OpenAM案件の傾向と対策

Out-of-the-box　OpenAM
アプリケーションの特性ごとにOSSTech製OpenAMで
対応したユースケースのご紹介

オープンソース・ソリューション・テクノロジ株式会社
代表取締役 チーフアーキテクト 小田切耕司

お問い合わせ info@osstech.co.jp

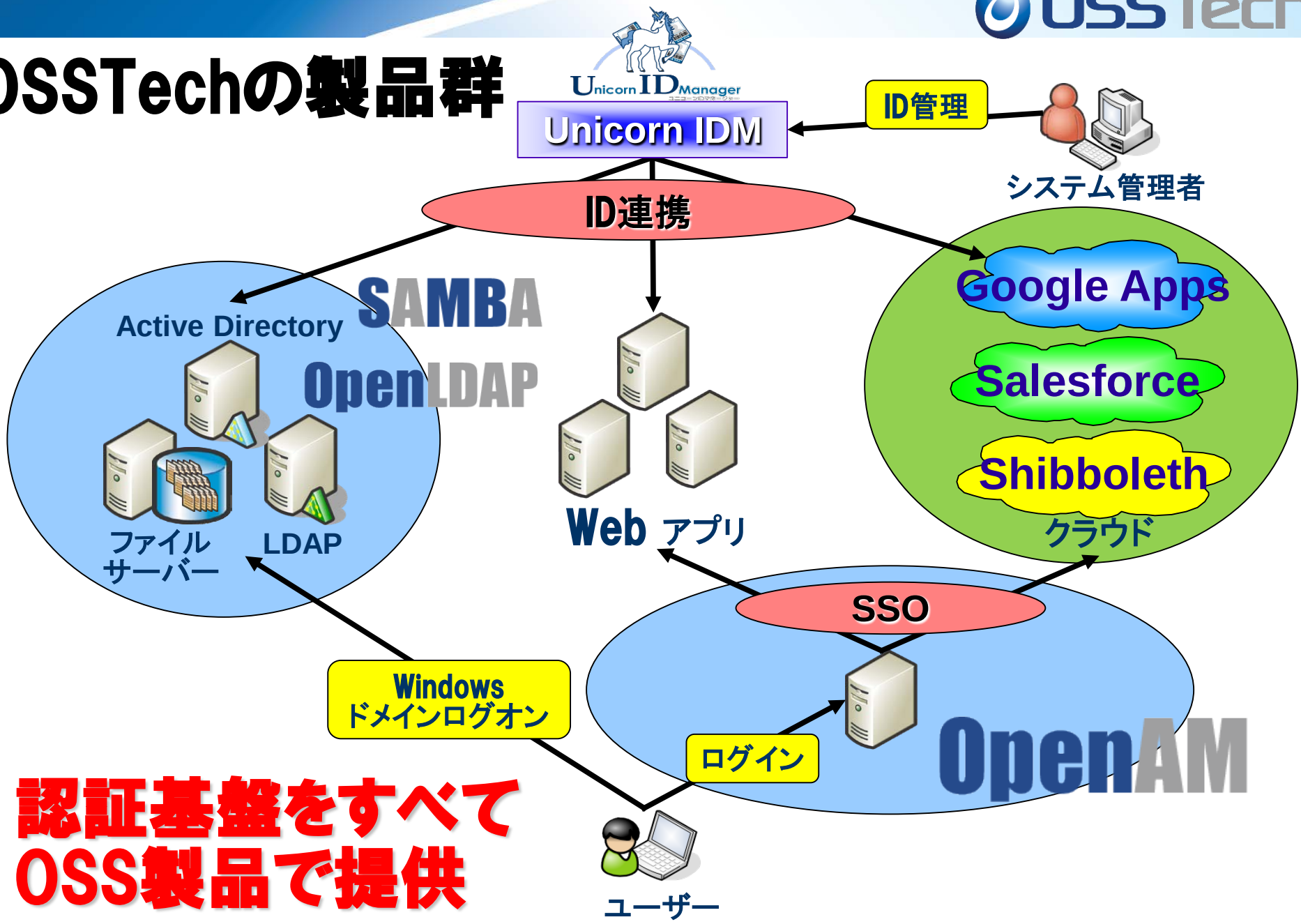
オープンソース・ソリューション・テクノロジ株式会社

「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

- **OSに依存しないOSSのソリューションを中心に提供**
  Linuxだけでなく、AIX, Solaris, Windowsなども対応！
- **OpenAM, OpenLDAP, Sambaによる認証統合／シングル・サイン・オン、ID管理ソリューションを提供**
  - 製品パッケージ提供
    機能証明、定価証明が発行可能
  - 製品サポート提供
    5年以上の長期サポート
    コミュニティでサポートが終わった製品のサポート
  - OSSの改良、機能追加、バグ修正などコンサルティング提供

OSSTechの製品群



認証基盤をすべて
OSS製品で提供

OSSTechの製品群(すべてOSSで提供)
Linux/AIX/Solaris版すべてRPMで提供

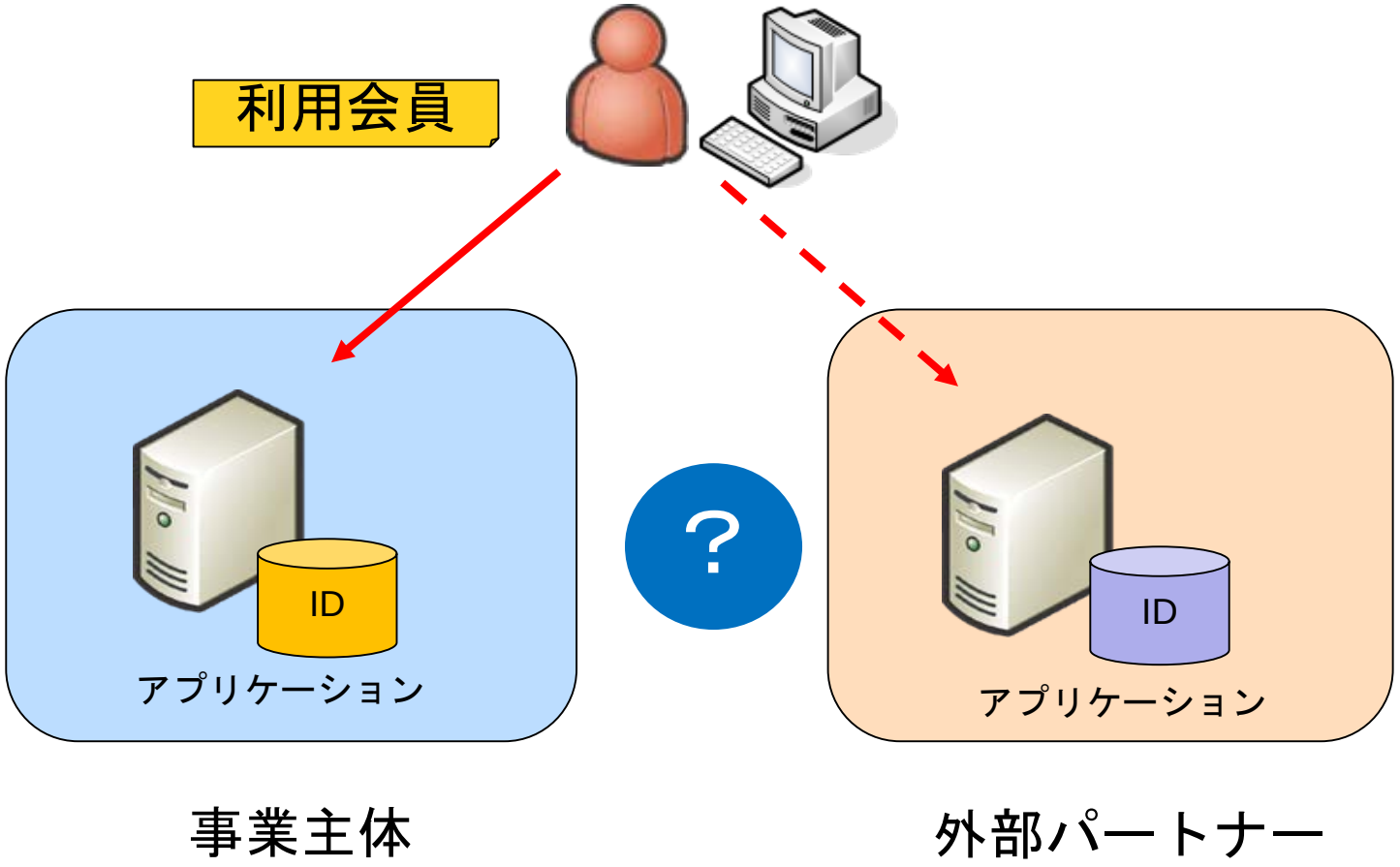
- OpenAM
  - Tomcat, OpenLDAP対応で高機能なシングルサインオン製品
- OpenLDAP
  - 認証統合、ディレクトリサービス、シングルサインオンのインフラ
- Samba
  - Active Directoryの代替、高性能NAS(CIFSサーバー)の代替
- Unicorn ID Manager
  - Google Apps, Active Directory, LDAP, Sambaに対応した統合ID管理製品
- ThothLink
  - WebブラウザからのWindowsファイルサーバアクセス機能を提供

