クラウド時代の
SSO(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
2009/11/20
岩片　靖

目次

- 認証と連携
- OpenSSOのご紹介
- デモその1
  - SAMLによる認証連携
  - エージェントによるアクセス制御
- デモその2
  - Windowsドメイン認証との連携
  - リバースプロキシ方式によるアクセス制御

講師紹介

- 岩片　靖（IWAKATA　Yasushi）
  - 1984年～　米国の大学にて数学の研究および教育に従事
  - 1990年～　日本の電機メーカーにて暗号ライブラリ等の開発
  - 1997年～　日本ネットスケープコミュニケーションズ勤務
  - 1999年～　iPlanet(Sun-Netscape Alliance)参加
  - 2001年～　サン・マイクロシステムズ勤務
  - 2008年～　オープンソース・ソリューション・テクノロジ勤務
- オハイオ州立大学　Ph.D.（専攻：組合せ論）
- 認証関連の様々な実証実験に参加
  - オンライン・バンキング、銀行間取引、クレジットカード決済
  - 学校間認証連携
- 日本、オーストラリア、韓国において大規模システムの設計、実装、問題解決を担当

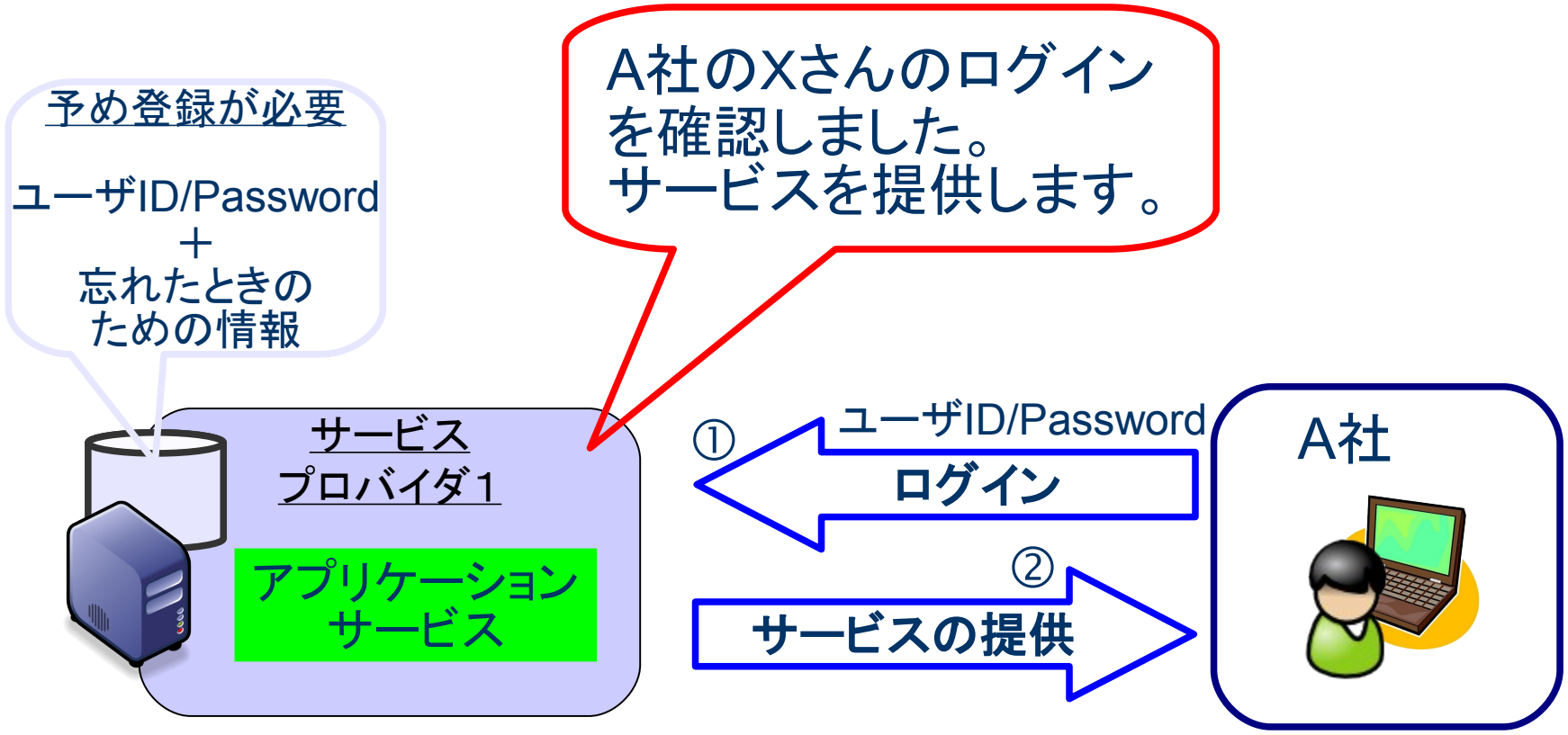
認証と連携

あなたの会社の従業員を

認証するのは誰ですか？

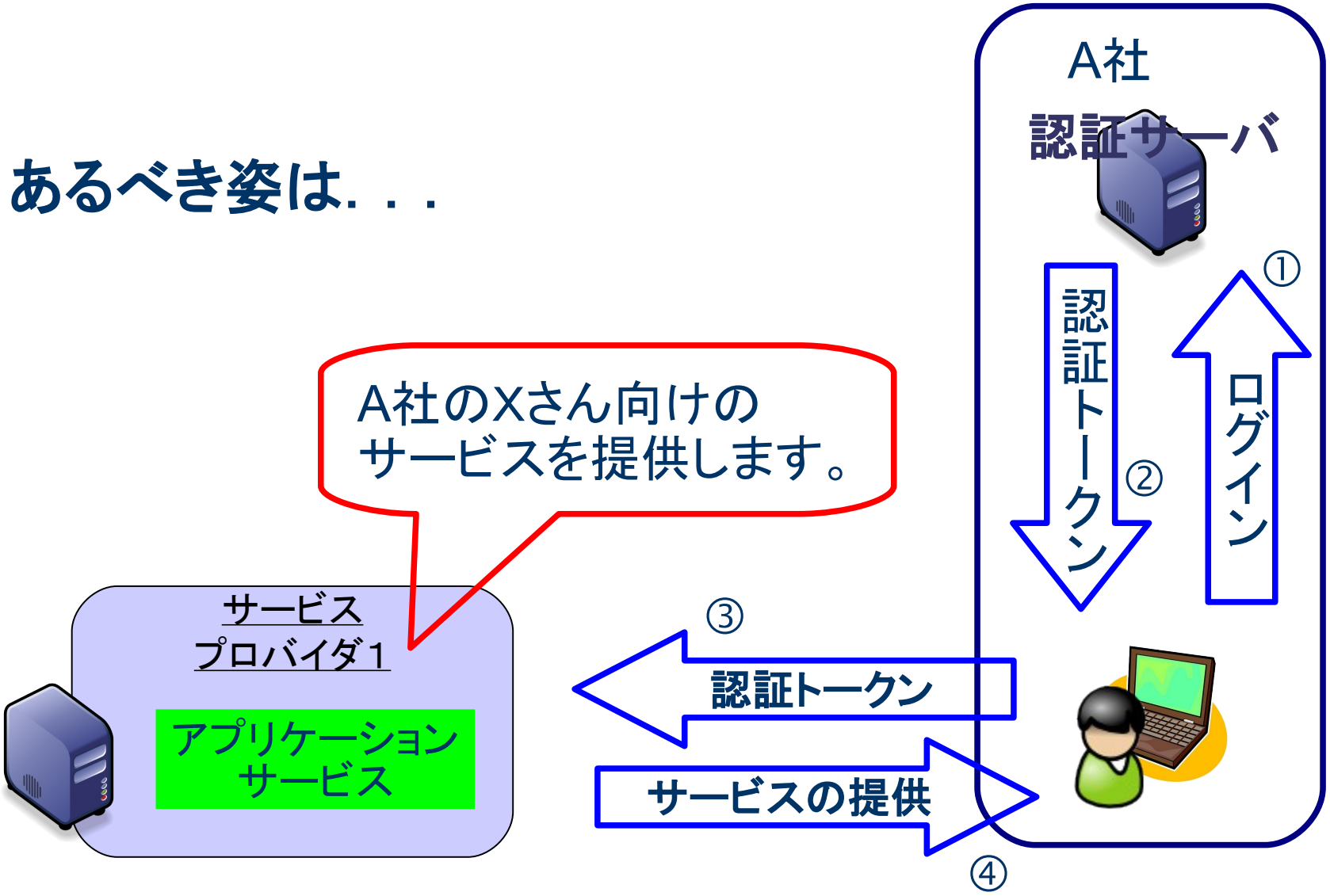
企業ユーザの認証

現状では. . .



