シングルサインオン（OpenAM）
統合ID管理（OpenIDM）
最新事例紹介

株式会社野村総合研究所
情報技術本部
オープンソースソリューション推進室
寺田　雄一

株式会社 野村総合研究所 情報技術本部 オープンソースソリューションセンター(OSSC)
Mail：ossc@nri.co.jp　Web：http://openstandia.jp/

はじめに

自己紹介

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

- 野村総合研究所にて、多くの大規模Webシステム構築プロジェクトに、ITアーキテクト（基盤リーダー）として従事、方式設計、基盤構築を行う。
- 2003年に、オープンソースソリューションセンター（OSSC）を企画、設立。
- 2004年にMySQL社とパートナー契約。
  2005年に旧JBoss社とパートナー契約。
- 2006年、社内ベンチャーにてOSサポート事業を外販を開始。サービス名称を、“OpenStandia”に。
  オープンソース・ワンストップサービスを展開。
  事業責任者として活動。
- 2008年6月、オープンソースビジネス推進協議会（OBCI）を企画、設立。事務局担当理事に就任。
- 2008年6月、オープンタイムアウト化支援コンソーシアム（OSAC）、理事就任。
- 2008年9月、ミック経済研究所による調査にて、
  野村総合研究所のOpenStandiaがOSSミドルウェア
  のサポートサービス分野でシェアNo.1を獲得。
- 2010年10月、JasperSoft社とパートナー契約。
- 2010年10月、OpenSSO&OpenAMコンソーシアムを企画、設立。会長就任。

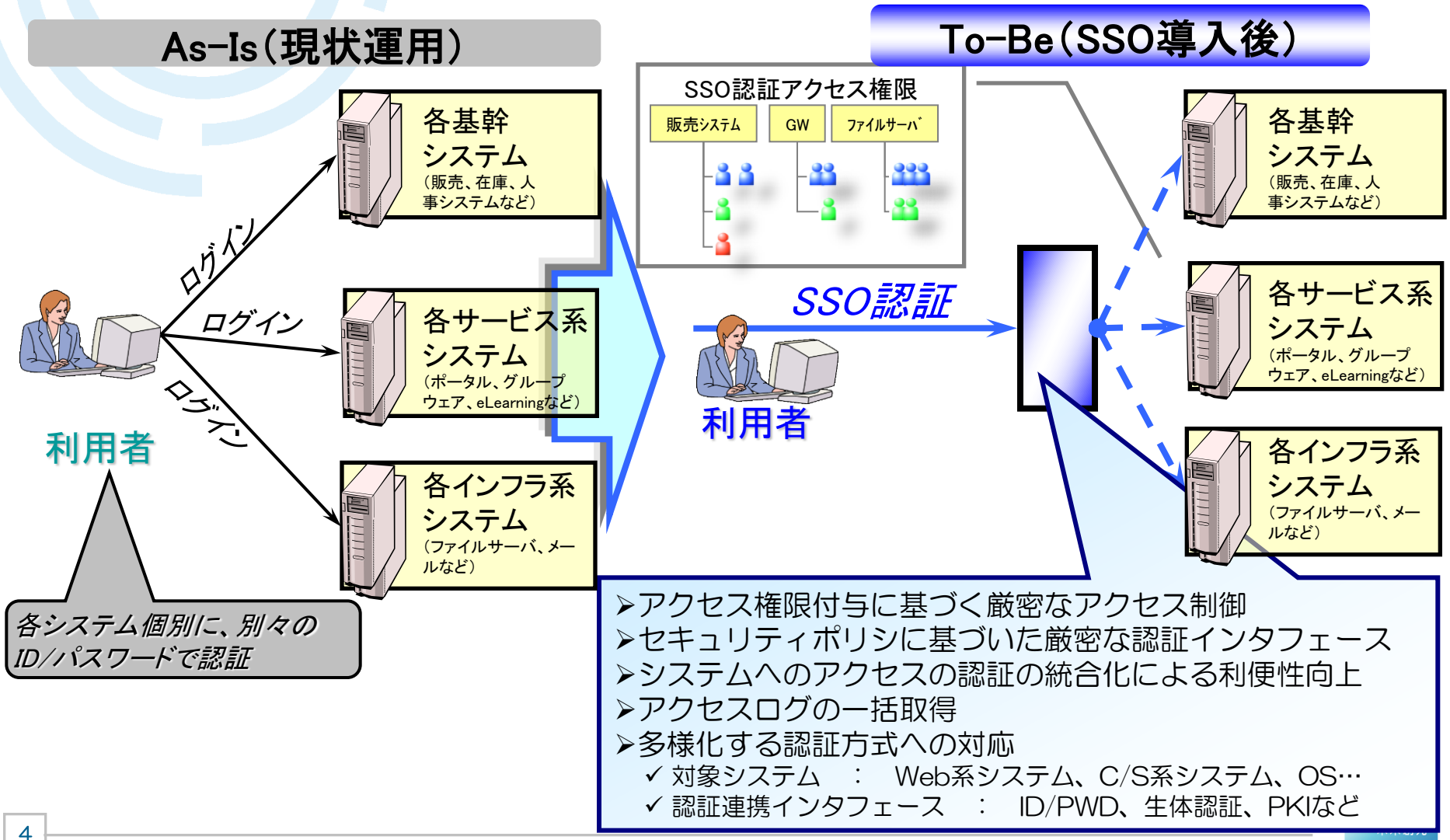
企業に
オープンソースを
普及させよう！

NRI 未来創発 Dream up the future.

- 高まるシングルサインオン・統合ID管理のニーズ

シングルサインオンについて

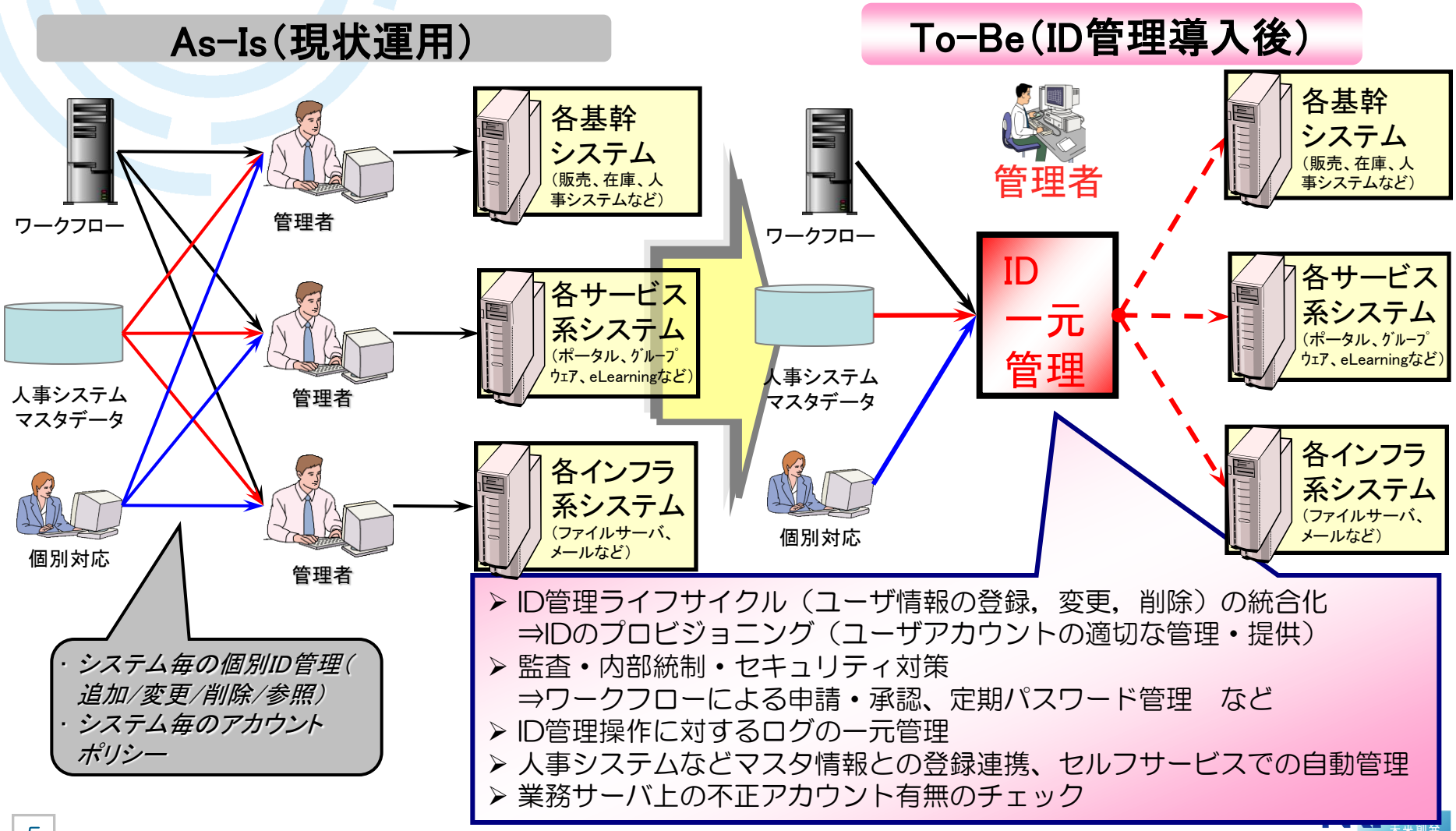
- SSO認証を導入すると、様々なシステムへのSSOとアクセス制御が可能となり、利用者の利便性向上やセキュリティ向上につながる



ID管理について

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

- 入社・退社・人事異動時に、利用システム毎のアカウントの個別ID管理（登録/修正/削除/参照）に対して、導入後は統合的に管理することにより、運用効率化・負担＆ID管理ミス軽減となる



高まるSSO・統合ID管理のニーズ

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

業務の自動化

- ID管理の効率化
- 内部統制、コンプライアンス強化、個人情報保護

IT環境の変化

- SaaS
- クラウド基盤
- モバイル端末、スマートフォン、タブレット

事業環境の変化

- グループ企業間、グローバル規模での情報システム共有
- 企業合併、社内認証基盤統合、サービス統合
- サービス事業強化

(出所)Tokyo, Japan - seen from the North Observatory 45th floor - Tokyo Metropolitan Government Building in Shinjuku. By UggBoy♥UggGirl [PHOTO // WORLD // TRAVEL]
http://www.flickr.com/photos/uggboy/5181846719/in/photostream/

