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
（2020年版）

2020/02/15

FileMaker Pro 東京ユーザーズミーティング 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 18 認定デベロッパ
  - ✓ kintone認定 アプリデザインスペシャリスト（2020年2月）
  - ✓ https://www.famlog.jp/
  - ✓ https://note.com/matsuo_atsushi

FileMaker 18 CERTIFIED DEVELOPER

kintone CERTIFIED App Design SP 2020

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

➡FMプランライト（月額19,800円）が新登場

- kintone導入支援・カスタマイズ開発
- **https://www.emic.co.jp/**

Claris Partner

今回の話題

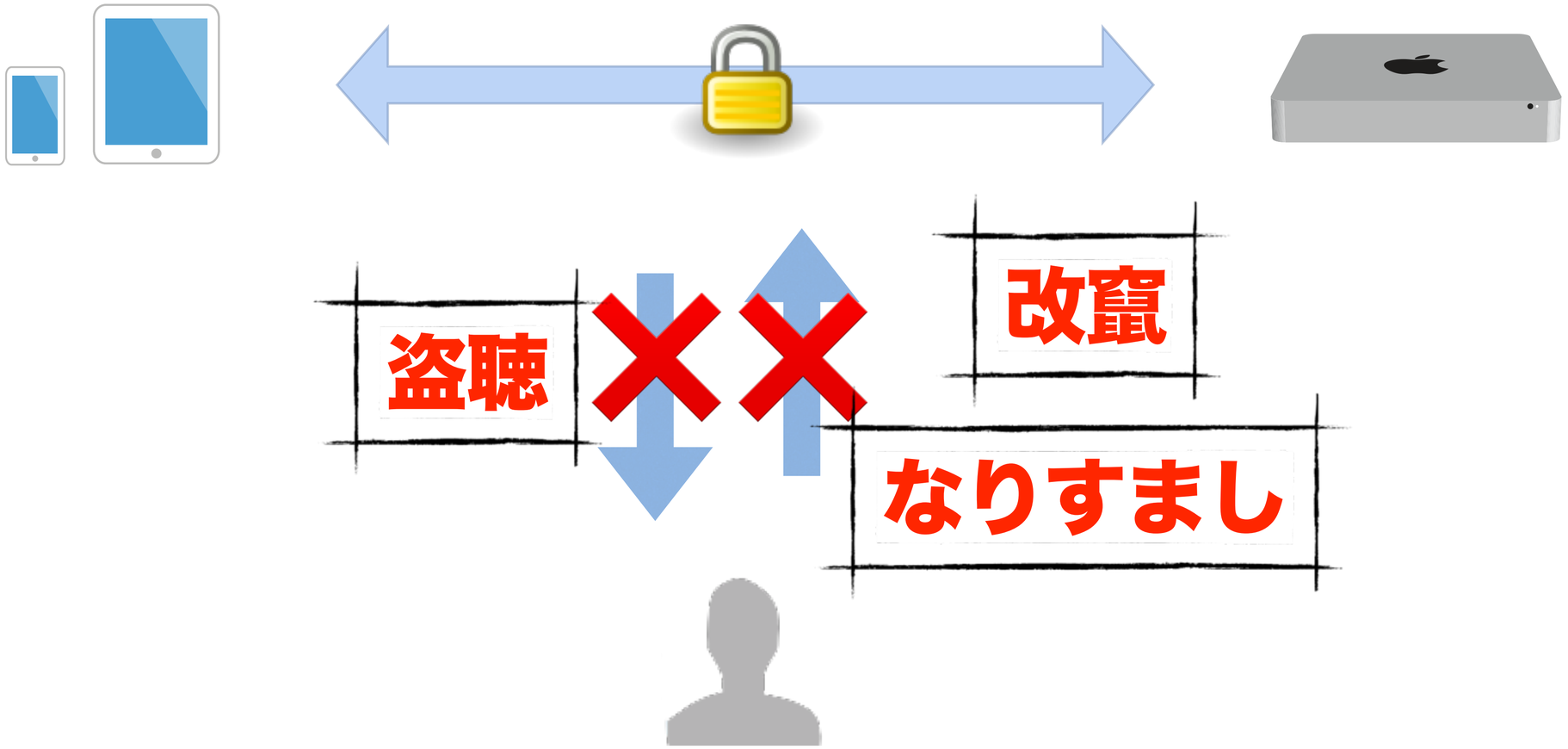
1. SSLの概要と最近の状況
2. FileMaker製品でSSLを利用するには
3. LANでSSLを利用するには

