

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
田中 穰



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 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 : osscc@nri.co.jp Web: <http://openstandia.jp/>



●はじめに

自己紹介:田中 穰(たなか ゆたか)

- 2004年 野村総合研究所のオープンソースを利用したプロジェクトのアーキテクチャ設計を複数担当。オープンソースの社内展開に従事。



- 2007年 NRI社内の企画事業立ち上げ施策でオープンソースビジネス(OpenStandia)の立ち上げ。



- 2012年 上海の関連会社で中国へビジネス展開するための調査&OJTを実施。
- 2013年 上海より10月に帰任。
技術担当から営業・マーケティング担当へ。

● 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と統合ID管理とは

● オープンソースを活用した統合認証基盤

- アーキテクチャ
- 各種シングルサインオン(SSO)方式
- 統合ID管理、プロビジョニング
- ID管理ポータル

● 事例紹介

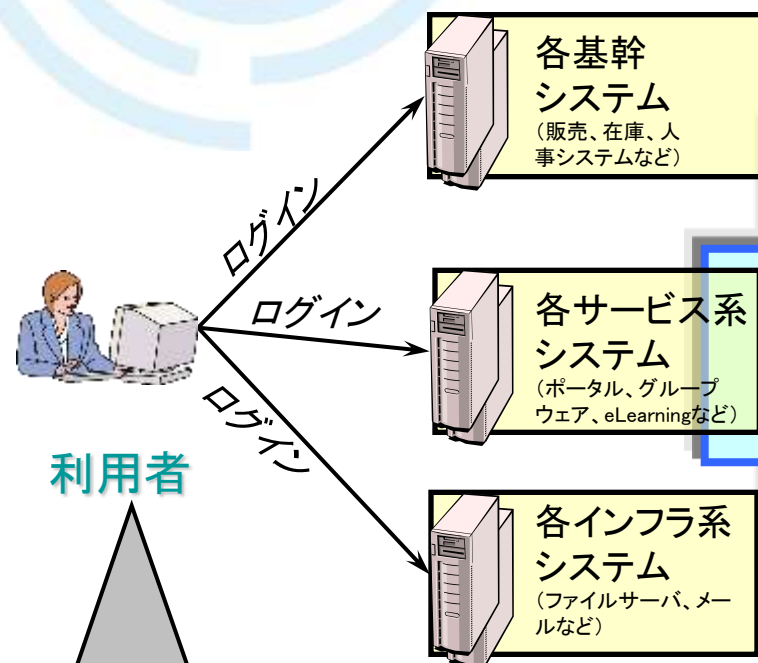
- 攻めの事例、守りの事例、グローバル事例、SaaS関連事例

● 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(SSO)について

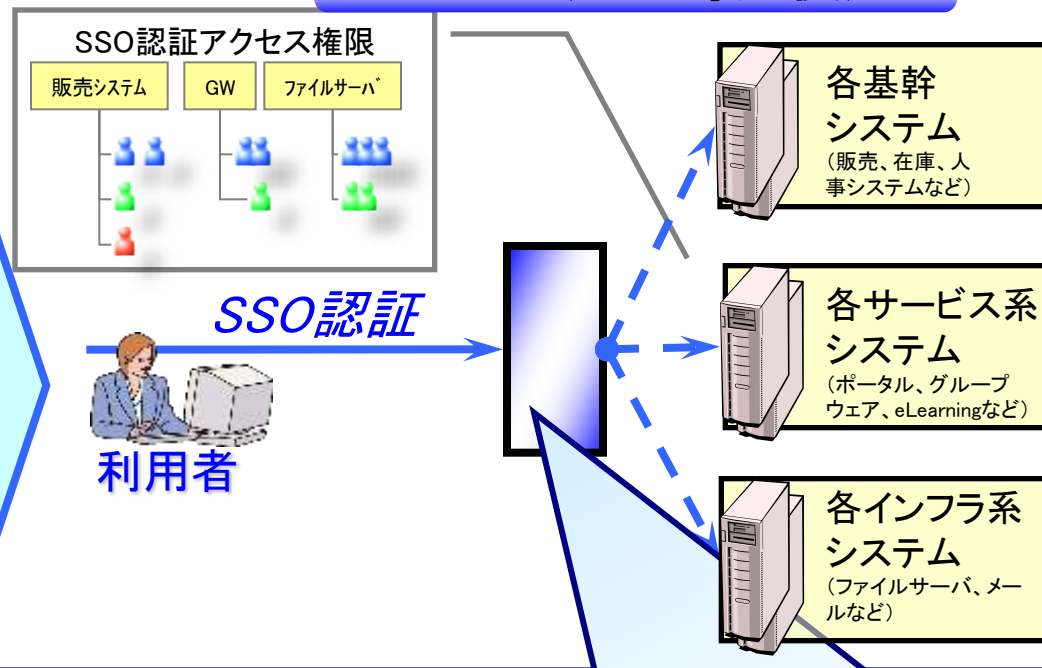
- SSO認証を導入すると、様々なシステムへのSSOとアクセス制御が可能となり、利用者の利便性向上やセキュリティ向上につながる

As-Is(現状運用)



各システム個別に、別々のID/パスワードで認証

To-Be(SSO導入後)

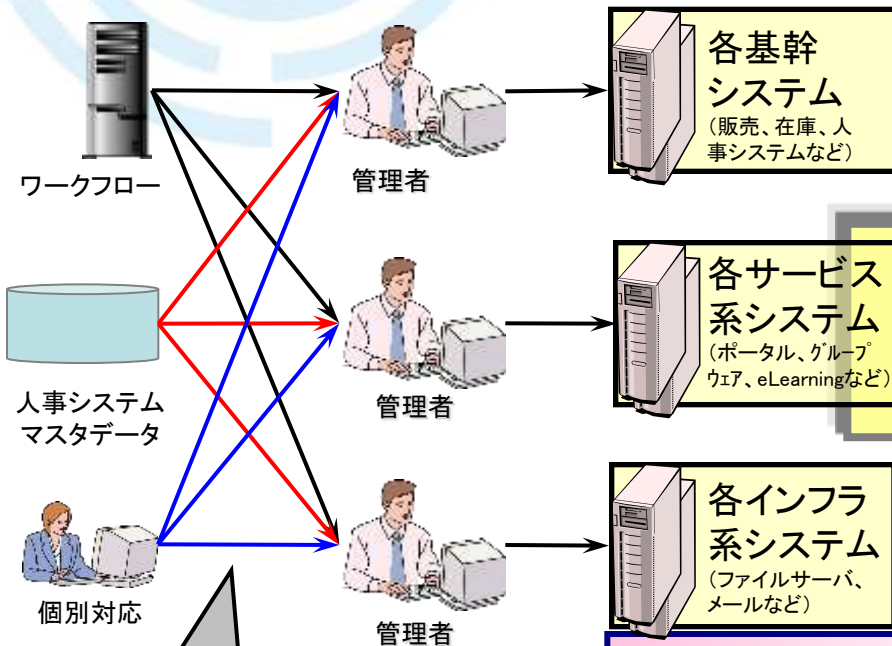


- アクセス権限付与に基づく厳密なアクセス制御
- セキュリティポリシーに基づいた厳密な認証インタフェース
- システムへのアクセスの認証の統合化による利便性向上
- アクセスログの一括取得
- 多様化する認証方式への対応
 - ✓ 対象システム : Web系システム、C/S系システム、OS...
 - ✓ 認証連携インタフェース : ID/PWD、生体認証、PKIなど

ID管理(プロビジョニング)について

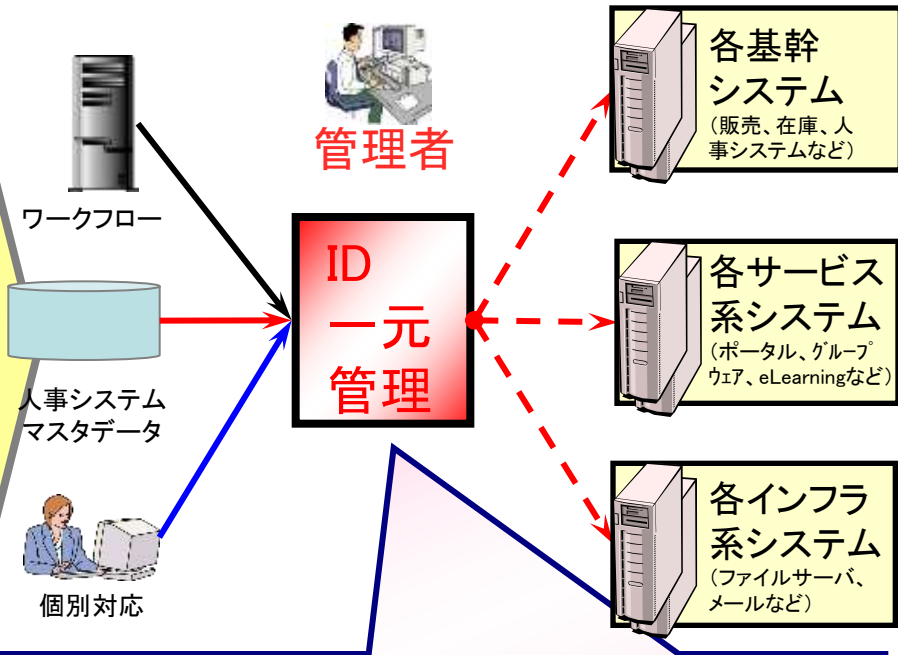
- 入社・退社・人事異動時に、利用システム毎のアカウントの個別ID管理(登録/修正/削除/参照)に対して、導入後は統合的に管理することにより、運用効率化・負担 & ID管理ミス軽減となる

As-Is(現状運用)



- ・システム毎の個別ID管理(追加/変更/削除/参照)
- ・システム毎のアカウントポリシー

To-Be(ID管理導入後)



- ID管理ライフサイクル(ユーザ情報の登録, 変更, 削除)の統合化
⇒IDのプロビジョニング(ユーザアカウントの適切な管理・提供)
- 監査・内部統制・セキュリティ対策
⇒ワークフローによる申請・承認、定期パスワード管理 など
- ID管理操作に対するログの一元管理
- 人事システムなどマスタ情報との登録連携、セルフサービスでの自動管理
- 業務サーバ上の不正アカウント有無のチェック

- 社内環境の変化、IT環境の変化、事業環境の変化により、いかに効果的にシステムを利用し、いかにその運用コストを下げるかが注目されてきている。

社内環境の変化

- 乱立するシステム、ユーザアカウント
- 内部統制、コンプライアンス強化、個人情報保護
- 増大する管理業務

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

内部統制、コンプライアンスの強化(守り)

- 退職者、契約切れ派遣社員などのIDの速やかな削除
- IDの追加、変更、削除、権限付与時に、ワークフローによる承認
- パスワードポリシーの強化
- 監査ログの記録と、監査レポート

利用者数の増大

広がる情報システムの利用範囲

部門 会社 派遣社員 取引先 グループ グローバル

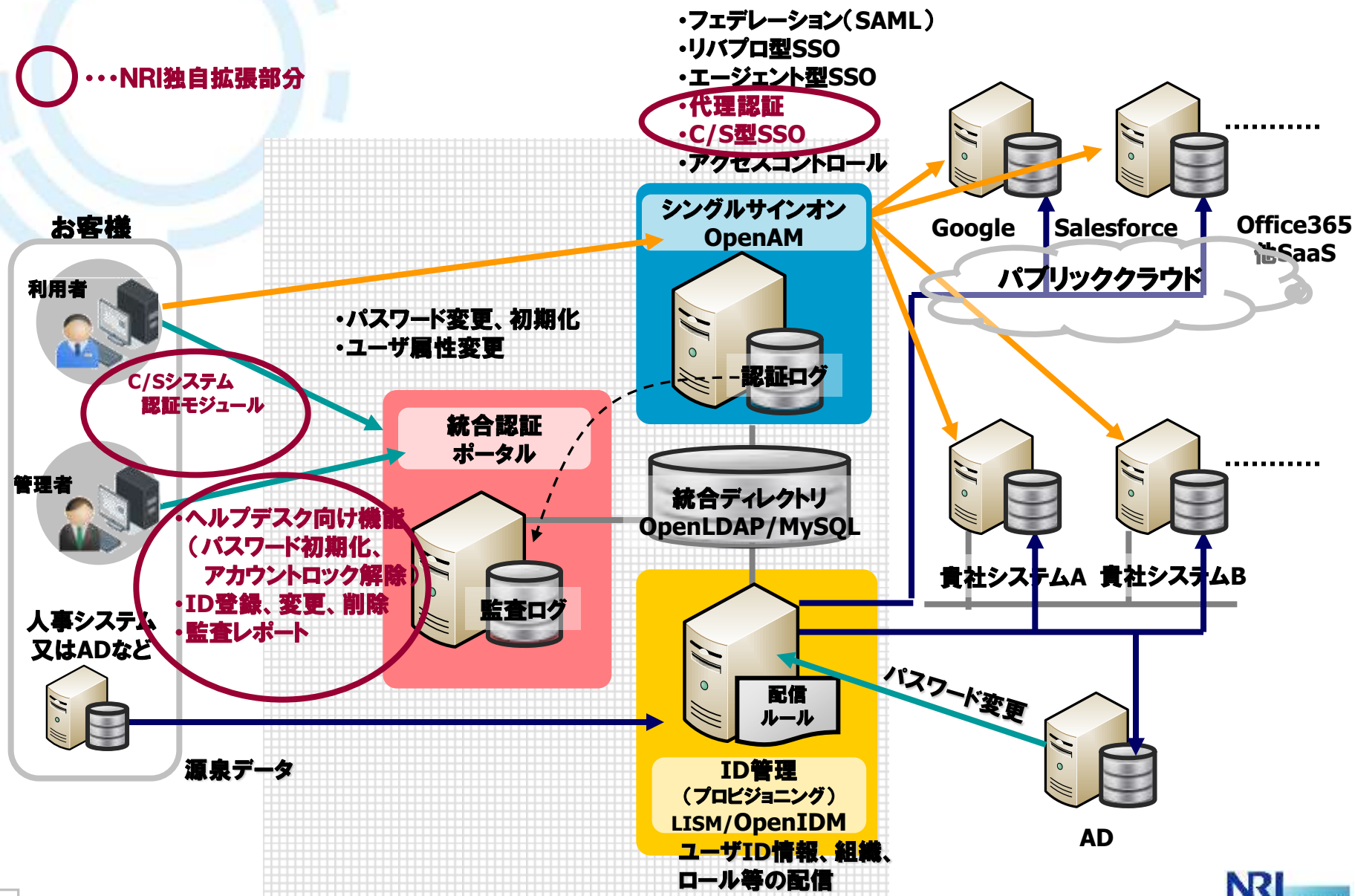
- 従来の部門内、会社という単位の情報システムの利用から、取引先、派遣社員、パートナー、グループ企業、グローバルなどへの範囲拡大
- グループ・グローバルでの人材流通を支えるID基盤

競争優位を実現する情報システム(攻め)

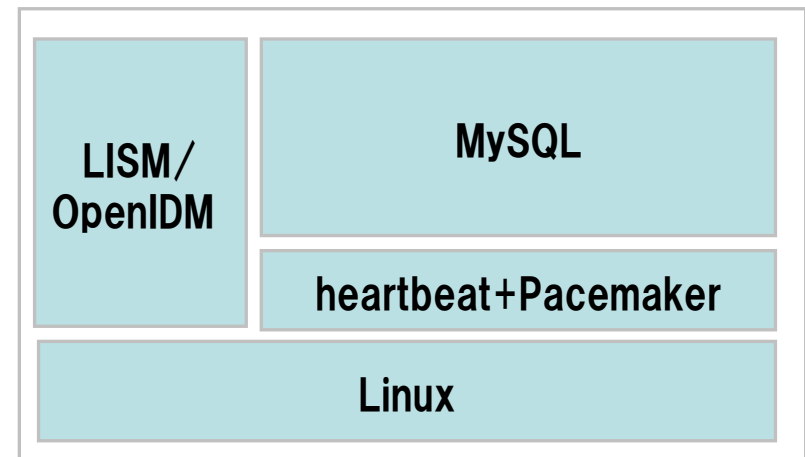
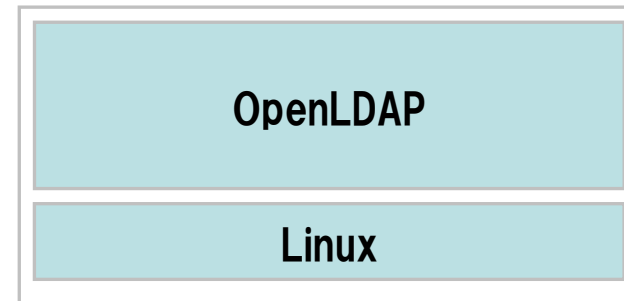
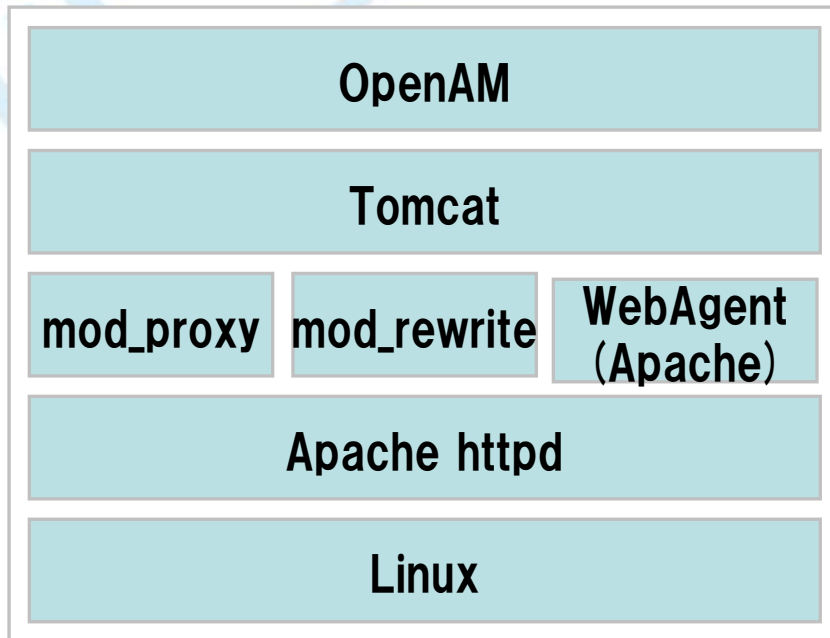
- **オープンソースを活用した統合認証基盤**
 - ▶ OpenStandia/SSO&IDM (OpenAM+OpenIDM+ α)

