特長と機能

このドキュメントでは、バージョン7.4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。

アップグレードと展開により、システムでトラフィックが処理されるか、他の操作をしなくても異なる動作が発生する場合、機能がアップグレードに影響を与えます。これは特に、新しい脅威検出およびアプリケーション識別機能で一般的です。または、アップグレードプロセスに特別な要件がある場合もあります。たとえば、アップグレードの前後に非標準のタスクを実行する必要がある場合があります（特定のコンフィギュレーションの編集または削除、ヘルスポリシーの適用、Web インターフェイスでの FlexConfig コマンドのやり直しなど）。

重要 アップグレードでバージョンがスキップされる場合は、リリースノートで機能の履歴情報とアップグレードの影響を確認するか、該当する新機能（リリース別）[英語] ガイドを参照してください。

Management Center 機能

新しい 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、通常は Management Center およびデバイスの両方で最新のリリースが必要です。 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。

バージョン 7.4.1 の Management Center 機能

新機能

表 *1* : *Management Center* バージョン *7.4.1* の新機能

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
再導入された機能			
以前のメンテナンスリリースから機能が再導入されました。	7.4.1	機能に依存	バージョン 7.4.1 では、奇数番号のバージョン（7.1、7.3）やバージョン 7.4.0 のメンテナンスリリースに含まれなかったが、偶数番号のバージョン（7.0、7.2）のメンテナンスリリースに含まれていた機能、機能強化、および重要な修正が再導入されています。 アップグレードの影響は、機能によって異なります。 再導入された機能は次のとおりです。 • バージョン 7.3 でサポートされているすべてのデバイスプラットフォーム、および Firepower 1010E（7.2 で最後にサポート）での Threat Defense のサポート。 • Management Center によるインターフェイス同期エラーの検出。 • Web 分析プロバイダーを更新しました。
プラットフォーム（Platform）			
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	7.4.1	Cisco Secure Firewall 3130 および 3140 は次のネットワークモジュールをサポートするようになりました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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	7.4.1	Firepower 9300 は、次の光トランシーバをサポートするようになりました。 • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR 以下のネットワークモジュールでサポート： • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G 参照： Cisco Firepower 9300 ハードウェア設置ガイド
Cisco Secure Firewall 3100 のパフォーマンスプロファイルのサポート。	7.4.1	7.4.1	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 3100 に適用されるようになりました。以前は、この機能は Firepower 4100/9300、Cisco Secure Firewall 4200、および Threat Defense Virtual でサポートされていました。 参照：「Configure the Performance Profile」
[インターフェイス（Interfaces）]			
Azure と GCP 上の 3 つのインターフェイスを使用して Threat Defense Virtual を展開します。	7.4.1	7.4.1	Azure と GCP で（4 つではなく）3 つのインターフェイスを使用して Threat Defense Virtual を展開できるようになりました。そのためには、診断インターフェイスを削除します。 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** 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。 DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、Option 82 がすでに設定されている DHCP パケットを Threat Defense DHCP リレーエージェントが受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合、Threat Defense のデフォルトではそのパケットはドロップされます。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指定することで、Option 82 を維持したままパケットを転送できます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイスの追加/編集（Add/Edit Device）]** > **[DHCP]** > **[DHCP リレー（DHCP Relay）]** 参照：「」「Configure the DHCP Relay Agent」
Device Management			
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。	7.4.1	いずれか	Threat Defense プラットフォーム設定（NetFlow、SSH アクセス、SNMP ホスト、syslog サーバー）で設定されたデバイス管理サービスが、ユーザー定義の Virtual Routing and Forwarding（VRF）インターフェイスでサポートされるようになりました。 プラットフォームの制限：コンテナインスタンスまたはクラスタ化されたデバイスではサポートされていません。 参照：「Platform Settings」
NAT			
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。	7.4.1	いずれか	NAT ルールの編集時に、ネットワークオブジェクトに加えてネットワークグループを作成できるようになりました。 参照：「Customizing NAT Rules for Multiple Devices」
高可用性/拡張性：Threat Defense			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure Firewall 3100 のマルチインスタンスモード。	7.4.1	7.4.1	Secure Firewall 3100 は、単一のデバイス（アプライアンスモード）または複数のコンテナインスタンス（マルチインスタンスモード）として展開できます。マルチインスタンスモードでは、完全に独立したデバイスとして機能する複数のコンテナインスタンスを 1 つのシャーシに展開できます。マルチインスタンスモードでは、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレード対象（シャーシのアップグレード）になることに注意してください。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [シャーシ（Chassis）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [Chassis Manager]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [新しいポリシー（New Policy）] > [シャーシプラットフォーム設定（Chassis Platform Settings）]** • **[デバイス（Devices）] > [シャーシのアップグレード（Chassis Upgrade）]** 新規/変更された Threat Defense CLI コマンド：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新規/変更された FXOS CLI コマンド：**create device-manager**、**set deploymode** プラットフォームの制限：Cisco Secure Firewall 3105 ではサポートされていません。 参照：「Multi-Instance Mode for the Secure Firewall 3100」 および Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
VMware および KVM 向け Threat Defense Virtual の 16 ノードクラスタ	7.4.1	7.4.1	VMware の仮想 Threat Defense と KVM の仮想 Threat Defense に 16 ノードクラスタを構成できるようになりました。 参照：「Clustering for Threat Defense Virtual in a Private Cloud」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
AWS のクラスタ化された Threat Defense Virtual デバイスのターゲットフェールオーバー。	7.4.1	7.4.1	AWS Gateway Load Balancer（GWLB）を使用して AWS のクラスタ化された Threat Defense Virtual デバイスのターゲットフェールオーバーを設定できるようになりました。 プラットフォームの制限：5 台および 10 台のデバイスライセンスでは使用できません。 参照：「Configure Target Failover for Threat Defense Clustering with GWLB in AWS」
Threat Defense 高可用性ペアの設定の不一致を検出します。	7.4.1	7.4.1	CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。 新規/変更された CLI コマンド：**show failover config-sync error**、**show failover config-sync stats** 参照：「Troubleshoot Configuration Sync Failure」および Cisco Secure Firewall Threat Defense コマンドリファレンス
高可用性：Management Center			
高可用性 Management Center 用の単一のバックアップファイル。	7.4.1	いずれか	高可用性ペアのアクティブ Management Center の設定だけのバックアップを実行すると、いずれかのユニットの復元に使用できる単一のバックアップファイルが作成されるようになりました。 参照：「」「Unified Backup of Management Centers in High Availability」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center の高可用性同期の機能拡張。	7.4.1	いずれか	Management Center の高可用性（HA）には、次の同期機能拡張が含まれています。 • 設定履歴ファイルが大きいと、遅延の大きいネットワークで同期が失敗する可能性があります。これを防ぐために、デバイス設定履歴ファイルは他の設定データと並行して同期されるようになりました。この機能拡張により、同期時間も短縮されます。 • Management Center は、設定履歴ファイルの同期プロセスをモニターし、同期がタイムアウトした場合に正常性アラートを表示するようになりました。 新規/変更された画面：次の画面でこれらのアラートを確認できます。 • [通知（Notifications）] > [メッセージセンター（Message Center）] > [正常性（Health）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）] > [ステータス （Status）]（[概要（Summary）] の下） 参照：「Viewing Management Center High Availability Status」
SD-WAN			
[Cisco SD-WANサマリー（SD-WAN Summary）] ダッシュボードのアプリケーションモニタリング。	7.4.1	7.4.1	[Cisco SD-WANサマリー（SD-WAN Summary）] ダッシュボードで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モニターできるようになりました。 新規/変更された画面：**[概要（Overview）] > [Cisco SD-WANサマリー（SD-WAN Summary）] > [アプリケーション モニタリング（Application Monitoring）]** 参照：「WAN Summary Dashboard」
VPN			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure Firewall 3100 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。	7.4.1	7.4.1	**アップグレードの影響。条件を満たす接続のオフロードが開始されます。** Cisco Secure Firewall 3100 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るようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。 この機能はアップグレードにより自動的に有効になります。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 参照：「IPSec Flow Offload」
Cisco Secure Firewall 4100/9300 の暗号デバッグの機能拡張。	7.4.1	7.4.1	バージョン 7.4.0 で導入された暗号デバッグの機能拡張は、Cisco Secure Firewall 3100 および Firepower 4100/9300 に適用されるようになりました。以前は、Cisco Secure Firewall 4200 でのみサポートされていました。 参照：「Troubleshooting Using Crypto Archives」
ルートベース VPN の VTI の詳細を表示します。	7.4.1	いずれか	管理対象デバイスのルートベース VPN の仮想トンネルインターフェイス（VTI）の詳細を表示できるようになりました。ダイナミック VTI の動的に作成されたすべての仮想アクセスインターフェイスの詳細も表示できます。 新規/変更された画面：[デバイス（Device）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit a device）] > [インターフェイス（Interfaces）] > [仮想トンネル（Virtual Tunnels）] タブ。 参照：「About Virtual Tunnel Interfaces」
ルーティング			
FlexConfig を使用して、IS-IS インターフェイスで BFD ルーティングを設定します。	7.4.1	7.4.1	FlexConfig を使用して、物理、サブインターフェイス、および EtherChannel IS-IS インターフェイスで Bidirectional Forwarding Detection（BFD）ルーティングを設定できるようになりました。 参照：「Guidelines for BFD Routing」
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	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Zero Trust アクセスの機能拡張。	7.4.1	7.4.1（Snort 3）	Management Center には、次の Zero Trust アクセスの機能拡張が含まれています。 • アプリケーションの送信元NAT を設定できます。設定されたネットワークオブジェクトまたはオブジェクトグループは、着信要求のパブリックネットワークの送信元 IP アドレスを、アプリケーション ネットワーク内のルーティング可能な IP アドレスに変換します。 • 診断ツールを使用して、Zero Trust 設定の問題をトラブルシューティングできます。 • エクスペリエンスを向上させるために、Zero Trust アプリケーションポリシーのテレメトリデータを収集するようになりました。 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[Zero Trustアプリケーション（Zero Trust Application）]** 新規/変更された CLI コマンド：**show running-config zero-trust**、**show zero-trust statistics** 参照： • アプリケーションの作成 • Zero Trust セッションのモニタリング • Cisco Secure Firewall Threat Defense コマンドリファレンス • Cisco Secure Firewall Management Center から収集される Cisco Success Network テレメトリデータ
CIP 検出。	7.4.1	7.4.1（Snort 3）	セキュリティポリシーで CIP およびイーサネット/IP（ENIP）アプリケーション条件を使用することで、Common Industrial Protocol（CIP）を検出して処理できるようになりました。 参照：「Application Rule Conditions」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
CIP 安全検出。	7.4.1	7.4.1（Snort 3）	CIP Safety は、産業自動化アプリケーションの安全な動作を可能にする CIP 拡張機能です。CIP インスペクタは、CIP トラフィック内の CIP Safety セグメントを検出できるようになりました。CIP Safety セグメントを検出してアクションを実行するには、Management Center のネットワーク分析ポリシーで CIP インスペクタを有効にし、アクセス コントロール ポリシーに割り当てます。 新規/変更された画面：[ポリシー（Policies）] > [アクセス制御（Access Control）] > [ポリシーの編集（Edit a policy）] > [ルールの追加（Add Rule）] > [アプリケーション（Applications）] タブの順に選択し、検索ボックスで CIP Safety を検索します。 参照：Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語]
Access Control：**Identity**			

