

OpenAM/OpenSSOの紹介



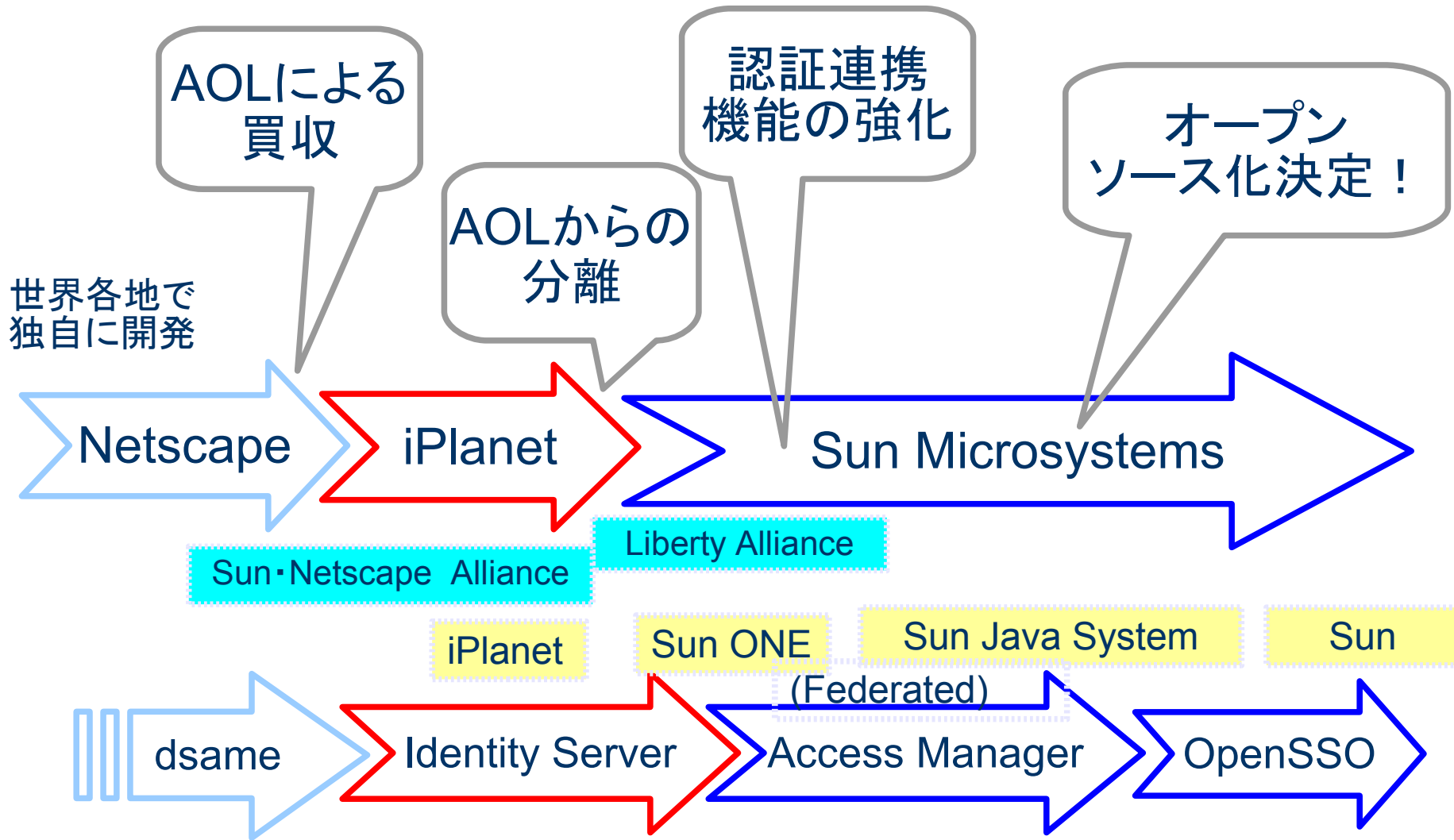
OSSTech

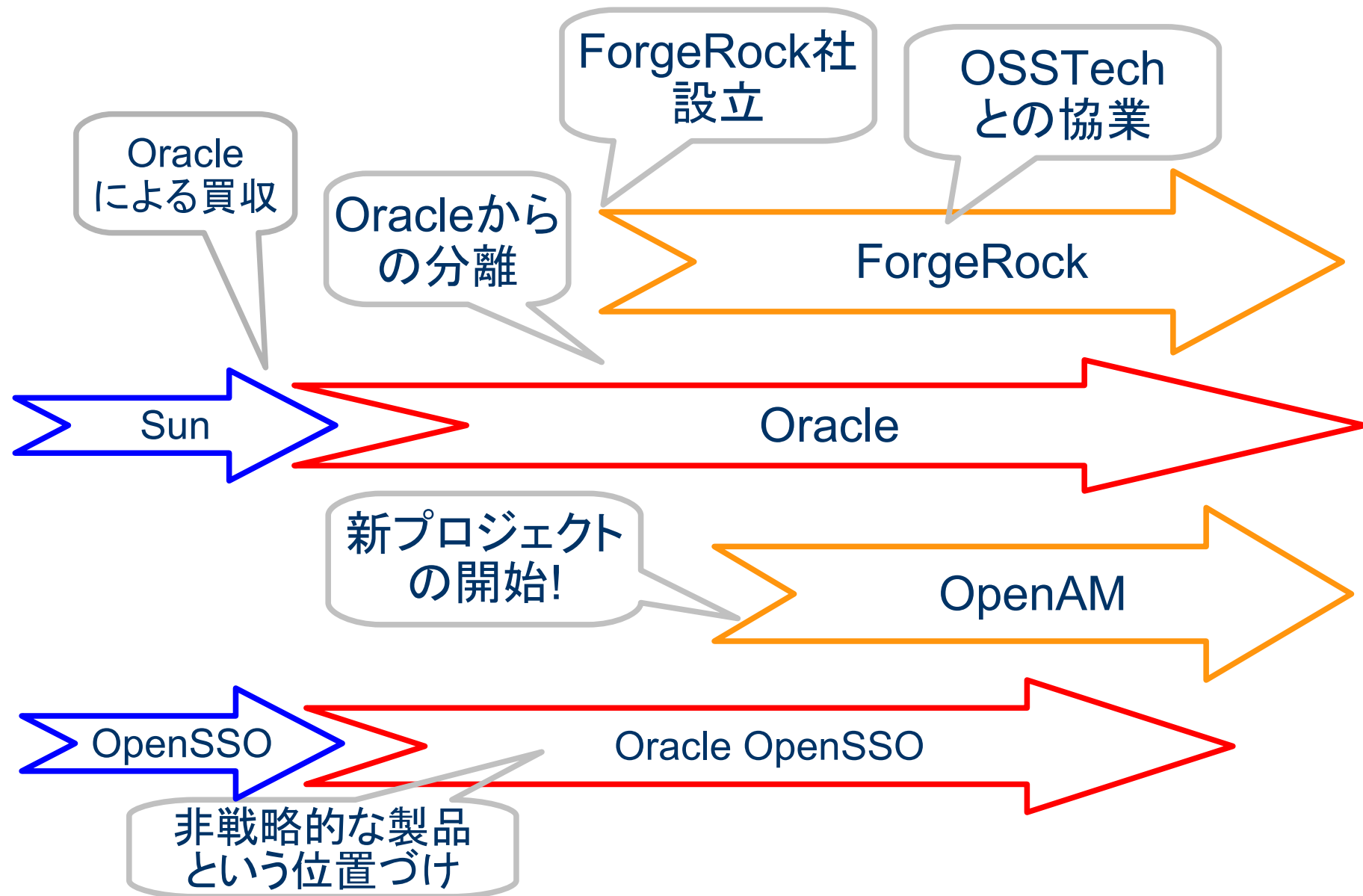
オープンソース・ソリューション・テクノロジー(株)
2010/8/6
岩片 靖

目次

- OpenSSO/OpenAMの歴史
- OpenAMになって変わったこと
- 基本機能のご紹介
- デモ

OpenSSO/OpenAM の歴史





OpenAMになって 変わったこと

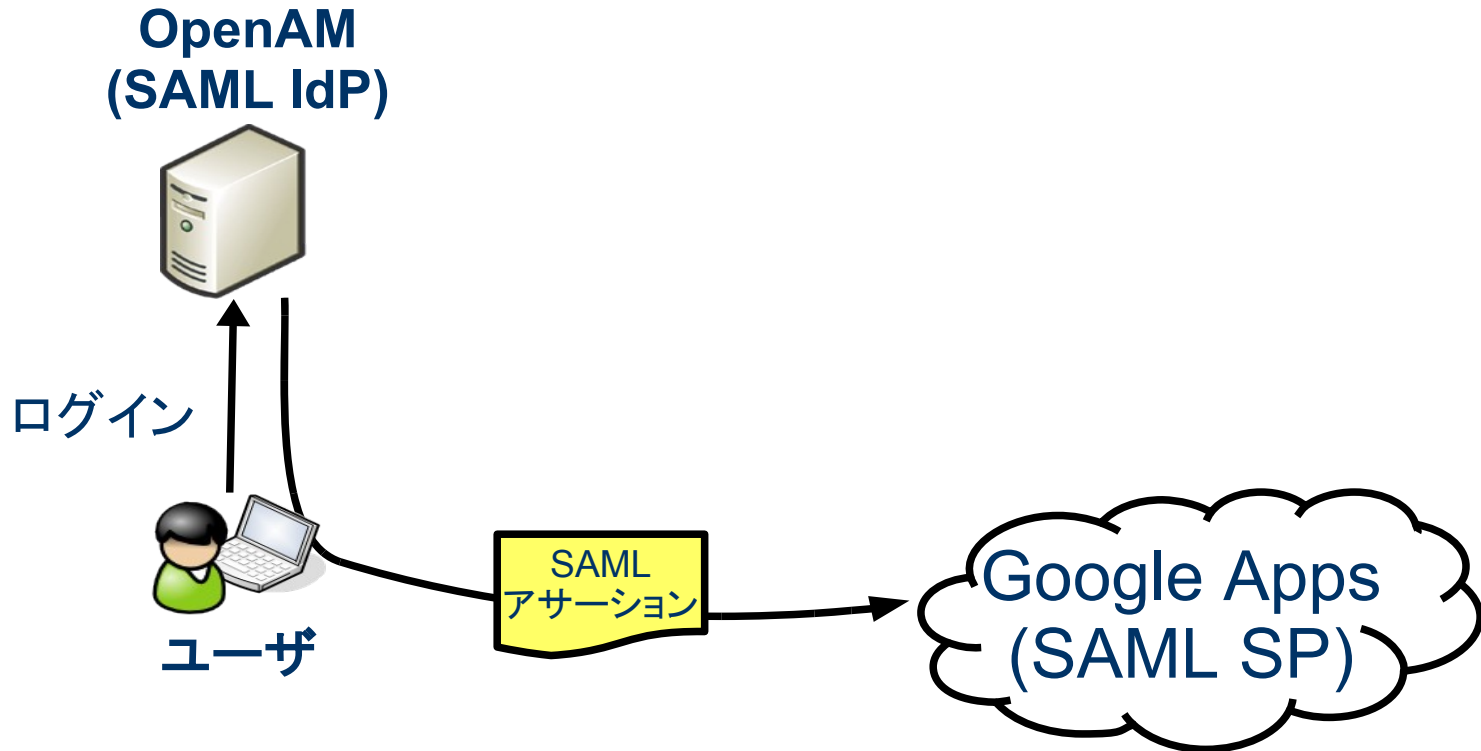
- 作っている人が同じ
 - OpenSSOを担当していたエンジニアが中心になり Forgerockを設立
- ベースにするソースコードが同じ
 - 最新のVer. 9.5では多量のバグフィックスを適用
- ユーザも同じ場合がほとんど
 - 既存ユーザからの移行促進(米国、ヨーロッパ)
 - 日本では多くが新規ユーザ

- 他のおSSとの整合性強化
 - リポジトリとしてのOpenLDAP, OpenDS, MySQL
 - 動作プラットフォームとしての CentOS, Tomcat
- ベンダ独自のパッケージング
 - 弊社ではOpenLDAP用拡張スキーマを提供
- 得意分野と組合わせた統合ソリューション
 - 生体認証等の認証方式との組み合わせ
 - プロビジョニングシステムとの組み合わせ
 - 人事管理システムとの組み合わせ
 - 弊社ではUnicorn IDマネージャと組合わせてGoogle Appsとのシングルサインオン ソリューションを提供

- クラウド対応
 - Google Apps, SalesforceとのSAML連携を強化
 - GUIによる操作で連携設定が可能
- OpenDSの最新版を内蔵
 - Version 2.3 安定版
 - 標準ツールの添付
- 多量のバグフィックス
 - OpenSSO Expressで開発してきたユーザへの対応
 - OpenAMへの移行促進

Google Appとの連携

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

このサーバー上に SAMLv2 アイデンティティプロバイダを作成します

設定 取消し

このページにより、OpenAM サーバーのこのインスタンスをアイデンティティプロバイダ (IDP) として設定できます。プロバイダの名前、トラストサークル (COT)、プロバイダのメタデータ、およびオプションとして署名証明書を設定できます。COT とは、相互に信頼しており、実質的にすべての連携通信が実行される範囲を表す IDP とサービスプロバイダ (SP) のグループです。メタデータは、連携プロトコル (たとえば、SAMLv2) を実行するために必要な設定や、この設定を COT 内のほかのエンティティ (たとえば、SP) に伝えるためのメカニズムを表します。メタデータがない場合でも、メタデータを簡単に生成できます。システムに複数のレルムがある場合は、このプロバイダのレルムを選択する必要があります。そうしない場合、このプロバイダは root レルムの下に設定されます。

* 必須入力フィールド

このプロバイダのメタデータがありますか?: はい いいえ ⓘ

メタデータ

* 名前: ⓘ
署名鍵:

