LM-9

シングルサインオンにおけるプライバシ保護について

Protecting Privacy in Single Sign-On

岡田 浩一† 大西 真樹† 冨士 仁†
Koichi Okada Masaki Onishi Hitoshi Fuji

1. はじめに

シングルサインオン（以下 SSO と略す）機能とは、複数のサービスを利用する際に必要となる認証を一度のみで済ますための機能である。この機能を、インターネット上の複数の Web サイトにまたがって提供することは、複数の Web サイトが自動連携する Web サービスの普及等のために必須であり、Microsoft[1]や Liberty Alliance Project[2]等が開発を進めている。この様に SSO の必要性が注目される一方で、SSO 機能の実装方式の中にはユーザを識別可能な情報を Web サイトに送信するものが多いため、プライバシ上の問題が懸念されている。

本稿では、SSO におけるプライバシ上の問題点を分析し、この問題を解決するための方法の一例として、筆者らの提案する SSO 実現方式である VPN-exchange 方式[3][4]を改良する方法を示す。VPN-exchange 方式は、複数のエクストラネットへの安全なアクセスと SSO を組み合わせたものであり、従来の SSO 方式よりも高いセキュリティを確保可能であるため、この方式においてプライバシ上の課題を解決することは意義があるといえる。

2. シングルサインオン方式

SSO を実現する方式は以下の 4 種類に分類される。

(1) クライアント方式 (Novell SSOv2 [5]等)

クライアント端末にインストールされたシステムが自動的に認証を行なう方式。サイト毎に登録した ID/PW を複数格納するもの、Web ブラウザのクッキーを使って同一サイト内でのシングルサインオンを実現するもの、電子証明書や、これを発展させた権利証明書[6]等を利用するもの等がある。

(2) サーバ方式 (Kerberos [7]等)

認証を行なったサーバが、他のサーバにユーザ ID もしくはアクセス権利に関する情報を伝達する方式。

(3) プロキシ方式 (Soliton Webgate [8] 等)

プロキシサーバに対して認証を行ない、その結果に応じてプロキシサーバがアクセス制御を行いつつ通信を中継する方式。

(4) VPN-exchange 方式 (筆者らの既提案方式[3][4])

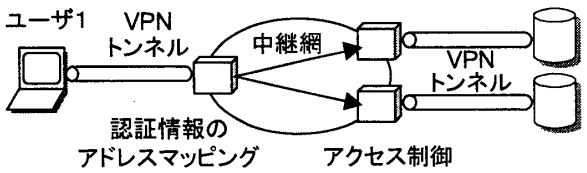

図 1. VPN-exchange 方式

各ユーザと中継地点との間で暗号コネクション（VPN トンネル）を構築し、その際に行なった認証の結果に応じてユーザ間のアクセス制御を行なうことにより、複数のエクストラネットへのアクセス時の SSO を実現する方式。プロキシ方式の構成をネットワークレイヤで実現することによりアプリケーション非依存性と高速性を確保し、中継地点内でパケットの送信元 IP アドレスとして認証情報を埋め込むこと（アドレスマッピング）により認証結果に応じたアクセス制御を複数の装置に分散可能にし、高いスケーラビリティを確保している。

SSO 方式として、ログイン制御の他に、氏名や住所等のユーザ情報を流通させる仕組みを含めたものもあるが、本稿ではログイン制御機能に限り検討の対象とする。

3. シングルサインオンにおけるプライバシの脅威

複数のサイトにまたがって SSO 機能を実現する場合において、ログイン制御を行なう際には、ユーザのプライバシの観点において以下の脅威がある。ここで、SSO における一回目の認証を行なう相手は信用し、通信先サイトは基本的には信用しないことを前提として考える。

(1) 同一サイト内でのユーザ行動の関連づけ

同一のユーザが同一サイトにおいて実際に行なった全ての行動が、そのサイトにおいて同一ユーザのものであることを認識されることが不都合な場合がある。たとえば、サイト内で匿名投票などを行なう場合がこれに該当する。Web ブラウザのクッキーでユーザのアクセスを管理している場合では、ユーザに無断でユーザ識別情報が送信されており問題となることがある。よって、SSO を利用して自動的にユーザ ID が送信されている場合でも、ユーザからの要求に従って一時的にユーザ ID の送信を停止し匿名でアクセスできるようにする必要がある。ここで、サイトに対して匿名でアクセスを行なう場合でも、予め指定されたユーザからのアクセスだけを許可することができれば、セキュリティを高めることができる点で有効である。

