特長と機能

このドキュメントでは、バージョン7.2の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。

重要 新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。

新機能

Management Center バージョン 7.2 の新機能

新しいハードウェアまたは仮想 management center で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。 新しいトラフィック処理機能では、management center とデバイスの両方で最新のリリースが前提条件となります。デバイスが明らかに関与していない機能（Webインターフェイスの外観の変更、クラウド統合）では、management centerの最新バージョンのみを必須条件としているにもかかわらず、それが保証されない場合があります。新機能の説明では、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

表 *1 : Management Center* バージョン *7.2.0* の新機能

機能	説明
プラットフォーム（Platform）	

機能	説明
スナップショットで AWS および Azure 向け Threat Defense Virtual をすばやく展開できます。	AWS または Azure インスタンスの Threat Defense Virtual のスナップショットを作成し、そのスナップショットを使用して新しいインスタンスをすばやく展開できるようになりました。この機能により、AWS および Azure の自動スケールソリューションのパフォーマンスも向上します。
AWS ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケール。	CloudFormation テンプレートを使用して、AWS ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケールをサポートするようになりました。
GCP 向け Threat Defense Virtual の自動スケール。	GCP の内部ロードバランサ（ILB）と GCP 外部ロードバランサ（ELB）の間に Threat Defense Virtua インスタンスグループを配置することにより、GCP 向け Threat Defense Virtua の自動スケールをサポートするようになりました。
クラウド管理型の脅威防御デバイス向けの分析モード。	バージョン 7.2 と同時に、クラウド提供型の Cisco Secure Firewall Management Center が導入されました。このクラウド提供型の管理センターは、Cisco Defense Orchestrator（CDO）プラットフォームを使用して、複数の Cisco セキュリティソリューションの管理を統合します。更新についてはシスコが行います。 お客様が導入したハードウェアおよびバージョン 7.2 以降を実行している仮想管理センターでは、クラウド管理型の脅威防御デバイスを「共同管理」できますが、用途はイベントのロギングと分析に限られます。お客様が導入した管理センターからこれらのデバイスにポリシーを展開することはできません。 新規/変更された画面： • クラウド管理型デバイスをお客様が導入した管理センターに追加する場合は、新しい [CDO管理対象デバイス（CDO Managed Device）] チェックボックスをオンにして、それが分析専用であることを指定します。 • [デバイス（Devices）] > [デバイス管理（Device Management）] を選択すると、分析専用のデバイスが表示されます。 新規/変更された CLI コマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** 詳細については、Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理を参照してください。
高可用性/拡張性	

機能	説明
パブリッククラウドとプライベートクラウドの両方で Threat Defense Virtual のクラスタリング。	次の Threat Defense Virtual プラットフォームのクラスタリングを設定できるようになりました。 • AWS 向け Threat Defense Virtual：16 ノードクラスタ • GCP 向け Threat Defense Virtual：16 ノードクラスタ • KVM 向け Threat Defense Virtual：4 ノードクラスタ • VMware 向け Threat Defense Virtual：4 ノードクラスタ 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）] • [Devices] > [Device Management] > [More] メニュー • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]
16 ノードクラスタのサポート。	次のプラットフォームに 16 ノードクラスタを設定できるようになりました。 • Firepower 4100/9300 • AWS 向け Threat Defense Virtual • GCP 向け Threat Defense Virtual Cisco Secure Firewall 3100 では、依然として 8 ノードしかサポートされません。
インターフェイス	
Firepower 2100 および Cisco Secure Firewall 3100 で LLDP をサポート。	Firepower 2100 および Cisco Secure Firewall 3100 シリーズのインターフェイスで Link Layer Discovery Protocol（LLDP）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）]** > **[インターフェイス（Interfaces）]** > **[ハードウェア構成（Hardware Configuration）]** > **[LLDP]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics**

機能	説明
Cisco Secure Firewall 3100 でハードウェアバイパスをサポート（「fail-to-wire」）。	Cisco Secure Firewall 3100 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能をサポートするようになりました（バージョン 7.2 の新しいハードウェアと仮想プラットフォーム （28 ページ） を参照してください）。 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）]>[物理インターフェイスの編集（Edit Physical Interface）]
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止。	トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [ネットワーク接続（Network Connectivity）]
Cisco Secure Firewall 3130 および 3140 のブレークアウトポート。	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成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）] > [シャーシの操作（Chassis Operations）]
Management Center の Web インターフェイスから VXLAN を設定。	Management Center の Web インターフェイスを使用して VXLAN インターフェイスを設定できるようになりました。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。 以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。 新規/変更された画面： • VTEP ソースインターフェイスは次の順にアクセスし、設定します：**[デバイス（Devices）] > [デバイスの管理（Device Management）] > [VTEP]** • VNI インターフェイスは次の順にアクセスし、設定します。**[デバイス（Devices）] > [デバイスの管理（Device Management）] > [インターフェイス（Interfaces）] > [VPNインターフェイスを追加（Add VNI Interface）]**

