

OpenIDの動向と課題

石川和也 ● 日本ベリサイン株式会社 リサーチ室 室長

さまざまなウェブサービスがOpenIDに対応 IDプロバイダーの信頼基準の確立が重要

ブログからECサイト、オンラインバンキングに至るまで、多くのウェブサイトが個別にユーザーIDとパスワードを発行し、そのIDによる認証を経てサービスを提供している。ユーザーにとっては利用するウェブサイトが増えるたびに発行されるIDが増え、それらを管理する手間も増える。自分のブログをトラックバックしたブログへコメントを返すときや、マッシュアップされたウェブサイトのように画面上では単なるリンクであったり単一サービスとして見えたりする場合でも、何度もユーザー登録や認証を求められることが非常に面倒だ。こうした不便を解消するのがOpenIDである。

OpenID利用の仕組み

OpenIDでは、ユーザーが、自分で選択したOpenIDプロバイダー(OP)にIDを登録し、そのIDで複数の異なるウェブサイトを利用する。OPで認証を受けたIDは、ウェブサイトごとに認証を行う必要はなく、OpenIDに対応しているどのウェブサイトでも利用可能だ。IDはURL形式(<http://ishikawa.openid.net/>など)もしくはXRI形式(=ishikawaなど)を利用でき、複数のIDを持つこともできる。

OpenIDではIDはサービス事業者によって割り振られるのではなく、ユーザー自身が利用目的、利便性、安全性を考慮してOPを選択して自分のIDを預け、用途によってIDとOPを使い分ける。たとえば、ブログではよりクールなID(OP)を利用し、ECサイトではより安全性の高い運営や認証を提供しているOPを利用する、などだ。IDを、ログイン用の鍵ではなく身分証明書のようなものと考えればよい。複数の種類の身分証を用途別に持つように、OpenIDでも複数のIDを使い分けて利用できる。

OpenIDのユーザーにとって、IDは自分が管理されるタグではなく、自分を示す識別子の役割を持つ。コミュニケーションのためにメールやブログのアドレスを公開するように、自分のIDも選択したり公開したりして利用できる。これがOpenIDがユーザー中心(セントリック)なデジタルIDと呼ばれるゆえんでもある。

もちろん、どの身分証でも同じ機能を果たすわけではないように、OpenIDでも、最終的にサービスを提供(許可)するかどうかはサービス事業者(Relying Party = RP)が決定する。OpenIDではユーザーがサービスに登録する手間が大幅に軽減されるため、事業者にとってはユーザー利便性の向上につながる。もちろん、そのサービスをより良くするために必要な個人情報は、OPもしくはユーザーから直接獲得することになんら問題はない。OpenIDに準拠することで、ほかのID認証用WebAPIとは異なり、複数のOPに登録されたユーザーの受け入れが可能となり、より多くのユーザーを低コストで呼び込めるのだ。

OpenIDのこれまでの動き

2005年に発表されたOpenIDは、当初、ほかのシングルサインオン(SSO)ソリューションと同様に、「もう1つのID」としていくつかのウェブサイト利用されるにとどまっていた。しかし2007年2月にマイクロソフトとAOLが相次いでサポートを表明したことに続き、同11月にグーグルが対応を発表したことで市場から注目される存在となった。

さらに、OpenID推進団体としてOpenIDファウンデーションが米国と欧州に相次いで設立され、標準化と知的財産管理を行う基盤も整ってきた。2008年1月にはヤフーもサポートを表明し、日米でIDの提供が開始された。グーグル、IBM、マイクロソフト、ベリサイン、ヤフーの5社が幹事会社としてOpenIDファウンデーションに加盟し、大手事業者による普及活動も始まっている。国内では2007年よりニフティ、はてな、ライブドアなどが対応した。2008年2月にはミクシィやインフォテリアも対応を発表し、シックス・アパート、日本ベリサイン、野村総合研究所が発起人となりOpenIDファウンデーションの日本支部が設立に向けて動き出した。2008年2月の時点で、世界中にユーザーは2億5000万人、利用サイト数は1万以上となっている。

プロバイダーの選択がOpenIDの課題

OpenIDの基本となるプロトコル(OpenID Authentication 2.0)には、現在のところセキュリティ上の問題は

発見されていない。いくつかの懸念はあるが、その多くは OpenID に限ったものではなく、SSO やインターネットサービスに共通の課題だ。あるいは、「1つのIDで複数のサービスが利用できるため、そのパスワードが盗まれるとすべてを盗まれてしまう」など、ユーザーの誤解や不注意による懸念もある。

