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

ID-WSFのサービス設定

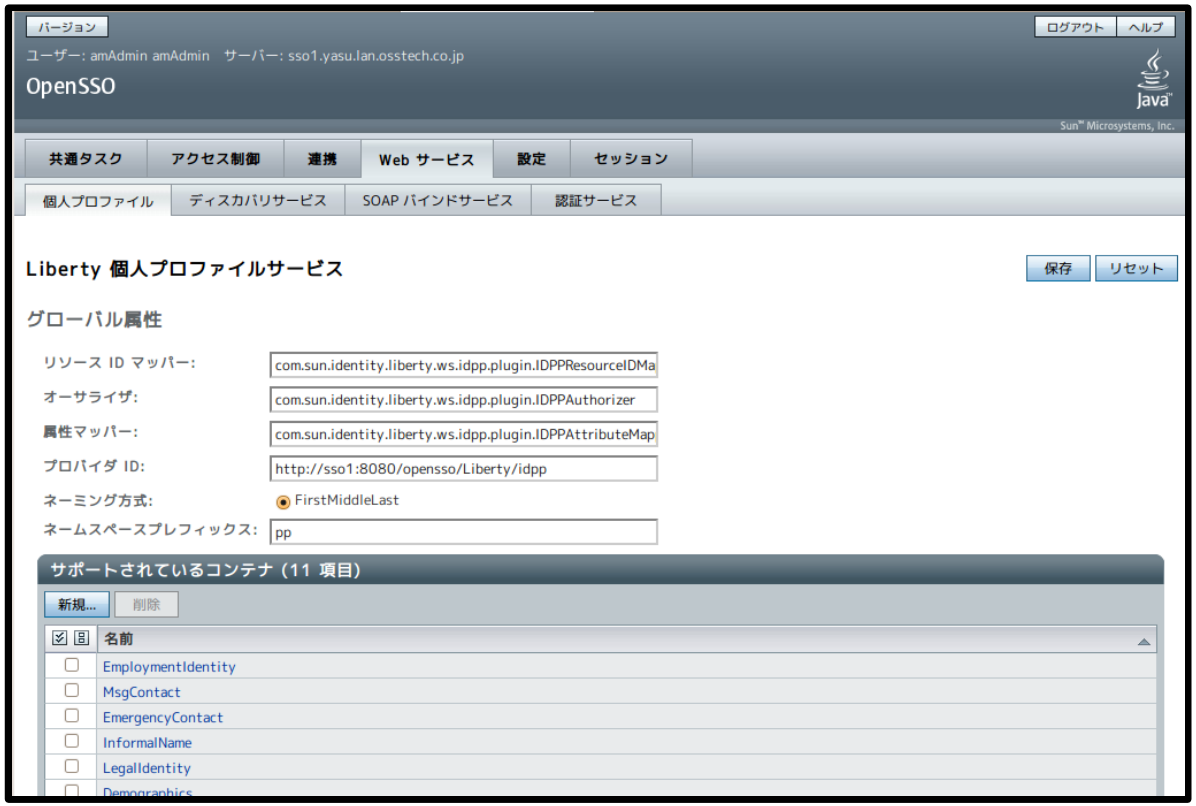
- IdP設定、SP設定
  - 「エンティティプロバイダ」の「新規」作成
  - 「プロバイダのプロトコル選択」
    - SAMLv2、IDFF、WS連携(AD連携)
  - 各サービスの値の設定

OpenSSOのID-WSF実装

- 管理画面の「Webサービス」
  - 「個人プロファイル」
    - 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

「個人プロファイル」

- Liberty AllianceのID-SISに基づいて、個人のプロファイル情報を交換するのための実装



「個人プロファイル」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
  - 個人プロファイルを要求する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?)

「個人プロファイル」パラメーター

- 属性マッパー
  - 個人プロファイルの属性を、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

「個人プロファイル」パラメーター

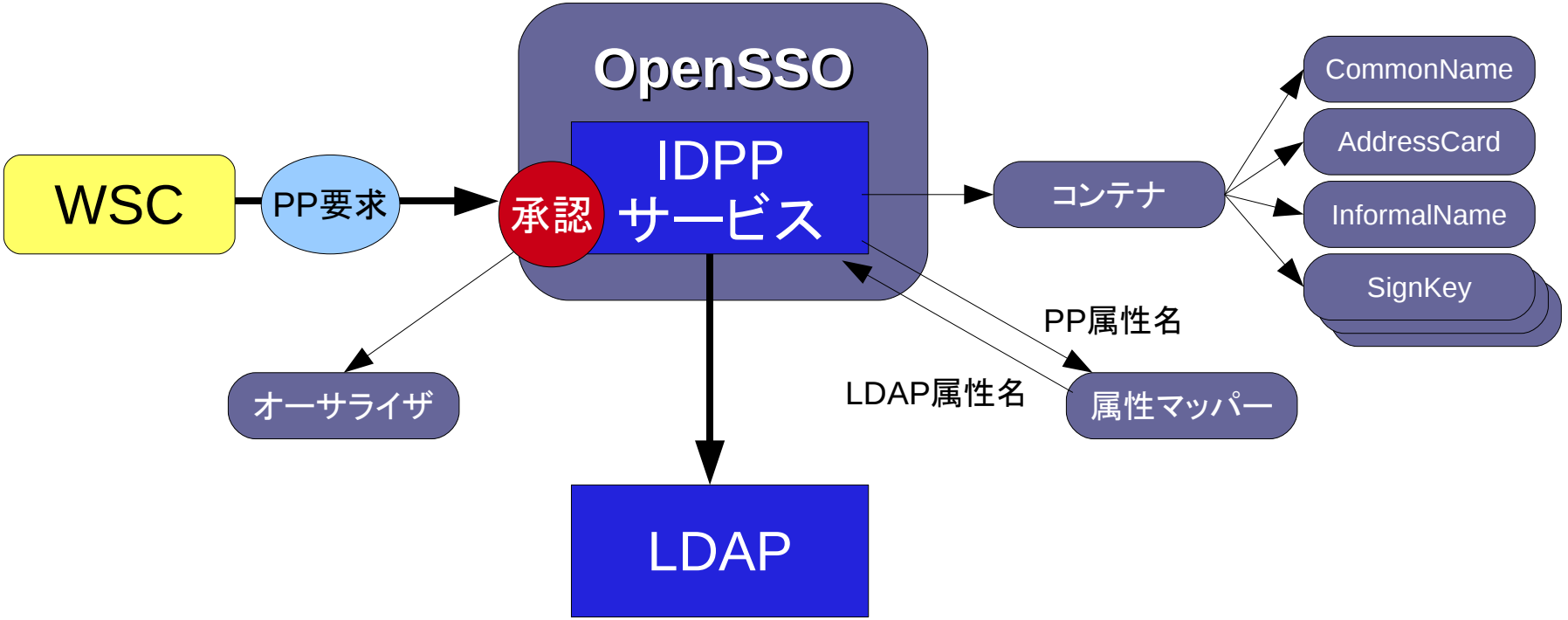
- ネーミング方式
  - 「FirstMiddleLast」しか選択できない...
  - ヘルプには「名姓」もあると書かれているが...
- ネームスペースプレフィックス
  - PPサービスのXMLプロトコルに含まれる要素名のプレフィックス
- サポートされるコンテナ
  - PPサービスで利用可能な属性名のリスト