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

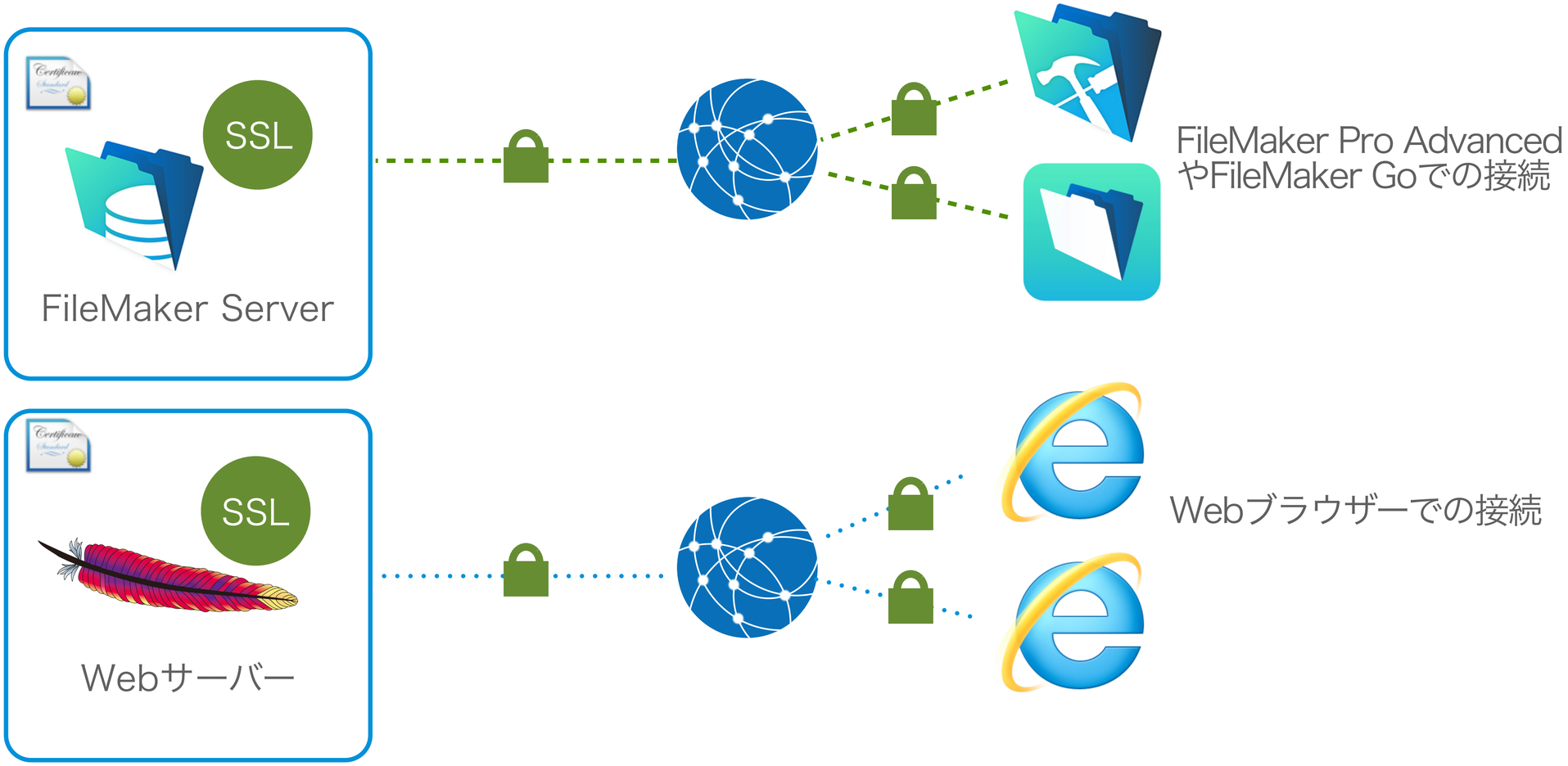
FileMaker製品は
SSL暗号化通信に対応

- FileMaker Pro Advanced/Goと
  FileMaker Server/Cloud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）

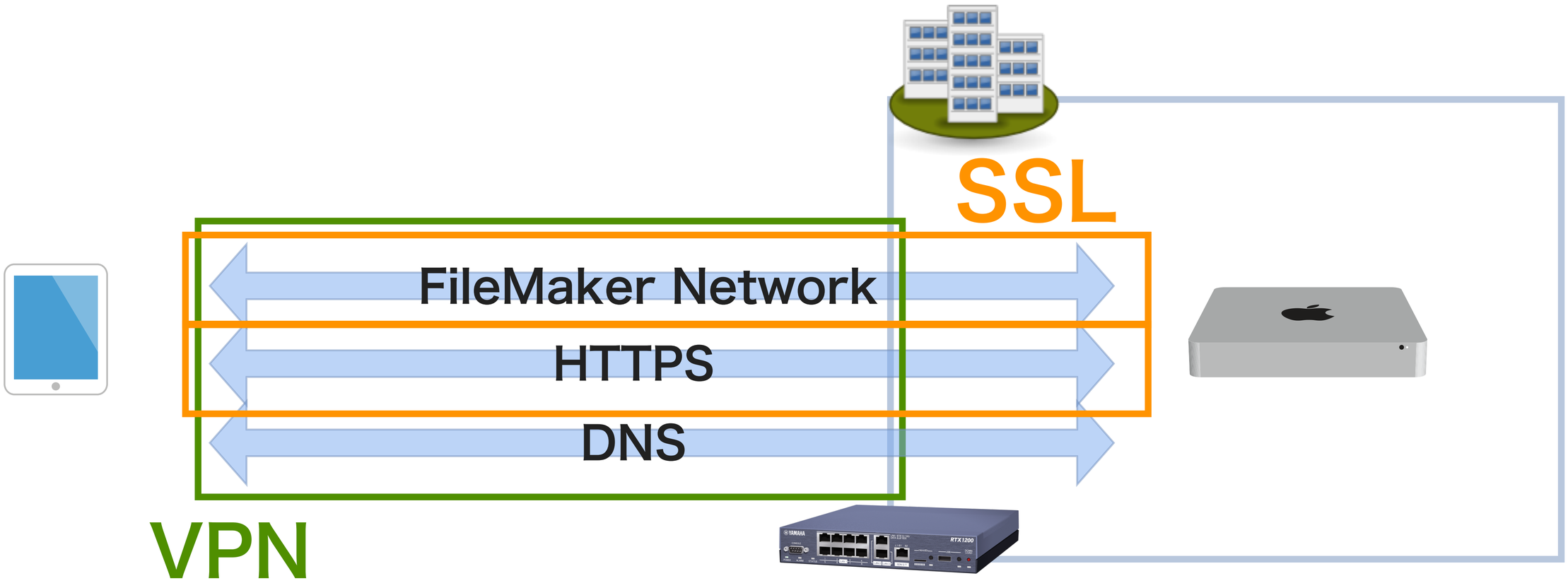
SSLの利用例

- TCP 5003番ポートを使用したネットワーク共有（サーバー製品利用時）
- Admin Console
- インタラクティブコンテンツのプログレッシブダウンロード
- ホストにアップロード etc.

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 1.3**（TLS：Transport Layer Security）
  - FileMaker製品はTLS 1.2をサポート
  - TLS 1.0やTLS 1.1の利用は非推奨に

SSL/TLS関連最新情報

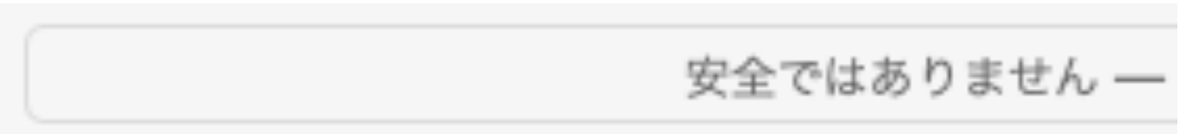
- 常時SSLが一般化・必須化
- 各ブラウザーでSSL未対応時に警告表示
- 各ブラウザーでアドレスバーにおけるEV SSL証明書の組織名表示が廃止
- 無料のSSLサーバー証明書として知られているLet's Encryptが普及

常時SSLが一般化・必須化

- 常時SSL
  - Webサイトのすべてのページを SSL暗号化通信対応にすること
- Google Chromeは今後混合コンテンツ（SSL対応ページ内のSSL未対応のコンテンツ）を段階的にブロック

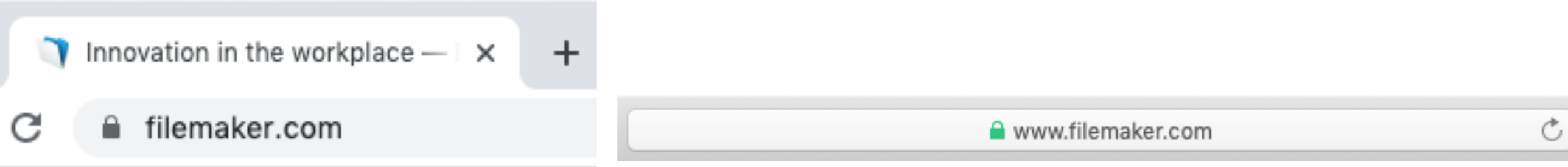
SSL未対応時に警告表示

- アドレスが「http://」で始まるSSL未対応のWebサイトでは警告が表示されるように



EV SSLで組織名の非表示

- EV SSL証明書を使用しているWebサイトで組織名が表示されないように



Let's Encryptが普及

- 公共の利益を目的としてInternet Security Research Group（ISRG）が運営
- 無料のSSLサーバー証明書
- 証明書の自動更新に対応

2. FileMaker製品で
SSLを利用するには

どのバージョンが必要？

（2020年2月現在）

- サポート対象製品であるバージョン
  - FileMaker Pro 16以降（FileMaker Pro Advancedも同様）
  - FileMaker Go 16以降
  - FileMaker Server 16以降
  - FileMaker Cloud for AWS 1.16以降

どのバージョンが必要？

（2020年2月現在）

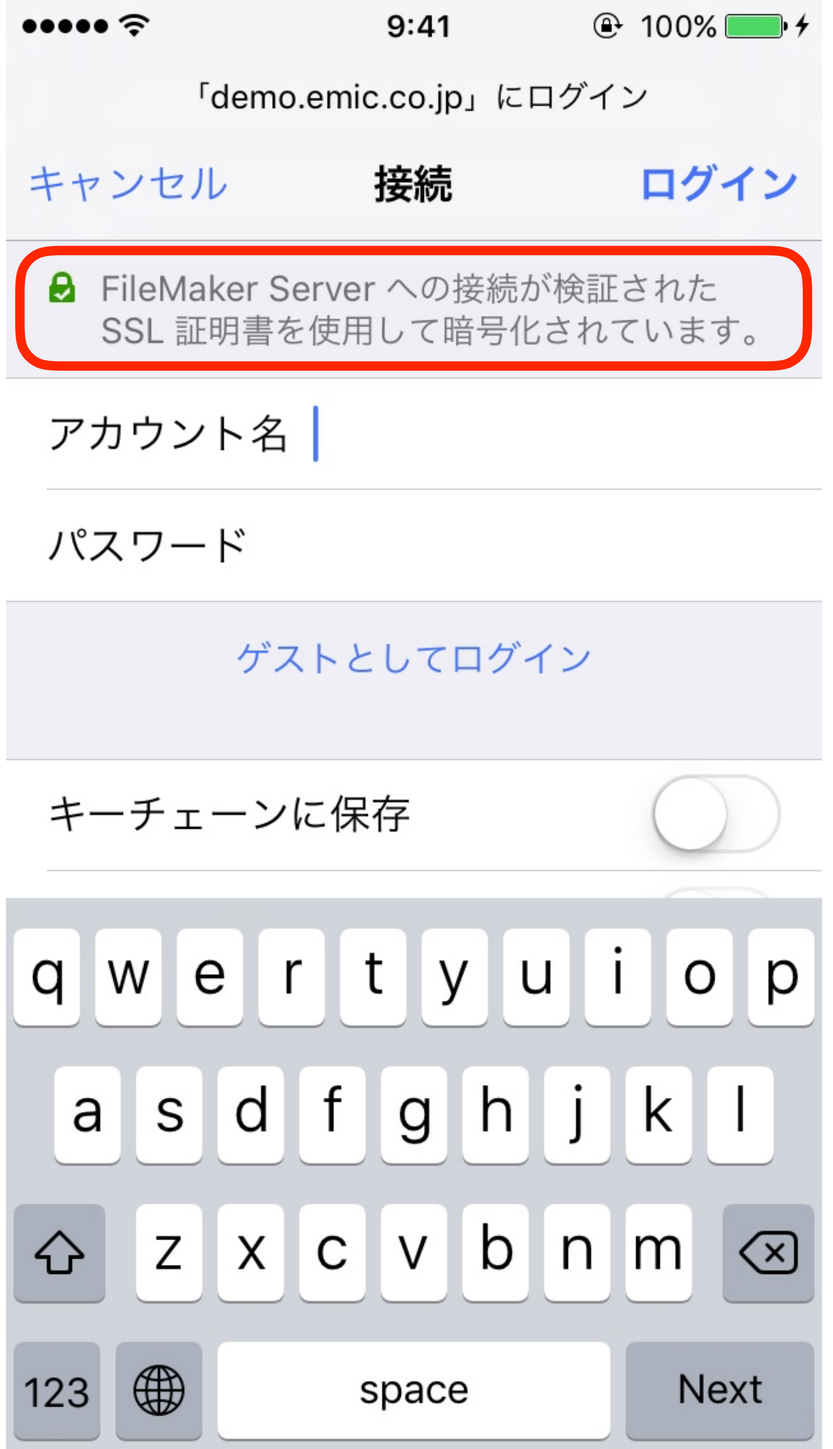
- バージョン14以前は中間認証局の変更に対応できない仕様になっている
- バージョン15のメーカーサポートはすでに終了している
- 2020年2月時点ではバージョン16以降の利用を強く推奨

