学認ShibbolethとOpenAMを連携させて学外と学内をシングルサインオン

OSSTech

オープンソース・ソリューション・テクノロジ株式会社

お問い合わせ info@osstech.co.jp

目次

- 会社紹介
- OpenAM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
- 学術認証フェデレーション（学認）：GakuNinとは？
  - 学認（Shibboleth）の特徴
- OpenAMとShibbolethとの連携

会社紹介

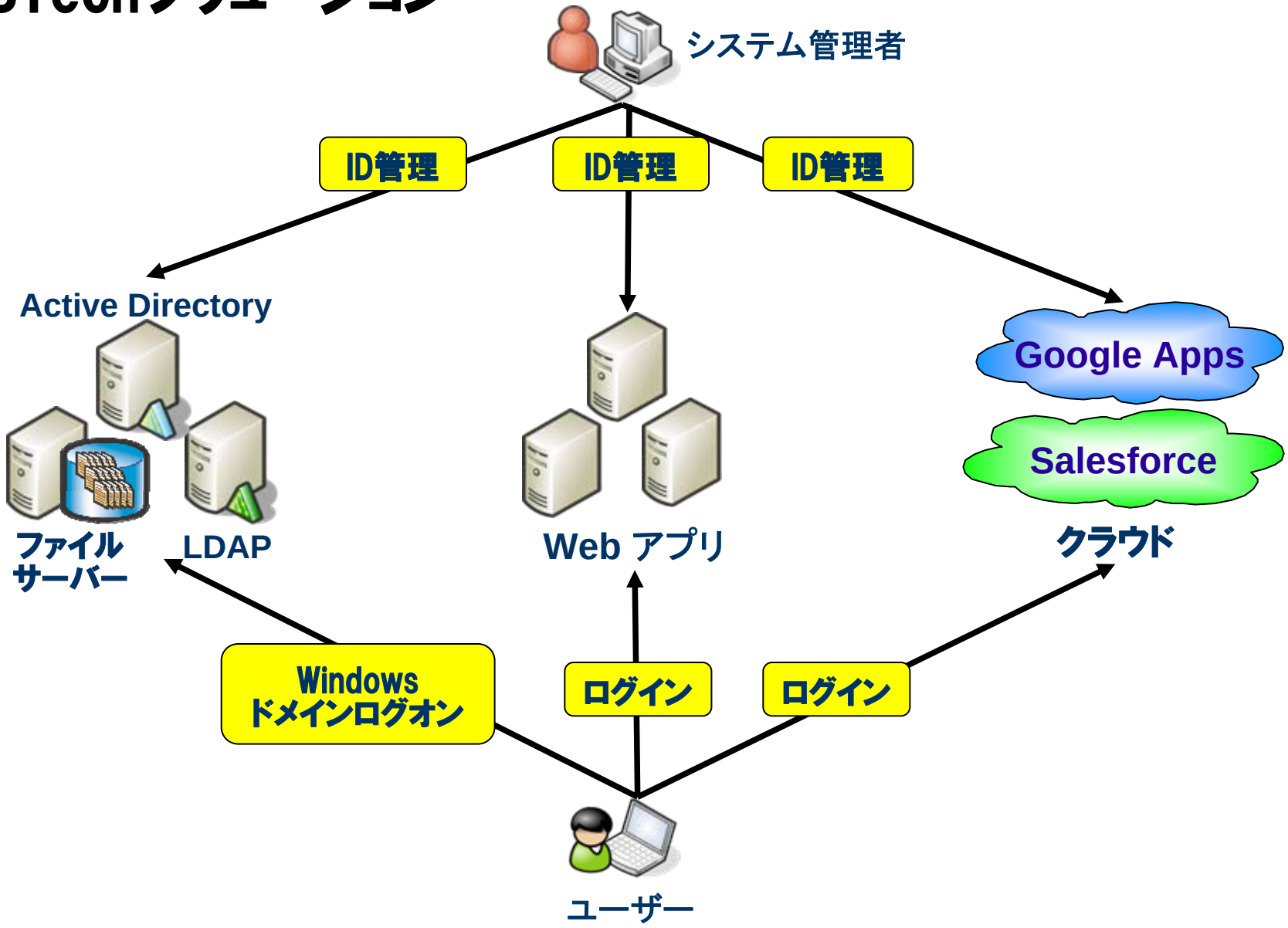
OSSTech会社紹介

- **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、Windows/Solaris/AIXへも対応
  - Windows/UNIX から Linux への移行も支援！

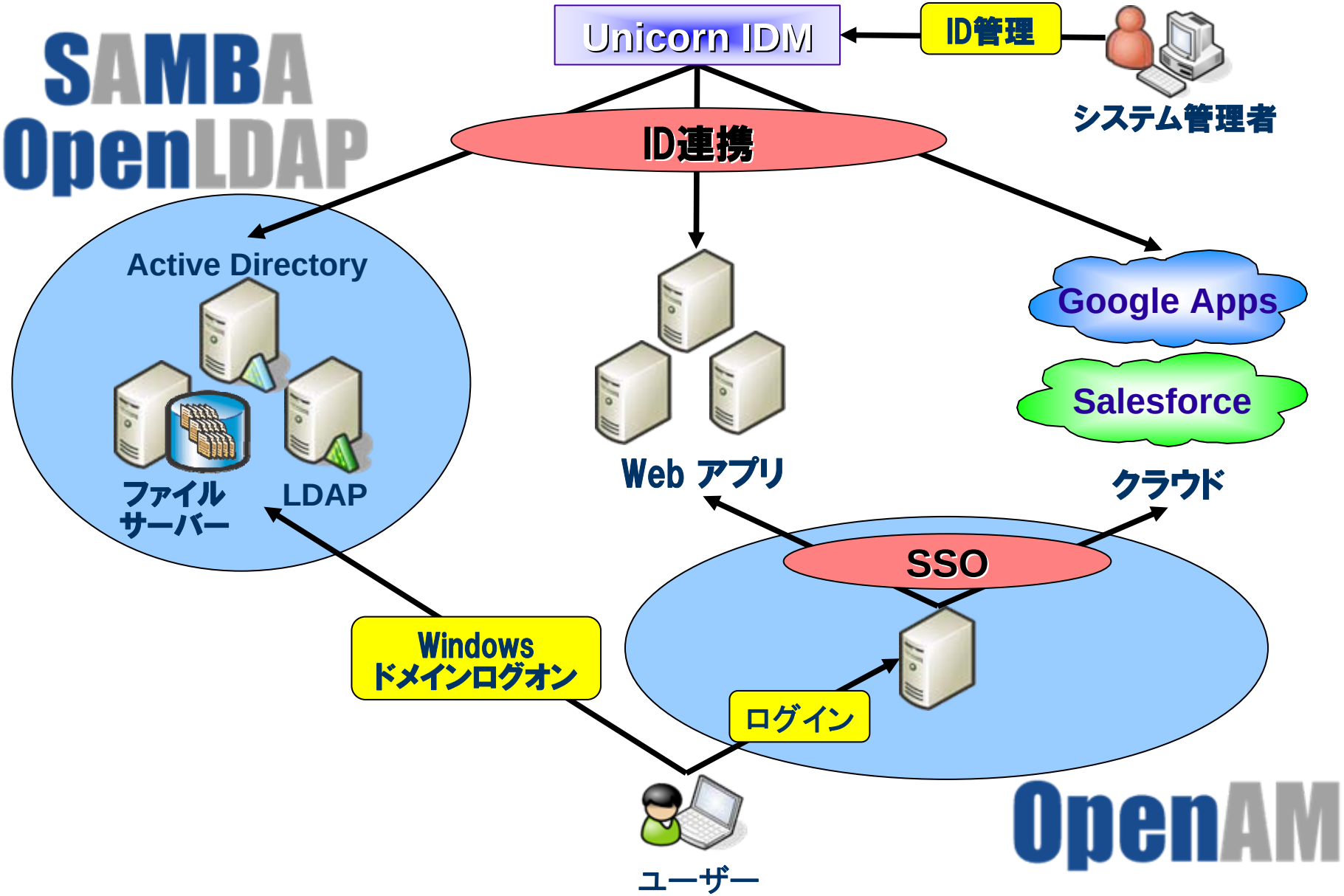
- **OSSを利用した認証基盤構築**が得意分野
  - LDAP認証、Windowsドメイン認証、Webアプリケーション認証、**クラウド認証**

- **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ソリューション



OSSTechの製品群とソリューション



OpenAM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

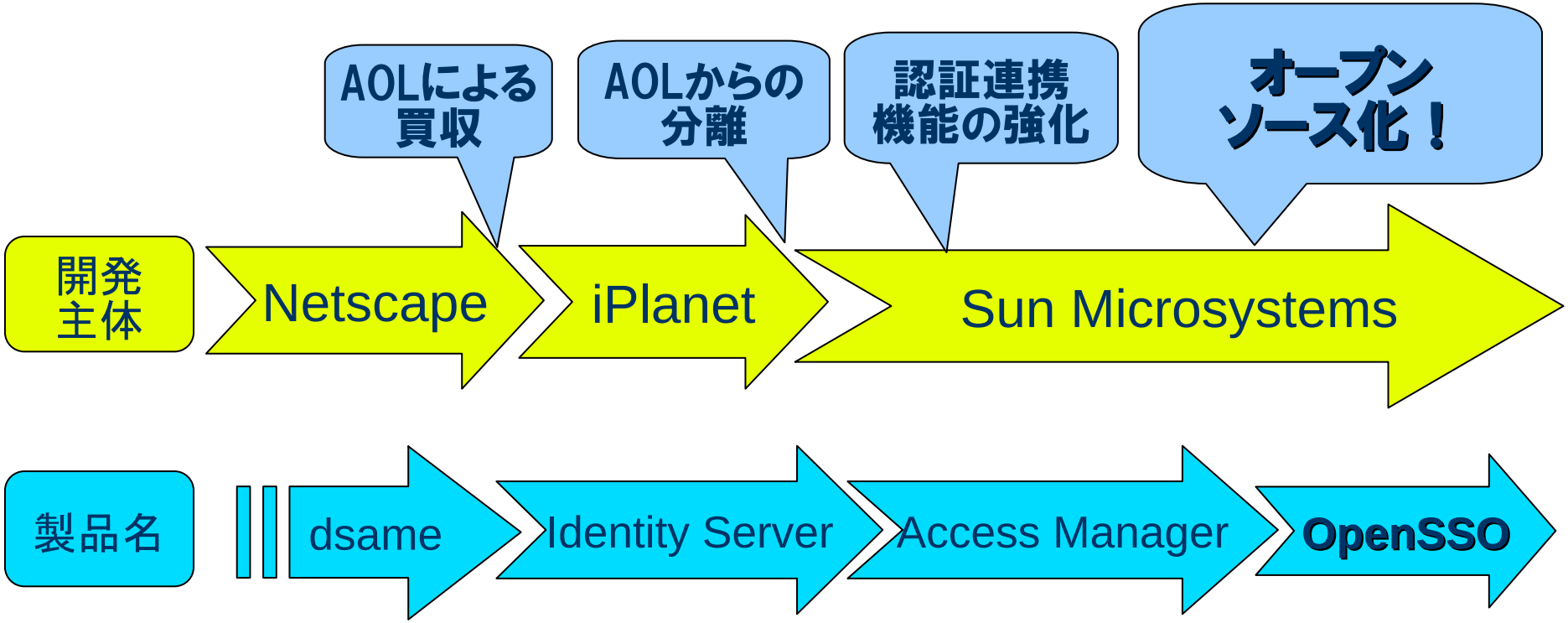
- ユーザー情報を格納するためのユーザーリポジトリ(ユーザーデータストア)として様々な LDAP サーバー、RDBに対応
  - RDBへの対応は OpenAM からサポート開始

- 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

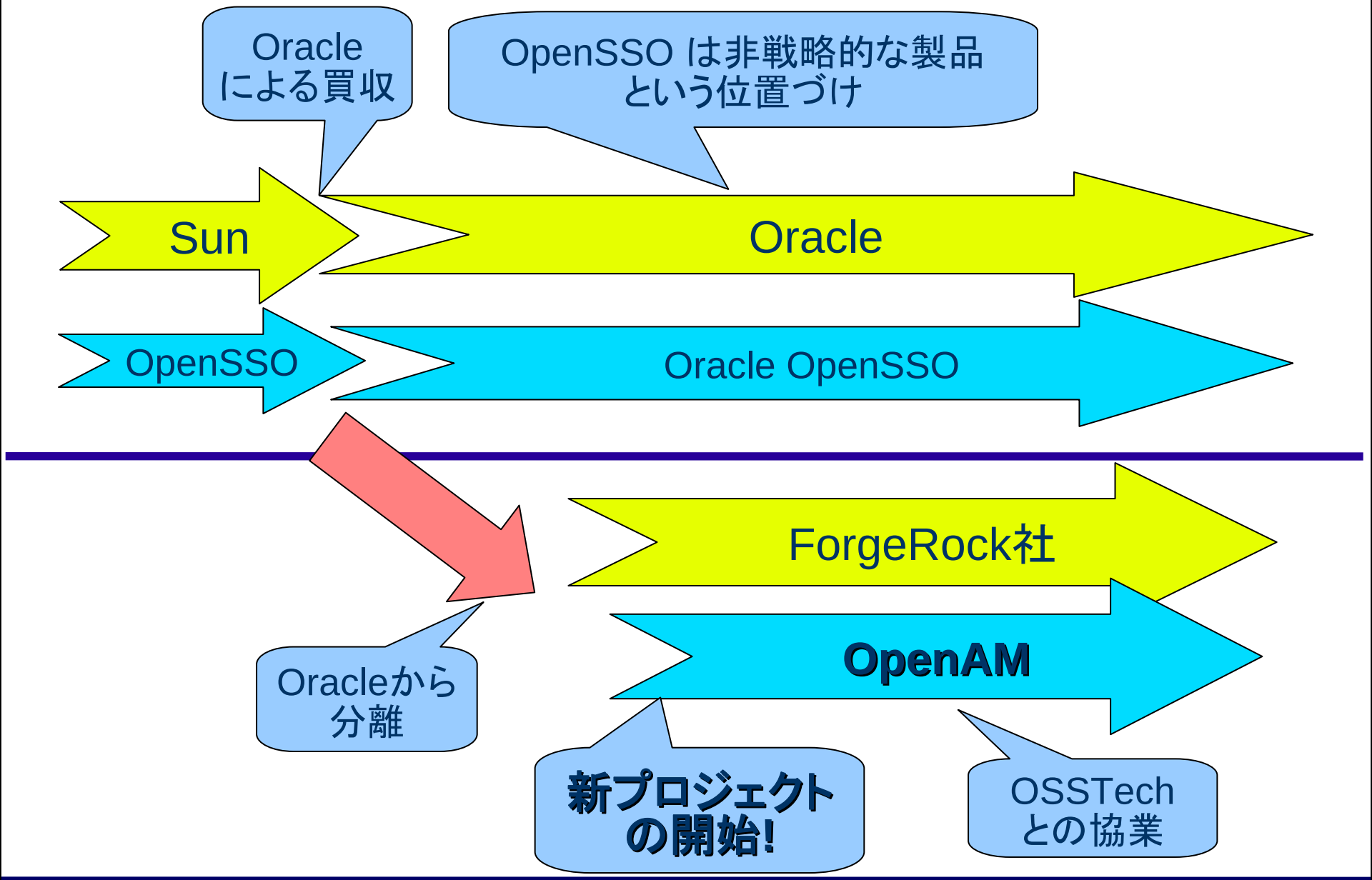
※用語解説

- SSO：Single Sign On
  - 一度（IdPで）認証されたら、すべての（認証なしで）アプリ（SP）が利用可能とする技術
  - 認証はIdPで行い、認可はSPでやるのが一般的
- IdP：Identity Provider
  - 認証プロバイダー：認証サーバー
  - 通常IDとパスワードを入れて認証してもらう
  - ワンタイムパスワードや生体認証、ICカードで認証も可能
- SP：Service Provider
  - ユーザへサービスを提供するアプリケーション
  - この資料の中ではWebアプリを指す
  - 上記IdPで認証されたユーザは、すべてのSPでSSO可能となる
  - ユーザ情報を元に認可を行うのはSPの一般的な役割だが、OpenAMではエージェントを使うことでSPの代わりに認可を行わせることが可能
- SAML：Secure Assertion Markup Lauguage
  - 認証情報をXMLでやりとりするための取り決め
  - IDとパスワードはネットワーク上を流れない
- DS：Discovery Service
  - 1つのSPに対し、複数のIdPが存在する場合、IdPをユーザーに選択（発見）させるためのサービス

