特長と機能

このドキュメントでは、バージョン6.6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。 Cisco Defense Orchestrator（CDO）の導入については、Cisco Defense Orchestrator の新機能 を参照してください。

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。

FMC バージョン 6.6 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、通常は FMC とデバイスの両方で最新のリリースが必要です。 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。このドキュメントでは、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。

（注） バージョン 6.6 は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。ユーザーエージェント設定を使用して FMC をバージョン 6.7 以降 にアップグレードすることはできません。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。これにより、ユーザー エージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、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。

詳細については、Cisco Firepower User Agent のサポート終了 [英語] 通知、および Firepower ユーザー ID：ユーザーエージェントから Identity Services Engine への移行 [英語] の技術メモを参照してください。

新機能

表 *1 : FMC* バージョン *6.6.3* の新機能

新機能	説明
アップグレードがスケジュールされたタスクを延期する。	**アップグレードの影響。** アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、バージョン 6.6.3 以降を実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 以降のパッチからアップグレードする場合を除き、バージョン 6.6.3 へのアップグレードはサポートされません。

新機能	説明
アプライアンス設定のリソース使用率の正常性モジュール。	**バージョン 6.7.0 のアップグレードの影響。** バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールであるアプライアンス設定のリソース使用率が導入されています。 モジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。詳細については、コンフィギュレーション ガイドの「アクセス制御のベストプラクティス」を参照してください。 アップグレードプロセスにより、すべての正常性ポリシーにこのモジュールが自動的に追加され、有効になります。アップグレード後、正常性ポリシーを管理対象デバイスに適用して、モニタリングを開始します。 （注） このモジュールには、FMC と管理対象デバイスの両方に、バージョン 6.6.3 以降の 6.6.x リリース、 またはバージョン 7.0 以降が必要です。 バージョン 6.7 では、このモジュールのサポートが部分的および一時的に廃止されています。詳細については、バージョン 6.7 リリースノートを参照してください。バージョン 7.0 ではフルサポートが提供され、モジュールの名前が構成メモリ割り当てに変更されています。

表 *2 : FMC* バージョン *6.6.0* の新機能

新機能	説明
プラットフォーム	
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。

新機能	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。** 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。 • C5.xlarge • C 5.2 xlarge • C5.4xlarge FMCv 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。 • C3.4xlarge • C4.4xlarge • C5.4xlarge AWS インスタンスタイプの既存の FMCv はすべて廃止になりました（c3.xlarge、c3.2xlarge、c4.xlarge、c4.2xlarge）。アップグレードする前に、サイズを変更する必要があります。詳細については、FMCv には 28 GB の RAM が必要 を参照してください。
クラウドベースの FTDv 展開の自動スケール。	AWS 自動スケール/Azure 自動スケールのサポートが導入されました。 クラウドベースの展開におけるサーバーレス 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。 サポートされているプラットフォーム：FTDv for AWS、FTDv for Azure
Firepower Threat Defense：**デバイス管理**	
DHCP を使用した初期管理インターフェイスの IP アドレスの取得。	Firepower 1000/2000 シリーズと ASA-5500-X シリーズのデバイスの場合、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得するようになりました。この変更により、既存のネットワーク上に新しいデバイスを簡単に展開できるようになりました。 この機能は、論理デバイスを展開するときに IP アドレスを設定する Firepower 4100/9300 シャーシではサポートされていません。また、FTDv や ISA 3000 でもサポートされていません。これらについては、引き続きデフォルトで 192.168.45.45 になります。 サポートされているプラットフォーム：Firepower 1000/2000 シリーズ、ASA-5500-X シリーズ

新機能	説明
CLI での MTU 値の設定。	FTD CLI を使用して、FTD デバイスインターフェイスの MTU（最大伝送単位）値を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。MTU の最大値は次のとおりです。 • 管理インターフェイス：1500 バイト • イベントインターフェイス：9000 バイト 新しい FTD CLI コマンド： **configure network mtu** 変更された FTD CLI コマンド：**mtu-event-channel** キーワードと **mtu-management-channel** キーワードが **configure network management-interface** コマンドに追加されました。 サポートされるプラットフォーム：FTD
内部 Web サーバーからの Threat Defense アップグレードパッケージの取得。	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6.0+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6.0 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更されたページ：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション サポートされるプラットフォーム：FTD
接続ベースのトラブルシューティングの機能拡張。	FTD CLI 接続ベースのトラブルシューティングに次の機能拡張が加えられました（デバッギング）。 • **debug packet-module trace**：モジュールレベルのパケットトレースを有効にするために追加されました。 • **debug packet-condition**：進行中の接続のトラブルシューティングをサポートするように変更されました。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：クラスタリング	