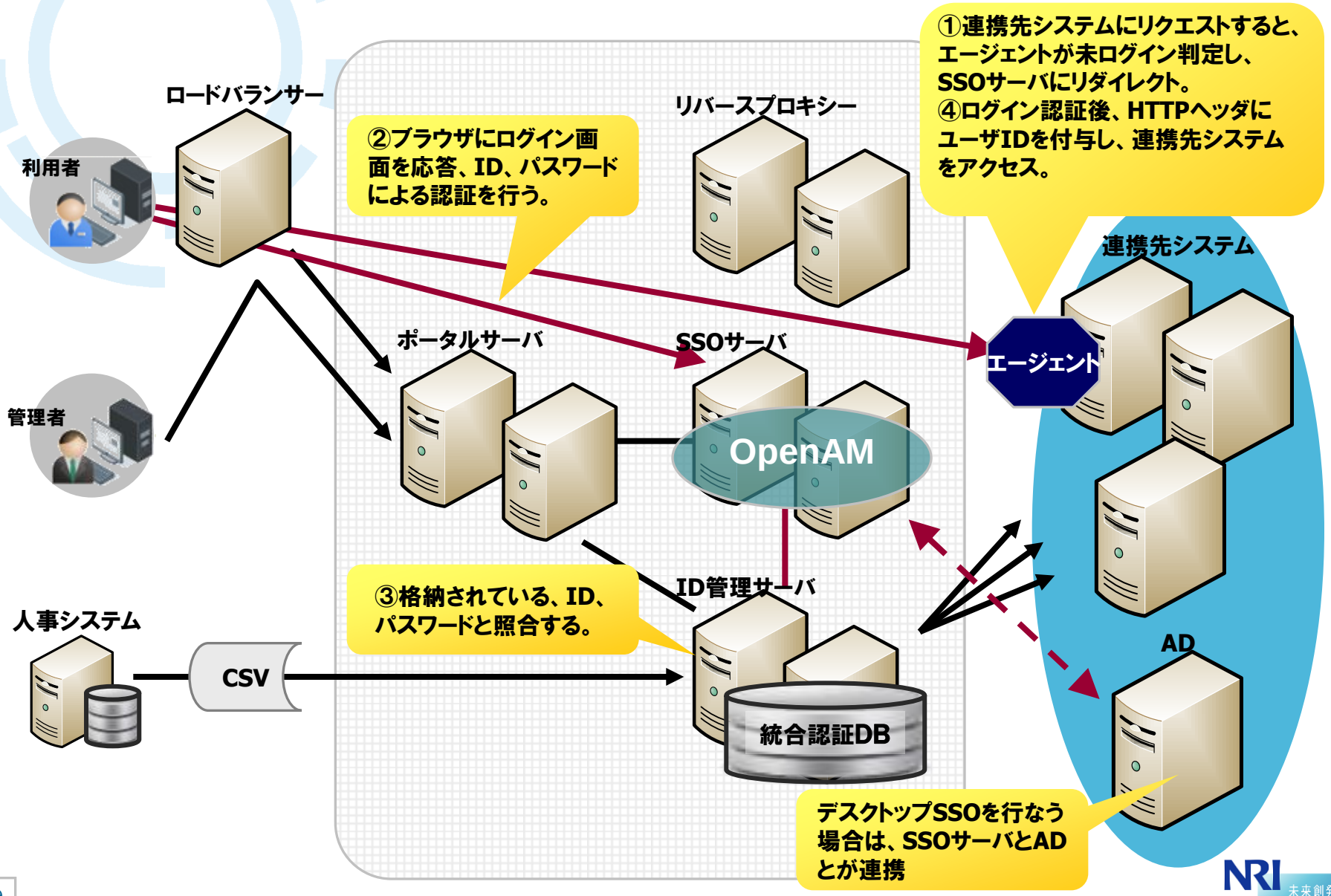
NRI 未来創発
Dream up the future.

- オープンソースで「シングルサインオン」、OpenAM

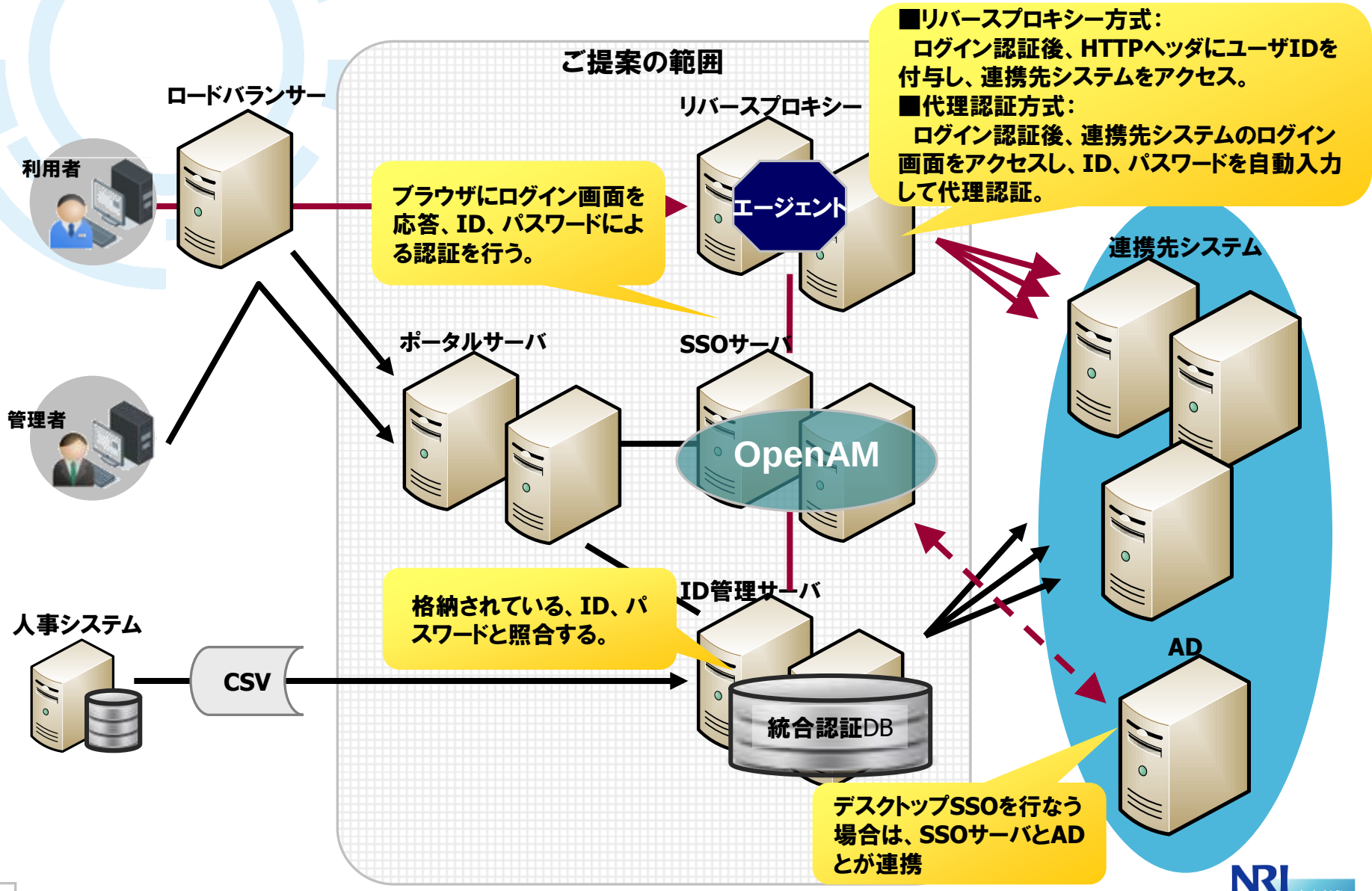
OpenAMとは

- シングルサインオンを実現するためのオープンソース。CDDLライセンス。Javaベース。
- 旧サン・マイクロシステムズ社が開発した「Access Manager」を同社がオープンソース化した「OpenSSO」がベース。ForgeRock社がフォークした。

