「OpenID」
共通の ID とパスワードで複数のサイトにログイン
エンドユーザーの利便性とサイトの集客力を向上

ビジネスや生活に深く浸透しているインターネットにおいて、もはや各種 Web サイトの提供するサービスは欠かせないものとなっています。その Web サイトの数が増えるに従って、課題となってきたのが認証です。ID やパスワードの管理が複雑になるし、これをおろそかにするとセキュリティレベルが低下してしまいます。
こうした中、注目を集めているのが OpenID です。1 つの共通したアカウントでさまざまな Web サイトの認証を実現する仕組みです。Web サイトごとの異なる ID とパスワードの管理が不要になります。この OpenID の魅力や仕組み、課題などを解説します。

■ OpenIDの魅力

個人を限定した情報のやり取り、物品の売買、メールの送受信……など、インターネットには会員制の Web サイトが多く見受けられますが、これらの Web サイトにおいては、認証が欠かせません。数が多くなると ID やそのパスワードはとても覚えきれず管理が大変になります。しかし、どのサイトも同じ ID とパスワードにしたのでは、セキュリティレベルが低下します。また、もう 1 つやっかいなのが、会員制サイトへの新規登録です。毎回同じように、名前と住所、生年月日などを入力する煩わしさを、どうにかして欲しいと思っている人は多いことでしょう。

そこで考えられたのが「OpenID」です。認証のための ID とパスワードを共通化して、1 つの ID でログインできるほか、会員登録の際の情報入力も、大幅に軽減できます。

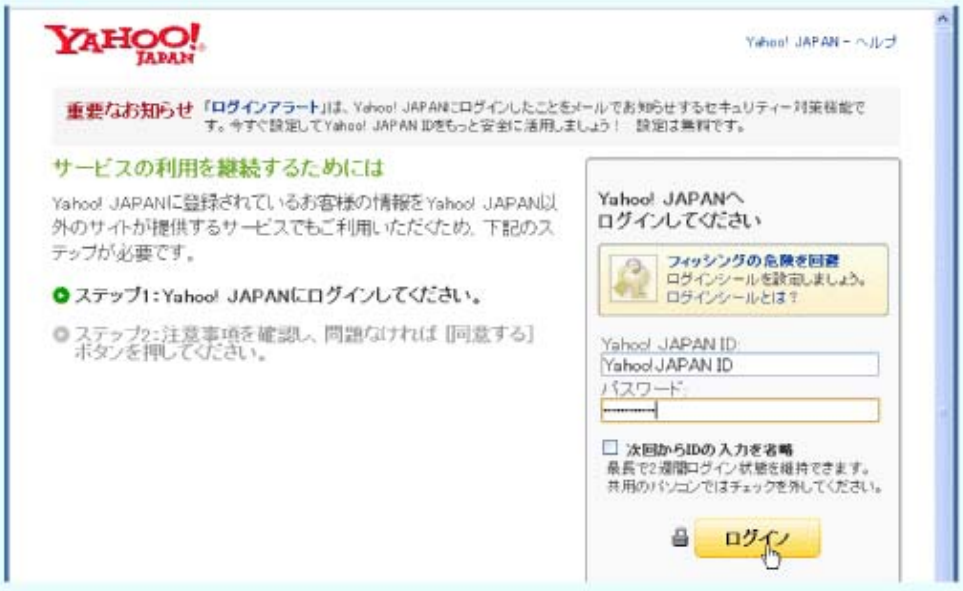
次の図 1-1～図 1-3 は、会員制 Web サイト「@nifty about me」（注 1）に未会員の方が、すでに所有している Yahoo! Japan の OpenID を使って、「@nifty about me」にログインする際の手順です。

まず、Yahoo! Japan のログインボタンをクリックします（図 1-1）。続いて表示された Yahoo! Japan サイトでログインし（図 1-2）、次の画面で「同意する」ボタンをクリックします（図 1-3）。これだけで「@nifty about me」の登録がほぼ完了し、ログインすることができるのです。

本来ならば名前や住所などの煩わしい会員登録操作ですが、対応する OpenID をもっていれば、その手間はほとんど必要ありません。エンドユーザーにとってはこの手軽さが最大のメリットです。