OpenAMの歴史 - その1



OpenAMの歴史 – その2

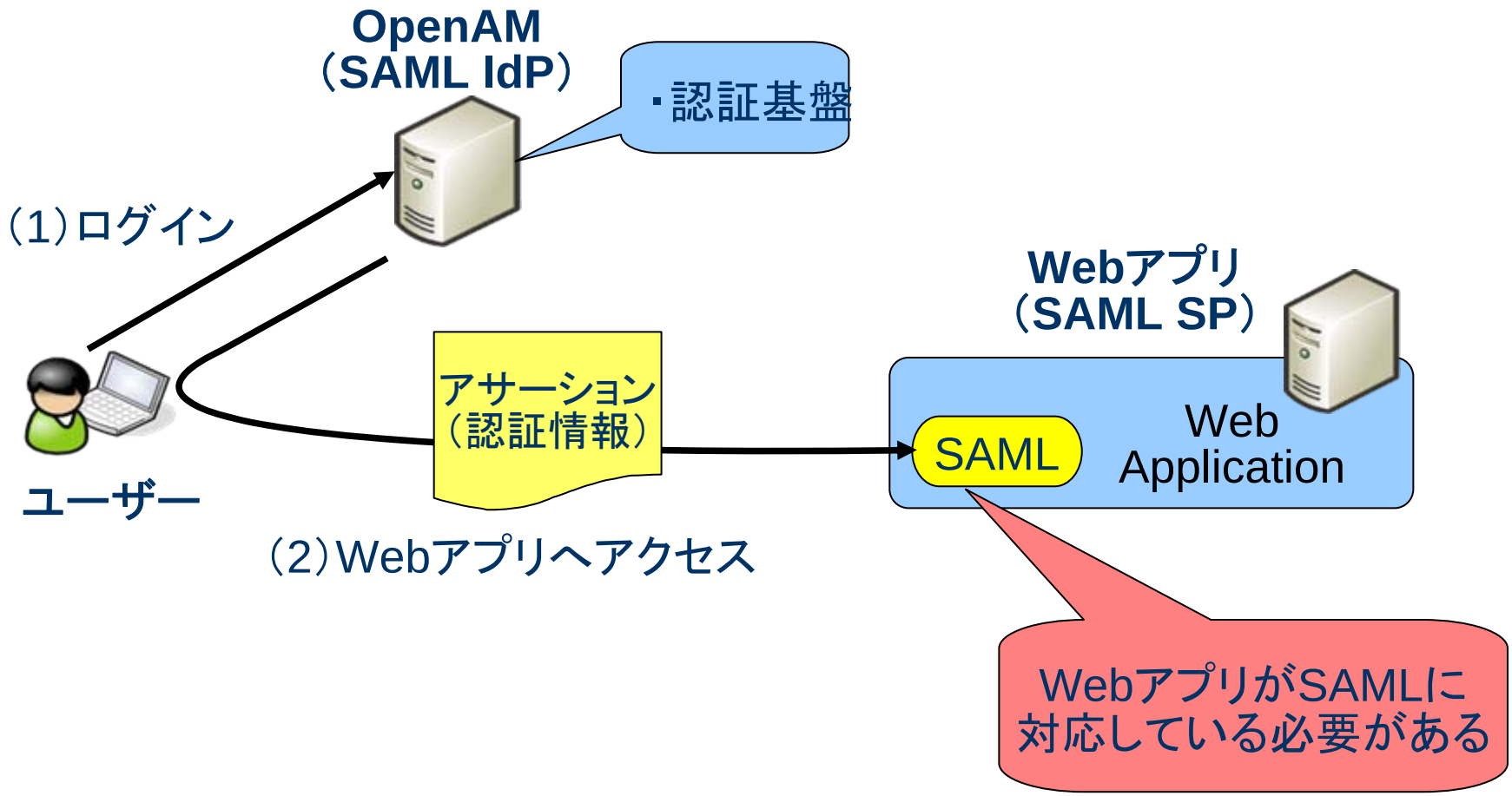


OpenAMの機能(その１)

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）

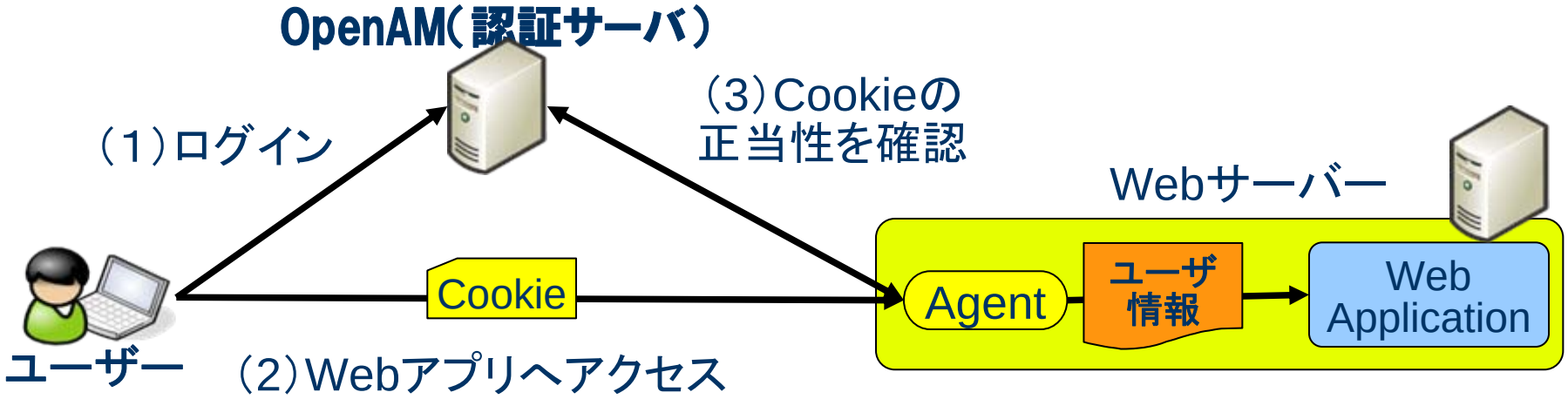
SAML



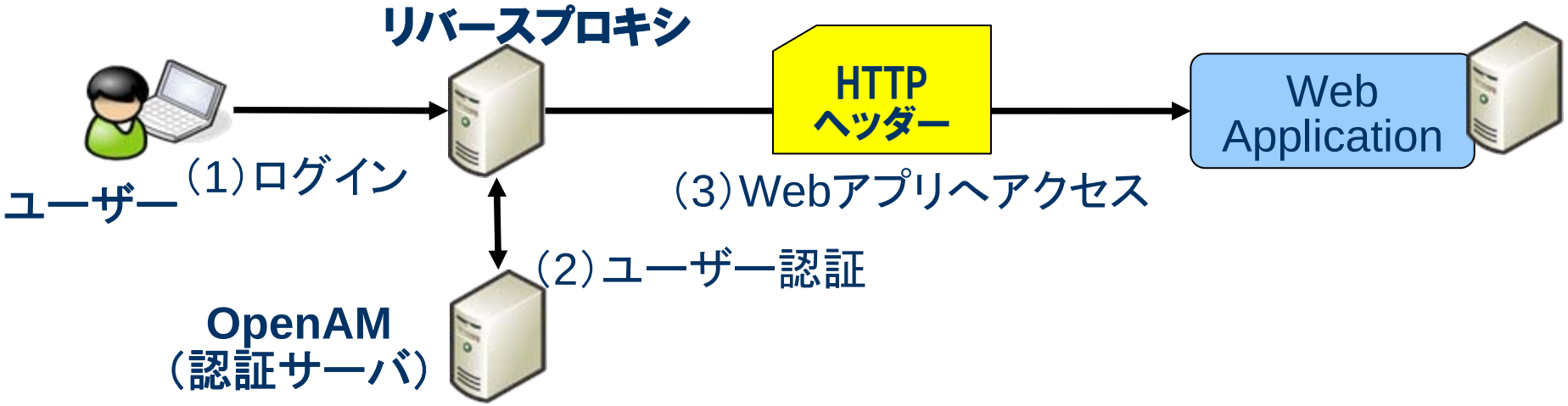
※この図は、HTTP Redirect Binding/HTTP POST Binding の場合の例

シングルサインオンの方式(２)