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
デジサート（旧シマンテック） 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
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

	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6,400円〜 （0円〜）	25,800円〜 （約9,000円〜）	71,500円〜 （約22,000円〜）
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**~~ 組織名は表示されない
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

- 認証局に提出する**CSRファイル**（と非公開のプライベートファイル）を生成
- Admin Consoleで認証局から発行された**SSLサーバー証明書**と**中間CA証明書**をインポート
- サーバーを再起動

CSRファイルの生成

- 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
- 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でもOK

証明書のインポート

- **Admin Console**上でインポートが可能
- **fmsadminコマンド**（fmsadmin certificate import）でもインポートが可能

証明書のインポート

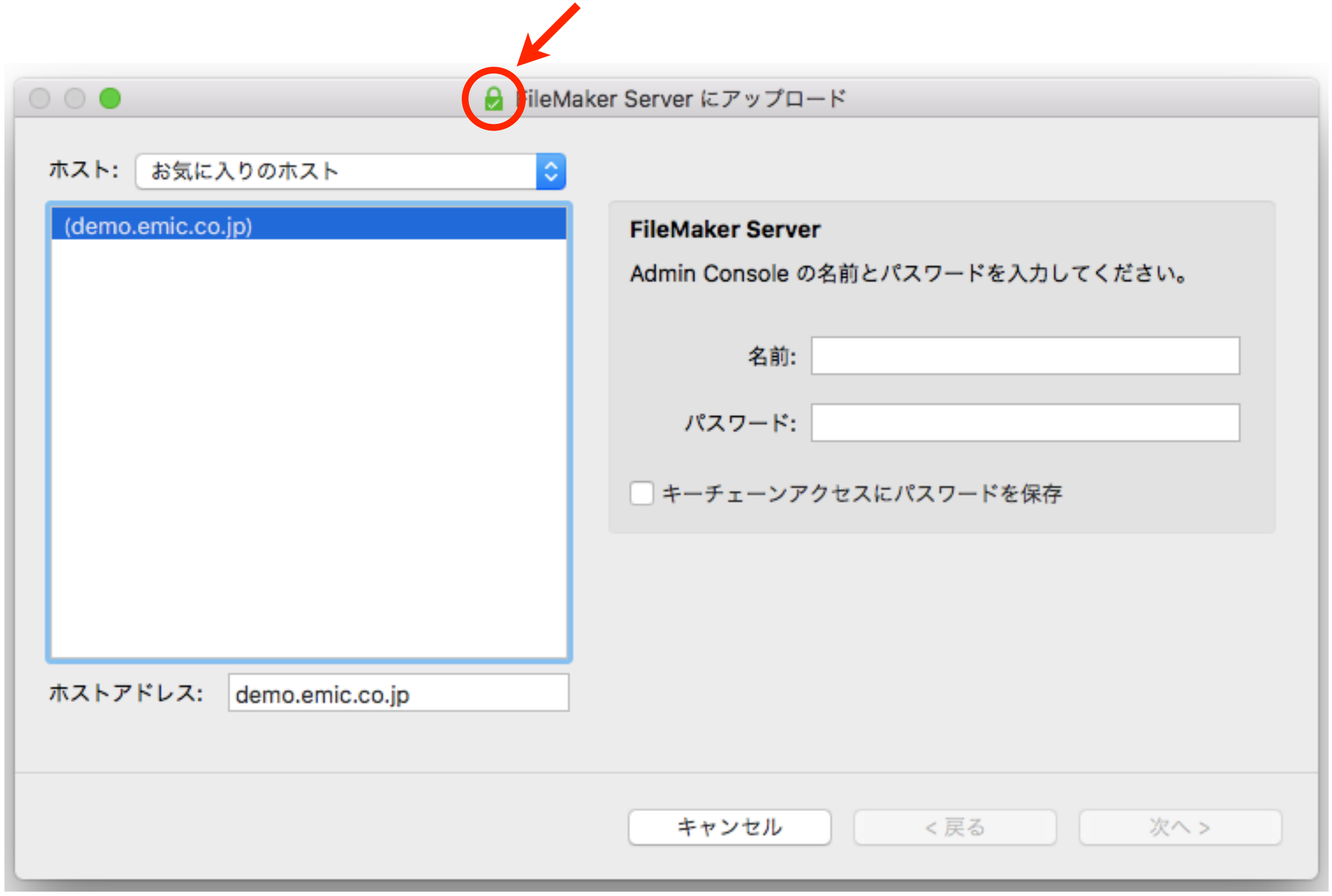

証明書のインポート
証明書をインポートすると、証明機関 (CA) から受け取った署名済み証明書ファイルと証明書署名要求の作成時に作成したプライベートキーファイル (serverKey.pem) が結合されます。
署名済みの証明書ファイル
参照...
プライベートキーファイル
参照...
中間証明書ファイル
参照...
プライベートキーパスワード
パスワード (オプション)
インポート
キャンセル

SSLを使用する設定に

- FileMaker Server 16の場合にはAdmin Consoleで［データベース接続に SSL を使用する］設定を有効化
  - バージョン17以降では証明書インポート時に自動で有効化
- データベースサーバーとWeb公開エンジンを再起動

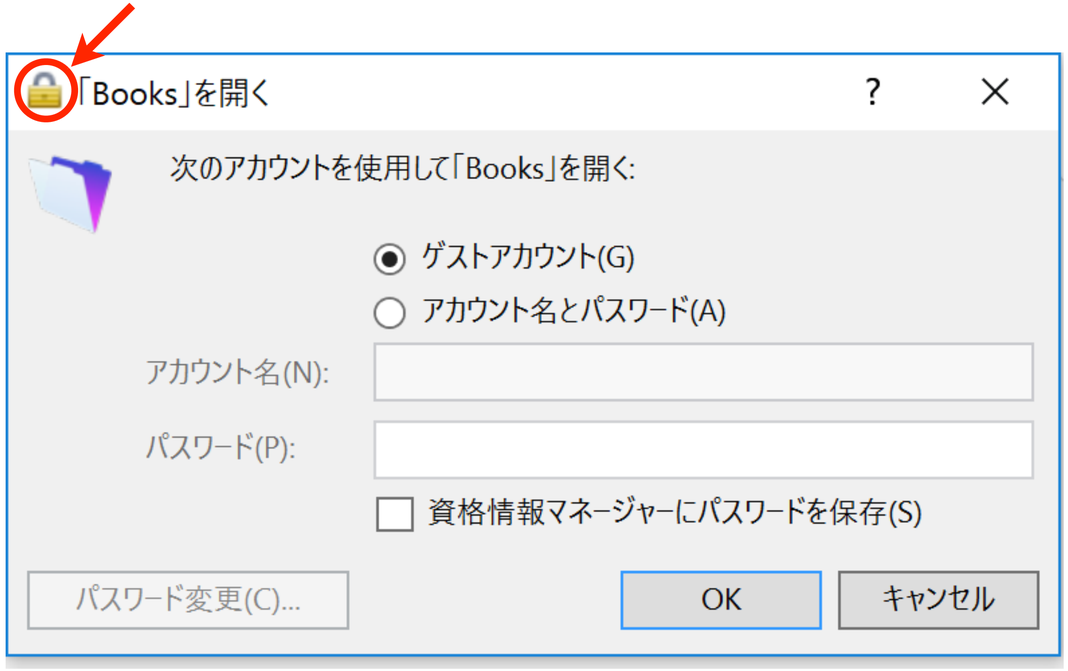
FileMakerクライアントからの接続

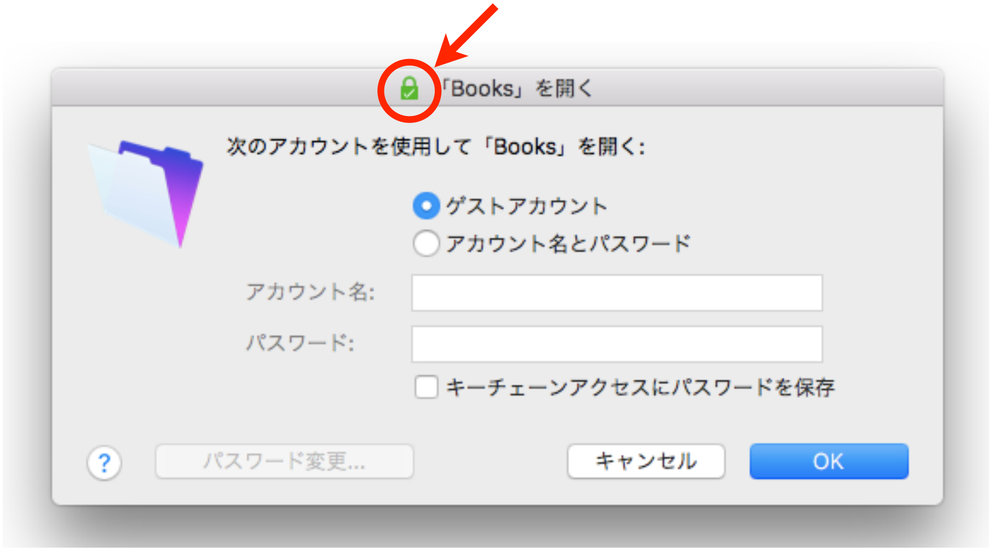
- FileMaker Pro AdvancedやFileMaker Goからサーバーに接続する際には**完全修飾ドメイン名**（サーバー名）を使用
  - IPアドレスの使用は不可

