

OSSTechのOpenAMへの取り組み



OSSTech

2012年10月19日

小田切 耕司

オープンソース・ソリューション・テクノロジー株式会社

<http://www.osstech.co.jp/>

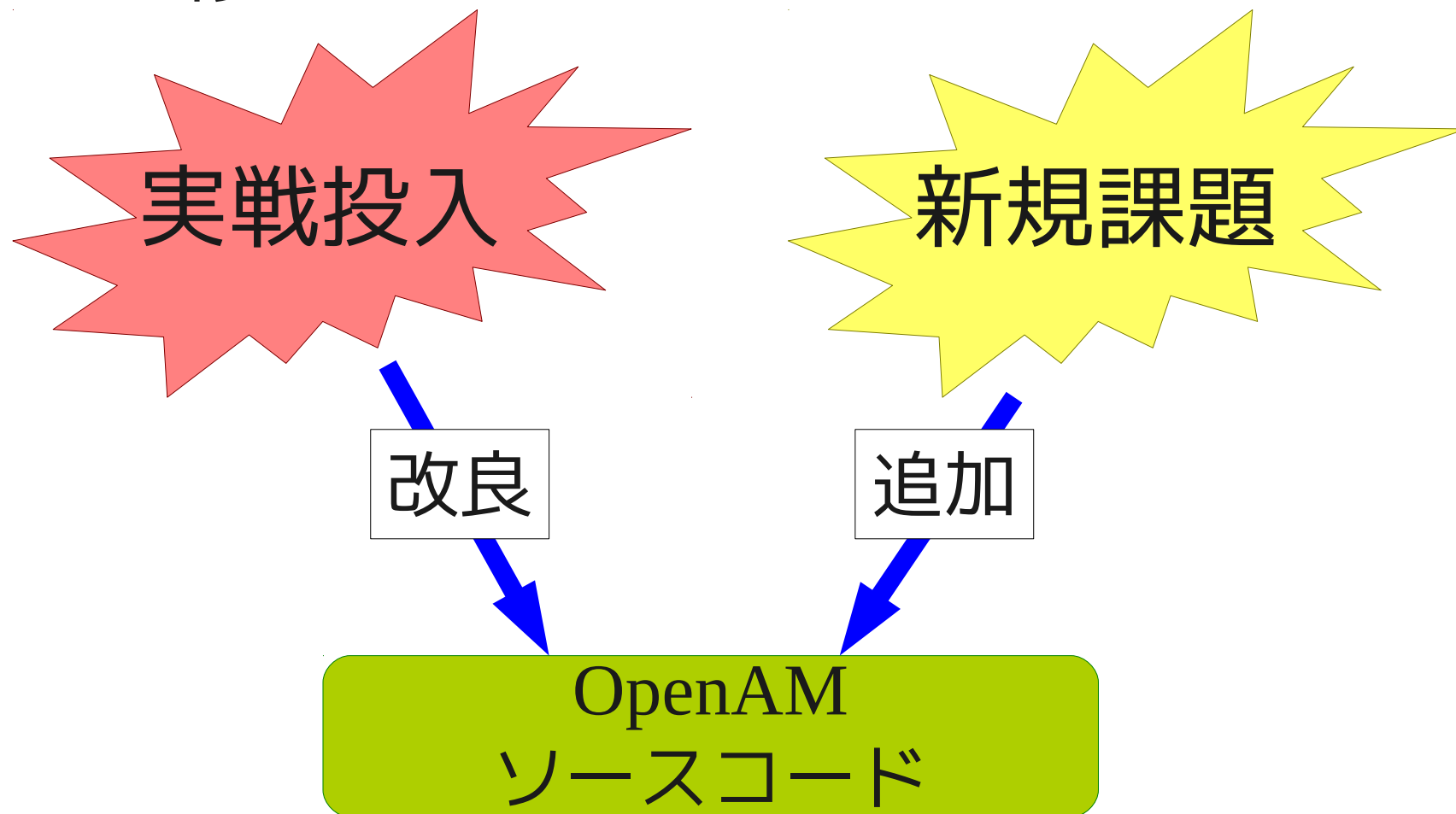
お問い合わせ info@osstech.co.jp

アジェンダ

- OpenSourceであること
- ForgeRockソースツリーへ
- OSSTech版カスタマイズ
- 案件個別カスタマイズ
- 導入事例

OpenSourceであること

