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

2022 年 12 月 13 日

表 *1* : 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するだけで、アップグレードできます。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、必要なアップグレードパッケージが自動的にデバイスにコピーされ、互換性チェックと準備状況チェックが実行されて、アップグレードが開始されます。ウィザードを手動でステップ実行する場合と同様に、（チェックの失敗などで）アップグレードの 1 つの段階に「合格」しないデバイスは、次の段階に含まれません。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から再開できます。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）]** > **[アクセスコントロール（Access Control）]** > **[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、[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）] タブページで、[復号-再署名（Decrypt - Resign）] ルールアクションを使用して、1 つ以上の復号ルールを設定します（同時に認証局のアップロードまたは生成を実行できます）。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）] タブページで、[復号-既知のキー（Decrypt - Known Key）] ルールアクションを使用して、1 つ以上の復号ルールを設定します（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 展開の通知	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。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です（たとえば、CDO 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 *2:* 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です。たとえば、CDO 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。

すべてのお客様は、CDO を使用して、Cisco Secure Firewall ASA、Meraki、Cisco IOS デバイス、Cisco Secure Firewall Cloud Native、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

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。