OpenAMユースケース

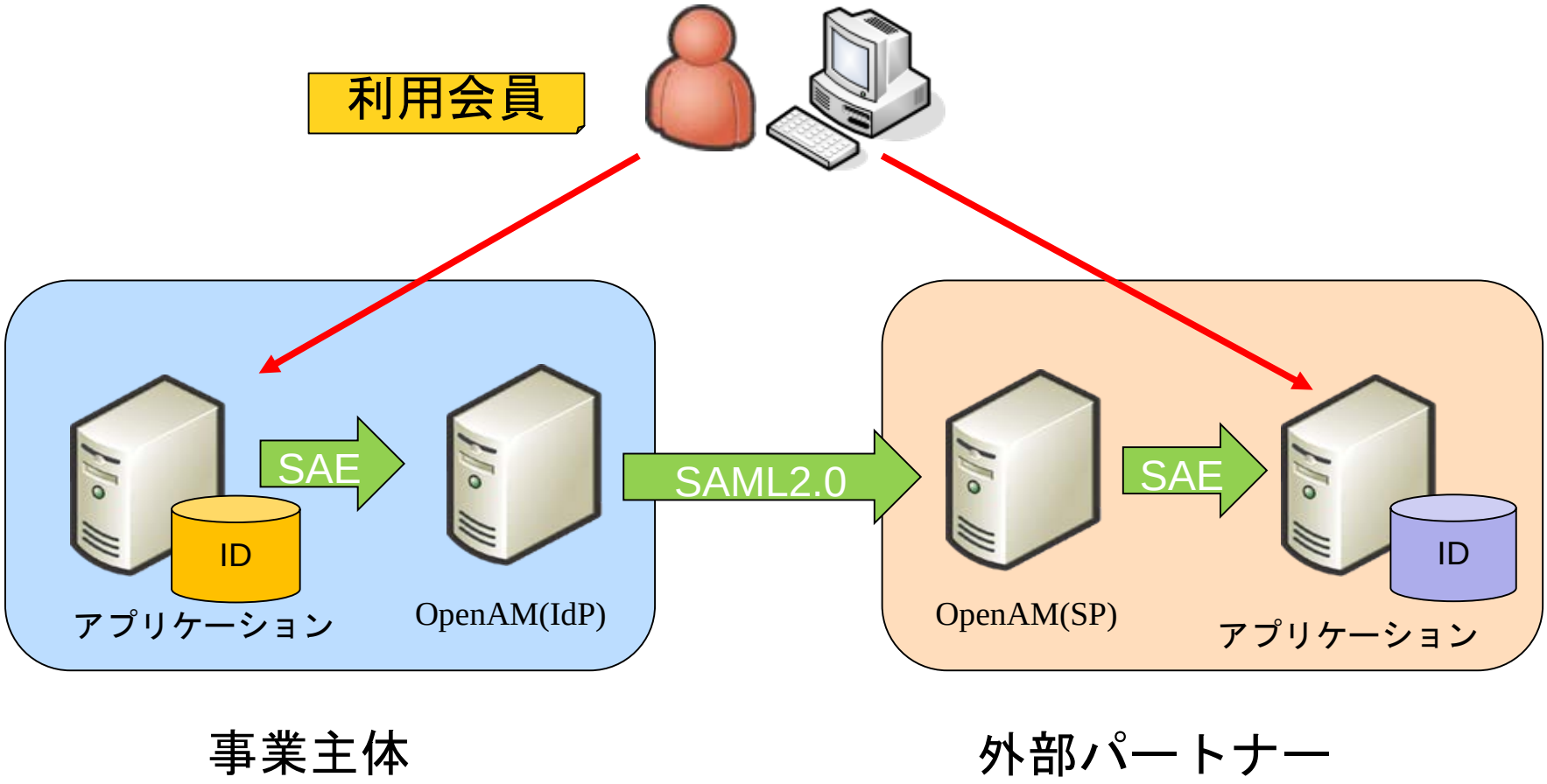
- ①仮想フェデレーション
- ②AWS連携
- ③スマートデバイス利用、REST API利用
- ④学認連携
- ⑤アクセス環境別認証
- ⑥拠点間認証連携
- ⑦Office365連携

