

# OpenAM & OpenIDM 活用事例セミナー



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 : [oss@nri.co.jp](mailto:oss@nri.co.jp) Web : <http://openstandia.jp/>



# ●はじめに

- 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OSS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、オープンスタンダード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。



オープンソースまるごと

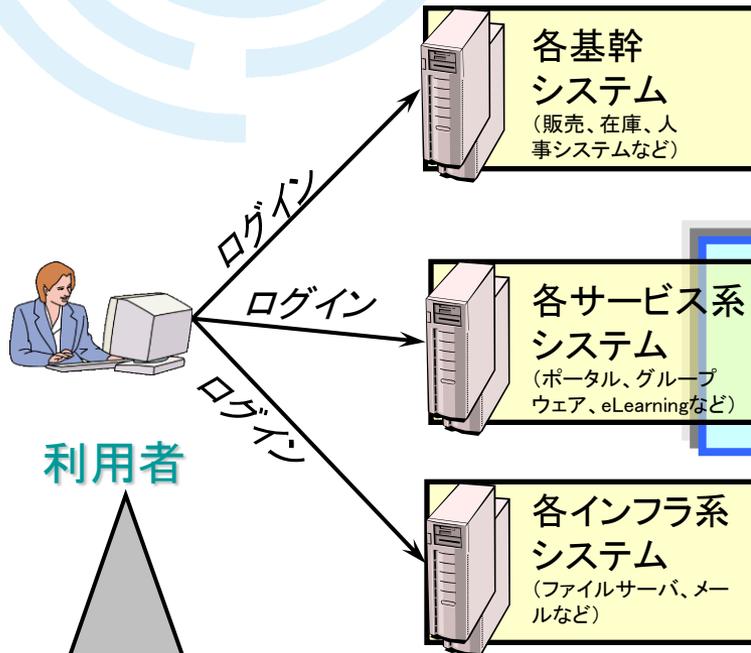


## ● 高まるシングルサインオン・統合ID管理のニーズ

# シングルサインオンについて

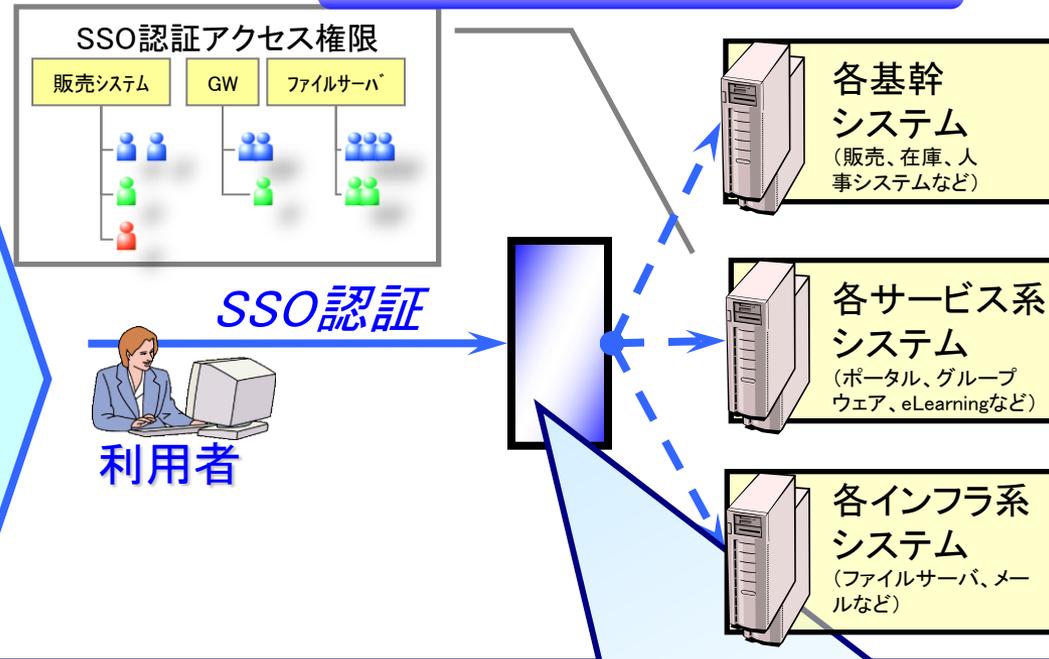
- SSO認証を導入すると、様々なシステムへのSSOとアクセス制御が可能となり、利用者の利便性向上やセキュリティ向上につながる

## 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)

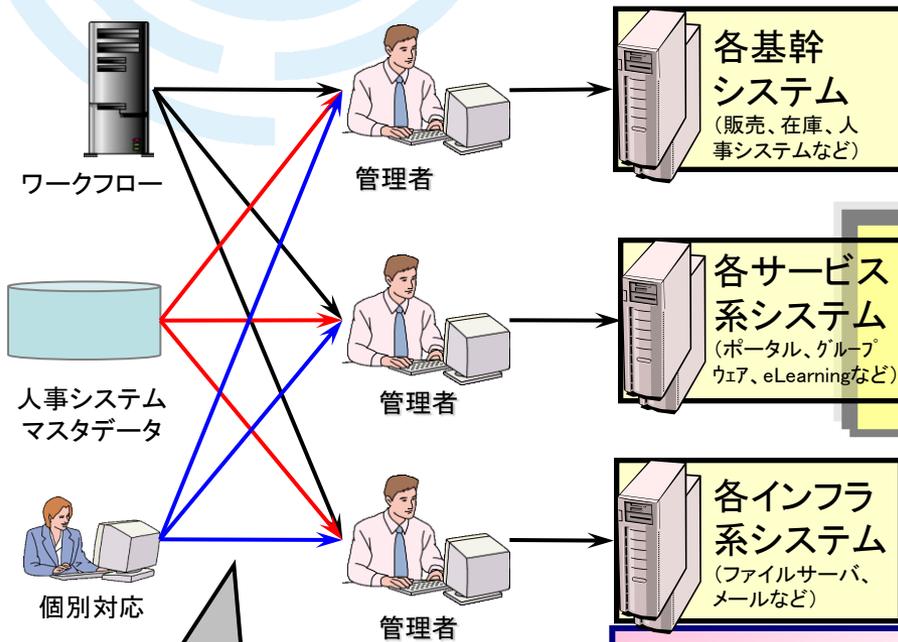


- ▶ アクセス権限付与に基づく厳密なアクセス制御
- ▶ セキュリティポリシーに基づいた厳密な認証インターフェース
- ▶ システムへのアクセスの認証の統合化による利便性向上
- ▶ アクセスログの一括取得
- ▶ 多様化する認証方式への対応
  - ✓ 対象システム : Web系システム、C/S系システム、OS…
  - ✓ 認証連携インターフェース : ID/PWD、生体認証、PKIなど

