PKI での証明書の許可および失効の設定

この章では、公開キー インフラストラクチャ（PKI）で証明書の許可および失効を設定する方法について説明します。証明書サーバへのハイ アベイラビリティのサポートに関する情報も挙げています。

機能情報の入手

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「証明書の許可および失効に関する機能情報」（P.47）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

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。

- Certificate Authority（CA; 認証局）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。

「crypto ca」から「crypto pki」への CLI 変更

Cisco IOS Release 12.3(7)T の時点で、コマンドの先頭に付けられていた「crypto ca」は、すべて「crypto pki」に変更されました。ルータは引き続き crypto ca コマンドを受け入れますが、すべての出力は crypto pki として読み替えられます。

ハイ アベイラビリティ

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

シャーシ内での Stateful Switchover（SSO）冗長性の PKI High Availability（HA）サポートは、現在 Cisco IOS Release 12.2 S ソフトウェアを実行するすべてのスイッチ上でサポートされていません。詳細については、Cisco Bug CSCtb59872 を参照してください。

証明書の許可および失効に関する情報

証明書の許可および失効を設定するには、次の概念を理解しておく必要があります。

- 「PKI の許可」（P.3）
- 「証明書ステータスのための PKI と AAA サーバの統合」（P.3）
- 「CRL または OCSP サーバ：証明書失効メカニズムの選択」（P.5）
- 「許可または失効用に証明書ベースの ACL を使用する場合」（P.7）
- 「PKI 証明書チェーンの検証」（P.8）
- 「ハイ アベイラビリティのサポート」（P.9）

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めます。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、外部サーバから証明書ベースの ACL 指示を取得する方が有利です（認証用に証明書ベースの ACL を使用する場合の詳細は、「許可または失効用に証明書ベースの ACL を使用する場合」を参照してください）。

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 サーバの統合

PKI を認証、認可、アカウンティング（AAA）サーバ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 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 をサポートする場合は、コンポーネントを直接指定できます。たとえば、アプリケーション コンポーネントには、「ipsec」、「ssl」、または「osp」のいずれかを指定できます（ipsec ＝ IP セキュリティ、ssl ＝ セキュア ソケット レイヤ、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 プロトコルの選択

AAA サーバは、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 サーバを設定する場合、許可に必要な RADIUS または TACACS アトリビュート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 サーバのユーザ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 サーバのユーザ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 サーバに PKI サービスを追加する必要があります。カスタム アトリビュート「cert-application=all」が、PKI サービスの特定のユーザまたはユーザ グループに追加され、特定のユーザ名が許可されます。

PKI と AAA サーバ統合用のアトリビュート値ペア

表 1 に、AAA サーバと PKI との統合を設定する場合に使用されるアトリビュート値（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、ユーザは、他のすべてのユーザの 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、ユーザごとに一意のユーザ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、証明書の所有者名全体を許可ユーザ名として使用するように指定できます。

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。
cisco-avpair=pki:cert-trustpoint=msca	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。 **（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。
cisco-avpair=pki:cert-serial=16318DB7000 100001671	この値は証明書のシリアル番号です。 **（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。
cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003	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。 **（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）。

CRL または OCSP サーバ：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 Certificate Revocation List（CRL; 証明書失効リスト）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 および AAA 証明書許可とステータス チェックに関する詳細は、「証明書ステータスのための PKI と AAA サーバの統合」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も、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 Distribution Point（CDP; CRL 配布ポイント）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 Security Association（SA; セキュリティ アソシエーション）および Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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 の方式と場所
  - 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。
  - この場所は、CRL の取得先を決定します。たとえば、サーバおよび 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。

（注） Cisco IOS Release 12.3(7)T 以前のリリースでは、証明書に 2 つ以上の CDP が含まれていても、Cisco IOS ソフトウェアは、CRL の取得を 1 回だけ試行します。

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（ナンス）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、ナンスを含むピアに応答します。応答のナンスが OCSP サーバからピアによって送信された元のナンスと一致しない場合、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 サーバを設定できます。詳細は、OCSP サーバのマニュアルを参照してください。

OCSP サーバを使用する場合

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。

（注） Cisco IOS Release 12.4(9)T 以降では、管理者は、CRL キャッシングを完全にディセーブルにするか、キャッシュされた CRL のトラストポイントごとに最大ライフタイムを設定することによって、CRL キャッシングを設定できます。

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を助けます。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）、Not equal（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）
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）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 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）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 サーバとは通信できません。AAA サーバ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 つのト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ト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。Cisco IOS Release 12.4(6) T 以降のリリースでは、管理者は、下位 CA 証明書を含むすべての証明書における証明書チェーンの処理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。

ハイ アベイラビリティのサポート

証明書サーバへのハイ アベイラビリティのサポートは、次の方法で実現します。

- 取り消しコマンドのスタンバイ証明書サーバとの同期
- 証明書の新規発行時のシリアル番号コマンドの送信

スタンバイ証明書サーバがアクティブになると、証明書と CRL を発行する手段の準備が完了します。

ハイ アベイラビリティのサポートをさらに高めるには、スタンバイとの次の同期を行います。

- 証明書サーバ設定
- 保留中の要求
- コマンドの許可と拒否
- 設定の同期がサポートされないボックスツーボックスのハイ アベイラビリティのためには、基本設定の同期メカニズムが冗長性機能上で動作します。
- トラストポイント設定同期のサポート

