Cisco Secure Firewall Management Center バージョン 10.0 強化ガイド

改訂：2026 年 4 月 16 日

はじめに

Cisco Secure Firewall Threat Defense（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。このドキュメントは、Cisco Secure Firewall Management Center （Firewall Management Center）の強化に役立ちます。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 Threat Defense Hardening Guide*
- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

このドキュメントで説明しているすべての設定が、Firewall Management Center 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。詳細については、以下を参照してください。

- *Cisco Secure Firewall Management Center* の新機能（リリース別）
- Cisco Secure Firewall Threat Defense ドキュメント一覧

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 デバイス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。Management Center のドキュメントおよび 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 Management Center 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 Management Center 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。シスコでは、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「アップデート」の章、および『*Secure Firewall Management Center アップグレードガイド*』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、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、**[管理（Administration）] > [アップグレードと更新（Upgrades & updates）] > [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 Firewall Management Center で GeoDB を更新します。
- インターネットにアクセスし、Firewall Management Center で GeoDB を更新します。

- インターネットにアクセスし、Firewall 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「ジオロケーション データベースの更新」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。これらの更アップデートを 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。

Firewall Management Center Web インターフェイスでは、侵入ルールを更新するための 3 つのアプローチが提供されており、すべて **[管理（Administration）] > [アップグレードと更新（Upgrades & updates）] > [コンテンツの更新（Content Updates）] > [ルールの更新（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 Management CenterFirewall 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、**[管理（Administration）] > [アップグレードと更新（Upgrades & updates）] > [コンテンツの更新（Content Updates）] > [ルールの更新（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 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。

Management Center の 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（**[管理（Administration）] > [アップグレードと更新（Upgrades & updates）] > [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（**[管理（Administration）] > [詳細設定（Advanced）] > [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）]>[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。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 Management Center 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 **[管理（Administration）]>[設定（Configuration）]>[UCAPL/CC遵守（UCAPL/CC Compliance）]** の下に表示されます。

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。Secure Firewall 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に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、詳細について『*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。

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 の導入では、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。これらの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ネットワーク資産のすべてを保護できます。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 **[管理（Administration）] > [設定（Configuration）] > [時間（Time）]** を使用し、「*Cisco Secure Firewall Management Center アドミニストレーション ガイド*」の「時刻の同期」の手順を実行します。

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。ローカル DNS サーバに接続するように Firewall Management Center を設定することは、初期設定プロセスの一環として、ご使用のハードウェアモデルの『Cisco Secure Firepower Management Center スタートアップガイド』に記載されています。

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、『DNS のベストプラクティス、ネットワーク保護および攻撃の識別』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

『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「SNMP ポーリング」で説明されているように、SNMP ポーリングを使用して Firewall Management Center をモニタリングできます。SNMP ポーリングを使用する場合は、SNMP Management Information Base（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。そのため、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する必要があります。

（Firewall Management Center WEB インターフェイスの **[管理（Administration）] > [設定（Configuration）] > [SNMP]** で）SNMP ポーリングを設定する場合、次のオプションを使用して、展開環境内の SNMP を強化します。

- 次をサポートする 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。
- 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
- ネットワーク管理アクセス用の [認証パスワード（Authentication Password）] を設定する場合には、強力なパスワードを使用します。
- **プライバシーパスワード**を設定する場合は、強力なパスワードを使用します。
- [プライバシープロトコル（Privacy Protocol）] にAES128を選択します。

さらに、SNMP アクセスのアクセス リストを、MIB のポーリングに使用される特定のホストに制限する必要もあります。このオプションは、**[管理（Administration）] > [設定（Configuration）] > [アクセスリスト（Access List）]** の Firewall Management Center Web インターフェイスに表示されます。「*Cisco Secure Firewall Management Center アドミニストレーション ガイド*」を参照してください。

また、Firewall Management Center は SNMP サーバへの外部アラートの送信もサポートしています。この機能を保護するには、セキュアな外部アラート （18 ページ） 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展開環境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「デバイステンプレートを使用した Firewall Management Center へのデバイスの追加」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。

管理対象デバイスへのセキュアなアクセス

Cisco Secure Firewall の展開には、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。これらのデバイスは、Firewall Management Center との間で情報を交換します。これらの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。環境内にあるデバイスを分析して、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。

Firewall Management Center ユーザー アクセスの強化

内部および外部ユーザー

Firewall Management Center 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：システムは、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は、システムは外部 LDAP または RADIUS の認証サーバーにクエリします。

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 インターフェイスの中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、管理対象デバイスだけでなく Firewall Management Center でも外部ユーザを認証できます。

