Cisco Secure Firewall Threat Defense 強化ガイド、バージョン 10.0

改訂：2026 年 3 月 9 日

はじめに

Cisco Secure Firewall Threat Defense はネットワークの資産や通信をサイバー脅威から守りますが、ご自身でも展開の設定を行う必要があります。これにより、強化されたサイバー攻撃に対する脆弱性がさらに軽減されます。このガイドでは、Firewall Threat Defense の強化について対処します。展開内の他のコンポーネントの強化については、次のドキュメントを参照してください。

- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

このドキュメントは、Firewall Threat Defense を設定する 3 つの方法について言及していますが、詳細な手順を示すものではありません。

- Firewall Management Center Web インターフェイスを使用して、一部の Firewall Threat Defense の構成を設定できます。詳細については、*Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド* [英語]を参照してください。
- Firewall Threat Defense の一部の設定は、Firewall Threat Defense のコマンドライン インターフェイス（CLI）を使用して設定できます。このドキュメントで言及しているすべての CLI コマンドの詳細については、『*Cisco Firepower Threat Defense Command Reference*』を参照してください。
- Firewall Threat Defense 構成の設定は、Cisco Secure Firewall Device Manager を使用して構成できます。詳細については、『*Cisco Secure Firewall Device Manager コンフィギュレーション ガイド*』を参照してください。

このドキュメントで説明しているすべての設定が、Firewall Threat Defense のすべてのバージョンで使用できるわけではありません。設定情報の詳細については、https://cisco.com/go/ftd-docs を参照してください。

セキュリティ認定準拠

お客様の組織が、米国国防総省や他の政府/自治体認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。該当する認定当局による認定を受けた後、認定に固有のガイダンス文書に従って設定を行うことで、Firewall Threat Defense は次の認定基準に準拠するようになります。

- コモンクライテリア（CC）：国際コモンクライテリア承認アレンジメントによって確立された、セキュリティ製品の要件を定義するグローバル標準規格
- Department of Defense Information Network Approved Products List（DoDIN APL）：米国国防情報システム局（DISA）によって制定された、セキュリティ要件を満たす製品のリスト

（注） 米国政府は、Unified Capabilities Approved Products List（UCAPL）の名称を DoDIN APL に変更しました。このドキュメントおよび Firewall Management Center Web インターフェイスでの UCAPL の参照は、DoDIN APL への参照として解釈できます。

- 連邦情報処理標準（FIPS）140：暗号化モジュールの要件に関する規定

認定ガイダンス文書は、製品認定が完了すると個別に入手できます。この強化ガイドの公開によってこれらの製品認定の完了が保証されるわけではありません。

このドキュメントで説明している設定は、認定機関が定める現在のすべての要件を厳密に遵守することを保証するものではありません。必要な強化手順の詳細については、認定機関から提供される本製品に関するガイドラインを参照してください。

このドキュメントでは、Firewall Threat Defense のセキュリティを強化するためのガイダンスを説明していますが、Firewall Threat Defense の一部の機能については、ここで説明している設定を行っても認定準拠がサポートされません。詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「セキュリティ認定準拠の推奨事項」を参照してください。シスコは、この強化ガイドと『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の内容が、認定固有のガイダンスと矛盾を起こさないように努めました。シスコのドキュメントと認定ガイダンスとの間で不一致がある場合は、認定ガイダンスを使用するか、システムの所有者にお問い合わせください。

シスコのセキュリティ アドバイザリおよびレスポンスの確認

Cisco Product Security Incident Response Team（PSIRT）では、シスコ製品のセキュリティ関連の問題についての PSIRT アドバイザリを投稿しています。比較的重大度の低い問題については、シスコではセキュリティ レスポンスも投稿しています。セキュリティアドバイザリおよびレスポンスは、「Cisco Security Advisories and Alerts」および「Cisco Security Vulnerability Policy」で確認できます。

セキュアなネットワークを維持するため、シスコのセキュリティ アドバイザリおよびレスポンスを常にご確認ください。これらのアドバイザリは、脆弱性がネットワークにもたらす脅威を評価するうえで必要な情報を提供します。この評価プロセスのサポートについては、「セキュリティ脆弱性アナウンスメントに対するリスクのトリアージ」を参照してください。

システムの最新状態の維持

シスコでは、問題に対処して改善を行うために、ソフトウェア アップデートを定期的にリリースしています。システム ソフトウェアを最新の状態に保つことは、強化されたシステムを維持するうえで不可欠です。システムソフトウェアが適切にアップデートされていることを確認してください。詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「更新」の章、および『*Cisco Secure Firewall Management Center Upgrade Guide*』を参照してください。

また、シスコでは、ネットワークと資産を保護するために使用するデータベースのアップデートも定期的に発行しています。最適な保護を実現するため、管理対象 Firewall Management Center の地理位置情報データベース、侵入ルールデータベース、および脆弱性データベースを最新の状態に維持してください。デプロイメントのいずれかのコンポーネントを更新する前に、更新プログラムに付属の『*Cisco Secure Firewall Threat Defense リリースノート*』を必ずお読みください。これらは、互換性、前提条件、新機能、動作の変更、警告など、重要かつリリースに固有の情報を提供します。アップデートによってはサイズが大きくなり、完了までに時間がかかる場合があります。システムパフォーマンスへの影響を軽減するため、これらのアップデートはネットワークの使用量が少ない時間帯に行ってください。

位置情報データベース

地理位置情報データベース（GeoDB）には、国や都市の座標などの地理データが含まれています。Management Center が、検出された IP アドレスと一致する GeoDB 情報を検出した場合、その IP アドレスに関連付けられている地理位置情報を表示できます。

Management Center Web インターフェイスから GeoDB を更新するには、[システム（System）]（⚙）>**[コンテンツの更新（Content Updates）]** > **[地理位置情報の更新（Geolocation Updates）]** を使用します。次の操作を実行できます。

- インターネットにアクセスせずに Management Center で GeoDB を更新します。
- インターネットにアクセスし、Management Center で GeoDB を更新します。
- インターネットにアクセスし、Management Center で GeoDB の定期的な自動更新をスケジュールします。

詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「地理位置情報データベース（GeoDB）の更新」を参照してください。

侵入ルール

新たな脆弱性が明らかになると、Cisco Talos Security Intelligence and Research Group（Talos）から侵入ルールの更新がリリースされます。これらの更新を Firewall Management Center にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装できます。それらの更新は、侵入ルール、プリプロセッサ ルール、およびルールを使用するポリシーに影響を及ぼします。