PKI に対して証明書の許可および失効を設定する方法

ここでは、次の各手順について説明します。

- 「AAA サーバとの PKI 統合の設定」（P.10）（必須）
- 「PKI 証明書ステータス チェックの失効メカニズムの設定」（P.13）（必須）

- 「証明書の許可および失効の設定」（P.15）（必須）
- 「証明書チェーンの設定」（P.24）（必須）
- 「証明書サーバのハイ アベイラビリティの設定」（P.25）

AAA サーバとの PKI 統合の設定

ピアによって提出された証明書から AAA ユーザ名を生成し、証明書内で AAA データベース ユーザ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。

PKI 許可用に所有者名全体を使用する際の制約事項

authorization username コマンドで所有者名として **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 サーバでは、ユーザ名の長さが制限されます（たとえば、64 文字まで）。その結果、証明書の全体の所有者名は、サーバの制約条件より長くできません。
- 一部の AAA サーバでは、ユーザ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 所有者名とはかぎりません。証明書要求に Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）、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所有者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 サーバが証明書を発行すると、CA サーバは、要求した所有者名フィールドを変更することがあります。たとえば、一部のベンダー製の CA サーバは、要求した所有者名の Relative Distinguished name（RDN; 相対識別名）を CN、OU、O、L、ST、C の順に変更します。ただし、別の CA サーバが、設定された LDAP ディレクトリ ルート（例えば、O=cisco.com）を要求された所有者名の末尾に付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、所有者名の 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）（所有者名）を持つ AAA サーバを対応するユーザ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 url** *url*
7. **revocation-check** *method*
8. **exit**

9. **authorization username** {**subjectname** *subjectname*}
10. **authorization list** *listname*
11. **tacacs-server host** *hostname* [**key** *string*]

    または

    radius-server host *hostname* [**key** *string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** **例：** `Router# 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	**aaa new-model** **例：** `Router(config)# aaa new-model`	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	**aaa authorization network** *listname* [*method*] **例：** `Router (config)# aaa authorization network maxaaa group tacacs+`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。 • *method*：**group radius**、**group tacacs+**、または **group group-name** を指定できます。
ステップ 5	**crypto pki trustpoint** *name* **例：** `Route (config)# crypto pki trustpoint msca`	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	**enrollment url** *url* **例：** `Router (ca-trustpoint)# enrollment url http://caserver.myexample.com`	CA の登録パラメータを指定します。 • *url* 引数は、ルータが証明書要求を送信する CA の URL です。

ステップ 7	`revocation-check method`
	
	例：
	`Router (ca-trustpoint)# revocation-check crl`
		（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	**exit** **例：** `Router (ca-trustpoint)# exit`	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。

	コマンドまたはアクション	目的
ステップ 9	**authorization username** {**subjectname** *subjectname*} **例：** `Router (config)# authorization username subjectname serialnumber`	AAA ユーザ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。 *subjectname* 引数には、次のいずれかを指定できます。 • **all**：証明書の識別名（所有者名）全体 • **commonname**：証明書の通常名 • **country**：証明書の国 • **email**：証明書の E メール • **ipaddress**：証明書の IP アドレス • **locality**：証明書の地域 • **organization**：証明書の組織 • **organizationalunit**：証明書の組織単位 • **postalcode**：証明書の郵便番号 • **serialnumber**：証明書のシリアル番号 • **state**：証明書の州フィールド • **streetaddress**：証明書の所在地 • **title**：証明書のタイトル • **unstructuredname**：証明書の非公式名
ステップ 10	**authorization list** *listname* **例：** `Route (config)# authorization list maxaaa`	AAA 認可リストを指定します。

ステップ 11	**tacacs-server host** *hostname* [**key** *string*]
	
	例：
	`Router(config)# tacacs-server host 192.0.2.2 key a_secret_key`
	
	または
	
	`radius-server host hostname [key string]`
	
	例：
	`Router(config)# radius-server host 192.0.2.1 key another_secret_key`
		TACACS+ ホストを指定します。
		
		または
		
		RADIUS ホストを指定します。

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 サーバ交換との成功した PKI 統合、および AAA サーバ交換との失敗した PKI 統合を示します）。

成功した交換

```
Router# 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_aaalist,
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

```
Router# 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に使用する方式（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 サーバとのナンスおよびピア通信

OCSP を使用すると、OCSP サーバとのピア通信時に、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 サーバ間にセキュアで信頼性の高い通信チャネルが確立されます。

OCSP サーバ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す。詳細は、OCSP サーバのマニュアルを参照してください。

前提条件

- クライアント証明書を発行する前に、サーバで適切な設定（CDP の設定など）を行う必要があります。
- OCSP サーバから CA サーバの失効ステータスを返すように設定するときは、CA サーバが発行した OCSP 応答署名証明書を OCSP サーバ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。

制約事項

- OCSP は、HTTP を使用してメッセージを転送するので、OCSP サーバ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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** **例：** `Router# 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	`crypto pki trustpoint name`
	
