iPad & iPhoneからのリモートアクセスをより安全にするネットワーク構築術

2014/11/27
FileMaker カンファレンス 2014 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
    - ブログ「FAMLog」 http://www.famlog.jp/
    - 「カスタムWeb勉強会」を隔月で開催
    - 執筆書籍「FileMaker Server カスタムWebテクニック」（BNN新社）
  - ✓ FileMaker 8 / 9 / 10 / 11 / 12 / 13 Certified Developer

NTER EDIATOR
Develop Simply, Realize Ideals.
http://inter-mediator.com

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
  - ✓ 今年で16年、「**FMPress**」としてサービスをリニューアル
  - ✓ 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/

FMPress

FMPress Publisher

FileMaker Proで作る

Webアプリとして使う

ポイント

- VPNを利用すると外出先から社内ネットワークに安全に接続できる
- SSLでクライアント・サーバー間の経路を暗号化できる

今回の話題

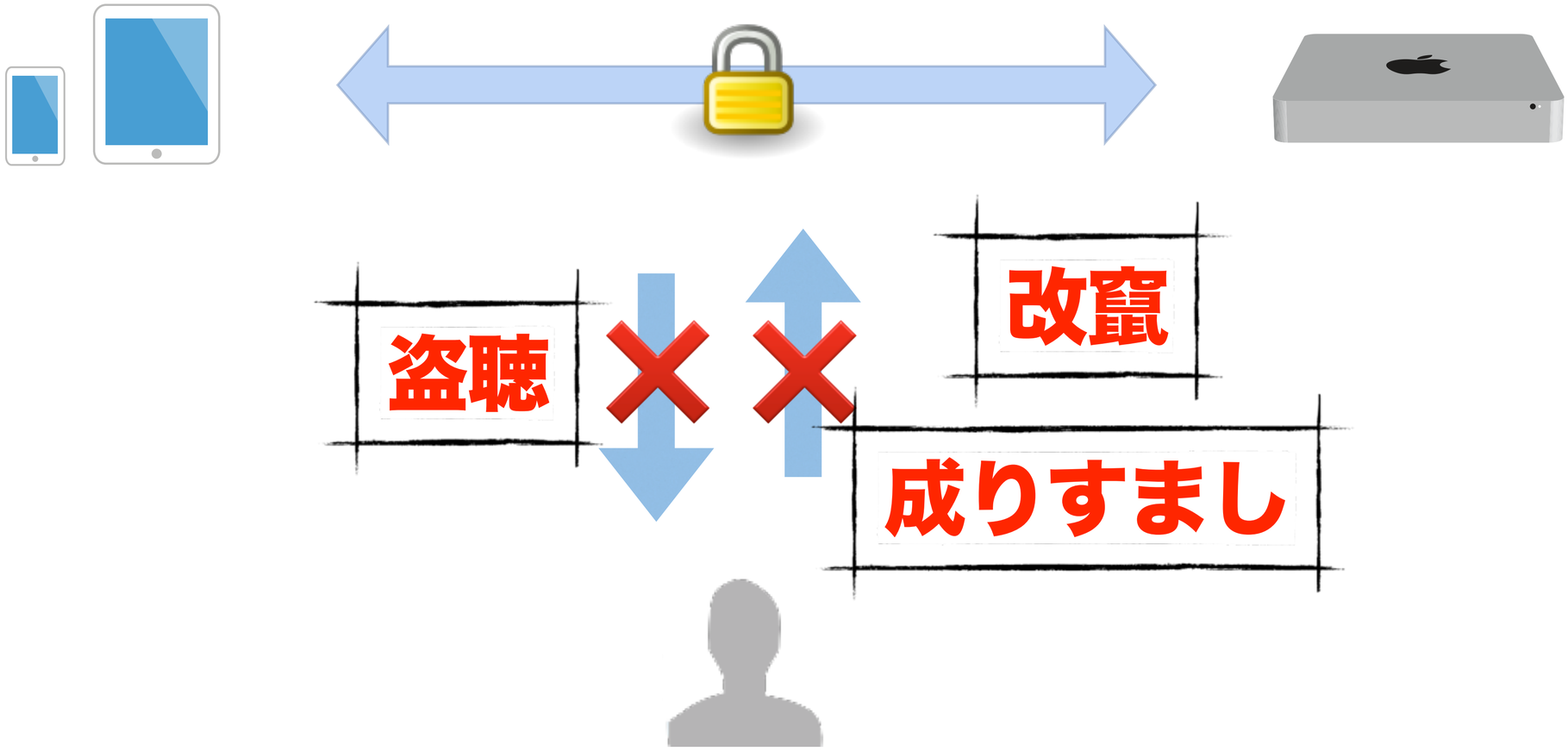
1. VPNとSSLの違いとは
2. iOSでVPNを利用するには
3. FileMaker GoでSSLを利用するには

1. VPNとSSLの違いとは

例えばこのようなとき

- iPadやiPhoneで外出先から社内サーバーにあるデータを見たい
- 利便性だけでなく安全性も考慮したい

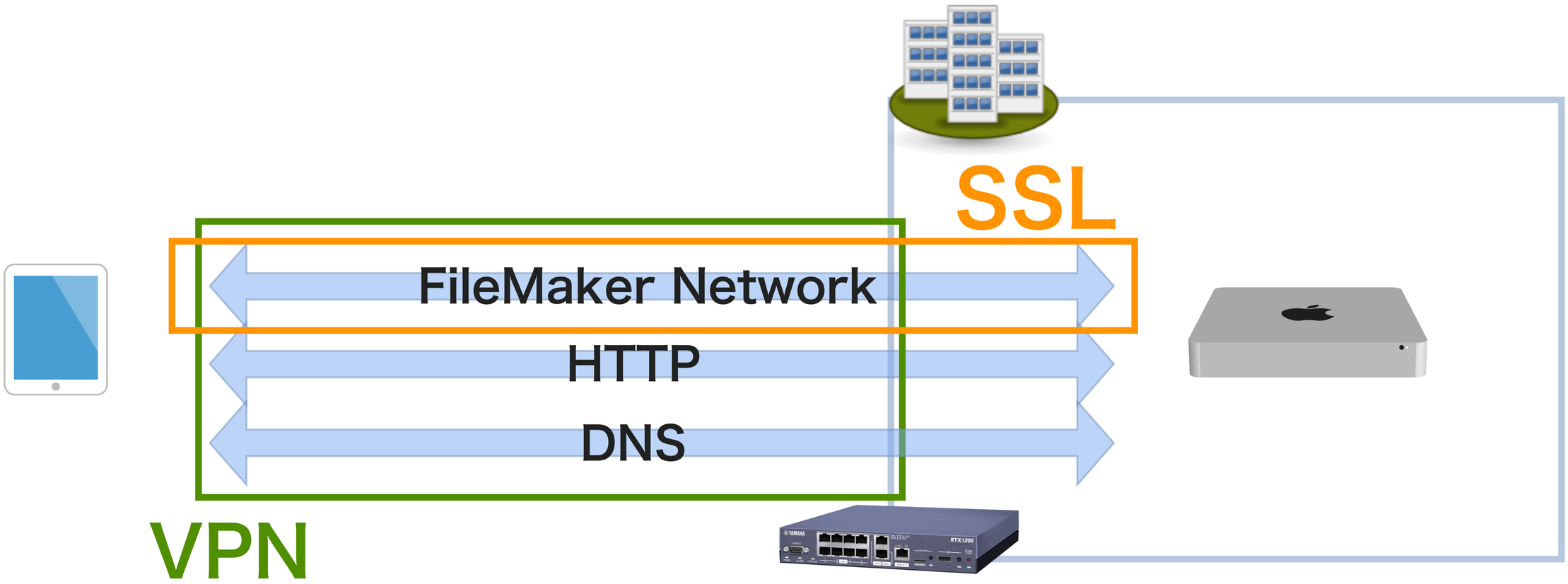
暗号化通信



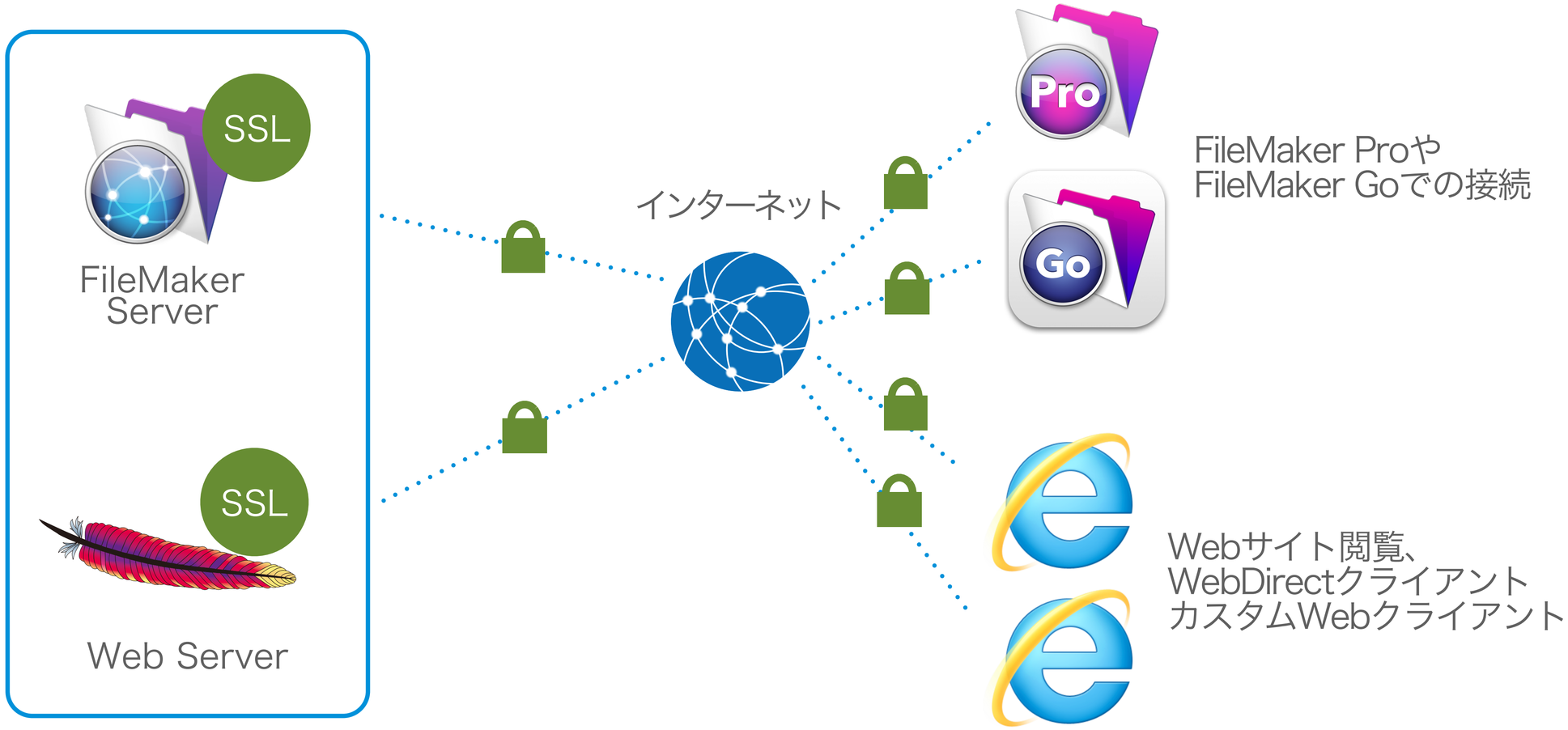
通信を暗号化する方法

- VPN（Virtual Private Network）
- SSL（Secure Sockets Layer）

VPNとSSLの違い



SSLはサービスごとに対応が必要



Virtual Private Network

- 離れた場所から社内ネットワークに安全に接続できる
  - トンネリング

  - 通信パケットの暗号化

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・サーバー間のすべての経路を暗号化

FileMaker Serverは SSLに対応

- 最新の規格はTLS 1.2（TLS：Transport Layer Security）
- FileMaker Pro／GoとFileMaker Server間の通信（TCP 5003番ポートの通信）をSSL/TLSで暗号化

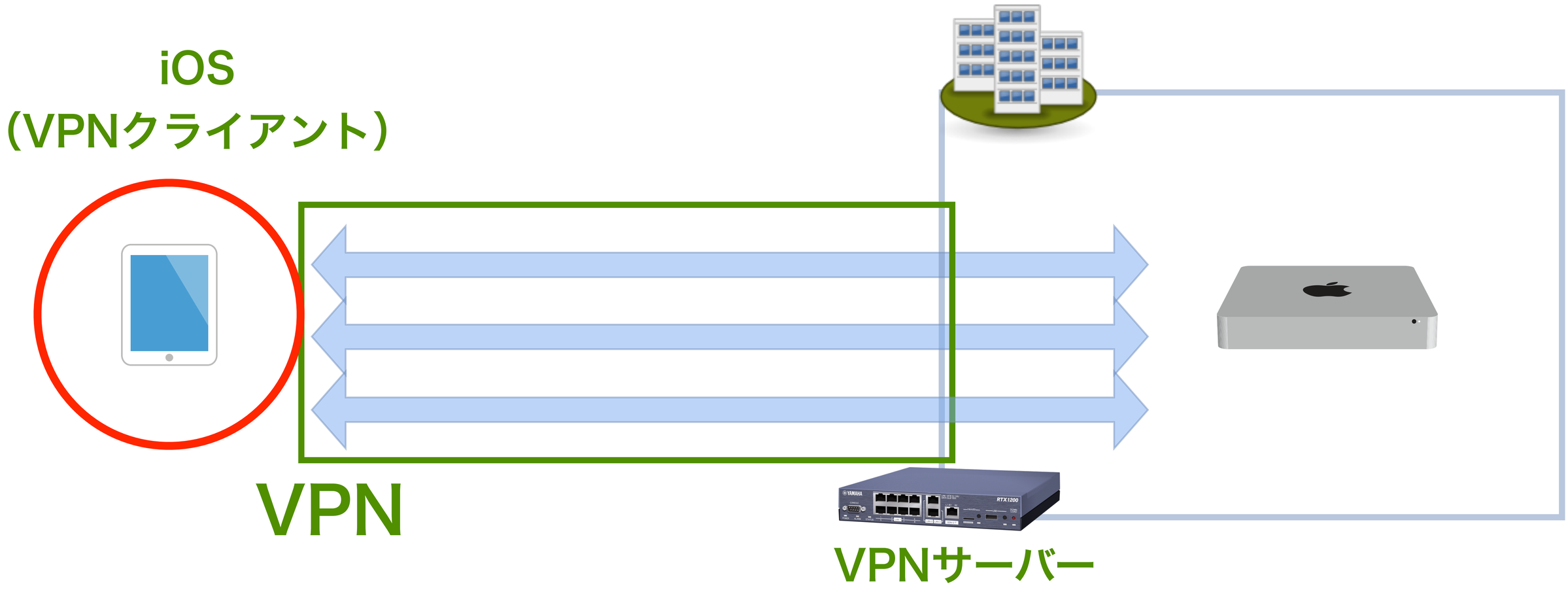
VPNは専用の機器やソフトウェアを利用

- VPNサーバー機能を搭載したルーター
- Windows ServerやOS X Server等に搭載されているVPNサーバー etc.

今回紹介する内容

- FileMaker GoとFileMaker Server間の通信（TCP 5003番ポートの通信）を暗号化する方法に限定

2. iOSでVPNを利用するには


iOS
（VPNクライアント）
VPN
VPNサーバー

iOSは標準でVPNに対応

- VPNサーバーが導入されていればiPadやiPhoneでの設定はとても簡単
- VPN接続完了後にFileMaker Goを起動し社内のFileMaker Serverに接続すればOK

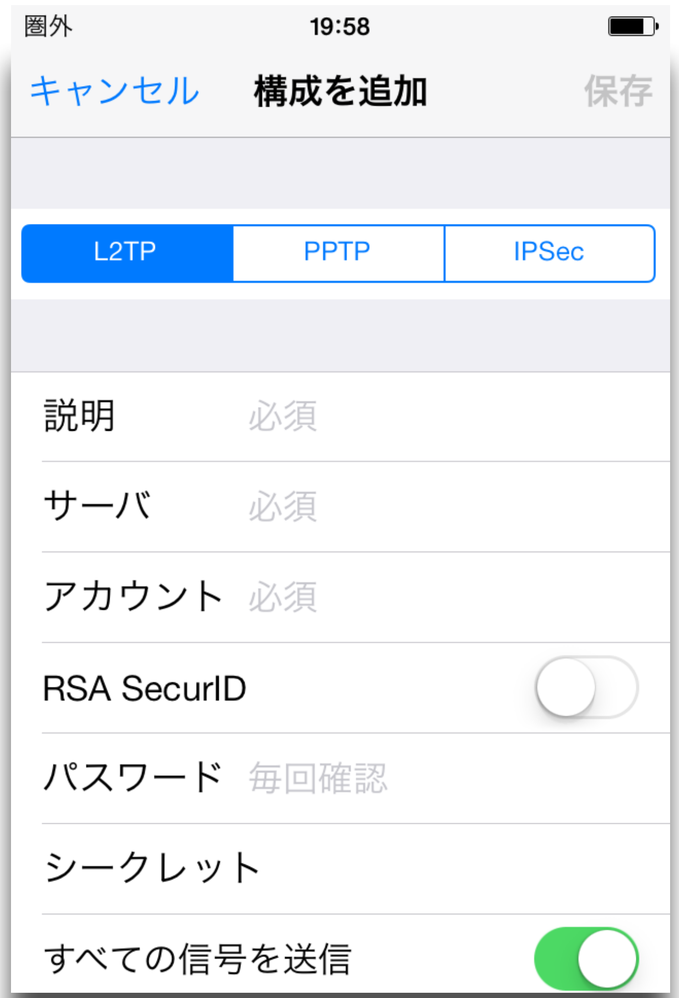
iOSは標準でVPNに対応

容易なVPN設定

圏外
19:58
一般
VPN
VPN
構成を選択...
VPN構成を追加...

iPad
17:23
80%
設定
一般
VPN
機内モード
Wi-Fi
オフ
Bluetooth
オフ
通知センター
コントロールセンター
おやすみモード
一般
サウンド
壁紙/明るさ
プライバシー
iCloud
メール/連絡先/カレンダー
メモ
VPN
構成を選択...
VPN構成を追加...

容易なVPN設定


圏外
19:58
キャンセル
構成を追加
保存
L2TP
PPTP
IPSec
説明 必須
サーバ 必須
アカウント 必須
RSA SecurID
パスワード 毎回確認
シークレット
すべての信号を送信

iPad
17:23
80%
設定
一般
VPN
機内モード
Wi-Fi
Bluetooth
通知センター
コントロールセンター
おやすみモード
一般
サウンド
壁紙/明るさ
プライバシー
iCloud
メール/連絡先/カレンダー
メモ
キャンセル
構成を追加
保存
L2TP
PPTP
IPSec
説明 必須
サーバ 必須
アカウント 必須
RSA SecurID
パスワード 毎回確認
シークレット
すべての信号を送信
プロキシ
オフ
手動
自動

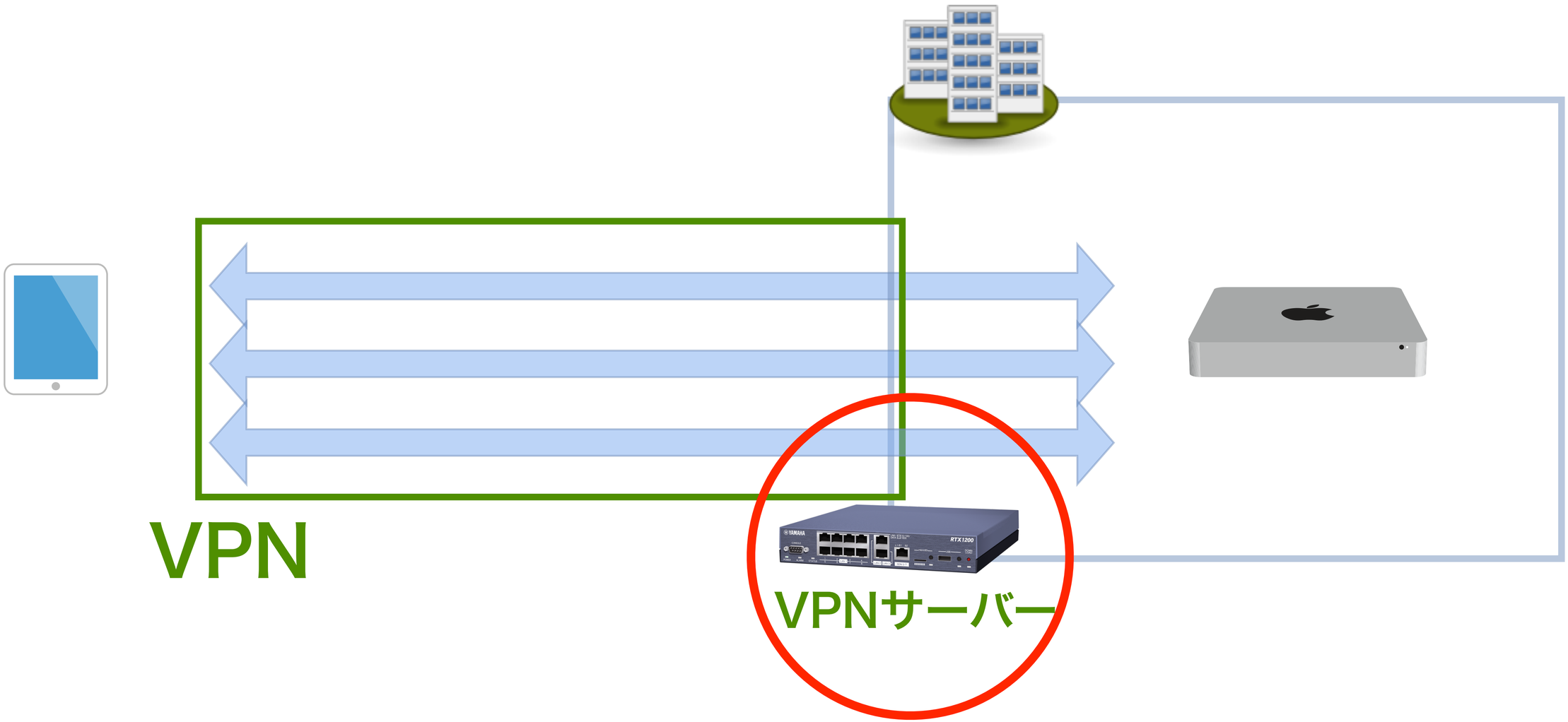
設定後は接続も簡単

圏外
VPN
20:06
設定
機内モード
Wi-Fi Ogikubo AirMac Extr…
VPN
Bluetooth オフ
モバイルデータ通信
キャリア
通知センター
コントロールセンター

iPad
VPN
17:29
79%
設定
一般
コントロールセンターから画面の向きをロックできます。
機内モード
Wi-Fi
Bluetooth オフ
VPN
通知センター
コントロールセンター
おやすみモード
一般
サウンド
壁紙/明るさ
プライバシー
iCloud
メール/連絡先/カレンダー
使用状況
Appのバックグラウンド更新
自動ロック 2分
パスコードロック オフ
機能制限 オフ
日付と時刻
キーボード
言語環境
iTunes Wi-Fi同期
VPN 接続中
リセット

iOS 8の新機能

- IKEv2およびVPN常時接続をサポート
  - Apple ConfiguratorもしくはOS X Serverのプロファイルマネージャを使用して設定


VPN
VPNサーバー

サーバー側で必要な機器

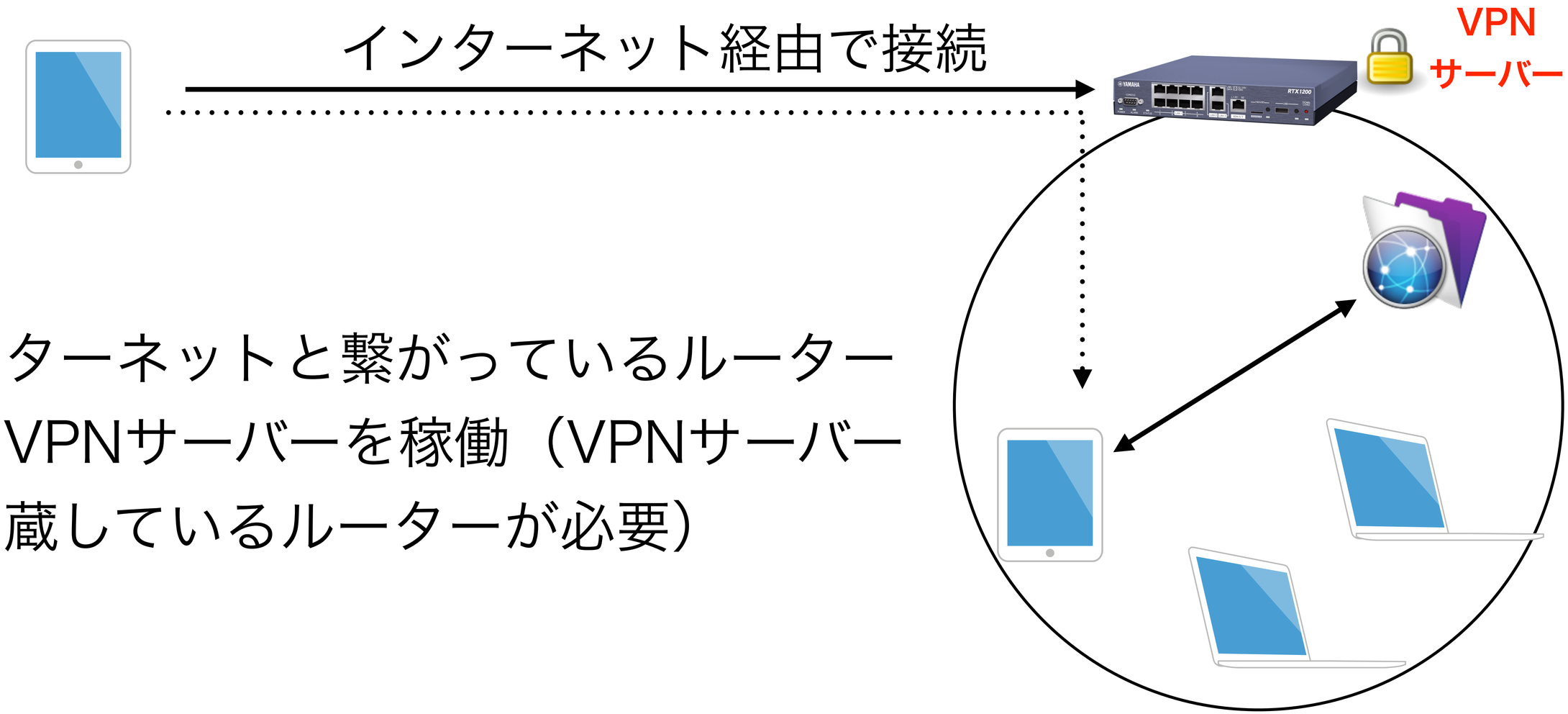
- VPNサーバーを内蔵したルーター

  - インターネットにつながっているルーターにVPNサーバー機能がない場合は？

通信するためのネットワーク設定

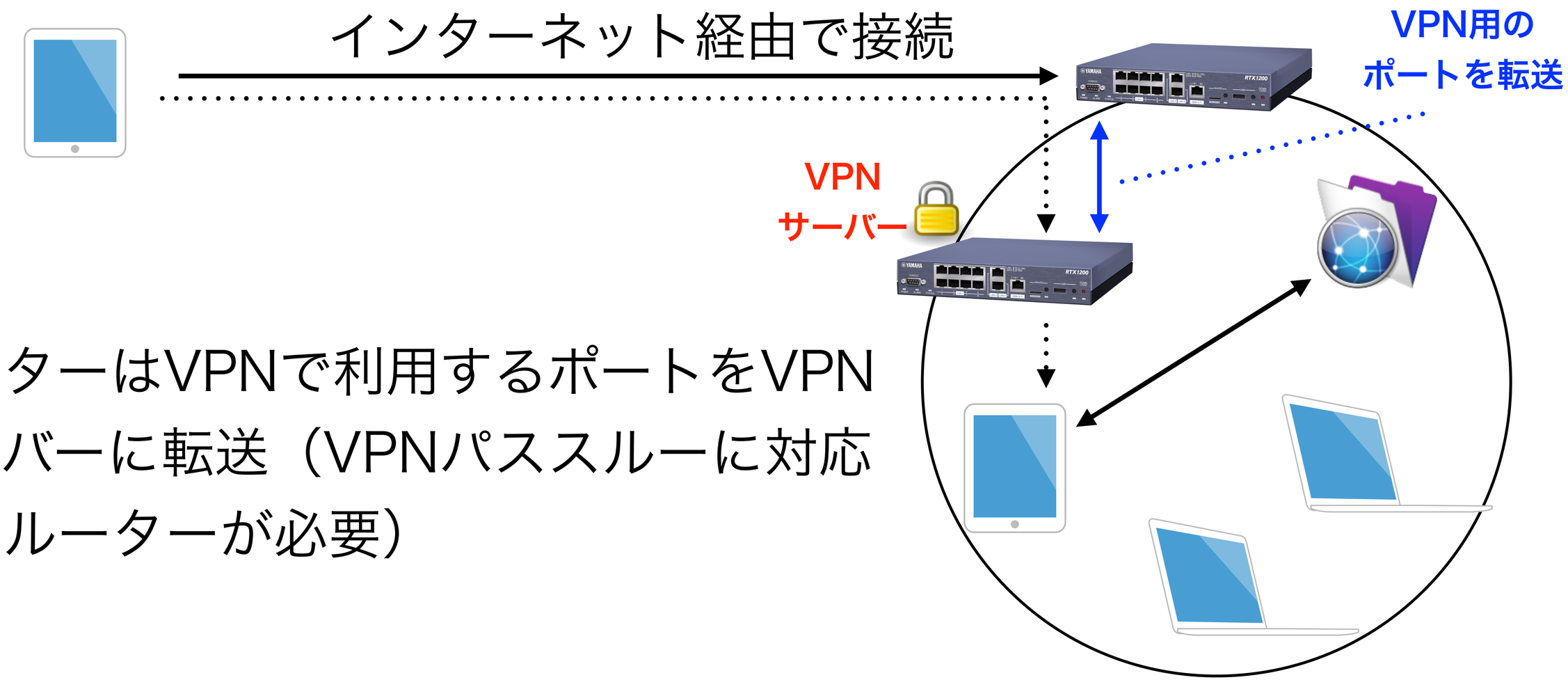
- はまるポイント -

(1) VPNサーバーをインターネット接続ルーター上で稼働



インターネットと繋がっているルーター上でVPNサーバーを稼働（VPNサーバーを内蔵しているルーターが必要）

(2) VPNサーバーを LAN内で稼働



ルーターはVPNで利用するポートをVPNサーバーに転送（VPNパススルーに対応したルーターが必要）

グローバルIPアドレスの有無を確認

- 社内にあるルーターが直接インターネットにつながっているか
- グローバルIPアドレスが固定であるのか動的であるのか

VPNサーバー機能の有無を確認

- インターネットにつながっているルーターがVPNサーバー機能を搭載しているか
  - 搭載していない場合にはVPNパススルー機能の有無を確認

VPNパススルー機能の確認

- インターネットにつながっているルーターがVPNパススルー機能に対応しているか
  - VPNで使うポートの解放および転送ができるか
  - 表記はメーカーによって違うことも

L2TP over IPSecで開ける必要があるポート

- UDP 500番ポート
- UDP 1701番ポート
- UDP 4500番ポート
- ESP（IPプロトコル番号50）

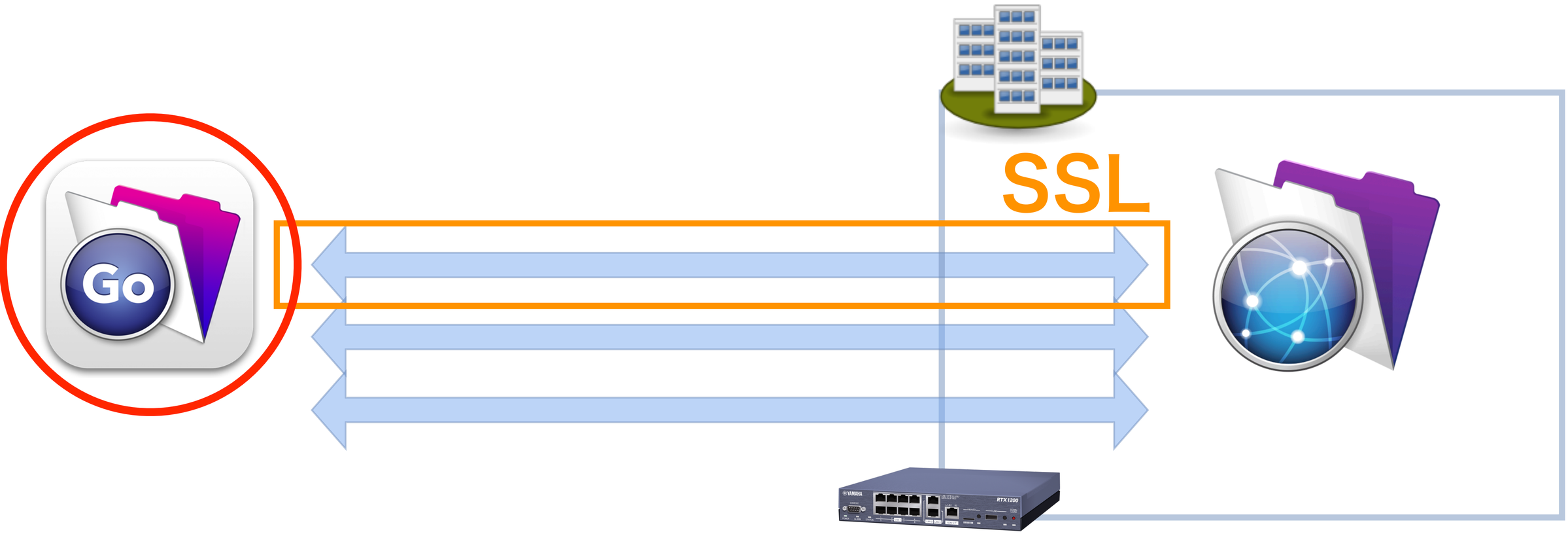
ポイント

- グローバルIPアドレスの有無
- VPNサーバー機能の有無
- ルーターのVPNパススルー機能
  - VPNで使うポートの解放と転送

3. FileMaker GoでSSLを利用するには

どのバージョンが必要？

- FileMaker Goはバージョン13
  （FileMaker Proも同様）
- FileMaker Serverは12もしくは13


SSL
Go
YAMAHA
RTX1200

FileMaker Goからの接続

- FileMaker Go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
- プログレッシブダウンロード用の通信は暗号化されない

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
iOS 8アプリケーション開発入門

著者
新居 雅行 (著)

カテゴリ
☐ FileMaker ☐ Mac OS X ☐ Access
☒ iOS ☐ Excel ☒ Windows

発売日・発売時期
2014/10/17

評価
5

ページ数

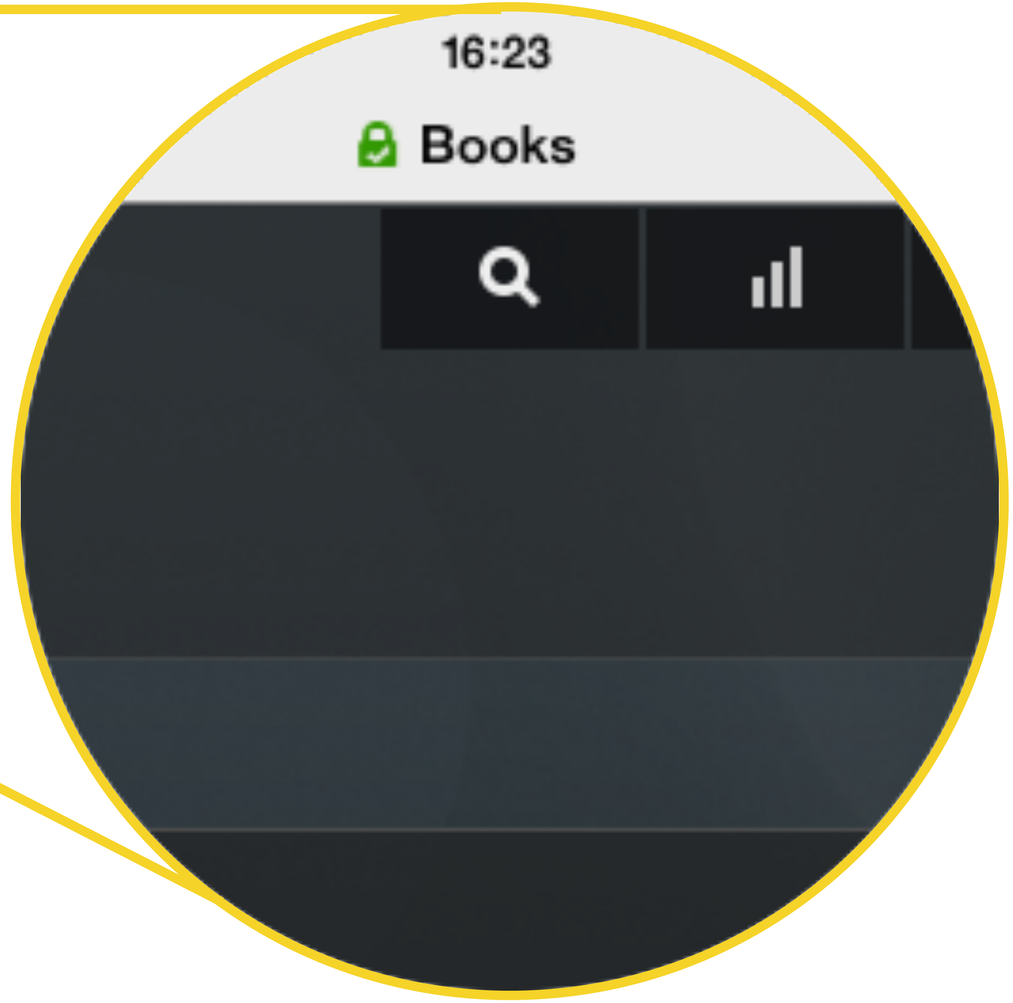
ISBN

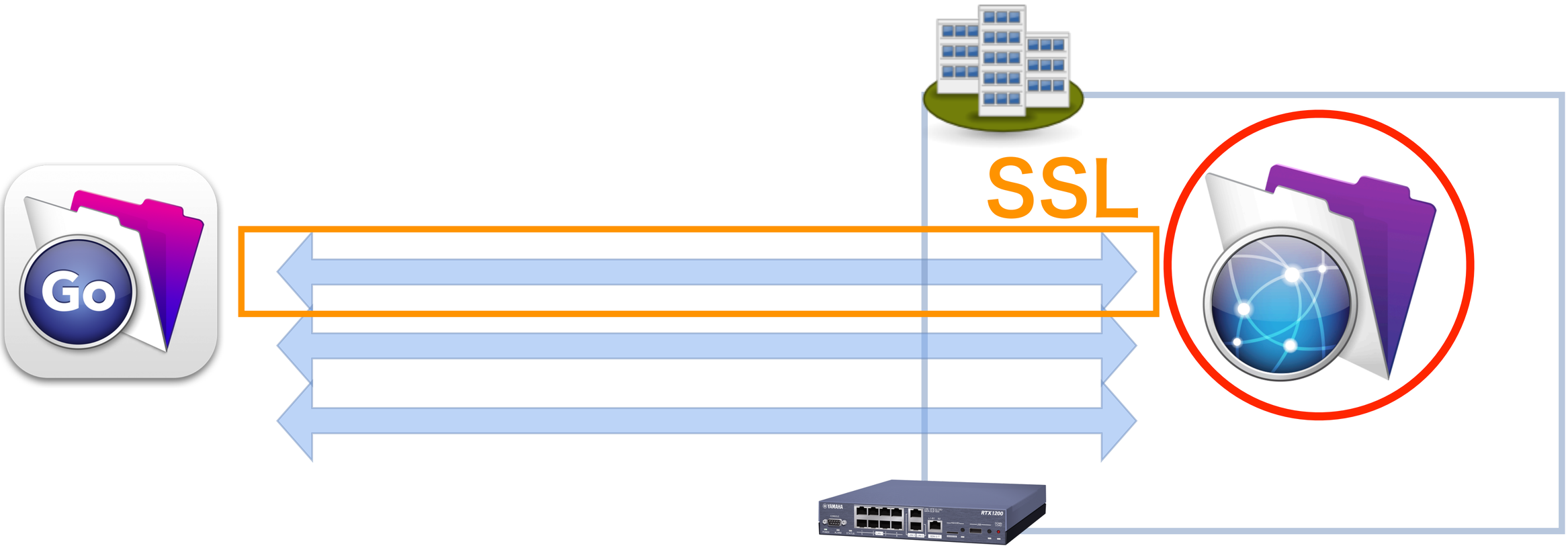
在庫
○ あり ● なし

出版社
自費出版

本書の概要
本書は、2012年にiOS 5向けに執筆し技術評論社より出版された『iOSアプリケーション開発入門』の一部がベースになっていますが、iOS 8向けに大幅に書き直した別の書籍です。
内容は、iOS 8での開発を基本から説明しています。ストーリーボードを使った開発、プロパティ、アウトレット、アクション、そしてナビゲーションコントロー

iOS 8アプリケーション開発入門 FMPressPublisher

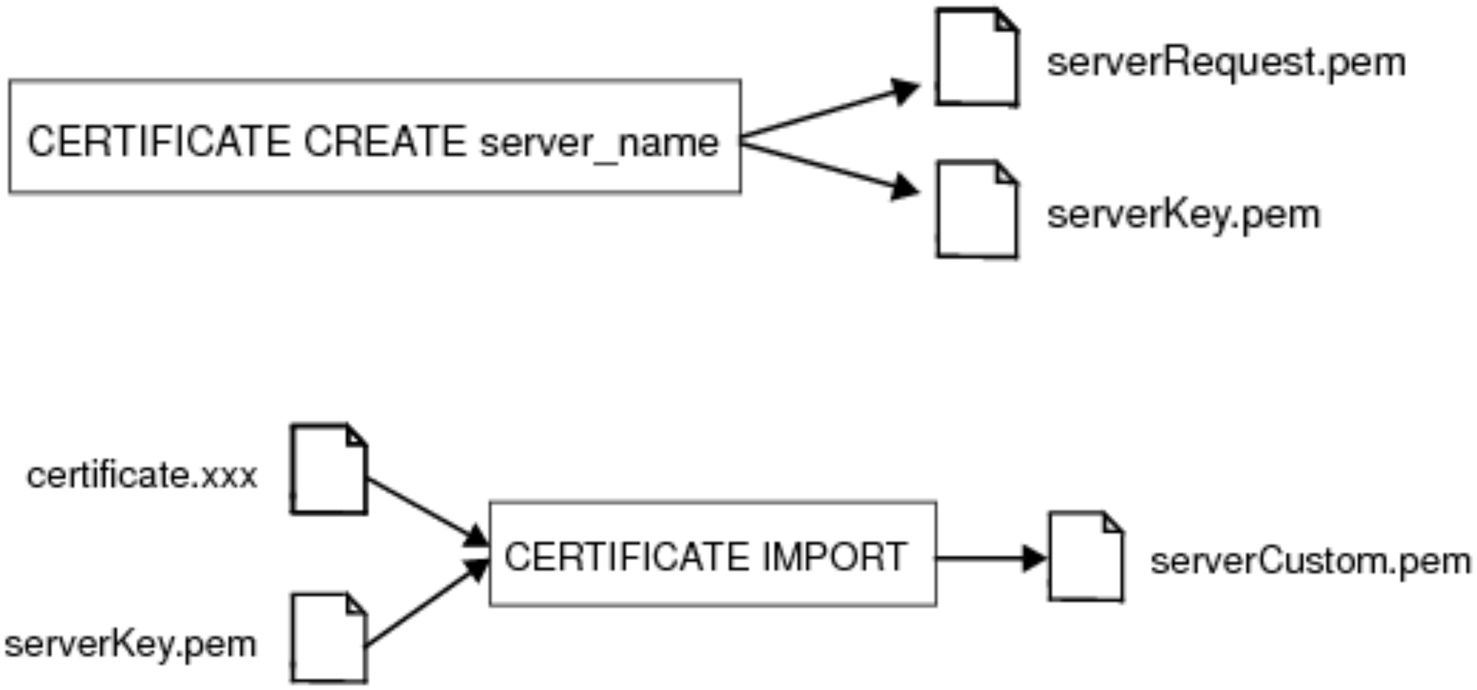



SSL
Go
YAMAHA
RTX1200

SSL対応手順概要

- 認証局からSSLサーバー証明書を購入
- fmsadmin certificateコマンドで証明書を読み込み、［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を再起動

fmsadminコマンド



（FileMaker Server 13 ヘルプより）

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

SHA-1からSHA-2へ

- 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来年まで
- 今後新規に発行する証明書はSHA-2版の選択を推奨

証明書購入時の注意点

- SHA-2版SSLサーバー証明書に対応しているFileMaker製品は最新バージョンのみ
- ワイルドカードSSLサーバー証明書には非対応（例：*.example.jp）
- EV SSL証明書にも非対応

SHA-2対応に必要なバージョン

- FileMaker Go 13.0.7
- FileMaker Pro 13.0v4（FileMaker Pro Advancedも同様）
- FileMaker Server 13.0v5

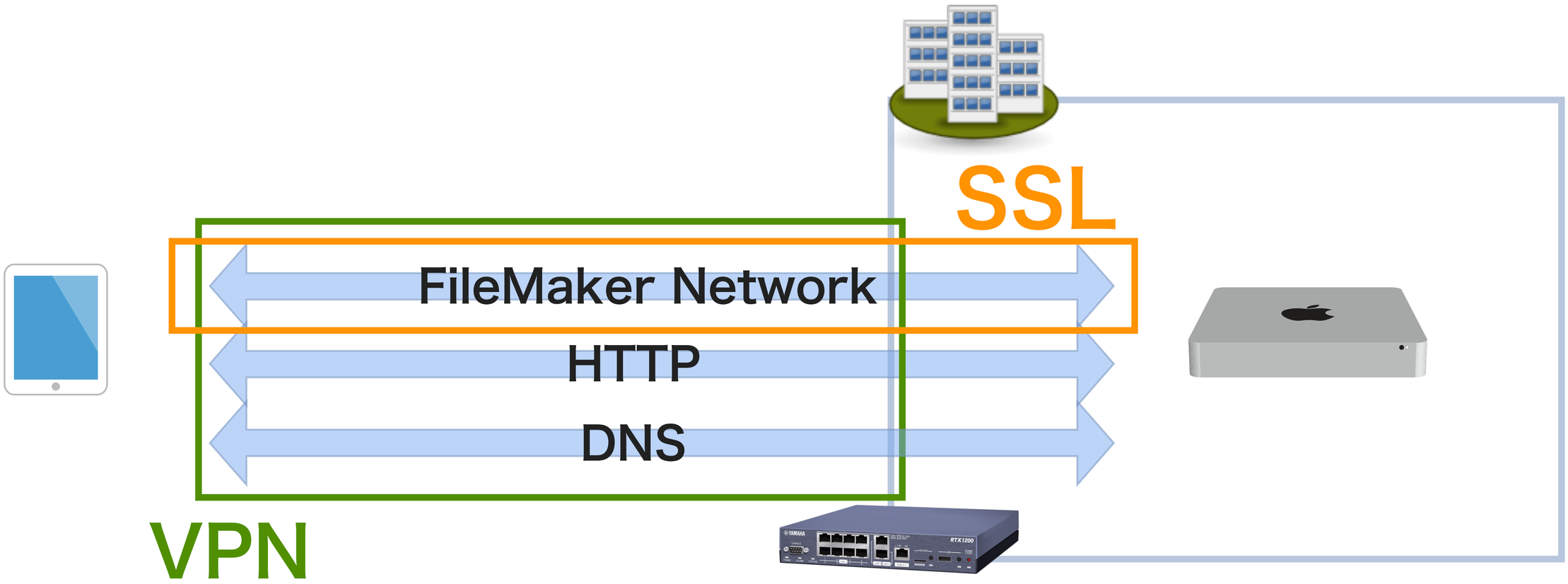
詳しくは

- FileMaker 製品でサポートされる SSL サーバー証明書の販売元と種類の一覧（FileMaker ナレッジベース）

  http://filemaker-jp.custhelp.com/app/answers/detail/a_id/12130

まとめ

VPNとSSLの違い



まとめ

- VPNを利用すると外出先から社内ネットワークに安全に接続できる
- SSLでクライアント・サーバー間の経路を暗号化できる
- SSLを使う場合は今後SHA-2へ要移行