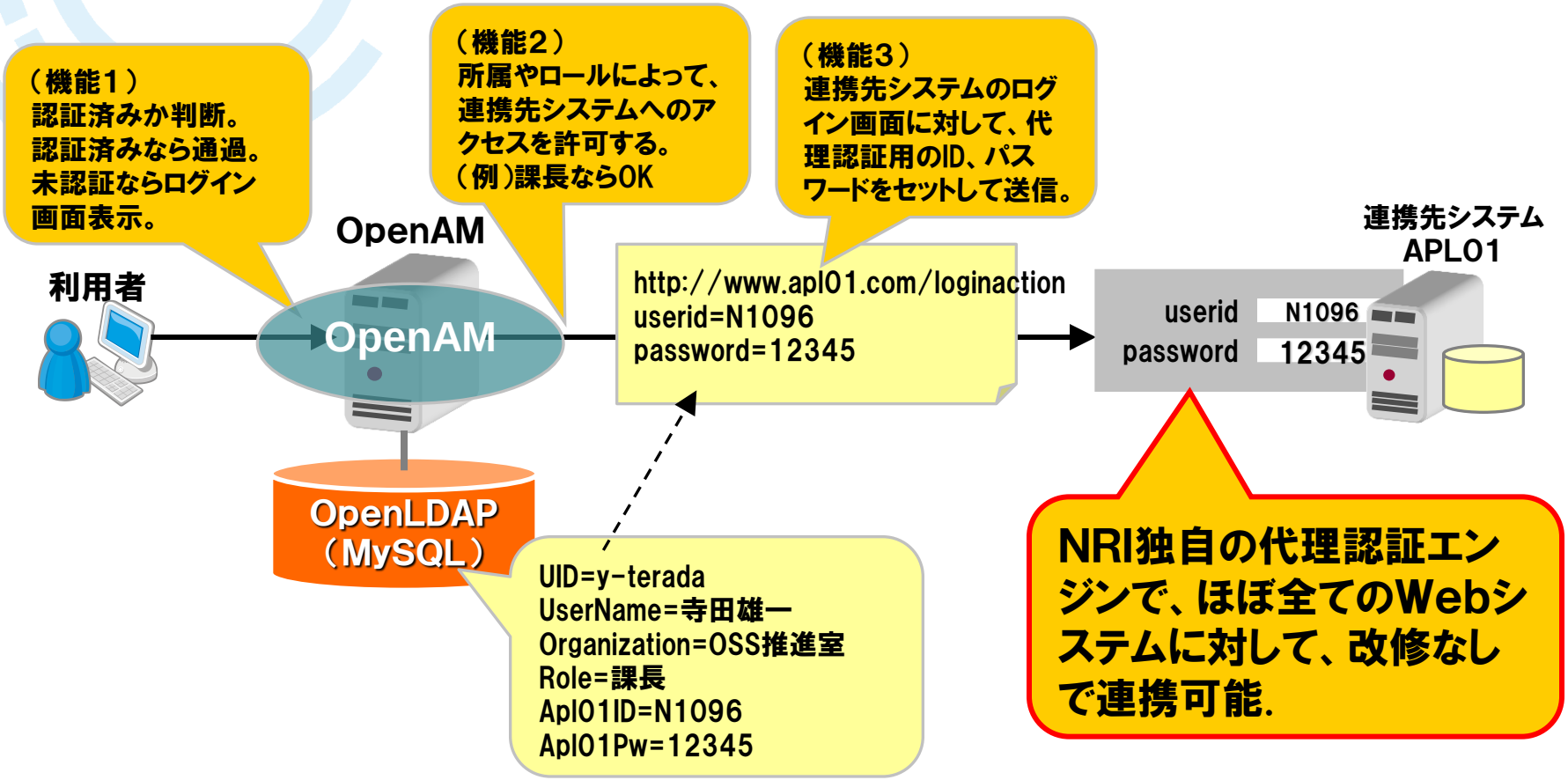
エージェント型認証処理シーケンス概要



リバースプロキシー、及び代理認証時の処理シーケンス概要



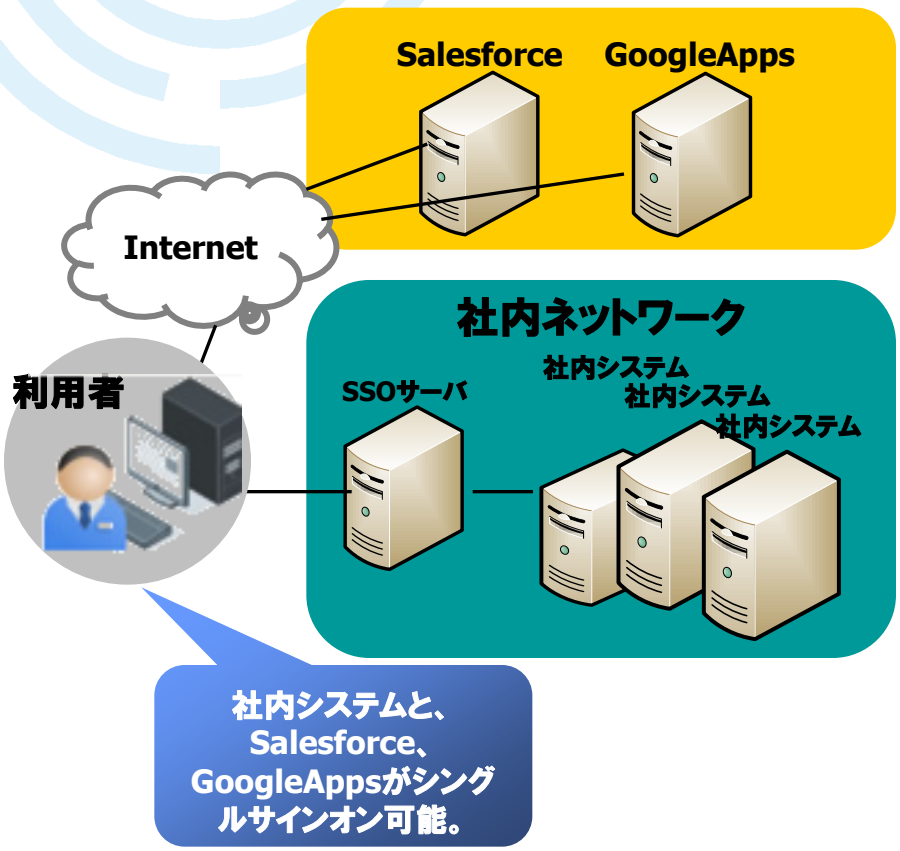
代理認証について

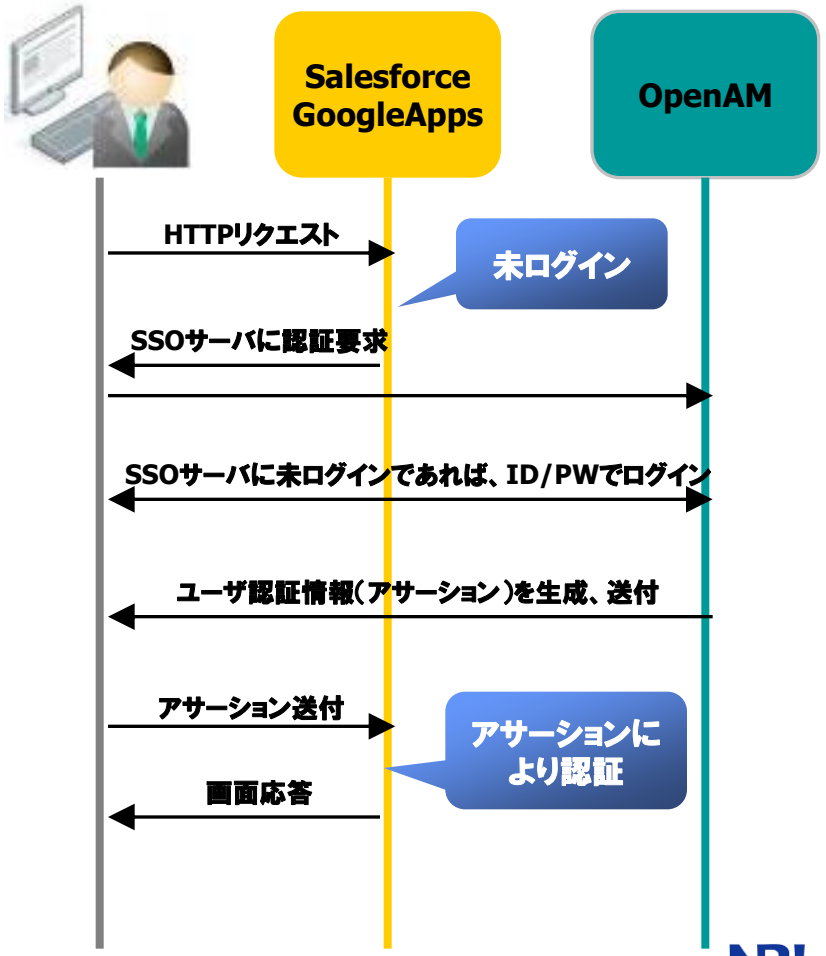


SalesforceやGoogleAppsとのシングルサインオン

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

OpenStandiaのSSOは、標準プロトコルであるSAMLに対応しており、SalesforceやGoogleAppsとのシングルサインオンが可能です。

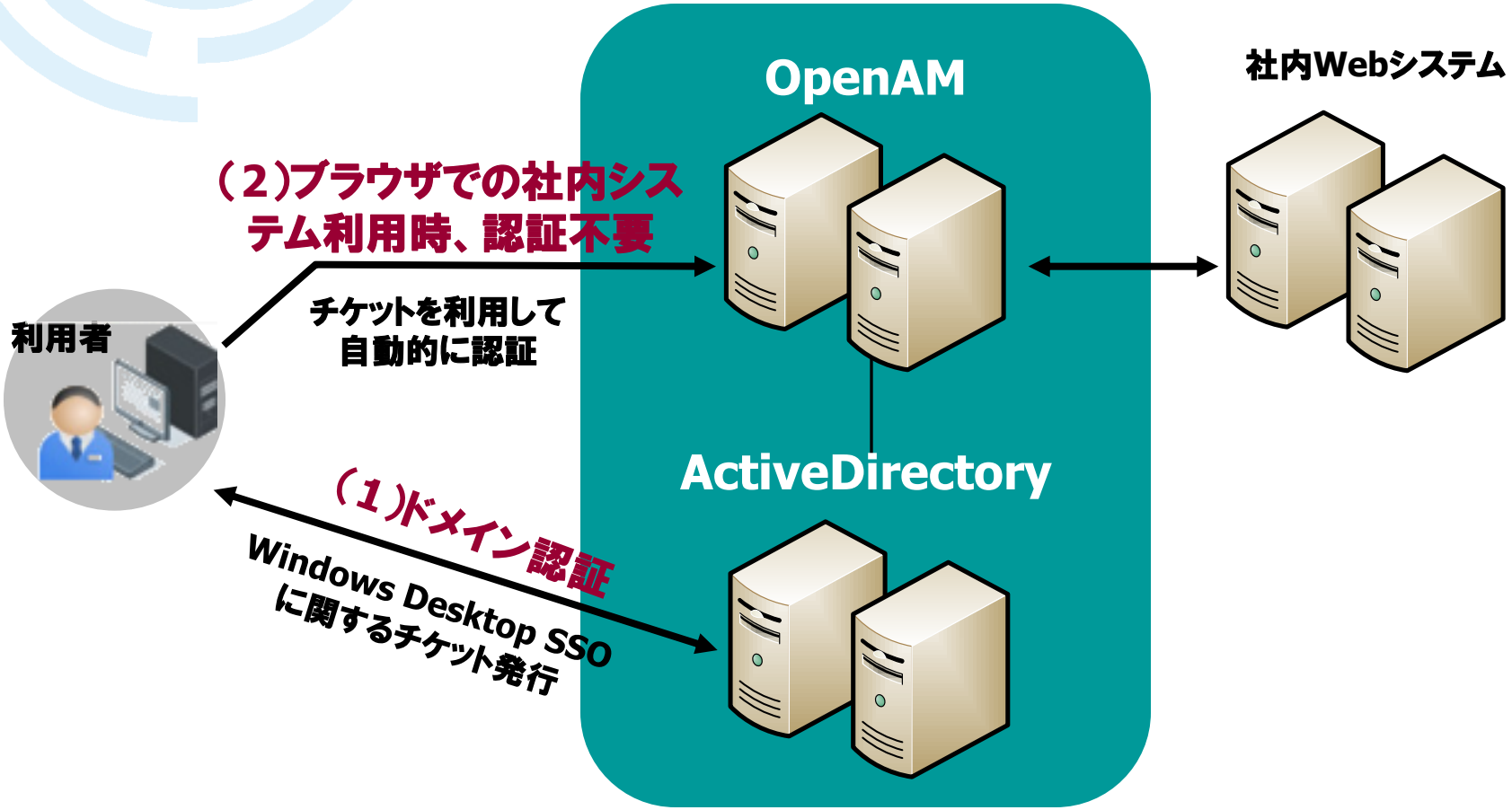




NRI 未来創発
Dream up the future.

WindowsデスクトップSSO

- Windowsにログインした情報を利用して、社内のWebシステムに自動的にログオンします。
- ブラウザでの、ID／パスワード入力は不要です。



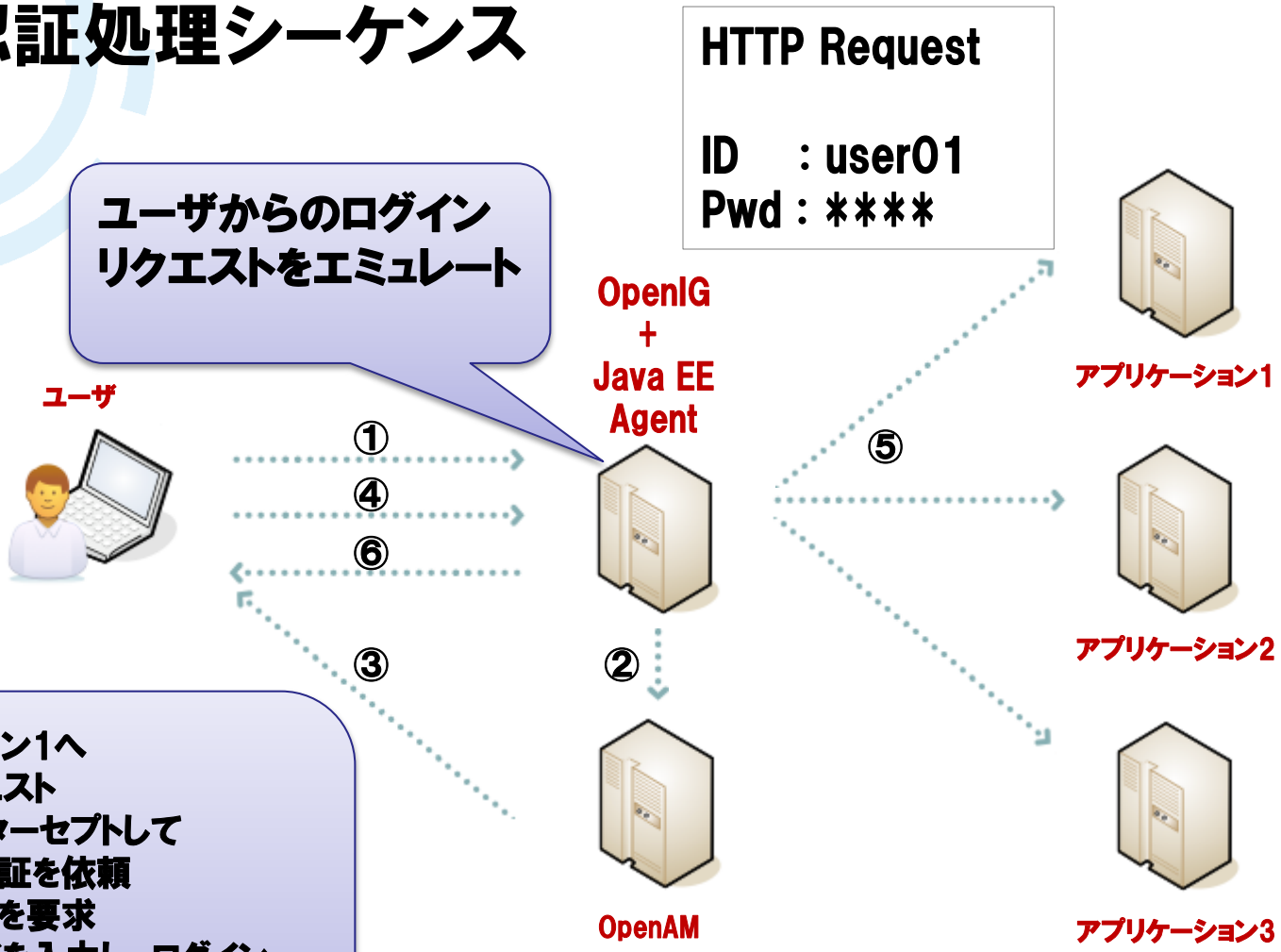
OpenAM 10.0 の新機能

- OpenIG
- REST APIのJSON出力（省略）
- リスクベース認証
- OAuth 2.0クライアント認証
- LDAPパスワードポリシーのサポート（省略）

OpenIGとは

- 代理認証を実現するソフトウェア
- OpenAMとは独立した製品
- 基本的にはOpenAMと連携して動作させる
- リバースプロキシ型
- 単独でリバースプロキシサーバとして動作
- HTTPリクエストをエミュレートして認証を代行

