オープンソースで実現する
認証基盤とID管理

オープンソース・ソリューション・テクノロジ株式会社

OSSTech

お問い合わせ info@osstech.co.jp

アジェンダ

- OpenAM製品紹介
  - OpenAM 13 新機能
  - OSSTech版 OpenAMのサポート
  - パートナー支援プログラム
  - シングルサインオン構成例
- Unicorn ID Manager v3 製品紹介
  - 機能紹介
  - Unicorn ID Manager システム構成例

OpenAM 13 新機能

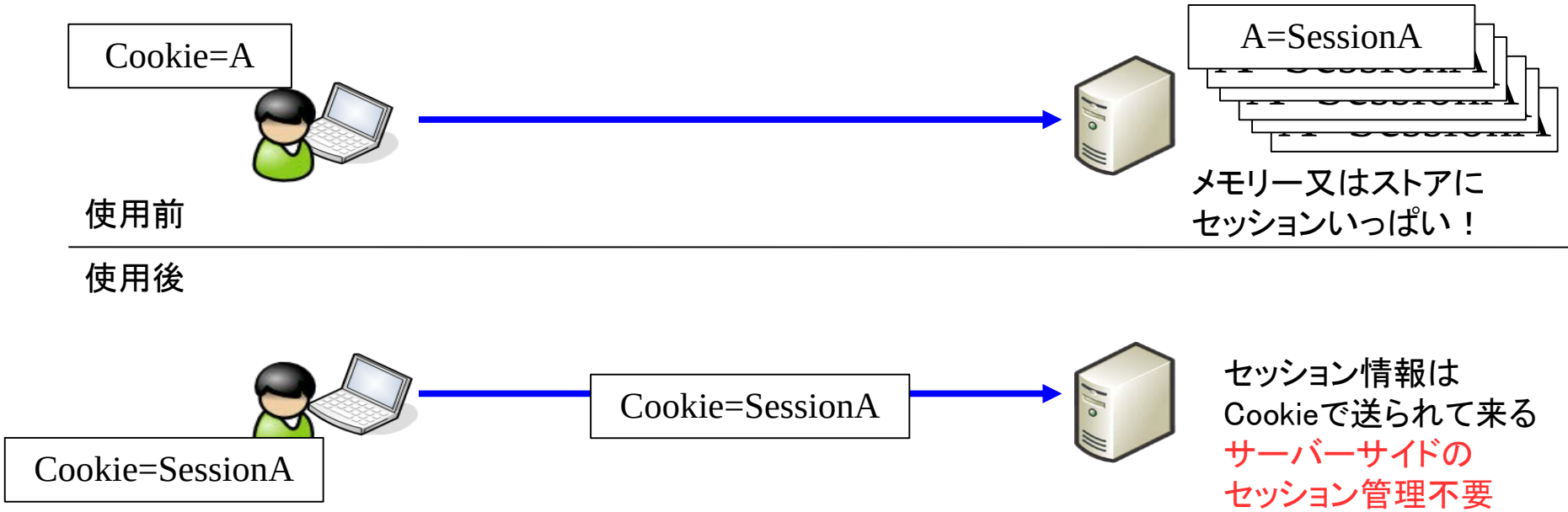
- SAML2 Authentication Module
- Stateles Sessions
- UMA Authorization Server
- Contextual Authorization
- OpenID Certified
- etc,etc…

SAML2 Authentication Module

- SAML-SPの機能を認証連鎖に組み入れられるようになりました。
- (例えば) 外部IdPで認証後、さらにワンタイムパスワードを入力するなどの用途に使えます。

