企業・大学における
シングルサインオン・システムの
最新技術動向と導入事例

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

OSSTech

お問い合わせ info@osstech.co.jp

講師紹介
オープンソース・ソリューション・テクノロジ
会社紹介

OSSTech

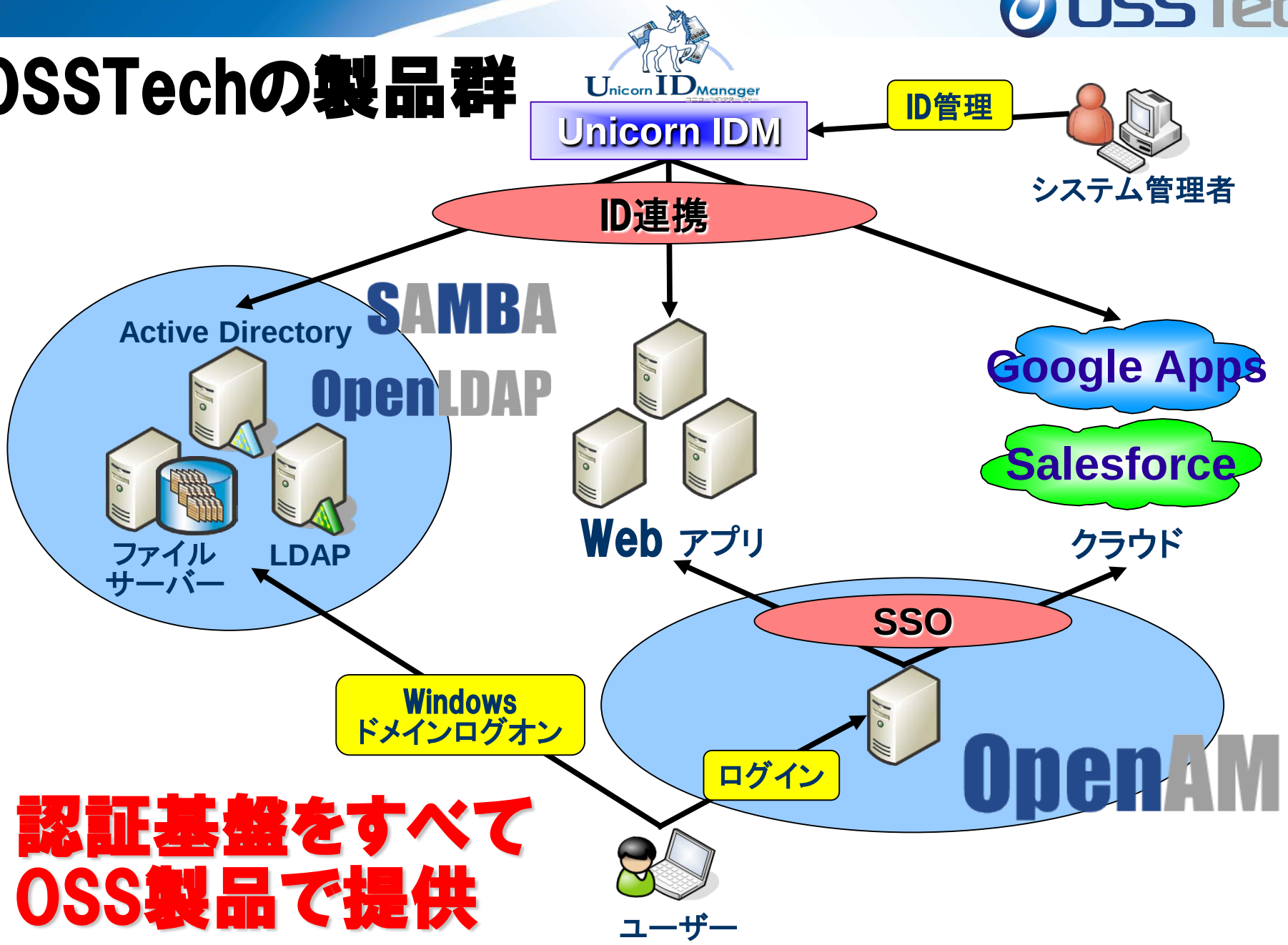
講師紹介

- 役　職 ： 代表取締役 チーフアーキテクト
- 氏　名 ： 小田切 耕司（おだぎり こうじ）
- 所属団体等
  - OpenAMコンソーシアム 副会長
  - OSSコンソーシアム 副会長
  - 日本LDAPユーザ会設立発起人
  - 日本Sambaユーザ会初代代表幹事
- 執筆関係
  - 日経Linux 2011年9月号～2012年2月号 連載中
    - 『Linux認証のすべて』（第1回～第6回）
    - http://itpro.nikkeibp.co.jp/linux/
  - ASCII.technologies 2011年2月号
    - 『キホンから学ぶLDAP』
    - http://tech.ascii.jp/elem/000/000/569/569412/
  - 技術評論社 Software Design 2010年9月号
    - 第1特集 クラウド対策もこれでOK！
      統合認証システム構築術
      OpenAM／SAML／OpenLDAP／Active Directory
    - http://gihyo.jp/magazine/SD/archive/2010/201009
  - @IT やってはいけないSambaサーバ構築：2008年版
  - 2006年5月 技術評論社 LDAP Super Expert
    - 巻頭企画
    - ［新規／移行］LDAPディレクトリサービス導入計画

オープンソース・ソリューション・テクノロジ株式会社

- **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

- Samba for Linux/Solaris/AIX
  - ADの代替、高性能NASの代替
- 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
- OpenAM for Linux/Windows/Solaris/AIX
  - Tomcat, OpenLDAP対応で高機能なシングルサインオン機能を提供(旧OpenSSO)
- Unicorn ID Manager for Linux/Solaris
  - Google Apps, Active Directory, LDAPに対応した統合ID管理

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

- 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
- LDAP Account Manager for Linux/Solaris
  - 管理機能の弱いOSSのLDAP/SambaにWebベースのGUIを提供
- 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
- Mailman for Linux/Solaris
  - 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
技術動向

OSSTech

SSO(OpenAM)導入動向

- クラウドの普及により、SSO(シングルサインオン)が急速に普及中
- IaaSやPaaSも増えつつあるが、やはりSaaSのGoogle Apps(大学／企業)とSalesforce(企業)をまず導入するケースが多い
- 企業ではSalesforceのセキュリティ強化を目的にOpenAM導入するケースが多い
- 大学ではGoogle AppsとイントラネットやShibbolethを連携させるケースが多い
- MS Office365を導入してSSOするにはADFSと社内アプリのSSO連携が必要になってきた。
- 企業では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
- IaaSやPaaSも普及し始め、これらの上で構築された社内向け個別アプリのSSOも普及しだしてきた。

