SSL暗号化通信を利用した
ネットワークセキュリティの向上

2016/11/11

FileMaker カンファレンス 2016講演資料

松尾篤（株式会社エミック）

自己紹介

- 松尾　篤（まつお　あつし）
  - ✓ 株式会社エミック　代表取締役
  - ✓ FileMaker Server対応Webフレームワーク「INTER-Mediator」コミッター
  - ✓ FileMaker 8 / 9 / 10 / 11 / 12 / 13 / 14 / 15 Certified Developer
  - ✓ http://www.famlog.jp/

株式会社エミック

- FileMaker Serverに特化したセキュリティコンサルティングサービスの提供を開始
- FileMaker製品対応ホスティングサービスを1998年から提供
- **https://www.emic.co.jp/**

Publisher

FileMaker Proデータベースから、
プログラムなしでWebアプリを生成

デモを
ご覧下さい

FileMaker Server ユーザ接続／同時接続ライセンスは不要

FileMaker Proでデータベースを作成

カスタムWebアプリを自動生成

今回の話題

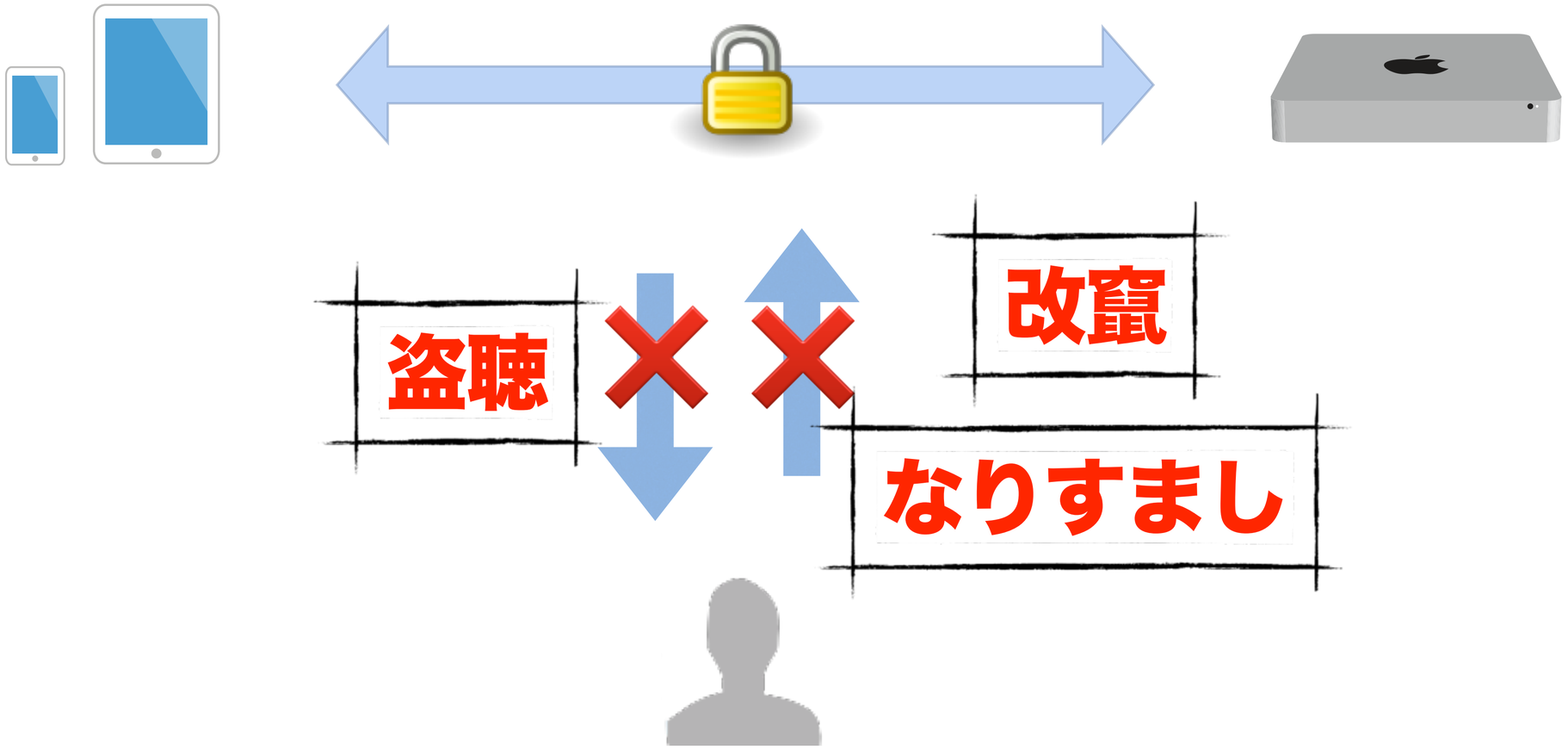
1. SSLの概要と最近の状況
2. FileMaker製品でSSLを利用するには
3. FileMaker 15における新機能と改善点

