OpenStandia/SSO&IDMのご紹介
～グローバル拠点のシングルサイオン、統合ID管理～

2014/07/25

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.

はじめに
グローバル企業が抱える構造的な課題（一般論）

本社期待と拠点実態の乖離は大きく、グローバルにおけるITの有効活用は思うように進展していないケースが多くみられます。海外単独で頑張ろうにも、リソース（金・人）と権限では対応に限界があるのが多くの日系企業での現状です。

グループ本社	地域統括会社	事業会社
ITガバナンスを強化したい セキュリティ・コンプラ対策は必須	中国・アジアと一括りにされても困る国・地域によってIT事情は異なる	重要なのはわかるけど、抽象的な指示では現場は回らない 理想と現実にギャップがありすぎ
拠点単体の部分最適でなく、グローバルに全体最適を達成したい。 事業の効率性を上げたい	簡単に言うけど、言葉の壁もあるし、人件費・教育水準も全然違う	自社のシステム化で手一杯。自社ITスタッフと地元のベンダーに頼むのが一番手っ取り早い（部分最適）
システムを統合・共有化してコスト削減したい	統合化＝コスト削減にはならないコスト高になっても統合すべきものは何かという視点で考えないと	ネットワーク費用・品質などを考えると、無理してIT化するよりも人手の方が安くて確実
国内システム案件で手一杯で海外（アジア）まで手が廻らない	カンパニー制、出資形態の問題などから、地域統括の言うことはなかなか聞いてくれない	やりたいことはいっぱいあるが、人も金も出てこない でも口は方々から出てくる

はじめに
グローバル企業が抱える構造的な課題（一般論）

グローバルにおけるITソリューション戦略のポイントは下記と考えています。

ITガバナンスの強化

- **同一ソフト**を全拠点で利用
- **汎用的なパッケージソフト**を横展開して有効活用

拠点経営の「見える化」、「所有」から「利用」で実現

- 拠点に**IT専任スタッフがいなくても**システムが利用可能であること
- **自社で資産をもたず**、拠点規模にあった投資

全体最適オペレーションの実現に向けた基礎作り

- 各拠点のデータを収集・活用。グローバルに同じ精度・粒度のデータを管理

はじめに
グローバル企業が抱える構造的な課題（一般論）

グローバルビジネスにおけるオープンソースの優位点

グローバルスタンダードなアーキテクチャ

- **グローバルスタンダード**なアーキテクチャであり、SaaS等との連携も可能
- **多言語対応**や**マルチ通貨対応**等が初めから実装されている

ローカライズ対応、現地メンテナンスも可能

- ソースが公開されているため、**ローカライズ実装が可能**である
- 情報がオープンであるため、**各国での技術者が確保しやすい**

コストモデルがグローバル展開に適している

- 無料、もしくは比較的**リーズナブルな価格設定**（サポート等）となっている
- **ユーザ数に比例しないコスト構造**になっているプロダクトが多い（※）

※プロダクトに依存します。

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
環境変化に対する企業の対応

環境変化は企業の対応次第で「機会」にも「脅威」にもなり得ます。

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

業務最適化、内部統制強化、運用コスト削減を満たす対策として、
統合認証基盤（SSO＆IDM）の導入・活用が1つの有効対策となります。

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）

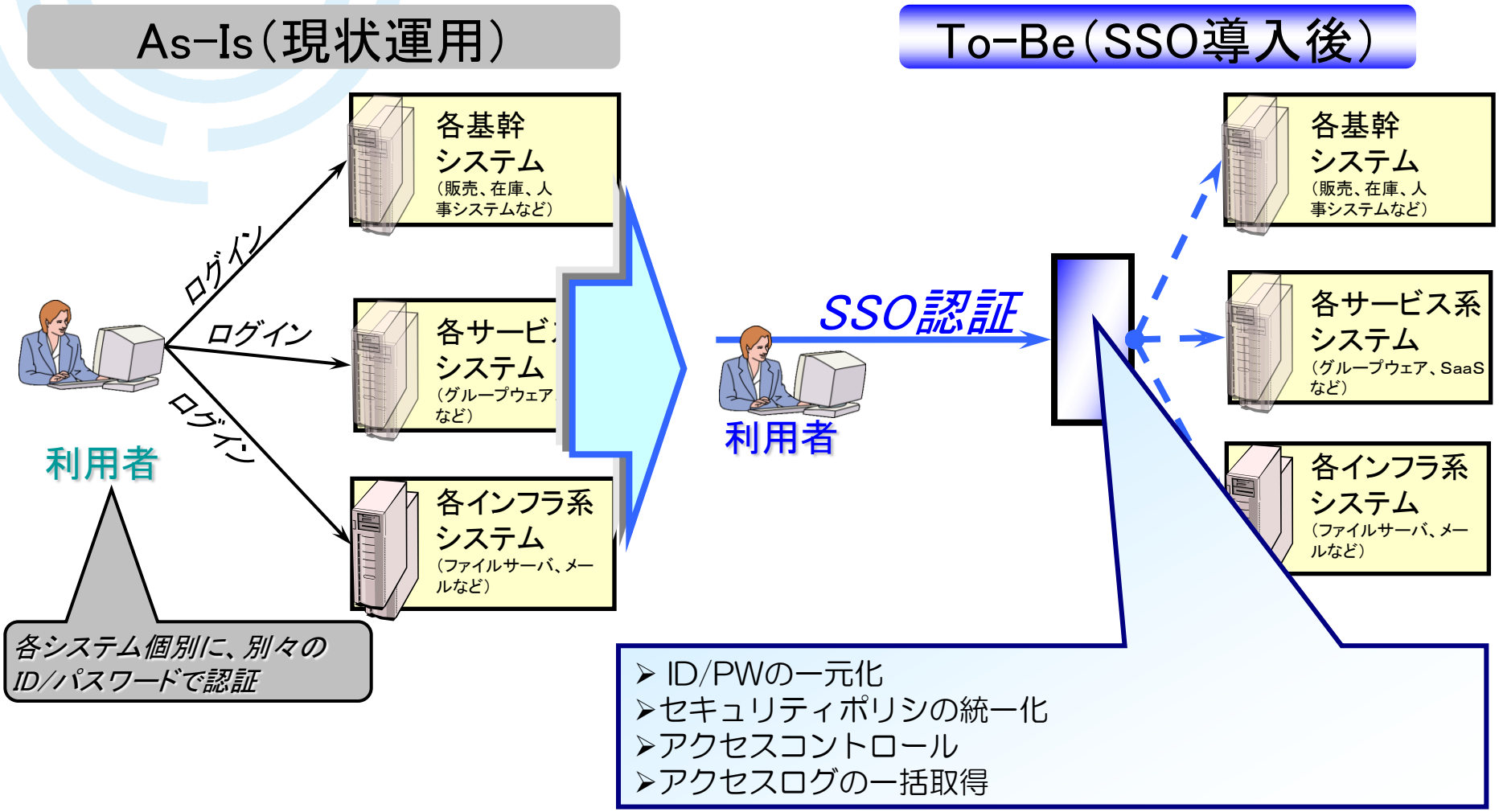
- 日本本社、グローバル拠点のシステム、IDライフサイクルを統一的に管理
- ローカルサービス、ローカルパッケージとのID連携

