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

お問い合わせ info@osstech.co.jp

OSSTech

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

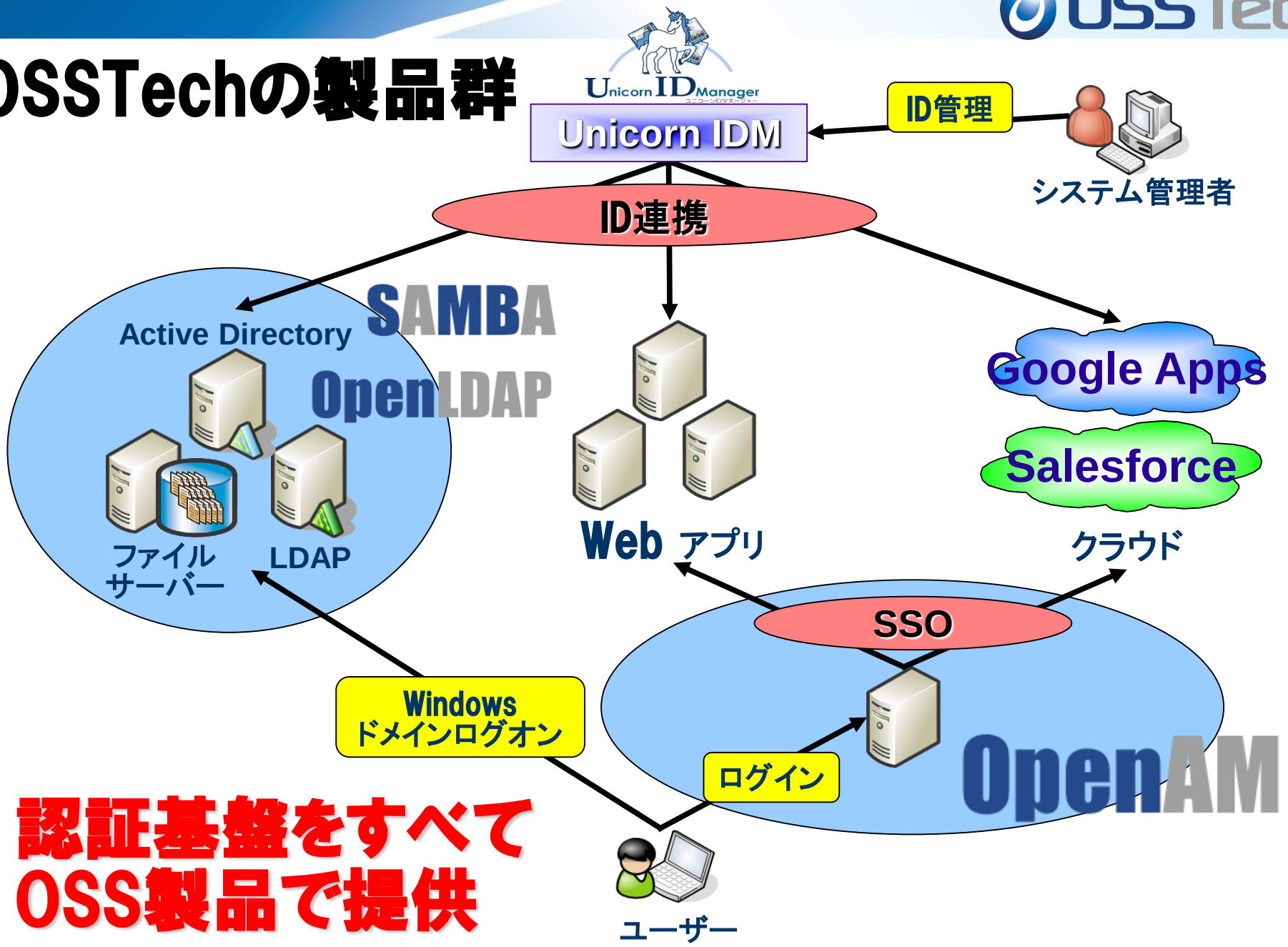
講師紹介

- 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

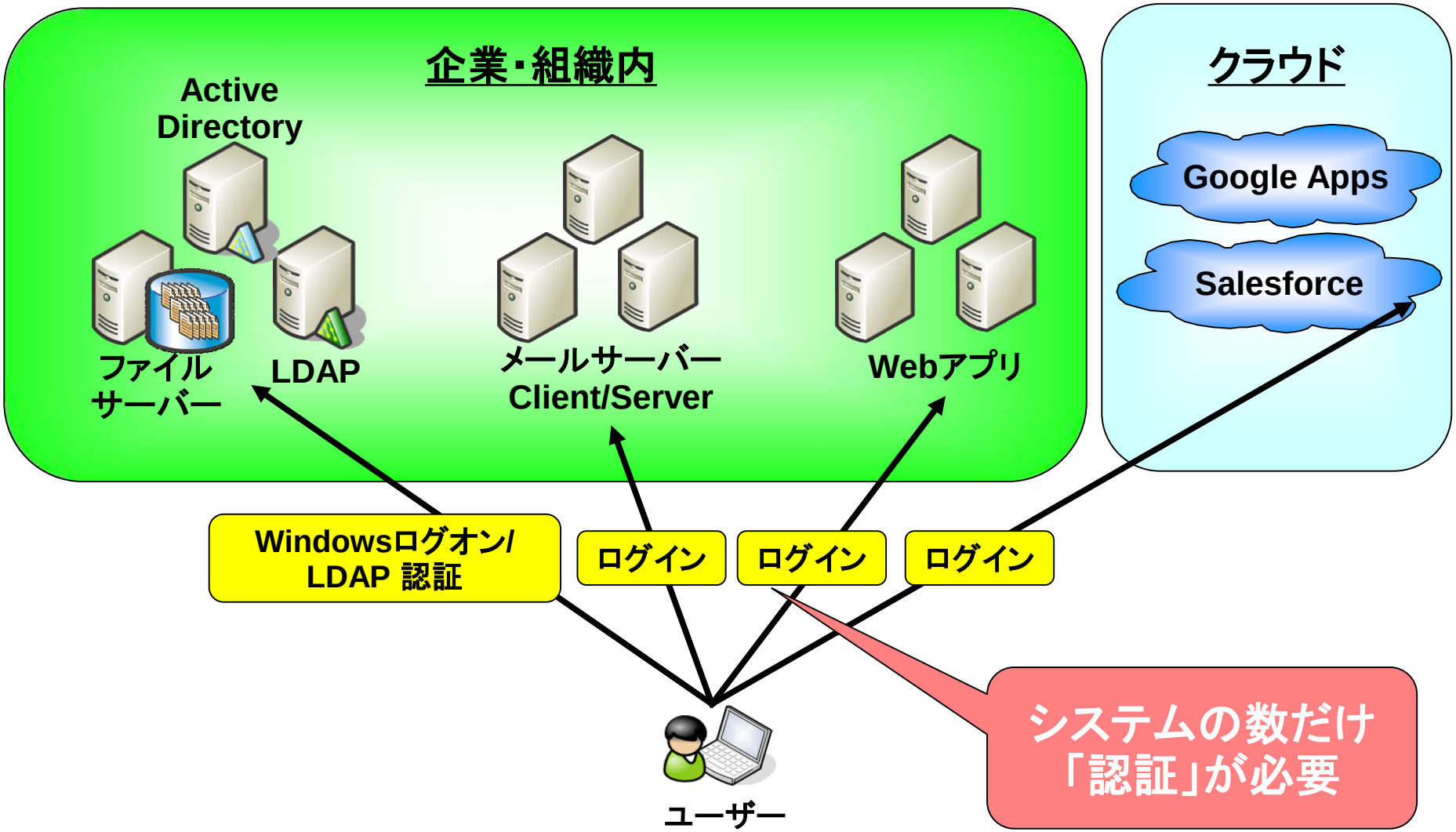
OSSTechの製品群(すべてOSSで提供)
原則Linux/Solaris/AIX共にRPMで提供

- 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

クラウドと共に普及する
シングルサインオン

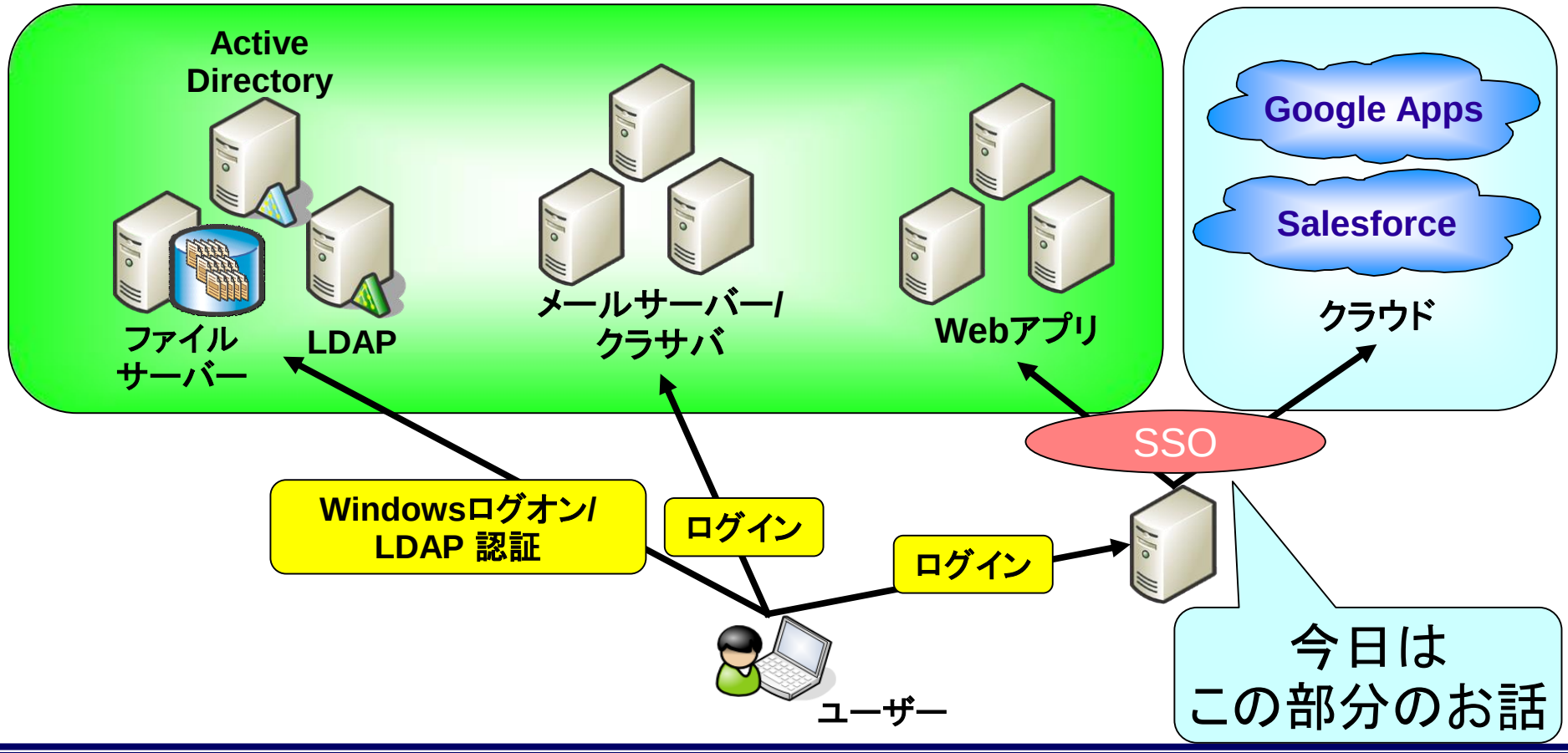
OSSTech

サービスを利用するには必ず必要な「認証」



SSO：シングルサインオンとは

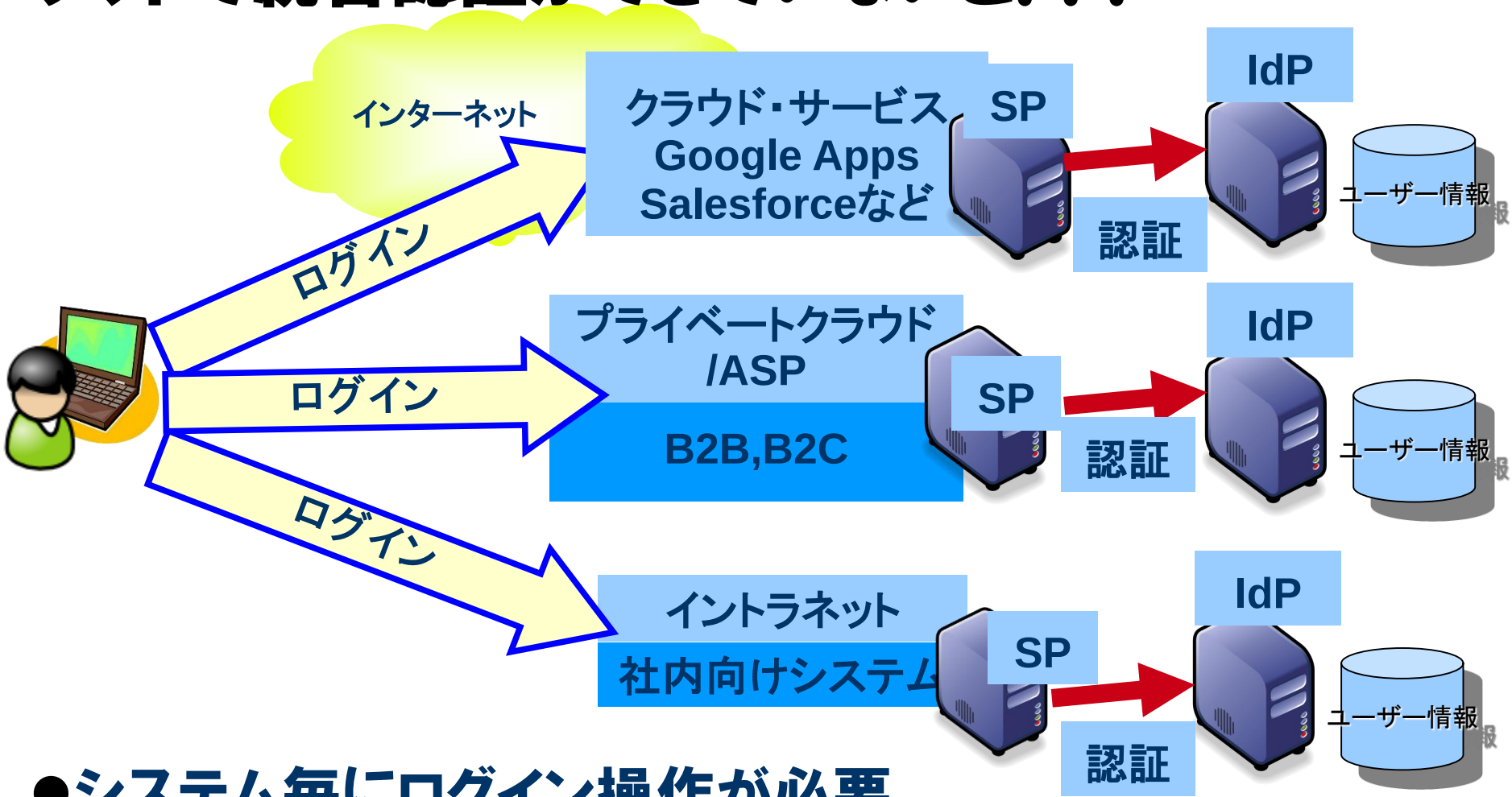
一度のログイン操作さえ完了すれば、複数のアプリケーションに認証操作することなくアクセスすることが可能になる。



SSO(シングルサインオン)とは

- １回のパスワード入力で複数のシステムやサービスを同時利用
- 「ID統合を使った統合認証」ではIDとパスワードの管理を1カ所でできるためユーザの追加も楽、社員が退社した場合に1カ所IDを削除すれば、すべてのシステムが利用不可となる
- 近年クラウドサービス(SaaS, PaaS, IaaS, HaaSなど)の普及により、(社外にある)サービス毎にID／パスワードを登録しなければならないケースが増えており、「ID連携による統合認証」を使わざるを得ないケースが増えている
- ところがこのID連携が費用の問題や技術的な問題で完全に実現されていない場合、例えば社員が退社した時に社内システムのIDを削除しても、SaaS側のIDが残っているとクラウド側のシステムは社外から使えてしまう、といった問題が起きてしまう

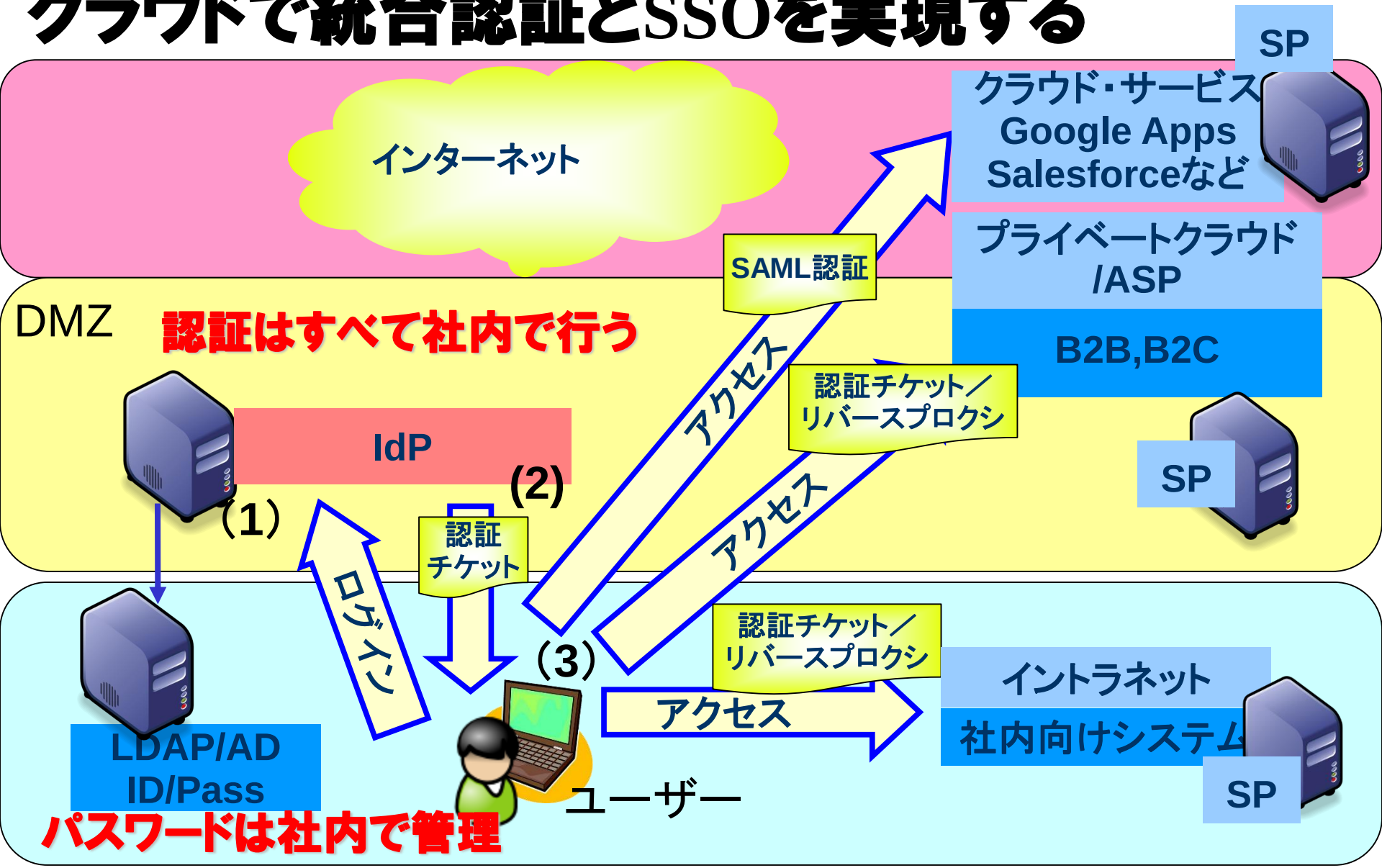
クラウドで統合認証ができていないと．．．



- システム毎にログイン操作が必要
- クラウドにID/パスワードとパスワードを置く必要がある

（パスワードを社外に置くと不正ログインされる危険性が高い）

クラウドで統合認証とSSOを実現する



シングルサインオンを実現するソフトウェア

OpenAM

- Webアプリケーションにおけるシングルサインオンを実現するためのプラットフォームとなるソフトウェア
- 現在はオープンソースだが、元はSun Microsystems社の商用製品（Access Manager）
- 弊社で製品パッケージを提供

Shibboleth

- SAMLを扱えるオープンソースのソフトウェア
  - Shibboleth1.3以前のバージョンがSAML1.1を実装
  - Shibboleth2.0よりSAML2.0を実装
- 学認フェデレーションでの主な認証ミドルウェアとして使用

