OpenIDM・OpenIGの機能紹介

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
和田　広之

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：ossc@nri.co.jp　Web：http://openstandia.jp/

はじめに

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

自己紹介

所属部署

- オープンソースソリューション推進室（OSSC）
- OSSを使ったシステム構築から運用までワンストップでサポート
- 対象OSSは50種類以上

私の担当

- OSSをベースとした製品開発を担当
  - ✓OpenStandia/Portal、OpenStandia/SSO&IDMなど
- OpenAM、OpenIDMの機能拡張、バグ修正も実施しています

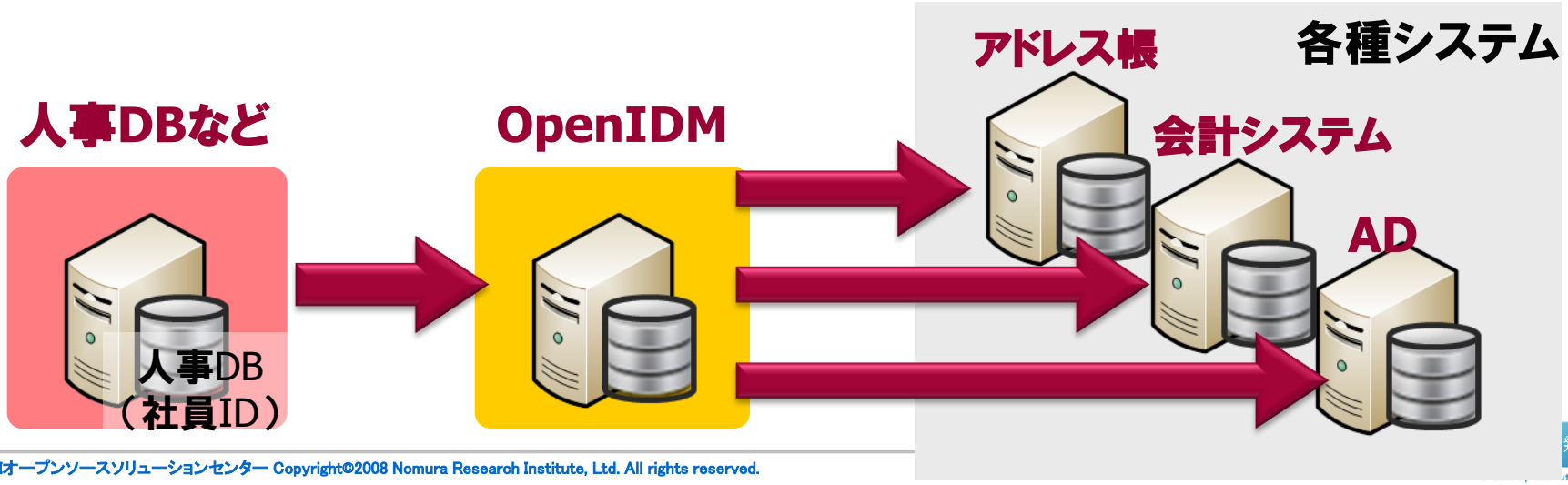
NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIDMの紹介