新機能	説明
マルチインスタンスクラスタリング。	コンテナインスタンスを使用してクラスタを作成できるようになりました。Firepower 9300 では、クラスタ内の各モジュールに 1 つのコンテナインスタンスを含める必要があります。セキュリティエンジン/モジュールごとに複数のコンテナインスタンスをクラスタに追加することはできません。 クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。 新しい FXOS CLI コマンド： **set port-type cluster** 新規/変更された Chassis Manager ページ： • [論理デバイス（Logical Devices）] > [クラスタの追加（Add Cluster）] • [インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）] ドロップダウンメニュー > [サブインターフェイス（Subinterface）] > [タイプ（Type）] フィールド サポートされるプラットフォーム：Firepower 4100/9300
FTD クラスタでのデータユニットへのパラレル設定同期。	FTD クラスタの制御ユニットは、デフォルトでスレーブユニットとの設定変更を同時に同期させるようになりました。以前は、同期が順番に行われていました。 サポートされるプラットフォーム：Firepower 4100/9300
クラスタへの参加の失敗や削除のメッセージを **show cluster history** に追加。	クラスタユニットがクラスタへの参加に失敗するか、クラスタを離脱する場合のために、新しいメッセージが **show cluster history** コマンドに追加されました。 サポートされるプラットフォーム：Firepower 4100/9300
Firepower Threat Defense：ルーティング	

新機能	説明
仮想ルータと 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るようになりました。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。 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。 作成できる仮想ルータの最大数は 5 ~ 100 の範囲で、デバイスのモデルによって異なります。完全なリストについては、『Firepower Management Center Configuration Guide』の「Virtual Routing for Firepower Threat Defense」の章を参照してください。 新規/変更されたページ：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ 新しい FTD CLI コマンド：**show vrf**。 変更された FTD CLI コマンド：［**vrf** *name* | **all**］キーワードセットを CLI コマンド **clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** 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に変更しました。 サポートされるプラットフォーム：FTD（Firepower 1010 および ISA 3000 を除く）
Firepower Threat Defense：**VPN**	
リモートアクセス VPN 内の DTLS 1.2。	Datagram Transport Layer Security（DTLS） 1.2 を使用して、RA VPN 接続を暗号化できるようになりました。 FTD プラットフォーム設定を使用して、FTD デバイスが RA VPN サーバーとして動作するときに使用する最小 TLS プロトコルバージョンを指定します。また、DTLS 1.2 を指定する場合は、最小 TLS バージョンとして TLS 1.2 を選択する必要もあります。 Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7 以降が必要です。 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）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [SSL] > [DTLS バージョン（DTLS Version）] オプション サポートされるプラットフォーム：FTD（ASA 5508-X および ASA 5516-X を除く）

新機能	説明
複数のピアに対するサイト間 VPN IKEv2 のサポート。	IKEv1 と IKEv2 のポイントツーポイント エクストラネットおよびハブアンドスポークトポロジのために、サイト間VPN接続にバックアップピアを追加できるようになりました。これまで設定できたのは、IKEv1 ポイントツーポイント トポロジのバックアップピアのみでした。 新規/変更されたページ：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [ポイントツーポイントまたはハブアンドスポーク FTD VPN トポロジの追加または編集（Add or Edit a Point to Point or Hub and Spoke FTD VPN Topology）] > [エンドポイントの追加（Add Endpoint）] > [IP アドレス（IP Address）] フィールドで、カンマ区切りのバックアップピアがサポートされるようになりました。 サポートされるプラットフォーム：FTD
セキュリティ ポリシー	
セキュリティポリシーの使いやすさの向上。	バージョン 6.6.0 を使用すると、アクセス制御ルールとプレフィルタルールが簡単に使用できるようになります。次の作業に進んでください。 • 1 回の操作（状態、アクション、ロギング、侵入ポリシーなど）で、複数のアクセス制御ルールの特定の属性を編集します。 アクセス コントロール ポリシー エディタで、関連するルールを選択し、右クリックして [編集（Edit）] を選択します。 • 複数のパラメータによってアクセス制御ルールを検索します。 アクセス コントロール ポリシー エディタで、[ルールの検索（Search Rules）] テキストボックスをクリックしてオプションを表示します。 • アクセス制御ルールまたはプレフィルタルール内のオブジェクトの詳細と使用状況を表示します。 アクセス コントロール ポリシー エディタまたはプレフィルタ ポリシー エディタで、ルールを右クリックし、[オブジェクトの詳細（Object Details）] を選択します。 サポートされるプラットフォーム：FMC

