オープンソースで実現する
シングルサインオンとID管理

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

OSSTech

オープンソース・ソリューション・テクノロジ（株）
会社紹介

OSSTech

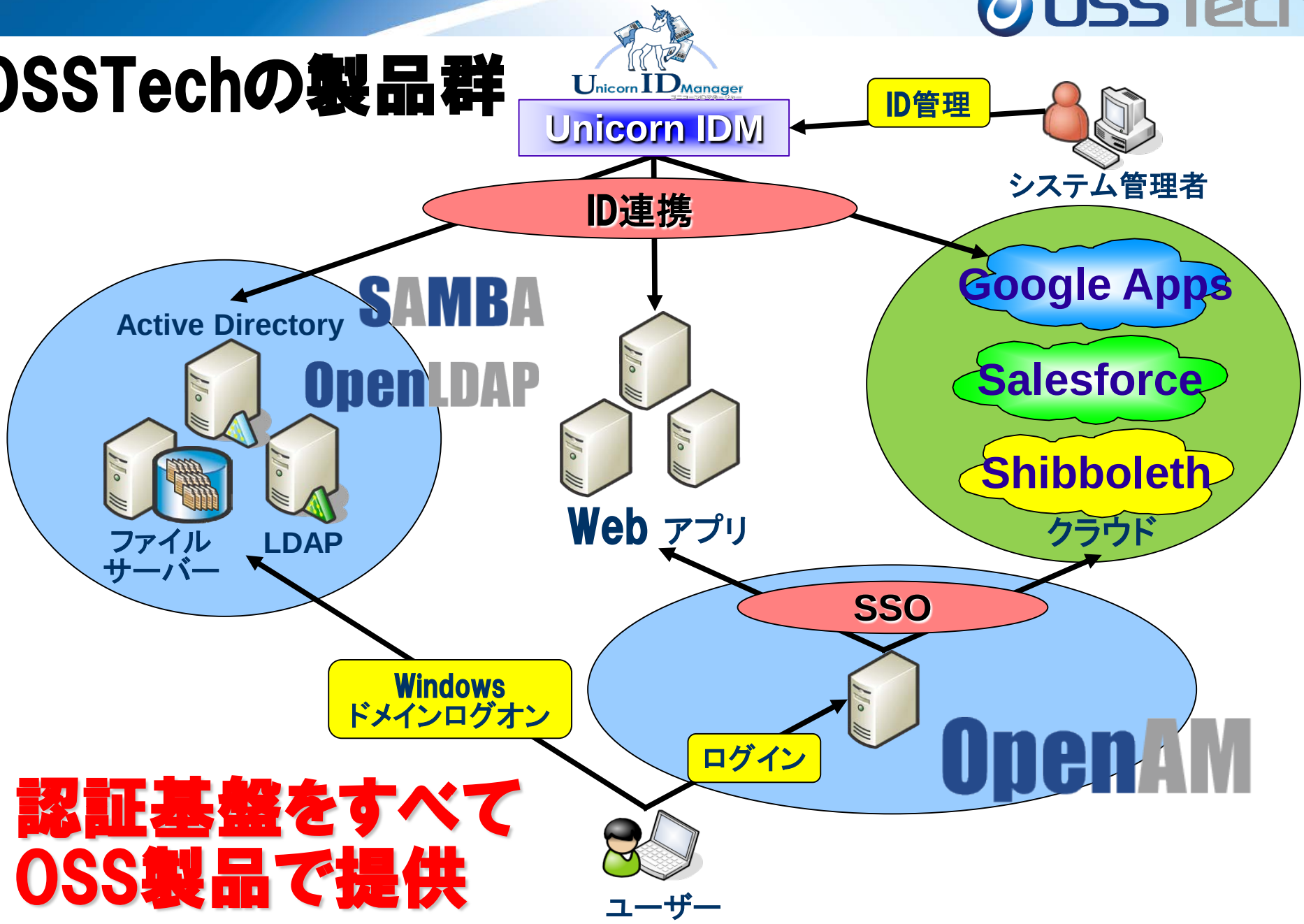
オープンソース・ソリューション・テクノロジ株式会社

「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
    3年～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)
原則Linux/Solaris/AIX共にRPMで提供

- OpenAM for Linux/Windows
  - Tomcat, OpenLDAP対応で高機能なシングルサインオン製品(旧OpenSSO, Sun Access Manager)
- OpenLDAP for Linux/Solaris/AIX
  - 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 for Linux/Solaris/AIX
  - Active Directoryの代替、高性能NAS(CIFSサーバー)の代替
- Unicorn ID Manager for Linux
  - Google Apps, Active Directory, LDAP, Sambaに対応した統合ID管理製品

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

- ThothLink(トートリンク) for Linux
  - 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
  - SSLBridge後継製品
- Chimera Search(キメラサーチ) for Linux
  - アクセス権の無いファイルは表示されない全文検索システム
- Mailman for Linux
  - 日本語での細かな問題を解決
  - YahooメールやGoogle Appsのメーリングリスト機能を補完

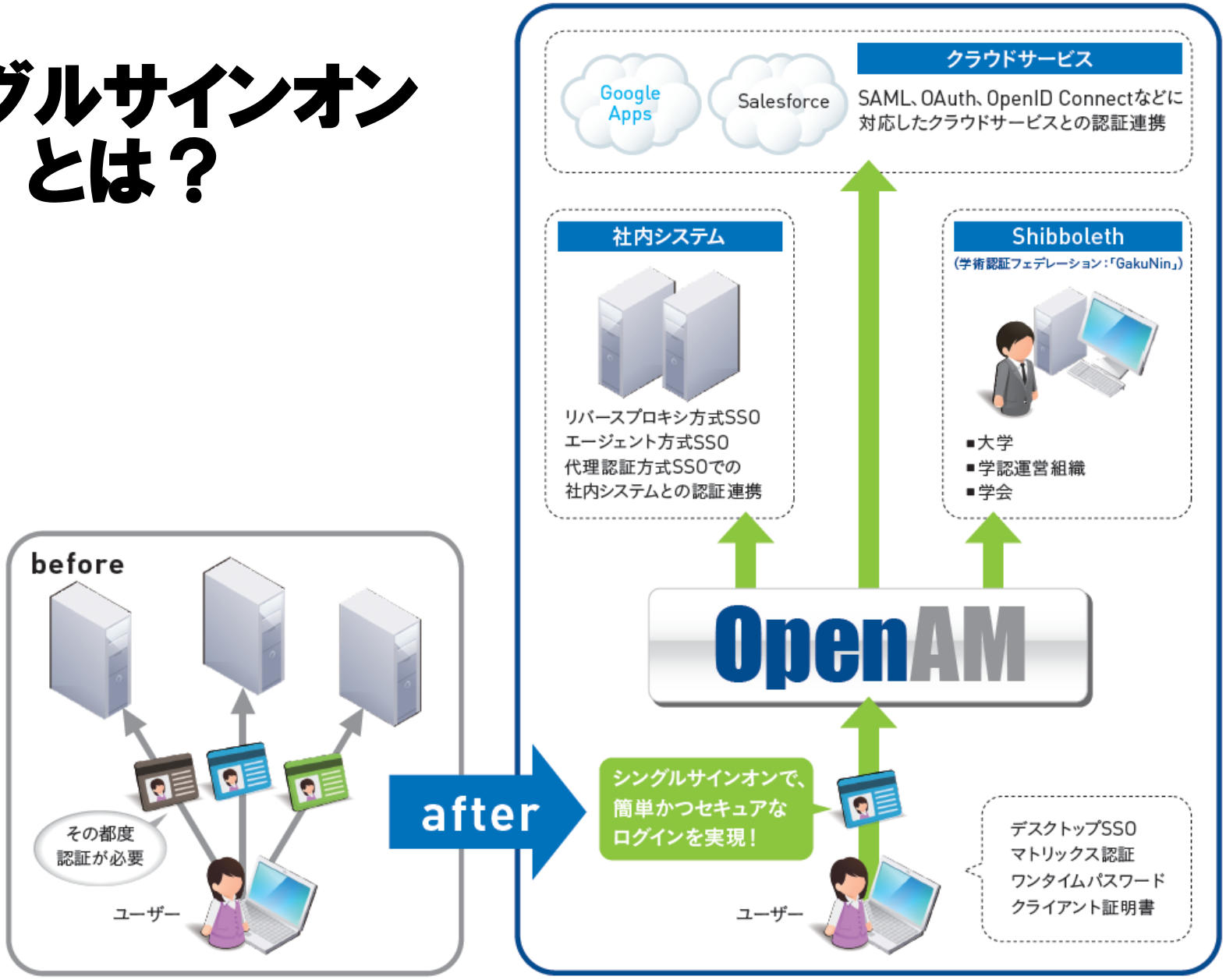
シングルサインオンと ID管理の市場動向

OSSTech

SSOとID管理の動向

- クラウドの普及
  - SaaSの普及
    Google Apps, Salesforce, Office365の普及
  - IaaSやPaaSの普及
    イントラネットとクラウドの混在環境が急増
- SSO(シングルサインオン)が急速に普及中
  - クラウドとイントラネットをシームレスに使うために
  - M&Aや会社合併のために増えすぎたアプリやIDを統合するためにSSOを導入
- SSOには認証強化のために多要素認証が要求される
- SaaSとのSSOではID管理も必要
- OpenID ConnectやSCIM(System for Cross-domain Identity Management)が今後注目

シングルサインオンとは？



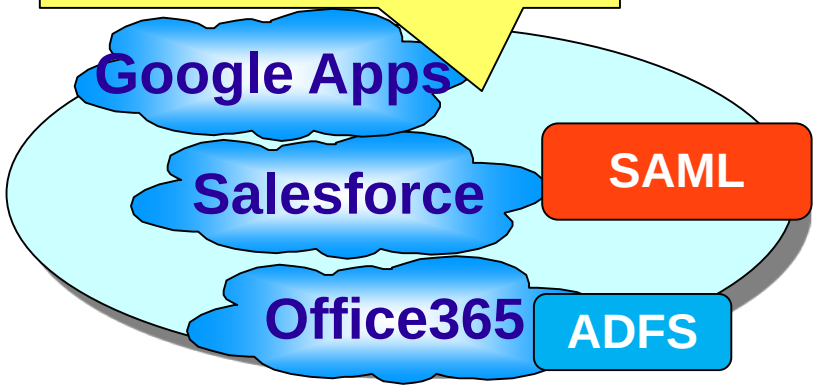
OpenAMで実現する
シングルサインオン・ハブ

OSSTech

オープンソースだから
高機能・安価に実現

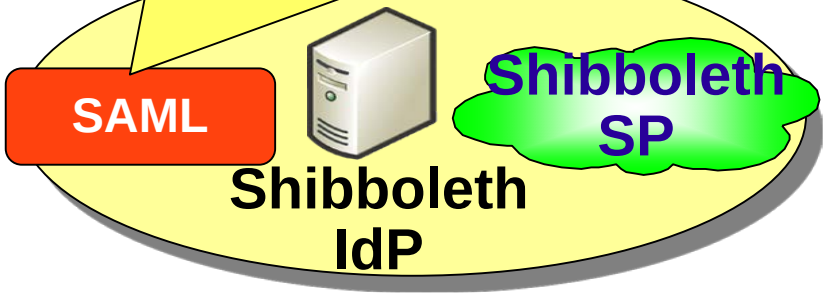
混在する複数のSSO環境

SAML IdP を導入して SSO を実現



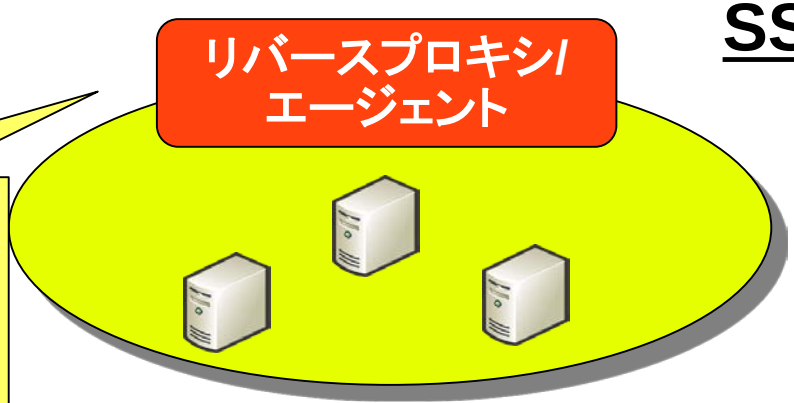
クラウドSSOセグメント

Shibboleth IdP で SSO を実現 (Shibboleth は SAML を利用しているが、仕様上 OpenAM では代替不可能)



