

2014 OpenAM Conference

野村総合研究所が手掛けるエンタープライズ 最新事例とOpenAM最新動向

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
高橋 雅人



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推進室

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

オープンソースまるごと



アジェンダ

1. 野村総合研究所のご紹介
2. OpenStandiaのご紹介
3. SSO/IDMに求められる解決すべき業務課題
4. 業務課題解決事例紹介
5. 今後のOpenAMに求められる要件
6. OpenAM普及に向けたOpenStandiaの取り組み

アジェンダ

1. 野村総合研究所のご紹介

2. OpenStandiaのご紹介

3. SSO/IDMに求められる解決すべき業務課題

4. 業務課題解決事例紹介

5. 今後のOpenAMに求められる要件

6. OpenAM普及に向けたOpenStandiaの取り組み

アジェンダ

1. 野村総合研究所のご紹介

2. OpenStandiaのご紹介

3. SSO/IDMに求められる解決すべき業務課題

4. 業務課題解決事例紹介

5. 今後のOpenAMに求められる要件

6. OpenAM普及に向けたOpenStandiaの取り組み

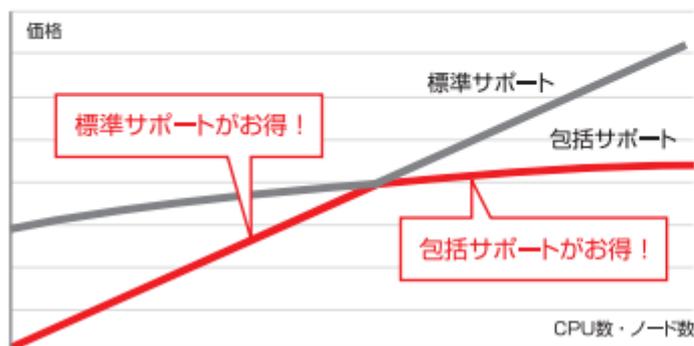
OpenStandiaのご紹介

OpenStandia(オープスタンディア)の特徴

- ✓ 約50種類のオープンソースを、**ワンストップ**でサポートします。
- ✓ **過去バージョン**もサポートします。現在お使いのオープンソースをそのままサポートします。
- ✓ 大手企業エンタープライズシステムへの**導入実績が豊富**です。

オープンソース包括サポート

全社でのOSS利用、大量サーバでのOSS利用は、**包括サポート**がお得です。



以下のようなお客様には、CPU数、ノード数にリンクしない、包括的なサポートをご提供します。

全社で標準的に OSS を活用する

クラウドサービスで大量ノードで OSS を活用する

その他、たくさん OSS を活用されるお客様

詳細はお問い合わせ下さい

OpenStandiaのご紹介

http://openstandia.jp

オープンソースまるごと [サイトマップ](#) | [サイト内検索](#) 

 **OpenStandia™**
Open Source Technology

[お問い合わせ](#) [資料請求](#) [メールマガジン配信](#)   [お電話でのお問い合わせはこちら](#)
045-335-9538

[オープンソースとは](#) | [サービス・ソリューション](#) | [OSS紹介](#) | [導入成功事例](#) | [セミナー・イベント](#) | [パートナー](#)


Single Sign-On Identity Manager

OpenAM
ソリューション

**シングルサインオン
統合ID管理を
オープンソースで実現**

オープンソース統合業務ソリューション
OpenStandia/ERP™

「パッケージに業務を合わせる」ではなく、
**貴社の強みである”業務”
にパッケージを合わせる**

これまでのERPの
常識を覆す新しい導入方法


OSS紹介
無料でアクセスできる
OSS最新情報!

導入成功事例


最新事例資料
無料配布中!

さあ
OSSを
導入しよう

OSS
導入サービス

対象OSS約50種類
24時間365日


安心のOSS年間
サポートサービス

 **Alfresco™**

クラウド連携による
新しい情報共有と活用の実現


オープンスタンディア
セミナー・イベント情報

サービス・ソリューション オープンソースのことならOpenStandiaにおまかせください! [» サービス・ソリューション詳細はこちら](#)

 **オープンソースを
導入したい**  **オープンソースの
年間サポートを受けたい**  **オープンソースを使って
低コストで課題を解決したい**

アジェンダ

1. 野村総合研究所のご紹介

2. OpenStandiaのご紹介

3. SSO/IDMに求められる解決すべき業務課題

4. 業務課題解決事例紹介

5. 今後のOpenAMに求められる要件

6. OpenAM普及に向けたOpenStandiaの取り組み

業務課題～システム利用の効率化、運用コスト低減

- 社内環境の変化、IT環境の変化、事業環境の変化に関連する業務課題

環境の変化

課題

社内環境の変化

- ① 乱立するシステム、ユーザアカウント
- ② 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

- ③ SaaSの利用
- ④ クラウド基盤の利用
- ⑤ スマートフォン、タブレットの利用

事業環境の変化

- ⑥ グループ企業間、グローバル規模での情報システム共有
- ⑦ 企業合併、社内認証基盤統合、サービス統合
- ⑧ 利用者(ID)の増大

SSO/IDMが解決する業務課題の対象領域

SSO

IDM

- ③ SaaSの利用
- ⑤ スマートフォン、タブレットの利用
- ⑥ グループ企業間、グローバル規模での情報システム共有
- ② 内部統制、コンプライアンス強化、個人情報保護
- ④ クラウド基盤の利用
- ⑦ 企業合併、社内認証基盤統合、サービス統合
- ⑧ 利用者 (ID) の増大
- ① 乱立するシステム、ユーザアカウント

