FileMaker Serverで Let's Encrypt

2016/08/21

FM-Tokyo発表資料

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
  - ✓ カスタムWeb勉強会を隔月で開催

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

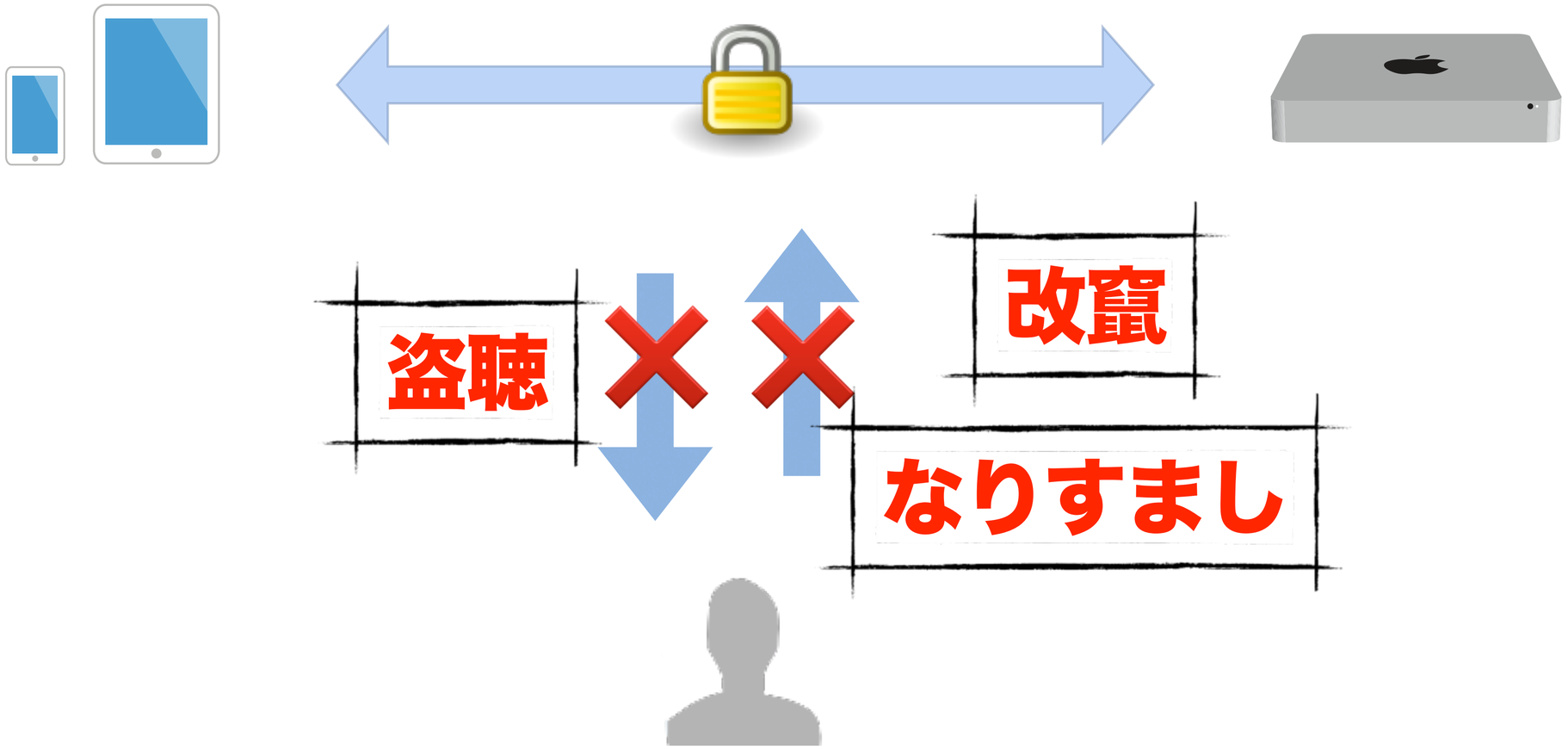
1. SSLとは何か
2. FileMaker製品でSSLを利用するには
3. Let's EncryptとFileMaker Server