新機能	説明
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、FTD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、ルールがどのように定義されているかや、FMC 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。 新規/変更されたページ：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [デバイス（Device）] タブ > [詳細設定（Advanced Settings）] > [オブジェクトグループ検索（Object Group Search）] オプション サポートされるプラットフォーム：FTD
アクセスコントロールポリシーとプレフィルタポリシーの時間ベースのルール。	適用するルールの絶対時間または反復時間、あるいは時間範囲を指定できるようになりました。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。 新規/変更されたページ： • アクセス コントロール ルール エディタまたはプレフィルタルールエディタ • [デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [タイムゾーン（Time Zone ）] • [オブジェクト（Objects）]> [オブジェクト管理（Object Management）] > [時間範囲（Time Range）] と [タイムゾーン（Time Zone）] サポートされるプラットフォーム：FTD

新機能	説明
出力最適化の再有効化。	**アップグレードの影響。** バージョン 6.6.0 では CSCvs86257 が修正されました。出力最適化が次のような状態だった場合があります。 • 有効になっていたがオフになり、アップグレードするとオンに戻る（機能が有効になっていた場合でも、バージョン 6.4.0 と 6.5.0 の一部のパッチでは出力最適化をオフにしていました）。 • 手動で無効にした場合は、アップグレード後に **asp inspect-dp egress-optimization** を使用して再度有効にすることをお勧めします。 サポートされるプラットフォーム：FTD
イベントロギングおよび分析	
新しいデータストアによるパフォーマンスの向上。	**アップグレードの影響。** パフォーマンスを向上させるために、バージョン 6.6.0 では、接続およびセキュリティ インテリジェンス 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 がリブートすると、履歴接続イベントとセキュリティ インテリジェンス イベントがバックグラウンドで移行され、リソースが制限されます。FMC モデル、システム負荷、および保存したイベント数に応じて、数時間から最大で 1 日かかることがあります。 履歴イベントは、経過時間ごとに、最新のイベントが最初に以降されます。移行されていないイベントは、クエリ結果やダッシュボードに表示されません。移行が完了する前に接続イベントデータベースの制限に達した場合（アップグレード後のイベントの場合など）、最も古い履歴イベントは移行されません。 イベントの移行の進行状況は、メッセージセンターでモニターできます。 サポート対象プラットフォーム：FMC
URL の接続イベントとセキュリティ インテリジェンス イベントを検索する場合のワイルドカードのサポート。	**example.com** のパターンを持つ URL の接続イベントとセキュリティ インテリジェンス イベントを検索する場合は、ワイルドカードを含めなければならなくなりました。このような検索の場合、具体的には ***example.com*** を使用します。 サポート対象プラットフォーム：FMC

新機能	説明
FTDデバイスを使用した最大 30 万の同時ユーザーセッションのモニタリング。	バージョン 6.6.0 では、FTD デバイスモデルの一部で、同時ユーザーセッション（ログイン）のモニタリングが新たにサポートされるようになります。 • 30 万セッション：Firepower 4140、4145、4150、9300 • 15 万セッション：Firepower 2140、4112、4115、4120、4125 他のすべてのデバイスは、2,000 に制限されている ASA FirePOWER を除き、以前の 64,000 の制限を引き続きサポートします。 新しい正常性モジュールでは、ユーザー ID 機能のメモリ使用率が設定可能なしきい値に達したときに、アラートを発行します。また、時間の経過に伴うメモリ使用率のグラフも表示できます。 新規/変更されたページ： • [システム（System）]>[正常性（Health）]>[ポリシー（Policy）]>[正常性ポリシーを追加または編集（Add or Edit Health Policy）]>[Snort アイデンティティメモリ使用率（Snort Identity Memory Usage）] • [システム（System）]>[正常性（Health）]>[モニター（Monitor）]>デバイスの選択>[Snort アイデンティティメモリ使用率（Snort Identity Memory Usage）] モジュールの [グラフ（Graph）] オプション サポートされるプラットフォーム：上記の FTD デバイス
IBM QRadar との統合。	IBM QRadar 向けの新しい Cisco Firepower アプリケーションをイベントデータを表示するための代替手段として使用して、ネットワークへの脅威を分析、ハント、および調査をすることができます。eStreamer が必要です。 詳細については、Integration Guide for the Cisco Firepower App for IBM QRadarを参照してください。 サポート対象プラットフォーム：FMC
管理とトラブルシューティング	