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

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



NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

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

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

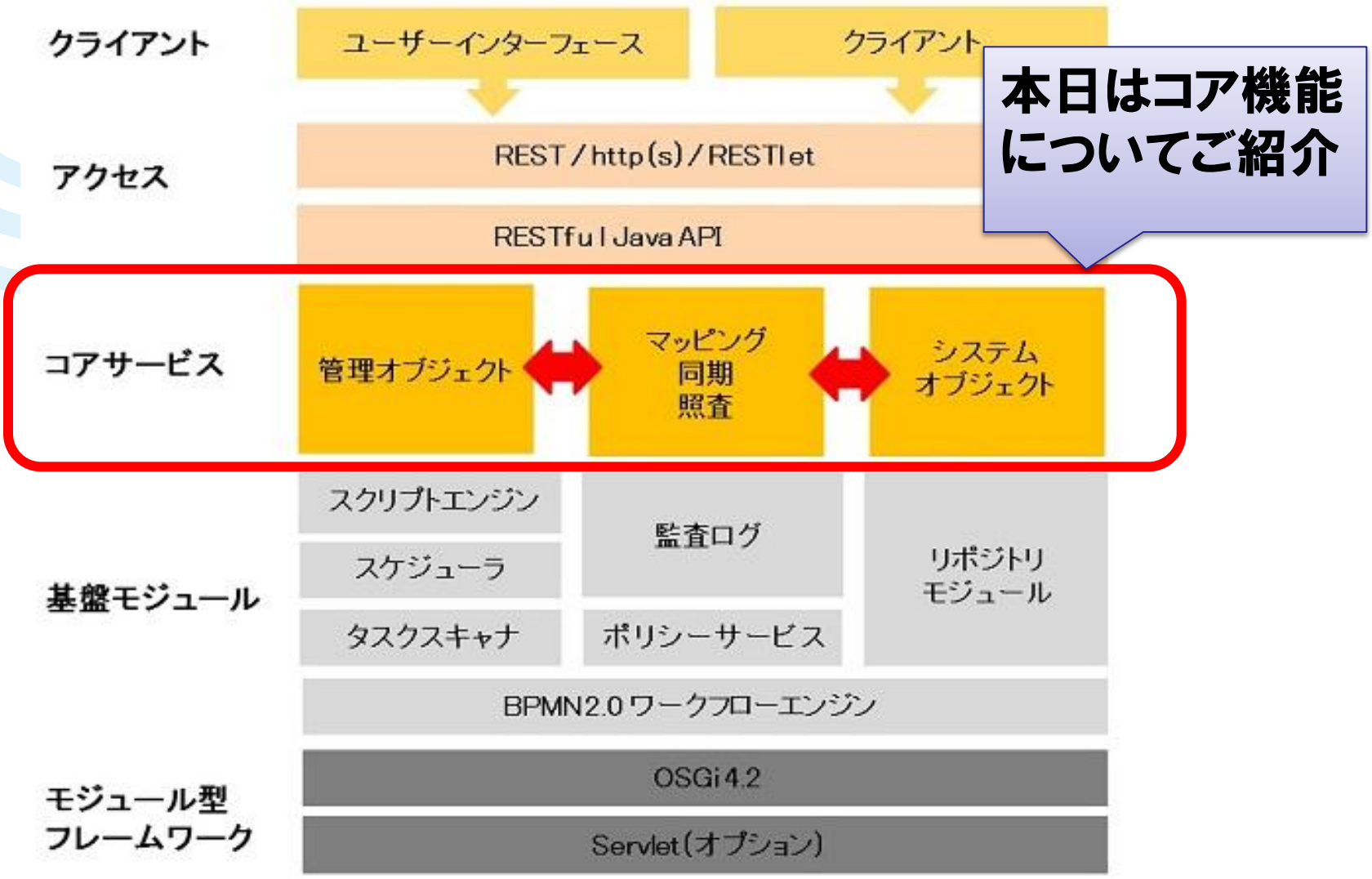
他製品との機能比較

- 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	○	○	○

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIDMのアーキテクチャ

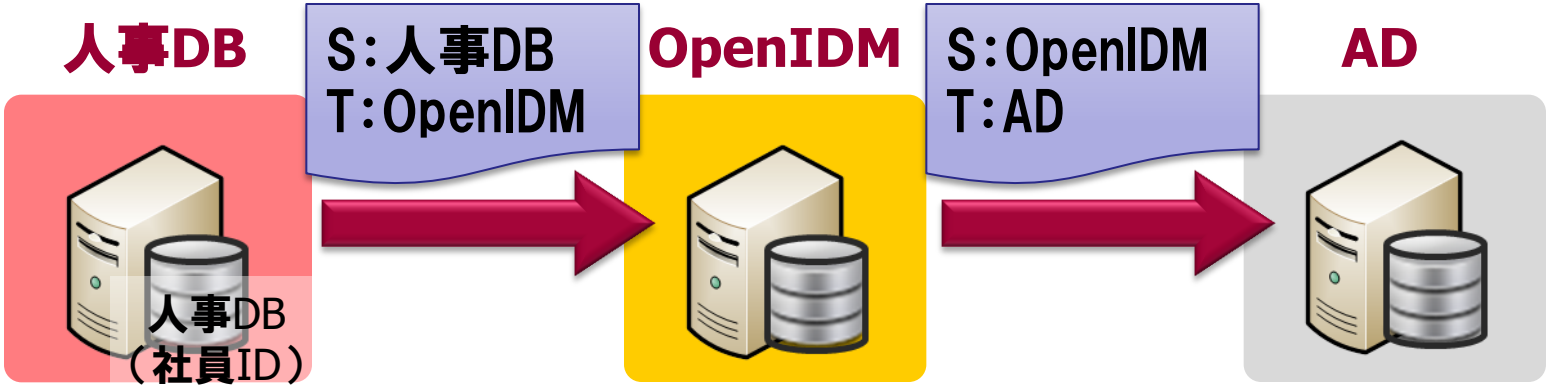


(出所)野村総合研究所 OpenStandia OSS紹介 OpenIDM最新情報 http://openstandia.jp/oss_info/openidm/

