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

2015/11/27
FileMaker カンファレンス 2015 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 8 / 9 / 10 / 11 / 12 / 13 / 14 Certified Developer
- ✓ FileMaker Server対応Webフレームワーク「INTER-Mediator」
  コミッター
- ✓ カスタムWeb勉強会を隔月で開催

株式会社エミック

- FileMaker製品対応ホスティングサービスを1998年から提供
  - ✓ FileMaker Server 14に対応した「**FMPress14**」
  - ✓ データベースからモバイル対応Webアプリを生成する「**FMPress Publisher**」を搭載
- 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

Webアプリで導入・運用コストを削減、同時接続ライセンスは不要です

FileMaker Proでデータベースを作成

Webアプリを自動生成

今回の話題

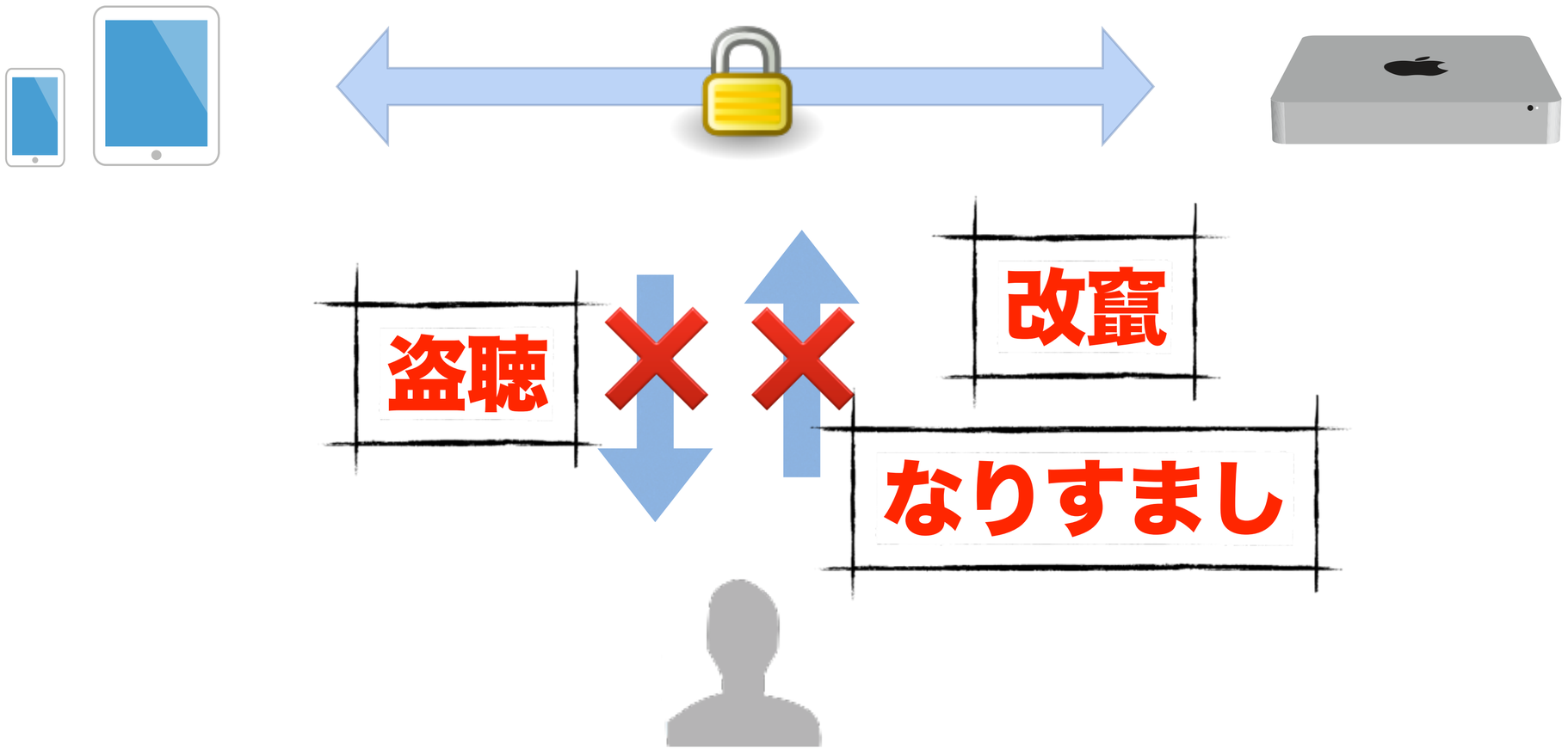
1. SSLとは何か
2. FileMaker製品でSSLを利用するには
3. SSL/TLS関連最新情報

