

# OpenSSO勉強会 OpenSSOのID-WSF実装



**OSSTech**

オープンソース・ソリューション・テクノロジー株式会社

2010/02/02

武田 保真

# ID-WSFサービスの構築

- 「連携」タブから設定



バージョン ログアウト ヘルプ

ユーザー: amAdmin amAdmin サーバー: sso1.yasu.lan.osstech.co.jp

OpenSSO Java  
Sun™ Microsystems, Inc.

共通タスク   アクセス制御   **連携**   Web サービス   設定   セッション

✖ トラストサークル設定   ✖ SAML1.x Configuration

### トラストサークル設定

このセクションは、トラストサークルのプロパティの設定に使用できます。エンティティテーブルは、プロバイダのインポートやエクスポートなどエンティティプロバイダの管理に使用できます。エンティティは、エンティティテーブルに作成した後で、トラストサークルに追加できます。

**トラストサークル (0 項目)**

名前	エンティティ	レルム	状態
利用可能な COT がありません。「新規...」ボタンを選択して作成してください。			

**エンティティプロバイダ (0 項目)**

名前	プロトコル	タイプ	場所	レルム
利用可能なエンティティがありません。「新規...」ボタンを選択して作成してください。				

⏪ 先前に戻る

# ID-WSFのサービス設定

- IdP設定、SP設定
  - 「エンティティプロバイダ」の「新規」作成
  - 「プロバイダのプロトコル選択」
    - SAMLv2、IDFF、WS連携(AD連携)
  - 各サービスの値の設定

# OpenSSOのID-WSF実装

- 管理画面の「Webサービス」
  - 「個人プロフィール」
    - idpp : ID Personal Profile
  - 「ディスカバリサービス」
    - disco: discovery service
  - 「SOAPバインドサービス」
  - 「認証サービス」
- 関連ソースコード
  - products/federation/library/source以下

# 「個人プロフィール」

- Liberty AllianceのID-SISに基づいて、個人のプロフィール情報を交換するための実装



The screenshot shows the OpenSSO administration console. At the top, it displays the user 'amAdmin' and server 'sso1.yasu.lan.osstech.co.jp'. The main navigation bar includes tabs for '共通タスク', 'アクセス制御', '連携', 'Web サービス', '設定', and 'セッション'. The '設定' (Settings) tab is active, and the '個人プロフィール' (Individual Profile) sub-tab is selected.

The configuration page is titled 'Liberty 個人プロフィールサービス' (Liberty Individual Profile Service). It contains the following fields:

- リソース ID マッパー:
- オーサライザ:
- 属性マッパー:
- プロバイダ ID:
- ネーミング方式:  FirstMiddleLast
- ネームスペースプレフィックス:

Below the configuration fields, there is a section titled 'サポートされているコンテナ (11 項目)' (Supported Containers (11 items)). It includes a table with checkboxes for selecting containers:

<input checked="" type="checkbox"/>	名前
<input type="checkbox"/>	EmploymentIdentity
<input type="checkbox"/>	MsgContact
<input type="checkbox"/>	EmergencyContact
<input type="checkbox"/>	InformalName
<input type="checkbox"/>	LegalIdentity
<input type="checkbox"/>	Demographics

# 「個人プロフィール」パラメーター

- リソースIDマッパー

- ユーザーIDとリソースIDをマッピングするためのJavaのクラスを指定

- デフォルト値

- `com.sun.identity.liberty.ws.interfaces.ResourceIDMapper.java` を指定

- `getResourceID()` : ユーザーIDからリソースIDを取得

- `getUserID()` : リソースIDからユーザーIDを取得

- オーサライザ

- 個人プロフィールを要求するWSCの承認を行うためのJavaのクラスを指定

- デフォルト値

- `com.sun.identity.liberty.ws.idpp.plugin.IDPPAuthorizer` (ソースが無い?)

