

# クラウド時代のOSS戦略

～シングルサインオン(OpenAM)、統合ID管理(LISM)など最新事例紹介～

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



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](mailto:osscc@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。



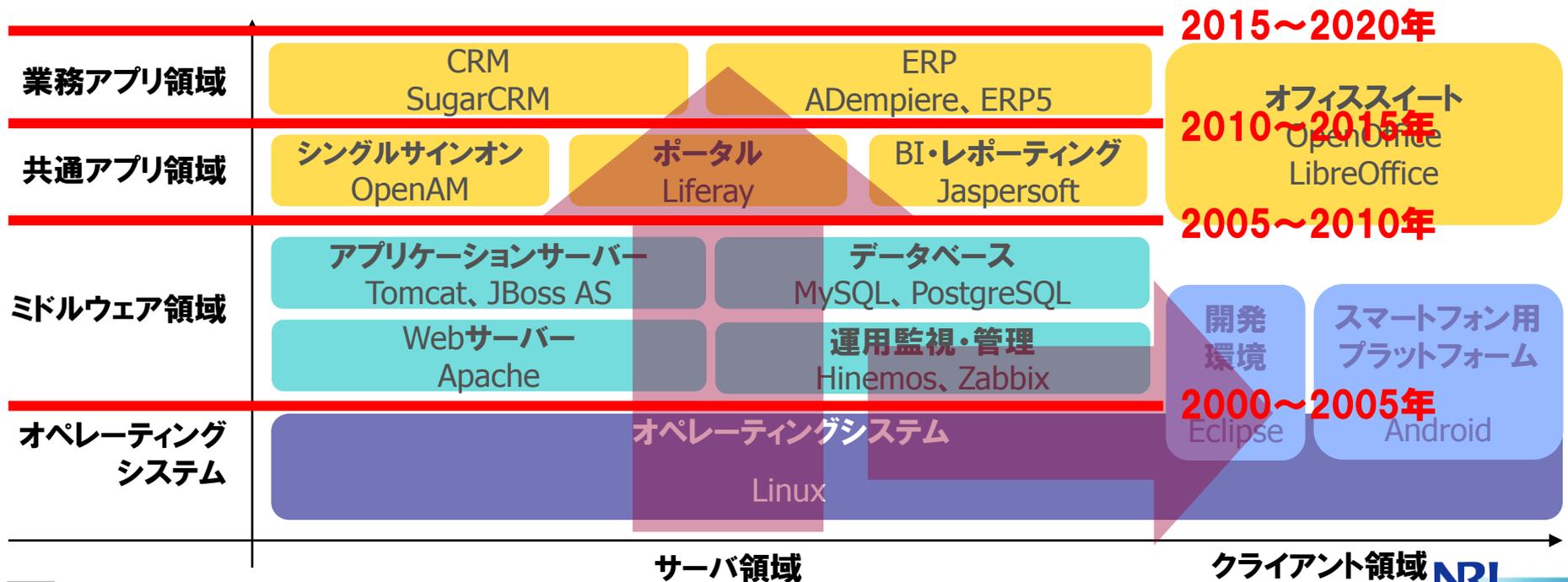
オープンソースまるごと



## なぜ、今「オープンソース」なのか？

# オープンソースの基本トレンド

- オープンソースの活用範囲は、OSから業務アプリケーション領域に、順次拡大している。
  - ▶ OS(Linux)、Webサーバ(Apache)、開発環境(Eclipse)は成熟。
  - ▶ APサーバ(JBoss、Tomcat)、DBMS(PostgreSQL、MySQL他)も、大手企業においても採用されるようになった。商用製品のシェアを奪いつつある。
  - ▶ シングルサインオン(OpenAM)や、ポータル(Liferay)、BI・レポートング(Jaspersoft)は、この1~2年で急速に導入事例が増え、シェアを伸ばしている。
  - ▶ 業務アプリケーション領域(ERPのADempiereなど)は、今後1~2年で立ち上がってくるものと予想される。
  - ▶ 一方、端末領域のOSS活用も進んでいる。



すでに普及している、オープンソース。

1,000社

すでに普及している、オープンソース。

各業界の「トップ企業グループ」が、既にオープンソースを活用し、  
 成果をあげています。(弊社事例)

業種	OSS
大手銀行、地銀、信用金庫	Tomcat、JBoss、他
大手証券会社	JBoss、MySQL、他
大手自動車メーカー	PostgreSQL、他
大手自動車部品メーカー	Apache、Tomcat、JBoss、OpenAM、Liferay、他
大手電子機器メーカー	Tomcat、JBoss、MySQL、OpenAM、Liferay、他
大手家電メーカー	Tomcat、Subversion、OpenAM、他
大手化学メーカー	Tomcat、PostgreSQL、他
通信会社	Tomcat、JBoss、OpenLDAP、他
電力会社、電力会社グループ企業	JBoss、PostgreSQL、OpenAM、Liferay、他
大手流通業	Apace、JBoss、Liferay、他
大手商社	JBoss、MySQL、他
大手メディア企業	JBoss、MySQL、他
大手システムインテグレーター	各種OSS、事例多数



**流通 = ECサイト**

**金融 = ネットバンク、オンライントレード、ダイレクト損保**

**製造業 = ファンサイト、コミュニティサイト、直販サイト  
製品 × インターネット**

(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/>

## 大量トランザクション(リクエスト)の処理

## 大量のログデータ(行動履歴)の分析

## ビッグデータ

## 大量のコンピューティング・リソースを使用

## クラウドサービスの利用

(出所)Information By Schlüsselbein2007  
<http://www.flickr.com/photos/schluesselbein/4157426778/in/photostream/>

使用リソース(ノード、CPU)の増大

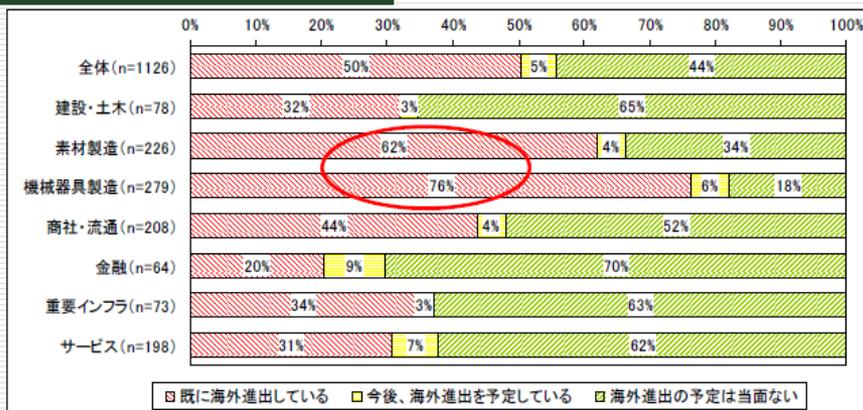
=ソフトウェア・ライセンス費用の増大

オープンソースの活用

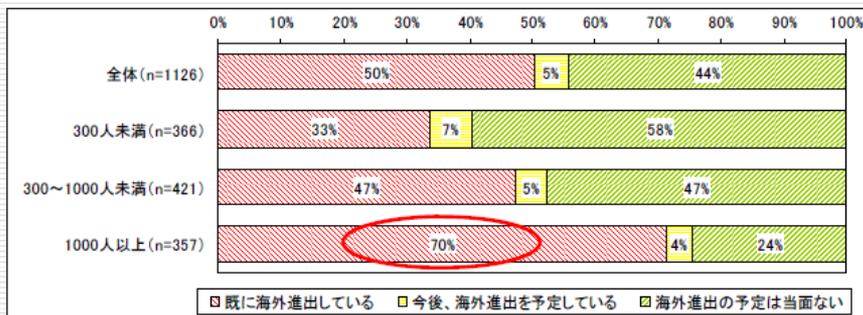
(出所)Red Arrows By peter pearson  
<http://www.flickr.com/photos/peterpearson/2682433551/>

＜大きく進展する企業のグローバル化＞ 重点は国内から海外市場へ  
 「素材製造」の6割、「機械器具製造」の4社に3社が、また大企業の7割  
 がすでに海外進出している実態が明らかに

業種グループ別  
 グローバル化の状況



企業規模別  
 グローバル化の状況

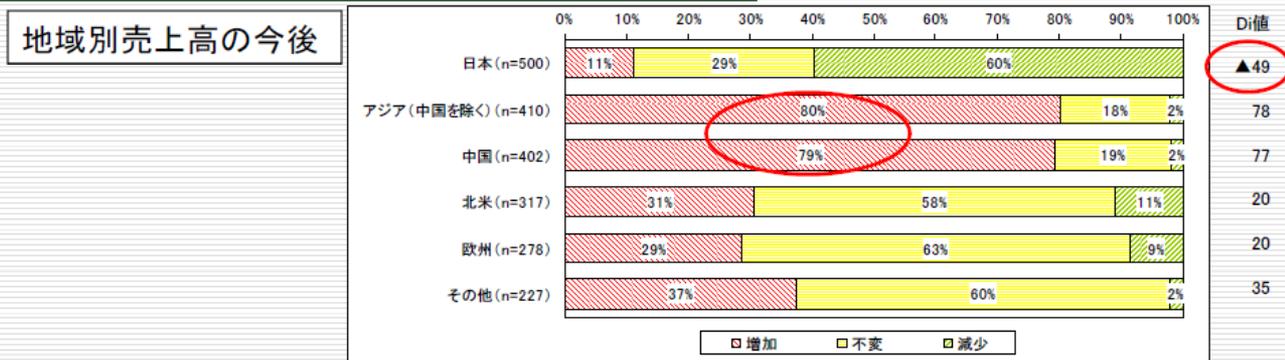


(C)JUAS 2011

16

(出所)JJUAS 第17回 企業IT動向調査2011(10年度調査)  
[http://www.juas.or.jp/servey/it11/it11\\_press\\_pp.pdf](http://www.juas.or.jp/servey/it11/it11_press_pp.pdf)