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

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



NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIDMの同期機能

2種類の同期処理方式

- Reconciliation (リコンシリエーション)
  - ✓いわゆる差分同期
  - ✓ソースとターゲットを比較し変更点を検知して同期を行う
- LiveSync
  - ✓外部リソースから変更点情報を取得して同期する方法
  - ✓不必要な差分チェックを行わないためリコンシリエーションと比べると軽いプロセス
  - ✓ただし、コネクタ・外部リソースがLiveSyncに対応している必要がある

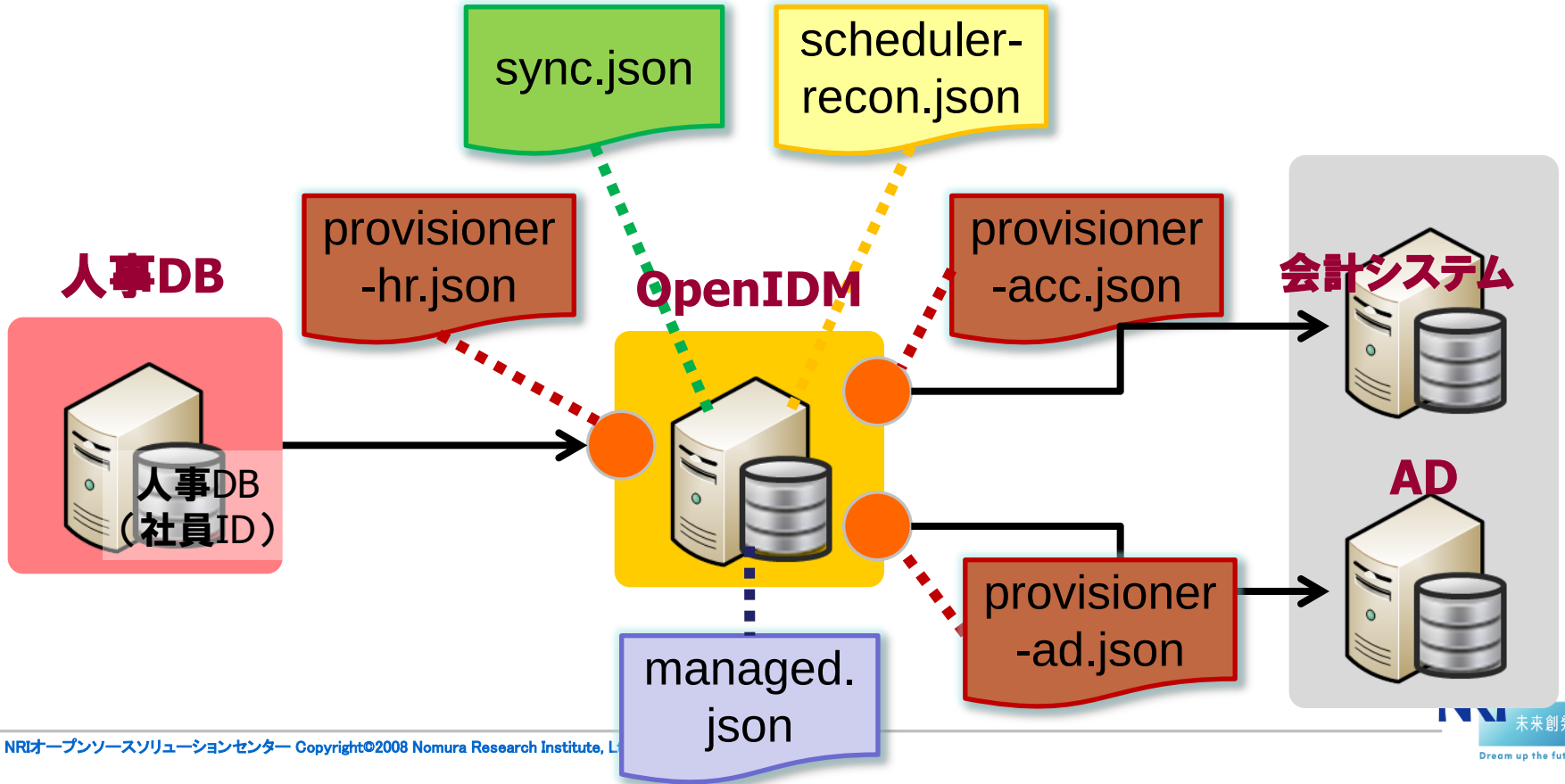
同期処理の実行トリガー

- REST APIによるマニュアル実行
- スケジューラによる自動実行
- リポジトリの更新検知による自動実行

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

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)



NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, L
NRI 未来創発 Dream up the future.

