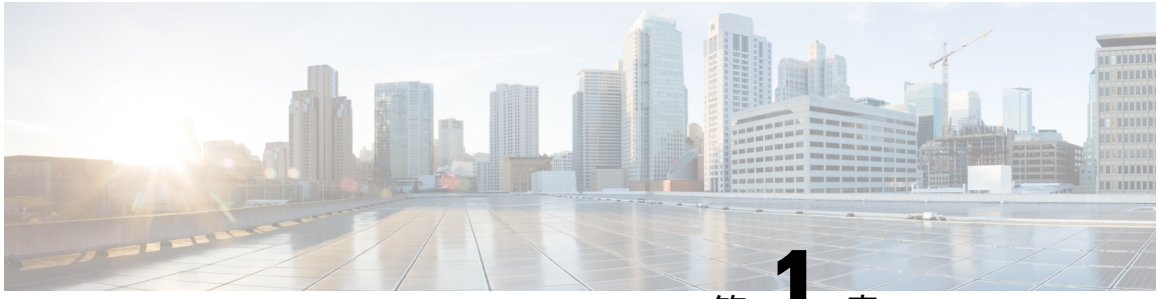
Cisco Firepower 4100/9300 FXOS 強化ガイド

初版：2019 年 5 月 10 日

最終更新：2023 年 5 月 29 日

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



第 1 章

はじめに

このドキュメントでは、4100および9300プラットフォームデバイスでCisco Firepower eXtensible Operating System（FXOS）を強化し、ネットワーク全体のセキュリティを向上させるのに役立つ情報を提供します。Firepower環境にある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 Guide to Harden ASA Firewall
- Cisco Firepower Management Center Hardening Guide, Version 6.4
- Cisco Firepower Threat Defense Hardening Guide, Version 6.4

ネットワークの3つの機能プレーン（管理、コントロール、およびデータプレーン）は、それぞれが異なる機能を提供し、それらは保護する必要があります。

管理プレーン

管理プレーンには、Cisco FXOS のプロビジョニング、メンテナンス、およびモニタリング機能をサポートするすべてのトラフィックの論理グループが含まれています。このグループのトラフィックには、HTTP/HTTPS、SSH、FTP、簡易ネットワーク管理プロトコル（SNMP）、Syslog、TACACS+、リモート認証ダイヤルイン ユーザー サービス（RADIUS）、および DNS が含まれます。管理プレーントラフィックは、常にローカル Cisco FXOS を宛先とします。

コントロール プレーン

コントロールプレーンには、すべてのスイッチング、シグナリング、リンク状態、および Link Layer Discovery Protocol（LLDP）や Link Aggregation Control Protocol（LACP）などのネットワークおよびインターフェイスの状態を作成および維持するために使用されるその他の制御プロトコルの論理グループが含まれています。コントロールプレーントラフィックの宛先は常にローカル Cisco FXOS デバイスです。

データ プレーン

データプレーンには、ネットワークでサポートされているホスト、クライアント、サーバー、およびアプリケーションで生成され、それらのデバイス間で送受信される顧客のアプリケーション トラフィックの論理グループが含まれます。

このドキュメントは、次の 3 つのセクションで構成されています。

- ネットワーク運用の保護

- 管理プレーンの強化
- User Management

このドキュメントのほとんどは、Cisco FXOSデバイスの安全な設定に焦点を当てていますが、設定だけではネットワークを完全に保護することはできません。ネットワークで使用されている操作手順、およびネットワークを管理する人は、基礎となるデバイスの設定と同じくらいセキュリティに貢献します。使用可能で適切な場合、このドキュメントには、実装された場合にCisco FXOS 展開を保護するのに役立つ推奨事項が含まれています。

- セキュリティ認定準拠 （2 ページ）

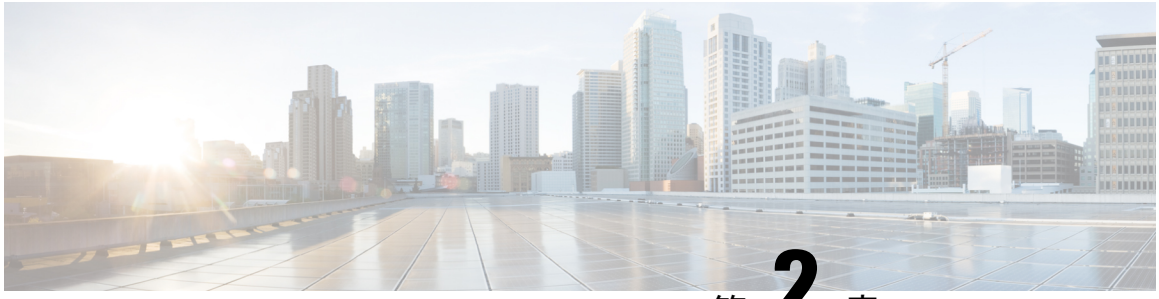
セキュリティ認定準拠

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ることに注意してください。

認定固有のガイダンスドキュメントに従って設定されている場合、Firepower System は次の認定基準への準拠をサポートします。

- 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 Firepower 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。