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

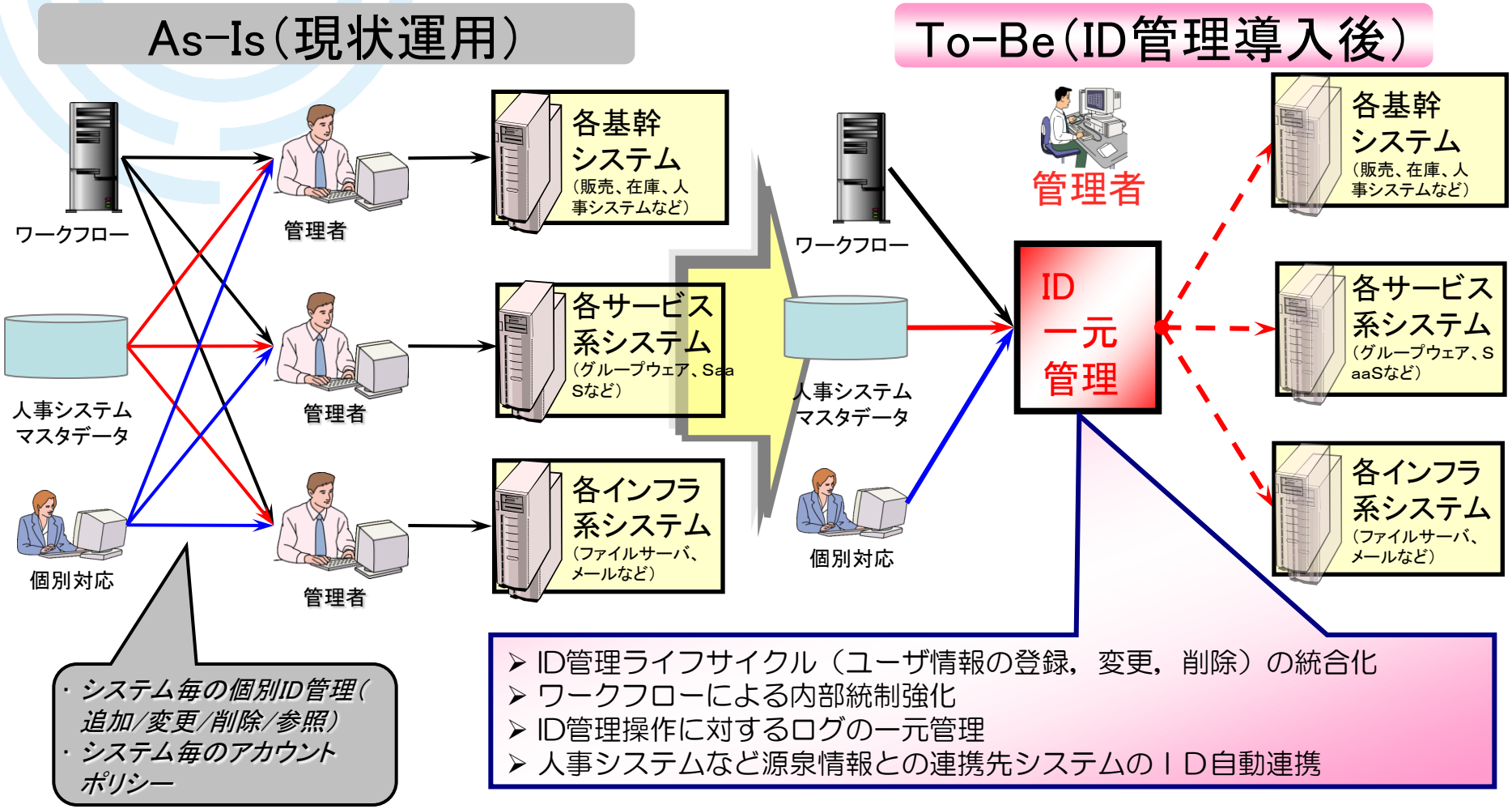
はじめに
シングルサインオン(SSO)について

シングルサインオン(SSO)とは1回の認証で複数のシステムに同時認証する仕組みです。



はじめに
アイデンティティ管理(IDM)について

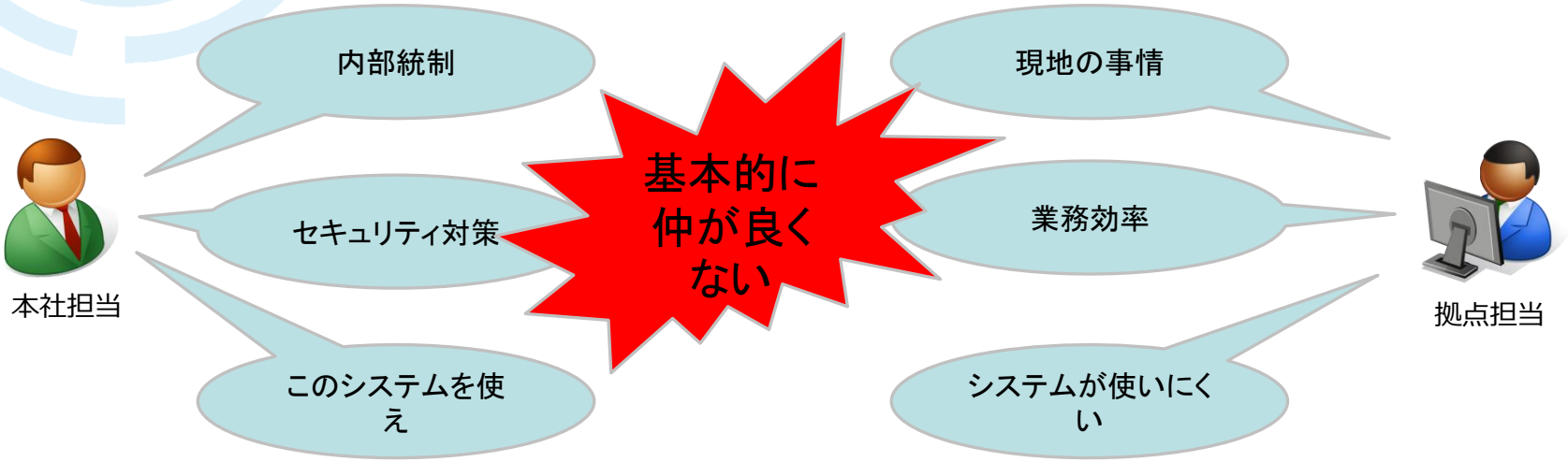
アイデンティティ管理(IDM)とはID/PWを含む、人、組織、権限等の情報管理のことです。



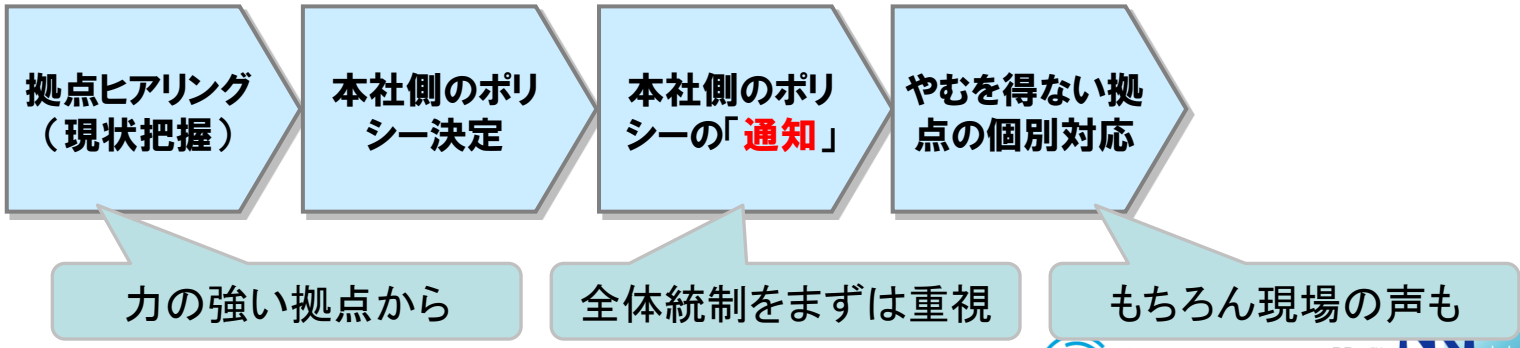
目次

プロジェクト推進に要求される要件とOpenStandiaの優位性
本社と拠点の関係

本社と拠点の主張は大体ぶつかるため、力関係にもよるが妥協点を探す活動になる。SSO＆IDM導入は「統合プロジェクト」であるため、本社主体のプロジェクトにするのが望ましい。

