OpenAM
コンソーシアム

2021年度
openam-dev
活動報告

アジェンダ

- コンソーシアム版 OpenAM 開発状況
  - OpenAM 開発
  - Web Agent 開発
  - コミュニティサイト

OpenAM 15 開発

状況	バージョン情報を15.0.0-SNAPSHOT として次バージョンの開発中。
実施内容	◘ セキュリティ FIX（2件） ◘ Node.js のアップデート ◘ Nightly Build 対応（対応中）
今後の予定	◘ 3～4 年のスパンで開発を想定 ◘ 新規機能の検討・開発 ➢ DevOps 推進 ➢ プロトコルの更新への追随（OAuth/OIDC/WebAuthn） ➢ REST API の拡充と XUI 化 ➢ ライブラリのアップデート・排除 ➢ OpenJDK 17 (次期 LTS 版) 対応 ➢ OGIS・OSSTech の独自機能の移行

OpenAM 開発 ー セキュリティFIX

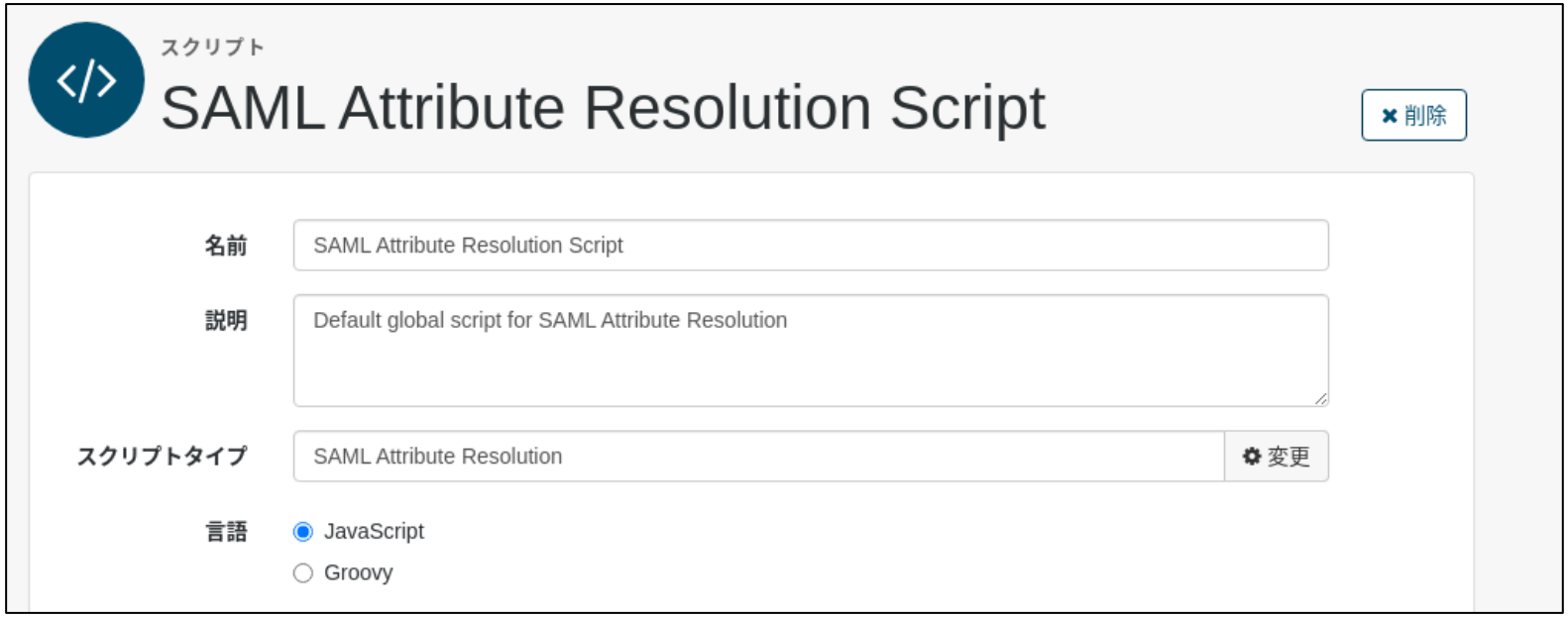
- CVE-2021-4201
  - アクセス制御の不備
  - セッションハイジャック攻撃に利用される恐れがある
- CVE-2022-31735
  - オープンリダイレクトの脆弱性
  - OpenAM コンソーシアムとして脆弱性を JPCERT/CC に報告して採番された CVE