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

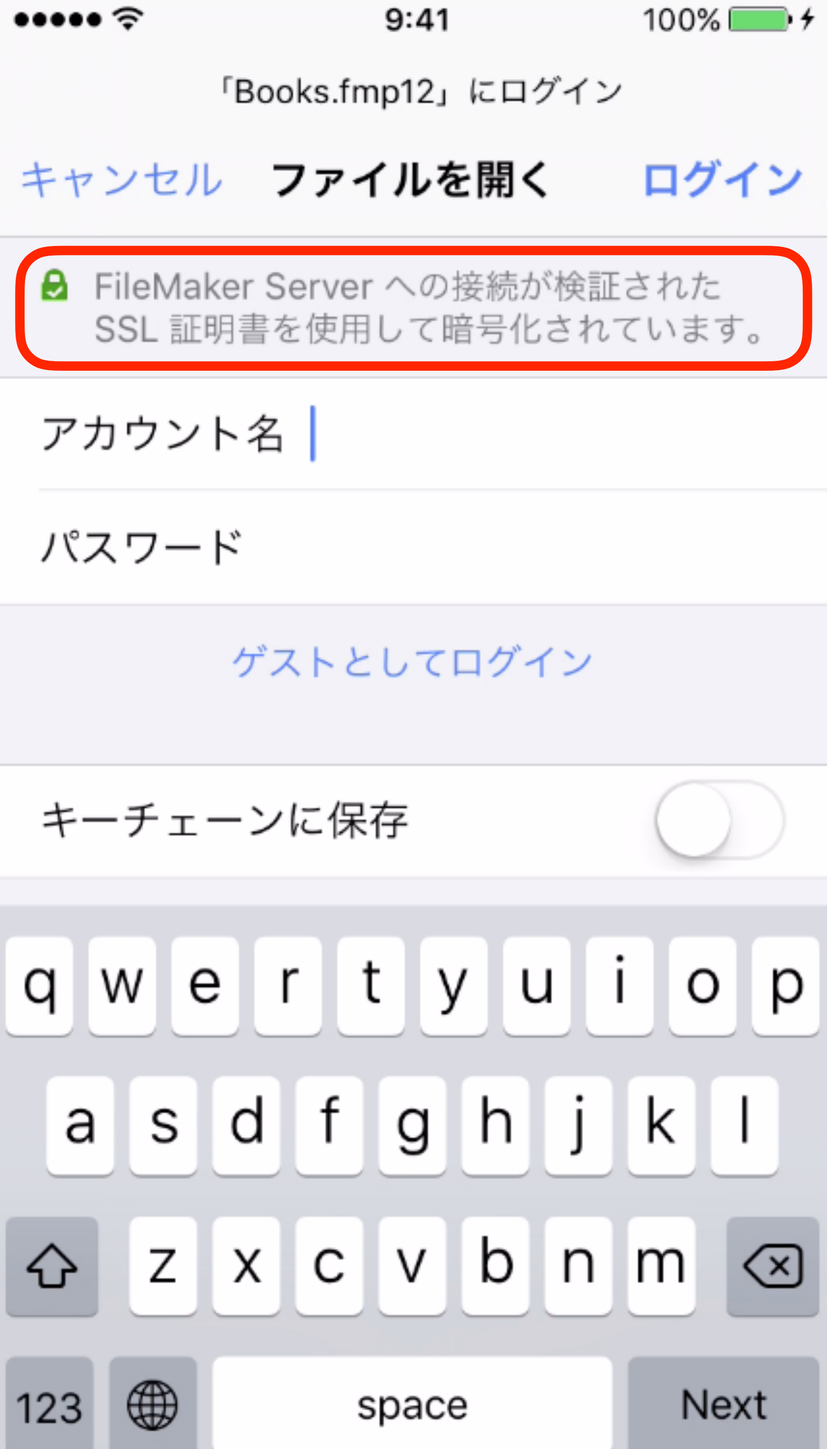


Secure Sockets Layer

- 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？

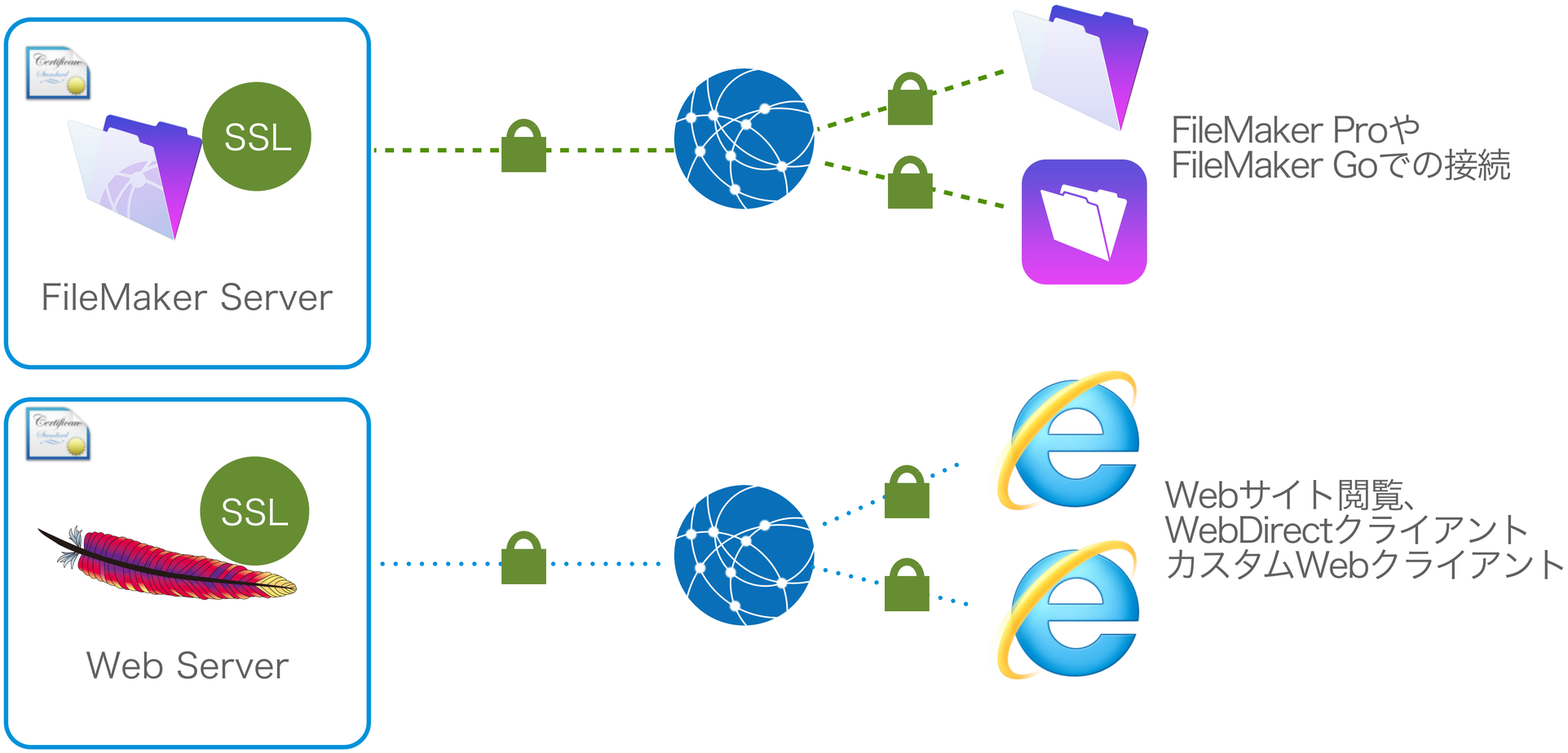

9:41
100%
「Books.fmp12」にログイン
キャンセル
ファイルを開く
ログイン
FileMaker Server の SSL 証明書が検証できません。実際の接続先に偽装したサーバーに接続している可能性があり、機密情報が漏えいするおそれがあります。
アカウント名
パスワード
ゲストとしてログイン
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
Next


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

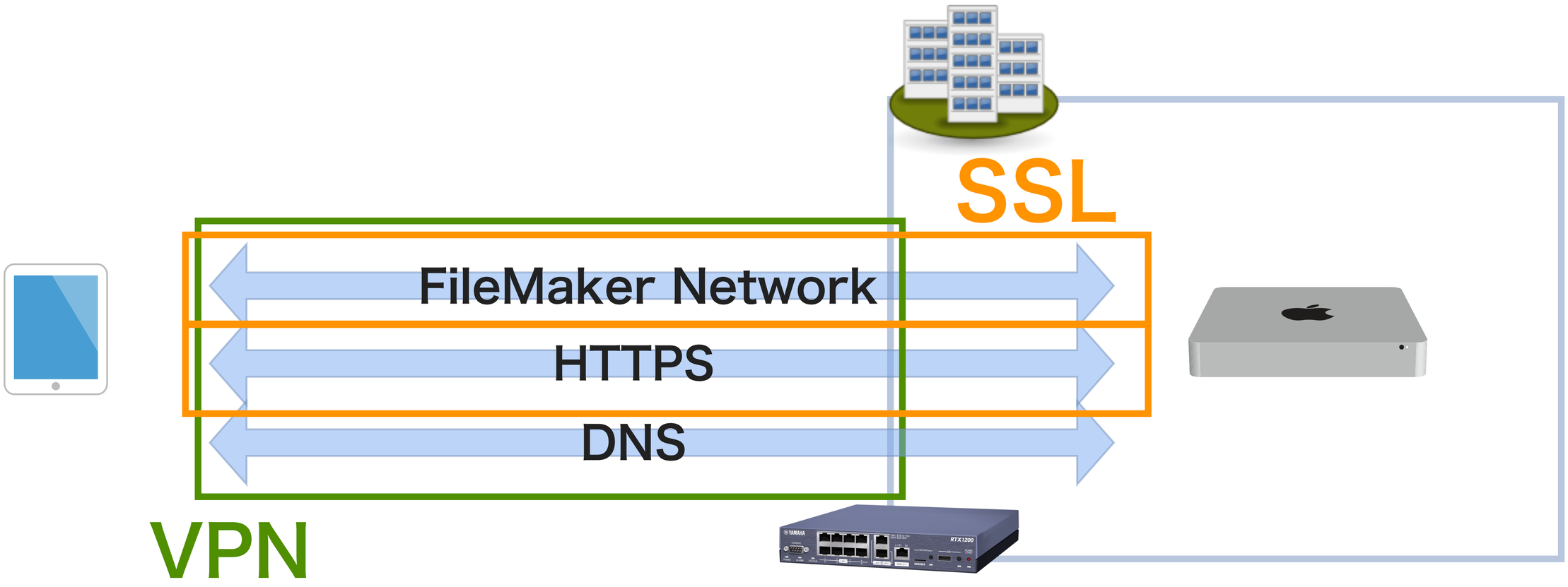
FileMaker Serverは SSL暗号化通信に対応

- 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）
  - 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

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8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

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**

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

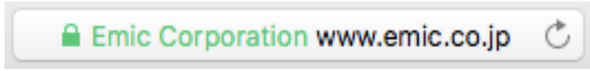
3.Admin Consoleで［データベース接続に SSL を使用する（保護された接続が必要）］設定を有効化

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

安全上の理由から SHA-1は廃止

- 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たのは2015年12月まで
- SHA-1のサポートは2016年末まで
- **今後はSHA-2**（SHA-256）版を選択

	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**

証明書購入時の注意点

- **ワイルドカードSSLサーバー証明書**は
  FileMaker 15で正式に対応
  - 対応クライアントはFileMaker Pro
    14.0.3 (Advanced)以降および
    FileMaker Go 15.0.1以降
- **EV SSL証明書**を購入する際には
  FileMaker 15 プラットフォームが必要

