OpenAM（OpenSSO）のご紹介

OSSTech

オープンソース・ソリューション・テクノロジ株式会社
2010/12/1
野村　健太郎

目次

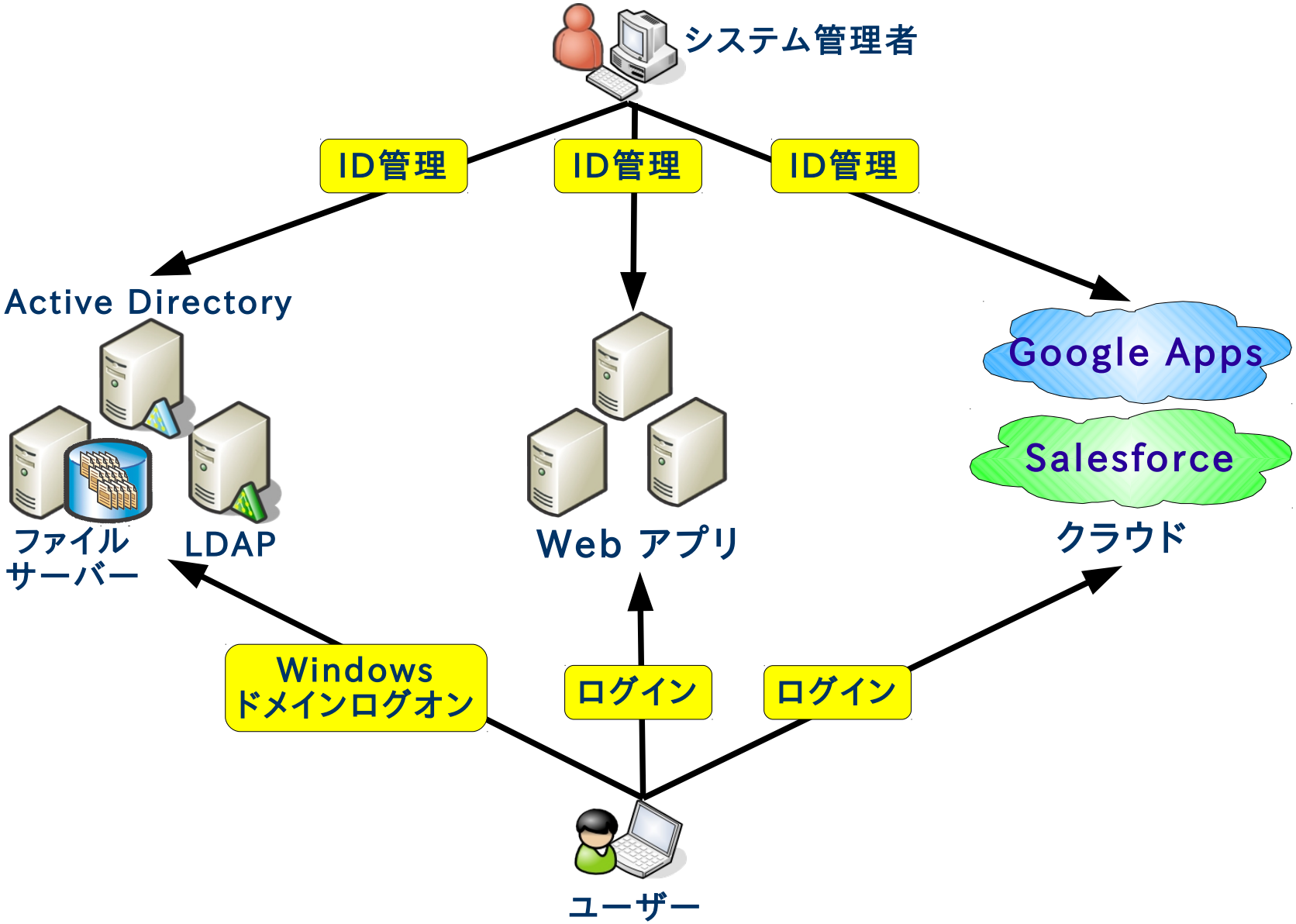
- 会社紹介
- OpenAM（OpenSSO）のご紹介
  - 概要、開発の歴史
  - シングルサインオン方式
  - 認証方式（認証連鎖による多様素認証）
  - レルムによるユーザー管理
  - 冗長化
  - 導入事例
- OpenAM（OpenSSO）デモ