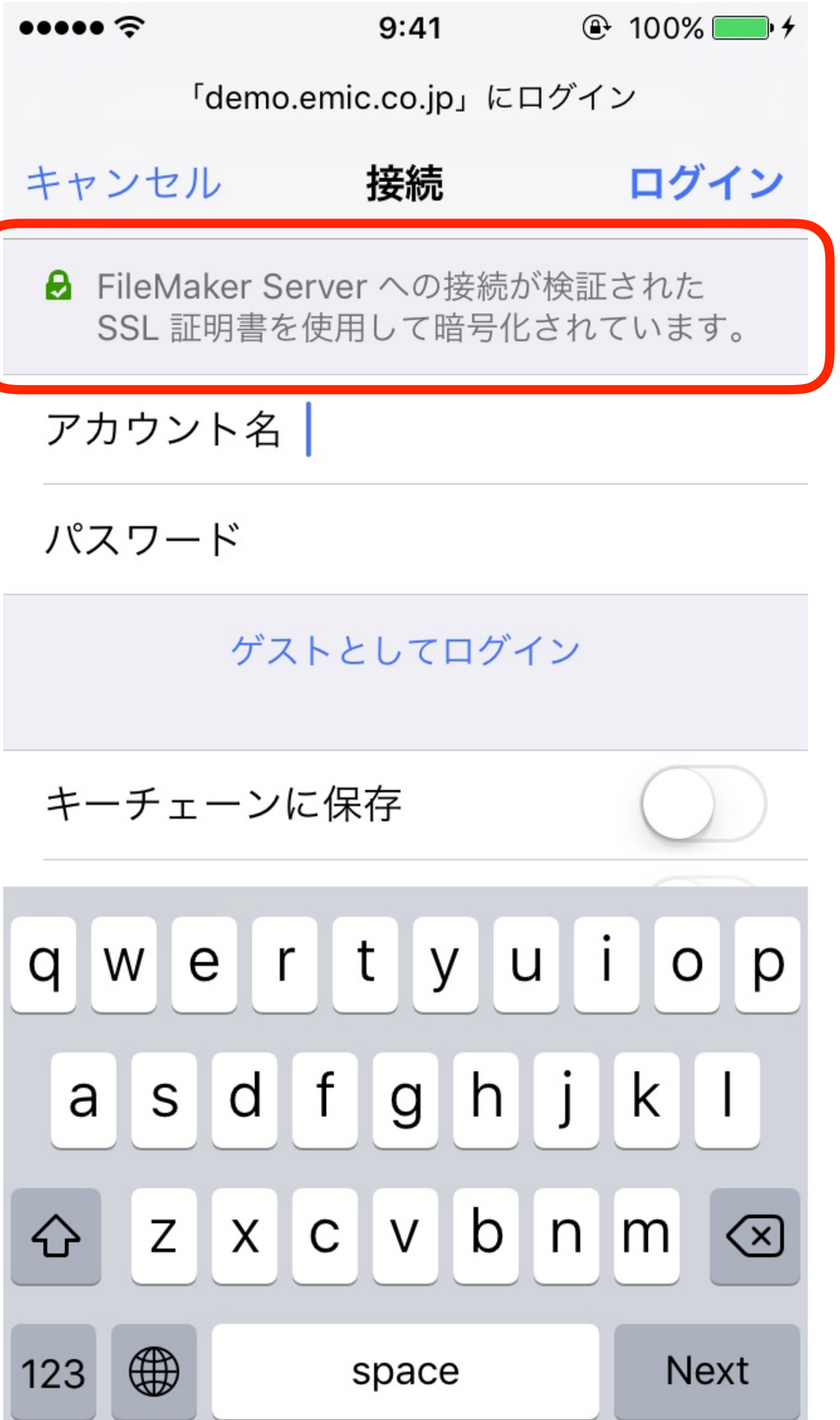

FileMaker Server にアップロード
ホスト:
お気に入りのホスト
(demo.emic.co.jp)
FileMaker Server
Admin Console の名前とパスワードを入力してください。
名前:
パスワード:
キーチェーンアクセスにパスワードを保存
ホストアドレス:
demo.emic.co.jp
キャンセル
< 戻る
次へ >


