Cisco Secure Firewall Management Center バージョン 7.2 強化ガイド

初版：2022 年 6 月 27 日

はじめに

Firepower はネットワークの資産やトラフィックをサイバー脅威から守りますが、Firepower が「強化」されるように Firepower 自体の設定を行うことも必要です。これにより、サイバー攻撃に対する Firepower の脆弱性がさらに軽減されます。このガイドでは、お使いの Firepower 環境の強化について、特に Secure Firewall Management Center（Management Center）を中心に説明します。Firepower 環境の他のコンポーネントに関する強化情報については、次のドキュメントを参照してください。

- *Cisco Firepower Threat Defense Hardening Guide, Version 7.2*
- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

このガイドは、Management Center Web インターフェイスの構成時の設定を示していますが、このインターフェイスの詳細なマニュアルとしての使用を意図したものではありません。

このマニュアルで説明されているすべての構成時の設定を、すべての Firepower バージョンで使用できるわけではありません。各リリースの新機能および廃止された機能の詳細については、『Cisco Firepower Management Center New Features by Release』を参照してください。Firepower 環境の設定の詳細については、ご使用のバージョンに対応した Firepower のマニュアル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、Firepower 環境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。Firepower のドキュメントおよび Secure 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 Firepower の設定は、認定機関が定める現在のすべての要件に厳密に準拠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、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、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 Administration Guide, 7.2*』の「Security Certifications Compliance Recommendations」を参照してください。この強化ガイドと『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』が認定固有のガイダンスと矛盾しないように努めてきました。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、「シスコのセキュリティ アドバイザリおよびアラート（Cisco Security Advisories and Alerts）」ページで確認できます。これらのコミュニケーション手段の詳細については、「シスコのセキュリティ脆弱性ポリシー」を参照してください。

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、Firepower 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更新されていることを確認するには、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』、

『*Firepower Management Center Upgrade Guide*』の「System Updates」の章の情報をご利用ください。

シスコでは、Firepower が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。Firepower 環境のいずれかのコンポーネントを更新する場合は、アップデートに付属する「Cisco Firepower 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、更新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）は、ルーティング可能な IP アドレスと関連付けられた地理的データ（国、都市、座標など）および接続関連のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。検出された IP アドレスと一致する GeoDB 情報が Firepower で検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。国や大陸以外の位置情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。

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）]**>**[更新（Updates）]**>**[地理位置情報の更新（Geolocation Updates）]** を使用し、次のいずれかの方法を選択します。

- 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 Administration Guide, 7.2*』の「Update the Geolocation Database」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 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ための 3 つのアプローチが提供されており、すべて**[システム（System）]**>**[更新（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 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 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 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 Administration Guide, 7.2*』の「Update Intrusion Rules」を参照してください。

また、**[システム（System）] > [更新（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。それらを Management Center にインポートする前に、『』の「Guidelines for Importing Local Intrusion Rules」、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Best Practices for Importing Local Intrusion Rules」を参照し、ローカル侵入ルールのインポートがセキュリティポリシーに準拠していることを確認します。

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 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）] > [更新（Updates）] > [製品の更新（Product 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 Administration Guide, 7.2*』の「Update the Vulnerability Database」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。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 Device Configuration Guide, 7.2*』の「Security Intelligence Lists and Feeds」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、Management Center の CC または UCAPL モードを選択します。この設定は、Management Center Web インターフェイスの **[システム（System）] > [設定（Configuration）] > [UCAPL/CC準拠（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 Administration Guide, 7.2*』の「Security Certification Compliance Characteristics」に記載されている変更が有効になります。Firepower 環境内のアプライアンスはすべて、同じセキュリティ認定準拠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 Administration Guide, 7.2*』の「Security Certifications Compliance」で詳細な情報を参照してください。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

Firepower 環境では、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、Firepower 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

Firepower を正常に動作させるには、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、 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。Management Center Web インターフェイスから **[システム（System）]** > **[設定（Configuration）]** > **[時刻の同期（Time Synchronization）]** を使用して、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Synchronize Time Using a Network NTP Server」の手順に従います。

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 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、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 ドメイン ネーム システム サーバに接続するように 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 Firepower Management Center Getting Started Guide』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 http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html 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 Administration Guide, 7.2*』の「SNMP Polling」で説明されているように、SNMP ポーリングを使用して Management Center を監視できます。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。

（Management Center WEB インターフェイスの **[システム（System）]** > **[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、Firepower 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。
- ネットワーク管理アクセス用の [認証パスワード（Authentication Password）] フィールドを設定する場合には、強力なパスワードを使用します。