学認（Shibboleth）SSOセグメント

大幅な改修はしたくないため、エージェント型/リバースプロキシ型で SSO を実現

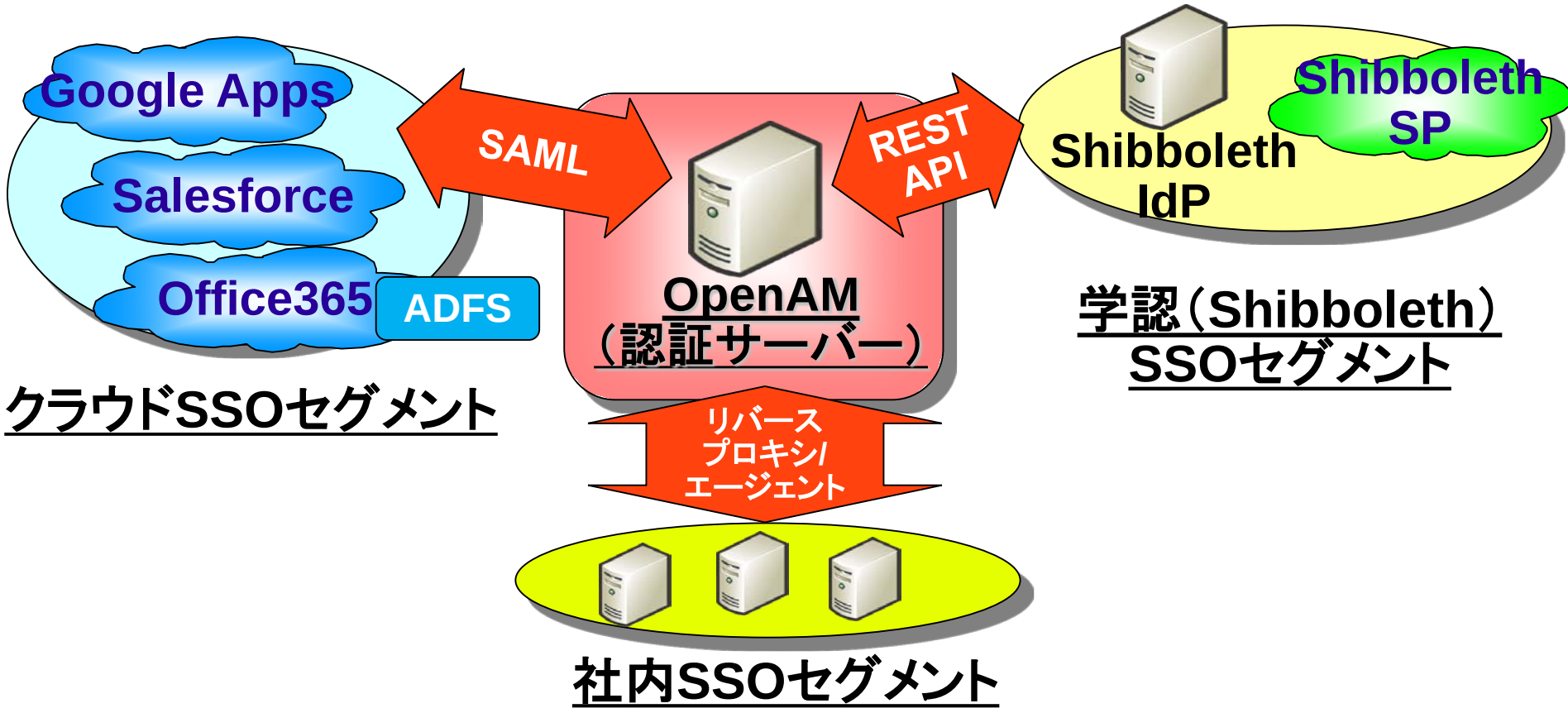


社内SSOセグメント

シングルサインオン・ハブを実現するための機能

- 高度な認証機能
  - ユーザーの本人性を確認する。セキュリティ強化のために、多要素認証が望ましい。
- ユーザー情報保存機能
  - 認証情報や他システムに連携するユーザー情報を保存する
- 外部システムと連携可能なインタフェース
  - フェデレーション（SAML, OpenID, OAuthなど）
  - REST API
  - SDK

OSSで実現するシングルサインオン・ハブ



SSO セグメントを結合するハブとして OpenAM を利用
ユーザーは OpenAM へのログインさえ完了していれば、
全てのアプリに SSO 可能にできる！

なぜオープンソース製品を使うのか？

高機能・高品質なオープンソースの業界標準シングルサインオン製品

OpenAM

技術力と経験で
ソースコードを磨いた日本版製品

高品質オープンソース

商用製品がベースである高品質なオープンソースソフトウェアだからこそ、独自拡張機能を追加しても低コストさらに経験10年以上のエンジニアによる高品質なサービス

低コスト

ユーザー数に依存しない価格体系のため、商用製品に比べて低コスト

業界標準仕様に対応

SAML、OAuth、OpenID Connect、Shibboleth（学術認証フェデレーション）などの業界標準フェデレーションプロトコルに対応

複数の認証方式

SAMLやOAuthによる認証、エージェント方式、リバースプロキシ方式、代理認証によるSSOなどに対応

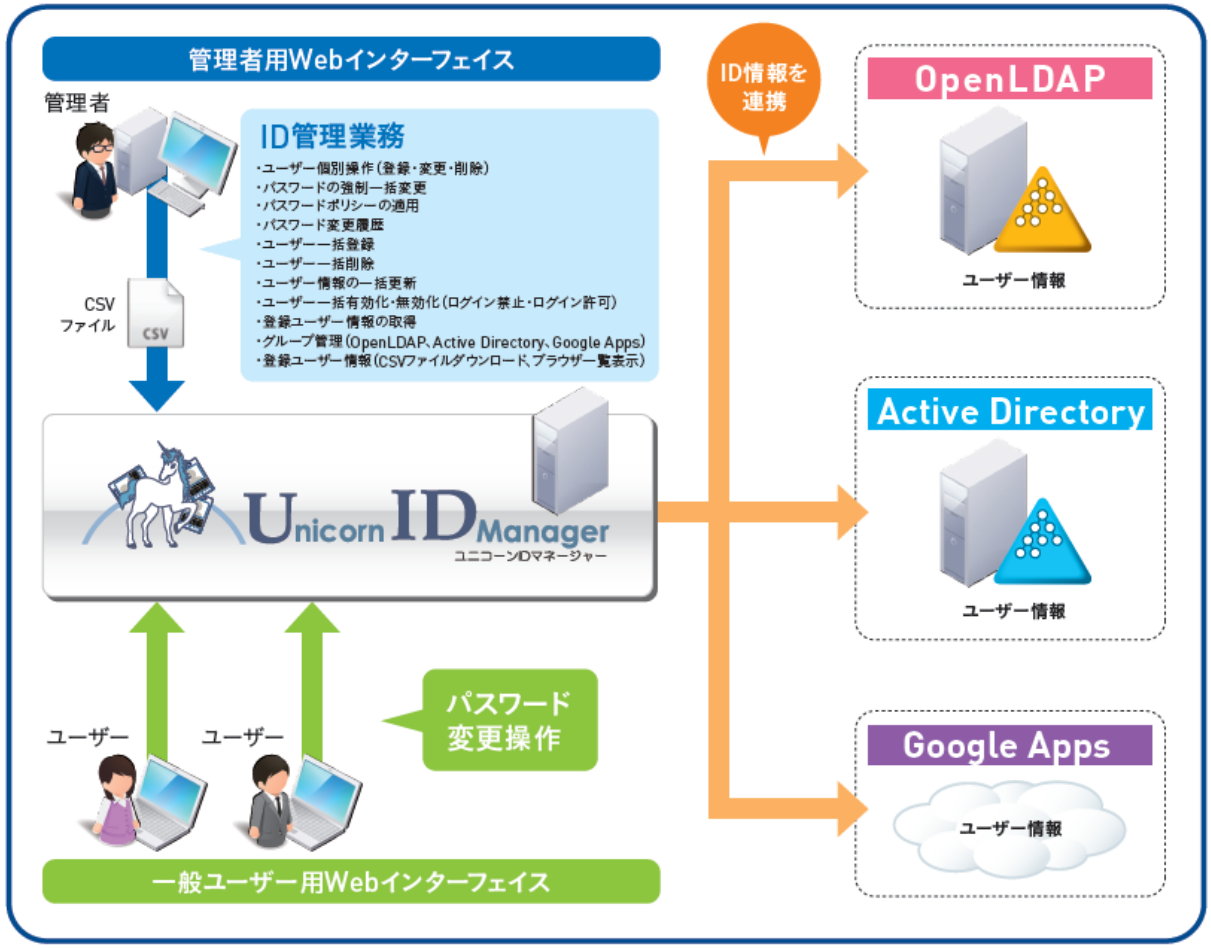
OSSTech独自拡張機能＋総合支援

OSSTech製OpenAMパッケージにTomcatを同梱し、OSSTech製OpenLDAPとの親和性も向上
お客様に最適なシングルサインオン構成の提案、独自カスタマイズによる拡張など、高い技術力と豊富な導入実績に基づく総合的なソリューションを提供

