できるようにリモートアクセス VPN 接続プロファイルが更新されました。 |

| 機能 | 説明 |
| --- | --- |
| AnyConnect モジュールプロファイルの Threat Defense API サポート | Threat Defense API を使用して、AMP イネーブラ、ISE ポスチャ、Umbrella といった AnyConnect で使用されるモジュールプロファイルをアップロードできます。これらのプロファイルは、AnyConnect プロファイル エディタ パッケージからインストールできるオフラインプロファイルエディタを使用して作成する必要があります。<br><br>AnyConnectClientProfile モデルに anyConnectModuleType 属性が追加されました。最初はモジュールプロファイルを使用する AnyConnect クライアント プロファイル オブジェクトを作成できますが、FDM で作成されたオブジェクトを変更して正しいモジュールタイプを指定するには、依然として API を使用する必要があります。 |
| **ルーティング機能** | |
| スマート CLI による EIGRP のサポート。 | 以前のリリースでは、FlexConfig を使用して、[詳細設定（Advanced Configuration）] ページで EIGRP を設定しました。今回、[ルーティング（Routing）] ページでスマート CLI を直接使用して EIGRP を設定するようになりました。<br><br>FlexConfig を使用して EIGRP を設定した場合は、リリース 6.7 にアップグレードするときに、FlexConfig ポリシーから FlexConfig オブジェクトを削除してから、スマート CLI オブジェクトで設定を再作成する必要があります。スマート CLI の更新が完了するまでは、参照用に EIGRP FlexConfig オブジェクトを保持できます。設定は自動的に変換されません。<br><br>[ルーティング（Routing）] ページに EIGRP スマート CLI オブジェクトが追加されました。 |
| **インターフェイス機能** | |

| 機能 | 説明 |
| --- | --- |
| ISA 3000 ハードウェアバイパスの持続性 | 永続化オプションを使用して、ISA 3000 インターフェイスペアのハードウェアバイパスを有効にできるようになりました。電源が回復した後、ハードウェアバイパスは手動で無効にするまで有効のままになります。持続性のないハードウェアバイパスを有効にすると、電源が回復した後にハードウェアバイパスが自動的に無効になります。ハードウェアバイパスが無効になっていると、短時間のトラフィック中断が発生する可能性があります。永続化オプションを使用すると、トラフィックの短時間の中断が発生するタイミングを制御できます。<br><br>新規/変更された画面：**[デバイス（Device）] > [インターフェイス（Interfaces）] > [ハードウェアバイパス（Hardware Bypass）] > [ハードウェアバイパスの設定（Hardware Bypass Configuration）]** |
| Firepower 4100/9300 における Threat Defense 動作リンク状態と物理リンク状態の同期 | Firepower 4100/9300 シャーシでは、Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Threat Defense アプリケーションインターフェイスの管理状態は考慮されません。Threat Defense からの同期がない場合は、たとえば、Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。<br><br>（注） この機能は、Radware vDP デコレータを使用する Threat Defense ではサポートされません。<br><br>新規/変更された シャーシマネージャ 画面：[Logical Devices] > [Enable Link State]<br><br>新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail**<br><br>サポートされているプラットフォーム： Firepower 4100/9300 |

| 機能 | 説明 |
| --- | --- |
| Firepower 1100 および 2100 SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました | 自動ネゴシエーションを無効にするように Firepower 1100 および 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。<br>新規/変更画面：[Device] > [Interfaces] > [Edit Interface] > [Advanced Options] > [Speed]<br>サポートされるプラットフォーム：Firepower 1100 および 2100 |
| **管理およびトラブルシューティングの機能** | |
| 失敗した Threat Defense ソフトウェアのアップグレードをキャンセルし、以前のリリースに戻す機能。 | Threat Defense のメジャー ソフトウェア アップグレードが失敗するか、正常に機能しない場合は、アップグレードインストールの実行時の状態にデバイスを戻すことができます。<br>FDM の [システムのアップグレード（System Upgrade）] パネルにアップグレードを元に戻す機能が追加されました。アップグレード時に、FDM ログイン画面にアップグレードステータスが表示され、アップグレードが失敗した場合にキャンセルしたり元に戻すためのオプションが表示されます。Threat Defense API に CancelUpgrade、RevertUpgrade、RetryUpgrade、および UpgradeRevertInfo リソースが追加されました。<br>Threat Defense CLI に **show last-upgrade status**、**show upgrade status**、**show upgrade revert-info**、**upgrade cancel**、**upgrade revert**、**upgrade cleanup-revert**、および **upgrade retry** コマンドが追加されました。 |
| データインターフェイス上の FDM/Threat Defense API アクセス用のカスタム HTTPS ポート。 | データインターフェイスで FDM または Threat Defense API アクセスに使用する HTTPS ポートを変更できます。ポートをデフォルトの 443 から変更することにより、管理アクセスと同じデータインターフェイスで設定されているその他の機能（リモートアクセス VPN など）の競合を回避できます。管理インターフェイスの管理アクセス HTTPS ポートは変更できないことに注意してください。<br>**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）] > [データインターフェイス（Data Interfaces）]** ページにポートを変更する機能が追加されました。 |

| 機能 | 説明 |
|---|---|
| Firepower 1000 および 2100 シリーズ デバイス上の Cisco Defense Orchestrator のロータッチプロビジョニング。 | Cisco Defense Orchestrator（CDO）を使用して新しい Threat Defense デバイスを管理する予定がある場合、デバイス セットアップ ウィザードを完了することなく、または FDM にログインすることさえなく、デバイスを追加できるようになりました。<br><br>新しい Firepower 1000 および 2100 シリーズ デバイスは、最初に Cisco Cloud に登録され、CDO で簡単に要求できます。CDO に入ると、CDO からデバイスをすぐに管理できます。このロータッチプロビジョニングでは、物理デバイスと直接やりとりする必要性が最小限に抑えられ、ネットワクデバイスに関する経験が浅い従業員が勤務するリモートオフィスなどの場所にとって理想的です。<br><br>Firepower 1000 および 2100 シリーズ デバイスの初期プロビジョニング方法が変更されました。また、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** ページに自動登録が追加されました。これにより、FDM を使用して以前に管理していたアップグレード済みデバイスおよびその他のデバイスのプロセスを手動で開始できます。 |
| SNMP 設定の Threat Defense API サポート。 | Threat Defense API を使用して FDM または CDO 管理対象 Threat Defense デバイスで SNMP バージョン 2c または 3 を設定できます。<br><br>API リソースの SNMPAuthentication、SNMPHost、SNMPSecurityConfiguration、SNMPServer、SNMPUser、SNMPUserGroup、SNMPv2cSecurityConfiguration、および SNMPv3SecurityConfiguration が追加されました。<br><br>（注） FlexConfig を使用して SNMP を設定した場合は、Threat Defense API SNMP リソースを使用して設定をやり直す必要があります。SNMP を設定するためのコマンドは、FlexConfig では使用できなくなりました。FlexConfig ポリシーから SNMP FlexConfig オブジェクトを削除するだけで、変更を展開できます。その後、API を使用して機能を再設定するときに、それらのオブジェクトを参照として使用できます。 |
| システムに保持されるバックアップファイルの最大数が 10 から 3 に減少。 | システムでは、10 個ではなく最大 3 個のバックアップファイルがシステムに保持されます。新しいバックアップが作成されると、最も古いバックアップファイルが削除されます。必要な場合にシステムを回復するために必要なバージョンを入手できるように、バックアップファイルは異なるシステムにダウンロードしてください。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense API バージョンの下位互換性 | Threat Defense バージョン 6.7 以降、ある機能の API リソースモデルがリリース間で変更されない場合、Threat Defense API は古い API バージョンに基づくコールを受け入れることができます。機能モデルが変更された場合でも、古いモデルを新しいモデルに変換する論理的な方法があれば、古いコールが機能します。たとえば、v4 コールを v5 システムで受け入れることができます。コールのバージョン番号として「latest（最新）」を使用する場合、「古い」コールは、このシナリオではv5 コールとして解釈されるため、下位互換性を利用するかどうかは、API コールの構築方法によって決まります。 |
| Threat Defense REST API バージョン 6（v6）。 | ソフトウェアバージョン 6.7 用の Threat Defense REST API はバージョン 6 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。<br><br>使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。 |

# FDM バージョン 6.7 で廃止された機能

表 *10 : FDM* バージョン *6.7.0* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| 安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。 | アップグレード後に展開ができないようにします。 | 次の FTD 機能のいずれかを使用している場合、アップグレード後の展開ができないことがあります。<br>• Diffie-Hellman グループ：2、5、および 24。<br>• 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。<br>• ハッシュアルゴリズム：MD5。<br>IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。 |
| FlexConfig コマンド。 | アップグレード後に展開ができないようにします。<br>アップグレード後に設定をやり直す必要があります。 | バージョン 6.7 では、FDM を使用する FTD の次の FlexConfig CLI コマンドは廃止されます。<br>• **router eigrp**：[ルーティング（Routing）] ページの **[デバイス（Device）] > [ルーティング（Routing）] > [EIGRP]** で直接スマート CLI EIGRP オブジェクトを作成して、使用できます。<br>• **snmp-server**：FTD API を使用して SNMP バージョン 2c または 3 を設定できるようになりました。<br>関連付けられている FlexConfig オブジェクトを削除するまで、アップグレード後に展開することはできません。 |
| バックアップファイルの保持。 | なし。アップグレードによって、ローカルのバックアップは常に消去されます。 | バージョン 6.7 では、保存されるバックアップファイルの数が 10 から 3 に減ります。<br>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お勧めします。アップグレードによって、ローカルに保存されたバックアップは消去されます。 |

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| Microsoft Internet Explorer | ブラウザを切り替える必要があります。 | Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。 |

## バージョン 6.7 で廃止されたハードウェアと仮想プラットフォーム

表 *11* : バージョン *6.7.0* で廃止されたハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| Firepower ソフトウェアを使用した ASA 5525-X、5545-X、および 5555-X デバイス。 | ASA 5525-X、5545-X、および 5555-X でバージョン 6.7 以降は実行できません。 |

# バージョン 6.6

## FDM バージョン 6.6 の新機能

表 *12* : *FDM* バージョン *6.6.0* の新機能

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| Amazon Web Services（AWS）クラウド用 Threat Defense Virtual における Device Manager のサポート。 | Device Manager を使用して AWS クラウド用 Threat Defense Virtual で Threat Defense を設定できます。 |
| Firepower 4112 用 Device Manager | Firepower 4112 用 Threat Defense が導入されました。<br>（注） FXOS 2.8.1 が必要です。 |
| **ファイアウォールと IPS の機能** | |

| 機能 | 説明 |
| --- | --- |
| デフォルトでは無効になっている、侵入ルールを有効にする機能。 | 各システム定義の侵入ポリシーには、デフォルトで無効になっているルールがいくつかあります。以前は、これらのルールのアクションをアラートまたはドロップに変更できませんでした。現在では、デフォルトで無効になっているルールのアクションを変更できるようになりました。<br><br>[侵入ポリシー（Intrusion Policy）] ページが変更され、デフォルトで無効になっているルールもすべて表示されるようになりました。また、これらのルールのアクションも編集できます。 |
| 侵入ポリシーの侵入検知システム（IDS）モード。 | 侵入検知システム（IDS）モードで動作するように侵入ポリシーを設定できるようになりました。IDS モードでは、アクティブな侵入ルールは、ルールアクションがドロップであってもアラートのみを発行します。したがって、侵入ポリシーをネットワーク内でアクティブな防御ポリシーにする前に、その侵入ポリシーの動作をモニタリングまたはテストできます。<br><br>Device Manager では、**[Policies]** > **[Intrusion]** ページの各侵入ポリシーに、検査モードの表示が追加されました。また [Edit] リンクが追加され、モードを変更できるようになりました。<br><br>Threat Defense API では、IntrusionPolicy リソースに inspectionMode 属性が追加されました。 |
| 脆弱性データベース（VDB）、地理位置情報データベース、および侵入ルールの更新パッケージを手動でアップロードするためのサポート。 | VDB、地理位置情報データベース、および侵入ルールの更アップデートパッケージを手動で取得し、Device Manager を使用してワークステーションから Threat Defense デバイスにアップロードできるようになりました。たとえば、Device Manager で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。<br><br>ワークステーションからファイルを選択してアップロードできるように、**[デバイス（Device）]** > **[更新（Updates）]** ページが更新されました。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense 時間に基づいて制限されているアクセス制御ルールの API サポート。 | Threat Defense API を使用して、時間範囲オブジェクトを作成できます。このオブジェクトでは、1 回限りの時間範囲または繰り返しの時間範囲を指定します。オブジェクトはアクセス制御ルールに適用します。時間範囲を使用すると、特定の時間帯または一定期間にわたってトラフィックにアクセス制御ルールを適用して、ネットワークを柔軟に使用できます。Device Manager を使用して時間範囲を作成したり、適用したりはできません。また、アクセス制御ルールに時間範囲が適用されている場合、Device Manager は表示されません。<br><br>TimeRangeObject、Recurrence、TimeZoneObject、DayLightSavingDateRange、および DayLightSavingDayRecurrence リソースが Threat Defense API に追加されました。時間範囲をアクセス制御ルールに適用するために、timeRangeObjects 属性が accessrules リソースに追加されました。さらに、GlobalTimeZone および TimeZone リソースに変更が加えられました。 |
| アクセス コントロール ポリシーのオブジェクトグループ検索。 | 動作中、Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されているかや、Device Manager にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。<br><br>Device Manager では、FlexConfig を使用して **object-group-search access-control** コマンドを有効にする必要があります。 |
| **VPN 機能** | |

