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

野村総合研究所
OpenStandiaチーム

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 OpenStandiaチーム
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

統合認証基盤（SSO＆IDM）の導入により下記効果が期待できます。

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社内システム利用

- 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 グローバル拠点の対応（統合 × ローカライズ）

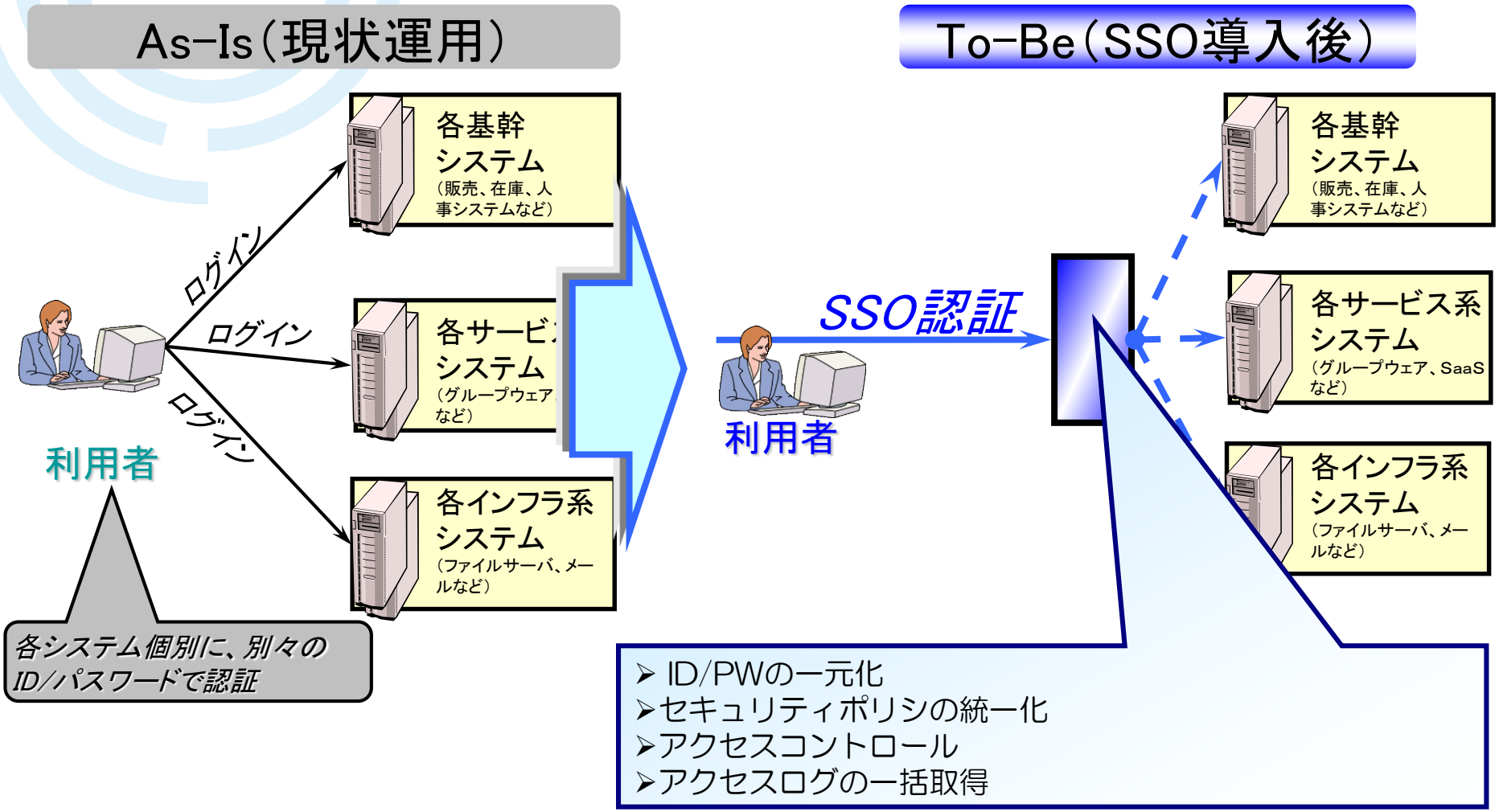
- グローバル拠点のシステム、IDライフサイクルも含めて統一的にID管理
- ローカルサービス、ローカルパッケージとのID連携

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

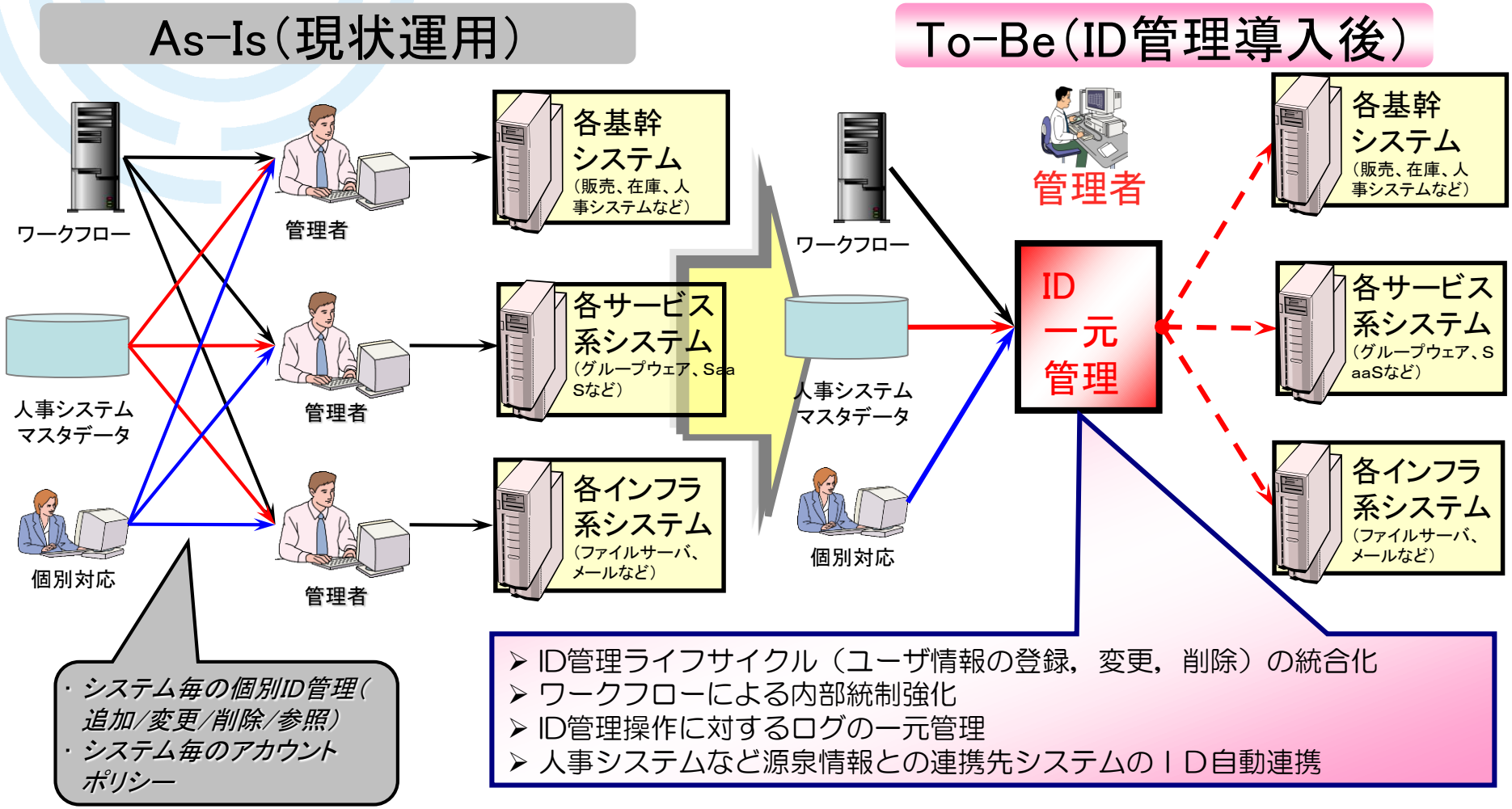
はじめに
シングルサインオン(SSO)について

イントラにおけるSSO導入はユーザ利便性、セキュリティ強化に効果があります。



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）も必要となります。



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

企業にSSO＆IDMを導入するために下記の認識が必要です。

パッケージ導入だけでなく、業務整理が必要な領域

- 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。
- 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