機能	説明
NAT	
一度に複数の NAT ルールの有効化、無効化、削除が可能。	複数の NAT ルールを選択して、すべてを同時に有効化、無効化、または削除できます。有効化および無効化の対象は手動 NAT ルールのみです。削除はすべての NAT ルールが対象になります。
VPN	
RA VPN 接続プロファイル用の証明書と SAML 認証。	RA VPN 接続プロファイル用の証明書と SAML 認証をサポートするようになりました。SAML 認証/承認が開始される前に、マシン証明書やユーザー証明書を認証できます。これは、ユーザー固有の SAML DAP 属性と DAP 証明書属性を使用して実行できます。 新規/変更された画面：RA VPN ポリシーの接続プロファイルの認証方法を選択するときに、[証明書と SML（Certificate & SAML）] オプションを選択できるようになりました。
ハブアンドスポークトポロジを使用したルートベースのサイト間 VPN。	ハブアンドスポークトポロジでのルートベースのサイト間 VPN のサポートが追加されました。以前は、このトポロジはポリシーベース（暗号マップ）VPN のみをサポートしていました。 新規/変更された画面：新しい VPN トポロジを追加し、[ルートベース (VTI)（Route Based (VTI)）] を選択すると、[ハブアンドスポーク（Hub and Spoke）] も選択できるようになりました。
Cisco Secure Firewall 3100 の IPsec フローのオフロード。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
ルーティング	

機能	説明
Management Center の Web インターフェイスから EIGRP を設定。	Management Center の Web インターフェイスを使用して EIGRP を設定できるようになりました。デバイスのグローバル仮想ルータに属するインターフェイスでのみ EIGRP を有効にできることに注意してください。 以前のバージョンの FlexConfig を使用して EIGRP を設定した場合、アップグレード後の展開は可能ですが、Web インターフェイスで EIGRP の設定をやり直すように警告が表示されます。新しい設定を確認したら、廃止された FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。 このプロセスを支援するために、コマンドライン移行ツールが用意されています。詳細については、コンフィギュレーション ガイドの FlexConfig ポリシーの移行 を参照してください。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[EIGRP]**
Firepower 1010 で仮想ルータをサポート。	Firepower 1010 で最大 5 つの仮想ルータを構成できるようになりました。
ユーザー定義の仮想ルータで VTI をサポート。	仮想トンネルインターフェイスをユーザー定義の仮想ルータに割り当てることができるようになりました。これまでは、VTI はグローバル仮想ルータにしか割り当てることができませんでした。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[仮想ルータのプロパティ（Virtual Router Properties）]**

機能	説明
パスのモニタリングによるポリシーベースのルーティング。	パスのモニタリング機能を使用して、デバイスの出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集できるようになりました。次に、収集したメトリックを使用して、ポリシーベースのルーティングの最適なパスを決定できます。 新規/変更された画面： • パスモニタリングを有効にし、収集するメトリックを選択するには、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）** > **[パスモニタリング（Path Monitoring）]**に移動します。 • ポリシーベースのルートを追加して転送アクションを指定する際、新規の [インターフェイスの順位付け（Interface Ordering）] オプションを使用します（**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]**）。 • 各デバイスのヘルスモニタリングダッシュボードでパスメトリックを監視します（**システム**（⚙）>**[ヘルス（Health）**>**[モニター（Monitor）]** > [ダッシュボードの追加（add dashboard）] > **[インターフェイス: パスメトリック（Interface - Path Metrics）]**）。 新規/変更された CLI コマンド：**show policy route**、**show path-monitoring**、**clear path-monitoring**
脅威インテリジェンス	

機能	説明
Cisco Umbrella からの DNS ベースの脅威インテリジェンス。	Cisco Umbrella から定期的に更新される情報を使用して、DNS ベースのセキュリティインテリジェンスをサポートするようになりました。二重の保護として、ローカル DNS ポリシーと Umbrella DNS ポリシーの両方を使用できます。 新規/変更された画面： • Umbrella への接続の設定：**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[クラウドサービス（Cloud Services）]** > **[Cisco Umbrella接続（Cisco Umbrella Connection）]** • Umbrella DNS ポリシーの設定：**[ポリシー（Policies）]** > **[DNS]** > **[DNSポリシーを追加（Add DNS Policy）]** > **[Umbrella DNAポリシー（Umbrella DNA Policy）]** • Umbrella DNS ポリシーのアクセスコントロールへの関連付け：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** > **[ポリシーを編集（Edit Policy）]** > **[セキュリティインテリジェンス（Security Intelligence）]** > **[Umbrella Cisco DNS ポリシー（Umbrella Cisco DNS Policy）]**
Amazon GuardDuty からの IP ベースの脅威インテリジェンス。	AWS の Management Center Virtual と統合している場合、Amazon GuardDuty によって検出された悪意のある IP アドレスに基づいてトラフィックを処理できるようになりました。カスタム セキュリティ インテリジェンス フィードまたは定期的に更新されるネットワーク オブジェクト グループを介して脅威インテリジェンスがシステムで活用され、ユーザーはそれをセキュリティポリシー内で使用できます。 詳細については、AWS クラウド向け 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。
アクセス制御と脅威検出	