第 2 章

ネットワーク運用の保護

ネットワーク運用の保護は重要なトピックです。このドキュメントのほとんどは、FXOS を実行する Firepower 4100/9300 デバイスの安全な設定に焦点を当てていますが、設定だけではネットワークを完全に保護することはできません。ネットワークで使用されている操作手順、およびネットワークを管理する人は、基礎となるデバイスの設定と同じくらいセキュリティに貢献します。

次のセクションには、FXOS 管理者が実施することをお勧めする運用上の推奨事項が含まれています。これらのセクションは、ネットワーク運用の特定の重要な領域を強調しており、包括的なものではありません。

Cisco セキュリティアドバイザリの監視

Cisco Product Security Incident Response Team（PSIRT）は、シスコ製品のセキュリティ関連問題に関して、シスコ セキュリティ アドバイザリと呼ばれる通知を作成し、維持しています。セキュリティアドバイザリは、http://www.cisco.com/go/psirt で入手できます。

Cisco PSIRT 脆弱性レポートについては、「Cisco Security Vulnerability Policy 」を参照してください。

安全なシステムを維持するために、Cisco FXOS 管理者は、シスコ セキュリティ アドバイザリで伝達される情報に注意する必要があります。脆弱性がネットワークにもたらす可能性のある脅威を評価する前に、脆弱性に関する詳細な知識が必要です。この評価プロセスのサポートについては、「Risk Triage for Security Vulnerability Announcements」を参照してください。

FXOS の最新バージョンへの更新

重要なセキュリティの更新は、FXOS の新しいプラットフォーム バンドル リリースごとに含まれています。できるだけ早くFXOSシステムを利用可能な最新バージョンに更新することをお勧めします。

さまざまな構成でのFXOSのサポートされている互換性とアップグレードパスの詳細については、Cisco.com の『*Cisco Firepower 4100/9300 FXOS Compatibility*』ガイドおよび『*Cisco Firepower 4100/9300 Upgrade Guide*』を参照してください。

ログイン前バナーのカスタマイズ

ユーザーが Firepower Chassis Manager または FXOS CLI にログインする前に、FXOS がユーザーに表示するメッセージを指定できます。強化の観点から、このメッセージは不正アクセスを防止するために使用する必要があります。

次の CLI の例では、FXOS Chassis Manager および FXOS CLI のログイン前バナーを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
 You must have explicit, authorized permission to access or configure this device.
 Unauthorized attempts and actions to access or use this system may result in civil
and/or
criminal penalties.
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

コモンクライテリアまたは FIPS モードの有効化

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、コモンクライテリアまたはFIPSモードを有効化して、1 つの設定で複数の強化変更を適用することができます。組織がセキュリティ認定コンプライアンス標準に準拠する必要がない場合でも、FXOS の FIPS またはコモンクライテリアモードを有効にすることができますが、これによりデバイスで互換性の問題が発生する可能性があることに注意してください。

コモンクライテリアまたは FIPS モードを有効にするオプションは、Firepower Chassis Manager Web インターフェイスの **[プラットフォーム設定（Platform Settings）]** > **[FIPS/コモンクライテリア（FIPS/Common Criteria）]**モードの下に表示されます。

（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、コモンクライテリアまたは FIPS 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。
- FIPS、コモンクライテリア、またはその両方が有効になっている場合は、デバイスアクセスに FIPS 準拠ツールを使用します。

ネットワーク タイム プロトコル（NTP）の保護

信頼された Network Time Protocol（NTP）サーバーを使用して、Firepower 4100/9300 FXOS デバイスとその関連サーバーのシステム時刻を同期させることを強く推奨します。

FXOS の NTP を有効にするには、最初に NTP キー ID とキー値を生成してから、FXOS Chassis Manager で次のワークフローを使用して NTP サーバーを FXOS シャーシに追加する必要があります。**Platform Settings > Set Time Source > Use NTP Server**。NTP をさらに強化するには、NTP サーバー認証を構成します。

FXOS の NTP サーバーおよび NTP サーバー認証を設定する方法の詳細については、『*Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*』の「Platform Settings」の章の「Setting the Date and Time Using NTP」トピックを参照してください。

