

OpenSSO&OpenAMコンソーシアム 技術セミナー

# **OSS活用型認証基盤構築事例のご紹介** **(認証基盤の作り方と広げ方)**

株式会社オージス総研  
IT基盤ソリューション第一部

八幡 孝

2010年11月18日

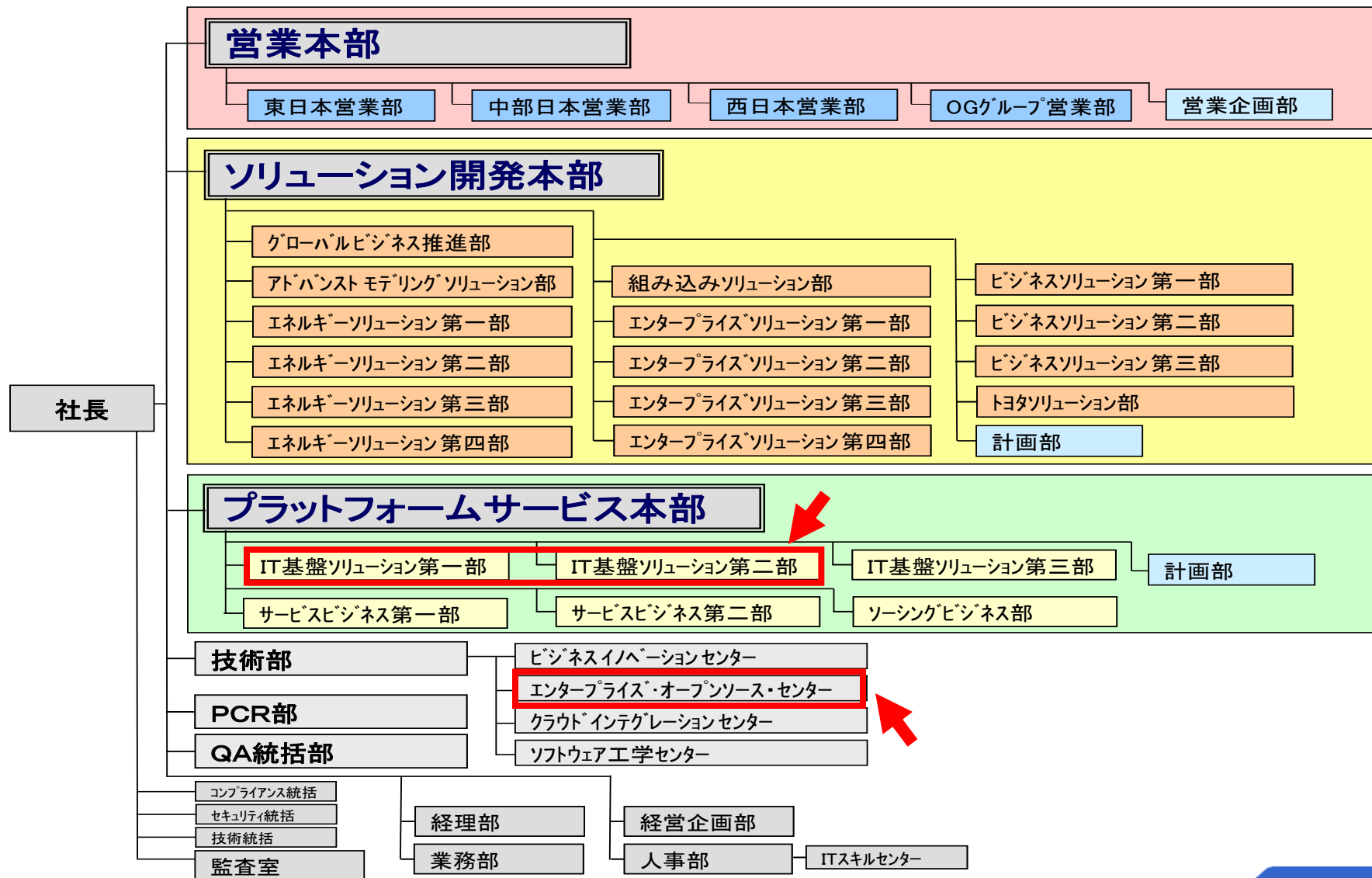
# オージス総研のご紹介

オージス総研 データセンター全景



- 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 509億円(連結) 257億円(単独) (※2009年度)
- 従業員数 2,841名(連結) 1,186名(単独) (※2010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

