

Tips: パスワード管理

Ver. 1.0
2019 年 10 月

概要：

- FileMaker プラットフォームでは、3 省 3 ガイドラインで要求されている初期パスワードの変更、パスワードの暗号化、パスワードの品質管理、パスワードの有効期間の設定などの機能を提供しています。
- FileMaker プラットフォーム上でさらに高度なパスワード管理を実現するために、FileMaker 関数、スクリプト、スクリプトトリガ等を利用することができます。

内容

Tips: パスワード管理	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. パスワードの秘匿管理・暗号化	1
1.3. パスワードの品質管理	2
1.4. パスワードの定期的変更と履歴管理	2
1.5. アカウント・ロック	3
1.6. その他	4
2. パスワードに関する FileMaker プラットフォームの基本機能	5
2.1. 初期パスワードの変更の強制	5
2.2. パスワードの暗号化	6
2.3. パスワードの品質管理	6
2.4. パスワードの有効期間の設定	7
3. FileMaker プラットフォームにおける高度なパスワード管理	8
4. 留意事項	8
4.1. FileMaker ファイルアカウントのデフォルトアカウント	8
4.2. FileMaker パスワードの保存	8

用語

本ドキュメントでの略称	ガイドライン
厚生省ガイドライン	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）
3 省 3 ガイドライン	（上記 3 ガイドラインをまとめている）

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として、医療情報システムの利用者識別・認証機能があります。

利用者認証を実施するためには、IDとパスワードの組合せが広く使われてきていますが、運用の便宜上、一つのIDを複数人で利用したり、容易に推測できるパスワードが長期間変更されずに使い続けられていたりするなどの誤った運用事例が散見されます。厚労省ガイドラインをはじめ、他の2ガイドラインでは、パスワードの秘匿管理、品質管理、定期的変更と履歴管理等について要求事項を挙げつつ、セキュリティ・デバイス、バイオメトリクス、ICカード等の2つ以上の独立した認証要素を用いて行う方式（2（多）要素認証）を採用することを推奨しています¹。

1.2. パスワードの秘匿管理・暗号化

利用者認証を実施するために、医療情報システムにアクセスするすべての職員及び関係者に対して、まず、個別のID及びパスワードを発行し、それを、本人しか知り得ない、又は持ち得ない状態に保つことが、3省3ガイドラインすべてにおいて求められています。

具体的には、以下に挙げるようなパスワードの秘匿管理、初期パスワードの変更、パスワードの暗号化、自動ログオンの禁止などの措置が求められています。

（パスワードの秘匿管理）

- システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはならない）。（厚労省ガイドライン）

（初期パスワードの変更）

- パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。（経産省ガイドライン）
- 利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないようにする。（総務省ガイドライン）
- 初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。（総務省ガイドライン）

（パスワードの暗号化）

- システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。（厚労省ガイドライン）
- 医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。（経産省ガイドライン）

¹ 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＞」

- パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業による閲覧を制限すること。（経産省ガイドライン）

（自動ログオンの禁止）

- パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。（経産省ガイドライン）

1.3. パスワードの品質管理

パスワードを第三者に容易に推測されないためには、一定の品質基準を設定し、これを遵守させる必要があります。各ガイドラインでは、以下のような基準を例示しています。

（品質基準の策定）

- パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実にすること。（経産省ガイドライン）
- 利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。（総務省ガイドライン）
- 作業者が医療情報システムへのログオン用パスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討することが望ましい。（経産省ガイドライン）

（品質基準）

- パスワードは（中略）、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）
- 類推しやすいパスワードを使用しないこと、（中略）。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。（厚労省ガイドライン）
- パスワードの品質基準としては、パスワードを十分に長くすること（8 文字以上等）、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。（経産省ガイドライン）
- パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8 文字以上等、十分に安全な長さの文字列等から構成されるルールとする。（総務省ガイドライン）

1.4. パスワードの定期的変更と履歴管理

パスワードを長期間変更せずに利用していると、パスワードが推測される可能性が高くなるため、3 省 3 ガイドラインにおいて以下のようなパスワードの定期的変更の強制、パスワードの履歴管理等の対策が求められています。

（定期的変更の強制）

- 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。）、（略）。（厚労省ガイドライン）
- 医療情報システムへのログイン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。（経産省ガイドライン）
- パスワードには十分な安全性を満たす有効期間を設定する。（略）（総務省ガイドライン）
- 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。（厚労省ガイドライン）