トラストサークル

表示されている既存のトラストサークルから選択するか、またはこの IDP を含むように作成するトラストサークルを指定します。COT とは、相互に信頼しており、すべての SAMLv2 通信が実行される範囲を提供する IDP と SP のグループです。

トラストサークル: 既存のトラストサークルに追加します 新しいトラストサークルに追加します

* 新しいトラストサークル:

属性マッピング

属性をマッピングすると、サービスプロバイダ (SP) とアイデンティティプロバイダ (IDP) でそれぞれ一意の名前を持つ可能性がある同一の属性を、両方で認識できるようにするのに役立ちます。たとえば、SP で UserName という名前の属性が、IDP では UserID という名前と呼ばれていることがあります。属性のマッピングによってこうした非一貫性を除去すると、データの正確な受け渡しが保証されます。

属性マッピング	
<input type="button" value="削除"/>	
表明内の名前	ローカル属性名
<input type="text"/>	<input type="text"/>
<input type="button" value="追加"/>	
<input type="text" value="属性を選択します。"/> ⓘ	

シングルサインオン用の Google Apps の設定

作成 取消し

メタデータを設定する前に、アイデンティティプロバイダとリモートサービスプロバイダの情報を指定する必要があります。OpenAM はアイデンティティプロバイダとして機能し、Google Apps はサービスプロバイダとして機能します。SAMLv2 は、アイデンティティプロバイダでトラストサークルを作成するためのシングルサインオンプロトコルです。

* 必須入力フィールド

* トラストサークル: testcot

* アイデンティティプロバイダ:

リモート SP の設定

* ドメイン名:

現在の値	<input type="text"/>	<input type="button" value="削除"/>
新しい値	<input type="text" value="ga.example.com"/>	<input type="button" value="追加"/>

Google Apps のシングルサインオンの設定

終了

Google Apps のシングルサインオンを設定するときは、次の情報を Google Apps に指定する必要があります。Google Apps のシングルサインオンの設定に進む前に、次の URL と検証証明書情報を保存します。

URL

サインインページの URL:	<input type="text" value="http://openam.example.com:8080/openam/SSORedirect/metaAlias/idp"/> OpenAM および Google Apps にサインインするための URL
サインアウトページの URL:	<input type="text" value="http://openam.example.com:8080/openam/UI/Logout?goto=http://openam.example.com:8080/openam"/> サインアウト時のユーザーのリダイレクト先 URL
パスワード変更の URL:	<input type="text" value="http://openam.example.com:8080/openam/idm/EndUser"/> ユーザーが OpenAM のパスワードを変更できる URL

検証証明書

検証証明書:

```
-----BEGIN CERTIFICATE-----  
  
省略  
  
-----END CERTIFICATE-----
```

[ダウンロードするには、ここをクリックします。](#)

このテキストをテキストファイルにコピーし、新しいテキストファイルを Google Apps の検証証明書にアップロードします。

ダッシュボード ユーザーとグループ ドメインの設定 **高度なツール** サポート サービスの設定 ▾

高度なツール

複数のユーザーを作成 [一括アップロード](#)
Upload a CSV file to create and update many user accounts at once.

[Download Directory Sync](#)

If you have an on-premise LDAP directory server, you can use Google Apps Directory Sync to automatically import users and groups into Google Apps. Google Apps Directory Sync is a client application that sets up rules for synchronizing Microsoft Active Directory, IBM Lotus Domino, and other LDAP servers with Google Apps. After creating your rules, you run the synchronization on your command line interface.

認証 [シングル サインオン \(SSO\) の設定](#)
SAML ベースのシングル サインオン (SSO) を使用して、Gmail やカレンダーなどのウェブベース アプリケーションでユーザーアカウントを認証できます。Google トーク、Gmail への POP アクセスなどのデスクトップアプリケーションについては、ユーザーは引き続き Google Apps のユーザー名とパスワードを使用して個別にログインする必要があります。 [詳細](#)

[ダッシュボード](#)[ユーザーとグループ](#)[ドメインの設定](#)[高度なツール](#)[サポート](#)[サービスの設定](#)[« 高度なツールに戻る](#)

シングル サインオン (SSO) の設定

SSO を設定するには次の情報を入力してください。 [SSO リファレンス](#)

シングル サインオンを有効にする

ログイン ページの URL *

システムと Google Apps へのログイン用 URL

ログアウト ページ URL *

ユーザーがログアウトするときリダイレクトする URL

パスワードの URL を変更 *

ユーザーがシステムでパスワードを変更する際にアクセスする URL

認証の確認 *

認証ファイルのアップロードが完了しました-[証明書を更新](#)

認証ファイルには、ログイン リクエストを確認するための Google 公開キーが含まれている必要があります。 [詳細](#)

ドメイン固有の発行元を使用

ドメインで IDP アグリゲータを使用して SAML リクエストを処理する場合は、これを選択する必要があります。有効になっていれば、SAML リクエストで送信した発行元は `google.com` ではなく `google.com/a/g.osstech.co.jp` となります。 [詳細](#)

ネットワーク マスク

ネットワーク マスクは、シングル サインオンで有効にできるアドレスを決定します。マスクが指定されない場合、ネットワーク全体に対して SSO 機能が適用されます。

マスクの区切りにはセミコロンを使用します。例: (64.233.187.99/8; 72.14.0.0/16)

範囲を指定する場合はダッシュを使用します。例: (64.233.167-204.99/32)

すべてのネットワーク マスクは CIDR で終わる必要があります。 [詳細](#)

OpenAMの基本機能(その1)

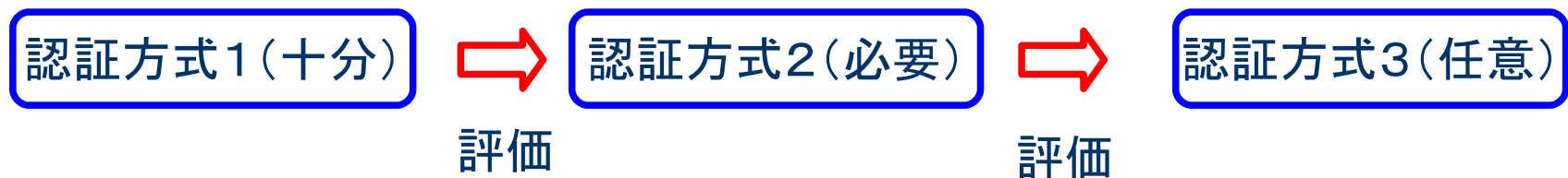
認証方式と多要素認証

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

認証方式を組み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

Windows Server
2000/2003/2008

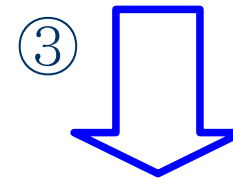
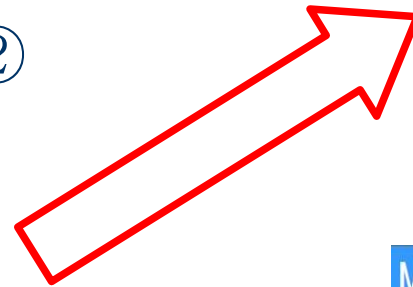
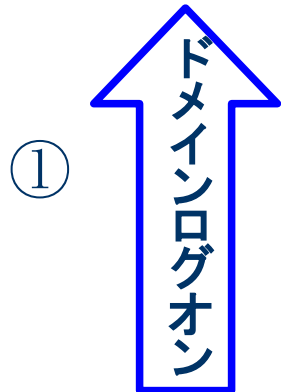


