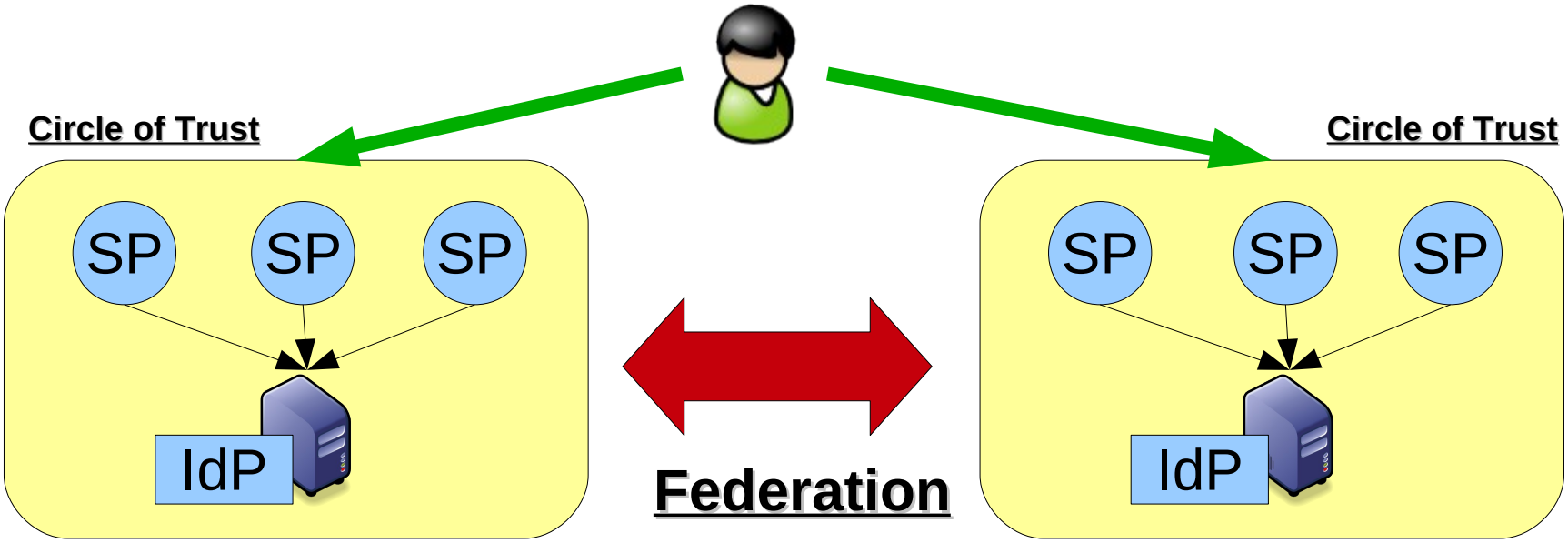
OpenSSO勉強会
ID-WSF と OpenSSO

OSSTech

オープンソース・ソリューション・テクノロジ株式会社
2009/12/01
武田 保真

ID-WSFとは

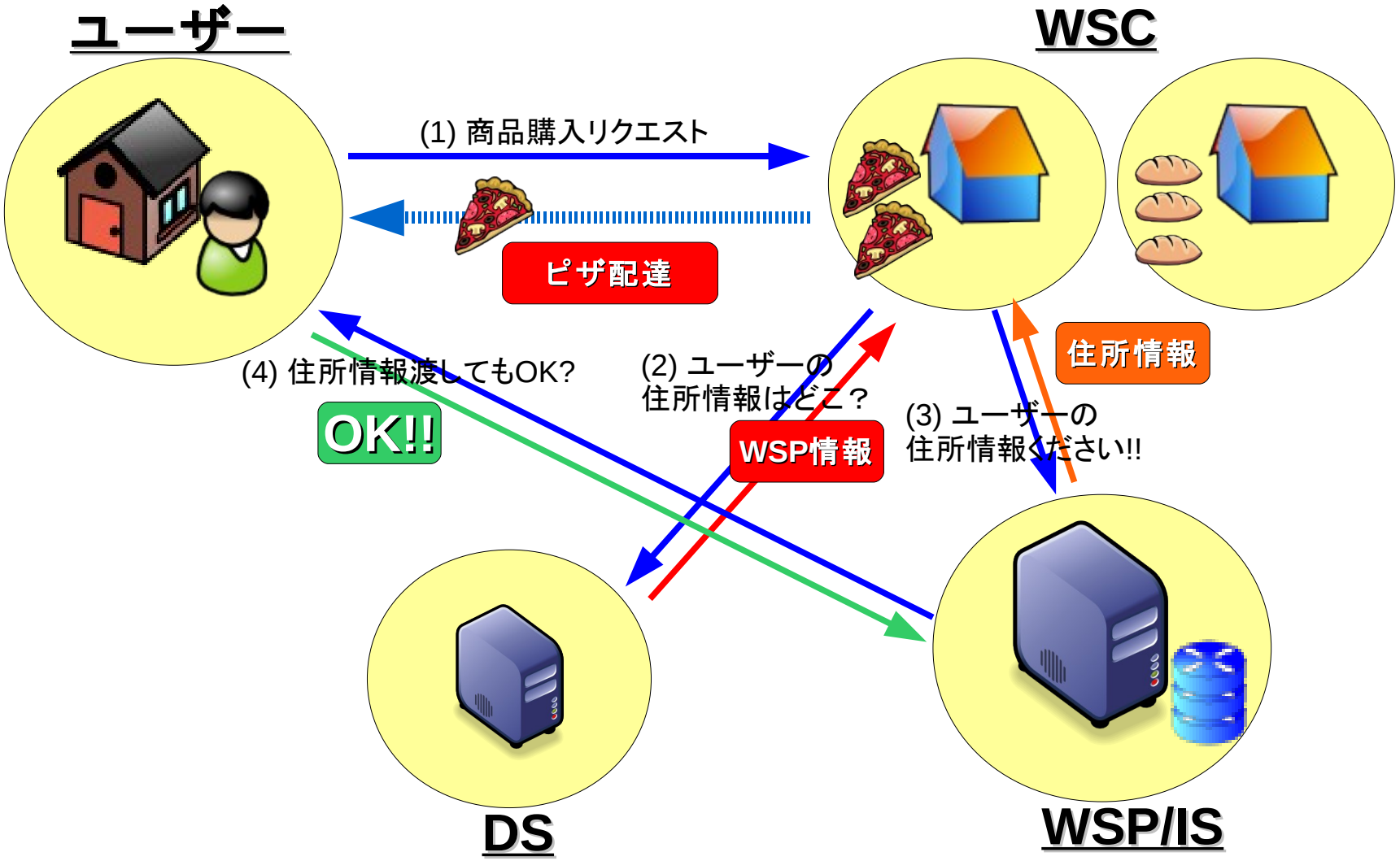
- ID-WSF (Identity Web Service Framework)
  - ID-WSFの目的
    - ID連携環境間の統合(Federation)
      - 属性情報の交換のための仕様



ID-WSFの重要キーワード(1)

- WSP (Web Service Provider)
  - ユーザーの属性情報を提供する
- WSC (Web Service Consumer)
  - ユーザーの属性情報を利用して、サービスを提供する
- DS (Discovery Service)
  - ユーザーが利用するWSPの情報などを管理、提供する
  - ユーザーがWSCを利用するための、本人識別情報(Identity Token)を提供
- IS (Interaction Service)
  - ユーザーに情報を提供してよいか確認するサービスを提供する

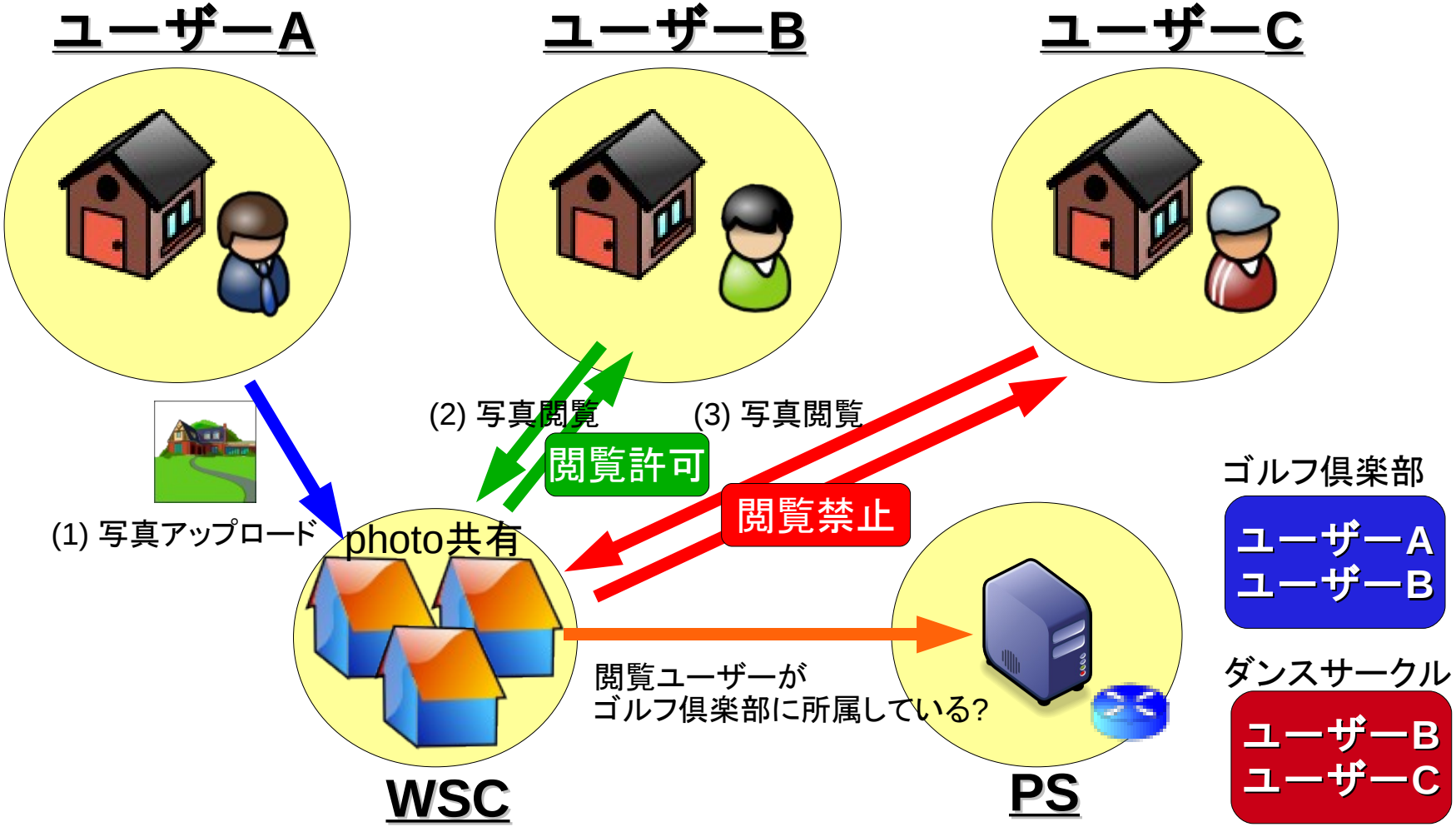
ID-WSFの連携概要(1)



