特長と機能

このドキュメントでは、バージョン7.1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 7.1 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 *7.1.0* の新機能

機能	説明
デバイスのセットアップ	

機能	説明
FDM を使用して、FMC による管理用に FTD を設定します。	FDM を使用して初期設定を実行すると、管理および FMC アクセス設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス設定が保持されます。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。FTD CLI を使用すると、管理と FMC 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設定は保持されません）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された FDM 画面：**[システム設定（System Settings）]** > **[管理センター（Management Center）]**
デバイスのアップグレード	
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**[システム（System）]** > **[更新（Updates）]**ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）]ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。

機能	説明
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。
Snort 3 後方互換性。	Snort 3 の場合、新しい機能と解決済みのバグでは、FMC とその管理対象デバイスを完全にアップグレードしている必要があります。Snort 2 とは異なり、新しい FMC（たとえば、バージョン 7.1）から展開して、古いデバイス（たとえば、バージョン 7.0）の検査エンジンを更新することはできません。 古いデバイスに展開すると、サポートされない設定が一覧表示され、それらの設定がスキップされることが警告されます。環境全体を常に更新することをお勧めします。
デバイス管理	

機能	説明
新しい Cisco Secure Firewall 3100 の設定と機能をサポート。	次の画面と CLI コマンドは、Secure Firewall 3100 に関連付けられています。これらの新しいモデルの詳細については、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 （31 ページ）を参照してください。 新規/変更された画面： • **[Devices]** > **[Device Management]** > **[Add Cluster]** • **[Devices]** > **[Device Management]** > **[More]** • **[Devices]** > **[Device Management]** > **[Cluster]** • **[Devices]** > **[Device Management]** > **[Chassis Operations]** • **[Devices]** > **[Device Management]** > **[Interfaces]** > 物理インターフェイスを編集 > [Hardware Configuration] • **[Devices]** > **[Device Management]** 新規/変更された FTD CLI コマンド： **configure network speed**、**configure raid**、**show raid**、**show ssd**
AWS インスタンスでの FTDv に対する Geneve インターフェイスサポート。	AWS ゲートウェイロードバランサ（GWLB）のシングルアームプロキシをサポートするために、Geneve カプセル化サポートが追加されました。AWS GWLB は、透過的なネットワークゲートウェイ（全トラフィックの唯一の出入口）と、トラフィックを分散し、トラフィックの需要に合わせて FTDv を拡張するロードバランサを組み合わせます。 このサポートには、Snort 3 が有効になっている FMC が必要であり、次のパフォーマンス階層で利用できます。 • FTDv20 • FTDv30 • FTDv50 • FTDv100
OCI 上の FTDv に対する Single Root I/O Virtualization（SR-IOV）のサポート	OCI 上の FTDv に Single Root Input/Output Virtualization（SR-IOV）を実装できるようになりました。SR-IOV により、FTDv のパフォーマンスを向上させることができます。SR-IOV モードでの vNIC としての Mellanox 5 はサポートされていません。

機能	説明
Firepower 1100 の LLDP サポート。	Firepower 1100 インターフェイスの Link Layer Discovery Protocol（LLDP）を有効にできるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [LLDP]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** サポートされるプラットフォーム：Firepower 1100（1120、1140、および 1150）
インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになり、インターフェイスの同期が改善されました。	インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになりました。また、FMC でインターフェイスを同期すると、ハードウェアの変更がより効果的に検出されます。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）]** サポートされるプラットフォーム：Firepower 1000/2100、Secure Firewall 3100
信頼された DNS サーバの指定のサポート。	FTD プラットフォーム設定を使用して、DNS スヌーピングに信頼できる DNS サーバーを指定できます。これは、ドメインを IP アドレスにマッピングすることにより、最初のパケットでアプリケーションを検出するのに役立ちます。デフォルトでは、信頼できる DNS サーバーには、DNS サーバーオブジェクト内の DNS サーバーと、dhcp-pool、dhcp-relay、および dhcp-client によって検出された DNS サーバーが含まれます。
デバイス設定のインポート/エクスポート。	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [全般（General）]**
高可用性/拡張性	