- SSO製品はある程度コモディティ化されてきており、機能差が少なくなってきています。
- 一方でSSOを実現するためのIDM（権限やロール）が考慮されていることが非常に重要です。
- 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
IDMに求められる共通要件

SSO導入はIDMを導入することで効果が高められます。IDM導入顧客のご要件の大部分は共通しています。（画面等は一般的に要件が異なるため個別対応になります）

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

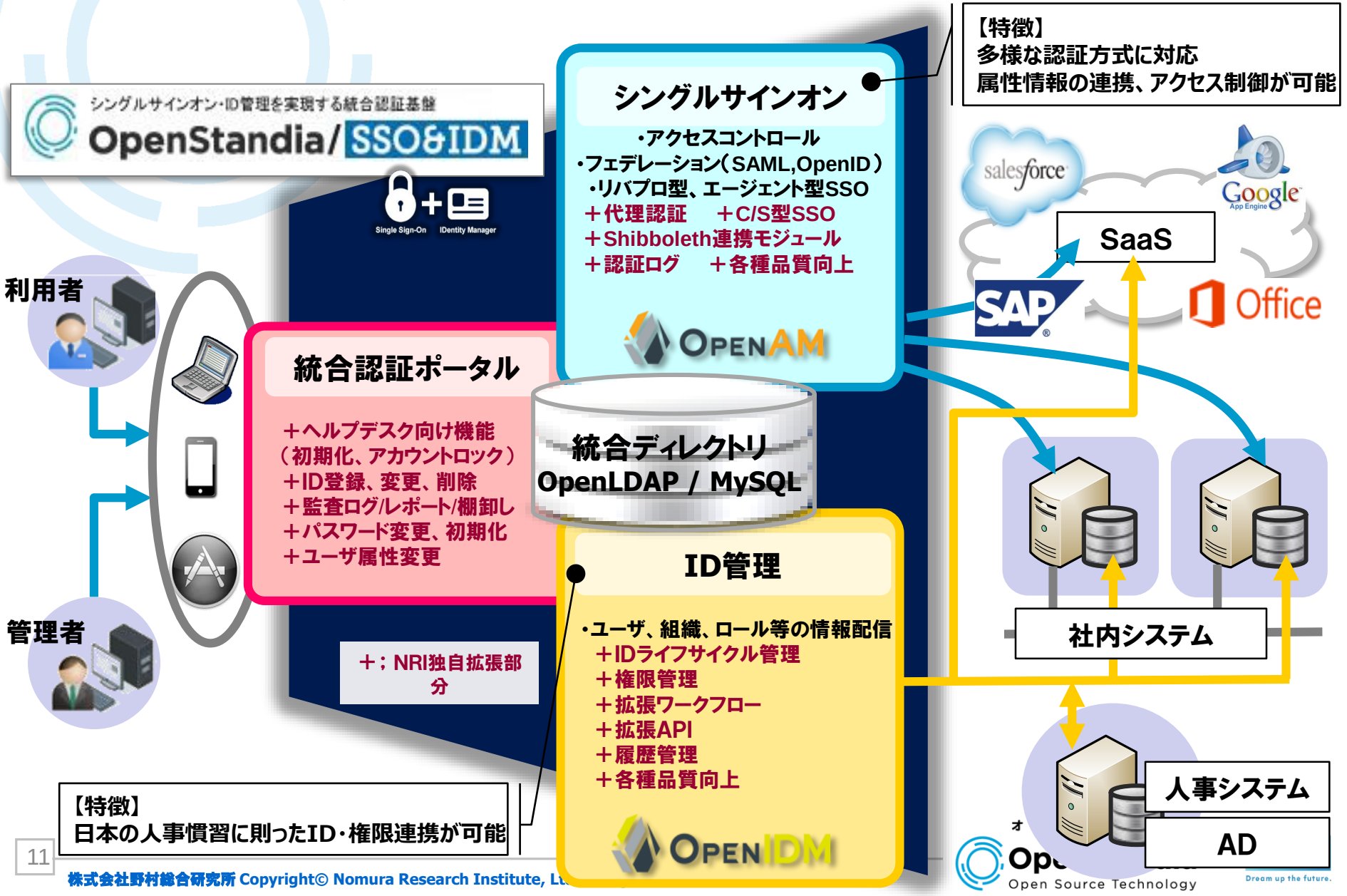
OpenStandia/SSO&IDMはオープンソースをベースにしたSSO/IDM製品です。

- レ **柔軟なシステム拡張性**
- レ **日系企業特有の人事制度、セキュリティ基準への対応**
- レ **システム保守体制**

OpenStandia/SSO&IDMの特徴

システム拡張、個別対応に強い	日系企業特有の人事制度に対応	スピーディでストレスの少ないワンストップ保守体制
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。	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。	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



SSO認証方式の検討

- OpenStandia/SSOでは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
シングルサインオン(SSO)の導入に向けて

- **SSO方式毎の各システムへの影響**
  - **a, b は対象システムがSSO基盤に合わせる方式**
    - ✓ **SSO対象システム側のSSO方式への対応(改修)が必要**
  - **c, d, e はSSO基盤が対象システムに合わせる方式**
    - ✓ **SSO対象システムのパスワードをSSO、IDMで管理することが必要**