| 機能 | 説明 |
| --- | --- |
| サイト間 VPN のバックアップピア（Threat Defense API のみ）。 | Threat Defense API を使用して、サイト間 VPN 接続にバックアップピアを追加できます。たとえば、2 つの ISP がある場合は、最初の ISP への接続が使用できなくなった場合に、バックアップ ISP にフェールオーバーするように VPN 接続を設定できます。<br><br>バックアップピアのもう 1 つの主な用途は、プライマリハブやバックアップハブなど、トンネルのもう一方の端に 2 つの異なるデバイスがある場合です。通常、システムはプライマリハブへのトンネルを確立します。VPN 接続が失敗すると、システムはバックアップハブとの接続を自動的に再確立できます。<br><br>SToSConnectionProfile リソースで outsideInterface に対して複数のインターフェイスを指定できるように、Threat Defense API が更新されました。また、BackupPeer リソースと remoteBackupPeers 属性が SToSConnectionProfile リソースに追加されました。<br><br>Device Manager を使用してバックアップピアを設定したり、バックアップピアの存在を Device Manager に表示したりはできません。 |
| リモートアクセス VPN での Datagram Transport Layer Security（DTLS）1.2 のサポート。 | リモートアクセス VPN で DTLS 1.2 を使用できるようになりました。これは、Threat Defense API のみを使用して設定できます。Device Manager を使用して設定することはできません。ただし、DTLS 1.2 はデフォルトの SSL 暗号グループの一部になったため、グループポリシーの AnyConnect 属性で Device Manager を使用して DTLS の一般的な使用が可能になりました。DTLS 1.2 は、ASA 5508-X または 5516-X モデルではサポートされていないことに注意してください。<br><br>DTLSV1_2 を列挙値として受け入れるように sslcipher リソースの protocolVersion 属性が更新されました。 |

| 機能 | 説明 |
| --- | --- |
| 安全性の低い Diffie-hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートを廃止。 | 次の機能は廃止されており、将来のリリースでは削除されます。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。これらの機能から移行し、実用可能になったらすぐにより強力なオプションを使用してください。<br>• Diffie-Hellman グループ：2、5、および 24。<br>• 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。<br>• ハッシュアルゴリズム：MD5。 |
| **ルーティング機能** | |
| 仮想ルータと Virtual Routing and Forwarding（VRF）-Lite。 | 複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。<br>仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。<br>[ルーティング（Routing）] ページが変更され、仮想ルータを有効化できるようになりました。有効にすると、[ルーティング（Routing）]ページに仮想ルータのリストが表示されます。仮想ルータごとに個別のスタティックルートとルーティングプロセスを設定できます。<br>また、［**vrf** *name* \| **all**］キーワードセットを次の CLI コマンドに追加し、必要に応じて出力が仮想ルータ情報を表示するよう変更しました。**clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters**<br>**show vrf** コマンドが追加されました。 |

| 機能 | 説明 |
| --- | --- |
| OSPF および BGP の設定を [Routing] ページに移動しました。 | 以前のリリースでは、スマート CLI を使用して、[詳細設定（Advanced Configuration）] ページで OSPF と BGP を設定しました。これらのルーティングプロセスは、これまでと同様にスマート CLI を使って設定しますが、そのオブジェクトを [ルーティング（Routing）] ページで直接使用できるようになりました。これにより、仮想ルータごとにプロセスを簡単に設定できます。<br><br>OSPF および BGP スマート CLI オブジェクトは、[詳細設定（Advanced Configuration）] ページでは使用できなくなりました。6.6 にアップグレードする前に、これらのオブジェクトを設定した場合は、アップグレード後に [ルーティング（Routing）] ページでそれらのオブジェクトを見つけることができます。 |
| **高可用性機能** | |
| 高可用性（HA）ペアのスタンバイ装置にログインする外部認証ユーザーの制限を削除。 | 以前は、外部認証されたユーザーは HA ペアのスタンバイユニットに直接ログインできませんでした。スタンバイユニットへのログインが可能になる前は、ユーザーは最初にアクティブ装置にログインしてから、設定を展開する必要がありました。<br><br>この制約は削除されました。外部認証されたユーザーは、有効なユーザー名/パスワードを提供している限り、アクティブ装置にログインしていない場合でも、スタンバイ装置にログインできます。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense API の BreakHAStatus リソースによって、インターフェイスがどのように処理されるかが変更。 | 以前は、 **clearIntfs** クエリパラメータを含めて、高可用性（HA）設定を中断するデバイス上のインターフェイスの動作ステータスを制御できました。<br><br>バージョン 6.6 以降では、clearIntfs クエリパラメータの代わりに使用する新しい属性 **interfaceOption** があります。この属性は、アクティブノードで使用する場合はオプションですが、非アクティブノードで使用する場合は必須です。次の 2 つのオプションのいずれかを選択できます。<br><br>• DISABLE_INTERFACES（デフォルト）：スタンバイデバイス（またはこのデバイス）上のすべてのデータインターフェイスが無効になります。<br><br>• ENABLE_WITH_STANDBY_IP：インターフェイスにスタンバイ IP アドレスを設定すると、スタンバイデバイス（またはこのデバイス）上のインターフェイスがスタンバイアドレスを使用するよう再設定されます。スタンバイアドレスを持たないインターフェイスはすべて無効になります。<br><br>デバイスが正常なアクティブ/スタンバイ状態になっているときにアクティブノードで [HAの中断（Break HA）] を使用すると、この属性がスタンバイノードのインターフェイスに適用されます。アクティブ/アクティブまたは一時停止などのその他の状態では、この属性が中断を開始するノードに適用されます。<br><br>clearIntfs クエリパラメータを使用する場合、clearIntfs=true は interfaceOption = DISABLE_INTERFACES のように動作します。つまり、clearIntfs=true のアクティブ/スタンバイペアを中断すると、両方のデバイスが無効にはならなくなり、スタンバイデバイスのみが無効になります。<br><br>Device Manager を使用して HA を中断すると、インターフェイスオプションには常に DISABLE_INTERFACES が設定されます。スタンバイ IP アドレスを使用してインターフェイスを有効にすることはできません。異なる結果が必要な場合は、API エクスプローラから API コールを使用します。 |
| 高可用性の問題の直近の失敗理由を [高可用性（High Availability）] ページに表示。 | 高可用性（HA）が何らかの理由で失敗した場合（アクティブデバイスが使用できなくなり、スタンバイデバイスにフェールオーバーするなど）、直近の失敗の理由がプライマリデバイスとセカンダリデバイスのステータス情報の下に表示されます。この情報には、イベントの UTC 時刻が含まれます。 |

| 機能 | 説明 |
|---|---|
| **インターフェイス機能** | |
| PPPoE のサポート。 | ルーテッドインターフェイスの PPPoE を設定できるようになりました。PPPoE は、ハイアベイラビリティ ユニットではサポートされません。<br>新規/変更された画面：**[デバイス（Device）] > [インターフェイス（Interfaces）] > [編集（Edit）] > [IPv4 アドレス（IPv4 Address）] > [タイプ（Type）] > [PPPoE]**<br>新規/変更されたコマンド：**show vpdn group、show vpdn username、show vpdn session pppoe state** |
| デフォルトでは DHCP クライアントとして機能する管理インターフェイス。 | 管理インターフェイスは、192.168.45.45 IP アドレスを使用する代わりに、デフォルトでは DHCP から IP アドレスを取得するように設定されています。この変更により、既存のネットワークに Threat Defense を簡単に展開できるようになりました。この機能は、Firepower 4100/9300（論理デバイスを展開するときに IP アドレスを設定する）と Threat Defense Virtual および ISA 3000（現在も 192.168.45.45 IP アドレスを使用）を除くすべてのプラットフォームに適用されます。管理インターフェイス上の DHCP サーバーも有効にならなくなりました。<br>デフォルト（192.168.1.1）では、デフォルトの内部 IP アドレスに引き続き接続できます。 |
| Device Manager 管理接続の HTTP プロキシサポート。 | Device Manager 接続で使用するために、管理インターフェイスの HTTP プロキシを設定できるようになりました。手動およびスケジュールされたデータベースの更新を含むすべての管理接続は、プロキシを通過します。<br>設定するための **[システム設定（System Setting）] > [HTTP プロキシ（HTTP Proxy）]** ページが追加されました。さらに、HTTPProxy リソースが Threat Defense API に追加されました。 |
| 管理インターフェイスの MTU の設定。 | 管理インターフェイスの MTU を最大 1500 バイトに設定できるようになりました。デフォルト値は 1500 バイトです。<br>新規/変更されたコマンド：**configure network mtu、configure network management-interface mtu-management-channel**<br>変更された画面はありません。 |
| **ライセンシング機能** | |

| 機能 | 説明 |
| --- | --- |
| スマートライセンシングとクラウドサービスの登録は分離され、登録を個別に管理可能 | スマートライセンスアカウントではなく、セキュリティアカウントを使用して、クラウドサービスを登録できるようになりました。Cisco Defense Orchestrator を使用してデバイスを管理する場合は、セキュリティアカウントを使用して登録することを推奨します。スマートライセンシングから登録解除せずに、クラウドサービスから登録解除することもできます。<br>**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** ページの動作を変更し、クラウドサービスから登録解除する機能を追加しました。さらに、このページからWeb分析機能が削除されました。この機能は、**[システム設定（System Settings）]** > **[Web分析（Web Analytics）]** ページに移動しました。Threat Defense API では、新しい動作を反映するように CloudServices リソースが変更されました。 |
| パーマネントライセンス予約のサポート。 | インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのためにCisco Smart Software Manager（CSSM）に直接登録することはできません。この場合は、ユニバーサル パーマネント ライセンス予約（PLR）モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせて、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。ISA 3000 はユニバーサル PLR をサポートしていません。<br>**[デバイス（Device）]**>**[スマートライセンス（Smart License）]** ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。Threat Defense API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、および CancelReservation のアクションが追加されました。 |
| **管理およびトラブルシューティングの機能** | |

| 機能 | 説明 |
| --- | --- |
| ISA 3000 デバイスの高精度時間プロトコル（PTP）設定用 Device Manager 直接サポート。 | Device Manager を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTPは、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。以前のリリースでは、PTP を設定するために FlexConfig を使用する必要がありました。<br><br>同じ [システム設定（System Settings）] ページの PTP と NTP をグループ化し、**[システム設定（System Settings）] > [NTP]** ページの名前を [タイムサービス（Time Services）] に変更しました。また、PTP リソースが Threat Defense API に追加されました。 |
| Device Manager 管理 Web サーバー証明書の信頼チェーン検証。 | Device Manager Web サーバーの非自己署名証明書を設定する場合は、すべての中間証明書とルート証明書を信頼チェーンに含める必要があります。システムはチェーン全体を検証します。<br><br>**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** ページの [管理Webサーバー（Management Web Server）] タブに、チェーン内の証明書を選択する機能が追加されました。 |
| バックアップファイルの暗号化のサポート。 | パスワードを使用して、バックアップファイルを暗号化できるようになりました。暗号化されたバックアップを復元するには、正しいパスワードを指定する必要があります。<br><br>定期的なジョブ、スケジュール済みジョブ、および手動ジョブのバックアップファイルを暗号化するかどうかを選択し、復元時にパスワードを提供する機能が、**[デバイス（Device）] > [バックアップと復元（Backup and Restore）]** ページに追加されました。また、encryptArchive 属性と encryptionKey 属性が BackupImmediate と BackupSchedule リソースに追加され、encryptionKey が Threat Defense API の RestoreImmediate リソースに追加されました。 |

| 機能 | 説明 |
|---|---|
| クラウドサービスで使用するために Cisco Cloud に送信するイベントを選択するサポート。 | Cisco Cloud にイベントを送信するようデバイスを設定すると、送信するイベントのタイプ（侵入、ファイル/マルウェア、接続）を選択できるようになりました。接続イベントの場合、すべてのイベントを送信することも、優先順位の高いイベント（侵入、ファイル、またはマルウェアイベントをトリガーする接続に関連するもの、またはセキュリティ インテリジェンスブロッキングポリシーと一致するもの）を送信することもできます。<br>[Cisco Cloudへのイベントの送信を有効にする（Send Events to the Cisco Cloud Enable）] ボタンが機能するよう変更されました。この機能は、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** ページにあります。 |
| Threat Defense REST API バージョン 5（v5）。 | ソフトウェアバージョン 6.6 用の Threat Defense REST API のバージョン番号が 5 になりました。API URL の v1/v2/v3/v4 を v5 に置き換える必要があります。または、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示します。<br>v5 の API には、ソフトウェアバージョン 6.6 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。 |

# バージョン 6.6 の新しいハードウェアと仮想プラットフォーム

**表 *13* : バージョン *6.6.0* の新しいハードウェアと仮想プラットフォーム**

| 機能 | 説明 |
|---|---|
| Firepower 4112 上の FTD。 | Firepower 4112 が導入されました。このプラットフォームでは、ASA 論理デバイスを展開することもできます。FXOS 2.8.1 が必要です。 |

| 機能 | 説明 |
|---|---|
| AWS の展開用の大型のインスタンス。 | **アップグレードの影響。**<br>FTDv for AWS により、次の大型のインスタンスのサポートが追加されています。<br>• C5.xlarge<br>• C 5.2 xlarge<br>• C5.4xlarge |

# FDM バージョン 6.6 で廃止された機能

表 *14 : FDM* バージョン *6.6.0* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| VMware 向け FTDv の e1000 インターフェイス。 | アップグレードされないようにします。 | バージョン 6.6 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。<br>詳細については、『VMware 向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。 |
| 安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。 | なし。ただし、今すぐ切り替える必要があります。 | バージョン 6.6 では、次の FTD セキュリティ機能は廃止されます。<br>• Diffie-Hellman グループ：2、5、および 24。<br>• 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。<br>• ハッシュアルゴリズム：MD5。<br>これらの機能はバージョン 6.7 で廃止されました。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。できるだけ強力なオプションに変更してください。 |

# バージョン 6.5

## FDM バージョン 6.5 の新機能

表 *15 : FDM* バージョン *6.5* パッチの新機能

| 機能 | 説明 |
|---|---|
| **バージョン 6.5.0.5**<br>デフォルトのHTTPSサーバー証明書 | **アップグレードの影響。**<br>デバイスで現在デフォルト設定されているHTTPSサーバー証明書の有効期間がすでに 800 日の場合を除き、バージョン 6.5.0.5以降にアップグレードすると証明書が更新されて、アップグレードの日から 800 日後に期限切れになります。その後の更新はすべて、有効期間が 800 日になります。<br>古い証明書には、生成日に応じて、次の期限が設定されています。<br>• 6.5.0 ～ 6.5.0.4：3 年<br>• 6.4.0.9 以降のパッチ：800 日<br>• 6.4.0 ～ 6.4.0.8：3 年<br>• 6.3.0 およびすべてのパッチ：3 年<br>• 6.2.3：20 年 |