「個人プロファイル」パラメーター

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

「個人プロファイル」サービス

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



IDPPサービスの実装

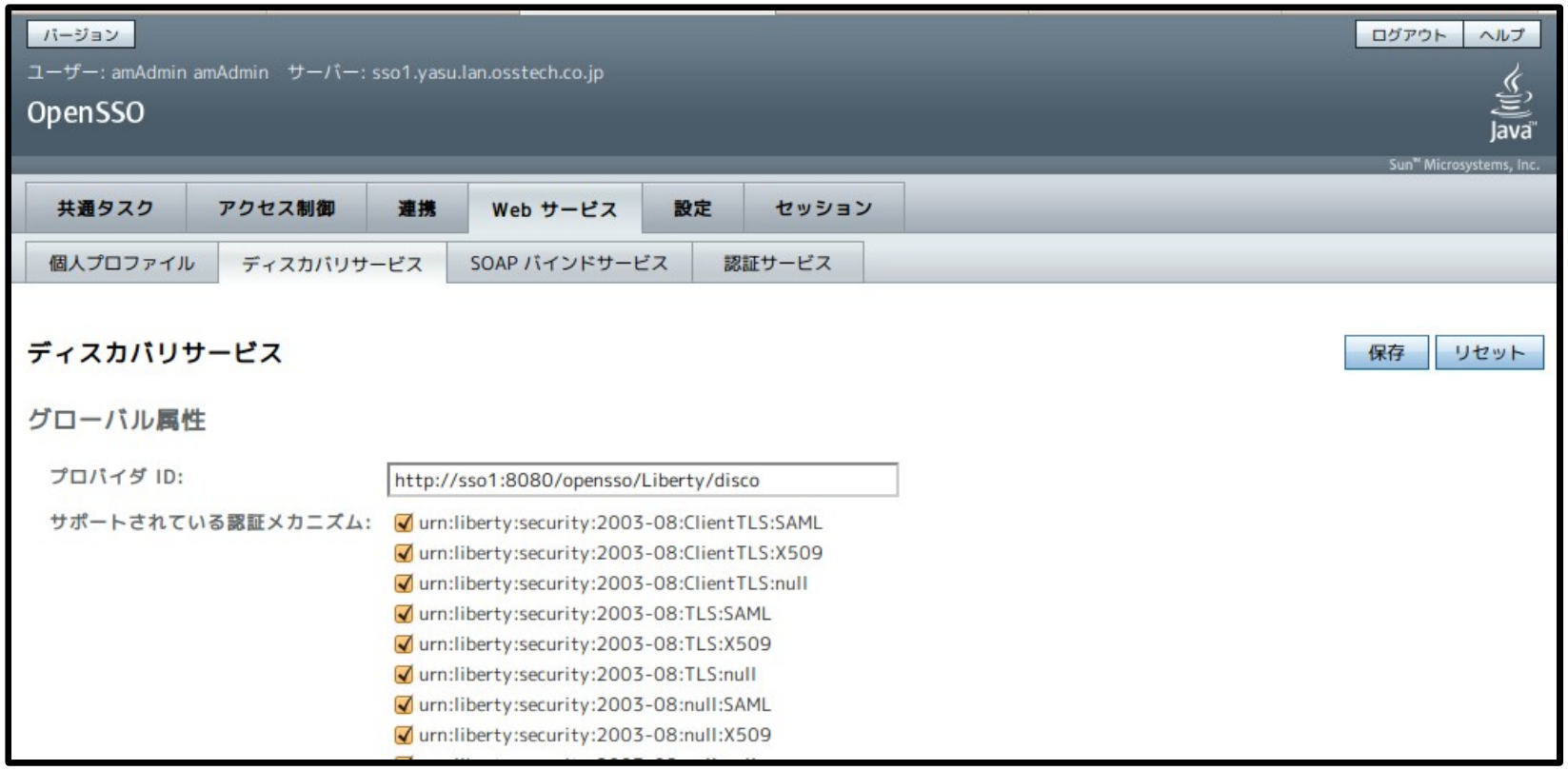
- com.sun.identity.liberty.ws.idpp
  - PPRequestHandler.java
    - IDPPサービスに対するSOAPメッセージ要求を、解析し、PersonalProfileに対する要求へと処理する。
  - PersonalProfile.java
    - WSCからのPP要求に対して、Directory Serviceから値の取得や更新を行う
      - WSCの認証
        - SessionManager.getProvider().isValid()
      - Directory Serviceに登録されているユーザーの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()
    - 取得したデーターをXMLに変換
      - container.toXMLDocument()

ディスカバリーサービス

- 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



「ディスカバリサービス」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
  - 各ディスカバリーサービスに対する、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

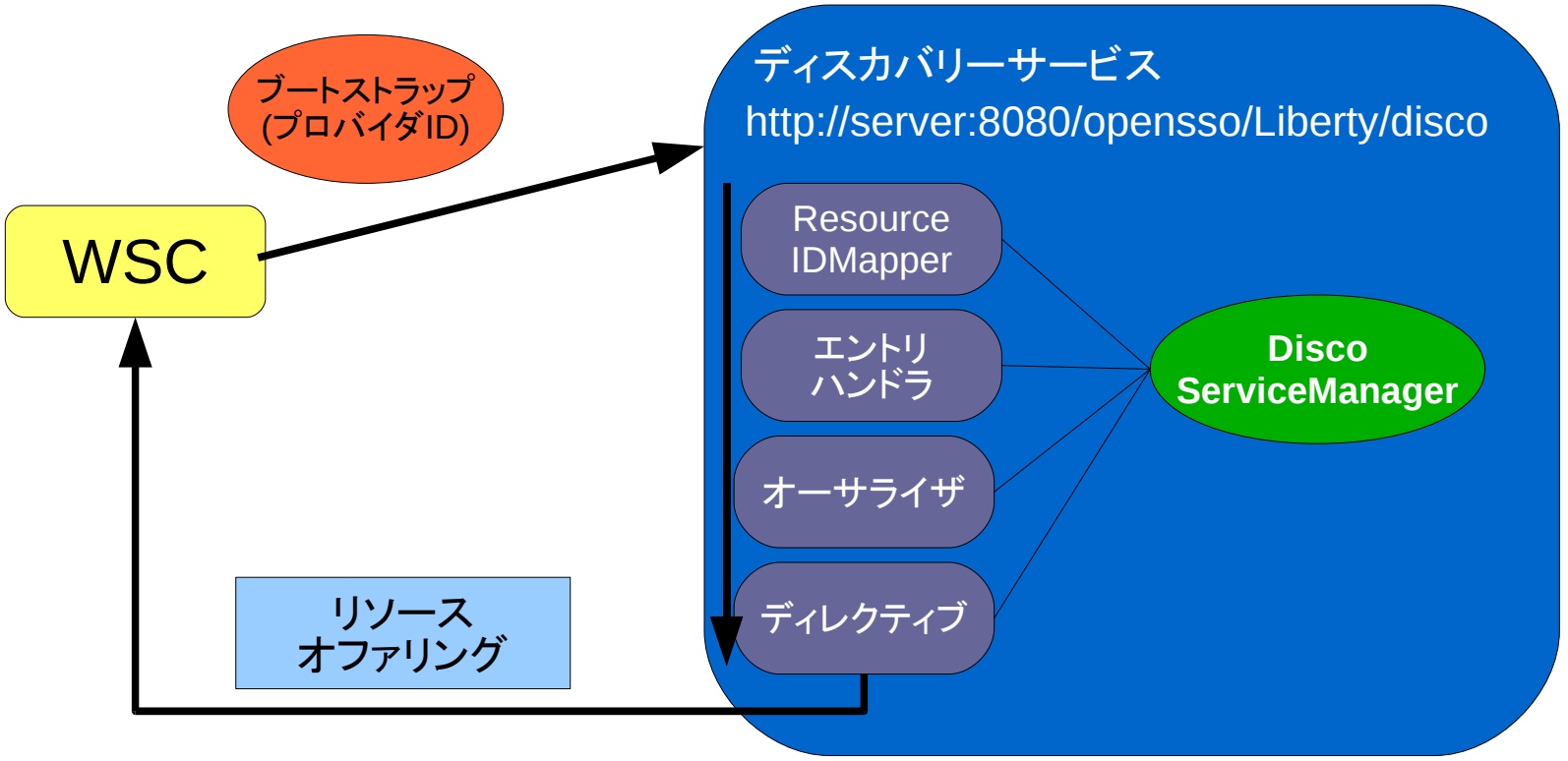
- 暗黙のリソース
  - デフォルト値: 無効
  - ID-WSF 1.x仕様のための実装
  - 有効にした場合、エントリハンドラとして、「グローバルエントリハンドラプラグインクラス」が使用される。
  - 無効(ID-WSF 2.0仕様)の場合、エントリハンドラとして、「エントリハンドラプラグインクラス」が利用される(デフォルト)

「ディスカバリーサービス」パラメーター

- ブートストラップとは
  - SSOアサーションに、ディスカ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、ディスカ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ァリング
  - 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
    - ディスカ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.DiscovertyService
  - ディスカバリーサービスの要求を処理
    - getAtuthenticationMechanism()
      - 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/xxxxxxxxx
- getUserID(providerID, resourceID)
  - リソースIDから、ユーザーIDを取得