機能	説明
動的オブジェクト管理： • クラウド提供型 Cisco Secure 動的属性コネクタ • オンプレミス Cisco Secure 動的属性コネクタ 2.0	バージョン 7.2 と同時に、Cisco Secure 動的属性コネクタの次の更新をリリースしました。 • クラウド提供型 Cisco Secure 動的属性コネクタ（CDO マネージドサービス） サポート対象管理センター：バージョン 7.1 以降およびクラウド提供型管理センター。 サポート対象仮想/クラウドワークロード：AWS、Azure、Azure サービスタグ、Google Cloud Connector、GitHub、Office 365。 詳細については、Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理 の「*Managing the Cisco Secure Dynamic Attributes Connector with Cisco Defense Orchestrator*」の章を参照してください。 • オンプレミス Cisco Secure 動的属性コネクタ 2.0 サポート対象管理センター：バージョン 7.0 以降およびクラウド提供型管理センター。 サポート対象仮想/クラウドワークロード：AWS、Azure、Azure サービスタグ、Google Cloud Connector、GitHub、Office 365、VMware。 詳細については、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイド 2.0 [英語] を参照してください。
Snort 3 デバイスで、インスペクションをバイパスするか、エレファントフローをスロットルします。	インスペクションの検出およびオプションでのバイパス、もしくはエレファントフローをスロットルできるようになりました。デフォルトでは、アクセス コントロール ポリシーは、システムが 1 GB/10 秒を超える暗号化されていない接続を検出したときにイベントを生成するように設定されています。レート制限は設定可能です。 Firepower 2100 シリーズでは、エレファントフローを検出できますが、インスペクションのバイパスやスロットルすることはできません。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスでは、引き続きインテリジェント アプリケーション バイパス（IAB）を使用します。 新規/変更された画面：[エレファントフローの設定（Elephant Flow Settings）] をアクセス コントロール ポリシーの [詳細（Advanced）] タブに追加しました。

機能	説明
Snort 3 デバイス向けの暗号化された可視性エンジン機能の拡張。	

機能	説明
	暗号化された可視性エンジン（EVE）に次の拡張機能が追加されています。 • EVEは、ホストが使用しているオペレーティングシステムを検出できます。これは、イベントとネットワークマップで報告されます。 • EVEは、高い信頼度で識別されたEVEプロセスをアプリケーションに割り当てることでアプリケーション トラフィックを検出できます。これをアクセスコントロールルールで使用してネットワークトラフィックを制御できます。（バージョン 7.1 では、接続の EVE プロセスを見ることができましたが、その情報をもとに行動することはできませんでした。） さらに割り当てを追加するには、カスタムアプリケーションやカスタムアプリケーションディテクタを作成します。カスタムディテクタに検出パターンを追加するときは、アプリケーションとして [暗号化された可視性エンジン（Encrypted Visibility Engine）] を選択します。次に、プロセス名と信頼度を指定します。 • EVE は QUIC トラフィックで動作するようになりました。 これらの機能拡張に伴い、次の接続イベントフィールドが変更されました。 [TLS Fingerprint Process Name] は次に変更されました。 [暗号化された可視性プロセス名（Encrypted Visibility Process Name）] [TLS Fingerprint Process Confidence Score] は次に変更されました。 [暗号化された可視性プロセスの信頼スコア（Encrypted Visibility Process Confidence Score）] [TLS Fingerprint Malware Confidence] は次に変更されました。 [暗号化された可視性脅威の信頼度（Encrypted Visibility Threat Confidence）] [TLS Fingerprint Malware Confidence Score] は次に変更されました。 [暗号化された可視性脅威の信頼スコア（Encrypted Visibility Threat Confidence Score）] 検出タイプ：TLS フィンガープリント は次に変更さ 検出タイプ：暗号化された可視性エンジン