システム全体概要

○ ……NRI独自拡張部分



- SSO、統合ID管理のソフトウェアスタックをフルオープンソースにて実現

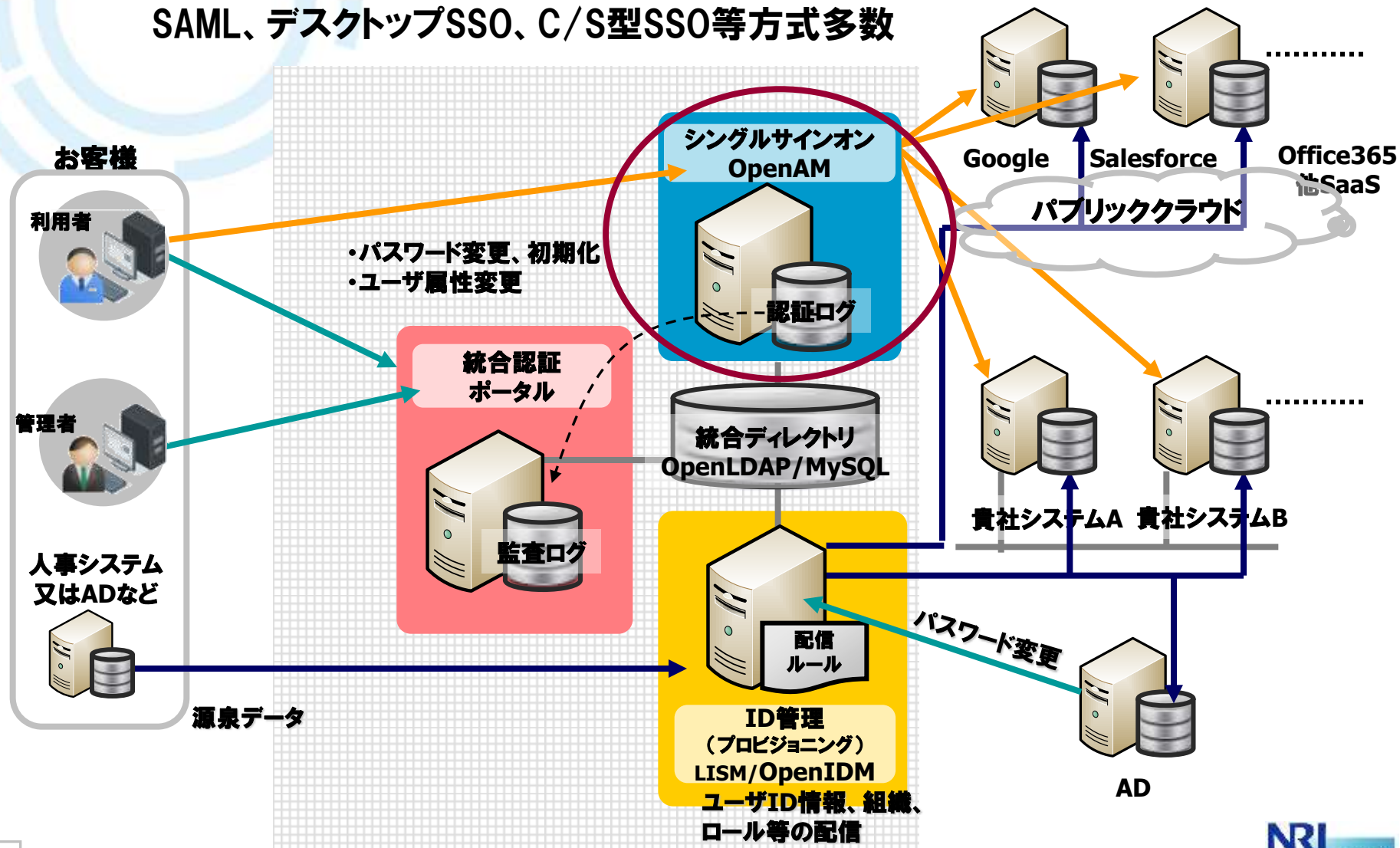


シングルサインオン
OpenAM

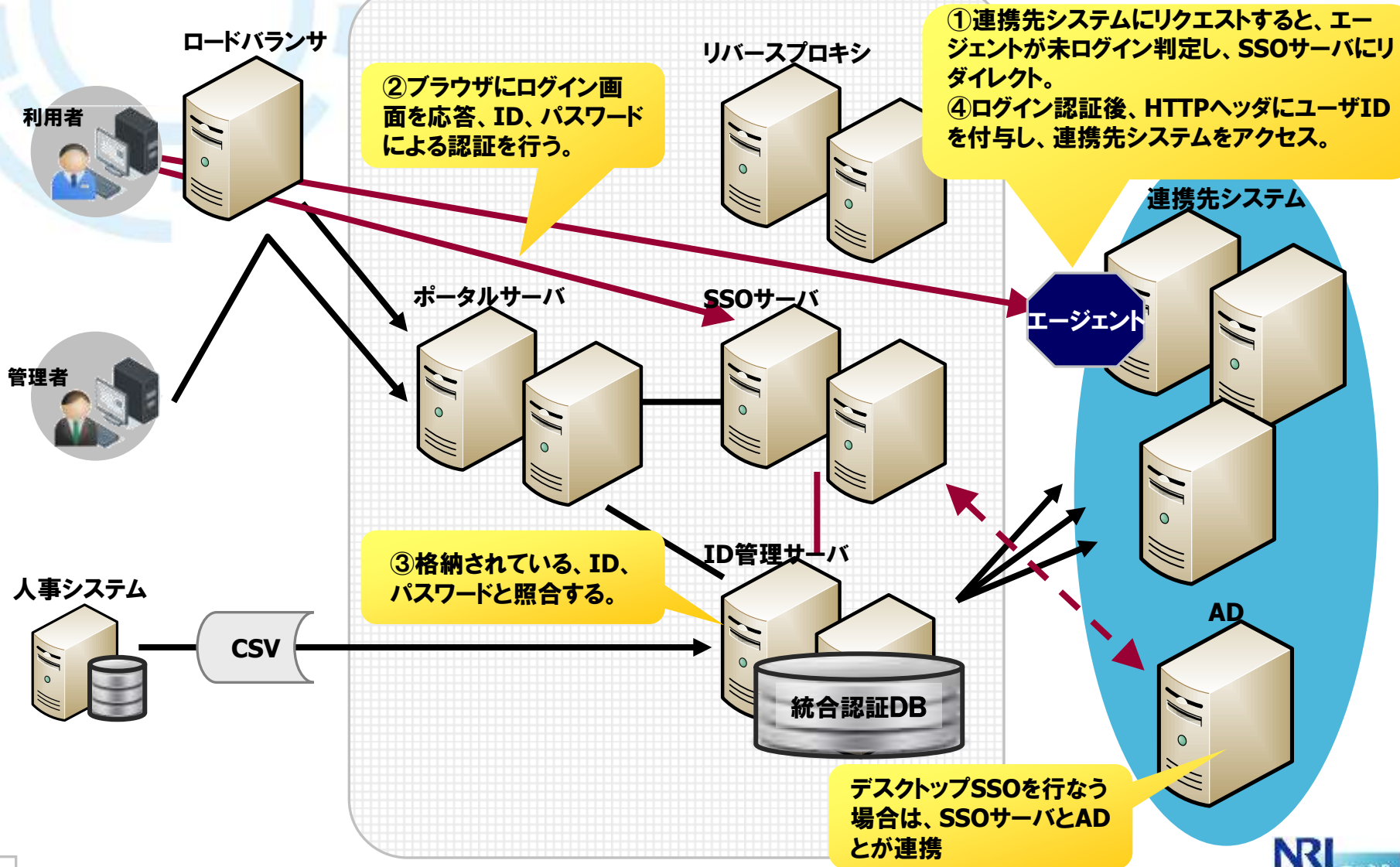
ID管理
(プロビジョニング)
LISM/OpenIDM

システム全体概要(SSO)

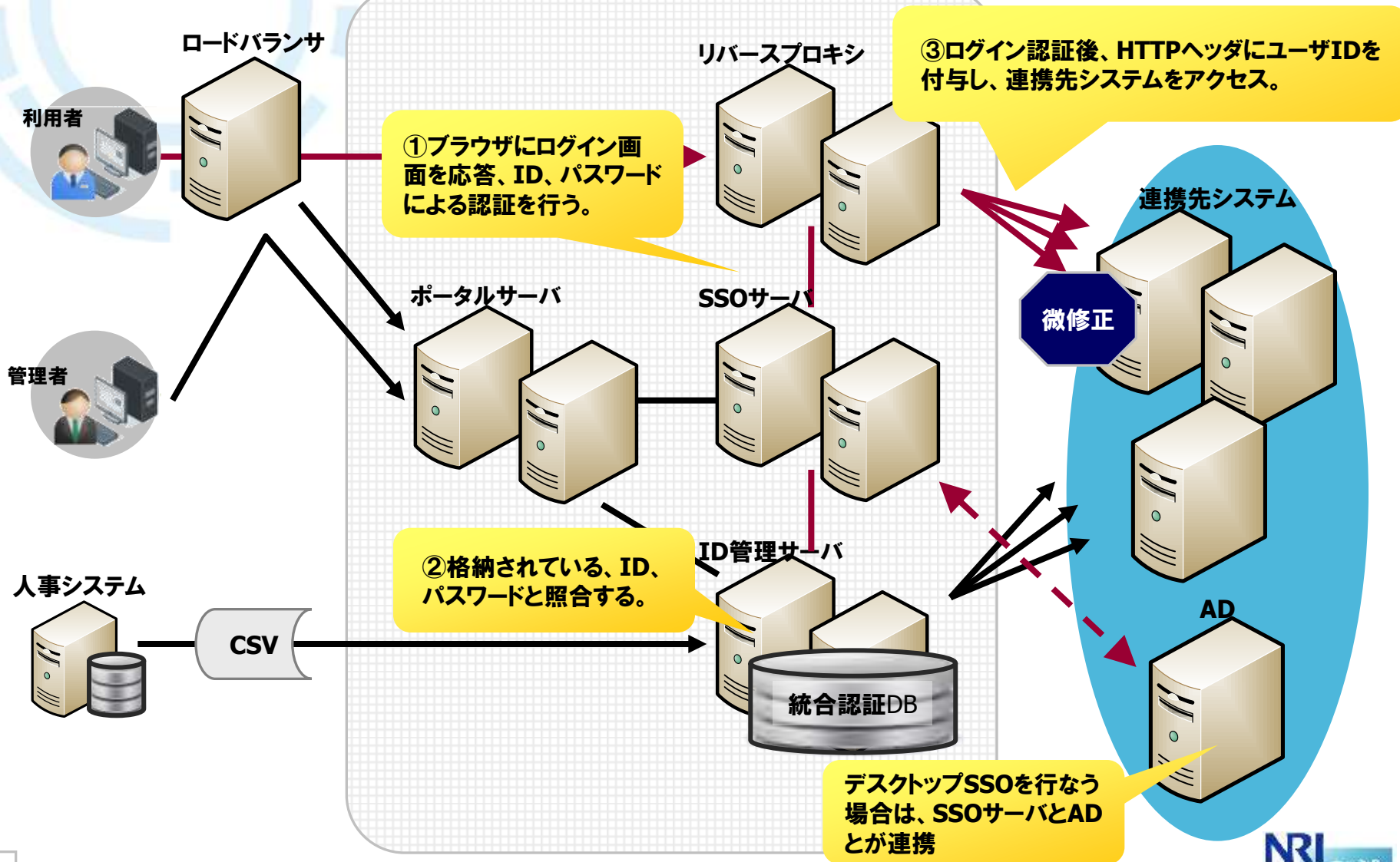
- エージェント型SSO、リバースプロキシ型SSO、代理認証、SAML、デスクトップSSO、C/S型SSO等方式多数



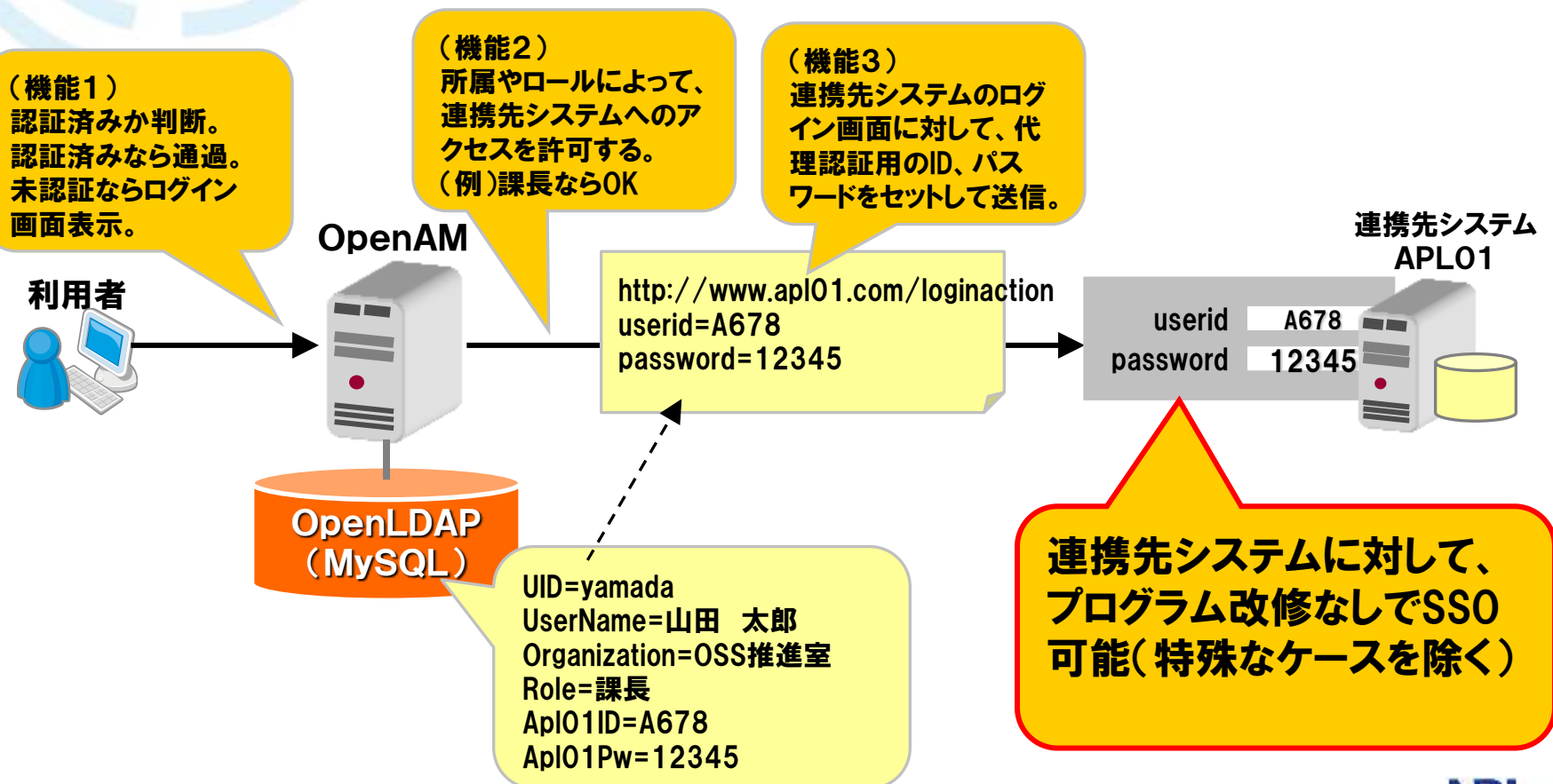
● 連携先システムへエージェントの導入が必要な一方、NW変更は不要



- 連携先システムへエージェントの導入が不要な一方、NW変更が必要

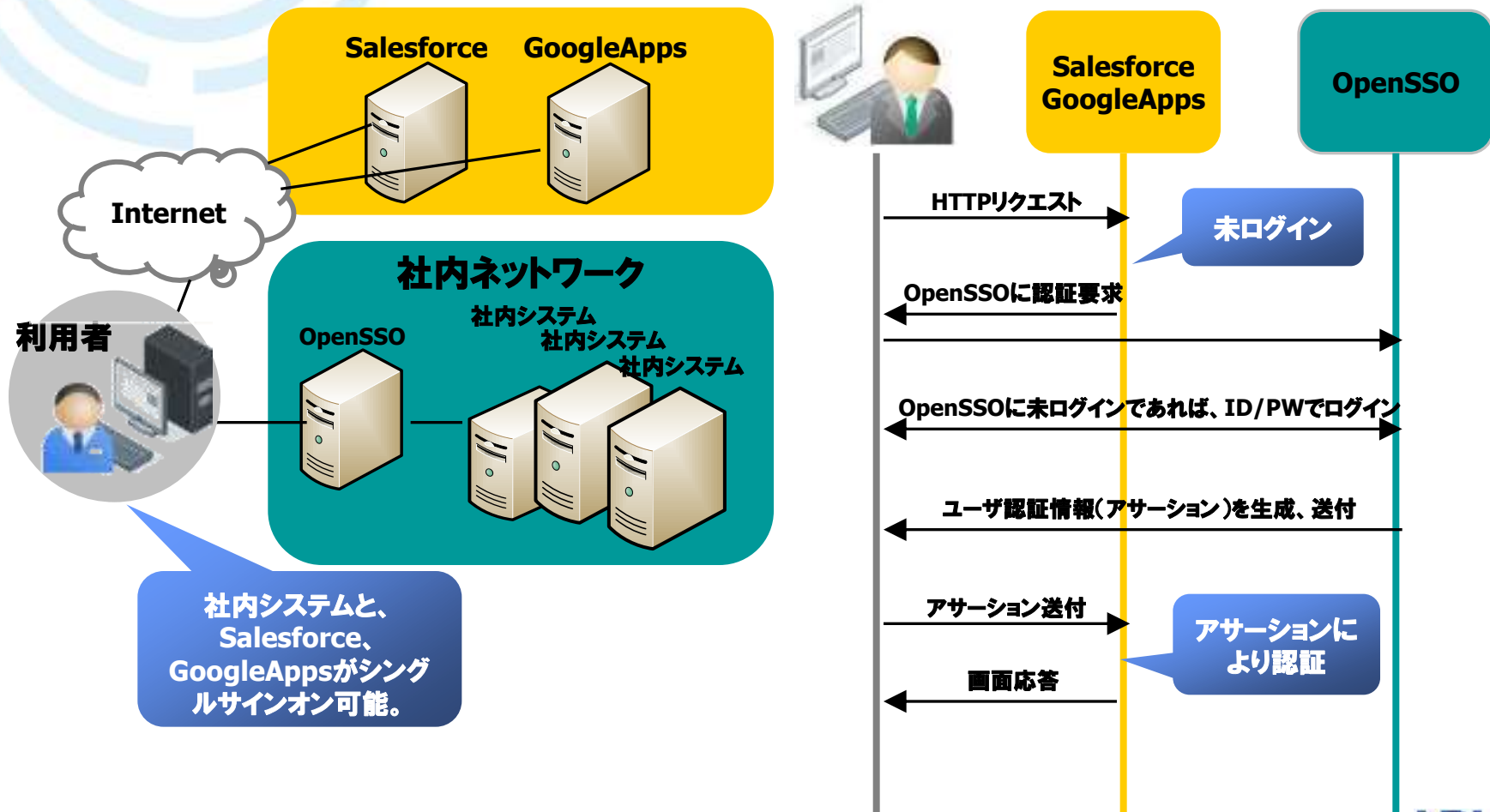


- (機能1)**
認証済みか判断。
認証済みなら通過。
未認証ならログイン
画面表示。

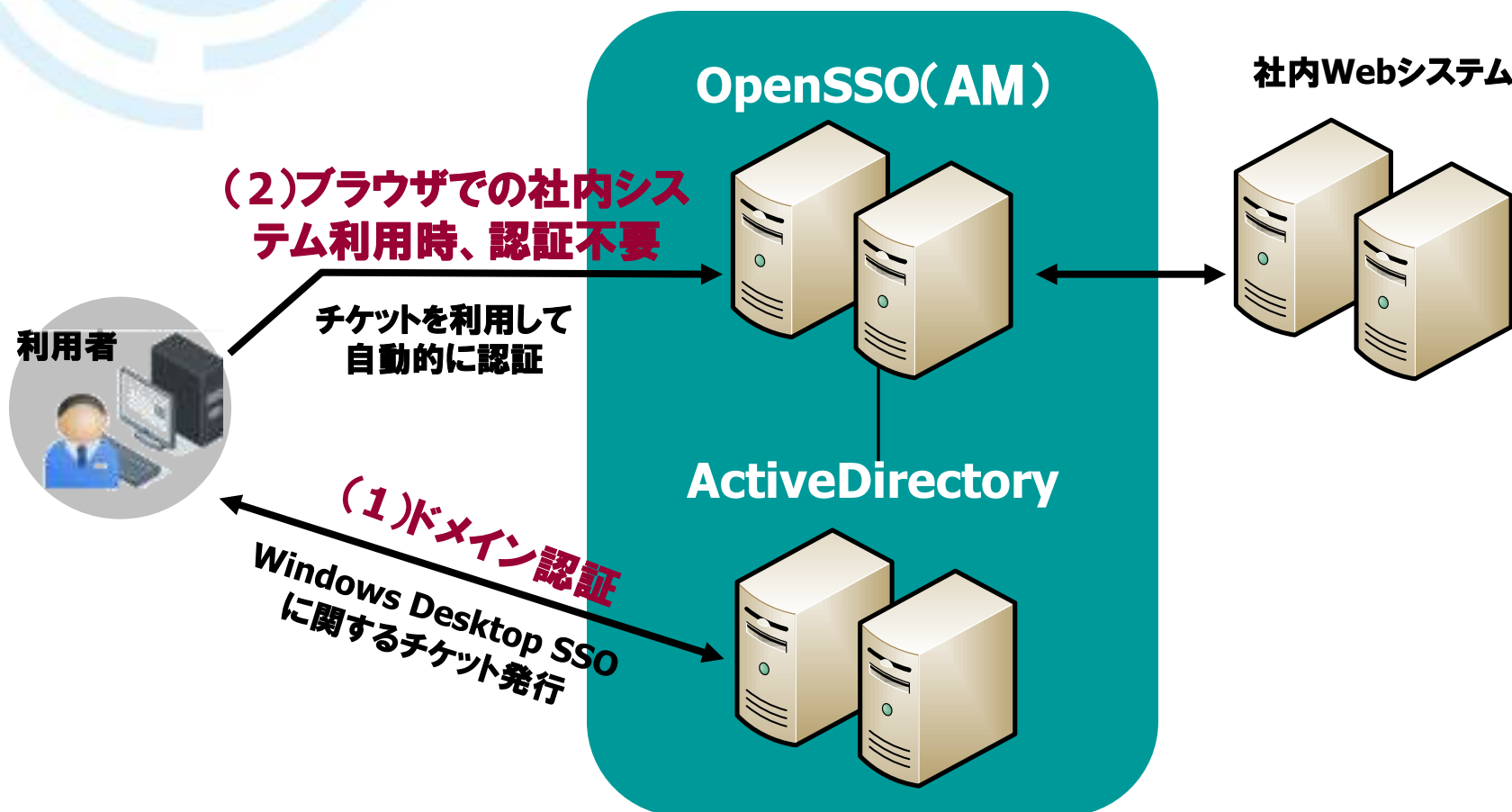


SAML認証によるSaaSとの連携

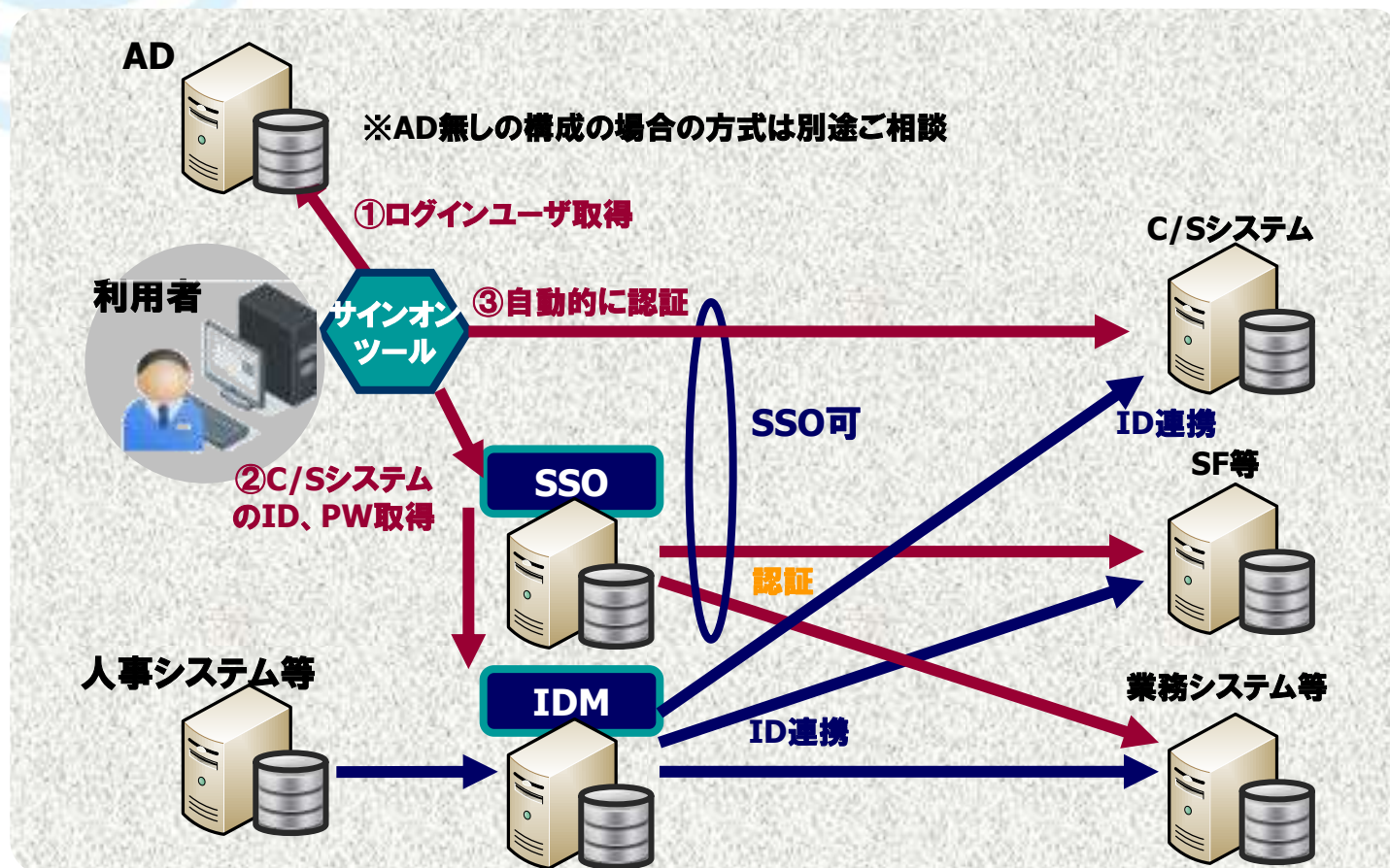
- 標準プロトコルである「SAML」に対応しているSalesforceやGoogleAppsとのSSO
- プログラムの改修が一切不要で設定のみでSSO可能



- Windows(AD)の認証情報を利用し、社内WebシステムにSSOする方式
- PC立ち上げ時(Windowsログイン時)にSSO認証済み状態になる。

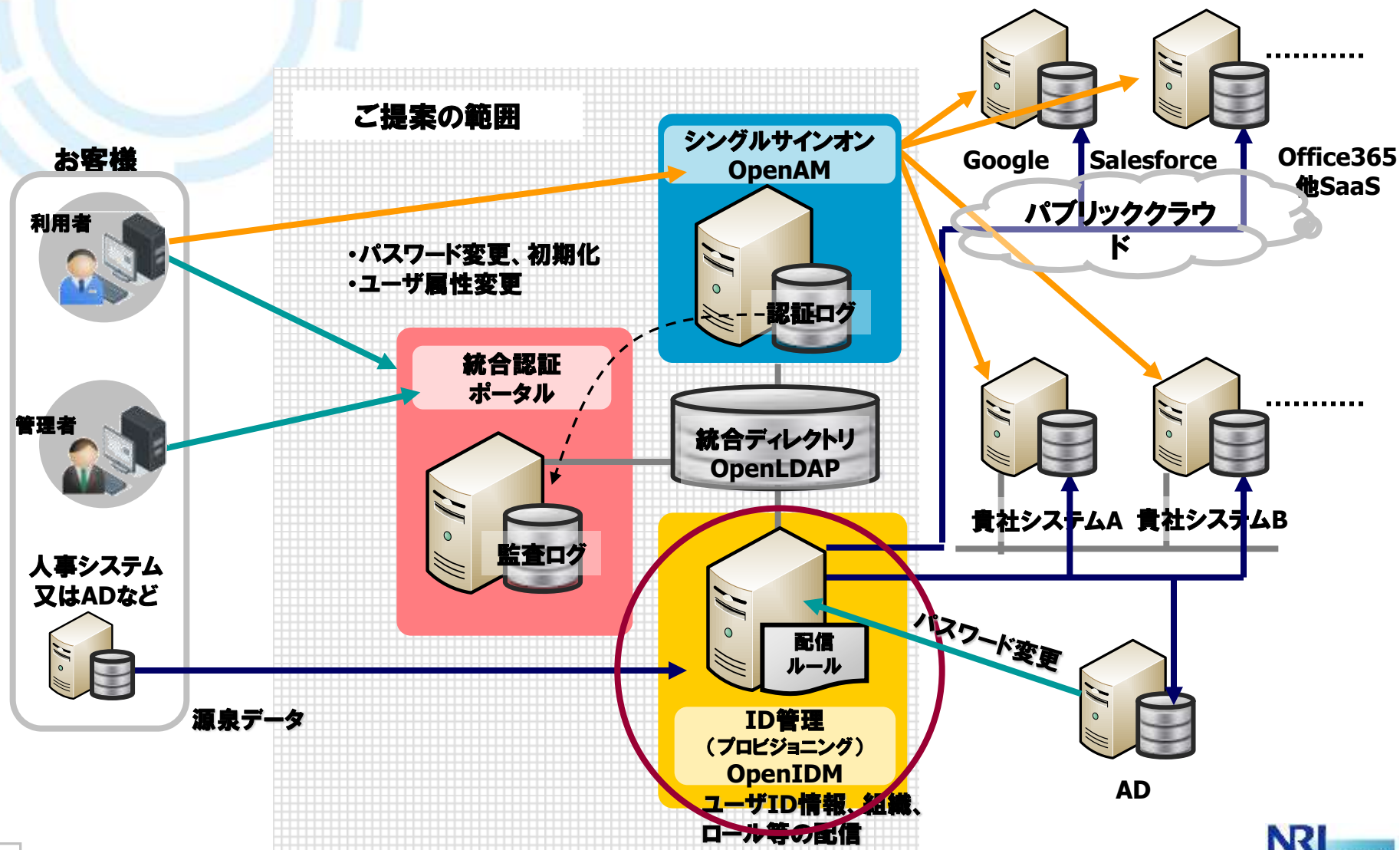


- WEBシステムではないC/S(クライアント/サーバ)システム(Notes等)とのSSO
- PC(端末側)にエージェントを導入し、Windowsアプリケーション等とSSO
- エージェント配布の仕組みが必要