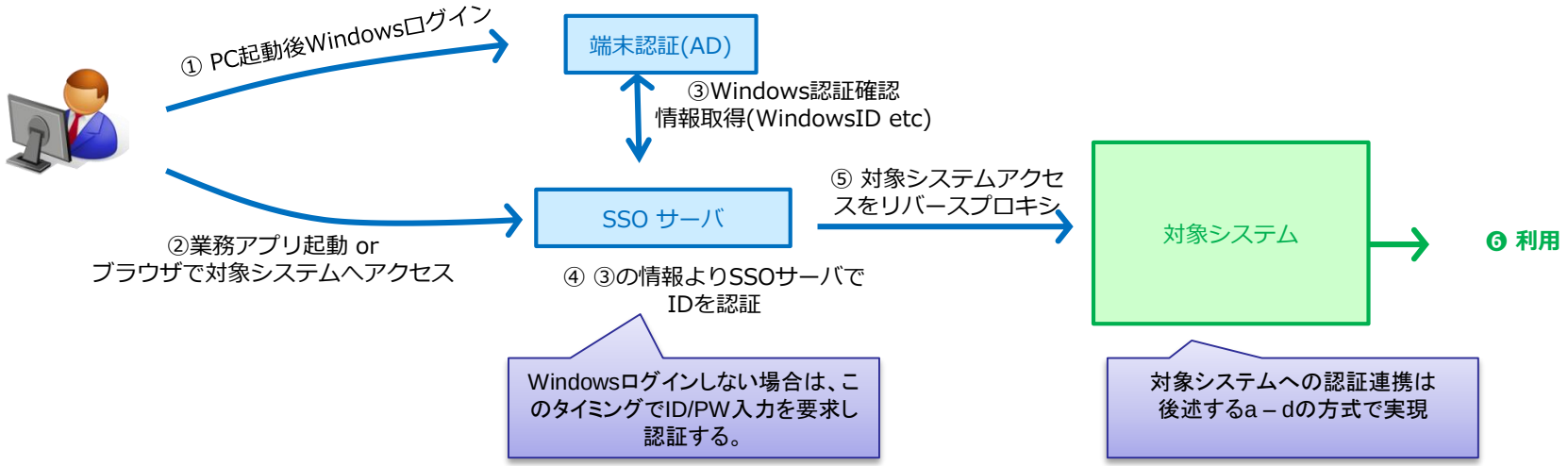
SSO方式	ユーザPC	SSO	IDM	対象システム		
				新規パッケージ	新規スクラッチ	既存システム
a. 公開プロトコル(フェデレーション)	無	小: 対象システムに応じた設定作業	小: 対象システムのユーザIDをSSOサーバに連携	小: 公開プロトコルに対応していれば設定作業のみ 不可: 未対応の場合	小: 公開プロトコル対応前提での開発が必要	中: 公開プロトコルへの対応(改修)が必要
b. リバプロWeb Agent (※)				小: HTTPヘッダ連携に対応していれば設定作業のみ 不可: 未対応の場合	小: HTTPヘッダ連携対応前提での開発が必要	中: HTTPヘッダ連携への対応(改修)が必要
c. フォーム認証(リバプロ型代理認証)(※)		中～大: 対象システムのログイン画面の分析・実機検証が必要 ログイン画面仕様によってはカスタマイズが必要(対応不可の可能性もあり)	小～中:対象システムのユーザIDに加え、パスワードの平文でのSSOサーバへの連携が必要	小: SSO基盤のパスワードポリシーとの整合性を取ることが必要 また、ユーザのパスワードをIDMサーバへの連携方式の検討が必要	小: ログイン画面の仕様、ユーザのパスワードをIDMサーバへの連携方式をSSO基盤で規定すべき	小: SSO基盤のパスワードポリシーとの整合性を取ることが必要 また、ユーザのパスワードをIDMサーバへの連携方式の検討が必要
d. フォーム認証(クライアントリレー型代理認証)						
e. C/S自動ログイン方式	専用モジュールのインストールが必要					

※リバプロ(b, c)型は、対象システムの設計・コンテンツによっては、SSOもしくは対象システムに大規模な改修が必要な可能性があります。

SSO認証方式の検討

- 各システムの認証連携(シングルサインオン)をどのように実現していくか検討します。方式の違いによって SSO・IDM・対象システムへの影響が異なります。
- 統合Windows認証(Windowsデスクトップ SSO)は、Windows認証をSSO基盤に認証連携するベースとなる認証方式です。
- 各連携システム毎に次ページの a-e 方式のいずれかの方式で認証連携を行います。

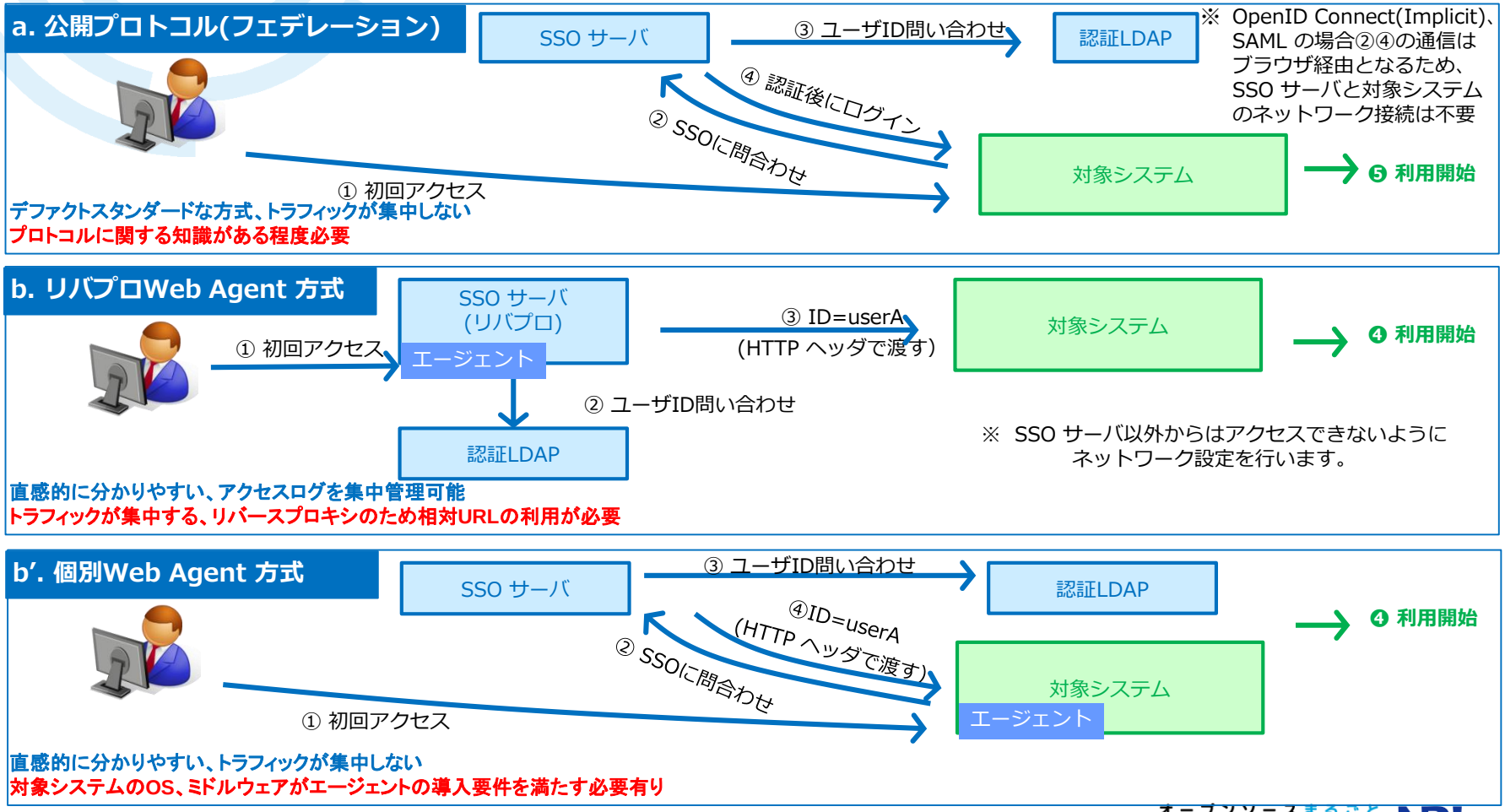
統合Windows認証（WindowsデスクトップSSO） ※ベースの認証方式。これに加え（a-e方式）のどれかを選択することで認証連携を行います。



OpenStandia製品紹介
SSO各方式のフロー

SSO方式の検討

✓対象システムがWebアプリケーションの場合です。



OpenStandia製品紹介
SSO各方式のフロー

SSO方式の検討

✓対象システムがWebアプリケーションの場合です。

c. フォーム認証方式(リバプロ型 代理認証)

① 初回アクセス

SSO サーバ
(リバプロ)

③ 初回アクセス
④ ログイン画面返送
⑤ ID/パスワード送信

対象システム

⑥ 利用開始

② ユーザID/パスワード問い合わせ

認証LDAP

対象システムの変更少、アクセスログを集中管理可能
トラフィックが集中する、リバースプロキシのため相対URLの利用が必要、IDMでのパスワード管理が必須、対応にはログイン画面の解析が必要

d. フォーム認証方式(クライアントリレー型 代理認証)

