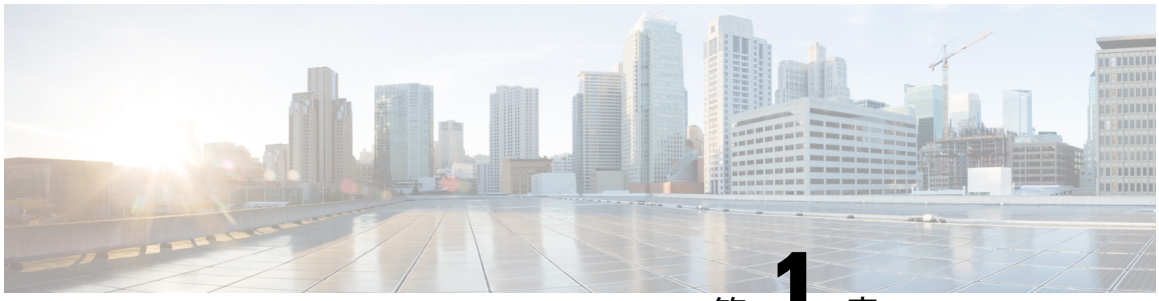
クラウド提供型 Firewall Management Center リリースノート：Cisco Defense Orchestrator の機能

最終更新：2025 年 3 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

クラウド提供型 Firewall Management Center について

Cisco Defense Orchestrator（CDO）はクラウド提供型 Firewall Management Center のプラットフォームです。

クラウド提供型 Firewall Management Center は、Cisco Secure Firewall Threat Defense デバイスを管理する Software as a Service（SaaS）製品です。提供する機能の多くはオンプレミス型 Cisco Secure Firewall Management Center と同じです。外観や動作もオンプレミス型の Cisco Secure Firewall Management Center と同じで、同じ FMC REST API が使用されています。

この製品は、オンプレバージョンの Cisco Secure Firewall Management Center から SaaS バージョンへの移行を希望される Cisco Secure Firewall Management Center のお客様向けに設計されました。

CDO オペレーションチームが、SaaS 製品の維持管理を担当します。新しい機能が導入されると、CDO オペレーションチームが CDO とクラウド提供型 Firewall Manager Center をお客様に代わって更新します。

お使いのオンプレミス型 Cisco Secure Firewall Management Center に登録されている Cisco Secure Firewall Threat Defense デバイスをクラウド提供型の Firewall Management Center に移行するための移行ウィザードが用意されています。

- 本リリースノートの対象ユーザー （1 ページ）

本リリースノートの対象ユーザー

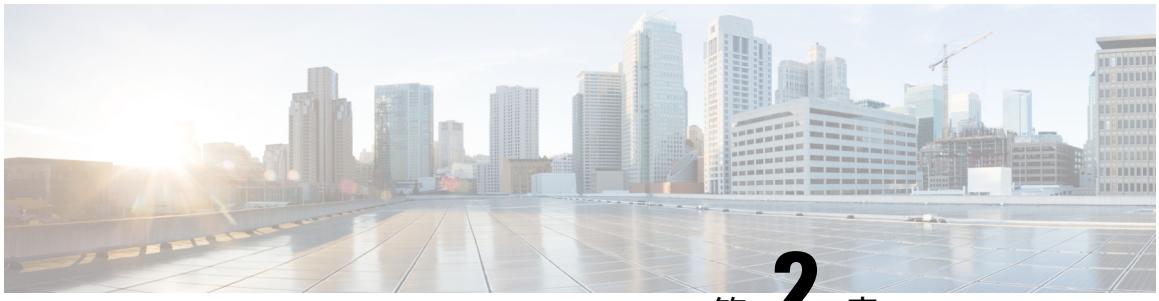
これらのリリースノートは、テナントに クラウド提供型 Firewall Management Center を展開している既存の Cisco Security Cloud Control（Security Cloud Control）ユーザーを対象としています。

Cisco Secure Threat Defense の用語

表 *1*:

製品名	説明
Cisco Cisco Secure Firewall Threat Defense	シスコの次世代ファイアウォール。ドキュメントでは、この名前が「Cisco Secure Firewall Threat Defense」または「脅威に対する防御」と略されることがよくあります。次のデバイスマネージャで設定および管理できます。 • クラウド提供型 Firewall Management Center。 • オンプレミスの Secure Firewall Management Center。 • Threat Defense イメージに含まれるローカルデバイスマネージャ。
クラウド提供型 Firewall Management Center	これは、Security Cloud Control とともに展開された Secure Firewall Management Center のバージョンを指します。 クラウド提供型 Firewall Management Center は、1 つ以上の Cisco Secure Firewall Threat Defense ファイアウォールを管理します。 クラウド提供型 Firewall Management Center は、製品ドキュメントで「Management Center」として参照されている場合があります。 **これらのリリースノートには、 このマネージャに関する情報が記載されています。**
オンプレミスの Cisco Secure Firewall Management Center	1 つ以上の Cisco Secure Firewall Threat Defense デバイスを管理します。 これらのデバイスは、製品ドキュメントで「Cisco Secure Firewall Management Center」または単に「Management Center」として参照されている場合があります。 オンプレミスの Cisco Secure Firewall Management Center は、お客様が管理し、一部のイメージは物理 Firepower アプライアンスにインストールするように設計されていますが、その他のイメージはお客様のプライベートクラウドにインストールおよび管理される仮想イメージです。インストールおよびアップグレードタスクはお客様が実行します。

製品名	説明
Cisco Secure Firewall Threat Defense デバイスマネージャ	このマネージャは、Cisco Secure Threat Defense ソフトウェアイメージとともに提供され、提供された単一の Cisco Secure Threat Defense デバイスのみを管理します。 CDO は、デバイスマネージャによって管理され、ローカル管理用に構成された Threat Defense デバイスを管理できます。 Threat Defense デバイスの管理タスクは、CDO またはデバイスマネージャで実行できます。CDO は、どのマネージャがどのタスクを実行したかを追跡し、CDO ユーザーに変更元に関するアラートを表示します。 CDO によってデバイスマネージャで管理される Threat Defense デバイスは、クラウド提供型 Firewall Management Center では管理できません。 Cisco Defense Orchestrator のドキュメントでは、デバイスマネージャによって管理される Threat Defense デバイスを「FDM 管理対象デバイス」または「FDM」と呼んでいます。



第 2 章

クラウド提供型 Firewall Management Center 2024 の新機能

Security Cloud Control の概要

Cisco Defense Orchestrator は「Cisco Security Cloud Control」になりました。

Security Cloud Control は、ネットワークセキュリティから始めて、Cisco Security Cloud を統合するように設計された新しい人工知能組み込みの管理機能ソリューションであり、更新されたユーザーインターフェイス、共通サービス、およびセキュリティクラウド全体の設定、ログやアラートを接続するサービスメッシュを備えた最新のマイクロアプリ アーキテクチャです。

Cisco Secure Firewall Threat Defense と ASA ファイアウォール、Multicloud Defense、および Hypershield を管理し、それらの管理機能を追加のセキュリティ製品に拡張します。さらに、Cisco AI Assistant はポリシーと設定をプロアクティブに最適化し、問題を検出してトラブルシューティングします。

次の Security Cloud Control の新機能を確認してください。

- ネットワーク セキュリティ ソリューションの一元管理エクスペリエンス
- 脅威に対する防御のデバイスを迅速にオンボーディングし、新機能を発見するのに役立つガイド付きの「Day 0」エクスペリエンス
- すべての管理対象デバイスをエンドツーエンドで可視性化する統合ダッシュボード

- アップグレードされたメニューナビゲーションと簡単なネットワークおよびセキュリティアプリケーションへのアクセスにより、合理化されたソリューションのユーザビリティ
- ファイアウォールルールの作成と管理を容易にする 人工知能アシスタント
- AIOps Insights による運用のシンプル化と強化されたセキュリティ
- セキュリティ態勢を改善し、不良構成を排除し、ルールを最適化するためのポリシー分析。
- 一貫したポリシーの適用とオブジェクト共有により強化されたハイブリッド環境での保護
- リモートアクセスおよびサイト間 VPN 接続のモニタリングの改善
- 1 つのテナントで最大 1,000 ファイアウォールをサポートするための拡張性の向上

詳細については、Security Cloud Control の製品ページ、Security Cloud Control のドキュメント、および『Cisco Security Cloud Control のよくある質問（FAQ）』を参照してください。

2024 年 12 月 13 日

表 *2*：バージョン *20241127* の機能

機能	最小の Threat Defense	詳細
ライセンシング機能		
評価ライセンスへの更新	7.6.0	クラウド提供型 Firewall Management Center で 90 日間の評価ライセンスが提供されるようになりました。この期間が経過した後も、脅威防御デバイスをオンボーディングできますが、クラウド提供型 Firewall Management Center が Cisco Smart Software Manager に登録されるまで展開はブロックされます。評価期間の有効期限が近づくと、Security Cloud Control でアラート通知を受信します。 参照：「ライセンス」

2024 年 11 月 8 日

表 *3*：バージョン *20241030* の機能

機能	最小の Threat Defense	詳細
プラットフォーム		

機能	最小の Threat Defense	詳細
Cisco Secure Firewall 1200	7.6.0	Cisco Secure Firewall 1200 が導入されました。これには、次のモデルが含まれます。 • Cisco Secure Firewall 1210CX（1000BASE-T ポート X 8） • Cisco Secure Firewall 1210CP（1000BASE-T ポート X 8）。ポート 1/5 ～ 1/8 は、Power on Ethernet（PoE）をサポートします。 • Cisco Secure Firewall 1220CX（1000BASE-T ポート X 8、SFP+ ポート X 2）。 Cisco Secure Firewall CSF-1210CE、CSF-1210CP、および CSF-1220CX Hardware Installation Guideを参照してください。
Firepower 1000 および Cisco Secure Firewall 3100/4200 の前面パネル USB-A ポートを無効にします。	7.6.0	Firepower 1000 および Cisco Secure Firewall 3100/4200 の前面パネル USB-A ポートを無効にできるようになりました。デフォルトでは、ポートは有効になっています。 新規/変更された Threat Defense CLI コマンド：**system support usb show**、**system support usb port disable**、**system support usb port enable** マルチインスタンスモードの Cisco Secure Firewall 3100 の新規/変更された FXOS CLI コマンド： **show usb-port**、**disable USB port**、**enable usb-port** 参照：Cisco Secure Firewall Threat Defense コマンドリファレンスおよびCisco Firepower 4100/9300 FXOS Command Reference
デバイス管理		

機能	最小の Threat Defense	詳細
デバイステンプレート。	7.4.1	デバイステンプレートを使用すると、事前にプロビジョニングされた初期デバイス設定（ゼロタッチプロビジョニング）を使用して、複数のブランチデバイスを展開できます。また、インターフェイス設定が異なる複数のデバイスに設定変更を適用し、既存のデバイスから設定パラメータを複製することもできます。 制約事項：デバイステンプレートを使用して、デバイスをサイト間 VPN トポロジのスポークとして設定できますが、ハブとして設定することはできません。デバイスは、複数のハブアンドスポークサイト間 VPN トポロジの一部にすることができます。 新規/変更された画面：**[デバイス（Devices）]**>**[テンプレート管理（Template Management）]** サポートされるプラットフォーム：Firepower 1000/2100、Cisco Secure Firewall 1200/3100。Firepower 2100 のサポートは Threat Defense 7.4.1 ～ 7.4.x のみであることに注意してください。これらのデバイスはバージョン 7.6.0 を実行できません。 参照：「Device Management Using Device Templates」および「*Onboard Threat Defense Devices using Device Templates to Cloud-delivered Firewall Management Center using Zero-Touch Provisioning*」[英語]
ユーザー定義の VRF インターフェイスの場合は AAA。	7.6.0	デバイスの認証、許可、およびアカウンティング（AAA）は、ユーザー定義の Virtual Routing and Forwarding（VRF）インターフェイスでサポートされるようになりました。デフォルトでは管理インターフェイスを使用します。 デバイスプラットフォームの設定で、VRF インターフェイスを持つセキュリティゾーンまたはインターフェイスグループを、設定済みの外部認証サーバーに関連付けることが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）]**>**[プラットフォーム設定（Platform Settings）]** > **[外部認証（External Authentication）]** 参照：プラットフォームの外部認証用の仮想ルータ認識インターフェイスの有効化

機能	最小の Threat Defense	詳細
アクセス制御のポリシーアナライザとオプティマイザ並列起動。	任意（Any）	ポリシーアナライザとオプティマイザは、冗長ルールやシャドウルールなどの異常に対するアクセス コントロール ポリシーを評価し、検出された異常を修正するアクションを実行できます。 アクセス コントロール ポリシー ページから直接ポリシーアナライザおよびオプティマイザを起動できるようになりました。**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** をクリックしてポリシーを選択し、[ポリシーの分析（Analyze Policies）] をクリックします。
高可用性/拡張性		
Cisco Secure Firewall 4200 のマルチインスタンスモード。	7.6.0	Cisco Secure Firewall 4200 でマルチインスタンスモードがサポートされるようになりました。 参照：Cisco Secure Firewall 3100/4200 のマルチインスタンスモード
Cisco Secure Firewall 3100/4200 の Management Center でのマルチインスタンスモード変換。	7.6.0	アプリケーションモードのデバイスを Management Center に登録し、CLI を使用せずにマルチインスタンスモードに変換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）]** > > **[マルチインスタンスに変換（Convert to Multi-Instance）]** • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[一括アクションの選択（Select Bulk Action）]** > **[マルチインスタンスに変換（Convert to Multi-Instance）]**
Cisco Secure Firewall 3100/4200 の16 ノードクラスタ	7.6.0	Cisco Secure Firewall 3100 および 4200 では、最大ノード数が 8 から 16 に増加しました。 参照：Cisco Secure Firewall 3100/4200 のクラスタリング

