OpenAM最新動向と
導入事例紹介

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

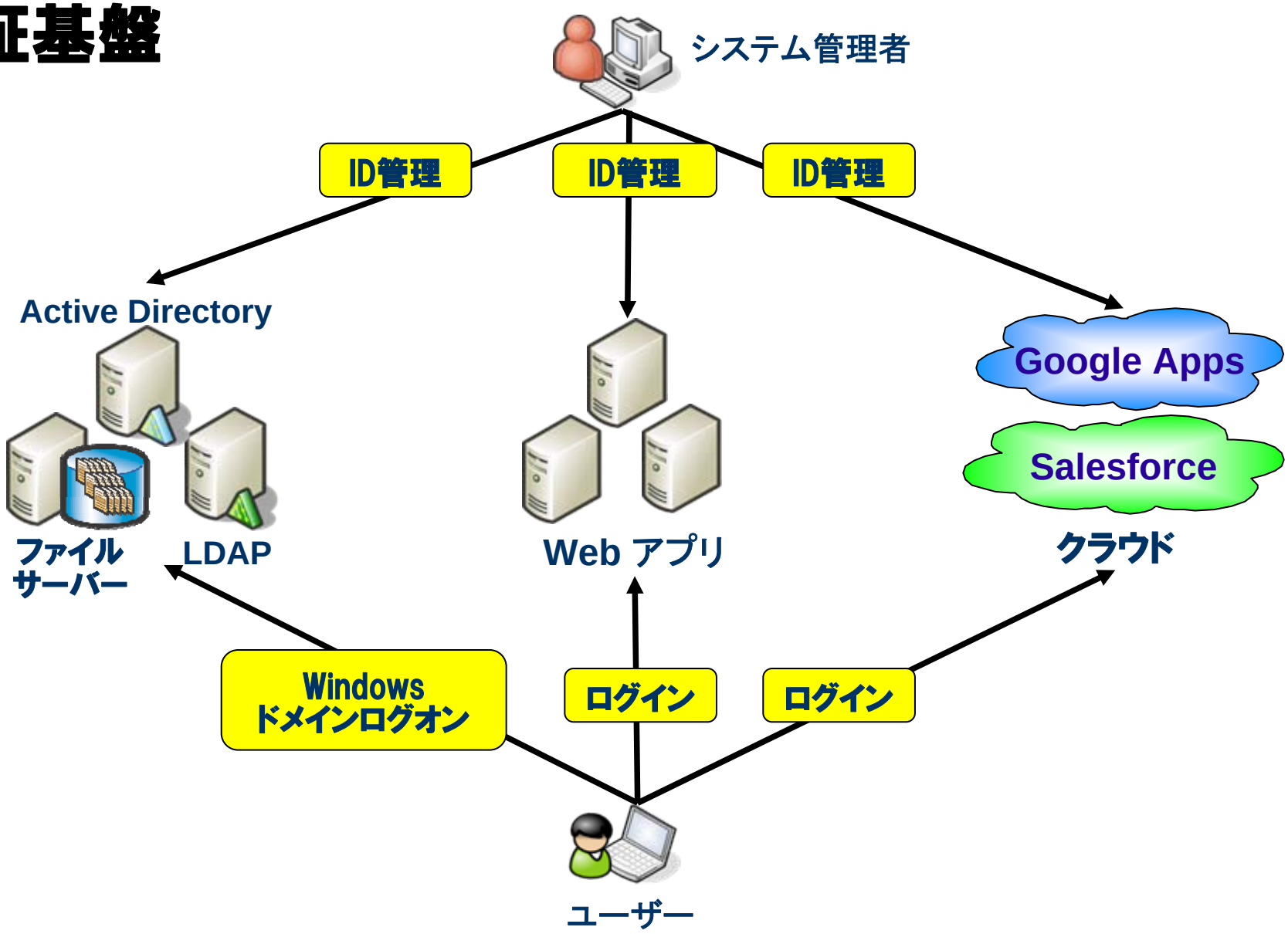
オープンソース・ソリューション・テクノロジ株式会社

- **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 ﾊﾟｰﾄﾅｰ様	・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		