Active Directory

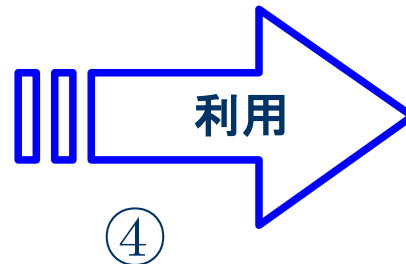
自動チケット送付



OpenAM



認証、認可、
属性情報



MosP勤怠管理 メニューガイド v8.2.0 ユーザー名: 人事 一郎

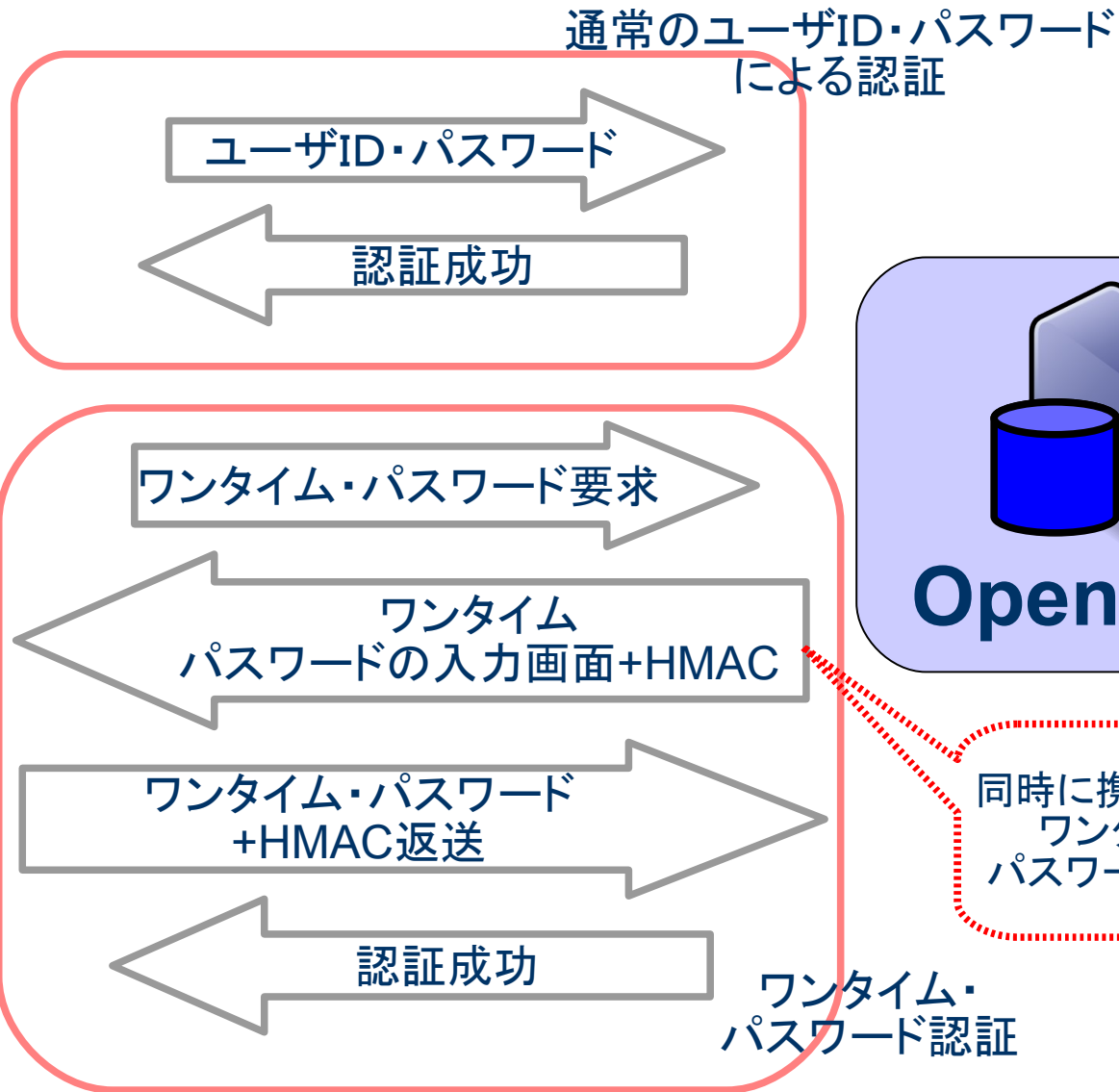
メニューガイド

勤怠入力

勤怠管理 給与管理 人事管理

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

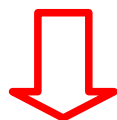


同時に携帯電話へ
ワンタイム・
パスワードを送付

- 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

- 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



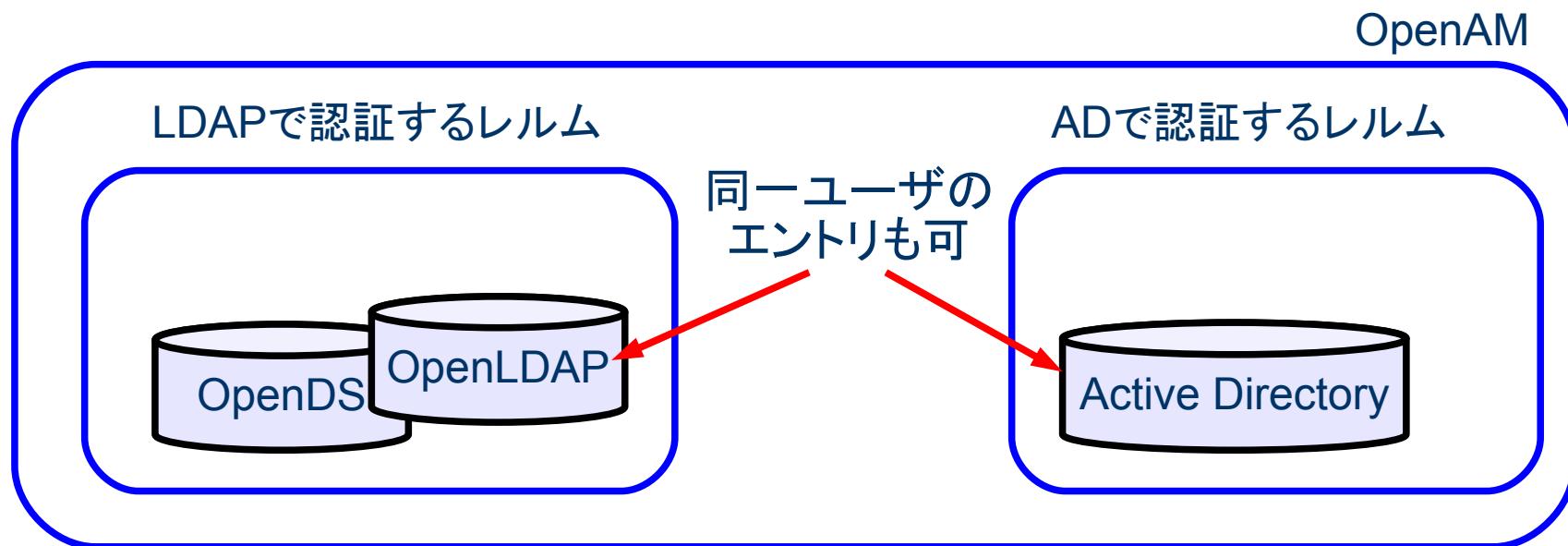
- 2つを組み合わせることにより便利かつ厳密な認証を行うことが可能
 - Windows Desktop SSO: 十分
 - ユーザID・パスワードによる認証: 必須
 - ワンタイム・パスワードによる認証: 必須