# オージス総研の組織図（2010年4月現在）



# エンタープライズ・オープンソース・センター (EOSC) のご紹介

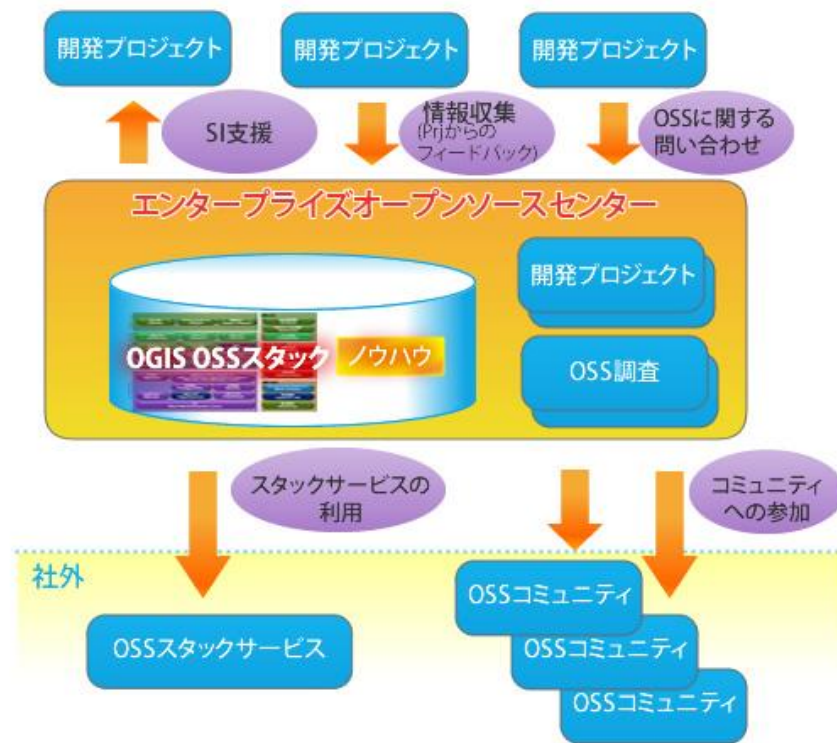


## ミッション

- SIやサービスビジネスなどへのOSS利用実績、ノウハウの蓄積
- オージス総研におけるOSS活用の促進、先端技術の提供

## 取り組み

- OSSの動向調査
- OSSリファレンススタックの整備
- 商用プロダクトとの相互運用性検証
- オープンソースコミュニティへの貢献
- 次世代ソリューションへのOSS適用技術開発
- OSSライセンスリスクの削減  
診断ソリューション・サービスの提供



2009年4月設立

# OGIS OSS リファレンススタック

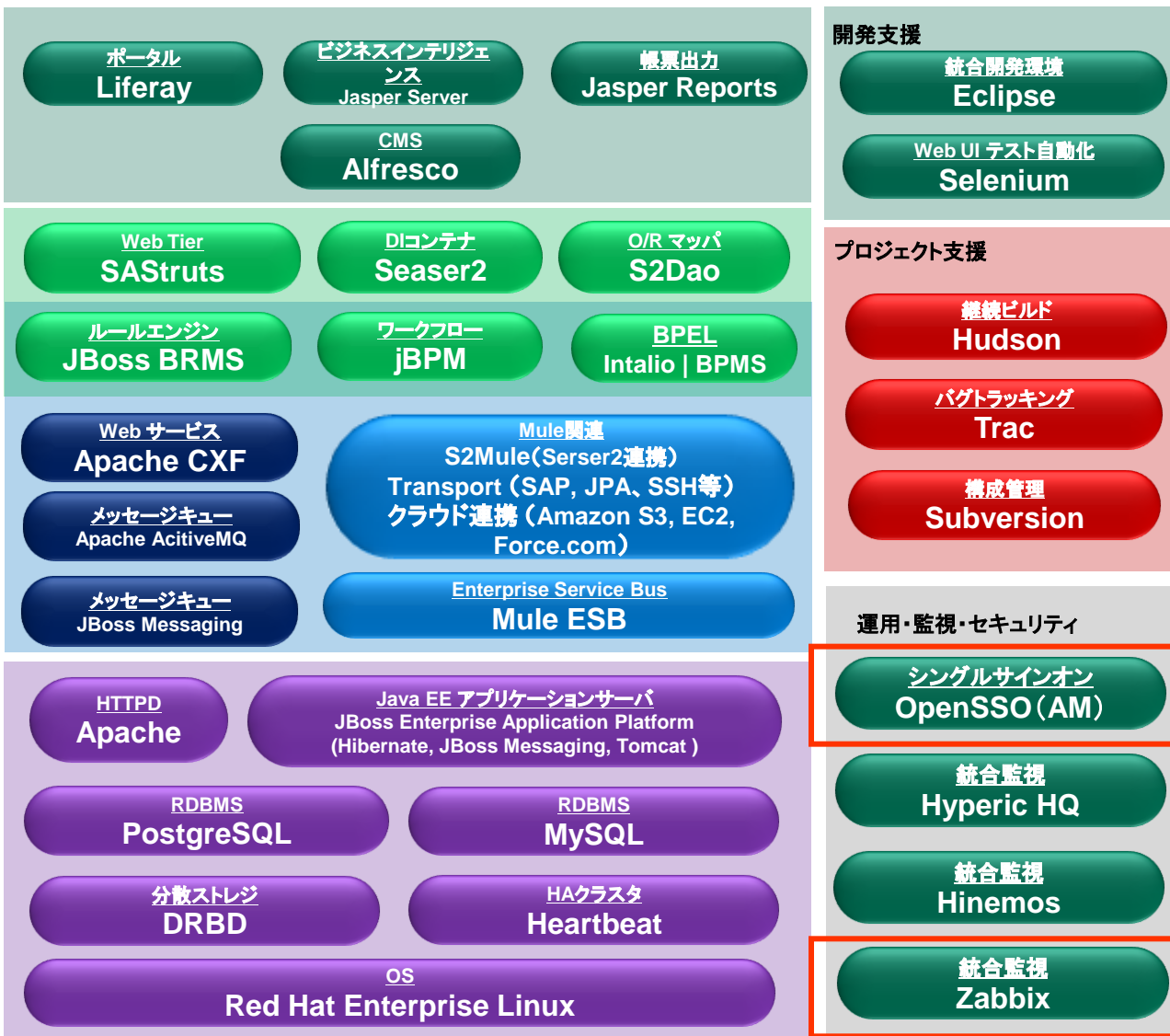


アプリケーション

アプリケーションコア

インテグレーション

インフラストラクチャ



**ThemiStruct**  
シリーズとして  
提供

# アジェンダ

1. 大阪ガスの認証基盤
2. 認証基盤展開の歴史
3. 認証基盤実現のねらい・メリット
4. 認証基盤のアーキテクチャ
5. 認証基盤を活用する
6. なぜOSS活用なのか？
7. 開発したSSOソフトウェアのアーキテクチャ
8. 今後の展開
9. ソリューション展開の方向性
10. ***ThemStruct-WAM***としてのソリューション化
11. ***ThemStruct-WAM***のアーキテクチャ
12. ***ThemStruct-WAM***での機能エンハンスメント
13. 弊社での他の構築実績
14. まとめ

# 1. 大阪ガスの認証基盤

- 用途に応じて、5つの認証基盤を構築
  1. 社内システム向け
  2. 代理店システム向け
  3. 携帯アプリケーション向け
  4. B2B顧客向け
  5. マイ大阪ガス(一般家庭顧客向け)

いずれもOSS活用型、リバースプロキシ構成で実現

# 1. 大阪ガスの認証基盤

## ■ 社内システム向け

- 社内ポータル(Liferay)、社内業務アプリ(Web)利用時の認証
- アプリ単位でのアクセス制御
- 社員証を使った認証(PKI)
- グループ会社向けへも提供

## ■ 代理店システム向け

- 代理店向け業務アプリ(Web)利用時の認証、アクセス制御
- PKIとID/パスワードの併用

## ■ 携帯アプリケーション向け

- iモード用Webアプリ利用時の認証
- 携帯電話向けの操作が簡易となる認証方式

## ■ B2B顧客向け

- 法人契約顧客向けアプリ(Web)利用時の認証、アクセス制御

## ■ マイ大阪ガス(一般家庭顧客向け)

- 大阪ガス利用の家庭ユーザ向けの情報サイトの認証
- 複数の情報画面(アプリ)間でのシングルサインオン

総ユーザ数  
約25,000ユーザ  
総アプリケーション数  
約600システム

「マイ大阪ガス」URL:

<http://www.osakagas.co.jp/my-page/index.html>



## 2. 認証基盤展開の歴史

- 2002年度
  - 社内向け認証基盤を商用の認証製品を使って構築
  - 開発標準を文書化
- 2003年度
  - 代理店向け認証基盤を商用の認証製品を使って構築
- 2004年度
  - 社内向け認証基盤へ、社員証(PKI)を使った認証機能を追加
- 2005年度
  - 社内向け認証基盤の社員証認証機能を運用開始
  - 携帯向け認証基盤をOSSを組合せて開発、構築（初期バージョン）
- 2006年度
  - B2B向け認証基盤をOSSを組合せて開発、構築（PC対応開始）
- 2007年度
  - 社内向け認証基盤をOSS化する開発、検証に着手（PC本格対応）
- 2009年度
  - 社内向け認証基盤のOSS活用型への移行完了
  - マイ大阪ガスサービス開始
- 2010年度
  - 代理店向け認証基盤のOSS活用型への移行完了
  - 携帯向け認証基盤の最新化完了予定

# 3. 認証基盤実現のねらい・メリット

## ■ セキュリティリスクの軽減

- ID管理、認証処理の一元管理
- システム単位でのアクセス制御の一元管理
- アカウントポリシー、パスワードポリシーの一元管理
- システムへのアクセス記録の一元管理

## ■ 開発のコスト削減

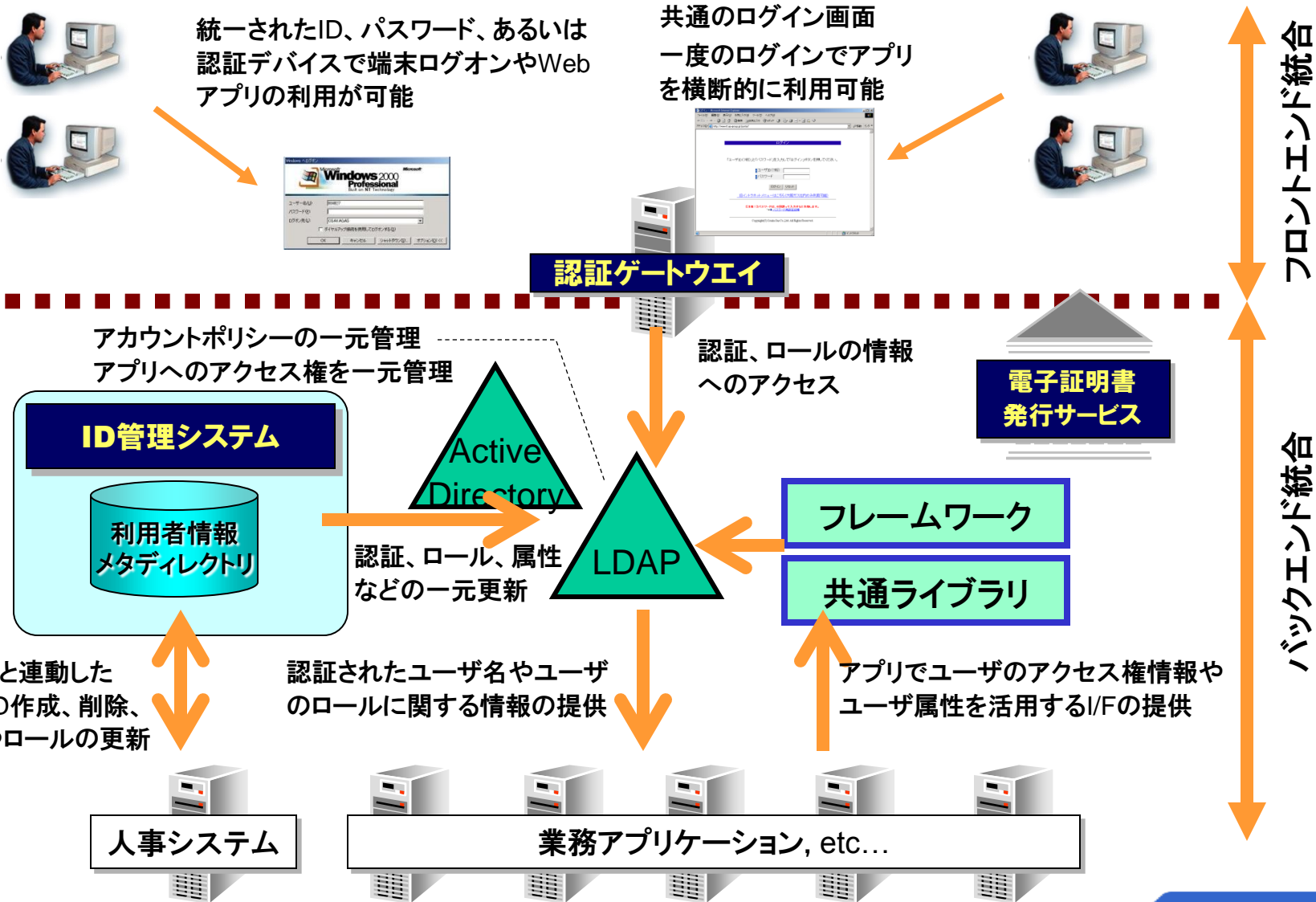
- 認証機能、アクセス制御機能の個別実装が不要
  - ・ 特にID管理、認証処理
- セキュリティポリシー変更時の個別開発が不要
  - ・ 認証方式の変更

## ■ ユーザの利便性向上

- ユーザID/パスワードが統一される
- 一度のログインで複数アプリケーションをシームレスに利用可能
- ユーザサポートコストの低減

# 4. 認証基盤のアーキテクチャ

認証基盤



# 5. 認証基盤を活用する

ねらい  
メリット

セキュリティリスクの軽減  
開発コストの削減  
ユーザの利便性の向上

広げる・永く使い続ける

アプリケーションを集める

アプリケーションをつなぐ

認証基盤を作る

?

コスト  
サポート

- 共通基盤としての利用ルール整備
- 接続方式のパターン化・標準化
- 開発担当向けガイドの提供
- レビュー等による標準外構成の除外

- 接続方式の決定・設定
- アプリケーションの修正
- 認証基盤側でのカスタマイズ対応

- SSO製品の導入
- IDM製品の導入

# 6. なぜOSS活用なのか？

## ■ コスト削減

- ユーザ数増加によるライセンス費用、保守費用の増加が抑制できる。

➡ コンシューマ向けサイト運用においても費用負担を大幅軽減

## ■ 構成の柔軟性

- オープンソースソフトウェアの活用により、特定のソフトウェア、ハードウェアへの依存度が減り、構成の柔軟性が確保される。

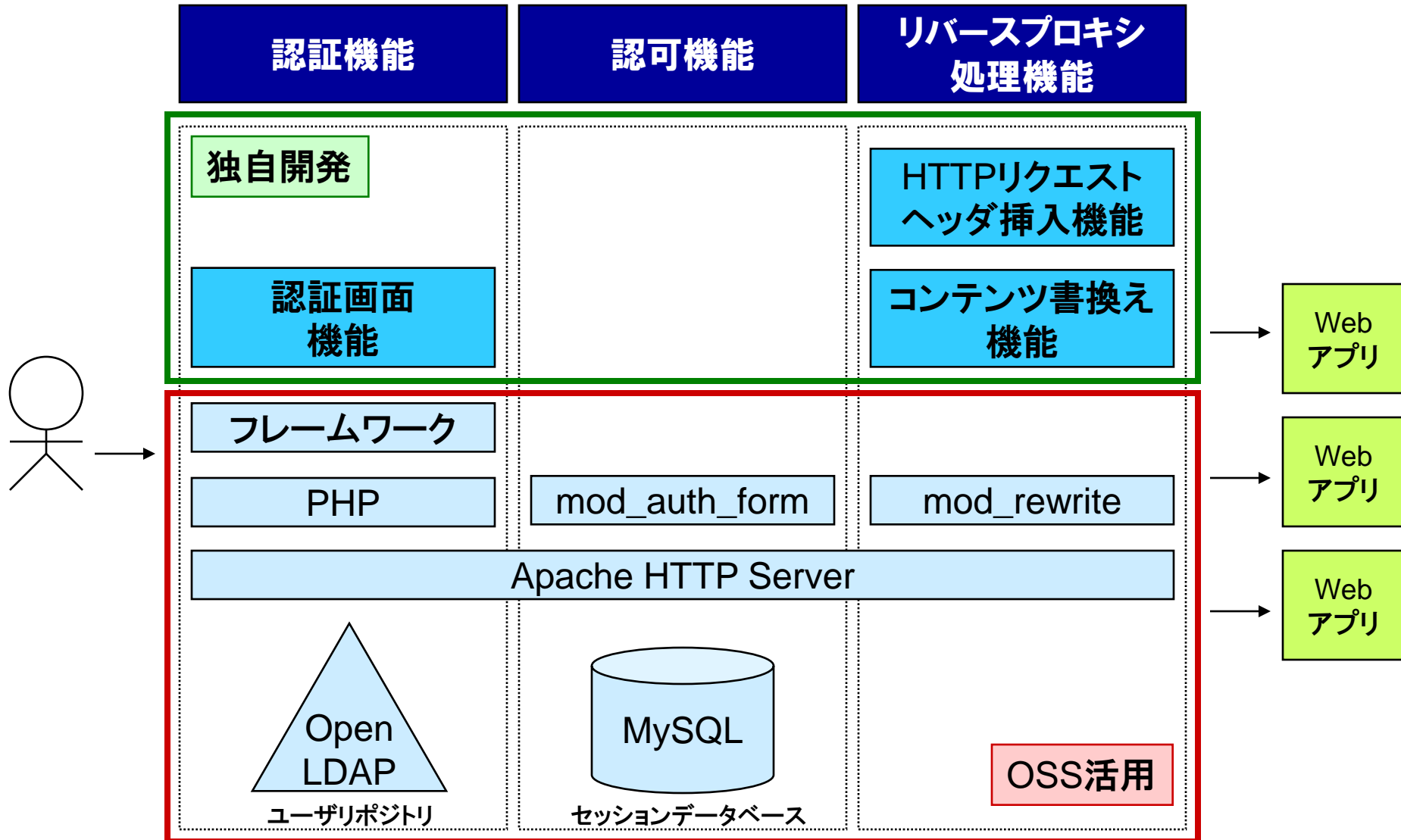
➡ 商用UNIXサーバからLinuxサーバへの変更、集約へ道筋

## ■ 長期間サポート

- オープンソースであるため、徹底的な原因究明が可能。
- ソースコードを使った長期間サポートが可能。

➡ 長い目で見た信頼性向上の実現

# 7. 開発したSSOソフトウェアのアーキテクチャ



# 8. 今後の展開

## センター内既存環境

認証システム

ThemiStruct-WAM  
(リバースプロキシ版、  
OpenAM版)



ID管理システム

ThemiStruct-IDM



ホスト



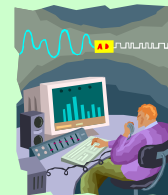
統合サーバ



個別分散サーバ



システム運用  
エンジニア



弊社  
データセンター

- ・認証情報の連携
- ・アカウント(ID)情報の連携

## Private Cloud 環境

個別分散サーバ      グループ会社向け  
共用サービス(メール、グループウェア、etc.)

1. グループ向けクラウドを使ったグループ全体最適

3. センター内既存アプリ、クラウド上のアプリの連携による、高度な業務システムの実現



Internet

2. パブリッククラウドサービスを使った効率的な業務アプリケーションの構築

## Public Cloud

アプリケーション環境として使うもの



## Public Cloud

サービスを使うもの  
アプリケーション機能を使うもの



# 9. オージス総研ソリューションの方向性

## ■ エージェント型構成への対応

- パッケージ製品を使ったアプリケーションへの対応の必要性
- Ajax利用のアプリケーションへの対応の必要性

➡ エージェント型構成に対応することで、コンテンツ書き換え機能の個別カスタマイズの必要性を回避

- リバースプロキシ型の構成の場合、コンテンツ内URLの書き換えが必要
- アプリケーションがURLの書き方のガイドを守っていない場合、個別対応が必要
- JavaScript内のURL書き換えは一般的に困難なケースが多い

## ■ 外部クラウドサービスとの認証連携への対応

- Salesforce.com / Force.com上のアプリケーションとの連携、SSO
- Google Appsとの連携、SSO

➡ 平たく言えば、SAMLを使った認証連携への対応

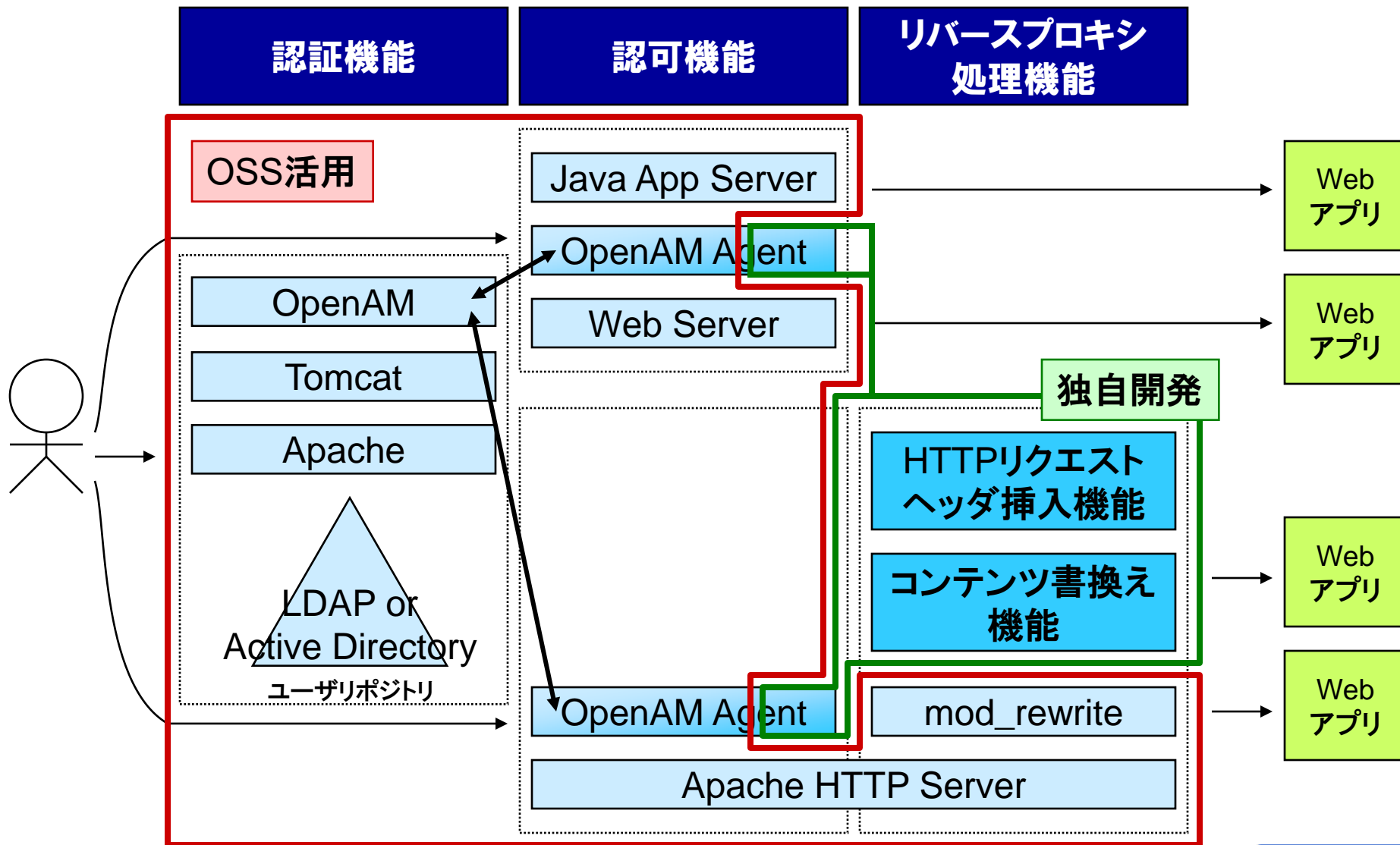


# 10. *ThemiStruct-WAM* としてのソリューション化

- アクセス管理ソリューション
- OpenSSO/OpenAM + リバースプロキシエンジン
  - SAML連携機能、エージェント型構成に OpenSSO/OpenAM に対応
  - 認証機能を OpenSSO/OpenAM へ統合
  - 大阪ガス向けで開発したリバースプロキシエンジンを採用
  - + OpenAM機能の独自エンハンスメント
- ***ThemiStruct-IDM*** と組み合わせ、認証、アクセス管理のトータルソリューションとして展開

※ ***ThemiStruct-IDM*** = OSS活用型 ID管理ソリューション (⇒ P21)

# 11. ThemisStruct-WAM のアーキテクチャ



## 12. *ThemisStruct-WAM* での機能エンハンスメント

- 長いパスワードが利用できる機能
  - 16文字より長いパスワードでの認証が可能に
- 認証用パスワードをアプリケーションに伝達できる機能
  - 認証時に入力したパスワードを、アプリケーションに伝達
  - アプリケーションへの認証代行を行なう機能で利用
- IISエージェントフィルタ対応機能
  - IIS + Java App Server を AJP で連携するための追加機能
- etc.

# 13. 弊社での他の構築実績

## ■ 私立大学さま

- 概要：学内システムのシングルサインオン環境を新規に構築
- ユーザ数：30,000ユーザ
- アプリケーション数：5システム
- エージェント型構成での実現

## ■ 住宅設備メーカーさま

- 概要：小規模向け商用認証基盤ソフトウェアからのリプレースを実施
- ユーザ数：2,000ユーザ
- アプリケーション数：2システム
- リバースプロキシ型構成での実現

## ■ …他にも複数のお客様で構築が進行中…

# ***ThemisStruct*** シリーズとは

オージス総研が提供する、

**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名です。**

## ■ ***Themis***

- テミス。ギリシャ神話上の法・掟の女神。「不変なる掟」との意味も。

## ■ ***Struct***

- ストラクチャ。構造。(IT)基盤の意味。

合わせてIT基盤上の掟(=ガバナンス、セキュリティ)を守るもの  
という意味を込めています。

# ***ThemisStruct*** シリーズラインナップ

■ ***ThemisStruct-IDM*** (IDentity Management)

ID管理ソリューション

■ ***ThemisStruct-WAM*** (Web Access Management)

アクセス管理ソリューション

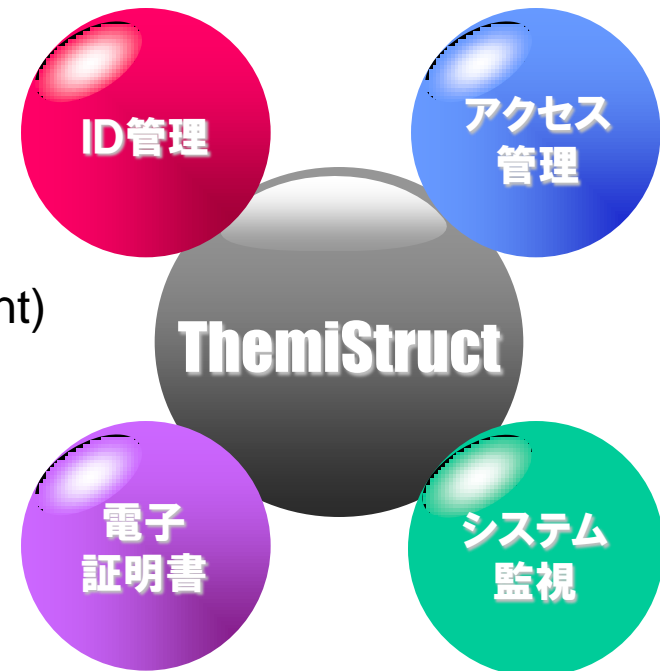
- ・ リバースプロキシ版
- ・ エージェント版

■ ***ThemisStruct-CM*** (Certificate Management)

電子証明書発行ソリューション

■ ***ThemisStruct-MONITOR***

システム監視ソリューション



# ThemisStruct シリーズ ソリューション概要

ソリューション名称	概要
<p>テミスストラクトーアイディエム  <b>ThemisStruct-IDM</b>                      IDentity Management</p>	<p><b>ID管理ソリューション</b>                      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、削除を自動化(プロビジョニング)する機能を提供。                      SalesforceやGoogle Appsへのプロビジョニングにも対応。</p>
<p>テミスストラクトーワム  <b>ThemisStruct-WAM</b>                      Web Access Management</p>	<p><b>アクセス管理ソリューション</b>                      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・利用が可能になるWebアプリケーションのシングルサインオン環境を提供。                      お客様の環境に合わせてリバースプロキシ版とエージェント版をご用意。                      SalesforceやGoogle Appsへのシングルサインオンにも対応。</p>
<p>テミスストラクトーシーエム  <b>ThemisStruct-CM</b>                      Certificate Management</p>	<p><b>電子証明書発行ソリューション</b>                      電子証明書を利用した、クライアント端末認証のための仕組みを提供。</p>
<p>テミスストラクトーモニター  <b>ThemisStruct-MONITOR</b></p>	<p><b>システム監視ソリューション</b>                      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、ログ監視をする機能を提供。                      クラウドサービスの安定稼働を実現するSOA基盤監視にも対応。</p>

# ***ThemisStruct*** が目指しているもの

必要な機能を厳選し、オープンソースソフトウェアを広範に利用することで  
それぞれのお客様に

**「フィットした価値」を「適正な価格」でご提供**

大阪ガスをはじめとし、複数の企業向け構築実績を基に、オープンソースソフトウェアをベースとして必要な機能を自社開発し、製品としてオージス総研が提供しています。

お客様の  
メリット

**ユーザ数に依存したライセンス費用・保守費用  
ではなく、一律の価格体系で利用できる**

**カスタマイズにも柔軟に対応できる**

**永く使っていただける**



# 14. まとめ

## ■ 認証基盤実現のねらい・メリット

- セキュリティリスクの軽減
- 開発コストの削減
- ユーザの利便性向上

## ■ 認証基盤の作り方・広げ方

- 認証基盤を作る
- 標準やガイドを作って、アプリケーションをつなぐ、集める
- 広げる、永く使い続ける

**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](mailto:info@ogis-ri.co.jp)