表 *16 : FDM* バージョン *6.5.0* の新機能

| 機能 | 説明 |
|---|---|
| Firepower 4100/9300 での Device Manager のサポート。 | Device Manager を使用して Firepower 4100/9300 で Threat Defense を設定できるようになりました。ネイティブインスタンスのみがサポートされています。コンテナインスタンスはサポートされていません。 |
| Microsoft Azure クラウド用 Threat Defense Virtual での Device Manager のサポート。 | Device Manager を使用して Microsoft Azure Cloud 用に Threat Defense Virtual を設定できます。 |
| Firepower 1150 でのサポート。 | Firepower 1150 用 Threat Defense が導入されました。 |

| 機能 | 説明 |
|---|---|
| Firepower 1010 ハードウェアスイッチのサポート、PoE+ のサポート。 | Firepower 1010 では、各イーサネット インターフェイスをスイッチポートまたは通常のファイアウォール インターフェイスとして設定できます。各スイッチポートを VLAN インターフェイスに割り当てます。Firepower 1010 は、Ethernet 1/7 と Ethernet 1/8 での Power over Ethernet+（PoE+）もサポートしています。<br><br>デフォルト設定で、Ethernet 1/1 が外部として設定され、Ethernet 1/2 ～ 1/8 が内部 VLAN1 インターフェイスのスイッチポートとして設定されるようになりました。バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。 |
| インターフェイスのスキャンと置き換え。 | インターフェイススキャンでは、シャーシ上で追加、削除、または復元されたインターフェイスが検出されます。設定で古いインターフェイスを新しいインターフェイスに置き換えることもでき、インターフェイスの変更をシームレスに行えます。 |
| インターフェイス表示の向上。 | **[デバイス（Device）]**>**[インターフェイス（Interfaces）]** ページが再編成されました。物理インターフェイス、ブリッジグループ、EtherChannel、および VLAN 用のタブが別々に設けられました。任意の対象デバイスモデルについて、モデルに関連するタブのみが表示されます。たとえば、[VLAN] タブは Firepower 1010 モデルでのみ使用できます。また、各インターフェイスの設定と使用方法に関する詳細情報がリストに表示されます。 |
| ISA 3000 の新しいデフォルト設定。 | ISA 3000 のデフォルト設定が次のように変更されました。<br>• すべてのインターフェイスが BVI1 のブリッジグループメンバーとなりました。BVI1 には名前が付いていないため、ルーティングには参加しません<br>• GigabitEthernet 1/1 および 1/3 は外部インターフェイスで、GigabitEthernet 1/2 および 1/4 は内部インターフェイスです<br>• 内部/外部ペアごとにハードウェアバイパスが有効になります（使用可能な場合）<br>• すべてのトラフィックについて、内部から外部、および外部から内部が許可されます<br><br>バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。 |

| 機能 | 説明 |
| --- | --- |
| ASA 5515-X のサポートが終了します。最後にサポートされるリリースは Threat Defense 6.4 です。 | ASA 5515-X には Threat Defense 6.5 をインストールできません。ASA 5515-X 用にサポートされる最後のリリースは Threat Defense 6.4 です。 |
| Cisco ISA 3000 デバイスのアクセス制御ルールにおける Common Industrial Protocol（CIP）および Modbus アプリケーション フィルタリングのサポート。 | Cisco ISA 3000 デバイスで Common Industrial Protocol（CIP）および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write のように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。<br><br>プリプロセッサを有効にするには、CLI セッション（SSH またはコンソール）でエキスパートモードに移行し、**sudo /usr/local/sf/bin/enable_scada.sh {cip \| modbus \| both}** コマンドを発行する必要があります。展開後にプリプロセッサがオフになるため、展開のたびにこのコマンドを発行する必要があります。 |
| ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。 | FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。<br><br>FlexConfig オブジェクトに、**ptp** と **igmp**（インターフェイス モード）コマンド、およびグローバルコマンド **ptp mode e2etransparent** と **ptp domain** を追加できるようになりました。また、Threat Defense CLI に **show ptp** コマンドが追加されました。 |

| 機能 | 説明 |
|---|---|
| EtherChannel（ポートチャネル）インターフェイス。 | EtherChannel インターフェイス（ポートチャネルとも呼ばれます）を設定できます。<br>（注） Device Manager の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。<br>**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページが更新され、EtherChannel の作成ができるようになりました。 |
| Device Manager からシステムを再起動およびシャットダウンする機能。 | 新しい [Reboot/Shutdown] システム設定ページからシステムを再起動またはシャットダウンできるようになりました。以前は、Device Manager の CLI コンソールを使用して、あるいは SSH またはコンソールセッションから、**reboot** および **shutdown** コマンドを発行する必要がありました。これらコマンドを使用するには、管理者権限が必要です。 |
| Device Manager CLI コンソールでの **failover** コマンドのサポート。 | Device Manager CLI コンソールで **failover** コマンドを発行できるようになりました。 |
| スタティックルート用のサービスレベル契約（SLA）モニター。 | スタティックルートとともに使用するためのサービスレベル契約（SLA）モニターオブジェクトを設定します。SLA モニターを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。SLA モニターオブジェクトを選択できるように、[Object] ページに [SLA Monitors] を追加し、スタティックルートを更新しました。 |

| 機能 | 説明 |
| --- | --- |
| スマート CLI および Threat Defense API でのルーティングの変更。 | このリリースには、スマート CLI および Threat Defense API でのルーティング設定に対するいくつかの変更が含まれています。以前のリリースでは、BGP 用として単一のスマート CLI テンプレートがありました。今回は、BGP（ルーティングプロセス設定）と BGP の一般設定（グローバル設定）用に別々のテンプレートが用意されました。<br><br>Threat Defense API では、新しい BGP 一般設定のメソッドを除いて、すべてのメソッドのパスが変更され、パスに “/virtualrouters” が挿入されました。<br><br>• スタティックルートメソッドのパスは、以前は /devices/default/routing/{parentId}/staticrouteentries でしたが、今後は /devices/default/routing/virtualrouters/default/staticrouteentries になります。<br><br>• BGP メソッドは、/devices/default/routing/bgpgeneralsettings と /devices/default/routing/virtualrouters/default/bgp の 2 つの新しいパスに分割されました。<br><br>• OSPF パスは、/devices/default/routing/virtualrouters/default/ospf と /devices/default/routing/virtualrouters/default/ospfinterfacesettings になりました。<br><br>Threat Defense API を使用してルーティングプロセスを設定している場合は、コールを調べて必要に応じて修正してください。 |

| 機能 | 説明 |
|---|---|
| 新しいURLカテゴリおよびレピュテーション データベース。 | システムは、Cisco Talos とは別の URL データベースを使用します。新しいデータベースでは、URL のカテゴリにいくつかの違いがあります。アップグレードすると、もう存在していないカテゴリがアクセス制御や SSL 復号ルールで使用されている場合、システムはそのカテゴリを適切な新しいカテゴリに置き換えます。変更を有効にするには、アップグレード後に設定を展開します。カテゴリの変更についての詳細は、[保留中の変更（Pending Changes）] ダイアログに表示されます。引き続き希望する結果が得られることを確認するために、URL フィルタリングポリシーを調べる必要がある場合があります。<br><br>また、アクセス コントロール ポリシーと SSL 復号ポリシーの [URL] タブ、および **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[URL フィルタリング設定（URL Filtering Preferences）]** ページに URL ルックアップ機能を追加しました。この機能を使用すると、特定の URL に割り当てられているカテゴリを確認できます。同意しない場合は、カテゴリの異議を送信するリンクもあります。このどちらの機能も、URL に関する詳細情報を提供する外部 Web サイトを使用します。 |
| セキュリティ インテリジェンスでは、ホスト名ではなく IP アドレスを使用する URL 要求に対して IP アドレスのレピュテーションが使用されます。 | HTTP/HTTPS リクエストの宛先が、ホスト名ではなく IP アドレスを使用する URL の場合は、ネットワークアドレスリストにある IP アドレスのレピュテーションが検索されます。ネットワークおよび URL リストで IP アドレスを重複させる必要はありません。これにより、エンドユーザーがプロキシを使用してセキュリティ インテリジェンスのレピュテーションのブロッキングを回避することが困難になります。 |
| 接続イベントおよび優先順位の高い侵入イベント、ファイルイベント、マルウェアイベントを Cisco Cloud に送信するためのサポート。 | Cisco Cloud サーバーにイベントを送信できます。このサーバーから、各種のシスコ クラウドサービスがイベントにアクセスできます。次に、Cisco Threat Response などのクラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。このサービスを有効にすると、デバイスから、接続イベントおよび優先順位の高い侵入イベント、ファイルイベント、マルウェアイベントが Cisco Cloud に送信されます。<br><br>**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** にある Cisco Threat Response の項目を「Cisco Cloud にイベントを送信（Send Events to the Cisco Cloud）」に変更しました。 |

| 機能 | 説明 |
| --- | --- |
| シスコ クラウドサービスのリージョンサポート。 | スマートライセンスへの登録時に、シスコ クラウドサービスリージョンの選択が求められるようになりました。このリージョンは、Cisco Defense Orchestrator、Cisco Threat Response、Cisco Success Network、および Cisco Cloud を通過するすべてのクラウド機能で使用されます。登録済みデバイスを以前のリリースからアップグレードすると、自動的に US リージョンに割り当てられます。リージョンを変更する必要がある場合は、スマートライセンスを登録解除して、改めて再登録して新しいリージョンを選択する必要があります。<br><br>[スマートライセンス（Smart License）]ページと初期デバイス セットアップ ウィザードで、ライセンス登録プロセスにステップを追加しました。リージョンは、**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** ページでも確認できます。 |
| Threat Defense REST API バージョン 4（v4）。 | ソフトウェアバージョン 6.5 用の Threat Defense REST API のバージョン番号が 4 になりました。API の URL の v1/v2/v3 を v4 に置き換える必要があります。v4 の API には、ソフトウェアバージョン 6.5 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense アクセス制御ルールで送信元および宛先の一致基準として使用できる TrustSec セキュリティ グループの API サポート。 | Threat Defense API を使用して、送信元または宛先のトラフィックの一致基準に TrustSec セキュリティグループを使用したアクセス コントロール ポリシー ルールを設定できます。ISE からセキュリティグループタグ（SGT）のリストがダウンロードされます。SXP の更新がないかリッスンし、スタティック SGT から IP アドレスへのマッピングを取得するように、システムを設定できます。<br><br>GET /object/securitygrouptag メソッドを使用して、ダウンロードしたタグのリストを表示し、SGTDynamicObject リソースを使用して 1 つ以上のタグを表す動的オブジェクトを作成できます。この動的オブジェクトをアクセス制御ルールで使用して、送信元または宛先のセキュリティ グループに基づくトラフィックの一致基準を定義できます。<br><br>セキュリティグループに関連する ISE オブジェクトまたはアクセス制御ルールに変更を加えると、Device Manager でそれらのオブジェクトを編集しても変更が保持されます。ただし、Device Manager でルールを編集する場合、アクセスルールのセキュリティグループの基準は確認できません。API を使用してセキュリティグループに基づくアクセスルールを設定する場合は、その後 Device Manager を使用してアクセス コントロール ポリシーのルールを編集する際に注意が必要です。<br><br>AccessRule（sourceDynamicObjects および destinationDynamicObjects 属性）、IdentityServicesEngine（subscribeToSessionDirectoryTopic および subscribeToSxpTopic 属性）、SecurityGroupTag、SGTDynamicObject の各 Threat Defense API リソースを追加または変更しました。<br><br>イベントビューアの列として、送信元と宛先のセキュリティグループタグと名前を追加しました。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense API を使用した設定のインポート/エクスポート。 | Threat Defense API を使用して、デバイス設定のエクスポートや設定ファイルのインポートを行えます。設定ファイルを編集して、インターフェイスに割り当てられている IP アドレスなどの値を変更できます。したがって、インポート/エクスポートを使用して新しいデバイス用のテンプレートを作成できます。そのため、ベースラインの構成をすばやく適用し、新しいデバイスをより迅速にオンラインにすることができます。デバイスのイメージを再作成した後、インポート/エクスポートを使用して設定を復元することもできます。または、単に一連のネットワークオブジェクトや他の項目をデバイスのグループに配布する目的で使用することもできます。<br><br>ConfigurationImportExport のリソースとメソッド<br>(/action/configexport、/jobs/configexports、/action/downloadconfig、/action/uploadconfig、/jobs/configs、/action/configimport、/jobs/configimports)<br>を追加しました。 |
| カスタムファイルポリシーの作成と選択。 | Threat Defense API を使用してカスタムファイルポリシーを作成し、Device Manager を使用してアクセス制御ルールでそれらのポリシーを選択することができます。<br><br>filepolicies、filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections の各 Threat Defense API FileAndMalwarePolicies リソースを追加しました。<br><br>また、「Office ドキュメントおよび PDF のアップロードをブロック、その他のマルウェアをブロック」と「Office ドキュメントのアップロードをブロック、その他のマルウェアをブロック」の 2 つの定義済みポリシーを削除しました。これらのポリシーを使用している場合は、アップグレード時に、ユーザーが編集できるユーザー定義ポリシーに変換されます。 |
| Threat Defense API を使用したセキュリティ インテリジェンス DNS ポリシーの設定。 | Threat Defense API を使用してセキュリティ インテリジェンス DNS ポリシーを設定できます。このポリシーは Device Manager に表示されません。<br><br>domainnamefeeds、domainnamegroups、domainnamefeedcategories、securityintelligencednspolicies の各 SecurityIntelligence リソースを追加しました。 |

