OpenAM これまでとこれから

2015/07/17

野村総合研究所　　田中　穣

株式会社 野村総合研究所 オープンソースソリューション推進室

Mail：ossc@nri.co.jp　　Web：http://openstandia.jp/

NRIのオープンソースに関する沿革

年	ＮＲＩの主なオープンソースへの取り組み
2003年	オープンソース専門組織の立ち上げ
2004年	JBoss.Inc, MySQL ABとパートナー契約締結
2005年	オープンソースサポートサービス OpenStandia を発表
2006年	OpenStandiaパートナープログラムの提供開始
2007年	２４時間以内に対応　オープンソース救急サービスの提供開始
2008年	企業情報ポータル OpenStandia/Portalの提供開始 オープンソースシングルサインオン OpenSSOのサポートを提供開始 オープンソースビジネス推進協議会（ＯＢＣＩ）を発起
2010年	シングルサインオン＆ＩＤ管理　OpenStandia/SSO&IDMの提供開始 Jaspersoftとのパートナー契約締結
2012年	オープンソースのバージョンアップ情報を無償公開 ビジネスアプリケーション OpenStandia/Bizの提供開始
2013年	オープンソースＩＤ管理　OpenIDMのサポートを提供開始 Alfresco Software, Ltdとパートナー契約締結 オープンソース24H365Dサポートサービスの開始 MongoDB.incとパートナー契約締結
2014年	ForgeRock.Inc.とのパートナー契約締結

1. SSOが求められる背景

2. SSO導入のポイントと事例

3. これまでのOpenAM

4. これからのOpenAM

シングルサインオン(SSO)・統合ID管理(IDM)に関する環境変化

近年さまざまな環境変化により、企業内システム利用の在り方、及びそれに基づくＩＤ管理の在り方、認証の仕組みが見直されてきています。

社内環境の変化

- システム、ユーザアカウント、権限の複雑化
- 内部統制・コンプライアンス・個人情報保護の強化
- 採用形態の複雑化（グローバル人材、アウトソース、出向等）

ＩＴ環境の変化

- クラウド時代の到来による「所有」から「利用」への流れ
- 社内システムのＳａａＳ利用
- モバイル端末、スマートフォン、タブレットの利用拡大

事業環境の変化

- グローバル化
- Ｍ＆Ａ、企業合併によるグループ企業の統廃合
- 新規サービス事業の開始

社内システムに統合認証基盤（SSO&IDM）を導入するメリット

企業内ＳＳＯ＆ＩＤＭが求めれる具体的要因の多くは下記に分類（もしくは複合的要因）されます。

レ 既存システム・クラウド・Ｓａａｓとの認証・認可連携

- 新規導入するSaaSと既存の社内システムを連携し、ＩＤ／ＰＷ及び認証を一本化（ＳＳＯ）
- 組織改編、人事発令によるシステムの組織・ＩＤ変更対応を自動化（ＩＤＭ）

レ モバイル端末・スマートフォンからのシステム利用

- 外出先の営業メンバがモバイル端末・スマートフォンで社内システム利用
- ビジネスをより便利に、よりセキュアに、よりスピーディに

レ グローバル対応（統合 × ローカライズ）

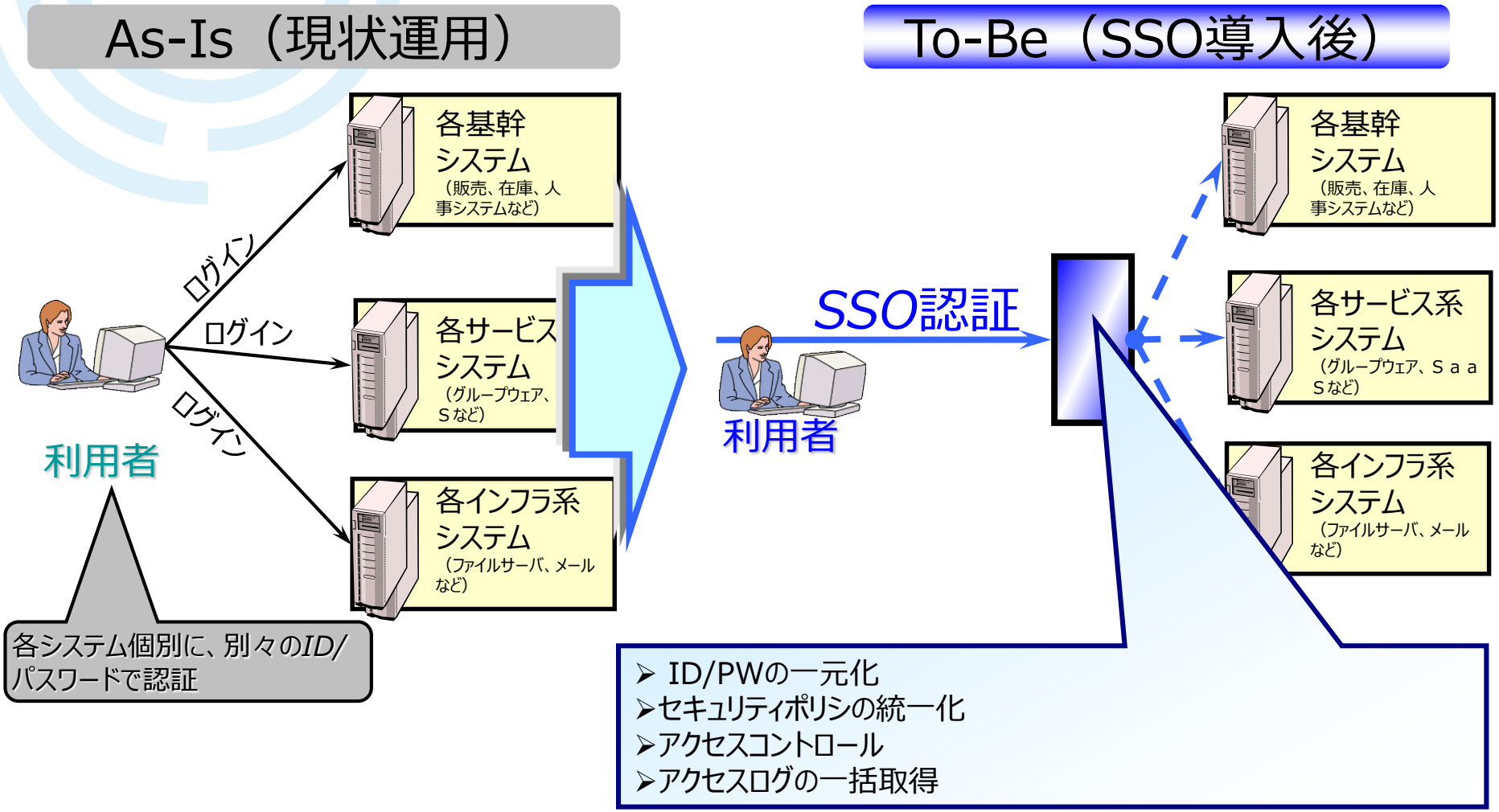
- グローバル拠点のシステム、ＩＤライフサイクルを統一的に管理
- ローカルサービス、ローカルパッケージとのＩＤ連携

