



セキュリティ認定準拠

- [セキュリティ認定コンプライアンス \(1 ページ\)](#)
- [SSH ホスト キーの生成 \(2 ページ\)](#)
- [IPSec セキュア チャネルの設定 \(3 ページ\)](#)
- [トラストポイントのスタティック CRL の設定 \(9 ページ\)](#)
- [証明書失効リストのチェックについて \(10 ページ\)](#)
- [CRL 定期ダウンロードの設定 \(15 ページ\)](#)
- [LDAP キー リング証明書の設定 \(17 ページ\)](#)
- [クライアント証明書認証の有効化 \(18 ページ\)](#)

セキュリティ認定コンプライアンス

米国連邦政府機関は、米国防総省およびグローバル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。Firepower 4100/9300 シャーシは、これらのセキュリティ認証基準のいくつかに準拠しています。

これらの基準に準拠する機能を有効にするステップについては、次のトピックを参照してください。

- [FIPS モードの有効化](#)
- [コモンクライテリア モードの有効化](#)
- [IPSec セキュア チャネルの設定 \(3 ページ\)](#)
- [トラストポイントのスタティック CRL の設定 \(9 ページ\)](#)
- [証明書失効リストのチェックについて \(10 ページ\)](#)
- [CRL 定期ダウンロードの設定 \(15 ページ\)](#)
- [NTP 認証の設定： NTP を使用した日付と時刻の設定](#)
- [LDAP キー リング証明書の設定 \(17 ページ\)](#)
- [IP アクセスリストの設定](#)

- [クライアント証明書認証の有効化 \(18 ページ\)](#)
- [最小パスワード長チェックの設定](#)
- [ログイン試行の最大回数の設定](#)



(注) これらのトピックは Firepower 4100/9300 シャーシ における認定準拠の有効化についてのみ説明していることに注意してください。Firepower 4100/9300 シャーシ で認定準拠を有効にしても、接続された論理デバイスにまでそのコンプライアンスは自動的に伝搬されません。

SSH ホスト キーの生成

FXOS リリース 2.0.1 より以前は、デバイスの初期設定時に作成した既存の SSH ホスト キーが 1024 ビットにハードコードされていました。FIPS およびコモンクライテリア認定に準拠するには、この古いホスト キーを破棄して新しいホスト キーを生成する必要があります。詳細については、[FIPS モードの有効化](#) または [コモンクライテリア モードの有効化](#) を参照してください。

古い SSH ホスト キーを破壊し、新しい証明書準拠キーを生成するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、サービス モードに入ります。

```
scope system
scope services
```

ステップ 2 SSH ホスト キーを削除します。

```
delete ssh-server host-key
```

ステップ 3 設定を確定します。

```
commit-buffer
```

ステップ 4 SSH ホスト キーのサイズを 2048 ビットに設定します。

```
set ssh-server host-key rsa 2048
```

ステップ 5 設定をコミットします。

```
commit-buffer
```

ステップ 6 新しい SSH ホスト キーを作成します。

```
create ssh-server host-key
```

commit-buffer

ステップ 7 新しいホスト キーのサイズを確認します。

```
show ssh-server host-key
```

```
ホスト キー サイズ : 2048
```

IPSec セキュア チャネルの設定

IPSec は Internet Engineering Task Force (IETF) で開発されたオープン規格のフレームワークです。IP ネットワークを介した、認証された信頼性の高いセキュアな通信を実現します。IPSec セキュリティサービスは、次の機能を提供します。

- コネクションレス型の完全性：受信トラフィックが変更されていないことを保証します。
- データ発信元の認証：トラフィックが正当な当事者によって送信されることを保証します。
- 機密性（暗号化）：ユーザーのトラフィックが許可されていない当事者によって調査されないことを保証します。
- アクセス制御：リソースの不正使用を防止します。



(注) IPSec 接続は FXOS からのみ開始できます。FXOS は着信 IPSec 接続要求を受け入れません。

IPSec トンネルとは、FXOS がピア間に確立する SA のセットのことです。SA とは、機密データに適用するプロトコルとアルゴリズムを指定するものであり、ピアが使用するキー関連情報も指定します。IPsec SA は、ユーザ トラフィックの実際の伝送を制御します。SA は単方向ですが、通常ペア（着信と発信）で確立されます。

Firepower Chassis Manager の IPSec には次の 2 つのモードがあります。

トランスポート モード

IP ヘッダー、IPSec ヘッダー、TCP ヘッダー、データ

トンネル モード

新しい IP ヘッダー、IPSec ヘッダー、元の IP ヘッダー、TCP ヘッダー、データ

IPSec の動作は、次の 5 つの主要なステップに分けられます。

1. **トラフィックの選択**：IPSec ポリシーに一致する対象トラフィックが IKE プロセスを開始します。たとえば、送信元/宛先ホスト IP またはサブネットを使用してトラフィックを選択できます。また、`admin` コマンドを使用して IKE プロセスをトリガーすることもできます。

2. IKE フェーズ 1 : IPSec ピアを認証し、セキュアなチャンネルをセットアップして IKE 交換を有効にします。
3. IKE フェーズ 2 : SA をネゴシエートして IPSec トンネルをセットアップします。SA は、セキュリティアソシエーション (Security Association) の略であり、データトラフィックを保護するために使用されるセキュリティサービスを記述する IPSec エンドポイント間の関係です。
4. データの転送 : データパケットは、SA に保存されているパラメータとキーを使用して、暗号化され、IPSec ヘッダーにカプセル化されます。
5. IPSec トンネルの終了 : IPSec SA は、削除またはタイムアウトによって終了します。

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、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。このオプションは、システムのコモンクライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、[セキュリティ認定コンプライアンス \(1 ページ\)](#) を参照してください。



- (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。
 - IKE 接続と SA 接続の間で一致する暗号キー強度の適用を設定する場合は、次のようになります (次の手順で sa-strength-enforcement を yes に設定します)。

SA の適用を有効にする場合	<p>IKE によりネゴシエートされたキー サイズが、ESP によりネゴシエートされたキー サイズより小さい場合、接続は失敗します。</p> <p>IKE によりネゴシエートされたキー サイズが、ESP によりネゴシエートされたキー サイズより大きいか等しい場合、SA 適用検査にパスして、接続は成功します。</p>
SA の適用を無効にした場合	SA 適用検査にパスし、接続は成功します。

IPSec セキュア チャンネルを設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 キー リングを作成します。

```
enter keyring ssp
```

```
! create certreq subject-name subject-name ip ip
```

ステップ 3 関連する証明書要求情報を入力します。

```
enter certreq
```

ステップ 4 国を設定します。

```
set country country
```

ステップ 5 DNS を設定します。

```
set dns dns
```

ステップ 6 電子メールを設定します。

```
set e-mail 電子メール
```

ステップ 7 IP 情報を設定します。

```
set ip ip-address
```

```
set ipv6 ipv6
```

ステップ 8 ローカリティを設定します。

```
set locality locality
```

ステップ 9 組織名を設定します。

```
set org-name org-name
```

ステップ 10 組織ユニット名を設定します。

```
set org-unit-name org-unit-name
```

ステップ 11 パスワードを設定します。

```
! set password
```

ステップ 12 状態を設定します。

```
set state state
```

ステップ 13 certreq のサブジェクト名を設定します。

```
set subject-name subject-name
```

ステップ 14 終了します。

```
exit
```

ステップ 15 モジュラスを設定します。

```
set modulus modulus
```

ステップ 16 証明書要求の再生成を設定します。

```
set regenerate { yes / no }
```

ステップ 17 トラストポイントを設定します。

```
set trustpoint interca
```

ステップ 18 終了します。

```
exit
```

ステップ 19 新しく作成されたトラストポイントを入力します。

```
enter trustpoint interca
```

ステップ 20 証明書署名要求を作成します。

```
set certchain
```

例 :

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2l2Y28xDTALBgNV
BAsMBFNUQlUxOzA1BgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3BAC3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJhFw0yNjEyMDYxOTMzNTJhMHAxOzA1BgNVBAYTA1VT
MQswCQYDVQQIDAJDQTEMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDAxNjBzENMA5G
A1UECwwEU1RCVTELMakGA1UEAwWCQ0ExGjAYBgkqhkiG9w0BCQEWc3NzcEBzc3Au
bmV0MIICljANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJd7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBoz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLdkss1nO
xP9+1+Lc690V18/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FIRHDJjPcSN
Yw1g/gcR2F7QUKRyGkckJKXDX2QliGYsctSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgl2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMODwBdeMG3EihxEEOPD0
Fdu0HrTM51vwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVI/QdPdbWShjflE/fP2Wj01PqXywQydzymVvgE
wEzaoFg+mlGjM0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32yS1
lla6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZIO4jcSIvidizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAaAObgTB/MC8GA1UdHwQoMcywJKAioCCG
Hmh0dHA6Ly8xOTUuMTY4LjQuMjkvcM9vdGNhLmNyBDAAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWVWxpo
pFahRhZyxVZ10DHKlzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DipBQ29yweCbUke9qiHKA0IbnvAxoroHwMbld
94LrJcggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqXuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/fluJ+s/VJSVZWK4tAWvR7wl
QngCKRjW6FYpzeyNBctiJ07wO+Wt4e3KhJjJdYvA9hFixWcVGDFr6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVp1bRUO20G3oRTmSx
8iLbjN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2l2Y28xDTALBgNV
BAsMBFNUQlUxOzA1BgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3BAC3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTM0NTRaMHwxOzA1BgNVBAYTA1VT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQLDAduZXdzdGJ1
```

```
MRMwEQYDVQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGluGdGVyTEtY2EubmV0MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegjhLANsodxuAumhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BX13DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfGQUq11stkIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLII
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFP LCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNLolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoidPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLIZgJ5txSaVUIgrVCJaf6/jrRRWoRJwt
AzvzYq12dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAANBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAggh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybyS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRfFEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKS YrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWoc3lZ1Oi
CC2tFvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66l8DG9uUzIWyD79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NwPwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFYeoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Twt
SjGAPHgeROzyTFDixCeiaROIgdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjkKIJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
```

ステップ 21 証明書署名要求を表示します。

show certreq

例 :

```
Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):

-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTELMakGA1UEBhMCVVMxMzA5BjBhNVBAgMAkNBMD8wDAYDVR0T
DANTSkMxMjE2OC40LjI5L2luZGVybyS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/
U1AwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3it0laoxPbfE
p/TKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClk/tsIxsPkV0
```

```
6OduZYXk2bnsLW56tNk3uzOIT2Q0FcZ1ET66C8fyKWTmrvZjDjkMm2nDFsPIX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzA1BgqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEArRBolnxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZI03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMI9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rmeSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWN06
DT3u0xImiPR1sqWljpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----
```

ステップ 22 IPSec モードに入ります。

scope ipsec

ステップ 23 ログ冗長レベルを設定します。

set log-level log_level

ステップ 24 IPSec 接続を作成し、入力します。

enter connection connection_name

ステップ 25 IPSec モードをトンネリングまたは伝送のために設定します。

set mode tunnel_or_transport

ステップ 26 ローカル IP アドレスを設定します。

set local-addr ip_address

ステップ 27 リモート IP アドレスを設定します。

set remote-addr ip_address

ステップ 28 トンネルモードを使用している場合、リモートサブネットを設定します。

set remote-subnet ip/mask

ステップ 29 (任意) リモート ID を設定します。

set remote-ike-ident remote_identity_name

ステップ 30 キーリング名を設定します。

set keyring-name name

ステップ 31 (任意) キーリングパスワードを設定します。

set keyring-passwd passphrase

ステップ 32 (任意) IKE-SA の有効期間を分単位で設定します。

set ike-rekey-time minutes

minutes 値には、60 ~ 1440 の範囲内の任意の整数を設定できます。

ステップ 33 (任意) 子の SA の有効期間を分単位 (30 ~ 480 分) で設定します。

set esp-rekey-time minutes

minutes 値には、30 ~ 480 の範囲内の任意の整数を設定できます。

ステップ 34 (任意) 初期接続中に実行する再送信シーケンスの番号を設定します。

set keyringtries retry_number

retry_number 値には、1 ~ 5 の範囲の任意の整数を指定できます。

ステップ 35 (任意) 証明書失効リスト検査を、有効または無効にします。

set revoke-policy { relaxed | strict }

ステップ 36 接続を有効にします。

set admin-state enable

ステップ 37 接続をリロードします。

reload-conns

システムはすべての接続を停止し、リロードします。すべての接続の再確立が試行されます。

ステップ 38 (任意) 既存のトラストポイント名を IPsec に追加します。

create authority trustpoint_name

ステップ 39 IKE 接続と SA 接続との間の、対応する暗号キー強度の適用を設定します。

set sa-strength-enforcement yes_or_no

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。このオプションは、システムのコモンクライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、[セキュリティ認定コンプライアンス \(1 ページ\)](#) を参照してください。

CRL 情報を使用してピア証明書を検証するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ2 トラストポイント モードに入ります。