機能	説明
高可用性 • AWS 用 FMCv • OCI 用 FMCv	AWS 用 FMCv および OCI 用 FMCv で高可用性がサポートされるようになりました。 FTD の展開では、2 つの同一ライセンスの FMC と、各管理対象デバイスに 1 つの FTD 権限が必要です。たとえば、FMCv10 高可用性ペアで 10 台の FTD デバイスを管理するには、2 個の FMCv10 権限と 10 個の FTD 権限が必要です。バージョン 6.5.0 ～ 7.0.x のクラシックデバイス（NGIPSv または ASA FirePOWER）のみを管理している場合は、FMCv 権限は必要ありません。 サポートされるプラットフォーム：FMCv10、FMCv25、FMCv300（FMCv2 ではサポートされません）
OCI用FTDvの自動スケール。	OCI 用 FTDv で自動スケーリングがサポートされるようになりました。 クラウドベースの展開におけるサーバレス インフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内のFTDvインスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。
ファイアウォールの変更に対するクラスタの展開がより迅速に完了します。	ファイアウォールの変更に対するクラスタの展開がより迅速に完了するようになりました。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100
ハイアベイラビリティ グループまたはクラスタ内のルートのクリア。	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在、ハイアベイラビリティグループまたはクラスタで動作している場合、コマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループまたはクラスタ内のすべてのユニットのルーティングテーブルをクリアします。
NAT	
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。
ルーティング	

機能	説明
仮想ルータを相互接続するための BGP 設定。	ユーザー定義の仮想ルータ間、およびグローバル仮想ルータとユーザー定義の仮想ルータ間でルートを動的にリークするように BGP 設定を構成できます。ルートのインポートおよびエクスポート機能が導入され、仮想ルータにルートターゲットのタグを付け、必要に応じて、一致したルートをルートマップでフィルタリングすることにより、仮想ルータ間でルートを交換します。この BGP 機能は、ユーザー定義の仮想ルータを選択した場合にのみ利用できます。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv4/v6] > [ルートのインポート/エクスポート（Route Import/Export）]**
ユーザー定義の仮想ルータでの BGPv6 サポート。	FTD は、ユーザー定義の仮想ルータでの BGPv6 の設定をサポートするようになりました。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv6]**
Equal-Cost-Multi-Path（ECMP）ゾーンのサポート。	トラフィックゾーンのインターフェイスをグループ化し、FMC で Equal-Cost-Multi-Path（ECMP）ルーティングを設定できるようになりました。 ECMP ルーティングは、以前は FlexConfig ポリシーを通じてサポートされていました。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [ECMP]**
ダイレクト インターネット アクセス/ポリシーベースルーティング	

機能	説明
ポリシーベースルーティングによるダイレクト インターネット アクセス。	FMC を介してポリシーベースルーティングを設定して、アプリケーションに基づいてネットワークトラフィックを分類し、ダイレクト インターネット アクセス（DIA）を実装して、ブランチ展開からインターネットにトラフィックを送信できるようになりました。PBR ポリシーを定義し、入力インターフェイスに設定して、一致基準と出力インターフェイスを指定できます。アクセス コントロール ポリシーに一致するネットワークトラフィックは、ポリシーで設定されている優先順位または順序に基づいて、出力インターフェイスを介して転送されます。 新規/変更された画面：ポリシー ベース ルーティング ポリシーを設定するための新しいポリシーページ：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** サポートされるプラットフォーム：FTD
ダイレクト インターネット アクセスとポリシーベースルーティングのための FMC REST API の機能拡張。	FMC REST API を使用して、ポリシーベースルーティングによるダイレクト インターネット アクセスを設定できます。これをサポートするために、FMC REST API に次の機能拡張が加えられました。 • ポリシーベースルーティング設定を作成、表示、編集、および削除できるようにする新しい API が追加されました。 • アプリケーションを定義する拡張アクセス制御リストの既存の API に新しいパラメータが追加されました。 • インターフェイスの優先順位を定義するデバイスインターフェイスの既存の API に新しいパラメータが追加されました。
リモートアクセス VPN	
RA VPN ポリシーのコピー。	既存のポリシーをコピーして、新しい RA VPN ポリシーを作成できるようになりました。**[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]**の各ポリシーの横にコピーボタンが追加されました。