アジェンダ

1. 野村総合研究所のご紹介

2. OpenStandiaのご紹介

3. SSO/IDMに求められる解決すべき業務課題

4. 業務課題解決事例紹介

5. 今後のOpenAMに求められる要件

6. OpenAM普及に向けたOpenStandiaの取り組み

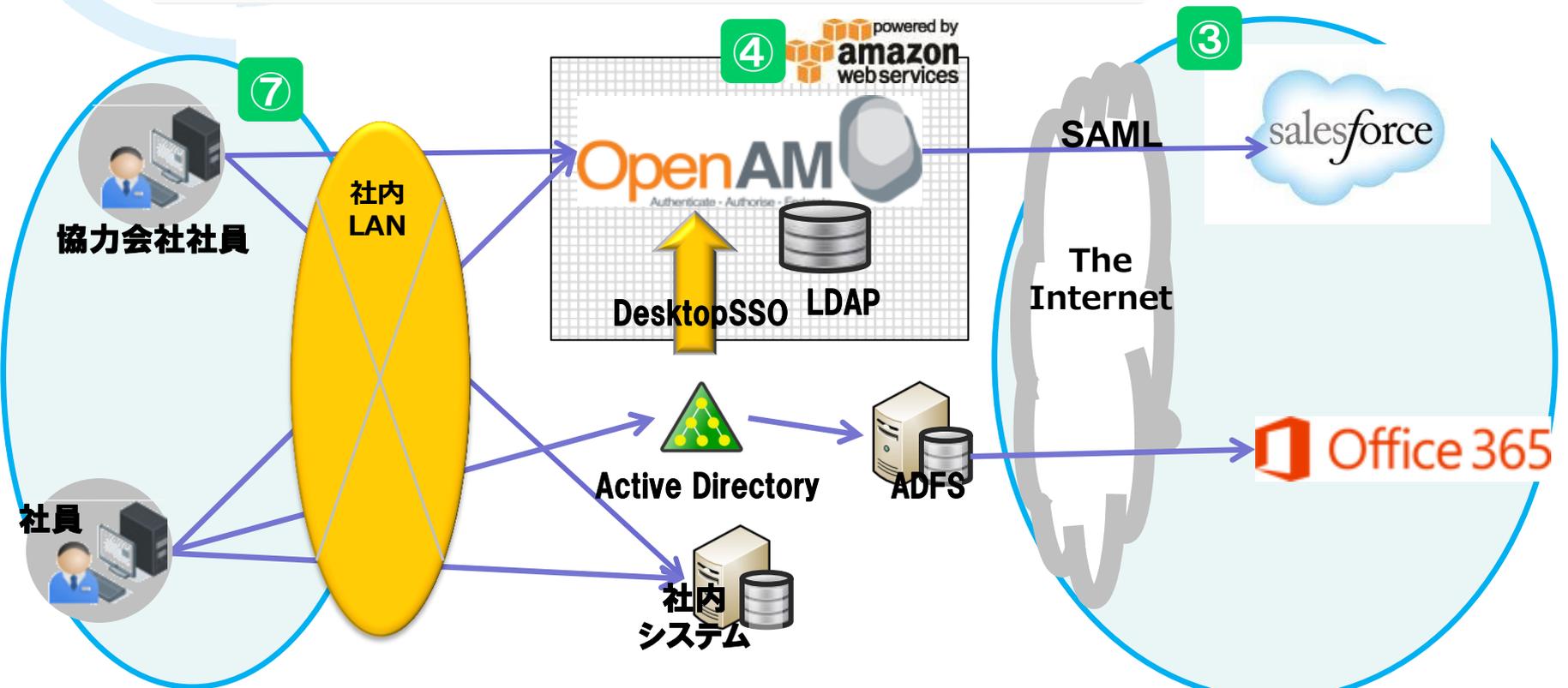
業務課題解決事例紹介

環境の変化	課題	事例1	事例2	事例3	事例4
社内環境の変化	① 乱立するシステム、ユーザアカウント		○		
	② 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	③ SaaSの利用	○			
	④ クラウド基盤の利用	○			
	⑤ スマートフォン、タブレットの利用		○		
事業環境の変化	⑥ グループ企業間、グローバル規模での情報システム共有				○
	⑦ 企業合併、社内認証基盤統合、サービス統合	○			○
	⑧ 利用者 (ID) の増大		○		