```
scope trustpoint trustname
```

ステップ3 取り消しモードに入ります。

```
scope revoke
```

ステップ4 CRL ファイルをダウンロードします。

```
import crl protocol://user_id@CA_or_CRL_issuer_IP/tmp/DoDCA1CRL1.crl
```

ステップ5 (任意) CRL 情報のインポート プロセスのステータスを表示します。

```
show import-task detail
```

ステップ6 CRL 専用の、証明書取り消し方法を設定します。

```
set certrevoke method {crl}
```

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

CRL 定期ダウンロードの設定

システムを、CRL を定期的にダウンロードして、証明書の検証に新しい CRL を 1～24 時間ごとに使用するように設定できます。

この機能とともに、次のプロトコルとインターフェイスを使用できます。

- FTP

- SCP
- SFTP
- TFTP
- USB



- (注)
- SCEP および OCSP はサポートされません。
 - CRL ごとに設定できるのは1つの定期ダウンロードのみです。
 - トラストポイントごとにサポートされるのは1つの CRL です。



- (注) 期間は1時間間隔でのみ設定できます。

CRL 定期ダウンロードを設定するには、次の手順を実行します。

始める前に

Firepower 4100/9300 シャーシが、ピア証明書を (CRL) 情報を使用して検証するように設定されていることを確認します。詳細については、[トラストポイントのスタティック CRL の設定 \(9 ページ\)](#) を参照してください。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

```
scope security
```

ステップ 2 トラストポイント モードに入ります。

```
scope trustpoint
```

ステップ 3 取り消しモードに入ります。

```
scope revoke
```

ステップ 4 取り消し設定を編集します。

```
sh config
```

ステップ 5 優先設定を設定します。

例 :

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
```



```
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

ステップ 6 設定ファイルを終了します。

exit

ステップ 7 (任意) 新しい CRL をダウンロードして、新しい設定をテストします。

例 :

```
Firepower-chassis /security/trustpoint/revoke # sh import-task
```

Import task:

File Name	Protocol	Server	Userid	
rootCA.crl	Scp	182.23.33.113	0	MyName
				Downloading

LDAP キー リング証明書の設定

Firepower 4100/9300 シャーシ上で TLS 接続をサポートする、セキュアな LDAP クライアント キー リング証明書を設定できます。このオプションは、システムのコモン クライテリア認定への準拠を取得するために提示される数の 1 つです。詳細については、[セキュリティ認定コンプライアンス \(1 ページ\)](#) を参照してください。



(注) コモン クライテリア モードを有効にする場合は、SSL が有効になっている必要があります。さらにキー リング証明書を作成するために、サーバ DNS 情報を使用する必要があります。

SSL を LDAP サーバ エントリに対して有効にすると、接続の形成時にキー リング情報が参照されて確認されます。

LDAP サーバ情報は、セキュア LDAP 接続 (SSL 使用可能) 用の、CC モードの DNS 情報である必要があります。

セキュア LDAP クライアントのキー リング証明書を設定するには、次の手順を実行します。

手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

scope security

ステップ 2 LDAP モードに入ります。

scope ldap

ステップ3 LDAP サーバ モードに入ります。

```
enter server {server_ip/server_dns}
```

ステップ4 LDAP キー リングを設定します。

```
set keyring keyring_name
```

ステップ5 設定をコミットします。

```
commit-buffer
```

クライアント証明書認証の有効化

HTTPS アクセスのユーザを認証するために、システムにクライアント証明書を LDAP と一緒に使用させることができます。Firepower 4100/9300 シャーシ上でのデフォルトの認証設定は、認証ベースです。



(注) 証明書認証が有効である場合、これは HTTPS に許可されている唯一の認証形式です。

証明書失効検査は、FXOS 2.1.1 リリースのクライアント証明書認証機能ではサポートされていません。

この機能を使用するには、クライアント証明書が次の要件を満たしている必要があります。

- ユーザ名が X509 属性 [サブジェクト代替名 : 電子メール (Subject Alternative Name - Email)] に含まれている必要があります。
- クライアント証明書は、その証明書をスーパーバイザ上のトラストポイントにインポートしているルート CA により署名されている必要があります。

手順

ステップ1 FXOS CLI から、サービス モードに入ります。

```
scope system
```

```
scope services
```

ステップ2 (任意) HTTPS 認証のオプションを表示します。

```
set https auth-type
```

例 :

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

ステップ 3 HTTPS 認証をクライアントベースに設定します。

```
set https auth-type cert-auth
```

ステップ 4 設定をコミットします。

```
commit-buffer
```
