証明書のモニタリングと失効タスクのフロー

証明書モニタリングの概要

管理者は、証明書を管理できる必要があります。どの証明書をいつ更新する必要があるかを認識することがその一部です。Cisco Unified Communications Manager には、どの証明書が更新間近であり、期限がいつであるかを管理者が把握するために役立つ自動システムがあります。次の操作を実行するようにシステムを設定できます。

- 証明書が期限切れに近づいたときに、証明書のステータスを継続的に監視し、電子メールで送信します。
- オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

オンライン証明書ステータス プロトコル（OCSP）による証明書失効（CRL）

Unified Communications Manager は、証明書失効をモニタリングするための OCSP をプロビジョニングします。スケジュールされた間隔、および証明書がアップロードされるたびにシステムが証明書のステータスをチェックし、有効性を確認します。

オンライン証明書状態プロトコル（OCSP）は、管理者がシステムの証明書要件を管理するのに役立ちます。OCSP を設定すると、証明書の有効性を確認したり期限切れの証明書をリアルタイムで無効化するための、シンプルかつ安全な自動メソッドを使用できます。

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。

有効性検査

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。

証明書の検証は、次のように行われます。

- 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、ステータスを確認するために OCSP 証明書に署名する必要があります。委任された信頼モデルが失敗すると、Unified Communications Manager が応答側の信頼モデル（TRP）にフォールバックし、指定された OCSP 応答の署名証明書を OCSP サーバから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ために、OCSP レスポンダが実行されている必要があります。

- **[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。OCSP の手動設定の詳細については、「OCSP による証明書失効の設定」を参照してください。

（注） リーフ証明書の場合、syslog、FileBeat、SIP、ILS、LBM などの TLS クライアントは、OCSP 要求を OCSP レスポンダに送信し、OCSP レスポンダからリアルタイムで証明書失効応答を受信します。

コモンクライテリア モードを有効にした状態で検証が実行されると、証明書に対して次のいずれかのステータスが返されます。

- **[良好（Good）]**：**良好**な状態とは、ステータスの問い合わせへの肯定的な応答を示します。この肯定的な応答は、少なくとも証明書が失効していないことを示しますが、必ずしもその証明書が発行済みであること、または、その応答が生成された時刻が証明書の有効期間内にあることを意味するものではありません。レスポンダが作成したアサーションに加えて、発行や有効性の肯定的なステートメントなど、レスポンダが作成した証明書のステータスに関する追加情報を伝送するためには、応答拡張を使用できます。
- **[失効（Revoked）]**：**失効**状態とは、証明書が失効している（恒久的または一時的に保留されている）ことを示します。
- **[不明（Unknown）]**：**不明**状態とは、OCSP レスポンダが要求された証明書を認識していないことを示します。

（注） コモンクライテリアモードでは、**失効**と**不明**の両方の場合において接続に失敗しますが、コモンクライテリアモードが有効になっていない状態では応答が**不明**ステータスである場合、接続に成功します。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する。
- 有効期限が切れた証明書を失効させる。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定 （3 ページ）	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。
ステップ 2	OCSP による証明書失効の設定 （4 ページ）	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。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

（注） [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、**[ツール（Tools）]** > **[コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択し、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

ステップ 1 （Unified Communications Manager の証明書モニタリングのために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書モニタリングのために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書モニタ（Certificate Management）]** を選択します。

ステップ 3 [通知開始時期（Notification Start Time）] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。

ステップ 4 [通知頻度（Notification Frequency）] フィールドには、通知を行う頻度を入力します。

ステップ 5 これはオプションです。[電子メール通知を有効にする（Enable E-mail notification）] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。

ステップ 6 [LSC モニタリングを有効にする（Enable LSC Monitoring）] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。

ステップ 7 [電子メール ID（E-mail IDs）] フィールドに、システムが通知を送信する電子メール アドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。

ステップ 8 [保存（Save）] をクリックします。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。OCSP による証明書失効の設定 （4 ページ）

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

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 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

ステップ 1 （Unified Communications Manager の証明書失効のために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書失効のために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

ステップ 3 [OCSP の有効化（Enable OCSP）] チェック ボックスをオンにして、次のタスクのいずれかを実行します。

- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する（Use configured OCSP URI）] ボタンを選択し、[OCSP 設定済み URI（OCSP Configured URI）] フィールドにレスポンダの URI を入力します。
- OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] ボタンを選択します。

ステップ 4 [失効チェックを有効にする（Enable Revocation Check）] チェック ボックスをオンにします。

ステップ 5 [チェック間隔（Check Every）] フィールドに失効チェックの間隔を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 これはオプションです。CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の 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 の管理から、**[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) [証明書の失効や有効期限（Certificate Revocation and Expiry）] で、[証明書有効性チェック（Certificate Validity Check）] パラメーターを [True] に設定します。

c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（注） **証明書失効**ウィンドウの [失効チェックを有効にする（Enable Revocation Check）] パラメーターの間隔値は、[有効チェック頻度（Validity Check Frequency）] エンタープライズ パラメーターの値よりも優先されます。

d) **[保存 (Save)]** をクリックします。