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

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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	7.4.1	以前に接続していたデバイスとは異なる管理対象デバイスに認証セッションが送信されたときに、ユーザーの認証が必要かどうかを決定します。ユーザーがロケーションまたはサイトを変更するたびに認証する必要がある組織の場合は、このオプションを無効にする必要があります。 • (デフォルト) 有効にすると、ユーザーはアクティブな認証アイデンティティルールに関連付けられた管理対象デバイスで認証できます。 • アクティブな認証ルールが展開されている別の管理対象デバイスでユーザーがすでに認証されている場合でも、別の管理対象デバイスでの認証をユーザーに要求する場合は無効にします。 新規/変更された画面：**[ポリシー（Policies）] > [アイデンティティ（Identity）] >（ポリシーの編集） > [アクティブ認証（Active Authentication）] > [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** 参照：「How to Configure the Captive Portal for User Control」
Management Center の Web インターフェイスを使用して、ダウンロード可能なアクセス制御リストを RADIUS アイデンティティソースのシスコ属性値ペア ACL とマージします。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** 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）] > [AAAサーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）] > [RADIUSサーバーグループの追加（Add RADIUS Server Group）] > [ダウンロード可能ACL とシスコAVペアACLの結合（Merge Downloadable ACL with Cisco AV Pair ACL）]** 新しい CLI コマンド： • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair** 参照：「RADIUS Server Group Options」
イベントロギングおよび分析			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
統合イベントビューアからパケットトレーサを開きます。	7.4.1	いずれか	統合イベントビュー（**[分析（Analysis）] > [統合イベント（Unified Events）]**）からパケットトレーサを開けるようになりました。目的のイベントの横にある省略記号アイコン（[...]）をクリックし、[パケットトレーサで開く（Open in Packet Tracer）] をクリックします。 参照：「Working with the Unified Event Viewer」
ヘルス モニタリング			
Firepower 4100/9300 のシャーシレベルのヘルスアラート。	7.4.1	FXOS 2.14.1 を搭載したすべて	**アップグレードの影響。新しい正常性モジュールを有効にし、アップグレード後にデバイス正常性ポリシーを適用します。** シャーシを読み取り専用デバイスとして Management Center に登録することで、Firepower 4100/9300 のシャーシレベルのヘルスアラートを表示できるようになりました。また、Firewall Threat Defense プラットフォーム障害のヘルスモジュールを有効にして、ヘルスポリシーを適用する必要があります。アラートは、メッセージセンター、ヘルスモニター（左側のペインの [デバイス（Devices）] でシャーシを選択）、およびヘルスイベントビューに表示されます。 マルチインスタンスモードで Cisco Secure Firewall 3100 のシャーシを追加し、正常性アラートを表示することもできます。これらのデバイスの場合は、Management Center を使用してシャーシを管理します。ただし、Firepower 4100/9300 シャーシの場合は、シャーシマネージャまたは FXOS CLI を使用する必要があります。 新規/変更された画面：**[デバイス（Devices）]> [デバイス管理（Device Management）] > [追加（Add）] > [シャーシ（Chassis）]** 参照：「Add a Chassis to the Management Center」
展開履歴（ロールバック）ファイルによって使用される過剰なディスク容量に関する正常性アラート。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に Management Center の正常性ポリシーを展開します。** Disk Usage 正常性モジュールは、展開履歴（ロールバック）ファイルが Management Center で過剰なディスク容量を使用している場合にアラートを発行するようになりました。 参照：「Disk Usage for Device Configuration History Files Health Alert」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
NTP 同期の問題に関する正常性アラート。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に Management Center の正常性ポリシーを展開します。** 新しい Time Server Status 正常性モジュールは、NTP 同期に関する問題を報告します。 参照：「」「Time Synchronization」および「Health Modules」
Management Center のメモリ使用率の計算、アラート、およびスワップメモリのモニタリングが改善されました。	7.4.1	いずれか	**アップグレードの影響。メモリ使用量アラートのしきい値が引き下げられる可能性があります。** Management Center のメモリ使用量の精度が向上し、デフォルトのアラートしきい値が警告は 88%、重大は 90% に引き下げられました。しきい値が新しいデフォルト値よりも高かった場合、アップグレードによって自動的に下げられます。この変更を有効にするために正常性ポリシーを適用する必要はありません。高メモリプロセスを終了できない場合、システムメモリが極めて少ない状態で Management Center が再起動する可能性があることに注意してください。 新規または既存の Management Center の正常性ダッシュボードに新しいスワップメモリ使用状況メトリックを追加することもできます。[メモリ（Memory）] 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（⚙） > [正常性（Health）] > [モニタリング（Monitoring）] > [Firewall Management Center][ダッシュボードの追加/編集（Add/Edit Dashboard）][メモリ（Memory）]** • **システム（⚙） > [正常性（Health）] > [ポリシー（Policy）] > [Management Center正常性ポリシー（Management Center Health Policy）] > [メモリ（Memory）]** 参照：「Using Management Center Health Monitor」
展開とポリシー管理			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
変更管理。	7.4.1	いずれか	変更を展開する前の監査追跡や正式な承認など、設定変更に関してより正式なプロセスを実装する必要がある組織の場合は、変更管理を有効にできます。 この機能を有効にするための **システム**（⚙）> **[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**（⚙）> **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。 参照：「Change Management」
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。	7.4.1	いずれか	前回の展開以降の設定変更に関する次のレポートを生成、表示、および（zip ファイルとして）ダウンロードできます。 • ポリシー内の追加、変更、または削除、あるいはデバイスに展開されるオブジェクトをプレビューする各デバイスのポリシー変更レポート。 • ポリシー変更レポート生成のステータスに基づいて各デバイスを分類する統合レポート。 これは、Management Center または Threat Defense デバイスのいずれかのアップグレード後に特に役立ち、展開する前にアップグレードによって加えられた変更を確認できます。 新規/変更された画面：**[展開（Deploy）]** > **[高度な展開（Advanced Deploy）]**。 参照：「Download Policy Changes Report for Multiple Devices」
デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。	7.4.1	いずれか	デバイスのロールバックのために保持する展開履歴ファイルの数を最大 10（デフォルト）まで設定できるようになったため、Management Center のディスク容量を節約できます。 新規/変更された画面：[展開（Deploy）] > **[Deployment History]**（🕘）> [展開設定（Deployment Setting）] > [構成バージョン設定（Configuration Version Setting）] 参照：「」「Set the Number of Configuration Versions」
のアップグレード			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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。	7.4.1	いずれか	