ユーザー アクセスのタイプ

Firewall Management Center は次の 2 種類のユーザー アクセスをサポートしています。

- Web インターフェイス (HTTP) ：内部と外部の両方のユーザーアカウントで使用できます。
- SSH、シリアル、またはキーボード / モニタ接続を使用したコマンドラインアクセス：CLI/シェルアクセス権を持つ**管理者**アカウントで利用でき、外部ユーザーにも提供できます。

管理権限の制限

Firewall Management Center は、2 つの **admin** アカウントをサポートしています。

- Web インターフェイス（HTTP）を介して Firewall Management Center にアクセスするための **admin** アカウント。
- SSH、シリアル、またはキーボードおよびモニタ接続を使用した CLI/シェル アクセス用の **admin** アカウント。デフォルト設定では、このアカウントは Linux シェルに直接アクセスできます。このアカウントは、Linux シェルではなく Firewall Management Center 補助 CLI にアクセスするように設定できます（シェル アクセスの制限 （10 ページ） を参照）。Firewall Management Center CLI 内から、このアカウントは CLI **expert** コマンドを使用して Linux シェルに直接アクセスできます（**expert** コマンドを無効にしていない場合。この点についても「シェル アクセスの制限 （10 ページ）」を参照）。

（注） Firewall Management Center の初期設定では、両方の **admin** アカウントのパスワードは同じですが、同じアカウントではないため、システムはこれらのパスワードをさまざまなデータベースに対して検証します。

admin アカウントには、同じ権限を持つ追加のアカウントを作成する権限など、他のユーザーよりも上位の設定権限があります。管理権限を持つ任意のアカウントへのアクセスが許可されるユーザを選択する場合には、慎重に検討してください。

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「Firewall Management Center のユーザーアカウントに関するガイドラインと制限事項」を参照してください。

シェル アクセスの制限

デフォルトでは、コマンドラインアクセス権を持つユーザーはログイン時に Linux シェルへ直接アクセスできます。CLI またはシェルユーザーが Linux シェルにアクセスするには、CLI の **expert** コマンドを実行する追加の手順が必要です。

（注） すべてのデバイスでは、SSH を介した CLI またはシェル SSH へのログイン試行が 3 回連続して失敗したら SSH 接続は終了します。

注意 すべてのデバイス上で、CLI/シェルへのアクセス権があるユーザはシェルのルート権限を取得できるため、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 セキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、CLI/シェルへのアクセス権があるユーザーのリストを適切に制限してください。
- シェルにユーザーを直接追加しないでください。ご使用のバージョンの『Cisco Secure Firewall Management Center 設定ガイド』で説明されている手順のみを使用して新しいアカウントを作成します。
- Cisco TAC による指示がない限り、シェルや CLI **expert** モードを使用して Firewall Management Center にアクセスしないでください。

Firewall Management Center アクセスタイプの詳細については、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「Web インターフェイスと CLI アクセス」を参照してください。

Firewall Management Center での Linux シェル アクセスに関連した、実行可能な最も安全な強化アクションは、シェルへのすべてのアクセスをブロックすることです。

- SSH、シリアルまたはキーボードおよびモニター接続を使用して Firewall Management Center にログインします（ご使用の Firewall Management Center モデルの『Getting Started Guide』を参照してください）。

- **system lockdown** コマンドを入力します。（『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「Cisco Secure Firewall Firewall Management Center コマンドラインリファレンス」の章を参照してください）

system lockdown コマンドを使用すると、コマンド ライン クレデンシャルで Firewall Management Center にログインしているユーザーがアクセスできるのは、Firewall Management Center の CLI コマンドのみになります。これは有効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。

Firewall Management Center CLI の詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「Secure Firewall Firewall Management Center コマンドラインリファレンス」の章を参照してください。

マルチテナント機能を使用した管理対象デバイス、設定、およびイベントへのユーザー アクセスのセグメント化

管理者は、Cisco Secure Firewall 展開内の管理対象デバイス、設定、およびイベントをドメインにグループ化し、選択したドメインへのアクセスを必要に応じて Firewall Management Center ユーザーに許可できます。ユーザーは、ユーザー ロールによって課された制限に加えて、ドメインの割り当てによって課されるアクセス制限の範囲内で操作します。たとえば、1 つのドメイン内で選択したアカウントへのフル管理者アクセスを許可したり、別のドメイン内でセキュリティ アナリスト アクセスを許可したり、3 番目のドメインへのアクセスを許可しなかったりすることができます。

[管理（Administration）] > [ドメイン（Domains）] を使用して、Firewall Management Center Web インターフェイスからドメインを作成および管理します。マルチテナントの実装についての詳細は、*Cisco Secure Firewall Management Center アドミニストレーション ガイド*の「ドメイン」を参照してください。

[管理（Administration）] > [ユーザー（Users）] > [ユーザーアカウント（User Accounts）] を使用して、Firewall Management Center Webインターフェイスからドメイン内のユーザーに権限を割り当てます。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「内部ユーザーの追加または編集」を参照してください。

