

Tips: ユーザ認証

Ver. 1.0
2019 年 10 月

概要：

- FileMaker プラットフォームでは、FileMaker Pro Advanced ファイル内にアカウント情報を持つ内部認証に加え、FileMaker Server や FileMaker Cloud for AWS で FileMaker Pro Advanced ファイルを共有する場合には、外部認証サーバーや OAuth アイデンティティプロバイダによる認証を利用することができます。
- OAuth アイデンティティプロバイダによる認証を利用する場合には、OAuth アイデンティティプロバイダによる多要素認証を利用することができます。
- FileMaker Go では、iOS の顔認証（Face ID）や指紋認証（Touch ID）等と FileMaker プラットフォームでの認証を組み合わせた多要素認証を利用することができます。

内容

Tips: ユーザ認証	i
1. ガイドライン要求事項の内容	1
1.1. ガイドライン要求事項の概要	1
1.2. 2 要素（多要素）認証	1
2. ユーザ認証に関する FileMaker プラットフォームの基本機能	3
2.1. FileMaker Pro 18 Advanced	3
2.1.1. FileMaker ファイルアカウント（内部認証）	3
2.2. FileMaker Server 18	3
2.2.1. 外部サーバーアカウントによる認証（外部認証）	4
2.2.2. OAuth アイデンティティプロバイダによる認証	6
2.3. FileMaker Cloud for AWS 1.18	6
2.3.1. OAuth アイデンティティプロバイダによる認証	6
2.4. FileMaker Go 18	6
3. その他のユーザ認証方法	9
3.1. 多要素認証を利用する	9
3.2. 他の医療情報システムのユーザ認証機能を利用する	9
4. 留意事項	11
4.1. FileMaker ファイルアカウントのデフォルトアカウント	11
4.2. FileMaker パスワードの保存	11

用語

本ドキュメントでの略称	ガイドライン
厚労省ガイドライン	厚生労働省 「医療情報システムの安全管理に関するガイドライン 第 5 版」(平成 29 年 5 月)
経産省ガイドライン	経済産業省 「医療情報を受託管理する情報処理事業者向けガイドライン (第 2 版)」 (平成 24 年 10 月)
総務省ガイドライン	総務省 「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン (第 1 版)」(平成 30 年 7 月)

本ドキュメントでは、以下の製品を対象としています。

- FileMaker Pro 18 Advanced
- FileMaker Server 18
- FileMaker Cloud for AWS 1.18
- FileMaker Go 18

1. ガイドライン要求事項の内容

1.1. ガイドライン要求事項の概要

医療情報システム自の利用者の識別・認証機能は、医療情報システムへのアクセスを正当な利用者のみに限定するための手段の一つです。

厚労省ガイドラインでは、医療情報システムの不正な利用（なりすまし）を防止する観点から、利用者を正しく識別し、認証を行うことを求めています。同様に、経産省ガイドラインでは「作業者は情報処理装置上においてユニークな作業者 ID によって識別されること」、総務省ガイドラインでは「情報システムの利用者を特定し識別できるように、アカウントの発行を行う」ことが求められています。

1.2. 2 要素（多要素）認証

利用者の認証には、ID とパスワードの組み合わせによる方法がこれまで広く利用されてきています。しかし、ID・パスワードのみによる認証では、厚労省ガイドライン「6.5 技術的安全対策／B. 考え方／(1) 利用者の識別および認証」に列挙されているように、その運用によってリスクが大きくなることが知られています。

これを受けて厚労省ガイドラインでは、パスワードの認証強度の維持に関する要求事項¹を挙げながらも、「このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。」とし、「（そこで、）IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）を採用することが望ましい。」としています²。同様に、経産省ガイドライン、総務省ガイドラインでも 2 要素（多要素）認証を推奨しています。

