今更聞けない認証関連OSSの話 ～クラウド移行の観点も含めて～

OSS コンソーシアム　BA＆教育ソリューション部会
オープンソース・ソリューション・テクノロジ株式会社

ビジネス＆教育ソリューション部会

OSS Consortium

- OSSビジネスアプリケーションの積極的な普及啓蒙活動を行うことにより、各ビジネスアプリケーションの繁栄を図り、OSSの普及にも貢献する。

2018年：部会紹介パンフレットとして
参加企業の合同紹介チラシの作成

2019年：OSCへの出展
Scratchを利用した
ドローンプログラミングの紹介

現在作成中…

2020年度：部会参加企業の
製品紹介コンテンツ動画の作成

会社紹介

- オープンソース・ソリューション・テクノロジとは
  - 『認証』関連OSSに特化したソフトウェア会社
    - 認証OSSを商用Linux上で動作するようパッケージとして提供
    - 認証OSSの保守
    - システム導入の際の認証・シングルサインオンを支援

独自改良を加えたOSS製品のパッケージ提供

OpenLDAP
SAMBA
OpenAM

自社製品の

サポートサービス

製品問い合わせ窓口

脆弱性アナウンス

パッチの作成・提供、等

自社製品の設計・導入や

認証関連コンサルティング

・シングルサインオン

・統合認証

・LDAPデータ移行

OSSTech製品年表

2006 2008 2010 2014 2017 2020

SAMBA
OpenLDAP

Samba 4
OpenLDAP

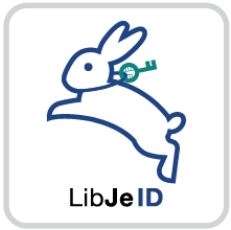
UNIX上でのNTドメイン、Active Directory実現や商用サポートが得られるLDAPサービス

OpenSSO OpenAM

クラウドの発展に合わせたシングルサインオン需要の加速

LibJeID

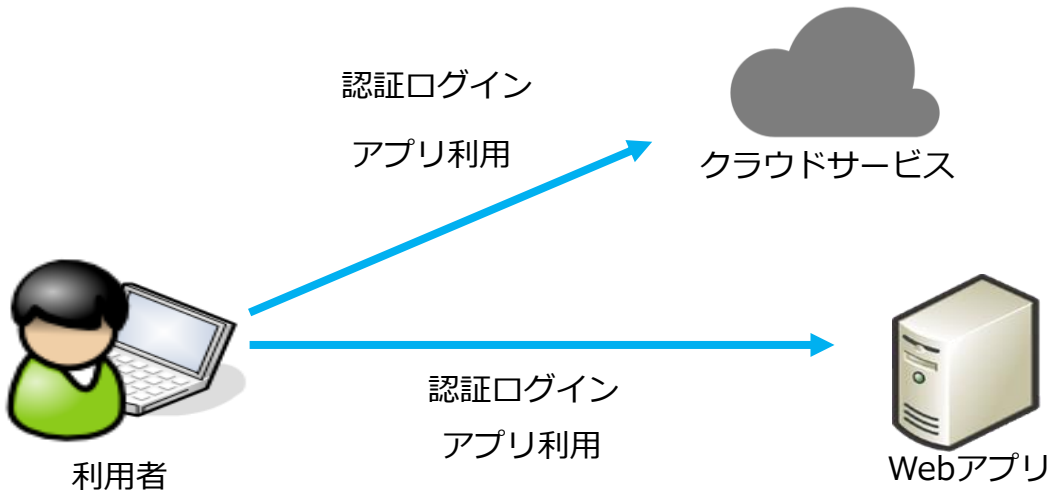
本人確認ビジネスの普及



今更聞けないシングルサインオンの話
＋
“企業ITのクラウドマイグレーションとOSSの役割”