代理認証処理シーケンス

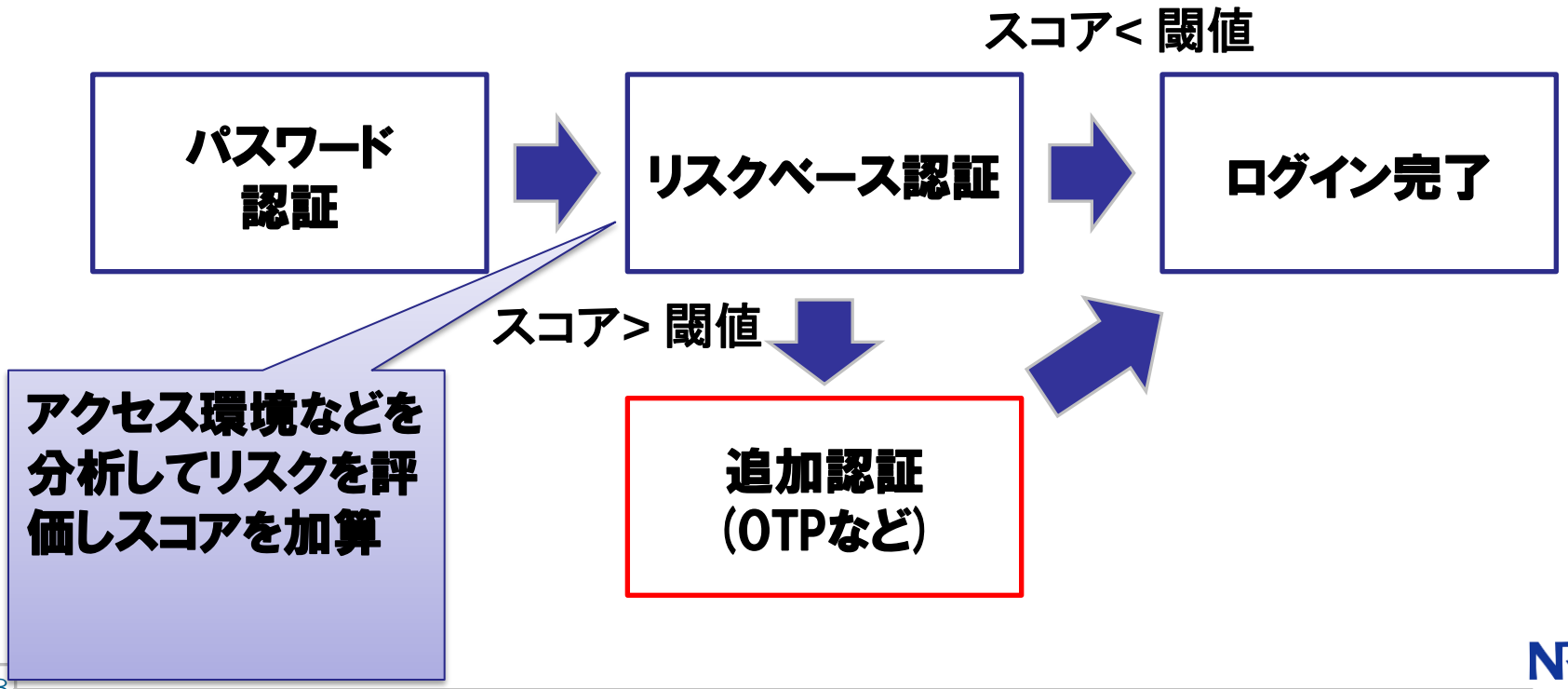


① アプリケーション1へ
ログインリクエスト
② Agentがインターセプトして
OpenAMへ認証を依頼
③ ユーザに認証を要求
④ ID、パスワードを入力し、ログイン
⑤ ユーザからのログインリクエストを
エミュレートし、認証を代行
⑥ ログインレスポンスを返す

SAML2.0 フェデレーションゲートウェイ機能

リスクベース認証

- 不正アクセスのリスクに配慮した認証方式
- ログイン時の地理的位置の評価、最終ログインからの経過時間や認証失敗回数のチェック、IPアドレスの履歴チェックを元に、追加の認証を要求する



リスク評価チェックロジック

チェック方法	概要
認証失敗チェック	ユーザーが過去に認証失敗をしているかをチェックする。 ※LDAPパスワードポリシーのアカウントロックと同時には使用不可。
IPレンジチェック	クライアントIPアドレスが指定した範囲内にあるかをチェックする。
IP履歴チェック	アクセスした際のIPアドレスがユーザープロファイルに記録されているIPアドレスの履歴リストに存在するかをチェックする。
既知のCookie値チェック	クライアントのリクエストに既知のCookieが存在し、正しい値を持っているかをチェックする。
最終ログインからの経過時間チェック	ユーザーのログインが、最後にログインした時刻から指定した経過時間内であるかをチェックする。
プロファイルのリスク属性チェック	ユーザープロファイルに指定した属性と値が含まれているかをチェックする。
デバイス登録Cookieチェック	クライアントリクエストに指定された名前のCookieが含まれているかをチェックする。
位置情報国コードチェック	位置情報データベースを利用してクライアントのIPアドレスをチェックする。 位置情報データベースはMaxMindのバイナリフォーマットが利用可能。
リクエストヘッダーチェック	クライアントリクエストが必須で指定されたヘッダーおよび値を含んでいるかをチェックする。

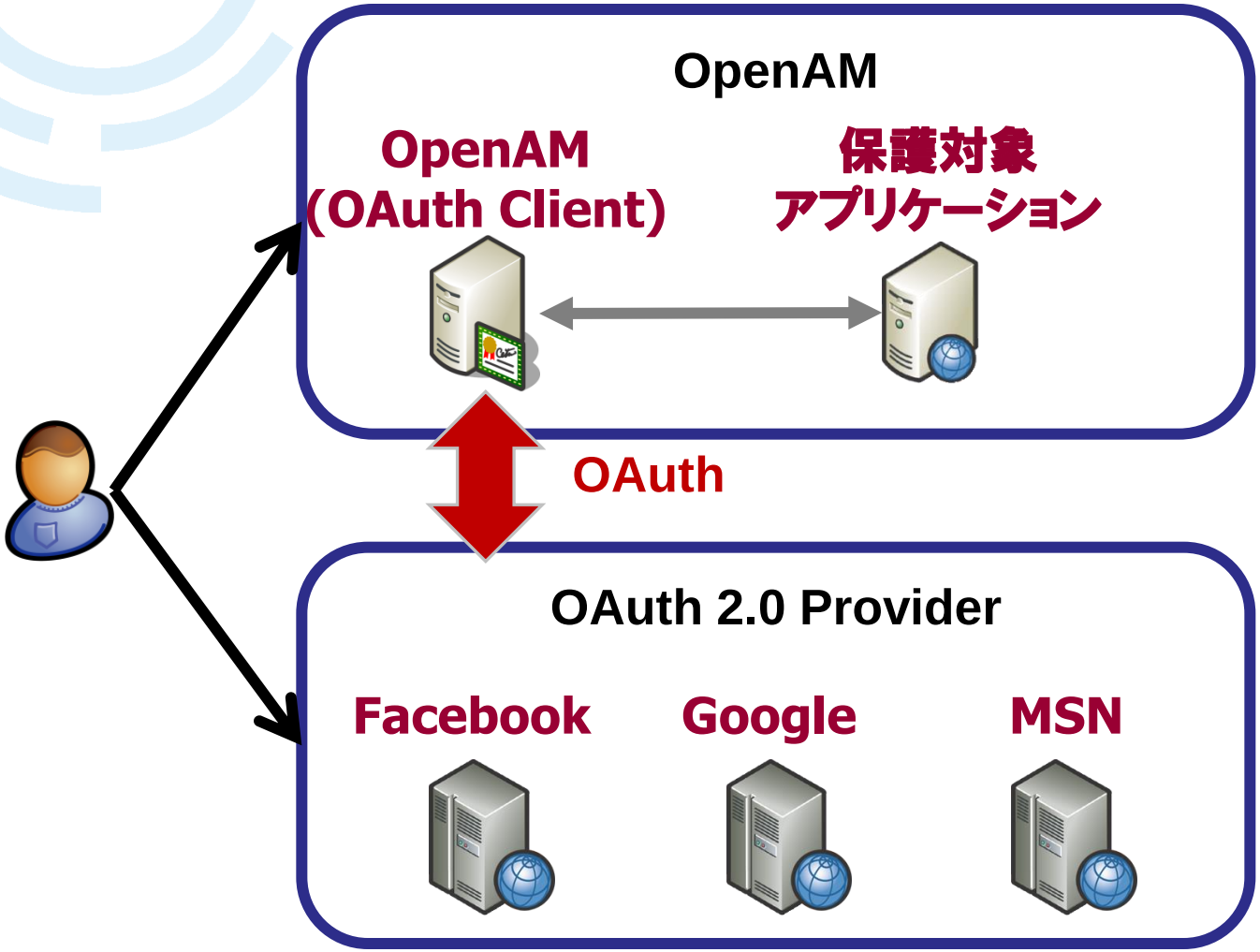
リスク評価

- 前述のチェックに設定したスコアの合計値が、リスク閾値に到達しなければ認証成功となる
  - 例）以下のように設定した場合
    a. 認証失敗のチェックのスコア = 1
    b. 位置情報国コードチェックのスコア = 2
    c. リクエストヘッダーチェックのスコア = 3
    d. リスク閾値 = 4

    ケース1: (a) + (b) < (d) ⇒ 認証成功
    ケース2: (a) + (c) = (d) ⇒ 認証失敗

OAuth 2.0 クライアント認証

- OpenAM 10.0ではクライアント認証機能が追加



OAuth 2.0 クライアント認証

- Facebook（プロバイダ）と連携した場合の動作は以下のようになる
  - ユーザがOpenAMにアクセス
  - Facebookのログインページにリダイレクト
  - ユーザはFacebookのIDとパスワードを入力する
  - アクセスの許可を問われるので、ユーザはそれを許可する（Yesボタンクリック）
  - OpenAMにログイン完了（この際にFacebookのユーザ情報がOpenAMにマッピングまたは登録される）