機能	説明
	れまし た。 この機能には脅威ライセンスが必要になりました。
Snort 3 デバイスの TLS 1.3 インスペクション。	TLS 1.3 トラフィックのインスペクションがサポートされるようになりました。 新規/変更された画面：SSL ポリシーの [詳細設定（Advanced Settings）] タブに [TLS 1.3復号の有効化（Enable TLS 1.3 Decryption）] オプションが追加されました。なお、このオプションはデフォルトで無効になっています。
Snort 3 デバイスのポートスキャン検出の改善。	改良されたポートスキャンディテクタを使用すると、ポートスキャンを検出または防止するようにシステムを簡単に設定できます。保護するネットワークを絞り込んだり、感度を設定したりできます。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスの場合、ポートスキャン検出には引き続きネットワーク分析ポリシーを使用します。 新規/変更された画面：[脅威検出（Threat Detection）] をアクセス コントロール ポリシーの [詳細（Advanced）] タブに追加しました。
Snort 3 デバイスの VBA マクロ検査。	Microsoft Office ドキュメントの VBA（Visual Basic for Applications）マクロのインスペクションがサポートされるようになりました。これは、マクロを解凍し、解凍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ます。 デフォルトでは、VBA マクロの解凍は、システムが提供するすべてのネットワーク分析ポリシーで無効になっています。これを有効にするには、imap、smtp、http_inspect、および pop Snort 3 インスペクタで decompress_vba 設定を使用します。 解凍されたマクロと照合するカスタム侵入ルールを設定するには、vba_data オプションを使用します。

機能	説明
Snort 3 デバイスの JavaScript インスペクションの改善。	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。新しいノーマライザの拡張機能には、改善されたホワイトスペースの正規化、セミコロンの挿入、クロスサイトスクリプトの処理、識別子の正規化とデエイリアシング、ジャストインタイム（JIT）インスペクション、および外部スクリプトを検査する機能が含まれます。 デフォルトでは、新しいノーマライザは、システムが提供するすべてのネットワーク分析ポリシーで有効になっています。カスタムネットワーク分析ポリシーでパフォーマンスを調整するか、機能を無効にするには、https_inspect Snort 3 インスペクターで js_norm（改良されたノーマライザ）および normalize_javascript（従来のノーマライザ）設定を使用します。 正規化された JavaScript と照合するようにカスタム侵入ルールを構成するには、次のように js_data オプションを使用します。 `alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)`
Snort 3 デバイスの SMB 3 インスペクションの改善。	次の状況下で SMB 3 トラフィックの検査がサポートされるようになりました。 • SMB 透過フェールオーバー用に構成されたクラスタのファイルサーバーノードのフェールオーバー中。 • SMB スケールアウトを使用したクラスタの複数ファイルサーバーノード内。 • SMB ディレクトリリースによるディレクトリ情報の変更時。 • SMB マルチチャネルによる複数の接続の分散時。
[ポリシー管理（Policy Management）]	
アクセスコントロールポリシーのロック。	アクセス コントロール ポリシーをロックして、他の管理者が編集できないようにすることが可能になりました。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。アクセス コントロール ポリシーを変更する権限を持つすべてのユーザーには、それをロックする権限があります。 ポリシーの編集時にポリシーをロックまたはロック解除するアイコンがポリシー名の横に追加されました。さらに、他の管理者によってロックされたポリシーのロックを解除できるようにする新しい権限（アクセス コントロール ポリシー ロックのオーバーライド）が追加されました。この権限は、デフォルトで管理者、アクセス管理者、およびネットワーク管理者のロールで有効になっています。

機能	説明
オブジェクトグループ検索をデフォルトで有効化。	**アップグレードの影響** [オブジェクトグループ検索（Object Group Search）] の設定がデフォルトで有効になりました。バージョン 7.2 以降にアップグレードすると、この設定が有効になります。 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（Device）]** > **[詳細設定（Advanced Settings）]**
アクセス制御ルールのヒットカウントは再起動後も存続します。	管理対象デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントはHAペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。 新規/変更された CLI コマンド：**show rule hits**。
アクセスコントロールポリシーのユーザビリティの改善。	アクセスコントロールポリシーで使用できる新しいユーザーインターフェイスが追加されました。従来のユーザーインターフェイスを引き続き使用することも、新しいユーザーインターフェイスを試すこともできます。 新しいインターフェイスは、ルールリストのテーブルビューとグリッドビュー、列を表示または非表示にする機能、高度な検索機能、無限スクロール機能を備え、アクセス コントロール ポリシーが割り当てられたポリシーに関するパケットフローのビューがより明確になりました。また、ルール作成用の追加/編集ダイアログボックスがシンプルになりました。アクセス コントロール ポリシーの編集中に、従来のユーザーインターフェイスと新しいユーザーインターフェイスを自由に切り替えることができます。
イベントロギングおよび分析	

機能	説明
SecureX との統合、SecureX とのオーケストレーションの改善	SecureX との統合プロセスが合理化されました。すでに SecureX アカウントを持っている場合は、新しい [統合（Integration）] > [SecureX] ページで該当するクラウドリージョンを選択し、[SecureXの有効化（Enable SecureX）] をクリックして、SecureX に対して認証するだけです。イベントをクラウドに送信するオプション、およびCisco Success Network と Cisco Support Diagnostics を有効にするオプションも、この新しいページに移動されました。 この新しいページでSecureXとの統合を有効にすると、システムのクラウド接続のライセンス管理が Cisco Smart Licensing から SecureX に切り替わります。SecureX を「従来の」方法ですでに有効にしている場合、このクラウド接続管理による利点を得るには、無効にしてから再度有効にする必要があります。 Webインターフェースで示されていない場合でも、このページでは対象のクラウドリージョンや、シスコのセキュリティ分析とロギング（SaaS） を使用して Secure Network Analytics（Stealthwatch）クラウドに送信するイベントタイプも管理することを覚えておいてください。以前のバージョンでは、このオプションは、**システム**（⚙）> [統合（Integration）] > [クラウドサービス（Cloud Services）] にありました。SecureX を有効にしても、Secure Network Analytics クラウドとの通信には影響しません。両方にイベントを送信できます。 management center は SecureX オーケストレーションもサポートするようになりました。これは、セキュリティツール全体のワークフローを自動化するために使用できる強力なドラッグアンドドロップインターフェイスです。SecureX を有効にすると、オーケストレーションを有効にできます。 この機能は、バージョン7.0.2以降のメンテナンスリリースでもサポートされています。バージョン 7.1 ではサポートされていません。

機能	説明
セキュリティイベントのログを複数の Cisco Secure Network Analytics オンプレミスデータストアに記録。	Cisco Secure Network Analytics Data Store（マルチノード）との統合を設定する際、セキュリティイベント用に複数のフローコレクターを追加できるようになりました。各フローコレクターを、バージョン 7.0 以降を実行している 1 つ以上の Threat Defense デバイスに割り当てます。 新規/変更された画面： • セットアップ：**[統合（Integration）]** > **[セキュリティ分析とロギング（Security Analytics & Logging）]** > **[Secure Network Analytics Data Store]** • 変更：**[統合（Integration）]** > **[セキュリティ分析およびロギング（Security Analytics & Logging）]** > **[デバイス割り当ての更新（Update Device Assignments）]** この機能には、Cisco Secure Network Analytics バージョン 7.1.4 が必要です。
データベースアクセスの変更。	10 個の新しいテーブルを追加し、1 個のテーブルを廃止し、6 個のテーブルで結合を禁止しました。また、Snort 3 サポートのためにさまざまなテーブルにフィールドを追加し、可読形式でタイムスタンプと IP アドレスを提供しました。 詳細については、『Cisco Secure Firewall Management Center Database Access Guide, Version 7.2』の新機能のトピックを参照してください。
eStreamer の変更。	新しい Python ベースの参照クライアントが SDK に追加されました。また、完全修飾イベントをリクエストできるようになりました。詳細については、『Cisco Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2』の新機能のトピックを参照してください。
アップグレード	

機能	説明
デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	management center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレード パッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、management center には依存しません。各デバイスは、5 つのパッケージの同時転送に対応できます。 この機能は、同じスタンドアロン management center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。 • コンテナインスタンス。 • デバイスの高可用性ペアとクラスタ。 バージョン 7.1 以降のグループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できます。アップグレードパッケージを 1 つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。 • 高可用性 management center によって管理されるデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • 分析モードで management center に追加された CDO 管理対象デバイス。 • management center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 新規/変更された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

機能	説明
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。	バージョン 7.2 以降の Management Center を使用して Threat Defense をアップグレードする場合、**Snort 2 から Snort 3 へのアップグレード**を実行するかどうかを選択できるようになりました。 ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。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、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 このオプションは、バージョン 7.2 以降への Threat Defense のメジャーアップグレードおよびメンテナンスアップグレードでサポートされています。バージョン 7.0 または 7.1 への Threat Defense のアップグレード、または任意のバージョン向けのパッチではサポートされていません。
単一ノードクラスタのアップグレード。	デバイスのアップグレードページ（**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**）を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ（**[システム（System）]** > **[更新（Updates）]**）ではサポートされていません。 この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100