① 初回アクセス

SSO サーバ

② ログオン画面取得
③ ログイン画面返送

④ ID/パスワード問い合わせ

⑤ ID/パスワードを
POST する
JavaScript を返送

認証LDAP

対象システム

⑥ 利用開始

⑥ 自動的に ID/パスワードを POST

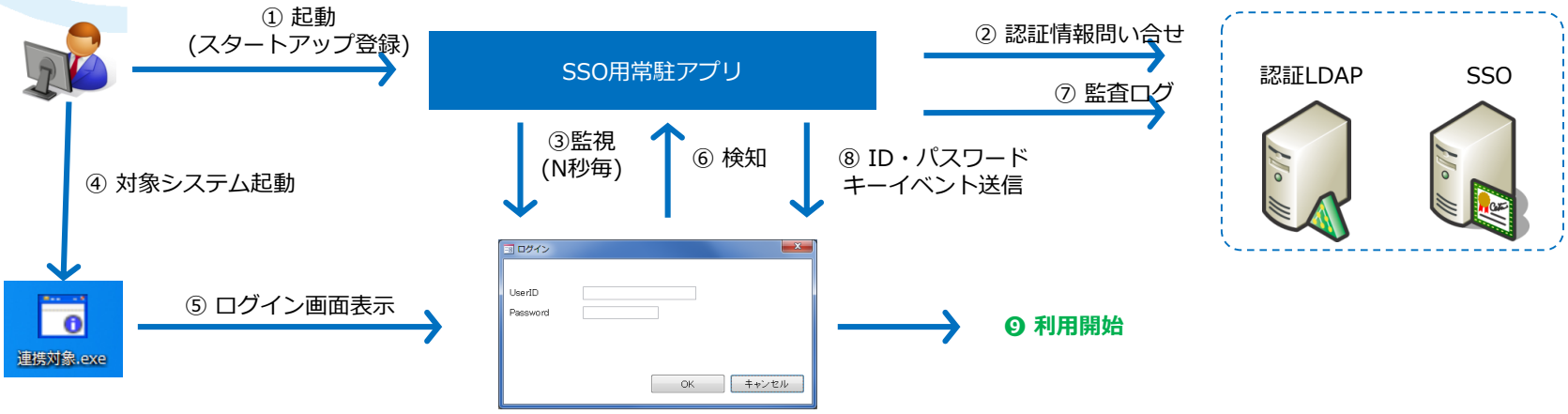
トラフィックが集中しない
IDMでのパスワード管理が必須、対応にはログイン画面の解析が必要、初回直接対象システムにアクセスした場合はログイン画面が表示される

SSO各方式のフロー

SSO方式の検討

✓対象システムがC/Sアプリケーションの場合です。

e C/S自動ログイン方式



※本連携方式にはクライアントPCに専用アプリケーションのインストールが必要になります。

OpenStandia製品紹介
拡張シングルサインオン(SSO)方式

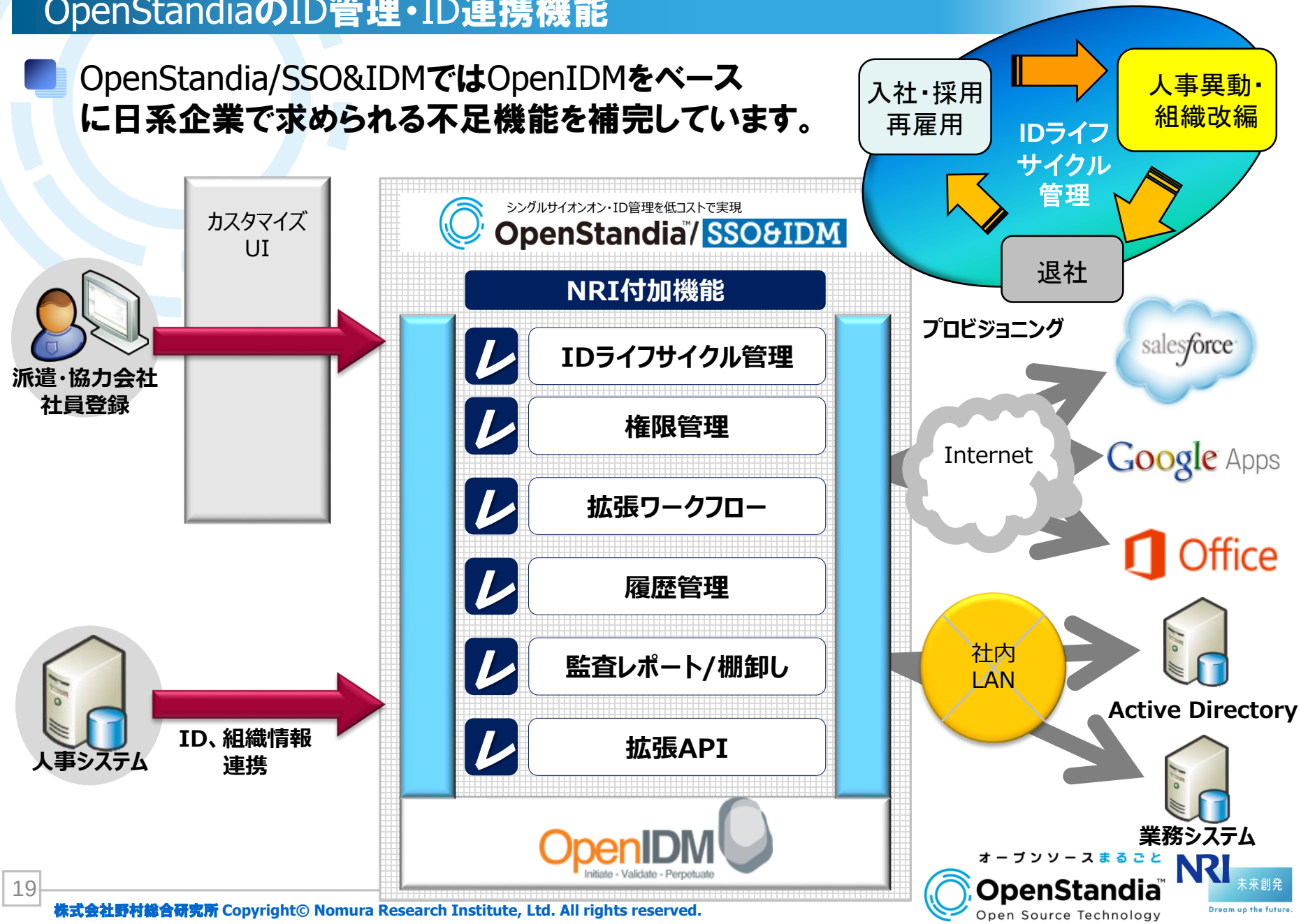
- OpenStandia/SSO&IDMで利用されるOpenAMでは認証・認可・IDプロビジョニング等の各機能をプラグインとして実装
  - 既に様々なプラグインが提供されている
  - 独自にプラグイン開発を行うことも可能