機能	最小の Threat Defense	詳細
Cisco Secure Firewall 3100/4200 クラスタの個別インターフェイスモード。	7.6.0	個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル IP アドレスを持ちます。各インターフェイスのメインクラスタ IP アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。アップストリームスイッチ上でロードバランシングを別途する必要があります。 制限事項：コンテナインスタンスではサポートされていません。 新規/変更された画面： • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタの追加（Add Cluster）] • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [インターフェイス/EIGRP/OSPF/OSPFv3/BGP（Interfaces / EIGRP / OSPF / OSPFv3 / BGP）]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレスプール（Address Pools）] > [MACアドレスプール（MAC Address Pool）]** 参照：Cisco Secure Firewall 3100/4200 のクラスタリングおよびアドレスプール
複数の AWS 可用性ゾーンへの Threat Defense Virtual クラスタの展開。	7.6.0	AWS リージョン内の複数の可用性ゾーンに Threat Defense Virtual クラスタを展開できるようになりました。これにより、ディザスタリカバリ中に継続的なトラフィック検査と動的拡張（AWS 自動拡張）が可能になります。 AWS への Threat Defense Virtual クラスタの展開を参照してください。

機能	最小の Threat Defense	詳細
GWLB を使用して、AWS の Threat Defense Virtual をツーアームモードで展開します。	7.6.0	GWLB を使用して、AWS の Threat Defense Virtual をツーアームモードで展開できるようになりました。これにより、ネットワークアドレス変換（NAT）を実行しながら、トラフィック インスペクション後にインターネットに向かうトラフィックを直接転送できます。ツーアームモードは、シングルおよびマルチ VPC 環境でサポートされます。 制限事項：クラスタリングではサポートされていません。 Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。
インターフェイス		
Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開します。	7.4.1	Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開できるようになりました。以前は、1 つの管理インターフェイス、1 つの診断インターフェイス、および少なくとも 2 つのデータインターフェイスが必要でした。新しいインターフェイスの要件： • Azure：管理 1、データ 2（最大 8） • GCP：管理 1、データ 3（最大 8） 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
SD-WAN		
SD-WAN ウィザード。	ハブ：7.6.0 スポーク：7.3.0	新しいウィザードを使用すると、中央の本社とリモートのブランチサイト間の VPN トンネルを簡単に設定できます。 新規/変更された画面：**[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]** > **[追加（Add）]** > **[SD-WAN トポロジ（SD-WAN Topology）]** 参照：SD-WAN ウィザードを使用した SD-WAN トポロジの設定
アクセス制御：脅威の検出とアプリケーションの識別		

機能	最小の Threat Defense	詳細
QUIC 復号。	Snort 3 搭載の 7.6.0	QUIC プロトコルで実行されているセッションに適用する復号ポリシーを設定できます。QUIC 復号はデフォルトで無効になっています。復号ポリシーごとに QUIC 復号を選択的に有効にし、QUIC トラフィックに適用する復号ルールを作成できます。QUIC 接続を復号することで、システムは侵入、マルウェア、またはその他の問題について接続を検査できます。また、アクセス コントロール ポリシーの特定の基準に基づいて、復号された QUIC 接続のきめ細かい制御とフィルタリングを適用することもできます。 復号ポリシーの [詳細設定（Advanced Settings）] が変更され、QUIC 復号を有効にするオプションが含まれるようになりました。 参照：復号ポリシーの詳細オプション
Snort ML：ニューラル ネットワーク ベースのエクスプロイト検出器。	Snort 3 搭載の 7.6.0	新しい Snort 3 インスペクタ snort_ml は、ニューラル ネットワーク ベースの機械学習（ML）を使用して既知の攻撃と 0-day 攻撃を検出します。複数のプリセットルールは必要ありません。インスペクタは HTTP イベントにサブスクライブし、HTTP URI を検出します。検出された HTTP URI は、エクスプロイト（現在は SQL インジェクションに限定されています）を検出するためにニューラルネットワークによって使用されます。新しいインスペクタは現在、最大検出を除くすべてのデフォルトポリシーで無効になっています。 新しい侵入ルール GID:411 SID:1 は、snort_ml が攻撃を検出するとイベントを生成します。このルールも現在、最大検出を除くすべてのデフォルトポリシーで無効になっています。 Snort 3 インスペクタ リファレンスを参照してください。

機能	最小の Threat Defense	詳細
Cisco Talos に、トラフィックを使用した Advanced Threat Hunting とインテリジェンス収集の実施を許可します。	Snort 3 搭載の 7.6.0	**アップグレードの影響。アップグレードすると、テレメトリが有効になります。** 脅威ハンティングテレメトリを有効にすることで、Talos（シスコの脅威インテリジェンスチーム）が脅威の状況をより包括的に理解する助けになります。この機能により、特別な侵入ルールからのイベントが Talos に送信され、攻撃分析、インテリジェンス収集、およびより優れた保護戦略の策定に役立ちます。この設定は、新規およびアップグレードされた展開ではデフォルトで有効になっています。 新規/変更された画面：[システム（System）]（⚙）> **[設定（Configuration）] > [侵入ポリシー設定（Intrusion Policy Preferences）] > [Talos脅威ハンティングテレメトリ（Talos Threat Hunting Telemetry）]** 参照：侵入ポリシーの設定
アクセス制御：アイデンティティ		
Microsoft AD のパッシブ ID エージェント。	いずれか	この機能が導入されます。 パッシブ ID エージェントのアイデンティティソースは、Microsoft Active Directory（AD）から Management Center にセッションデータを送信します。パッシブ ID エージェントソフトウェアは、以下でサポートされています。 • Microsoft AD サーバー（Windows Server 2008 以降） • Microsoft AD ドメインコントローラ（Windows Server 2008 以降） • モニタリングするドメインに接続されている任意のクライアント（Windows 8 以降） 参照：パッシブ ID エージェントによるユーザー制御。

機能	最小の Threat Defense	詳細
pxGrid クラウド アイデンティティ ソース。		Cisco Identity Services Engine（Cisco ISE） pxGrid クラウド アイデンティティ ソースを使用すると、クラウド提供型 Firewall Management Center アクセスコントロールルールで Cisco ISE からのサブスクリプションとユーザーデータを使用できるようになります。 pxGrid クラウドアイデンティティ ソース によって、ISE からの絶えず変化するダイナミックオブジェクトの使用が可能になり、クラウド提供型 Firewall Management Center でのアクセス コントロール ポリシーによるユーザー制御に使用できます。 新規/更新された画面：**[統合（Integration）] > [その他の統合（Other Integrations）] > [アイデンティティ ソース（Identity Sources）] > [アイデンティティ サービス エンジン（pxGrid Cloud）（Identity Services Engine (pxGrid Cloud)）]** 参照：pxGrid クラウド アイデンティティ ソースによるユーザー制御
Cisco Secure 動的属性コネクタ の新しいコネクタ	任意	Cisco Secure 動的属性コネクタ は、AWS セキュリティグループ、AWS サービスタグ、および Cisco Cyber Vision をサポートするようになりました。 バージョンの制限：オンプレミス Cisco Secure 動的属性コネクタ 統合の場合、バージョン 3.0 が必要です。 「Amazon Web Services Connector—About User Permissions and Imported Data」[英語] を参照してください。

機能	最小の Threat Defense	詳細
アクティブまたはパッシブ認証用の Microsoft Azure AD レルム。	アクティブ：Snort 3 搭載の 7.6.0 パッシブ：Snort 3 搭載の 7.4.1	アクティブおよびパッシブ認証に Microsoft Azure Active Directory（AD）レルムを使用できるようになりました。 • Azure AD を使用したアクティブ認証：Azure AD をキャプティブポータルとして使用します。 • Cisco ISE を使用したパッシブ認証（バージョン 7.4.0 で導入）：Management Center は Azure AD からグループを取得し、ISE からログイン ユーザー セッション データを取得します。 SAML（セキュリティ アサーション マークアップ言語）を使用して、サービスプロバイダー（認証要求を処理するデバイス）とアイデンティティ プロバイダー（Azure AD）の間に信頼関係を確立します。アップグレードされた Management Center の場合、既存の Azure AD レルムは SAML - Azure AD レルムとして表示されます。 **アップグレードの影響**。アップグレード前に Microsoft Azure AD レルムを設定していた場合は、パッシブ認証用に設定された SAML - Azure AD レルムとして表示されます。以前のすべてのユーザーセッションデータは保持されます。 新規/変更された画面：**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** > **[レルムを追加（Add Realm）]** > **[SAML - Azure AD]** 新規/変更された CLI コマンド：なし 参照：Microsoft Azure AD（SAML）レルムの作成。
イベントロギングおよび分析		

機能	最小の Threat Defense	詳細
接続イベントに含まれる MITRE およびその他のエンリッチメント情報。	Snort 3 搭載の 7.6.0	接続イベントの MITRE およびその他のエンリッチメント情報により、検出された脅威のコンテキスト情報に簡単にアクセスます。これには、Talos および暗号化された可視性エンジン（EVE）からの情報が含まれます。EVE エンリッチメントの場合は、EVE を有効にする必要があります。 接続イベントには、統合イベントビューアと従来のイベントビューアの両方で使用可能な 2 つの新しいフィールドがあります。 • [MITRE ATT&CK]：進行グラフをクリックすると、戦術や手法を含む脅威の詳細の拡張ビューが表示されます。 • [その他のエンリッチメント（Other Enrichment）]：クリックすると、EVE からの情報など、利用可能なその他のエンリッチメント情報が表示されます。 新しい Talos 接続ステータス正常性モジュールは、この機能に必要な Talos を使用して Management Center の接続をモニターします。必要な特定のインターネットリソースについては、「Internet Access Requirements」を参照してください。 「Configure EVE」[英語] を参照してください。
管理		
Management Center の新しいテーマ。、	任意（Any）	クラウド提供型 Firewall Management Center を効率よく使用するために、左側に新しいナビゲーションを導入し、インターフェイスのルックアンドフィールを更新しました。

2024 年 8 月 23 日

表 *4 :* バージョン *20240808* の機能

機能	最小の Threat Defense	詳細
プラットフォーム		

機能	最小の Threat Defense	詳細
Threat Defense バージョン 7.6.0 のサポート。	7.6.0	バージョン 7.6.0 を実行している Threat Defense デバイスを管理できるようになりました。 （注） Firepower 2100 は、バージョン 7.6.0 で廃止されました。バージョン 7.0.3 ～ 7.4.x を実行しているデバイスは引き続き管理できますが、アップグレードはできません。最新バージョンをカバーする単一の設定ガイドがあるため、古いデバイスでのみサポートされている機能については、使用している Threat Defense バージョンに一致するオンプレミス Management Center のガイドを参照してください。 （注） クラウド提供型 Firewall Management Center はオンプレミス Management Center よりも広範な管理対象デバイスのバージョンをサポートしているため、バージョン 7.0.x デバイスで分析にオンプレミス Management Center を使用している場合、可能であれば、デバイスをバージョン 7.2.x 以降にアップグレードすることを推奨します。アップグレードすると、最新リリースを実行しているデバイスを追加しながら、古いデバイスからイベントを取得できます。詳細については、サポート終了：すべての Threat Defense デバイスの分析専用機能。を参照してください。
高可用性/拡張性		

機能	最小の Threat Defense	詳細
Cisco Secure Firewall 3100 のマルチインスタンスモード。	7.4.1	Secure Firewall 3100 は、単一のデバイス（アプライアンスモード）または複数のコンテナインスタンス（マルチインスタンスモード）として展開できます。マルチインスタンスモードでは、完全に独立したデバイスとして機能する複数のコンテナインスタンスを 1 つのシャーシに展開できます。マルチインスタンスモードでは、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレード対象（シャーシのアップグレード）になることに注意してください。 新規/変更された画面： • **[インベントリ（Inventory）] > [FTDシャーシ（FTD Chassis）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [シャーシマネージャ（Chassis Manager）]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [新しいポリシー（New Policy）] > [シャーシプラットフォーム設定（Chassis Platform Settings）]** • **[デバイス（Devices）] > [シャーシのアップグレード（Chassis Upgrade）]** 新規/変更された Threat Defense CLI コマンド：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新規/変更された FXOS CLI コマンド：**create device-manager**、**set deploymode** プラットフォームの制限：Cisco Secure Firewall 3105 ではサポートされていません。 参照：「Use Multi-Instance Mode for the Secure Firewall」および「クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド」
アクセス制御：脅威の検出とアプリケーションの識別		