Management Center Web インターフェイスでは、侵入ルールを更新する 3 つのアプローチが用意されており、すべて [システム（System）]（⚙） **[Content Updates** > **Rule Updates]** で使用できます。

- インターネットにアクセスできない Firewall Management Center の侵入ルールを更新します。
- インターネットにアクセスできる Firewall Management Center の侵入ルールを更新します。
- インターネットにアクセスできる Firewall Management Center の侵入ルールの定期的な自動更新をスケジュールします。

詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「侵入ルールの更新」を参照してください。

また、[システム（System）]（⚙） **[Content Updates** > **Rule Updates]** を使用してローカル侵入ルールをインポートすることもできます。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル侵入ルールを作成することができます。これらを Firewall Management Center にインポートする前に、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「ローカル侵入ルールのインポートに関するガイドライン」を参照して、ローカル侵入ルールのインポートプロセスが組織のセキュリティポリシーに準拠するようにしてください。

脆弱性データベース

脆弱性データベース（VDB）は、ホストが影響を受ける可能性がある既知の脆弱性、およびオペレーティングシステム、クライアント、アプリケーションのフィンガープリントを格納するデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

Firewall Management Center Web インターフェイスでは、VDB を更新するための 2 つのアプローチが提供されています。

- VDB（[システム（System）]（⚙） > **[コンテンツの更新（Content Updates）]** > **[VDBの更新（VDB Updates）]**）を手動で更新します。
- VDB の更新（[システム（System）]（⚙） >**[ツール（Tools）]**>**[スケジューリング（Scheduling）]**）をスケジュールします。

詳細については、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「脆弱性データベース（VDB）の更新」を参照してください。

セキュリティ インテリジェンスのリストとフィード

セキュリティ インテリジェンスのリストとフィードは、リストまたはフィードのエントリに一致するトラフィックをすばやくフィルタリングするために使用できる IP アドレス、ドメイン名、および URL のコレクションです。

システム提供のフィードと、事前定義されたリストがあります。カスタムフィードとリストを使用することもできます。これらのリストとフィードを表示するには、**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence ）]** を選択します。システム提供のフィードの一部として、シスコはセキュリティ インテリジェンス オブジェクトとして次のフィードを提供しています。

- セキュリティ インテリジェンス フィードは、Talos の最新の脅威インテリジェンスで定期的に更新されます。
  - Cisco-DNS-and-URL-Intelligence-Feed（[DNS Lists and Feeds] の下）
  - Cisco-Intelligence-Feed（IPアドレス用、[Network Lists and Feeds] の下）

  システムが提供するフィードは削除できませんが、更新頻度を変更（または無効に設定）できます。Firewall Management Center は、5 分または 15 分ごとに Cisco-Intelligence-Feed データを更新できるようになりました。
- Cisco-TID-Feed（[Network Lists and Feeds] の下）

  TID 監視可能データのコレクションであるこのフィードを使用するには、Threat Intelligence Director を有効にして設定する必要があります。

詳細については、『*Cisco Secure Firewall Management Center* デバイス設定ガイド』の「カスタム セキュリティ インテリジェンスのリストとフィード」を参照してください。

CC または UCAPL モードの有効化

1 つの設定で複数の強化設定変更を適用するには、Firewall Threat Defense の CC または UCAPL モードを選択します。この設定は、Firewall Management Center Web インターフェイスの Firewall Threat Defense プラットフォーム設定ポリシー（**[Devices > Platform Settings]**）で適用します。変更は、新しい設定を展開するまでは Firewall Threat Defense で有効になりません。詳細については、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「セキュリティ認定コンプライアンスの有効化」を参照してください。

これらの設定オプションの 1 つを選択すると、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「セキュリティ認定準拠の特性」に記載されている変更が有効になります。展開内のアプライアンスはすべて、同じセキュリティ証明書コンプライアンスモードで動作する必要があることに注意してください。

注意 この設定を有効にした後は、無効にすることはできません。CC または UCAPL モードを有効にする前に、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「セキュリティ認定準拠」で詳細を確認してください。この設定を元に戻す必要が生じた場合は、Cisco TAC にご連絡ください。

（注） セキュリティ認定準拠を有効にしても、選択したセキュリティ モードのすべての要件への厳密な準拠が保証されるわけではありません。このドキュメントでは、CC または UCAPL モードで提供されるものを超えて展開を強化するために推奨されるその他の設定について説明します。完全準拠に必要な強化手順の詳細については、認定機関から提供される本製品に関するガイドラインを参照してください。

NetFlow によるトラフィックの可視性の向上

シスコの IOS NetFlow を使用すると、ネットワーク内の通信フローをリアルタイムでモニターできます。Firewall Threat Defense は、ランタイムカウンタの表示およびリセットなど、一部の NetFlow 機能と連携できます。**show flow-export counters** および **clear flow-export counters** CLI コマンドを参照してください。

Firewall Management Center Web インターフェイスを使用して、NetFlow によってキャプチャされるものと同じ冗長な Firewall Threat Defense syslog メッセージを無効にすることができます。これを行うには、[**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、メニューから [**Syslog**] を選択します。[Syslogの設定（Syslog Settings）] タブで、[NetFlowと同等のSyslog（NetFlow Equivalent Syslogs）] チェックボックスをオンにします（どの syslog メッセージが冗長であるかを判別するには、**show logging flow-export-syslogs** CLI コマンドを使用します）。

NetFlow を使用してネットワーク デバイスを設定する場合は、これらの機能を利用できます。フロー情報がリモート コレクタにエクスポートされるかどうかに関係なく、必要に応じて NetFlow を受動的に使用できます。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「NetFlow データ」を参照してください。

ローカル ネットワーク インフラストラクチャの保護

Cisco Secure Firewall のデプロイメントでは、さまざまな目的で他のネットワークリソースとやり取りする場合があります。そうした他のサービスを強化することで、Cisco Secure Firewall システムだけでなくすべてのネットワーク資産を保護できます。対処する必要があるすべてのものを特定するには、ネットワークとそのコンポーネント、資産、ファイアウォール設定、ポート設定、データ フロー、およびブリッジング ポイントを図式化することを試みてください。

セキュリティ上の問題を考慮した、ネットワークの運用セキュリティ プロセスを確立し、遵守します。

ネットワーク タイム プロトコル サーバーの保護

Firewall Management Center とその管理対象デバイスのシステム時刻を同期させることが不可欠です。セキュアで信頼された Network Time Protocol（NTP）サーバーを使用して、 Firewall Management Center とその管理対象デバイスのシステム時刻を同期させることを強く推奨します。

