



# PKI での証明書の許可および失効の設定

• PKI での証明書の許可および失効の設定 (1 ページ)

## PKI での証明書の許可および失効の設定

### 証明書の許可および失効に関する前提条件

#### PKI ストラテジの計画



**ヒント** 実際の証明書の展開を開始する前に、全体の PKI ストラテジを計画することを強く推奨します。

ユーザーまたはネットワーク管理者が次の作業を完了した後に、許可および失効が発生します。

- 認証局 (CA) の設定。
- ピア デバイスの CA への登録。
- ピアツーピア通信に使用される (IP セキュリティ (IPsec) またはセキュア ソケット レイヤ (SSL) などの) プロトコルの確認および設定。

許可および失効に固有の情報をピアデバイス証明書に含めなければならない場合があるため、ピア デバイスを登録する前に、設定する許可および失効ストラテジを決定する必要があります。

#### 高可用性

ハイ アベイラビリティのため、IPsec 保護された Stream Control Transmission Protocol (SCTP) はアクティブ ルータとスタンバイ ルータの両方で設定する必要があります。同期を機能させるには、SCTP を設定した後に、証明書サーバーの冗長性モードを ACTIVE/STANDBY に設定する必要があります。

## 証明書の許可および失効に関する制約事項

- Cisco IOS リリースに応じて、Lightweight Directory Access Protocol (LDAP) がサポートされます。

## 証明書の許可および失効に関する情報

### PKI の許可

PKI 認証では、許可を行いません。多くの場合、一元的に管理されるソリューションが必要ですが、現在の許可用のソリューションは、設定対象のルータに固有です。

それによって証明書を特定の作業に対して許可し、その他の作業に対しては許可しない、と定義できる標準的なメカニズムはありません。アプリケーションが証明書ベースの許可情報を認識する場合、この許可情報を証明書自体に取り込みます。このソリューションでは、許可情報をリアルタイムで更新するための簡単なメカニズムを提供していないため、証明書に組み込まれた固有の許可情報を認識するように各アプリケーションに強制します。

証明書ベースの ACL メカニズムがトラストポイント認証の一部として設定される場合、該当アプリケーションは、この許可情報を判別する役割を担うことはなく、どのアプリケーションに対して証明書を許可するのか指定できません。ルータ上の証明書ベースの ACL は、大きくなりすぎて管理できないことがあります。また、外部サーバーから証明書ベースの ACL 指示を取得する方が有利です。

許可の問題にリアルタイムで対処する現在のソリューションでは、新しいプロトコルの指定や新しいサーバーの構築（それとともに管理およびデータ配布などの関連作業）が必要になります。

### 証明書ステータスのための PKI と AAA サーバーの統合

PKI を認証、許可、アカウントिंग (AAA) サーバーと統合することにより、既存の AAA インフラストラクチャを活用する代替オンライン証明書ステータスソリューションを実現します。証明書を適切な許可レベルで AAA データベースに一覧表示できます。PKI-AAA を明示的にサポートしないコンポーネントでは、デフォルト ラベルの「all」を指定すると、AAA サーバーからの許可が可能になります。また、AAA データベースのラベルが「none」の場合、指定された証明書が有効でないことを示します（アプリケーションラベルが欠如していることと同じですが、「none」は完全性および明確性のために含まれます）。アプリケーション コンポーネントが PKI-AAA をサポートしている場合、コンポーネントを直接指定できる場合があります。たとえば、アプリケーション コンポーネントを「ipsec」、「ssl」、または「osp」に指定できます（ipsec = IP セキュリティ、ssl = セキュア ソケット レイヤ、および osp = Open Settlement Protocol）。



(注) 現在、アプリケーション ラベルの指定をサポートするアプリケーション コンポーネントはありません。

- AAA サーバーにアクセスしたときに、時間遅延が生じる場合があります。AAA サーバーを利用できない場合、許可は失敗します。

## RADIUS または TACACS+ : AAA サーバー プロトコルの選択

AAA サーバーは、RADIUS または TACACS+ プロトコルと連動するように設定できます。PKI 統合用に AAA サーバーを設定する場合、許可に必要な RADIUS または TACACS 属性を設定する必要があります。

RADIUS プロトコルが使われている場合は、AAA サーバーのユーザー名に設定するパスワードを「cisco」に設定する必要があります。証明書の検証が認証を行い、AAA データベースは許可の目的だけに使用されているので、このパスワードは受け入れ可能です。TACACS プロトコルを使用する場合、TACACS では認証が不要な許可をサポートする（認証にパスワードを使用）ので、AAA サーバーのユーザー名に対して設定されるパスワードとは無関係です。

さらに、TACACS を使用する場合は、AAA サーバーに PKI サービスを追加する必要があります。カスタム属性「cert-application=all」が、PKI サービスの特定のユーザーまたはユーザーグループに追加され、特定のユーザー名が許可されます。

## PKI と AAA サーバー統合用の属性値ペア

次の表に、AAA サーバーと PKI との統合を設定する場合に使用される属性値 (AV) ペアを示します (表に示す値は、可能な値であることに注意してください)。AV ペアはクライアント設定と一致する必要があります。AV ペアが一致しない場合、ピア証明書は許可されません。



- (注) 場合によっては、ユーザーは、他のすべてのユーザーの AV ペアとは異なる AV ペアを持つことができます。その場合、ユーザーごとに一意のユーザー名が必要になります。(authorization username コマンド内に) all パラメータを設定すると、証明書のサブジェクト名全体を許可ユーザー名として使用するよう指定できます。

表 1: 一致する必要がある AV ペア

AV ペア	値
cisco-avpair=pki:cert-application=all	有効な値は、[all] および [none] です。

AV ペア	値
cisco-avpair=pki:cert-trustpoint=msca	<p>この値は、Cisco IOS コマンドライン インターフェイス (CLI) 設定のトラストポイント ラベルです。</p> <p>(注) cert-trustpoint AV ペアの指定は、通常任意です。このペアが指定されている場合、Cisco IOS ルータクエリーは、一致するラベルを持つ証明書トラストポイントから受信する必要があり、認証された証明書は、指定された証明書シリアル番号を持っている必要があります。</p>
cisco-avpair=pki:cert-serial=16318DB7000100001671	<p>この値は証明書のシリアル番号です。</p> <p>(注) cert-serial AV ペアの指定は、通常任意です。このペアが指定されている場合、Cisco IOS ルータクエリーは、一致するラベルを持つ証明書トラストポイントから受信する必要があり、認証された証明書は、指定された証明書シリアル番号を持っている必要があります。</p>
cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003	<p>cert-lifetime-end AV ペアは、証明書で指示された期間を越えた証明書のライフタイムを人為的に延長する場合に使用できます。cert-lifetime-end AV ペアを使用する場合は、cert-trustpoint および cert-serial AV ペアも指定する必要があります。この値は、時/分/月/日/年の形式と一致する必要があります。</p> <p>(注) 月を表す最初の 3 文字 (Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec) だけが使用されます。月を表す文字として 4 文字以上入力すると、残りの文字は無視されます (たとえば、Janxxxx)。</p>

## CRL または OCSP サーバー：証明書失効メカニズムの選択

証明書が適切に署名された証明書として有効になった後、証明書失効方法を実行して、証明書が発行元 CA によって無効にされていないことを確認します。Cisco IOS ソフトウェアは、2 つの失効メカニズムとして証明書失効リスト (CRL) と Online Certificate Status Protocol (OCSP) をサポートします。Cisco IOS ソフトウェアも、証明書のチェックのために AAA 統合をサポートしますが、これには追加の許可機能が含まれます。PKI と AAA 証明書の許可とステータス確認に関する詳細については、「証明書ステータスのための PKI と AAA サーバーの統合」を参照してください。

次の項では、各失効メカニズムの機能方法について説明します。

### CRL とは

CRL とは、失効した証明書のリストです。CRL は、証明書を発行した CA によって作成され、デジタル署名されます。CRL には、各証明書の発行日と失効日が含まれています。

CA は、新しい CRL を定期的に、あるいは CA が責任を負う証明書が失効したときに公開します。デフォルトでは、現在キャッシュされている CRL が失効すると、新しい CRL がダウンロードされます。管理者は、CRL がルータのメモリにキャッシュされる時間を設定したり、CRL キャッシングを完全にディセーブルにしたりできます。CRL キャッシング設定は、トラストポイントに関連付けられたすべての CRL に適用されます。

CRL が失効すると、ルータはキャッシュから CRL を削除します。証明書が検証用に表示されると、新しい CRL がダウンロードされます。ただし、検証中の証明書を記載した新しいバージョンの CRL がサーバー上にあるにもかかわらず、ルータがキャッシュ内の CRL を使用し続ける場合、ルータは証明書が失効したことを認識しません。証明書は拒否されるはずのもので、失効チェックに合格します。

CA は、証明書を発行すると、証明書にその CRL 配布ポイント (CDP) を含めることができます。Cisco IOS クライアントデバイスは、CDP を使用して適切な CRL を見つけ、ロードします。Cisco IOS クライアントは複数の CDP をサポートしますが、Cisco IOS CA は現在 1 つの CDP しかサポートしません。ただし、サードパーティベンダー製の CA には、証明書ごとに複数の CDP または異なる CDP をサポートするものがあります。CDP が証明書に指定されていない場合、クライアントデバイスは、デフォルトの Simple Certificate Enrollment Protocol (SCEP) 方式を使用して CRL を取得します (CDP の場所は、**cdp-url** コマンドを使用して指定できます)。

