# 特長と機能

このドキュメントでは、Version7.0 の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。

重要 新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。



# 新機能

## FMC バージョン 7.0 の新機能

新しい FMC で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。新しいトラフィック処理機能では、FMC とデバイスの両方で最新のリリースが前提条件となります。 デバイスが明らかに関与していない機能（Web インターフェイスの外観の変更、クラウド統合）では、FMC の最新バージョンのみを必須条件としているにもかかわらず、それ

が保証されない場合があります。新機能の説明では、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

表 *1 : FMC* バージョン *7.0.3* の新機能

| 機能 | 説明 |
| --- | --- |
| クラウド提供型の管理センターの FTD サポート | |

| 機能 | 説明 |
| --- | --- |
| | バージョン 7.0.3 FTD デバイスは、2022 年春に導入されたクラウド提供型の管理センターによる管理をサポートします。このクラウド提供型の管理センターは、Cisco Defense Orchestrator（CDO）プラットフォームを使用して、複数の Cisco セキュリティソリューションの管理を統合します。機能の更新はシスコが行います。<br><br>次の場合は、クラウド提供型の管理センターでバージョン 7.0.3 FTD を使用する必要があります。<br><br>• 現在、お客様が導入したハードウェアまたは仮想 FMC を使用しています。<br><br>• 今すぐクラウド提供型の管理センターに移行したいと考えている。<br><br>• デバイスをバージョン 7.2 以降にアップグレードする必要はありません。バージョン 7.2 以降は、クラウド提供型の管理センターによる管理もサポートしています。<br><br>この状況に当てはまる場合は、次のことを実行してください。<br><br>**1.** 現在の FMC をバージョン 7.2 以降にアップグレードします。<br><br>技術的にはバージョン 7.0.3 または 7.1 FMC を使用して FTD をバージョン 7.0.3 にアップグレードできますが、デバイスをクラウド提供型の管理センターに簡単に移行することも、イベントのログ記録と分析の目的でのみ（「分析専用」）、お客様が導入した管理センターにデバイスを登録したままにすることもできません。<br><br>**2.** アップグレードされた FMC を使用して、デバイスをバージョン 7.0.3 にアップグレードします。<br><br>**3.** デバイスでクラウド管理を有効にします。<br><br>バージョン 7.0.x デバイスの場合のみ、デバイスの CLI から **configure manager-cdo enable** を実行してクラウド管理を有効にする必要があります。**show manager-cdo** コマンドは、クラウド管理が有効になっているかどうかを表示します。<br><br>**4.** CDO の [FTDをクラウドに移行する（Migrate FTD to cloud）] ウィザードを使用して、クラウド提供型の管理センターにデバイスを移行します。<br><br>必要に応じて、お客様が導入した管理センターにデバイスを分析専用デバイスとして登録したままにします。あるいは、シスコのセキュリティ分析とロギング（SaaS） を使用して、Cisco Cloud にセキュリティイベントを送信できます。 |

| 機能 | 説明 |
| --- | --- |
| | クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン7.2以降に直接アップグレードすることをお勧めします。<br><br>新規/変更された CLI コマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers**<br><br>詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center による Firewall Threat Defense の管理を参照してください。 |

表 *2 : FMC* バージョン *7.0.2* の新機能

| 機能 | 説明 |
| --- | --- |
| ダイナミックオブジェクト名でダッシュ文字を使用できるようになりました。 | ダイナミックオブジェクト名でダッシュ文字を使用できるようになりました。これは、ACI エンドポイント更新アプリ（ダッシュ文字が許可されている）を使用して、テナントのエンドポイントグループを表すダイナミックオブジェクトをFMC で作成する場合に特に便利です。<br><br>（注） この機能を使用するには、FMC とデバイスの両方にバージョン 7.0.2 が必要です。 |

| 機能 | 説明 |
| --- | --- |
| SecureX との統合、SecureX とのオーケストレーションの改善 | SecureX との統合プロセスが合理化されました。すでに SecureX アカウントを持っている場合は、新しい [統合（Integration）] > [SecureX] ページで該当するクラウドリージョンを選択し、[SecureX の有効化（Enable SecureX）] をクリックして、SecureX に対して認証するだけです。イベントをクラウドに送信するオプション、および Cisco Success Network と Cisco Support Diagnostics を有効にするオプションも、この新しいページに移動されました。<br><br>この新しいページで SecureX との統合を有効にすると、システムのクラウド接続のライセンス管理が Cisco Smart Licensing から SecureX に切り替わります。SecureX を「従来の」方法ですでに有効にしている場合、このクラウド接続管理による利点を得るには、無効にしてから再度有効にする必要があります。<br><br>Web インターフェースで示されていない場合でも、このページでは対象のクラウドリージョンや、シスコのセキュリティ分析とロギング（SaaS）を使用して Secure Network Analytics（Stealthwatch）クラウドに送信するイベントタイプも管理することを覚えておいてください。以前のバージョンでは、このオプションは、**システム**（⚙）> [統合（Integration）] > [クラウドサービス（Cloud Services）] にありました。SecureX を有効にしても、Secure Network Analytics クラウドとの通信には影響しません。両方にイベントを送信できます。<br><br>FMC は SecureX オーケストレーションもサポートするようになりました。これは、セキュリティツール全体のワークフローを自動化するために使用できる強力なドラッグアンドドロップ インターフェイスです。SecureX を有効にすると、オーケストレーションを有効にできます。<br><br>（注） これらの変更はバージョン 7.1 で一時的に廃止されましたが、バージョン 7.2 で復活しました。新しい方法で SecureX との統合を有効にした場合は、バージョン 7.1.x にアップグレードする前に、この機能を無効にする必要があります。アップグレードが正常に完了したら、この機能を再度有効にできます。バージョン 7.2 以降へのアップグレードは影響を受けません。 |