シングルサインオンがない環境

- 組織内に存在する様々なWebアプリ、クラウドサービスに個別に認証している状態

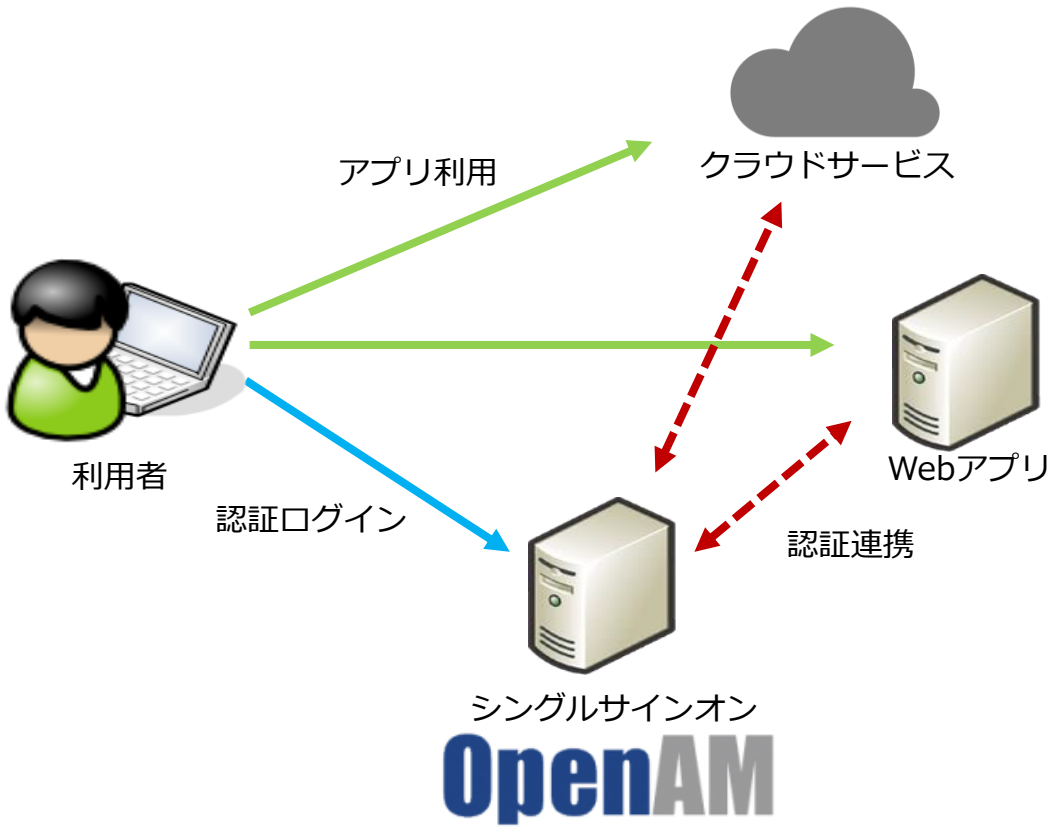


- 覚えるID/パスワードが増える
  - 付箋メモ、簡単なパスワードの使いまわし、紛失等のリスク増加

- 個々に認証処理を検討する必要がある
- クラウドサービスが増えるほどパスワードを管理する箇所が増える

シングルサインオン（SSO）とは

- クラウド、オンプレミスを問わずシステムで混在する認証を一元化し、一度の認証ですべてのシステムの利用を可能にする仕組み



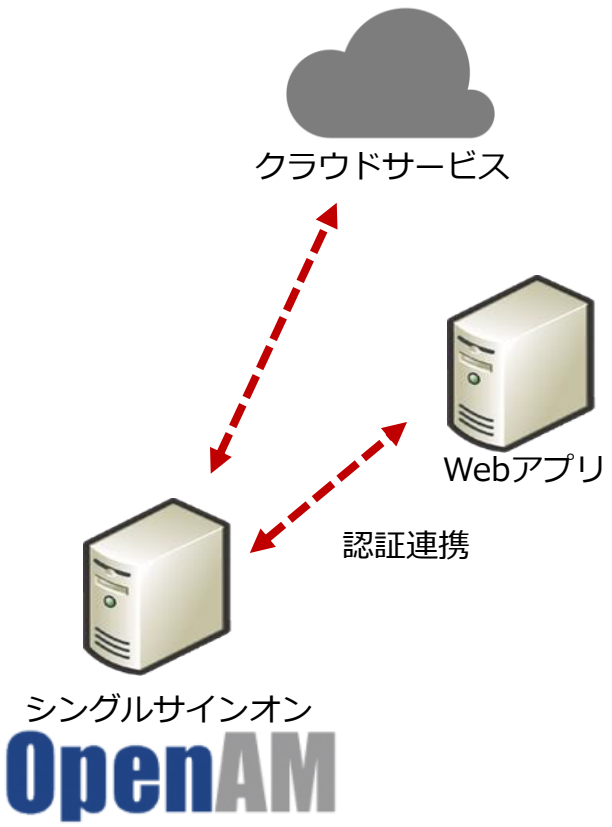
利用者

- 覚えるID/パスワードは一つだけ！