シングルサインオン
技術動向

OSSTech

SSO(OpenAM)導入動向

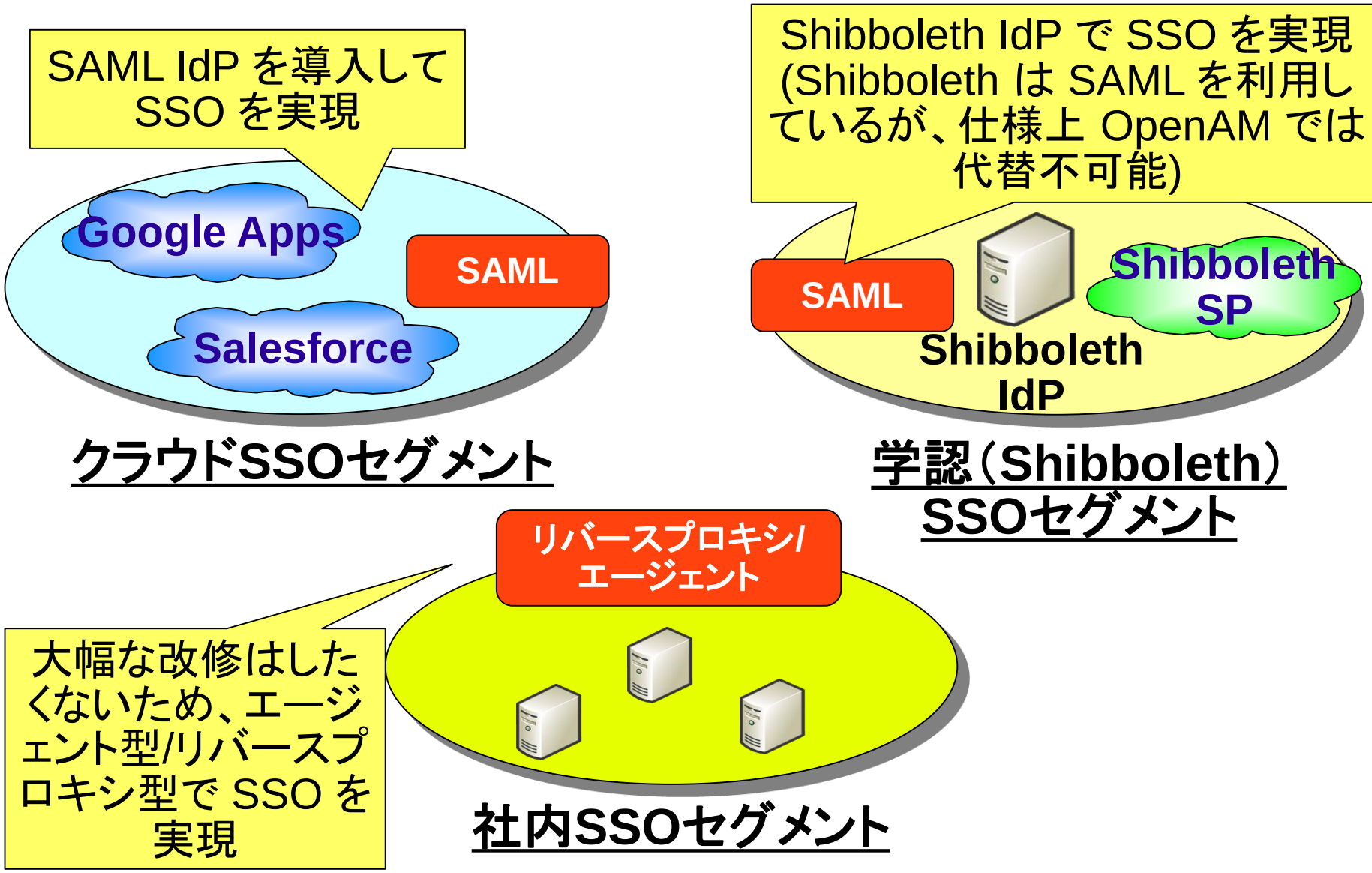
- クラウドの普及により、SSO(シングルサインオン)が急速に普及中
- IaaSやPaaSも増えつつあるが、やはりSaaSのGoogle Apps(大学／企業)とSalesforce(企業)をまず導入するケースが多い
- 企業ではSalesforceのセキュリティ強化を目的にOpenAM導入するケースが多い
- 大学ではGoogle AppsとイントラネットやShibbolethを連携させるケースが多い
- 企業ではM&Aや会社合併のために増えすぎたアプリやIDを統合するためにSSOを導入
- IaaSやPaaSも普及し始め、これらの上で構築された社内向け個別アプリのSSOも普及しだしてきた。

OpenAMで実現する
シングルサインオン・ハブ

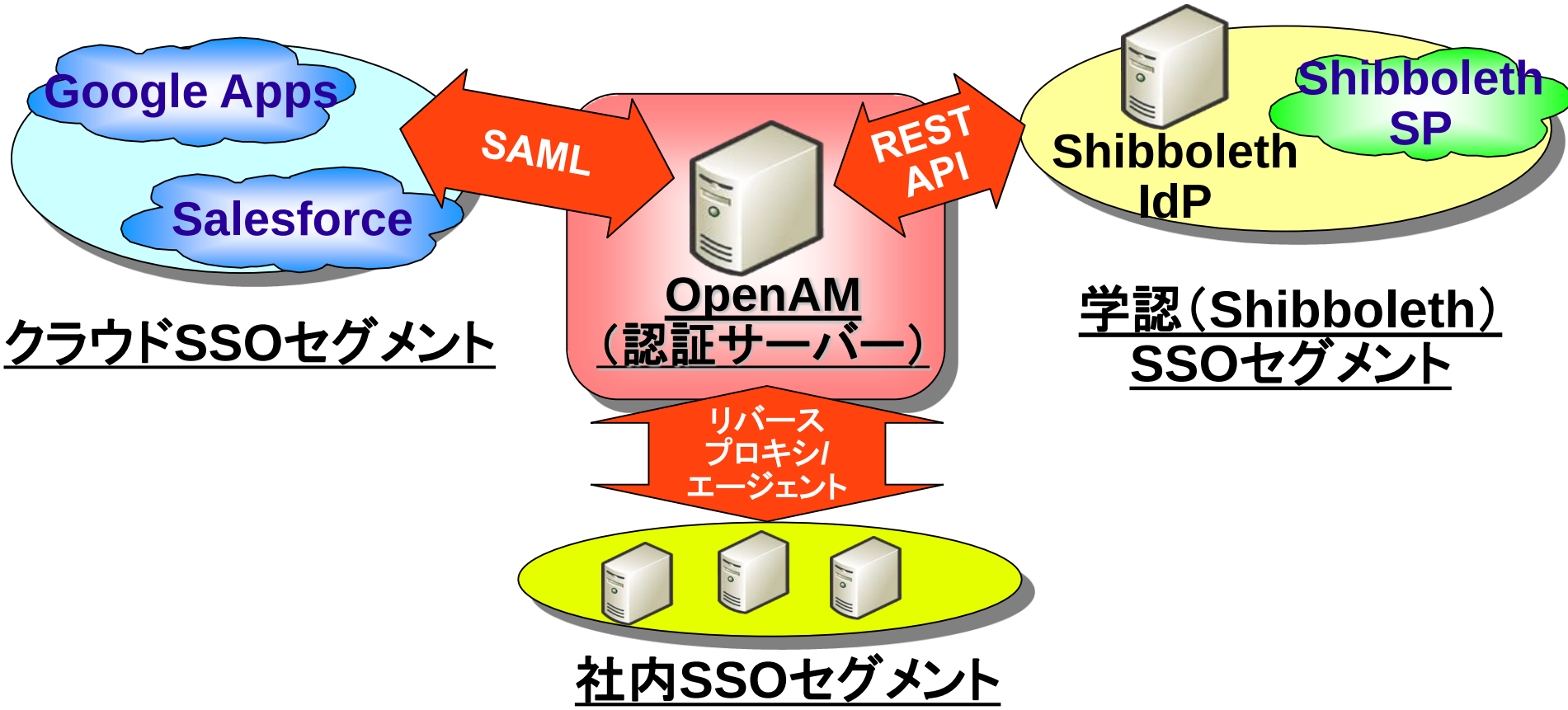
オープンソースのOpenAMだから
高機能・安価に実現できる

OSSTech

混在する複数のSSO環境



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

シングルサインオン方式

シングルサインオン方式の詳細(1)

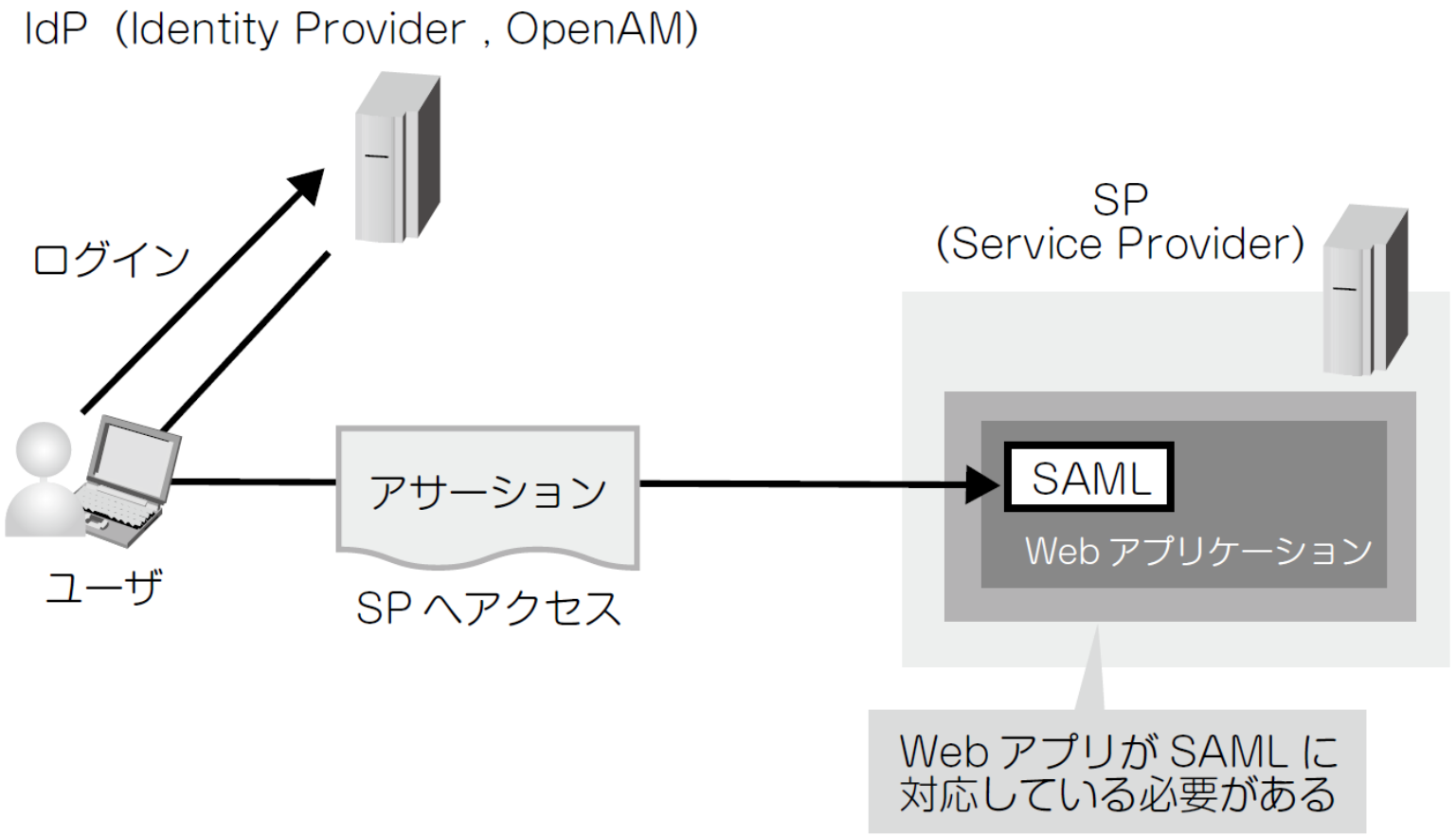
- フェデレーション:SAMLによるシングルサインオン
  - Secure Assertion Markup Language
  - 認証、認可、ユーザ属性情報などをXMLで送受信するためのフレームワーク
  - 標準化団体OASISにより策定
  - GoogleApps, Salesforceなどが採用
  - 今後OpenIDの普及によりOpenAMでOAuth実装予定
- エージェント方式
  - SSO対象のWebアプリが動作するサーバー上にアクセス制御用のモジュールを配置する方式
  - サーバーのバージョンに影響を受ける

シングルサインオン方式の詳細(2)

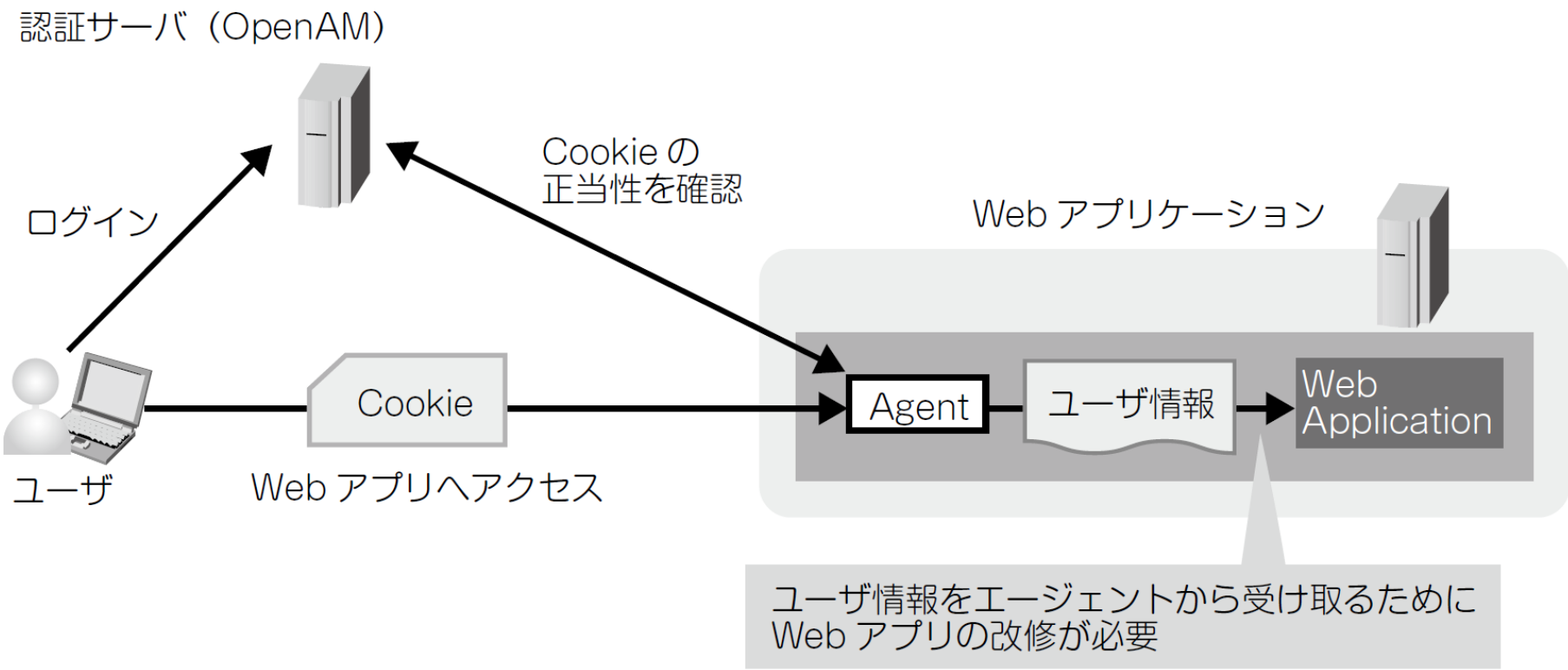
- リバースプロキシ方式
  - リバースプロキシを使用してアクセス制御を行う
  - ユーザーデータの受け渡しはHTTPヘッダーを利用
  - SSO対象Webアプリのバージョンや設定変更の影響が少ない
  - リバースプロキシが性能上のボトルネックになる可能性がある

- 代理認証方式
  - SSO対象Webアプリの既存ログイン画面に対して、OpenAMがユーザーの代理でログインID/パスワードを送信する
  - SSO対象Webアプリの改修が不要
  - 細かなアクセス制御はできない(ログイン処理の代理実行のみ)