| 機能 | 説明 |
| --- | --- |
| Duo LDAP を使用したリモートアクセス VPN 二要素認証。 | リモートアクセス VPN 接続プロファイルの 2 番目の認証ソースとして Duo LDAP を設定し、Duo パスコード、プッシュ通知、または通話を使用して二要素認証を実現できます。Threat Defense API を使用して Duo LDAP アイデンティティ ソース オブジェクトを作成する必要がありますが、Device Manager を使用してそのオブジェクトを RA VPN 接続プロファイルの認証ソースとして選択できます。<br><br>duoldapidentitysources のリソースとメソッドを Threat Defense API に追加しました。 |
| Threat Defense リモートアクセス VPN 接続の認可に使用する LDAP 属性マップの API サポート。 | カスタムの LDAP 属性マップを使用して、リモートアクセス VPN の LDAP 認証を強化できます。LDAP 属性マップにより、顧客固有の LDAP 属性名および値がシスコの属性名および値と同等になります。これらのマッピングを使用して、LDAP 属性値に基づいてユーザーにグループポリシーを割り当てることができます。これらのマップは Threat Defense API を使用してのみ設定できます。Device Manager を使用して設定することはできません。ただし、API を使用してこれらのオプションを設定すると、後に Device Manager で Active Directory アイデンティティの送信元を編集して設定を保存できます。<br><br>LdapAttributeMap、LdapAttributeMapping、LdapAttributeToGroupPolicyMapping、LDAPRealm、LdapToCiscoValueMapping、LdapToGroupPolicyValueMapping、RadiusIdentitySource の各 Threat Defense API オブジェクトモデルを追加または変更しました。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense サイト間 VPN 接続におけるリバース ルート インジェクションとセキュリティ アソシエーション（SA）のライフタイムの API サポート。 | Threat Defense API を使用して、サイト間 VPN 接続のリバース ルート インジェクションを有効にできます。逆ルート注入（RRI）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。デフォルトでは、接続の設定時にルートが追加されるスタティック RRI が有効になっています。ダイナミック RRI は無効になっています。ダイナミック RRI では、セキュリティ アソシエーション（SA）が確立されたときにのみルートが挿入され、その後 SA が切断されたときにルートが削除されます。ダイナミック RRI は IKEv2 接続でのみサポートされています。<br><br>接続のセキュリティ アソシエーション（SA）のライフタイムは、秒単位または送信キロバイト単位でも設定できます。ライフタイムを期限なしに設定することもできます。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。ライフタイムに到達すると、エンドポイントで新しいセキュリティ アソシエーションと秘密鍵がネゴシエートされます。<br><br>Device Manager を使用してこれらの機能を設定することはできません。ただし、API を使用してこれらのオプションを設定すると、後に Device Manager で接続プロファイルを編集して設定を保存できます。<br><br>dynamicRRIEnabled、ipsecLifetimeInSeconds、ipsecLifetimeInKiloBytes、ipsecLifetimeUnlimited、rriEnabled の各属性を SToSConnectionProfile リソースに追加しました。 |
| IKE ポリシーの Diffie-Hellman グループ 14、15、および 16 のサポート。 | DH グループ 14 を使用するように IKEv1 ポリシーを設定し、DH グループ 14、15、および 16 を使用するように IKEv2 ポリシーを設定できるようになりました。IKEv1 を使用している場合は、グループ 2 と 5 が今後のリリースで削除されるため、すべてのポリシーを DH グループ 14 にアップグレードしてください。また、IKEv2 ポリシーで DH グループ 24 を使用したり、IKE バージョンで MD5 を使用しないでください。これらも今後のリリースで削除されます。 |

| 機能 | 説明 |
|---|---|
| 変更を展開する際のパフォーマンスの向上。 | システムの強化により、アクセス制御ルールを追加、編集、または削除した場合に、以前のリリースと比べて変更がより迅速に展開されるようになりました。<br>フェールオーバー用のハイアベイラビリティグループに設定しているシステムでは、展開した変更をスタンバイデバイスに同期させるプロセスが改善され、同期がより短時間で完了するようになりました。 |
| システムダッシュボード上の CPU およびメモリ使用率の計算の改善。 | CPU とメモリの使用率を計算する方法が改善され、システムダッシュボードに表示される情報に、デバイスの実際の状態がより正確に反映されるようになりました。 |
| Threat Defense 6.5 にアップグレードした場合、履歴レポートデータは使用できなくなります。 | 既存のシステムを Threat Defense 6.5 にアップグレードした場合、データベーススキーマの変更のために履歴レポートデータが使用できなくなります。そのため、アップグレード前の時点における使用状況データはダッシュボードに表示されません。 |

# バージョン 6.5 の新しいハードウェアと仮想プラットフォーム

表 *17* : バージョン *6.5.0* の新しいハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| Firepower 1150 上の FTD。 | Firepower 1150 が導入されました。 |
| Azure 向け FTDv がより大規模なインスタンスに対応。 | Microsoft Azure 向けの FTDvで、より大規模なインスタンス D4_v2 および D5_v2 がサポートされるようになりました。 |
| VMware vSphere/VMware ESXi 6.7 のサポート | VMware vSphere/VMware ESXi 6.7 に FTDvを展開できるようになりました。 |

# FDM バージョン 6.5 で廃止された機能

表 *18 : FDM* バージョン *6.5* パッチで廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| **バージョン 6.5.0.2**<br>出力最適化。 | パッチを適用すると、出力最適化処理がオフになります。 | CSCvq34340 を軽減するため、FTD デバイスにパッチを適用してバージョン 6.5.0.2 以降にすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。<br>（注） この問題が修正されているバージョン 6.6+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。<br>バージョン 6.5.0 または 6.5.0.1 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。<br>詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。 |

表 *19 : FDM* バージョン *6.5.0* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| デフォルトの HTTPS サーバー証明書。 | なし。 | バージョン 6.4.0.9 以降からアップグレードする場合、デフォルトの HTTPS サーバー証明書の lifespan-on-renew は 3 年に戻りますが、バージョン 6.5.0.5 以降および 6.6 以降で再び 800 日に更新されます。<br>現在のデフォルトの HTTPS サーバー証明書は、いつ生成されたかに応じて、次のように期限切れになるように設定されています。<br>• 6.4.0.9 以降のパッチ：800 日<br>• 6.4.0 ～ 6.4.0.8：3 年<br>• 6.3.0 およびすべてのパッチ：3 年<br>• 6.2.3：20 年 |

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| VDB、GeoDB、および SRU 更新の手動アップロード。 | なし。ただし、バージョン 6.6.0 以降にアップグレードするまでこの機能は廃止されます。 | バージョン 6.5 では、VDB、GeoDB、および SRU の更新を手動でデバイスにアップロードすることはできません。<br>この機能は、バージョン 6.4.0.10 以降のパッチ、およびバージョン 6.6 以降でサポートされています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5 を中間バージョンとして使用せずに、直接バージョン 6.6 以上にアップグレードすることを推奨します。 |
| ユニバーサル永久ライセンス予約（PLR）モード。 | なし。ただし、バージョン 6.6.0 以降にアップグレードするまでこの機能は廃止されます。 | バージョン 6.5 は、ユニバーサル永久ライセンス予約（PLR）モードをサポートしていません。このモードでは、Cisco Smart Software Manager（CSSM）との直接通信を必要としないライセンスを適用できます。<br>この機能は、バージョン 6.4.0.10 以降のパッチ、およびバージョン 6.6 以降でサポートされています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5 を中間バージョンとして使用せずに、直接バージョン 6.6 以上にアップグレードすることを推奨します。 |

# バージョン 6.5 で廃止されたハードウェアと仮想プラットフォーム

表 *20 :* バージョン *6.5.0* で廃止されたハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| ASA 5515-X、ASA 5585-X シリーズ | ASA 5515-X では、バージョン 6.5 以降を実行できません。 |

# バージョン 6.4

## FDM バージョン 6.4 の新機能

表 *21 : FDM* バージョン *6.4* パッチの新機能

| 機能 | 説明 |
|---|---|
| **バージョン 6.4.0.10**<br><br>VDB、GeoDB、およびSRU更新の手動アップロード | VDB、地理位置情報データベース、および侵入ルールの更新パッケージを手動で取得し、FDM を使用してワークステーションからFTDデバイスにアップロードできるようになりました。たとえば、FDM で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。<br><br>ワークステーションからファイルを選択してアップロードできるように、[Device] > [Updates] ページが更新されました。<br><br>この機能はバージョン6.5.0ではサポートされていないことに注意してください。バージョン 6.6.0 では再導入されています。バージョン6.4.0.10以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン6.6.0以上にアップグレードすることをお勧めします。 |

| 機能 | 説明 |
| --- | --- |
| **バージョン 6.4.0.10**<br><br>ユニバーサル永久ライセンス予約（PLR）モード | インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのために Cisco Smart Software Manager（CSSM）に直接登録することはできません。この場合は、ユニバーサル パーマネント ライセンス予約（PLR）モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせて、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。<br><br>[Device] > [Smart License] ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。FTD API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、および CancelReservation のアクションが追加されました。<br><br>この機能はバージョン 6.5.0 ではサポートされていないことに注意してください。バージョン 6.6.0 では再導入されています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。 |
| **バージョン 6.4.0.9**<br><br>デフォルトの HTTPS サーバー証明書 | **アップグレードの影響。**<br><br>FDM をバージョン 6.4.0 ～ 6.4.0.8 から以降のバージョン 6.4.0.x のパッチに（または 6.6.0+ に）アップグレードすると、デフォルトの HTTPS サーバー証明書が更新されます。この証明書は、アップグレードの日から 800 日後に期限切れになります。その後の更新はすべて、有効期間が 800 日になります。<br><br>古い証明書には、生成日に応じて、次の期限が設定されています。<br><br>• 6.4.0 ～ 6.4.0.8：3 年<br><br>• 6.3.0 およびすべてのパッチ：3 年<br><br>• 6.2.3 以前：20 年<br><br>バージョン 6.5.0 ～ 6.5.0.4 では、更新時の有効期限が 3 年に戻ることに注意してください。ただし、バージョン 6.5.0.5 および 6.6.0 では 800 日に更新されます。 |

| 機能 | 説明 |
|---|---|
| **バージョン 6.4.0.4**<br>新しい syslog フィールド | 次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。<br>• センサー UUID<br>• 最初のパケット時間<br>• 接続インスタンス ID<br>• 接続数カウンタ<br>これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。 |

表 *22 : FDM* バージョン *6.4.0* の新機能

| 機能 | 説明 |
|---|---|
| Firepower 1000 シリーズ デバイス設定 | Device Manager を使用して、 Firepower 1000 シリーズ デバイス上の Threat Defense を設定できます。<br>Power over Ethernet（PoE）ポートを通常のイーサーネット ポートとして使用することはできますが、PoE に関連するプロパティを有効にしたり設定することはできないことにご注意ください。 |
| ISA 3000 のハードウェア バイパス | ISA 3000 のハードウェアバイパスは、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページで設定できるようになりました。リリース 6.3 では、FlexConfig を使用してハードウェアバイパスを設定する必要がありました。FlexConfig を使用している場合は、[Interfaces] ページで設定をやり直し、FlexConfig からハードウェア バイパス コマンドを削除してください。ただし、TCP シーケンス番号のランダム化の無効化専用の FlexConfig の部分は引き続き推奨されます。 |
| Device Manager CLI コンソールからシステムを再起動およびシャットダウンする機能 | Device Manager で CLI コンソールを使用して **reboot** コマンドと **shutdown** コマンドを発行できるようになりました。以前は、システムを再起動またはシャットダウンするために、デバイスに対して個別の SSH セッションを開く必要がありました。これらコマンドを使用するには、管理者権限が必要です。 |

| 機能 | 説明 |
| --- | --- |
| RADIUS を使用した Threat Defense CLI ユーザーの外部認証および認可。 | Threat Defense CLI にログインするユーザーを、外部 RADIUS サーバーを使用して認証および認可できます。外部ユーザーに設定（管理者）または基本（読み取り専用）のアクセス権を付与できます。<br>**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** ページの [AAA設定（AAA Configuration）] タブに SSH 設定を追加しました。 |
| ネットワーク範囲オブジェクトとネストされたネットワーク グループ オブジェクトのサポート | IPv4 アドレスまたは IPv6 アドレスの範囲を指定するネットワークオブジェクトと、その他のネットワークグループ（つまりネストされたグループ）を含むネットワーク グループ オブジェクトを作成できるようになりました。<br>これらの機能を含むようにネットワークオブジェクトとネットワーク グループ オブジェクトの [Add/Edit] ダイアログボックスを変更し、そのタイプのアドレス指定がポリシーの文脈の中で合理的か否かを条件として、これらのオブジェクトを使用できるようにさまざまなセキュリティポリシーを変更しました。 |
| オブジェクトとルールの全文検索オプション | オブジェクトおよびルールでは、全文検索を実行できます。多数の項目を含むポリシーまたはオブジェクトリストを検索することで、ルールまたはオブジェクト内の任意の場所で検索文字列を含むすべての項目を検索できます。<br>ルールを持つすべてのポリシーと [Object] リストのすべてのページに検索ボックスを追加しました。さらに、API でサポートされているオブジェクトの GET コールで **filter=fts~*search-string*** オプションを使用して、全文検索に基づいて項目を取得できます。 |
| Device Manager 管理対象 Threat Defense デバイスでサポートされている API バージョンのリストの取得 | GET/api/versions（ApiVersions）メソッドを使用して、デバイスでサポートされる API バージョンのリストを取得できます。API クライアントを使用すると、サポートされるバージョンで有効なコマンドとシンタックスを使用したデバイスへの通信および設定を行うことができます。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense REST API バージョン 3（v3） | ソフトウェア バージョン 6.4 向けの Threat Defense REST API のバージョン番号が 3 になりました。API URL の v1/v2 は v3 で置き換える必要があります。v3 の API には、ソフトウェア バージョン 6.4 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、ログインした後に、Device Manager の URL の最後を **/#/api-explorer** に変更します。 |
| アクセス制御ルールのヒットカウント | アクセス制御ルールのヒットカウントを表示できます。ヒットカウントには、接続がルールに一致した頻度が示されます。<br>ヒットカウント情報が含まれるようにアクセス コントロール ポリシーを更新しました。Threat Defense API では、HitCounts リソースと、**includeHitCounts** オプションおよび **filter=fetchZeroHitCounts** オプションを GET アクセスポリシー ルールのリソースに追加しました。 |
| ダイナミック アドレス指定と証明書認証のためのサイト間 VPN の強化 | ピアの認証に事前共有キーではなく証明書を使用したサイト間 VPN 接続を設定できるようになりました。リモートピアに不明な（ダイナミック）IP アドレスがある接続も設定できます。サイト間 VPN ウィザードと IKEv1 ポリシーオブジェクトにオプションが追加されました。 |
| リモート アクセス VPN での RADIUS サーバーと認可変更のサポート | リモートアクセス VPN（RA VPN）ユーザーの認証、認可、およびアカウンティングに RADIUS サーバーを使用できるようになりました。また、Cisco ISE RADIUS サーバーの使用時に認証後にユーザーの認可を変更するために、ダイナミック認証とも呼ばれる Change of Authentication（CoA）を設定できます。<br>RADIUS サーバーとサーバー グループ オブジェクトに属性を追加し、RA VPN 接続プロファイル内の RADIUS サーバーグループを選択できるようになりました。 |
| リモートアクセス VPN の複数の接続プロファイルとグループ ポリシー | 複数の接続プロファイルを設定し、そのプロファイルで使用するグループ ポリシーを作成できます。<br>接続プロファイルおよびグループポリシーが別々のページとなるように **[デバイス（Device）]** > **[リモートアクセス VPN（Remote Access VPN）]** ページを変更し、グループポリシーを選択できるように RA VPN 接続ウィザードを更新しました。以前にウィザードで設定した項目の一部は、グループポリシーで設定するようになります。 |

