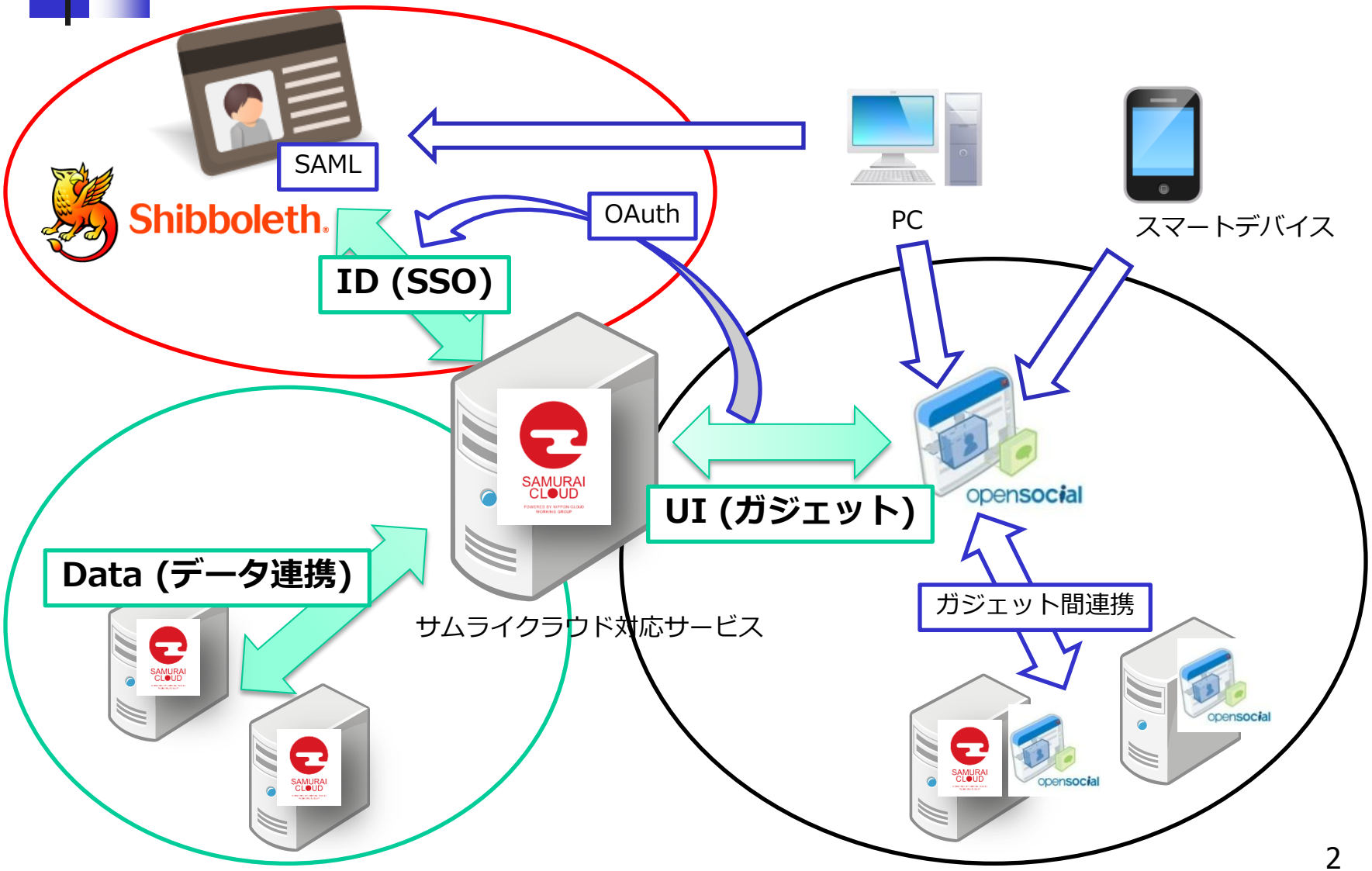
～　シングルサインオンソリューション　～

Shibbolethについて

株式会社セシオス

サムライクラウド連携図



概要（1）

- Shibbolethとは？
  - ✓ Internet2によって発足したプロジェクトで開発されました。
  - ✓ SAML、eduPerson等の標準仕様を利用した、シングルサインオンを実現するミドルウェア（オープンソースソフトウェア）です。
  - ✓ 主に欧米でShibbolethによるフェデレーションが運用、拡大されています。
  - ✓ 国内では、学術認証フェデレーションがあります。