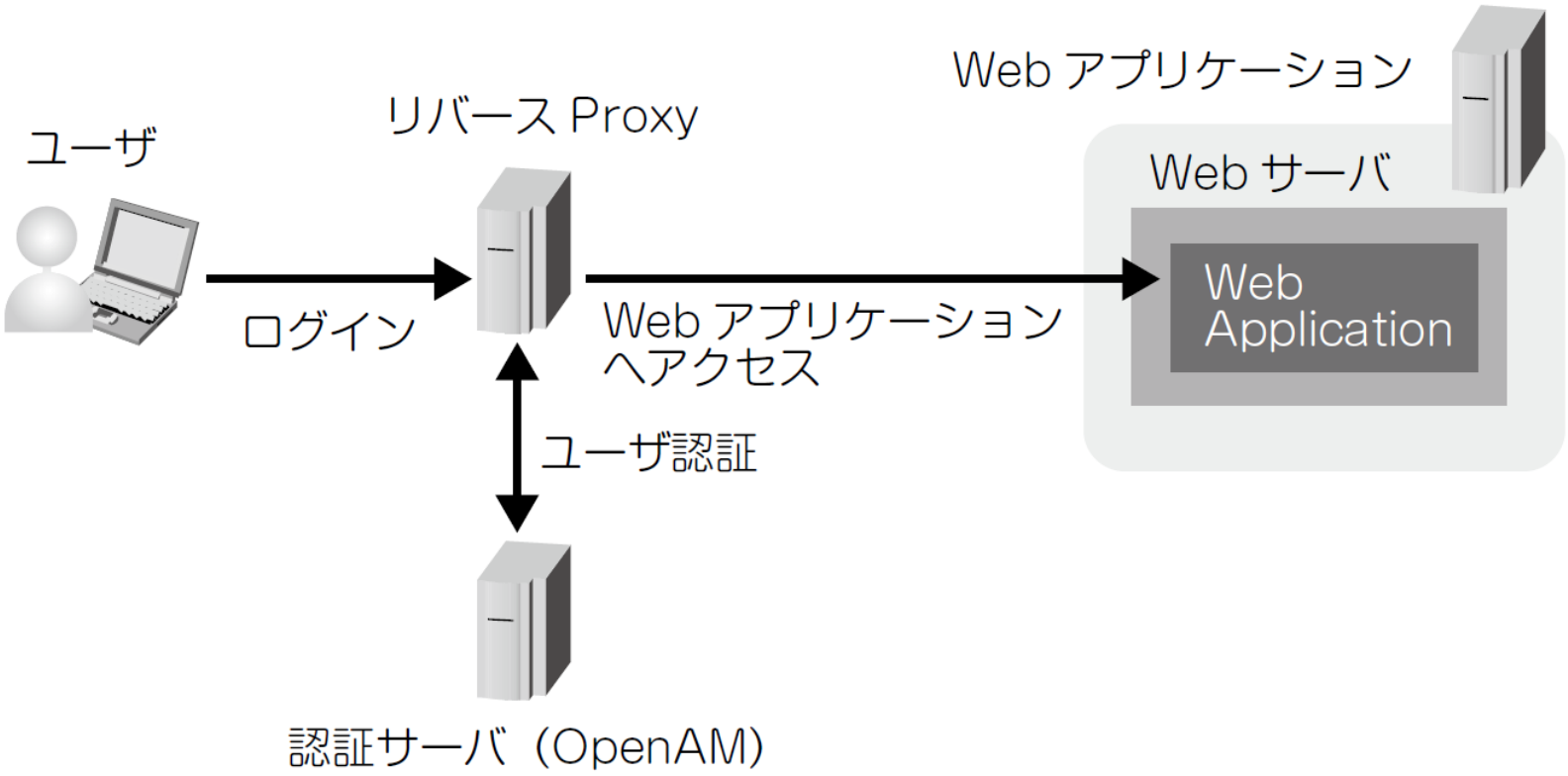
フェデレーション：SAMLによるシングルサインオン



エージェント型

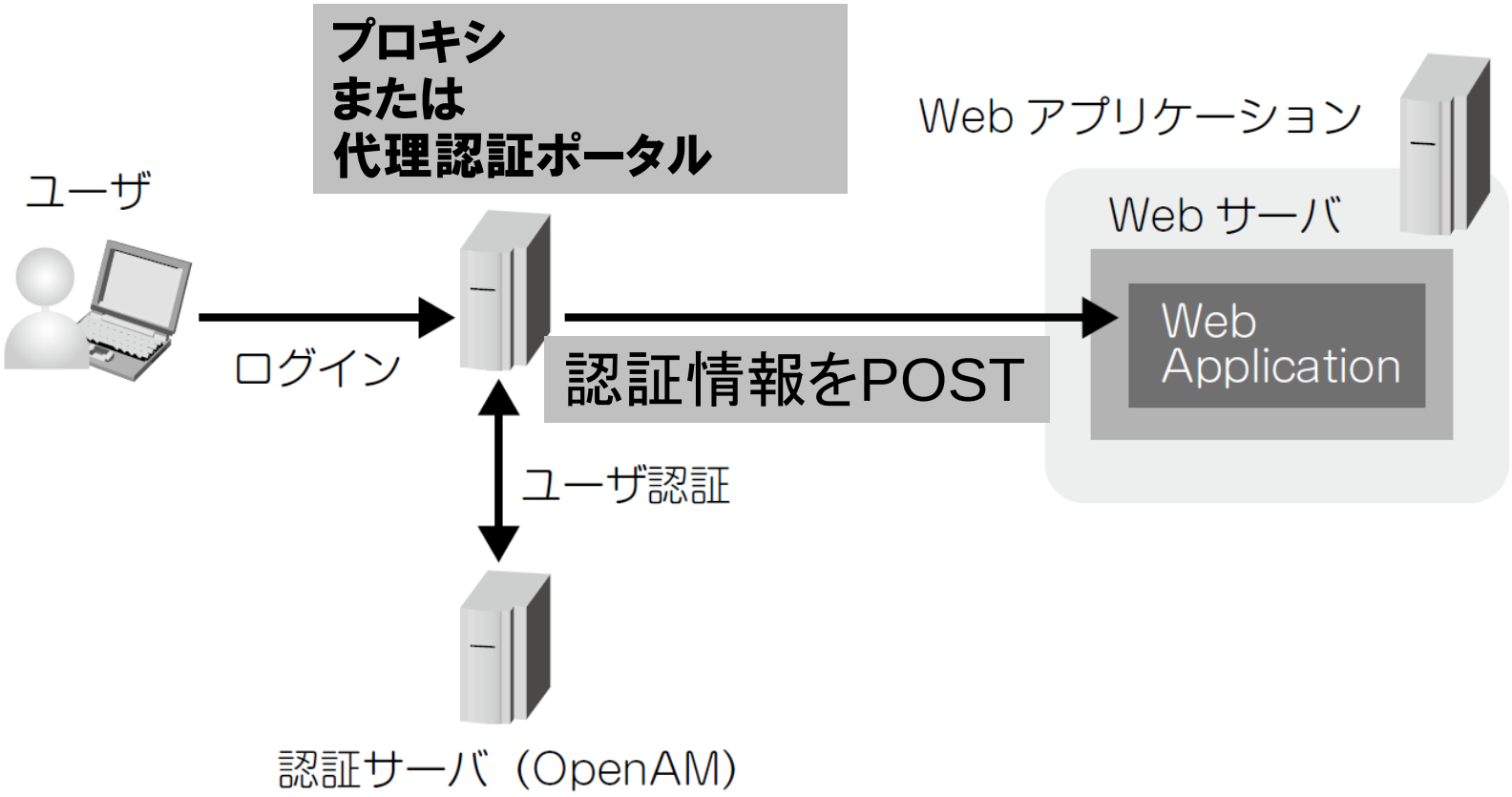


リバースプロキシ型



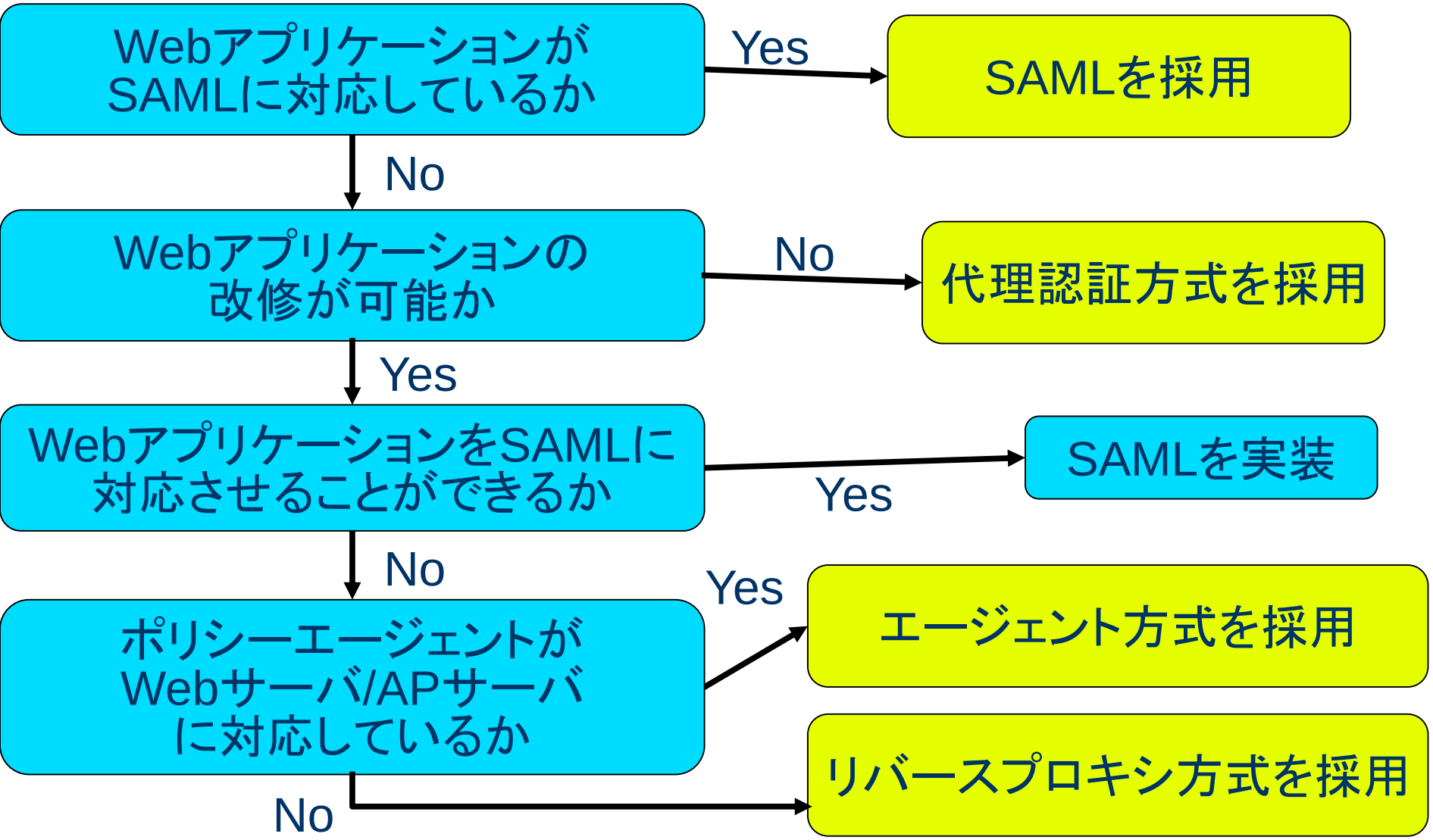
- 後方のサーバを仮想的に1台に見せることも可能
- 認証とサーバへのアクセス制御はプロキシサーバで行う
- 後方のサーバは認証なしもしくはBasic認証でアクセス可能

代理認証方式



- 認証サーバで認証したら後方のサーバへ認証情報をPOSTして認証する
- 後方のサーバが独自の認証画面を持っていてもSSO可能

シングルサイオン方式の採用基準



本当はやってはいけない「代理認証」

「既存アプリに手を入れられない」という理由で代理認証を採用するユーザーは多いが本当はやってはいけない！

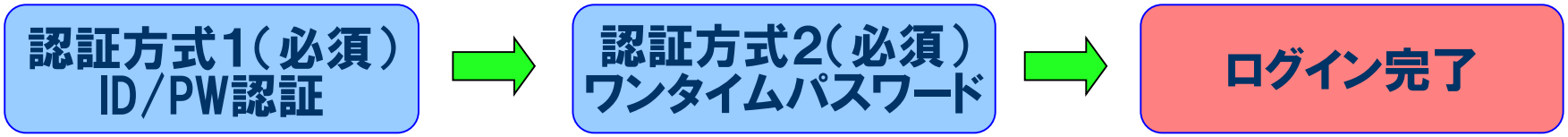
- IDとパスワードを(HTTPSでも)ネットワークに何度も流すのは良くない。(SSO入り口の1カ所に限定すべき)
- 代理認証はイントラネットのみに限るべき
- クラウドへの代理認証は危険
- SAMLに対応しているGoogle AppsやSalesforceに対して、代理認証は絶対にやってはいけない！
  (SAMLを使ってIdPを社内に置けばパスワードはクラウドに流れない)

OpenAMの認証方式（多要素認証）

OSSTech

OpenAMの機能 - 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



多要素認証

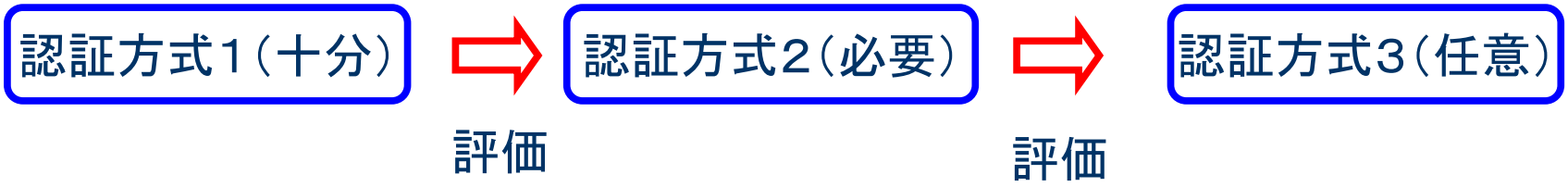
複数の認証方式を組合わせて認証を行うことにより個々の認証方式の欠点を補完

- 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

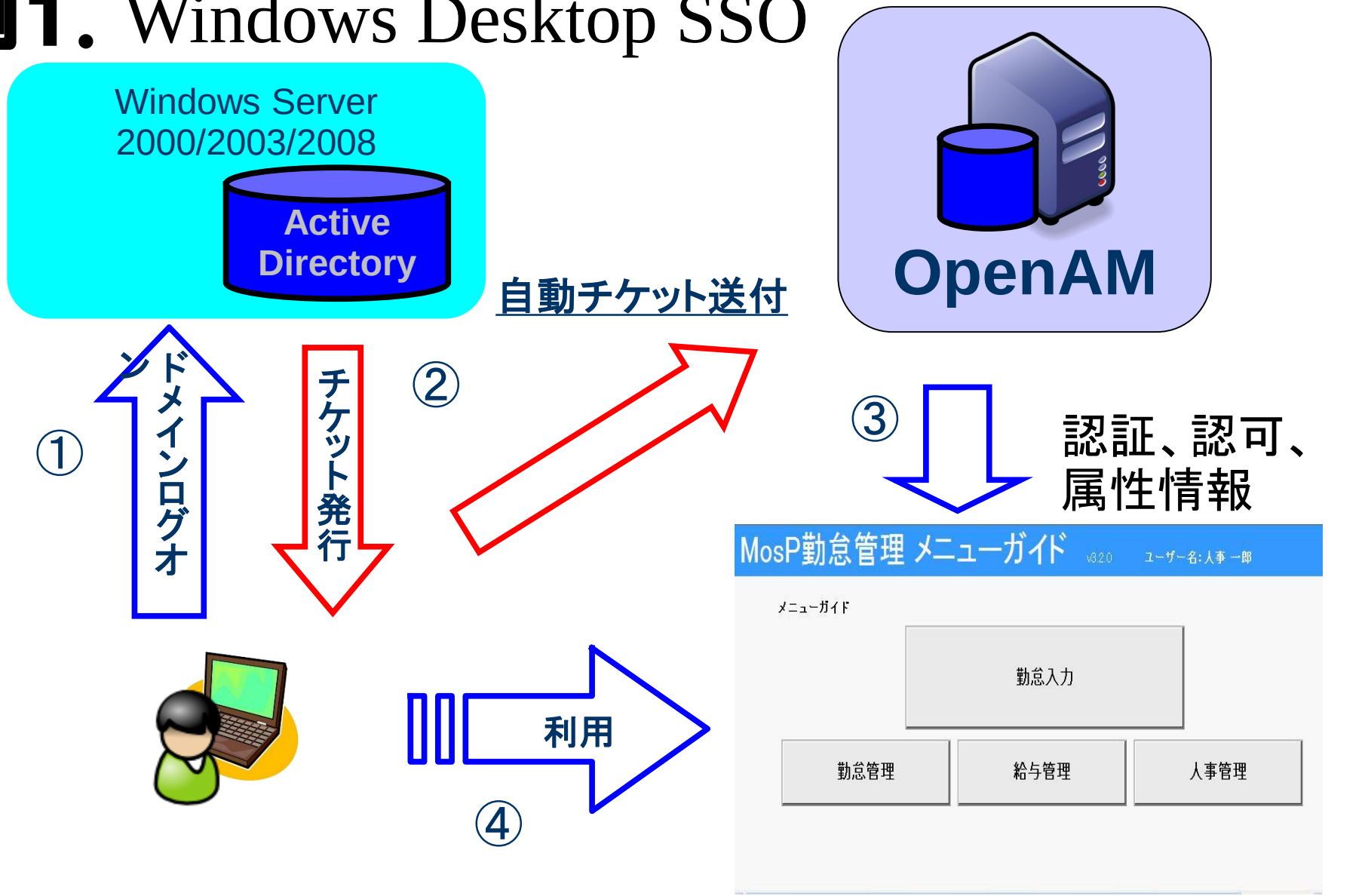
認証連鎖

認証方式を組合わせる方法を指定する

- **認証方式にはそれぞれ適用条件を指定する**
  - **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**
  - **必須：失敗したらそこで終了**
  - **任意：認証結果には関係しない付随的な処理**
- **認証成功時には認証方式に応じて認証レベルが設定される**



例1. Windows Desktop SSO

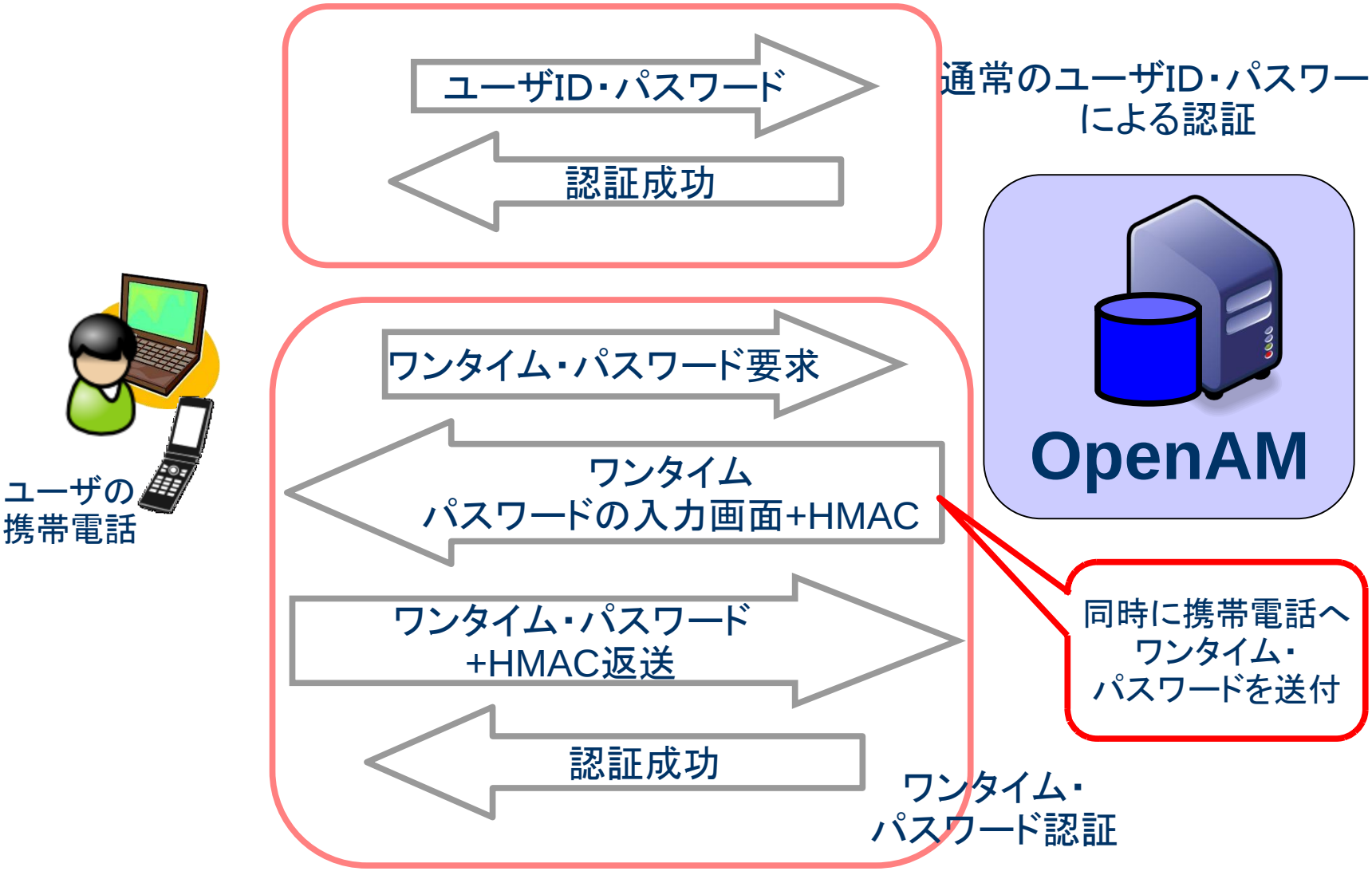


例1. Windows Desktop SSO

Windowsドメインログオンするだけで Webアプリケーションにも SSOが可能になる便利な方式

- いつも、全てのユーザがドメインログオン可能であるとは限らない
  - リモート・アクセスの場合
  - 非常勤社員の場合
- 通常のユーザID・パスワードによる認証と組み合わせて以下のように認証連鎖構成する
  - Windows Desktop SSO: 十分
  - ユーザID・パスワードによる認証：必須

例2. 携帯電話を使ったワンタイム・パスワード



例2. 携帯電話を使ったワンタイム・パスワード

- 所持物認証と知識認証の組合わせによる厳密なユーザ認証が可能
- 携帯電話を使うことによる利点
  - 導入コストの低減
  - 所持品の軽減
- フィッシングへの対応
  - HMAC(RFC2104:Keyed-Hashing for Message Authentication)を利用
  - 両方のパスワードが盗まれた場合は問題
  - 参考:RSAセキュリティ(株)による月例記者会見

http://internet.watch.impress.co.jp/docs/news/20100728_383861.html

応用例

- Windows Desktop SSOによる認証は便利なのでぜひ使いたいが全てのユーザがドメインログオン可能とは限らない
- ワンタイム・パスワードは厳密な認証が出来る点は良いが、いつも携帯電話を開いてパスワードを確認するのは面倒だ

- **2つを組合わせることにより便利かつ厳密な認証を行うことが可能**
  - **Windows Desktop SSO: 十分**
  - **ユーザID・パスワードによる認証： 必須**
  - **ワンタイム・パスワードによる認証： 必須**