OpenAMユースケース①
仮想フェデレーション

外部パートナーのサービス利用要件



OpenAMを仲介して接続

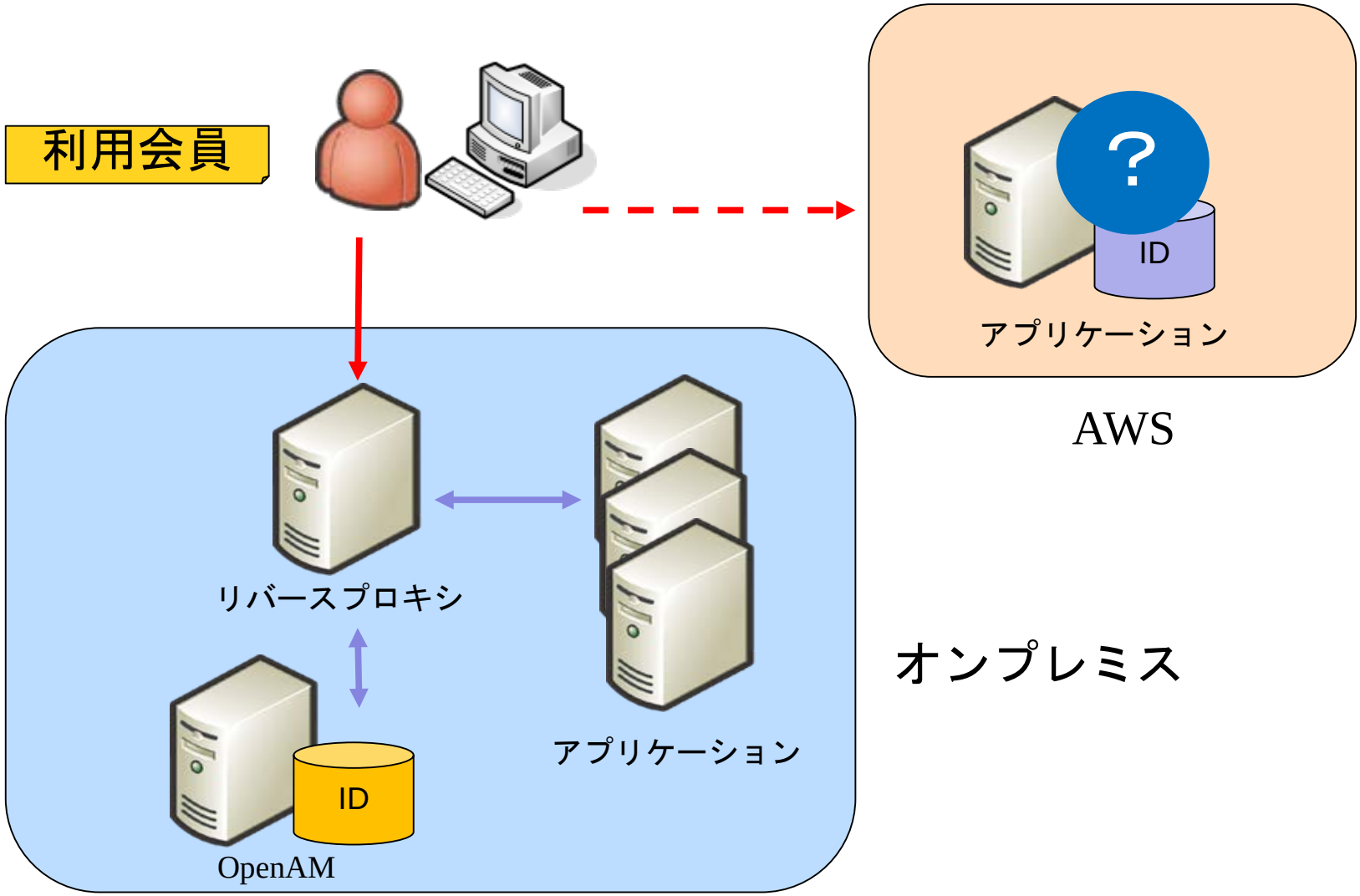


☆このユースケースでのポイント

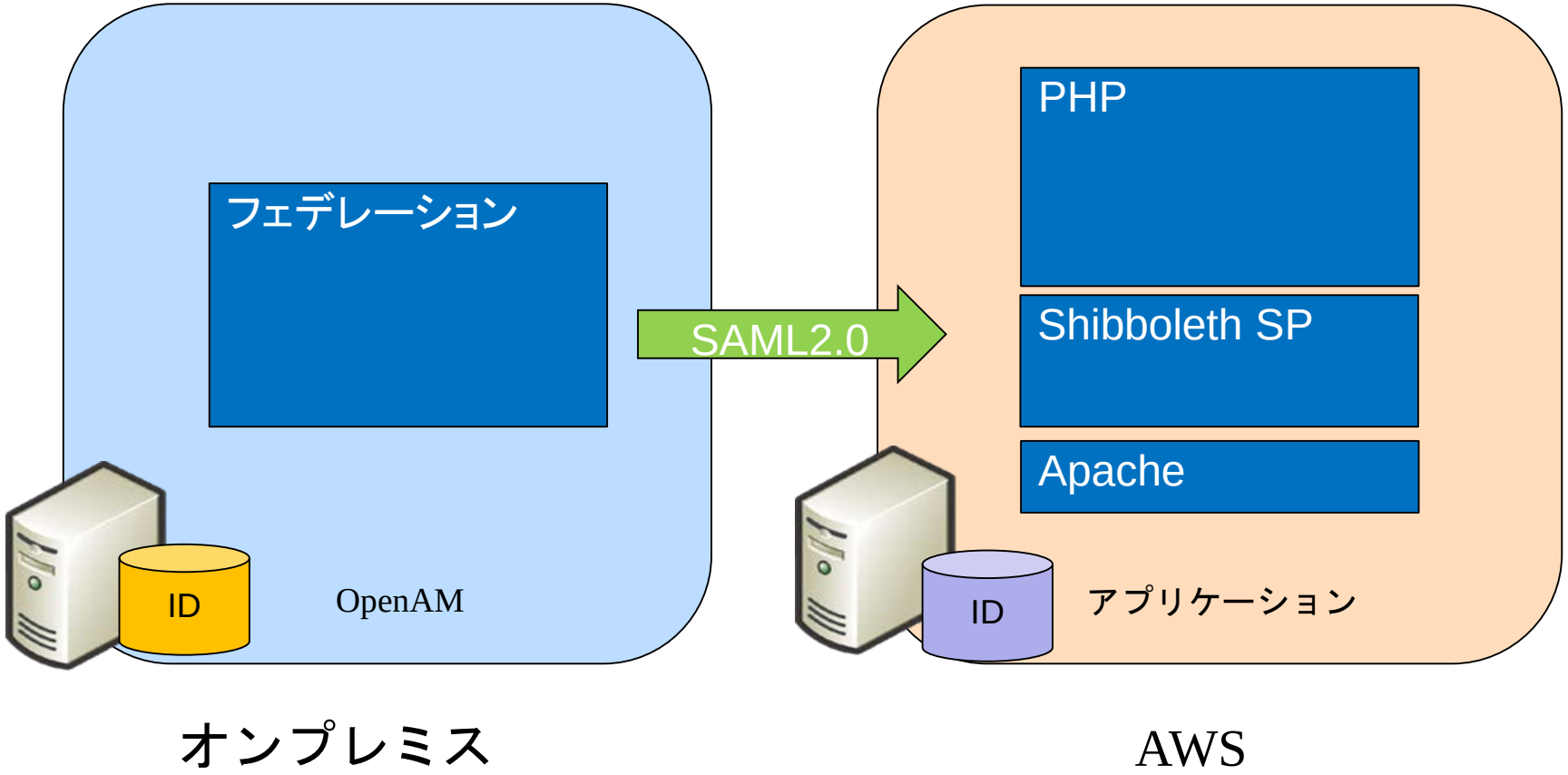
- OpenAMのSAE認証モジュールとSAML2.0フェデレーション機能を利用
- IdP、SPはアプリケーションとSAEでセキュアな接続（公開鍵Iもしくは共通鍵で暗号化）
- アプリケーションにはSAEの接続コンポーネントを配置
- アプリケーションの特性によりSAEを使用せず、OSSTech開発認証モジュールにて接続したケースもある