# ID管理について

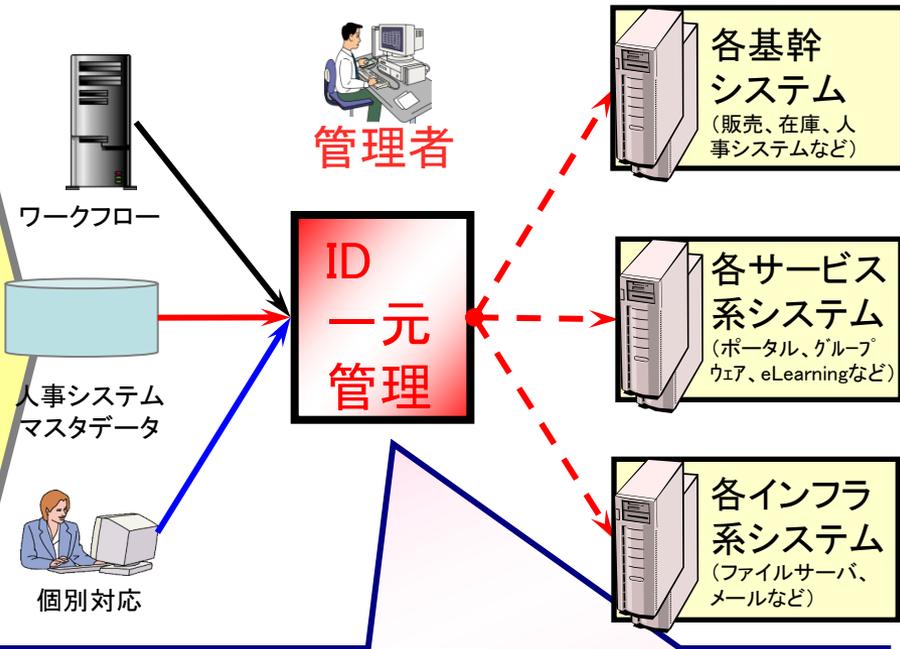
- 入社・退社・人事異動時に、利用システム毎のアカウントの個別ID管理(登録/修正/削除/参照)に対して、導入後は統合的に管理することにより、運用効率化・負担 & ID管理ミス軽減となる

## 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

## 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/>

## ● クラウド(SaaS)、ASP事業者

## ● 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

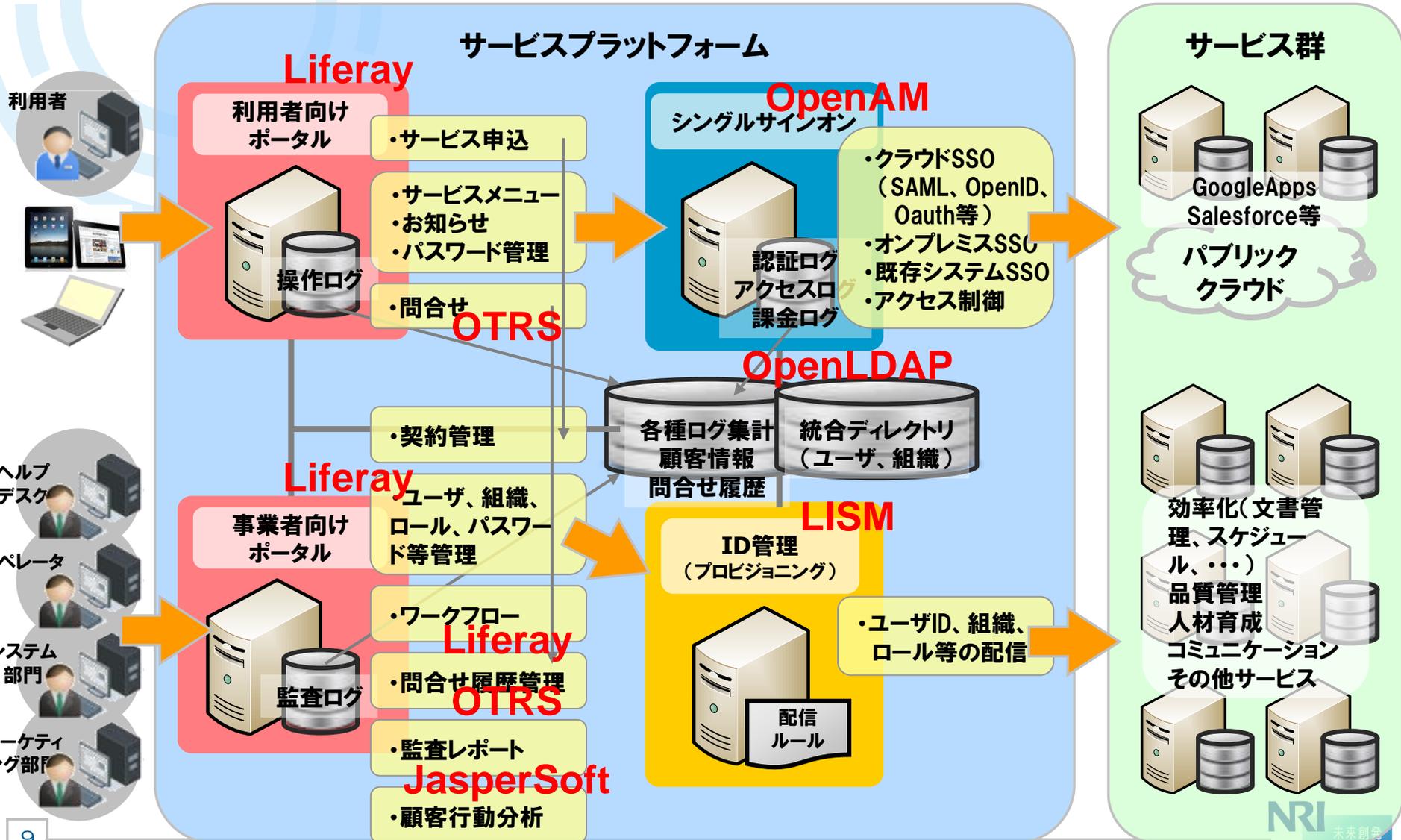
- ▶ 競合他社との差別化のため、サービス提供に力を入れている。
- ▶ 顧客である医療機関に対して、製品情報、医療機関同士の情報交換、医療機関の事務効率化などを目的としたサービスの提供を計画。
- ▶ 既存のパッケージやクラウドサービスをフルに活用し、短期間に多くのサービスを提供できるようにするための、プラットフォームを構築。

### ● 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

## ● 大手製造業など



# ● 光回線の契約顧客に回線＋「サービス」を提供

## ● 導入目的

- ▶ 光回線を契約している顧客に対して、様々な「サービス」の提供を行う、新たなビジネスを計画。
- ▶ 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。
- ▶ アプリケーションのユーザ管理のみならず、特権ID(OSユーザID)の管理も視野に。