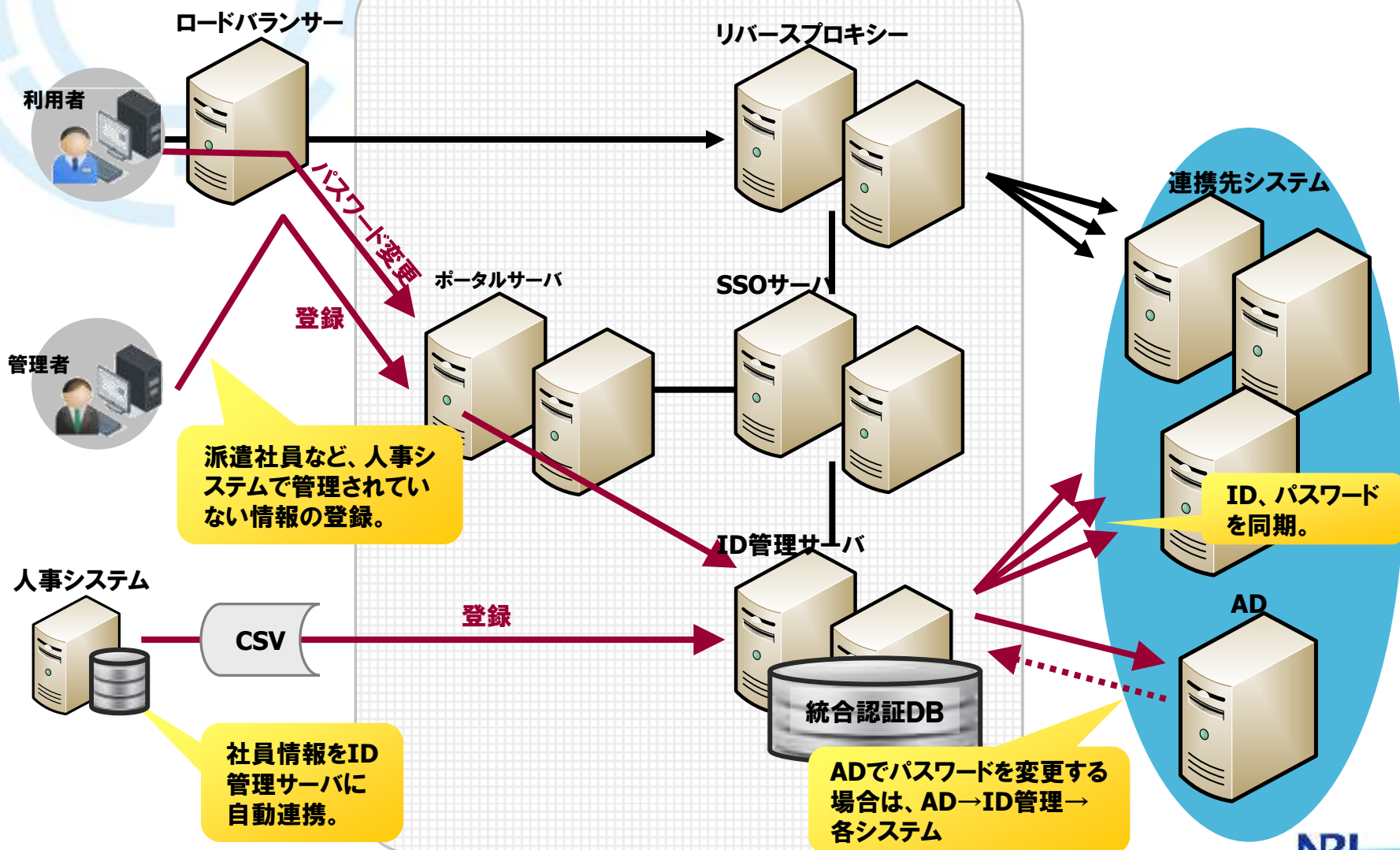


システム全体概要(ID管理)

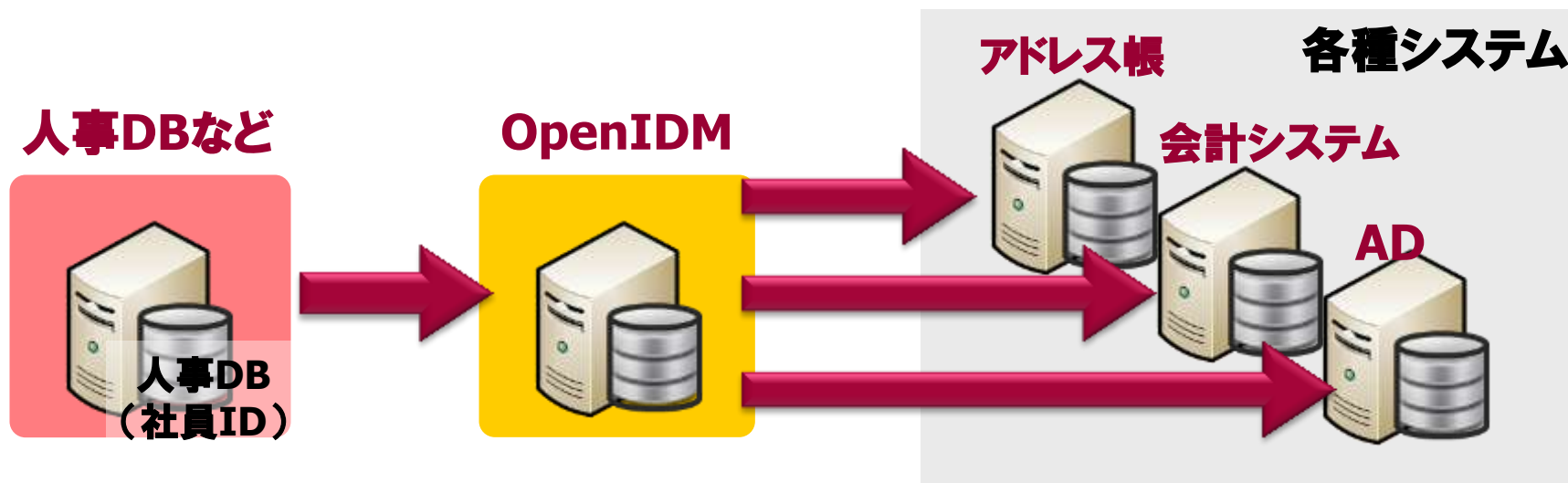
● 「統合ID管理」のIDを他システムに連携する仕組み



- 画面入力によるID管理(一般ユーザ、管理者)、CSVによる一括管理の2つの方法



- オープンソース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



● REST APIの採用

- ▶ OpenIDMに対する操作を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

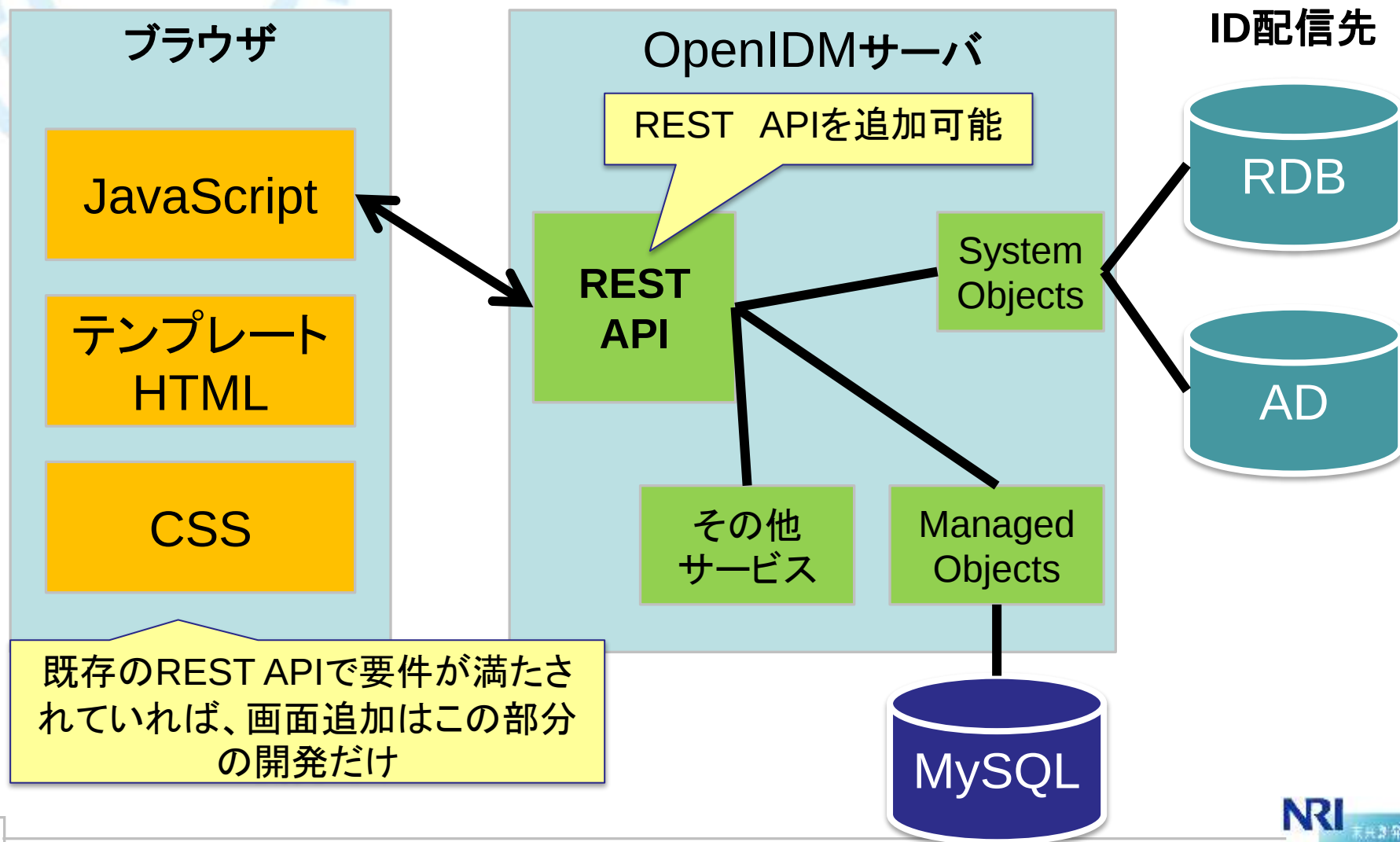
● サーバーサイドスクリプトエンジン

- ▶ Java上で動作するJavaScriptエンジン (Rhino:ライノ) 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

● OpenIDMの全体アーキテクチャ



● 例) ユーザー一覧表示画面の開発

OpenStandia/SSO&IDM x

localhost:8080/idm/index.html#users/

test プロフィール セキュリティデータの変更

users/ の時にユーザー一覧画面を表示する

ダッシュボード

システム管理

ユーザー

メンテナンス

履歴参照

監査ログ参照

組織改正・人事異動管理

組織改正情報

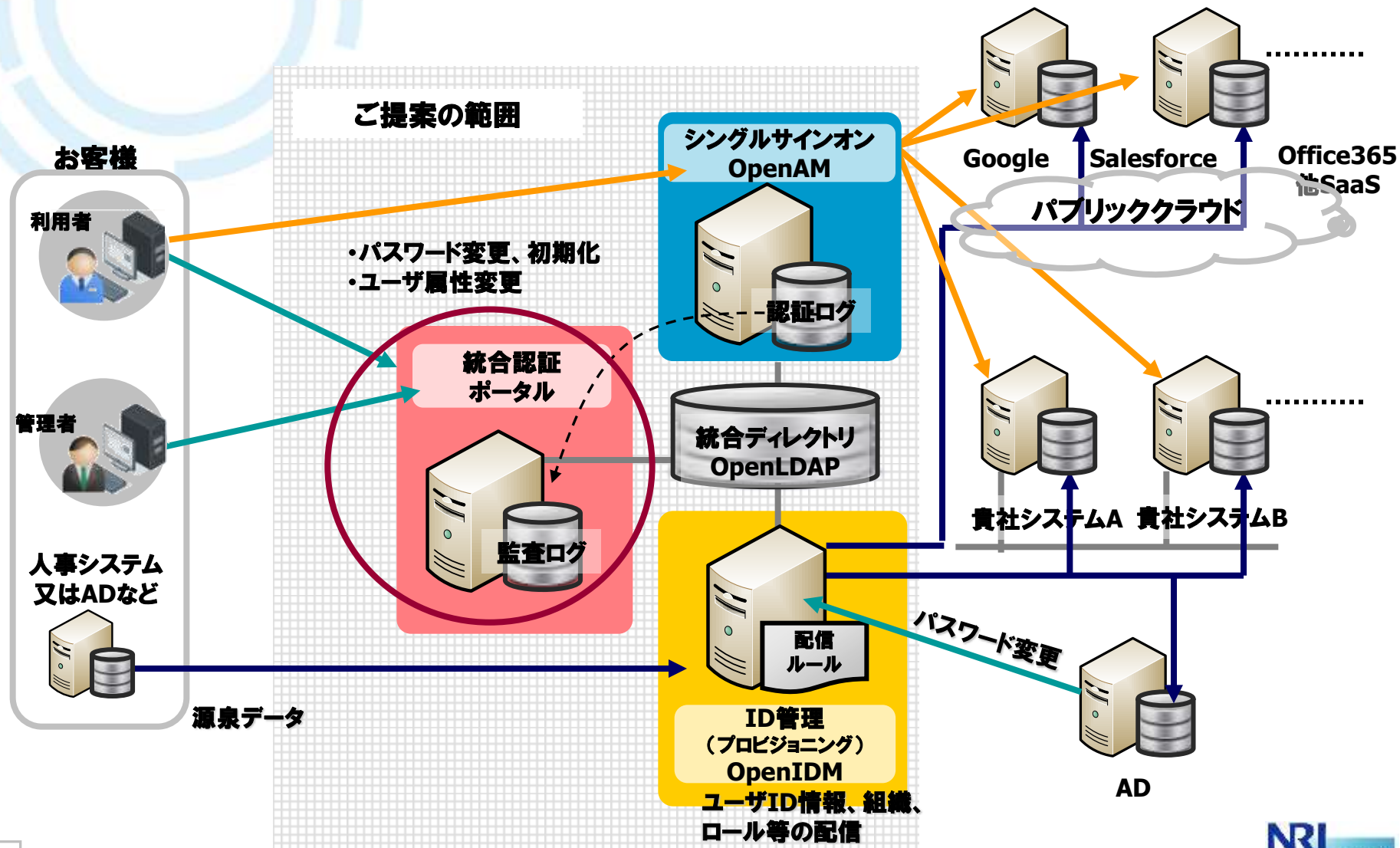
ユーザー一覧

表示件数: 10 ユーザー追加

	ユーザー名	名前	ステータス
☐	test001	野村 太郎	active
☐	test002	野村 花子	active

1 から 2 までを表示中 (全 2 件)

システム全体概要(統合認証ポータル)



ポータル機能、ダイナミックメニュー

The screenshot shows the OpenStandia portal interface. A red circle highlights the top navigation bar, which includes links like HOME, SSO対象サイト1, SSO対象サイト2, SSO対象サイト3, and ワークフロー. A yellow callout points to this bar, stating: **所属する組織や、付与されている権限(ロール)によって、表示されるメニューを変えることができる。**

Another red circle highlights the left sidebar menu, which contains items like パスワード変更, 属性変更, お知らせの登録, お知らせの管理, ユーザ登録申請, ユーザの検索と管理, 組織の検索と管理, and コミュニティの管理. A yellow callout points to this menu, stating: **パスワード変更、ユーザ属性変更などの利用者向けメニュー。及びユーザ登録申請などの管理者向けメニュー。**

A yellow callout points to the 'お知らせ' (Notice) section, which displays a table of notices. The table has columns for 種類 (Type), 名前 (Name), 公開開始日時 (Publication Start Date/Time), and サムネイル (Thumbnail). The first row shows '全体' (All) for the '統合認証ポータルデモサイト公開' (OpenStandia Portal Demo Site Release) on 12/02/21 13:52. Below the table, it says '該当件数: 1 件' (Number of matches: 1 item).

A yellow callout points to the 'ワークフロー追跡' (Workflow Tracking) section, which shows a flow diagram for 'ユーザ登録申請' (User Registration Application). The flow starts with '申請' (Application) by '寺田 雄一' (Terada Yuichi), followed by '部長承認' (Department Head Approval) by '寺田 雄一', and then '情シス承認' (IT/Systems Approval) for 'デモ 001'. A yellow callout points to this section, stating: **申請・承認ワークフロー**.

At the bottom, a yellow callout points to a calendar view for April 2012, showing a grid of dates and times for various events like '朝会' (Morning Meeting) and '定例会議' (Regular Meeting).