機能	説明
AnyConnect VPN SAML 外部ブラウザ。	AnyConnect VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。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。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。 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。
Microsoft Azure 上の SAML ID プロバイダーにおける複数のトラストポイント。	Microsoft Azure の要求に応じて、SAML ID プロバイダーに複数の RA VPN トラストポイントを追加できるようになりました。 Microsoft Azure ネットワークでは、Azure は同じエンティティ ID に対して複数のアプリケーションをサポートできます。（通常は別のトンネルグループにマップされる）各アプリケーションには、一意の証明書が必要です。この機能により、Microsoft Azure 向け FTDv で RA VPN に複数のトラストポイントを追加できます。
サイト間 VPN	
VPN フィルタ。	トンネリングされたデータパケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって許可するか拒否するかを決定するルールを使用して、サイト間 VPN フィルタを設定できるようになりました。 VPN フィルタは、トンネルから出た後の復号化後のトラフィックと、トンネルに入る前の暗号化前のトラフィックに適用されます。
IKEv2 の一意のローカルトンネル ID。	ポリシーベースとルートベースのサイト間 VPN の両方に IKEv2 トンネルごとのローカルトンネル ID を設定できるようになりました。FMC Web インターフェイスまたは REST API からローカルトンネル ID を設定できます。 このローカルトンネル ID 設定により、FTD との Umbrella SIG 統合が可能になります。

機能	説明
複数の IKE ポリシー。	ポリシーベースとルートベースのサイト間 VPN の両方に複数の IKE ポリシーを設定できるようになりました。 FMC GUI および REST API を使用して複数の IKE ポリシーを設定できます。
VPN 監視ダッシュボード。	**ベータ版。** サイト間 VPN 監視ダッシュボードは次の機能を提供します。 • 全デバイスのトンネルステータス分布の可視化 • VPN トンネルで構成されるネットワークトポロジの可視化 • トポロジ、デバイス、ステータスなどの基準に基づいてトンネルを視覚的に切り離して調べる機能 （注） サイト間監視ダッシュボードはベータ機能であり、期待どおりに動作しない場合があります。実稼働環境では使用しないでください。
セキュリティ インテリジェンス	
プロキシされたトラフィックでのセキュリティ インテリジェンスのための Snort 3 サポート。	Snort 3 では、IP アドレスが HTTP リクエストに埋め込まれている HTTP プロキシトラフィックにセキュリティ インテリジェンスを適用できるようになりました。たとえば、ユーザーが IP アドレスまたはネットワークを含むブロックリストまたは許可リストをアップロードすると、システムはプロキシ IP ではなく宛先サーバーの IP を照合します。その結果、宛先サーバーへのトラフィックを（セキュリティ インテリジェンスの設定に応じて）ブロック、監視、または許可することができます。
侵入検知と防御	

機能	説明
ルールアクションのドロップ、拒否、書き換え、およびパスに対する Snort 3 のサポート。	バージョン 7.1 FMC は、バージョン 7.0 デバイスを含む、Snort 3 を使用した FTD デバイスで次の侵入ルールアクションをサポートするようになりました。 • ドロップ：一致するパケットをドロップし、この接続でそれ以上のトラフィックをブロックしません。侵入イベントを生成します。 • 拒否：一致するパケットをドロップし、この接続の以降のトラフィックもブロックします。TCP トラフィックの場合、TCP リセットを送信します。UDP トラフィックの場合、送信元および宛先ホストに ICMP ポート到達不能を送信します。侵入イベントを生成します。 • 書き換え：ルールの置換オプションに基づいて一致するパケットを上書きします。侵入イベントを生成します。 • パス：一致するパケットが他の侵入ルールによる評価なしで通過することを許可します。侵入イベントを生成しません。 これらの新しいルールアクションを設定するには、侵入ポリシーの Snort 3 バージョンを編集し、各ルールの [ルールアクション（Rule Action）] ドロップダウンを使用します。
TLS ベースの侵入ルールに対する Snort 3 のサポート。	Snort 3 で復号化された TLS トラフィックを検査する TLS ベースの侵入ルールを作成できるようになりました。この機能により、Snort 3 侵入ルールで TLS 情報を使用できます。
SMB2 上の DCE/RPC のインスペクションに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1 は、SMB2 での DCE/RPC インスペクションをサポートします。 Snort 3 デバイスへの最初のアップグレード後の展開の後、既存の DCE/RPC ルールは、SMB2 での DCE/RPC の検査を開始します。以前は、これらのルールは SMB1 での DCE/RPC のみを検査していました。
侵入ルールの推奨に対する Snort 3 のサポート。	バージョン 7.1 FMC は、バージョン 7.0 デバイスを含む、Snort 3 を使用した FTD デバイスで侵入ルールの推奨をサポートするようになりました。 この機能を設定するには、侵入ポリシーの Snort 3 バージョンを編集し、左側のペインの [すべてのルール（All Rules）] の横にある [推奨（Recommendations）] ボタンをクリックします。