内部ユーザー アカウントの強化

内部ユーザは、 Web インターフェイスを介してのみ Firewall Management Center にアクセスできます。管理者は、**[管理（Administration）] > [ユーザー（Users）] > [ユーザーアカウント（User Accounts）]** の次の設定を使用して、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を強化することができます。

- アカウントをロックする前の、Web インターフェイスログインの最大失敗回数を制限します。
- パスワード長の最小値を適用します。
- パスワードの有効日数を設定します。
- 強力なパスワードを要求します。
- Web インターフェイス セッション タイムアウトの適用からユーザーを除外しません。
- アカウントに必要なアクセス タイプのみに適合するユーザ ロールを割り当てます。
- ユーザーに必要なアクセス タイプに適合するドメインを割り当てます。

- 次回のログイン時に、ユーザにアカウント パスワードのリセットを強制します。

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「ユーザー」の章を参照してください。

管理者は、**[管理（Administration）]** > **[設定（Configuration）]** > **[ユーザー設定（User Configuration）]** の内部 Web インターフェイス ユーザすべてに対して、次の設定をグローバルに実行することもできます。

- パスワード再利用の制限
- 成功したログインの追跡
- 選択した回数のログインに失敗したユーザーの、Web インターフェイスアクセスを一時的にブロックする

これらの設定の詳細については、『*Cisco Secure Firewall Management Center* アドミニストレーション ガイド』の「ユーザーの設定」を参照してください。

カスタムユーザーロールを作成し、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を提供できるようになりました。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「カスタムユーザーロールの作成」を参照してください。

外部ユーザ アカウントの強化

Firewall Management Center は、外部サーバ（LDAP または RADIUS）に保存されているユーザ データベースに対して外部ユーザ アカウントを認証します。

（注） 外部認証の使用を選択する場合には、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 （20 ページ） の情報を確認してください。

（注） 外部認証を使用するには、Firewall Management Center で DNS を使用する必要があります。DNS を使用するように Firewall Management Center を設定することは、通常、初期設定プロセス中に行われます。セキュリティに関する業界推奨のベスト プラクティスに従って、ローカル DNS が設定されていることを確認してください。ドメイン ネーム システム（DNS）の保護 （7 ページ） を参照してください。

重要 LDAP または RADIUS サーバとのセキュアな接続を Firewall Management Center 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。

Firewall Management Center ユーザ認証用に外部サーバを設定するには、**[管理（Administration）]** > **[ユーザー（Users）]** > **[外部認証（External Authentication）]** で外部認証オブジェクトを作成する必要があります。外部認証されたユーザ アカウントを使用した攻撃に対して Firewall Management Center を強化するには、外部認証オブジェクトで次のオプションを使用します。

- アカウントへのシェル アクセスを使用したユーザのアクセスを慎重に制限します。シェル ユーザーは 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。
- アカウントに必要以上のアクセス権を付与しないでください。
  - LDAP を使用している場合、適切な Firewall Management Center ユーザーロールを LDAP ユーザーまたはユーザーグループに関連付けます。
  - RADIUS を使用している場合、適切な Firewall Management Center ユーザーロールを RADIUS 属性に関連付けます。
- LDAP を使用している場合、外部認証オブジェクトの設定時に、[拡張オプション（Advanced Options）] で TLS または SSL 暗号化を設定します。

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「Firewall Management Centerの外部認証の設定」を参照してください。

セッション タイムアウトの確立

アカウントのログイン セッションの長さを制限すると、権限のないユーザーが無人セッションを悪用する機会が減少します。

Firewall Management Center でセッション タイムアウトを設定するには、**[管理（Administration）] > [設定（Configuration）] > [セッションタイムアウト（Session Timeout）]** を使用します。ここで、次のインターフェイス タイムアウト値を分単位で設定できます。

- **ブラウザ セッション タイムアウト**：Firewall Management Center Web インターフェイスセッションのタイムアウト。
- **CLI タイムアウト**：CLI アクセスのタイムアウト。

これらの設定は、アクセス ロールに関係なく、内部および外部アカウントに適用されます。『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「セッションタイムアウト」を参照してください。

REST API アクセスの無効化

Firewall Management Center 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。Firewall Management Center の REST API の詳細については、ご使用のバージョンの『Secure Firewall Management Center REST API スタートアップガイド』を参照してください。

デフォルトでは、Firewall Management Centerはアプリケーションからの REST API を使用した要求を許可します。Firewall Management Center を強化するには、このアクセスを無効にする必要があります。Firewall Management Center Web インターフェイスで **[管理（Administration）] > [設定（Configuration）] > [REST APIの優先設定（REST API Preferences）]** を選択し、[REST APIを有効にする（Enable REST API）] チェックボックスをオフにします。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「REST API 設定」を参照してください。