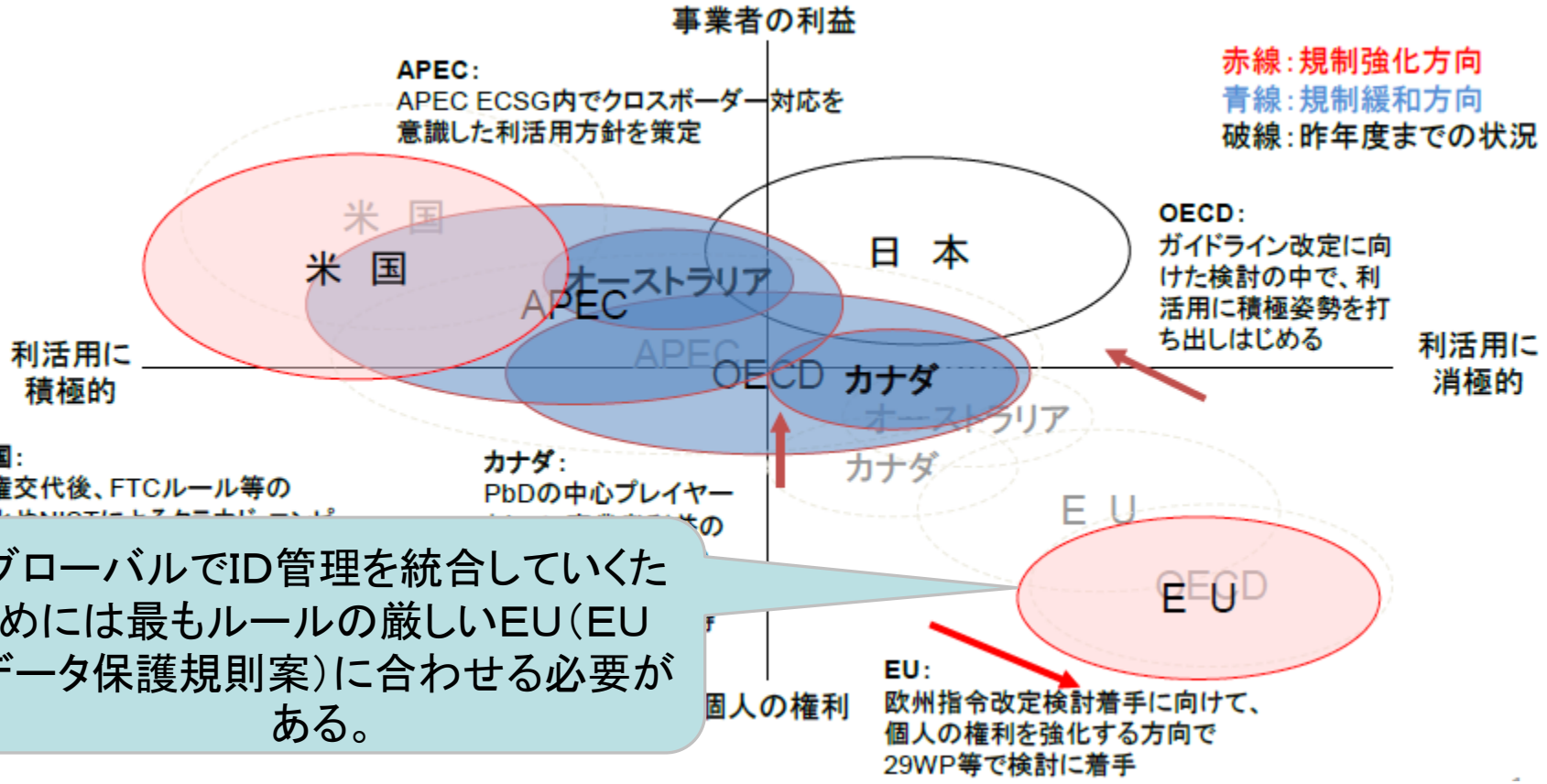


グローバルSSO＆IDMプロジェクトのモデルケース



プロジェクト推進に要求される要件とOpenStandiaの優位性
グローバルでの個人情報の扱い

- 世界各国において、個人情報に関する議論が積極的に行われている中で、経済通産省資料ではパーソナルデータの活用が新産業創出に重要な役割を果たすと明示している。一方で規制に対する各国の方向性は多種多様となっている。



グローバルでID管理を統合していくためには最もルールの厳しいEU(EUデータ保護規則案)に合わせる必要がある。

出展:パーソナルデータに関する海外動向(経済通産省)

プロジェクト推進に要求される要件とOpenStandiaの優位性
EUデータ保護規則

日本の「個人情報保護法」と「EUデータ保護規則」を比較して注目すべきは、「EUデータ保護規則」ではEU内の個人情報はEU外（例：日本）に保持してはならないこと。

【参考】 日本の個人情報保護法とEUデータ保護規則の比較

日本の個人情報保護法は、以下に挙げるような多くの点で、EU 規則案よりも規定が緩やかでああると言える。

- 対象事業者（個人情報取扱事業者）の範囲が狭い
- 第三者提供など一定の場合を除いて本人の同意取得が必要とされていない
- 特定カテゴリの情報（特定機微情報）の取扱いに関する規定がない
- 開示・訂正・消去請求権が本人の権利として明示的には認められていない
- ダイレクトマーケティングに対する異議申立の権利がない
- プロファイリングを受けない権利の規定がない
- 個人情報漏洩時等の報告・連絡義務がない
- 第三国への個人情報移転を禁じていない
- 独立的な監督機関（第三者機関）に関する規定がない
- 司法救済を求める個人の権利が規定されていない 等

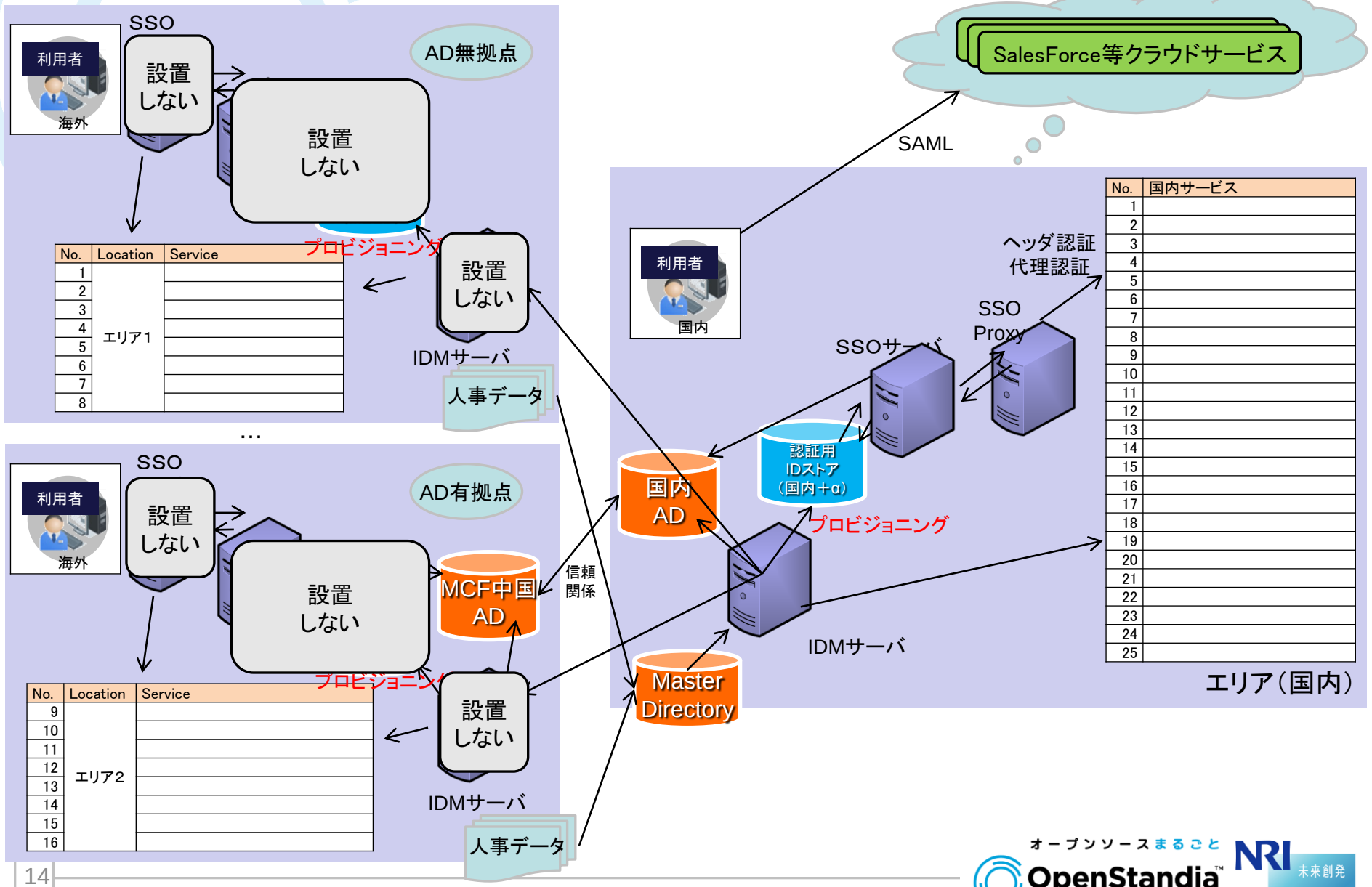
出展：パーソナルデータに関する海外動向（経済通産省）

一方で「個人情報」の定義は非常に曖昧（ID、メアド、パスワード、電話番号、生年月日、IP・・・。

各社毎に「個人情報」を定義・判断しているのが実情。

某社プロジェクトでは・・・
会社メアド、社内パスワード、社員番号等、「会社に属している限りにおいてのみ個人を特定できる情報」は個人情報ではないと定義して日本のデータセンターに情報保持

プロジェクト推進に要求される要件とOpenStandiaの優位性
サーバ群のリージョン分散　vs　サーバ群の日本集約（１／２）



プロジェクト推進に要求される要件とOpenStandiaの優位性
サーバ群のリージョン分散　vs　サーバ群の日本集約（２／２）

「耐障害性、性能等の非機能要件」と「拠点展開のしやすさ」が議論の争点。
拠点毎にシステムを構築するのではなく、システムは日本側で集約し、拠点展開スピードを重視して、案5の拠点側での最小構成（日本側に集約する）を採用。

グローバルシステム構成案	拠点側のサーバー構成				特徴				備考
	ローカルIDストア（LDAP）	認証サーバ（OpenAM）	ローカルID管理サーバ（IDM）	プロキシサーバ（OpenAM Proxy）	耐障害性（サーバ）	耐障害性（ネットワーク）	性能（IDM）	性能（SSO）	
案1	有	有	有	有	○	○	○	○	最大構成
案2	有	有	無	有	△	○	×	○	
案3	無	無	有	有	△	×	○	△	
案4	無	無	無	有	×	×	×	△	
案5	無	無	無	無	×	×	×	×	最小構成

プロジェクト推進に要求される要件とOpenStandiaの優位性
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とOpenStandiaの優位性
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。

