ウェブサイトのサービスを利用するとき、IDとパスワードを設定して、
氏名や住所などの本人情報を入力、また別のサービスを
利用するときにも同じようにIDとパスワードを……というように延々とIDとパスワード、
本人情報を入力し続けなければサービスを受けられない、
といった経験のある人は少なくないでしょう。
もっと簡略に、しかもプライバシーやセキュリティは守られたまま、
インターネットの世界に点在するサービスへの認証を行う方法はないのでしょうか?
このような複数のサービスをより簡単に利用するための認証システムを
研究・開発している秋山豊和先生に、最先端の認証システムについてお話を伺いました。

ネットワークメディア学科
秋山　豊和 准教授

より安全で快適な認証システムを目指して

利便性も欲しい プライバシーの保護も大事

情報技術の進展によりインターネットを利用したさまざまなサービスが拡充されています。ところが、サービスが増えるに従って、利用者本人であることを確認する頻度も増えています。複数のIDとパスワードを管理したり、登録のたびに個人情報を入力したりという手間はもちろん、初めて利用するサービスに個人情報を教えて本当に安全なのかという心配も出てきます。

信頼できるサイトに1度サインインしたら、後はずっと「本人」としてサービスを利用できれば、飛躍的に便利になります。しかし、本人であることを証明する情報がサービス間で自由にやり取りされると、個人情報が危険に晒されてしまいます。利便性を高めれば安全性が犠牲になり、安全性を重視すると不便になってしまうジレンマがありました。

安全で便利なシングルサインオン (Single Sign On: SSO)

図1のように、ユーザは利用したいSP(Service Provider)にサインインします。SPが本人認証を行うIdP(Identity Provider)に問い合わせると、IdPは「確かに本人であることを保障するチケット」を発行し、パスワードなどユーザの個人情報を知らせることなく、確かに本人であると伝えるのです。ユーザが許可すれば個人情報など必要な情報をSPに渡すこともできます。本人認証とインターネット上のサービスとを分離することで、安全性を確保しつつ、1度の登録で複数のサービスを利用できるという利便性も得られます。

複数のサービスを 組み合わせるためのSSO

SSOの応用により、図2の「OAuth」のように、ユーザの権限をSP間で受け渡して、複数のSPが連携したサービスの提供も可能になります。

写真管理サイトとプリントサービスとの例を見てみましょう。ユーザはプリントサービスのサイトSP1にサインインして写真管理サイトSP2に保存している写真のプリントを要求します。しかし、SP1はSP2から勝手に写真を取ることはできません。そこで、SP1はユーザを経由してSP2にアクセス、ユーザはSP2からSP1への権限委譲を許可します(この場合は写真の提供許可)。SP1はSP2から必要な写真だけ受け取れるようになります。

SP2がSP1に発行するのは「一定時間、許可した写真へアクセスする権限のチケット」です。そのため、悪意のある人物がSP1を乗っ取ったとしても、SP2にあるユーザの写真は守られます。この技術には、さまざまなサービスの組み合わせにより、今までにないサービスの創出が期待されています。

たくさんの計算機を 利用するためのSSO

権限の委譲は「グリッドコンピューティング※」にも応用されています。

多数のコンピュータ間での計算の受け渡しの度にユーザが認証を行うのは手間も無駄も大きく、分散しているコンピュータ群に認証用の個人情報をばら撒くのも危険です。そこで、IdPが発行したチケットを「Proxy証明書」(図3)を使って、計算結果とともに受け渡ししながら、最後にユーザのもとに提供します。「Proxy証明書」は異なるコンピュータに処理を依頼するたびに発行される、より限られた権限をもつチケットなので、途中で奪われても被害は最小限で済みます。

認証システムの将来

サービスごとに認証を行うのが一般的であった時代から、認証をひとつの独立したシステムとして捉える時代に変わりつつあります。

認証という情報技術のインフラが共通化していくことで、エンジニアはインフラ整備からサービス向上に力点を移すことができるようになります。そのために、どうすればいいのか、さらに考えていきたいと思います。

※インターネット上に分散する多数のコンピュータを1つのチームにして、計算結果を受け渡しながら高度な計算を実行したり、大規模な記憶領域を作り出したりするコンピュータの利用方法。

図1　シングルサインオンの技術

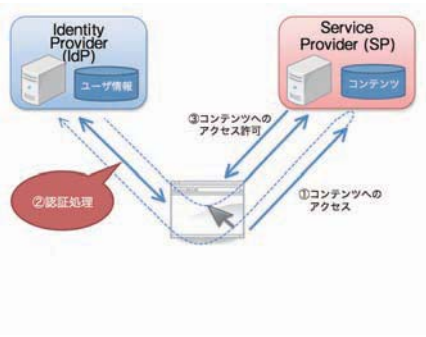

図2　サービスへの権限委譲(OAuth)

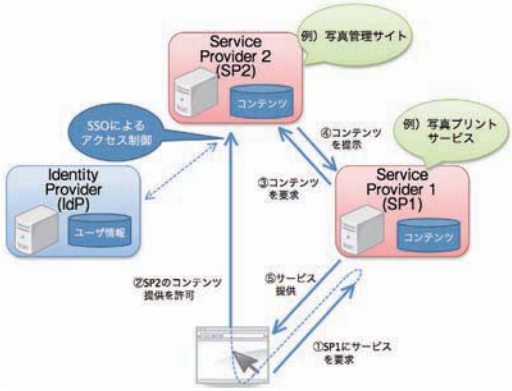

図3　サービスへの権限委譲(Proxy証明書)