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、**[System]** > **[Configuration]** > **[Access List]** の Management Center Web インターフェイスに表示されます。『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configuring the Access List for Your System」を参照してください。

また、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、「サードパーティ データベース アクセスのブロック」を参照してください。

重要 Firepower 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 トラフィック内の送信元 IP アドレスや宛先 IP アドレスを再割り当てするために、ネットワーク アドレス変換（NAT）を使用します。Firepower 環境を保護し、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 Firepower 展開を設定する方法については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「NAT Environments」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、Management Center の初期設定を実行する場合。
- 『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Add Devices to the Firepower Management Center」の説明に従って、管理対象デバイスを Management Center に登録する場合。

管理対象デバイスへのセキュアなアクセス

Firepower 環境には、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、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。

Management Center ユーザー アクセスの強化

内部および外部ユーザー

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：ユーザがローカル 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、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 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

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）。これは内部と外部両方のユーザ アカウントで使用できます。
- SSH、シリアル、またはキーボードおよびモニタ接続を使用したコマンド ライン アクセス。これは、CLI/シェル アクセス **admin** アカウントで使用でき、外部ユーザーにも使用を許可できます。

管理権限の制限

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 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 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 （9 ページ） を参照）。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 （9 ページ）」を参照）。

（注） 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 Administration Guide, 7.2*』の「User Accounts for Management Access」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を持つユーザーは、ログイン時に Linux シェルに直接アクセスできます。 CLI またはシェルユーザーは、Linux シェルにアクセスするため、CLI **expert** コマンドを入力する追加の手順を実行する必要があります。

（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『Firepower Management Center Configuration Guide』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 Management Center にアクセスしないでください。

Management Center アクセスのタイプに関する詳細については、と、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Web Interface and CLI Access」を参照してください。

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 Management Center にログインします（ご使用の 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。（を参照してください。を参照してください）。

システムのロックダウンが完了すると、コマンド ライン クレデンシャルで Management Center にログインしているユーザがアクセスできるのは、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。

Management Center CLI の詳細については、を参照してください。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、Firepower 環境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 Management Center ユーザに許可できます。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。

[System] > **[Domains]** メニュー オプションを使用して、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。マルチテナンシーの展開に関する完全な情報は、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「」、Domains」にあります。

[System] > **[Users]** > **[Users]** を使用して、Management Center Web インターフェイスからドメイン内でのユーザー権限を割り当てます。全詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Add an Internal User at the Web Interface」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 Management Center にアクセスできます。管理者は、**[System]** > **[Users]** > **[Users]** 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。

- 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。この回数を超えるとアカウントがロックアウトされ、管理者による再アクティブ化が必要になります。
- 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。

これらの設定の詳細については、『』の「」、『』の「」、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Users」を参照してください。

管理者は、**[システム（System）]**>**[設定（Configuration）]**>**[ユーザ設定（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試行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

設定の詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Global User Configuration Settings」を参照してください。

外部ユーザ アカウントの強化

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、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 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 （6 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 Firepower 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。

Management Center ユーザ認証用に外部サーバを設定するには、**[System]** > **[Users]** > **[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 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 Firepower ユーザ ロールを LDAP ユーザまたはユーザ グループに関連付けます。
  - RADIUS を使用している場合、適切な Firepower 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 Administration Guide, 7.2*』の「Configure External Authentication」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。

Management Center でセッションタイムアウトを設定するには、**[システム（System）] > [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**：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 Administration Guide, 7.2*』の「Session Timeouts」を参照してください。

REST API アクセスの無効化

Firepower 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。Firepower の REST API の詳細については、ご使用のバージョンの『Firepower Management Center REST API Quick Start Guide』を参照してください。

デフォルトでは、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。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。Management Center Web インターフェイスで **[System] > [Configuration] > [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 Administration Guide, 7.2*』の「REST API Preferences」を参照してください。

リモート アクセスの制限

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 Firepower から SNMP サーバ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 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 [システム（System）] > [設定（Configuration）] > [アクセスリスト（Access List）] に表示されます。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Access List」を参照してください。

修復は使用しない

修復は Firepower 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。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、Management Center と Firepower の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 Firepower システム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 Administration Guide, 7.2*』の「Remediations」を参照してください。

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 Management Center の間の接続を保護することにより、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。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。

Management Center の HTTPS 証明書を設定するには、Management Center Web インターフェイスの **[システム（System）] > [設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）]** を使用します。『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「HTTPS Certificates」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）] > [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（Edit）] 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。

別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、次の権限を更新する必要があります。[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセスコントロールポリシー（Access Control Policy）] > [アクセスコントロールポリシーの変更（Modify Access Control Policy）] > [アクセスコントロールポリシーロックのオーバーライド（Override Access Control Policy Lock）]。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 Device Configuration Guide, 7.2*』の「Locking an Access Control Policy」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、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、Management Center Web インターフェイスの **[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** の下に表示されます。詳細については、『』の「」、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Back up the Management Center」を参照してください。

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。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。

Threat Defense アップグレードを元に戻す

Management Center を使用して、Threat Defense のメジャーおよびメンテナンスアップグレードを元に戻すことができます。元に戻すと、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（スナップショットとも呼ばれます）の直前の状態に戻ります。パッチ適用後に元に戻すと、パッチが削除されます。元に戻す動作は、Management Center

とデバイス間の通信が中断された場合にのみ発生します。高可用性や拡張性の展開では、すべてのユニットを同時に元に戻すと、元に戻す操作が成功する可能性が高くなります。

元に戻される設定には、Snort バージョン、デバイス固有の設定、デバイス固有の設定で使用されるオブジェクトが含まれます。元に戻されない設定には、複数のデバイスで使用できる共有ポリシーが含まれます。

アップグレードが成功した後に元に戻す必要があると思われる場合は、管理センターで **[システム（System）]** > **[更新（Updates）]** を選択して Threat Defense をアップグレードし、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを設定します。デフォルトで、このオプションは有効になっています。このオプションを有効にすることを推奨します。

復元スナップショットは、Management Center とデバイスに 30 日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。詳細については、『*Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2*』の「Revert the Upgrade」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

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。これを使用して、同じ Firepower バージョンを実行している別の Management Center に同じ設定をインポートすることができます。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、Management Center と Web ブラウザ間の通信を保護します。Management Center と Web ブラウザの間のセキュア通信 （13 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、Firepower 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、Management Center Web インターフェイスの **[System]** > **[Tools]** > **[Import/Export]** に表示されます。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「」、「Import/Export」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）]>[デバイス（Device）]>[展開の設定（Deployment Settings）]を使用して自動ロールバック設定を有効にし、接続モニター間隔を設定することをお勧めします。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 Device Configuration Guide, 7.2*』の「Edit Deployment Settings」を参照してください。

レポートの保護

Firepowerシステム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。ここで説明するすべてのレポートタイプは、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、Management CenterとWebブラウザ間の通信を保護します。（「Management CenterとWebブラウザの間のセキュア通信」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。

  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**[Overview]**>**[Reporting]**に表示されます。これらのレポートの場合、Firepowerにはローカルダウンロードに加えて2つのストレージオプションが用意されており、それぞれにセキュリティリスクがあります。

  - 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。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。

  標準レポートとリスクレポートの設計と生成に関する詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「」、「Reports」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。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、**[System]**>**[Health]**>**[Monitor]**を使用して、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の

「Health Monitor Reports for Troubleshooting」の手順を実行します。Management Center は、.tar.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。ポリシー レポートを生成するには、リポートするポリシーの管理ページにアクセスし、レポート アイコン（  ）をクリックします。レポートをサポートするポリシーの完全なリストについては、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Generating Current Policy Reports」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 Device Configuration Guide, 7.2*』の「Comparing Policies」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 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。

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。（Management Center Web インターフェイスの **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[アラート（Alerts）]** > **[アラートの作成（Create Alert）]** > **[Syslog アラートの作成（Create Syslog Alert）]**）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 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、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、Management Center Web インターフェイスから **[システム（System）]** > **[設定（Configuration）]** > **[電子メール通知（Email Notification）]** を使用して行います。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configuring a Mail Relay Host and Notification Address」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、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。

  - 『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Creating an Email Alert Response」で説明されている電子メールアラート応答。(この設定は、Management Center Web インターフェイスの **[ポリシー（Polices）]** > **[アクション（Actions）]** > **[アラート（[Alerts）]** > **[アラートの作成（Create Alert）]** > **[電子メールアラートの作成（Create Email Alert）]** を使用してこの設定を構成します。)

- 『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configuring Database Event Limits」で説明されているデータプルーニング通知。（この設定は、Management Center Web インターフェイスの **[システム（System）]** > **[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、Management Center Web インターフェイスの **[ポリシー（Polices）]** > **[アクション（Actions）]** > **[アラート（Alerts）]** > **[アラートの作成（Create Alert）]** > **[SNMP アラートの作成（Create SNMP Alert）]** で次のオプションを使用して保護できます。

