2014 Japan Identity and Could Summit

企業内IDライフサイクル管理を行い適正なプロビジョニングを！

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/

アジェンダ

1. 自己紹介
2. 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
3. 企業内IDライフサイクル管理に求められる要件
4. OpenStandiaの取り組み

自己紹介

1. 自己紹介
2. 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
3. 企業内IDライフサイクル管理に求められる要件
4. OpenStandiaの取り組み

自己紹介

- 入社～2008年　OLTPシステム、分散オブジェクト技術、J2EEをベースとした基盤ミドルの開発及び導入プロジェクトの基盤リーダーとして、方式設計～プログラム開発、基盤構築を行う。
- 2008年、OpenStandiaに参画。OpenStandia実行部隊のリーダーとしてOSSを活用した基盤方式設計、構築に従事。
- 2009年、Sun MicroSystemsのOpenSSOに出会い、格闘。
- 以降、OpenAM(OpenSSO)を中心としたシングルサインオン、と統合ID管理システムの方式設計、構築に従事。

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

1. 自己紹介
2. 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
3. 企業内IDライフサイクル管理に求められる要件
4. OpenStandiaの取り組み

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

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あたったものが多い。

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。

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

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
大企業になると、これらが全て別の管掌で行われることも

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。

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

まとめ　ID連携は便利な製品が各ベンダから提供されている。
ID統合管理には、これらの製品の導入に先立つ適切なID管理業務の整理こそが命題。

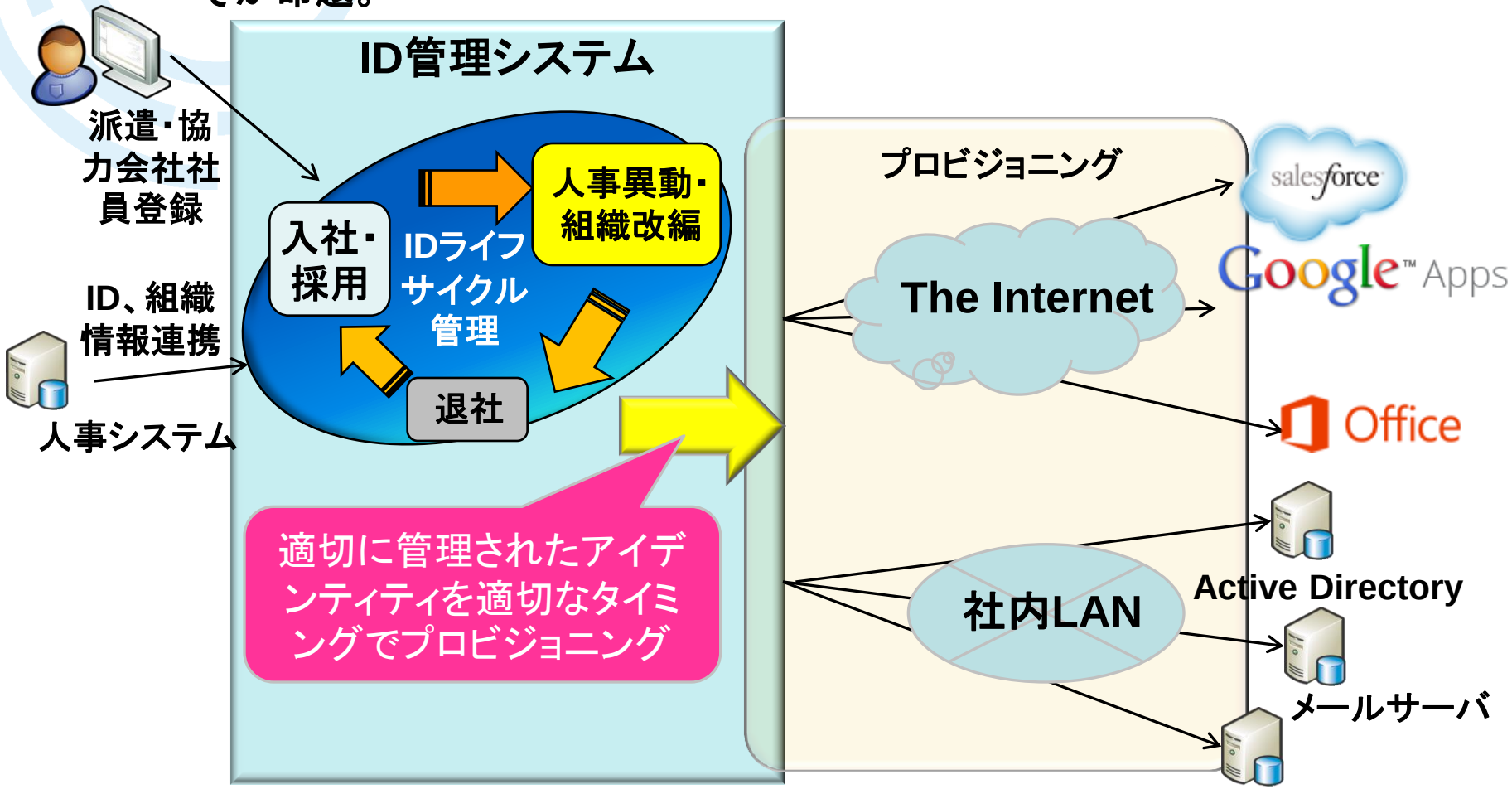


図1. プロビジョニングと企業内IDライフサイクル管理

企業内IDライフサイクル管理に求められる要件

1. 自己紹介
2. 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
3. 企業内IDライフサイクル管理に求められる要件
4. OpenStandiaの取り組み

