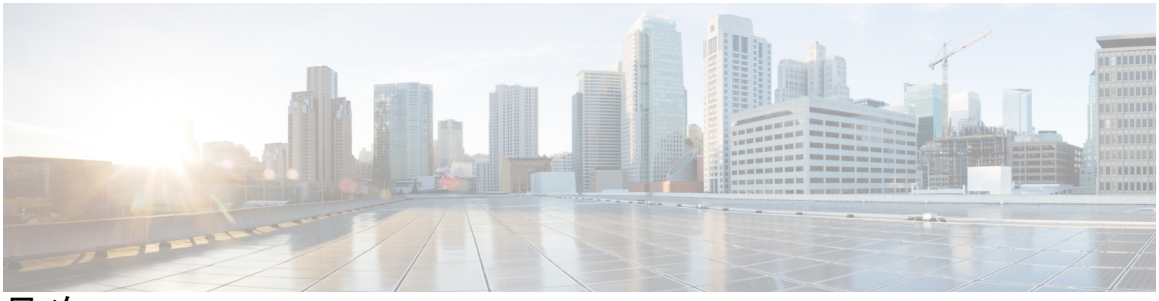
Cisco Secure Firewall ASA から Threat Defense への機能マッピング

初版：2023 年 2 月 21 日

最終更新：2023 年 5 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

このマニュアルについて

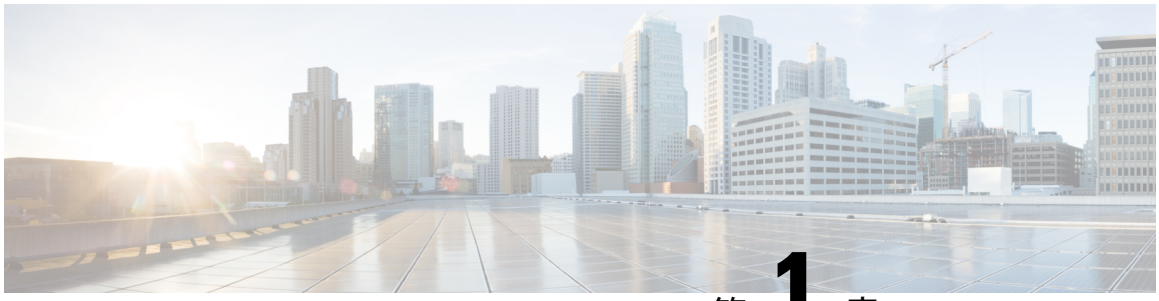
このドキュメントでは、一般的に使用される ASA の機能と同等のThreat Defense の機能をリストしています。（ASA 設定ガイドの章またはセクションに関連する）各 ASA 機能について、Threat Defense の同等の機能を、Secure Firewall Management Center または Cisco Defense Orchestrator（CDO）クラウド提供の Firewall Management Center で機能を設定する場所の UI パスとともに一覧表示します。Management Centerドキュメントのリンクも記載していますので、機能の実装について詳しく読むことができます。各機能について、既知の制限事項または相違点がある場合はそれを記載します。

Management Centerは、複数のデバイスにセキュリティポリシーを適用できるマルチデバイスマネージャです。

Threat Defense には、ASA にはない便利なセキュリティ機能と、ASA の管理方法では利用できないManagement Centerによって提供される管理機能が含まれています。このガイドには、ASA で使用できないThreat Defense 機能は記載されていません。

（注） Management Centerは、FlexConfig と呼ばれる CLI ツールを使用して、いくつかの ASA 機能をサポートします。

このマニュアルについて



第 1 章

一般的な操作機能

使用する前に

表 *1:* 使用する前に

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
構成用の ASA CLI	構成用の制限された Threat Defense CLI、完全な GUI 構成 『Getting Started Guides (console access)』、『Command Reference』、『Device Configuration Guide』を参照してください	Threat Defense CLI には、初期設定のみの限定されたコマンドと、いくつかの特別な操作が含まれています。設定は、デバイス設定の検出が制限されている Management Center で実行する必要があります。
モニタリング用の ASA CLI	モニタリング用の Threat Defense CLI UI パス：システム（⚙） > **[正常性（Health）] > [モニタ（Monitor）]> [高度なトラブルシューティング（Advanced Troubleshooting）] > [Threat Defense CLI]** 『Getting Started Guides (console access)』、『Command Reference』、「Using the Threat Defense CLI from the Web Interface」を参照してください	ASA で使用できるコマンドと同じ **show** コマンドを使用できます。 コンソールで SSH を使用して CLI にアクセスするか、CLI Web ツールを使用できます。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
初期設定	**初期設定** 『Getting Started Guides (console access)』を参照してください	CLI または Device Manager を使用して、ネットワーク設定を設定し、Management Center に登録します。
設定の変更	**設定の展開** UI パス：[展開（Deploy）] 「Configuration Deployment」を参照してください	Management Center から変更を展開する必要があります。
スマートライセンス	**スマート ライセンス** UI パス：**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** 「Licenses」を参照してください 手順：Management Center を Cisco スマートアカウントに登録する	ライセンスは、Management Center によって使用され、割り当てられます。
トランスペアレントファイアウォール モードまたはルーテッド ファイアウォール モード	**トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード** 「トランスペアレントファイアウォールモードまたはルーテッド ファイアウォール モード」を参照してください	ASA と同様に、デバイスを Management Center に登録する前に、CLI を使用してファイアウォールモードを変更する必要があります。

