オンラインイベント

Claris FileMaker Server で多要素認証を導入するには

松尾 篤

セッション ID：
T-22

松尾 篤

株式会社エミック

自己紹介

Claris FileMaker CERTIFIED DEVELOPER

kintone CERTIFIED Associate 2020

kintone CERTIFIED App Design SP 2020

kintone CERTIFIED Customization SP 2020

- 松尾篤
  - 株式会社エミック（東京都杉並区）代表取締役社長
  - Claris FileMaker 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）
  - kintone認定 カスタマイズスペシャリスト（2020年3月）

株式会社エミック

- Claris FileMaker 対応ホスティングサービスを 1998 年から提供
- 定額制オンライン対面開発サービス
  - WordPress を利用した Web アプリ開発
  - 各種クラウドサービスとの連携の設計および設定

https://www.emic.co.jp/

今回の話題

- 安全性を向上する多要素認証
- Claris FileMaker Server と多要素認証
- Keycloak を用いた多要素認証の導入

Demo

安全性を向上する多要素認証

クラウドサービスのセキュリティ

- 基本は ID およびパスワードによる本人認証方式
- 近年ではより安全性を向上できる多要素認証も普及

不正ログイン防止策

- 強固なパスワードの設定と適切な管理
  - できるだけ長く
  - 複雑で
  - 使い回さない
- 多要素認証の設定を有効にする

多要素認証（MFA）

- MFAはMulti-Factor Authenticationの略
- 認証の3要素のうち2つ以上の要素を用いた方式の認証
  - 要素が2つの場合は2要素認証と呼ばれることも

認証の3要素

要素	概要	例
記憶情報	本人のみが記憶しているデータを用いて利用者を認証する方法	暗証番号 パスワード PIN コード
所持情報	本人のみが所持している物によって利用者を認証する方法	キャッシュカード スマートフォン ハードウェアトークン
生体情報	本人の生体に基づくデータにより利用者を認証する方法	静脈 指紋 顔

Claris FileMaker Cloud の場合

- Claris ID では 2 ステップ検証の設定が可能
  - 有効化するとサインイン時にパスワードと検証コードの入力が必要に
  - 検証コードはテキストメッセージとして設定した電話番号に送信される

Claris FileMaker Server と多要素認証

FileMaker Server と多要素認証

- FileMaker Server で共有されているカスタム App には Claris ID によるサインインは不可（Claris ID の 2 ステップ検証プロセスは利用不可）
- OAuth アイデンティティプロバイダ認証を有効化した場合に多要素認証に対応可能

FileMaker Server & OAuth

- バージョン 16 以降の FileMaker Server で OAuth に対応
- OAuth アイデンティティプロバイダの資格情報を使用してカスタム App にサインインできるように設定可能

FileMaker Server & OAuth

- サポートされている定義済み OAuth アイデンティティプロバイダ
  - Amazon
  - Google
  - Microsoft
  - AD FS

FileMaker Server & OAuth

- バージョン 19.4 以降ではカスタム OAuth アイデンティティプロバイダにも対応可能
- 動作確認済みのカスタム OAuth アイデンティティプロバイダ
  - Okta、Ping、OneLogin、Auth0、LinkedIn

参考

- FileMaker Server の外部認証に対応したカスタマイズ可能な OAuth アイデンティティプロバイダ（Claris ナレッジベース）

  https://support.claris.com/s/answerview?anum=000035893&language=ja

今回は Keycloak を紹介

- 標準で多要素認証に対応
- オープンソースソフトウェアであり自社で管理・運用することも可能

Keycloak を用いた多要素認証の導入

Keycloak

- オープンソースのアイデンティティ・アクセス管理ソフトウェア
  - 標準で多要素認証に対応
  - オープンソースソフトウェアであり自社で管理・運用することも可能
  - グループでの認証にも対応しているためアカウント管理の手間を軽減可能

Keycloak の設定準備

- Keycloak の管理者ユーザーを作成
- 管理者ユーザーで Keycloak の管理コンソールにサインイン
- ［Realm settings（レルムの設定）］＞［Localization］でデフォルト・ロケールを日本語に変更可能