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			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。これには、Management Center、Threat Defense デバイス、およびすべての古いNGIPSv/ASA FirePOWER デバイスが含まれます。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。 リスト/直接ダウンロードアップグレードパッケージを取得するには、インターネットアクセスが必要です。インターネットアクセスがない場合は、手動管理に限定されます。適切なメンテナンスリリースのアプライアンスが少なくとも 1 つある（またはパッチを手動でアップロードした）場合を除き、パッチは表示されません。ホットフィックスは手動でアップロードする必要があります。 新規/変更された画面： • **システム**（⚙）> **製品のアップグレード**では、Management Center とすべての管理対象デバイスをアップグレードし、アップグレードパッケージを管理します。 • **システム**（⚙）> **[コンテンツの更新（Content Updates）]**で、侵入ルール、VDB、およびGeoDB を更新できるようになりました。 • **[デバイスの脅威防御のアップグレード**>（**Devices 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。 • **システム**（⚙）> **[ユーザー（Users）]** > **[ユーザーロール（User Role）]** > **[ユーザーロールの作成（Create User Role）]** > **[メニューベースの権限（Menu-Based Permissions）]**を使用すると、[製品のアップグレード（Product Upgrades）]（システムソフトウェア）へのアクセスを許可せずに、[コンテンツの更新（Content Updates）]（VDB、GeoDB、侵入ルール ）へのアクセスを許可できます。 廃止された画面/オプション： • **システム**（⚙）> **[更新（Updates）]**は廃止されました。脅威防御アップグレードはすべてウィザードを使用するようになりました。 • 脅威防御アップグレードウィザードの [アップグレードパッケー

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			ジの追加（Add Upgrade Package）]ボタンは、新しいアップグレードページへの[アップグレードパッケージの管理（Manage Upgrade Packages）]リンクに置き換えられました。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
推奨リリースの通知。	7.4.1	いずれか	新しい推奨リリースが利用可能になると、Management Center から通知されるようになりました。今すぐアップグレードしない場合は、後でシステムに通知するか、次の推奨リリースまでリマインダを延期できます。新しいアップグレードページには、推奨リリースも示されます。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）
アップグレード：Threat Defense			
Threat Defense のアップグレードウィザードからの復元の有効化。	7.4.1	いずれか	脅威防御アップグレードウィザードからの復元を有効化できます。 その他のバージョンの制限：Threat Defense をバージョン 7.1 以降にアップグレードする必要があります。 参照：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。	7.4.1	いずれか	Threat Defense アップグレードウィザードの最終ページで、アップグレードの進行状況をモニターできるようになりました。この機能は、[デバイス管理（Device Management）]ページの[アップグレード（Upgrade）]タブおよび Management Center の既存のモニタリング機能に追加されます。新しいアップグレードフローを開始していない限り、**[デバイス（Devices）] > [Threat Defenseアップグレード（Threat Defense Upgrade）]**によってこのウィザードの最後のページに戻り、現在の（または最後に完了した）デバイスのアップグレードの詳細なステータスを確認できます。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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。	7.4.1	いずれか	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。マルチインスタンスモードの Cisco Secure Firewall 3100（バージョン 7.4.1 の新機能）には、FXOS とファームウェアのアップグレードもバンドルされています。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
アップグレード：Management Center			
Management Center の新しいアップグレード ウィザード。	7.4.1	いずれか	新しいアップグレード開始ページとウィザードにより、Management Center のアップグレードを簡単に実行できます。**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]**を使用して、Management Center で適切なアップグレードパッケージを入手したら、[アップグレード（Upgrade）] をクリックして開始します。 その他のバージョンの制限：バージョン 7.4.1 以降からの Management Center のアップグレードでのみサポートされます。 Management Center を任意のバージョンにアップグレードするには、Management Center で現在実行しているバージョンのアップグレードガイドを参照してください。：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド。バージョン 7.4.0 を実行している場合は、バージョン 7.3.x のガイドを使用できます。