	例：
	`Router(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。

	コマンドまたはアクション	目的
ステップ 4	**ocsp url** *url* **例：** `Router(ca-trustpoint)# ocsp url http://ocsp-server`	（任意）OCSP サーバの URL を指定して、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します。この URL によって、証明書の Authority Info Access（AIA）拡張部に指定されている OCSP サーバの URL（存在する場合）が上書きされます。
ステップ 5	**revocation-check** *method1* [*method2* [*method3*]] **例：** `Router(ca-trustpoint)# revocation-check ocsp none`	証明書の失効ステータスをチェックします。 • **crl**：証明書チェックが CRL によって実行されます。これがデフォルトのオプションです。 • **none**：証明書のチェックを無視します。 • **ocsp**：OCSP サーバによって証明書をチェックします。 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（サーバがダウンしている場合など）にだけ使用されます。
ステップ 6	**ocsp disable-nonce** **例：** `Router(ca-trustpoint)# ocsp disable-nonce`	（任意）OCSP サーバ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。
ステップ 7	**exit** **例：** `Router(ca-trustpoint)# 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 8	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 9	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（任意）証明書に関する情報を表示します。
ステップ 10	**show crypto pki trustpoints** [**status** | *label* [**status**]] **例：** `Router# show crypto pki trustpoints`	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。

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。
- **match certificate** コマンド、**skip revocation-check** キーワード、**match certificate** コマンドおよび **allow expired-certificate** キーワードを最初のステップで作成または確認したトラストポイントに追加できます。

（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 サーバ設定の上書き

管理者は、**ocsp url** コマンドを発行して、クライアント証明書の Authority Information Access（AIA）フィールドに指定されている OCSP サーバの設定値を上書きまたは設定できます。**match certificate override ocsp** コマンドを使用すると、複数の OCSP サーバ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 ocsp** 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 **ocsp 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 キャッシュをディセーブルにできます。指定できるのは、**crl-cache delete-after** コマンドまたは **crl-cache none** コマンドだけです。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、**erial-number** フィールドを持つ証明書マップまたは **cert-serial-not** コマンドを使用する AAA アトリビュートのいずれかを使用して設定できます。

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 アトリビュートを使用すると、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。

前提条件

- 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イネーブルにする、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 および AAA サーバ統合を正常に完了して、「証明書ステータスのための PKI と AAA サーバの統合」の手順に従って AAA アトリビュートを使用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. **crl-cache none**

   または

   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*} {*label*}
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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** **例：** `Router# 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	`crypto pki certificate map` *label sequence-number* **例：** `Router(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	*field-name match-criteria match-value* **例：** `Router(ca-certificate-map)# subject-name co MyExample`	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。 *field-name* 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。 • **alt-subject-name** • **expires-on** • **issuer-name** • **name** • **serial-number** • **subject-name** • **unstructured-subject-name** • **valid-start** **（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。 *match-criteria* には、次の論理演算子のいずれかを指定します。 • **co**：含む（名前およびシリアル番号フィールドでのみ有効） • **eq**：等しい（名前、シリアル番号、および日付フィールドで有効） • **ge**：以上（日付フィールドでのみ有効） • **lt**：未満（日付フィールドでのみ有効） • **nc**：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） • **ne**：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） *match-value* は、match-criteria 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。 **（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	**exit** **例：** `Router(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	**crypto pki trustpoint** *name* **例：** `Router(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。

	コマンドまたはアクション	目的

ステップ 7	**crl-cache none**
	
	例：
	`Router(ca-trustpoint)# crl-cache none`
	
	または
	
	crl-cache delete-after *time*
	
	例：
	`Router(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。
		
		crl-cache none 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。
		• *time*：CRL が削除されるまでの時間（分単位）。
		
		crl-cache delete-after 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	**match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**] **例：** `Router(ca-trustpoint)# match certificate Group skip revocation-check`	（任意）証明書ベース ACL（**crypto pki certificate map** 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。 • *certificate-map-label*：**crypto pki certificate map** コマンドで指定された *label* 引数と一致する必要があります。 • **allow expired-certificate**：失効した証明書を無視します。 • **skip revocation-check**：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。 • **skip authorization-check**：AAA サーバとの 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。
ステップ 9	**match certificate** *certificate-map-label* **override cdp** {**url** | **directory**} *string* **例：** `Router(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com`	（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。 • *certificate-map-label*：事前に定義された **crypto pki certificate map** コマンドに指定された *label* 引数と一致する必要があるユーザ指定ラベル。 • **url**：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。 • **directory**：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。 • *string*：URL またはディレクトリ指定。 **（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。