1. SSLの概要と最近の状況

例えばこのようなとき

- 重要な情報をインターネット上でやり取りする際にデータを安全に送受信したい

暗号化通信



Secure Sockets Layer

- データを暗号化してやり取りする手順の決まり（プロトコル）
- クライアント・サーバー間の通信を暗号化できる

FileMaker Serverは SSL暗号化通信に対応

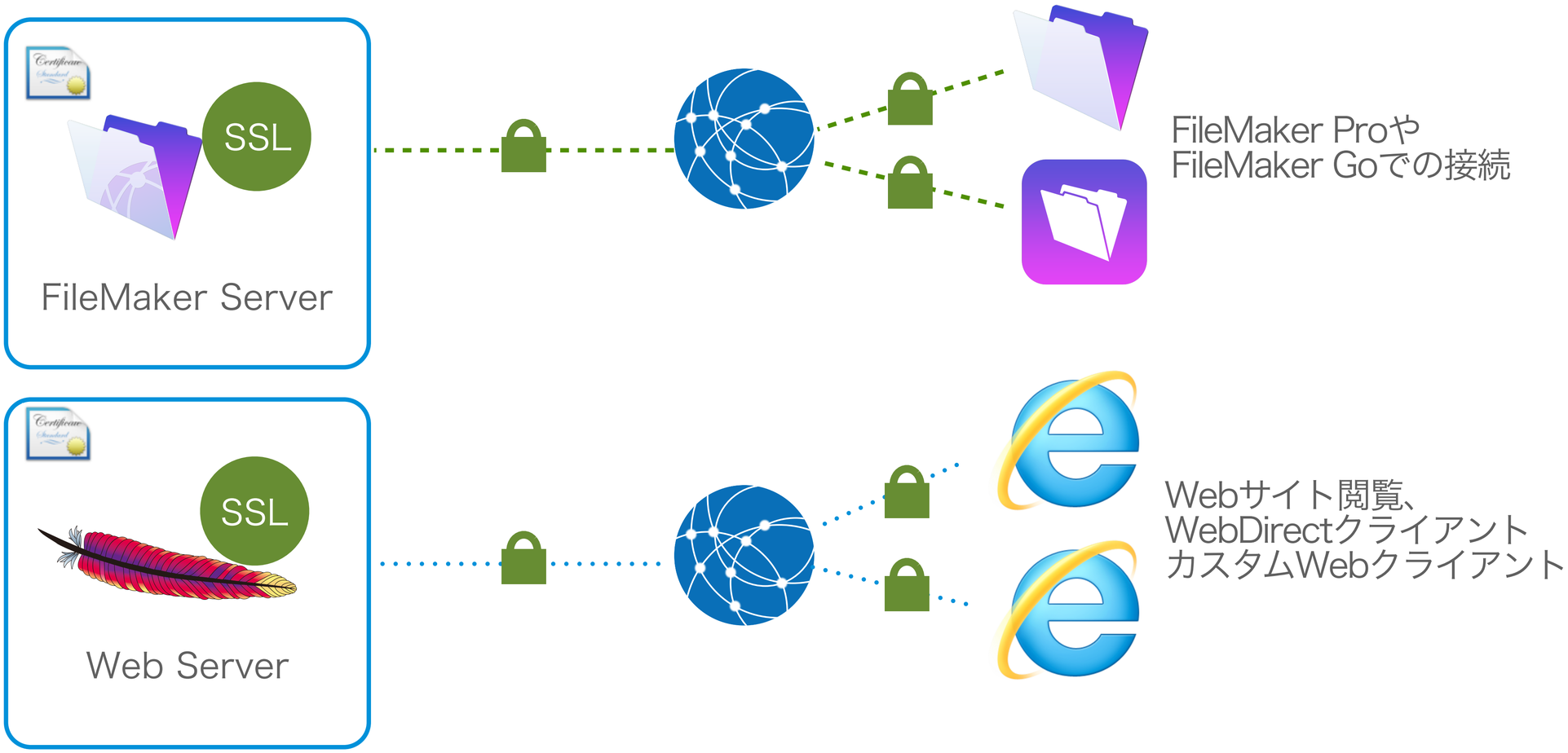
- FileMaker Pro/GoとFileMaker Server間の通信（TCP 5003番ポート）
- ブラウザーとWebサーバー間の通信（TCP 443／16000番ポート）