機能	説明
ssl_version および **ssl_state** キーワードに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1 では、**ssl_version** および **ssl_state** 侵入ルールキーワードがサポートされています。 シスコが提供する侵入ポリシーには、これらのキーワードを使用するアクティブルールが含まれます。これらを使用して、カスタム/サードパーティルールを作成、アップロード、および展開することもできます。バージョン 7.0.x では、これらのキーワードは Snort 2 でのみサポートされていました。Snort 3 では、これらのキーワードを含むルールはトラフィックに一致しないため、アラートを生成したり、トラフィックに影響を与えたりすることはできませんでした。ルールが予期したとおりに機能していないという通知はありませんでした。バージョン 7.1 以降の Snort 3 デバイスへの最初のアップグレード後の展開の後、これらのキーワードを含む既存のルールはトラフィックと一致します。
Identity Services およびユーザー制御	
HTTP/2 トラフィックのインターセプトに対する Snort 3 キャプティブポータルのサポート。	キャプティブポータルを使用したユーザー認証のために、HTTP/2 トラフィックをインターセプトしてリダイレクトできるようになりました。 ブラウザがリダイレクトを受信すると、ブラウザはリダイレクトに従い、HTTP/1 キャプティブポータルと同じプロセスを使用して idhttpsd（Apache Web サーバー）で認証します。認証後、idhttpsd によりユーザーは元の URL にリダイレクトされます。
ホスト名ベースのリダイレクトに対する Snort 3 キャプティブポータルのサポート。	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。 新規/変更された画面：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。
暗号化トラフィックの処理（TLS/SSL）	

機能	説明
TLS 証明書フィード。	ライブ TLS 証明書フィードに基づいて TLS/SSL ルールを作成できるようになりました。ライブ TLS 証明書フィードを使用すると、TLS 証明書フィンガープリントの管理オーバーヘッドが削減され、より最新の情報に基づいたルールが可能になります。
拡張 TLS/SSL ポリシーオプション。	[SSLポリシー（SSL Policy）] ページの [詳細設定（Advanced Settings）] タブで、次の拡張 TLS/SSL ポリシーオプションを設定できるようになりました。 • ESNI（暗号化されたサーバー名識別）を要求するフローをブロックする • HTTP/3 アドバタイズメントを無効にする • 信頼できないサーバー証明書をクライアントに伝播する
暗号化されたセッションを可視化するための暗号化された可視性エンジン。	**ベータ版。** 暗号化された可視性エンジンを有効にすると、復号を必要とせずに暗号化されたセッションを可視化することができます。このエンジンによってトラフィックのフィンガープリントが収集され、分析されます。FMC 7.1 では、暗号化された可視性エンジンにより、TLS や QUIC などのプロトコルを含む暗号化されたトラフィックの可視性が向上します。そのトラフィックに対してアクションは適用されません。 暗号化された可視性エンジンは、デフォルトで無効になっています。これは、[実験段階の機能（Experimental Features）] セクションのアクセス コントロール ポリシーの [詳細（Advanced）] タブで有効にすることができます。 新規/変更された画面：**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [*Access Control Policy name*] > [詳細（Advanced）]** **（注）** 暗号化された可視性エンジンは、可視性のために提供される実験段階のベータ機能です。誤検出を起こす可能性があります。
サービス ポリシー	
初期接続の最大セグメントサイズ（MSS）を設定します。	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 新規/変更された画面：[サービスポリシーの追加/編集（Add/Edit Service Policy）] ウィザードの [接続設定（Connection Settings）]。

機能	説明
ネットワークディスカバリ	
ネットワーク検出の Snort 3 サポートの改善（リモートネットワーク アクセスのサポート）。	ネットワーク検出とリモートネットワークアクセスのサポートの改善により、Snort 3 はこれらの機能について Snort 2 と同等になりました。強化された機能は次のとおりです。 • SMB トラフィックのホストとアプリケーションの検出：ネットワーク上の SMB トラフィックの場合、ホストはネットワークマップで検出され、SMB アプリケーションプロトコルと関連するオペレーティングシステム情報が検出されます。 • NetBIOS トラフィックの検出：NetBIOS トラフィックの場合、NetBIOS 名と、クライアントアプリケーションやオペレーティングシステムなどのアプリケーション関連情報が検出されます。 • ネットワーク検出ポリシーによって監視されるホスト/ネットワークのみのアプリケーションの検出：このフィルタリングロジックの機能拡張により、ネットワーク検出ルールに基づいて監視されているネットワークのアプリケーションを検出できます。 Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が常に有効になっています。
イベントロギングおよび分析	