機能	最小の Threat Defense	詳細
機密性の高い、復号できないトラフィックの復号を簡単にバイパスできます。	任意	機密性の高い、復号できないトラフィックの復号を簡単にバイパスできるようになりました。これにより、ユーザーが保護され、パフォーマンスが向上します。 新しい復号ポリシーには、事前定義されたルールが含まれるようになりました。このルールを有効にすると、機密URLカテゴリ（金融や医療など）、復号できない識別名、および復号できないアプリケーションの復号を自動的にバイパスできます。識別名とアプリケーションは通常、復号不能なTLS/SSL証明書のピン留めを使用するため、復号できません。 アウトバウンド復号の場合は、ポリシーの作成の一環としてこれらのルールを有効または無効化にします。インバウンド復号の場合、ルールはデフォルトで無効になっています。ポリシーを作成した後、ルール全体を編集、並べ替え、または削除できます。 新規/変更された画面：**[ポリシー（Policies）]>[アクセス制御（Access Control）]>[復号（Decryption）]>[復号ポリシーの作成（Create Decryption Policy）]** 参照：復号ポリシーの作成 参照：復号ポリシーの作成
アクセス制御：アイデンティティ		
ユーザー ID ソースとしての Microsoft Azure AD。	7.4.2	Microsoft Azure Active Directory（Azure AD）レルムと ISE を使用すると、ユーザーを認証したりユーザー制御のためにユーザーセッションを取得したりできます。 新規/変更された画面： • [統合（Integration）]>[その他の統合（Other Integrations）]>[レルム（Realms）]>[レルムを追加（Add Realm）]>[Azure AD（Azure AD）] • [統合（Integration）]>[その他の統合（Other Integrations）]>[レルム（ Realms）]>[アクション（Actions）]（ユーザーのダウンロード、コピー、編集、削除など） サポートされている ISE バージョン：3.0 パッチ 5 以降、3.1（任意のパッチレベル）、3.2（任意のパッチレベル） 参照：「Microsoft Azure Active Directory レルムの作成」
ヘルス モニタリング		

機能	最小の Threat Defense	詳細
アラートなしで正常性データを収集します。	任意（Any）	正常性データの収集を続行しながら、ASP ドロップ、CPU、およびメモリ正常性モジュールの正常性アラートや正常性アラートサブタイプを無効にできるようになりました。これにより、正常性アラートのノイズを最小限に抑え、最も重大な問題に集中できます。 新規/変更された画面：正常性ポリシー（[システム（System）]（⚙） **[正常性ポリシー（Health Policy）]**）には、ASP ドロップ（脅威防御のみ）、CPU、およびメモリの正常性アラートのサブタイプを有効または無効にするチェックボックスが追加されました。 参照：正常性ポリシー
デバイス登録時にデフォルトの正常性ポリシーを適用します。	任意（Any）	デバイス登録時に適用するデフォルトの正常性ポリシーを選択できるようになりました。[正常性ポリシー（Health Policy）] ページでは、ポリシー名によってどれがデフォルトであるかが示されます。特定のデバイスの登録後に別のポリシーを使用する場合は、そこで変更します。デフォルトのデバイス正常性ポリシーは削除できません。 新規/変更された画面：[システム（System）]（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]** > [その他（More）]（⋮） > **[デフォルトとして設定（Set as Default）]** 参照：デフォルトの正常性ポリシーの設定

機能	最小の Threat Defense	詳細
Firepower 4100/9300 のシャーシレベルのヘルスアラート。	7.4.1	シャーシを読み取り専用デバイスとして Management Center に登録することで、Firepower 4100/9300 のシャーシレベルのヘルスアラートを表示できるようになりました。また、Firewall Threat Defense プラットフォーム障害のヘルスモジュールを有効にして、ヘルスポリシーを適用する必要があります。アラートは、メッセージセンター、ヘルスモニター（左側のペインの [デバイス（Devices）] でシャーシを選択）、およびヘルスイベントビューに表示されます。 マルチインスタンスモードで Cisco Secure Firewall 3100 のシャーシを追加し、正常性アラートを表示することもできます。これらのデバイスの場合は、Management Center を使用してシャーシを管理します。ただし、Firepower 4100/9300 シャーシの場合は、シャーシマネージャまたは FXOS CLI を使用する必要があります。 新規/変更された画面：**[インベントリ（Inventory）] > [FTD シャーシ（FTD Chassis）]** 参照：シャーシのオンボーディング
管理		
Threat Defense の高可用性は、バックアップから復元した後に自動的に再開されます。	7.6.0	高可用性ペアで障害が発生したユニットを交換する場合、復元が完了してデバイスが再起動した後に、高可用性を手動で再開する必要がなくなりました。ただし引き続き、展開する前に、高可用性が再開されたことを確認することは必要です。 バージョンの制限：Threat Defense バージョン 7.0 ～ 7.0.7、7.1.x、7.2.0 ～ 7.2.9、7.3.x、または 7.4.0 ～ 7.4.2 ではサポートされていません。 参照：Restore Security Cloud Control-Managed Devices
変更管理チケットの引き継ぎ、承認ワークフローのその他の機能。	任意（Any）	別のユーザーのチケットを引き継ぐことができるようになりました。これは、チケットがポリシーに対する他の更新をブロックしており、ユーザーが使用できない場合に役立ちます。 これらの機能が承認ワークフローに含まれるようになりました：復号ポリシー、DNS ポリシー、ファイルおよびマルウェアポリシー、ネットワーク検出、証明書および証明書グループ、暗号スイートリスト、識別名オブジェクト、シンクホールオブジェクト。 参照：「Change Management」
トラブルシューティング		

機能	最小の Threat Defense	詳細
CPU とルールプロファイラを使用して Snort 3 のパフォーマンスの問題をトラブルシュートします。	Snort 3 搭載の 7.6.0	新しい CPU とルールプロファイラは、Snort 3 のパフォーマンスの問題のトラブルシュートに役立ちます。以下をモニタリングできるようになりました。 • Snort 3 モジュール/インスペクタがパケットを処理するために要した CPU 時間。 • 各モジュールが消費している CPU リソース（Snort 3 プロセスによって消費された合計 CPU と比較）。 • Snort 3 が CPU を大量に消費している時に、パフォーマンスが不十分なモジュール。 • パフォーマンスが不十分な侵入ルール。 新規/変更された画面：**[デバイス（Devices）]**>**[トラブルシュート（Troubleshoot）]** > **[Snort 3プロファイリング（Snort 3 Profiling）]** プラットフォームの制限：コンテナインスタンスではサポートされていません。 参照：Advanced Troubleshooting for the Secure Firewall Threat Defense Device 参照：Advanced Troubleshooting for the Secure Firewall Threat Defense Device
廃止された機能		

機能	最小の Threat Defense	詳細
サポート終了：すべての Threat Defense デバイスの分析専用機能。	任意	

機能	最小の Threat Defense	詳細
		バージョン 7.0.x デバイスで分析にオンプレミス Management Center を使用している場合、可能であれば、デバイスをバージョン 7.2.x 以降にアップグレードすることを推奨します。アップグレードすると、最新リリースを実行しているデバイスを追加しながら、古いデバイスからイベントを取得できます。 クラウド提供型 Firewall Management Center はオンプレミス Management Center よりも広範な管理対象デバイスのバージョンをサポートしているため、分析にオンプレミス Management Center を使用する場合、共同管理するデバイスが「古すぎる」または「新しすぎる」ために問題が発生することがあります。 次のことを防ぐことができます。 • Management Center のアップグレードが古いデバイスによってブロックされているため、新しいデバイスが Analytics Management Center に登録される。 • Analytics Management Center が古いリリースで「スタック」しているため、共同管理デバイスが最新リリースにアップグレードされる。 • デバイスのアップグレードを元に戻した場合に、デバイスの Analytics Management Center との互換性が失われる。 例として、共同管理バージョン 7.0.x のデバイスが現在含まれている展開に、共同管理バージョン 7.6.0 のデバイスを追加するシナリオについて考えます。クラウド提供型 Firewall Management Center は該当範囲のデバイスをすべて管理できますが、オンプレミス Analytics Management Center は管理できません。 優先順位に従って、次のことができます。 • バージョン 7.0.x のデバイスをバージョン 7.2.0 以降にアップグレードし、Analytics Management Center をバージョン 7.6.0 にアップグレードしてから、バージョン 7.6.0 のデバイスを両方の Management Center に追加します。 • Analytics Management Center からバージョン 7.0.x のデバイスを削除し、Analytics Management Center をバージョン 7.6.0 にアップグレードしてから、バージョン 7.6.0 のデバイスを両方の Management Center に追加します。 • Analytics Management Center はそのままにして、バージョ

機能	最小の Threat Defense	詳細
		ン 7.6.0 のデバイスは追加しないでください。 次の選択肢があります。 • すべてのデバイスからイベントを取得するには、Analytics Management Center と古いデバイスをアップグレード（または交換）します。 • 古いデバイスからのイベントを除外するには、Analytics Management Center のみをアップグレード（または交換）します。 • 新しいデバイスからのイベントを除外するには、Analytics Management Center を古いリリースのままにします。

2024 年 6 月 6 日

Cisco AI Assistant を使用したファイアウォール管理

CDO 管理者は、Cisco Defense Orchestrator（CDO）の Cisco AI Assistant とクラウド提供型 Firewall Management Center の統合により、Cisco Secure Firewall Threat Defense ポリシーをより効率的に管理し、ドキュメントにアクセスできるようになりました。Cisco AI Assistant には、いくつかの主要な機能があります。

- [事前有効化アシスタント（Pre-Enabled Assistant）]：Cisco AI Assistant は、すべての CDO テナントでデフォルトで有効になっています。必要に応じて、テナントの[一般設定（General Settings）] ページで無効化できます。
- [容易なアクセス（Easy Access）]：CDO のネットワーク管理者と管理者は、ロギング後にテナントのダッシュボードの上部にあるメニューバーから Cisco AI Assistant に直接アクセスできます。

- [ユーザーオリエンテーション（User Orientation）]：Cisco AI Assistant ウィジェットを初めて開くとカルーセルウィンドウが表示され、Cisco AI Assistant の紹介、データプライバシー保護に関する説明、効果的な使用に関するヒントが提供されます。
- [ポリシールールアシスタンス（Policy Rule Assistance）]：Cisco AI Assistant は、Cisco Secure Firewall Threat Defense デバイスでポリシールールの作成プロセスを簡素化します。管理者は、簡単なプロンプトを使用してアクセス制御ルールを迅速に作成できます。

- [製品ナレッジリソース（Product Knowledge Resource）]：Cisco AI Assistant には、CDO とクラウド提供型のファイアウォール管理のドキュメントが取り込まれており、サポートが必要な場合は、質問できます。
- **ユーザーフレンドリーなインターフェイス**：
  - [シンプルテキスト入力ボックス（Simple Text Input Box）]：ウィンドウの下部にあり、Cisco AI Assistant を簡単に操作できます。
  - [スレッド履歴（Thread History）]：Cisco AI Assistant に尋ねる質問や一連の質問は、スレッドと呼ばれます。Cisco AI Assistant にはスレッド履歴が保持されるため、自分の過去の質問を参照できます。
  - [フィードバック（Feedback）]：Cisco AI Assistant の応答に対する高評価または低評価のフィードバックを提供します。

詳細については、『Cisco AI Assistant ユーザーガイド』を参照してください。

2024 年 5 月 30 日

表 *5*：バージョン *20240514* の機能

機能	最小の Threat Defense	詳細
プラットフォームの移行		
クラスタ化された脅威に対する防御デバイスをオンプレミス Management Center から クラウド提供型 Firewall Management Center に移行します。	7.0.6 7.2.1	クラスタ化された 脅威に対する防御 デバイスは、オンプレミス Management Center から クラウド提供型 Firewall Management Center に移行するときに、残りの設定とともに移行されるようになりました。 参照：Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center [英語]
展開とポリシー管理		
変更管理。	任意（Any）	変更を展開する前の監査追跡や正式な承認など、設定変更に関してより正式なプロセスを実装する必要がある組織の場合は、変更管理を有効にできます。 この機能を有効にするために、[システム（System）]（⚙）>**[設定（Configuration）]**>**[変更管理（Change Management）]** ページが追加されました。有効にすると、[システム（System）]（⚙）>**[変更管理ワークフロー（Change Management Workflow）]** ページが表示され、メニューに新しい [チケット（Ticket）]（📋）のクイックアクセスアイコンが表示されます。 参照：「Change Management」

2024 年 4 月 2 日

このリリースでは、安定性、ハードニング、パフォーマンスの機能強化が導入されています。

2024 年 2 月 13 日

表 *6* : バージョン *20240203* の機能

機能	最小の Threat Defense	詳細
プラットフォーム		
Threat Defense バージョン 7.4.1 のサポート。	7.4.1	バージョン 7.4.1 を実行している Threat Defense デバイスを管理できるようになりました。
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	7.4.1	Cisco Secure Firewall 3130 および 3140 は次のネットワークモジュールをサポートするようになりました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド
Firepower 9300 ネットワークモジュール用の光トランシーバ。	7.4.1	Firepower 9300 は、次の光トランシーバをサポートするようになりました。 • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR 以下のネットワークモジュールでサポート： • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G 参照：Cisco Firepower 9300 ハードウェア設置ガイド
Cisco Secure Firewall 3100 のパフォーマンスプロファイルのサポート。	7.4.1	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 3100 に適用されるようになりました。以前は、この機能は Firepower 4100/9300、Cisco Secure Firewall 4200、および Threat Defense Virtual でサポートされていました。 参照：「Configure the Performance Profile」
NAT		

機能	最小の Threat Defense	詳細
NAT ルールの編集時にネットワークグループを作成します。	いずれか	NAT ルールの編集時に、ネットワークオブジェクトに加えてネットワークグループを作成できるようになりました。 参照：「複数のデバイスの NAT ルールのカスタマイズ」
デバイス管理		
ユーザー定義の VRF インターフェイスでサポートされるデバイス管理サービス。	いずれか	Threat Defense プラットフォーム設定（NetFlow、SSH アクセス、SNMP ホスト、syslog サーバー）で設定されたデバイス管理サービスが、ユーザー定義の Virtual Routing and Forwarding（VRF）インターフェイスでサポートされるようになりました。 プラットフォームの制限：コンテナインスタンスまたはクラスタ化されたデバイスではサポートされていません。 「Platform Settings」を参照
SD-WAN		
Cisco SD-WAN サマリーダッシュボード	7.4.1	WAN サマリーダッシュボードには、WAN デバイスとデバイスのインターフェイスのスナップショットが表示されます。また、WAN ネットワーク、デバイス正常性に関する情報、インターフェイス接続、アプリケーションスループット、および VPN 接続に関するインサイトが表示されます。WAN リンクを監視し、予防的かつ迅速な回復措置を実行できます。さらに、[アプリケーションモニタリング（Application Monitoring）] タブを使用して、WAN インターフェイス アプリケーションのパフォーマンスを監視することもできます。 新規/変更された画面：**[分析（Analysis）]** > **[Cisco SD-WANサマリー（SD-WAN Summary）]** 参照：「Cisco SD-WAN サマリーダッシュボード」
アクセス制御：アイデンティティ		

機能	最小の Threat Defense	詳細
複数の Active Directory レルム（レルムシーケンス）のキャプティブ ポータル サポート。	7.4.1	**アップグレードの影響。カスタム認証フォームの更新。** LDAP レルム、Microsoft Active Directory レルム、またはレルムシーケンスに対してアクティブ認証を設定できます。さらに、レルムまたはレルムシーケンスを使用してアクティブ認証にフォールバックするパッシブ認証ルールを設定できます。必要に応じて、アクセス制御ルールで同じ ID ポリシーを共有する管理対象デバイス間でセッションを共有できます。 さらに、以前にアクセスしたデバイスとは別の管理対象デバイスを使用してシステムにアクセスするときに、ユーザーに再認証を要求するオプションがあります。 HTTP 応答ページ認証タイプを使用する場合は、Threat Defense をアップグレードした後、カスタム認証フォームに **`<select name="realm" id="realm"></select>`** を追加する必要があります。これにより、ユーザーはレルムを選択できます。 制限事項：Microsoft Azure Active Directory ではサポートされていません。 新規/変更された画面： • **[ポリシー（Policies）] > [アイデンティティ（Identity）] >（ポリシーの編集）> [アクティブ認証（Active Authentication）] > [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** • **[IDポリシー（Identity policy）]>（編集）> [ルールの追加（Add Rule）]> [パッシブ認証（Passive Authentication）] > [レルムと設定（Realms & Settings）] > [パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）]** • **[IDポリシー（Identity policy）]>（編集）> [ルールの追加（Add Rule）]> [アクティブ認証（Active Authentication）] > [レルムと設定（Realms & Settings）] > [パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）]** 参照：「How to Configure the Captive Portal for User Control」

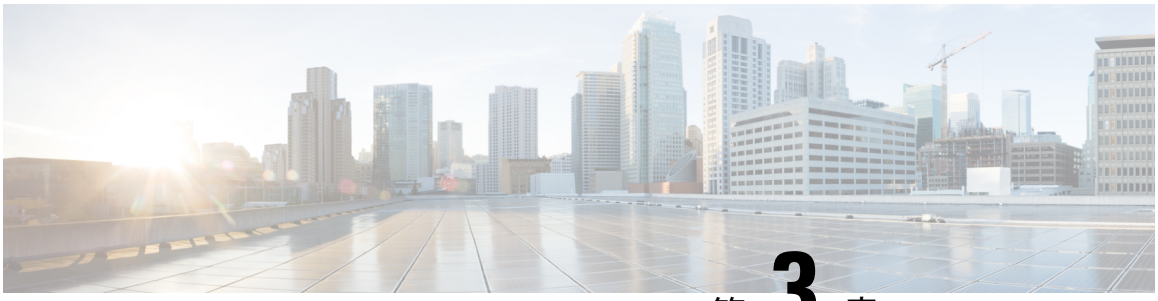
機能	最小の Threat Defense	詳細
ファイアウォール全体でキャプティブポータルアクティブ認証セッションを共有します。	7.4.1	以前に接続していたデバイスとは異なる管理対象デバイスに認証セッションが送信されたときに、ユーザーの認証が必要かどうかを決定します。ユーザーがロケーションまたはサイトを変更するたびに認証する必要がある組織の場合は、このオプションを無効にする必要があります。 • (デフォルト) 有効にすると、ユーザーはアクティブな認証アイデンティティルールに関連付けられた管理対象デバイスで認証できます。 • アクティブな認証ルールが展開されている別の管理対象デバイスでユーザーがすでに認証されている場合でも、別の管理対象デバイスでの認証をユーザーに要求する場合は無効にします。 新規/変更された画面：**[ポリシー（Policies）]>[アイデンティティ（Identity）]>（ポリシーの編集）>[アクティブ認証（Active Authentication）]>[ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** 参照：「How to Configure the Captive Portal for User Control」
展開とポリシー管理		
前回の展開以降の設定変更に関するレポートを表示および生成します。	任意（Any）	前回の展開以降の設定変更に関する次のレポートを生成、表示、および（zip ファイルとして）ダウンロードできます。 • ポリシー内の追加、変更、または削除、あるいはデバイスに展開されるオブジェクトをプレビューする各デバイスのポリシー変更レポート。 • ポリシー変更レポート生成のステータスに基づいて各デバイスを分類する統合レポート。 これは、のアップグレード後に特に役立ち、展開する前にアップグレードによって加えられた変更を確認できます。 新規/変更された画面：**[展開（Deploy）]>[高度な展開（Advanced Deploy）]**。 参照：「Download Policy Changes Report for Multiple Devices」
推奨リリースの通知。	任意（Any）	新しい推奨リリースが利用可能になると、Management Center から通知されるようになりました。今すぐアップグレードしない場合は、後でシステムに通知するか、次の推奨リリースまでリマインダを延期できます。新しいアップグレードページには、推奨リリースも示されます。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）

機能	最小の Threat Defense	詳細
Threat Defense のアップグレードウィザードからの復元の有効化。	任意（Any）	脅威防御アップグレードウィザードからの復元を有効化できます。 その他のバージョンの制限：Threat Defense をバージョン 7.2 以降にアップグレードする必要があります。 参照：クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。	任意（Any）	Threat Defense アップグレードウィザードの最終ページで、アップグレードの進行状況をモニターできるようになりました。この機能は、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブおよび Management Center の既存のモニタリング機能に追加されます。新しいアップグレードフローを開始していない限り、**[デバイス（Devices）]**>**[Threat Defense アップグレード（Threat Defense Upgrade）]**によってこのウィザードの最後のページに戻り、現在の（または最後に完了した）デバイスのアップグレードの詳細なステータスを確認できます。 参照：クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
FXOS アップグレードに含まれるファームウェアのアップグレード。	任意（Any）	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。マルチインスタンスモードの Cisco Secure Firewall 3100（バージョン 7.4.1 の新機能）には、FXOS とファームウェアのアップグレードもバンドルされています。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド
アップグレード		

機能	最小の Threat Defense	詳細
アップグレードの開始ページとパッケージ管理が改善されました。	任意（Any）	新しいアップグレードページでは、アップグレードの選択、ダウンロード、管理、および展開全体への適用が容易になります。このページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。パッケージを選択してシスコから簡単に直接ダウンロードしたり、パッケージを手動でアップロードおよび削除したりできます。 適切なメンテナンスリリースのアプライアンスが少なくとも 1 つある（またはパッチを手動でアップロードした）場合を除き、パッチは表示されません。ホットフィックスは手動でアップロードする必要があります。 新規/変更された画面： • [システム（System）]（⚙）>**[製品のアップグレード（Product Upgrades）]** では、デバイスをアップグレードし、アップグレードパッケージを管理します。 • [システム（System）]（⚙）>**[コンテンツの更新（Content Updates）]** で、侵入ルール、VDB、およびGeoDB を更新できるようになりました。 • **[デバイス（Devices）]** > **[脅威防御のアップグレード（Threat Defense Upgrade）]** を選択すると、脅威防御のアップグレードウィザードに直接移動します。 廃止された画面/オプション： • [システム（System）]（⚙）>**[更新（Updates）]** は廃止されました。脅威防御アップグレードはすべてウィザードを使用するようになりました。 • 脅威防御アップグレードウィザードの [アップグレードパッケージの追加（Add Upgrade Package）] ボタンは、新しいアップグレードページへの [アップグレードパッケージの管理（Manage Upgrade Packages）] リンクに置き換えられました。 参照：クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
管理		
ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。	任意（Any）	Management Center では、ソフトウェアアップグレードパッケージの直接ダウンロードの場所が sourcefire.com から amazonaws.com に変更されています。 参照：「Internet Access Requirements」

機能	最小の Threat Defense	詳細
スケジュール済みタスクでは、パッチおよびVDB更新のみダウンロードされます。	任意（Any）	[最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、[システム（System）]（⚙）>**[製品のアップグレード（Product Upgrades）]** を使用します。 参照：「Software Update Automation」
メモリが少ない Snort 2 デバイス用の小規模 VDB。	すべて（Snort 2）	VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB（別称：*VDB lite*）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 メモリが少ないデバイス：ASA-5508-X および ASA 5516-X 参照：「Update the Vulnerability Database」
廃止された機能		
廃止：FlexConfig を使用した DHCP リレーの信頼できるインターフェイス。	任意（Any）	Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。 参照：「Configure the DHCP Relay Agent」
廃止：ダウンロード可能なアクセス制御リストと、FlexConfig を使用した RADIUS アイデンティティソースのシスコ属性値ペア ACL のマージ。	任意（Any）	この機能は、Management Center の Web インターフェイスでサポートされるようになりました。
廃止：イベント正常性アラートの頻繁なドレイン。	7.4.1	[ディスク使用量（Disk Usage）] 正常性モジュールは、イベントの頻繁なドレインでアラートを生成しなくなりました。も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをバージョン 7.4.1 以降にアップグレードする（アラートの送信を停止する）まで、アラートが表示され続ける場合があります。 参照：「Disk Usage and Drain of Events Health Monitor Alerts」

2024 年 2 月 13 日



第 3 章

クラウド提供型 Firewall Management Center 2023 の新機能

2023 年 11 月 30 日

表 *7*：新機能：バージョン *20231117*

機能	Threat Defense の最小バージョン要件	詳細
管理		
クラウド提供型 Firewall Management Center での Cisco Secure Firewall Threat Defense デバイスバックアップのスケジュール	任意	クラウド提供型 Firewall Management Center を使用して、管理する Cisco Secure Firewall Threat Defense デバイスのスケジュール済みバックアップを実行します。 詳細については、「Schedule Remote Device Backups」[英語] を参照してください。

2023 年 10 月 19 日

表 *8* : 新機能：バージョン *20230929*

機能	Threat Defense の最小バージョン要件	詳細
プラットフォーム		
Threat Defense バージョン 7.4.0 のサポート。	7.4.0	バージョン 7.4.0 を実行している Threat Defense デバイスを管理できるようになりました。 バージョン 7.4.0 は、Cisco Secure Firewall 4200 でのみ使用できます。バージョン 7.4.0 が必要な機能には、Cisco Secure Firewall 4200 を使用する必要があります。他のすべてのプラットフォームのサポートは、バージョン 7.4.1 で再開されます。
Cisco Secure Firewall 4200。	7.4.0	Cisco Secure Firewall 4215、4225、および 4245 を クラウド提供型 Firewall Management Center で管理できるようになりました。 これらのデバイスは、以下の新しいネットワークモジュールをサポートしています。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR4K-XNM-2X100G） • 4 ポート 200G QSFP+ ネットワークモジュール（FPR4K-XNM-4X200G） 参照： Cisco Secure Firewall 4215、4225、4245 ハードウェア設置ガイド
Cisco Secure Firewall 4200 のパフォーマンスプロファイルのサポート。	7.4.0	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 4200 に適用されるようになりました。以前は、この機能は Firepower 4100/9300 および Threat Defense Virtual でのみサポートされていました。 参照：「Configure the Performance Profile」
クラウド提供型のファイアウォール管理システムの番号付け規則。	任意	クラウド提供型のファイアウォール管理システムは、CDO の機能です。トラブルシューティングのために、[FMCサービス（FMC Services）] ページでクラウド提供型 Firewall Management Center のバージョン番号を特定します。 参照：「View Services Page Information」[英語]。
プラットフォームの移行		

機能	Threat Defense の最小バージョン要件	詳細
Firepower 1000/2100 から Cisco Secure Firewall 3100 への移行。	任意（Any）	Firepower 1000/2100 から Cisco Secure Firewall 3100 に設定を簡単に移行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）] > [移行（Migrate）]** プラットフォームの制限：Firepower 1010 または 1010E からの移行はサポートされていません。 参照：新しいモデルへの設定の移行。

機能	Threat Defense の最小バージョン要件	詳細
Firepower Management Center 1000/2500/4500 からクラウド提供型 Firewall Management Center へのデバイスの移行。	任意（Any）	

機能	Threat Defense の最小バージョン要件	詳細
		Firepower Management Center 1000/2500/4500 から クラウド提供型 Firewall Management Centerにデバイスを移行できます。 デバイスを移行するには、オンプレミス Management Center をバージョン 7.0.3（7.0.5 を推奨）からバージョン 7.4.0 に一時的にアップグレードする必要があります。バージョン 7.0 の Management Center ではクラウドへのデバイスの移行がサポートされていないため、この一時的なアップグレードが必要です。さらに、バージョン 7.0.3 以降（7.0.5 を推奨）を実行しているスタンドアロンおよび高可用性 Threat Defense デバイスのみが移行の対象となります。クラスタの移行は現時点ではサポートされていません。 **重要** バージョン 7.4.0 は、移行プロセス中に 1000/2500/4500 でのみサポートされます。Management Center のアップグレードとデバイスの移行までの間隔は最小限に抑える必要があります。 移行プロセスを要約すると、次のようになります。 **1.** アップグレードと移行の準備をします。リリースノート、アップグレードガイド、および移行ガイドに記載されているすべての前提条件を読み、理解し、条件を満たしてください。 アップグレードする前に、古い Management Center の「移行準備ができている」こと、つまり、移行するデバイスのみ管理していること、設定の影響（VPN の影響など）を評価していること、新たに展開されていて、完全にバックアップされていること、すべてのアプライアンスが正常な状態であることなどが特に重要です。 また、クラウドテナントのプロビジョニング、ライセンス付与、および準備もする必要があります。これには、セキュリティ イベント ロギングの方法を含める必要があります。サポートされていないバージョンが実行されるため、分析のためにオンプレミス Management Center を保持することはできません。 **2.** オンプレミス Management Center とそのすべての管理対象デバイスを少なくともバージョン 7.0.3 にアップグレードします（バージョン 7.0.5 を推奨）。 すでに最小バージョンを実行している場合は、この手順をスキップできます。 **3.** オンプレミス Management Center をバージョン 7.4.0 にアップグレードします。 アップグレードパッケージを解凍し（ただし、展開はしない）、Management Center

