Cisco での証明書の管理 ISE-PIC

証明書は、個人、サーバ、会社、またはその他のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。公開キーインフラストラクチャ（PKI）は、セキュアな通信を可能にし、デジタル署名を使用してユーザのIDを確認する暗号化技術です。証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。証明書は、自己署名するか、外部の認証局（CA）がデジタル署名できます。自己署名証明書は、独自の作成者によって署名されます。CA 署名付きデジタル証明書は業界標準と見なされており、より安全です。ISE-PIC は pxGrid の外部 CA として機能し、pxGrid サブスクライバの pxGrid 証明書にデジタル署名できます。

Cisco ISE-PICは、ノード間通信（各ノードが相互に通信するためにもう一方のノードに証明書を提示する）や pxGrid との通信（ISE-PIC と pxGrid が相互に証明書を提示する）のために証明書を使用します。これら2つの目的それぞれに、1つの証明書をノードごとに生成できます。証明書は pxGrid に対して Cisco ISE ノードを識別し、pxGrid と Cisco ISE ノード間の通信を確保します。

インストール時に、ISE-PIC は ISE-PIC ノードごとの自己署名証明書（インストール時に管理者はプライマリノードからセカンダリノーそに対して自動的に生成された証明書を承認するように求められます）と、プライマリ ISE-PIC ノードによってデジタル署名されたpxGridサービス用の証明書が自動的に生成されます。その後、pxGridとサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE-PIC からサブスクライバにユーザ ID を渡すことが可能になります。ISE-PIC の [証明書（Certificate）] メニューは、証明書の表示、追加の ISE-PIC 証明書の生成、および一部の高度なタスクの実行に使用できます。

（注） 管理者は企業証明書を使用できますが、デフォルトでは、サブスクライバの pxGrid 証明書の発行には内部認証局を使用するように ISE-PIC は設計されています。

Cisco ISE-PIC の証明書の一致

展開内でCisco ISE-PIC ノードをセットアップすると、2つのノードが相互に通信します。システムは各 ISE-PIC ノードの FQDN を調べ、FQDN が一致することを確認します（たとえば ise1.cisco.com と ise2.cisco.com、またはワイルドカード証明書を使用している場合は *.cisco.com）。また、外部マシンから ISE-PIC サーバに証明書が提示される場合、認証のために提示される外部証明書が、ISE-PIC サーバの証明書と照合されます。2 つの証明書が一致すると、認証は成功します。

Cisco ISE-PIC は、サブジェクト名の一致を次のようにして確認します。

1. Cisco ISE-PIC により証明書のサブジェクト代替名（SAN）の拡張が確認されます。SAN に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカード ドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. SAN に DNS 名が存在しない場合、または SAN 全体が欠落している場合は、証明書の [サブジェクト（Subject）]フィールドの一般名（CN）または証明書の[サブジェクト（Subject）]フィールドのワイルドカード ドメインが、ノードの FQDN に一致している必要があります。
3. 一致しない場合、証明書は拒否されます。

ワイルドカード証明書

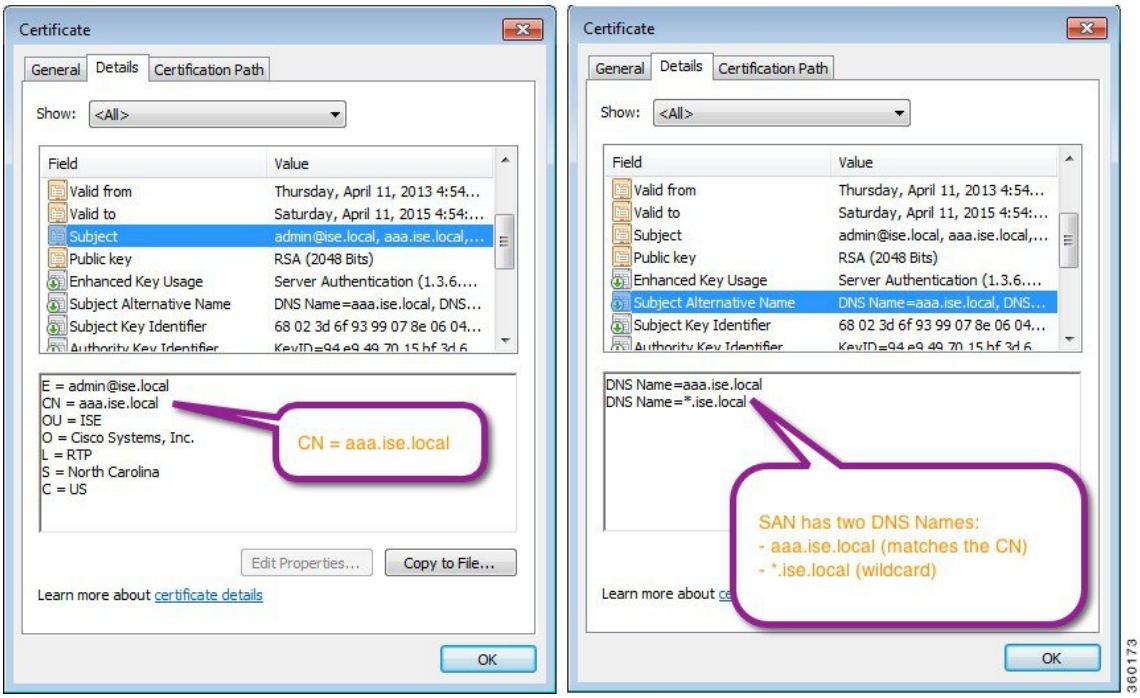
ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用し、組織の複数のホスト間で証明書を共有できるようにします。たとえば、証明書サブジェクトの CN 値は aaa.ise.local などの汎用ホスト名であり、SAN フィールドには、同じ汎用ホスト名と DNS.1=aaa.ise.local および DNS.2=*.ise.local などのワイルドカード表記が含まれます。

psn.ise.local. のように *.ise.local を使用してワイルドカード証明書を設定すると、その同じ証明書を使用して、次のようなDNS名が「.ise.local」で終了する他のすべてのホストを保護することができます。

ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

次の図に、Web サイトの保護に使用されるワイルドカード証明書の例を示します。

図 *1*：ワイルドカード証明書の例



SAN フィールドでアスタリスク（*）を使用すると、（2 つのノードをインストールしている場合は）両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