すべての RADIUS 応答に Message-Authenticator 属性を強制します。

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と使用できます（[管理（Administration）]>[ユーザー（Users）]>[外部認証（External Authentication）]>[外部認証オブジェクトの追加（Add External Authentication Object）]>[RADIUS]の順に選択します）。

リモート アクセスの制限

Firewall Management Center では、アクセス リストを使用して、IP アドレスとポートを基準にシステムへのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：CLI/シェル アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。

👉

重要 Firewall Management Center から SNMP サーバーへのセキュアな接続を設定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。

よりセキュアな環境で運用するには、これらの形式でのアクセスを特定の IP アドレスにアクセスする場合にのみ許可するように Firewall Management Center を設定し、任意の IP アドレスへの HTTPS または SSH アクセスを許可するデフォルト ルールを無効にします。これらのオプションは、Management Center Web インターフェイスの **[管理（Administration）]** > **[設定（Configuration）]** > **[アクセスリスト（Access List）]** の下に表示されます。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「アクセスリスト」を参照してください。

修復は使用しない

修復は、 Firewall Management Center システムが相関ポリシー違反に応じて起動するプログラムです。Firewall Management Center では複数のタイプの修復を設定できますが、どのタイプの場合も、Firewall Management Center と外部のエンティティが安全ではない方法で通信する必要があります。このため、強化された Firewall Management Center で修復を使用するように設定しないことをお勧めします。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「修復」を参照してください。

Firewall Management Center と Web ブラウザの間のセキュア通信

クライアントとサーバーの両方の HTTPS 証明書を使用して、Web インターフェイスを実行しているブラウザと Firewall Management Center の間の接続を保護することにより、Firewall Management Center とローカルコンピュータの間で送信される情報を保護します。Firewall Management Center ではデフォルトの自己署名証明書が使用されますが、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に置き換えることをお勧めします。

Firewall Management Center の HTTPS 証明書を設定するには、Firewall Management Center Web インターフェイスの **[管理（Administration）]** > **[設定（Configuration）]** > **[HTTPS証明書（HTTPS Certificate）]** を使用します。「*Cisco Secure Firewall Management Center アドミニストレーション ガイド*」の「HTTPS 証明書」を参照してください。

アクセス コントロール ポリシーのロック

アクセスコントロールポリシーをロックして、他の管理者が編集できないようにすることができます。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。ロックしない場合、複数の管理者がポリシーを同時に編集すると、最初に変更を保存したユーザーが他の全ユーザーの変更を上書きします。このロックはアクセス コントロール ポリシー用であり、ポリシーで使用されるオブジェクトには適用されません。ロックすると、他の管理者にはポリシーへの読み取り専用アクセス権が付与されます。ただし、他の管理者は、ロックされたポリシーを管理対象デバイスに割り当てることができます。ポリシーを編集する際に、アクセス コントロール ポリシーをロックすることをお勧めします。

1. **[ポリシー（Policies）]** > **[セキュリティポリシー（Security policies）]** > **[アクセス制御（Access Control）]** を選択します。
2. ロックまたはロック解除するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。
3. ポリシー名の横にあるロックアイコンをクリックして、ポリシーをロックまたはロック解除します。

他の管理者によってロックされているポリシーのロックを解除するには、**[ポリシー（Policies）]** > **[セキュリティポリシー（Security policies）]** > **[アクセス制御（Access Control）]** の権限を更新して、[アクセス コントロール ポリシー（Access Control Policy）]をクリックする必要があります。次に、[アクセス コントロール ポリシーの変更（Modify Access Control Policy）] > [アクセス コントロール ポリシー ロックの上書き（Override Access Control Policy Lock）] の順にクリックします。デフォルトでは、管理ユーザーロールに対してこの権限が有効になります。この権限を有効にしないことを推奨します。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「アクセス コントロール ポリシーのロック」を参照してください。

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 Management Center 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 **[管理（Administration）]** > **[詳細設定（Advanced）]** > **[バックアップと復元（Backup & Restore）]** の下に表示されます。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「Firewall Management Center のバックアップ」を参照してください。

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。

設定のエクスポートとインポートを保護する

Firewall Management Center は、さまざまなシステム設定（ポリシー、カスタムテーブル、レポートテンプレートなど）をファイルにエクスポートする機能を備えています。これらの設定は、同じバージョンを実行している別の Firewall Management Center にインポートできます。これは、環境に新しいアプライアンスを追加する管理者のための時間節約になる機能ですが、セキュリティ違反を防ぐためには慎重に使用する必要があります。エクスポート/インポート機能を使用する場合は、次の注意事項に留意してください。