新機能	説明
設定変更を展開するための新しいオプション。	FMC メニューバーの [展開（Deploy）] ボタンが次の機能を追加するオプションが備わったメニューになりました。 • [ステータス（Status）] : デバイスごとに、変更を展開する必要があるかどうか、展開前に解決する必要がある警告またはエラーがあるかどうか、最後の展開が処理中、失敗、正常に完了のうちのどの状態かが表示されます。 • [プレビュー（Preview）] : デバイスに対して最後に展開してから行った、適用可能なすべてのポリシーとオブジェクトの変更が表示されます。 • [展開の選択（Selective Deploy）] : 管理対象デバイスに対して展開するポリシーと設定から選択します。 • [展開時間の見積もり（Deploy Time Estimate）] : 特定のデバイスに対して展開するためにかかる時間の見積もりが表示されます。すべての展開のみでなく、特定のポリシーや設定の見積もりを表示することができます。 • [履歴（History）] : 以前の展開の詳細が表示されます。 新規/変更されたページ : • **[展開（Deploy）] > [展開（Deployment）]** • **[展開（Deploy）] > [展開履歴（Deployment History）]** サポート対象プラットフォーム：FMC

新機能	説明
初期設定による VDB の更新と、SRUの更新のスケジュール設定。	新規および再イメージ化された FMC では、セットアッププロセスは次のようになりました。 • 最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。 • 毎日の侵入ルール（SRU）のダウンロードを有効にします。これらのダウンロード後は、セットアッププロセスで自動展開が有効にならないことに注意してください。ただし、この設定は変更できます。 アップグレードされた FMC は影響を受けません。 新規/変更されたページ： • [システム（System）] > [更新（Updates）] > [製品の更新（VDB の更新）（Product Updates (VDB updates)）] • [システム（System）] > [更新（Updates）] > [ルールの更新（SRU の更新）（Rule Updates (SRU updates)）] サポート対象プラットフォーム：FMC
FMC を復元するための VDB の一致は不要。	バックアップからの FMC の復元に交換用 FMC 上に同じ VDB を使用する必要はなくなりました。ただし、復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられます。 サポート対象プラットフォーム：FMC
サブジェクト代替名（SAN）を使用した HTTPS 証明書。	SAN を使用して複数のドメイン名または IP アドレスを保護する HTTPS サーバー証明書を要求できるようになりました。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。 新規/変更されたページ：[システム（System）]>[設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）] > [新しい CSR の生成（Generate New CSR）] > [サブジェクト代替名（Subject Alternative Name）] フィールド サポート対象プラットフォーム：FMC
FMC ユーザーアカウントに関連付けられている実名。	FMC ユーザーアカウントを作成または変更するときに、実名を指定できるようになりました。これには、個人名、部署名、またはその他の識別属性を指定できます。 新規/変更されたページ：[システム（System）]>[ユーザー（Users）] > [ユーザー（Users）] > [実名（Real Name）] フィールド サポート対象プラットフォーム：FMC

