オンラインコンテンツ本格化時代に必須の認証方式

SSO
Single Sign On

ブロードバンドコンテンツを利用するためには、“ユーザーID”と“パスワード”は欠かせない。しかしあちこちのサイトでこれらを利用していると、手元にユーザーIDとパスワードがどんどん増えていき、しまいには収拾がつかなくなっている読者もいるだろう。またあるサイトのサービスを利用するためにIDを発行してもらうには、名前や住所などを入力し、さらに別のサイトのサービスを利用するときに同じ情報を……と何度も同じ情報を入力するのも面倒だ。

このような問題が発生するのは、あたりまえのことだがユーザーIDがサービスサイトの数だけあることに起因する。ブロードバンドビジネスを普及させるためにはこのような煩雑さを少しでも軽減させる必要があるだろう。その方法の1つが今回取り上げる“シングルサインオン”だ。

text：加畑健志

SSOはおもに3タイプに分類される

一般的にシングルサインオン（以下SSO）は1つのユーザーIDとパスワードで複数のサイトやサービスを利用できるようにする仕掛けのことだとされている。実はそれだけではなく、名前や住所など共通に利用する可能性のある情報を複数のサイトで利用できるようにすることもSSOの目的に含まれる。またSSOはウェブサイトに特有の技術ではない。電子メールやほかのネットワークサービスも適用範囲だが、今回はウェブサイトでユーザーを識別するという場合に絞って話をすすめる。

SSOを使った場合の具体的なメリットとはどのようなものなのだろうか。ユーザー側から見たメリットは以下のようになる。

❶1つのユーザーIDで複数のサイトやサービスを利用できる。
❷何度も同じ情報を入力する必要がない。

そしてサイト側のメリットは以下のようになるだろう。

❶ユーザーがパスワードやユーザーIDを忘れないため、サポートコストが低減できる。
❷共通情報の入力が不要、または削減できるため、ほかのサイトのユーザーを自分のサイトへ誘導しやすくなる。

つまりサイトやサービスをSSOに対応させることでユーザーの利便性を向上させ、同時にビジネスを効率化できるのだ。

このような特徴を持つSSOはおもに3つの方法で実現されている。その3つとは❶代行認証サーバーを使う（図1）、❷認証サーバー同士を連携させる（図2）、❸メタ認証サーバーを使う（図3）というものだ。

代行認証サーバーを使う方式は各サービスのユーザーIDとパスワードを代行認証サーバーに格納しておき、サービスを利用する際はその代行認証サーバー経由でアクセスするというものだ。

認証サーバー同士を連携させる方式は、ある認証サーバーが自分で判断できないユーザーIDとパスワードを受け取ると、それを認証できる別の認証サーバーに送り、自分の代わりに認証してもらう方法だ。RADIUS（Lucent Technologies社によって開発されたダイアルアップ接続で

のユーザー認証方式）とウィンドウズサーバーを組み合わせた認証はこの方法の一例だといえる。

最後のメタ認証サーバーとは各サイトが個別にユーザーIDとパスワードなどを管理するのではなく、メタ認証サーバーにユーザーID発行作業などを依頼し、認証もそのメタ認証サーバーに代行してもらうというものだ。もちろん各サイトは自社の顧客である個々のユーザーIDは管理しているが、メタ認証サーバー内のすべてのデータを見ることはできないようになっている。