SSLの利用例

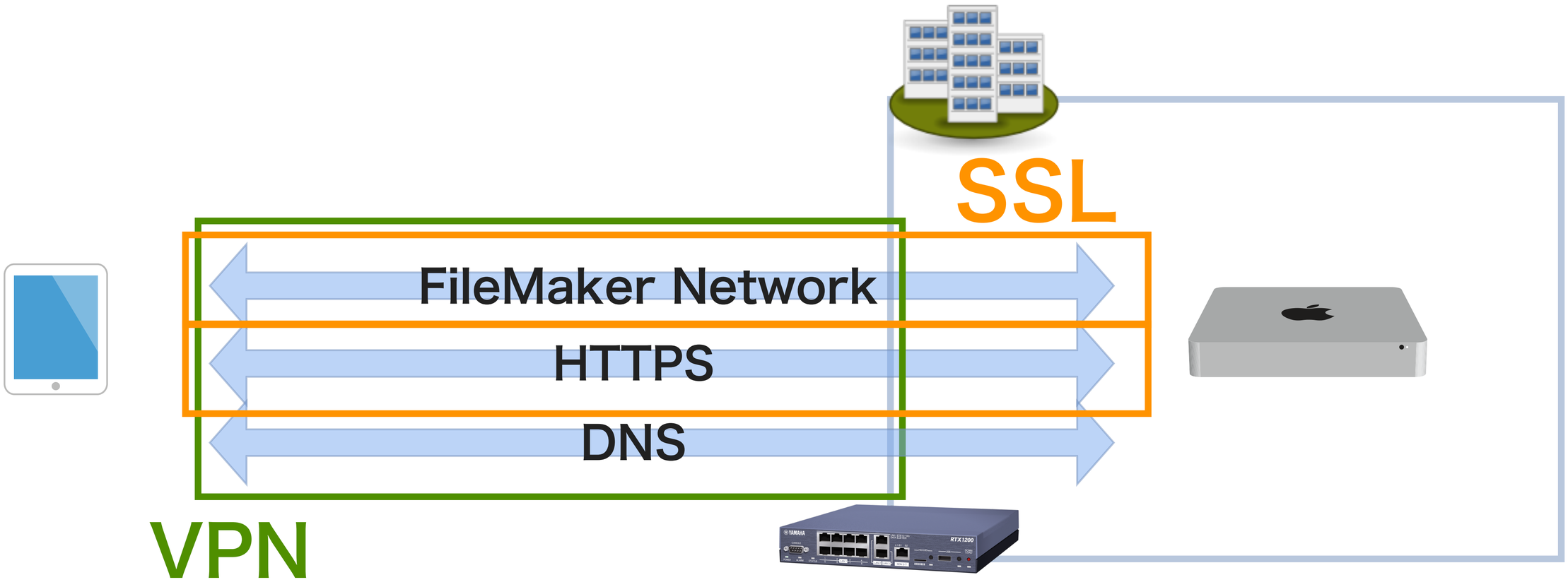
- FileMaker Server Admin Console
- TCP 5003番ポートを利用したネットワーク共有
  （要FileMaker Server）
- FileMaker Server にアップロード
- FileMaker Pro 15（ユーザ接続用）による
  FileMaker Server 15へのサインイン etc.

  （参考）http://filemaker-jp.custhelp.com/app/answers/detail/a_id/14940

SSLはサービスごとに対応が必要



参考：SSLとVPNの違い



TLS：SSLの後継規格

- 最新の規格は**TLS 1.2**（TLS：Transport Layer Security）
  - 現在TLS 1.3の策定が進められている
- SSL/TLSは世界で最も利用されている暗号化通信の方法

SSL/TLS関連最新情報

- 安全上の理由からSHA-1は廃止に
- 常時SSL化・HTTPS対応の動きが加速

安全上の理由から SHA-1は廃止に

- 署名ハッシュアルゴリズムがSHA-1であるSSLサーバー証明書の発行が終了
- SHA-1証明書のサポートは今年まで
- SHA-2（SHA-256）へ移行

常時SSL化の動きが加速

- Web上のすべての通信をHTTPS化
  - GoogleがSEOでHTTPSを優遇
  - 無料のSSLサーバー証明書を発行する Let's Encryptの普及
  - iOSアプリのApp Transport Security 導入が来年から義務化

HTTPSのみで利用可能

- HTTP/2
- Geolocation API
- Service Worker
- Credential Management API etc.

2. FileMaker製品で
SSLを利用するには

どのバージョンが必要？

（2016年11月現在）

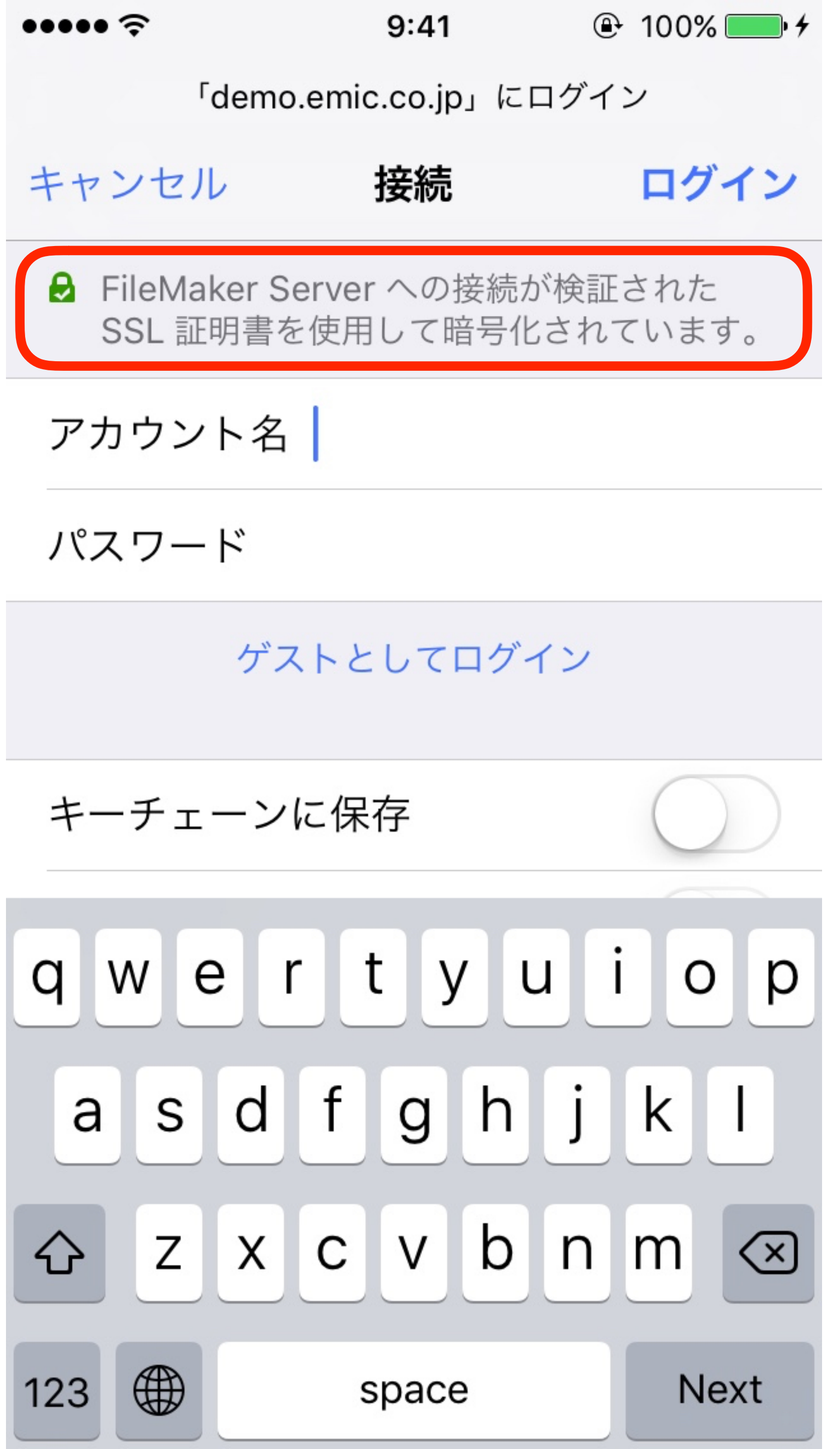
- FileMaker Server 13.0v9以降
- FileMaker Pro 13.0v9以降
  （FileMaker Pro Advancedも同様）
- FileMaker Go 13.0.9以降

次のようなエラーに遭遇したことはありませんか？


9:41
100%
ホスト
セキュリティ警告
FileMaker Go では demo-fm.dbsv.jp を識別できません。このホストに接続しますか?
接続しない
接続
常に接続を許可
最近使った項目
デバイス
ホスト


9:41
100%
「demo-fm.dbsv.jp」にログイン
キャンセル
接続
ログイン
FileMaker Server の SSL 証明書が検証できません。実際の接続先に偽装したサーバーに接続している可能性があり、機密情報が漏えいするおそれがあります。
アカウント名
パスワード
ゲストとしてログイン
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
Next


9:41
100%
「demo-fm.dbsv.jp」にログイン
キャンセル
接続
ログイン
FileMaker Server の SSL 証明書が検証できません。実際の接続先に偽装したサーバーに接続している可能性があり、機密情報が漏えいするおそれがあります。
アカウント名
パスワード
ゲストとしてログイン
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
Next

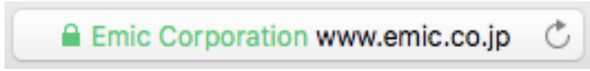

9:41
100%
「demo.emic.co.jp」にログイン
キャンセル
接続
ログイン
FileMaker Server への接続が検証された SSL 証明書を使用して暗号化されています。
アカウント名
パスワード
ゲストとしてログイン
キーチェーンに保存
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
Next

SSL導入にあたって

- 認証局から**証明書を購入**
- 管理下に置いている**ドメイン名が必要**
  - 例：emic.co.jp

サポートされる証明書の販売元および商品名	種類	署名ハッシュアルゴリズム
シマンテック・ウェブサイトセキュリティ シマンテック セキュア・サーバID	実在認証型	SHA-2
コモドジャパン 企業認証タイプ SSL（Elite SSL Certificate）、EVタイプ SSL*	実在認証型	SHA-2
ジオトラスト トゥルービジネスID	実在認証型	SHA-2
DigiCert * ワイルドカード証明書*、マルチドメイン証明書*、EV マルチドメイン証明書*	実在認証型	SHA-2
Thawte SSL123	ドメイン認証型	SHA-2 (under SHA-1 Root)
GoDaddy Standard SSL	ドメイン認証型	SHA-2

*がついているものはFlleMaker 15で対応、上記以外に**InCommon**の証明書も15ではサポート対象

	ドメイン認証 (DV)	実在認証 (OV)	拡張認証 (EV)
価格（年間）の目安	約8,000円～ (0～31,300円)	25,800円～ (約9,000～138,000円)	69,600円～ (約22,000～219,000円)
用途	個人、開発用、 社内ネットワーク用	企業、一般用	企業、一般用
運営者の実在性審査	-	実施	厳格に実施
アドレスバー	組織名は表示されない	組織名は表示されない	**組織名が表示される** 
証明書ビューア	組織名は表示されない	**組織名が表示される**	**組織名が表示される**

SSL対応手順概要

1.認証局に提出する**CSRファイル**（と非公開のプライベートキーファイル）を生成

2.認証局から発行された**SSLサーバー証明書**をFileMaker Serverにインポート

3.Admin Consoleで［**データベース接続にSSL を使用する**（保護された接続が必要）］および［**プログレッシブダウンロードに SSL を使用する**］設定を有効化

CSRの生成

- 認証局に提出する署名リクエスト
  (Certificate Signing Request)
  - **fmsadminコマンド**で生成可
  - FileMaker Server 15であれば**Admin Console**上でCSRファイルを生成できる
  - 認証局で案内されている**opensslコマンド**を使った一般的な方法もOK

証明書のインポート

- FileMaker Server 14以降では**Admin Console**上でインポートが可能
  - FileMaker Server 15で中間CA証明書のインポートもできるように改善
- Admin Consoleでインポートできない場合は**fmsadminコマンド**（fmsadmin certificate import）を利用