| 機能 | 説明 |
| --- | --- |
| Web インターフェイスの変更：SecureX、脅威インテリジェンス、およびその他の統合。 | |

| 機能 | 説明 |
| --- | --- |
| | 以下の FMC メニューオプションが変更されました。<br>（注） これらの変更はバージョン 7.1 で一時的に廃止されましたが、バージョン 7.2 で復活しました。<br>[AMP] > [AMP管理（AMP Management）] は次に変更されました。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）]<br>[AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]<br>[インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）]<br>[インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）]<br>[インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）]<br>[インテリジェンス（Intelligence）] > [インシデント（Incidents）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）] |

| 機能 | 説明 | | |
|---|---|---|---|
| | **システム**（⚙） > [統合（Integration）] | は次に変更されました。 | [統合（Integration）] > [その他の統合（Other Integrations）] |
| | **システム**（⚙） > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics and Logging）] | は次に変更されました。 | [統合（Integration）] > [セキュリティ分析とロギング（Security Analytics and Logging）] |
| | **システム**（⚙） > [SecureX] | は次に変更されました。 | [統合（Integration）] > [SecureX] |

表 *3 : FMC* バージョン *7.0.1* の新機能

| 機能 | 説明 |
|---|---|
| Snort 3 の rate_filter インスペクタ。 | Snort 3 rate_filter インスペクタが導入されました。<br>これにより、ルールに対する過剰な一致に対応して侵入ルールのアクションを変更できます。レートベースの攻撃を特定の期間ブロックし、イベントの生成中でも一致するトラフィックを許可するように戻すことができます。詳細については、『Snort 3 Inspector Reference』を参照してください。<br>（注） この機能を使用するには、FMC とデバイスの両方にバージョン 7.0.1 以降が必要です。また、lsp-rel-20210816-1910 以降を実行している必要があります。**[システム（System）] > [アップデート（Updates）] > [ルールアップデート（Rule Updates）]** で LSP を確認および更新できます。<br>新規/変更されたページ：カスタムネットワーク分析ポリシーの Snort 3 バージョンを編集して、インスペクタを設定します。<br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| ASA FirePOWER サービスを使用する ISA 3000 の新しいデフォルトパスワード | 新しいデバイスの場合、admin アカウントのデフォルトパスワードは Adm!n123 になりました。以前は、デフォルトの admin パスワードは Admin123 でした。<br>バージョン 7.0.1 以降にアップグレードまたは再イメージ化しても、パスワードは変更されません。ただし、すべてのユーザアカウント（特に管理者アクセス権を持つユーザアカウント）に強力なパスワードを設定することを推奨します。<br>サポートされるプラットフォーム：ASA FirePOWER サービスを使用する ISA 3000 |

**表 *4 : FMC* 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 | 説明 |
| --- | --- |
| FTDvパフォーマンス階層型のスマートライセンス。 | **アップグレードの影響。**<br>FTDv 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 ソフトウェア ライセンスをサポートするようになりました。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。<br>新しいデバイスを追加する前に、お使いのアカウントに必要なライセンスが含まれていることを確認してください。追加のライセンスを購入するには、シスコの担当者またはパートナーの担当者にお問い合わせください。<br>FTDv をバージョン 7.0 にアップグレードすると、デバイスが自動的に FTDv50 階層に割り当てられます。レガシー（非階層型）ライセンスを引き続き使用するには、アップグレード後に階層を [変数（Variable）] に変更します。<br>サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当するスタートアップガイドを参照してください。<br>新規/変更されたページ：<br>• [デバイス（Device）] > [デバイス管理（Device Management）] ページで FTDv デバイスを追加または編集するときに、パフォーマンス階層を指定できるようになりました。<br>• [システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] ページでパフォーマンス階層を一括編集できます。 |
| **高可用性/拡張性** | |

| 機能 | 説明 |
| --- | --- |
| クラスタリング用の PAT ポートブロック割り当ての改善 | PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するには、FlexConfig を使用して **cluster-member-limit** コマンドを実行して、予定しているクラスタ内の最大ノード数を設定します。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは16ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。<br><br>新規/変更されたコマンド：**cluster-member-limit**（FlexConfig）、**show nat pool cluster [summary]**、**show nat pool ip detail**<br><br>サポートされるプラットフォーム：Firepower 4100/9300 |
| FTD CLI **show cluster history** の改善。 | 新しいキーワードを指定すると、**show cluster history** コマンドの出力をカスタマイズできます。<br><br>新規/変更されたコマンド：**show cluster history** [**brief**] [**latest**] [**reverse**] [**time**]<br><br>サポートされるプラットフォーム：Firepower 4100/9300 |
| クラスタから永久に削除するための FTD CLI コマンド。 | FTD CLI を使用して、ユニットをクラスタから完全に削除し、その設定をスタンドアロンデバイスに変換できるようになりました。<br><br>新規/変更されたコマンド： **cluster reset-interface-mode**<br><br>サポートされるプラットフォーム：Firepower 4100/9300 |
| **NAT** | |
| 優先順位付けされたシステム定義の NAT ルール。 | 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。<br><br>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。<br><br>サポートされるプラットフォーム：FTD |
| 仮想ルーティング | |

| 機能 | 説明 |
| --- | --- |
| ISA 3000 の仮想ルータサポート。 | ISA 3000 デバイスには最大 10 台の仮想ルータを設定できるようになりました。<br>サポートされるプラットフォーム：ISA 3000 |
| **サイト間 VPN** | |
| ルートベースのサイト間 VPN 向けバックアップ用仮想トンネルインターフェイス（VTI）。 | 仮想トンネルインターフェイスを使用するサイト間 VPN を設定する場合、トンネルのバックアップ VTI を選択できます。<br>バックアップ VTI を指定すると復元力が得られるため、プライマリ接続がダウンした場合でもバックアップ接続は継続して機能します。たとえば、プライマリ VTI をあるサービスプロバイダーのエンドポイントに接続し、バックアップ VTI を別のサービスプロバイダーのエンドポイントに接続できます。<br>新規/変更されたページ：ポイントツーポイント接続の VPN タイプとして [ルートベース（Route-Based）] を選択した場合に、サイト間 VPN ウィザードにバックアップ VTI を追加する機能が追加されました。<br>サポートされるプラットフォーム：FTD |
| **Remote Access VPN** | |
| ロード バランシング。 | RA VPN ロードバランシングがサポートされるようになりました。システムは、セッション数によってグループ化されたデバイス間でセッションを分散します。トラフィック量やその他の要因は考慮されません。<br>新規/変更された画面：RA VPN ポリシーの [詳細設定（Advanced Settings）] にロード バランシング オプションが追加されました。<br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| ローカル認証。 | RA VPN ユーザーのローカル認証がサポートされるようになりました。これは、プライマリまたはセカンダリ認証方式として、または設定されたリモートサーバーに到達できない場合のフォールバックとして使用できます。<br>**1.** ローカルレルムを作成します。<br>ローカルユーザー名とパスワードは、ローカルレルムに保存されます。レルムを作成し（**[システム（System）] > [統合（Integration）] > [レルム（Realms）]**）、新しい **[ローカル（LOCAL）]** レルムタイプを選択すると、1つ以上のローカルユーザーを追加するように求められます。<br>**2.** ローカル認証を使用するように RA VPN を設定します。<br>RA VPN ポリシーを作成または編集し（**[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]**）、そのポリシー内に接続プロファイルを作成して、その接続プロファイルでプライマリ、セカンダリ、またはフォールバック認証サーバーとして **[ローカル（LOCAL）]** を指定します。<br>**3.** 作成したローカルレルムを RA VPN ポリシーに関連付けます。<br>RA VPN ポリシーエディタで、新しい **[ローカルレルム（Local Realm）]** 設定を使用します。ローカル認証を使用する RA VPN ポリシーのすべての接続プロファイルは、ここで指定したローカルレルムを使用します。<br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| ダイナミック アクセス ポリシー。 | 新しいダイナミック アクセス ポリシーを使用すると、変化する環境に自動的に適応するリモートアクセス VPN 認証を設定できます。<br>**1.** AnyConnect HostScan パッケージを AnyConnect ファイルとしてアップロードして、HostScan を設定します（**[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[VPN]>[AnyConnect ファイル（AnyConnect File）]**）。**[ファイルタイプ（File Type）]** ドロップダウンリストに新しい **[HostScan パッケージ（HostScan Package）]** オプションがあります。<br>このモジュールはエンドポイントで実行され、ダイナミック アクセス ポリシーが使用するポスチャアセスメントを実行します。<br>**2.** ダイナミック アクセス ポリシーを作成します（**[デバイス（Devices）] [ダイナミック アクセス ポリシー（Dynamic Access Policy）]**）。<br>ダイナミック アクセス ポリシーは、ユーザーがセッションを開始するたびに評価するセッション属性（グループメンバーシップやエンドポイントセキュリティなど）を指定します。その後、その評価に基づいてアクセスを拒否または許可できます。<br>**3.** 作成したダイナミック アクセス ポリシーを RA VPN ポリシーに関連付けます。<br>リモートアクセス VPN ポリシーエディタで、新しい **[ダイナミック アクセス ポリシー（Dynamic Access Policy）]**設定を使用します。<br>サポートされるプラットフォーム：FTD |
| マルチ証明書認証。 | リモートアクセス VPN ユーザのマルチ証明書認証をサポートするようになりました。SSL または IKEv2 EAP フェーズで AnyConnect クライアントを使用して VPN アクセスを許可するためにユーザの ID 証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。<br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| AnyConnect カスタム属性。 | AnyConnect カスタム属性をサポートし、AnyConnect クライアント機能を設定するためのインフラストラクチャを、これらの機能の明示的なサポートをシステムに追加することなく、提供するようになりました。<br>サポートされるプラットフォーム：FTD |
| **アクセス制御** | |

| 機能 | 説明 |
| --- | --- |
| FTD 用 Snort 3。 | |

| 機能 | 説明 |
| --- | --- |
| | 新規に FTD を展開する場合、Snort 3 がデフォルトの検査エンジンになります。アップグレードされた展開では引き続き Snort 2 が使用されますが、いつでも切り替えることができます。<br><br>Snort 3 を使用する利点は次のとおりですが、これに限定されません。<br><br>• パフォーマンスの向上。<br>• SMBv2 インスペクションの改善。<br>• 新しいスクリプト検出機能。<br>• HTTP/2 インスペクション。<br>• カスタムルールグループ。<br>• カスタム侵入ルールを記述しやすくする構文。<br>• 侵入イベント内の「would have dropped」インライン結果の理由。<br>• VDB、SSL ポリシー、カスタム アプリケーション ディテクタ、キャプティブポータル ID ソース、および TLS サーバ ID 検出へ変更を展開するときに Snort が再起動しない。<br>• Cisco Success Network に送信される Snort 3 固有のテレメトリデータ、およびトラブルシューティングログの改善による、有用性の向上。<br><br>Snort 3 侵入ルールの更新は、SRU ではなく LSP（Lightweight Security Package）と呼ばれます。Snort 2 には引き続き SRU が使用されます。シスコからのダウンロードには、最新の LSP と SRU の両方が含まれており、設定に適したルールセットが自動的に使用されます。<br><br>FMC は、Snort 2 と Snort 3 の両方のデバイスでの展開を管理でき、各デバイスに正しいポリシーを適用します。ただし、Snort 2 とは異なり、FMC のみをアップグレードしてから展開することで、デバイス上の Snort 3 を更新することはできません。Snort 3 では、新しい機能と解決済みのバグにより、FMC 上のソフトウェアとその管理対象デバイスをアップグレードする必要があります。各ソフトウェアバージョンに含まれている Snort の詳細については、Cisco Firepower Compatibility Guide のバンドルされたコンポーネントのセクションを参照してください。<br><br>**重要** Snort 3 に切り替える前に、Firepower Management Center Snort 3 Configuration Guide を読んで理解することを強く推奨します。機能の制限と移行手順には特に注意してく |

| 機能 | 説明 |
| --- | --- |
| | ださい。Snort 3 へのアップグレードは影響を最小限に抑えるように設計されていますが、機能は正確にマッピングされません。慎重に計画して準備することで、トラフィックが期待どおりに処理されるようにできます。<br><br>Snort 3 の Webサイト（https://snort.org/snort3）にもアクセスできます。 https://snort.org/snort3<br><br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| ダイナミックオブジェクト。 | ダイナミックオブジェクトは、アクセスコントロールルールで使用できます。<br><br>ダイナミックオブジェクトは、単に IP アドレスまたはサブネットのリストです（範囲なし、FQDN なし）。ただし、ネットワークオブジェクトとは異なり、ダイナミックオブジェクトへの変更はすぐに有効になり、再展開する必要はありません。これは、IP アドレスがワークロードリソースに動的にマッピングされる仮想環境やクラウド環境で役立ちます。<br><br>ダイナミックオブジェクトを作成および管理するには、Cisco Secure 動的属性コネクタを使用することをお勧めします。コネクタは、ワークロードの変更に基づいてファイアウォールポリシーを迅速かつシームレスに更新する別個の軽量アプリケーションです。そのためには、環境内のタグ付きリソースからワークロード属性を取得し、指定した基準に基づいて IP リストをコンパイルします（「動的属性フィルタ」）。次に、FMC でダイナミックオブジェクトを作成し、IP リストを入力します。ワークロードが変更されると、コネクタによってダイナミックオブジェクトが更新され、新しいマッピングに基づいてすぐにトラフィックの処理が開始されます。詳細については、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイドを参照してください。<br><br>作成したダイナミックオブジェクトは、アクセス コントロール ルール エディタの新しい [動的属性（Dynamic Attributes）] タブでアクセスコントロールルールに追加できます。このタブは、フォーカスの狭い [SGT/ISE 属性（SGT/ISE Attributes）] タブに代わるものです。ここで、SGT 属性を使用したルールの設定を続行します。<br><br>（注） FMC でダイナミックオブジェクトを作成することもできます（**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [外部属性（External Attributes）] > [ダイナミックオブジェクト（Dynamic Objects）]**）。ただし、この場合はコンテナのみ作成されます。その後、REST API を使用してデータを入力して管理する必要があります。Firepower Management Center REST API バージョン 7.0 クイックスタートガイド [英語] を参照してください。<br><br>サポート対象プラットフォーム：FMC<br><br>Cisco Secure Dynamic Attributes Connector の統合でサポートされる仮想/クラウドワークロード：Microsoft Azure、AWS、VMware |

| 機能 | 説明 |
| --- | --- |
| Active Directory ドメインのクロスドメイン信頼。 | Microsoft Active Directory フォレスト（相互に信頼する AD ドメインのグループ）のユーザーを使用してユーザー アイデンティティ ルールを設定できるようになりました。<br>新規/変更されたページ：<br>• レルムとディレクトリを同時に設定するようになりました。<br>• 新しい [同期結果（Sync Results）] ページ（[システム（System）] > [統合（Integration）] > [レルム（Realms）] > [同期結果（Sync Results）]）に、クロスドメイン信頼関係のユーザーおよびグループのダウンロードに関連するエラーが表示されます。<br>サポート対象プラットフォーム：FMC |
| DNS フィルタリング。 | バージョン 6.7 でベータ機能として導入された DNS フィルタリングは、完全にサポートされるようになり、新しいアクセス コントロール ポリシーではデフォルトで有効になっています。<br>サポートされるプラットフォーム：すべて |
| **イベントロギングおよび分析** | |

| 機能 | 説明 |
| --- | --- |
| Secure Network Analytics オンプレミス展開でのイベント保存プロセスの改善。 | 新しいシスコのセキュリティ分析とロギング（オンプレミス）アプリと新しいFMCウィザードにより、オンプレミスSecure Network Analyticsソリューションのリモートデータストレージをより簡単に設定できます。<br>**1.** ハードウェアまたは仮想Stealthwatchアプライアンスを展開します。<br>Stealthwatch Management Consoleを単独で使用することも、Stealthwatch Management Console、フローコレクタ、およびデータストアを設定することもできます。<br>**2.** Stealthwatch Management Consoleに新しいCisco Security Analytics and Logging（オンプレミス）アプリをインストールして、Stealthwatchをリモートデータストアとして設定することができます。<br>**3.** FMCで、**[システム（System）]>[ロギング（Logging）]>[セキュリティ分析とロギング（Security Analytics & Logging）]**ページの新しいウィザードのいずれかを使用して、Stealthwatch展開に接続します。<br>Stealthwatchのコンテキストクロス起動を設定するために使用したフォーカスの狭いページは、ウィザードによって置き換えられます。現在、これはウィザードのステップの1つです。<br>syslogを使用してFirepowerイベントをStealthwatchに送信するアップグレードされた展開では、ウィザードを使用する前にこれらの設定を無効にします。そうしないと、二重にイベントが発生します。Stealthwatchへのsyslog接続を削除するには、FTDプラットフォーム設定を使用します（[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]）。syslogへのイベント送信を無効にするには、アクセス制御ルールを編集します。<br>Stealthwatchのハードウェア要件およびソフトウェア要件を含む詳細については、オンプレミスにおけるシスコのセキュリティ分析とロギング：Firepowerイベント統合ガイドを参照してください。<br>サポート対象プラットフォーム：FMC |

| 機能 | 説明 |
| --- | --- |
| Secure Network Analytics オンプレミス展開でリモートに保存されたイベントを操作する。 | FMC を使用して、Secure Network Analytics オンプレミス展開でリモートに保存された接続イベントを操作できるようになりました。<br><br>接続イベントページ（[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]）と統合イベントビューア（[分析（Analysis）] > [統合イベント（Unified Events）]）の新しいデータソースオプションを使用して、処理する接続イベントを選択できます。デフォルトでは、時間範囲に何も存在しない場合、ローカルに保存された接続イベントが表示されます。その場合、システムはリモートに保存されたイベントを表示します。<br><br>また、リモートで保存された接続イベントに基づいてレポートを生成できるように、レポートテンプレートにデータソースオプションが追加されました（[概要（Overview）]>[レポート（Reporting）] > [レポートテンプレート（Report Templates）]）。<br><br>（注） この機能は、接続イベントでのみサポートされます。クロス起動は、リモートで保存されたセキュリティインテリジェンス、侵入、ファイル、およびマルウェアのイベントを調べる唯一の方法です。統合イベントビューアでも、システムはこれらのタイプのローカルに保存されたイベントのみを表示します。<br><br>ただし、すべてのセキュリティ インテリジェンス イベントに同一の接続イベントが存在することに注意してください。これらは「IP ブロック」や「DNS ブロック」などの理由を持つイベントです。これらの重複イベントは、接続イベントページまたは統合イベントビューアで処理できますが、専用のセキュリティインテリジェンス イベント ページでは処理できません。<br><br>サポートされるプラットフォーム：FMC。 |

| 機能 | 説明 |
| --- | --- |
| すべての接続イベントを Secure Network Analytics クラウドに保存する。 | Cisco Security Analytics and Logging（SaaS）を使用して、すべての接続イベントを Stealthwatch クラウドに保存できるようになりました。以前は、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアのイベント、およびそれらに関連する接続イベントに限定されていました。<br><br>クラウドに送信するイベントを変更するには、[システム（System）] > [統合（Integration）] を選択します。[クラウドサービス（Cloud Services）] タブで、[シスコクラウドイベントの設定（Cisco Cloud Event Configuration）] を編集します。優先順位の高い接続イベントをクラウドに送信する古いオプションは、[すべて（All）]、[なし（None）]、または [セキュリティイベント（Security Events）] の選択肢に置き換えられました。<br><br>（注） これらの設定は、SecureX に送信するイベントも制御します。ただし、すべての接続イベントをクラウドに送信するように選択した場合でも、SecureX はセキュリティ（優先度の高い）接続イベントのみを消費します。また、[分析（Analysis）] > [SecureX] で SecureX 接続自体を設定することにも注意してください。<br><br>サポート対象プラットフォーム：FMC |
| 統合イベントビューア。 | 統合イベントビューア（**[分析（Analysis）] > [統合イベント（Unified Events）]**）では、1 つのテーブルで接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアの各イベントが表示されます。これは、異なるタイプのイベント間の関係を調べるのに役立ちます。<br><br>単一の検索フィールドを使用すると、複数の条件に基づいてビューを動的にフィルタリングできます。また、[本番稼働（Go Live）] オプションでは、管理対象デバイスから受信したイベントがリアルタイムで表示されます。<br><br>サポート対象プラットフォーム：FMC |

| 機能 | 説明 |
| --- | --- |
| SecureX のリボン。 | FMC 上の SecureX のリボンは SecureX にピボットされ、シスコのセキュリティ製品全体の脅威の状況を即座に確認できます。<br><br>SecureX に接続してリボンを有効にするには、[分析（Analysis）] > [SecureX] を使用します。クラウドリージョンを選択し、SecureX に送信するイベントを指定するには、引き続き [システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] を使用する必要があります。<br><br>詳細については、Cisco Secure Firewall Threat Defense および SecureX 統合ガイドを参照してください。<br><br>サポート対象プラットフォーム：FMC |
| ローカルストレージをオフにすると、すべての接続イベントのレート制限が免除されます。 | イベントレート制限は、FMC に送信されるすべてのイベントに適用されます。ただし、セキュリティイベント（セキュリティ インテリジェンス、侵入、ファイル、マルウェアのイベント、およびそれらに関連する接続イベント）は例外です。<br><br>ローカル接続イベントストレージを無効にすると、セキュリティイベントだけでなく、すべての接続イベントがレート制限から除外されるようになりました。これを行うには、[システム（System）] > [設定（Configuration）] > [データベース（Database）] ページで [最大接続イベント数（Maximum Connection Events）] を 0 に設定します。<br><br>（注） [最大接続イベント数（Maximum Connection Events）] は、0 に設定してオフにすること以外では、接続イベントのレート制限を制御しません。このフィールドに 0 以外の数値を指定すると、優先順位の低い接続イベントがすべてレート制限されます。<br><br>ローカルイベントストレージを無効にしても、リモートイベントストレージには影響せず、接続の概要や相関にも影響しないことに注意してください。システムは、引き続き、トラフィックプロファイル、相関ポリシー、ダッシュボード表示などの機能に接続イベント情報を使用します。<br><br>サポート対象プラットフォーム：FMC |