海外進出企業・進出予定企業は、国内市場での売上げが減少していく中、北米、欧州といった先進国市場での売上げは維持しつつ、アジア、中国、その他の新興国市場での売上げを増加させていく予定



<業種グループ別「地域別売上高の今後」のDI値>

- 「日本」: 「金融」▲73、「機械器具製造」▲63、「素材製造」▲57、「建設・土木」▲44、「重要インフラ」▲37、「商社・流通」▲24、「サービス」▲19
- 「中国」: 「素材製造」83、「商社・流通」82、「機械器具製造」77、「サービス」77、「建設・土木」62、「重要インフラ」57、「金融」56
- 「アジア(中国を除く)」: 「重要インフラ」87、「機械器具製造」82、「金融」79、「サービス」79、「素材製造」77、「商社・流通」76、「建設・土木」59

- ・特に「金融」や「製造業」では、国内市場の位置付けがますます小さくなるとする企業が多く見られる。
- ・かわって、「素材製造」では「中国」、「機械器具製造」では「アジア(中国を除く)」にシフトしていくとする企業が多い。
- ・同様に「商社・流通」では「中国」のウエイトが高まると見ている。
- ・また、「重要インフラ」が「アジア(中国を除く)」での成長を考えていることもうかがわれる。



(C)JUAS 2011

17

(出所)JUAS 第17回 企業IT動向調査2011(10年度調査)

[http://www.juas.or.jp/servey/it11/it11\\_press\\_pp.pdf](http://www.juas.or.jp/servey/it11/it11_press_pp.pdf)

## 情報システムのグローバル化

**グローバル規模での全体最適**

**グローバル・ビジネスのスピードアップ**

**サプライチェーン全体の品質向上**

**海外拠点のセキュリティ向上**

ユーザ数の増大(グローバル、取引先)

=ソフトウェア・ライセンス費用の増大

**オープンソースの活用**

(出所)Red Arrows By peter pearson  
<http://www.flickr.com/photos/peterpearson/2682433551/>

オープンソースを活用しないと、  
コンシューマにアプローチできない。

オープンソースを活用しないと、  
クラウドを十分に活用できない。

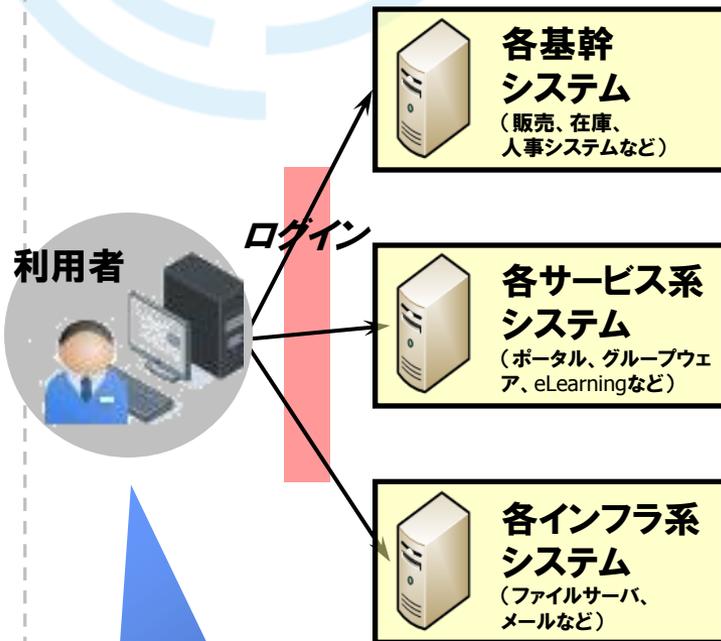
オープンソースを活用しないと、  
グローバルビジネスに対応できない。

- **グループ企業、グローバル企業**
- **クラウド(SaaS)、ASP利用者**
- **クラウド(SaaS)、ASP事業者**
- **モバイルPC・スマートフォン・タブレットPC活用企業**
- **既存のSSO・ID管理システムのリプレース**

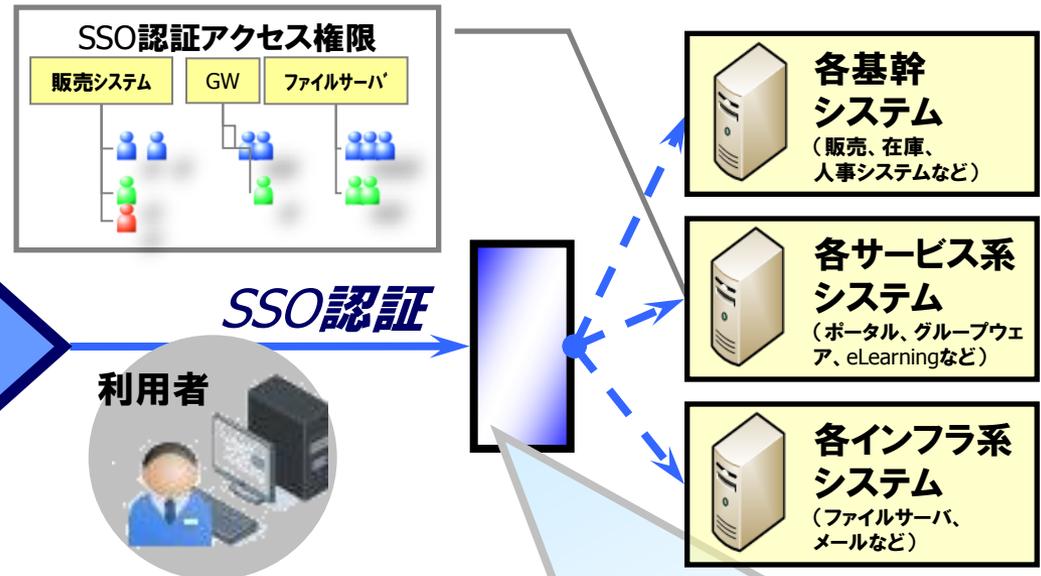
# シングルサインオンについて

- 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)



## To-Be(SSO導入後)

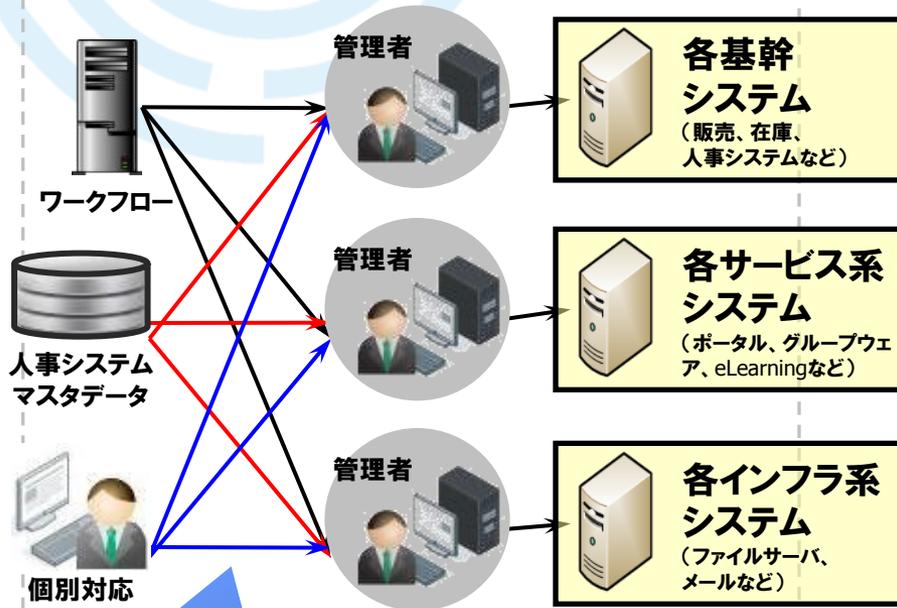


- アクセス権限付与に基づく厳密なアクセス制御
- セキュリティポリシーに基づいた厳密な認証インターフェース
- システムへのアクセスの認証の統合化による利便性向上
- アクセスログの一括取得
- 多様化する認証方式への対応
  - ✓ 対象システム : Web系システム、C/S系システム、OS...
  - ✓ 認証連携インターフェース : ID/PWD、生体認証、PKIなど