機能	説明
CLI からの Threat Defense アップグレードの復元。	Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべてのユニットを同時に復元すると、復元が成功する可能性が高くなります。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。 **注意** CLIから復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。
管理とトラブルシューティング	
Secure Firewall 3100 のパケットドロップ統計。	新しい **show packet-statistics** 脅威防御 CLI コマンドは、ポリシーに関連しないパケットドロップに関する包括的な情報を表示します。これまでは、いくつかのコマンドを使用してこの情報を表示する必要がありました。
DNS 要求を解決するための複数の DNS サーバーグループ。	クライアントシステムからの DNS 要求を解決するために、複数の DNS グループを設定できます。これらの DNS サーバー グループを使用して、さまざまな DNS ドメインの要求を解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバーを使用するキャッチオールのデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部 DNS サーバーを使用する別のグループを構成できます。したがって、組織のドメイン名を使用した FQDN への接続は、内部 DNS サーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS サーバーを使用します。 新規/変更された画面：**[プラットフォーム設定（Platform Settings）]** > **[DNS]**
使用タイプごとに脅威防御を使用して証明書の検証を設定します。	トラストポイント（脅威防御デバイス）で検証が許可される使用タイプを指定できるようになりました：IPsec クライアント接続、SSL クライアント接続、および SSL サーバー証明書。 新規/変更された画面：証明書登録オブジェクトに [検証の使用（Validation Usage）] オプションを追加しました：**[オブジェクト（Objects）]** > **[オブジェクトマネージャ（Object Manager）]** > **[PKI]** > **[証明書の登録（Cert Enrollment）]**。

機能	説明
展開で管理接続が失われた場合の自動ロールバック。	展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできるようになりました。以前は、**configure policy rollback** コマンドを使用して手動で設定をロールバックすることしかできませんでした。 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（Device）] > [展開設定（Deployment Settings）] • [展開（Deploy）] > [高度な展開（Advanced Deploy）] > [プレビュー（Preview）] • [展開（Deploy）] > [展開履歴（Deployment History）] > [プレビュー（Preview）]
設定の変更を展開するときに、レポートを生成して電子メールで送信します。	任意の展開タスクのレポートを生成できるようになりました。このレポートには、展開された設定に関する詳細が含まれています。 新規/変更されたページ：**[展開（Deploy）] > [展開履歴（Deployment History）]**[アイコン（icon）]**その他**（⋮）[全般的なレポート（Generate Report）]。
GeoDB を 2 つのパッケージに分割。	2022 年 5 月、バージョン 7.2 リリースの直前に、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 バージョン 7.2 以降の Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、または シスコ サポートおよびダウンロード サイト から 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されてインポートされます。ただし、更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、必ず両方の GeoDB パッケージを取得してインポートしてください。 • 国コードパッケージ：Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP パッケージ：Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar 地理位置情報の更新（**システム**（⚙） > [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）]）ページと概要ページ（[ヘルプ（Help）] > [概要（About）]）には、システムで現在使用されているパッケージのバージョンが一覧表示されます。

機能	説明
Webインターフェイスのフランス語オプション。	Management Center の Web インターフェイスをフランス語に切り替えることができるようになりました。 新規/変更された画面：**システム**（⚙）>[設定（Configuration）]>[言語（Language）]
Webインターフェイスの変更：展開とユーザーアクティビティの統合。	バージョン 7.2 では、すべてのケースで以下の Management Center メニューオプションが変更されています。 **[展開（Deploy）]>[展開履歴（Deployment History）]** は次に変更されました。 [展開（Deploy）]>**[展開履歴（Deployment History）]**（右下隅） **[展開（Deploy）]>[展開（Deployment）]** は次に変更されました。 [展開（Deploy）]>[高度な展開（Advanced Deploy）] [分析（Analysis）]>[ユーザー（Users）]>[アクティブなセッション（Active Sessions）] は次に変更されました。 [統合（Integration）]>[ユーザー（Users）]>[アクティブなセッション（Active Sessions）] [分析（Analysis）]>[ユーザー（Users）]>[ユーザー（Users）] は次に変更されました。 [統合（Integration）]>[ユーザー（Users）]>[ユーザー（Users）] [分析（Analysis）]>[ユーザー（Users）]>[ユーザーアクティビティ（User Activity）] は次に変更されました。 [統合（Integration ）]>[ユーザー（Users）]>[ユーザーアクティビティ（User Activity）]

機能	説明
Webインターフェイスの変更：SecureX、脅威インテリジェンス、およびその他の統合。	

機能	説明
	バージョン 7.0.1 以前、またはバージョン 7.1 からアップグレードする場合、バージョン 7.2 では Management Center のメニューオプションが変更されます。 （注） バージョン 7.0.2 またはそれ以降のバージョン 7.0.x メンテナンスリリースからアップグレードする場合、メニュー構造はすでに次のようになっています。 [AMP] > [AMP管理（AMP Management）] は次に変更されました。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）] [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] [インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] [インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）] [インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）] [インテリジェンス（Intelligence）] > [インシデント（Incidents）] は次に変更さ [統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）]