OpenAMユースケース②
AWS連携

AWS上で構築したPHPアプリケーション連携



AWSで構築したPHPアプリケーション連携

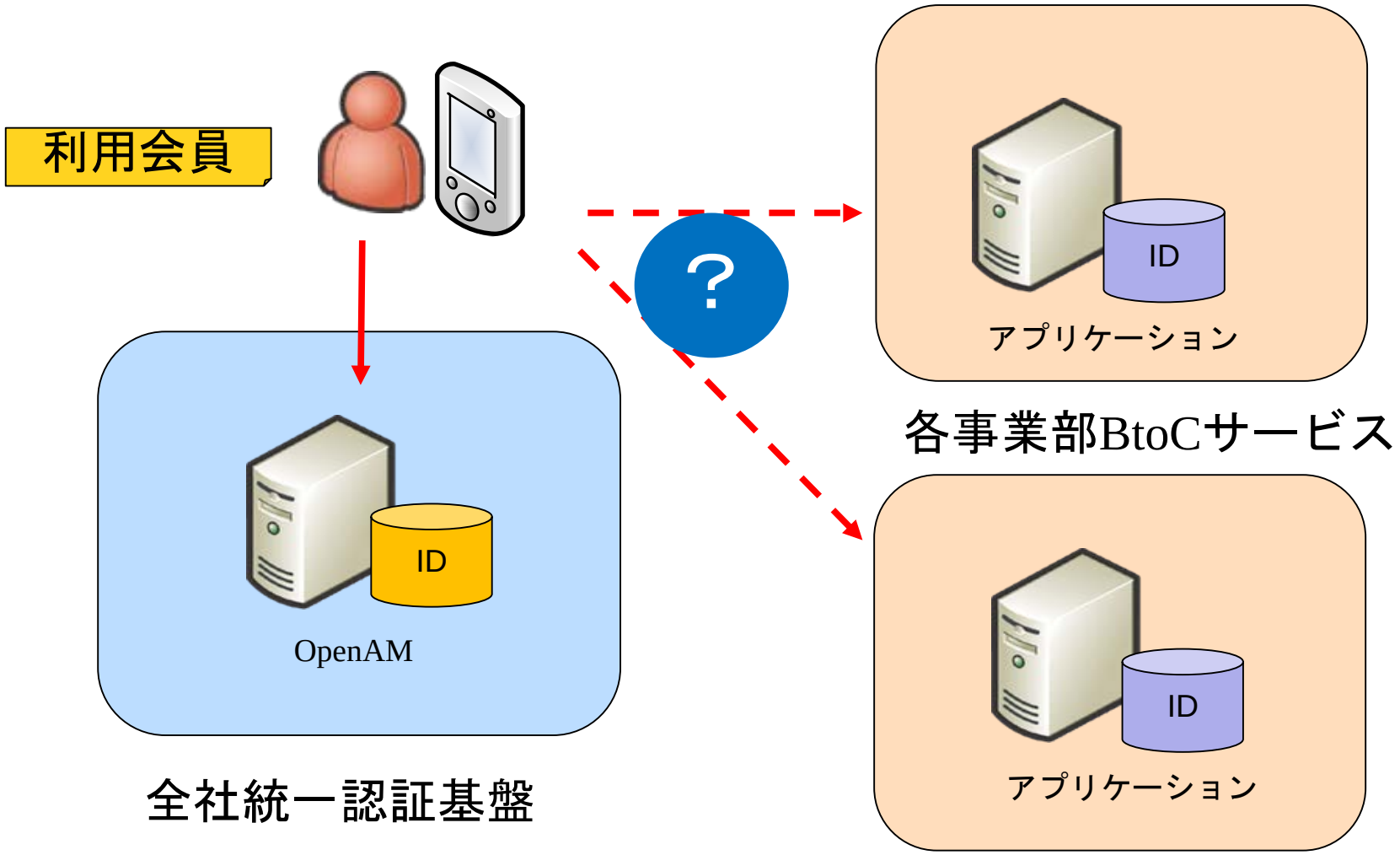


☆このユースケースでのポイント

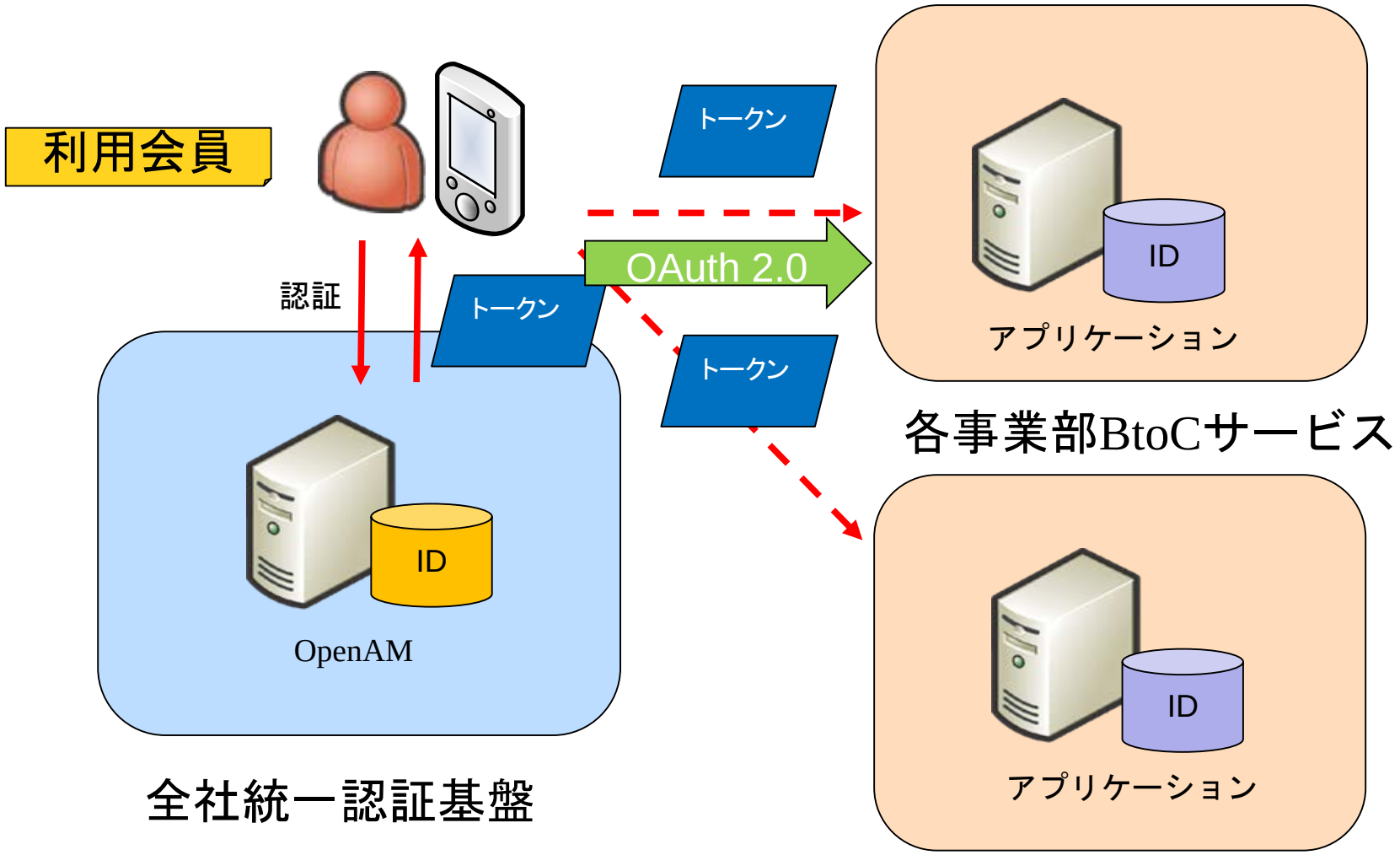
- OpenAMのSAML2.0フェデレーション機能を利用
- アプリケーション側にはShibboleth SPを導入して、SAML実装のコストを大幅に削減
- アプリケーションはShibboleth SPを通して認証情報を取得する
- クラウドとオンプレミスのSSO連携を実現