Managed Objects と System Objects

Managed Objects

- OpenIDMのリポジトリで管理されるオブジェクト
- JSON形式で格納される
- デフォルトではユーザーオブジェクトのみだが、任意のオブジェクトを定義可能
  - ✓managed.jsonで定義

```
{
   "objects": [
      { “name”: “user”    },
      { "name": "group” }
      ・・・
```

System Objects

- 連携先の外部システムのデータを表すオブジェクト
- コネクタ定義を行うことで表現
  - ✓provisioner-*.jsonで定義

```
{
  "name" : “HR",
  "connectorRef" : { ・・・}
  "poolConfigOption" : { ・・・}
  "configurationProperties " : { ・・・}
  "objectTypes" : {
      "account" : {
```


NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

マッピング定義

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

- sync.jsonにソースとターゲット間でマッピングする項目名を定義する
- スクリプトで加工することも可能
  - 例えば、姓と名を結合して渡す場合など

```
{
   "mappings" : [
      {
         "name" : "systemHrAccounts_managedUser",
         "source" : "system/HR/account",
         "target" : "managed/user",
         "properties" : [
            { "source" : "_id",           "target" : "_id" },
            { "source" : "lastName",  "target" : "lastName" },
            { "source" : "firstName",  "target" : "firstName" },
            { "source" : "",              "target" : "displayName",
              "transform" : {
                 "type" : "text/javascript",
                 "source" : "source.lastName + ' ' + source.firstName"
              }
            }
            ...
```

ソース：System Objects
ターゲット：Managed Objects
を指定

姓・名を結合

スケジュール設定

- schedule-*.jsonに同期（リコンシリエーション）の実行タイミングを定義する

実行間隔を指定

```
{
    "enabled" : true,
    "type": "cron",
    "schedule": "* * 2 * * ?",
    "concurrentExecution" : false,
    "invokeService": "sync",
    "invokeContext": {
        "action": "reconcile",
        "mapping": "systemHrAccounts_managedUser"
    }
}
```