注 1：「@nifty about me」は Yahoo! Japan の OpenID に対応しています。

【図1-1】Yahoo! JapanのOpenIDに対応しているWebサイト「@nifty about me」



【図1-2】Yahoo! Japanのサイトでログイン

【図1-3】「同意する」をクリックすることでほぼ登録完了
登録済みのユーザーはそのまま「@nifty about me」にログイン可能

OpenID 利用のメリットはエンドユーザー側だけではありません。サイトを運営するサービス提供者側にもあります。

まず、会員登録の敷居を低くして、利用者を拡大することができます。Yahoo! Japan や mixi などの膨大な会員をもっているサイトのエンドユーザーを、取り込むことができるかも知れないのです。OpenID への対応は、爆発的なビジネス拡大のチャンスとなるかもしれません。

加えて、ほかのサイトと連携したサービスの実現も可能となります。同じ OpenID の採用企業が、それぞれに得意なサービスを提供し、総合的なサービスを提供できる可能性もあります。

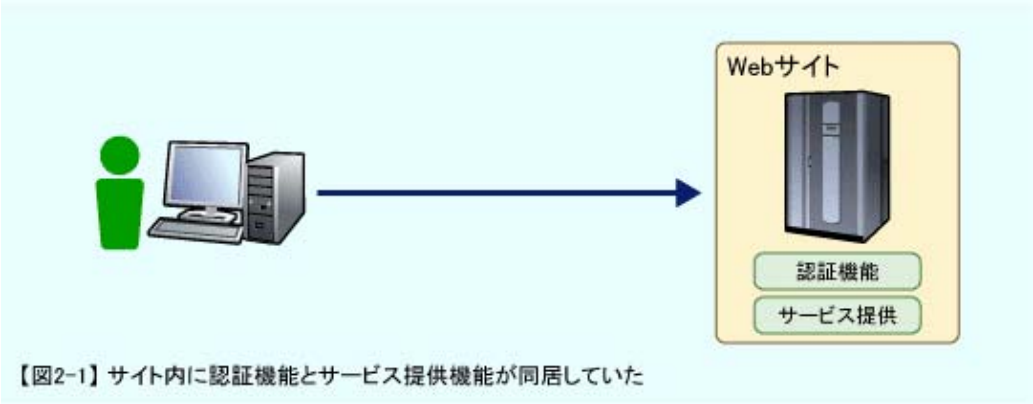
OpenID 認証に限っていえば、認証のプログラムの作成負荷を軽減できるのもメリットの 1 つでしょう。おびただしいエンドユーザーの ID やパスワード管理の手間も省けます。パスワードを忘れたなどの会員への対応からも解放されます。

そして、すでに OpenID 発行側に登録されている利用者は、OpenID 対応サイト側としては、まったく新規に登録する利用者に比べて安心できるので、不正ユーザー登録を防ぐ仕組みとして期待できます。

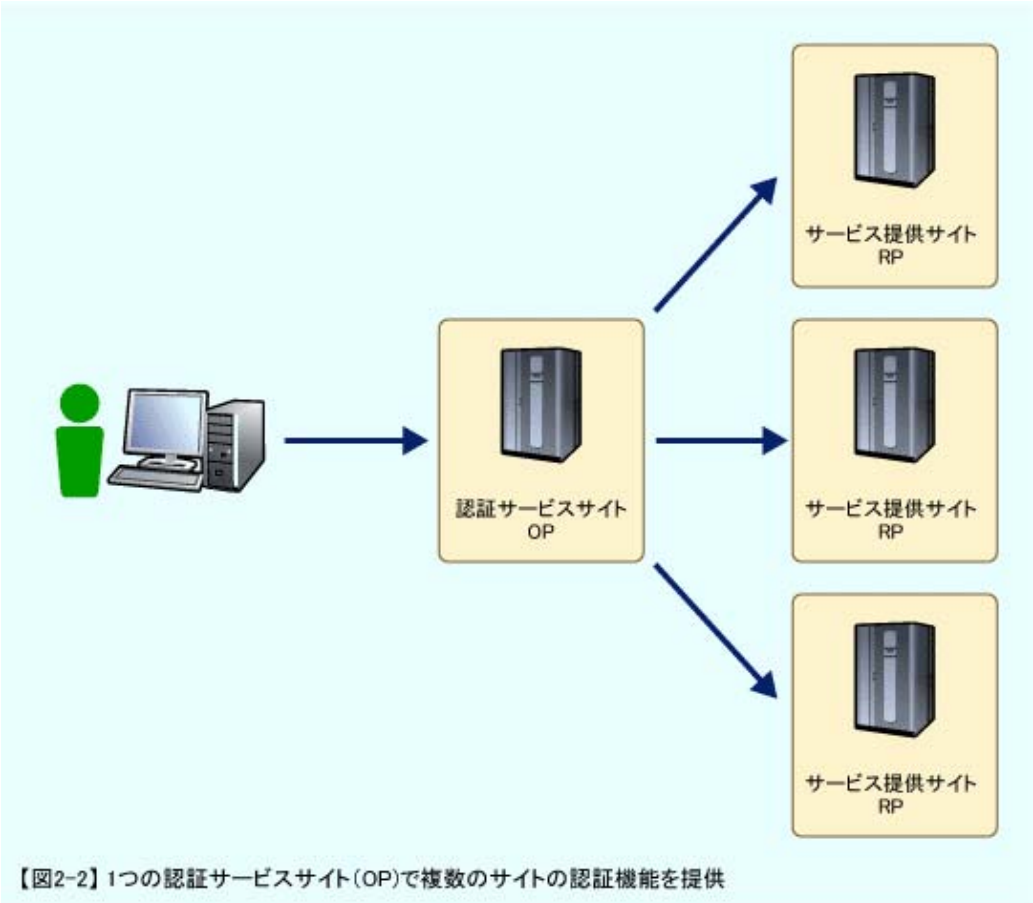
もちろん、OpenID 認証以外のユーザーも共存するため、サイト側が認証や情報管理の課題を、すべて解消できるわけではありません。多くのエンドユーザーが手間なくログインできることは、逆に簡単にほかのサイトへ逃げられることでもあります。囲い込みが難しくなるのです。また、e コマース（電子商取引）サイトの場合は、決済方法や関連する情報、配送先などの情報を別に入手する手段を用意しなければならず、また、追加入手した情報の厳重な管理の手間も変わりません。

■ OpenIDの仕組み

それでは OpenID はどのような仕組みで複数サイトでの認証を可能にしているのでしょうか。その最大のポイントは、認証サービスを提供するサイト（OpenID Provider）と、その認証を受け入れるサイト（Relying Party、以下 RP と記述）を分離したことにあります。従来、認証と各種サービスを提供する機能は、同じサイト内で一体化されていました（図 2-1）。この機能を分離させ、認証機能を外部の OP に出すことで複数のサイトがその認証機能を利用できるようになったのです（図 2-2）。