証明書のインポート

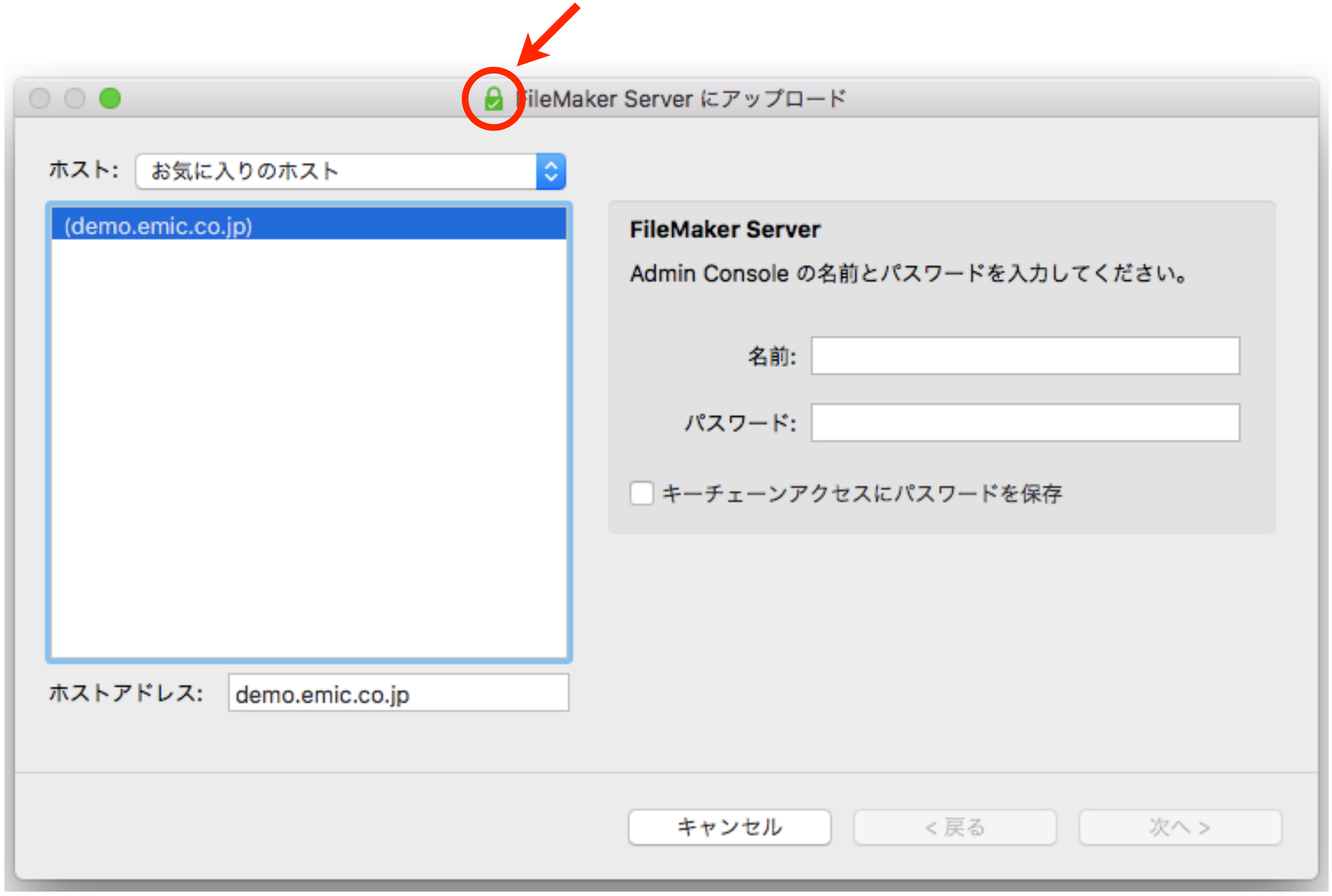

証明書のインポート
証明書をインポートすると、証明機関 (CA) から受け取った署名済み証明書ファイルと証明書署名要求の作成時に作成したプライベートキーファイル (serverKey.pem) が結合されます。
署名済みの証明書ファイル:
参照...
プライベートキーファイル:
参照...
CA から受け取った証明書の種類によっては、中間証明書ファイルも選択する必要があります。
中間証明書ファイル:
参照...
プライベートキーファイル (serverKey.pem) の作成時に暗号化パスワードを設定した場合は、プライベートキーのパスワードを入力します。
プライベートキーパスワード:
キャンセル
インポート

SSLを使用する設定に

- Admin Consoleで［データベース接続に SSL を使用する（保護された接続が必要）］設定を有効化
- データベースサーバーとWeb公開エンジンを再起動

