OSSTechのOpenAMへの取り組み

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・テクノロジ株式会社

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

お問い合わせ info@osstech.co.jp

Copyright © 2012 Open Source Solution Technology, Corp.

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

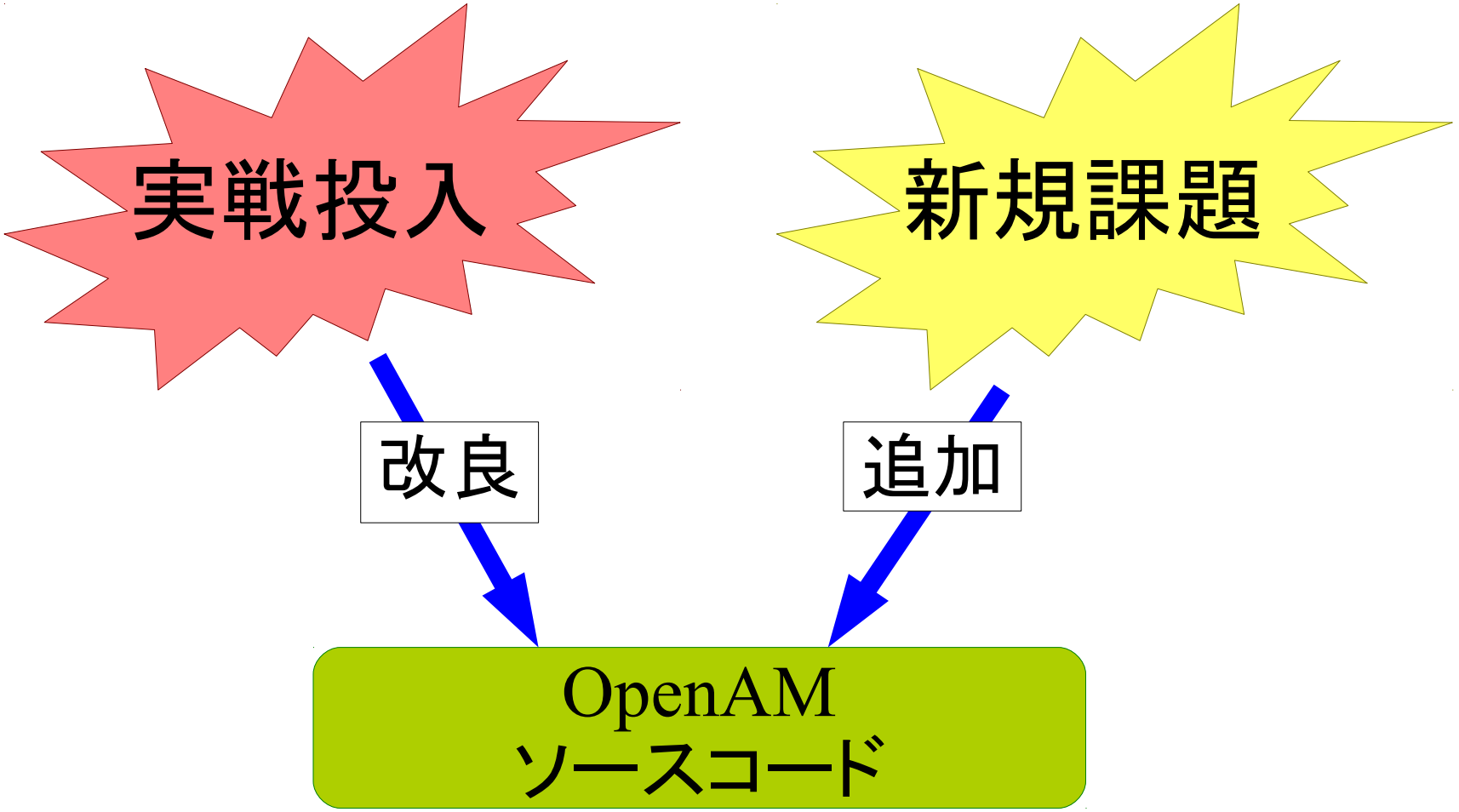
Copyright © 2012 Open Source Solution Technology, Corp.

OpenSourceであること

Copyright © 2012 Open Source Solution Technology, Corp.

OpenSourceであること

- **ソース修正はオープンソースだからこそ**

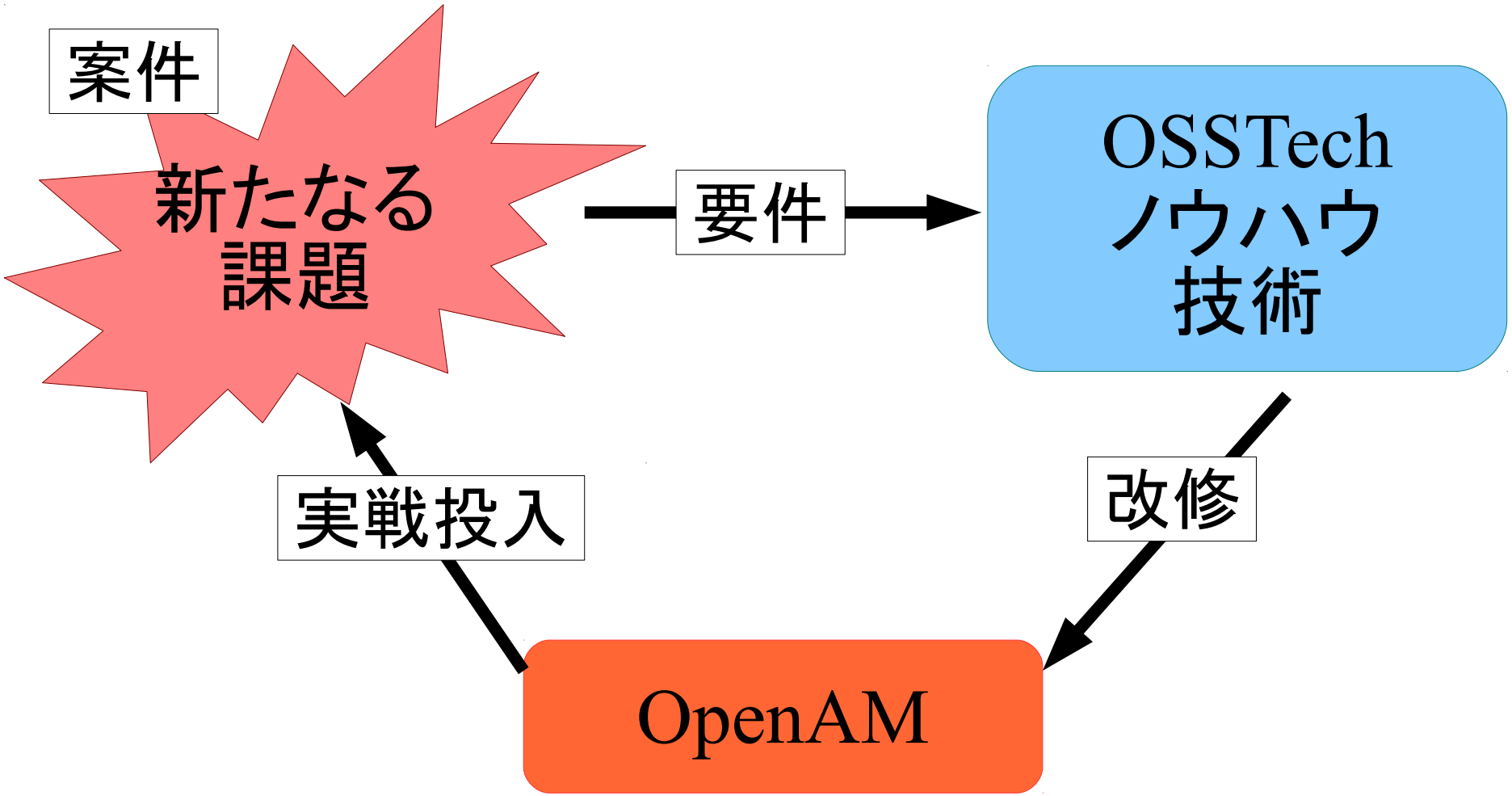


問題点の改良、要件に合わせた機能追加

Copyright © 2012 Open Source Solution Technology, Corp.

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

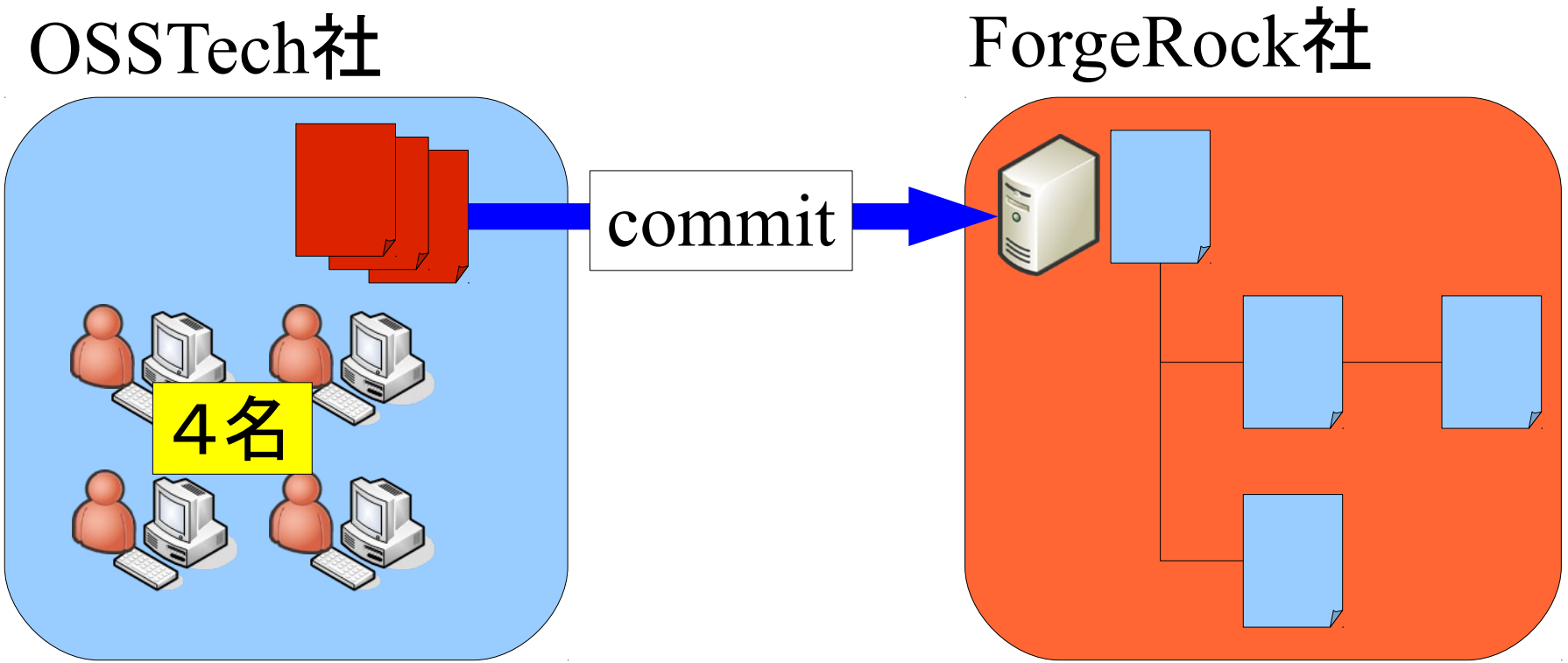
Copyright © 2012 Open Source Solution Technology, Corp.

ForgeRock ソースコードへの貢献

Copyright © 2012 Open Source Solution Technology, Corp.

コミッター数

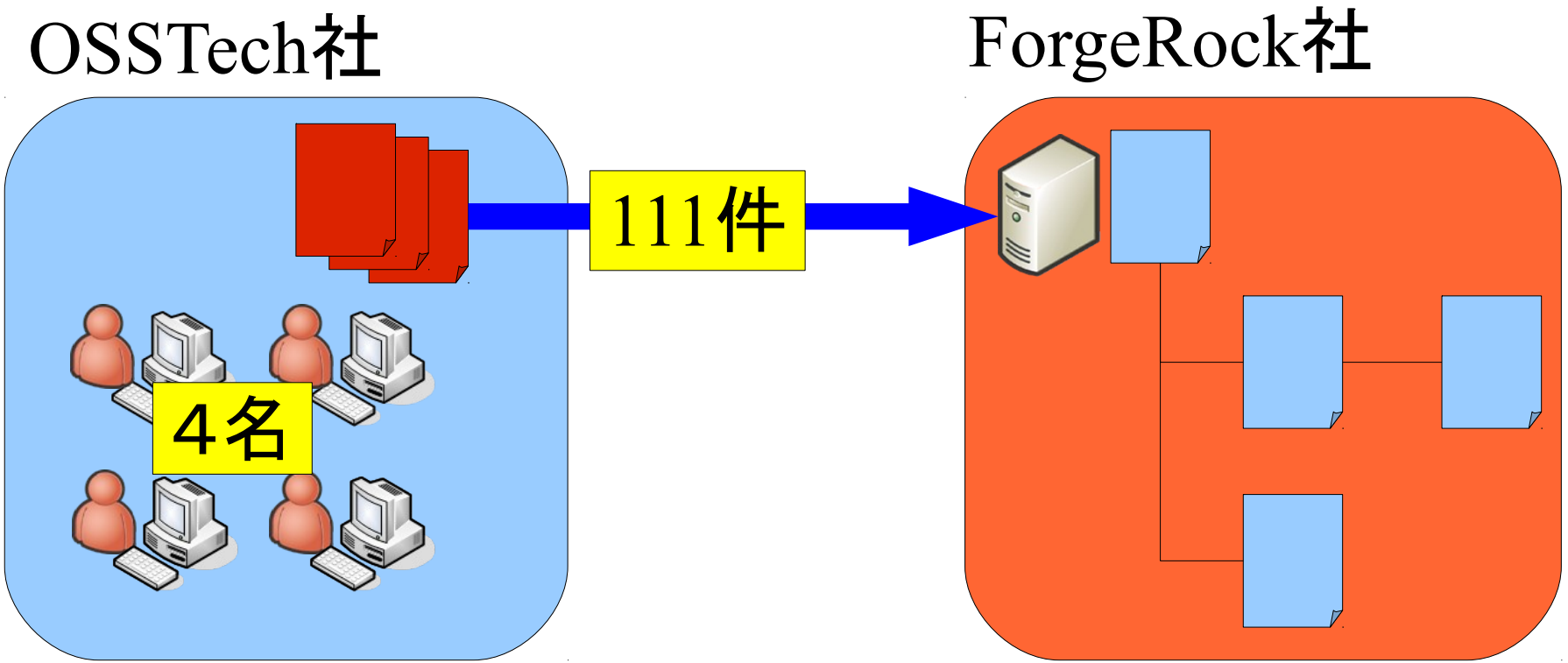
- 社内開発者6名
- コミット権限のある社内開発者4名
- OpenAM コミッター総数37名



Copyright © 2012 Open Source Solution Technology, Corp.