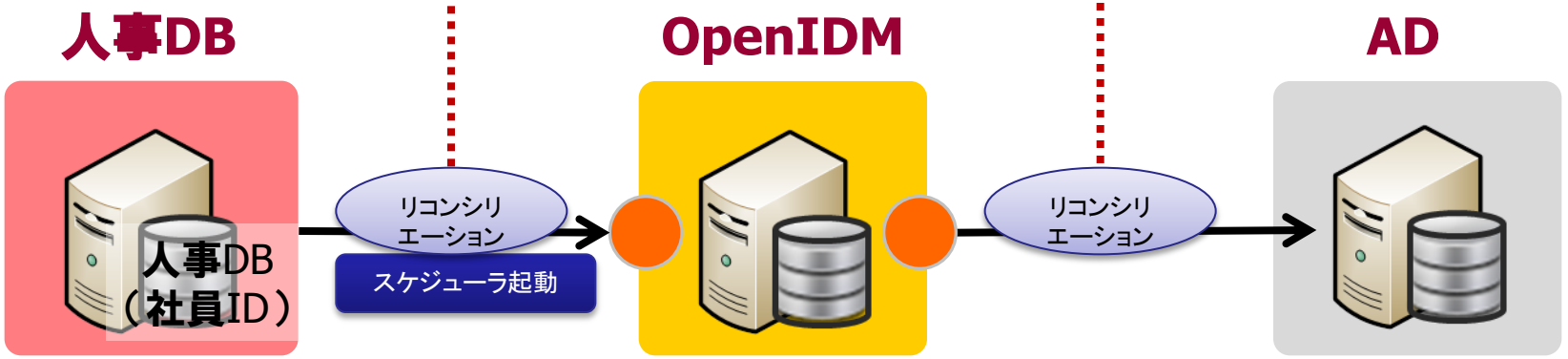
実行する同期処理のマッピング定義名を指定

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

リコンシリエーションによる同期例

① スケジューラ機能で源泉データ取り込みのリコンシリエーションを実行指示
(毎日AM 2時)人事DBのデータとOpenIDMを比較して差分同期

② ①の同期完了後、ソース(この場合OpenIDM)の変更を検知し、リコンシリエーションが自動実行される
OpenIDMとADを比較して差分同期される



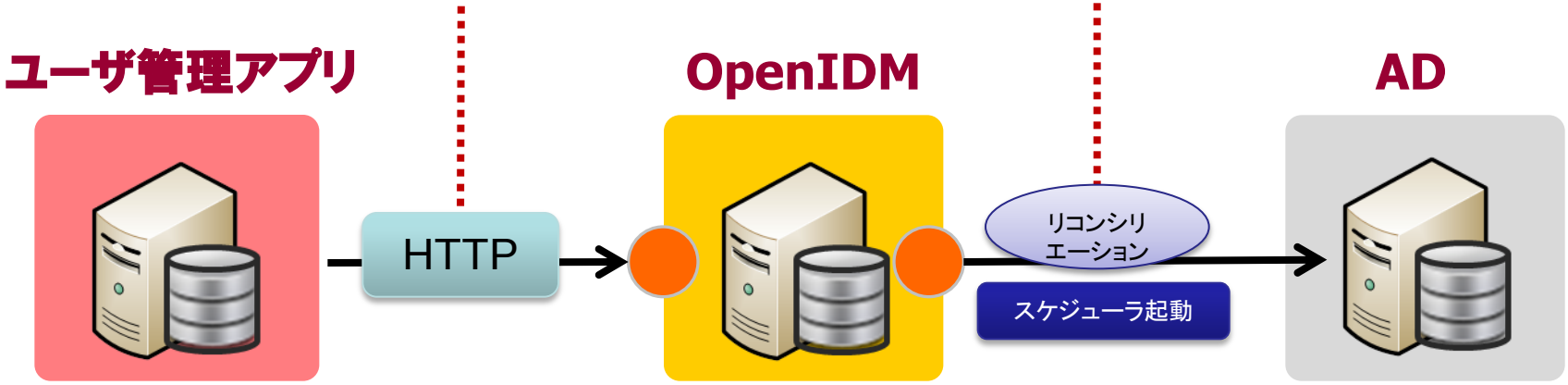
NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

より高度なプロビジョニング

- 発令日ベースで連携先システムにIDをプロビジョニングするケース

① REST APIで直接データを登録・更新
発令日を登録

② スケジューラ機能でADへのプロビジョニングのリコンシリエーションを実行指示(毎日AM 4時)
OpenIDMとADを比較して差分同期を行うが、対象を 発令日 >= システム日付 のユーザとする。



NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIDMで連携可能な外部リソース

- 標準では以下のコネクタが利用可能
  - CSV File
  - LDAP
  - Scripted SQL
  - XML File

- OpenICFで提供される追加コネクタ
  - GoogleApps Connectior
  - Salesforce Connector

・・・などが提供されている