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

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 一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

FileMaker Server 17 以降の変更点

- Admin ConsoleからCSRファイル作成機能が削除
  - fmsadminコマンドやopensslコマンドを使用して作成する必要がある

3. LANでSSLを利用するには

LANでSSLを利用するには

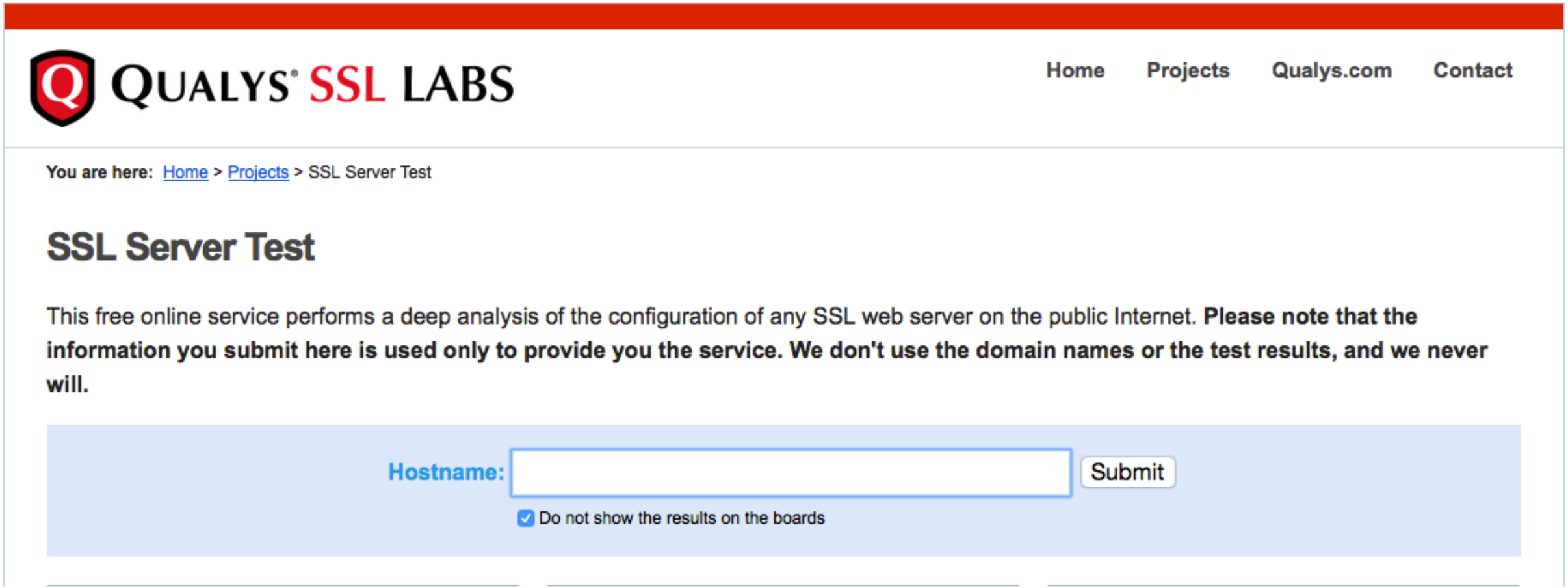
- 名前解決できるネットワーク環境が必要
  - 代表的な方法としては以下のいずれか
    - DNSレコード情報を設定できるルーターを使用
    - LAN内にネームサーバーを構築
    - 各クライアント端末のhostsファイルを編集

関連情報

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



証明書の検証は重要

- ［URL から挿入］スクリプトステップでSSL接続する際には必ず［SSL 証明書の検証］にチェックをつける
  - 証明書の検証不備は脆弱性に相当

    https://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja&useSynonym=1&keyword=%8F%D8%96%BE%8F%91+%8C%9F%8F%D8

証明書の検証は重要


URL から挿入
1
URL から挿入 [選択 ; ダイアログあり: オフ ; ターゲット: blog::url ;
"https://www.famlog.jp/" ; SSL 証明書の検証]
内容全体を選択
ターゲット:
指定...
URL を指定
指定...
SSL 証明書の検証
cURL オプションの指定
指定...

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が一般化・必須化
- FileMaker製品でSSLを使うのであればメーカーサポート対象バージョンを使用