ハイブリッド・クラウド時代における Webアプリの認証セキュリティ対策

～シングルサインオンでセキュリティと利便性を両立させる～

オープンソース・ソリューション・テクノロジ株式会社

代表取締役 チーフアーキテクト 小田切耕司

お問い合わせ info@osstech.co.jp

OSSTech

Part 1
講師紹介
オープンソース・ソリューション・テクノロジ
会社紹介

OSSTech

講師紹介

- 役　職 ： 代表取締役 チーフアーキテクト
- 氏　名 ： 小田切 耕司（おだぎり こうじ）
- 所属団体等
  - OpenSSO&OpenAMコンソーシアム 副会長
  - OSSコンソーシアム 副会長
  - 日本LDAPユーザ会設立発起人
  - 日本Sambaユーザ会初代代表幹事
- 執筆関係
  - 日経Linux 2011年9月号～2012年2月号 連載中
    - 『Linux認証のすべて』（第1回～第6回）
    - http://itpro.nikkeibp.co.jp/linux/
  - ASCII.technologies 2011年2月号
    - 『キホンから学ぶLDAP』
    - http://tech.ascii.jp/elem/000/000/569/569412/
  - 技術評論社 Software Design 2010年9月号
    - 第1特集 クラウド対策もこれでOK！
      統合認証システム構築術
      OpenAM／SAML／OpenLDAP／Active Directory
    - http://gihyo.jp/magazine/SD/archive/2010/201009
  - @IT やってはいけないSambaサーバ構築：2008年版
  - 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

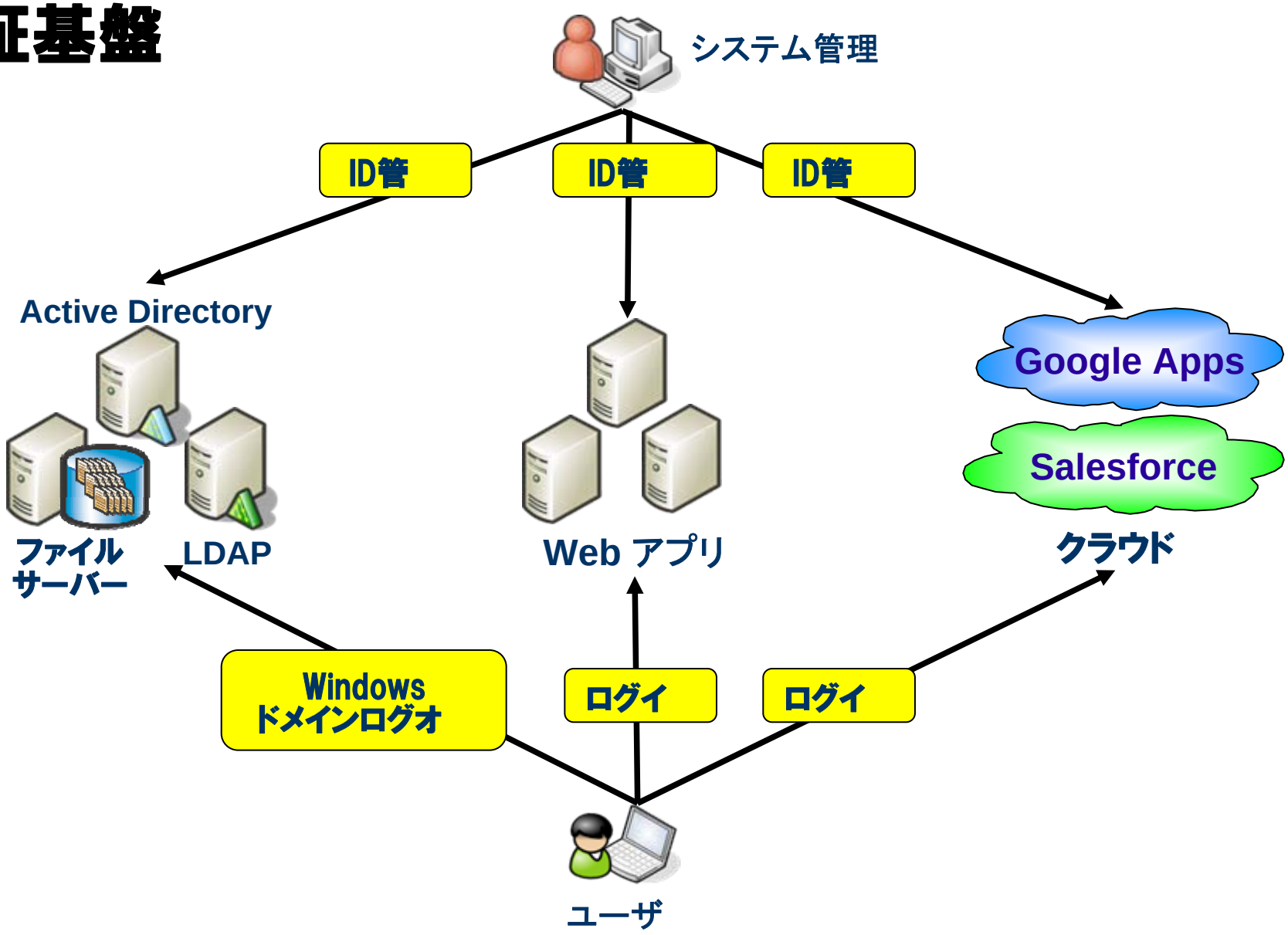
オープンソース・ソリューション・テクノロジ株式会社

- **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/AIXへも対応
  - Windows/UNIX から Linux への移行も支援！
- **OSSを利用した認証基盤構築**が得意分野
  - LDAP認証、Windowsドメイン認証、Webアプリケーション認証、クラウド認証
- **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
  - OSSの製品パッケージ・製品サポートを提供
  - OSSの改良、バグ修正などコンサルティングにも対応

会社概要

会 社 名	オープンソース・ソリューション・テクノロジ株式会社	所属 団体等	OpenSSO&OpenAMコンソーシアム理事 副会長 OSSコンソーシアム理事 副会長 OSCA (Open Standard Cloud Association) 理事 LPI-Japanビジネスパートナー デルISVアリーナ パートナー NEC CLUSTERPRO WORKSパートナー レッドハット レディ・ビジネス・パートナー
英語表記	Open Source Solution Technology Corporation		
社名略称	OSSTech(オーエスエステック)または OSSテクノロジ		
業務内容	・OSS(オープンソース)を中心とするソフトウエアの 企画、開発、販売およびサポート ・システムの導入に関するコンサルティング ・ソフトウエアに関する教育、研修	取引先 および パートナー様	・株式会社野村総合研究所 ・デル株式会社 ・株式会社バッファロー ・日本電気株式会社 ・株式会社 大塚商会 ・キヤノンITソリューションズ株式会社 ・伊藤忠テクノソリューションズ株式会社 ・新日鉄ソリューションズ株式会社 ・株式会社PFU ・株式会社 日立ソリューションズ ・三菱電機インフォメーションシステムズ株式会社 ・ソフトバンク・テクノロジー株式会社 ・ニフティ株式会社 ・三井情報株式会社 ・ダイワボウ情報システム株式会社 ・NTTデータ先端技術株式会社
役 員	代表取締役　　小田切 耕司 技術取締役　　武田 保真		
オフィス	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		
Web	http://www.osstech.co.jp/		
設立	2006年9月		
資本金	1500万円		

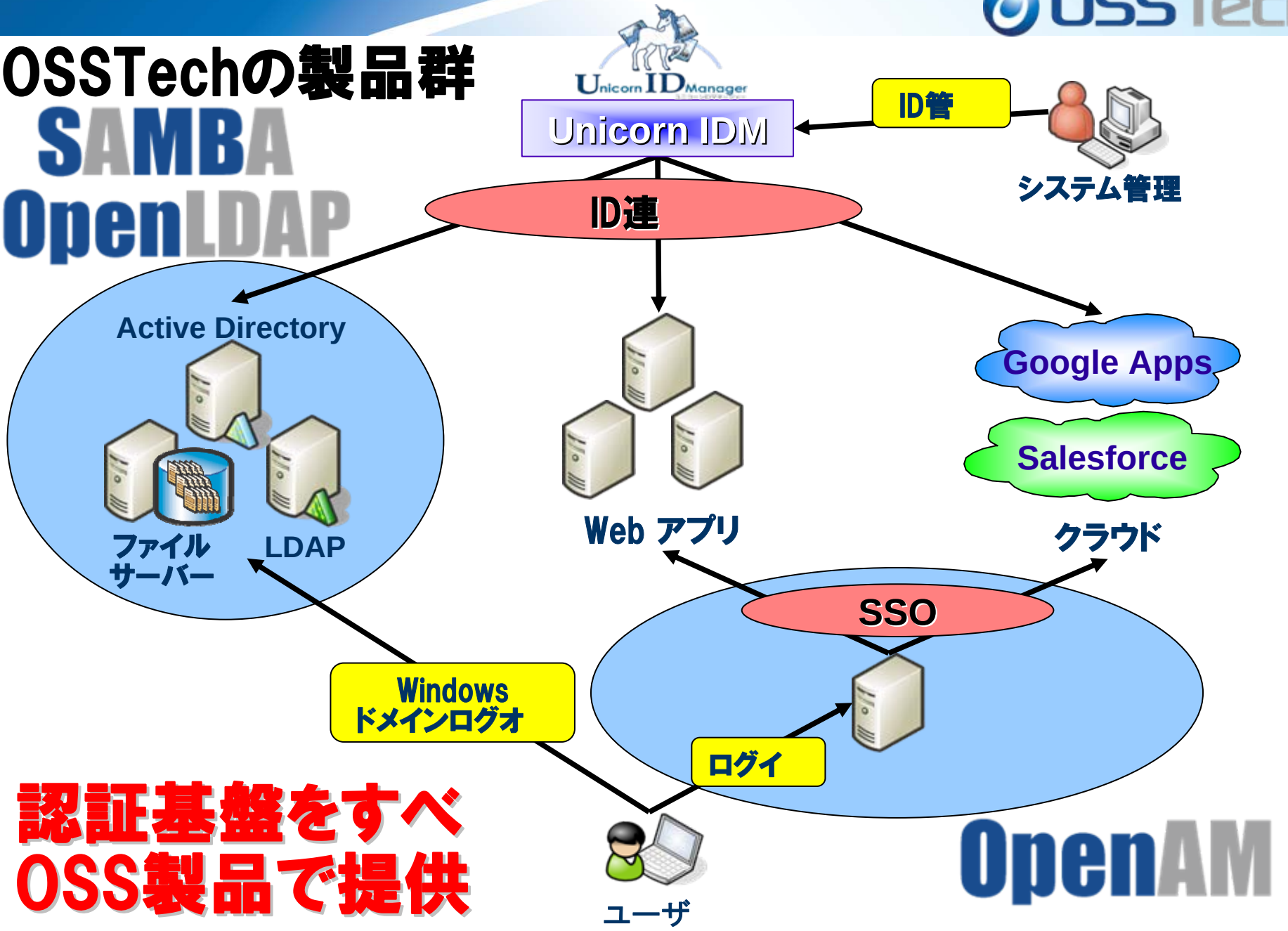
認証基盤



OSSTechの製品群

SAMBA

OpenLDAP



認証基盤をすべ
OSS製品で提供

OpenAM

OSSTechの製品群(すべてOSSで提供)

原則Linux/Solaris/AIX共にRPMで提供

① Samba for Linux/Solaris/AIX
- ADの代替、高性能NASの代替

② OpenLDAP for Linux/Solaris/AIX
- 認証統合、ディレクトリサービス、シングルサインオンのインフラ

③ OpenAM for Linux/Windows/Solaris
- Tomcat,OpenLDAP対応で高機能なシングルサインオン機能を提供

④ Unicorn ID Manager for Linux/Solaris
- Google Apps,ActiveDirectory,LDAP, Yahoo!メール Academic Editionに対応した統合ID管理

OSSTechの製品群(すべてOSSで提供)

原則Linux/Solaris/AIX共にRPMで提供

⑤ Chimera Search for Linux
- アクセス権の無いファイルは表示されない全文検索システム

⑥ LDAP Account Manager for Linux/Solaris
- 管理機能の弱いOSSのLDAP/SambaにWebベースのGUIを提供

⑦ ThothLink for Linux
- リモートからのWindowsファイルサーバアクセス機能を提供

⑧ Mailman for Linux/Solaris
- Google Appsのメーリングリスト機能を補完

⑨ Netatalk for Linux/Solaris
- UTF-8に対応したMac OS対応のAFPファイルサーバー

現在開発中

- Nginxのポリシーエージェント開発中
  - 開発が終了した従来のSun Web Proxy Serverの代替用途として
  - Apacheよりも軽量で高速、高セキュリティ
  - Windows版の製品化も検討

エンジニア募集中です！

特にOpenAM（Java）のエンジニア募集中

http://www.osstech.co.jp/company/recruit

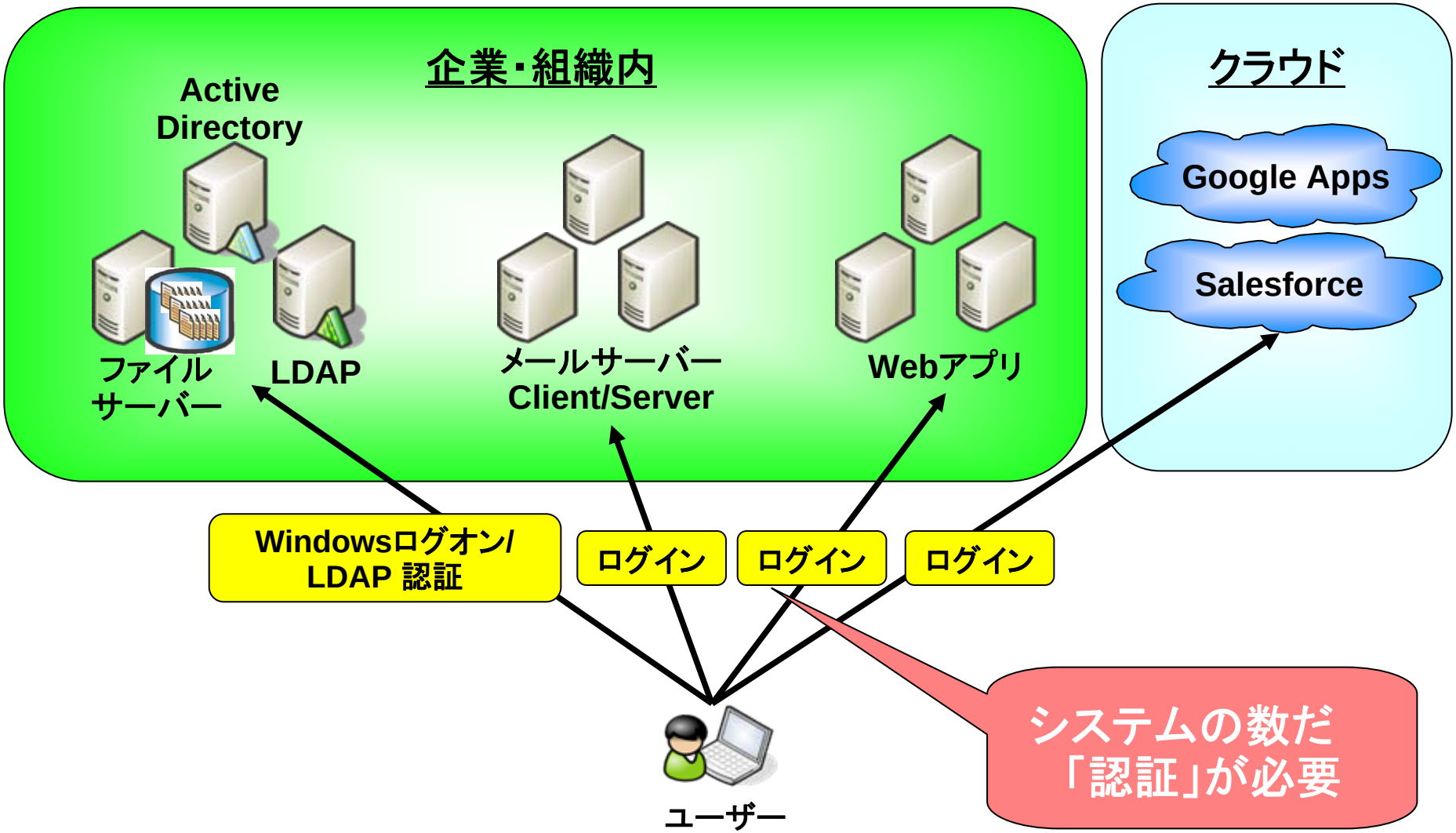
recruit@osstech.co.jp

- OpenAM（OpenSSO）を使ったシングルサインオンもしくはSamba、OpenLDAPを使った統合認証に関する開発エンジニア、コンサルタント、アーキテクト
- シングルサインオン、統合認証、Linux / UNIX / OSS経験
- Java,Cの知識があり、前向きに自分でスキル向上を目指せる方
- 紹介会社などを通さず**直接弊社へ募集エントリされた方には、入社後現金20万円を差し上げます**