OpenICFの仕様に従って独自のコネクタを作ることも可能

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIDMの参考情報

英語

- Release Notes
  - ✓http://docs.forgerock.org/en/openidm/2.1.0/release-notes/index/index.html
- Install Guide
  - ✓http://docs.forgerock.org/en/openidm/2.1.0/install-guide/index/index.html
- Integrator's Guide
  - ✓http://docs.forgerock.org/en/openidm/2.1.0/integrators-guide/index/index.html
- ForgeRockによるOpenIDM Wiki
  - ✓https://wikis.forgerock.org/confluence/display/openidm/Home
- ForgeRockによるOpenIDM blog
  - ✓http://blogs.forgerock.com/OpenIDM/

日本語

- OpenStandiaによるOpenIDM最新情報
  - ✓http://openstandia.jp/oss_info/openidm/index.html

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIGの紹介

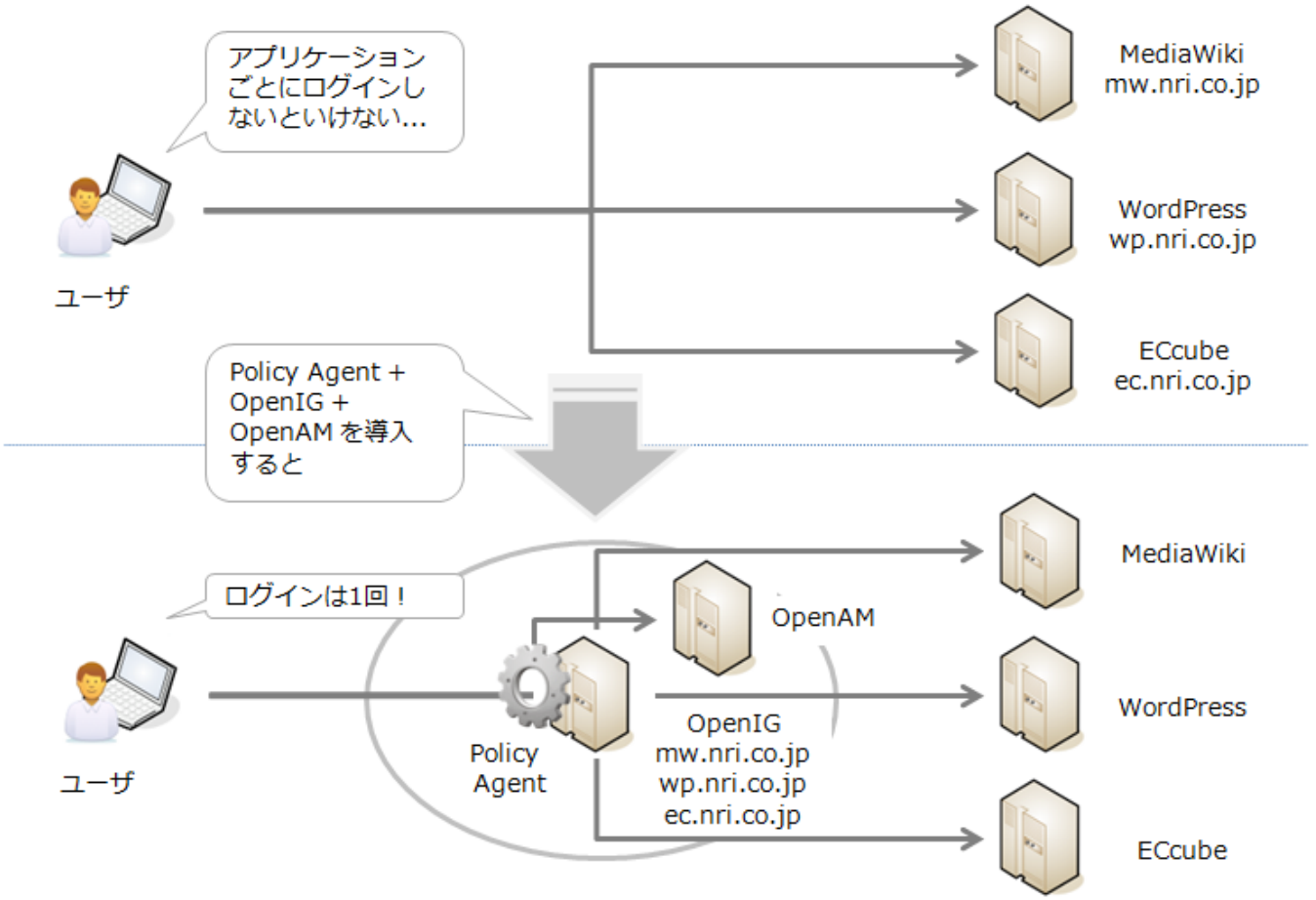
NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