| 機能 | 説明 |
| --- | --- |
| 証明書ベースの 2 番目の認証ソース、およびリモート アクセス VPN での二要素認証のサポート | ユーザー認証に証明書を使用したり、接続を確立する前にユーザーを 2 回認証する必要があるセカンダリ認証ソースを設定することができます。また、2 つ目の要素として RSA トークンまたは Duo パスコードを使用して二要素認証を設定できます。<br><br>これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。 |
| 複数のアドレス範囲を持つ IP アドレス プールとリモート アクセス VPN 向けの DHCP アドレス プールのサポート。 | サブネットを指定する複数のネットワークオブジェクトを選択することで、複数のアドレス範囲を持つアドレスプールを設定できるようになりました。さらに、DHCP サーバーでアドレスプールを設定し、そのサーバーを使用して RA VPN クライアントにアドレスを提供できます。認可に RADIUS を使用する場合は、代わりに RADIUS サーバーでアドレスプールを設定できます。<br><br>これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。必要に応じて、接続プロファイルではなくグループポリシーでアドレスプールを設定できます。 |
| Active Directory レルムの強化 | 1 つのレルムに最大 10 の冗長 Active Directory（AD）サーバーを含められるようになりました。また、複数のレルムを作成したり、不要になったレルムを削除できます。さらに、レルム内のユーザーのダウンロードの制限は、以前のリリースの 2,000 から 50,000 に増えています。<br><br>複数のレルムとサーバーをサポートするように、**[オブジェクト（Objects）]>[アイデンティティ ソース（Identity Sources）]** ページを更新しました。レルム内のすべてのユーザーにルールを適用するため、アクセス制御と SSL 復号化ルールのユーザーの基準でレルムを選択することができます。アイデンティティ ルールと RA VPN 接続プロファイルでレルムを選択することもできます。 |
| ISE サーバーの冗長性サポート | パッシブ認証向けの ID ソースとして Cisco Identity Services Engine（ISE）を設定する際に、ISE ハイアベイラビリティ設定がある場合は、セカンダリ ISE サーバーを設定できるようになりました。<br><br>ISE アイデンティティ オブジェクトにセカンダリサーバーの属性が追加されました。 |

| 機能 | 説明 |
| --- | --- |
| ファイル/マルウェアイベントを外部 syslog サーバーに送信 | アクセス制御ルールで設定されたファイルポリシーによって生成されるファイル/マルウェアイベントを受信するように、外部 syslog サーバーを設定できるようになりました。ファイルイベントはメッセージ ID 430004 を使用し、マルウェアイベントは 430005 を使用します。<br><br>ファイル/マルウェア syslog サーバーのオプションが **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ログの設定（Logging Settings）]** ページに追加されました。 |
| 内部バッファのログおよびカスタムイベントのログフィルタのサポート | 内部バッファをシステムロギングの宛先として設定できるようになりました。さらに、イベントログフィルタを作成して、syslog サーバーおよび内部バッファロギングの宛先に対して生成されるメッセージをカスタマイズできます。<br><br>イベント ログ フィルタ オブジェクトを [オブジェクト（Objects）]ページに追加し、オブジェクトを使用する機能を **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ログの設定（Logging Settings）]** ページに追加しました。内部バッファ オプションも [ログの設定（Logging Settings）] ページに追加しました。 |
| Device Manager Web サーバーの証明書。 | Device Manager の設定インターフェイスへの HTTPS 接続に使用される証明書を設定できるようになりました。Web ブラウザがすでに信頼している証明書をアップロードすることで、デフォルトの内部証明書を使用するときに、Untrusted Authority メッセージを回避できます。**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** > **[管理Webサーバー（Management Web Server）]** ページが追加されました。 |
| Cisco Threat Response のサポート | Cisco Threat Response のクラウドベースのアプリケーションに侵入イベントを送信するようにシステムを設定できます。Cisco Threat Response は侵入分析に使用できます。<br><br>Cisco Threat Response を **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** ページに追加しました。 |

# バージョン 6.4 の新しいハードウェアと仮想プラットフォーム

表 *23* : バージョン *6.4.0* の新しいハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| Firepower 1010、1120、1140 上の FTD。 | Firepower 1010、1120、および 1140 を導入しました。 |
| Firepower 4115、4125、4145 上の FTD。 | Firepower 4115、4125、および 4145 が導入されました。 |
| Firepower 9300 SM-40、SM-48、および SM-56 のサポート | 新しい 3 つのセキュリティ モジュール（SM-40、SM-48、SM-56）を導入しました。<br>FXOS バージョン 2.6.1 では、同じシャーシ内に異なるタイプのセキュリティモジュールを混在できます。 |
| 同じ Firepower 9300 上の ASA および FTD。 | FXOS 2.6.1 では、ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 |

# FDM バージョン 6.4 で廃止された機能

表 *24* : *FDM* バージョン *6.4* パッチで廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| **バージョン 6.4.0.7**<br>出力最適化。 | パッチを適用すると、出力最適化処理がオフになります。 | CSCvq34340 を軽減するため、FTD にパッチを適用してバージョン 6.4.0.7 以降にすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。<br>（注） この問題が修正されているバージョン 6.6.0+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。<br>バージョン 6.4.0 ～ 6.4.0.6 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。<br>詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。 |

表 *25 : FDM* バージョン *6.4.0* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| SSL ハードウェア アクセラレーション FTD CLI コマンド | なし。 | TLS crypto アクセラレーション機能の一部として、次の FTD CLI コマンドを削除しました。<br>• **system support ssl-hw-accel enable**<br>• **system support ssl-hw-accel disable**<br>• **system support ssl-hw-status**<br>代替手段の詳細については、新しい機能のマニュアルを参照してください。 |

# バージョン 6.3

## FDM バージョン 6.3 の新機能

表 *26 : FDM* バージョン *6.3* パッチの新機能

| 機能 | 説明 |
|---|---|
| **バージョン 6.3.0.1**<br>EMS 拡張機能のサポート | **アップグレードの影響。**<br>バージョン 6.3.0.1 では EMS 拡張機能のサポートが再導入されます。これは、バージョン 6.2.3.8/6.2.3.9 で導入されましたが、バージョン 6.3.0 には含まれていませんでした。<br>[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、再び ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になります。EMS 拡張機能は、 RFC 7627 によって定義されています。 |

表 *27 : FDM* バージョン *6.3.0* の新機能

| 機能 | 説明 |
|---|---|
| 高可用性設定。 | 2 つのデバイスをアクティブ/スタンバイ高可用性ペアとして設定できます。ハイ アベイラビリティまたはフェールオーバーセットアップは、プライマリ デバイスの障害時にセカンダリ デバイスで引き継ぐことができるように、2 つのデバイスを結合します。これにより、デバイスの障害時にネットワーク運用を維持できます。デバイスは、同じモデルで、同じ数と同じタイプのインターフェイスを備えており、同じソフトウェア バージョンを実行している必要があります。ハイ アベイラビリティは [デバイス（Device）] ページから設定できます。 |
| パッシブ ユーザー アイデンティティ取得のサポート。 | パッシブ認証を使用するようにアイデンティティ ポリシーを設定できます。パッシブ認証では、ユーザにユーザ名とパスワードを求めることなくユーザ アイデンティティを収集します。システムは、ユーザーが指定したアイデンティティ ソース（Cisco Identity Services Engine（ISE）/Cisco Identity Services Engine Passive Identity Connector（ISE PIC）を指定可能）からマッピングを取得します。または、リモート アクセス VPN ユーザーからログインを取得します。<br><br>変更には、**[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** でのパッシブ認証ルールのサポートと、または **[オブジェクト（Objects）]** > **[アイデンティティ ソース（Identity Sources）]** の ISE 設定が含まれます。 |
| リモート アクセス VPN およびユーザー アイデンティティに関するローカル ユーザーのサポート。 | Device Manager で直接ユーザーを作成できるようになりました。その後、これらのローカル ユーザー アカウントを使用して、リモート アクセス VPN への接続を認証できます。ローカル ユーザ データベースは、プライマリまたはフォールバック認証ソースとして使用できます。さらに、ローカル ユーザー名がダッシュボードに反映され、それらをポリシーでのトラフィック照合に利用できるように、アイデンティティ ポリシーでパッシブ認証ルールを設定できます。<br><br>**[オブジェクト（Objects）]** > **[ユーザー（Users）]** ページが追加されました。また、リモート アクセス VPN ウィザードが更新され、フォールバック オプションが追加されました。 |

| 機能 | 説明 |
| --- | --- |
| アクセス コントロール ポリシーでの VPN トラフィック処理のデフォルト動作の変更（**sysopt connection permit-vpn**）。 | アクセス コントロール ポリシーによる VPN トラフィックの処理方法に対するデフォルト動作が変更されました。6.3 以降では、アクセス コントロール ポリシーによりすべての VPN トラフィックが処理されるのがデフォルトです。これにより、URL フィルタリング、侵入防御、およびファイルポリシーを含む高度なインスペクションを VPN トラフィックに適用することができます。VPN トラフィックを許可するアクセス制御ルールを設定する必要があります。または、FlexConfig を使用して **sysopt connection permit-vpn** コマンド設定することもできます。このコマンドは、VPN 終端トラフィックがアクセス コントロール ポリシー（および高度なインスペクション）をバイパスするようにシステムに指示します。 |
| FQDN ベースのネットワーク オブジェクトのサポートと、DNS ルックアップに関するデータ インターフェイスのサポート。 | 静的 IP アドレスではなく完全修飾ドメイン名（FQDN）によってホストを指定するネットワーク オブジェクト（およびグループ）を作成できるようになりました。システムは、アクセス制御ルールで使用される FQDN オブジェクトに関して、FQDN から IP アドレスへのマッピングのルックアップを定期的に実行します。これらのオブジェクトはアクセス制御ルールのみで使用できます。<br><br>オブジェクトページに DNS グループオブジェクトが追加されました。また、**[システム設定（System Settings）] > [DNS サーバー（DNS Server）]** ページが、データインターフェイスにグループを割り当てられるように変更され、アクセス制御ルールが、FQDN ネットワークオブジェクトを選択できるように変更されました。さらに、管理インターフェイスの DNS 設定では、DNS サーバーアドレスのセットリストの代わりに DNS グループが使用されるようになりました。 |
| TCP Syslog のサポートと、管理インターフェイスを介して診断 Syslog メッセージを送信する機能。 | 以前のリリースでは、診断 Syslog メッセージは（接続および侵入メッセージとは対照的に）常にデータ インターフェイスを使用していました。すべてのメッセージが管理インターフェイスを使用するように Syslog を設定できるようになりました。最終的な送信元 IP アドレスは、データ インターフェイスを管理インターフェイスのゲートウェイとして使用するかどうかによって異なります。使用する場合は、IP アドレスがデータ インターフェイスのものになります。UDP ではなく TCP をプロトコルとして使用するように Syslog を設定することもできます。<br><br>**[オブジェクト（Objects）] > [Syslog サーバー（Syslog Servers）]** から Syslog サーバーを追加/編集できるようにダイアログボックスが変更されました。 |

| 機能 | 説明 |
|---|---|
| RADIUS を使用した Device Manager ユーザーの外部認証および認可。 | Device Manager にログインするユーザーを、外部 RADIUS サーバーを使用して認証および認可できます。外部ユーザーに、管理者アクセス権、読み取り/書き込みアクセス権、または読み取り専用アクセス権を付与できます。Device Manager は 5 つの同時ログインをサポートでき、6 番目のセッションは、最も古いセッションから自動的にログオフされます。必要に応じて、Device Manager のユーザーセッションを強制的に終了させることができます。<br>**[オブジェクト（Objects）] > [アイデンティティソース（Identity Sources）]** ページに RADIUS サーバーおよび RADIUS サーバーグループオブジェクトが追加され、それらのオブジェクトを設定できるようになりました。**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** に [AAA設定（AAA Configuration）] タブが追加され、サーバーグループを使用できるようになりました。さらに、**[モニタリング（Monitoring）] > [セッション（Sessions）]** ページにはアクティブユーザーのリストが表示され、管理ユーザーはセッションを終了させることができます。 |
| 保留中の変更のビューと展開の改善。 | 展開ウィンドウが変更され、展開される保留中の変更がより明確に表示されるようになりました。また、変更を破棄し、変更をクリップボードにコピーして、変更を YAML 形式のファイルでダウンロードするオプションが追加されました。さらに、監査ログで簡単に見つけることができるように、展開ジョブに名前を付けることが可能になりました。 |
| 監査ログ。 | 展開、システム タスク、設定の変更、管理ユーザーのログイン/ログアウトなどのイベントを記録する監査ログを表示できます。**[デバイス（Device）] > [デバイス管理（Device Administration）] > [監査ログ（Audit Log）]** ページが追加されました。 |
| 設定をエクスポートする機能。 | 記録を保持するためにデバイス設定のコピーをダウンロードできます。ただし、この設定をデバイスにインポートすることはできません。この機能は、バックアップ/復元に代わるものではありません。**[デバイス（Device）] > [デバイス管理（Device Administration）] > [設定のダウンロード（Download Configuration）]** ページが追加されました。 |