Part 2
シングルサインオンとは

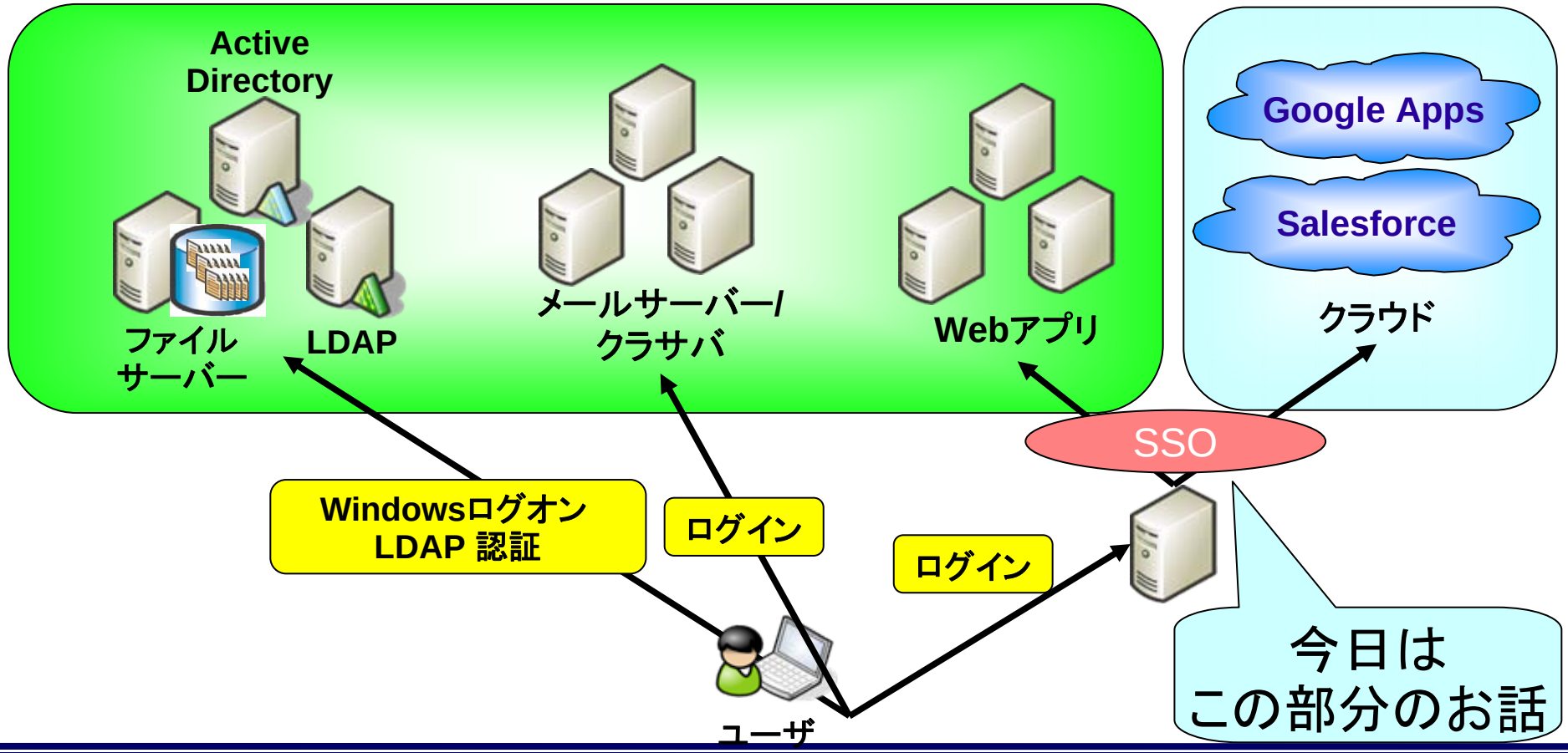
OSSTech

サービスを利用するには必ず必要な「認証」



SSO：シングルサインオンとは

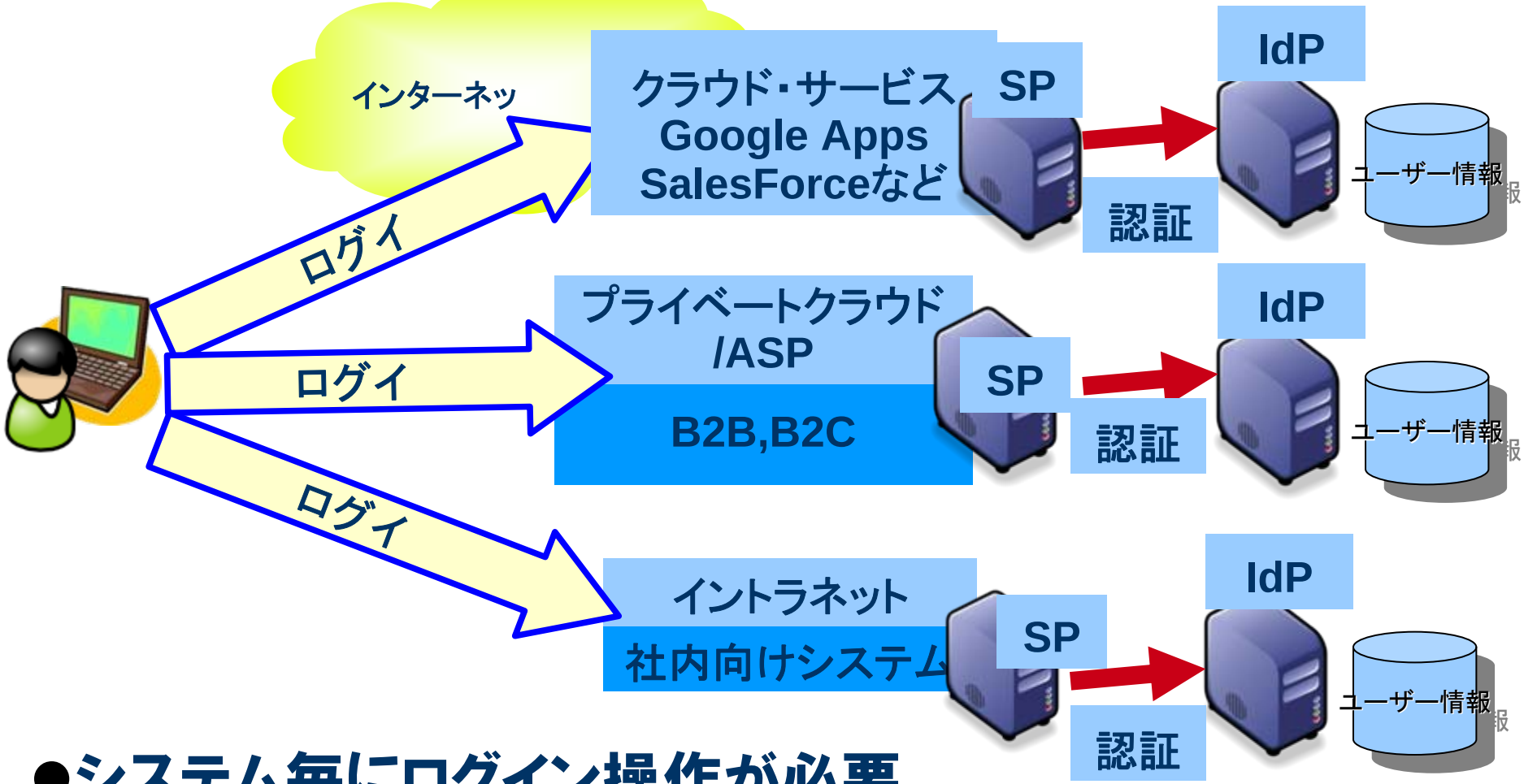
一度のログイン操作さえ完了すれば、複数のアプリケーションに認証操作することなくアクセスすることが可能になる。



SSO(シングルサインオン)とは

- １回のパスワード入力で複数のシステムやサービスを同時利用
- 「ID統合を使った統合認証」ではIDとパスワードの管理を1カ所でできるためユーザの追加も楽、社員が退社した場合に1カ所IDを削除すれば、すべてのシステムが利用不可となる
- 近年クラウドサービス(SaaS, PaaS, IaaS, HaaSなど)の普及により、(社外にある)サービス毎にID／パスワードを登録しなければならないケースが増えており、「ID連携による統合認証」を使わざるを得ないケースが増えている
- ところがこのID連携が費用の問題や技術的な問題で完全に実現されていない場合、例えば社員が退社した時に社内システムのIDを削除しても、SaaS側のIDが残っているとクラウド側のシステムは社外から使えてしまう、といった問題が起きてしまう

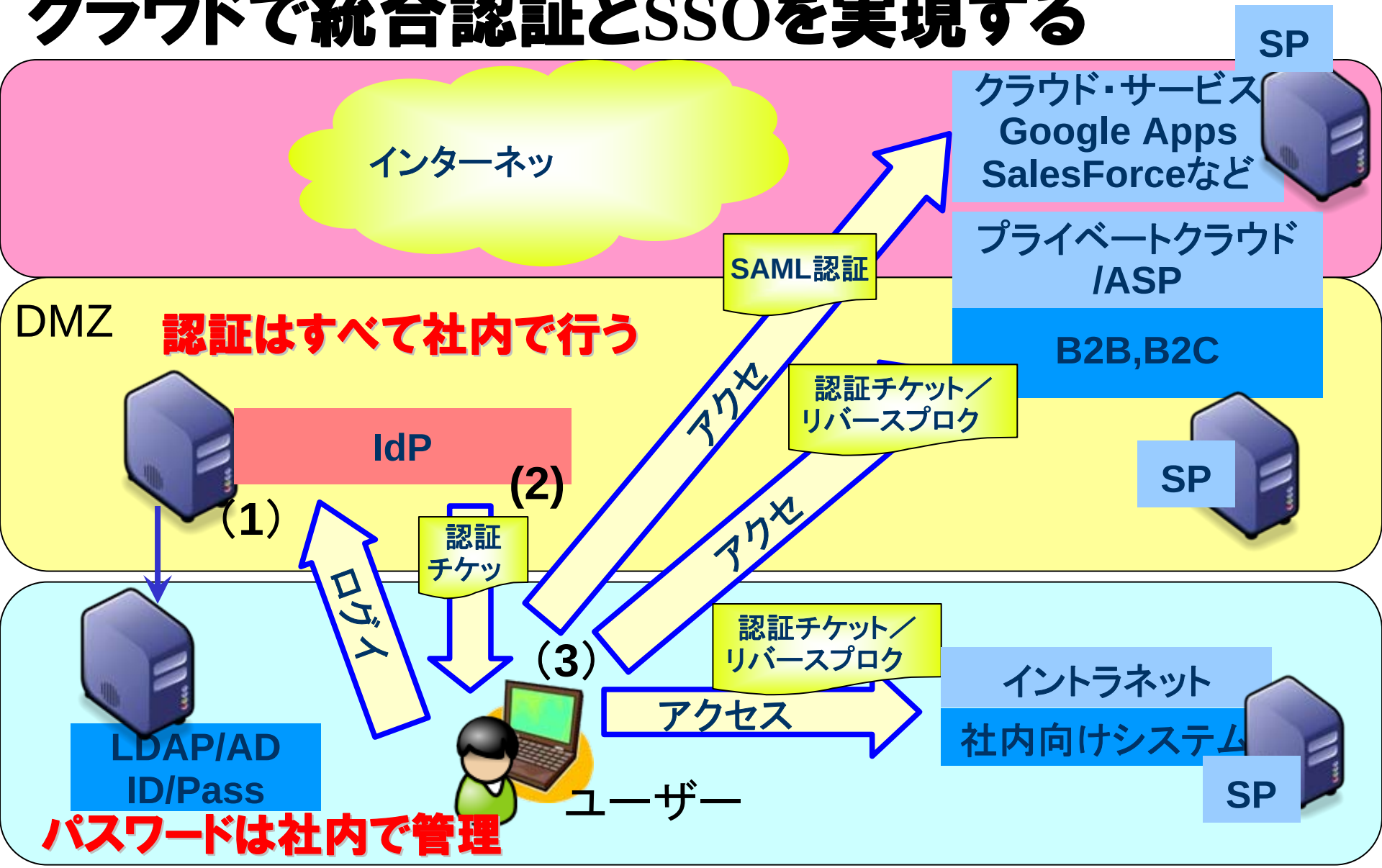
クラウドで統合認証ができていないと．．．



- システム毎にログイン操作が必要
- クラウドにID/パスワードとパスワードを置く必要がある

（パスワードを社外に置くと不正ログインされる危険性が高い）

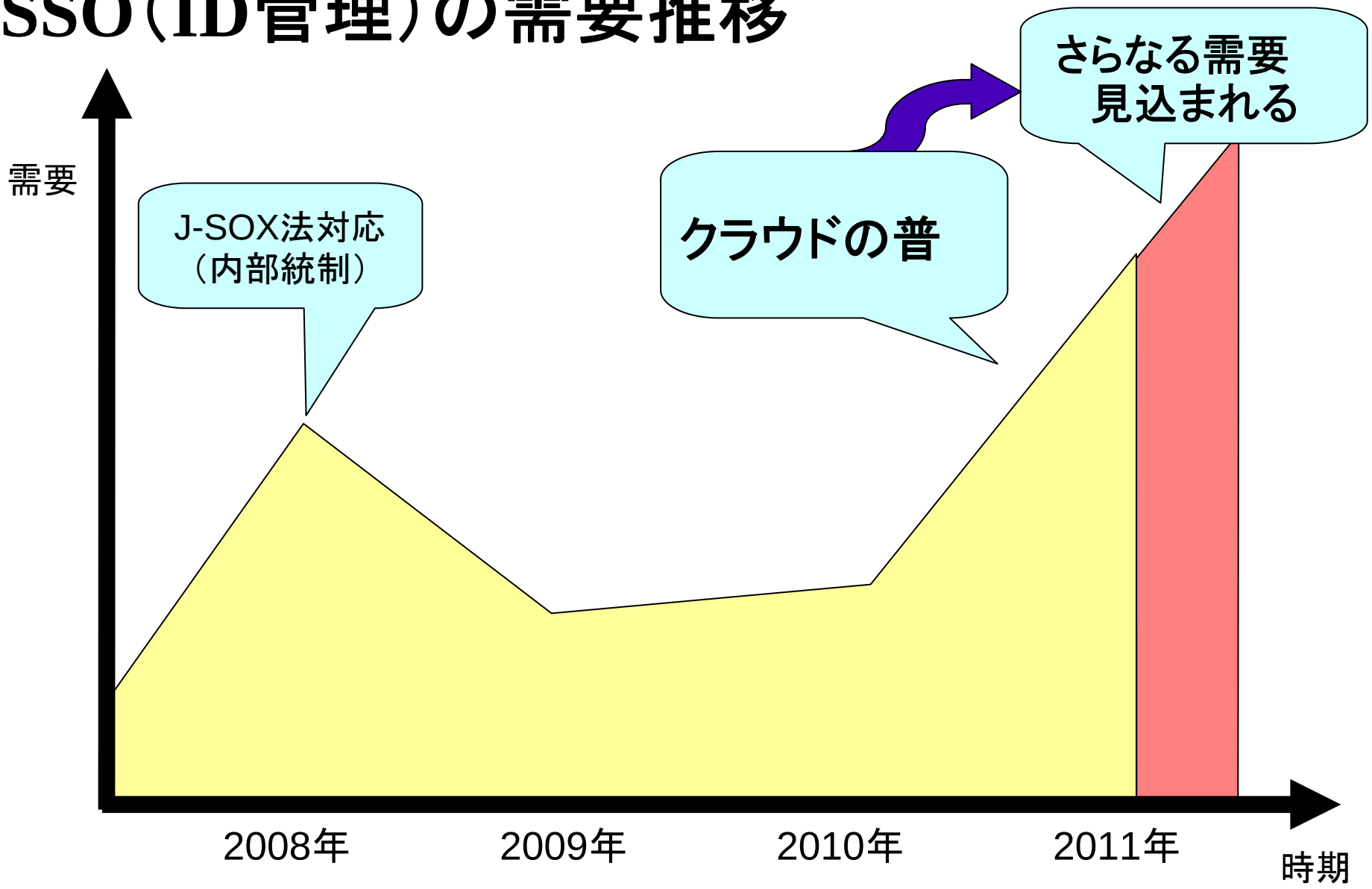
クラウドで統合認証とSSOを実現する



Part 3
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

OSSTech

SSO（ID管理）の需要推移



SSO(OpenAM)導入動向

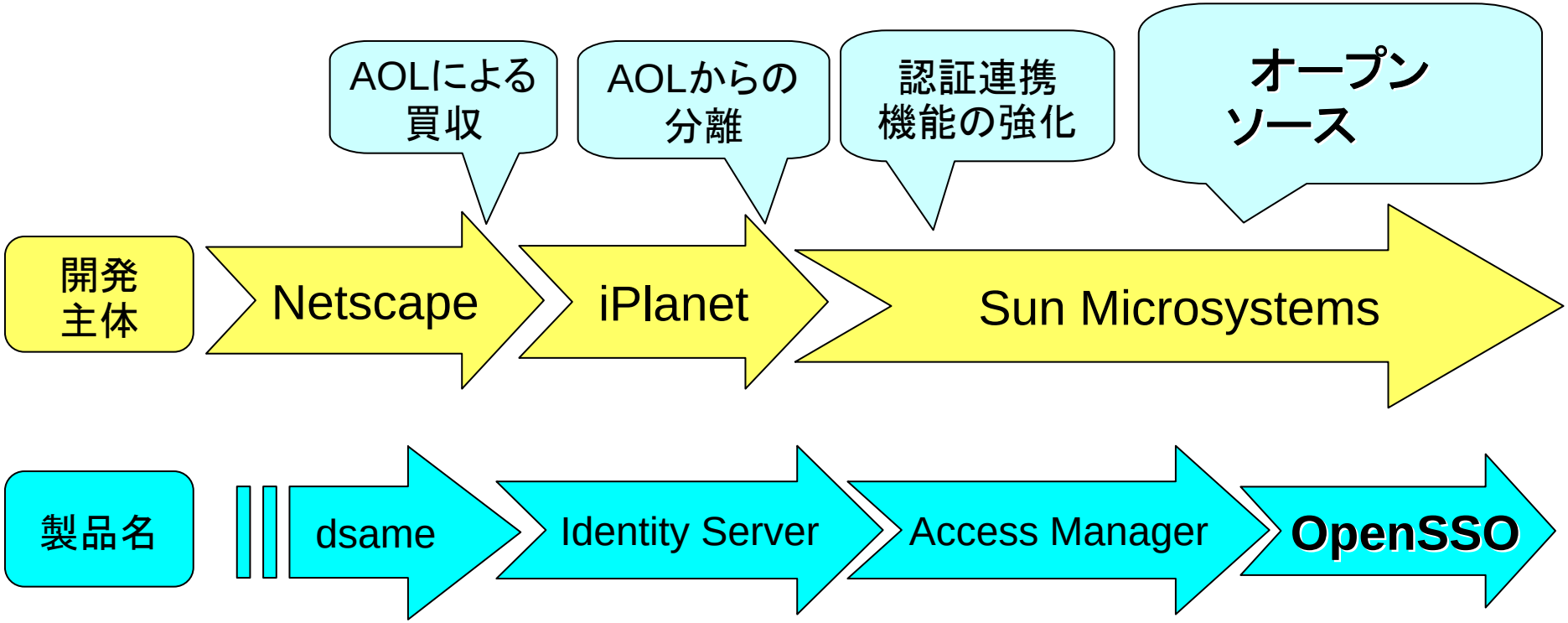
- クラウドの普及により、SSO(シングルサインオン)が急速に普及中
- IaaSやPaaSも増えつつあるが、やはりSaaSのGoogle Apps(大学／企業)とSalesforce(企業)をまず導入するケースが多い
- 企業ではSalesforceのセキュリティ強化を目的にOpenAM導入するケースが多い
- 大学ではGoogle AppsとイントラネットやShibbolethを連携させるケースが多い
- 企業ではM&Aや会社合併のために増えすぎたアプリやIDを統合するためにSSOを導入
- 今後は、IaaSやPaaSがさらに普及し、これらの上で構築された社内向け個別アプリのSSOが普及しそう

Part 4
OpenAM（旧OpenSSO）の紹介

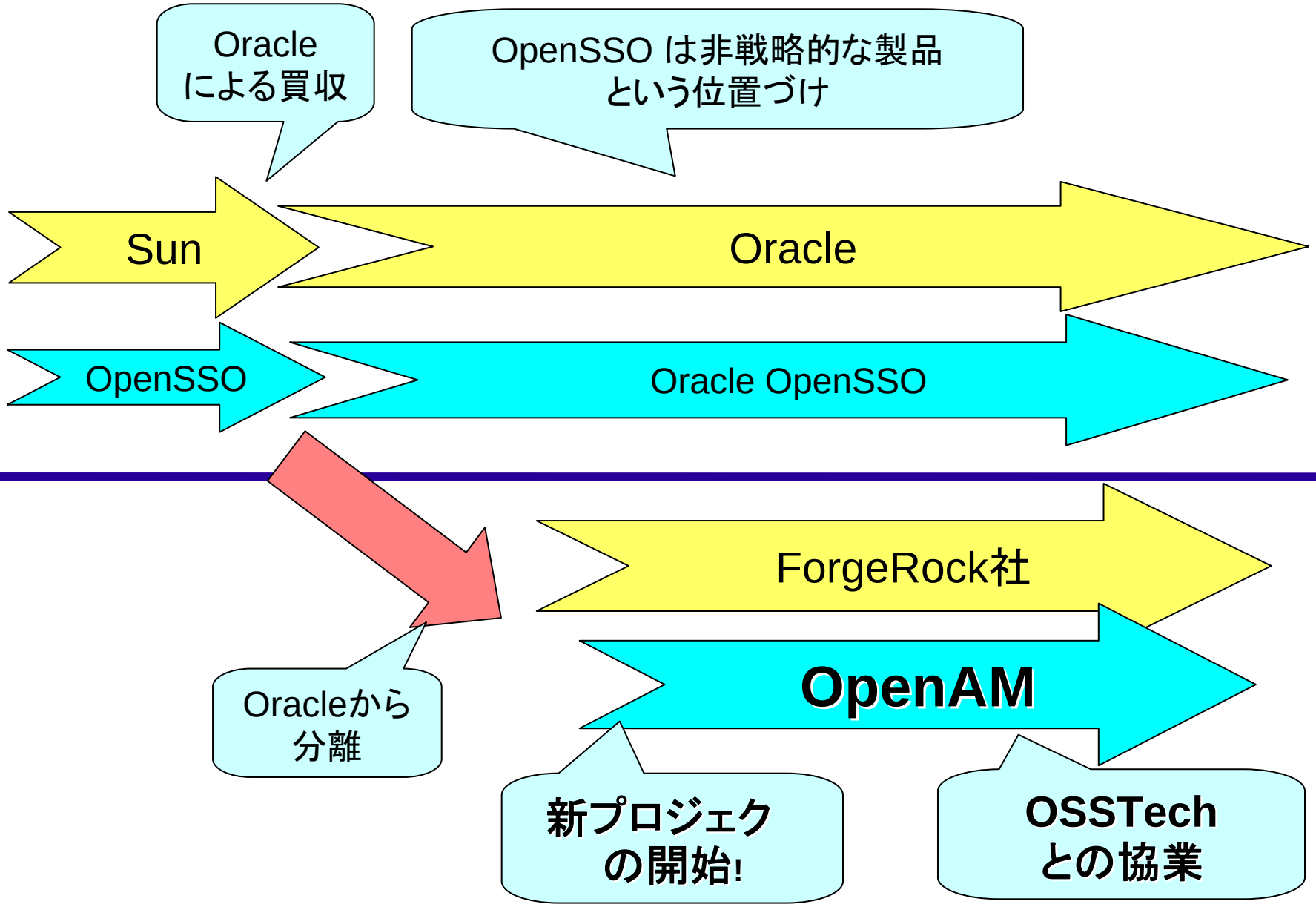
OpenAMとは

- 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

Part 5
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）

Part 6
OpenAMが提供する
シングルサインオン方式

シングルサインオン方式の詳細(1)

- SAMLによるシングルサインオン
  - Secure Assertion Markup Lauguage
  - 認証、認可、ユーザ属性情報などをXMLで送受信するためのフレームワーク
  - 標準化団体OASISにより策定
  - GoogleApps、Salesforceなどが採用

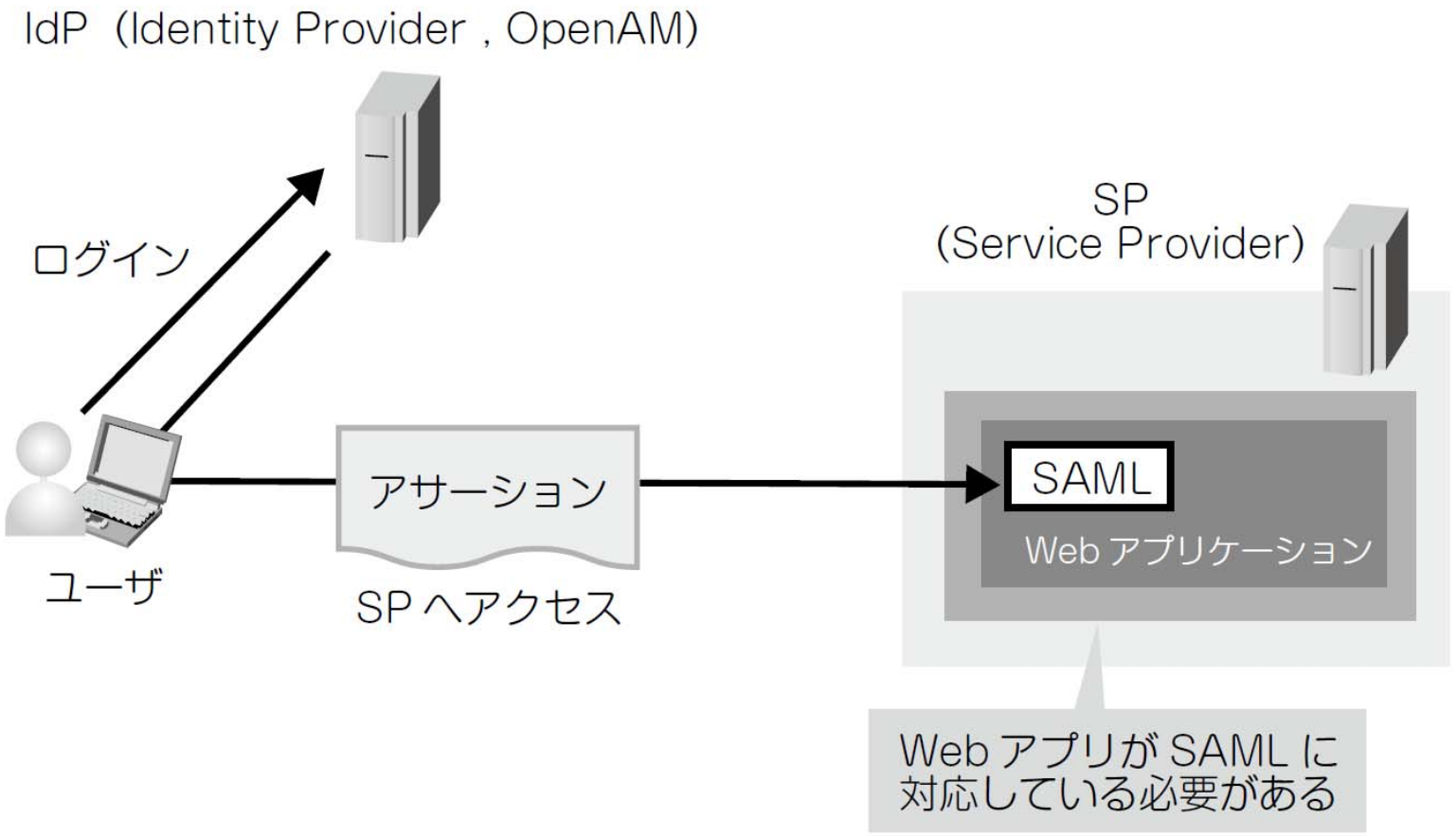
- エージェント方式
  - SSO対象のWebアプリが動作するサーバー上にアクセス制御用のモジュールを配置する方式
  - サーバーのバージョンに影響を受ける

シングルサインオン方式の詳細(2)

- リバースプロキシ方式
  - リバースプロキシを使用してアクセス制御を行う
  - ユーザーデータの受け渡しはHTTPヘッダーを利用
  - SSO対象Webアプリのバージョンや設定変更の影響が少ない
  - リバースプロキシが性能上のボトルネックになる可能性がある

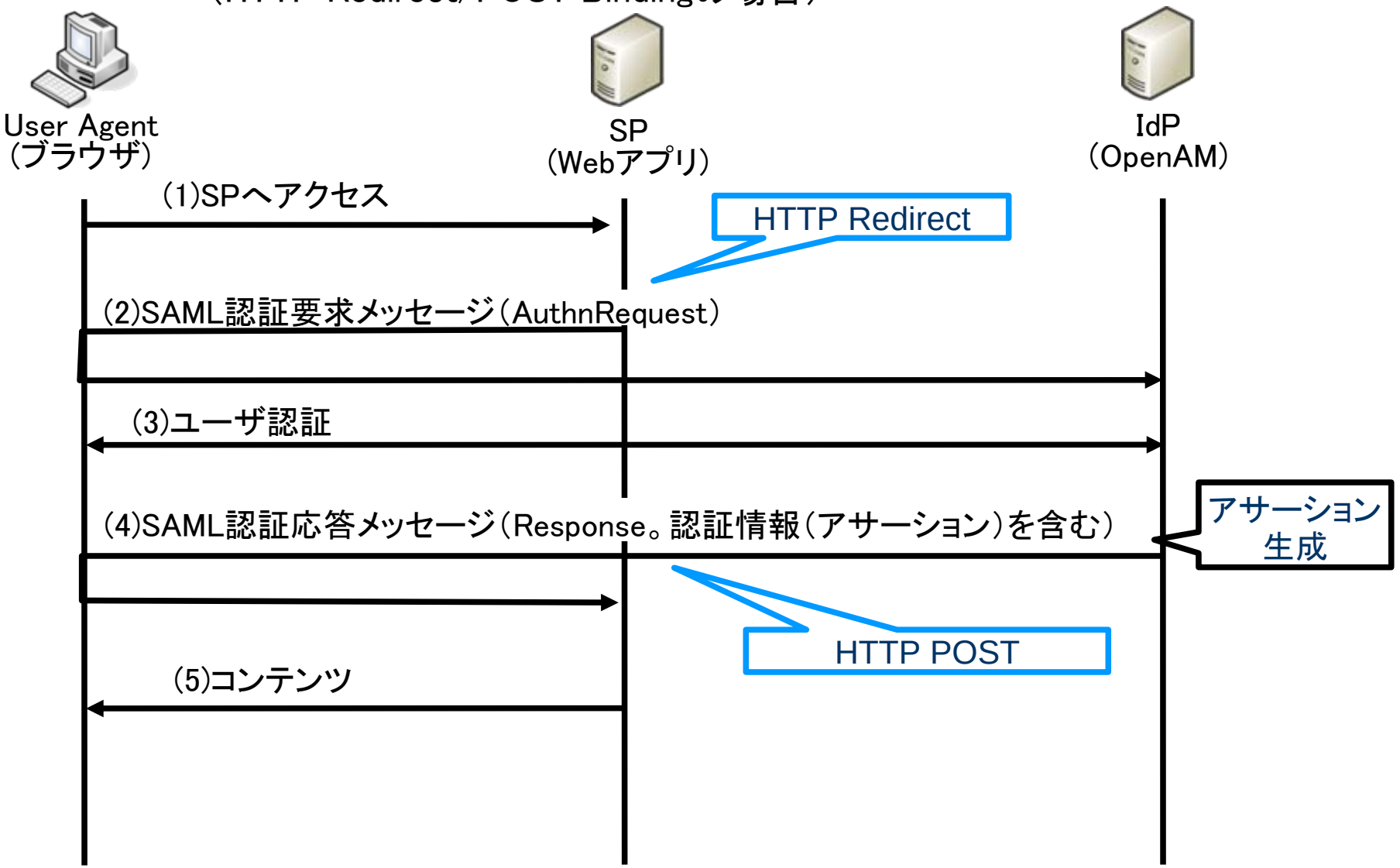
- 代理認証方式
  - SSO対象Webアプリの既存ログイン画面に対して、OpenAMがユーザーの代理でログインID/パスワードを送信する
  - SSO対象Webアプリの改修が不要
  - 細かなアクセス制御はできない(ログイン処理の代理実行のみ)

SAMLによるシングルサインオン

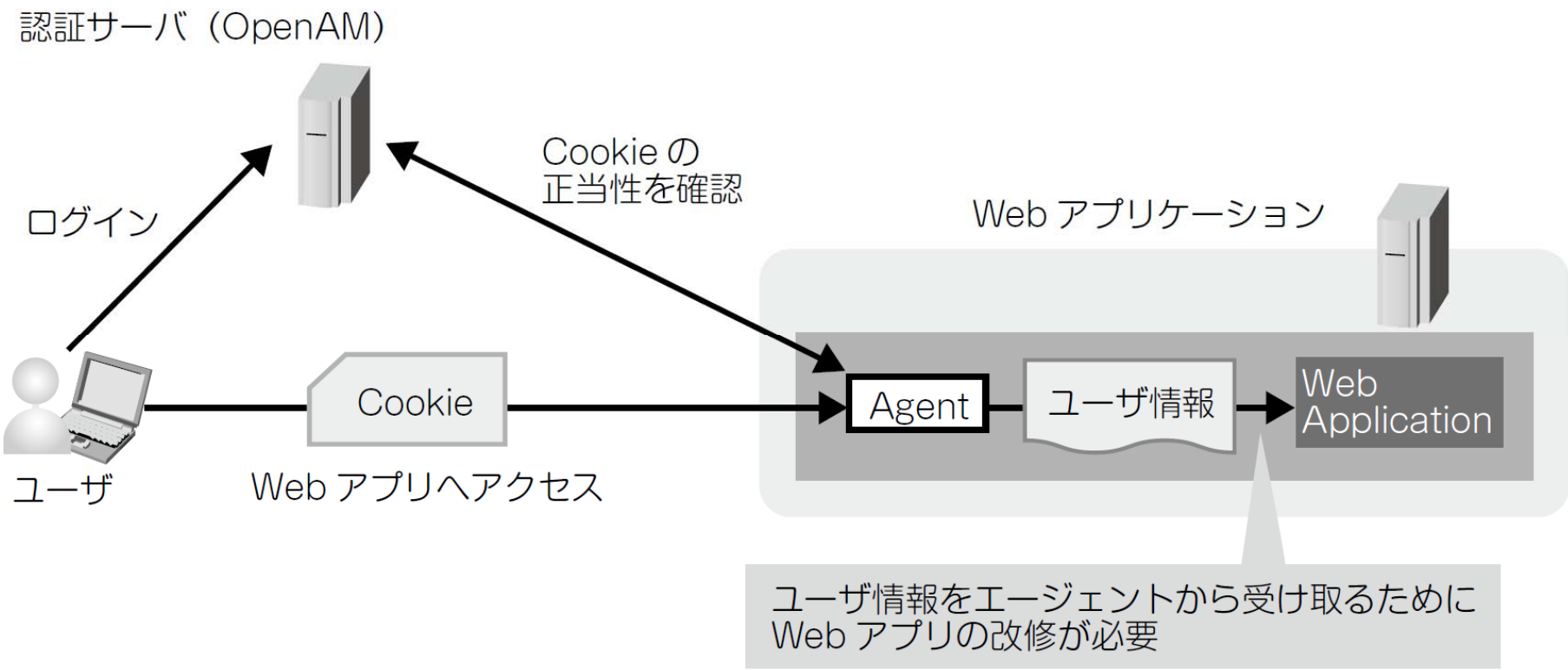


SAMLによるシングルサインオン

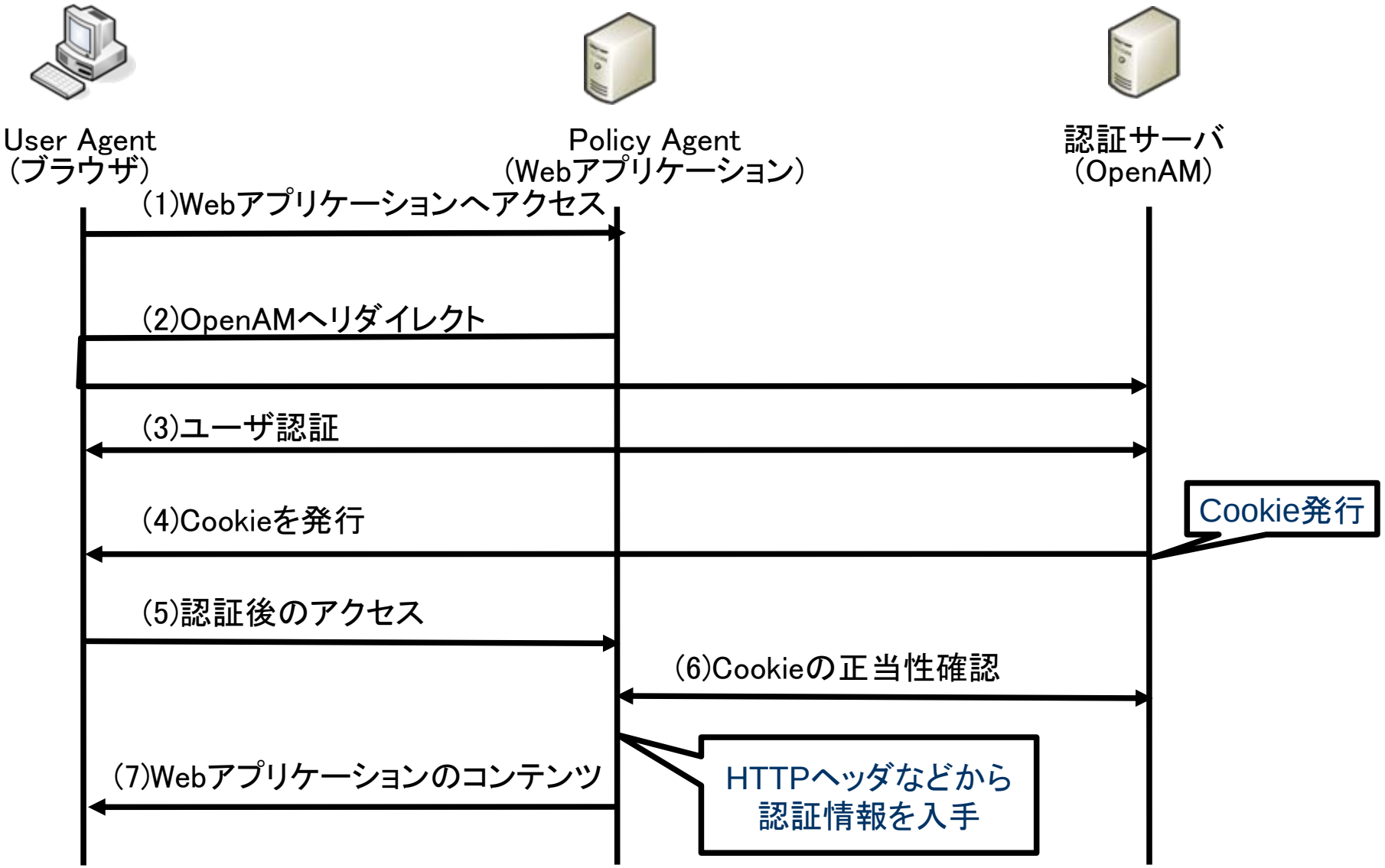
（HTTP Redirect/POST Bindingの場合）



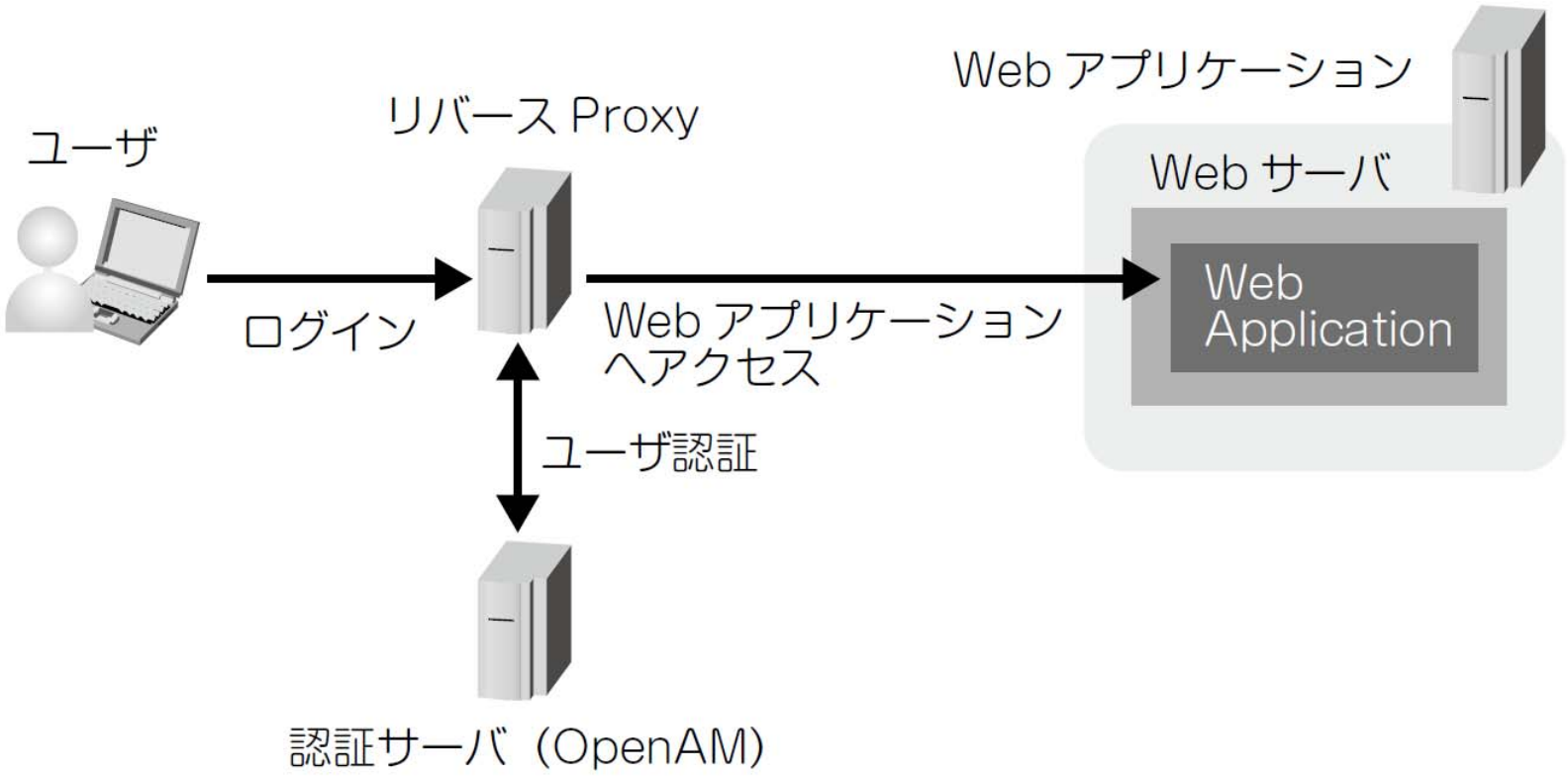
エージェント型



エージェント方式によるシングルサインオン

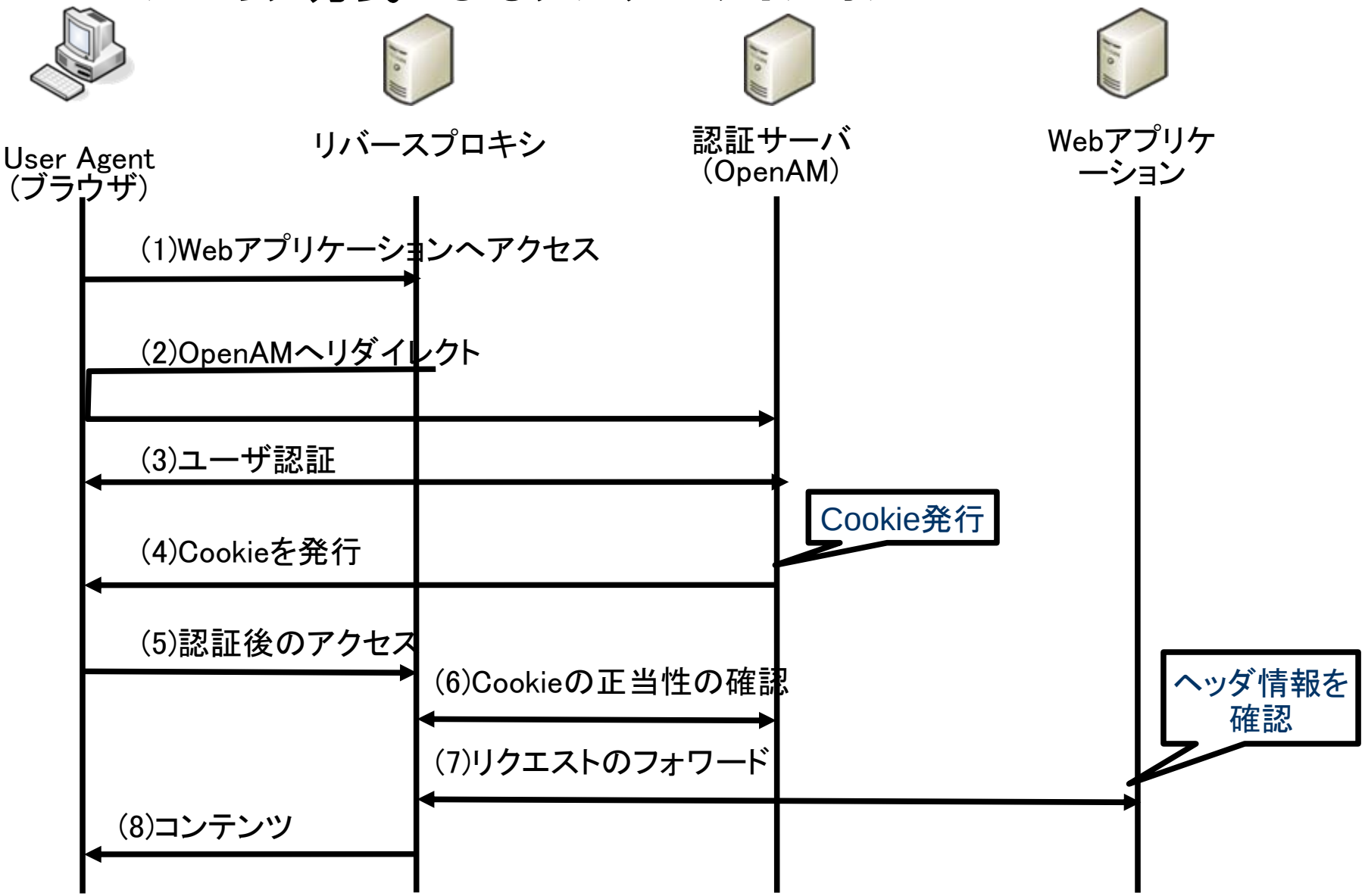


リバースプロキシ型

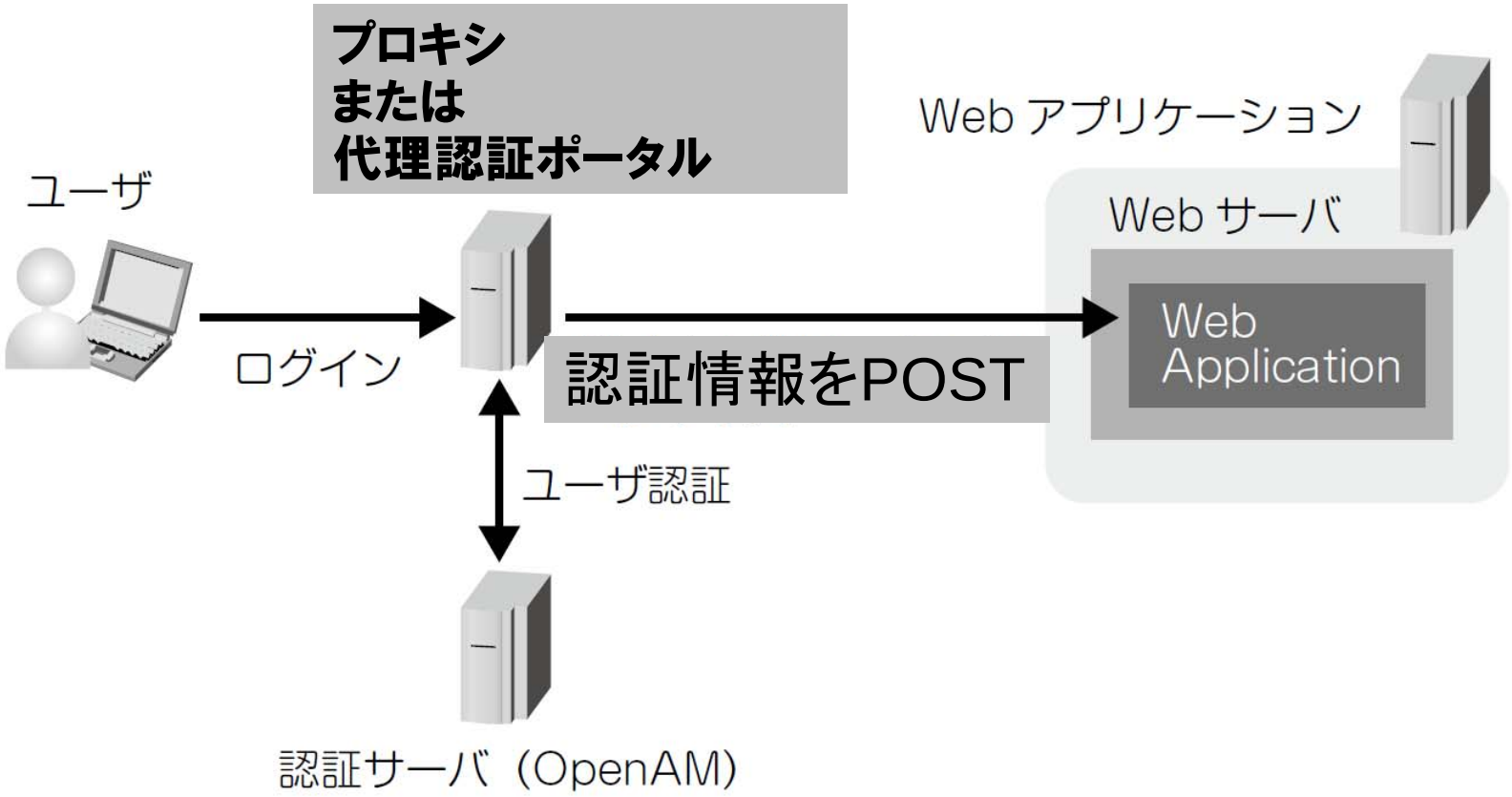


- 後方のサーバを仮想的に1台に見せることも可能
- 認証とサーバへのアクセス制御はプロキシサーバで行う
- 後方のサーバは認証なしもしくはBasic認証でアクセス可能

リバースプロキシ方式によるシングルサインオン

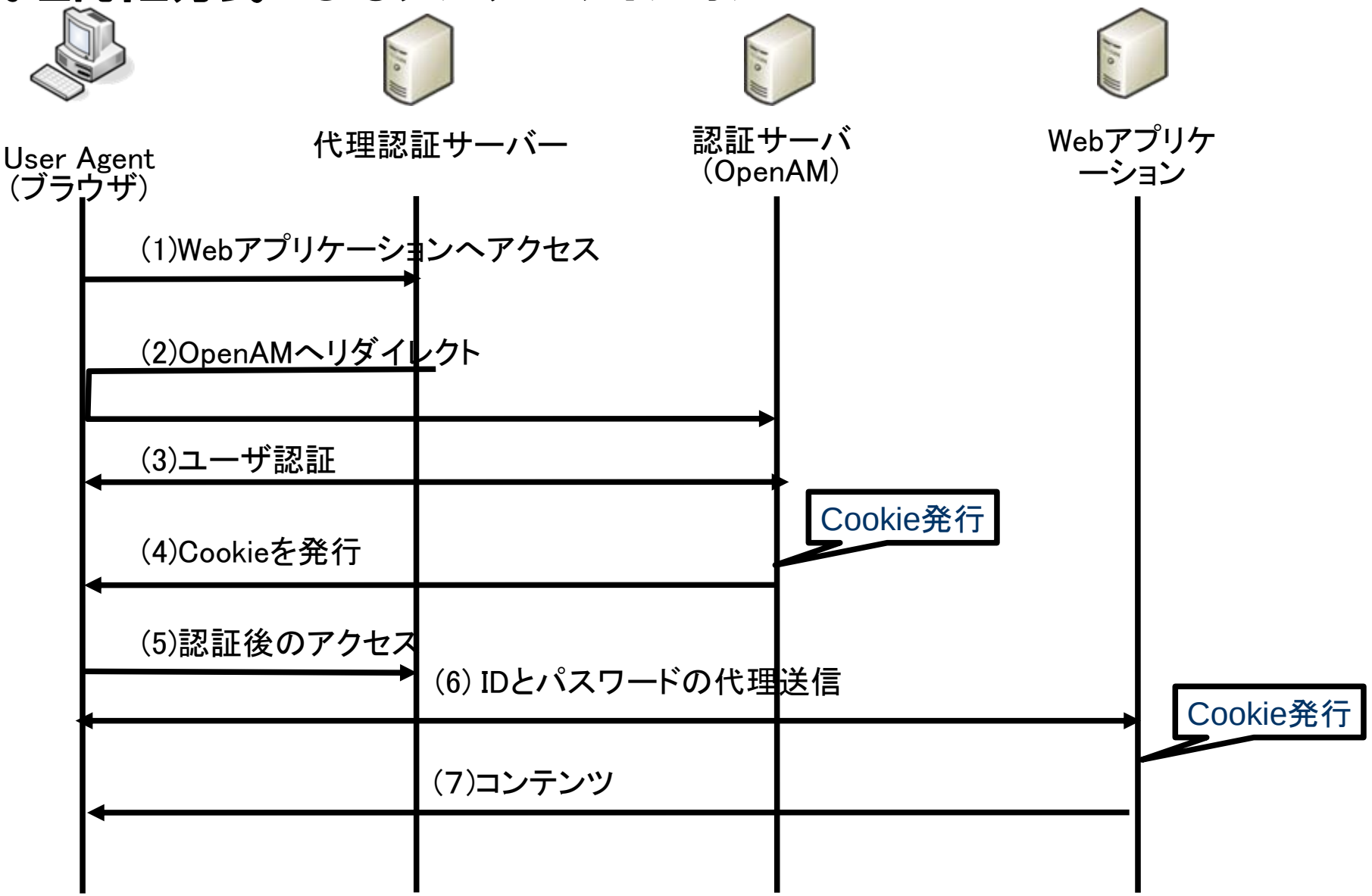


代理認証方式



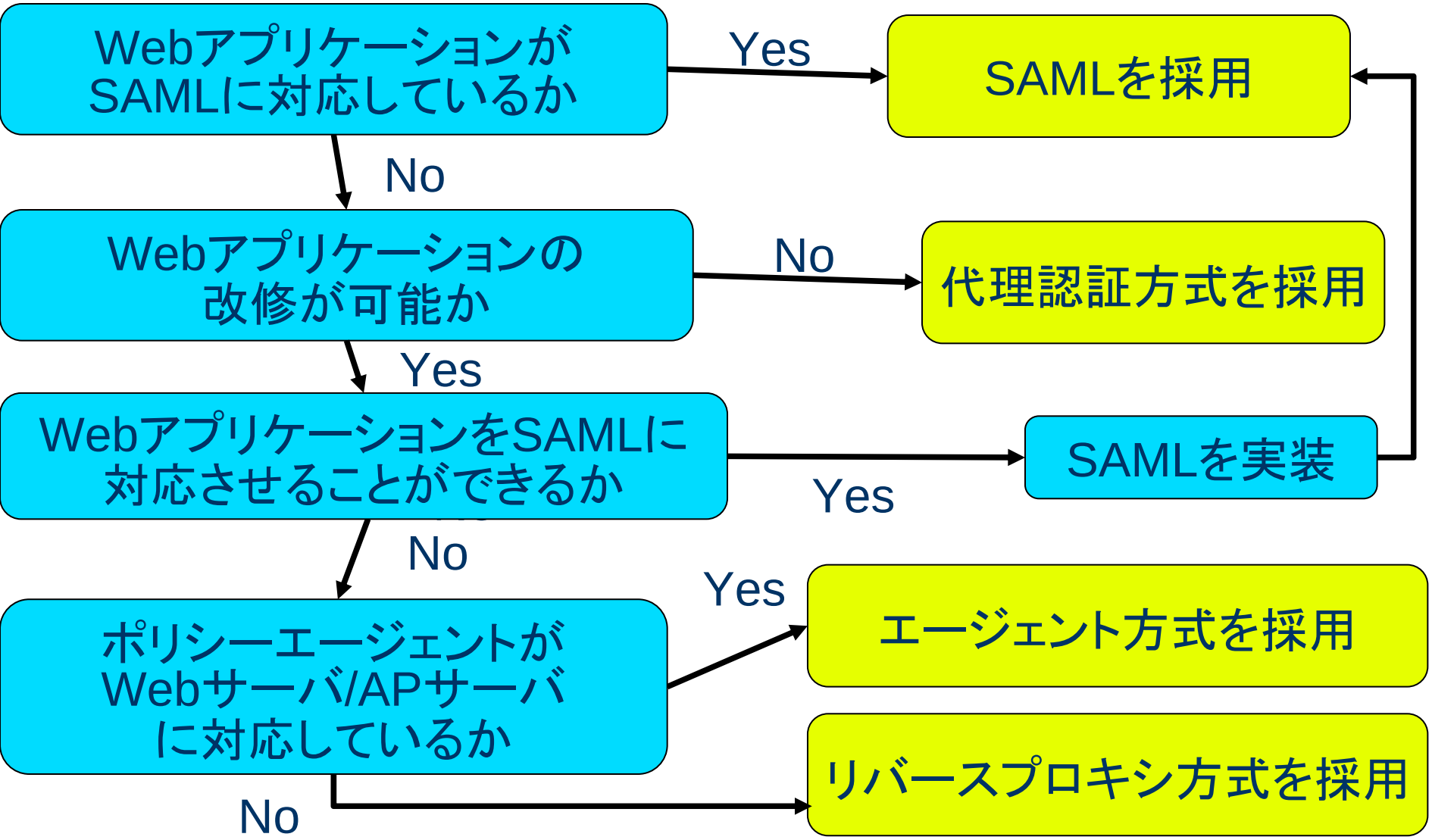
- 認証サーバで認証したら後方のサーバへ認証情報をPOSTして認証する
- 後方のサーバが独自の認証画面を持っていてもSSO可能

代理認証方式によるシングルサインオン



方式	Webアプリケーションの改修	長所・短所
SAML	SAMLに対応していれば不要	■標準的な仕様に準拠したSSOシステムを構築可能。他製品との互換性が高い ■認証サーバー(IdP)を社内に設置し、クラウドサービスであっても、アクセスを社内のみからに制限することも可能(サービスのSAML実装に依る) ■WebアプリケーションがSAMLに対応している必要がある
エージェント	必要	■Webアプリケーションへの全ての通信をエージェントがフックするため、細かなアクセス制御が可能 ■サーバーに対応したエージェントが必要
リバースプロキシ	必要	■Webアプリケーションへの全ての通信をリバースプロキシがフックするため、細かなアクセス制御が可能 ■リバースプロキシがボトルネックになる可能性もある
代理認証	不要	■既存Webアプリケーションの改修が不要 ■代理認証不可能な場合もある

シングルサイオン方式の採用基準



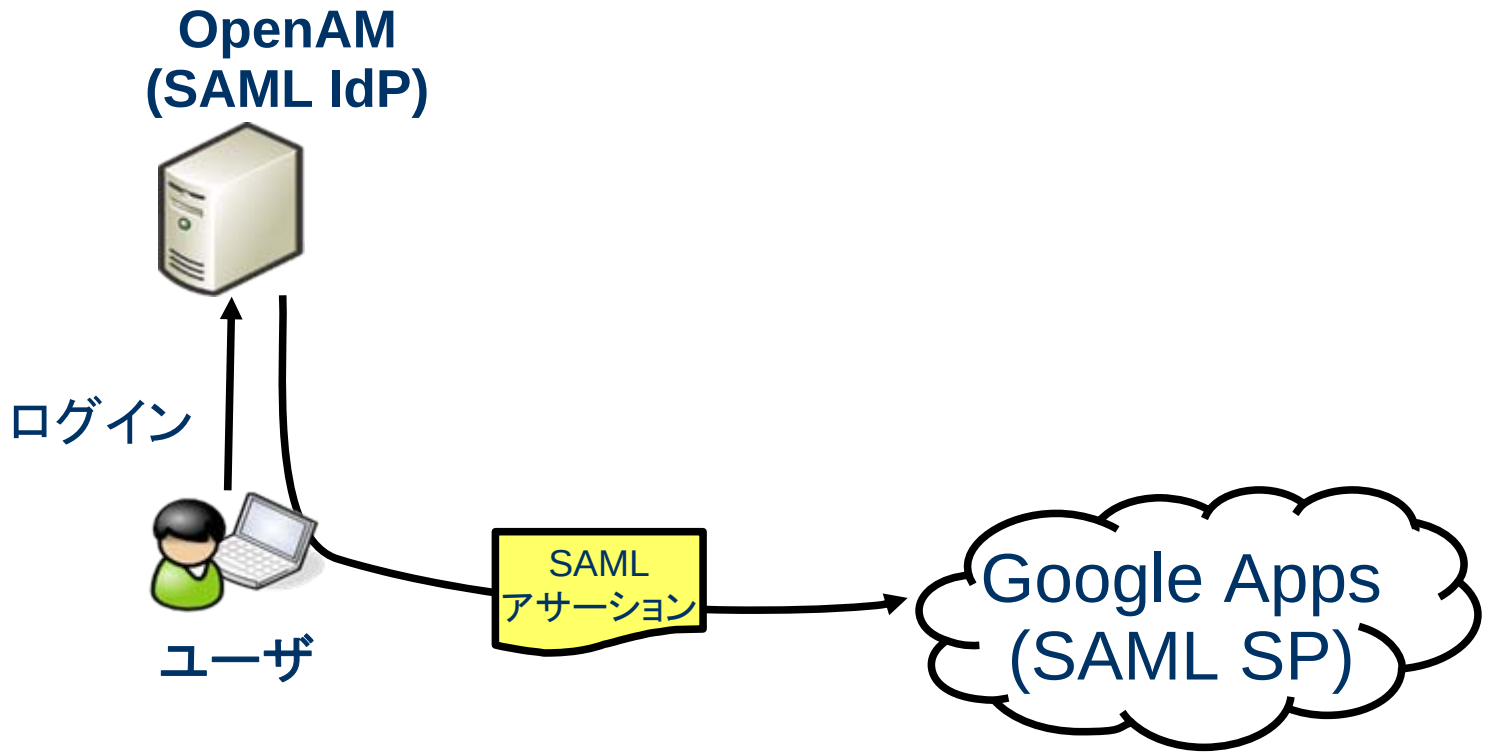
本当はやってはいけない「代理認証」

「既存アプリに手を入れられない」という理由で代理認証を採用するユーザーは多いが本当はやってはいけない！

- IDとパスワードを(HTTPSでも)ネットワークに何度も流すのは良くない。(SSO入り口の1カ所に限定すべき)
- 代理認証はイントラネットのみに限るべき
- クラウドへの代理認証は危険
- SAMLに対応しているGoogle AppsやSalesforceに対して、代理認証は絶対にやってはいけない！
  (SAMLを使ってIdPを社内に置けばパスワードはクラウドに流れない)

Part 7
Google Appとの連携
設定手順

Google AppsへのSSO

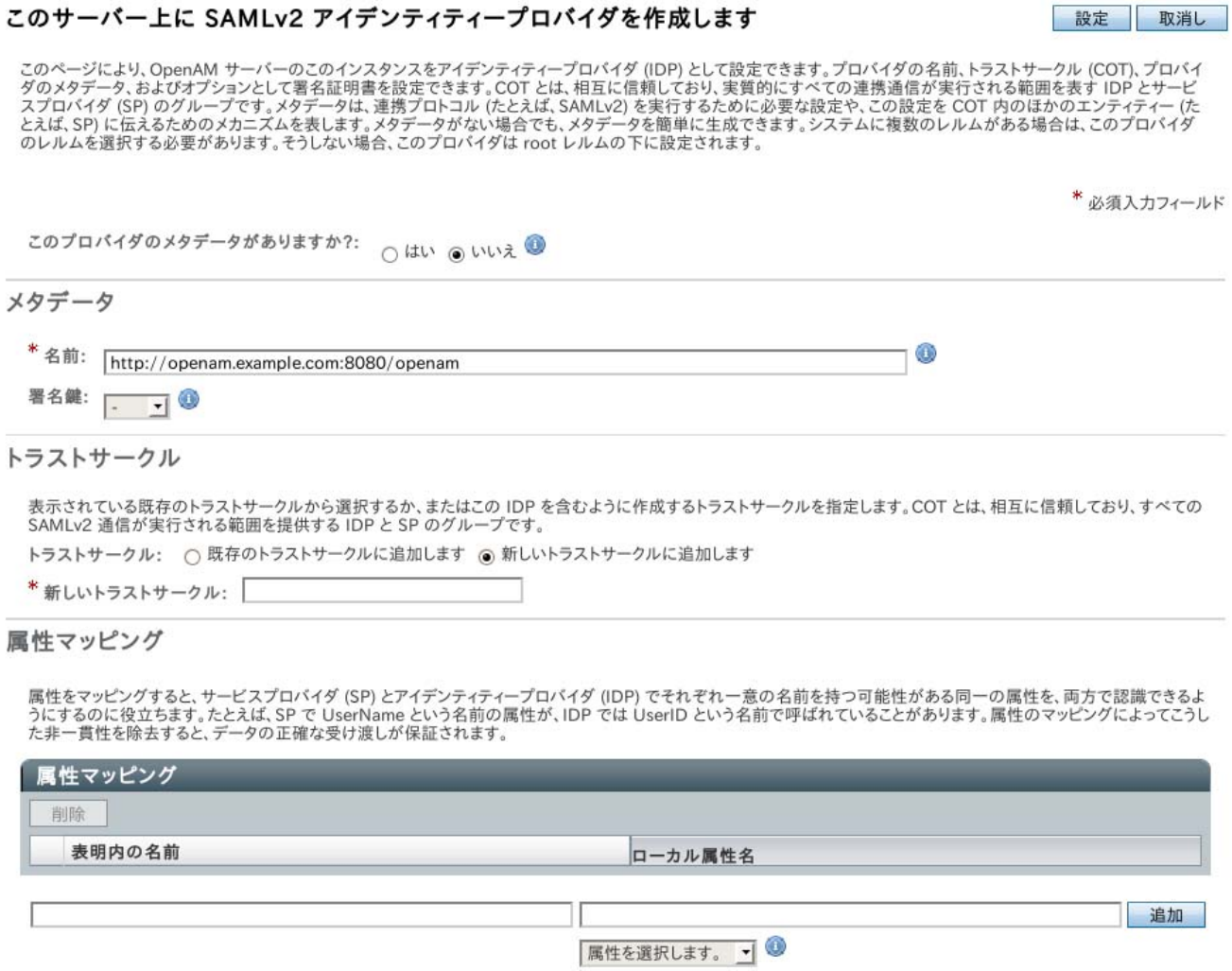


設定手順

OpenAMのメニューに従い設定を行う

- OpenAMをIdPとして設定する
  - 新規にトラスト・サークルを作成する
- Google AppsをSPとして設定する
  - OpenAM側での設定
  - Google Apps側での設定
    - OpenAMが表示する値をGoogle Appsに反映

手順1： IdPの作成



手順2： Google AppsをSPとして登録

手順3： Google Appsで設定するSAMLパラメータ

手順4： Google AppsのSSOを有効化

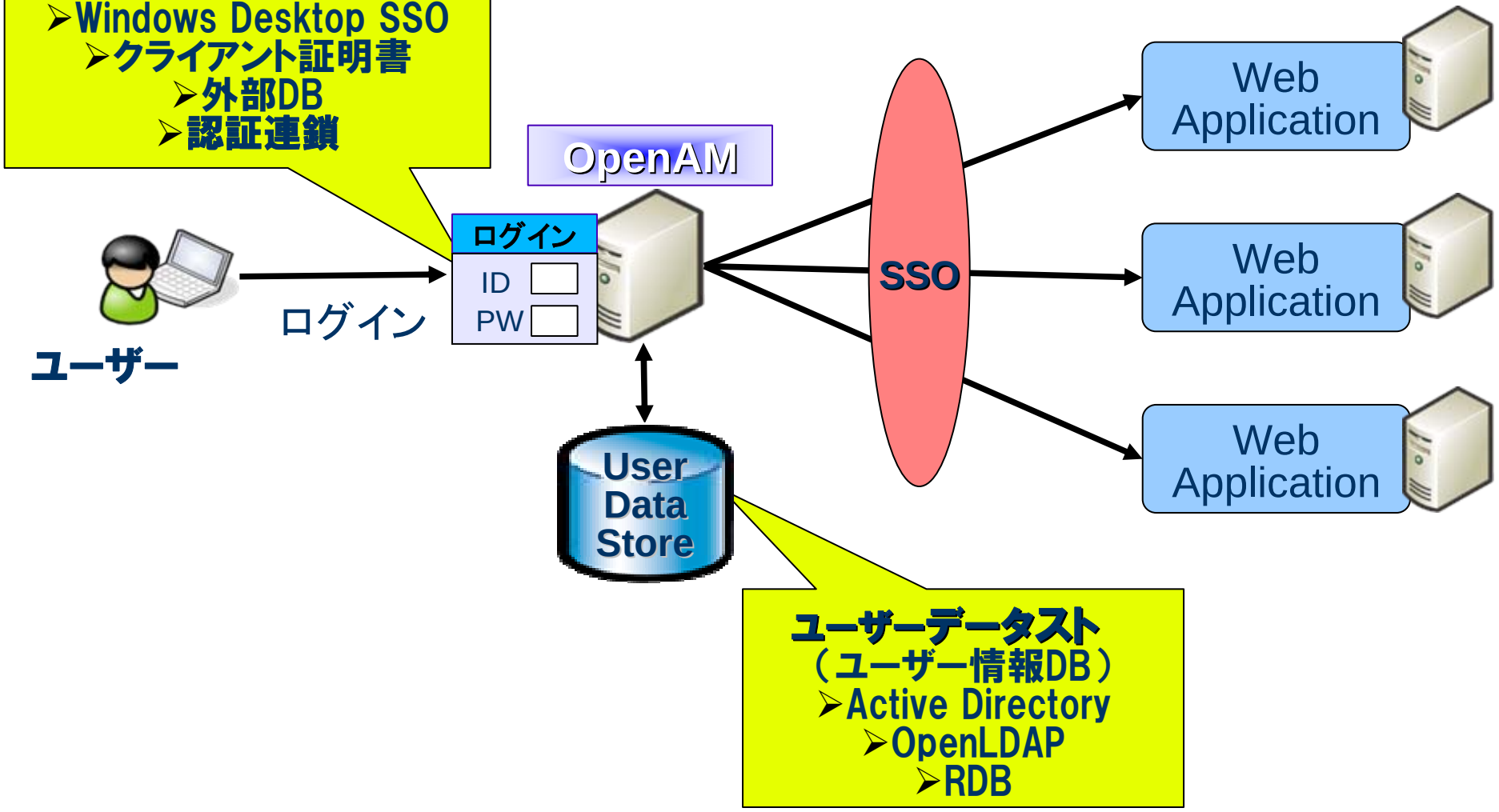
手順5： Google Appsのシングルサイン設定

Part 8
OpenAMの機能(その2)

認証方式(多様素認証)

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
- 指静脈認証
- 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（ユーザー情報DB）
- Active Directory
- OpenLDAP
- RDB

OpenAMの機能 - 認証方式

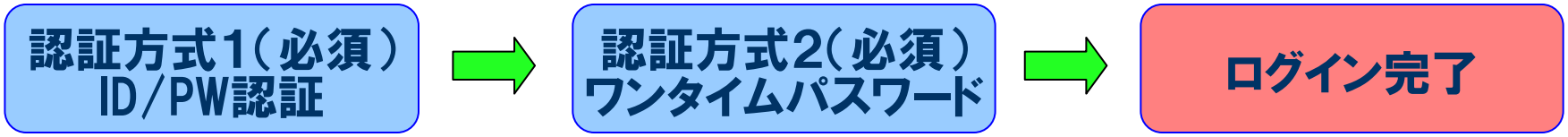
- 基本的には OpenAM のユーザーデータストアに保存された ID/パスワードにより認証を行なう
- ユーザー認証時に外部のデータベースを参照することも可能(更新できない参照のみのものでも可能)
  - LDAP、Active Directory、RADIUS、RDB(JDBC)
- よりセキュアな認証方式も使用可能
  - ワンタイムパスワード(電子メールを利用)
  - クライアント証明書による認証
  - Windows Desktop SSO(統合Windows認証)
- 複数の認証方式を組み合わせて使用可能:**認証連鎖**

OpenAMの機能 - ユーザー情報DB

- 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(更新権限が必須)
    - Active Directory
    - Open LDAP
    - 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(OpenAMから対応)

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により個々の認証方式の欠点を補完
- 認証連鎖
  - 複数の認証方式を組み合わせて利用可能
  - 認証方式にはそれぞれ適用条件を指定する
    - 必須：失敗したらそこで終了
    - 十分：成功したらそこで終了
    - 必要：成功しても失敗しても次に継続
    - 任意：認証結果には関係しない付随的な処理



多要素認証

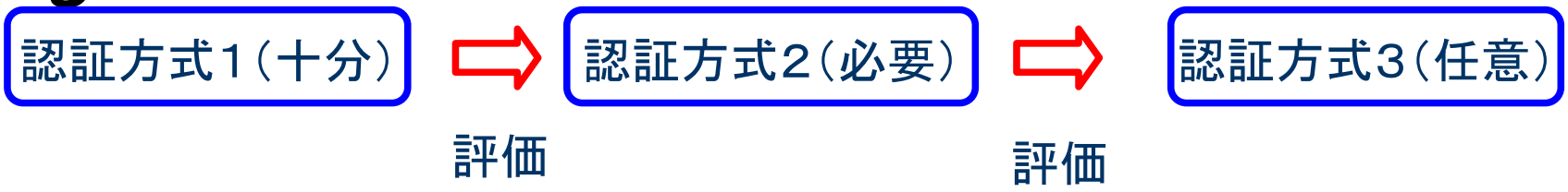
複数の認証方式を組合わせて認証を行うことにより個々の認証方式の欠点を補完

- 厳密なユーザ認証
  - 異なるタイプの認証方式を組合わせることが重要
- 使い勝手の向上
  - いつも同じ認証方式が使えるとは限らない
  - 状況により要求される認証の精度が異なる
- 認証方式間での連携
  - 組合わせて使うことを前提にしている認証方式もある

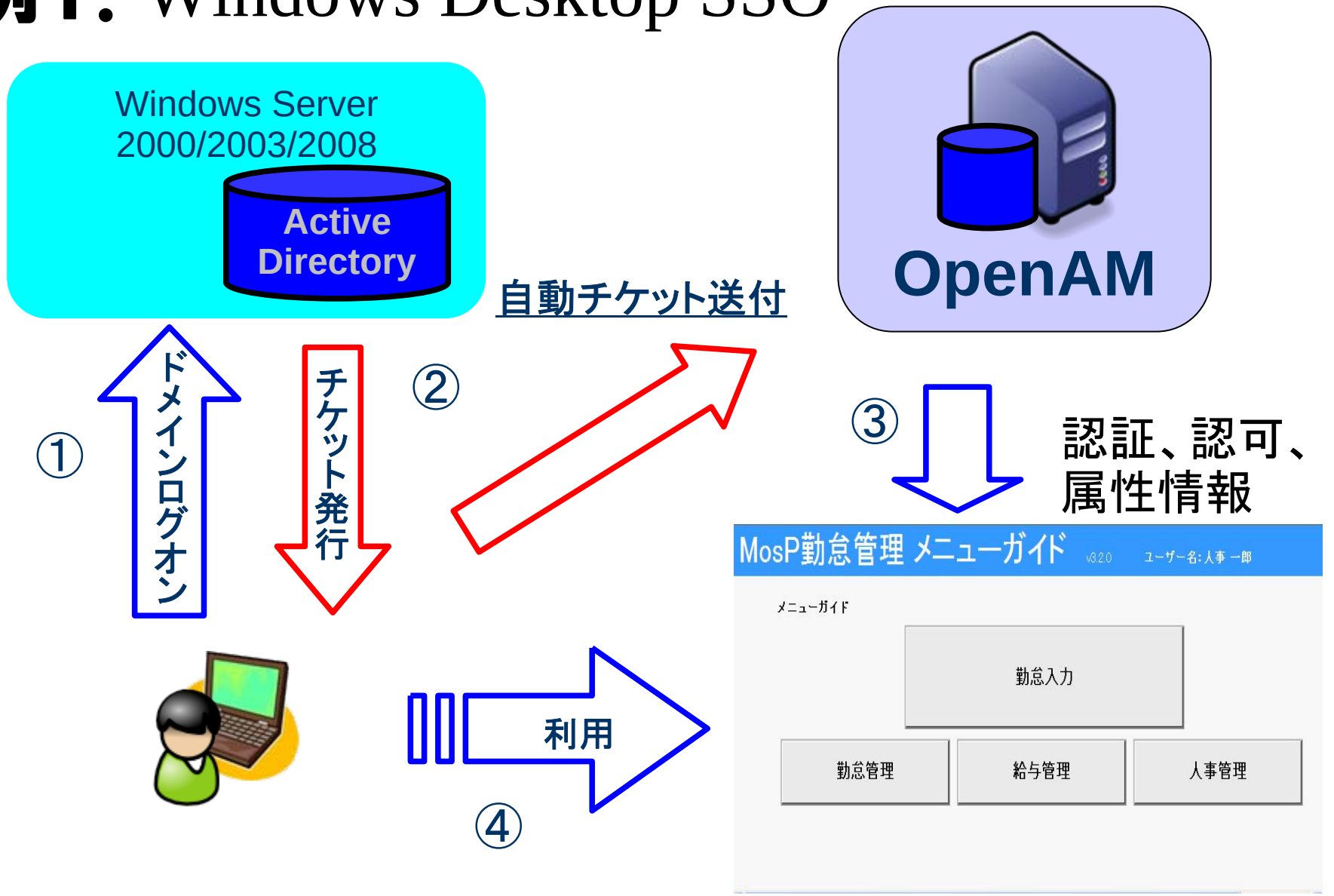
認証連鎖

認証方式を組合わせる方法を指定する

- **認証方式にはそれぞれ適用条件を指定する**
  - **十分：成功したらそこで終了**
  - **必要：成功しても失敗しても次に継続**
  - **必須：失敗したらそこで終了**
  - **任意：認証結果には関係しない付随的な処理**
- **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**



例1. Windows Desktop SSO

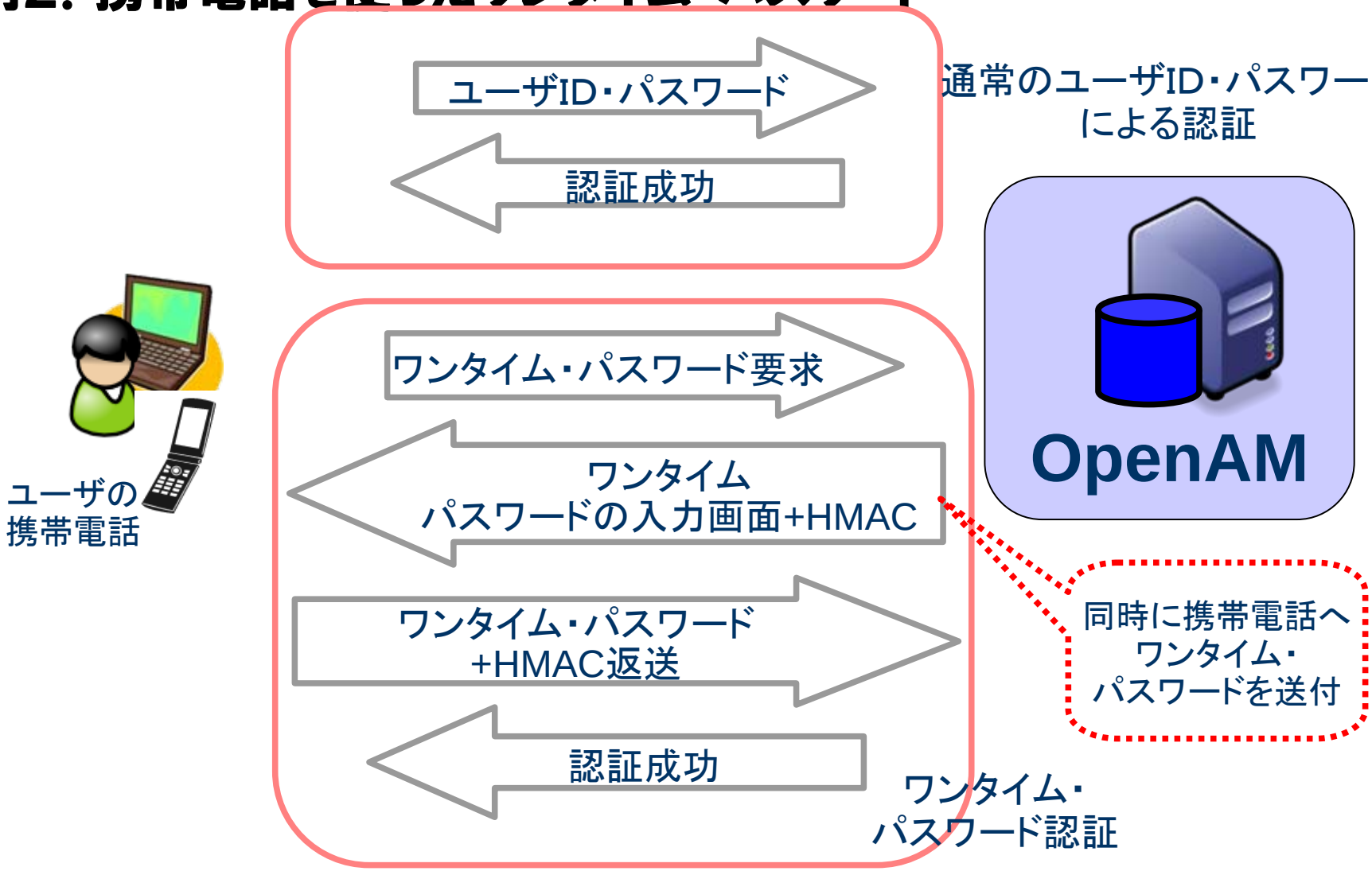


例1. Windwos Desktop SSO

Windowsドメインログオンするだけで Webアプリケーションにも SSOが可能になる便利な方式

- いつも、全てのユーザがドメインログオン可能であるとは限らない
  - リモート・アクセスの場合
  - 非常勤社員の場合
- 通常のユーザID・パスワードによる認証と組み合わせて以下のように認証連鎖構成する
  - Windows Desktop SSO: 十分
  - ユーザID・パスワードによる認証：必須

例2. 携帯電話を使ったワンタイム・パスワード



例2. 携帯電話を使ったワンタイム・パスワード

- 所持物認証と知識認証の組合わせによる厳密なユーザ認証が可能
- 携帯電話を使うことによる利点
  - 導入コストの低減
  - 所持品の軽減
- フィッシングへの対応
  - HMAC(RFC2104:Keyed-Hashing for Message Authentication)を利用
  - 両方のパスワードが盗まれた場合は問題
  - 参考:RSAセキュリティ(株)による月例記者会見

http://internet.watch.impress.co.jp/docs/news/20100728_383861.html

応用例

- Windows Desktop SSOによる認証は便利なのでぜひ使いたいが全てのユーザがドメインログオン可能とは限らない
- ワンタイム・パスワードは厳密な認証が出来る点は良いが、いつも携帯電話を開いてパスワードを確認するのは面倒だ

- **2つを組合わせることにより便利かつ厳密な認証を行うことが可能**
  - **Windows Desktop SSO: 十分**
  - **ユーザID・パスワードによる認証： 必須**
  - **ワンタイム・パスワードによる認証： 必須**

アダプティブ・リスク認証モジュール

リスク評価に基づく認証強度の選択

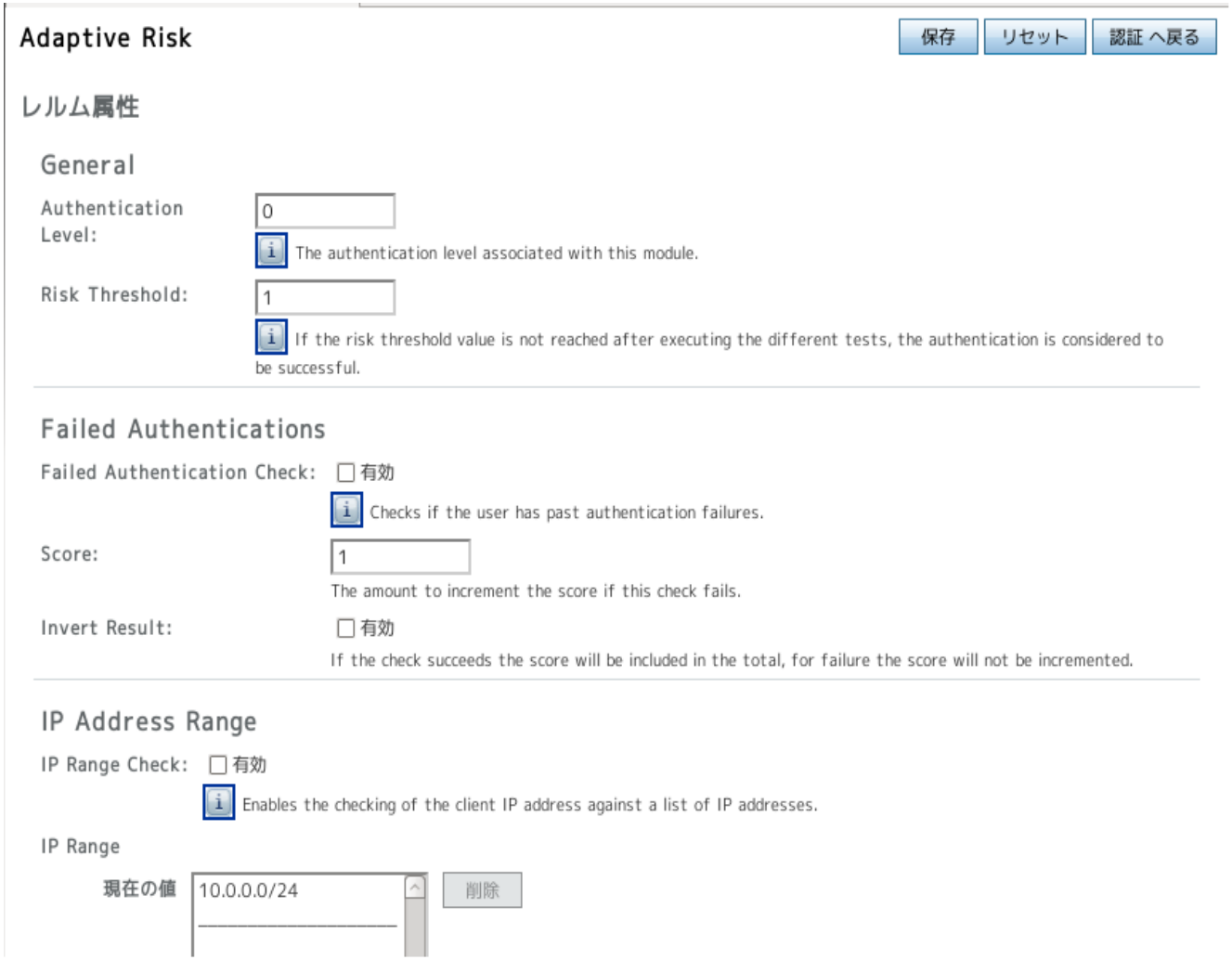
アダプティブ・リスクの考え方

- 認証時にリスクを評価することによりリスクに見合った認証方式を動的に追加
  - Risk Based 認証とも呼ばれる
  - リスクの評価
    - 予め各リスクについて重み付けを行う
    - 認証時にすべてのリスクについてそれらを合算する
    - 既定の閾値を超えた場合は認証失敗とする

リスクの例

- リスクが高いと評価される例
  - パスワードを間違えたユーザからのアクセス
    - 最終的に正しいパスワードを入力したとしてもリスクは高い
    - アカウント・ロックとの併用／代用
  - 長期間アクセスがなかったユーザからのアクセス
  - 特定のIPアドレスの範囲からのアクセス
    - 例：社外からのアクセス
  - 特定の地域からのアクセス
    - 例：日本国外
  - いつもとは異なる端末からのアクセス（複数可）
  - いつもとは異なるIPアドレスからのアクセス（複数可）
  - 特定の属性を持つユーザからのアクセス
    - 例：正社員でない

アダプティブ・リスク認証モジュールの設定

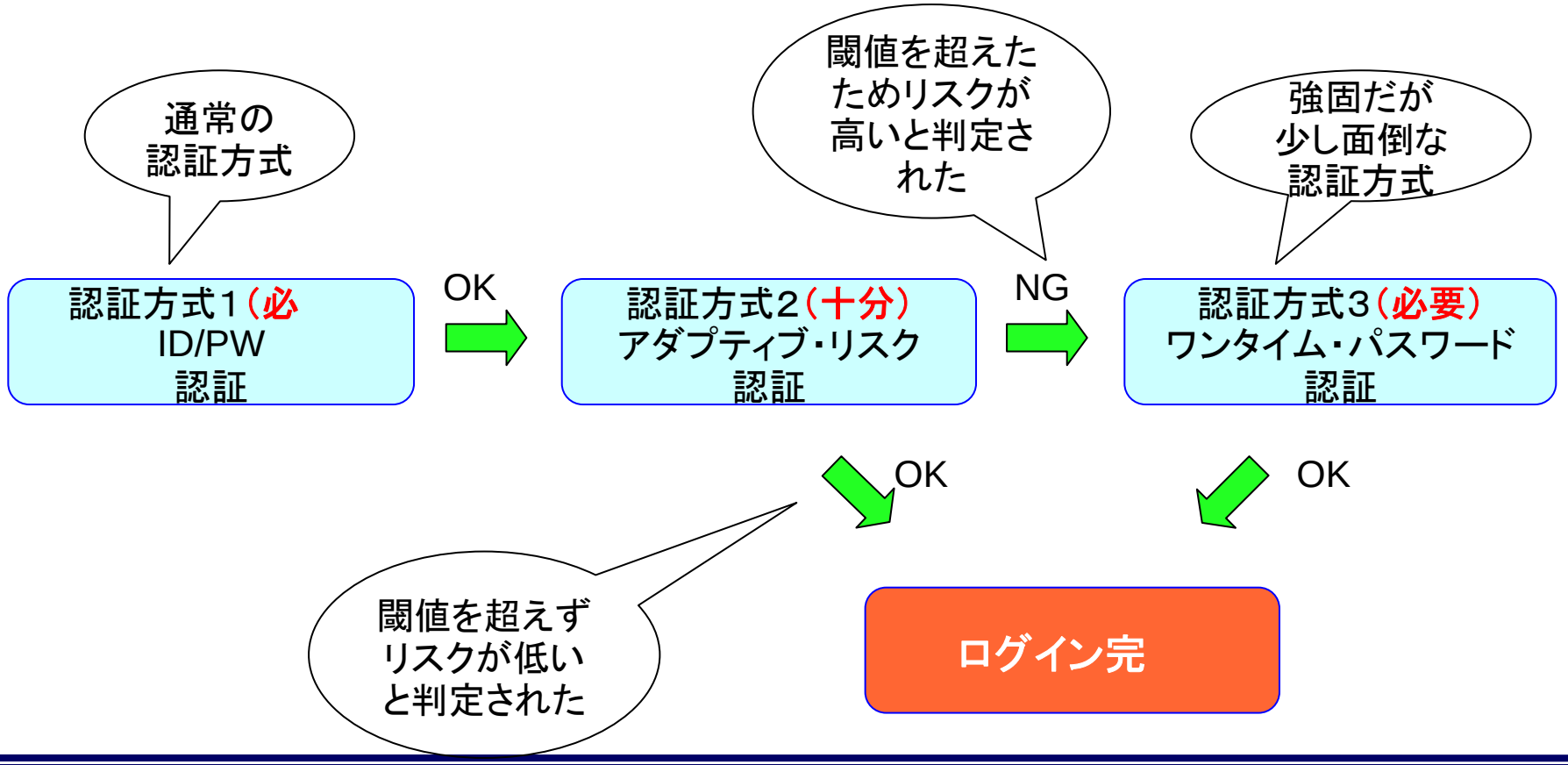


認証連鎖と組み合わせたソリューション例

認証連鎖

- 複数の認証方式を組み合わせ
高いセキュリティを実現

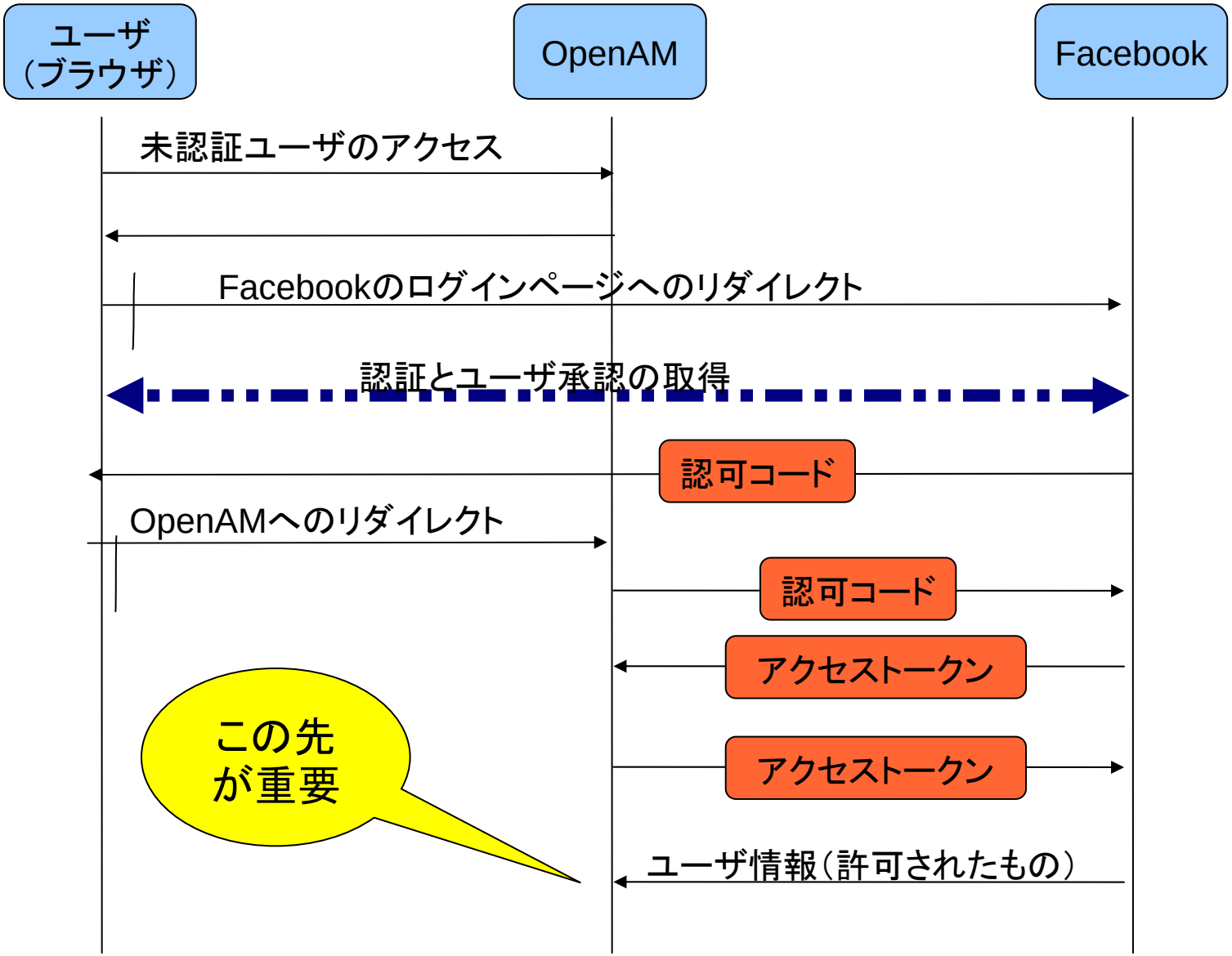
でも毎回だ
少し面倒！



Oauth 2.0を使ったFacebookとの連携

連携に基づく様々なシナリオ

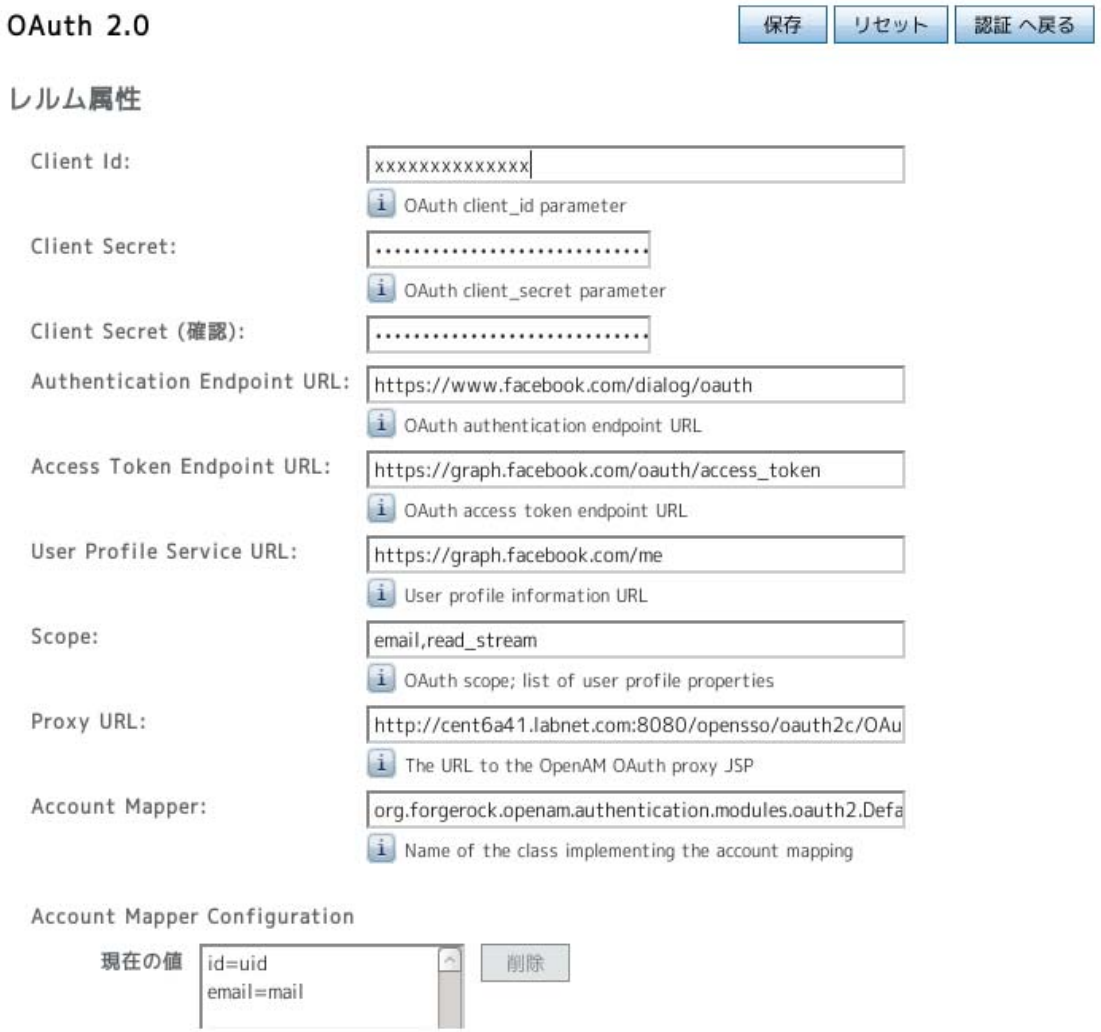
Oauth 2.0を使ったやりとり



取得したユーザ情報の取り扱い

- セッション情報としてメモリ上にのみ保存
  - 必要に応じてセッションオブジェクトからユーザ情報を取得
  - 一時的な利用に限られ、Facebook経由でのアクセス時のみ有効
- DB等に永続的に保存
  - 取得したユーザ情報をLDAPやRDBに保存
  - 必要に応じてユーザIDやパスワードを追加
  - 登録されたメールアドレスに確認コードを送ることも可能
  - 次回からは直接アクセスすることも可能
- ユーザ情報を元にDB上の既存ユーザにマップ
  - メールアドレス等をキーにして対応付けを行う
  - 勝手に対応付けると問題になるかも？
- 上記を組み合わせることにより様々なシナリオが考えられる

Oauth 2.0 認証モジュールの設定（その1）



Attribute Mapper Configuration

現在の値

```
id=uid
last_name=sn
email=mail
last_name=facebook-lname
first_name=givenname
first_name=facebook-fname
name=cn
_____
```

削除

新しい値 追加

Mapping of OAuth attributes to local OpenAM attributes

Save attributes in the session: ☑ 有効
If this option is enabled, the attributes configured in the attribute mapper will be saved into the OpenAM session

Email attribute in OAuth2 Response:
Attribute from the OAuth2 response used to send activation code emails.

Create account if it does not exist: ☐ 有効
If the OAuth2 account does not exist in the local OpenAM data store, an account will be created dynamically.

Prompt for password setting and activation code: ☐ 有効
Users must set a password and complete the activation flow during dynamic profile creation.

Map to anonymous user: ☐ 有効
Enabled anonymous user access to OpenAM for OAuth authenticated users

Anonymous User: anonymous
Username of the OpenAM anonymous user

OAuth 2.0 Provider logout service:
The URL of the OAuth Identity Providers Logout service

Logout options:
- ○ Do not logout
- ○ Log out
- ◉ Prompt

Part 2.
OpenAM導入事例

国立大学法人 北見工業大学 様

http://www.kitami-it.ac.jp/

北見工業大学様 システムの特徴

- ユーザー(学生や教職員)はOpenAMに一度ログインすると、複数のWebアプリケーションをログイン操作なしで利用できます。
- ログインするとポータルメニューが表示されますが、ユーザー権限やログイン場所(学内/学外)によって表示されるメニューが変化します。
- ログインしたユーザーが利用できないアプリケーションは表示されず、インターネットからログインするとイントラネット専用アプリケーションも表示されません。
  - システム全体設計やプロジェクトとりまとめは、兼松エレクトロニクス株式会社が行いました。
  - シングルサインオン システム構築は、 オープンソース・ソリューション・テクノロジ株式会社が行いました。

北見工業大学様