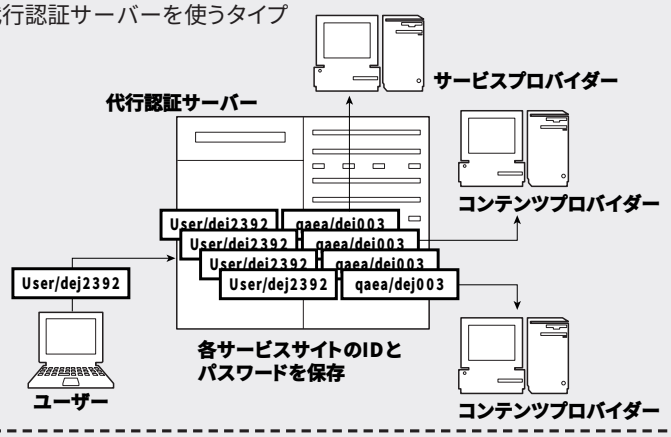
メタ認証を使う「パスポート」とサーバーを連携させる「リバティ」

SSOが価値を発揮するためには1つのユーザーIDでどのくらいの数のサイトやサービスを利用できるかにかかっているといっても過言ではない。コンテンツビジネスを含むインターネット上のビジネスを発展させるためにSSOが重要であることは業界も認識している。言い換えるとSSOのスタンダードを握るということはコンテンツビジネス市場に対して非常に大きな影響力を及ぼすといってもいい。そしてこのような背景に対し、マイクロソフトとサン・マイクロシステムズはそれぞれ異なったアプローチで覇権を争っている。

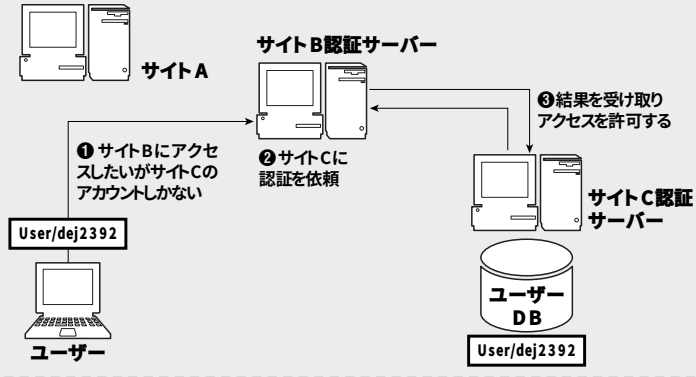
マイクロソフトの「パスポート」というサービスは同社が運用する、2億人を超えるメタ認証サーバーを使うことでSSOを実現しようとしている。さらにSSO技術のウィンドウズOSへの標準搭載や、「パスポート」対応のSSOサイトを構築するためのSDKもリリースするなど活発な動きを見せている。また「パスポート」が閉鎖的であるという批判を受けたことから、後述の「リバティアライアンス」との接続も可能にし、さらに「TrustBridge」（他社システムからアクセスしてきたユーザーの身元をSSOで認証する技術。自社のリソースを特定の企業に公開する際に効果を発揮する）のリリースで企業同士のSSO利用も視野に入れている。

対するサン・マイクロシステムズは「リバティアライアンス」というSSOの方式で対抗している。「リバティアライアンス」は認証サーバー同士を連携させるアプローチを採用している。そして規格を公開して「リバティアライアンスプロジェクト」という団体も結成している。この団体は現在、ソニー、NTTドコモ、AOLタイムワーナー、ノキア、ゼネラルモーターズといった企業や米国のいくつかの公共機関などを加え、160社を超える規模に成長している。この団体のおもな活動は規格立案にあったことから、具体的な製品の登場は少なかった。しかし2003年4月にHPが対応製品をリリースするなど、ここにきてベンダーの市場参入が活発化し始めている。

