OpenAMを利用した学認(Shibboleth)への参加

OSSTech

2012年7月19日
プリンシパル・エンジニア 相本 智仁

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***

目次

- 会社紹介
- シングルサインオンとは
- OpenAMとは
- 学認とは
- OpenAMとShibbolethとの連携
- 事例紹介

会社紹介

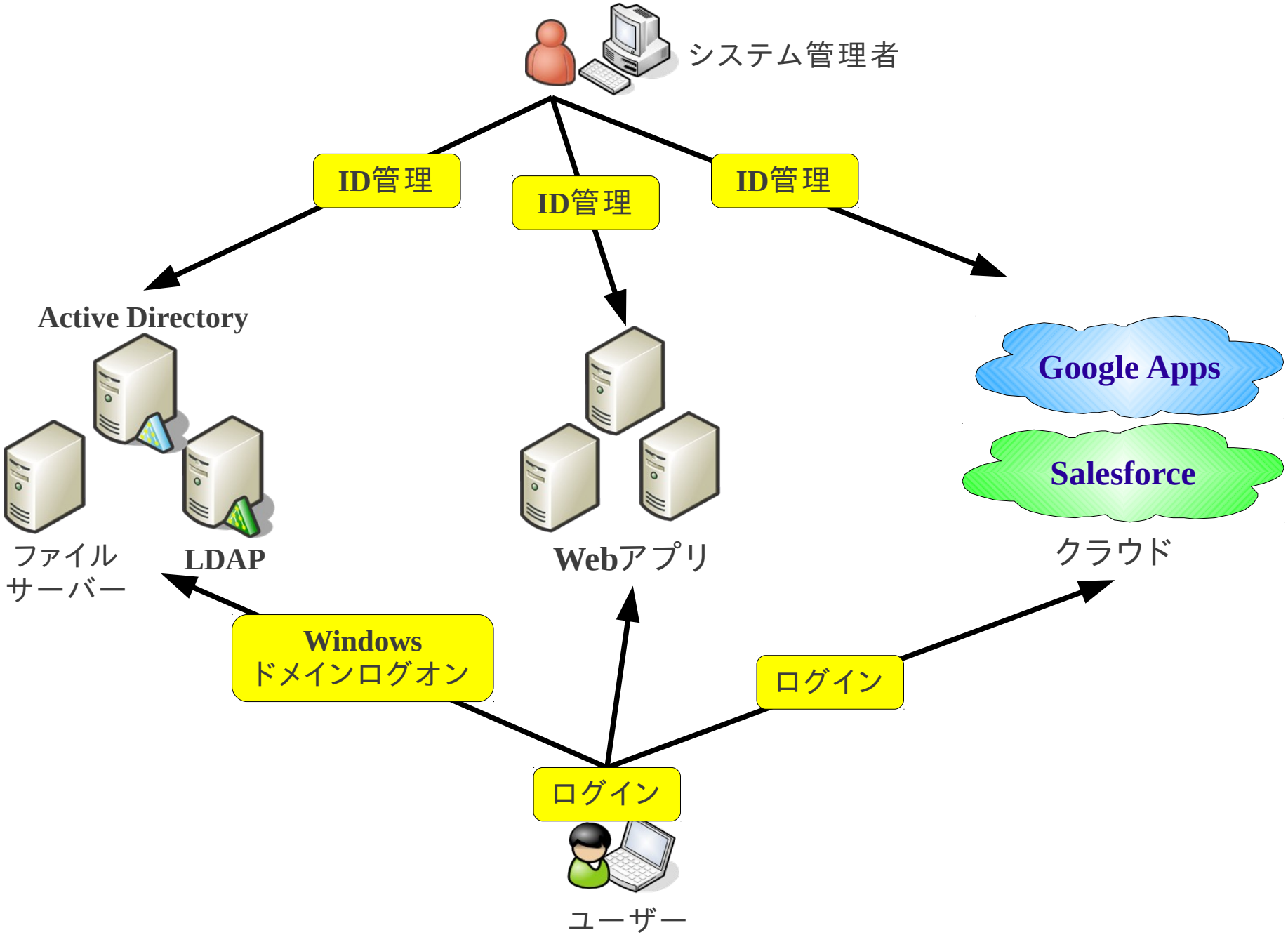
オープンソース・ソリューション・テクノロジ株式会社

- **OSに依存しないOSSのソリューション**を中心に提供
  - Linuxだけでなく、Windows/Solaris/AIXなどへも対応!
- **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
  - 製品パッケージ提供
  - 製品サポート提供
  - OSSの改良、バグ修正などコンサルティング提供
- **Windows Active Directory, CLUSTERPROなどの商用ソフトのソリューション,Sun Java Directory Server**も提供
  - 商用製品とOSSの柔軟な組み合わせに対応

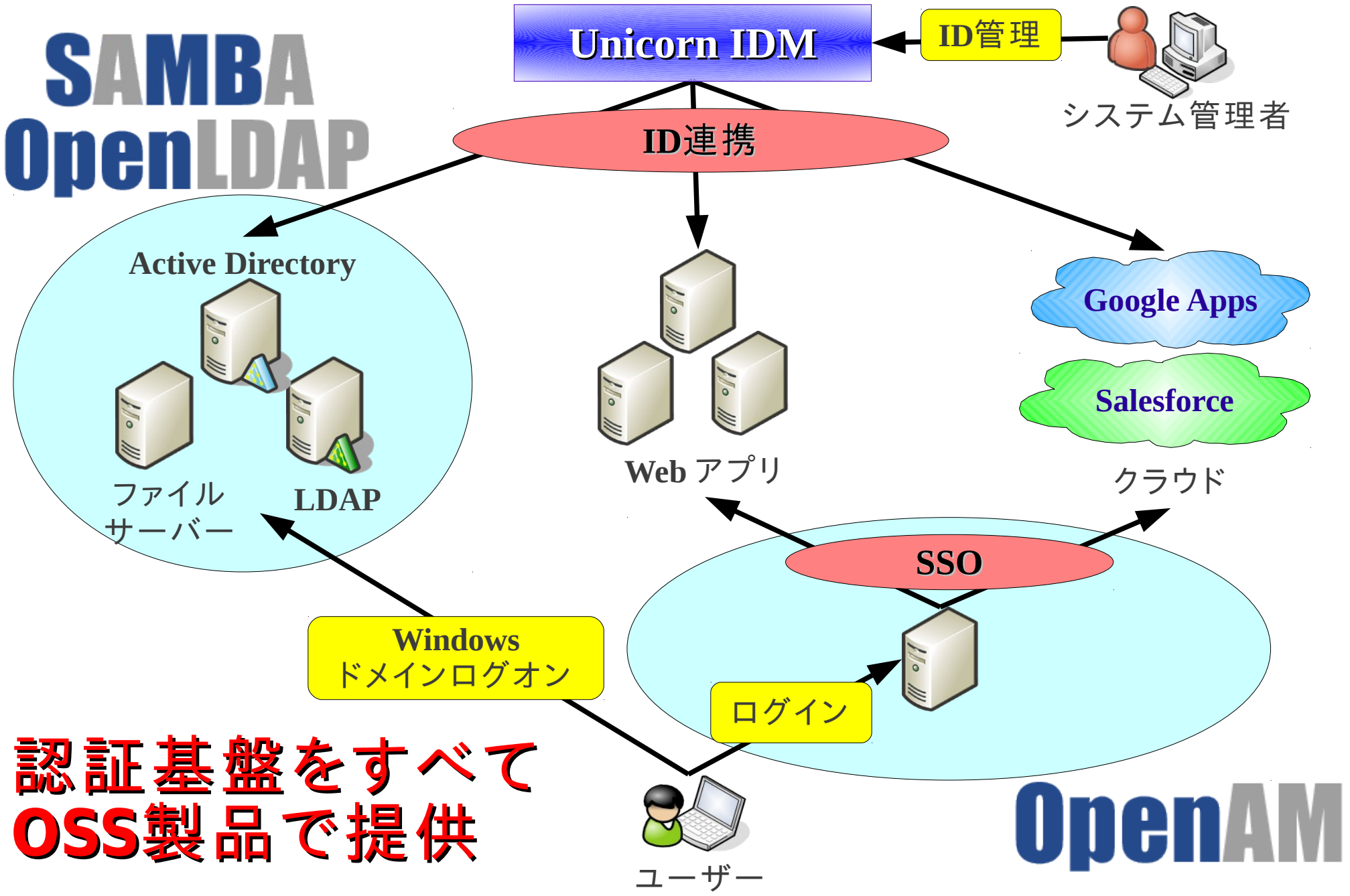
会社概要

会 社 名	オープンソース・ソリューション・テクノロジ株式会社	所属 団体等	OpenSSO&OpenAMコンソーシアム理事 副会長 OSSコンソーシアム理事 副会長 OSCA(Open Standard Cloud Association)理事 LPI-Japanビジネスパートナー デルISVアリーナ パートナー NEC CLUSTERPRO WORKSパートナー レッドハット レディ・ビジネス・パートナー
英語表記	Open Source Solution Technology Corporation		
社名略称	OSSTech（ｵｰｴｽｴｽﾃｯｸ）または OSSテクノロジ		
業務内容	・OSS（オープンソース）を中心とするソフトウエアの 企画、開発、販売およびサポート ・システムの導入に関するコンサルティング ・ソフトウエアに関する教育、研修	取引先 および ﾊﾟｰﾄﾅｰ様	・株式会社野村総合研究所 ・デル株式会社 ・株式会社バッファロー ・日本電気株式会社 ・株式会社 大塚商会 ・キヤノンITソリューションズ株式会社 ・伊藤忠テクノソリューションズ株式会社 ・新日鉄ソリューションズ株式会社 ・株式会社PFU ・株式会社 日立ソリューションズ ・三菱電機インフォメーションシステムズ株式会社 ・ソフトバンク・テクノロジー株式会社 ・ニフティ株式会社 ・三井情報株式会社 ・ダイワボウ情報システム株式会社 ・NTTデータ先端技術株式会社
役 員	代表取締役　　小田切 耕司 技術取締役　　武田 保真		
オフィス	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		
Web	http://www.osstech.co.jp/		
設立	2006年9月		
資本金	1500万円		

OSSTechのソリューション領域



OSSTechのソリューション導入効果



認証基盤をすべて
OSS製品で提供

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
  - Tomcat,OpenLDAP対応で高機能なシングルサインオン機能を提供
- Unicorn ID Manager for Linux/Solaris
  - Google Apps,ActiveDirectory,LDAP, Yahoo!メール Academic Editionに対応した統合ID管理

OSSTechの製品群（すべてOSSで提供）

- Chimera Search 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 for Linux
  - リモートからのWindowsファイルサーバアクセス機能を提供
- Mailman for Linux/Solaris
  - Google Appsのメーリングリスト機能を補完
- Netatalk for Linux/Solaris
  - UTF-8に対応したMac OS対応のAFPファイルサーバー

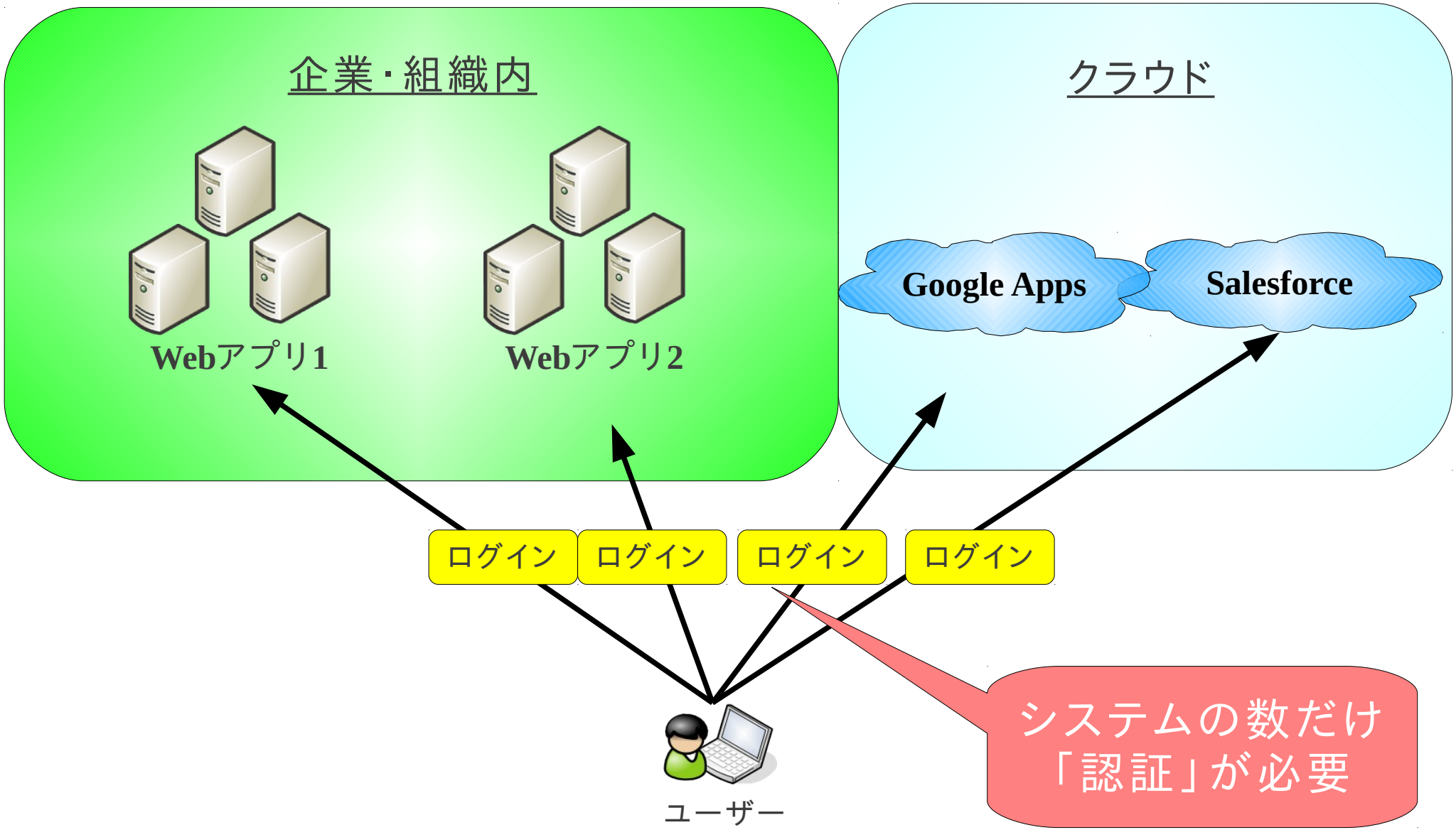
特にOpenAM(Java)のエンジニア募集中

- http://www.osstech.co.jp/company/recruit
- recruit@osstech.co.jp

- **OpenAM(OpenSSO)**を使ったシングルサインオンもしくは**Samba**、**OpenLDAP**を使った統合認証に関する開発エンジニア、コンサルタント、アーキテクト
- シングルサインオン、統合認証、**Linux / UNIX / OSS**経験
- **Java,C**の知識があり、前向きに自分でスキル向上を目指せる方
- 紹介会社などを通さず直接弊社へ募集エントリされた方には、入社後現金20万円を差し上げます

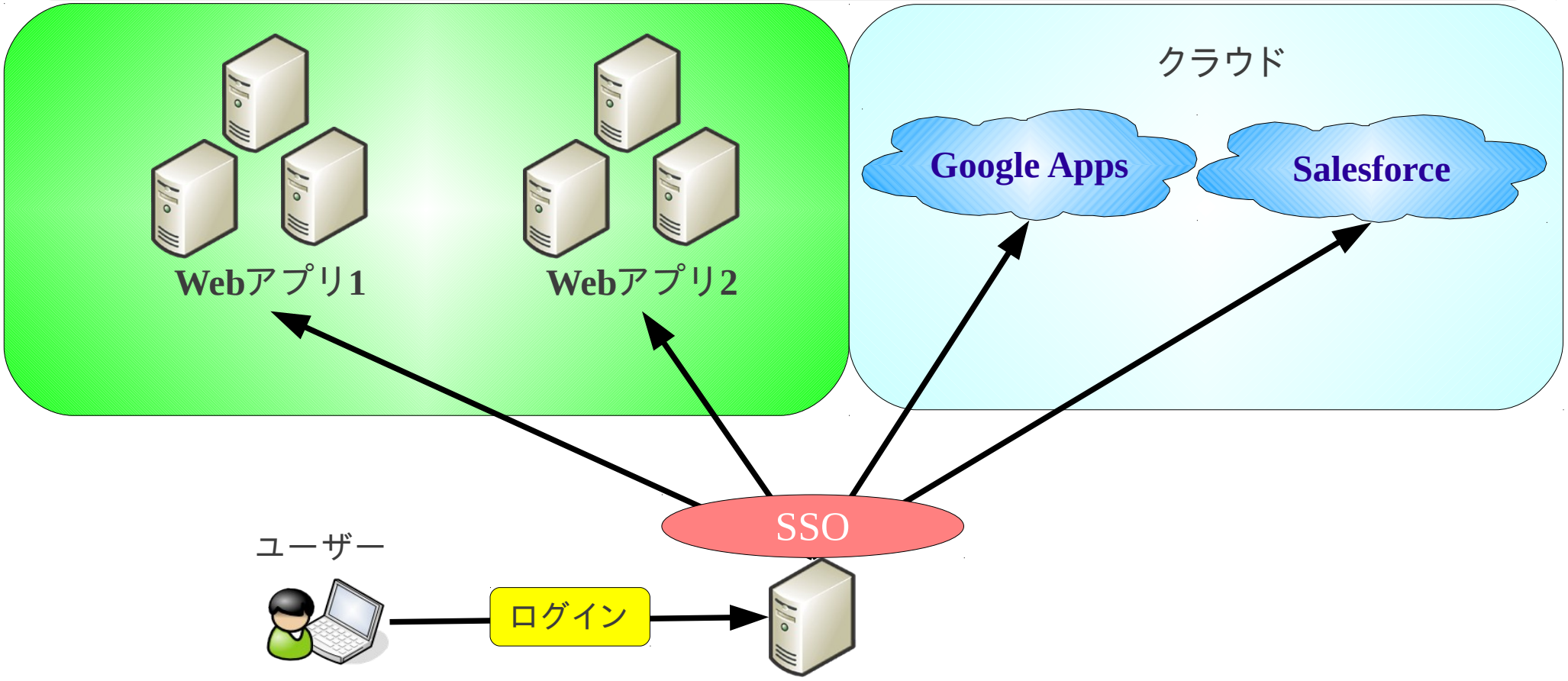
シングルサインオンとは

システムには必ず必要な「認証」



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Web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。
（以後、SSO と略すことも）



シングルサインオンを実現するソフトウェア

OSSTech

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

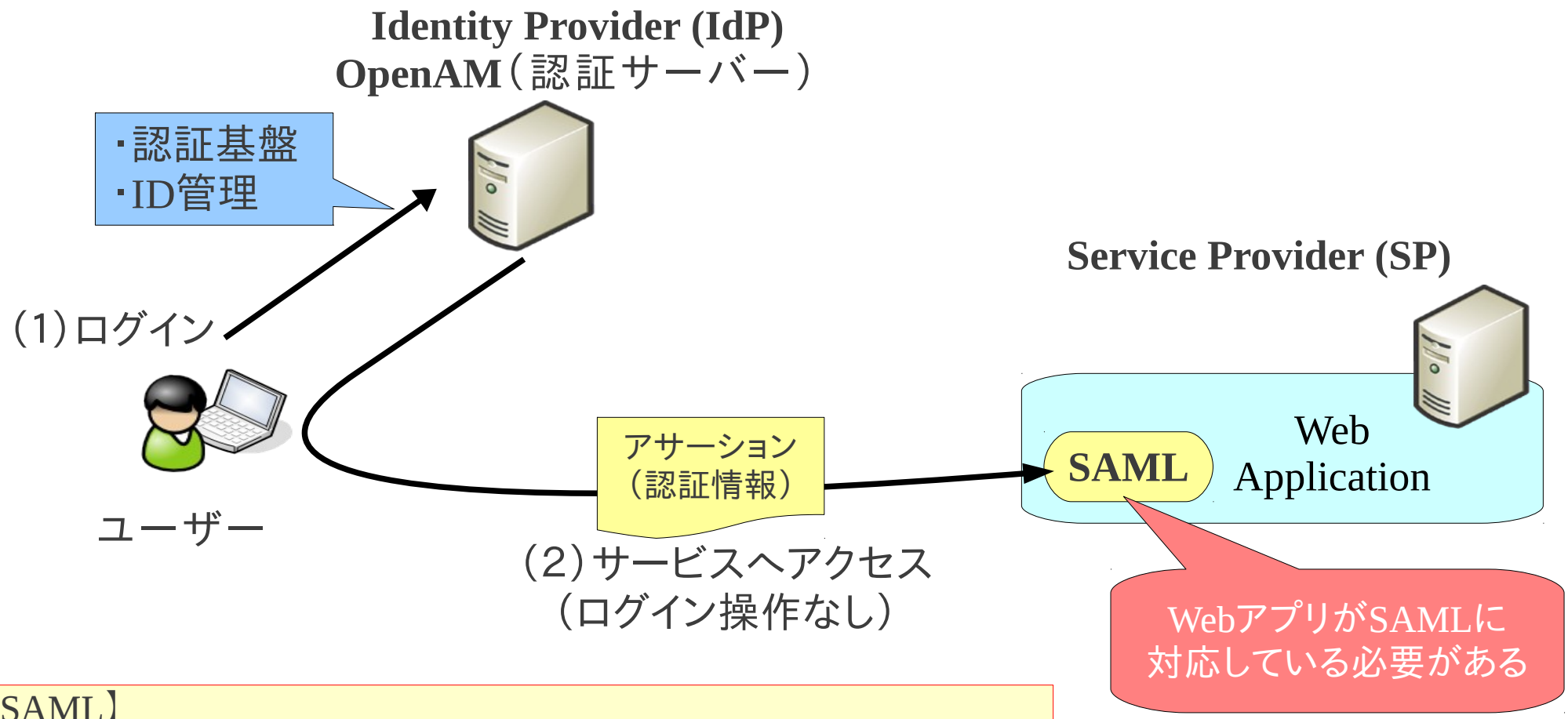
OpenAMとは？

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
  - SAMLよるシングルサインオン
  - エージェント方式によるシングルサインオン
  - リバースプロキシ方式によるシングルサインオン
- **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
- FedletやPolicy AgentなどのアプリケーションにOpenAMによる認証/認可を実現する仕組みを用意
- GUIによる管理が可能

シングルサインオンの方式（1）

SAML

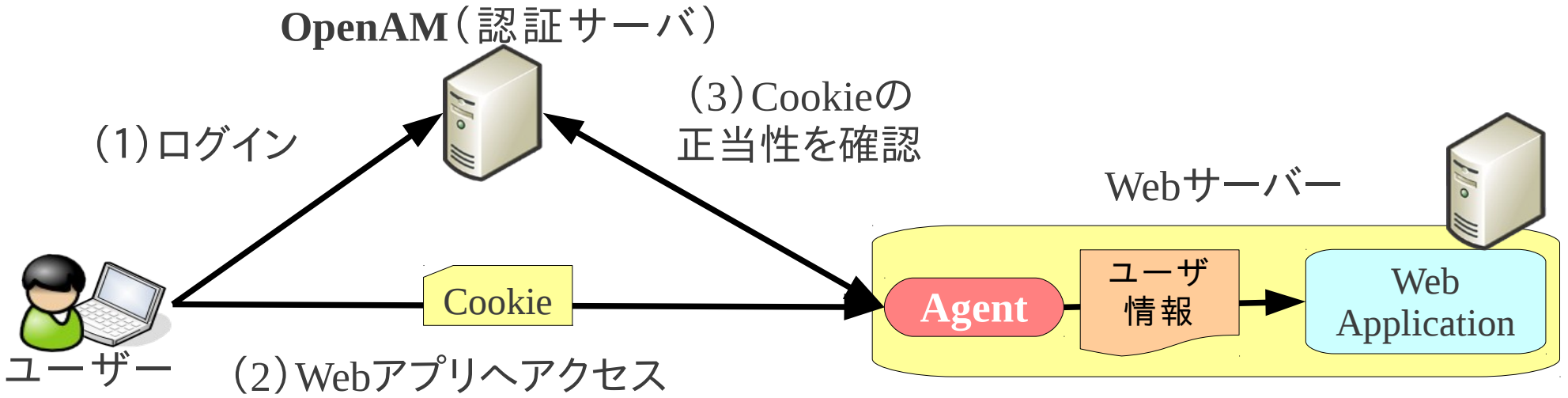


【SAML】
認証連携を行うための標準規格
GoogleやSalesforce等のクラウドサービスで利用

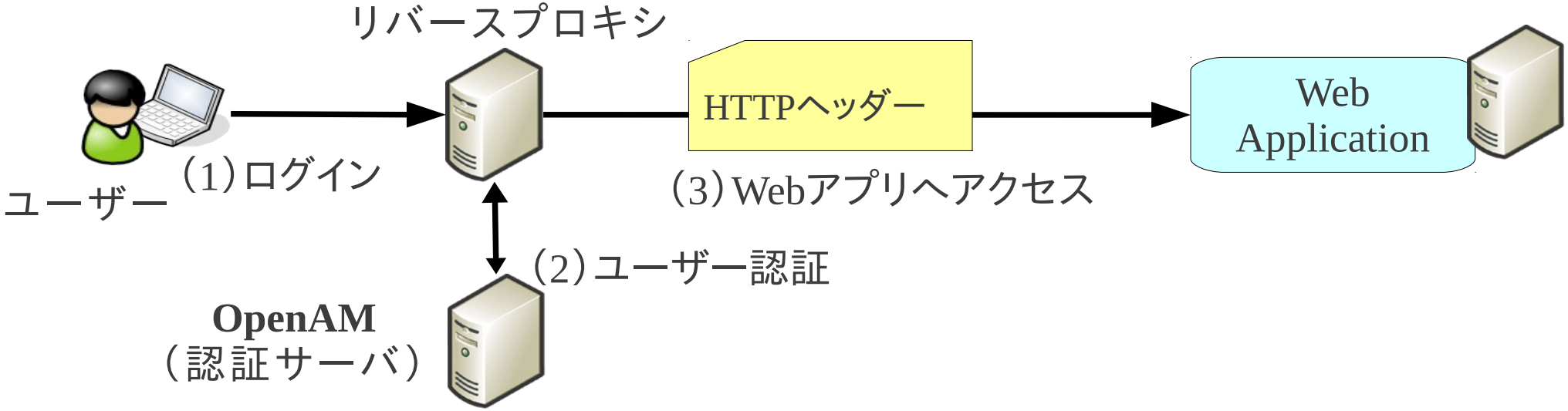
※この図は、HTTP Redirect Binding/HTTP POST Binding の場合の例です。

シングルサインオンの方式(2)

エージェント方式

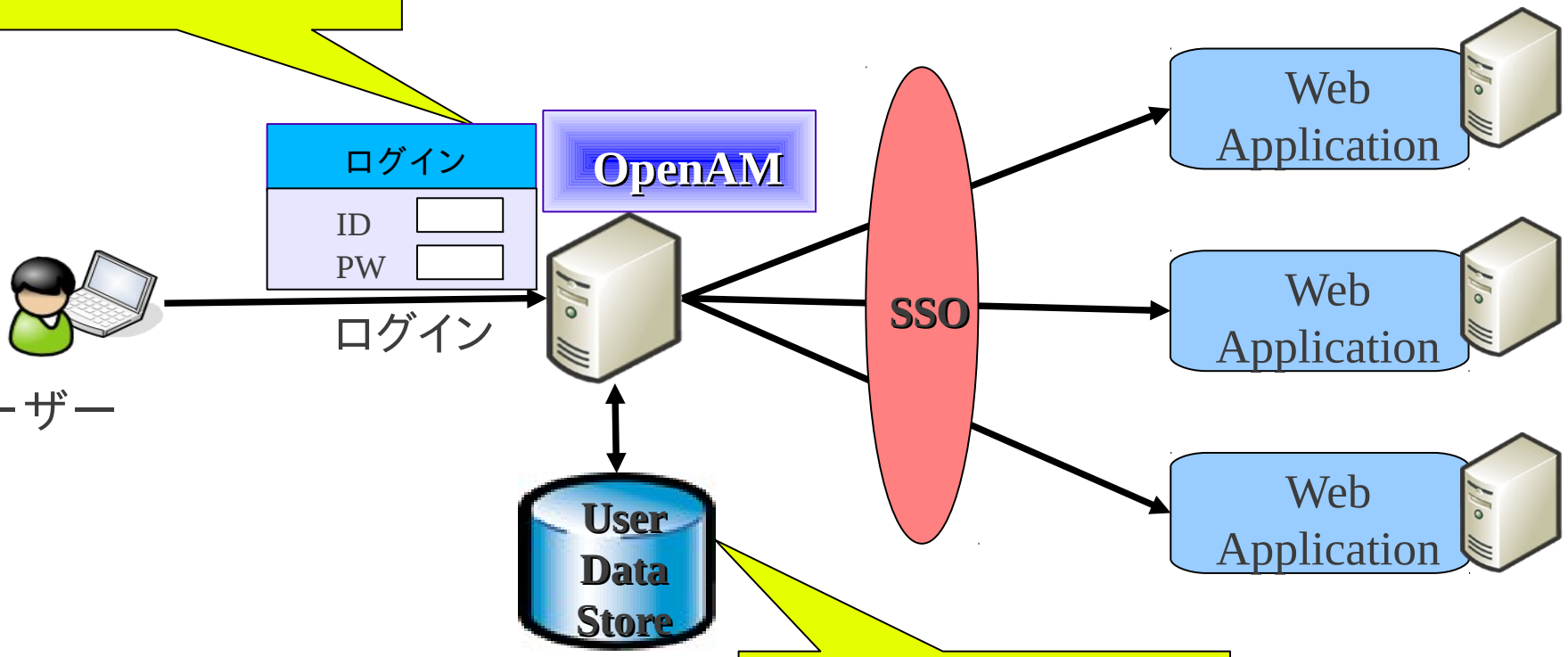


リバースプロキシ方式



OpenAMの機能-データストアと認証方式

認証方式
- ワンタイムパスワード
- Windows Desktop SSO
- クライアント証明書
- 外部DB
- 認証連鎖



ユーザーデータストア
（ユーザー情報DB）
- Active Directory
- OpenLDAP
- RDB

OpenAMの機能 - 認証方式

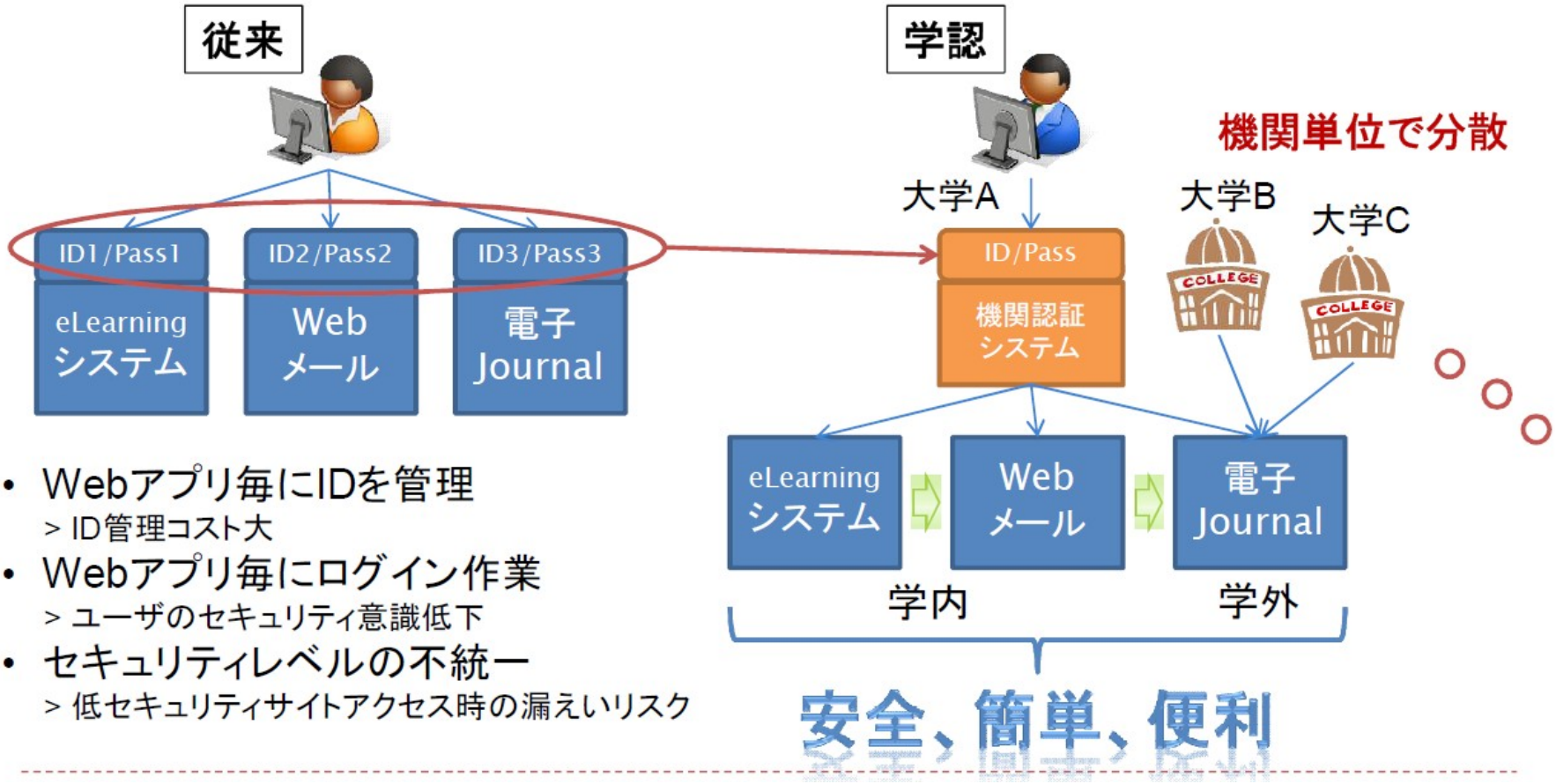
- 基本的には OpenAM のユーザーデータストアに保存された ID/パスワードにより認証を行なう
- ユーザー認証時に外部のデータベースを参照することも可能（更新できない参照のみのものでも可能）
  - LDAP、Active Directory、RADIUS、RDB（JDBC）
- よりセキュアな認証方式も使用可能
  - ワンタイムパスワード（電子メールを利用）
  - クライアント証明書による認証
  - Windows Desktop SSO（統合Windows認証）
- 複数の認証方式を組み合わせて使用可能：認証連鎖

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

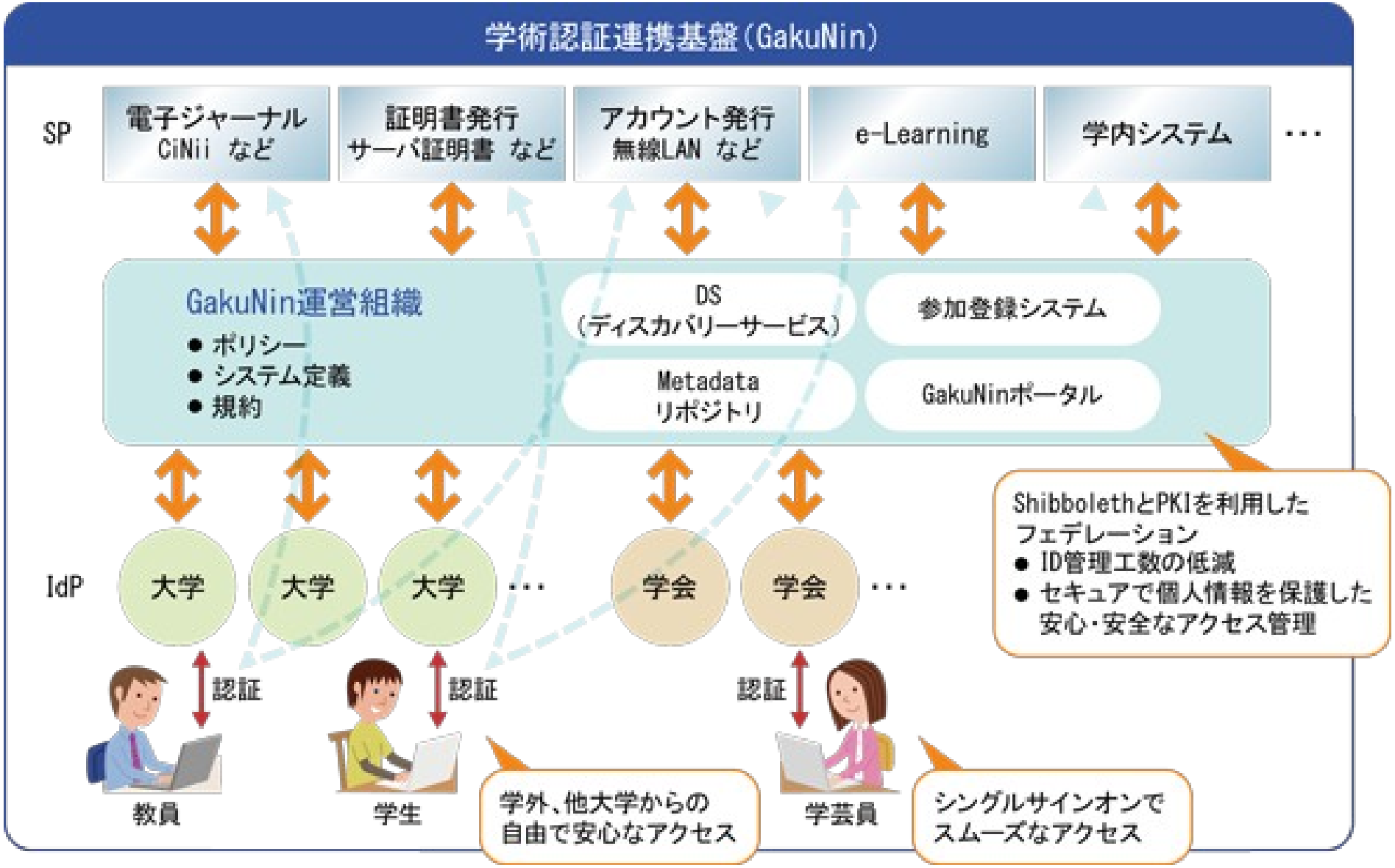
- Webアプリケーションへのシングル・サイン・オン（SSO）技術を、組織を越えて活用する分散型認証基盤



- 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/

学認で利用されている技術

- SAML（Security Assertion Markup Language）
  - 認証情報の連携を行うプロトコル
  - 学認のSP - IdPのやりとりはSAMLで行うと取り決め

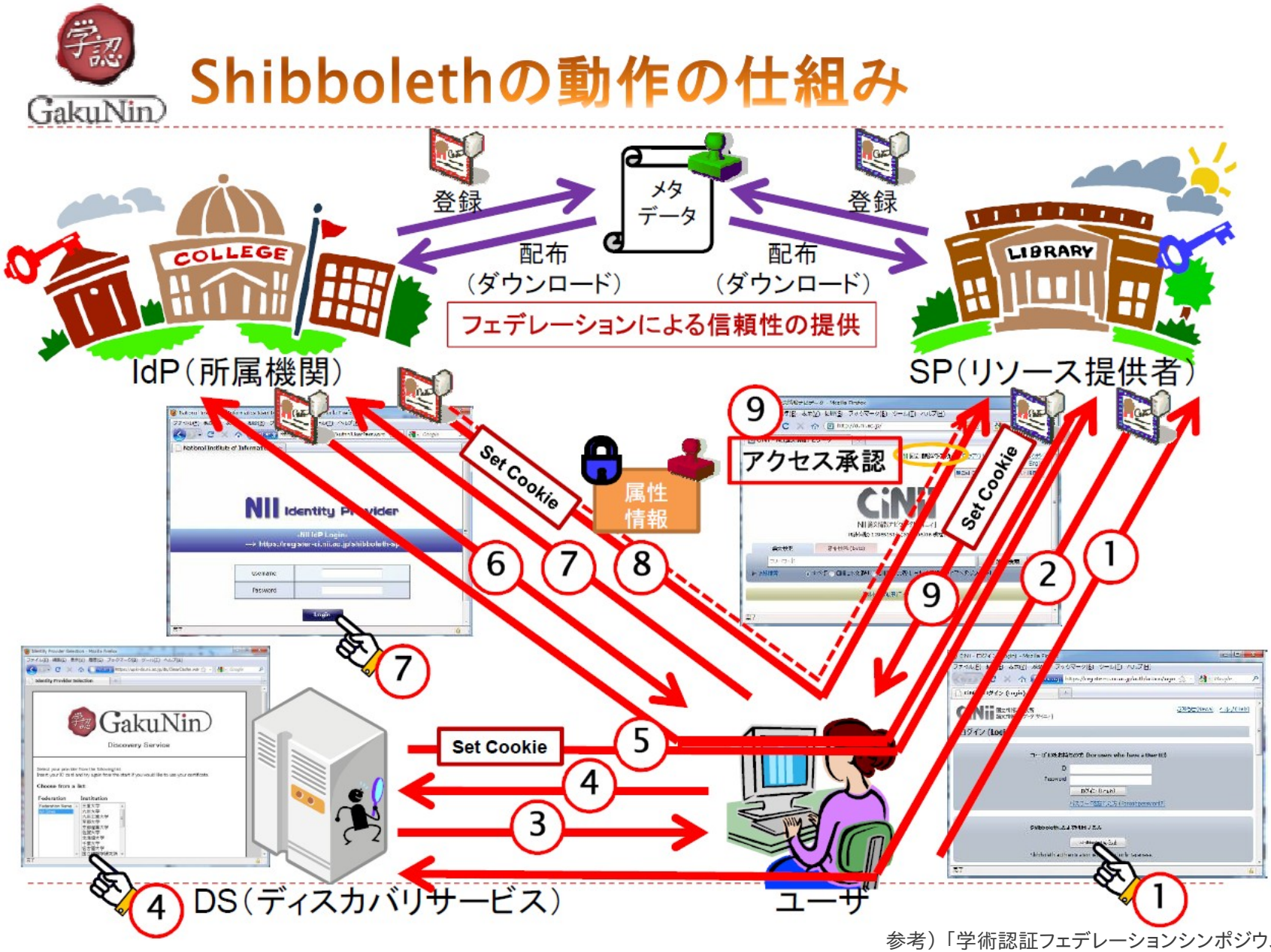
- 学認に参加し、SPやIdPと連携するためには・・・
  - SAMLを扱える認証基盤の構築が必要
  - ソフトウェアはSAMLを扱えれば何でも良い

- しかし、実際はほとんどShibbolethで構築
  - 学認のシステム運用基準で推奨されている

> GakuNin では，フェデレーション内で利用するソフトウェアとして，上記プロトコルの実装例であるShibboleth を利用することが推奨される。
> （※上記プロトコルとはSAMLのこと）
>
> 学術認証フェデレーションシステム運用基準（*Ver 1.2*）より引用
> *https://www.gakunin.jp/docs/files/GakuNin_System_SpecV1.2.pdf*

  - 学認のWebページにShibbolethの情報があり、構築しやすい

学認(Shibboleth)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

- 学認テストフェデレーションデモ
  - 前ページのフローを実際にやってみる。

- SPへアクセス
- DSへアクセス
- DSにて自身が所属する機関を選択
- IdP(自身の機関)へアクセス
- IdPにて認証
- SPのサービスを扱える

OpenAMとShibbolethの連携

学内の認証をShibbolethで？ (1)

- 学認へ参加する場合はShibbolethで構築するのが良い
  - Shibbolethが学認推奨のソフトウェアである点
  - メタデータの取扱いや属性情報の用意等、Shibboleth独自の機能を使った方が運用上において楽な点

【例えばOpenAMで学認に参加することを考える】
SAMLでやりとりを行うため、OpenAMと学認との連携は技術的には可能。
しかし、OpenAMで学認との連携するシステムを運用していくためは、Shibbolethの独自機能を補う仕組みを用意する必要がある。

- Shibbolethによる学内のシングルサインオン
  - 学認用に導入したShibboleth IdPを使い、学内のシングルサインオンを実現できないか？（せっかくシングルサインオン製品を導入したのだから）

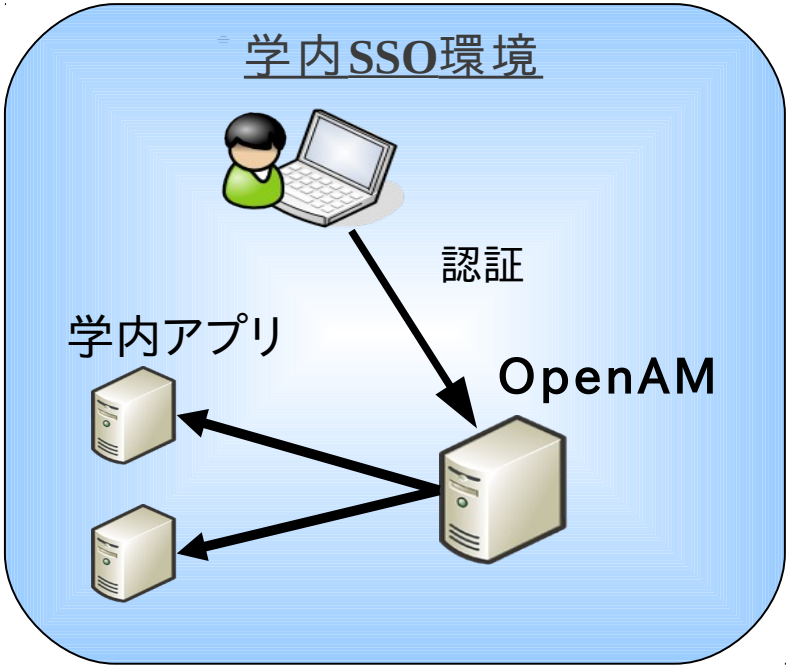
学内の認証をShibbolethで？ (2)

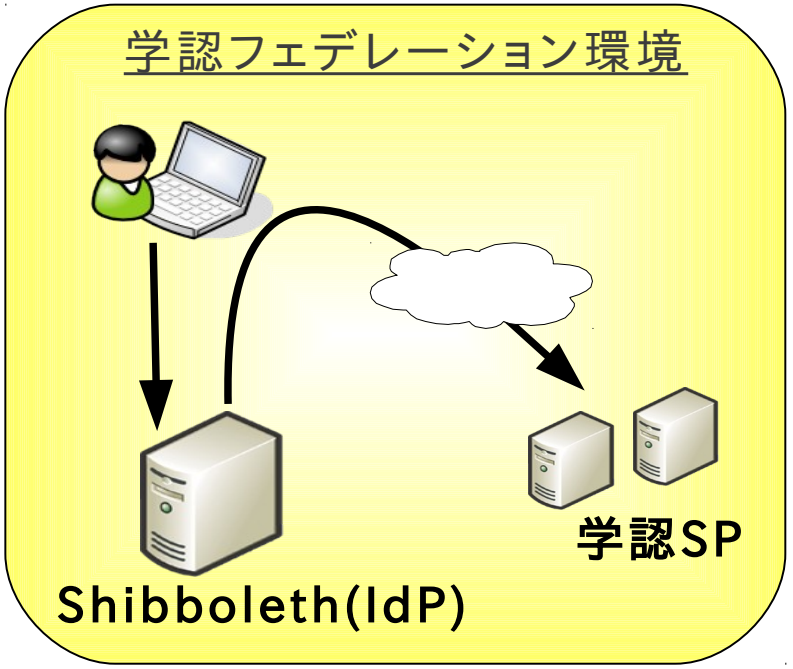
- 学内のアプリケーションをSAML化すればShibbolethでのシングルサインオン環境を実現できる
  - SAMLに対応していないアプリは改修が必要
- 他にもこんな懸念も・・・
  - 学認との接続ノウハウの情報はあるが、学内アプリのSSO化の情報が少ない
    - アプリケーションのSAML化ってどうすれば良いかわからない
    - アプリケーションの改修にコストがかかる
  - Shibbolethの標準機能では認証方式はID/Password形式
    - デスクトップSSO/クライアント証明書等柔軟な認証方式を採用できない
    - 複数の認証方式の組み合わせ認証連鎖を行えない
  - Shibbolethでは認証のみ提供。認可の提供はない。

Shibbolethは学内アプリケーションのシングルサインオンに不向き

学内のシングルサインオンはOpenAM

- 学内のシングルサインオンはOpenAMで行うのが良い
  - OpenAMはシングルサインオンの方式としてSAML以外も用意
    - 様々な方式を用意しアプリの改修なしでシングルサインオンを実現可能
  - 多様な認証方式を用意
    - ID/パスワード認証以外に認証方式を標準で備えており、システムのセキュリティや用途にあった認証方式の選択が可能
- 学内はOpenAM、学認はShibbolethという構成がベスト





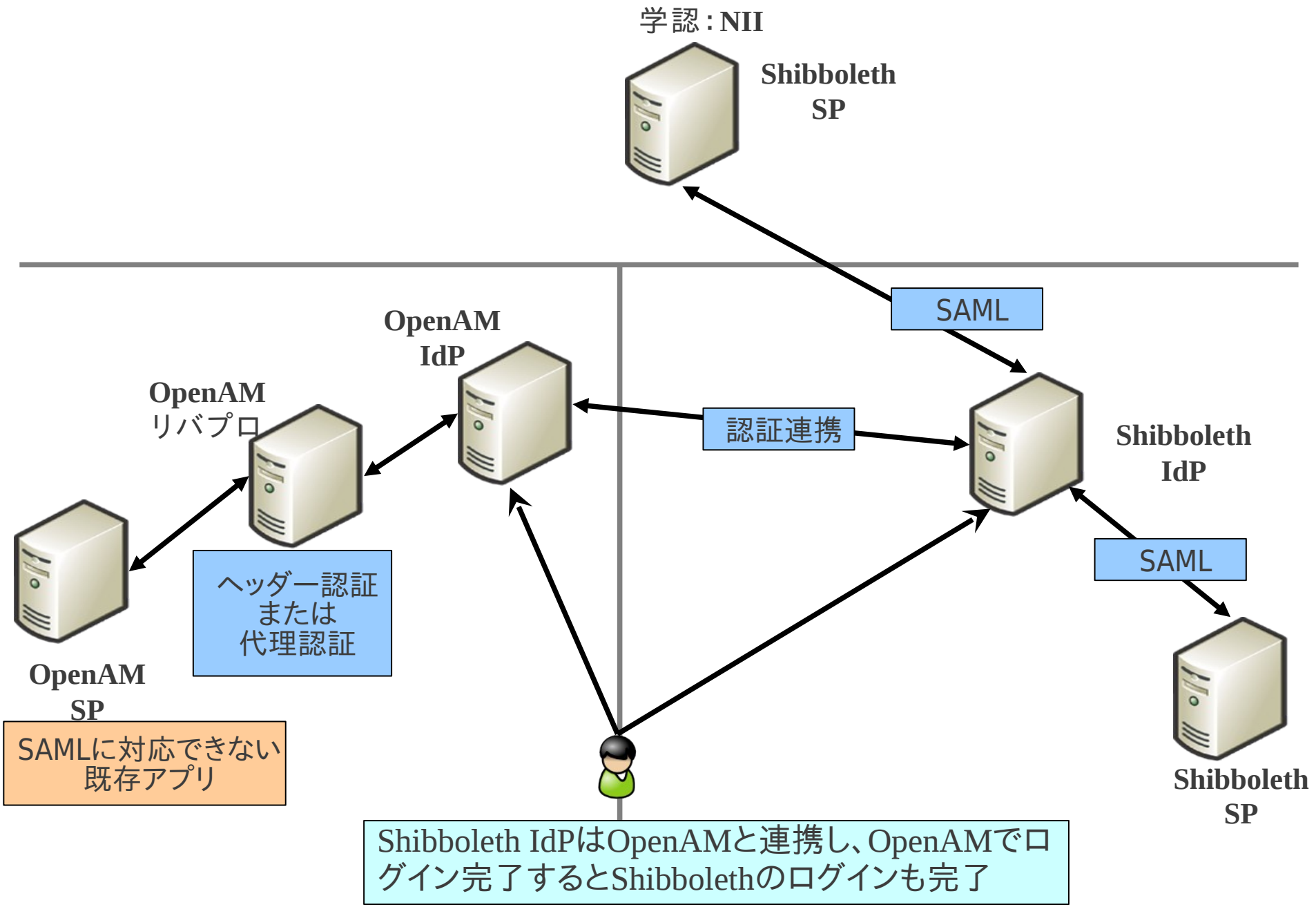
•OpenAMとShibbolethの連携

- OpenAMとShibbolethが別々では、それぞれで認証が必要
  - シングルサインオン製品を活かせていない！

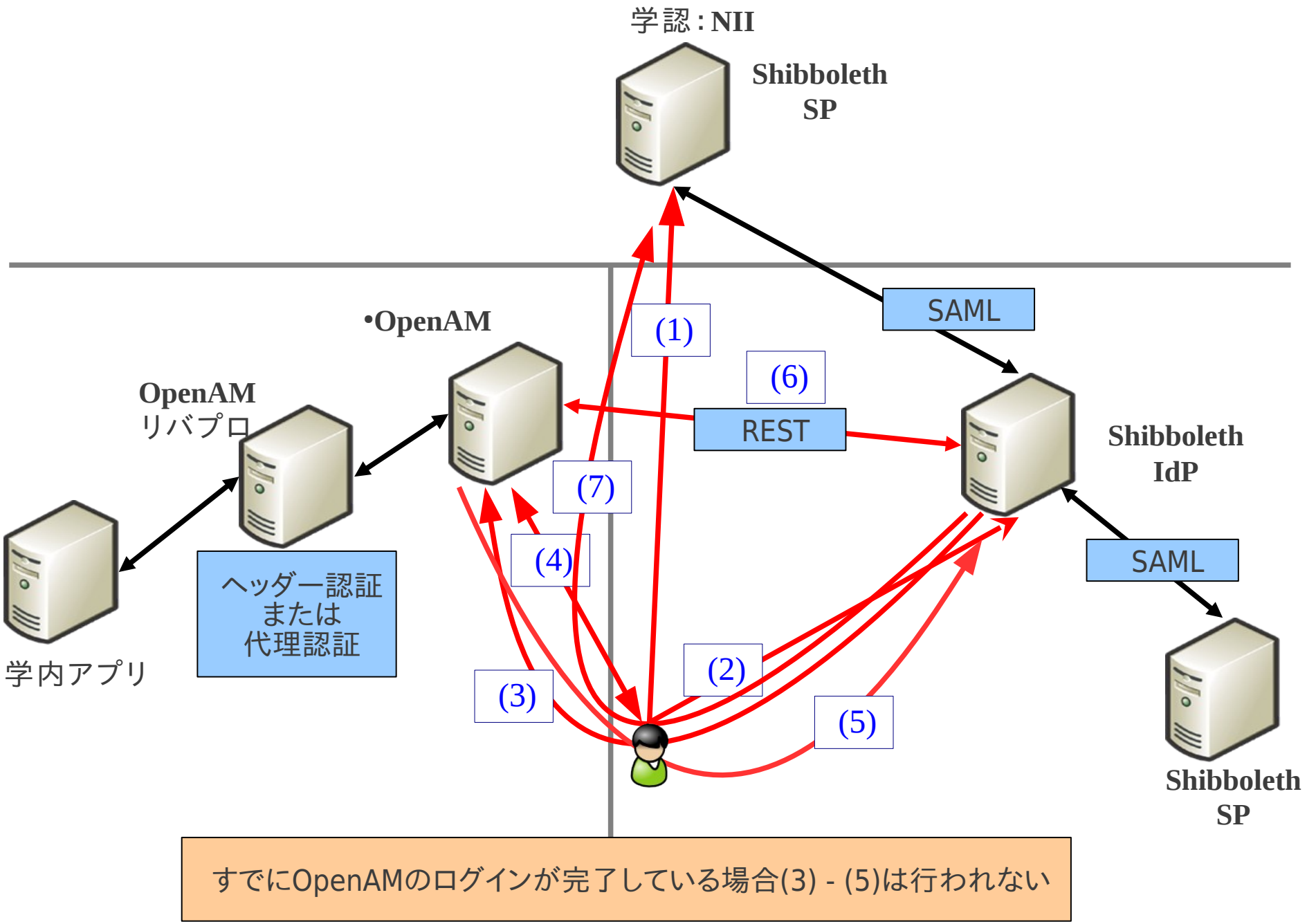
- そこでOpenAMとShibbolethを連携する
  - Shibboleth IdPの認証をOpenAMで行う
    - 具体的にはShibbolethがOpenAMにRest APIによる認証有無の問い合わせを行い、ユーザーはShibbolethでのログイン操作は行わなくて済む

ユーザーは一度の認証で、学認、学内のアプリケーションが使用可能

OpenAMとShibbolethの構成



OpenAMとShibbolethの構成

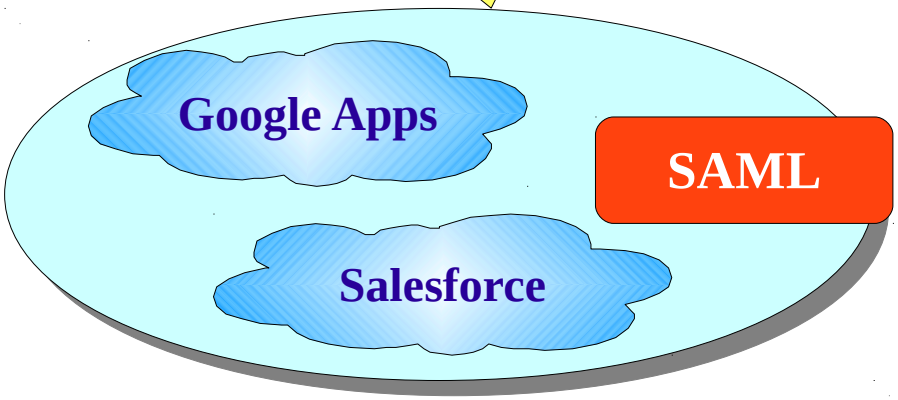


- OpenAMとShibbolethの連携
  - 学認テストフェデレーションをOpenAMで認証
  - 前ページのフローを実際にやってみる。
    - デモ1と異なり、DSにてIdP選択後OpenAMの認証画面表示
    - OpenAM認証完了すると学認SPが利用可能
  - 学内のアプリケーション
    - OpenAMで学内アプリのシングルサインオンを実現

まとめ

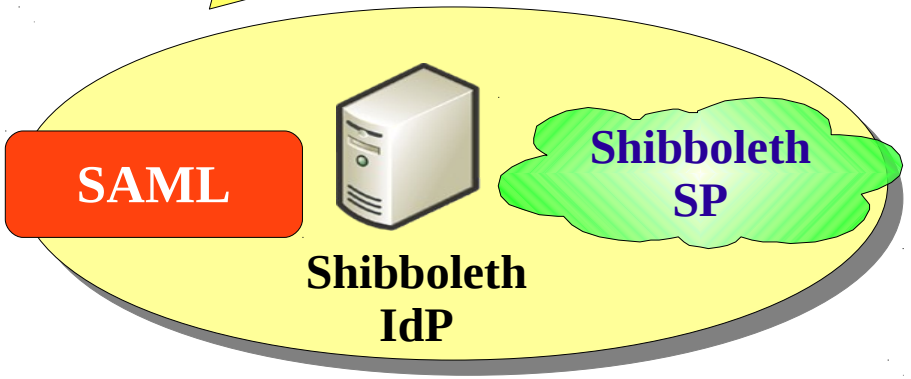
これからのSSO - 混在する複数のSSO環境

SAML IdP を導入して
SSO を実現

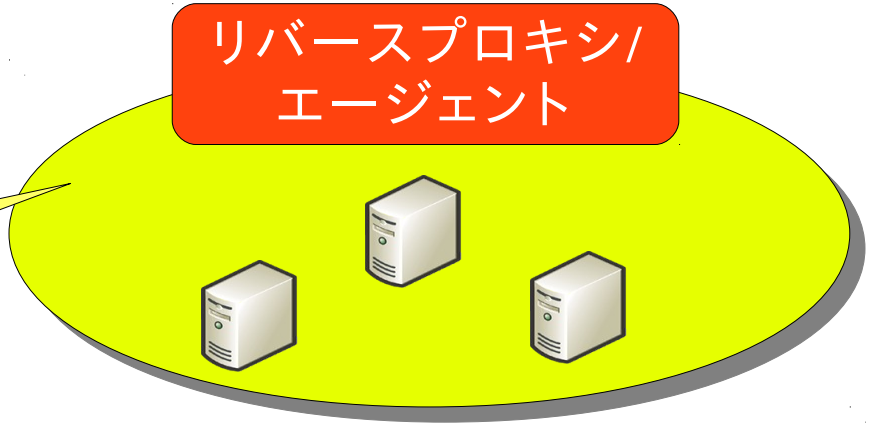


クラウドSSOセグメント

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

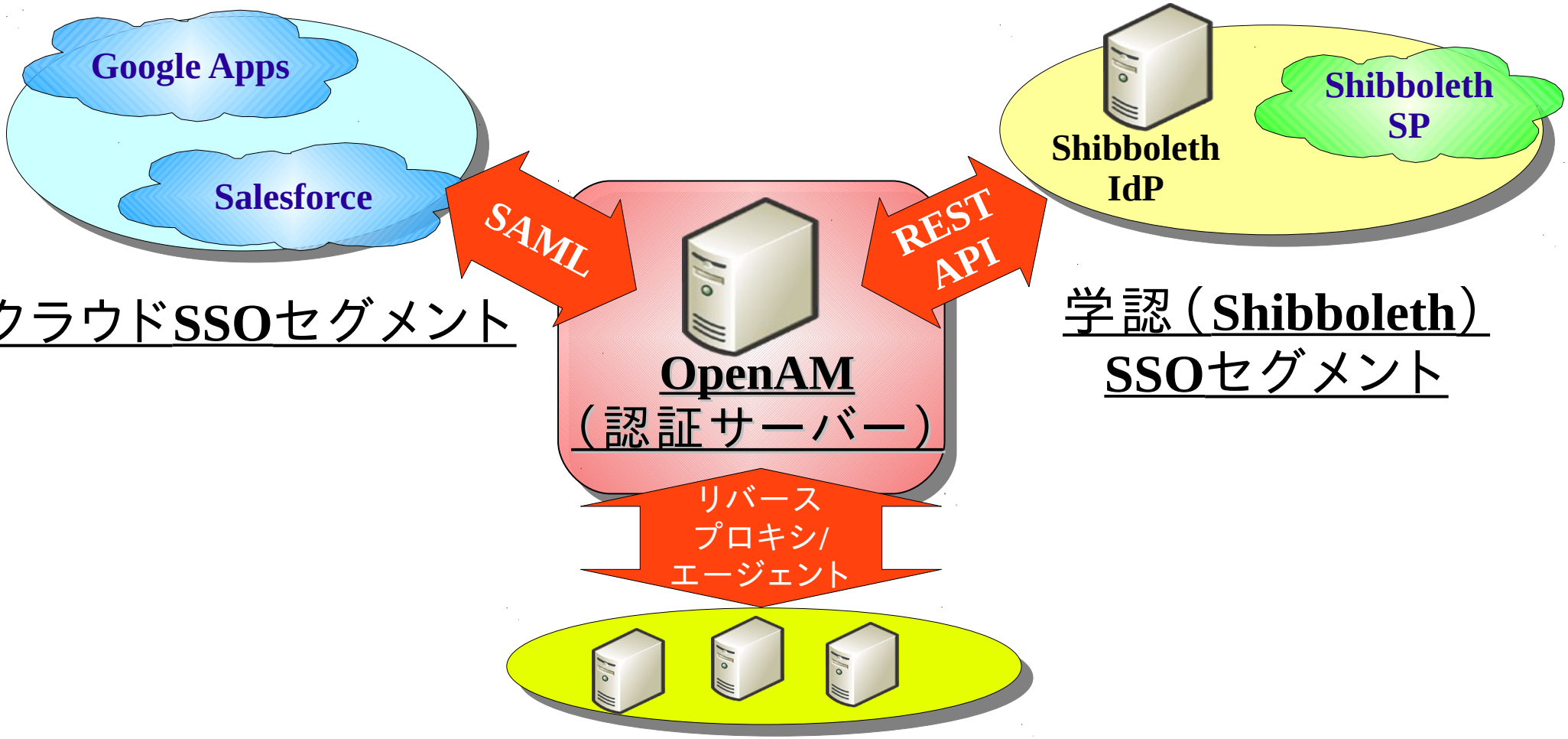
学内SSOセグメント

これからのSSO - 混在する複数のSSO環境

- 今後は複数のシングルサインオン環境（仮に"シングルサインオンセグメント"と表現）が混在するようなシステムの需要が予想される
- 発生する課題
  - 1つのシングルサインオンソフトウェアでは全てのアプリケーションの認証を行えない場合がある
  - 同じプロトコル（SAMLなど）を実装しているソフトウェアでも、代替不可能な場合がある
    - 例：Shibboleth（学認）は SAML を実装しているが、Shibboleth は独自の仕組みも実装しているため、他の SAML を実装したソフトウェアでは代替が困難
- シングルサインオンセグメントを統合管理する必要がある
  - 複数のインタフェースを装備し、プロトコルや仕様の違いを吸収できる柔軟なシングルサインオンソフトウェアが必要

OpenAM なら実現可能！

OpenAM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

事例紹介

- 福岡大学様認証基盤システム

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

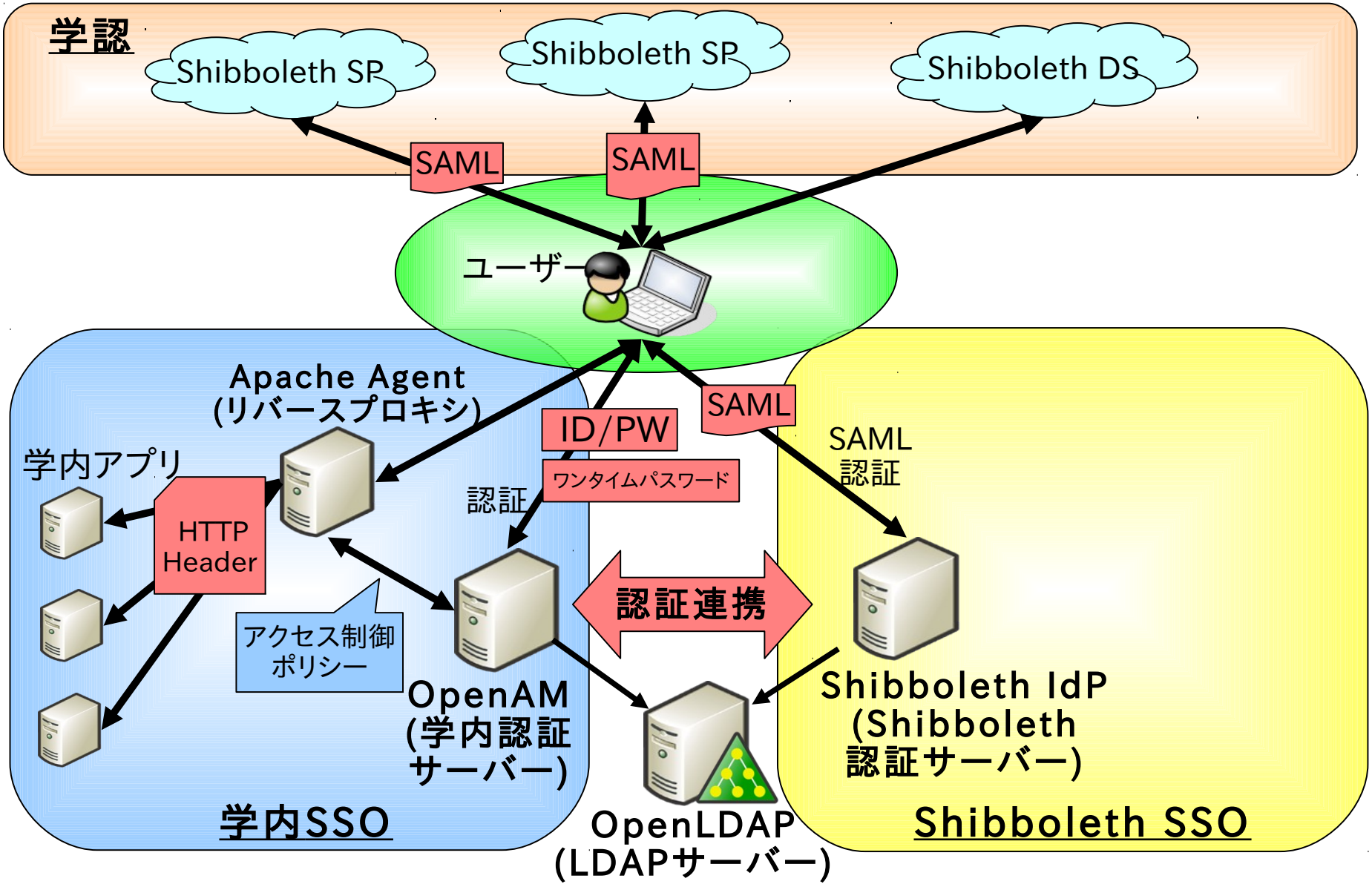
ミッション

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

システム構成



- **OpenAMとShibbolethを連携したシステムを構築**
  - 学認とはShibbolethで認証連携
  - 学内ではOpenAMに認証を集約

    アクセス条件によってワンタイムパスワードの認証求める、Shibbolethだけでは実現できないセキュアなシステム構成を実現
  - 学認と学内のSSOを実現
    - ユーザーが1度の認証で学内、学認のシステムを使用可能な構成を実現

- フルオープンソースで **SSO** 基盤を構築
  - 学内認証サーバー：OpenAM
  - Shibbolethサーバー：Shibboleth-IdP
  - LDAPサーバー：OpenLDAP
  - リバースプロキシサーバー：Apache + OpenAM Policy Agent

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