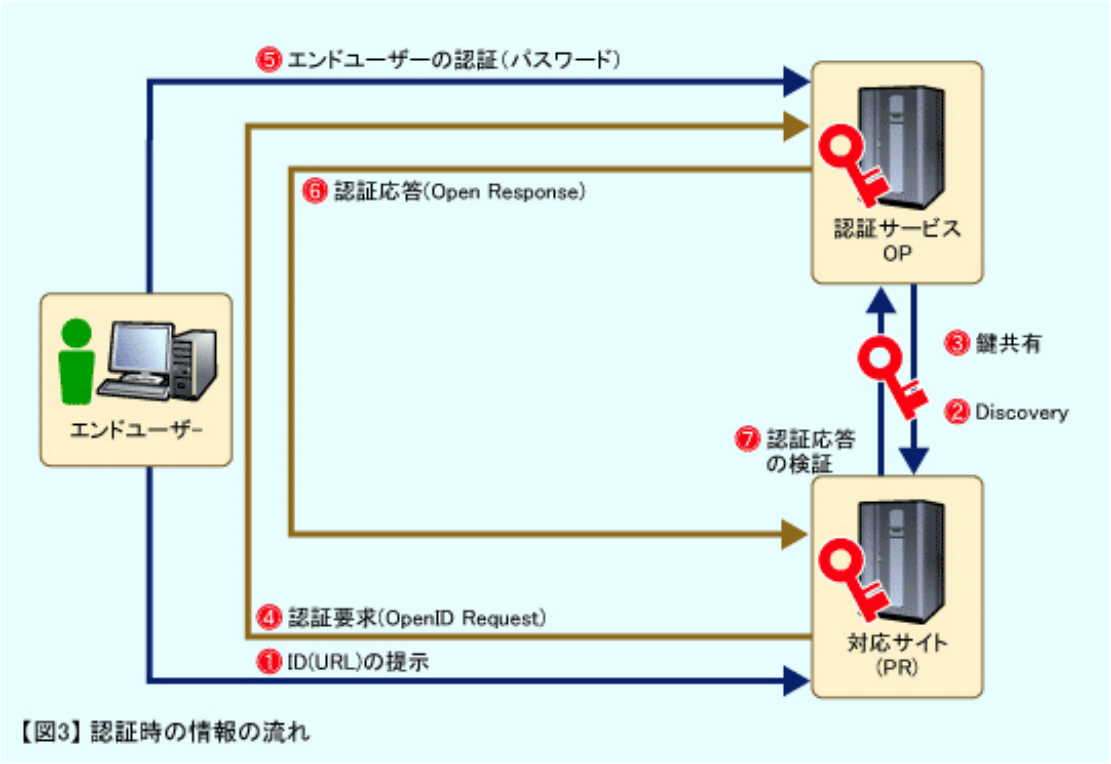
【図2-1】サイト内に認証機能とサービス提供機能が同居していた



【図2-2】1つの認証サービスサイト(OP)で複数のサイトの認証機能を提供

〈コラム〉 認証時の情報の流れ

図 1-1～1-3 で示したような簡単なステップでログインが許可されますが、その裏では意外なほど複雑なやり取りがなされています（図 3）。



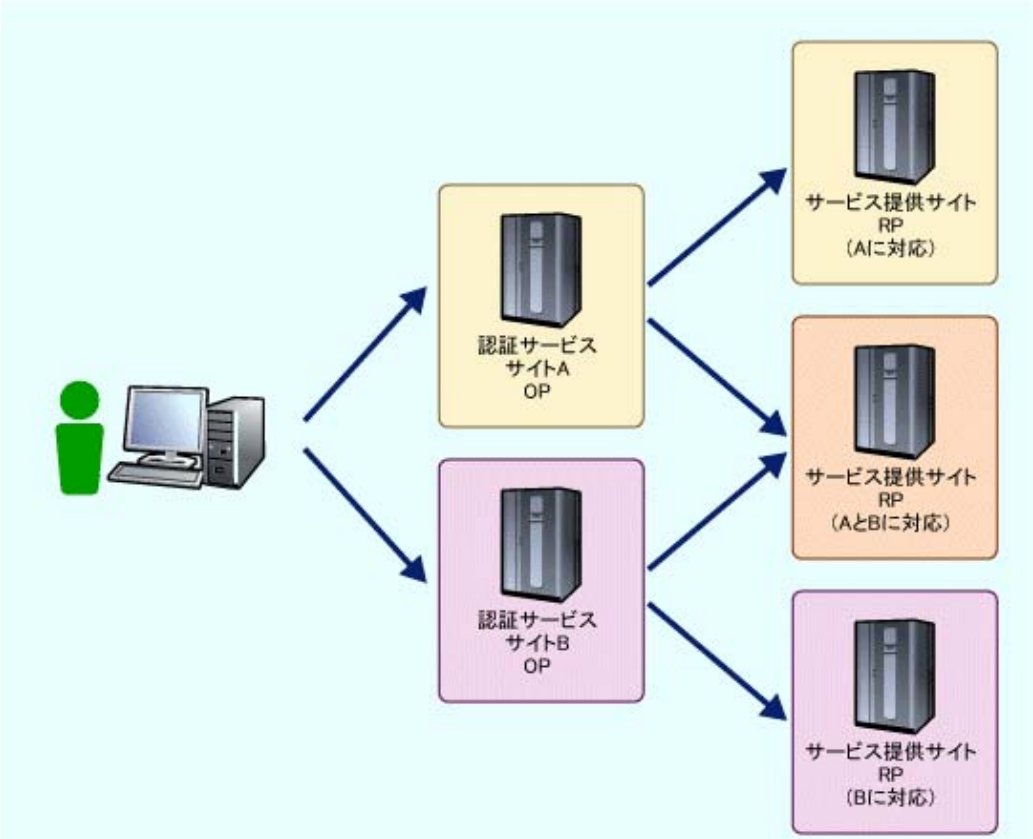
【図3】認証時の情報の流れ

①エンドユーザーは RP のログイン画面で自身の OpenID を入力する（本文中の図 1-1）。
②③入力された OpenID から、対応する OP にアクセスして、鍵の交換を行う。
（この鍵はこれ以降行われる RP と OP 間の情報解読に使われる。重要な情報のやり取りなので、途中で盗み見されたり、改ざんされたりしないように暗号化されている。その暗号を解くのが鍵の役割である）
④RP は OP へ認証を要求する。
⑤エンドユーザーは OP で認証する（本文中の図 1-2 と図 1-3）。
⑥OP はエンドユーザーの認証結果を RP へ連絡。
⑦RP は OP から受け取った認証結果でエンドユーザーの認証を確認してログインを許可する。

■ OpenIDの取得方法

複数のサイトにログインできるとはいえ、1 つの OpenID だけで、OpenID 対応のサイトすべてにログインできるわけではありません。OpenID の提供サイト（OP）はいくつもあり、その OP に対応しているサイト（RP）でなければなりません。例えば Yahoo! Japan の OpenID を所有しているからといって、OpenID 対応の世界中の RP を利用できるとは限りません。利用できるのは Yahoo! Japan の OpenID 対応済みの RP に限られます。

もっとも、複数の OP が提供する OpenID に対応しているサイトも少なくありません（図 4）。



【図4】1つの認証サービスサイト(OP)で複数のサイトの認証機能を提供

OpenID の取得も簡単です。例えば Yahoo! Japan で OpenID を取得するには以下のサイトにアクセスして、申請します（図 5-1）。すでに Yahoo! Japan の ID をもっている方であれば、ログインと画像認証をクリアすることで、その場で OpenID が取得できます（図 5-2）。

【図5-1】Yahoo! JapanのOpenID取得サイト（http://openid.yahoo.co.jp/）

【図5-2】取得したOpenID

取得したOpenIDはURLの形をとっています。「https://me.yahoo.co.jp/」まではOPの情報で、この後がエンドユーザー固有のIDになります。OpenIDを見ると、どのOPかがわかります。それに

より OpenID の信頼度を推し量ることが可能となります。個人ドメインの URL を OpenID に含めることも可能ですが、一般的に知名度があるサイトの方が信頼度が高いとされています。

■ OpenIDの課題

OpenID は利便性を追求するものであり、決してセキュリティレベルを保証するものではありません。逆に OpenID が他人の手に渡ってしまうと、「なりすまし」でいくつもの RP にログインし、個人情報などさまざまな機密情報が盗まれたり、勝手に買い物をされたりする危険性も高いのです。下記は現状考えられるいくつかの課題です。

・情報漏えいの危険性

OpenID を提供する OP の認証サーバがハッキングされれば、登録しているエンドユーザーすべての情報が漏えいしてしまう危険性があります。このため、エンドユーザーの判断に委ねられる OP の選択には特に注意が必要です。

信頼できる OpenID が提供されているサイトの場合、それだけ取得時に複雑な処理が求められます。簡単に取得できる OpenID は信頼性に不安が残りますし、信頼性を求めようとすると取得が面倒になるということです。知名度などを頼りに信頼できる OP を選択するなどは、対策として有効と考えられます。

・誰にでも構築できる RP サイト

RP の選択時も注意が必要です。そのサイトが OP に対応しているからといっても、OpenID でログインするのには注意が必要です。なぜならば、OpenID の API（注 2）は公開されており、RP は誰にでも構築できるからです。OpenID を使用するしないにかかわらず、怪しげなサイトに近づくのは危険であるということです。

もっとも、RP 側では OP の認証情報を受け取るだけで、名前やメールアドレスなどの個人情報は一切受け取れません。このため、RP にログインしてから再度メールアドレスなどの提示を求められることもあります。このときに、要求を拒むことが可能です。

注 2　Application Program Interface：アプリケーションプログラミング時に、比較的簡潔にプログラムできるように設定されたインターフェース、またその規約の集合。

・現状での企業側の負担

RP となった企業側が、OpenID サービスの提供者である OP に振り回される負担は避けられません。OP は、操作性向上やユーザー保護のための工夫を個々に行っているためです。この工夫とは、ユーザーが OpenID でログインする際のアカウント名として長い文字列になりがちな URL 以外に、OpenID 専用のアカウントを設けたり、なりすましやスパム防止のために OpenID アカウント名から OP 側での元の ID を類推できないようにするなどといったことです。しかし、ユーザーのためのこうした OP の仕様の追加や変更は、一方で OpenID でログインするユーザーに対応するための、RP 側での仕

様変更の手間を生みます。中でも OP が認証サービスを中止する、あるいはシステムトラブルがあった場合は、エンドユーザーはサービスを利用できなくなることもあるのです。

以上のような理由により、OpenID に対応しているサイトの数がまだまだ少ないのが事実です。先述のように、完全に 1 つだけの OpenID であらゆる会員制サイトにログインできるわけでもありません。それら情報への対応も課題といえるでしょう。

■ OpenIDのさらなる普及に向けて

日本国内では、2007 年 2 月に「OpenID.ne.jp」が OpenID を発行し、以来 10 社ほどのサイトで OpenID を取得できるようになりました。既出 Yahoo! Japan のほかにも「livedoor Auth」「はてなで OpenID」「mixi」などがあります。

現在は多くのサイトが、ほかのサイトの動向を見定めている導入期ですが、これから OpenID のメリットが認められ、対応するサイトが増えていけば、さらに多くのエンドユーザーが OpenID の利用を開始していくと予想されます。

この OpenID の国内での推進役となっているのが、普及と啓蒙を目的にした団体「OpenID ファウンデーション・ジャパン」です。2008 年 10 月に設立され、会員企業は 50 社に及んでいます（2009 年 8 月現在）。Web 系だけでなく、銀行、保険、運輸、教育機関など幅広い業種から参加しているのが特徴です。OpenID 公開仕様の日本語化やコミュニティー支援、講習会、講演会、セミナーなどを積極的に展開しています。個々のユーザーに対応する Web サービスの増加、クラウドコンピューティングの普及や組織の境界を越えたシステム間の協調など、ID の連携技術は、今後ますます重要な役割を果たすことは間違いありません。OpenID はその性格上、複数の企業や組織・団体が協調や連携なしでは実現できません。その中核を担う OpenID ファウンデーション・ジャパンに期待が寄せられています。

SAML

OpenID と同様に、シングルサインオンを実現するのに SAML（Security Assertion Markup Language）を利用する方法があります。SAML とは、OASIS（Organization for the Advancement of Structured Information Standards、ビジネスにおける情報交換のための技術標準を策定する非営利組織）によって策定された、ID やパスワードなどの認証情報を安全に交換するための XML 仕様です。

OpenID との大きな違いは、SAML は柔軟でかつ強化されたセキュリティのシングルサインオン実現を目的に開発されており、認証情報以外にユーザーの資格や役職などの属性情報と特定のサービスやページへのアクセス権などのアクセス制御情報を伝達することです。これにより、OpenID が実現する認証だけでなく、認証後にユーザーの資格などの属性によってアクセスできるページやサービスを制限したり、また与えられたアクセス権限により資源へのアクセス（読み、書き、実行など）を制御したりすることが可能になります。

参考：強力なSSOを実現するXML認証・認可サービス（SAML）

〈参考サイト〉

OpenIDファウンデーション・ジャパン

☆OpenID 発行サイト（日本語で登録が可能なサイト）

Yahoo! JAPAN

openid.ne.jp

livedoor Auth

はてなでOpenID

JugemKey

mixi

BIGLOBE OpenID

エキサイトOpenID

（2009 年 9 月末現在）

☆OpenID 対応サイト（OpenID で利用可能なサイトのリンク集）

eXcite OpenID対応サイト リンク集

Yahooカテゴリ　OpenID対応サイト

OpenID対応サイト一覧