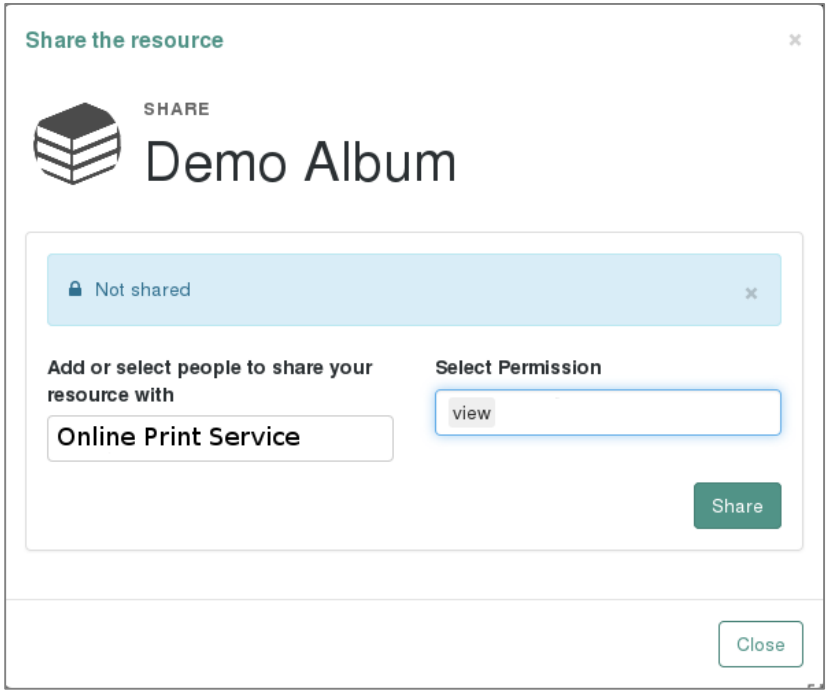
Stateless Sessions

- OpenAM内部にセッションを保持しなくても良い
- アクティブユーザー数が多いBtoCの世界へ



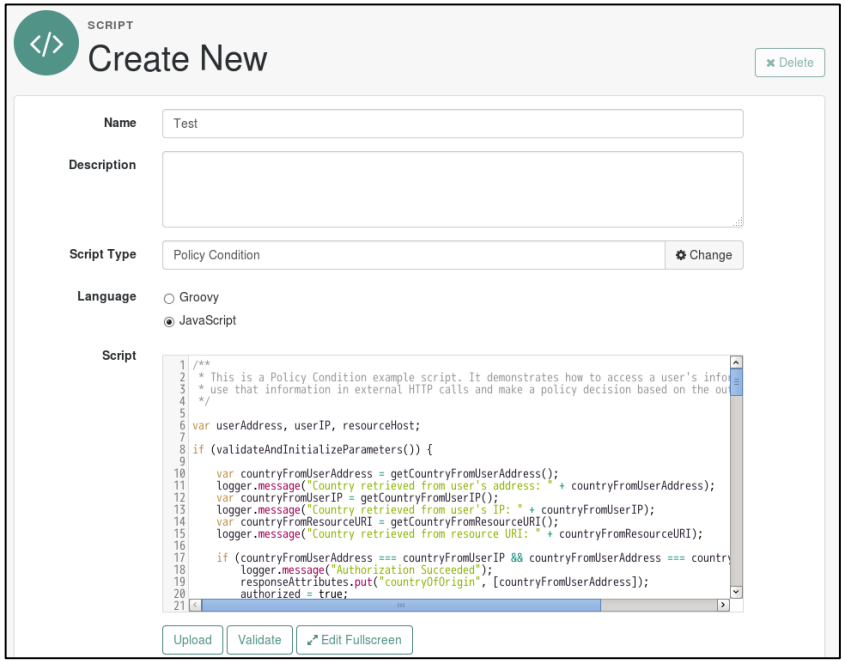
UMA Authorization Server

- UMA (User Managed Access)
  ユーザーによる認可管理機能
- OpenAMにおいてユーザー(リソースオーナー)自身がリソースへのアクセス認可を行うインターフェースが実装された。



Contextual Authorization

- 認可ポリシーをスクリプト等で動的に判断できるようにする
- スクリプトエディタまで内蔵



OpenID Certified

- OpenID Foundationのサーティファイ
  - http://openid.net/certification/

The OpenID Foundation enables implementations of OpenID Connect to be certified to specific conformance profiles to promote interoperability among implementations. The foundation's certification process utilizes self-certification and a conformance test suite developed by the foundation. Certified implementations can use the "OpenID Certified" certification mark. These resources are available to those considering or seeking certification:

- OpenID Certification Frequently Asked Questions (FAQ)
- OpenID Connect Conformance Profiles
- OpenID Certification Terms and Conditions
- OpenID Certification of Conformance (docx) (PDF)
- Attestation Statement (used with Dynamic OP profile only) (docx) (PDF)
- How to run conformance tests and gather data demonstrating conformance
- How to request certification after successfully completing conformance testing
- OpenID Certified Mark

These implementations have been granted certifications for these conformance profiles:

Organization	Implementation	OP Basic	OP Implicit	OP Hybrid	OP Config	OP Dyna
Auth0	Auth0	24-May-2016			24-May-2016	
Dominick Baier & Brock Allen	IdentityServer3 v1.6	8-May-2015	8-May-2015	8-May-2015	8-May-2015	
Clareity Security	Identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016	
ClassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015	
CZ.NIC	mojeID	7-Jul-2016		31-Jul-2016	7-Jul-2016	7-Jul-2016
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015	
ForgeRock	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015	

その他の機能

- コアトークンサービスのリファクタリングで高速化
- 認可ログの汎用性向上
- Oauth 2.0 デバイスフローへの対応

OpenAM セキュリティアップデート

- 塩漬けで運用していませんか?
- セキュリティアップデートリリース回数

バージョン	2012	2013	2014	2015	2016
OpenAM 9.5.x	3	0	2	3	3
OpenAM 11.x	-	-	2	5	3
OpenAM 13.x	-	-	-	-	(4)

本来は脆弱性が無いのが良いのでしょうが…
安全に長くご利用いただくためには、不可避なサービスです。

OpenAM11 2016年対応Fix

- 今年に限定したOpenAMの脆弱性のリストです。OSSTech版は対応済みです。
- もしコミュニティ版11.0.0をお使いならこれらは全て未対応です。

セキュリティIssue番号
Issue #201605-01: Credential Forgery
Issue #201605-02: Insufficient Authorization
Issue #201605-03: Authentication Bypass
Issue #201605-04: Cross-Site Request Forgery
Issue #201605-05: Cross Site Scripting (XSS)
Issue #201605-06: Credentials appear in CTS access log
Issue #201605-07: Content Spoofing Vulnerability
Issue #201604-01: User Impersonation via OAuth2 access tokens
Issue #201604-02: Open Redirect
Issue #201604-03: Cross Site Scripting
Issue #201604-04: Insufficient Authorization

セキュリティIssue番号
Issue #201604-04: Insufficient Authorization
Issue #201604-05: Information Leakage via Account Lockout
Issue #201604-06: Information Leakage
Issue #201601-01: Open Redirect
Issue #201601-02: Potential Denial of Service attack in multi-site deployments
Issue #201601-03: Cross Site Scripting
Issue #201601-04: Open Redirect
Issue #201601-05: Business Logic Vulnerability

OSSTech版OpenAMパッケージ

- RPMパッケージの採用

弊社メンバーの15年を超えるOSS経験から導き出されたお客様への回答！

- ソフトウェアサポートセキュリティアップデート作業まで運用チームへ渡せますか?
- ものすごく長い手順書じゃないですか？
- OSSTech版ならrpmコマンドが使えます。

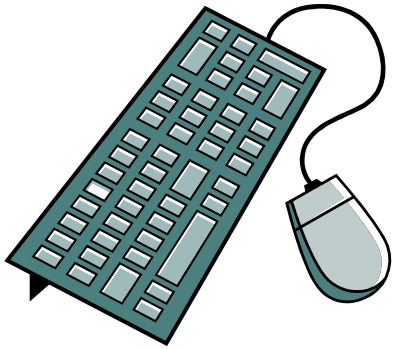
```
[root@openam01] # service osstech-tomcat7 stop
[root@openam01] # rpm -Uvh osstech-openam11-11.0.0-xxxx.noarch.rpm
[root@openam01] # service osstech-tomcat7 start
```

パートナー支援

- 無償ハンズオン
- 構築手順書
- ドキュメントテンプレート
- 設計支援
- 営業支援

パートナー支援：無償ハンズオン

- OpenAMパッケージのインストールから、SAML、エージェント、代理認証までを1日のカリキュラムで実機にてレクチャーします。



ハンズオンセミナー　タイムテーブル

時間	内容
10:00～10:30	- セミナー概要 - OpenAM説明
10:30～12:00	- OpenAMの初期設定 - SAML設定
12:00～13:00	昼食
13:00～15:30 ※休憩は適宜	- リバースプロキシ設定 - 代理認証設定
15:30～16:00	Q & A

Copyright © 2014 Open Source Solution Technology

パートナー支援：構築手順書提供

- ハンズオンのカリキュラムでは網羅できない、2重化やパスワードポリシー、代理認証のバリエーションなど、詳細な手順書とマニュアルをお渡ししています。QAも可能です。
- ノウハウの出し惜しみ無し!

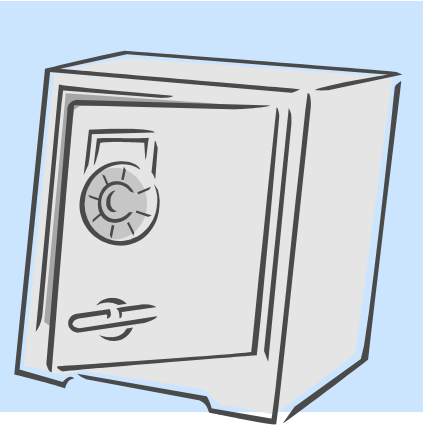
手順書マニュアル例
OpenAM ハンズオンテキスト（ノートつき）
OpenAM インストールガイド
OpenAM 初期設定ガイド
OpenAM インストールガイド
OpenAM 初期設定ガイド
OpenAM リリースノート
OpenAM コマンドライン利用手順書
OpenAM 画面カスタマイズガイド
OpenLDAP 認証モジュール利用手順書
OpenAM SAML 設定ガイド
Apache Policy Agent リファレンスマニュアル
Apache Policy Agent パッケージ インストールガイド
etc...

パートナー支援：ドキュメントテンプレート

- 設計時、納品時に必要なドキュメントのテンプレートを提供しています。

ーから作ると大変ですから是非活用してください。

ドキュメントテンプレートの一例
OpenAM基本設計書(方式設計)
OpenAM詳細設計書(パラメーターシート)
OpenAMテスト結果報告書
OpenAM運用手順書
リバースプロキシ詳細設計書
リバースプロキシテスト結果報告書
リバースプロキシ運用手順書
OpenLDAP関連 etc...



パートナー支援

- 設計支援
  - パートナー様のご要望に合わせて、各工程での支援をお受けしています。

パートナー支援

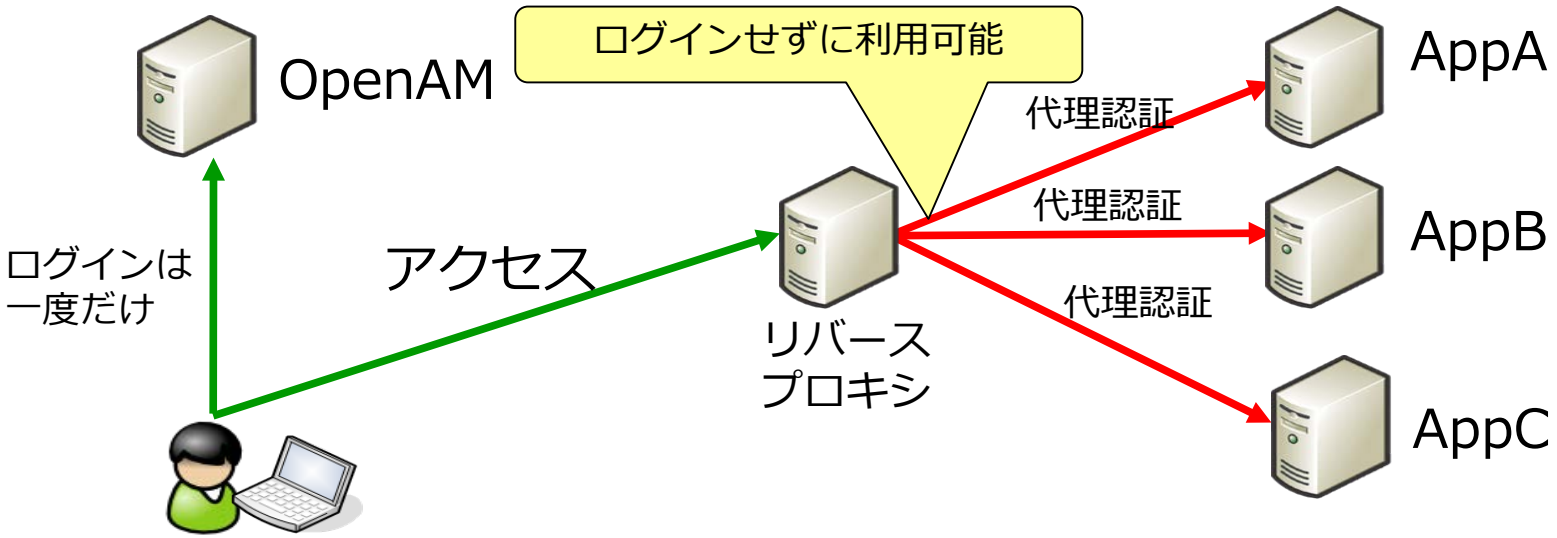
- 営業支援
  - もちろん営業同行します。

シングルサインオン構成例

- リバースプロキシ型 代理認証
- クラウドアプリケーション
- 学認
- WebサービスのSSO化

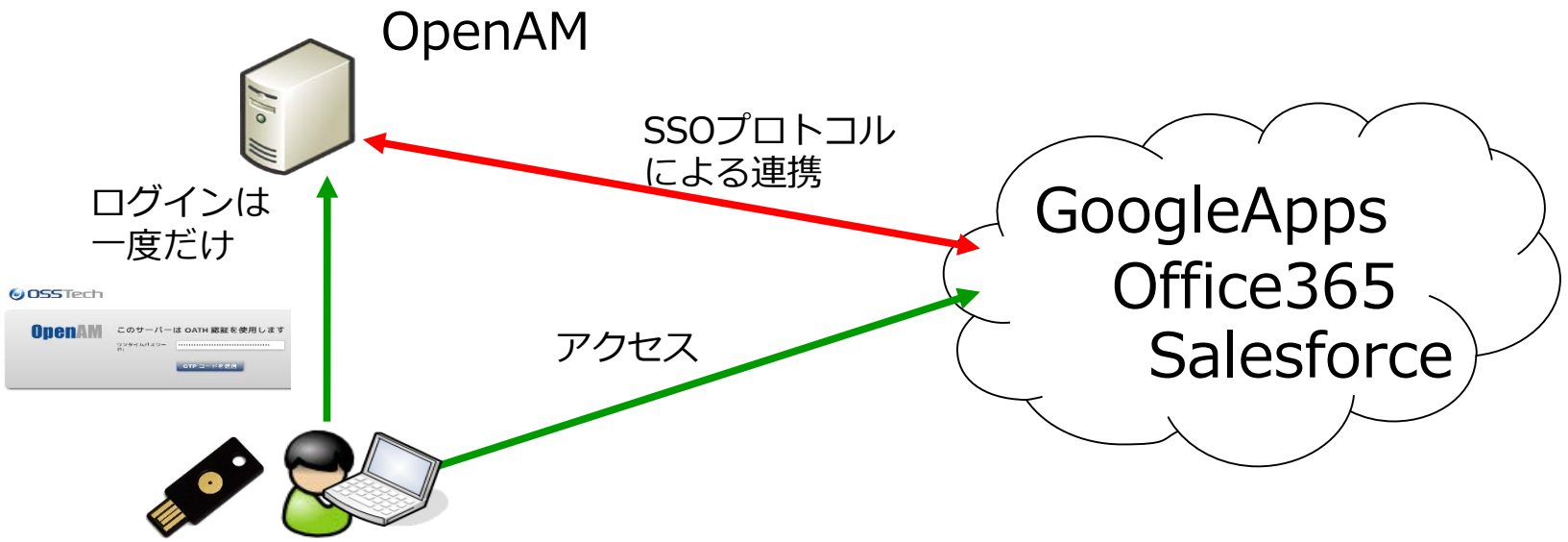
シングルサインオン構成例

- リバースプロキシ型 代理認証
  - アプリケーションを改修せずにSSO化
  - Form認証方式のログイン画面にリバースプロキシ上のモジュールが代理でID/PWを入力(代理認証)



シングルサインオン構成例

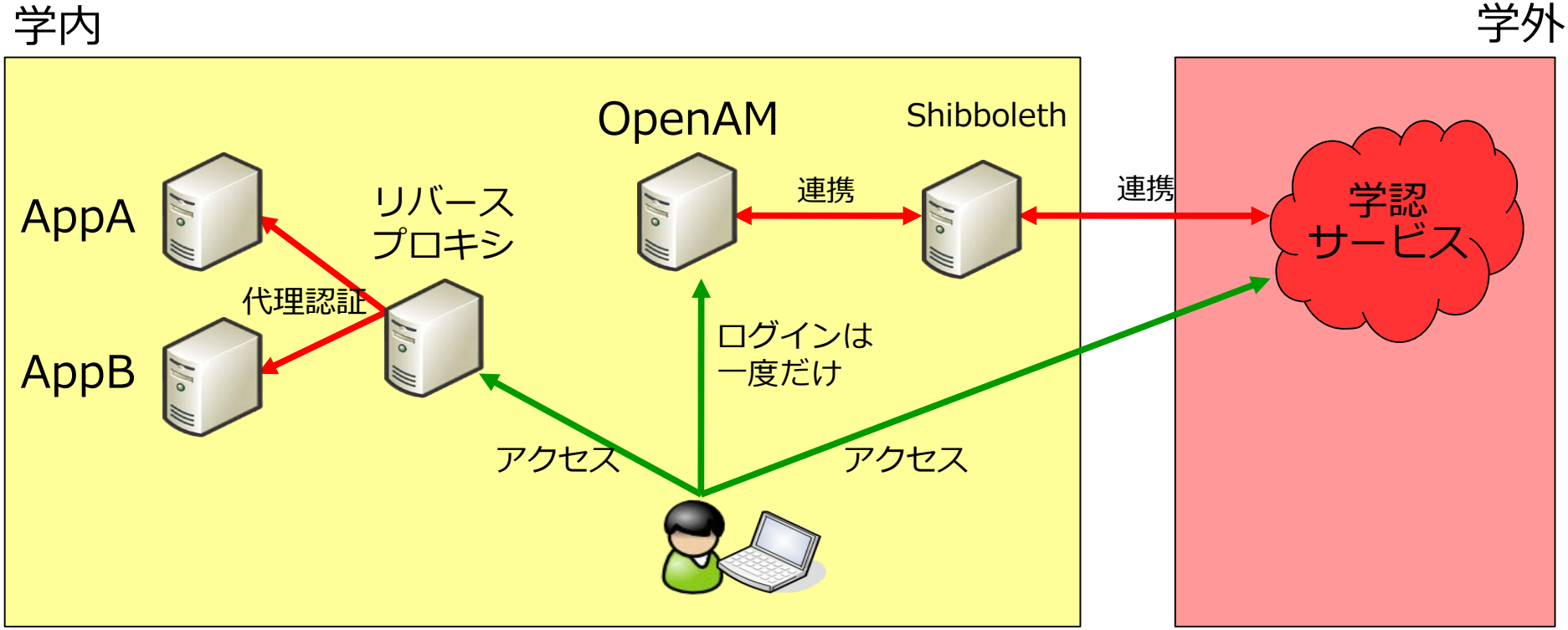
- クラウドアプリケーション
  - 認証をOpenAMへ移管することによるアクセスの一元管理
  - クラウドサービスの認証を多要素認証に



クラウド個別の多要素認証ではなくOpenAMで一元管理された多要素認証が可能

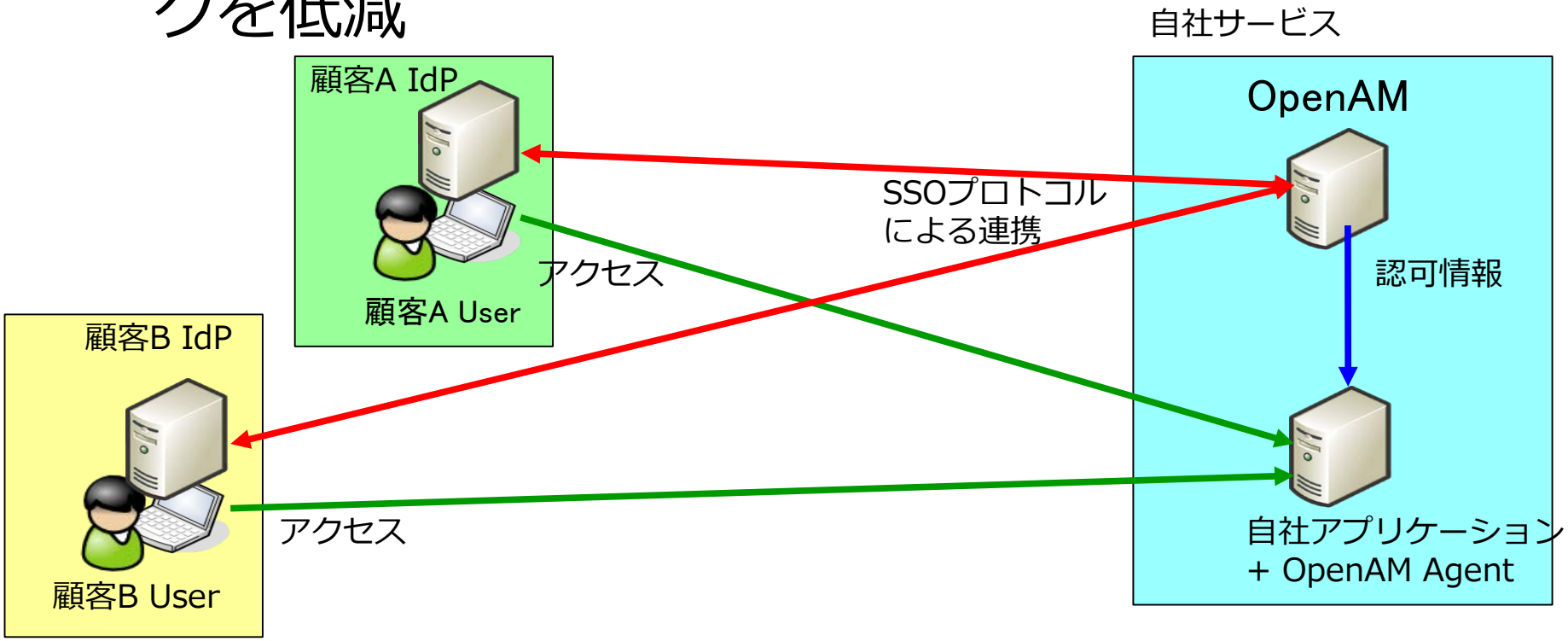
シングルサインオン構成例

- 学認連携
  - 学内アプリと学認両方へのアクセスを一元管理
  - 学内をリバースプロキシ型、学認をShibboleth連携



シングルサインオン構成例

- サービスのSSO化
  - フェデレーションプロトコルに関する部分をOpenAMへ移管し開発コスト、セキュリティリスクを低減



Unicorn ID Manager
ユニコーンIDマネージャー

製品紹介

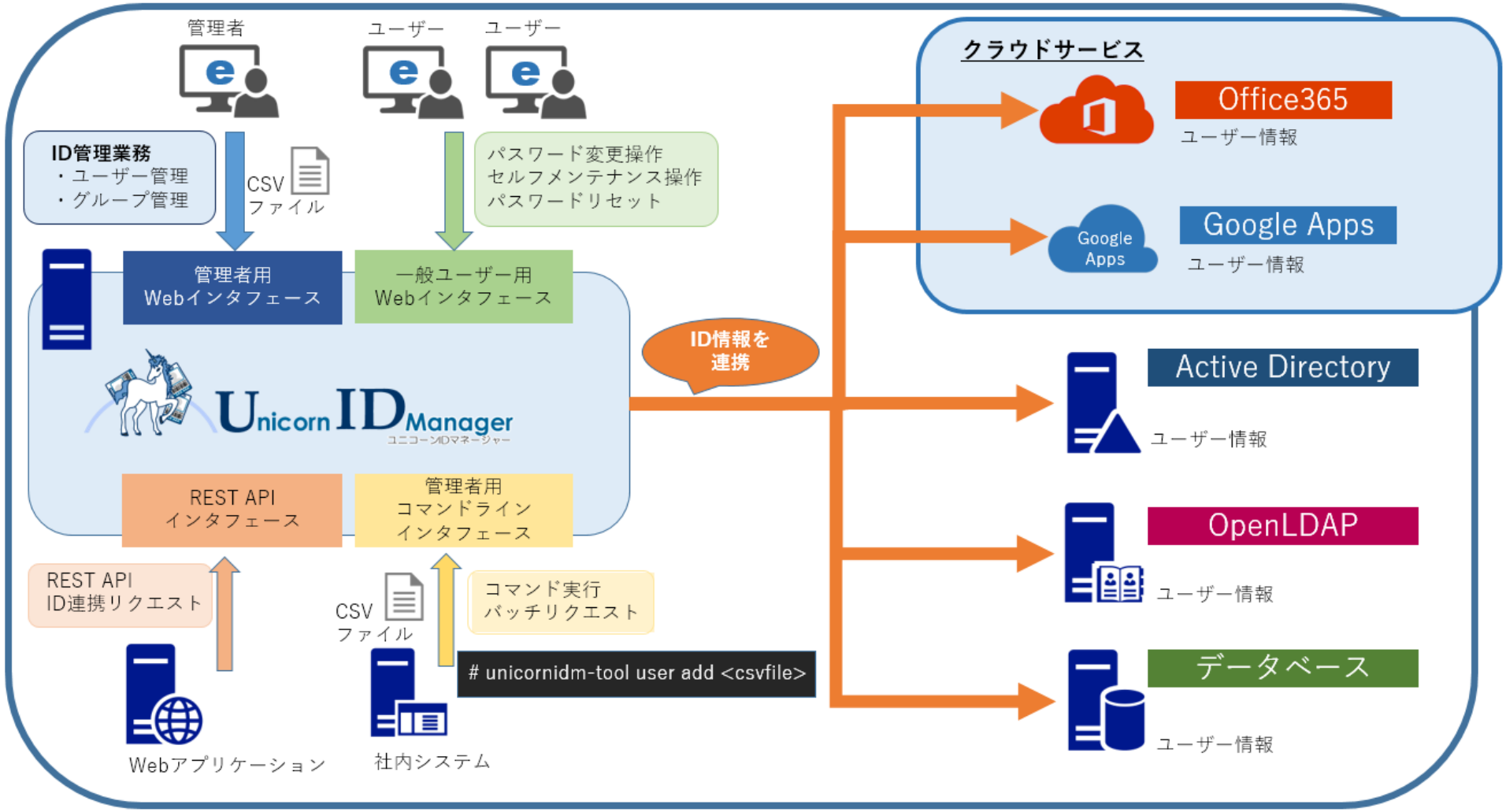
Unicorn ID Manager とは?

- ID管理 / ID連携 を 実現する製品
  - WebブラウザでID管理
  - クラウドサービス & オンプレミスのIDを対象

- 特長
  - Linux(RHEL7/CentOS7)で稼働
  - メタディレクトリを持たない

はじめてID管理製品を
導入する方へ

Unicorn ID Manager v3 概要図

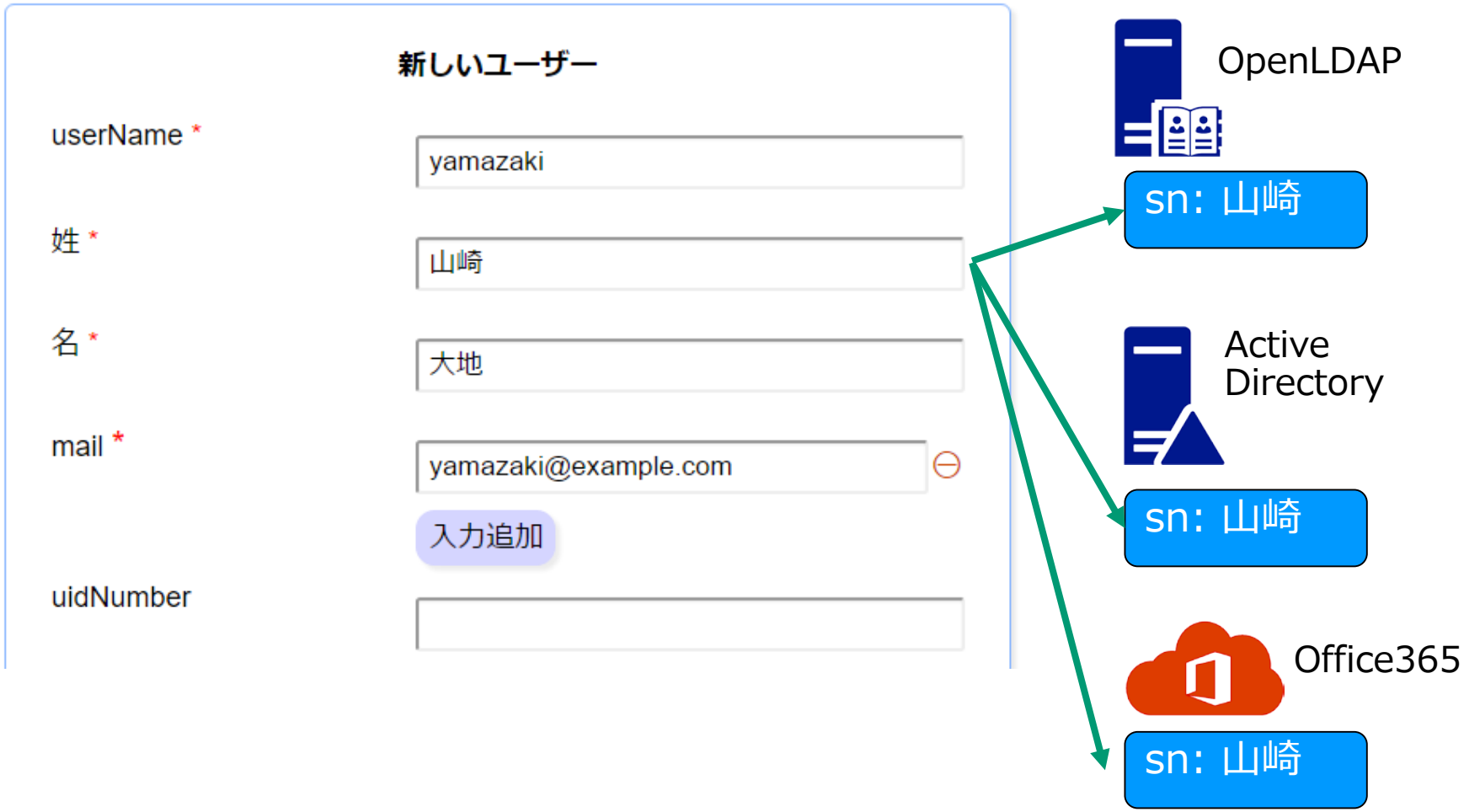


WebブラウザでID管理

パスワード変更

ターゲットと連携先

入力項目と属性マッピング



新機能

- セルフメンテナンス
- パスワードリセット

運用管理機能の拡充

- 管理者ロール機能
  - 管理者権限の委譲と制限
- 設定情報のテキストファイル化
  - 構成管理ツールによる導入・設定の自動化

```
User = {
    "objectClass": [
        "top",
        "person",
        "organizationalPerson",
        "inetOrgPerson",
        "posixAccount",
    ],
    "uid": userName,
    "cn": userName,
    "uidNumber": default(uidNumber),
    "gidNumber": default(gidNumber, 100),
    "loginShell": default(loginShell, "/bin/bash"),
    "homeDirectory": default(unixHomeDirectory, "/home/%(userName)s"),
    "sn": familyName,
    "givenName": givenName,
    "userPassword": password,
```

連携用APIの拡充

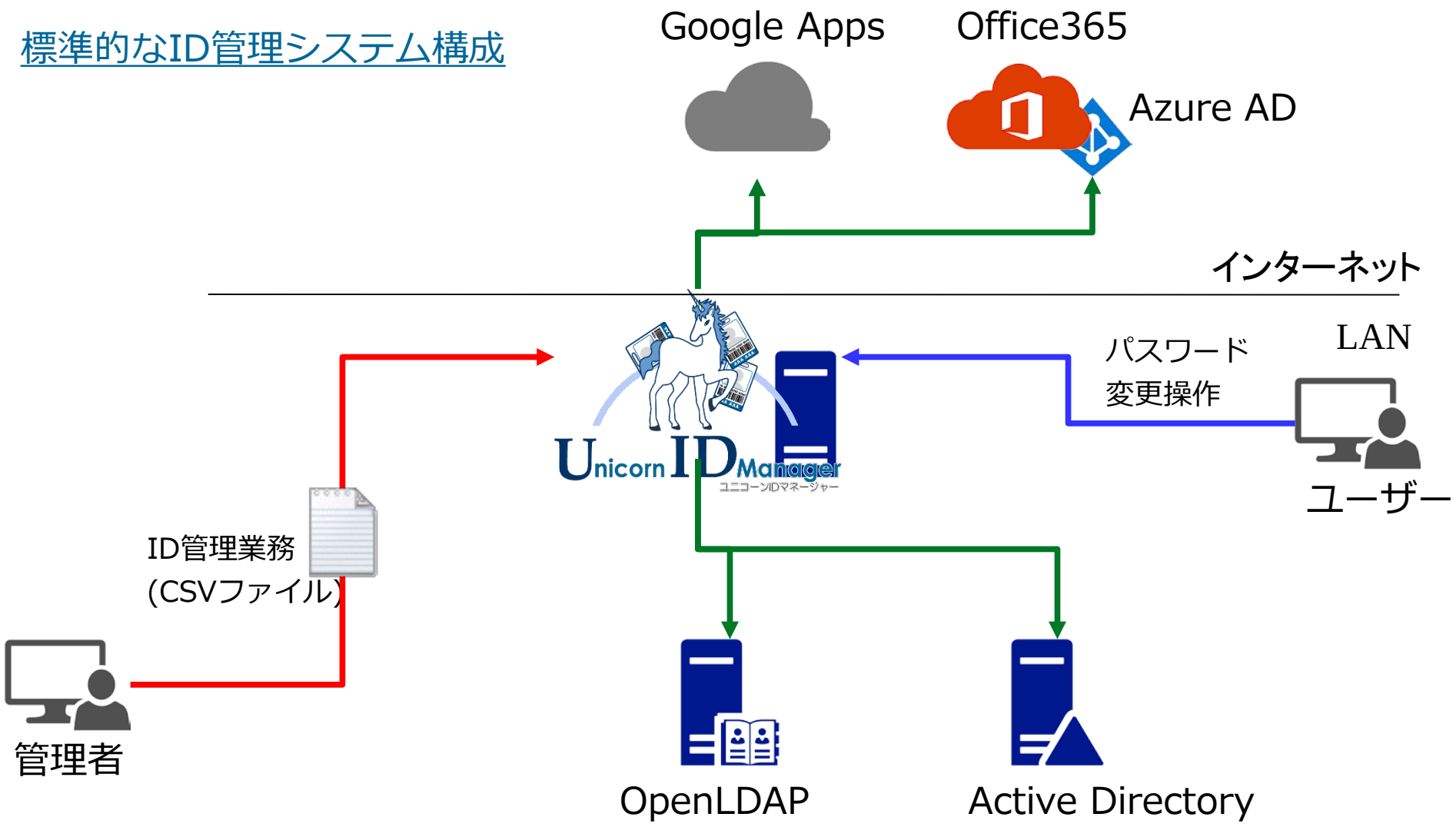
- コマンドラインインタフェース
  - Linux上でコマンドによるCSVファイル一括操作

```
# unicornidm-tool user add <csvfile>
```

- REST API(SCIM)
  - HTTP経由によるID連携操作

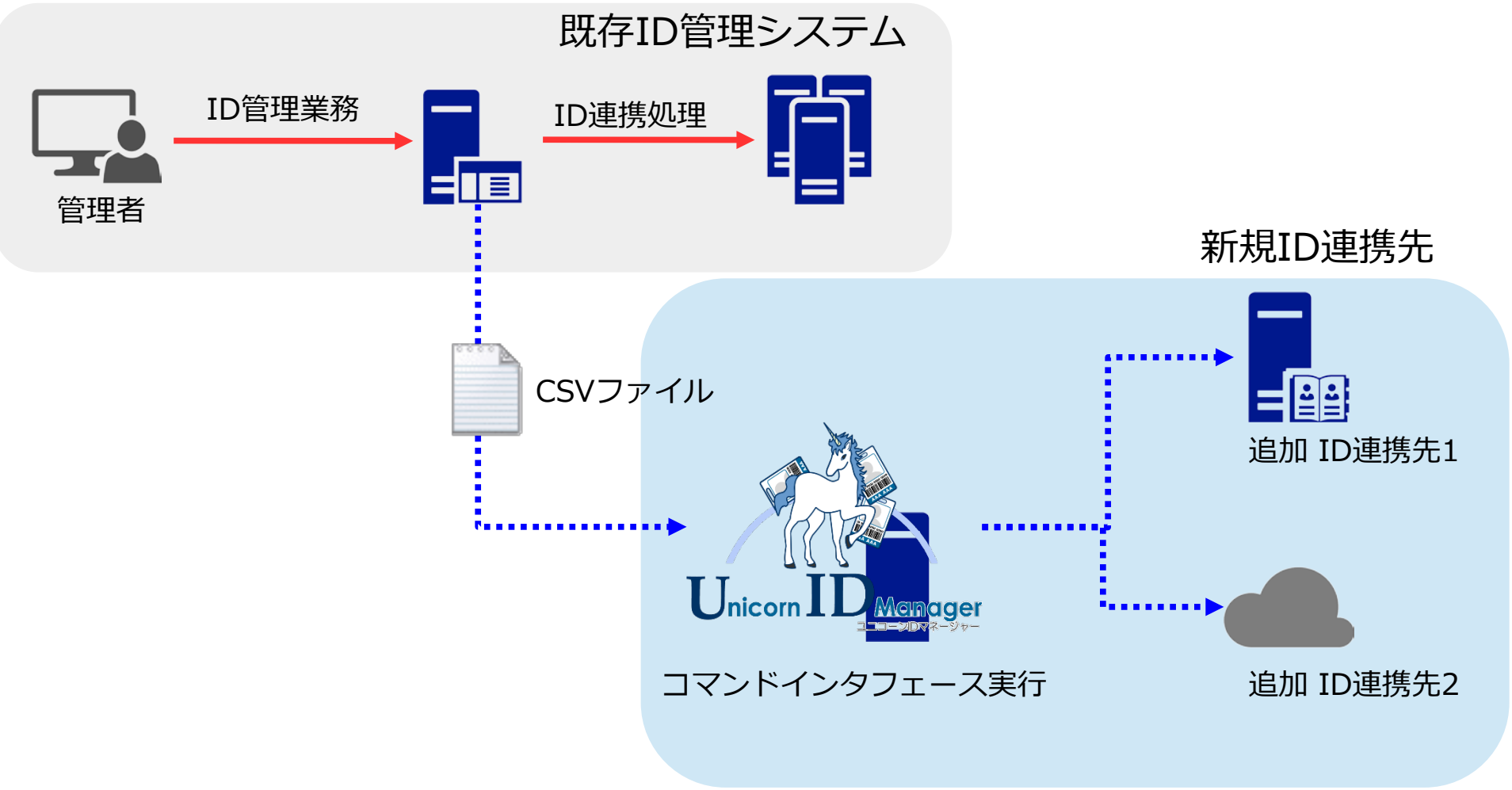
Unicorn ID Manager構成例

標準的なID管理システム構成



Unicorn ID Manager構成例2

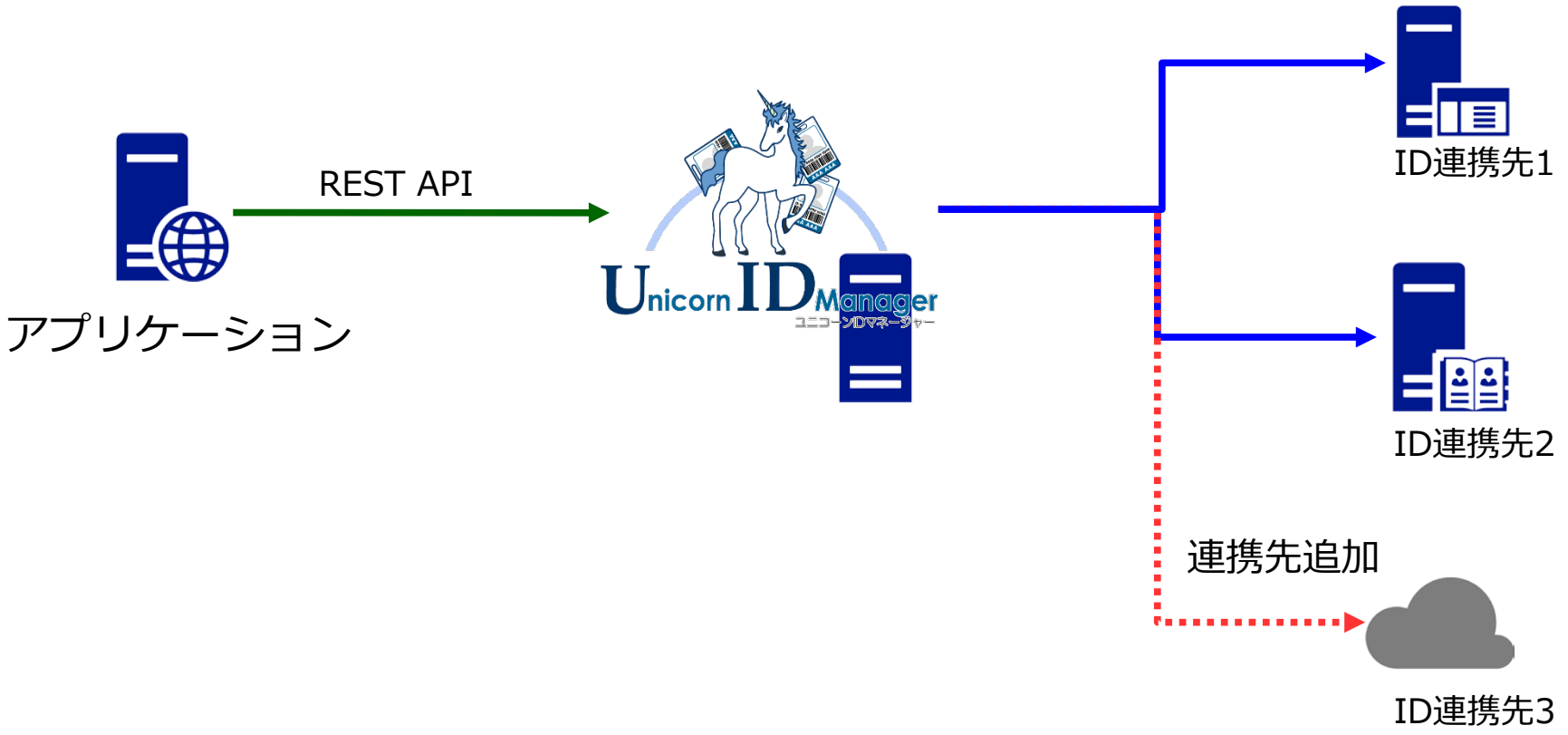
既存ID管理システムと統合



Unicorn ID Manager構成例3

ID管理APIの共通化に利用

- 連携先が追加されても同じAPIでID管理の連携が可能



Unicorn ID Manager 製品情報

- 製品情報
  http://www.osstech.co.jp/product/unicornidm/

- 管理者ドキュメント
  https://www.osstech.co.jp/download/updates/docs/unicornidm3/

- 製品価格
  - パッケージ　：60万円/1ノード
  - 年間サポート：24万円/年

「オープンソースソフトウェア」の新しい価値を創造し、高機能・高品質を追求する

統合認証 シングルサインオン アイデンティティ管理ソリューション

OSSTech オープンソース・ソリューション・テクノロジ株式会社 Open Source Solution Technology Corporation
〒141-0031 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 Mail:info@osstech.co.jp