Keycloak 設定の流れ

- レルムを追加
- クライアントを追加
- クライアント・スコープの設定
- グループを追加
- ユーザーを追加

Keycloak における用語

用語	説明
レルム	Keycloak における管理単位（用途に応じてレルム単位で定義／はじめから定義されているmasterレルムとは別のレルム［FMS］を作成）
クライアント	認証・認可サーバーである Keycloak のサービスを利用するアプリケーション
クライアント・スコープ	複数のクライアントで共通のマッピング設定を保持するための仕組み （ FileMaker Server のカスタム IdP 認証でグループによる認証に対応させる場合に必要）

Keycloak でクライアントを作成（設定例）

- Client type ： OpenID Connect
- クライアント ID ： filemaker-server（デモの設定例）
- クライアント認証：オン
- Authentication flow：「Direct access grants」のチェックを外す

Keycloak でクライアントを作成（設定例）

- 有効なリダイレクト URL
  - https://filemaker-server.emic.co.jp/oauth/redirect（デモの設定例）

FileMaker Server での設定

- FileMaker Server Admin Console で外部認証の設定を行う
  - Admin Consoleの［管理］>［**外部認証**］において［**カスタム IdP 認証設定**］>［**カスタム OAuth**］にある［変更］をクリック

FileMaker Server Admin Console の設定例

カスタム IdP 認証設定項目	エンドポイントのパスおよび設定内容
認証コードエンドポイント	/realms/FMS/protocol/open-id/auth
認証トークンエンドポイント	/realms/FMS/protocol/open-id/token
認証プロファイルエンドポイント	/realms/FMS/protocol/open-id/userinfo
カスタム IdP ユーザアカウントスキーマ	email
カスタム IdP ユーザグループスキーマ	groups
範囲	openid groups email
種類	OpenID Connect（OIDC）

FileMaker Server での設定

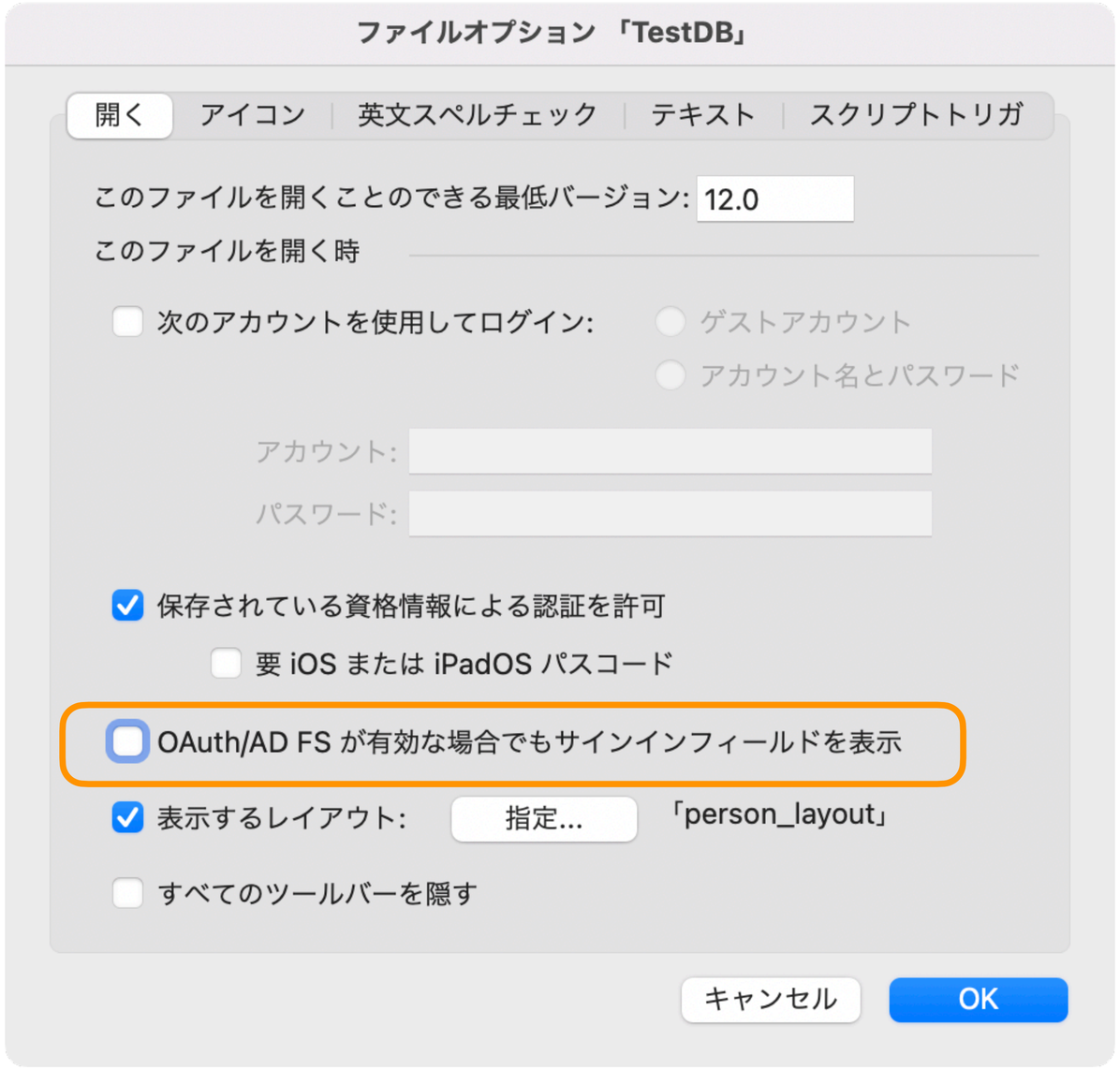
- Admin Consoleの［管理］>［外部認証］において［**データベースにサインイン**］＞［**外部サーバーアカウント**］を「有効」に変更
  - さらに［**Keycloak**］（入力したカスタム IdP 名）を有効に変更