会社紹介

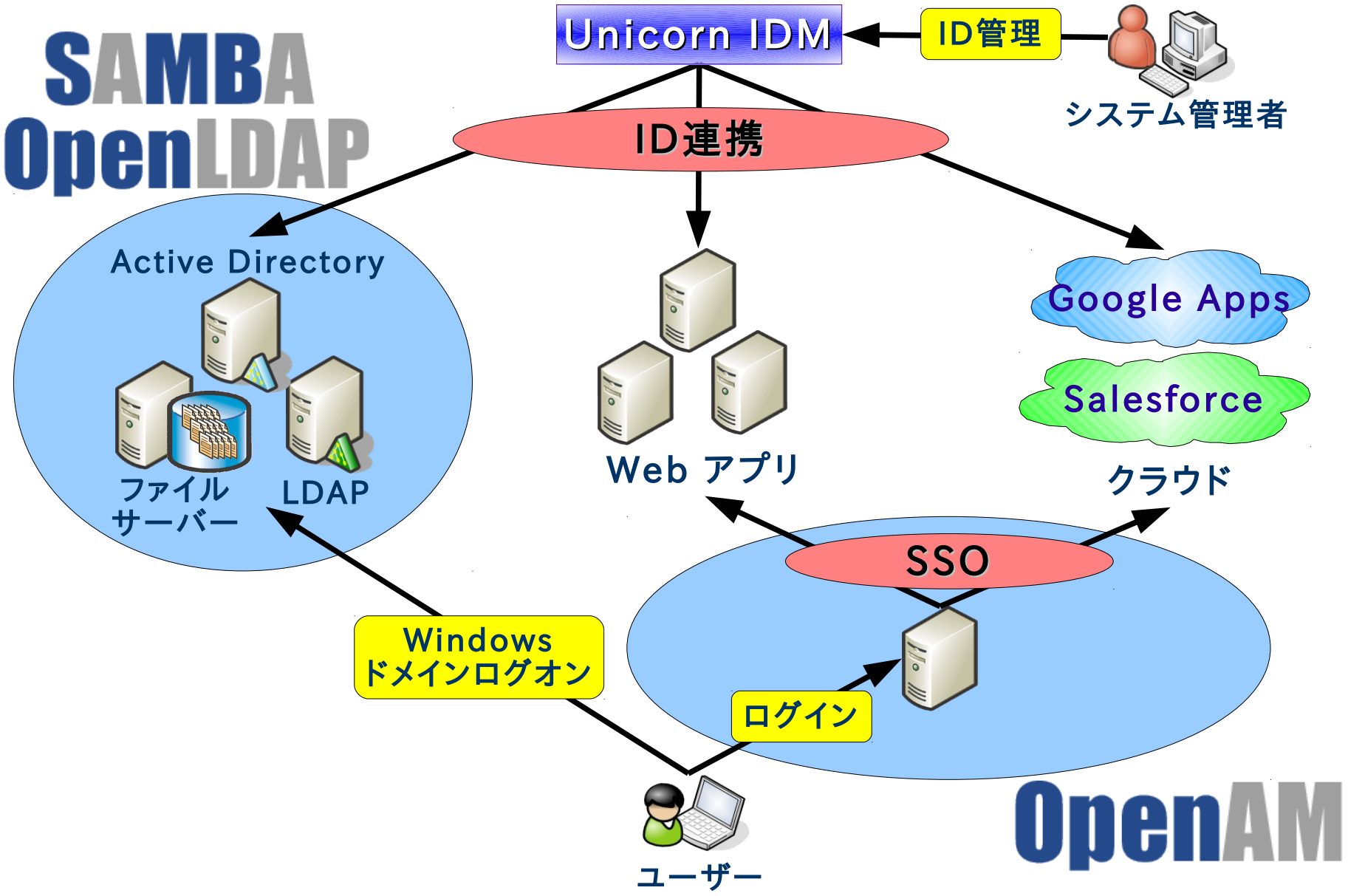
オープンソース・ソリューション・テクノロジ株式会社

- **OSに依存しないOSSのソリューション**を中心に提供
  - Windows/Solaris から Linux への移行も支援!
- **OSSを利用した認証基盤構築**が得意分野
  - LDAP認証、Windowsドメイン認証、Webアプリケーション認証、**クラウド認証**
- **Samba,OpenLDAP,OpenAM,IDM**などによる認証統合/シングルサインオン、ID管理ソリューションを提供
  - OSSの製品パッケージ・製品サポートを提供
  - OSSの改良、バグ修正などコンサルティングにも対応

OSSTechのソリューション領域



OSSTechのソリューション導入効果



OpenAM（OpenSSO）概要

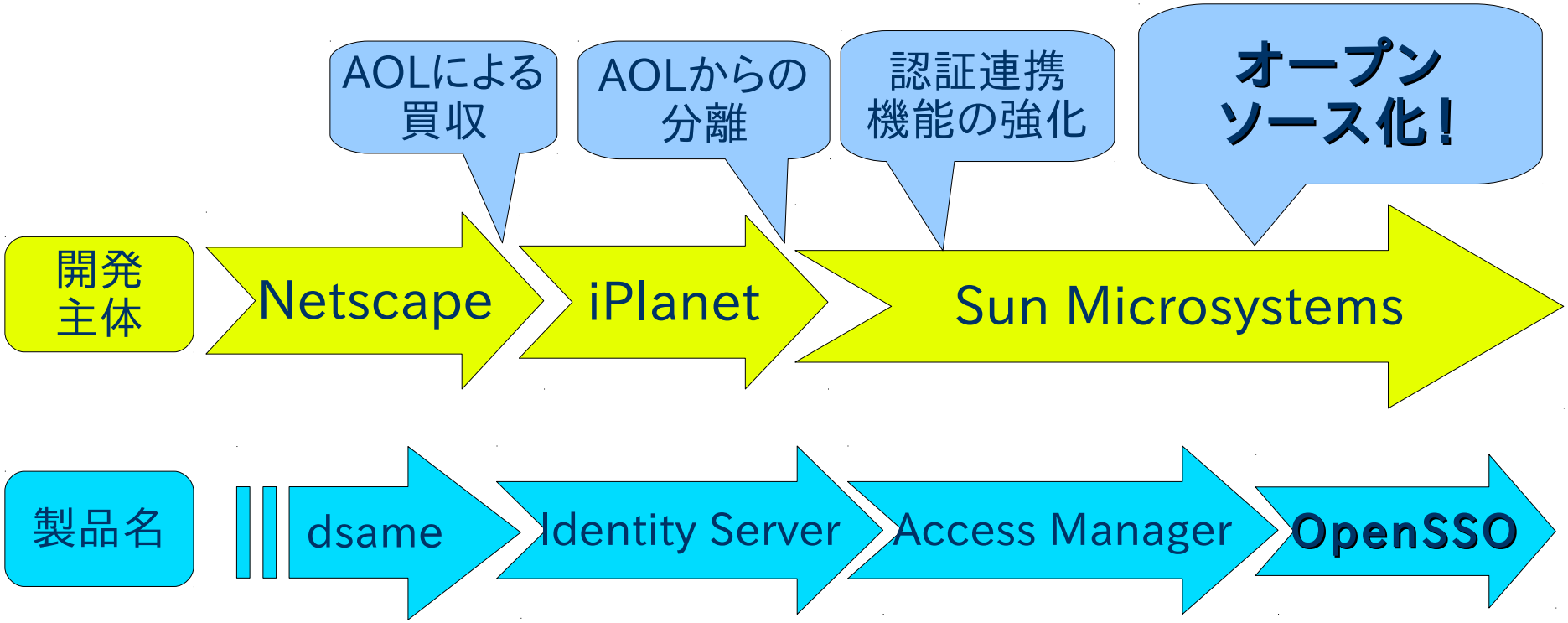
OpenAMとは

- 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
  - **シングルサインオン（SSO）**：一度のログイン操作さえ完了すれば、複数の Web アプリケーションにログイン操作することなくログインすることが可能