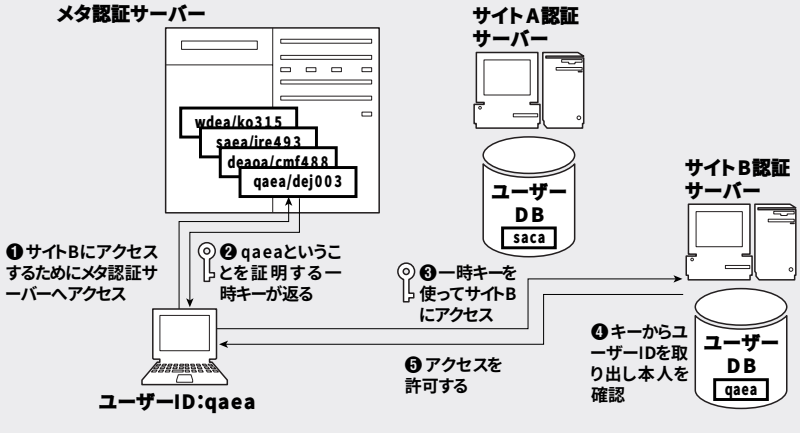
■図1 代行認証サーバーを使うタイプ



■図2 認証サーバー同士が連携するタイプ



■図3 メタ認証サーバーを使うタイプ



「パスポート」は巨大データベースアクセスに必要なプロトコル

マイクロソフトの「パスポート」は巨大なユーザーデータベースへのアクセス方法を定義したプロトコル、つまり“約束事”だということができる。

その“約束事”をわかりやすく説明するために、ユーザーのあるサイトへの登録の手順を図4に示す。ポイントはPUIDと呼ばれるユニークなIDを使うということだ。このPUIDはユーザーが「パスポート」上にアカウントを作成したときに生成され、各サービスサイトはこのPUIDを使うことでユーザーの認証を行う。言い換えるとサービスサイトは自分のサイトにアクセスしてきたユーザーが持つPUID（の入ったcookie）を読み取ることで、アクセスしてきているのが該当ユーザーであるということを識別できることになる。

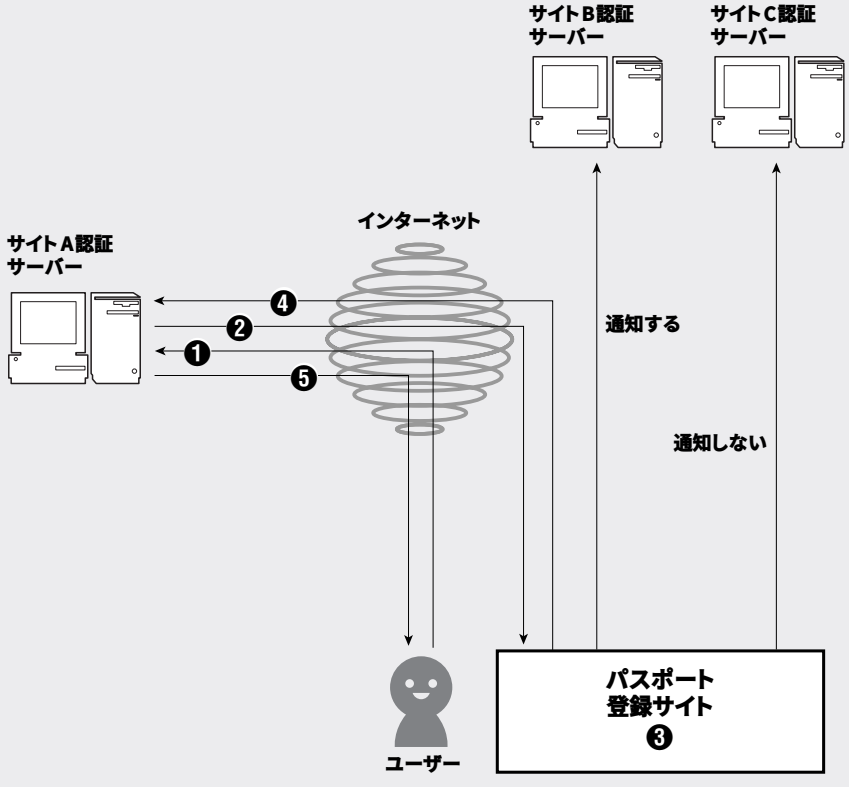
実際はこのPUIDとともに、そのサイトが必要とするプロファイルを加えたcookieと認証チケット情報の入ったcookieが使われる。これらのcookieは「パスポート」サーバーによって対象サービスサイト用暗号化キーで暗号化されている。そのためこのcookieを第三者が入手しても使うことはできない。

住所や名前などのプロファイルは、ID作成時に入力する必要はない。これらはサービスサイトを利用する際に必要になったときに入力が要求される。またPUIDにはプロファイルや資格情報が一切含まれていないので、PUIDをキーにそれらの情報にアクセスすることはできない。

「パスポート」対応のサイトを利用する際にユーザー側に求められるのはcookie、SSL、JavaScriptが使えるブラウザーのみ。また「パスポート」のアカウント作成自体にも費用はかからない。これに対し、サービスサイトを「パスポート」対応にするためには、サイト自体の認証システムを改造しなければならない。そのためのSDKはマイクロソフトから無償でダウンロードできる。ただし登録が必要なのと、ベリサインなどの公的デジタル証明書も必要になるため気軽に試すというわけにはいかないだろう。