OpenAMの基本機能(その2)

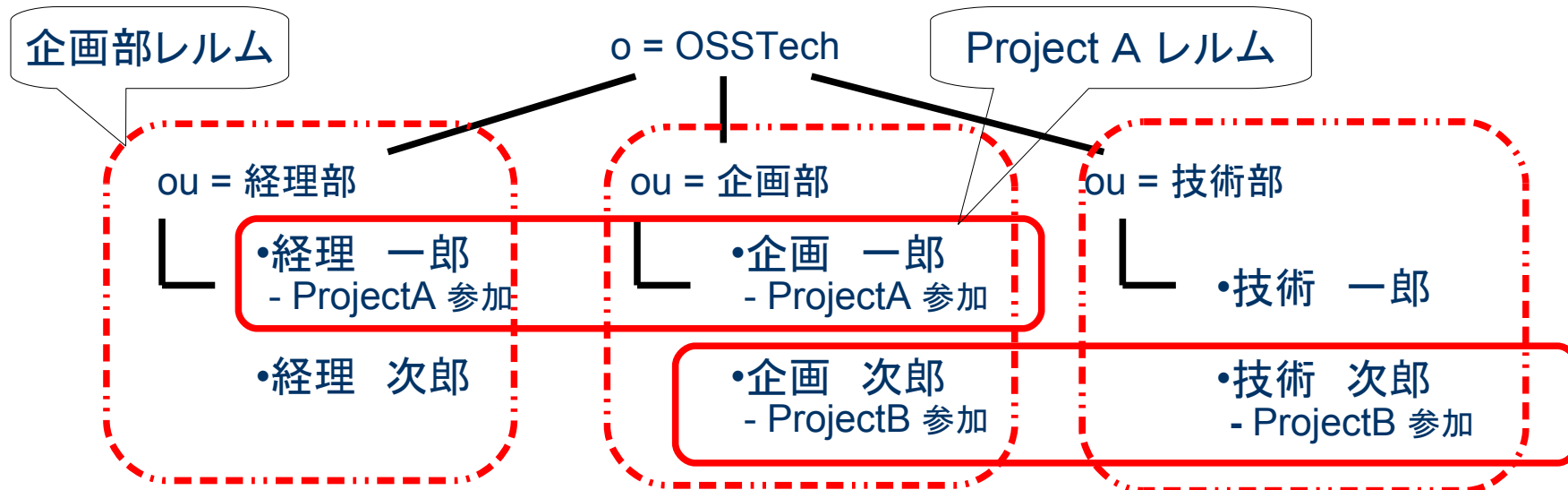
レールムと委任による

ユーザ管理

- レルム: 設定を管理するための単位
 - ユーザリポジトリ (OpenLDAP, OpenDS, AD, RDB...)
 - 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
- レルム毎に管理者を置き管理を委任することが可能



- 社員は組織別に分けられてLDAPサーバに保存されている
- 社内Projectでは組織を横断してメンバーが参加する
- 管理は組織単位で行う他にProject単位でも行いたい
 - 組織単位のレルム: ベースDNを指定
 - プロジェクト単位のレルム: ユーザ属性をフィルタに指定
 - 管理を各レルムの管理者に委任



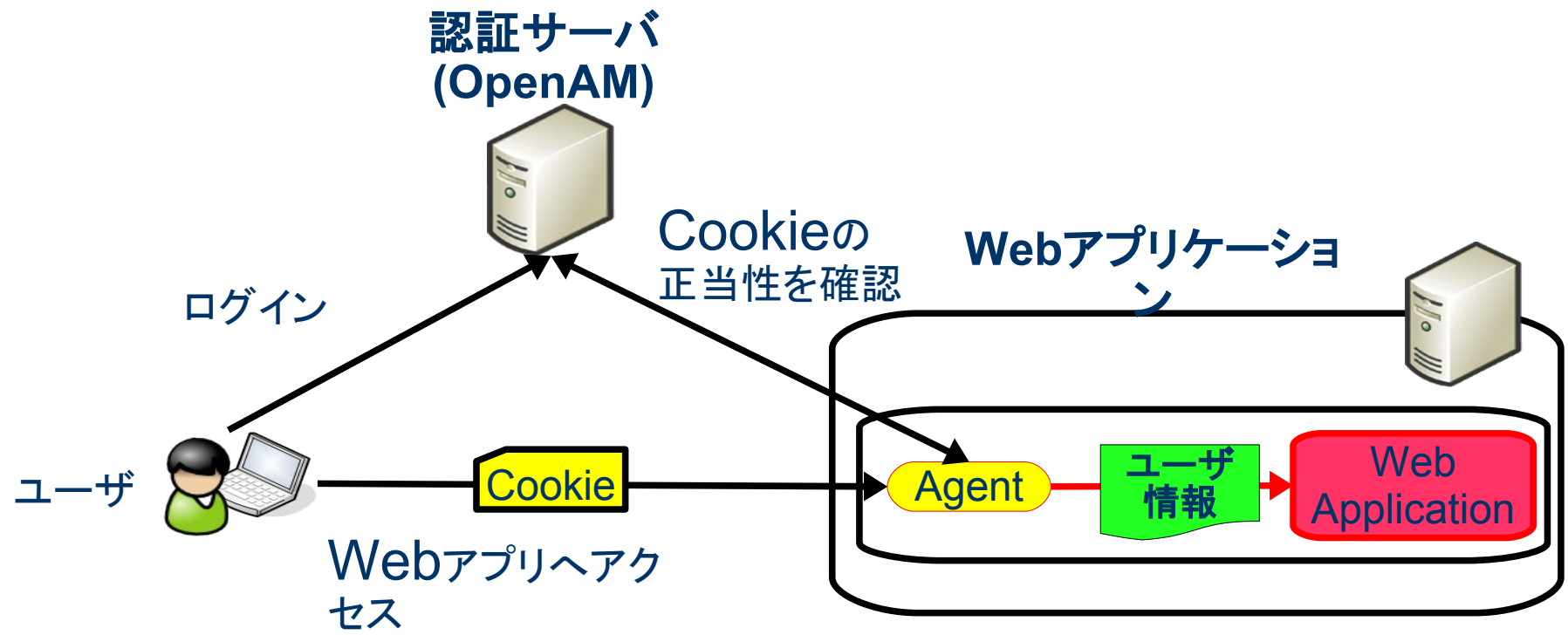
OpenAMの基本機能(その3)