コミット件数

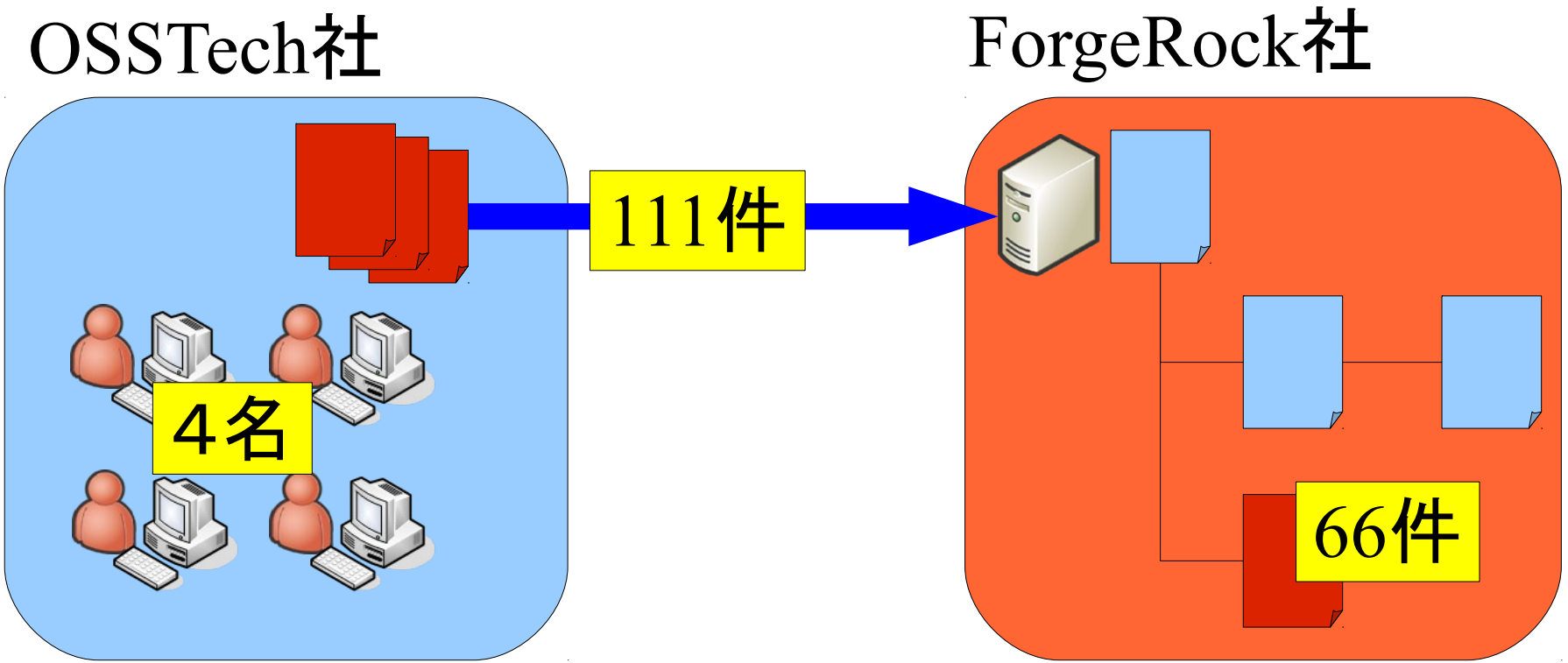
- 社内コミッターによるコミット件数111件
- ForgeRockツリーのコミット総数は3346件



Copyright © 2012 Open Source Solution Technology, Corp.

問題修正件数

- 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)



Copyright © 2012 Open Source Solution Technology, Corp.

コミット例

- nginex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

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

修正フロー

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
　→解決していな問題は修正する
　→解決している問題は修正を適用する

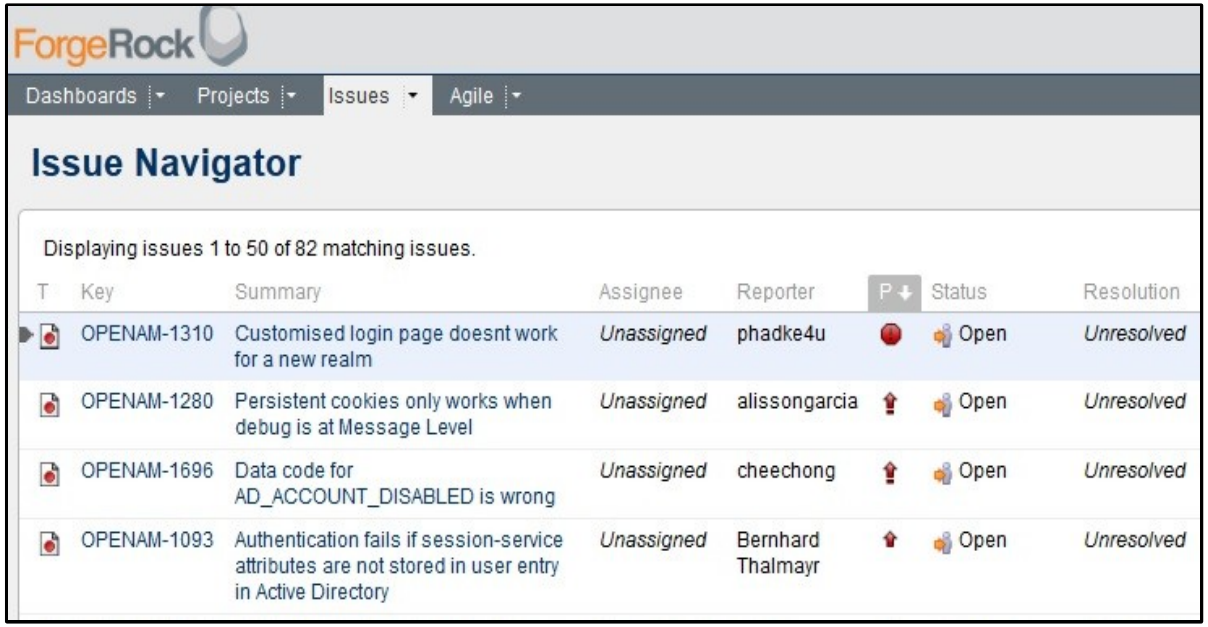


図:プロジェクト管理ツール(JIRA)

Copyright © 2012 Open Source Solution Technology, Corp.

修正フロー

問題の確認

修正

レビュー

適用

ステータス変更

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

修正したコードにOSSTechのコピーライトを
追加する
現在、150以上のファイルにOSSTechのコ
ピーライトあり

```
/*
* Portions Copyrighted 2012 ForgeRock Inc
* Portions Copyrighted 2012 Open Source Solution
Technology Corporation
*/
```

図：コピーライトの例

Copyright © 2012 Open Source Solution Technology, Corp.

修正フロー

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

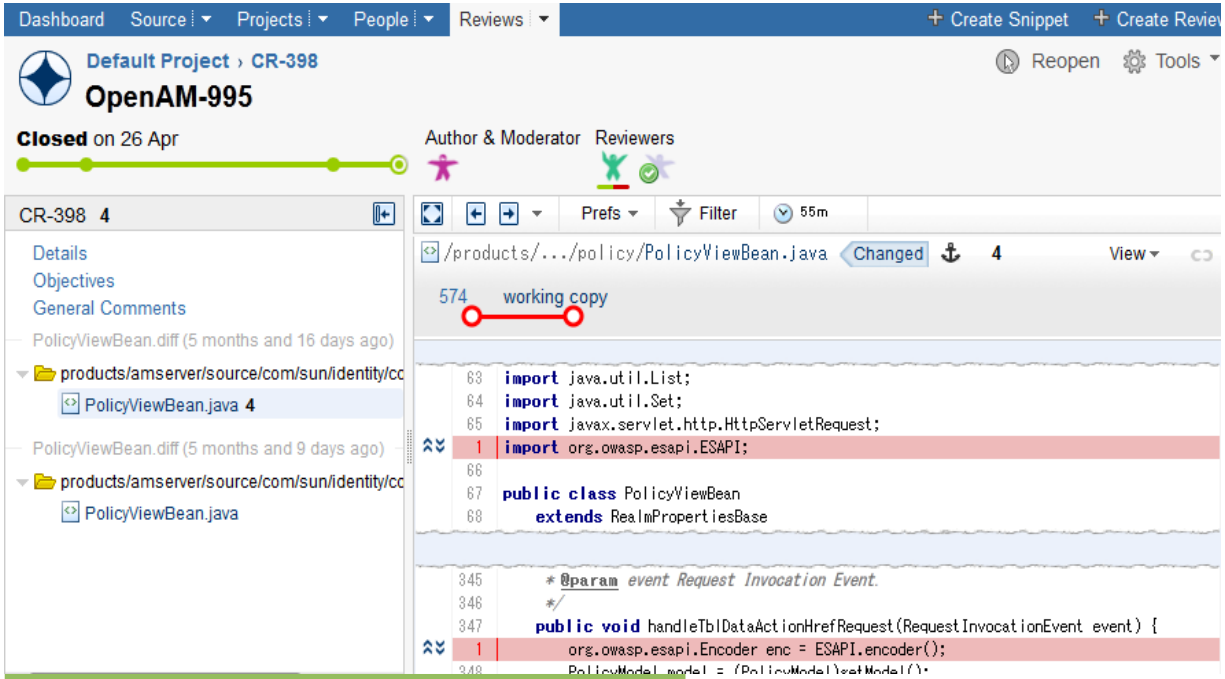


図:コードレビュー(crucible)

Copyright © 2012 Open Source Solution Technology, Corp.

修正フロー

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"
```

図:コミット コマンド例

Copyright © 2012 Open Source Solution Technology, Corp.

修正フロー

問題の確認

修正

レビュー

適用

ステータス変更

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

修正した問題の一部はリリースノートに記載される

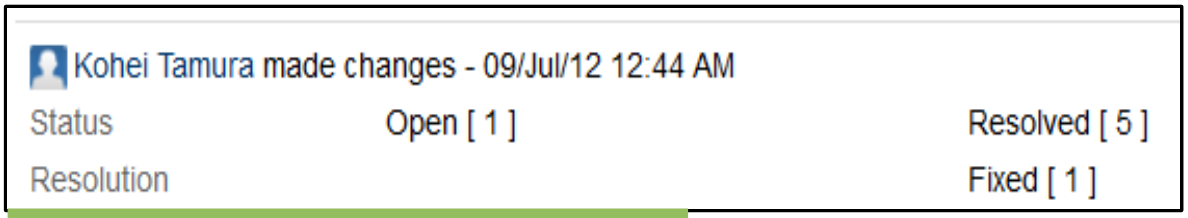


図:ステータス変更例(JIRA)

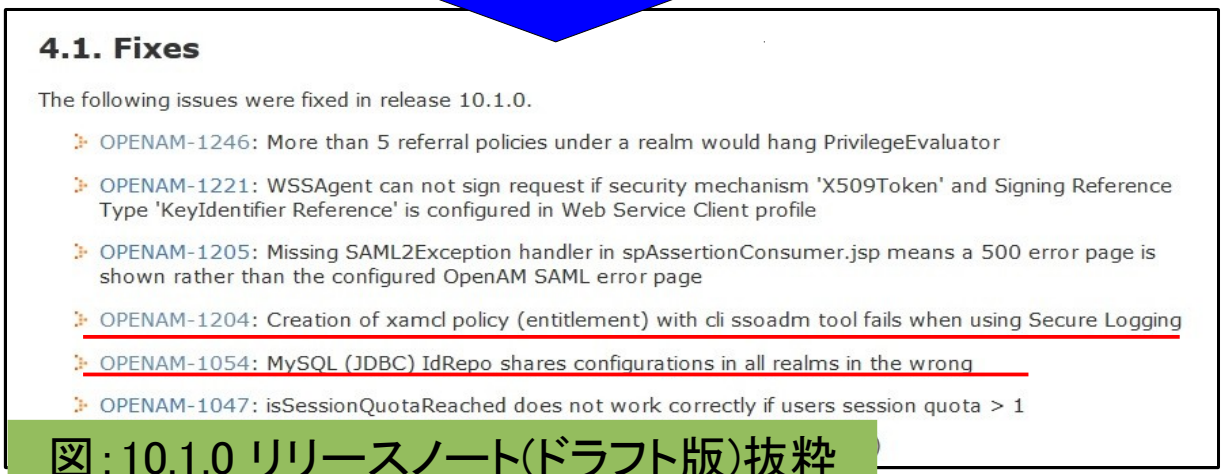


図:10.1.0 リリースノート(ドラフト版)抜粋

Copyright © 2012 Open Source Solution Technology, Corp.

OSSTech版カスタマイズ

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

OSSTech版カスタマイズ

- 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

Copyright © 2012 Open Source Solution Technology, Corp.

OSSTech版カスタマイズ

- 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

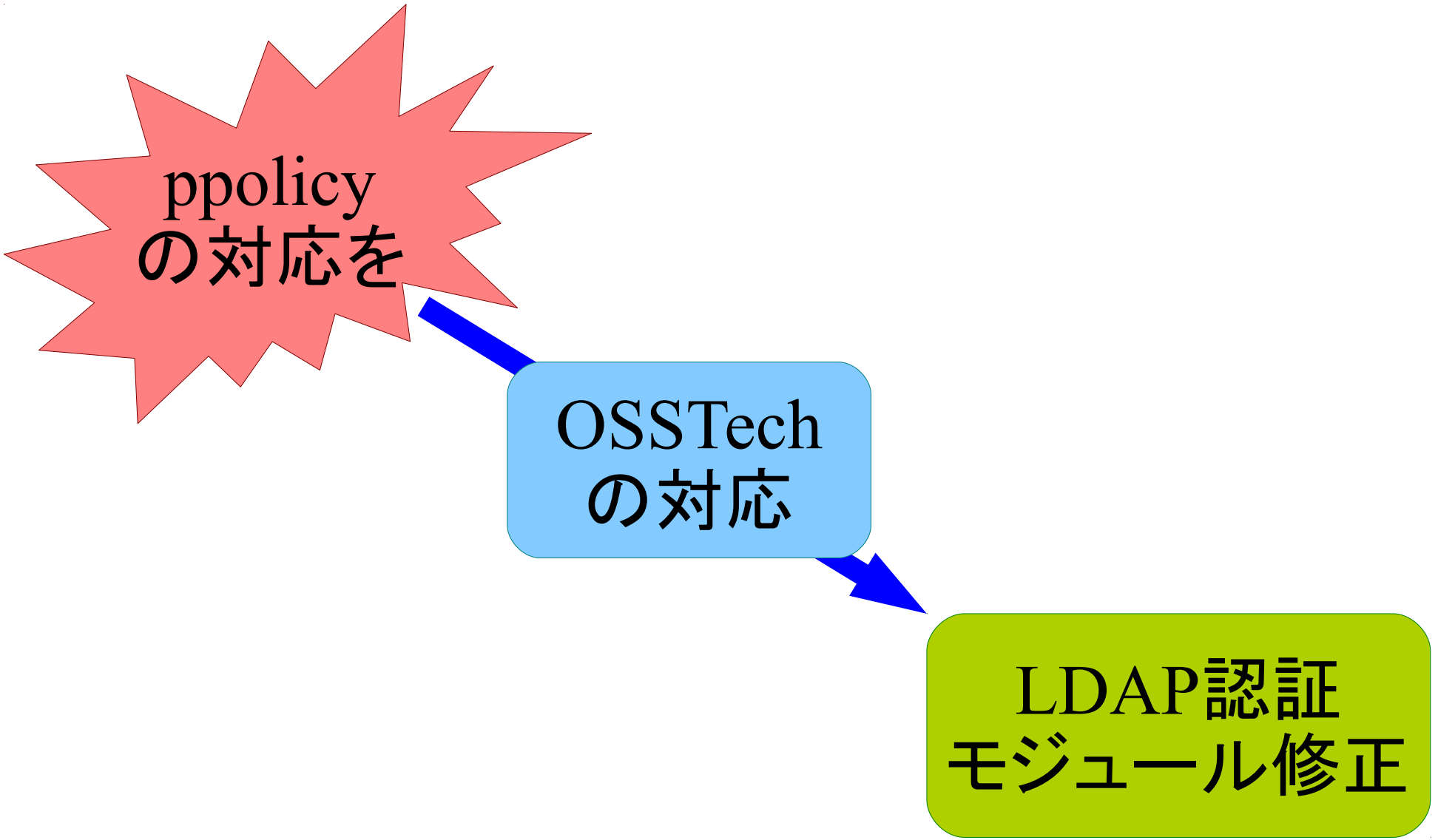
Copyright © 2012 Open Source Solution Technology, Corp.

案件個別カスタマイズ

Copyright © 2012 Open Source Solution Technology, Corp.

カスタマイズ事例

- OpenLDAP パスワードポリシー対応

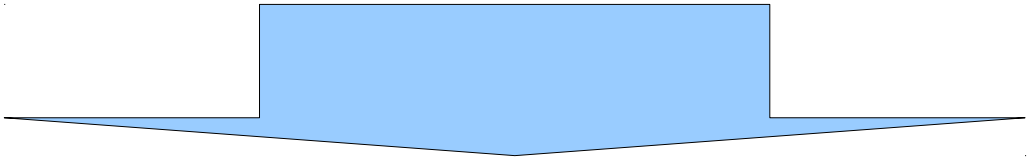


Copyright © 2012 Open Source Solution Technology, Corp.

カスタマイズ事例

- 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



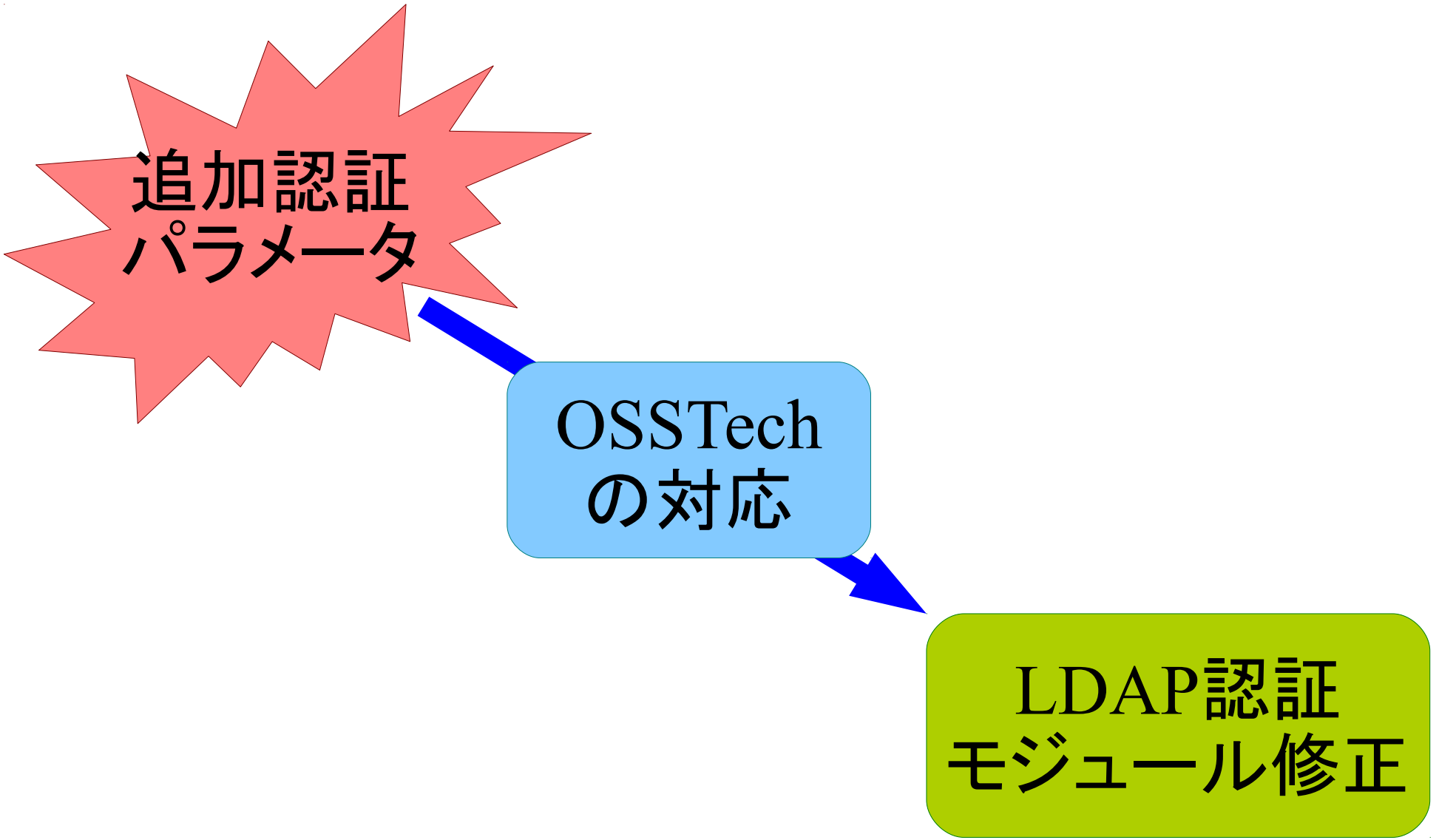
- LDAP認証モジュールにLDAPのアカウントポリシー(パスワード有効期限、ロック等)エラーをハンドリングし、個別のエラー遷移するよう改修

※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

Copyright © 2012 Open Source Solution Technology, Corp.

カスタマイズ事例

- 認証パラメータの追加



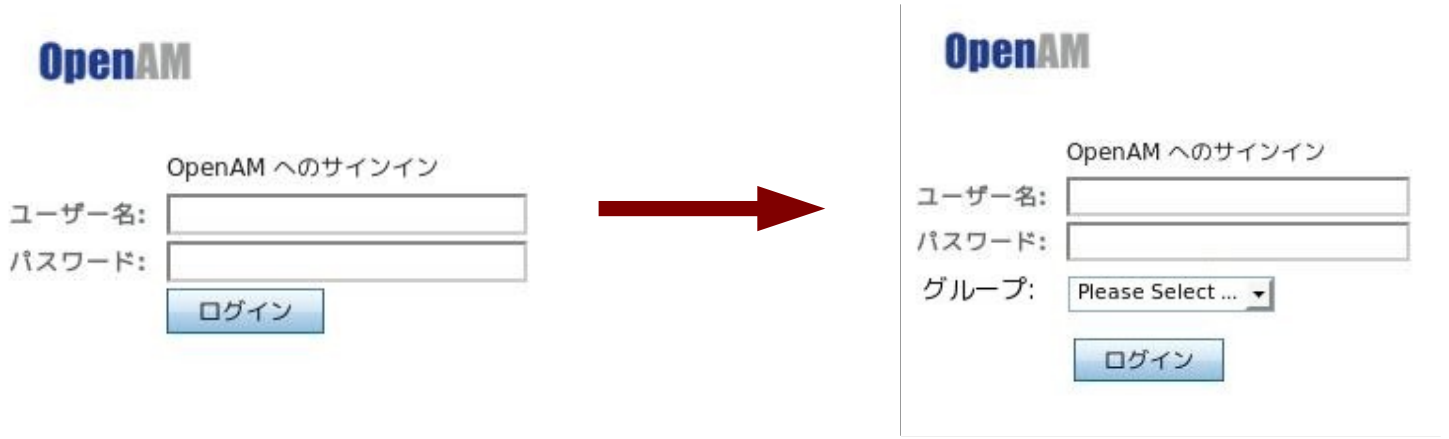
Copyright © 2012 Open Source Solution Technology, Corp.

カスタマイズ事例

- 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

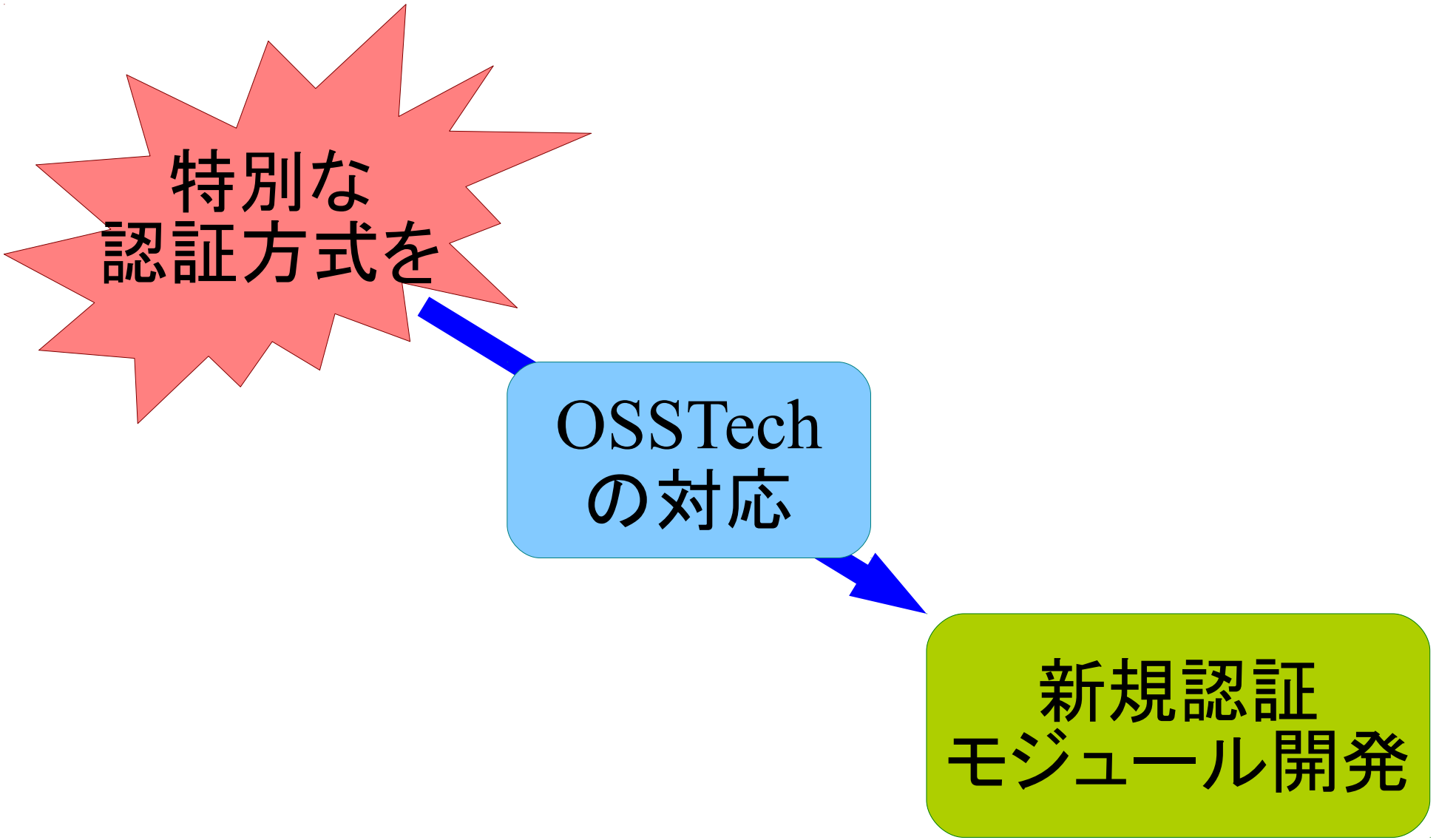
- LDAP認証モジュールを別パラメーター取得、表示可能なよう改修した



Copyright © 2012 Open Source Solution Technology, Corp.

カスタマイズ事例

- 認証モジュールの開発

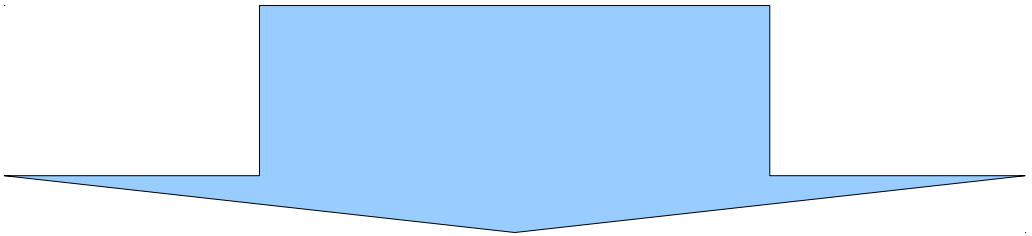


Copyright © 2012 Open Source Solution Technology, Corp.

カスタマイズ事例

- 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

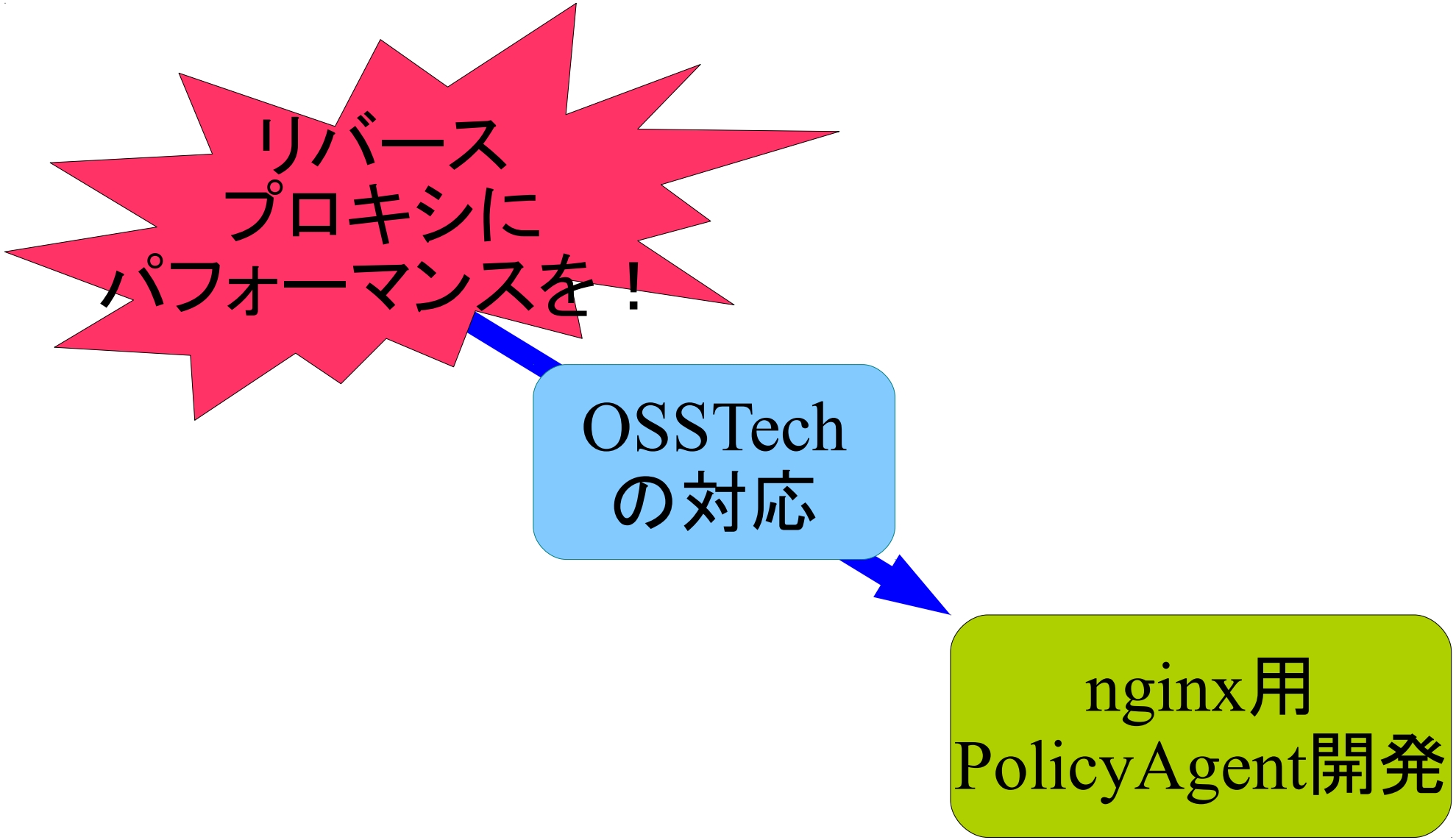


- 要件に合った認証モジュールを開発し、既存モジュールとの認証連鎖とした。

Copyright © 2012 Open Source Solution Technology, Corp.

開発事例

- Apacheより早いリバースプロキシを構築したい



Copyright © 2012 Open Source Solution Technology, Corp.

開発事例

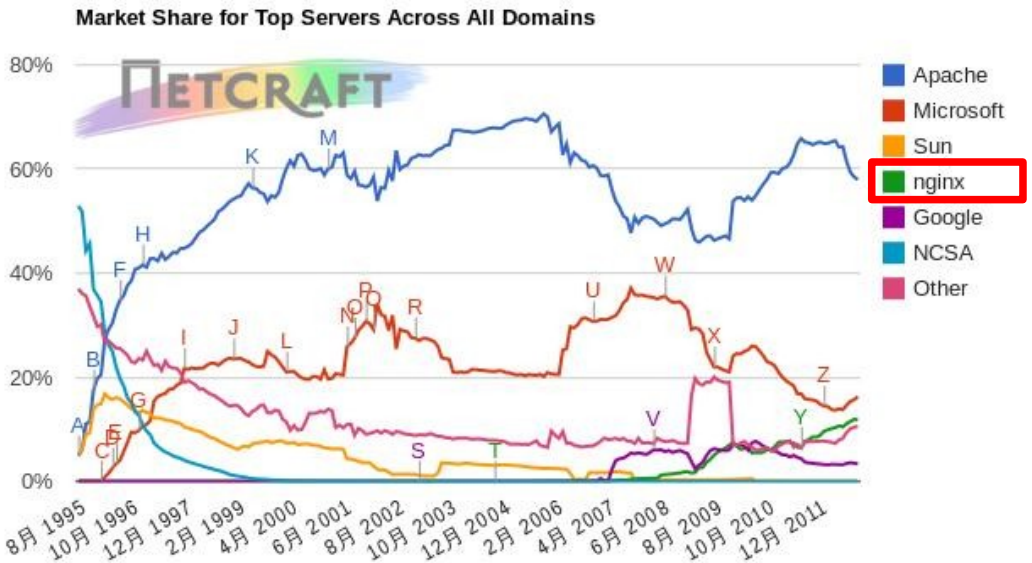
- Apacheより早いリバースプロキシを構築したい

- Apacheによるリバースプロキシよりスケーラビリティが欲しい

- nginx※用 Policy Agentの開発

※nginxとはスケーラビリティ、
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
十分の機能を持たせられる



Copyright © 2012 Open Source Solution Technology, Corp.

導入事例

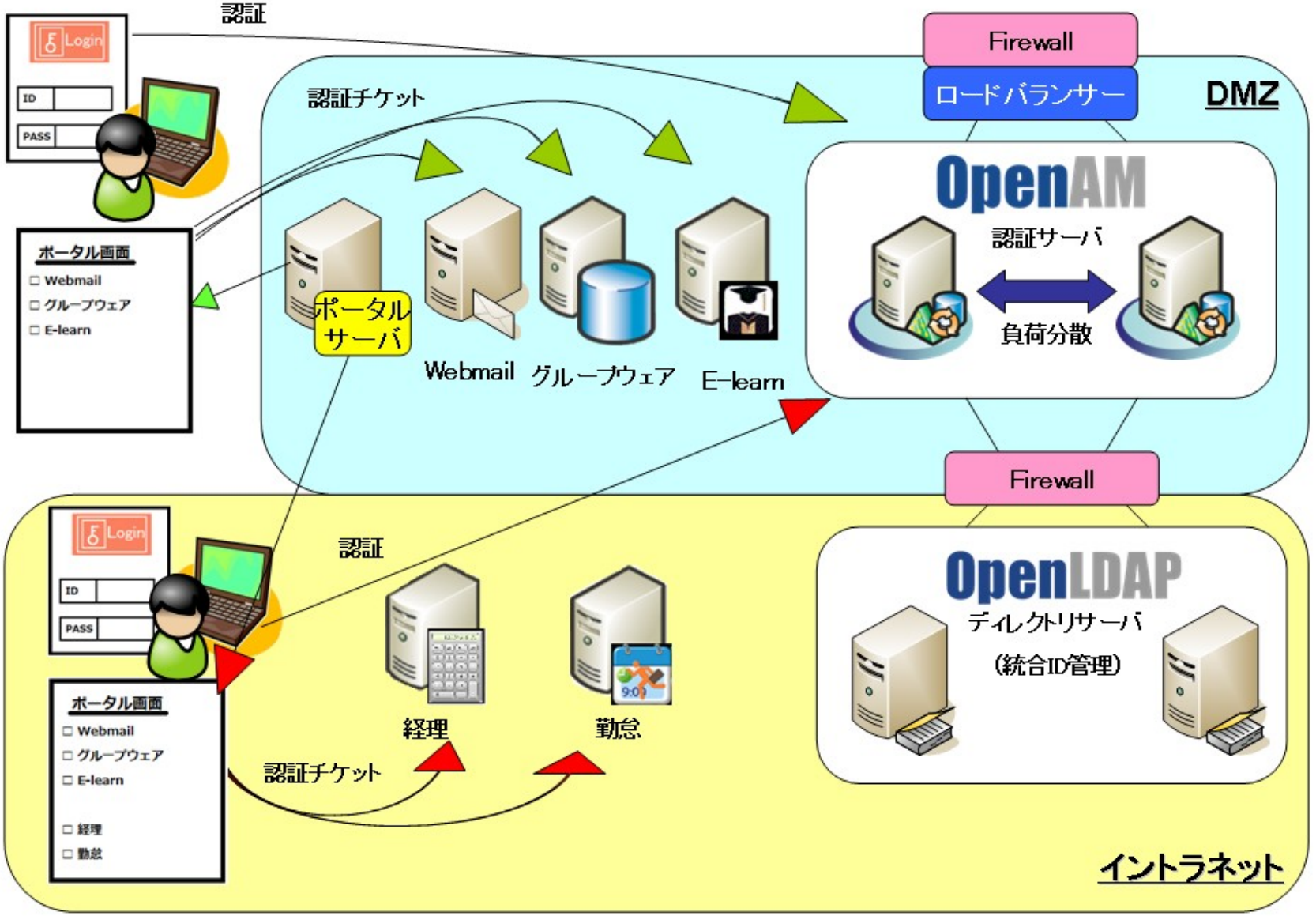
Copyright © 2012 Open Source Solution Technology, Corp.

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・テクノロジ株式会社が行いました。

北見工業大学様


認証
Login
ID
PASS
ポータル画面
□ Webmail
□ グループウェア
□ E-learn
認証チケット
Firewall
ロードバランサー
DMZ
OpenAM
認証サーバ
負荷分散
ポータル
サーバ
Webmail
グループウェア
E-learn
Firewall
認証
OpenLDAP
ディレクトリサーバ
(統合ID管理)
ポータル画面
□ Webmail
□ グループウェア
□ E-learn
□ 経理
□ 勤怠
経理
勤怠
認証チケット
イントラネット

国立大学法人 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

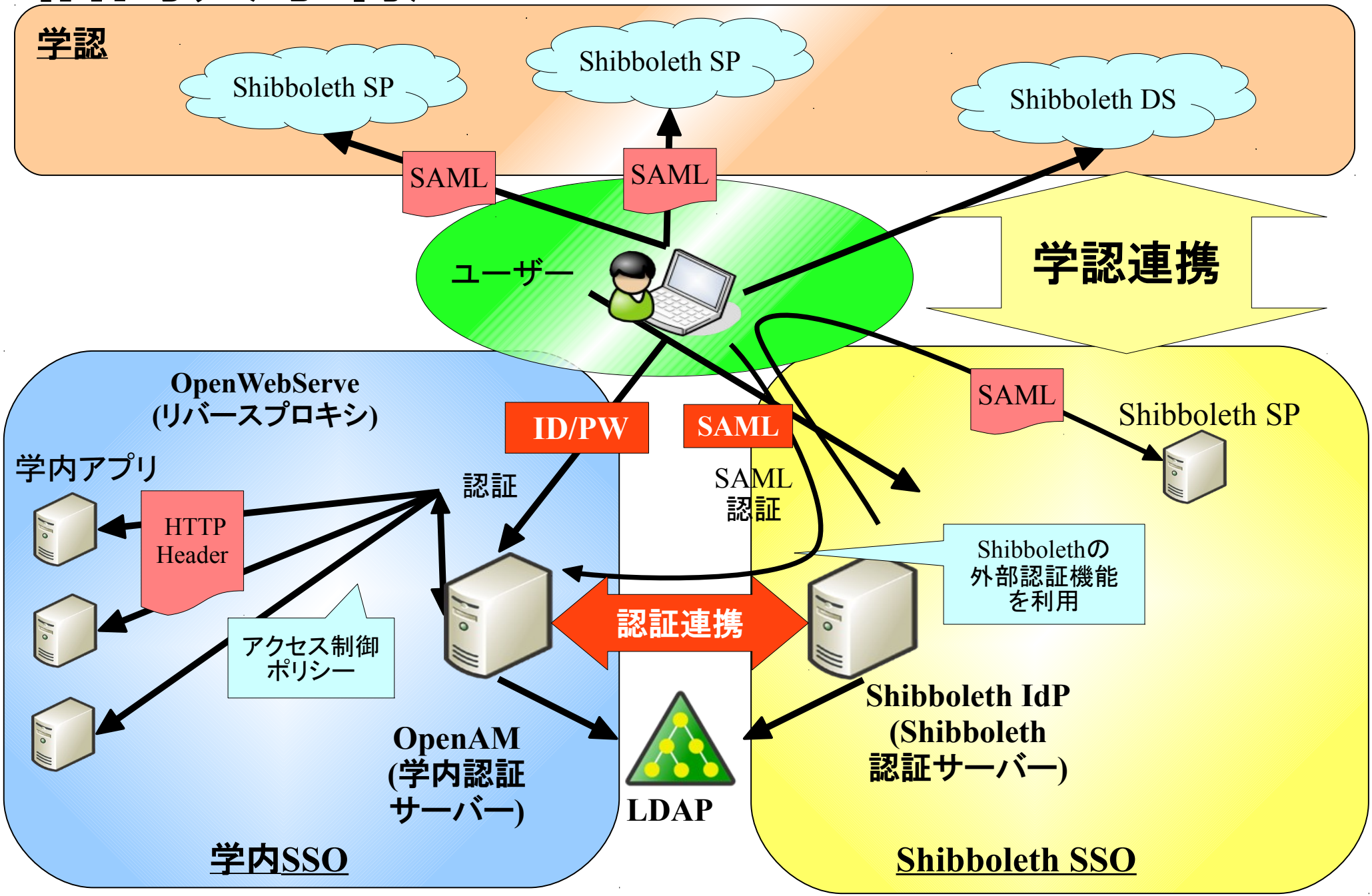
高い拡張性と柔軟性を持つ先進的SSO基盤の構築

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

Copyright © 2012 Open Source Solution Technology, Corp.

福岡大学様


学認
Shibboleth SP
Shibboleth SP
Shibboleth DS
SAML
SAML
ユーザー
学認連携
OpenWebServe
(リバースプロキシ)
ID/PW
SAML
SAML
Shibboleth SP
学内アプリ
認証
SAML
認証
HTTP
Header
Shibbolethの
外部認証機能
を利用
認証連携
アクセス制御
ポリシー
Shibboleth IdP
(Shibboleth
認証サーバー)
OpenAM
(学内認証
サーバー)
LDAP
学内SSO
Shibboleth SSO

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*

Copyright © 2012 Open Source Solution Technology, Corp.