証明書失効の概要

このセクションでは、証明書失効について説明します。Cisco UCM は、証明書失効をモニタするためにオンライン証明書ステータスプロトコル（OCSP）をプロビジョニングします。証明書がアップロードされるたびに、スケジュールされたタイムラインで、システムはそのステータスをチェックして有効性を確認します。

コモンクライテリアモードが有効になっている FIPS 展開の場合、OCSP はシステムのコモンクライテリア要件への準拠にも役立ちます。

• 証明書失効の設定 （1 ページ）

証明書失効の設定

[有効性検証（Validation Checks）] では、Unified Communications Manager は証明書のステータスを確認し、有効性を確認します。

証明書の検証手順は次のとおりです。

- Unified Communications Manager は代理信頼モデル（DTM）を使用し、OCSP 署名属性のルート CA または中間 CA をチェックします。ルート CA または中間 CA は、OCSP 証明書に署名してステータスを確認する必要があります。
- 代理信頼モデルが失敗した場合は、レスポンダの信頼モデル（TRP）に戻ります。次に、Unified Communications Manager は OCSP サーバからの指定された OCSP 応答署名証明書を使用して証明書を検証します。

（注） 証明書の失効ステータスを確認するには、OCSP 応答側が実行されている必要があります。

期限切れの証明書が自動的に失効するように OCSP を設定します。[証明書失効（Certificate Revocation）] ウィンドウで OCSP オプションを有効にすると、最も安全な方法でリアルタイムに証明書失効をチェックすることができます。オプションから、証明書の OCSP URI を使用するか、または設定済みの OCSP URI を使用するかを選択します。

（注） syslog、FileBeat、SIP、ILS、LBM など、TLS クライアントは OCSP からリアルタイムで失効応答を受信します。

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性で設定されたルート CA 証明書または中間 CA 証明書、または tomcat-trust にアップロードされた、指定 OCSP 署名証明書を使用できます。

手順

Step 1 Cisco Unified OS Administration で、**[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

Step 2 **[ANATの有効化（Enable OCSP）]** チェックボックスを選択します。

Step 3 証明書に OCSP レスポンダ URI が設定されている場合は、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] オプションをクリックします。

または

Step 4 OCSP チェックに OCSP レスポンダを指定する場合は、[設定された OCSP URI を使用（Use Configured OCSP URI Option）] をクリックします。

Step 5 レスポンダの [OCSP の設定済み URI] を入力します。

Step 6 失効チェックを有効にするには、[失効チェックの有効化（Enable Revocation Check）] チェックボックスをオンにします。

Step 7 失効ステータスを確認する**頻度**を入力し、[時間（Hours）] または [Days（日）] から**時間間隔**をクリックします。

Step 8 [保存（Save）] をクリックします。

（注） シスコサービスのリストを再起動して、リアルタイム OCSP を有効にするように求める、アラートがポップアップ表示されます。このポップアップは、**[OCSP の有効化（Enable OCSP）]** チェックボックスをオンにした場合、または以降の変更を保存した場合にのみ表示されます。

OCSP レスポンダは、検証とコモンクライテリアモードがオンの場合に、次のいずれかのステータスを返します。

- [良好（Good）]：OCSP レスポンダがステータスの照会に対して肯定的な応答を送信していることを示します。証明書は失効しませんが、証明書が発行されたという意味でも、応答時間が証明書の有効期間内にあるという意味でもありません。Response 拡張機能は、発行、有効性など、証明書のステータスに関してレスポンダが行ったより多くの要求を伝えます。
- [失効（Revoked）]：証明書が永久的または一時的に失効（保留）ステータスにあることを示します。
- [不明（Unknown）]：OCSP レスポンダが要求された証明書について認識していないことを示しています。

警告　コモンクライテリアモードを有効にした場合、接続は **[失効済み（Revoked）]** および **[不明（Unknown）]** のケースで失敗します。コモンクライテリアモードを無効にすると、接続は **[不明（Unknown）]** のケースで成功します。

Step 9　（任意）CTI、IPsec または LDAP リンクがある場合は、これらの長期的に中断しない接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) Cisco Unified CM Administration から、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
b) [証明書失効と有効期限（Certificate Revocation and Expiry）] ペインに移動します。
c) [証明書有効性チェック（Certificate Validity Check）] パラメータを [有効（Enabled）] に設定します。
d) [有効性チェック頻度（Validity Check Frequency）] パラメータの値を入力します。

（注）　**[証明書失効（Certificate Revocation）]** ページの **[失効チェックの有効化（Enable Revocation Check）]** パラメータの間隔値は、**[有効性チェックの頻度（Validity Check Frequency）]** エンタープライズパラメータの値よりも優先されます。

e) [保存（Save）] をクリックします。