	コマンドまたはアクション	目的
ステップ 10	**match certificate** *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url* **例：** `Router(ca-trustpoint)# match certificate mycertmapname override ocsp trustpoint mytp 15 url http://192.0.2.2`	（任意）OCSP サーバ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。 • *certificate-map-label*：既存の証明書マップ名。 • **trustpoint**：OCSP サーバ証明書を検証するときに使用されるトラストポイント。 • *sequence-number*：**match certificate override ocsp** 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 オーバライド設定が上書きされます。 • **url**：OCSP サーバの URL。 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 **ocsp url** コマンド設定値は、指定された OCSP サーバで上書きされます。 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。 • 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。 • **ocsp url** 設定が存在する場合は、**ocsp url** 設定が引き続きクライアント証明書に適用されます。
ステップ 11	**exit** **例：** `Router(ca-trustpoint)# 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 12	**aaa new-model** **例：** `Router(config)# aaa new-model`	（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	**aaa attribute list** *list-name* **例：** `Router(config)# aaa attribute list crl`	（任意）ルータにローカルで AAA アトリビュート リストを定義し、config-attr-list 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 14	**attribute type** {*name*}{*value*} **例：** `Router(config-attr-list)# attribute type cert-serial-not 6C4A`	（任意）ルータの AAA アトリビュート リストにローカルに追加される AAA アトリビュート 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、*value* フィールドの特定の証明書を、*name* が **cert-serial-not** 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アトリビュート 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。 使用可能な AAA アトリビュート タイプのリストを表示するには、**show aaa attributes** コマンドを実行してください。

ステップ 15	**exit**
	
	例：
	`Router(ca-trustpoint)# exit`
	
	例：
	`Router(config-attr-list)# 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 16	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 17	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（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す。

```
Certificate:
        Data:
            Version: v3
            Serial Number:0x14
            Signature Algorithm:MD5withRSA - 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:(1024 bits) :
                        <snip>

            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:MD5withRSA - 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 ocsp** 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 ocsp 5 url http://192.0.2.3/
show running-configuration
.
.
.
        match certificate map3 override ocsp 5 url http://192.0.2.3/
        match certificate map1 override ocsp 10 url http://192.0.2.1/
        match certificate map2 override ocsp 15 url http://192.0.2.2/
```

次の例は、既存の **match certificate override ocsp** 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 ocsp trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
.
.
.
        match certificate map3 override ocsp trustpoint tp3 5 url http://192.0.2.3/
        match certificate map1 override ocsp trustpoint tp1 10 url http://192.0.2.1/
        match certificate map4 override ocsp trustpoint tp4 10 url
              http://192.0.2.4/newvalue
        match certificate map2 override ocsp 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。

前提条件

- 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。

制約事項

- 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に対して **continue** キーワードとともに設定します。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 trustpoint** *name*
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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** **例：** `Router# 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	`crypto pki trustpoint name`
	
	例：
	`Router(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	**chain-validation** [{**stop** | **continue**} [*parent-trustpoint*]] **例：** `Router(ca-trustpoint)# chain-validation continue ca-sub1`	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。 • **stop** 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。 • **continue** 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。 • *parent-trustpoint* 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。
ステップ 5	**exit** **例：** `Router(ca-trustpoint)# 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。

証明書サーバのハイ アベイラビリティの設定

取り消しコマンドを同期させ、新しい証明書を発行するときにシリアル番号コマンドを送信するように証明書サーバを設定し、アクティブになった場合に証明書と CRL を発行できるように、スタンバイ証明書サーバを準備することができます。

前提条件

証明書サーバのハイ アベイラビリティを確保するには、次の条件を満たす必要があります。

- IPsec 保護された 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、証明書サーバの冗長性モードを ACTIVE/STANDBY に設定する必要があります。

この項目は次のサブ項目から構成されます。

- 「アクティブおよびスタンバイ証明書サーバでの SCTP の設定」（P.25）（必須）
- 「証明書サーバの冗長性モードの ACTIVE/STANDBY の設定」（P.27）（必須）
- 「アクティブ証明書サーバとスタンバイ証明書サーバの同期」（P.29）（必須）

アクティブおよびスタンバイ証明書サーバでの SCTP の設定

この作業は、アクティブおよびスタンバイの両方の証明書サーバで SCTP を設定するためにアクティブ ルータで実行します。

手順の概要

1. **configure terminal**
2. **ipc zone default**
3. **association** *association-ID*
4. **no shutdown**

5. **protocol sctp**
6. **local-port** *local-port-number*
7. **local-ip** *device-real-ip-address [device-real-ip-address2]*
8. **exit**
9. **remote-port** *remote-port-number*
10. **remote-ip** *peer-real-ip-address*
11. スタンバイ ルータに対してステップ 1 ～ 10 を繰り返し、ステップ 7 とステップ 10 で指定したローカル ピアおよびリモート ピアの IP アドレスを逆にします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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 2	**ipc zone default** **例：** `Router(config)# ipc zone default`	デバイス内通信プロトコルである、Inter-Process Communication（IPC）を設定し、IPC ゾーン コンフィギュレーション モードを開始します。 このコマンドを使用して、アクティブ ルータとスタンバイ ルータとの間の通信リンクを開始します。
ステップ 3	**association** *association-ID* **例：** `Router(config-ipczone)# association 1`	2 つのデバイス間におけるアソシエーションを設定し、IPC アソシエーション 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	**no shutdown** **例：** `Router(config-ipczone-assoc)# no shutdown`	サーバ アソシエーションがデフォルトの状態（イネーブル）であることを確認します。
ステップ 5	**protocol sctp** **例：** `Router(config-ipczone-assoc)# protocol sctp`	SCTP をトランスポート プロトコルとして設定し、SCTP プロトコル コンフィギュレーション モードを開始します。
ステップ 6	**local-port** *local-port-number* **例：** `Router(config-ipc-protocol-sctp)# local-port 5000`	冗長ピアとの通信に使用されるローカル SCTP ポート番号を定義して、IPC トランスポート SCTP ローカル コンフィギュレーション モードを開始します。 • *local-port-number*：デフォルト値は存在しません。デバイス内の冗長性をイネーブルにするには、この引数によってローカル ポートの設定を行う必要があります。有効なポート値：1 ～ 65535。 ローカル ポート番号は、ピア ルータ上のリモート ポート番号と同じにする必要があります。