ハイ アベイラビリティとスケーラビリティ

表 *2:* ハイ アベイラビリティとスケーラビリティ

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
マルチ コンテキスト モード	**マルチインスタンスモード**または**仮想ルータ** UI パス： • Firepower 4100/9300 マルチインスタンス：**[論理デバイス（Logical Devices）] > [追加（Add）]**（シャーシ マネージャ） • 仮想ルータ：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [ルーティング（Routing）] > [仮想ルータの管理（Manage Virtual Routers）]** 「Using Multi-Instance Capability on the Firepower 4100/9300」、「Virtual Routers」を参照してください 手順：仮想ルータの作成、仮想ルータへのインターフェイスの割り当て、仮想ルータの NAT の構成、重複するアドレス空間によるインターネットアクセスの提供、ルーティングポリシーの構成	多くの場合、お客様は完全な分離ではなく、個別のルーティングテーブルのみを必要とする場合があります。この場合、仮想ルータを使用できます。 構成を完全に分離するには、サポートされているプラットフォームでマルチインスタンスモードを使用します。この実装はASAマルチコンテキストモードとは異なりますが、機能は似ています。
アクティブ/スタンバイ フェールオーバー	**ハイ アベイラビリティ** UI パス：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [ハイアベイラビリティ（High Availability）]** 「High Availability」を参照してください 手順：ハイアベイラビリティ（HA）ペアを作成する	

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
クラスタリング	クラスタリング UI パス： • Firepower 4100/9300： **[論理デバイス（Logical Devices）] > [追加（Add）]**（シャーシマネージャ） **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [デバイス（Device）]**（Management Center） • パブリッククラウドの Threat Defense Virtual：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [デバイス（Device）]** • Cisco Secure Firewall 3100：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [クラスタ（Cluster）]** • プライベートクラウドの Threat Defense Virtual：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [クラスタ（Cluster）]** 「Deploy a Cluster for Threat Defense on the Secure Firewall 3100」、「Deploy a Cluster for Threat Defense on the Firepower 4100/9300」、「Deploy a Cluster for Threat Defense Virtual in a Public Cloud」、「Deploy a Cluster for Threat Defense Virtual in a Private Cloud」を参照してください 手順：クラスタの作成、既存のクラスタの変更、既存のクラスタへのノードの追加、クラスタからのデータノードの削除、クラスタの解除、クラスタの削除、クラスタリングからのノードの解除、クラスタリングからのデータノードの削除	サイト間クラスタリングおよび分散型サイト間VPNクラスタリングはサポートされていません。

インターフェイス

Threat Defense の場合、インターフェイスはデバイスごとに設定されます。ただし、ほとんどの機能では、インターフェイスをセキュリティゾーンに割り当ててから、ポリシーを直接インターフェイスに適用するのではなく、ゾーンに適用します。ゾーンは、セキュリティポリシー自体と同様に、複数のデバイス間で共有できるオブジェクトとして構成されます。

（注） Threat Defense は、ASA などの通常のファイアウォール インターフェイスをサポートしますが、別のタイプの IPS 専用インターフェイスもサポートします。

表 *3*:インターフェイス

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
[管理インターフェイス（Management Interface）]	[管理インターフェイス（Management Interface）] UI パス：[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [デバイス（Devices）] > [管理（Management）] 「Complete the Threat Defense Initial Configuration」を参照してください	ASA には、独自のルーティングテーブルを持つ管理専用インターフェイスがありますが、ほとんどの場合、データインターフェイスのように動作します。 Threat Defense には、データインターフェイスとは別の管理インターフェイスがあります。これは、管理センターにデバイスをセットアップして登録するために使用されます。また、固有の IP アドレスとスタティック ルーティングを使用します。
物理インターフェイス	物理インターフェイス UI パス：[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [インターフェイス（Interfaces）] 「Interface Overview」を参照してください 手順：インターフェイスの設定	
Firepower 1010 スイッチポート	Firepower 1010 スイッチポート UI パス：[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [インターフェイス（Interfaces）] 「Configure Firepower 1010 Switch Ports」を参照してください	
EtherChannel	EtherChannel UI パス：[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [インターフェイス（Interfaces）] 「Configure EtherChannel Interfaces」を参照してください	

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
ループバック インターフェイス	ループバック インターフェイス UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[インターフェイス（Interfaces）]** 「Configure Loopback Interfaces」を参照してください	
VLAN サブインターフェイス	**VLAN サブインターフェイス** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[インターフェイス（Interfaces）]** 「Configure VLAN Subinterfaces and 802.1Q Trunking」を参照してください	
VXLAN インターフェイス	**VXLAN インターフェイス** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[インターフェイス（Interfaces）]** 「Configure VXLAN Interfaces」を参照してください	
ルーテッドモードおよびトランスペアレントモードのインターフェイス	ルーテッド モードおよびトランスペアレント モードのインターフェイス UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[インターフェイス（Interfaces）]** 「Configure Routed and Transparent Mode Interfaces」を参照してください	
高度なインターフェイス設定	高度なインターフェイス設定 UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[インターフェイス（Interfaces）]** 「Configure Advanced Interface Settings」を参照してください	
トラフィック ゾーン	**ECMP** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[ECMP]** 「ECMP」を参照してください	

基本設定

表 *4*:基本設定

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
DNS サーバー	**DNS サーバー** UI パス： • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DNSサーバーグループ（DNS Server Group）]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [DNS]** 「DNS Server Group」、「Configure DNS」、「FlexConfig Policies」を参照してください	DNS サーバーは、複数のデバイスに適用できるプラットフォーム設定の一部です。 （注） Threat Defense 専用の管理インターフェイスの DNS サーバーは、**configure network dns servers** コマンドおよび **configure network dns searchdomains** コマンドを使用して CLI で構成されます
ISA 3000 ハードウェアバイパス	**ISA 3000 ハードウェアバイパス** UI パス： • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）]** • **[デバイス（Devices）] > [FlexConfig]** 「停電時の自動ハードウェアバイパスの設定方法（ISA 3000）」を参照してください	この機能は、FlexConfig を使用して設定できます。
ISA 3000 Precision Time Protocol	**ISA 3000 Precision Time Protocol** UI パス： • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）]** • **[デバイス（Devices）] > [FlexConfig]** 「How to Configure Precision Time Protocol (ISA 3000)」を参照してください	この機能は、FlexConfig を使用して設定できます。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
ISA 3000 デュアル電源	**ISA 3000 高精度デュアル電源** UI パス： • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）]** • **[デバイス（Devices）] > [FlexConfig]** 「FlexConfig Policies」を参照してください	この機能は、FlexConfig を使用して設定できます。
DHCP サーバ	**DHCP サーバ** UI パス： • IPv4：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [DHCP] > [DHCP サーバー（DHCP Server）]** • IPv6：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [インターフェイス（Interfaces）] > [IPv6] > [DHCP]** 「Configure the DHCPv4 Server」、「Configure the DHCPv6 Stateless Server」を参照してください	
DHCP リレー エージェント	**DHCP リレー エージェント** UI パス：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [DHCP] > [DHCPリレー（DHCP Relay）]** 「Configure the DHCP Relay Agent」を参照してください	
DDNS	**DDNS** UI パス：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [DHCP] > [DDNS]** 「Configure Dynamic DNS」を参照してください	