OpenAMユースケース③
スマートデバイス利用
REST API利用

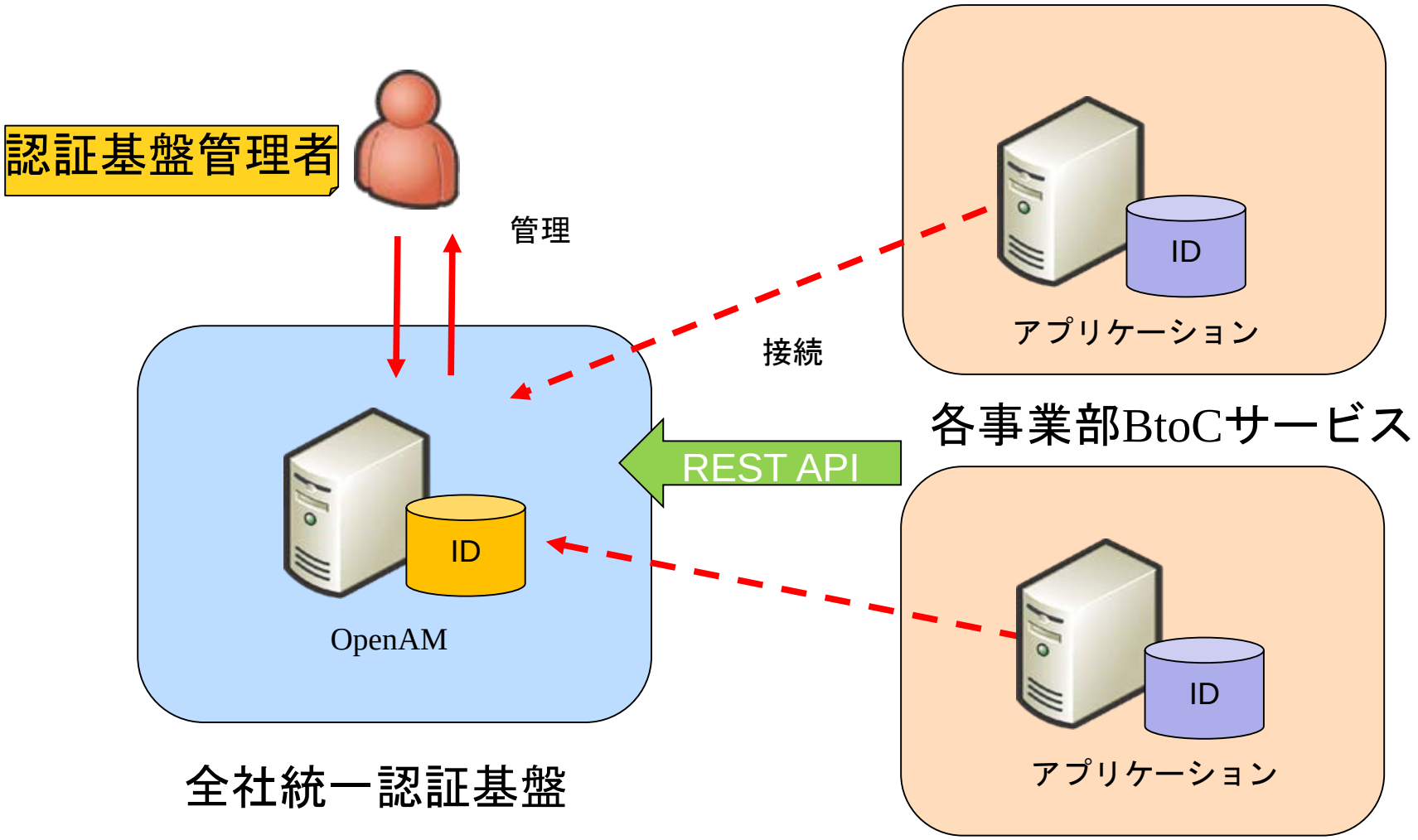
スマートデバイスから各サービスへの認可



OAuth2.0でシームレスなサービス連携



REST APIを活用してレガシーなエージェント接続から脱却



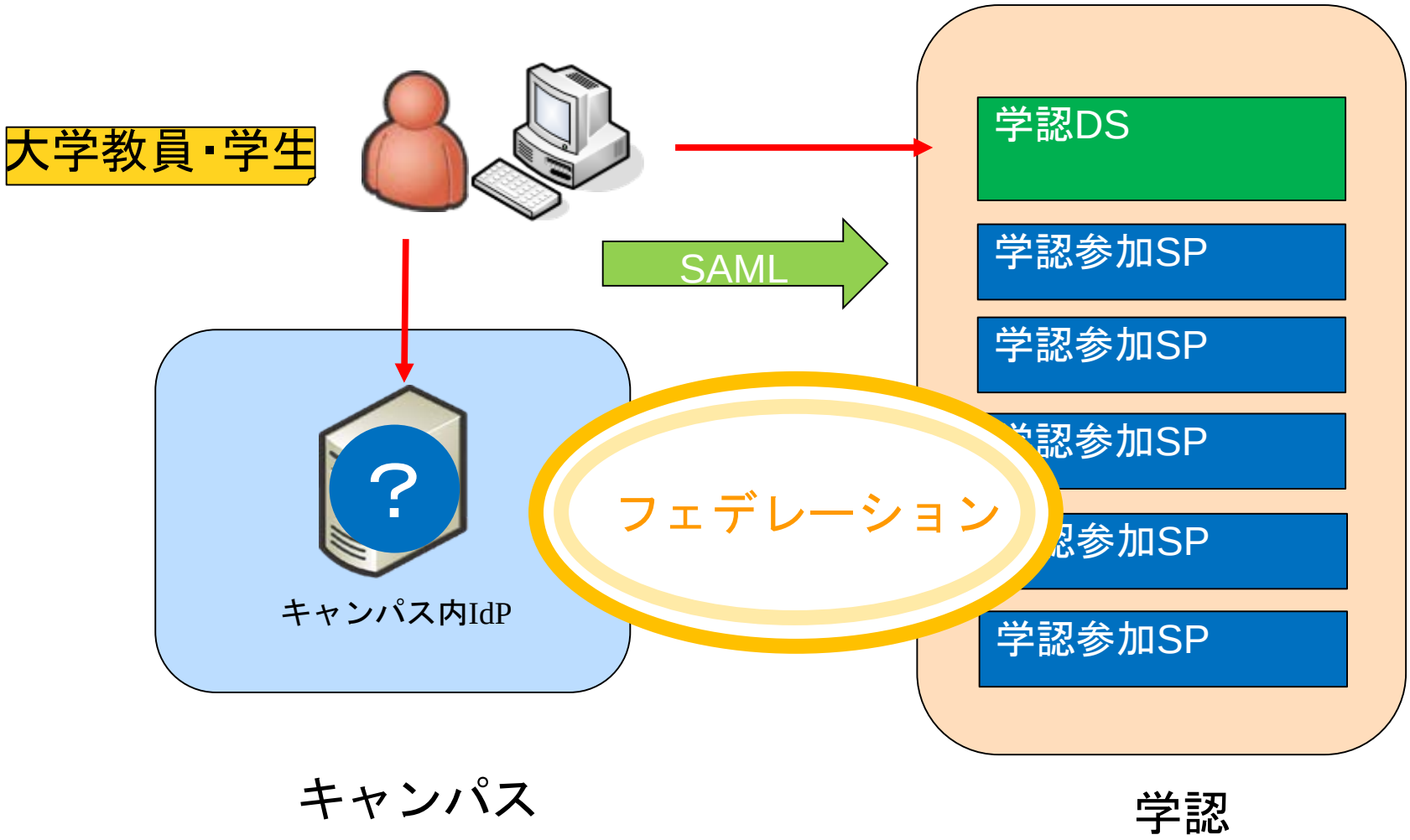
☆このユースケースでのポイント

- OpenAMのOAuth2.0機能を利用
- OpenAMのREST APIを積極的に利用して、柔軟で短時間の接続を実現
- 各事業部が個別に展開していたサービスをシームレスに接続