（履歴管理）

- 医療情報システムへのログイン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。（経産省ガイドライン）
- 利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するのに必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。（総務省ガイドライン）

ただし、厚労省ガイドラインでも触れられているように、パスワードの定期的な変更を強制することにより、パスワードの作り方がパターン化して簡単なものになることや、使いまわしをするようになることよって、「類推しやすいパスワードを使用しない」という要件を満たさないことになるリスクが指摘されています。

このため、総務省の「国民のための情報セキュリティサイト」では、パスワードは「定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定すること」²が求められていますが、厚労省ガイドラインでは、「しかしながら、患者情報を取り扱う医療情報システムの性格に鑑み、容易に類推できないパスワードを使用しつつ、その定期的な変更を行うことが必要である。」³としています。

1.5. アカウント・ロック

第三者が類推したパスワードを連続して試行することを防ぐため、3 省 3 ガイドラインでは以下のように、連続して一定回数のパスワード入力が失敗した場合に一定期間ログインを受け付けない対策が求められています。

- パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。（厚労省ガイドライン）
- パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。（厚労省ガイドライン）
- パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受け付けない機構とすること。（経産省ガイドライン）
- パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログインが失敗した場合は再入力を一定期間受け付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。（経産省ガイドライン）

² http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html

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＞」

- パスワード認証に係る以下のルールを実現する措置を講じる。（総務省ガイドライン）
 - ・ パスワード入力不成功に終わった場合の再入力に対して一定の不応時間を設定する。
 - ・ パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。

1.6. その他

3 省 3 ガイドラインでは、上記のような利用されているパスワード自体の管理に加え、アカウント情報を適宜棚卸して利用されていないアカウントを削除するなどの運用管理による対策の併用が求められています。

2. パスワードに関する FileMaker プラットフォームの基本機能

FileMaker プラットフォームでは、基本的に、アカウント名とパスワードの組合せを使用してユーザを認証します。このユーザ認証には、以下に示す 3 種類のアカウントを利用できます。

- 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

これらのアカウントの詳細については、FileMaker Pro Advanced のヘルプや、FileMaker 利用リファレンス添付の「Tips：ユーザ認証」を参照してください。

以下、FileMaker プラットフォームにおけるパスワード管理について簡単に紹介します。詳しくは、FileMaker Pro 18 Advanced ヘルプを参照してください。

2.1. 初期パスワードの変更の強制

「FileMaker ファイルアカウント」を利用する場合、アカウント作成時に管理者が設定した一時的なパスワードを、次回サインイン時に利用者自身が変更できるようにすることができます。

次回サインイン時にパスワード変更を要求するには、FileMaker Pro Advanced の「セキュリティ」の管理ダイアログボックスにおいて、「次回サインイン時にパスワード変更を要求」を選択（チェック）します（図 1）。