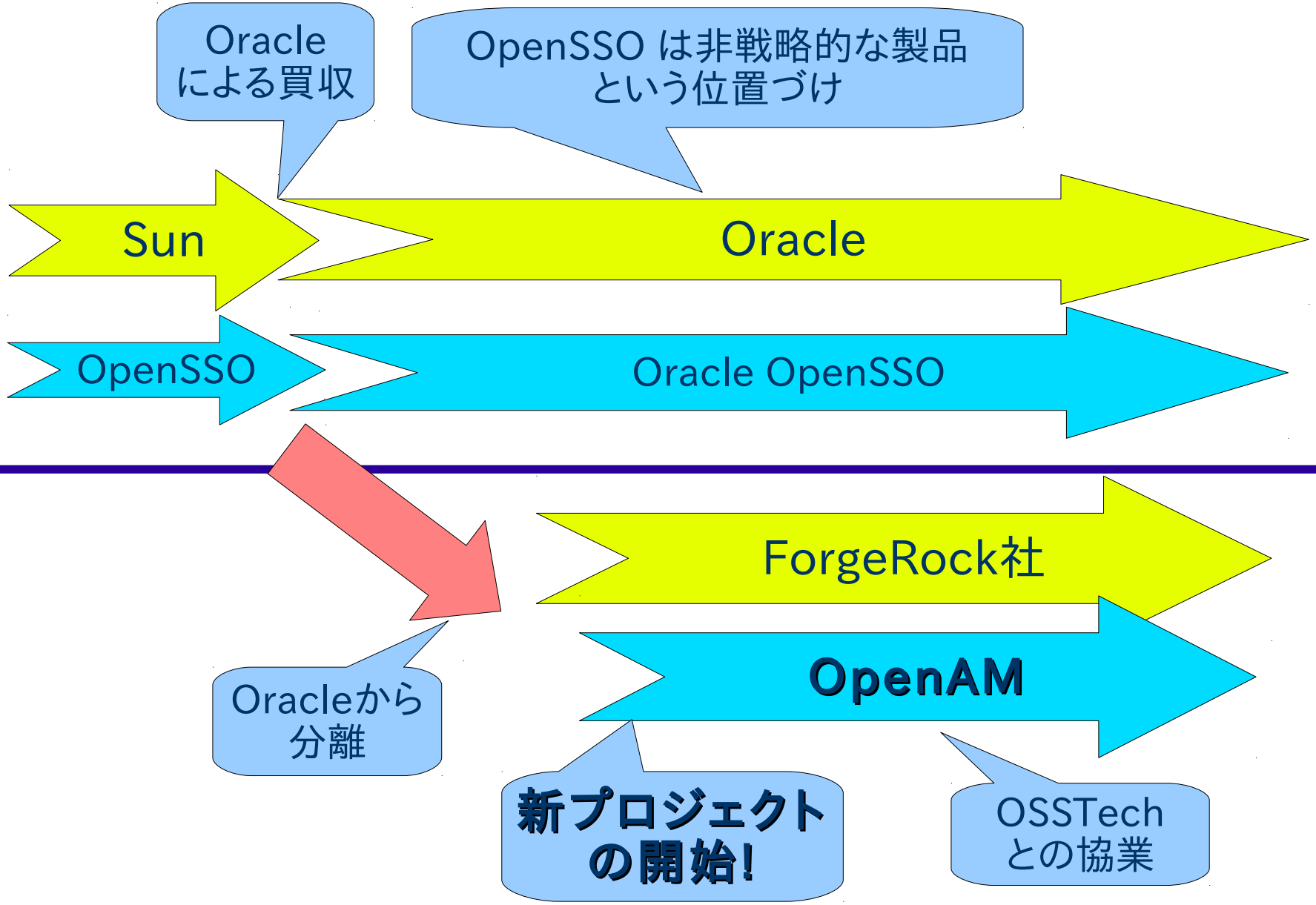
- ユーザー情報を格納するためのユーザーリポジトリ（**ユーザーデータストア**）として様々な LDAP サーバー、RDBに対応
  - RDBへの対応は OpenAM からサポート開始

- **SAML、OpenID、OAuth、ID-WSF**などの認証・認可に関連した複数のプロトコルをサポート

OpenAMの歴史 - その1



OpenAMの歴史 - その2



OpenAMのこれから（技術面）

- OpenAM は OpenSSO の正常進化形
  - OpenSSO を担当していたエンジニアが中心になり Forgerock社を設立
  - ベースにするソースコードが同じ
  - 最新の Ver. 9.5 では多量のバグフィックスを適用
  - OpenSSOと完全互換
- クラウド対応
  - Google Apps, Salesforce とのシングルサインオン（SAML）連携機能を強化
  - GUI による操作でシングルサインオン設定が可能
- 機能拡充
  - ワンタイムパスワード機能の追加
  - ユーザーリポジトリしてRDBをサポート