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
デジタル証明書	**証明書、PKI** UI パス： • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI]** • **[デバイス（Devices）] > [証明書（Certificates）]** 「PKI」、「Certificates」を参照してください 手順： • リモートアクセス（RA）VPN の証明書認証：RA VPN での証明書認証用の証明書マップの作成、接続プロファイルへの証明書マップの関連付け • リモートアクセス VPN 設定用のデバイスでの ID 証明書の作成とインストール：PKCS12 証明書登録オブジェクト、手動証明書登録オブジェクト、自己署名証明書登録オブジェクト、SCEP 証明書登録オブジェクト、手動証明書のインストール、PKCS12、SCEP、または自己署名証明書のインストール、リモートアクセス VPN の設定 • VPN の設定：手動再登録を使用して証明書を更新する、自己署名、SCEP、または EST 登録を使用して証明書を更新する	再利用可能な証明書オブジェクトを作成し、デバイスごとに適用します。
ARP インスペクションと MAC アドレス テーブル	**ARP インスペクションと MAC アドレス テーブル** UI パス： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [インターフェイス（Interfaces）] > [詳細設定（Advanced）] > [ARPおよびMAC（ARP and MAC）]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [ARPインスペクション（ARP Inspection）]** 「Advanced Interface Settings」、「Configure ARP Inspection」を参照してください	ARP インスペクションは、複数のデバイスに適用できるプラットフォーム設定の一部です。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
WCCP	**WCCP** UI パス： • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）]** • **[デバイス（Devices）] > [FlexConfig]** 「FlexConfig Policies」を参照してください	この機能は、FlexConfig を使用して設定できます。

ルーティング

ルーティングはデバイスごとに構成されます。

表 *5:* ルーティング

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
データと管理のルーティングテーブル	データと管理のルーティングテーブル 「Reference for Routing」を参照してください 手順：ルーティングポリシーを設定する	ASA と Threat Defense には、トラフィックのデフォルトが管理ルーティングテーブルとデータルーティングテーブルで異なるデフォルトがあります。 （注） 専用の管理インターフェイスには、CLI で構成できる個別の Linux ルーティングテーブルがあります。
スタティックルートとデフォルトルート	スタティック ルートとデフォルト ルート UI パス：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [ルーティング（Routing）] > [スタティックルート（Static Route）]** 「Static and Default Routes」を参照してください 手順：VTI のスタティックルートを設定する	

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
ポリシーベースルーティング	ポリシーベースルーティング UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** 「Policy Based Routing」を参照してください	
ルート マップ	ルート マップ UI パス：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[ルートマップ（Route Map）]** 「Route Map」を参照してください	
双方向フォワーディング検出ルーティング	双方向フォワーディング検出ルーティング UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[BFD]** 「Bidirectional Forwarding Detection Routing」を参照してください	
BGP	**BGP** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[BGP]** 「BGP」を参照してください 手順：VTI の BGP ルーティングを設定する	
OSPF	**OSPF** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[OSPF]** 「OSPF」を参照してください	
ISIS	**ISIS** UI パス： • **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Object）]** • **[デバイス（Devices）]** > **[FlexConfig]** 「FlexConfig Policies」を参照してください	この機能は、FlexConfig を使用して設定できます。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
EIGRP	**EIGRP** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[EIGRP]** 「EIGRP」を参照してください	
マルチキャスト ルーティング	**マルチキャスト ルーティング** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[マルチキャストルーティング（Multicast Routing）]** 「Multicast」を参照してください	
RIP	**RIP** UI パス：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[ルーティング（Routing）]** > **[RIP]** 「RIP」を参照してください	

AAA サーバー

Threat Defense では、AAA サーバーを VPN アクセスに使用できます。AAA サーバーと管理アクセス用のローカルデータベースについては、システム管理 （13 ページ）を参照してください。

表 *6 : AAA*サーバ

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
VPN の RADIUS	**VPN の RADIUS** UI パス：**[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）]** 「Add a RADIUS Server Group」を参照してください	

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
VPN の LDAP	**VPN の LDAP** UI パス：**[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** 「Create an Active Directory Realm and Realm Directory」を参照してください 手順：リモートアクセス VPN の LDAP 属性マップを構成する	
VPN の SAML シングルサインオン	**VPN の SAML シングルサインオン** UI パス：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAAサーバー（AAA Server）] > [シングルサインオンサーバー（Single Sign-On Server）]** 「Add a Single Sign-on Server」を参照してください 手順：SAML シングル サインオン サーバー オブジェクトを追加する	

