



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 \(1 ページ\)](#)
- [管理セッションの制御と暗号化 \(2 ページ\)](#)
- [トラスト ID 証明書のインストール \(3 ページ\)](#)
- [証明書、キーリング、トラストポイント \(3 ページ\)](#)
- [HTTPS の設定 \(4 ページ\)](#)
- [SSH の設定 \(5 ページ\)](#)
- [SNMP の保護 \(6 ページ\)](#)
- [Secure Syslog \(7 ページ\)](#)
- [IP アクセスリストの設定 \(7 ページ\)](#)
- [IPSec セキュア チャネルの設定 \(8 ページ\)](#)
- [証明書失効リストのチェックについて \(8 ページ\)](#)
- [トラストポイントのスタティック CRL の設定 \(13 ページ\)](#)

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、通常の場合は 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 チャンネルの設定

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 チャン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 チャン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 チャンネルの設定](#)」、「[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 ファイルに存在する必要があります。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、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、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、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。

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。