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

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIGによる代理認証

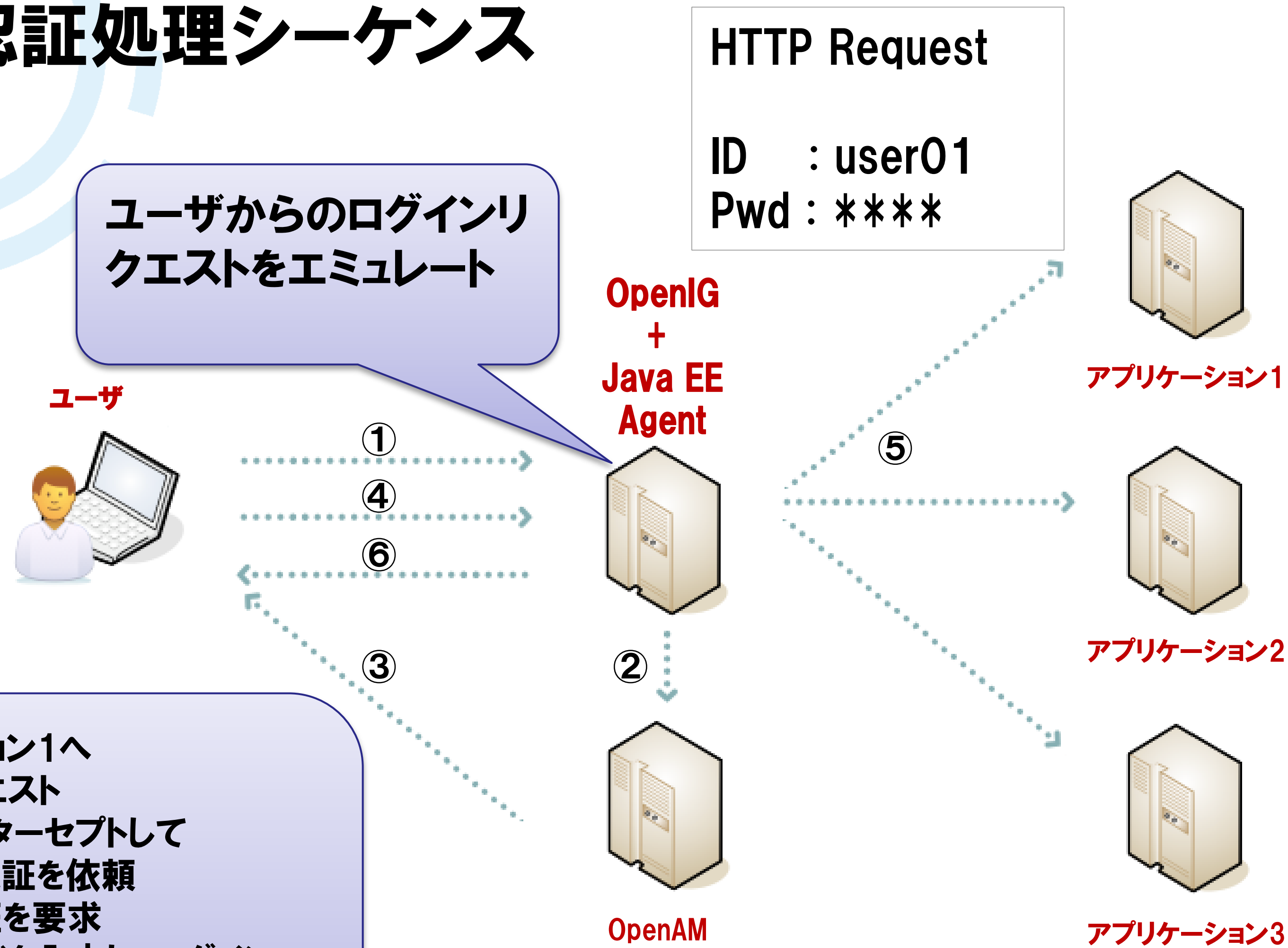


NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

NRI 未来創発
Dream up the future.

OpenIG (Open Identity Gateway)

代理認証処理シーケンス

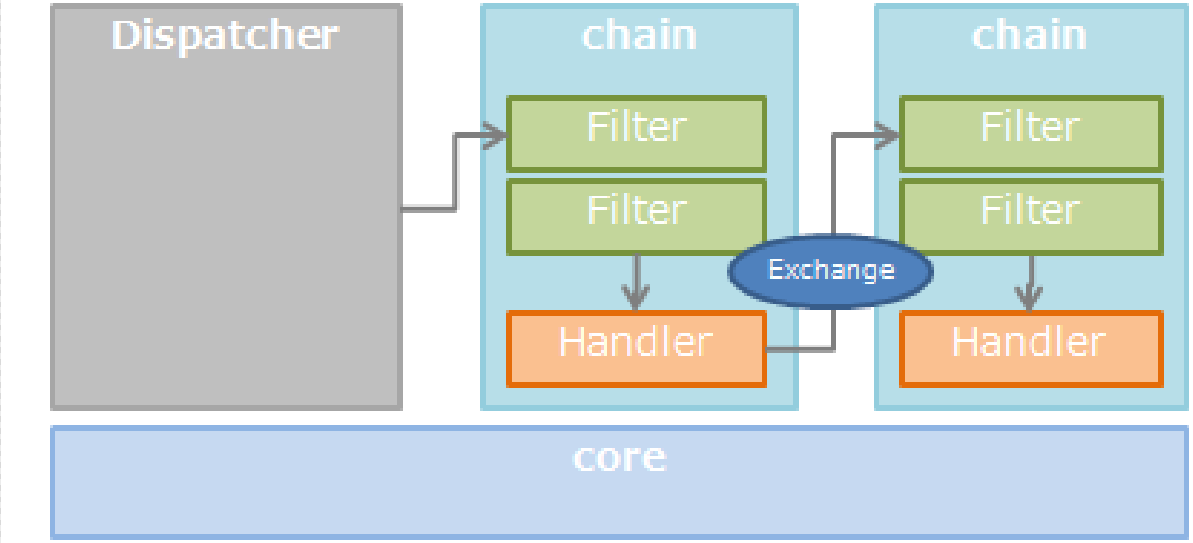


① アプリケーション1へ
ログインリクエスト
② Agentがインターセプトして
OpenAMへ認証を依頼
③ ユーザに認証を要求
④ ID、パスワードを入力し、ログイン
⑤ ユーザからのログインリクエストを
エミュレートし、認証を代行
⑥ ログインレスポンスを返す

Institute, Ltd. All rights reserved.