CRL を実装する際は、次の設計上の注意事項を考慮する必要があります。

- CRL ライフタイムとセキュリティアソシエーション (SA) およびインターネットキー交換 (IKE) ライフタイム
- CRL ライフタイムにより、CA が CRL の更新を発行する時間間隔が決まります。デフォルト CRL ライフタイム値は 168 時間 (1 週間) です。これは、**lifetime crl** コマンドで変更できます。
- CDP のこの方式により、CRL の取得方法が決まり、この方式として、HTTP、Lightweight Directory Access Protocol (LDAP)、SCEP、または TFTP を選択できます。最も一般的に使用されている方式は、HTTP、TFTP、および LDAP です。Cisco IOS ソフトウェアでは、

SCEP にデフォルト設定されていますが、CRL を使用して大容量のインストールを実行する場合、HTTP CDP を推奨します。HTTP では高いスケーラビリティを実現できるからです。

- CDP のこの場所は、CRL の取得先を決定します。たとえば、サーバーおよび CRL の取得先となるファイルパスを指定できます。

### 失効チェック中にすべての CDP を照会

CDP サーバが要求に返答しない場合、Cisco IOS ソフトウェアはエラーを報告し、その結果、ピアの証明書が拒否されることがあります。証明書に複数の CDP がある場合、証明書が拒否されないようにするために、Cisco IOS ソフトウェアは、証明書に表示されている順序で CDP を使用しようと試みます。ルータは、それぞれの CDP URL またはディレクトリ指定を使用して CRL を取得しようと試みます。ある CDP を使用してエラーが発生すると、次の CDP を使用して試行します。



**ヒント** Cisco IOS ソフトウェアは、指示された CDP のいずれかから CRL を取得するためにあらゆる試行を行いますが、CDP 応答の遅延によりアプリケーションのタイムアウトを避けるために、HTTP CDP サーバを高速の冗長 HTTP サーバと併用することを推奨します。

### OCSP とは

OCSP は、証明書の有効性を判別するために使用されるオンラインのメカニズムであり、失効メカニズムとして次のような柔軟性を備えています。

- OCSP では、証明書ステータスをリアルタイムでチェックできます。
- OCSP を使用すると、ネットワーク管理者は、中央 OCSP サーバを指定でき、これにより、ネットワーク内のすべてのデバイスにサービスを提供できます。
- また、OCSP により、ネットワーク管理者は、クライアント証明書ごと、またはクライアント証明書のグループごとに複数の OCSP サーバを柔軟に指定できます。
- OCSP サーバの検証は通常、ルート CA 証明書または有効な下位 CA 証明書に基づいて実行されますが、外部の CA 証明書または自己署名証明書を使用できるように設定することもできます。外部の CA 証明書または自己署名証明書を使用すると、代替の PKI 階層から OCSP サーバ証明書を発行し、有効にできます。

ネットワーク管理者は、さまざまな CA サーバから CRL を収集し、更新するように OCSP サーバを設定できます。ネットワーク内のデバイスは、OCSP サーバに依存して、ピアごとに CRL を取得してキャッシュすることなく証明書ステータスをチェックできます。ピアは、証明書の失効ステータスをチェックする必要がある場合、OCSP 要求に関して疑わしい証明書のシリアル番号およびオプションの固有識別情報（ナンズ）を含む OCSP サーバにクエリーを送信します。OCSP サーバは、CRL のコピーを保持して、CA がその証明書を無効として記載しているかどうか判別します。次に、サーバは、ナンズを含むピアに応答します。応答のナンズが OCSP サーバからピアによって送信された元のナンズと一致しない場合、応答は

無効と見なされ、証明書の検証が失敗します。OCSP サーバーとピア間の対話での帯域幅の消費量は、ほとんどの場合、CRL ダウンロードより少なくなります。

OCSP サーバーが CRL を使用する場合は、CRL 時間の制約事項が適用されます。つまり、追加の証明書失効情報を含む CRL によって新しい CRL が発行されていても、まだ有効な CRL が OCSP サーバーで使用されることがあります。CRL 情報を定期的にダウンロードするデバイスが少なくなっているため、CRL ライフタイム値を小さくするか、CRL をキャッシュしないように OCSP サーバーを設定できます。詳細は、OCSP サーバーのマニュアルを参照してください。



- (注) OCSP の複数応答処理：応答パケットの OCSP レスポンダからの複数の OCSP 単一応答の処理はサポートされています。このデバッグログメッセージに加えて、次のデバッグログメッセージが表示されます。
- CRYPTO\_PKI : OCSP 応答の単一応答の数 : 1 (この値は応答の数に応じて変化します)。

### OCSP サーバーを使用する場合

PKI に次のいずれかの特性がある場合、CRL よりも OCSP の方が適している場合があります。

- リアルタイムの証明書失効ステータスが必要。CRL が定期的にしか更新されず、必ずしも最新の CRL がクライアント デバイスでキャッシュされていない場合があります。たとえば、最新の CRL がまだクライアントにキャッシュされておらず、また、新たに無効にされた証明書がチェック中の場合は、無効にされた証明書が失効チェックに合格します。
- 無効にされた大量の証明書または複数の CRL があります。大きな CRL をキャッシュすると、Cisco IOS メモリの大部分が消費されてしまい、他のプロセスに使用できるリソースが減少することがあります。
- CRL が頻繁に失効するため、CDP は大量の CRL を処理します。

### 許可または失効用に証明書ベースの ACL を使用する場合

証明書には、指定された処理の実行をデバイスまたはユーザーが許可されているかどうかの判別に使用されるフィールドがいくつか含まれています。

証明書ベース ACL はデバイス上に設定されるため、大量の ACL を十分にスケーリングしません。ただし、証明書ベースの ACL では、特定のデバイスの動作を非常に細かく制御できます。また、証明書ベース ACL は追加機能で活用され、失効、許可、またはトラストポイントなどの PKI コンポーネントを使用するタイミングを判別するのに役立ちます。証明書ベース ACL は全般的なメカニズムを提供しており、このメカニズムによりユーザーは、許可または追加処理に対して有効になっている特定の証明書または証明書のグループを選択できます。

証明書ベース ACL では、証明書内の 1 つ以上のフィールドおよび指定された各フィールドで許可される値を指定します。証明書内でチェックする必要があるフィールドと、それらのフィールドで認められる値または認められない値を指定できます。

フィールドと値との比較には、6つの論理テスト（Equal（等しい）、Notequal（等しくない）、Contains（含む）、Less than（未満）、Does not contain（含まない）、Greater than or equal（以上））を使用できます。1つの証明書ベース ACL で複数のフィールドを指定した場合、その ACL と一致するには、ACL 内のすべてのフィールド条件に合致しなければなりません。同じ ACL 内で、同じフィールドを複数回指定できます。複数の ACL を指定できます。一致するものが見つかるか、または ACL の処理がすべて完了するまで、各 ACL が順に処理されます。

## 証明書ベース ACL を使用した失効チェックの無視

証明書ベース ACL を設定して、有効なピアの失効チェックおよび失効した証明書を無視するようルータに指示できます。したがって、指定基準を満たす証明書は、証明書の有効期間にかかわらず受け入れることができます。また、証明書が指定基準を満たしている場合は失効チェックを実行する必要がなくなります。AAA サーバーとの通信が証明書で保護される場合にも、証明書ベース ACL を使用して失効チェックを無視できます。

### 失効リストの無視

トラストポイントが特定の証明書を除いて CRL を適用できるようにするには、**skip revocation-check** キーワードを指定して **match certificate** コマンドを入力します。このような適用は、スポークツースポークの直接接続も可能なハブアンドスポーク設定に最も便利です。純粋なハブアンドスポーク設定では、すべてのスポークはハブだけに接続するので、CRL チェックはハブ上だけで済みます。スポークが別のスポークと直接通信する場合、ネイバーピア証明書に対して、各スポーク上で CRL を要求する代わりに、**skip revocation-check** キーワードを指定して **match certificate** コマンドを使用できます。

### 失効した証明書の無視

失効した証明書を無視するようにルータを設定するには、**allow expired-certificate** キーワードを指定して **match certificate** コマンドを入力します。このコマンドには、次のような目的があります。

- このコマンドは、ピアの証明書が失効した場合にピアが新しい証明書を取得するまで、失効した証明書を「許可する」ために使用できます。
- ルータクロックがまだ正しい時間に設定されていない場合、クロックが設定されるまで、ピアの証明書はまだ有効ではないものとして表示されます。このコマンドは、ルータクロックが未設定であっても、ピアの証明書を許可する場合に使用できます。



(注) ネットワークタイムプロトコル (NTP) が IPSec 接続だけで（通常、ハブアンドスポーク設定のハブによって）利用可能な場合は、ルータクロックを絶対に設定できません。ハブの証明書がまだ有効でないため、ハブへのトンネルを「アップ」状態にできません。

- 「失効」とは、失効している証明書またはまだ有効ではない証明書の総称です。証明書には、開始時刻と終了時刻が指定されます。ACL を目的とした、失効証明書は、ルータの現在時刻が証明書で指定された開始および終了時刻の範囲外の証明書です。



### 証明書の AAA チェックのスキップ

AAA サーバーとの通信が証明書で保護され、証明書の AAA チェックをスキップする場合は、**skip authorization-check** キーワードを指定して **match certificate** コマンドを使用します。たとえば、すべての AAA トラフィックがバーチャルプライベートネットワーク (VPN) トンネルを通過するように設定され、このトンネルが証明書で保護されている場合は、**skip authorization-check** キーワードを指定して **match certificate** コマンドを使用すると、証明書チェックをスキップしてトンネルを確立できます。