ID管理も オープンソースで

クラウド時代のID管理支援! OSSTech製オープンソース統合ID管理製品

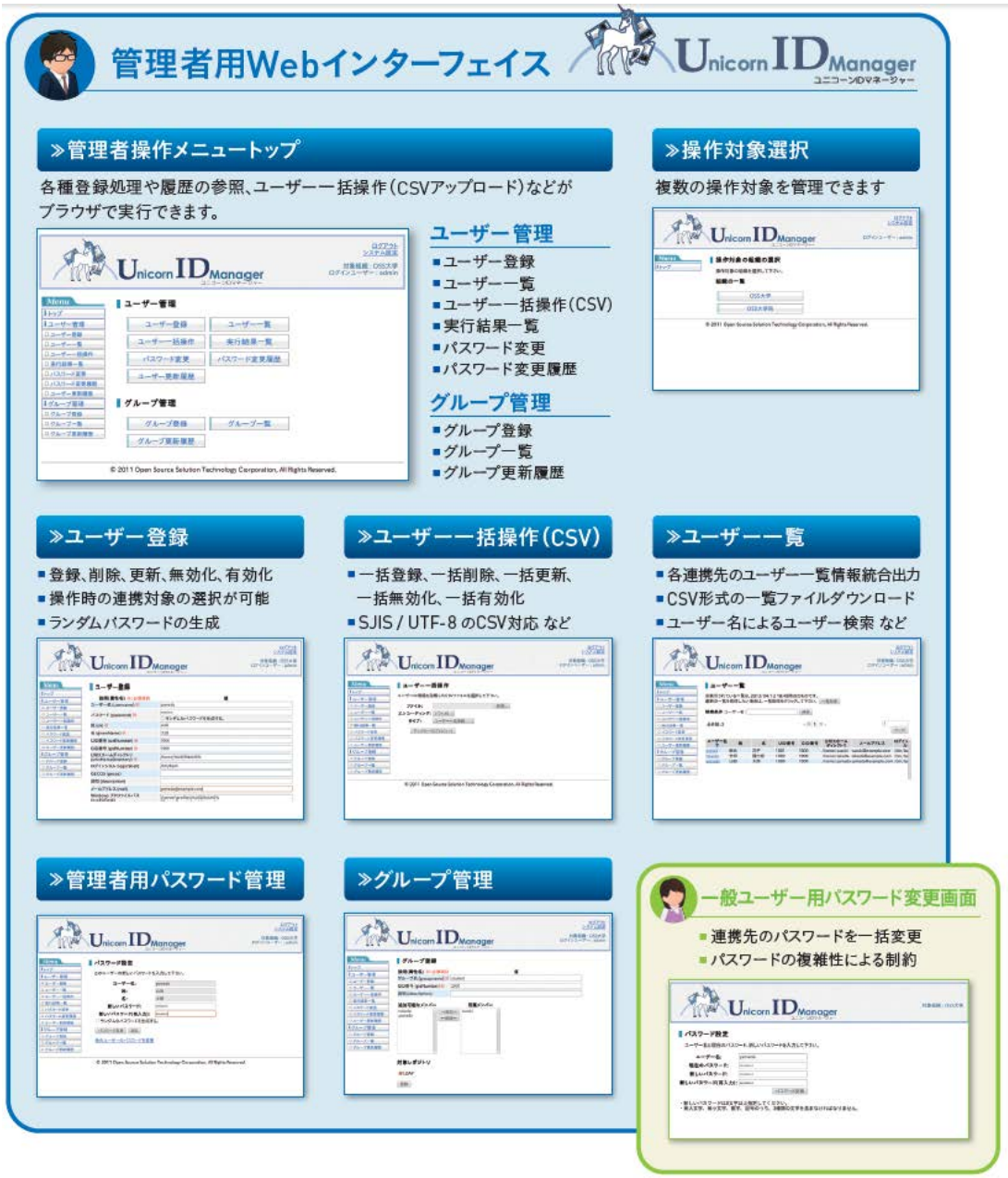
Unicorn IDManager
ユニコーンIDマネージャー



ID管理も オープンソース

シンプルな機能を 低価格で提供

定価(税別)	パッケージ:¥600,000／ノード 年間サポート:¥240,000／システム



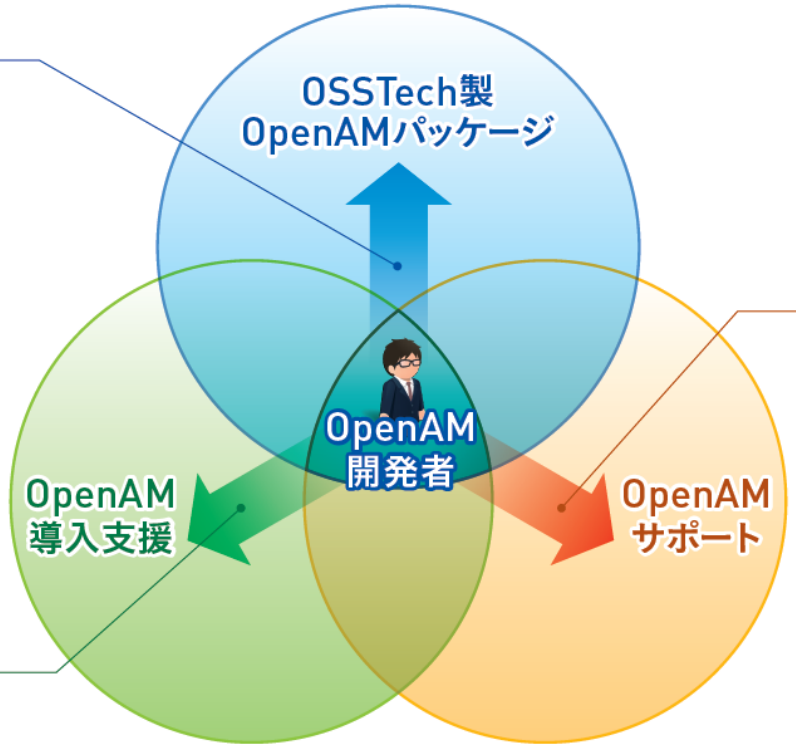
OSSTech製OpenAMは
コミュニティ版とは品質・機能が違う！

経験と実績のOSSTech製SSOソリューション

国内随一の技術力を持つOpenAM開発者が、日本市場でのOpenAM利用を完全バックアップ

安心・安定の製品品質

自社で独自に機能強化、検証を実施したOpenAM製品パッケージ



万全の開発体制とサポート

OpenAM開発者およびオープンソースソフトウェアに関する知識や経験が豊富なメンバーがソースコードの隅々まで解析、確かな技術力で正確かつ迅速なサポートサービスを提供
オープンソースソフトウェアの利点を生かし、OpenAMコミュニティに依存しない長期保守体制も確立

柔軟なソリューション

長年の豊富な導入実績と経験に基づくシングルサインオンシステム構成を提案
独自モジュール開発や独自カスタマイズも考慮する柔軟な対応

OSSTech製のOpenAMはここが違う

最先端のシングルサインオン基盤に必要な機能・特長を自社開発し、安定した運用を支援します

OSSTechがリリースする日本版OpenAMの特長

OpenLDAPの親和性向上	要望の多いパスワードポリシー対応とLDAP更新時のタイムラグに対処し、OpenLDAPとの組み合わせを実運用レベルへ
マトリックス型認証モジュール	2次認証としてニーズの高いマトリックス型認証サーバとの連携モジュールを追加開発
代理認証モジュール	アプリケーション改修が不要となるSSO連携モジュールを開発し、ラインナップに追加
nginxポリシーエージェント	新鋭の高速Webサーバーnginx用ポリシーエージェントを開発、サポート
Shibboleth 連携モジュール	学術系で採用の多いShibbolethとの共存、ハイブリッドSSO化を行う連携モジュールを開発
RPMパッケージ	rpmコマンドだけでインストール、アップデートが可能なパッケージ構成を採用
Tomcatを同梱	動作に必要なJavaアプリケーションサーバーTomcatをOpenAM向けに調整し同梱
バグ修正	安定度を優先し版数はコミュニティ版に追随せず、セキュリティ・運用に関わる修正を優先的にバックポートまたは自社開発
カスタマイズ後のサポート	案件向け独自改修を行った場合でも、開発元ならではの確実なサポートを提供可能

OSSTech版カスタマイズ

- OpenLDAPと親和性向上＞OSSTech独自拡張
  - OpenAMにOpenLDAP専用の設定を追加
  - OSSTech社製OpenLDAP向け拡張スキーマを用意
  - OSSTech社製OpenLDAPをSHA-2対応にアドオンモジュール開発

OSSTech版カスタマイズ

- Tomcatとの親和性向上＞環境の統一化
  - OpenAM向けにパラメータを調整したTomcatを
    OpenAMとセットで提供

- パッケージング＞セットアップ容易化
  - RPMパッケージとして提供
  - Windowsインストーラー提供

OSSTech版カスタマイズ

- OpenAM10からのバックポート
  - 重要な修正、必要な機能をバックポート
  - 多重構成でのセッション数の共有
  - ポリシーの設定方法の改善
  - メモリリークの修正
- プラットフォーム毎にエージェントを提供
  - RHEL5でも動作可能なApache2.2エージェントの提供
- 日本語化
  - 画面の文字化け対策