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

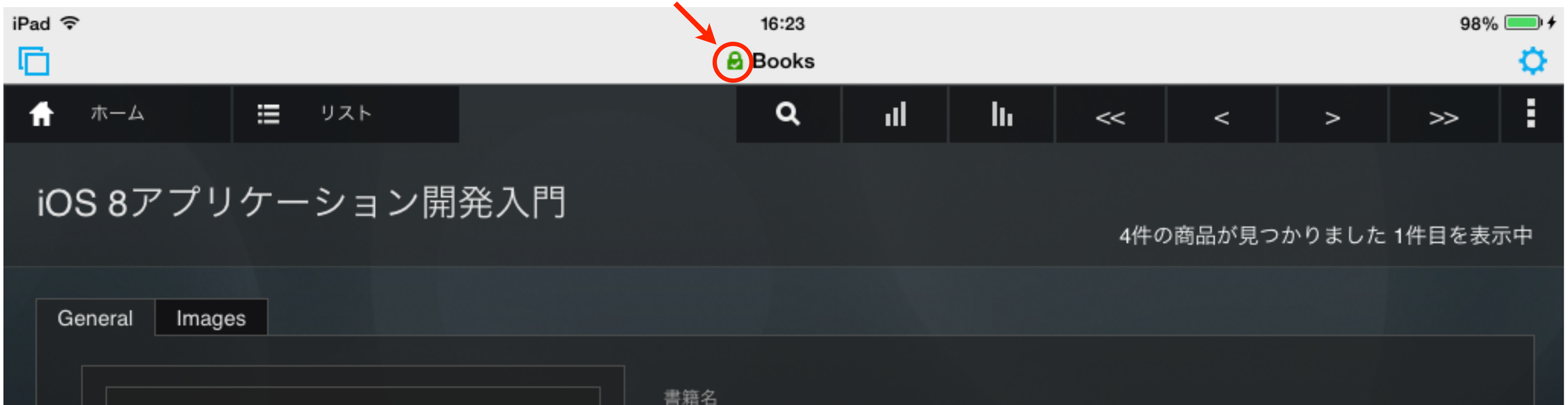
SSL暗号化通信の有効化

- 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

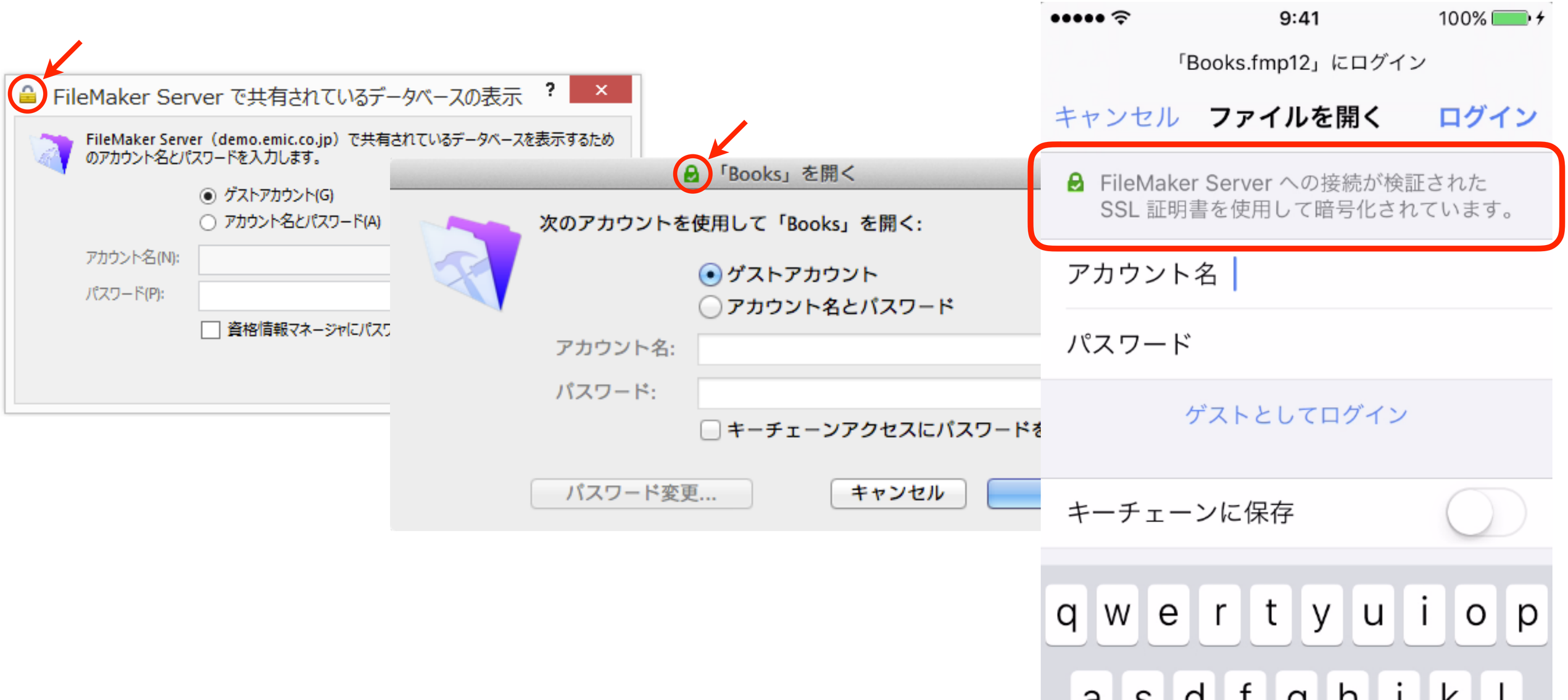
FileMaker Go/Pro からの接続

- 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


100
ブラウズ


iPad
16:23
98%
Books
ホーム
リスト
<<
<
>
>>
iOS 8アプリケーション開発入門
4件の商品が見つかりました 1件目を表示中
General
Images
書籍名


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)
ホストアドレス:
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:
キャンセル
< 戻る
次へ >


FileMaker Server で共有されているデータベースの表示
FileMaker Server（demo.emic.co.jp）で共有されているデータベースを表示するための
のアカウント名とパスワードを入力します。
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):
「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
パスワード変更...
キャンセル
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

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）

3. Let's Encryptと FileMaker Server

Let's Encrypt