新機能	説明
追加の FTD プラットフォームでの Cisco Support Diagnostics。	**アップグレードの影響。** Cisco Support Diagnostics は、すべての FMC および FTD デバイスで完全にサポートされるようになりました。以前は、サポートは FMC、FTD 搭載 Firepower 4100/9300、および Azure 向け FTDv に限定されていました。詳細については、「シスコとのデータの共有」を参照してください。 サポートされるプラットフォーム：FMC、FTD
ユーザビリティ	
ライトテーマ。	FMC はデフォルトでバージョン 6.5.0 のベータ機能として導入されたライトテーマに設定されます。バージョン 6.6.0 にアップグレードすると、ライトテーマに自動的に切り替わります。これは、ユーザー設定で従来のテーマに戻すことができます。 すべてに返信することはできませんが、ライトテーマについてのフィードバックを歓迎します。[ユーザー設定（User Preferences）] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com からフィードバックをお送りください。 サポート対象プラットフォーム：FMC
アップグレードの残り時間の表示。	FMC のメッセージセンターに、アップグレードが完了するまでのおおよその残り時間が表示されるようになりました。これには、リブート時間は含まれません。 新規/変更されたページ：メッセージセンター サポート対象プラットフォーム：FMC
セキュリティと強化	
デフォルトの HTTPS サーバー証明書の更新期限は 800 日。	**アップグレードの影響。** 現在のデフォルトの HTTPS サーバー証明書がすでに 800 日である場合を除き、バージョン 6.6.0 にアップグレードすることで証明書が更新され、有効期限がアップグレード日から 800 日後になりました。今後の更新はすべて、有効期間が 800 日になります。 古い証明書は、生成日に応じて期限切れになるように設定されていました。 サポート対象プラットフォーム：FMC
Firepower Management Center REST API	

新機能	説明
新しい REST API 機能。	バージョン 6.6.0 の機能をサポートするための次の REST API サービスが追加されました。 • bgp、bgpgeneralsettings、ospfinterface、ospfv2routes、ospfv3interfaces、ospfv3routes、virtualrouters、routemaps、ipv4prefixlists、ipv6prefixlists、aspathlists、communitylists、extendedcommunitylists、standardaccesslists、standardcommunitylists、policylists：ルーティング • virtualrouters、virtualipv4staticroutes、virtualipv6staticroutes、virtualstaticroutes：仮想ルーティング • timeranges、globaltimezones、timezoneobjects：時間ベースのルール • commands：REST API から CLI コマンドの限定的なセットを実行 • pendingchanges：保留中の改善点を展開 古い機能をサポートするために、次の REST API サービスが追加されました。 • intrusionrules、intrusionpolicies：侵入ポリシー サポート対象プラットフォーム：FMC
拡張アクセスリストの REST API サービス名の変更。	**アップグレードの影響。** FMC REST API の extendedaccesslist（単数形）サービスは、extendedaccesslist**s**（複数形）になりました。クライアントを更新していることを確認します。古いサービス名を使用すると失敗し、無効な URL エラーが返されます。 要求タイプ：GET 特定の ID に関連付けられている拡張アクセスリストを取得するための URL： • 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} すべての拡張アクセスリストを取得するための URL： • 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** サポート対象プラットフォーム: FMC

廃止された機能

表 *3*：バージョン *6.6.1* で廃止された機能

廃止された機能	説明
ルールが競合してもカスタム侵入ルールのインポートが失敗しない。	バージョン 6.6.0 では、ルールの競合があった場合、FMC はカスタム（ローカル）侵入ルールのインポートの完全な拒否を開始しました。バージョン 6.6.1 ではこの機能を廃止し、競合が発生したルールをサイレントでスキップする、バージョン 6.6 より前の動作に戻ります。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーション ガイドでローカル侵入ルールをインポートするためのベストプラクティスを参考にすることを推奨します。 バージョン 6.7 では、ルールの競合に関する警告が追加されます。

表 *4*：バージョン *6.6.0* で廃止された機能

廃止された機能	説明
廃止：クラウドベースの FMCv 展開でのメモリ不足のインスタンス。	パフォーマンス上の理由から、次の FMCv インスタンスはサポートされなくなりました。 • AWS での c3.xlarge • AWS での c3.2xlarge • AWS での c4.xlarge • AWS での c4.2xlarge • Azure での Standard_D3_v2 AWS インスタンスタイプの既存の FMCv はすべて廃止になりました（c3.xlarge、c3.2xlarge、c4.xlarge、c4.2xlarge）。アップグレードする前に、サイズを変更する必要があります。詳細については、FMCv には 28 GB の RAM が必要 を参照してください。 さらに、バージョン 6.6 リリースの時点で、クラウドベースの FMCv の展開におけるメモリ不足のインスタンスタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv インスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。