事例1. 大手不動産会社様 社内システムとSaaSのSSO連携

解決する課題

- ③ SaaSの利用
- ④ クラウド基盤の利用
- ⑦ 企業合併、社内認証基盤統合、サービス統合



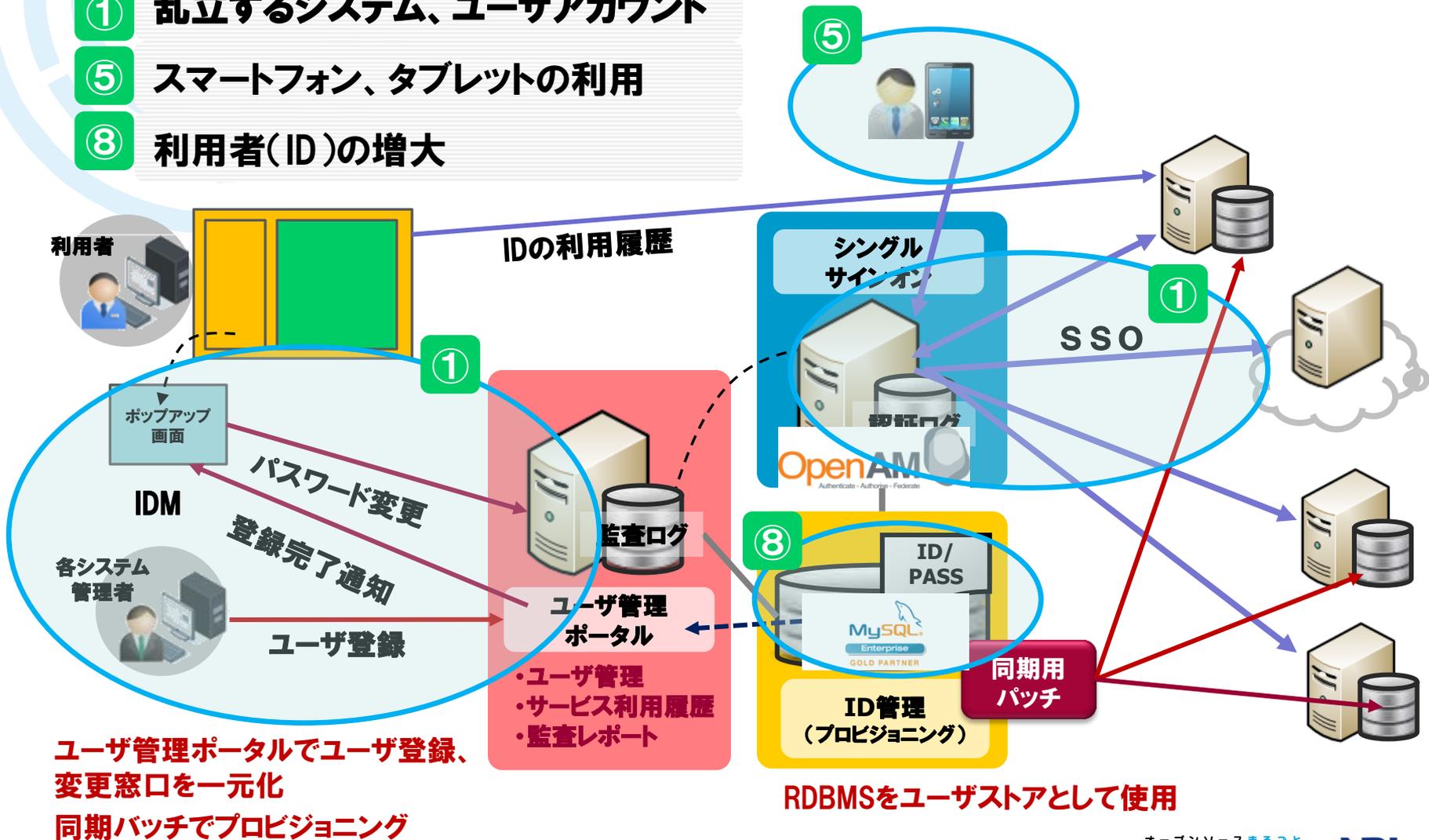
社員と協力会社社員の認証を統合

事例2.