概要（2）

➢ 学術認証フェデレーションとは？

- ✓ 国内のフェデレーションで、国立情報学研究所が中心となり運営しています。愛称は、学認（GakuNin）です。
- ✓ 組織を越えて活用する分散型学術認証基盤（Webアプリケーションへのシングルサインオン）
  - 定められた規程（ポリシー）を信頼しあうことで相互に認証連携を実現し、学術リソースを利用・提供する機関や組織から構成された連合体です。
  - 大学などの機関（IdP）がIDと個人の情報を管理し、サービス提供者（SP）がそれを利用して認可する仕組みです。
- ✓ 現在、約80のIdP/SPが運用されています。

Shibbolethの構成

- IdP（Identity Provider）

  サービス利用者側（大学など）が運用します。
  機関内（学内）にある、認証基盤（LDAP、AD、RDBなど）を利用した認証が行えます。

- SP（Service Provider）

  サービス提供側（主に企業など）が運用します。
  認証を受けた人に対して、サービスを提供します。

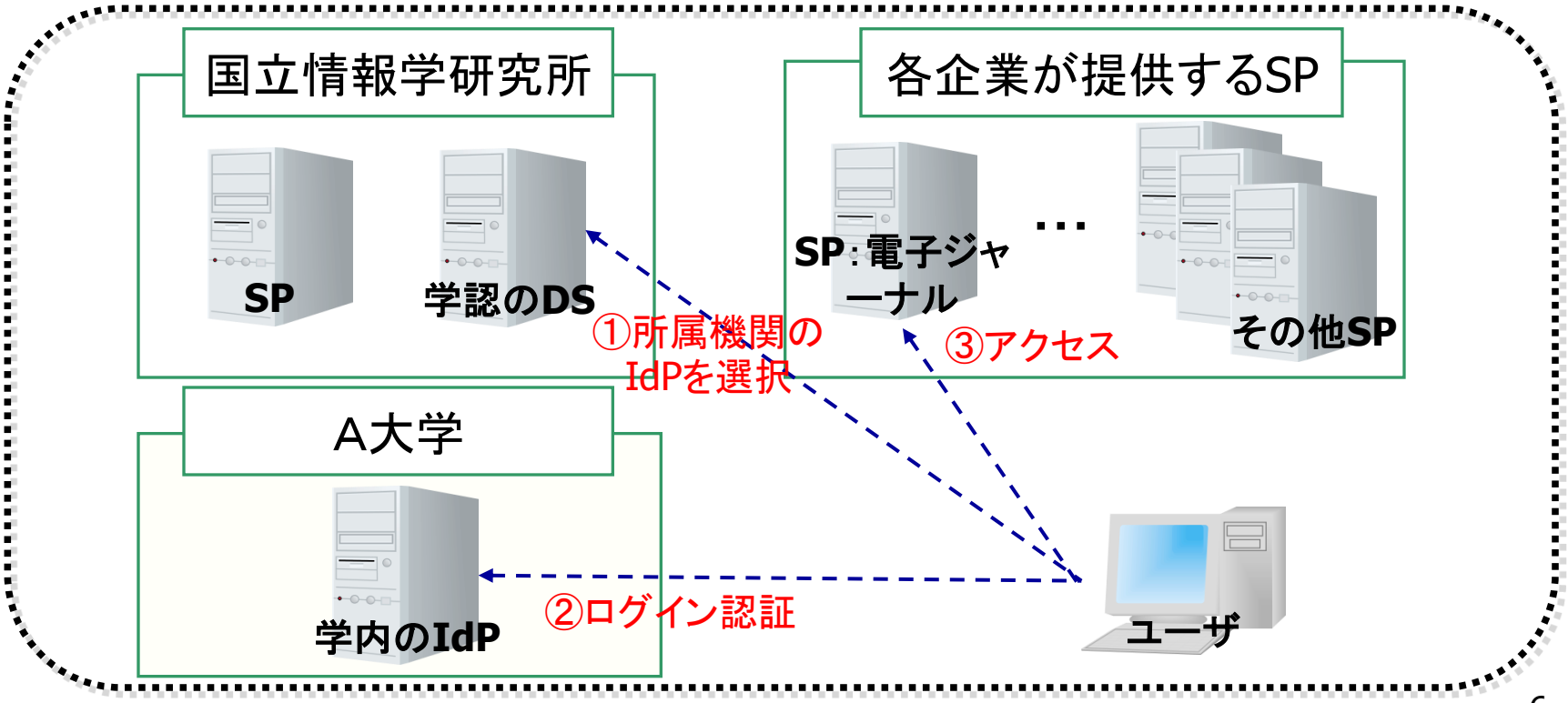
- DS（Discovery Service）

  SPへのアクセス時にIdPを検索するシステムです。
  学術認証フェデレーションでは国立情報学研究所にて管理されています。
  ※通常は、特に構築する必要がありません。