- スマートデバイスのサービス利用をセキュアでオープンな仕様を選択

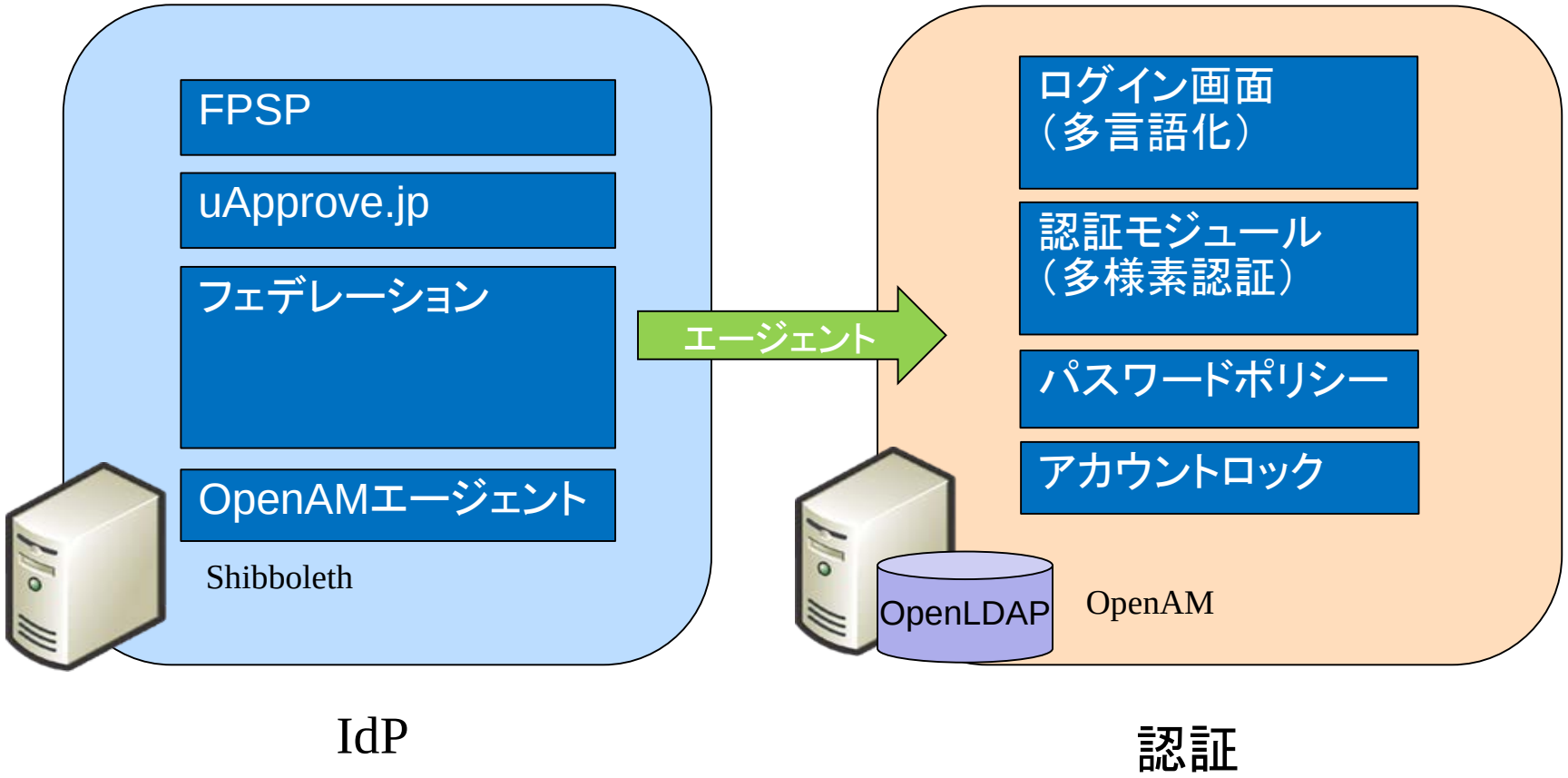
※今後のOpenAM機能拡張もREST APIによる実装の強化を目指している

OpenAMユースケース④
学認連携

学認連携



キャンパス内IdPの構築



☆このユースケースでのポイント

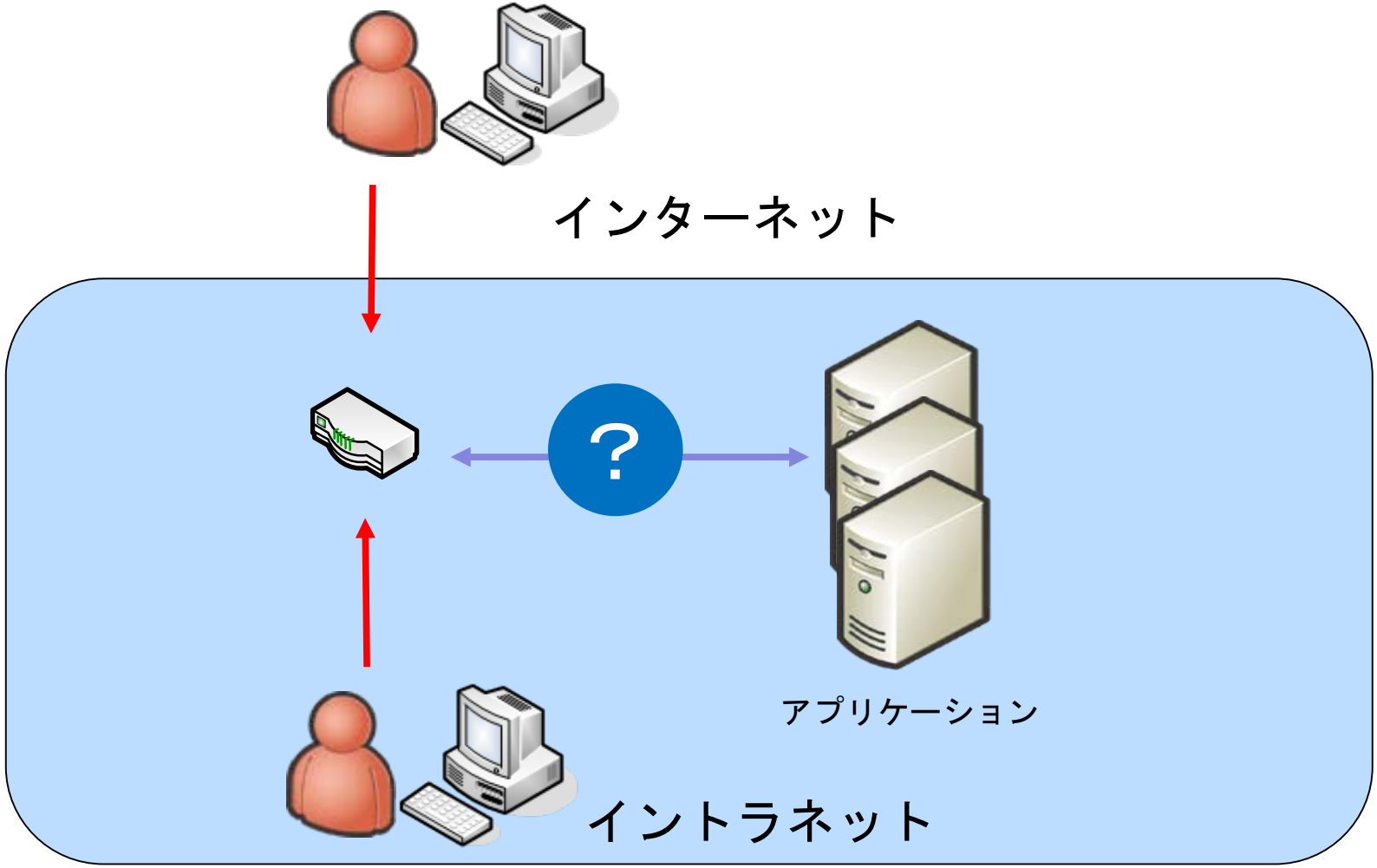
- フェデレーション機能にはShibbolethを利用
- 認証機能にはOpenAMを利用したハイブリッド構成
- 学認フェデレーションのきめ細かい要件に弊社のノウハウで対応
- OpenAMを利用することにより学内アプリケーションSSOも対応可能