1. SSLとは何か

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

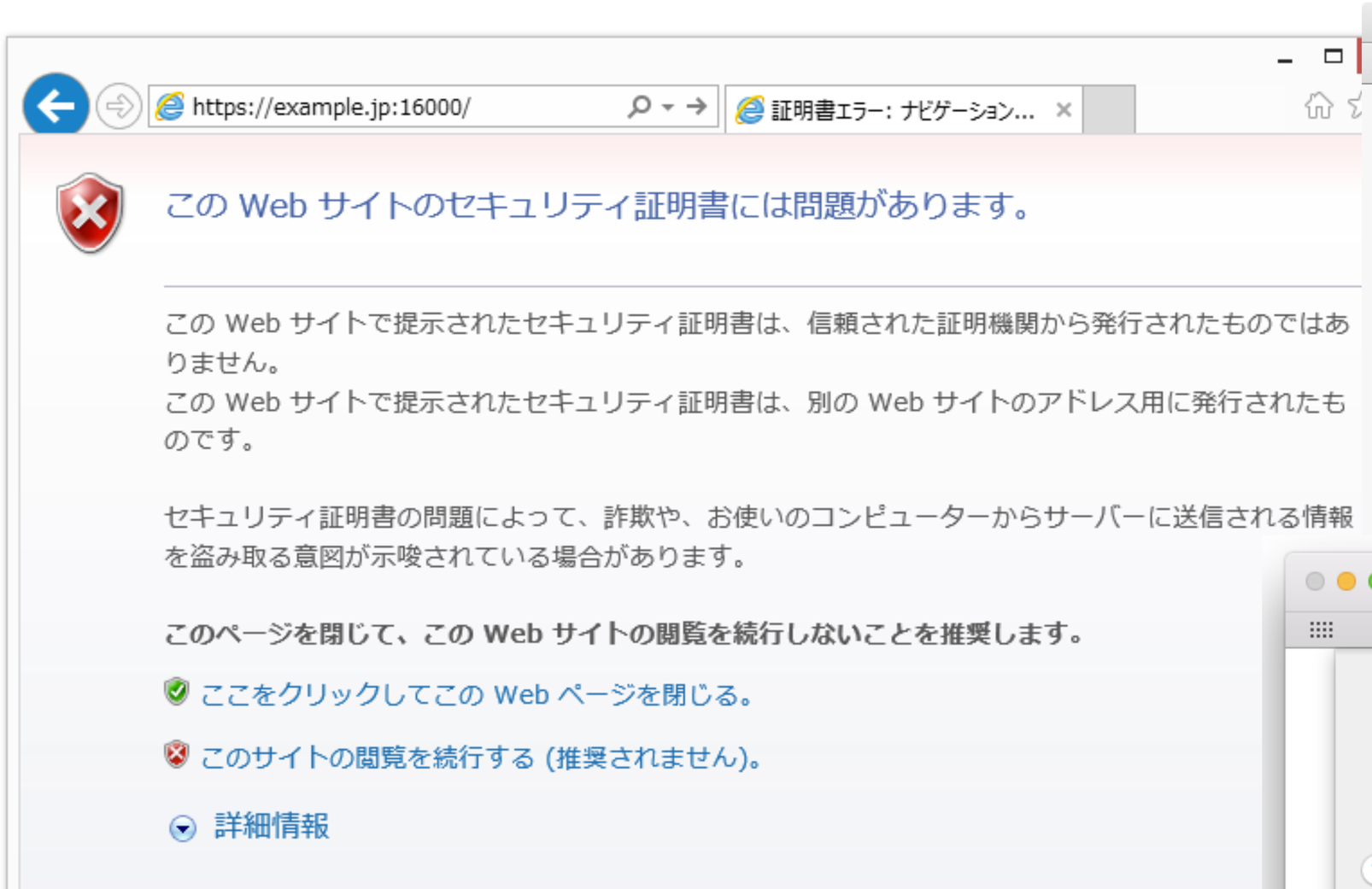
暗号化通信



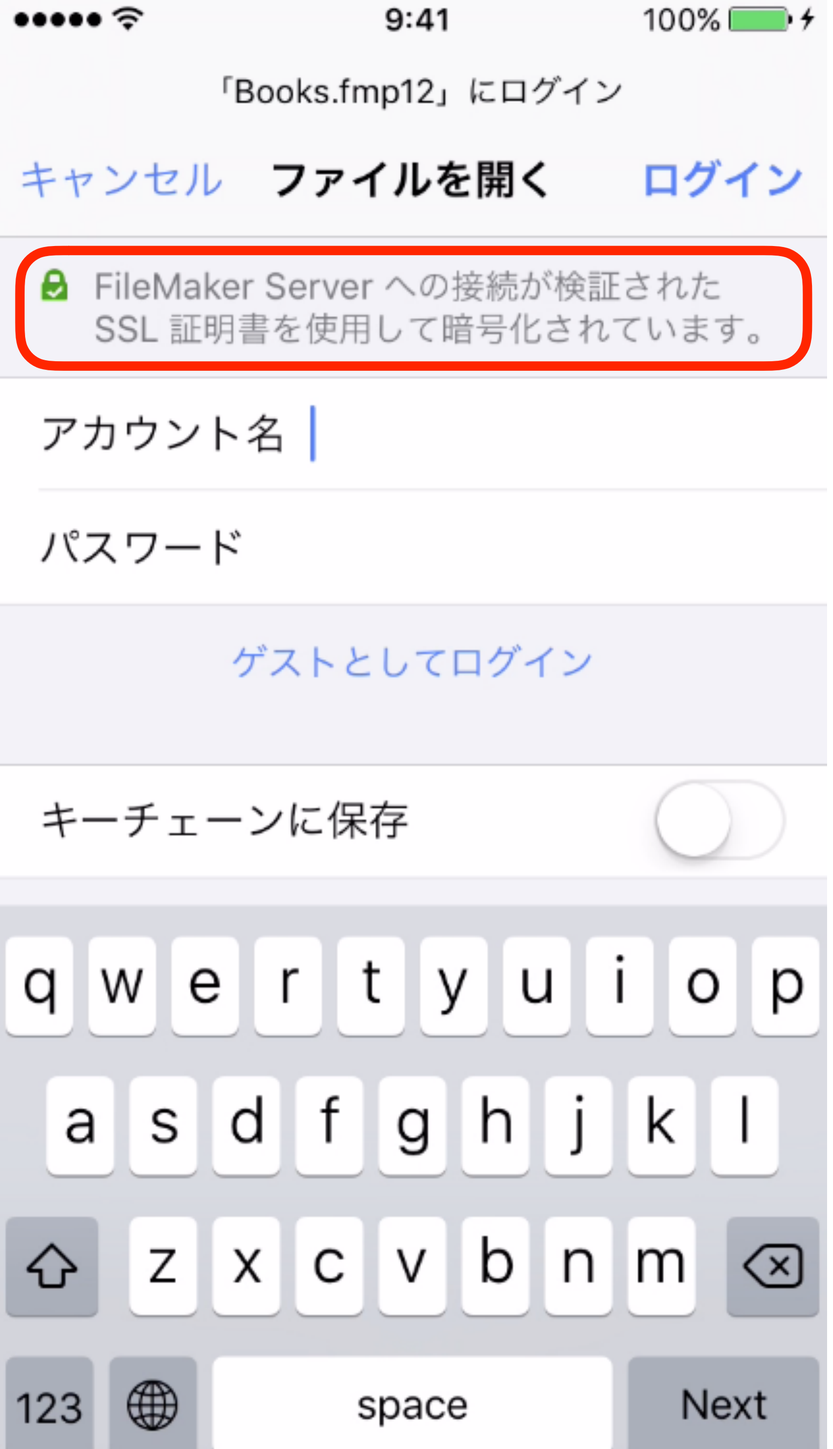
Secure Sockets Layer