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center のアップグレード後に設定変更レポートを自動的に生成します。	7.4.1	いずれか	Management Center のメジャーおよびメンテナンスアップグレード後に、設定変更に関するレポートを自動的に生成できます。このレポートは、展開しようとしている変更を理解するのに役立ちます。レポートが生成されたら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。 その他のバージョンの制限：バージョン 7.4.1 以降の Management Center のアップグレードでのみサポートされます。バージョン 7.4.1 以前のバージョンへのアップグレードはサポートされていません。 新規/変更された画面：**システム**（⚙）**>[設定（Configuration）]>[設定のアップグレード（Upgrade Configuration）]>[アップグレード後のレポートの有効化（Enable Post-Upgrade Report）]** 参照：「Upgrade Configuration」
同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。	7.4.1	任意	ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
管理（Administration）			
Management Center ハードウェアのハードドライブを消去します。	7.4.1	いずれか	Management Center CLI を使用してリブートし、ハードドライブデータを完全に消去できます。消去が完了したら、新しいソフトウェアイメージをインストールできます。 新規/変更された CLI コマンド： **secure erase** 参照：「Secure Firewall Management Center Command Line Reference」
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。	7.4.1	いずれか	**アップグレードの影響。システムは新しいリソースに接続します。** Management Center では、ソフトウェア アップグレード パッケージの直接ダウンロードの場所が sourcefire.com から amazonaws.com に変更されています。 参照：「」「 Internet Access Requirements」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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。	7.4.1	いずれか	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [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**（⚙）>**[製品のアップグレード（Product Upgrades）]**を使用します。 参照：「」「Software Update Automation」
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			
アクセス制御オブジェクトの最適化を有効または無効にします。	7.4.1	いずれか	Management Center の Web インターフェイスからアクセス制御オブジェクトの最適化を有効化または無効化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）]**>**[アクセス コントロールの設定（Access Control Preferences）]**>**[オブジェクトの最適化（Object Optimization）]** 参照：「Access Control Preferences」および「Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations」。
クラスタ制御リンク ping ツール。	7.4.1	いずれか	ping を実行して、すべてのクラスタノードがクラスタ制御リンクを介して相互に到達できることを確認できます。ノードがクラスタに参加できない主な原因の 1 つは、クラスタ制御リンクの設定が正しくないことです。たとえば、クラスタ制御リンクの MTU が、接続しているスイッチの MTU よりも大きい値に設定されている可能性があります。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**その他**（⋮）>**[クラスタのライブステータス（Cluster Live Status）]** 参照：「」「Perform a Ping on the Cluster Control Link」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
トラブルシューティングファイルの生成とダウンロードは、[デバイス（Device）] および [クラスタ（Cluster）] ページから実行できます。	7.4.1	7.4.1	[デバイス（Device）] ページの各デバイス、および [クラスタ（Cluster）] ページのすべてのクラスタノードのトラブルシューティングファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。または、**[デバイス（Devices）] > [デバイス管理（Device Management）] > その他**（⋮）> [トラブルシューティング ファイル（Troubleshoot Files）] メニューからファイル生成をトリガーできます。 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（Device）] > [全般（General）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [全般（General）]** 参照：「Generate Troubleshooting Files」
クラスタへの参加に失敗した場合のノードでのトラブルシューティングファイルの自動生成。	7.4.1	7.4.1	ノードがクラスタに参加できない場合、そのノードのトラブルシューティング ファイルが自動的に生成されます。[タスク（Tasks）] または [クラスタ（Cluster）] ページからファイルをダウンロードできます。 参照：「Troubleshooting the Cluster」
デバイスまたはデバイスクラスタの CLI 出力を表示します。	7.4.1	いずれか	デバイスまたはクラスタのトラブルシューティングに役立つ一連の定義済み CLI 出力を表示できます。また、任意の **show** コマンドを入力して、出力を確認できます。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [全般（General）]** 参照：「View CLI Output」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Snort 3 はメモリ使用量が過剰になると再起動し、HA フェールオーバーがトリガーされることがあります。	7.4.1	7.4.1（Snort 3）	操作の継続性を向上させるために、Snort によるメモリ使用が過剰な場合、高可用性フェールオーバーをトリガーできるようになりました。これは、プロセスのメモリ使用が過剰な場合に Snort 3 が再起動されるようになったためです。Snort プロセスを再起動すると、デバイスでのトラフィックフローと検査が一時的に中断され、高可用性展開ではフェールオーバーがトリガーされる可能性があります（スタンドアロン展開では、インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます）。 この機能は、デフォルトでイネーブルにされています。CLI を使用して無効にしたり、メモリしきい値を設定したりできます。 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。 新規/変更された CLI コマンド：**configure snort3 memory-monitor**、**show snort3 memory-monitor-status** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Snort 3 コアダンプの頻度を設定します。	7.4.1	7.4.1（Snort 3）	Snort 3 コアダンプの頻度を設定できるようになりました。Snort がクラッシュするたびにコアダンプを生成する代わりに、次回 Snort がクラッシュしたときにのみコアダンプを生成できます。または、過去 1 日あるいは 1 週間以内にクラッシュが発生していない場合に生成します。 Snort 3 コアダンプは、スタンドアロンデバイスではデフォルトで無効になっています。高可用性およびクラスタ化されたデバイスの場合、デフォルトの頻度が毎回ではなく 1 日に 1 回になりました。 新規/変更された CLI コマンド：**configure coredump snort3**、**show coredump** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Cisco Secure Firewall 3100/4200 でドロップされたパケットをキャプチャします。	7.4.1	7.4.1	MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100/4200 は、これらのドロップされたパケットをキャプチャできるようになりました。 新規/変更された CLI コマンド：**capture** コマンドの [**drop** { **disable** | **mac-filter** }]。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
データプレーン障害後の迅速なリカバリ。	7.4.1	7.4.1	データプレーンプロセスがクラッシュした場合、デバイスをリブートする代わりに、データプレーンプロセスのみリロードするようになりました。データプレーンプロセスのリロードに加えて、Snortおよび他のいくつかのプロセスもリロードされます。 ただし、ブートアップ中にデータプレーンプロセスがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードプロセスループの発生を回避できます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。 新規/変更された CLI コマンド：**data-plane quick-reload**、**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 プラットフォームの制限：マルチインスタンスモードではサポートされていません。 参照：Cisco Secure Firewall Threat Defense コマンドリファレンス および『Cisco Secure Firewall ASA シリーズ コマンド リファレンス』

廃止された機能

表 *2 : Management Center* バージョン *7.4.1* で廃止済みの機能

機能	Management Center では廃止	Threat Defense では廃止	詳細（Details）
廃止：イベント正常性アラートの頻繁なドレイン。	7.4.1	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。Management Center のアップグレード後も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをバージョン 7.4.1 以降にアップグレードする（アラートの送信を停止する）まで、アラートが表示され続ける場合があります。 参照：「Disk Usage and Drain of Events Health Monitor Alerts」

機能	Management Center では廃止	Threat Defense では廃止	詳細（Details）
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。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。 参照：「Configure the DHCP Relay Agent」
廃止：ダウンロード可能なアクセス制御リストと、FlexConfig を使用した RADIUS アイデンティティソースのシスコ属性値ペア ACL のマージ。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** 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。

バージョン 7.4.0 の Management Center 機能

（注） バージョン 7.4.0 は、Cisco Secure Firewall Management Center および Cisco Secure Firewall 4200 でのみ使用できます。バージョン 7.4.0 Management Center は他のデバイスモデルの古いバージョンを管理できますが、Threat Defense 7.4.0 を必要とする機能には Cisco Secure Firewall 4200 を使用する必要があります。他のすべてのデバイス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。

新機能

表 *3 : Management Center* バージョン *7.4.0* の新機能

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
以前のメンテナンスリリースから機能が再導入されました。	7.4.0	機能に依存	バージョン 7.4.0 では、奇数番号のバージョン（7.1、7.3）のメンテナンスリリースに含まれなかったが、偶数番号のバージョン（7.0.x、7.2.x）のメンテナンスリリースに含まれていた機能、機能拡張および重要な修正が再度サポートされます。 再導入された機能は次のとおりです。 • アクセス制御のパフォーマンスの向上（オブジェクトの最適化）。
プラットフォーム			
Management Center 1700、2700、4700。	7.4.0	いずれか	最大 300 台のデバイス管理が可能な Cisco Secure Firewall Management Center 1700、2700、および 4700 が導入されました。Management Center の高可用性がサポートされています。 参照： Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide
Microsoft Hyper-V 向けの Management Center Virtual。	7.4.0	いずれか	最大 25 台のデバイスを管理できる Microsoft Hyper-V 向けの Cisco Secure Firewall Management Center Virtual を導入しました。Management Center の高可用性がサポートされています。 参照： Cisco Secure Firewall Management Center Virtual 入門ガイド
Cisco Secure Firewall 4200。	7.4.0	7.4.0	Cisco Secure Firewall 4215、4225、および 4245 を導入しました。Management Center を使用してこれらのデバイスを管理する必要があります。デバイスマネージャはサポートしていません。 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