さらに実際に運用するためにはサイトの存在証明用に18万円と利用料1,200万円を毎年マイクロソフトに支払わなくてはならない。非常に高いように思えるが、「パスポート」が管理する2億人以上のユーザーに対して一元的なサービスを提供できること、さらにマイクロソフトもプロモーションに協力することを考えれば理解できる範囲といえるだろう。

■図4「パスポート」の登録認証プロセス



❶この例ではユーザーはサイト Aを参照し、［サインイン］ボタンをクリックする。
❷サイトAはユーザーをパスポートの登録サイトに誘導する。ここでユーザーはサインイン先（ここではサイトA）以外の パスポート 対応サイト（サイトB、Cなど）に自分のプロファイルなどの情報を通知するかどうかを選択できる。
❸ユーザーが使用条件を読んで同意した場合、自分の情報が書き込まれたフォームをパスポートの登録サイトに送信する。
❹その後、ユーザーは暗号化された認証チケットとPUIDを含むプロファイル情報が添付された状態でサイト A に再度アクセスすることになる。
❺サイト A は暗号化された認証チケットとプロファイル情報を復号化し、登録プロセスを続行。サイトへのアクセスを許可する。

認証サーバーの連携を定義する「リバティアライアンス」

サン・マイクロシステムズが提唱している「リバティアライアンス」は認証サーバー（IDプロバイダーと呼んでいる）同士が連携する方法を定義する仕様と言える。このリバティアライアンス仕様に加え、認証情報などを伝達するフレームワークSAML（Security Assertion Markup Language）仕様を使うことで企業間でのSSOにも対応している。

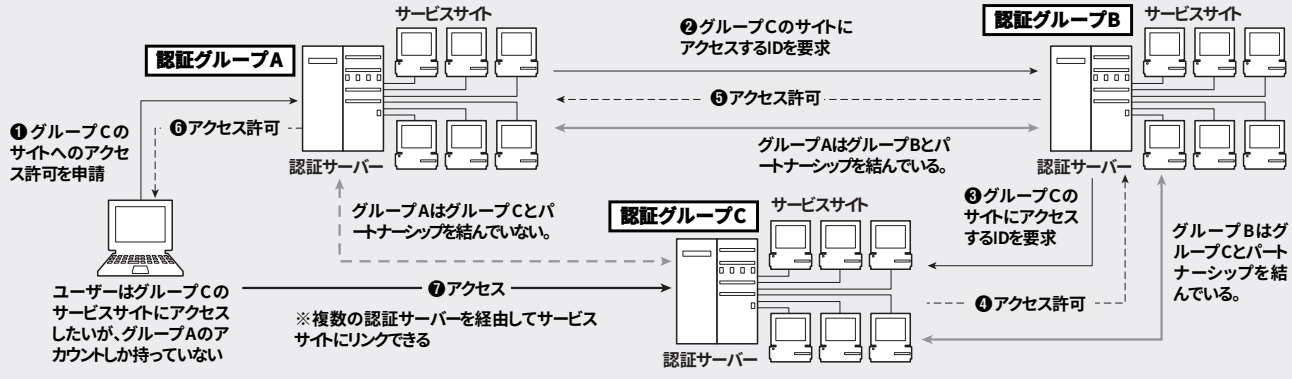
「リバティアライアンス」のポイントはフェデレーションと呼ばれる「信頼の輪」だ（図5）。これは1つの認証サーバーが複数のサービスサイトを束ね、さらに複数の認証サーバーが1つの認証グループを構成し、あたかも1つの認証サービスとして動作するイメージのことを指している。ユーザーはこれらのフェデレーション（認証グループ）のどれに登録するかを選ぶということになる。認証グループ同士の結びつきをリンクと呼ぶ。図5にもあるように、複数のリンク（経路）でコンテンツなどの利用が可能な場合、ユーザーが各フェデレーションのどのリンクを有効にするかを自ら決めることができる。それぞれの認証サーバーはクライアント／サーバー型認証方式KerberosとSAMLを使って認証情報や個人情報をやり取りする。このやり取りの際にどの個人情報を渡していいかどうかは前述のリンクを行う際に決めることになるが、それはユーザーが定めたセキュリティーやプライバシーポリシーがベースになる。