- 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

次のようなエラーに遭遇
したことはありませんか？



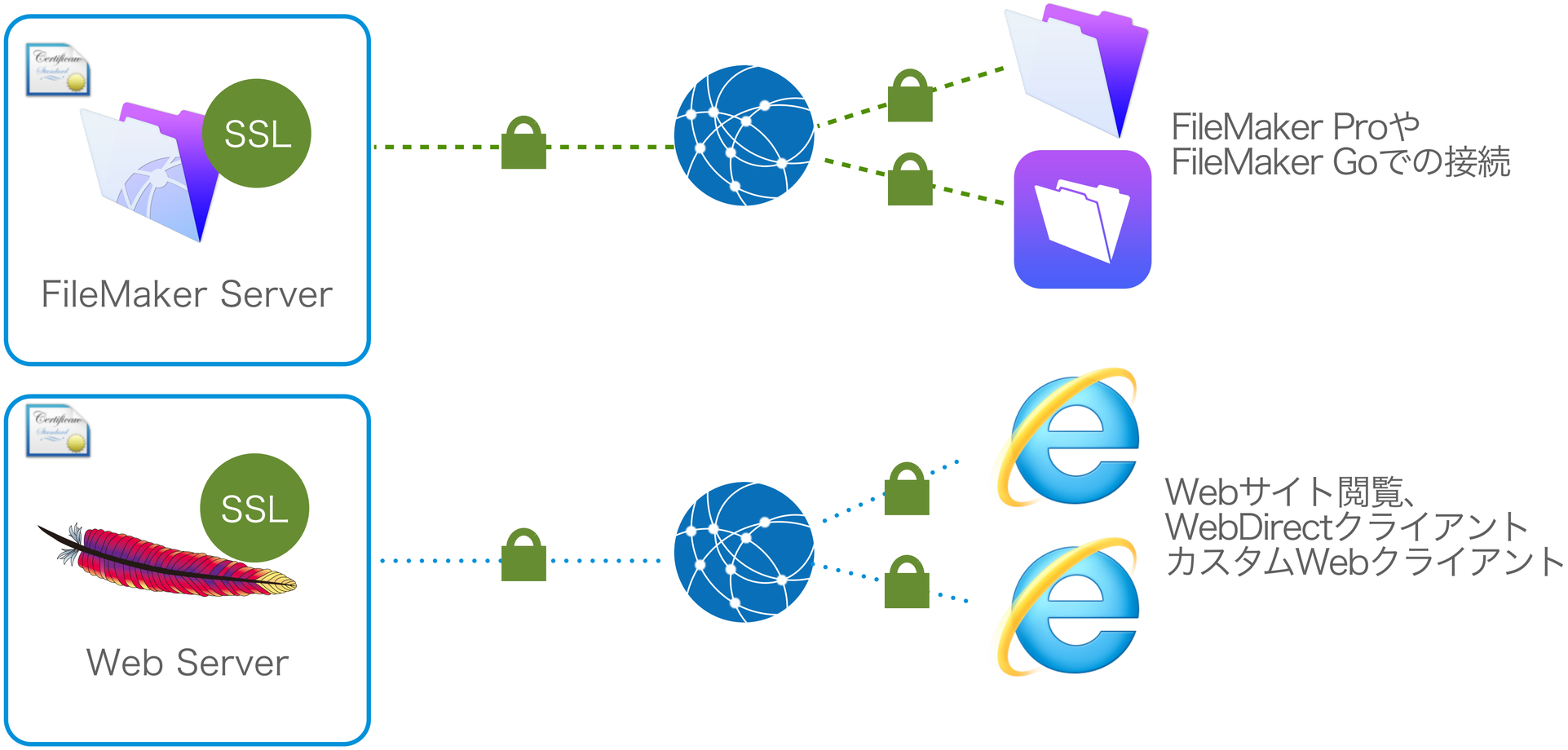

9:41
100%
「Books.fmp12」にログイン
キャンセル
ファイルを開く
ログイン
FileMaker Server の SSL 証明書が検証できません。実際の接続先に偽装したサーバーに接続している可能性があり、機密情報が漏えいするおそれがあります。
アカウント名
パスワード
ゲストとしてログイン
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
Next


9:41
100%
「Books.fmp12」にログイン
キャンセル
ファイルを開く
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

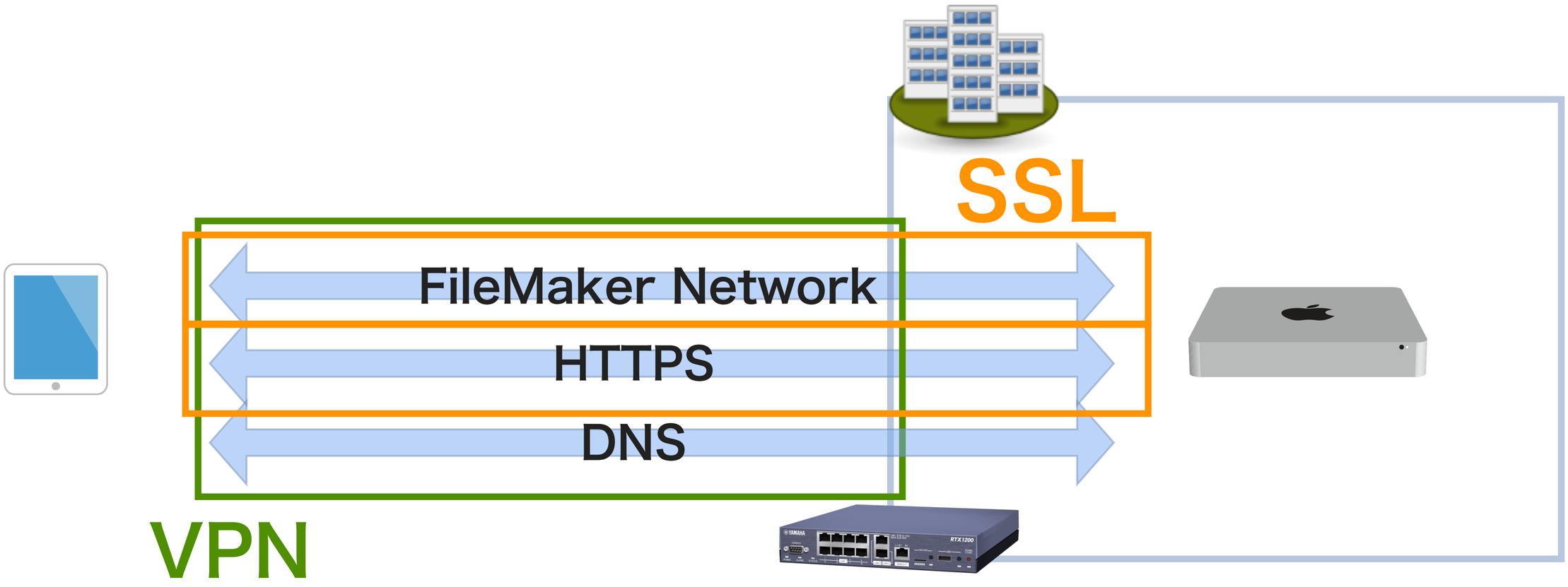
FileMaker Serverは SSL暗号化通信に対応

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

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）
- SSL/TLSは世界で最も利用されている暗号化通信の方法

2. FileMaker製品で
SSLを利用するには

どのバージョンが必要？

（2015年11月現在）

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

（最新版であるバージョン14の利用を推奨）

SSL対応手順概要

1.認証局に提出する**CSR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

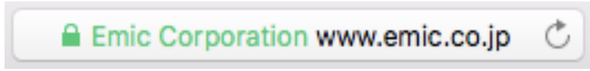
3.Admin Consoleで［データベース接続に SSL を使用する（保護された接続が必要）］設定を有効化

SSL導入にあたって

- SSL暗号化通信を実現するには**認証局から証明書を購入**する必要がある
- FileMaker製品でサポートされているSSLサーバー証明書の販売元と種類は限られている

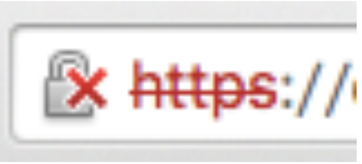
サポートされる証明書の販売元および商品名	種類	署名ハッシュアルゴリズム
シマンテック・ウェブサイトセキュリティ シマンテック セキュア・サーバID	実在認証型	SHA-1 SHA-2
コモドジャパン 企業認証タイプ SSL	実在認証型	SHA-1 SHA-2
ジオトラスト トゥルービジネスID	実在認証型	SHA-2
ジオトラスト クイックSSL プレミアム	ドメイン認証型	SHA-1 SHA-2
Thawte SSL123	ドメイン認証型	SHA-1 SHA-2
GoDaddy Standard SSL	ドメイン認証型	SHA-1 SHA-2