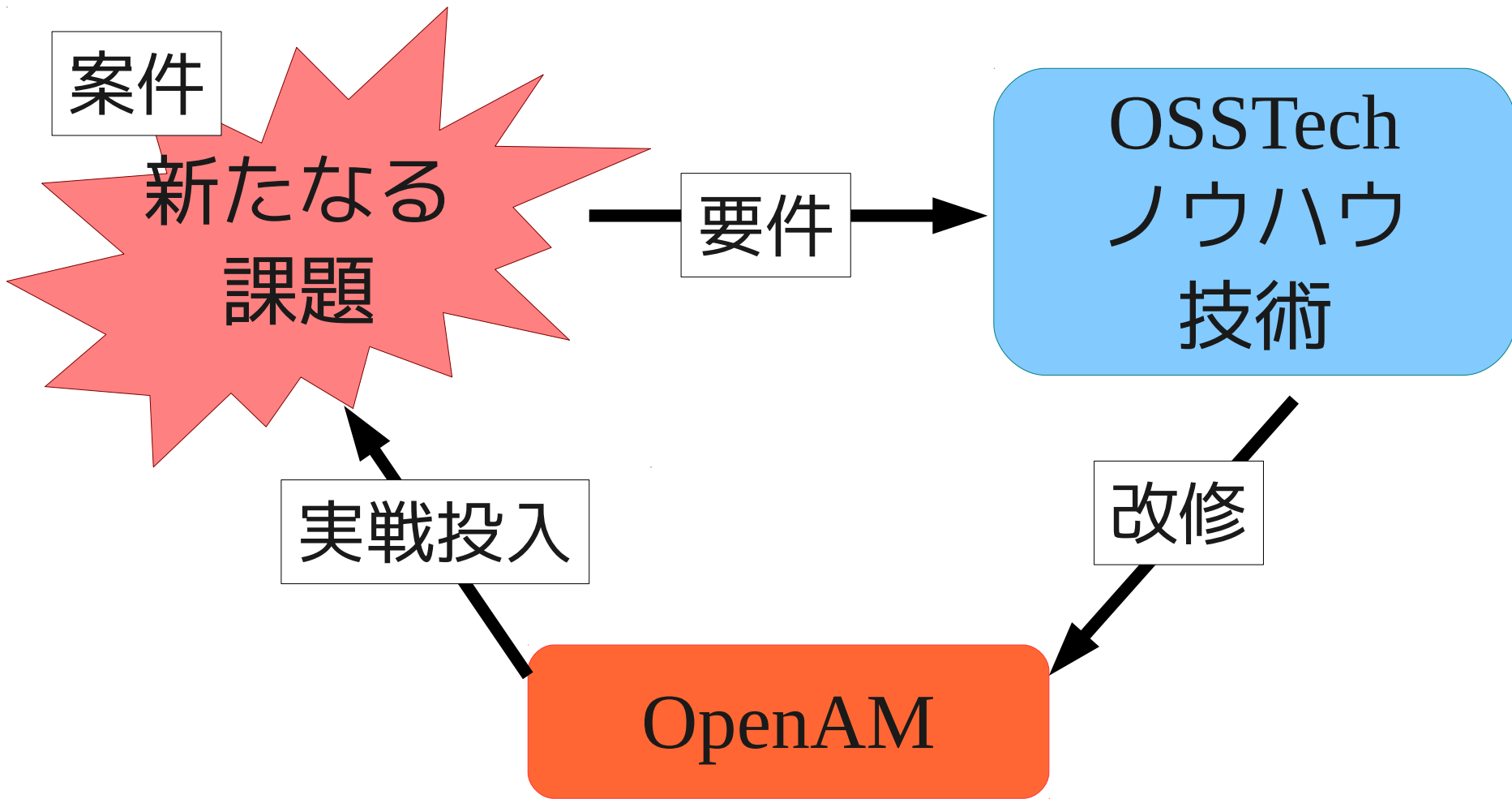
- ソース修正はオープンソースだからこそ



問題点の改良、要件に合わせた機能追加

OpenSourceであること

- ソース改修力は課題解決力

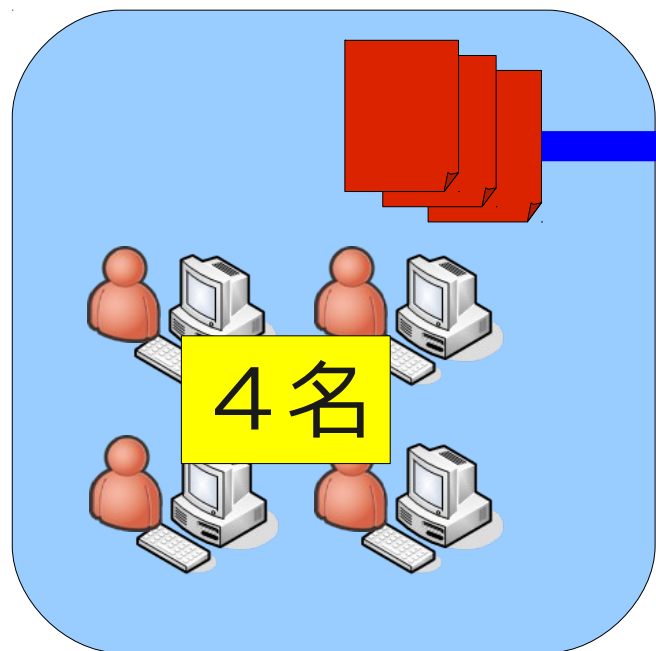


全てのサイクルをサポートできる

ForgeRock ソースコード への貢献

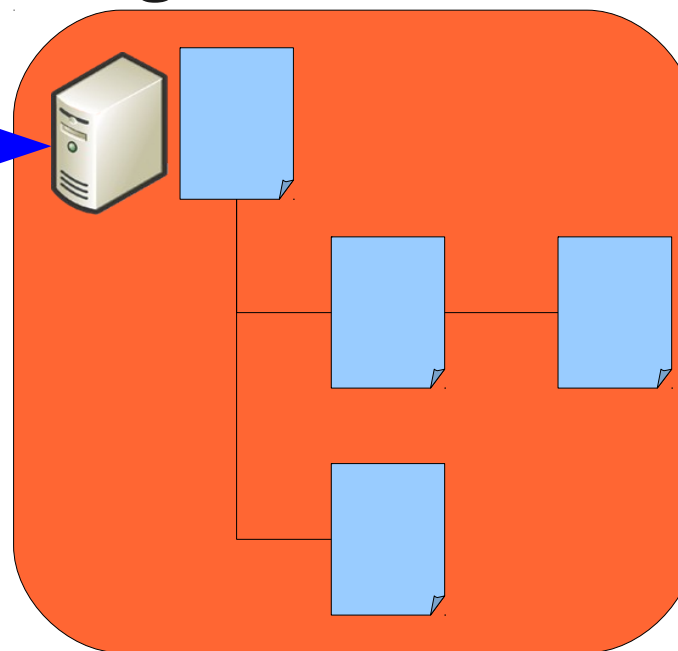
- 社内開発者6名
- コミット権限のある社内開発者4名
- OpenAM コミッター総数37名

OSSTech社

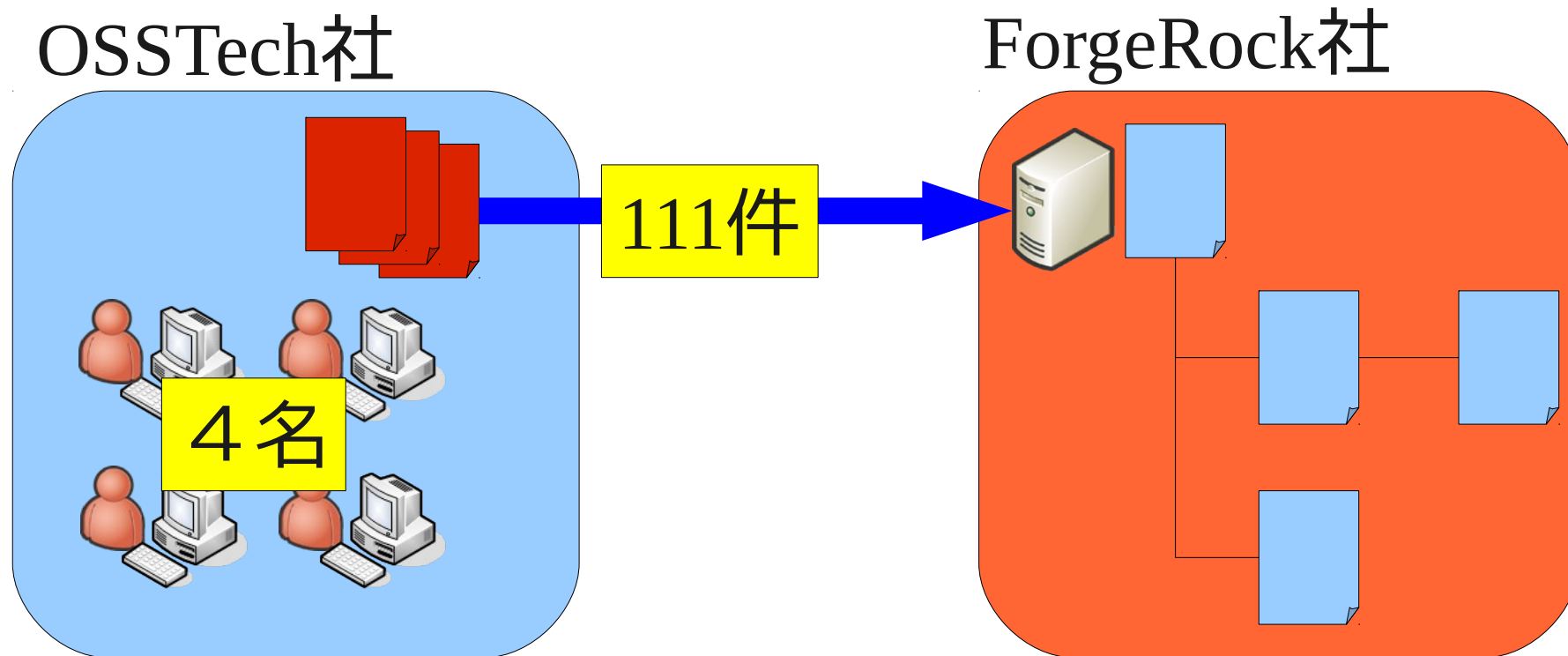


commit

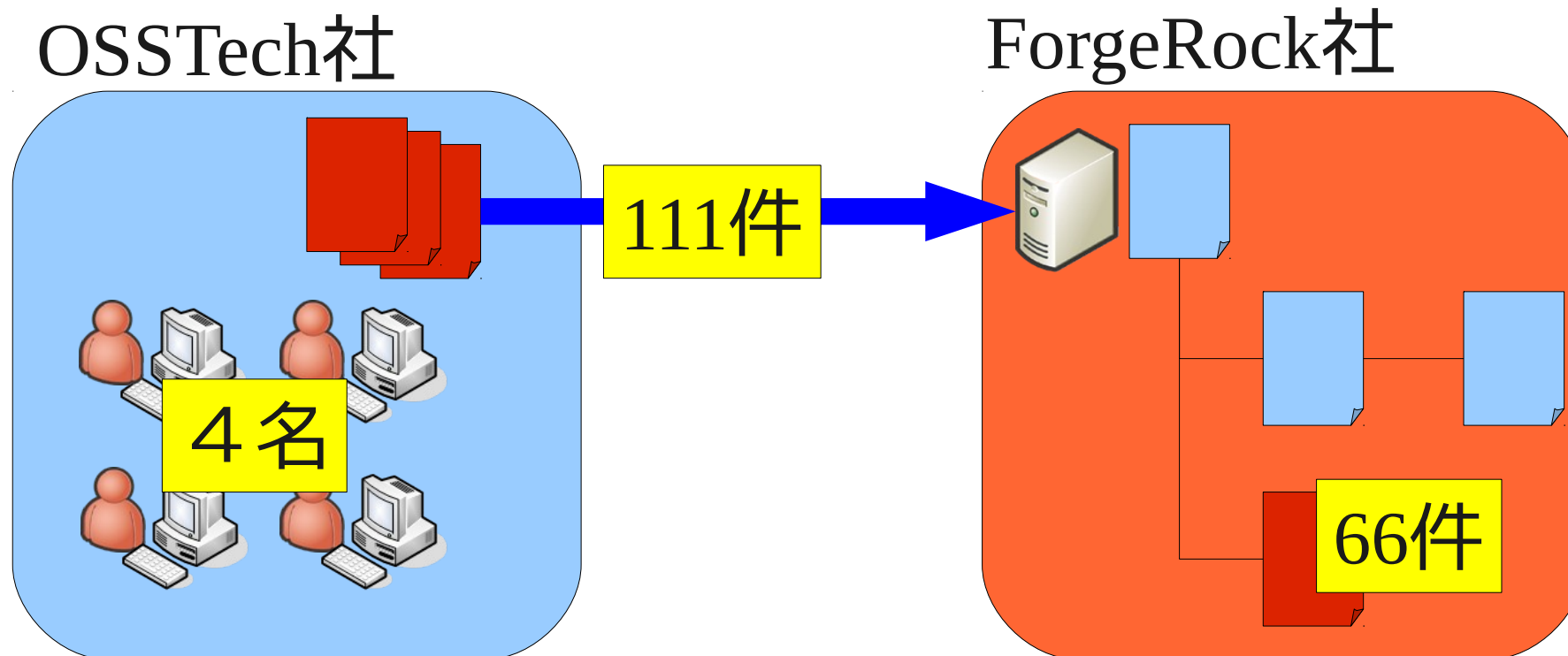
ForgeRock社



- 社内コミッターによるコミット件数111件
- ForgeRockツリーのコミット総数は3346件



- 社内コミッターによる修正件数66件
- 現在のチケット数1739(重複等含む)



- nginxエージェント開発
- ユーザーデータストアの修正
 - ▶ JDBCの設定が共有されてしまう問題
 - ▶ ログ出力の改善
- コマンドツール(ssoadm など)の修正
 - ▶ エージェントの設定に不正な値が登録される問題
 - ▶ Windows 用ツールが動作しない問題
- ファイルアップロードの修正
 - ▶ Safari・Chromeでファイルアップロードが動作しない問題

コミット例

- メモリリーク関連の修正
 - ▶ エージェントのメモリリーク
 - ▶ HTTPコネクションのリーク
 - ▶ DBコネクションのリーク
- マルチバイト文字
 - ▶ マルチバイト文字の表示の問題
- 日本語化
 - ▶ 日本語表示の追加
 - ▶ 誤訳の修正

問題の確認

修正

レビュー

適用

ステータス変更

ForgeRockのプロジェクト管理ツール(JIRA)でOpenAMの問題を確認する

- ・ 報告されていない問題
→ 登録
- ・ 報告されている問題
→ 解決していない問題は修正する
→ 解決している問題は修正を適用する

T	Key	Summary	Assignee	Reporter	P	Status	Resolution
	OPENAM-1310	Customised login page doesnt work for a new realm	Unassigned	phadke4u	High	Open	Unresolved
	OPENAM-1280	Persistent cookies only works when debug is at Message Level	Unassigned	alissongarcia	High	Open	Unresolved
	OPENAM-1696	Data code for AD_ACCOUNT_DISABLED is wrong	Unassigned	cheechong	High	Open	Unresolved
	OPENAM-1093	Authentication fails if session-service attributes are not stored in user entry in Active Directory	Unassigned	Bernhard Thalmayr	High	Open	Unresolved

図：プロジェクト管理ツール(JIRA)

問題の確認

バージョン管理システム (Subversion) からソースコードを取得して問題を修正する

修正

修正したコードにOSSTechのコピーライトを追加する

レビュー

現在、150以上のファイルにOSSTechのコピーライトあり

適用

```
/*
```

```
* Portions Copyrighted 2012 ForgeRock Inc
```

```
* Portions Copyrighted 2012 Open Source Solution  
Technology Corporation
```

```
*/
```

図：コピーライトの例

ステータス変更

問題の確認

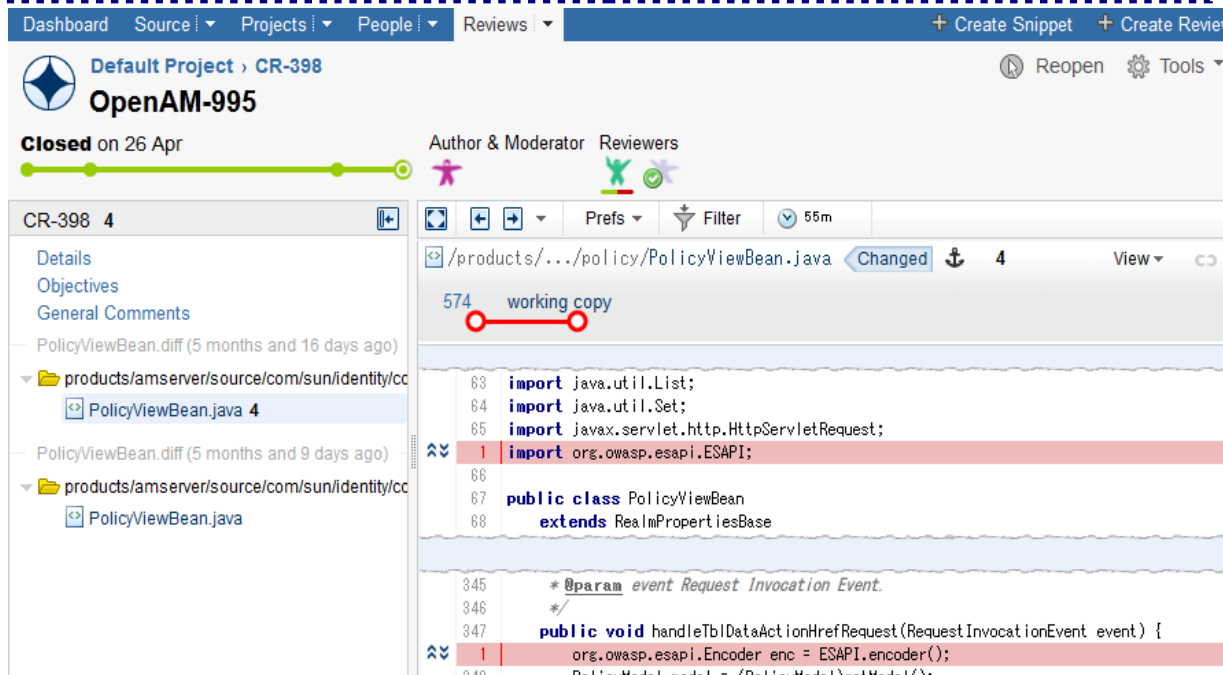
修正

レビュー

適用

ステータス変更

コードレビューツール(crucible)で ForgeRockの開発者を交えてレビューを行う



☒ : コードレビュー(crucible)



問題の確認

修正

レビュー

適用

ステータス変更

レビューの完了したソースコードファイルをバージョン管理システム (Subversion) に適用する(コミット)

```
svn commit -m "OPENAM-985:: LDAPv3Repo and associated classes can cause leak in the shutdown manager due to LDAP exceptions"
```

☒ : コミット コマンド例

問題の確認

プロジェクト管理ツール(JIRA)でOpenAMの問題のステータスを変更する

修正

修正した問題の一部はリリースノートに記載される

レビュー

Kohei Tamura made changes - 09/Jul/12 12:44 AM

Status Open [1] Resolved [5]

Resolution Fixed [1]

☒ : ステータス変更例(JIRA)

適用

4.1. Fixes

The following issues were fixed in release 10.1.0.

- ☛ OPENAM-1246: More than 5 referral policies under a realm would hang PrivilegeEvaluator
- ☛ OPENAM-1221: WSSAgent can not sign request if security mechanism 'X509Token' and Signing Reference Type 'KeyIdentifier Reference' is configured in Web Service Client profile
- ☛ OPENAM-1205: Missing SAML2Exception handler in spAssertionConsumer.jsp means a 500 error page is shown rather than the configured OpenAM SAML error page
- ☛ OPENAM-1204: Creation of xamcl policy (entitlement) with cli ssoadm tool fails when using Secure Logging
- ☛ OPENAM-1054: MySQL (JDBC) IdRepo shares configurations in all realms in the wrong
- ☛ OPENAM-1047: isSessionQuotaReached does not work correctly if users session quota > 1

☒ : 10.1.0 リリースノート(ドラフト版)抜粋

ステータス変更

OSSTech版カスタマイズ

- OpenLDAPと親和性向上 > 自社ソリューション
 - OpenAMにOpenLDAP専用の設定を追加
 - OSSTech社製OpenLDAP向け拡張スキーマを用意



OpenAM

ステップ 1/2: データストアのタイプを選択

戻る 次へ 取消し

* 必須入力フィールド

* 名前:

* タイプ:

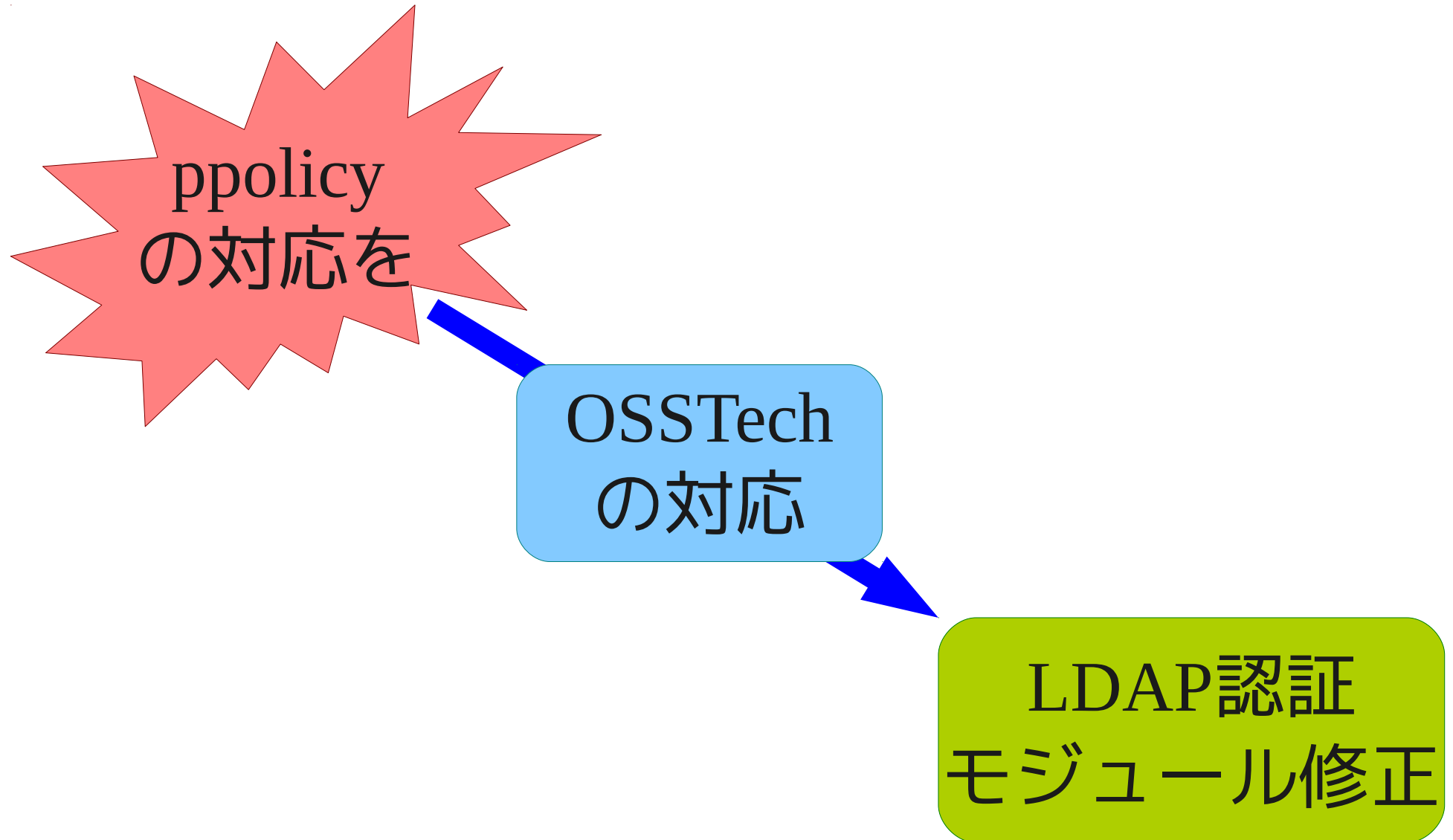
- Active Directory
- Active Directory アプリケーションモード (ADAM)
- OpenAM スキーマを含んだ Sun Directory Server
- OpenDS
- OpenLDAP
- Tivoli Directory Server
- データベースリポジトリ (アーリーアクセス)

- Tomcatとの親和性向上 > 環境の統一化
 - ▶ OpenAM向けにパラメータを調整したTomcatをOpenAMとセットで提供
- パッケージング > セットアップ容易化
 - ▶ RPMパッケージとして提供
 - ▶ Windowsインストーラー提供

- OpenAM10からのバックポート
 - ▶ 重要な修正、必要な機能をバックポート
 - ▶ 多重構成でのセッション数の共有
 - ▶ ポリシーの設定方法の改善
 - ▶ メモリリークの修正
- プラットフォーム毎にエージェントを提供
 - ▶ RHEL5でも動作可能なApache2.2エージェントの提供
- 日本語化
 - ▶ 画面の文字化け対策

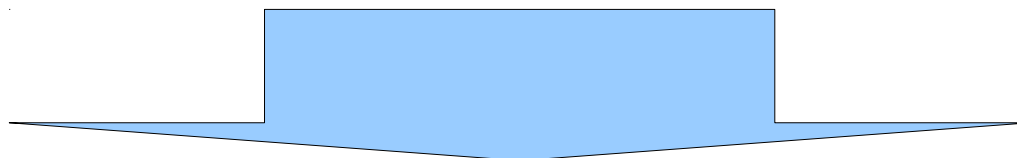
案件個別カスタマイズ

- OpenLDAP パスワードポリシー対応



• OpenLDAP パスワードポリシー対応

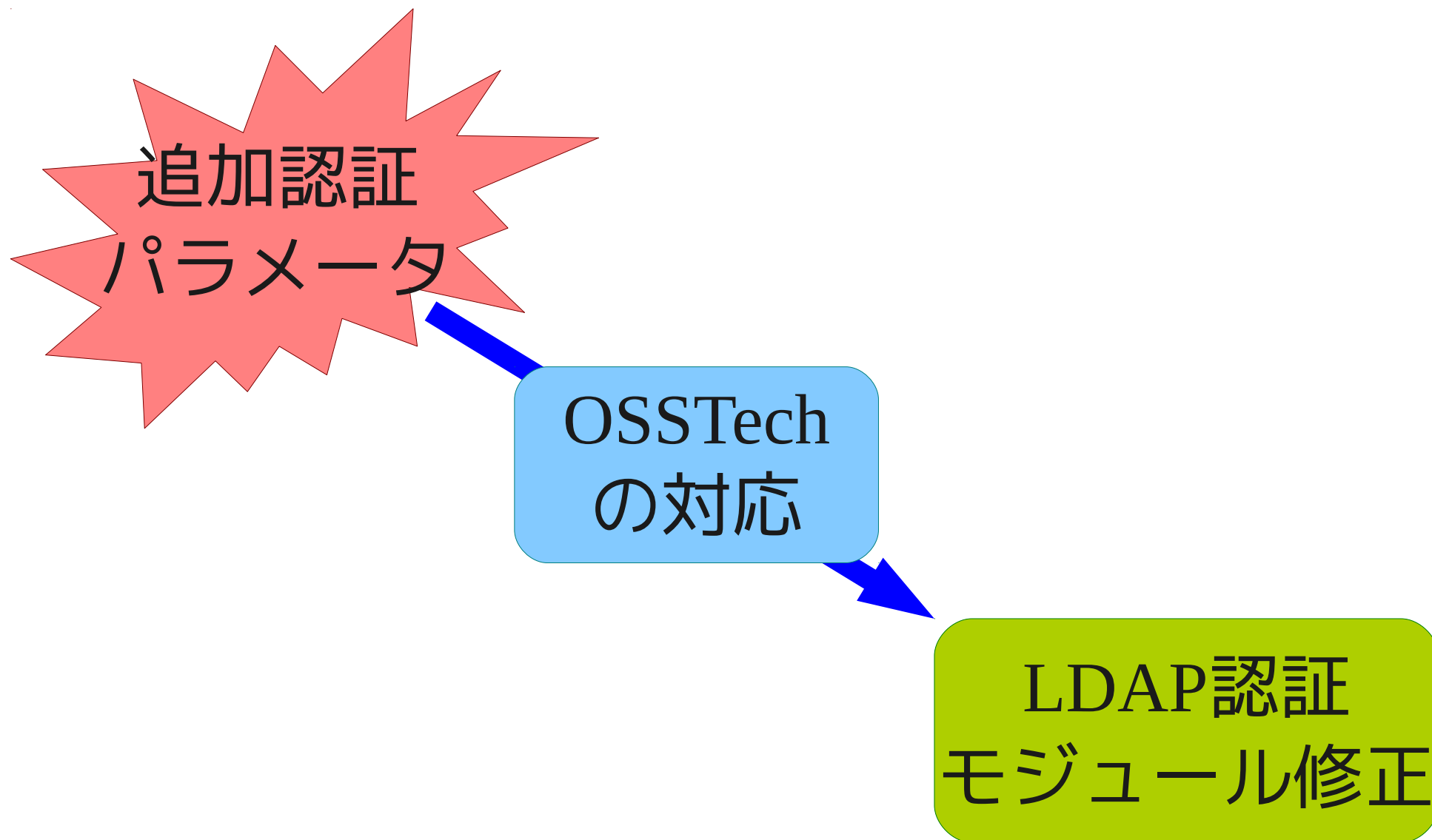
- OpenAM-9.5系ではLDAP標準のアカウントポリシー※に未対応
- 全て同一の認証エラーとなるという課題



- LDAP認証モジュールにLDAPのアカウントポリシー(パスワード有効期限、ロック等)エラーをハンドリングし、個別のエラー遷移するように改修

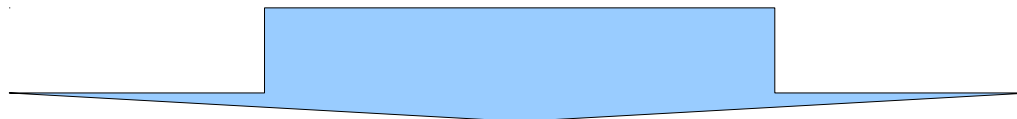
※アカウントポリシーとはパスワード有効期限、アカウントロックアウト等
SunJavaDSやOpenDSを利用する場合は独自実装で対応されていた。
OpenAM-10から対応開始

- 認証パラメータの追加



- 認証パラメータの追加

- LDAP認証時に入力するユーザー名、パスワード以外に別パラメーターをドロップダウンリストとして表示し入力したい



- LDAP認証モジュールを別パラメーター取得、表示可能なよう改修した

OpenAM

OpenAM へのサインイン

ユーザー名:

パスワード:



OpenAM

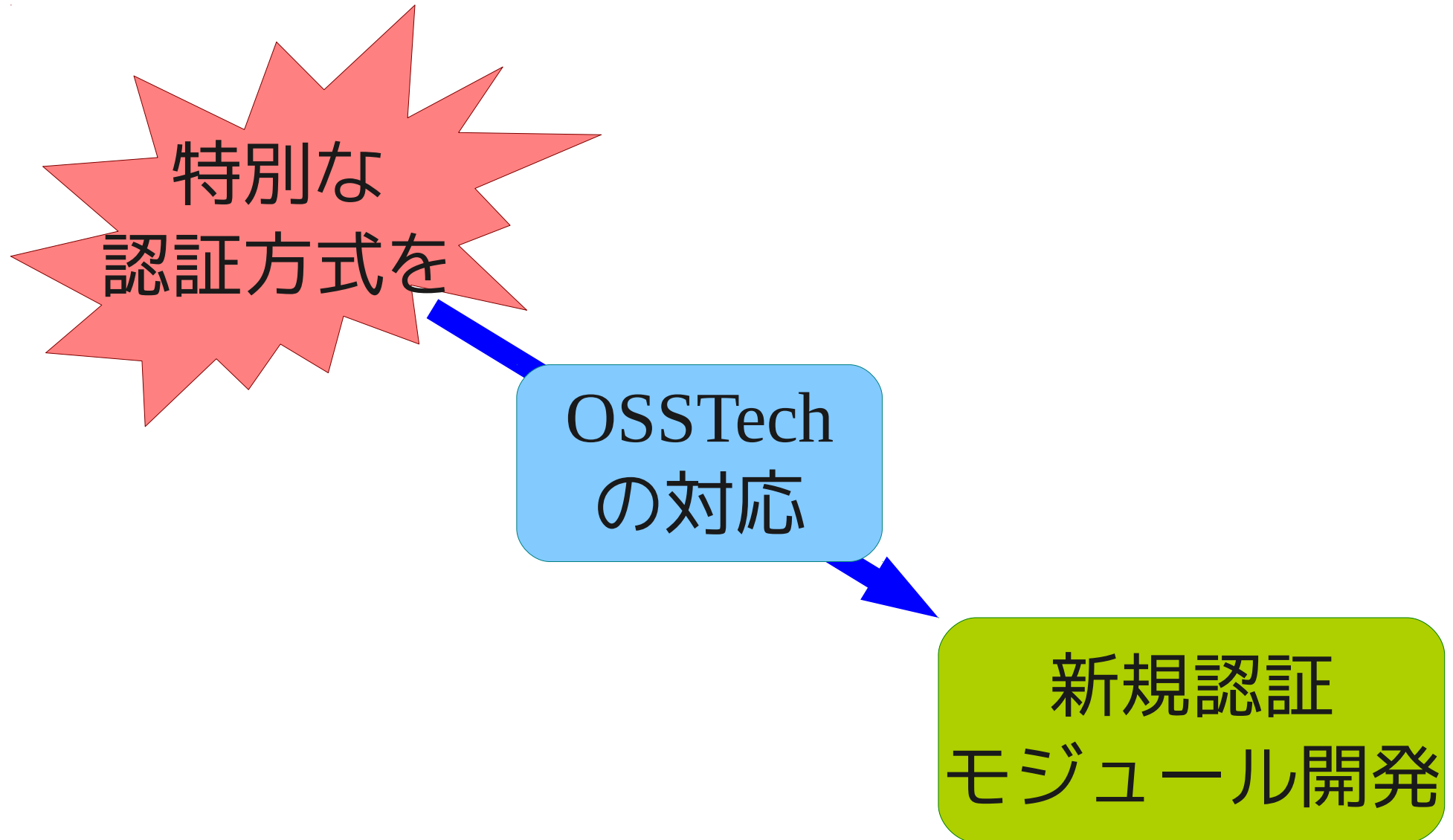
OpenAM へのサインイン

ユーザー名:

パスワード:

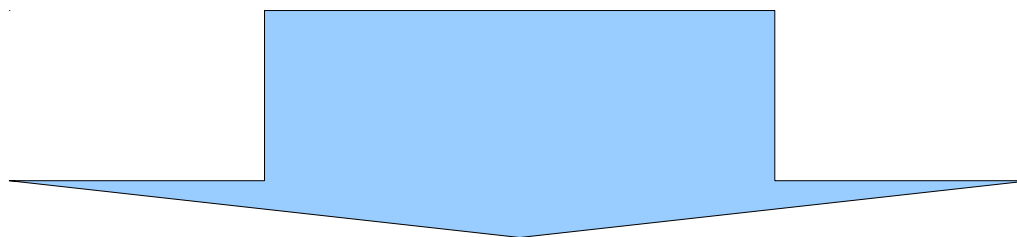
グループ:

- 認証モジュールの開発



• 認証モジュールの開発

- 既存認証モジュールでは対応できない認証方式(リクエストヘッダ)で認証したい



- 要件に合った認証モジュールを開発し、既存モジュールとの認証連鎖とした。

- Apacheより早いリバースプロキシを構築したい

リバース
プロキシに
パフォーマンスを！

OSSTech
の対応

nginx用
PolicyAgent開発

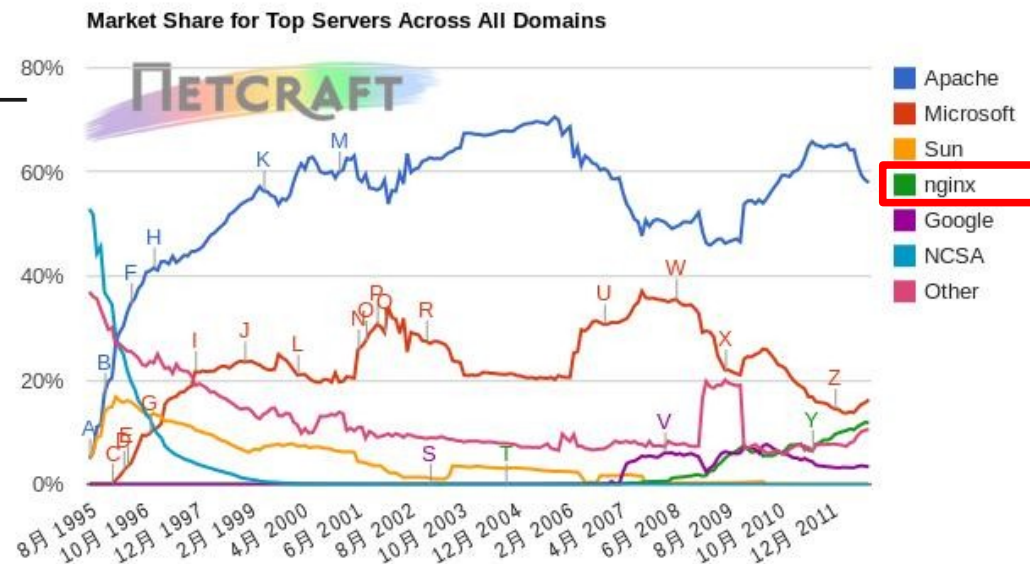
- Apacheより早いリバースプロキシを構築したい

- Apacheによるリバースプロキシよりスケラビリティが欲しい

- nginx※用 Policy Agentの開発

※nginxとはスケラビリティ、パフォーマンスに優れる第三のhttpサーバー

netcraftの2011年資料
第3位にnginxが伸びてきている
apacheほど多機能ではないが、
リバースプロキシ利用では
十分な機能を持たせられる



導入事例

国立大学法人 北見工業大学 様

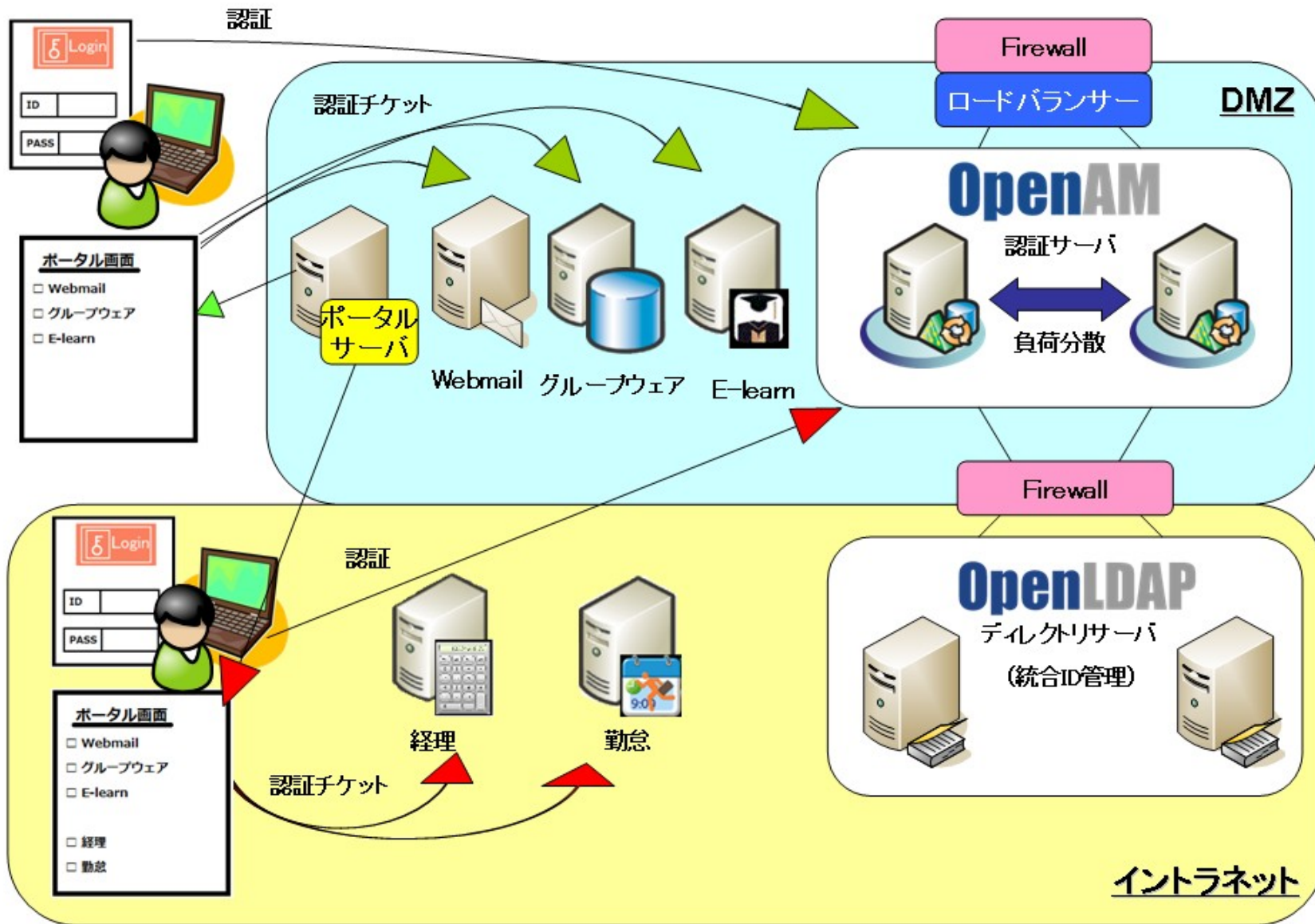