（注）

- 有効にすると、NTP認証機能はFXOSに関連付けられた設定済みのすべてのサーバーでグローバルに機能します。
- NTP サーバー認証では SHA1 のみがサポートされます。
- サーバを認証するには、キー ID とキー値が必要です。キー ID は、メッセージ ダイジェストのコンピューティング時に、使用するキー値をクライアントとサーバーの両方に指示するために使用されます。キー値は、nip-keygen を使用して導出される固定値です。

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。

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。シスコでは次のドキュメントでガイドラインを提供しています。https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html。

認証、認可、アカウンティングの活用

認証、認可、アカウンティング（AAA）フレームワークは、ネットワークデバイスへのインタラクティブアクセスを保護するのに重要です。AAA フレームワークは、ネットワークのニーズに基づいて調整できる高度に設定可能な環境を提供します。

RADIUS と TACACS+ は両方とも FXOS システムでサポートされています。TACACS+ は、ユーザー名とパスワードの両方を含む TCP ペイロード全体を暗号化します。RADIUS はパスワードのみを暗号化します。さらに、TACACS+ はコマンド認可を提供しますが、RADIUS は認証とアカウンティングのみを提供します。したがって、認証セキュリティを最大化するために TACACS+ を使用することをお勧めします。

さらに、ユーザー認証に LDAP を使用できます。LDAP 認証交換を暗号化するには、CLI オプションを使用して SSL を使用します。

```
Firepower /security/ldap/server # set ssl yes
```

AAA の設定方法の詳細と完全な手順については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Platform Settings」の章の「Configuring AAA」セクションを参照してください。

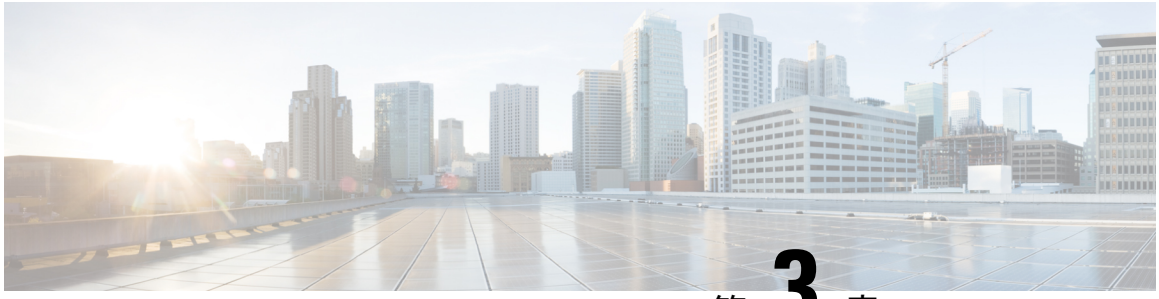
セキュアなプロトコルの使用

Cisco FXOS は、機密性の高いネットワーク管理データを伝送するために多くのプロトコルを使用します。可能な限り、安全なプロトコルを使用する必要があります。安全なプロトコルの選択には、認証データと管理情報の両方が暗号化されるように、Telnet の代わりに SSH を使用することが含まれます。さらに、構成データをコピーするときは、安全なファイル転送プロトコルを使用する必要があります。たとえば、FTP または TFTP の代わりに Secure Copy Protocol（SCP）を使用します。安全なプロトコルの使用方法の詳細については、このドキュメントの「管理プレーン （7 ページ）」セクションを参照してください。

構成管理

構成管理は、構成の変更が提案、レビュー、承認、および展開されるプロセスです。

Cisco FXOS デバイスの設定には、ユーザー名、パスワード、アクセスコントロールリスト（ACL）の内容など、機密性の高い多くの詳細が含まれています。Cisco FXOS デバイス設定のアーカイブに使用されるリポジトリは保護する必要があり、アクセスはアクセスを必要とするロールと機能のみに制限する必要があります。この情報への安全でないアクセスは、ネットワーク全体のセキュリティを損なう可能性があります。



第 3 章

管理プレーン

管理プレーンは、ネットワークの管理目標を達成する機能で構成されています。この目標には、SSHを使用するインタラクティブ管理セッションや、SNMPによる統計情報収集が含まれます。ネットワークデバイスのセキュリティを検討する場合は、管理プレーンを保護することが重要です。セキュリティインシデントによって管理プレーンの機能が弱体化すると、ネットワークを回復または安定化できなくなる可能性があります。

次のセクションでは、管理プレーンの強化に役立つ Cisco FXOS で利用可能なセキュリティ機能と設定について詳しく説明します。

管理プレーンの強化

管理プレーンにより、デバイスのアクセス、設定、および管理と、デバイスの動作やデバイスが導入されているネットワークのモニタリングを行うことができます。管理プレーンは、これらの機能の操作のためにトラフィックを送受信します。コントロールプレーンの操作は管理プレーンの操作に直接影響するため、デバイスの管理プレーンとコントロールプレーンの両方を保護する必要があります。次のリストには、管理プレーンで使用されるプロトコルが含まれています。

- SNMP

- [Telnet]
- SSH
- SFTP
- [FTP]
- TFTP
- [HTTP/HTTPS]
- Secure Copy Protocol（SCP）
- TACACS+
- RADIUS
- LDAP
- ネットワーク タイム プロトコル（NTP）
- Syslog

管理者は、セキュリティインシデントの際に管理プレーンとコントロールプレーンの整合性を確保するための対策を講じる必要があります。これらのプレーンの1つが悪用されると、すべてのプレーンが侵害される可能性があります。

管理セッションの制御と暗号化

対話型管理セッション中に情報が開示される可能性があるため、悪意のあるユーザーが送信されているデータを読み取れないようにトラフィックを暗号化する必要があります。トラフィックを暗号化すると、デバイスへの安全なリモートアクセス接続が可能になります。管理セッションのトラフィックがネットワーク経由でプレーンテキストで送信される場合、デバイスとネットワークに関する機密情報を不正に取得される危険性があります。FXOS では、次のプロトコルがサポートされています。

- SSH
- TLS
- HTTPS
- SNMP
- LDAP
- Telnet

（注） Telnet は安全なプロトコルではないため、FXOS の管理者は使用しないことをお勧めします。

次の節で、管理セッションプロトコルの詳細な強化設定オプションについて説明します。

トラスト ID 証明書のインストール

初期設定後に、自己署名 SSL 証明書が FXOS シャーシ Web アプリケーションで使用するために生成されます。その証明書は自己署名であるため、クライアントブラウザが自動的に信頼することはありません。新しいクライアントブラウザで FXOS シャーシ Web インターフェイスに初めてアクセスするときに、ブラウザは SSL 警告をスローして、ユーザーが FXOS シャーシにアクセスする前に証明書を受け入れることを要求します。FXOS CLI を使用して証明書署名要求（CSR）を生成し、FXOS シャーシで使用する結果の ID 証明書をインストールするには、以下の手順を使用できます。この ID 証明書により、クライアント ブラウザは接続を信頼し、警告なしで Web インターフェイスを起動できるようになります。

信頼できる ID 証明書をインストールする完全な手順については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Install a Trusted Identity Certificate」トピックを参照してください。

証明書、キー リング、トラスト ポイント

HTTPS は、公開キー インフラストラクチャ（PKI）を使用してクライアントのブラウザと Firepower 9300 シャーシ などの 2 つのデバイス間でセキュアな通信を確立します。

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。通常、長いキーは短いキーよりもより安全です。FXOS では最初に 2048 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

証明書

セキュアな通信を準備するには、まず2つのデバイスがそれぞれのデジタル証明書を交換します。証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。暗号化された通信をサポートするために、デバイスは独自のキーペアと独自の自己署名証明書を生成できます。リモートユーザが自己署名証明書を提示するデバイスに接続する

場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。デフォルトでは、FXOS にはデフォルトのキーリングからの公開キーを含む組み込みの自己署名証明書が含まれます。

トラスト ポイント

FXOS に強力な認証を提供するために、デバイスの ID を証明する信頼できるソース（つまり、トラストポイント）からサードパーティ証明書を取得し、インストールできます。サードパーティ証明書は、発行元トラスト ポイント（ルート認証局（CA）、中間 CA、またはルート CA につながるトラスト チェーンの一部となるトラスト アンカーのいずれか）によって署名されます。新しい証明書を取得するには、FXOS で証明書要求を生成し、トラストポイントに要求を送信する必要があります。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

HTTPS の設定

次のワークフローを使用して、FXOS シャーシで HTTPS を設定して強化します。

1. キーリングを作成します（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Creating a Key Ring」トピックを参照してください）。
2. キーリングの証明書要求を作成します（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Creating a Certificate Request for a Key Ring with Advanced Options」トピックを参照してください）。
3. 信頼できるポイントを作成します（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Creating a Trusted Point」トピックを参照してください）。
4. 証明書をキーリングにインポートします（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Importing a Certificate Into a Key Ring」トピックを参照してください）。

次の追加オプションを使用して、HTTPS を強化します。

- ドメインで使用される暗号スイートセキュリティのレベルを指定します（**set https cipher-suite-mode**）。**strong** または **custom** の値をお勧めします。custom を選択した場合は、ドメインに対してカスタムレベルの暗号スイートセキュリティを指定します（**set https cipher-suite** *cipher-suite-spec-string*）。
- 証明書失効リスト検査を有効にします。