nginx用PolicyAgent

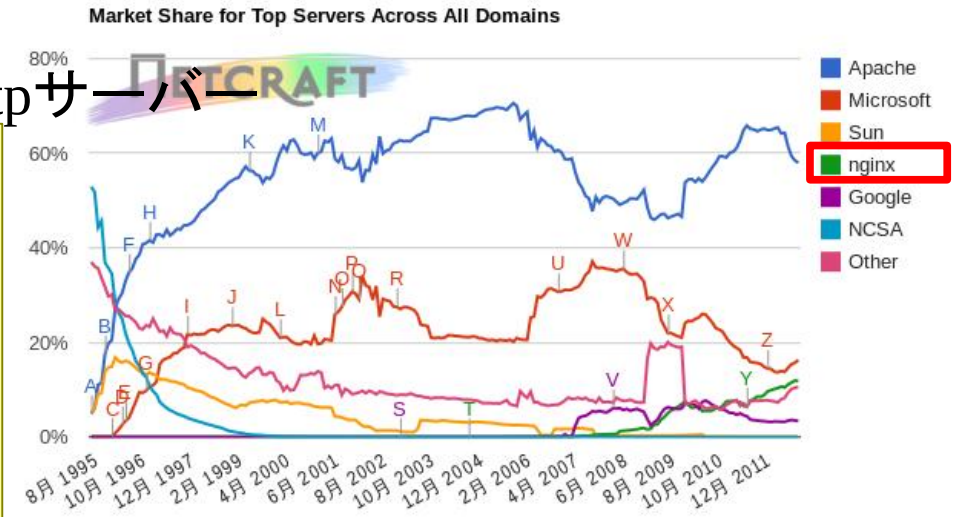
- Apache**より早いリバースプロキシを構築したい**

  - Apacheによるリバースプロキシよりスケーラビリティが欲しい

  - nginx※用 Policy Agentの開発

※nginxとはスケーラビリティ、
パフォーマンスに優れる第三のhttpサーバー

netcraftの2011年資料
第3位にnginxが伸びてきている
apacheほど多機能ではないが、
リバースプロキシ利用では
十分の機能を持たせられる



OpenAMの認証方式

多要素認証による
認証強化

OSSTech

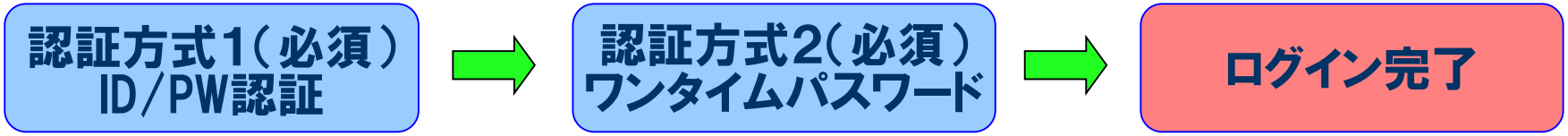
多要素認証

**複数の認証方式を組合わせて認証を行うことにより
シングルサインオンの認証を強化する**

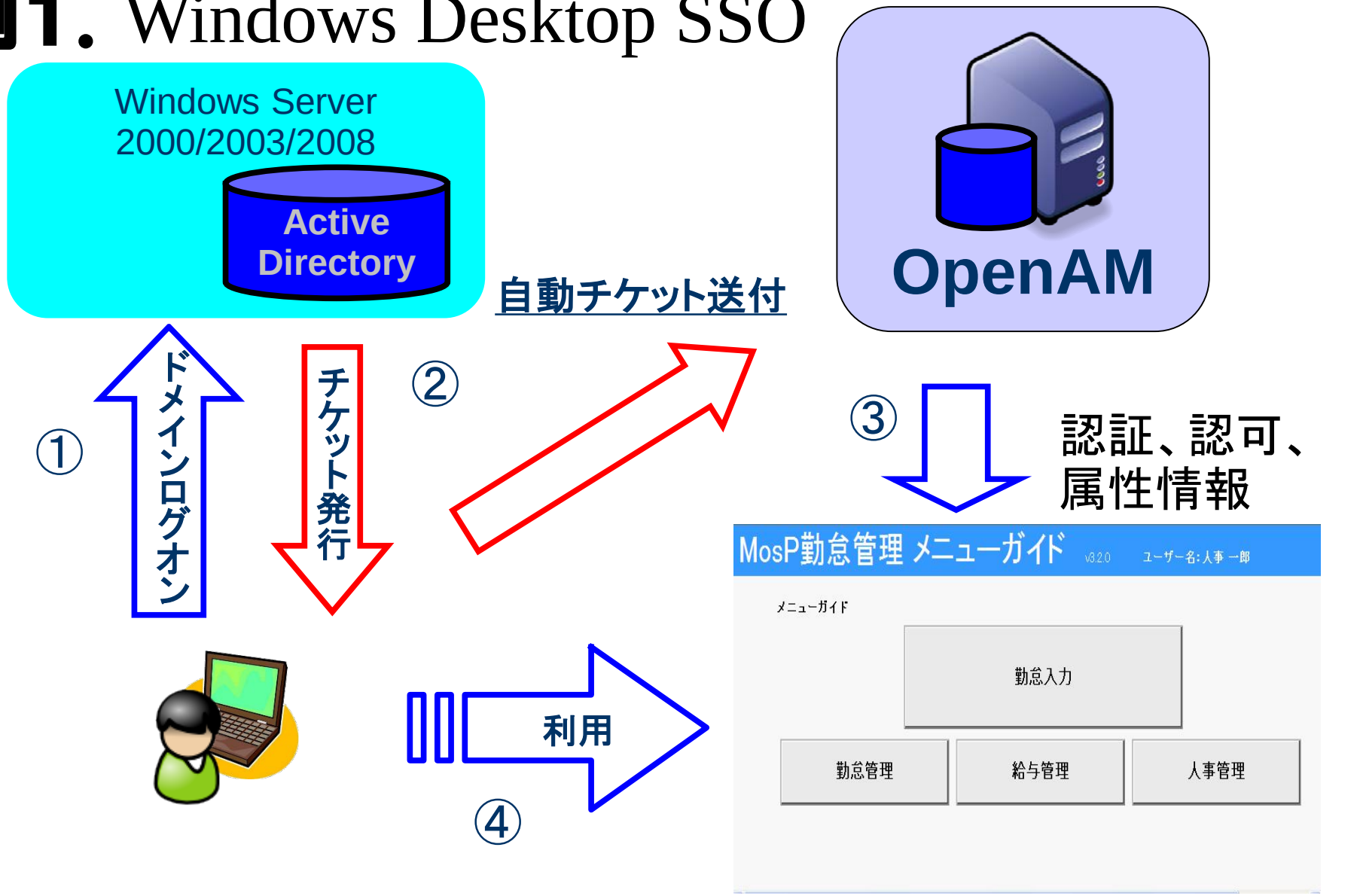
- 厳密なユーザ認証
  - 異なるタイプの認証方式を組合わせることが重要
- 使い勝手の向上
  - いつも同じ認証方式が使えるとは限らない
  - 状況により要求される認証の精度が異なる
- 認証方式間での連携
  - 組合わせて使うことを前提にしている認証方式もある

認証連鎖

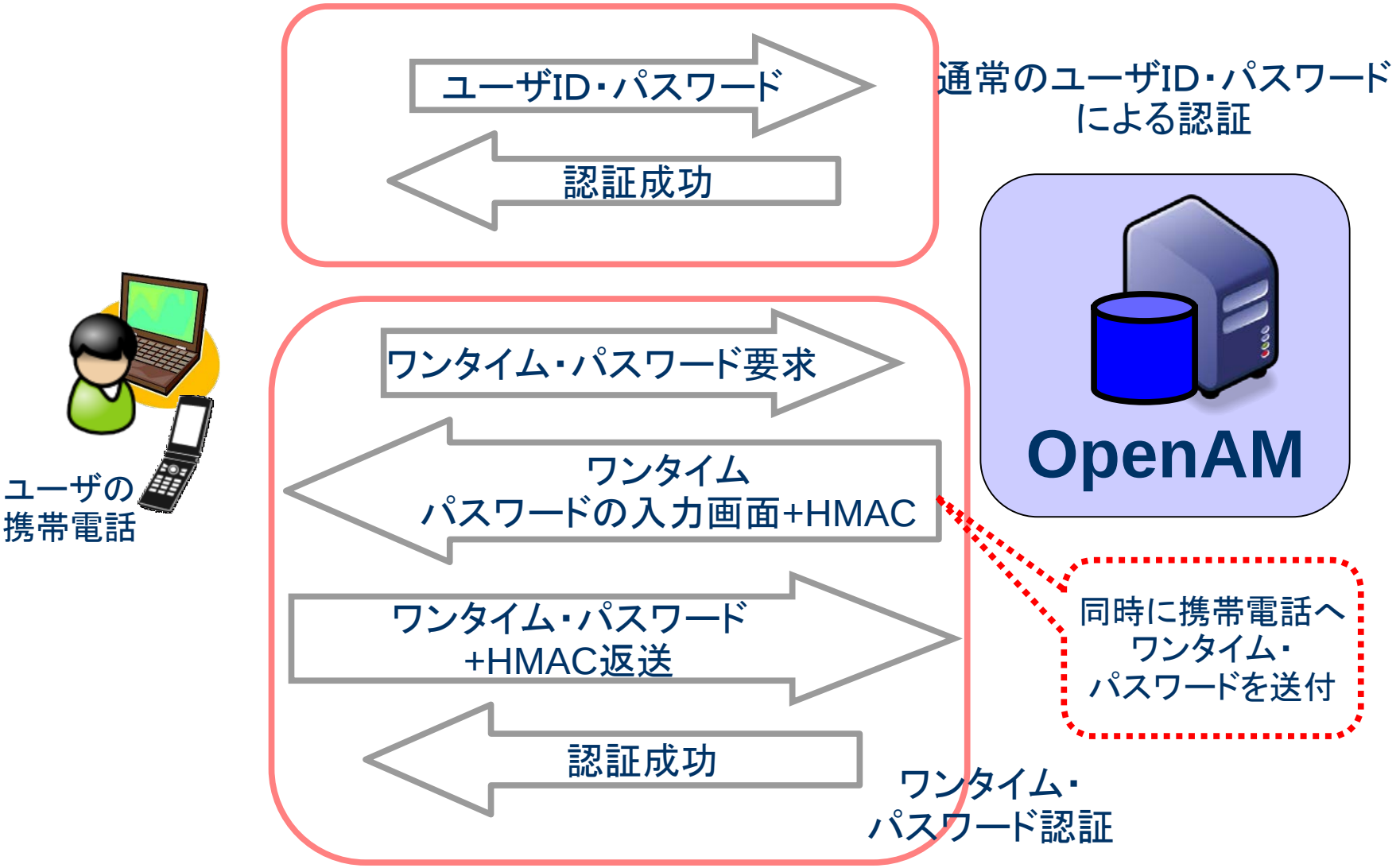
- 多要素認証の必要性
  - 複数の認証方式を組合わせて認証を行うことにより個々の認証方式の欠点を補完
- **認証連鎖**
  - 複数の認証方式を組み合わせて利用可能
  - 認証方式にはそれぞれ適用条件を指定する
    - 必須：失敗したらそこで終了
    - 十分：成功したらそこで終了
    - 必要：成功しても失敗しても次に継続
    - 任意：認証結果には関係しない付随的な処理