- 認証局（CA：Certificate Authority）
  - free
  - automated
  - open
- 利用者は無料でドメイン認証型の証明書を取得できる

Let's Encrypt

- 公共の利益を目的としてInternet Security Research Group（ISRG）が運営
- https://letsencrypt.org/

基本方針

- Free
- Automatic
- Secure
- Transparent
- Open
- Cooperative

仕組み

- ACME（Automated Certificate Management Environment）プロトコル
  - 対象ドメイン名を管理下に置いていることが証明された場合に自動的に証明書を発行
  - 証明書管理エージェントをWebサーバー上で実行する必要がある
- https://letsencrypt.org/how-it-works/

証明書管理エージェント

- 推奨クライアントは**Certbot**
  - 証明書の取得を自動化できるツール
  - CertbotがサポートしているOSは
    LinuxやBSD系列のOS
- Certbot以外のツールも多数存在

FileMaker Serverで Let's Encrypt

- FileMaker Serverに次のファイルをインポート（バージョン15が必要）
  - 証明書管理エージェントを使って発行されたSSLサーバー証明書
  - プライベートキー
  - Let's Encryptの中間CA証明書

Demo

注意点

- Let's Encryptから発行された証明書は
  3ヶ月で失効
  - 定期的に証明書を更新する必要がある
    →自動化が必要

まとめ

まとめ

- Let's Encryptを使うと**無料**でドメイン認証型のSSLサーバー証明書を取得できる
- **FileMaker 15**であればLet's Encryptから発行された証明書を利用可能
- Let's Encryptの証明書は**3ヶ月で失効**するので注意が必要