機能	説明		
		れました。	
	システム（⚙）>[統合（Integration）]	は次に変更されました。	[統合（Integration）]>[その他の統合（Other Integrations）]
	システム（⚙）>[ロギング（Logging）]>[セキュリティ分析とロギング（Security Analytics and Logging）]	は次に変更されました。	[統合（Integration）]>[セキュリティ分析とロギング（Security Analytics and Logging）]
	システム（⚙）>[SecureX]	は次に変更されました。	[統合（Integration）]>[SecureX]

Management Center REST API

新機能と既存の機能をサポートするために、Management Center REST API サービスと操作が追加されました。詳細については、『Cisco Secure Firewall Management Center REST API Quick Start Guide, Version 7.2』を参照してください。廃止されたサービス/操作については、Management Center バージョン 7.2 で廃止済みの機能 （30 ページ）を参照してください。

シャーシ	• breakoutinterfaces • evaluateoperation • joininterfaces
展開	• downloadreports • emailreports
デバイス	• eigrproutes • devicesettings • changemanagers

機能	説明
統合	• ebssnpshot • umbrellaconnections、testumbrellaconnections
License	• devicelicenses • smartlicenses
オブジェクト	• anyconnectexternalbrowserpackages、anyconnectpackages、anyconnectprofiles • certenrollments • certificatemaps • grouppolicies • hostscanpackages • ipv4addresspools、ipv6addresspools • radiusservergroups • ssoservers • umbrellaprotectionpolicies
ポリシー	• DNS：umbrelladnspolicies、umbrelladnsrules • NAT：autonatrules、manualnatrules • Health：healthpolicies • Remote access VPN：addressassignmentsettings、certificatemapsettings、connectionprofiles、ipsecadvancedsettings、ipseccryptomaps、ldapattributemaps、ravpns • Site-to-site VPN：s2svpnsummaries • Operational（non-policy-specific）：policylocks
検索	• デバイス
Status	• taskstatuses
トラブルシューティング	• task
アップグレード	• upgradesnapshot

Device Manager バージョン 7.2 の新機能

機能	説明
ファイアウォールと IPS の機能	
オブジェクトグループ検索は、アクセス制御のためにデフォルトで有効になっています。	CLI 構成コマンド **object-group-search access-control** は現在、デフォルトで有効になっています。FlexConfig を使用してコマンドを構成している場合は、FlexConfig オブジェクトを削除できます。この機能を無効にする必要がある場合は、FlexConfig を使用して **no object-group-search access-control** コマンドを実装します。
ルールのヒットカウントは再起動後も存続します。	デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。 次の Threat Defense CLI コマンドを変更しました：**show rule hits**。
VPN 機能	
IPsec フローがオフロードされます。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
インターフェイス機能	
Cisco Secure Firewall 3130 および 3140 のブレークアウトポートのサポート。	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成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）]** > **[インターフェイス（Interfaces）]**
インターフェイスでの Cisco TrustSec の有効化または無効化。	名前付きか名前なしかにかかわらず、物理、サブインターフェイス、EtherChannel、VLAN、管理、または BVI インターフェイスで Cisco TrustSec を有効または無効にできます。デフォルトでは、インターフェイスに名前を付けると、Cisco TrustSec が自動的に有効になります。 インターフェイス構成ダイアログボックスに [Propagate Security Group Tag] 属性を追加し、さまざまなインターフェイス API に **ctsEnabled** 属性を追加しました。
ライセンシング機能	

機能	説明
ISA 3000 の永久ライセンス予約のサポート。	ISA 3000 は、承認されたお客様向けのユニバーサル永久ライセンスの予約をサポートするようになりました。
管理およびトラブルシューティングの機能	
完全な展開を強制する機能。	変更を展開すると、システムは通常、最後の正常な展開以降に加えられた変更のみを展開します。ただし、問題が発生した場合は、デバイスの構成を完全に更新するフル展開を強制するように選択できます。展開ダイアログボックスに [Apply Full Deployment] オプションを追加しました。
Threat Defense REST API バージョン 6.3（v6）。	ソフトウェアバージョン 7.2 の Threat Defense REST API はバージョン 6.3 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.3 の URL バージョンパス要素は、6.0、6.1 および 6.2 と同じ v6 である点に注意してください。 使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、Device Manager にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。