OpenAMのこれから（ビジネス面）

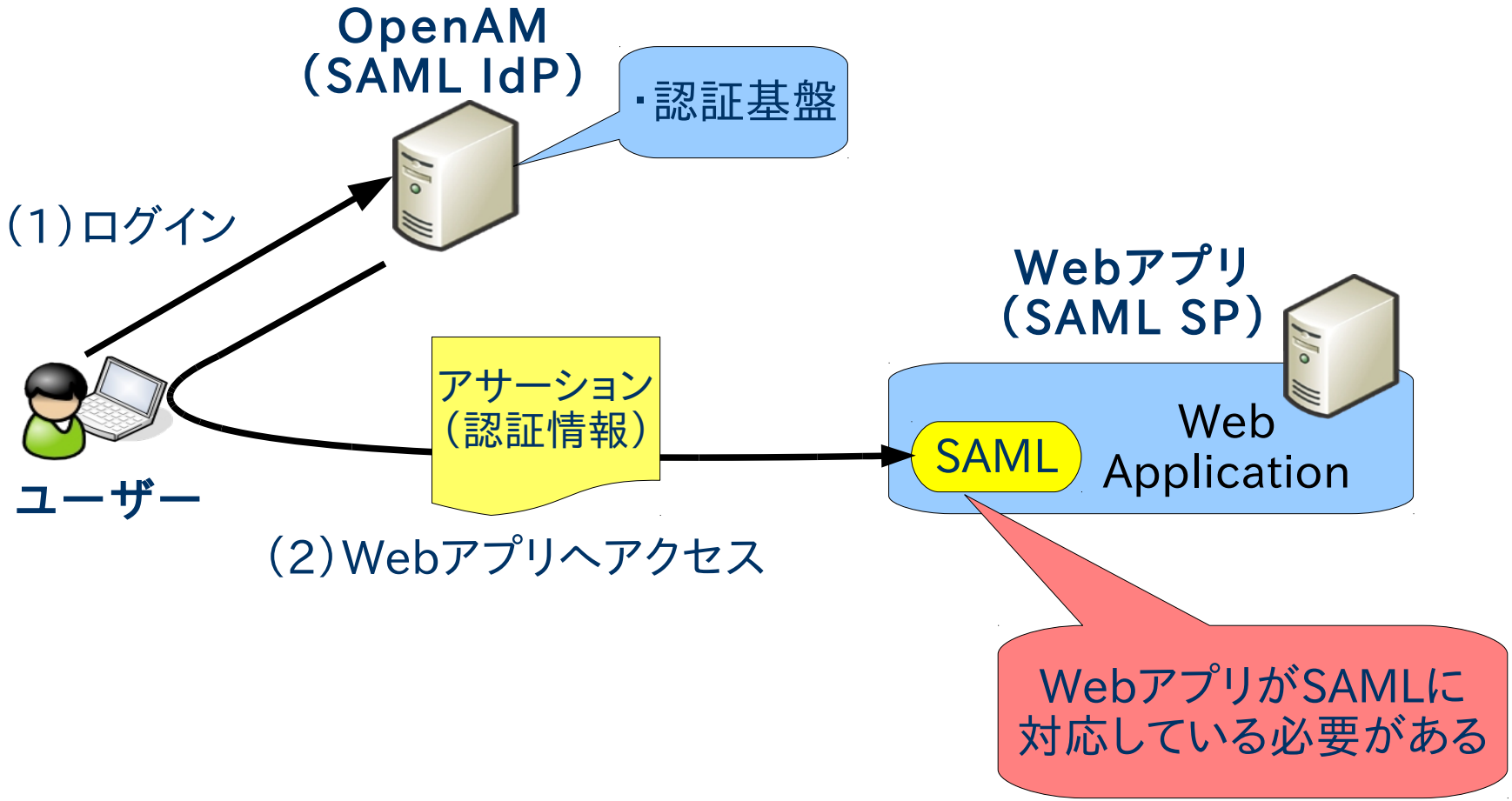
- ベンダ独自のパッケージングも可能
  - 生体認証などの独自認証方式を組み合わせる
  - ID管理システムと組み合わせる
  - OSSTech 版 OpenAM の特徴
    - OpenLDAP 用拡張スキーマを提供
    - ID管理製品（Unicorn IDM）との組合わせ
    - Google Apps シングルサインオンソリューションを提供
- 需要
  - 日本では多くが新規ユーザー
  - 企業・大学などの認証基盤として OpenAM を利用
  - **クラウドにおける認証基盤**として OpenAM を利用
  - 既存ユーザー（Sun Access Manager、OpenSSO）からの移行（米国、ヨーロッパ）

OpenAMの機能（その1）

多様なシングルサインオン方式

シングルサインオンの方式（1）

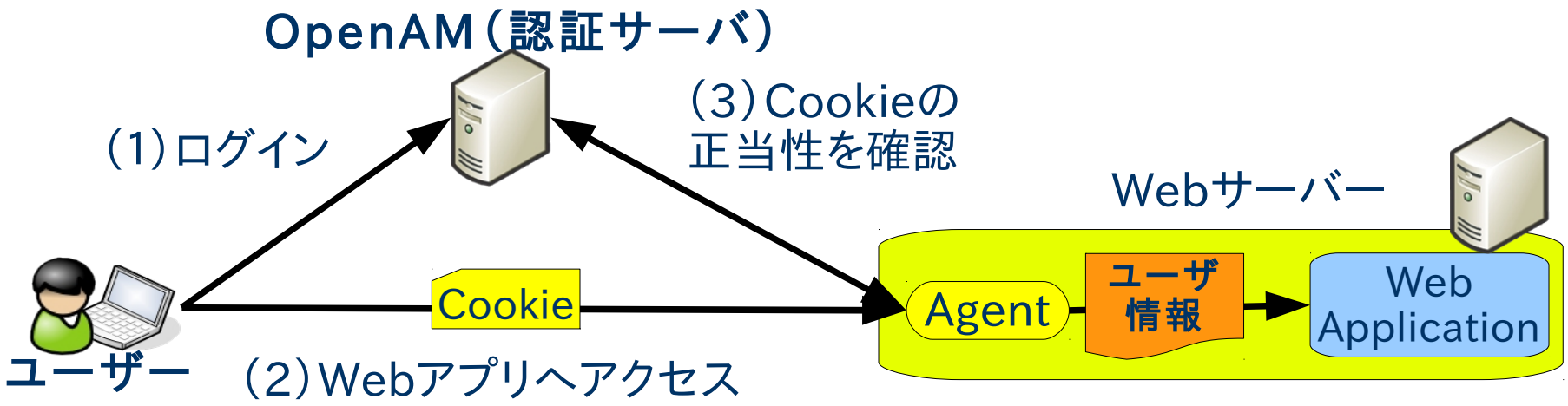
SAML



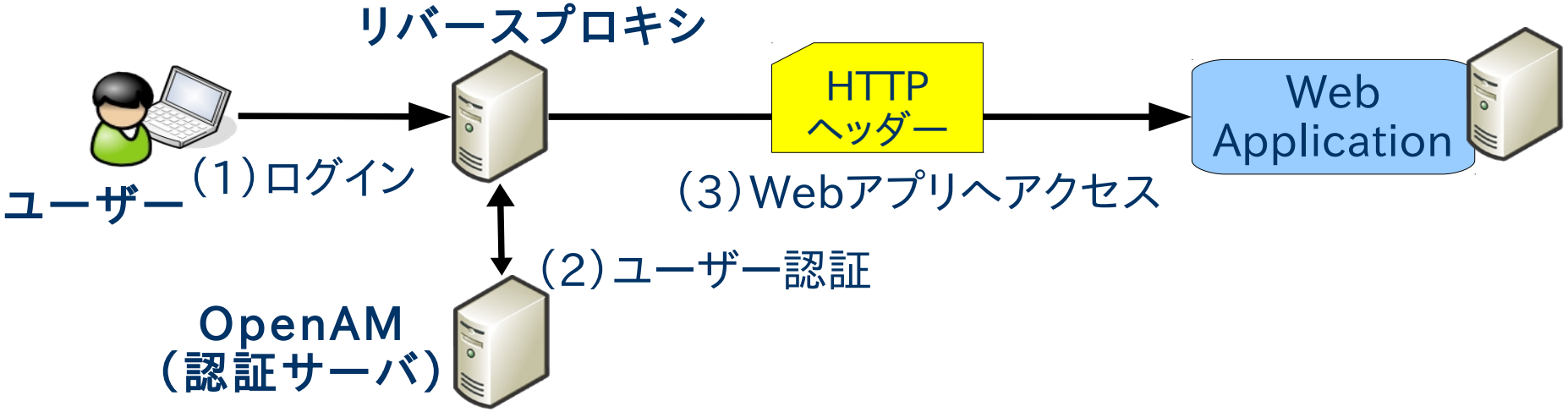
※この図は、HTTP Redirect Binding/HTTP POST Binding の場合の例です。