システム管理

表 *7:* システム管理

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
デバイス管理用のローカルデータベース	**内部ユーザー（Management Center）** UI パス：**システム（⚙） > [ユーザー（Users）]** 「Add an Internal User」を参照してください **ユーザー（Threat Defense ）** 「Add an Internal User at the CLI」を参照してください	Management Center と Threat Defense は、別々のユーザーデータベースを維持します。Web アクセスおよびCLI アクセス用に Management Center ユーザーを設定できます。 Threat Defense ユーザーを追加するには、CLI を使用する必要があります。Threat Defense ユーザーは SSH アクセスを持っています。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
デバイス管理用の RADIUS	**RADIUS（Management Center）** UI パス：**システム（⚙）> [ユーザー（Users）] > [外部認証（External Authentication）]** 「Add a RADIUS External Authentication Object for Management Center」を参照してください **RADIUS（Threat Defense ）** UI パス： • **システム（⚙）> [ユーザー（Users）] > [外部認証（External Authentication）]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [編集（Edit）] > [外部認証（External Authentication）]** 「Configure External Authentication for SSH」を参照してください	Threat Defense ユーザーの場合、プラットフォーム設定の一部として RADIUS 認証オブジェクトを有効にします。
デバイス管理用の LDAP	**LDAP（Management Center）** UI パス：**システム（⚙）> [ユーザー（Users）] > [外部認証（External Authentication）]** 「Add an LDAP External Authentication Object for Management Center」を参照してください **LDAP（Threat Defense ）** UI パス： • **システム（⚙）> [ユーザー（Users）] > [外部認証（External Authentication）]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [編集（Edit）] > [外部認証（External Authentication）]** 「Configure External Authentication for SSH」を参照してください	Threat Defense ユーザーの場合、プラットフォーム設定の一部として LDAP 認証オブジェクトを有効にします。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
SSH	アクセスリスト（Management Center） UI パス：システム（⚙） > [構成（Configuration）] > [アクセスリスト（Access List）] 「Access List」を参照してください セキュアシェル（Threat Defense ） UI パス：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [セキュアシェル（Secure Shell）] 「Configure Secure Shell」を参照してください	Management Center の場合、SSH はデフォルトで有効になります。システム構成でアクセスを制限できます。 Threat Defense の場合、SSH は、専用の管理インターフェイスに対してデフォルトで有効になっています。**configure ssh-access-list** コマンドを使用してアクセスを制限できます。 データインターフェイスへの SSH については、プラットフォーム設定で有効にします。プラットフォーム設定は、複数のデバイスに適用できます。
HTTPS	アクセス リスト（Access List） UI パス：システム（⚙） > [構成（Configuration）] > [アクセスリスト（Access List）] 「Access List」を参照してください	Management Center への HTTPS アクセスは、システム設定で制御できます。 Management Center によって管理されている場合、Threat Defense は HTTPS アクセスをサポートしません。
ソフトウェアのアップグレード	ソフトウェアのアップグレード UI パス：システム（⚙） > [更新（Updates）] 「Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center」を参照してください 手順：Cisco Secure Firewall Threat Defense のアップグレード	Management Center を使用してすべてのアップグレードを実行します。
ダウングレード	復帰 UI パス：[デバイス（Devices）] > [デバイス管理（Device Management）] > [その他（More）] > [アップグレードを元に戻す（Revert Upgrade）] 「Revert the Upgrade」を参照してください	
バックアップと復元	バックアップと復元 UI パス：システム（⚙） > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] 「Backup and Restore」を参照してください	

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
SSD のホットスワップ（Cisco Secure Firewall 3100）	**SSD のホットスワップ（Cisco Secure Firewall 3100）** 「Hot Swap an SSD on the Secure Firewall 3100」を参照してください	CLI を使用して、ホットスワップを実行します。
デバッグ メッセージ	**デバッグ メッセージ** 「Command Reference」のデバッグコマンドを参照してください	
パケット キャプチャ	**パケット キャプチャ** UI パス：**[デバイス（Devices）] > [パケットキャプチャ（Packet Capture）]** 「Use the Capture Trace」を参照してください 手順：Threat Defense デバイスのパケットキャプチャの収集	
Packet Tracer	**Packet Tracer** UI パス：**[デバイス（Devices）] > [パケットトレーサ（Packet Tracer）]** 「Use the Packet Tracer」を参照してください 手順：パケットトレースを収集して、Threat Defense デバイスのトラブルシューティングを行う	
ping	**ping** UI パス：**システム（⚙） > [正常性（Health）] > [モニタ（Monitor）]> [高度なトラブルシューティング（Advanced Troubleshooting）] > [Threat Defense CLI]** 「Command Reference」の ping コマンドを参照してください	
traceroute	**traceroute** UI パス：**システム（⚙） > [正常性（Health）] > [モニタ（Monitor）]> [高度なトラブルシューティング（Advanced Troubleshooting）] > [Threat Defense CLI]** 「Command Reference」のトレースルートコマンドを参照してください	

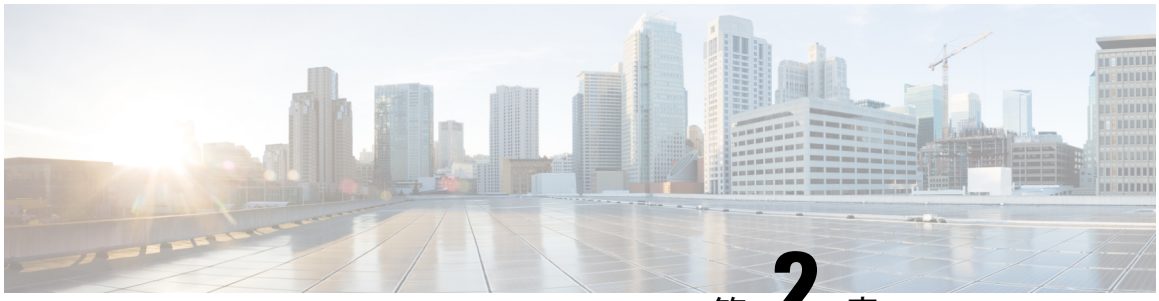
ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
接続の監視	**接続の監視** UI パス：**システム**（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** > **[高度なトラブルシューティング（Advanced Troubleshooting）]** > **[Threat Defense CLI]** 「Command Reference」の show conn コマンドを参照してください	
show asp drop	**ASP ドロップ** UI パス：**システム**（⚙） > **[Health]** > **[Policy]** 「Health Modules」を参照してください	

モニタリング

表 *8*：モニタリング

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
Logging	**Syslog** UI パス： • ASA スタイルの syslogs：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[Syslog]** • ファイルとマルウェア、接続、セキュリティ インテリジェンス、および侵入イベントのアラート：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** > **[編集（Edit）]** > **[ロギング（Logging）]** • アクセスコントロールルール、侵入ルール、およびその他の高度なサービスのアラート：**[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]** 「Configure Syslog」、「About Sending Syslog Messages for Security Events」、「Creating a Syslog Alert Response」を参照してください	Threat Defense は、ASA と同じ syslog 機能をサポートします。ただし、Threat Defense のみがサポートする次世代 IPS サポートによって生成されたログとアラートもサポートします。 Syslog 設定は、複数のデバイスに適用できるプラットフォーム設定の一部です。
SNMP	**SNMP** UI パス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** 「Configure SNMP」を参照してください	SNMP 設定は、複数のデバイスに適用できるプラットフォーム設定の一部です。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
Cisco Success Network	**Cisco Success Network** UI パス：**[統合（Integration）]** > **[SecureX]** > **[Cisco Cloud サポート（Cisco Cloud Support）]** 「Configure Cisco Success Network Enrollment」を参照してください	
ISA 3000 のアラーム	**ISA 3000 のアラーム** UI パス：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Object）]** 「Alarms for the Cisco ISA 3000」を参照してください	この機能は、FlexConfig を使用して設定できます。



第 2 章

ファイアウォール機能

次のトピックでは、Secure Firewall Management Center またはクラウド提供の Firewall Management Center を使用して Secure Firewall Threat Defense で ASA ファイアウォール機能、または同等の機能を設定する方法について説明します。これらの機能は、『*CLI/ASDM Book 2: Cisco Secure Firewall ASA Series Firewall CLI/ASDM Configuration Guide*』ドキュメントに記載されている方法に基づいて大まかに編成されています。

アクセス コントロール

ASA CLI または ADSM を使用して ASA を設定する場合、常に一度に 1 つのデバイスを設定していることになります。

これに対して、Secure Firewall Management Center のアクセス コントロール ポリシーは常に共有ポリシーです。ポリシーを作成したら、1 つ以上のデバイスに割り当てます。

通常、複数のデバイスに対してアクセス コントロール ポリシーを作成します。たとえば、すべてのリモート ロケーション ファイアウォール（リモートサイトをメインの企業ネットワークに接続する）に同じポリシーを割り当てることができます。次に、コアデータセンターにあるファイアウォールに対して別のポリシーを設定することもできます。もちろん、デバイスごとに個別のポリシーを作成することもできますが、それは複数のデバイスマネージャを効率的に使用する方法ではありません。

特定のアクセスコントロールルールがデバイスに適用されるかどうかは、ルールで指定されたインターフェイスによって制御されます。

- インターフェイスを指定しない場合、ルールは、ポリシーが割り当てられているすべてのデバイスに適用されます。
- 特定のデバイスインターフェイスのリストであるオブジェクトであるセキュリティゾーンを指定した場合、ルールは、指定されたゾーンにインターフェイスを持つデバイスにのみ適用され、展開されます。セキュリティゾーンには、インターフェイス名だけでなく、

「デバイス上のインターフェイス」のペアも含まれます。たとえば、「inside on device1」は、「inside on device2」を含まないゾーンにある可能性があります。

次の表に、ASA の主なアクセスコントロール機能と、それらの機能または同等の機能を Secure Firewall Threat Defense デバイス上で設定する場所を示します。