## ● 導入効果

- ▶ 統合ID管理、シングルサインオン、ポータルなど、サービス提供に必要な機能をパッケージで提供。ソフトウェアコストも抑えることで、ビジネス拡大に貢献。

## ●クラウド(SaaS)、ASP利用者

# (事例)大手家電メーカー クラウドサービスとのSSO

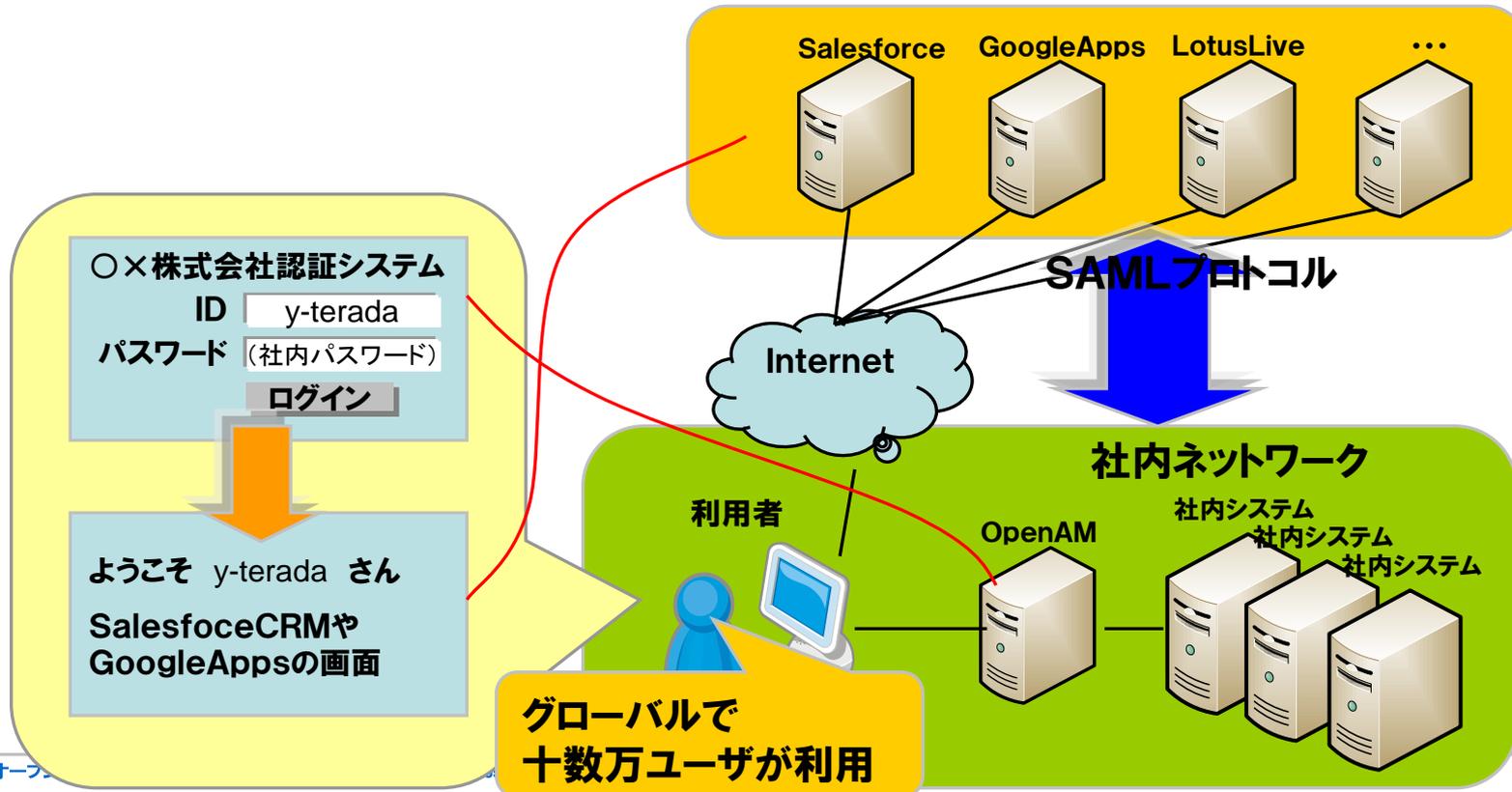
## ● GoogleAppsやSalesforceCRMとのシングルサインオン

### (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、Salesforce CRM、GoogleAppsにログイン可能に。



## ● 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

## 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

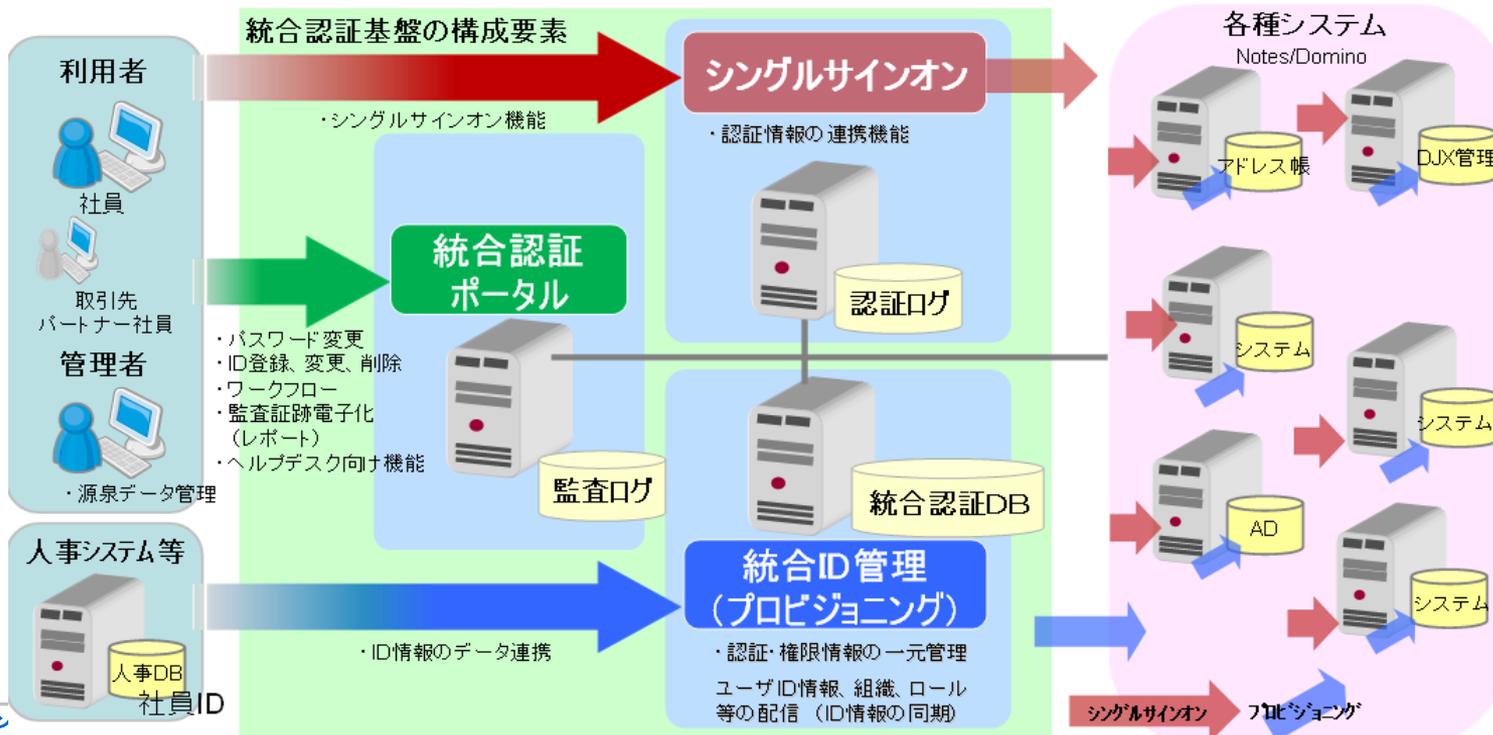
- ▶ 人事、会計など、基幹業務システムと、AD、NotesなどのOA系・情報共有系システム。GoogleAppsの利用や、スマートフォンからの情報照会を新たに開始。