各ガイドラインの多要素認証の要求事項を表 1 にまとめます。

表 1 多要素認証に関する要求事項

ガイドライン	章節	要求事項
厚労省	6.5 D.	5. 認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又は IC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。 ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。
経産省	7.6.14 C.	（作業者のログオンについて推奨される安全管理策） (5) ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。
総務省	3.2.3 C. (ア) 4.	① 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2 要素認証以上の認証強度のある方法による。

¹ 例：「(1) パスワードは定期的に変更し（最長でも 2 ヶ月以内 ※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。」（厚労省ガイドライン「6.5 技術的安全対策／C. 最低限のガイドライン／11」）

² 厚労省ガイドライン「6.5 技術的安全対策／B. 考え方／(1) 利用者の識別及び認証／＜認証強度の考え方＞」

総務省	3.2.3 C. (ア) 4.	② 利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。
総務省	3.2.3 C. (ア) 4.	③ 利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合には、固定式の ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。 なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第 5 版の公表（平成 29 年 5 月）から約 10 年後を目途に 2 要素認証について厚生労働省ガイドライン 6.5 章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。

なお、現版の厚労省ガイドラインでは、多要素認証は「D.推奨されるガイドライン」の位置付けですが、以下に引用³のとおり、2027 年頃を目処に、多要素認証が最低限要求されるガイドラインとなることが想定されています。

※ 認証技術の端末等への実装状況等を鑑み、本ガイドライン第 5 版の公表から約 10 年後を目処に「C.最低限のガイドライン」とすることを想定する。

³ 厚労省ガイドライン「6.5 技術的安全対策／B. 考え方／(1) 利用者の識別及び認証／＜認証強度の考え方＞」

2. ユーザ認証に関する FileMaker プラットフォームの基本機能

2.1. FileMaker Pro 18 Advanced

FileMaker プラットフォームでは、次の 3 種類のアカウントを利用することができます。

- ① FileMaker ファイルアカウント（内部認証）
- ② 外部サーバーアカウント（外部認証）
- ③ OAuth アイデンティティプロバイダアカウント

これらのうち、②外部認証と③OAuth アイデンティティプロバイダ認証は、FileMaker カスタム App を FileMaker Server もしくは FileMaker Cloud for AWS を使って共有した場合に利用可能ですが、設定は FileMaker Pro Advanced 上で行います。詳しくは、本資料の 2.2.1 および 2.2.2 を参照してください。

2.1.1. FileMaker ファイルアカウント（内部認証）

FileMaker ファイルアカウントは、アカウント名とパスワードを FileMaker Pro Advanced ファイルに保存します。FileMaker ファイルアカウントの設定方法については、FileMaker Pro 18 Advanced ヘルプ「FileMaker ファイルアカウントの編集」⁴を参照してください。

なお、FileMaker プラットフォームにおいて、5 分間の間に、同じアカウント名に異なるパスワードを 5 回試行してログインに失敗すると、そのアカウント名が 5 分間ロックされます。この機能は、FileMaker ファイルアカウントについてのみ有効です。この場合、クライアントではなくアカウントがロックされるので、同じクライアントから別の有効なアカウントを使ってログインすることができます（図 1）。



図 1 同一アカウントで異なるパスワードを 5 回失敗時のアラート（FileMaker Pro Advanced）

2.2. FileMaker Server 18

FileMaker Server で FileMaker Pro Advanced のファイルを共有する場合、FileMaker ファイルアカウント（内部認証）に加え、次のような外部で定義されたアカウントとグループによる認証を利用することができます。

- (1) マスタマシン上にローカルに定義された Windows または macOS のアカウントおよびグループ（ローカル認証）
- (2) 一元管理された認証サーバー上に保存可能な、Apple Open Directory (OD) および Windows Active Directory (AD) のアカウントとグループ（ドメイン認証）
- (3) Login with Amazon, Google Identity Platform および Microsoft などの OAuth アイデンティティプロバイダ

⁴ https://fmhelp.filemaker.com/help/18/fmp/ja/index.html#page/FMP_Help%2Fediting-filemaker-file-accounts.html%23