OpenAMによるシングルサインオン システム導入事例

OSSTech

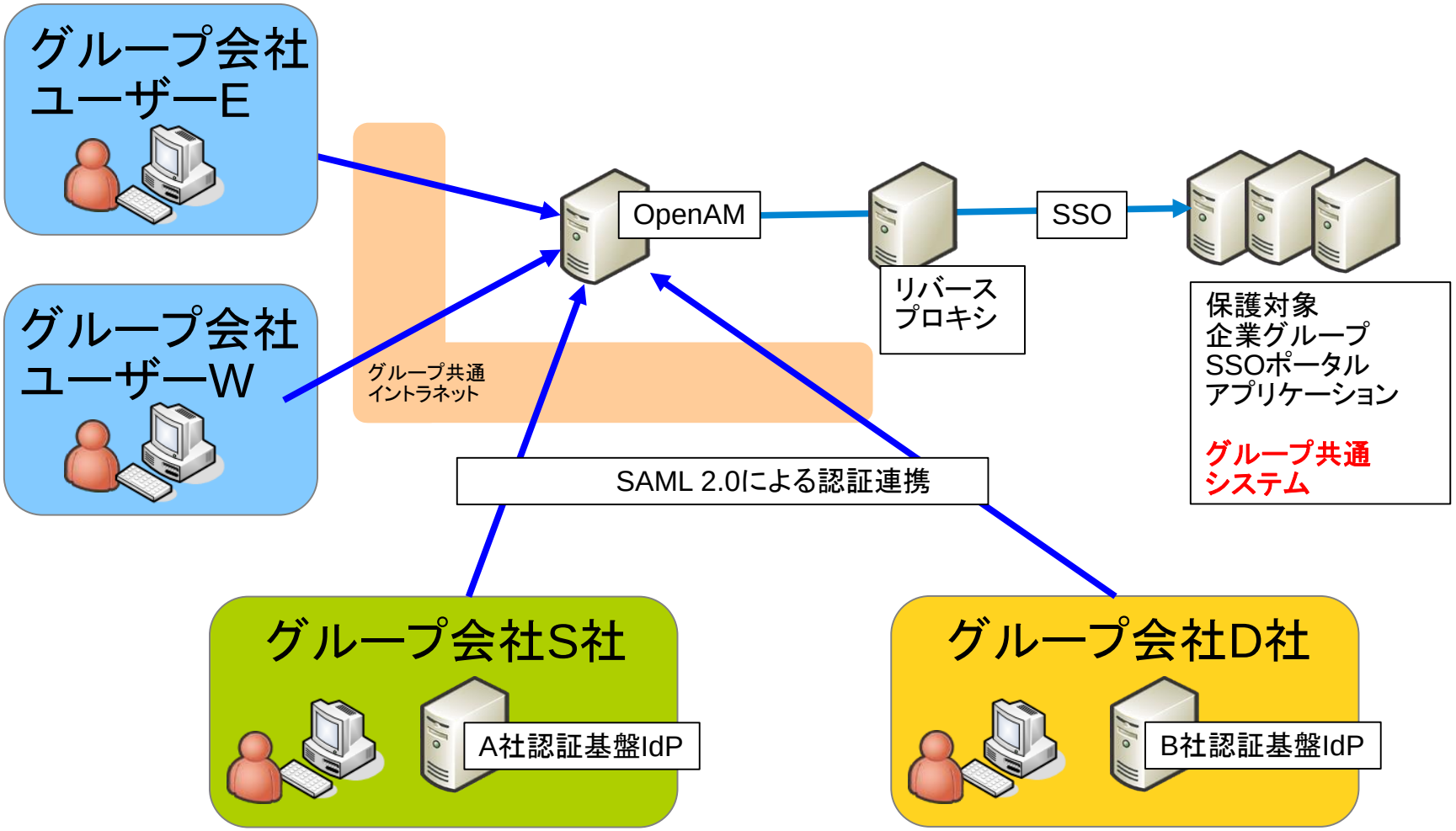
某通信会社グループ共通
シングルサインオンシステム

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

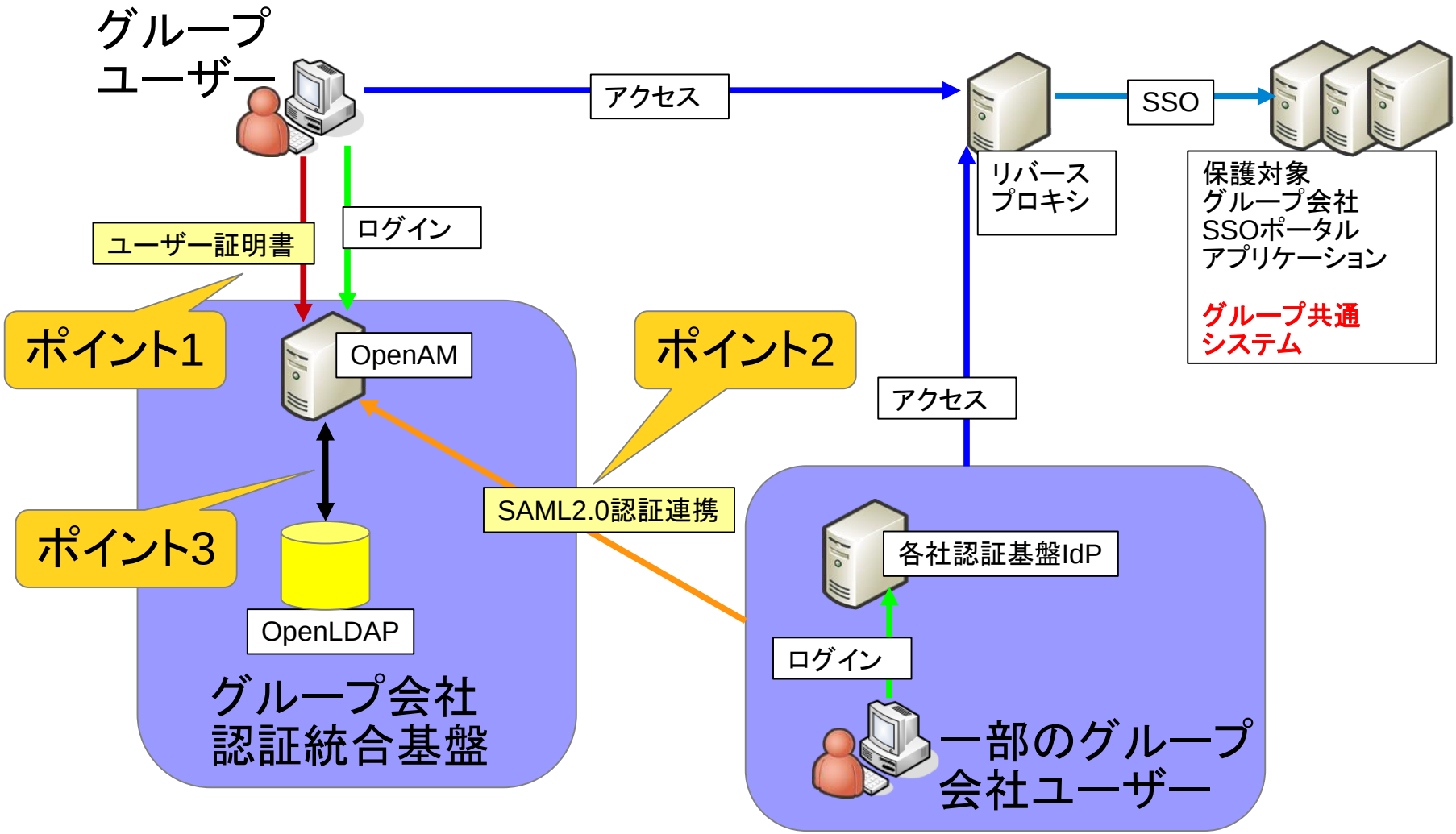
- ユーザー総数　約２５万人
- ID/パスワードとユーザー証明書の多要素認証（認証連鎖）
- 一部グループ会社ユーザーはSAML 2.0対応IdPによる認証連携
- OpenLDAPのパスワードポリシー対応モジュールの開発
- 保護対象アプリケーションとの連携はPolicyAgentを用いたリバースプロキシ型

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

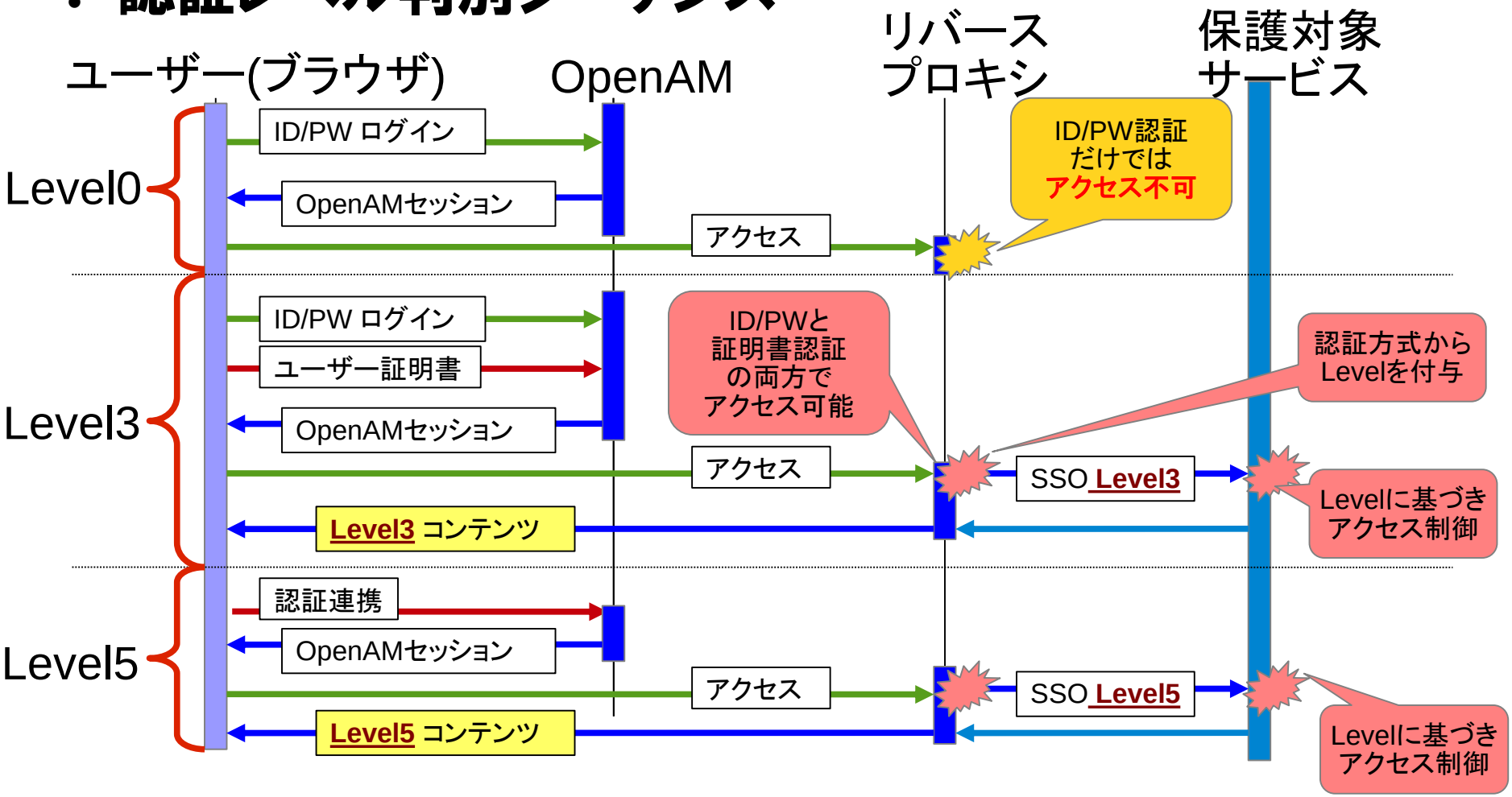


多要素認証

- 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

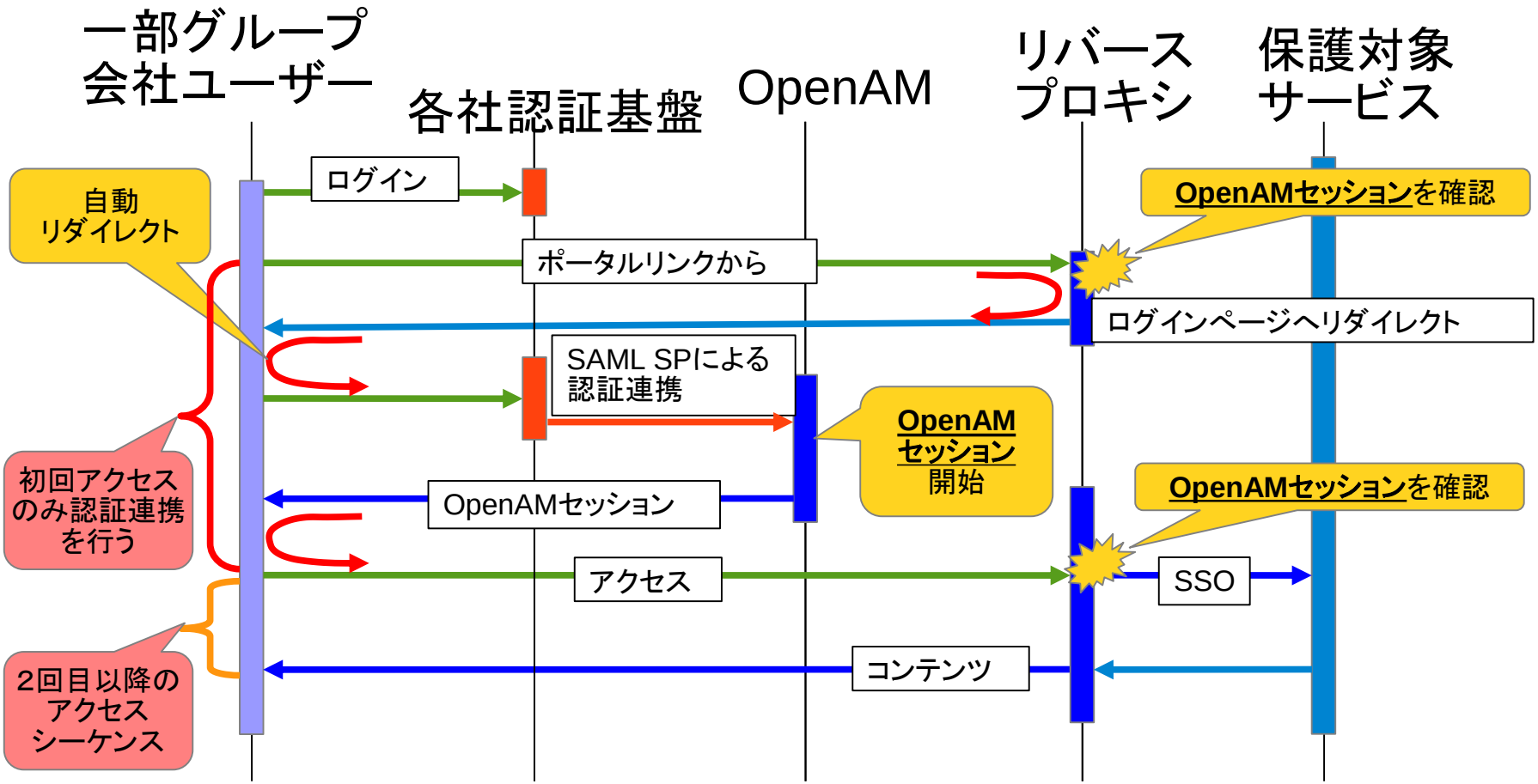
- 認証レベル判別シーケンス



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

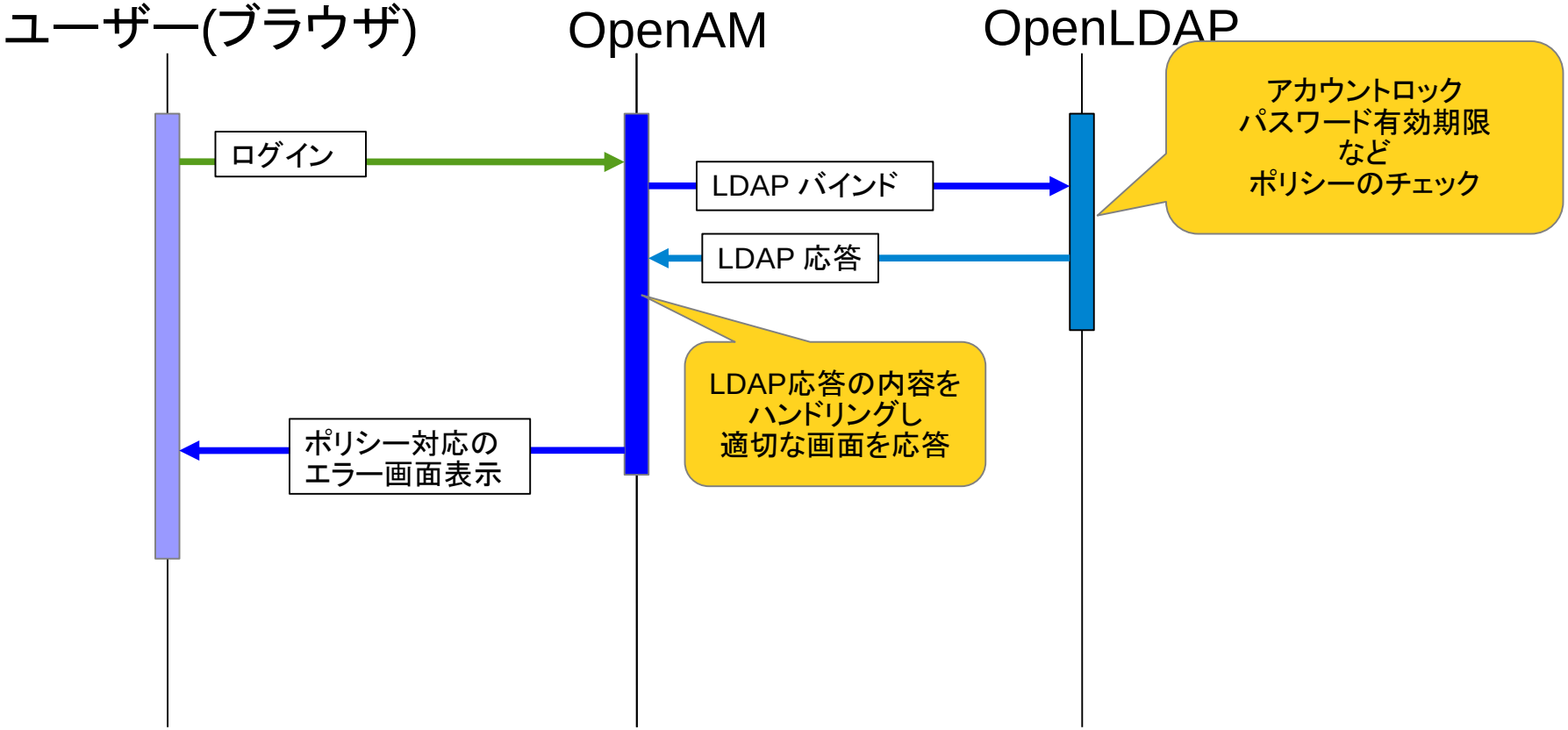


OpenLDAPポリシーへの対応

- 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



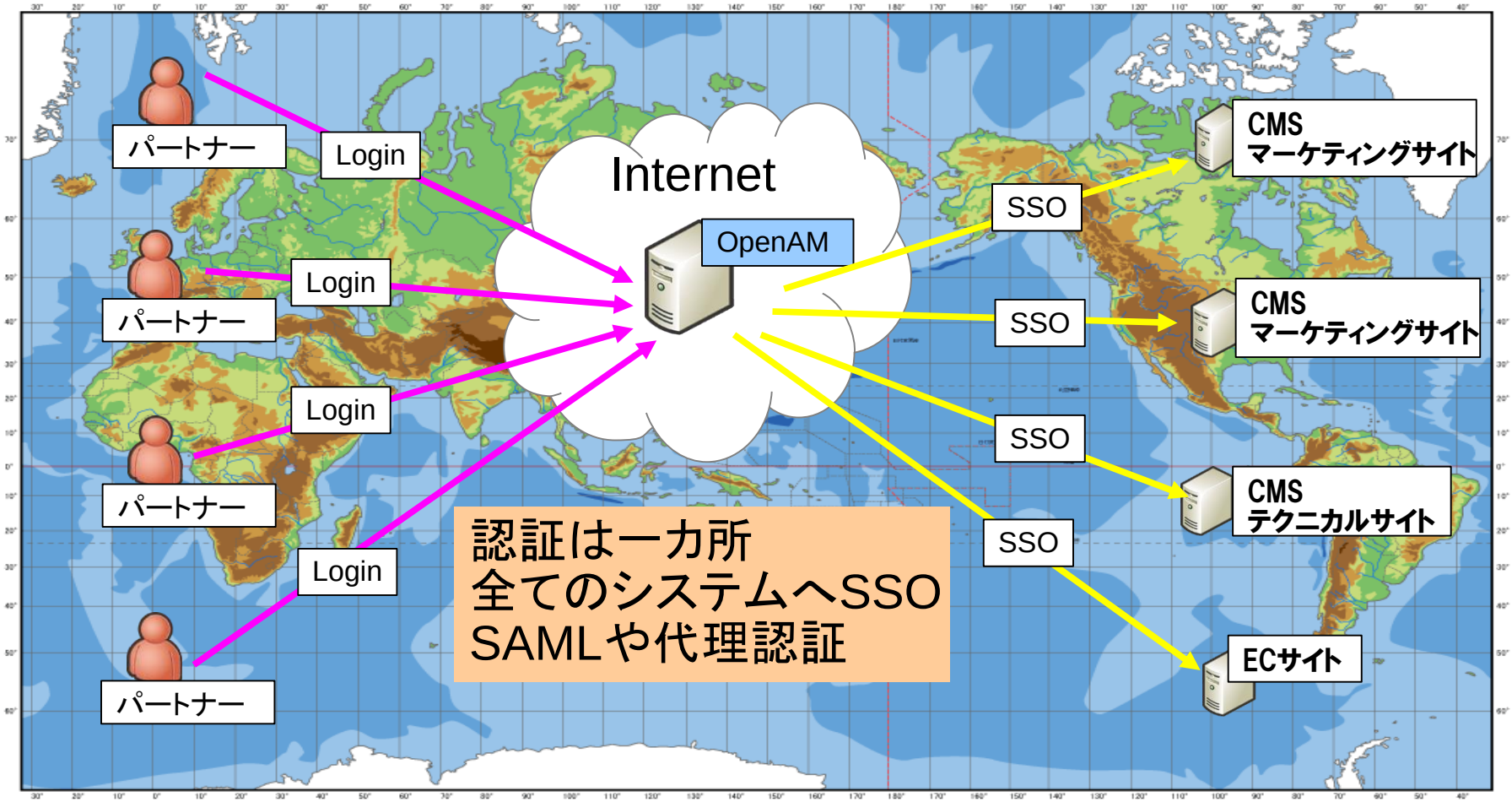
某総合電機メーカー シングルサインオン システム

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



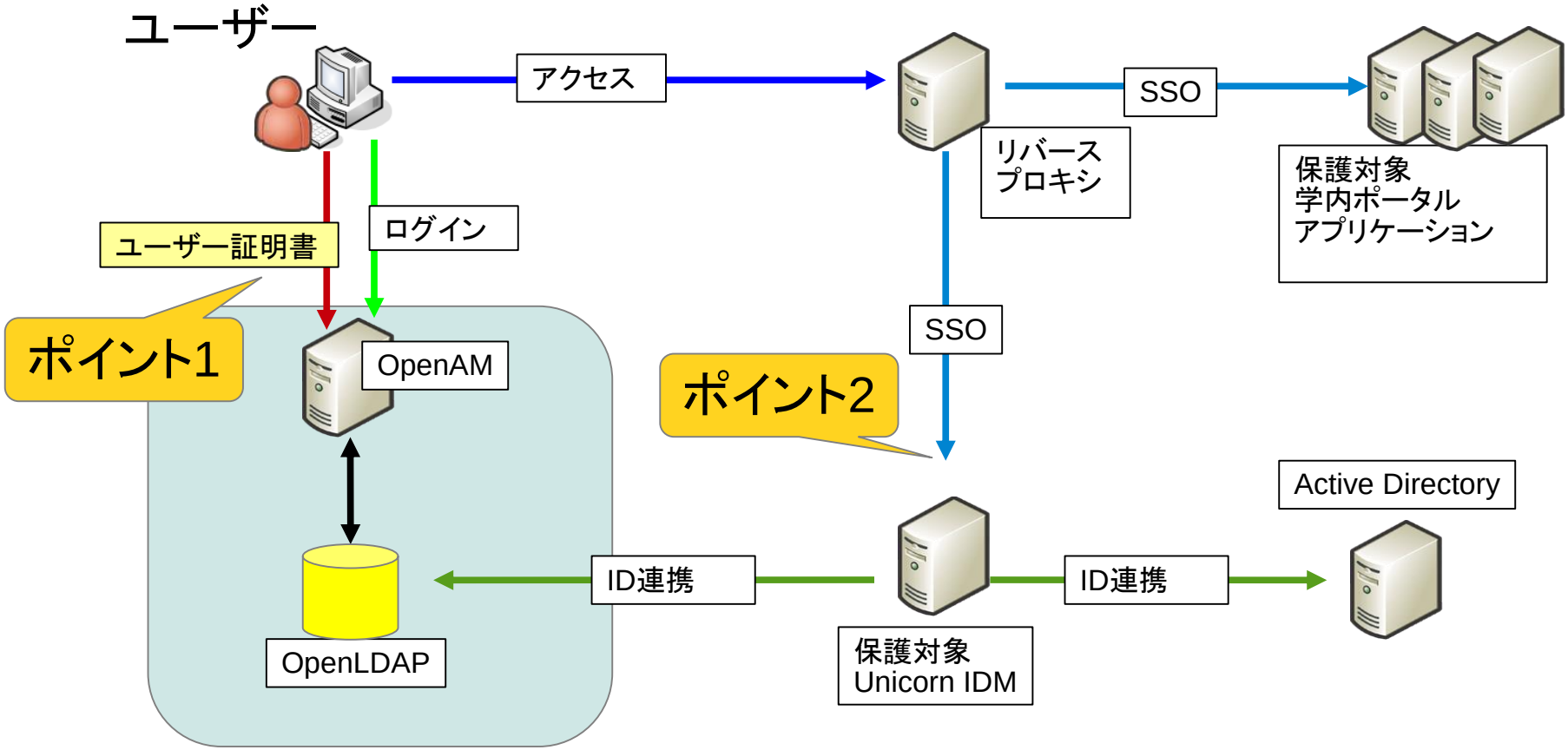
国立大学法人
名古屋工業大学

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

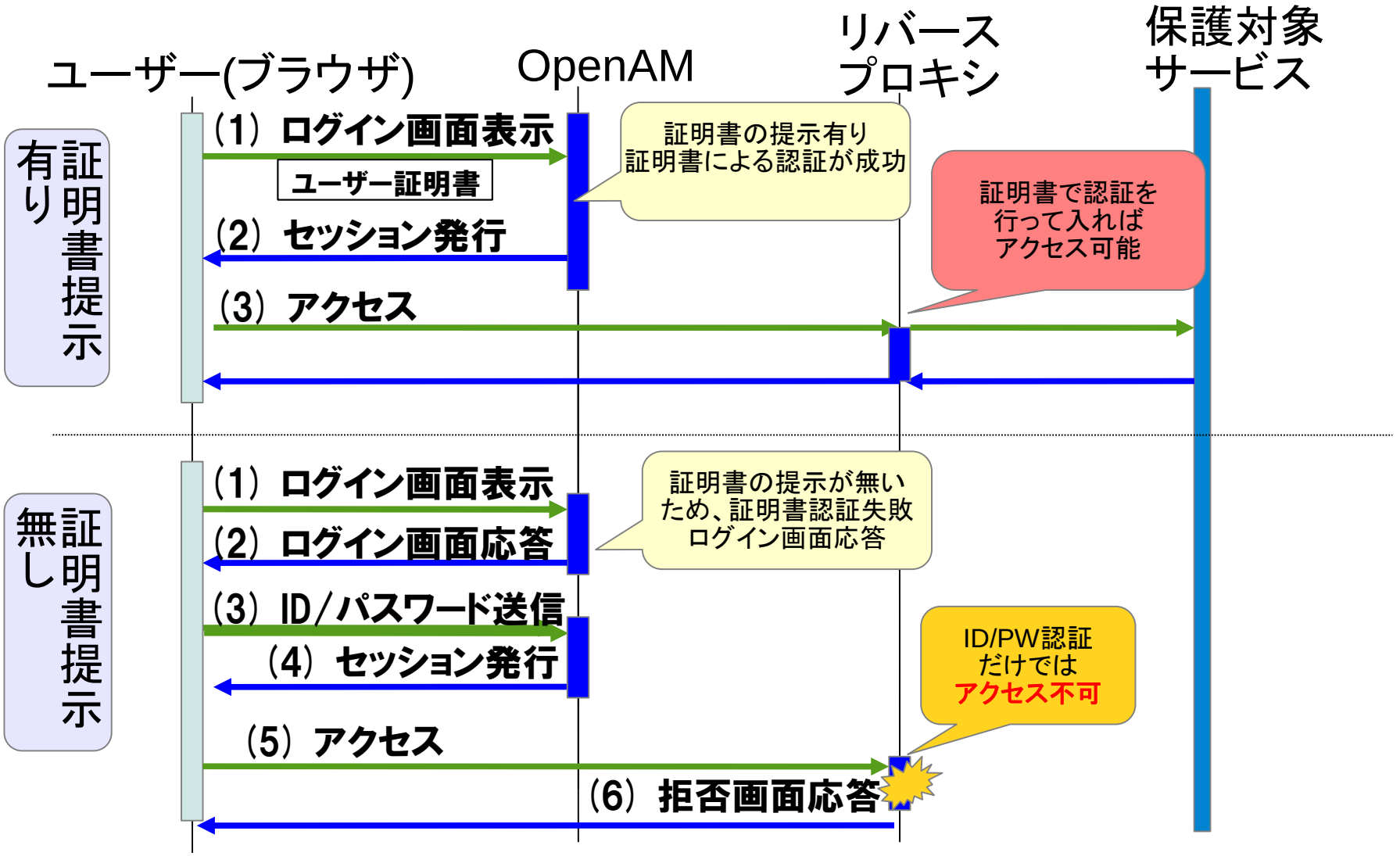
名古屋工業大学　構成図



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

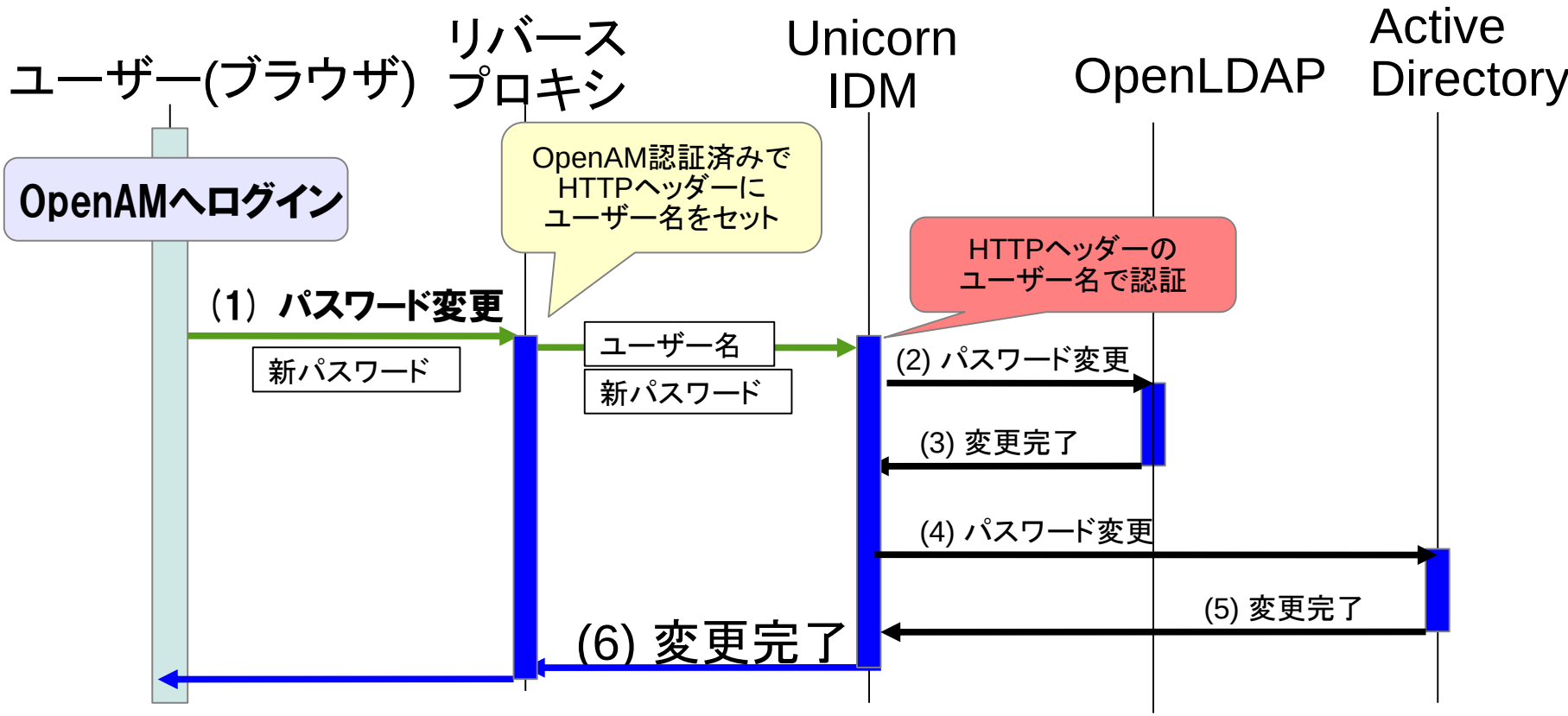
名古屋工業大学 認証シーケンス



名古屋工業大学　ID管理

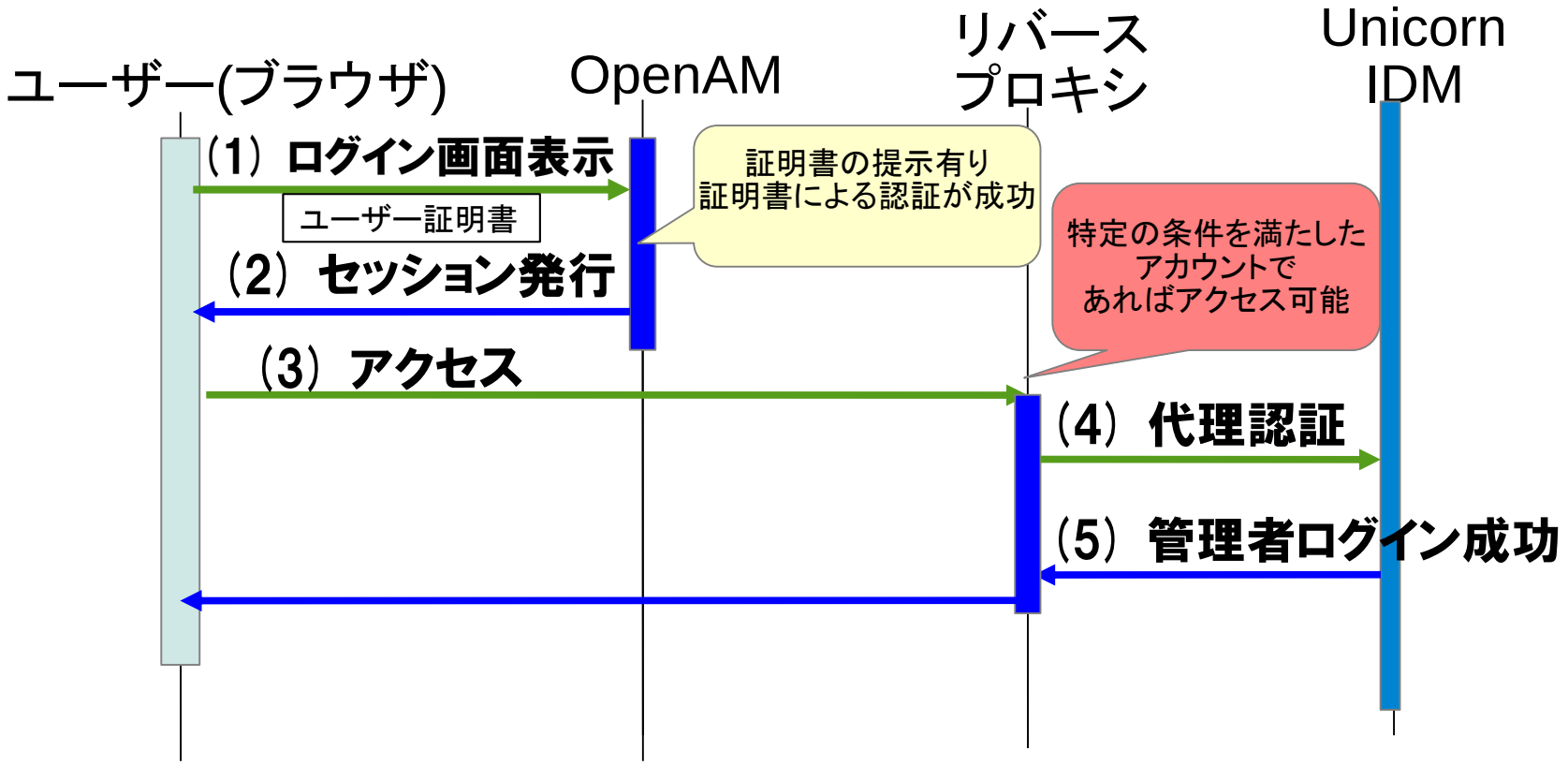
- ポイント2
  - Unicorn IDMによるID連携を実施
    - Active Directory と OpenLDAPのアカウントを同期
  - OpenAMとのシングルサインオンを実現
    - ユーザーはOpenAMにログイン済みであれば、再度の認証無しでパスワードの変更が可能
    - UnicronIDMの管理者アカウントもシングルサインオンを実現

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

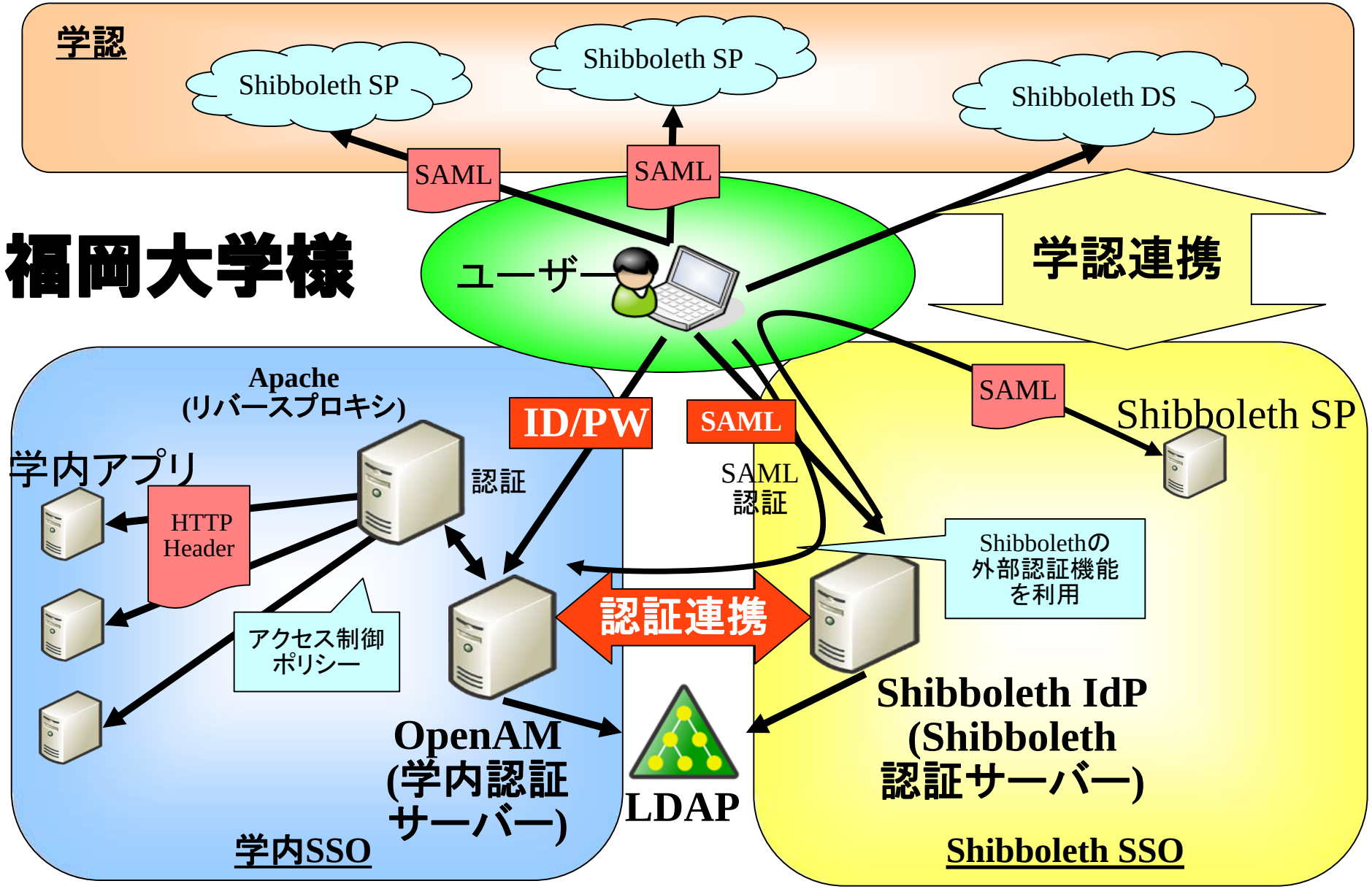
9つの学部、2つの病院、22の付置施設で構成される総合大学
学生数 約21,000人
教職員数 約3,000人

