Mac OS X Serverの
WebサービスとSSL暗号化通信

2011/01/13
Mac OS X Server Night! ライトニングトーク発表資料

松尾 篤（株式会社エミック）

株式会社エミック

Mac OS X Serverの
Webサービス

WebサーバーはApache HTTP Server 2.2.15

（Mac OS X Server 10.6.6の場合）

HTTPとHTTPSの違い

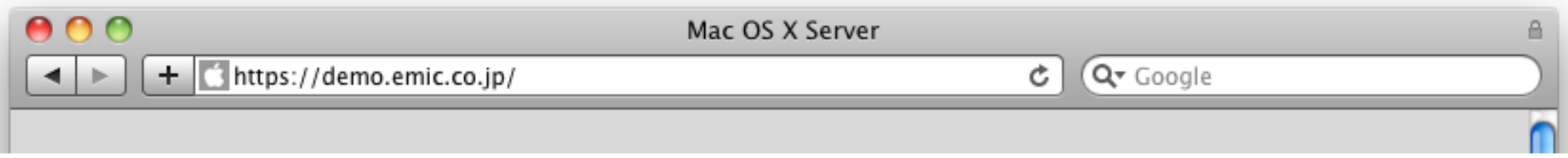
- HTTPによるブラウザーとWebサーバー間の通信は暗号化されていない
- 通信内容の暗号化にはSSL/TLSへの対応が必要（HTTP over SSL/TLS）
- HTTPSのポート番号は443番

SSLの重要な役割

- Webサイトとの通信を暗号化して安全な通信環境を実現
  （盗聴や改ざんを防止）
- サイト運営団体の実在性等を確認

WebサーバーのSSL対応

- サイトにSSLサーバー証明書を導入
- https://で始まるURLでサーバーに接続
- Webブラウザーに鍵マークのアイコンが表示されることを確認



証明書の導入手順

- サーバーの準備・確認
- 秘密鍵とCSRの生成
- 認証局に申請（認証局から購入）
- 認証局が発行した証明書をサーバーにインストール

サーバーの準備・確認

- SSL対応の準備が整っているか確認
- Webサーバーの種類
- サーバーのネットワーク構成
- コモンネーム（FQDN）の決定

秘密鍵とCSRの生成

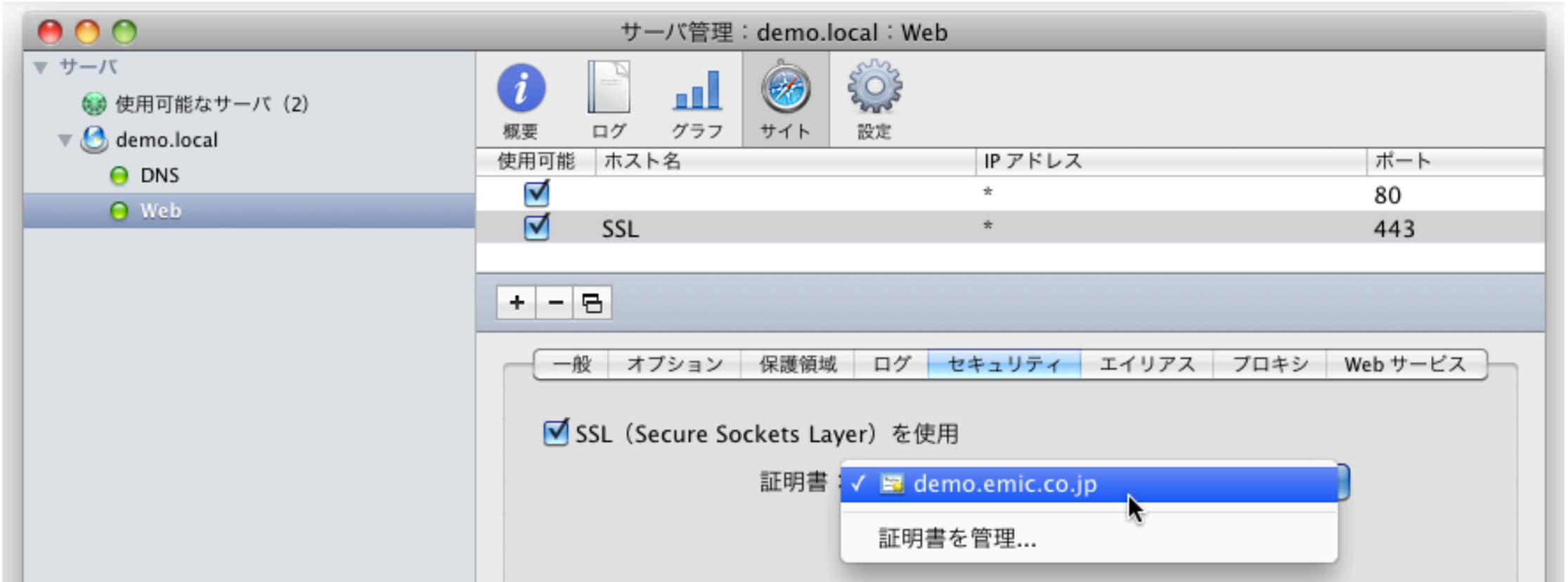
- CSR：Certificate Signing Request
- コマンドラインで生成する場合はopensslコマンドを使用

発行申請

- CSRや申請者情報を認証局に送付
- 場合によっては書類の提出や電話による申請意思の確認（コールバック）

証明書のインストール

- 送られてくるSSLサーバー証明書及び中間CA証明書をサーバーにインストール



概要 ログ グラフ ファイル共有 サーバアップデート 証明書 アクセス 設定

証明書識別情報は公開証明書と秘密鍵で構成されます。次の証明書識別情報を、サービスを提供するためのネットワーク通信のセキュリティ保護に利用できます。

名前	有効期限

証明書識別情報を作成...
証明書識別情報を読み込む...

サーバ管理：demo.local：証明書

サーバ
使用可能なサーバ（2）
demo.local

秘密鍵と証明書の情報が含まれるファイルを追加します。サーバの証明書 ID を作成するときは、これらのファイルを読み込んでください。

秘密鍵
demokey.pem

demo.emic.co.jp
発行元：VeriSign Trial Secure Server CA – G2

1 個の識別情報なし 証明書 が追加されます

キャンセル 読み込む

設定

明書識別情報を、サービス
できます。

有効期限

サーバ管理：demo.local：証明書

概要 ログ グラフ ファイル共有 サーバアップデート 証明書 アクセス 設定

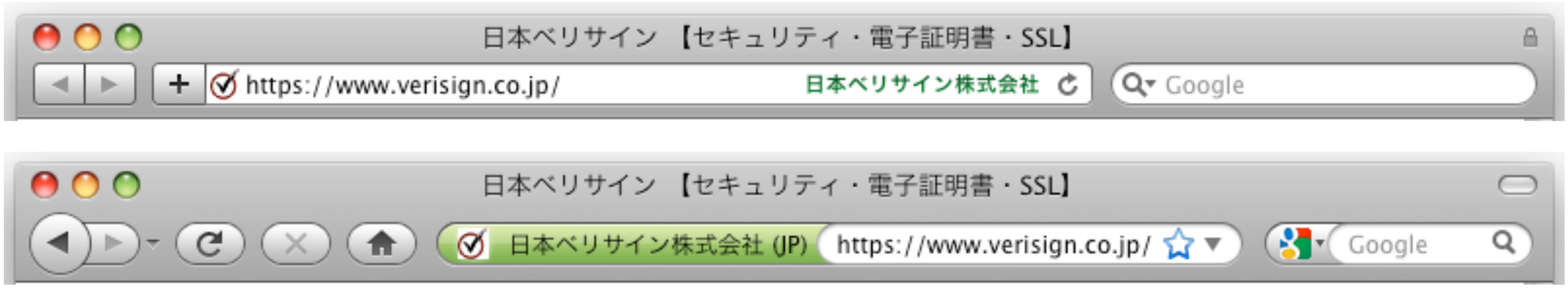
証明書識別情報は公開証明書と秘密鍵で構成されます。次の証明書識別情報を、サービスを提供するためのネットワーク通信のセキュリティ保護に利用できます。

名前	有効期限
demo.emic.co.jp	11/01/27

注意点

- 中間CA証明書のインストールを忘れないようにする
- 名前ベースのバーチャルホストでSSLを利用する場合には要注意（TLS拡張のServer Name Indicationへの対応が必要）

EV SSL証明書



- 厳格な審査で実在証明確認を強化
- アドレスバーにサイト運営者の組織名称が緑色で表示

  （Internet Explorer 7以降、 Safari 3.2以降、 Firefox 3以降、 Opera 9.5以降、 Chrome 1.0以降）

まとめ

- HTTPSでは通信内容が暗号化される
- 暗号化通信では接続先の確認が重要
- モダンブラウザーではEV SSLに対応済