# ID管理について

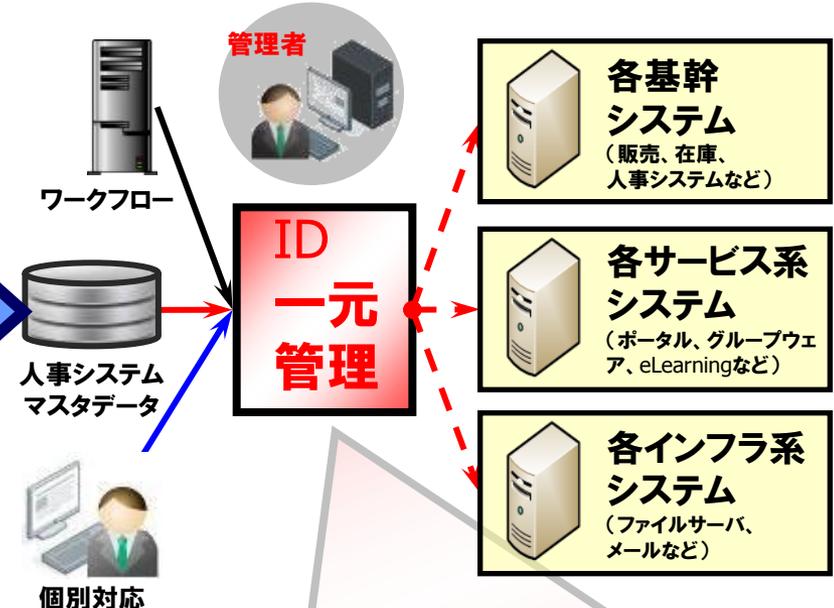
- 入社・退社・人事異動時に、利用システム毎のアカウントの個別ID管理(登録/修正/削除/参照)に対して、導入後は統合的に管理することにより、運用効率化・負担&ID管理ミス軽減となる

## 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

## 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

広がる情報システムの利用範囲

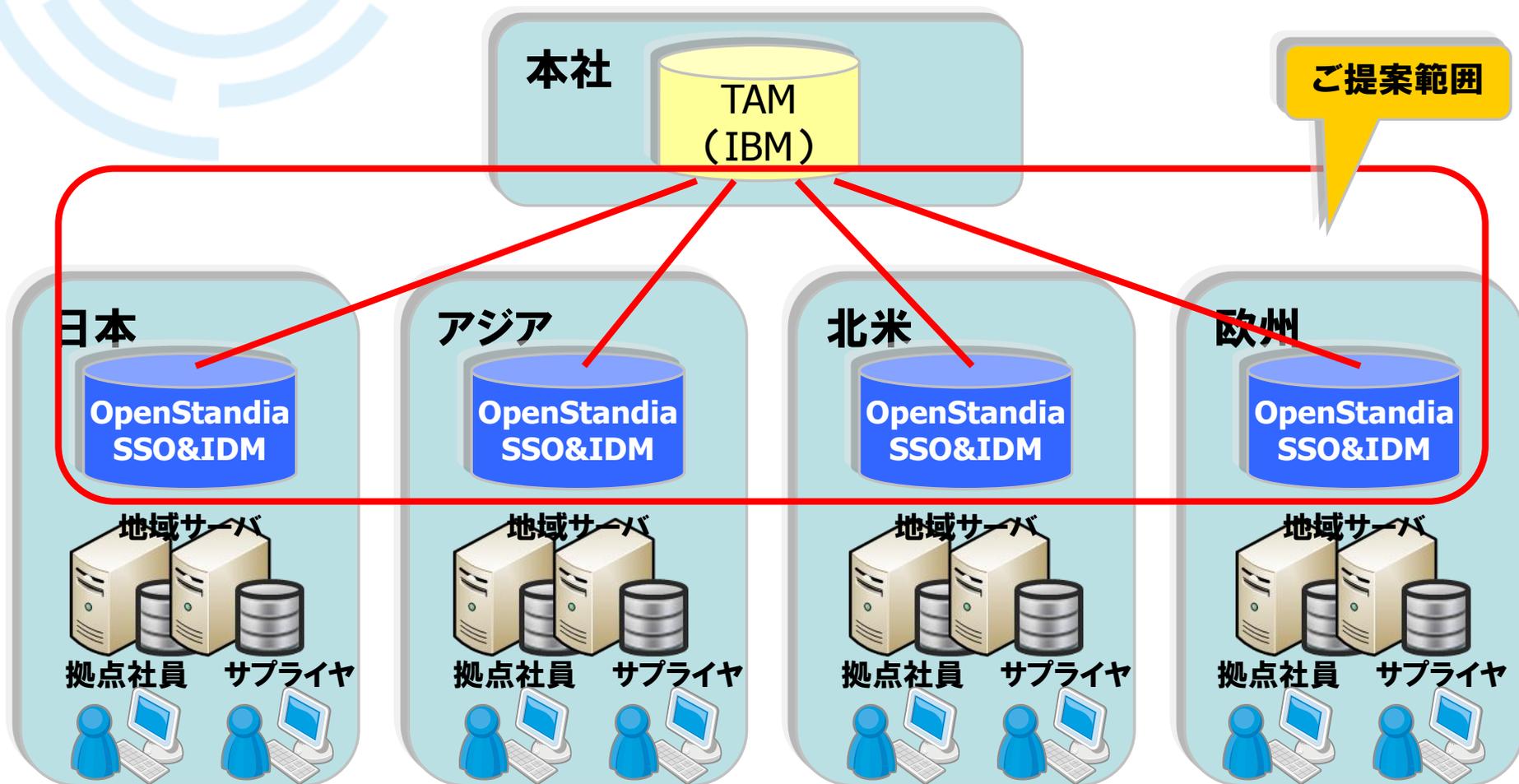


- 従来の部門内、会社という単位の情報システムの利用から、取引先、派遣社員、パートナー、グループ企業、グローバルなどへの範囲拡大
- グループ・グローバルでの人材活用(人材流通)を支えるID基盤

## 競争優位を実現する情報流通(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。



## 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

## ■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。

ユーザ数  
当初約3,000名  
今後グローバル展開

別途、10万人規模の事例  
もあり。  
(別の大手家電メーカー)

利用者



インターネット

SAML

SAML

## インターネット

SalesforceCRM

GoogleApps



## 社内ネットワーク

OpenAM

LDAP

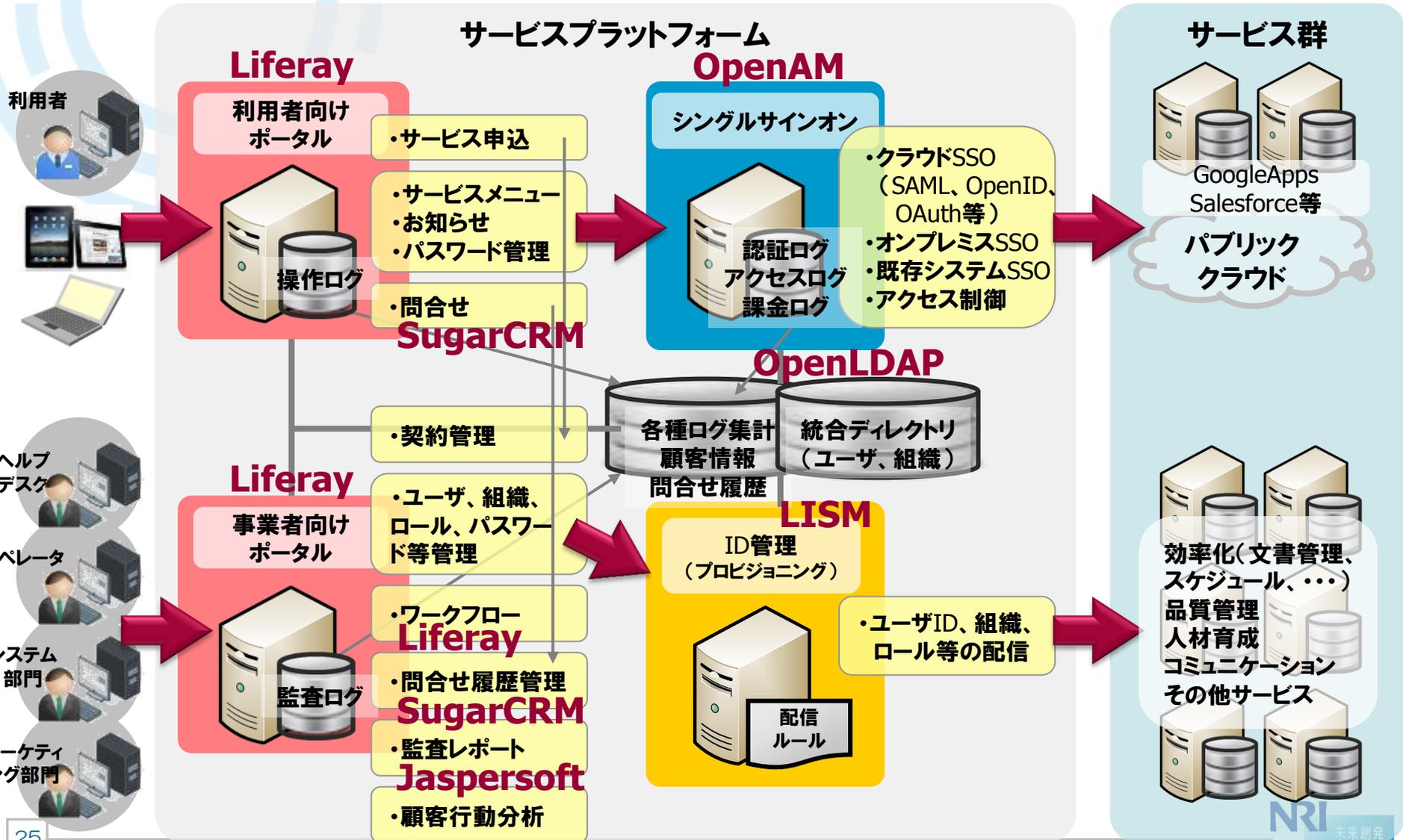
社内システム



## クラウド(SaaS)、ASP事業者

# (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



## 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



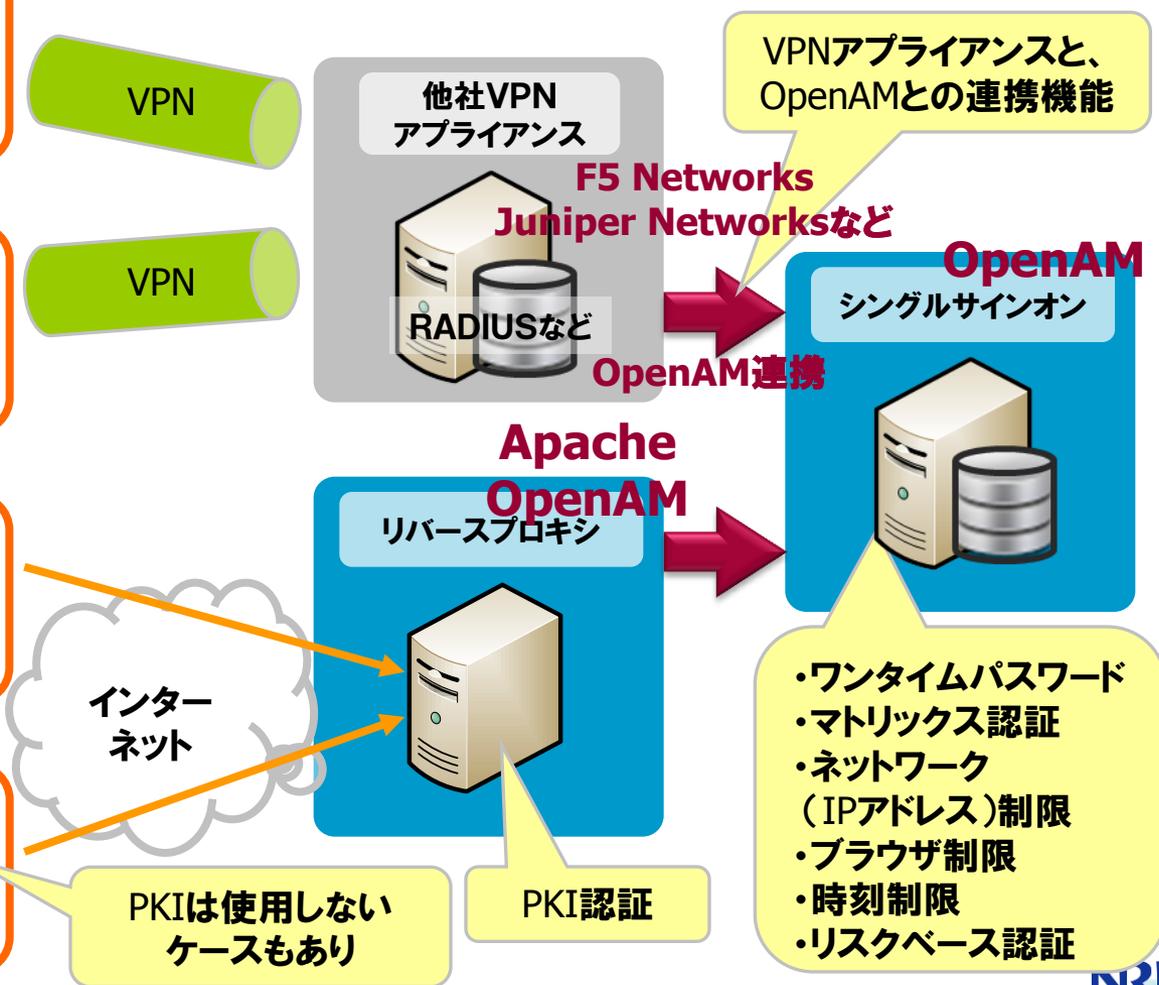
スマホ・タブレットからのアクセス



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



## 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 ▼

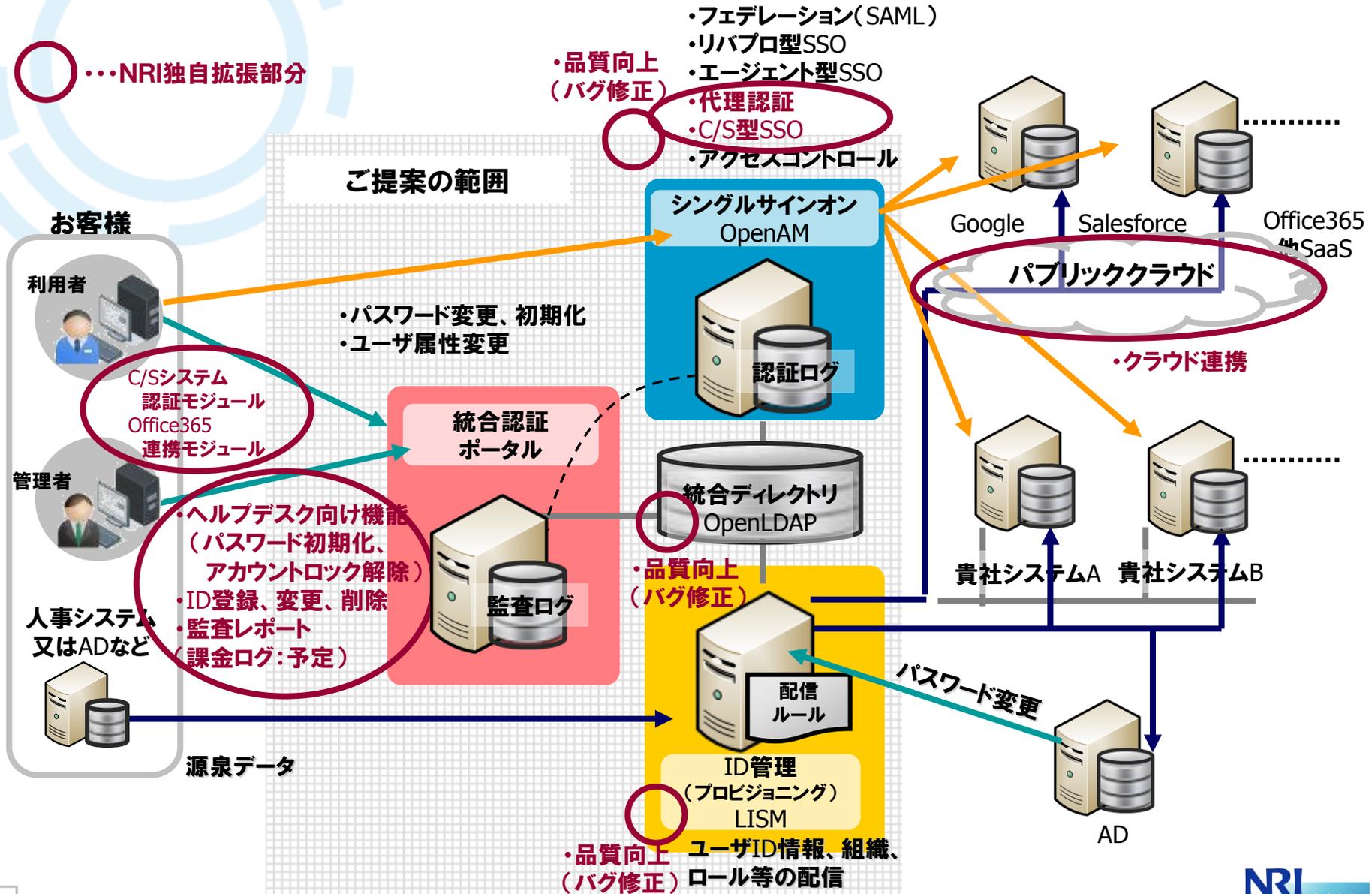
- **利用範囲の拡大(たとえば、グループ企業を対象に加える)により、大幅なユーザライセンス費用の増加が発生する。**
- **クラウドサービス連携のためにSAMLを使いたいが、別オプションであり、追加のライセンス費用が高額。**
- **現在の認証基盤が複雑で、維持管理ができない。**

# 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

# オープンソースを活用した統合認証基盤の概要図

○ ……NRI独自拡張部分



# NRI付加機能

## ● 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
- ・Office365とのSSO(予定)

#### 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

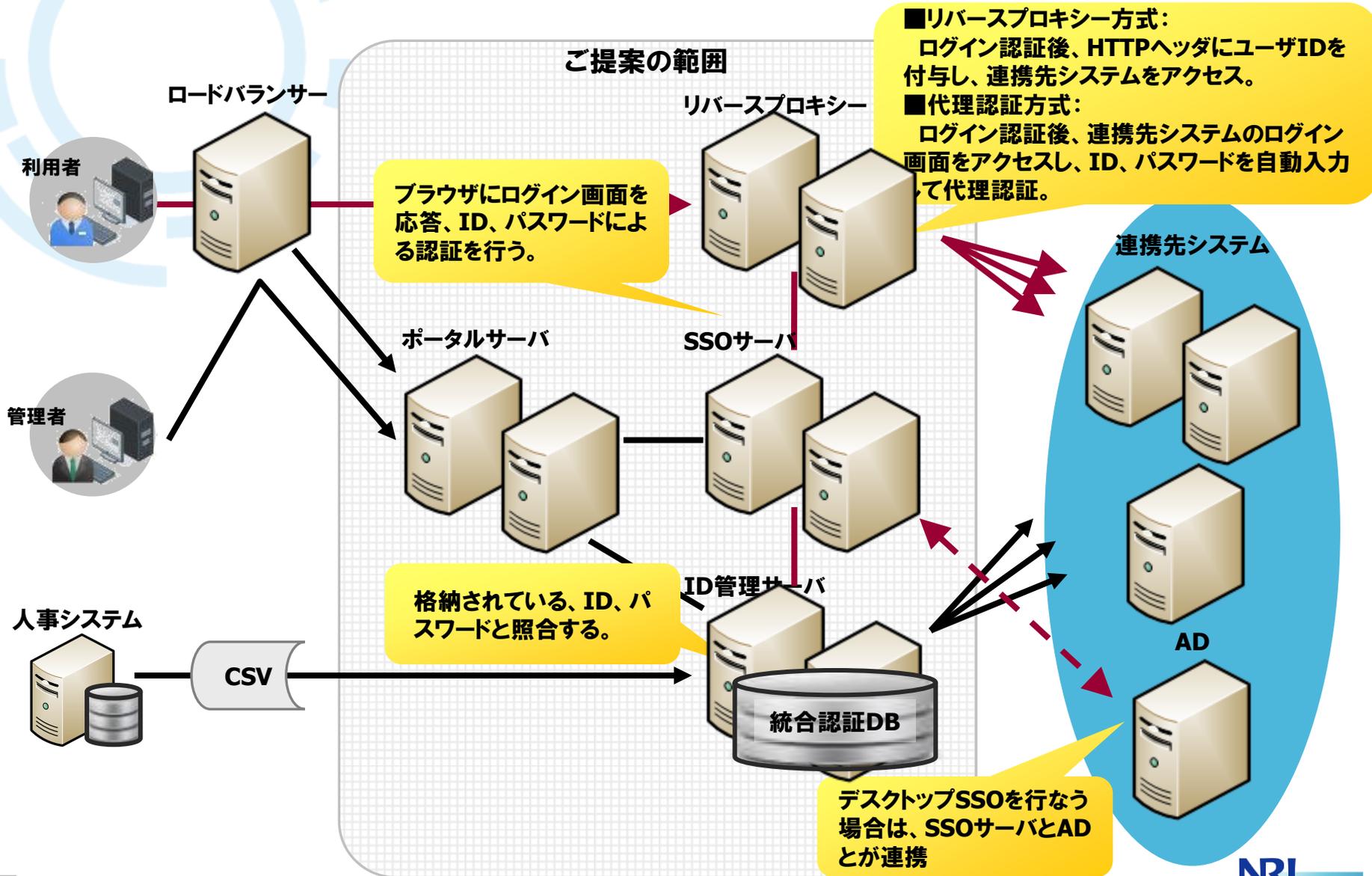


配信  
ルール

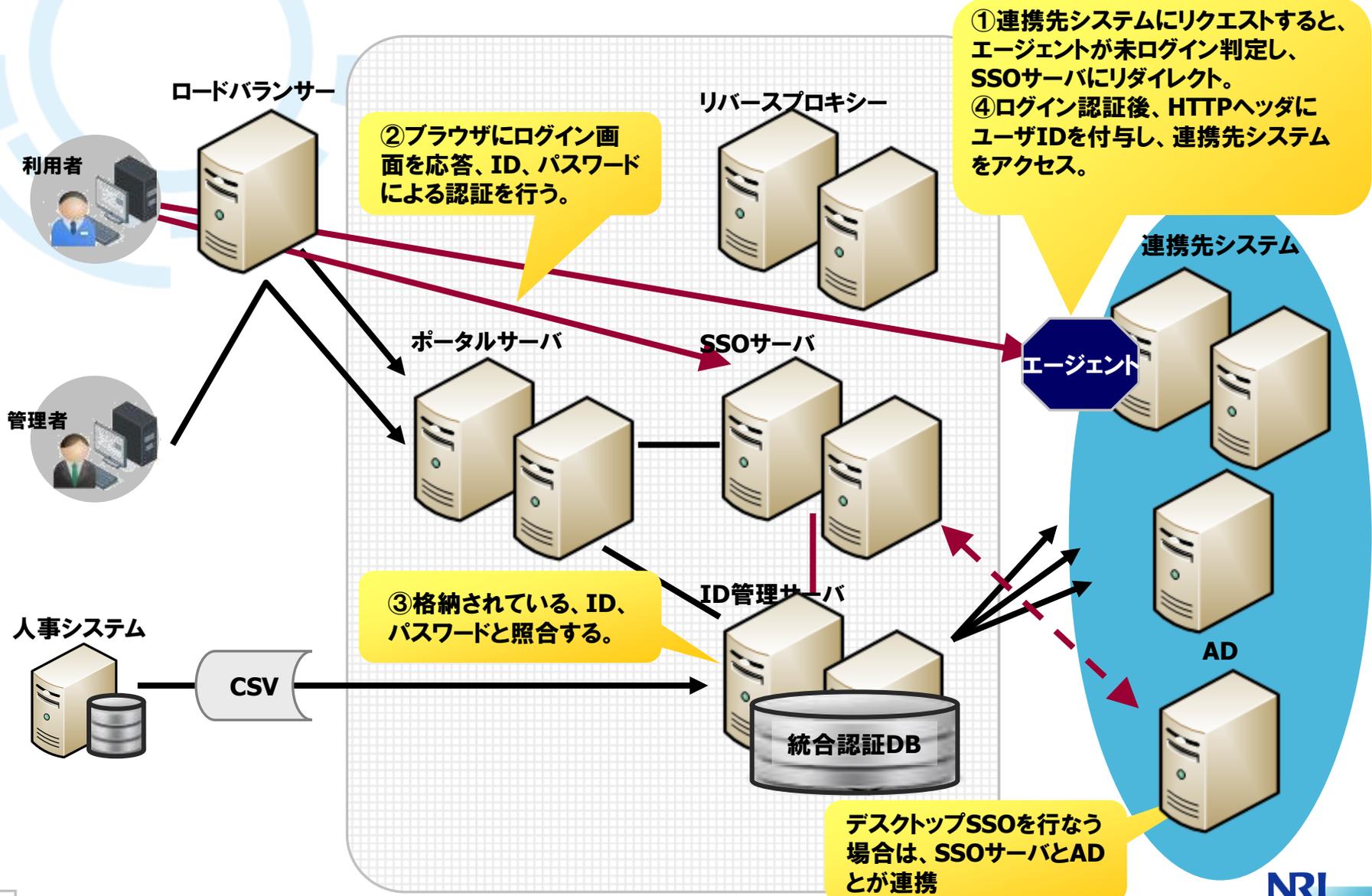
- ・プロビジョニング

ID管理  
(プロビジョニング)  
LISM

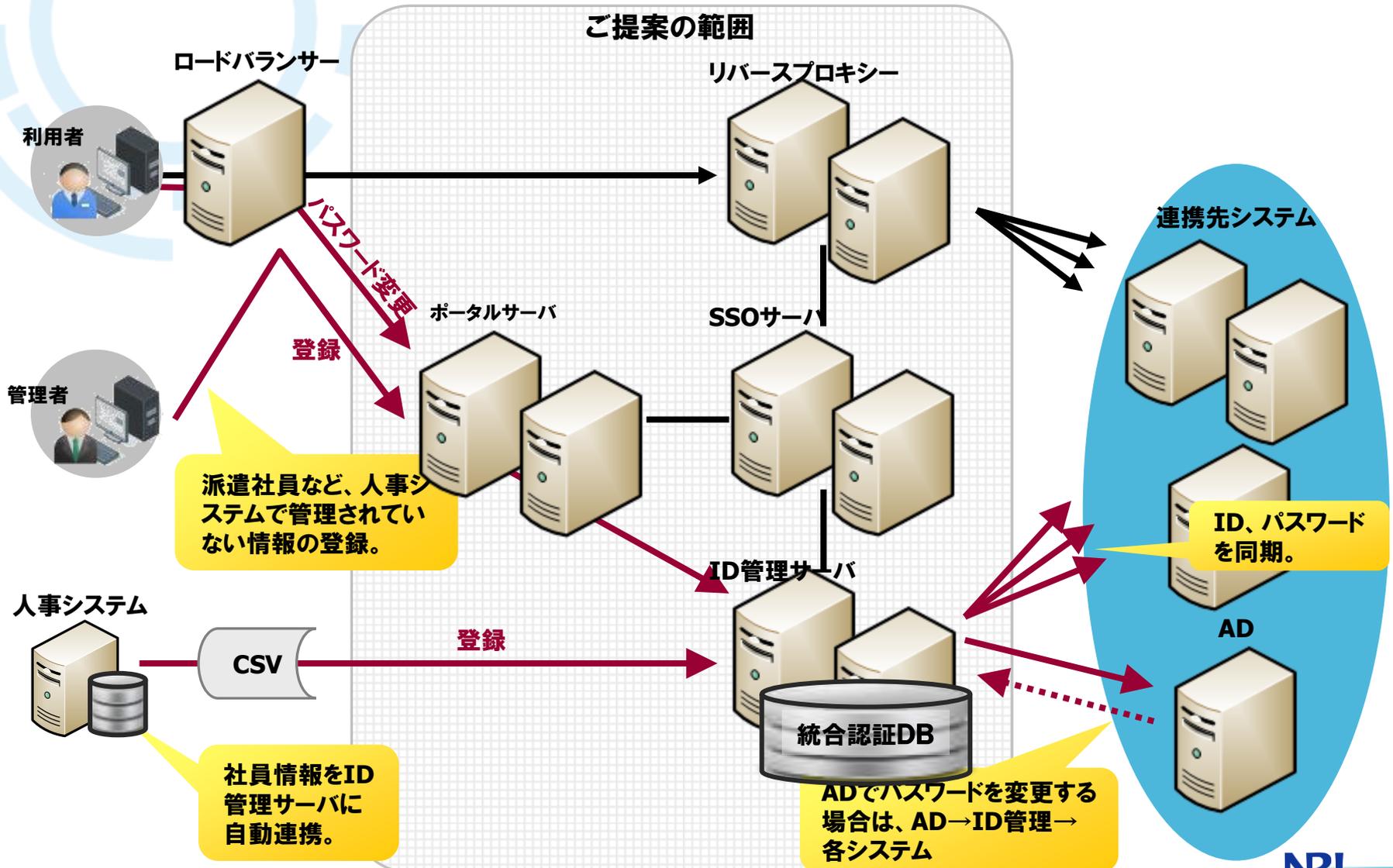
# リバースプロキシ、及び代理認証時の処理シーケンス概要



# エージェント型認証処理シーケンス概要

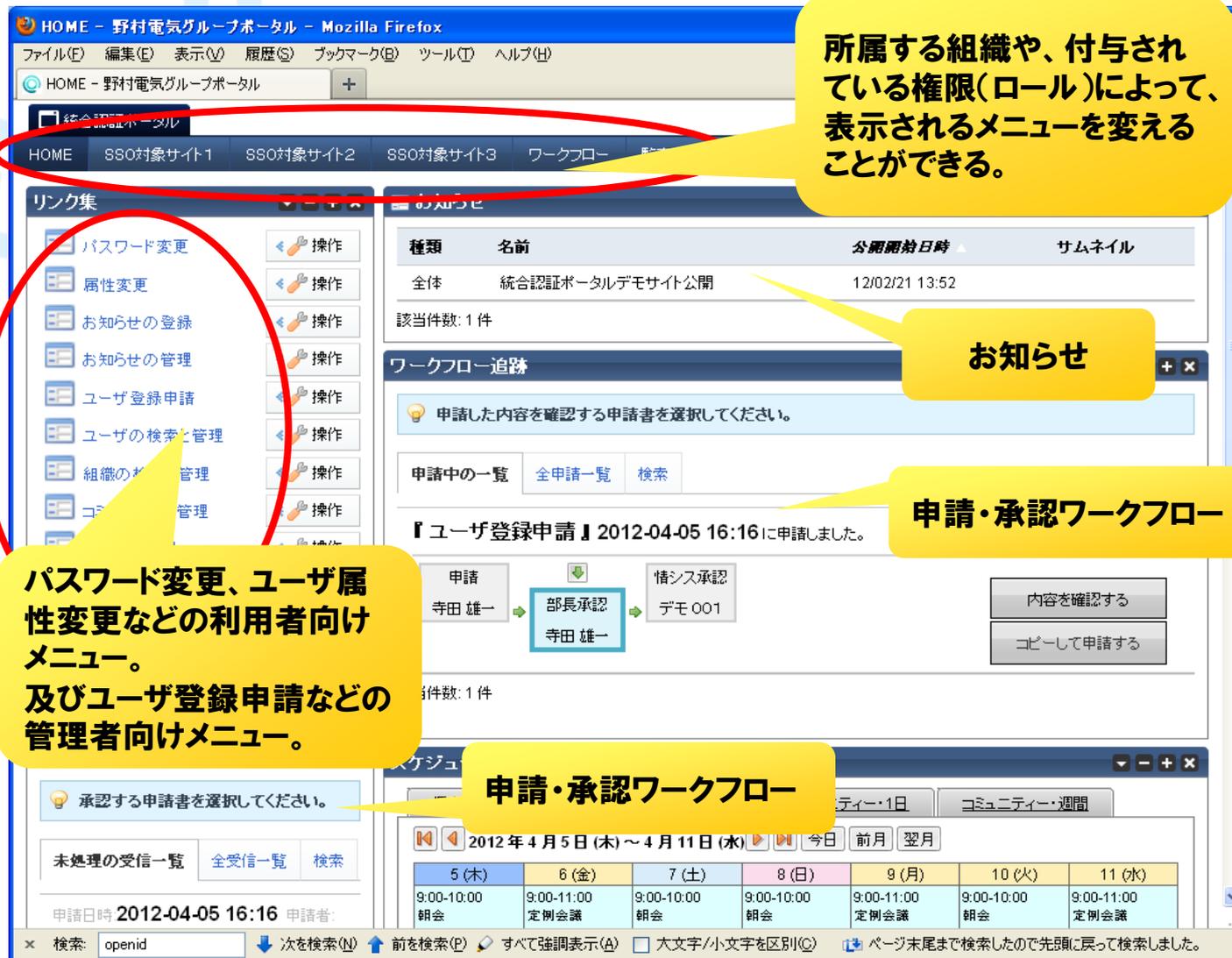


# ID管理(プロビジョニング)処理シーケンス



# 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



HOME - 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)

HOME - 野村電気グループポータル

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

**リンク集**

- 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
- ユーザの管理

**お知らせ**

種類	名前	公開開始日時	サムネイル
全体	統合認証ポータルデモサイト公開	12/02/21 13:52	

該当件数: 1件

**ワークフロー追跡**

申請した内容を確認する申請書を選択してください。