Firewall Management Center Web インターフェイスから Firewall Threat Defense デバイスの NTP 時刻同期を設定するには、[**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、ポリシーページ内の [**Time Synchronization**] タブを選択します。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「時刻同期の設定」を参照してください。

MD5、SHA-1、または AES-128 CMAC 対称キー認証を使用して、NTP サーバーとの通信を保護することをお勧めします。

⚠

注意 Firewall Management Center と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。適切な同期を確保するため、Firewall Management Center とそのすべての管理対象デバイスについて、同じ NTP サーバーを使用するように設定してください。

ドメイン ネーム システム（DNS）の保護

ネットワーク環境で相互に通信しているコンピュータは、DNS プロトコルを利用して、IP アドレスとホスト名の間のマッピングを提供します。ドメインネームシステム（DNS）の管理インターフェイスを介した通信をサポートするためにローカル ドメインネームシステム（DNS）と接続するよう Firewall Threat Defense デバイスを設定することは、初期設定プロセスの一部となっており、ご使用のモデルのクイックスタートガイドで説明しています。

データ インターフェイスまたは診断インターフェイスを使用する特定の Firewall Threat Defense 機能も DNS を使用します。たとえば、NTP、アクセス コントロール ポリシー、Firewall Threat Defense/ping/traceroute により提供される VPN サービスなどがあります。データインターフェイスまたは診断インターフェイス用に DNS を設定するには、[**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、左ペインから [**DNS**] を選択します。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「DNS の設定」を参照してください。

DNS は、セキュリティを考慮して設定されていない DNS サーバーの弱点を利用するようにカスタマイズされた、特定のタイプの攻撃の影響を受ける可能性があります。業界で推奨されているセキュリティのベストプラクティスに従って、ローカル DNS サーバーを設定してください。シスコでは、ドキュメント『DNS Best Practices, Network Protections, and Attack Identification』でガイドラインを提供しています。

セキュアな SNMP ポーリングおよびトラップ

『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「SNMP の構成」で説明しているように、SNMP ポーリングおよびトラップをサポートするように Firewall Threat Defense を設定できます。SNMP ポーリングを使用する場合は、SNMP 管理情報ベース（MIB）に、連絡先情報、管理情報、位置情報、サービス情報、IP アドレッシングおよびルーティング情報、伝送プロトコルの使用統計情報など、環境の攻撃に利用される可能性のあるシステムの詳細情報が含まれていることに注意する必要があります。SNMP に基づく脅威からシステムを保護するための設定オプションを選択します。

Firewall Threat Defense の SNMP 機能を設定するには、[**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、左ペインから [**SNMP**] を選択します。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「SNMP の構成」を参照してください。

Firewall Threat Defense デバイスへの SNMP アクセスを強化するには、次のオプションを使用します。

- SNMP ユーザーの作成時に SNMPv3 を選択します。これにより、AES128 と読み取り専用ユーザーによる暗号化のみがサポートされます。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「SNMP ホストの追加」を参照してください。
- SNMP ユーザーを作成する際、以下をサポートする SNMPv3 を選択します。
  - SHA、SHA224、SHA256、SHA384 などの認証アルゴリズム。
  - AES256、AES192、および AES128 による暗号化。

- 読み取り専用ユーザー。

- 次のオプションを使用して SNMPv3 ユーザを作成します。
  - [セキュリティレベル（Security Level）]として [特権（Priv）] を選択します。
  - [暗号化パスワードタイプ（Encryption Password Type）] として [暗号化 (Encrypted）] を選択します。

詳細な手順については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「SNMPv3 ユーザーの追加」を参照してください。

重要 Firewall Management Center から SNMP サーバーへのセキュアな接続を確立することはできますが、認証モジュールは FIPS に準拠していません。

セキュアなネットワーク アドレス変換（NAT）

通常、ネットワーク接続されたコンピュータは、ネットワーク通信内の送信元 IP アドレスや宛先 IP アドレスを再割り当てするために NAT を使用します。展開を保護し、NAT に基づく悪用からネットワーク インフラストラクチャ全体を保護するため、業界のベストプラクティスや NAT プロバイダーからの推奨事項に従って、ネットワーク内の NAT サービスを設定します。

NAT 環境で動作するようにデプロイメントを設定する方法については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「NAT 環境」を参照してください。この情報は、環境を確立する際に次の 2 つの段階で使用します。

- お使いのハードウェア モデルの『Cisco Firepower Management Center Getting Started Guide』の説明に従って、Firewall Management Center の初期設定を実行する場合。
- 『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「Add a Device to the Firewall Management Center Using a Device Template」の記述に従って、Firewall Management Center に管理対象デバイスを登録する場合。

展開内のアプライアンスの保護

展開には、Firewall Threat Defense と、Firewall Management Center によって管理されるセキュリティデバイスが含まれており、それぞれが異なるアクセス手段を提供します。管理対象デバイスは Firewall Management Center との間で情報を交換しますが、デバイスのセキュリティは環境全体のセキュリティにとって重要です。環境内にあるアプライアンスを分析して、ユーザー アクセスの保護や不要な通信ポートのクローズなど、必要に応じて強化の設定を適用してください。

ネットワーク プロトコル設定の強化

Firewall Threat Defense デバイスは、いくつかのプロトコルを使用して他のネットワーク デバイスとやり取りできます。Firewall Threat Defense デバイスや FTD が送受信するデータを保護するために、ネットワーク通信の設定を選択してください。

- デフォルトでは、Firewall Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。定期的にパケットをフラグメント化するアプリケーション（NFS over UDP など）がある場合は、ネットワーク上でフラグメントを許可する必要がある場合があります。ただし、フラグメント化されたパケットはサービス妨害（DoS）攻撃に利用されることが多いため、フラグメントを許可しないことを推奨します。
  - Firewall Threat Defense デバイスのフラグメント設定を構成するには、[**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、左ペインから [**Fragment Settings**] を選択します。
  - Firewall Threat Defense デバイスによって処理されるネットワーク通信内のフラグメントを禁止するには、[**Chain (Packet)**] オプションを 1 に設定します。

  詳細な手順については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「フラグメント設定」を参照してください。
- Firewall Management Center によって管理されている Firewall Threat Defense デバイスでは、Firewall Threat Defense との HTTPS 接続は、トラブルシューティングの目的でパケット キャプチャ ファイルをダウンロードする場合にのみ使用できます。