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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	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」
プラットフォームの移行			
Firepower 1000/2100 から Cisco Secure Firewall 3100 への移行。	7.4.0	いずれか（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：「About Secure Firewall Threat Defense Model Migration」
Firepower Management Center 4600 から Cisco Secure Firewall Management Center for AWS への移行。	7.4.0	いずれか	Firepower Management Center 4600 から Cisco Secure Firewall Management Center for AWS（300 台のデバイスライセンスあり）への移行。 参照： Cisco Secure Firewall Management Center モデル移行ガイド
Firepower Management Center 1600/2600/4600 から Cisco Secure Firewall Management Center 1700/2700/4700 への移行。	7.4.0	いずれか	Firepower Management Center 1600/2600/4600 を Cisco Secure Firewall Management Center 1700/2700/4700 に移行できます。 参照： Cisco Secure Firewall Management Center モデル移行ガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Firepower Management Center 1000/2500/4500 から Cisco Secure Firewall Management Center 1700/2700/4700 への移行。	7.4.0	7.0.0	

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			Firepower Management Center 1000/2500/4500 を Cisco Secure Firewall Management Center 1700/2700/4700 に移行できます。移行するには、古い Management Center をバージョン 7.0 からバージョン 7.4 に一時的にアップグレードする必要があります。 **重要** バージョン 7.4 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、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。新しい Management Center も設定する必要があります。 **2.** 古い 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 7.0.0 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.** 古い Management Center をバージョン 7.4 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 にアップロードします。Special Release からダウンロードします。 **4.** モデル移行ガイドの説明に従って、Management Center を移行します。 **5.** 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せず、元に戻す場合、1000/2500/4500 の一般的な操作ではバージョン 7.4 がサポートされていないことに注意してください。古い Management Center をサポートされているバージョンに戻すには、バージョン 7.0 に再イメージ化し、バッ

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			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 • Cisco Secure Firewall Management Center モデル移行ガイド 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。

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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。	7.4.0	7.0.3	

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			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 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 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 にアップグレードします。