申請中の一覧 [全申請一覧](#) [検索](#)

【ユーザ登録申請】2012-04-05 16:16に申請しました。

申請: 寺田 雄一 → 部長承認: 寺田 雄一 → 情シス承認: デモ 001

内容を確認する  
コピーして申請する

申請・承認ワークフロー

承認する申請書を選択してください。

未処理の受信一覧 [全受信一覧](#) [検索](#)

申請日時: 2012-04-05 16:16 申請者:

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。

2012年4月5日(木)~4月11日(水)

5(木)	6(金)	7(土)	8(日)	9(月)	10(火)	11(水)
9:00-10:00 朝会	9:00-11:00 定例会議	9:00-10:00 朝会	9:00-10:00 朝会	9:00-11:00 定例会議	9:00-10:00 朝会	9:00-11:00 定例会議

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。

お知らせ

申請・承認ワークフロー

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。

申請・承認ワークフロー

## ● ユーザーの一覧

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

ポータル

ユーザー

組織  
コミュニケーション管理  
ユーザー

サーバー

サーバー管理者  
ポータルインスタンス

新規ユーザーの登録

ユーザー属性の追加

ユーザー一覧のCSVダウンロード

ユーザーの検索

複数ユーザーを選択してアカウントを停止

完全にユーザーを削除する場合は、一旦停止にしてから、削除する。

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	肩書き	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  ⓘ

