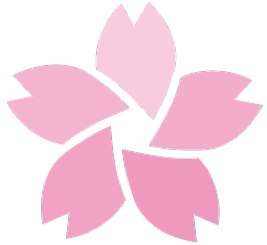
クラウド時代の
シングル・サイン・オン



OSS Consortium

OSSTech

オープンソース・ソリューション・テクノロジ株式会社
小田切耕司、岩片靖

2009/06/02

お問い合わせ info@osstech.co.jp

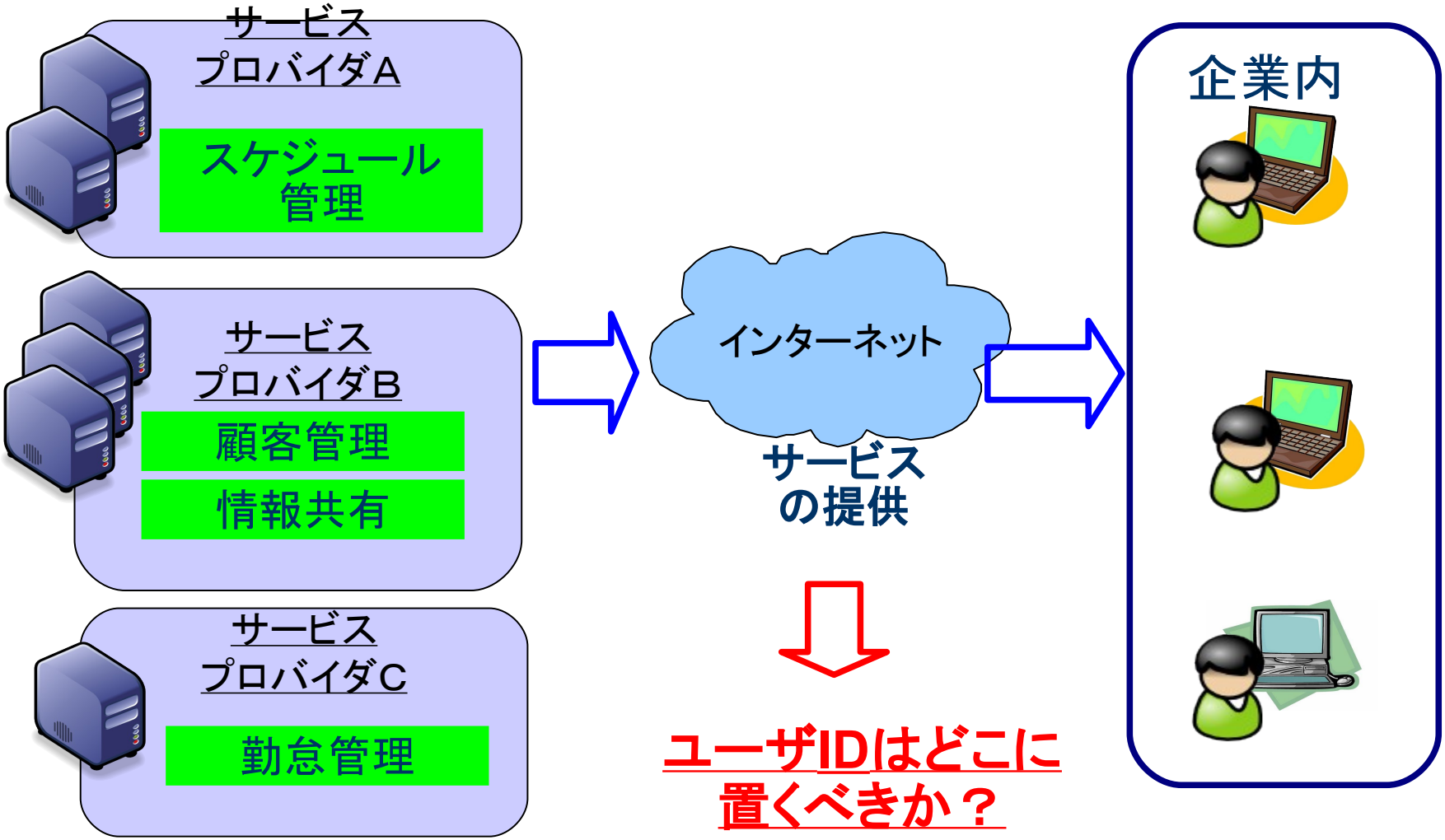
目次

- クラウド・コンピューティングと認証
  - 認証は誰がどこで行うべきか？
- OpenIDとSAML
  - それぞれの特徴
  - OSSでOpenID, SAMLを実現する
- OpenSSO： デモ
  - 連携するアプリの紹介
  - デモで使う組織の構造