詳しくは、FileMaker Pro Advanced ヘルプ「FileMaker ファイルアカウントの編集」を参照してください⁴。

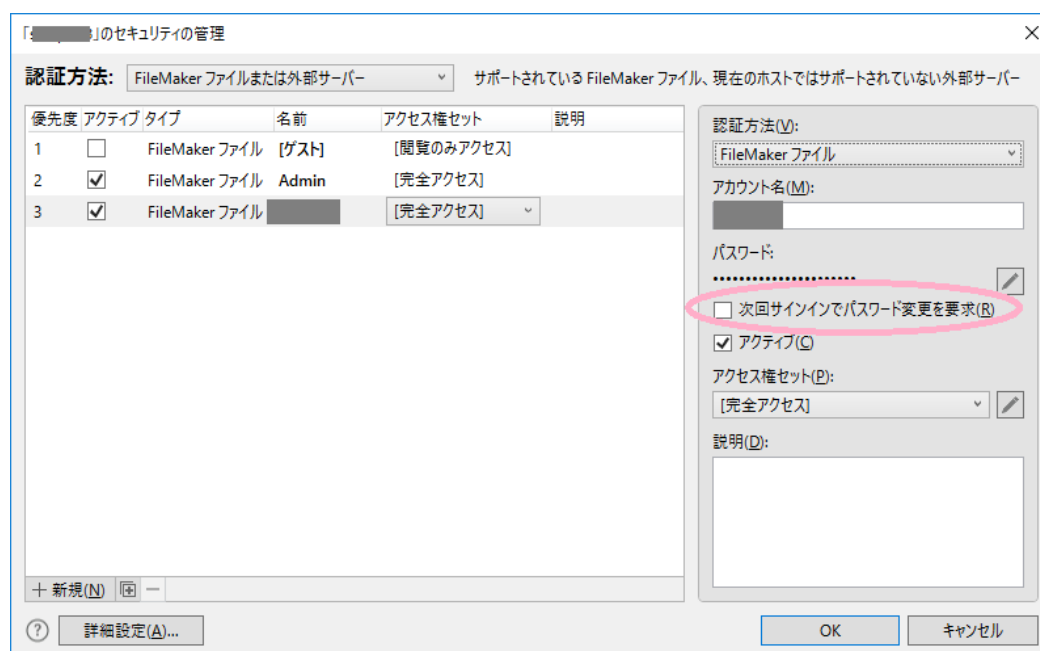


図 1 FileMaker Pro Advanced での初期パスワード変更の設定画面

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

Active Directory 等を用いた「外部サーバーアカウント」を使用している場合は、初回のサインイン時にユーザーにパスワードの変更を要求することができます。詳しくは、組織の Active Directory 管理者に確認して下さい。

なお、OAuth アイデンティティプロバイダを使用した外部認証の場合、事前に取得したアクセストークンを使用して OAuth アイデンティティプロバイダに認証を委ねるため、FileMaker Pro Advanced 側からは初期パスワードの変更を強制することはできません。

2.2. パスワードの暗号化

「FileMaker ファイルアカウント」を利用する場合、パスワードは一方方向ハッシュにより暗号化されて FileMaker カスタム App ファイル内に保存されます。また、FileMaker Server あるいは FileMaker Cloud for AWS の Admin Console のパスワードも同様に、一方方向ハッシュにより暗号化されます。

FileMaker プラットフォームで使用される暗号化の種類については、FileMaker 18 セキュリティガイド「FileMaker で使用される暗号化の種類」⁵を参照してください。

なお、Active Directory 等を用いた「外部サーバーアカウント」を利用する場合、暗号化ハッシュによりパスワードは保護されているため、FileMaker プラットフォームでは、パスワードの暗号化に関して措置を講じる必要はありません。また、OAuth アイデンティティプロバイダを使用した外部認証を行う場合は、OAuth アイデンティティプロバイダによって保護されているアカウントとパスワードの組み合わせを使用するため、FileMaker プラットフォームでは、パスワードの暗号化に関して措置を講じる必要はありません。

2.3. パスワードの品質管理

「FileMaker ファイルアカウント」もしくは「外部サーバーアカウント」を利用する場合、パスワードには、a ～ z、A ～ Z、0 ～ 9、および「!」や「%」などの ASCII 文字だけが使用できます。アクセント記号付きの文字や、半角英数字以外の文字 (キリル文字や日本語など) が含まれるパスワードは使用できない場合があります。これは特に、異なるプラットフォームでのデータベースソリューションや、FileMaker WebDirect でアクセスされるファイルの場合に問題になります。

パスワードでは、大文字と小文字が区別されます。たとえば、「zFootBall2」というパスワードが設定されている場合、「zfootball2」と入力するとログイン失敗になります。アカウントのパスワードを入力する場合、キーボードの Caps Lock キー (Windows) または caps lock キー (OS X) が誤って有効になっていないことを確認してください。

なお、「FileMaker ファイルアカウント」を利用する場合、パスワードを設定する際にパスワードの質 (「弱」「中」「強」) が計算されて表示されるので (図 2)、利用者が強度の高いパスワードを設定する助けとなります。