(独自調査の結果)

	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9,000～31,300円 （無料、千～1.5万円）	25,800～81,000円 （約9千～13.8万円）	- （約2.4万～21.9万円）
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**

安全上の理由から SHA-1は非推奨に

- 署名ハッシュアルゴリズムがSHA-1であるSSLサーバー証明書が発行されるのは今年12月まで
- SHA-1証明書のサポート廃止が2016年6月に前倒しされる可能性あり
- **今後はSHA-2**（SHA-256）版を選択



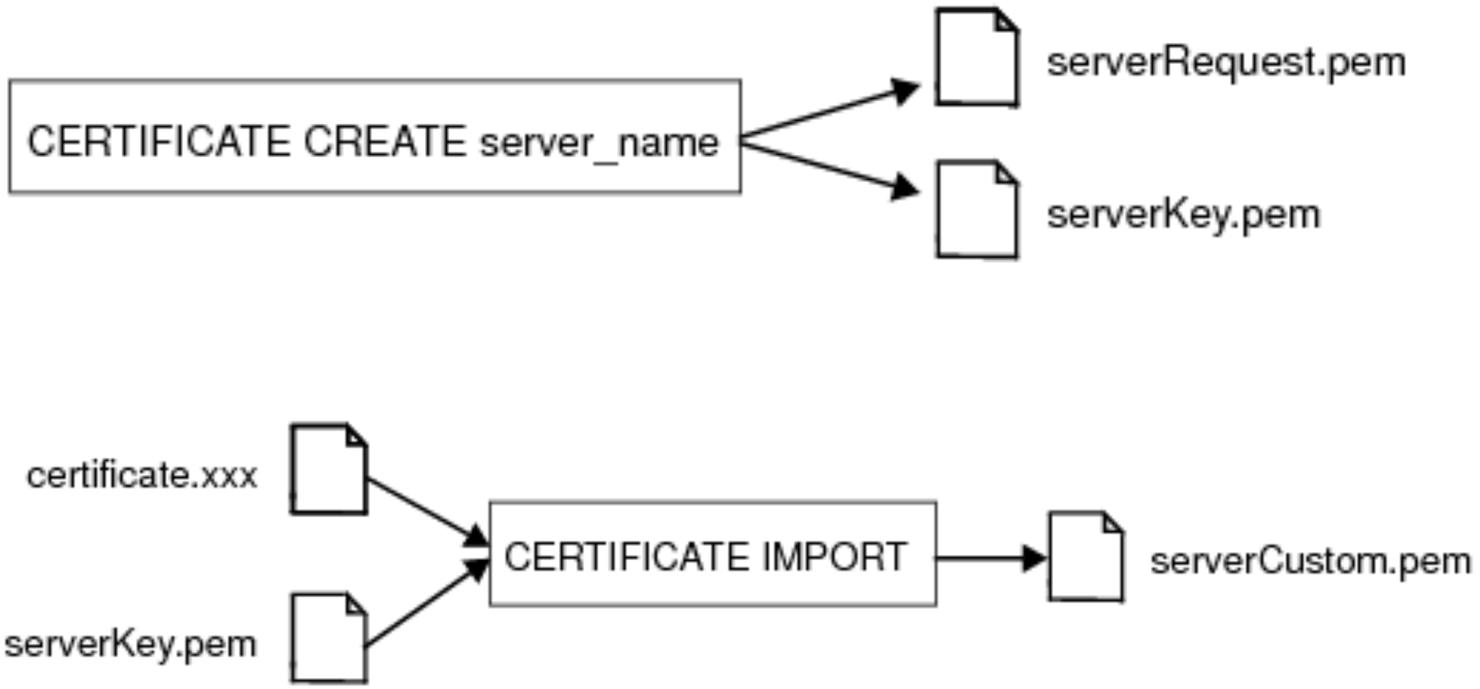
証明書購入時の注意点

- FileMaker 12はSHA-2版SSLサーバー証明書に非対応
- **ワイルドカードSSLサーバー証明書**に対応しているのはFileMaker Pro 14.0.3 (Advanced)以降のみ（独自調査の結果）
- **EV SSL証明書**には未対応