| 機能 | 説明 |
|---|---|
| 未知の URL に関する URL フィルタリングの改善。 | アクセス制御ルールでカテゴリベースの URL フィルタリングを実行する場合、ユーザは、カテゴリとレピュテーションが URL データベースに定義されていない URL にアクセスする可能性があります。以前は、Cisco Collective Security Intelligence（CSI）からそれらの URL のカテゴリとレピュテーションのルックアップを実行するオプションを手動で有効にする必要がありました。現在は、このオプションがデフォルトで有効になっています。さらに、ルックアップの結果に関して存続可能時間（TTL）を設定できるようになりました。これにより、システムは、未知の URL ごとにカテゴリまたはレピュテーションを更新できるようになりました。**[デバイス（Device）] > [システム設定（System Settings）] > [URL フィルタリングの設定（URL Filtering Preferences）]** ページが更新されました。 |
| デフォルトで、セキュリティ インテリジェンス ロギングが有効になりました。 | セキュリティ インテリジェンス ポリシーは 6.2.3 で導入され、ロギングはデフォルトで無効になっていました。6.3.0 以降、ロギングはデフォルトで有効になります。6.2.3 からアップグレードした場合、ロギング設定は有効または無効なまま保持されます。ポリシー適用の結果を表示したい場合は、ロギングを有効にします。 |
| パッシブ モード インターフェイス | インターフェイスはパッシブ モードで設定できます。パッシブに機能する場合、インターフェイスは（ハードウェア デバイスの）スイッチそのものまたは（Threat Defense Virtual の）プロミスキャス VLAN に設定されたモニタリング セッションで送信元ポートからのトラフィックを単にモニターします。<br><br>パッシブ モードを使用すると、アクティブなファイアウォールとして展開した場合の Threat Defense Virtual デバイスの動作を評価できます。また、IDS（侵入検知システム）サービスが必要な実稼働ネットワーク（脅威について知る必要があるが、デバイスに脅威をアクティブに防止させない）でパッシブ インターフェイスを使用できます。物理インターフェイスの編集時やセキュリティ ゾーンの作成時にパッシブ モードを選択できます。 |
| OSPF に関する Smart CLI の機能拡張と、BGP のサポート。 | Smart CLI の OSPF 設定機能が拡張されました。これには、標準/拡張 ACL、ルート マップ、AS パス オブジェクト、IPv4/IPv6 プレフィックス リスト、ポリシー リスト、および標準/拡張コミュニティ リストに関する新しい Smart CLI オブジェクト タイプが含まれます。また、Smart CLI を使用して BGP ルーティングを設定できるようになりました。これらの機能は、**[デバイス（Device）] > [詳細設定（Advanced Configuration）]** ページから使用できます。 |

| 機能 | 説明 |
|---|---|
| ISA 3000 デバイスに関する機能拡張。 | ISA 3000 のアラーム、ハードウェア バイパス、および SD カードによるバックアップ/復元の各機能を設定できるようになりました。アラームとハードウェア バイパスの設定には FlexConfig を使用します。SD カードについては、Device Manager のバックアップおよび復元ページが更新されました。 |
| Threat Defense 6.3 以降での ASA 5506-X、5506W-X、5506H-X、および 5512-X のサポートの削除。 | Threat Defense の 6.3 以降のリリースを ASA 5506-X、5506W-X、5506H-X、および 5512-X にインストールすることはできません。これらのプラットフォームに関してサポートされる Threat Defense の最後のリリースは 6.2.3 です。 |
| Threat Defense REST API バージョン 2（v2）。 | ソフトウェア バージョン 6.3 用の Threat Defense REST API のバージョン番号が 2 になりました。API の URL の v1 を v2 に置き換える必要があります。v2 の API には、ソフトウェア バージョン 6.3 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、ログインした後に、Device Manager の URL の最後を **/#/api-explorer** に変更します。 |
| 製品の使用情報をシスコに提供するための Web 分析。 | ページのヒットに基づいて製品の使用情報を匿名でシスコに提供する Web 分析を有効にできます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブデータは送信されません。Web 分析はデフォルトで有効になっています。<br>**[デバイス（Device）] > [システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** ページに Web 分析が追加されました。 |
| 脆弱性データベース（VDB）の更新のインストールにより Snort が再起動しなくなりました。 | VDB の更新のインストール時に Snort が自動的に再起動されなくなりました。ただし、Snort は、引き続き、次回の設定展開時に再起動します。 |
| Snort が再起動されない侵入ルール（SRU）データベースの更新の展開。 | 侵入ルール（SRU）の更新をインストールした後は、新しいルールを有効にするために設定を展開する必要があります。SRU の更新の展開時に Snort が再起動されなくなりました。 |

# FDM バージョン 6.3 で廃止された機能

表 *28 : FDM* バージョン *6.3.0* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| 復号化のための EMS 拡張機能のサポート（一時的に中止）。 | パッチまたはアップグレードを行うまで、EMS 拡張機能のサポートは中止されます。 | バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが一時的に中止されます。つまり、[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポート（よりセキュアな通信が可能）しなくなります。EMS 拡張機能は、 RFC 7627 によって定義されています。<br>サポートはバージョン 6.3.0.1 で再導入されています。 |

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| FlexConfig コマンド。 | アップグレード後に設定をやり直す必要があります。 | バージョン 6.3 では、FDM を使用する FTD の次の FlexConfig コマンドは廃止されます。<br>• **access-list**：スマート CLI 拡張アクセスリストまたは標準アクセスリストオブジェクトを使用して、**extended** および **standard** アクセスリストを作成できるようになりました。その後、それらは、サービスポリシー トラフィック クラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド（**match access-list** など）で使用できます。<br>• **as-path**：スマート CLI AS パスオブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、自律システムパスフィルタを設定できるようになりました。<br>• **community-list**：スマート CLI 拡張コミュニティ リスト オブジェクトまたは標準コミュニティ リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、コミュニティリストフィルタを設定できるようになりました。<br>• **dns-group**：**[オブジェクト（Objects）] > [DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）] > [システム設定（System Settings）] > [DNSサーバー（DNS Server）]** を使用してグループ割り当てができるようになりました。<br>• **policy-list**：スマート CLI ポリシーリストオブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシーリストを設定できるようになりました。<br>• **prefix-list**：スマート CLI IPv4 プレフィックス リスト オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、IPv4 用のプレフィックスリストフィルタリングを設定できるようになりました。<br>• **route-map**：スマート CLI ルートマップオブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルートマップを設定できるようになりました。<br>• **router bgp**：BGP にスマート CLI テンプレートを使用できるようになりました。 |

## バージョン 6.3 で廃止されたハードウェアと仮想プラットフォーム

表 *29* : バージョン *6.3.0* で廃止されたハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| VMware vSphere/VMware ESXi 5.5 のサポート。 | バージョン 6.3 では、VMware vSphere/VMware ESXi 6.0 での仮想展開のサポートが廃止されています。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。 |
| ASA 5512-X および 5506-X シリーズ。 | ASA 5506-X、5506H-X、5506W-X、および 5512-X では、バージョン 6.3 以降を実行できません。 |

# バージョン 6.2.3

## FDM バージョン 6.2.3 の新機能

表 *30* : *FDM* バージョン *6.2.3* パッチの新機能

| 機能 | 説明 |
|---|---|
| **バージョン 6.2.3.8**<br>EMS 拡張機能のサポート | [復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になりました。EMS 拡張機能は、RFC 7627 によって定義されています。<br>（注） バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコ サポートおよびダウンロードサイトから削除されました。バージョン 6.2.3.9 にアップグレードすると、EMS 拡張機能のサポートも有効になります。バージョン 6.3.0 では EMS 拡張機能のサポートが中止されています。サポートはバージョン 6.3.0.1 で再導入されています。 |

| 機能 | 説明 |
|---|---|
| **バージョン 6.2.3.7**<br>FTD の TLS v1.3 ダウングレード CLI コマンド | 新しい CLI コマンドを使用すると、TLS v1.3 接続を TLS v1.2 にダウングレードするタイミングを指定できます。<br>多くのブラウザでは、デフォルトで TLS v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗します。<br>詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスで **system support** コマンドを参照してください。これらのコマンドは、Cisco TAC に問い合わせてから使用することをお勧めします。 |

表 *31 : FDM* バージョン *6.2.3* の新機能

| 機能 | 説明 |
|---|---|
| SSL/TLS の復号 | 接続の内容を調べることができるように、SSL/TLS 接続を復号できます。復号しないと、暗号化された接続は、侵入およびマルウェアの脅威を識別したり、URL およびアプリケーション使用状況ポリシーへの準拠を強制したりするための効果的な検査が行えません。**[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** ページおよび **[モニタリング（Monitoring）]** > **[SSL復号（SSL Decryption）]** ダッシュボードが追加されました。<br>**注目** アクティブな認証を実装するアイデンティティポリシーは、SSL 復号ルールを自動的に生成します。SSL 復号をサポートしていないリリースからアップグレードする場合、SSL 復号ポリシーは、この種類のルールがある場合、自動的に有効になります。ただし、アップグレードの完了後、再署名の復号ルールで使用する証明書を指定する必要があります。アップグレード後すぐに SSL 復号設定を編集してください。 |

| 機能 | 説明 |
| --- | --- |
| セキュリティ インテリジェンスのブラックリスト登録 | 新しい **[ポリシー（Policies）]** > **[セキュリティ インテリジェンス（Security Intelligence）]** ページから設定できるセキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先URLに基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。<br><br>また、[ポリシー（Policies）] ダッシュボードの名前を [アクセスおよびSIルール（Access And SI Rules）] に変更し、セキュリティ インテリジェンス同等のルールがアクセス ルールとともにダッシュボードに含まれるようになりました。 |
| 侵入ルールの調整 | アクセス制御ルールを適用する事前に定義された侵入ポリシー内の侵入ルールのアクションを変更できます。トラフィックに一致するイベント（警告）をドロップまたは生成する各ルールを設定したり、ルールを無効にしたりできます。有効になっているルールのアクション（ドロップまたは警告に設定）のみ変更できます。デフォルトで無効になっているルールを有効にはできません。侵入ルールを調整するには、**[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。 |
| 侵入ポリシーに基づく自動ネットワーク分析ポリシー（NAP）割り当て | 以前のリリースでは、[Balanced Security and Connectivity] ネットワーク分析ポリシーが、特定の送信元/送信先のセキュリティゾーンとネットワーク オブジェクトの組み合わせに割り当てられた侵入ポリシーに関係なく、プリプロセッサ設定で常に使用されました。システムは自動的に NAP ルールを生成し、同じ名前の NAP と侵入ポリシーをそれらの基準に基づいてトラフィックに割り当てるようになりました。レイヤ 4 または 7 の基準を使用して異なる侵入ポリシーをトラフィック（それ以外は同じ送信元/送信先のセキュリティ ゾーンおよびネットワーク オブジェクトと一致する）に割り当てる場合、完全に一致するNAPおよび侵入ポリシーは取得されないことに注意してください。カスタム ネットワーク分析ポリシーは作成できません。 |
| 脅威、攻撃、およびターゲットのダッシュボード用のドリル ダウン レポート | 脅威、攻撃、およびターゲットのダッシュボードに移動して、報告された項目についての詳細を表示できるようになりました。これらのダッシュボードは [Monitoring] ページで使用できます。<br><br>これらの新しいレポートのため、6.2.3 より前のリリースからアップグレードする場合は、これらのダッシュボードのレポートデータが失われます。 |

| 機能 | 説明 |
|---|---|
| [Web Applications] ダッシュボード | 新しい [Web Applications] ダッシュボードは、Google など、ネットワークで使用されている上位の Web アプリケーションを示します。このダッシュボードはアプリケーションのダッシュボードを強化し、HTTP の使用率などのプロトコル指向の情報を提供します。 |
| 新しいゾーンのダッシュボードが入力ゾーンと出力ゾーンのダッシュボードを置き換え | 新しいゾーンのダッシュボードは、デバイスに入ってから出るトラフィックに対する上位セキュリティ ゾーンのペアを示します。このダッシュボードは、入力および出力ゾーンに対する個別のダッシュボードを置き換えます。 |
| 新しいマルウェア ダッシュボード | 新しいマルウェアダッシュボードは、上位のマルウェアのアクションと判定結果の組み合わせを示します。ドリルダウンして、関連付けられているファイル タイプの情報を参照できます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。 |
| 自己署名入りの内部証明書、および内部 CA 証明書 | 自己署名入りの内部アイデンティティ証明書を生成できるようになりました。また、SSL 復号ポリシーで使用するための、自己署名付きの内部 CA 証明書を生成したり、アップロードできるようになりました。これらの機能を、**[オブジェクト（Objects）]** > **[証明書（Certificates）]** ページで設定します。 |
| インターフェイスのプロパティ編集時に DHCP サーバーの設定を編集する機能 | インターフェイスのプロパティを編集すると同時に、インターフェイスに設定されている DHCP サーバーの設定を編集できるようになりました。これにより、インターフェイスの IP アドレスを別のサブネットに変更する必要がある場合に、DHCP アドレス プールを簡単に再定義できます。 |
| 製品を改善し、効果的な技術サポートを提供するための、Cisco Success Network によるシスコへの利用状況や統計データの送信 | Cisco Success Network に接続し、シスコにデータを送信できます。Cisco Success Network を有効にすることで、テクニカル サポートを提供するために不可欠な、使用状況の情報と統計情報をシスコに提供します。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。Cisco Smart Software Manager でデバイスを登録するとき、または後から好きなときに、接続を有効にできます。接続はいつでも無効にできます。<br><br>Cisco Success Network はクラウド サービスです。**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウド管理（Cloud Management）]** ページの名前が [クラウドサービス（Cloud Services）] に変更されました。同じページから、Cisco Defense Orchestrator を設定できます。 |

| 機能 | 説明 |
| --- | --- |
| Threat Defense Virtual カーネルベースの仮想マシン（KVM）のハイパーバイザデバイス用の設定 | Device Manager を使用して、KVM 用の Threat Defense Virtual デバイス上の Threat Defense を設定できます。以前は、VMware のみがサポートされていました。<br>（注） Device Manager のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Device Manager に切り替えることはできません。 |
| ISA 3000（Cisco 3000 シリーズ産業用セキュリティアプライアンス）デバイスの設定 | Device Manager を使用して ISA 3000 デバイス上の Threat Defense を設定できます。ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。 |
| ルール データベースまたは VDB の更新でのオプションの展開 | 侵入ルール データベースまたは VDB を更新する、または更新スケジュールを設定する際に、更新が即時展開しないようにすることができます。更新プログラムは検査エンジンを再起動するため、展開時に瞬間的なトラフィックのドロップが発生します。自動的に展開しないことにより、トラフィックのドロップの影響が最小になる場合に展開を開始できます。<br>（注） VDB ダウンロードは、単独で Snort を再起動することもできますが、展開時に再起動が発生します。ダウンロード時の再起動を止めることはできません。 |
| 展開が Snort を再起動するかどうかを示す、改善されたメッセージ。さらに、展開時の Snort を再起動する必要性の低下 | 展開を開始する前に、Device Manager により、設定の更新で Snort の再起動が必要かどうかが示されます。Snort の再起動は、トラフィックの瞬間的なドロップを発生させます。したがって、展開がトラフィックに影響を与えず、すぐに実行できるかどうかがわかるようになったため、混乱が少ないときに展開できます。<br>さらに、以前のリリースでは展開の実行の度に Snort が再起動されていました。Snort は、次の理由でのみ再起動されるようになりました。<br>• ユーザが SSL 復号ポリシーを有効または無効にする<br>• 更新されたルール データベースまたは VDB がダウンロードされた<br>• ユーザーが 1 つまたは複数の物理インターフェイス（ただしサブインターフェイスではない）で MTU を変更した |