  パケットキャプチャのダウンロードを許可する必要がある IP アドレスに対してのみ HTTPS アクセスを許可するように Firewall Threat Defense を設定します。Firewall Management Center Web インターフェイスの [**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、目次から [**HTTP Access**] を選択します。『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「HTTP アクセス」を参照してください。
- デフォルトでは、Firewall Threat Defense は IPv4 か IPv6 を使用して任意のインターフェイスで ICMP パケットを受信できます。ただし、2 つの例外があります。
  - Firewall Threat Defense は、ブロードキャストアドレス宛ての ICMP エコー要求に応答しません。
  - Firewall Threat Defense は、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、Firewall Threat Defense インターフェイス経由で離れたインターフェイスに送信できません。

  ICMP に基づく攻撃から Firewall Threat Defense デバイスを保護するために、ICMP ルールを使用して、選択したホスト、ネットワーク、または ICMP タイプに ICMP アクセスを限定できます。Firewall Management Center Web インターフェイスの [**Devices > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、目次から [**ICMP Access**] を選択します。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「ICMP アクセス」を参照してください。
- Firewall Threat Defense を、DHCP および DDNS サービスを提供するように設定できます（『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「DHCP サービスと DDNS サービスについて」を参照してください）。これらのプロトコルはその性質上、攻撃に対して脆弱です。Firewall Threat Defense で DHCP または DDNS を設定する場合は、セキュリティに関する業界のベストプラクティスを適用し、ネットワーク資産を物理的に保護する機能を用意し、Firewall Threat Defense デバイスへのユーザーアクセスを強化することが重要です。
- Firepower 1000 シリーズ、2100 シリーズ、および Secure Firewall 3100 で、LLDP を有効にすることができます。この機能により、Firewall Threat Defense は LLDP 対応ピアとパケットを交換できます。デフォルトでは、LLDP 送受信はポートで無効になっています。LLDP を介して送信される情報は、攻撃に対して脆弱です。Firewall Threat Defense デバイスで LLDP を設定する場合は、セキュリティに関する業界のベストプラクティスを適用し、Firewall Threat Defense へのユーザーアクセスを強化することが重要です。セキュリティを強化するために、ファイアウォー

ルがピアからLLDPパケットを受信できるようにすることをお勧めします。このアクションにより、ファイアウォールは、その識別情報を他のピアデバイスに公開することなく、ピアデバイスに関する情報を取得できるようになります。詳細については、『*Cisco Secure Firewall Management Center* デバイス設定ガイド』の「物理インターフェイスの有効化およびイーサネット設定の構成」を参照してください。

セキュア VPN サービス

Firewall Threat Defense は、リモートアクセス仮想プライベートネットワーク（RA VPN）とサイト間仮想プライベートネットワークの2種類の仮想プライベートネットワーク（VPN）サービスを提供するように設定できます。デバイスのライセンスによっては、サイト間 および RA VPN 送信に強力な暗号化を適用できる場合があります。強力な暗号化を備えた VPN には特別なライセンスが必要です。『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「輸出規制対象の機能のライセンス」を参照してください。

リモートアクセス仮想プライベートネットワーク

RA VPN接続を介してリモートクライアント間で送受信されるメッセージの送信を保護する場合、Firewall Threat Defense は Transport Layer Security（TLS）または IPsec IKEv2 を使用できます。

Firewall Threat Defense に RA VPN 設定を展開する前に、Firewall Management Center はライセンスの前提条件が満たされていることを確認します。詳細については、*Cisco Secure Firewall Management Center* デバイス コンフィギュレーション ガイド [英語]を参照してください。

Firewall Threat Defense の RA VPN は、認証用の AD、LDAP、SAML ID プロバイダー、および RADIUS AAA サーバーをサポートします。ユーザーが RA VPN の AAA 設定を指定する場合、セキュリティを強化するために、次の認証方法のいずれかを使用することを推奨します。

- [クライアント証明書とSAML（Client Certificate and SAML）]：各ユーザーはクライアント証明書と SAML サーバーの両方を使用して認証されます。
- [クライアント証明書とAAA（Client Certificate and AAA）]：各ユーザーはクライアント証明書とAAAサーバーの両方を使用して認証されます。

RA VPN は、ローカル認証と複数証明書認証をサポートしています。

- [ローカル認証（Local Authentication）]：この認証方式は、プライマリまたはセカンダリ認証方式として、または設定されたリモートサーバーに到達できない場合のフォールバックとして使用できます。ローカル認証には、強力なパスワードを使用することをお勧めします。詳細については、『*Cisco Secure Firewall Management Center* デバイス設定ガイド』の「ローカルレルムとリモートアクセス VPN ポリシーの関連付け」を参照してください。
- [複数証明書認証（Multi-certificate Authentication）]：この認証方式を使用して、単一の証明書認証を使用したマシンまたはデバイスの証明書を検証できます。この認証により、デバイスが企業支給のデバイスであることを確認し、ユーザーID証明書を認証してVPNアクセスを許可します。この認証方式を使用することをお勧めします。詳細については、『*Cisco Secure Firewall Management Center* デバイス設定ガイド』の「複数証明書認証の設定」を参照してください。

サイト間仮想プライベートネットワーク

サイト間 VPN 接続を介してリモートネットワーク間で送受信されるメッセージの送信を保護する場合、Firewall Threat Defense は IPsec IKEv1 または IPsec IKEv2 を使用できます。

サイト間 VPN には、ポリシーベース（暗号マップ）とルートベース（仮想トンネルインターフェイス（VTI））の 2 種類があります。セキュリティを強化するために、ルートベースの VTI VPN を使用することを推奨します。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「サイト間 VPN」を参照してください。

Firewall Threat Defense VPN IKE および IPsec オプションを設定する場合は（**[Devices > VPN > Site To Site > Add]** をクリックし、[**IKE**] または [**IPsec**] タブをクリック）、次の点を推奨します。

- IKEv2 を選択してください。
- 事前共有手動キーには強力なキーを使用してください。
- デフォルトの IKEv2 ポリシーを使用してください。たとえば、AES-GCM-NULL-SHA-LATEST などのポリシーです。
- [セキュリティアソシエーション（SA）の強度適用の有効化（Enable Security Association (SA) Strength Enforcement）] チェックボックスをオンにしてください。

  このオプションを有効にすると、子 IPsec SA で使用される暗号化アルゴリズムが、親 IKE SA よりも強くなることはありません。
- [Perfect Forward Secrecyの有効化（Enable Perfect Forward Secrecy）] オプションをオンにします。