  - 生態認証等を利用することでパスワードレスでの認証も実現可能

管理者

- 高度な認証方式を採用しやすい
  - 多要素認証、生態認証
- 認証連携の方法によっては、クラウド側にパスワードを持たせずに済む

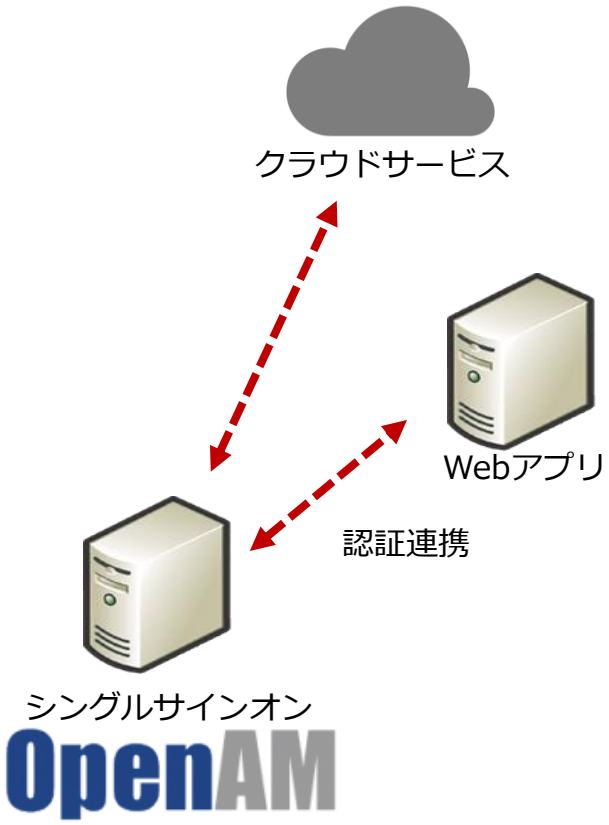
主だった認証連携の方法

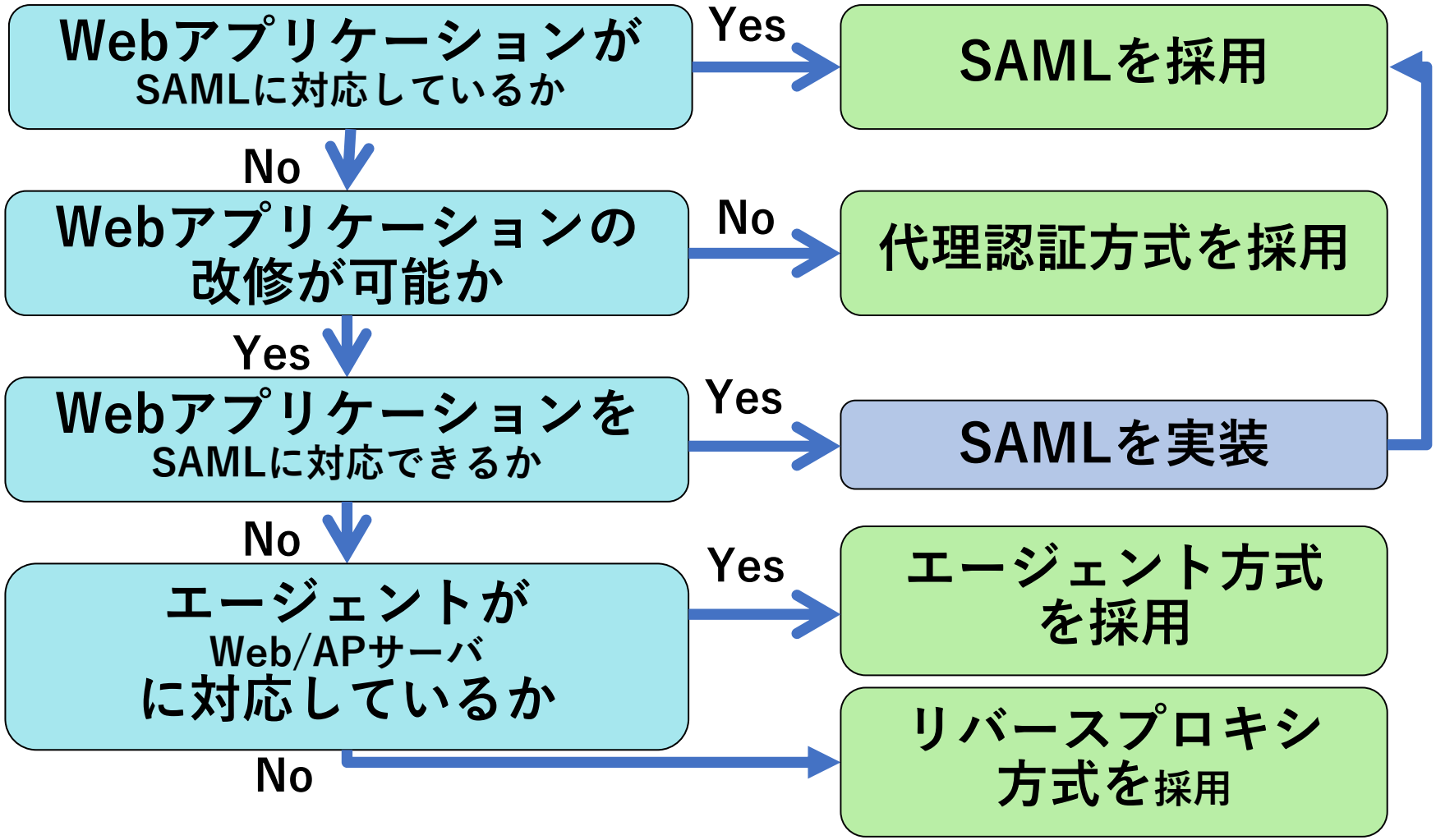


認証連携方式	セキュリティ	特徴
SAML、OpenID Connect（フェデレーションプロトコル）	高	• 業界標準のフェデレーションプロトコルであるSAML(Security Assertion Markup Language)を用いた実装形式(OpenID ConnectやOAuthにも対応可能) • Office365, G suite(旧Google Apps), Salesforce等のSAMLに対応しているクラウドサービスやWebアプリケーションとの連携等で利用
エージェント、リバースプロキシ（HTTPヘッダ）	高	• Policy Agentと呼ばれる認可を行うためのモジュールをSSO対象のサーバに導入する実装形式 • SSO対象のサーバにモジュールの導入などが困難な場合、Policy Agentを導入したリバースプロキシを用いて実装可能
代理認証	低*	• 上記2つの形式での実装が困難な場合に利用する実装形式 • OpenAMから得た認証情報をSSO対象のサーバにPOSTすることでSSOを実施(Basic認証、FORM認証に対応)