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**

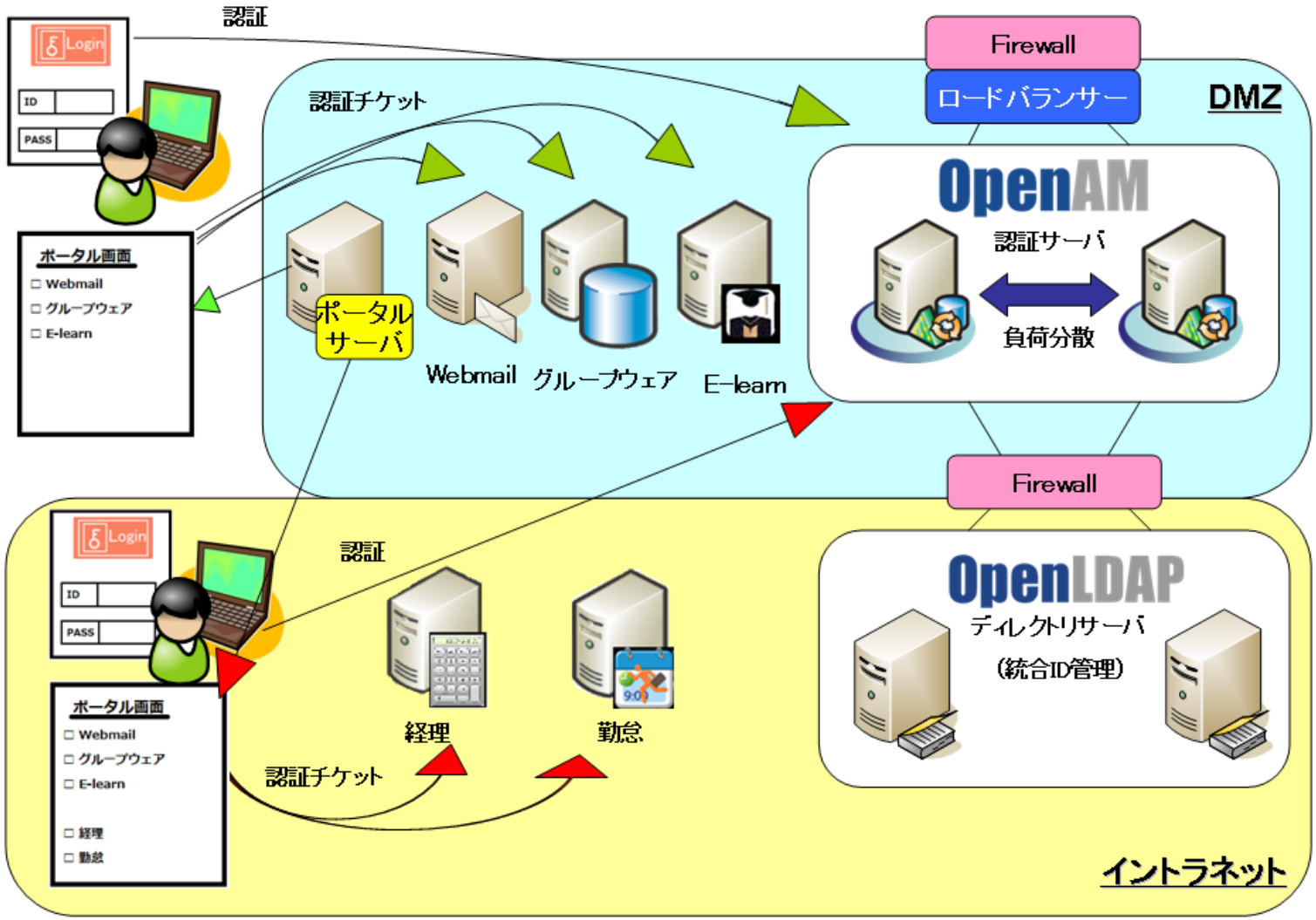


国立大学法人 北見工業大学 様

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



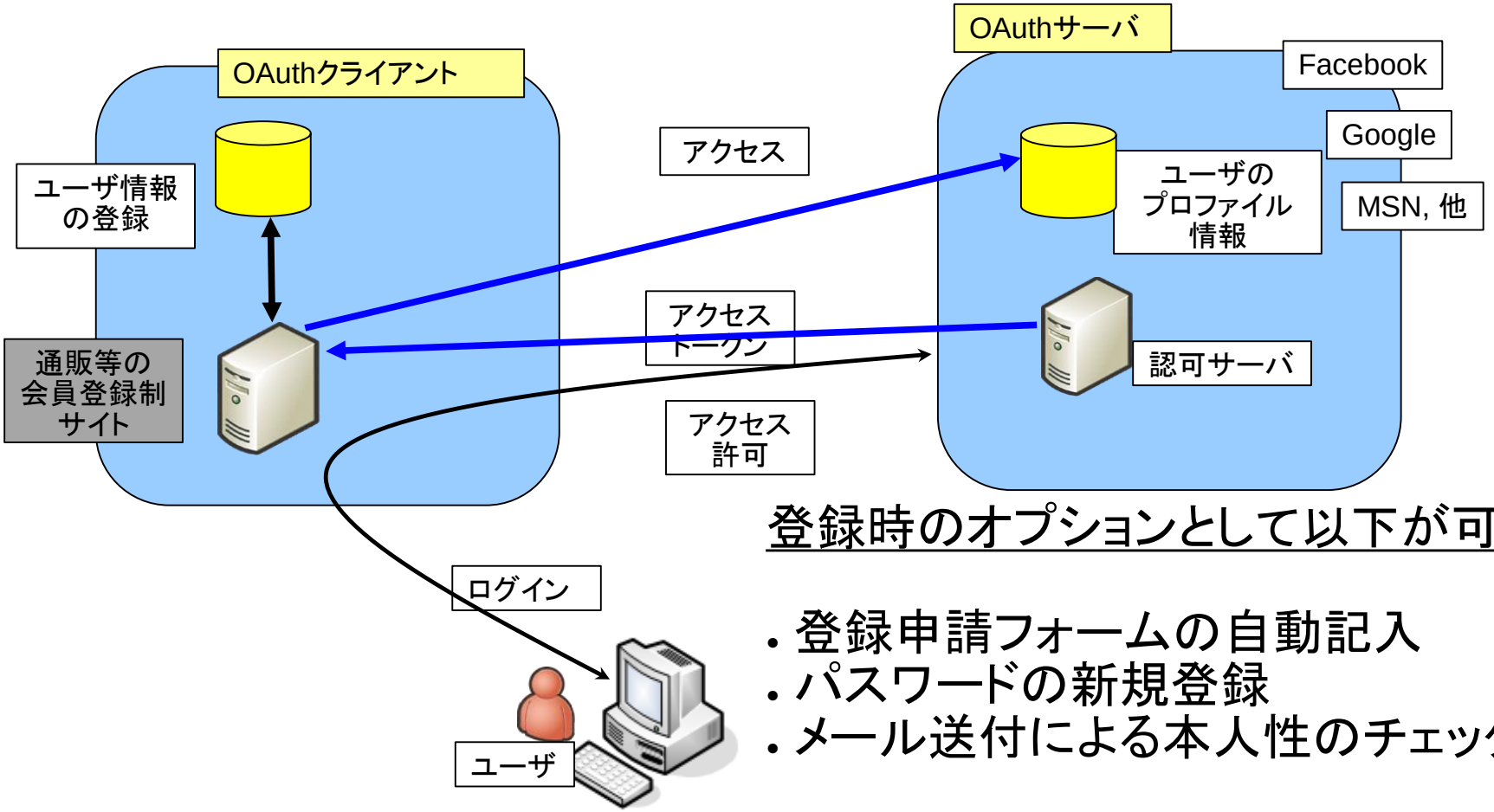
OpenAM 10

OAuth 2.0の機能

OSSTech

Facebook認証のアプリを簡単開発！

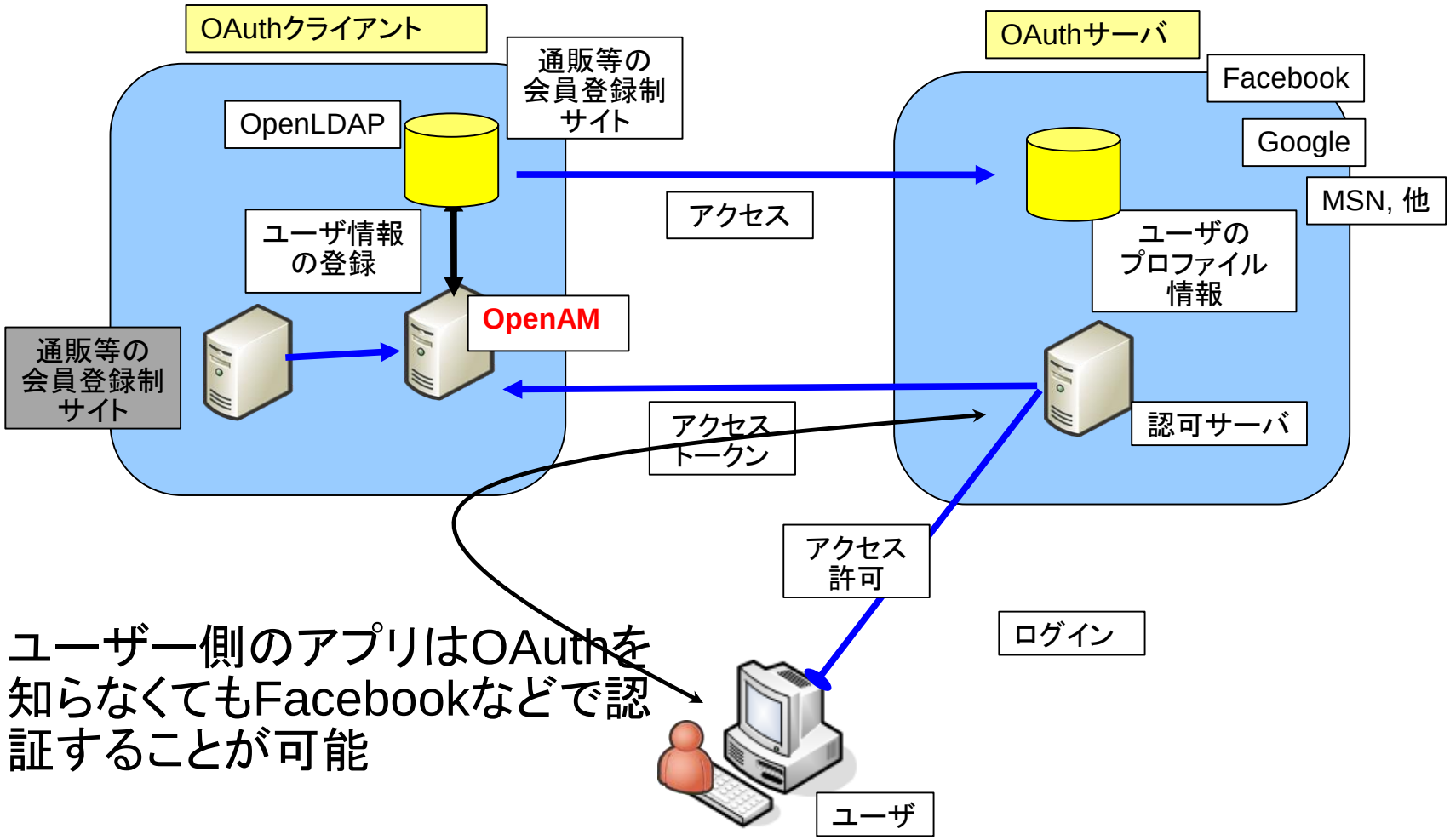
自社のサービスにFacebookなどのアカウントで ログインしてもらうOAuth クライアント機能



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



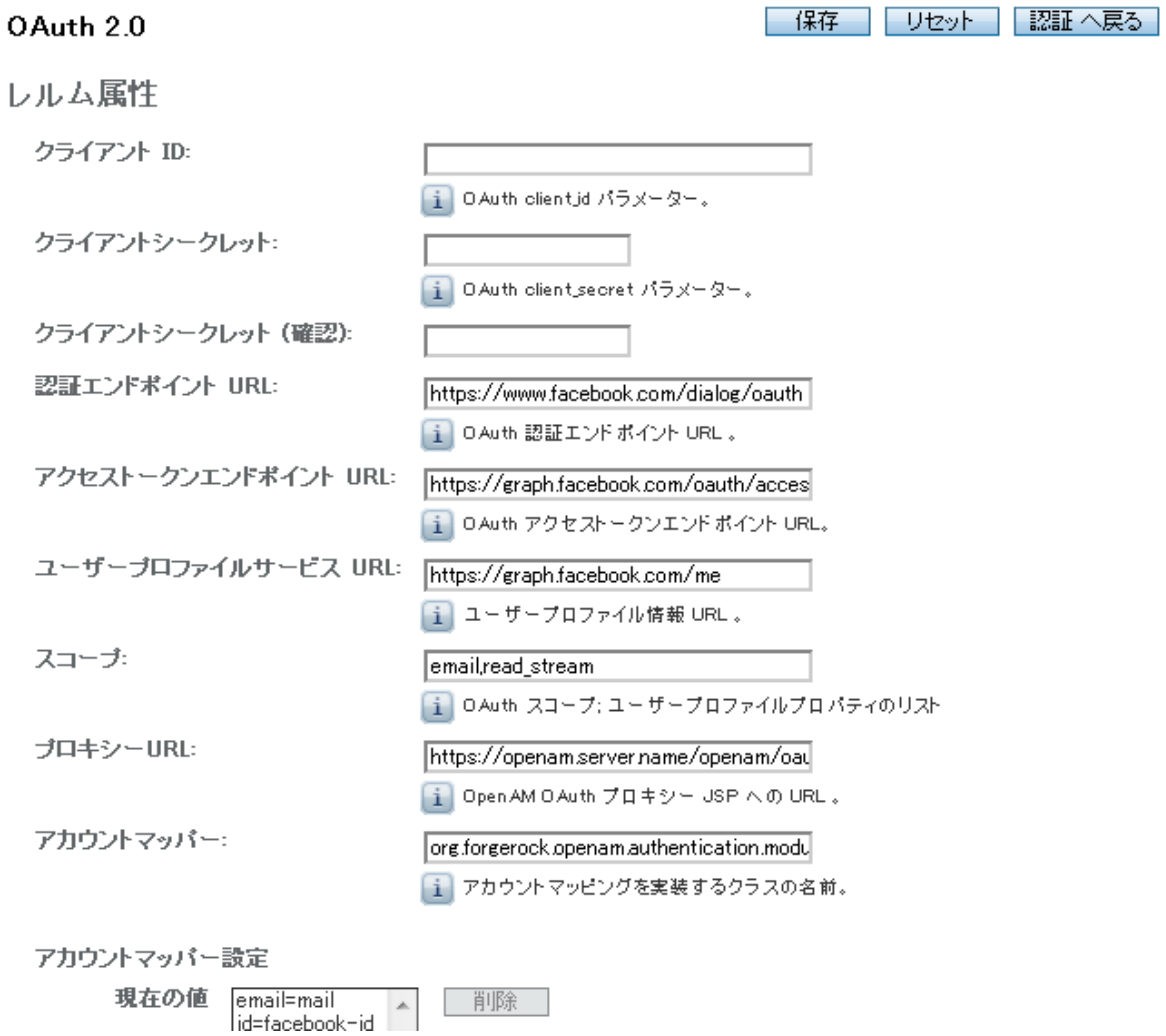
ユーザー側のアプリはOAuthを知らなくてもFacebookなどで認証することが可能

OAuth 2.0 のクライアントとして使う設定

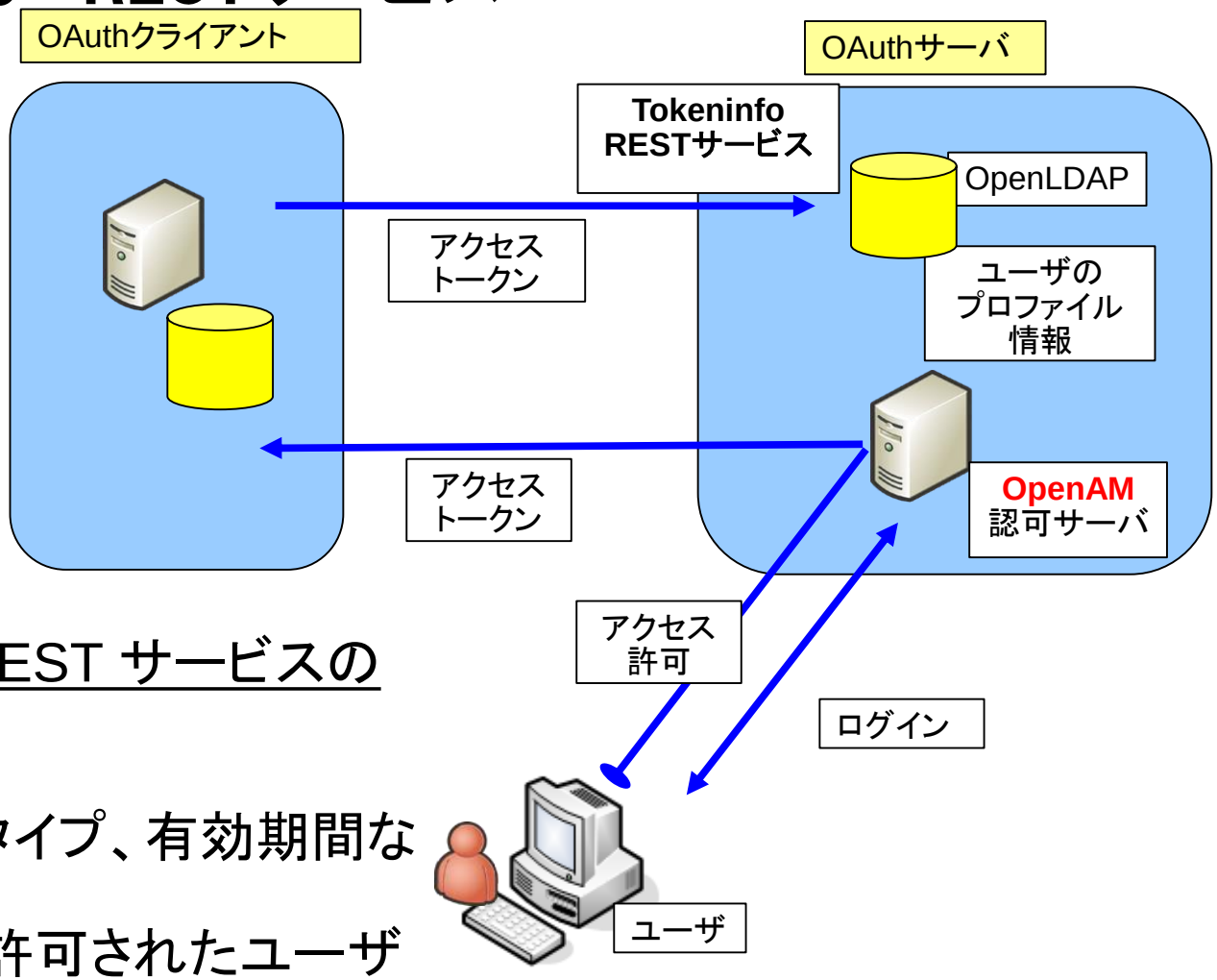
管理コンソールで

簡単設定

詳細手順は弊社ホームページで紹介中



認可サーバとしての OpenAMと“tokeninfo” RESTサービス



Tokeninfo REST サービスの応答内容

- トークンのタイプ、有効期間など
- スコープで許可されたユーザ情報

OpenAMのREST API

- RFCで規定されたもの
  - access_toke エンドポイント
  - authorize エンドポイント
- OpenAM独自
  - tokeninfoエンドポイント
    - トークンの検証
    - 属性の設定
  - トークン管理用エンドポイント

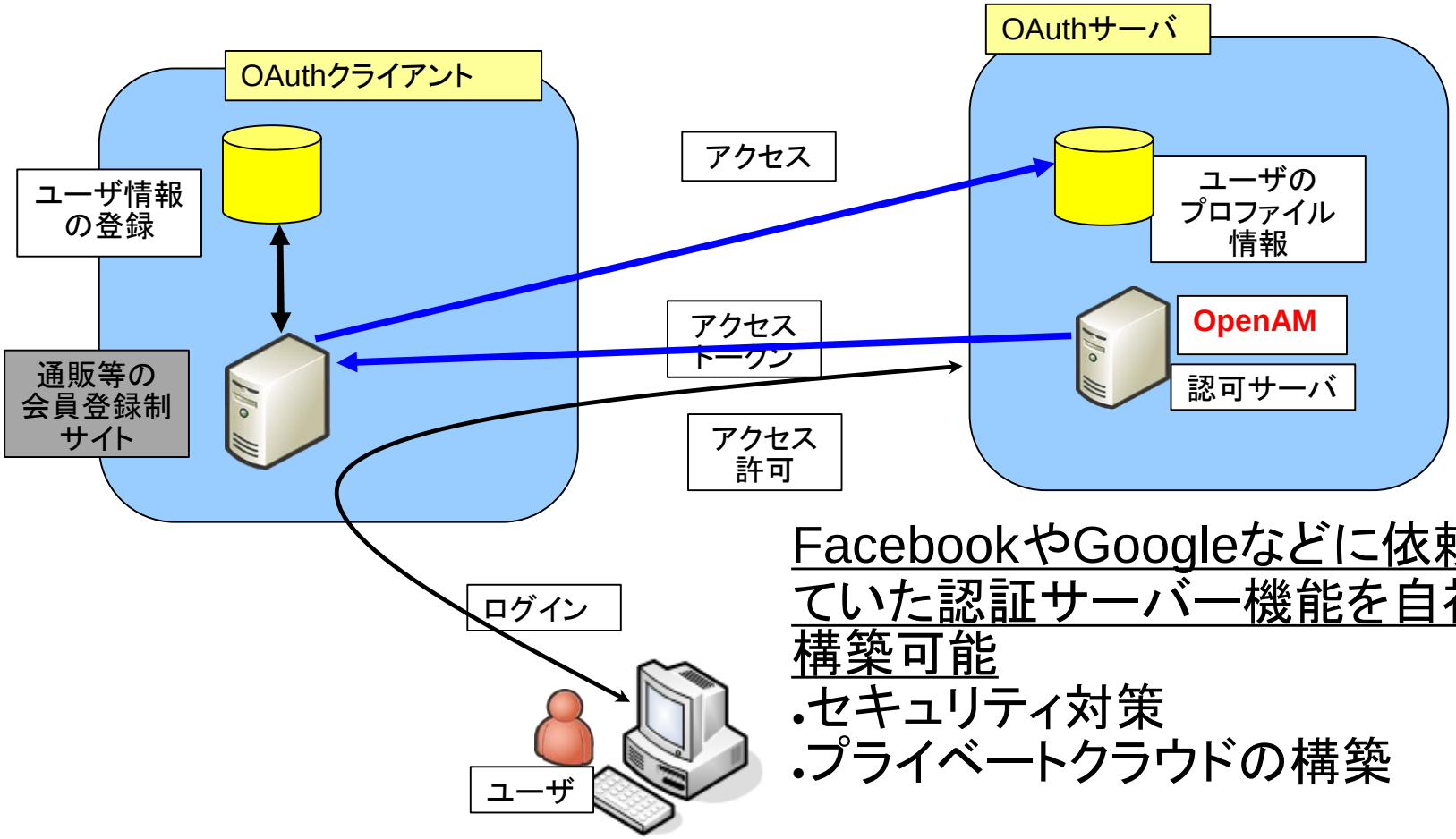
OAuth 2.0の認可サーバとして使う設定

管理者用GUIを使って簡単に設定可能

OpenID Connect は対応中！

- OAuth 2.0 の土台の上にOpenIDを構築
- OpenAM 10.2 (2013, Q2) で対応予定
- Facebook相当のOpenIDの認証サーバーを OpenAMを使って自社(オンプレミスやプライベートクラウド)で構築可能になる

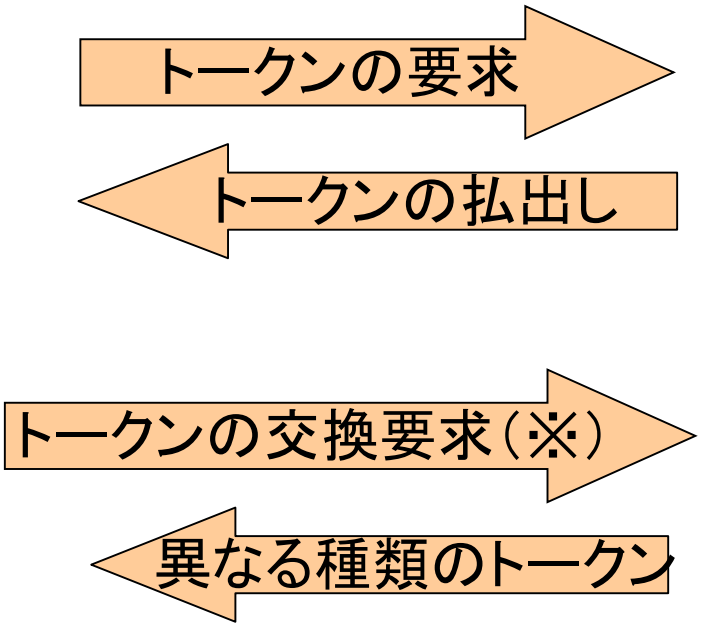
自社のサービスにFacebookなどのアカウントでログインしてもらうOAuth クライアント機能