  このオプションは、暗号化された交換ごとに一意のセッションキーを生成して使用します。この一意のセッションキーにより、交換は、後続の復号化から保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] ドロップダウンリストから、PFS セッションキーの生成時に使用する Diffie-Hellman キー導出アルゴリズムを選択します。

上記の Firewall Threat Defense VPN IKE オプションの詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』を参照してください。

これらのサービスを設定するには、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「VPN の概要」を参照してください。

Firewall Management Center は、幅広い暗号化アルゴリズムとハッシュアルゴリズムをサポートしており、Diffie-Hellman グループを選択できます。強固な暗号化はシステムのパフォーマンスを低下させる可能性があるため、効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出す必要があります。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「VPN 接続の安全性を確保する方法」を参照してください。

Firewall Threat Defense ユーザー アクセスの強化

Firewall Threat Defense は次の 2 種類のユーザーをサポートしています。

- 内部ユーザー：デバイスは、ローカル データベースでユーザー認証を確認します。
- 外部ユーザー：ユーザーがローカル データベースに存在しない場合、システムは外部 LDAP または RADIUS の認証サーバに問い合わせます。

ユーザー管理をネットワーク環境の既存のインフラストラクチャと統合したり、二要素認証などの機能を活用したりする目的で、LDAP や RADIUS などの外部認証メカニズムを使用したユーザー アクセスの確立を検討する場合があります。外部認証を確立するには、Firewall Management Center Web インターフェイス内で外部認証オブジェクトを作成する必要があります。外部認証オブジェクトを共有して、Firewall Management Center だけでなく Firewall Threat Defense でも外部ユーザーを認証できます。

外部認証を使用するには、展開用にドメインネームシステム（DNS）を設定する必要があることに注意してください。DNS の強化に関する推奨事項に必ず従ってください。ドメイン ネーム システム（DNS）の保護 （8 ページ）を参照してください

Firewall Management Center によって管理される Firewall Threat Defense は、単一のユーザーアクセス手段としてコマンドラインインターフェイスを提供します。物理デバイスの場合は、SSH、シリアル、またはキーボードとモニターの接続を使用してコマンド ライン インターフェイスにアクセスできます。特定の設定を適切に行うことで、これらのユーザーは Linux シェルにもアクセスできます。

設定権限の制限

デフォルトでは、Firewall Threat Defense はすべての Firewall Threat Defense CLI コマンドに対して完全な管理者権限を持つ、単一の **admin** ユーザーを提供します。このユーザーは、追加のアカウントを作成でき、 **configure user access** CLI コマンドを使用して、次の 2 つのレベルのアクセス権限のいずれかを付与できます。

- Basic：ユーザーは、システム構成に影響を与えない Firewall Threat Defense CLI コマンドを使用できます。
- Config：ユーザーは、重要なシステム構成機能を提供するコマンドを含めて、すべての Firewall Threat Defense CLI コマンドを使用できます。

アカウントに Config アクセス権を割り当てる場合や、Config アクセス権を持つアカウントへのアクセス権を付与するユーザーを選択する場合は、慎重に検討してください。

Linux シェルへのアクセスの制限

Firewall Management Center によって管理される Firewall Threat Defense は、自身の管理インターフェイスを介して、SSH、シリアル、またはキーボードとモニタの接続を使用した CLI アクセスのみをサポートします。このアクセスは「admin」アカウント、内部ユーザーが使用でき、外部ユーザーにも使用を許可できます。

config レベルのアクセス権を持つユーザーは、CLI で **expert** コマンドを使用して Linux シェルにアクセスできます。

⚠

注意 すべてのデバイスで、CLI の Config レベルのアクセス権または Linux シェルへのアクセス権を持つアカウントは、Linux シェルの sudoer 権限を取得できます。このため、セキュリティ上のリスクが生じる可能性があります。システムのセキュリティを強化するには、次のことを推奨します。

- Firewall Threat Defense 上の外部認証されたアカウントへのアクセス権をユーザーに付与すると、Firewall Threat Defense 上の外部認証されたすべてのアカウントが CLI Config レベルのアクセス権を持つことに注意してください。
- 新しいアカウントを Linux シェルに直接追加しないでください。Firewall Threat Defense で、**configure user add** CLI コマンドのみを使用して新しいアカウントを作成してください。
- Firewall Threat Defense の CLI コマンド **configure ssh-access-list** を使用して、Firewall Threat Defense が自身の管理インターフェイス上で SSH 接続を受け入れる IP アドレスを制限してください。

管理者はまた、**system lockdown-sensor** CLI コマンドを使用して Linux シェルへのすべてのアクセスをブロックするように Firewall Threat Defense を設定することもできます。システムのロックダウンが完了すると、Firewall Threat Defense にログインしているユーザーはすべて、Firewall Threat Defense の CLI コマンドにのみアクセスできます。これは大きな強化措置となる可能性がありますが、Cisco TAC からのホットフィックスがないと元に戻すことができないため、使用にあたっては慎重に検討してください。

内部ユーザー アカウントの強化

個々の内部ユーザーを設定する場合、Config アクセス権を持つユーザーは **configure user** Firewall Threat Defense CLI コマンドを使用することで、Web インターフェイスのログイン メカニズムを利用した攻撃に対してシステムの保護を強化できます。以下の設定を使用できます。

- ユーザーがロックアウトされるまでに許可されるログイン失敗の最大回数を制限します。
- パスワードの最小長さを適用します（**configure user minpasswdlen**）。
- パスワードの有効日数を設定します（**configure user aging**）。
- 強力なパスワードを必須にします（**configure user strengthcheck**）。
- ユーザーが必要とするアクセスのタイプにのみ適したユーザー アクセス権限を割り当てます（**configure user access**）。
- 次回のログイン時にユーザーにアカウント パスワードのリセットを強制します（**configure user forcereset**）。

展開でマルチテナンシーを使用している場合は、デバイスへのユーザーアクセスを許可するときに、Firewall Threat Defense が属するドメインについて考慮してください。

詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「ドメイン管理の履歴」を参照してください。

外部ユーザ アカウントの強化

Firewall Threat Defense のユーザ認証に外部サーバを使用する場合は、外部ユーザが常に Config 権限を持っていることに注意してください。他のユーザ ロールはサポートされていません。[**Devices] > [Platform Settings**] > [Add/Edit Policy] > [**External Authentication**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、Firewall Management Center Web インターフェイスから Firewall Threat Defense ユーザーの外部認証を設定します。外部ユーザ アカウントを設定するには、外部認証オブジェクトを使用して LDAP または RADIUS サーバとの接続を確立する必要があります。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「SSH および SSH アクセスリストの設定」を参照してください。