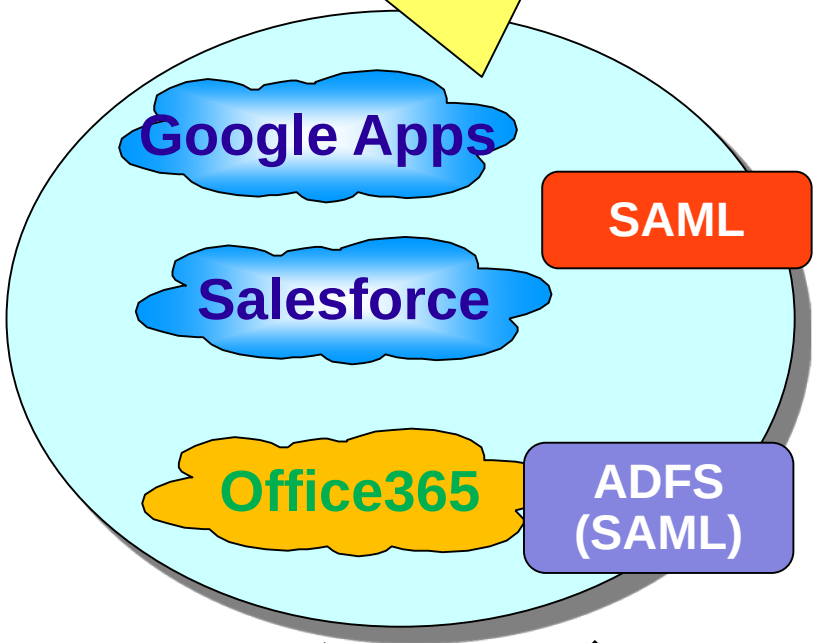
OpenAMで実現する
シングルサインオン・ハブ

オープンソースのOpenAMだから
高機能・安価に実現できる

OSSTech

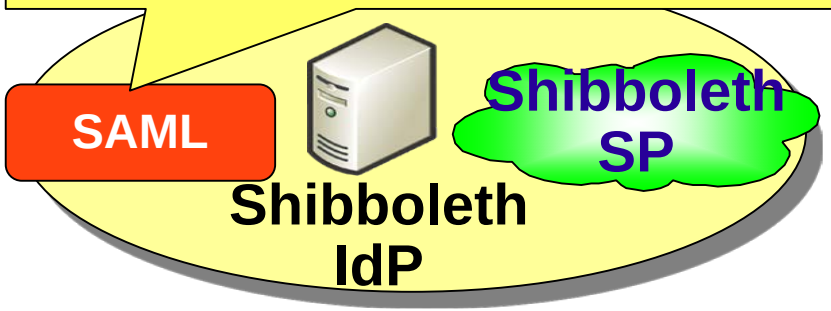
混在する複数のSSO環境

SAML IdP を導入して
SSO を実現



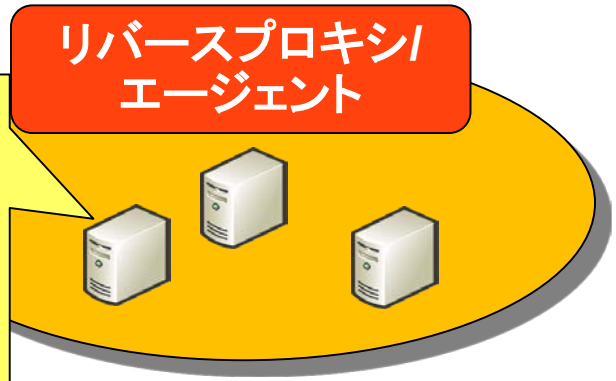
クラウドSSOセグメント

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)



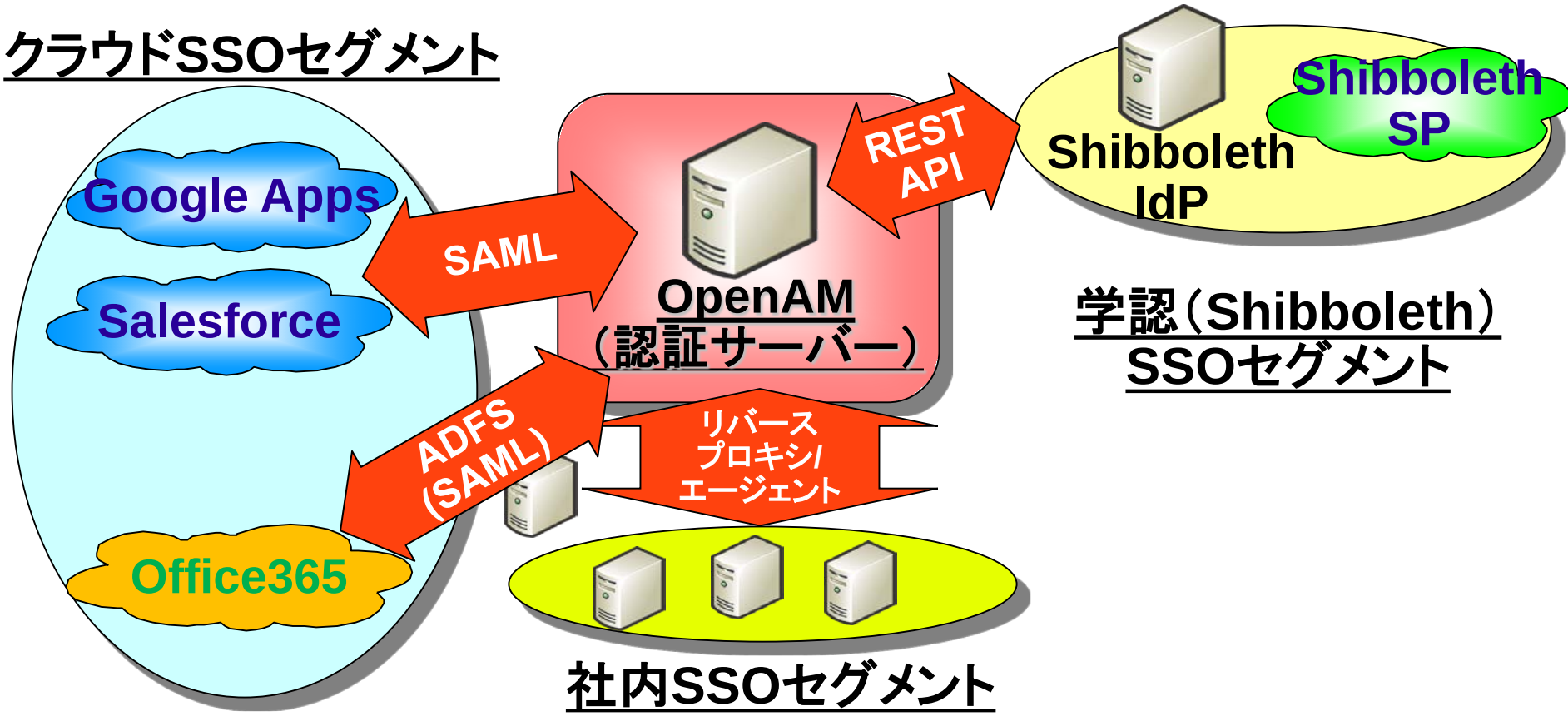
学認（Shibboleth）
SSOセグメント

App改修不可能なため、代理認証/リバースプロキシでSSO を実現



社内SSOセグメント

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

シングルサインオン・ハブを実現するための機能

- 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

OpenAMによるシングルサインオン システム導入事例

OSSTech

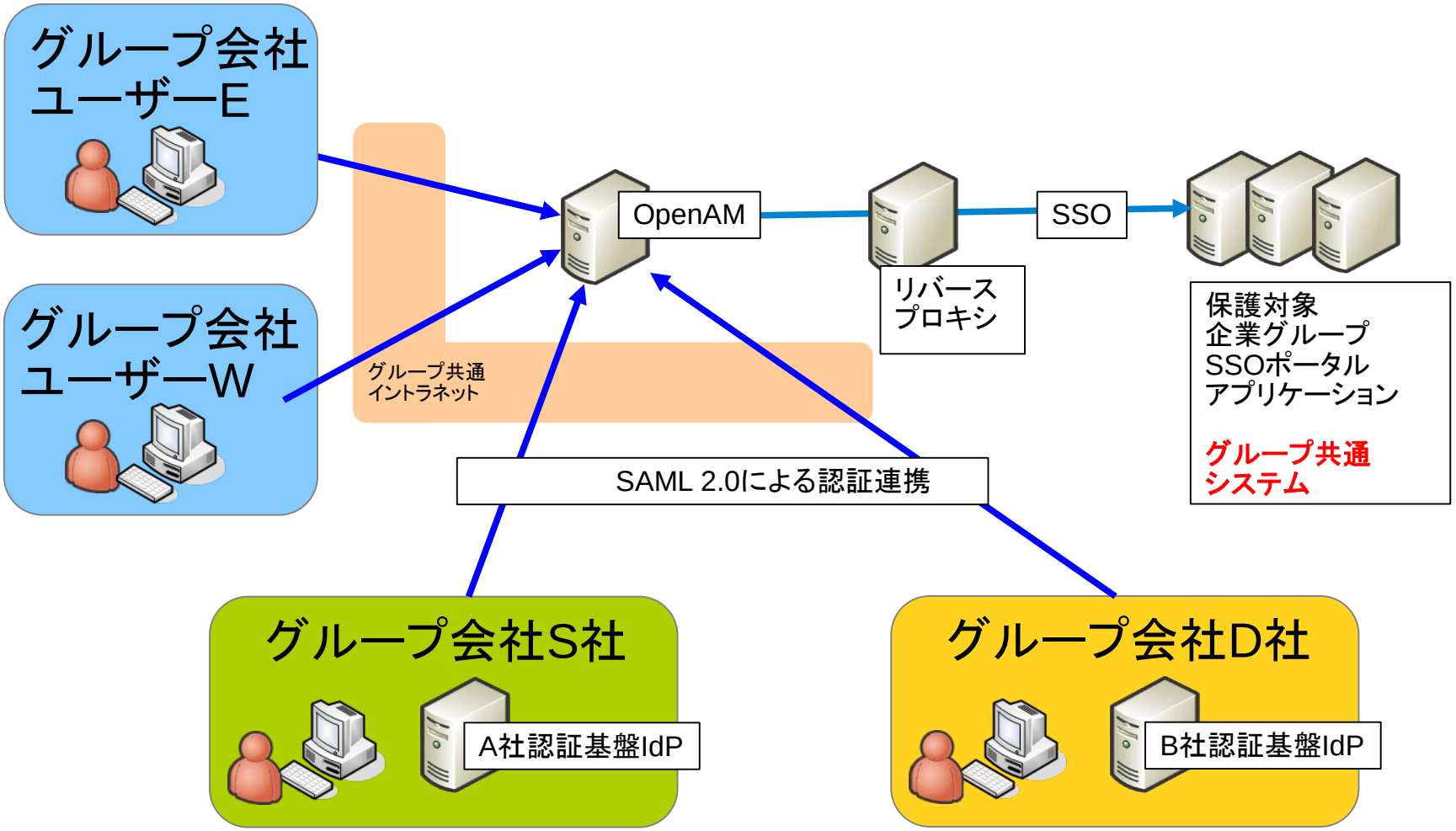
某通信会社グループ共通
シングルサインオンシステム

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

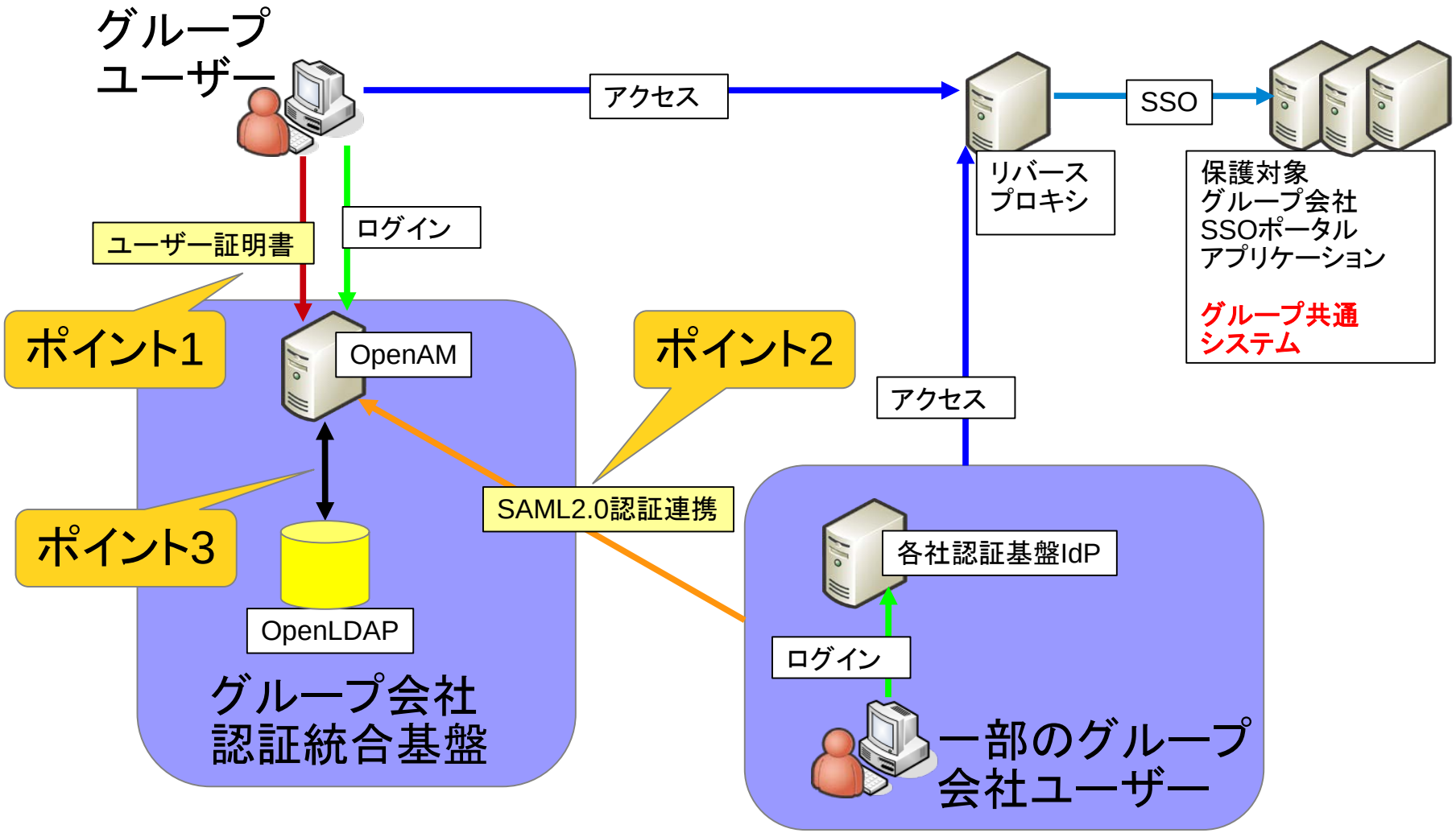
- ユーザー総数　約25万人
- ID/パスワードとユーザー証明書の多要素認証（認証連鎖）
- 一部グループ会社ユーザーはSAML 2.0対応IdPによる認証連携
- OpenLDAPのパスワードポリシー対応モジュールの開発
- 保護対象アプリケーションとの連携はPolicyAgentを用いたリバースプロキシ型