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

プロジェクト推進に要求される要件とOpenStandiaの優位性
OpenStandia/SSO&IDMの特徴

最適なSSO＆IDMパッケージを選択するためのポイントとは下記ととらえています。

- 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

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。

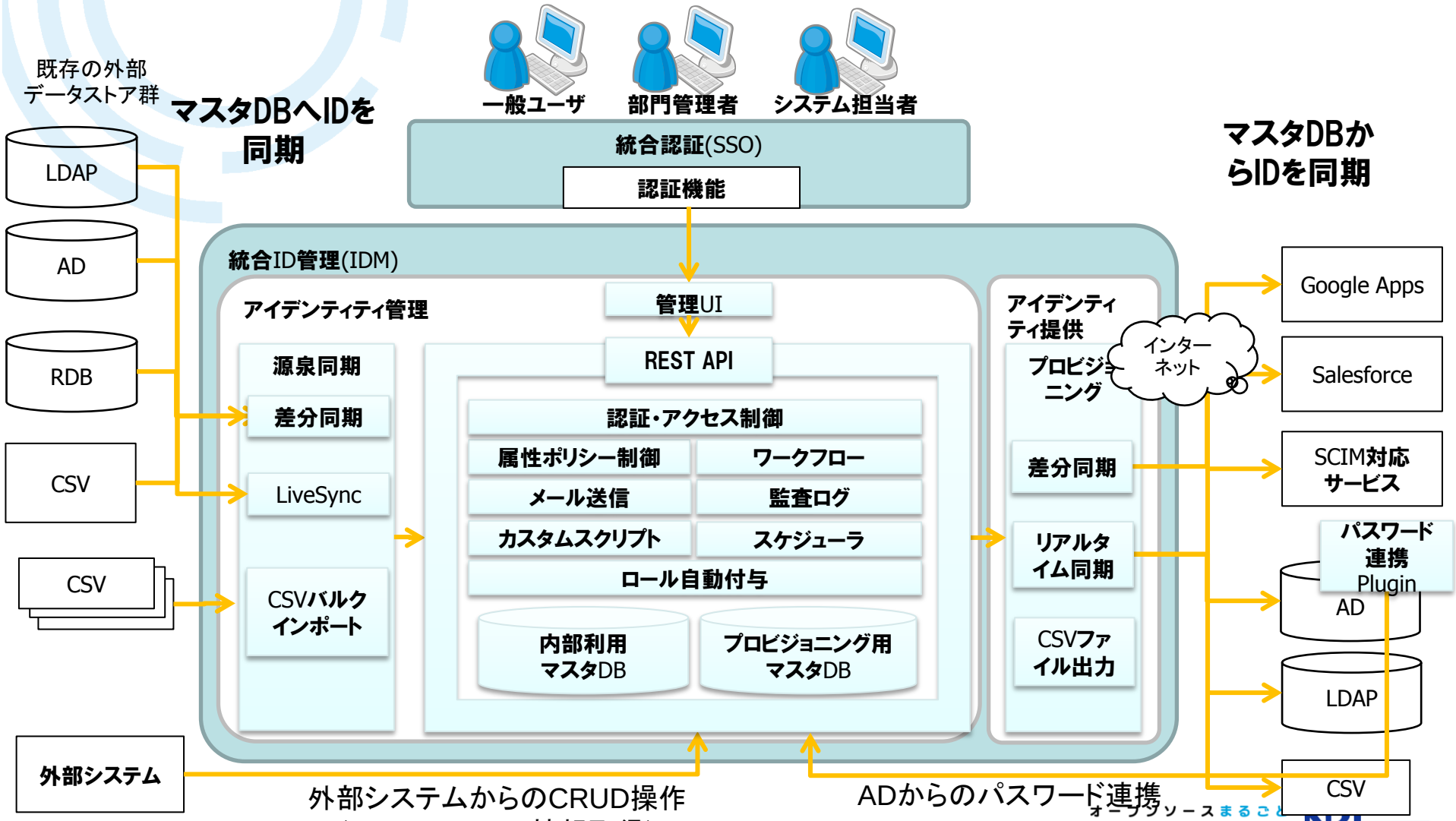
スピーディでストレスの少ないワンストップ保守体制

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。

目次

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

OpenStandia/SSO&IDMはオープンソースベース(拡張)のSSO／IDM製品です。

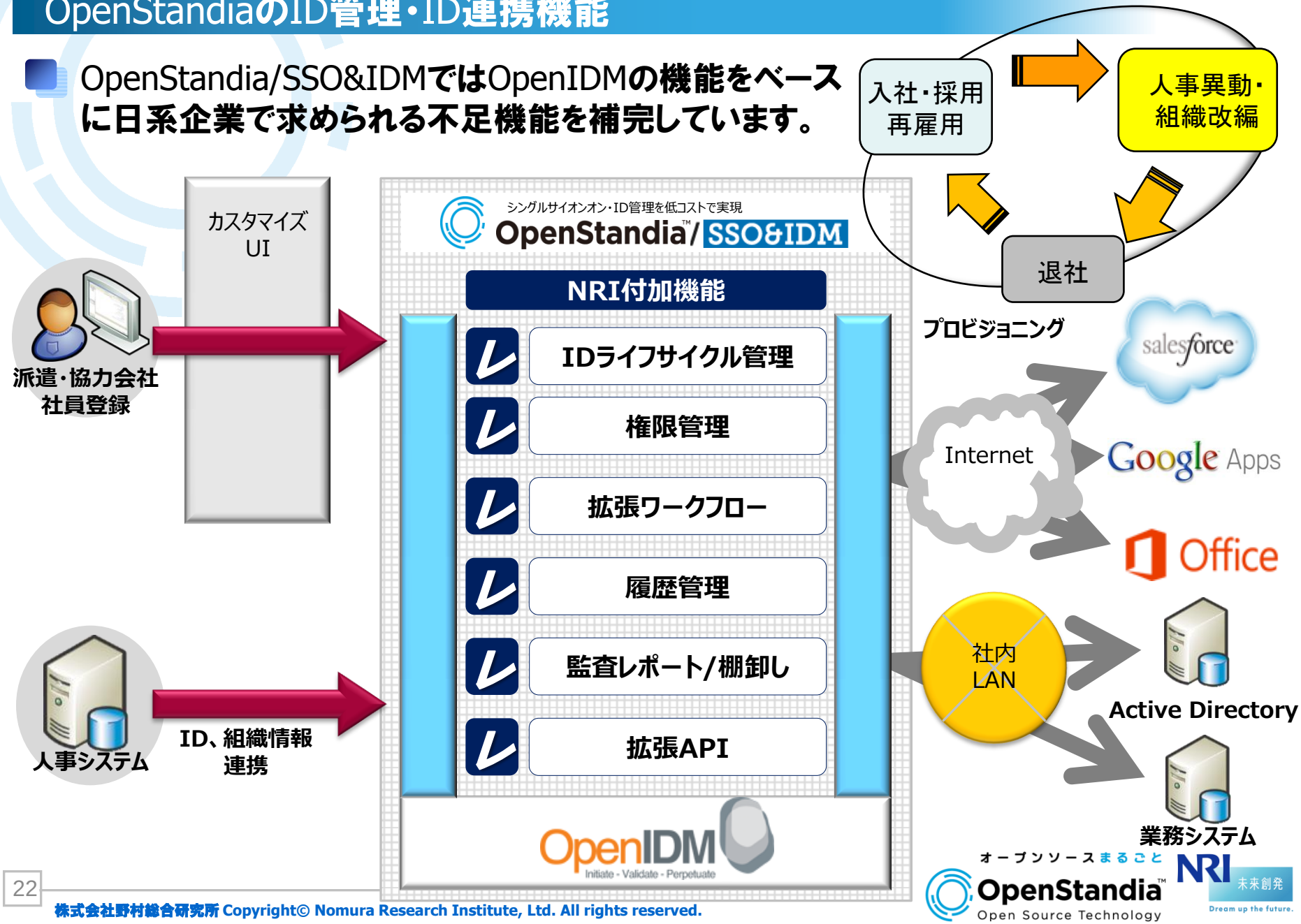


OpenStandia/SSO&IDMの主要なSSO機能

No.	連携システム	概要	カテゴリ
1	Windows(AD)	Windows(AD)へのログオンを起点として他システムへのSSOを行う	SSO起点
2	端末認証	生体認証、デバイス認証などの認証端末を利用した端末とのSSO	SSO起点 （多くはAD認証と連携）
3	WEBアプリ	ブラウザから利用するパッケージやスクラッチアプリケーションなどのWEBアプリケーションへのSSO	SSO対象システム
4	クライアント導入型アプリ	PCにアプリケーションをインストールしてサーバと接続して利用するタイプのSSO	SSO対象システム
5	SaaS	GoogleApps, SalesForce, Office365等のSAML方式に対応しているSaaSへのSSO	SSO対象システム
6	高度認証	ワンタイムパスワード、リスクベース認証などの高度なSSO	拡張SSO方式

プロジェクト推進に要求される要件とOpenStandiaの優位性
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.