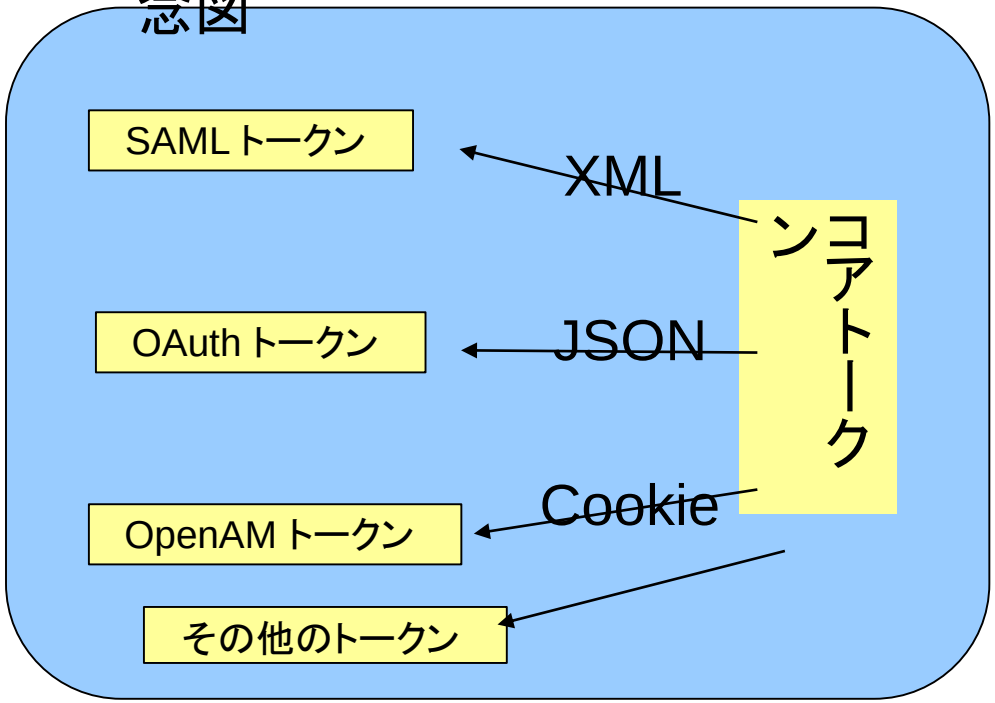
FacebookやGoogleなどに依頼していた認証サーバー機能を自社で構築可能

- セキュリティ対策
- プライベートクラウドの構築

コアトークン・サービス
（様々な認証トークンに柔軟に対応）



コアトークンサービスの概念図



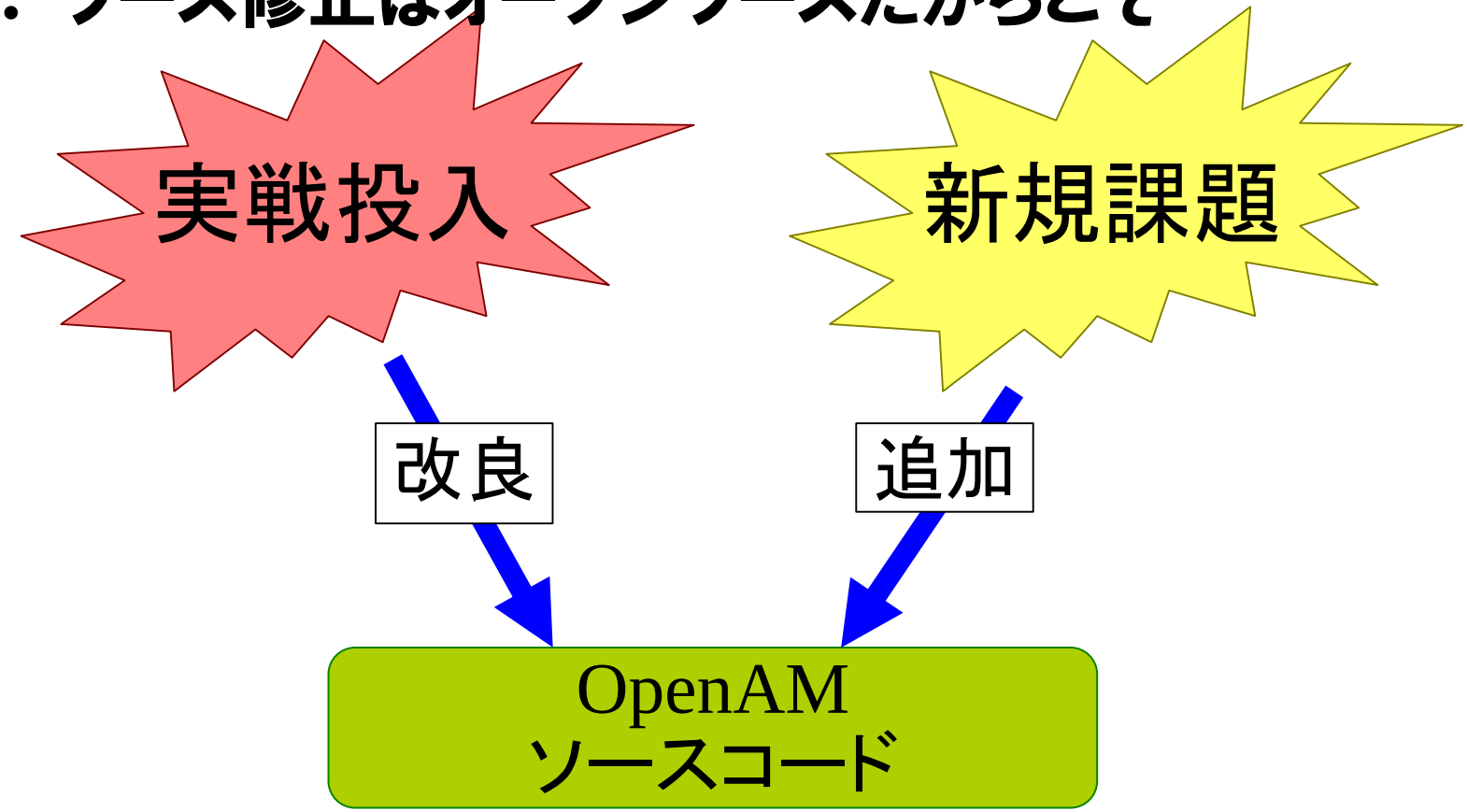
(※）token exchange はOpenAM 10.9で予定されている機能で現在は使用できません。

OSSTechのOpenAMへの取り組み

OSSTech

オープンソースであること

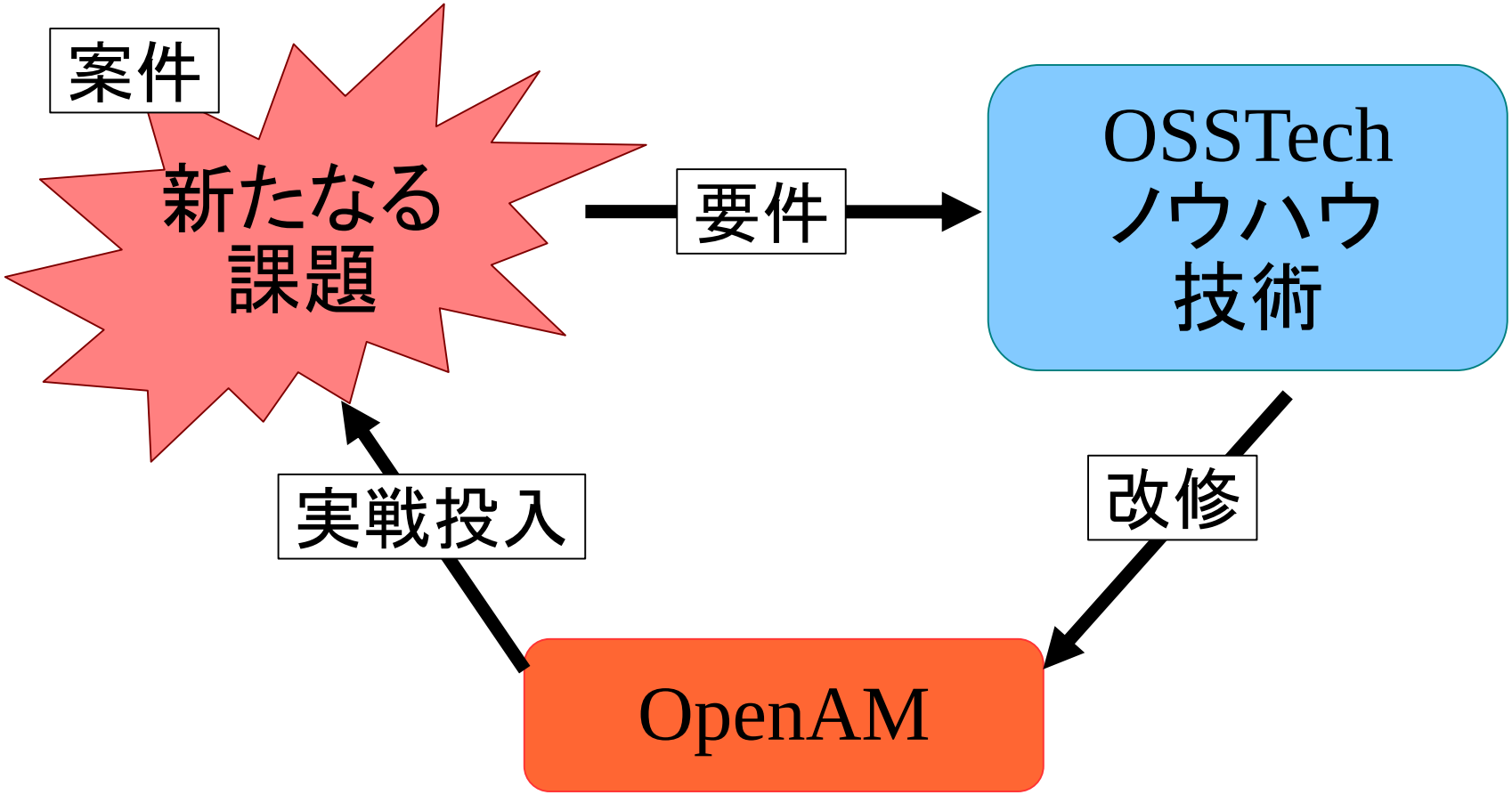
- ソース修正はオープンソースだからこそ



問題点の改良、要件に合わせた機能追加

オープンソースであること

・ソース改修力は課題解決力



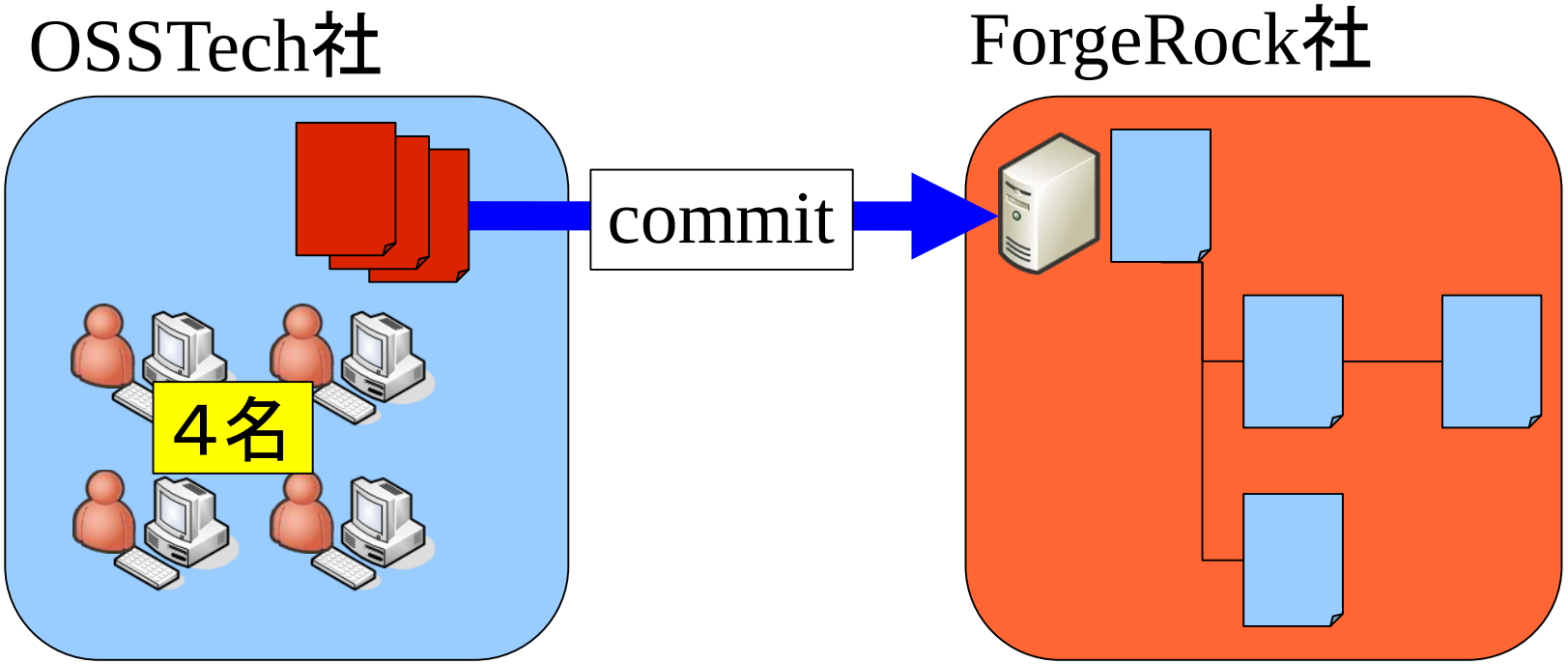
全てのサイクルをサポートできる

OpenAM ソースコードへの貢献

OSSTech

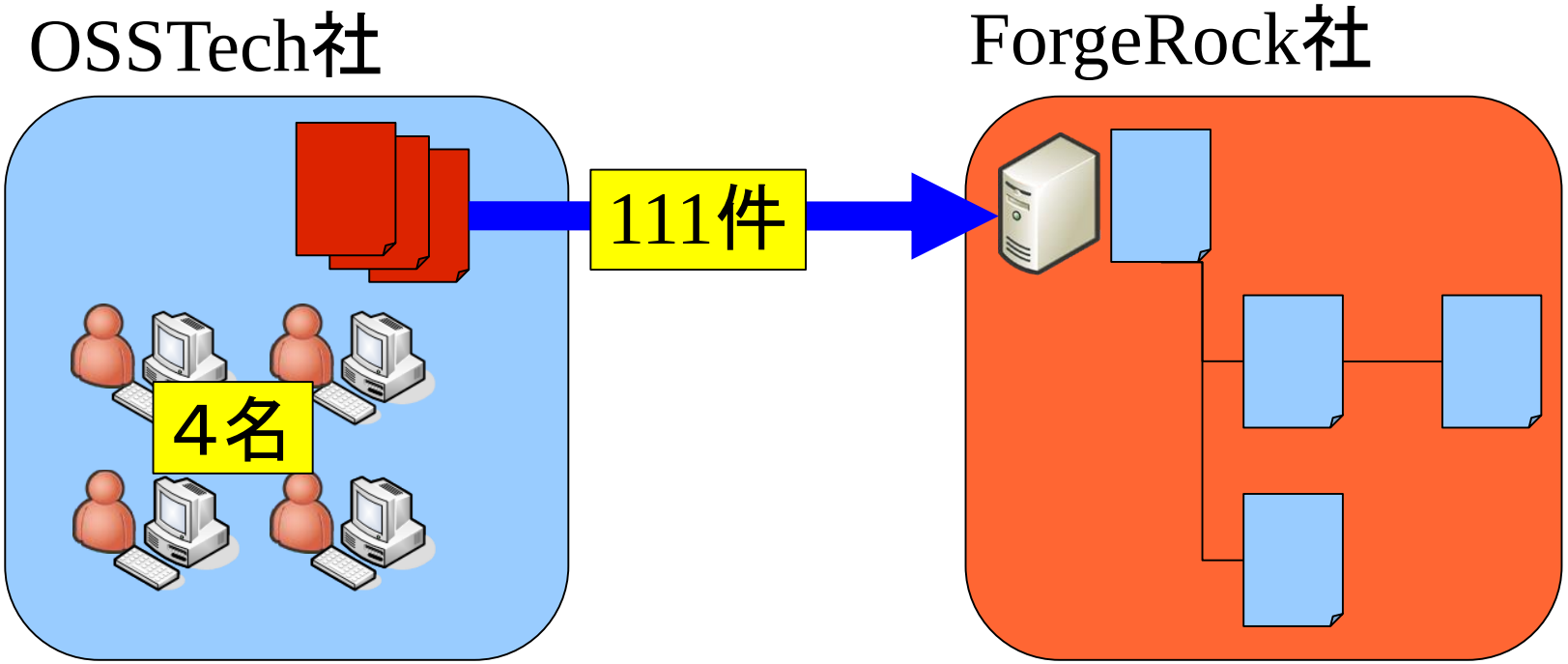
コミッター数

- 社内開発者6名
- コミット権限のある社内開発者4名
- OpenAM コミッター総数37名



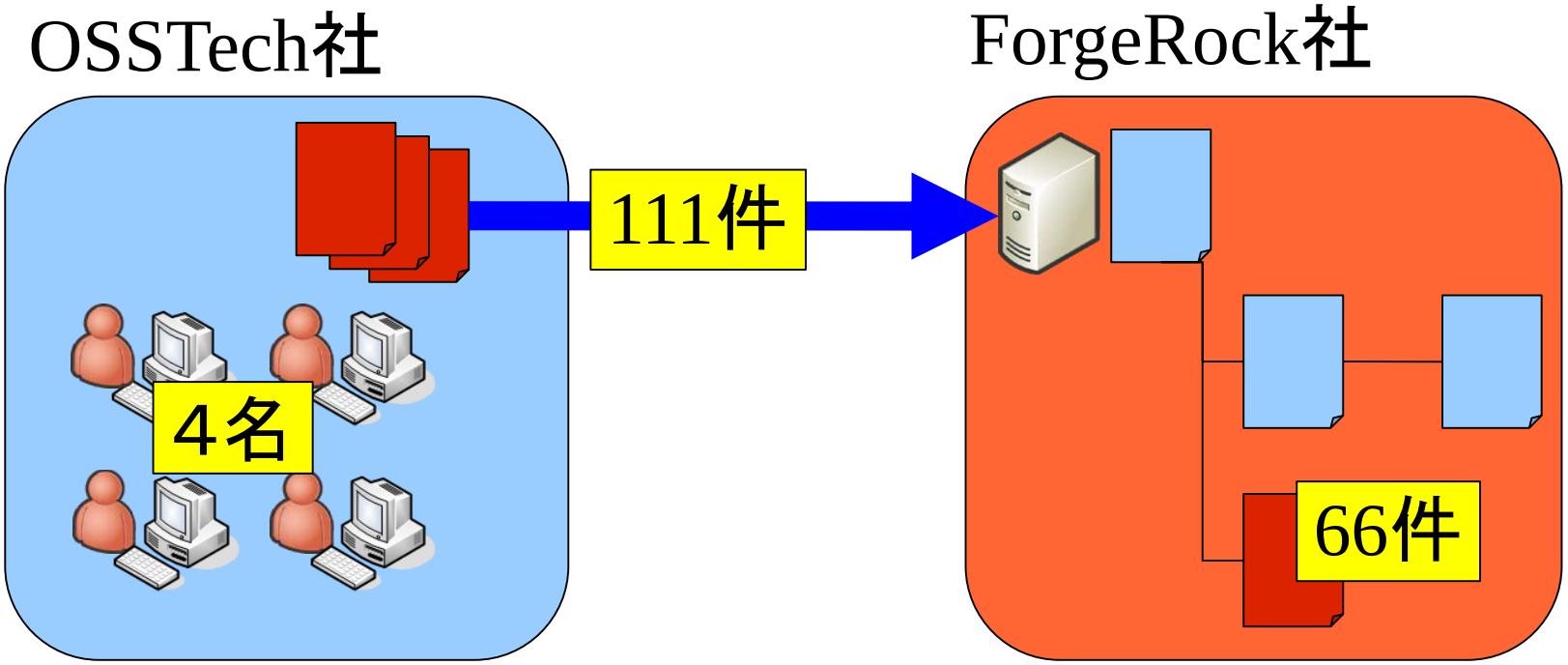
コミット件数

- 社内コミッターによるコミット件数111件
- ForgeRockツリーのコミット総数は3346件



問題修正件数

- 社内コミッターによる修正件数66件
- 現在のチケット数1739(重複等含む)



コミット例

- nginexエージェント開発
- ユーザーデータストアの修正
  - JDBCの設定が共有されてしまう問題
  - ログ出力の改善
- コマンドツール(ssoadm など)の修正
  - エージェントの設定に不正な値が登録される問題
  - Windows 用ツールが動作しない問題
- ファイルアップロードの修正
  - Safari・Chromeでファイルアップロードが動作しない問題