北見工業大学様 システムの特徴

- 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

北見工業大学様



学校法人 福岡大学 様

福岡大学様 システムの特徴

規模

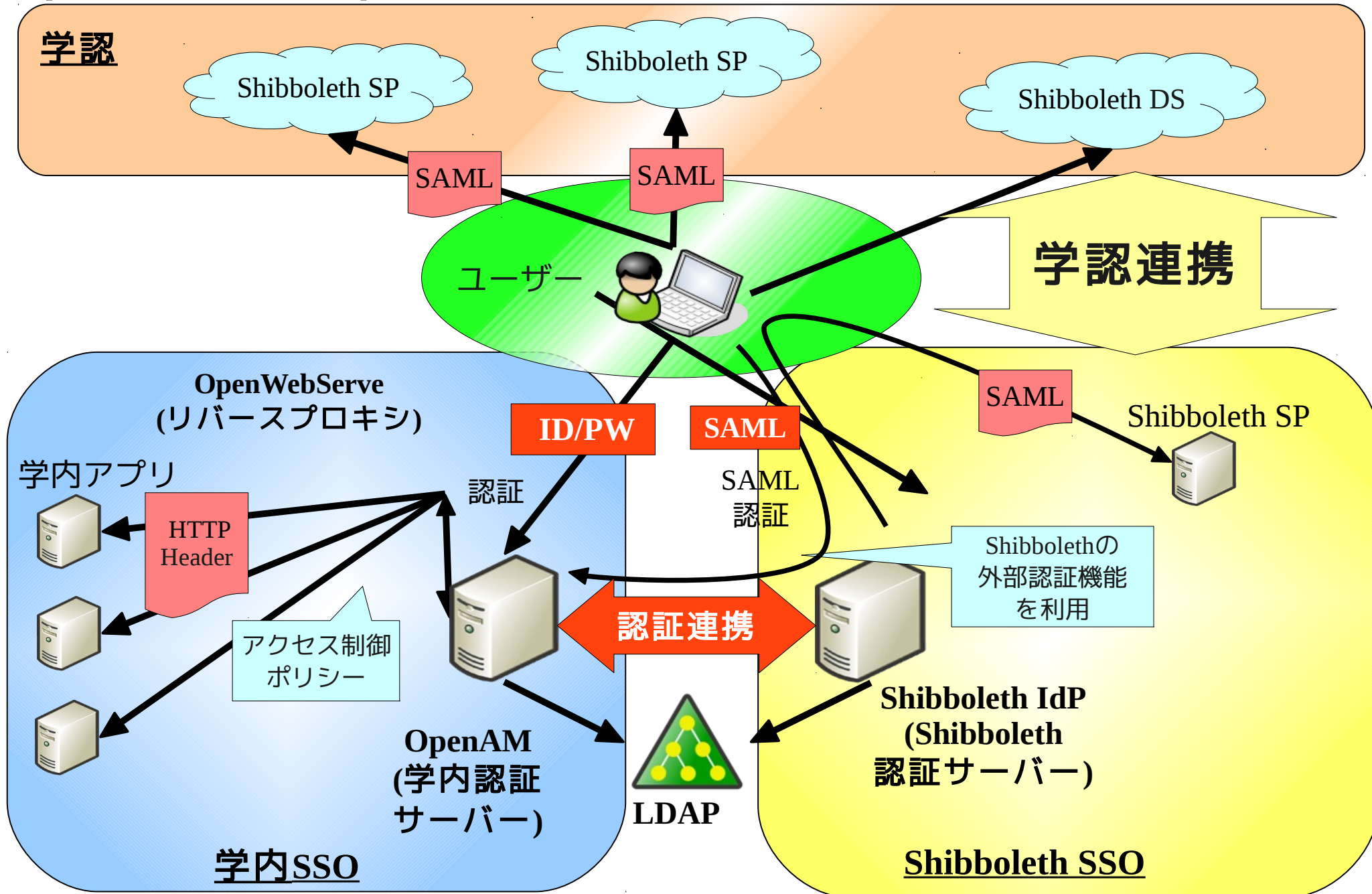
9つの学部、2つの病院、22の付置施設で構成される総合大学
学生数 約21,000人
教職員数 約3,000人

ミッション

高い拡張性と柔軟性を持つ先進的SSO基盤の構築

日立製作所とオープンソース・ソリューション・テクノロジーで実現

- ▶ OpenAMとShibbolethによるハイブリッド型SSO基盤
 - システムのシングルサインオンを実現する認証基盤をOpenAMとShibbolethを使って実現
 - 様々なアプリケーションとのシングルサインオンを実現する基盤
 - ユーザーは1度の認証で学認と学内のアプリケーションを利用可能





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

<http://www.osstech.co.jp/>

お問い合わせ info@osstech.co.jp