➤ 従来の統合認証に関する商用製品(SSO、IDM)への課題とオープンソースの優位性

商用製品

属性追加時に追加開発が必要

属性や連携先追加の際に、追加開発やカスタマイズが発生し、想定外のコストが発生する場合がある。

ライセンス費用が高額

ビジネスの発展、会社規模の拡大によりライセンス費用がリニアに高額になっていく。

サポート品質に満足していない

ほとんどのID管理、SSO製品は、国外産であるため、開発SEが国内におらず、仕様に不明な点も多く、不具合時の対応に時間がかかる。又は対応できないケースがある。

スクリプト定義等で簡単に対応

OpenStandiaでは、多くの場合スクリプト定義等で簡単に対応可能。

保守費が低コスト

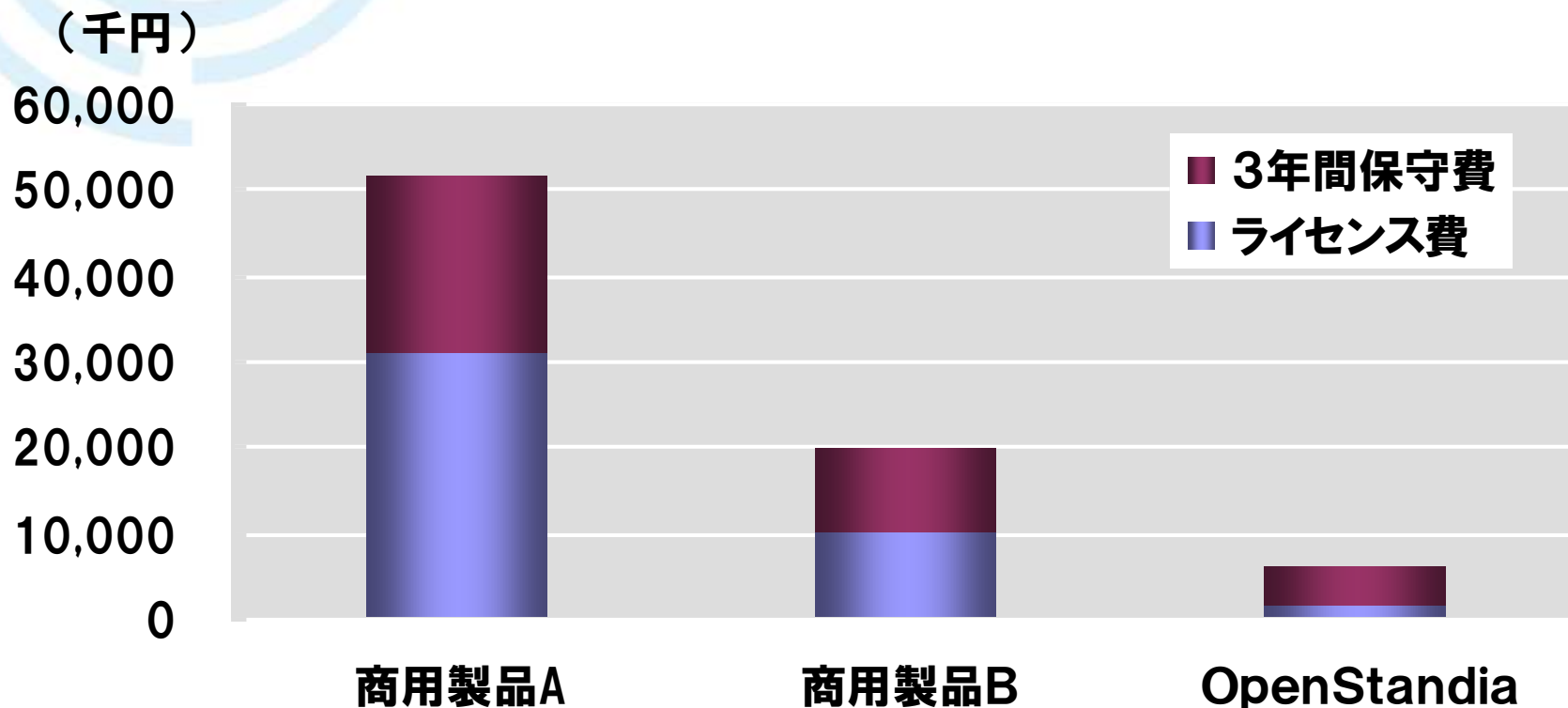
サポートを委託する場合、基本的にサーバ単位でのコストとなるため、保守コストが抑えられる。

商用製品以上のサポート品質

OpenStandiaでは、野村総合研究所が全てのソースコードを管理。万が一のトラブル時も全て弊社エンジニアが迅速に対応。

(ご参考)コスト比較例

■ 統合ID管理 3年間コスト比較例

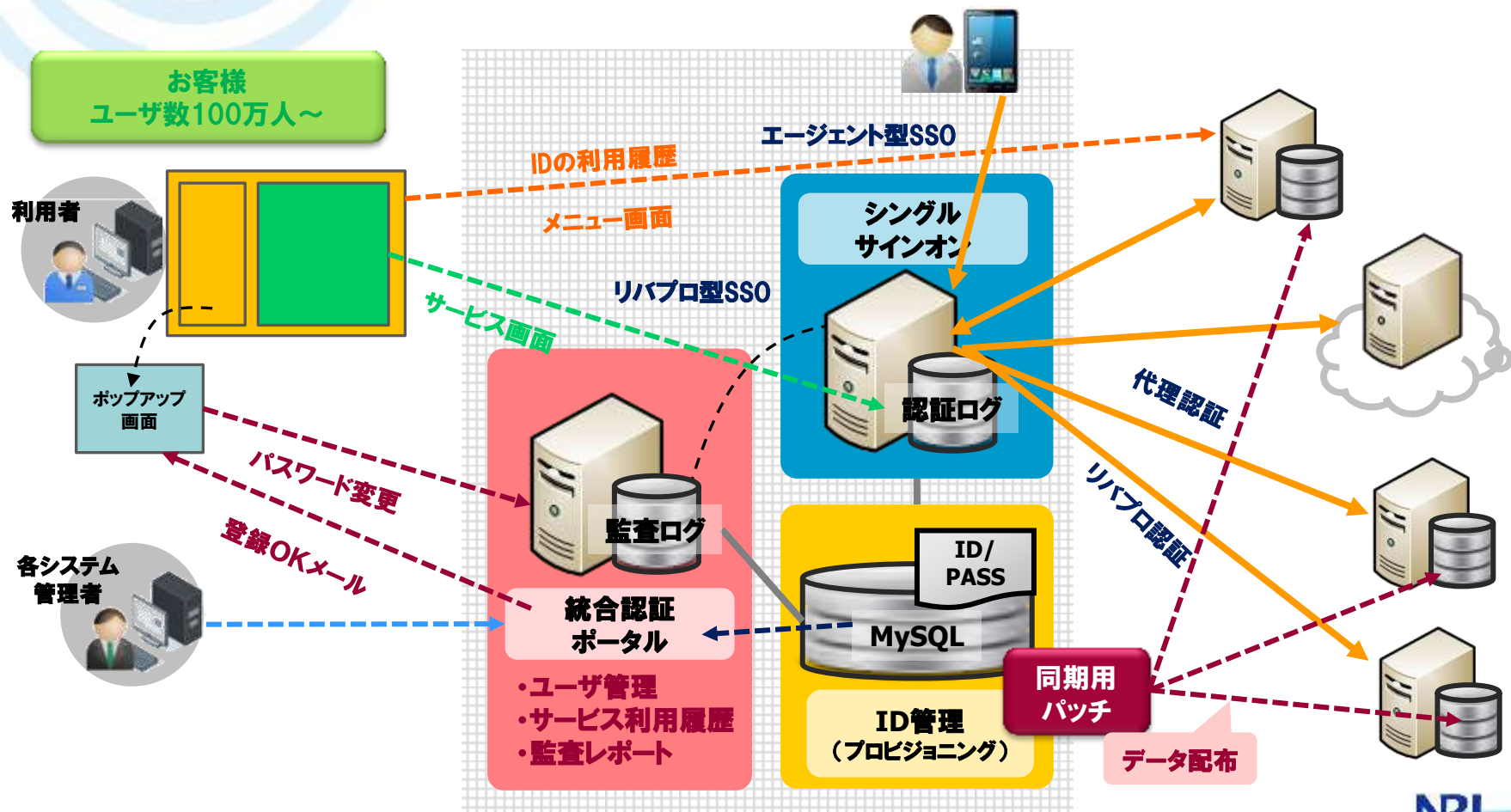


※1,000ユーザを想定

● 事例紹介

(事例)資格試験サイト様 数百万会員のシングルサインオン

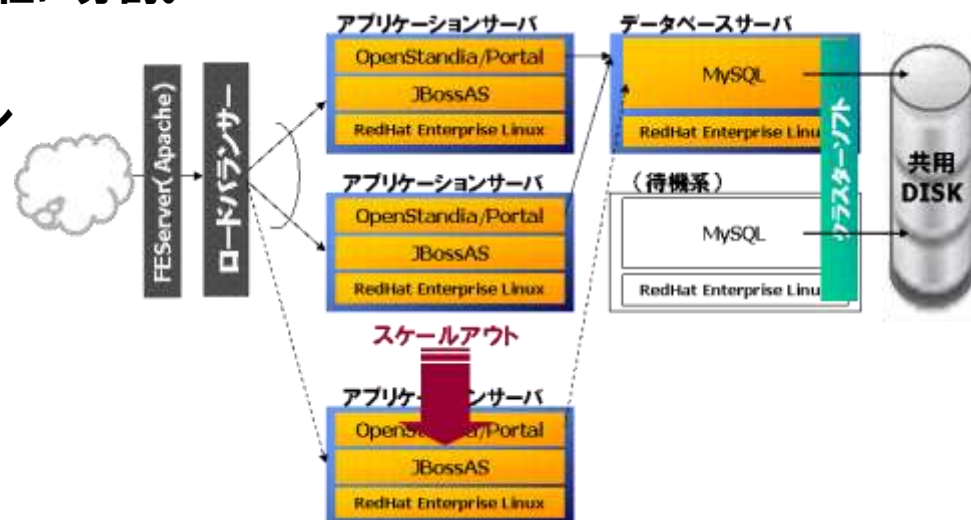
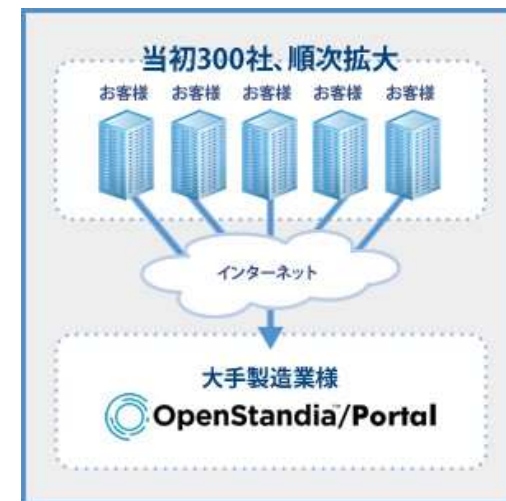
- 会員数、数百万人
＝ 商用製品の場合、億単位のライセンス費用
- 試験合否発表のサイトと教材販売のサイト等を連携



(事例)大手製造業様 カスタマーポータル

大手製造業様 カスタマーポータル(SaaS基盤)

- 大手製造業様の顧客である、中小規模の事業所向けに、社内ポータルの機能を提供。
- スケジュール、施設予約、文書管理、掲示板などの機能を提供。
- 当初は300社、1万人程度に提供し、順次拡大予定。90万人を想定。
- OpenStandia/Portalの「マルチテナント機能」を利用して、ポータルシステムを論理的に300社に分割。
- 既存の統合認証基盤(OpenAM利用)と連携し、他システムとのシングルサインオンを実現。
- 利用人数が多く、商用製品では価格的に成り立たないため、OSSでの構築をご希望。
- 柔軟なカスタマイズが可能な点、お客様が自ら機能拡張ができる点などを評価。



人事異動時のID管理業務を効率化

● 現行システム概要

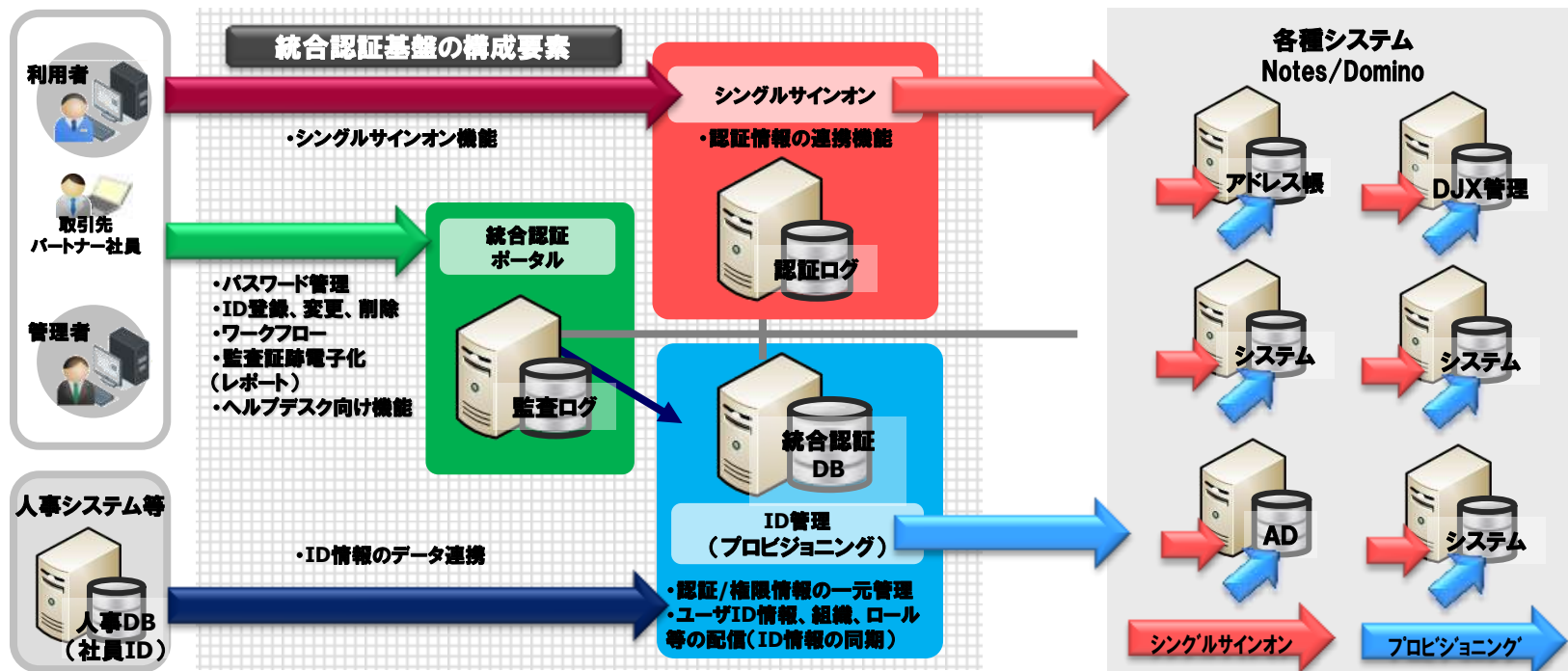
- ▶ 人事、会計など、基幹業務システムと、AD、NotesなどのOA系・情報共有系システム。GoogleAppsの利用や、スマートフォンからの情報照会を新たに開始。