	コマンドまたはアクション	目的
ステップ 7	**local-ip** device-real-ip-address [device-real-ip-address2] **例：** `Router(config-ipc-local-sctp)# local-ip 10.0.0.1`	冗長ペアと通信を行うために使用されるローカル IP アドレスを最低 1 つ定義します。 • ローカル IP アドレスは、ピア ルータ上のリモート IP アドレスと一致している必要があります。1 つまたは 2 つの IP アドレスを指定できます。このアドレスはグローバルな VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）のものである必要があります。仮想 IP アドレスは使用できません。
ステップ 8	**exit** **例：** `Router(config-ipc-local-sctp)# exit`	IPC トランスポート - SCTP ローカル コンフィギュレーション モードを終了します。
ステップ 9	**remote-port** *remote-port-number* **例：** `Router(config-ipc-protocol-sctp)# remote-port 5000`	冗長ピアとの通信に使用されるリモート SCTP ポート番号を定義して、IPC トランスポート SCTP リモート コンフィギュレーション モードを開始します。 **（注）** *remote-port-number*：デフォルト値は存在しません。デバイス内の冗長性をイネーブルにするには、この引数によってリモート ポートの設定を行う必要があります。有効なポート値：1 ～ 65535。リモート ポート番号は、ピア ルータ上のローカル ポート番号と同じにする必要があります。
ステップ 10	**remote-ip** *peer-real-ip-address* **例：** `Router(config-ipc-remote-sctp)# remote-ip 10.0.0.2`	ローカル デバイスとの通信に使用される冗長ピアのリモート IP アドレスを定義します。 すべてのリモート IP アドレスによって同じデバイスが参照される必要があります。 仮想 IP アドレスは使用できません。
ステップ 11	スタンバイ ルータに対してステップ 1 ～ 10 を繰り返し、ステップ 7 とステップ 10 で指定したローカル ピアおよびリモート ピアの IP アドレスを逆にします。	仮想 IP アドレス（10.0.0.3）は、両方のルータで同じになります。

証明書サーバの冗長性モードの ACTIVE/STANDBY の設定

この作業は、証明書サーバの冗長性モードを ACTIVE/STANBY に設定することで、同期をイネーブルにするためにアクティブ ルータで実行します。

1. **configure terminal**
2. **redundancy inter-device**
3. **scheme standby** *standby-group-name*
4. **exit**
5. **interface** *interface-name*
6. **ip address** *ip-address mask*
7. **no ip route-cache cef**
8. **no ip route-cache**
9. **standby ip** *ip-address*

10. **standby priority** *priority*
11. **standby name** *group-name*
12. **standby delay minimum** [*min-seconds*] **reload** [*reload-seconds*]
13. スタンバイ ルータに対してステップ 1 ～ 12 を繰り返し、アクティブ ルータの IP アドレスとは異なる IP アドレスを使用してインターフェイスを設定します（ステップ 6）。
14. **exit**
15. **exit**
16. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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 2	**redundancy inter-device** **例：** `Router(config)# redundancy inter-device`	冗長性を設定し、デバイス内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	**scheme standby** *standby-group-name* **例：** `Router(config-red-interdevice)# scheme standby SB`	使用する冗長性スキームを定義します。 • サポートされているスキームは「standby」だけです。 • *standby-group-name*：**standby name** インターフェイス コンフィギュレーション コマンドで指定したスタンバイ名と一致させる必要があります。また、スタンバイ名は両方のルータで同じである必要があります。
ステップ 4	**exit** **例：** `Router(config-red-interdevice)# exit`	デバイス内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 5	`interface interface-name`
	
	例：
	`Router(config)# interface gigabitethernet0/1`
		ルータのインターフェイス タイプを設定し、インターフェイス 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	**ip address** *ip-address mask* **例：** `Router(config-if) ip address 10.0.0.1 255.255.255.0`	インターフェイスにローカル IP アドレスを設定します。
ステップ 7	**no ip route-cache cef** **例：** `Router(config-if)# no ip route cache cef`	インターフェイスでシスコ エクスプレス フォワーディングの動作をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**no ip route-cache** **例：** `Router(config-if)# no ip route cache`	インターフェイスで高速スイッチングをディセーブルにします。

ステップ 9	`standby ip ip-address`
	
	例：
	`Router(config-if)# standby ip 10.0.0.3`
		Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）をアクティブにします。
		（注） アクティブ ルータおよびスタンバイ ルータに同じアドレスを設定します。