（注） FQDN の例の一部は、ISE のフル インストールの例であるため、ISE-PIC インストールに関連するアドレスとは異なることがあります。

ワイルドカード証明書を使用する利点

- コスト削減。サードパーティの認証局によって署名された証明書には高額な費用がかかります（特にサーバ数が多い場合）。ワイルドカード証明書は、Cisco ISE 展開内の複数ノードで使用できます。
- 運用の効率化。ワイルドカード証明書は、すべてのポリシー サービス ノード（PSN）EAP および Web サービスが同じ証明書を共有することを可能にします。証明書を 1 回作成して、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。
- 認証エラーの低減。ワイルドカード証明書は、クライアントがプロファイル内に信頼された証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライ

アントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼された認証局が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。

- 簡素化されたサプリカントの設定。たとえば、PEAP-MSCHAPv2 およびサーバ証明書の信頼が有効になっている Microsoft Windows サプリカントで、各サーバ証明書を信頼するように指定することが必要とされており、そのように指定されていない場合、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザにプロンプトが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバ証明書を信頼するだけで済みます。
- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザ エクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書は ISE ノードごとの固有のサーバ証明書よりも安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティ リスクに勝っています。

ASA などのセキュリティ デバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を展開する場合には注意が必要です。たとえば、*.company.local を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は company.local ドメイン内のすべてのサーバをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベストプラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク（*）を追加します。

たとえば、*.ise.company.local に対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は通常、証明書サブジェクトの一般名（CN）としてリストされているワイルドカードを使用して作成されます。Cisco ISE は、このタイプの作成をサポートします。ただし、すべてのエンドポイントサプリカントが証明書サブジェクトのワイルドカード文字をサポートするわけではありません。

テスト済みのすべての Microsoft ネイティブ サプリカント（Windows Mobile を含む）の一部は、証明書のサブジェクトのワイルドカード文字をサポートしていません。

Cisco AnyConnect Network Access Manager（NAM）など、[サブジェクト（Subject）] フィールドでのワイルドカード文字の使用をサポートできる他のサプリカントを使用することができます。

また、DigiCert の Wildcard Plus など、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoftサプリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoft のネイティブ サプリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

このためには、サブジェクトにワイルドカードを使用する代わりに、[Subject Alterative Name (SAN)] フィールドでワイルドカード文字を使用します。SAN フィールドはドメイン名（DNS 名）を検査するように設計された拡張を保持します。詳細については、RFC 6125 および 2128 を参照してください。

ISE-PIC での証明書階層

ISE-PICから、すべての証明書の証明書階層または信頼書トラスト チェーンを表示できます。証明書階層には、証明書、すべての中間認証局（CA）の証明書、およびルート証明書が含まれています。たとえば、ISE-PIC からシステム証明書を表示すると、デフォルトでは該当するシステム証明書の詳細が表示されます。証明書階層は、証明書の上部に表示されます。詳細を表示するには、その階層で証明書をクリックします。自己署名証明書には階層または信頼チェーンがありません。

証明書のリスト ページで、[ステータス（Status）] 列に次のアイコンのいずれかが表示されます。

- 緑色のアイコン：有効な証明書（有効な信頼チェーン）を示します
- 赤色のアイコン：エラーを示します（たとえば、信頼証明書の欠落または期限切れ）
- 黄色のアイコン：証明書が期限切れ間近であることを警告し、更新処理を求めます

システム証明書

Cisco ISE-PIC システム証明書は、展開内のその他のノードおよびクライアントアプリケーションに対して Cisco ISE-PIC ノードを識別するサーバ証明書です。システム証明書にアクセスするには、**[証明書（Certificates）]** > **[システム証明書（System Certificates）]** を選択します。システム証明書の用途は次のとおりです。

- Cisco ISE-PIC 展開でノード間通信に使用されます。この証明書の場合、[使用方法（Usage）] フィールドで [管理（Admin）] オプションを選択します。
- pxGrid コントローラとの通信に使用されます。この証明書の場合、[使用方法（Usage）] フィールドで [pxGrid] オプションを選択します。

Cisco ISE-PIC 展開で、各ノードで有効なシステム証明書をインストールする必要があります。デフォルトでは、インストール時に Cisco ISE-PIC ノードに 2 つの自己署名証明書と、内部 Cisco ISE CA により署名された 1 つの証明書が作成されます。

- [管理（Admin）] および [pxGrid] を使用するための自己署名サーバ証明書（キー サイズは 2048 で 1 年間有効です）。
- SAML IdP との安全な通信に使用できる自己署名 SAML サーバ証明書（キー サイズは 2048 で 1 年間有効です）。
- pxGrid クライアントとの安全な通信に使用できる内部 Cisco ISE CA 署名付きサーバ証明書（キー サイズは 4096 で 1 年間有効です）。

展開をセットアップし、セカンダリ ノードを登録すると、pxGrid コントローラ用の証明書が自動的にプライマリ ノードの CA 署名付き証明書に置き換わります。したがってすべての pxGrid 証明書が同一 PKI トラスト階層の一部となります。

（注） お使いのリリースでサポートされているキーと暗号情報を確認するには、適切なバージョンの『Cisco Identity Services Engine Network Component Compatibility』ガイドを参照してください。

セキュリティを強化するために、自己署名証明書を CA 署名付き証明書で置き換えることを推奨します。CA 署名付き証明書を取得するには、以下を行う必要があります。

1. 証明書署名要求の作成と認証局への CSR の送信 （19 ページ）
2. 信頼できる証明書ストアへのルート証明書のインポート （16 ページ）
3. CSR への CA 署名付き証明書のバインド （19 ページ）

システム証明書の表示

[システム証明書（System Certificate）] ページに、Cisco ISE-PIC に追加されたすべてのシステム証明書が一覧表示されます。

ステップ 1 **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** を選択します。。

[システム証明書（System Certificate）]ページが表示されます。このページには、システム証明書に関する次の情報が表示されています。

- [フレンドリ名（Friendly Name）]：証明書の名前。
- [使用者（Used By）]：この証明書が使用されるサービス。
- [ポータル グループ タグ（Portal group tag）]：ポータルを使用するように指定された証明書に対してのみ適用できます。どの証明書をポータルに使用しなければならないかを指定します。
- [発行先（Issued To）]：証明書のサブジェクトの一般名。
- [発行元（Issued By）]：証明書発行者の一般名
- [有効期限の開始（Valid From）]：証明書の作成日付（Not Before 証明書属性）。
- [期限日（Expiration Date）]：証明書の有効期限（Not After 証明書属性）。証明書の有効期限を示します。ここには、アイコンが関連付けられた 5 つのカテゴリがあります。
  - [91 日以上で期限切れ（Expiring in more than 90 days）]（緑のアイコン）
  - [90 日以内に期限切れ（Expiring in 90 days or less）]（青のアイコン）
  - [60 日以内に期限切れ（Expiring in 60 days or less）]（黄色のアイコン）
  - [30 日以内に期限切れ（Expiring in 30 days or less）]（オレンジのアイコン）
  - [期限切れ（Expired）]（赤のアイコン）

ステップ 2 証明書を選択し、[表示（View）] を選択して証明書の詳細を表示します。

システム証明書のインポート

管理者ポータルから、任意の Cisco ISE-PIC ノードのシステム証明書をインポートできます。

（注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ管理ノード（PAN）の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

始める前に

- クライアント ブラウザを実行しているシステムに、システム証明書と秘密キー ファイルがあることを確認します。

- インポートするシステム証明書が外部 CA によって署名されている場合は、関連するルート CA および中間 CA の証明書を信頼できる証明書ストアにインポートします（[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）。
- インポートするシステム証明書に、CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

ステップ 1 **[証明書（Certificates）] > [システム証明書（Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。
[サーバ証明書のインポート（Import Server Certificate）] 画面が表示されます。

ステップ 3 インポートする証明書の値を入力します。

ステップ 4 **[送信（Submit）]** をクリックします。

自己署名証明書の生成

自己署名証明書を生成することにより、新しいローカル証明書を追加できます。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE-PIC を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE-PIC ノードのホスト名を変更する必要がある場合は、Cisco ISE-PIC ノードにログインし、古いホスト名が使用された自己署名証明書を削除し、新しい自己署名証明書を生成します。そうしないと、Cisco ISE-PIC は古いホスト名が使用された自己署名証明書を引き続き使用します。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。。

ステップ 2 [自己署名証明書の生成（Generate Self Signed Certificate）] をクリックし、[自己署名証明書の生成（Generate Self Signed Certificate）] ページに詳細を入力します。

ステップ 3 自己署名したワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）を生成する場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。

ステップ 4 この証明書を使用するサービスに基づいて [使用方法（Usage）] 領域のチェックボックスをオンにします。

ステップ 5 証明書を生成するには、[送信（Submit）] をクリックします。

CLI からセカンダリ ノードを再起動するには、指定された順序で次のコマンドを入力します。

a) **application stop ise**

b) **application start ise**

システム証明書の編集

このページを使用して、システム証明書を編集し、自己署名証明書を更新できます。ワイルドカード証明書を編集すると、変更が展開内のすべてのノードに複製されます。ワイルドカード証明書を削除した場合、そのワイルドカード証明書は展開内のすべてのノードから削除されます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 自己署名証明書を更新するには、[更新期間（Renewal Period）] チェックボックスをオンにして、有効期限 TTL（存続可能時間）を日、週、月、または年単位で入力します。

ステップ 4 [Save（保存）] をクリックして変更内容を保存します。

[管理者（Admin）] チェックボックスがオンになっている場合、Cisco ISE-PIC ノードのアプリケーションサーバが再起動されます。

（注） Chrome 65 以上を使用して ISE を起動すると、URL が正しくリダイレクトされたにもかかわらず、BYOD ポータルまたはゲスト ポータルがブラウザで起動に失敗することがあります。これは、すべての [サブジェクトの別名（Subject Alternative Name）] フィールドに証明書を必要とする、Google で導入された新しいセキュリティ機能が原因です。ISE 2.4 以降のリリースの場合、[サブジェクトの別名（Subject Alternative Name）] フィールドを入力する必要があります。

Chrome 65 以上で起動するには、次の手順に従います。

1. [サブジェクトの別名（Subject Alternative Name）] フィールドに入力することで、ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。

2. ISE サービスが再起動します。

3. Chrome ブラウザでポータルにリダイレクトされます。

4. ブラウザで [証明書の表示（View Certificate）] > [詳細（Details）] > [コピー（Copy）] の順に選択し、base-64 エンコードを選択して、証明書をコピーします。

5. 高信頼パスで証明書をインストールします。

6. Chrome ブラウザを終了し、ポータルのリダイレクトを試みます。

（注） Win RS4 または RS5 のオペレーティング システムでブラウザ Firefox 64 以降のワイヤレス BYODセットアップを設定する場合は、証明書の例外を追加することができない場合があります。この現象は Firefox 64 以降の新規インストール時に発生することがあります。以前のバージョンから Firefox 64 以降にアップグレードした場合は発生しません。次の手順では、このような場合でも証明書の例外を追加することができます。

1. BYOD フローのシングル/デュアル PEAP または TLS を設定します。

2. Windows のすべてのオプションで CP ポリシーを設定します。

3. エンド クライアント Windows RS4/RS5 で Dot1.x/MAB SSID に接続します。

4. ゲスト/BYOD ポータルにリダイレクトするために、FF64 ブラウザに 1.1.1.1 と入力します。

5.**[例外を追加（Add Exception）] > [証明書を追加できない（Unable to add certificate）]** をクリックし、フローを続行します。

これを回避するには、**[オプション（Options）]** > **[プライバシーと設定（Privacy & Settings）]** > **[証明書の表示（View certificates）]** > **[サーバ（Servers）]** > **[例外を追加（Add Exception）]** に移動して、Firefox 64 に証明書を手動で追加する必要があります。

システム証明書の削除

今後使用しないシステム証明書を削除できます。

システム証明書ストアから複数の証明書を一度に削除できますが、管理認証に使用できる証明書を少なくとも 1 つ所有する必要があります。また、管理または pxGrid コントローラに使用される証明書は削除できません。ただし、サービスがディセーブルの場合は、pxGrid 証明書を削除できます。

ワイルドカード証明書を削除することを選択した場合、証明書は展開内のすべてのノードから削除されます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

システム証明書のエクスポート

選択したシステム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント 値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカード システム証明書をエクスポートしてノード間通信用に他のノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE-PIC ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）] をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は Privacy Enhanced Mail 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は Privacy Enhanced Mail 形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

信頼できる証明書ストア

信頼できる証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol（SCEP）用の X.509 証明書が含まれています。

X.509 証明書が有効なのは、指定された特定の日付までのみです。システム証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、システム証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、[システム証明書（System Certificates）] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 有効期限のアラームは、有効期限の 90 日前、60 日前に生成され、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。CA 署名付き証明書の場合は、CA から新しい証明書を取得するのに十分な期間を確保する必要があります。

Cisco ISE は、次の目的で信頼できる証明書を使用します。

- エンドポイントによる認証と、証明書ベースの管理者認証を使用してISE-PICにアクセスする Cisco ISE 管理者による認証に使用するクライアント証明書を確認するため。
- 展開内の Cisco ISE-PIC ノード間のセキュアな通信を可能にするため。信頼できる証明書ストアには、展開内の各ノードのシステム証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
  - 自己署名証明書をシステム証明書に使用する場合は、各ノードの自己署名証明書を PAN の信頼できる証明書ストアに配置する必要があります。
  - CA 署名付き証明書をシステム証明書に使用する場合は、CA ルート証明書だけでなく、信頼チェーン内のすべての中間証明書も PAN の信頼できる証明書ストアに配置する必要があります。

（注）
- Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail（PEM）または Distinguished Encoding Rules（DER）形式である必要があります。証明書チェーン（システム証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。
- ゲスト ポータルにパブリック ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、ISE サービスが再起動されるまで証明書チェーンは送信されません。

インストール時に、自動的に生成された信頼できる証明書が、信頼できる証明書ストアに取り込まれます。ルート証明書（Cisco Root CA）は、製造業者（Cisco CA Manufacturing）証明書に署名します。

信頼できる証明書の命名の制約

CTL の信頼できる証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

次の名前の制約がサポートされています。

- ディレクトリ名

  ディレクトリ名の制限は、サブジェクト/SAN のディレクトリ名のプレフィクスです。次の例を参考にしてください。

  - 正しいサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

    クライアント証明書のサブジェクト：O=Cisco,CN=Salomon

  - 不正なサブジェクト プレフィクス：

CA 証明書の名前の制約：Permitted: O=Cisco

クライアント証明書のサブジェクト：CN=Salomon,O=Cisco

- DNS
- E-mail
- URI（URI の制約は、http://、https://、ftp://、または ldap:// のような URI プレフィクスで始まる必要があります）。

次の名前の制約はサポートされていません。

- IP アドレス
- Othername

信頼できる証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

信頼できる証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                 DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100

                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
           Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

信頼できるストア証明書の表示

[信頼できる証明書（Trusted Certificates）] ページに、Cisco ISE-PIC に追加されたすべての信頼できる証明書が一覧表示されます。

すべての証明書を表示するには、**[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。[信頼できる証明書（Trusted Certificates）] ページが表示され、すべての信頼できる証明書が一覧表示されます。

信頼できる証明書ストアの証明書のステータス変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE-PIC が信頼の確立にこの証明書を使用できるようになります。証明書が信頼できる証明書ストアにインポートされると、この証明書は自動的に有効になります。

ステップ 1 **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 有効または無効にする証明書の隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 ステータスを変更します。

ステップ 4 [保存（Save）] をクリックします。

信頼できる証明書ストアへの証明書の追加

[証明書ストア（Certificate Store）] ページを使用して、Cisco ISE-PIC に CA 証明書を追加することができます。

始める前に

- ブラウザを実行しているコンピュータのファイル システムに、証明書ストアの証明書が存在することを確認します。証明書は PEM または DER 形式である必要があります。
- Admin 認証または EAP 認証に証明書を使用する場合は、基本制約が証明書に定義され、CA フラグが true に設定されていることを確認します。

ステップ 1 **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 必要に応じてフィールドの値を設定します。

EAP認証用または証明書ベースの管理者認証用に証明書チェーンにサブCA証明書を使用する場合は、ルート CA までに証明書チェーンにすべての証明書をインポートする際に [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）] チェックボックスを必ずオンにしてください。CISCO ISE 2.4 パッチ 8 以降、同じサブジェクト名を持つ複数の CA 証明書をインポートできます。証明書ベースの管理者認証の場合は、信頼できる証明書を追加する際に、[証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）] チェックボックスをオンにします。同じサブジェクトを持つ別の証明書がストアにあり、[証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）] チェックボックスが有効になっている場合、信頼できるストアの証明書の [証明書ベースの管理者認証用に信頼する（Trust for certificate based admin authentication）] オプションは変更できません。

パスワードベースの認証から証明書ベースの認証に認証タイプを変更すると、Cisco ISE-PIC は展開内の各ノードでアプリケーション サーバを再起動します。PAN のアプリケーション サーバから開始されます。

信頼できる証明書の編集

証明書を信頼できる証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

ステップ 1 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 必要に応じて編集可能なフィールドを変更します。

ステップ 4 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

信頼できる証明書の削除

今後使用しない信頼できる証明書を削除できます。ただし、ISE-PIC 内部 CA（認証局）の証明書は削除しないでください。ISE-PIC 内部 CA 証明書を削除できるのは、展開全体の ISE-PIC ルート証明書チェーンを置き換える場合のみです。

ステップ 1 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。ISE-PIC 内部 CA 証明書を削除することを選択した場合は、次のとおりにクリックします。

- [削除（Delete）]：ISE-PIC 内部 CA 証明書を削除する場合。ISE-PIC 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。エンドポイントをネットワークで再度有効にするには、信頼できる証明書ストアに同じ ISE-PIC 内部 CA 証明書をインポートします。
- [削除および取消（Delete & Revoke）]：ISE-PIC 内部 CA 証明書を削除して取り消します。ISE-PIC 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。この操作は取り消すことができません。展開全体の ISE-PIC ルート証明書チェーンを置き換える必要があります。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

信頼できる証明書ストアからの証明書のエクスポート

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） 内部 CA から証明書をエクスポートし、そのエクスポートを使用してバックアップから復元する場合は、CLI コマンド `application configure ise` を使用する必要があります。詳細については、Cisco ISE CA 証明書およびキーのエクスポート （32 ページ）を参照してください。

ステップ 1 **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。.