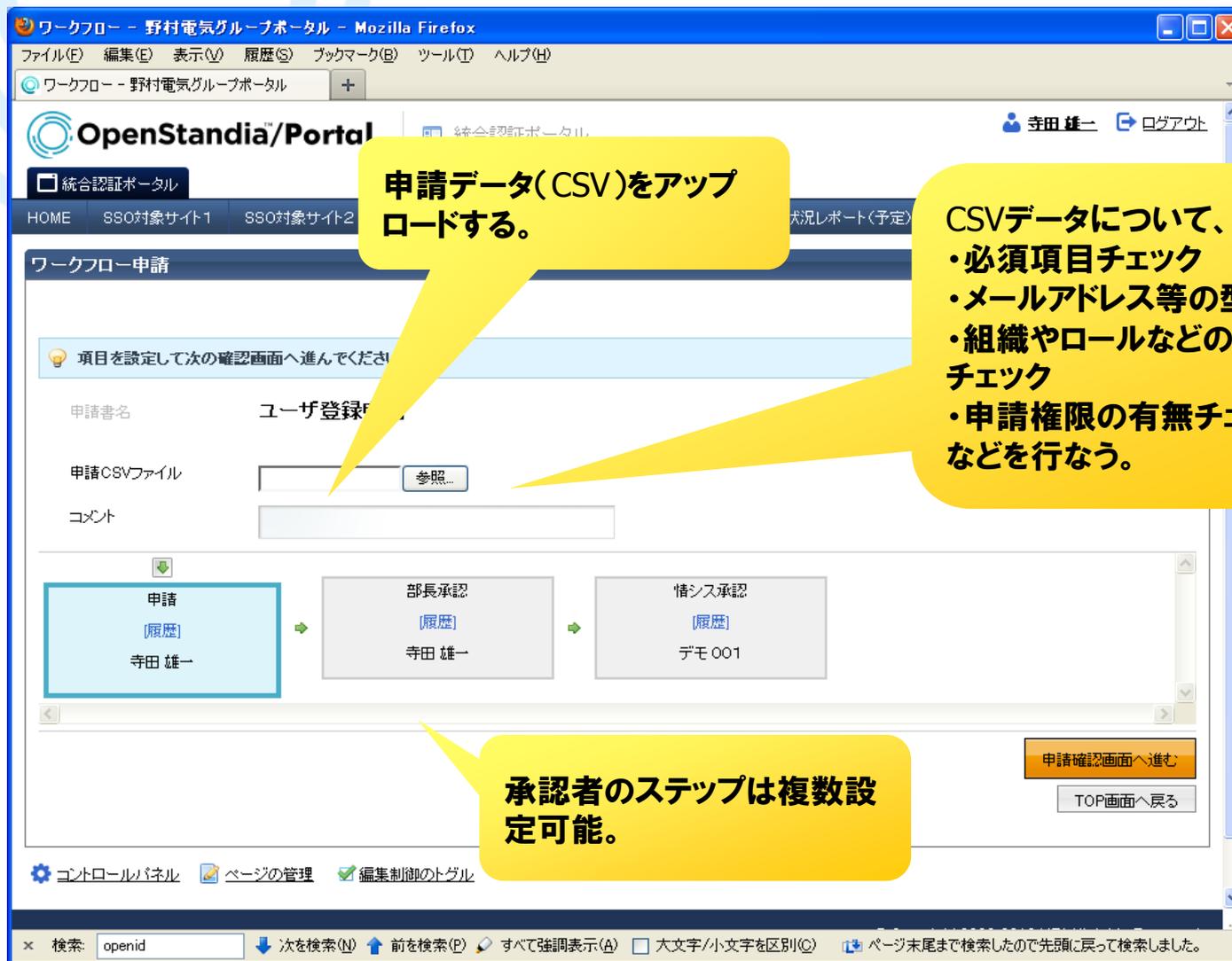
猶子回数  ⓘ

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 状況レポート(予定)

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

検索実行

time	Data	LoginID	ContextID	IPAddr	LogLevel	Domain
2011/03/22 17:23:57	Login Success[service StandardSSO	id=14,uFuser,dc=openesso,dc=java,dc=net	310830264a82805301	192.178.185.		
2011/03/22 17:23:57	Login Success[service StandardSSO	id=15,uFuser,dc=openesso,dc=java,dc=net	201908acc0110a4701	192.178.185.		
2011/03/22 17:23:57	Login Success[service StandardSSO	id=13,uFuser,dc=openesso,dc=java,dc=net	63a8e3d25f532b3301	192.178.185.		
2011/03/22 17:25:42	Login Success[service StandardSSO	id=15,uFuser,dc=openesso,dc=java,dc=net	f289ea37330a77f01	192.178.185.		
2011/03/22 17:25:42	Logout[service StandardSSO	id=14,uFuser,dc=openesso,dc=java,dc=net	335c0be0d...	192.178.185.		
2011/03/22 17:25:42	Logout[service StandardSSO	id=15,uFuser,dc=openesso,dc=java,dc=net	6eb821658da8d3ed01	192.178.185.217	INFO	dc=openesso, ...
2011/03/22 17:25:42	Login	id=15,uFuser,dc=openesso,dc=java,dc=net	28308af922ab20c01	192.178.185.217	INFO	dc=openesso, ...

「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。

最終ログイン日時	ユーザ名	権限	パスワード有効期限	アカウントロック
2011/03/24	Administrator	Administrator	2999/01/01	
2011/03/23	Administrator,Power User,管理職	営業部,製品開発部	2015/11/01	
2011/03/20	Power User	営業部	2011/08/01	
2012/11/15	Power User	製品開発部	2012/11/15	
2011/11/01	Power User	経理部	2011/11/01	
2011/11/01	Power User	野村販売(株)	2011/11/01	
2011/11/01	Power User	野村電気上海(工場)	2011/11/01	
2011/03/24	Power User,管理職	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	2011/11/01	

# その他の主な事例

#	時期	業種	提供ソリューション	ユーザ数	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	5,000 ～ 100,000	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(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	5,500 ～40,000	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数約3,000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
統合認証ポータル(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	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。			○	
3	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。			○	
4	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。			○	
5	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。			○	
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。			○	
統合認証ポータル(ヘルプデスク向け機能)						
7	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。			○	
8	組織、ロール(LDAPグループ)の作成、変更				○	
9	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。			○	
10	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			○	
11	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)			○	
12	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			○	
13	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			○	
14	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			○	
15	ユーザー検索機能	ユーザーを検索する。			○	
16	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。			○	
17	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。			○	
18	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。			○	
19	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
<b>申請・承認ワークフロー機能</b>						
20	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。			○	
21	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。			○	
22	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。			○	
23	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。			○	
<b>監査レポート機能</b>						
24	監査ログ	監査レポート。			○	
25	ユーザーアカウント一覧	監査レポート。			○	
26	管理者権限ユーザーアカウント一覧	監査レポート。			○	
27	申請承認イベント一覧	監査レポート。			○	
28	特定ユーザー認証成功/失敗イベント一覧	監査レポート。			○	
29	特定システム認証成功/失敗イベント一覧	監査レポート。			○	
30	長期間未ログインユーザー一覧	監査レポート。			○	
31	パスワード有効期限切れユーザー一覧	監査レポート。			○	
32	アカウントロックユーザー一覧	監査レポート。			○	
33	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	
34	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	OpenAM	Open LDAP	NRI 独自拡張	LISM
認証・シングルサインオン						
35	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。	○			
36	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。	○			
37	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。			○	
38	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。	○			
39	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	
40	SalesforceCRM、GoogleAppsなど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。	○			
41	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			
42	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			
43	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	○			
44	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。	○			
45	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。	○			
46	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	OpenAM	Open LDAP	NRI 独自拡張	LISM
<b>ID管理、プロビジョニング</b>						
47	源泉データの取り込み	CSVによる源泉データの取り込み				○
48	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。				○
49	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
50	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
51	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
52	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				○
53	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
54	パスワードの暗号化	パスワードの暗号化		○		
55	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		○		
56	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）		○		

## オープンソース、徹底活用への3ステップ

- プロジェクト単位に、オープンソースを導入。

## ユーザ企業

### ○×業務システム



商用WebAP  
商用フレーム  
ワーク  
商用DBMS

### ○×業務システム



商用WebAP  
商用フレーム  
ワーク  
商用DBMS

### ○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

**有償サポート**

**年間〇〇円×n台**



**OSSサポートベンダー**

- 全社的に、オープンソースを導入。

## ユーザ企業

○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

**有償サポート**

**年間〇〇円で、包括サポート  
サーバ台数、CPU数無制限**

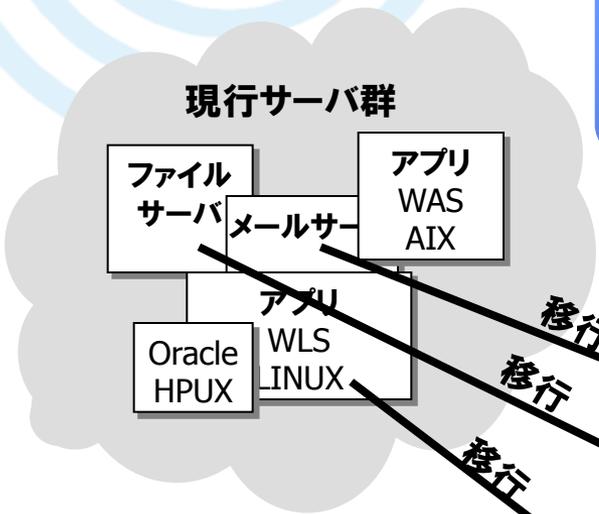
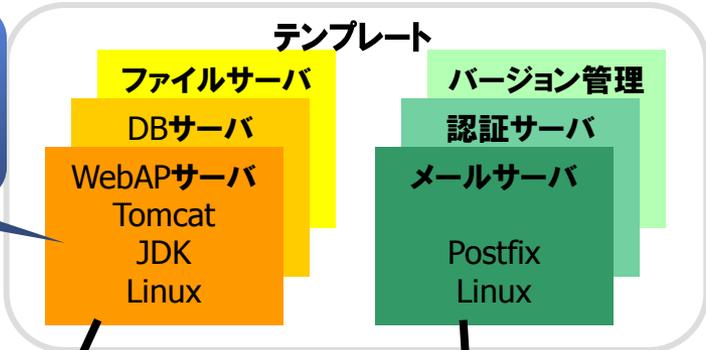