- 既存の主な認証プラグイン

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

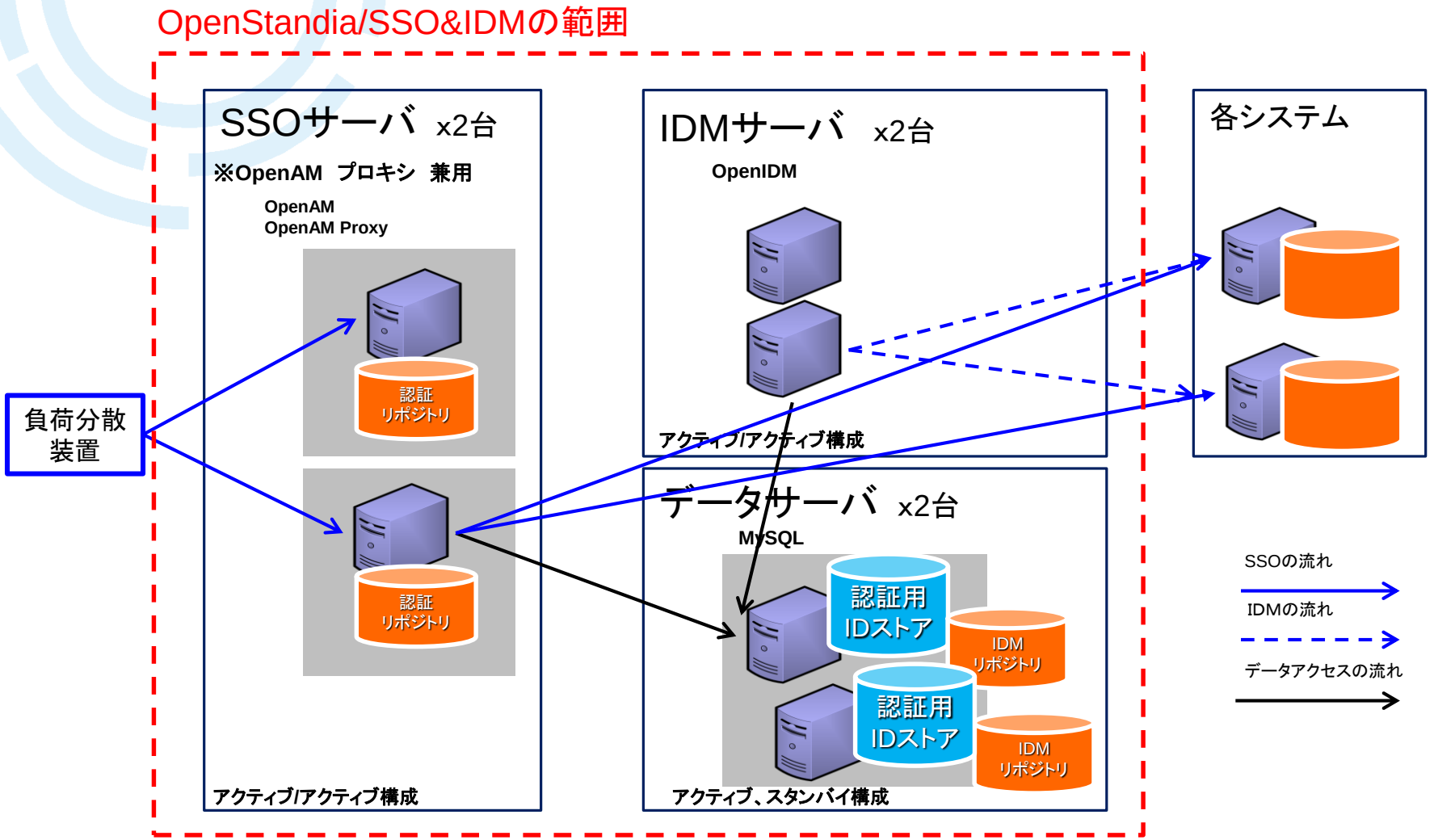
- OpenStandia/SSO&IDMではOpenIDMをベースに日系企業で求められる不足機能を補完しています。



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
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。

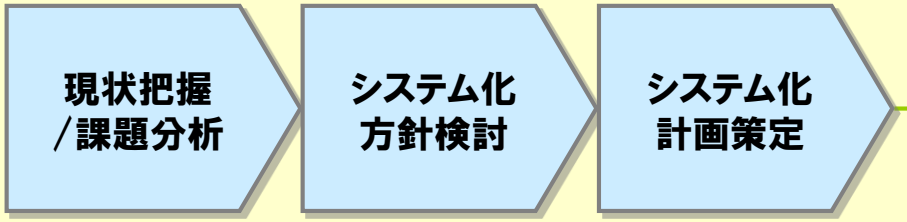


目次

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。

要件定義フェーズ（約2～3ヶ月）



■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管理に関わるシステムの可視化
- ■現行システムの問題点・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

構築フェーズ（約3～12ヶ月）

■前フェーズで決定した方針や要件をもとにシステム実装を行うフェーズ。

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

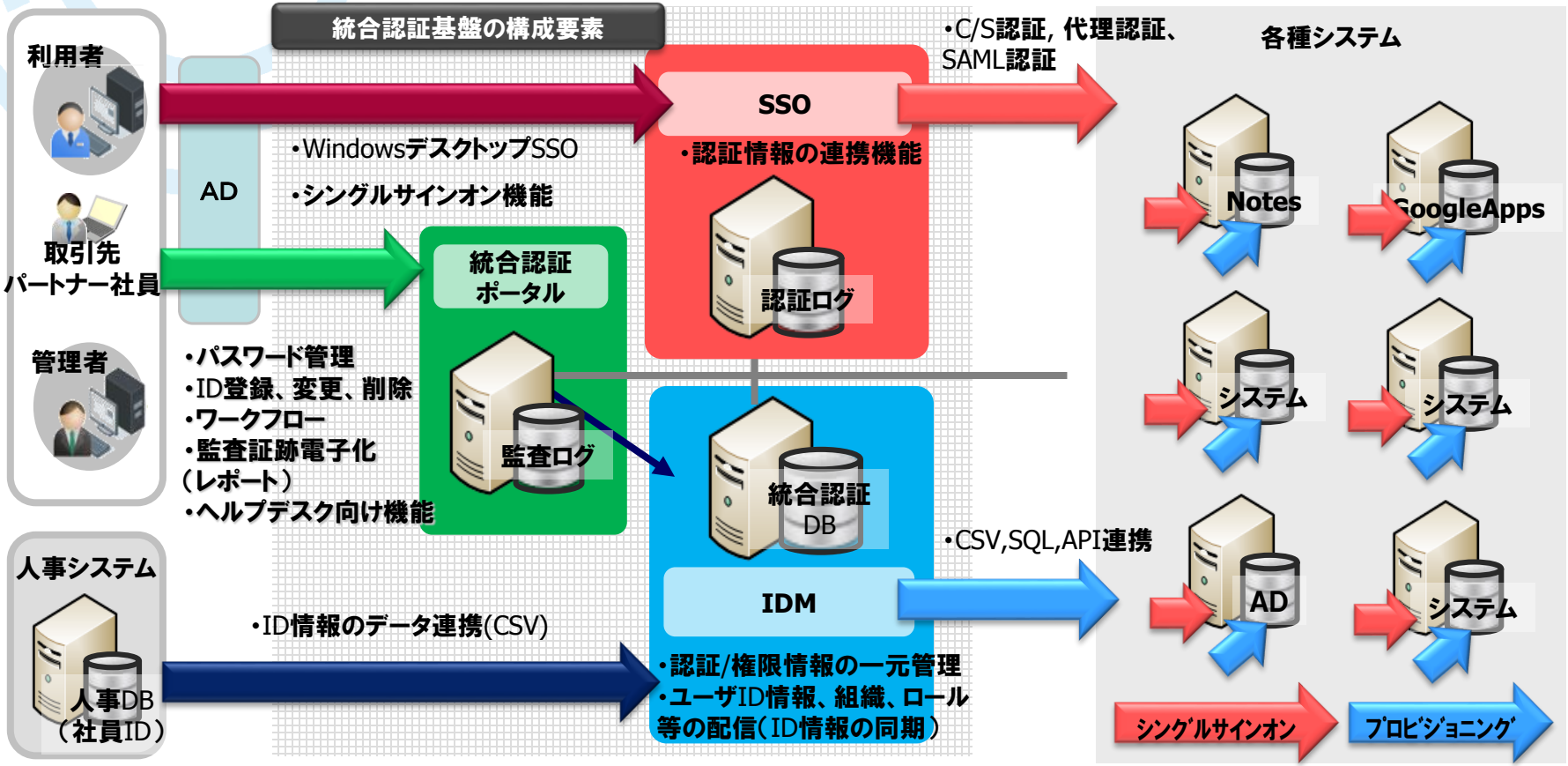
- 現在の各システムの認証の仕組みは個別の技術が使われていること、さらにIDを管理する部署が異なっている場合がある。
- グループウェア、Windowsドメイン、各業務システムの権限情報はそれぞれにあり、管理している。
- 人事異動時期のIDの棚卸し、変更管理作業は運用担当にとって非常に高い負荷である。