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

信頼できる証明書ストアへのルート証明書のインポート

ルート CA 証明書および中間 CA 証明書をインポートするとき、信頼できる CA 証明書を使用する対象のサービスを指定できます。

始める前に

CSR に署名し、デジタルで署名された CA 証明書を返した認証局のルート証明書および他の中間証明書が必要です。

ステップ 1 **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 表示された [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、[ファイルの選択（Choose File）] をクリックし、CA によって署名され、返されたルート CA 証明書を選択します。

ステップ 4 **わかりやすい名前**を入力します。

わかりやすい名前を入力しないと、Cisco ISE-PIC により、このフィールドには、*common-name#issuer#nnnnn* 形式（、*nnnnn* は一意の番号）で名前が自動的に入力されます。再度証明書を編集して、**わかりやすい名前**を変更できます。

ステップ 5 この信頼できる証明書を使用するサービスの横にあるチェックボックスをオンにします。

ステップ 6 （任意）[説明（Description）] フィールドに証明書の説明を入力します。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

信頼できる証明書ストアに中間 CA 証明書をインポートします（該当する場合）。

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は Privacy-Enhanced Mail（PEM）の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CA によって発行されたクライアントまたはサーバ証明書である必要があります。
- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 ステップのプロセスです。

1. 管理者ポータルで信頼できる証明書ストアに証明書チェーン ファイルをインポートします。この操作により、信頼できる証明書ストアにある最後の 1 つを除き、すべての証明書がファイルからインポートされます。
2. CA 署名付き証明書のバインド操作を使用して証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてファイルからインポートされます。

信頼できる証明書のインポート設定

次の表では、認証局（CA）証明書を Cisco ISE-PIC に追加するために使用できる [信頼できる証明書のインポート（Trusted Certificate Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** > **[インポート（Import）]** です。

表 *1*: 信頼できる証明書のインポート設定

フィールド	説明
証明書ファイル（Certificate file）	[参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE-PIC により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。

フィールド	説明
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書を（他の ISE-PIC ノードまたは LDAP サーバから）サーバ証明書の検証に使用する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE-PIC 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE-PIC に接続するエンドポイントの認証 • syslog サーバの信頼
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書の拡張の検証（Validate Certificate Extensions）	（[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。
説明	任意で説明を入力します。

関連トピック

信頼できる証明書ストア （11 ページ）
証明書チェーンのインポート （17 ページ）
信頼できる証明書ストアへのルート証明書のインポート （16 ページ）

証明書署名要求

認証局（CA）が署名付き証明書を発行するためには、証明書署名要求（CSR）を作成してCAに送信する必要があります。

自分が作成した証明書署名要求（CSR）のリストは、[証明書署名要求（Certificate Signing Requests）] ページで使用できます。認証局（CA）から署名を取得するには、CSR をエクスポー

トし、その証明書を CA に送信する必要があります。証明書は CA によって署名され、返されます。

管理者ポータルから証明書を一元的に管理できます。展開内のすべてのノードの CSR を作成およびエクスポートできます。その後、CSR を CA に送信し、CA から CA 署名付き証明書を取得し、CA によって返されたルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートし、CSR に CA 署名付き証明書をバインドする必要があります。

証明書署名要求の作成と認証局への CSR の送信

証明書署名要求（CSR）を生成して、展開内のノードの CA 署名付き証明書を取得できます。展開の選択ノードまたは展開のすべてのノード用の CSR を生成できます。

ステップ 1 **[証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 CSR を生成するための値を入力します。各フィールドの詳細については、「証明書署名要求の設定」を参照してください。

ステップ 3 [Generate（生成）] をクリックして CSR を生成します。

CSR が生成されます。

ステップ 4 [Export（エクスポート）] をクリックして、メモ帳で CSR を開きます。

ステップ 5 「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までのすべてのテキストをコピーします。

ステップ 6 選択した CA の証明書要求に、この CSR の内容を貼ってください。

ステップ 7 署名済みの証明書をダウンロードする。

CA によっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zip ファイルの形式で、Cisco ISE-PIC の信頼された証明書ストアに追加する必要がある、新規発行の証明書と CA のパブリック署名証明書が含まれています。デジタル署名された CA 証明書、ルート CA 証明書、および他の中間 CA 証明書（該当する場合）がクライアント ブラウザを実行するローカル システムにダウンロードされます。

CSR への CA 署名付き証明書のバインド

CA からデジタル署名付き証明書を受け取った後、それを証明書署名要求（CSR）にバインドする必要があります。管理者ポータルから展開内のすべてのノードに対してバインド操作を実行できます。

始める前に

- デジタル署名付き証明書、および関連するルート中間 CA 証明書を CA から受け取る必要があります。

- 関連するルートおよび中間CA証明書を信頼できる証明書ストアにインポートします（**[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]**。）。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

CA 署名付き証明書に CSR をバインドするノードの隣にあるチェックボックスをオンにします。

ステップ 2 [バインド（Bind）] をクリックします。

ステップ 3 [参照（Browse）] をクリックし、CA 署名付き証明書を選択します。

ステップ 4 証明書の [フレンドリ名（Friendly Name）] を指定します。

ステップ 5 Cisco ISE-PIC に証明書の拡張の検証を許可する場合は、[証明書の拡張の検証（Validate Certificate Extensions）] チェックボックスをオンにします。

[証明書の拡張の検証（Validate Certificate Extensions）] オプションが有効になっており、インポートする証明書にCAフラグがtrueに設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

（注） ISE では、EAP-TLS クライアント証明書にデジタル署名キー使用拡張を使用する必要があります。

ステップ 6 この証明書が使用領域で使用されるサービスを確認します。

この情報は、CSR の生成時に [使用方法（Usage）] オプションを有効にした場合は自動入力されます。 証明書のバインディング時に使用方法を指定しない場合は、[使用方法（Usage）] オプションをオフにします。後で証明書を編集し、使用方法を指定できます。

（注） プライマリ PAN の管理者ロール証明書の証明書を変更すると、他のすべてのノードのサービスが再起動します。

プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ管理ノード（PAN）の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

ステップ 7 [送信（Submit）] をクリックし、CA 署名付き証明書をバインドします。

Cisco ISE-PIC ノード間通信にこの証明書を使用するように選択した場合、Cisco ISE-PIC ノードでアプリケーション サーバが再起動されます。

他のノードで CA 署名付き証明書に CSR をバインドするために、このプロセスを繰り返します。

次のタスク

信頼できる証明書ストアへのルート証明書のインポート （16 ページ）

証明書署名要求のエクスポート

このページを使用して、証明書署名要求をエクスポートすることができます。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 [OK] をクリックして、クライアントブラウザを実行しているファイルシステムにファイルを保存します。