- 転送される設定情報を保護するため、Firewall Management Center と Web ブラウザ間の通信を保護します。Firewall Management Center と Web ブラウザの間のセキュア通信 （15 ページ）を参照してください。
- エクスポートされた設定ファイルが保存されているローカル コンピュータへのアクセスを保護します。このファイルを保護することは、展開環境のセキュリティにとって重要です。
- 秘密キーを含む PKI オブジェクトを使用する設定をエクスポートすると、エクスポートの前に秘密キーが復号されることに注意してください。エクスポートされた秘密キーはクリアテキストで保存されます。インポート時に、キーはランダムに生成されたキーで暗号化されます。

設定のエクスポートとインポートの機能は、Firewall Management Center Web インターフェイスの **[管理（Administration）] > [詳細設定（Advanced）] > [インポートとエクスポート（Import & Export）]** に表示されます。この機能の詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「インポート/エクスポート」を参照してください。

自動ロールバックを使用した管理接続の保護

展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできます。Management Center へのアクセスにデータインターフェイスを使用している状況で、データインターフェイスを誤って設定すると、展開の自動ロールバックが発生します。

[デバイス（Devices）] > **[デバイス管理（Device Management）]** を使用して自動ロールバック設定を有効にし、[編集（Edit）]（✎）をクリックすることを推奨します。次に、[デバイス（Device）] > [展開設定（Deployment Settings）] の順にクリックし、接続モニター間隔を設定します。自動ロールバックは、高可用性展開やクラスタリング展開、およびトランスペアレントモードではサポートされていません。詳細については、『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「展開設定の編集」を参照してください。

レポートの保護

Firewall Management Center にはいくつかのタイプのレポートが用意されています。これらすべてには、権限のない人によるアクセスから保護する必要がある機密情報が含まれています。すべてのレポートタイプは、Firewall Management Center からローカルコンピュータに暗号化されていない形式でダウンロードできます。転送される情報を保護するため、レポートをダウンロードする前に、Firewall Management Center と Web ブラウザ間の通信を保護します。Firewall Management Center と Web ブラウザの間のセキュア通信 （15 ページ） を参照してください。）さらに、レポートが保存されているローカル コンピュータへのアクセスを保護します。

- 標準レポートは、システムの全側面に関する詳細でカスタマイズ可能なレポートで、HTML、CSV、PDF 形式で入手できます。リスク レポートは、組織で検出されたリスクの概要を HTML 形式で示します。

  Firewall Management Center Web インターフェイスでは、標準レポートとリスクレポートの両方が [インサイトとレポート（Insights & Reports）] > [レポート作成（Reporting）] > [レポート（Reports）] に表示されます。これらのレポートには、ローカルダウンロードに加えて 2 つの保存オプションがあり、それぞれにセキュリティリスクが伴います。

  - レポートを選択したサーバに電子メールで自動送信できます。電子メールを保護できないため、強化されたシステムでこの機能を使用することはお勧めしません。
  - レポートをリモート デバイスに自動保存できます。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、強化されたシステムにこの機能を使用することはお勧めしません。

  標準レポートおよびリスクレポートの設計および生成の詳細については、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「レポート」を参照してください。

- トラブルシューティングのヘルス モニタ レポートには、システムに問題が発生した場合の診断に Cisco TAC が使用できる情報が含まれています。Firewall Management Center Web インターフェイスからこれらのレポートを生成するには、**[トラブルシューティング（Troubleshooting）]** > **[ヘルス（Health）]** > **[モニター（Monitor）]** を使用して、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「トラブルシューティング用のヘルスモニタリングレポート」の手順を実行します。Firewall Management Center は、.tar および .gz 形式のトラブルシューティングファイルを生成します。

- ポリシー レポートは、現在保存されているポリシーの設定についての詳細を示す PDF ファイルです。レポートをサポートするポリシーの全リストについては、『*Cisco Secure Firewall Management Center アドミニストレーション ガイド*』の「現在のポリシーレポートの生成」を参照してください。

- 比較レポートを使用して、組織の標準規格への準拠やシステム パフォーマンスの最適化を目的としたポリシー変更を確認できます。2 つのポリシーの相違点や、保存されたポリシーと実行コンフィギュレーションの相違点を調べることができます。比較レポート（PDF 形式のみで入手可能）を生成するには、比較するポリシー タイプの管理ページにアクセスし、[ポリシーの比較（Compare Policies）] を選択します。『*Cisco Secure Firewall Management Center デバイス設定ガイド*』の「ポリシーの比較」を参照してください。

セキュアな外部アラート

選択したイベントが発生したときに、外部サーバーへのアラート応答と呼ばれる通知を発行するようにFirewall Management Centerを設定できます。これらのアラートは、システムアクティビティのモニタリングに役立つ可能性がありますが、外部サーバーへの接続を保護できない場合、セキュリティリスクが生じる可能性があります。