### ● 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。



## ● グループ企業、グローバル企業

# 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、スムーズ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。

## 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

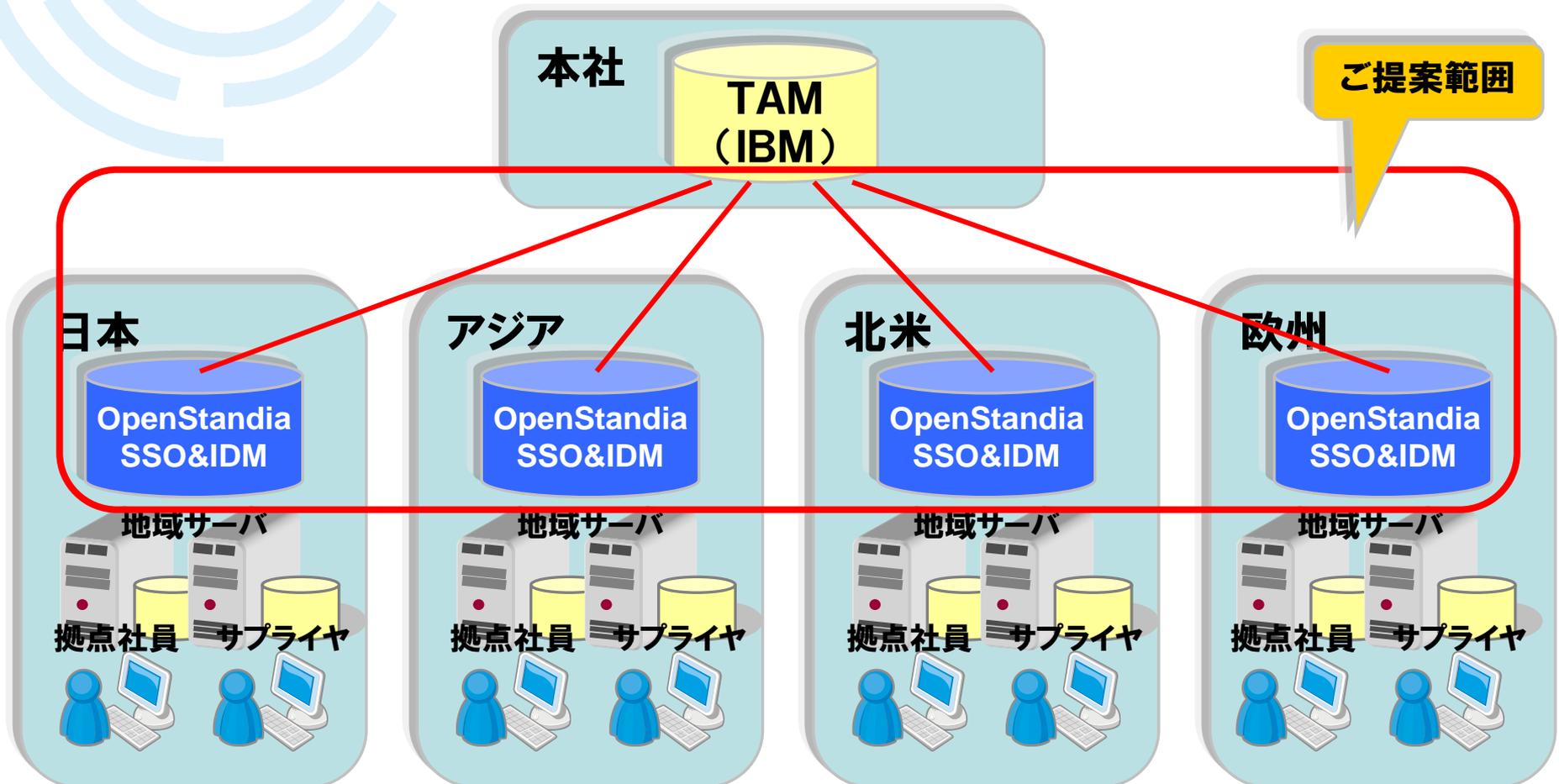
部門 会社 派遣社員 取引先 グループ グローバル

- 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活用(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)

## (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。



## ● モバイルPC・スマートフォン・タブレット活用時

# 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アプライアンスと、OpenAMとの連携機能



- ・ワンタイムパスワード
- ・マトリクス認証
- ・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

PKIは使用しないケースもあり

PKI認証

## ● 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



## ● OSSでは不足している機能を、統合認証ポータルとしてご提供

### 利用者向け機能の提供

- ・ポータル(ダイナミックメニュー)
- ・パスワード変更画面
- ・パスワード初期化機能
- ・その他

### ヘルプデスク・管理者向け機能の提供

- ・ユーザ管理、一括登録
- ・組織管理、一括登録
- ・ロール管理
- ・パスワードポリシーの変更
- ・パスワード初期化
- ・パスワード期限切れ通知メール
- ・アカウントロック解除
- ・承認ワークフロー
- ・監査レポート
- ・課金ログ(予定)、その他

### OpenAMカスタマイズ

- ・C/SシステムとのSSO
- ・代理認証

### シングルサインオン OpenAM



- ・リバプロ型SSO
- ・エージェント型SSO
- ・SAML対応
- ・DesktopSSO
- ・アクセス制御

### 統合認証 ポータル



監査ログ

### 統合ディレクトリ OpenLDAP



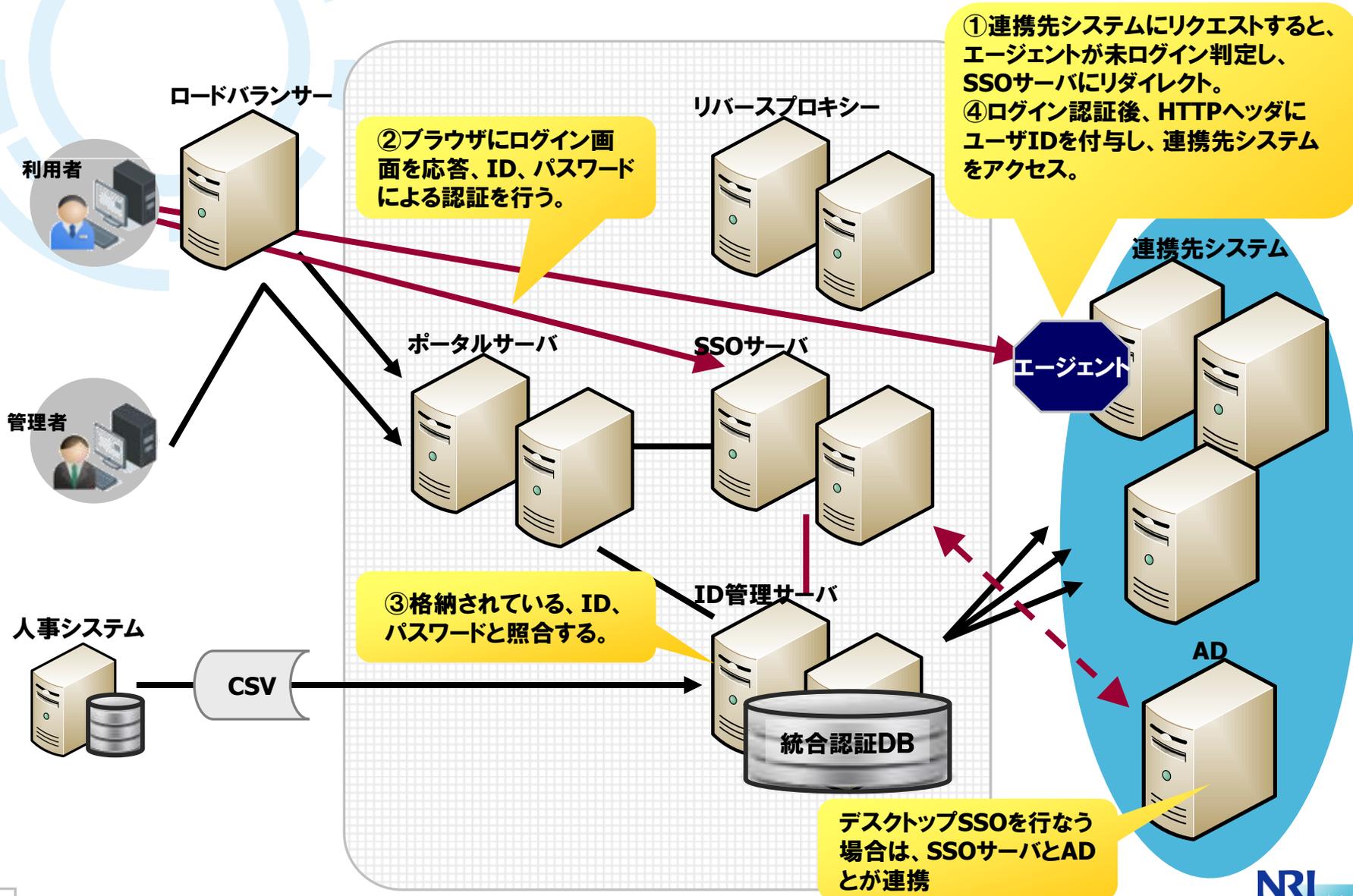
- ・ID、Pw管理
- ・ID、Pw認証



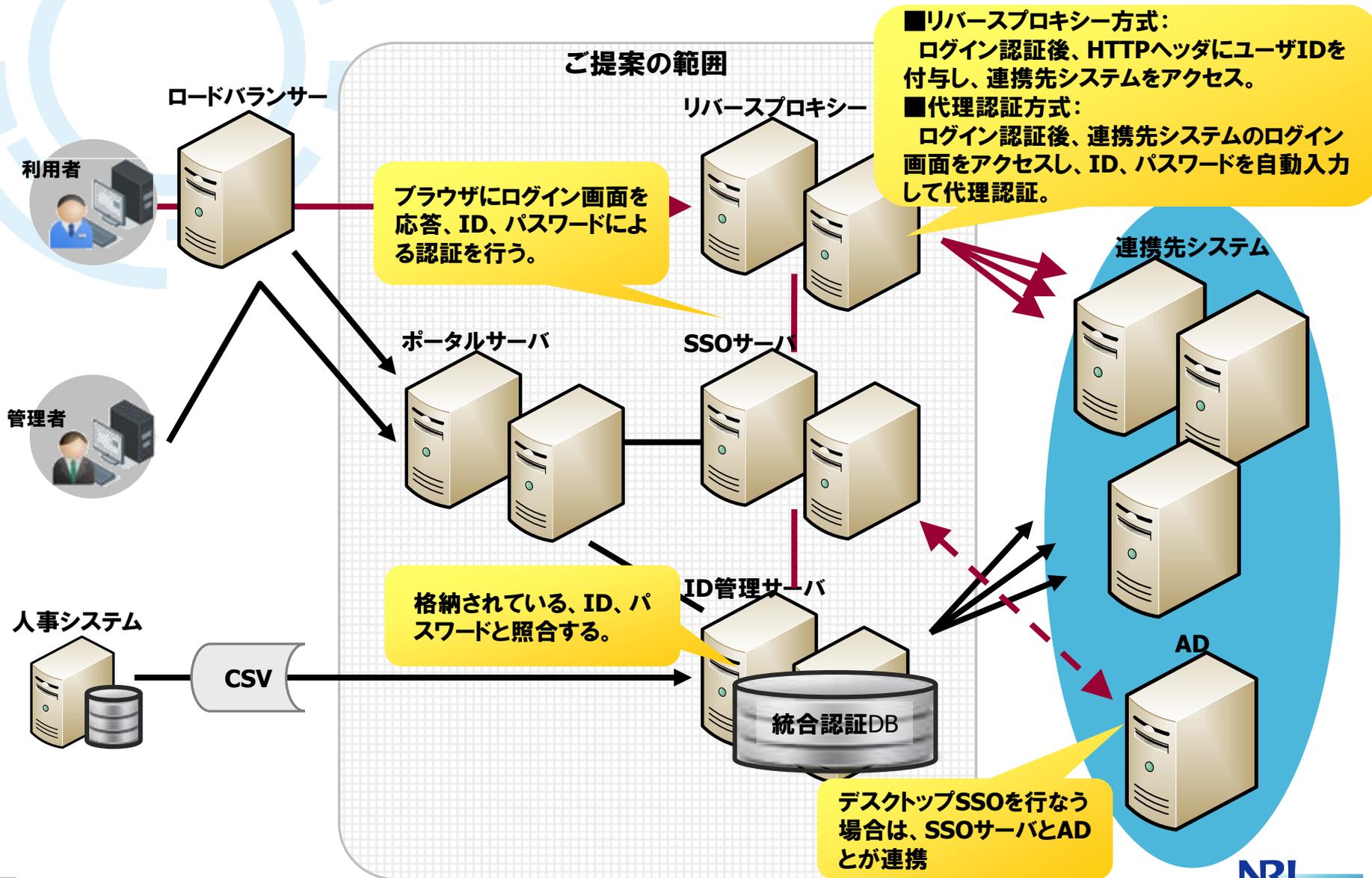
### ID管理 (プロビジョニング) LISM

- ・プロビジョニング

# 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、及び代理認証時の処理シーケンス概要



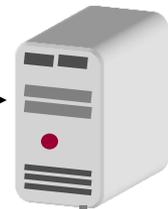
# 代理認証について

(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。

利用者



OpenAM



OpenLDAP  
 (MySQL)



(機能2)  
 所属やロールによって、  
 連携先システムへのア  
 クセスを許可する。  
 (例)課長ならOK

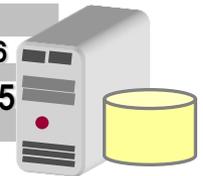
(機能3)  
 連携先システムのログ  
 イン画面に対して、代  
 理認証用のID、パス  
 ワードをセットして送信。

```
http://www.apl01.com/loginaction
userid=N1096
password=12345
```

UID=y-terada  
 UserName=寺田雄一  
 Organization=OSS推進室  
 Role=課長  
 Apl01ID=N1096  
 Apl01Pw=12345