証明書署名要求の設定

Cisco ISE-PIC では、1 つの要求で、管理者ポータルから展開内のノードの CSR を生成することができます。また、展開内の単一ノードまたはノードのどちらの CSR を生成するのか選択することもできます。単一ノードの CSR を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名（FQDN）を自動的に置き換えます。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE-PIC ノードの FQDN を入力する必要があります。展開内の両方のノードの CSR を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE-PIC ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE-PIC ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表に、認証局（CA）が署名可能な証明書署名要求（CSR）の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドを示します。このページのナビゲーション パスは **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[署名所署名要求（Certificate Signing Request）]** です。

表 *2:* 証明書署名要求の設定

フィールド	使用上のガイドライン
証明書の用途（**Certificate(s) will be used for**）	

フィールド	使用上のガイドライン
	証明書を使用するサービスを選択します。 **Cisco ISE ID 証明書** • [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS 認証、pxGrid）に使用されます。複数使用の証明書は、クライアントとサーバ両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [管理者（Admin）]：サーバ認証に使用されます（管理者ポータルとの通信および展開内の ISE-PIC ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバ証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） • [pxGrid]：クライアント認証とサーバ認証の両方に使用されます（pxGrid クライアントとサーバ間の通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1） （注）

フィールド	使用上のガイドライン

	拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。
	`source=local ; type=fatal ; message="unsupported certificate"`
	
	Cisco ISE 認証局証明書
	• [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。
	• [ISE 中間 CA（ISE Intermediate）]：（ISE-PIC が外部 PKI の中間 CA として機能する場合に内部 CA サービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。
	  • [基本制約（Basic Constraints）]：重要、認証局
	  • [キーの用途（Key Usage）]：証明書の署名、デジタル署名
	  • [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9）
	• [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部 CA サービスにのみ適用可能）展開全体の ISE-PIC OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE-PIC OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。

ワイルドカード証明書の許可（Allow Wildcard Certificates）	証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ問題が発生する可能性があります。

フィールド	使用上のガイドライン
これらのノードの CSR の生成（Generate CSRs for these Nodes）	証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。
Common Name（CN）	デフォルトでは、一般名は CSR を生成する ISE-PIC ノードの FQDN です。$FQDN$ は ISE-PIC ノードの FQDN を意味します。展開内の複数ノードの CSR を生成すると、CSR の [一般名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。
Organizational Unit（OU）	組織ユニット名。Engineering など。
Organization（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
Country（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。 • [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE-PIC ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。 • [IP アドレス（IP Address）]：証明書に関連付けられる ISE-PIC ノードの IP アドレス。 • [Uniform Resource Identifier]：証明書に関連付ける URI。 • [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。
キー タイプ	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。

フィールド	使用上のガイドライン
キーの長さ（**Key Length**）	公開キーのビット サイズを指定します。 RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA の署名付き証明書を取得する場合は 2048 以上を選択します。
署名するダイジェスト（**Digest to Sign With**）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（**Certificate Policies**）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

Cisco ISE CA サービス

証明書は、自己署名したり、外部の認証局（CA）がデジタルで署名したりできます。ISE-PIC は、pxGrid 証明書にデジタル署名を行う pxGrid の外部認証局（CA）として機能できます。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。ISE-PIC CA には次の機能があります。

- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求（CSR）を検証し、署名します。
- キー管理：キーと証明書を生成し、セキュアに保存します。
- 証明書ストレージ：ユーザやデバイスに発行された証明書を保存します。
- Online Certificate Status Protocol（OCSP）サポート：OCSP 応答側に証明書の有効性を確認する手段を提供します。

CA サービスがプライマリ管理ノードで無効になっている場合でも、CA サービスはセカンダリ管理ノードの CLI で実行中として表示されます。理想的には、CA サービスは無効として表示される必要があります。これは、Cisco ISE の既知の問題です。

楕円曲線暗号化証明書のサポート

Cisco ISE-PIC CA サービスが、楕円曲線暗号化（ECC）アルゴリズムに基づく証明書をサポートするようになりました。ECC は、より小さいキー サイズを使用している場合でも、他の暗号化アルゴリズムよりも高いセキュリティとパフォーマンスを提供します。

次の表では、ECC および RSA のキー サイズとセキュリティ強度を比較しています。

ECC のキー サイズ（ビット単位）	RSA のキー サイズ（ビット単位）
160	1024
224	2048
256	3072
384	7680
521	15360

キー サイズが小さいため、暗号化が迅速になります。

Cisco ISE-PIC では、次の ECC 曲線タイプがサポートされています。曲線タイプまたはキー サイズが大きくなると、セキュリティが強化されます。

- P-192
- P-256
- P-384
- P-521

ISE-PIC は、証明書の EC 部分の明示的なパラメータをサポートしていません。明示的なパラメータで証明書をインポートしようとすると、「証明書の検証に失敗しました」というエラーが表示されます。名前付き ECParameters のみがサポートされています。

証明書プロビジョニング ポータルから ECC 証明書を生成することができます。

Cisco ISE-PIC 認証局証明書

[認証局（CA）証明書（Certificate Authority (CA) Certificates）] ページには、内部 Cisco ISE-PIC CA に関連するすべての証明書が表示されます。これらの証明書は、このページにノード方式で表示されます。ノードを展開して、その特定のノードの ISE-PIC CA 証明書をすべて表示することができます。プライマリおよびセカンダリ管理ノードには、ルート CA、ノード CA、下位 CA、OCSP レスポンダ証明書があります。展開内の他のノードには、エンドポイント下位 CA および OCSP 証明書があります。

Cisco ISE-PIC CA サービスを有効にすると、すべてのノードでこれらの証明書が自動的に生成され、インストールされます。また、ISE-PIC ルート CA チェーン全体を置き換えると、すべてのノードでこれらの証明書が自動的に再生成され、インストールされます。手動による介入は必要ありません。

Cisco ISE-PIC CA 証明書は **Certificate Services** <**エンドポイント サブ *CA*/ノード *CA*/ルート *CA*/*OCSP* レスポンダ**>-<ノードのホスト名>#証明書番号という命名規則に従います。

[CA 証明書（CA Certificates）] ページで Cisco ISE-PIC CA 証明書を編集、インポート、エクスポート、削除、表示できます。

Cisco ISE-PIC CA 証明書の編集

証明書を Cisco ISE-PIC CA 証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。.

