# 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 11 月 8 日

表 *1 :* 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 | | |
| 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。<br>• Cisco Secure Firewall 1210CX（1000BASE-T ポート X 8）<br>• 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。<br>• Cisco Secure Firewall 1220CX（1000BASE-T ポート X 8、SFP+ ポート X 2）。<br>Cisco Secure Firewall CSF-1210CE、CSF-1210CP、および CSF-1220CX Hardware Installation Guideを参照してください。 |

| 機能 | 最小の Threat Defense | 詳細 |
|---|---|---|
| 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。<br><br>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**<br><br>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**<br><br>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** | | |
| 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。<br><br>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。<br><br>新規/変更された画面：**[デバイス（Devices）]**>**[テンプレート管理（Template Management）]**<br><br>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。<br><br>詳細：<br>• 「Device Management Using Device Templates」[英語] を参照してください。<br>• 「ゼロタッチプロビジョニングを使用したクラウド提供型 Firewall Management Center へのデバイステンプレートを使用した Threat Defense デバイスのオンボード」を参照してください。 |

| 機能 | 最小の Threat Defense | 詳細 |
|---|---|---|
| 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。<br>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。<br>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）]**<br>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 |
| 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。<br>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。<br>参照：Cisco Secure Firewall 3100/4200 のマルチインスタンスモード |

| 機能 | 最小の Threat Defense | 詳細 |
|---|---|---|
| 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。<br>新規/変更された画面：<br>• **[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）]**<br>• **[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。<br>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。<br><br>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。<br><br>新規/変更された画面：<br><br>• [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタの追加（Add Cluster）]<br><br>• **[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）]**<br><br>• **[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）]**<br><br>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。<br><br>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。<br>制限事項：クラスタリングではサポートされていません。<br>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：<br>• Azure：管理 1、データ 2（最大 8）<br>• GCP：管理 1、データ 3（最大 8）<br>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。<br>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<br>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。<br>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）]**<br>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。<br><br>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。<br><br>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。<br><br>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。<br><br>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。**<br>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。<br>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）]**<br>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。<br>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。<br>• Microsoft AD サーバー（Windows Server 2008 以降）<br>• Microsoft AD ドメインコントローラ（Windows Server 2008 以降）<br>• 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）<br>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。<br><br>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。<br><br>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)）]**<br><br>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。<br><br>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。<br><br>「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<br>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。<br>• 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。<br>• 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。<br>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。<br>**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。<br>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]**<br>新規/変更された CLI コマンド：なし<br>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。<br>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。<br>• [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。<br>• [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。<br>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。<br>「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 *2 :* 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。<br>（注）<br>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。<br><br>（注）<br>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。<br><br>新規/変更された画面：<br>• **[インベントリ（Inventory）] > [FTDシャーシ（FTD Chassis）]**<br>• **[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）]**<br>• **[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）]**<br>• **[デバイス（Devices）] > [シャーシのアップグレード（Chassis Upgrade）]**<br><br>新規/変更された Threat Defense CLI コマンド：**configure multi-instance network ipv4**、**configure multi-instance network ipv6**<br><br>新規/変更された FXOS CLI コマンド：**create device-manager**、**set deploymode**<br><br>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。<br><br>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。<br><br>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。<br><br>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。<br><br>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）]**<br><br>参照：復号ポリシーの作成<br><br>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。<br><br>新規/変更された画面：<br><br>• [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）]<br><br>• [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）<br><br>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）<br><br>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。<br><br>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。<br><br>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。<br><br>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）]**<br><br>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。<br><br>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。<br><br>新規/変更された画面：**[インベントリ（Inventory）] > [FTD シャーシ（FTD Chassis）]**<br><br>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。<br><br>バージョンの制限：Threat Defense バージョン 7.0 ～ 7.0.6、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。<br><br>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 | 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。<br><br>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。<br><br>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。<br>• 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。<br>• 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）。<br>• 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。<br>• パフォーマンスが不十分な侵入ルール。<br>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）]**<br>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。<br>参照：Advanced Troubleshooting for the Secure Firewall Threat Defense Device<br>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。<br><br>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。<br><br>次のことを防ぐことができます。<br><br>• 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。<br><br>• 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。<br><br>• 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。<br><br>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。<br><br>優先順位に従って、次のことができます。<br><br>• 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。<br><br>• 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。<br><br>• 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。<br><br>次の選択肢があります。<br>• 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。<br>• 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。<br>• 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 *3*：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<br>7.2.1 | クラスタ化された Cisco Secure Firewall Threat Defense 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。<br>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。<br>この機能を有効にするための [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）]（⚙）>**変更管理のワークフロー**ページが表示され、メニューに新しい [チケット（Ticket）]（📄）クイックアクセスアイコンが表示されます。<br>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 *4 :* 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。<br>• 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G）<br>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。<br>• QSFP-40/100-SRBD<br>• QSFP-100G-SR1.2<br>• QSFP-100G-SM-SR<br>以下のネットワークモジュールでサポート：<br>• FPR9K-NM-4X100G<br>• FPR9K-NM-2X100G<br>• FPR9K-DNM-2X100G<br>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。<br>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。<br>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。<br>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。<br>「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。<br>新規/変更された画面：**[分析（Analysis）]** > **[Cisco SD-WANサマリー（SD-WAN Summary）]**<br>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。**<br><br>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。<br><br>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。<br><br>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。<br><br>制限事項：Microsoft Azure Active Directory ではサポートされていません。<br><br>新規/変更された画面：<br><br>• **[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）]**<br><br>• **[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）]**<br><br>• **[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）]**<br><br>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。<br>• (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。<br>• 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。<br>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）]**<br>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。<br>• 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。<br>• 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。<br>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。<br>新規/変更された画面：**[展開（Deploy）]>[高度な展開（Advanced Deploy）]**。<br>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。<br>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。<br>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。<br>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。<br>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。**<br>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。<br>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。<br>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。 | いずれか | 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。<br><br>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。<br><br>新規/変更された画面：<br><br>• [システム（System）]（⚙）>**[製品のアップグレード（Product Upgrades）]**では、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。<br><br>• [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。<br><br>• **[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。<br><br>廃止された画面/オプション：<br><br>• [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。<br><br>• 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。<br><br>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。<br><br>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。<br>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。<br>メモリが少ないデバイス：ASA-5508-X および ASA 5516-X<br>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。<br>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：イベントの頻繁なドレインの正常性アラート。 | 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。<br>参照：「Disk Usage and Drain of Events Health Monitor Alerts」 |

2024 年 2 月 13 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。