資格試験サイト様 数百万ユーザのシングルサインオン

解決する課題

- ① 乱立するシステム、ユーザアカウント
- ⑤ スマートフォン、タブレットの利用
- ⑧ 利用者(ID)の増大



ユーザ管理ポータルでユーザ登録、
変更窓口を一元化

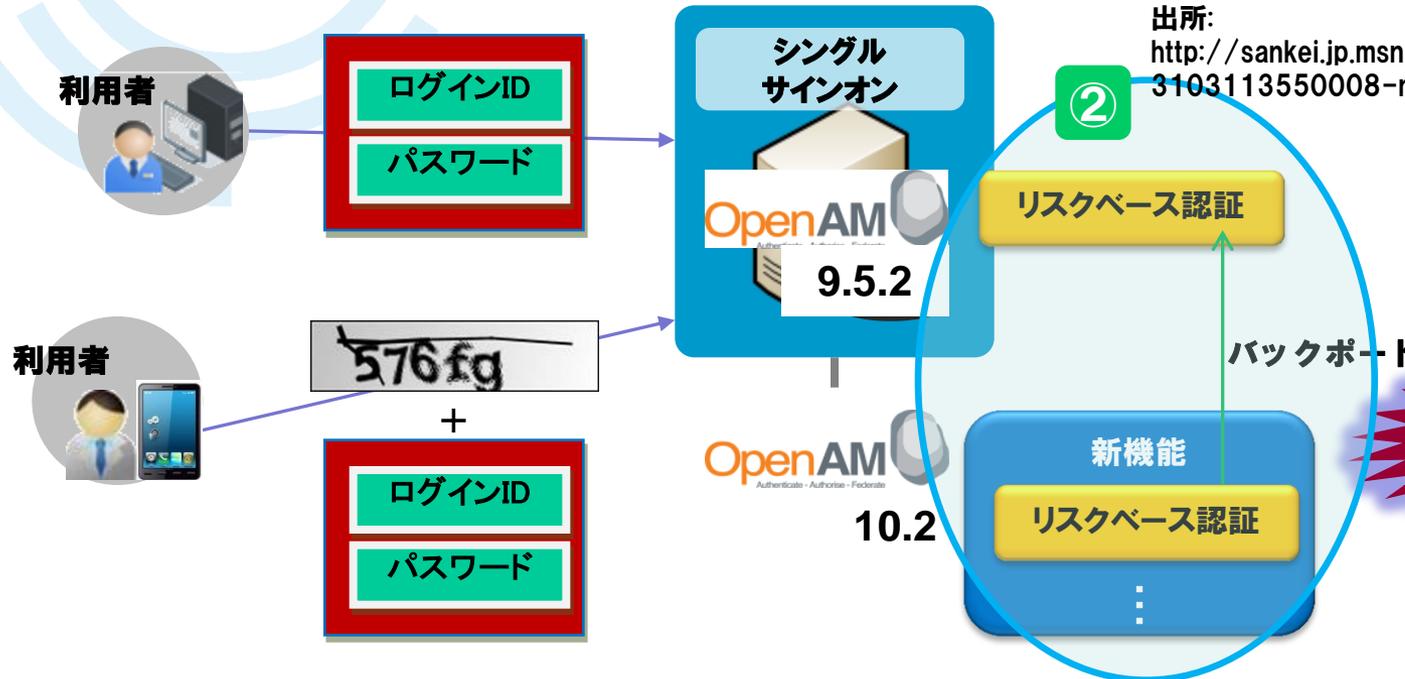
同期バッチでプロビジョニング

RDBMSをユーザストアとして使用

事例3. 資格試験サイト様 リスクベース認証によるセキュリティ強化

解決する課題

② 内部統制、コンプライアンス強化、個人情報保護



元上司のID使って不正アクセス、大阪市職員を懲戒
免職 税証明書偽造も

2013.10.31 13:53 【ネット犯罪】

大阪市は31日、元上司のIDを使って大阪役所のネットワークへの侵入を繰り返して、不正アクセス禁止法違反の罪で略式命令を受けた建設局の西野和晃職員(32)を懲戒免職にした。

出所:

<http://sankei.jp.msn.com/affairs/news/131031/crm13103113550008-n1.htm>

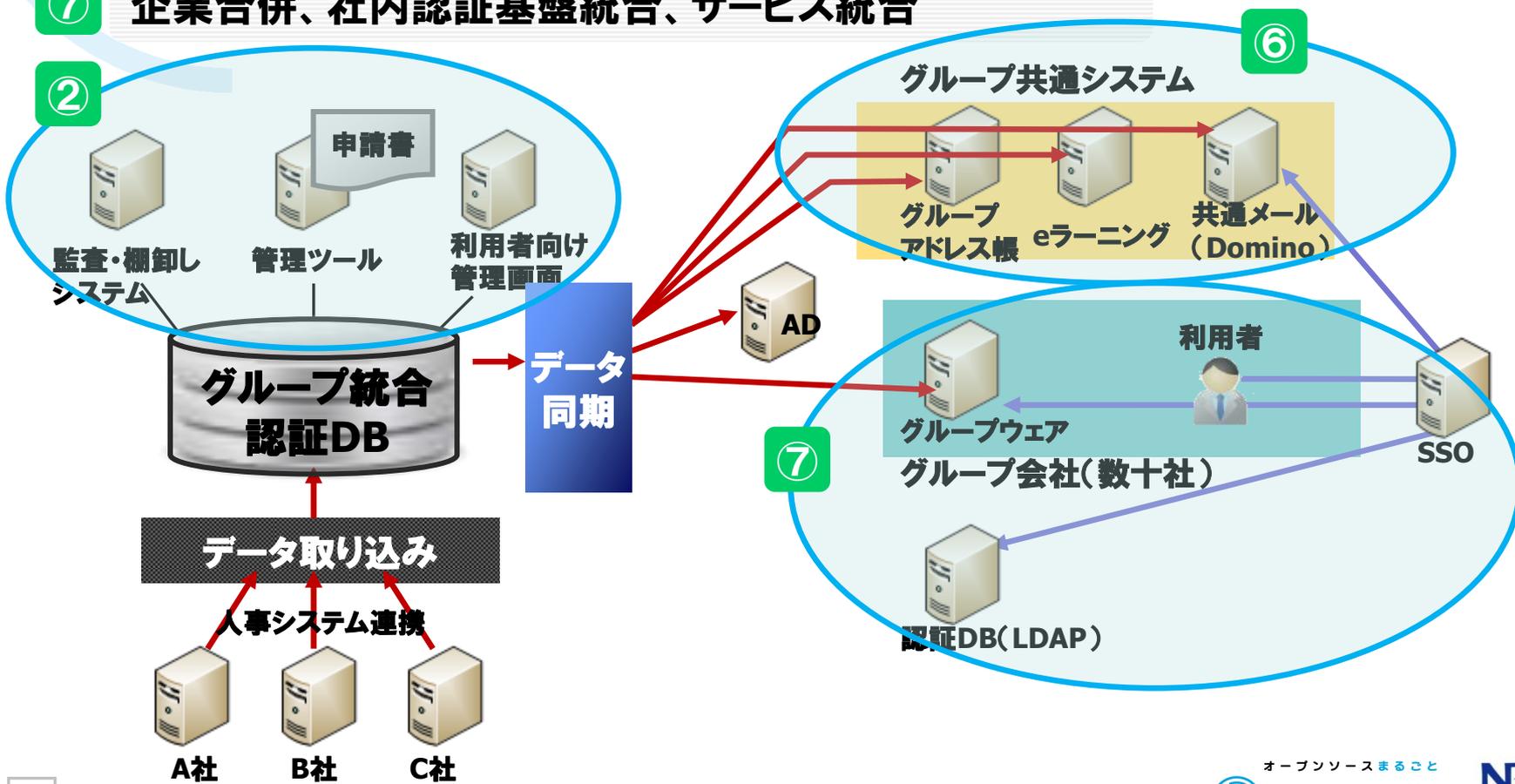
「ユーザストアの大規模化」で紹介した顧客のシステムに対してOpenAMの最新版(当時は10.2)で追加されたリスクベース認証機能を追加。

- 認証履歴に無いIPアドレスや端末からのアクセスされた場合、通常のID/パスワードに加えて画による認証を行うことでセキュリティを強化。
- リリース済みのシステムであり、機能追加にあたってはバージョンアップの影響範囲が懸念された。ver10.2から該当機能部分のソースを抽出し、ver9.5.2にバックポートすることで、影響範囲を極小化した。

事例4. 大手グループ企業(ホールディングス)統合認証基盤

解決する課題

- ② 内部統制、コンプライアンス強化、個人情報保護
- ⑥ グループ企業間、グローバル規模での情報システム共有
- ⑦ 企業合併、社内認証基盤統合、サービス統合



アジェンダ

1. 野村総合研究所のご紹介

2. OpenStandiaのご紹介

3. SSO/IDMに求められる解決すべき業務課題

4. 業務課題解決事例紹介

5. 今後のOpenAMに求められる要件

6. OpenAM普及に向けたOpenStandiaの取り組み

今後のOpenAMに求められる要件

簡単にインストール、設定、動作確認まで出来るマニュアルやウィザードの充実

OpenAMは高機能だが、導入までの敷居はまだまだ高い。
誰でも簡単に導入出来るマニュアル、ウィザードがあれば普及の促進が期待出来る。

エージェントや他社製OAM連携モジュールの充実

SharePointやサイボウズ、NTT Data intra-martといった国内で普及しているポータルやグループウェアと連携するエージェントやHP IceWallやOracle Access Manager、IBM Tivoli Access Managerとの連携モジュールを充実していくことで、新たな利用促進が期待出来る。

Office365連携(のアンナウンス)

昨今は、Office365とのSSO要件が多い。
理屈上はSAML標準をサポートしているOffice365との連携は可能なはずだが、マニュアルに明記されていないため、顧客も二の足を踏んでいる。
本家本元のForgeRockのお墨付きがあれば、顧客も安心してOpenAMを選択できるだろう。