機能	説明
エレファントフローの識別とモニタリングに対する Snort 3 のサポート。	Snort 3 を実行する FTD では、エレファントフロー（システム全体のパフォーマンスに影響を与えるのに十分な大きさのシングルセッション ネットワーク接続）を識別できるようになりました。デフォルトでは、エレファントフローの検出は自動的に有効になり、1GB/10 秒を超える接続を追跡および記録します。 接続イベントの新しい定義済み検索（Reason = Elephant Flow）を使用すると、エレファントフローをすばやく特定できます。ヘルスモニタを使用して、デバイス上のアクティブなエレファントフローを表示し、エレファントフローの発生率を CPU 使用率などの他のデバイスメトリックと関連付けるカスタム ヘルス ダッシュボードを作成することもできます。 この機能を無効にするか、サイズと時間のしきい値を設定するには、FTD CLI を使用します。 新規/変更された FTD CLI コマンド： • **show elephant-flow status** • **show elephant-flow detection-config** • **system support elephant-flow-detection enable** • **system support elephant-flow-detection disable** • **system support elephant-flow-detection bytes-threshold** *bytes-in-MB* • **system support elephant-flow-detection time-threshold** *time-in-seconds*
FMC からセキュアネットワーク分析クラウドに侵入イベントとレトロスペクティブ マルウェア イベントを送信します。	**アップグレードの影響。** Cisco Security Analytics and Logging（SaaS）を使用してセキュリティイベントを Stealthwatch クラウドに送信するようにシステムを設定すると、FMC は次を送信します。 • 侵入イベント。これにより、リモートで保存された侵入イベントに影響フラグデータを含めることができます。以前は、これらのイベントは FTD によってクラウドに送信され、影響フラグは含まれていませんでした。 • レトロスペクティブ マルウェア イベント。これらは、デバイスによって引き続きクラウドに送信される「元の性質」ファイルとマルウェアイベントを補完します。 この機能が有効になっている場合、FMC はアップグレードの成功後にこの情報の送信を開始します。

機能	説明
侵入イベントの新しいデータストアによるパフォーマンスの向上。	パフォーマンスを向上させるために、バージョン 7.1 では、侵入イベントに新しいデータストアを使用します。アップグレードが完了し、FMCが再起動すると、履歴イベントが、最新のイベントが先頭になるようにバックグラウンドで移行されます。 この移行の一部として、侵入インシデント、侵入イベントクリップボード、および侵入イベントのカスタムテーブルは廃止されました。詳細については、FMC バージョン 7.1 で廃止された機能（34 ページ）を参照してください。 また、侵入イベントテーブルに、[送信元ホストの重要度（Source Host Criticality）] と [宛先ホストの重要度（Destination Host Criticality）] という 2 つの新しいフィールドが導入されました。
接続およびセキュリティインテリジェンス イベントの NAT IP アドレスおよびポート情報。	NAT 変換の可視性を高めるために、次のフィールドが接続およびセキュリティ インテリジェンス イベントに追加されました。 • NAT 送信元 IP（NAT Source IP） • NAT 宛先 IP（NAT Destination IP） • NAT 送信元ポート（NAT Source Port） • NAT 宛先ポート（NAT Destination Port） イベントのテーブルビューでは、デフォルトでこれらのフィールドは非表示にされています。表示されるフィールドを変更するには、任意の列名の [x] をクリックしてフィールド選択ツールを表示します。