ステップ 10	`standby priority priority`
	
	例：
	`Router(config-if)# standby priority 50`
		HSRP のプライオリティを 50 に設定します。
		指定できるプライオリティの範囲は 1 ～ 255 です。1 は一番低いプライオリティ、255 は一番高いプライオリティを意味します。一番高いプライオリティの値を持つ HSRP グループのルータがアクティブ ルータになります。

ステップ 11	`standby name group-name`
	
	例：
	`Router(config-if)# standby name SB`
		スタンバイ グループの名前を設定します。
		• 名前には、使用されている HSRP グループを指定します。HSRP グループ名はそのルータで一意である必要があります。

ステップ 12	**standby delay minimum** [*min-seconds*] **reload** [*reload-seconds*] **例：** `Router(config-if)# standby delay minimum 30 reload 60`	HSRP グループの初期化の遅延を次のように設定します。 • インターフェイスがアップした後に HSRP グループを初期化するまでの遅延の最小値は 30 秒です。 • ルータがリロードされた後の遅延は 60 秒です。
ステップ 13	スタンバイ ルータに対してステップ 1 ～ 12 を繰り返し、アクティブ ルータのインターフェイスの IP アドレス（ステップ 6）とは異なる IP アドレスを使用して、インターフェイスを設定します。	—
ステップ 14	**exit** **例：** `Router(config-if)# 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 15	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show redundancy states** **例：** `Router# show redundancy states`	（任意）冗長性の状態（スタンバイまたはアクティブ）を確認します。

アクティブ証明書サーバとスタンバイ証明書サーバの同期

この作業は、アクティブ サーバとスタンバイ サーバを同期にするために実行します。

手順の概要

1. **configure terminal**
2. **crypto key generate rsa general-keys redundancy label** *key-label* **modulus** *modulus-size*
3. **exit**
4. **show crypto key mypubkey rsa**
5. **configure terminal**
6. **ip http server**
7. **crypto pki server** *cs-label*
8. **redundancy**
9. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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 2	**crypto key generate rsa general-keys redundancy label** *key-label***modulus** *modulus-size* **例：** `Router (config)# crypto key generate rsa general-keys redundancy label HA modulus 1024`	証明書サーバの HA という名前の RSA キー ペアを生成します。 **（注）** **redundancy** キーワードを指定すると、キーはエクスポート不可能であることを意味します。
ステップ 3	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	**show crypto key mypubkey rsa** **例：** `Router# show crypto key mypubkey rsa`	冗長性がイネーブルであることを確認します。
ステップ 5	**configure terminal** **例：** `Router# 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 6	**ip http server** **例：** `Router(config)# ip http server`	ご使用のシステムの HTTP サーバをイネーブルにします。
ステップ 7	**crypto pki server** *cs-label* **例：** `Router(config)# crypto pki server HA`	ステップ 2 で生成した RSA キー ペアを、証明書サーバのラベルとして指定します。

	コマンドまたはアクション	目的
ステップ 8	**crypto pki server** *cs-label* **redundancy** **例：** `Router (config)# redundancy`	サーバがスタンバイ サーバと同期されていることを確認します。
ステップ 9	**no shutdown** **例：** `Router(cs-server)# no shutdown`	証明書サーバをイネーブルにします。 **（注）** SCRP トラフィックを使用するルータ インターフェイスが保護されていない場合、ハイ アベイラビリティ デバイス間の SCTP トラフィックが IPsec を使用して保護されていることを確認します。

証明書の許可および失効の設定例

ここでは、次の設定例を示します。

PKI AAA 認可の設定および検証：例

ここでは、PKI AAA 認可の設定例を示します。

ルータの設定例

次の **show running-config** コマンド出力は、AAA サーバ機能との 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。

```
Router# 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 1024
 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 AAEEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
  54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078BB
  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 3des
 group 2
!
!
crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
!
```

```
crypto ipsec profile ISC_IPSEC_PROFILE_2
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set ISC_TS_1
!
!
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
```

成功した PKI AAA 認可のデバッグ例

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

```
Router# 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

Router#
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
Router#
Router#
May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 192.0.2.171 (Tunnel0) is
up: new adjacency
Router#

Router# show crypto isakmp sa

dst             src             state          conn-id slot
192.0.2.22    192.0.2.102   QM_IDLE             84    0
```

失敗した PKI AAA 認可のデバッグ例

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。

```
Router# 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

Router#
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)
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_INVAL_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_INVAL_CERT: Certificate received from 192.0.2.162 is
bad: certificate invalid
Router#

Router# show crypto iskmp sa

dst             src             state          conn-id slot
192.0.2.2       192.0.2.102   MM_KEY_EXCH         95    0
```

失効メカニズムの設定：例

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。

- 「OCSP サーバの設定例」（P.36）
- 「CRL および OCSP サーバの指定例」（P.36）

OCSP サーバの設定例

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

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

CRL および OCSP サーバの指定例

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。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

OCSP サーバの設定例

次の例では、HTTP URL「http://myocspserver:81」にある OCSP サーバを使用するようにルータを設定する方法を示します。このサーバがダウンしている場合、失効チェックは無視されます。