SSH の設定

TCP ポート 22 を使用してデフォルトで有効になっている SSHv2 を使用することをお勧めします。サーバーとクライアントで有効にできる次の SSH 強化設定オプションに注意してください。

RSA キー強度（set ssh-server host-key rsa/set ssh-client host-key rsa）

モジュラス値（ビット単位）は、1024 ～ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

暗号化アルゴリズム（set ssh-server encrypt-algorithm/set ssh-client encrypt-algorithm）

FXOS では、次の暗号化アルゴリズムがサポートされています。

```
3des-cbc    3DES  CBC
aes128-cbc  AES128 CBC
aes128-ctr  AES128 CTR
aes192-cbc  AES192 CBC
aes192-ctr  AES192 CTR
aes256-cbc  AES256 CBC
aes256-ctr  AES256 CTR
```

（注） 3des-cbc はコモンクライテリアに準拠していません。

Diffie-Hellman キー交換アルゴリズム（set ssh-server kex-algorithm/set ssh-client kex-algorithm）

DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホスト キーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

FXOS では、次の DH アルゴリズムがサポートされています。

```
diffie-hellman-group14-sha1  Diffie-Hellman Group14 SHA1
```

サーバーおよびクライアント MAC アルゴリズム（set ssh-server mac-algorithm/set ssh-client mac-algorithm）

FXOS では、次の MAC アルゴリズムがサポートされています。

```
hmac-sha1      Hmac SHA1
hmac-sha2-256  HMAC SHA2 256
hmac-sha2-512  HMAC SHA2 512
```

キー再生成のボリューム制限（set ssh-server rekey-limit volume/set ssh-client rekey-limit volume）

接続で許可されるトラフィックの量を KB 単位で決定します。この値を超えると、FXOS はセッションを切断します。

キー再生成の時間制限（set ssh-server rekey-limit time/set ssh-client rekey-limit time）

SSHセッションがアイドル状態を続けられる時間の上限を分単位で決定します。この値を超えると、FXOS はセッションを切断します。

厳密なホストキーチェックの設定（set ssh-client stricthostkeycheck）

SSH ホストキーチェックを制御します。

- **enable**：FXOS が認識するホストファイルにそのホストキーがまだ存在しない場合、接続は拒否されます。システムスコープまたはサービススコープの FXOS CLI コマンド **enter ssh-host** を使用して、手動でホストを追加する必要があります。
- **prompt**：シャーシにまだ保存されていないホストキーを許可または拒否するように求められます。
- **disable**：（デフォルト）シャーシは過去に保存されたことがないホストキーを自動的に許可します。

FXOS シャーシでの SSH の設定に関する完全な手順については、『*Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide*』および『*Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*』の「プラットフォーム設定」の章を参照してください。

SNMP の保護

簡易ネットワーク管理プロトコル（SNMP）を適切に保護して、ネットワークデータとこのデータが通過するネットワークデバイスの両方の機密性、整合性、および可用性を保護することが重要です。SNMP は、ネットワークデバイスの正常性に関する豊富な情報を提供します。この情報は、このデータを利用してネットワークに対して攻撃を実行しようとする悪意のあるユーザーから保護する必要があります。

SNMPv3 では、セキュリティモデルとセキュリティ レベルの両方が提供されています。セキュリティモデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティモデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP コミュニティストリングは、デバイス上の SNMP データへの読み取り専用アクセスと読み取り/書き込みアクセスの両方を制限するために FXOS シャーシに適用されるパスワードです。これらのコミュニティストリングは、すべてのパスワードと同様に、単純なものにならないように慎重に選択する必要があります。コミュニティストリングは、定期的にネットワークセキュリティのポリシーに合わせて変更する必要があります。たとえば、ネットワーク管理者がロールを変更する場合や会社を退社する際には、コミュニティストリングを変更する必要があります。

サポートされているレベルの SNMP セキュリティモデルおよびレベルの詳細については、『*Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*』の「Platform Settings」の章にある「Configure SNMP」セクションを参照してください。

Secure Syslog

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。syslogサービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログ用の保護された長期ストレージを提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

ロギング情報をリモート Syslog サーバーに送信すると、ネットワークデバイス全体のネットワークイベントとセキュリティイベントをより効果的に関連付けて監査することができます。syslog メッセージはクリアテキストで送信されることに注意してください。このため、ネットワークが管理トラフィックに提供する保護（暗号化や帯域外アクセスなど）は、syslog トラフィックを含むように拡張する必要があります。信頼できないネットワーク上で syslog トラフィックがクリアテキストで送信されないようにするために、IPSec セキュアチャネルを設定できます。IPSec では、エンドツーエンドのデータ暗号化や、パブリックネットワーク内を移動するデータパケットに対する認証サービスを提供できます。