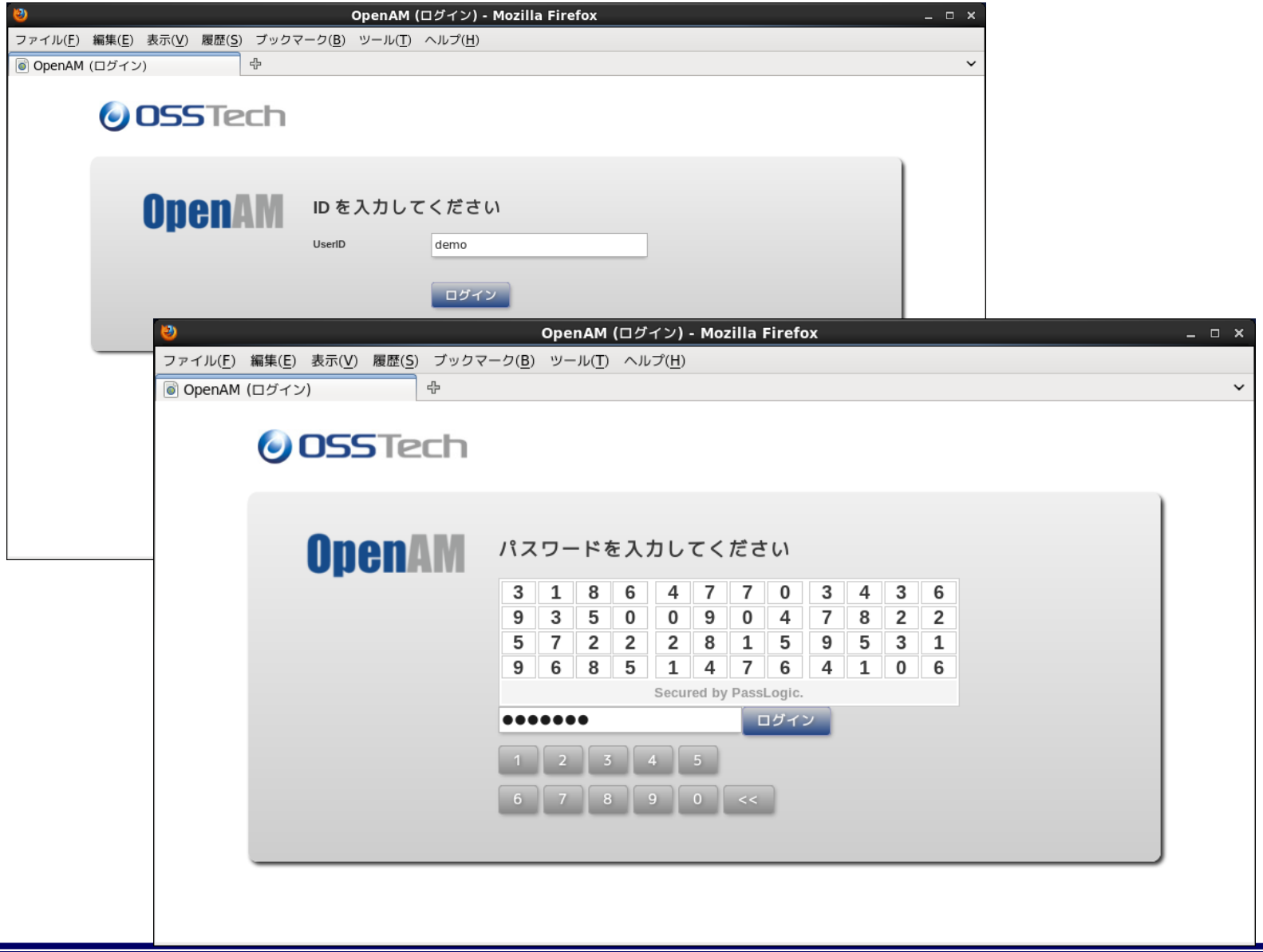
例1. Windows Desktop SSO



例2. 携帯電話を使ったワンタイム・パスワード



マトリックス型認証モジュール（Passlogic連携）



アダプティブ・リスク認証モジュール

リスク評価に基づく認証強度の選択

OSSTech

アダプティブ・リスクの考え方

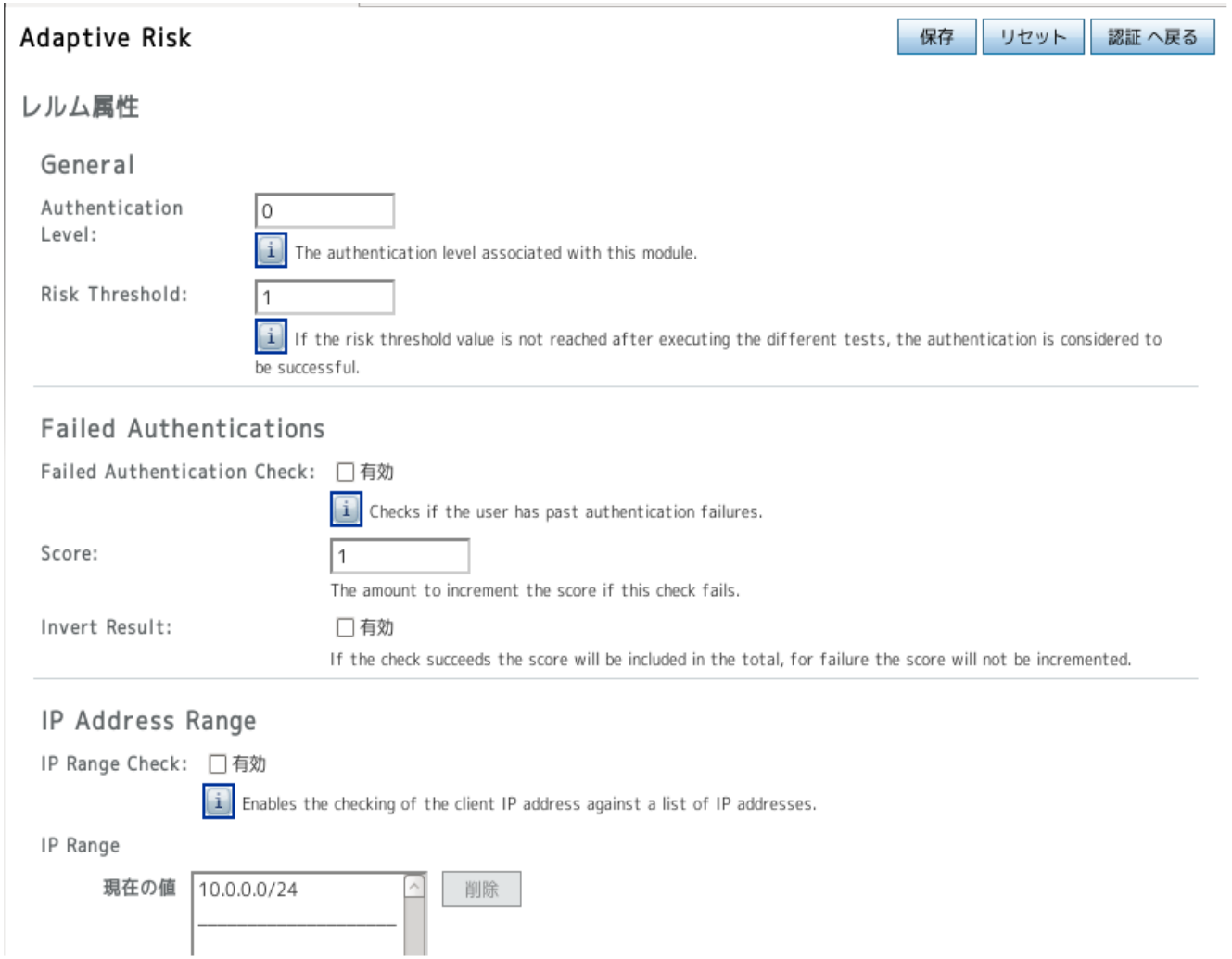
- 認証時にリスクを評価することによりリスクに見合った認証方式を動的に追加
  - Risk Based 認証とも呼ばれる
  - リスクの評価
    - 予め各リスクについて重み付けを行う
    - 認証時にすべてのリスクについてそれらを合算する
    - 既定の閾値を超えた場合は認証失敗とする
  - 認証連鎖への組み込み
    - 多要素認証のなかのひとつの認証方式
    - 認証連鎖の定義

リスクの例

．リスクが高いと評価される例

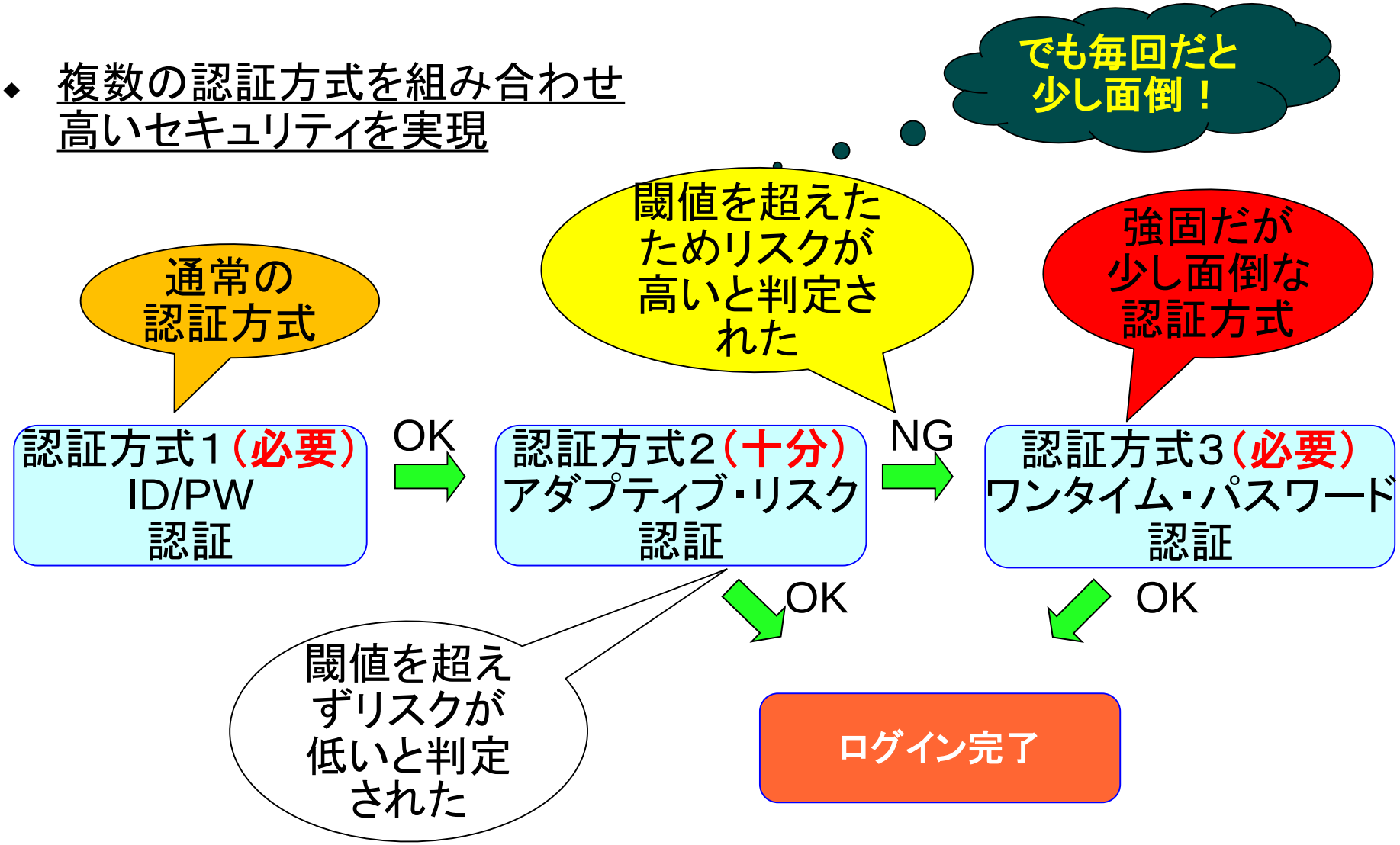
- パスワードを間違えたユーザからのアクセス
  - 最終的に正しいパスワードを入力したとしてもリスクは高い
  - アカウント・ロックとの併用／代用
- 長期間アクセスがなかったユーザからのアクセス
- 特定のIPアドレスの範囲からのアクセス
  - 例：社外からのアクセス
- 特定の地域からのアクセス
  - 例：日本国外
- いつもとは異なる端末からのアクセス（複数可）
- いつもとは異なるIPアドレスからのアクセス（複数可）
- 特定の属性を持つユーザからのアクセス
  - 例：所属部署が営業とか？