レ 内部統制強化、運用コスト削減

- IDライフサイクル管理、ワークフロー、適切な認証・認可管理、監査ログ保存
- 手作業によるID管理業務を自動化。現場からの対応要望にスピーディに対応

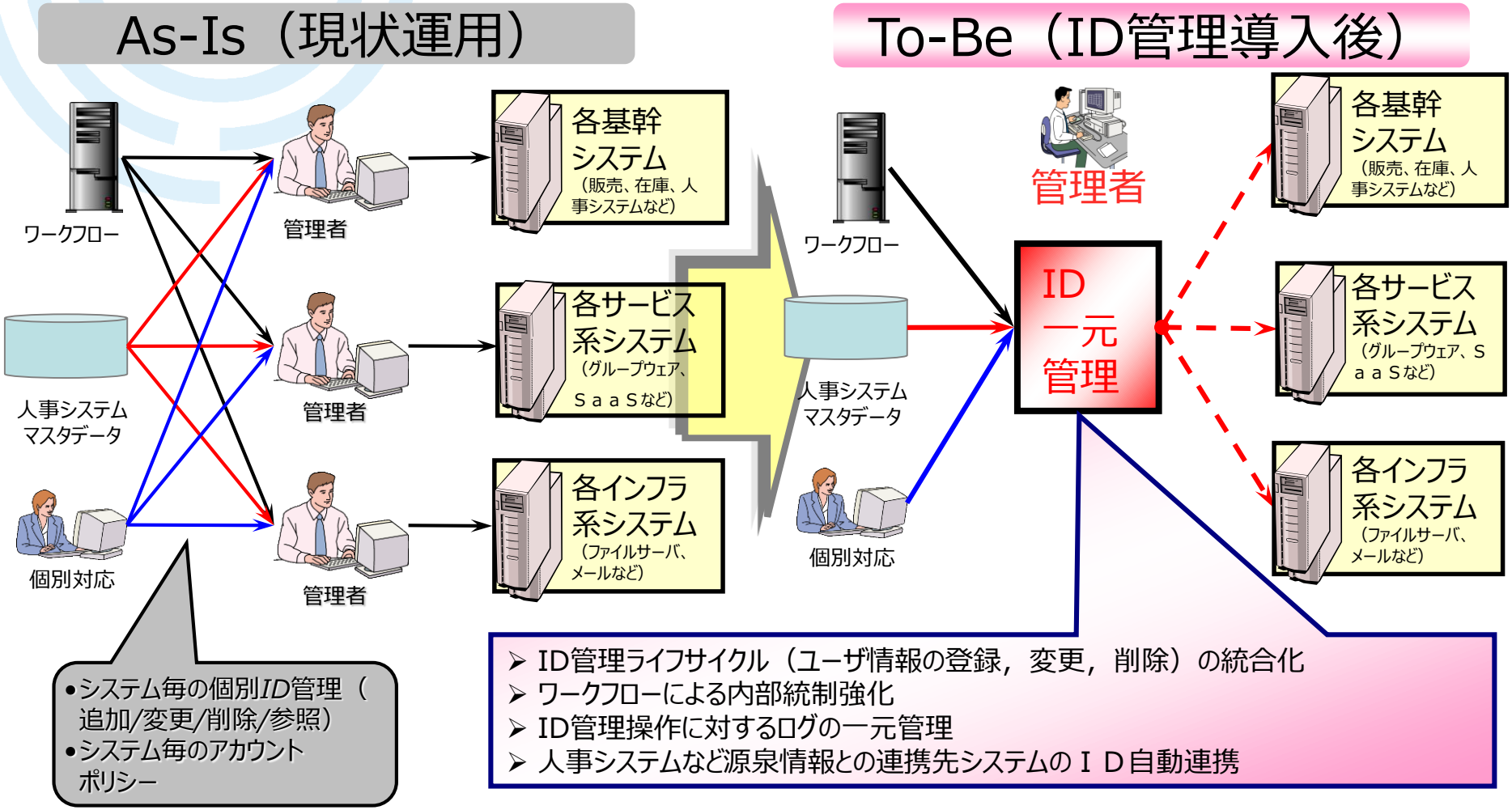
シングルサインオン（SSO）について

イントラにおけるSSO導入は利便性、セキュリティ強化に特に効果があります。



アイデンティティ管理（ＩＤＭ）について

SSOを更なる有効活用をするためにアイデンティティ管理（ＩＤＭ）も必要です。



1. SSOが求められる背景

2. SSO導入のポイントと事例

3. これまでのOpenAM

4. これからのOpenAM

SSO&IDM導入のポイント

企業にSSO&IDMを導入するために下記の認識が必要です。

レ 製品機能だけではなく、業務整理がキーとなる

- サービス、商用、OSS等多くのプロダクトがありますが、製品導入だけで完結しにくい領域です。
- 導入前に業務整理（ID運用ルール、セキュリティポリシー等）が必要となります。
- 業務整理結果とプロダクトを元に、カスタマイズが必要となることが多いです。

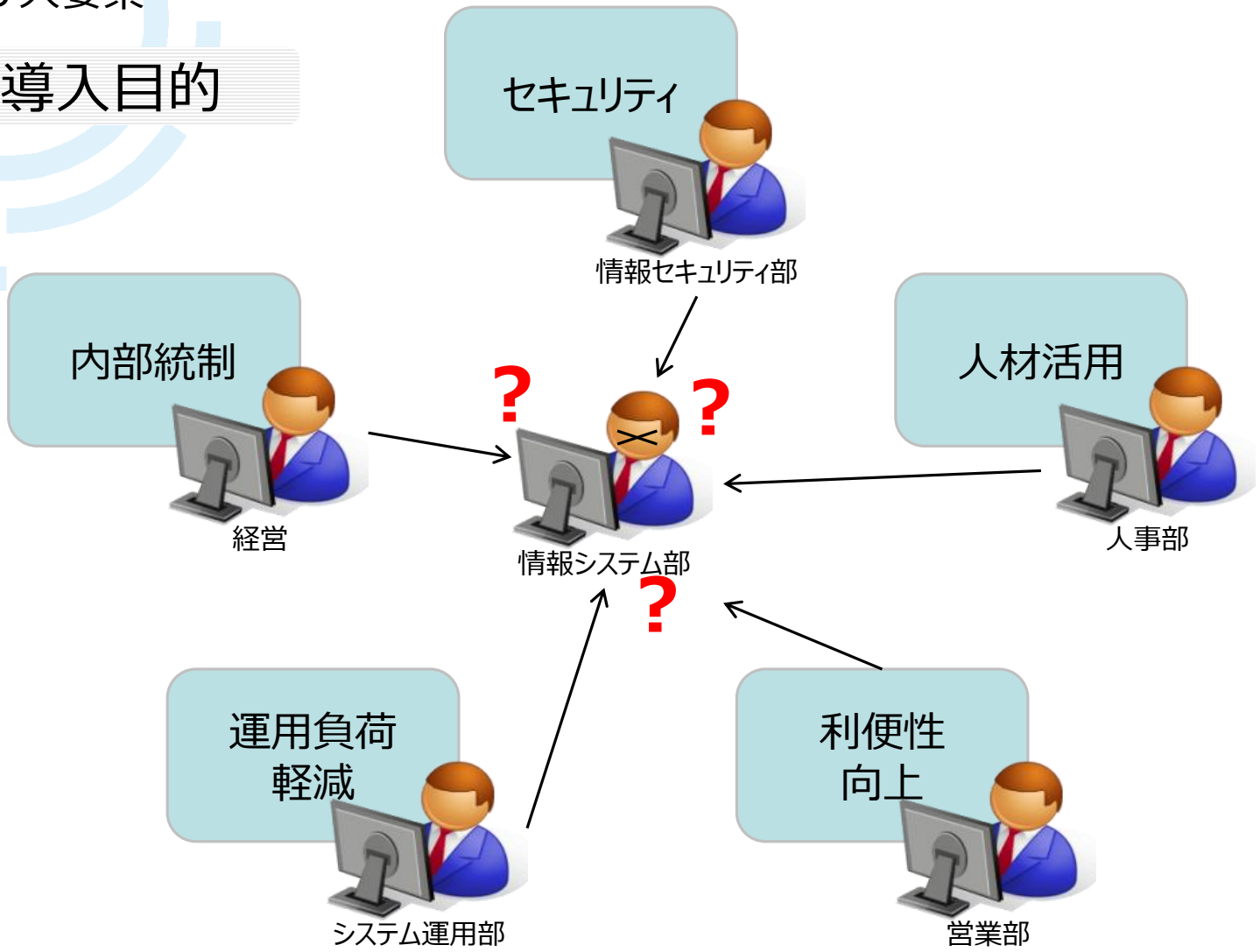
レ SSOはコモディティ化、IDMは多種多様

- SSO製品はある程度コモディティ化（標準化）されてきており、拡張性、性能、高度認証機能、管理機能などが差別化ポイントとなってくることが多いです。
- 一方でSSOを実現するためのIDMも対応したプロダクト構成になっていることが重要です。
- 日系企業の人事制度(IDライフサイクル)は特殊なため、IDMは日本用のローカライズが必要です。
- 業務整理により「例外管理」をどこまでなくせるかがシステム導入効果を高めるポイントです。

ブレの三大要素（1/3）

ブレの３大要素

レ ①導入目的



ブレの三大要素（2/3）

ブレの３大要素

レ ②オーナー

協力して対応よろしく。

経営

新規開発システム

費用負担を情シスがしてくれないなら、期限もあるので個別認証にしたい。ユーザ属性は情シスで管理してね。

○○プロジェクト部

SSO

情報システム部

連携先システムの状況が分からない。予算オーバー、どこを対象外にするか？誰が判断するのか？

海外拠点

本社は海外拠点のことを全くわかっていない。いままのままでも問題ない。拠点側に負担をかけるのは勘弁してほしい。

上海支社

社外

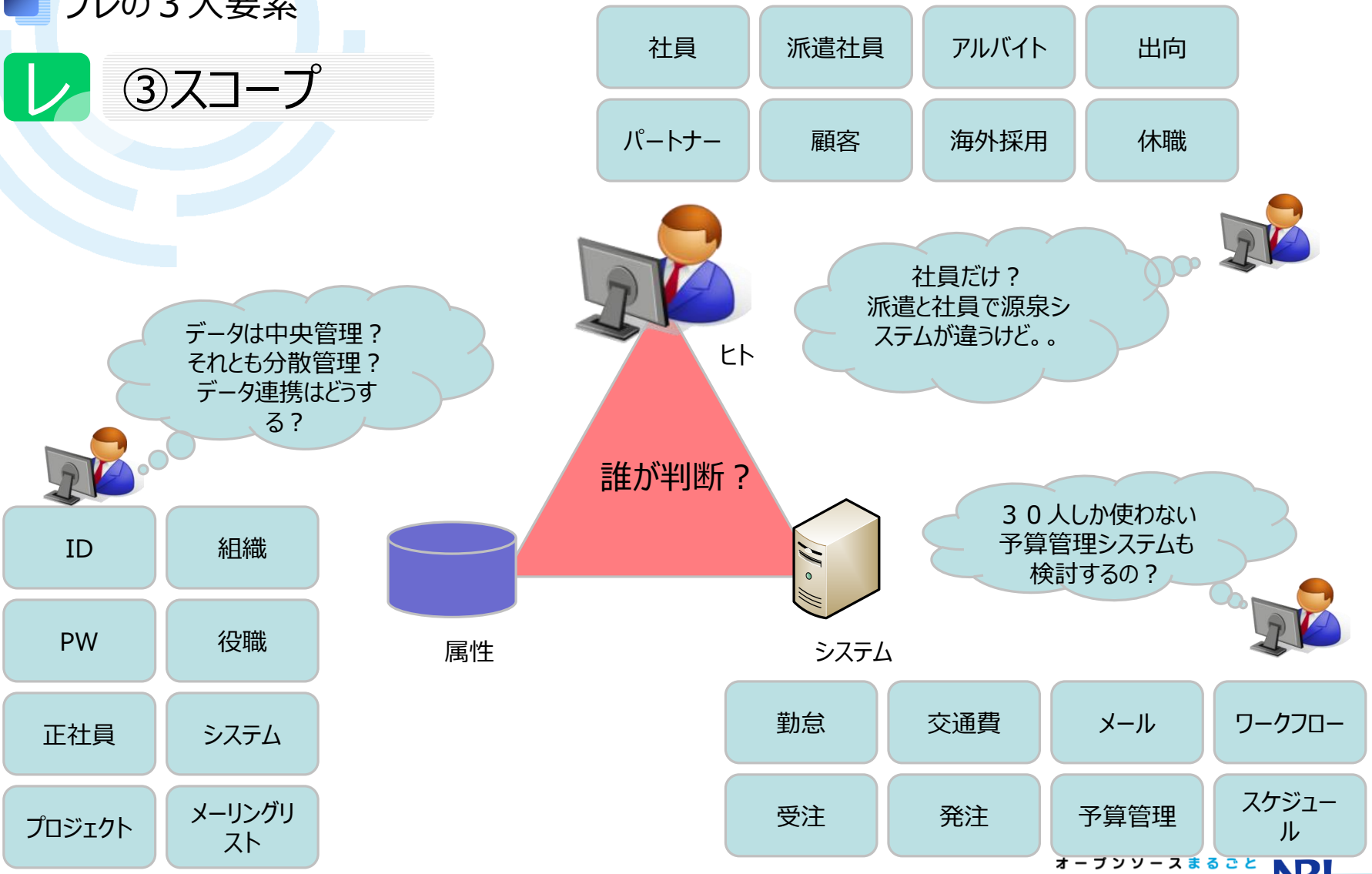
構想や計画はそちらにお願いしたい。うちがやることは設計からという前提。

××株式会社

ブレの三大要素（3/3）

ブレの３大要素

レ ③スコープ



プロダクト・ベンダ選定のポイント

SSO/IDM導入プロジェクト成功のポイントは下記と考えています

認証基盤導入プロジェクト成功のポイント

レ グローバルスタンダードな仕様に対応したプロダクト選定

➢導入後の保守やシステム拡張、SaaSサービス対応(Office365等)のために、グローバルスタンダードな仕様(認証連携の標準プロトコルであるOpenID Connect や SAML)に対応している、もしくはすぐに対応可能なプロダクトを選択することが望ましいです。

レ 高い拡張性を持つプロダクト選定

➢ビジネスの成長に伴い、ユーザの多様化、システムの追加・拡張、セキュリティの強化等が期待されるため、拡張可能な連携インタフェースを持つプロダクトを選択することが望ましいです（特定の多要素認証の導入、新たな認証方式への対応等）。

レ 安心できるシステム保守サポートを持つプロダクト・ベンダ選定

➢認証基盤は複数システムの入り口となるため多くの人に影響を与えます。そのため導入実績が豊富で、かつ安心して利用するためのサポートが必要となります。

モデルケース①：大手不動産業様
人事システムと業務システムとのＳＳＯ・ＩＤＭ

よくお問い合わせいただく人事システムと業務システムのＩＤ連携・ＳＳＯを実現する企業システムへの統合認証基盤導入のモデルケースをご紹介します。

背景

- 社内ユーザーはグループウェア、業務システムを使う際に、システムごとにログイン認証を行っており非効率である。
- 現行グループウェアの老朽化、利便性低下によりSaaS（SalesForce,GoogleApps等）の導入を検討中であるが、さらなるIDの増加は避け、SaaSのＩＤも含めて管理したい。

課題認識

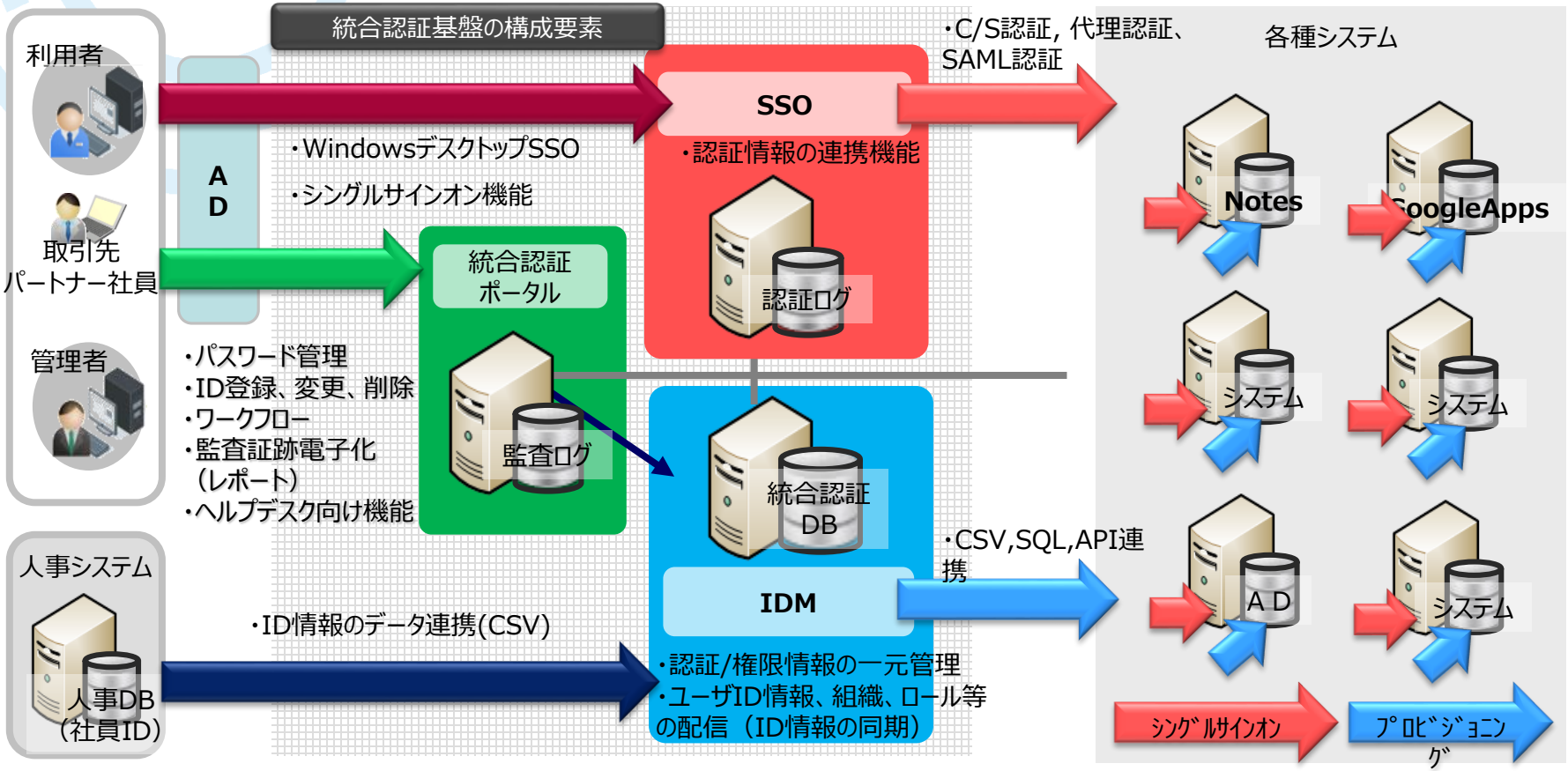
- 現在の各システムの認証の仕組みは個別の技術が使われていること、さらにIDを管理する部署が異なっている場合がある。
- グループウェア、Windowsドメイン、各業務システムの権限情報はそれぞれにあり、管理している。
- 人事異動時期のIDの棚卸し、変更管理作業は運用担当にとって非常に高い負荷である。