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

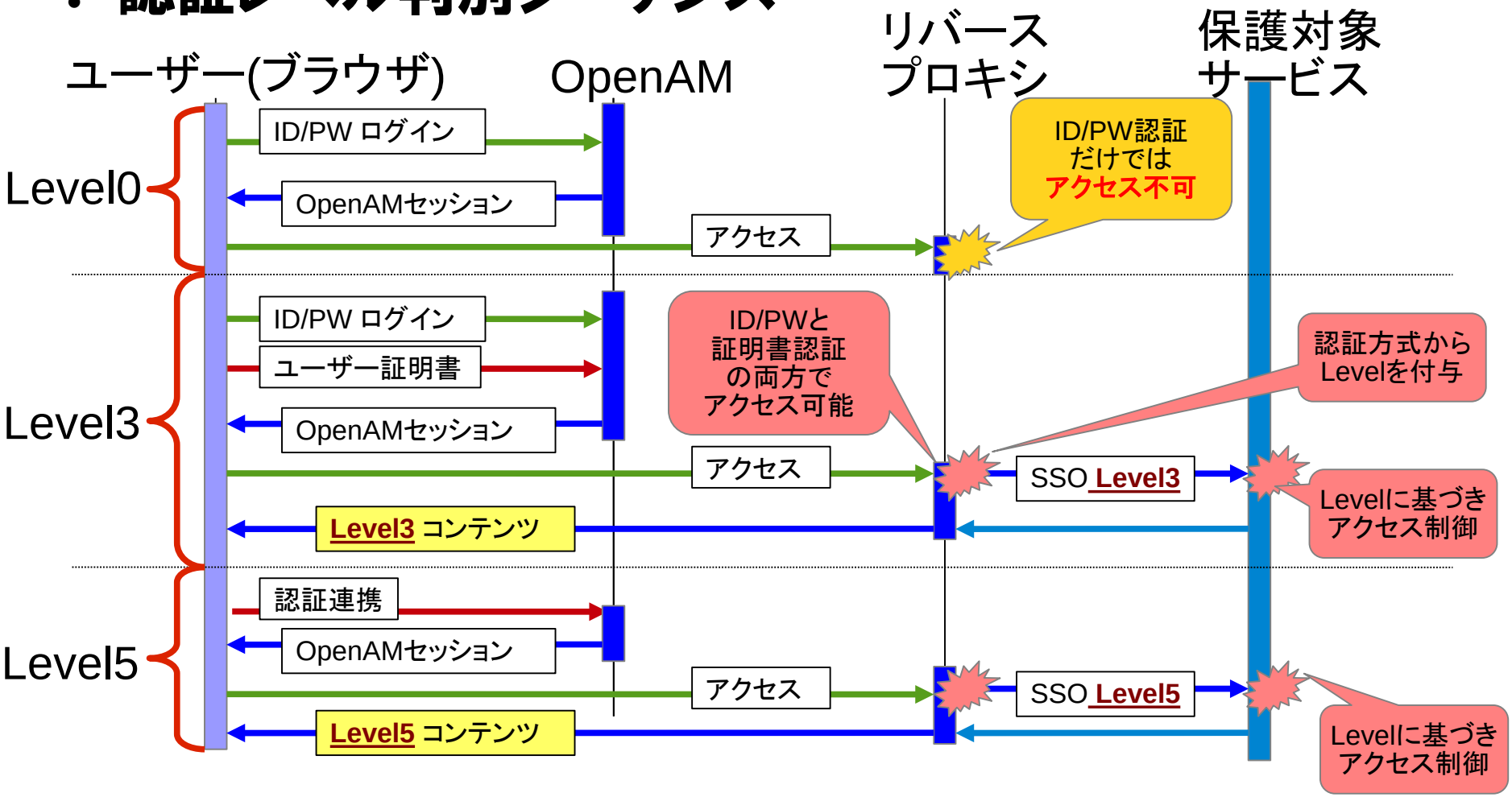


多要素認証

- ポイント1
  - ID/パスワードとユーザー証明書を用いた多要素認証
  - 「認証連携」での接続方法も、同等の認証レベルをセットするカスタム認証モジュールを開発
  - OpenAMリバースプロキシのポリシーでレベルをチェックしアクセス制御

多要素認証時の認証・認可シーケンス

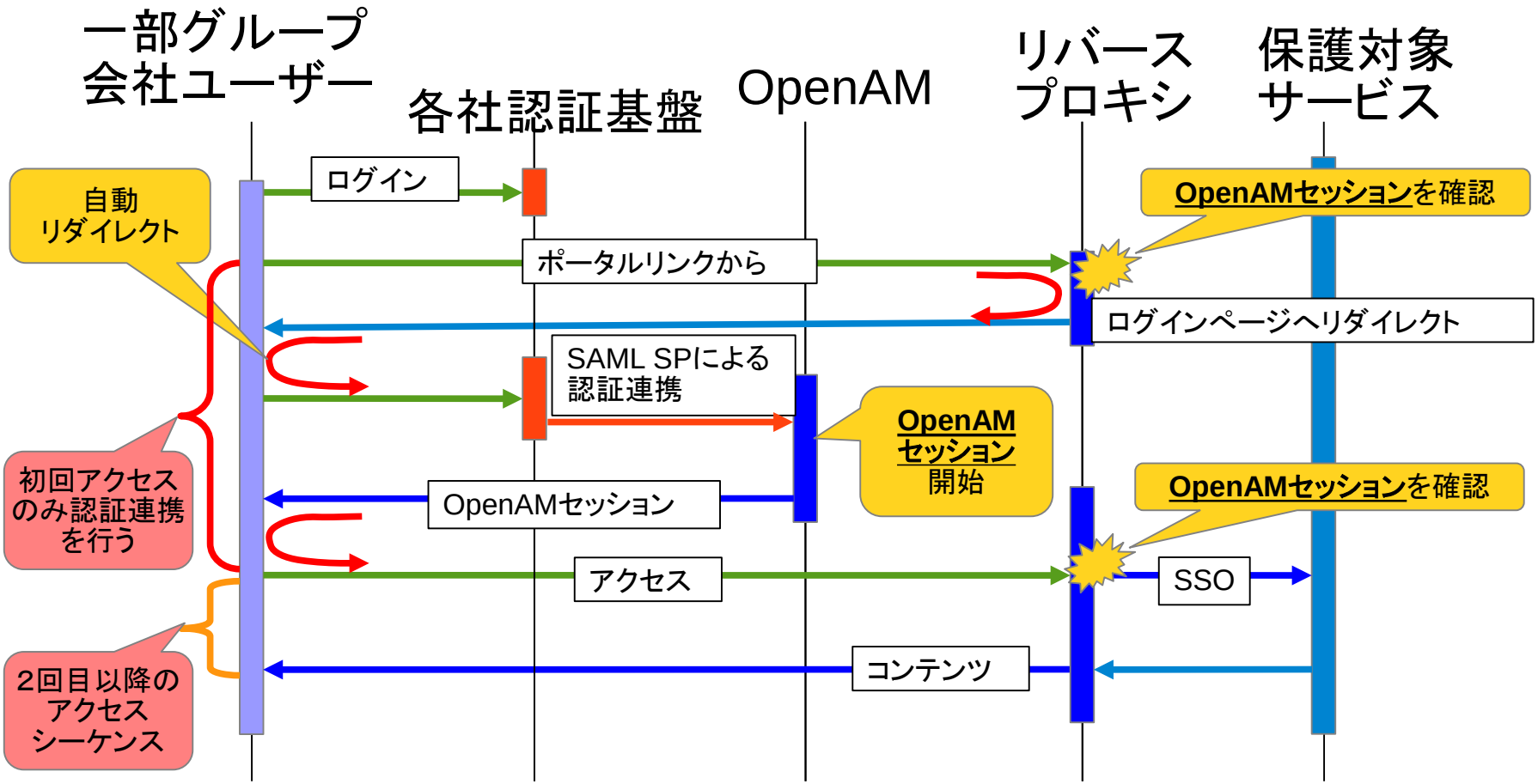
- 認証レベル判別シーケンス



異なるIdP製品との認証連携

- ポイント2
  - 一般的にユーザーはOpenAMで認証を行う。
  - 一部のグループ会社ユーザーは各社認証基盤のIdPで認証を行い、OpenAM保護下のグループ会社SSOポータルアプリケーションとはSAML認証連携でアクセス可能とする。