Firewall Management Center は、次の 3 つの形式でアラート応答の送信をサポートします。

- Syslogに送信されるアラート応答を保護することはできません。Firewall Management Center Webインターフェイスで**[管理（Administration）]**>**[アラート（Alerts）]**を選択し、[アラートの作成（Create Alert）]>[Syslogアラートを作成（Create Syslog Alert）]をクリックします。強化された環境でこのようなアラートを送信するようにFirewall Management Center を設定することは推奨されません。
- メール リレー ホストとの接続に暗号化（TLS または SSLv3）を使用し、ユーザー名とパスワードを要求するように設定することで、Firewall Management Centerが電子メールで外部サーバーに送信する情報を保護することができます。これは**[管理（Administration）]**>**[設定（Configuration）]**>**[Eメール通知（Email Notification）]**を使用して Firewall Management Center Web インターフェイスで実行します。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「メールリレーホストおよび通知アドレスの設定」を参照してください。

  メール リレー ホストとの接続を保護すると、Firewall Management Center が次の機能を使用して送信するデータが保護されます。

  - 電子メールアラート応答は、「*Cisco Secure Firewall Management Center* アドミニストレーション ガイド」の「電子メールアラート応答の作成」で説明されています。（この設定は**[管理（Administration）]**>**[アラート（Alerts）]**を使用して設定し、Firewall Management Center Web インターフェイスで[アラートの作成（Create Alert）]>**[電子メールアラートの作成（Create Email Alert）]**をクリックします。）
  - データプルーニング通知は、「*Cisco Secure Firewall Management Center* アドミニストレーション ガイド」の「データベースイベント数の制限の設定」で説明されています。（この設定は、Firewall Management Center Web インターフェイスの**[管理（Administration）]**>**[設定（Configuration）]**>**[データベース（Database）]**の下でこの設定を構成します。）

- SNMP サーバーに送信されるアラートは、**[管理（Administration）]**>**[アラート（Alerts）]**で以下のオプションを使用し、Firewall Management Center Web インターフェイスで[アラートの作成（Create Alert）]>[SNMPアラートの作成 （Create SNMP Alert）]をクリックすることで保護できます。
  - [バージョン（Version）]については SNMP v3 を選択します。このプロトコルは以下をサポートします。
    - 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。
  - 接続を保護する**認証プロトコル**（MD5 または SHA）を選択して、**パスワード**を入力します。
  - [プライバシープロトコル（Privacy Protocol）]として DES、AES、または AES128 を選択し、[パスワード（Password）]を入力します。キーが長いほど安全になりますが、パフォーマンスは低下します。

- システムがメッセージのエンコードに使用する**エンジン ID**を指定します。Firewall Management Center の IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Firewall Management Center の IP アドレスが 10.1.1.77 である場合、0a01014D0 を使用します。

SNMP アクセスのアクセスリストを、Firewall Management Center が SNMP アラートを送信する特定のホストに制限する必要があります。**[管理（Administration）] > [設定（Configuration）] > [アクセスリスト（Access List）]**を選択します。「*Cisco Secure Firewall Management Center アドミニストレーション ガイド*」を参照してください。

Firewall Management Center は、SNMP ポーリングもサポートしています。この機能を保護するには、セキュアな SNMP ポーリング （7 ページ） を参照してください。

重要 Firewall Management Center から SNMP サーバーまたは SMTP サーバーへのセキュアな接続を設定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。

外部アラートの全詳細については、「*Cisco Secure Firewall Management Center アドミニストレーション ガイド*」の「アラートの応答を使用した外部アラート」を参照してください。

監査ログの保護

Firewall Management Center は、[イベントとログ（Events & Logs）] > [分析（Analysis）] > [監査ログ（Audit Logs）] を使用して設定されたユーザーアクティビティの読み取り専用ログを保持します。Firewall Management Center のメモリリソースを節約するため、これらのログを外部（Syslog または HTTP サーバーへのストリーミング）で保存することもできます。ただし、この方法では、TLS を有効にし、TLS 証明書を使用して相互認証を確立することによって、監査ログストリーミングのチャネルを保護しない限り、セキュリティリスクが生じる可能性があります。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「監査ログのセキュアなストリーミング」を参照してください。

eStreamer への接続の保護

Event Streamer（eStreamer）を使用すると、Firewall Management Center からの数種類のイベント データを、カスタム開発されたクライアントアプリケーションにストリーム配信できます。詳細については、ご使用のバージョンの『*Secure Firewall eStreamer 統合ガイド*』を参照してください。組織が eStreamer クライアントの作成と使用を選択した場合、次の予防措置を講じてください。

