News Release

2014 年 11 月 5 日
株式会社野村総合研究所

オープンソースの統合認証・管理ソリューション「OpenStandia/SSO&IDM」の新バージョンを提供開始

～「OpenAM」「OpenIDM」の最新版の取り込みと NRI 独自機能の追加～

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、企業等の情報システムにおける認証や ID 管理の基盤をすべてオープンソース・ソフトウェアで実現する統合認証・管理ソリューション「OpenStandia/SSO&IDM（オープンスタンディア/エスエスオー・アンド・アイディーエム）」の新バージョン（V2）を 11 月 5 日に提供開始しました。

SaaS 等、外部の共同利用型サービスとの連携や、スマートフォンやタブレット端末の活用が進むなど、企業の情報システムを取り巻く IT（情報技術）環境が多様化しています。そのため、情報システムのシングル・サインオン（SSO）[*1] 化に取り組む企業が増えてはいるものの、その実現は困難なものとなっています。一方で、内部統制や規制の強化にともなって、コンプライアンスや個人情報保護の重要性が増しており、それを担う認証システムの安全性や透明性が極めて重要になっています。

このような背景から、NRI は、オープンソースで実現する ID 基盤として、2010 年から「OpenStandia/SSO&IDM」を提供してきました。その特長は、利用者の利便性を損なうことなく、情報システム全体を安全かつ柔軟に低コストで維持管理することが可能となる点にありました。

この度、NRI は、本年 7 月に提携した ForgeRock 社[*2] から提供を受けたオープンソース・ソフトウェア「OpenAM（オープンエーエム）」と「OpenIDM（オープンアイディーエム）」の最新版を組み込んだ新バージョン、「OpenStandia/SSO&IDM V2」の提供を開始しました。

新バージョンでは、企業システムごとのさまざまな認証環境への対応に加え、「OpenID（オープンアイディー）」[*3] 等の ID フェデレーション[*4] の標準技術にも対応しています。
また、認証強度を高める手段として、多要素認証[*5] やリスクベース認証[*6] をおこなうことが可能です。さらに、日本企業の特有の人事制度や慣習に適合した ID ライフサイクル管理、権限管理、ワークフロー、証跡管理等においても、機能の強化を図っています。

NRI は、今後もオープンソース・ワンストップサービス「OpenStandia」を通じて、企業の情報システムにおけるオープンソースの活用を推進し、安心安全で便利な IT 社会の実現を目指します。

*1 シングル・サインオン（SSO）：

一度の認証処理によって、複数のコンピュータ上のリソースが利用可能になる認証機能。例えば、あるコンピュータにログインした後、グループウェア等のアプリケーションを使用する際、あるいは他のサーバ上のアプリケーションを使用する際に、再度ログインが求められるとユーザーは複数の ID とパスワードを管理しなければならない。シングル・サインオン環境においては、ユーザーはひとつの ID とパスワードによって、すべての機能を使用することができる。

*2 ForgeRock 社（フォージロック社）：

近年急成長している、オープンソースの ID 管理製品ベンダー。大企業や政府機関に対して、安心安全な Web 環境を提供する。2010 年に創設され、ネットワーク経由での ID を利用した新しいビジネスモデルを築いている。会社および製品の詳細は、下記 URL を参照。

http://forgerock.com/

*3 OpenID：

ひとつの ID で、さまざまな Web サービスの認証を実現する仕様。一度 ID を取得すれば、他の対応サイトでも同じ ID でログインできる。この技術により、ユーザーは ID を複数使い分ける必要がなく、ID の管理が容易になる。またインターネット事業者は、他の対応サイトで登録された ID を自社のサービスで受け入れることが可能になるので、より多くのユーザーの獲得・維持ができる。公開された仕様などは、下記 URL を参照。

http://openid.net/

*4 ID フェデレーション：

情報システムや IT サービスが個々に管理しているユーザーの ID 情報を紐づけることによって、サービス間のデータや機能を、ユーザーを中心に連携する方法。OpenID、SAML 等の技術を活用して実現する。

*5 多要素認証：

ユーザーが記憶している ID・パスワードに加え、ユーザーが持っているもの（複製できない、もしくは複製しづらい機器）を組み合わせて認証をおこなうことで、セキュリティレベルを高める方法。たとえ ID・パスワードが漏えいしても、他の要素が揃ってない限り、ログインすることができない。

*6 リスクベース認証：

第三者のなりすましによる犯罪などを防ぐためのセキュリティ対策。ログイン時に、ユーザーが普段利用している利用環境（端末情報など）と異なる場合、本人確認のための追加認証をおこなう機能。

【ニュースリリースに関するお問い合わせ】

株式会社野村総合研究所　コーポレートコミュニケーション部　十河、海藤

TEL：03-6270-8100　E-mail：kouhou@nri.co.jp

【ソリューションに関するお問い合わせ】

IT 基盤イノベーション事業本部　オープンソースソリューション推進室　内山、田中

TEL：045-335-9538　E-mail：ossc@nri.co.jp　URL：http://openstandia.jp/　Twitter：@oss_info

---

【ご参考】

【OpenStandia/SSO&IDM V2 の主な特長】

- 大量アクセス/大規模システムに対応可能なアーキテクチャ
- 認証・認可・ID プロビジョニング等の各機能をプラグインとして実装
- 既存の企業システムのさまざまな認証環境に対応（フェデレーション、リバースプロキシ、エージェント、Active Directory Windows ログオン）
- ID フェデレーションの国際標準プロトコル「OpenID Connect」「OAuth」「SAML」「WS-Federation」をサポート
- ワンタイムパスワード等の多要素認証やリスクベース認証についてのプラグイン対応
- ID ライフサイクル管理、権限管理、ワークフロー、証跡管理機能の強化