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。

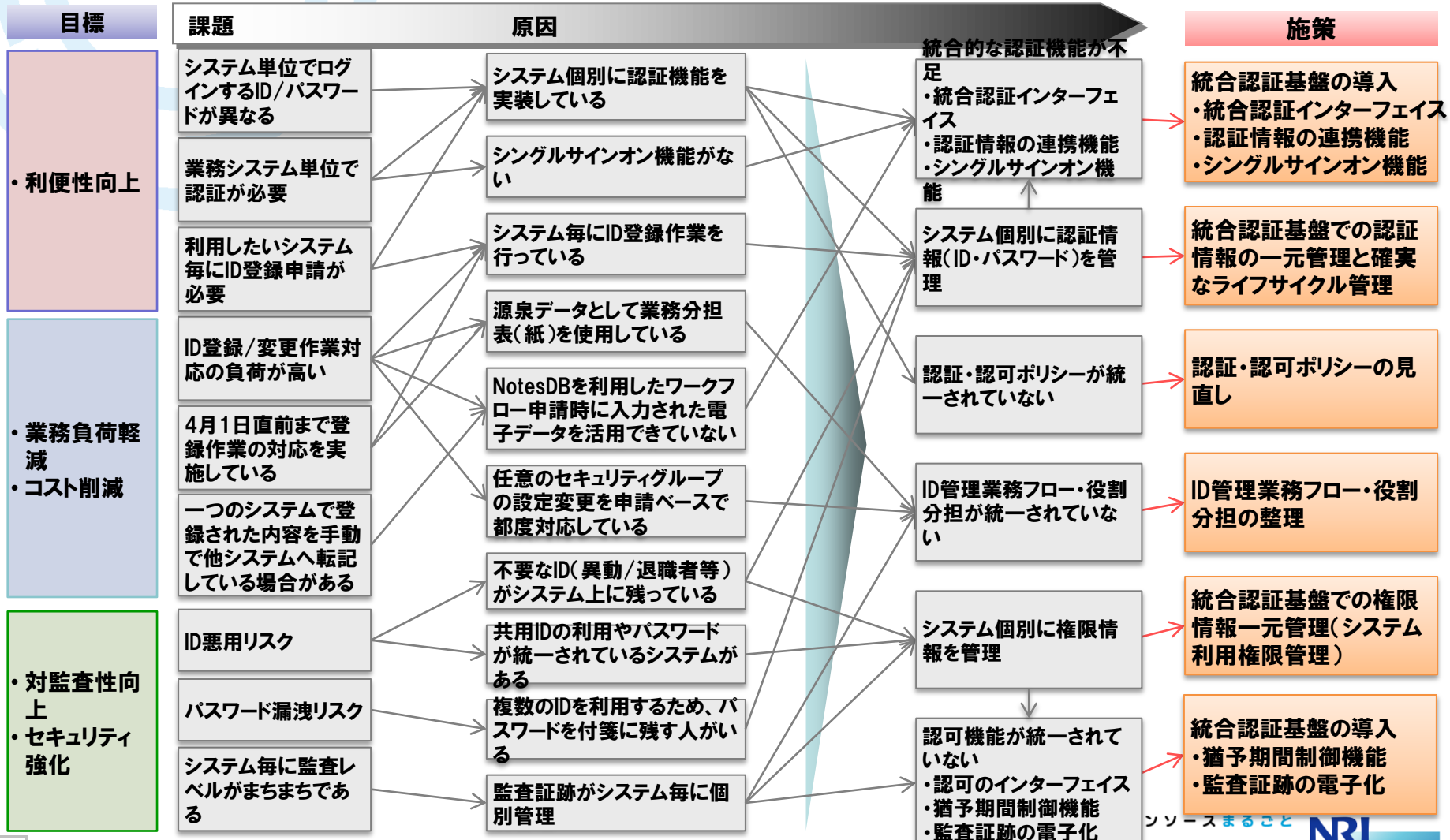
- ●自社リソースで実施するには負荷が高いパッケージのFit＆Gap分析を提案ベンダに依頼できる
- ●競争原理が有効に機能し、各社から安価な提案を引き出せる（場合によっては戦略的価格を引き出すことが可能）
- ●パッケージ優劣のみならず、ベンダーの力量も評価できる
- ●システム化計画フェーズで算出した概算費用の精緻化が可能

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

成果物の例（現状把握・課題分析）

現状を調査し、課題分析から本質的な原因・問題を明らかにする。



成果物の例（現状把握・課題分析）
連携先システムの情報の持ち方、データ連携手段を押さえることが肝要

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ID基盤対象を検討するうえで現状調査・把握は重要。

連携対象システム一覧

項番	システム名	システム形式	システム概要	所管部署	利用ユーザー	利用部署	利用ユーザ数	システム導入時期／次期更改予定時期	IDの種類	権限・グループ情報	IDの登録部署	ID作成の申請方法と登録方法	パスワード失効時の手続き・対応	人事異動時期の手続き	監査・棚卸時の手続き	懸念点、課題など
1	Windows（Active Directory）	（Windows Directory Service）	（Windows Directory Service）	情報システム部	・正社員 ・契約社員 ・派遣社員 ・一部のｱﾙﾊﾞｲﾄ	・全部署 ・一部グループ会社	1400程度	ー／未定	・個別ID（社員個々人のID）。 ・共用ID（共用PCログイン用のID）	セキュリティグループには、 ・所属グループ ・プロジェクトグループ が用意されている。そのほかフォ	情報システム部／AD管理担当者	No2を兼用 〈新規作成〉 3月＝User-ID申請DB	情報システム部／運用担当者3名が初期ﾊﾟｽﾜｰﾄﾞにﾘｾｯﾄ（直接若しくは、ﾍﾙﾌﾟﾃﾞｽｸ経	・所属グループ（セキュリティグループ）の修正を担当者一人がすべて手作業で行ってい	情報システム部運用担当が年1回棚卸し実施	・源泉データが人事部から入手する業務分担表（紙）である。人事異動時期はこの表に従って専任担当者が手作業で入力してい
2	Notes（ｸﾗｲｱﾝﾄ）		現行グループウェアシステム	情報システム部	・正社員 ・契約社員 ・派遣社員 ・一部のｱﾙﾊﾞｲﾄ	・全部署 ・一部グループ会社	1500(1300+200)	ー／未定	・個別ID	・所属グループ ・各種申請ベースで作られるアクセス権限グループ（Notes-DB-Accessで始まるグループ）	CECのオペレータ	〈新規作成〉 3月＝User-ID申請DB （Excel添付）	情報システム部／Nots担当者（ﾍﾙﾌﾟﾃﾞｽｸ経由）	・所属グループ ・アクセス権グループの修正を担当者一人がすべて手作業で行ってい	情報システム部Notes運用担当が年2回棚卸し実施	・源泉データが人事部から入手する業務分担表（紙）である。人事異動時期はこの表に従って専任担当者（ADとは別）が手作業
3	Client Access（AS/400）		オフコン管理用のﾐ-										情報システム部 〈ｻｰﾊﾞ/ｱﾌﾟﾘ管理用〉 の	特に無し （必要に応じて申請ベースで対応）	〈ｻｰﾊﾞ接続用〉は情報システム部にて実施	・Notesの登録申請用DBの電子データはワークフロー用に利用されるのみ。システム登録への連携はない。
4	GoogleApps（今後導入予定）															
5	Company Web												人事部勤労Gに問い合わせ、初期ﾊﾟｽﾜｰﾄﾞにﾘｾｯﾄ	人事部にてメンテナンスを実施。情報システム部は特に対応無し。	ユーザー管理部門が毎月棚卸し実施（手続きはなし）	・Companyの社員マスタ作成時には業務分担表（紙）からデータの入力を行っているが、AD、Notesともに別の作業者が並行
6	連結会計	に配置 ﾊﾟ，DBｻｰﾊﾞ	のﾊﾟ STRAVIS）		・一部のｱﾙﾊﾞｲﾄ	子会社）							部経理部連結決算Gに問い合わせ、初期ﾊﾟｽﾜｰﾄﾞにﾘｾｯﾄ	アクセス権管理DBで登録削除や、権限メニューの変更を申請する。	部経理部連結決算Gが年1回棚卸し実施（IT全般統制に沿って）	同上 ADとの連携あり（ADにユーザがないと本システムは使えない）
7	eラーニング		社内研修のWebシステム（富士通のパッケージ）	情報システム部	・正社員 ・契約社員 ・派遣社員 ・一部のｱﾙﾊﾞｲﾄ	・全部署 ・ｸﾞﾙｰﾌﾟ会社	884	2004/4導入／予定無し	・個別ID（No.1と同一。ﾊﾟｽﾜｰ 同一の	グループ管理な						