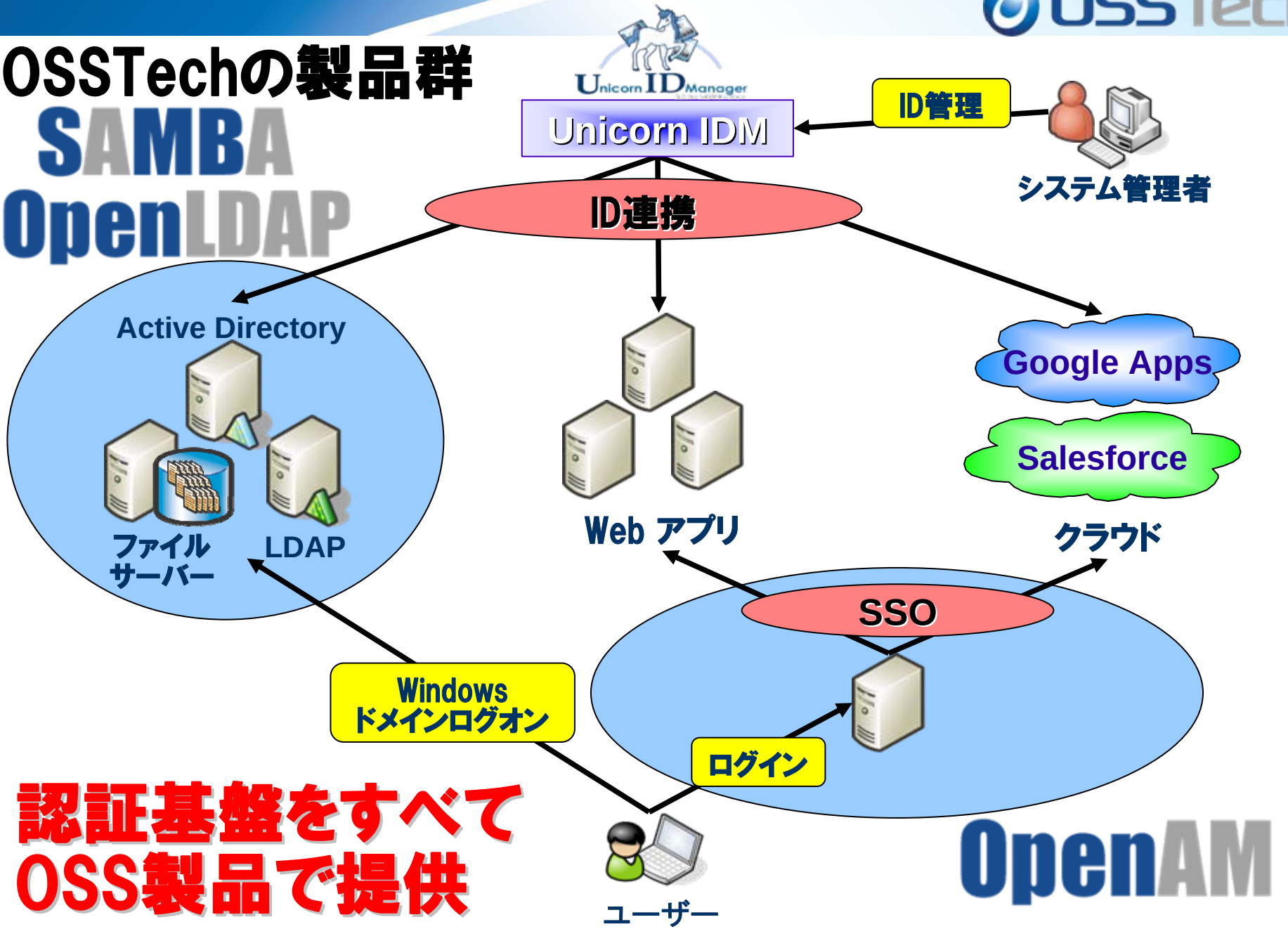
認証基盤



OSSTechの製品群

SAMBA

OpenLDAP



認証基盤をすべて
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

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/

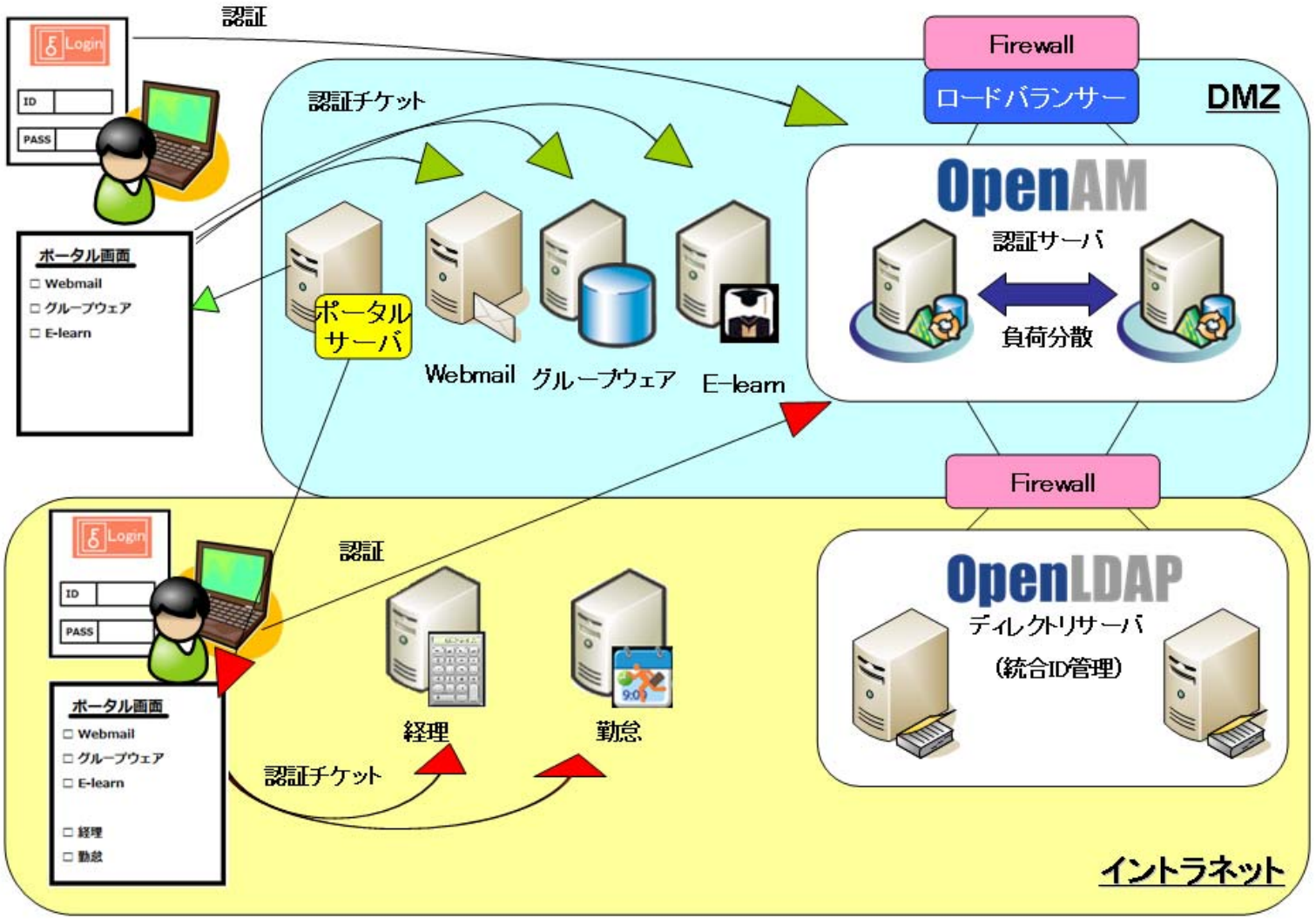
OpenAM導入動向

- 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

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



第2回OpenSSO＆OpenAM コンソーシアムセミナー

OpenAM 10の新機能紹介

2012年4月5日
オープンソース・ソリューション・テクノロジ株式会社
岩片　靖
http://www.osstech.co.jp/
お問い合わせ info@osstech.co.jp

目次

- ForgeRockの近況
  - 企業としての評価
  - OpenAM関連製品
  - OpenAM ロードマップ
- 便利な新機能
  - 開発に便利な新機能
  - 運用・管理に便利な新機能
- アダプティブ・リスク認証モジュール
  - アダプティブ・リスクの考え方
  - 設定例
- Oauth 2.0を使ったFacebookとの連携
  - Oauth 2.0に基づくユーザ情報の取得
  - 様々なシナリオ

最近のForgeRock

とっても元気！

最近のForgeRock

- Gartnerによる評価
  - “Cool Vendors in Identity and Access Management, 2011”
  - 先進的な技術を持ち今後の成長が注目されるベンダー
- Accel Partnersからの資金調達
  - $7M規模のシリーズAファンド
  - Accel Partnersの成功事例：
    - 2005年にFacebookへ$12Mのシリーズファンド
    - その他Groupon、LinkedInなど多数
- OSSTechとの協業
  - Nginxのポリシーエージェント開発
  - 現在はソースコードレビュー中
  - テスター募集中！

OpenAM関連製品

- OpenDJ (LDAPサーバ)
  - ユーザ事例：Ziggo（オランダの通信大手）
    - 250万ユーザエントリ
    - Sun DSEEからの移行
    - OpenAMによる認証とアクセス制御
- OpenIG (Identity Gateway)
  - 旧Apex Identity社の製品
  - リバース・プロキシ方式によるアクセス制御機能
  - パスワード・リプレイ機能、SAMLゲートウェイ機能
- OpenIDM（ID管理）
  - ForgeRock社で開発中
  - OpenAMとの連携機能強化

OpenAM　ロードマップ

- OpenAM 10 アーリーアクセス
  - 現在ダウンロード可能
- OpenAM 10 正式リリース
  - 4月16日にリリース予定
- OpenAM 10.1
  - Oauth 2.0 Provider
  - UIの改良（認証画面、セルフサービス画面）
  - セッション冗長化の改良
  - クラウド対応強化
- OpenAM 11.0
  - 様々な機能強化
  - スケーラビリティの向上

便利な新機能

リリースノートから
面白そうなものを抽出しました

開発に便利な新機能

- 大きな変更は無いが開発者の負担を軽減するような改良が追加されている
  - 認証モジュールを単一JARファイルとしてインストール
  - SAML2.0 IdPアダプタープラグイン
  - セッション数の上限に達した際の動作のカスタマイズ
  - REST　APIによるセッションのリフレッシュおよび残り時間の取得
  - セッション・アップグレード時に引き継ぐ属性を明示的に指定
  - .Net Fedletで暗号化されたアサーションに対応

運用・管理に便利な新機能

- より細かな管理と監視
  - LDAP接続プールの監視
  - ADとの連携強化
  - ユーザ毎のタイムゾーンに基づいたポリシー評価
  - デバックファイルのローテーション
- 新規認証モジュール（後述）
  - アダプティブ・リスク認証モジュール
  - Oauth 2.0 認証モジュール