AAA サーバーとの PKI 統合が設定されると、**match certificate** コマンドと **skip authorization-check** キーワードを設定する必要があります。



- (注) AAA サーバーが IPSec 接続によってのみ使用可能な場合は、IPSec 接続が確立されるまで AAA サーバーとは通信できません。AAA サーバーの証明書がまだ有効でないため、IPSec 接続を「アップ」状態にできません。

## PKI 証明書チェーンの検証

証明書チェーンにより、ピア証明書からルート CA 証明書までの、一連の信頼できる証明書を確立します。階層型 PKI 内では、登録されているすべてのピアが信頼できるルート CA 証明書または共通の下位 CA を共有している場合、証明書を相互に検証できます。各 CA が 1 つのラストポイントに対応します。

証明書チェーンをピアから受信すると、最初の信頼できる証明書またはラストポイントに到達するまで、証明書チェーンパスのデフォルト処理が続けられます。管理者は証明書チェーンが、すべての証明書（下位 CA 証明書を含む）で処理されるレベルを設定できます。

証明書チェーンの処理レベルを設定すると、信頼できる証明書の再認証、信頼できる証明書チェーンの延長、および欠落のある証明書チェーンの補完が可能になります。

### 信頼できる証明書の再認証

このデフォルト動作でルータは、チェーンを検証する前に、ピアによって送信された証明書チェーンから任意の信頼できる証明書を削除します。管理者は証明書チェーンパス処理を設定して、チェーン検証の前にすでに信頼されている CA 証明書をルータが削除しないようにできます。そのため、チェーン内のすべての証明書は現在のセッションに対して再度認証されます。

### 信頼できる証明書チェーンの延長

このデフォルト動作でルータは、ピアによって送信された証明書チェーンに欠落している証明書がある場合、その信頼できる証明書を使用して証明書チェーンを延長します。ルータが検証するのは、ピアによって送信されたチェーンの証明書だけです。管理者は証明書チェーンパス処理を設定して、ピアの証明書チェーンの証明書およびルータの信頼できる証明書を、指定したポイントに対して有効にできます。

### 証明書チェーンの欠落の補完

管理者は証明書チェーン処理を設定して、設定済みの Cisco IOS トラストポイント階層に欠落がある場合、ピアによって送信された証明書を使用して証明書のセットを有効にできます。



(注) 親検証を要求するようにトラストポイントが設定され、ピアが完全な証明書チェーンを提示しない場合、欠落を補完できないため証明書チェーンは拒否され、無効になります。



(注) 親検証を要求するようにトラストポイントが設定されていて、設定済みの親トラストポイントがない場合は、設定エラーです。発生する証明書チェーンの欠落を補完できず、下位 CA 証明書を有効にできません。この証明書チェーンは無効です。

## PKI に対して証明書の許可および失効を設定する方法

### AAA サーバーとの PKI 統合の設定

ピアによって提出された証明書から AAA ユーザー名を生成し、証明書内で AAA データベース ユーザー名の作成に使用するフィールドを指定するには、次の作業を実行します。



(注) **authorization username** コマンドでサブジェクト名として **all** キーワードを使用する際に、次の制約事項を考慮する必要があります。

- 一部の AAA サーバーでは、ユーザー名の長さが制限されます（たとえば、64 文字まで）。その結果、証明書の全体のサブジェクト名は、サーバーの制約条件より長くできません。
- 一部の AAA サーバーでは、ユーザー名に使用できる文字セットが制限されます（たとえば、スペース ( ) および等号 (=) を使用できない場合があります）。このような文字セットの制限がある AAA サーバーでは、**all** キーワードを使用できません。
- トラストポイント設定の **subject-name** コマンドは、必ずしも最終の AAA サブジェクト名とは限りません。証明書要求に完全修飾ドメイン名 (FQDN)、シリアル番号、またはルータの IP アドレスが含まれている場合は、発行された証明書のサブジェクト名フィールドにもこれらのコンポーネントが含まれます。コンポーネントをオフにするには、**fqdn**、**serial-number**、および **ip-address** の各コマンドに **none** キーワードを使用します。
- CA サーバーが証明書を発行すると、CA サーバーは、要求したサブジェクト名フィールドを変更することがあります。たとえば、一部のベンダーの CA サーバーが要求したサブジェクト名の相対識別名 (RDN) を CN、OU、O、L、ST、および C に切り替えます。ただし、別の CA サーバーは、設定した LDAP ディレクトリルート (O=cisco.com など) を要求したサブジェクト名の最後に追加する場合があります。
- 証明書の表示用に選択するツールによっては、サブジェクト名の RDN の印刷順序が異なることがあります。Cisco IOS ソフトウェアでは、重要度が最低の RDN を先頭に表示しますが、Open Source Secure Socket Layer (OpenSSL) などの、他のソフトウェアでは、重要度が最高の RDN を先頭に表示します。したがって、完全な識別名 (DN) (サブジェクト名) を持つ AAA サーバーを対応するユーザー名として設定する場合は、Cisco IOS ソフトウェアスタイル (つまり、重要度が最低の RDN を先頭に表示) が使用されていることを確認してください。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization network listname [method]**
5. **crypto pki trustpoint name**
6. **enrollment [mode] [ retry period minutes] [ retry count number] url url [pem]**
7. **revocation-check method**
8. **exit**
9. **authorization username subjectname subjectname**
10. **authorization list listname**
11. **tacacs server server-name**
12. **address {ipv4 | ipv6} ip-address**
13. **key string**

## 14. end

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>aaa new-model</b> 例： Device(config)# <b>aaa new-model</b>	AAA アクセスコントロールモデルをイネーブルにします。
ステップ 4	<b>aaa authorization network listname [method]</b> 例： Device(config)# <b>aaa authorization network maxaaa group tacacs+</b>	ネットワークへのユーザー アクセスを制限するパラメータを設定します。  • <b>method</b> : <b>group radius</b> 、 <b>group tacacs+</b> 、または <b>group group-name</b> のいずれか。
ステップ 5	<b>crypto pki trustpoint name</b> 例： Device(config)# <b>crypto pki trustpoint msca</b>	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	<b>enrollment [mode] [retry period minutes] [retry count number] url url [pem]</b> 例： Device(ca-trustpoint)# <b>enrollment url http://caserver.myexample.com</b>  または Device(ca-trustpoint)# <b>enrollment url http://[2001:DB8:1:1::1]:80</b>	CA の次の登録パラメータを指定します。  • (任意) CA システムが登録局 (RA) を提供する場合、 <b>mode</b> キーワードとして RA モードを指定します。デフォルトでは、RA モードは無効です。  • (任意) <b>retry period</b> キーワードおよび <i>minutes</i> 引数は、CA に別の証明書要求を送信するまでルータが待機する期間を分単位で指定します。有効値は 1 ~ 60 です。デフォルトは 1 です。  • (任意) <b>retry count</b> キーワードおよび <i>number</i> 引数は、直前の要求に対する応答をルータが受信しない場合、ルータが証明書要求を再送信する回数を指定します。有効な値は、1 ~ 100 です。デフォルトは 10 です。  • <i>url</i> 引数は、ルータが証明書要求を送信する CA の URL です。

	コマンドまたはアクション	目的
		<p>(注) IPv6 アドレスは <b>http:</b> 登録方式に追加できます。たとえば、 http://[ipv6-address]:80 です。URL 内の IPv6 アドレスは括弧で囲む必要があります。</p> <ul style="list-style-type: none"> <li>(任意) <b>pem</b> キーワードは、証明書要求にプライベート強化メール (PEM) の境界を追加します。</li> </ul>
ステップ 7	revocation-check method 例 : Device (ca-trustpoint) # <b>revocation-check crl</b>	(任意) 証明書の失効ステータスをチェックします。
ステップ 8	<b>exit</b> 例 : Device (ca-trustpoint) # <b>exit</b>	CA トラストポイントコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	<b>authorization username subjectname subjectname</b> 例 : Device (config) # <b>authorization username subjectname serialnumber</b>	AAA ユーザー名の構築に使用する異なる証明書フィールドのパラメータを設定します。 <i>subjectname</i> 引数には、次のいずれかを指定できます。 <ul style="list-style-type: none"> <li><b>all</b> : 証明書の識別名 (サブジェクト名) 全体。</li> <li><b>commonname</b> : 証明書の共通名。</li> <li><b>country</b> : 証明書の国。</li> <li><b>email</b> : 証明書の電子メール。</li> <li><b>ipaddress</b> : 証明書の IP アドレス。</li> <li><b>locality</b> : 証明書の地域。</li> <li><b>organization</b> : 証明書の組織。</li> <li><b>organizationalunit</b> : 証明書の組織単位。</li> <li><b>postalcode</b> : 証明書の郵便番号。</li> <li><b>serialnumber</b> : 証明書のシリアル番号。</li> <li><b>state</b> : 証明書の州フィールド。</li> <li><b>streetaddress</b> : 証明書の住所。</li> <li><b>title</b> : 証明書のタイトル。</li> </ul>

## ■ トラブルシューティングのヒント

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>unstructuredname</b> : 証明書の非公式名。</li> </ul>
ステップ 10	<b>authorization list</b> <i>listname</i> 例 : Device(config)# <b>authorization list maxaaa</b>	AAA 認可リストを指定します。
ステップ 11	<b>tacacs server</b> <i>server-name</i> 例 : Device(config)# <b>tacacs server yourserver</b>	TACACS+ サーバーを指定します。
ステップ 12	<b>address {ipv4   ipv6}</b> <i>ip-address</i> 例 : Device(config-server-tacacs)# <b>address ipv4 192.0.2.2</b>	TACACS サーバーの IP アドレスを設定します。
ステップ 13	<b>key string</b> 例 : Device(config-server-tacacs)# <b>key a_secret_key</b>	スイッチと TACACS サーバーとの間で使用される許可および暗号キーを設定します。
ステップ 14	<b>end</b> 例 : Device(config-server-tacacs)# <b>end</b> 例 :	特権 EXEC モードに戻ります。