エージェント方式

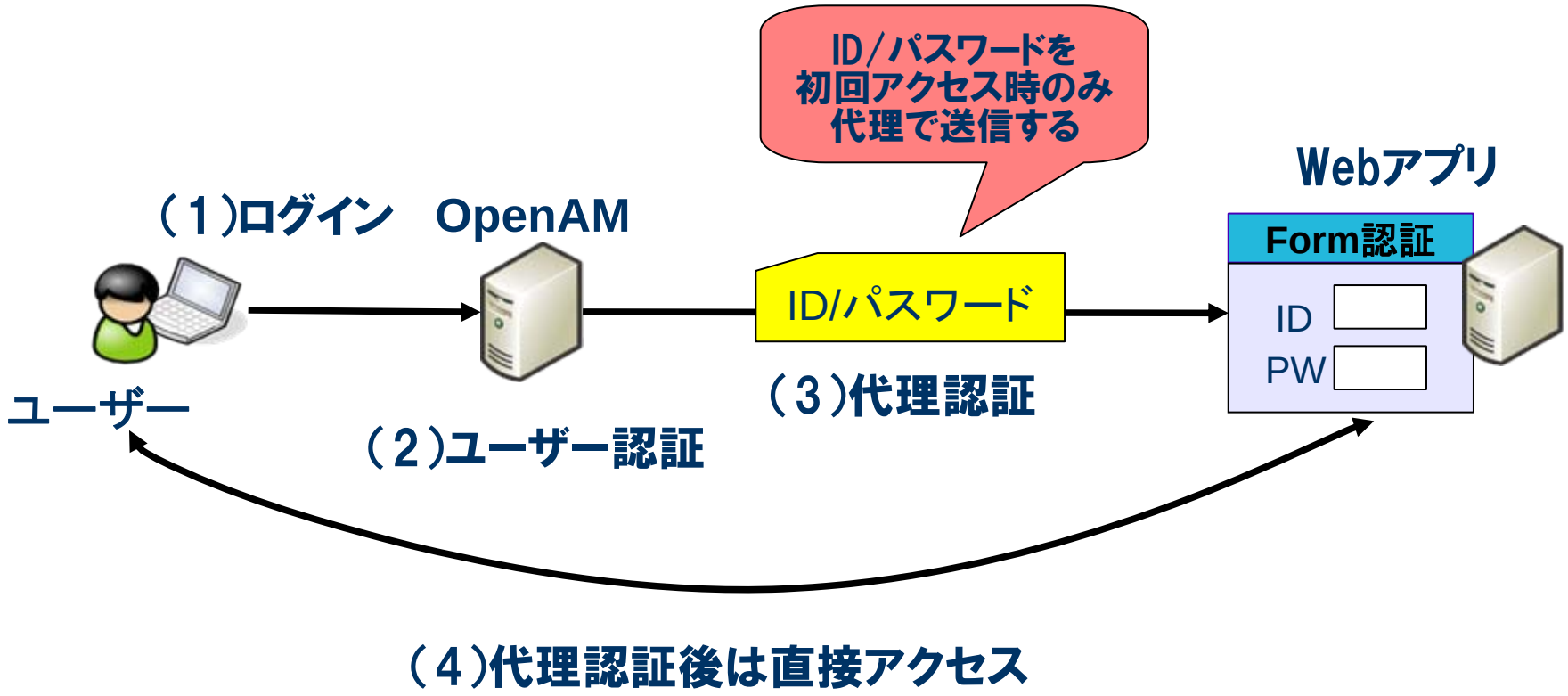


リバースプロキシ方式



シングルサインオンの方式(3)

代理認証方式



※リバースプロキシー方式で代理認証する方法もある
上記は代理認証用ポータルを用意する方法

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
  - Secure Assertion Markup Lauguage
  - 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

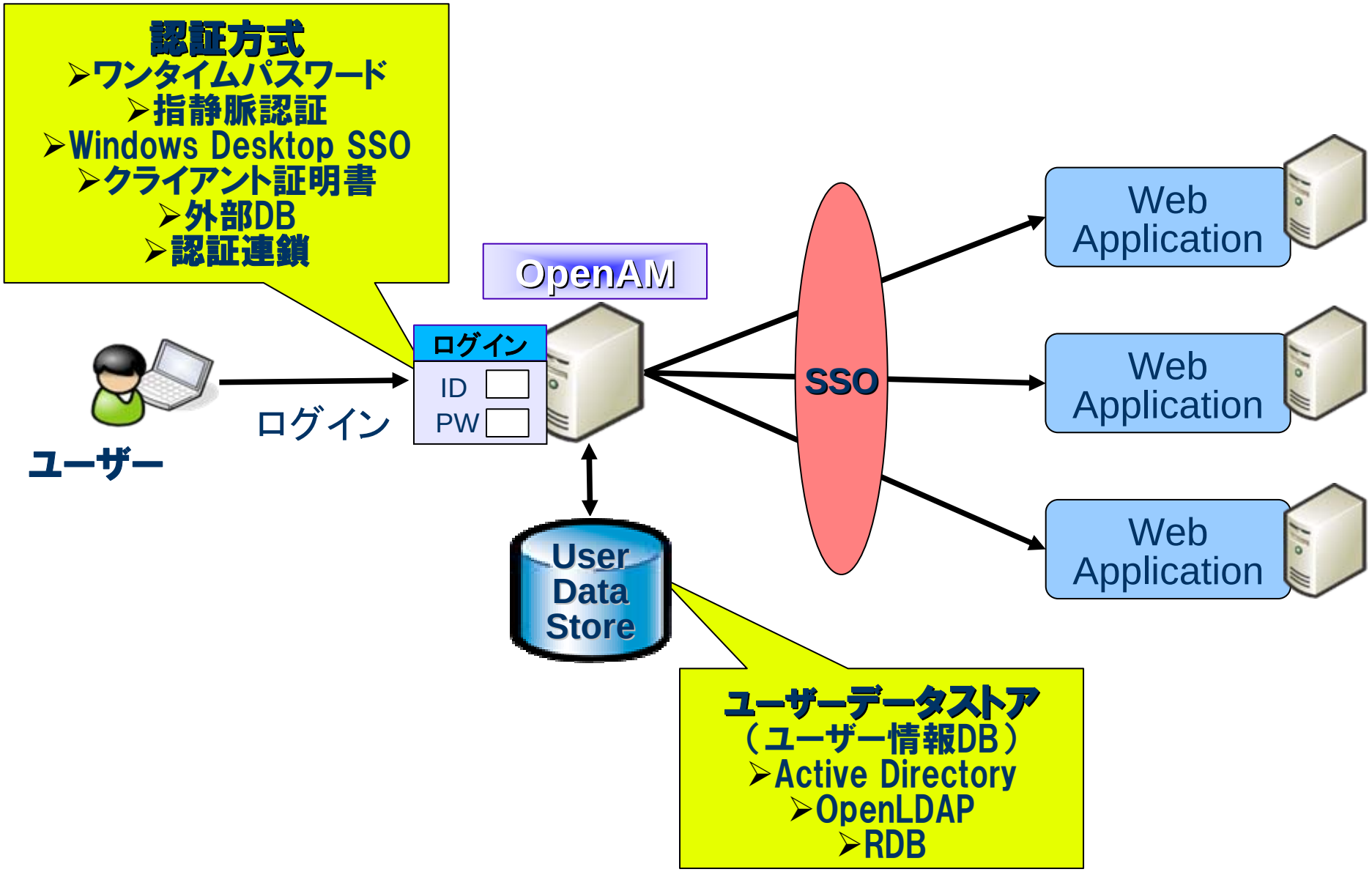
- リバースプロキシ方式
  - リバースプロキシを使用してアクセス制御を行う
  - ユーザーデータの受け渡しはHTTPヘッダーを利用
  - SSO対象Webアプリのバージョンや設定変更の影響が少ない
  - リバースプロキシが性能上のボトルネックになる可能性がある

- 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(更新できない参照のみのものでも可能)
  - 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**

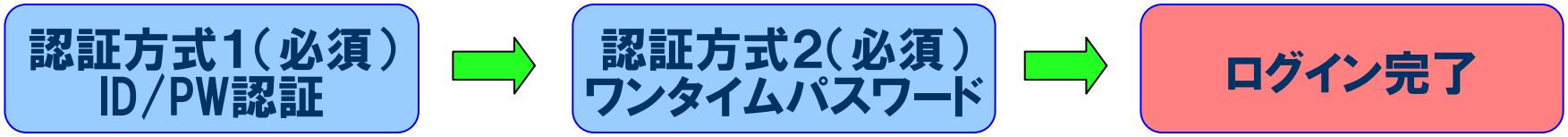
OpenAMの機能 - ユーザー情報DB

- 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(更新権限が必須)
    - 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