アダプティブ・リスク認証モジュール

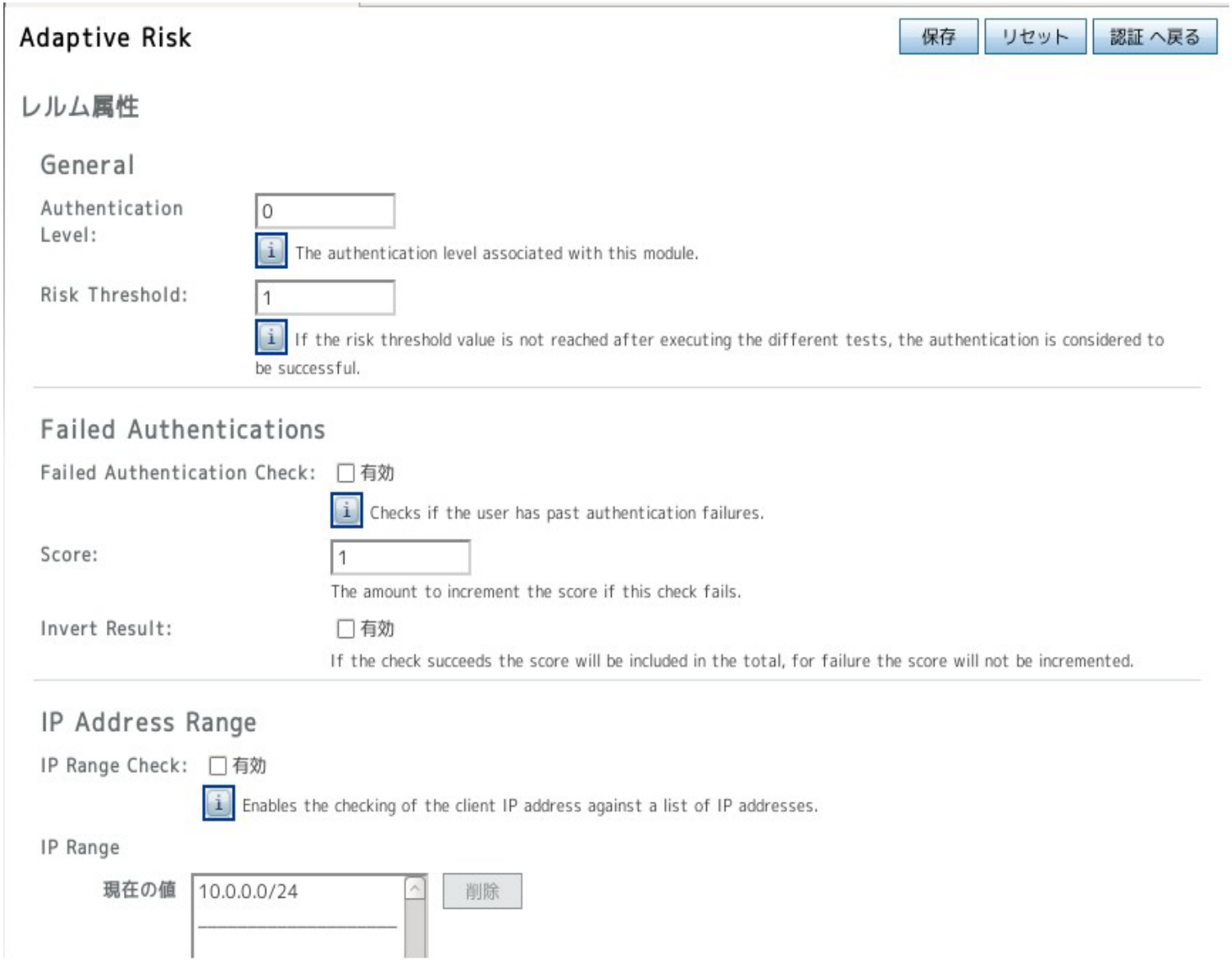
リスク評価に基づく認証強度の選択

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
  - 認証連鎖への組み込み
    - 多要素認証のなかのひとつの認証方式
    - 認証連鎖の定義

- 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：所属部署が営業とか？

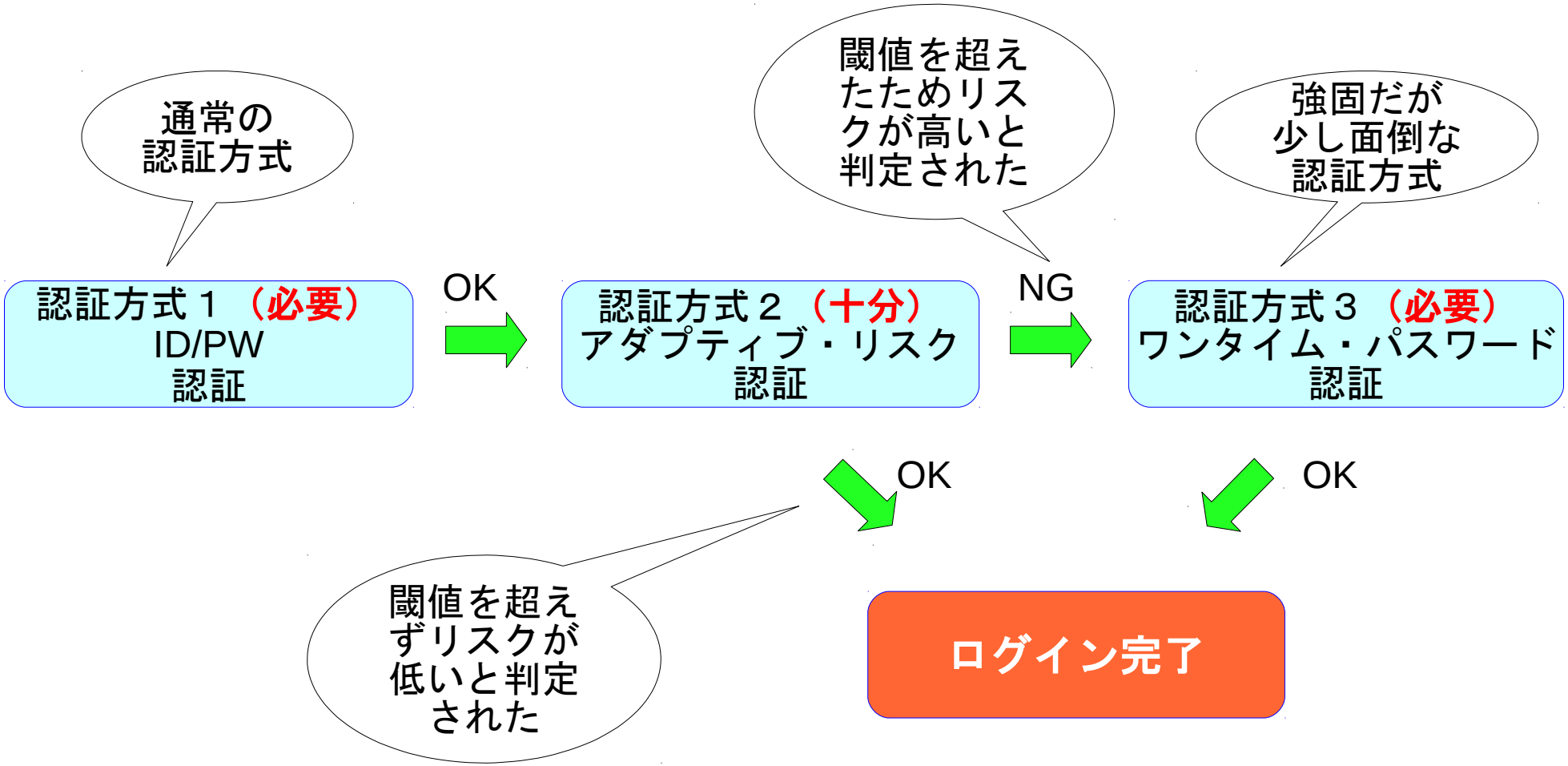
アダプティブ・リスク認証モジュールの設定



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

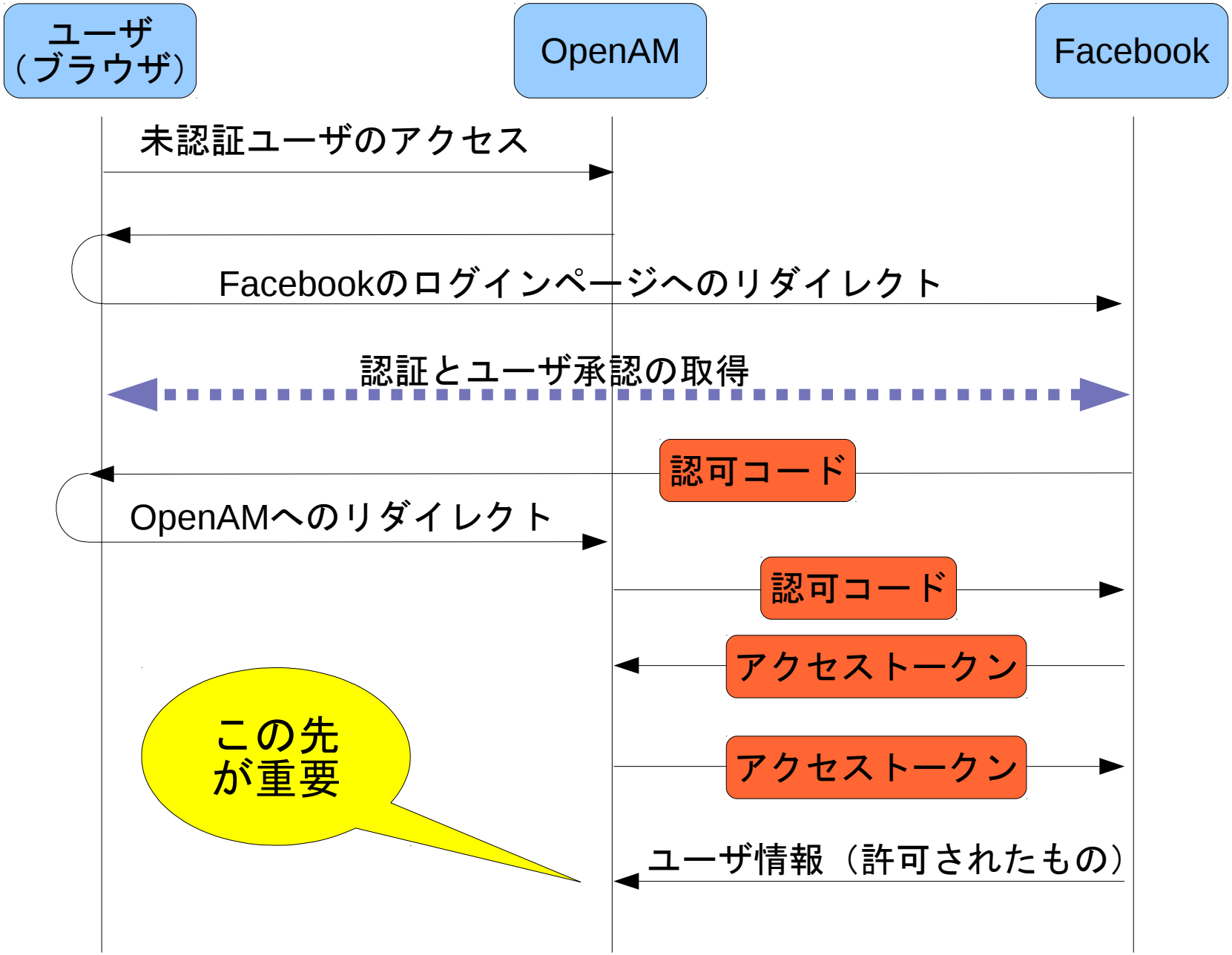
でも毎回だと
少し面倒！



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

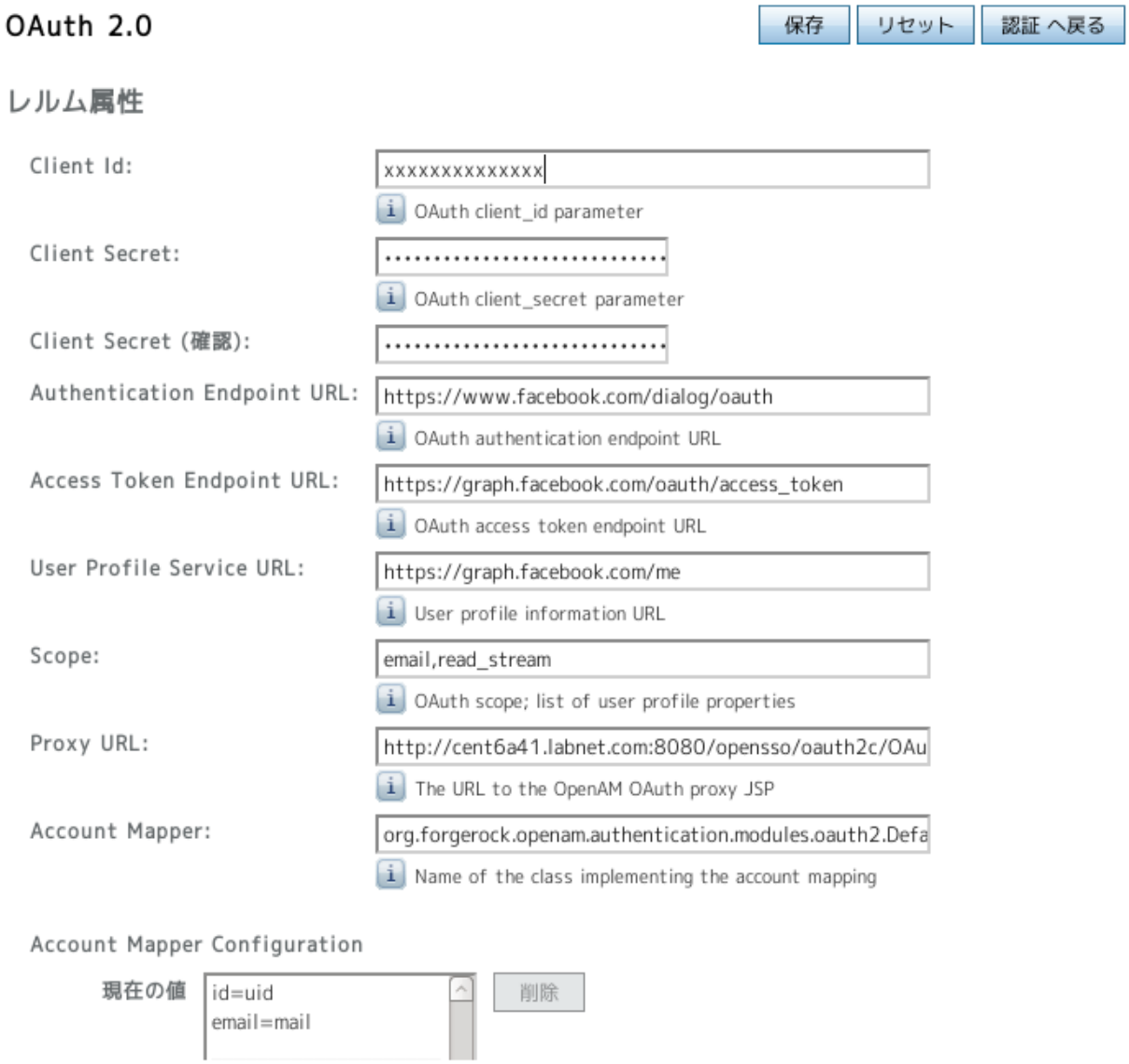
Oauth 2.0を使ったやりとり



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）



Oauth 2.0 認証モジュールの設定（その２）

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

OSSTech

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ *info@osstech.co.jp*