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

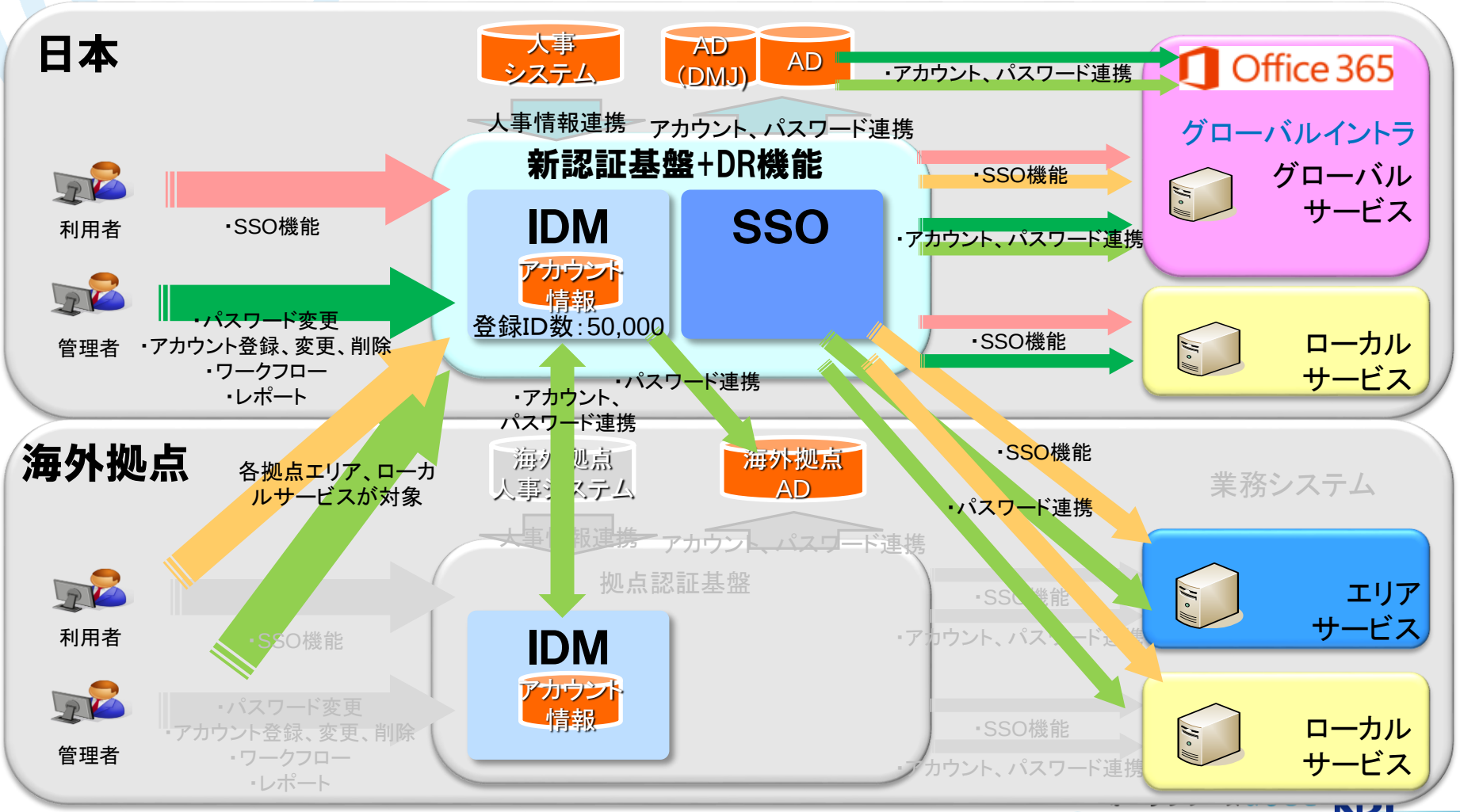
- 拠点ごとに個別で導入したシステムが乱立しており、本社側で管理できない状況にある
- 人事情報を本社と拠点で個別管理しており、IDライフサイクルが管理できていない
- 現地のシステム対応が十分でないため、アクセス権設定、監査ログの取得ができていない

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.

- **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 OpenStandiaへ

ossc@nri.co.jp

http://openstandia.jp/

NRI 未来創発

Dream up the future.

【ご参考】
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	企業でのOSS利用動向
2003年	**オープンソース専門組織の立ち上げ**	OSS OS(Linux)**の普及**
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**	**OSSミドルウェアの普及初期**
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**	**OSS共通アプリの普及初期**
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**	**OSS業務アプリの普及初期**

※赤字は認証、IDに関連する取り組みです。

【ご参考】
OpenAM/OpenIDM開発元のフォージロック社との提携について

NRIはOpenAM提供元のForgeRock社と業務提携しOpenAMエンタープライズ版の提供を開始しました。（ 2014/07/30 ）

提携のポイント①：コミュニティ版の制限

ver9.5.5,10.0.0よりコミュニティ版（CE）のバグFIX、セキュリティパッチ、マイナーバージョンのソースコードが公開されません。CE利用の場合、独自調査でのバグ調査、バグ改修が必要となります。

提携のポイント②：高度なサービス提供

コア部品のバグFIX,パッチ開発はForgeRock社が担当し、NRIは日本企業向けアドオン機能開発や、切り分けからの一括（１次、２次）サポートを提供することにより、より価値の高いサービス提供を目指します。ForgeRockから正式パッチが出るまでの間の暫定パッチもNRIから提供します。

【ご参考】
フォージロック社との提携について

- **提携の概要**
  - ForgeRock製品販売
    - ▶NRIがお客様の代理としてForgeRock社製品サブスクリプションに関する各種手続き、及びForgeRock社への問い合わせを行います。
  - **日本語サポート**
    - ▶NRIが、ForgeRock社製品の日本語サポート窓口を担当致します。
      - ✓1次、2次窓口をNRIで、パッチ開発やソースコードレベルでの調査が必要な3次窓口レベルでのサポートをFR社が担当致します。
      - ✓緊急の場合、NRIから暫定パッチの開発・ご提供も行います。

1次、2次窓口
テンポラリパッチ開発

これまでに培ってきたFR製品に関する技術力は維持します。

【ご参考】
ForgeRock社とNRI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。(http://forgerock.com/)
NRIは日本国内における唯一の販売パートナー。

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

【ご参考】
フォージロック社との提携について

- CE版（Free）とEE版(Subscription)の違い

Benefit	Free	Subscription
Major Releases (e.g. 9.0, 10.0, 11.0)	Development License	Development & Production License
Major Release Source Code	●	●
Community Forums	●	●
Maintenance Releases (e.g. 9.0.1, 10.0.1, 11.0.1)		●
Maintenance Release Source Code		●
Product Support		●
Legal Indemnification		●

【ご参考】
フォージロック社との提携について

NRIとForgeRockとの関係

OpenAMコンソーシアム	2012年 第3回 OpenAMコンソーシアムセミナー　CTO Allan Foster氏来日 2014年 第5回 OpenAMコンソーシアムセミナー　CTO Allan Foster氏来日
カンターライニシアティブ	理事長 ForgeRock CTO Allan Foster氏 理事　NRI 崎村
業務提携、技術交流	2013年　7月 サンフランシスコ ForgeRock本社にて情報交換会 2013年11月 サンフランシスコ ForgeRock本社にて業務提携の意見交換 2014年　2月 サンフランシスコ ForgeRock本社にて業務提携の打合せ 以上、出席者 FR Lasse Andresen CTO、Rich Link VP of corporate & Business Development NRI 崎村、高橋 2014年　2月 横浜 NRIオフィスにAllan Foster氏を招いて技術交換会
コミュニティ活動	OpenAMコミッタ1名在籍 直近3ヶ月のコミット件数 10件、バグ報告件数　15件

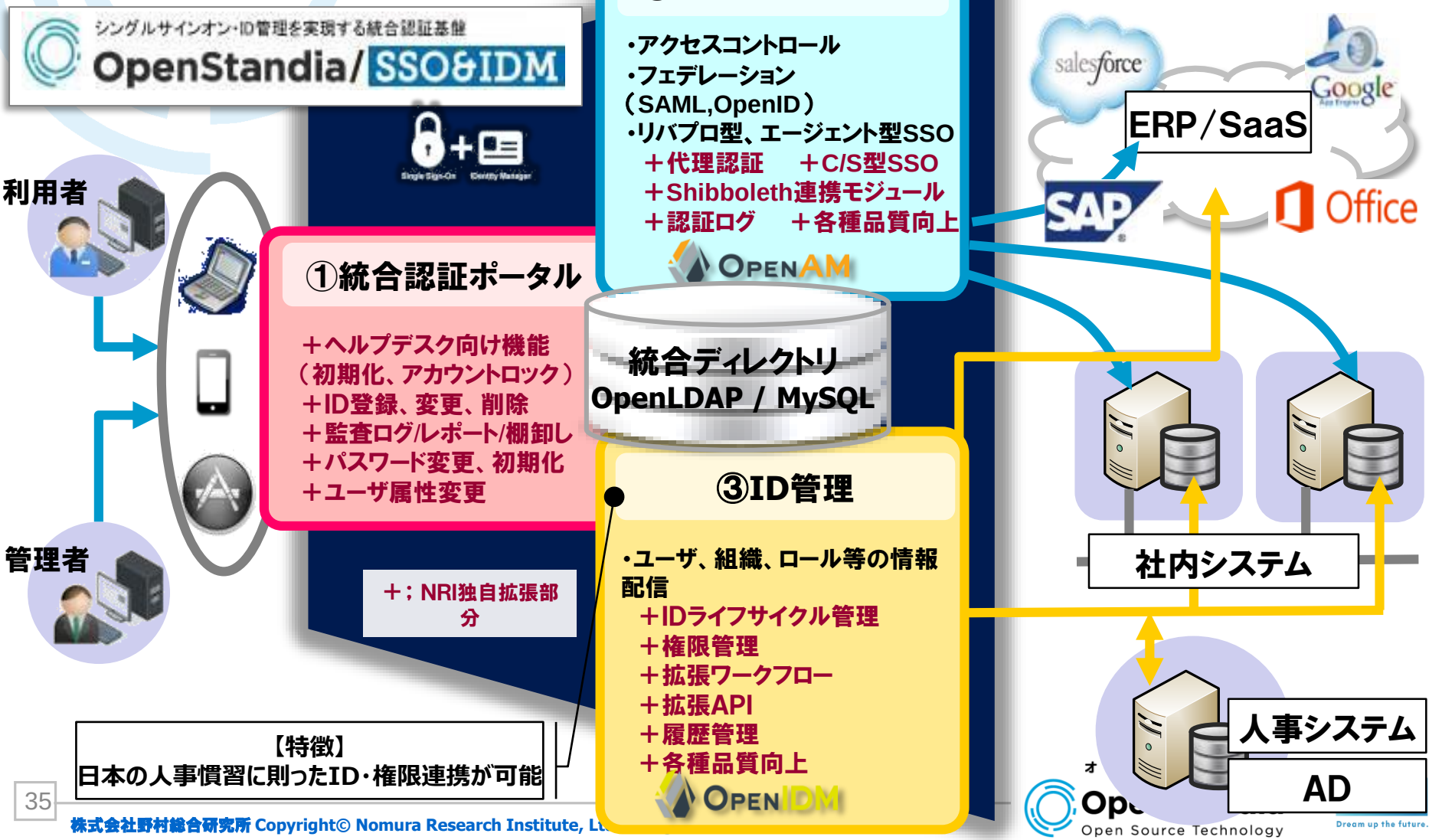
OpenAM コンソーシアム：OpenAMの普及を目的として、OSSTech、オージス総研、NRIが中心となって設立した団体。
会長はNRI 高橋（OpenStandiaチーム）

カンターライニシアティブ：アイデンティティ管理について、業界横断的に規格策定、相互運用を推進するための団体。
NRI 崎村が名付け親かつ理事。

【ご参考】オープンソースによるNRIの統合ID管理・認証基盤ソリューション

OpenStandia/SSO＆IDM 概要

OpenStandia/SSO&IDMはForgeRock版OpenAM/IDMに独自機能をアドオンした製品です。



機能紹介　①統合認証ポータル

【ご参考】OpenStandia／SSO＆IDM機能
①統合認証ポータル（1/3）

#	機能	説明
利用者向け機能		
1	ポータル機能	各機能を統合された画面から利用できるようにする機能。お知らせ機能やファイル共有機能などもある。
2	ダイナミックメニュー機能	CSVデータによるユーザーの一括登録、削除について、ワークフローによる承認を経てからこれを実施する。
3	ユーザ属性変更機能	CSVデータによるユーザーの一括変更について、ワークフローによる承認を経てからこれを実施する。
4	パスワード変更機能	CSVデータによるユーザーの一括変更について、ワークフローによる承認を経てからこれを実施する。
5	マルチアカウントログイン機能	CSVデータによるユーザの一括登録、変更、削除について、CSVデータのフォーマットや値の正当性をチェックする。
6	パスワード忘れ対応（初期化）機能	利用者がパスワードを忘れた際に、利用者自身がパスワードを初期化する。
ヘルプデスク向け機能		
7	ユーザ登録/削除機能	Webブラウザで、ユーザを管理する。
8	組織、ロールの作成、変更	Webブラウザで、組織、ロールを管理する。
9	ユーザへのロール付与	Webブラウザで、ロールをユーザに付与する。
10	ユーザの組織への配属	Webブラウザで、組織にユーザを配属させる。
11	組織ごとに異なるパスワードポリシーの設定	組織ごとに、別々のパスワードポリシーを提供できる
12	パスワード有効期限切れ通知メール機能	利用者のパスワードの有効期限が切れる前（３ヶ月前、１週間前、３日前など）に、自動的に利用者にメールで通知（警告）する。
13	ユーザ検索機能	ユーザを検索する。
14	パスワード初期化機能	利用者からの依頼を受けて、利用者のパスワードを初期化する。
15	アカウントロック/ロック解除機能	利用者のアカウントをロック、及びロック解除する。
16	ユーザー一括登録・更新	CSVデータをアップロードしてユーザを一括登録・更新する機能。

【ご参考】OpenStandia／SSO＆IDM機能
①統合認証ポータル(2/3)