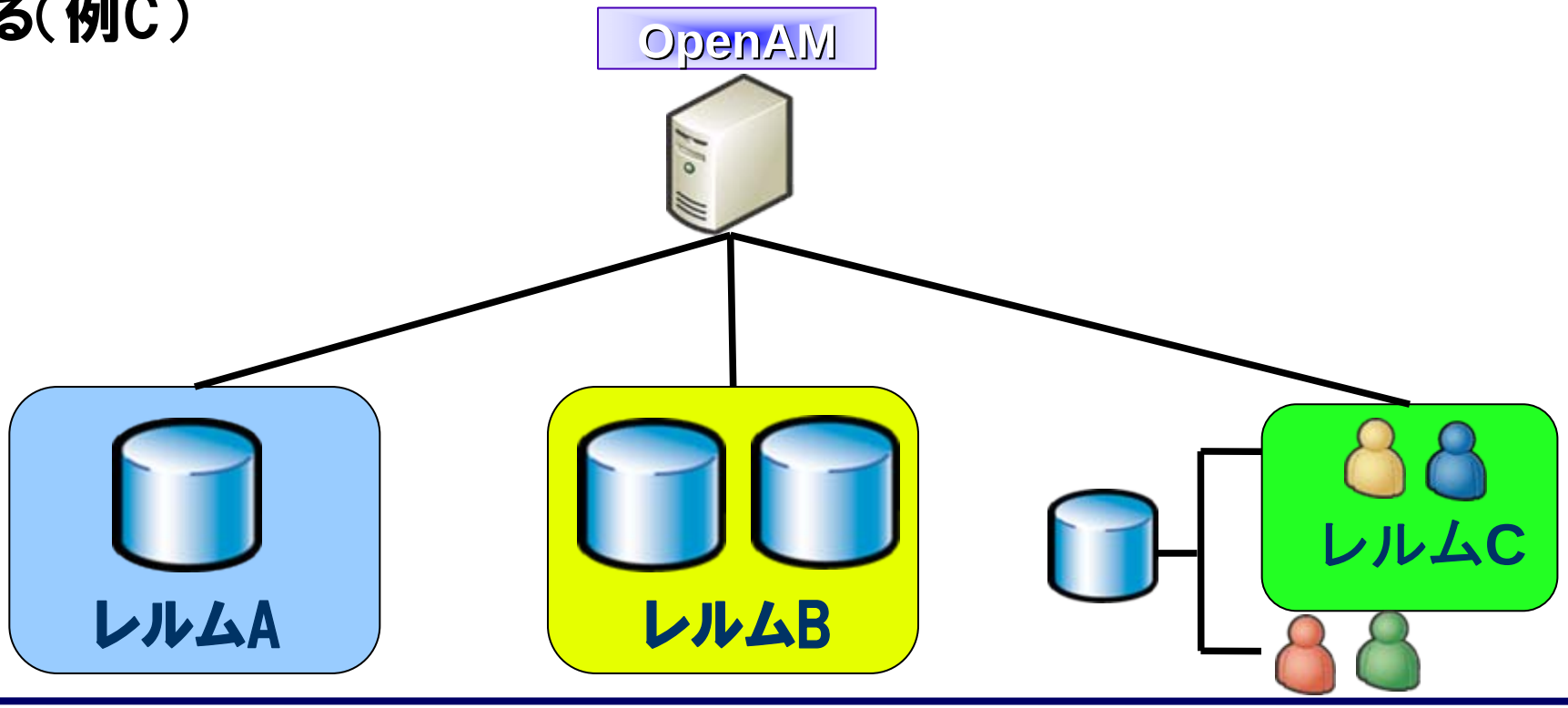
- 以下の設定をレルム単位で管理
  - ユーザーデータストア(LDAPベースDN、検索フィルタなども指定可能)
  - アクセス制御ポリシー
  - 認証方式

- 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)