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			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 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 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。
Device Management			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
シリアル番号を使用して Firepower 1000/2100 および Cisco Secure Firewall 3100を Management Centerに登録するロータッチプロビジョニング。	7.4.0	Management Center がパブリックに到達可能：7.2.0 Management Center がパブリックに到達できない：7.2.4	ロータッチプロビジョニングを使用すると、Firepower 1000/2100 および Cisco Secure Firewall 3100 デバイスで初期セットアップを実行することなく、シリアル番号でデバイスを Management Center に登録できます。Management Center は、この機能のために SecureX および Cisco Defense Orchestrator と統合されています。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（Device）]** > **[シリアル番号（Serial Number）]** その他のバージョンの制限：この機能は、Management Center がパブリックに到達できない場合、バージョン 7.3.x または 7.4.0 Threat Defense デバイスではサポートされません。バージョン 7.4.1 でサポートが再開されています。 参照：「Add a Device to the Management Center Using the Serial Number (Low-Touch Provisioning)」
[インターフェイス（Interfaces）]			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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	7.4.0	**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、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。 7.4 以降にアップグレードし、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** 参照：「Merge the Management and Diagnostic Interfaces」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
VXLAN VTEP IPv6 のサポート。	7.4.0	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	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	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	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
データインターフェイスを使用して、Threat Defense ハイアベイラビリティペアを管理します。	7.4.0	7.4.0	Threat Defense ハイアベイラビリティでは、Management Center との通信に通常のデータインターフェイスを使用できるようになりました。以前は、スタンドアロンデバイスのみがこの機能をサポートしていました。 参照：「Using the Threat Defense Data Interface for Management」
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	7.4.0	参照：「」「Heartbeat Module Redundancy」
SD-WAN			
WAN サマリーダッシュボード。	7.4.0	7.2.0	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。 新規/変更された画面：[概要（Overview）] > [WANサマリー（WAN Summary）] 参照：「WAN Summary Dashboard」
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。	7.4.0	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」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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	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できます。 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			
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	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	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	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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。	7.4.0	7.1.0	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 Cisco Secure Client」
VPN：サイト間			
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。	7.4.0	いずれか	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 」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
接続イベントのサイト間 VPN 情報	7.4.0	7.4.0（Snort 3）	接続イベントに、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、[VPNアクション（VPN Action）] の 3 つの新しいフィールドが含まれるようになりました。ポリシーベースおよびルートベースのサイト間 VPN トラフィックの場合、これらのフィールドにより、接続が暗号化または復号化（またはその両方）されたかどうか、および実行ユーザーが示されます。 新規/変更された画面：**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）] > [イベントのテーブルビュー（Table View of Events）]** 参照：「Site to Site VPN Connection Event Monitoring」
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。	7.4.0	いずれか	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」
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。	7.4.0	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	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
動的 VTI による仮想ルーティング。	7.4.0	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			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
クライアントレスの Zero Trust アクセス。	7.4.0	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」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
暗号化された可視性エンジン機能の拡張。	7.4.0	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」
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	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」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
カスタム アプリケーションディテクタを使用した最初のパケットアプリケーションの識別。	7.4.0	7.4.0（Snort 3）	新しい Lua ディテクタ API が導入され、TCP セッションの最初のパケットの IP アドレス、ポート、およびプロトコルがアプリケーションプロトコル（サービス AppID）、クライアントアプリケーション（クライアント AppID）、および Web アプリケーション（ペイロード AppID）にマッピングされます。この新しい Lua API addHostFirstPktApp は、パフォーマンスの向上、再検査、およびトラフィック内の攻撃の早期検出に使用されます。この機能を使用するには、カスタムアプリケーション ディテクタの高度なディテクタで検出基準を指定して、Lua ディテクタをアップロードする必要があります。 参照：「Custom Application Detectors」
機密データの検出とマスキング。	7.4.0	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」
JavaScript インスペクションの改善。	7.4.0	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]
ファイルおよびマルウェアイベントに含まれる MITRE 情報。	7.4.0	7.4.0	ファイルおよびマルウェアイベントに MITRE 情報（ローカルマルウェア分析結果）が含まれるようになりました。以前は、この情報は侵入イベントについてのみ利用可能でした。MITRE 情報は、クラシックイベントビューと統合イベントビューの両方で表示できます。MITRE 列は、両方のイベントビューでデフォルトで非表示になっていることに注意してください。 参照：「Local Malware Analysis」および「File and Malware Event Fields」
Access Control：**Identity**			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure 動的属性コネクタによる動的オブジェクト管理の機能強化。	7.4.0	いずれか（Any）	次を使用した動的オブジェクト管理がサポートされるようになりました。 • Management Center の Cisco Secure 動的属性コネクタ。 • スタンドアロン アプリケーションとしての Cisco Secure 動的属性コネクタ 2.1。 参照：「Cisco Secure Dynamic Attributes Connector」および Cisco Secure Dynamic Attributes Connector コンフィギュレーション ガイド、バージョン2.1 [英語]