● 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

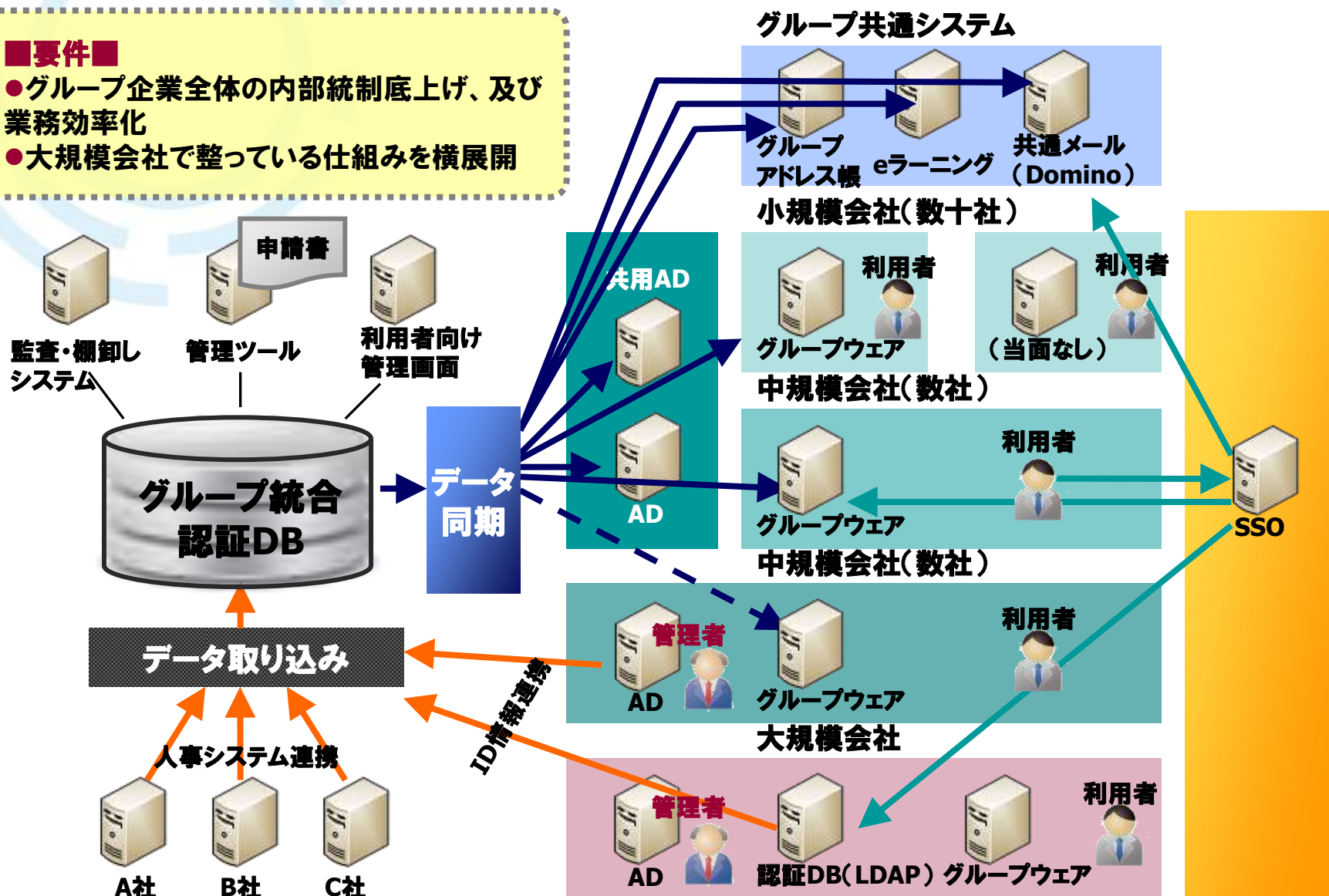
- ▶ ばらばらだったIDを統合管理し、**人事システムとも連携。異動業務を自動化し、効率化。**従来紙で行っていた各事業部との人事異動に関するやりとりも、システム化、ワークフロー化。



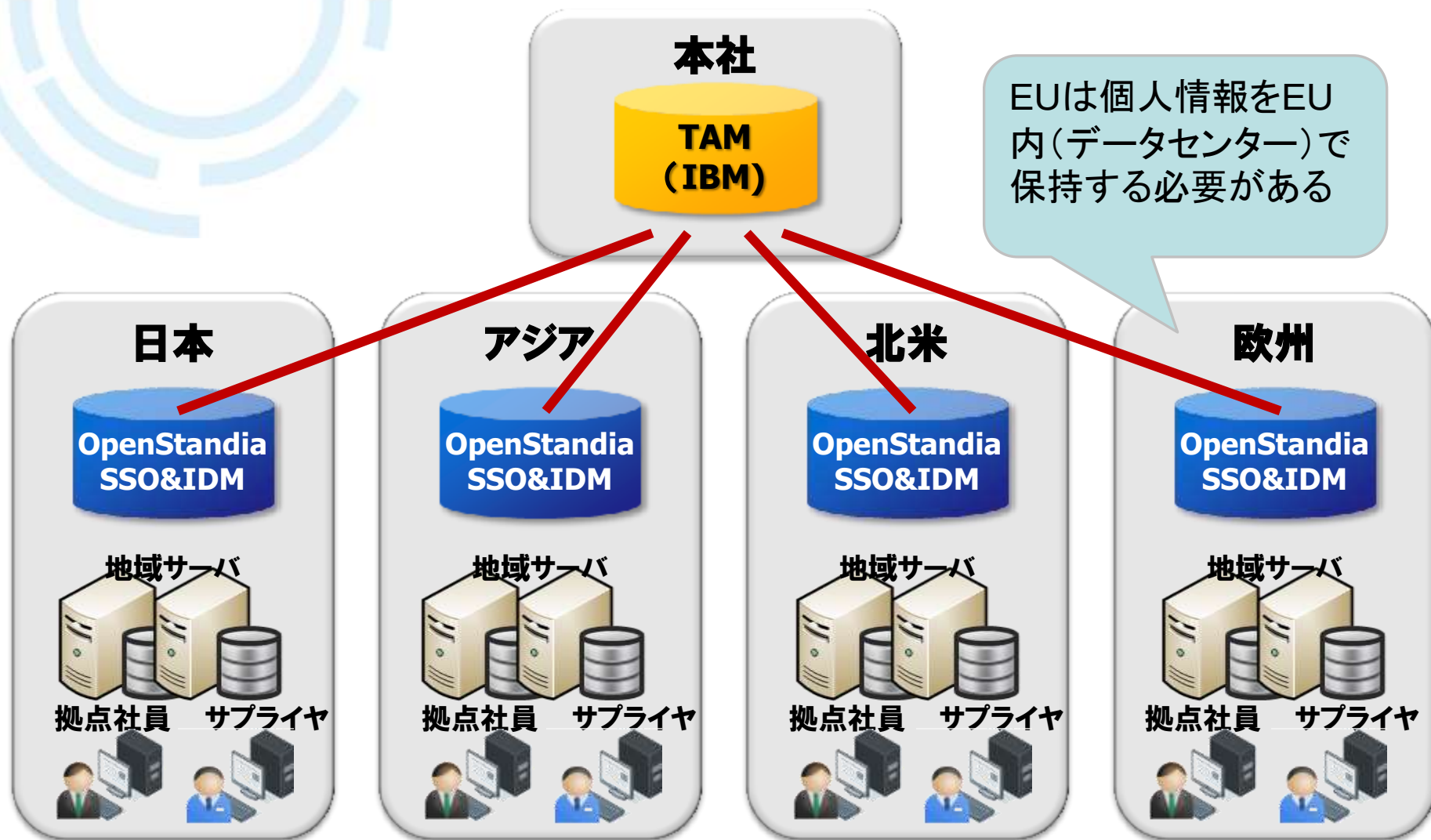
(事例)大手グループ企業(ホールディングス) 統合認証基盤

■要件■

- グループ企業全体の内部統制底上げ、及び業務効率化
- 大規模会社で整っている仕組みを横展開



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



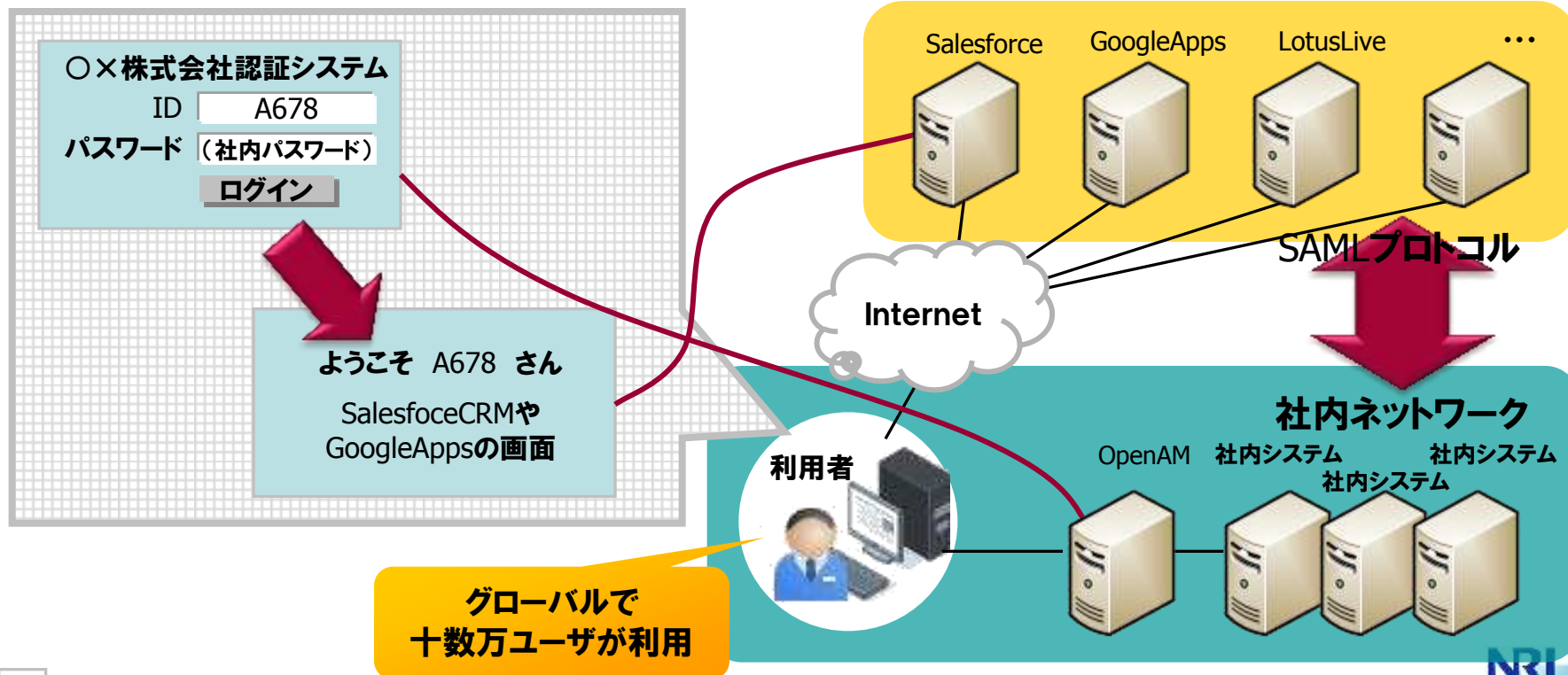
GoogleAppsやSalesforceCRMとのシングルサインオン

■要件■

- 社内システムのID、PWを使って、SalesforceCRM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

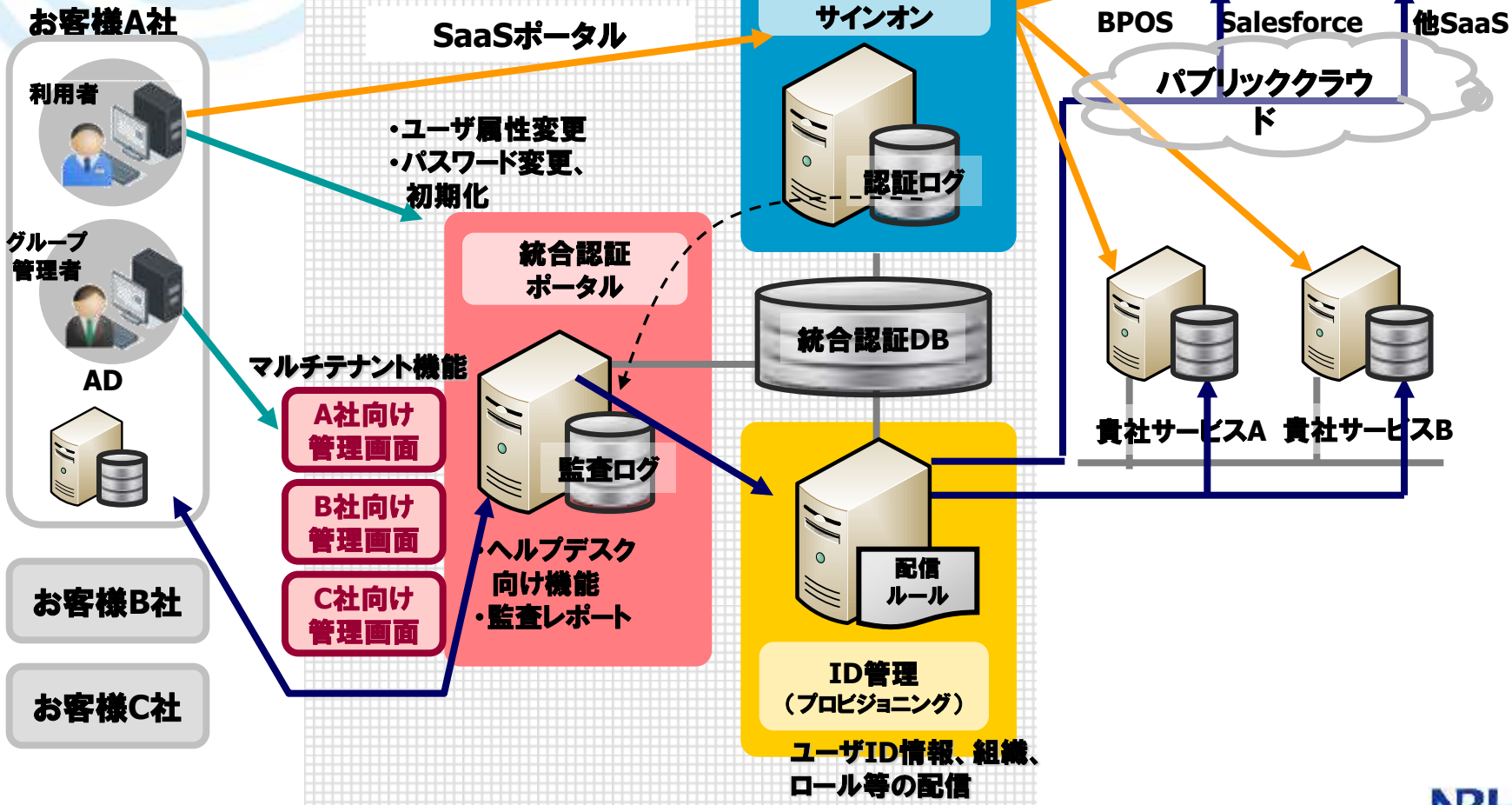
- 業界標準の「SAML」プロトコルを用いて、社内システムとSalesforceCRM、GoogleAppsとを接続(シングルサインオン)。
- 社内LDAPのID/Pwを使って、SalesforceCRM、GoogleAppsにログイン可能に。



(事例)電力系ISP様 SaaSプラットフォーム構築

■要件■

- 自社サービス(パッケージ)、パブリッククラウドを統合するID管理、認証基盤
- 各サービスへの入り口としてのポータル画面
- ユーザ企業が自社のIDを追加できる管理画面



モバイルPC、スマートフォン、タブレットからの認証

- モバイルPC、スマートフォン、タブレットからの、セキュアなアクセスを実現。

モバイルPCからのアクセス



スマホ・タブレットからのアクセス



モバイルPCからのアクセス



スマホ・タブレットからのアクセス



VPN

VPN

他社VPN
アプライアンス



F5 Networks
Juniper Networksなど

OpenAM連携

VPNアプライアンスと、
OpenAMとの連携機能

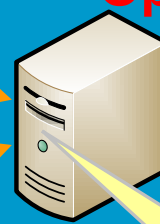
シングルサインオン

OpenAM



リバースプロキシ

Apache
OpenAM



インター
ネット

PKI認証

PKIは使用しないケー
スもあり

- ・ワンタイムパスワード
- ・マトリックス認証
- ・ネットワーク(IPアドレ
ス)制限
- ・ブラウザ制限
- ・時刻制限
- ・リスクベース認証

VPN
方式

PKI
方式

会員サイト様 OSSによるシングルサインオン

- 会員数3万名の、複数のサイトをOSSでシングルサインオン。
- 認証サーバとしては、ActiveDirectoryを利用。

外資系企業 内部統制の強化

- 米国上場企業の国内法人。
- SOX法監査での指摘事項について改善するため、ID管理を導入。

大手法人様 人事システムとSalesforceCRMとをシングルサインオン

- 数万名の大手法人。人事システムとSalesforceCRMとをシングルサインオン。
- ID管理として、オープンソースのLISMを利用。

学校法人様 学内システムをシングルサインオン

- 学生、教職員あわせてユーザ数約3,000名。
- 複数の学内システムをリバースプロキシ型でシングルサインオン。

パッケージベンダー様 自社パッケージのSAML対応

- 業界標準の認証プロトコルであるSAMLに、自社パッケージを対応。

大手サービス業様 複数サイトのシングルサインオン

- 既存のサイトをシングルサインオン。今後、ID管理も統合予定。
- NRIが、クラウドサービスとして認証基盤を提供。

会員サービス様 サービス提供サイトとイントラネットとのシングルサインオン

- 提供するサービス提供サイトと、顧客イントラネットサイトとのシングルサインオン
- 携帯電話からのアクセスにも対応

大手建材メーカー様 社外からのシステム利用時のシングルサインオン、ID管理

- サプライヤーを含めた、社外からのシステム利用時のシングルサインオン、ID管理を、クラウド上に構築。

● よくお話をいただく、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、大幅なユーザー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、グローバル化)