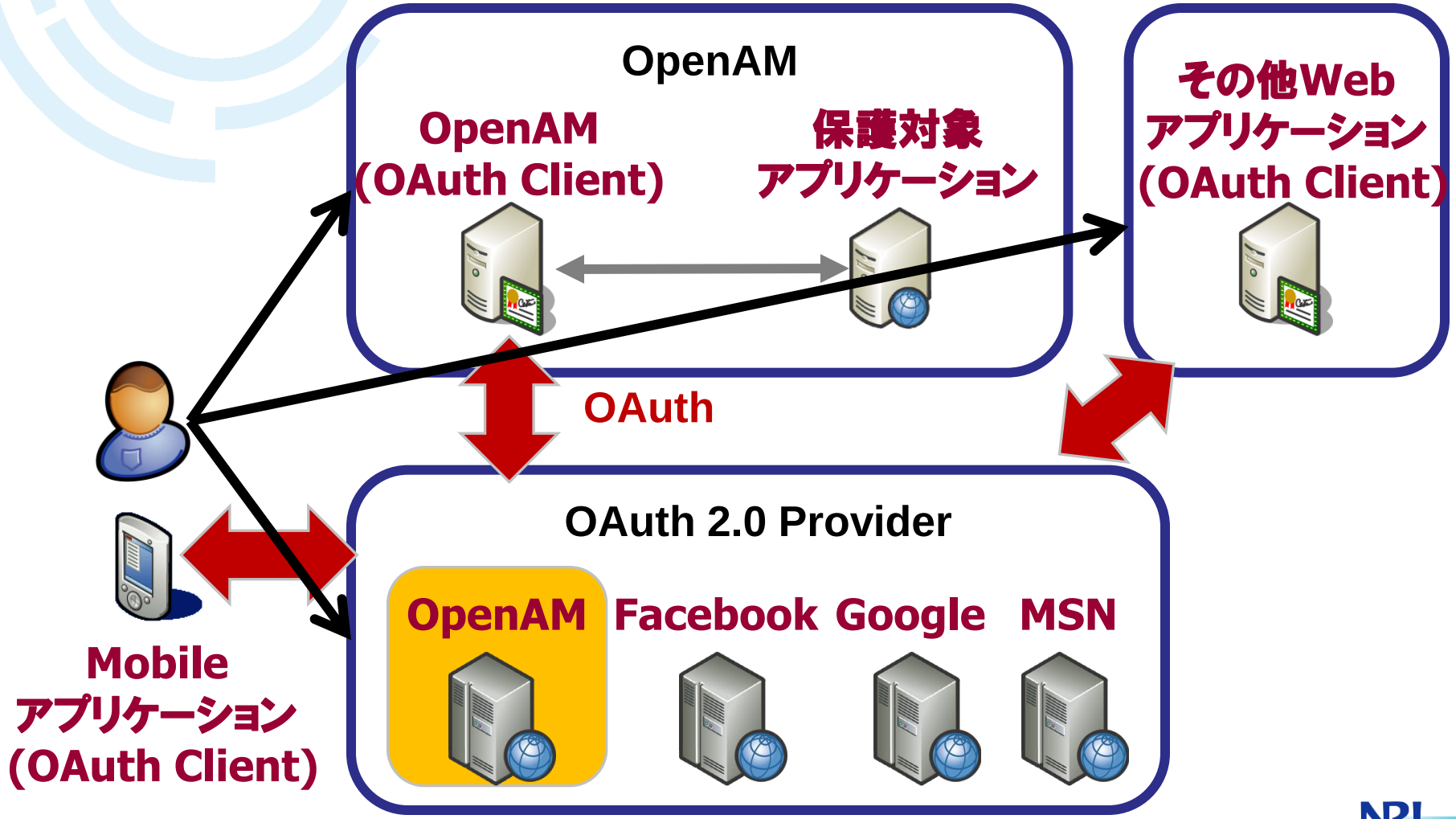
Facebookなど、OAuthに対応したサービスのアカウント情報でOpenAMにログイン可能となる

OpenAM 10.1 Xpress の新機能

- OAuth 2.0 プロバイダ機能
- セッションフェイルオーバの改良 （省略）
- OATH対応

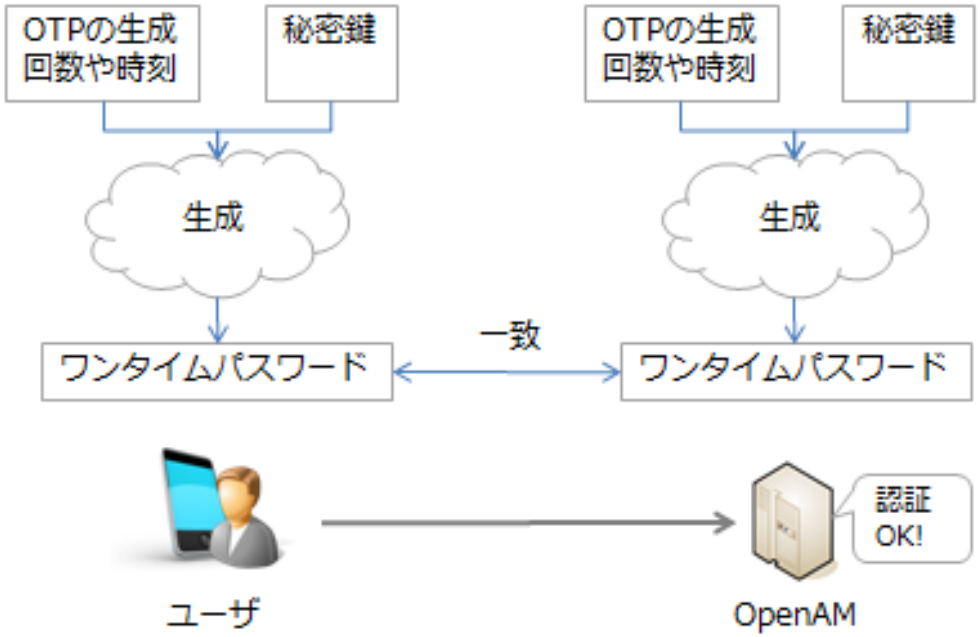
OAuth 2.0 プロバイダ機能

- OpenAM 10.1 Xpressではプロバイダ機能が追加



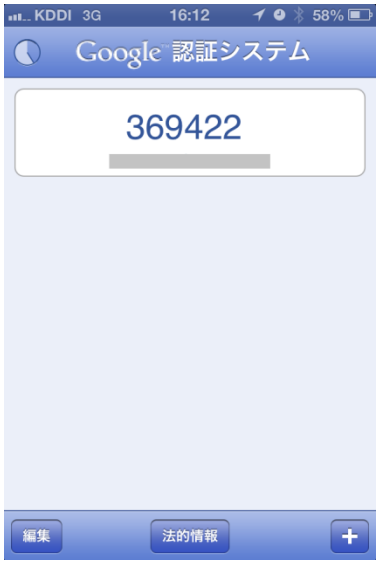
OATH対応

- オープンな認証仕様であるOATH(Initiative for Open AuTHentication)に準拠したワンタイムパスワード認証に対応
- 2種類のワンタイムパスワード方式
  - HOTP：カウンタベース
    - ✓OTPの生成回数(カウンタ)をもとにOTPを生成
  - TOTP：時刻ベース
    - ✓時刻をもとにOTPを生成



OATH対応

- オープンな標準仕様のため、OATH対応のトークン発行アプリ/デバイスをそのまま利用可能
  - Google Authenticator
  - Android Token
  - DS3 Oath
  - Yubikey

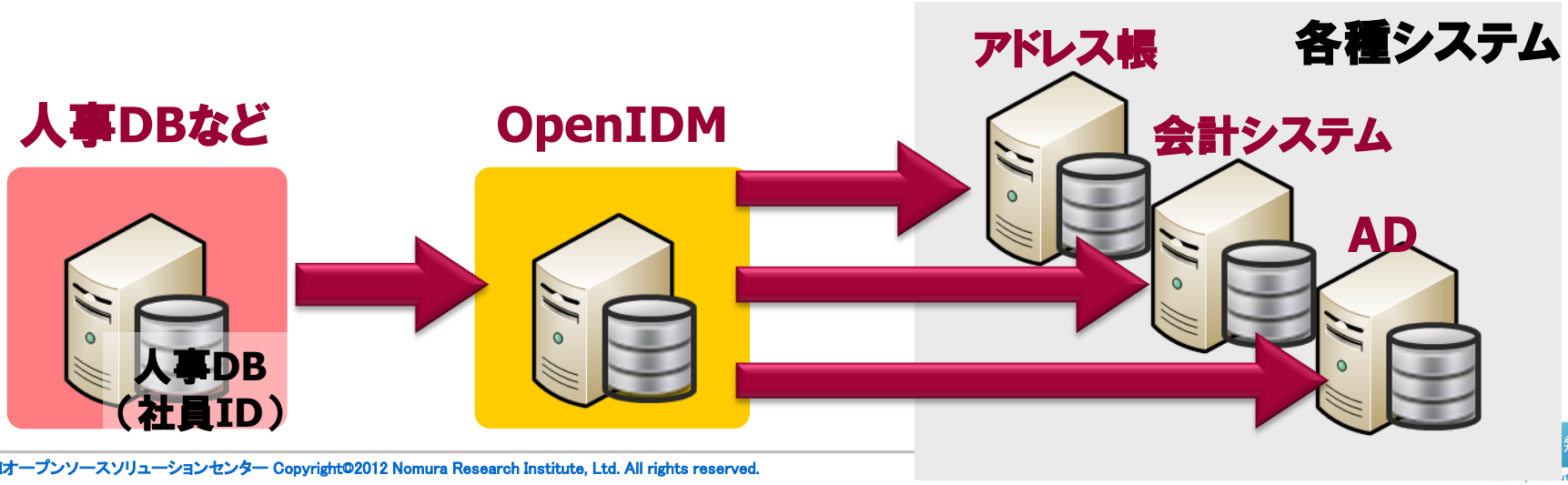


(出所) Android Token https://code.google.com/p/androidtoken/
DS3 Oath https://play.google.com/store/apps/details?id=uk.co.bitethebullet.android.token&hl=ja
Yubikey http://www.flickr.com/photos/yubikey/8357169183/

- オープンソースで「統合ID管理」、OpenIDM

OpenIDMの概要

- OSSのアイデンティティ管理(ID管理、アイデンティティーマネジャー)製品
- ForgeRock社により2010年からフルスクラッチで開発
- オープンスタンダードな技術の採用、モジュラー型アーキテクチャ、外部リソースとのコネクタにOpenICFを採用、REST APIの採用などによって、高い柔軟性と拡張性を備えたアイデンティティ管理製品



OpenIDMの特徴

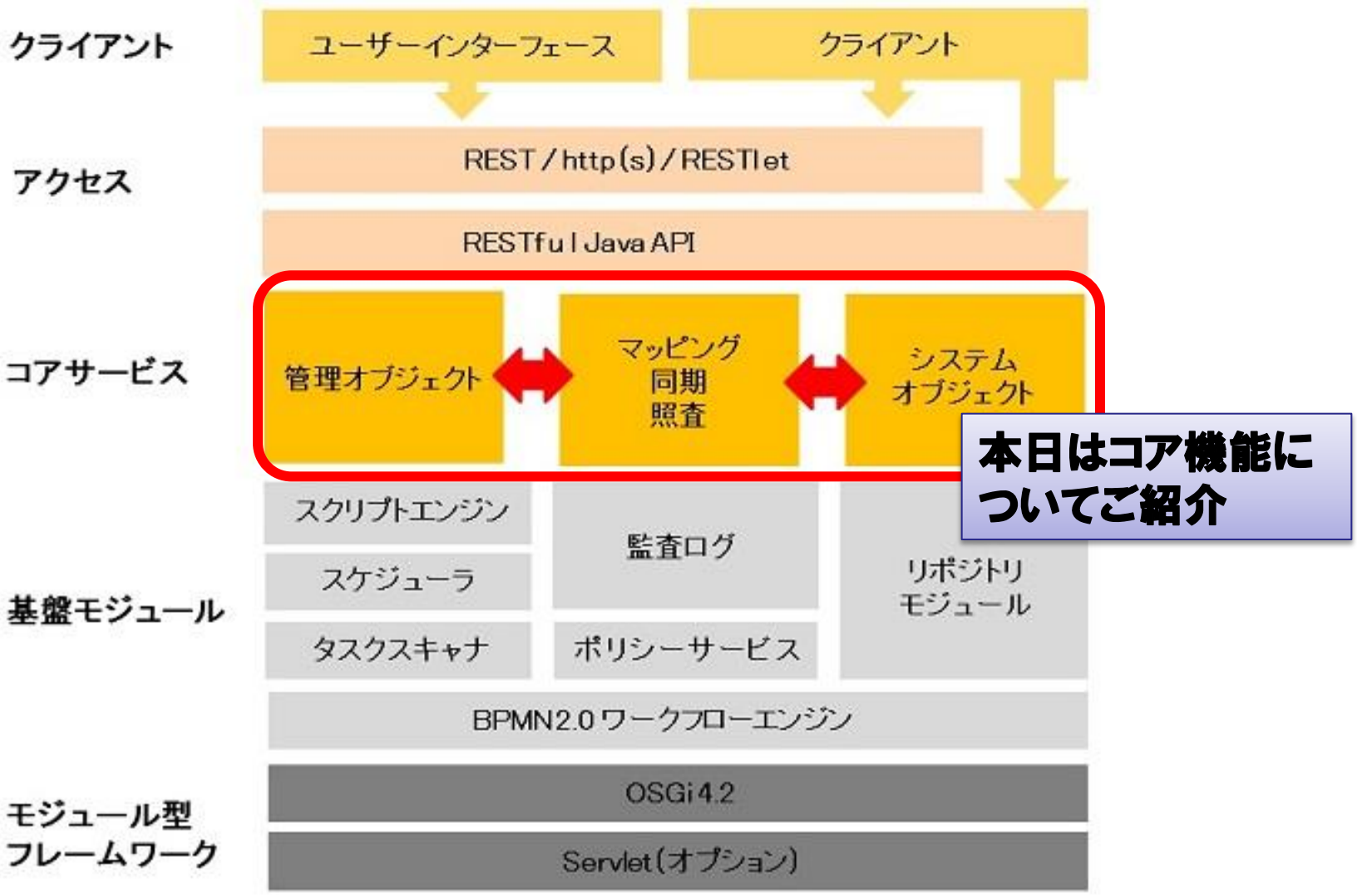
- **REST APIの採用**
  - OpenIDMに対するあらゆる操作をHTTPで行うことが可能であり、他システムとの連携が容易に可能
- **サーバーサイドスクリプトエンジン**
  - Java上で動作するJavaScriptエンジン（Rhino）を組み込んでおり、設定情報、マッピング情報、カスタムロジックを柔軟に定義可能
- **柔軟なデータモデル**
  - ID情報のスキーマを要件に合わせて柔軟に定義可能
  - データはJSON形式で格納される