重要 LDAP または RADIUS サーバーとのセキュアな接続は Firewall Management Center からセットアップできますが、認証モジュールは FIPS に準拠していません。

- すべての Firewall Threat Defense 外部ユーザは Config アクセス権を持ち、**system lockdown-sensor** コマンドを使用して Linux シェルへのアクセスをブロックしない限り、これらのユーザは Linux シェルにアクセスできることに注意してください。Linux シェルユーザは root 権限を取得できます。このため、セキュリティ上のリスクが生じます。
- 外部認証に LDAP を使用する場合は、[拡張オプション（Advanced Options）] で TLS または SSL 暗号化を設定します。

セッション タイムアウトの確立

Firewall Management Center への接続時間を制限すると、権限のないユーザーが無人セッションをエクスプロイトする機会が減少します。

Firewall Management Center デバイスでセッションタイムアウトを設定するには、[**Device > Platform Settings**] > [Add/Edit Policy] > [**Timeouts**] で Firewall Management Center プラットフォーム設定ポリシーを作成します。詳細な手順については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「タイムアウト」を参照してください。

Firewall Threat Defense REST API の考慮事項

Firewall Threat Defense の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準 HTTP メソッドを使用してアプライアンス設定を表示および管理するための軽量のインターフェイスを提供します。API については『*Cisco Secure Firewall Threat Defense REST API Guide*』で説明しています。

重要 TLS を使用して Firewall Threat Defense と REST API クライアント間でセキュアな接続を確立できますが、認証モジュールは FIPS に準拠していません。

すべての RADIUS 応答における Message-Authenticator 属性の強制

すべての RADIUS 応答で Message-Authenticator 属性を要求できるようになりました。これにより、Threat Defense VPN ゲートウェイで、リモートアクセス VPN 用でもデバイス自体へのアクセス用でも、RADIUS サーバーからのすべての

応答を安全に検証できるようになります。新しい RADIUS サーバーでは、[RADIUSサーバー対応メッセージオーセンティケータ（RADIUS Server-Enabled Message Authenticator）] オプションがデフォルトで有効になっています。既存のサーバーでも有効にすることを推奨します。無効にすると、ファイアウォールが攻撃にさらされる可能性があります。

このパラメータは、RADIUS 認証オブジェクトを設定する場合に使用できます（[**Administration > Users > External Authentication > Add External Authentication Object > RADIUS**] を選択します）。

バックアップの保護

システム データとその可用性を保護するため、Firewall Threat Defense の定期的なバックアップを実行してください。バックアップ機能は、Firewall Management Center Web インターフェイスの [**System > Tools > Backup/Restore**] に表示されます。その説明については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「バックアップ/復元」を参照してください。保存されている Firewall Threat Defense の設定を復元するには、Firewall Threat Defense CLI **restore** コマンドを使用します。

Firewall Management Center は、リモート デバイスにバックアップを自動的に保存する機能を備えています。強化システムでこの機能を使用することはお勧めできません。Firewall Management Center とリモート ストレージ デバイス間の接続を保護できないためです。

Firewall Threat Defense デバイスのアップグレードを元に戻す

アップグレード後 30 日以内に Threat Defense が攻撃に対して脆弱であることがわかった場合は、アップグレード中に復元スナップショットを保存してあれば復元できます（推奨）。Firewall Threat Defense を復元すると、ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレードの直前の状態に戻ります。パッチ適用後に復元すると、パッチも必然的に削除されます。

復元される設定と復元されない設定、高可用性（HA）デバイスおよびクラスター化デバイスを復元するためのガイドライン、追加の要件などの復元の詳細については、Firewall Management Center で現在実行され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。

データのエクスポートの保護

Firewall Threat Defense CLI は、特定のファイルを Firewall Threat Defense からローカル コンピュータにダウンロードする機能を備えています。この機能は、システムのトラブルシューティング時に Cisco TAC に提供する情報を収集できるように提供されているものであり、必要な場合以外は使用しないでください。Firewall Threat Defense からダウンロードするファイルを保護するための予防措置を講じてください。ダウンロード時は使用可能なオプションから最も安全なものを選択し、データの保存場所となるローカル コンピュータを保護してください。また、TAC にファイルを送信する際は使用可能なプロトコルから最も安全なものを使用してください。特に、次のコマンドを使用する場合に起こりうるリスクに注意してください。

- **show asp inspect-dp snort queue-exhaustion** [**snapshot** *snapshot_id*] [**export** *location*]

  export オプションでは TFTP のみサポートされています。

- **file copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  このコマンドは、セキュリティで保護されていない FTP を使用してリモート ホストにファイルを転送します。

- **copy [/noverify] /noconfirm** {**/pcap capture:**/[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

  src_url および *dest_url* の次のオプションは、コピーされたデータを保護する方法を提供します。

  - 内部フラッシュ メモリ
  - システム メモリ
  - オプションの外部フラッシュ ドライブ
  - パスワードで保護された HTTPS
  - パスワードで保護された SCP（SCP サーバーでターゲット インターフェイスを指定）
  - パスワードで保護された FTP
  - パスワードで保護された TFTP（TFTP サーバーでターゲット インターフェイスを指定）

  強化システムでは、*src_url* および *dest_url* で次のオプションを使用しないことをお勧めします。

  - SMB UNIX サーバーのローカル ファイル システム
  - クラスタ トレース ファイル システム（セキュリティ認定準拠が有効になっているシステムではクラスタはサポートされません）

- **cpu profile dump** *dest_url*

  dest_url の次のオプションは、データ ダンプをセキュリティで保護する方法を提供します。

  - 内部フラッシュ メモリ
  - オプションの外部フラッシュ ドライブ
  - パスワードで保護された HTTPS
  - SMB UNIX サーバーのローカル ファイル システム
  - パスワードで保護された SCP（SCP サーバーでターゲット インターフェイスを指定）
  - パスワードで保護された FTP
  - パスワードで保護された TFTP（TFTP サーバーでターゲット インターフェイスを指定）

  強化システムでは、*src_url* および *dest_url* のオプションでクラスタ ファイル システムを使用しないことをお勧めします。

- **file secure-copy** *host_name user_id path filename_1* [*filename_2 ... filename_n*]