# 「個人プロフィール」パラメーター

- 属性マッパー
  - 個人プロフィールの属性を、OpenSSOの属性にマッピングするクラスを指定
    - デフォルト値
      - `com.sun.identity.liberty.ws.idpp.plugin.IDPPAttributeMapper`
        - `getDSAttribute()`  
Personal Profileの属性名に対するLDAPの属性名を返す
- プロバイダID
  - Personal Profileサービスを提供するID
    - デフォルト値
      - `http://サーバー:8080/opensso/Liberty/idpp`

# 「個人プロフィール」パラメーター

- ネーミング方式
  - 「FirstMiddleLast」しか選択できない...
  - ヘルプには「名姓」もあると書かれているが...
- ネームスペースプレフィックス
  - PPサービスのXMLプロトコルに含まれる要素名のプレフィックス
- サポートされるコンテナ
  - PPサービスで利用可能な属性名のリスト

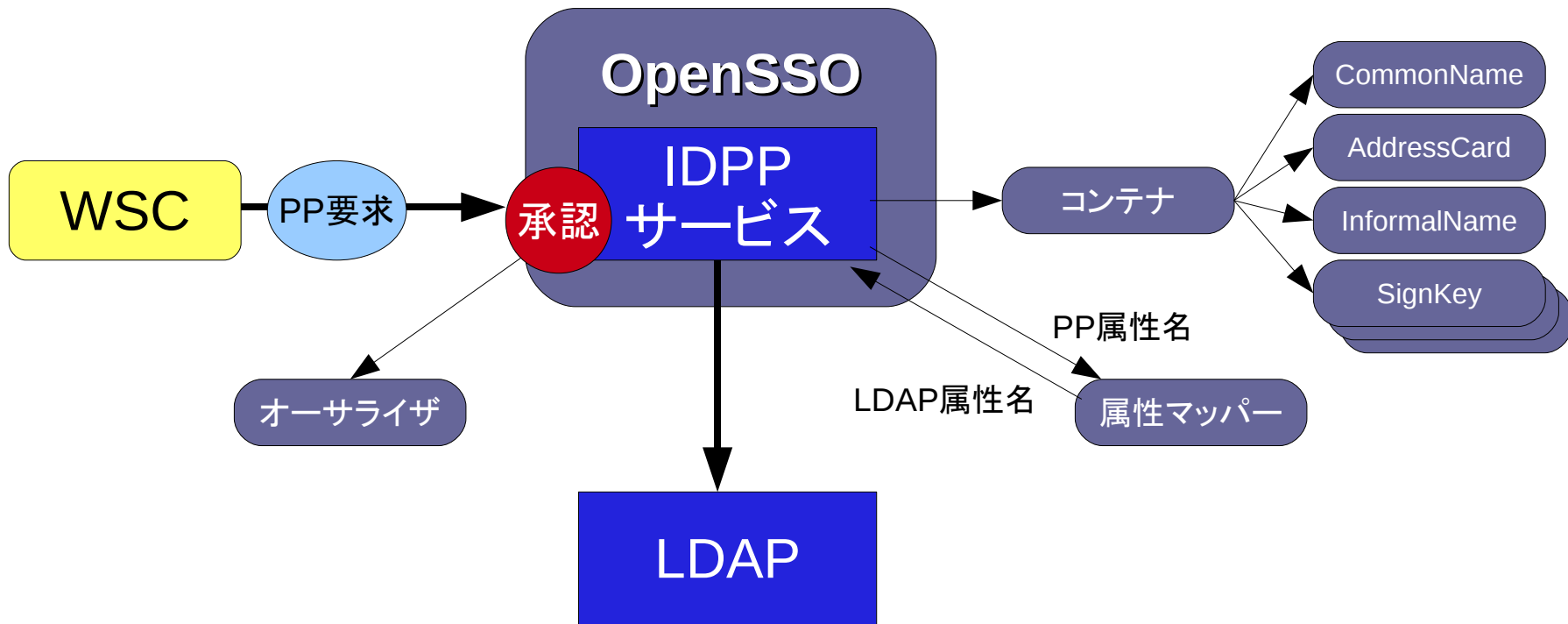


# 「個人プロフィール」パラメーター

- PPLDAP属性マッピングリスト
  - PPサービスの属性とLDAP属性の1対1マッピングの情報

# 「個人プロフィール」サービス

http://server:8080/opensso/Liberty/idpp



# IDPPサービスの実装

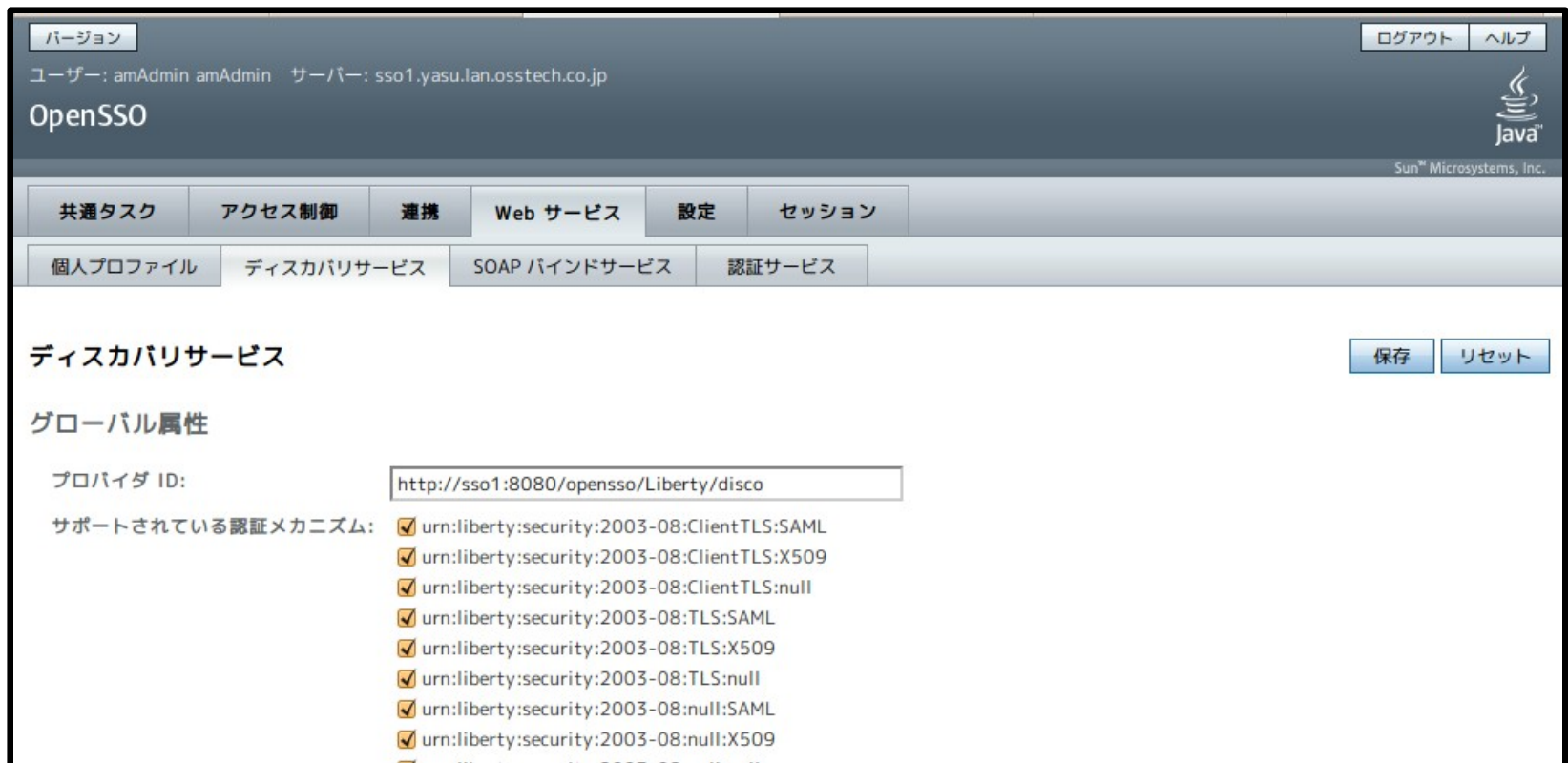
- `com.sun.identity.liberty.ws.idpp`
  - `PPRequestHandler.java`
    - IDPPサービスに対するSOAPメッセージ要求を、解析し、`PersonalProfile`に対する要求へと処理する。
  - `PersonalProfile.java`
    - WSCからのPP要求に対して、Directory Serviceから値の取得や更新を行う
      - WSCの認証
        - `SessionManager.getProvider().isValid()`
      - Directory Serviceに登録されているユーザーのDN取得
        - `getUserDN()`
      - 要求されたユーザーの属性値の取得
        - `getUserData()`

# PersonalProfile.java

- queryData()
  - IDPPサービスに対して要求されたリソースIDに対して、LDAPに登録されている該当ユーザーの各属性値を返す
    - WSCの認証
      - SessionManager.getProvider().isValid()
    - リソースIDからユーザーのDNへのマッピング
      - getUserDN()
    - IDPPに要求された属性情報をLDAPから取得
      - getUserData()
    - 取得したデータをXMLに変換
      - container.toXMLDocument()