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 必要に応じて編集可能なフィールドを変更します。フィールドの説明については、「証明書設定の編集」を参照してください。

ステップ 4 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

Cisco ISE CA 証明書のエクスポート

Cisco ISE ルート CA およびノード CA 証明書をエクスポートするには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

Cisco ISE-PIC CA 証明書のインポート

クライアントが別の展開の Cisco ISE-PIC CA によって発行された証明書を使用してネットワークへの認証を試みる場合、Cisco ISE-PIC ルート CA、ノード CA、エンドポイント サブ CA 証

明書をその展開から Cisco ISE-PIC の信頼できる証明書ストアにインポートする必要があります。

始める前に

- ISE-PIC ルート CA、ノード CA、エンドポイント サブ CA 証明書を、エンドポイント証明書が署名されている展開からエクスポートし、ブラウザが実行されているコンピュータのファイル システムに保存します。

ステップ 1 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 必要に応じてフィールドの値を設定します。詳細については、「信頼できる証明書のインポート設定」を参照してください。

クライアント証明書ベースの認証が有効である場合は、Cisco ISE-PIC により展開内の各ノードのアプリケーション サーバが再起動されます（最初に PAN のアプリケーション サーバが再起動されます）。

証明書設定の編集

次の表では、認証局（CA）証明書属性を編集するために使用できる [証明書ストアの証明書編集（Certificate Store Edit Certificate）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [証明書（Certificate）] > [編集（Edit）]** です。

表 *3:* 証明書ストア編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	
フレンドリ名（Friendly Name）	証明書のフレンドリ名を入力します。
Status（ステータス）	[有効（Enabled）] または [無効（Disabled）] を選択します。[無効（Disabled）] の場合、ISE は信頼を確立するために証明書を使用しません。
説明	任意で説明を入力します。
使用方法	
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の ISE ノードまたは LDAP サーバから）サーバ証明書を検証する場合は、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
クライアント認証および syslog 用に信頼する（**Trust for client authentication and Syslog**）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE に接続するエンドポイントの認証 • syslog サーバの信頼
シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書ステータスの検証（**Certificate Status Validation**）	ISEは、特定のCAが発行するクライアントまたはサーバ証明書の失効ステータスをチェックする2とおりの方法をサポートしています。1 つは、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSP は、CA によって保持される OCSP サービスに要求を行います）。もう 1 つは、ISEにCAからダウンロードした証明書失効リスト（CRL）に対して証明書を検証することです。両方の方法は、OCSPを最初に使用し、ステータスを判断できないときに限り CRL を使用する場合に使用できます。
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	認証ステータスが OCSP によって判別されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSPサービスによって不明のステータス値が返されると、ISEは現在評価されているクライアントまたはサーバ証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP応答側が到達不能な場合にISEが要求を拒否するには、このチェックボックスをオンにします。

フィールド名	使用上のガイドライン
CRL のダウンロード（Download CRL）	Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISE が CRL を再度ダウンロードするまでに待機する時間間隔を設定します。
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （11 ページ）
信頼できる証明書の編集 （15 ページ）

Cisco ISE-PIC CA 証明書およびキーのバックアップと復元

PPAN に障害が発生し、セカンダリ管理ノードを外部 PKI のルート CA または中間 CA として機能させるために昇格する場合に備え、Cisco ISE-PIC CA 証明書およびキーをセキュアにバックアップして、セカンダリ管理ノードにこれらを復元できるようにする必要があります。Cisco ISE-PIC 設定のバックアップには、CA 証明書とキーは含まれていません。CA 証明書およびキーをリポジトリにエクスポートおよびインポートするには、代わりにコマンドライン インターフェイス（CLI）を使用する必要があります。**application configure ise** コマンドには、CA 証明書およびキーのバックアップと復元のためのエクスポートおよびインポートのオプションが含まれています。

信頼できる証明書ストアからの次の証明書が、セカンダリ管理ノードで復元されます。

- Cisco ISE ルート CA 証明書
- Cisco ISE サブ CA 証明書
- Cisco ISE エンドポイント RA 証明書
- Cisco ISE OCSP 応答側証明書

次の場合、Cisco ISE CA 証明書およびキーのバックアップおよび復元が必要となります。

- 展開内にセカンダリ管理ノードが存在する
- Cisco ISE-PIC CA ルート チェーン全体を置き換える
- 外部 PKI の下位 CA として機能するように Cisco ISE-PIC ルート CA を設定する
- 設定のバックアップからデータを復元する。この場合、最初に Cisco ISE-PIC CA ルート チェーンを再生成し、次に ISE CA 証明書およびキーのバックアップと復元を行う必要があります。

Cisco ISE CA 証明書およびキーのエクスポート

CA 証明書およびキーを PAN からエクスポートし、セカンダリ管理ノードでインポートする必要があります。このオプションでは、PAN がダウンした場合にセカンダリ管理ノードでエンドポイントの証明書を発行および管理し、セカンダリ管理ノードを PAN に昇格させることができます。

始める前に

CA 証明書およびキーを格納するためのリポジトリを作成したことを確認します。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 7 を入力して、証明書およびキーをエクスポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 暗号キーを入力します。

エクスポートされた証明書のリスト、件名、発行者、およびシリアル番号とともに成功メッセージが表示されます。

例：

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE-PIC CA 証明書およびキーのインポート

セカンダリ管理ノードを登録したら、PAN から CA 証明書およびキーをエクスポートし、セカンダリ管理ノードにインポートします。

ステップ 1 Cisco ISE-PIC CLI から、**application configure ise** コマンドを入力します。

ステップ 2 8 を入力して、CA 証明書およびキーをインポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 インポートするファイルの名前を入力します。ファイル名は **ise_ca_key_pairs_of_<vm hostname>** 形式である必要があります。

ステップ 5 ファイルを復号化するための暗号キーを入力します。

処理が正常に完了したことを知らせるメッセージが表示されます。

例：

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5
```

```
Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

ルート CA および下位 CA の生成

展開をセットアップする場合、CiscoISE-PICは、ノード。ただし、ノードのドメイン名またはホスト名を変更する場合は、プライマリ PAN でルート CA、PSN で下位 CA をそれぞれ再生成する必要があります。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。 を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用先（Certificate(s) will be used for）] ドロップダウン リストから ISE ルート CA を選択します。