※ 認証情報を保持する箇所が増えるため

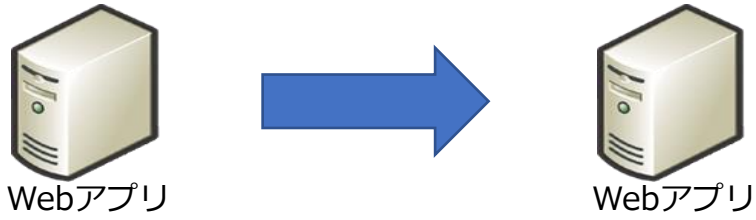
認証連携方式の適用チャート



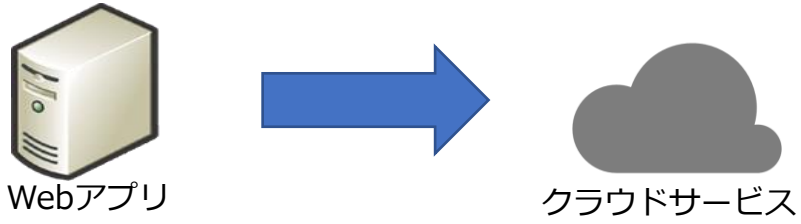


クラウド移行すると…？

- IaaS, PaaS等で移行する場合



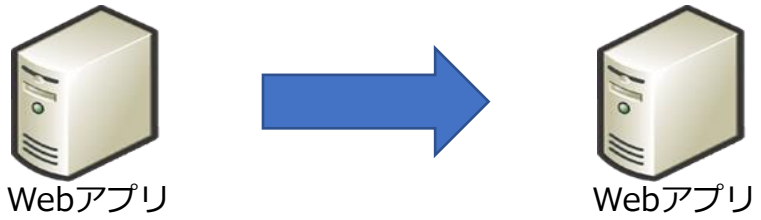
- SaaSに移行する場合



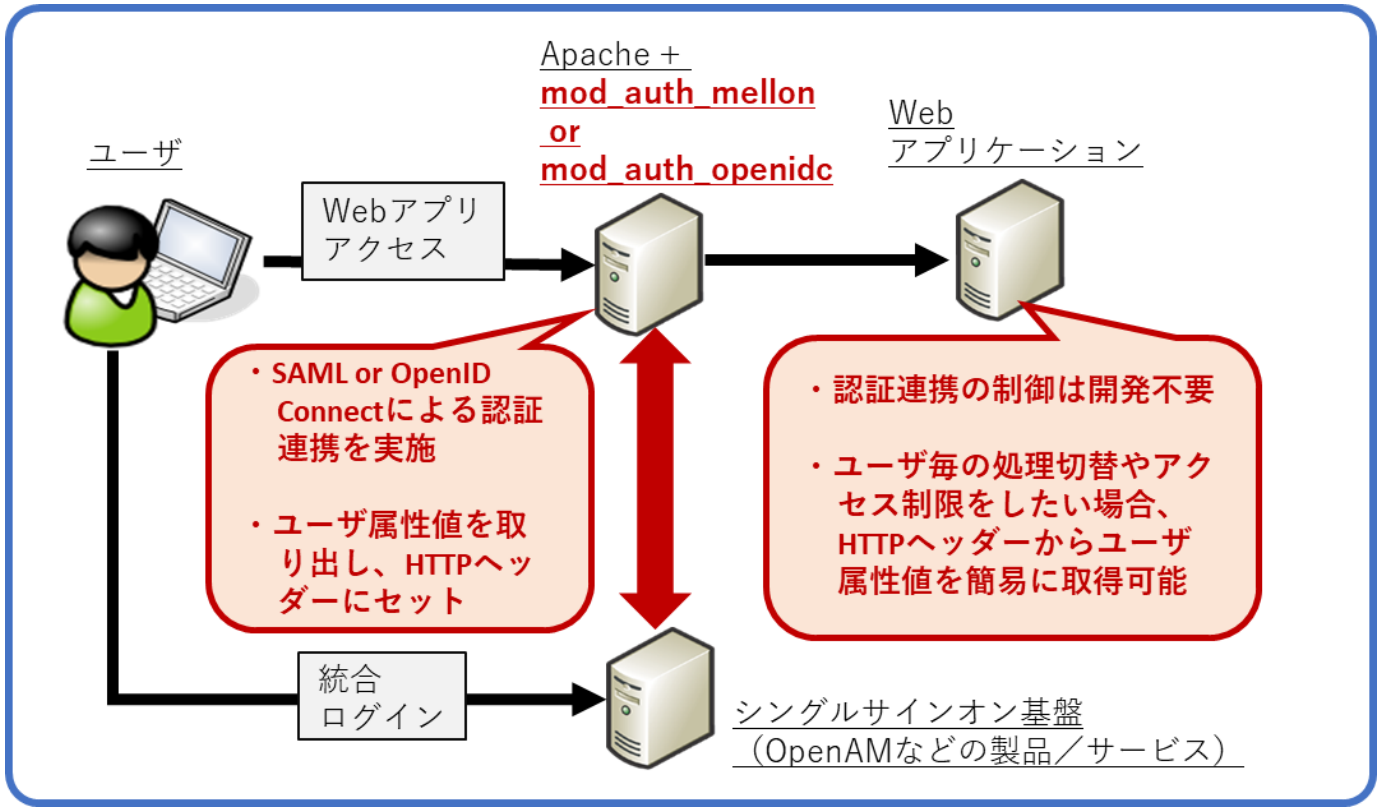
IaaS, PaaSの場合

- IaaS, PaaS等で移行する場合

mod_auth_mellon
mod_auth_openidc

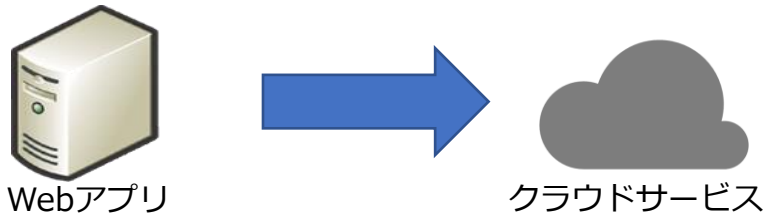


現行の認証連携方式を踏襲
or
フェデレーションプロトコル対応



SaaSの場合

- SaaSの類似サービスへ移行する場合



連携方式の再検討が必須
＋
代理認証はしない！

代理認証の流れ

クラウドサービスのログインUIが
突然変わるかもしれない

- Webアプリのログイン画面を検知
- ログインしていない場合、
  認証に必要な情報（ID/パスワード）を応答

通信が暗号化されていてもパスワードを
NWに何度も流さない方がいい

ハイブリッドクラウドへの対応

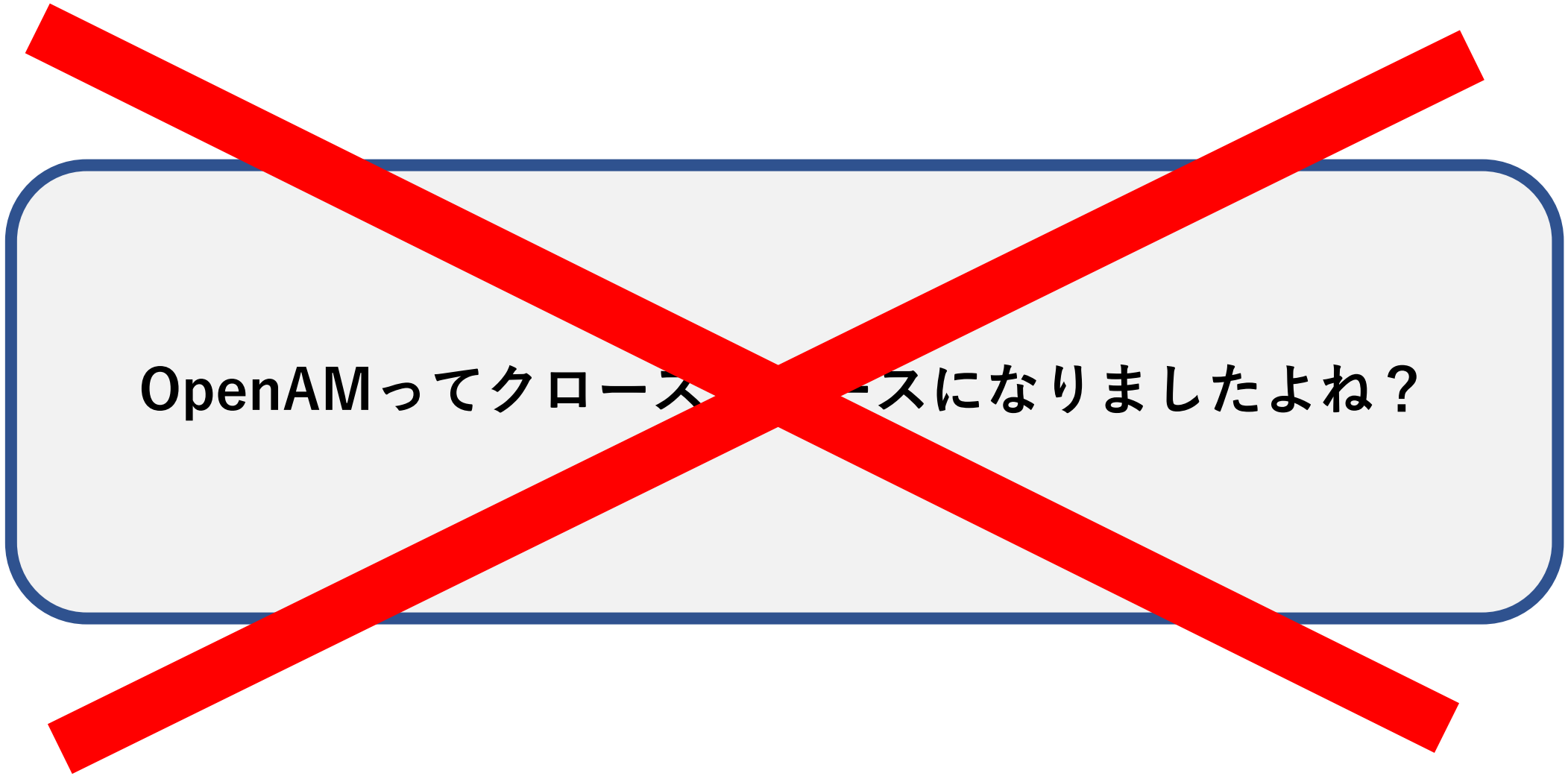
OSSTech

OpenAM

10年以上の歴史を持つ商用製品が元となったシングルサインオン製品

 **高品質なオープンソース**	**商用製品がベースで実績のあるオープンソースソフトウェアを採用し、独自機能追加など拡張に対するサポートも万全**
 **多彩なSSO連携機能**	**フェデレーション機能、エージェント方式、リバースプロキシ方式、代理認証方式によるSSOに対応**
 **複数の認証方式に対応**	**通常のIDとパスワードによる認証に加え、ワンタイムパスワードや統合Windows認証等、任意の組み合わせによる多要素認証が可能 アクセスURLを分けることにより、複数の認証方式を利用可能**

ところで…



OpenAMの歴史

2006　2008　2010　2014　2017　2019

OpenSSO OpenAM

クラウドの発展に合わせたシングルサインオン需要の加速

OSSとしてのOpenAM/OpenSSOの開発主体

Sun Microsystems → ForgeRock → OpenAMコンソーシアム

Oracleの買収に伴い、
OSSとしての先行きが不透明に

最新版ソースコードのクローズ
＋ForgerockAMとして発売

OpenAMコンソーシアム

- OpenAMコンソーシアムとしてソースコードを公開中
  https://github.com/openam-jp

https://www.openam.jp/

OpenAMの普及・促進を目的としたビジネスコンソーシアム
- OpenAMを取り扱う加盟企業でセミナー・技術記事寄稿
- OSSTech、オージス総研様が中心となって開発の実施

- ソースコード公開に至る経緯はインタビュー記事として公開中です！
- オープンソースソフトウェアのシングルサインオン製品が求められる理由
  - https://www.atmarkit.co.jp/ait/articles/1811/05/news006.html

OpenAMコンソーシアム 最新バージョンの公開

- OSSTech版、OpenAMコンソーシアム版共に、

  2019年12月に最新バージョン『OpenAM14』を公開

  - WebAuthn対応
    - FIDO2に規定されている最新の認証規格に対応
  - Java11(openjdk11)対応
    - 現行のJava 8は公式アップデートの終了が近い
    - Java 9はリリースモデルが変更となっている
    - 最新かつ長期間のサポートが可能なJava 11をサポート！