異なるIdP製品との認証連携シーケンス

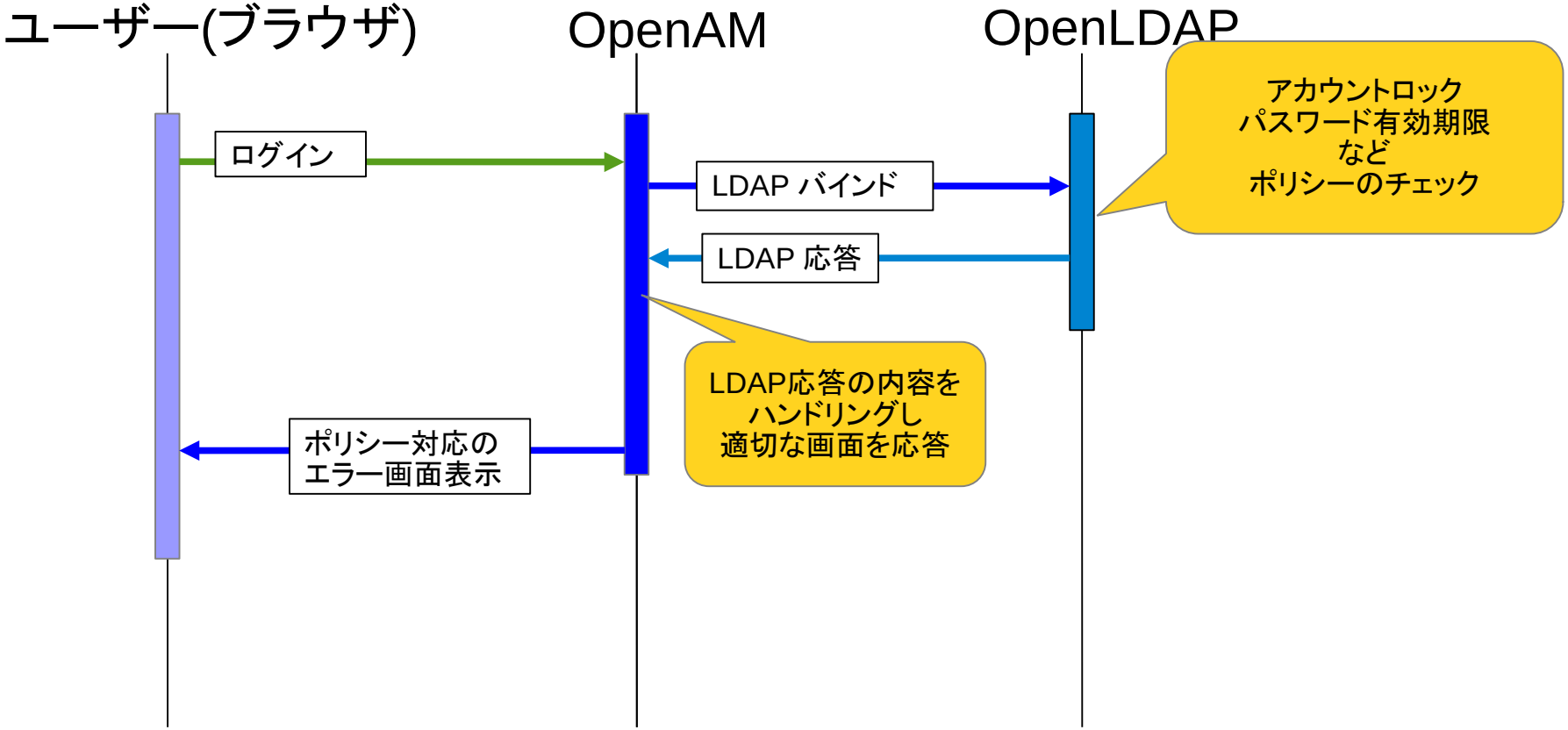


OpenLDAPポリシーへの対応

- ポイント3
  - OpenAM 9系では対応していないOpenLDAP（RFC標準）のアカウントポリシーエラー対応のためOpenAMの拡張開発を行った。
  - 拡張を行ったOpenAMは、パスワード有効期限切れなどOpenLDAPからの戻り値を判定し、任意のURLへ遷移する。