# ディスカバリサービス

- IDサービスを提供しているWebサービスプロバイダの情報を、クライアントに提供するためのサービス



The screenshot shows the OpenSSO administration interface. At the top, it displays the user 'amAdmin', server 'sso1.yasu.lan.osstech.co.jp', and the OpenSSO logo. A navigation menu includes '共通タスク', 'アクセス制御', '連携', 'Web サービス', '設定', and 'セッション'. The 'Web サービス' menu is expanded to show '個人プロフィール', 'ディスカバリサービス', 'SOAP バインドサービス', and '認証サービス'. The 'ディスカバリサービス' page is active, showing a '保存' (Save) and 'リセット' (Reset) button. Under the 'グローバル属性' (Global Properties) section, the 'プロバイダ ID' (Provider ID) is set to 'http://sso1:8080/opensso/Liberty/disco'. A list of supported authentication mechanisms is shown, all of which are checked:

- urn:liberty:security:2003-08:ClientTLS:SAML
- urn:liberty:security:2003-08:ClientTLS:X509
- urn:liberty:security:2003-08:ClientTLS:null
- urn:liberty:security:2003-08:TLS:SAML
- urn:liberty:security:2003-08:TLS:X509
- urn:liberty:security:2003-08:TLS:null
- urn:liberty:security:2003-08:null:SAML
- urn:liberty:security:2003-08:null:X509

# 「ディスクカバリサービス」パラメーター

- プロバイダID
  - ディスクカバリサービスを提供するURI
    - デフォルト値
      - `http://server:8080/opensso/Liberty/disco`
- サポートされている認証メカニズム
  - WSCが要求を行った際に、WSPで認証するためのメカニズム
- サポートされているディレクティブ
  - ディレクトリサービスのリソースをWSCに提供する際に、WSCに求められるアクセスポリシーを設定
- オーサライザプラグインクラス
  - WSCの認証を行うクラスの設定
    - `com.sun.identity.liberty.ws.disco.plugins.DefaultDiscoAuthorizer`

# 「ディスカバリサービス」パラメーター

- エントリハンドラプラグインクラス
  - ディスカバリサービスの処理を行うハンドラクラス
    - デフォルト値
      - `com.sun.identity.liberty.ws.disco.plugins.UserDiscoEntryHandler` (用意されていない)
- リソースIDマッパープラグイン用のクラス
  - 各ディスカバリサービスに対する、IDマッパーの実装
    - デフォルト値
      - `com.sun.identity.liberty.ws.disco.plugins.Default64ResourceIDMapper`

# 「ディスカバリーサービス」パラメーター

- 暗黙のリソース
  - デフォルト値: 無効
  - ID-WSF 1.x仕様のための実装
  - 有効にした場合、エン트리ハンドラとして、「グローバルエントリハンドラプラグインクラス」が使用される。
  - 無効(ID-WSF 2.0仕様)の場合、エントリハンドラとして、「エントリハンドラプラグインクラス」が利用される(デフォルト)