OpenIGのアーキテクチャ

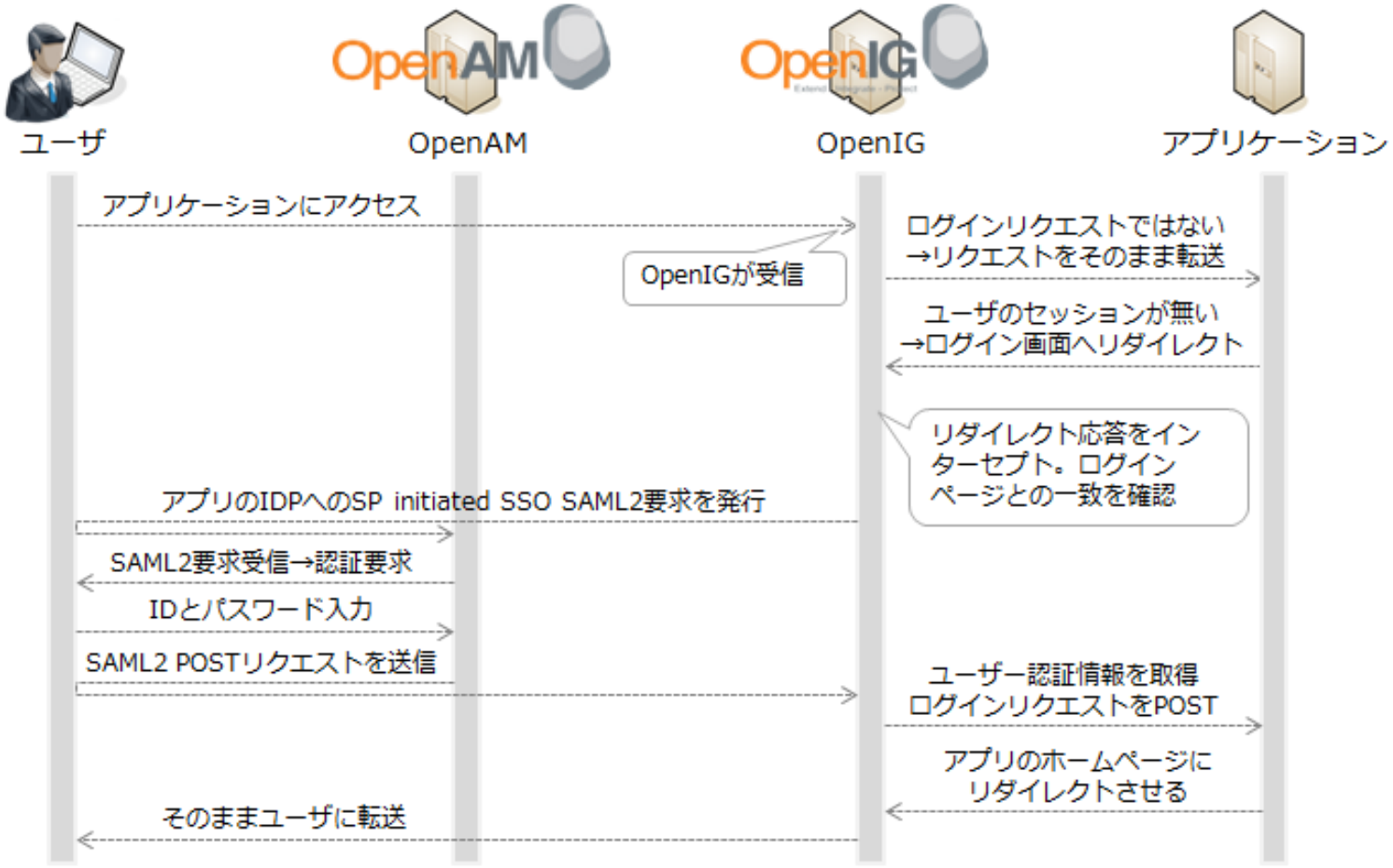
- 設定ファイルはJSON形式
- フィルターでデータの加工・作成を行い、ハンドラーで処理を実行する
- 連携先に合わせて必要なフィルターとハンドラーの組み合わせを考え、設定する必要がある
  - 設定を行うにはアーキテクチャの理解が必要



NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

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

SAML2.0 フェデレーションゲートウェイ機能



NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

NRI 未来創発
Dream up the future.

OpenIG と NRI独自代理認証機能の比較

	OpenIG	NRI独自
アーキテクチャ	•Javaで実装 •J2EEエージェントと組みわせる	•mod_perlで実装 •Apache Webエージェントと組み合わせる
拡張性	•フィルター、ハンドラーで拡張可能	•利用者向けの拡張ポイントなし
ログイン方式	•サーバサイドでログイン処理のPOSTを行う •POSTする項目を1つ1つ定義する必要あり	•クライアントサイドでログイン処理のPOSTを行う •POSTする項目を定義する必要なし（埋め込むログインID、パスワードのフィールドID指定のみ）
リライト機能	•HTTPヘッダの書き換えが可能	•HTTPヘッダ、コンテンツ内容（HTML、JS、CSSなど）を対象に正規表現で書き換え可能
フェデレーションゲートウェイ（SAML）	あり	なし

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

OpenIGの参考情報

英語

- Release Notes
  - ✓http://docs.forgerock.org/en/openig/2.1.0/release-notes/index/index.html
- Guide to OpenIG
  - ✓http://docs.forgerock.org/en/openig/2.1.0/gateway-guide/index/index.html
- Config Reference
  - ✓http://docs.forgerock.org/en/openig/2.1.0/reference/index/index.html

NRIオープンソースソリューションセンター Copyright©2008 Nomura Research Institute, Ltd. All rights reserved.

- 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

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/

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。

NRI 未来創発

Dream up the future.

NRIオープンソースソリューションセンター Copyright©2013 Nomura Research Institute, Ltd. All rights reserved.