機能	説明
パケットトレーサの機能拡張。	バージョン 7.1 では、より使いやすくするためにパケット トレーサ インターフェイスが更新されています。さらに、次のことができるようになりました。 • メインメニューから直接パケットトレーサにアクセス：**[デバイス（Devices）] > [トラブルシュート（Troubleshoot）] > [パケットトレーサ（Packet Tracer）]** • パケットトレースの保存。 • 複数デバイスでの並列パケットトレースの実行。 • デバイスを介した PCAP の再生。 • Snort 3 デバイスの場合、L2 から L7 までのトラフィック評価のフェーズ（アプリケーション識別、ファイル/マルウェア検出、侵入検出、セキュリティ インテリジェンスなど）、および各フェーズにかかる時間に関して新しい詳細を提供する拡張出力の表示。 新規/変更された FTD CLI コマンド： • **packet-tracer input***source_interface* **pcap***pcap_filename*
オブジェクト管理	
HTTP、ICMP、および SSH プラットフォーム設定のネットワークオブジェクトのサポート。	Threat Defense プラットフォーム設定ポリシーで IP アドレスを設定するときに、ホストまたはネットワークのネットワークオブジェクトを含むネットワーク オブジェクト グループを使用できるようになりました。
ネットワーク ワイルドカードマスク オブジェクトの Snort 3 サポート。	[オブジェクト管理（Object Management）] ページで、ネットワーク ワイルドカード マスク オブジェクトを作成および管理できるようになりました。アクセス制御、プレフィルタ、およびNAT ポリシーでネットワーク ワイルドカード マスク オブジェクトを使用できます。
オブジェクトの展開プレビューの機能拡張。	地理位置情報、ファイルリスト、およびセキュリティ インテリジェンス オブジェクトへの展開の変更をプレビューできるようになりました。 更新された画面：**[展開（Deploy）] > [展開（Deployment）]**。[プレビュー（Preview）] 列で、デバイスの [プレビュー（Preview）] アイコンをクリックすると、ファイルリストオブジェクトへの変更が表示されます。
統合	

機能	説明
Cisco ACI Endpoint Update App バージョン 2.0 および修復モジュールのサポート。	Cisco ACI Endpoint Update App のバージョン 2.0 では、以前のバージョンに比べて次の点が改善されています。 • 最小更新間隔（アプリケーションが FMC を更新する頻度）が 10 秒になりました。以前は 30 秒でした。 • サイトプレフィックス（各 APIC テナントに関連付けられた FMC にネットワーク グループ オブジェクトを作成する文字列）が 10 文字に制限されました。以前は 5 文字でした。 この更新では、新しい Cisco ACI Endpoint 修復モジュールも利用できます。
ユーザビリティ、パフォーマンス、およびトラブルシューティング	
ヘルスモニタリングの強化。	ヘルスモニタは次のように更新されました。 • ヘルスポリシーエディタは、類似するヘルスモジュールをグループ化するようになりました。モジュールグループ全体を有効または無効にできます。 • ヘルスポリシー除外エディタが更新され、使いやすくなりました。また、アラートからデバイスまたはヘルスモジュールを除外するときに、除外の期間を 15 分から永久まで指定できるようになりました。 • ヘルス モニタ アラート エディタが更新され、使いやすくなりました。 • ヘルスポリシーの展開インターフェイスが更新され、使いやすくなりました。 （注） 更新されたヘルスモニタを使用するには、**[システム（System）] > [設定（Configuration）] > [REST API設定（REST API Preferences）]**で REST API アクセスを有効にする必要があります。 新規/変更された画面： • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] > [ポリシーの編集（Edit Policy）]** • **[システム（System）] > [ヘルス（Health）] > [除外（Exclude）]** • **[システム（System）] > [ヘルス（Health）] > [モニタアラート（Monitor Alerts）]** • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] > [ポリシーの展開（Deploy Policy）]**

機能	説明
展開履歴の機能拡張。	展開ジョブをブックマークし、ジョブの展開に関する注意を編集して、レポートを生成できるようになりました。
グローバル検索の機能拡張。	グローバル検索に次の機能が追加されました。 • FMC ウォークスルーの全文を検索できます（how-tos）。 • 拡張コミュニティリスト名または設定値を検索できます。 • ドメインごとに検索を制限できます。
新しいウォークスルー。	次のウォークスルーが追加されました。 • Snort 3 侵入ポリシーの作成。 • 個々のデバイス上での Snort 3 の有効化と無効化。 • Snort 3 ネットワーク分析ポリシーの作成。 • ネットワーク分析ポリシーのマッピングの表示。 • FTD のアップグレード。 • クラスタの作成および管理。 • FMC アクセスインターフェイスの管理からデータへの変更。 • FMC アクセスインターフェイスのデータから管理への変更。
Cisco Success Network に送信された Snort メモリ使用量テレメトリ。	有用性を向上させるために、Snort メモリおよびスワップ使用率（メモリ不足イベントを含む）に関するテレメトリを Cisco Success Network に送信するようになりました。 この情報は、Snort 2 と Snort 3 の両方に送信されます。Cisco Success Network の登録はいつでも変更できます。
Snort 3 は、フロー開始イベントとフロー終了イベントの統計情報をサポートします。	Snort 3 を使用する FTD の場合、**show snort statistics** コマンドの出力で、フロー開始イベントとフロー終了イベントに関する統計情報が報告されるようになりました。

