証明書失効/期限切れステータスの確認

この章では、[Unified Communications Manager Administration] においてセッションのために生成された証明書のステータスをチェックする方法の概要を示します。Unified Communications Manager とその他のサービスとの間の長時間セッションは、証明書サービスによって定期的にチェックされます。長時間セッションの継続時間は、6 時間以上です。チェックは、次の長時間セッションに対して実行されます。

- JTAPI/TAPI アプリケーションとの CTI 接続。
- Unified Communications Manager と SunOne サーバとの LDAP 接続。
- IPSec 接続。

また、証明書失効と有効期日を確認するためのエンタープライズパラメータの設定方法についても説明します。

エンタープライズ パラメータ [Certificate Revocation and Expiry] によって、証明書検証チェックを制御できます。失効と有効期日チェックのパラメータは、Unified Communications Manager の **[Enterprise Parameter]** ページで有効化します。このエンタープライズ パラメータ値が無効化された場合、長時間セッションの証明書の有効期限は確認されません。

Unified Communications Manager の [Operating System Administration] で [Enable Revocation] が選択され、失効と有効期日のチェック パラメータが有効として設定された場合、LDAP と IPSec 接続に対して証明書失効サービスがアクティブになります。IPSec 接続チェックの周期は、[Check Every] の値に基づきます。[Enable Revocation] チェックボックスがオフの場合、証明書の失効チェックは実行されません。

（注） X.509 公開キーインフラストラクチャ証明書と証明書失効リスト (CRL) プロファイルの一般 Izedtime 値は、グリニッジ標準時 (GMT) で表現する必要があり、さらに秒数 (つまり、時間は **YYYYMMDDHHMMSSZ**) を含める必要があります。番号は 0 です。GeneralizedTime 値には、秒の小数部分を含めることはできません。ピアエンティティがこのルールに違反する証明書を提供するか、またはピアエンティティからの信頼ストアに証明書が読み込まれた場合は、証明書の検証プロセスが失敗する可能性があります。

証明書失効/期限切れステータスの確認

証明書失効/期限切れステータスの確認

この章では、[Unified Communications Manager Administration] においてセッションのために生成された証明書のステータスをチェックする方法の概要を示します。Unified Communications Manager とその他のサービスとの間の長時間セッションは、証明書サービスによって定期的にチェックされます。長時間セッションの継続時間は、6 時間以上です。チェックは、次の長時間セッションに対して実行されます。

- JTAPI/TAPI アプリケーションとの CTI 接続。
- Unified Communications Manager と SunOne サーバとの LDAP 接続。
- IPSec 接続。

また、証明書失効と有効期日を確認するためのエンタープライズパラメータの設定方法についても説明します。

エンタープライズ パラメータ [Certificate Revocation and Expiry] によって、証明書検証チェックを制御できます。失効と有効期日チェックのパラメータは、Unified Communications Manager の **[Enterprise Parameter]** ページで有効化します。このエンタープライズ パラメータ値が無効化された場合、長時間セッションの証明書の有効期限は確認されません。

Unified Communications Manager の [Operating System Administration] で [Enable Revocation] が選択され、失効と有効期日のチェック パラメータが有効として設定された場合、LDAP と IPSec 接続に対して証明書失効サービスがアクティブになります。IPSec 接続チェックの周期は、[Check Every] の値に基づきます。[Enable Revocation] チェックボックスがオフの場合、証明書の失効チェックは実行されません。

（注） X.509 公開キーインフラストラクチャ証明書と証明書失効リスト (CRL) プロファイルの一般 Izedtime 値は、グリニッジ標準時 (GMT) で表現する必要があり、さらに秒数 (つまり、時間は **YYYYMMDDHHMMSSZ**) を含める必要があります。番号は 0 です。GeneralizedTime 値には、秒の小数部分を含めることはできません。ピアエンティティがこのルールに違反する証明書を提供するか、またはピアエンティティからの信頼ストアに証明書が読み込まれた場合は、証明書の検証プロセスが失敗する可能性があります。

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。

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。

OCSP 応答での委任信頼モデルのサポート

Online Certificate Status Protocol（OCSP）により、デバイスは特定の証明書のステータスに関するリアルタイム情報を取得できます。認証ステータスの例としては [Good]、[Revoked]、[Unknown] などが挙げられます。

Unified Communications Manager は OCSP を使用して、Unified Communications Manager の信頼ストアにアップロードされるサードパーティの証明書を検証します。Unified Communications Manager は、OCSP レスポンダ URL が HTTP 経由で OCSP レスポンダ サーバに接続するよう要求します。レスポンダに HTTP 要求を送信して証明書を検証します。

Unified Communications Manager は現在、OCSP 応答が OCSP サーバの自己署名証明書によって署名される、OCSP の信頼レスポンダ モデルをサポートしています。この自己署名証明書は OCSP 要求を開始する前に信頼ストアにアップロードされます。この証明書は OCSP 応答の署名を検証するために使用されます。

Unified Communications Manager 11.0 以降では OCSP レスポンダ の委任信頼モデル（DTM）をサポートしています。OCSP 応答 は自己署名証明書では承認されませんが、認証局（ルート CA または 下位 CA）から発行されます。CA 証明書は OCSP レスポンダ証明書を検証します。Unified Communications Manager 信頼ストアに OCSP レスポンダ証明書を発行した CA 証明書が、OCSP 応答が署名した証明書の代わりに必要です。OCSP 応答を受信すると、応答の署名の検証に CA の証明書が使用されます。

（注） DTM 実行障害が発生しても、OCSP 応答は自己署名証明書を使用して検証されます。