HTTPS の復号化に使用する WSA 証明書

目次

概要

このドキュメントでは、Cisco Web セキュリティ アプライアンス（WSA）上で HTTPS 復号化に使用すべき証明書のタイプについて説明します。

証明書の概要

WSA は、HTTPS 復号化で使用する最新の証明書と秘密キーを選択することができます。 ただし、すべての x.509 証明書が機能するわけではないため、使用すべき証明書のタイプで混乱が生じる可能性があります。

証明書には、次の 2 つの主要なタイプが存在します。 **サーバ証明書**と**ルート証明書**です。 すべての x.509 証明書に、証明書のタイプを識別する Basic Constraints フィールドが含まれています。

- **Subject Type=End Entity**：サーバ証明書
- **Subject Type=CA**：ルート証明書

> **注:** WSA 上の HTTPS 復号化には、認証局（CA）署名証明書とも呼ばれるルート証明書を使用する必要があります。

ルート証明書

ルート証明書は、サーバ証明書に署名するために特別に作成されます。 独自の CA を作成して運用し、独自のサーバ証明書に署名することができます。

> **注:** ルート証明書は他の証明書にしか署名しないため、それを Web サーバ上の HTTPS 暗号

化および復号化に使用することはできません。

WSA は、ルート証明書を使用して、HTTPS 復号化用のサーバ証明書を積極的に生成する必要があります。 ルート証明書に使用可能な 2 つのオプションがあります。

- WSA 上でルート証明書を生成します。 WSA は、独自のルート証明書と秘密キーを作成し、このキーのペアを使用してサーバ証明書に署名します。
- 現在のルート証明書とその秘密キーを WSA にアップロードすることができます。 ルート証明書の Common Name（CN）フィールドは、その署名を含むサーバ証明書を信頼するエンティティ（通常は法人名）を識別します。

  注: サーバ証明書を信頼するには、公開キーが Web ブラウザで入力されたルート証明書で署名する必要があります。

サーバ証明書

サーバ証明書は、HTTPS 暗号化および復号化に使用され、特定のサーバの信頼性を確認するために特別に作成されます。 サーバ証明書は、CA ルート証明書を使用して CA によって署名されます。 CA の一般的な例が VeriSign と Thawte です。

注: サーバ証明書は他の証明書に署名するためには使用できません。 そのため、サーバ証明書が WSA にインストールされている場合は、HTTPS 復号化が機能しません。

サーバ証明書内の CN フィールドは、証明書が使用されるホストを指定します。 たとえば、**https://www.verisign.com** は **www.verisign.com** の CN を持つサーバ証明書を使用します。

関連情報

- Web セキュリティ アプライアンス（WSA）証明書の使用（HTTPS 復号化、GUI ログイン、クレデンシャル暗号化）
- WSA で HTTPS プロキシおよび証明書署名要求（CSR）オプションを有効にする手順
- WSA で HTTPS プロキシおよびルート/中間証明書オプションのアップロードを有効にする手順
- テクニカル サポートとドキュメント – Cisco Systems