第2回　OpenSSO&OpenAMコンソーシアムセミナー

OSS活用型認証基盤構築事例のご紹介
（当社構築事例にみるOpenAMの活用法）

株式会社オージス総研

IT基盤ソリューション第二部

吉田 貴英

2012年4月5日

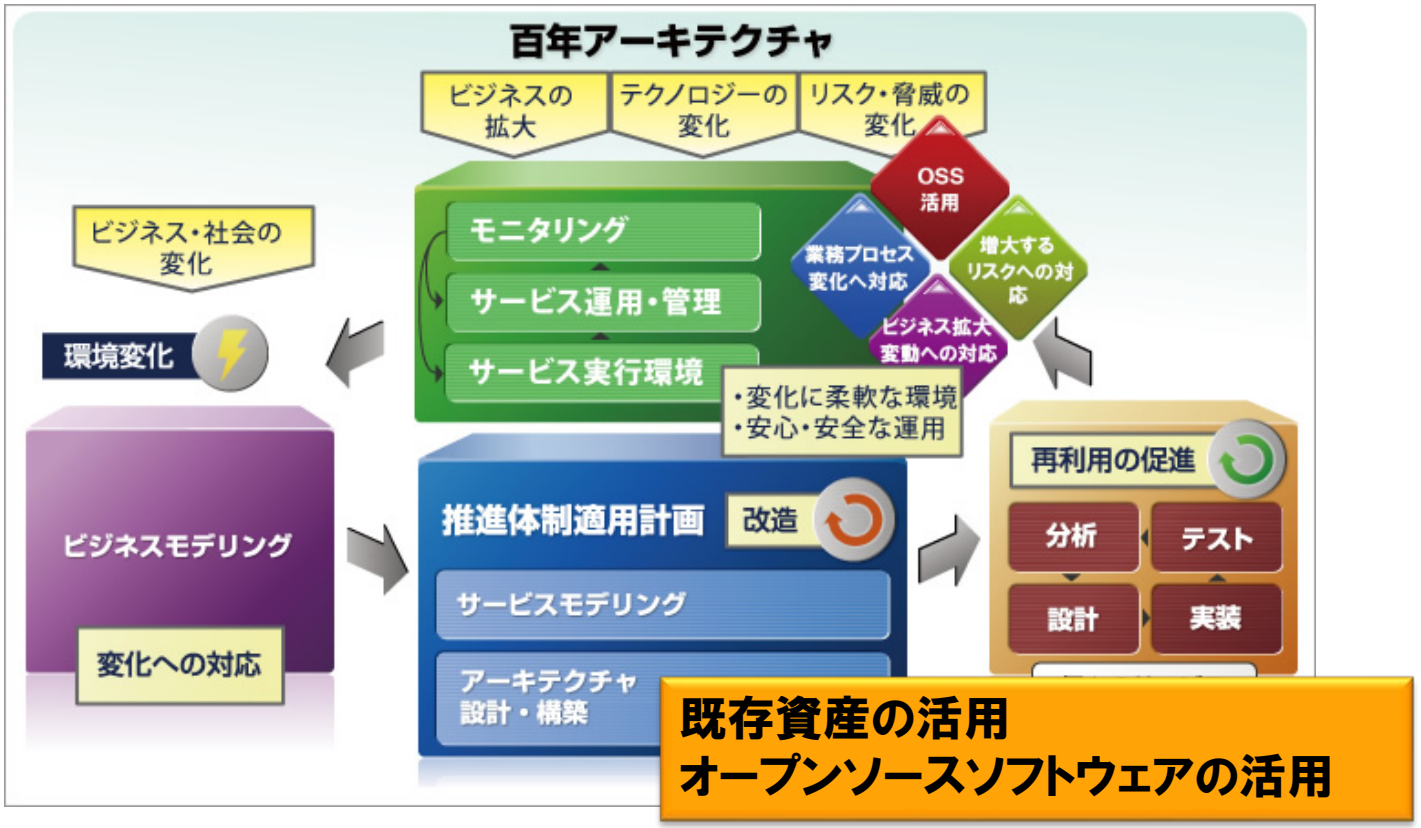
オージス総研のご紹介

- 社名　株式会社オージス総研
- 代表者　取締役社長　平山　輝
- 設立　1983年6月29日
- 資本金　4億円（大阪ガス株式会社100%出資）
- 売上実績　512億円（連結）　270億円（単体）（※2010年度）
- 従業員数　2,847名（連結）　1,248名（単体）（※ 2011年3月31日現在）
- 連結対象　さくら情報システム（株）、（株）宇部情報システム、（株）システムアンサー、OGIS International, Inc.
- 事業内容　ソフトウェア開発、情報処理サービス、コンピュータ機器・ソフトウェアの販売

持続可能なビジネスシステムを目指して

百年アーキテクチャ

持続可能なIT、再生可能なITについてオージス総研ができることは何か…
そこから生まれたもの、それが「百年アーキテクチャ」という概念です。



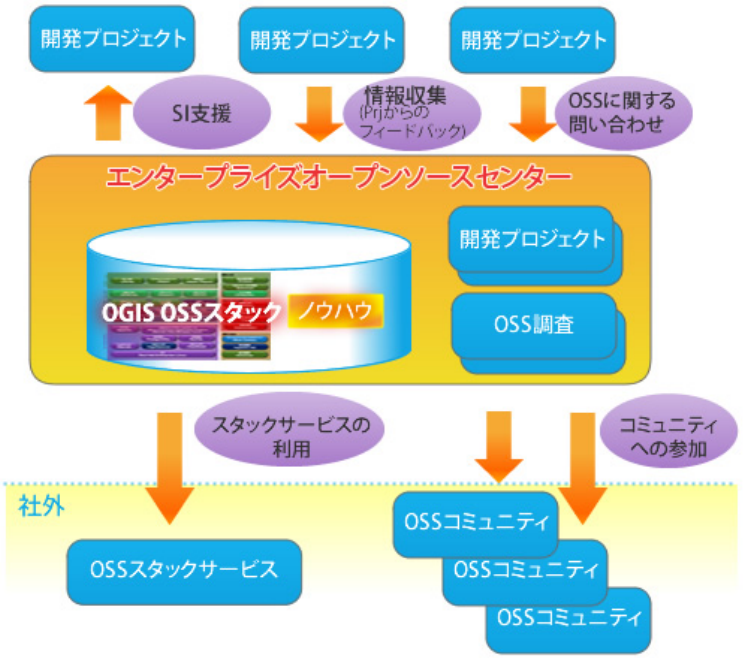
オープンソースソフトウェアへの積極的な取り組み

取り組み

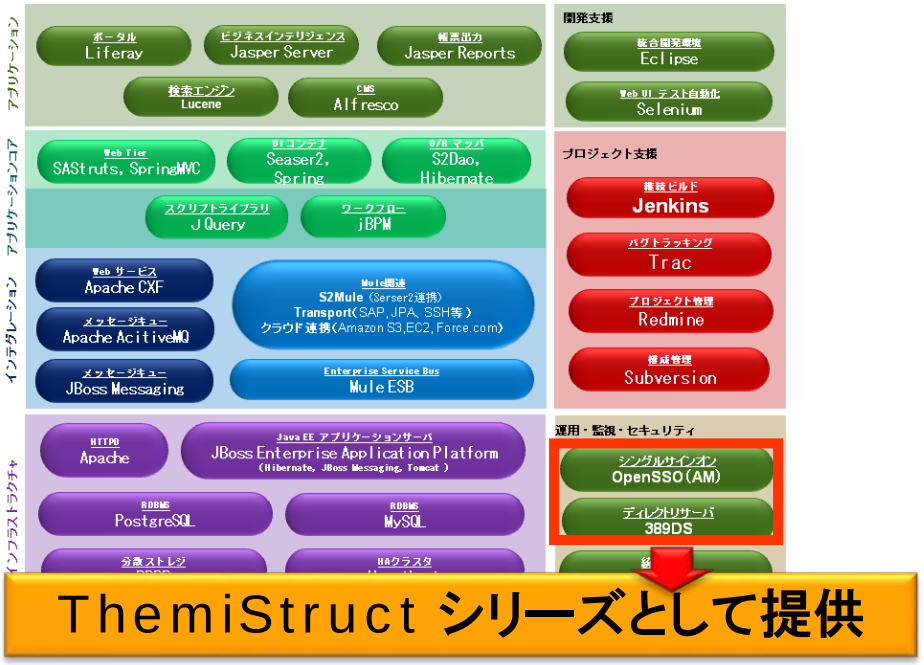
より長く、安心してオープンソースソフトウェア(OSS)をお使い頂くために社内にエンタープライズ・オープンソース・センターという技術の統括部門を設けて、実証実験や技術開発を推進しています。

2009年4月設立

体制



OSSリファレンススタック



OGIS-RI

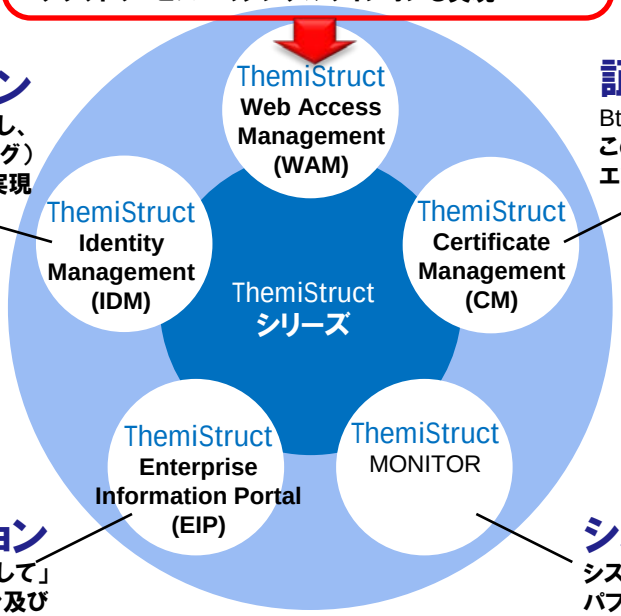
ThemiStruct®（テミストラクト）シリーズラインナップ

ThemiStructとは

ThemiStructはOSS(オープンソースソフトウェア)を活用したIT基盤ソリューション全体を指すブランドです。提唱する百年アーキテクチャを具現化し、業務に合わせた柔軟で持続可能なソリューションを「適正な価格」で提供します。

アクセス管理ソリューション

ユーザが一度認証を受ければ、他の許可されている
システムへのログイン、利用が可能（シングルサインオン）
クラウドサービスへのシングルサインオンも実現



ID管理ソリューション

ユーザのアカウント情報を一元管理し、
アカウントの作成、更新、削除の自動化（プロビジョニング）
クラウドサービスへのプロビジョニングも実現

証明書管理ソリューション

BtoB ECでよく利用されるクライアント端末認証、
この時に利用する電子証明書の発行、
エンドユーザ向けダウンロード環境の提供

企業向け情報ポータルソリューション

「企業の情報を統合した情報ポータルとして」
インターネット、イントラネットに分散したアプリケーション及び
情報を一元的に表示することが可能

システム管理ソリューション

システムの稼働監視(サーバ、プロセス、サービスなど)、
パフォーマンス監視、ログ監視が可能

アジェンダ

I. 当社におけるOpenAM活用方法
   i. 社内/社外のシステムのシングルサインオン
   ii. ESBとSAMLを組み合わせたシステムインテグレーション

II. 事例紹介
   i. グループ会社共通認証基盤構築
   ii. リモートアクセス対応した社内認証基盤構築

III. 認証基盤に求められる要件
   i. リバースプロキシのポイント
   ii. 二要素認証のポイント

IV. まとめ

Ⅰ. 当社におけるOpenAM活用方法

当社におけるOpenAM活用方法

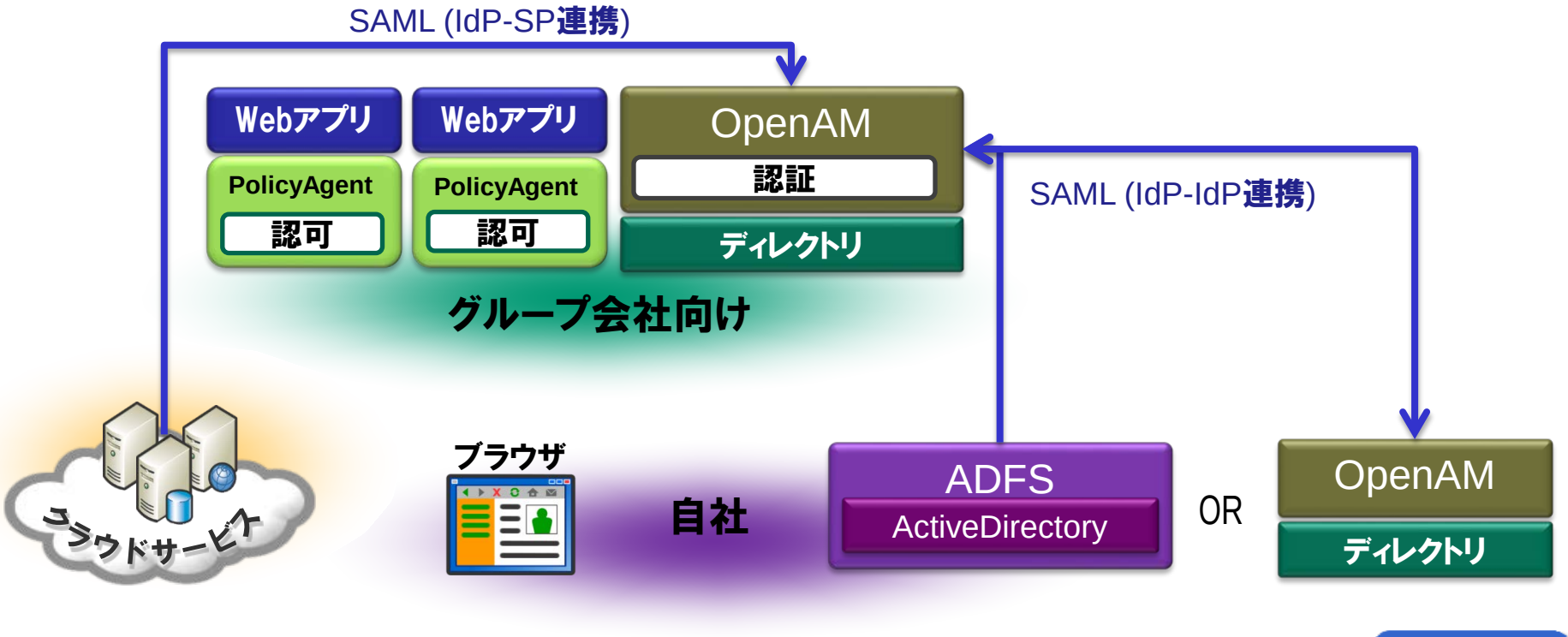
当社の構築・開発案件パターン

- 社内/社外のシステムのシングルサインオン
- ESBとSAMLを組合せたシステムインテグレーション

社内/社外のシステムのシングルサインオン

社内/社外のシステムのシングルサインオン

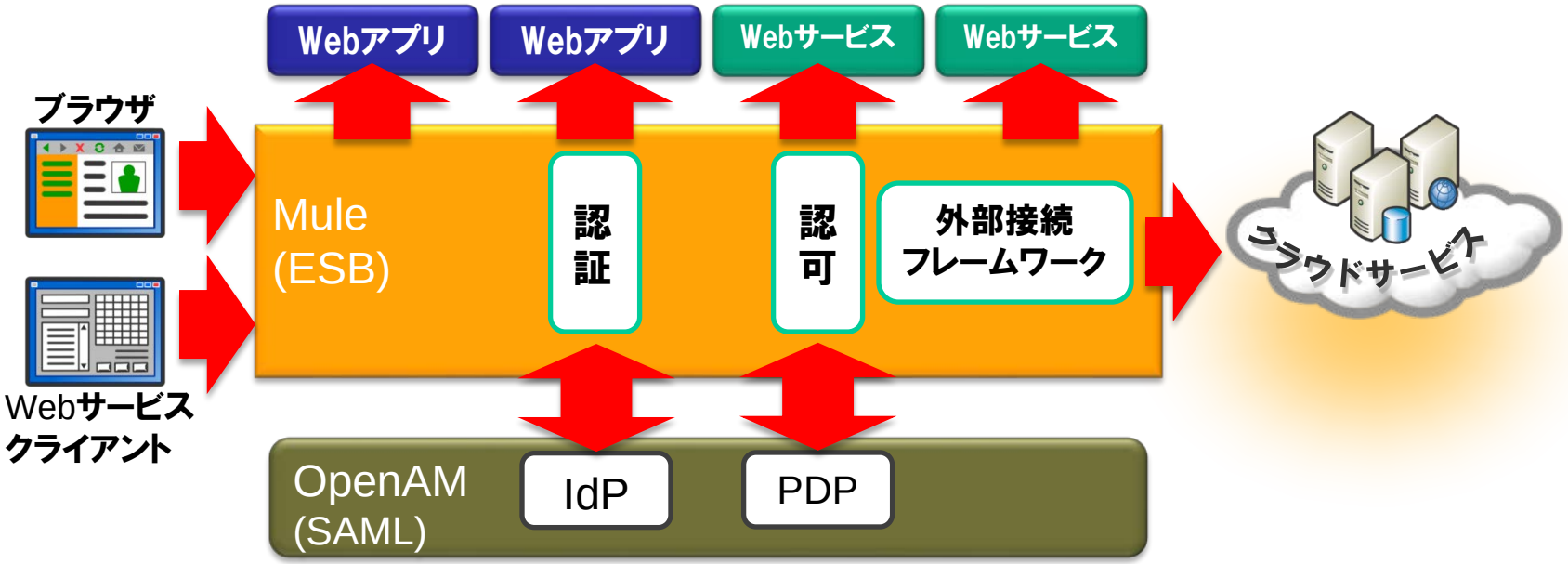
自社内向け・グループ会社向け・取引会社向けにおけるWebアクセスをシームレスに実現できるようにシングルサインオン環境の構築を実施



ESBとSAMLを組合せたシステムインテグレーション

ESBとSAMLを組合せたシステムインテグレーション

安全にシステム連携をする仕組みを実現するために、ESB(Mule)と
SAML(OpenAM,OpenSAML)**を組み合わせたシステムを構築する。**



II. 事例紹介

事例紹介

以下の事例についてご紹介いたします。

某運輸業様
グループ会社共通認証基盤構築

オージス総研
リモートアクセス対応した社内認証基盤構築

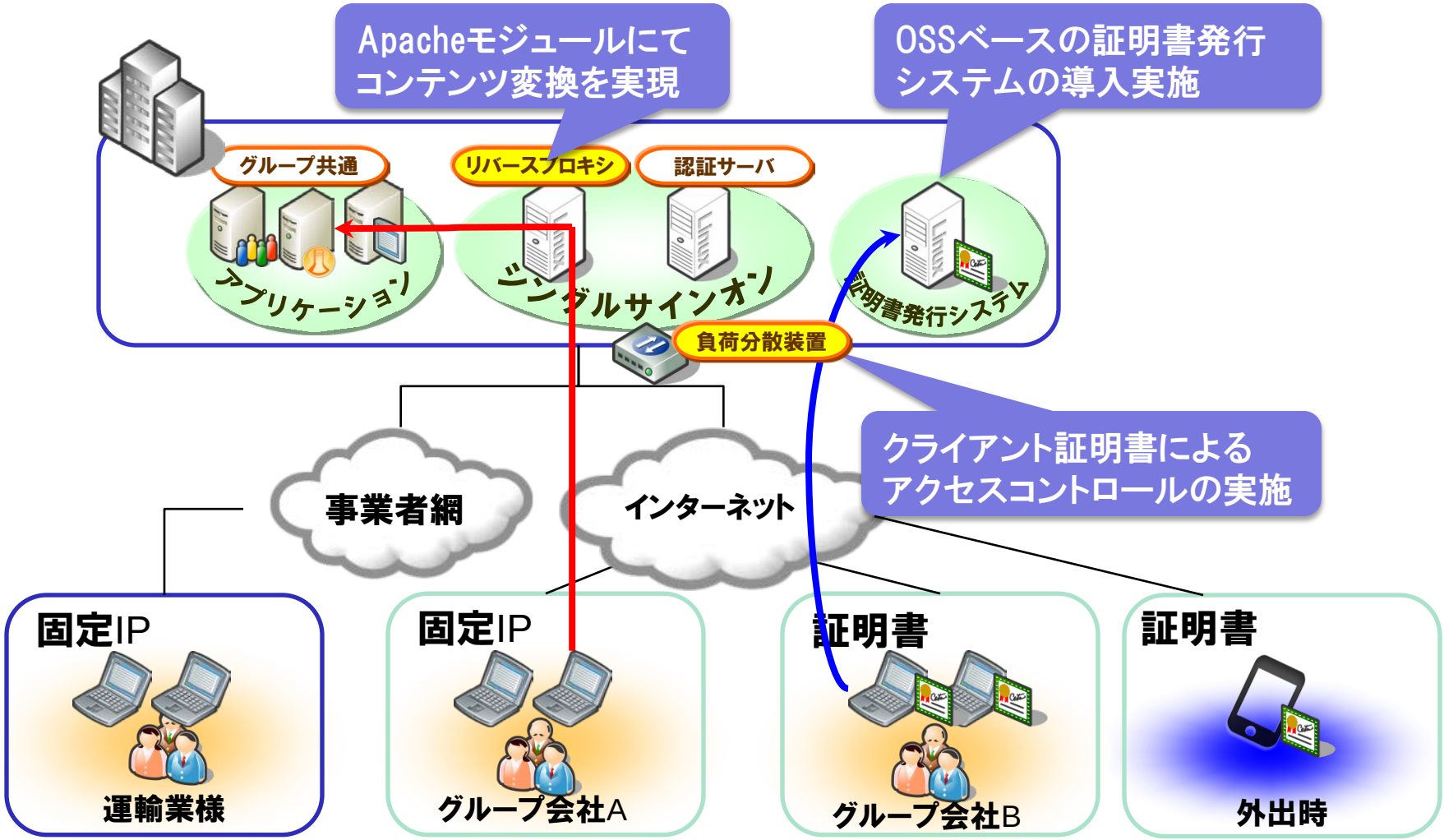
事例1　グループ会社共通認証基盤構築①

システム構築の目的