- セキュリティに関する業界のベストプラクティスを使用してアプリケーションを開発する
- データが安全に送信されるように、Firewall Management Center と eStreamer クライアント間の接続を設定します。[統合（Integrations）] > [+さらに表示（+ Show more）] > [eStreamer] の順に選択し、eStreamer クライアントを実行するホストとの接続を保護する証明書ファイルを暗号化するためのパスワードを指定して、[クライアントの作成（Create Client）] をクリックします。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「eStreamer クライアント通信の設定」を参照してください。

Cisco Security Analytics and Logging への接続の保護

より長い保持期間でストレージを増やすために、Firewall Management Center イベントデータを保存するように Cisco Security Analytics and Logging（オンプレミス）を設定できます。

から Firewall Management Center Cisco Secure Network Analytics Manager へのクエリは、TLS 暗号化接続を介して行われます。デフォルトでは、Security Analytics and Logging は、Firewall Management Center が自動的にダウンロードできる自己署名証明書を使用します。Security Analytics and Logging への接続を保護するため、次の点を推奨します。

- 安全なチャネルを使用して証明書を手動で転送し、Firewall Management Center にアップロードしてください。
- 世界的に知られていて信頼できる証明機関が生成した証明書を使用してください。

イベントは、syslog を使用して Cisco Security Analytics and Logging（オンプレミス）に送信されます。syslog 機能を設定するときは、安全なオプションを選択してください。

外部データベースアクセスの廃止

外部データベースアクセスのサポートが廃止されました。サードパーティのレポートツール、カスタムアプリケーション、および RunQuery などのシスコ提供ツールを使用して Firewall Management Center のデータベースにアクセスすることはできなくなりました。データベースアクセスを有効にし、関連ツールをダウンロードするオプションは、システム設定では使用できなくなりました。

外部データベースアクセス機能の廃止により、サードパーティのレポートツールやカスタムアプリケーションに関連する潜在的な攻撃経路が排除され、Firewall Management Center データベースの整合性が損なわれるリスクが低減され、セキュリティが大幅に強化されます。安全に導入するため、データベースへのアクセスおよびクエリはすべて Firewall Management Center の統合管理機能を通じて実行し、厳格な制御を維持するとともに脆弱性リスクを低減してください。

ログイン バナーのカスタマイズ

Firewall Management Center へのアクセスが許可されているかどうかにかかわらず、ユーザはシステムのログインページを表示できます。ログインバナーをカスタマイズして、誰が見ても差し支えない情報のみが表示されるようにします。Firewall Management Center Web インターフェイスで、**[管理（Administration）] > [設定（Configuration）] > [ログインバナー（Login Banner）]** を選択します。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「ログインバナー」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

Firewall Management Center 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 Management Center 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 （12 ページ）」の情報を確認してください。

（注） Firewall Management Center 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。

（注） Firewall Management Center は、RADIUS サーバーを使用してネットワークに VPN 機能を提供することもできます。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*』の「VPN の概要」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

Firewall Management Center オブジェクトは、レルムと呼ばれ、Active Directory 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「レルム」の章を参照してください。

（Firewall Management Center Web インターフェイスの [統合（Integration）] > [その他の統合（Other Integration）] > [レルム（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 サーバとの接続を設定するには、Firewall Management Center Web インターフェイスの **[オブジェクト（Objects）]** > **[AAAサーバー（AAA Server）]** > **[RADIUSサーバーグループ（RADIUS Server Group）]** で RADIUS サーバ 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 サーバ間でデータを暗号化するための [キー（Key）] と [キーの確認（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。
- Microsoft Azure AD

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）]** > **[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、[ESTサーバー証明書の検証を無視する（Ignore EST Server Certificate Validations）] チェックボックスをオンにしないことをお勧めします。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 2048 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。これらの制限を上書きするには、[Weak-Cryptoを有効にする（Enable Weak-Crypto）] オ

プション (**[デバイス（Devices）]** > **[証明書（Certificates）]**) を使用できます。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 を有効にして、ピア証明書の検証などを可能にすることができます。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）]** > **[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。次に、[デバイス（Device）] > [詳細設定（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 Management Center 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 Management Center モデル 1000、1600、2000、2500、2600、4000、4500、および 4600 の場合、 Firewall Management Center ソフトウェアの基盤となるハードウェア デバイスのコンポーネントを強化するには、『*Cisco UCS 強化ガイド*』を参照してください。

セキュアな HTTP プロキシ設定

Firewall Management Center は、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。ただし、管理インターフェース用にプロキシサーバーを使用することができ、HTTP ダイジェストを使用して認証できます。HTTP プロキシサーバーを設定するには、以下の手順に従ってください。