目的

- ユーザアカウント管理省力化によるシステム維持管理負荷やコストの低減を図る。
- 認証機能の一元化（シングルサインオン導入）によりセキュリティ向上、ユーザーへの利便性向上を図る。

モデルケース①：大手不動産業様
人事システムと業務システムとのＳＳＯ・ＩＤＭ

人事異動時のID管理業務を効率化したモデルケースのシステム構成例です。



モデルケース②：大手製造業様
本社＋グローバル拠点でＳＳＯ・ＩＤＭを実現するモデルケース

本社側でグローバル拠点も含めた内部統制管理をするため、本社＋グローバル拠点でＩＤ管理・シングルサインオンを実現するモデルケースをご紹介します。

背景

- 各リージョン・各グローバル拠点でID管理が個別最適化されている
- 人の出入りが速いため、ＩＤが氾濫し、ＩＤライフサイクルが十分に管理できていない
- システムに対してのアクセス権、誰が、いつ、なにを、どうした、を把握できていない。

課題認識

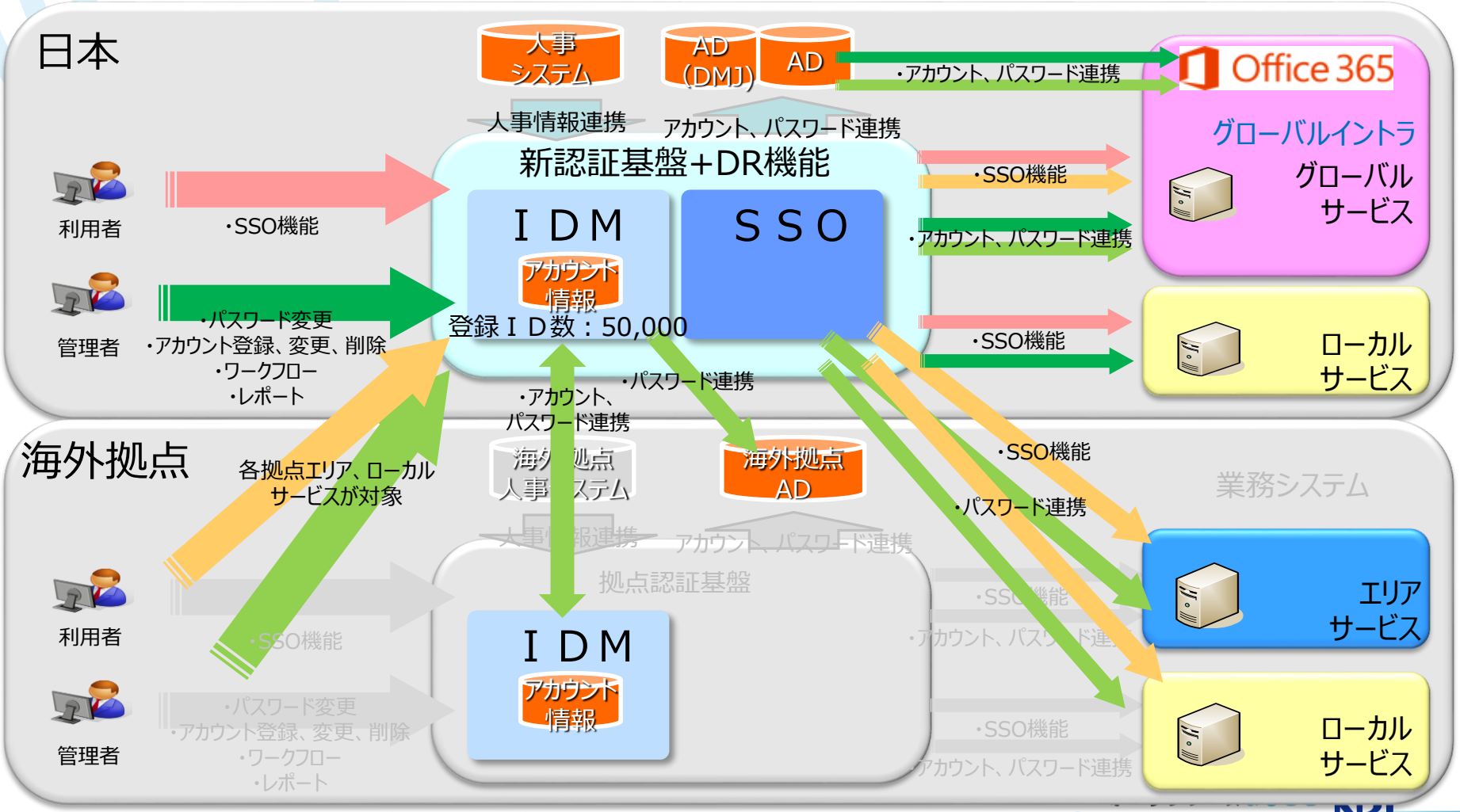
- 拠点ごとに個別で導入したシステムが乱立しており、本社側で管理できない状況にある
- 人事情報を本社と拠点で個別管理しており、ＩＤライフサイクルが管理できていない
- 現地のシステム対応が十分でないため、アクセス権設定、監査ログの取得ができていない

目的

- グローバル拠点間でID/PWDを統合管理し、本社側から内部統制を効かせる
- グローバル拠点間でのアクセスコントロールやシングルサインオンを実現し、セキュリティリスクを低減する

モデルケース②：大手製造業様
本社＋グローバル拠点でＳＳＯ・ＩＤＭを実現するモデルケース

認証基盤再構築にて本社／グローバル拠点の各サービスに対するＩＤＭ・ＳＳＯ機能を実現した構成例です。



OpenStandia™ Open Source Technology

NRI 未来創発 Dream up the future.

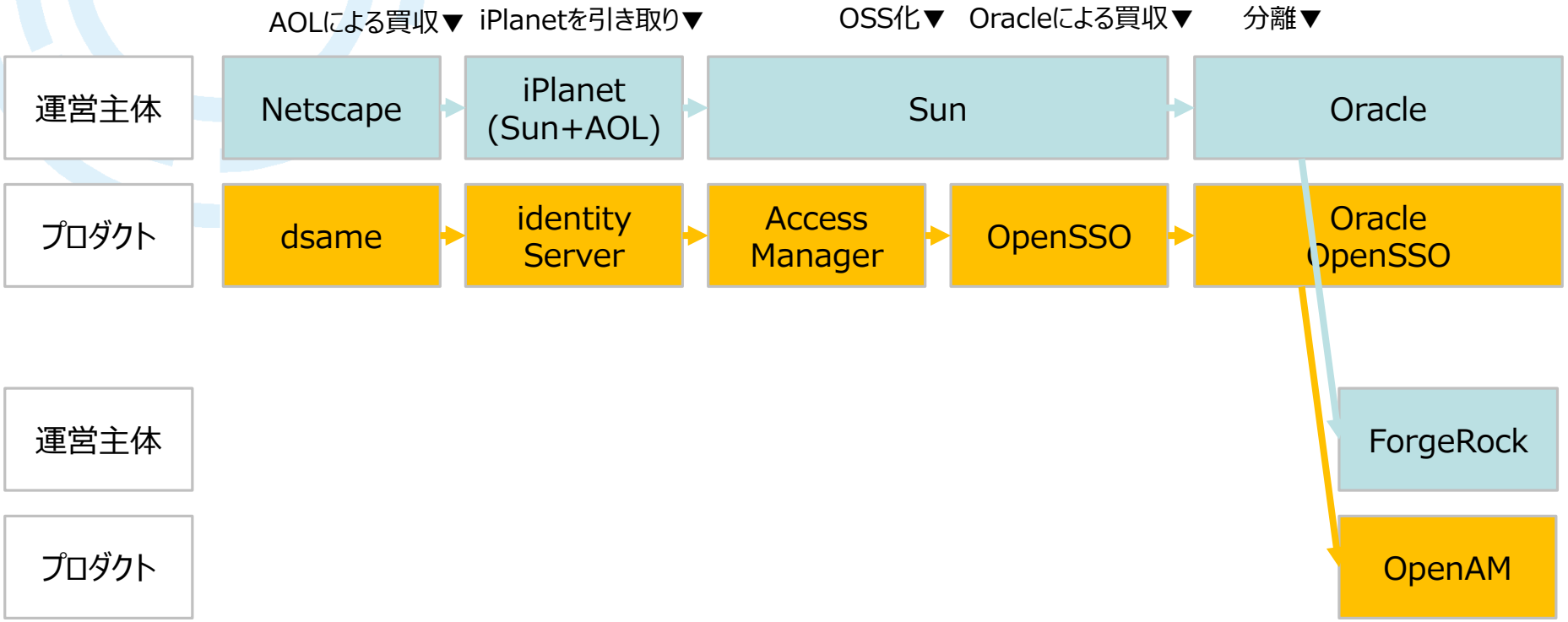
1. SSOが求められる背景

2. SSO導入のポイントと事例

3. これまでのOpenAM

4. これからのOpenAM

OpenAMの歴史



ForgeRock社について

ForgeRock.Inc.（フォージロック社）

サン・マイクロシステムズによって開発されたオープンソースのSSO製品「OpenSSO」をオラクルの買収を契機に開発者がスピンアウトして2010年に創設した会社。OpenAM、OpenIDMをはじめとしたオープンソースによるID関連製品を提供。この分野で現在急速に成長している。IRM（Identity Relationship Management）をコンセプトにユーザIDを利用した新しいビジネスモデルを築いている。（出所：http://forgerock.com/）

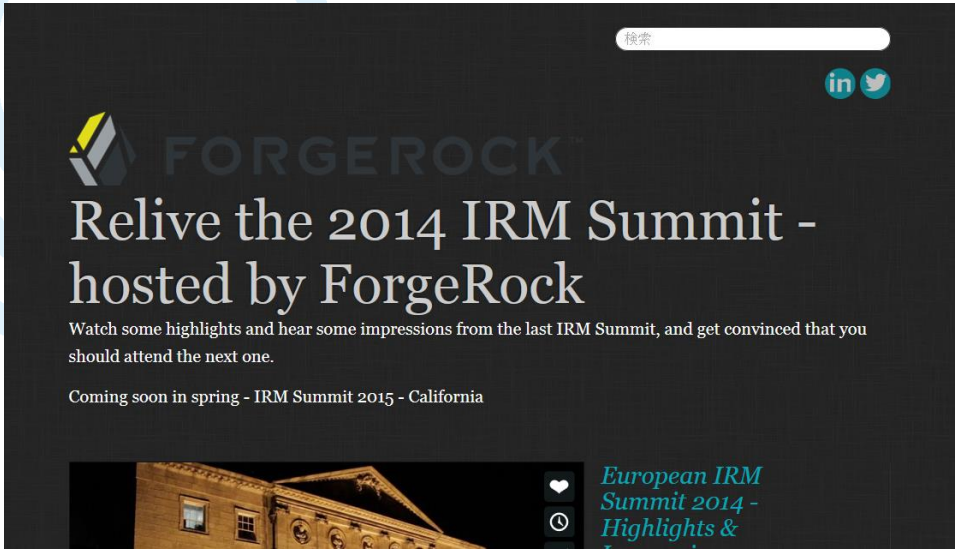
Mike Ellis
Chief Executive Officer

With more than 30 years of experience in the software and technology industries, Mike has held senior executive roles **at SAP, i2 Technologies, Oracle, and Apple**. Mike has also provided consulting expertise to some of the largest software firms and venture-funded startups to define and drive new growth and execution opportunities.
Mike has played and performed professionally as a guitarist and keyboard player and still enjoys playing.

Lasse Andresen
Chief Technology Officer

A powerhouse of tireless can-do enthusiasm, Lasse brings a unique blend of business, technical and people skills to ForgeRock. His 20+ years of experience in the software industry includes leadership roles at both Sun Microsystems (he served as **CTO for Sun Central and Northern Europe**) and Texas Instruments. Lasse was also the co-founder and CTO of Gravityrock. Lasse's passion and vision for entrepreneurship ensures ForgeRock is always ready to execute and deliver

OpenAM関連のグローバルセミナー



出所：
http://vimeopro.com/forgerock/re-live-the-2014-european-irm-summit-hosted-by-forgerock

出所：
http://summits.forgerock.com/

IDENTITY SUMMIT SERIES 2015: EUROPE

hosted by FORGEROCK in partnership with CDO SUMMIT

Co-Sponsored by accenture

WHY ATTEND ?

- Learn how digital transformation requires identity
- Make identity the center of customer relationships

CONTENT OVERVIEW

- Interactive expert panels & industry keynotes
- Sessions on customers' digital transformation

WHO WILL BE THERE

- Industry-leading analysts & businesses
- CIOs, CDOs, & CEOs embracing digital identity
- CISOs, Lead Architects, & Technical

ForgeRockプロダクト群

OpenIDM 属性データ連携

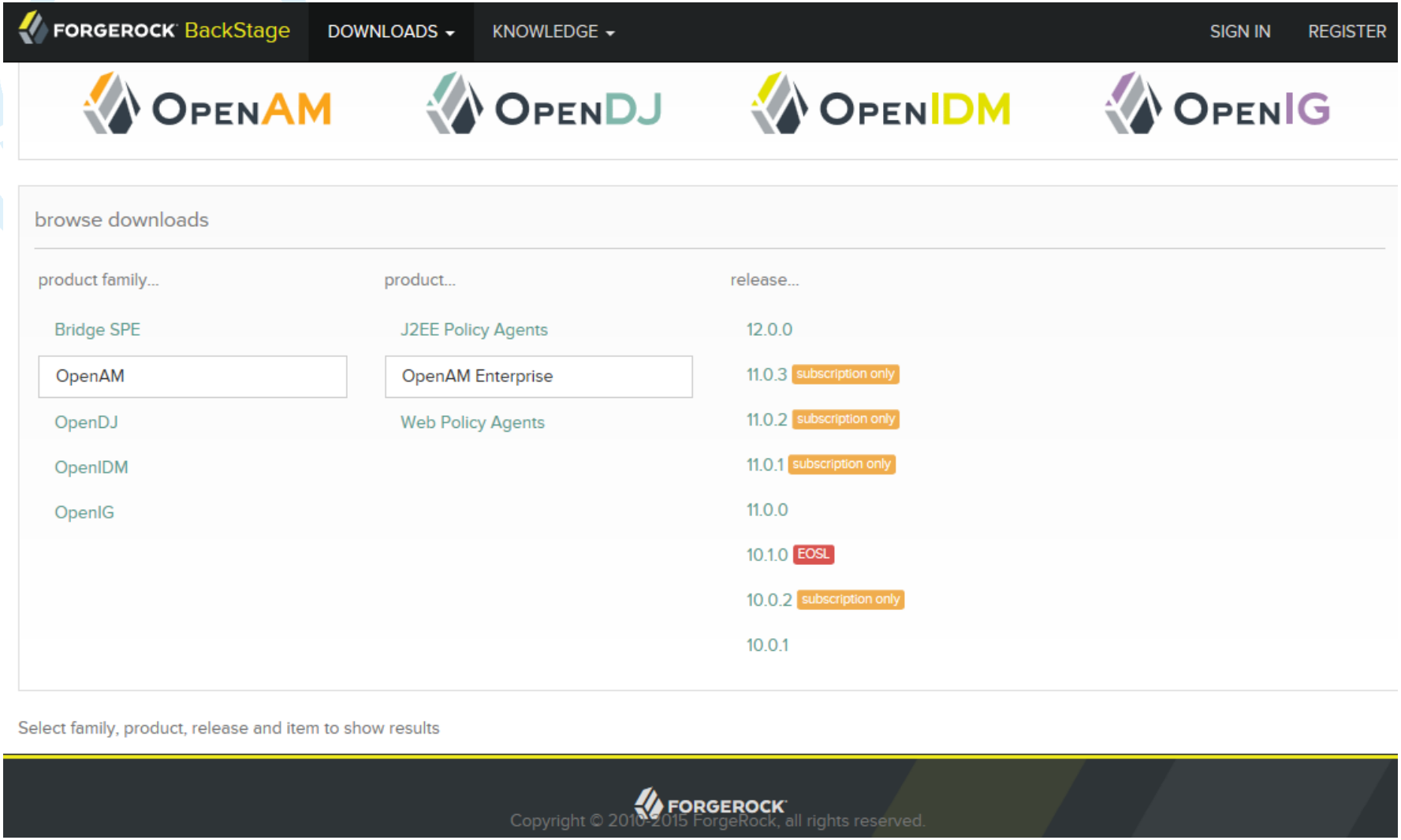
OpenAM 認証認可

OpenIG 認証ゲートウェイ

属性データストア OpenDJ

出所：
https://www.forgerock.com/products/

OpenAMのダウンロードサイト



出所:
https://backstage.forgerock.com/#!/downloads/OpenAM/OpenAM%20Enterprise#browse

コミュニティ版とサブスクリプション版の違い

価値	コミュニティ版	サブスクリプション版
メジャーリリース (9.0, 10.0, 11.0等)	開発ライセンス	開発ライセンス 商用ライセンス
メジャーリリース ソースコード	○	○
コミュニティフォーラム	○	○
メンテナンスリリース （9.0.1,10.0.1,11.0.1等）		○
メンテナンスリリース ソースコード		○
プロダクトサポート		○
法的保障 （知的財産権リスク）		○

NRIとForgeRock社の提携

NEWS RELEASE

NRIが米フォージロック社との提携によりオープンソースのシングルサインオン・ユーザ情報管理製品の国内提供を開始

2014年07月30日
株式会社野村総合研究所
ForgeRock.Inc.

印刷用ページ PDF 186KB | お問い合わせ

株式会社野村総合研究所（本社：東京都千代田区、代表取締役社長：嶋本 正、以下「NRI」）は、ForgeRock.Inc.*1（本社：サンフランシスコ、CEO：M.エリス、以下「フォージロック社」）との間で、日本国内におけるオープンソースのシングルサインオン*2・ユーザ情報関連事業でパートナー契約を締結しました。

フォージロック社は、シングルサインオンやユーザ情報管理等のIRM（Identity Relationship Management）*3業界における世界的なリーディングカンパニーです。日本においても注目されつつあるフォージロック社のオープンソースIRM製品を、本日、NRIは日本で初めて提供開始するとともに、日本語でのサポートをおこないます。

近年、企業内ではユーザIDやそれに紐付く属性情報など、ユーザ情報を厳格に管理するニーズが加速しており、それに伴って、世界的にIRMソリューション市場が成長しています。フォージロック社は、日本でのシェア拡大に向けて、NRIとの提携に至りました。

また、NRIは、グローバルで革新的なIRMサービスを顧客に提供するためには、フォージロック社が最良のパートナーであると考え、顧客の業務改革や新サービス開発のためのコンサルティングおよび、技術支援サービスを提供する際、フォージロック社のIRM製品を活用していきます。

- レ Enterprise版の国内販売
- レ 日本語サポート
- レ EOSL(リリースより３年＋１年)後のサポート

OpenAMの特徴

	OpenAM	商用製品（一例）
技術の公開	オープンソースで**技術は公開**されている	商用製品で**技術は非公開**
機能	基本的な機能を持つ （ID管理機能、プロビジョニング機能、SSO、フェデレーション機能）	基本的な機能を持つ （ID管理機能、プロビジョニング機能、SSO、フェデレーション機能）
設計・特徴	**最新のオープンアーキテクチャ** 認証・認可・IDプロビジョニング等の**各機能をプラグインとして実装**	**10年以上前の製品がベース** **DB等の基盤全般を同社製品で統一する必要がある**
新技術/機能への対応	**標準仕様策定に関与。** また、**サードパーティからも周辺製品が多数提供。** （例：ワンタイムパスワード、多要素認証、リスクベース認証プラグインなど）	**最新の標準仕様には追随する（方向）**
カスタマイズ	製品機能をAPIを使って呼び出せるため、独自機能の多くを**製品カスタマイズなく実装**可能	機能変更は**製品のカスタマイズ**になる
性能	**数千万人単位のユーザ**を扱うことを前提に設計	**数万～10万人程度までがターゲット**
ライセンス	サブスクリプション（年間）	製品ライセンス＋年間保守料

拡張性

- OpenAMではSSO,IDMの機能をプラグインで拡張可能
  - 既に様々なプラグインが提供されている（下記表）
  - 独自にプラグインを追加することも可能

種類	名称	説明	備考
多要素認証	OATH認証	OATH仕様に準拠したOTP(ワンタイムパスワード)認証	http://www.atmarkit.co.jp/ait/articles/1310/17/news003_2.html
	Yubikey認証	OATH仕様に準拠したUSBドングル	
リスクベース認証	アダプティブリスク認証	ログイン時の地理的位置、最終ログインからの経過時間や認証失敗回数、IPアドレスの履歴などから、ログインしようとするユーザーが本人ではないリスクを評価し、必要に応じて追加の認証を要求	http://www.atmarkit.co.jp/ait/articles/1310/17/news003.html
	デバイスプリント認証	ユーザーの使用しているOSの画面解像度や色深度、インストールされているフォントの種類、ブラウザの種類やバージョンなどから、ログインしようとするユーザーが本人ではないリスクを評価し、必要に応じて追加の認証を要求	http://www.atmarkit.co.jp/ait/articles/1310/17/news003_2.html

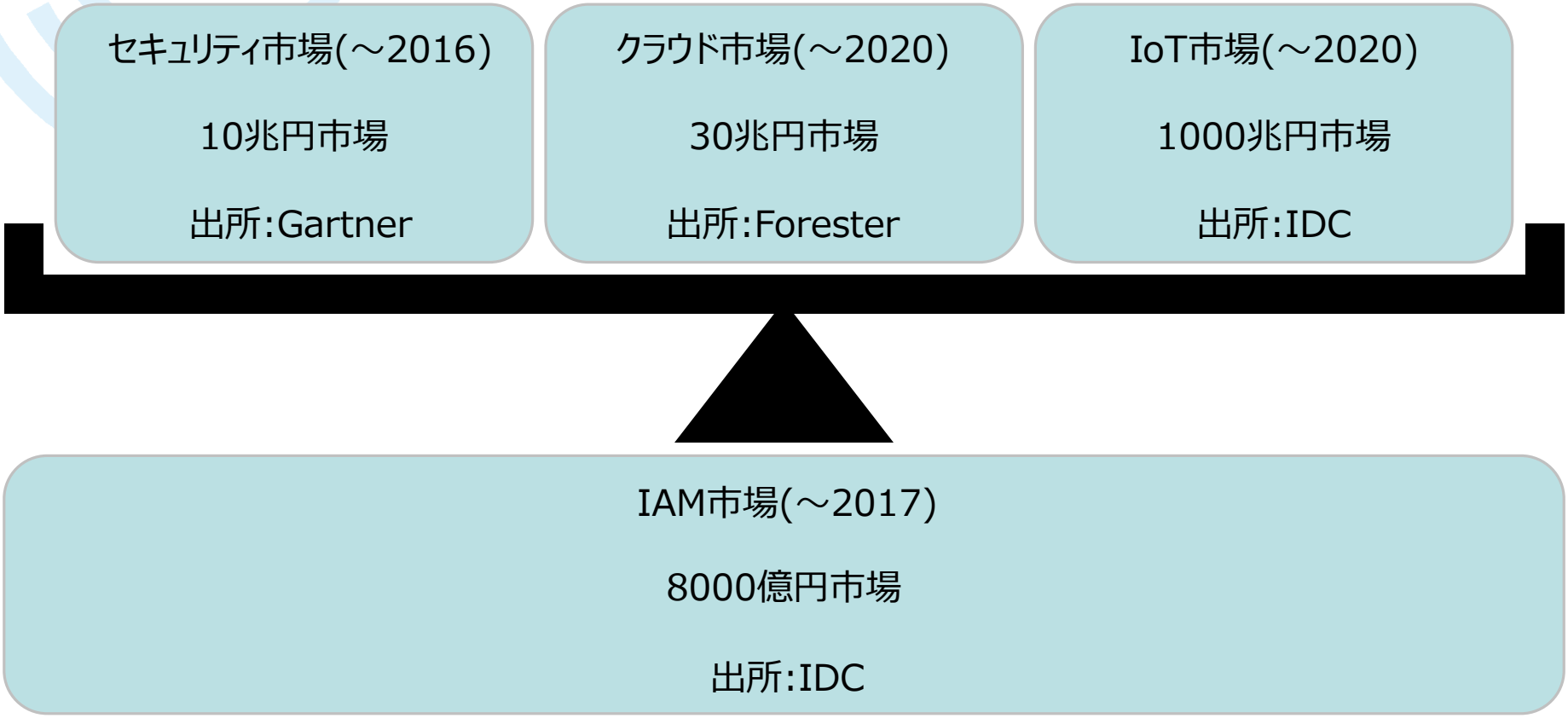
1. SSOが求められる背景

2. SSO導入のポイントと事例

3. これまでのOpenAM

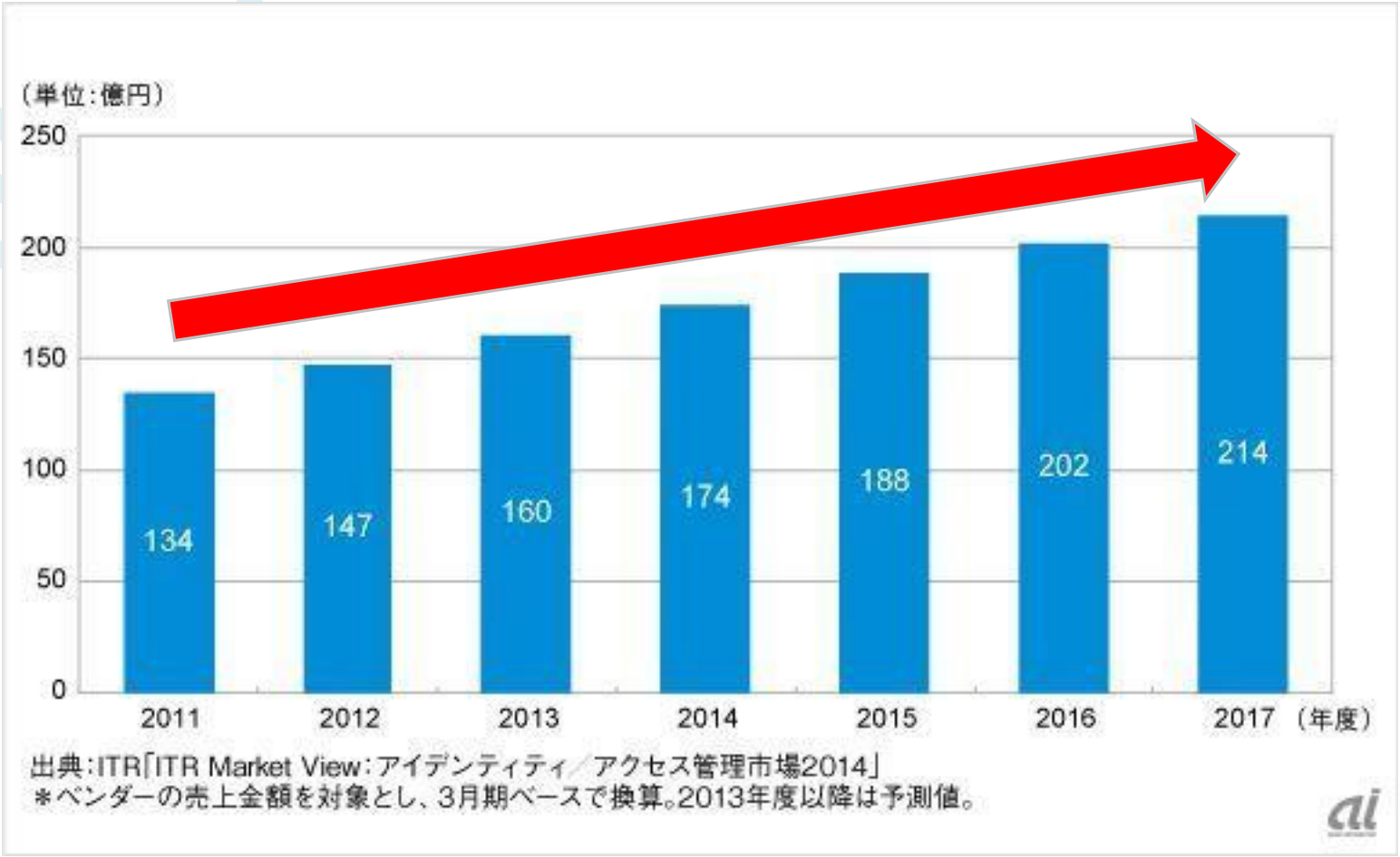
4. これからのOpenAM

グローバル市場規模



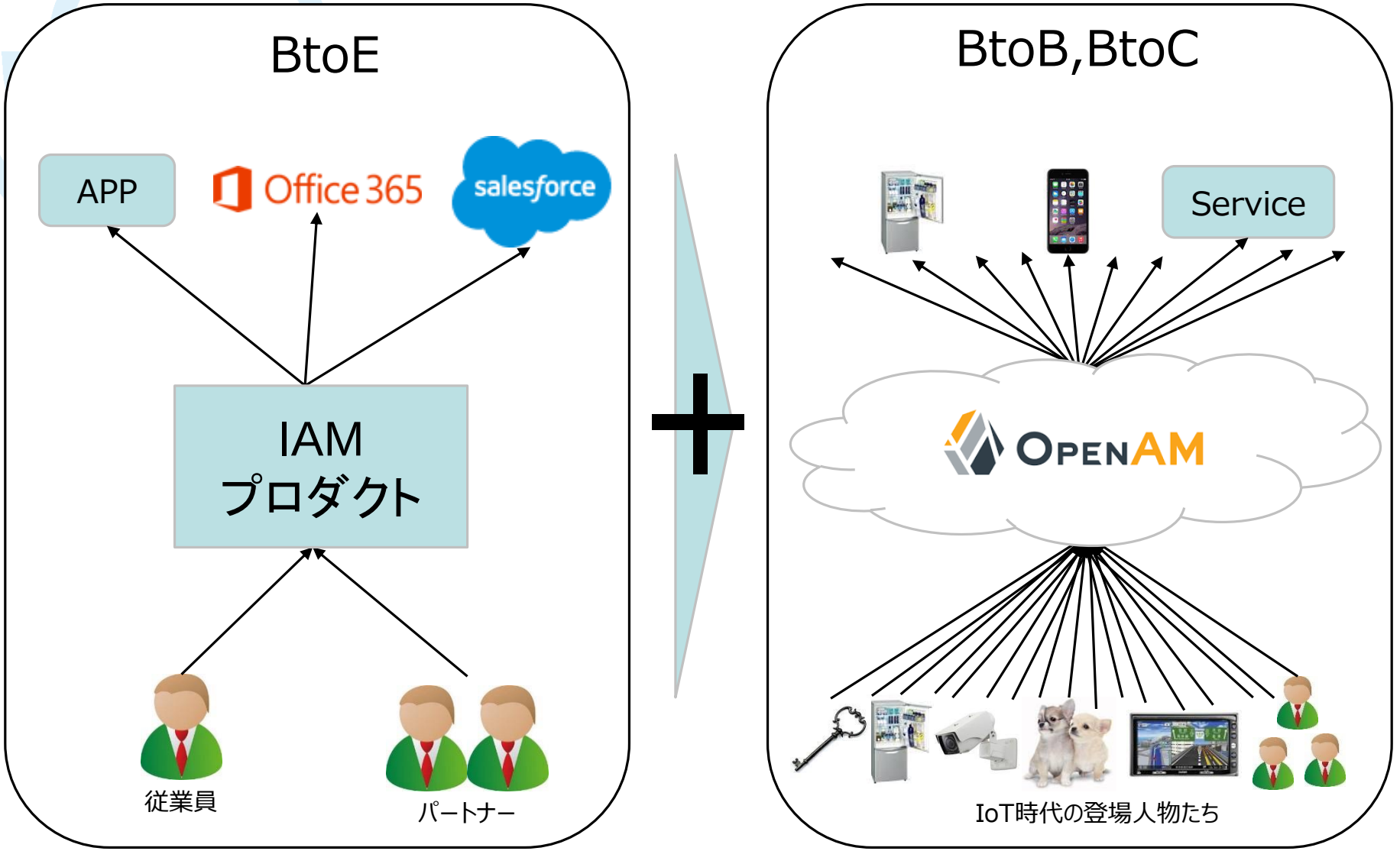
※講演当時の為替レートで日本円換算

国内市場規模



出所：http://japan.zdnet.com/article/35049181/

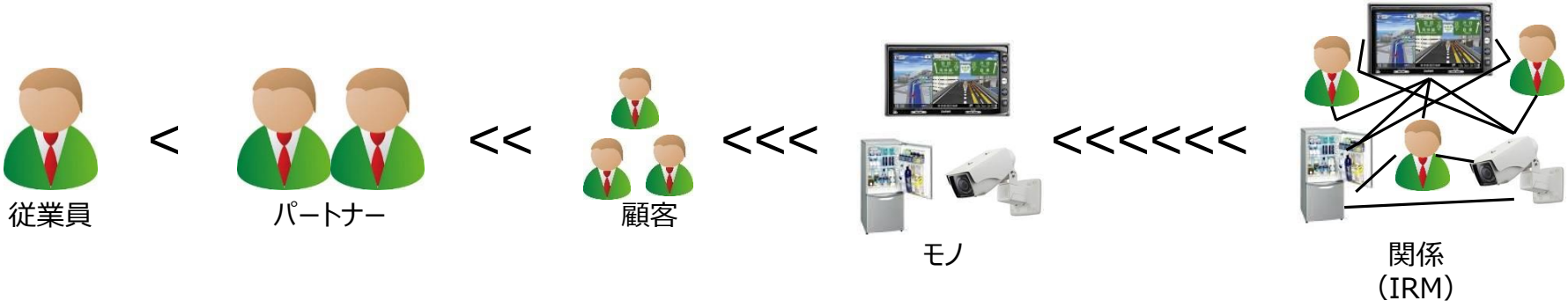
IAMのこれから



なにが変わるのか？

ID数、認証数

ID数と認証数の変化



性能

ターゲット性能

SSO

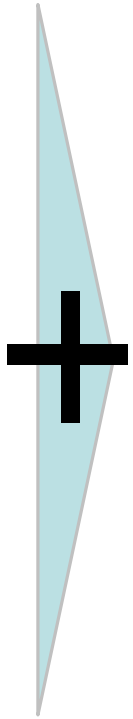
１００００ID

IDM

秒間１０件

DB

１０同時接続



OpenAM

１億ID

OpenIDM

秒間１００件

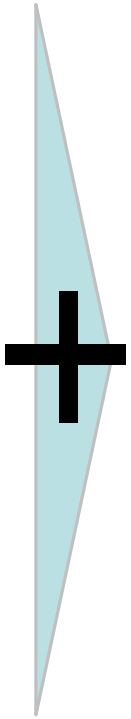
OpenDJ

１０００同時接続

作り方

作り方

【個別最適】
代理認証
クラサバ
ヘッダ連携
CSV
SQL
スクラッチ

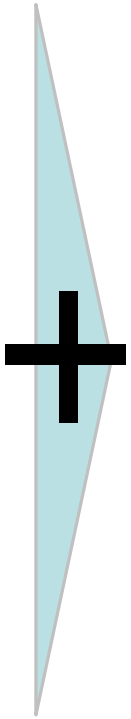


【標準化＆API】
SAML
WS Federation
OpenID Connect
OAuth
REST
UMA

サービスレベル

サービスレベル

ビジネスタイム
計画停止
Active-Active

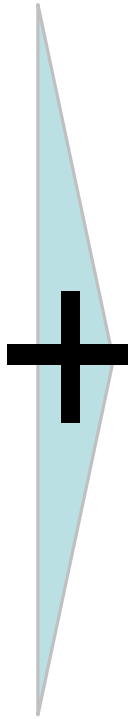


24H365D
無停止リリース
自動スケール

目的

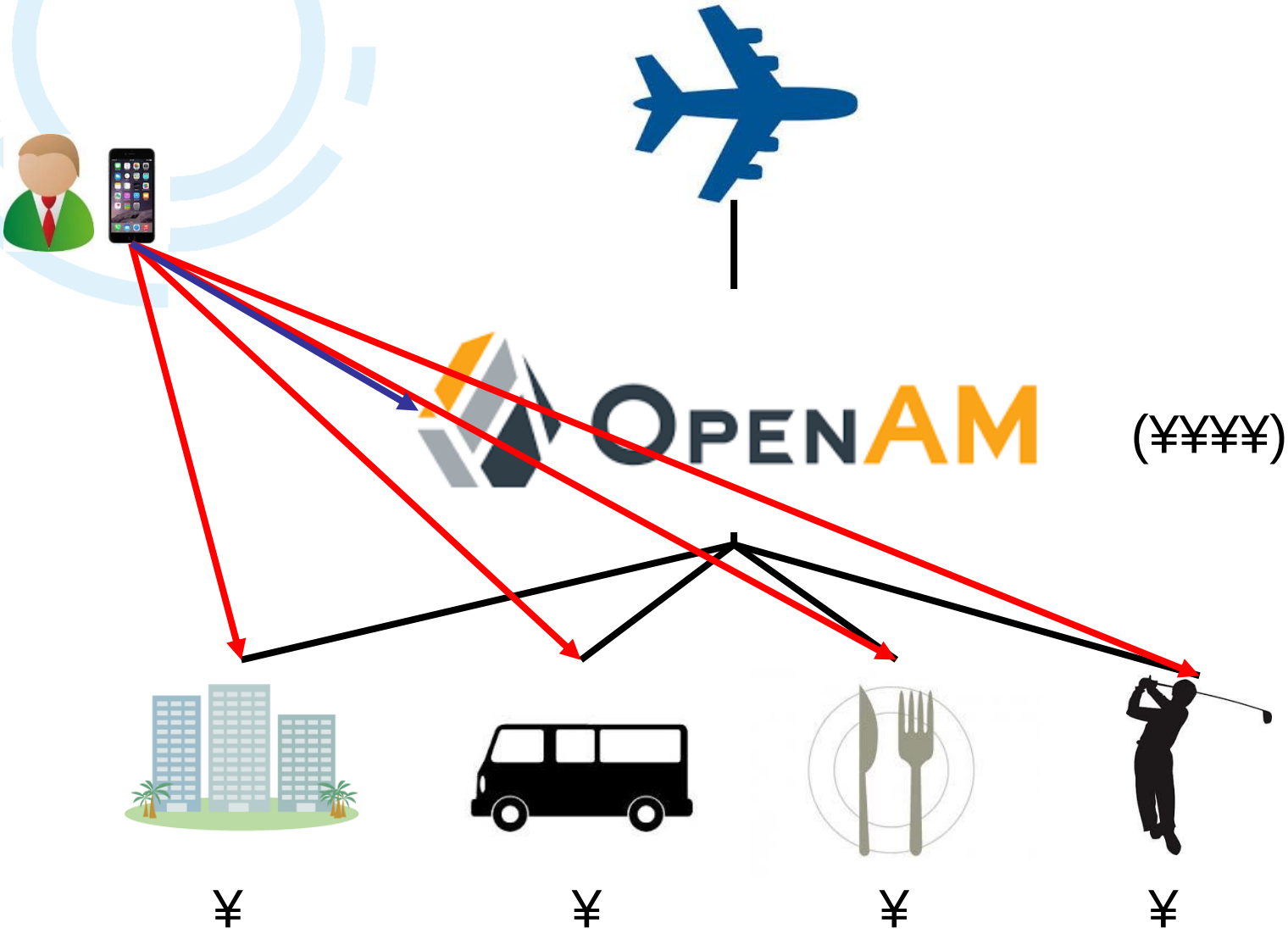
目的

利便性向上
コンプライアンス
コスト削減

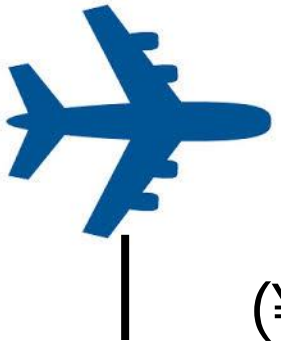


アジリティ
バリューチェーン
売上向上

カスタマーエクスペリエンス



カスタマーエクスペリエンスとバリュー



(¥¥¥¥¥¥¥¥¥¥) x ? x M

OPENAM

サービス ¥ サービス ¥ サービス ¥ サービス ¥ サービス ¥ サービス ¥ サービス ¥ サービス ¥ サービス ¥ サービス ¥

最後に

- レ 時代は「IAM」から「IRM」へ
- レ 「認証」から「カスタマーエクスペリエンス」へ
- レ 「安いオープンソース」から「価値のあるオープンソース」へ

本資料に掲載されている会社名、製品名、
サービス名は各社の登録商標、又は商標です。

- **OpenStandiaは、「攻めのIT」を支援します。**
- **オープンソースのことなら、なんでもご相談ください！**

オープンソースまるごと

OpenStandia™

Open Source Technology

お問い合わせは、NRIオープンソースソリューション推進室へ

ossc@nri.co.jp

http://openstandia.jp/

NRI 未来創発

Dream up the future.