廃止された機能	説明
廃止：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。 詳細については、『Cisco Secure Firewall Threat Defense Virtual Getting Started Guide』を参照してください。
廃止：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。	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。 • Diffie-Hellman グループ：2、5、および 24。 • 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）。 • ハッシュアルゴリズム：MD5。 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。
廃止：接続イベントのカスタムテーブル。	バージョン 6.6 は、接続イベントとセキュリティ インテリジェンス イベントのカスタムテーブルのサポートを終了します。アップグレード後は、これらのイベントの既存のカスタムテーブルは引き続き「利用可能」ですが、結果は返されません。これらのテーブルを削除することをお勧めします。 他のタイプのカスタムテーブルに変更はありません。 廃止されたオプション： • [分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル （Custom Tables）] > [カスタムテーブルの作成（Create Custom Table）] > [テーブル（Tables）] ドロップダウンリスト > [接続イベント（Connection Events）] と、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] のクリック

廃止された機能	説明
廃止：イベントビューアから接続イベントを削除する機能。	バージョン 6.6 は、接続イベントとセキュリティ インテリジェンス イベントをイベントビューアから削除するためのサポートを終了しています。データベースを消去するには、**[システム（System）]**>**[ツール（Tools）]** > **[データの消去（Data purge）]** を選択します。 廃止されたオプション： • **[分析（Analysis）]**>**[接続（Connections）]**>**[イベント（Events）]** > [削除（Delete）] と [すべて削除（Delete All）] • **[分析（Analysis）]** > **[接続（Connections）]** > **[セキュリティ インテリジェンス イベント（Security Intelligence Events）]** > [削除（Delete）] と [すべて削除（Delete All）]
廃止：地理位置情報の詳細。	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。

FDM バージョン 6.6 の新機能

表 *5: FDM* バージョン *6.6* の新機能と廃止された機能

機能	説明
プラットフォーム機能	

機能	説明
Amazon Web Services（AWS）クラウド用 FTDv における FDM のサポート。	FDM を使用して AWS クラウド用 FTDv で Firepower Threat Defense を設定できます。
Firepower 4112 用 FDM。	Firepower 4112 用 Firepower Threat Defense が導入されました。 （注）　FXOS 2.8.1 が必要です。
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。 詳細については、『Cisco Secure Firewall Threat Defense Virtual Getting Started Guide』を参照してください。
ファイアウォールと IPS の機能	
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。 [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。 FDM 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。 Firepower Threat Defense API では、IntrusionPolicy リソースに inspectionMode 属性が追加されました。

機能	説明
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、FDMを使用してワークステーションから Firepower 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、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。 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。
Firepower 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。	Firepower 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。FDM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、FDM は表示されません。 TimeRangeObject、Recurrence、TimeZoneObject、DayLightSavingDateRange、および DayLightSavingDayRecurrence リソースが Firepower 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。

機能	説明
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、Firepower 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、FDM 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。 FDM 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	
サイト間 VPN のバックアップピア（Firepower Threat Defense API のみ）。	Firepower 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。 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。 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、Firepower 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。 FDM 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 FDM に表示したりはできません。

機能	説明
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、Firepower Threat Defense API のみを使用して設定できます。FDM 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 FDM 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。 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。
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。 • Diffie-Hellman グループ：2、5、および 24。 • 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）。 • ハッシュアルゴリズム：MD5。
ルーティング機能	

機能	説明
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。 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。 [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。 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** **show vrf** コマンドが追加されました。
OSPF および BGP の設定を [ルーティング（Routing）] ページに移動。	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。 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	

機能	説明
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。 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
Firepower 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。 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。 • 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。 • 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。 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。 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。 FDM 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。 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]** 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 Firepower 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 FTDv 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。 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。
FDM 管理接続の HTTP プロキシサポート。	FDM 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。 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 Firepower 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。 新規/変更されたコマンド：**configure network mtu、configure network management-interface mtu-management-channel** 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。 **[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。Firepower 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。 **[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。Firepower 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 FDM 直接サポート。	FDM 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。 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 Firepower Threat Defense API に追加されました。
FDM 管理 Web サーバー証明書の信頼チェーン検証。	FDM 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。 **[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。 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 Firepower 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。 [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。
Firepower 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 Firepower 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。 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、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。

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 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。