## ■ トラブルシューティングのヒント

CA とルータ間のインタラクションのトレース (メッセージタイプ) に関するデバッグメッセージを表示するには、**debug crypto pki transactions** コマンドを使用します (サンプル出力を参照してください。ここでは、AAA サーバー交換との成功した PKI 統合、および AAA サーバー交換との失敗した PKI 統合を示します)。

### 成功した交換

```
Device# debug crypto pki transactions
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check
```

「CRYPTO\_PKI\_AAA」と表示されている各行は、AAA 認可チェックの状態を示します。各 AAA AV ペアが示され、認可チェックの結果が表示されます。

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aalist,
PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "15DE")
```

```
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

### 失敗した交換

```
Device# debug crypto pki transactions
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint"= "CA1")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "233D")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: timezone specific extended
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end check failed.
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: authorization failed
```

上記の失敗した交換では、証明書が失効しています。

## PKI 証明書ステータス チェックの失効メカニズムの設定

証明書失効メカニズム（CRL または OCSP）として CRL を設定し、PKI の証明書のステータスをチェックするには、次の作業を実行します。

### revocation-check コマンド

**revocation-check** コマンドを使用し、ピアの証明書が無効にされていないことを確認するための方式（OCSP、CRL、または失効チェックのスキップ）を少なくとも 1 つ指定します。複数の方式を指定する場合、方式を適用する順序は、このコマンドで指定した順序になります。

ルータに適用可能な CRL がなく、いずれの CRL も取得できない場合、あるいは OCSP サーバーがエラーを返す場合、設定に **none** キーワードを含めないかぎり、ルータはピアの証明書を拒否します。**none** キーワードを設定した場合、失効チェックは実行されず、証明書は常に受け入れられます。

### OCSP サーバーとのナンスおよびピア通信

OCSP を使用すると、OCSP サーバーとのピア通信時に、OCSP 要求に関するナンス（固有識別情報）がデフォルトで送信されます。ナンスを使用することにより、ピアと OCSP サーバー間にセキュアで信頼性の高い通信チャンネルが確立されます。

OCSP サーバーがナンスをサポートしていない場合は、ナンスの送信をディセーブルにできません。詳細は、OCSP サーバのマニュアルを参照してください。

### 始める前に

- クライアント証明書を発行する前に、サーバーで適切な設定（CDP の設定など）を行う必要があります。
- OCSP サーバーから CA サーバーの失効ステータスを返すように設定するときは、CA サーバーが発行した OCSP 応答署名証明書を OCSP サーバーに設定する必要があります。署名証明書が正しいフォーマットであることを確認してください。署名証明書のフォーマットが正しくない場合、ルータは、OCSP 応答を受理しません。詳細については、OCSP のマニュアルを参照してください。



- (注)
- OCSP は、HTTP を使用してメッセージを転送するので、OCSP サーバーにアクセスする際に遅延が発生する場合があります。
  - OCSP サーバーが、失効ステータスのチェックを通常の CRL 処理に依存している場合、CRL の遅延は OCSP にも適用されます。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint name**
4. **ocsp url url**
5. **revocation-check method1 [method2 method3]**
6. **ocsp disable-nonce**
7. **exit**
8. **exit**
9. **show crypto pki certificates**
10. **show crypto pki trustpoints [status | label [status]]**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>crypto pki trustpoint name</b> 例： Device(config)# crypto pki trustpoint hazel	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	<b>ocsp url url</b> 例： Device(ca-trustpoint)# ocsp url http://ocsp-server または	<i>url</i> 引数は、トラストポイントが証明書ステータスをチェックできるように OCSP サーバーの URL を指定します。この URL は、証明書の AIA 拡張部に指定されている OCSP サーバーの URL（存在する場合）を上書きします。設定したトラストポイントに関連するすべての証明書は、OCSP サーバーに



	コマンドまたはアクション	目的
	<pre>Device(ca-trustpoint)# ocspl url http://10.10.10.1:80</pre> <p>または</p> <pre>Device(ca-trustpoint)# ocspl url http://[2001DB8:1:1::2]:80</pre>	<p>よって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。</p>
ステップ 5	<p><b>revocation-check method1 [method2 method3]</b></p> <p>例 :</p> <pre>Device(ca-trustpoint)# revocation-check ocspl none</pre>	<p>証明書の失効ステータスをチェックします。</p> <ul style="list-style-type: none"> <li>• <b>crl</b> : CRL によって証明書をチェックします。これがデフォルトのオプションです。</li> <li>• <b>none</b> : 証明書のチェックを無視します。</li> <li>• <b>ocspl</b> : OCSP サーバーによって証明書をチェックします。</li> </ul> <p>2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバーがダウンしている場合など）にだけ使用されます。</p>
ステップ 6	<p><b>ocspl disable-nonce</b></p> <p>例 :</p> <pre>Device(ca-trustpoint)# ocspl disable-nonce</pre>	<p>(任意) OCSP サーバーとピアが通信するときに、ナンス (OCSP 要求に関する固有識別情報) が送信されないように指定します。</p>
ステップ 7	<p><b>exit</b></p> <p>例 :</p> <pre>Device(ca-trustpoint)# exit</pre>	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 8	<p><b>exit</b></p> <p>例 :</p> <pre>Device(config)# exit</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 9	<p><b>show crypto pki certificates</b></p> <p>例 :</p> <pre>Device# show crypto pki certificates</pre>	<p>(任意) 証明書に関する情報を表示します。</p>
ステップ 10	<p><b>show crypto pki trustpoints [status   label [status]]</b></p> <p>例 :</p> <pre>Device# show crypto pki trustpoints</pre>	<p>ルータに設定されているトラストポイントに関する情報を表示します。</p>

## 証明書の許可および失効の設定

証明書ベース ACL の指定、失効チェックまたは失効した証明書の無視、手動によるデフォルトの CDP の場所の上書き、手動による OCSP サーバー設定の上書き、CRL キャッシングの設定、あるいは証明書シリアル番号に基づくセッションの受理/拒否の設定を行うには、必要に応じて次の作業を実行します。

### 失効チェックを無視するように証明書ベース ACL を設定

証明書ベース ACL を使用して、失効チェックおよび失効証明書を無視するようにルータを設定するには、次の手順を実行します。

- 既存のトラストポイントの識別またはピアの証明書の検証に使用される新しいトラストポイントを作成します。トラストポイントがまだ認証されていない場合は、認証してください。必要に応じて、ルータをこのトラストポイントに登録できます。**match certificate** コマンドと **skip revocation-check** キーワードを使用する場合は、トラストポイントにオプションの CRL を設定しないでください。
- 証明書自体の CRL をチェックする必要がない証明書の固有の特性と、許可する必要がある失効証明書の固有の特性を判別します。
- 前のステップで確認した特性と一致する証明書マップを定義します。
- 最初の手順で作成または指定したトラストポイントに、**match certificate** コマンドと **skip revocation-check** キーワード、**match certificate command** と **allow expired-certificate** キーワードを追加できます。



(注) 証明書マップは、ピアの公開キーがキャッシュされている場合でも確認されます。たとえば、ピアによって公開キーがキャッシュされており、証明書マップがトラストポイントに追加されて証明書が禁止されると、証明書マップが有効になります。これにより、過去に一度接続され、現在は禁止されている証明書を持つクライアントが再接続することを防ぎます。

### 証明書内の CDP の手動による上書き

ユーザーは、手動で設定した CDP で証明書内の CDP を上書きできます。証明書の CDP の手動による上書きは、特定のサーバーが長時間利用できない場合に便利です。元の CDP を含む証明書のすべてを再発行しなくても、証明書の CDP を URL またはディレクトリ指定に置き換えることができます。

### 手動による証明書の OCSP サーバー設定の上書き

管理者はクライアント証明書の Authority Information Access (AIA) フィールドに指定された、または **ocsp url** コマンドを発行して設定された OCSP サーバーの設定値を上書きできます。**match certificate override ocsp** コマンドを使用すると、1つまたは複数の OCSP サーバーをクライアント証明書ごとに、またはクライアント証明書のグループごとに手動で指定できます。失効チェック時にクライアント証明書が証明書マップに正常に照合された場合、**match certificate**

**override ocspl** コマンドを発行すると、クライアント証明書 AIA フィールドまたは **ocspl url** コマンド設定が上書きされます。



(注) 1つのクライアント証明書には、OCSP サーバーを1つだけ指定できます。

## CRL キャッシュ コントロールの設定

デフォルトでは、現在キャッシュされている CRL が失効すると、新しい CRL がダウンロードされます。管理者は、**crl cache delete-after** コマンドを発行して、CRL がキャッシュに保持される最大時間（分単位）を設定するか、**crl cache none** コマンドを発行して CRL キャッシュを無効にできます。**crl-cache delete-after** コマンドまたは **crl-cache none** コマンドのみを指定できます。トラストポイントに両方のコマンドを入力した場合は、後に実行されたコマンドが有効になり、メッセージが表示されます。