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
    - CStoreフォルダ内のserverRequest.pem
  - FileMaker Server 14であれば認証局で案内されている手順を参照して生成するのがオススメ
  - 所有しているドメイン名が必要

fmsadminコマンド



（FileMaker Server 13 ヘルプより）

CStoreフォルダ内のファイル

- serverKey.pem
  - プライベートキーファイル（パスフレーズを削除したもの）
- serverCustom.pem
  - fmsadmin certificate importで発行されたSSLサーバー証明書ファイルをインポートして生成されたファイル

証明書のインポート

- FileMaker Server 14ではAdmin Console上でインポートが可能
- FileMaker Server 13の場合にはfmsadminコマンド（fmsadmin certificate import）を利用

FileMaker Server 14

SSL暗号化通信の有効化

- 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

Windows環境での注意点

- クライアント環境がWindowsで
  FileMaker ProもしくはFileMaker Pro
  Advancedを使用する場合

➡Windowsアカウントのユーザー名に
漢字やひらがな等のマルチバイト文字
を含めないようにする

3. SSL/TLS関連
最新情報

FileMaker Server 13.0v1a / 13.0v2

- OpenSSLの**Heartbleed**脆弱性を修正
- FileMaker Pro (Advanced)はバージョン13.0v3で、FileMaker Goはバージョン13.0.4で上記脆弱性を修正

FileMaker Server 13.0v5

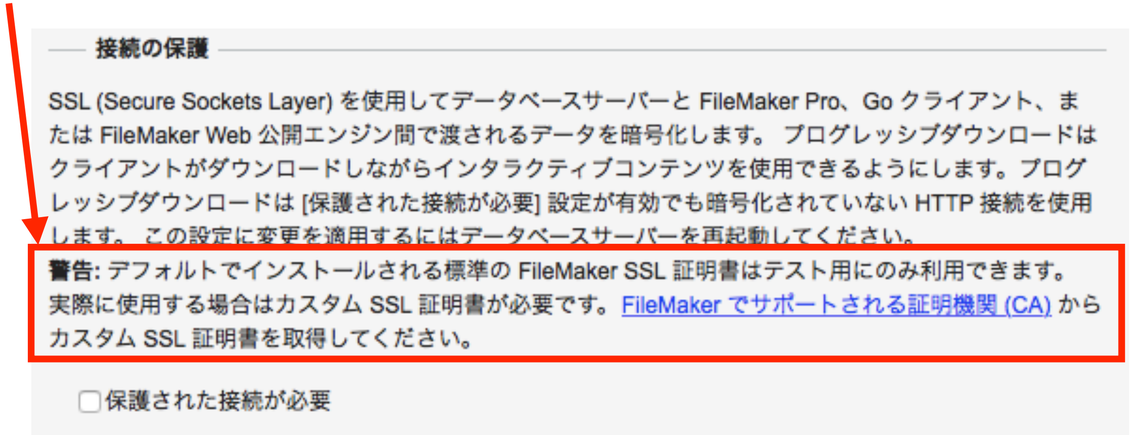
- SSL/TLSの脆弱性を突いた**FREAK**攻撃に対応
- SSL 3.0の脆弱性を突く**POODLE**攻撃への対策のためにSSL 3.0を無効化（OS X版FileMaker ServerのWebサーバーにおいて）

FileMaker 13.0v9

- SSL関連のセキュリティアップデート
  - FileMaker Server 13.0v9
  - FileMaker Pro 13.0v9
  - FileMaker Pro 13.0v9 Advanced
  - FileMaker Go 13.0.9

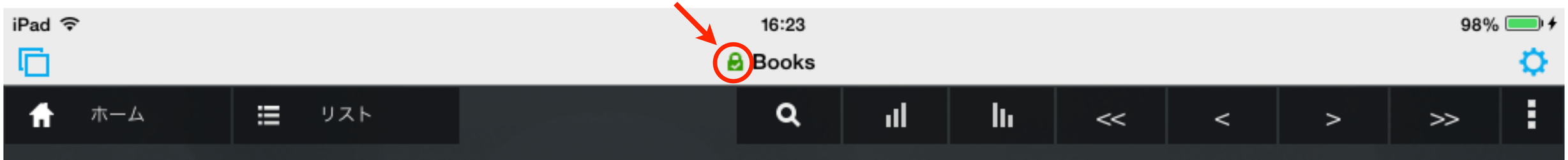
Admin Consoleにおいて証明書に関する説明に変化

- “デフォルトでインストールされる標準の FileMaker SSL 証明書はテスト用にのみ利用できます。実際に使用する場合はカスタム SSL 証明書が必要です。”



