CUCM での証明書および権限の概要

目次

概要

このドキュメントの目的は、証明書と認証局の基本を理解することです。 このドキュメントは、Cisco Unified Communications Manager（CUCM）の暗号化機能や認証機能に関する他のシスコドキュメントを補完するものです。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

証明書の目的

エンドポイント間では、データの信頼性を構築するために、認証や暗号化の際に証明書が使用されます。 これにより、エンドポイントは意図したデバイスと確実に通信できるようになり、2 台のエンドポイント間でデータを暗号化するオプションが備わります。

証明書の観点からの信頼の定義

証明書の最も重要な部分は、エンドポイントが信頼できるエンドポイントを定義することです。このドキュメントでは、データを暗号化する方法と、目的の Web サイト、電話、FTP サーバなどとデータを共有する方法を理解および定義するのに役立つ情報を提供します。

システムが証明書を信頼する場合、これは適切なエンドポイントと情報を共有していることに 100 % の信頼を置いていると宣言する証明書がシステムにプレインストールされていることを意味します。 そうでない場合、システムはこれらのエンドポイント間の通信を終了します。

これに関する非技術的な例は運転免許証です。 この免許証（サーバ/サービス証明書）は、自身で主張するその人の身元が正しいこと、 および国の車両管理局（DMV）（認証局）から権限を付与された地方の車両管理支局（中間証明書）から免許証を取得したことを証明するために使用されます。 職員に免許証（サーバ/サービス証明書）を提示する必要があるときには、職員は DMV 支局（中間証明書）と車両管理局（認証局）が信頼できることを知っており、この免許証がその機関（認証局）によって発行されたことを確認できます。 職員は身元を確認し、自身で主張するその人の身元が正しいことを信頼します。 DMV（中間証明書）によって署名されていない偽の免許証（サーバ/サービス証明書）を提示した場合、職員は、自身で主張するその人の身元を信頼しません。 このドキュメントの残りの部分では、証明書階層に関する技術的な詳細説明を提供します。

ブラウザによる証明書の使用法

1. Web サイトにアクセスするときには、http://www.cisco.com などの URL を入力します。
2. DNS がそのサイトをホストするサーバの IP アドレスを見つけます。
3. ブラウザがそのサイトに移動します。

証明書がなければ、不正な DNS サーバが使用されていないか、または別のサーバにルーティングされていないかを知ることはできません。 証明書により、銀行の Web サイトなどの目的の Web サイトに適切かつ安全にルーティングされ、そこで入力する個人情報または機密情報が保護されることが保証されます。

表示されるアイコンはブラウザによって異なりますが、通常は次のような南京錠がアドレス バーに表示されます。

1. 南京錠をクリックすると、次のウィンドウが表示されます。**図 1： Web サイトの識別**

2. [証明書の表示] をクリックしてサイトの証明書を表示します。次に例を示します。**図 2： 証明書の情報、[General] タブ** 強調されている情報が重要です。[Issued by]：システムがすでに信頼している会社または認証局（CA）です。[Valid from/to]：この証明書が使用可能な日付範囲です（証明書の CA を信頼していることがわかっているにもかかわらず、その証明書が有効でないことがあります。 必ず日付を調べて、証明書の有効期限が切れていないかどうかを確認してください）。**ヒント：** ベスト プラクティスは、カレンダーにリマインダを作成し、有効期限が切れる前に証明書を更新することです。 こうすることで今後の問題を回避できます。

PEM 証明書と DER 証明書の違い

PEM は ASCII で、 DER はバイナリです。 図 3 に、PEM 証明書の形式を示します。

図 3： PEM 証明書の例
図 4 に、DER 証明書を示します。

図 4： DER 証明書の例
VeriSign や Thawt などのほとんどの CA 企業は、顧客への証明書の送信に PEM 形式を使用します。PEM 形式は電子メールで扱いやすいためです。 顧客は、文字列全体をコピーし、 **----------BEGIN CERTIFICATE----------** および **----------END CERTIFICATE----------**を含め、その文字列をテキスト ファイルにペーストし、.PEM または .CER の拡張子で保存する必要があります。

Windows は、独自の証明書管理アプレットで DER 形式と CER 形式を読み取り、図 5 のような証明書を表示します。

図 5： Certificate Information
場合によっては、デバイスで特定の形式（ASCII またはバイナリ）が必要になります。 これを変更するには、CA から必要な形式の証明書をダウンロードするか、https://www.sslshopper.com/ssl-converter.html などの SSL コンバータ ツールを使用します。

証明書階層

あるエンドポイントからの証明書を信頼するには、サードパーティ CA との信頼関係がすでに確立されている必要があります。たとえば、図 6 は 3 つの証明書の階層を示しています。

図 6： 証明書階層
- **VeriSign** は CA です。
- **VeriSign Class 3 Extended Validation SSL CA** は、中間証明書または署名サーバ証明書（自身の名前で証明書を発行することが CA から許可されているサーバ）です。
- **www.website.com** はサーバ証明書またはサービス証明書です。

エンドポイントは、SSL ハンドシェイク（詳細は下記を参照）によって提供されるサーバ証明書が信頼できることを確認する前に、まず CA と中間証明書の両方が信頼できることを確認する必要があります。 この信頼の仕組みをより深く理解するには、このドキュメントの次のセクションを参照してください。 **証明書の観点からの「信頼」の定義**

自己署名証明書とサードパーティ証明書の比較

自己署名証明書とサードパーティ証明書の主な違いは、誰が証明書に署名したか、その署名者を

信頼するかどうかです。

自己署名証明書は、証明書を提供するサーバによって署名される証明書です。 したがって、サーバ/サービス証明書と CA 証明書は同じです。

サードパーティ CA は、パブリック CA (VeriSign、Entrust、Digicert など) 、またはサーバ/サービス証明書の有効性を管理するサーバ (Windows 2003、Linux、UNIX、IOS など) によって提供されるサービスです。

それぞれが CA になることができます。最も重要なのは、使用しているシステムがその CA を信頼するかどうかです。

共通名とサブジェクトの別名

共通名 (CN) とサブジェクトの別名 (SAN) は、IP アドレス、または要求されるアドレスの完全修飾ドメイン名 (FQDN) への参照です。 たとえば、「https://www.cisco.com」と入力する場合は、CN または SAN のヘッダーに www.cisco.com が含まれている必要があります。

図 7 の例では、証明書に www.cisco.com という CN があります。 ブラウザからの www.cisco.com への URL 要求では、URL FQDN と証明書の情報が照合されます。 この場合、これらは一致し、SSL ハンドシェイクに成功したことが表示されます。 この Web サイトは正しい Web サイトであることが確認され、デスクトップと Web サイト間の通信が暗号化されます。

図 7： Web サイトの確認

同じ証明書に、3 つの FQDN/DNS アドレスに対応する SAN ヘッダーがあります。

図 8： SAN ヘッダー

この証明書では、www.cisco.com (CN でも定義されています) 、cisco.com、および cisco-images.cisco.com を認証および確認できます。 つまり、cisco.com と入力しても、この同じ証明書でこの Web サイトを認証および暗号化することができます。

CUCM は SAN ヘッダーを作成できます。 SAN ヘッダーの詳細については、サポート コミュニティにある Jason Burn のドキュメント『CCMAdmin Web GUI 証明書の CUCM へのアップロード』を参照してください。

ワイルド カード証明書

ワイルドカード証明書は、アスタリスク (*) を使用して URL セクションの任意の文字列を表す証明書です。 たとえば、www.cisco.com、ftp.cisco.com、ssh.cisco.com などに対応する証明書が必要な場合、管理者は *.cisco.com の証明書を作成するだけで済みます。 コストを節約するために、管理者が購入する必要がある証明書は 1 つだけです。複数の証明書を購入する必要はありません。

この機能は、Cisco Unified Communications Manager （ CUCM ）では現在サポートされていません。 ただし、この機能拡張については次で追跡することができます。 CSCta14114： CUCM と秘密キーのインポートでのワイルドカード証明書のサポートの要求。

証明書の識別

複数の証明書に同じ情報が含まれている場合は、それらが同じ証明書かどうかを確認できます。 すべての証明書には一意のシリアル番号があります。 このシリアル番号を使用して、証明書が同

じ証明書であるか、再生成されたものであるか、または偽造されたものであるかを確認できます。 図 9 に例を示します。

図 9： Certificate Serial Number

CSR とその目的

CSR は証明書署名要求（Certificate Signing Request）のことです。 CUCM サーバ用のサードパーティ証明書を作成する場合は、CA に提示する CSR が必要です。 この CSR は PEM（ASCII）証明書によく似ています。

注: これは証明書ではないため、証明書としては使用できません。

CUCM は、Web GUI を介して CSR を自動的に作成します。 [Cisco Unified Operating System Administration] > [Security] > [Certificate Management] > [Generate CSR] > 証明書を作成するサービスを選択 > [Generate CSR]。 このオプションを使用するたびに、新しい秘密キーと CSR が生成されます。

注: 秘密キーは、このサーバとサービスに固有のファイルです。 秘密キーは誰にも渡さないでください。 秘密キーを誰かに渡すと、証明書のセキュリティが損なわれます。 また、古い CSR を使用して証明書を作成する場合は、同じサービス用の新しい CSR を再生成しないでください。 CUCM によって古い CSR と秘密キーが削除され、両方とも置き換えられます。その結果、古い CSR が使用できなくなります。