手順

ステップ 1 **[管理（Administration）] > [設定（Configuration）]**を選択します。

ステップ 2 左ペインで. [管理インターフェース（Management Interfaces）] を選択します。

ステップ 3 [プロキシ（Proxy）] の下で、[有効化（Enabled）] チェックボックスをオンにします。

ステップ 4 [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 [ポート（Port）] フィールドに、ポート番号を入力します。

ステップ 6 [プロキシ認証を使用（Use Proxy Authentication）] チェックボックスをオンにし、認証ログイン情報を入力します。

プロキシの**パスワード**を設定するときには、強力なパスワードを使用してください。

ループバック インターフェイスの保護

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。

ヘルスモニタリングの設定

Firewall Management Center の正常性モニターでは、さまざまな正常性インジケータを追跡して、システムのハードウェアとソフトウェアが正常に動作することを確認します。ヘルスモニタリングを使用して、展開全体の重要な機能のステータスを確認できます。各アプライアンスごとに、CPU 使用率、シャーシ環境ステータス、ハードウェアアラーム、電源、ディスクステータス、メモリ使用率、プロセスステータスを含む専用のヘルスポリシーを設定し、ヘルスモニタリングアラートを構成することを推奨します。アプライアンスにヘルスポリシーを適用すると、対応するヘルステストがアプライアンスのプロセスおよびハードウェアの健全性を自動的に監視します。また、ボックスの状態に関するメトリックも収集できます。さらに、デフォルトのヘルスポリシーも設定できます。デバイスを Firewall Management Center に追加すると、Firewall Management Center は管理対象デバイスにデフォルトの正常性ポリシーを適用します。重大なアラートがデフォルトのヘルスポリシーに含まれていることを確認します。

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「ヘルスモニタリングについて」を参照してください。

変更管理承認の確認

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（**[管理（Administration）] > [設定（Configuration）] > [変更管理（Change Management）]**）を有効にできます。変更管理には、変更を展開する前の監査追跡と公式承認が含まれます。管理者は、設定の変更を確認して検証してから承認することを推奨します。

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「変更管理」を参照してください。

Secure Erase コマンドの確認と実行

Secure Erase コマンドは、以下のタイプの管理センターのハードドライブデータを完全に消去します。

- Firepower Firewall Management Center 1600、2600、4600
- Firewall Firewall Management Center 1700、2700、4700

管理者権限を持つユーザーだけがこのコマンドを使用するようにしてください。

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「Secure Erase」を参照してください。

ストリーミングテレメトリ用の gNMI サーバーへのセキュア接続

Firewall Management Center のOpenConfig ストリーミング テレメトリ オプションは、gNMI（gRPCネットワーク管理インターフェイス）プロトコルを使用して、Threat Defense デバイスからデータ収集システムへのテレメトリストリームを制御および生成できるようにします。ヘルスポリシーをデバイスに展開すると、OpenConfig ストリーミングテレメトリ設定によってgNMIサーバーがアクティブ化され、データコレクターからのリモートプロシージャコール（RPC）メッセージのリッスンが開始されます。

データが安全に送信されるように、Firewall Management Center と gNMI サーバー間の接続を設定します。gNMI サーバーと gNMI クライアント間のすべての通信で TLS 暗号化が使用されるため、TLS 暗号化用の秘密鍵を使用して一連の証明書を生成する必要があります。gNMI サーバーへの接続を保護するには、以下が推奨されます。

- 安全なチャネルを使用して証明書を手動で転送し、Firewall Management Center にアップロードしてください。
- 世界的に知られていて信頼できる証明機関が生成した証明書を使用してください。
- SSL 証明書に強力なパスフレーズまたは秘密鍵を使用してください。
- 強力なパスワードを使用して gNMI コレクタを認証してください。

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「OpenConfig を使用したベンダー中立のテレメトリストリーミングの送信」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「Firewall Management Center デバイステンプレートを使用してデバイスを追加する」を参照してください。

アクセス制御ルールの作成と構成の最適化

アクセス制御ルールは、意図したトラフィックフローを制御し、不正アクセスを最小限に抑え、望ましくないトラフィックがネットワークにアクセスして侵害するのを防ぎます。これらのルールにより、意図したサイトや承認されたサイトにアクセスすることもできます。

次のことをお勧めします。

- 正確かつ簡潔で、適切な順序に配置されたルールを設計してください。
- デフォルトアクションを「ブロック」に設定してください。
- パブリックインターネットにアクセスするための許可アクセスルールを設定してください。

- 一般的なルールより前に、特定のアクセス コントロール ポリシーを設定してください。

（注） 注：アクセスルールの設定ミスや順序の誤りは、正常なトラフィックをブロックし、ネットワークの可用性に影響を与える可能性があります。

詳細については、『*Cisco Secure Firewall Management Center デバイス設定*』の「アクセス制御」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。