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
	バージョン 7.0.2 以降のバージョン 7.0.x メンテナンスリリースからアップグレードする場合、バージョン 7.1 では以下の FMC メニューオプションが変更されます。 （注） これらの変更は、バージョン 7.2 で元に戻ります。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）] は次に変更されました。 [AMP] > [AMP管理（AMP Management）] [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [インテリジェンス（Intelligence）] > [ソース（Sources）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [インテリジェンス（Intelligence）] > [要素（Elements）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [インテリジェンス（Intelligence）] > [設定（Settings）] [統合（Integration）] > [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 [インテリジェンス（Intelligence）] > [インシデント（Incidents）]

機能	説明		
		た。	
	[統合（Integration）] > [その他の統合（Other Integrations）]	は次に変更されました。	**システム**（⚙） > [統合（Integration）]
	[統合（Integration）] > [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。	**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）]
	[統合（Integration）] > [SecureX]	は次に変更されました。	**システム**（⚙） > [SecureX]
FMC REST API			

機能	説明
FMC REST API サービス/操作。	

機能	説明
	新機能と既存の機能をサポートするために、複数の 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 7.1 クイックスタートガイド [英語] を参照してください。 新しい FMC REST API には次のものが含まれます。 • シャーシ管理：管理対象シャーシ、シャーシインターフェイス、ネットワークモジュール、およびブレークアウト インターフェイス用のシャーシ管理 API が追加されました。 • 展開：ジョブ履歴の API が追加されました。 • デバイスクラスタ：準備状況チェックを実行し、クラスタリングを変更するための API が追加されました。 • デバイス：次の API が追加されました。 • FTD インターフェイスの取得 • Packet Tracer • ルーティング • 仮想 LAN • 正常性：トンネル API が追加されました。 • オブジェクト：次の API が追加されました。 • 自律サービスパス • 拡張コミュニティ リスト • 拡張コミュニティ リスト • 拡張アクセス リスト • IPv4 プレフィックスリスト • IPv6 プレフィックスリスト • ポリシー リスト • ルート マップ • 標準アクセス リスト • 標準コミュニティ リスト • ポリシー：自動および手動の NAT ルールを変更するための API が追加されました。

機能	説明
	• ユーザー：Duo 設定を取得および変更するための API が追加されました。 • トラブルシューティング：パケットトレーサ PCAP 機能が追加されました。 • 更新：アップグレードを元に戻すための API が追加されました。 • ネットワークマップ：ホストと脆弱性のための API が追加されました。

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。 新しい/変更された画面：**[Devices]** > **[Interfaces]** 新しい/変更された FTD コマンド： configure network speed、configure raid、show raid、show ssd
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 FTD 7.0 です。	ASA 5508-X または 5516-X に FTDFTD 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 FTD 7.0 です。
ファイアウォールと IPS の機能	

機能	説明
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、FDM 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。 [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。 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。 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。 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。 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。 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、FDM または FTD 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。 FDM を使用して DDNS を設定し、FMC 管理に切り替えると、DDNS 構成が保持され、FMC 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。 FDM で、**[System Settings]** > **[DDNS Service]**ページが追加されました。FTD 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。
FDM を使用した DHCP リレー構成。	FDM 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。 [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。 > >
FDM の自己署名証明書のキータイプとサイズ。	FDM 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。

機能	説明
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。 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。
FDM での**管理者**パスワードの生成。	FDM での初期システム設定時、または FDM 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。 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。
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。 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。

