

**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	<ul style="list-style-type: none"><li>❑ セキュリティ FIX (2件)</li><li>❑ Node.js のアップデート</li><li>❑ Nightly Build 対応 (対応中)</li></ul>
今後の予定	<ul style="list-style-type: none"><li>❑ 3~4年のスパンで開発を想定</li><li>❑ 新規機能の検討・開発<ul style="list-style-type: none"><li>➢ DevOps 推進</li><li>➢ プロトコルの更新への追随 (OAuth/OIDC/WebAuthn)</li><li>➢ REST API の拡充と XUI 化</li><li>➢ ライブラリのアップデート・排除</li><li>➢ OpenJDK 17 (次期 LTS 版) 対応</li><li>➢ OGIS・OSSTech の独自機能の移行</li></ul></li></ul>

## ◆ OpenAM 開発 – 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 – 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して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 – 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

スクリプト

### SAML Attribute Resolution Script ✕ 削除

名前

説明

スクリプトタイプ  ⚙️ 変更

言語  JavaScript  
 Groovy

## ◆ 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

送信先のサービス: 属性同意機能テスト用 SP

 OSSTech

テスト用のSPです。このSPはOpenAMで構築されています。

送信する情報	
ID	test1
電話番号	08012345678
メールアドレス	test1@example.co.jp

続行すると、上記の情報がサービスに対して送信されます。このサービスにアクセスするたびに、情報を送信することに同意しますか？

次回送信時にもう一度確認する。

このサービスに送信する属性が変更された場合、もう一度確認する。

連携している全てのサービスに対して全ての属性の送信を許可し、今後この画面を表示しない。

## ◆ 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



サービス  
OAUTH2 プロバイダ ✕ 削除

Use Stateless Access & Refresh Tokens  ⓘ

認可コードの有効期間(秒)  ⓘ

リフレッシュトークンの有効期間(秒)  ⓘ

アクセストークンの有効期間(秒)  ⓘ

グラントタイプ  ⓘ

## ◆ OpenAM 開発 – 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 – 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 へのサインイン

ユーザー名

パスワード

ログイン

 プライバシー  
利用規約

## ◆ OpenAM 開発 – 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。  <a href="https://github.com/openam-jp/web-agents">https://github.com/openam-jp/web-agents</a>
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。  <a href="https://openam-jp.github.io/ja/">https://openam-jp.github.io/ja/</a>  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。

OpenAM  
コンソーシアム

<https://www.openam.jp/>