コミット例

- メモリリーク関連の修正
  - エージェントのメモリリーク
  - HTTPコネクションのリーク
  - DBコネクションのリーク
- マルチバイト文字
  - マルチバイト文字の表示の問題
- 日本語化
  - 日本語表示の追加
  - 誤訳の修正

OSSTech版カスタマイズ

OSSTech版カスタマイズ

- OpenLDAPと親和性向上＞自社ソリューション
  - 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

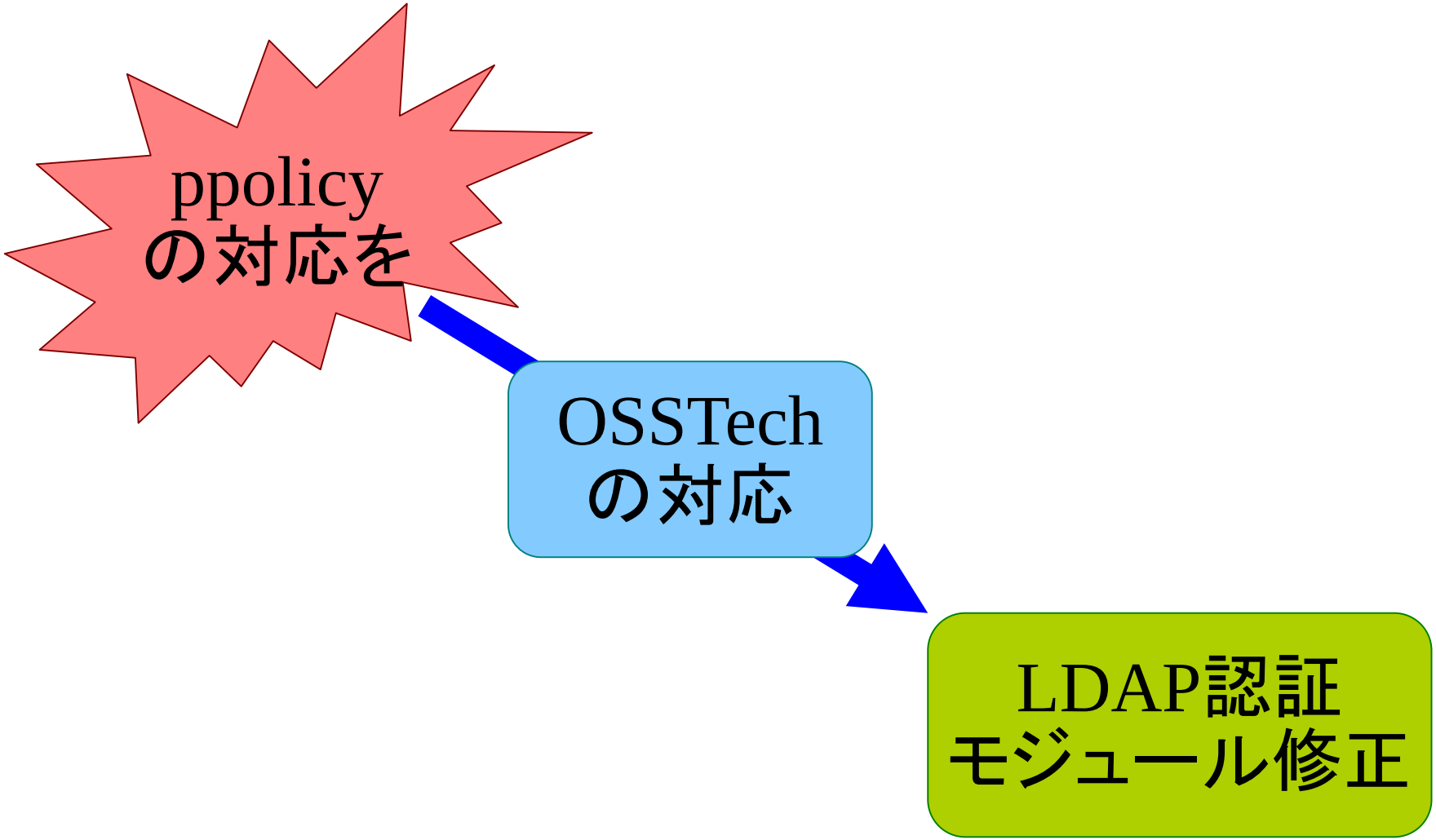
OSSTech版カスタマイズ

- 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

案件個別カスタマイズ

カスタマイズ事例

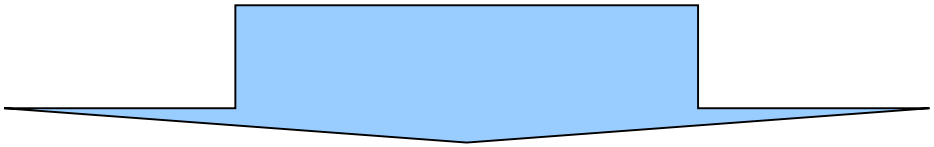
- OpenLDAP **パスワードポリシー対応**



カスタマイズ事例

- OpenLDAP **パスワードポリシー対応**

- OpenAM-9.5系ではLDAP標準のアカウントポリシー※に未対応
- 全て同一の認証エラーとなるという課題

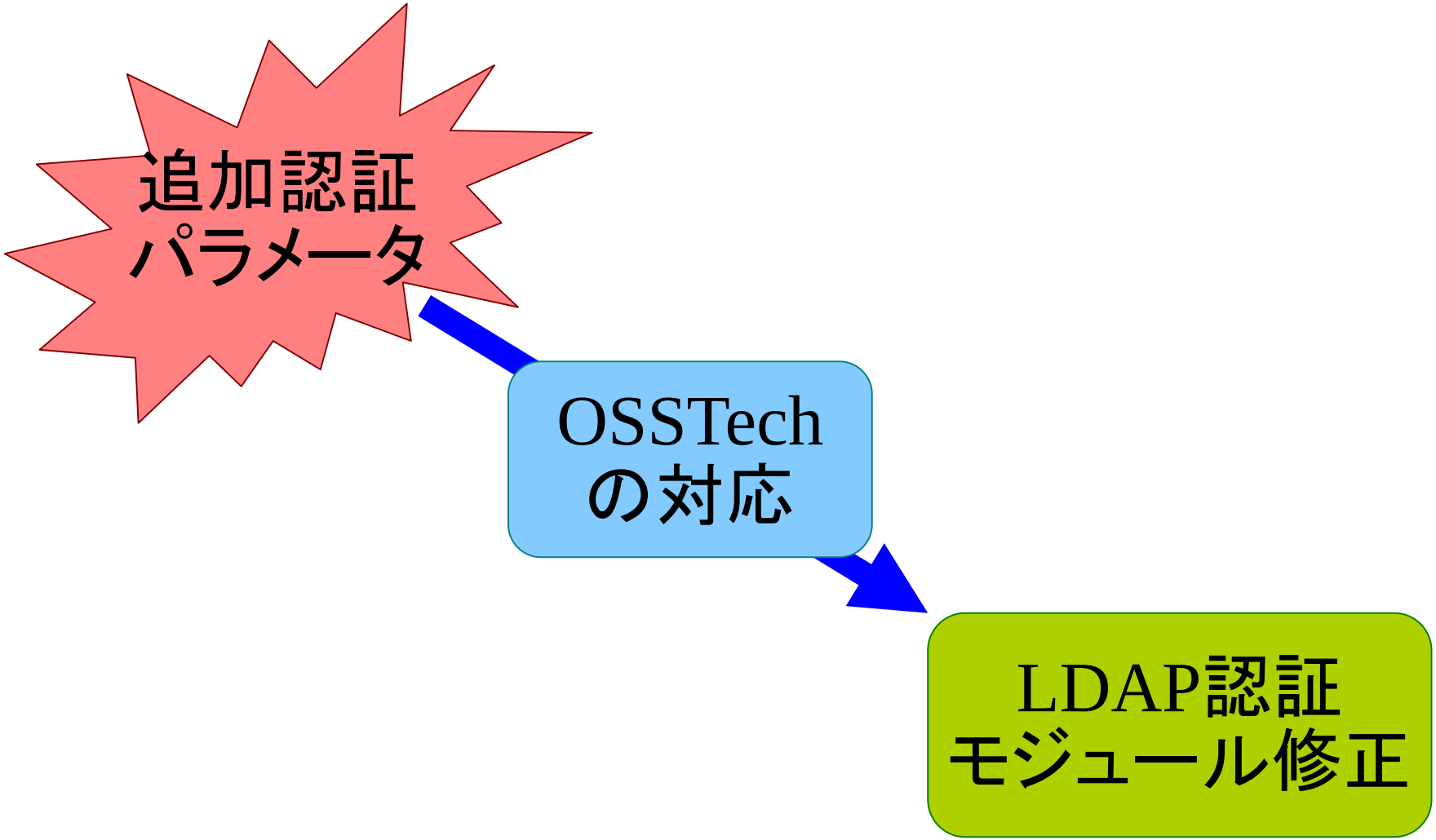


- LDAP認証モジュールにLDAPのアカウントポリシー(パスワード有効期限、ロック等)エラーをハンドリングし、個別のエラー遷移するよう改修

※アカウントポリシーとはパスワード有効期限、アカウントロックアウト等
SunJavaDSやOpenDSを利用する場合は独自実装で対応されていた。
OpenAM-10から対応開始

カスタマイズ事例

- 認証パラメータの追加

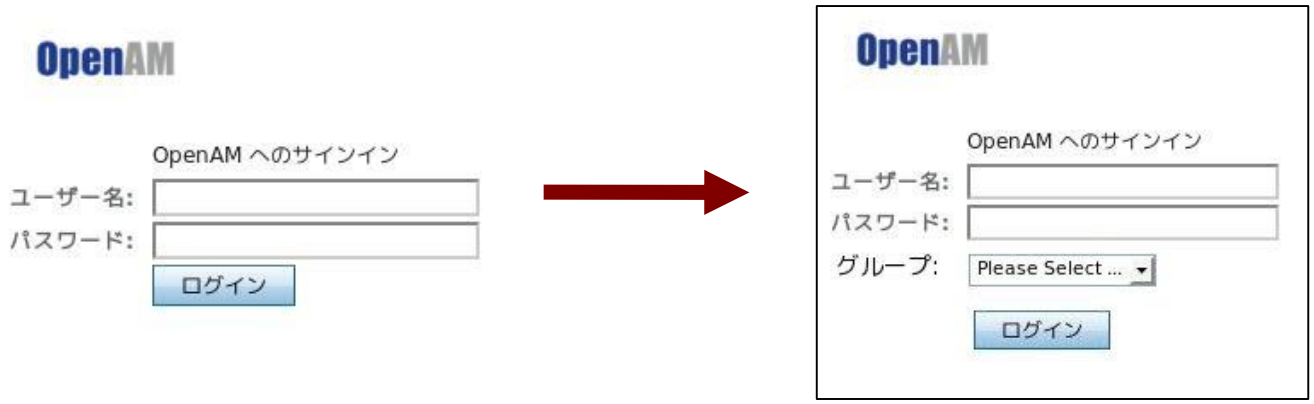


カスタマイズ事例

- 認証パラメータの追加

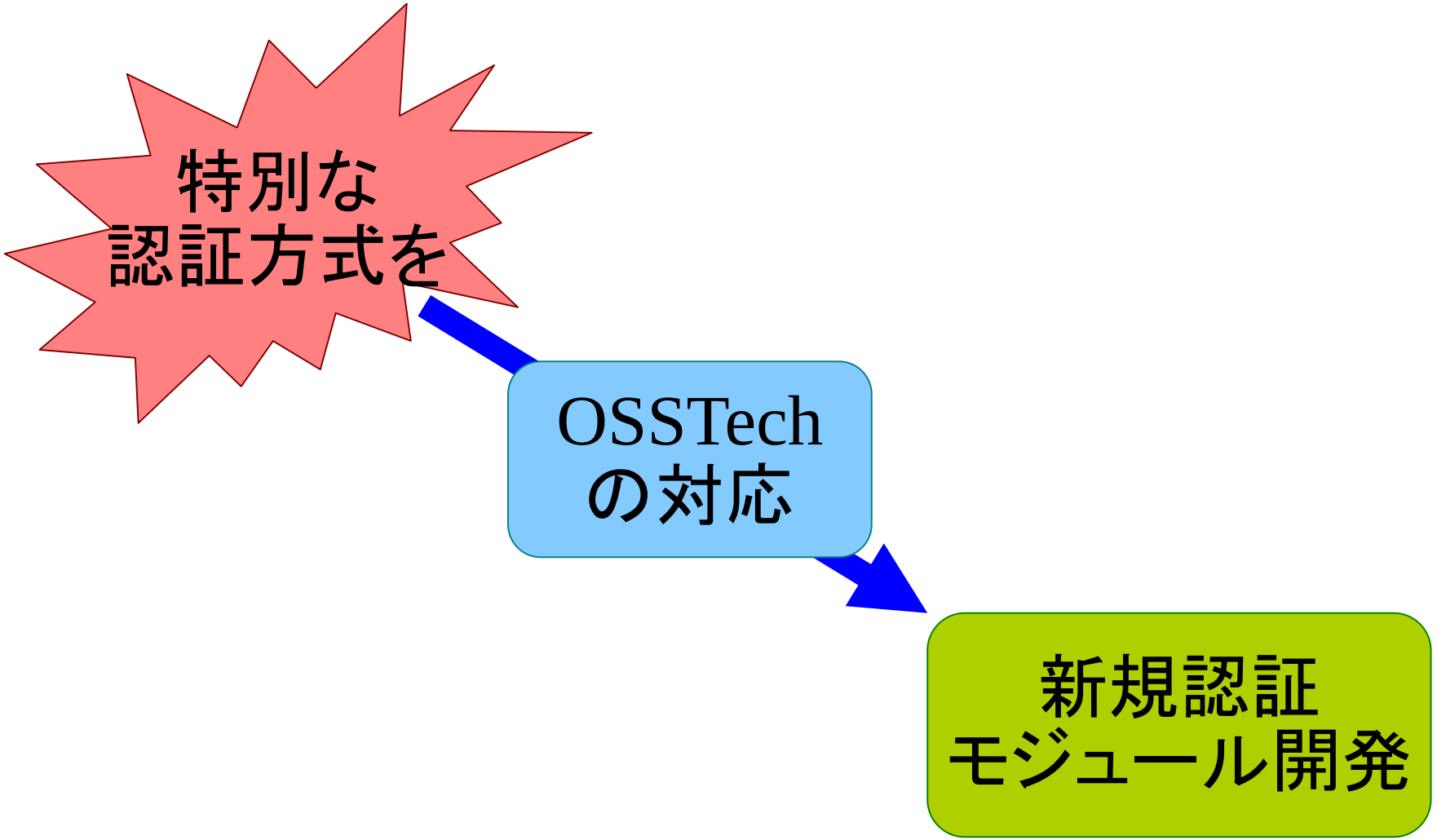
- LDAP認証時に入力するユーザー名、パスワード以外に別パラメーターをドロップダウンリストとして表示し入力したい

- LDAP認証モジュールを別パラメーター取得、表示可能なよう改修した



カスタマイズ事例

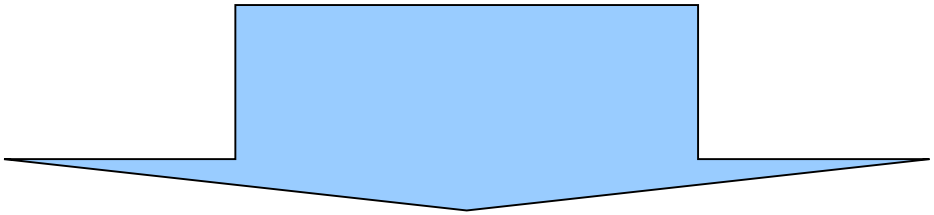
- 認証モジュールの開発



カスタマイズ事例

- 認証モジュールの開発

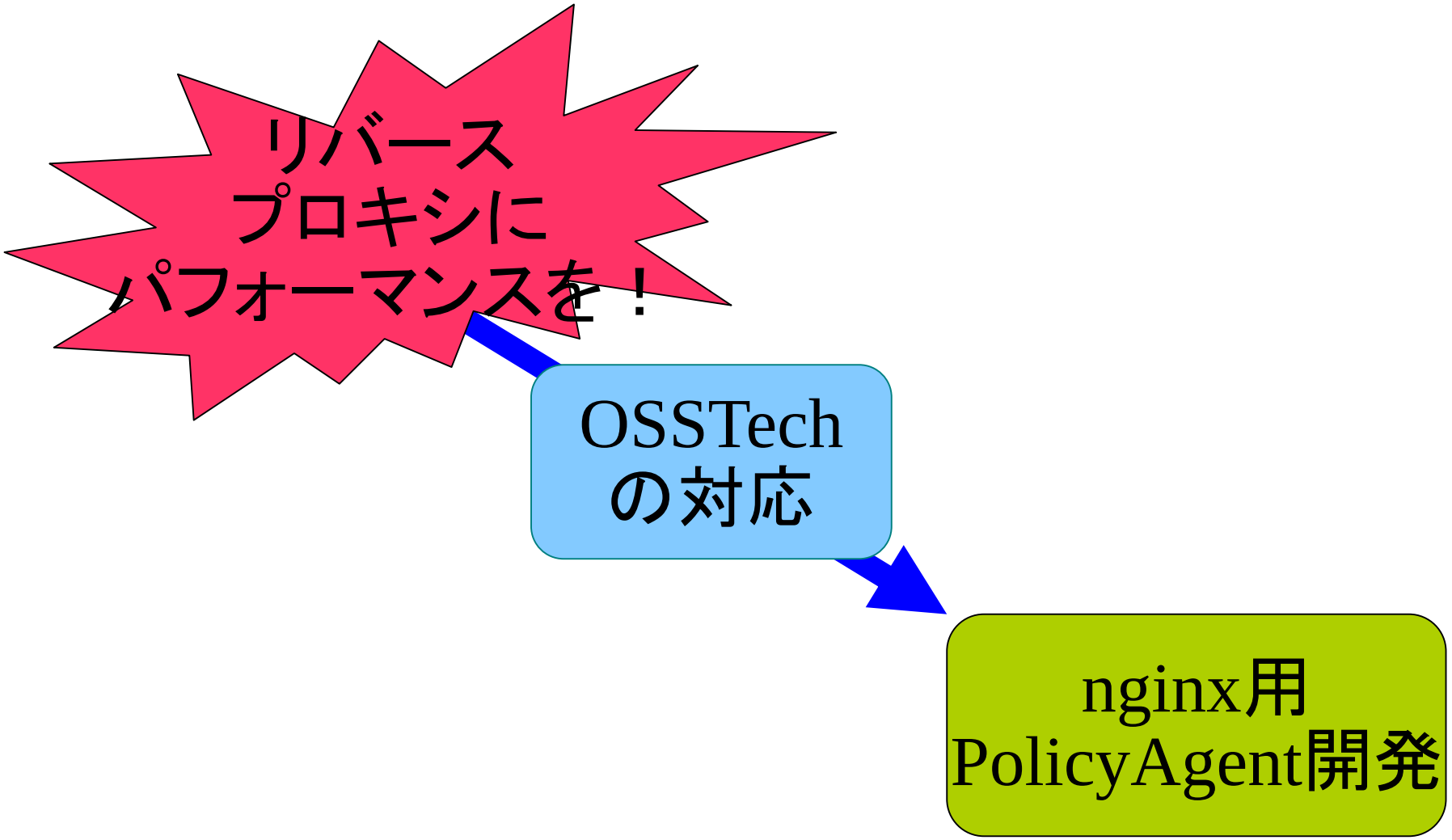
- 既存認証モジュールでは対応できない認証方式(リクエストヘッダ)で認証したい



- 要件に合った認証モジュールを開発し、既存モジュールとの認証連鎖とした。

開発事例

- Apache**より早いリバースプロキシを構築したい**



開発事例

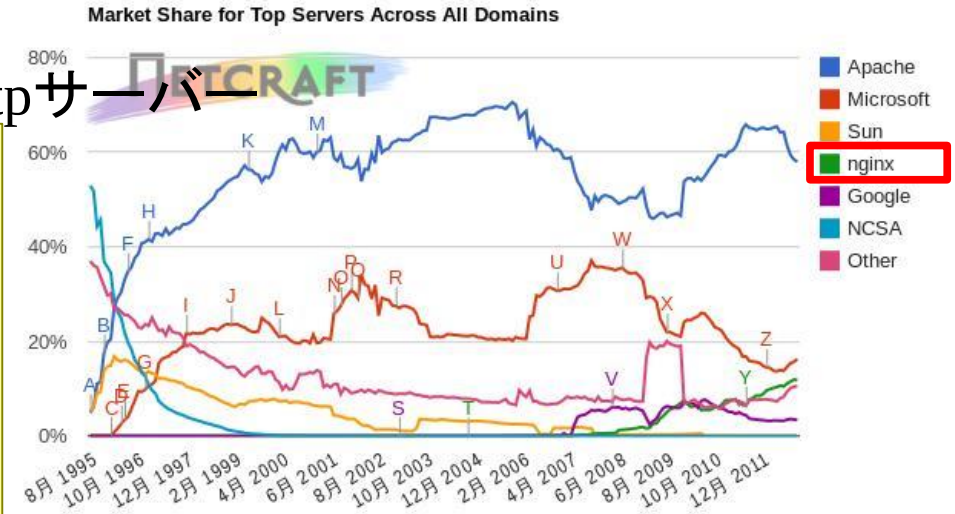
- Apacheより早いリバースプロキシを構築したい

- 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



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*