アダプティブ・リスク認証モジュールの設定



認証連鎖と組み合わせたソリューション例

- 複数の認証方式を組み合わせ
  高いセキュリティを実現



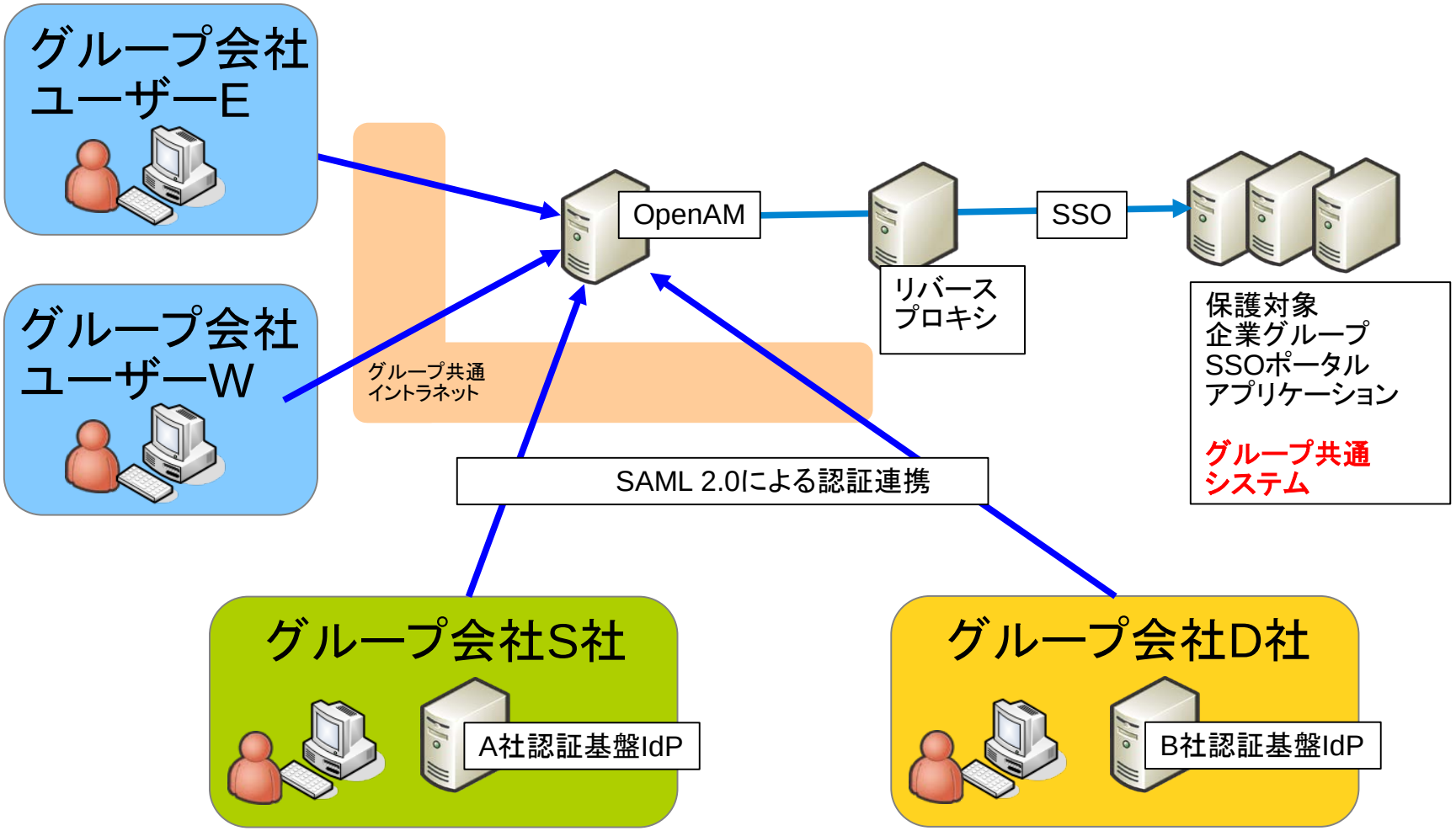
OpenAMによるシングルサインオン システム導入事例

OSSTech

某通信会社グループ共通 シングルサインオンシステム

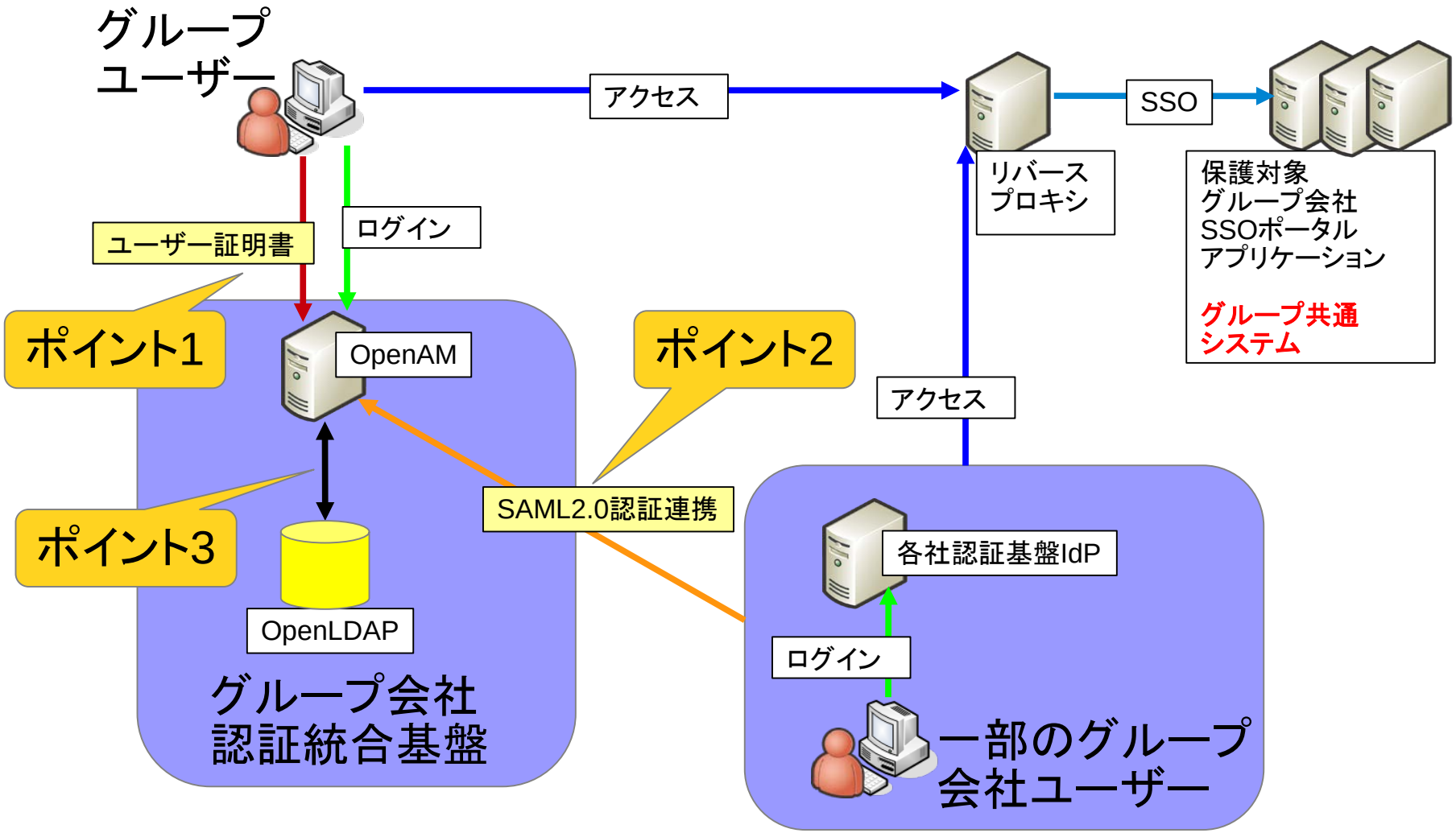
- ユーザー総数　約25万人
- ID/パスワードとユーザー証明書の多要素認証（認証連鎖）
- 一部グループ会社ユーザーはSAML 2.0対応IdPによる認証連携
- OpenLDAPのパスワードポリシー対応モジュールの開発
- 保護対象アプリケーションとの連携はPolicyAgentを用いたリバースプロキシ型

某通信会社グループ　全体構成図



一部グループ会社では各社の認証基盤をIdPとしてOpenAMと連携

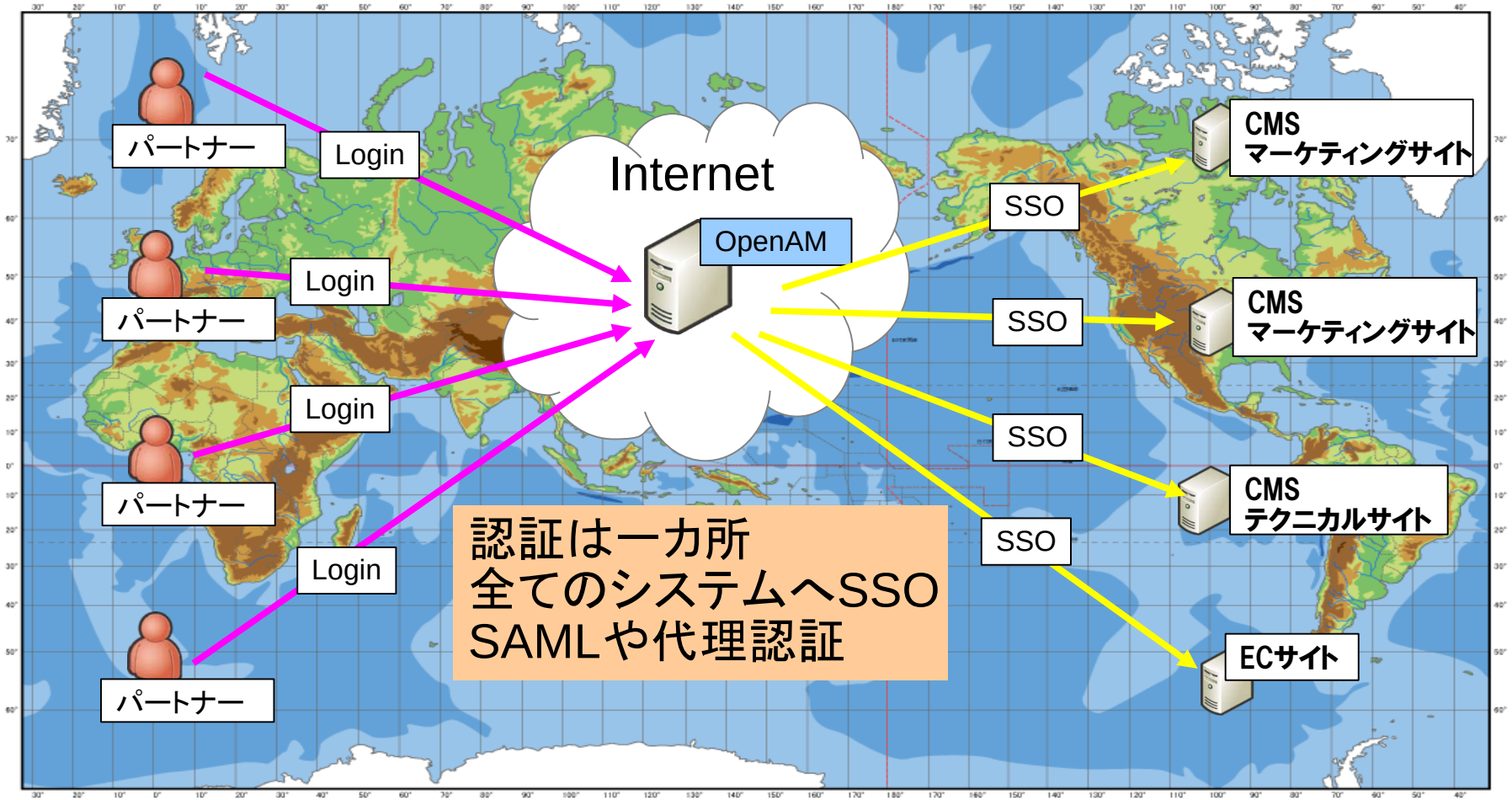
某通信会社グループ 構築のポイント



某総合電機メーカー
シングルサインオンシステム

- 規模：グループ企業7社、約5000人、海外22拠点
  今後拡大予定
- 海外ディーラー向けの技術情報やマーケティング情報のCMSおよびECサイトへのシングルサインオン
- CMS, ECサイトとの連携はOpenAM PolicyAgentとお客様開発の連携モジュール
- SAML認証と代理認証を利用
- 対象ユーザー、保護対象アプリケーションはインターネット上に点在

