

FileMaker 12 セキュリティ更新 に関する考察

2015/06/20

FM-Tokyo ライトニングトーク発表資料

松尾篤（株式会社エミック）

Agenda

- FileMaker 13.0v9に関するおさらい
- FileMaker 12 セキュリティ更新
- FileMaker 14での改良点

FileMaker 13.0v9 に関するおさらい

13.0v9 アップデータ

- 2015年4月7日にリリース
 - FileMaker Pro 13.0v9
 - FileMaker Pro 13.0v9 Advanced
 - FileMaker Server 13.0v9

13.0v9はセキュリティ修正

- “FileMaker 13 プラットフォームの潜在的な SSL の問題を解決”

http://filemaker-jp.custhelp.com/app/answers/detail/a_id/14307

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。”

Pro 13.0v9からサーバーに 接続できない場合が存在

- 証明書未購入でSSLを有効にしている
FileMaker Server 13（かつバージョン
13.0v9に未更新の場合）
- SSLを有効にしているFileMaker Server
12（セキュリティ更新未適用の場合）

アップデート手順に要注意

- 接続できないケースに該当する場合
 - 先にFileMaker Serverをアップデート
 - サーバーをアップデートした後に
FileMaker Pro/Goを13.0v9/13.0.9に更新
- ➡ 正確には“一斉アップデートが必要”

一斉アップデートが 不要なケース

- FileMaker Serverを使用していない場合
- FileMaker ServerでSSL（保護された接続が必要）を有効化していない場合
- FileMaker Server 13で認証局から購入した証明書を使用している場合

SSL利用時の留意点

- 暗号化通信の実現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サーバー証明書は限られている

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

FileMaker 13.0v9での修正

- FileMaker Pro 13とFileMaker Go 13に含まれる**FileMaker ルート証明書の削除**が更新の主目的と推測される
- 信頼できないルート証明書が組み込まれていると暗号化通信全体が無意味に

詳しくは

- FileMaker 13.0v9の修正点に関する考察

<http://www.famlog.jp/article/2710>

FileMaker 12 セキュリティ更新

2015年4月22日にリリース

- FileMaker Pro 12 セキュリティ更新
- FileMaker Pro 12 Advanced セキュリティ更新
- FileMaker Server 12 セキュリティ更新

FileMaker Go 13.0.9

- FileMaker 12 セキュリティ更新と同時にリリース
- FileMaker Go 12の修正版はリリースされないなのでSSL利用時にはFileMaker Go 13.0.9もしくは14に要アップグレード

いくつかの疑問点

- FileMaker Server 12の場合は認証局から購入したカスタムSSL証明書を使用している場合でも一斉アップデートが必要
- 13で追加されたFileMaker ルート証明書の削除自体はFileMaker Pro 12には関係ないはず

いくつかの疑問点から

- ということは、ナレッジベースで言及されている点以外に何か挙動を修正している点があるのでは？

http://filemaker-jp.custhelp.com/app/answers/detail/a_id/14597

証明書の鍵長

- FileMaker Server 12 セキュリティ更新適用前：1024bit
- FileMaker Server 12 セキュリティ更新適用後：2048bit

証明書の鍵長

```
$ openssl x509 -in "/Library/FileMaker  
Server/CStore/server.pem" -text | grep "RSA  
Public Key"
```

RSA Public Key: (1024 bit)



RSA Public Key: (2048 bit)

証明書の鍵長

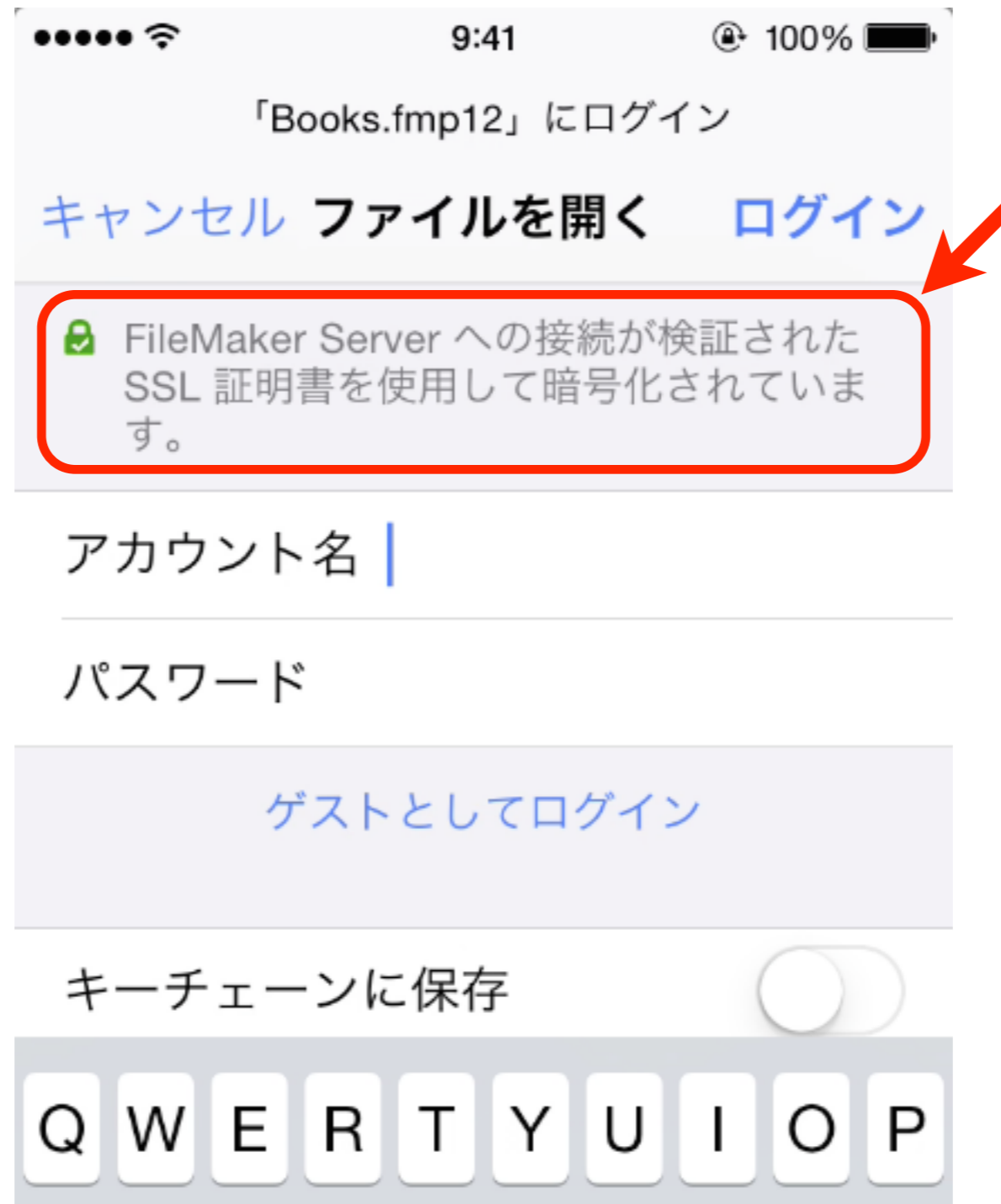
- FileMaker 13.0v9およびFileMaker 12 セキュリティ更新には、鍵長2048bit未満の証明書を無効化する修正も含まれているのでは？

FileMaker 14での改良点

FileMaker Pro 14



FileMaker Go 14



FileMaker Server 14



まとめ

SSLを使うのであれば

- FileMaker Proは13.0v9以降に、FileMaker Goは13.0.9以降に必ず更新
- デフォルトのSSLサーバー証明書ではなく認証局から購入した証明書を使う
- SHA-2 (SHA-256) 対応を考慮するとFileMaker Serverも13.0v9以降に要更新