**OSSサポートベンダー**

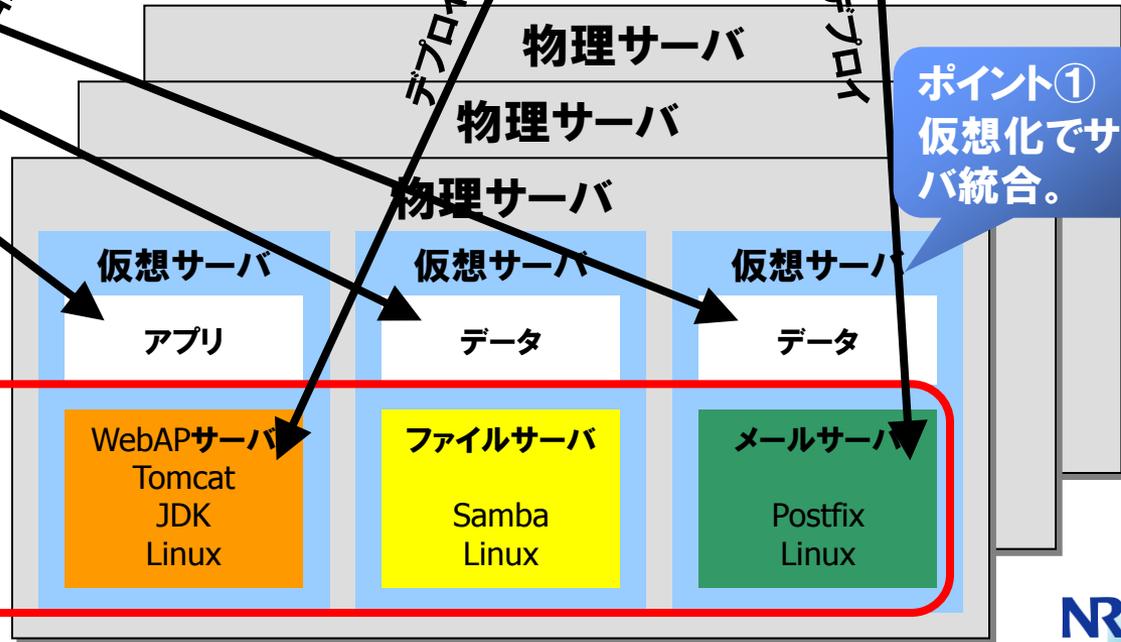
# (事例)550台サーバ統合 & セキュリティ強化

@ITで紹介されました。 <http://www.atmarkit.co.jp/flinux/reasai/tco03/tco03a.html>

ポイント②  
基盤(OS+ミドル)の  
テンプレート化



ポイント①  
仮想化でサーバ  
統合。



ポイント③  
運用、セキュリティの標準化

統合ID管理・アクセス制御  
 統合システム運用  
 統合バックアップ

## NEWS RELEASE

クラウド環境向けオープンソース・サポートサービスの新メニューを提供開始

～仮想サーバ数が多い場合や複数システムが稼働する環境でコスト削減を可能に～

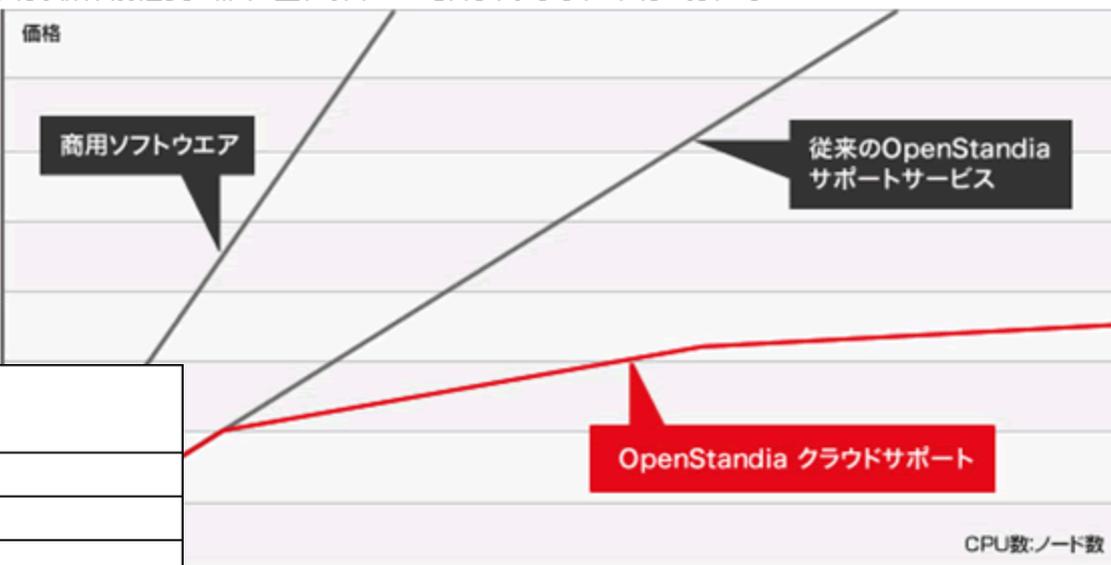
2012年7月12日

株式会社野村総合研究所

株式会社野村総合研究所(本社:東京都千代田区、代表取締役社長:嶋本 正、以下「NRI」)は、クラウド環境において

オープンソース・ソフトウェアを利用する企業向けの、新しいパブリッククラウドやプライベートクラウド上に、情報システムを構築することで、ハードウェアのコストは削減できても、ソフトウェアのコストが高額になるケースが多いのが実情です。

NRIでは、オープンソース・ワンストップサポートサービスに適した新たなサービスメニュー「OpenStandiaクラウドサポート」は、このサービスを使うことにより、ソフトウェアコストを削減



	年間サポート費用(税別)			単位
	Apache	Tomcat	JBossAS	
1～16CORE	45	25	60	万円
17～32CORE	90	45	120	万円
33～48CORE	135	70	180	万円
49～128CORE	1.5	0.8	2	万円/1COREあたり
129～256CORE	1.1	0.6	1.5	万円/1COREあたり
257CORE以上	0.75	0.4	1	万円/1COREあたり

- 自社エンジニアで、オープンソースをサポート。

## ユーザ企業

○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

○×業務システム



Apache  
Tomcat  
Struts  
PostgreSQL

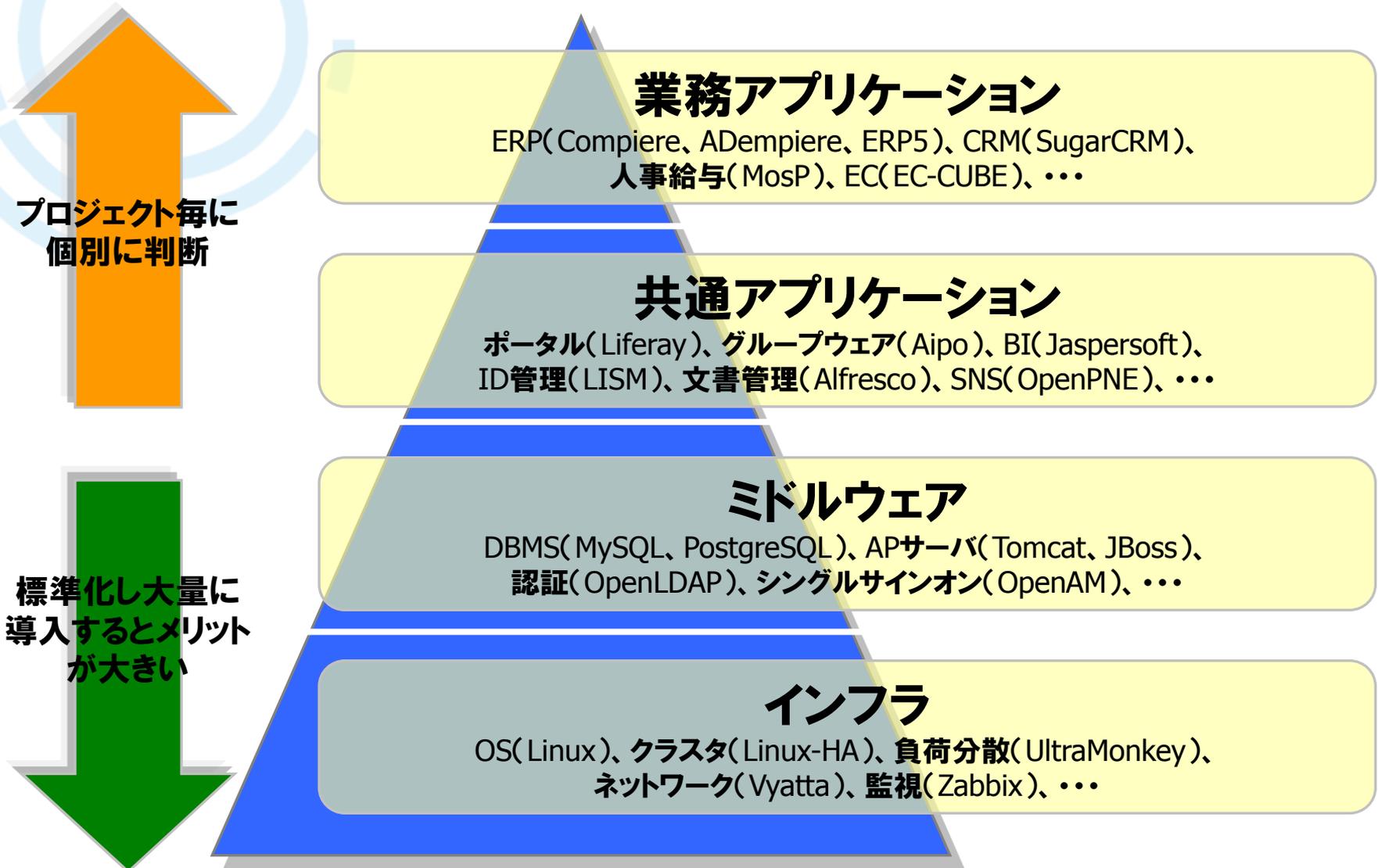
社内サポート

社内サポート

社内サポート

OSS専門組織

OSSサポートベンダー



## オープンソースは重要な社会インフラ

オープンソースを使わずして、  
ビジネスの成功はあり得ない。

ステップ2、3のオープンソースの活用

**NRI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/>