このマニュアルについて

Important ソフトウェアバージョン X12.5 以降の新機能は、Cisco TelePresence Video Communication Server（VCS）製品ではサポートされません。これらの新機能は Cisco Expressway シリーズ製品（Expressway）にのみ適用されます。このソフトウェアバージョンはメンテナンスおよびバグ修正のみを目的として VCS に用意されています。

バージョン X12.5 以降、このガイドは、Cisco Expressway シリーズ（Expressway）製品のみに適用され、Cisco TelePresence Video Communication Server（VCS）製品には適用されなくなります。Cisco.com の古い VCS は、各ガイドのタイトル ページで指定されている VCS バージョンで引き続き有効です。

この導入ガイドでは、Cisco Expressway（Expressway）で使用する X.509 暗号化証明書を作成する方法と、それを Expressway にロードする方法について説明します。

この章では、次の内容について説明します。

変更履歴

次の表では、製品で追加または変更された情報について説明します。

表 *1:* 変更履歴

リリース日	変更内容	理由
2023 年 4 月	「Certificate Manager ECDSA サポート」という新しいシナリオを追加。 「証明書署名要求の生成」および「Expressway を使用した証明書署名要求の作成」の項を更新。	X14.3 リリース
2020 年 6 月	「PKI の概要」項から偏った表現を削除。	ドキュメントの訂正
2020 年 6 月	X12.6 用に更新	X12.6 リリース
2020 年 2 月	マルチ SAN 証明書に関する「Expressway を使用した証明書署名要求の作成」項を更新。	ドキュメントの訂正
2019 年 12 月	ACME 証明書サービスを展開するための前提条件を更新。	ドキュメントの訂正
2019 年 4 月	メンテナンスリリース X12.5.2 を更新。	X12.5.2 リリース
2019 年 1 月	ACME 証明書管理の X12.5 用に更新。その他のマイナー修正。	X12.5 リリース
2018 年 9 月	X8.11 が使用できなくなったため、ソフトウェアバージョンを X8.11 から X8.11.1 に変更しました。	X8.11.1 リリース
2018 年 7 月	X8.11 用に更新。	X8.11 リリース（破棄）
2017 年 9 月	999 文字の SAN 制限を削除。	X8.10 リリースで修正済み
2017 年 7 月	サーバー証明書のアップロードに関する新しい警告メッセージの説明を追加。UI メニューパスを変更。VCS バージョンと Expressway バージョンを統合。	X8.10 リリース
2016 年 12 月	MRA 証明書の要件を明確化。	X8.9 リリース
2016 年 6 月	X8.8 用に更新。	X8.8 リリース
2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。	
2015 年 7 月	X8.6 用に更新。	
2015 年 4 月	X8.5.2 用に更新。CRL 情報の変更、証明書署名要求生成ページのデフォルト、SAN の 999 文字制限。	
2015 年 1 月	X8.5.1用に更新。ユーザーインターフェイスにダイジェストアルゴリズムを選択させるオプションを導入。デフォルトは、SHA-256（ハッシュアルゴリズム）に設定されている。	

リリース日	変更内容	理由
2014年12月	X8.5用に再発行。2050年の日付管理とサポートされていないOIDの注釈を挿入。付録2「OpenSSLのみを使用する証明書の生成」の手順を変更。	
2014年7月	X8.2用に再発行。Unified Communications展開時のサーバー証明書用の推奨オプションを変更。	
2014年6月	X8.2用に再発行。Unified Communications展開用のサーバー証明書要件を強化。	
2013年12月	Expressswayバージョンの初期リリース。 （以前のVCS専用バージョンとの比較）X8.1用に更新。「Microsoft OCSを使用した証明書の生成」の付録を削除。「OpenSSLのみを使用する証明書の生成」付録のさまざまな改善と明確化。	

このガイドに記載されていない情報

本書では、次のExpressway構成のトピックについては説明しません。これらのトピックについては、『*Expressway* 管理者ガイド』を参照してください。