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。

- 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！



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



osscc@nri.co.jp



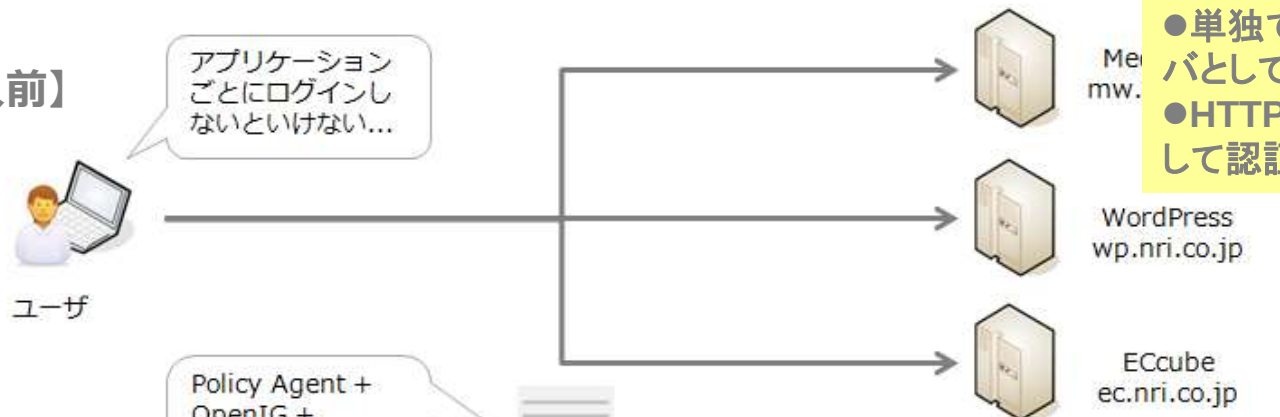
<http://openstandia.jp/>

●ご参考

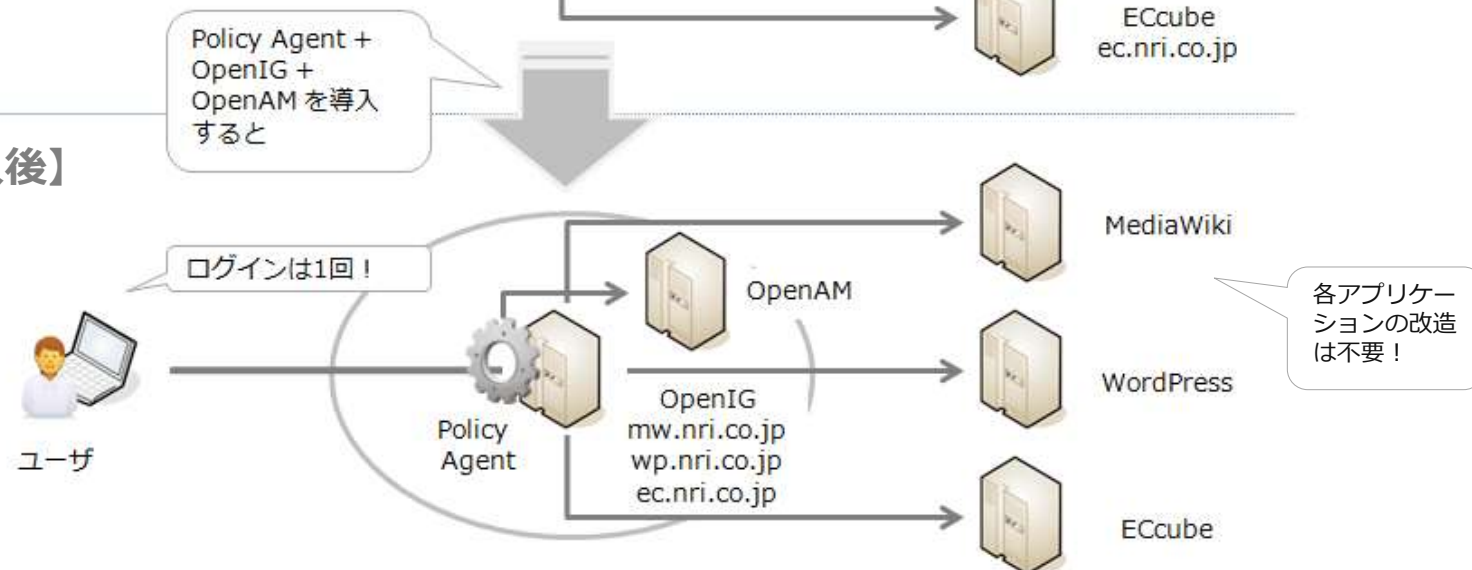
● OpenIG (Open Identity Gateway)

▶ 代理認証を実現するソフトウェア

【導入前】



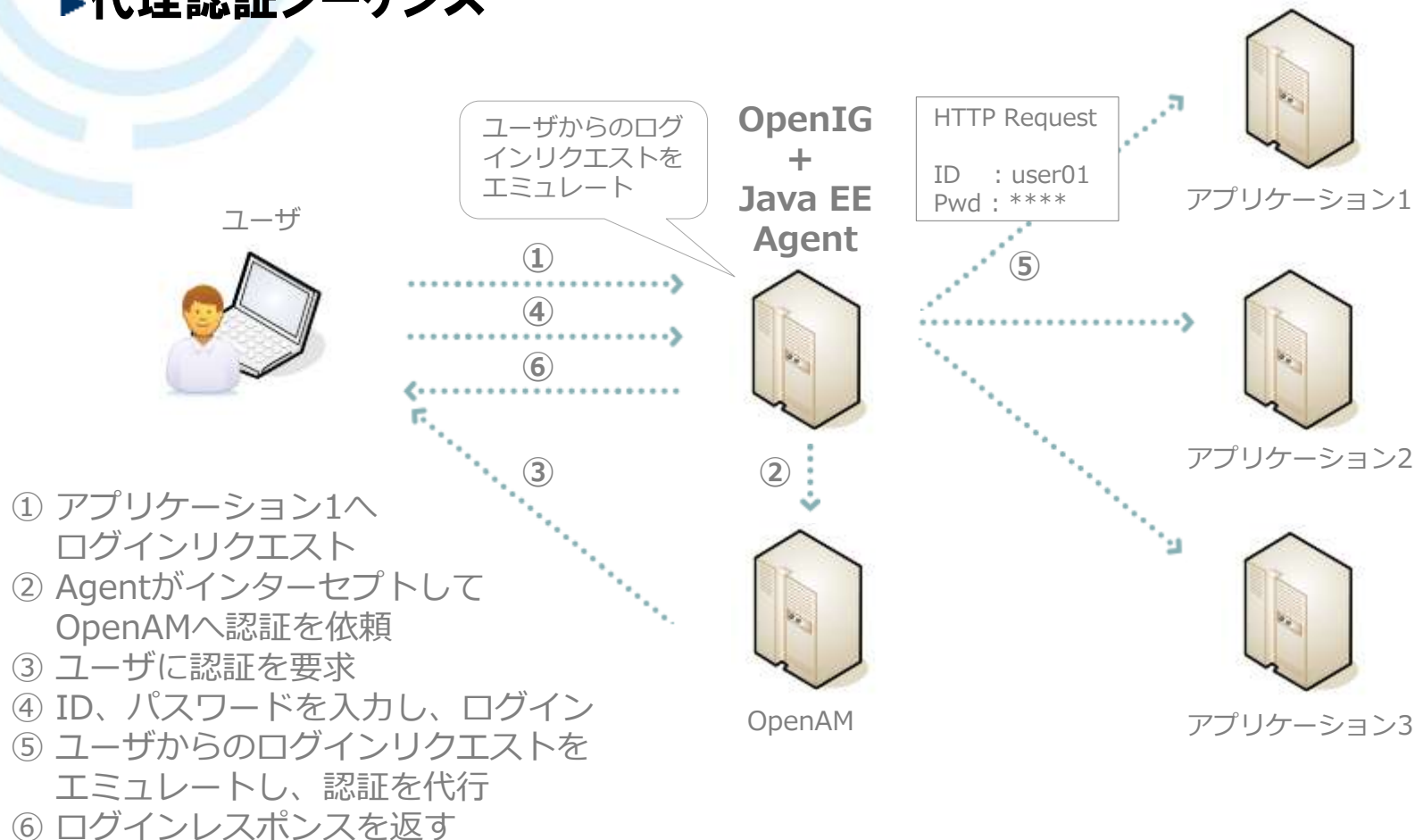
【導入後】



- 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

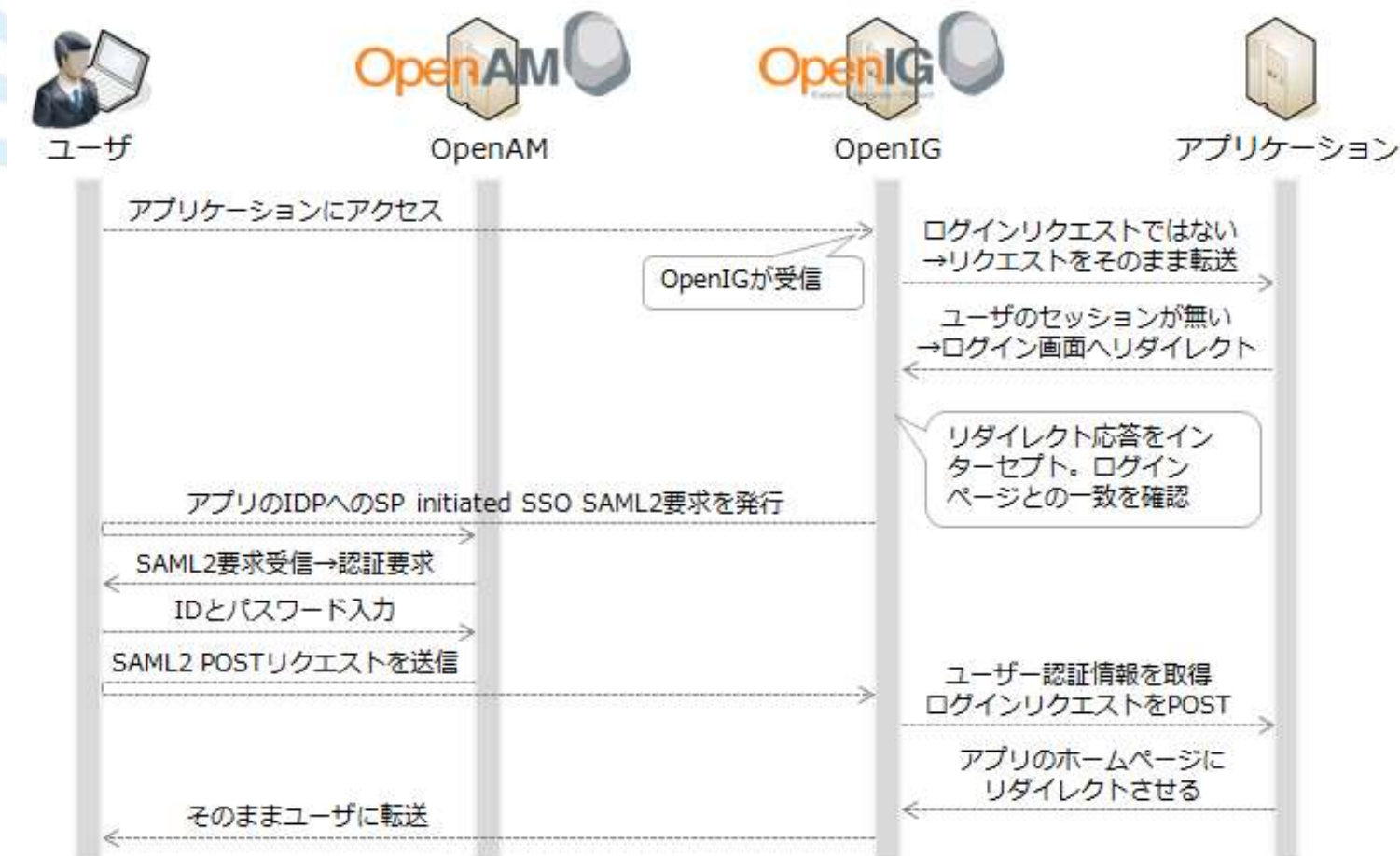
● OpenIG (Open Identity Gateway)

▶ 代理認証シーケンス

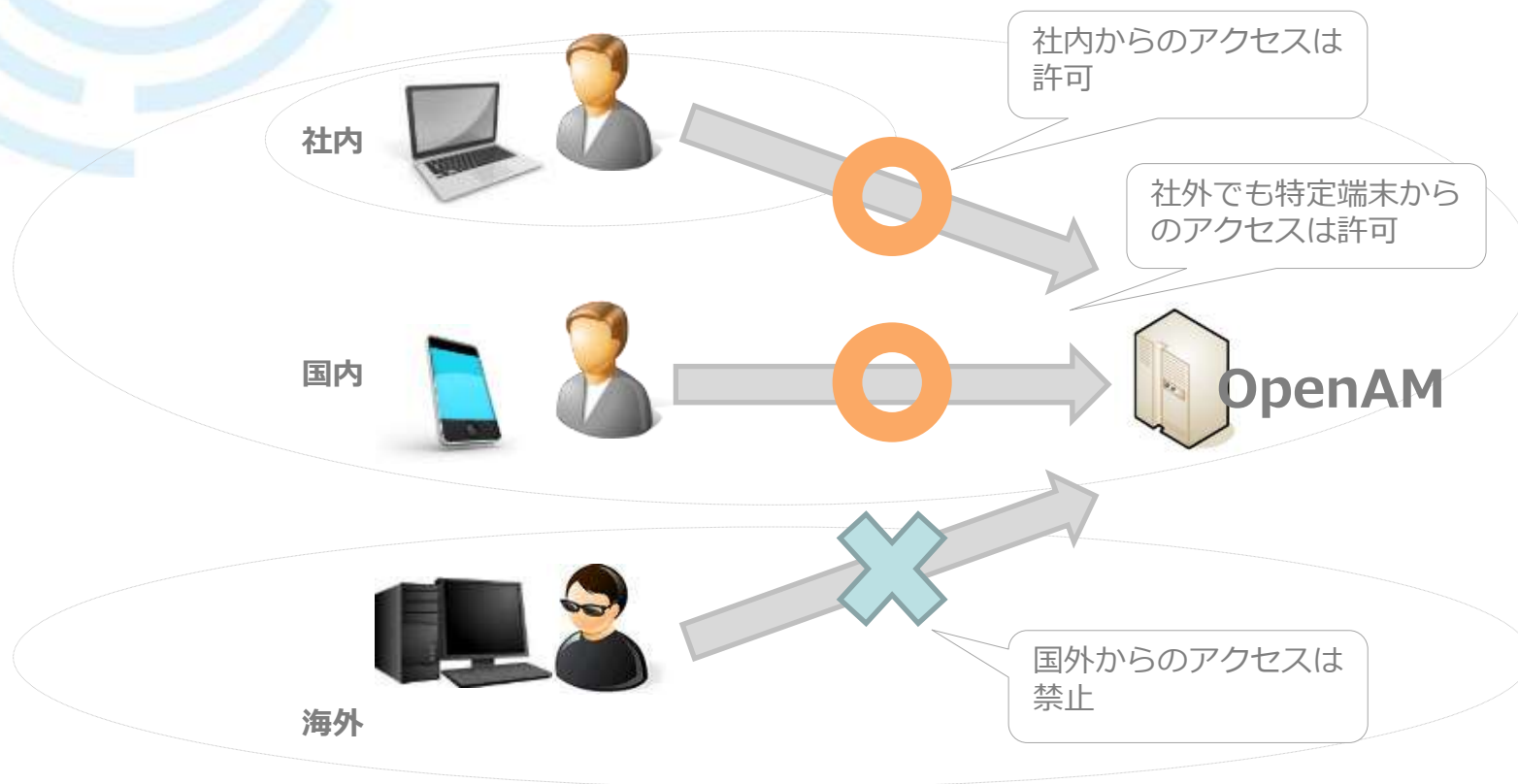


● OpenIG (Open Identity Gateway)

▶ SAML2.0 フェデレーションゲートウェイ機能



●不正アクセスのリスクに配慮した認証方式



● チェック機能

- ▶ 認証失敗チェック
- ▶ IPレンジ・履歴チェック
- ▶ Cookie値チェック
- ▶ 最終ログインからの経過時間チェック
- ▶ プロファイルのリスク属性チェック
- ▶ 位置情報国コードチェック
- ▶ リクエストヘッダーチェック