今後は図6に示すような世界を実現するために、アイデンティティーサービスのサイト情報を提供する機能やユーザーの属性情報を交換するための機能などの策定と実装が行われることになっている。

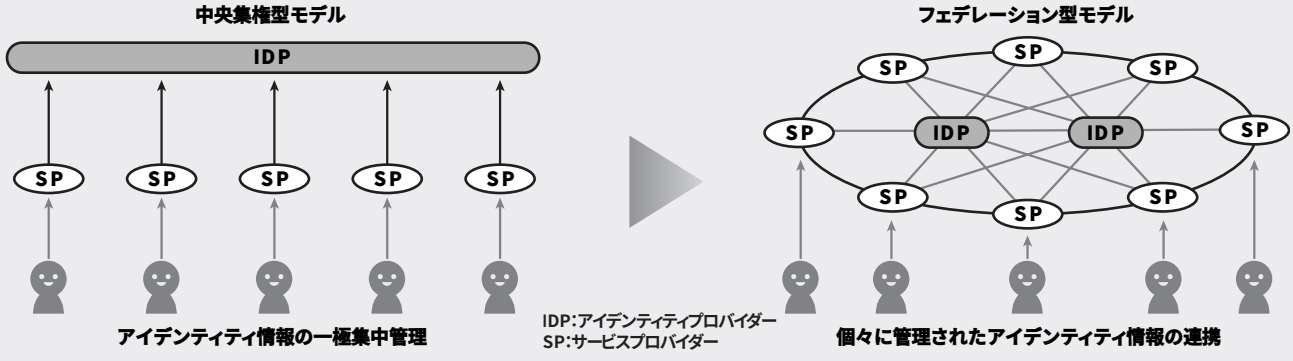
ユーザーが「リバティアライアンス」を利用するための条件は「パスポート」と同じく通常のウェブブラウザーがあればいい。また「リバティアライアンス」に対応したサイトを作成するためには、この規格に準拠した製品を購入し、サービスサイトの認証システムと組み合わせることになる。あるいはLiberty Version1.1やSAMLの仕様が公開されているため自力で行うことも可能だが、SDK などが用意されているわけではないので、1から作るのは簡単というわけではない。

ただ対応製品の動作環境がJavaであるものが多いため、適用できるサイトの制限は「パスポート」に比べると広いといえるだろう。

■図5「リバティーアライアンス」の進めるフェデレーション



■図6 フェデレーション型モデルへの進化



ユーザーIDを管理するアイデンティティプロバイダーが、それぞれ連携することで、ユーザーが多くのサイトを利用できるような仕組みを作ろうとしている。

現実にコンテンツプロバイダーがSSOを利用しようとする場合の参考として、既存のSSOサービスと、すでにそれを利用したサイトをいくつか紹介する。

マイクロソフトの「パスポート」を利用できるサイト

オムニドメインが提供する総合型販売サイトサービスを利用すると「パスポート」対応サイトの構築が簡単に行える。そのサービスを利用したサイトの1つが自転車の製作を手がけるnh-guild.comだ。このサイトでは商品の購入やメールマガジンの購読などに「パスポート」を使用する。通常であれば「パスポート」対応サイトの構築にはコストも時間もかかるが、このようなサービスを利用することで迅速に自社のサービスを「パスポート」対応にできるだろう。また東京三菱クイックアラートも「パスポート」に対応した新サービスだ。サービス自体はマイクロソフトのMessengerクライアントを利用した情報のポップアップ表示サービス「.NET Alert」サービスを使うものだが、ユーザーは自分の「パスポート」を使って、認証作業を行いながら、マーケット分析、為替情報など契約したサービスからリアルタイムに情報を受け取ることができる。

リバティアライアンスに対応したサイトを構築するための製品群

リバティアライアンスのメンバーであるノベルが提供しているのはSSO対応を可能にするウェブセキュリティーソフト「iChain」だ。「iChain」は「iChain」やリバティアライアンスに対応したサーバーと連携してSSOを実現できる。大きなものでは世界最大規模の航空会社連合であるスターアライアンスの社内システムにSSOを実現するコンポーネントとして利用されている。

またHPは同社のセキュリティーソフトウェア「hp IceWall SSO」でSSOを実現している。この製品を使ったサービスの1つにNTTデータ保険会社共同ゲートウェイがある URL 01 。ここでは、複数の保険会社に対して代理店が1つのアカウントでアクセスできるようなソリューションが実現されている。