表 *9*:アクセスコントロール機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
アクセスコントロールの**オブジェクト**	**オブジェクト** UI パス：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**。 「Object Management」を参照してください。 手順：動的オブジェクトを設定する	アクセス コントロール ポリシーを編集するときに、ネットワークおよびポート（サービス）オブジェクトを作成することもできます。 また、セキュリティグループタグと時間範囲もサポートされています。ネットワークサービスとローカルユーザーグループはサポートされていません（または必要ありません）。 アクセスコントロールルールで使用できる追加オブジェクト：アプリケーションフィルタ、地理位置情報、インターフェイス セキュリティ ゾーン、URL、およびVLANタグ。これらのオブジェクトは、ASA で使用できない機能に適用されます。
非アクセス コントロール グループ/ルールの**アクセスコントロールリスト（ACL）**。	**アクセス コントロール リスト（ACL）** UI パス：標準および拡張 ACL：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**。 Ethertype ACL：**[デバイス（Devices）]** > **[FlexConfig]**。 「Object Management」および「FlexConfig Policies」を参照してください。 手順： • リモートアクセス（RA）VPN接続のトラフィックフィルタリングの設定：RA VPN 接続のトラフィックをフィルタリングするための拡張アクセスリストの作成、RA VPN 接続のトラフィックをフィルタリングするためのグループポリシーへの拡張アクセスリストの追加	標準または拡張 ACL のオブジェクトを作成し、ルーティングまたは ACL を必要とするその他の機能を設定するときにそれらのオブジェクトを使用します。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
アクセスコントロールルール：基本（ネットワーク、ポート、プロトコル、ICMP）。	**アクセス コントロール ルール** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」を参照してください。 手順： • デバイスのセットアップ：アクセスコントロールルールの追加 — 機能のウォークスルー、アクセス コントロール ポリシーの作成 • VTI トンネルの設定：VTI 経由の暗号化されたトラフィックを許可するアクセスコントロールルールの設定 • 新しいアクセス コントロール ポリシー UI：機能のウォークスルー – 新しい AC ポリシー UI へのアクセス、新しい AC ポリシー UI – ルールテーブル、新しい AC ポリシー UI – ルールの作成、新しい AC ポリシー UI – ルールの編集	アクセス コントロール ポリシーは、基本的な 5 タプルおよび VLAN アクセスコントロールルールをサポートします。さらに、地理位置情報オブジェクトを使用して、特定の地理的位置に関連付けられた IP アドレスをターゲットにすることができます。 プレフィルタポリシーを使用して、トンネルトラフィック（GRE など）やその他の 5 タプルトラフィックを制御することもできます。プレフィルタルールはアクセスコントロールルールの前に処理され、ASA では使用できません。**[ポリシー（Policies）]**>**[プレフィルタ（Prefilter）]**を参照してください。
アクセスコントロールルール：ユーザーベースの制御	**アクセス コントロール ルール** UI パス：ユーザー名とグループのマッピングを取得するためのルールを設定するには、**[ポリシー（Policies）]**>**[アイデンティティ（Identity）]**に移動します。 その後、アクセスコントロールルールでユーザー名とグループを選択できます。**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」および「User Identity Policies」を参照してください。 手順：動的オブジェクトのアクセス コントロール ポリシー ルールを設定する	ASA と比較して、ユーザー/グループ メンバーシップを取得するためのオプションは数多くあります。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
アクセスコントロールルール：セキュリティグループと Trustsec	**アクセス コントロール ルール** UI パス：Identity Services Engine を設定するには、**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[アイデンティティソース（Identity Sources）]**に移動します。 その後、アクセスコントロールルールでセキュリティグループタグを選択できます。**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」および「User Control with ISE/ISE-PIC」を参照してください。	Identity Services Engine を使用して、ユーザーベースの制御のためにユーザー名/ユーザーグループ情報を収集することもできます。
（ASA では使用できません。）アクセスコントロールルール：レイヤ 7 アプリケーション制御。	**アクセス コントロール ルール** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」を参照してください。	たとえば、同じプロトコルとポートを使用するアプリケーションのアクセスコントロールルールを記述して、さまざまなタイプの HTTP/HTTPS トラフィックを区別することができます。アプリケーションフィルタリングは、ASA で使用できるものよりも詳細な制御を適用するのに役立ちます。
アクセスコントロールルール：URL フィルタリング。	**アクセス コントロール ルール** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「URL Filtering」を参照してください。	URL カテゴリとレピュテーションに基づいてアクセスを制御するには、URL フィルタリングライセンスが必要です。 アクセス コントロール ポリシー内で定義されたセキュリティインテリジェンス ポリシーを使用して、URL またはネットワークオブジェクトに基づいて早期フィルタリングを行うこともできます。DNS ポリシーは、DNS ルックアップ要求に対して同じことを行うことができます。
デバイスへのトラフィックの **ICMP アクセスルール**（**icmp permit/deny** および **ipv6 icmp permit/deny** コマンド）。	**ICMP アクセスルール** UI パス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**、[ICMPアクセス（ICMP Access）] ページ。. 「Platform Settings」を参照してください。	アクセス コントロール ポリシーと同様に、プラットフォーム設定ポリシーは共有され、複数のデバイスにポリシーを適用できます。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
Cisco Umbrella	**Cisco Umbrella** UI パス：**[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）]** **[ポリシー（Policies）] > [DNS]** **[デバイス（Devices）] > [VPN：サイト間（VPN: Site-to-Site）] > [SASE トポロジ（SASE Topology）]**。 「DNS Policies」および「Site-to-Site VPNs for Secure Firewall Threat Defense」を参照してください。	Cisco Umbrella DNS ポリシーと Cisco Umbrella SASE VPN トポロジを作成できます。

ネットワーク アドレス変換

アクセス コントロール ポリシーと同様に、ネットワークアドレス変換（NAT）ポリシーも共有されます。NAT ポリシーを作成してから、それを 1 つ以上のデバイスに割り当てます。FlexConfig ポリシーも共有されます。

特定の NAT ルールがデバイスに展開されるかどうかは、ルールをインターフェイスによって制限するか、すべてのインターフェイスにルールを適用するかによって異なります。

- インターフェイスを指定しない場合、ルールは、ポリシーが割り当てられているすべてのデバイスに適用されます。
- インターフェイス オブジェクトを指定すると、ルールは、指定されたオブジェクトにインターフェイスを持つデバイスにのみ適用され、展開されます。

次の表に、ASA の主なネットワークアドレス変換機能と、それらの機能または同等の機能を Secure Firewall Threat Defense デバイス上で設定する場所を示します。

表 *10*：ネットワークアドレス変換機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
ネットワークアドレス変換（**NAT**）：動的 NAT/PAT、静的 NAT、アイデンティティ NAT。	**ネットワーク アドレス変換（NAT）** UI パス：**[デバイス（Devices）]** > **[NAT]**。 「Network Address Translation (NAT)」を参照してください。 手順： • デバイスのセットアップ：NAT ポリシーの作成 — 機能のウォークスルー • 仮想ルーティングの設定：重複するアドレス空間によるインターネットアクセスの提供、仮想ルータの NAT の設定	オブジェクトと Twice NAT の両方を設定できます。ただし、それらは Secure Firewall Threat Defense では自動 NAT および手動 NAT と呼ばれます。
ポートブロック割り当てによるポートアドレス変換（**PAT**）。	**ポートブロック割り当てによるポートアドレス変換（PAT）。** UI パス：グローバル PAT ポートブロック割り当て設定（**xlate block-allocation** コマンド）を構成するには、**[デバイス（Devices）]** > **[FlexConfig]**を使用します。 次に、**[デバイス（Devices）]** > **[NAT]**を使用して PAT ルールを設定できます 「Network Address Translation (NAT)」および「FlexConfig Policies」を参照してください。	この機能は、キャリアグレードまたは大規模な PAT に使用されます。
Per-Session PAT または **Multi-Session PAT**（**xlate per-session** コマンド）。	**Per-Session PAT または Multi-Session PAT** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	Secure Firewall Threat Defense デフォルト設定には、ASA と同じ事前定義されたセッションごとのルールが含まれています。デフォルト以外の動作が必要な場合にのみ、構成が必要です。
アドレスとポートのマッピング（**MAP**）	**アドレスとポートのマッピング（MAP）** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	アドレスとポートのマッピング（MAP）は、IPv4 アドレスを IPv6 に変換するためのキャリアグレードの機能です。