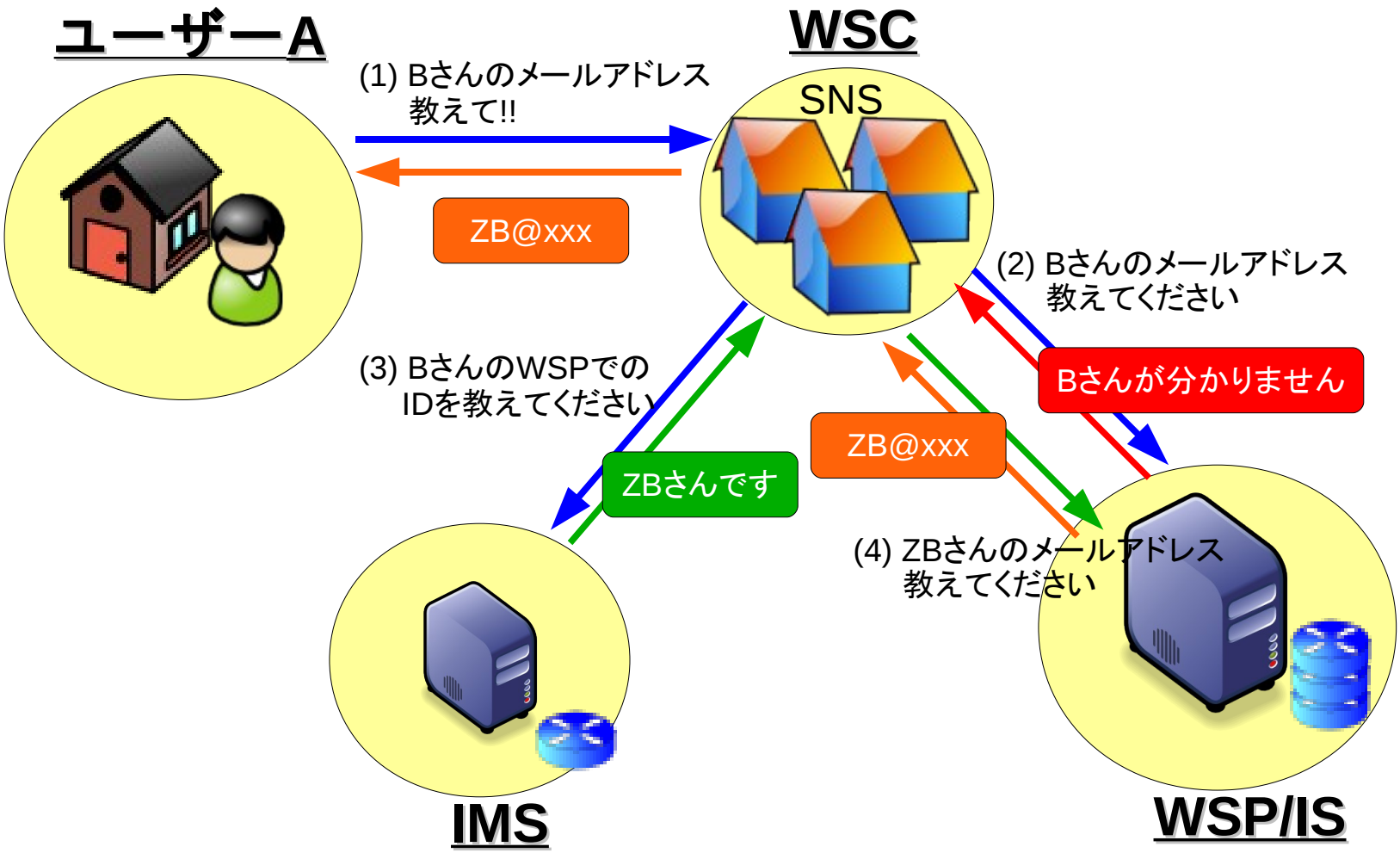
ID-WSFの重要キーワード(2)

- PS (People Service)
  - ユーザーの人間関係に関する情報を提供するサービス
    - ユーザーの友人情報やグループ情報など
- AS/SSOS/IMS（Authentication, Single Sign On, Identity Mapping Service)
  - ユーザーの認証情報やIdentity Tokenを提供するサービス
  - Identity Tokenのマッピングを実施