- Expressway で証明書ベースの認証を有効にする方法
- Expressway にプレインストールされているルート CA の詳細
- 最小限の TLS バージョンと暗号スイートの構成方法
- クライアント証明書のテスト方法
- mTLS 証明書の管理（モバイルおよびリモートアクセスの展開）
- マルチテナント用のドメイン証明書とサーバー名表示（ホステッドコラボレーションソリューション展開）

PKI の概要

Public Key Infrastructure（PKI）では、セキュアな通信を確立し（暗号化され完全性が保護される）、ID を確認できるメカニズムが提供されます。基本的な PKI は次のとおりです。

- **公開/秘密キーのペア：**公開キーがサーバーに送信されるデータを暗号化するために使用されますが、そのデータを復号化するには秘密キー（サーバーによって秘密が保持される）のみを使用できます。

- **データの署名**：データは、データおよびサーバーの秘密キーの暗号ハッシュの組み合わせを使用して「署名」できます。クライアントは、サーバーの公開キーと同じハッシュを使用して署名を検証できます。これにより、データが意図したサーバーから送信され、改ざんされていないことが保証されます。
- **証明書**：証明書は、公開キーのラッパーであり、キーの所有者に関する情報を X.509 フォーマットで提供します。これには通常サーバー名と連絡先詳細が含まれます。
- **証明書チェーン**：認証局（CA）は、独自の秘密キーを使用してサーバー証明書に署名します。次に、CA の証明書（公開キー）に対して署名をチェックすることで、証明書が署名されていることを確認できます。Web ブラウザと他のクライアントには、信用する CA 証明書のリストがあり、個々のサーバーの証明書を確認することができます。

Transport Layer Security（TLS）は、TCP/IP ネットワーク上のホスト間のセキュアな TCP 接続を確立する標準メカニズムです。たとえば、セキュアな HTTP（HTTPS）は TLS を使用してトラフィックを暗号化し確認します。TLS 接続を確立するには、次の手順に従います。

1. クライアントがそのキャパシティ（暗号スイートを含む）と乱数を送信し、初期 TCP 接続を確立します。
2. サーバーは、これらキャパシティの選択、その他乱数その証明書に応答します。
3. クライアントは、信頼できる CA がサーバー証明書を発行し（署名し）、廃止されていないかを検証します。
4. クライアントは、サーバーの公開キーで暗号化された「事前秘密」を送信します。
5. この事前秘密は、交換された乱数（リプレイアタックを防ぐため）と組み合わせて、「共有秘密」を生成するために使用されます。この共有秘密は、クライアントとサーバーの間で暗号化されたこの TLS セッションの残りの通信を保持します。

次の項では、これらの PKI コンポーネントを Expressway でどのように使用できるかについて説明します。

Expressway での証明書の使用の概要

Expressway は次に対して証明書を必要とします。

- TLS（HTTPS）接続によるセキュアな HTTP
- SIP シグナリング、エンドポイントおよびネイバーゾーンの TLS 接続
- Unified CM、Cisco TMS、LDAP サーバーおよび syslog サーバーなどの他のシステムへの接続

これは、は信頼された認証局（CA）証明書のリストおよび関連する証明書失効リスト（CRL）を使用して、接続するその他デバイスを検証します。

Expressway は、サーバー証明書と秘密キーを使用して、署名済み証明書を提供し、Expressway がそのデバイスであるという証拠を提示します。これは、Microsoft Lync または Unified CM などのネイバーデバイスおよび Web インターフェイスを使用する管理者が使用できます。

証明書は、Expressway を識別します。これには、名前が含まれ、この名前によって認識されて、トラフィックがルーティングされます。クラスタの一部である場合など、これらの目的でExpressway が複数の名前によって認識される場合は、RFC5922 のガイダンスに従って X.509 のサブジェクトデータでこれを表す必要があります。証明書には、Expressway 自体とクラスタの両方の FQDN が含まれている必要があります。次のリストには、選択された導入モデルに応じて X.509 サブジェクトに含める必要があるものを示します。

Expressway がクラスタ化されない場合：

- サブジェクトの共通名 = Expressway の FQDN
- サブジェクトの代替名 = 空欄のまま*

Expressway がクラスタ化され、Expressway ごとに個別の証明書がある場合：

- サブジェクトの共通名 = クラスタの FQDN
- サブジェクトの代替名 = Expressway ピアの FQDN とクラスタの FQDN*

[サーバー証明書（Server certificate）] ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]**）から Expressway のサーバー証明書を管理します。TLS 暗号化を使用してクライアント システムと通信するときや HTTPS を使用して Web ブラウザと通信するときに Expressway を識別するためにこの証明書を使用します。「サーバ証明書（Server certificate）」ページを使用すると、次のことを実行できます。

- 現在ロードされている証明書に関する詳細の表示
- 証明書署名要求の生成
- 新しいサーバ証明書のアップロード

証明書生成の概要

X.509 証明書がサードパーティから提供されることがあります。または、OpenSSL などの証明書発行システムやMicrosoft認証局などのアプリケーションで使用できるツールで生成されることがあります。管理された環境またはテスト環境での Expressway の導入では内部で生成された証明書を使用できますが、認識された認証局から提供されたサードパーティ証明書を推奨します。

Expressway は Automated Certificate Management Environment（ACME）もサポートしており、*Let's Encrypt*® 認証局によって署名された証明書を自動的に要求して展開するように設定できます。

Cisco Expressway の以前のリリースでは、RSA 証明書のみがサポートされていました。ただし、Cisco Expressway X14.3 リリース以降では、楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）証明書が既存の RSA 証明書とともに追加されています。

証明書マネージャでは、キー長の値が異なる ECDSA 証明書の生成がサポートされています。

Cisco Expressway を更新またはインストールすると、自己署名証明書が生成されます。

証明書生成には通常 3 段階のプロセスがあります。

- ステージ 1：秘密キーの生成
- ステージ 2：証明書要求の作成
- ステージ 3：証明書の承認と作成

本書では、ルート証明書、Expressway用のクライアント/サーバー証明書、および秘密キーを生成する代替方法を提示します。

- 「証明書署名要求（証明書署名要求）の生成」では、Expressway 自体を使用して、秘密キーと証明書要求を生成する方法について説明します。
- 「付録 2：OpenSSL のみを使用した証明書生成」では、サードパーティまたは内部管理された CA で使用できる OpenSSL 専用のプロセスについて説明します。

相互 TLS 認証の場合、Expressway サーバー証明書は、クライアント証明書としても使用できる必要があります。よって、Expressway が隣接サーバーに対しクライアントデバイスとして認証することができます（「付録 5：AD CS を有効化して、「クライアントとサーバー」証明書を発行する」を参照）。

留意点

- 外部システムを使用して証明書署名要求を生成する場合は、証明書署名要求にサポートされていない OID が含まれていないことを確認します。現在、次の拡張検証 OID のみがサポートされています。
  - 1.3.6.1.4.1.311.60.2.1.1 jurisdictionOfIncorporationLocalityName
  - 1.3.6.1.4.1.311.60.2.1.2 jurisdictionOfIncorporationStateOrProvinceName
  - 1.3.6.1.4.1.311.60.2.1.3 jurisdictionOfIncorporationCountryName

  証明書にサポートされていない OID があるかどうかを確認する方法の詳細については、「SSH の失敗とサポートされていない OID に関する問題」の項を参照してください。

  .
- ワイルドカード証明書では、複数のサブドメインと、それらがサポートするサービス名を管理します。SAN証明書よりも安全性が低い場合があり、Expresswayではサポートされません。
- 2050 年から日付の処理方法が変更されると、有効期限が 2050 年以降の証明書によって運用上の問題が発生する場合があります。
- CA 証明書チェックの Expressway メカニズムでは、BasicConstraints 拡張が存在する必要があります。

- RSA キーに基づく証明書を使用することを強く推奨します。DSA キーに基づく証明書など他のタイプの証明書はテストされておらず、あらゆるシナリオで Expressway と連携するとは限りません。
- サーバー証明書を期限切れにしないでください。期限が切れるとほかの外部システムが証明書を拒否し、Expressway がそれらのシステムに接続できなくなります。

留意点

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。