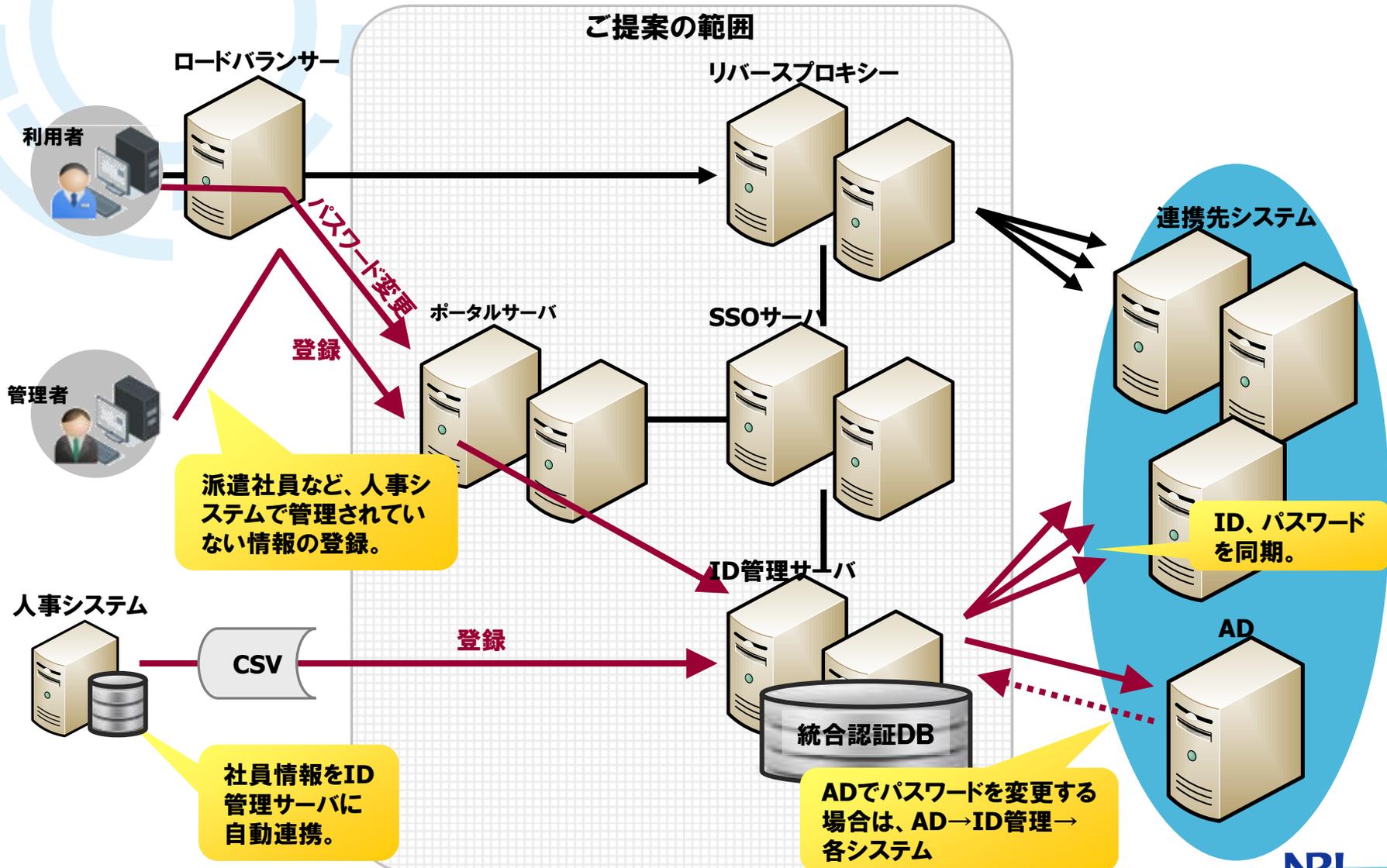
連携先システム  
 APL01

```
userid N1096
password 12345
```



**NRI独自の代理認証エン  
 ジンで、ほぼ全てのWebシ  
 ステムに対して、改修なし  
 で連携可能。**

# ID管理(プロビジョニング)処理シーケンス



# 統合認証ポータル(利用者向け)

## ●ポータル機能、ダイナミックメニュー

The screenshot shows a web browser window displaying the OpenStandia portal. The browser title is "HOME - 野村電気グループポータル - Mozilla Firefox". The page has a navigation menu with items like "HOME", "SSO対象サイト1", "SSO対象サイト2", "SSO対象サイト3", "ワークフロー", and "監査レポート". A red circle highlights this menu, with a callout box 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。" (Menus can be changed depending on the organization you belong to or the permissions (roles) you have been granted.)

On the left side, there is a "リンク集" (Link Collection) menu. A red circle highlights 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", and "ユーザの管理". A callout box explains: "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。" (Menus for users such as password change and user attribute change. And menus for administrators such as user registration application.)

The main content area shows a table of announcements. A callout box labeled "お知らせ" (Notice) points to the table. Below the table, there is a "ワークフロー追跡" (Workflow Tracking) section. A callout box labeled "申請・承認ワークフロー" (Application/Approval Workflow) points to the workflow diagram. The diagram shows a process: "申請" (Application) by 寺田 雄一 → "部長承認" (Department Head Approval) by 寺田 雄一 → "情シス承認" (IT Approval) by デモ 001. There are buttons for "内容を確認する" (Check content) and "コピーして申請する" (Copy and apply).

At the bottom, there is a "スケジュール" (Schedule) section with a calendar view for April 5th to 11th, 2012. A callout box labeled "申請・承認ワークフロー" (Application/Approval Workflow) points to the calendar.

## ● ユーザーの一覧

The screenshot shows a web application interface for user management. The main content area displays a table of users with columns for selection, name, user ID, department, and organization. Callouts point to various UI elements: '新規ユーザーの登録' (New user registration) points to the '追加' (Add) button; 'ユーザー属性の追加' (Add user attributes) points to the 'カスタム属性' (Custom attributes) button; 'ユーザー一覧のCSVダウンロード' (Download CSV of user list) points to the 'エクスポート' (Export) button; 'ユーザーの検索' (Search for users) points to the search input field; 'ユーザー情報の編集、及びアカウント停止' (Edit user information and stop account) points to the '操作' (Action) buttons; '複数ユーザーを選択してアカウントを停止' (Stop account for multiple selected users) points to the '停止にする' (Stop) button; and '完全にユーザーを削除する場合は、一旦停止してから、削除する。' (When deleting a user completely, stop them first and then delete) points to the '操作' buttons.

ユーザー - 野村電気グループポータル - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

ユーザー - 野村電気グループポータル

コントロールパネル

寺田 雄一

アカウント情報  
マイページ

内容

Web コンテンツ  
ファイルの管理  
画像の管理  
ブックマーク  
掲示板

組織  
コミュニティ  
ユーザー

新着情報の管理

サーバー  
サーバー管理者  
ポータルインスタンス

ユーザー

すべてを参照 追加 カスタム属性 エクスポート

検索

検索オプション >

停止にする

<input type="checkbox"/>	姓	名前	ユーザID	部署	組織	操作
<input type="checkbox"/>	デモ	001	demo001	部長	人事部 営業部 経理部 総務部 製品開発部 野村販売(株) 野村電気上海(工場)	操作
<input type="checkbox"/>	デモ	サイ ト	管理 者	oss		操作
<input type="checkbox"/>	デモ	002	demo002	営業部		操作
<input type="checkbox"/>	デモ	003	demo003	製品開発部		操作
<input type="checkbox"/>	デモ	004	demo004	経理部		操作
<input type="checkbox"/>	デモ	005	demo005	野村販売(株)		操作
<input type="checkbox"/>	デモ	006	demo006	野村電気上海(工場)		操作
<input type="checkbox"/>	寺田	雄一	y-terada	営業部 製品開発部		操作

該当件数: 8 件

## ● パスワードポリシーの設定

### パスワード権文確認

権文確認  ⓘ

辞書に載っている言葉を許可  ⓘ

最小の長さ  ⓘ

許可文字の使用  ⓘ

許可文字  ⓘ

### パスワード履歴

履歴有効  ⓘ

履歴回数  ⓘ

### パスワード有効期限

有効期限の設定  ⓘ

有効期限  ⓘ

有効期限の残り期間  ⓘ

猶子回数  ⓘ

有効期限切れメールを送信する  ⓘ

メール通知タイミング  12時間前  1日前  2日前  3日前  4日前  5日前  6日前  1週間前  2週間前 ⓘ

# 申請・承認ワークフロー

## ● 申請画面



ワークフロー - 野村電気グループポータル - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

ワークフロー - 野村電気グループポータル

OpenStandia™/Portal

統合認証ポータル

HOME SSO対象サイト1 SSO対象サイト2

ワークフロー申請

項目を設定して次の確認画面へ進んでください。

申請書名 ユーザ登録申請

申請CSVファイル  参照...