アダルトサイトの年齢認証でも必要とされるSSO

日本ではあまり知られていないシステムだが、米国ではAVS（Age Verification Service）というある種のSSOサービスがある。Age Verificationという名前のとおり、基本的には成人向けコンテンツを提供するサイト向けのサービスになる。このサービスを利用したいサイトはAVSをと契約する。各サイトはユーザーIDとパスワードは管理しない。つまりAVSがアクセス制限とアカウント管理を提供することでSSOを実現しているのだ。そのユーザーIDとパスワードはAVSに加盟しているサイト全部で共通しているため、1つのアカウントですべてを利用することができるというわけだ。

マイクロソフトの「パスポート」と似ているように思える。しかし「パスポート」の場合、ユーザーの身元とサイトを保証し、実際のアクセス制御は各サイトが行う点が大きく異なる。

URL 01 http://www.jpn.hp.com/biz/casebank/cases/ntt_data/

「パスポート」を利用した事例

オムニドメイン社の提供する総合型販売サイトサービスを利用しているnh-guild.com。「パスポート」を低価格で導入する手段だ。
URL http://www.cahincast.com/

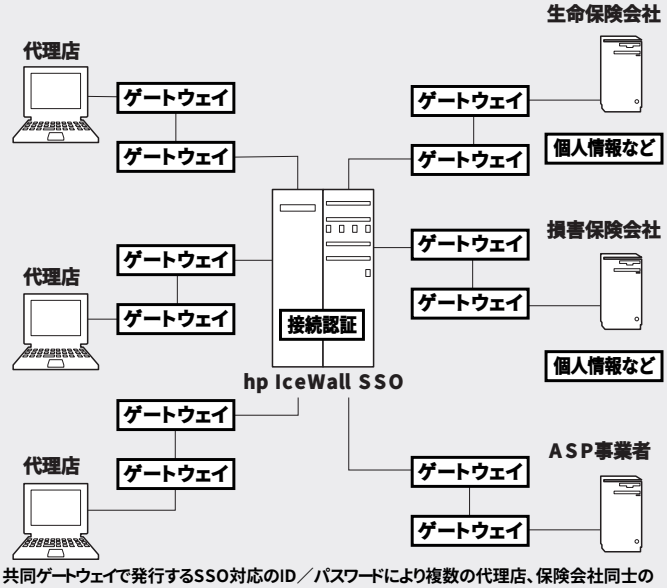
東京三菱クイックアラートはMSN メッセンジャーに外国為替相場情報や株式に関する情報を送信するサービスで、.NETAlertを利用する。リアルタイムでさまざまな経済情報を得ることが可能。
URL https://alerts.btmportal.com/BTMAlerts/default1.aspx/

リバティアライアンスに準拠した製品

ノベルが提供するウェブセキュリティーソフト「iChain」。スターアライアンスなどですでに使用されている。
URL http://www.novell.co.jp/products/ichain/

HPは同社のセキュリティーソフトウェア「hp IceWall SSO」。NTTデータ保険会社共同ゲートウェイなどに利用されいる。
URL http://www.jpn.hp.com/hpc/sp/icewall/

■図7「hp IceWall SSO」を利用した保険会社共同ゲートウェイ



共同ゲートウェイで発行するSSO対応のID／パスワードにより複数の代理店、保険会社同士のシステムを接続する。

将来SSOの普及を妨げかねないポイントはここだ

複数の‘個人情報’を選択できないとSSOの普及速度は鈍る

先日クレジットカードを1枚だけなくしてしまった。新しいカードと古いカードを間違えて捨ててしまったようだ。カード会社に電話をして再発行の手続きを行ったあとで、そのカードで登録している各種サービスの変更手続きをしようとしてちょっと困ってしまった。新しいカードと古いカードではクレジットカード番号が違うため、新しいカードが来て、番号を確認しないと変更手続きができなかったのだ。

もしSSOが実現していたらこの情報（カードの番号の変更）を各サイトに通知しなくても自動的にすべて変更してくれて便利なのかもしれない。ただし、筆者はサービスサイトによってクレジットカードを使い分けている。現状のどのSSOソリューションを見てもユーザーが自分の情報（住所やプロフィール）を各サイトで別々に設定できるようにはなっていない。