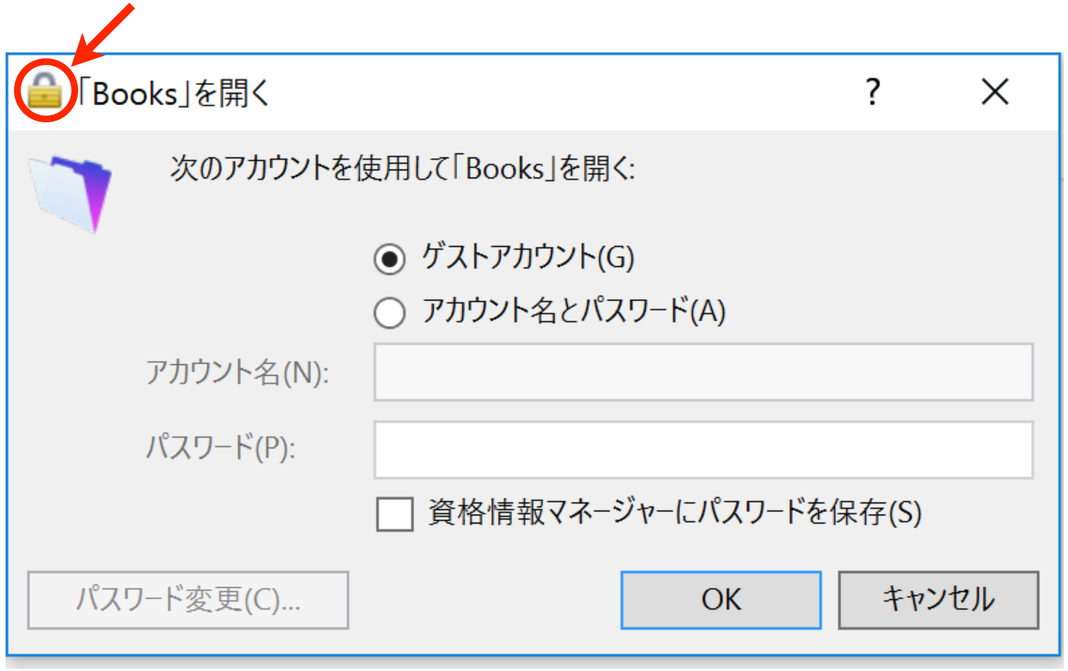
FileMaker Go/Pro からの接続

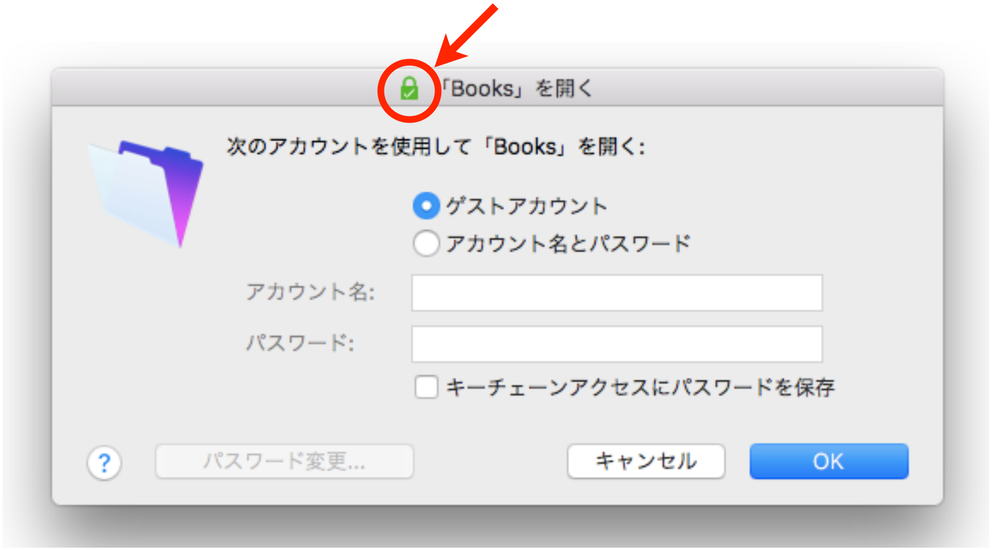
- FileMaker Go/ProからFileMaker Serverに接続する際にはSSLサーバー証明書のコモンネーム（サーバー名）を使用

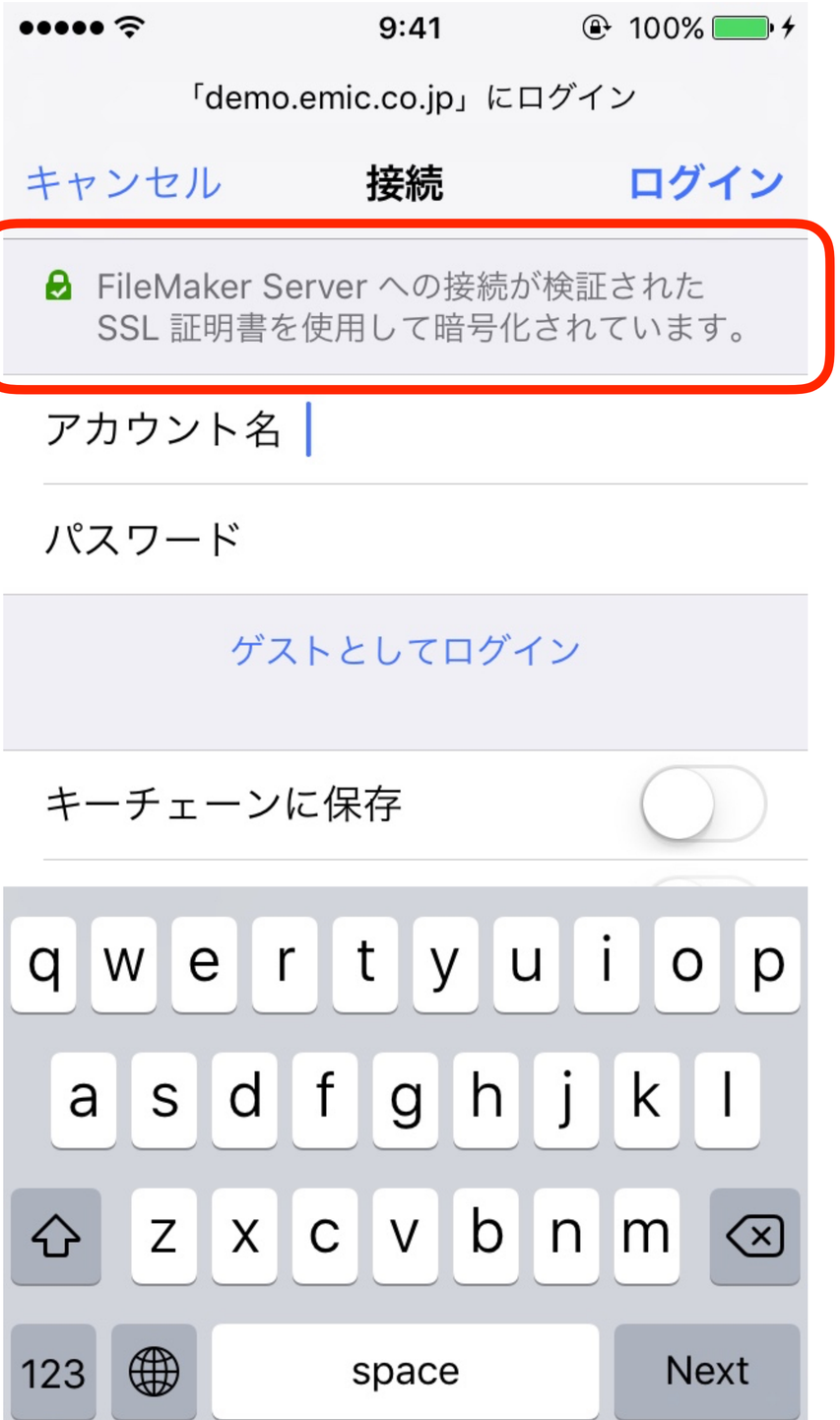

FileMaker Server にアップロード
ホスト:
お気に入りのホスト
(demo.emic.co.jp)
FileMaker Server
Admin Console の名前とパスワードを入力してください。
名前:
パスワード:
キーチェーンアクセスにパスワードを保存
ホストアドレス:
demo.emic.co.jp
キャンセル
< 戻る
次へ >


100
ブラウズ


9:41
100%
Books (demo.emic.co.jp)
書籍詳細
INTER-Mediator Training Course
INTER-Mediator
Training Course
I-M
NTER EDIATOR
Nobuo Hayashi, Editor
Masayuki Nii, Author
カテゴリ
FileMaker
Windows
iOS
その他
Mac OS X
Excel


「Books」を開く
次のアカウントを使用して「Books」を開く:
ゲストアカウント(G)
アカウント名とパスワード(A)
アカウント名(N):
パスワード(P):
資格情報マネージャーにパスワードを保存(S)
パスワード変更(C)...
OK
キャンセル


「Books」を開く
次のアカウントを使用して「Books」を開く:
ゲストアカウント
アカウント名とパスワード
アカウント名:
パスワード:
キーチェーンアクセスにパスワードを保存
パスワード変更...
キャンセル
OK


9:41
100%
「demo.emic.co.jp」にログイン
キャンセル
接続
ログイン
FileMaker Server への接続が検証された
SSL 証明書を使用して暗号化されています。
アカウント名
パスワード
ゲストとしてログイン
キーチェーンに保存
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
Next

Windows	macOS	暗号化通信の状態
		接続が暗号化されていません
		実際の接続先を装ったサーバーに接続している可能性があり、お客様の認証情報が危険に曝される可能性があります
		接続はカスタム SSL 証明書によって暗号化されています

（FileMaker ナレッジベースより）

サーバー移行時の注意点

- FileMaker Serverフォルダ直下にあるCStoreフォルダ内のファイルを保管・コピーする必要がある
  - プライベートキーファイルを紛失するとーから再発行手続きが必要