某総合電機メーカー　構成図



福岡大学様 システムの特徴

規模

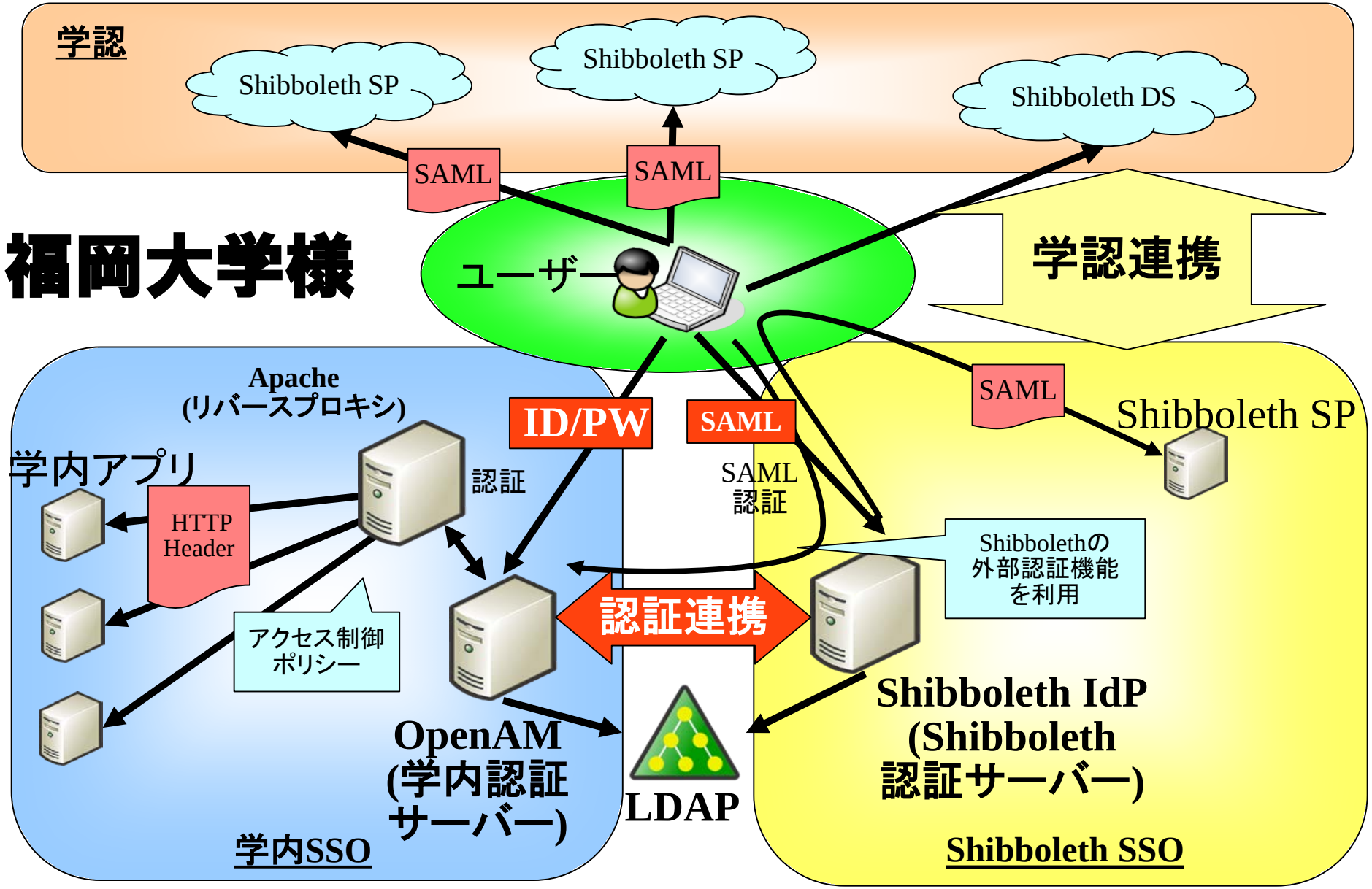
9つの学部、2つの病院、22の付置施設で構成される総合大学
学生数 約21,000人
教職員数 約3,000人

ミッション

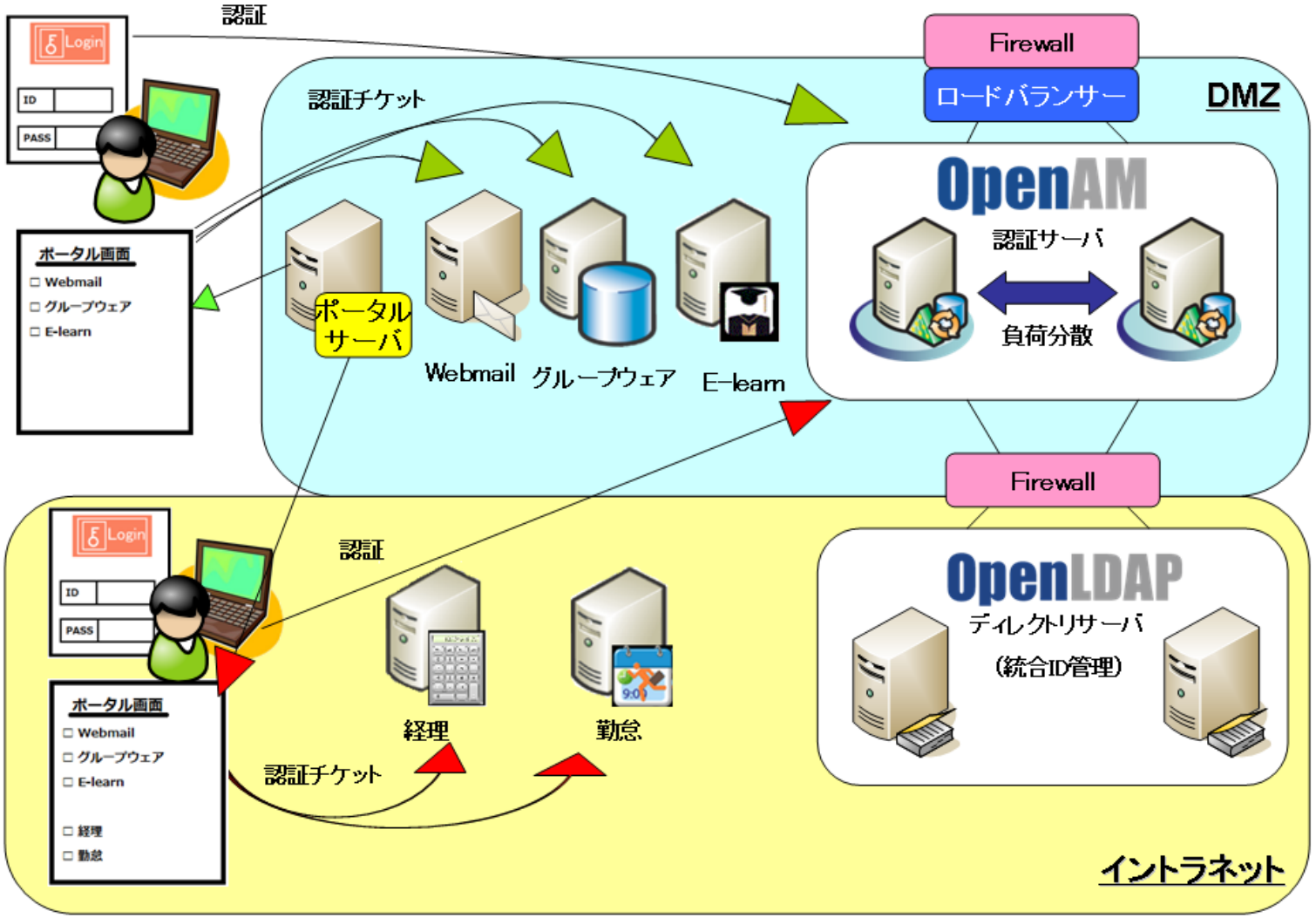
高い拡張性と柔軟性を持つ先進的SSO基盤の構築

日立製作所とオープンソース・ソリューション・テクノロジで実現

- **OpenAMとShibbolethによるハイブリッド型SSO基盤**
  - **システムのシングルサインオンを実現する認証基盤をOpenAMとShibbolethを使って実現**
  - **様々なアプリケーションとのシングルサインオンを実現する基盤**
  - **ユーザーは1度の認証で学認と学内のアプリケーションを利用可能**