OpenLDAPポリシーへの対応

- OpenLDAPエラー情報判定シーケンス



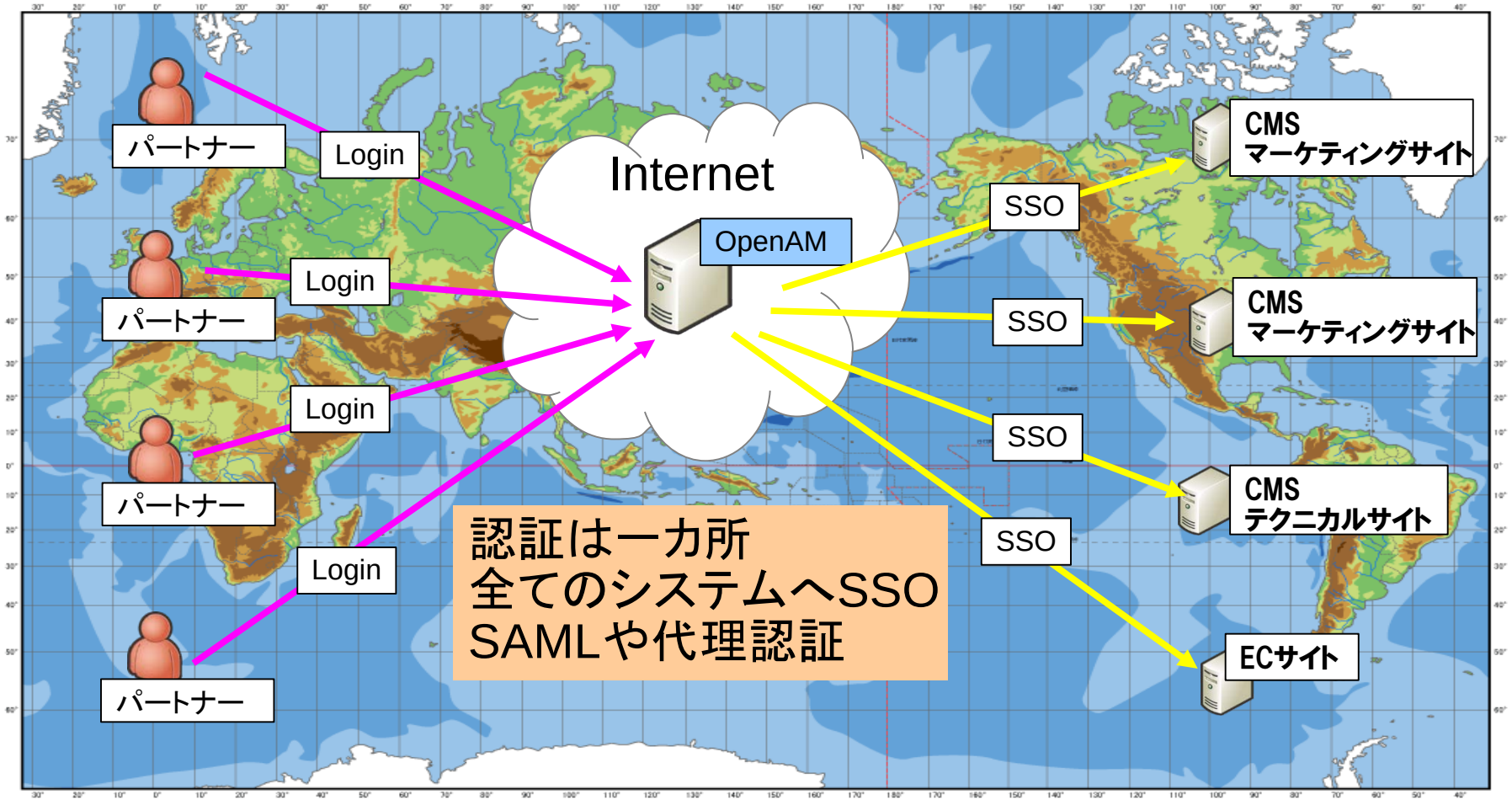
某総合電機メーカー シングルサインオン システム

OSSTech

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



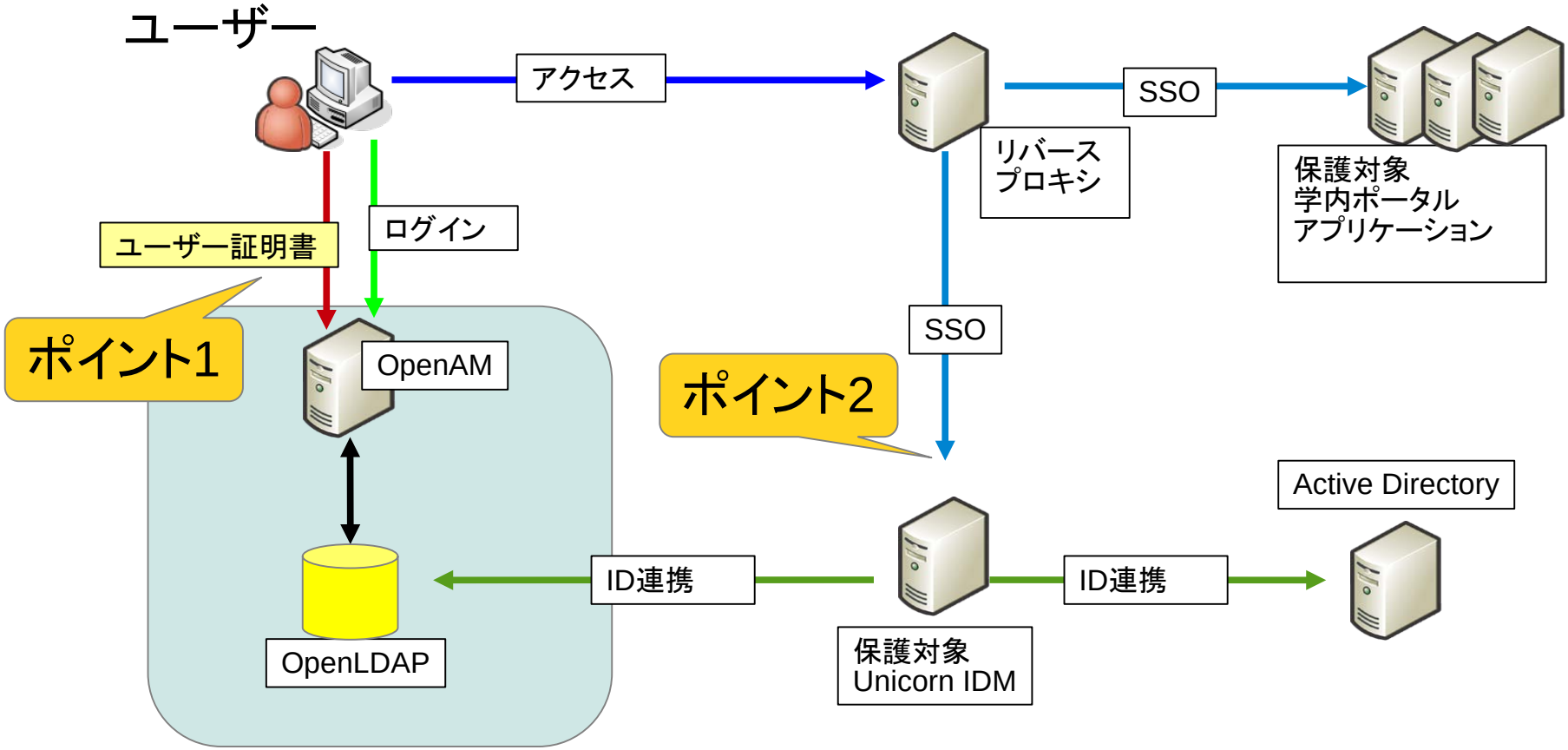
国立大学法人
名古屋工業大学

OSSTech

名古屋工業大学様　事例のポイント

- 規模 学生数 約5,800人 教職員数 約510人
- 旧Sun製品の置き換え
  - 旧Sun製品(Sun Java System Access Manager)からの移行を実現
  - 旧Sun製品のOracle後継製品を導入する場合はコスト高
  - Sun Java System Access Managerの後継であり、OSSのOpenAMを採用
  - 他にもLDAPにOpenLDAP, ID管理にUnicorn IDMと積極的にOSSを採用
- ICカードによる認証とID/パスワードによる認証の使い分け
  - アクセスリソースに対しての認証レベルの使いわけ
  - 「ICカードによる証明書認証」と「ID/パスワードによる認証」の二つの認証方式を用意
  - 重要なリソースへのアクセスの際にはより安全なICカードで認証したユーザーのみをアクセス可能とした
- 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

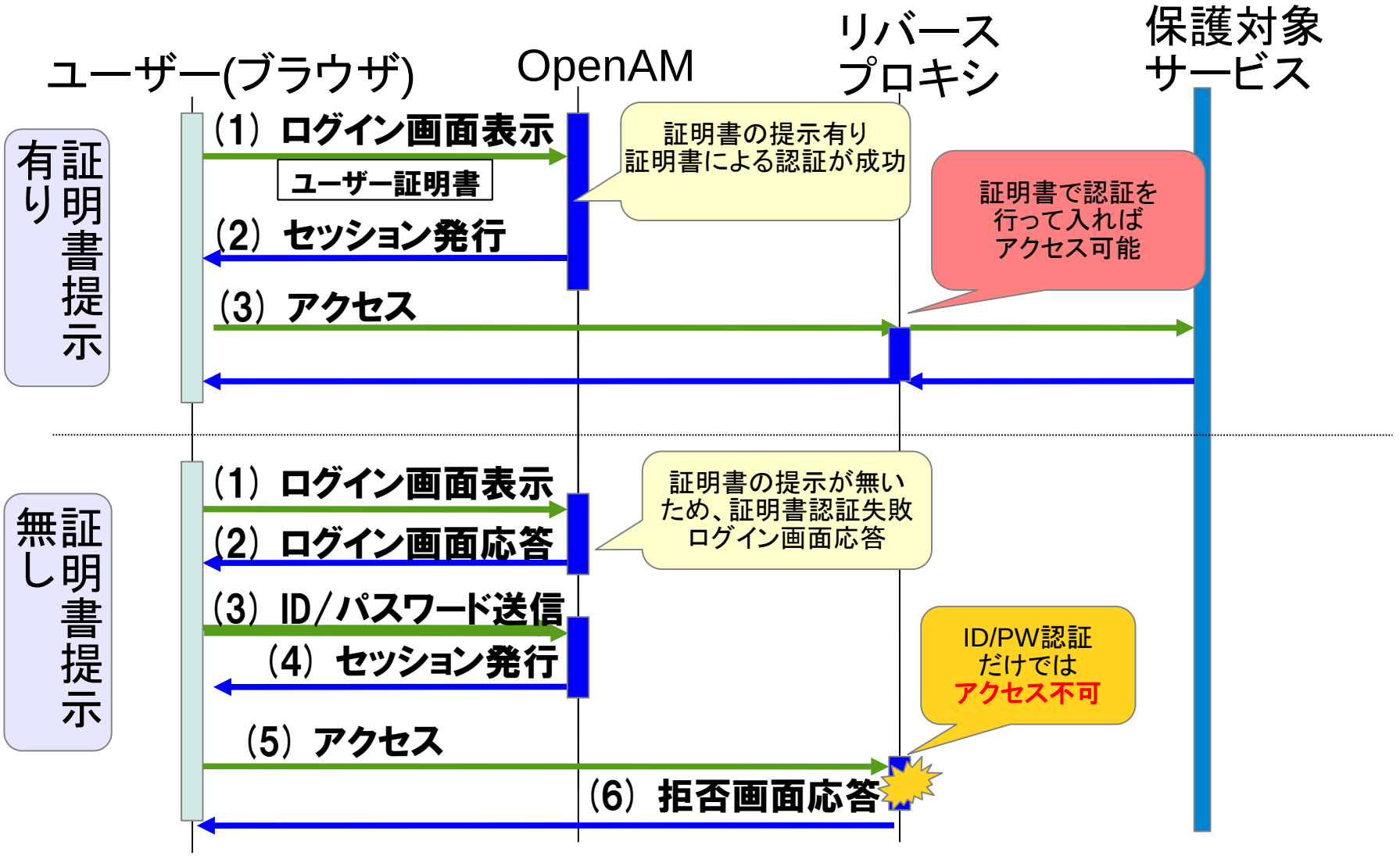
名古屋工業大学　構成図



名古屋工業大学　認証の使い分け

- ポイント1
  - ICカードを使った証明書認証を基本とする
  - 証明書認証に失敗した場合(証明書の提示が無い)にログイン画面を表示しID/パスワードを用いた認証
  - 証明書認証とID/パスワード認証では異なる認証レベルをセット
  - OpenAMリバースプロキシのポリシーでレベルをチェックしアクセス制御