#	機能	説明
システム管理者向け機能		
17	マスタ管理機能	管理者による各種マスタ管理を行うための機能
18	源泉同期・プロビジョニング管理機能	IDの源泉同期・プロビジョニングを画面から実行するための機能
19	リアルタイム同期の再実行機能	エラーとなったIDのリアルタイム同期を、画面から再実行するための機能
20	パスワードポリシーの設定	英字＋数字の混合、８文字以上、など、パスワードを類推されにくくするための機能
21	パスワードの有効期限設定	有効期限が切れたパスワードは使用できなくなる
22	過去利用したパスワードの再利用の禁止設定画面	過去利用したパスワードの再利用の禁止
23	アカウントロックポリシーの設定機能	アカウントロックの有無、アカウントをロックする認証失敗回数の設定、などの設定。
24	アカウントロック自動解除機能	一定時間経過すると自動的にアカウントロックを解除する機能。
人事異動・組織改正向け機能		
25	先日付(未来日付)対応	人事異動・組織改正による変更情報を事前に登録し、管理するための機能
26	適用イベント処理機能	適用開始日を迎えたタイミングで、先日付情報を現在のデータに人事異動・組織改正による変更情報を自動的に反映する機能
27	権限自動付与機能	適用イベント処理にて、ユーザの属性情報(役職など)に応じて自動的に権限を割り当てる機能
28	権限管理機能	組織別の権限情報の管理機能。 管理対象組織のユーザに対して、権限付与・削除を一括で可能な管理画面を提供。
29	履歴管理機能	人事異動・組織改正による変更情報を履歴データとして保持するための機能を提供。参照画面もあり。

【ご参考】OpenStandia／SSO＆IDM機能
①統合認証ポータル(3/3)

#	機能	説明
申請・承認ワークフロー機能		
30	ワークフロー定義	ワークフローの定義のカスタマイズ、連携カスタムスクリプトの定義(承認時にOpenIDMにユーザ登録など)
31	ユーザ申請	ユーザの作成・更新・削除の申請
32	組織申請	組織の作成・更新・削除の申請
33	ダッシュボード(トップ画面)	ワークフローの申請状況やアサインされたタスクをまとめて表示するダッシュボード画面
34	Excel一括申請	Excelファイルをアップロードすることによる一括申請
監査レポート機能		
35	ユーザアカウント一覧	ユーザアカウントの一覧出力
36	管理者権限ユーザアカウント一覧	管理者権限ユーザの一覧出力
37	申請承認イベント一覧	ワークフローの申請・承認情報の一覧出力
38	ユーザ認証成功/失敗ログ一覧	ユーザ認証の成功。失敗ログ出力
39	認可ログ一覧	ユーザ認可のログ出力
40	長期間未ログインユーザ一覧	長期間見ログインユーザの一覧出力
41	パスワード有効期限切れユーザ一覧	パスワード有効期限切れユーザの一覧出力
42	アカウントロックユーザ一覧	アカウントロックユーザの一覧出力
43	棚卸し機能	アカウントの正当性を、各部や利用者本人に確認させる。
44	監査レポート出力機能	監査レポートの出力機能。
45	不正ＩＤ確認機能	統合ＩＤ管理の管理対象外で作成されたＩＤの一覧を表示する。

機能紹介　②認証・シングルサインオン

【ご参考】OpenStandia／SSO＆IDM機能
②認証・シングルサインオン（1/2）

#	機能	説明
認証・シングルサインオン		
1	エージェント型のシングルサインオン	連携先の業務システムに、認証のためのエージェントを組み込むことで、シングルサインオンを実現する。
2	リバースプロキシー型のシングルサインオン	通信経路上のリバースプロキシーに、認証のためのエージェントを組み込むことで、シングルサインオンを実現する。代理認証機能がない場合は、連携先システムに改修が必要になるケースがある。
3	代理認証機能	連携先業務システムの認証画面に対して、ID、パスワードを自動的に代理入力することによって、業務システム側の変更無しにシングルサインオンを実現する。
4	認証失敗時のアカウントロック	認証失敗時のアカウントロック
5	パスワード有効期限切れチェック	有効期限が切れたパスワードでは認証できないようにする
6	初回ログイン時、パスワード初期化後のパスワード強制変更機能	初回ログイン時や、パスワード初期化直後について、パスワードを強制的に変更させる。
7	セッションタイムアウト	システムを一定期間使用していない場合に、自動的にログオフ。
8	アクセスコントロール	ユーザが、URLに対してアクセスを許可するかどうかを設定。通常は、組織や権限（ロール）ごとに設定を行なう。
9	認証ログの記録	日時、ユーザID、成功/失敗、IPアドレスなどのログ出力
10	認可ログの記録	認可情報のログ出力(アクセスコントロール設定されたURLに対して、許可・禁止の出力)
11	エージェント型のシングルサインオン	連携先の業務システムに、認証のためのエージェントを組み込むことで、シングルサインオンを実現する。
12	リバースプロキシー型のシングルサインオン	通信経路上のリバースプロキシーに、認証のためのエージェントを組み込むことで、シングルサインオンを実現する。代理認証機能がない場合は、連携先システムに改修が必要になるケースがある。
13	代理認証機能	連携先業務システムの認証画面に対して、ID、パスワードを自動的に代理入力することによって、業務システム側の変更無しにシングルサインオンを実現する。
14	認証失敗時のアカウントロック	認証失敗時のアカウントロック

【ご参考】OpenStandia／SSO＆IDM機能
②認証・シングルサインオン（2/2）

#	機能	説明
認証・シングルサインオン		
15	パスワード有効期限切れ	有効期限が切れたパスワードでは認証できないようにする
16	初回ログイン時、パスワード初期化後のパスワード強制変更機能	初回ログイン時や、パスワード初期化直後について、パスワードを強制的に変更させる。
フェデレーション		
17	SAML2.0対応	フェデレーションを実現するための、業界標準の認証プロトコル「SAML2.0」への対応。SAML2.0に対応しているSalesforceCRM、GoogleApps、Office365などとのシングルサインオンが可能に。
18	SAMLエージェント	連携先の業務システムを、「SAML2.0対応」にするためのエージェント。
19	C/SシステムとのSSO	C/Sシステムとのシングルサインオン。
20	OAuth2 Server対応	業界標準の認可プロトコル「OAuth2」のサーバ機能。
21	OpenID Connect対応	フェデレーションを実現するための、業界標準の新しい認証プロトコル「OpenID Connect」への対応。
認証モジュール		
22	WindowsデスクトップSSO	Windowsドメインへの認証をもって、連携先の各業務システムや、クラウド/SaaSなどへシングルサインオンする機能。
23	RDB認証	MySQLやOracle等任意のRDBを利用した認証機能
24	リスクベース認証	事前定義したチェック内容により、多要素認証に動的に切り替える機能。
25	OATH認証	オープン認証規格OATHのOTPへの対応。 (ワンタイムパスワードの標準規格への対応)
26	OAuth2 Client認証	業界標準の認可プロトコル「OAuth2」を利用した認証への対応。
27	OpenIDM認証	OpenIDMを認証サーバとして使用するための機能

機能紹介　③ID管理

【ご参考】OpenStandia／SSO＆IDM機能
③ID管理

#	機能	説明
ID管理		
1	CSV、AD、LDAP、RDB(Oracle、MySQLなど)からの源泉データの取り込み	源泉データをIDMのID情報に同期する。
2	CSV、AD、LDAP、RDB(Oracle、MySQLなど)へのプロビジョニング	IDMのID情報と、各システムのID情報とを同期する。
3	SalesforceCRM、GoogleAppsなどへのプロビジョニング	IDMのID情報と、各システムのID情報とを同期する。
4	その他のシステムへのプロビジョニング	IDMのID情報と、各システムのID情報とを同期する。
5	リアルタイム同期	リアルタイム同期
6	ADパスワードのリアルタイム同期	ADのパスワード変更を、統合認証DBにリアルタイム同期
7	パスワードの暗号化	パスワードを暗号化してリポジトリに格納する
8	監査ログ記録	ユーザ、組織などの更新情報の記録 プロビジョニング情報の記録
9	アクセスコントロール	IDMに対するURLベースのアクセスコントロール機能
10	発番機能	定義したルールに従いIDを発番するための機能
11	メール送信機能	メール送信機能