アプリケーション インスペクション

Snort は Secure Firewall Threat Defense デバイスの主要検査エンジンです。ただし、ASA 検査は引き続き実行され、Snort 検査の前に適用されます。

Snort は多くの HTTP 検査を実行するため、ASA HTTP 検査エンジンはまったくサポートされておらず、設定できません。

多くの ASA 検査エンジンは、デフォルト設定によりデフォルトで有効になっています。ASA 検査エンジンが追加設定をサポートしている場合は、FlexConfig（共有ポリシー）を使用して設定を構成する必要があります。複数のデバイスに同じ設定を使用する場合、検査設定用に単一の FlexConfig ポリシーを作成し、該当するすべてのデバイスに適用できます。

単に検査をオフ（またはオン）にする必要がある場合は、FlexConfig の代わりに、各デバイスのデバイス CLI で **configure inspection** コマンドを使用できます。ただし、すべての可能なプロトコル検査がコマンドで使用できるわけではありません。

次の表に、さまざまな ASA 検査エンジンをリストし、Secure Firewall Threat Defense デバイスでデフォルトで有効になっているものを特定します。

表 *11*：アプリケーション インスペクション機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
基本インターネットプロトコルの**検査**	**(Inspection)]** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	サポートされている検査は次のとおりです。太字は、デフォルト設定で検査が有効になっていることを示します。 • DCERPC • **DNS** • **FTP** • **ICMP** • **ICMP エラー** • ILS • **IP オプション** • IPsec Pass Through • IPv6 • Lisp • **NetBIOS** • PPTP • **RSH** • SMTP/ESMTP • **SNMP** • **SQL*Net** • **Sun RPC** • **TFTP** • WAAS • XDMCP • VXLAN サポートされていません（Snort によって実行されます）：HTTP、IM（インスタントメッセージング）。

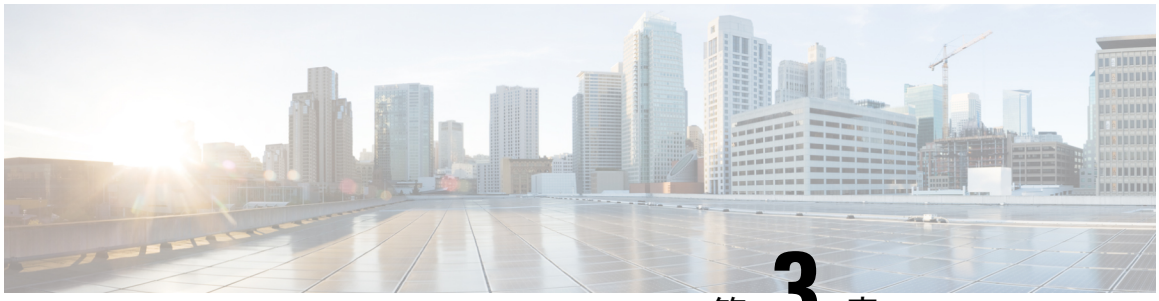
ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
音声とビデオのプロトコルの検査	**(Inspection)]** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	サポートされている検査は次のとおりです。太字は、デフォルト設定で検査が有効になっていることを示します。 • CTIQBE • **H.323 H.225** • **H.323 RAS** • MGCP • **rtsp** • **SIP モード（SIP** • **Skinny** • STUN
モバイルネットワークの検査	**(Inspection)]** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	サポートされている検査は次のとおりです。これらの検査には、Carrier ライセンスが必要です。いずれもデフォルトでは有効になっていません。 • Diameter • GTP/GPRS • M3UA • SCTP • RADIUS アカウンティング（この検査には Carrier ライセンスは必要ありません）

サービスポリシー、接続設定、脅威検出

次の表に、デバイスを通過する接続のいくつかの側面を制御する、大まかに関連する機能をいくつか示します。これらの設定のほとんどには、ほとんどの場合に機能するデフォルトがあります。

表 *12*：サービス ポリシー、接続設定、脅威検出機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
グローバル タイムアウト	**グローバル タイムアウト** UI パス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**、[タイムアウト（Timeouts）] ページ。 「Platform Settings」を参照してください。	プラットフォーム設定は共有ポリシーです。これらの設定は、ポリシーが割り当てられた各デバイスに適用されます。
接続設定の**サービスポリシー**	**Threat Defense サービス ポリシー** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択してから、ポリシーの編集中に [詳細設定（Advanced Settings）] で [脅威防御サービスポリシー（Threat Defense Service Policy）] を見つけます。 「Service Policies」を参照してください。	これらの設定には、TCP ステートバイパス、TCP シーケンスランダム化、TCP インターセプト、デッド接続検出（DCD）、TCP 正規化、およびトラフィッククラスごとの一般的な接続制限とタイムアウトが含まれます。 脅威防御サービスポリシーは、アクセス コントロール ポリシーの一部として定義されます。これは、1 つ以上のデバイスに割り当てる共有ポリシーです。 特定のインターフェイスに制限するルールは、そのインターフェイスを含むデバイスでのみ構成されます。グローバルルールは、アクセス コントロール ポリシーに割り当てられたすべてのデバイスに適用されます。
Quality of Service（QoS）	**Quality of Service（QoS）** UI パス：**[デバイス（Devices）]** > **[QoS]**。 「Quality of Service」を参照してください。	QoS ポリシーは共有されますが、ポリシーの各ルールは 1 つ以上のインターフェイスを指定する必要があります。ルールにデバイス上のインターフェイスが含まれている場合にのみ、ルールはデバイスに構成されます。
脅威検出（threat-detection コマンド）。	**脅威の検出** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択してから、ポリシーの編集中に [詳細設定（Advanced Settings）] で [脅威検出（Threat Detection）] を見つけます。 「Threat Detection」を参照してください。	Secure Firewall Threat Defense 機能は、ASA 機能と完全に重複するものではありませんが、新しい機能が含まれています。FlexConfig を使用して、ASA コマンドバージョンを展開することもできます。