コメント

申請 (履歴) 寺田 雄一

部長承認 (履歴) 寺田 雄一

情シス承認 (履歴) デモ 001

申請確認画面へ進む

TOP画面へ戻る

コントロールパネル ページの管理 編集制御のトグル

検索: openid 次を検索(N) 前を検索(P) すべて強調表示(A) 大文字/小文字を区別(O) ページ末尾まで検索したので先頭に戻って検索しました。

申請データ(CSV)をアップロードする。

CSVデータについて、

- ・必須項目チェック
- ・メールアドレス等の型チェック
- ・組織やロールなどのマスタ存在チェック
- ・申請権限の有無チェックなどを行なう。

承認者のステップは複数設定可能。

# 監査レポート画面例

## ● 認証ログ・ユーザ情報・監査ログを分析

認証ログ - 野村電気グループポータル - Mozilla Firefox

検索条件: time 3月 24 2011 ~以後

time	Data	LoginID	ContextID	IPAddr	LogLevel	Domain
2011/03/22 17:23:57	Login Success service StandardSSO	id=14,ou=user,dc=opennsso,dc=java,dc=net	316830264e82805301	192.178.185.217		
2011/03/22 17:23:57	Login Success service StandardSSO	id=15,ou=user,dc=opennsso,dc=java,dc=net	201908acc0110c4701	192.178.185.217		
2011/03/22 17:23:57	Login Success service StandardSSO	id=13,ou=user,dc=opennsso,dc=java,dc=net	83a9e3d25f532b3301	192.178.185.217		
2011/03/22 17:25:42	Login Success service StandardSSO	id=15,ou=user,dc=opennsso,dc=java,dc=net	f299ea37330a77f01	192.178.185.217		
2011/03/22 17:25:42	Logout service StandardSSO	id=14,ou=user,dc=opennsso,dc=java,dc=net	335cdbe0b1c372501	192.178.185.217	INFO	dc=opennsso,dc=java,dc=net
2011/03/22 17:25:42	Logout service StandardSSO	id=15,ou=user,dc=opennsso,dc=java,dc=net	8eb821658da8d3ed01	192.178.185.217	INFO	dc=opennsso,dc=java,dc=net
2011/03/22 17:25:42	Login Success service StandardSSO	id=15,ou=user,dc=opennsso,dc=java,dc=net	29308af91b28ab30c01	192.178.185.217	INFO	dc=opennsso,dc=java,dc=net

「認証に失敗したユーザーの一覧」、  
「特定のユーザーの認証履歴」、  
「特定のシステムに対する認証の履歴」  
などを検索できる。

あるユーザに対して、いつ、だれが、どのような操作(権限付与、パスワード変更、...)を行ったのかを確認できる。

「一定期間ログインしていないユーザ」、  
「パスワードの有効期限が切れているユーザ」、  
「特定の権限を持つユーザ」、  
「アカウントロック中のユーザ」、  
などを検索できる。

ユーザ名	所属組織	権限	パスワードの有効期限	最終ログイン日時
demo002	野村電気	Administrator	2999/01/01	2011/03/24
demo003	営業部, 製品開発部	Administrator, Power User, 管理職	2015/11/01	2011/03/23
demo004	営業部	Power User	2011/08/01	2011/03/20
demo005	製品開発部	Power User	2012/11/15	
demo006	経理部	Power User	2011/11/01	
	野村販売(株)	Power User	2011/11/01	
	野村電気上海(工場)	Power User	2011/11/01	
	人事部, 営業部, 経理部, 総務部, 製品開発部, 野村販売(株), 野村電気	Power User, 管理職	2011/11/01	2011/03/24

## (ご参考)テンプレート付随のドキュメント一覧

**Slerとしてのノウハウに基づき、主にOSS製品導入にあたって設計しなければならない技術要素に関して、設計書を提供しております。**

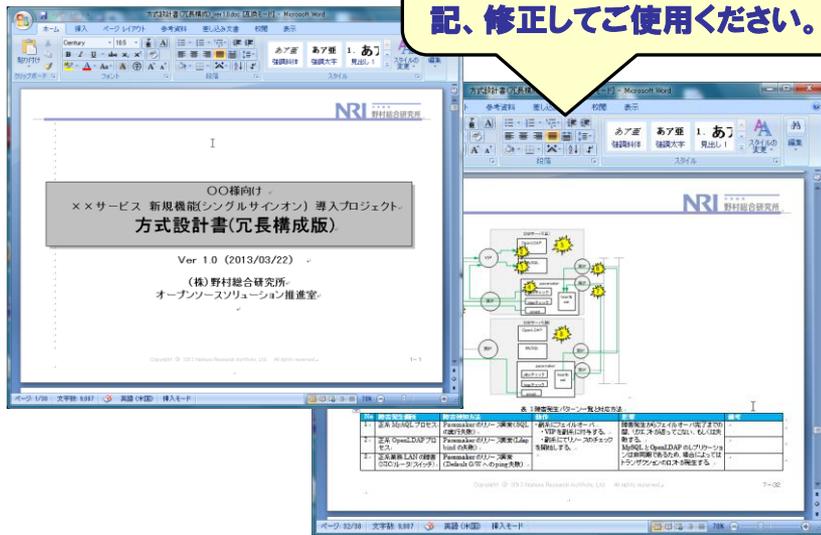
#	分類	工程/カテゴリ	ドキュメント名称(例)
1	設計ドキュメント	概要設計	【要件定義・別紙】アクター・権限一覧.xls
2		基本設計	方式設計書_ver1.0.doc
3			方式設計書(冗長構成)_ver1.0.doc
4			【別紙】認証データ関連関連表.xlsx
5		詳細設計	DBサーバ_パラメータ設定書_ver1.0.xlsx
6			DBサーバ_パラメータ設定書(冗長構成)_ver1.0.xlsx
7			SSOサーバ_パラメータ設定書_ver1.0.xlsx
8			SSOサーバ_パラメータ設定書(冗長構成)_ver1.0.xlsx
9			IDMポータルサーバ_パラメータ設定書_ver1.0.xlsx
10			IDMポータルサーバ_パラメータ設定書(冗長構成)_ver1.0.xlsx
11			エラー画面詳細設計.xlsx
12			パスワード一覧.xlsx
13	マニュアル	VM導入手順書	VM導入手順書【シングル構成】.docx
14			VM導入手順書【冗長化構成】.docx
15		運用手順書	運用手順書【シングル構成】.doc
16			運用手順書【冗長構成】.doc

# (ご参考)テンプレート付随のドキュメント一覧

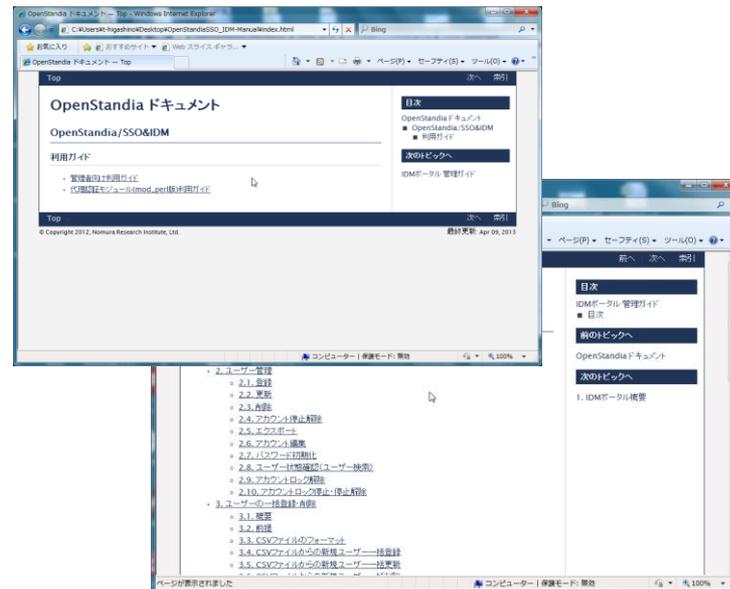
#	分類	工程/カテゴリ	ドキュメント名称(例)
17	マニュアル	運用手順書	代理認証サイト追加【mod_perl版:フォーム認証】.docx
18			代理認証サイト追加【ベーシック認証】.docx
19			変更手順書【SAML】.docx
20			変更手順書【リバプロ】.docx
21	オンラインマニュアル	一式(HTML)形式	