FXOS シャーシで syslog を設定する方法の詳細については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Platform Settings」の章の「Configuring Syslog」セクションを参照してください。IPSec の設定方法の詳細については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Configure IPSec Secure Channel」トピックを参照してください。

IP アクセスリストの設定

デフォルトでは、FXOS シャーシはローカル Web サーバーへのすべてのアクセスを拒否します。各プロトコルで許可されるホストまたはサブネットの IP アドレスを使用して、IP アクセスリストを構成する必要があります。

IP アクセスリストは、次のプロトコルをサポートします。

- HTTPS
- SSH
- SNMP

IP アドレス（v4 または v6）の各リストで、最大 100 個の異なるサブネットを各サービスに対して設定できます。サブネットを 0、プレフィックスを 0 と指定すると、サービスに無制限にアクセスできるようになります。

FXOS シャーシでの IP アクセスリストの設定に関する詳細および完全な手順については、『Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide』および『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Platform Settings」の章の「Configure the IP Access List」トピックを参照してください。

IPSec セキュア チャネルの設定

Firepower 4100/9300 シャーシ上で IPSec を設定して、エンドツーエンドのデータ暗号化や、パブリックネットワーク内を移動するデータパケットに対する認証サービスを提供します。

（注） FIPS モードで IPSec セキュア チャネルを使用している場合は、IPSec ピアで RFC 7427 をサポートしている必要があります。

FXOS シャーシに IPSec セキュアチャネルを設定する方法の詳細については、『*Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*』の「Security Certifications Compliance」の章にある「Configure IPSec Secure Channel」トピックを参照してください。

証明書失効リストのチェックについて

証明書失効リスト（CRL）チェック モードを、IPSec、HTTPS およびセキュアな LDAP 接続で厳格または緩和に設定できます。

FXOS は、動的な CRL 情報を示すダイナミック（非スタティック）CRL 情報を、X.509 証明書の CDP 情報から収集します。システム管理によってスタティック CRL 情報を手動でダウンロードします。この情報は、FXOS システムのローカルな CRL 情報を示します。FXOS では、ダイナミック CRL 情報は証明書チェーン内で現在処理中の証明書に対してのみ処理されます。スタティック CRL は、ピアの証明書チェーン全体に適用されます。

セキュアな IPSec、LDAP および HTTPS 接続の証明書失効のチェックを有効または無効にする手順については、「IPSec セキュアチャネルの設定」、「LDAP プロバイダーの作成」、および「HTTPS の設定」を参照してください。

（注）
- 証明書失効のチェック モードが厳格に設定されている場合、スタティック CRL はピア証明書チェーンのレベルが 1 以上のときにのみ適用されます（たとえば、ピア証明書チェーンにルート CA 証明書およびルート CA によって署名されたピア証明書のみが含まれているとき）。
- IPSec に対してスタティック CRL を設定している場合、[Authority Key Identifier (authkey)] フィールドはインポートされた CRL ファイルに存在している必要があります。そうでない場合、IPSec はそれを無効と見なします。
- スタティック CRL は、同じ発行元からのダイナミック CRL より優先されます。FXOS でピア証明書を検証するときに、同じ発行者の有効な（決定済みの）スタティック CRL があれば、ピア証明書の CDP は無視されます。
- 次のシナリオでは、デフォルトで厳格な CRL チェックが有効になっています。
  - 新しく作成したセキュアな LDAP プロバイダー接続、IPSec 接続、またはクライアント証明書エントリ
  - 新しく展開した FXOS シャーシマネージャ（FXOS 2.3.1.x 以降の初期開始バージョンで展開）

次の表は、証明書失効リストのチェックの設定と証明書の検証に応じた接続の結果を示しています。

表 *1*：厳格（ローカル スタティック *CRL* なし）に設定した証明書失効のチェック モード

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A	○
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンで CDP が 1 つ欠落している	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）
有効な署名付きピア証明書チェーンの 1 つの CDP CRL が空です	接続に成功	接続に成功	接続に失敗（syslog メッセージあり）
ピア証明書チェーンの CDP がダウンロードできません	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）
証明書に CDP はありますが、CDP サーバがダウンしています	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）
証明書に CDP があり、サーバはアップしており、CRL は CDP にありますが、CRL に無効な署名があります	接続に失敗（syslog メッセージあり）	ピア証明書：接続に失敗（syslog メッセージあり） 中間 CA：接続に失敗	接続に失敗（syslog メッセージあり）