CSR の作成方法の詳細については、サポート コミュニティにある Jason Burn のドキュメント『CCMAdmin Web GUI 証明書の CUCM へのアップロード』を参照してください。

エンドポイントと SSL/TLS ハンドシェイク プロセス間での証明書の使用

ハンドシェイク プロトコルは、データ転送セッションのセキュリティ パラメータをネゴシエートする一連の順序付けられたメッセージです。 『SSL/TLS in Detail』を参照してください。 このドキュメントには、ハンドシェイク プロトコルのメッセージ シーケンスが記載されています。 これらのメッセージはパケット キャプチャ（PCAP）で確認できます。 詳細には、クライアントとサーバ間で送受信される初期メッセージ、後続のメッセージ、最終メッセージが含まれます。

CUCM による証明書の使用法

tomcat と tomcat-trust の違い

証明書を CUCM にアップロードするときには、Cisco Unified Operating System Administration > [Security] > [Certificate Management] > [Find] でサービスごとに 2 つのオプションを使用できます。

次に、CUCM での証明書の**管理**に使用できる 5 つのサービスを示します。

- tomcat
- IPSec
- callmanager
- capf

- tvs（CUCM リリース 8.0 以降）

次に、CUCM に証明書を**アップロード**できるサービスを示します。

- tomcat
- tomcat-trust
- IPSec
- ipsec-trust
- callmanager
- callmanager-trust
- capf
- capf-trust

これらは、CUCM リリース 8.0 以降で使用できるサービスです。

- tvs
- tvs-trust
- phone-trust
- phone-vpn-trust
- phone-sast-trust
- phone-ctl-trust

これらのタイプの証明書の詳細については、『リリース別 CUCM セキュリティ ガイド』を参照してください。 このセクションでは、サービス証明書と信頼証明書の違いについてのみ説明します。

たとえば、**tomcat** では、**tomcat-trust** で CA と中間証明書をアップロードします。その結果、この CUCM ノードは、CA および中間サーバによって署名されたすべての証明書が信頼できることを確認できます。 tomcat 証明書は、エンドポイントがこのサーバに HTTP 要求を実行した場合に、このサーバ上の tomcat サービスによって提供される証明書です。 tomcat がサードパーティ証明書を提供できるようにするには、CA と中間サーバが信頼できることを CUCM ノードが確認する必要があります。 したがって、tomcat（サービス）証明書をアップロードする前に、CA と中間証明書をアップロードする必要があります。

CUCM に証明書をアップロードする方法を理解するのに役立つ情報については、サポート コミュニティにある Jason Burn の『CCMAdmin Web GUI 証明書の CUCM へのアップロード』を参照してください。

各サービスには固有のサービス証明書と信頼証明書があります。 サービスと証明書が別々に機能するようになることはありません。 つまり、tomcat-trust サービスとしてアップロードされた CA および中間証明書は、callmanager サービスでは使用できません。

注: CUCM の証明書はノード単位です。 したがって、パブリッシャにアップロードされた証明書と同じ証明書をサブスクライバに提供する必要がある場合、CUCM リリース 8.5 より前のリリースでは、証明書を各サーバと各ノードにアップロードする必要があります。 CUCM リリース 8.5 以降では、アップロードされた証明書をクラスタ内の残りのノードに複製するサービスがあります。

注: ノードごとに異なる CN があります。 そのため、サービス固有の証明書を提供するには、各ノードで CSR を作成する必要があります。

CUCM セキュリティ機能についてその他の具体的な疑問がある場合は、セキュリティ ドキュメントを参照してください。

結論

このドキュメントは、証明書に関する高レベルの知識を身に付けるのに役立ちます。 このテーマは重要であり、より詳しく説明することもできますが、ここでは証明書の扱いに十分慣れ親しんでいただくだけにとどめます。 CUCM のセキュリティ機能について疑問がある場合は、『リリース別 CUCM セキュリティ ガイド』を参照してください。

関連情報

- Cisco Unified Communications Manager (CallManager) のメンテナンスおよびセキュリティ ガイド
- Cisco Unified Communications Manager (CallManager)
- Cisco Unified Communications Manager Express
- シスコ サポート コミュニティ： CCMAdmin Web GUI 証明書の CUCM へのアップロード
- バグ CSCta14114： CUCM と秘密キーのインポートでのワイルドカード証明書のサポートの要求
- Cisco Emergency Responder (CER) の説明
- テクニカルサポートとドキュメント - Cisco Systems