セキュリティーやビジネス状の理由により、サービスやサイトごとに登録する住所やカード番号、メールアドレスなどを変えるというパターンはよくある。つまりネット上では複数の人格（のようなもの）が存在しているということになる。また現実社会であっても買い物の種類や場所によってクレジットカードを使い分けるという場合もある。ところが現状のSSOはサービスサイトの種類によってどの情報をそこで使うべきかを自動的に判断してくれるほど洗練されてはいない。

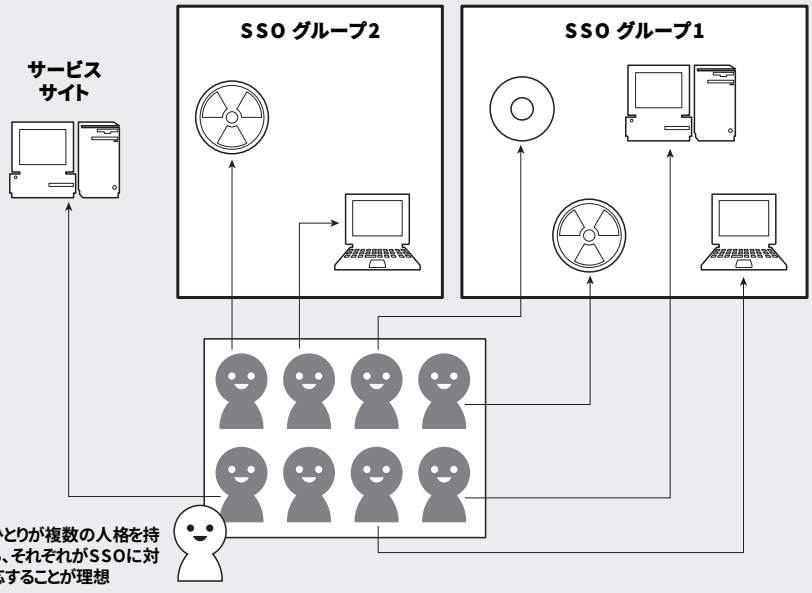
SSOを使うことでコンテンツサービスやオンラインショッピングが便利に使えるようになることは間違いない。しかしSSOの導入で、ユーザーの選択肢がせばまったり、より複雑な手順を要求されるのではまったく意味がない。図8のように一人が複数の人格をもちつつSSOが利用できるようになってこそ、SSOに乗り換えることができるといえるだろう。

「一極集中」vs「分散」。どちらが安全か判断できない

SSOを自社のビジネスに利用する場合を考えてみる。ビジネスを行う際に信頼性は非常に重要なポイントだ。ユーザーが自社のサービスを利用しようとしてもSSOがダウンしているとどうしようもない。SSOの場合、そのリスクは複数の業者に渡ることになる。認証サーバー同士を連携させるような分散型のSSOであれば局地的な被害で済むかもしれないが、別の問題がそこに潜んでいる。その理由とはあなたのサービスサイトが悪者になる可能性があるということだ。

逆説的なるが、SSOの停止による被害が広ければ広いほど、各サービスサイトへのクレームは小さいと考えられる。つまり障害原因がSSO自体であるという認識が広く伝わる＝私だけではない＝サービスサイトは悪くないということだ。ところが分散型の場合、被害が小さい＝サービスサイトに問題があるのではないか？ということになるのだ。ところがこれにこりてコンテンツプロバイダーなどが別のSSOに乗り換えようと思っても、ユーザーIDをすべて移行しなければならないという問題に直面する。このユーザーIDはそれぞれの認証サーバーが発行しているので、認証サーバーが変われば、ユーザーIDも変わるということになり、現実的には不可能ということだ。つまりそのSSOに囲い込まれてしまうということになるのだ。ほかにも、同じSSOを使っている別の会社がなんらかの情報漏洩を犯したとしてもSSOを替えることができないのは致命的になりうる。企業のSSO乗り換えが難しいという点も普及を妨げる大きなポイントになるだろう。

■図8



［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

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、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）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、写真の撮影者、イラストの作成者、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収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用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する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時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が、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的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。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp