OpenStandia/SSO&IDMのご紹介
～企業システムのシングルサインオン、統合ID管理～

2015/02/26

野村総合研究所
オープンソースソリューション推進室
田中　穣

野村総合研究所のOpenStandia（オープンスタンディア）は、おかげさまで、2006年のサービス開始から2011年までの5年間で契約数累計が1,000件を突破いたしました！

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/

オープンソースまるごと
OpenStandia™
Open Source Technology

NRI 未来創発
Dream up the future.

目次

はじめに
シングルサインオン・統合ID管理が求められる時代の環境変化

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

はじめに
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）

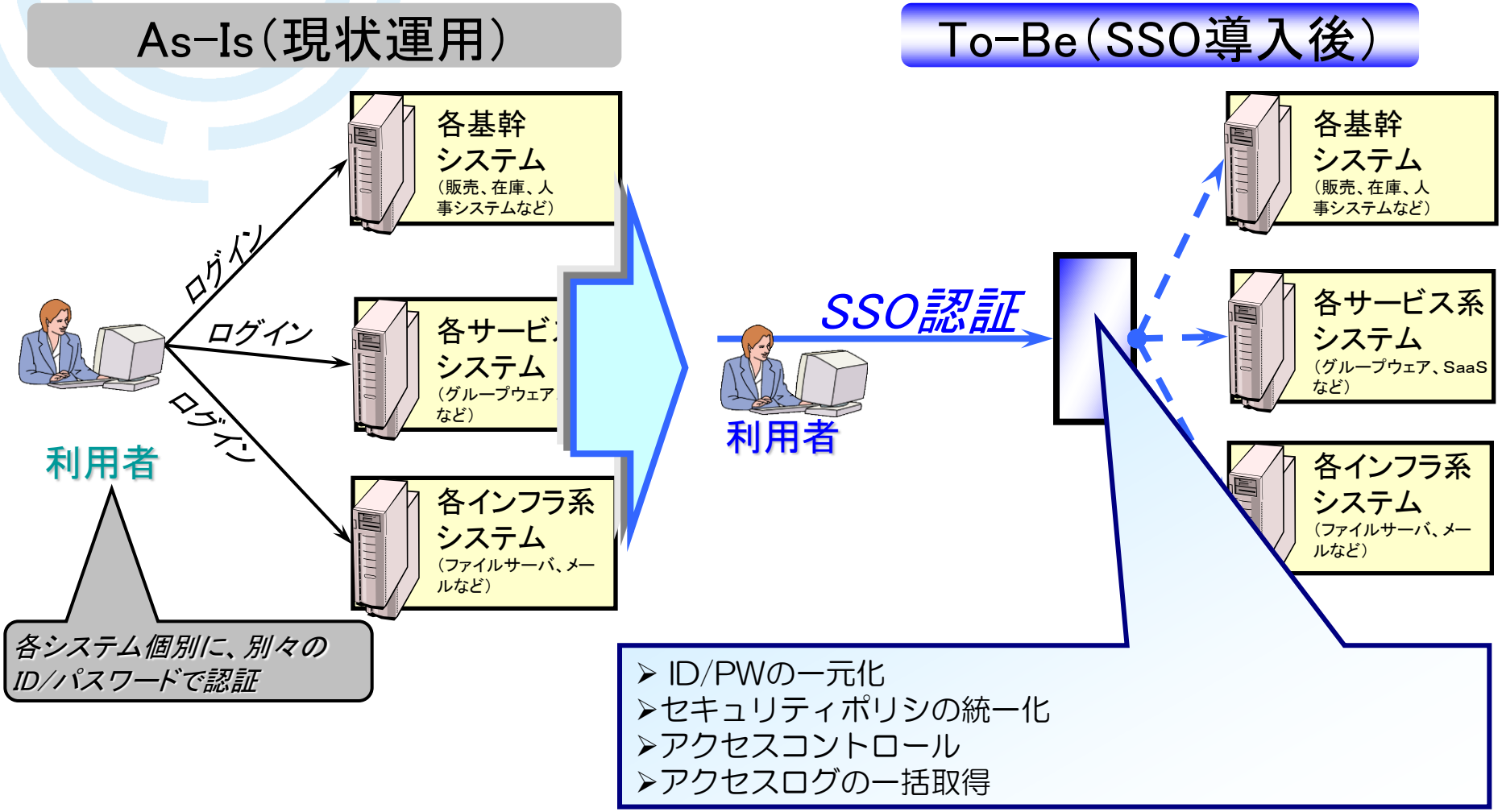
- グローバル拠点のシステム、IDライフサイクルを統一的に管理
- ローカルサービス、ローカルパッケージとのID連携

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

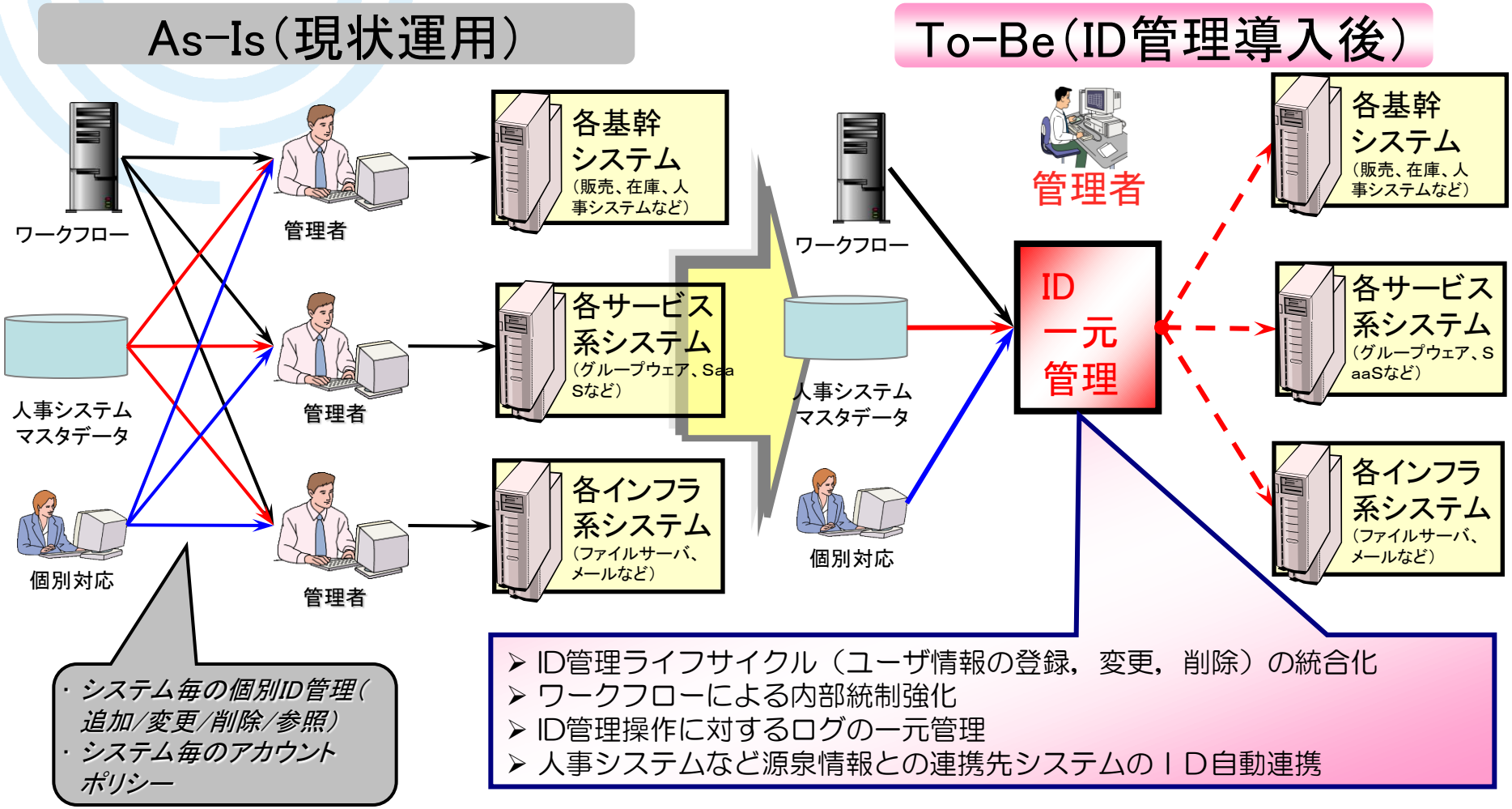
はじめに
シングルサインオン(SSO)について

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。



はじめに
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。

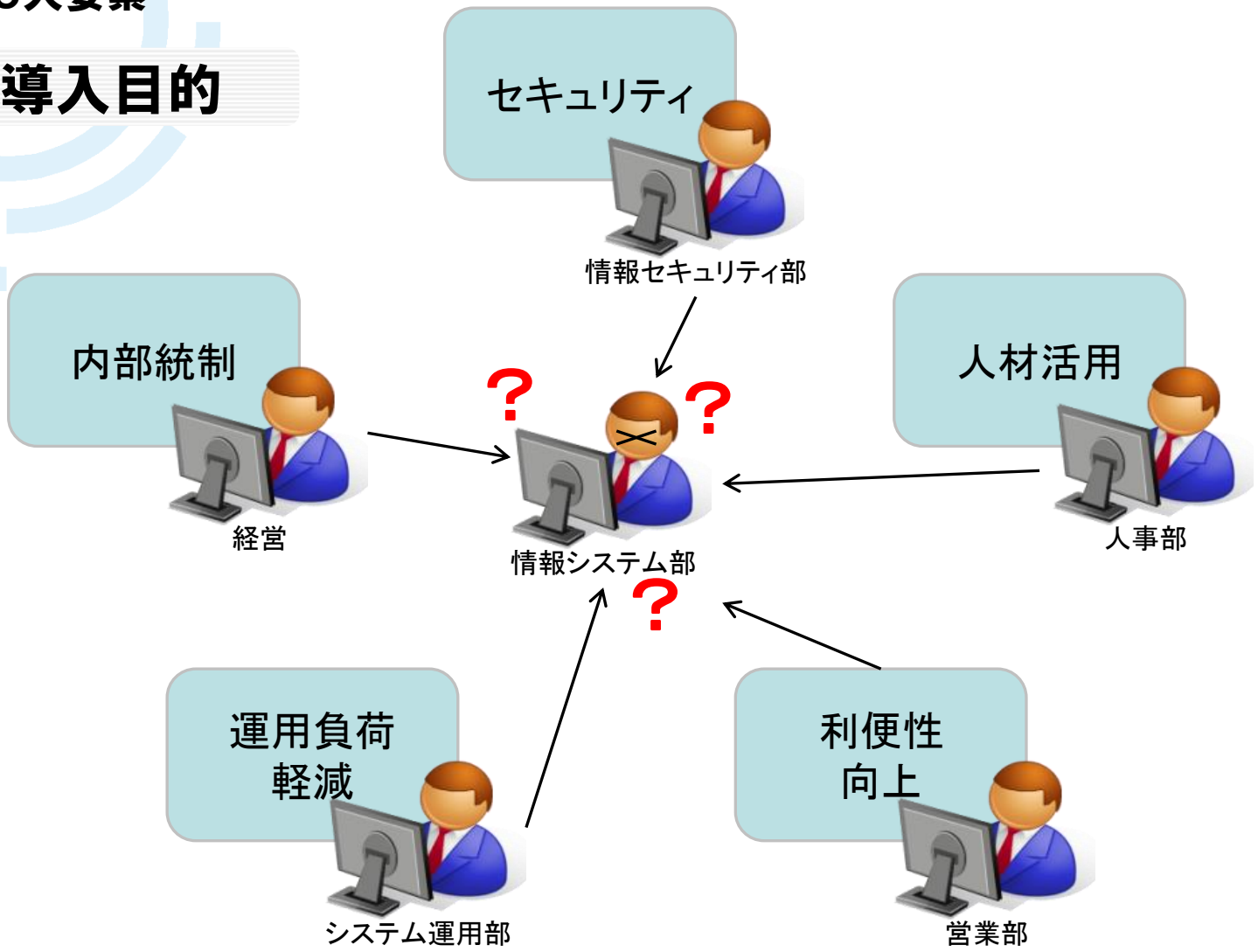


目次

プロジェクト推進に要求される要件
企業へのSSO＆IDM導入にあたり理解していただきたいこと

ブレの3大要素

①導入目的



プロジェクト推進に要求される要件
企業へのSSO＆IDM導入にあたり理解していただきたいこと

ブレの3大要素

レ ②オーナー

経営

協力して対応よろしく。

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？

新規開発システム

〇〇プロジェクト部

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。

海外拠点

上海支社

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。

社外

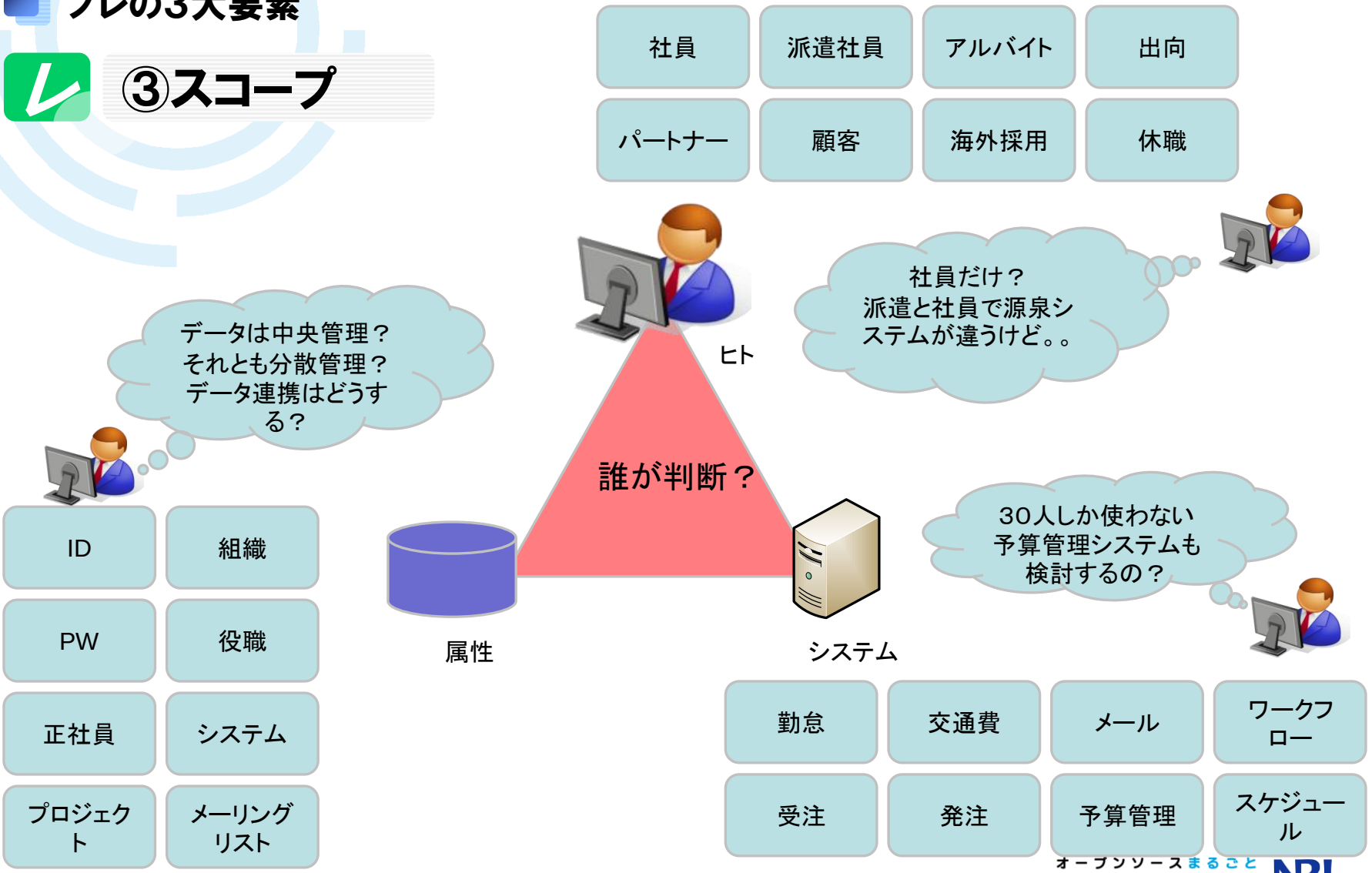
××株式会社

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。

プロジェクト推進に要求される要件
企業へのSSO＆IDM導入にあたり理解していただきたいこと

ブレの3大要素

③スコープ



プロジェクト推進に要求される要件
企業へのSSO＆IDM導入にあたり理解していただきたいこと

企業にSSO＆IDMを導入するために下記の認識が必要です。

製品力だけではなく、業務整理がキーとなる

- 多くの製品がありますが、製品導入と設定だけで完結しにくい領域です（もちろん整理がされていれば完結する場合もあります）。
- 事前に企業毎の業務整理（ID運用ルール、セキュリティポリシー等）が必要です。
- 業務整理結果とパッケージを元にカスタマイズ（設定、特殊なものは個別実装）が必要です。

SSOはコモディティ化、IDMが導入のカギ

- 特にSSO製品はある程度コモディティ化されてきており、拡張性、性能、高度認証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は世界的に特殊なため、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。

プロジェクト推進に要求される要件
SSO導入プロジェクト成功のポイント

SSO導入プロジェクト成功のポイントは下記になります。

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。

プロジェクト推進に要求される要件
IDM導入プロジェクト成功のポイント

SSOはIDMを導入することで効果が高められます。IDM製品導入する場合、下記にどこまで容易に対応できるかどうかがポイントとなります。

IDライフサイクル管理(期日管理)

- IDの作成(入社)、削除/無効化(退社)、変更(異動)
- 発令日ベースのIDライフサイクル管理(変更反映予定の事前登録)
- 兼務／出向対応

権限管理

- 役職と所属による権限管理
- 権限の個別設定(出来る限り排除することが望ましいが現実的には必要)

内部統制対応

- ワークフロー
- 履歴管理
- 棚卸し
- 監査ログ

目次

OpenStandia製品紹介
OpenStandia/SSO&IDMの特徴

- OpenStandia/SSO&IDMはオープンソース（OpenAM, OpenIDM, OpenDJ, OpenIG）をベースにNRI独自機能を追加したSSO/IDM製品です。

OpenStandia/SSO&IDMの特徴

システム拡張、個別対応に強い

グローバルスタンダードなオープンソースアーキテクチャをベースにしつつ、多くの拡張APIにより外部システム（クラサバ、SaaS、スクラッチアプリ）との連携及び個別要件にも対応可能です。

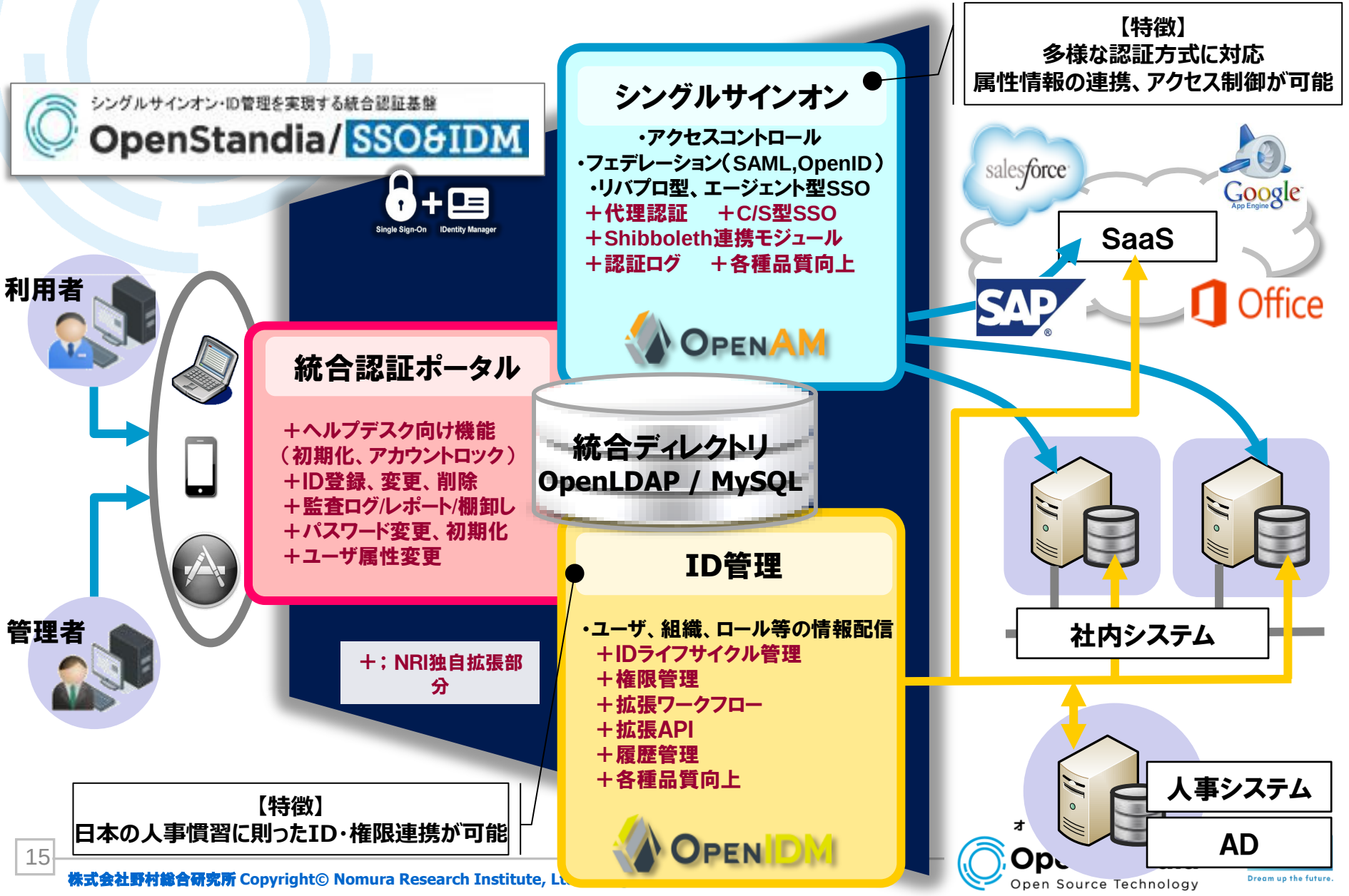
日系企業特有の人事制度に対応

人事異動、出向、兼務といった日系企業独自の制度に対応しています。辞令、発令、業務引継完了までのタイムラグ管理もプロダクトとして吸収することが可能です。

スピーディでストレスの少ないワンストップ保守体制

野村総合研究所社内にて、製品開発チームとサポートチームが一体となってスピーディかつストレスのないワンストップサポートをご提供いたします。

OpenStandia製品紹介
OpenStandia/SSO&IDM全体概要



OpenStandia製品紹介
OpenStandiaのSSO機能

OpenStandia/SSO&IDMの主要なSSO機能（下記は機能の一部です）

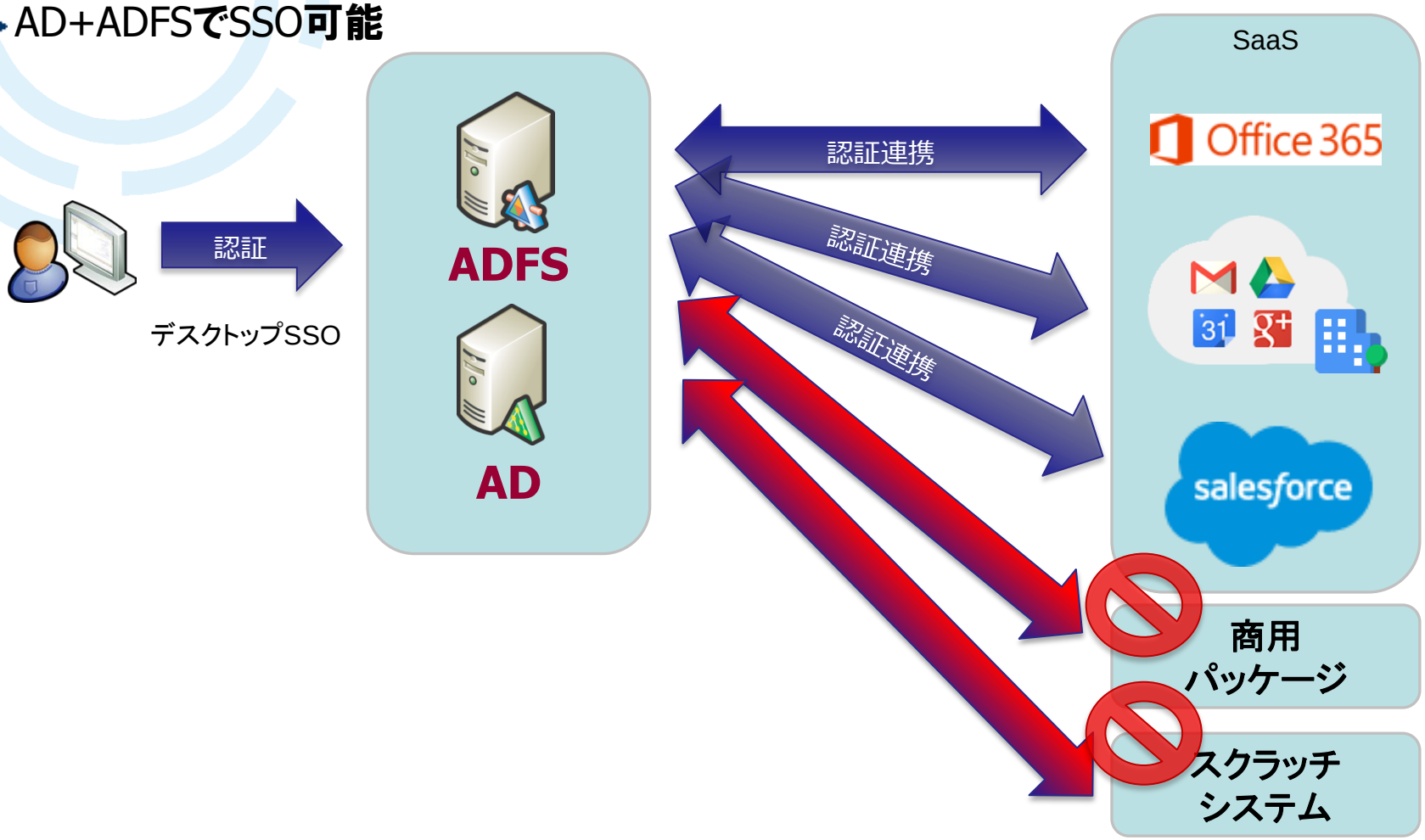
- OpenStandia/SSOでは主に5種類のSSO認証方式を選択可能です。
- 方式の違いによって SSO・IDM・SSO対象システムへの影響が異なります。

SSO認証方式		概要
a	公開プロトコル(フェデレーション)方式	Microsoft, Google, 国内キャリア始め、多くのSaaSベンダ、パッケージベンダが対応するグローバルスタンダードな認証連携プロトコル(OpenID Connect / SAML)でSSOを実現する方式
b	リバプロWeb Agent 方式	ユーザIDをHTTPヘッダ等で連携する方式 （a. の公開プロトコル策定以前から、比較的多くのパッケージベンダが対応するレガシーな SSO 実現方式）
c	フォーム認証 (リバプロ型代理認証)方式	SSO 基盤が（SSO 対象システムのログイン画面に対して）対象システムで利用される ユーザID/パスワード を自動入力する方式 対象システムへの全てのアクセスは SSO 基盤を経由する
d	フォーム認証 (クライアントリレー型代理認証)方式	Cのフォーム認証と同様の方式ではあるが、c. と異なり、ログイン画面のみ SSO 基盤を経由する
e	C/S自動ログイン方式	Windows PCにインストールされた専用アプリが、C/Sアプリのログイン画面に対して、対象アプリのユーザID/パスワード を自動入力する方式

※a～d は対象システム：Webアプリの場合 の方式
　e は対象システム　　：C/Sアプリの場合　の方式

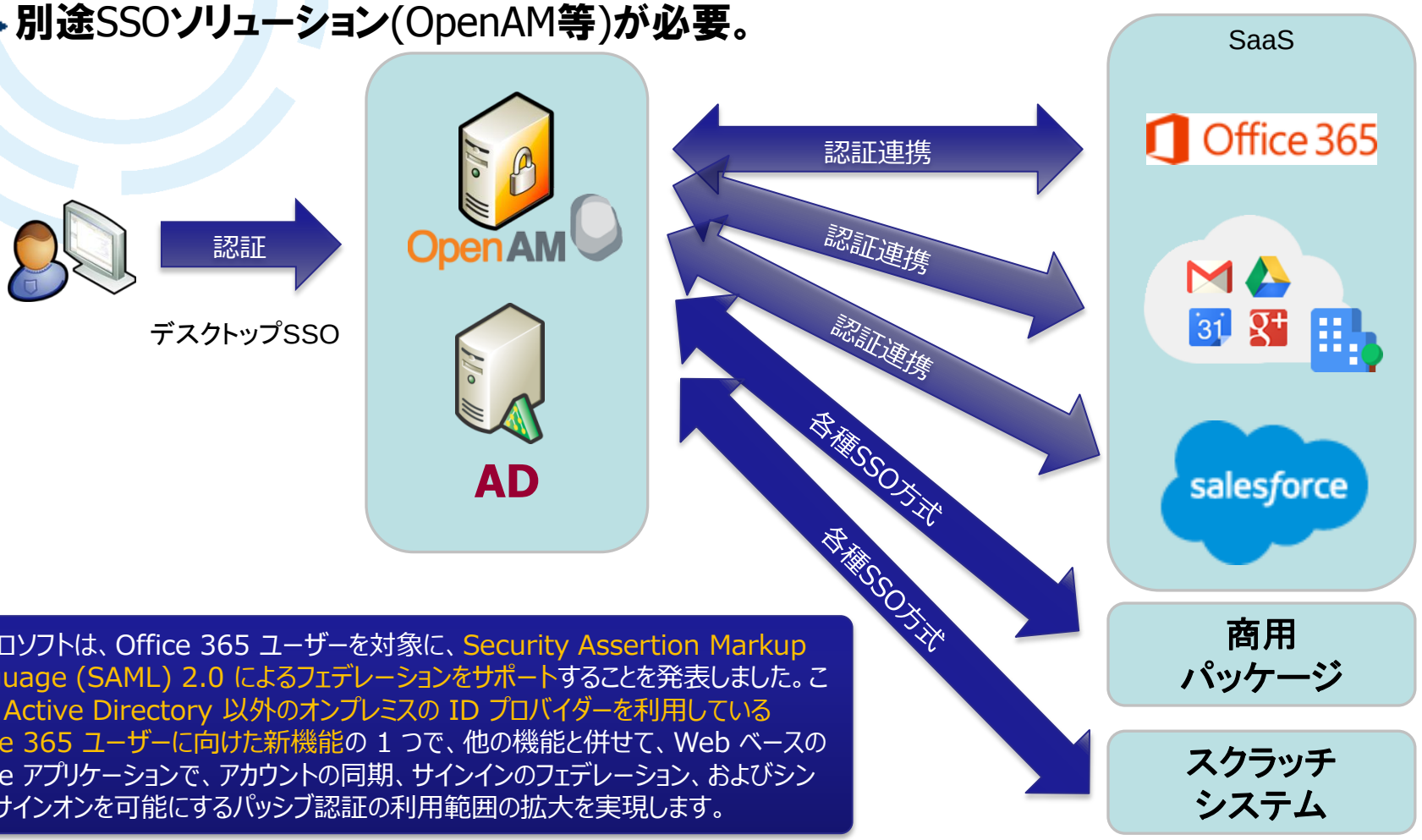
OpenStandia製品紹介
Office365連携

- Office365+SaaSのみを利用する場合
  - AD+ADFSでSSO可能



OpenStandia製品紹介
Office365連携

- **パッケージ(人事、ERP等)やスクラッチ開発アプリも対象とする場合**
  - **別途SSOソリューション(OpenAM等)が必要。**



マイクロソフトは、Office 365 ユーザーを対象に、Security Assertion Markup Language (SAML) 2.0 によるフェデレーションをサポートすることを発表しました。これは、Active Directory 以外のオンプレミスの ID プロバイダーを利用している Office 365 ユーザーに向けた新機能の 1 つで、他の機能と併せて、Web ベースの Office アプリケーションで、アカウントの同期、サインインのフェデレーション、およびシングル サインオンを可能にするパッシブ認証の利用範囲の拡大を実現します。

(出所) http://community.office365.com/ja-jp/b/office_365_community_blog/archive/2014/03/07/office-365-saml-2-0.aspx

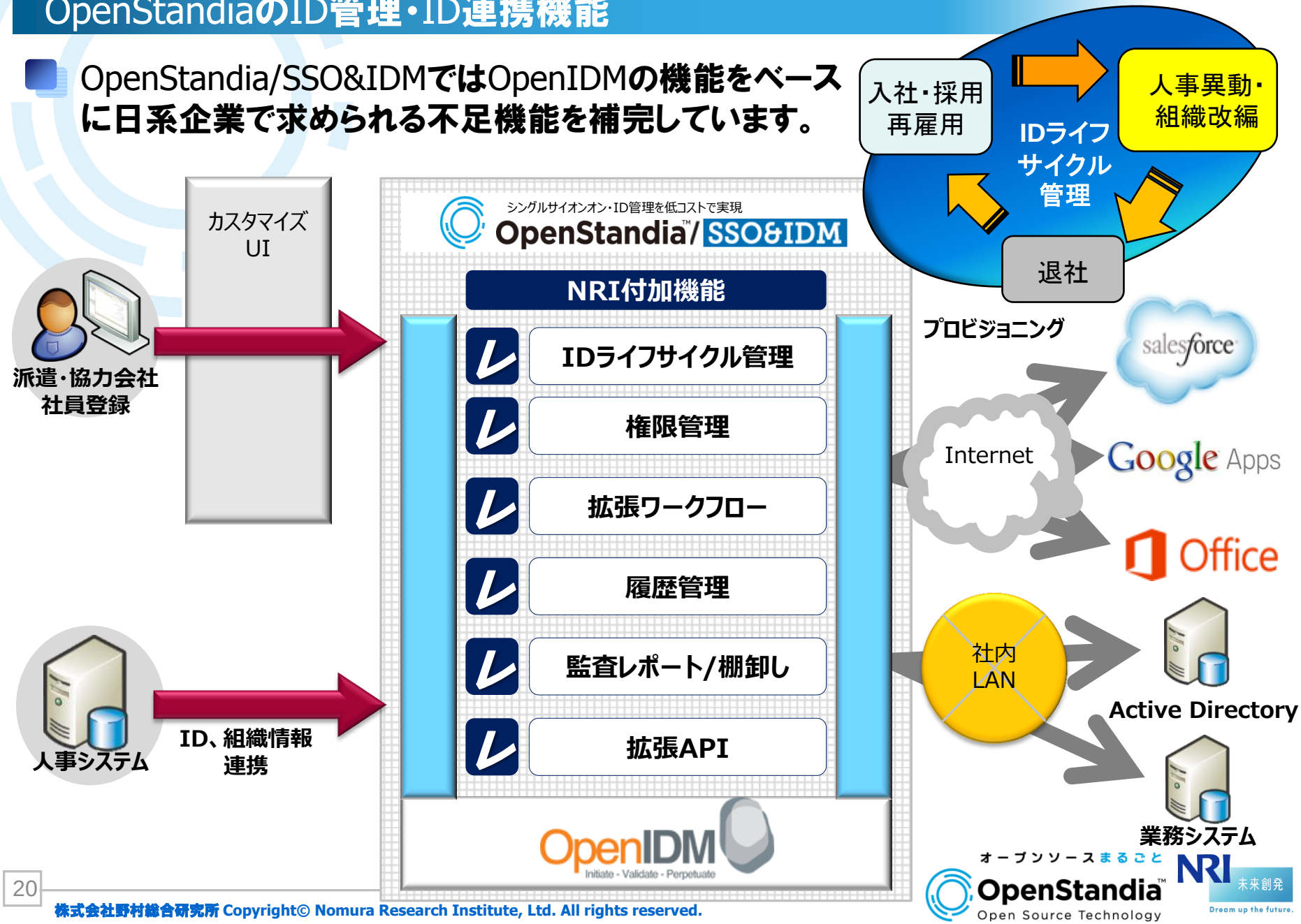
OpenStandia製品紹介
デバイス認証

- OpenStandiaSSO&IDM(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

OpenStandia製品紹介
OpenStandiaのID管理・ID連携機能

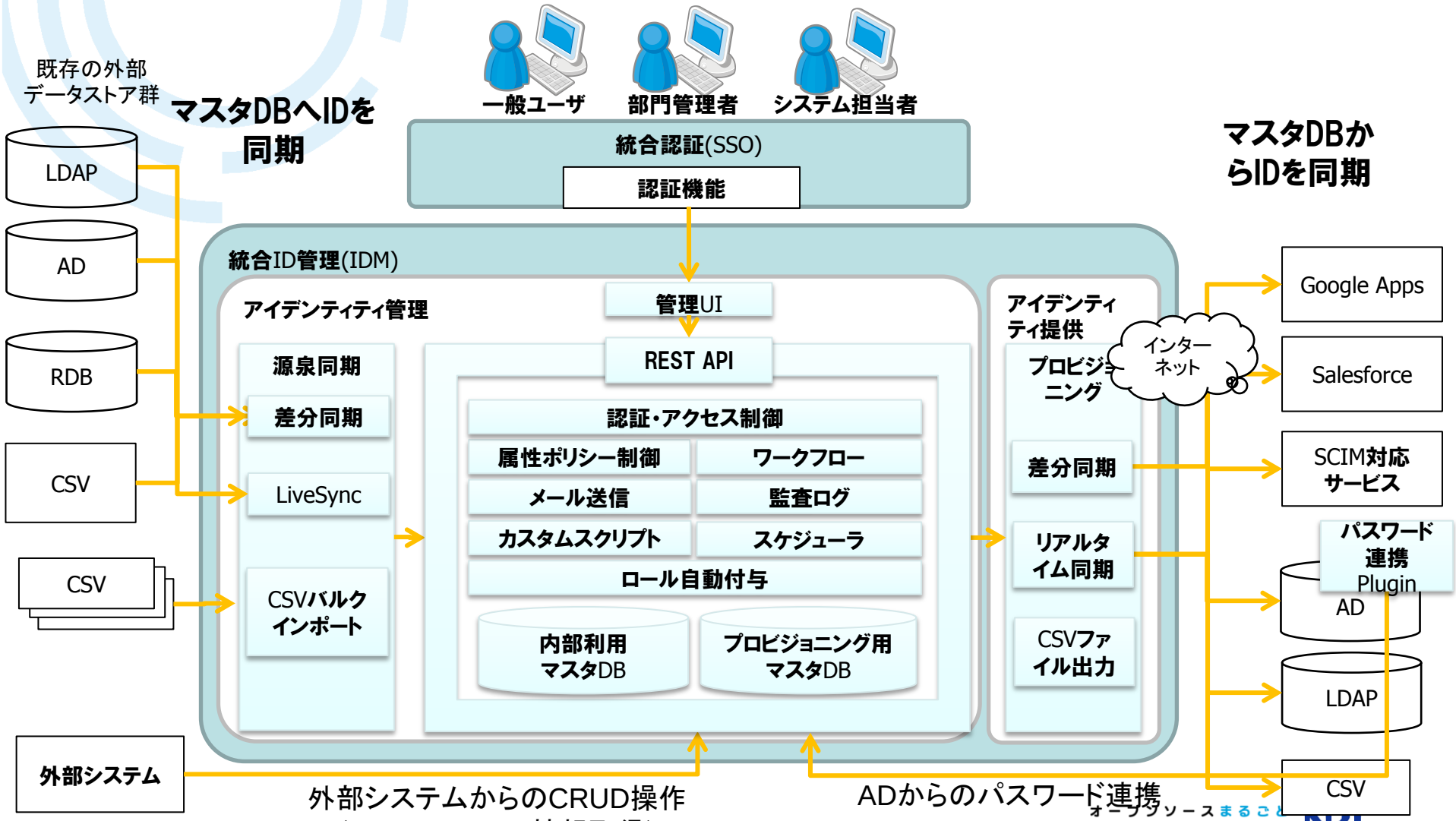
- OpenStandia/SSO&IDMではOpenIDMの機能をベースに日系企業で求められる不足機能を補完しています。



オープンソースまるごと
OpenStandia™
Open Source Technology
NRI 未来創発
Dream up the future.

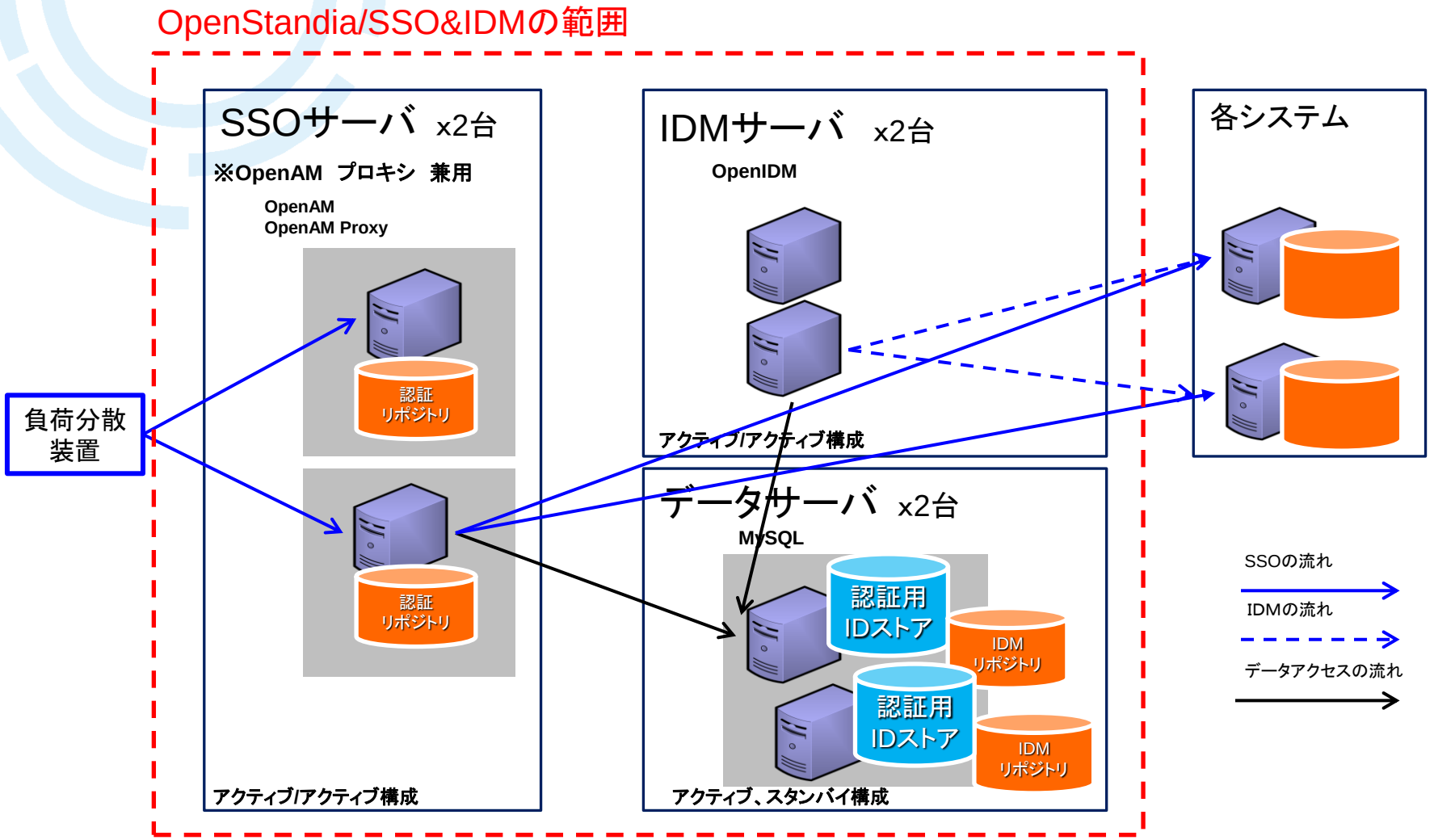
OpenStandia製品紹介
OpenStandia/IDMのアーキテクチャ

IDMは様々なAPIが用意されており、連携方法と拡張性が高いのが一番の特徴です。



OpenStandia製品紹介
サーバ構成例

一般的なサーバ構成案を下記に示します。ご要件に応じて最適化いたします。



目次

プロジェクトの進め方
導入までのスケジュール例

標準的なスケジュール例をご紹介いたします。※業務要件により異なります。

システム化計画フェーズ（2～3ヶ月）

現状把握／課題分析 → システム化方針検討 → システム化計画策定

■統合認証を実現するうえで、最も重要なフェーズ。ユーザ企業主体で如何に要求事項を整理し、ベンダーへ正確に伝えることが出来るかによって、完成するシステムの出来が大きく左右される

- ■ID管理に関わる業務・システムの可視化
- ■現行業務・システムの問題点・要望事項の抽出
- ■スケジュール、体制、概算費用、期待効果のまとめ

ベンダ調達フェーズ（1～2ヶ月）

RFP提示 → 評価基準策定 / 提案書作成 → 提案評価・契約

■ベンダ調達を行うことによって、以下のメリットが得られる。

- ●自社リソースで実施するには負荷が高いパッケージのFit＆Gap分析を提案ベンダに依頼できる
- ●競争原理が有効に機能し、各社から安価な提案を引き出せる（場合によっては戦略的価格を引き出すことが可能）
- ●パッケージ優劣のみならず、ベンダーの力量も評価できる
- ●システム化計画フェーズで算出した概算費用の精緻化が可能

システム導入フェーズ（約3～12ヶ月）

要件定義（詳細） → 設計～導入

目次

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

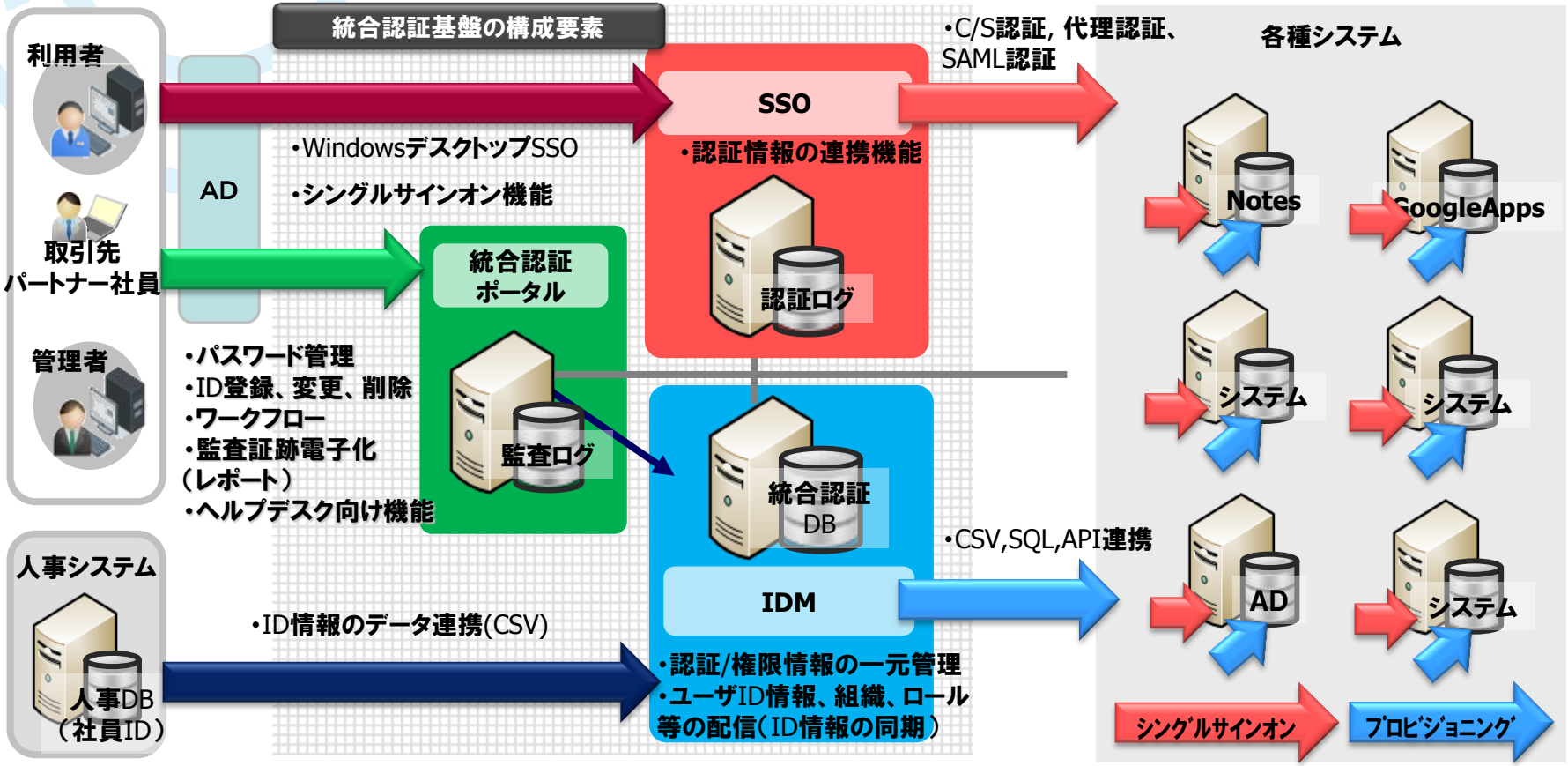
- 現在の各システムの認証の仕組みは個別の技術が使われていること、さらにIDを管理する部署が異なっている場合がある。
- グループウェア、Windowsドメイン、各業務システムの権限情報はそれぞれにあり、管理している。
- 人事異動時期のIDの棚卸し、変更管理作業は運用担当にとって非常に高い負荷である。