OpenID では、認証をパスワードに限定しているわけではない。ID の安全性をより高めたいと思うユーザーは、パスワードより強力な認証機能を提供する OP を選択すればよい。RP が個別に認証の強化対応を行わなくてもユーザー自身が自分のIDの安全性を高めることができ、前述の懸念も低減される。したがって、その OP の選択こそが最大の課題であると言われている。

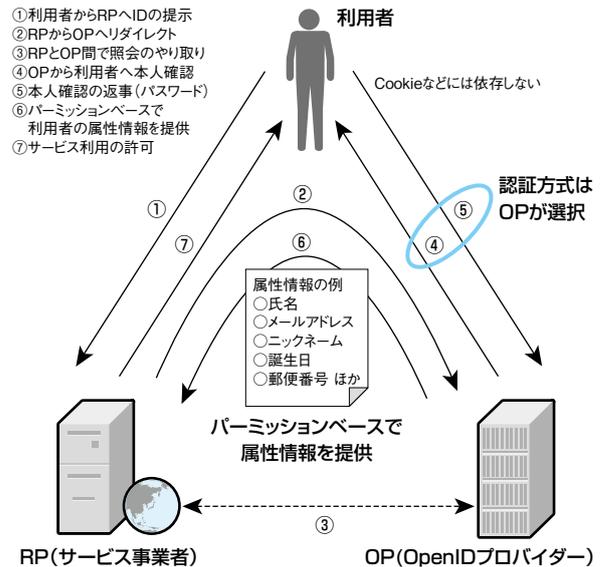
OP がどのような認証を行い、どのようにIDを登録・管理するかについて統一的な基準や公開義務がないために、ユーザーはどのOPが自分の利用目的に合った認証を提供しているか判断が難しい。また、RP は各OPで発行されたIDを受け入れるかどうか自社で判断しなければならないが、そのOPの信頼性に対する基準やそれを知る手立てがないのが現状である。そのため、ユーザーが自分の情報登録を止めてしまったり、サービス事業者がRPになるのを躊躇したり、もしくは自社でもOPとしてのサービスを行い登録されたユーザーのみを受け入れるという状況が発生したりしている。これでは OpenID のメリットが十分に活かされているとは言えない。

このように、ユーザーとRPが、どのようにOPを選ぶ(受け入れる)かが非常に重要なポイントであり、この信頼関係が機能しないと OpenID を安心して利用することは難しい。そのため、OpenID ファウンデーションが中心となり、OPの信頼性や評判、認証の強度、運用レベルをユーザーやRPが知ることができるようにする動きが始まっている。たとえば、PAPE と呼ばれる拡張機能により、RPがOPの認証レベルを確認したり、OPの評判を数値化したり、などが検討されている。2008年2月のRSAカンファレンスでも、OPとRPの契約面や法律面での検討が行われるなど、この課題を解決するために業界全体が動き出している。2008年中にはこれらの仕様が固まり、それに準拠したより信頼できるOPの業務が始まることで、OpenID が普及していくと思われる。

OpenIDの今後の動き

2008年に注目したいもう1つの点は、イントラネットでの利用に向けた動きである。Eメールやウェブに代表され

図1 OpenIDでの認証の流れ



るように、インターネットで普及した技術がイントラネットでも利用されることは珍しくなく、OpenIDも長期的には社内で使うIDとしての普及が予想される。インターネットでウェブサイトごとに異なるIDが発行されているように、イントラネットでもアプリケーションごとにそれぞれ個別のIDを利用している。この状況を解決するため、OpenIDを利用して1つのIDで複数のアプリケーションを利用できるようにすることが考えられる。

特に、社内システムをSaaSなどの外部サービスを利用して構築し、利便性を向上させようとする場合、サービスごとに社員情報を外部に預けるのは、管理コストを増加させるだけでなく、リスクも増やしてしまう。したがって、社員情報とIDを一元管理し、SaaSから切り離して管理することが必要になる。SSOの導入によりID管理だけを各SaaSから切り離すことはそれほど難しいことではない。しかし、現状では複数のSSOが乱立しており、SaaS事業者もそれらすべてをサポートできるわけではなく、対応は様子見の状態であった。

SaaS事業者がOpenIDを採用すれば、インターネットサービスとシームレスに統合でき、より多くのサービスと連携することが可能となると同時に、SSOに個別対応する必要もなくなる。各SSO技術でも、OpenIDに対応することで、ほかのSSOとの相互接続を確保し、利用面・運用面の手間が軽減される。今後は、こうした利点により対応の検討が進んでいこう。いずれにせよ、OpenIDが標準の地位を確立するためには、SaaS事業者との連携によるイントラネットでの利用がどこまで進むかも大きなポイントであり、2008年はそのための標準化と実証・検証が活発になるものと思われる。



[インターネット白書 ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<http://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp