

認証技術、OpenAM、ThemiStruct

テ ミ ス ト ラ ク ト

これまでとこれから

株式会社オージス総研
サービス事業本部

八幡 孝

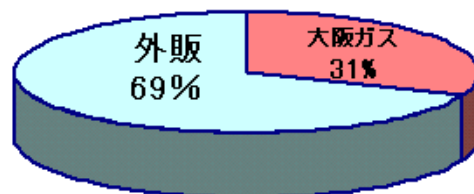
2014年2月7日



会社概要

株式会社オーガス総研

- 代表者: 代表取締役社長 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)
- 事業内容: システム開発、プラットフォームサービス、
コンピュータ機器・ソフトウェアの販売、
コンサルティング、研修トレーニング
- 主な事業所
 - 本 社: 大阪府大阪市西区千代崎3-南2-37 ICCビル
 - 東京本社: 東京都港区港南2-15-1 品川インターシティA棟
 - 名古屋オフィス: 愛知県名古屋市中区錦1-17-13 名興ビル
- 売上実績: 550億円(連結) 283億円(単体) (2012年度)
- 従業員数: 3,064名(連結) 1,268名(単体)
- 関連会社: 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、上海欧計斯软件有限公司(中国)
- オーガス総研グループ 売上構成比 (連結)



Design Your Energy 夢ある明日を



取得許可認定



我々はどこへ行くのか？

しっかりした基本構造

モデリング アーキテクチャ
オープンソース・ソフトウェア

変化への適応力

SOA、クラウドインテグレーション
アジャイル開発

持続可能な企業情報システムの実現

百年アーキテクチャ

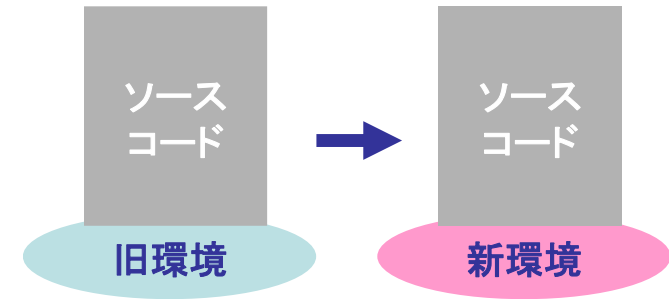
オープンソースソフトウェア

耐久性のある材料

なぜ耐久性があるのか？

ソースコードが公開

- 新環境へ移動可能
- カスタマイズ可能
- 使用継続可能



サポート打ち切り ベンダーロックイン

リスクからの開放

なぜ今オープンソースか？

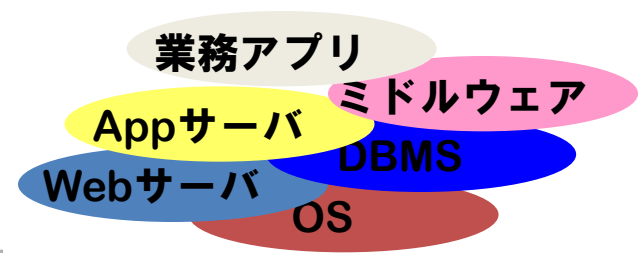
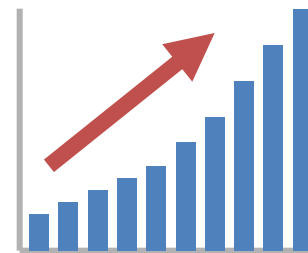
高価なライセンス料 バージョンアップ

質・量が飛躍的に向上

- 高機能、高品質
- あらゆるジャンル

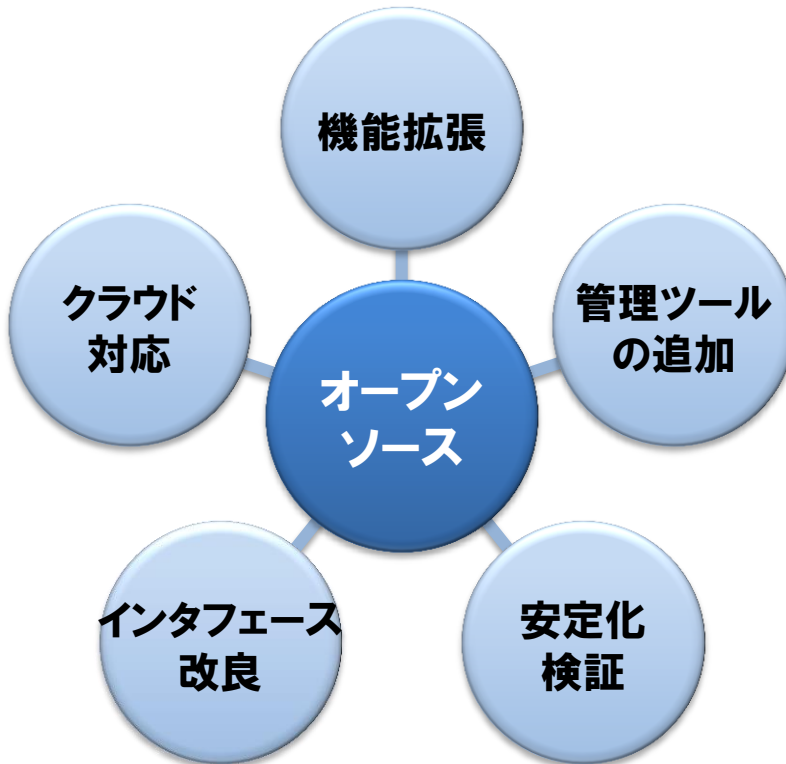
低コスト

- サポートは必要



ThemiStruct ラインナップ

テ ミ ス ト ラ ク ト



- **ThemiStruct-WAM** (OpenAM)
 - シングルサインオン認証基盤ソリューション
- **ThemiStruct-IDM** (OpenIDM)
 - ID管理ソリューション
- **ThemiStruct-CM** EJBCA
PKI BY PRIMEKEY
 - 電子証明書発行・管理ソリューション
- **ThemiStruct-OTP**
 - ワンタイムパスワードソリューション
- **ThemiStruct-WorkFlow**
 - 申請承認ワークフローソリューション
- **ThemiStruct-MONITOR** **ZABBIX**
 - システム監視ソリューション
- **ThemiStruct for Office365**
 - Microsoft Office365認証強化ソリューション

今日の話題

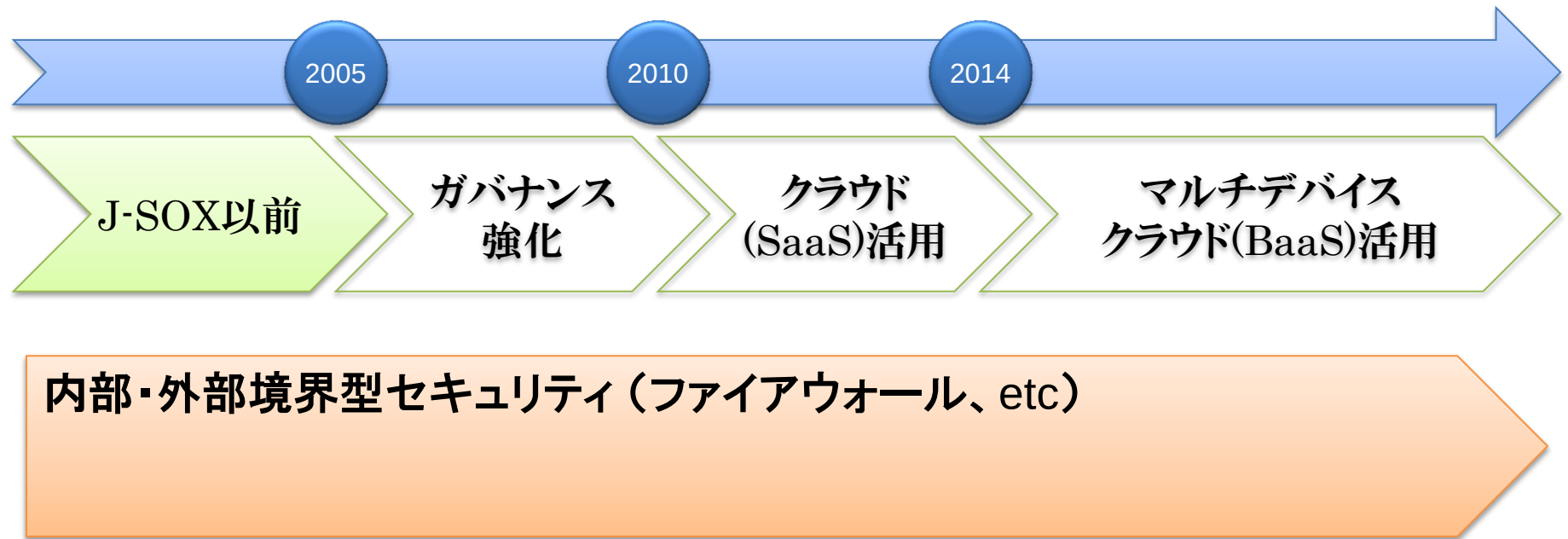
1. 認証技術の、これまでとこれから
2. オープンソースソフトウェアでいきましょう
(OpenAM & OpenIDM & etc.)
3. **ThemiStruct** テミストラクト でやってきたこと、やっていくこと

認証技術の、これまでとこれから

認証に関連するニーズの変遷

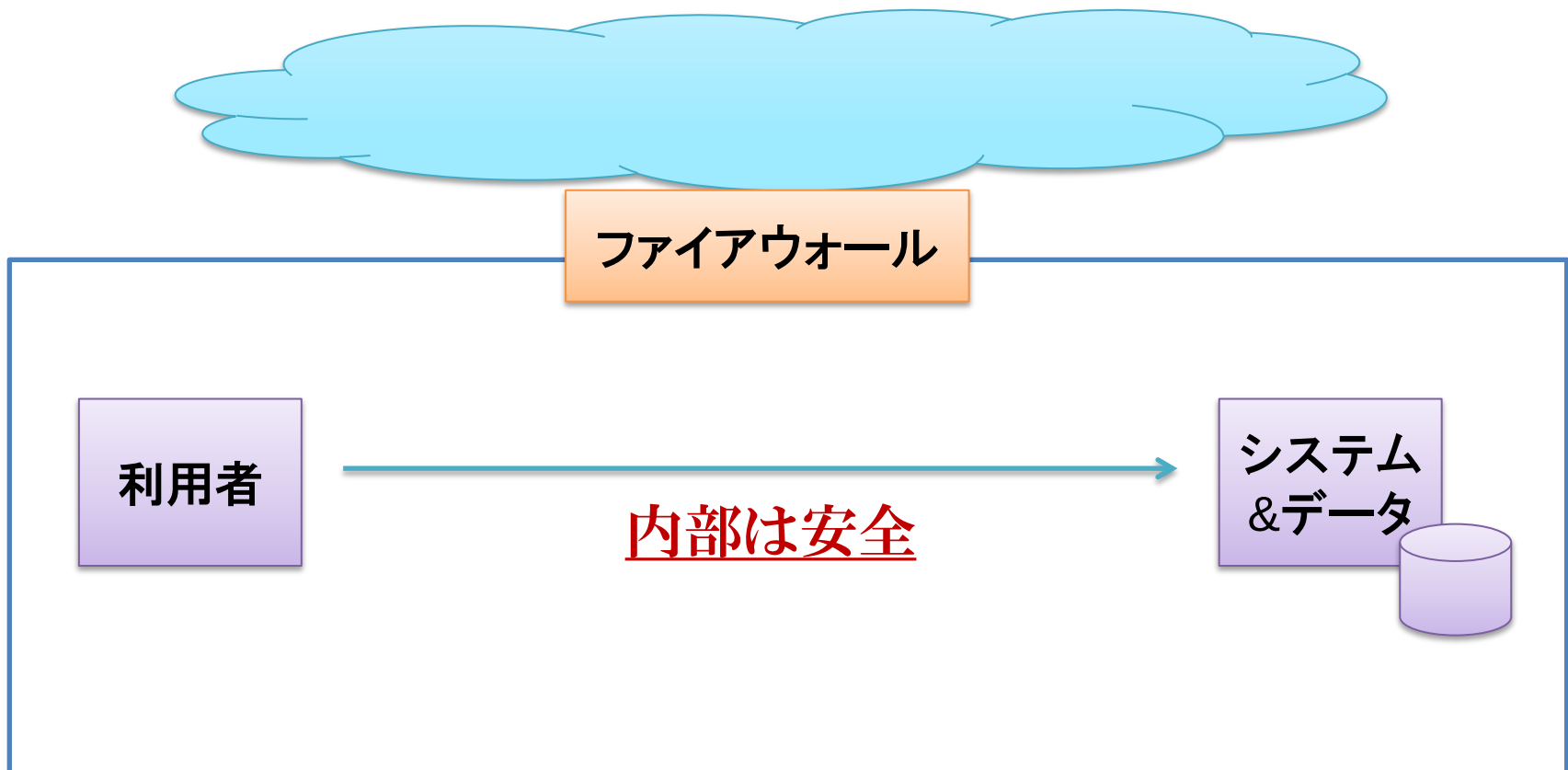


外部からの脅威に対応

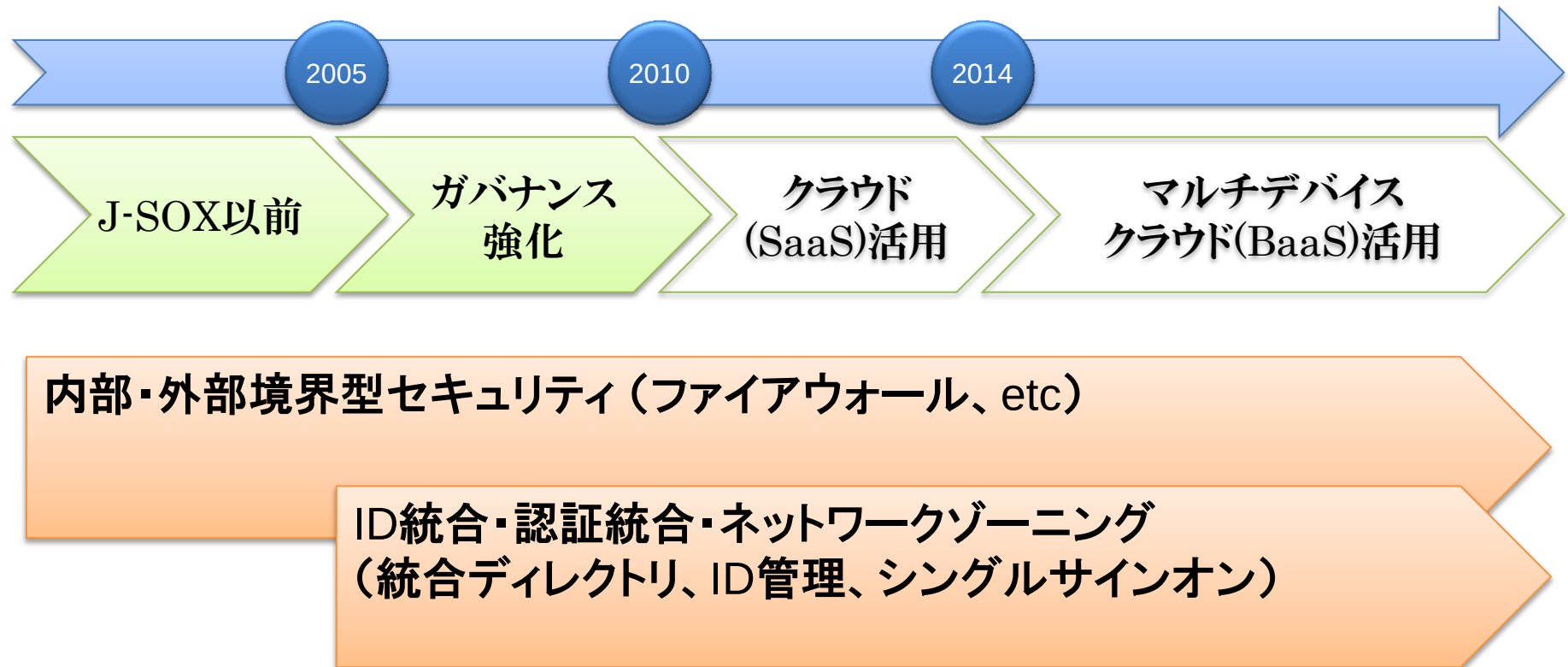


境界型セキュリティ

脅威は外部に



組織内でのガバナンス強化

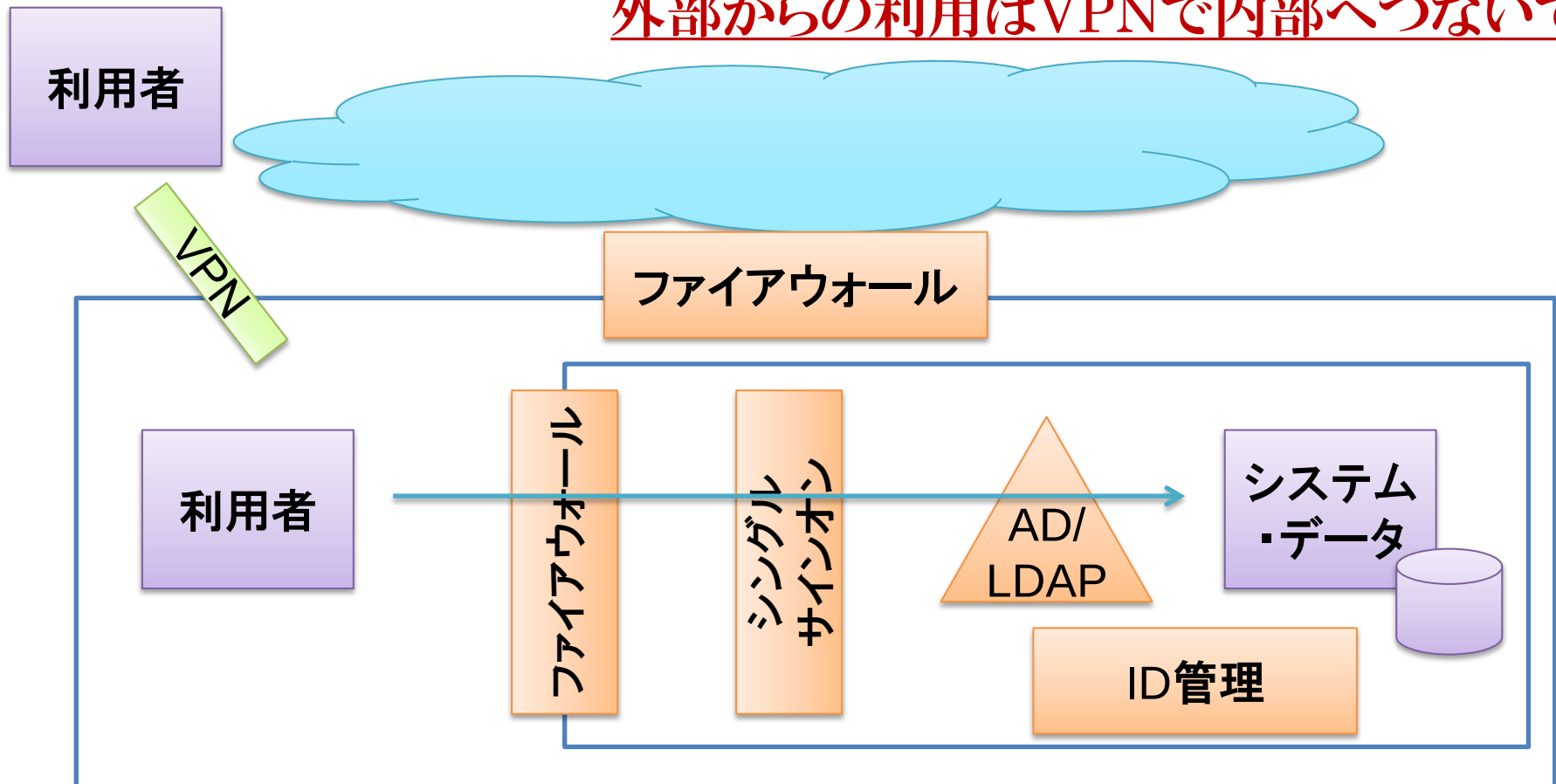


ID統合・認証統合・ネットワークゾーニング

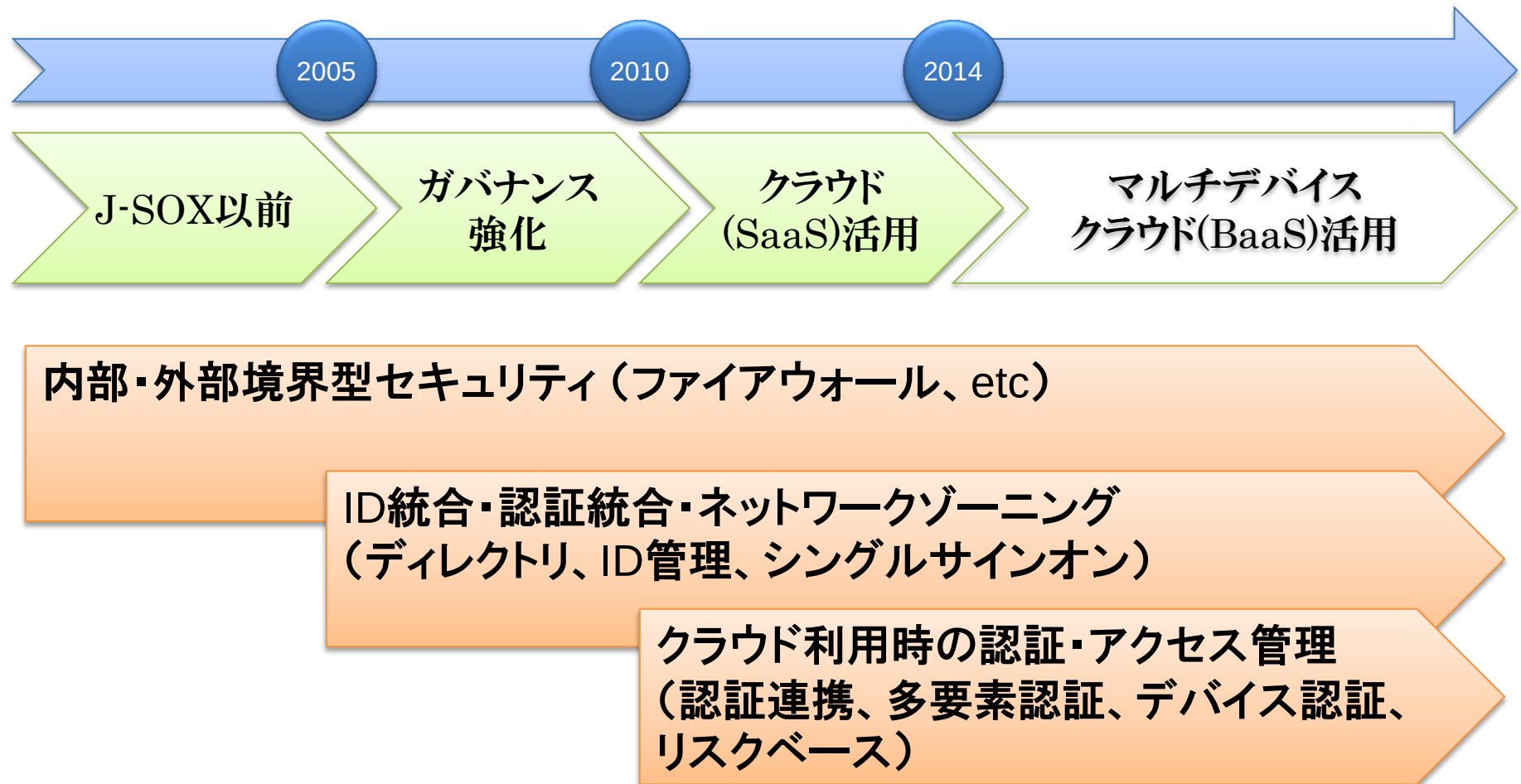
一般ゾーンとサーバーゾーンへの分離

ネットワーク層の制御と、認証で保護

外部からの利用はVPNで内部へつないで

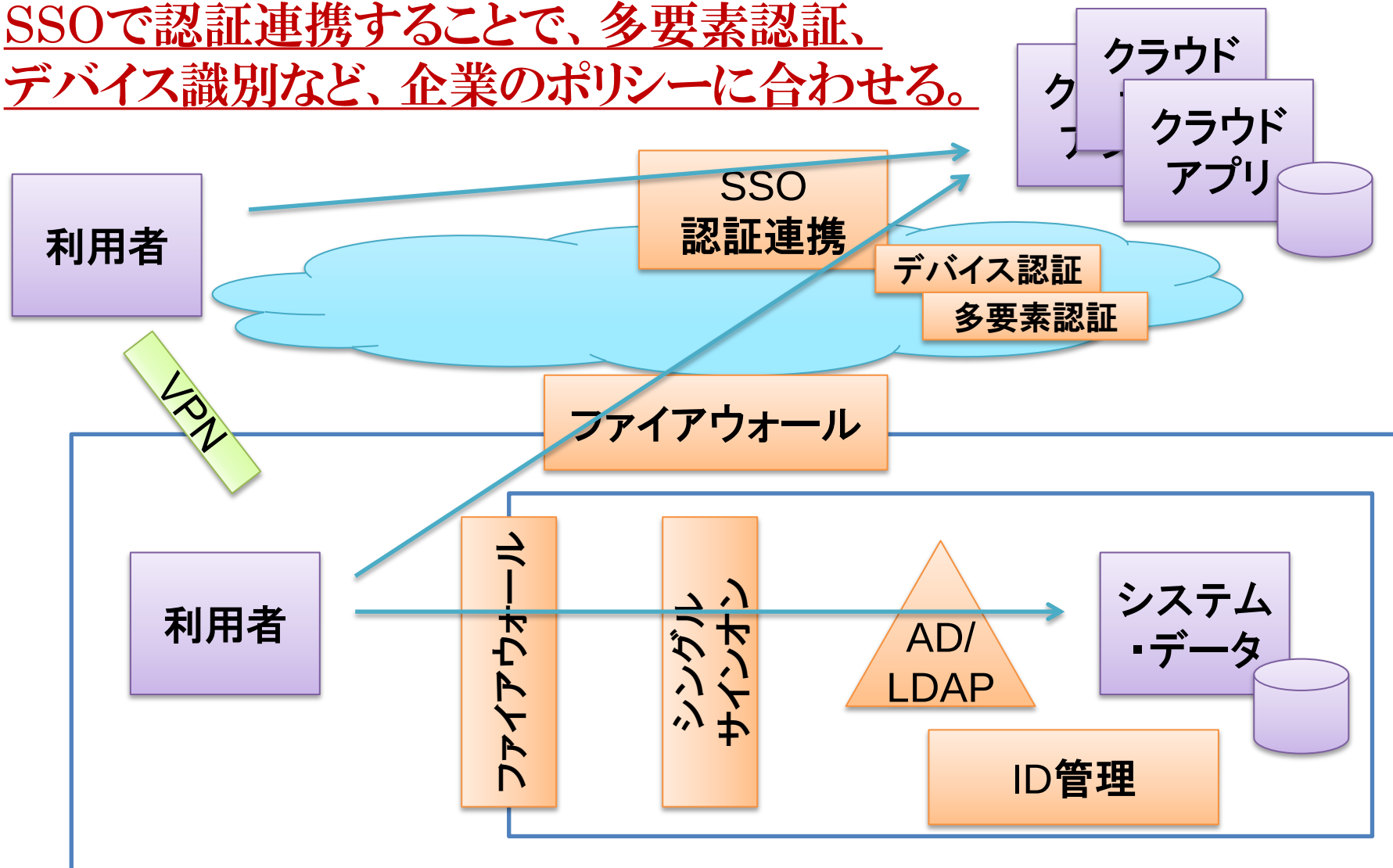


クラウド活用への対応



クラウド利用時の認証・アクセス管理

SSOで認証連携することで、多要素認証、デバイス識別など、企業のポリシーに合わせる。

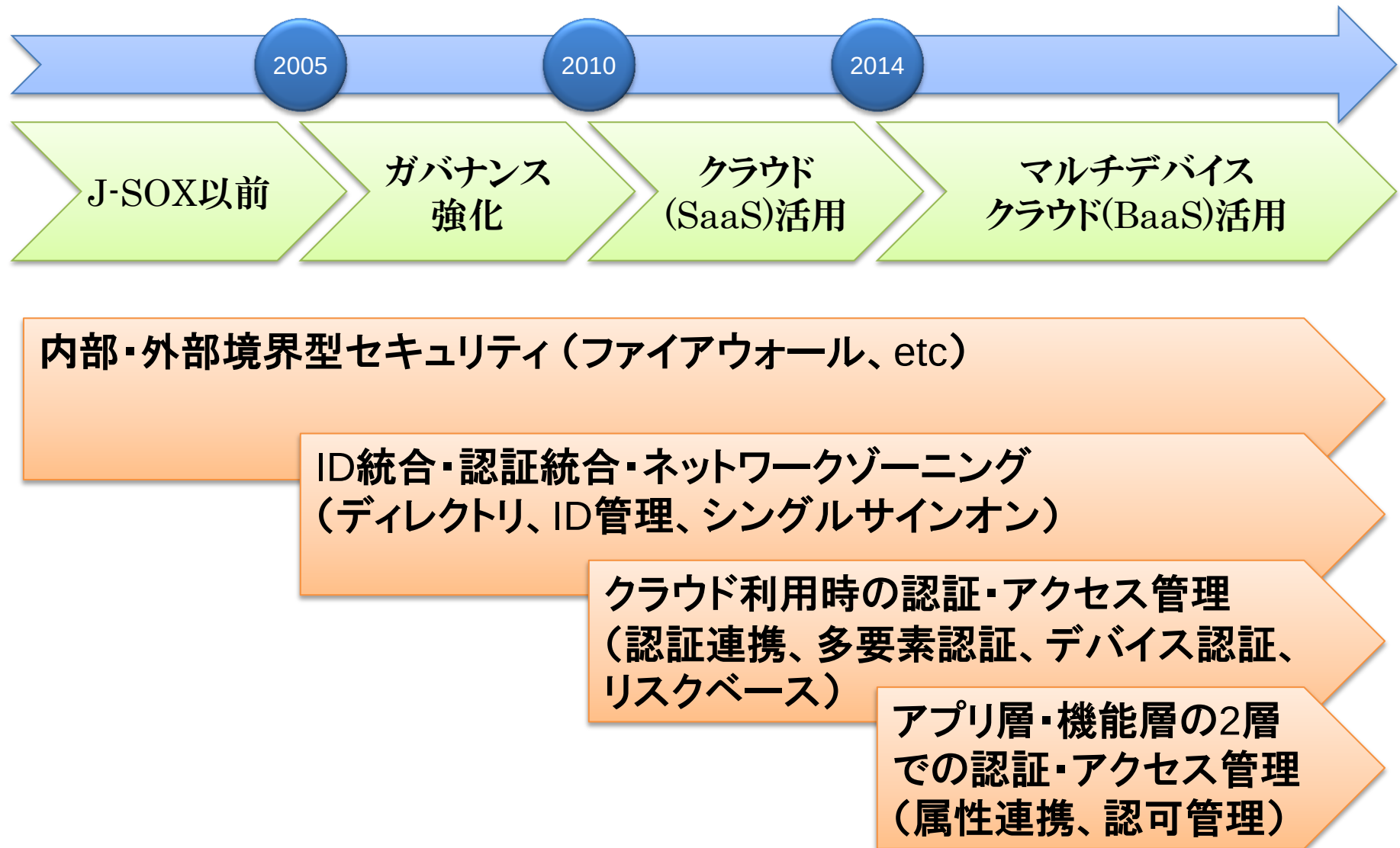


クラウド利用時の認証・アクセス管理

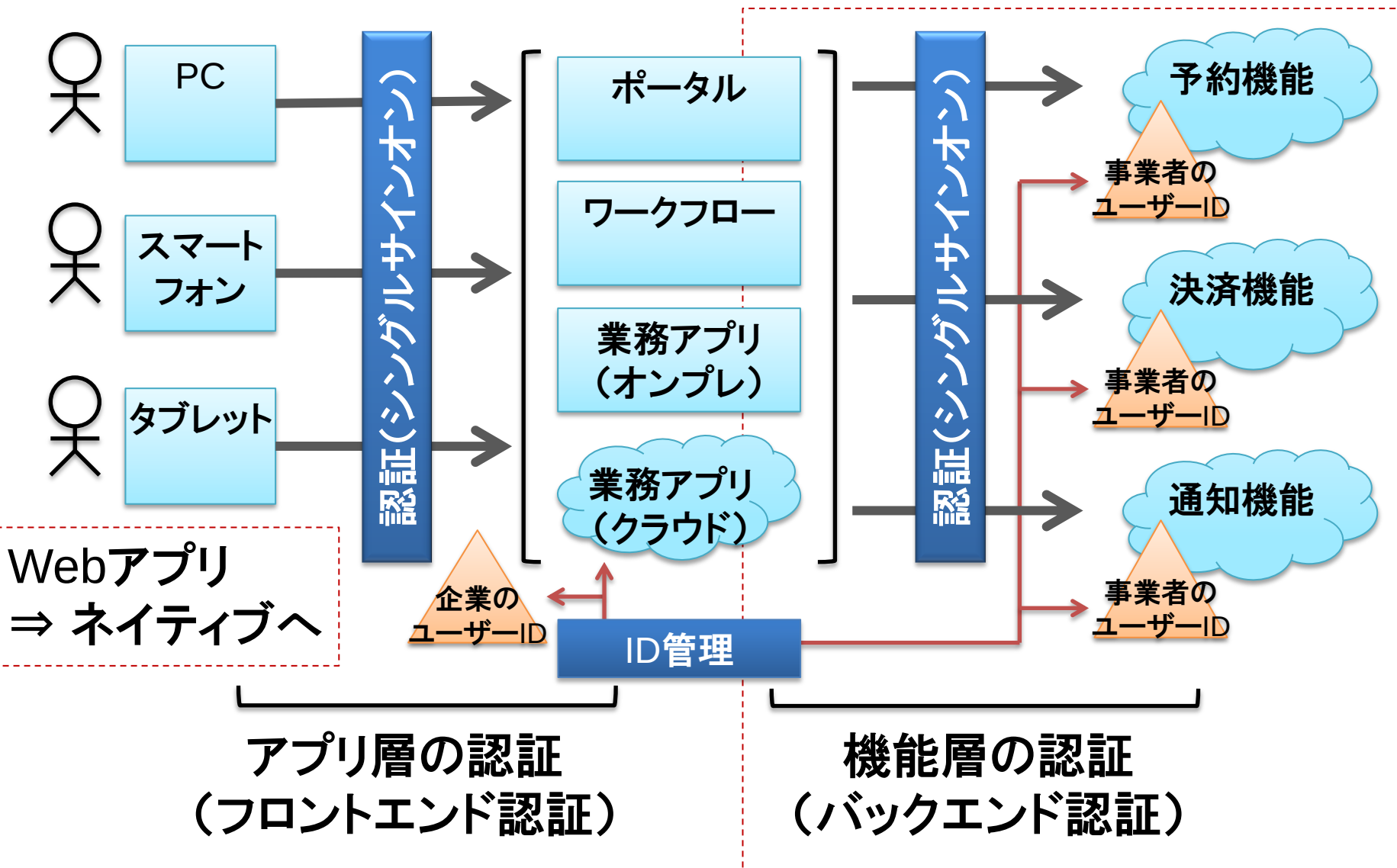
今までは境界型のセキュリティで守られた中で動いていた認証技術だったが・・・。
今では認証技術がセキュリティ境界となっている。

今後、認証基盤の重要性がいっそう高くなる。

このあとマルチデバイス・BaaS活用が進む



アプリケーションのアーキテクチャが変わる



アプリケーションのアーキテクチャが変わる

機能層の認証のための技術への対応が必要

- OAuth2.0, OpenID Connect, JIT Provisioning, SCIM, ...

アプリ層・機能層の透過的認証、アクセス権限の統制のための技術への対応が必要

- ... (これから何が来るか?)



これらの新技術に追従できる認証基盤の実現がエンタープライズでも求められる。

（フロントエンド認証）

（バックエンド認証）

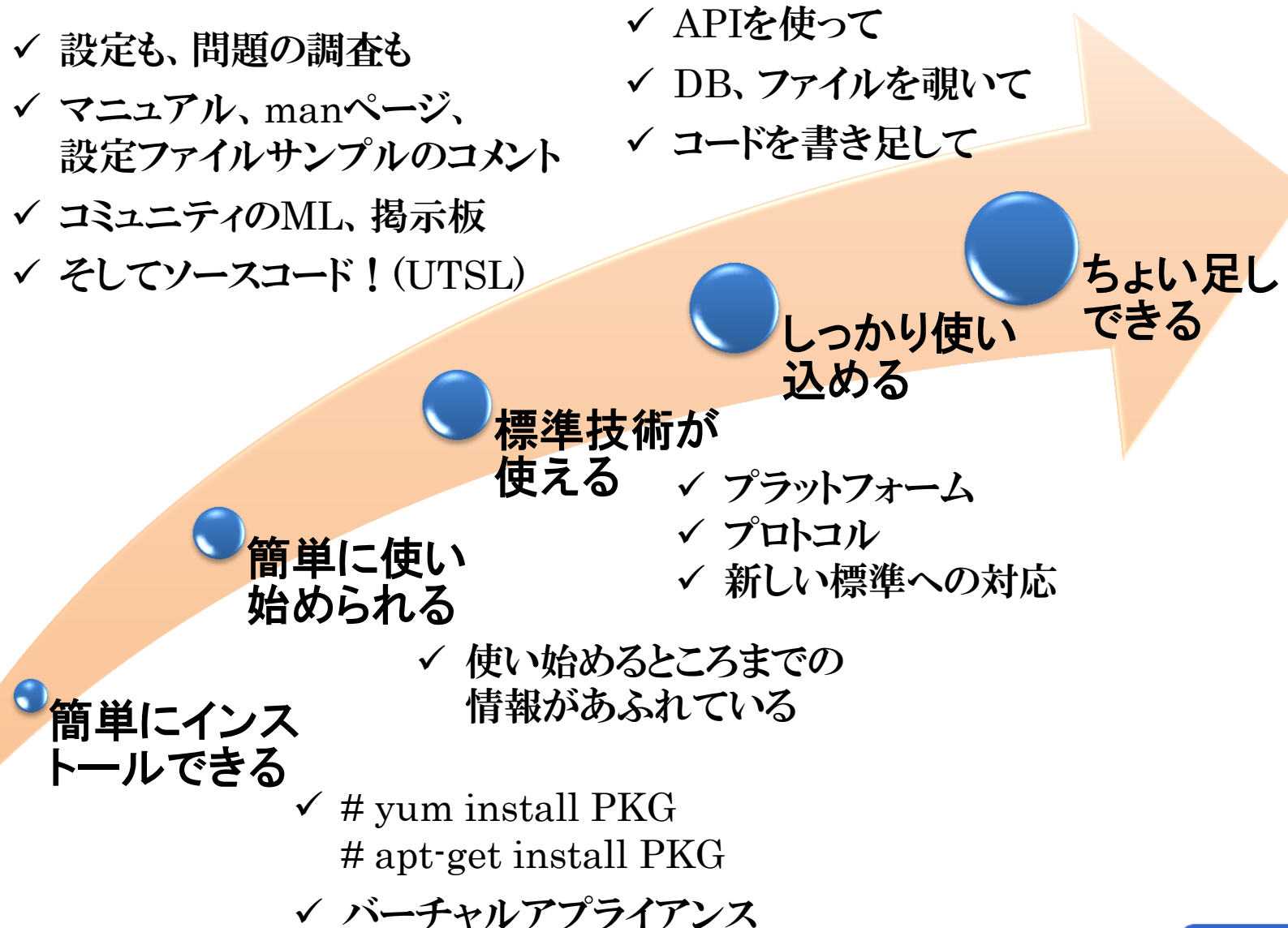
ここまでのまとめ

- 今後、認証基盤の重要性がいっそう高くなる。
- 新技術に追従できる認証基盤の実現がエンタープライズでも求められる。

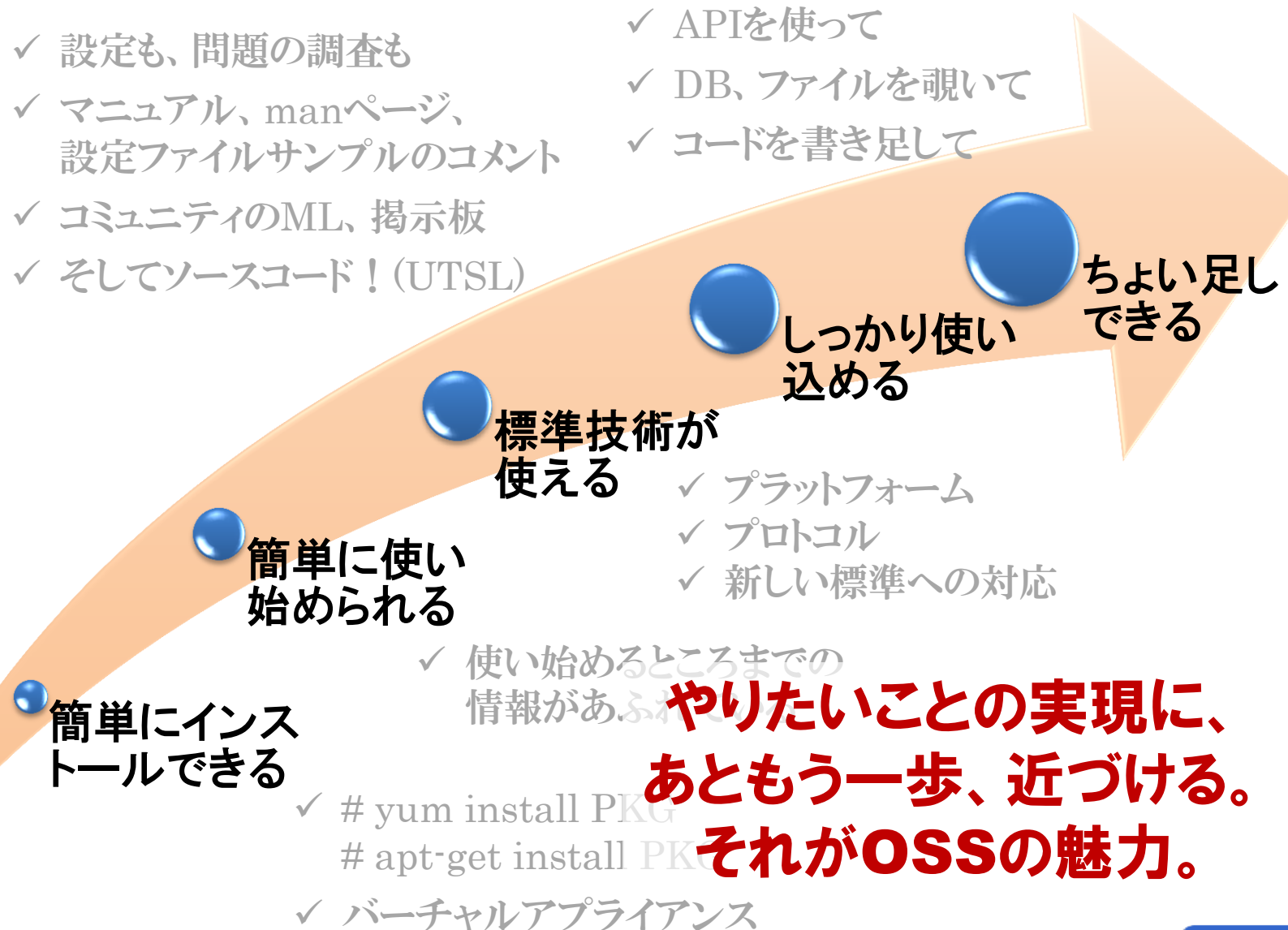
オープンソースソフトウェアで いきましょう

(OpenAM & OpenIDM & etc.)

なぜOSSを使ってきたのか？



OSS利用は魅力的選択



OpenAM & OpenIDM

- unified open source identity stack
- 新技術への追従
 - OAuth2, OpenID Connect, SCIM, ...
- OSSプロジェクトとして高いアクティビティ
- ソースコードへのアクセス
- コミュニティでのNightly buildの提供

ThemiStructで やってきたこと、やっていくこと

今日は3つほどご紹介

■ Case1: 簡単にはじめられるパッケージング

- Microsoft Office365 認証強化ソリューション
ThemiStruct for Office365 のパッケージング

■ Case2: ソースコードを使った問題調査と改善

- OpenAM冗長構成時の両系統障害発生事象の原因調査と改善 (**ThemiStruct-WAM**)

■ Case3: やりたいことにもう一歩近づく機能開発

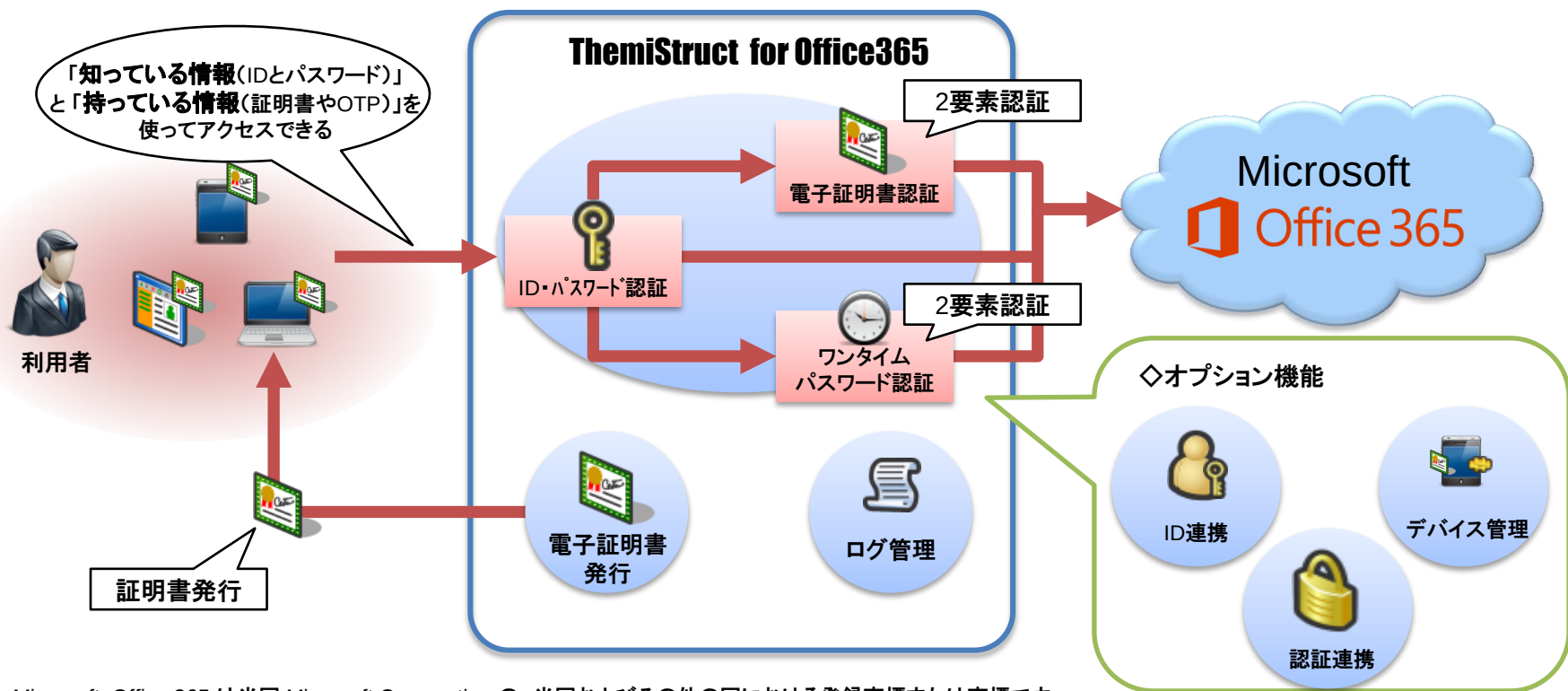
- Identity Integrated Interface & Self Service Interface for **ThemiStruct-IDM**

Case1: 簡単にはじめられるパッケージング

Office365をよりセキュアに利用するための認証強化ソリューション

ThemiStruct for Office365

ThemiStruct for Office365 はOffice365のID・パスワード認証に電子証明書認証やワンタイムパスワード認証を付加し、2要素認証を実現致します。さらに、これまで**ThemiStruct**シリーズで提供してきた電子証明書発行、デバイス管理、シングルサインオン、ID管理のテクノロジーを組合せ、Office365をより便利にご利用頂くことが可能です。



Microsoft, Office 365 は米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

Case2: ソースコードを使った問題調査と改善

■ 環境

- OpenAM認証サーバ冗長化（セッションフォワード、セッションレプリケーションあり）
- 冗長化されたリバースプロキシサーバ構成（Apache Policy Agent）

■ 起こったこと

- OpenAM認証サーバ1系にOSハングアップが発生
- OpenAM認証サーバ2系を使ってサービス続行
- OpenAM認証サーバ1系を再起動したところ、両系統のリバースプロキシサーバがサービス不能状態となる

Case2: ソースコードを使った問題調査と改善

■ アクティビティ

- 事象発生時に採取されたログとソースコードから挙動を想定、原因の絞込みを実施
- お客様にご協力いただき、3日間に及ぶ事象再現実験を実施（改めてご協力いただいたお客様に感謝）
- 得られたデバッグログから事象再現手順を確立
- 徹底した調査により Naming Service の処理に問題が潜んでいることを特定
- Naming Service のパッチを作成し問題を改善

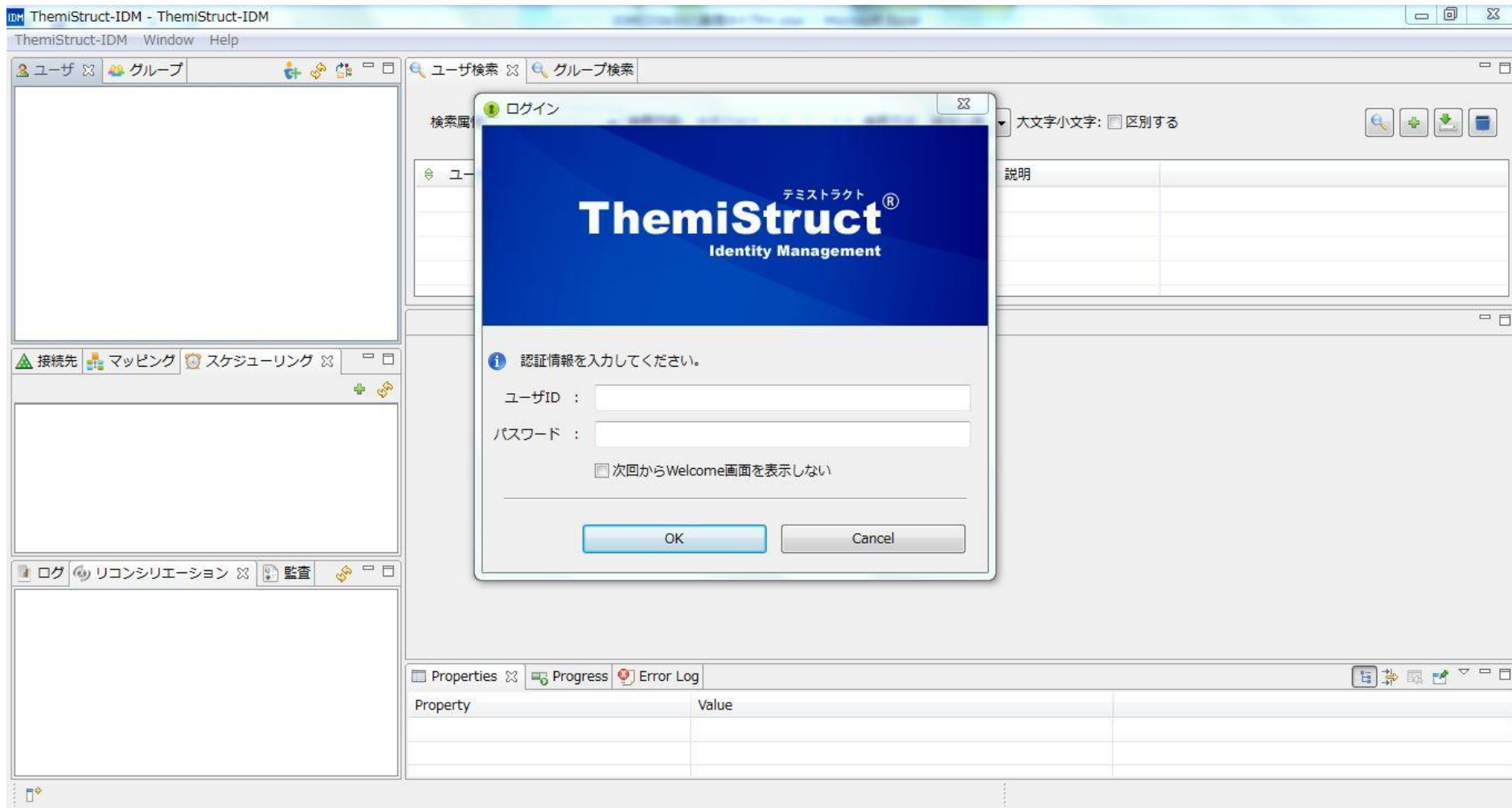
⇒ ソースコードのコントリビュートを準備中

Case3: やりたいことにもう一步近づく機能開発

- Identity Integrated Interface (III)
 - OpenIDMの設定 & ユーザー管理用UI
- Self Service Interface (SSI)
 - エンドユーザー & ID管理業務担当者をターゲットとしたWebUI
 - 日本でのUIカスタマイズ要望にお応えするべく
- OpenIDM の REST API を使うアドオンアプリケーションとして実装

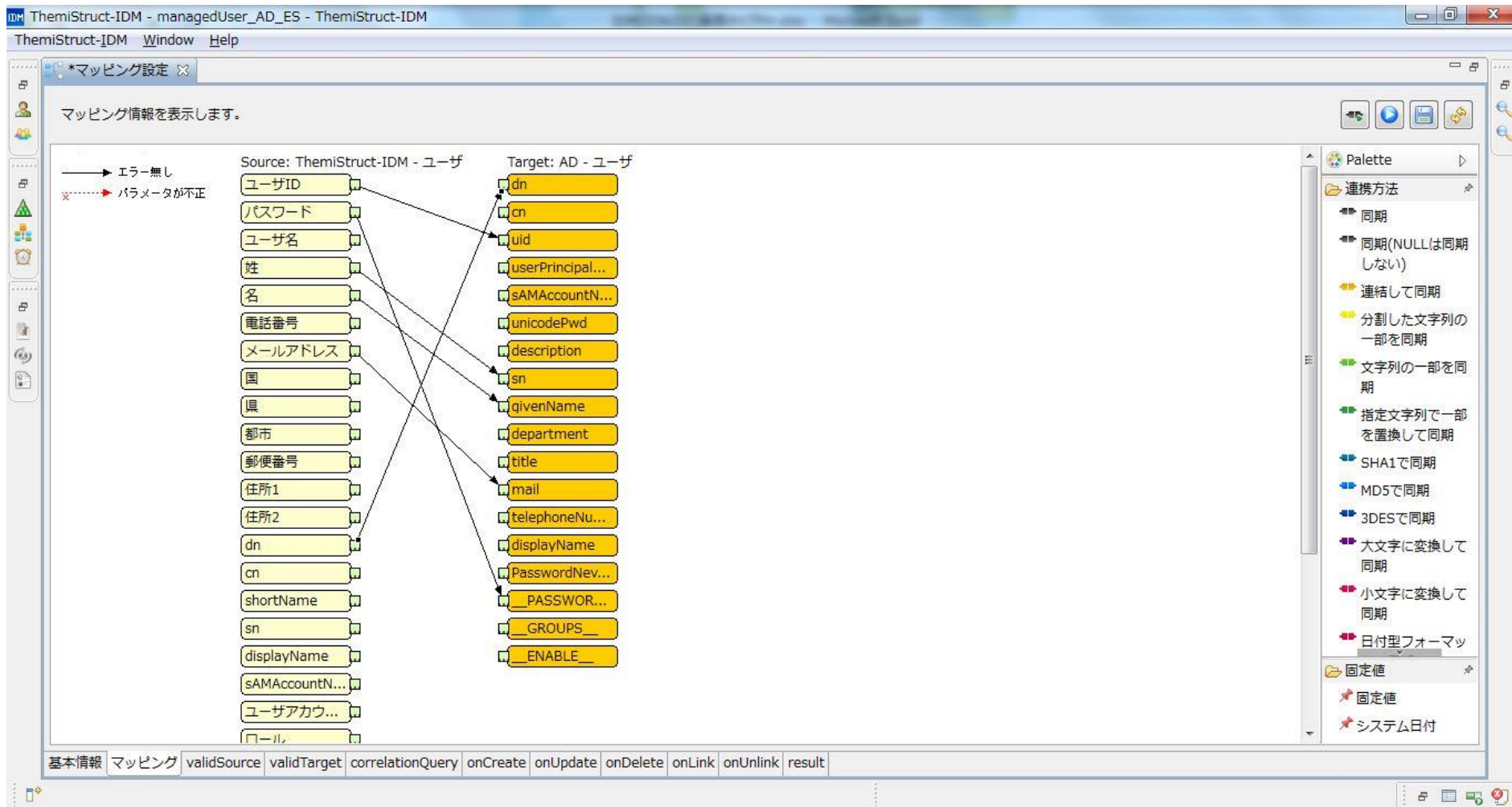
Identity Integrated Interface

Login window. Authenticated by OpenIDM via REST API.



Identity Integrated Interface

Mapping Editor can generate/update sync.json file.



Identity Integrated Interface

User Attribute Editor. Changed attributes are saved into OpenIDM.

ThemStruct-IDM - 000006 - ThemStruct-IDM

ThemStruct-IDM Window Help

ユーザ情報

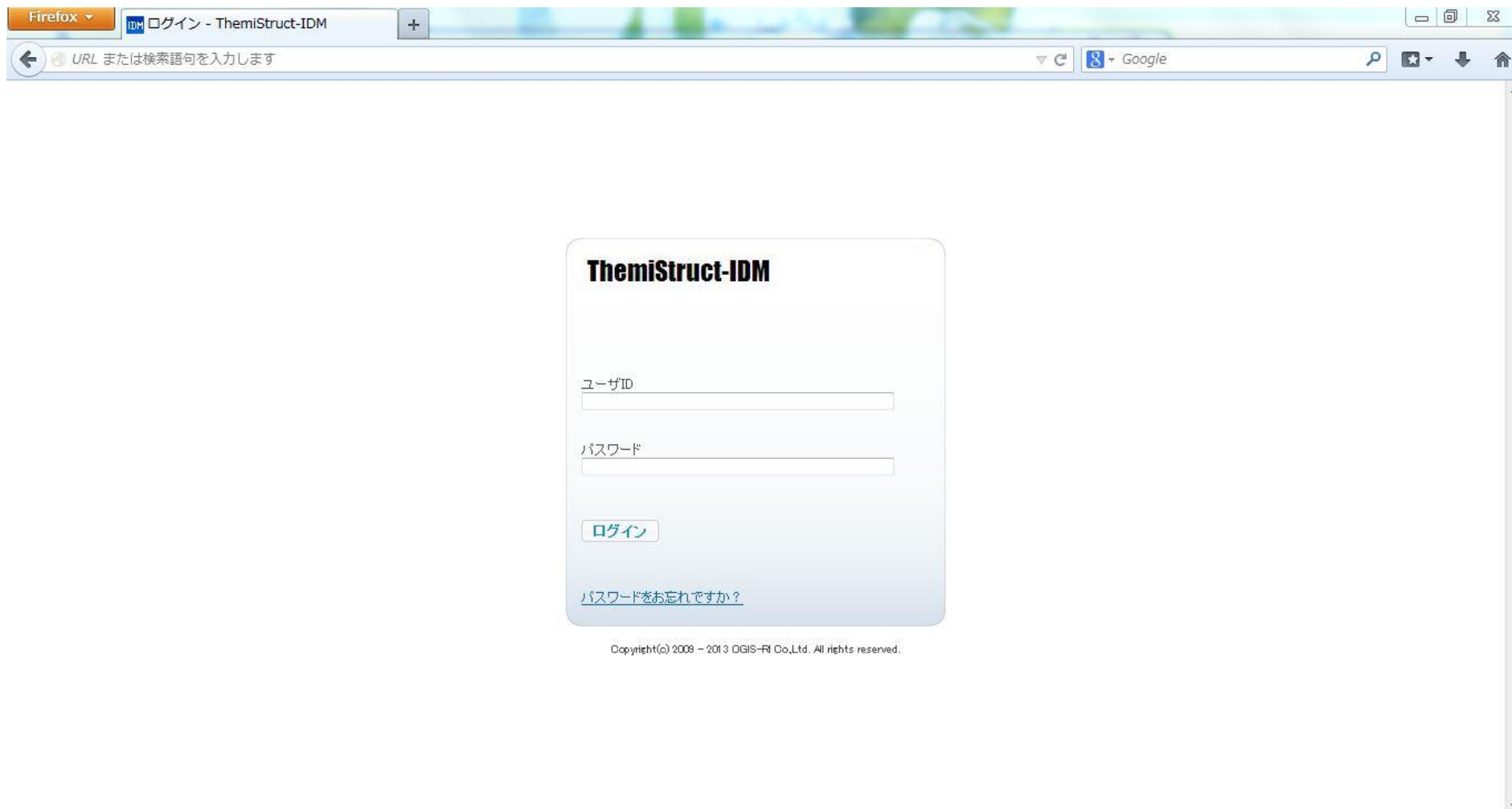
ユーザ情報を表示します。

属性	値
accountstatus	inactive
auth_cd_wq	021001
create_tmstamp	2013/07/08 12:51:11
dis_pry_gr	99999
disable_tmstamp	
email_alternate	
first_nm	haken49
first_nm_kj	派遣
first_nm_kn	ハケン
full_nm	haken49 ojisu
full_nm_jp	ojisu haken49
full_nm_kj	大路須 派遣
full_nm_kn	オジス ハケン
hon_adsgp	
hon_adsgp_disp	
hon_jnm_hr	
hon_scd_gr	
hon_scd_hr	
hon_scd_wq	
hon_snm_gr	
hon_snm_hr	
hon_snm_wq	
hon_ycd_gr	

基本情報 所属するグループ

Self Service Interface BETA

Login window. Authenticated by OpenIDM via REST API.



The screenshot shows a web browser window with the title "ログイン - ThemisStruct-IDM". The address bar contains the text "URL または検索語句を入力します". The main content area displays the "ThemisStruct-IDM" login form. The form includes two input fields: "ユーザID" (User ID) and "パスワード" (Password). Below these fields is a "ログイン" (Login) button. At the bottom of the form, there is a link that says "パスワードをお忘れですか?" (Forgot your password?). The footer of the page contains the text "Copyright(c) 2009 - 2013 OGIS-RI Co.,Ltd. All rights reserved."

Self Service Interface BETA

Users can maintenance their own password and attributes.

The screenshot shows a web browser window with the title "パスワード変更 - ThemiStruct-IDM". The address bar shows "URL または検索語句を入力します". The page header includes the "ThemiStruct-IDM" logo and navigation links: "ホーム", "パスワード変更" (selected), and "自身の情報".

The main content area is titled "パスワードポリシーについて" (About Password Policy) and lists the following rules:

- 文字数は8文字以上で入力してください。
- 半角数字、半角英小文字、半角英大文字、各1文字以上必ず含めてください。
- 以下の特殊文字は使用できません。
ダブルクォート「"」、カンマ「,」、円「¥」
- 現在設定されているパスワードと同じパスワードには変更することはできません。
- 自身のユーザID、姓(英字)、名(英字)を含めることはできません。

A red notice states: 次回PCログイン時は新しいパスワードが適用されます。

The password change form includes the following fields:

- 現パスワード * (Current Password): Masked with black dots, with a green checkmark icon.
- 新パスワード * (New Password): Empty, with a red X icon.
- 新パスワード(確認) * (New Password Confirmation): Empty, with a red X icon.

A "保存" (Save) button is located below the form fields.

Self Service Interface BETA

Security manager can create, edit and delete user accounts.

Firefox アカウント管理 - ThemiStruct-IDS

URL または検索語句を入力します

ThemiStruct-IDS

ホーム パスワード変更

ID統合管理システムに登録されているアカウント情報の編集を行います。

ユーザID: 000001 ユーザID: 000001 ログアウト

検索条件

- ☒ ユーザID
- ☒ 姓(漢字)
- ☒ 名(漢字)

検索

追加 更新 削除

アカウント一覧

ユーザID	氏名(漢字)
000001	大路須 総研

ユーザID: 000001

氏名(漢字): 大路須 総研

氏名(カナ): オオジス シウケン

氏名(英字): ogis soken

管理権限: システム管理者

アカウントステータス: 有効

メールアドレス: soken@ogis-ri.test

連絡先: 1234567

事業所名: 東京本社

組織名: 国際事業部

役職名: マネジャー

戻る 確認

これらの活動の成果を皆さんに！

- オージス総研、IT基盤ソリューション「**ThemiStruct**(R) (テミストラクト)」を大幅リニューアル (2014年1月28日)

実績のある
オープンソース
ソフトウェア



独自の機能拡張
や管理ツールの
追加



1,000項目以上の
徹底的なテストや
検証などを実施

継続的に実行可能な開発・テストプロセスを整備



お客様に安心してお使い
いただけるソフトウェアと
サポートをご提供



開発コミュニティへ
バグフィックス等の成果を
フィードバック

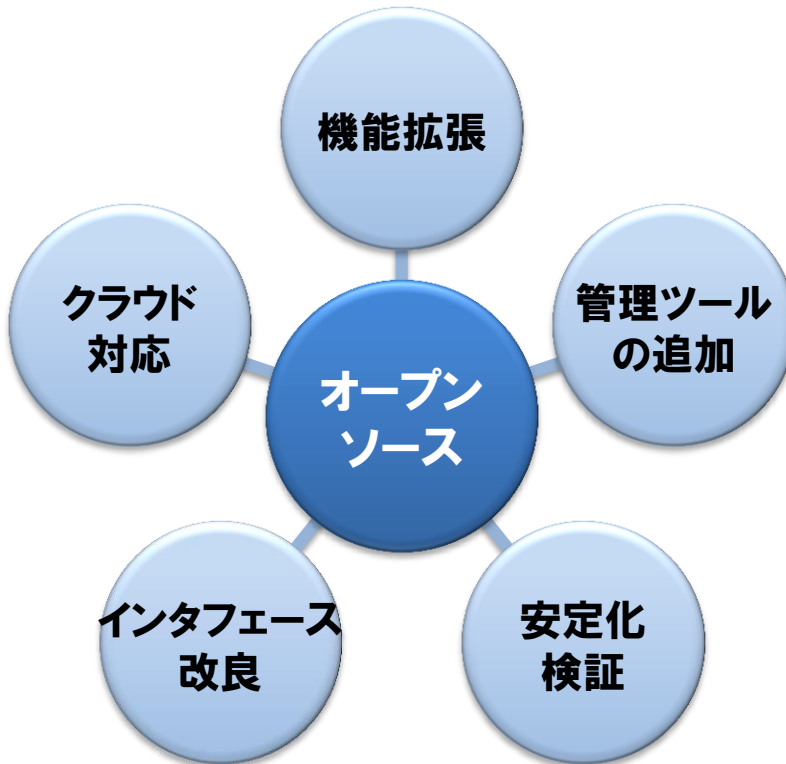
2013年度のアクティビティ

- オージス総研、IT基盤ソリューション「**ThemiStruct**(R) (テミストラクト)」を大幅リニューアル (2014年1月28日)
- Microsoft Office365 認証強化ソリューション、「**ThemiStruct**(R) (テミストラクト)-**WAM/CM for Office365**」の販売開始。(2013年10月16日)
- 認証強化ソリューション「**ThemiStruct-CM/OTP**」を仮想アプライアンスで提供開始(2013年9月19日)
- 「**ThemiStruct-MONITOR**」(運用監視ソリューション) 拡販のため、コアソフト開発元Zabbix社とパートナー契約を締結しました。(2013年5月15日)
- 「**ThemiStruct-CM**」(電子証明書発行ソリューション) 拡販のため、コアソフト開発元PrimeKey社と日本初のパートナー契約を締結しました。(2013年5月15日)

<http://www.ogis-ri.co.jp/pickup/themistruct/>

ThemiStruct ラインナップ

テ ミ ス ト ラ ク ト



- **ThemiStruct-WAM** (OpenAM)
 - シングルサインオン認証基盤ソリューション
- **ThemiStruct-IDM** (OpenIDM)
 - ID管理ソリューション
- **ThemiStruct-CM** EJBCA
PKI BY PRIMEKEY
 - 電子証明書発行・管理ソリューション
- **ThemiStruct-OTP**
 - ワンタイムパスワードソリューション
- **ThemiStruct-WorkFlow**
 - 申請承認ワークフローソリューション
- **ThemiStruct-MONITOR** **ZABBIX**
 - システム監視ソリューション
- **ThemiStruct for Office365**
 - Microsoft Office365認証強化ソリューション

ThemiStruct ラインナップ

プロダクト		コアOSS	概要
認証ソリューション	シングルサインオン認証基盤ソリューション ThemiStruct-WAM テミストラクト ワム	OpenAM	Webアプリケーションの統合認証 - リバースプロキシ型とエージェント型の両方式に対応可能 - クラウドサービスへのシングルサインオンにも対応
	ID管理ソリューション ThemiStruct-IDM テミストラクト アイディーエム	OpenIDM	アカウント情報を一元管理するID管理 クラウドサービスへのプロビジョニングにも対応
	電子証明書発行・管理ソリューション ThemiStruct-CM テミストラクト シーエム	 EJBCA PKI BY PRIMEKEY	電子証明書を利用したプライベート端末認証 - 外部認証局方式と比較して安価で必要十分なセキュリティ - スマートフォンやタブレットなど外部からアクセスする端末の増加に対応可能
	ワンタイムパスワードソリューション ThemiStruct-OTP テミストラクト オーティーピー	Google Authenticator	端末IDから生成するワンタイムパスワードを発行 スマートフォンやタブレットなどを利用したソフトウェアトークン方式なので、専用ハードウェア方式と比較して低コストかつ容易な維持管理が可能
申請承認ワークフローソリューション ThemiStruct-WorkFlow テミストラクト ワークフロー		jBPM	必要かつ十分な機能を備えたワークフロー 申請書(フォーム)と経路(フロー)が担当者と自由にデザインできるエンジンを標準装備
システム監視ソリューション ThemiStruct-MONITOR テミストラクト モニター		 ZABBIX	システム監視 - サーバや仮想基盤における稼働(死活、プロセス、サービスログなど)やパフォーマンスの監視が可能 - リアルタイムの統計や履歴データへのアクセスが可能
Microsoft Office365認証強化ソリューション ThemiStruct for Office365 テミストラクト フォー オフィス365		—	Microsoft Office365認証強化 ThemiStruct-WAMおよびCMを活用し、Office365のセキュリティ(認証機能)を強化するための多要素認証を低コストで実現

ThemiStruct ラインナップ

テ ミ ス ト ラ ク ト

ThemiStruct で提供する3つのサービス

テ ミ ス ト ラ ク ト

テクニカルサポート サービス

- 利用方法等の問合せに回答
- 障害時の調査
- 回避策や代替案の提示
- 復旧の技術支援

プロフェッショナル サービス

- 要件実現方法の相談、回答
- PoC、技術検証の支援
- 自社で実施する開発、構築の技術支援

SIサービス

- お客様の要求に応じたシステムの実現を責任を持ってお引受け

当社サービスの活用事例

顧客(業種)	提供サービス	ユーザー数	実施内容	プロダクト
インフラ	SIサービス	約20,000	・グループ認証基盤構築 (商用製品からオープンソースへの移行)	WAM
インフラ	SIサービス	数万	・取引先向け電子証明書発行	CM
インフラ	SIサービス	数万	・顧客向けポータルID管理	IDM/WAM
文教	SIサービス	約30,000	・教員・学生向けWeb-SSO基盤構築	WAM
製造	SIサービス	約2,000	・EDI向けユーザー認証システム構築	WAM/CM
製造	SIサービス	約20,000	・B2Bシステム用Web-SSO/ID管理 ・認証基盤の構築	WAM/IDM
製造	SIサービス	約17,000	・全社統合ID基盤の構築 (既存のID管理システムの連携部分をThemiStruct-IDMでリプレイス)	IDM
インフラ	SIサービス	約5,000	・グループ共用Web-SSO/証明書発行 ・認証基盤の構築	WAM/CM
文教	SIサービス	約16,000	・教員・学生向けシステム向け ・統合ID管理基盤の構築 ・サーバ、NW機器監視基盤の構築	IDM/MONITOR
金融	SIサービス	約20,000	・基幹業務システム再構築に伴う、グループ共通認証基盤の構築	IDM/WAM /WorkFlow
製造	SIサービス	約200	・B2Bシステム向け電子証明書発行基盤の構築	CM
金融	SIサービス	約5,000	・電子証明書発行基盤の構築	CM
インフラ	SIサービス	約8,000	・BPO進捗管理システムとして新設 ・社内電子決裁システムリプレイス ・グループ企業横断決裁フローを実現	WorkFlow
サービス	SIサービス	約1,500	・社内向けID管理システム構築	IDM
製造	SIサービス		・社内SSOリプレイス	WAM
公共	SIサービス	約3,000		CM
サービス	SIサービス	約7,000	・派遣登録者向けポータルシステムのためのSSO基盤構築	WAM
製造	SIサービス	約1,500	・ID管理とSSOの実現。大手商用パッケージを使用していたが、 管理が常駐パートナー依存のため、それを改善。	IDM/WAM
製造	SIサービス	監視約80台	・大手商用パッケージからのリプレイス。監視システム構築。	MONITOR

当社サービスの活用事例

顧客(業種)	提供サービス	ユーザー数	実施内容	プロダクト
流通	SIサービス	約4,000 監視約10台	・MONITORは大手商用パッケージからのリプレース。 ・全部署及びグループ向けの決裁システムのエンジン ・電子決裁システムリプレース(SAP連携)	MONITOR/WorkFlow
マスコミ	SIサービス		・ポータルへの導入がトリガー(社外からアクセス出来ず) ・大手商用パッケージからのリプレース	WAM
製造	SIサービス	監視約150台	・大手商用パッケージからのリプレース。監視システム構築。	MONITOR
製造	プロフェッショナルサービス		・ワールドワイドの製造拠点のSSO/ID管理共通基盤の構築にOpenAM、ThemiStruct-IDMを利用 ・企画、検証、導入支援 ・WAM/IDMサポートサービス提供	WAM/IDM
公共	プロフェッショナルサービス		・自治体のシステムのOSS化に伴い、OSSサポートの依頼を受けたOSSサポートサービス提供	OSS全般
製造	プロフェッショナルサービス		・Liferayを使ったB2B2Cポータルシステムの構築における技術支援	Portal
製造	プロフェッショナルサービス		・Liferay(ポータル)、OpneAM(シングルサインオン)の導入・設定支援サポートサービス提供	Portal/WAM
製造	プロフェッショナルサービス		・OpenAMの導入設定支援	WAM
流通	プロフェッショナルサービス		・ESBを利用した認証システム連携機能開発の技術支援	WAM
製造	プロフェッショナルサービス		・グループ共用のID管理システムの企画検討支援	IDM
インフラ	プロフェッショナルサービス		・病院システム用の認証システムとしてOpenAMを採用 ・システムの導入設定技術支援	WAM
製造	プロフェッショナルサービス		・将来3,000台規模の監視を行なう為のサーバ構築設計支援	MONITOR

まとめ

- 今後、認証基盤の重要性がいっそう高くなる。
- オージス総研では **ThemiStruct** で OpenAM & OpenIDM 向けのサービスをご提供。
テ ミ ス ト ラ ク ト
- お客様に安心していただけるソフトウェアとサポートの提供を提供していきます。

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
ソリューション営業部

TEL 03-6712-1201

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