オープンソース技術解説セミナー

クラウドとイントラネットのログインを統合する
シングルサインオン・ハブ を
オープンソースで構築しよう

OSSTech

2011年10月21日
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
http://www.osstech.co.jp/
お問い合わせ info@osstech.co.jp

目次

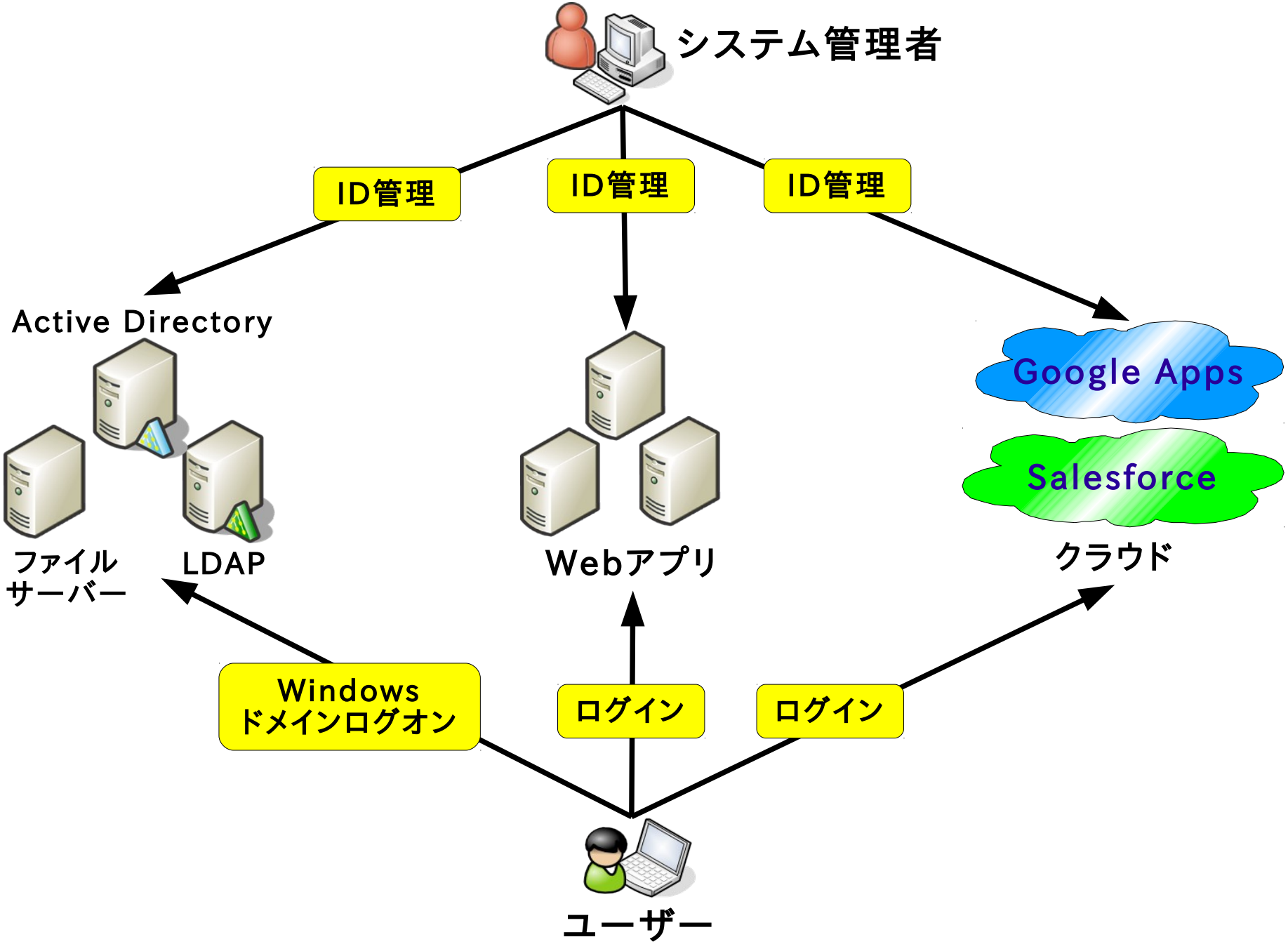
- 会社紹介
- シングルサインオンとは
- OpenAMのご紹介
- シングルサインオン方式
- OpenAMで実現するシングルサインオン・ハブ
- ID管理との組み合わせで導入効果倍増

会社紹介

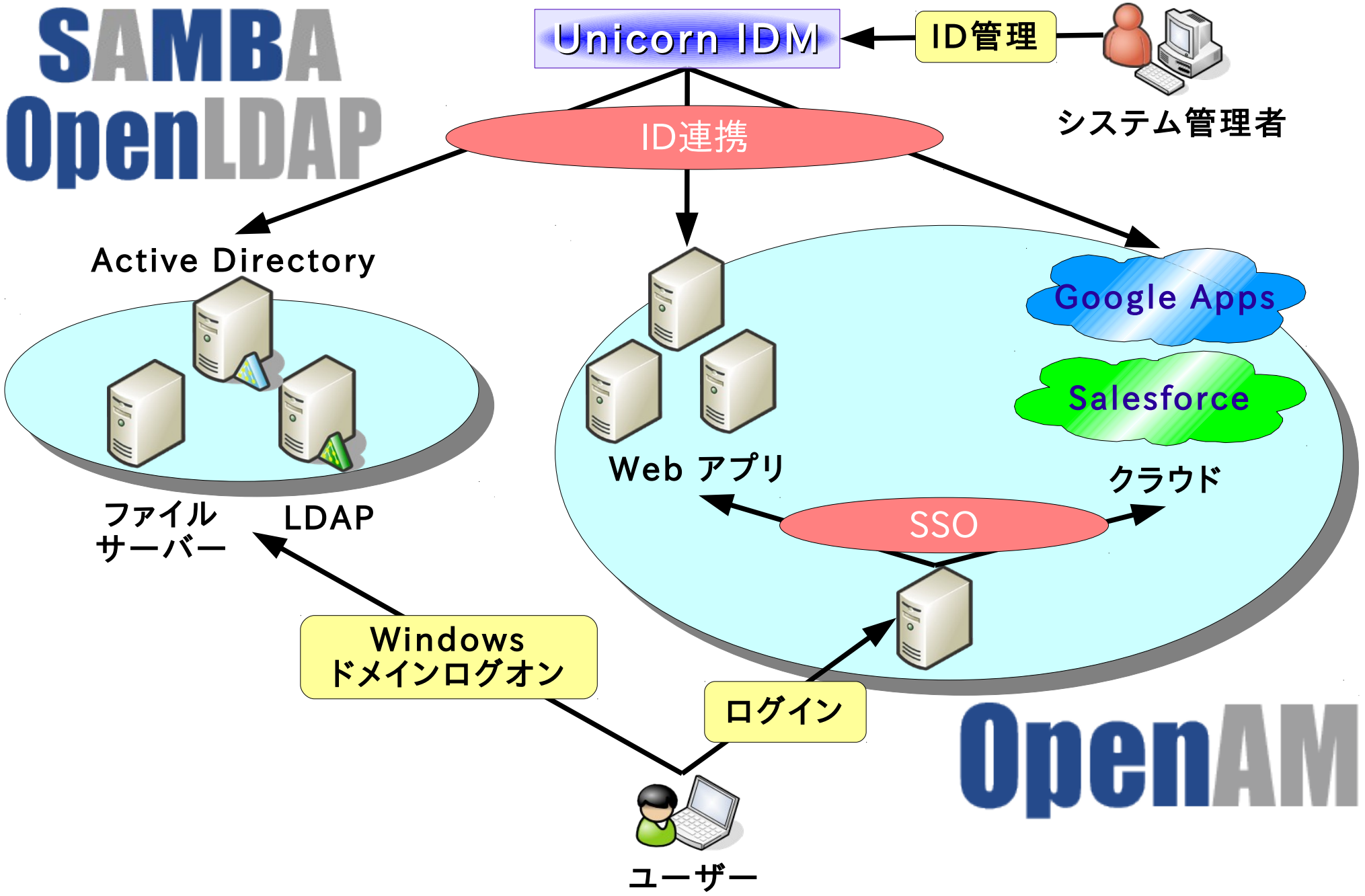
オープンソース・ソリューション・テクノロジ株式会社

- 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,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も提供
  - 商用製品とOSSの柔軟な組み合わせに対応

OSSTechのソリューション領域



OSSTechのソリューション導入効果

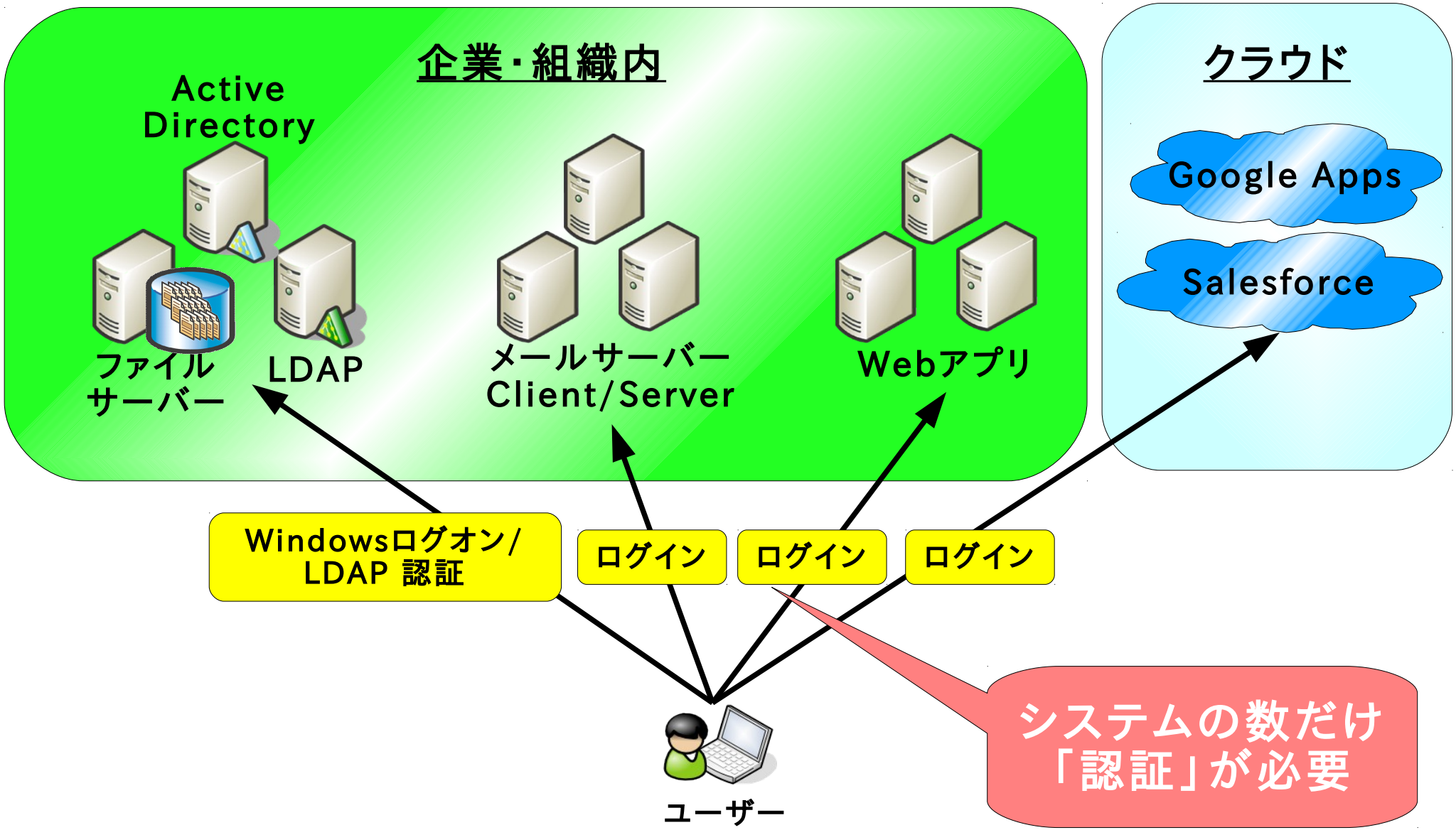


社員著作紹介

- 2005年10月, 日経BP社「セキュアなSambaサーバの作り方」
- 2006年5月, 技術評論社「LDAP Super Expert」
  - 巻頭企画［新規/移行］LDAPディレクトリサービス導入計画
- 2010年9月, 技術評論社「Software Design」
  - クラウド対策もこれでOK! 統合認証システム構築術
- **2011年9月～, 日経BP社「日経Linux」**
  - **連載中!「Linux認証のすべて」**
- その他
  - http://www.osstech.co.jp/company

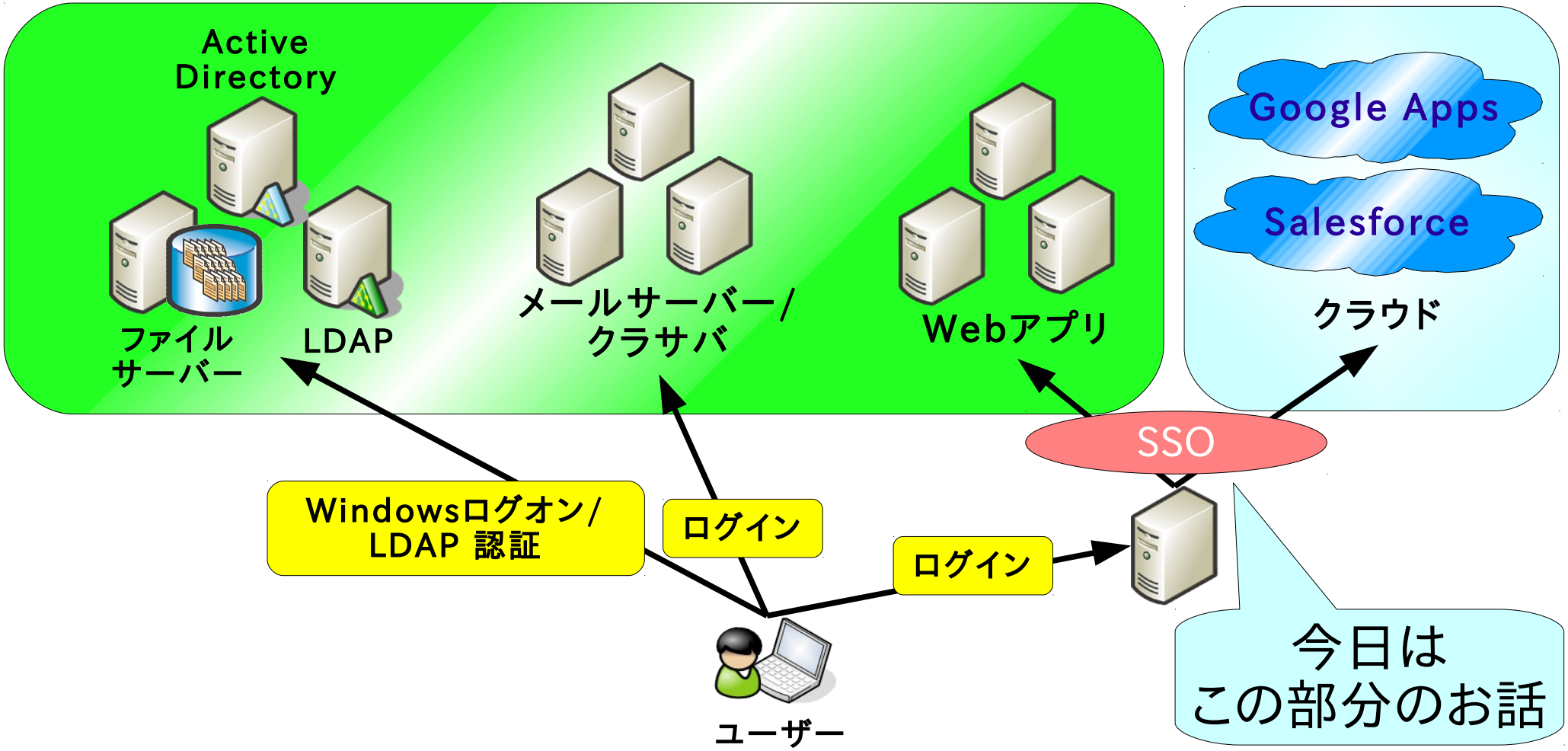
シングルサインオンとは

システムには必ず必要な「認証」



シングルサインオンとは

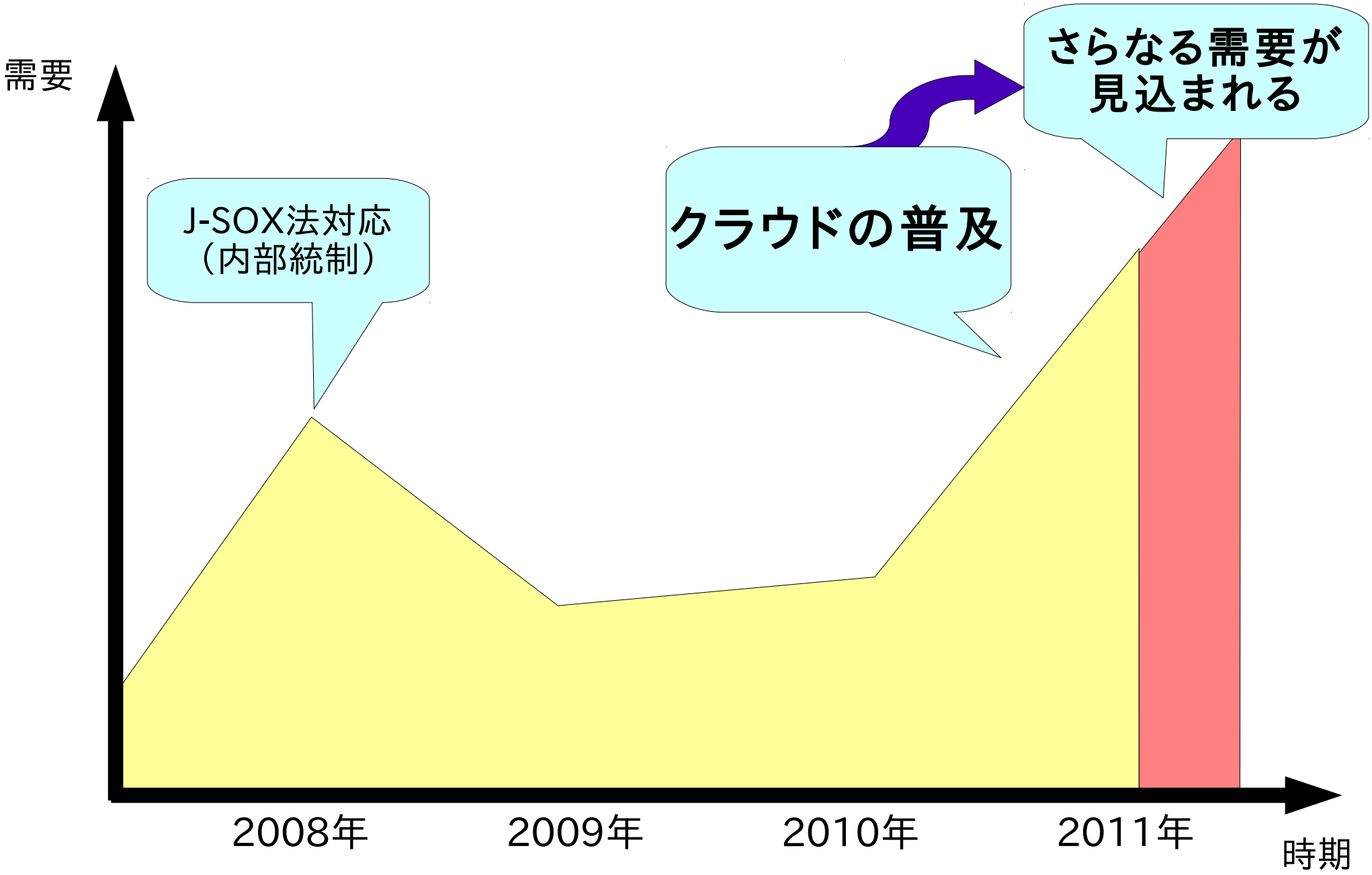
一度のログイン操作さえ完了すれば、複数のWebアプリケーションに認証操作することなくアクセスすることが可能になる。
（以後、SSO と略すことも）



今こそシングルサインオン！

なぜ今シングルサインオンが必要なのか

SSO（ID管理）の需要推移



今後の需要

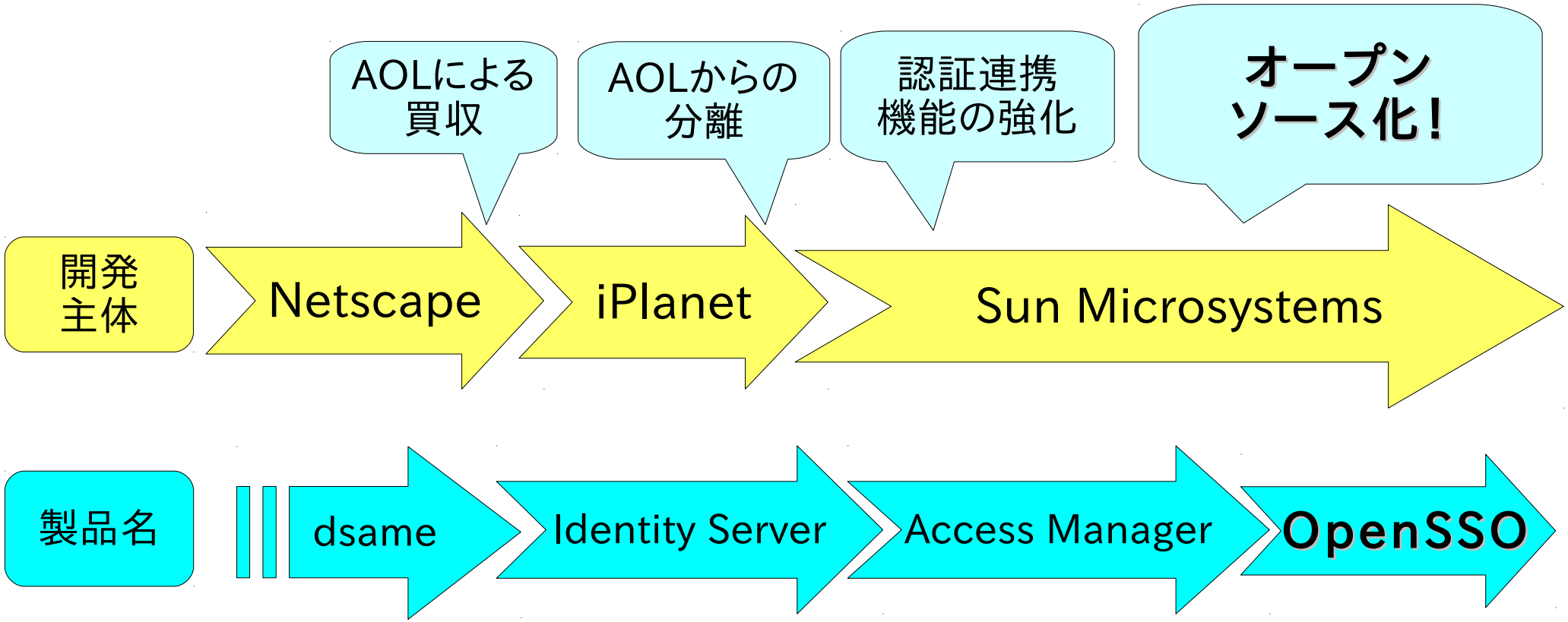
- クラウド（外部のWebサービスの業務利用）が普及したことで、ID管理・シングルサインオンの需要が急上昇
- よくある問い合わせ
  - 社内にある多数のWebアプリ（オンプレミス）へのアクセスをシングルサインオンで管理し、利便性を向上させたい
  - 社内のWebアプリと**外部のWebサービス（Google Apps、Salesforceなど）をシングルサインオン連携したい**（クラウドサービス利用者）
  - **学術認証フェデレーション（Shibboleth）**に参加したい（文教系）

OpenAM（旧OpenSSO）の紹介

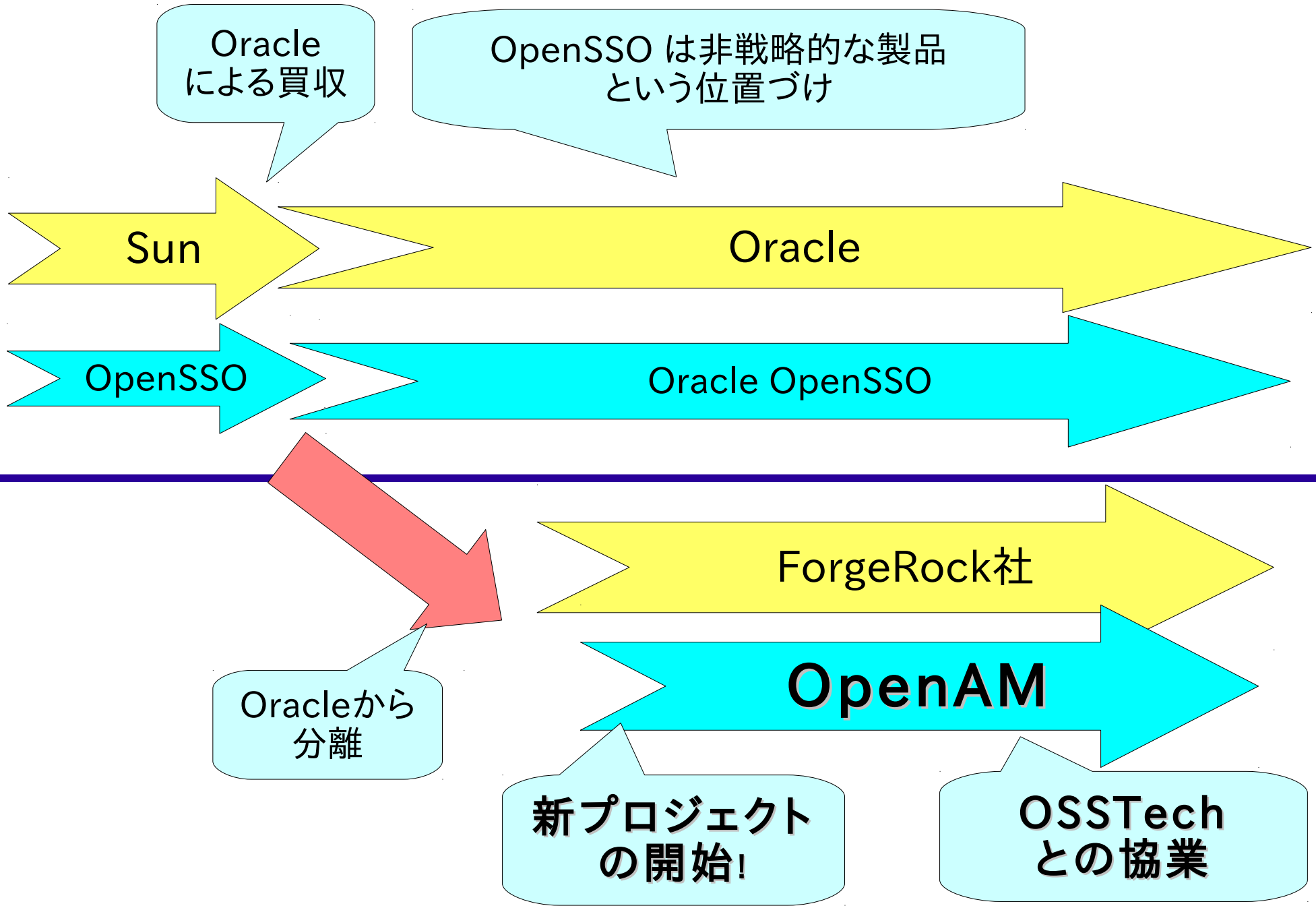
OpenAMとは

- 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オープンソースソフトウェア
- **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
- ユーザー情報を格納するためのユーザーリポジトリ（ユーザーデータストア）として様々な LDAP サーバー、RDBに対応
- 充実した管理 GUI

OpenAMの歴史 - その1



OpenAMの歴史 - その2



OpenAMのこれから（技術面）

- OpenAM は OpenSSO の正常進化形
  - OpenSSO を担当していたエンジニアが中心になりForgerock社を設立
  - OpenSSOと完全互換(ベースにするソースコードが同じ)
- クラウド対応強化
  - Google Apps, Salesforce とのシングルサインオン（SAML）連携機能を強化
  - GUI による操作でシングルサインオン設定が可能
- 機能拡充
  - ワンタイムパスワード機能の追加
  - ユーザーリポジトリしてRDBをサポート
- 次期バージョン（OpenAM 10）では更なる認証機能の強化を検討中
  - リスクベース認証：ID/PW認証に加え、ユーザーのアクセス元IPアドレス、ブラウザ（デバイス）情報などから不正アクセスのリスクを判定し、必要に応じて多要素認証などをユーザーに要求する。

OpenAMのこれから（ビジネス面）

- ベンダ独自のパッケージングも可能
  - 生体認証などの独自認証方式を組み合わせる
  - ID管理システムと組み合わせる
  - OSSTech 版 OpenAM の特徴
    - OpenLDAP 用拡張スキーマを提供
    - ID管理製品（Unicorn IDM）との組合わせ
    - Google Apps/Salesforce/学認などと連携するシングルサインオンソリューションを提供
- 需要
  - 日本では多くが新規ユーザー
  - 企業・大学などの認証基盤として OpenAM を利用
  - クラウドにおける認証基盤・認証強化ツールとして OpenAM を利用
  - 既存ユーザー（Sun Access Manager、OpenSSO）からの移行（米国、ヨーロッパ）
  - **複数のシングルサインオン環境を統合する”ハブ”システムとして利用**

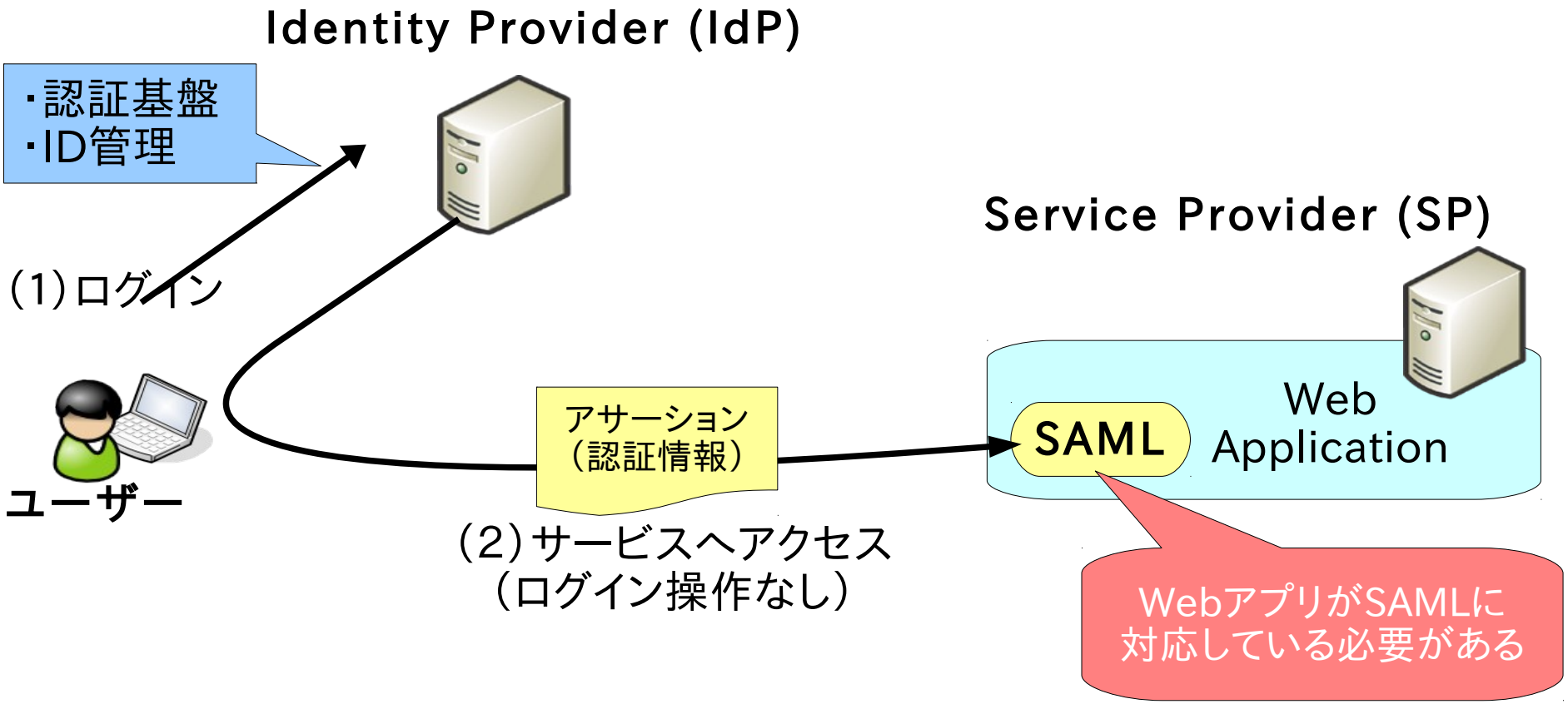
シングルサインオン方式

何が違う?「認証」と「認可」

- 認証（Authentication）
  - 本人性を確認する
  - ID/パスワード認証、生体認証、ワンタイムパスワード認証など
- 認可（Authorization）
  - あるリソースへアクセスするための権限を与える（認証後のアクセス制御）

シングルサインオンの方式（1）

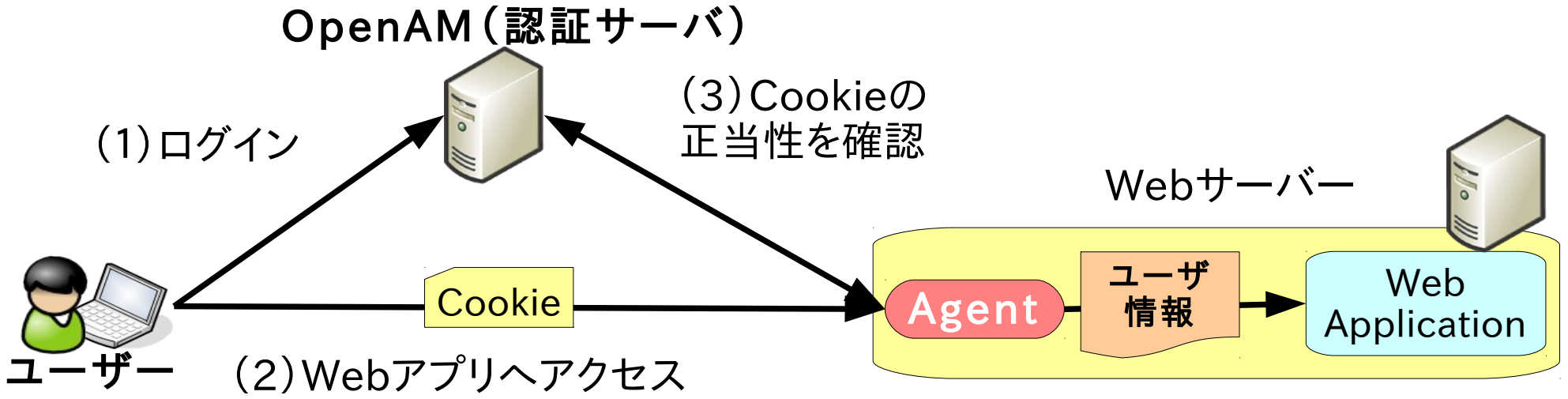
SAML



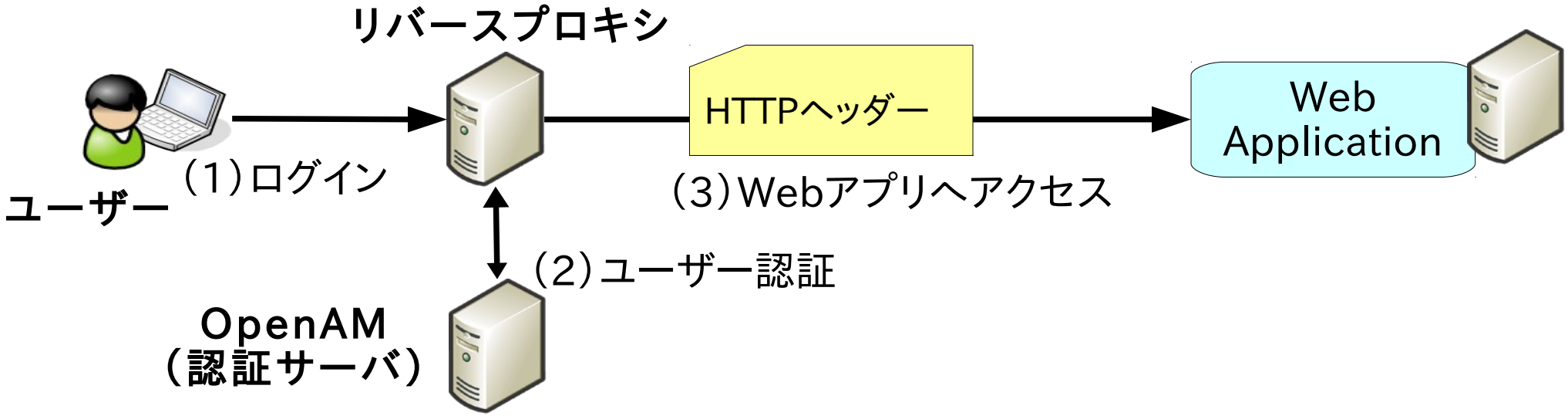
※この図は、HTTP Redirect Binding/HTTP POST Binding の場合の例です。

シングルサインオンの方式（2）

エージェント方式



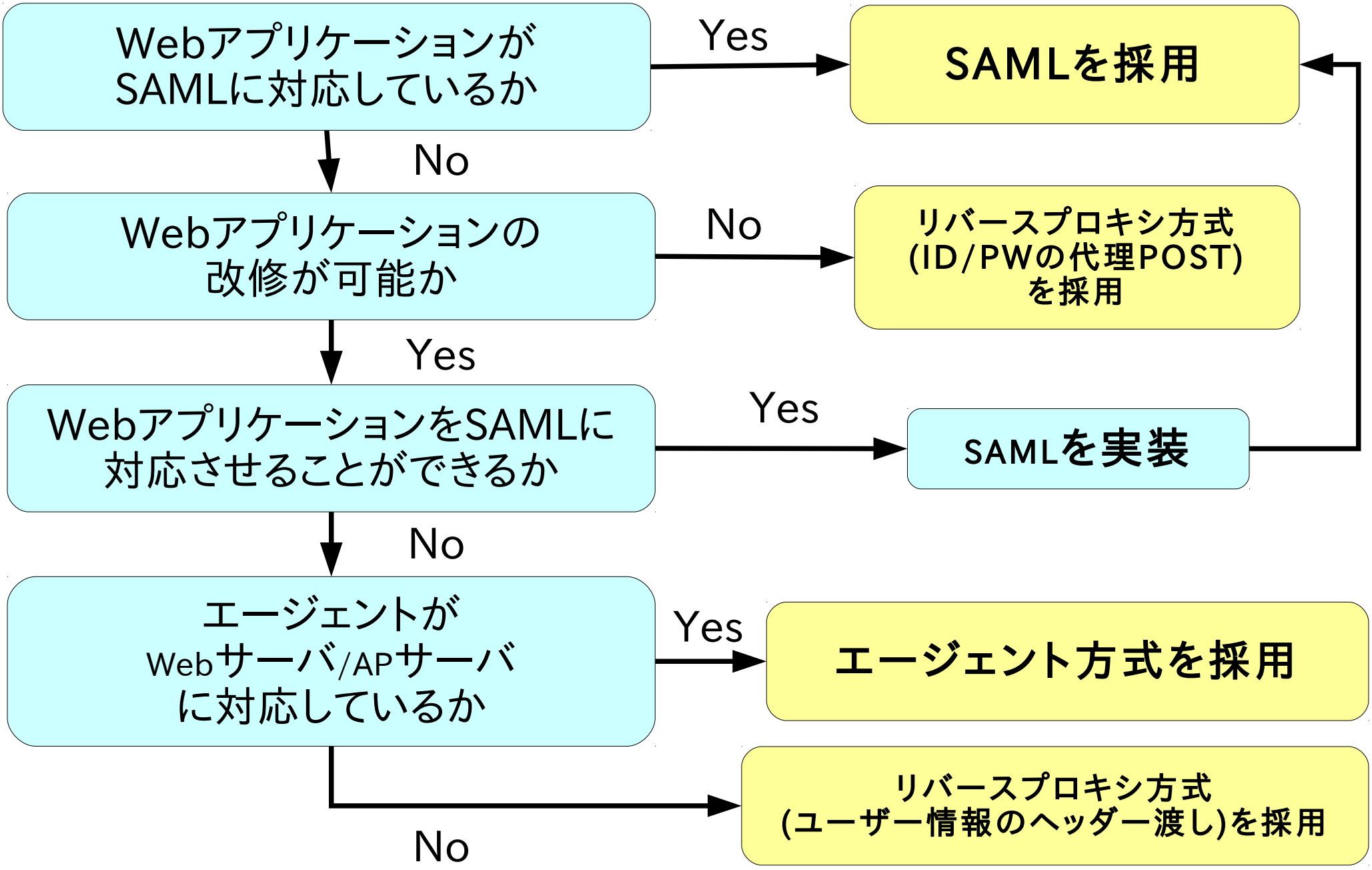
リバースプロキシ方式



シングルサインオン方式の比較

方式	用途	改修	長所・短所
SAML	認証 (認可)	必要	■他のWebサービス・SSO製品との互換性が高い ■細かなアクセス制御をするには実装が大変 ■異なるネットワーク/ドメイン構成でも対応可能
エージェント	(認証) 認可	必要	■細かなアクセス制御(認可)が可能 ■Webサーバー/APサーバーに対応したエージェントが必要 ■できれば同じネットワーク/ドメインがよい
リバース プロキシ	(認証) 認可	必要 or 不要	■細かなアクセス制御(認可)が可能 ■ユーザー情報をHTTPヘッダーで渡す場合は改修が必要な場合あり ■ID/PWを代理でHTTP POSTする場合は改修不要 ■リバースプロキシがボトルネックになる可能性もある ■できれば同じネットワーク/ドメインがよい

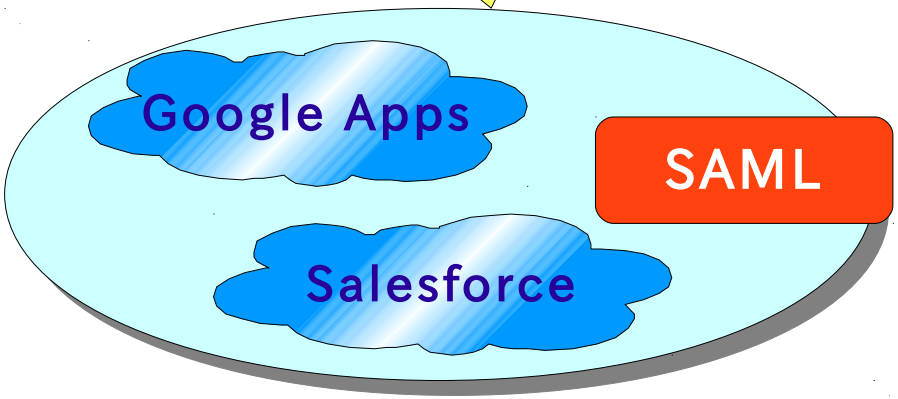
シングルサイオン方式の採用基準



OpenAMで実現する
シングルサインオン・ハブ

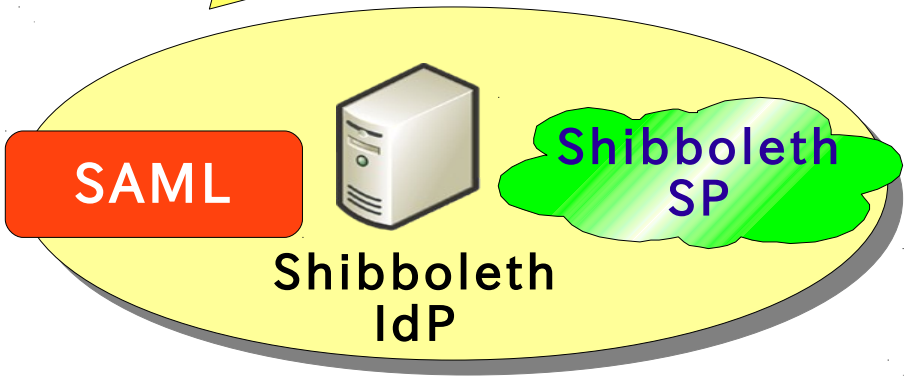
これからのSSO - 混在する複数のSSO環境

SAML IdP を導入して
SSO を実現

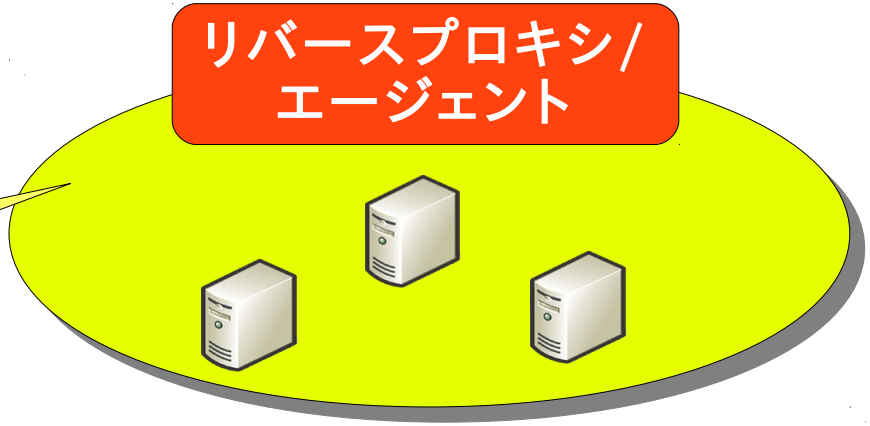


クラウドSSOセグメント

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

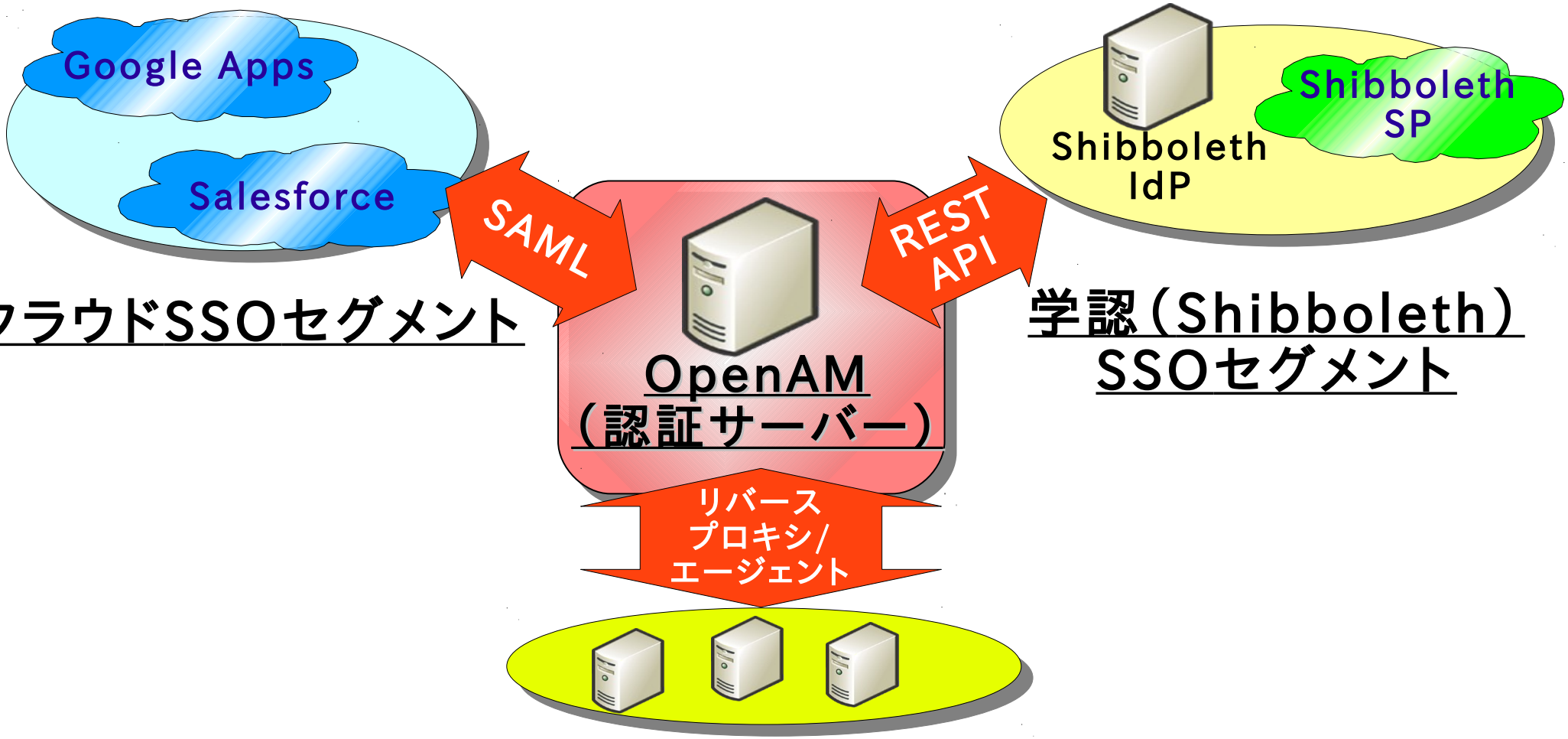
社内SSOセグメント

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できない
- **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

シングルサインオン・ハブを実現するための機能

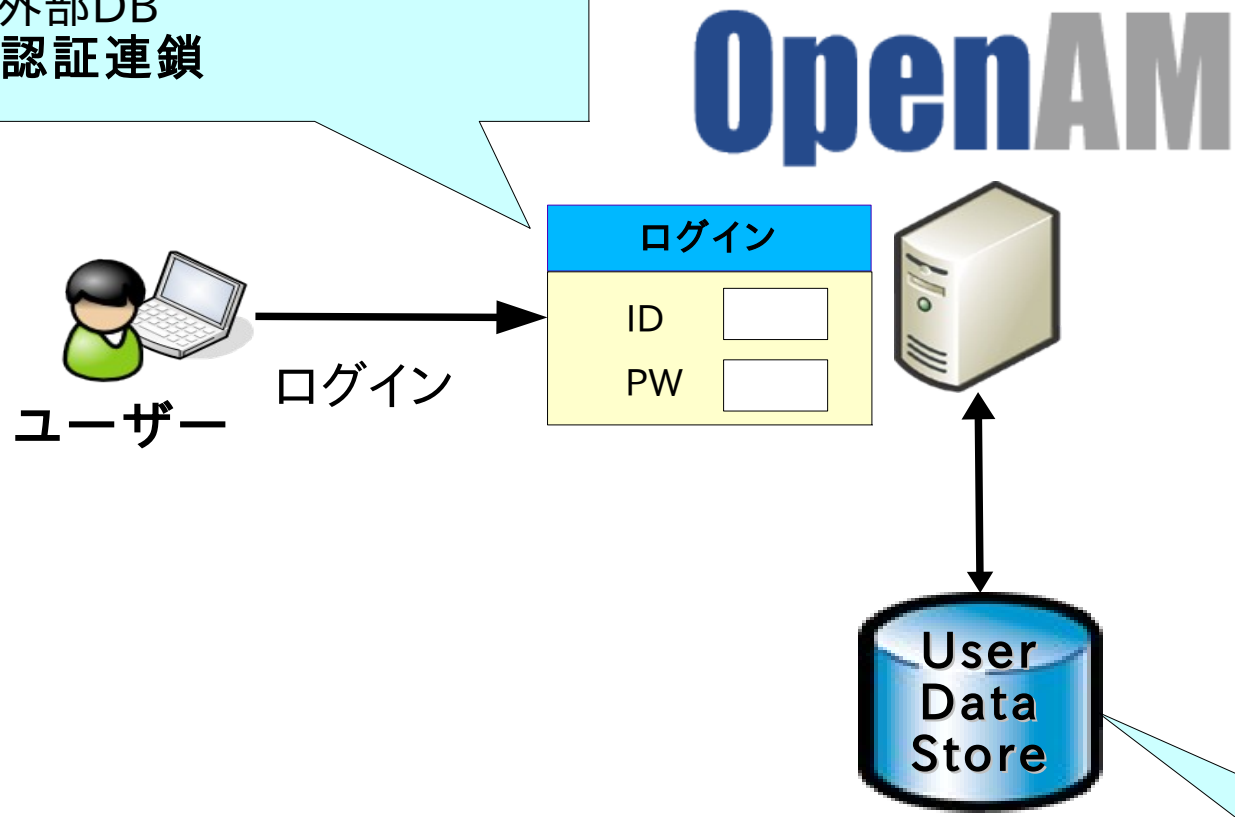
- **認証機能**
  - ユーザーの本人性を確認する。セキュリティ強化のために、多要素認証が望ましい。
- **ユーザー情報保存機能**
  - 認証情報や他システムに連携するユーザー情報を保存する
- **外部システムと連携可能なインタフェース**
  - フェデレーション（SAML、OpenID、OAuthなど）
  - REST API
  - SDK

OpenAMの機能

認証機能
ユーザー情報保存機能

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
  - 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**

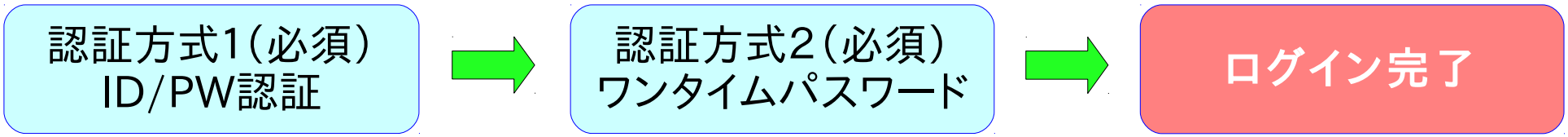
OpenAMの機能 - ユーザーデータストア

- OpenAMのユーザー情報を格納するLDAPサーバー/データベースサーバー
  - Active Directory
  - Open LDAP（弊社は独自にサポート）
  - Sun Directory Server
  - OpenDS（Sun Directory Server のオープンソース版。OpenAMに標準で組み込まれている）
  - RDB（Oracle、MySQL）

OpenAMの機能 - 認証連鎖

- 多様素認証の必要性
  - 複数の認証方式を組合わせて認証を行うことでセキュリティを強化

- **認証連鎖**
  - 複数の認証方式を任意に組み合わせて利用可能



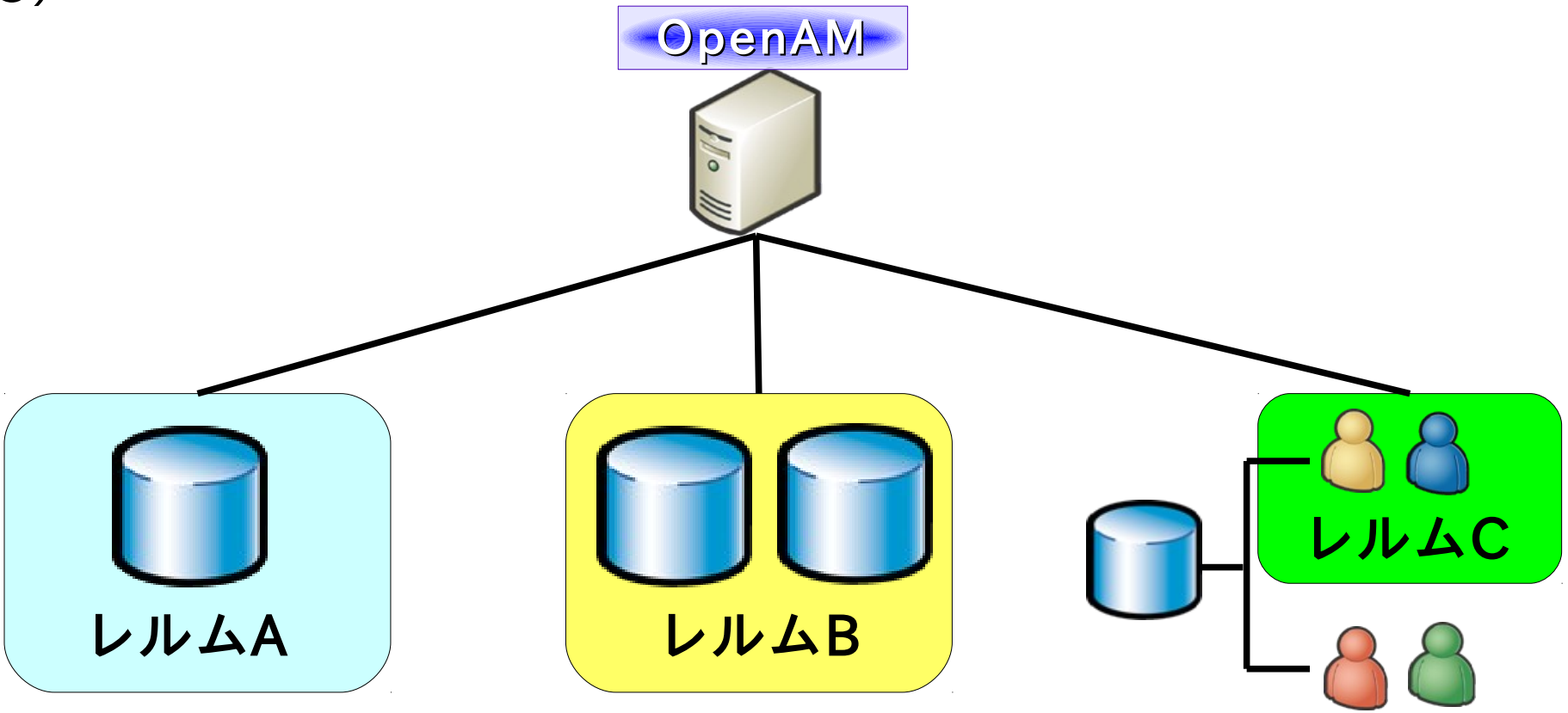
OpenAMの機能 - レルム

- 「レルム」：OpenAMの設定を管理するための単位

- 以下の設定をレルム単位で管理
  - ユーザーデータストア（LDAPベースDN、検索フィルタなども指定可能）
  - アクセス制御ポリシー
  - 認証方式
- 基本的には、ユーザー情報DB単位でレルムを分ける
- レルム毎に管理者を置き管理を委任することが可能

OpenAMの機能 - レルム使用の具体例

- 複数組織（複数の企業など）のシングルサインオン基盤を OpenAM で構築し、組織毎に設定を行なう（マルチテナント）
- 複数の DB を一つのレルムに登録し、全てのユーザーに同一のシングルサインオン環境を提供する（例B）
- DB内の特定のユーザーに対してのみ、シングルサイオン可能にする（例C）



OpenAMの機能

外部システムと連携可能なインタフェース

シングルサインオン・ハブを実現するための機能

- OpenAM が持つインタフェース
  - **フェデレーション機能**
    - SAML、OpenID、OAuth、ID-WSFなどの標準プロトコルを利用してSSO を実現。
  - **エージェント**
    - 様々な Web サーバー/アプリケーションサーバーに対応したエージェントを準備。アプリケーションの開発工数を最小限に抑えながら、OpenAM で管理可能とする。
  - **REST API**
    - 認証情報の検証などを行う API を装備。HTTP でアクセス可能であり、システム間通信に利用可能。他の認証サーバーが受け取った ID/PW や Cookie を OpenAM に送信し、認証を行うなどする。
  - **ClientSDK（Java）**
    - OpenAMの認証部分のコア機能を利用するアプリの開発が可能。
    - OpenAM の現在の OpenID、OAuth の機能は ClientSDK を利用。

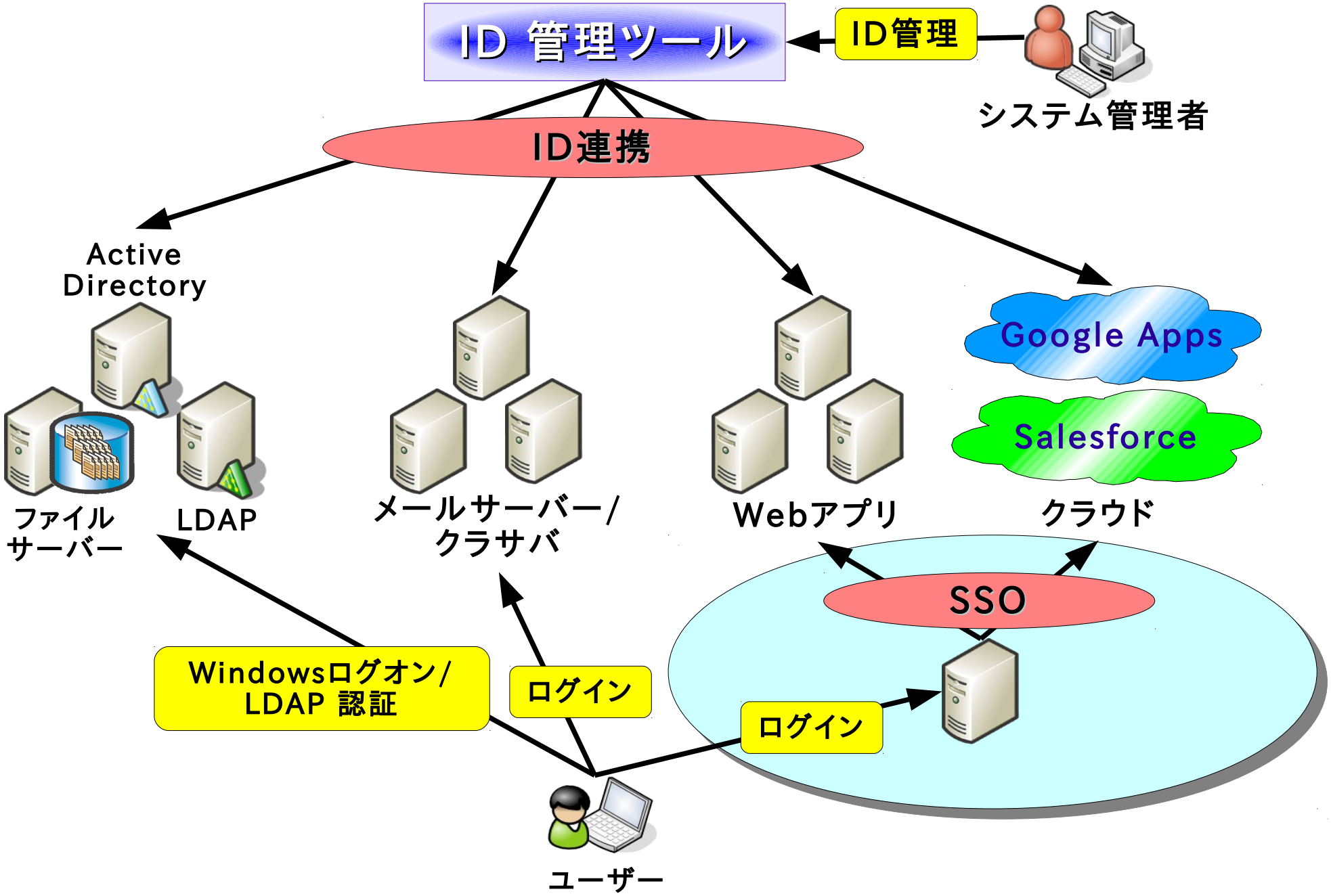
ID管理との組み合わせで効果倍増！

ID管理との連携

- シングルサインオンとID管理は一緒に使うことで最大の効果を発揮する
  - ユーザーID/パスワードはシングルサインオンシステムで一元管理可能でも、各アプリケーション・サービス毎に必要なユーザー情報は、基本的には個々に管理される
  - ID管理ツールなどを利用したID一元管理をしなければ、シングルサインオンシステムの運用は破綻する

- クラウドサービスにおいても、ID管理は必要
  - クラウドサービス側にもユーザー情報を保存することから、ID管理の対象となる
  - ID管理用のAPI（プログラムインタフェース）を備えているものが多い（Google Apps、Yahoo! など）

ID 管理 & SSO



OSSTech

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