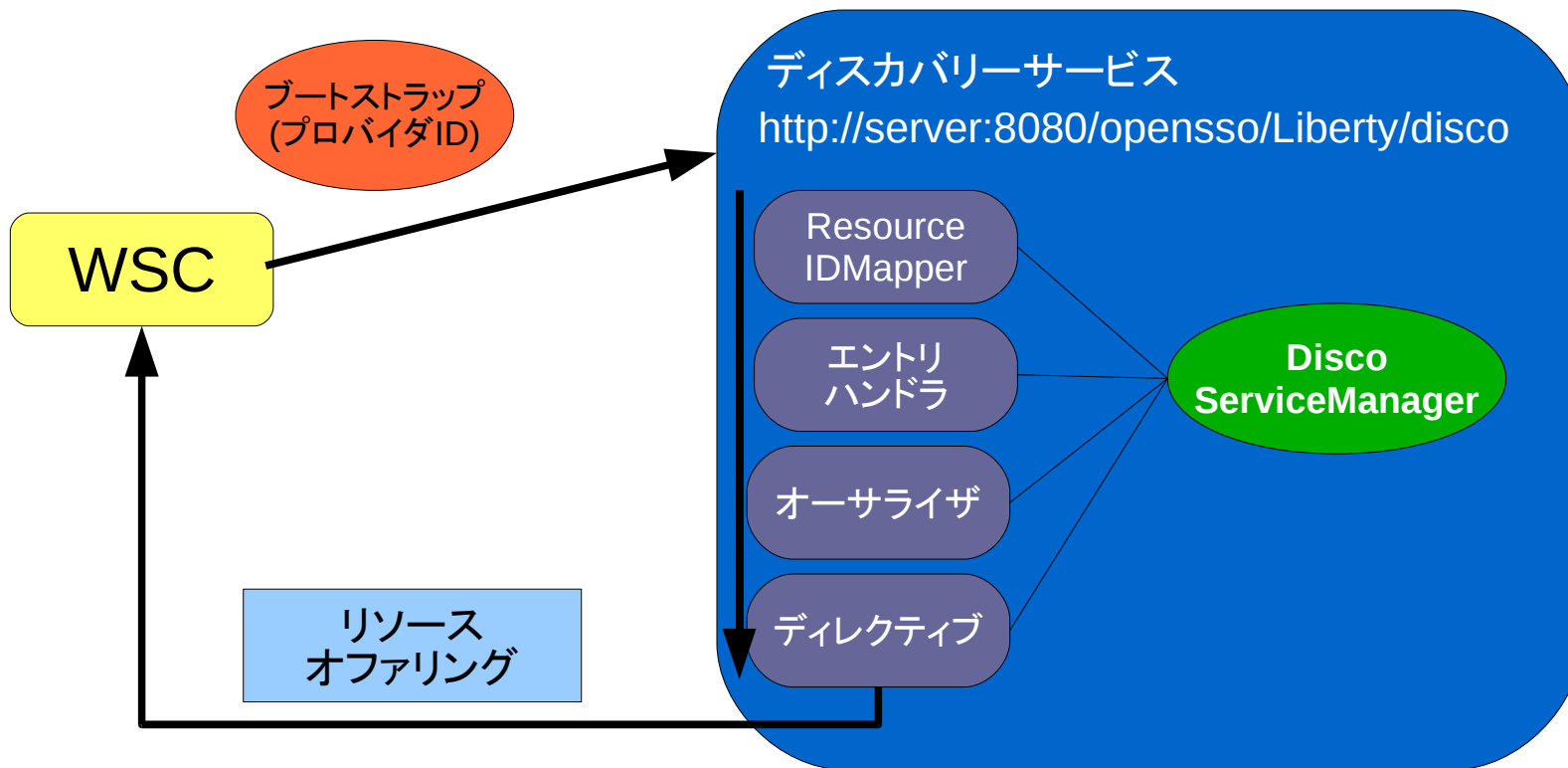


# 「ディスクバリーサービス」パラメーター

- ブートストラップとは
  - SSOアサーションに、ディスクバリーサービスのプロバイダID(URL)などを含めて、WSCに提供する機能
  - SSO完了後に、WSCは受け取ったプロバイダIDを使って、ディスクバリーサービスに対して、WSPを探索するためのQueryを発行することができる。
- ブートストラップのリソースオフリング
  - ブートストラップには、1つだけリソース情報を含めることが可能
    - ディスクバリーサービスのプロバイダIDなどを設定

<http://docs.sun.com/app/docs/doc/820-3885/ggmjr?a=view>

# 「ディスカバリーサービス」概要



# ディスカバリーサービスの実装

- `com.sun.identity.liberty.ws.disco.DiscoveryService`
  - ディスカバリーサービスの要求を処理
    - `getAuthenticationMechanism()`
      - リクエスト中の認証メカニズムを判定(X509, SAML, BEARER,null)
    - `lookup()`
      - 要求されたリソース情報を提供
        - `getResourceID()`
        - `idMapper = DiscoServiceManager.getResourceIDMapper()`
        - `userDN = idMapper.getUserID()`
        - `entryHandler = DiscoServiceManager.getDiscoEntryHandler()`
        - `authorizer = DiscoServiceManager.getAuthorizer()`
        - `returnMap = DiscoUtils.checkPolicyAndHandleDirectives()`

# com.sun.identity.liberty.ws.disco.plugins.Default64ResourceIDMapper.java

- getResourceID(providerID, userID)
  - ユーザーIDを、プロバイダから取得するためのリソースIDに変換
  - 書式は、「providerID + “/” + base64encode(userID)」
    - <http://server:8080/opensso/Liberty/disco/xxxxxxxxxx>
- getUserID(providerID, resourceID)
  - リソースIDから、ユーザーIDを取得