北見工業大学様

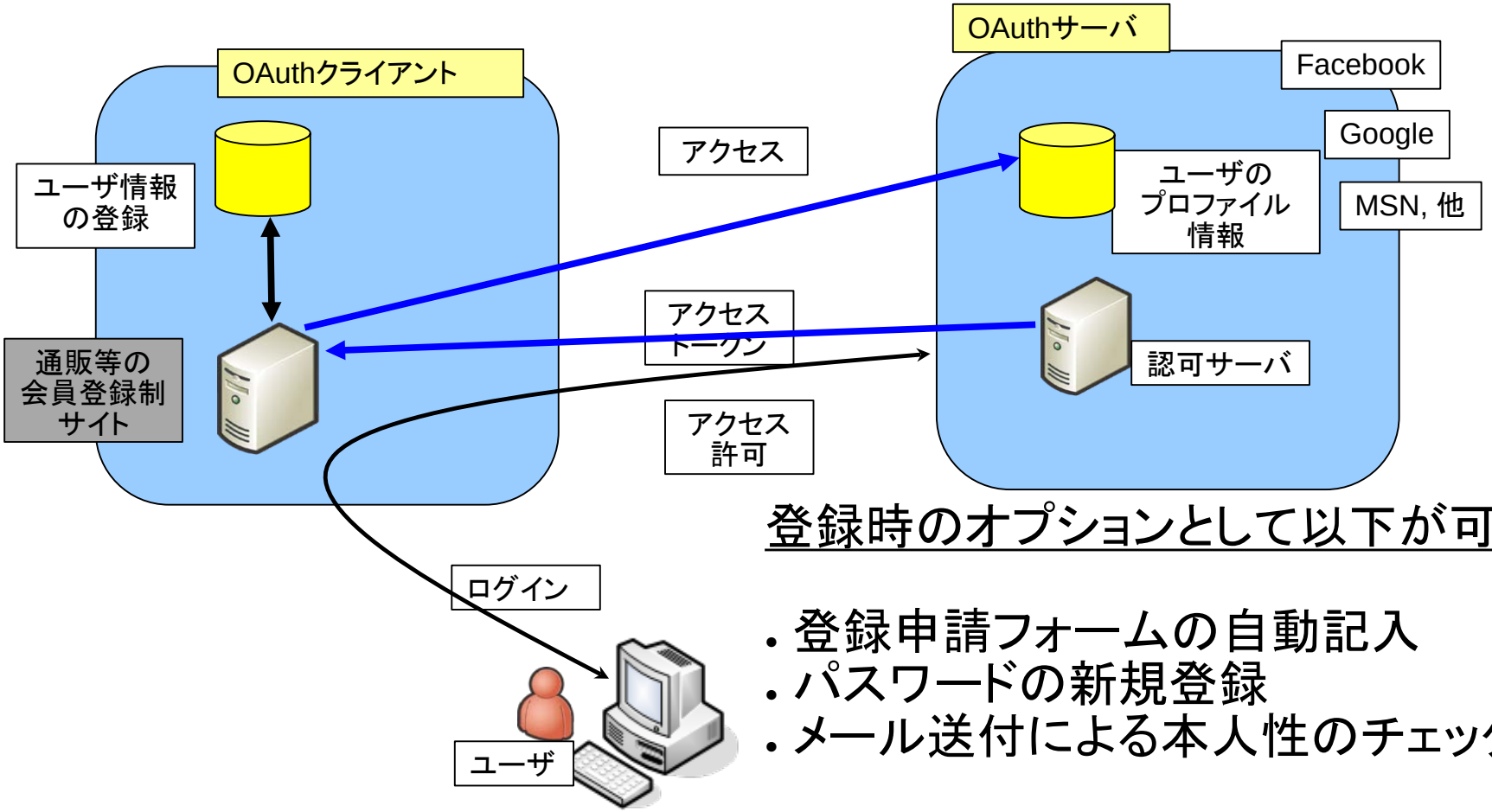


進化し続けるOpenAM

新機能と
製品ロードマップ

OSSTech

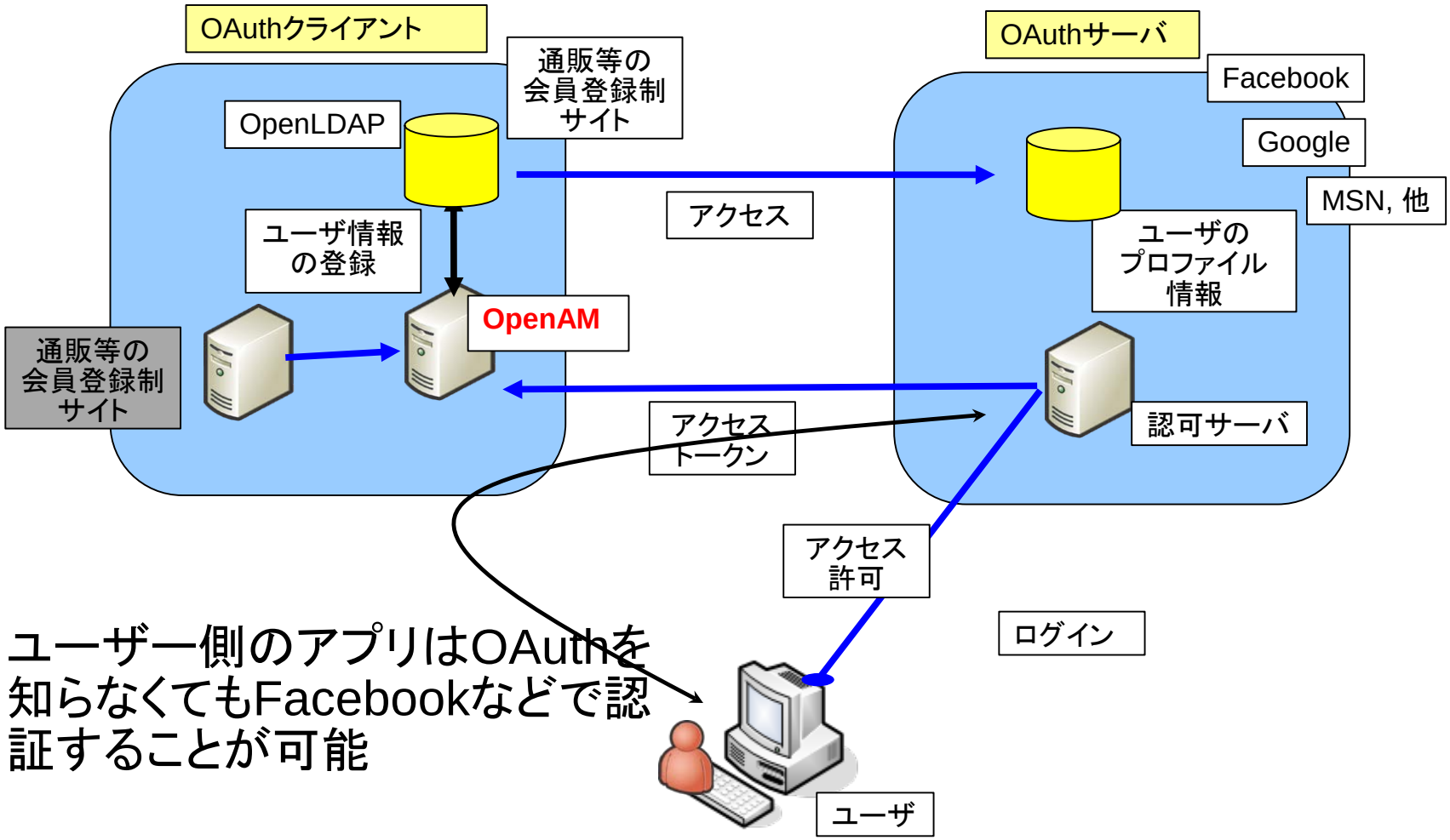
自社のサービスにFacebookなどのアカウントでログインしてもらうOAuth クライアント機能



登録時のオプションとして以下が可能

- 登録申請フォームの自動記入
- パスワードの新規登録
- メール送付による本人性のチェック

OAuth クライアントとしてOpenAMを使う



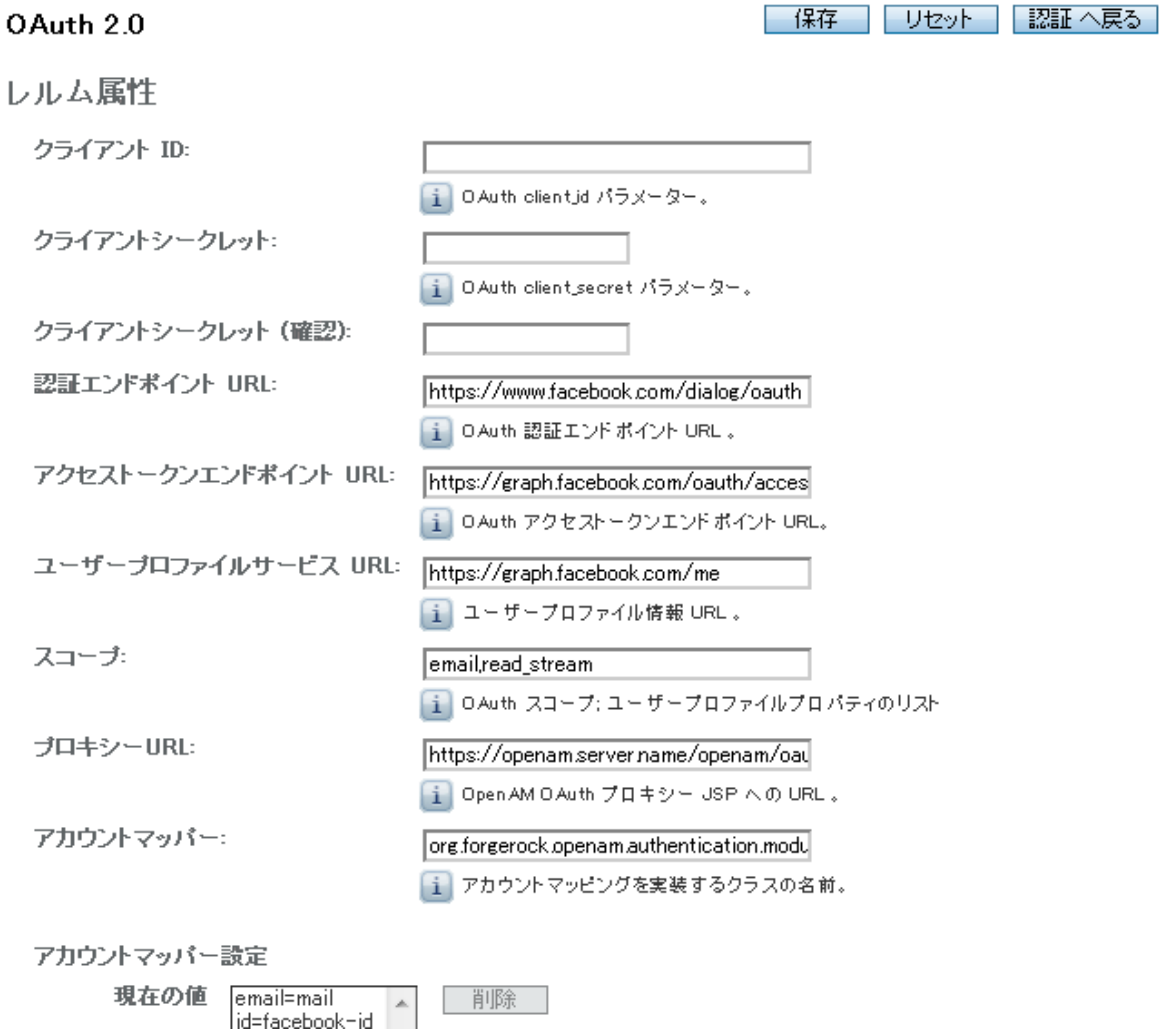
ユーザー側のアプリはOAuthを知らなくてもFacebookなどで認証することが可能

OAuth 2.0 のクライアントとして使う設定

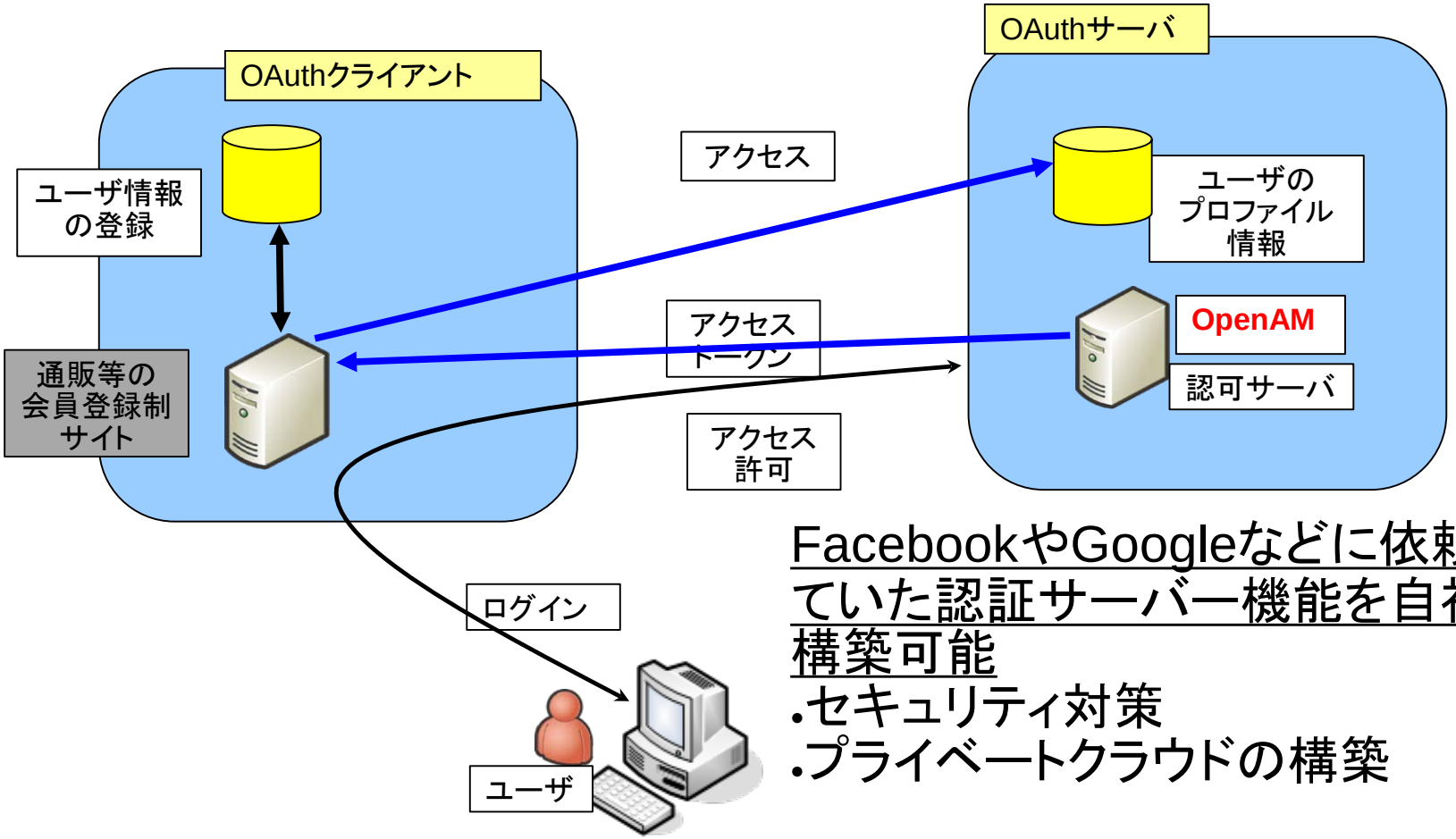
管理コンソールで

簡単設定

詳細手順は弊社ホームページで紹介中



Oauth/OpenID Connectサーバ機能：Facebookなどの認証サーバーを独自に構築可能



FacebookやGoogleなどに依頼していた認証サーバー機能を自社で構築可能

- セキュリティ対策
- プライベートクラウドの構築

「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