**crl-cache none** コマンドまたは **crl-cache delete-after** コマンドのいずれを実行しても現在キャッシュされている CRL に影響はありません。**crl-cache none** コマンドを設定した場合、このコマンドを発行すると、ダウンロードされたすべての CRL はキャッシュされません。**crl-cache delete-after** コマンドを設定した場合、このコマンドの発行後に設定されたライフタイムだけがダウンロードされた CRL に影響します。

この機能は、CA が失効日を指定せずに CRL を発行する場合、あるいは失効日が数日後または数週間後に迫っている場合に役立ちます。

## 証明書のシリアル番号セッションコントロールの設定

証明書検証要求がセッションのトラストポイントによって受け入れられる、または拒否されるように証明書シリアル番号を指定できます。証明書のシリアル番号セッションコントロールによっては、証明書がまだ有効であっても、セッションが拒否される場合があります。証明書のシリアル番号セッションコントロールは、**serial-number** フィールドを持つ証明書マップまたは AAA 属性のいずれかを使用して **cert-serial-not** コマンドで設定できます。

セッションコントロールに証明書マップを使用すると、管理者は、1つの証明書シリアル番号を指定できます。AAA 属性を使用すると、管理者は、セッションコントロールに証明書シリアル番号を指定できます。

### 始める前に

- 証明書マップをトラストポイントに関連付ける前に、トラストポイントを定義し、認証する必要があります。
- CDP オーバライド機能を有効にする、または **serial-number** コマンドを発行する前に、証明書マップを設定する必要があります。
- PKI と AAA サーバーとの統合は、「証明書ステータスのための PKI と AAA サーバーの統合」の説明のとおり AAA 属性を使用して正常に完了する必要があります。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki certificate map** *label sequence-number*
4. *field-name match-criteria match-value*
5. **exit**
6. **crypto pki trustpoint** *name*
7. 次のいずれかを実行します。
  - **crl-cache** *none*
  - **crl-cache delete-after** *time*
8. **match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**]
9. **match certificate** *certificate-map-label* **override cdp** {*url* | *directory*} *string*
10. **match certificate** *certificate-map-label* **override ocsp** [*trustpoint trustpoint-label*] *sequence-number url ocsp-url*
11. **exit**
12. **aaa new-model**
13. **aaa attribute list** *list-name*
14. **attribute type** {*name*} {*value*}
15. **exit**
16. **exit**
17. **show crypto pki certificates**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例 :  Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>crypto pki certificate map</b> <i>label sequence-number</i> 例 :  Device(config)# crypto pki certificate map Group 10	証明書において、一致する必要がある値または一致する必要がない値を定義し、CA 証明書マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<p><i>field-name match-criteria match-value</i></p> <p>例 :</p> <pre>Device(ca-certificate-map)# subject-name co MyExample</pre>	<p>1 つまたは複数の証明書フィールドと、これらのフィールドの一致基準および照合する値を指定します。</p> <p><i>field-name</i> には、次のいずれかの名前文字列（大文字と小文字を区別しない）または日付を指定します。</p> <ul style="list-style-type: none"> <li>• <b>alt-subject-name</b></li> <li>• <b>expires-on</b></li> <li>• <b>issuer-name</b></li> <li>• <b>name</b></li> <li>• <b>serial-number</b></li> <li>• <b>subject-name</b></li> <li>• <b>unstructured-subject-name</b></li> <li>• <b>valid-start</b></li> </ul> <p>(注) 日付フィールドのフォーマットは、dd mm yyyy hh:mm:ss または mmm dd yyyy hh:mm:ss です。</p> <p><i>match-criteria</i> には、次の論理演算子のいずれかを指定します。</p> <ul style="list-style-type: none"> <li>• <b>co</b> : 含む（名前およびシリアル番号フィールドでのみ有効）</li> <li>• <b>eq</b> : 等しい（名前、シリアル番号、および日付フィールドで有効）</li> <li>• <b>ge</b> : 以上（日付フィールドでのみ有効）</li> <li>• <b>lt</b> : 未満（日付フィールドでのみ有効）</li> <li>• <b>nc</b> : 含まない（名前およびシリアル番号フィールドでのみ有効）</li> <li>• <b>ne</b> : 等しくない（名前、シリアル番号、および日付フィールドで有効）</li> </ul> <p><i>match-value</i> は、<i>match-criteria</i> で割り当てられた論理演算子を使用してテストする名前または日付です。</p>

	コマンドまたはアクション	目的
		(注) このコマンドは、証明書ベース ACL を設定する場合にだけ使用し、失効チェックまたは失効した証明書を無視するように証明書ベース ACL を設定する場合には使用しないでください。
ステップ 5	<b>exit</b> 例：  Device(ca-certificate-map)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<b>crypto pki trustpoint name</b> 例：  Device(config)# crypto pki trustpoint Access2	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 7	次のいずれかを実行します。  • <b>crl-cache none</b>  • <b>crl-cache delete-after time</b> 例：  Device(ca-trustpoint)# crl-cache none 例：  Device(ca-trustpoint)# crl-cache delete-after 20	(任意) トラストポイントに関連付けられたすべての CRL の CRL キャッシングを完全にディセーブルにします。  <b>crl-cache none</b> コマンドを実行しても、現在キャッシュされている CRL に影響はありません。このコマンドが設定された後にダウンロードされるすべての CRL は、キャッシュされません。  (任意) トラストポイントに関連付けられたすべての CRL に関して、CRL がキャッシュに保持される最大時間を指定します。  • <i>time</i> : CRL が削除されるまでの時間 (分単位)。  <b>crl-cache delete-after</b> コマンドを実行しても、現在キャッシュされている CRL に影響はありません。設定されたライフタイムは、このコマンドが設定された後にダウンロードされた CRL だけに影響します。
ステップ 8	<b>match certificate certificate-map-label [allow expired-certificate   skip revocation-check   skip authorization-check]</b> 例：  Device(ca-trustpoint)# match certificate Group skip revocation-check	(任意) 証明書ベース ACL ( <b>crypto pki certificate map</b> コマンドによって定義されている) をトラストポイントに関連付けます。  • <i>certificate-map-label</i> : <b>crypto pki certificate map</b> コマンドを使用して指定した <i>label</i> 引数と一致する必要があります。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>allowexpired-certificate</b> : 失効した証明書を無視します。</li> <li>• <b>skip revocation-check</b> : トラストポイントが、特定の証明書を除く CRL を適用できるようにします。</li> <li>• <b>skip authorization-check</b> : AAA サーバーとの PKI 統合を設定すると、証明書の AAA チェックをスキップします。</li> </ul>
ステップ 9	<p><b>match certificate</b> <i>certificate-map-label</i> <b>override cdp</b> <b>{url   directory}</b> <i>string</i></p> <p>例 :</p> <pre>Device(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com</pre>	<p>(任意) URL またはディレクトリが指定された証明書の、既存の CDP エントリを手動で上書きします。</p> <ul style="list-style-type: none"> <li>• <b>certificate-map-label</b> : ユーザー指定のラベル。事前に定義された <b>crypto pki certificate map</b> コマンドに指定した <i>label</i> 引数と一致する必要があります。</li> <li>• <b>url</b> : 証明書の CDP が HTTP または LDAP URL で上書きされるように指定します。</li> <li>• <b>directory</b> : 証明書の CDP が LDAP ディレクトリ指定で上書きされるように指定します。</li> <li>• <b>string</b> : URL またはディレクトリ指定。</li> </ul> <p>(注) 一部のアプリケーションは、すべての CDP が試行される前にタイムアウトすることがあり、エラーメッセージで報告します。エラーメッセージはルータに影響を及ぼしません。また、Cisco IOS ソフトウェアは、すべての CDP が試行されるまで CRL の取得を続行します。</p>
ステップ 10	<p><b>match certificate</b> <i>certificate-map-label</i> <b>override ocsp</b> [<b>trustpoint</b> <i>trustpoint-label</i>] <i>sequence-number</i> <b>url</b> <i>ocsp-url</i></p> <p>例 :</p> <pre>Device(ca-trustpoint)# match certificate mycertmapname override ocsp trustpoint mytp 15 url http://192.0.2.2</pre>	<p>(任意) OCSP サーバーをクライアント証明書ごとに、またはクライアント証明書のグループごとに指定し、複数回発行して、追加の OCSP サーバーおよびクライアント証明書の設定 (代替の PKI 階層を含む) を指定できます。</p> <ul style="list-style-type: none"> <li>• <b>certificate-map-label</b> : 既存の証明書マップ名。</li> <li>• <b>trustpoint</b> : OCSP サーバー証明書を検証するときに使用されるトラストポイント。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>sequence-number</i> : <b>match certificate override</b> <b>ocsp</b> コマンド文を検証対象の証明書に適用する順序。照合が最低のシーケンス番号から最高のシーケンス番号に実行されます。同じシーケンス番号で複数のコマンドを発行すると、前の OCSP サーバー オーバライド設定が上書きされます。</li> <li>• <b>url</b> : OCSP サーバーの URL。</li> </ul> <p>証明書が設定された証明書マップと一致すると、クライアント証明書の AIA フィールドおよび以前に発行された <b>ocsp url</b> コマンド設定値は、指定された OCSP サーバーで上書きされます。</p> <p>マップベースの一致が発生しない場合、引き続き次の2つのケースがクライアント証明書に適用されます。</p> <ul style="list-style-type: none"> <li>• OCSP を失効方法として指定すると、AIA フィールド値がクライアント証明書に引き続き適用されます。</li> <li>• <b>ocsp url</b> 設定が存在する場合は、<b>ocsp url</b> 設定が引き続きクライアント証明書に適用されます。</li> </ul>
ステップ 11	<b>exit</b> 例 : <pre>Device(ca-trustpoint)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	<b>aaa new-model</b> 例 : <pre>Device(config)# aaa new-model</pre>	(任意) AAA アクセス コントロール モデルをイネーブルにします。
ステップ 13	<b>aaa attribute list</b> <i>list-name</i> 例 : <pre>Device(config)# aaa attribute list crl</pre>	(任意) ルータにローカルで AAA 属性リストを定義し、 <b>config-attr-list</b> コンフィギュレーション モードを開始します。
ステップ 14	<b>attribute type</b> <i>{name}</i> <i>{value}</i> 例 : <pre>Device(config-attr-list)# attribute type cert-serial-not 6C4A</pre>	(任意) ルータの AAA 属性リストにローカルに追加される AAA 属性タイプを定義します。 証明書のシリアル番号セッションコントロールを設定するために、管理者は、 <i>value</i> フィールドの特定



	コマンドまたはアクション	目的
		<p>の証明書を、<i>name</i> が <b>cert-serial-not</b> に設定されているシリアル番号に基づき受け入れるか、拒否するか指定できます。証明書のシリアル番号が属性タイプ設定で指定されたシリアル番号と一致した場合、証明書は拒否されます。</p> <p>使用可能な AAA 属性タイプのリストを表示するには、<b>show aaa attributes</b> コマンドを実行してください。</p>
ステップ 15	<b>exit</b> 例： <pre>Device(ca-trustpoint)# exit</pre> 例： <pre>Device(config-attr-list)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	<b>exit</b> 例： <pre>Device(config)# exit</pre>	特権 EXEC モードに戻ります。
ステップ 17	<b>show crypto pki certificates</b> 例： <pre>Device# show crypto pki certificates</pre>	(任意) CA 証明書が認証されたら、ルータにインストールされた証明書のコンポーネントを表示します。

## 例

次に、サンプル証明書を示します。OCSP 関連の拡張子は感嘆符を使用して示されません。

```
Certificate:
  Data:
    Version: v3
    Serial Number:0x14
    Signature Algorithm:SHAwithRSA - 1.2.840.113549.1.1.4
    Issuer:CN=CA server,OU=PKI,O=Cisco Systems
    Validity:
      Not Before:Thursday, August 8, 2002 4:38:05 PM PST
      Not After:Tuesday, August 7, 2003 4:38:05 PM PST
    Subject:CN=OCSP server,OU=PKI,O=Cisco Systems
    Subject Public Key Info:
      Algorithm:RSA - 1.2.840.113549.1.1.1
      Public Key:
        Exponent:65537
        Public Key Modulus:(2048 bits) :
          <snip>
```

## トラブルシューティングのヒント

```

Extensions:
  Identifier:Subject Key Identifier - 2.5.29.14
    Critical:no
    Key Identifier:
      <snip>
  Identifier:Authority Key Identifier - 2.5.29.35
    Critical:no
    Key Identifier:
      <snip>
!
  Identifier:OCSP NoCheck:- 1.3.6.1.5.5.7.48.1.5
    Critical:no
  Identifier:Extended Key Usage:- 2.5.29.37
    Critical:no
    Extended Key Usage:
      OCSPSigning
!

  Identifier:CRL Distribution Points - 2.5.29.31
    Critical:no
    Number of Points:1
    Point 0
      Distribution Point:
[URIName:ldap://CA-server/CN=CA server,OU=PKI,O=Cisco Systems]
  Signature:
    Algorithm:SHAwithRSA - 1.2.840.113549.1.1.4
  Signature:
    <snip>

```

次の例は、既存のシーケンスの先頭に **match certificate override ocs** コマンドを追加したときの実行コンフィギュレーション出力の抜粋を示します。

```

match certificate map3 override ocs 5 url http://192.0.2.3/
show running-configuration
.
.
.
      match certificate map3 override ocs 5 url http://192.0.2.3/
      match certificate map1 override ocs 10 url http://192.0.2.1/
      match certificate map2 override ocs 15 url http://192.0.2.2/

```

次の例は、既存の **match certificate override ocs** コマンドが置き換えられ、トラストポイントが代替のPKI階層を使用するように指定された場合の、実行コンフィギュレーション出力の抜粋を示します。

```

match certificate map4 override ocs trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
.
.
.
      match certificate map3 override ocs trustpoint tp3 5 url http://192.0.2.3/
      match certificate map1 override ocs trustpoint tp1 10 url http://192.0.2.1/
      match certificate map4 override ocs trustpoint tp4 10 url
http://192.0.2.4/newvalue
      match certificate map2 override ocs trustpoint tp2 15 url http://192.0.2.2/

```

## トラブルシューティングのヒント

失効チェックまたは失効した証明書を無視した場合は、慎重に設定を確認する必要があります。証明書マップが、当該の証明書または許可する証明書、あるいはスキップするAAAチェッ

クのいずれかと適切に一致していることを確認してください。管理された環境で、証明書マップを変更して想定どおりに機能していないものを判別します。

## 証明書チェーンの設定

ピア証明書の証明書チェーンパスに処理レベルを設定するには、次の作業を実行します。

### 始める前に

- デバイスを PKI 階層に登録する必要があります。
- 適切なキー ペアを証明書に関連付ける必要があります。



- (注)
  - ルート CA に関連付けられたトラストポイントは、次のレベルに対して有効になるように設定できません。

**chain-validation** コマンドは、ルート CA に関連付けられたトラストポイント用に **continue** キーワードを指定して設定します。エラーメッセージが表示され、チェーン検証はデフォルトの **chain-validation** コマンド設定に戻ります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpointname**
4. **chain-validation** [{stop | continue} [parent-trustpoint]]
5. **exit**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>crypto pki trustpointname</b> 例： Device(config)# crypto pki trustpoint ca-sub1	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<b>chain-validation</b> [{stop   continue} [parent-trustpoint]] 例： <pre>Device(ca-trustpoint)# chain-validation continue ca-sub1</pre>	証明書チェーンが、すべての証明書（下位 CA 証明書を含む）で処理されるレベルを設定します。 <ul style="list-style-type: none"> <li>• <b>stop</b> キーワードを使用して、証明書がすでに信頼できることを明示します。これがデフォルトの設定です。</li> <li>• <b>continue</b> キーワードを使用して、トラストポイントに関連付けられた下位 CA 証明書を有効にする必要があることを明示します。</li> <li>• <i>parent-trustpoint</i> 引数は、証明書を照合する必要がある親トラストポイント名を指定します。</li> </ul>
ステップ 5	<b>exit</b> 例： <pre>Device(ca-trustpoint)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。

## 証明書の許可および失効の設定例

### PKI AAA 許可の設定および確認の例

ここでは、PKI AAA 認可の設定例を示します。

例：ルータ設定

次の **show running-config** コマンド出力は、AAA サーバー機能との PKI 統合を使用して、VPN 接続を許可するように設定されたルータの動作設定を示します。

```
Device#show running-config

Building configuration...
!
version 12.3
!
hostname router7200router7200
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSLab group tacacs+
aaa authorization network ACSLab group tacacs+
aaa accounting exec ACSLab start-stop group tacacs+
aaa accounting network default start-stop group ACSLab
aaa session-id common
!
```

```

ip domain name example.com
!
crypto pki trustpoint EM-CERT-SERV
enrollment url http://192.0.2.33:80
serial-number
crl optional
rsakeypair STOREVPN 2048
auto-enroll
authorization list ACSLab
!
crypto pki certificate chain EM-CERT-SERV
certificate 04
 30820214 3082017D A0030201 02020104 300D0609 2A864886 F70D0101 04050030
 17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30343031
 31393232 30323535 5A170D30 35303131 38323230 3235355A 3030312E 300E0603
 55040513 07314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
 312E6772 696C2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500 03818D00
 30818902 818100BD F3B837AA D925F391 2B64DA14 9C2EA031 5A7203C4 92F8D6A8
 7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB BE5A1E74 B1AA5AE0
 5CA162FF 8C3ACA4F B3EE9F27 8B031642 B618AE1B 40F2E3B4 F996BEFE 382C7283
 3792A369 236F8561 8748AA3F BC41F012 B859BD9C DB4F75EE 3CEE2829 704BD68F
 FD904043 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
 16861468 7474703A 2F2F3633 2E323437 2E313037 2E393330 0B060355 1D0F0404
 030205A0 301F0603 551D2304 18301680 1420FC4B CF0B1C56 F5BD4C06 0AFD4E67
 341AE612 D1300D06 092A8648 86F70D01 01040500 03818100 79E97018 FB955108
 12F42A56 2A6384BC AC8E22FE F1D6187F DA5D6737 C0E241AC AAAEC75D 3C743F59
 08DEEFF2 0E813A73 D79E0FA9 D62DC20D 8E2798CD 2C1DC3EC 3B2505A1 3897330C
 15A60D5A 8A13F06D 51043D37 E56E45DF A65F43D7 4E836093 9689784D C45FD61D
 EC1F160C 1ABC8D03 49FB11B1 DA0BED6C 463E1090 F34C59E4
quit
certificate ca 01
 30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30333132
 31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
 55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
 01050003 818D0030 81890281 8100C14D 833641CF D784F516 DA6B50C0 7B3CB3C9
 589223AB 99A7DC14 04F74EF2 AAEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
 54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078B8
 E9DE981E B733B868 AA8916C0 A8048607 D34B83C0 64BDC101 161FC103 13C06500
 22D6EE75 7D6CF133 7F1B515F 32830203 010001A3 63306130 0F060355 1D130101
 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
 16041420 FC4BCF0B 1C56F5BD 4C060AFD 4E67341A E612D130 1F060355 1D230418
 30168014 20FC4BCF 0B1C56F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
 F70D0101 04050003 81810085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
 BD572026 528E92ED 02F3A0AE 1803F2AE AA4C0ED2 0F59F18D 7B50264F 30442C41
 0AF19C4E 70BD3CB5 0ADD8DE8 8EF636BD 24410DF4 DB62DAFC 67DA6E58 3879AA3E
 12AFB1C3 2E27CB27 EC74E1FC AEE2F5CF AA80B439 615AA8D5 6D6DEDC3 7F9C2C79
 3963E363 F2989FB9 795BA8
quit
!
!
crypto isakmp policy 10
encr aes
group 14
!
!
crypto ipsec transform-set ISC_TS_1 esp-aes esp-sha-hmac
!
crypto ipsec profile ISC_IPSEC_PROFILE_2
set security-association lifetime kilobytes 53000000
set security-association lifetime seconds 14400
set transform-set ISC_TS_1
!
!

```

## 例：成功した PKI AAA 許可のデバッグ

```

controller ISA 1/1
!
!
interface Tunnel0
  description MGRE Interface provisioned by ISC
  bandwidth 10000
  ip address 192.0.2.172 255.255.255.0
  no ip redirects
  ip mtu 1408
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 500
  ip nhrp server-only
  no ip split-horizon eigrp 101
  tunnel source FastEthernet2/1
  tunnel mode gre multipoint
  tunnel key 101
  tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
  ip address 192.0.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet2/1
  ip address 192.0.2.2 255.255.255.0
  duplex auto
  speed auto
!
!
tacacs-server host 192.0.2.55 single-connection
tacacs-server directed-request
tacacs-server key company lab
!
ntp master 1
!
end

```

## 例：成功した PKI AAA 許可のデバッグ

次の **show debugging** コマンド出力は、AAA サーバー機能との PKI 統合を使用して、成功した許可を示します。

```

Device#show debugging

General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto PKI Trans debugging is on
Device#
May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.805: CRYPTO_PKI: cert revocation status unknown.
May 28 19:36:12.805: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
  <all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSLab'
May 28 19:36:12.813: TPLUS: Queuing AAA Authorization request 66 for processing
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to None .....Skipping

```

```

May 28 19:36:12.813: TPLUS: Sending AV service=pki
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD5.example.com)
May 28 19:36:12.813: TPLUS: Using server 192.0.2.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27
bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/203A4628: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed
Device#
Device#
May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 192.0.2.171 (Tunnel0)
is up: new adjacency
Device#
Device# show crypto isakmp sa
dst          src          state          conn-id slot
192.0.2.22   192.0.2.102  QM_IDLE       84      0

```

### 例：失敗した PKI AAA 許可のデバッグ

次の **show debugging** コマンド出力は、ルータが、VPN を使用しての接続を許可されていないことを示します。このメッセージは、このような状況で表示される典型的なメッセージです。

この例においてピア ユーザ名は、Cisco Secure ACS の VPN\_Router\_Disabled と呼ばれる Cisco Secure ACS グループに移動することにより、許可されていないものとして設定されました。ルータ (router7200.example.com) は、任意のピアに VPN 接続を確立する前に、Cisco Secure ACS AAA サーバに確認するように設定されています。

```

Device#show debugging

General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto PKI Trans debugging is on

Device#
May 28 19:48:29.837: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:31.509: CRYPTO_PKI: Found a issuer match
May 28 19:48:31.525: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:31.525: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:31.533: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
<all>)
May 28 19:48:31.533: AAA/BIND(00000044): Bind i/f
May 28 19:48:31.533: AAA/AUTHOR (0x44): Pick method list 'ACSLab'
May 28 19:48:31.533: TPLUS: Queuing AAA Authorization request 68 for processing
May 28 19:48:31.533: TPLUS: processing authorization request id 68
May 28 19:48:31.533: TPLUS: Protocol set to None .....Skipping
May 28 19:48:31.533: TPLUS: Sending AV service=pki
May 28 19:48:31.533: TPLUS: Authorization request created for 68(POD5.example.com)
May 28 19:48:31.533: TPLUS: Using server 192.0.2.55
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT/203A4C50: Started 5 sec timeout
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:48:31.533: TPLUS: Would block while reading pak header
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 12 header bytes (expect 6 bytes)

```

## 例：失効メカニズムの設定

```

May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 18 bytes response
May 28 19:48:31.537: TPLUS(00000044)/0/203A4C50: Processing the reply packet
May 28 19:48:31.537: TPLUS: received authorization response for 68: FAIL
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:31.537: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:31.537: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.example.com' failed.
May 28 19:48:31.537: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162
is bad: certificate invalid
May 28 19:48:39.821: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:41.481: CRYPTO_PKI: Found a issuer match
May 28 19:48:41.501: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:41.501: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:41.505: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
<all>)
May 28 19:48:41.505: AAA/BIND(00000045): Bind i/f
May 28 19:48:41.505: AAA/AUTHOR (0x45): Pick method list 'ACSLab'
May 28 19:48:41.505: TPLUS: Queuing AAA Authorization request 69 for processing
May 28 19:48:41.505: TPLUS: processing authorization request id 69
May 28 19:48:41.505: TPLUS: Protocol set to None .....Skipping
May 28 19:48:41.505: TPLUS: Sending AV service=pki
May 28 19:48:41.505: TPLUS: Authorization request created for 69(POD5.example.com)
May 28 19:48:41.505: TPLUS: Using server 198.168.244.55
May 28 19:48:41.509: TPLUS(00000045)/0/IDLE/63B22834: got immediate connect on new 0
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE/63B22834: Started 5 sec timeout
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE: wrote entire 46 bytes request
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 18 bytes response
May 28 19:48:41.509: TPLUS(00000045)/0/63B22834: Processing the reply packet
May 28 19:48:41.509: TPLUS: received authorization response for 69: FAIL
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:41.509: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:41.509: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.example.com' failed.
May 28 19:48:41.509: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162
is bad: certificate invalid
Device#
Device# show crypto iskmp sa
dst          src          state          conn-id slot
192.0.2.2    192.0.2.102 MM_KEY_EXCH    95      0

```

## 例：失効メカニズムの設定

ここでは、PKIの失効メカニズムを指定する際に使用できる設定例を示します。

## 例：OCSP サーバーの設定

次の例では、証明書の AIA 拡張部で指定された OCSP サーバーを使用するようにルータを設定する方法を示します。

```

Device(config)#crypto pki trustpoint mytp
Device(ca-trustpoint)#revocation-check ocsf

```



### 例：CRLの指定後のOCSPサーバーの指定

次の例では、CRLをCDPからダウンロードするようにルータを設定する方法を示します。CRLを利用できない場合は、証明書のAIA拡張部で指定されるOCSPサーバーが使用されます。両方のオプションが失敗した場合、証明書の検証も失敗します。

```
Device(config)#crypto pki trustpoint mytp
Device(ca-trustpoint)#revocation-check crl ocsf
```

### 例：OCSPサーバーの指定

以下に、HTTPURL「http://myocspserver:81」にあるOCSPサーバーを使用するようにルータを設定する例を示します。このサーバーがダウンしている場合は、失効チェックは行われません。

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# ocsf url http://myocspserver:81
Device(ca-trustpoint)# revocation-check ocsf none
```

### 例：OCSPサーバーとの通信でのナンスの無効化

次の例は、OCSP要求に関するナンス（固有識別情報）が、OCSPサーバーとの通信でディセーブルになっている場合の通信を示します。

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# ocsf url http://myocspserver:81
Device(ca-trustpoint)# revocation-check ocsf none
Device(ca-trustpoint)# ocsf disable-nonce
```

### 例：証明書失効チェック用に中央サイトでハブルータを構成する

次の例では、複数のブランチオフィスにセントラルサイトへの接続を提供しているセントラルサイトにあるハブルータを示します。

ブランチオフィスも追加のIPSecトンネルを使用して、ブランチオフィス間で直接相互に通信できます。

CAは、セントラルサイトにあるHTTPサーバーのCRLを公開します。セントラルサイトは、各ピアとIPSecトンネルを設定する場合、そのピアのCRLをチェックします。

次の例では、IPSec設定を示しません。PKI関連の設定だけを示します。

#### ホームオフィスのハブ設定

```
crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
```

例：証明書失効チェック用に中央サイトでハブルータを構成する

## セントラルサイトのハブルータ

```
Device# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE14000000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Central VPN Gateway
    cn=Central VPN Gateway
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end   date: 00:53:26 GMT Sep 26 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: VPN-GW
CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: VPN-GW
```

## ブランチオフィスルータのトラストポイント

```
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none

ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
```

証明書マップがブランチ オフィス ルータに入力されます。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
branch1(config)# crypto pki certificate map central-site 10
branch1(ca-certificate-map)#
```

セントラルサイトのハブルータ上で発行された **show certificate** コマンドの出力では、証明書が以下によって発行されたことを示しています。

```
cn=Central Certificate Authority
o=Home Office Inc
```

この2行は、行を区切るためのカンマ (,) を使用して1行に結合され、元の2行が最初の一致基準として追加されています。

```
Device(ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home
Office Inc
!The above line wrapped but should be shown on one line with the line above it.
```

セントラルサイトルータの証明書の所有者名についても、同じように組み合わせられています（「Name:」で始まる行は、所有者名の一部ではなく、証明書マップ基準を作成する際に無視する必要があることに注意してください）。これが証明書マップで使用されるサブジェクト名です。

```
cn=Central VPN Gateway
o=Home Office Inc
```

```
Device(ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc
```

これで、以前に設定された証明書マップがトラストポイントに追加されます。

```
Device(ca-certificate-map)# crypto pki trustpoint home-office
Device(ca-trustpoint)# match certificate central-site skip revocation-check
Device(ca-trustpoint)# exit
Device(config)# exit
```

設定がチェックされます（大部分の設定は示されていません）。

```
Device# write term
!Many lines left out
.
.
.
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
  match certificate central-site skip revocation-check
!
!
crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
!many lines left out
```

今後のピアの証明書との照合のために、発行者名の行とサブジェクト名の行が矛盾しないように再フォーマットされていることに注意してください。

ブランチオフィスがAAAをチェックする場合は、トラストポイントには次のような行があります。

```
crypto pki trustpoint home-office
```

例：証明書失効チェック用に中央サイトでハブルータを構成する

```
auth list allow_list
auth user subj commonname
```

証明書マップが上記のように定義されると、次のコマンドがトラストポイントに追加され、セントラルサイトハブのAAAチェックがスキップされます。

```
match certificate central-site skip authorization-check
```

両方のケースにおいてブランチサイトルータは、CRLのチェックまたはAAAサーバと通信するために、セントラルサイトにIPSecトンネルを確立する必要があります。ただし、**match certificate** コマンドと **central-site skip authorization-check (argument and keyword)** を使用しないと、ブランチオフィスがCRLまたはAAAサーバを確認するまで、トンネルを確立することはできません (**match certificate** コマンドと **central-site skip authorization-check** 引数およびキーワードを使用しない限り、トンネルは確立されません)。

ブランチサイトにあるデバイスの証明書が失効していて、その証明書を更新するためにセントラルサイトにトンネルを確立する必要がある場合、セントラルサイトで **match certificate** コマンドと **allow expired-certificate** キーワードを使用できます。

### セントラルサイトルータのトラストポイント

```
crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
```

### ブランチ1サイトルータのトラストポイント

```
Device# show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 2F62BE1400000000CA0
Certificate Usage: General Purpose
Issuer:
  cn=Central Certificate Authority
  o=Home Office Inc
Subject:
  Name: Branch 1 Site
  cn=Branch 1 Site
  o=Home Office Inc
CRL Distribution Points:
  http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
  start date: 00:43:26 GMT Sep 26 2003
  end date: 00:53:26 GMT Oct 3 2003
  renew date: 00:00:00 GMT Jan 1 1970
Associated Trustpoints: home-office
CA Certificate
Status: Available
Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
Certificate Usage: Signature
Issuer:
  cn=Central Certificate Authority
  o=Home Office Inc
```

```

Subject:
  cn=Central Certificate Authority
  o=Home Office Inc
CRL Distribution Points:
  http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
  start date: 22:19:29 GMT Oct 31 2002
  end   date: 22:27:27 GMT Oct 31 2017
Associated Trustpoints: home-office

```

証明書マップがセントラル サイト ルータに入力されます。

```

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# crypto pki certificate map branch1 10
Device(ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
!The above line wrapped but should be part of the line above it.
Device(ca-certificate-map)# subject-name eq cn=Brahcn 1 Site,o=home office inc

```

証明書マップがトラストポイントに追加されます。

```

Device(ca-certificate-map)# crypto pki trustpoint VPN-GW
Device(ca-trustpoint)# match certificate branch1 allow expired-certificate
Device(ca-trustpoint)# exit
Router (config) #exit

```

設定がチェックされます（設定の大部分は示されていません）。

```

Device# write term
!many lines left out
crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
  match certificate branch1 allow expired-certificate
!
!
crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
! many lines left out

```

**match certificate** コマンド、**branch1 allow expired-certificate**（引数とキーワード）および証明書マップは、ブランチルータが新しい証明書を取得した後すぐに削除する必要があります。

## 例：証明書の許可および失効の設定

この項では、CRL キャッシュ コントロールの設定または証明書のシリアル番号セッション コントロールを指定する場合に使用する設定例を示します。

### CRL キャッシュ コントロールの設定

次の例では、CA1 トラストポイントに関連付けられたすべての CRL の CRL キャッシングをディセーブルにする方法を示します。

```
crypto pki trustpoint CA1
enrollment url http://CA1:80
ip-address FastEthernet0/0
crl query ldap://ldap_CA1
revocation-check crl
crl-cache none
```

上記の例の設定を実行した直後は、まだ現在の CRL がキャッシュされています。

#### Device# show crypto pki crls

```
CRL Issuer Name:
cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

現在の CRL が失効すると、次の更新時に新しい CRL がルータにダウンロードされます。**crl-cache none** コマンドが有効になり、トラストポイントの CRL はすべてキャッシュされなくなります。また、キャッシュは無効になります。**show crypto pki crls** コマンドを実行して、CRL がキャッシュされていないことを確認できます。キャッシュされている CRL がないため、出力は表示されません。

次の例では、CA1 トラストポイントに関連付けられたすべての CRL に 2 分の最大ライフタイムを設定する方法を示します。

```
crypto pki trustpoint CA1
enrollment url http://CA1:80
ip-address FastEthernet0/0
crl query ldap://ldap_CA1
revocation-check crl
crl-cache delete-after 2
```

CRL の最大ライフタイムを設定するために上記例の設定を実行した直後でも、依然現在の CRL がキャッシュされます。

#### Device# show crypto pki crls

```
CRL Issuer Name:
cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
ldap://ldap.example.com/CN=name Cert Manager,O=example.com
When the current CRL expires, a new CRL is downloaded to the router at the next update
and the crl-cache delete-after
command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after
a maximum lifetime of 2 minutes.
You can verify that the CRL will be cached for 2 minutes by executing the show crypto
pki crls
command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.
```

#### Device# show crypto pki crls

```
CRL Issuer Name:
cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 22:57:42 GMT Nov 26 2005
```

```
NextUpdate: 22:59:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
```

```
ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

## 証明書のシリアル番号セッションコントロールの設定

次の例では、CA1 トラストポイントの証明書マップを使用した証明書のシリアル番号セッションコントロールの設定を示します。

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  chain-validation stop
  crl query ldap://ldap_server
  revocation-check crl
  match certificate crl
!
crypto pki certificate map crl 10
  serial-number co 279d
```



- (注) *match-criteria* 値が **co** (含む) ではなく **eq** (等しい) に設定されている場合、シリアル番号はスペースを含めて、証明書マップのシリアル番号に正確に一致する必要があります。

次の例では、AAA 属性を使用した証明書のシリアル番号セッションコントロールの設定を示します。この場合、証明書にシリアル番号「4ACA」がなければ、有効な証明書はすべて受け入れられません。

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  aaa new-model
!
aaa attribute list crl
attribute-type aaa-cert-serial-not 4ACA
```

サーバーログは、シリアル番号「4ACA」を持つ証明書が拒否されたことを示しています。証明書の拒否は、感嘆符で表示されます。

```
.
.
.
Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Certificate validated without revocation check
Dec 3 04:24:39.135: CRYPTO_PKI: Selected AAA username: 'PKIAAAA'
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list:'CRL'
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: checking AAA authorization (CRL, PKIAAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x4)
```

## 例：証明書チェーン検証の設定

```

Dec 3 04:24:39.135: AAA/BIND(00000021): Bind i/f
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'
.
.
.
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
!
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: cert-serial doesn't match ("4ACA" != "4ACA")
!
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: post-authorization chain validation status (0x7)
!
Dec 3 04:24:39.175: CRYPTO_PKI: AAA authorization for list 'CRL', and user 'PKIAAA'
failed.
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain
validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
!
Dec 3 04:24:39.175: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.43 is
bad: certificate invalid
Dec 3 04:24:39.175: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with
peer at 192.0.2.43
.
.
.

```

## 例：証明書チェーン検証の設定

この項では、デバイス証明書の証明書チェーン処理レベルを指定する場合に使用する設定例を示します。

## ピアからルート CA への証明書チェーン検証の設定

次の設定例では、ピア、SubCA11、SubCA1、および RootCA のすべての証明書が検証されます。

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsa-keypair RootCA
crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsa-keypair SubCA1
crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsa-keypair SubCA11

```

## ピアから下位 CA への証明書チェーン検証の設定

次の設定例では、ピア証明書および SubCA1 証明書が有効にされます。

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none

```



```

rsa-keypair RootCA
crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa-keypair SubCA1
crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
rsa-keypair SubCA11

```

## 証明書チェーンの欠落確認の設定

次の設定例では、SubCA1 が、設定済みの Cisco IOS 階層にはないが、提出された証明書チェーンでピアによって提示されたと想定しています。

ピアが、提出された証明書チェーンで SubCA1 証明書を提示した場合、ピア、SubCA11、および SubCA1 の各証明書が有効になります。

ピアが、提出された証明書チェーンで SubCA1 証明書を提示しない場合、チェーンの検証は失敗します。

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
rsa-keypair RootCA
crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa-keypair SubCA11

```

## PKI での証明書の許可および失効の追加リファレンス

### シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="https://www.cisco.com/cisco/web/support/index.html">https://www.cisco.com/cisco/web/support/index.html</a>

## PKI での証明書の許可および失効の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
	PKIでの証明書の許可および失効	証明書には、指定された処理の実行をデバイスまたはユーザーが許可されているかどうかの判別を使用されるフィールドがいくつか含まれています。また、証明書ベース ACL は失効、許可、またはトラストポイントなどの PKI コンポーネントを使用するタイミングを判別するのに役立ちます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

## 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。