表 *2:* 厳格（ローカル スタティック *CRL* あり）に設定した証明書失効のチェック モード

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンで CDP が 1 つ欠落している（証明書チェーン レベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの CDP をダウンロードできません（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP がありますが、CDP サーバがダウンしています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗（syslog メッセージあり）	CDP と組み合わせて使用すると、接続に成功します CDP がなければ、接続に失敗し、syslog メッセージが表示されます

表 *3:* 緩和（ローカル スタティック *CRL* なし）に設定した証明書失効のチェック モード

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーン内の CDP のチェック	完全な証明書チェーン	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A	○

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンで CDP が 1 つ欠落している	接続に成功	接続に成功	接続に失敗（syslog メッセージあり）
有効な署名付きピア証明書チェーンの 1 つの CDP CRL が空です	接続に成功	接続に成功	接続に成功
ピア証明書チェーンの CDP がダウンロードできません	接続に成功	接続に成功	接続に成功
証明書に CDP はありますが、CDP サーバがダウンしています	接続に成功	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります	接続に成功	接続に成功	接続に成功

表 *4:* 緩和（ローカル スタティック *CRL* あり）に設定した証明書失効のチェック モード

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーン内の CDP のチェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	○	N/A

ローカル スタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンで CDP が 1 つ欠落している（証明書チェーン レベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンの CDP をダウンロードできません（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP がありますが、CDP サーバがダウンしています（証明書チェーンのレベルは 1）	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL が CDP にありますが、CRL に無効な署名があります（証明書チェーンのレベルは 1）	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗（syslog メッセージあり）	CDP と組み合わせて使用すると、接続に成功します CDP がなければ、接続に失敗し、syslog メッセージが表示されます

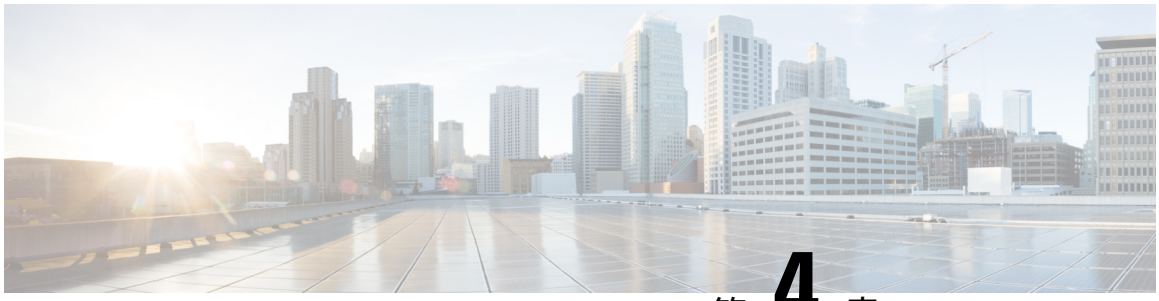
トラストポイントのスタティック CRL の設定

失効した証明書は、証明書失効リスト（CRL）で保持されます。クライアントアプリケーションは、CRL を使用してサーバの認証を確認します。サーバ アプリケーションは CRL を使用して、信頼されなくなったクライアントアプリケーションからのアクセス要求を許可または拒否します。

証明書失効リスト（CRL）情報を使用して、Firepower 4100/9300 シャーシがピア証明書を検証するように設定できます。

証明書失効リスト情報を使用してピア証明書を検証するように設定したら、証明書を検証するために新しい CRL が 1 ～ 24 時間ごとに使用されるように、CRL を定期的にダウンロードするようにシステムを設定することもできます。

トラストポイントの証明書失効リストを設定する方法の詳細については、『*Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*』の「Security Certifications Compliance」の章にある「Configure Static CRL for a Trustpoint」トピックを参照してください。



第 4 章

ロールベース アクセス コントロールの保護

ユーザーロールには、そのユーザーがシステムで実行できることを定義する特権が割り当てられます。システムには、次のユーザ ロールが用意されています。

管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

読み取り専用

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

操作

NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ（syslog サーバとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

AAA アドミニストレータ

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

FXOS Chassis Manager Web インターフェイスまたは FXOS CLI を使用して、システムの各ユーザーアカウントに次の設定を構成できます。

- [ユーザーロール（User Role）]：ユーザーアカウントに割り当てる権限を表すロール。

  すべてのユーザはデフォルトでは読み取り専用ロールが割り当てられます。このロールは選択解除できません。複数のロールを割り当てるには、**Ctrl** を押したまま、目的のロールをクリックします。

