OSSのアイデンティティ情報管理システム
―高度化するセキュリティ要求に対応―

昨今、アイデンティティ情報（以下、ID情報）の漏えいや、成り済ましなどの不正利用が相次いでいる。ID情報に関わる不正アクセスの問題や運用コストの増加は、多くの企業にとって悩みの種となっている。本稿では、オープンソースソフトウェア（OSS）を使った低コストのシングルサインオンおよびID情報管理システムを紹介する。

ますます強まる不正アクセスのリスク

グローバル化やM&A（合併・吸収）による統合、SaaS（Software as a Service）などのクラウドサービスの利用増加などにより、企業ユーザーが利用するシステムの数は増加の一途をたどっている。また、PCに加えてスマートフォンやタブレット端末など、業務システムで利用するデバイスの多様化が進み、デバイスを一律に管理することが難しくなってきている。

これらのシステムは、ユーザーを認証し利用を認可するために、IDとパスワードをはじめとするID情報を必要とするが、一般に、ID情報がシステムの増加によって散在してしまうと、ユーザーもシステム管理者もID情報を適切に管理することが難しくなる。例えば、複数のシステムを利用する場合に、ユーザーはID情報を全て頭に入れておくことは現実的には不可能なため、パスワードを同じにしたり、「2013April」のような推測されやすいパスワードにしたりすることが少なくない。このようなケースでは不正アクセスのリスクが増大する。

実際に、昨今はいわゆるパスワードリスト攻撃（リスト型アカウントハッキング）が急増している。これは、パスワードの使い回しが多いことを利用して、あるWebサイトから不正に得たIDとパスワードのリストを使って、攻撃対象のサイトに不正ログインを試みるものである。

パスワードリスト攻撃は主にオンラインゲームなどの消費者向けサービスで被害が拡大しているが、今後は企業システムの分野でも同様のリスクが高まると考えられる。これまでは社内に閉じたネットワーク内でシステムを利用するケースが多かったが、近年はインターネットを経由したシステム利用の形態が増えているためである。

今後はBYOD（Bring Your Own Device：個人所有端末の業務利用）がますます普及することが予想され、加えてインターネット上にあるクラウドサービスの利用が増加していることもあり、ますます不正アクセスのリスクは強まっていくであろう。

新たなID管理へのニーズ

クラウドサービスやマルチデバイスの活用などによってシステムの多様化が進み、冒頭で述べた不正アクセスのリスクが高まるなか

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
主任テクニカルエンジニア
和田広之（わだひろゆき）
専門はOSSの技術支援、製品開発

で、その対策としてシングルサインオンおよびID情報管理システム（以下、SSO/IDM）へのニーズが高まっている。SSO/IDM製品に求められているのは主に以下の2つの対策である。

(1)高度な認証機能

1つ目は、高度な認証機能である。不正ログインに対する対策として、一般的にはパスワードの見直しが有効である。桁数（文字数）を多くする、辞書にあるような意味のある単語は使わない、アルファベットの大文字・小文字および数字を組み合わせるといったルールにすれば、破られにくいパスワードとなる。

しかし、このようにパスワードを強化しても、それが流出してしまえば同じことである。パスワードリスト攻撃のような不正アクセスの試みに対しては、以下で述べる2要素認証やリスクベース認証といった、より高度な認証方式が対策として有効となる。

2要素認証は、通常のパスワード認証にワンタイムパスワード（ランダムに生成された一時的に有効なパスワード）などを加えた2つの認証を併用する方式である。たとえパスワードが漏えいしても、ワンタイムパスワードを知られることがなければ不正ログインを防ぐことが可能である。

リスクベース認証は、ログインを試みたユーザーの行動を分析して、不審な場合に認証方式を変更する仕組みである。例えば、ユーザーが通常とは異なるアクセス元からログインすると、それを検知して2要素認証に切り替える。

2要素認証は、セキュリティ強度を高くできるが、追加の操作が必要である分、ユーザーの利便性を損なうというデメリットがある。従って多くの場合では、普段どおりの操作で済むリスクベース認証と、2要素認証を組み合わせて用いることが望ましい。

(2)認証連携

2つ目は認証連携（ID連携）である。これは外部のクラウドサービスを利用する場合などに有効で、異なるサービス間で認証情報を交換することによって実現される。そのためのプロトコルにSAML（Security Assertion Markup Language）などがある。認証連携を利用した認証方式では、社内システム利用時のパスワードを連携させる必要がないので、安全にクラウドサービスを利用することが可能となる。

NRIのSSO/IDMソリューション

前述のとおり、SSO/IDMには高度で多様な機能が求められている。商用のSSO/IDM製品は豊富な機能によってその要求に応えるが、以下のような問題もある。

①高コスト

一般的に、商用SSO/IDM製品はユーザー数に応じて課金される。ユーザー数が多ければ多いほど、ライセンス費用、保守サポート

費用が高くなる。

②カスタマイズが難しい

商用製品は当然のことながらソースコードは公開されておらず、自社の要件に合わせた柔軟なカスタマイズは難しい。

そこで野村総合研究所（NRI）では、より低コストで構築でき、カスタマイズも容易なOSSベースのSSO/IDMソリューション「OpenStandia/SSO&IDM」を提供している。OSSはライセンス費用がかからないため、商用製品に比べて導入・保守サポート費用を大幅に削減することが可能である。また、ソースコードは全て公開されているため、きめ細かなカスタマイズにも対応可能である。商用製品の場合は業務を製品に合わせることが定石だが、OSSであれば製品を業務に合わせるという逆のアプローチが可能であり、業務の無用な変更で現場を混乱させるといったことを避けつつ、高度な認証の要求に対応することが可能になる。

「OpenStandia/SSO&IDM」のベースになっているのは米国ForgeRock社のOSS製品「Open Identity Stack」（ID管理製品群）である。OSSは商用製品と比較して機能面で劣っていることも少なくないが、SSO/IDMの代表的なOSSである「Open Identity Stack」は商用製品と同等の機能を持ち実績もある。

ForgeRock社は、Web SSOを実現するためのオープンソースの技術・規格である「OpenSSO」（OpenAMの前身）の開発元Sun Microsystems社がOracle社に買収された後、開発・サポートを継続するために、開発者によって設立された企業である。

「Open Identity Stack」はもともと商用製品として開発・販売されていたものがOSSとして公開されたという経緯があり、機能的にも充実している。「OpenStandia/SSO&IDM」は、この「Open Identity Stack」の中核となっているOpenAMとOpenIDMをベースに作られている。不正アクセスのリスク対策として、前述した2要素認証やリスクベース認証、クラウドサービスとの認証連携にも、これらを利用することで対応可能としている。

「OpenStandia/SSO&IDM」が予定する新機能

最後に、「OpenStandia/SSO&IDM」が予定している新機能を2つ紹介する。この機能により、クラウドサービスも含めたSSO/IDMがより低コストで実現可能になり、併せてこれまでは商用製品でもうまく実現できなかった、日本企業に特有の組織・人事への対応が可能になると期待している。

(1) クラウドサービスとの連携強化

現在、「Open Identity Stack」は新たな機能対応を予定しており、「OpenStandia/SSO&IDM」もこれを取り込むことになっている（表1参照）。

①OpenAMのOpenID Connect対応

②OpenIDMのSCIM対応

表1 「Open Identity Stack」が対応を予定しているOpenAMおよびOpenIDMの重要な新機能

分類	項目	概要
OpenAM	OpenID Connect対応	OpenID Connectは認証連携の標準プロトコルである。現バージョンのOpenAMでは、SAMLやWS-Federationで認証連携を行う必要があるが、次期OpenAMではOpenID Connectを使用した連携が可能となる。SAMLやWS-Federationは大手SaaSプロバイダーでは採用されているが、仕様が複雑であることから多くのサービスでは利用されていない。OpenID Connectは、コンシューマー系で普及している認可プロトコルであるOAuth 2.0をベースとした軽量なプロトコロルであり、今後の標準技術として普及が期待されている。
OpenIDM	SCIM対応	SCIM（System for Cross-domain Identity Management）は、IDプロビジョニングAPIの標準仕様である。同様の仕様としてSPML（Service Provisioning Markup Language）があるが、現在普及は進んでいない。SCIMはSPMLとは異なり、クラウドサービスにフォーカスしたよりシンプルな仕様を目指しており、OpenID Connectと同様に普及が期待されている。

OpenID Connectは認証連携に関する仕様、SCIM（System for Cross-domain Identity Management）はID情報の同期に関する仕様である。双方ともクラウドサービスとの連携を意識した仕様であり、クラウドサービスも含めたSSO/IDMがより簡単に実現できるようになる。SSO/IDM製品を選択するポイントして、今後はこのようなクラウドサービスとの連携容易性を備えているかどうかが重要になってくるであろう。

(2) 日本企業の慣習に対応

日本企業の慣習に対応するため、以下のようなID情報のライフサイクル管理機能の提供を予定している。

①組織改正・人事異動発令前の事前データの登録とシミュレーション機能

多くの日本企業では、4月と9月に組織改正・人事異動が行われる。そこで、事前にデータを登録してシミュレーションを行い、問題が起きないかを検証できるようにする。

②兼務の形態に対応

日本企業では、1人の社員が複数の組織に所属するケースが多い。そのため、通常の兼務に加えて出向なども含めて管理できるようにする。

③人事異動の発令から着任までのタイムラグに対応

人事異動の発令から実際に着任するまでにはタイムラグがある。そこで、着任するまでは異動元の権限を残すことを可能にする。

多くのSSO/IDM製品では、このような日本企業の慣習には対応せず、カスタマイズも難しいため、SSO/IDM製品の外側に個別開発していることが多い。「OpenStandia/SSO&IDM」では、ソースコードが公開されているOSSのメリットを生かして、このような機能拡張も低コストで提供することが可能である。 ■