  - [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。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、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。

  さらに、SNMP アクセスのアクセス リストを、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もあります。（このオプションは、**[System]** > **[Configuration]** > **[Access List]** の Management Center Web インターフェイスに表示されます。『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configure an Access List」を参照してください。

  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」を参照してください。

重要 Firepower から SNMP サーバまたは SMTP サーバ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 Administration Guide, 7.2*』の「External Alerting with Alert Response」を参照してください。

監査ログの保護

Management Center は、**[システム（System）] > [設定（Configuration）] > [監査ログ（Audit Log）]** を使用して設定されたユーザ アクティビティの読み取り専用ログを保持します。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 Administration Guide, 7.2*』の「Securely Stream Audit Logs」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、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『Firepower eStreamer Integration Guide』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、Management Center と eStreamer クライアント間の接続を設定します。この設定は、**[統合（Integrations）]>[その他の統合（Other Integrations）]> [eStreamer] > [クライアントの作成（Create Client）]** の Management Center Web インターフェイスで、eStreamer クライアントを実行中の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することによって実行します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Configuring eStreamer Client Communications」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、ファイアウォール 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。

Management Center から 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、FMC 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、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。

サードパーティ データベース アクセスのブロック

サードパーティのクライアント アプリケーションが Management Center データベースにアクセスできないことを確認します。Management Center Web インターフェイスの **[システム（System）] > [設定（Configuration）] > [外部データベースアクセス（External Database Access）]** で、[外部データベースアクセスの許可（Allow External Database Access）] チェックボックスがオフになっていることを確認します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「External Database Access Settings」を参照してください。

ログイン バナーのカスタマイズ

システム ログイン ページは、Management Center へのアクセスが許可されているユーザーと許可されていないユーザーの両方に表示される可能性があります。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。Management Center Web インターフェイスで、**[システム（System）]>[設定（Configuration）]>[ログインバナー（Login Banner）]** を使用します。詳細については、『』、『』、『*Cisco Secure Firewall Management Center Administration Guide, 7.2*』の「Login Banners」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

Firepower アイデンティティ 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、 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 Active Directory
- Linux OpenLDAP
- RADIUS

重要 LDAP、Microsoft AD、または RADIUS サーバへのセキュアな接続を Firepower 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 （11 ページ）」の情報を確認してください。

（注） Firepowerはこれらの各サーバを使用して、ユーザ 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 Device Configuration Guide, 7.2*』の「About User Identity Sources」を参照してください。

（注） Firepowerは、RADIUSサーバ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 Device Configuration Guide, 7.2*』の「VPN Overview」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

Firepowerには「レルム」と呼ばれるオブジェクトがあります。レルムは、Active Directoryサーバーまたは 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。レルム設定の詳細については、『』、『』、『*Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*』の「Create and Manage Realms」を参照してください。

（Management Center Web インターフェイスの **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[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、Management Center Web インターフェイスの **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [RADIUS サーバ 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。

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 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）] > [オブジェクト管理（Object Management）] を選択し、ナビゲーションウィンドウから [PKI] > [証明書登録（Cert Enrollment）] を選択します。
2. [証明書登録の追加（Add Cert Enrollment）] をクリックし、[CA情報（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。

Threat Defense に EST サーバー証明書を検証させたくない場合は、[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、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 Device Configuration Guide, 7.2*』の「Certificate Enrollment Object EST Options」を参照してください。

Management Center と Threat Defense のバージョン 7.0 以降では、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。7.0 より前のバージョンを実行している Threat Defense を管理する Management Center 7.0 で該当する制限をオーバーライドするには、[Weak-Cryptoの有効化（Enable Weak-Crypto）] オプションを使用できます（**[デバイス（Devices）] > [証明書（Certificates）]**）。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。FMC および FTD バージョン 7.0 以降では、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）]>[オブジェクト管理（Object Management）] を選択し、ナビゲーションウィンドウから [PKI] > [証明書登録（Cert Enrollment）] を選択します。
2. [証明書登録の追加（Add Cert Enrollment）] をクリックし、[CA情報（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 Device Configuration Guide, 7.2*』の「Adding Certificate Enrollment Objects」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

動作中、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）] > [デバイス（Device）] > [詳細設定（Advanced Settings）]**）。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 Device Configuration Guide, 7.2*』の「Configure Object Group Search」を参照してください。

サポート コンポーネントの強化

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。
- Management Center モデル 1000、1600、2000、2500、2600、4000、4500、および 4600 の場合、 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 Hardening Guide*』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。

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。