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。

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。