ステップ 4 [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate chain）] をクリックします。

ルート CA と下位 CA 証明書が、展開内のすべてのノードに対して生成されます。

次のタスク

展開にセカンダリ PAN がある場合は、プライマリ PAN から CiscoISE-PIC CA 証明書およびキーのバックアップを取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN がルート CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

外部 PKI の下位 CA としての Cisco ISE-PIC ルート CA の設定

外部 PKI の下位 CA として機能するプライマリ PAN のルート CA が必要な場合は、ISE-PIC 中間 CA 証明書署名要求を生成して、外部 CA に送信し、ルートおよび CA 署名付き証明書を入手して、ルート CA 証明書を信頼できる証明書ストアにインポートし、CA 署名付き証明書を CSR にバインドします。この場合、外部 CA はルート CA、ノードは外部 CA の下位 CA、PSN はノードの下位 CA です。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用目的（Certificate(s) will be used for）] ドロップダウン リストから [ISE 中間 CA（ISE Intermediate CA）] を選択します。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 CSR をエクスポートし、外部 CA に送信して、CA 署名付き証明書を取得します。

ステップ 6 信頼できる証明書ストアに外部 CA のルート CA 証明書をインポートします。
ステップ 7 CSR に CA 署名付き証明書をバインドします。

OCSP サービス

Online Certificate Status Protocol（OCSP）は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト（CRL）に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバと通信し、認証で証明書のステータスを検証する機能があります。OCSP のコンフィギュレーションは、Cisco ISE で設定されるいずれかの認証局（CA）証明書から参照できる再利用可能な設定オブジェクトで設定されます。

CRL 検証と OCSP 検証の両方または一方を CA ごとに設定できます。両方を選択すると、Cisco ISE では最初に OCSP を介した検証が実行されます。プライマリ OCSP サーバとセカンダリ OCSP サーバの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ

Cisco ISE CA OCSP 応答側は、OCSP クライアントと通信するサーバです。Cisco ISE CA の OCSP クライアントには、Cisco ISE の内部 OCSP クライアントと適応型セキュリティ アプライアンス（ASA）の OCSP クライアントがあります。OCSP クライアントは、RFC 2560、5019 で定義されている OCSP 要求/応答構造を使用して、OCSP 応答側と通信する必要があります。

Cisco ISE CA は、OCSP 応答側に証明書を発行します。OCSP 応答側は、着信要求をポート 2560 でリッスンします。このポートは、OCSP トラフィックのみを許可するように設定されています。

OCSP 応答側は RFC 2560、5019 で規定された構造に従って要求を受け入れます。OCSP 要求ではナンス拡張がサポートされます。OCSP 応答側は証明書のステータスを取得し、OCSP 応答を作成して署名します。OCSP 応答は、OCSP 応答側ではキャッシュされませんが、クライアントでは最大 24 時間 OCSP 応答をキャッシュすることができます。OCSP クライアントでは、OCSP 応答の署名を検証する必要があります。

PAN 上の自己署名 CA 証明書（ISE が外部 CA の中間 CA として機能する場合は、中間 CA 証明書）によって、OCSP 応答側証明書が発行されます。PAN 上のこの CA 証明書によって、PAN および PSN の OCSP 証明書が発行されます。この自己署名 CA 証明書は、展開全体に対するルート証明書でもあります。展開全体のすべての OCSP 証明書が、これらの証明書を使用して署名された応答を ISE で検証するために、信頼できる証明書ストアに格納されます。

OCSP 証明書のステータスの値

OCSP サービスでは、所定の証明書要求に対して次の値が返されます。

- [良好（Good）]：ステータスの問い合わせへの肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [失効（Revoked）]：証明書は失効しています。
- [不明（Unknown）]：証明書のステータスは不明です。この OCSP 応答側の CA で証明書が発行されなかった場合、OCSP サービスはこの値を返します。
- [エラー（ERROR）]：OCSP 要求に対する応答を受信しませんでした。

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大 2 つの OCSP サーバを設定でき、それらのサーバはプライマリおよびセカンダリ OCSP サーバと呼ばれます。各 OCSP サーバ設定には、次のパラメータが含まれます。

- [URL]：OCSP サーバの URL。
- [ナンス（Nonce）]：要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [応答の検証（Validate Response）]：Cisco ISE は OCSP サーバから受信した応答の署名を検証します。

Cisco ISE がプライマリ OCSP サーバと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバに切り替えます。

Cisco ISE はプライマリ サーバの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバを使用します。

OCSP の障害

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

- OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の失敗による障害。
- 失敗した OCSP 応答側のシナリオ。例：

  最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答します。

  Cisco ISE OCSP 要求からエラーまたは応答が受信されません。

  OCSP 応答側が、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。

  - tryLater
  - signRequired
  - unauthorized

- internalError
- malformedRequest

  OCSP 要求には、多数の日時チェック、署名の有効性チェックなどがあります。詳細については、エラー状態を含むすべての可能性のある状態について説明している『*RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』を参照してください。

- 失敗した OCSP レポート

OCSP クライアント プロファイルの追加

[OCSP クライアント プロファイル（OCSP Client Profile）] ページを使用して、Cisco ISE に新しい OCSP クライアント プロファイルを追加できます。

始める前に

認証局（CA）が非標準ポート（80 または 443 以外）で OCSP サービスを実行している場合は、そのポートで Cisco ISE と CA 間の通信を可能にするためにスイッチで ACL を設定する必要があります。次に例を示します。

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP* ポート番号 >

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > [OCSP クライアント プロファイル（OCSP Client Profile）] を選択します。

ステップ 2 OCSP クライアント プロファイルを追加するための値を入力します。

ステップ 3 **[送信（Submit）]** をクリックします。

OCSP 統計情報カウンタ

Cisco ISE では、OCSP カウンタを使用して、OCSP サーバのデータと健全性をロギングおよびモニタリングします。ロギングは 5 分ごとに実行されます。Cisco ISE はモニタリング ノードに syslog メッセージを送信し、それはローカル ストアに保持されます。ローカル ストアには過去 5 分のデータが含まれています。Cisco ISE が syslog メッセージを送信した後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

次の表に、OCSP syslog メッセージとその説明を示します。

表 *4 : OCSP Syslog* メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数

メッセージ	説明
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数
OCSPCertsCleanedUpCount	t間隔の後にクリーンアップされたキャッシュエントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数