⁵ <https://fmhelp.filemaker.com/docs/18/ja/security/index.html#types-encryption>

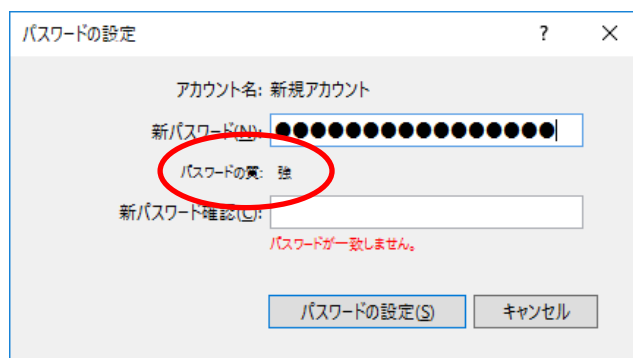


図 2 FileMaker ファイルアカウントのパスワード設定画面

Active Directory 等を用いた「外部サーバアカウント」を利用する場合、Active Directory 側に設定されているパスワードのポリシーによって、パスワードの複雑度合いが変わります。また、OAuth アイデンティティプロバイダを利用する場合、FileMaker プラットフォームに対応した、OAuth アイデンティティプロバイダごとにパスワードポリシーが設けられています。FileMaker プラットフォームから、「外部サーバアカウント」あるいは、「OAuth アイデンティティプロバイダアカウント」を利用したサインインを行う場合は、それぞれに設定されているパスワードポリシーに従うことになります。

2.4. パスワードの有効期間の設定

「FileMaker ファイルアカウント」を利用する場合、パスワードの変更を要求する間隔を設定することができます。

パスワードの変更要求の設定は、アクセス権セットの設定で行います。「変更を要求する間隔(C):」の項目に、何日ごとに変更要求を行うか、日数を数字で指定します（図 3）。

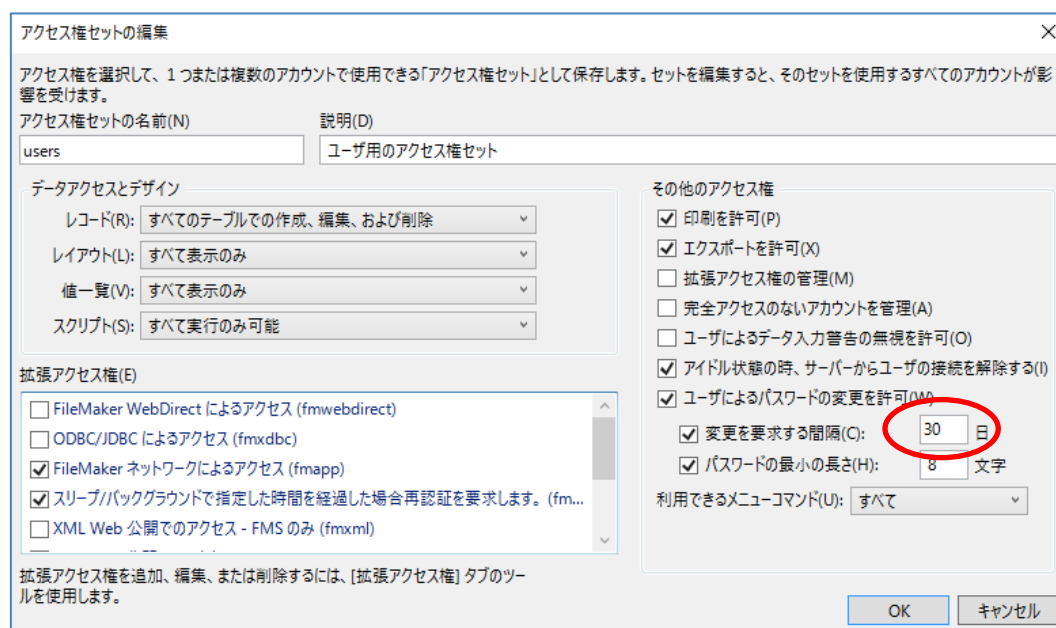


図 3 パスワードの変更を要求する間隔の設定

3. FileMaker プラットフォームにおける高度なパスワード管理

FileMaker 関数、スクリプト、スクリプトトリガ等を利用することにより、パスワード管理に関する FileMaker プラットフォームの基本機能（2 章）に加え、パスワードの品質評価や履歴管理などの高度な管理が可能となります。

例えば、アカウントとパスワードを管理するテーブルを作成し、アカウントごとに過去に設定したパスワードの履歴を保存することができます。このとき、利用者がスクリプトによって制御されたパスワード変更機能を利用してパスワードの変更要求を行うと、該スクリプトは、パスワード管理用テーブルに保存された現在のアカウントに関する過去のパスワード履歴と新たに設定されたパスワードとを比較します。そして、過去の使用したことのあるパスワードと同じパスワードが指定されたことを検出した場合、利用者に通知を行い、新たなパスワードを要求することができます。

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、念のため、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、何らかの手段あるいはタイミングで第三者が 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 のセキュリティ強度が弱まることになります。

このため、特に差し迫った必要がない場合には、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。