機能	Threat Defense の最小バージョン要件	詳細
		にアップロードします。Special Release からダウンロードします。 4. オンプレミス Management Center を CDO にオンボードします。 5. 移行ガイドの説明に従って、すべてのデバイスをオンプレミス Management Center から クラウド提供型 Firewall Management Center に移行します。 移行するデバイスを選択する場合は、[オンプレミスFMCからFTDを削除する（Delete FTD from On-Prem FMC）] を選択してください。変更をコミットするか、14 日が経過するまで、デバイスは完全には削除されないことに注意してください。 6. 移行が成功したことを確認します。 移行しても期待どおりに機能しない場合は、14 日以内に戻すことができます。戻さない場合は自動的にコミットされます。ただし、バージョン 7.4.0 は一般的な操作ではサポートされていないことに注意してください。オンプレミス Management Center をサポートされているバージョンに戻すには、再移行したデバイスを削除し、バージョン 7.0.x に再イメージ化し、バックアップから復元して、デバイスを再登録する必要があります。 参照： • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • オンプレミス Management Center 管理対象 Cisco Secure Firewall Threat DefenseFirepower Threat Defense のクラウド提供型 Firewall Management Center への移行 移行プロセスの任意の時点で質問がある場合、またはサポートが必要な場合は、Cisco TAC にお問い合わせください。
FTD からクラウドへの移行における S2S VPN のサポート。VPN ポリシーを使用して Threat Defense デバイスをオンプレミスから クラウド提供型 Firewall Management Center に移行します。	7.0.3 ～ 7.0.x 7.2 以降	Cisco Secure Firewall Threat Defense デバイスのサイト間 VPN 設定は、デバイスがオンプレミスの Firewall Management Center からクラウド提供型 Firewall Management Center に移行されるときに、残りの設定とともに移行されるようになりました。 参照：Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center [英語]
インターフェイス		

機能	Threat Defense の最小バージョン要件	詳細
マージされた管理インターフェイスと診断インターフェイス。	7.4.0	

機能	Threat Defense の最小バージョン要件	詳細
		アップグレードの影響。 アップグレード後にインターフェイスをマージします。 7.4 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。 7.4 以降にアップグレードした場合： • 診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 • 診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。 マージモードでは、デフォルトでデータルーティングテーブルを使用するようにAAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。 プラットフォーム設定の場合、これは次のことを意味します。 • 診断インターフェイスで、HTTP、ICMP、または SMTP を有効にすることはできなくなりました。 • SNMP については、診断インターフェイスではなく管理インターフェイスでホストを許可できます。 • Syslog サーバーについては、診断インターフェイスではなく管理インターフェイスでアクセスできます。 • Syslog サーバーまたは SNMP ホストのプラットフォーム設定で診断インターフェイスが名前で指定されている場合、マージされたデバイスとマージされていないデバイスに別々のプラットフォーム設定ポリシーを使用する必要があります。 • インターフェイスを指定しない場合、DNS ルックアップは管理専用ルーティングテーブルにフォールバックしなくなりました。 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）]** 新規/変更されたコマンド： **show management-interface convergence**

機能	Threat Defense の最小バージョン要件	詳細
		参照：「Merge the Management and Diagnostic Interfaces」
VXLAN VTEP IPv6 のサポート。	7.4.0	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 は、Threat Defense Virtual クラスタ制御リンクまたは Geneve カプセル化ではサポートされていません。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [VTEP] > [VTEPの追加（Add VTEP）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Devices）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** 参照：「Configure Geneve Interfaces」
BGP および管理トラフィックのループバックインターフェイスのサポート。	7.4.0	AAA、BGP、DNS、HTTP、ICMP、IPsec フローオフロード、NetFlow、SNMP、SSH、および syslog にループバック インターフェイスを使用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）] > [デバイスの編集（Edit Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [ループバックインターフェイス（Loopback Interface）] 参照：「Configure Loopback Interfaces」
ループバックおよび管理タイプのインターフェイス グループ オブジェクト。	7.4.0	管理専用インターフェイスまたはループバック インターフェイスのみを含むインターフェイス グループ オブジェクトを作成でき、作成したグループを DNS サーバー、HTTP アクセス、SSH などの管理機能に使用できます。ループバックグループは、ループバック インターフェイスを利用できるすべての機能で使用できますが、DNS では管理インターフェイスはサポートされていない点に注意してください。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）] > [追加（Add）] > [インターフェイスグループ（Interface Group）]** 参照：「Interface」
高可用性/拡張性		

機能	Threat Defense の最小バージョン要件	詳細
Threat Defense の高可用性のための「誤フェールオーバー」の削減。	7.4.0	その他のバージョンの制限：Threat Defense バージョン 7.3.x ではサポートされていません。 参照：「Heartbeat Module Redundancy」
SD-WAN		
HTTP パスのモニタリングを使用したポリシーベースのルーティング。	7.2.0	ポリシーベースルーティング（PBR）は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集された評価指標（RTT、ジッター、パケット損失、および MOS）を使用できるようになりました。インターフェイスの HTTP ベースのアプリケーション モニタリング オプションは、デフォルトで有効になっています。モニタリング対象のアプリケーションが搭載され、パスを決定するためのインターフェイスの順序付けを行う一致 ACL を使用して、PBR ポリシーを設定できます。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [インターフェイスの編集（Edit interface）] > [パスモニタリング（Path Monitoring）] > [HTTPベースのアプリケーション モニタリングの有効化（Enable HTTP based Application Monitoring）] チェックボックス。 プラットフォームの制限：クラスタ化されたデバイスではサポートされていません。 参照：「Configure Path Monitoring Settings」
ユーザー ID と SGT を使用したポリシーベースのルーティング。	7.4.0	ユーザーとユーザーグループ、および PBR ポリシーの SGT に基づいてネットワークトラフィックを分類できるようになりました。PBR ポリシーの拡張 ACL を定義するときに、ID および SGT オブジェクトを選択します。 新規/変更された画面：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）] > [拡張アクセスリストの追加/編集（Add/Edit Extended Access List）] > [拡張アクセスリストエントリの追加/編集（Add/Edit Extended Access List Entry）] > [ユーザー（Users）] および [セキュリティグループタグ（Security Group Tag）] 参照：「Configure Extended ACL Objects」
VPN		

機能	Threat Defense の最小バージョン要件	詳細
Cisco Secure Firewall 4200 向け VTI ループバックインターフェイスの IPSec フローのオフロード。	7.4.0	Cisco Secure Firewall 4200 では、VTI ループバックインターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされます。以前は、この機能は Secure Firewall 3100 の物理インターフェイスでサポートされていました。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 その他の要件：FPGA ファームウェア 6.2 以降 参照：「IPSec Flow Offload」
Cisco Secure Firewall 4200 の暗号デバッグの機能拡張。	7.4.0	暗号デバッグの機能拡張は次のとおりです。 • 暗号アーカイブは、テキスト形式とバイナリ形式で使用できるようになりました。 • 追加の SSL カウンタをデバッグに使用できます。 • スタックした暗号化ルールは、デバイスを再起動せずに ASP テーブルから削除できます。 新規/変更された CLI コマンド： **show counters** 参照：「Troubleshooting Using Crypto Archives」
VPN：リモートアクセス		

機能	Threat Defense の最小バージョン要件	詳細
Secure Client のメッセージ、アイコン、画像、接続/切断スクリプトをカスタマイズします。	7.2.0	Secure Client をカスタマイズして、それらのカスタマイズを VPN ヘッドエンドに展開できるようになりました。サポートされている Secure Client のカスタマイズは次のとおりです。 • GUI テキストとメッセージ • アイコンとイメージ • スクリプト • バイナリ • Customized Installer Transforms • Localized Installer Transforms エンドユーザーが Secure Client から接続すると、Threat Defense によりそれらのカスタマイズがエンドポイントに配布されます。 新規/変更された画面： • [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [Secure Clientのカスタマイズ（Secure Client Customization）] • [デバイス（Device）] > [リモートアクセス（Remote Access）] > [VPNポリシーの編集（Edit VPN policy）] > [詳細設定（Advanced）] > [Secure Client のカスタマイズ（Secure Client Customization）] 参照：「Customize Secure Client」
VPN：サイト間		

機能	Threat Defense の最小バージョン要件	詳細
NAT 変換からサイト間 VPN トラフィックを簡単に免除します。	任意（Any）	サイト間 VPN トラフィックを NAT 変換から簡単に免除できるようになりました。 新規/変更された画面： • エンドポイントの NAT 免除の有効化：**[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [サイト間VPNの追加/編集（Add/Edit Site to Site VPN）] > [エンドポイントの追加/編集（Add/Edit Endpoint）] > [ネットワークアドレス変換からVPNトラフィックを免除する（Exempt VPN traffic from network address translation）]** • NAT ポリシーのないデバイスの NAT 免除ルールの表示：**[デバイス（Devices）] > [NAT] > [NAT免除（NAT Exemptions）]** • 単一デバイスの NAT 免除ルールの表示：**[デバイス（Devices）] > [NAT] > [Threat Defense NATポリシー（Threat Defense NAT Policy）] > [NAT免除（NAT Exemptions）]** 参照：「NAT Exemption」
VPN ノードの IKE および IPsec セッションの詳細を簡単に表示できます。	任意（Any）	サイト間 VPN ダッシュボードで、VPN ノードの IKE および IPsec セッションの詳細を使いやすい形式で表示できます。 新規/変更された画面：[概要（Overview）] > [サイト間VPN（Site to Site VPN）] の順に選択し、[トンネルステータス（Tunnel Status）] ウィジェットの下で、トポロジにカーソルを合わせて [表示（View）] をクリックし、[CLIの詳細（CLI Details）] タブをクリックします。 参照：「サイト間 VPN モニタリング」
アクセス制御：脅威の検出とアプリケーションの識別		
機密データの検出とマスキング。	7.4.0（Snort 3）	**アップグレードの影響。 デフォルトポリシーの新しいルールが有効になります。** 社会保障番号、クレジットカード番号、E メールなどの機密データは、インターネットに意図的に、または誤って漏洩される可能性があります。機密データの検出は、機密データの漏洩の可能性を検出してイベントを生成するために使用され、大量の個人識別情報（PII）データが転送された場合にのみイベントを生成します。機密データの検出では、組み込みパターンを使用して、イベントの出力で PII をマスクできます。 データマスキングの無効化はサポートされていません。 参照：「Custom Rules in Snort 3」

機能	Threat Defense の最小バージョン要件	詳細
クライアントレスの Zero Trust アクセス。	7.4.0（Snort 3）	Zero Trust アクセスが導入され、外部の SAML ID プロバイダー（IdP）ポリシーを使用して、ネットワークの内部（オンプレミス）または外部（リモート）から保護された Web ベースのリソース、アプリケーション、またはデータへのアクセスを認証および承認できます。 設定では、ゼロトラスト アプリケーション ポリシー、アプリケーショングループ、およびアプリケーションを指定します。 新規/変更された画面： • **[ポリシー（Policies）] > [Zero Trustアプリケーション（Zero Trust Application）]** • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** • **[概要（Overview）] > [ダッシュボード（Dashboard）] > [Zero Trust]** 新規/変更された CLI コマンド： • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** 参照：「Zero Trust Access」
ルーティング		
IPv6 ネットワークで BGP のグレースフルリスタートを構成します。	7.3.0	管理対象デバイスのバージョン 7.3 以降の IPv6 ネットワークに対しては、BGP グレースフルリスタートを設定できます。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）] > [BGP] > [IPv6] > [ネイバー（Neighbor）] > [ネイバーの追加/編集（Add/Edit Neighbor）]。 参照：「Configure BGP Neighbor Settings」

機能	Threat Defense の最小バージョン要件	詳細
動的 VTI による仮想ルーティング。	7.4.0	ルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを設定できるようになりました。 新規/変更された画面：[使用可能なインターフェイス（Available Interfaces）] の下の [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）] > [仮想ルータのプロパティ（Virtual Router Properties）] > [ダイナミックVTIインターフェイス（Dynamic VTI interfaces）]。 プラットフォームの制限：ネイティブモードのスタンドアロンまたは高可用性デバイスでのみサポートされます。コンテナインスタンスやクラスタ化されたデバイスではサポートされていません。 参照：「About Virtual Routers and Dynamic VTI」
アクセス制御：脅威の検出とアプリケーションの識別		
暗号化された可視性エンジン機能の拡張。	7.4.0（Snort 3）	暗号化された可視性エンジン（EVE）で、次のことができるようになりました。 • 脅威スコアに基づいて暗号化トラフィック内の悪意のある通信をブロックする。 • EVE で検出されたプロセスに基づいてクライアント アプリケーションを判断する。 • 検出のために、フラグメント化された Client Hello パケットを再構成する。 新規/変更された画面：アクセス コントロール ポリシーの詳細設定を使用して EVE を有効にし、これらの設定を行います。 参照：「Encrypted Visibility Engine」

