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

2023 年 11 月 30 日

表 *1* : 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 *2 :* 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：「Monitoring the Site-to-Site VPNs」
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 *3* : 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 *4* : 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 *5 :* 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 *6 :* 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 *7 :* 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 *8 :* 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。

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。