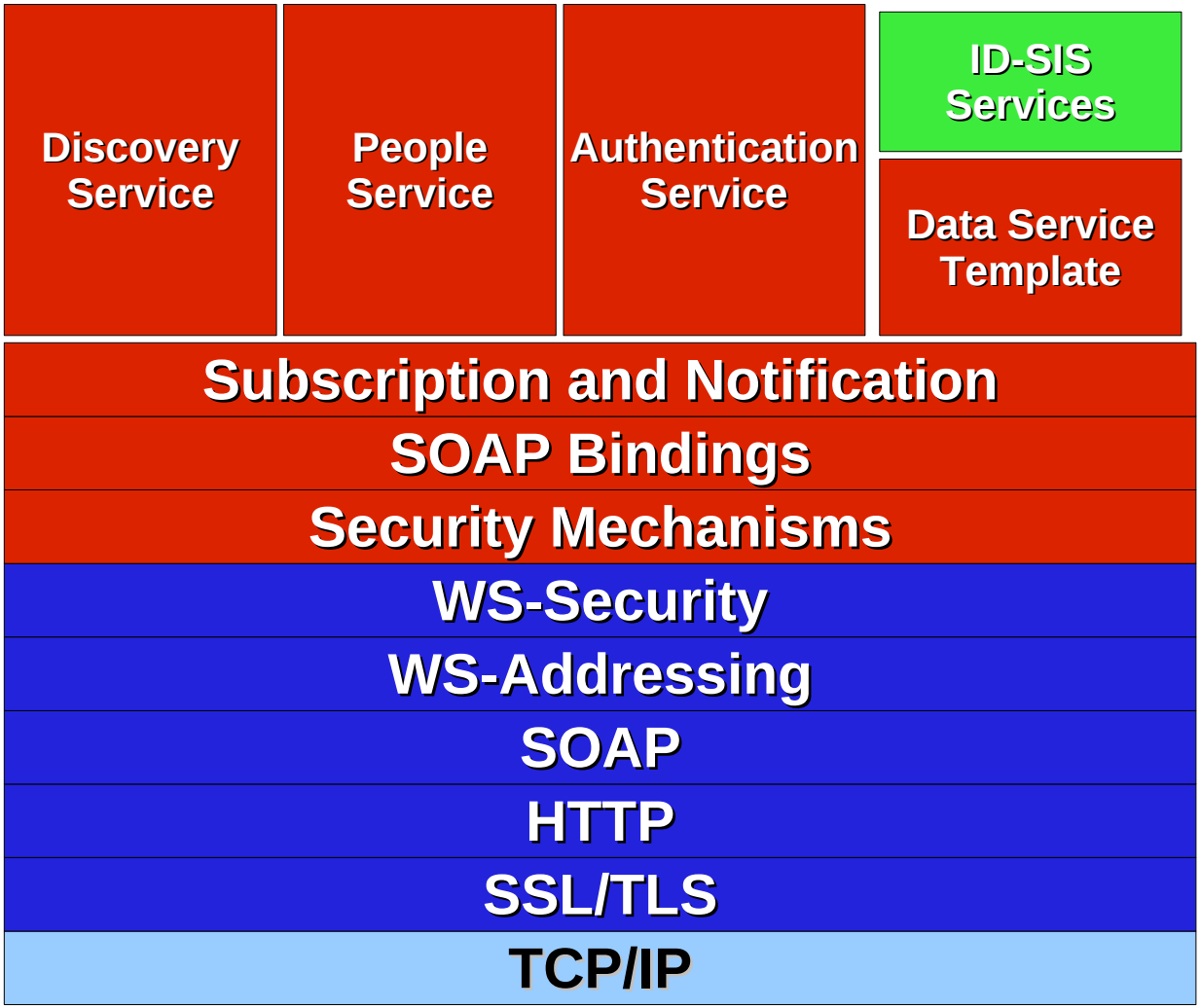
People Serviceの連携

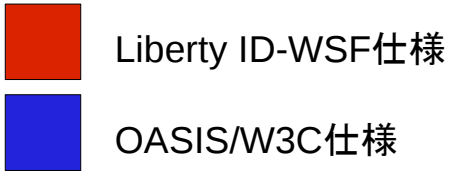


AS/SSOS/IMSの連携



ID-WSFのコンポーネント構成





ID-WSF SOAP Bindings

- ID-WSFは、ID連携の際のSOAPベースの統一フレームワークを定義
  - SOAP: Softwareがメッセージ交換するためのプロトコル

ID-WSF Security Mechanisms

- ID-WSF Security Mechanisms Core
  - ID連携サービスを安全に使うための要件定義
  - IdP間のIDトークンを定義
  - SP間のプライバシー保護のための要件定義
- ID-WSF Security Mechanisms SAML Profile
  - SAML Assertion Profileを定義
  - WS-Security SAML Token Profileを定義

ID-WSF Discovery Service

- ID連携の利用者に、登録されているサービスを発見するための手段を提供
  - DSは、ID-WSFのエンドポイント(End Point Reference)情報を提供
  - DSは、利用者のSecurity Tokenを発行

ID-WSF Data Service Template

- ID-WSFで提供するData Serviceのテンプレートを定義
  - データーの作成･更新･削除手順などを定義
  - 共通の属性の定義など

ID-WSF Subscriptions and Notification

- プロバイダ間のイベント通知メカニズムを定義

ID-WSF Interaction Service

- ユーザーからアクセス許可などを得るためのアクションを行うためのプロトコルを定義

ID-WSF Profiles for Liberty enabled User Agents or Devices (LUAD)

- ユーザーエージェントやデバイスが保持するLibertyのプロファイル情報の定義

Reverse HTTP Binding

- HTTPのレスポンス内のSOAPリクエストを扱うことを可能にする
- この機能を利用して、インターネットから直接アクセスできないIDサービスと連携可能となる

ID-WSF Authentication, Single Sign On, Identity Mapping Services

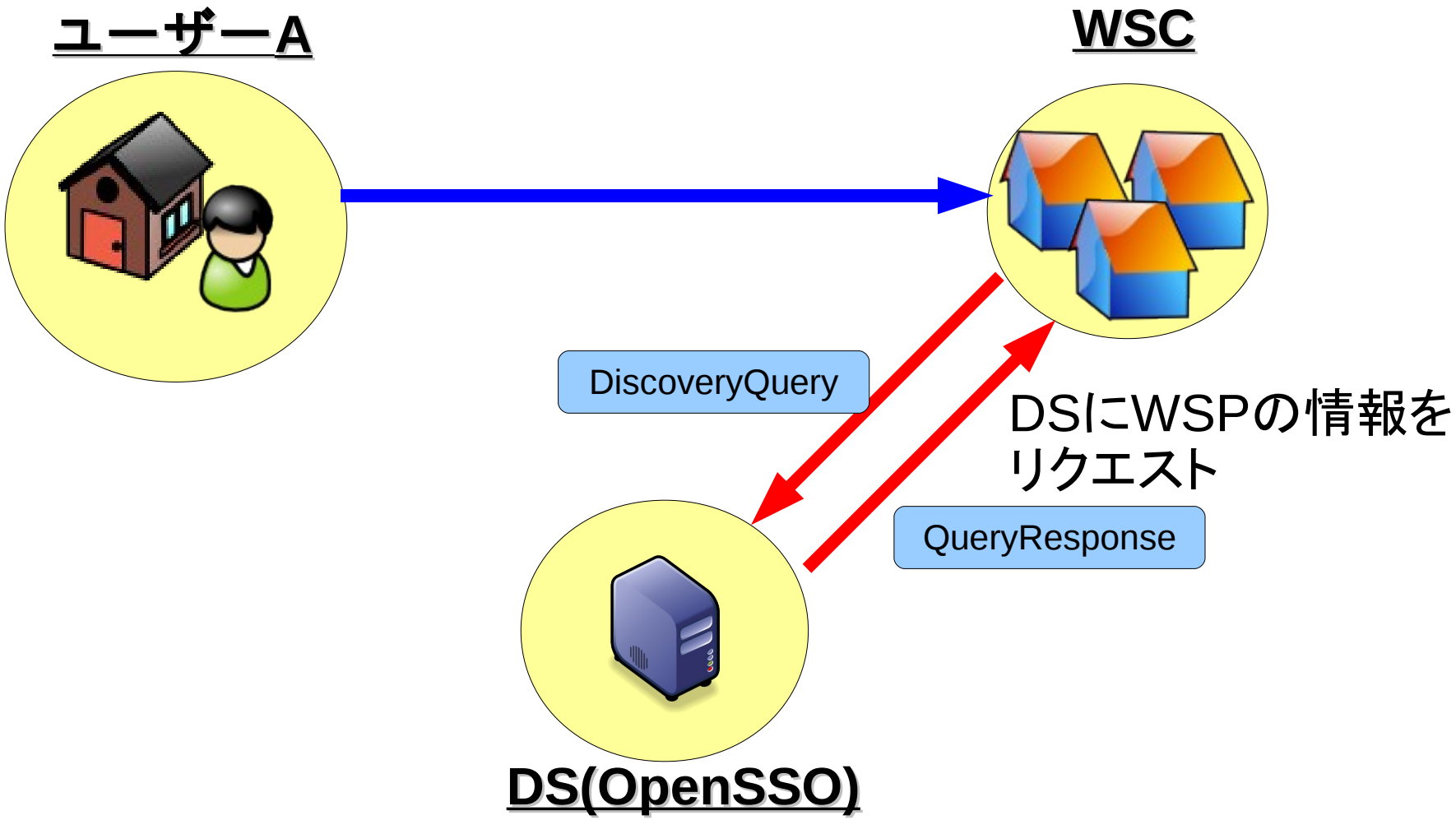
- WSCやユーザー(LUAD)が、SAMLを使ってIdPと通信する際の認証手段を定義

ID-WSF People Service

- ユーザーが他のユーザーの属性情報にアクセスするためのセキュリティやプライバシー保護の要件の定義

OpenSSOソースコード解析

属性情報の取得の流れ



Discovery Service

- products/federation/library/source/com/sun/identity/saml2/idpdiscovery

ファイル名	処理内容
ConfiguratorFilter.java	IdPのDS設定関連
CookieReaderServlet.java	SPのReader Service
CookieUtils.java	HTTPのCookieの処理
CookieWriterServlet.java	IdPのWriter Service
Debug.java	デバッグ用の処理
IDPDiscoveryConstatns.java	定数の定義
IDPDiscoveryWARConfigurator.java	IdPのDiscovery設定用のクラスファイル
SystemProperties.java	システム設定読み取り用の処理

OpenSSOのWSF関連処理

- products/federation/library/source/com/sun/identity/wsfederation/servlet
  - WSFederationServlet.java
    - Servletの処理
      - GET : doGet()
      - POST : doPost()

```
doGet(request, response){
   action = WSFederationActionFactory.createAction(request,response)
   action.process()
}
```

product/federation/library/source/com/sun/identity/wsfederation/servlet/WSFederationServlet.java : WSFederationAction.createAction()

リクエストに含まれる各種パラメーターの値の取り出し
request.getParameter()

“wa”	: action
“wresult”	: result
“whr”	: home realm
“wtrealm”	: requesting realm
“wreply”	: destination url
“wct”	: current time
“wctx”	: context value

リクエストの種類に応じたインスタンスの作成

GETの処理
wtrealmがあるなら→ **IPSigninRequest()**
wtrealmがなければ→ RPSigninRequest()

POSTの処理
RPSigninResponse()

products/federation/library/source/com/sun/identity/wsfederation/servlet/IPSigninRequest.java : IPSigninRequest.process()

IdPのメタ情報の取得
WSFederationMetaUtils.getMetaAliasByUri()

IdP情報の取得
WSFederationMetaManager.getEntityByMetaAlias()
WSFederationMetaUtils.getRealmByMetaAlias()
WSFederationMetaManager.getEntityByTokenIssuerName()

リモートPRの確認 WSFederationMetaManager.isTrustedProvider()

セッション情報取得 WSFederationUtils.sessionProvider.getSession()

まだログインしていない場合 redirectAuthentication()

sendResponse()

products/federation/library/source/com/sun/identity/wsfederation/meta/WSFederationMetaUtils.java : getMetaAliasByUri()

- 与えられたURIに”metaAlias” + αの文字列が含まれていれば、”metaAlias” 以降の文字列を追加して返す

定数埋め込み：index + 9 は良くないのでは...

products/federation/library/source/com/sun/identity/wsfederation/meta/WSFederationMetaManager.java : getEntityByMetaAlias()

- metaAliasとして指定された文字列を基に、FederationIDを返す

レルム名の取得
WSFederationMetaUtils.getRealmByMetaAlias()

レルム名から全entityIDの取得
configInst.getAllConfigurationNames()

レルム名とentityIDからIdPかSPの設定情報の取得
getEntityConfig()
FederationConfigElement.getIDPSSOCOnfigOrSPSSOConfig()

エイリアス名が一致するconfig情報をリターン

参考資料

- Liberty Alliance ID-WSF 2.0仕様書
  - http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates/
    - liberty-idwsf-overview-v2.0.pdf
    - liberty-idwsf-disco-svc-v2.0-original.pdf
- Liberty Alliance Wiki
  - http://wiki.projectliberty.org/index.php/JapanSIG/Documents/TechTutorials
    - Liberty Alliance ID-WSF仕様について