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。

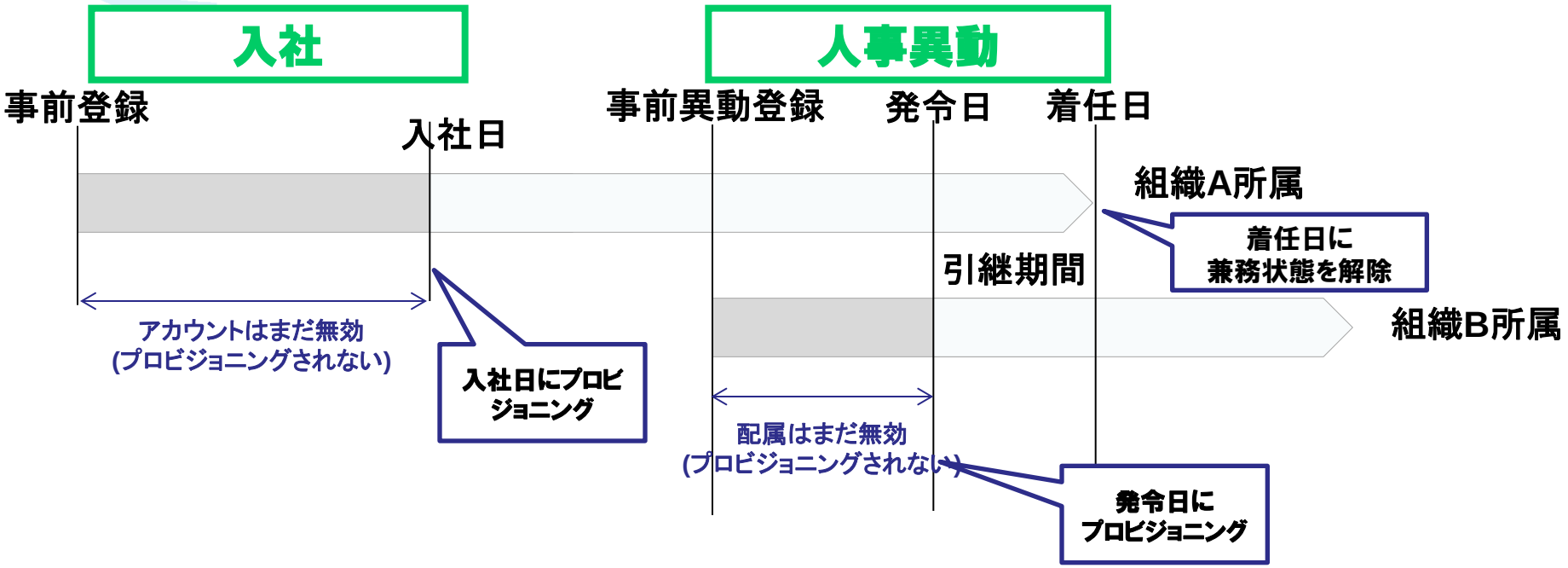


図2. 発令日ベースのIDライフサイクル管理の一例

OpenStandiaの取り組み