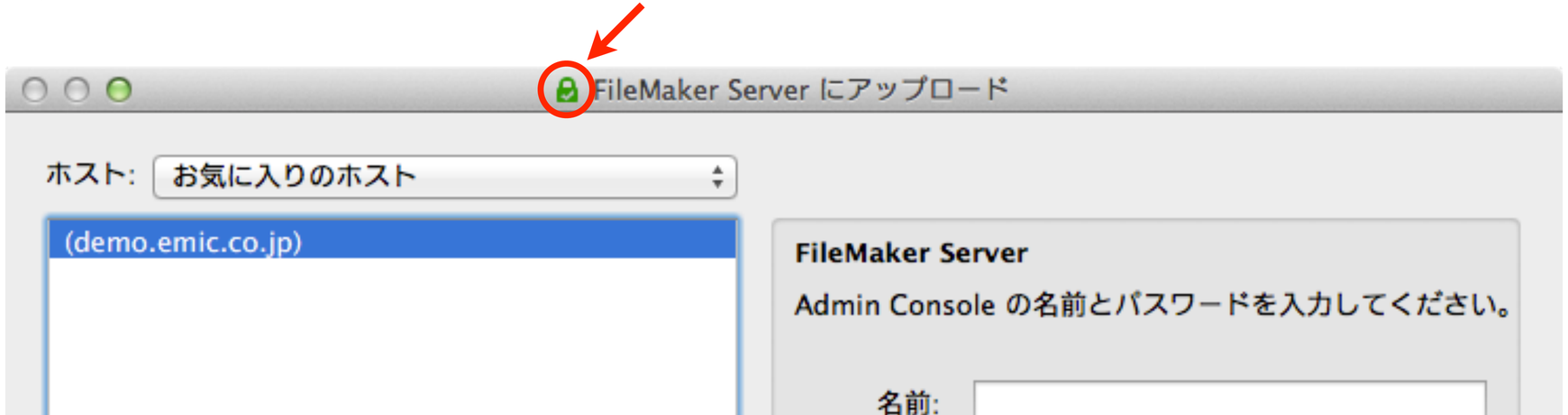
FileMaker Pro 13
FileMaker Go 13

- ウインドウにロックアイコンが表示されるように



FileMaker Pro 13.0v4

- ［FileMaker Serverにアップロード］ダイアログボックスにロックアイコンが表示されるように



Windows	OS X	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

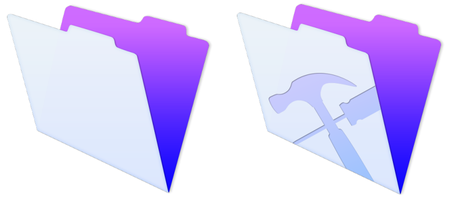
（FileMaker ナレッジベースより）

FileMaker 14

- アカウント名とパスワードを入力するダイアログボックスにおいてロックアイコンが表示されるように

FileMaker Pro 14.0.3

- ネットワーク共有で**ワイルドカードSSLサーバー証明書**に対応（独自調査の結果）
  - 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



SSL/TLS関連最新情報

- SNI（Server Name Indication）
- 常時SSL（Always on SSL）
- HTTP/2

SNI
(Server Name Indication)

- 1台のサーバー上で複数のSSL対応Webサイトを運用可能
  - 従来はIPアドレス1つにつき1つ

常時SSL
(Always on SSL)

- Web上のすべての通信をHTTPS化
  - GoogleがSEOでHTTPSを優遇
- HTTP Strict Transport Security (HSTS)

HTTP/2

- HTTP/1.1が今年16年ぶりに改訂
  （RFC 7540）
- Webを高速化するHTTP/2は現時点で
  は実質的にTLSが必須

まとめ

まとめ

- SSL/TLSはさまざまなプロトコル上で使用できる（HTTPに限らない）
- SSL/TLSを実際に使用する場合は**認証局から証明書を購入**する必要がある
- 安全上の理由からSHA-1版SSLサーバー証明書の使用は非推奨に（**今後はSHA-2**に要移行）