| 機能 | 説明 |
| --- | --- |
| Device Manager の CLI コンソール | Device Manager から CLI コンソールを開くことができるようになりました。CLI コンソールは SSH またはコンソールセッションを模倣していますが、コマンドのサブセットのみ（**show**、**ping**、**traceroute**、および **packet-tracer**）を許可します。トラブルシューティングとデバイスのモニターリングに CLI コンソールを使用します。 |
| 管理アドレスへのアクセスのブロックのサポート | 管理 IP アドレスにアクセスできないようにするため、プロトコルのすべての管理アクセスリストのエントリを削除できるようになりました。以前は、すべてのエントリを削除すると、すべてのクライアント IP アドレスからのアクセスを許可するようにシステムのデフォルトが設定されていました。6.2.3 へのアップグレードでは、以前からのプロトコル（HTTPS または SSH）用の空の管理アクセス リストがあった場合、システムはすべての IP アドレス用のデフォルトの許可ルールを作成します。必要に応じて、これらのルールを削除できます。<br><br>また、SSH または HTTPS アクセスを無効にする場合を含み、Device Manager は CLI から管理アクセスリストに加えた変更を認識します。<br><br>少なくとも 1 つのインターフェイスに対する HTTPS アクセスを有効にしてください。そうしないとデバイスを設定および管理することができません。 |

| 機能 | 説明 |
| --- | --- |
| デバイス CLI を使用した、機能の設定のための Smart CLI および FlexConfig | Smart CLI と FlexConfig により、まだ Device Manager ポリシーおよび設定では直接サポートされていない機能を設定できます。Threat Defense は、いくつかの機能を実装するために ASA 設定コマンドを使用します。ASA 設定コマンドの知識があり、専門家ユーザーの場合、次の方法を使用して、デバイスでこれらの機能を設定できます。<br>• Smart CLI：（推奨される方法です。）Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。このリリースでは、Smart CLI を使用して、OSPFv2 を設定できます。<br>• FlexConfig：FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。<br>**注意** Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI または FlexConfig を介して機能を有効にすると、その他の設定済みの機能に予期しない結果が発生する可能性があります。 |
| Threat Defense REST API、および API エクスプローラ | REST API を使用して、Device Manager を介してローカルで管理している Threat Defense デバイスをプログラムで操作できます。オブジェクトモデルを表示し、クライアントプログラムから作成できるさまざまな呼び出しのテストに使用できる API エクスプローラがあります。API エクスプローラを開くには、Device Manager にログインし、URL のパスを /#/api-explorer（https://ftd.example.com/#/api-explorer など）に変更します。 |

# バージョン 6.2.3 の新しいハードウェアと仮想プラットフォーム

表 *32* : バージョン *6.2.3* の新しいハードウェアと仮想プラットフォーム

| 機能 | 説明 |
|---|---|
| ISA 3000 の FTD。 | ISA 3000 シリーズで FTD を実行できるようになりました。<br>ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。ハードウェアバイパスやアラームポートなど、ASA でサポートされていた ISA 3000 の特別な機能は、このリリースの FTD ではサポートされていません。 |
| VMware ESXi 6.5 のサポート。 | VMware vSphere/VMware ESXi 7.5 に FTDv 仮想アプライアンスを展開できるようになりました。 |
| カーネル ベースの仮想マシン（KVM）ハイパーバイザデバイス用 FTDv の設定。 | FDM を使用して KVM デバイスの FTDv で FTD を設定できます。以前は、VMware のみがサポートされていました。<br>FDM のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして FDM に切り替えることはできません。 |

# FDM バージョン 6.2.3 で廃止された機能

表 *33* : *FDM* バージョン *6.2.3* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| **pager** FlexConfig コマンド。 | アップグレード後に設定をやり直す必要があります。 | バージョン 6.2.3 では、FDM を使用した FTD の場合、**pager** FlexConfig CLI コマンドがブロックされます。 |

# バージョン 6.2.2

## FDM バージョン 6.2.2 の新機能

表 *34 : FDM* バージョン *6.2.2* の新機能

| 機能 | 説明 |
|---|---|
| ASA 5500-X シリーズ デバイスのリモートアクセス VPN の設定 | ASA 5500-X シリーズ デバイスでは、AnyConnect クライアント用にリモートアクセス SSL VPN を設定できます。**[Device]** > **[Remote Access VPN]** グループから RA VPN を設定します。**[Device]** > **[Smart License]** グループから RA VPN ライセンスを設定します。 |
| Threat Defense Virtual for VMware デバイス設定。 | Device Manager を使用して、VMware デバイス対応の Threat Defense Virtual 上で Threat Defense を設定できます。その他の仮想プラットフォームは Device Manager ではサポートされません。<br>（注） Device Manager のサポートを得るには、新しい 6.2.2 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Device Manager に切り替えることはできません。 |

# バージョン 6.2.1

## FDM バージョン 6.2.1 の新機能

このリリースは Firepower 2100 シリーズのみに適用されます。

表 *35 : FDM* バージョン *6.2.1* の新機能

| 機能 | 説明 |
|---|---|
| リモートアクセス VPN の設定 | AnyConnect クライアントのリモート アクセス SSL VPN を設定できます。**[Device]** > **[Remote Access VPN]** グループから RA VPN を設定します。**[Device]** > **[Smart License]** グループから RA VPN ライセンスを設定します。 |
| Firepower 2100 シリーズ デバイス設定 | Device Manager を使用して、 Firepower 2100 シリーズ デバイス上の Threat Defense を設定できます。 |

# バージョン 6.2

## FDM バージョン 6.2 の新機能

表 *36 : FDM* バージョン *6.2.0* の新機能

| 機能 | 説明 |
|---|---|
| Cisco Defense Orchestrator（CDO）のクラウド管理。 | Cisco Defense Orchestrator のクラウドベースのポータルを使用してデバイスを管理できます。**[Device]** > **[System Settings]** > **[Cloud Management]** を選択します。Cisco Defense Orchestrator の詳細については、http://www.cisco.com/go/cdo を参照してください。 |
| アクセスルールのドラッグアンドドロップ。 | ルールテーブルで、アクセスルールをドラッグアンドドロップして移動できます。 |
| Threat Defense ソフトウェアを Device Manager からアップグレードします。 | Device Manager からソフトウェアアップグレードをインストールできます。**[Device]** > **[Updates]** を選択します。 |

| 機能 | 説明 |
| --- | --- |
| デフォルトの設定変更。 | 新しいデバイスまたは再イメージ化されたデバイスでは、デフォルト設定に次の重要な変更が含まれます。<br>• （ASA 5506-X、5506W-X、5506H-X）最初のデータ インターフェイスと ASA 5506W-X の Wi-Fi インターフェイスを除き、これらのデバイス モデルのその他すべてのデータインターフェイスは、「内部」ブリッジ グループに構造化され、有効化されます。DHCP サーバーは内部のブリッジ グループにあります。ブリッジドインターフェイスにエンドポイントまたはスイッチを接続することができ、エンドポイントは 192.168.1.0/24 ネットワーク上のアドレスを取得します。<br>• 内部インターフェイス IP アドレスは 192.168.1.1 です。DHCP サーバーは、アドレス プールの 192.168.1.5 ～ 192.168.1.254 のインターフェイスで定義されます。<br>• HTTPS アクセスは内部インターフェイス上で有効になるため、デフォルト アドレスの 192.168.1.1 で内部インターフェイスを介して Device Manager を開くことができます。ASA 5506-X モデルでは、内部ブリッジ グループ メンバー インターフェイス経由でこれを実行できます。<br>• 管理ポートは、192.168.45.0/24 ネットワークの DHCP サーバーをホストします。ワークステーションを管理ポートに直接接続して、IP アドレスを取得し、Device Manager を開いてデバイスを設定できます。<br>• OpenDNS のパブリック DNS サーバーは、現在、管理インターフェイスのデフォルト DNS サーバーです。以前は、デフォルト DNS サーバーはありませんでした。デバイスの設定時に、別の DNS サーバーを設定できます。<br>• 管理 IP アドレスのデフォルト ゲートウェイでは、データ インターフェイスを使用してインターネットにルーティングします。したがって、Management 物理インターフェイスをネットワークに配線する必要はありません。 |

| 機能 | 説明 |
| --- | --- |
| 管理インターフェイスおよびアクセスの変更。 | 管理アドレス機能および Device Manager へのアクセス方法に対するいくつかの変更：<br>• HTTPS（Device Manager 用）および SSH（CLI 用）接続に対するデータインターフェイスを開くことができます。デバイスを管理するために、別の管理ネットワークを必要としたり、管理/診断物理ポートを内部ネットワークに接続したりする必要はありません。**[Device]** > **[System Settings]** > **[Management Access List]** を選択します。<br>• システムは、外部インターフェイスのゲートウェイ経由でシステムデータベースのアップデートを取得できます。管理インターフェイスまたはネットワークからインターネットへの明示的なルートは必要ありません。デフォルトでは、データ インターフェイスを介して内部ルートを使用します。ただし、別の管理ネットワークを使用する場合、特定のゲートウェイを設定できます。**[Device]** > **[System Settings]** > **[Management Interface]** を選択します。<br>• Device Manager を使用して、DHCP を介して IP アドレスを取得するように管理インターフェイスを設定できます。**[Device]** > **[System Settings]** > **[Management Interface]** を選択します。<br>• スタティック アドレスを設定する場合、管理アドレスで DHCP サーバーを設定できます。**[Device]** > **[System Settings]** > **[Management Interface]** を選択します。 |

| 機能 | 説明 |
| --- | --- |
| さまざまなユーザーインターフェイスの変更。 | 次に、Device Manager ユーザーインターフェイスの注目すべき変更を示します。<br>• [デバイス（Device）] メインメニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは、[デバイスダッシュボード（Device Dashboard）] ではなく [デバイスサマリー（Device Summary）] と呼ばれます。<br>• デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。<br>• **[Device]** > **[System Settings]** > **[Cloud Preferences]** は、**[Device]** > **[System Settings]** > **[URL Filtering Preferences]** と呼ばれます。<br>• **[System Settings]** > **[DHCP Server]** ページは 2 つのタブで構成され、グローバルパラメータとは異なる DHCP サーバーテーブルが表示されます。 |
| サイト間 VPN 接続。 | 事前共有キーを使用して、サイト間のバーチャル プライベート ネットワーク（VPN）接続を設定できます。IKEv1 および IKEv2 接続を設定できます。 |

| 機能 | 説明 |
| --- | --- |
| 統合ルーティングおよびブリッジングのサポート | 統合ルーティングおよびブリッジングによって、ブリッジ グループとルーテッド インターフェイスの間でルーティングする機能が提供されます。ブリッジ グループは、Threat Defense デバイスがルーティングではなくブリッジするインターフェイスのグループです。Threat Defense デバイスは、Threat Defense デバイスがファイアウォールとして継続的に機能する本当のブリッジではありません。インターフェイス間のアクセス コントロールは管理され、すべての通常のファイアウォール チェックが実行されます。<br><br>この機能によって、ブリッジ グループを設定したり、ブリッジ グループ間およびブリッジ グループとルーテッドインターフェイスの間でルーティングするようにブリッジ グループを設定したりできます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。Threat Defense デバイスにブリッジ グループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ 2 スイッチを使用するのではない別の方法が提供されます。BVI は、名前付きインターフェイスにすることができ、メンバー インターフェイスとは別にいくつかの機能（DHCP サーバーなど）に参加できます。ここで、ブリッジ グループ メンバー インターフェイスで他の機能（NAT、アクセス コントロール ルールなど）を設定します。<br><br>**[Device]** > **[Interfaces]** を選択して、ブリッジグループを設定します。 |

# Version 6.1

## FDM バージョン 6.1 の新機能

表 *37 : FDM* バージョン *6.1.0* の新機能

| 機能 | 説明 |
| --- | --- |
| サポートされるデバイス。 | Firepower Device Manager を使用して、次のデバイスタイプを管理できます。<br><br>• ASA 5506-X、5506H-X、5506W-X、5508-X、5516-X<br><br>• ASA 5512-X、5515-X、5525-X、5545-X、5555-X |

| 機能 | 説明 |
| --- | --- |
| サポートされるファイアウォールモード。 | ルーテッドモードで動作するデバイスのみを設定できます。トランスペアレント モードはサポートされていません。 |
| サポートされるインターフェイスタイプおよびモード。 | ルーテッドインターフェイスのみを設定できます。インライン、インラインタップ、またはパッシブインターフェイスは設定できません。<br>また、物理インターフェイスとサブインターフェイスのみを設定できます。EtherChannel や冗長インターフェイスは設定できません。また、PPPoE を設定することもできません。 |
| セキュリティポリシー。 | 次のタイプのセキュリティポリシーを設定できます。<br>• アクセスコントロール：デバイスを通過できる接続を決定します。次のタイプのアクセス制御を実行できます。<br>  • セキュリティゾーン、IP アドレス、地理位置情報、プロトコル、およびポートのフィルタリング。<br>  • ユーザー名とユーザーグループのフィルタリング。<br>  • アプリケーション フィルタリング。<br>  • URL カテゴリ、レピュテーション、および個別の URL のフィルタリング。<br>  • 侵入ポリシー、脅威対策。<br>  • ファイルポリシー、マルウェア対策。<br>• ID ポリシー：IP アドレスに関連付けられているユーザーを判断します。このシステムはアクティブ認証のみをサポートし、パッシブ認証はサポートしていません。<br>• ネットワークアドレス変換：内部アドレスと外部アドレスを変換します。PAT プールを除き、ほとんどの NAT 機能がサポートされています。 |
| ルーティング。 | スタティックルートを設定できます。ダイナミック ルーティング プロトコルはサポートされていません。 |
| システムモニタリングと syslog。 | Firepower Device Manager には、最近の接続イベントを表示できるイベントビューアが含まれています。長期分析用にイベントを収集するために、外部 syslog サーバーを設定することもできます。<br>また、システムおよびシステムを通過するトラフィックに関する統計情報を提供する多数のダッシュボードもあります。 |

| 機能 | 説明 |
|---|---|
| 管理インターフェイスの設定。 | Firepower Device Manager から管理アドレスとインターフェイスを設定できます。CLI を使用する必要はありません。CLI または Firepower Device Manager にアクセスできる IP アドレスを制限するために、システムホスト名、管理 IP アドレスとゲートウェイ、DNS サーバー、NTP サーバー、およびアクセスルールを設定できます。 |
| 更新のスケジュール。 | システムデータベースの更新頻度を制御できます。<br>• [デバイス（Device）] メイン メニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは、[デバイスダッシュボード（Device Dashboard）] ではなく [デバイスサマリー（Device Summary）] と呼ばれます。<br>• デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。<br>• **[Device]** > **[System Settings]** > **[Cloud Preferences]** は、**[Device]** > **[System Settings]** > **[URL Filtering Preferences]** と呼ばれます。<br>• **[System Settings]** > **[DHCP Server]** ページは 2 つのタブで構成され、グローバルパラメータとは異なる DHCP サーバーテーブルが表示されます。 |
| バックアップと復元。 | Firepower Device Manager からシステムをバックアップおよび復元できます。 |
| トラブルシューティング ファイル。 | シスコテクニカルサポートと連携する際に、Firepower Device Manager からトラブルシューティング ファイルを生成できます。 |