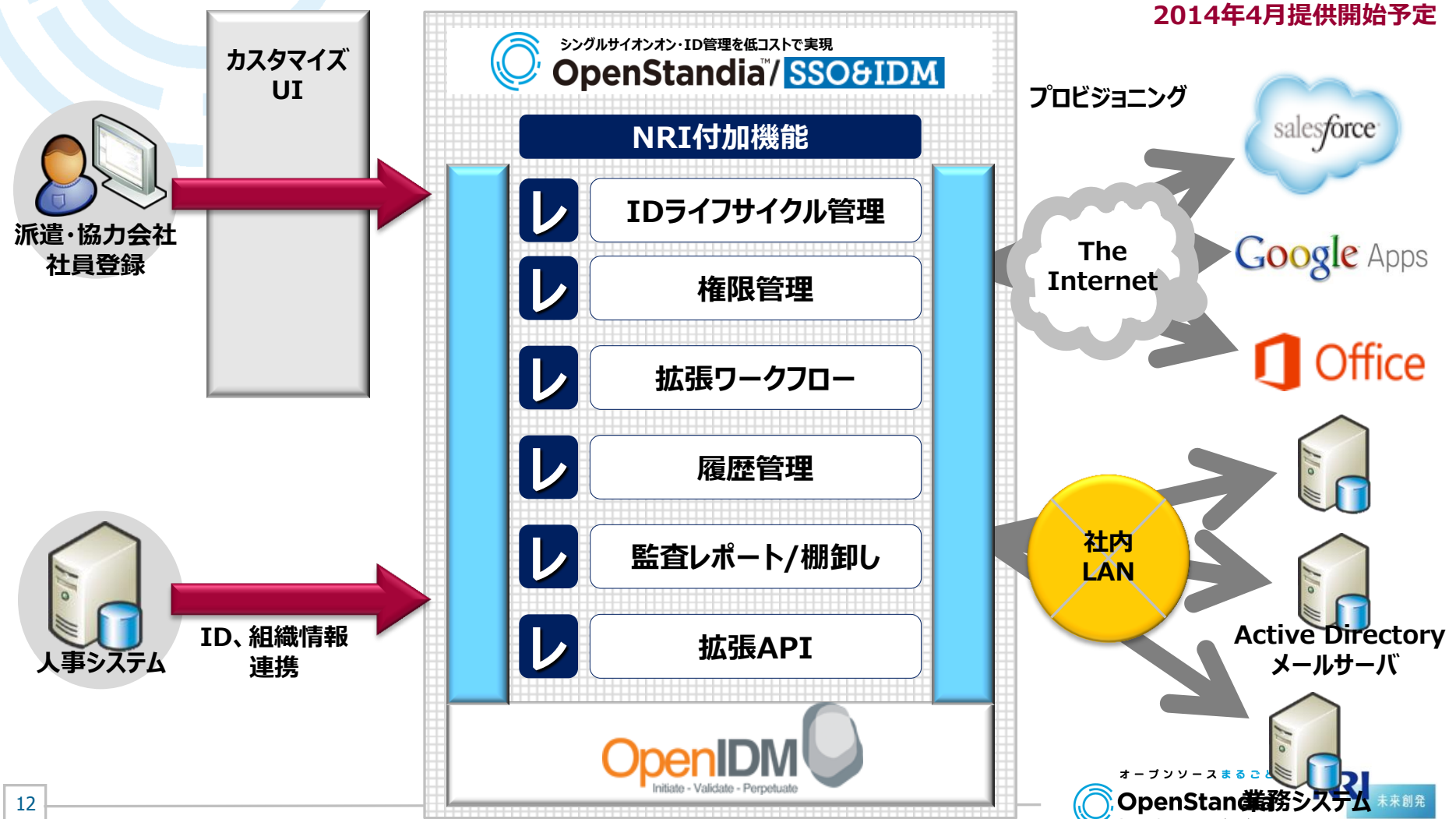
1. 自己紹介
2. プロビジョニング（ID連携）と企業内IDライフサイクル管理
3. 企業内IDライフサイクル管理に求められる要件
4. **OpenStandiaの取り組み**

IDライフサイクル管理におけるNRIの取り組み

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



OpenStandia付加されている機能

● 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。

※Lifelayベースとの比較

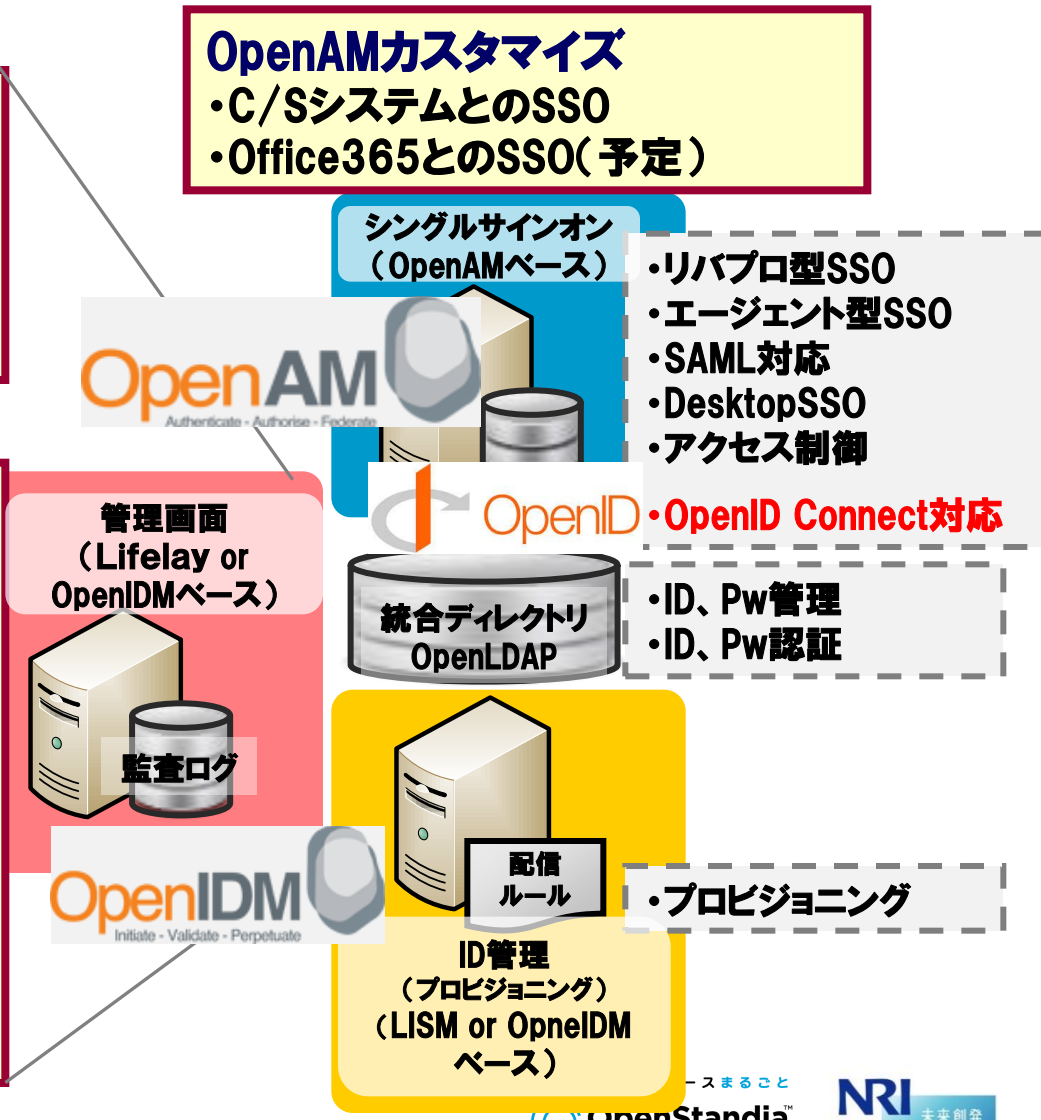
利用者向け機能の提供

- 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

※Lifelayベースとの比較

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



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

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推進室へ

ossc@nri.co.jp

http://openstandia.jp/

NRI 未来創発

Dream up the future.