機能	Threat Defense の最小バージョン要件	詳細
特定のネットワークとポートをエレファントフローのバイパスまたはスロットリングから免除します。	7.4.0（Snort 3）	エレファントフローのバイパスまたはスロットリングから特定のネットワークとポートを免除できるようになりました。 新規/変更された画面： • アクセス コントロール ポリシーの詳細設定でエレファントフロー検出を構成するときに、[エレファントフローの修復（Elephant Flow Remediation）] オプションを有効にすると、[ルールの追加（Add Rule）] をクリックして、バイパスまたはスロットリングから免除するトラフィックを指定できるようになりました。 • システムがバイパスまたはスロットリングから免除されているエレファントフローを検出すると、[エレファントフローが免除されました（Elephant Flow Exempted）] という理由でフロー中接続イベントを生成します。 プラットフォームの制限：Firepower 2100 シリーズではサポートされていません。 参照：「Elephant Flow Detection」
JavaScript インスペクションの改善。	7.4.0（Snort 3）	JavaScript を正規化し、正規化されたコンテンツに対してルールを照合することで実行される JavaScript インスペクションを改善しました。 参照：「HTTP Inspect Inspector」および Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語]
アクセス制御：アイデンティティ		
Management Center の Cisco Secure 動的属性コネクタ。	いずれか	Management Center の Cisco Secure Dynamic Attributes コネクタを設定できるようになりました。以前は、スタンドアロン アプリケーションとしてのみ使用できました。 参照：「Cisco Secure Dynamic Attributes コネクタ」
イベントロギングおよび分析		

機能	Threat Defense の最小バージョン要件	詳細
Management Center の Web インターフェイスから、Threat Defense デバイスを NetFlow エクスポータとして設定できます。	いずれか	NetFlow は、パケットフローの統計情報を提供するシスコアプリケーションの 1 つです。Management Center の Web インターフェイスを使用して、Threat Defense デバイスを NetFlow エクスポータとして設定できるようになりました。既存の NetFlow FlexConfig があり、Web インターフェイスで設定をやり直す場合は、廃止された FlexConfig を削除するまで展開できません。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[Threat Defense設定ポリシー（Threat Defense Settings policy）]** > **[NetFlow]** 参照：「Configure NetFlow」
ヘルス モニタリング		
新しい ASP ドロップメトリック。	7.4.0	新規または既存のデバイス正常性ダッシュボードに、600 を超える新しい ASP（高速セキュリティパス）ドロップメトリックを追加できます。[ASP ドロップ（ASP Drops）] メトリックグループを選択していることを確認します。 新規/変更された画面：[システム（System）]（⚙）>**[正常性（Health）]**>**[モニター（Monitor）]** > **[デバイス（Device）]** 参照：「show asp drop Command Usage」
管理		
証明書の失効を確認する際の IPv6 URL のサポート。	7.4.0	以前は、Threat Defense は IPv4 OCSP URL のみをサポートしていました。現在、Threat Defense は IPv4 と IPv6 の両方の OCSP URL をサポートしています。 参照：「 Certificate Enrollment Object Revocation Options」
Threat Defense のバックアップファイルはリモートの安全な場所に保存してください。	任意	デバイスをバックアップすると、クラウド提供型 Firewall Management Center は、そのセキュアなクラウドストレージにバックアップファイルを保存します。 参照：「Backup/Restore」[英語]
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		

機能	Threat Defense の最小バージョン要件	詳細
ユーザービリティの拡張。	いずれか	次の作業に進んでください。 • [システム（System）]（⚙）>**[スマートライセンス（Smart Licenses）]** から Threat Defense クラスタのスマートライセンスを管理します。以前は、[デバイス管理（Device Management）] ページを使用する必要がありました。 参照：クラスタリングのライセンス • メッセージセンター通知のレポートをダウンロードします。メッセージセンターで、[通知を表示（Show Notifications）] スライダの横にある新しい [レポートのダウンロード（Download Report）] アイコンをクリックします。 参照：システムメッセージの管理 • すべての登録済みデバイスのレポートをダウンロードします。**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**に移動し、ページの右上にある新しい [デバイスリストレポートのダウンロード（Download Device List Report）] リンクをクリックします。 参照：管理対象デバイスリストのダウンロード • カスタム ヘルス モニタリング ダッシュボードを簡単に作成し、既存のダッシュボードを簡単に編集できます。 参照：「Correlating Device Metrics」
Secure Firewall 4200 のパケットキャプチャでキャプチャするトラフィックの方向を指定します。	7.4.0	Secure Firewall 4200 では、 コマンドで新しい**direction**キーワード**capture**を使用できます。 新規/変更された CLI コマンド：**capture***capture_name***switchinterface***interface_name* [**direction** {**both** | **egress** | **ingress**}] 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Management Center REST API		
クラウド提供型 Firewall Management Center REST API	機能に依存	Management Center REST API の変更については、API クイックスタートガイドの「What's New」を参照してください。

表 *9* : 廃止された機能：バージョン *20230929*

機能	Threat Defense では廃止	詳細
廃止：FlexConfig を使用した NetFlow。	任意（Any）	Management Center の Web インターフェイスから、Threat Defense デバイスを NetFlow エクスポータとして設定できるようになりました。この設定をすると、廃止された FlexConfig を削除するまで展開できません。 参照：「Configure NetFlow」
廃止：アンマネージドディスク使用率が高いアラート。	7.0.6 7.2.4 7.4.0	ディスク使用状況モジュールは、管理対象外のディスク使用率が高い場合にアラートを出さなくなりました。正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスを 7.0.6、7.2.4、または 7.4 にアップグレードする（アラートの送信を停止する）まで、これらのアラートが表示され続ける場合があります。 残りのディスク使用量アラートについては、「Disk Usage and Drain of Events Health Monitor Alerts」を参照してください。

2023 年 8 月 3 日

表 *10* : 新機能：*2023* 年 *8* 月 *3* 日

機能	説明
Firewall 移行ツールの更新	CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Cisco Secure Firewall ASA デバイスの複数のコンテキストをルーテッドモードインスタンスにマージし、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスに移行できるようになりました。さらに、移行ツールは、Virtual Routing and Forwarding（VRF）機能を活用して、マルチコンテキストの Cisco ASA 環境で観察される分離されたトラフィックフローを複製できるようになりました。複製されたフローは新たにマージされた設定の一部になります。 詳細については、Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行ガイド [英語] の「Migrating Secure Firewall ASA Managed by CDO」を参照してください。

2023 年 7 月 20 日

表 *11* : 新機能：*2023* 年 *7* 月 *20* 日

機能	説明
GCP によって管理される仮想 脅威防御 デバイスの EasyDeploy	仮想 脅威に対する防御 デバイスを作成し、Google Cloud Platform（GCP）プロジェクトに同時に展開できるようになりました。EasyDeploy メソッドでは、新しい仮想デバイスを作成し、デバイスをクラウド環境に関連付けるために必要な手順を組み合わせることで、手順が合理化され、セットアップに必要な時間が最小限に抑えられます。 オンボーディングフローでは、クラウド提供型 Firewall Management Center を有効にする**必要があります**。詳細については、「Deploy a Threat Defense Device to Google Cloud Platform」[英語] を参照してください。 必要最低限の Threat Defense： • 7.0.3 および 7.0.x 以降のバージョン • 7.2 以降のバージョン

2023 年 6 月 8 日

表 *12* : 新機能：*2023* 年 *6* 月 *8* 日

機能	説明
AWS または Azure を使用した Cisco Secure Firewall Threat Defense の EasyDeploy	AWS または Azure 環境で同時に Cisco Secure Firewall Threat Defense デバイスを作成して展開できるようになりました。Security Cloud Control でデバイスをオンボードし、クラウド提供型 Firewall Management Center で環境を管理します。詳細については、「Deploy a Threat Defense Device with AWS」[英語] および「Deploy a Threat Defense Device with an Azure VNet」[英語] をそれぞれ参照してください。 必要最低限の Threat Defense： • 7.0.3 および 7.0.x 以降のバージョン • 7.2 以降のバージョン

2023 年 5 月 25 日

表 13 : 新機能：2023 年 5 月 25 日

機能	説明
Threat Defense バージョン 7.3.1 のサポート。	バージョン 7.3.1 を実行している Threat Defense デバイスを管理できるようになりました。
Firepower 1010E。	Power over Ethernet（PoE）をサポートしていない Firepower 1010E を クラウド提供型 Firewall Management Center で管理できるようになりました。 必要最低限の Threat Defense：7.2.3

2023 年 3 月 9 日

このリリースでは、安定性、ハードニング、パフォーマンスの機能強化が導入されています。

2023 年 2 月 16 日

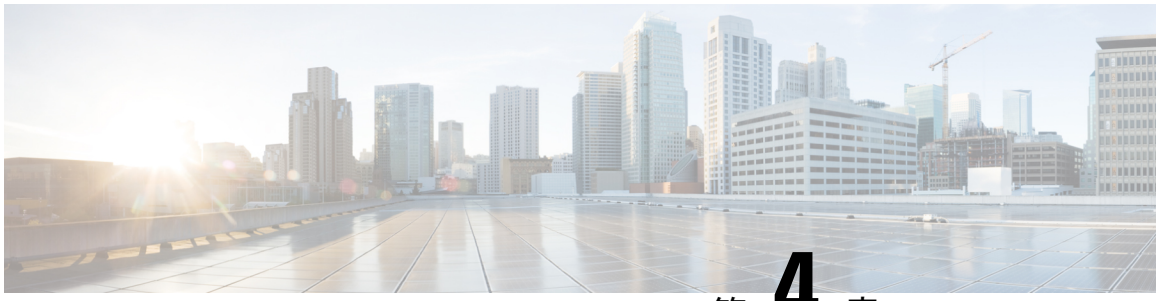
このリリースでは、安定性、ハードニング、パフォーマンスの機能強化が導入されています。

2023 年 1 月 18 日

表 14 : 新機能：2023 年 1 月 18 日

機能	説明
Remote Access VPN	

機能	説明
CDO でリモートアクセス VPN セッションを監視します。	CDO を使用して、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイス上の RA VPN セッションを監視できるようになりました。アクティブなセッションと履歴セッションのリスト、および各セッションに関連付けられているデバイスとユーザーの詳細を確認できます。 サポートされている Threat Defense のバージョン： • 7.0.3 および 7.0.x 以降のバージョン • 7.2 以降のバージョン 詳細については、コンフィギュレーション ガイドの「Monitor Remote Access VPN Sessions」を参照してください。



第 4 章

クラウド提供型 Firewall Management Center 2022 の新機能

2022 年 12 月 13 日

表 *15 :* 新機能：*2022* 年 *12* 月 *13* 日

機能	説明
CDO へのオンボーディングと Threat Defense のアップグレード	
追加のデバイスサポートとオンボーディング	クラスタ化されたデバイス、AWS VPC 環境、および Azure VNet 環境を クラウド提供型 Firewall Management Center にオンボードできるようになりました。現在、これらのデバイスのオンボーディングにはログイン情報が必要です。クラスタ化されたデバイスは、指定された管理プラットフォームですでに形成されている必要があります。詳細については、https://docs.defenseorchestrator.com で次のトピックを参照してください。 • クラスタのオンボード • AWS VPC に関連付けられたデバイスをオンボードします。 • Azure VNet 環境のオンボード

機能	説明
Threat Defense の無人アップグレード	脅威に対する防御 アップグレードウィザードは、新しい [無人モード（Unattended Mode）] メニューを使用して無人アップグレードをサポートするようになりました。アップグレードするターゲットバージョンとデバイスを選択し、いくつかのアップグレードオプションを指定して、その場から離れるだけです。ログアウトしたり、ブラウザを閉じたりすることもできます。 無人アップグレードを使用すると、システムは自動的に必要なアップグレードパッケージをデバイスにコピーし、互換性チェックと準備状況チェックを実行してアップグレードを開始します。ウィザードを手動でステップ実行する場合と同様に、アップグレードのステージに「合格」しなかったデバイス（たとえば、チェックの失敗）は、次のステージに含まれません。アップグレードが完了したら、検証とアップグレード後のタスクを開始します。 コピーフェーズとチェックフェーズの間に無人モードを一時停止して再開できます。ただし、無人モードを一時停止しても、進行中のタスクは停止しません。開始されたコピーとチェックは完了するまで実行されます。同様に、無人モードを停止して進行中のアップグレードをキャンセルすることはできません。アップグレードをキャンセルするには、[デバイス管理（Device Management）] ページの [アップグレード（Upgrade）] タブおよびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。 Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド [英語] の「Upgrade Threat Defense」を参照してください。

機能	説明
Snort 3 への自動アップグレード	脅威に対する防御 をバージョン 7.3 以降にアップグレードすると、[Snort 2からSnort 3にアップグレードする（Upgrade Snort 2 to Snort 3）] オプションは無効化できなくなります。ソフトウェアのアップグレード後、設定を展開すると、対象となるすべてのデバイスが Snort 2 から Snort 3 にアップグレードされます。個々のデバイスを元に戻すことはできますが、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスが自動アップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。 移行のサポートについては、Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語] を参照してください。
Firepower 4100/9300 の CDO 管理対象 Cisco Secure Firewall Threat Defense デバイス	Firepower 4100/9300 は柔軟なセキュリティ プラットフォームで、1 つ以上の論理デバイスをインストールできます。Threat Defense を Management Center に追加する前に、Cisco Secure Firewall シャーシマネージャまたは FXOS CLI を使用して、シャーシインターフェイスを設定し、論理デバイスを追加し、Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。 デバイスの作成時にマネージャとして CDO を設定することにより、Firepower 4100/9300 で CDO 管理対象のスタンドアロンの論理 Threat Defense デバイスを作成できるようになりました。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Configure Logical Devices」を参照してください。
インターフェイス	