FileMaker Pro での設定

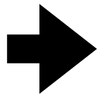
- ［ファイル］メニュー＞［管理］＞［セキュリティ...］において［認証方法］を「**カスタム OAuth**」に変更
  - グループを新規追加（グループまたはユーザで「**グループ**」を選択）
    - グループ名にKeycloakで設定した**グループ名**を入力
    - アクセス権セットは専用のものを作成して割り当てることを推奨

FileMaker Pro での設定

- FileMaker Pro 19.2.2でOAuthでサインインする際にアカウント名およびパスワードフィールドが表示されないように
  - ［ファイル］メニュー＞［ファイルオプション...］の［**OAuth/AD FS が有効な場合でもサインインフィールドを表示**］オプションで調整可
  - Shiftキー（Windows）またはoptionキー（macOS）を押しながらファイルを開く方法でもサインインフィールドを一時的に表示可


ファイルオプション 「TestDB」
開く
アイコン
英文スペルチェック
テキスト
スクリプトトリガ
このファイルを開くことのできる最低バージョン: 12.0
このファイルを開く時
次のアカウントを使用してログイン:
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:
パスワード:
保存されている資格情報による認証を許可
要 iOS または iPadOS パスコード
OAuth/AD FS が有効な場合でもサインインフィールドを表示
表示するレイアウト:
指定...
「person_layout」
すべてのツールバーを隠す
キャンセル
OK


「TestDB」を開く
filemaker-server.emic.co.jp
サインインして「TestDB」を開きます。
Keycloak
?
キャンセル




「TestDB」を開く
filemaker-server.emic.co.jp
サインインして「TestDB」を開きます。
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
または次を使用してサインイン:
Keycloak
?
キャンセル
サインイン

Keycloak で OTP を用いた多要素認証を構成

- Keycloak は標準で OTP（ワンタイムパスワード）を用いた多要素認証に対応
  - ［認証］＞［Browser］＞［**Browser - Conditional OTP**］の設定を「Conditional」から「Required」に変更すると多要素認証を必須化

まとめ

まとめ

- 近年ではより安全性を向上できる多要素認証が普及
- FileMaker Server では OAuth アイデンティティプロバイダ認証を有効化した場合に多要素認証に対応可能
- オープンソースの認証・認可サーバーである Keycloak を用いて多要素認証に対応させることも可能に