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

OCSP サーバとの通信でのナンスのディセーブル例

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。

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

セントラル サイトにあるハブ ルータを証明書失効チェック用に設定する例

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
```

セントラル サイトのハブ ルータ

```
Router# 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。

```
Router# 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。

```
Router (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されています（「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所有者名です。

cn=Central VPN Gateway

o=Home Office Inc

```
Router (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。

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

```
Router# 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、発行者名の行と所有者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
 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（引数とキーワード）**を使用しない場合、ブランチ オフィスは、CRL または AAA サーバのチェックを完了するまでトンネルを確立できません（**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かぎり、トンネルは確立されません）。

ブランチ サイトにあるルータ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** キーワードを使用します。

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

```
Router# 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: 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。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# crypto pki certificate map branch1 10
Router (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.
Router (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。

```
Router (ca-certificate-map)# crypto pki trustpoint VPN-GW
Router (ca-trustpoint)# match certificate branch1 allow expired-certificate
Router (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）。

```
Router# 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。

証明書の許可および失効の設定：例

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」（P.40）
- 「証明書のシリアル番号セッション コントロールの設定」（P.41）

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。

```
Router# 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、キャッシュはディセーブルになります。**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。

```
Router# 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、**crl-cache delete-after** コマンドが有効になります。この新しくキャッシュされた CRL とそれに続くすべての CRL は、2 分の最大ライフタイムの後に削除されます。

show crypto pki crls コマンドを実行すると、CRL が 2 分間キャッシュされることを確認できます。NextUpdate の時間が LastUpdate の時間の 2 分後であることに注意してください。

```
Router# 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 アトリビュート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す。

```
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 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: 'PKIAAA'
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, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x4)
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_INVAL_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
.
.
.
```

証明書チェーン検証の設定：例

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」（P.43）
- 「ピアから下位 CA への証明書チェーン検証の設定」（P.43）
- 「証明書チェーンの欠落確認の設定」（P.44）

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
 rsakeypair RootCA

crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1

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

crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1


crypto pki trustpoint SubCA11
 enrollment terminal
```

```
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair 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
 rsakeypair RootCA

crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA11
```

証明書サーバのハイ アベイラビリティの設定：例

次の例では、SCTP の設定、アクティブおよびスタンバイ証明書サーバの冗長性の設定、およびこれらのサーバ間の同期のアクティブ化を示します。

アクティブ ルータ

```
ipc zone default
 association 1
 no shutdown
 protocol sctp
  local-port 5000
   local-ip 10.0.0.1
   exit
  remote-port 5000
   remote-ip 10.0.0.2
```

スタンバイ ルータ

```
ipc zone default
 association 1
 no shutdown
 protocol sctp
  local-port 5000
   local-ip 10.0.0.2
   exit
  remote-port 5000
   remote-ip 10.0.0.1
```

アクティブ ルータ

```
redundancy inter-device
 scheme standby SB
```

```
interface GigabitEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache

 standby 0 ip 10.0.0.3
 standby 0 priority 50
 standby 0 name SB
 standby delay min 30 reload 60
```

スタンバイ ルータ

```
redundancy inter-device
 scheme standby SB

interface GigabitEthernet0/1
 ip address 10.0.0.2 255.255.255.0
 no ip route-cache cef
 no ip route-cache

 standby 0 ip 10.0.0.3
 standby 0 priority 50
 standby 0 name SB
 standby delay min 30 reload 60
```

アクティブ ルータ