- アカウントの有効期限日

- [アカウントステータス（Account Status）]：ステータスが [アクティブ（Active）] に設定されている場合、ユーザーはログイン ID とパスワードを使用して Firepower Chassis Manager と FXOS CLI にログインできます。

ローカルで認証されたアカウントで最大限のセキュリティを確保するには、暗号化されたセッションに SSH を構成します。

- パスワード管理 （22 ページ）
- ローカル認証されたユーザーアカウントの強化 （22 ページ）
- リモート認証されたユーザーアカウントの強化 （23 ページ）

パスワード管理

パスワードはリソースまたはデバイスへのアクセスを制御し、管理者は要求を認証するためのパスワードを定義します。FXOS がリソースまたはデバイスへのアクセス要求を受信すると、要求はパスワードと ID の検証のチャレンジが行われ、結果に基づいてアクセスが許可、拒否、または制限されます。セキュリティのベストプラクティスでは、パスワードは LDAP、TACACS+、または RADIUS 認証サーバーで管理する必要があります。ただし、LDAP、TACACS+、または RADIUS サービスが失敗した場合は、アクセス用にローカルに設定されたパスワードが引き続き必要です。デバイスは、NTP キーや SNMP コミュニティストリングなど、他のパスワード情報をその設定内に持つこともできます。

ローカル認証されたユーザーアカウントの強化

個々の内部ユーザーロールを設定する場合、管理者アカウントユーザーは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。

- ロックアウト前にユーザーに許可されるログイン試行の最大回数を設定します（set max-login-attempts）。この回数を超えると、指定した時間だけ Firepower 4100/9300 シャーシからロックアウトされることになります
- ログイン試行の最高回数を超えた後、ユーザーがシステムからロックアウトされる時間を指定します（set user-account-unlock-time）
- パスワード長の最小値を適用します（set min-password-length）
- ローカル認証されたユーザーが、新しく作成したパスワードを変更する前に待機する最小時間数を指定します（set no-change-interval）
- ローカルユーザーアカウントが有効な日数を設定します（set expiration）
- 強力なパスワードを要求します（set enforce-strong-password yes）
- 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（create role）

リモート認証されたユーザーアカウントの強化

リモート認証されたユーザ アカウントとは、LDAP、RADIUS、または TACACS+ を通じて認証されたユーザ アカウントのことです。リモート認証では、最大 16 の TACACS+ サーバー、16 の RADIUS サーバー、および 16 の LDAP プロバイダー（合計 48 のプロバイダー）が許可されます。

AAA は、コンピュータ リソースへのアクセスを制御し、ポリシーを使用し、使用率を評価することでサービス課金に必要な情報を提供する、一連のサービスです。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

ユーザーがローカルユーザーアカウントとリモートユーザーアカウントを同時に保持する場合、ローカルユーザーアカウントで定義されたロールはリモートユーザーアカウントに保持された値を上書きします。

TACACS+は、FXOS シャーシがリモート AAA サーバーに対して管理ユーザーを認証するために使用できる認証プロトコルです。これらの管理ユーザーは、SSH、HTTPS、Telnet、または HTTP を介して FXOS シャーシにアクセスできます。FXOS シャーシにアクセスするときは、最大限のセキュリティのために SSH をお勧めします。多数の認証方法により、セキュリティが強化されています。

TACACS+認証（より一般的にはAAA認証）では、ネットワーク管理者ごとに個別のユーザーアカウントを使用できます。単一の共有パスワードに依存しない場合、ネットワークのセキュリティが向上し、責任が強化されます。

RADIUS は、TACACS+ と似た目的のプロトコルですが、ネットワーク経由で送信されるパスワードのみを暗号化します。一方、TACACS+ は、ユーザー名とパスワードの両方を含む TCP ペイロード全体を暗号化します。このため、AAA サーバーで TACACS+ がサポートされている場合は、RADIUS ではなく TACACS+ を使用することをお勧めします。

LDAP は、Microsoft Active Directory などのディレクトリサービスにアクセスするためのクライアント サーバー プロトコルです。LDAP では、クライアントとサーバー間のセキュリティは必要ありません。ただし、SSL を使用することにより、LDAP はクライアントとサーバー間のユーザーセッションを暗号化できます。これにより、ネットワーク経由で LDAP トランザクションにより転送されるすべての情報が安全に保たれます。このため、TLS よりも LDAP を使用することを強くお勧めします。

FXOS シャーシで RADIUS、TACAS+、および LDAP を設定する方法の詳細と詳細な手順については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Platform Settings」の章の「Configuring AAA」セクションを参照してください。

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。