| 機能 | 説明 |
| --- | --- |
| ファイルおよびマルウェアイベントテーブルに一緒に表示されるポートとプロトコル。 | ファイルおよびマルウェアイベントテーブルでは、[ポート（Port）] フィールドにプロトコルが表示されるようになり、[ポート（Port）] フィールドでプロトコルを検索できます。アップグレード前に存在したイベントの場合、プロトコルが不明な場合は「TCP」が使用されます。<br>新規/変更されたページ：<br>• **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]**<br>• **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]**<br>サポートされるプラットフォーム：FMC |
| **のアップグレード** | |
| FTD のアップグレードパフォーマンスとステータスレポートの改善。 | FTD のアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい **[アップグレード（Upgrades）]** タブでは、アップグレードステータスとエラーレポートがさらに強化されています。<br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| FTD の [アップグレード（Upgrade）] ウィザード。 | |

| 機能 | 説明 |
| --- | --- |
| | FMC の新しいデバイス アップグレード ページ（[デバイス（Devices）] > [アップグレード（Upgrade）]）には、バージョン 6.4 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。<br><br>開始するには、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [アクションの選択（Select Action）]）で新しい [Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）] アクションを使用します。<br><br>続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。<br><br>ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。<br><br>（注） FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き [システム更新（System Updates）] ページ（**[システム（System）] > [更新（Updates）]**）を使用する必要があります。また、[システム更新（System Updates）] ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。<br><br>（注） バージョン 7.0 では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは 1 つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1 つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1 つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1 つユニットでアップグレードを開始すると、すべてのユニットで開始されます。 |

| 機能 | 説明 |
| --- | --- |
| | 時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。<br><br>サポートされるプラットフォーム：FTD |
| 多くの FTD デバイスを一度にアップグレードします。 | FTD アップグレードウィザードでは、次の制限が解除されます。<br>• デバイスの同時アップグレード。<br>一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。<br>**重要** この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古い FTD リリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。<br>• デバイスモデルによるアップグレードのグループ化。<br>システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。<br>以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズ デバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。<br><br>サポートされるプラットフォーム：FTD |
| **管理とトラブルシューティング** | |
| SD カードを使用した ISA 3000 でのゼロタッチ復元。 | ローカルバックアップを実行すると、バックアップファイルが SD カードにコピーされます（カードがある場合）。交換用デバイスの設定を復元するには、新しいデバイスに SD カードを取り付け、デバイスの起動中に [リセット（Reset）] ボタンを 3 ー 15 秒間押します。<br><br>サポートされるプラットフォーム：ISA 3000 |

| 機能 | 説明 |
| --- | --- |
| RA およびサイト間 VPN ポリシーを選択的に展開する。 | バージョン 6.6 で導入された選択的ポリシーの展開では、リモートアクセスとサイト間VPNポリシーがサポートされるようになりました。<br>新規/変更されたページ：[展開（Deploy）]>[展開（Deployment）] ページに VPN ポリシーオプションが追加されました。<br>サポートされるプラットフォーム：FTD |

| 機能 | 説明 |
| --- | --- |
| 新しいヘルス モジュール。 | 次の正常性モジュールが追加されました。<br>• AMP 接続ステータス<br>• AMP Threat Grid のステータス<br>• ASP ドロップ<br>• 高度な Snort 統計情報<br>• シャーシステータス FTD<br>• イベント ストリーム ステータス<br>• FMC アクセス設定の変更<br>• FMC HA ステータス（古い HA ステータスの交換）<br>• FTD HA ステータス<br>• ファイルシステムの整合性チェック<br>• フロー オフロード<br>• ヒット カウント（Hit Count）<br>• MySQL ステータス<br>• NTP ステータス FTD<br>• Rabbit MQ ステータス<br>• ルーティング統計情報<br>• SSE 接続ステータス<br>• Sybase ステータス<br>• 未解決グループモニター<br>• VPN 統計情報<br>• xTLS カウンタ<br>さらに、バージョン 6.6.3 で [アプライアンス設定のリソース使用率（Appliance Configuration Resource Utilization）] モジュールとして導入された [構成メモリ割り当て（Configuration Memory Allocation）] モジュールは、バージョン 6.7 では完全にはサポートされていませんでしたが、完全にサポートされます。<br>サポートされるプラットフォーム：FMC |
| **セキュリティと強化** | |

| 機能 | 説明 |
| --- | --- |
| AWS 導入用の新しいデフォルトパスワード。 | 初期展開時にユーザーデータ（ [高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]）を使用してデフォルトパスワードを定義していなければ、adminアカウントのデフォルトパスワードは AWS のインスタンス ID です。<br>以前は、デフォルトの admin パスワードは Admin123 でした。<br>サポートされているプラットフォーム：FMCv for AWS、FTDv for AWS |
| 証明書の登録用の EST。 | 証明書の登録用の Enrollment over Secure Transport のサポートが提供されました。<br>新規/変更されたページ：[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [CA情報（CA Information）] タブ設定時の新しい登録オプション。<br>サポート対象プラットフォーム：FMC |
| EdDSA 証明書タイプのサポート。 | 新しい証明書キータイプ：EdDSA（キーサイズ 256）が追加されました。<br>新規/変更されたページ：[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [キー（Key）] タブの設定時の新しい証明書キーオプション。<br>サポート対象プラットフォーム：FMC |
| NTP サーバーの AES-128 CMAC 認証。 | AES-128 CMAC キーを使用して、FMC と NTP サーバー間の接続を保護できるようになりました。<br>新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]**。<br>サポートされるプラットフォーム：FMC |
| SNMPv3 ユーザーは、SHA-224 または SHA-384 認証アルゴリズムを使用して認証できます。 | SNMPv3 ユーザーは、SHA-224 または SHA-384 アルゴリズムを使用して認証できるようになりました。<br>新規/変更されたページ：[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）] > [認証アルゴリズムタイプ（Auth Algorithm Type）]<br>サポートされるプラットフォーム：FTD |
| **ユーザビリティとパフォーマンス** | |