他製品との機能比較

- 基本的な機能は実装されつつある
- OpenIDMで不足している機能については拡張機能としてNRIで実装予定

機能	OpenIDM	他OSS製品	商用製品A
Webブラウザによる設定画面	○	○	○
データ管理機能	○	○	○
データ検索機能	○	○	○
データ同期機能	○	○	○
IDの一括登録、一括変更	○(CSV)	○(CSV)	○
LDAPグループの作成、変更	○	○	○
IDのLDAPグループへの配属情報の一括登録	○	○	○
CSVアップロード機能	×	○	○
CSVダウンロード機能	×	○	○
パスワード自動生成機能理	△	×	○
メール通知機能	○	×	○
オンラインサインアップ機能	○	×	○
マルチバリューカラムの編集	○	×	○
プロビジョニング先としての任意テーブルの選択	○	○	○
アカウントロック解除機能	×	×	○
複数管理者によるユーザー管理機能	○	×	○
管理者の階層化機能	×	○	○
管理範囲の指定機能	○	○	○
エンドユーザへの情報公開機能(ユーザー自身のプロフィール画面)	○	×	○
プロビジョニング先としてOracle、LDAPおよびMySQLのサポート	○	○	○
ロールによる権限管理	○	×	○
認証DB更新履歴出力機能	○	×	○
ログ出力	○	○	○

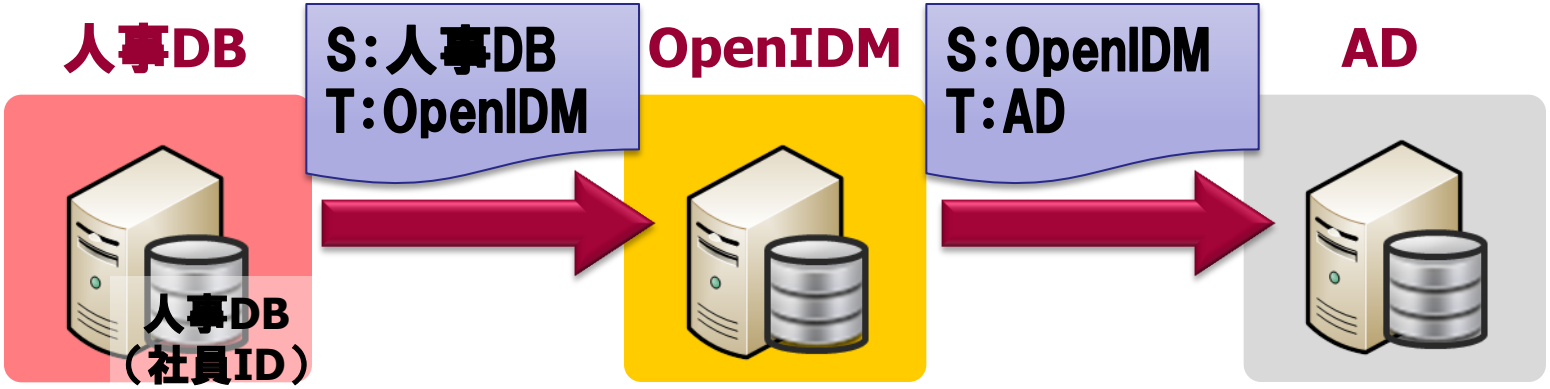
OpenIDMのアーキテクチャ



(出所)野村総合研究所 OpenStandia OSS紹介 OpenIDM最新情報 http://openstandia.jp/oss_info/openidm/

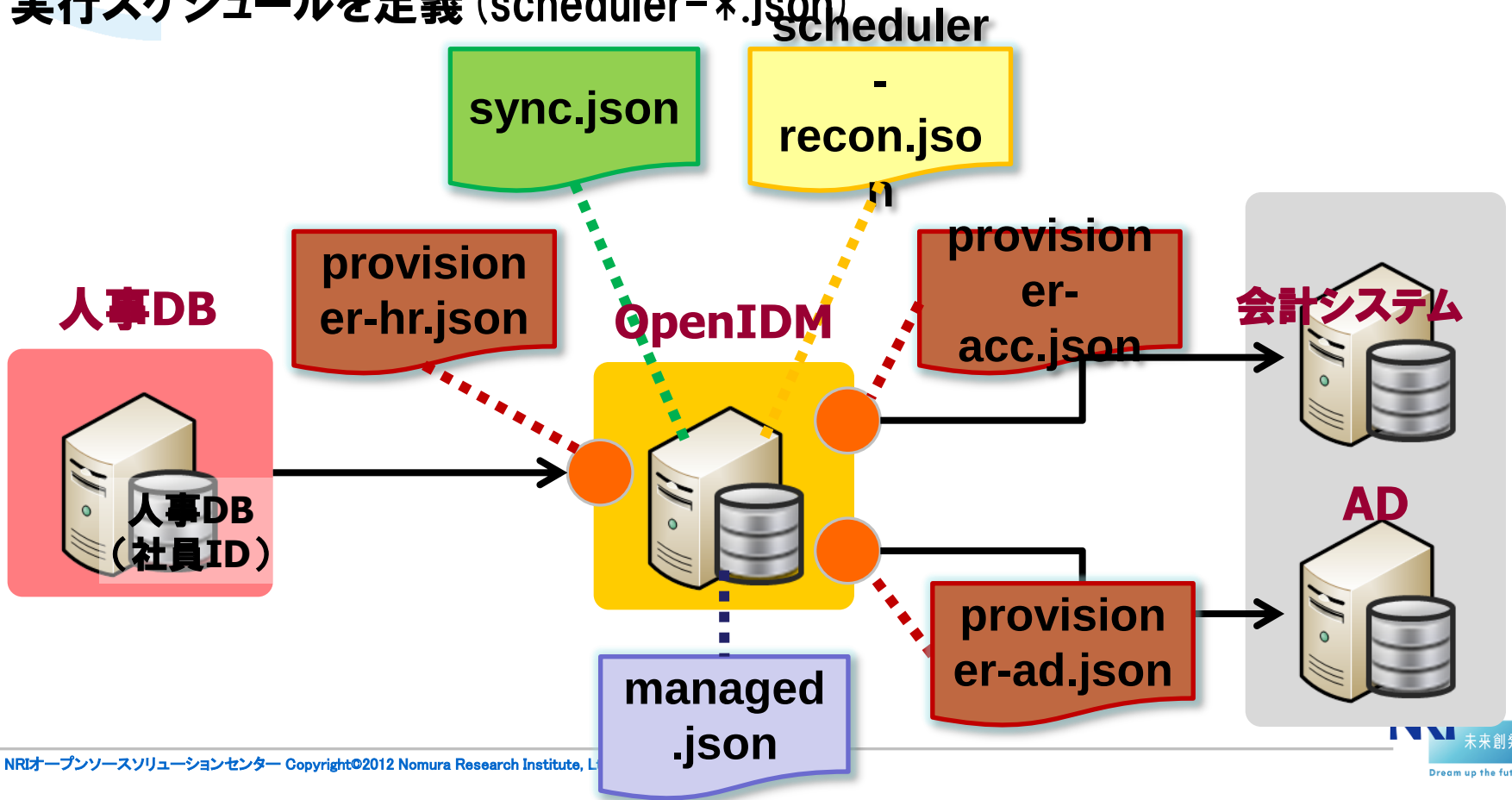
OpenIDMの同期機能

- OpenIDMでは双方向の同期をサポートしている
- ソースとターゲットを指定して同期の設定を行う
  - ソースを源泉データ、ターゲットをOpenIDMのリポジトリのデータと設定すると源泉データからのデータ取り込みとなる
  - 逆に、ソースをOpenIDMのリポジトリ、ターゲットを外部リソースに設定すれば、プロビジョニング処理となる



同期に関する設定 全体像

- OpenIDMのリポジトリに格納するデータ(Managed Objects)を定義(managed.json)
- 外部リソース(System Objects)を表すコネクタ定義を設定 (provisioner-*.json)
- System ObjectsとManaged Objectsをマッピング定義(sync.json)
- 実行スケジュールを定義(scheduler-*.json)



- （事例）企業がクラウドサービス（SaaS）を利用

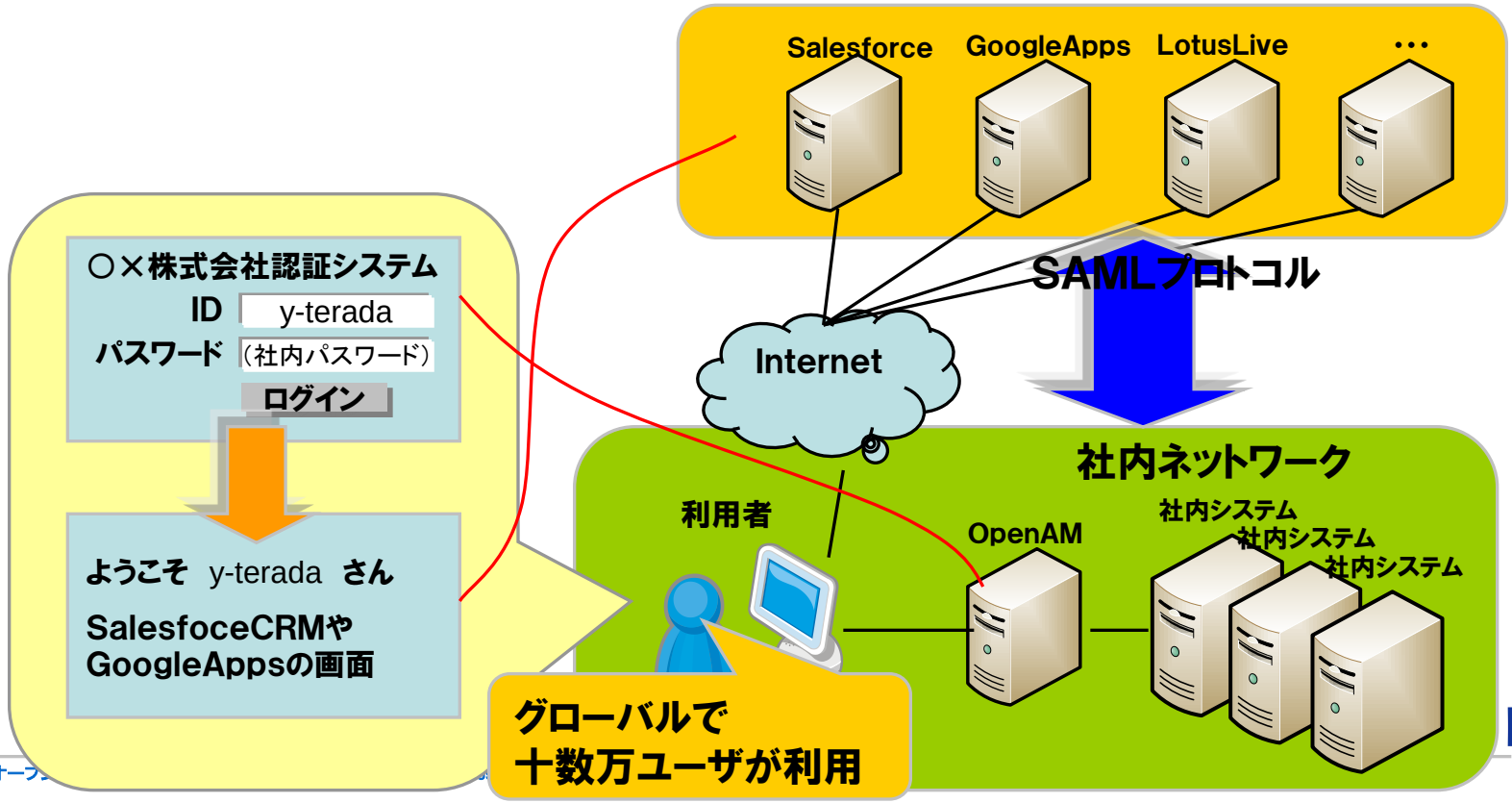
（事例）大手家電メーカー　クラウドサービスとのSSO

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

GoogleAppsやSalesforceCRMとのシングルサインオン

（要件）
・社内システムのID、Pwを使って、Salesforce CRMやGoogleAppsにログインしたい。
・パスワードは社外（SalesforceCRMなど）に置きたくない。

（ソリューション）
・業界標準の「SAML」プロトコルを用いて、社内システムとSalesforeceCRM、GoogleAppsとを接続（シングルサインオン）。
・社内LDAPのID／Pwを使って、Salesforece CRM、GoogleAppsにログイン可能に。



NRI 未来創発
Dream up the future.