OpenAM 開発 ーNightly Build 対応

- 現状ではコンソーシアムで提供しているバイナリーは14.0.0のリリース版のみ
- 最新のコードによるバイナリーを入手でいたほうが開発者と利用者共にメリットがある
- GitHub の CI 機能を利用した仕組みを準備中

OpenAM 開発 ー 開発中の機能 (1)

- SAML 属性や NameID 値をスクリプトで書く機能
  - 既存に存在する OpenID Connect のクレームスクリプトのように SAML 属性をスクリプトで加工する機能



OpenAM 開発 － 開発中の機能 (2)

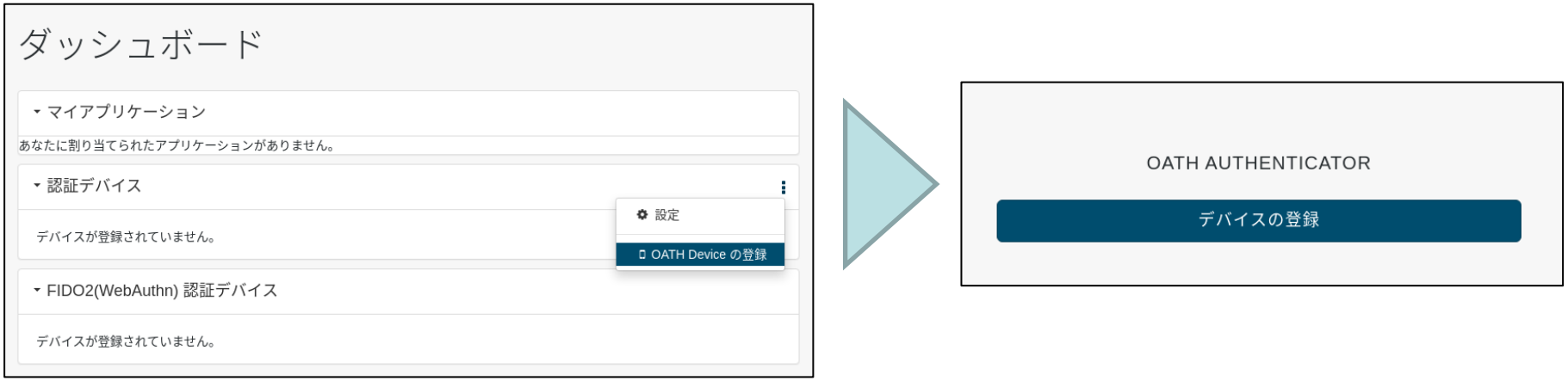
- SAML の属性送信の同意機能
  - SP に送信する属性情報についてユーザーに同意を求める機能

OpenAM 開発 － 開発中の機能 (3)

- OAuth のグラントタイプを制御する機能
  - リソースオーナーパスワード等の利用を想定していないグラントタイプを無効化することができる

OpenAM 開発 ー 開発中の機能 (4)

- OATH デバイスをダッシュボードから登録・再登録する機能
  - 初回ログイン時のみメール OTP、次回以降はデバイス OTPを使うような運用が可能
  - また、機種変更後に新しいスマホに鍵を登録できる



OpenAM 開発 ー 開発中の機能 (5)

- reCAPTCHA v3 認証
  - ID・PW認証に reCAPTCHA v3 によるボット判定機能を追加できる
  - ボット判定時に OTP を求めたり認証を失敗させることができる

OpenAM 開発 ー 開発中の機能 (6)

- その他のエンハンス
  - LDAP サービスにセカンダリー LDAP サーバーの設定項目を追加
  - SAML の NameID 値マップの設定項目を IdP だけでなく SP にも追加
  - SAML のホストプロバイダー作成時にベース URL の入力欄を追加
  - OpenID Connect Dynamic Client Registration を無効化するオプションの追加

Agent 4.2 開発開始

状況	これまでコンソーシアム版として OpenAM を対象としてきた。 新たに Web Agent もフォークし、開発を開始した。 https://github.com/openam-jp/web-agents
実施内容	今年度は進捗無し。
今後の予定	OGIS、OSSTech のパッチをマージして 4.2.0 としてリリース予定。

コミュニティサイトの作成

状況	GitHub Pages でコミュニティサイトを作成。 https://openam-jp.github.io/ja/ 現時点のコンテンツはOpenAM 14のリリース時に GitHub wiki で公開した内容（リリースノートや新機能の説明など）。
実施内容	今年度は進捗無し。
今後の予定	コンテンツを拡充していく。新機能を追加した際に利用手順等を追加する。

https://www.openam.jp/