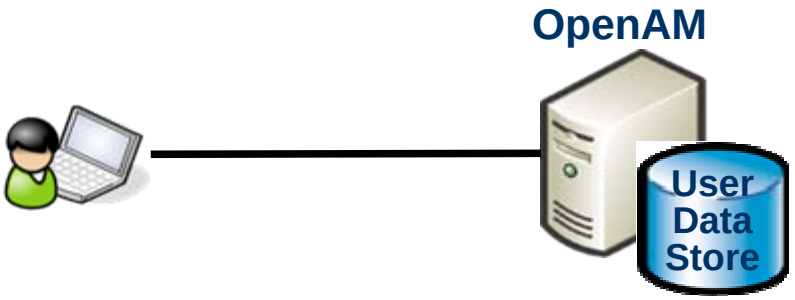


OpenAMの機能（その4）

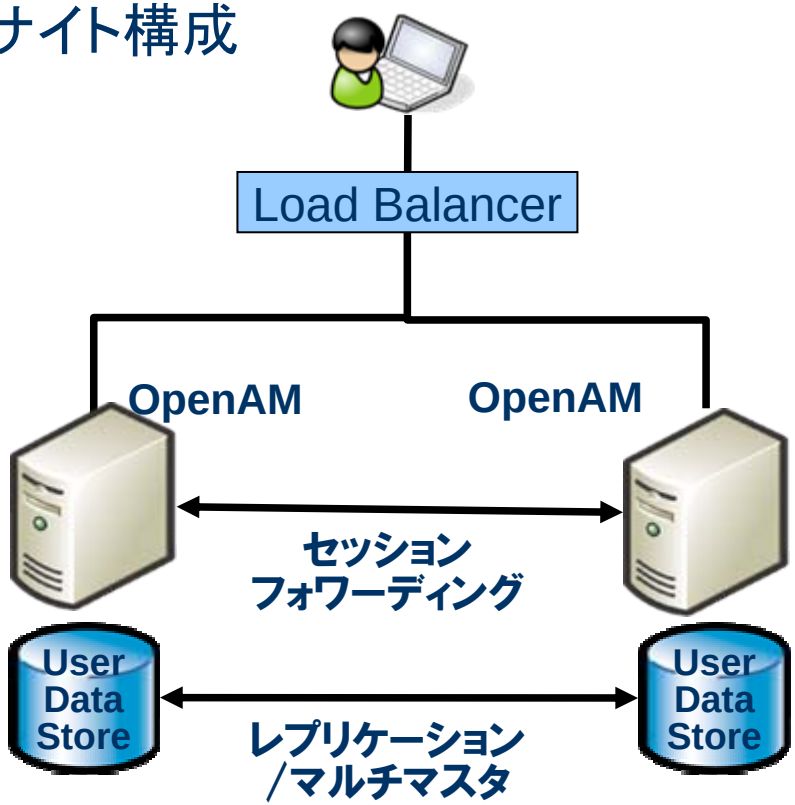
冗長化

OpenAMの機能 - 冗長化

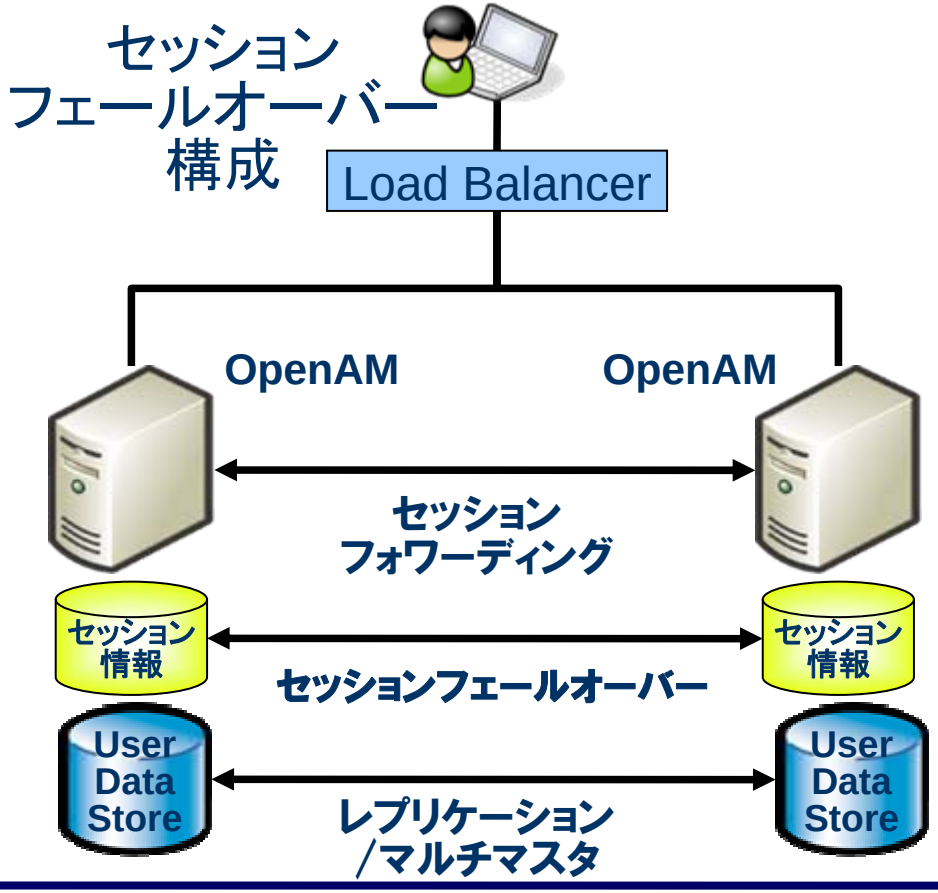
シングルサーバ構成



サイト構成



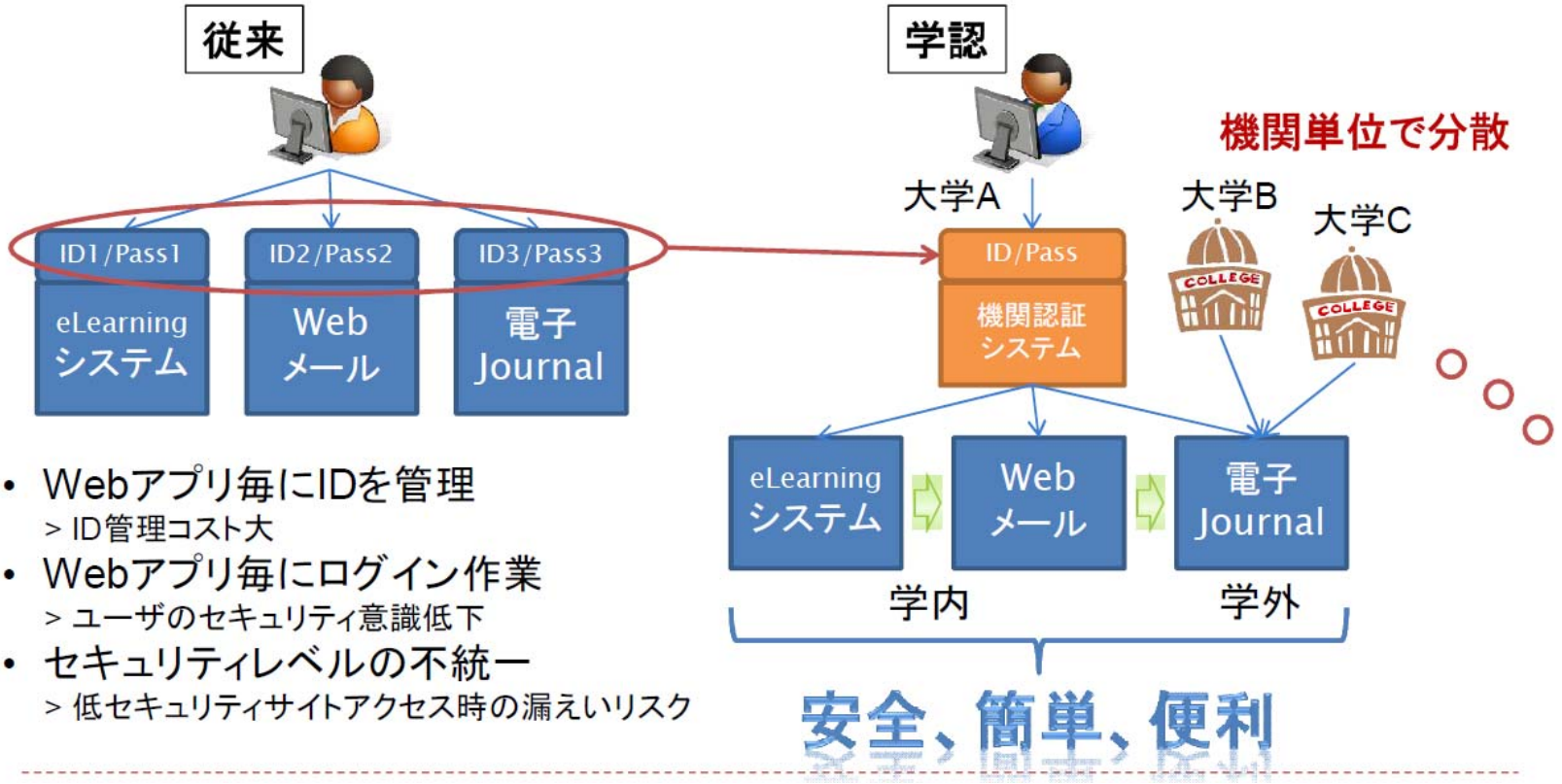
セッション フェールオーバー 構成



学術認証フェデレーション
学認：GakuNinとは？

学術認証フェデレーション「学認」とは

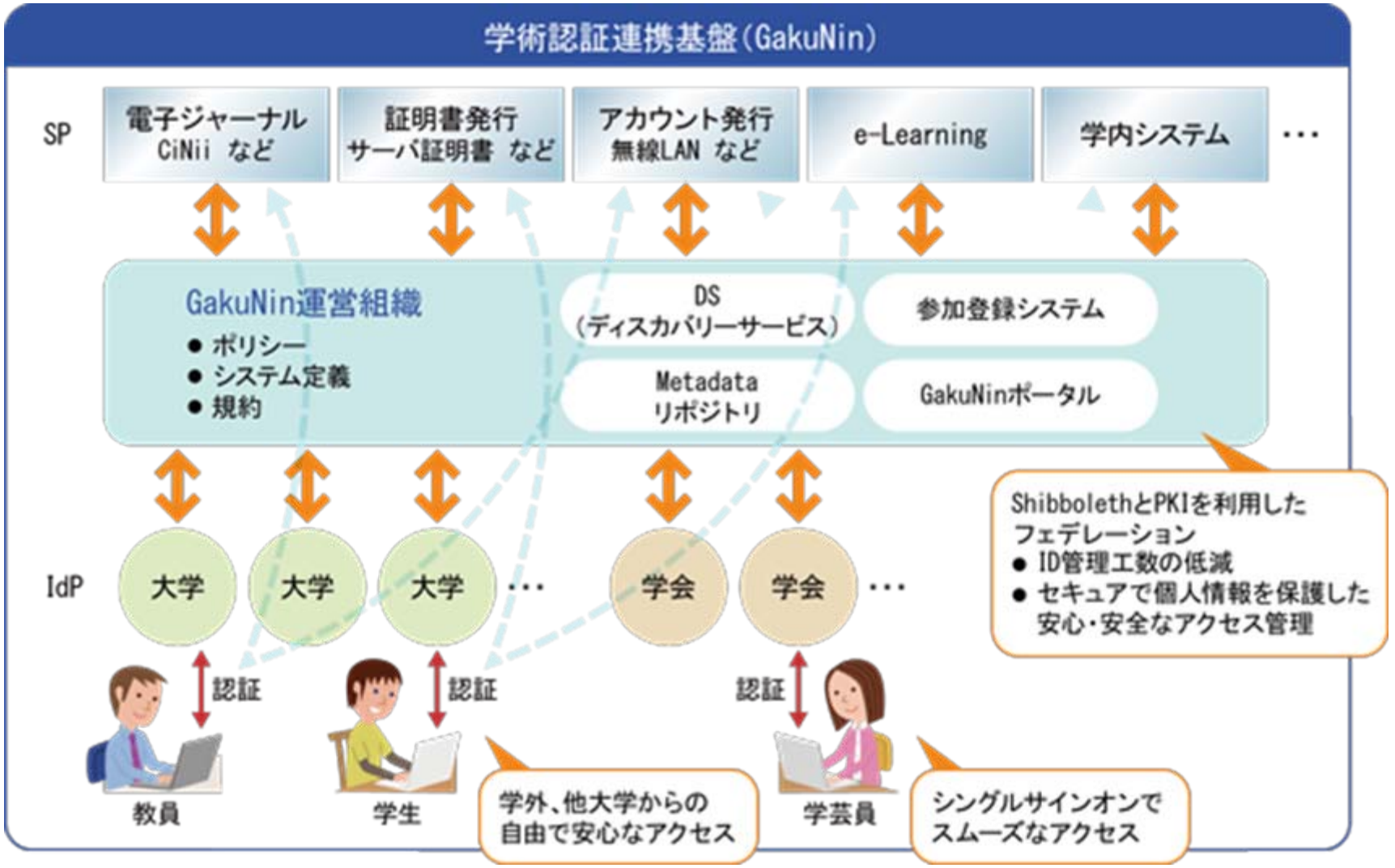
- Webアプリケーションへのシングル・サイン・オン（SSO）技術を、組織を越えて活用する分散型認証基盤



- Webアプリ毎にIDを管理
  > ID管理コスト大
- Webアプリ毎にログイン作業
  > ユーザのセキュリティ意識低下
- セキュリティレベルの不統一
  > 低セキュリティサイトアクセス時の漏えいリスク

