# サードパーティ CA 署名付き証明書の有効化

このセクションでは、次の点について説明します。



# サードパーティ CA 署名付き証明書の有効化

セキュアなデータ転送のために、自分の会社の署名付き証明書をインポートすることができます。この証明書を使用するブラウザで、SSL を有効にする必要があります。

## CA 署名付き証明書のインストール

セキュアなデータ転送のための CA 署名付き証明書のインストール：

### 始める前に

セキュリティを強化し、管理を容易にし、証明書管理を実践するために、情報資産を保護する目的で、次の要素が検証されます。

**Cisco Prime Collaboration リリース 12.1 SP3 以降の場合**

CA の署名付き証明書は、次の要件のリストを満たしている必要があります。要件：

- "Primecollab" エイリアスを含む。
- 正しいパスワードを使用してインポートできる。
- 30 年以上にわたって有効な状態を維持する。
- 有効期限が設定されている。有効期限が
  - 切れていないこと

    例：現在の日付が 20/9/2019 の場合、有効期間（20/8/1970-20/8/2000）は無効です。
  - 将来の日付に設定されていないこと

例：現在の日付が 20/9/2019 の場合、有効期間（20/12/2020-20/12/2025）は無効です。

- 「有効なサンプル」有効期間

  例：現在の日付が 20/9/2019 の場合、有効期間（20/9/2019-20/9/2025）は有効です。

- 証明書に指定する CN（共通名）または SAN（サブジェクトの別名）が、PCA サーバの FQDN（完全修飾ドメイン名）と一致する必要があります。
  - PCA サーバの FQDN が CN と一致しない場合は、SAN のリストと照合されます。
  - ユーザは、CN に FQDN を使用して CSR（証明書署名要求）を生成するか、または SAN のリストに FQDN を含める必要があります。例：pcatest.cisco.com（FQDN）。
- 署名アルゴリズムが、TBSCertificate シーケンスに存在する署名アルゴリズム ID と一致する必要があります。
- 拡張を重複させることはできません。
- サポート対象外の重要な拡張は使用できません。
  - チェックは、重要としてマークされている拡張のみに適用されます。
  - サポート対される拡張は、BC（BasicConstraints）、KU（KeyUsage）、EKU（ExtendedkeyUsage）、SAN（SubjectAlternativeName）、IAN（IssuerAlternativeName）、SIA（SubjectInfoAccess）、AIA（AuthorityInfoAccess）です。
- 重要な KeyUsage（KU）があり、有効であること
  - KU 拡張が重要としてマークされていれば、チェックが適用されます。
  - 有効な KU は keyCertSign、cRLSign、digitalSignature です。
- 重要な ExtendedKeyUsage（EKU）があり、有効であること。
  - EKU 拡張が重要としてマークされていれば、チェックが適用されます。
  - 有効な EKU は serverAuth、clientAuth、OCSPSigning です。

上記の要件を 1 つでも満たしていない場合、証明書は拒否され、該当するエラーメッセージによってユーザにアラートが送られます。

**Cisco Prime Collaboration リリース 11.5 以降の場合**

- ルート証明書が、署名付き証明書に含まれている。
- SSL がブラウザで有効であり、CA 署名付き証明書を使用できる。

**ステップ 1** 選択 **[システム管理（System Administration）] > [証明書の管理（Certificate Management）] > [Cisco Prime Collaboration 証明書の管理（Cisco Prime Collaboration Certificate Management]**.

**ステップ 2** ローカル システムから、（PKCS12 形式の）CA 署名付き証明書を参照します。

**ステップ 3** （任意）証明書の生成中にパスワードを設定した場合は、PKCS#12 ファイルの証明書のパスワードを入力して確認します。設定していない場合は、入力する必要はありません。

**ステップ 4** [インポート（Import）] をクリックします。

「サービスが再起動されます」という内容の警告メッセージが表示されます。

**ステップ 5** 警告メッセージが表示されたら、[Continue] をクリックします。
証明書がサーバにインポートされます。

（注） 証明書をインポートした後は、Cisco Prime Collaboration Assurance を手動で再起動する必要があります。

**Cisco Prime Collaboration リリース 12.1 SP3 以降の場合**

Cisco Prime Collaboration Assurance サーバを再起動するには、*root* としてログインし、次のコマンドを実行します。

**1。プロセスを停止します。**

```
「root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh stop」
```

**2。プロセスのステータスを確認します。** - Verify whether the processes have stopped:

```
「root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh status」
```

**3。プロセスを再起動します。**

```
「root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh start」
```

サービス再起動後、ログインページが表示されます。セキュリティ警告ページ（ログインページが表示されるよう選択を行うページ）は、これ以降表示されません。

（注） Cisco Prime Collaboration Assurance サーバを起動する前に、プライマリおよびセカンダリの中間証明書をブラウザへインポートしておくことをお勧めします。これにより、CA 署名付き証明書をインストールした後、最初にサーバを起動したときに、接続がプライベートでないという警告が表示されないようになります。

PKCS12 証明書は、どのエイリアス名でもインポートできます。

PEM/DER 形式（.pem、.cer、.der、.key など）はサポートされないため、KCS#12 形式（.pfx または .p12）の証明書を使用する必要があります。

**Cisco Prime Collaboration リリース 11.6 以降の場合**

（注） PKCS12（.pfx または .p12）形式の署名付き証明書がインポートされていることを確認してください。

証明書には、**primecollab** エイリアスが含まれている必要があります。

**primecollab** エイリアスのキーのパスワードは、証明書のパスワードと同じである必要があります。

**Cisco Prime Collaboration リリース 12.1 以降の場合**

PKCS7 または PKCS12 の証明書を適用したバージョン 11.x の Cisco Prime Collaboration Assurance を、バージョン 12.1 に移行すると、証明書が復元されません。Cisco Prime Collaboration Assurance 12.1 用に証明書を再生成する必要があります。

（注） Cisco Prime Collaboration Assurance 11.6 以降では、PKCS12 の証明書のみがサポートされています。

プライマリ/中間/セカンダリの証明書をブラウザへインポートするには、次の表を参照してください。

| ブラウザ | 操作 |
|---|---|
| Internet Explorer | 選択 **[ツール（Tools）]** > **[インターネット オプション（Internet Options）]**> **[コンテンツ（Content）]**> **[証明書（Certificates）]**> **[信頼されたルート証明機関（Trusted root certification authorities）]** > **[インポート（Import）]** |
| Mozilla Firefox | 選択 **[ツール（Tools）]** > **[オプション（Options）]**> **[拡張機能（Advanced）]**> **[証明書（Certificates）]**> **[証明書を表示（View certificates）]** > **[インポート（Import）]** |
| Chrome | 選択 **[設定（Settings）]** > **[詳細設定（Advanced settings）]** > **[HTTP/SSL証明書の管理（ HTTP/SSL Manage certificates）]**> **[信頼されたルート証明機関（Trusted root certification authorities）]**> **[インポート（Import）]** |