機能	説明
IPv6 DHCP の機能拡張	Dynamic Host Configuration Protocol（DHCP）は、IP アドレスなどのネットワーク設定パラメータを DHCP クライアントに提供します。Threat Defense デバイスは、Threat Defense デバイスインターフェイスに接続されている DHCP クライアントに DHCP サーバーを提供できます。DHCP サーバは、ネットワーク構成パラメータを DHCP クライアントに直接提供します。 クラウド提供型 Firewall Management Center で Cisco Secure Firewall Threat Defense デバイスに対する IPv6 アドレッシングの次の機能がサポートされるようになりました。 • DHCPv6 アドレスクライアント：Threat Defense は、DHCPv6 サーバーから IPv6 グローバルアドレスとオプションのデフォルトルートを取得します。 • DHCPv6 プレフィックス委任クライアント：Threat Defense は DHCPv6 サーバーから委任プレフィックスを取得します。また、取得したプレフィックスを使用して他の Threat Defense インターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータアドバタイズメント。 • DHCPv6 ステートレスサーバー：SLAAC クライアントが Threat Defense に情報要求（IR）パケットを送信すると、Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。 詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Configure IPv6 Addressing」を参照してください。

機能	説明
ループバック インターフェイスのサポート	ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェアインターフェイスであり、IPv4 および IPv6 アドレスを持つ複数の物理インターフェイスを介して到達できます。 静的および動的 VTI VPN トンネルの冗長性のためにループバック インターフェイスを設定できます。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Regular Firewall Interfaces」を参照してください。
Azure ゲートウェイロードバランサの Threat Defense Virtual のペアプロキシ VXLAN	Azure ゲートウェイ ロードバランサ（GWLB）で使用するために、Azure の 脅威に対する防御 Virtual のペアプロキシモード VXLAN インターフェイスを設定できます。脅威に対する防御 Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Clustering for Threat Defense Virtual in a Public Cloud」を参照してください。
冗長マネージャ アクセス データ インターフェイス	マネージャアクセスにデータインターフェイスを使用しているときに、プライマリインターフェイスがダウンした場合に管理機能を引き継ぐようにセカンダリ データ インターフェイスを設定できるようになりました。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含む等コストマルチパス（ECMP）ゾーンを追跡し、管理トラフィックが両方のインターフェイスを使用できるようにします。詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Configure a Redundant Manager Access Data Interface」を参照してください。
リモートアクセス VPN	
リモートアクセス VPN の TLS 1.3	TLS 1.3 を使用して、リモートアクセス VPN 接続を暗号化できます。デバイスがリモートアクセス VPN サーバーとして機能する場合、Threat Defense プラットフォーム設定を使用して、そのデバイスでは TLS 1.3 プロトコルを使用する必要があることを指定します。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Platform Settings」を参照してください。

機能	説明
サイト間 VPN	
ダイナミック仮想トンネルインターフェイスのサポート	ダイナミック VTI を作成し、それを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できます。以前は、スタティック VTI のみを使用して、ハブアンドスポークトポロジでルートベースのサイト間 VPN を設定できました。 ダイナミック VTI は、大規模な企業向けハブアンドスポーク展開でのピアの構成を容易にします。ハブの複数のスタティック VTI 構成を単一の ダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Site-to-Site VPNs for Cisco Secure Firewall Threat Defense」を参照してください。
ルーティング	
Bidirectional Forwarding Detection（BFD）のサポート	クラウド提供型 Firewall Management Center は、Cisco Secure Firewall Threat Defense で Bidirectional Forwarding Detection（BFD）設定をサポートするようになりました。BFD は、2 つのシステム間の転送データ プロトコルすべてに加えて、ユニキャストのポイントツーポイント モードで動作します。ただし、Threat Defense では、BFD は BGP プロトコルでのみサポートされます。デバイスの BFD 設定には、テンプレートとポリシーの作成と、BGP ネイバー設定での BFD サポートの有効化が含まれます。 詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Bidirectional Forwarding Detection Routing」を参照してください。
仮想トンネルインターフェイスでの EIGRP（IPv4）ルーティングのサポート	EIGRP（IPv4）ルーティングが仮想トンネルインターフェイスでサポートされるようになりました。EIGRP（IPv4）を使用して、ルーティング情報を共有し、ピア間の VTI ベースの VPN トンネルを介してトラフィックフローをルーティングできます。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Additional Configurations for VTI」を参照してください。

機能	説明
OSPF の仮想トンネルインターフェイス（VTI）のサポート	IPv4 または IPv6 OSPF は、Threat Defense デバイスの VTI インターフェイスで設定できます。OSPF を使用してルーティング情報を共有し、デバイス間の VTI ベースの VPN トンネルを介してトラフィックをルーティングできます。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Site-to-Site VPNs for Secure Firewall Threat Defense」を参照してください。
アクセス制御と脅威検出	
復号ポリシー	機能をより適切に反映するために、機能の名前が SSL ポリシーから復号ポリシーに変更されました。1 つ以上の [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] ルールを同時に使用して復号ポリシーを設定できるようになりました。 まず、**[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [復号（Decryption）]** に移動します。 [復号ポリシーの作成（Create Decryption Policy）] ダイアログボックスには、[アウトバウンド接続（Outbound Connections）] と [インバウンド接続（Inbound Connections）] の 2 つのタブページが追加されました。 [アウトバウンド接続（Outbound Connections）] タブページを使用して、1 つ以上の復号ルールを [復号-再署名（Decrypt - Resign）] ルールアクションで構成します。(You can either upload or generate certificate authorities at the same time）. CA とネットワークおよびポートの組み合わせごとに、1 つの復号ルールが作成されます。 [インバウンド接続（Inbound Connections）] タブページを使用して、1 つ以上の復号ルールを [復号-既知のキー（Decrypt - Known Key）] ルールアクションで構成します。（同時にサーバーの証明書をアップロードできます。）サーバー証明書とネットワークおよびポートの組み合わせごとに、1 つの復号ルールが作成されます。
ヘルス モニタリング	

機能	説明
CDO でのクラウド提供型 Firewall Management Center 展開通知	CDO は、クラウド提供型 Firewall Management Center で実行された展開のステータスについて通知するようになりました。通知メッセージには、展開が成功したか、失敗したか、または進行中であるか、展開の日時、および クラウド提供型 Firewall Management Center の [展開履歴（Deployment History）] ページへのリンクが含まれます。詳細については、*Cisco Defense Orchestrator での FDM デバイスの管理* [英語] の「Notifications」を参照してください。https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-ftd-with-cdo/managing-ftd-with-cisco-defense-orchestrator.html
クラスタのヘルスモニターの設定	クラウド提供型 Firewall Management Center の Web インターフェイスでクラスタのヘルスモニターの設定を編集できるようになりました。以前のバージョンの FlexConfig を使用してこれらの設定を行う場合、展開は許可されますが、FlexConfig 設定が優先されるため、設定をやり直すように警告も表示されます。 詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Edit Cluster Health Monitor Settings」を参照してください。
デバイスクラスタのヘルスモニタリングの改善	各クラスタのヘルスモニターを使用して、全体的なクラスタステータス、負荷分散メトリック、評価指標、クラスタ制御リンク（CCL）、およびデータスループットなどを表示できるようになりました。 詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Cluster Health Monitor」を参照してください。
新しいヘルスモニタリングのアラート	クラウド提供型 Firewall Management Center には、Firepower 4100/9300 シャーシの温度と電源を監視するための新しいヘルスモジュールが用意されています。 新しい環境ステータスおよび電源ヘルスモジュールを使用して、カスタムヘルスダッシュボードを作成し、物理アプライアンスの温度と電源のしきい値を設定できます。詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Health Monitor Alerts」を参照してください。
ライセンシング	

機能	説明
キャリア ライセンス	シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。クラウド提供型 Firewall Management Center は、既存のスマートライセンスに加えて、キャリアライセンスをサポートするようになりました。キャリアライセンスを使用すると、GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定できます。Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Licenses」を参照してください。
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	
コア割り当てのパフォーマンスプロファイル	Cisco Secure Firewall Threat Defense デバイスの CPU コアは、Lina と Snort の 2 つのメインシステムプロセスに割り当てられます。Lina は、VPN 接続、ルーティング、およびその他の基本的なレイヤ 3/4 処理を処理します。Snort は、侵入とマルウェアの防止、URL フィルタリング、アプリケーション フィルタリング、および詳細なパケットインスペクションを必要とするその他の機能を含む、高度なインスペクションを提供します。 パフォーマンスプロファイルを使用して、データプレーンと Snort に割り当てられるシステムコアの割合を調整して、システムパフォーマンスを調整できます。VPN および侵入ポリシーの相対的な使用に基づいて、必要なパフォーマンスプロファイルを選択できます。詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Configure the Performance Profile」を参照してください。
ID（Identity）	

機能	説明
プロキシシーケンス	プロキシシーケンスは、LDAP、Active Directory、または ISE/ISE-PIC サーバーとの通信に使用できる 1 台以上の管理対象デバイスです。Security Cloud Control が Active Directory か ISE/ISE-PIC サーバーと通信できない場合にのみ必要になります。（たとえば、Security Cloud Control がパブリッククラウドにある一方、Active Directory または ISE/ISE-PIC がプライベートクラウドにあるといったケースが考えられます）。 1 台の管理対象デバイスをプロキシシーケンスとして使用することはできますが、1 台の管理対象デバイスが Active Directory か ISE/ISE-PIC と通信できない場合に別の管理対象デバイスが引き継げるよう、2 台以上設定することを強くお勧めします。 **[統合（Integration）]>[その他の統合（Other Integrations）]>[レルム（Realms）]>[プロキシシーケンス（Proxy Sequence）]** の順に選択して、プロキシシーケンスを作成します。

2022 年 10 月 20 日

ポリシーベースのルートマップでのネクストホップ IP アドレスの設定のサポート

ポリシーベースルーティング（PBR）は、宛先ネットワーク基準ではなく、送信元ポート、宛先アドレス、宛先ポート、プロトコル、アプリケーションなど、またはこれらのオブジェクトの組み合わせの優先順位に基づいて、指定したアプリケーションのネットワークトラフィックをルーティングするのに役立ちます。たとえば、PBR を使用して、優先順位が高いネットワークトラフィックを高帯域幅で高価なリンク経由でルーティングし、優先順位が低いネットワークトラフィックを低帯域幅で低コストのリンク経由でルーティングできます。

クラウド提供型 Firewall Management Center は、ポリシーベースのルートマップを作成するときに、ネクストホップ IP アドレスの定義をサポートするようになりました。詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「About Policy Based Routing」および「Configure Policy-Based Routing Policy」を参照してください。

URL フィルタリングの機能拡張

URL フィルタリングを使用すると、ネットワークのユーザーが使用できる Web サイトを制御できます。デバイスに URL フィルタリングライセンスが必要なカテゴリとレピュテーションに基づいて、または URL を指定して手動で Web サイトをフィルタリングできます。カテゴリおよびレピュテーションベースのフィルタリング（URL フィルタリングのより迅速かつスマートな方法）では、シスコの最新の脅威インテリジェンス情報が使用されるため、使用を強く推奨します。

クラウド提供型 Firewall Management Center は、ローカルデータベース情報を使用する代わりに、最新の URL カテゴリとレピュテーション情報を Cisco Talos クラウドから直接クエリできるようになりました。ローカルデータベースは 24 ～ 48 時間ごとに更新されます。詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「URL Filtering Options」を参照してください。

クラウド提供型 Firewall Management Center を使用した Cisco Umbrella トンネルと Cisco Secure Firewall Threat Defense の統合

クラウド提供型 Firewall Management Center を使用して、脅威に対する防御 デバイスから Cisco Umbrella に IPsec IKEv2 トンネルを自動的に展開できるようになりました。このトンネルは、インターネットに向かうすべてのトラフィックを、検査とフィルタリングのために Cisco Umbrella Secure Internet Gateway（SIG）に転送します。Cisco Umbrella トンネルを設定および展開するには、シンプルなウィザードを使用して、新しいタイプの静的 VTI ベースのサイト間 VPN トポロジである SASE トポロジを作成します。

詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「About Umbrella SASE Topology」を参照してください。

FTD からクラウドへの移行におけるリモートアクセス VPN ポリシーのサポート

CDO は、FTD のクラウドへの移行中にリモートアクセス VPN ポリシーをインポートするようになりました。

詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Migrate FTD to Cloud」を参照してください。

Flex で設定されたルーティングポリシーの移行

クラウド提供型 Firewall Management Center は、ユーザーインターフェイスの [移行構成（Migration Config）] オプションを使用して、Flex で設定された ECMP、VxLAN、および EIGRP ポリシーの移行をサポートするようになりました。

詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「Migrating FlexConfig Policies」を参照してください。

スマートライセンスの標準化

クラウド提供型 Firewall Management Center で使用されるライセンス名が変更されました。

表 *16 :* スマートライセンス名の変更

古い名前	は次に変更されました。	新しい名前（**New Name**）
Base	は次に変更されました。	Essentials
脅威	は次に変更されました。	IPS
マルウェア	は次に変更されました。	マルウェア防御
RA VPN/AnyConnect ライセンス	は次に変更されました。	Cisco Secure Client
AnyConnect Plus	は次に変更されました。	Cisco Secure Client Advantage
AnyConnect Apex	は次に変更されました。	Cisco Secure Client Premier
AnyConnect Apex および Plus	は次に変更されました。	Cisco Secure Client Premier および Advantage
AnyConnect VPN Only	は次に変更されました。	Cisco Secure Client VPN のみ