グループ全体でIT利用の効率化・コスト削減を実現するために、グループ企業へのサービス提供を実施する。
そのための基本となる認証基盤の構築を行う。

- グループ会社全体のセキュリティ向上
- グループ会社で共用することによるコスト削減
- 各グループ会社におけるシステム要員の負担軽減

事例1　グループ会社共通認証基盤構築②



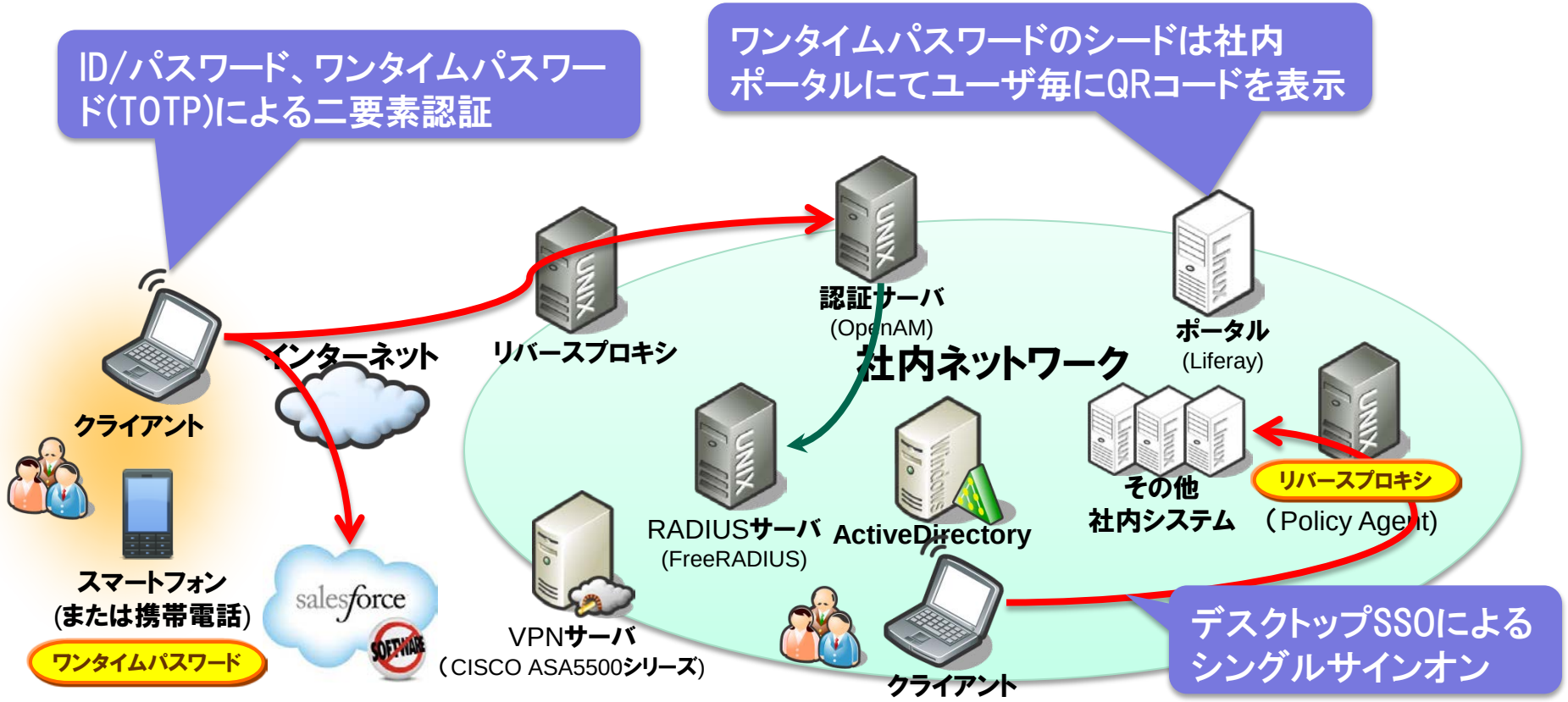
事例2　リモートアクセス対応した社内認証基盤構築①

システム構築の目的

社内システムの利便性向上を実現するために、シングルサインオン環境を構築する。
また、既存の商用リモートアクセス環境に対しても本シングルサインオン環境で認証することでコスト削減を実施する。

- 社内システムの利便性向上の実現
- リモートアクセス環境の有効活用によるコスト削減
- スマートデバイス・クラウドサービス利用に向けて基盤準備

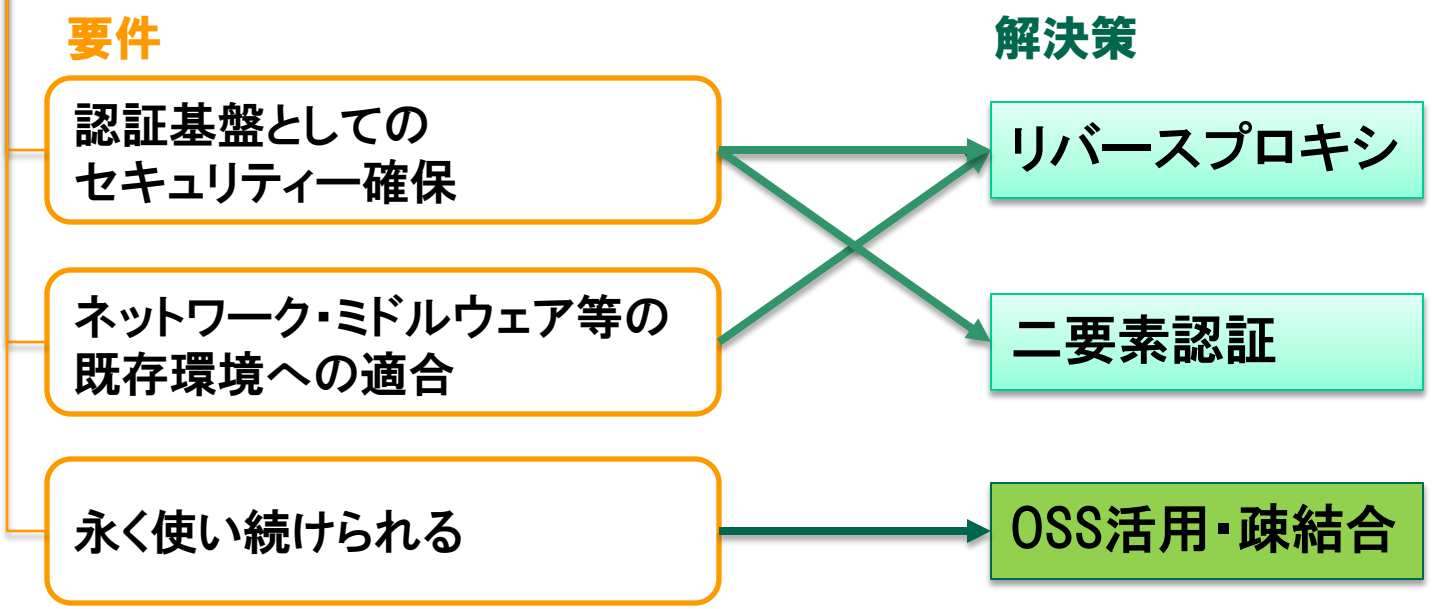
事例2　リモートアクセス対応した社内認証基盤構築②



III.認証基盤に求められる要件

認証基盤に求められる要件

当社が実施してきたOpenAM関連の案件において
共通して求められる要件は以下の通り。



リバースプロキシのポイント①

リバースプロキシ

リバースプロキシを実現する上で…

通常機能で実現

- セキュリティの確保
- 既存の環境に手を加えない
- パッケージ製品への対応

＋

標準機能にないニーズ

- パスワード連携
- 代理認証
- コンテンツ変換

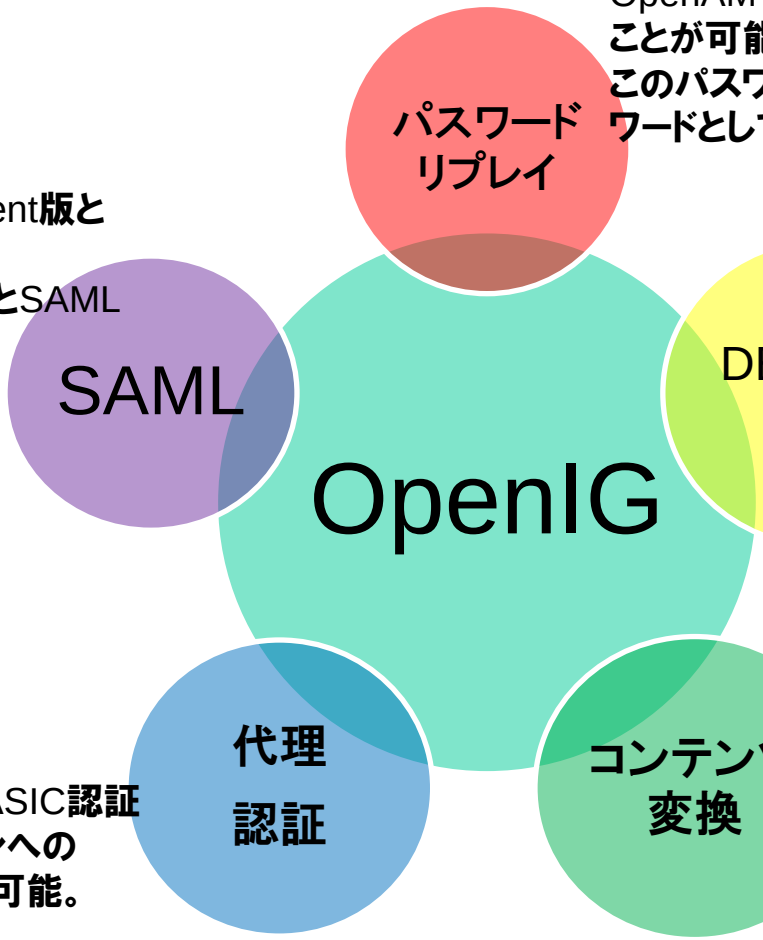
リバースプロキシ型に
に求められる機能は多い

これまで	これからは
mod_rewrite ＋ 独自Apacheモジュール	Identity Gateway OpenIG

参照：第1回　OpenSSO&OpenAMコンソーシアム　技術セミナー
オージス総研 講演資料

リバースプロキシのポイント②

- OpenIGの機能



OpenAMへのログイン時パスワードを連携することが可能。
このパスワードを利用して代理認証用のパスワードとして利用可能。

OpenIGにはPolicy Agent版とFedlet版がある。
Fedlet版ではOpenAMとSAML通信が可能。

データベース・ディレクトリ上のデータへアクセス可能。
それらのデータを利用して代理認証などで利用可能。

設定でForm認証・BASIC認証などのアプリケーションへのシングルサインオンが可能。

独自フィルターを実装・組込みが可能。
当社では正規表現によるコンテンツ変換用フィルタを実装。

二要素認証のポイント①

二要素認証

二要素認証を実施するにあたり

典型的な二要素認証は…

ID/パスワード ＋ ワンタイムパスワード OR 電子証明書

しかし、課題も….

- ハードウェアトークンの管理
- 認証実施に伴うコスト
- 標準HOTPモジュールの利便性

- オープンソースソフトウェアを活用して
- 適度なセキュリティーで

Google認証
(ワンタイムパスワード生成)

EJBCA
(クライアント証明書発行)

二要素認証のポイント②

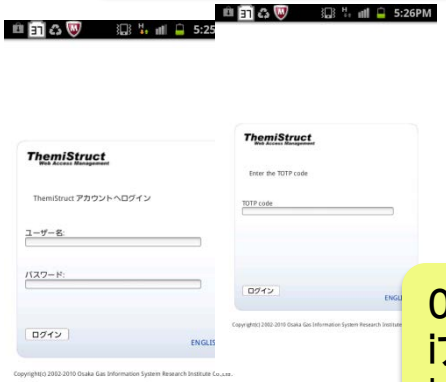
コストを抑えたワンタイムパスワードの実現方法例

ワンタイムパスワード用シードをディレクトリから取得し、QRコードとして表示する。
Google認証はカメラを利用してQRコードからユーザ個別のシードをセットすることができる。

TOTP用QRコード表示Portlet

Liferay

Google認証(TOTP)をワンタイムパスワードアプリとして利用する場合は以下のサイトからソース入手可能。
https://code.google.com/p/google-authenticator/



ディレクトリ
(ActiveDirectory, LDAP)

OTP用シード

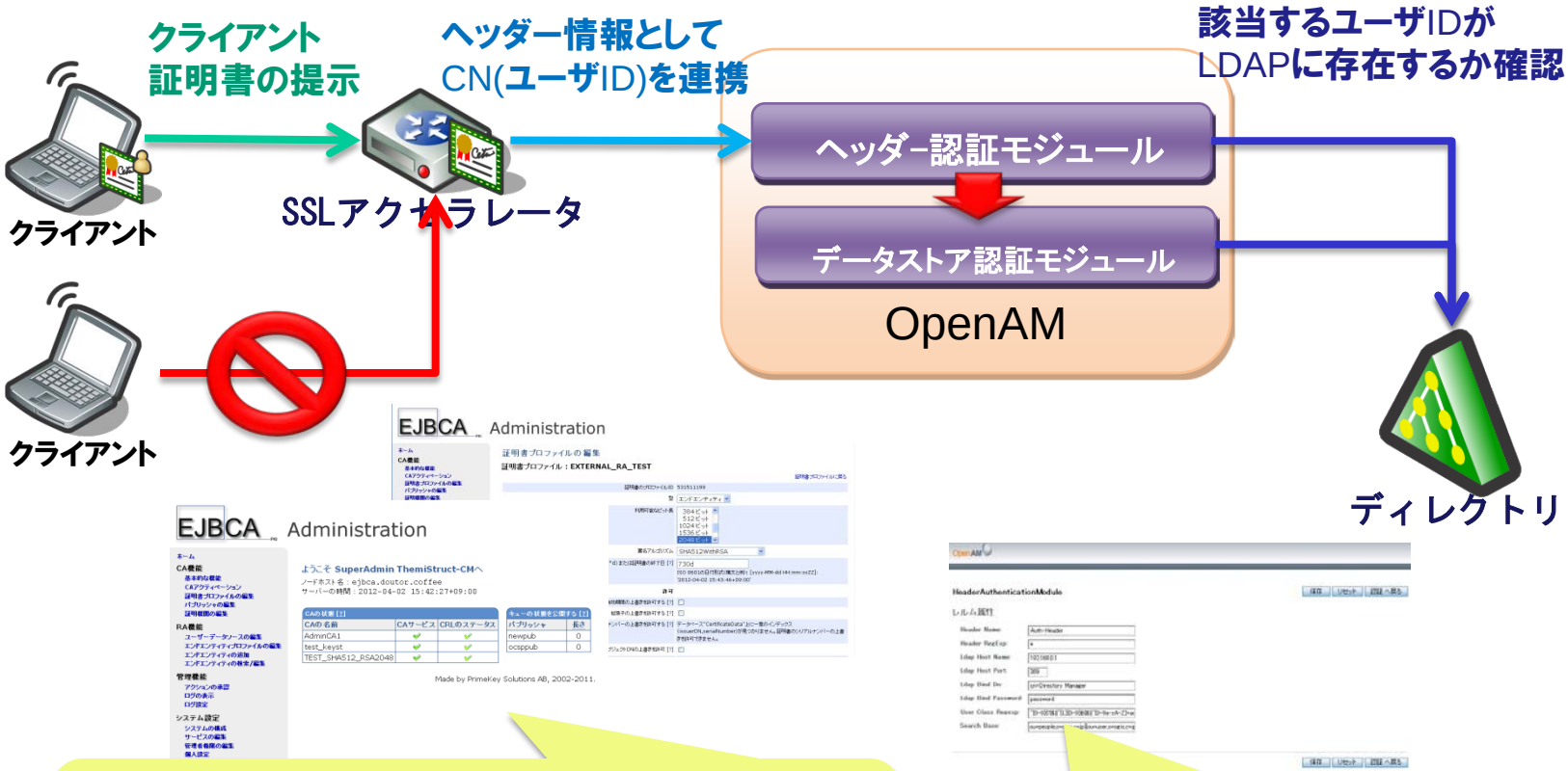
TOTP認証モジュール

OpenAM

OpenAM用TOTP認証モジュールを以下で公開
iアプリ用のTOTPモジュールも提供中。
https://code.google.com/p/themistruct-wam/

二要素認証のポイント③

オープンソースソフトウェアを用いた証明書による二要素認証の実現方法例



OSSクライアント証明書発行システムEJBCA 4.0.11 から日本語化ファイルが追加される。
http://www.ejbca.org/

独自ヘッダ認証モジュールの管理画面例

IV.まとめ

まとめ

認証基盤の実装方法とそのねらい・メリット

■リバースプロキシの実装方法
- 独自Apacheモジュール
- OpenIG

■二要素認証の実装方法
- Google認証
- EJBCA

その他のオープンソースソフトウェアと組合せて利用すること以下のメリットが得られます。

セキュリティリスク軽減 | **開発コスト削減** | **ユーザ利便性向上**

参照：第1回　OpenSSO&OpenAMコンソーシアム 技術セミナー
オージス総研 講演資料

持続可能なビジネスシステムを実現へ

OGIS-RI

ご清聴ありがとうございました

【お問合せ先】

株式会社オージス総研

東日本営業部

TEL 03-5440-4771

E-mail info@ogis-ri.co.jp