※Shibbolethはバージョン3.0以降がリリースされている。

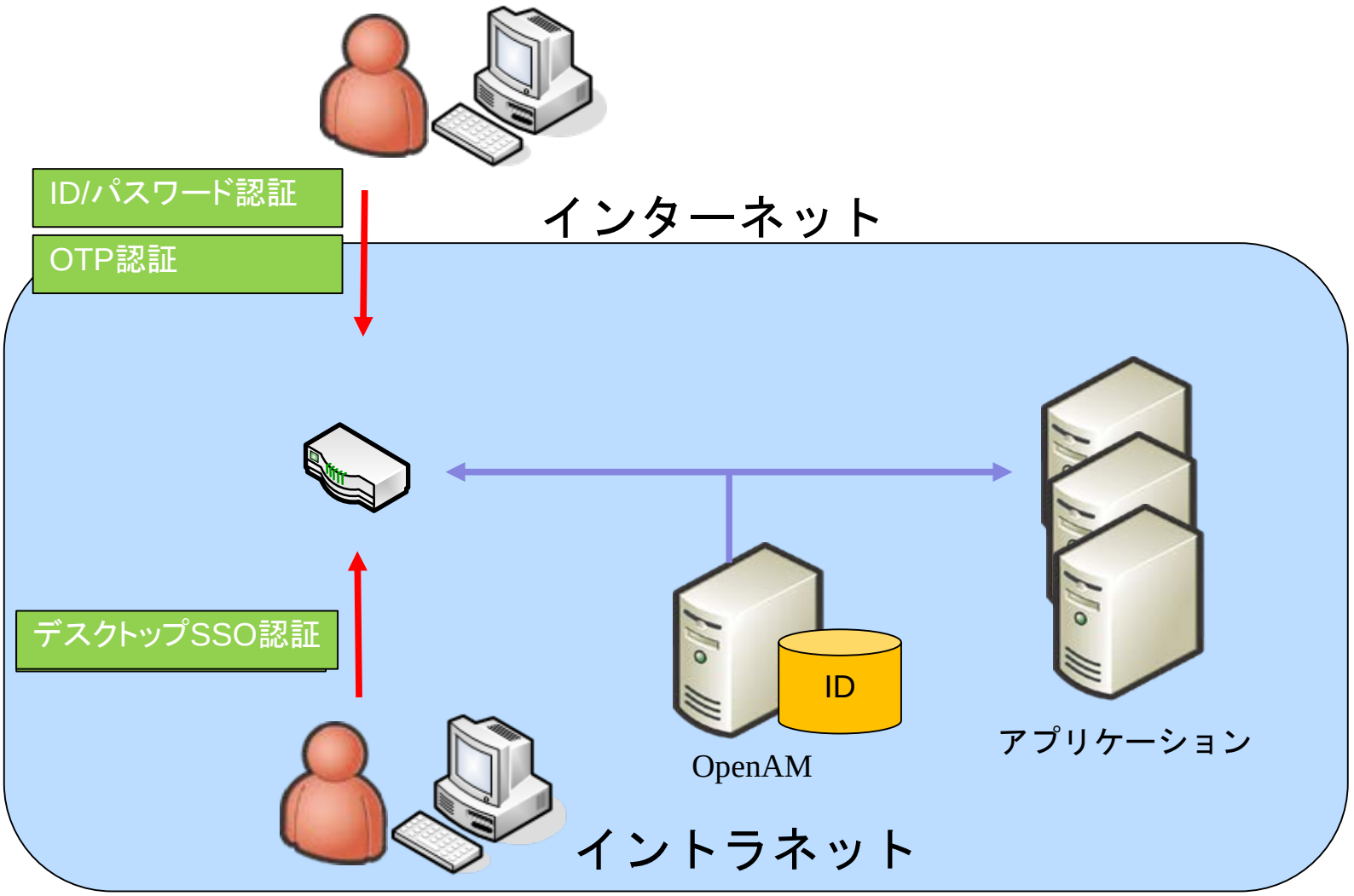
現行多く利用されている2.xからの移行に向けて弊社ではいち早く準備中である。

OpenAMユースケース⑤
アクセス環境別認証

アクセス環境が異なる場合の認証



アクセス環境が異なる場合の認証

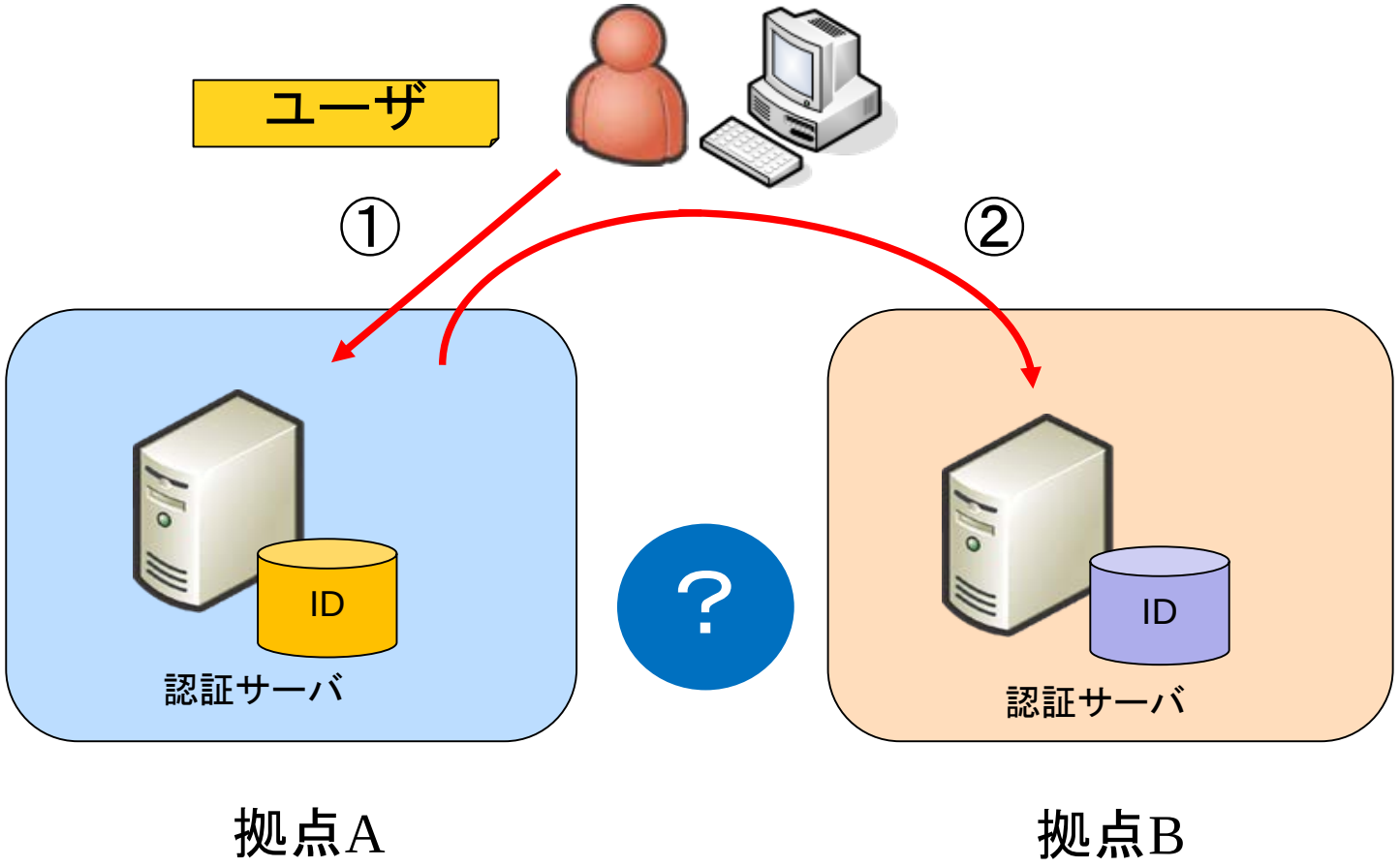


☆このユースケースでのポイント

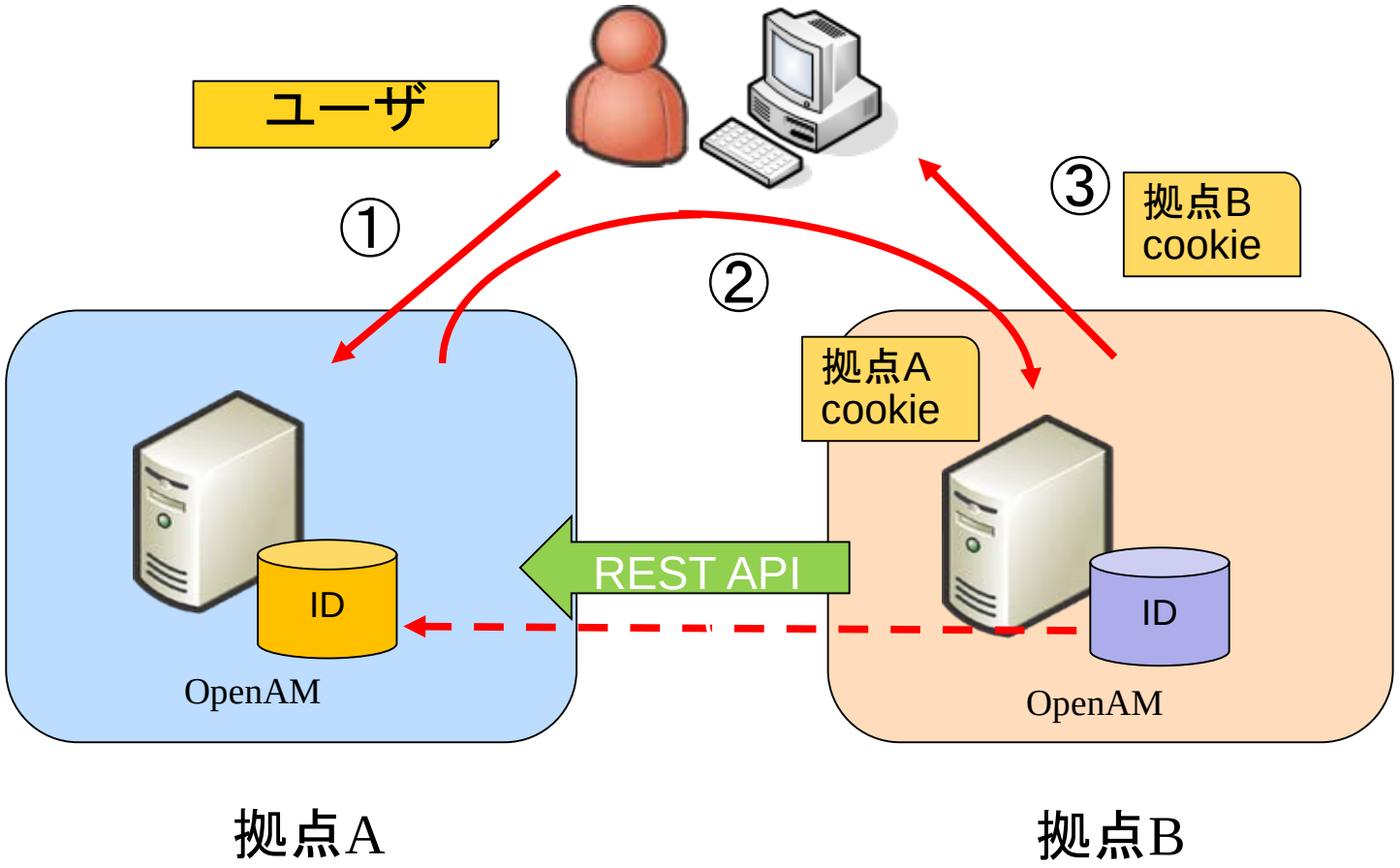
- OpenAMのアダプティブリスク認証、認証連鎖機能、認可条件を利用
- アクセス元により、認証方法を変更したり、認証要素を追加することでセキュリティの強度を変更する