詳細については、Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語] の「License Types and Restrictions」を参照してください。

2022 年 6 月 9 日

Cisco Defense Orchestrator（CDO）がクラウド提供型 Firewall Management Center のプラットフォームになりました。

クラウド提供型 Firewall Management Center は、Cisco Secure Firewall Threat Defense デバイスを管理する Software as a Service（SaaS）製品です。提供する機能の多くはオンプレミス型 Cisco Secure Firewall Management Center と同じです。外観や動作もオンプレミス型の Cisco Secure Firewall Management Center と同じで、同じ FMC API が使用されています。

この製品は、オンプレバージョンの Cisco Secure Firewall Management Center から SaaS バージョンへの移行を希望される Cisco Secure Firewall Management Center のお客様向けに設計されました。

CDO オペレーションチームが、SaaS 製品として維持管理を担当します。新しい機能が導入されると、CDO オペレーションチームが CDO とクラウド提供型 Firewall Manager をお客様に代わって更新します。

お使いのオンプレミス型 Cisco Secure Firewall Management Center に登録されている Cisco Secure Firewall Threat Defense デバイスをクラウド提供型の Firewall Management Center に移行するための移行ウィザードが用意されています。

Cisco Secure Firewall Threat Defense デバイスの導入準備は CDO で実行します。シリアル番号によるデバイスの導入準備といった一般的なプロセスを実行するか、登録キーを含む CLI コマンドを使用します。デバイスの導入準備が完了すると、CDO とクラウド提供型 Firewall Management Center の両方に表示されますが、デバイスの設定はクラウド提供型 Firewall Management Center で行います。バージョン 7.2 以降を実行している Cisco Secure Firewall Threat Defense デバイスの導入準備が可能です。

クラウド提供型 Firewall Management Center のライセンスはデバイスごとに管理されるライセンスであるため、クラウド提供型 FMC 自体のライセンスは不要です。既存の Cisco Secure Firewall Threat Defense デバイスは既存のスマートライセンスを再利用し、新しい Cisco Secure Firewall Threat Defense デバイスは FTD に導入された各機能に対して新しいスマートライセンスをプロビジョニングします。

リモートの分散拠点が展開されている場合、脅威防御デバイスのデータインターフェイスは、デバイス上の管理インターフェイスではなく、Cisco Defense Orchestrator の管理で使用されます。ほとんどのリモート分散拠点には 1 つのインターネット接続しかないため、外部から CDO にアクセスして中央管理を行えるようにします。リモートの分散拠点が展開されている場合、CDO はデータインターフェイスを介して管理対象の脅威防御デバイスに高可用性サポートを提供します。

セキュリティ分析とロギング（SaaS）またはセキュリティ分析とロギング（オンプレミス）を使用して、導入準備した脅威防御デバイスで生成された syslog イベントを分析できます。SaaS バージョンでは、イベントがクラウドに保存され、CDO でイベントを表示します。オンプレミスバージョンでは、イベントがオンプレミスの Cisco Secure Network Analytics アプライアンスに保存され、オンプレミスの Cisco Secure Firewall Management Center で分析されます。どちらの場合も、現在のオンプレミス FMC と同様に、選択したログコレクタにセンサーから直接ログを送信できます。

FTD ダッシュボードには、すべての脅威防御デバイスで収集および生成されたイベントデータを含むステータスの概要が表示されます。脅威防御デバイスはクラウド提供型の Firewall Management Center によって管理されます。このダッシュボードを使用して、環境内のデバイスの状態や全体的な正常性に関連する一連の情報を表示できます。FTD ダッシュボードが提供する情報はシステムのライセンス方法、設定方法、展開方法によって異なる点に注意してくだ

さい。FTD ダッシュボードには、CDO で管理されているすべての脅威防御デバイスに関するデータが表示されますが、デバイスベースのデータをフィルタリングすることもできます。また、時間範囲を選択して特定の時間範囲の情報を表示することもできます。

Cisco Secure Dynamic Attributes Connector を使用すると、クラウド提供型 Firewall Management Center のアクセス制御ルールで、さまざまなクラウド サービス プラットフォームのサービス タグとカテゴリを使用できます。ワークロードの動的な性質と IP アドレスの重複の必然性により、IP アドレスなどのネットワーク構造は、仮想、クラウド、およびコンテナ環境では一時的なものです。お客様は、IP アドレスや VLAN が変更されてもファイアウォールポリシーが持続するように、VM 名やセキュリティグループなどの非ネットワーク構造に基づいてポリシールールを定義する必要があります。

1 台以上の管理対象デバイスの **プロキシシーケンス**は、LDAP、Active Directory、または ISE/ISE-PIC サーバーとの通信に使用できます。Cisco Defense Orchestrator（CDO）が Active Directory か ISE/ISE-PIC サーバーと通信できない場合にのみ必要になります。たとえば、CDO はパブリッククラウドにあり、Active Directory や ISE/ISE-PIC がプライベートクラウドにある場合があります。

1 台の管理対象デバイスをプロキシシーケンスとして使用することはできますが、1 台の管理対象デバイスが Active Directory か ISE/ISE-PIC と通信できない場合に別の管理対象デバイスが引き継げるよう、2 台以上設定することを強くお勧めします。

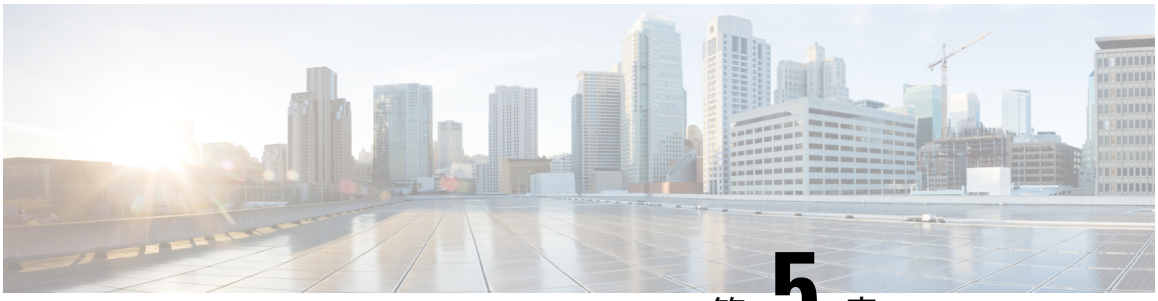
すべてのお客様は、CDO を使用して、Cisco Secure Firewall ASA、Cisco Meraki、Cisco IOS デバイス、Cisco Umbrella、AWS 仮想プライベートクラウドなどの他のデバイスタイプを管理できます。CDO を使用して、Firepower Device Manager によるローカル管理用に構成された Cisco Secure Firewall Threat Defense デバイスを管理する場合、CDO で引き続き管理できます。CDO を初めて使用する場合は、新しいクラウド提供型の Firewall Management Center および他のすべてのデバイスタイプを使用して、Cisco Secure Firewall Threat Defense デバイスを管理できます。

クラウドで提供型の Firewall Management Center でサポートされている Firewall Management Center 機能の詳細をご覧ください。

- ヘルス モニタリング
- Cisco Secure Firewall Threat Defense デバイスのバックアップ/復元
- スケジューリング
- Import/Export
- アラート応答による外部アラート
- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード
- Cisco Secure Firewall Threat Defense デバイスの高可用性
- インターフェイス
- ネットワーク アクセス コントロール（NAT）
- 静的ルートとデフォルトルート、およびその他のルーティング設定
- オブジェクト管理および証明書

- リモートアクセス VPN およびサイト間 VPN の設定
- アクセス コントロール ポリシー
- Cisco Secure 動的属性コネクタ
- 侵入検知と防御ポリシー
- ネットワークにおけるマルウェア対策およびファイルポリシー
- 暗号化トラフィックの処理
- ユーザ アイデンティティ
- FlexConfig ポリシー

2022 年 6 月 9 日



第 5 章

未解決のバグおよび解決されたバグ

このドキュメントでは、2024 年 8 月 23 日時点でのクラウド提供型 Firewall Management Center の未解決のバグと解決済みのバグをリストしています。

（注） バグリストは一度自動生成されると、クラウド提供型 Firewall Management Center の更新間では更新されません。バグがシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。

未解決のバグ

重要 バグリストは 1 回自動生成され、その後は更新されません。バグがシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。サポート契約がある場合は、Cisco バグ検索ツールを使用して以下のバグを確認できます。

表 *17* : クラウド提供型 *Firewall Management Center* の *2024* 年 *11* 月 *8* 日のアップデートで未解決のバグ

不具合 ID	タイトル
CSCwh24268	CdFMC：Cisco Secure Firewall Threat Defense の移行中に一括登録の問題が発生する
CSCwi31218	クラスタに IP プールが設定されており、データノードが制御ノードと同期されていない場合、ノードの除外に失敗する
CSCwj30329	cdFMC：FTD クラスタ登録が内部エラーで失敗する
CSCwk68830	チケットが「進行中」状態で、ポリシーを作成できない：オープンチケットが必要であることを示すエラーが表示される

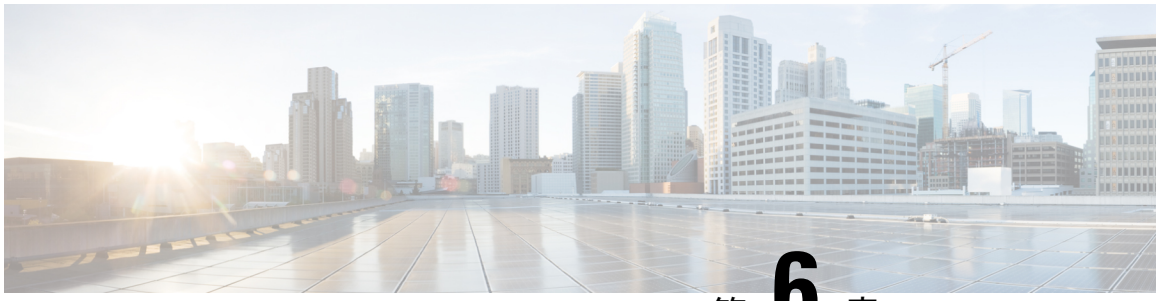
不具合 ID	タイトル
CSCwm34180	ポートチャネル/ポートチャネル サブインターフェイスのトラフィックがデバイステンプレート登録で機能しない
CSCwm38714	変更管理：セキュリティゾーンがウィザードにインラインで追加される場合、SD-WAN トポロジの保存でエラーが発生する
CSCwm46752	BGP が有効である場合、Cisco Secure Firewall 3100 L3 クラスタで「設定の編集」が失敗する
CSCwn13421	クラウド提供型 Firewall Management Center の拡張：Syslog への監査ログが無効な IPv6 syslog ホストで設定されている場合、ポリシーの展開が失敗する

解決済みのバグ

表 *18 :* クラウド提供型 *Firewall Management Center* の *2024* 年 *8* 月 *23* 日のアップデートで解決済みのバグ

ID	見出し
CSCwd79150	クラスタデバイスのデバイス API healthStatus がデバイスリストのヘルスステータスと一致しない
CSCwd88641	デバイスモデルと snort エンジンに基づいて VDB パッケージをプッシュするための展開の変更である
CSCwf02673	[cdfmc] ネットワーク検出ポリシー（ND）：サポートされていない機能に関する通知メッセージ
CSCwf14031	アプリケーションディテクタが無効になっているため、Lua ファイルが見つからずに Snort がダウンする（VDBM 側）
CSCwf89265	CDFMC：ディザスタリカバリの実行後に古いバージョンにロールバックする VDB バージョン
CSCwh89058	ccdFMC へのログイン試行が /api/ui_platform/v1/uiauth/generatetoken に対して 401 Unauthorized を返す
CSCwi31563	cdFMC：ルール更新インポートログ UI のテーブルビューでエラーが発生し、SRU 更新ログを確認できない
CSCwi65988	cdFMC：TPK MI シャーシマネージャを cdFMC に移行できない
CSCwj08822	cdFMC：複数の正常性モニターウィジェットで、データの取得中にエラーが発生する

ID	見出し
CSCwj29351	正常性ポリシーの設定：ポリシーからデバイスを削除できない
CSCwj68360	クラスタの移行：削除されたクラスタノードの分析専用（AO）モードをオンプレミス FMC に再登録できない
CSCwj95574	cdFMC：Cisco Secure Firewall Threat Defense の移行がエラーで失敗する：デバイスが CMW チケットによってロックされる
CSCwk27628	Security Cloud Control：Security Cloud Control へのシャーシのオンボーディングがホスト名で失敗する



第 6 章

ドキュメントとサポートリソース

関連する Cisco Defense Orchestrator 製品のドキュメント

その他の役立つドキュメントについては、以下を参照してください。

- Cisco Defense Orchestrator のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理 [英語]
- 他のすべての Cisco Defense Orchestrator ドキュメントへのリンク

シスコサポートリソース

クラウド提供型 Firewall Management Ceneter 内でサポートケースを開く

次の手順に従って、クラウド提供型 Firewall Management Center からサポートケースを開きます。

1. クラウド提供型 Firewall Management Center で、[ヘルプ（Help）]（?）アイコンをクリックします。
2. [サポートとダウンロード（Support & Downloads）] で、[TACサポートケース（TAC Support Cases）] をクリックします。

シスコへのお問い合わせ

Cisco Technical Assistance Center（TAC） に連絡するその他の方法は次のとおりです。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447

- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先

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。