| 機能 | 説明 |
|---|---|
| ポリシーとオブジェクトのグローバル検索。 | 特定のポリシーを名前で検索し、特定のオブジェクトを名前と設定値で検索できるようになりました。この機能は、クラシックテーマでは使用できません。<br><br>新規/変更されたページ：[展開（Deploy）] メニューの左側にある [FMC] メニューバーに [検索（Search）] アイコンとフィールドの機能が追加されました。<br><br>サポート対象プラットフォーム：FMC |
| Intel QuickAssist Technology（QAT）を使用した FTDv でのハードウェア暗号化アクセラレーション。 | VMware の FTDv および KVM の FTDv でハードウェア暗号化アクセラレーション（CBC 暗号のみ）がサポートされるようになりました。この機能を使用するには、ホスティング プラットフォームに Intel QAT 8970 PCI アダプタ/バージョン 1.7 以降のドライバが必要です。リブートすると、ハードウェア暗号化アクセラレーションが自動的に有効になります。<br><br>サポートされるプラットフォーム：VMware の FTDv、KVM の FTDv |
| 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**<br><br>サポートされるプラットフォーム：FTD |
| **FMC REST API**：新しいサービスと操作<br><br>新機能と既存の機能をサポートするために、次の FMC REST API サービス/操作が追加されました。詳細については、Firepower Management Center REST API バージョン 7.0 クイックスタートガイド [英語] を参照してください。 | |
| デバイス | alerts：GET |
| 統合 | fmchastatuses：GET<br><br>securexconfigs：GET および PUT |

| 機能 | 説明 |
| --- | --- |
| オブジェクト | anyconnectcustomattributes、anyconnectpackages、anyconnectprofiles：GET<br>anyconnectcustomattributes/overrides：GET<br>applicationfilters：PUT、POST、および DELETE<br>certificatemaps：GET<br>dnsservergroups：GET<br>dnsservergroups/overrides：GET<br>dynamicobjectmappings：POST<br>dynamicobjects：GET、PUT、POST、および DELETE<br>dynamicobjects/mappings：GET および PUT<br>geolocations：PUT、 POST、および DELETE<br>grouppolicies：GET<br>hostscanpackages：GET<br>intrusionrules、intrusionrulegroups：GET、PUT、POST、および DELETE<br>intrusionrulesupload：POST<br>ipv4addresspools、ipv6addresspools：GET<br>ipv4addresspools/overrides、ipv6addresspools/overrides：GET<br>localrealmusers：GET、PUT、POST、DELETE<br>radiusservergroups：GET<br>realms：PUT、POST、および DELETE<br>sidnsfeeds、sidnslists、sinetworkfeeds、sinetworklists：GET<br>sinkholes：GET<br>ssoservers：GET<br>ssoservers/overrides：GET<br>usage：GET |

| 機能 | 説明 |
|---|---|
| ポリシー | accesspolicies/securityintelligencepolicies：GET<br>dnspolicies：GET<br>dnspolicies/allowdnsrules、dnspolicies/blockdnsrules：GET<br>dynamicaccesspolicies：GET、PUT、POST、および DELETE<br>identitypolicies：GET<br>intrusionpolicies：PUT、POST、および DELETE<br>intrusionpolicies/intrusionrulegroups、intrusionpolicies/intrusionrules：GET および PUT<br>networkanalysispolicies：GET、PUT、POST、および DELETE<br>networkanalysispolicies/inspectorconfigs：GET<br>networkanalysispolicies/inspectoroverrideconfigs：GET および PUT<br>ravpns：GET<br>ravpns/addressassignmentsettings、ravpns/certificatemapsettings、ravpns/connectionprofiles：GET |
| 検索（Search） | globalsearch：GET |

# 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 FTDv 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、FTDv 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** | |

| 機能 | 説明 |
|---|---|
| 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。 |
| 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。FDM 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。FDM 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。 |
| FDM 管理対象システムの Snort 3 の新機能 | FDM 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（FTD 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。 |

| 機能 | 説明 |
|---|---|
| **VPN 機能** | |
| リモートアクセス VPN の FDM SSL 暗号設定 | FDM 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、FTD 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 FTD 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、FTD 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、FTD 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。FTD 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 サーバーについて | 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 | FDM 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** | |
| FTDv のパフォーマンス階層型ライセンス | FTDv 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 FTDv 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** | |
| FTD API を使用した DHCP リレー設定。 | FTD 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>FTD 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 FDM への早期ログイン | FDM 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 FDM 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** |
| FDM 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 FTD 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。 |
| FTD REST API バージョン 6.1（v6） | ソフトウェアバージョン 7.0 の FTD 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、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。 |

# 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 FMCv、FTDv、および NGIPSv 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<br>• OpenStack (FDM 管理のサポートなし) |

# 新しい侵入ルールとキーワード

アップグレードにより侵入ルールをインポートして自動的に有効化が可能です。

侵入ルールを更新（SRU/LSP）すると、新規および更新された侵入ルールとプリプロセッサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。現在のバージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、SRU/LSP を更新しても、そのルールはインポートされません。

アップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

Snort のバージョンを確認するには、互換性ガイドの「バンドルされたコンポーネント」の項を参照するか、次のコマンドのいずれかを使用します。

- FMC：**[ヘルプ（Help）]** > **[概要（About）]**を選択します。
- FDM：**show summary** CLI コマンドを使用します。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

# 廃止された機能

## FMC バージョン 7.0 で廃止された機能

表 *7 : FMC* バージョン *7.0.2* で廃止された機能

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| REST API で SecureX との統合を設定。 | なし。 | SecureX 統合の改善の一環として（FMC バージョン 7.0 の新機能 （1 ページ） を参照）、REST API を使用して SecureX との統合を設定できなくなりました。FMC の Web インターフェイスを使用する必要があります。 |

表 *8 : FMC* 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 |
|---|---|---|
| キーが 2048 ビット未満の RSA 証明書、または署名アルゴリズムで SHA-1 を使用する RSA 証明書。 | FTD デバイスを介したアップグレード後の VPN 接続を防止します。 | バージョン 7.0 では、キーが 2048 ビット未満の RSA 証明書、または署名アルゴリズムで SHA-1 を使用する RSA 証明書のサポートが削除されています。<br><br>アップグレードする前に、オブジェクトマネージャを使用し、より強力なオプションを使用して PKI 証明書の登録を更新します（[オブジェクト（Objects）]>[PKI]>[証明書の登録（Cert Enrollment）]）。更新しない場合、アップグレードしても現在の設定は保持されますが、デバイスを介した VPN 接続は失敗します。<br><br>弱いオプションを使用して古い FTD デバイス（バージョン 6.4 ー 6.7.x）のみを管理し続けるには、[デバイス（Devices）] > [証明書（Certificates）] ページで各デバイスの新しい [弱暗号化の有効化（Enable Weak-Crypto）] オプションを選択します。 |

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化（削除）。 | アップグレード後に展開ができないようにします。 | バージョン 7.0 では、FTD デバイスにおける SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化のサポートが削除されています。<br>FTD をバージョン 7.0 にアップグレードすると、FMC の設定に関係なく、該当ユーザーがデバイスから削除されます。プラットフォーム設定ポリシーでこれらのオプションを使用している場合は、FTD をアップグレードする前に構成を変更して確認してください。<br>これらのオプションは、Threat Defense プラットフォーム設定ポリシー（[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]）で SNMPv3 ユーザーを作成または編集する際の [認証アルゴリズムタイプ（Auth Algorithm Type）] および [暗号化タイプ（Encryption Type）] ドロップダウンにあります。 |
| AMP クラウドとのポート 32137 通信。 | FMC がアップグレードされないようにします。 | バージョン 7.0 では、パブリックおよびプライベート AMP クラウドからファイル配置データを取得するためにポート 32137 を使用する FMC オプションが廃止されています。プロキシを設定しない限り、FMC はポート 443/HTTPS を使用するようになりました。<br>アップグレードする前に、[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] ページで [ネットワーク用 AMP にレガシーポート 32137 を使用（Use Legacy Port 32137 for AMP for Networks）] オプションを無効にします。AMP for Networks の展開が期待どおりに機能するまで、アップグレードを続行しないでください。 |
| HA ステータス正常性モジュール。 | なし。 | バージョン 7.0 では、[HA ステータス（HA Status）] 正常性モジュールの名前が変更されています。これからは、[FMC HA ステータス（FMC HA Status）] 正常性モジュールです。これは、新しい [FTD HA ステータス（FTD HA Status）] モジュールと区別するためです。 |
| レガシー API エクスプローラ。 | なし。 | バージョン 7.0 では、FMC REST API レガシー API Explorer のサポートが削除されています。 |

| 機能 | アップグレードの影響 | 説明 |
|---|---|---|
| 地理位置情報の詳細。 | なし。これは日付ベースで廃止予定です。 | 2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。<br><br>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-*date-build*）です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IP パッケージではなく、必ず国コードパッケージを取得してください。<br><br>**重要** この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみに依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。 |
| Web インターフェイスの変更。 | なし | バージョン 7.0 では、次の点が変更されています。<br><br>• アクセス コントロール ルール エディタでは、[動的属性（Dynamic Attributes）] タブが、フォーカスの狭い [SGT/ISE 属性（SGT/ISE Attributes）] タブに置き換わります。ここで、SGT 属性を使用したルールの設定を続行します。<br><br>• **[システム（System）]** > **[SecureX]** で、SecureX 統合を設定するようになりました以前は、これらの設定は**[システム（System）]** > **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]** で行っていました。<br><br>• **[ヘルプ（Help）]** > **[使用方法（How-Tos）]** でウォークスルーが呼び出されるようになりました。以前は、ブラウザウィンドウの下部にある [使用方法（How-Tos）] をクリックしていました。 |

# FDM バージョン 7.0 で廃止された機能

表 *9 : 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><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><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><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 *10 :* 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。 |

# 廃止された FlexConfig コマンド

このドキュメントでは、今回のリリースで廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドと以前のリリースで廃止になった機能の完全なリストについては、コンフィギュレーション ガイドを参照してください。

⚠

**注意** ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

### FlexConfig について

いくつかの FTD の機能は、ASA 設定コマンドを使用して設定されます。Smart CLI または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。ご使用の構成は自動的に変換されません。アップグレード後は、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできません。

アップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。廃止されたコマンドが含まれている場合、メッセージは問題を示します。設定をやり直すことをお勧めします。新しい設定を確認したら、問題のある FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。