OpenAMユースケース⑥
拠点間認証連携

遠隔地の拠点間での認証連携要件



遠隔地の拠点間での認証連携要件

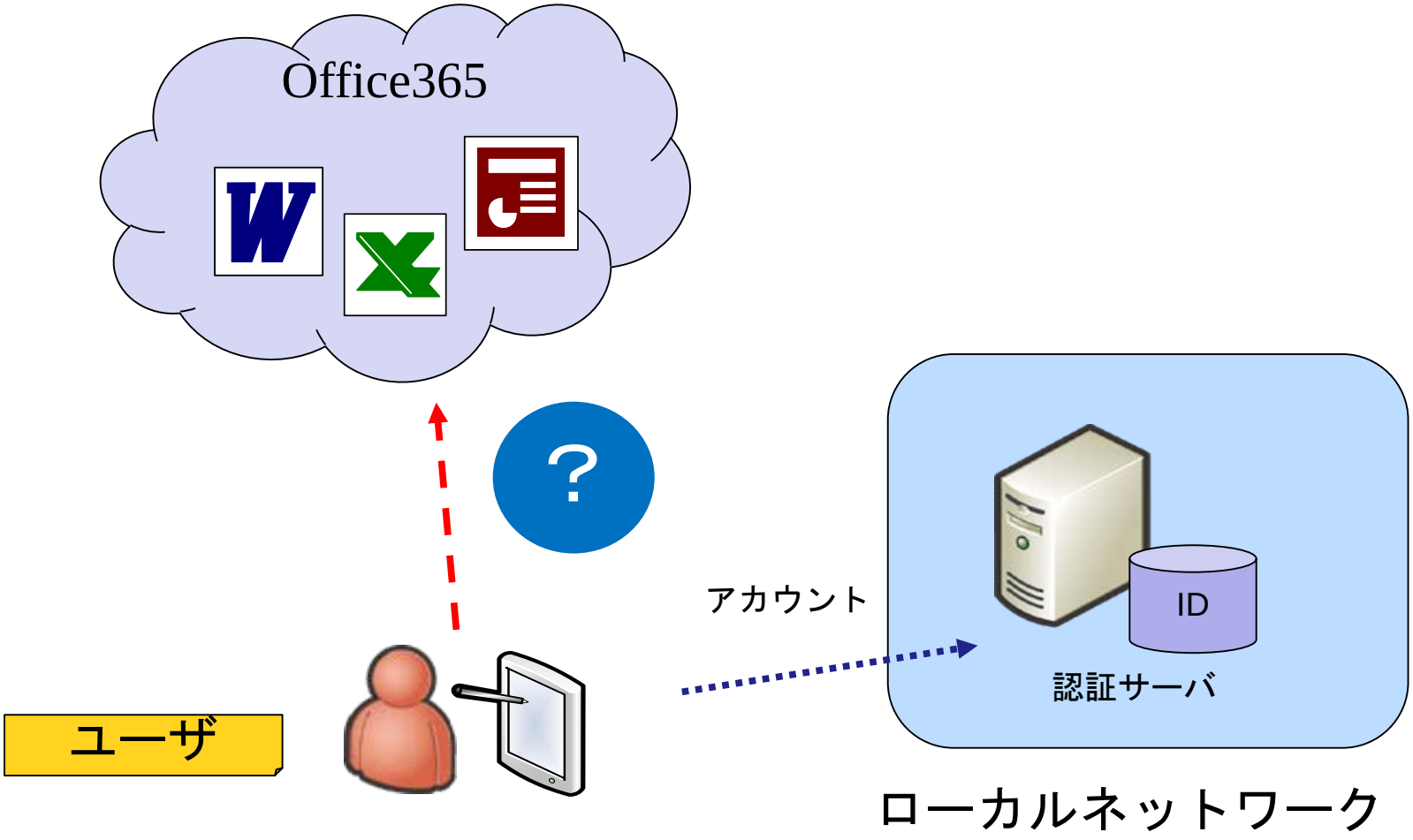


☆このユースケースでのポイント

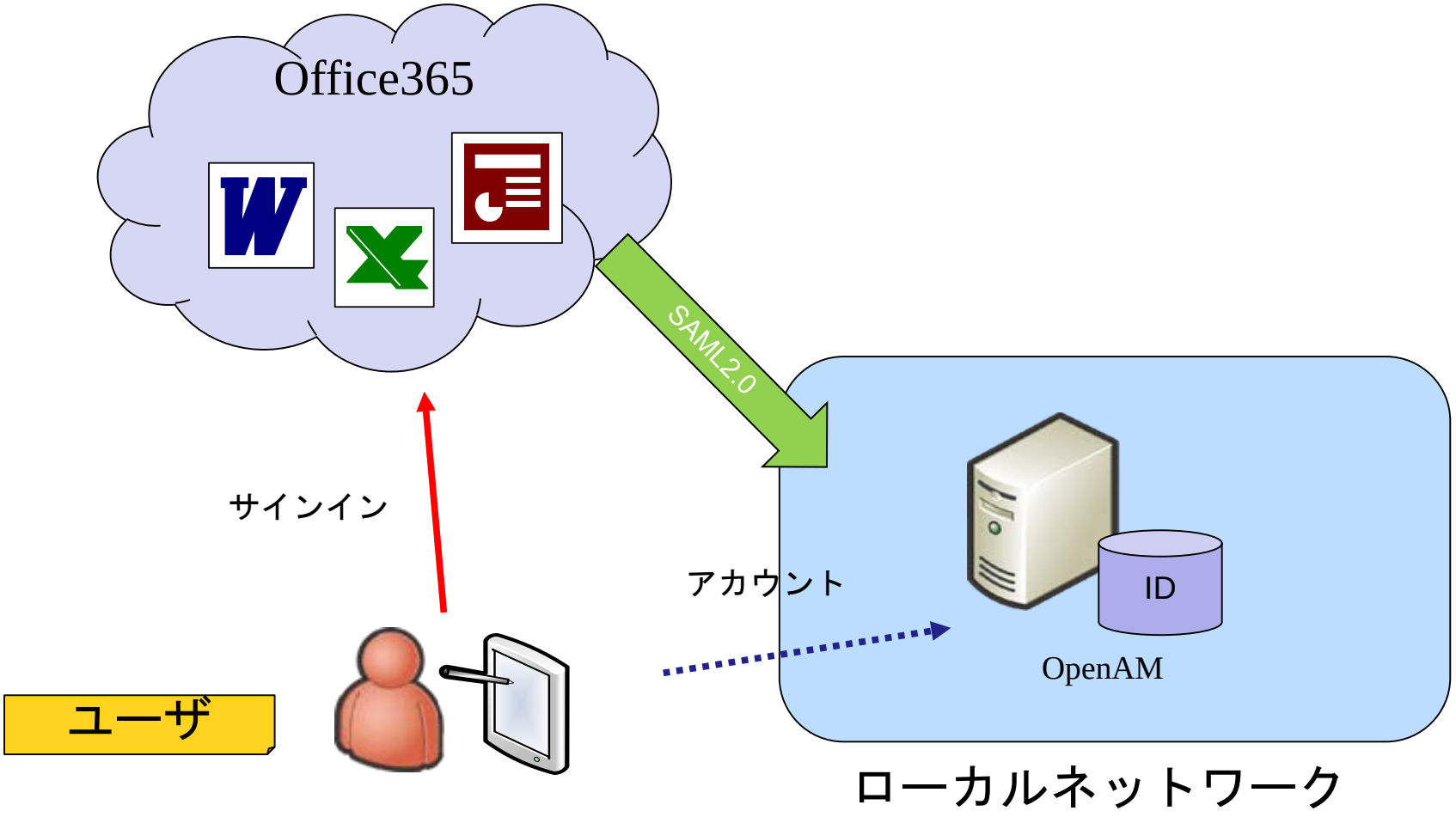
- OpenAMの認証モジュール機能を利用する
- 他拠点のOpenAMの認証情報にREST APIでアクセスする
- 拠点ごとに異なるクッキー名を使用する
- 仮想セッションフォワーディングで拠点間の認証連携を実現する

OpenAMユースケース⑦
Office365連携

Office365利用での認証連携要件



Office365利用での認証連携要件

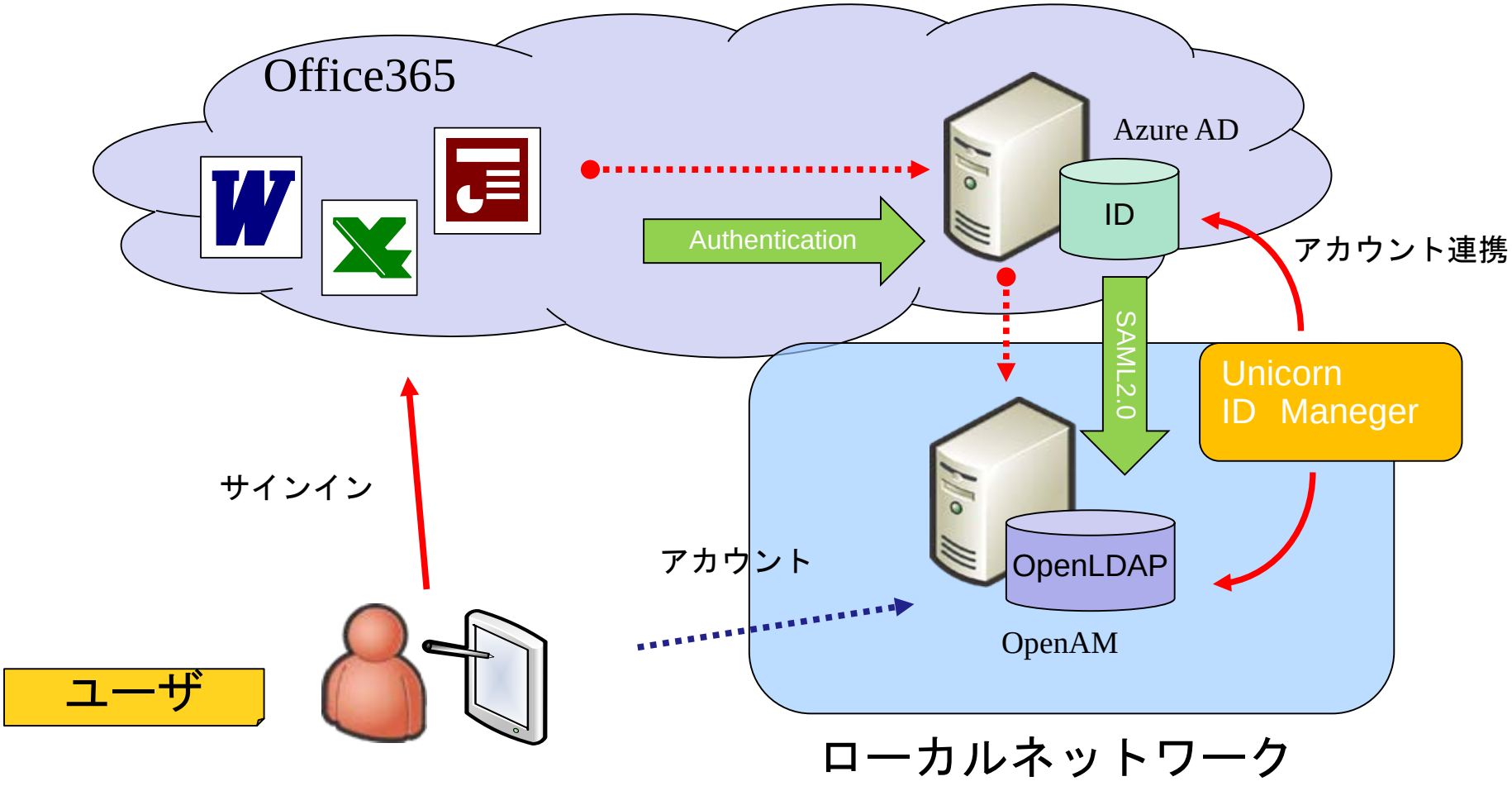


☆このユースケースでのポイント

- Office365とOpenAMはSAML2.0で接続する
- Office365のサインイン画面とOpenAMのログイン画面での認証をおこなう

※ブラウザからのOffice365アクセスはこの方法で利用できます。デスクトップアプリケーションは今後のロードマップでSAML2.0によるパッシブ認証を予定しています。

Office365利用での認証連携要件



ダウジャパン株式会社との連携ソリューション紹介

OpenAM＆ワンタイムパスワード

連携イメージ

GrippinTower概要

- ワンタイムパスワードをはじめとするセキュリティプロダクトベンダーであるダウジャパンが販売
- 韓国の金融機関及び企業で800万個のトークンを供給し、シェア80％以上
- 物理トークンでパスワードを自動生成
- ネットワークから盗聴できないセキュアな認証

GrippinTowerラインナップ

- 携帯に便利なカードタイプトークン
- Android/iOS対応のソフトウェアタイプトークン
- NFC連動タイプトークン

Windows10 標準ブラウザ Microsoft Edgeの検証

- データストア認証　○
- Windows統合認証　○
  ※IEでセキュリティゾーンの設定が必要
- エージェント　○
  ※IEでセキュリティゾーンの設定が必要
- SAML　○

「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

OSSTech オープンソース・ソリューション・テクノロジ株式会社 Open Source Solution Technology Corporation
〒141-0031 東京都品川区西五反田1-29-1 コイズミビル 8F Tel:03-6417-0753 Fax:03-6417-0754 Mail:info@osstech.co.jp