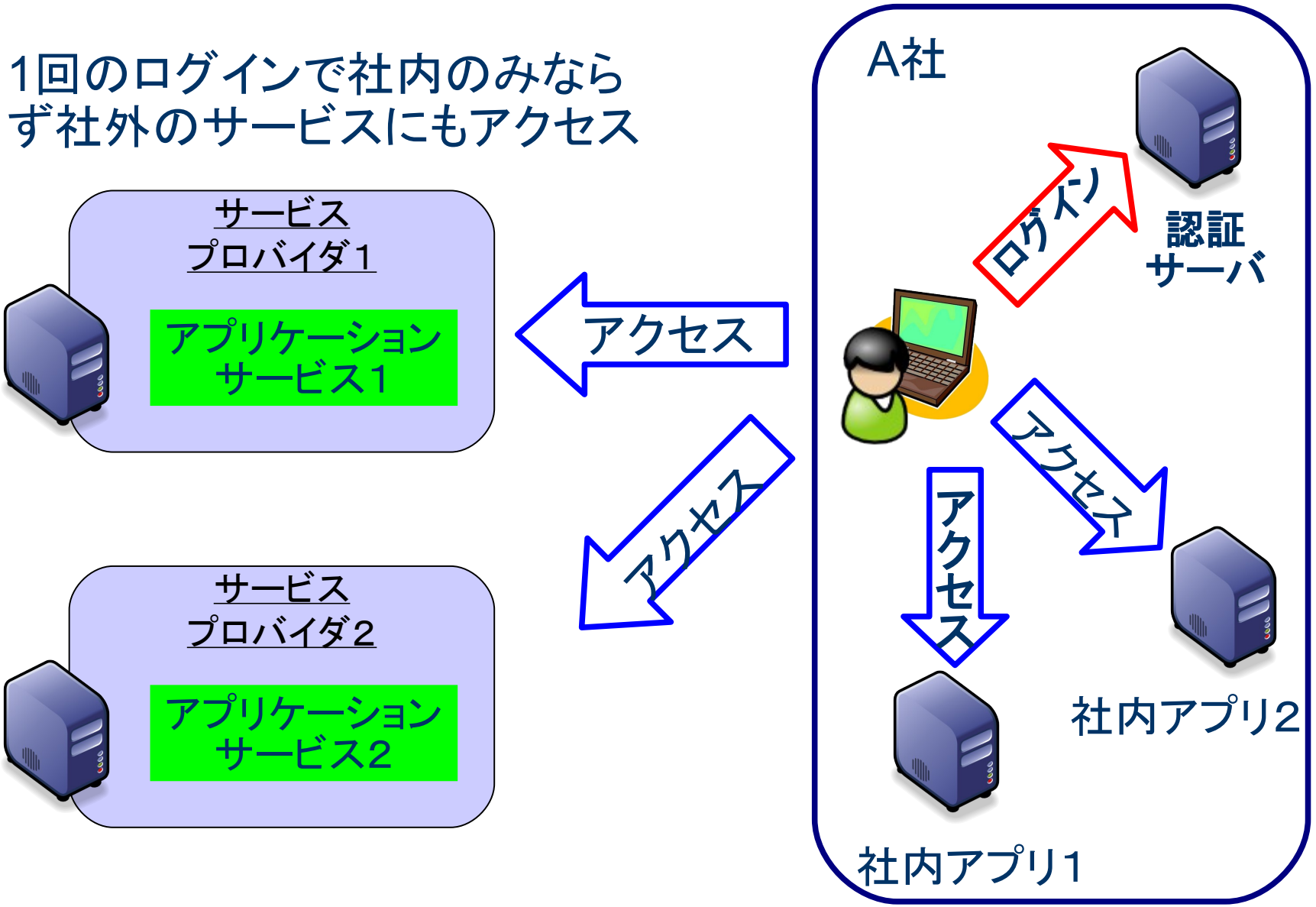
企業ユーザの認証

あるべき姿は. . .