ユーザー ID ソースとしての Microsoft Azure AD。	7.4.0	7.4.0	Microsoft Azure Active Directory（Azure AD）レルムと ISE を使用すると、ユーザーを認証したりユーザー制御のためにユーザーセッションを取得したりできます。 新規/変更された画面： • [統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [レルムを追加（Add Realm）] > [Azure AD（Azure AD）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（ Realms）] > [アクション（Actions）]（ユーザーのダウンロード、コピー、編集、削除など） サポートされている ISE バージョン：3.0 パッチ 5 以降、3.1（任意のパッチレベル）、3.2（任意のパッチレベル） 参照：「Create a Microsoft Azure Active Directory Realm」
イベントロギングおよび分析			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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。	7.4.0	いずれか（Any）	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** 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」
ログに記録された暗号化接続での「不明な」SSL アクションに関する詳細。	7.4.0	7.4.0	イベントレポートおよび復号ルールマッチングの有用性が向上しました。 • 暗号化された接続の SSL ハンドシェイクが完了していないかどうかを示す新しい**SSL ステータス**。ログに記録された接続の SSL ハンドシェイクが完了していない場合、接続イベントの [SSL ステータス（SSL Status）] 列に「不明（不完全なハンドシェイク）（Unknown (Incomplete Handshake)）」と表示されます。 • 証明書のサブジェクト代替名（SAN）は、強化された復号ルールマッチングの認証局（CA）名を照合するときに使用されるようになりました。 新規/変更された画面： • [分析（Analysis）] > [接続（Connections）] > [イベント（Events）] > [SSL ステータス（SSL Status）] • [分析（Analysis）] > [接続（Connections）] > [セキュリティ関連イベント（Security-Related Events）] > [SSL ステータス（SSL Status）] 参照：「Connection and Security-Related Connection Event Fields」
ヘルス モニタリング			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
OpenConfig を使用して、テレメトリを外部サーバーにストリーミング。	7.4.0	7.4.0	OpenConfigを使用して、メトリックとヘルスモニタリング情報をThreat Defenseデバイスから外部サーバー（gNMIコレクタ）に送信できるようになりました。TLSにより暗号化された接続を開始するようにThreat Defenseまたはコレクタを設定できます。 新規/変更された画面：**システム**（⚙）>**[ヘルス（Health）]**>**[ポリシー（Policy）]**>**[Firewall Threat Defenseポリシー（Firewall Threat Defense Policies）]**>**[設定（Settings）]**>**[OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）]** 参照：「Send Vendor-Neutral Telemetry Streams Using OpenConfig」
新しいASPドロップメトリック。	7.4.0	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**（⚙）>**[正常性（Health）]**>**[モニター（Monitor）]**>**[デバイス（Device）]** 参照：「show asp drop Command Usage」
管理（Administration）			
詳細な Management Center の監査ログを syslog に送信します。	7.4.0	いずれか	構成データの形式とホストを指定することにより、構成変更を監査ログデータの一部としてsyslogにストリーミングできます。Management Centerは、監査構成ログのバックアップと復元をサポートしています。 新規/変更された画面：**システム**（⚙）>[設定（Configuration）]>[監査ログ（Audit Log）]>[設定変更の送信（Send Configuration Changes）]。 参照：「Stream Audit Logs to Syslog」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
アクセスコントロールポリシーとルールを変更するための詳細なアクセス許可。	7.4.0	いずれか	カスタムユーザーロールを定義して、アクセスコントロールポリシーおよびルールの侵入設定と、その他のアクセスコントロールポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。 ユーザーロールを定義するときに、**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセスコントロールポリシー（Access Control Policy）] > [アクセスコントロールポリシーの変更（Modify Access Control Policy）] > [脅威設定の変更（Modify Threat Configuration）]**オプションを選択して、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの構成、およびポリシーのデフォルトアクションの侵入アクションを選択できるようにします。[残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] を使用して、ポリシーの他のすべての側面を編集する機能を制御できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、引き続きすべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。 参照：「Create Custom User Roles」
国コードの地理位置情報パッケージのみをダウンロードします。	7.4.0	いずれか	IP アドレスを国や大陸にマッピングする地理位置情報データベース（GeoDB）の国コードパッケージのみをダウンロードするようにシステムを設定できるようになりました。追加のロケーションの詳細や接続情報を含むコンテキストデータを含む大規模な IP パッケージは、オプションになりました。デフォルトでは、両方のパッケージがダウンロードされます。 新規/変更された画面：**システム（⚙） > [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）] > [IPパッケージの設定（IP Package Configuration）]** 参照：「」「Update the Geolocation Database」
証明書の失効を確認する際の IPv6 URL のサポート。	7.4.0	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：「Requiring Valid HTTPS Client Certificates」および「Certificate Enrollment Object Revocation Options」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
デフォルトの NTP サーバーが更新されました。	7.4.0	いずれか	新しい Management Center の展開では、デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。Management Center を使用して、独自のデバイスに時刻を提供することを推奨します。**システム**（⚙）>**[設定（Configuration）]**>**[時刻の同期（Time Synchronization）]**で Management Center の NTP サーバーを更新できます。 参照：「Internet Access Requirements」
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	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
ユーザービリティの拡張。	7.4.0	いずれか	次の作業に進んでください。 • **システム**（⚙）> **[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：デバイスクラスタのライセンス • 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 • ネットワークおよびポートオブジェクトを複製します。オブジェクトマネージャ（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**）で、ポートまたはネットワークオブジェクトの横にある新しい [クローン（Clone）] アイコンをクリックします。その後、新しいオブジェクトのプロパティを変更し、新しい名前で保存できます。 参照：ネットワークオブジェクトの作成およびポートオブジェクトの作成 • 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」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
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	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
Snort 3 が無応答になると再起動し、HA フェールオーバーがトリガーされる可能性があります。	7.4.0	7.4.0（Snort 3）	操作の継続性を向上させるために、応答しない Snort が高可用性フェールオーバーをトリガーできるようになりました。これは、プロセスが応答しなくなった場合に Snort 3 が再起動されるようになったために発生します。Snort プロセスを再起動すると、デバイスでのトラフィックフローと検査が一時的に中断され、高可用性展開ではフェールオーバーがトリガーされる可能性があります（スタンドアロン展開では、インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます）。 この機能は、デフォルトでイネーブルにされています。CLI を使用してフェールオーバーを無効にするか、Snort を再起動する条件として時間や無応答スレッド数を設定できます。 新規/変更された CLI コマンド： **configure snort3-watchdog** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Management Center REST API			
Management Center REST API。	7.4.0	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 in Version 7.4」を参照してください。