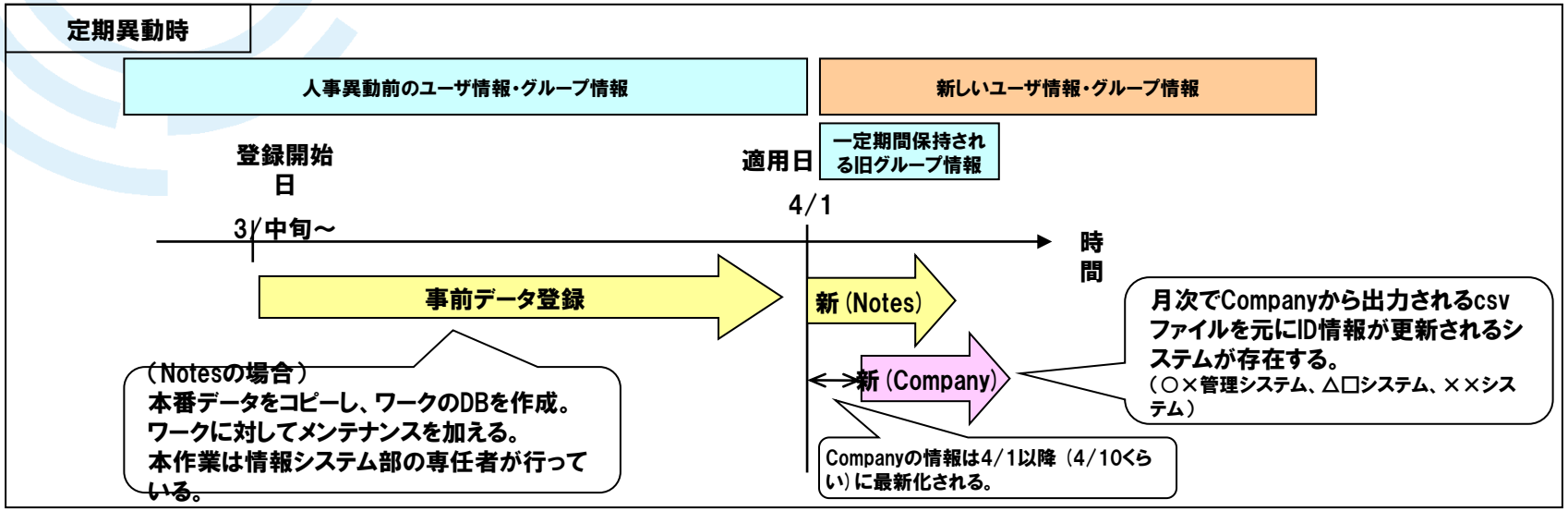
【例】
国内　36システム
海外　65システム
そのほか移行対象のID管理システム　15システム

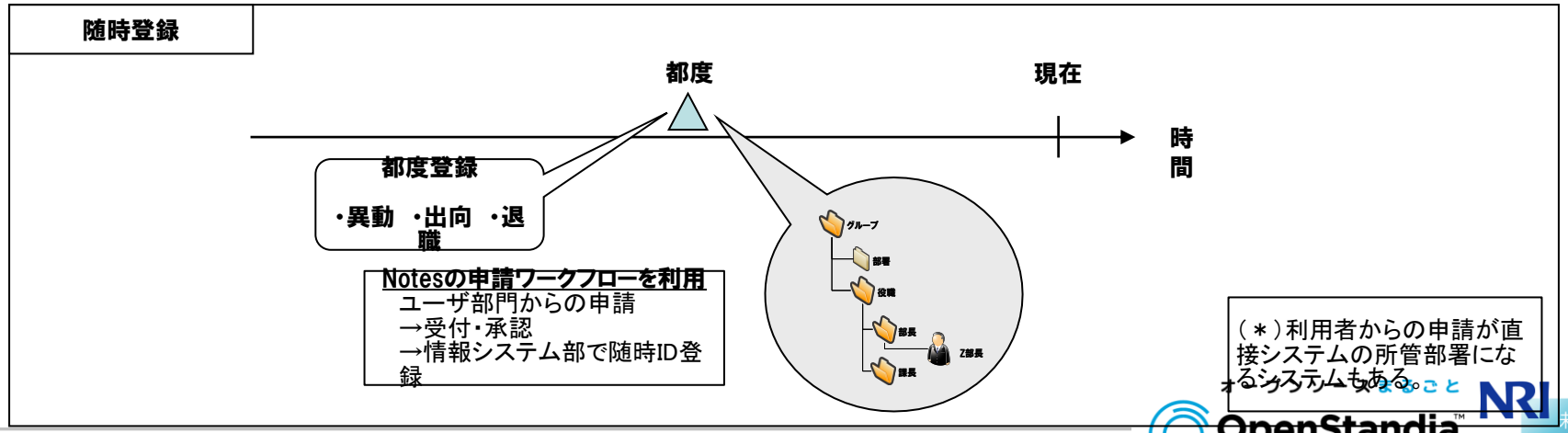
統合管理対象のシステム、サーバーの正確な調査が必要。

成果物の例（現状把握・課題分析）
IDのライフサイクル確認する。各国の事情に合わせたタイムライン要確認

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

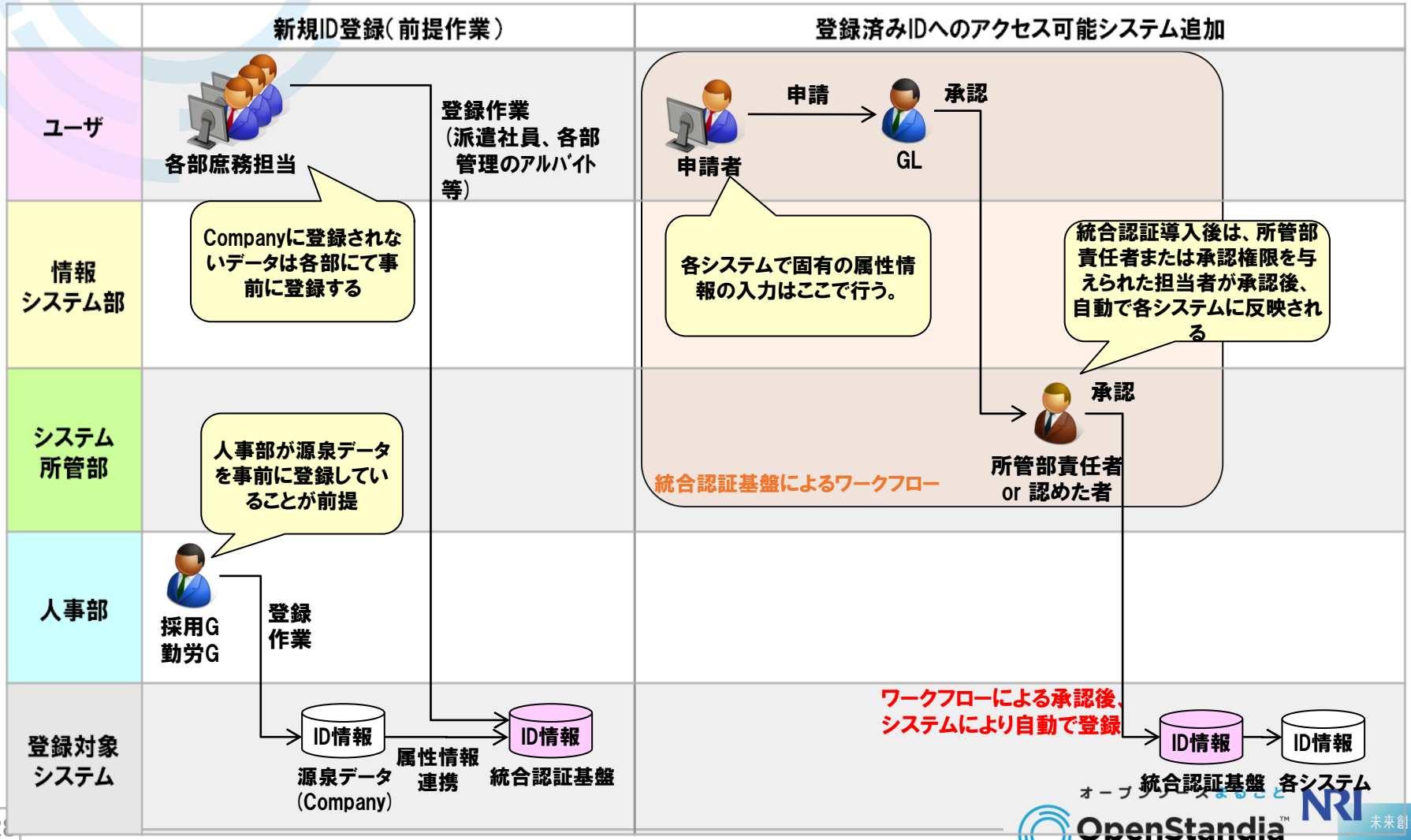
- ID登録フロー・時期を確認し、どのタイミングでどのようなIDの発生・消滅があるかをおさえます。





成果物の例（現状把握・今後の方針検討）
ID登録フローの現状と今後を調整しながら運用負荷の低い方法を考案

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



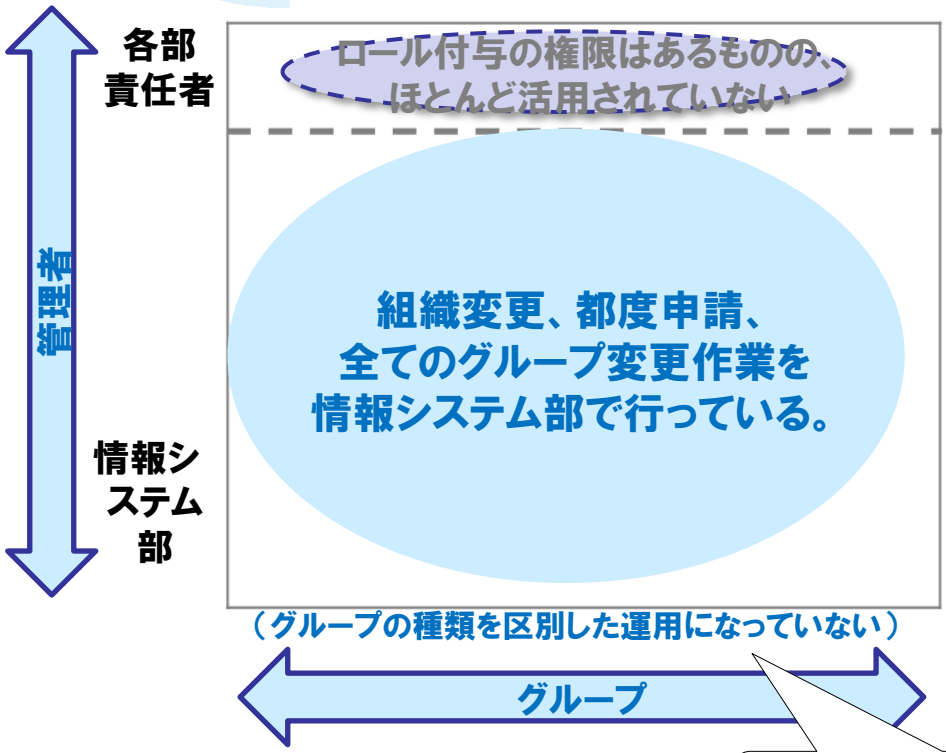
成果物の例（システム化方針検討）
システムの重要度や更改時期を考慮しながら最終形までの道筋を考える

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

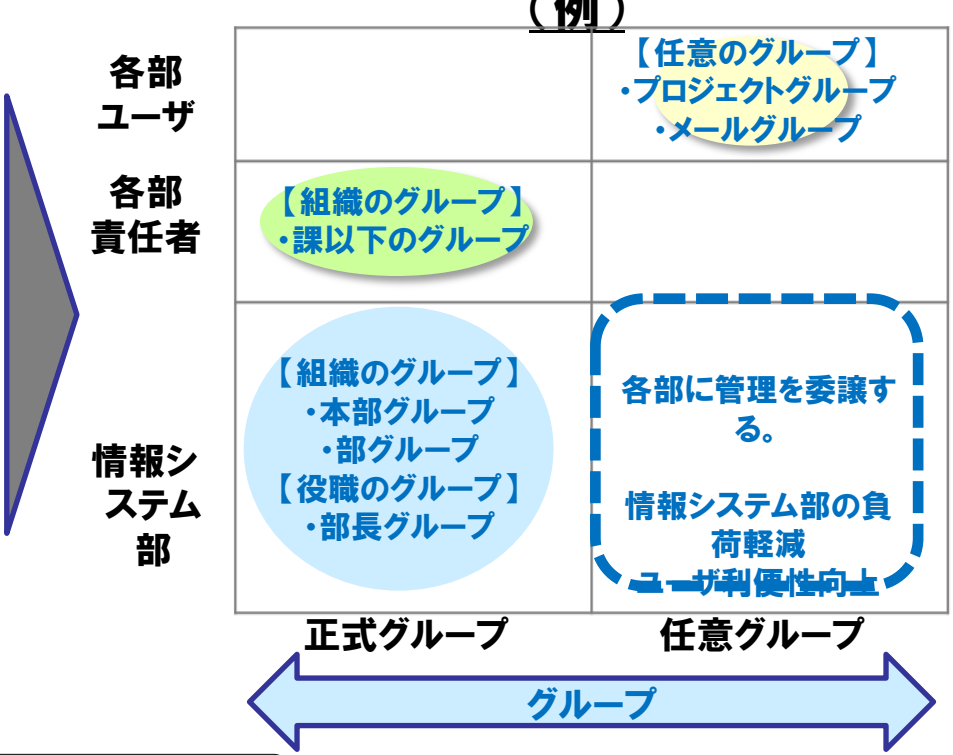
成果物の例（システム化方針検討）
運用面を考慮しながら認証情報と認可情報の管理スキームを考える

- 認証・認可情報の管理範囲を現状を確認しながら今後の方針を検討する。

現状のグループ管理イメージ



今後のグループ管理イメージ（例）

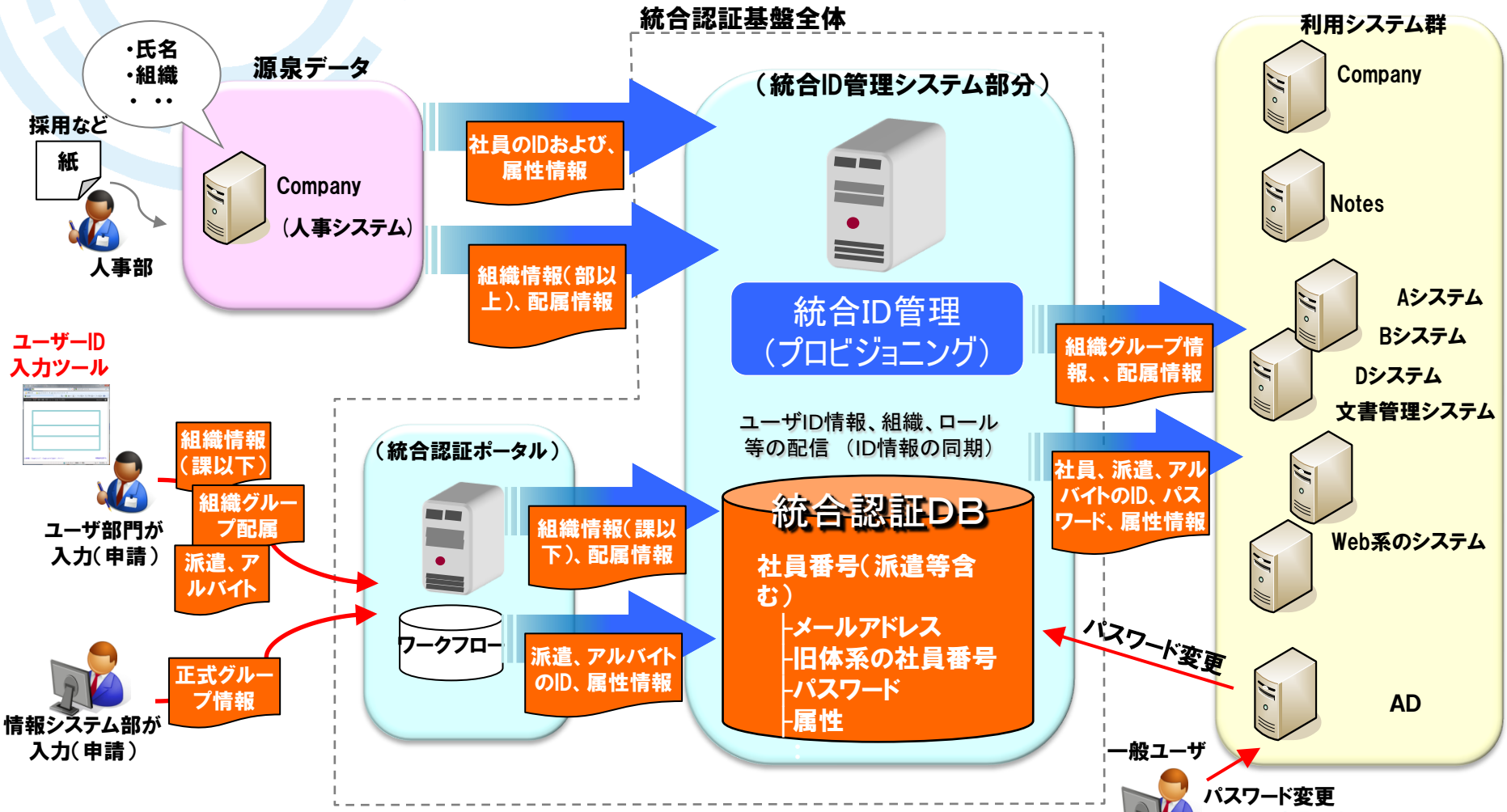


A企業では数千のグループの棚卸しを行いました。

成果物の例（システム化方針検討）
ID連携先システムごとに連携方法や今後の方針を一覧化して合意する

No.	システム名	プロビジョニング（ID連携）	プロビジョニング方式	パスワード連携	備考
1	Windows (ActiveDirectory)	○	LDAP接続	LDAP接続	
2	Notes	○	LDAP接続	LDAP接続	
3	Aシステム	×			ﾒｯｾｰｼﾞｷｭｰが必要であるため不可
4	Google Apps	○	独自API	独自API	
5	Company	○	CSV連携	SQL	
6	Bシステム　※J-SOX対象	×			CSV連携は開発すれば可能性はあるが、前提連携システムが更改不可
7	Cシステム　※J-SOX対象	×			
8	会計システム　※J-SOX対象	×			仕様非公開
9	eラーニング	×			回答無し
10	Dシステム	○	SQL	SQL	
11	Eシステム	○	SQL	SQL	
12	Fシステム	○	SQL	SQL	
13	Gシステム	○	SQL		

成果物の例（システム化方針検討）
IDデータのフローを全体俯瞰出来るように整理する



目次

モデルケース：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

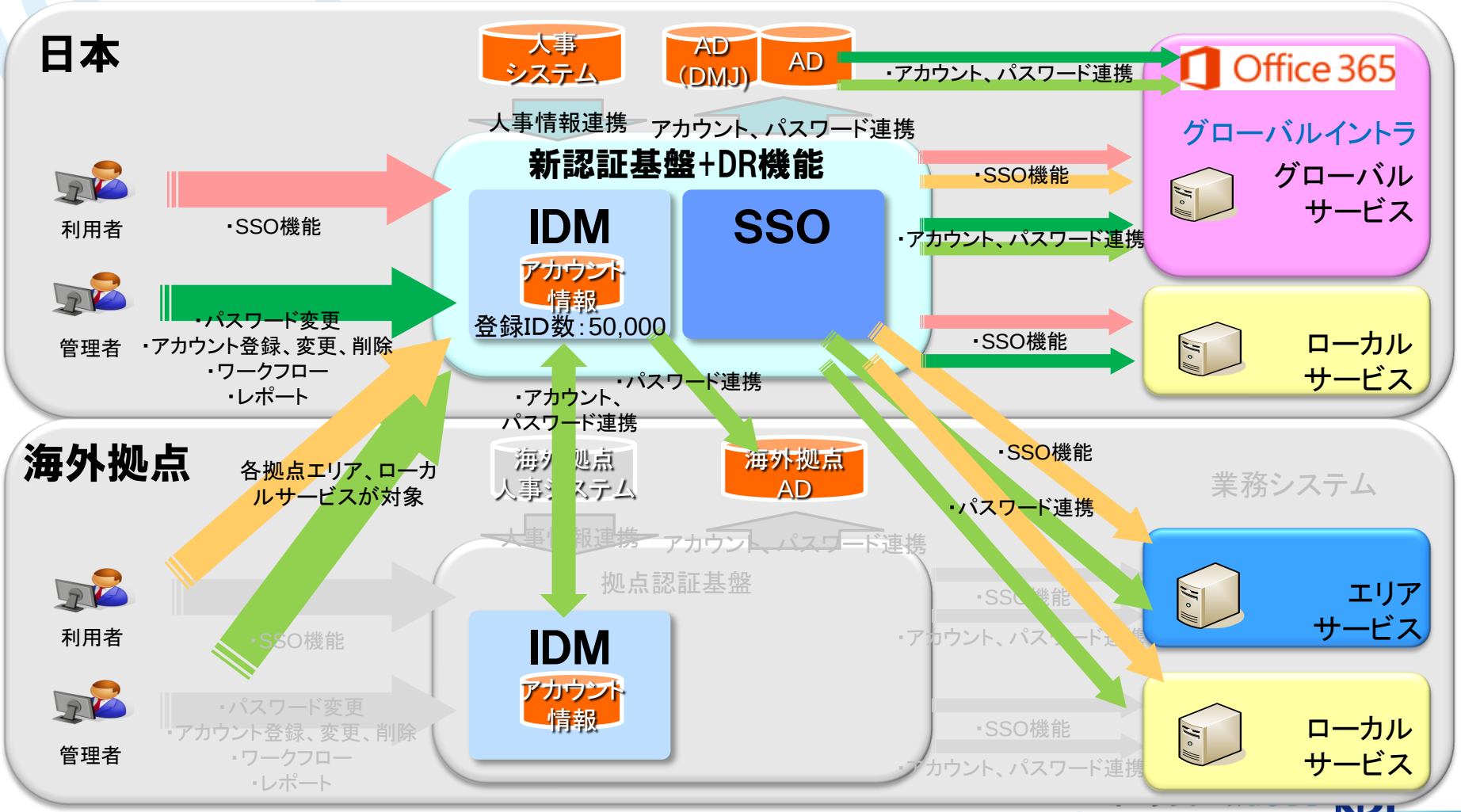
- 拠点ごとに個別で導入したシステムが乱立しており、本社側で管理できない状況にある
- 人事情報を本社と拠点で個別管理しており、IDライフサイクルが管理できていない
- 現地のシステム対応が十分でないため、アクセス権設定、監査ログの取得ができていない

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：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。



モデルケース③：大手不動産業様（国内）
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

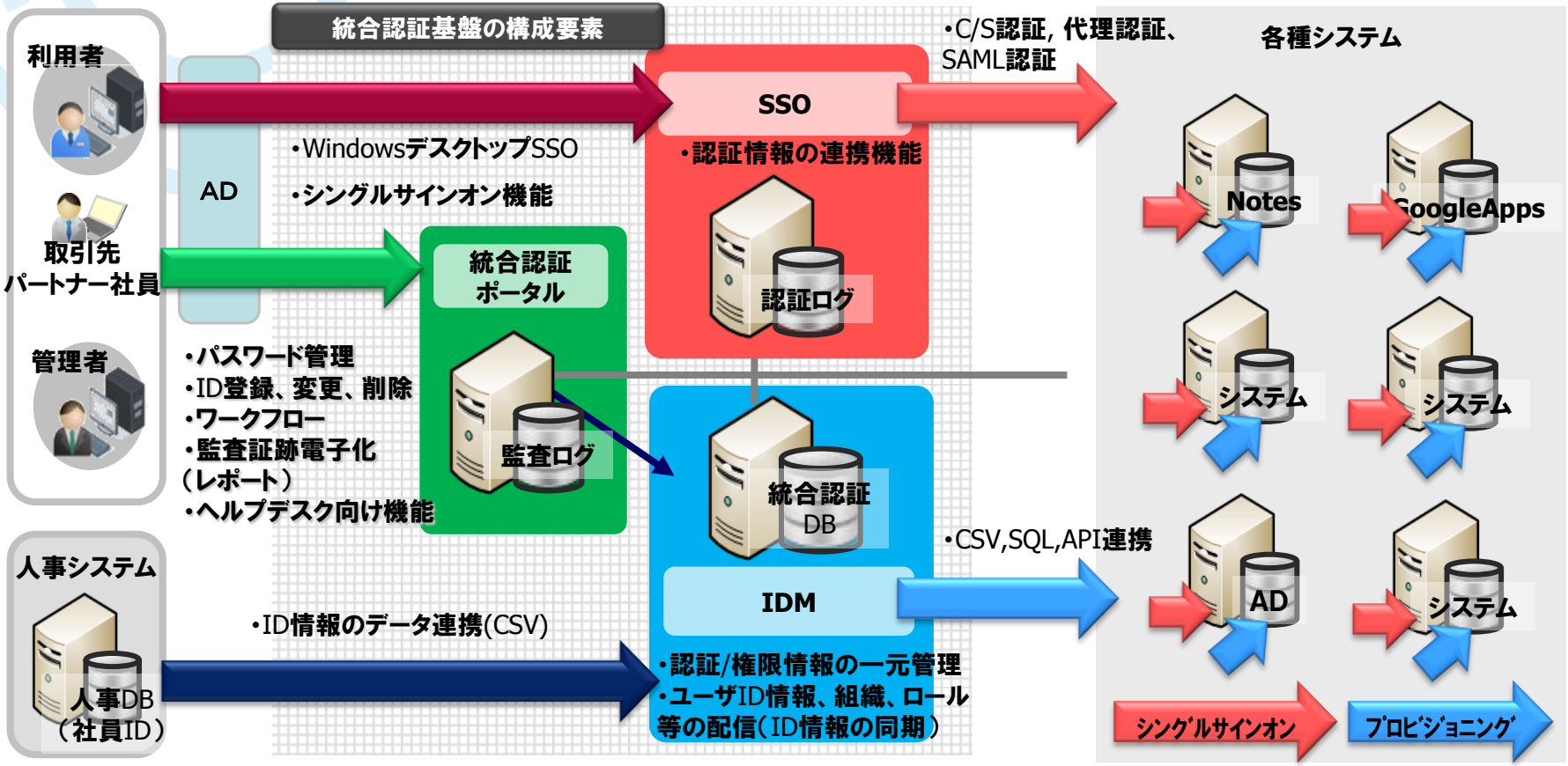
- 現在の各システムの認証の仕組みは個別の技術が使われていること、さらにIDを管理する部署が異なっている場合がある。
- グループウェア、Windowsドメイン、各業務システムの権限情報はそれぞれにあり、管理している。
- 人事異動時期のIDの棚卸し、変更管理作業は運用担当にとって非常に高い負荷である。

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③：大手不動産業様（国内）
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。



- **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.