証明書失効リスト（CRL）の管理

証明書失効リストファイル（CRL）は、TLS/HTTPS を介して Expressway と通信するクライアントブラウザおよび外部システムにより提示される証明書を検証するために Expressway によって使用されます。CRL は、廃棄され Expressway との通信に使用できなくなった証明書を識別します。

TLS/HTTPS クライアントおよびサーバ証明書に署名する CA の CRL データをアップロードすることを推奨します。イネーブルの場合、CRL のチェックはトラスト チェーンのすべての CA に適用されます。

この章では、次の内容について説明します。

証明書失効ソース

Expressway は複数のソースから証明書失効情報を取得できます。

- CRL 分散ポイントからの CRL データの自動ダウンロード
- 証明書内のチェック対象 OCSP（Online Certificate Status Protocol）レスポンダ URI 経由（SIP TLS のみ）
- CRL データの手動アップロード
- Expressway の**信頼できる CA 証明書**ファイル内に組み込まれた CRL データ

制限事項と使用上のガイドライン

次の制約事項および使用上のガイドラインが適用されます。

- SIP TLS 接続を確立するときに、CRL データソースは、**[SIP 構成（SIP configuration）]** ページの **[証明書失効確認（Certificate revocation checking）]** 設定を必要とします。

- 自動的にダウンロードされた CRL ファイルが、手動でロードされた CRL ファイルを上書きする場合（SIP TLS 接続を確認する場合、手動でアップロードされた CRL データと自動でダウンロードされた CRL データの両方を使用する可能性がある場合は除く）
- 外部ポリシー サーバによって提示された証明書を検証する際に、Expressway は手動でロードされた CRL のみを使用します。
- リモート ログイン アカウント認証用に LDAP サーバーとの TLS 接続を検証する際、Expressway は **信頼できる CA 証明書（[ツール（Tools）] > [セキュリティ（Security）] > [信頼できる CA 証明書（Trusted CA certificate）]）** に組み込まれた CRL データのみを使用します。

  LDAP 接続の場合、Expressway はサーバの証明書配布ポイントの URL または発行する CA 証明書から CRL をダウンロードしません。また、[CRL 管理（CRL management）] ページの手動または自動更新設定も使用しません。

自動 CRL 更新

自動 CRL 更新を実行するように Expressway を構成することが推奨されます。これにより、最新の CRL が証明書の検証に使用できるようになります。

CRL の自動更新用に Expressway を構成するには次を実行します。

手順

Step 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [CRL 管理（CRL management）]** の順に選択します。

Step 2 **[自動 CRL 更新（Automatic CRL updates）]** を *[有効（Enabled）]* に設定します。

Step 3 Expressway が CRL ファイルを取得できる **HTTP/HTTPS 分散ポイント**のセットを入力します。

- 新しい行にそれぞれ分散ポイントを指定する必要があります。
- HTTP/HTTPS 分散ポイントのみがサポートされます。HTTPS を使用する場合、分散ポイントのサーバ自体に有効な証明書が必要です。
- PEM および DER エンコード CRL ファイルがサポートされています。
- 分散ポイントは、CRL ファイルまたは複数の CRL ファイルを含む ZIP および GZIP アーカイブを直接示す場合があります。
- URL またはダウンロードしたアーカイブから解凍されたファイルのファイル拡張子は、Expressway がその基盤となるファイル タイプを決定するため、重要ではありませんが、代表的な URL は次の形式となります。
  - http://example.com/crl.pem
  - http://example.com/crl.der

- http://example.com/ca.crl
- https://example.com/allcrls.zip
- https://example.com/allcrls.gz

Step 4 **[Daily update time]** を入力します（UTC 単位で）。これは、Expressway が分散ポイントからその CRL の更新を試行するおおよその時刻です。

Step 5 [保存（Save）] をクリックします。

手動 CRL 更新

CRL ファイルは Expressway に手動でアップロードできます。外部ポリシー サーバによって提示された証明書は、手動でロードされた CRL に対してのみ検証できます。

CRL ファイルをアップロードするには、次の手順を実行します。

（注） CRL ファイルのサイズが 16 MB 未満であることを確認します。

手順

Step 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [CRL 管理（CRL management）]** の順に選択します。

Step 2 **[参照（Browse）]** をクリックして、ファイル システムから必要なファイルを選択します。また、PEM エンコード形式である必要があります。

Step 3 [CRL ファイルのアップロード（Upload CRL file）] をクリックします。

これによって、選択したファイルがアップロードされ、以前にアップロードしたCRLファイルが置換されます。

Expresswayから手動でアップロードされたファイルを削除する場合は、**[失効リストの削除（Remove revocation list）]** をクリックします。

注：認証局の CRL が期限切れの場合、その CA から発行されたすべての証明書が無効として扱われます。

オンライン証明書ステータス プロトコル（OCSP）

Expressway は OCSP レスポンダとの接続を確立して特定の証明書のステータスを照会することができます。Expressway は使用する OCSP レスポンダを、確認する証明書に示されているレスポン

ダURIから決定します。OCSPレスポンダは「良好（good）」、「失効（revoked）」、または「不明（unknown）」で証明書のステータスを送信します。

OCSPの利点は、失効リスト全体をダウンロードする必要がないことです。OCSPはSIP TLS接続のみでサポートされます。

OCSPレスポンダへ接続するには、Expressway-Eからのアウトバウンド通信が必要です。使用しているOCSPレスポンダのポート番号（ポート80または443）をチェックし、Expressway-Eからそのポートへのアウトバウンド通信が可能であることを確認します。

SIP TLS 接続を確認する失効の構成

証明書失効確認がSIP TLS接続でどのように管理されるかを設定する必要があります。

手順

Step 1 **[構成（Configuration）] > [SIP]** の順に選択します。

Step 2 **[証明書失効確認（Certificate revocation checking）]** セクションまでスクロールし、適宜設定を行います。

フィールド	説明	使用方法のヒント
Certificate revocation checking mode	失効確認がSIP TLS接続の確立時に交換された証明書に対し実行されるかどうかを制御します。	失効確認をイネーブルにすることを推奨します。
Use OCSP	Online Certificate Status Protocol（OCSP）を証明書失効確認を実行するために使用するかどうかを制御します。	OCSPを使用するには、以下の条件が必要です。 • チェック対象のX.509証明書にOCSPレスポンダのURIが含まれている必要があります。 • OCSPレスポンダーは、SHA-256ハッシュアルゴリズムをサポートしている必要があります。サポートされていない場合、OCSP失効チェックと証明書検証は失敗します。

フィールド	説明	使用方法のヒント
Use CRLs	証明書失効リスト（CRL）を証明書失効確認を実行するために使用するかどうかを制御します。	CRL は、証明書が OCSP をサポートしていない場合に使用できます。
Allow CRL downloads from CDPs	X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。	
Fallback behavior	たとえば、失効の送信元に連絡を取れないなど、失効ステータスを確立できない場合に、失効確認の動作を制御します。 *[失効として処理（Treat as revoked）]*：証明書を失効したとして処理します（そのため、TLS 接続を許可しません）。 *[失効していないものとして処理（Treat as not revoked）]*：失効していないものとして証明書を処理します。 デフォルト：[Treat as not revoked]	*[失効していないものとして処理（Treat as not revoked）]*では、失効の送信元に連絡をとれない場合、システムは通常の方法で稼働し続けますが、失効した証明書が承認される可能性があることを意味します。

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