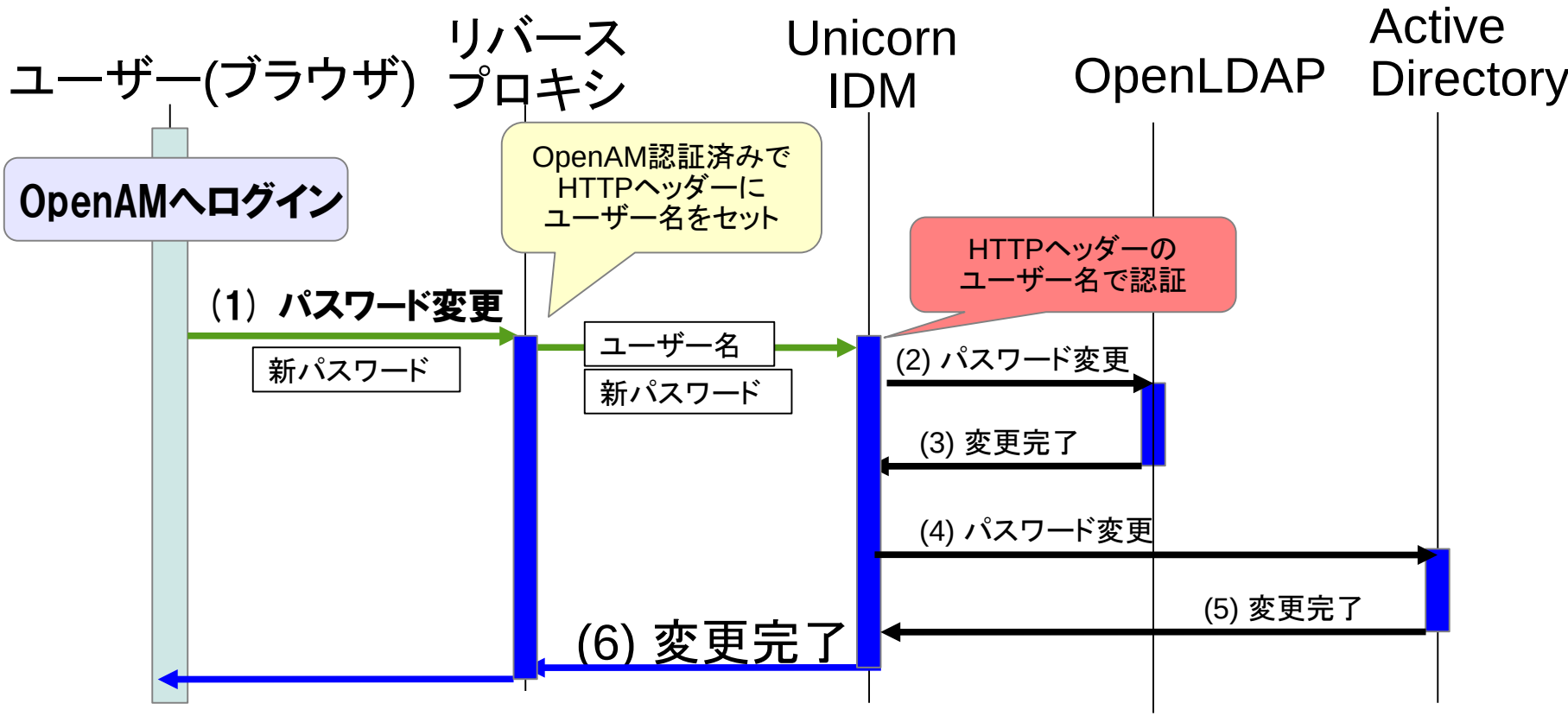
名古屋工業大学 認証シーケンス



名古屋工業大学　ID管理

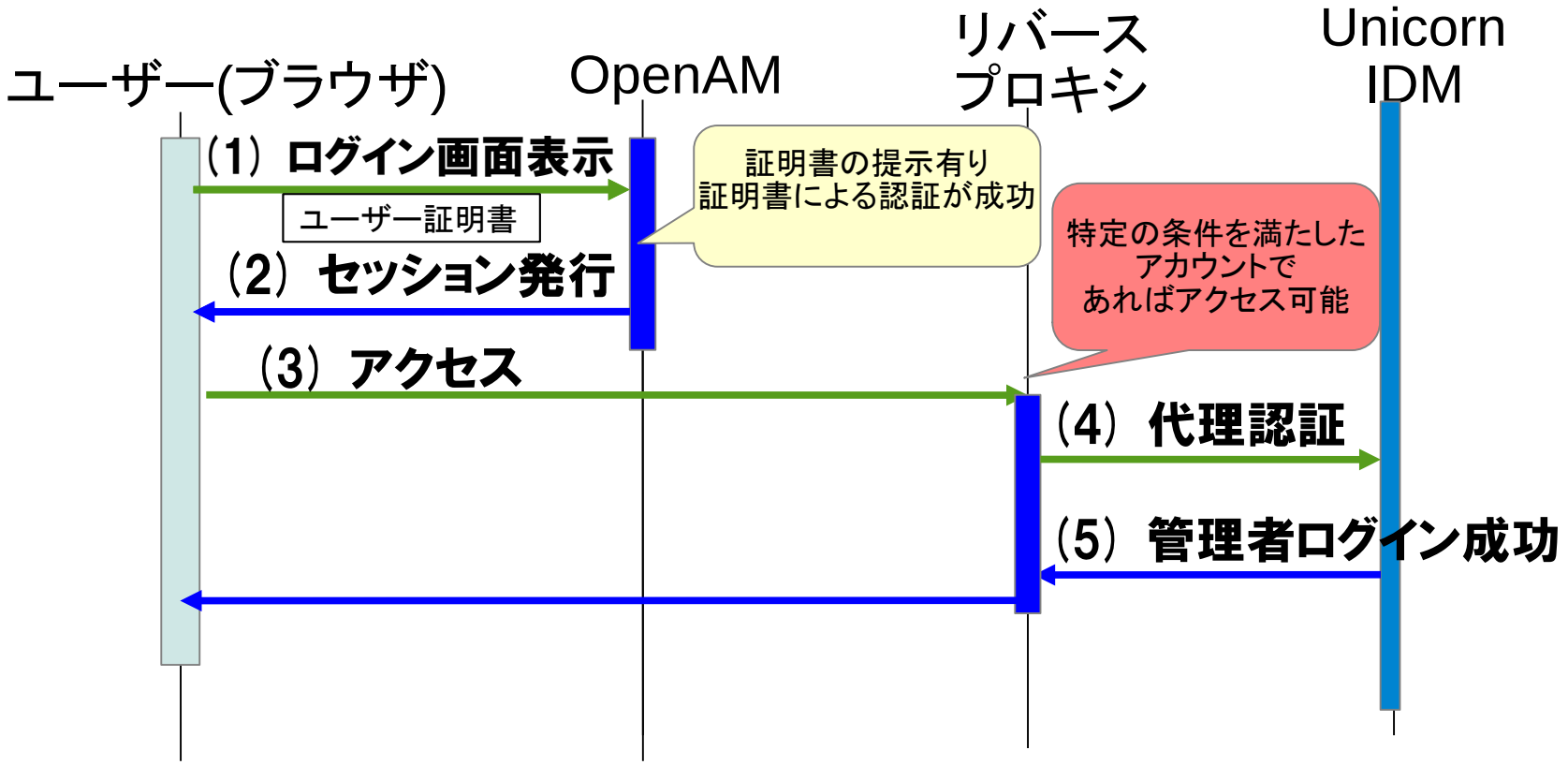
- ポイント2
  - Unicorn IDMによるID連携を実施
    - Active Directory と OpenLDAPのアカウントを同期
  - OpenAMとのシングルサインオンを実現
    - ユーザーはOpenAMにログイン済みであれば、再度の認証無しでパスワードの変更が可能
    - UnicronIDMの管理者アカウントもシングルサインオンを実現

名古屋工業大学 パスワード変更



- ユーザーはOpenAMログイン済みなので新パスワードのみでパスワード変更可能
- Unicorn IDMによりOpenLDAPとActive Directoryのパスワードが同時変更

名古屋工業大学 管理者シーケンス



特定の条件を満たしたアカウントはOpenAMにログインすることで、Unicorn IDMの管理者としてログインすることができる。

大学法人 福岡大学 様

福岡大学様 システムの特徴

規模

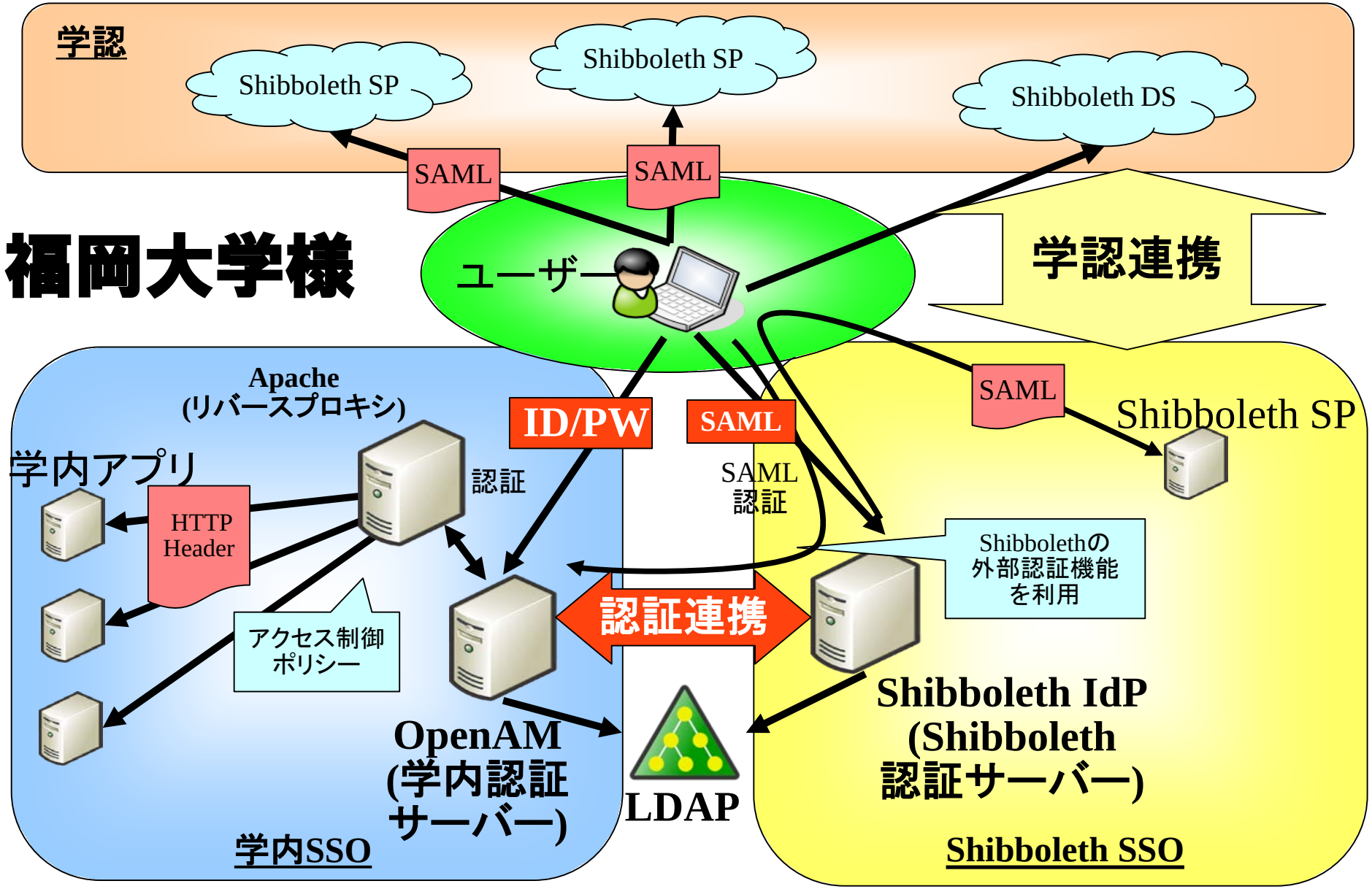
9つの学部、2つの病院、22の付置施設で構成される総合大学
学生数 約21,000人
教職員数 約3,000人

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

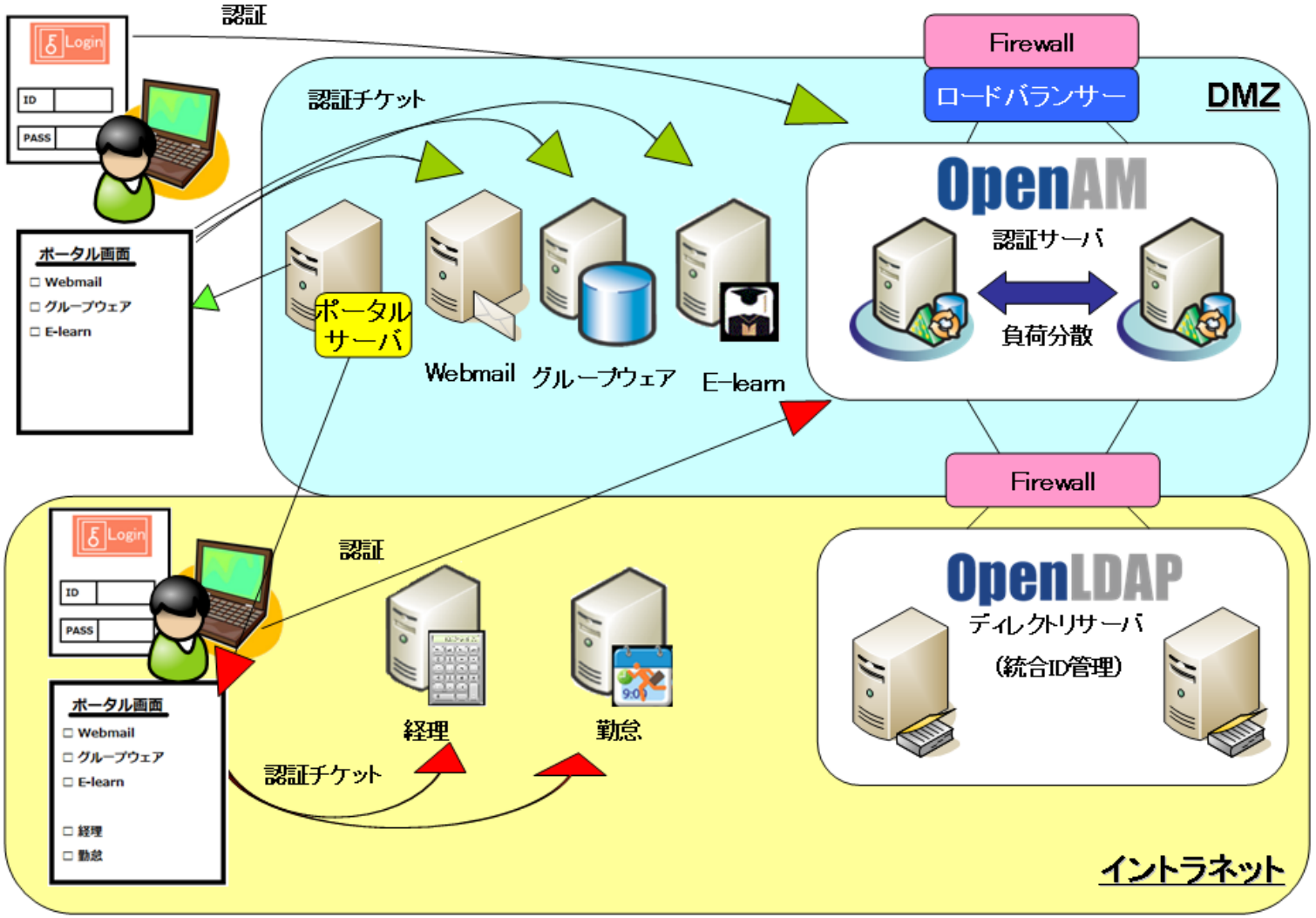


国立大学法人 北見工業大学 様

北見工業大学様 システムの特徴

- ユーザー(学生や教職員)はOpenAMに一度ログインすると、複数のWebアプリケーションをログイン操作なしで利用できます。
- ログインするとポータルメニューが表示されますが、ユーザー権限やログイン場所(学内/学外)によって表示されるメニューが変化します。
- ログインしたユーザーが利用できないアプリケーションは表示されず、インターネットからログインするとイントラネット専用アプリケーションも表示されません。
  - システム全体設計やプロジェクトとりまとめは、兼松エレクトロニクス株式会社が行いました。
  - シングルサインオン システム構築は、オープンソース・ソリューション・テクノロジ株式会社が行いました。

北見工業大学様



オープンソース・ソリューション・テクノロジ株式会社

http://www.osstech.co.jp/

お問い合わせ *info@osstech.co.jp*