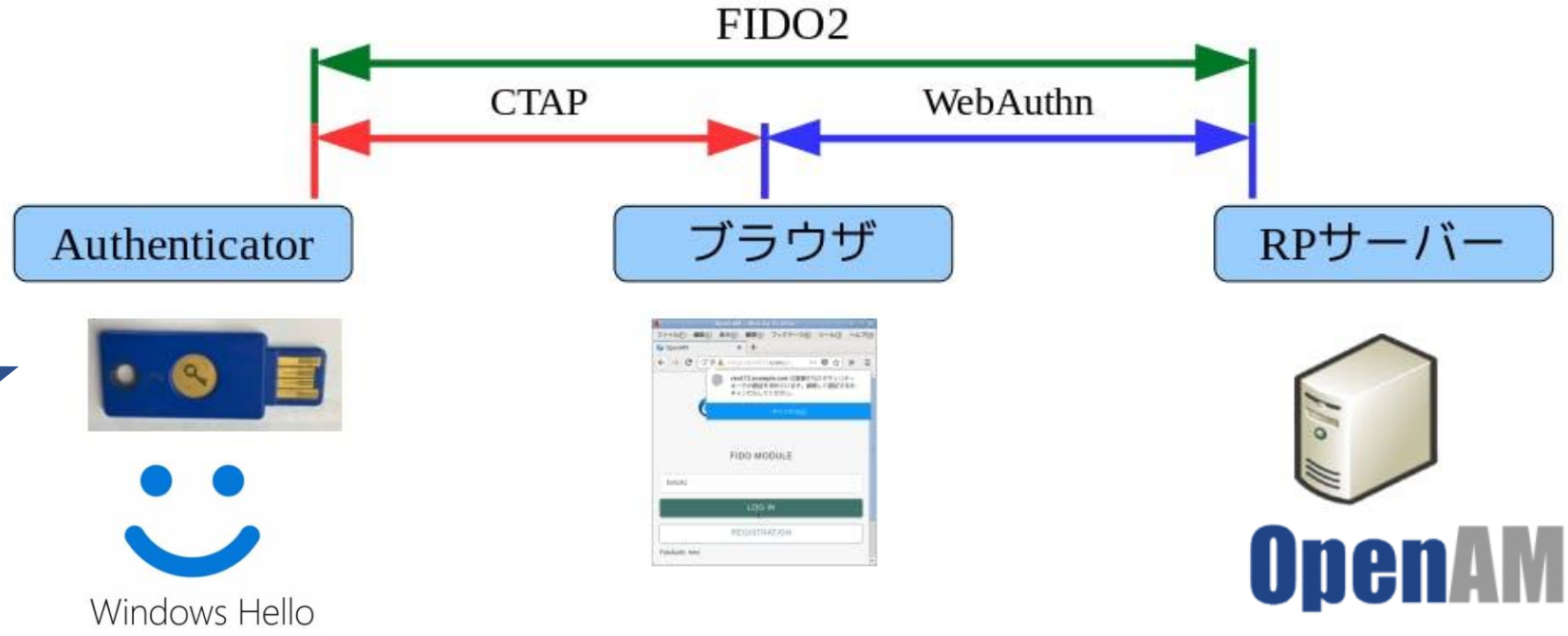
FIDO2とは

- FIDO2（Fast IDentity Online 2）
  - FIDOアライアンスが策定したパスワードを必要としない新しい認証方式
  - 公開鍵暗号方式をベースとしており、下記の特徴がある
    - パスワードを利用しない
    - 認証するサービスごとに鍵の情報を変更
    - ネットワークに機微な情報を流さない

WebAuthnとは

- FIDOアライアンスでFIDO2での認証に必要な登場人物及びプロトコルを定義しており、サーバ側の実装はWebAuthnで定義されている
  - Authenticator（TPM内蔵PCの指紋リーダー、USBやBluetoothデバイスなど)
  - ブラウザ（Firefox、Edge、Chromeなど)
  - RPサーバー（FIDO2/WebAuthn 認証サーバー、サービスなど)

iPhoneで TouchID / FaceIDをAuthenticatorとして利用可能になりました！



お問い合わせ：sales@osstech.co.jp

OSSTech

「オープンソースソフトウェア」の新しい価値を創造し、高機能・高品質を追求する

統合認証　シングルサインオン　アイデンティティ管理ソリューション