バージョン 7.2 の新しいハードウェアと仮想プラットフォーム

表 *2:* バージョン *7.2.0* の新しいハードウェアと仮想プラットフォーム

機能	説明
Secure Firewall 3100 の NetMod。	Cisco Secure Firewall 3100 向けに次の NetMod が導入されました。 • 6 ポート 1 G SFP Fail-to-Wire ネットワークモジュール、SX（マルチモード）（FPR3K-XNM-6X1SXF） • 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-6X10SRF） • 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X10LRF） • 6 ポート 25 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-X25SRF） • 6 ポート 25 G Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X25LRF） • 8 ポート 1 G 銅ケーブル Fail-to-Wire ネットワークモジュール（銅ケーブル）（FPR3K-XNM-8X1GF） Management Center を導入すると、これらの NetMod がハードウェアバイパスをサポートします。
Alibaba 向け Management Center Virtual および Threat Defense Virtual。	Alibaba 向けの Secure Firewall Management Center Virtual および Secure Firewall Threat Defense が導入されました。Management Center を使用して、Alibaba 向け Threat Defense Virtual を管理する必要があります。デバイスマネージャーはサポートされていません。 Alibaba インフラストラクチャの根本的な問題により、Threat Defense Virtual のインスタンスタイプ ecs.g5ne.4xLarge は、特に 1 秒あたりの接続数（CPS）に関してパフォーマンスが低いことに注意してください。2xlarge または 4xlarge を推奨します。
デバイスマネージャが GCP 向け Threat Defense Virtual をサポート。	デバイスネージャを使用して、GCP 対応 Threat Defense Virtual を構成できるようになりました。

新しい侵入ルールとキーワード

アップグレードにより侵入ルールをインポートして自動的に有効化が可能です。

侵入ルールを更新（SRU/LSP）すると、新規および更新された侵入ルールとプリプロセッサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。現在のバージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、SRU/LSP を更新しても、そのルールはインポートされません。

アップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

Snort のバージョンを確認するには、互換性ガイドの「バンドルされたコンポーネント」の項を参照するか、次のコマンドのいずれかを使用します。

- Management Center：**[ヘルプ（Help）]** > **[概要（About）]**を選択します。
- Device Manager ：**show summary** CLI コマンドを使用します。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

廃止された機能

Management Center バージョン 7.2 で廃止済みの機能

表 *3 : Management Center* バージョン *7.2.0* で廃止済みの機能

機能	アップグレードの影響	説明
EIGRP FlexConfig オブジェクト。	なし。ただし、アップグレード後に構成をやり直す必要があります。	Management Center の Web インターフェイスから EIGRP ルーティングを設定できるようになりました。Management Center バージョン 7.2 の新機能 （1 ページ） を参照してください。 次の FlexConfig オブジェクトは不要になりました：Eigrp_Configure、Eigrp_Interface_Configure、Eigrp_Unconfigure、Eigrp_Unconfigure_all。 および、次の関連するテキストオブジェクトが廃止されました：eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary、eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon。 システムでは、アップグレード後に展開できますが、EIGRP 構成をやり直すように警告されます。このプロセスを支援するために、コマンドライン移行ツールが用意されています。詳細については、コンフィギュレーションガイドの FlexConfig ポリシーの移行 を参照してください。

機能	アップグレードの影響	説明
VXLAN FlexConfig オブジェクト。	なし。ただし、アップグレード後に構成をやり直す必要があります。	Management Center の Web インターフェイスから VXLAN インターフェイスを設定できるようになりました。Management Center バージョン 7.2 の新機能 （1 ページ） を参照してください。 次の FlexConfig オブジェクトは不要になりました：VxLAN_Clear_Nve、VxLAN_Clear_Nve_Only、VxLAN_Configure_Port_And_Nve、VxLAN_Make_Nve_Only、VxLAN_Make_Vni。 これらの関連するテキストオブジェクト：vxlan_Port_And_Nve、vxlan_Nve_Only、vxlan_Vni。 以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。
アップグレード前の自動トラブルシューティング。	管理センターのアップグレードは高速化され、使用するディスク容量も少なくなりましたが、アップグレード前のトラブルシューティング ファイルは含まれません。	時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。 管理センターのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。
REST API で SecureX との統合を設定。	なし。	SecureX 統合の改善の一環として（Management Center バージョン 7.2 の新機能 （1 ページ） を参照）、REST API を使用して SecureX との統合を設定できなくなりました。管理センターの Web インターフェイスを使用する必要があります。

廃止された FlexConfig コマンド

このドキュメントでは、今回のリリースで廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドと以前のリリースで廃止になった機能の完全なリストについては、コンフィギュレーション ガイドを参照してください。

⚠

注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

FlexConfig について

いくつかの Threat Defense の機能は、ASA 設定コマンドを使用して設定されます。Smart CLI または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。ご使用の構成は自動的に変換されません。アップグレード後は、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできません。

アップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。廃止されたコマンドが含まれている場合、メッセージは問題を示します。設定をやり直すことをお勧めします。新しい設定を確認したら、問題のある FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。