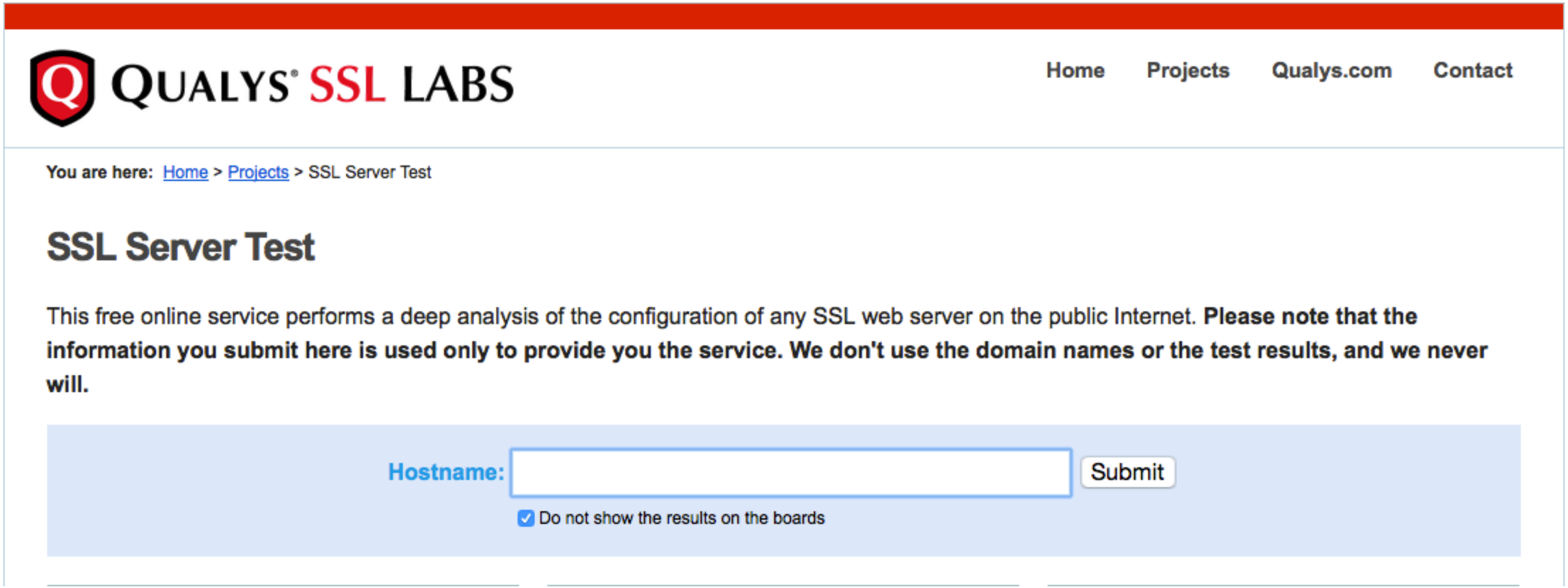
CStoreフォルダ内のファイル

- serverRequest.pem
  - CSR（証明書署名要求）
- **serverKey.pem**
  - プライベートキーファイル
- **serverCustom.pem**
  - 証明書ファイルをインポートして生成されたファイル

Qualys SSL Labs
SSL Server Test

- WebサーバーのSSL設定をさまざまな観点からチェック
  - 古くて弱い暗号を使っていないか
  - 適切にサーバーが設定されているか
  - 脆弱性がないか etc.

Qualys SSL Labs
SSL Server Test



IISでSSL 3.0を無効化

- PowerShell等で次のコマンドを実行してからOSを再起動
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /v Enabled /t REG_DWORD /d 0 /f

3. FileMaker 15
における新機能と改善点

SSL/TLS関連の改善

- サポートされる認証局および証明書の増加
- 証明書署名要求（CSR）をAdmin Consoleで作成可能に
- 中間CA証明書をインポート可能に
- セキュリティ事前警告や［SSL 証明書の検証］オプション

サポートされる認証局および証明書の増加

- 新しくサポートされた認証局
  - DigiCert、InCommon
- Comodo EV SSL
- 詳細はFileMaker ナレッジベース（アンサーID：12130）を参照

FileMaker 15で
新たに対応した証明書

- ワイルドカードSSLサーバー証明書
- サブジェクトの別名
- EV SSL証明書

ワイルドカード SSLサーバー証明書

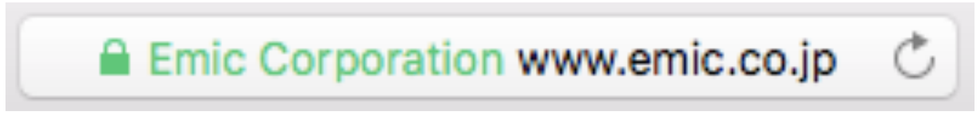
- １枚のSSLサーバー証明書（*.example.jp）で複数のサブドメイン（a.example.jp/b.example.jp…）に対応した証明書

サブジェクトの別名

- 1枚のSSLサーバー証明書で複数の別ドメイン（FQDN）に対応した証明書
  - 例：www.emic.co.jp / emic.net
- Subject Alternative Name（SAN）という拡張領域を利用

EV SSL証明書

- 業界統一基準に則って企業の実在性をより確実に認証する証明書
- Webブラウザーではアドレスバーにサイト運営者の組織名称が表示される
  - サイトの信頼性を分かり易くアピール



サポートされる証明書の販売元および商品名	種類	署名ハッシュアルゴリズム
シマンテック・ウェブサイトセキュリティ シマンテック セキュア・サーバID	実在認証型	SHA-2
コモドジャパン 企業認証タイプ SSL（Elite SSL Certificate）、EVタイプ SSL*	実在認証型	SHA-2
ジオトラスト トゥルービジネスID	実在認証型	SHA-2
DigiCert * ワイルドカード証明書*、マルチドメイン証明書*、EV マルチドメイン証明書*	実在認証型	SHA-2
Thawte SSL123	ドメイン認証型	SHA-2 (under SHA-1 Root)
GoDaddy Standard SSL	ドメイン認証型	SHA-2

*がついているものはFlleMaker 15で対応、上記以外に**InCommon**の証明書も15ではサポート対象

CSRをAdmin Consoleで作成可能に

- CSR：証明書署名要求
  - SSLサーバー証明書を購入する際に認証局（CA）に送付するファイル
  - ファイル名：serverRequest.pem

CSRをAdmin Console で作成可能に

中間CA証明書を
インポート可能に

- 認証局が中間認証局を変更した場合にも適切に更新・対応できるように改善
- SSL/TLS利用時にはFileMaker 15の導入を強く推奨

中間CA証明書をインポート可能に

fmsadminコマンドの新しいオプション

- certificate import --intermediateCA
- certificate delete

まとめ

まとめ

- SSL/TLSは世界で最も利用されている暗号化通信の方法
- 最近では常時SSL化の動きが加速
- FileMaker 15ではSSL/TLS関連の機能が大幅に改善