## <方式設計書の例>

目次だけではなく内容も記述済みです。  
お客様環境や要件に関する部分を追記、修正してご使用ください。



## <オンラインマニュアルの例>



※設計書およびマニュアルはOpenStandia  
のオリジナルドキュメントです。(日本語版です)

# その他の主な事例

#	時期	業種	提供ソリューション	ユーザー数	使用OSS	タイトル	システムの概要
1	2012/01 ～	医療機器メーカー	OpenStandia/SSO&IDM	10,000	OpenAM, OpenLDAP, LISM, Liferay, Apache, Tomcat, JBossAS, MySQL	次世代サービスプラットフォームにおける統合認証基盤を構築	品質管理や情報共有、コミュニケーションといった様々なサービスを、グローバルの顧客に対して提供するための、「サービスプラットフォーム」。契約管理、顧客管理、行動分析などの提供も予定されるが、ベースとなる統合認証基盤を構築。
2	2011/12 ～	不動産	OpenStandia/SSO&IDM	6,000	OpenAM, OpenLDAP, LISM, Liferay, Apache, Tomcat, JBossAS, MySQL	人事異動時のID管理業務を大幅に効率化、GoogleAppsにも対応	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。
3	2011/07 ～	電子機器メーカー	OpenStandia/SSO&IDM	500,000	OpenAM, OpenLDAP, LISM, Liferay, Apache, Tomcat, JBossAS, MySQL	グローバル・サービス提供のための統合認証基盤を構築	自社顧客にインターネット経由で提供している複数サービスに関する統合認証基盤。統合ID管理、及びシングルサインオンを提供。顧客（消費者）の利便性を高めるとともに、高度なCRMを実現。
4	2011/09 ～	教育機関	OpenStandia/SSO&IDM	1,000,000	OpenAM, Liferay, Apache, Tomcat, JBossAS, MySQL	大規模会員サイトのシングルサインオン	会員数約100万人の大手教育機関。会員向けの各種サービスにおける、シングルサインオン導入プロジェクト。
5	2011/04 ～	建材メーカー	OpenStandia/SSO&IDM	10,000	OpenAM, OpenLDAP, LISM, Liferay, Apache, Tomcat, JBossAS, MySQL	取引先を含めた情報システムの活用を支える、統合認証基盤	取引先などを含めたシステム。クラウド提供。取引先を含めたIDを管理し、取引先が情報システムにセキュアにアクセスできるようにすることで、ビジネスのスピードアップを図る。

# その他の主な事例

#	時期	業種	提供ソリューション	ユーザー数	使用OSS	タイトル	システムの概要
6	2010/12 ～	ISP	OpenStandia/SSO&IDM	10,000	OpenAM, OpenLDAP, LISM, Liferay, Apache, Tomcat, JBossAS, MySQL	ISPによるサービス提供プラットフォームの構築	ISPが自社顧客に、SaaSを提供する基盤。自社開発の各アプリと、Salesforceなどのパブリッククラウドとの統合認証基盤。各サービスの玄関口となるポータルも提供。
7	2011/01 ～	ヘルスケア	OpenStandia/SSO&IDM	10,000	OpenAM、Tomcat	自社サービスと顧客システムとのシングルサインオンを実現	インターネット上に複数のサービス(サイト)を展開している。
8	2010/12 ～	家電メーカー	OpenStandia/SSO&IDM	5000 ～ 100000	OpenAM、Tomcat	自社認証基盤と、クラウドサービスを、SAML連携	既に、自社に統合認証基盤を構築済み。これと外部のサービス(LotusLive)と統合認証したい。
9	2009/11 ～	家電メーカー	OpenStandia/SSO&IDM	3,000	OpenAM、Tomcat	自社認証基盤と、クラウドサービスを、SAML連携	既に、自社に統合認証基盤を構築済み。これと外部のサービス(Salesforce、GoogleApps)と統合認証したい。
10	2010/08 ～	会員サイト	OpenStandia/SSO&IDM	5500 ～ 40000	OpenAM, OpenLDAP, Apache, Tomcat	インターネット・サービス向け認証基盤をSaaS提供	インターネット上に複数の会員サイトを保有している。
11	2010	パッケージベンダー	OpenStandia/SSO&IDM	不明	OpenSSO	アプリケーション・パッケージのSAML対応を支援	自社パッケージをSAMLに対応するための改修。
12	2010	大学	OpenStandia/SSO&IDM	3,000	OpenSSO、Tomcat	大学の学内システムをシングルサインオン対応	学生、教職員あわせてユーザー数約3000名。複数の学内システム。

## その他の主な事例

#	時期	業種	提供ソリューション	ユーザー数	使用OSS	タイトル	システムの概要
13	2009	大手法人	OpenStandia/SSO&IDM	100,000	OpenAM, OpenLDAP, LISM, Tomcat	10万人規模の統合ID管理システム	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。
14	2009	外資系企業	OpenStandia/SSO&IDM	500	—	SOX法対応のための統合ID管理	米国上場企業の国内法人の社内システム。
15	2009	会員サイト	OpenStandia/SSO&IDM	30,000	OpenSSO、Tomcat	3万人規模の会員サイトをシングルサインオン対応	インターネット上に、会員数3万名の、複数のサイト保有。認証サーバとしては、ActiveDirectoryを利用。
16	2008	SaaSベンダー	OpenStandia/SSO&IDM OpenStandia/Portal	30,000	OpenSSO、Liferay	SaaSプラットフォームとしての認証基盤とポータル	新しいSaaSビジネスを開始するにあたり、プラットフォームとして認証基盤とポータルを検討。

## ●ご参考

# OpenStandia / SSO & IDM機能

#	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、パスワードを類推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などの設定、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。			○	

# OpenStandia / SSO & IDM機能

#	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	

# OpenStandia / SSO & IDM機能

#	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、パスワードを類推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

# OpenStandia/Bizシリーズ

## オープンソースを活用した、低コストな統合業務システムソリューション

### OpenStandia/Bizシリーズの特徴



- オープンソースの活用により、ソフトウェアコストを大幅に削減。
- シンプルかつ基本的な機能を提供することで、短期間の導入が可能。
- オープンソースでありながら、会計、販売管理、購買管理、在庫管理、人事、給与計算、勤怠管理といった業務間でデータ連携を自動化した「統合業務システム」を実現。  
これにより、二重入力などの手間を省き業務の効率化や経営の見える化を実現。
- オープンソースであるため設計情報、データ構造が公開されており、統合管理されたデータを活用した周辺システムの開発が容易。また、パッケージ本体とは独立しているため、パッケージのバージョンアップの影響を受けにくく、維持管理費用を削減可能。さらに、お客様の既存システム(例えば既存の会計システム)などとの連携も容易。

### OpenStandia/Bizシリーズの概要

- 「OpenStandia/Bizシリーズ」は、以下の11のコンポーネントで構成されます。



### 主なオープンソース

- MosP(人事システム)
- ADempiere / iDempiere (統合業務システム)

## 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



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](mailto:ossc@nri.co.jp)



<http://openstandia.jp/>