ログイン認証の流れ

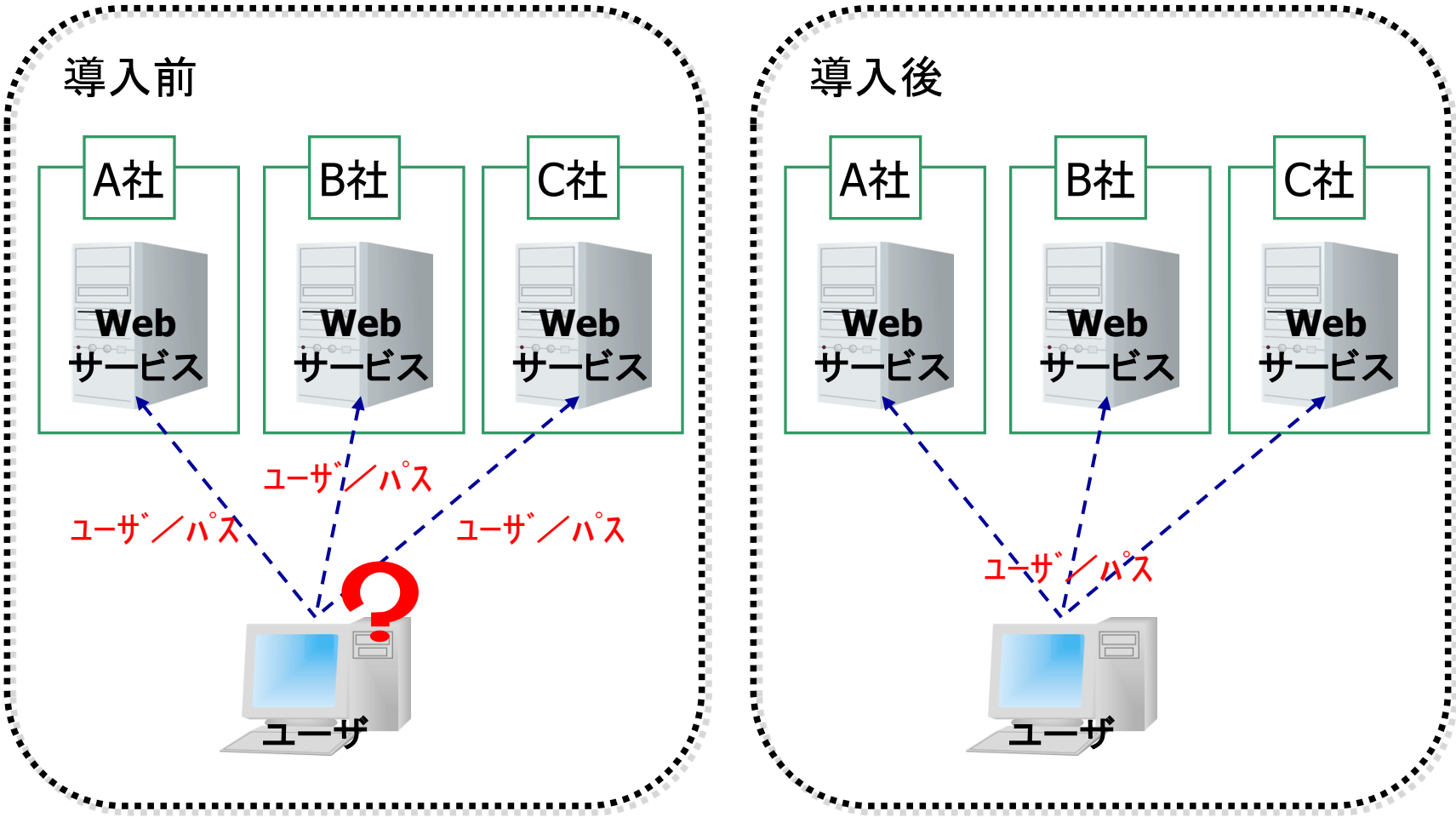
以下は、学術認証フェデレーションでサービスを使用する場合の図です。

SPへアクセスすると、①学認のDSで所属機関を選択 → ②学内のIdPでログイン認証、といった流れになります。認証後は、③Webサービス（SP）にログインされ、使用することが可能となります。



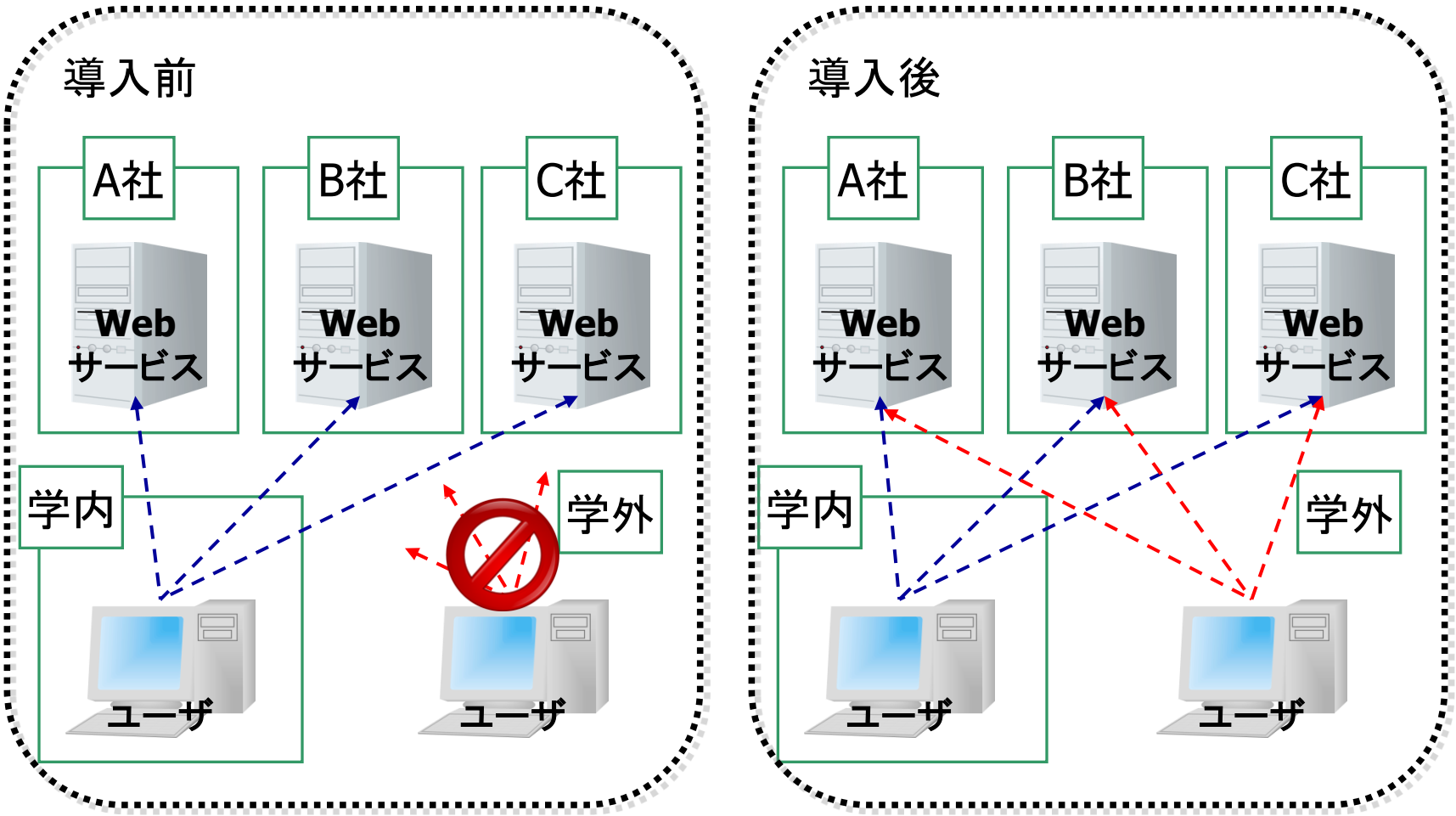
学認参加によるメリット（1）

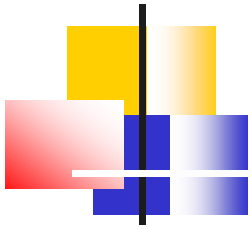
シングルサインオンでのアクセスが可能となります。



学認参加によるメリット（2）

学内からだけでなく、学外からもアクセスが可能となります。





Shibbolethの問題点

- シングルログアウトが未対応
- IdP側でのアクセス制御が行えない

学認参加SP

学術コンテンツ

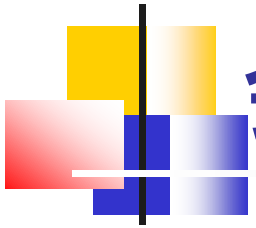
- Science Direct / SCOPUS (Elsevier)
- SpringerLink (Springer)
- Web of Knowledge / EndNote(Thomson Reuters)
- OvidSP (Ovid)
- RefWorks (ProQuest)
- Cambridge Journals Online (CUP)
- Pathology Images (Atlases)
- EBSCOhost (EBSCO)
- KOD (研究社)
- CiNii (NII)
- IEEE Xplore (IEEE)
- 360 Search, 360 Link, ElectronicJournal Portal(Serials Solutions)
- IMCデータリポジトリ（金沢大学）

開発環境

- DreamSpark (Microsoft)

ネットワークサービス

- Fshare（大容量ファイル交換）サービス（NII）
- FaMCUs (テレビ会議多地点接続)サービス(NII)
- Eduroam-Shib（eduroam用一時アカウント発行）サービス（京大&NII）
- SecurityLearningシステム(e-Learning)（NII）
- WebELS eLearningシステム(e-Learning)（NII）
- edubase Cloud(クラウドサービス)（NII）
- Foodle(予定調整サービス) (UNINETT)
- ゲスト用ネットワークアクセス認証（佐賀大学、広島大学）
- ファイル送信サービス（金沢大学）
- 科学技術の学術情報共有のための双方向コミュニケーションサービス（山形大学）



会社紹介

会社名： 株式会社セシオス

設立： 2007年5月

資本金: 1300万円

事業内容:

コンサル

OpenLDAP、Shibbolethの設計・導入

OSSによるシングルサインオン・統合ID管理の導入

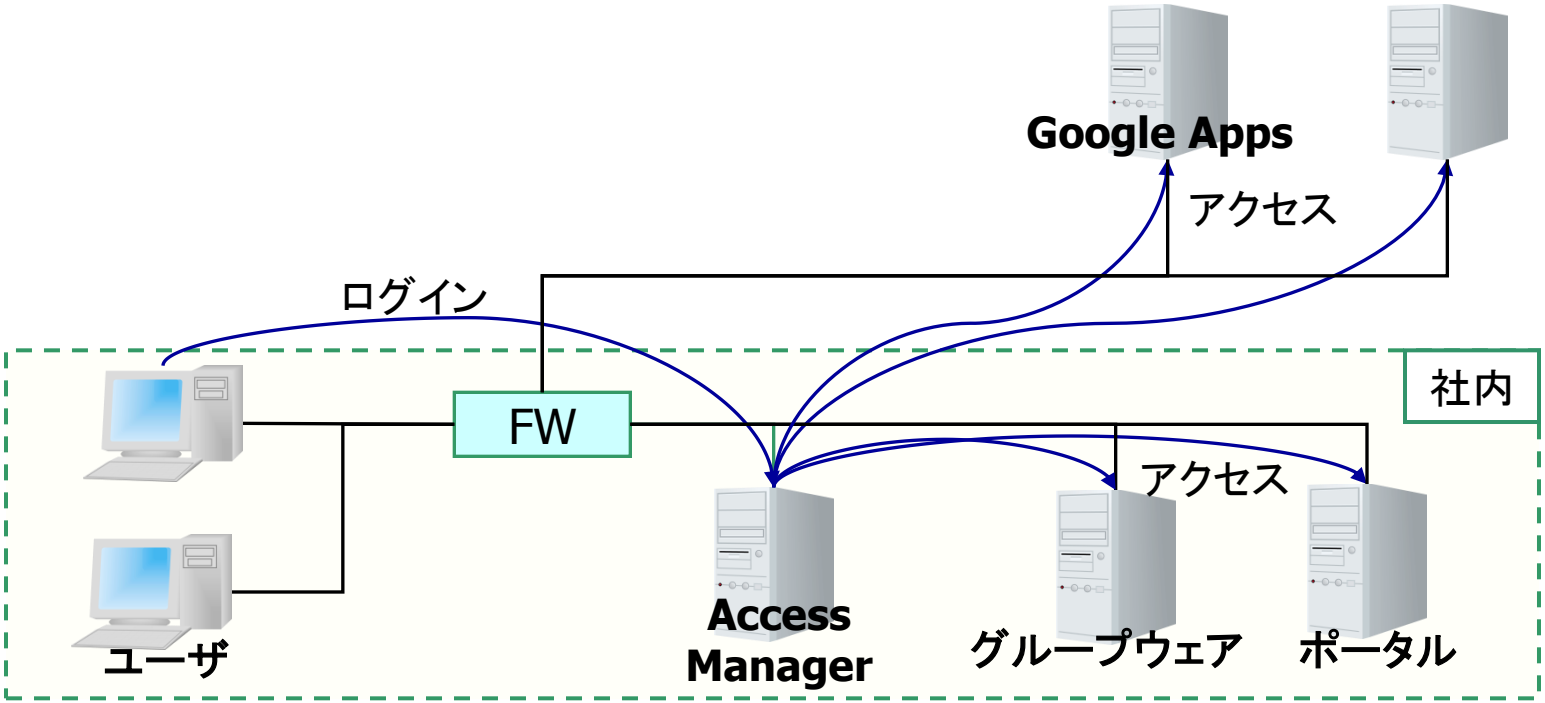
ソリューション販売

シングルサインオン・統合ID管理ソリューションの販売・サポート

シングルサインオンソリューション（1）

オンプレミス型のシングルサインオンサービス
（Secioss Access Manager）

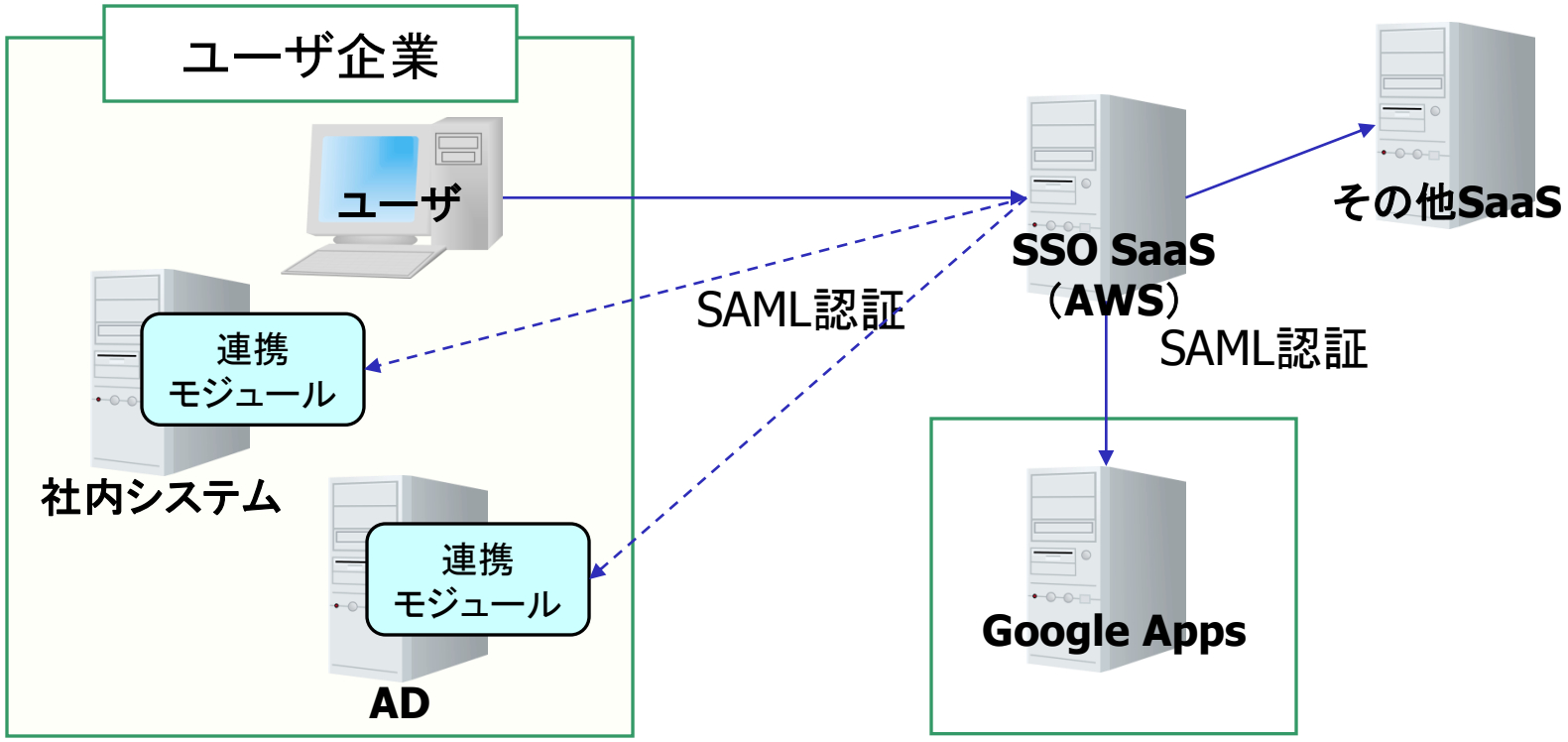
●社内のWebアプリケーションから社外のSaaSまで統合的なシングルサインオンが可能です。



シングルサインオンソリューション（2）

SaaS型のシングルサインオンサービス
（SeciossLink）

●「Secioss Access Manager」がベースとなっています。



Secioss Access Managerの機能について

項目	対応機能
シングルサインオン方式	リバースプロキシ エージェント OpenID SAML 代理認証
認証方式	ID/パスワード 統合Windows認証 証明書認証 端末認証（スマホ/PC） ワンタイムパスワード認証
アクセス制御	ユーザ グループ ネットワーク 時間帯 認証方式