アジェンダ

1. 野村総合研究所のご紹介

2. OpenStandiaのご紹介

3. SSO/IDMに求められる解決すべき業務課題

4. 業務課題解決事例紹介

5. 今後のOpenAMに求められる要件

6. OpenAM普及に向けたOpenStandiaの取り組み

OpenAM普及に向けたOpenStandiaの取り組み

- OpenAMの方式設計、導入手順書を公開しております。

http://openstandia.jp/oss_info/openam/index.html

ログインユーザのIDを連携

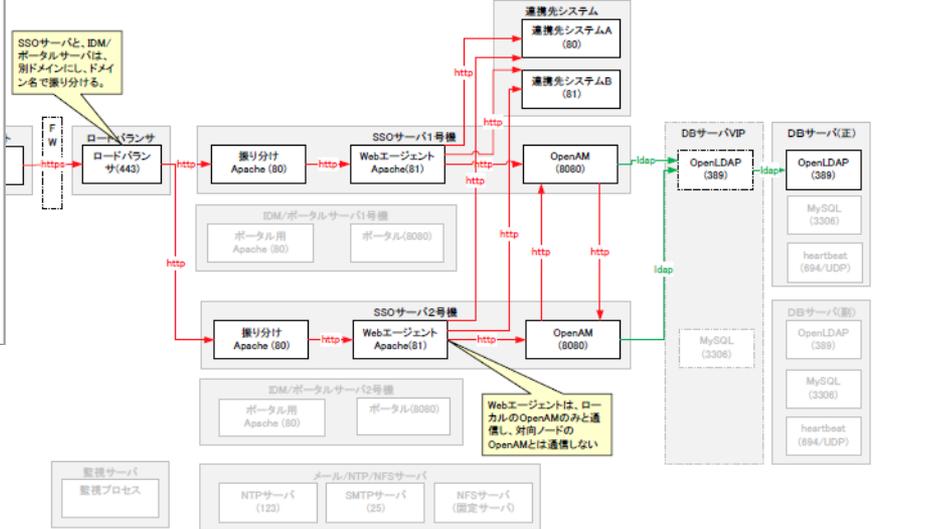
オープンソースまるごと
OpenStandia
Open Source Technology

- HTTPヘッダにユーザIDを追加して連携する
 - ▶ アクセス制御 > (最上位のレルム) > エージェントと遷移
 - ▶ エージェントの名前をクリックしてアプリケーションタブを開く

54
NR 総合研究所 Copyright© Nomura Research Institute, Ltd. All rights reserved.

導入手順書

信経路一覧
グルサインオン



設計意図

- SSO サーバと IDM/ポータルサーバは別ドメインにする。
 - ▶ ロードバランサにコンテキストパスでリクエストを振り分ける機能がない事が想定されるため(クラウドのロードバランサはほとんどこの機能がない)
- Web エージェントは、ローカルの OpenAM のみを登録し、対向ノードの OpenAM とは通信しない。OpenAM の標準構成は、対向ノードと通信する方式であるが採

Copyright © 2013 Nomura Research Institute, Ltd. All rights reserved

3-15

OpenAM普及に向けたOpenStandiaの取り組み

● コミュニティへの貢献

バグの報告及びバグFixを行っております。

Repositories Projects People Reviews Search Log in

openam / trunk / openam / openam-core / src / main / java / com / sun / identity / log / service
LogRecWrite.java

All trunk Search for branch/tag

Activity Revisions Users Reports Source

7773 7773 Changeset Raw Annotation Highlighting Columns

Legend

- 15 days old (3 lines)
- 2 years and 5 months old (8 lines)
- 3 years and 11 months old (191 lines)

Line History

Commit Activity

Author	Revision
Peter Major	1029
Kohei	7773
Peter Major	1029
root	6

```
26 *  
27 */  
28  
29 /*  
30 * Portions Copyrighted 2011 ForgeRock AS  
31 * Portions Copyrighted 2013 Nomura Research Institute, Ltd  
32 */  
33 package com.sun.identity.log.service;  
34  
35 import java.util.Hashtable;  
36 import java.util.Iterator;
```

Crucible: Open Source License registered to ForgeRock AS.
Version 3.2.4 is available.

バグFixの一例 OPENAM-3116 エージェントログが抜ける不具合の改修

出所: <http://sources.forgerock.org/>

OpenAM普及に向けたOpenStandiaの取り組み

- **ニーズが高くOSSでは不足している機能**を、OpenStandiaで付加しています。
過去、OpenAMに対して付加機能を開発してきましたが、昨今はIdMの領域について、日本固有の要件を満たす製品が存在しない、また「適切なIdM無くしてSSO (OpenAM) の普及無し」という課題認識の下、OpenIDMの付加機能開発を推進しております。

NRI付加機能

- IDライフサイクル管理
- 権限管理
- 拡張ワークフロー
- 履歴管理
- 監査レポート/棚卸し
- 拡張API

- C/SシステムとのSSO
- RDBMS認証
- 代理認証



OpenIDM NRI付加機能について

1. プロビジョニング (ID連携) と企業内IDライフサイクル管理
2. 企業内IDライフサイクル管理に求められる要件
3. OpenIDM NRI付加機能

OpenIDM NRI付加機能について

1. プロビジョニング (ID連携) と企業内IDライフサイクル管理

2. 企業内IDライフサイクル管理に求められる要件

3. OpenIDM NRI付加機能



プロビジョニング

社内システムやクラウド上のサービスへのアイデンティティ連携
連携プロトコル

- SCIM (Systems for Cross-domain Identity Management)
- JDBC、LDAP、AD、CSV etc…

狭義のプロビジョニング(ID連携)は、指示された通りに連携先システムに対象のアイデンティティを転送することが主な役割。
プロビジョニング製品にはID連携にフォーカスが当たったものが多い。



企業内のアイデンティティ管理

日本固有、企業個別の
様々なアイデンティティ、様々なイベント、様々な手続き…

企業内には、プロビジョニングの前にやるべきことが沢山ある。

📌 様々なアイデンティティ

正社員、派遣社員、海外拠点社員、グループ会社社員、協力会社社員...

📌 様々なイベント

入社、人事異動、退社、転籍、入場、退場、組織改編、M&A...

📌 様々な手続き

ID／電話番号／メールアドレス付与、システム利用権限付与、確認作業及びそれに伴う申請～承認フロー

企業によって手続きのやり方は異なる。

適切なIDライフサイクル管理を実現する為には、企業の組織構造に合った適切なID管理業務の整理が不可欠。



多くの事例でここで
四苦八苦。

適切なIDライフサイクル管理を実現すると、適切に管理されたアイデンティティを適切なタイミングでプロビジョニング(ID連携)出来る様になる。

企業内IDライフサイクル管理に求められる要件

1. プロビジョニング (ID連携) と企業内IDライフサイクル管理

2. 企業内IDライフサイクル管理に求められる要件

3. OpenIDM NRI付加機能

企業内IDライフサイクル管理に求められる要件

顧客企業(10数社)の共通要件

IDライフサイクル管理

- 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
- 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(上と矛盾する概念だが、実際には良くある)

内部統制対応

- ワークフロー
- 履歴管理
- 棚卸し
- 監査ログ

企業内IDライフサイクル管理に求められる要件

補足 発令日ベースのIDライフサイクル管理

- 一般的にID管理システムにアイデンティティが登録されるタイミングと、プロビジョニングのタイミングにはズレがある。
- また、発令日直後は業務引継のため、着任日まで一時的に兼務とするケースが多い。

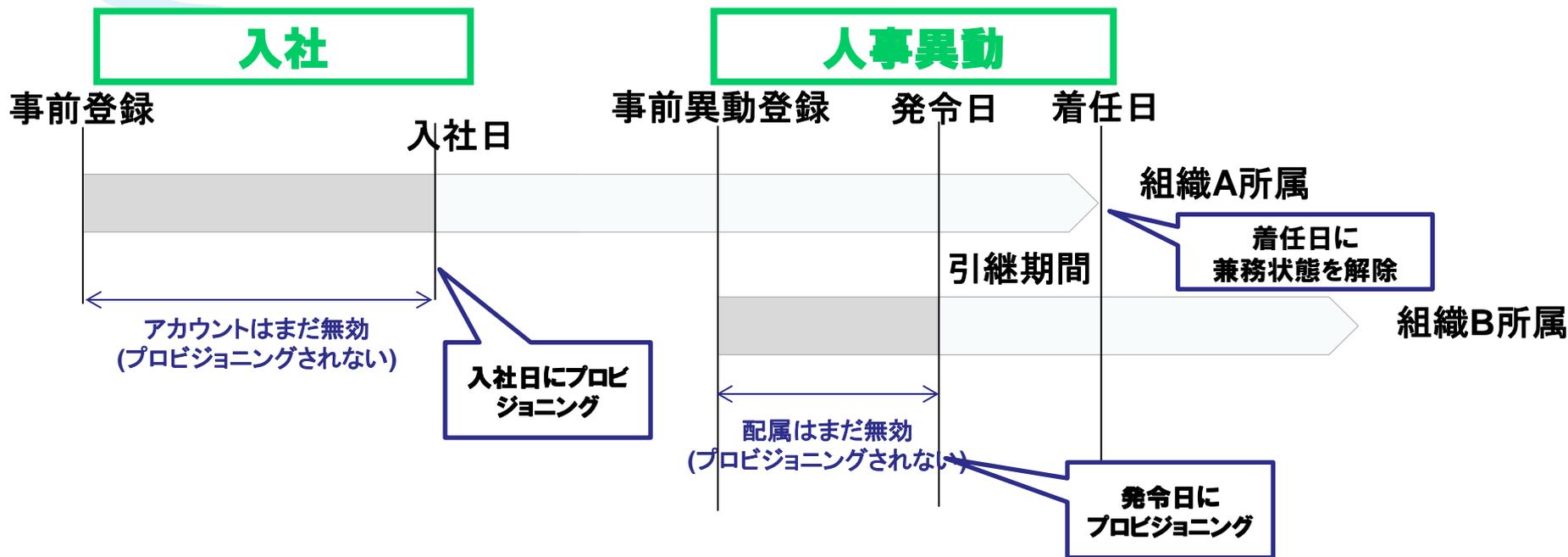


図2. 発令日ベースのIDライフサイクル管理の一例

OpenIDM NRI付加機能

1. プロビジョニング (ID連携) と企業内IDライフサイクル管理

2. 企業内IDライフサイクル管理に求められる要件

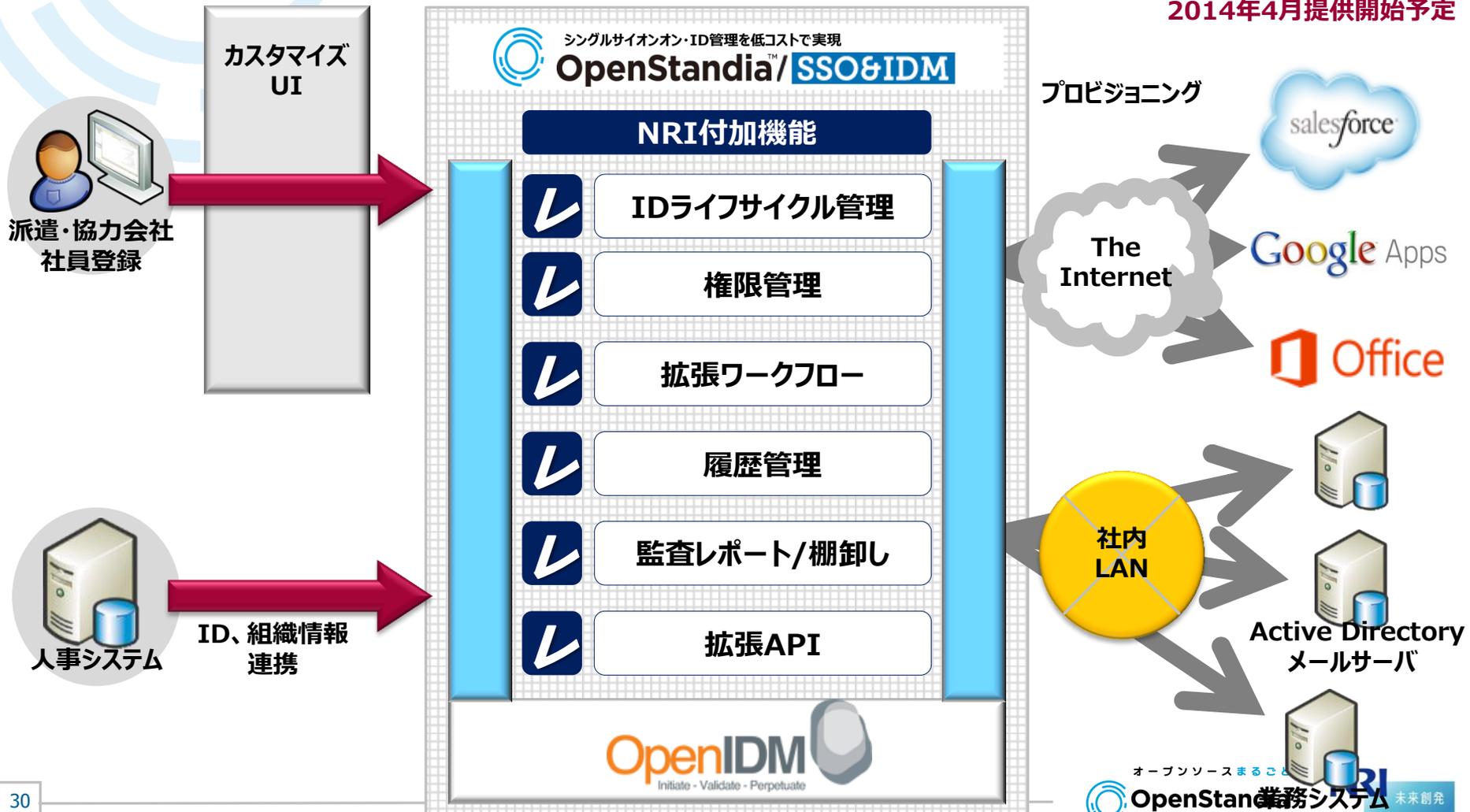
3. OpenIDM NRI付加機能

OpenIDM NRI付加機能

ForgeRock社のID管理製品である、OpenIDMの優れたプロビジョニング機能に、NRI独自の企業内IDライフサイクル管理／内部統制機能をアドオン開発。

Coming Soon!

2014年4月提供開始予定



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！

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推進室へ



osscc@nri.co.jp



<http://openstandia.jp/>