  SCP を使用してリモート ホストにファイルをコピーします。

Secure Syslog

Firewall Threat Defense は、syslog メッセージを外部の syslog サーバに送信できます。syslog 機能を設定する場合は、セキュアなオプションを選択します。

1. [**Devices > Platform Settings**]で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、左ペインから [**Syslog**] を選択します。[**Syslog Servers**] タブで syslog サーバーを追加するときに、TCP プロトコルを選択し、[**Enable secure syslog**] チェックボックスをオンにします。これらのオプションは、デバイス設定の別の場所で上書きしなければ、Firewall Threat Defense によって生成される syslog メッセージに適用されます。

（注） デフォルトでは、セキュアな syslog が有効になっていると、TCP を使用する syslog サーバーがダウンした場合に Firewall Threat Defense はトラフィックを転送しません。この動作を無効化するには、[**Allow user traffic to pass when TCP syslog server is down**] チェックボックスをオンにします。

これら 2 つの設定を適用すると、Firewall Threat Defense の syslog は次のように動作します。

- プラットフォーム設定ポリシーの syslog 設定は、デバイスとシステムのヘルスに関連する syslog メッセージ、およびネットワーク設定に関連する syslog メッセージに適用されます。
- 『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「syslog にセキュリティイベントデータを送信するためのシステムの設定について」に記載されているいずれかの場所でアクセス コントロール ポリシーの設定をオーバーライドしない限り、プラットフォーム設定の syslog 設定は、接続およびセキュリティ インテリジェンス イベントの syslog に適用されます。これらのオーバーライドではセキュアな syslog オプションは提供されないため、セキュアな環境での使用はお勧めできません。
- 『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「セキュリティ イベントの syslog の設定場所」に記載されているいずれかの場所でアクセス コントロール ポリシーの設定をオーバーライドしない限り、プラットフォーム設定ポリシーの syslog 設定は、侵入イベントの syslog に適用されます。これらのオーバーライドではセキュアな syslog オプションは提供されないため、セキュアな環境での使用はお勧めできません。

ログイン バナーのカスタマイズ

ユーザが CLI にログインするときにユーザに必要な情報を伝えるように、Firewall Threat Defense デバイスを設定できます。セキュリティの観点から、ログイン バナーでは不正アクセスを防止する必要があります。次の例のようなテキストを考慮してください。

> 安全なデバイスにログインしました。このデバイスにアクセスする権限を持っていない場合は、すぐにログアウトしないと犯罪と認識されるおそれがあります。

Firewall Threat Defense デバイスのログインバナーを設定するには、[**Device > Platform Settings**] で Firewall Threat Defense プラットフォーム設定ポリシーを作成し、左ペインから [**Banner**] を選択します。詳細な手順については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「バナー」を参照してください。

ネットワーク ユーザーの権限のあるログイン、認識、および制御をサポートするサーバーへのセキュアな接続

ID ポリシーは、アイデンティティソースを使用してネットワークユーザーを認証し、ユーザーを認識し、制御する目的でユーザーデータを収集します。ユーザ アイデンティティ ソースを確立するには、 Firewall Management Center または管理対象デバイスと、次のいずれかのタイプのサーバとの間の接続が必要です。

- Microsoft Azure AD
- Microsoft Active Directory
- Linux OpenLDAP
- RADIUS

重要 LDAP、Microsoft AD、または RADIUS サーバーへのセキュアな接続を Firewall Threat Defense から設定できますが、認証モジュールは FIPS に準拠していません。

（注） 外部認証に LDAP または Microsoft AD を使用する場合は、「外部ユーザ アカウントの強化 （15 ページ）」の情報を確認してください。

（注） Firewall Threat Defense は、これらの各サーバーを使用して、ユーザーアイデンティティ機能の候補のさまざまな組み合わせをサポートします。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「ユーザー アイデンティティ ソースについて」を参照してください。

Active Directory サーバーおよび LDAP サーバーとの接続の保護

「レルム」と呼ばれるオブジェクトは、Active Directory（AD）または LDAP サーバー上のドメインに関連付けられている接続設定を記述するものです。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「レルム」を参照してください。

（Firewall Management Center Web インターフェイスの [**Integration > Other Integration > Realms**] で）レルムを作成する場合は、AD サーバーまたは LDAP サーバーとの接続を保護するため、次の点に注意してください。

Active Directory サーバーに関連付けられるレルムの場合：

- [AD 参加パスワード（AD Join Password）] と [ディレクトリ パスワード（Directory Password）] で強力なパスワードを選択します。
- Active Directory レルムにディレクトリを追加する際に次のようにします。
  - [暗号化（Encryption）] モードとして [STARTTLS] または [LDAPS] を選択します（[なし（None）] は選択しないでください）。

- Active Directory ドメイン コントローラへの認証に使用する [SSL 証明書（SSL Certificate）] を指定します。世界的に知られていて信頼できる認証局が生成した証明書を使用することをお勧めします。

LDAP サーバーに関連付けられるレルムの場合：

- [ディレクトリ パスワード（Directory Password）] で強力なパスワードを選択します。
- LDAP レルムにディレクトリを追加する際に次のようにします。
  - [暗号化（Encryption）] モードとして [STARTTLS] または [LDAPS] を選択します（[なし（None）] は選択しないでください）。
  - LDAP サーバーへの認証に使用する [SSL 証明書（SSL Certificate）] を指定します。世界的に知られていて信頼できる認証局が生成した証明書を使用することをお勧めします。

RADIUS サーバーとの接続の保護

RADIUS サーバーとの接続を設定するには、Firewall Management Center Web インターフェイスの [**Objects > Object Management > AAA Server > RADIUS Server Group**] で RADIUS サーバー グループ オブジェクトを作成し、そのグループに RADIUS サーバーを追加します。RADIUS サーバとの接続を保護するには、[新しい RADIUS サーバ（New RADIUS Server）] ダイアログで次のオプションを選択します。

- 管理対象デバイスと RADIUS サーバー間でデータを暗号化するための [**Key**] と [**Confirm Key**] を指定します。
- セキュアなデータ送信をサポートできる接続用のインターフェイスを指定します。

（注） Firewall Threat Defense は、リモートアクセス VPN（ユーザー アイデンティティソースとして使用される）を提供するように展開内の管理対象 Firewall Threat Defense デバイスが設定されている場合にのみ、ユーザーアイデンティティのために RADIUS サーバーと接続します。リモートアクセス VPN の構成については、ネットワークプロトコル設定の強化 （9 ページ） を参照してください。