これらの認証機能により、FileMaker カスタム App それぞれで独立したアカウント集合を管理することなく、既存の認証サーバーを利用して FileMaker カスタム App へのアクセスを制御することができます。

2.2.1. 外部サーバーアカウントによる認証（外部認証）

FileMaker カスタム App を利用する組織において、ユーザとグループに対して一元管理された認証方法 (Apple Open Directory あるいは Windows Active Directory によるドメイン認証) を使用している場合は、FileMaker Pro Advanced において、その認証サーバーに基づいてユーザグループを認証するアカウントアクセスを設定することができます。

外部サーバーアカウントによる認証を行う場合、まず、FileMaker Server に外部サーバーアカウントを使用するための設定が必要です。これは、FileMaker Server の Admin Console の「管理」タブの「外部認証」において、「外部サーバーアカウント」を有効にすることによって行います（図 2）。そして、FileMaker Pro Advanced では、FileMaker ファイルアカウントの「セキュリティの管理」で、認証サーバーに定義されているグループ名のみを設定することで、FileMaker クライアントは、外部サーバーに接続してユーザアカウントの資格情報の認証を行うことが可能になります。（図 3）。

外部サーバーアカウントの作成または編集は、FileMaker Pro Advanced の「セキュリティ」の管理のためのダイアログボックスで行います。詳しくは、FileMaker Pro 18 Advanced ヘルプ「外部サーバーアカウントアクセスの編集」⁵を参照してください。

⁵ https://fmhelp.filemaker.com/help/18/fmp/ja/index.html#page/FMP_Help%2Fediting-external-server-accounts.html%23

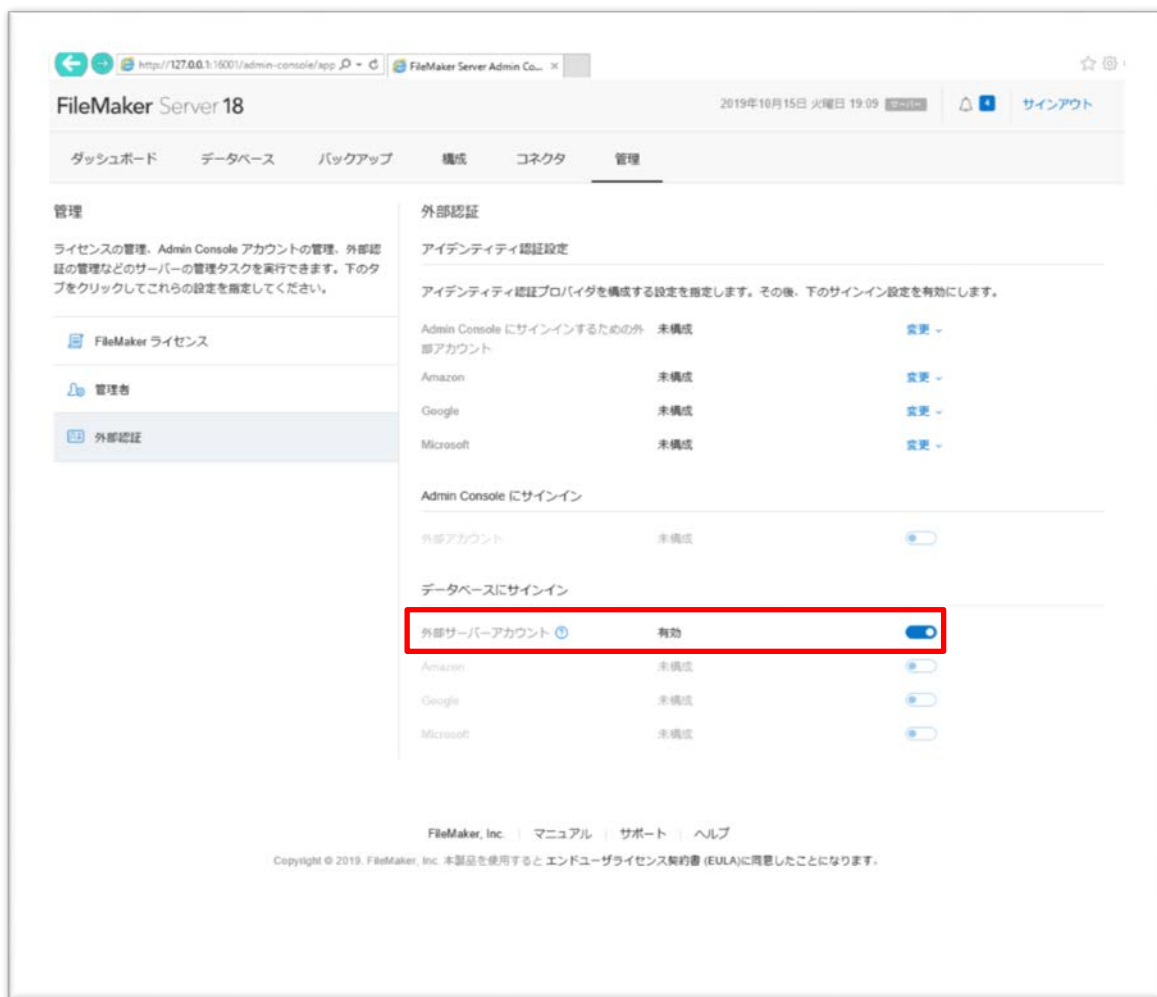
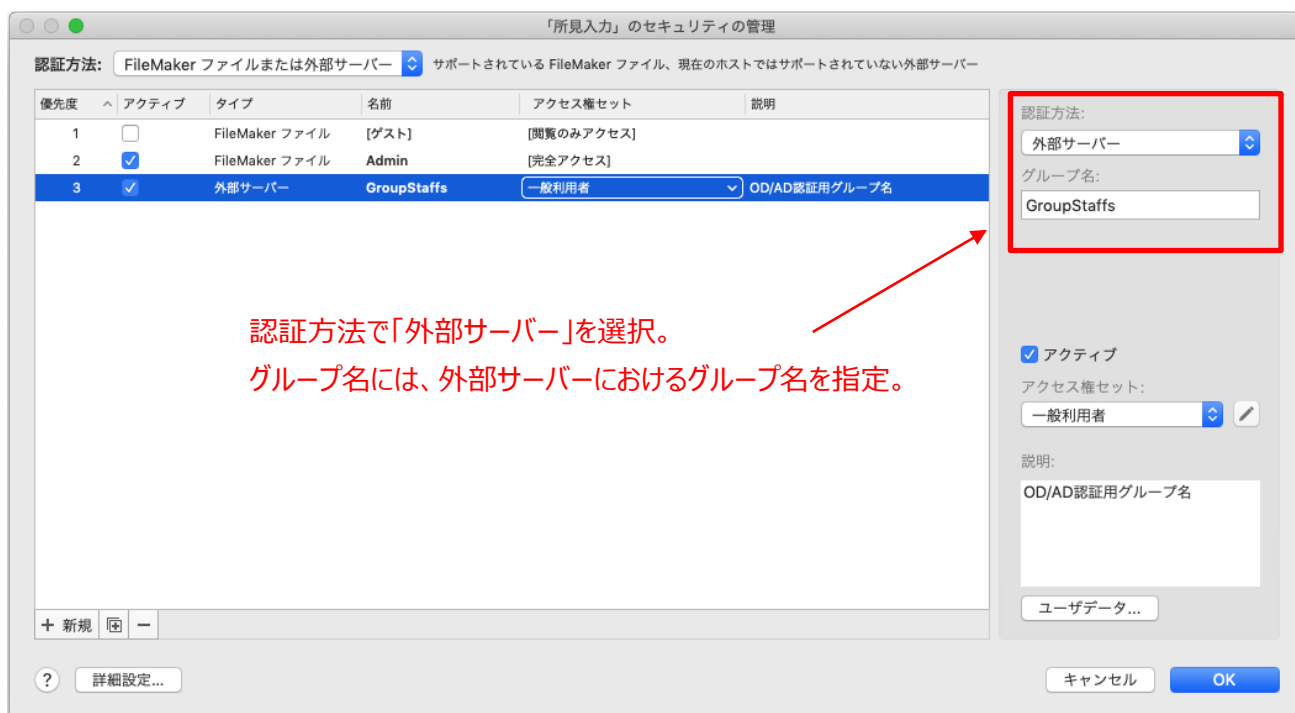


図 2 FileMaker Server Admin Console における外部サーバーアカウントによる認証設定



認証方法で「外部サーバー」を選択。
グループ名には、外部サーバーにおけるグループ名を指定。

図 3 FileMaker ファイルアカウントで外部サーバーアカウントへの認証設定

2.2.2. OAuth アイデンティティプロバイダによる認証

FileMaker Pro Advanced のファイルを FileMaker Server または FileMaker Cloud for AWS で共有する場合、OAuth アイデンティティプロバイダ (Amazon、Google、Microsoft など) でユーザを認証できます。これにより、サードパーティのアイデンティティプロバイダを使用してファイルへのアクセスを制御することができただけでなく、追加のセキュリティ対策として、多要素認証なども利用できるようになります (本資料 3.1 参照)。

OAuth アイデンティティプロバイダアカウントアクセスの作成または編集は、FileMaker Pro Advanced の「セキュリティ」の管理のためのダイアログボックスで行います。FileMaker Pro Advanced ファイルでは、外部サーバーアカウントによる認証と同様にユーザ名とグループ名のみを保存し、FileMaker クライアントは OAuth アイデンティティプロバイダに接続してユーザアカウントの資格情報を認証します。詳しくは、FileMaker Pro 18 Advanced ヘルプ「OAuth アカウントアクセスの編集」⁶を参照してください。

なお、OAuth アイデンティティプロバイダでユーザを認証するには、FileMaker Server または FileMaker Cloud for AWS の Admin Console において追加のオプションを設定する必要があります。詳しくは、FileMaker Server ヘルプ「OAuth アイデンティティプロバイダを使用する FileMaker クライアントの認証」⁷を参照してください。

2.3. FileMaker Cloud for AWS 1.18

FileMaker Cloud for AWS で FileMaker Pro Advanced のファイルを共有する場合、FileMaker Server と同様に、OAuth アイデンティティプロバイダによる認証を利用することができます。

2.3.1. OAuth アイデンティティプロバイダによる認証

OAuth アイデンティティプロバイダアクセスの概要、作成および編集については、2.2.2 を参照してください。

FileMaker Cloud for AWS でアイデンティティプロバイダを構成するには、まず、対象のプロバイダでアカウントを作成し、次に、FileMaker Cloud for AWS の Admin Console でプロバイダ情報を設定します。設定はプロバイダにより異なります。詳しくは、FileMaker Cloud for AWS ヘルプ「外部認証の設定」⁸を参照してください。

2.4. FileMaker Go 18

FileMaker Go では、利用する FileMaker カスタム App ファイルで設定されたアカウント認証に加え、iOS デバイスのパスコード、指紋認証 (Touch ID) あるいは顔認証 (Face ID) を利用することができます。FileMaker プラットフォームのアカウント認証機能と iOS のこれらの認証機能を組み合わせることによって、2 要素 (多要素) 認証を実現することができます。

2.4.1. パスワードをキーチェーンに保存する機能

⁶ https://fmhelp.filemaker.com/help/18/fmp/ja/index.html#page/FMP_Help%2Fediting-oauth-accounts.html%23

⁷ https://fmhelp.filemaker.com/help/18/fms/ja/#page/FMS_Help%2Fconfig-auth-oauth.html

⁸ <https://fmhelp.filemaker.com/cloud/18/ja/fmchelp/index.html#client-authenticate>

FileMaker Pro Advanced を使用して iOS のキーチェーンにパスワードを保存できるようにファイルを設定し、FileMaker Go でパスワードを保存することによって、保護されたファイルを開くか、またはホストに接続する場合のパスワード入力を省略することができます。詳しくは、FileMaker Pro Advanced ヘルプ「ファイルオプションの設定」⁹、FileMaker Go ヘルプ「キーチェーンを管理する」¹⁰を参照してください。

ただし、この場合は 2 要素認証によるセキュリティ強化の効果がなくなることに留意してください（図 4）。

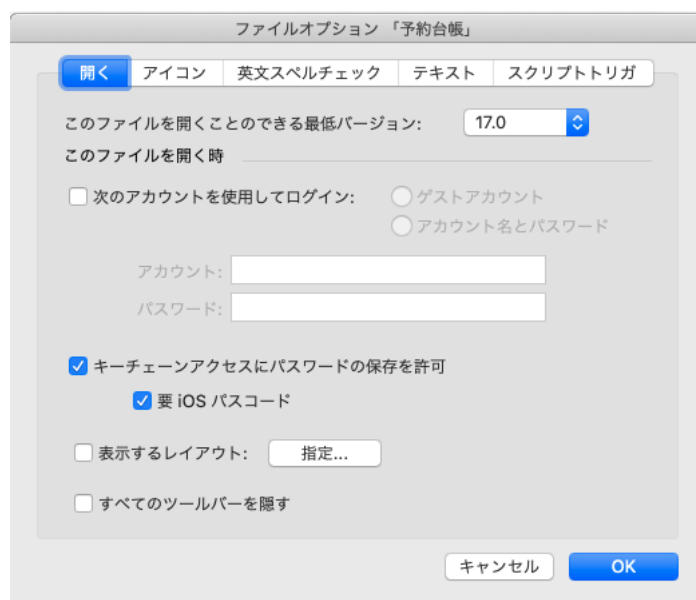


図 4 パスワードをキーチェーンに保存する機能

2.4.2. デバイスを使用した認証

FileMaker Pro Advanced のスクリプトを使用して iOS デバイスのデバイス認証を実現することができます。すなわち、FileMaker カスタム App ファイルで設定されたアカウント認証に加え、iOS デバイス認証を行うことで、事前に登録を行ったデバイスのみが FileMaker カスタム App ファイルを利用できるようになります。

デバイス認証を行うには、以下の準備とスクリプトの実装を行います。

1. デバイスを特定する情報を取得し、デバイスの登録を行う

デバイスを特定するための情報として事前に、持続 ID をデバイスから取得し、持続 ID 検証用のテーブルに、持続 ID、端末名と端末所有者等の情報をレコードとして保存します。なお、持続 ID の取得は、FileMaker Pro Advanced の「Get (持続 ID)」関数をデバイスで実行することで取得できます。

なお、通常、デバイスを特定するための値を取得するためには、「Get(システム NIC アドレス)」関数を用いますが、iOS デバイスの場合は、Media Access Control (MAC) アドレスが偽装されることを懸念し、セキュリティ強化のために、

⁹ https://fmhelp.filemaker.com/help/18/fmp/ja/index.html#page/FMP_Help%2Ffile-options.html

¹⁰ https://fmhelp.filemaker.com/help/18/fmg/ja/index.html#working-files_keychain

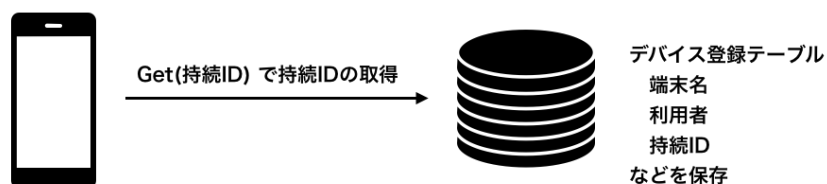
iOS によって NIC アドレスが変えられ場合があります。その前提があるため、本例では「Get (持続 ID)」関数を使用しています。

2. 認証機能の実装

カスタム App ファイルへのログイン後に、予めスクリプトトリガによって指定された、自動的に最初に実行されるスクリプト内で、現在のデバイスの持続 ID を取得し、事前に登録しておいたデバイス情報を持続 ID で検索します。検索の結果、事前に登録したデバイスが検索された場合は、カスタム App ファイルへのアクセスを許可し、デバイスが見つからなかった場合は、エラーメッセージを表示して、カスタム App ファイルを閉じます。

なお、デバイスから FileMaker Go を削除すると、デバイスから取得できる持続 ID が変わる可能性があります。

1. デバイスの登録



2. アクセス時の端末存在確認

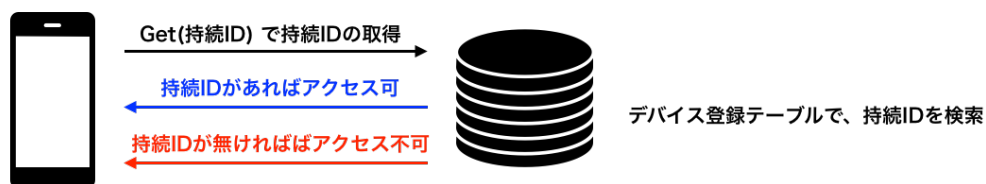


図 5 デバイス認証の手順

3. その他のユーザ認証方法

3.1. 多要素認証を利用する

FileMaker カスタム App において多要素認証を実装するには、OAuth アイデンティティプロバイダの提供する多要素認証機能を利用します。

例えば、Google アカウントの 2 段階認証プロセスを利用する場合には、あらかじめ、Google のアカウント設定において、「2 段階認証プロセスを有効にする」を開始し、次に 2 段階目の認証方法を設定します。2 段階目の認証方法には、SMS への認証コード送信や、メールによる認証プロンプトの送信など、認証方法を選択します。この設定を行うことで、1 段階目であるパスワードによる認証と 2 段階目で指定した認証方法を用いた 2 段階で行うことができるようになります。

備考： Google アカウントヘルプ「2 段階認証プロセスを有効にする」¹¹

備考： AWS Identity and Access Management ユーザーガイド「AWS での多要素認証（MFA）の使用」¹²

3.2. 他の医療情報システムのユーザ認証機能を利用する

医療機関等において、電子カルテシステム等、他の医療情報システムのユーザ認証機能を利用して FileMaker カスタム App を利用することができます。すなわち、認証後の電子カルテシステム等のメニュー画面から、FileMaker Server で共有されている FileMaker カスタム App ファイルを開くための URL を実行することで、FileMaker カスタム App ファイルを開くことができます（図 6）。

このとき、事前に電子カルテシステムと FileMaker カスタム App ファイル側の認証情報を統一し、電子カルテシステム等で使用しているアカウントとパスワードを FileMaker カスタム App ファイル側に登録しておくことによって、複数のシステムをまたがったシングルサインオンを実現するだけでなく、FileMaker カスタム App 利用における真正性を確保することができます。

一方、電子カルテと FileMaker カスタム App の認証情報を統一せずに、使用する URL に FileMaker カスタム App ファイルを開くためのアカウントとパスワードを含めて URL を生成することで、電子カルテシステム等からシームレスに FileMaker カスタム App ファイルを開くこともできます。なお、URL にアカウントとパスワードを含める場合、アカウントとパスワードが平文でネットワーク上に送信されますので、IPsec などネットワーク層における暗号化を同時に検討してください。

備考： FileMaker Pro 18 Advanced ヘルプ「URL を使用してファイルを開く」¹³

¹¹ https://support.google.com/accounts/answer/185839?hl=ja&ref_topic=2954345

¹² https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html

¹³ https://fmhelp.filemaker.com/help/18/fmp/ja/index.html#page/FMP_Help/opening-files-url.html

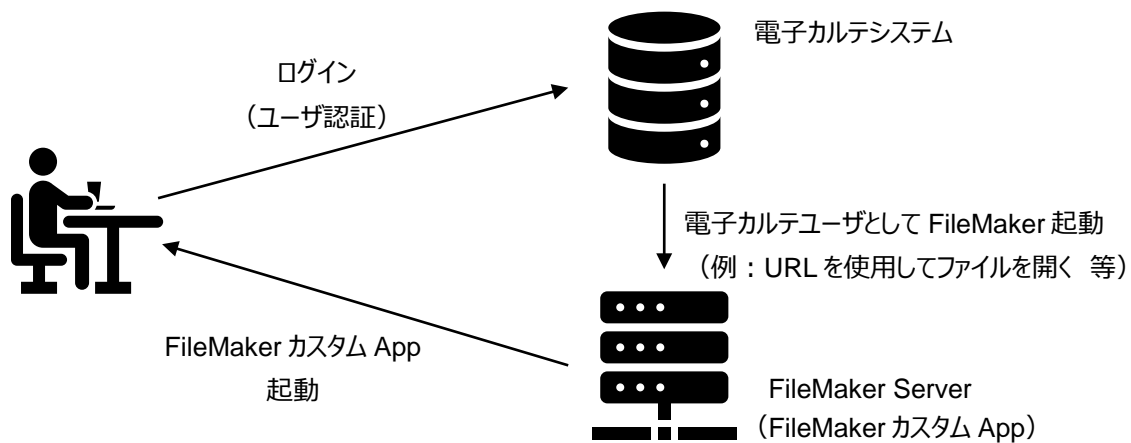


図 6 電子カルテシステムの認証機能を利用したユーザ認証の概念図

4. 留意事項

4.1. FileMaker ファイルアカウントのデフォルトアカウント

FileMaker カスタム App には、最初から「Admin」と「ゲスト」の 2 つの FileMaker ファイルアカウントが含まれていますが、セキュリティの観点からそれぞれについてユーザによる対応が必要です。

(1) 「Admin」アカウント

デフォルトで[完全アクセス]アクセス権セットが割り当てられるアカウントですが、当初はパスワードが割り当てられていません。カスタム App 利用前にまず、必ず、「Admin」アカウントにパスワードを割り当ててください。

また、「Admin」アカウントは無効にし、別の名前の管理者アカウントを作成することも検討してください。

(2) 「ゲスト」アカウント

このアカウントを使用することにより、利用者は自分のアカウント情報を入力せずに FileMaker カスタム App にアクセスできます。このアカウントには任意のアクセス権セットを割り当てることができる一方で、アカウントの削除、アカウント名の変更およびパスワードの割り当てを行うことができません。デフォルトでは、「ゲスト」アカウントは非アクティブですが、安全のため、原則として、アクティブ（有効）にしないでください。また、「ゲスト」アカウントには、データアクセスが「すべてアクセスなし」のアクセス権セットを新規に作成し、これを割り当てておくことを推奨します。

4.2. FileMaker パスワードの保存

FileMaker Pro Advanced のファイルオプションの設定によって、FileMaker アカウント、外部サーバーアカウント、OAuth のアカウントのパスワードを、Windows の資格情報マネージャ、または、macOS および iOS のキーチェーンに保存することができます。ただし、この場合、端末がログイン状態で放置されていると、第三者が FileMaker カスタム App にパスワードを入力することなくアクセスすることができるため、FileMaker カスタム App において強固なセキュリティを設定していても意味を成さなくなります。

このため、パスワードを保存する設定を行う場合には、端末から目を離すときには、ログイン状態で放置せず、OS レベルでログイン前の状態にしておくなど、運用ルールの策定が必要です。運用ルールが曖昧な場合には、パスワードを保存する設定をしないことをお勧めします。