廃止された機能

表 *4 : Management Center* バージョン *7.4.0* で廃止済みの機能

機能	Management Center では廃止	Threat Defense では廃止	詳細（Details）
廃止：FlexConfig を使用した NetFlow。	7.4.0	いずれか	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」

Device Manager の機能

この表では、Threat Defense バージョン 7.4 で使用可能な新機能と廃止された機能について説明します。

（注） バージョン 7.4 の機能に対する Device Manager のサポートは、バージョン 7.4.1 から始まります。これは、Device Manager をサポートするプラットフォームではバージョン 7.4.0 を使用できないためです。

バージョンごとの Snort 拡張機能の詳細については、Management Center が Device Manager よりも多くの設定可能オプションを提供する可能性があることに注意してくださいManagement Center の新機能リストを参照してください。Snort は、Device Manager または Management Center のどちらを使用しているか関係なく、Threat Defense の主要な検査エンジンです。

表 *5 : Device Manager* バージョン *7.4.1* の新機能と廃止された機能

機能	説明
プラットフォーム機能	
Firepower 1010E のサポートが再開されています。。	バージョン 7.2.3 で導入され、バージョン 7.3 で一時的に廃止された Firepower 1010E のサポートが再開されています。 参照：「Cabling for the Firepower 1010」

機能	説明
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	Cisco Secure Firewall 3130 および 3140 向けに次のネットワークモジュールが導入されました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド
VPN 機能	
Cisco Secure Firewall 3100 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。	**アップグレードの影響。 条件を満たす接続のオフロードが開始されます。** Cisco Secure Firewall 3100 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るようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。この機能はアップグレードにより自動的に有効になります。 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	

機能	説明
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。	**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、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。 7.4 以降にアップグレードし、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。 新規/変更された画面： • **[Devices] > [Interfaces] > [Management]** インターフェイス • （インターフェイスに移動）**[System Settings] > [Management Interface]** • **[Devices] > [Interfaces] > [Merge Interface action needed] > [Management Interface Merge]** 新規/変更されたコマンド： **show management-interface convergence**
Azure と GCP 上の 3 つのインターフェイスを使用して Threat Defense Virtual を展開します。	Azure と GCP で（4 つではなく）3 つのインターフェイスを使用して Threat Defense Virtual を展開できるようになりました。そのためには、診断インターフェイスを削除します。 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 に対するインラインセット。	Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 デバイスでインラインセットを設定できます。[インターフェイス（Interface）] ページに [インラインセット（inline sets）] タブを追加しました。

機能	説明
ライセンシング機能	
ライセンス名の変更およびキャリアライセンスのサポート。	ライセンス名が次のように変更されました。 • Threat は IPS に変更 • Malware は Malware Defense に変更 • Base は Essentials に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更 さらに、キャリアライセンスを適用できるようになりました。これにより、GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定できます。これらの機能を設定するには、FlexConfig を使用します。 参照：「Licensing the System」
管理およびトラブルシューティングの機能	
デフォルトの NTP サーバーが更新されました。	**アップグレードの影響。システムは新しいリソースに接続します。** デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。別の NTP サーバーを使用するには、[デバイス（Device）] を選択し、[システム設定（System Settings）] パネルで [タイムサービス（Time Services）] をクリックします。
HTTPS 管理ユーザーアクセス用の SAML サーバー。	HTTPS 管理アクセスに外部認証を提供するように SAML サーバーを設定できます。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバーを使用する場合は、ログインに共通アクセスカード（CAC）を使用できます。 SAML アイデンティティ ソース オブジェクトの設定を更新し、該当オブジェクトを受け入れるように**[システム設定（System Settings）] > [管理アクセス（Management Access）]** ページを更新しました。

機能	説明
Threat Defense 高可用性ペアの設定の不一致を検出します。	CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。 新規/変更された CLI コマンド：**show failover config-sync error**、**show failover config-sync stats** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Cisco Secure Firewall 3100 でドロップされたパケットをキャプチャします。	MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100 は、これらのドロップされたパケットをキャプチャできるようになりました。 新規/変更された CLI コマンド：**capture** コマンドの [**drop** { **disable** | **mac-filter** }]。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
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。	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 以降への 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。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide

機能	説明
Firepower 1000/2100 および Firepower 4100/9300 のデータプレーン障害後の迅速な回復。	Firepower 1000/2100 または Firepower 4100/9300 のデータプレーンプロセスがクラッシュすると、デバイスを再起動する代わりにプロセスがリロードされます。データプレーンをリロードすると、Snort を含む他のプロセスも再起動します。ブートアップ中にデータプレーンがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードループが回避されます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。 新規/変更された ASA CLI コマンド：**data-plane quick-reload**、**show data-plane quick-reload status** 新規/変更された Threat Defense CLI コマンド：**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 参照：Cisco Secure Firewall Threat Defense コマンドリファレンスおよびCisco Secure Firewall ASA シリーズ コマンド リファレンス

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。

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。