セキュアな証明書登録

Enrollment over Secure Transport（EST）を使用した証明書登録の設定

安全なチャネルを介した Firewall Threat Defense の証明書の登録を設定できます。Enrollment over Secure Transport（EST）は、CA から ID 証明書を取得するためにデバイスによって使用されます。EST は、セキュアなメッセージ転送に TLS を使用します。

EST の設定方法：

1. **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [証明書登録（Certificate Enrollment）]**を選択します。
2. [**Add Cert Enrollment**] をクリックし、[**CA Information**] タブをクリックします。

3. [登録タイプ（Enrollment Type）] ドロップダウンリストから、[EST] を選択します。

Firewall Threat Defense によって EST サーバー証明書を検証しない場合は、[**Ignore EST Server Certificate Validations**] チェックボックスをオンにしないことを推奨します。デフォルトでは、Firewall Threat Defense は EST サーバー証明書を検証します。EST 登録タイプは、RSA キーと ECDSA キーのみをサポートし、EdDSA キーをサポートしません。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「証明書の登録オブジェクト EST オプション」を参照してください。

Firewall Management Center と Firewall Threat Defense では、RSA キーサイズが 2,048 ビット未満の証明書と、SHA-1 を使用するキーは登録できません。これらの制限をオーバーライドするには、[**Enable Weak-Crypto**] オプション（**[デバイス（Devices）] > [証明書（Certificates）]**）を使用します。デフォルトでは、Weak-Crypto オプションは無効になっています。weak-crypto キーを有効にすることは推奨しません。weak-crypto キーは、キーサイズが大きいキーほど安全ではないためです。weak-crypto を有効にすると、ピア証明書の検証などが可能になります。ただし、この設定は証明書の登録には適用されません。

証明書の検証の設定

特定の CA 証明書を使用して SSL や IPSec クライアントを検証したり、CA 証明書を使用して SSL サーバーからの接続を検証したりできます。検証使用法の種類を設定する方法：

1. **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [証明書登録（Certificate Enrollment）]**を選択します。
2. [**Add Cert Enrollment**] をクリックし、[**CA Information**] タブをクリックします。
3. [検証用法（Validation Usage）]：VPN 接続中に証明書を検証するオプションから選択します。
   - [IPsecクライアント（IPsec Client）]：サイト間 VPN 接続の IPSec クライアント証明書を検証します。
   - [SSLクライアント（SSL Client）]：リモートアクセス VPN 接続の試行中に SSL クライアント証明書を検証します。
   - [SSLサーバー（SSL Server）]：Cisco Umbrella サーバー証明書など、SSL サーバー証明書を検証する場合に選択します。

詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「証明書の登録オブジェクトの追加」を参照してください。

オブジェクトグループ検索設定の強化

Firewall Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイスオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます（**[デバイス（Devices）] > [デバイス管理（Device Management）]**、[編集（Edit）]（  ）をクリックします。次に、[**Device > Advanced Settings**] の順にクリックします。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイスオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。

オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU 使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセス コントロール ポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。1000 シリーズ、2110、2120 などのローエンドの Firepower デバイスでは、CPU 使用率の増大によりデバイスが遅くなります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。デフォルトでは、オブジェクトグループ検索の設定が有効になっています。

オブジェクトグループの検索を有効にしてから、デバイスを設定し、しばらくの間操作した場合、この機能を無効にすると、望ましくない結果になる可能性があります。オブジェクトグループの検索を無効にすると、既存のアクセス制御ルールがデバイスの実行コンフィギュレーションで拡張されます。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。デバイスが正常に動作している場合は、一度有効にしたオブジェクトグループ検索を無効にしないでください。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「オブジェクトグループ検索の構成」を参照してください。

サポート コンポーネントの強化

Firewall Threat Defense ソフトウェアは、基盤となる複雑なファームウェアとオペレーティング システム ソフトウェアに依存しています。これらの基盤となるソフトウェア コンポーネントには独自のセキュリティ リスクが潜んでおり、対処する必要があります。

- セキュリティ上の問題を考慮した、ネットワークの運用セキュリティ プロセスを確立してください。
- Firewall Threat Defense モデル 2100、4100、および 9300 デバイスでは、Firewall Threat Defense を実行する Firepower Extensible Operating System を保護してください。『*CiscoFirepower 4100/9300 FXOS Hardening Guide*』を参照してください。

Firepower 1000 および Cisco Secure Firewall 3100/4200 の前面パネル USB-A ポートの無効化

ポートはデフォルトで有効になっているため、セキュリティ上の理由により Firepower 1000 および Secure Firewall 3100/4200 の前面パネル USB-A ポートを無効化することを推奨します。

- USB ポートの現在の管理状態および動作状態を表示するには、**system support usb show** コマンドを使用します。
- 前面パネルの USB ポートを無効化するには、**system support usb port disable** コマンドを使用します。

詳細については『*Cisco Secure Firewall Threat Defense コマンドリファレンス*』を参照してください。

セキュアな HTTP プロキシ設定

Threat Defense デバイスとインターネットの間に直接接続がない場合は、管理インターフェイスの HTTP プロキシを設定できます。するとシステムは、すべての管理接続にそのプロキシを使用します。Threat Defense デバイスの CLI で `configure network http-proxy` コマンドを使用して、HTTP プロキシを設定できます。プロキシパスワードを設定する際は、必ず強力なパスワードを使用してください。

セキュアなループバック インターフェイス

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、任意の物理インターフェイスからアクセスできるため、経路の障害を解決するのに役立ちます。あるインターフェイスがダウンした場合は、別のインターフェイスからループバック インターフェイスにアクセスできます。

ループバック インターフェイスは、AAA、BGP、DNS、HTTP、ICMP、IPsec フロー オフロード（Secure Firewall 3100 および 4200 のみ）、NetFlow、SNMP、SSH、静的およびダイナミック VTI トンネル、Syslog などのサービスに使用できます。ループバック インターフェイスでは、必要なサービスのみを有効にしてください。

詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「ループバック インターフェイスの設定」を参照してください。

デバイス登録キーまたはシリアル番号を使用したデバイスのセキュアな導入準備

デバイスのシリアル番号または登録キーを使用して、Firewall Management Center に対するデバイスの導入準備を簡単に行えます。また、デバイステンプレートを使用して、事前にプロビジョニングされた設定でデバイスを起動できます。導入準備プロセスの前に、デバイスのシリアル番号または登録キーを保護することを推奨します。

詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「Add a Device to the Firewall Management Center Using a Device Template」を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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/

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。