# リリース日

表 *38* : バージョン *7.2* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 7.2.0.1 | 12 | 2022 年 8 月 10 日 | すべて |
| 7.2.0 | 82 | 2022-06-06 | すべて |

表 *39* : バージョン *7.1* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 7.1.0.2 | 36 | 2022 年 8 月 3 日 | FMC/FMCv<br>Secure Firewall 3100 シリーズ |
| 7.1.0.1 | 28 | 2022 年 02 月 24 日 | FMC/FMCv<br>Secure Firewall 3100 シリーズを除くすべてのデバイス |
| 7.1.0 | 90 | 2021 年 12 月 1 日 | すべて（All） |

表 *40* : バージョン *7.0* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 7.0.4 | 55 | 2022 年 8 月 10 日 | すべて |
| 7.0.3 | 37 | 2022-06-30 | すべて |
| 7.0.2.1 | 10 | 2022-06-27 | すべて |
| 7.0.2 | 88 | 2022 年 5 月 5 日 | すべて（All） |
| 7.0.1.1 | 11 | 2022 年 02 月 17 日 | すべて（All） |
| 7.0.1 | 84 | 2021-10-07 | すべて（All） |
| 7.0.0.1 | 15 | 2021 年 7 月 15 日 | すべて |
| 7.0.0 | 94 | 2021 年 5 月 26 日 | すべて |

表 *41* : バージョン *6.7* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.7.0.3 | 105 | 2022 年 02 月 17 日 | すべて（All） |
| 6.7.0.2 | 24 | 2021 年 5 月 11 日 | すべて（All） |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.7.0.1 | 13 | 2021 年 3 月 24 日 | すべて |
| 6.7.0 | 65 | 2020 年 11 月 2 日 | すべて |

表 *42 :* バージョン *6.6* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.6.7 | 223 | 2022 年 7 月 14 日 | すべて（All） |
| 6.6.5.2 | 14 | 2022 年 03 月 24 日 | すべて |
| 6.6.5.1 | 15 | 2021 年 12 月 6 日 | すべて（All） |
| 6.6.5 | 81 | 2021 年 8 月 3 日 | すべて（All） |
| 6.6.4 | 64 | 2021 年 4 月 29 日 | Firepower 1000 シリーズ |
| | 59 | 2021 年 4 月 26 日 | FMC/FMCv<br>Firepower 1000 シリーズを除くすべてのデバイス |
| 6.6.3 | 80 | 2020 年 3 月 11 日 | すべて |
| 6.6.1 | 91 | 2020 年 9 月 20 日 | すべて |
| | 90 | 2020 年 9 月 8 日 | — |
| 6.6.0.1 | 7 | 2020 年 7 月 22 日 | すべて |
| 6.6.0 | 90 | 2020 年 5 月 8 日 | Firepower 4112 |
| | | 2020 年 4 月 6 日 | FMC/FMCv<br>Firepower 4112 を除くすべてのデバイス |

表 *43* : バージョン *6.5* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム：アップグレード | プラットフォーム：再イメージ化 |
|---|---|---|---|---|
| 6.5.0.5 | 95 | 2021 年 2 月 9 日 | すべて | — |
| 6.5.0.4 | 57 | 2020 年 3 月 2 日 | すべて | — |
| 6.5.0.3 | 30 | 2020 年 2 月 3 日 | 利用できなくなりました。 | — |
| 6.5.0.2 | 57 | 2019 年 12 月 19 日 | すべて | — |
| 6.5.0.1 | 35 | 2019 年 11 月 20 日 | 利用できなくなりました。 | — |
| 6.5.0 | 123 | 2020 年 2 月 3 日 | FMC/FMCv | FMC/FMCv |
| | 120 | 2019 年 10 月 8 日 | — | — |
| | 115 | 2019 年 9 月 26 日 | すべてのデバイス | すべてのデバイス |

表 *44* : バージョン *6.4* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0.15 | 26 | 2022-05-31 | すべて（All） |
| 6.4.0.14 | 67 | 2022 年 02 月 18 日 | すべて |
| 6.4.0.13 | 57 | 2021 年 12 月 2 日 | すべて |
| 6.4.0.12 | 112 | 2021 年 5 月 12 日 | すべて（All） |
| 6.4.0.11 | 11 | 2021 年 1 月 11 日 | すべて（All） |
| 6.4.0.10 | 95 | 2020 年 10 月 21 日 | すべて |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0.9 | 62 | 2020 年 5 月 26 日 | すべて |
| 6.4.0.8 | 28 | 2020 年 1 月 29 日 | すべて |
| 6.4.0.7 | 53 | 2019 年 12 月 19 日 | すべて |
| 6.4.0.6 | 36 | 2019 年 10 月 16 日 | 利用できなくなりました。 |
| 6.4.0.5 | 23 | 2019 年 9 月 18 日 | すべて |
| 6.4.0.4 | 34 | 2019 年 8 月 21 日 | すべて |
| 6.4.0.3 | 29 | 2019 年 7 月 17 日 | すべて |
| 6.4.0.2 | 35 | 2019 年 7 月 3 日 | FMC/FMCv<br>FTD/FTDv（FirePOWER 1000 シリーズ以外） |
| | 34 | 2019 年 6 月 27 日 | — |
| | | 2019 年 6 月 26 日 | Firepower 7000/8000 シリーズ<br>ASA FirePOWER<br>NGIPSv |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0.1 | 17 | 2019 年 6 月 27 日 | FMC 1600、2600、4600 |
| | | 2019 年 6 月 20 日 | Firepower 4115、4125、4145<br>SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300 |
| | | 2019 年 5 月 15 日 | FMC 750、1000、1500、2000、2500、3500、4000、4500<br>FMCv<br>Firepower 2110、2120、2130、2140<br>Firepower 4110、4120、4140、4150<br>SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300<br>ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X<br>ASA 5585-X-SSP-10、-20、-40、-60<br>ISA 3000<br>FTDv<br>Firepower 7000/8000 シリーズ<br>NGIPSv |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.4.0 | 113 | 2020 年 3 月 3 日 | FMC/FMCv |
| | 102 | 2019 年 6 月 20 日 | Firepower 4115、4125、4145<br>SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300 |
| | | 2019 年 6 月 13 日 | Firepower 1010、1120、1140 |
| | | 2019 年 4 月 24 日 | Firepower 2110、2120、2130、2140<br>Firepower 4110、4120、4140、4150<br>SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300<br>ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X<br>ASA 5585-X-SSP-10、-20、-40、-60<br>ISA 3000<br>FTDv<br>Firepower 7000/8000 シリーズ<br>NGIPSv |

表 *45 :* バージョン *6.3* のリリース日

| バージョン | ビルド | 日付 | プラットフォーム：アップグレード | プラットフォーム：再イメージ化 |
|---|---|---|---|---|
| 6.3.0.5 | 35 | 2019 年 11 月 18 日 | Firepower 7000/8000 シリーズ<br>NGIPSv | — |
| | 34 | 2019 年 11 月 18 日 | FMC/FMCv<br>すべての FTD デバイス<br>ASA FirePOWER | — |
| 6.3.0.4 | 44 | 2019 年 8 月 14 日 | すべて | — |

| バージョン | ビルド | 日付 | プラットフォーム：アップグレード | プラットフォーム：再イメージ化 |
|---|---|---|---|---|
| 6.3.0.3 | 77 | 2019 年 6 月 27 日 | FMC 1600、2600、4600 | — |
| | | 2019 年 5 月 1 日 | FMC 750、1000、1500、2000、2500、3500、4000、4500<br>FMCv<br>すべてのデバイス | — |
| 6.3.0.2 | 67 | 2019 年 6 月 27 日 | FMC 1600、2600、4600 | — |
| | | 2019 年 3 月 20 日 | FMC 750、1000、1500、2000、2500、3500、4000、4500<br>FMCv<br>すべてのデバイス | — |
| 6.3.0.1 | 85 | 2019 年 6 月 27 日 | FMC 1600、2600、4600 | — |
| | | 2019 年 2 月 18 日 | FMC 750、1000、1500、2000、2500、3500、4000、4500<br>FMCv<br>すべてのデバイス | — |
| 6.3.0 | 85 | 2019 年 1 月 22 日 | Firepower 4100/9300 | Firepower 4100/9300 |
| | 84 | 2018 年 12 月 18 日 | FMC/FMCv<br>ASA FirePOWER | — |
| | 83 | 2019 年 6 月 27 日 | — | FMC 1600、2600、4600 |
| | | 2018 年 12 月 3 日 | Firepower 4100/9300 を除くすべての FTD デバイス<br>Firepower 7000/8000<br>NGIPSv | FMC 750、1000、1500、2000、2500、3500、4000、4500<br>FMCv<br>Firepower 4100/9300 を除くすべてのデバイス |

表 *46 :* バージョン *6.2.3* の日付

| バージョン | ビルド | 日付 | プラットフォーム：アップグレード | プラットフォーム：再イメージ化 |
|---|---|---|---|---|
| 6.2.3.18 | 50 | 2022 年 02 月 16 日 | すべて | — |
| 6.2.3.17 | 30 | 2021 年 6 月 21 日 | すべて | — |
| 6.2.3.16 | 59 | 2020 年 7 月 13 日 | すべて | — |
| 6.2.3.15 | 39 | 2020 年 2 月 5 日 | FTD/FTDv | — |
| | 38 | 2019 年 9 月 18 日 | FMC/FMCv<br>Firepower 7000/8000<br>ASA FirePOWER<br>NGIPSv | — |
| 6.2.3.14 | 41 | 2019 年 7 月 3 日 | すべて | — |
| | 36 | 2019 年 6 月 12 日 | すべて | — |
| 6.2.3.13 | 53 | 2019 年 5 月 16 日 | すべて | — |
| 6.2.3.12 | 80 | 2019 年 4 月 17 日 | すべて | — |
| 6.2.3.11 | 55 | 2019 年 3 月 17 日 | すべて | — |
| | 53 | 2019 年 3 月 13 日 | — | — |
| 6.2.3.10 | 59 | 2019 年 2 月 7 日 | すべて | — |
| 6.2.3.9 | 54 | 2019 年 1 月 10 日 | すべて | — |
| 6.2.3.8 | 51 | 2019 年 1 月 2 日 | 利用できなくなりました。 | — |

| バージョン | ビルド | 日付 | プラットフォーム：アップグレード | プラットフォーム：再イメージ化 |
|---|---|---|---|---|
| 6.2.3.7 | 51 | 2018 年 11 月 15 日 | すべて | — |
| 6.2.3.6 | 37 | 2018 年 10 月 10 日 | すべて | — |
| 6.2.3.5 | 53 | 2018 年 11 月 6 日 | FTD/FTDv | — |
| | 52 | 2018 年 12 月 9 日 | FMC/FMCv<br>Firepower 7000/8000<br>ASA FirePOWER<br>NGIPSv | — |
| 6.2.3.4 | 54 | 2018 年 8 月 13 日 | すべて | — |
| 6.2.3.3 | 76 | 2018 年 7 月 11 日 | すべて | — |
| 6.2.3.2 | 46 | 2018 年 6 月 27 日 | すべて | — |
| | 54 | 2018 年 6 月 6 日 | — | — |
| 6.2.3.1 | 47 | 2018 年 6 月 28 日 | すべて | — |
| | 45 | 2018 年 6 月 21 日 | — | — |
| | 43 | 2018 年 5 月 2 日 | — | — |

| バージョン | ビルド | 日付 | プラットフォーム：アップグレード | プラットフォーム：再イメージ化 |
|---|---|---|---|---|
| 6.2.3 | 113 | 2020 年 6 月 1 日 | FMC/FMCv | FMC/FMCv |
| | 111 | 2019 年 11 月 25 日 | — | FTDv: AWS, Azure |
| | 110 | 2019 年 6 月 14 日 | — | — |
| | 99 | 2018 年 9 月 7 日 | — | — |
| | 96 | 2018 年 7 月 26 日 | — | — |
| | 92 | 2018 年 7 月 5 日 | — | — |
| | 88 | 2018 年 6 月 11 | — | — |
| | 85 | 2018 年 4 月 9 日 | — | — |
| | 84 | 2018 年 4 月 9 日 | Firepower 7000/8000 シリーズ<br>NGIPSv | — |
| | 83 | 2018 年 4 月 2 日 | FTD/FTDv<br>ASA FirePOWER | FTD：物理プラットフォーム<br>FTDv：VMware、FVM<br>Firepower 7000/8000<br>ASA FirePOWER<br>NGIPSv |
| | 79 | 2018 年 3 月 29 日 | — | — |

表 *47* : バージョン *6.2.2* の日付

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.2.2.5 | 57 | 2018 年 11 月 27 日 | すべて |

| バージョン | ビルド | 日付 | プラットフォーム |
|---|---|---|---|
| 6.2.2.4 | 43 | 2018 年 9 月 21 日 | FTD/FTDv |
| | 34 | 2018 年 7 月 9 日 | FMC/FMCv<br>Firepower 7000/8000<br>ASA FirePOWER<br>NGIPSv |
| | 32 | 2018 年 6 月 15 日 | — |
| 6.2.2.3 | 69 | 2018 年 6 月 19 日 | すべて |
| | 66 | 2018 年 4 月 24 日 | — |
| 6.2.2.2 | 109 | 2018 年 2 月 28 日 | すべて |
| 6.2.2.1 | 80 | 2017 年 12 月 5 日 | Firepower 2100 シリーズ |
| | 78 | 2017 年 11 月 20 日 | — |
| | 73 | 2017 年 11 月 6 日 | FMC/FMCv<br>Firepower 2100 シリーズを除くすべてのデバイス |
| 6.2.2 | 81 | 2017 年 9 月 5 日 | すべて |

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。