クラウド・コンピューティング

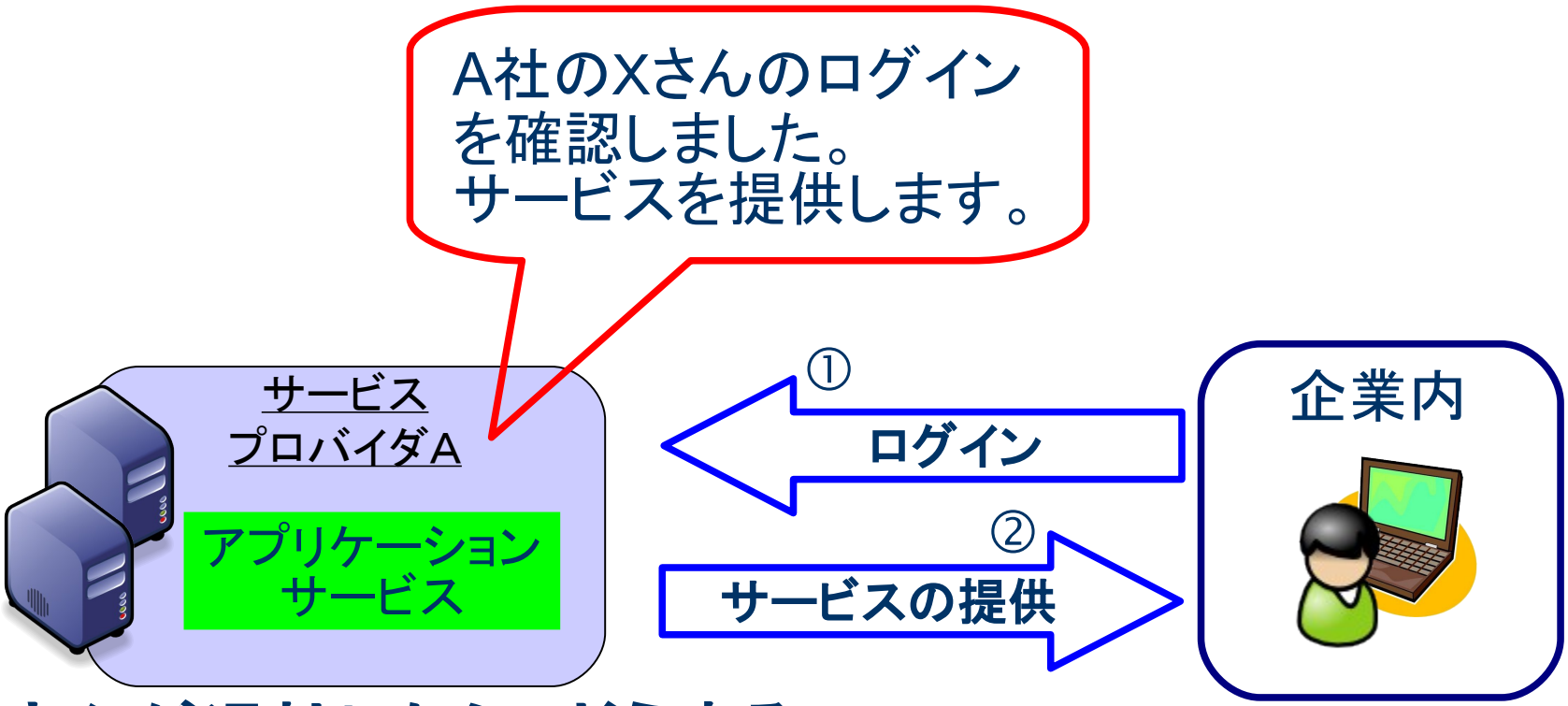
- コンピューティング（コンピュータ処理）を会社や個人が所有するコンピュータでなく、クラウド（社外のインターネット）上で行う
- 様々なコンピュータ処理がインターネット上で処理される
- 個人のデータがインターネット上におかれる
  - mixi, yahoo, Facebook, Blog
- 会社のデータがインターネット上におかれる
  - Google Apps, SalesForceなど
- ユーザ情報やパスワードもクラウド上に置くのか？
  - **クラウド上に共通なIDを置く → OpenID**
  - **社内にIDを置いてクラウド利用を社内から制御 → SAML**

クラウド・コンピューティング



企業内ユーザの認証

従来のイントラネットでは. . .