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

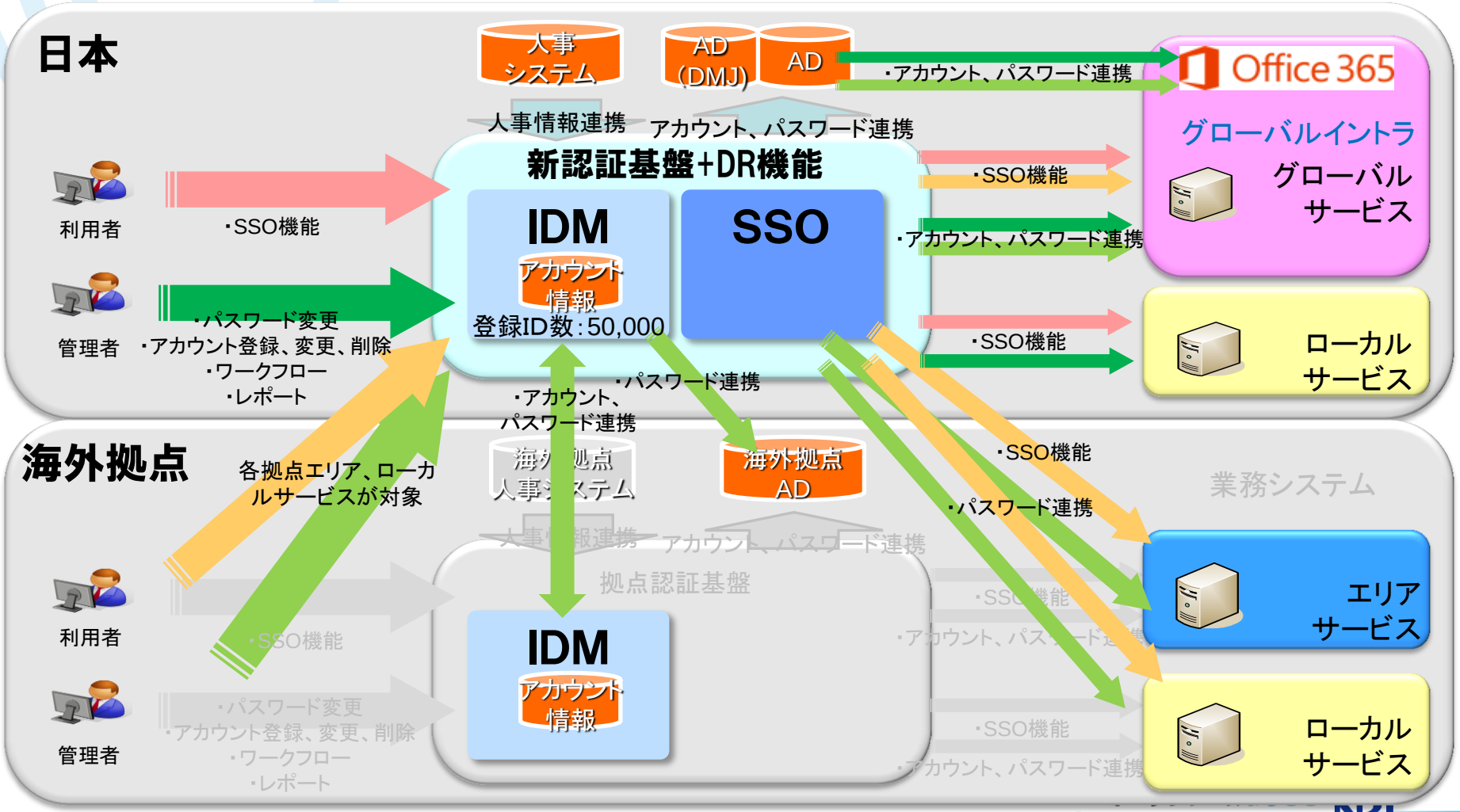
- 拠点ごとに個別で導入したシステムが乱立しており、本社側で管理できない状況にある
- 人事情報を本社と拠点で個別管理しており、IDライフサイクルが管理できていない
- 現地のシステム対応が十分でないため、アクセス権設定、監査ログの取得ができていない

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.

おわりに

2014年07月30日にOpenAM/OpenIDM/OpenDJの提供元の米ForgeRock社とNRIの事業提携をプレスリリースしました。

https://www.nri.com/jp/news/2014/140730.aspx

http://openstandia.jp/solution/id_management/overview/spec.html

http://forgerock.com/news-articles/forgerock-and-nomura-research-institute-enter-strategic-reseller-agreement-to-offer-identity-relationship-management-in-japan/

それに伴い、以下のサービスを開始いたしました。

- レ Enterprise版OpenAM,OpenIDM,OpenDJ,OpenIGの日本国内販売
- レ 上記製品群の日本語でのサポート
- レ 新しく機能強化したOpenStandia/SSO&IDMパッケージ
- レ 技術トレーニング、簡易QA、導入コンサルティングのお手軽パックサービス

- **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.