さらなるメリット： SSO

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



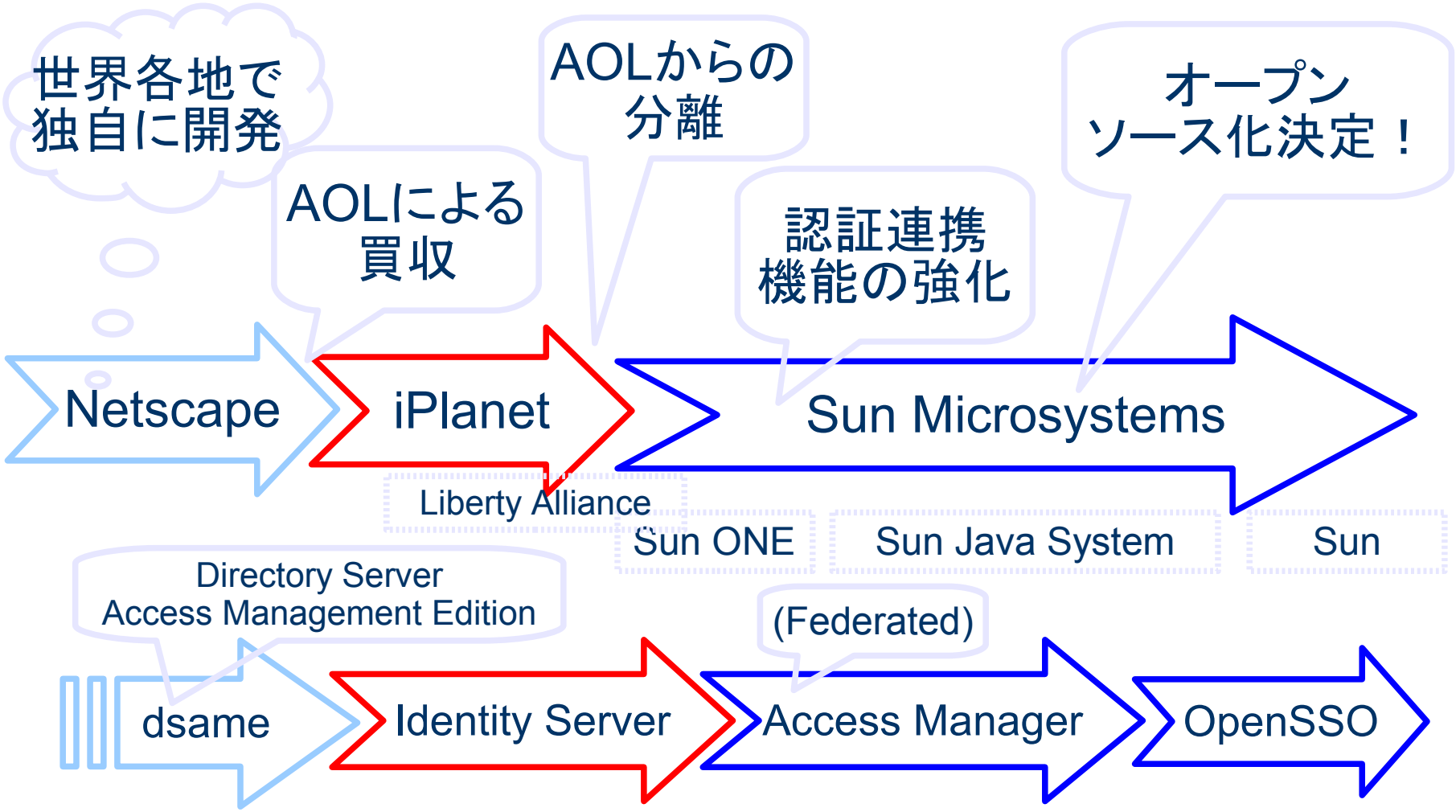
ここまでのまとめ

- 企業側のメリット
  - パスワードや個人情報を社外に出さずに済む
  - 生体認証等の厳密な認証方式が採用可能になる
  - 「入り口」を一箇所にすることにより監視が容易になる
- ユーザ（従業員）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

ユーザの認証は各企業で行う、そして**連携**させる

OpenSSOのご紹介

OpenSSOの歴史



SSO（シングル・サイン・オン）システム

一回ログオンしただけで、
様々なサーバ上の
コンテンツを利用可能に
するシステム

- 利便性のみが強調され過ぎている
- システムの実際の動作とは異なる

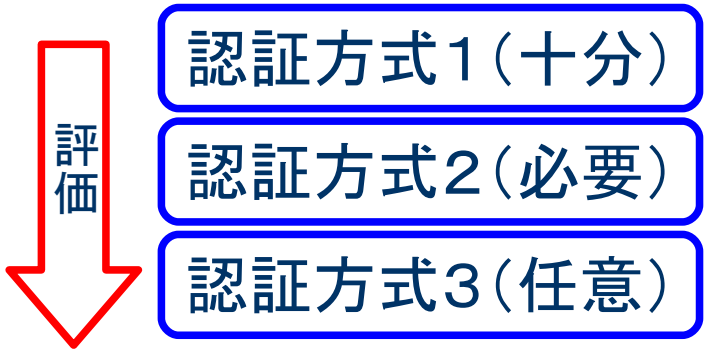
SSO（シングル・サイン・オン）システム

- 一回ログオンするだけ？
  - 必要に応じてより厳密な認証方式を組合わせて多要素認証を行う必要がある（認証連鎖）
- 様々なサーバ上のコンテンツを利用可能？
  - 適切な権限を持つユーザが必要とされる認証方式で認証済みである場合のみアクセスを許可する必要がある（アクセス制御ポリシー）

これらを含むOpenSSOの基本機能について説明します

認証方式と認証連鎖

- 様々な認証方式を組合わせて認証連鎖を設定する
- 各認証方式には適用条件(十分、必要、必須、任意)を指定する
- 認証成功時には認証方式に応じて認証レベルが設定される



使用例

- Windowsドメインにログオンしていないユーザにのみログイン画面を表示する
- 指静脈認証などの生体認証で認証済みのユーザには高い認証レベルを付与する

アクセス制御ポリシー

誰が ＋ 何に対して ＋ どのような操作ができるか

- 所属組織、グループ
- ロール
- 認証方式（認証レベル）
- 個人
- アクセス方法

URLを正規表現で指定

POST & GET

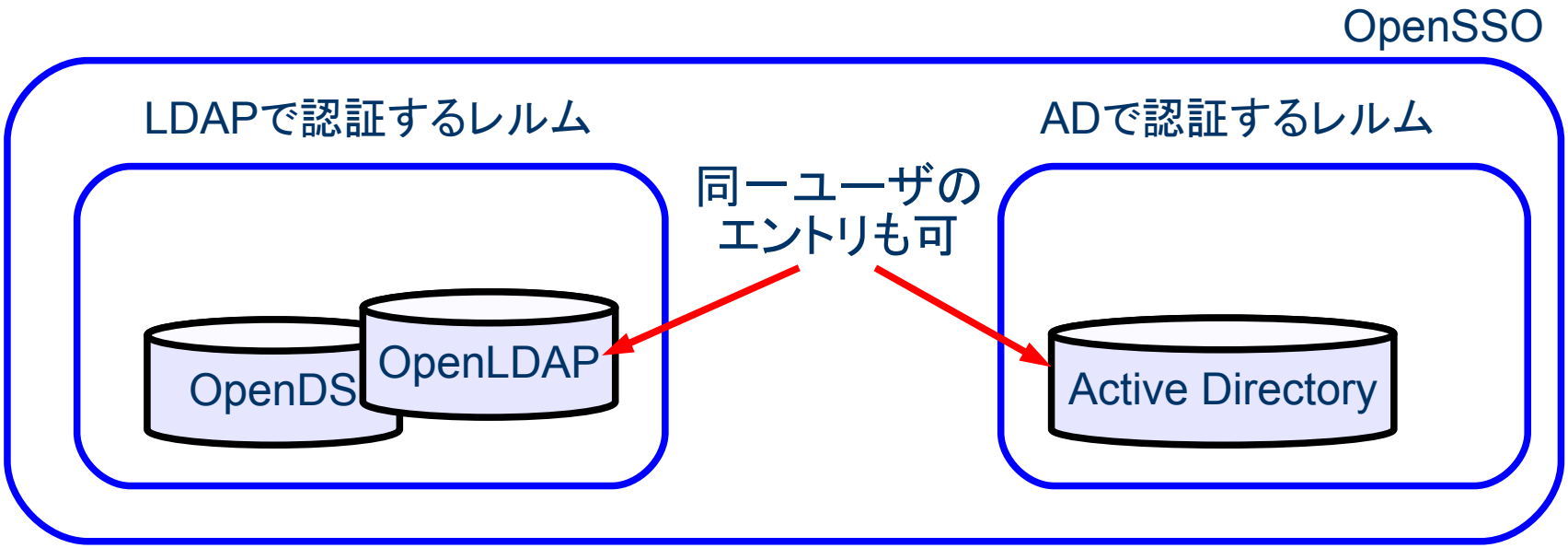
…を定めたルールの集まり

OpenSSOの基本機能（その3）

レルムとユーザリポジトリ

- レルム：設定を管理するための単位
  - ユーザリポジトリ
  - アクセス制御ポリシー
  - 認証方式
- ユーザは複数のレルムの所属することが可能
- ひとつのレルムに複数のリポジトリを設定可能

この機能はDirectory Server Access Management Editionでの反省に基づいています。



エージェント方式とリバースプロキシ方式

- エージェント方式
  - 保護対象のアプリが動作するサーバ上にアクセス制御用のモジュールを配置する方式
  - APIレベルでの細かな連携が可能
  - 保護対象のアプリやサーバのバージョンや設定変更に影響されやすい
- リバースプロキシ方式
  - リバースプロキシを使ってアクセス制御を行う方式
  - データの受け渡し方法がHTTPヘッダに限定
  - 保護対象のバージョンや設定変更の影響が少ない
  - 性能のボトルネックになる可能性も

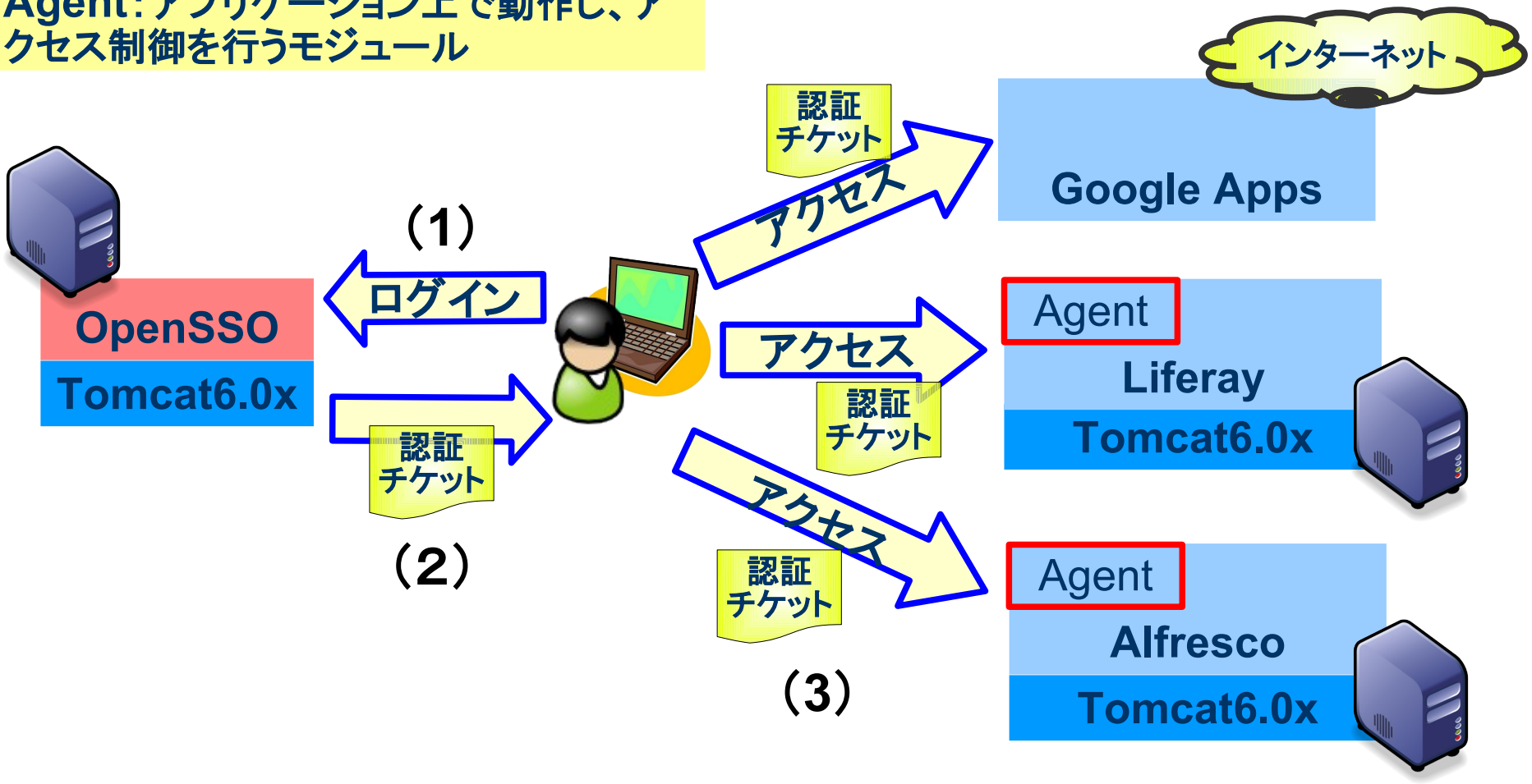
デモ その1

SAMLによる認証連携と

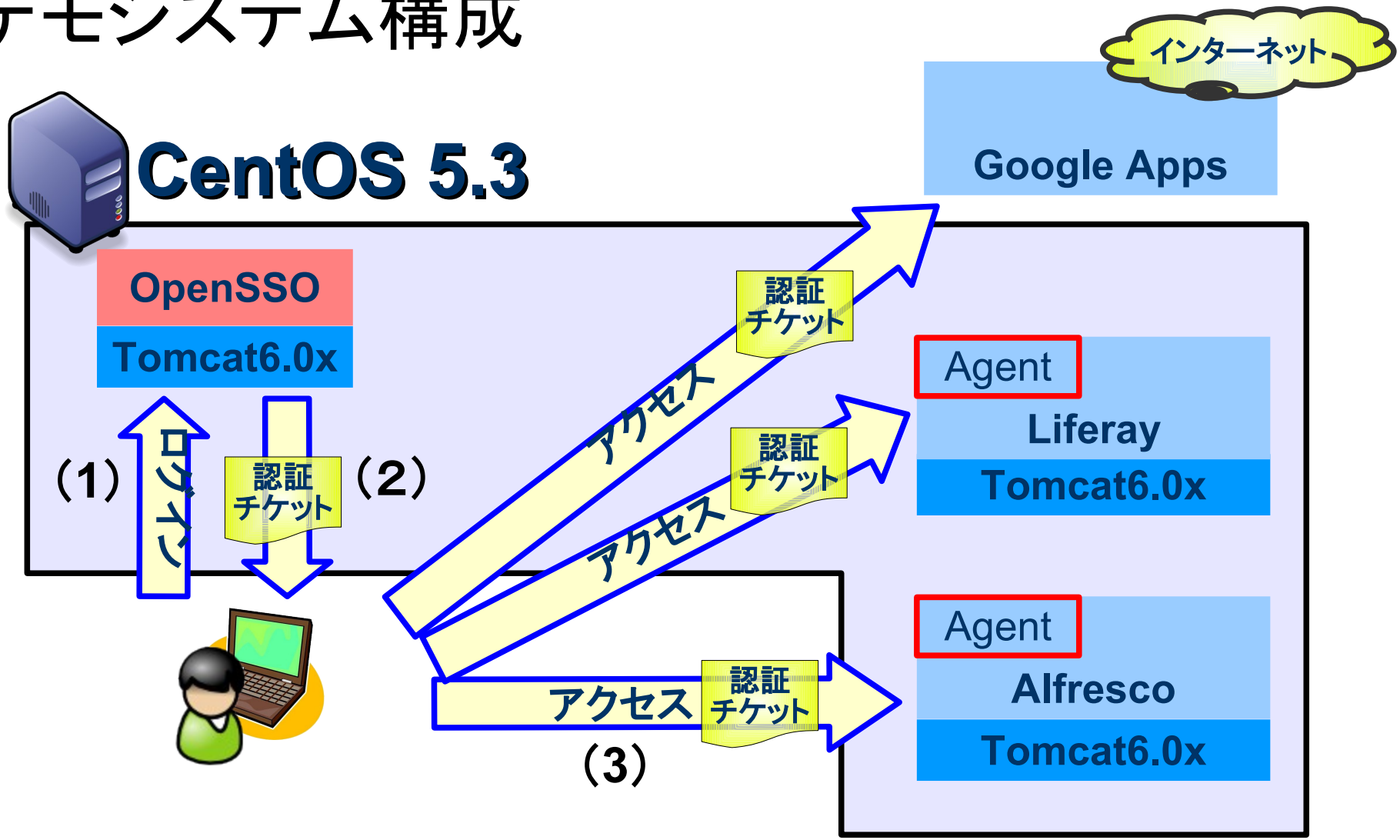
エージェントによるアクセス制御

システム構成 – SSO構成（エージェント方式）

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



デモシステム構成



1つのOSの中で3つのAPサーバを起動

デモ その2

Windowsドメイン認証との連携

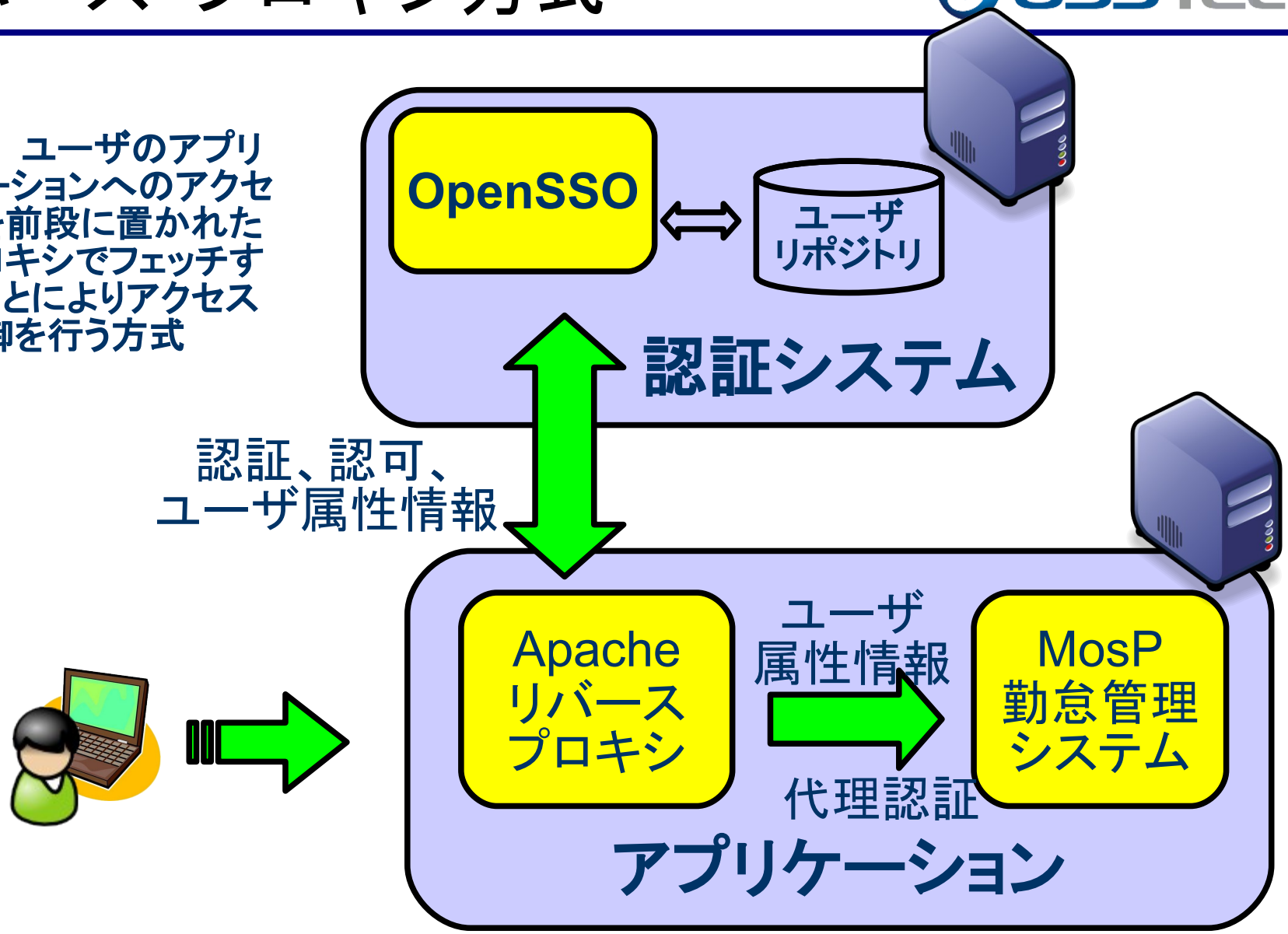
&

リバースプロキシ方式による

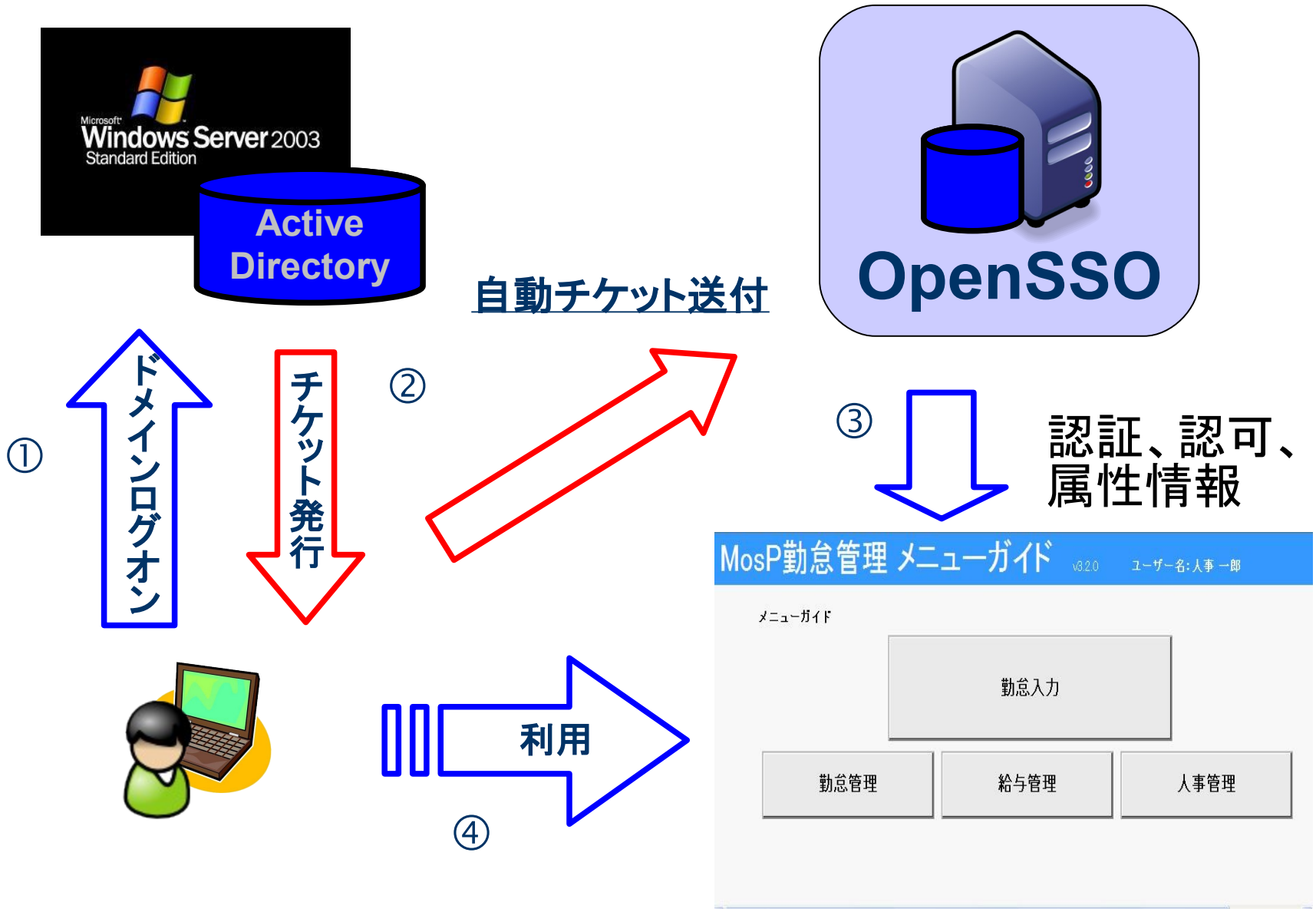
アクセス制御

リバース・プロキシ方式

注： ユーザのアプリケーションへのアクセスを前段に置かれたプロキシでフェッチすることによりアクセス制御を行う方式



デモの概要



本日のまとめ

- 認証は社内で行い、認証連携によりクラウドサービスを利用する方法をお勧めします。
- 様々なプロトコルに対応したOpenSSOを利用することにより容易に連携を行うことができます。
- OpenSSOは様々なアプリケーションに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。
- シングル・サイン・オンは利便性の向上だけでなく、社内システムのセキュリティ向上にも効果があります。