シングルサインオンの方式（2）

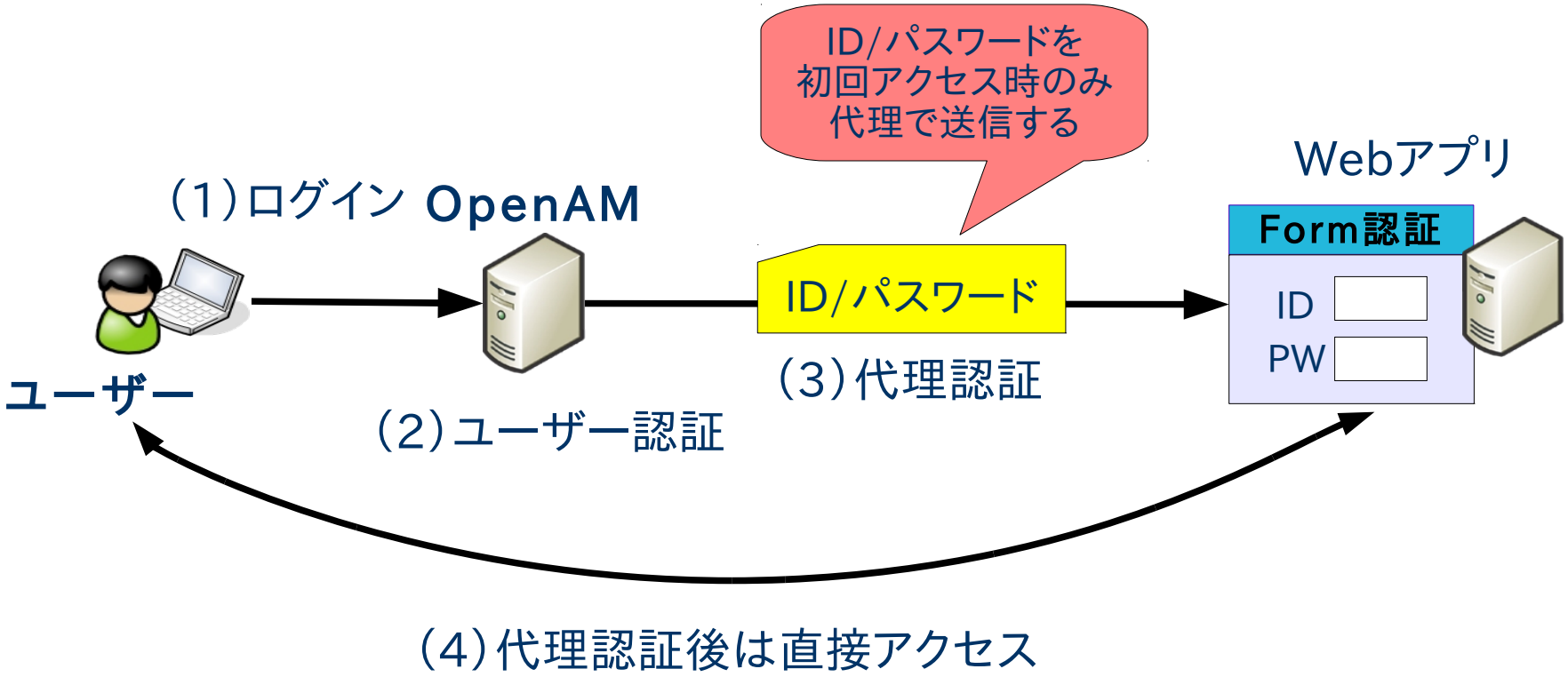
エージェント方式



リバースプロキシ方式



代理認証方式



OpenAMの機能- シングルサインオン

- SAMLによるシングルサインオン
  - ***S***ecure ***A***ssertion ***M***arkup ***L***auguage
  - 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
- 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

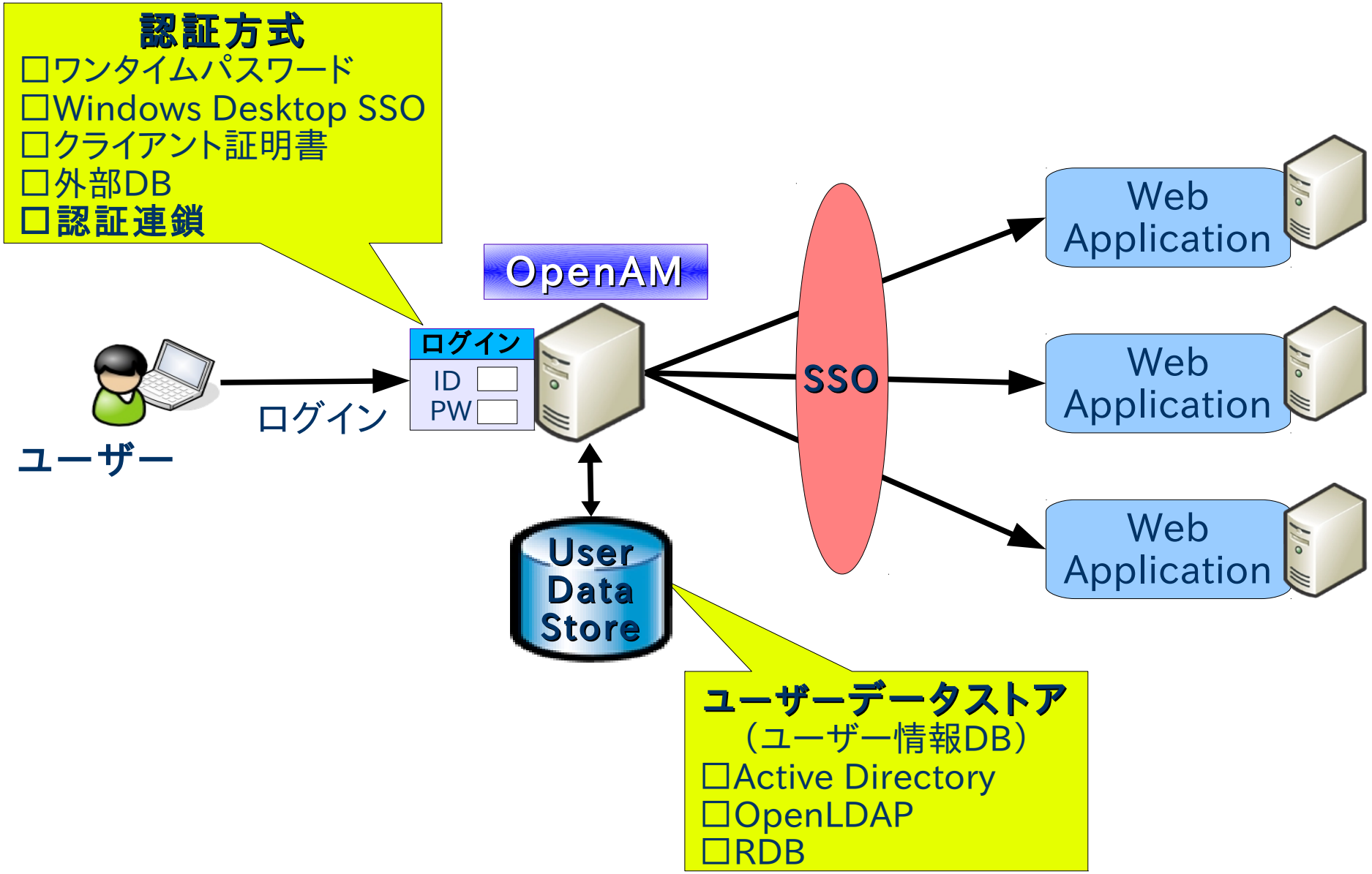
OpenAMの機能 - シングルサインオン

- 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）

OpenAMの機能（その2）

認証方式（多様素認証）

OpenAMの機能-データストアと認証方式



OpenAMの機能 - 認証方式

- 基本的には OpenAM のユーザーデータストアに保存された ID/パスワードにより認証を行なう
- ユーザー認証時に外部のデータベースを参照することも可能
  - LDAP、Active Directory、RADIUS、RDB（JDBC）
- よりセキュアな認証方式も使用可能
  - ワンタイムパスワード（電子メールを利用）
  - クライアント証明書による認証
  - Windows Desktop SSO（**統合Windows認証**）
- 複数の認証方式を組み合わせて使用可能：**認証連鎖**

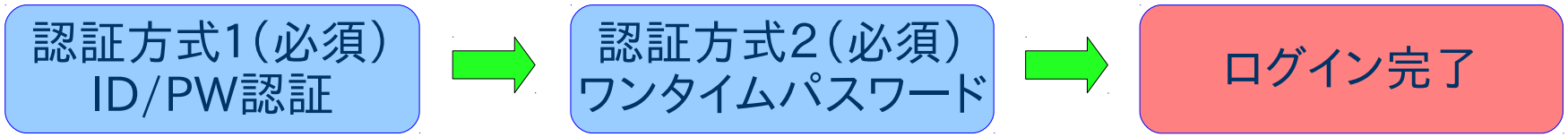
OpenAMの機能 - ユーザー情報DB

- ユーザーデータストア
  - OpenAMのユーザー情報を格納するLDAPサーバー/データベースサーバー
    - Active Directory
    - Open LDAP
    - Sun Directory Server
    - OpenDS（Sun Directory Server のオープンソース版。OpenAMに標準で組み込まれている）
    - RDB（OpenAMから対応）

OpenAMの機能 - 認証連鎖

- 多様素認証の必要性
  - 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



OpenAMの機能（その3）

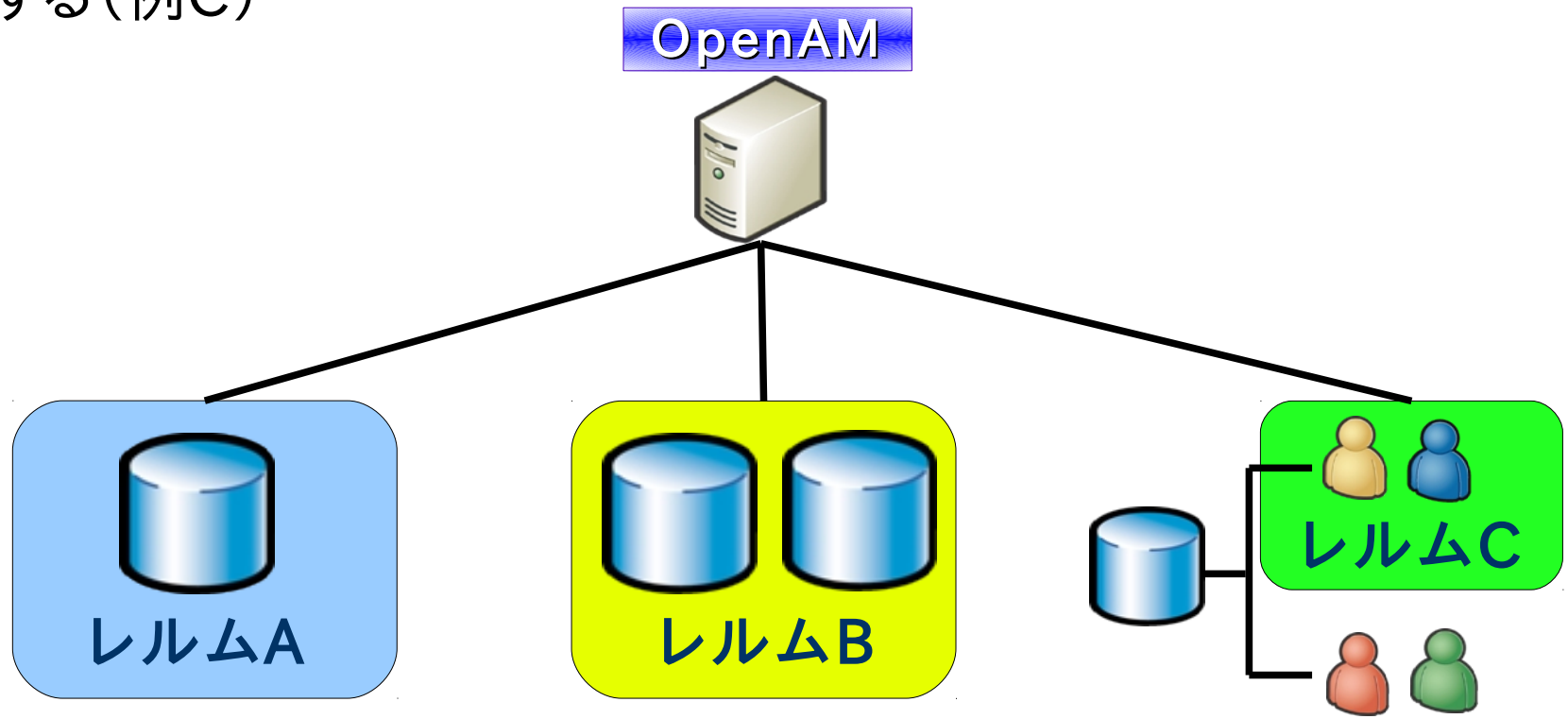
「レルム」によるユーザー管理

OpenAMの機能 - レルム

- 「レルム」:OpenAMの設定を管理するための単位の
- 以下の設定をレルム単位で管理
  - ユーザーデータストア(LDAPベースDN、検索フィルタなども指定可能)
  - アクセス制御ポリシー
  - 認証方式
- 基本的には、ユーザー情報DB単位でレルムを分ける
- レルム毎に管理者を置き管理を委任することが可能

OpenAMの機能 - レルム使用の具体例

- 複数組織（複数の企業など）のシングルサインオン基盤をOpenAM で構築し、組織毎に設定を行なう
- 組織内に存在する複数の DB を一つのレルムに登録し、全てのユーザーに同一のシングルサインオン環境を提供する（例B）
- DB内の特定のユーザーに対してのみ、シングルサイオン可能にする（例C）