● 各チェックの点数の合計がしきい値に達すると・・・

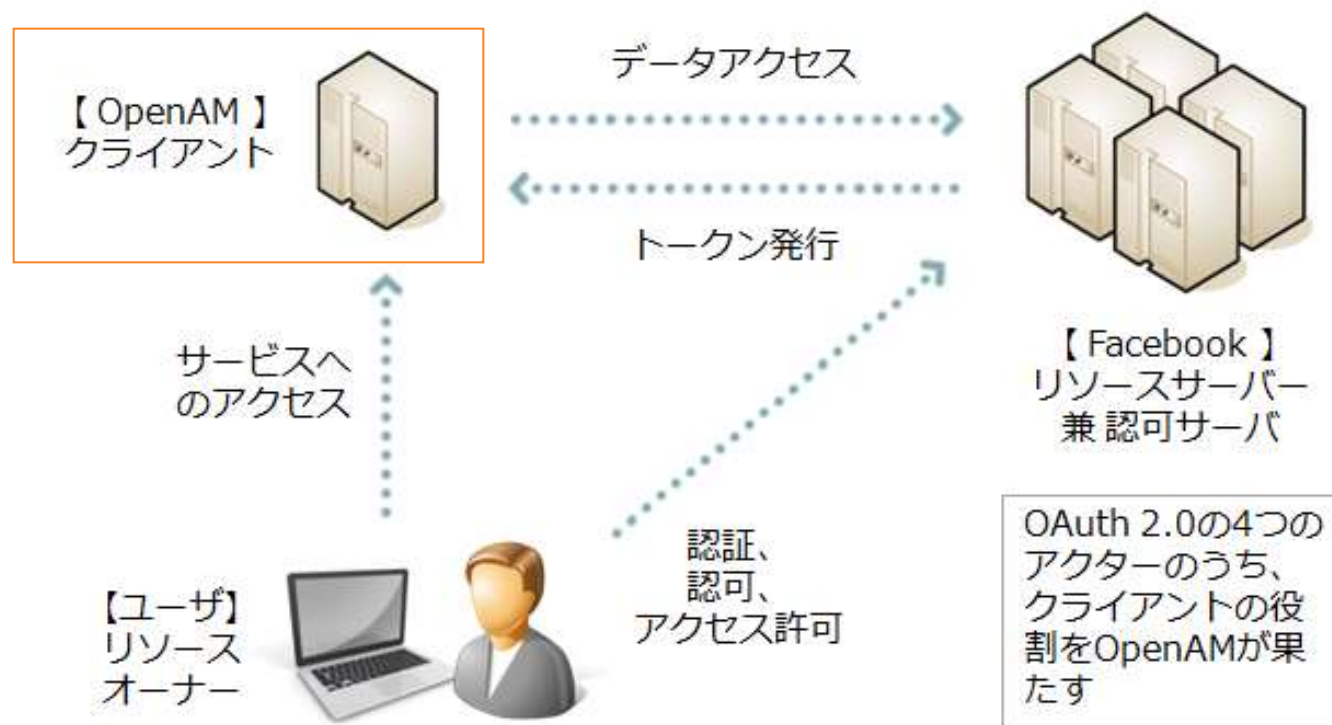
- | | |
|-----------------------|---------|
| 1. IPレンジチェック (3点) | NG → 3点 |
| 2. Cookie値チェック (1点) | OK → 0点 |
| 3. 位置情報国コードチェック (4点) | OK → 0点 |
| 4. リクエストヘッダーチェック (2点) | NG → 2点 |

しきい値 5点

合計 5点

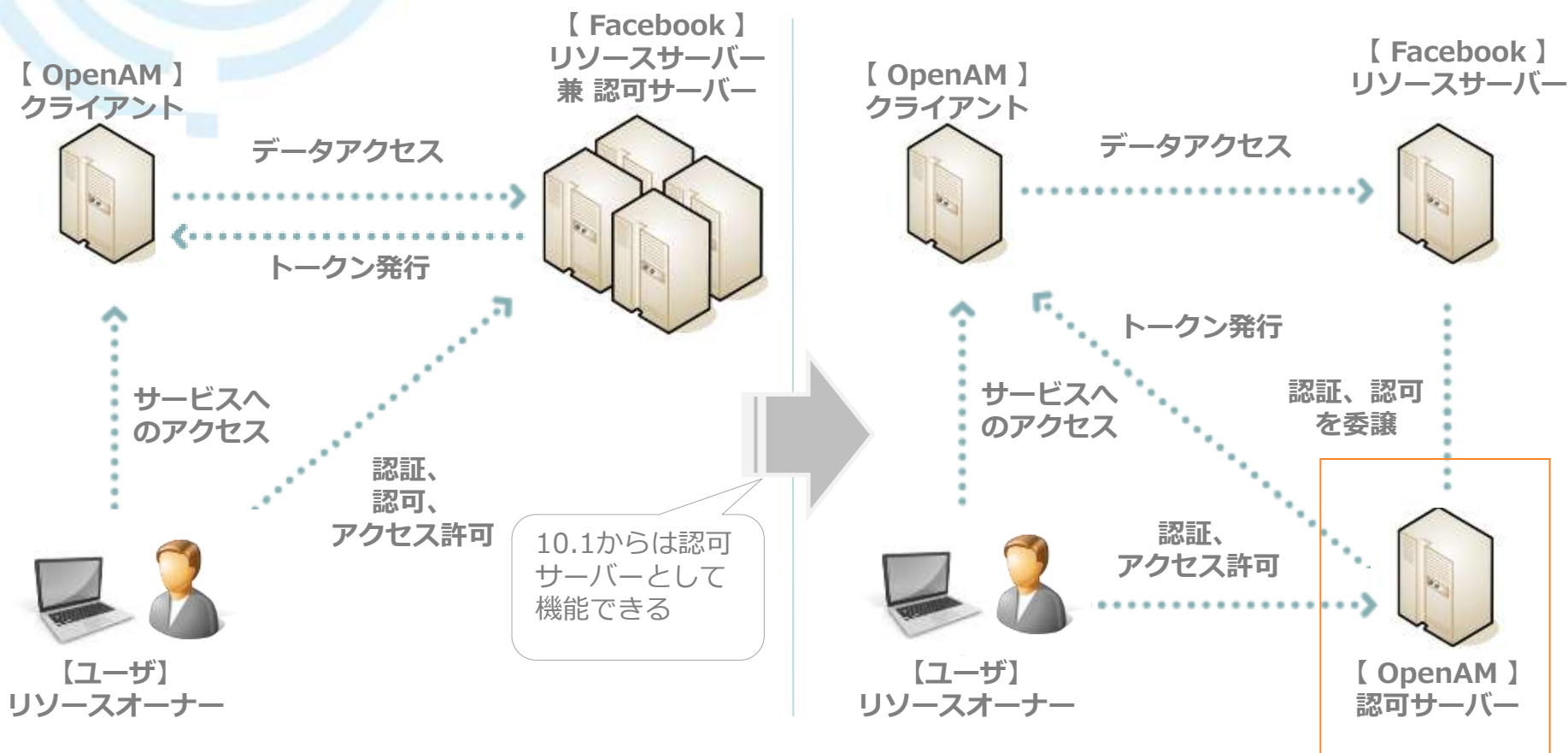
→ **不正なアクセス！認証エラー**

● OAuth2.0クライアント認証



● OAuth2.0クライアント認証

▶ OpenAMが本来行うべき認証・認可機能は10.1～



#	機能	説明	OpenAM	Open LDAP	NRI独自拡張	LISM
1	統合認証ポータル(利用者向け機能)					
2	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。			○	
3	ダイナミックメニュー機能	所属している組織や、付与されている権限(ロール)によって、メニューの表示/非表示を制御する。			○	
4	ユーザー属性変更機能	利用者自身がユーザー属性を変更する。			○	
5	パスワード変更機能	利用者自身がパスワードを変更する。			○	
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	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。			○	
8	統合認証ポータル(ヘルプデスク向け機能)					
9	ユーザー登録/削除機能	Webブラウザで、ユーザーを登録する。			○	
10	組織、ロール(LDAPグループ)の作成、変更				○	
11	ユーザーの組織、ロール(LDAPグループ)への配属	組織(LDAPグループ)へ、ユーザIDを配属させる。また権限(ロール、LDAPグループ)をユーザIDに付与する。			○	
12	パスワードポリシーの設定画面	英字+数字の混合、8文字以上、など、パスワードを推奨されにくくするための機能			○	
13	パスワードの有効期限設定画面	有効期限が切れたパスワードは使用できなくなる(ログイン画面で、パスワード変更を促す)			○	
14	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			○	
15	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			○	
16	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。 また、画面			○	
17	ユーザー検索機能	ユーザーを検索する。			○	
18	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。			○	
19	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。			○	
20	アカウントロックポリシーの設定画面	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数の設定、などの設定。			○	
21	アカウントロック自動解除機能	アカウントロックを夜間バッチなどで自動的に解除する。			○	

#	機能	説明	OpenAM	Open LDAP	NRI独自拡張	LISM
22	申請・承認ワークフロー機能					
23	ユーザー一括登録/削除登録	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。			○	
24	ユーザー属性一括変更機能	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。			○	
25	ユーザーの組織、ロール(LDAPグループ)への配属情報の一括登録	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。			○	
26	一括登録データ値チェック機能	CSVデータによるユーザーの一括登録、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。			○	
27	監査レポート機能					
28	監査ログ	監査レポート。			○	
29	ユーザーアカウント一覧	監査レポート。			○	
30	管理者権限ユーザーアカウント一覧	監査レポート。			○	
31	申請承認イベント一覧	監査レポート。			○	
32	特定ユーザー認証成功/失敗イベント一覧	監査レポート。			○	
33	特定システム認証成功/失敗イベント一覧	監査レポート。			○	
34	長期間未ログインユーザー一覧	監査レポート。			○	
35	パスワード有効期限切れユーザー一覧	監査レポート。			○	
36	アカウントロックユーザー一覧	監査レポート。			○	
37	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。			オプション	
38	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。			オプション	

#	機能	説明	OpenSSO OpenAM	Open LDAP	NRI独自拡張	LISM
39	認証・シングルサインオン					
40	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。	○			
41	リバースプロキシ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。	○			
42	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。			○	
43	SAML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「SAML」への対応。	○			
44	SAMLエージェント	連携先の業務システムを、「SAML対応」にするためのエージェント。			オプション	
45	SalesforceCRM、GoogleAppsなどとのシングルサインオン	SAMLを利用した、クラウドやSaaSとのシングルサインオン。	○			
46	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。	オプション			
47	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。	オプション			
48	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	○			
49	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。	○			
50	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。	○			
51	認証ログの記録	日時、ユーザID、成功/失敗、IPアドレスなど	○			

#	機能	説明	OpenSS O OpenAM	Open LDAP	NRI独自 拡張	LISM
52	ID管理、プロビジョニング					
53	源泉データの取り込み	CSVによる源泉データの取り込み				○
54	AD、LDAP、Oracleなどへのプロビジョニング	メタディレクトリのID情報と、各システムのID情報とを同期する。				○
55	Notes、サイボウズなどへのプロビジョニング	メタディレクトリのID情報と、各システムのID情報とを同期する。				オプション
56	SalesforceCRM、GoogleAppsなどへのプロビジョニング	メタディレクトリのID情報と、各システムのID情報とを同期する。				オプション
57	その他のシステムへのプロビジョニング	メタディレクトリのID情報と、各システムのID情報とを同期する。				オプション
58	パスワードのリアルタイム同期	パスワードのリアルタイム同期				○
59	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				オプション
60	パスワードの暗号化	パスワードの暗号化		○		
61	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、パスワードを推奨されにくくするための機能		○		
62	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（ログイン画面で、パスワード変更を促す）		○		

● その他のソリューション

約50種類のオープンソースを、ワンストップでサポート

機能	オープンソース
OS	CentOS、RedHat Enterprise Linux
データベース	MySQL、MySQL Cluster、PostgreSQL、MongoDB
言語	PHP、Ruby
Webサーバ	Apache HTTP Server
プロキシサーバ	Squid
APサーバ	Apache Tomcat、JBoss AS、JBoss EAP、JBoss EWS
フレームワーク	Apache Struts、Spring、Seasar2、JBoss Seam、Ruby on Rails
ORMマッピング	Hibernate、MyBatis(iBATIS)
ログ管理	Log4j
SOAP	Apache Axis2
ビジネスプロセス	JBoss jBPM
ルールエンジン	JBoss BRMS
SOA	JBoss SOA
ネットワーク	Vyatta
DNS	BIND

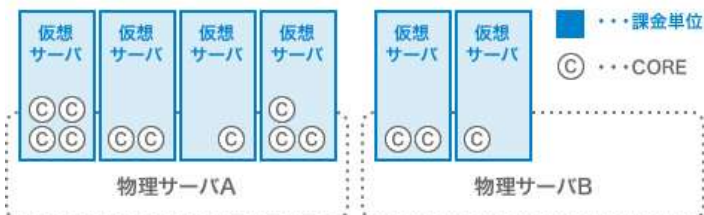
機能	オープンソース
ファイルサーバ	Samba
認証サーバ	OpenLDAP
メールサーバ	Postfix、sendmail
POP3/IMAP	Dovecot、Courier-IMAP
バージョン管理	CVS、Apache Subversion
インシデント管理	OTRS、Redmine
クラスタリング	Heartbeat、Pacemaker、DRBD
シングルサインオン	OpenSSO、OpenAM
ID管理	LISM
運用監視	Hinemos、Zabbix
BI・レポート作成	Jaspersoft、JasperReports、iReport、Pentaho
ポータル・文書管理	Liferay、Alfresco、Joomla!
グループウェア	Aipo
オフィススイート	Apache OpenOffice、LibreOffice
業務システム	ADempiere、MosP、SugarCRM、vtiger CRM

クラウド環境でのソフトウェアコストを削減します

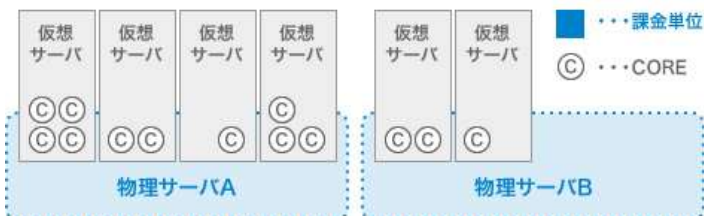
- OSSと異なる多くの商用ソフトウェアは、クラウド環境に適合した価格体系でないため、高コストになる場合がある。
- クラウド環境に適したOSSサポートサービスメニュー「OpenStandia クラウドサポート」の利用により、コスト削減が可能。

商用ソフトウェアの主な課金ケース

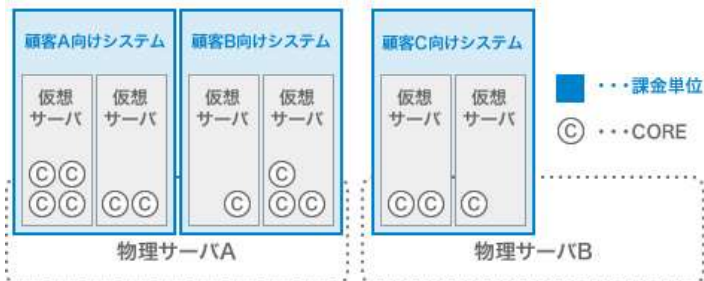
ケース1) 仮想サーバ単位



ケース2) 物理サーバ単位



ケース3) 顧客単位、又はサブシステム単位



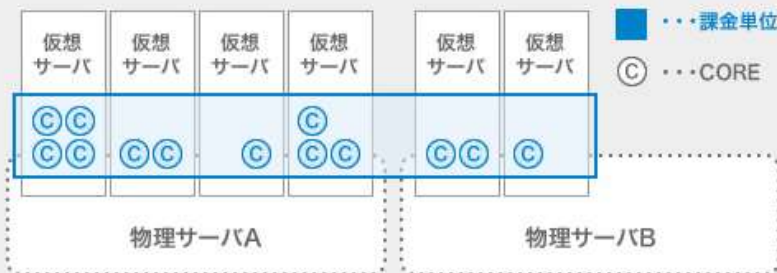
クラウド環境向け
オープンソース
サポートサービス

OpenStandia
クラウドサポート
を利用すると

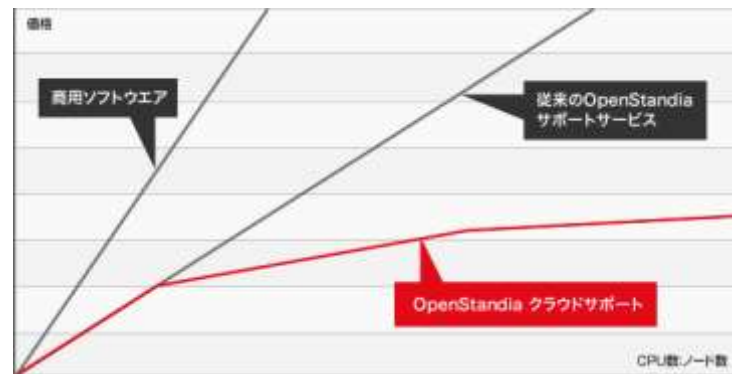
■ 実際に利用しているCORE数によって課金。

■ クラウド環境上に複数のシステムが稼働する場合であっても、クラウド環境全体のCORE数を合算して、価格を算出。

同一クラウド環境上の全てのCORE数を合算し、CORE数に応じて課金。
ムダの無い価格設定を実現。



■ 利用するCORE数が多いクラウド環境においては、ボリュームディスカウントを適用。



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。

- 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！



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



osscc@nri.co.jp



<http://openstandia.jp/>