- （事例）企業がクラウドサービス（SaaS）、ASPを提供

（事例）シスメックス株式会社

競合他社と差別化し、将来の収益の柱として、顧客への「サービス」を強化

導入目的

- 競合他社との差別化のため、サービス提供に力を入れている。
- 顧客である医療機関に対して、製品情報、医療機関同士の情報交換、医療機関の事務効率化などを目的としたサービスの提供を計画。
- 既存のパッケージやクラウドサービスをフルに活用し、短期間に多くのサービスを提供できるようにするための、プラットフォームを構築。

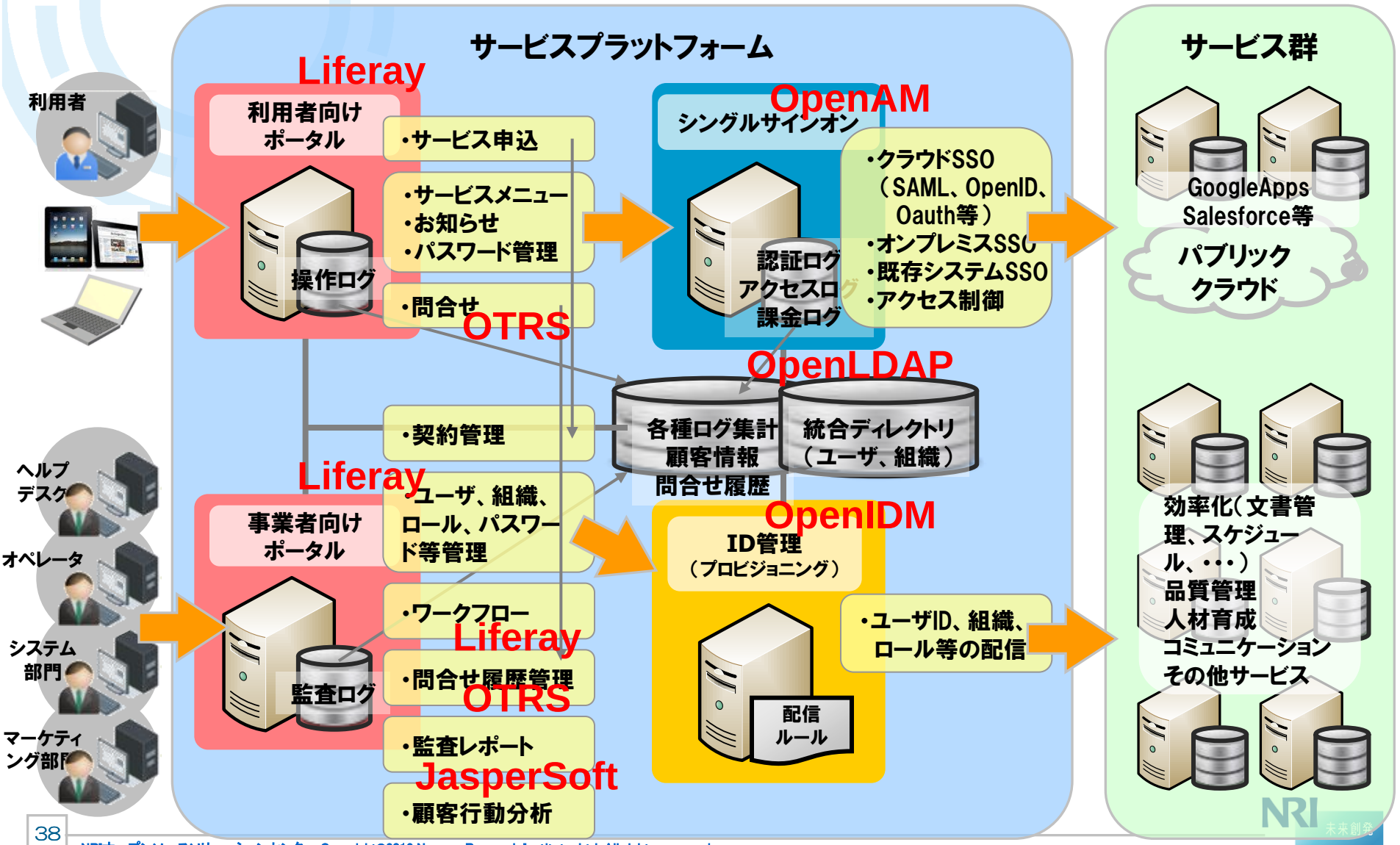
導入効果

- プラットフォームが完成し、今後様々なサービスを短期間に提供することが可能に。
- 今後、情報分析（BI）も導入し、効果を測定しながらサービスを追加。

（事例）サービスプラットフォームとしての提供

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

- 大手製造業など



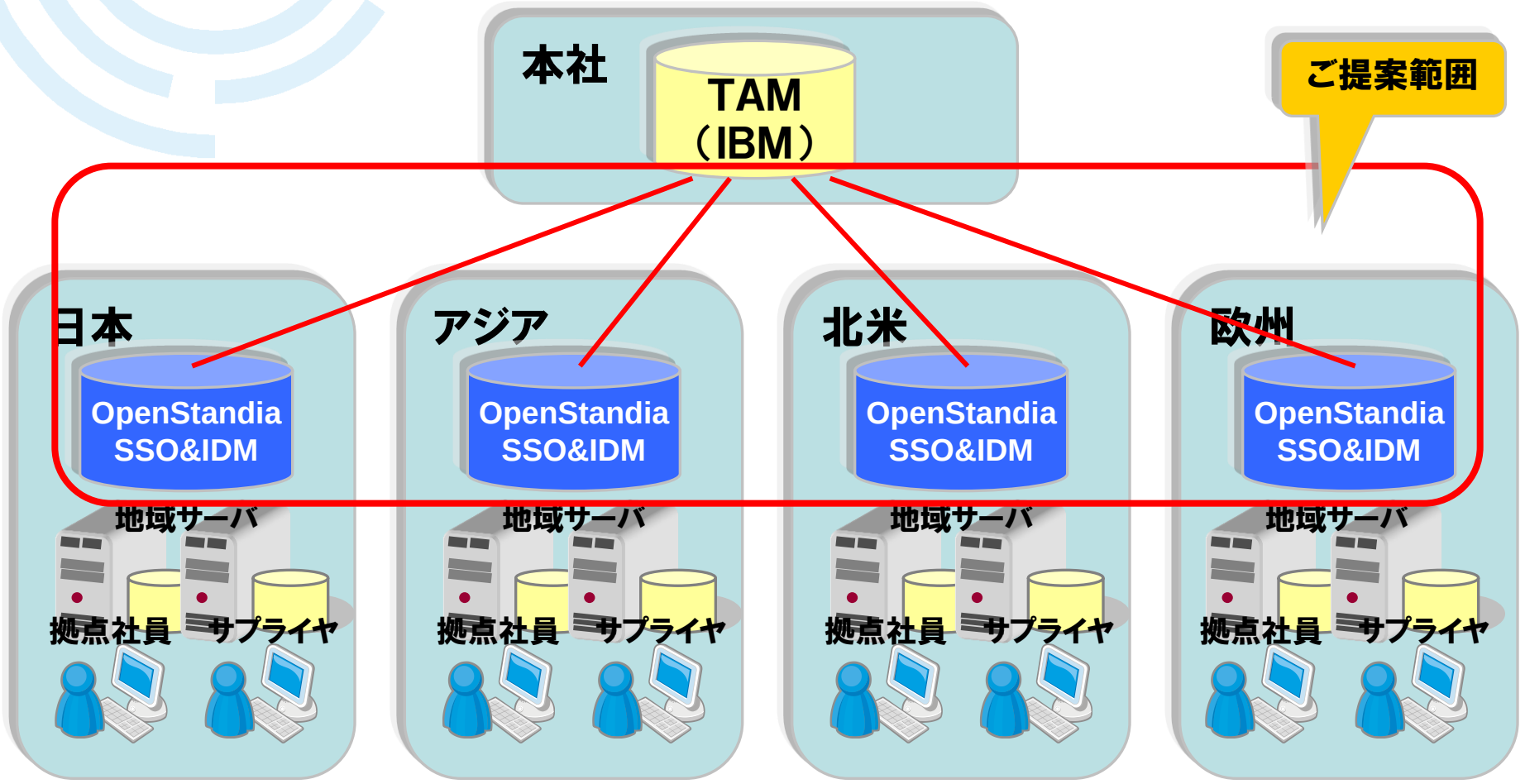
- （事例）グループ企業、グローバル規模での統合認証、統合ID管理

グループ・グローバル企業での統合認証基盤の目的

- **内部統制の強化**
  - 各社、各国(各拠点)に任せるのではなく、グループ、グローバルとしてID管理、認証、認可の機能を提供することで、品質を確保。
    - ✓但し、既に高度なID管理を実現できている会社については、その仕組みを継続利用。
- **積極的な人材活用**
  - 異動先、出向先でも、スムースに情報システムにアクセスできるための、統合的なID管理、及びアクセス制御の仕組みを構築。グループ、グローバルでの積極的な人材活用を推進。
- **管理業務の効率化**
  - 各社に対してID管理業務をシェアードサービスとして提供することで、グループ全体のID管理業務を効率化する。
- **情報共有/情報システム活用の強化**
  - グループ、グローバルでの情報共有/情報システム活用を強化する(グループ、グローバルで共有するシステムが増える)にあたり、グループ、グローバルでの認証基盤、シングルサインオン基盤を整備する。

（事例）大手製造業 グローバル統合認証基盤

- 各拠点のユーザIDをOpenStandiaで統合し、さらに本社のTAM（既存）と連携。



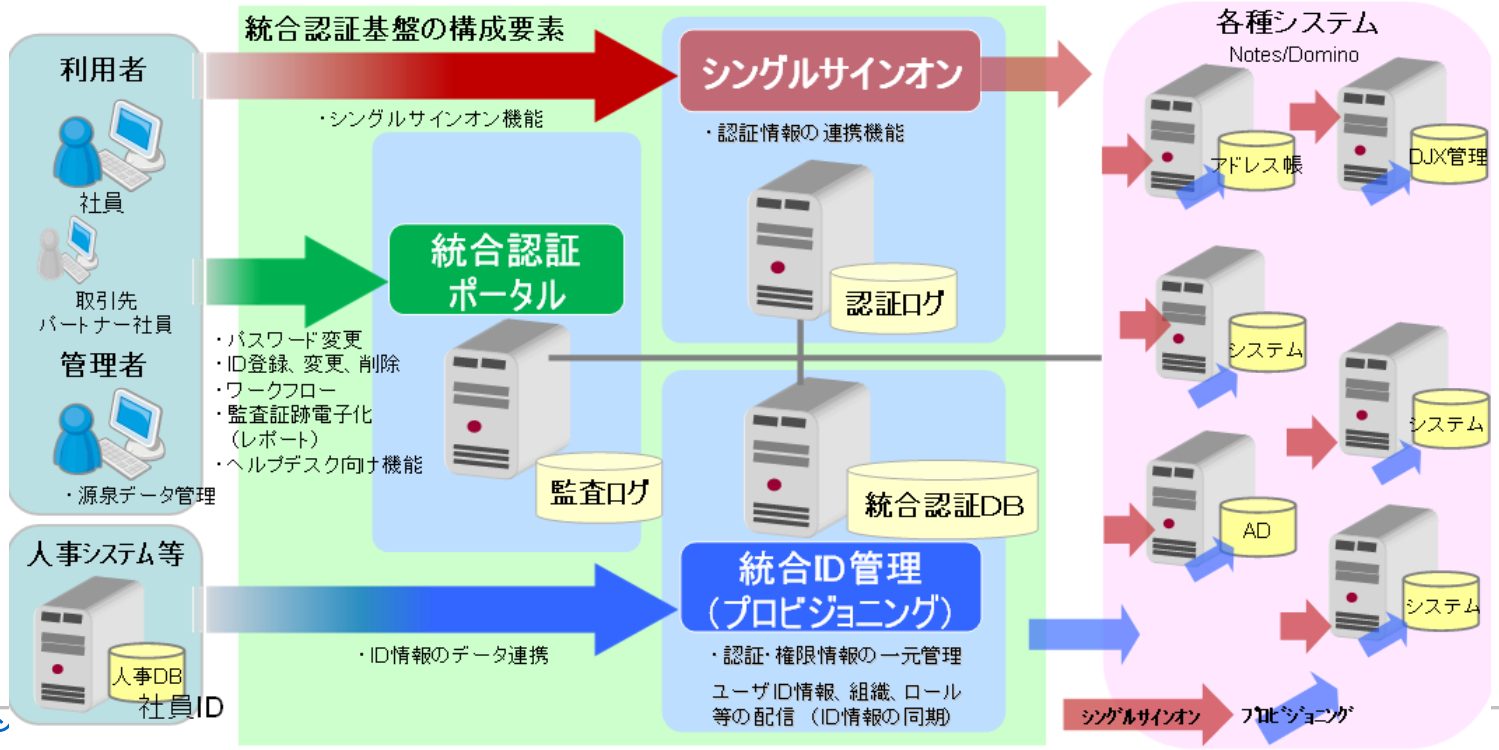
- （事例）ID管理業務の効率化、内部統制の強化

（事例）大手不動産会社　人事異動業務の効率化

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

人事異動時のID管理業務を大幅に効率化、GoogleAppsにも対応

- **現行システム概要**
  - 人事、会計など、基幹業務システムと、AD、NotesなどのOA系・情報共有系システム。GoogleAppsの利用や、スマートフォンからの情報照会を新たに開始。
- **課題**
  - 従来は、人事異動時のユーザIDの更新業務を、全て人手で行っており、情報システム部の大きな負担となっていた。GoogleAppsの利用を開始するにあたり、さらなる負担増を避ける必要があった。
- **ソリューション**
  - ばらばらだったIDを統合管理し、人事システムとも連携。異動業務を自動化し、大幅に効率化。従来紙で行っていた各事業部との人事異動に関するやりとりも、システム化、ワークフロー化。



NRI 未来創発
Dream up the future.

- （事例）既存のSSO・ID管理システムのリプレース

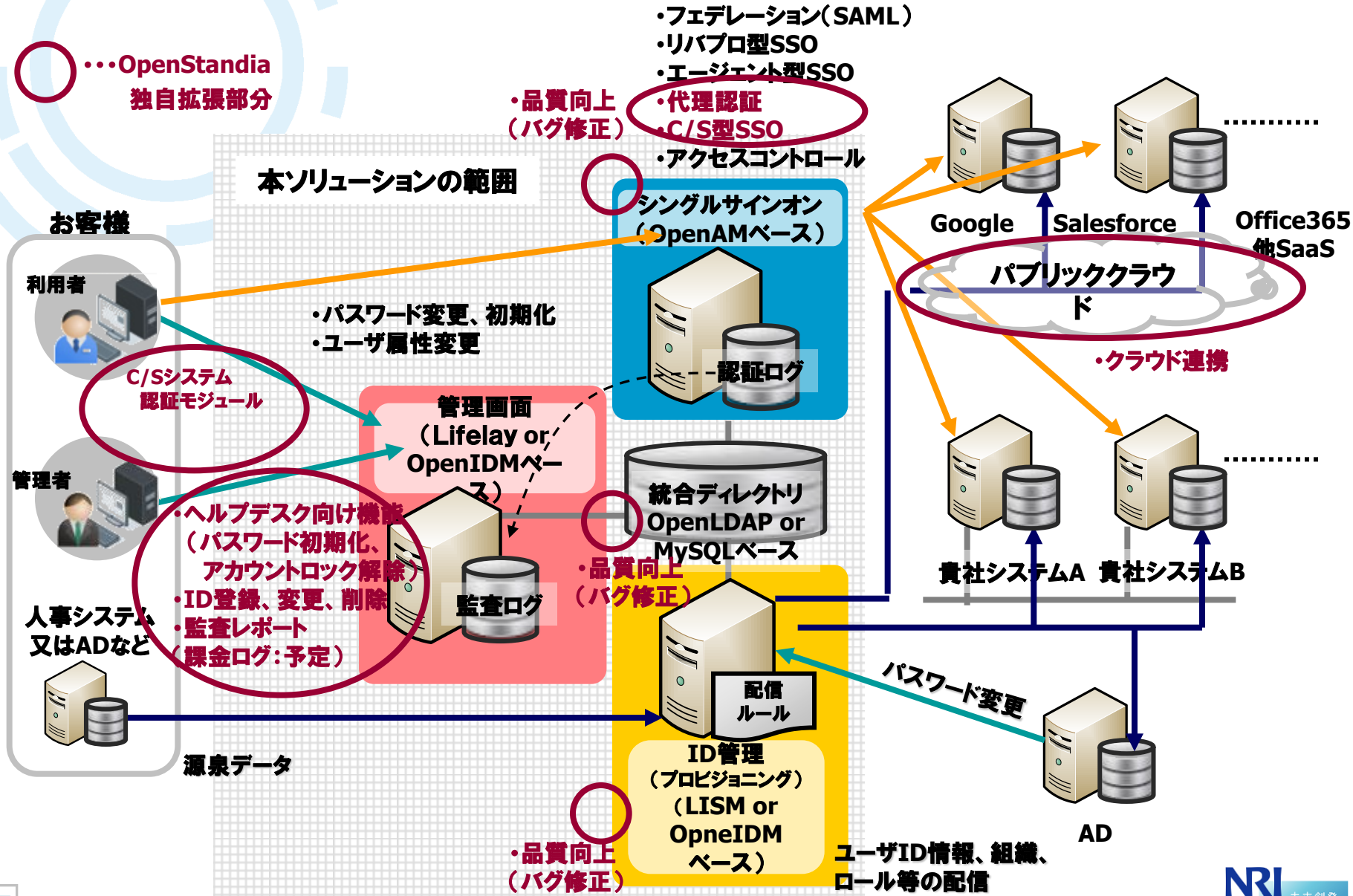
既存のSSO・ID管理システムのリプレース

- よくお話しをいただく、移行元対象製品
  - Tivoli Access Manager（TAM）
  - Oracle Access Manager（OAM）
    Oracle Identity Manager（OIM）
  - CA Site Minder
  - RSA Access Manager
  - Sun Access Manager/OpenSSO Enterprise
    Sun Identity Manager

- 移行理由
  - 利用範囲の拡大（たとえば、グループ企業を対象に加える）により、大幅なユーザライセンス費用の増加が発生する。
  - クラウドサービス連携のためにSAMLを使いたいが、別オプションであり、追加のライセンス費用が高額。
  - 現在の認証基盤が複雑で、維持管理ができない。

- **オープンソースを活用した統合認証基盤の構築**
  - シングルサインオン（SSO）、ID管理、ID連携、認証、LDAP、AD
  - SAML対応、GoogleApps連携、SalesforceCRM連携

ソリューション全体概要



OpenStandia SSO&IDMとは

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

**OpenStandia/SSO&IDMは、ID管理を一元化し、
統合的なシングルサインオン環境を低コストで構築するパッケージソューションです。**

※ オープンソース製品を組み合わせ、バグFIXおよび動作保証を行い、さらにお客様企業のID管理業務の効率化を実現するための独自の機能を追加しております。

■ 弊社のOpenStandiaをご利用いただく場合には以下5つのメリットがあります。

ユーザ数無制限のライセンス

一般の商用製品は、ユーザ数が多くなるとライセンスが非常に高額になります。OpenStandia/SSO&IDMは、オープンソースをベースとしております。年間サポートサービスは、サーバ台数によって課金させていただいており、ユーザ数は無制限です。

豊富な導入実績

250人程度の中小企業様から3万人を超える大企業や、100万人を超えるクラウドサービスなどへ導入いただいており、これら全てのお客様に高い評価をいただいております。

独自の機能拡張が豊富

オープンソースの弱点と言われる管理系の機能を大幅に増強しました。また、ワークフロー機能や、システム利用状況の分析などの周辺機能も充実しております。

導入コンサルが可能

250人程度の中小企業様から3万人を超える大企業や、100万人を超えるクラウドサービスなどへ導入いただいており、これら全てのお客様に高い評価をいただいております。

運用維持管理も引き受け可能

ご要望に応じて、年間サポートサービスを拡張した維持管理サービスをご提供します。

NRI 未来創発
Dream up the future.

OpenStandia SSO&IDMとは

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

OpenStandia/SSO&IDMは、商用製品以上の機能及び動作保証を実現しながら、オープンソースのメリットを生かして低コストで提供します。

	商用製品	OpenStandia	素のOSS（OpenAM/IDM、Lifelay、LISM等）
初期パッケージコスト	× 高い（値引きしてもロックインしてから保守で回収）	○ 安い	○ 不要
サポート費用（製品の場合は保守料）	× 高い（ユーザ数が多い場合）	○ 安い（素のOSSよりやや高いレベル）	○ 安い（一般のOSSサポートを想定）
製品機能	○ 充実	○ 充実	× 不足する機能がある（管理機能、監査機能、その他特殊接続要件など）
標準仕様対応	× 遅い・オプション（SAMLやKerberosがオプション、OAuth、SCIMなどに未対応）	○ 早い・標準装備（SAML、Kerberos、Oauth、SCIM対応、OpenID近日対応）	○ 早い・標準装備（SAMLは標準装備、Oauth、SCIM対応、OpenID近日対応）
マルチチャネル	× ブラウザのみ	○ ブラウザ、C/S、スマートフォン、タブレット、ソーシャル等に対応	○ ブラウザ、C/S、スマートフォン、タブレット、ソーシャル等に対応
動作保証・サポート	△ 有り（サポート期限短くVerUP必要）	○ 有り（10年以上長期サポート可能）	× 無し
導入リスク	○ 低い（製品保証があるため）	○ 低い（製品保証があるため）	× 高い（自己責任、バグFIXや不足部分の開発等、専門知識が必要）

- 最後に

（まとめ）オープンソースの活用は新たな段階へ

オープンソースは重要な社会インフラ

企業にとって、必要不可欠となったオープンソース
（サービスによる差別化、グローバル）

全社的なオープンソースの活用

NRI OpenStandiaは、オープンソースを『社会インフラ』として、普及・発展させます。

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。

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センターへ

ossc@nri.co.jp

http://openstandia.jp/

NRI 未来創発

Dream up the future.