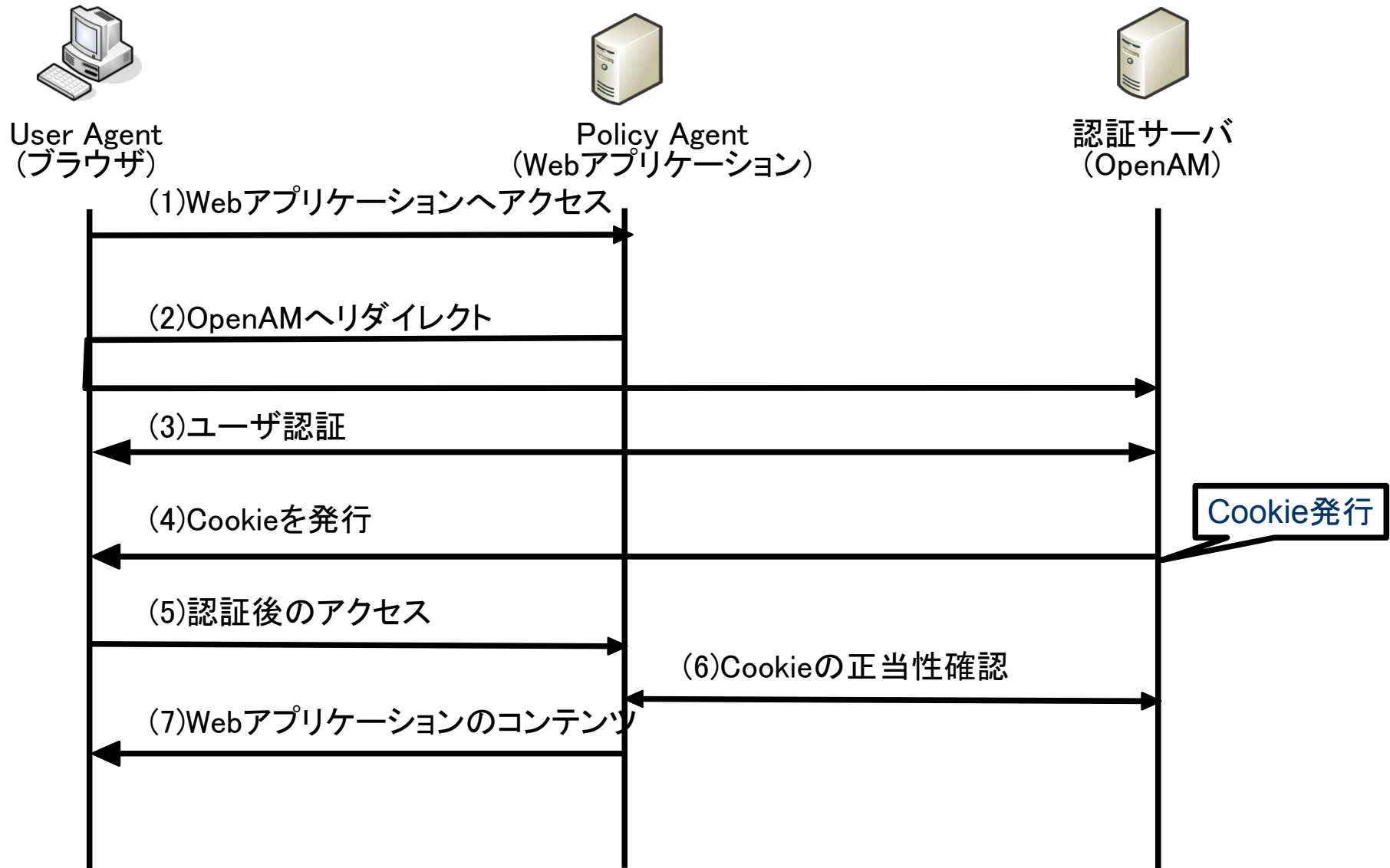
多様な

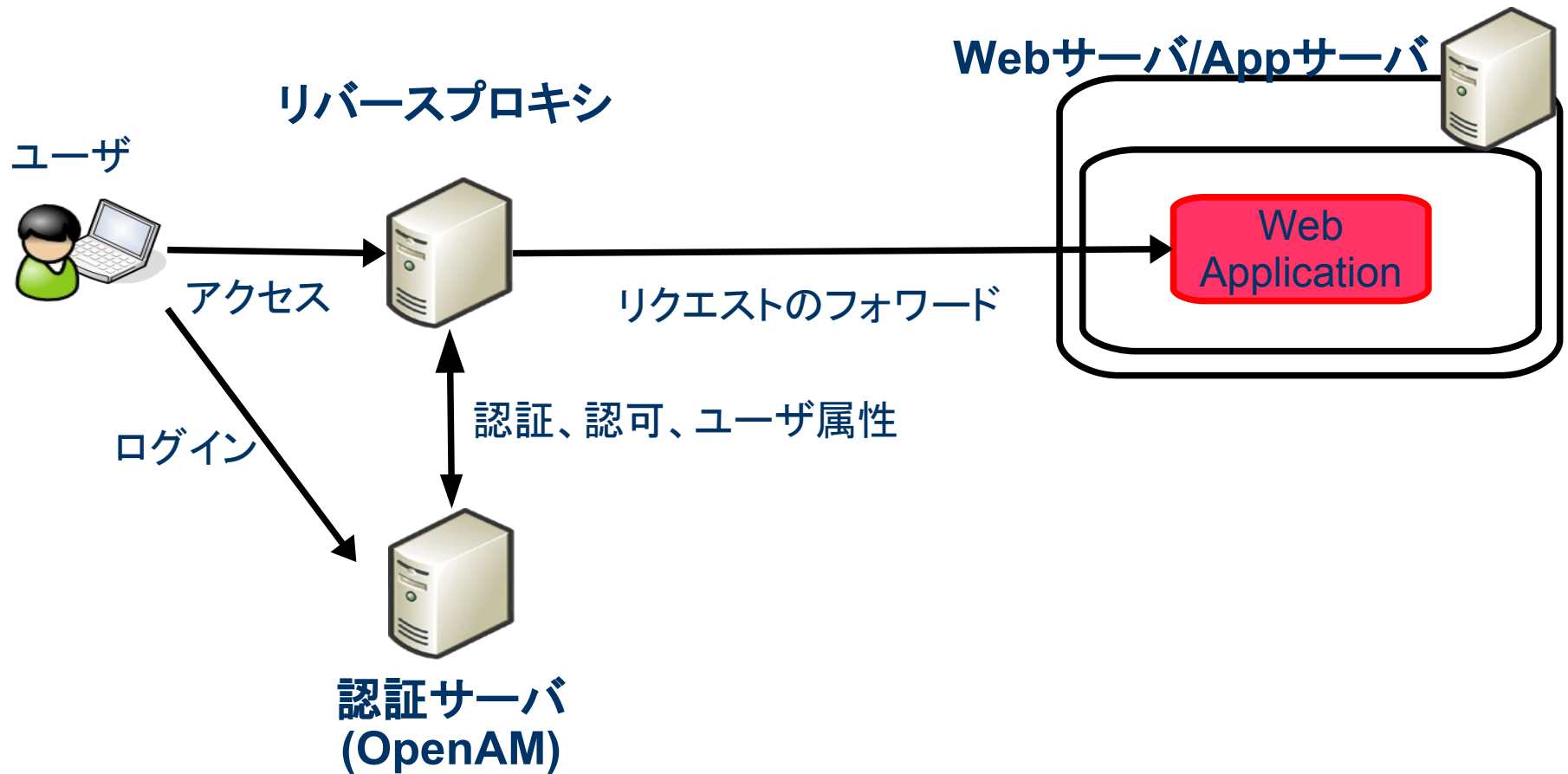
シングルサインオン方式

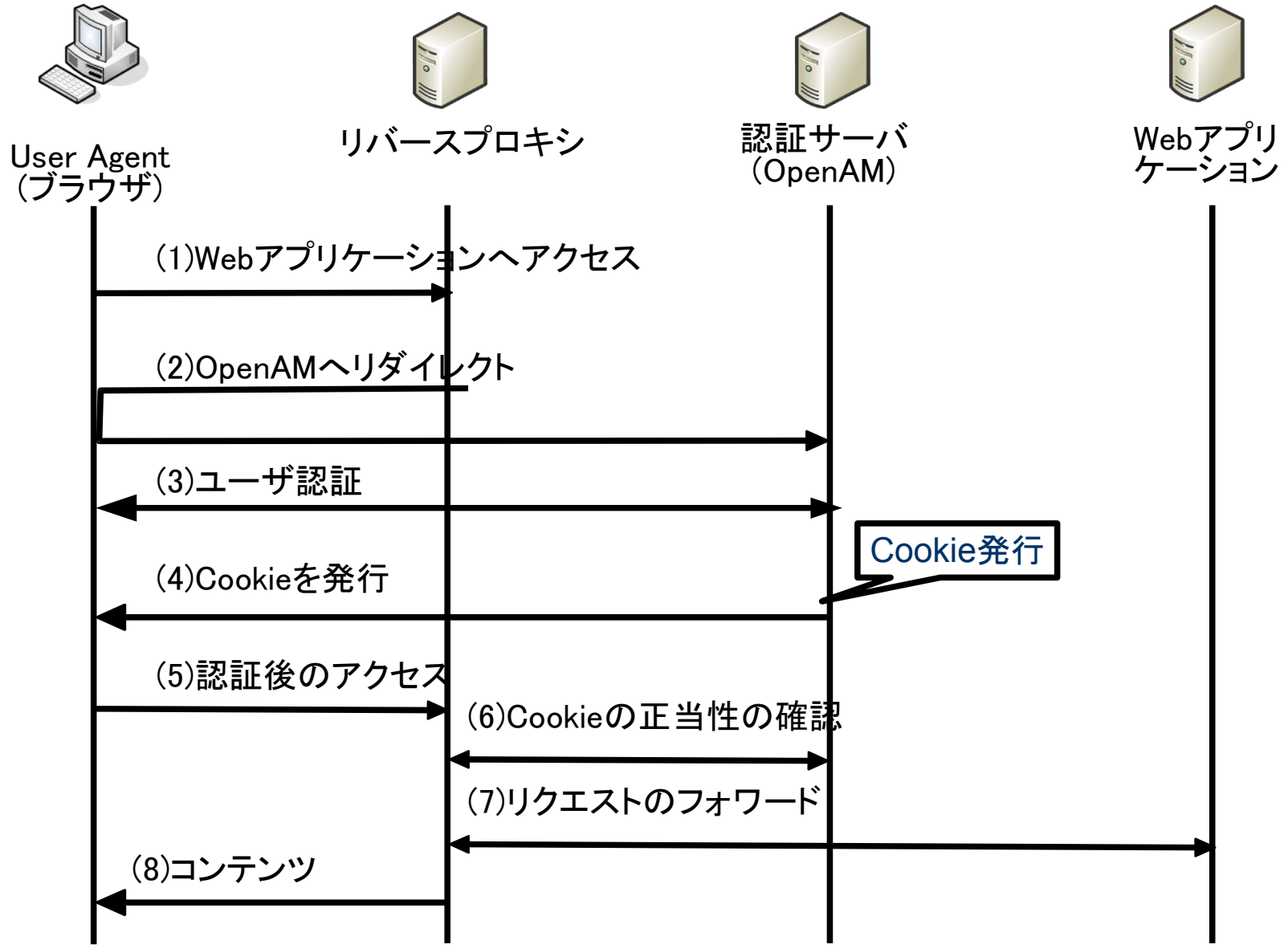
- エージェント方式
 - 保護対象のアプリが動作するサーバ上にアクセス制御用のモジュールを配置する方式
 - APIレベルでの細かな連携が可能
 - 保護対象のアプリやサーバのバージョンや設定変更に影響されやすい
- リバースプロキシ方式
 - リバースプロキシを使ってアクセス制御を行う方式
 - データの受け渡し方法がHTTPヘッダに限定
 - 保護対象のバージョンや設定変更の影響が少ない
 - 性能のボトルネックになる可能性も

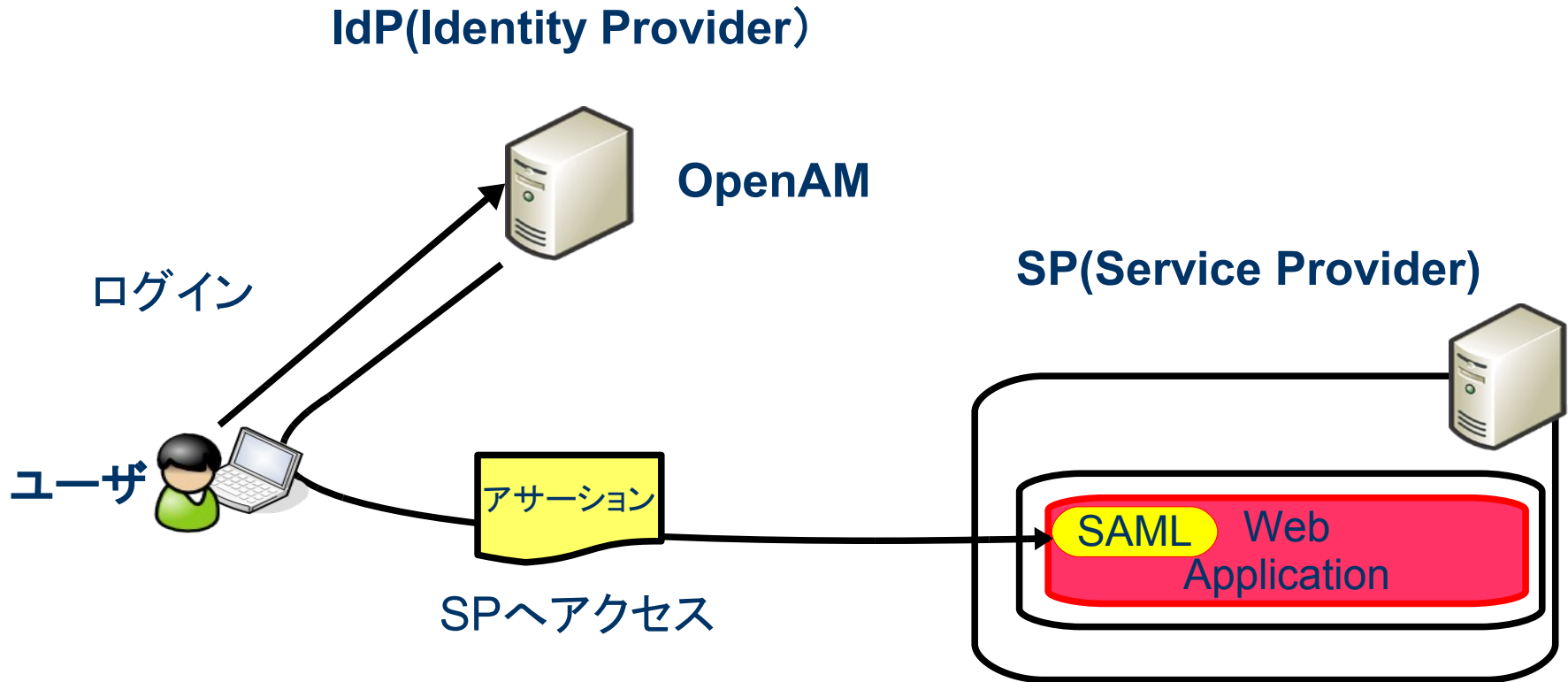
- SAML
 - Secure Assertion Markup Language
 - 認証、認可、ユーザ属性情報などをXMLで送受信するためのフレームワーク
 - 標準化団体OASISにより策定
 - 通常はサイト間連携で使用











(HTTP Redirect/POST Bindingの場合)



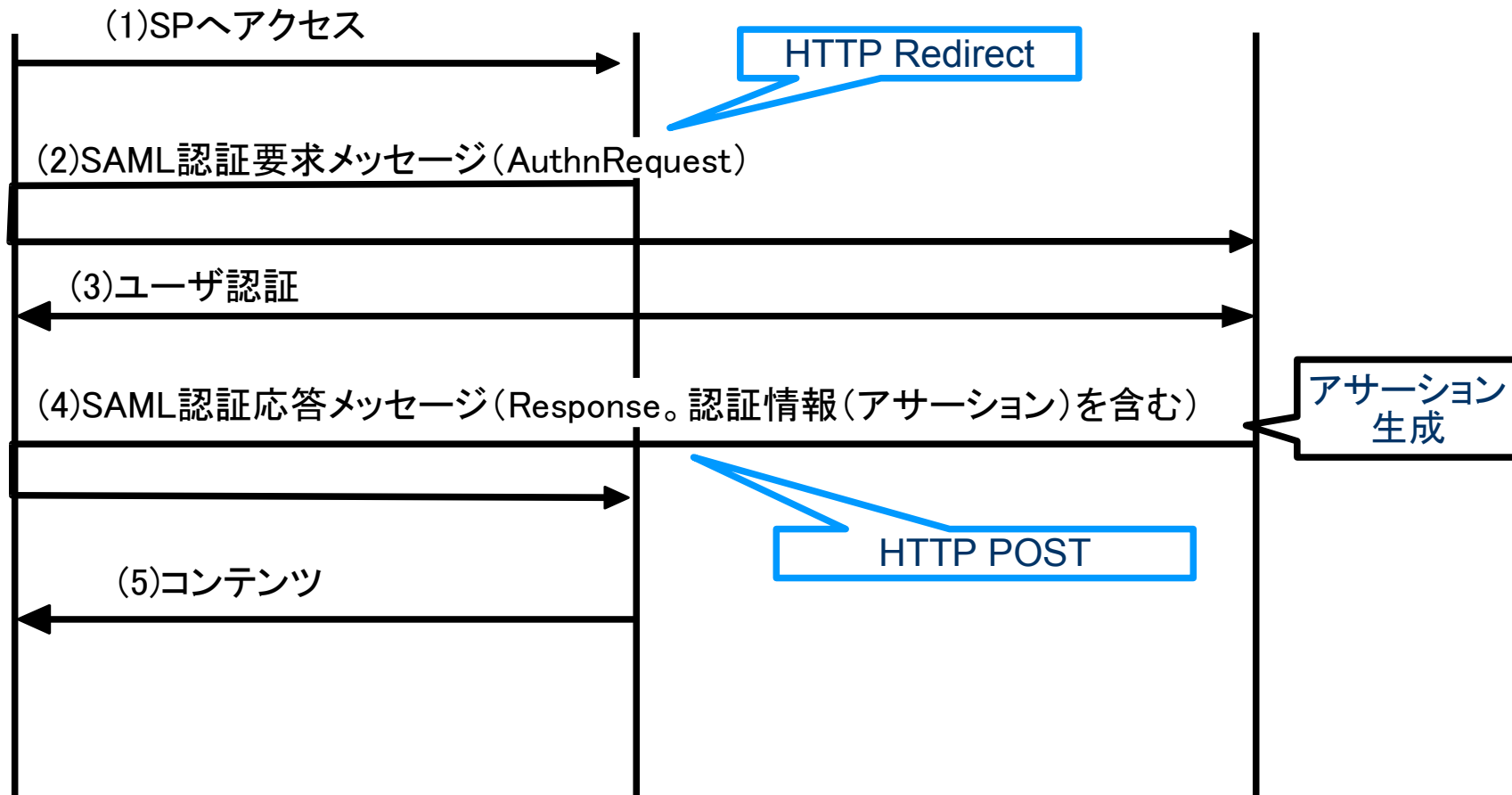
User Agent
(ブラウザ)



SP
(Webアプリ)



IdP
(OpenAM)



OpenAMの基本機能(その4)

アクセス制御ポリシー

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

…を定めたルールが集まり

- OpenAMは長い期間をかけて着実に進化してきました
- OpenAMの最新版はクラウド対応と安定稼動を目標としています
- コミュニティ・ベースの開発になることによって、様々な提供形態が出現することが予想されます
- OpenAMはユーザ管理、シングルサインオン、アクセス制御に関して様々なオプションを提供しています
- OpenAMはGoogle Appsとの連携に使いたいというユーザから、本格的なクラウドサービスを構築したいというユーザまで幅広く対応可能です