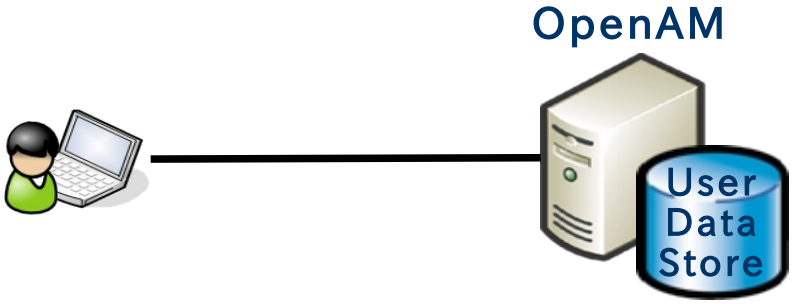


OpenAMの機能（その4）

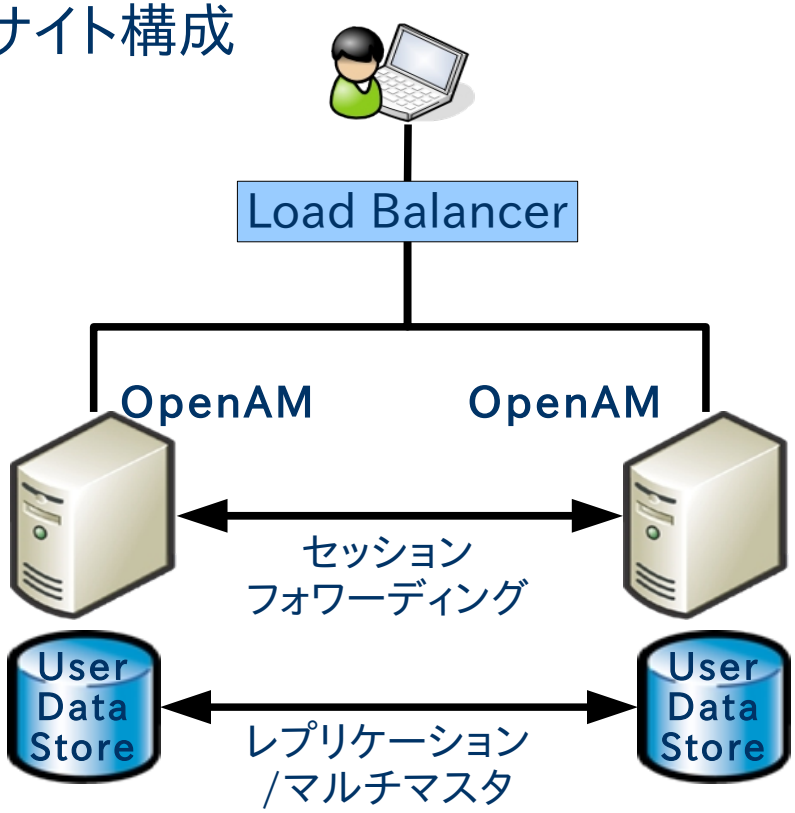
冗長化

OpenAMの機能 - 冗長化

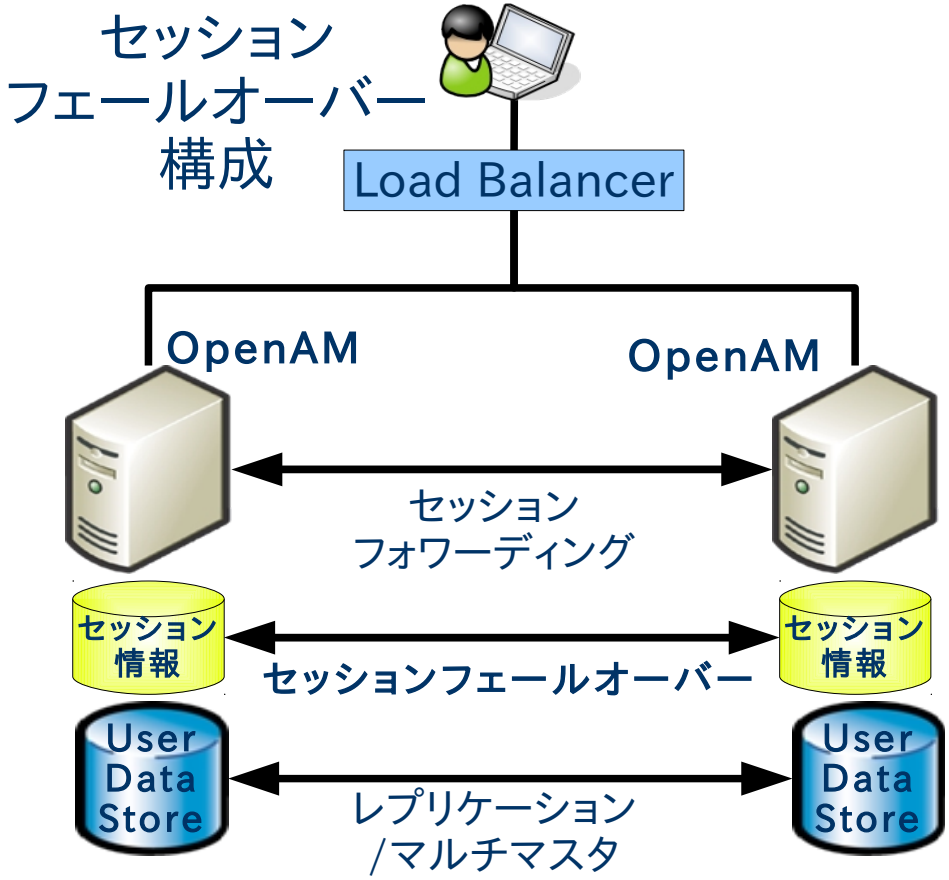
シングルサーバ構成



サイト構成



セッション フェールオーバー 構成



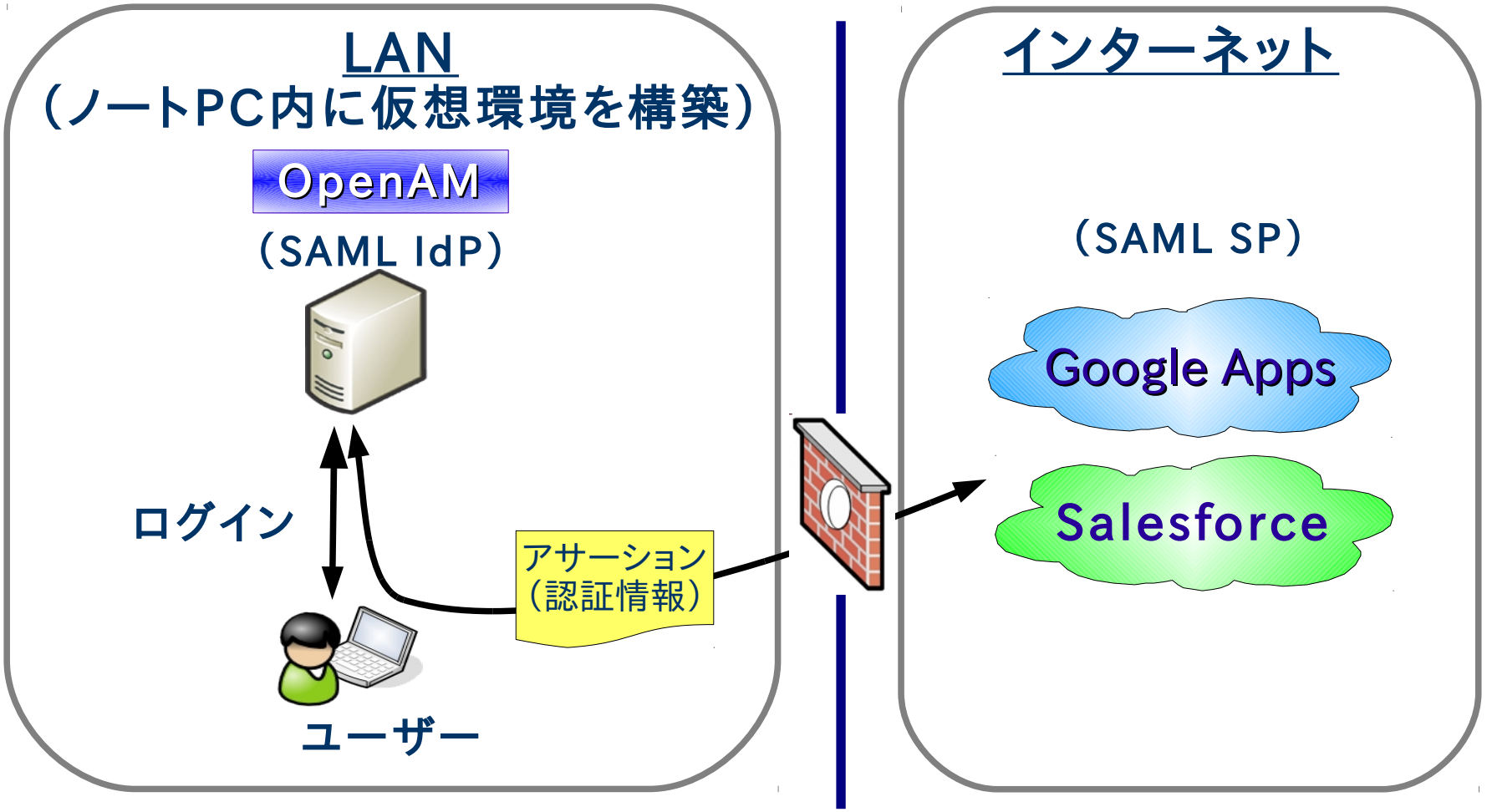
OpenAM（OpenSSO）の導入事例

事例紹介

- 九州工業大学様
  - OpenSSO + OpenLDAP を使ったシングルサインオンシステムを構築
  - シングルサインオン方式
    - SAML
    - リバースプロキシ
- その他

OpenAMデモ

OpenAM デモ環境



※Google Apps の SAML は HTTP Redirect Binding/HTTP POST Binding を採用しています。

OpenAM デモ内容

- (1)SAMLによるシングルサインオン
  - Google Apps と Salesforce にシングルサインオンでアクセスする
- (2)認証連鎖
  - ワンタイムパスワード認証を追加して二要素認証を行なう

まとめ

- OpenAM（OpenSSO）はシングルサインオンを実現するための基盤となるソフトウェアです
- ユーザーの Web アプリへのアクセス時の利便性の向上・セキュリティの強化に役立ちます
- OpenAMは長い期間をかけて着実に進化してきました。今後も開発は継続し、最新の機能が取り込まれていきます（クラウド対応など）

ご清聴ありがとうございました