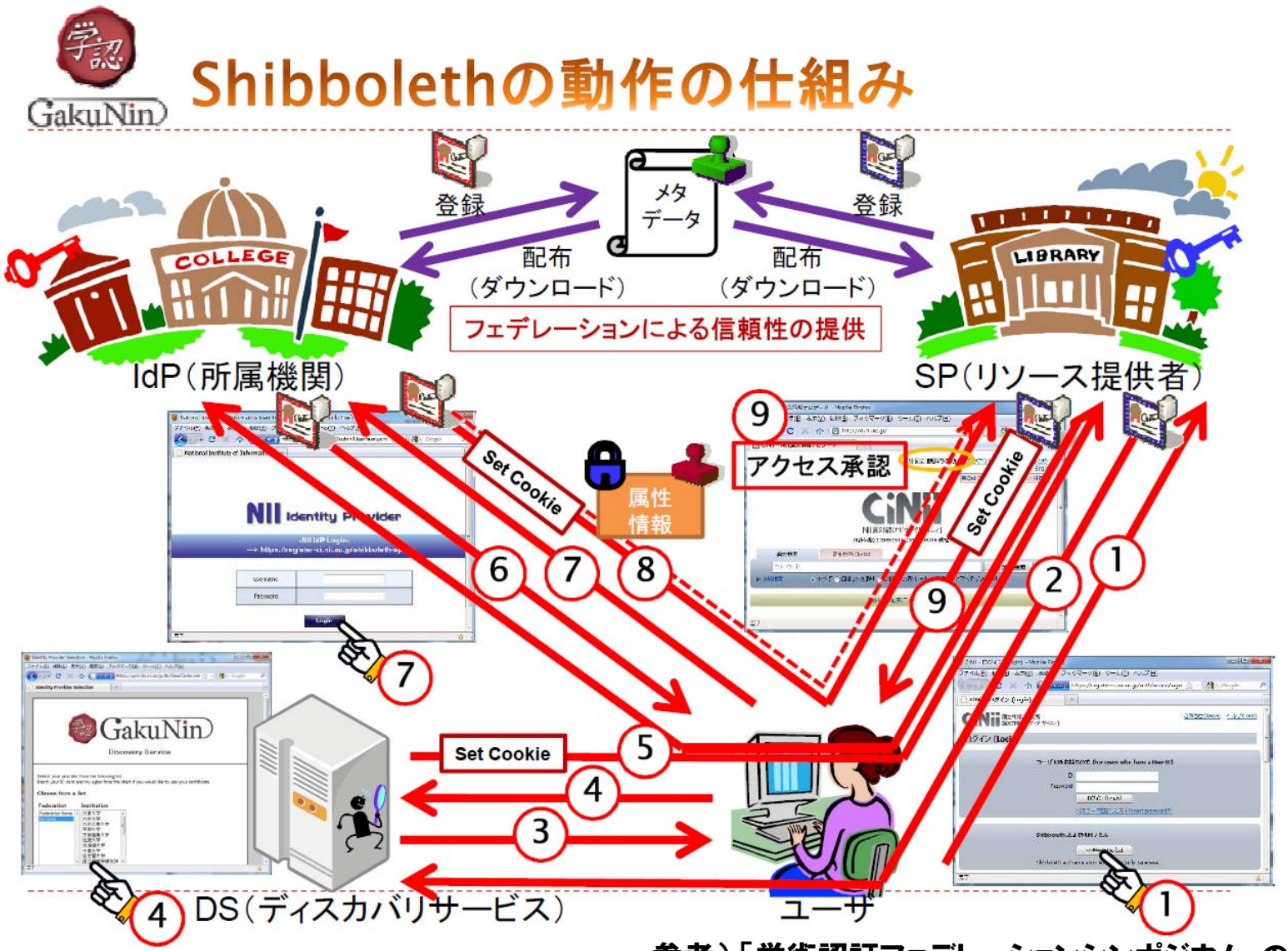
参考）「学術認証フェデレーションシンポジウム」の資料より
https://www.gakunin.jp/docs/open/3

学認の構成



参考）学術認証フェデレーションの資料より
https://www.gakunin.jp/

学認の動作の仕組み



参考）「学術認証フェデレーションシンポジウム」の資料より
https://www.gakunin.jp/docs/open/3

学認(Shibboleth)の特徴

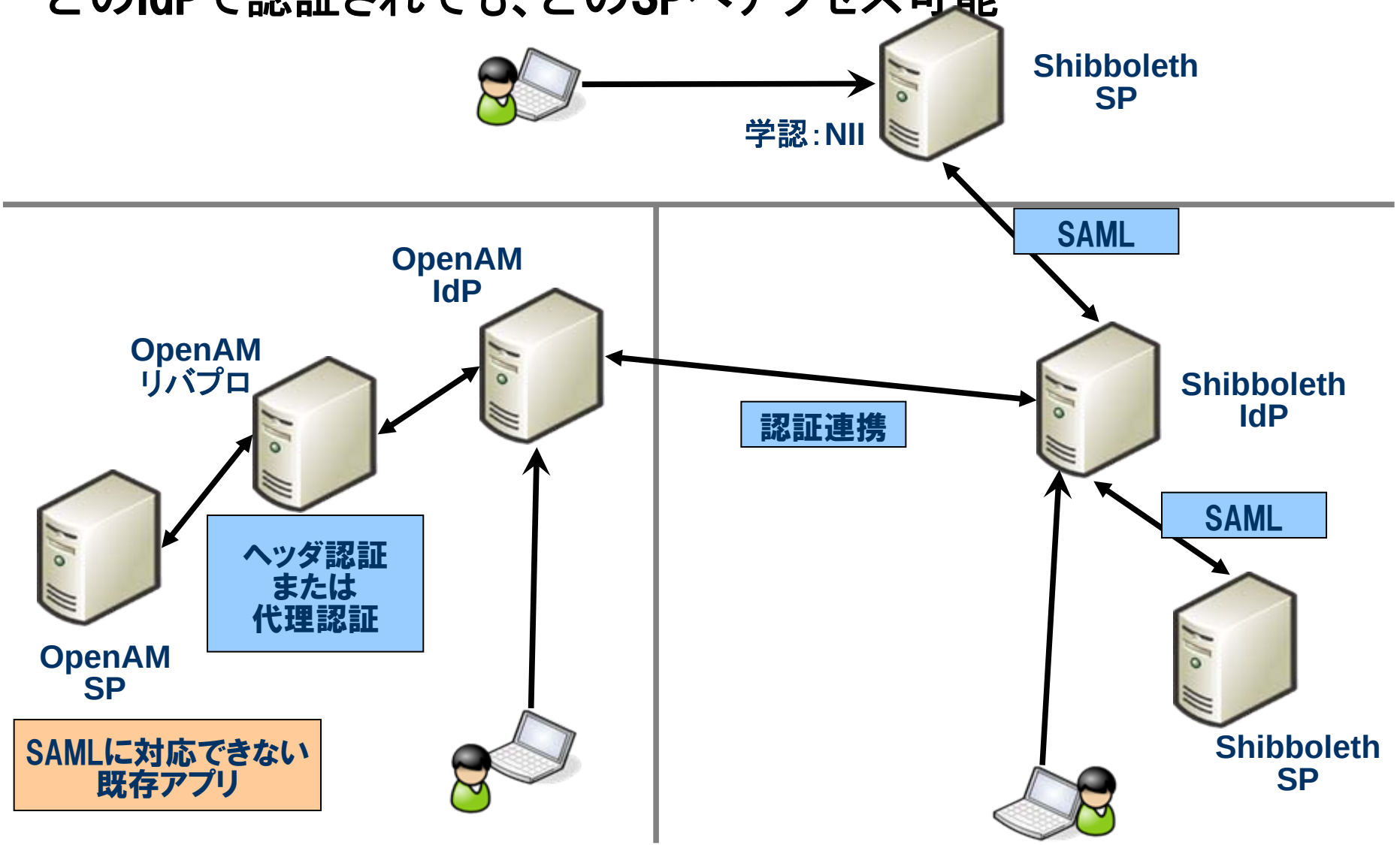
- SSO方式としてSAMLを標準
  - 代理認証やヘッダ認証などの方式には対応していない
- 多要素認証に対応していない
  - 学認では認証強度を伝える取り決めがない
- レルムといったマルチテナントの考え方がない
  - 職員、学生、卒業生といった属性で認証方式を切り替えられない
- ロードバランサーで負荷分散は可能だが、セッションルーティングやセッションフェイルオーバーの機能は持っていない
- SPのための専用Webサーバー(Apache)が必要
  - OpenAMはFedletを使ってアプリをSAML対応にできる
- 認可はSP側の役割でShibboleth IdPでは行えない
  - OpenAMではエージェント使って(SAMLや代理認証、ヘッダ認証のアプリでも)認可をOpenAMで集中管理可能
- GUIの管理ツールがない
  - OpenAMにはIdPとSP(エージェント)を集中管理できるWeb GUIが付属
- 1つのShibbolethをIdPとSPの両方同時に動かすのは容易ではない
  - OpenAMはIdPでありながらSPとしても動作させることが可能

OpenAMとShibbolethとの連携

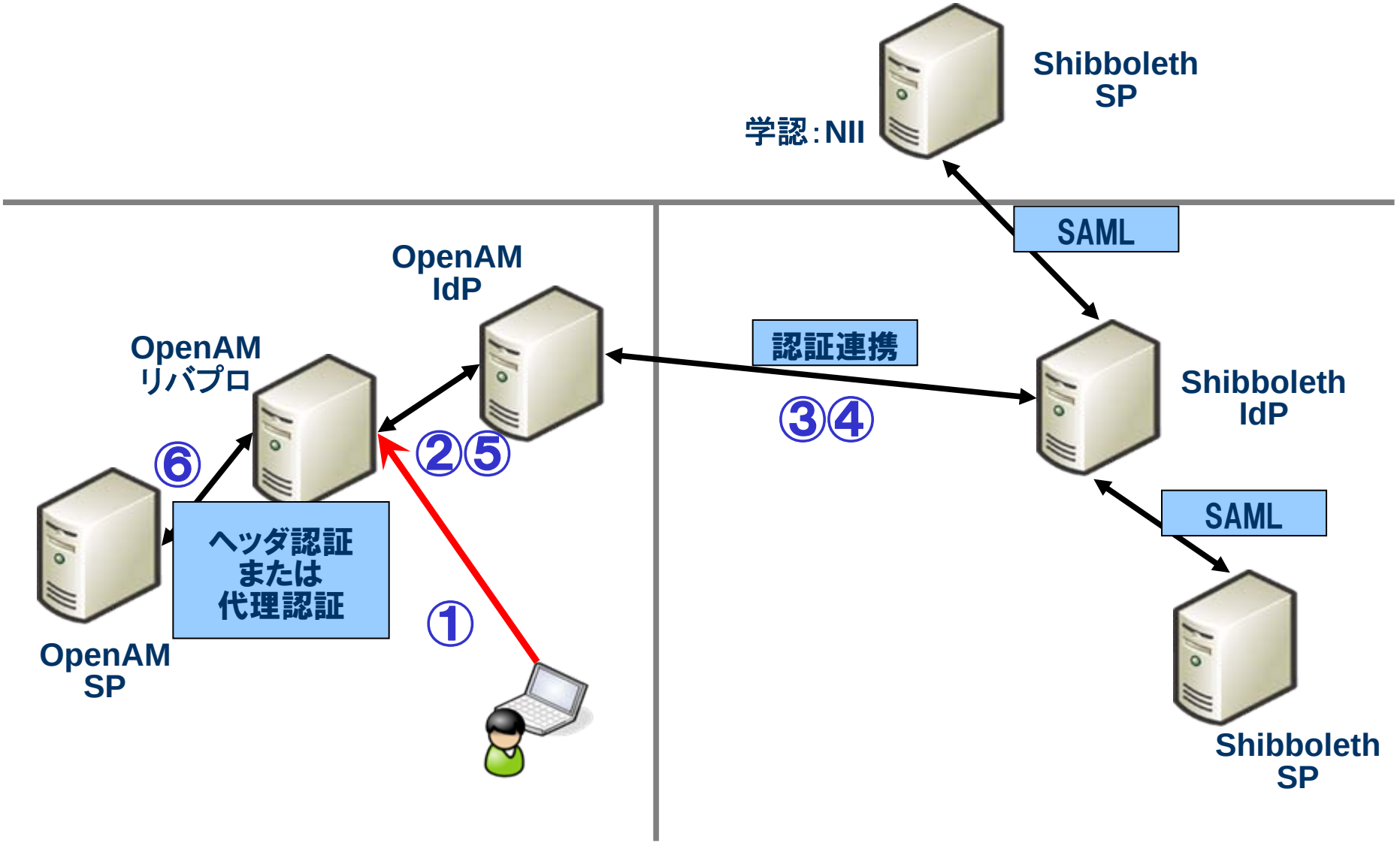
ShibbolethとOpenAMの連携

- ShibbolethはSAMLを使うので、Shibbolethの代わりにOpenAMを使うことは可能
  - 学認では、まずShibbolethありき、となっているが
- Shibbolethを入れてすべてのWebアプリをShibboleth SPとしてしまうのが理想だがSAML対応にするのは容易ではない
- OpenAMでは代理認証やヘッダ認証などの方式が利用でき、既存アプリの修正を最小限(修正なし)でSSO対応させることが可能
- OpenAMはIdPとしても(SAMLの)SPとしても振る舞うことが可能
- ShibbolethをIdPとしても(SAMLの)SPとしても振る舞わせるには難しい
- Shibbolethの足りない部分をOpenAMで補い、連携させることで柔軟で高機能なSSOシステムが可能となる

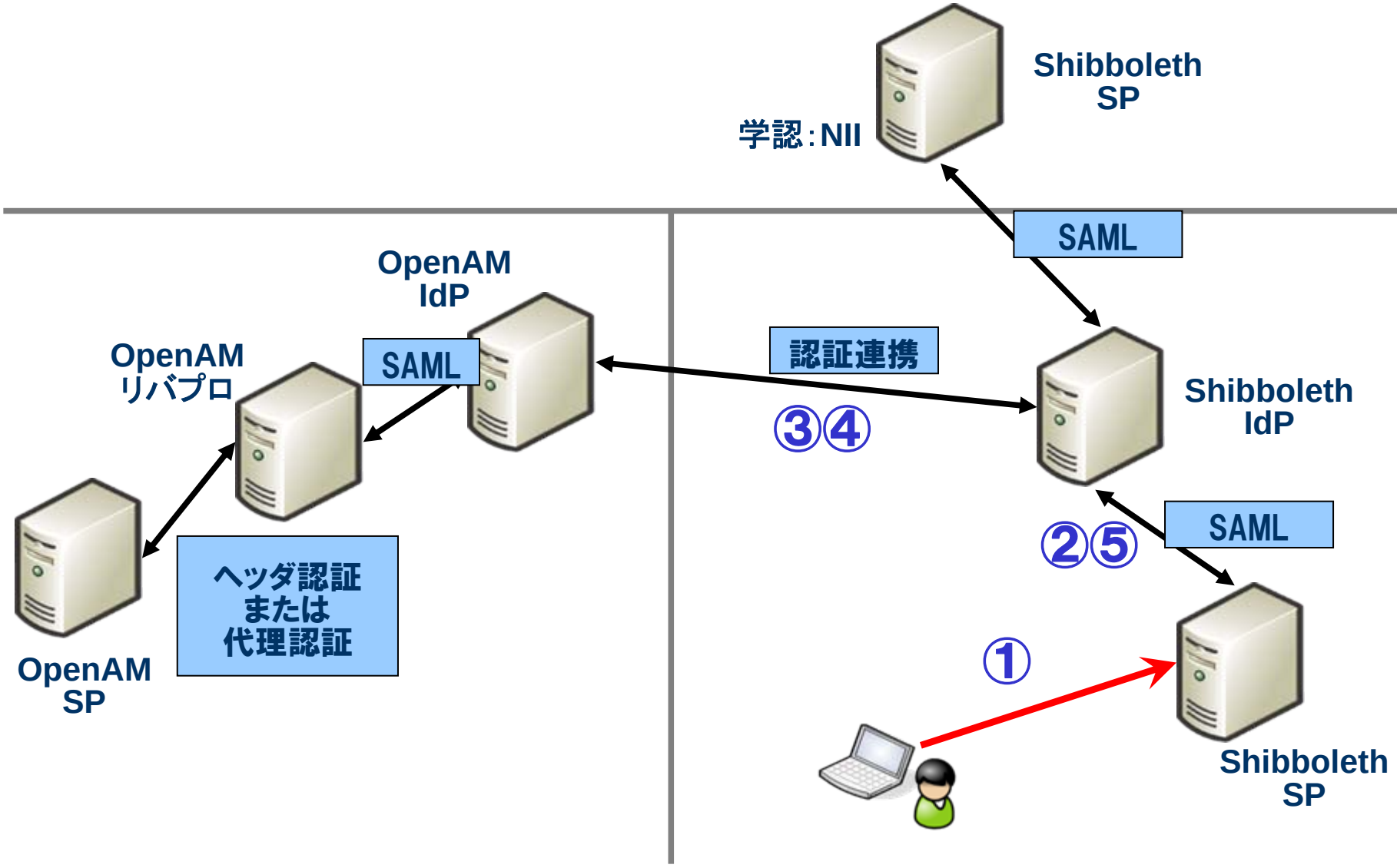
OpenAMとShibbolethとの連携
どのIdPで認証されても、どのSPへアクセス可能



OpenAMとShibbolethとの連携（1）
◎Shibbolethで認証されたユーザからOpenAMのSPへアクセス



OpenAMとShibbolethとの連携 (2)
◎ OpenAMで認証されたユーザからShibbolethのSPへアクセス



まとめ

- 今後、学認(Shibboleth)の導入は大学(教育機関)での導入は必須となっていく
- ShibbolethだけでSSO環境を構築するのは容易ではない
- OpenAMは商用製品なので、実績のある商用SSOソリューションが多数存在する
  - ICカード、ワンタイム、生体認証など
  - 代理認証やヘッダ認証など既存アプリの変更を最小限にしてSSO化が可能
- OpenAMとShibbolethを連携させることで既存環境と学認環境を平行運用しながら順次SSO対応化させていくことが可能