```
crypto pki server mycertsaver
crypto pki server mycertsaver redundancy
```

その他の参考資料

ここでは、PKI 証明書の許可および失効に関する関連資料について説明します。

関連資料

内容	参照先
PKI コマンド：完全なコマンドの構文、コマンドモード、デフォルト、使用上の注意事項、例	『*Cisco IOS Security Command Reference*』
PKI の概要（RSA キー、証明書登録、および CA を含む）	「Cisco IOS PKI Overview: Understanding and Planning a PKI」の章
RSA キーの生成および展開	「Deploying RSA Keys Within a PKI」の章
証明書登録：サポートされる方法、登録プロファイル、設定作業	「Configuring Certificate Enrollment for a PKI」の章
Cisco IOS 証明書サーバの概要および設定作業	「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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。	http://www.cisco.com/techsupport

証明書の許可および失効に関する機能情報

表 2 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「Implementing and Managing PKI Features Roadmap」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 2　PKI 証明書の許可および失効に関する機能情報

機能名	リリース	機能情報
認証失効リストのキャッシュ コントロール拡張機能	12.4(9)T	この機能を使用すると、ユーザは CRL キャッシングをディセーブルにしたり、ルータのメモリに CRL がキャッシュされる最大ライフタイムを指定したりできます。この機能は、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の機能も提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「CRL とは」 • 「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の設定：例」 この機能により、**crl-cache delete-after**、**crl-cache none**、**crypto pki certificate map** の各コマンドが導入または変更されました。
Certificate-Complete チェーンの検証	12.4(6)T	この機能を使用すると、すべての証明書（下位 CA 証明書を含む）で証明書チェーンが処理されるレベルを設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「PKI 証明書チェーンの検証」 • 「証明書チェーンの設定」 • 「証明書チェーン検証の設定：例」 この機能により、次のコマンドが導入されました。 **chain-validation**
OCSP：代替階層からのサーバ認証	12.4(6)T	この機能は、複数 OCSP サーバ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できる柔軟性を備えています。また、この機能を使用すると、外部の CA 証明書または自己署名証明書に基づいて OCSP サーバを検証できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OCSP とは」 • 「証明書の許可および失効の設定」 この機能により、**match certificate override ocsp** コマンドが導入されました。

表 2　PKI 証明書の許可および失効に関する機能情報 （続き）

機能名	リリース	機能情報
オプションの OCSP ナンス	12.2(33)SR 12.4(4)T	この機能では、OCSP 通信時にナンス（OCSP 要求に関する固有識別情報）を送信するように設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OCSP とは」 • 「PKI 証明書ステータス チェックの失効メカニズムの設定」 • 「OCSP サーバとの通信でのナンスのディセーブル例」
証明書のセキュリティ アトリビュート ベースのアクセス コントロール	12.2(15)T 1	IPsec プロトコルでは、CA の相互運用性により、Cisco IOS デバイスと CA が通信を行い、Cisco IOS デバイスは、CA からデジタル証明書を取得し、使用できるようになります。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。この機能により、ACL の指定が可能な証明書にフィールドを追加し、証明書ベース ACL を作成できます。 この機能に関する詳細については、次の各項を参照してください。 • 「許可または失効用に証明書ベースの ACL を使用する場合」 • 「証明書の許可および失効の設定」 この機能により、次のコマンドが導入または変更されました。**crypto pki certificate map**、**crypto pki trustpoint**、**match certificate**
Online Certificate Status Protocol（OCSP）	12.3(2)T	この機能により、CRL の代わりに OCSP をイネーブルにして、証明書のステータスをチェックできます。証明書のステータスを定期的に提供するだけの CRL とは異なり、OCSP では証明書ステータスに関する情報をタイムリーに利用できます。 この機能に関する詳細については、次の各項を参照してください。 • 「CRL または OCSP サーバ：証明書失効メカニズムの選択」 • 「PKI 証明書ステータス チェックの失効メカニズムの設定」 この機能により、**ocsp url** および **revocation-check** コマンドが導入されました。

表 2　PKI 証明書の許可および失効に関する機能情報 （続き）

機能名	リリース	機能情報
所有者名全体を使用した PKI AAA 認可	12.3(11)T	この機能により、ユーザは、所有者名全体を一意の AAA ユーザ名として使用し、証明書から AAA サーバを照会できます。 この機能に関する詳細については、次の各項を参照してください。 • 「PKI と AAA サーバ統合用のアトリビュート値ペア」 • 「AAA サーバとの PKI 統合の設定」 この機能により、**authorization username** コマンドが変更されました。
AAA サーバとの PKI 統合	12.3(1)	この機能では、ピアによって提出された証明書から AAA ユーザ名を生成することにより、許可に関するスケーラビリティが向上します。AAA サーバは、内部コンポーネントでの証明書の使用を許可するか決定するよう尋ねられます。許可は、コンポーネントで指定されたラベルによって示され、このラベルはユーザの AV ペアに存在している必要があります。 この機能に関する詳細については、次の各項を参照してください。 • 「証明書ステータスのための PKI と AAA サーバの統合」 • 「AAA サーバとの PKI 統合の設定」 この機能により、**authorization list** および **authorization username** コマンドが導入されました。
PKI：証明書失効チェック時の複数のサーバ照会	12.3(7)T	Cisco IOS ソフトウェアではこの機能により、特定のサーバが利用できない場合に操作を続行できるように CRL の取得を複数回試行できます。また、証明書の CDP を、手動で設定した CDP で上書きすることもできます。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。 この機能に関する詳細については、次の各項を参照してください。 • 「失効チェック中にすべての CDP を照会」 • 「証明書内の CDP の手動による上書き」 この機能により、**match certificate override odp** コマンドが導入されました。

表 2　PKI 証明書の許可および失効に関する機能情報 （続き）

機能名	リリース	機能情報
証明書 ACL を使用して失効チェックおよび失効した証明書の無視	12.3(4)T	この機能により、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。証明書 ACL は、証明書を受け入れるために満たす必要がある基準を指定する場合や、失効チェックを回避する場合に使用されます。さらに、AAA 通信が証明書によって保護されている場合、この機能は無視される証明書に対して AAA チェックを実行します。 この機能に関する詳細については、次の各項を参照してください。 • 「証明書ベース ACL を使用した失効チェックの無視」 • 「失効チェックを無視するように証明書ベース ACL を設定」 この機能により、**match certificate** コマンドが変更されました。
トラストポイントごとのクエリー モードの定義	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。
PKI ハイ アベイラビリティ	15.0(1)M	次のコマンドが導入または変更されました。**crypto pki server**、**crypto pki server start**、**crypto pki server stop**、**crypto pki trustpoint**、**crypto key generate rsa**、**crypto key import pem**、**crypto key move rsa**、**show crypto key mypubkey rsa**