機能	説明
FDM を使用した FMC による管理のための FTD の構成	FDM を使用して初期設定を実行すると、管理および FMC アクセス設定に加えて、管理のために FMC に切り替えたときに、FDM 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。FTD CLI を使用すると、管理と FMC 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）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 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）] >
FTD 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 FTD 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。 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、[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。 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。 管理センターの展開では、これらのデバイスはスパンド EtherChannel クラスタリング用に最大 8 つのユニットをサポートします。 （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。FMC の場合、新しいオンラインヘルプがバージョン 7.1.0.2 に含まれています。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。 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、FMC バージョン 7.1 の新機能 （1 ページ）およびFDM バージョン 7.1 の新機能 （25 ページ）を参照してください。
AWS 用 FMCv300 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。 • c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • c5d.xlarge、c5d.2xlarge、c5d.4xlarge • c5n.xlarge、c5n.2xlarge、c5n.4xlarge • i3en.xlarge、i3en.2xlarge、i3en.3xlarge • inf1.xlarge、inf1.2xlarge • m5.xlarge、m5.2xlarge、m5.4xlarge • m5a.xlarge、m5a.2xlarge、m5a.4xlarge • m5ad.xlarge、m5ad.2xlarge、m5ad.4xlarge • m5d.xlarge、m5d.2xlarge、m5d.4xlarge • m5dn.xlarge、m5dn.2xlarge、m5dn.4xlarge • m5n.xlarge、m5n.2xlarge、m5n.4xlarge • m5zn.xlarge、m5zn.2xlarge、m5zn.3xlarge • r5.xlarge、r5.2xlarge、r5.4xlarge • r5a.xlarge、r5a.2xlarge、r5a.4xlarge • r5ad.xlarge、r5ad.2xlarge、r5ad.4xlarge • r5b.xlarge、r5b.2xlarge、r5b.4xlarge • r5d.xlarge、r5d.2xlarge、r5d.4xlarge • r5dn.xlarge、r5dn.2xlarge、r5dn.4xlarge • r5n.xlarge、r5n.2xlarge、r5n.4xlarge • 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。 • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

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 7.1 で廃止された機能

表 *4 : FMC* バージョン *7.1.0* で廃止された機能

機能	アップグレードの影響	説明
侵入インシデントと侵入イベントクリップボード。	インシデントに関連するすべてのデータが削除されます。 クリップボードをデータソースとして使用するレポート テンプレート セクションは削除されます。	バージョン 7.1 では、侵入インシデント機能と関連する侵入イベントクリップボードが削除されています。 廃止された画面/オプション： • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）] • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • 侵入イベントワークフローページおよびパケットビューでの [コピー（Copy）] および [すべてコピー（Copy All）] • レポートテンプレートにセクションを追加する場合（[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）]）、データソースとして [クリップボード（Clipboard）] テーブルを選択できなくなりました。
侵入イベントのカスタムテーブル。	侵入イベントテーブルのフィールドを含むカスタムテーブルは削除されます。	バージョン 7.1 では、侵入イベントのカスタムテーブルのサポートが終了します。 カスタムテーブルにフィールドを追加する場合（[分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル（Custom Tables）]）、データソースとして [侵入イベント（Intrusion Events）] テーブルを選択できなくなりました。

機能	アップグレードの影響	説明
SecureX との統合、SecureX とのオーケストレーションの改善	バージョン 7.0.2 以降でこの機能を新たに有効にした場合、バージョン 7.1 にアップグレードできません。	バージョン 7.1 では、バージョン 7.0.2 で導入された SecureX との統合およびオーケストレーションの改善を一時的に中止します。 バージョン 7.0.2 またはそれ以降のメンテナンスリリースで SecureX との統合を新たに有効にした場合は、バージョン 7.1 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、以前の方法を使用して、この機能を再度有効にできます。 バージョン 7.0.0 または 7.0.1 で SecureX との統合を有効にした場合は、アップグレードの際に問題は発生しません。
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。 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。 **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。

機能	アップグレードの影響	説明
NGIPS ソフトウェア（ASA FirePOWER、NGIPSv）。	アップグレードは禁止されています。	バージョン 7.1 は、FMC および FTD デバイスでのみサポートされます。ASA FirePOWER または NGIPSv デバイスではサポートされていません。 バージョン 7.1 の FMC を引き続き使用して、バージョン 6.5 ～ 7.0 を実行している古いデバイス（FTD、ASA FirePOWER および NGIPSv）を管理できます。

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 *5:* 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。
FMC 1000、2500、4500	FMC モデルの FMC 1000、2500、および 4500 ではバージョン 7.1 以降を実行できません。これらの FMC を使用してバージョン 7.1 以降のデバイスを管理することはできません。

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。

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。