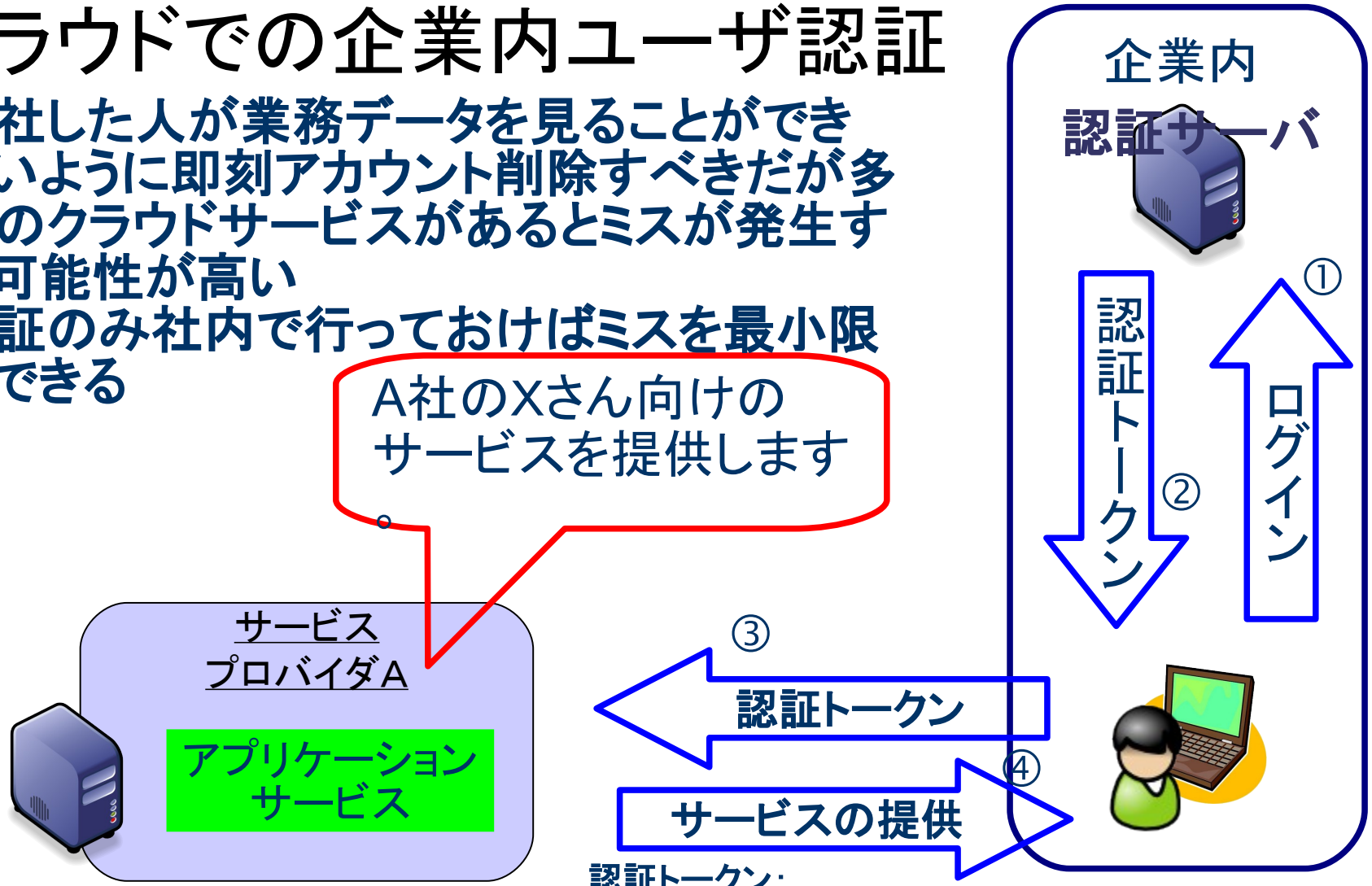


Xさんが退社したら、どうする？

イントラネットでは社内に入れないのであまり心配ないが、クラウドでは社外から会社のデータにアクセスできてしまう

クラウドでの企業内ユーザ認証

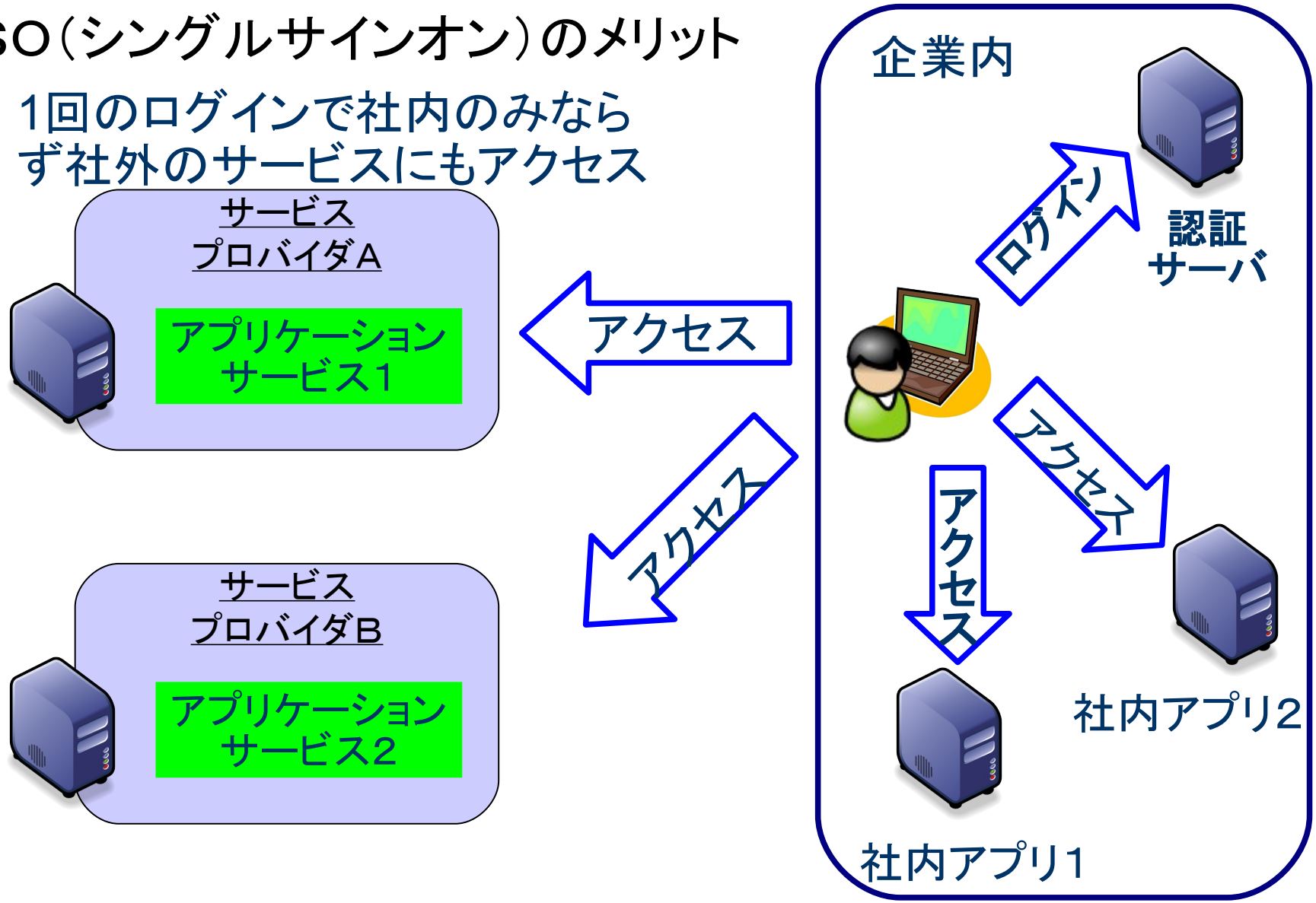
退社した人が業務データを見ることができないように即刻アカウント削除すべきだが多数のクラウドサービスがあるとミスが発生する可能性が高い
認証のみ社内で行っておけばミスを最小限にできる



認証トークン:
ユーザが認証済みであることを示す小さなデータ。Cookieが使われることが多い。

SSO（シングルサインオン）のメリット

1回のログインで社内のみならず社外のサービスにもアクセス

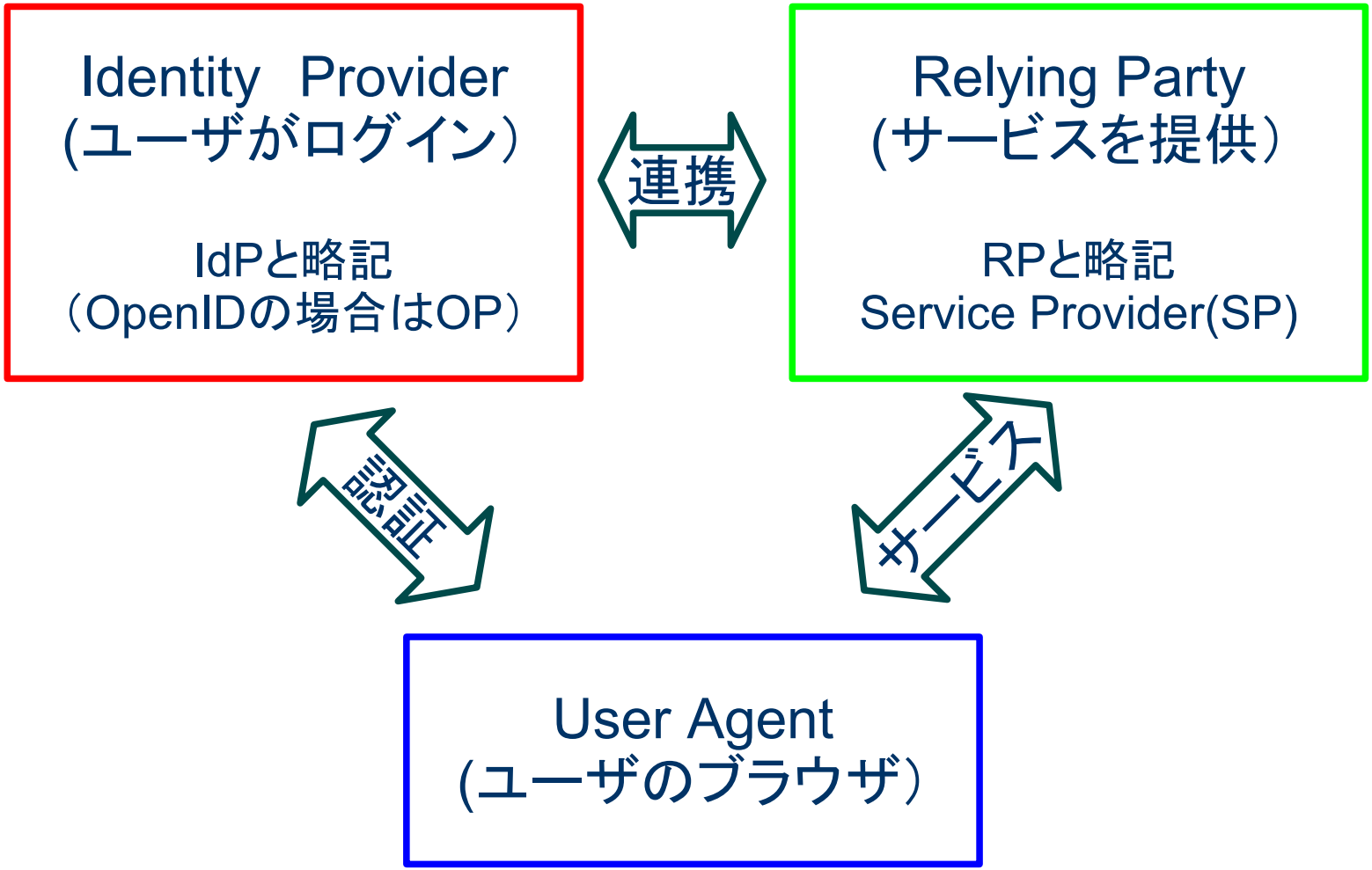


クラウドを使うにはSSOは必須となっていく

- 企業側のメリット
  - パスワードや個人情報を外に出す必要がなくなる
  - 「入り口」を一箇所にすることにより監視が容易になる
  - 退職社員は1カ所で削除すればすべての業務が利用不可とできる
- ユーザ（社員）のメリット
  - IDやパスワードを多数覚えなくてもすむ
  - 社内だけでなく社外のシステムにもシームレスにアクセス可能になる

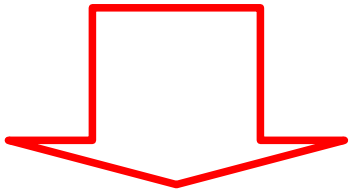
企業ユーザの認証は各企業で行う、そして**連携**させる

認証連携



クラウドでの認証

コンシューマー向けサービスでは
サービス提供側で、企業ユーザの
認証は各企業が行う方向に進む



各企業がIdPの機能を持つ

実際にはどうするか？

SAMLとOpenIDとは？

- SAMLとは
  - Security Assertion Markup Language
  - 標準化団体OASISによって策定された、認証や認可の情報を安全に交換するためのXML仕様。
  - AuthXMLとS2MLを統合して標準化したもの。
  - 認証情報の交換方法はSAMLプロトコルとしてまとめられており、メッセージの送受信にはSOAP/HTTPが使われる。
- オープンID 【OpenID】とは
  - 様々なWebサイトで共通のID情報を利用できる認証方式の一つ。また、そのID情報自体のこと。
  - オープンIDに対応しているサイトでは自分の持つオープンIDでログインして会員向けサービスなどを利用できる。

クラウドでの代表的なSSOプロトコル

OpenID と SAMLの比較

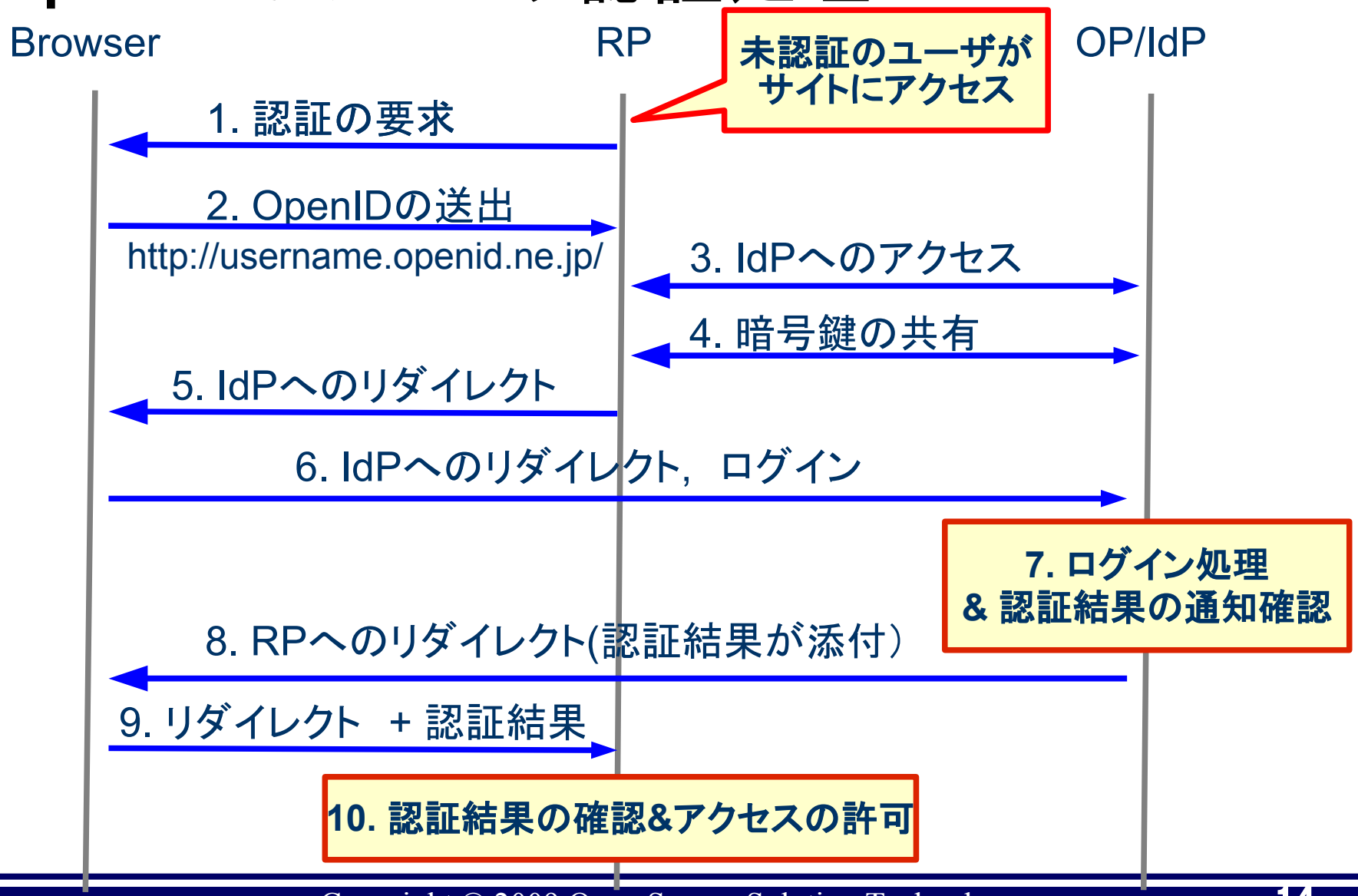
プロトコル	使用するID	IdP(OP)の選択	RPの動作
OpenID	IDとしてURLを使用する	ユーザが選択	ユーザが選択したIdPと協調して認証処理を行わなければならない
SAML (Browser SSO Profile)	IdPとRP間でIDを交換することはない (pseudonymを使用)	管理者が予めIdPとRPの間の信頼関係を結んでおく(Circle of Trust)	信頼関係がないIdPとRPは連携しない

OpenIDとSAMLの特徴

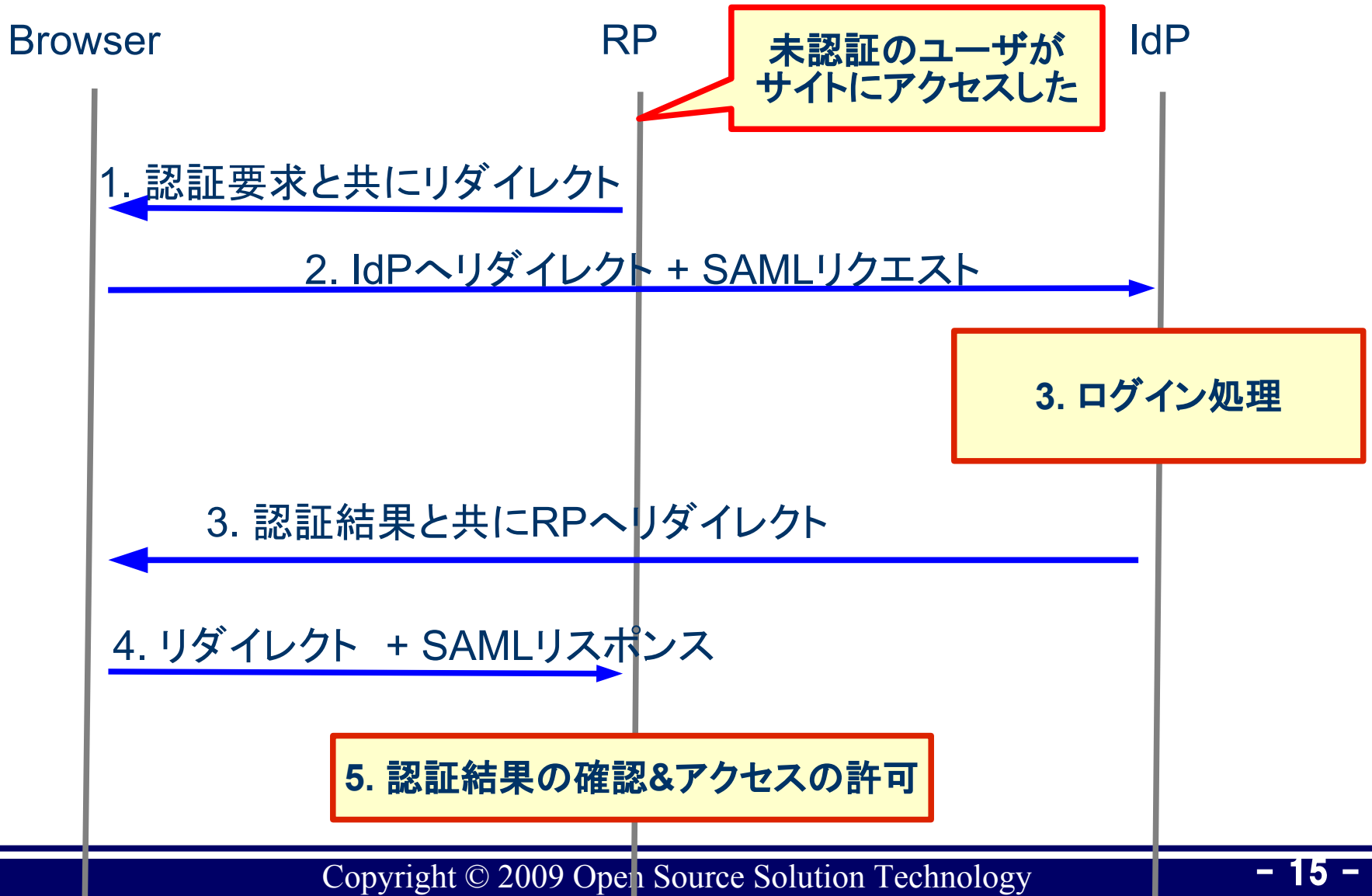
- OpenID
  - IDはクラウドに置く
  - ユーザの視点
  - 開放指向
- SAML (Browser Post Profile)
  - IDは企業内に置く
  - IdPの視点
  - 管理指向



OpenIDでのユーザ認証処理



SAMLでのユーザ認証処理



OpenID, SAMLをOSSで実現しよう！

多数のシステム、多数の連携先

⇩

多くのプロトコルに対応した認証サーバを導入

⇩

すべてオープンソースで実現できれば
低コスト、高機能なものができる

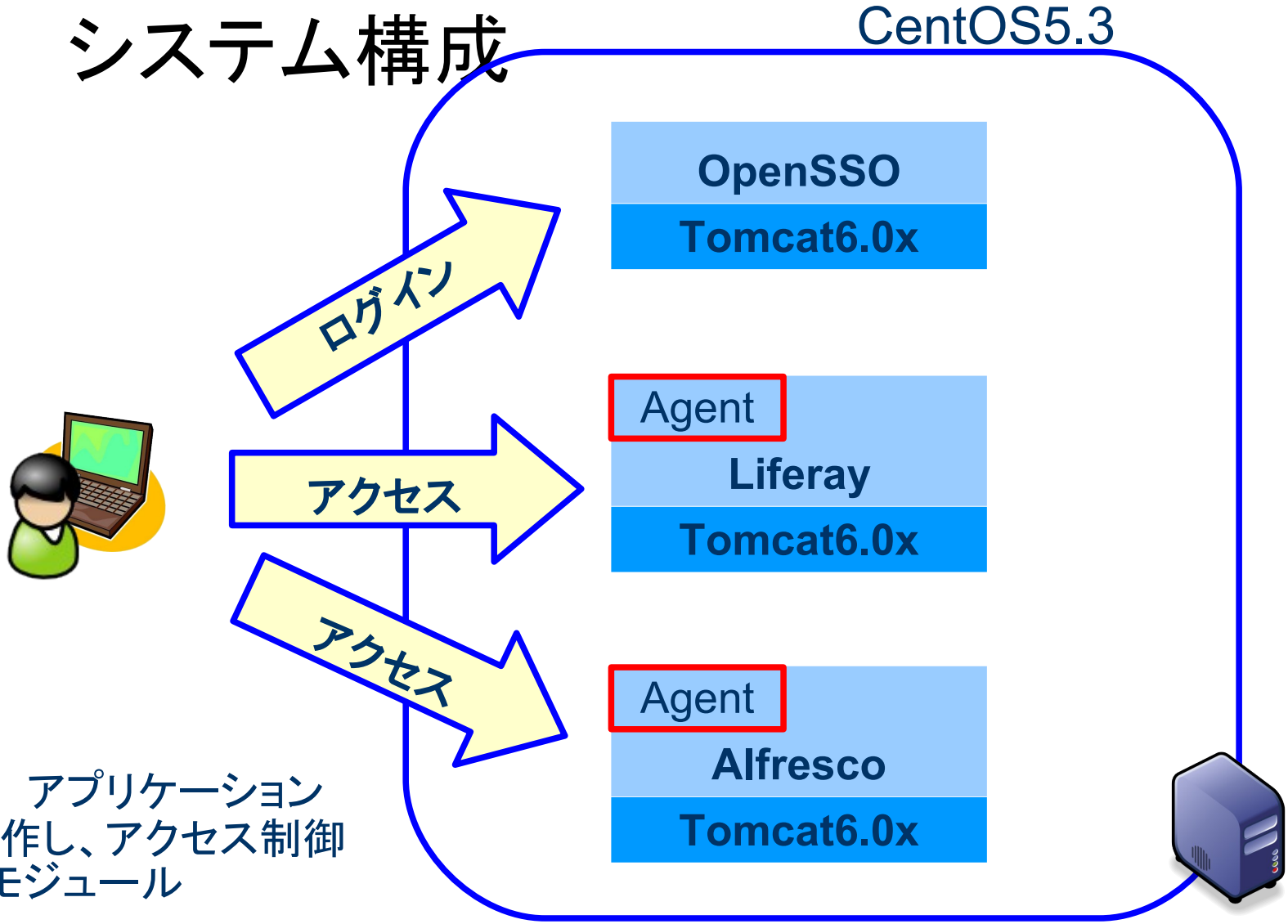
⇩

Multi-Protocol HubとしてのOpenSSO

デモで使用するS/W（すべてOSS）

- **CentOS 5.3（Apache 2.2 , Tomcat 6）**
- **OpenSSO 8.0**
  - Sun Microsystem社により開発されたOSSのSSOソフト
  - AgentおよびReverse Proxy方式,OpenID,SAMLによるSSOを提供
- **OpenLDAP**
  - ユーザIDを入れるための格納場所
  - OpenSSO向けの拡張スキーマをOSSTechで用意
- **Liferay**
  - オープンソースのEIP（企業向け情報ポータル）用ソフトウェア
  - OpenSSO向けのAgentモジュールが標準で付属
- **Alfresco**
  - オープンソースのECM(企業向けコンテンツ管理）用ソフトウェア
  - OpenSSO向けのAgentをOSSTechで開発

デモ： システム構成



Agent: アプリケーション上で動作し、アクセス制御を行うモジュール

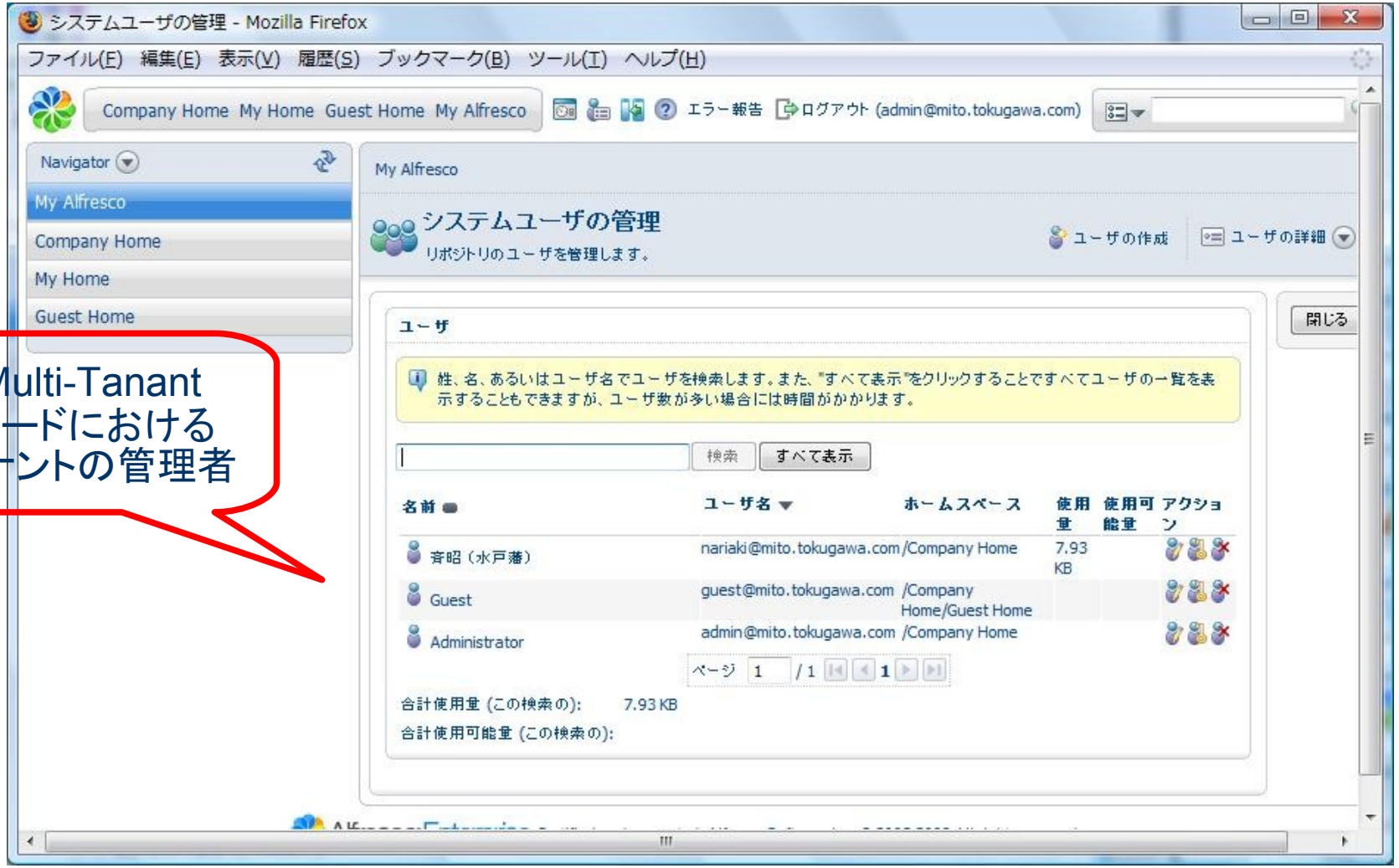
デモで使う組織構造

- 徳川御三家
  - 尾張藩
    - 徳川宗春
  - 紀州藩
    - 徳川吉宗
  - 水戸藩
    - 徳川斉昭

OpenSSO 管理コンソール

Liferay 管理コンソール

Alfresco: 管理コンソール



本日のまとめ

- 企業利用では認証を外部に任せるのはやめましょう。
  社内にIdPの機能を持ちましょう。
- OpenIDとSAML(browser sso profile)は認証連携を目的にしたプロトコルですが重視する点が異なっています。
- 様々なプロトコルに対応したOpenSSOを利用してMulti-Protocol Hubを構成するという方法もあります。
- OpenSSOは様々なアプリケーションにも対応しているため社内システムのSSO化にも効果があります。
- クラウド対応OSSアプリケーションの標準になりつつある

付録.
オープンソース・ソリューション・テクノロジ
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/FreeBSDなどへも対応！
- **Samba,OpenLDAP,OpenSSOなどによる認証統合/シングル・サイン・オン 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
- **Sun Java Directory Server, Windows Active Directory, CLUSTERPROなどの商用ソフトのソリューションも提供**
  - 商用製品とOSSの柔軟な組み合わせに対応

OSSTech製品紹介（すべてOSSで提供）

- Samba 3.0/3.2 for Solaris / Linux
  - Windows認証サーバー／ファイルサーバー
  - 独自の不具合修正と改良(Solaris ZFS,SunJDS対応）
- OpenLDAP 2.3/2.4 for Solaris / Linux
  - 認証統合／SSOのための必須ソフト
  - 独自の不具合修正と改良(OpenSSO対応）
- LDAP Account Manager
  - LDAPやSambaのWebベース管理ツール
- SSLBridge：インターネット経由でファイルサーバーへアクセス
- OpenSSO：クラウド時代のSSO
- Chimera Search：Windowsアクセス権対応 全文検索システム