第 3 章

仮想プライベートネットワーク機能

この章では、Secure Firewall Management Center を使用して Secure Firewall Threat Defense で ASA 仮想プライベートネットワーク機能を設定するための高レベルの情報を提供します。

サイト間 VPN

表 *13* : サイト間 *VPN*

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
LAN-to-LAN IPsec	**ポリシーベース VPN** UI パス：[デバイス（Devices）]>[サイト間（Site To Site）] > [ポリシーベース（暗号マップ）（Policy Based (Crypto Map)）]。 「Configure a Policy-based Site-to-Site VPN」を参照してください。 手順：ポリシーベースのサイト間 VPN の設定、既存のサイト間 VPN 展開の IKE オプションのカスタマイズ、既存のサイト間VPN展開のIPsecオプションのカスタマイズ、既存のサイト間 VPN 展開の詳細設定のカスタマイズ	Management Center は、ピアで VPN を設定するための単一のウィザードを提供します。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
仮想トンネルインターフェイス（VTI）	**ルートベース VPN** UI パス：[デバイス（Devices）] > [サイト間（Site To Site）] > [ルートベース（VTI）（Route Based (VTI)）]。 「Create a Route-based Site-to-Site VPN」を参照してください。 手順：ルートベース VPN（VTI）の作成、VTI の静的ルートの設定、VTI の BGP ルーティングの設定、VTI 経由の暗号化トラフィックを許可するアクセスコントロールルールの設定	動的 VTI を持つハブと静的 VTI を持つスポークの間に VPN を作成することは、ウィザードを使用して Management Center で作成するよりずっと簡単です。 ASDM にはウィザードがありません。
Umbrella SASE	**Umbrella に SASE トンネルを展開する** UI パス：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [+SASE トポロジ（+SASE Topology）]。 「Umbrella に SASE トンネルを展開する」を参照してください。	
サイト間 VPN のモニタリング	**サイト間 VPN のモニタリング** UI パス：[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site to Site VPN）]。 「サイト間 VPN のモニタリング」を参照してください。	

リモート アクセス VPN

表 *14*：リモート アクセス *VPN*

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
リモートアクセス IPsec（IKE v2）VPN	**リモートアクセス VPN ポリシー** UI パス：[デバイス（Devices）] > [VPN] > [リモートアクセス（Devices）] > [ポリシーの割り当て（Policy Assignment）] > [VPNプロトコル（VPN Protocols）] > [IPsec-IKEv2]。 「Configuring a Remote Access VPN Connection」を参照してください。 手順： • リモートアクセス（RA）VPN 接続のトラフィックフィルタリングの設定：RA VPN 接続のトラフィックをフィルタリングするための拡張アクセスリストの作成、RA VPN接続のトラフィックをフィルタリングするためのグループポリシーへの拡張アクセスリストの追加 • リモートアクセス（RA）VPN の証明書認証：RA VPN での証明書認証用の証明書マップの作成、接続プロファイルへの証明書マップの関連付け • リモートアクセス VPN 設定用のデバイスでの ID 証明書の作成とインストール：PKCS12 証明書登録オブジェクト、手動証明書登録オブジェクト、自己署名証明書登録オブジェクト、SCEP 証明書登録オブジェクト、手動証明書のインストール、PKCS12、SCEP、または自己署名証明書のインストール、リモートアクセス VPN の設定 • VPN の設定：手動再登録を使用した証明書の更新、自己署名、SCEP、または EST 登録を使用した証明書の更新、リモートアクセス VPN の LDAP 属性マップの設定、SAML シングル サインオン サーバー オブジェクトの追加、リモートアクセス VPN の動的アクセスポリシーの設定	接続プロファイルとグループ ポリシー オブジェクトの設定は、Management Center でも ASA と同じままです。 ローカルユーザーと Active Directory/LDAP を作成するためのレルムオブジェクトを作成する必要があります。レルムとは、Management Center とサーバー上にあるユーザーアカウントの間の接続です。
リモートアクセス SSL VPN		

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
	リモートアクセス VPN ポリシー UI パス：[デバイス（Devices）] > [VPN] > [リモートアクセス（Devices）] > [ポリシーの割り当て（Policy Assignment）] > [VPNプロトコル（VPN Protocols）] > [SSL]。 「Configuring a Remote Access VPN Connection」を参照してください。 手順：リモートアクセス VPN を設定します。	
VPN ロード バランシング	**VPN ロード バランシング** UI パス：リモートアクセス VPN ポリシーを編集します。 [詳細設定（Advanced）] > [ロードバランシング（Load Balancing）] 「Configuring VPN Load Balancing」を参照してください。	VPN ロードバランシングは、VPN ロードバランシンググループ内のデバイス間でリモートアクセス VPN トラフィックを均一に分散するメカニズムです。
ダイナミック アクセス ポリシー	**ダイナミック アクセス ポリシー** UI パス：[デバイス（Devices）] > [ダイナミックアクセスポリシー（Dynamic Access Policy）]。 「Dynamic Access Policies」を参照してください。 手順：リモートアクセス VPN のダイナミック アクセス ポリシーを設定します。	VPN 環境のダイナミクスに対応する許可を構成できます。
VPN の監視	**リモートアクセス VPN ダッシュボード** UI パス：[概要（Overview）] > [ダッシュボード（Dashboards）] > [リモートアクセスVPN（Remote Access VPN）] 「Remote Access VPN Monitoring」を参照してください。	
セキュアクライアント Hostscan	**VPN ファイルオブジェクト** UI パス：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [セキュアクライアントファイル（Secure Client File）]。 「File Objects」を参照してください。	
セキュアクライアント カスタム属性	**セキュアクライアント カスタム属性オブジェクト** UI パス：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [カスタム属性（Custom Attribute）]。 Secure Client カスタム属性オブジェクト	

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。