(2) 複数サイト間でのユーザ行動の関連づけ

同一のユーザ ID を複数のサイトで共有する場合、それらのサイトが結託することにより、ユーザが意図したよりも多くの情報が流出する可能性がある。例えば、あるサイトに対して氏名や住所を送信していない場合でも、そのサイトと同じユーザ ID を共有しているサイトにこれら氏名や住所等の情報を提供している場合、両者が結託すると、前者のサイトにおける行動に対して氏名や住所を関連づけることが可能となってしまう。同一の電子証明書を認証目的のために複数のサイトで利用する場合、この問題が発生する。この問題に対処するためには、同一ユーザに対してサイト毎に個別の ID を用意し、ユーザの同意なしでこれらの ID 間の関係が流出しないようにする。

(3) 送信元情報の流出

SSO の使用、非使用にかかわらず、ユーザから送信されたパケットの送信元アドレス等から、ユーザの所属組織名や、ユーザ

† NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

同一性等のプライバシ情報が流出する場合がある。クライアント方式およびサーバ方式では、ユーザは直接通信先にアクセスを行なうため送信元IPアドレスの情報が流出してしまう。[6]における方式でも、この問題は解決されていない。プライバシ保護のために、これらIPアドレス等の情報を隠蔽する必要があり、それと同時に、匿名性を利用した犯罪を防止するために後から送信先ユーザを特定することができるようにする必要もある。

4. VPN-exchangeにおけるプライバシ保護

プロキシ型SSOは前節に示したプライバシ上の問題点を持たない点で優れているが、スケーラビリティおよびアプリケーション依存性の点等で問題がある[4]。VPN-exchange方式は、プロキシ型SSO方式におけるこれらの問題点を解決するように拡張したものである。しかし、中継地点において、ユーザ認証の結果に応じて送信元IPアドレスをユーザ特定可能なアドレスに変換するため、中継地点を経由して通信を行なった場合、通信先サイトにおいてパケットの送信元IPアドレスによって、ユーザを一意に識別できてしまうことになる。これにより前述した問題点(1)、(2)および(3)を引き起こす可能性がある。よって、プライバシの観点では、VPN-exchange方式はプロキシ方式の利点を損なっていることになる。

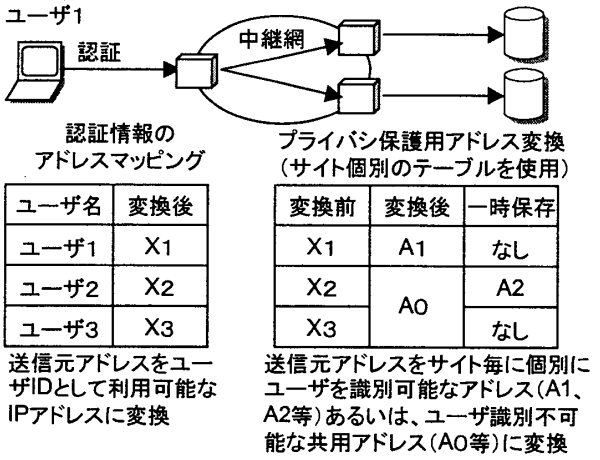

図2. VPN-exchangeにおけるプライバシ保護

そこで、これらのプライバシ上の問題点を解決するために、アクセス制御を行なう送信先側ゲートウェイにおいて、送信元アドレスを隠蔽するためのアドレス変換を実施する。この時、全ユーザで共用のアドレスへ変換することにより通信先サイト内においてユーザを識別できないようにすることと、相手サイト内でのみ一意に識別可能なアドレスに変換することの両方に対応可能にする（図2)。この様にアドレスを隠蔽する場合でも、中継地点から出るパケットのアドレス変換前にアクセス制御を行なうことにより、匿名性を確保しつつアクセス制御を可能にする。また、ユーザを識別できる状態からできない状態に変更した場合でも、後で再び識別できるように復元することができるように、識別用のアドレスを一時的に保管できるようにする。

そして、図3の様に、このアドレス変換の設定のインタフェイスを用意する。このインタフェイスの呼び出しを、ユーザからだけではなく、通信先サイトからも呼び出してユーザによる設定変更を促すことができるようにすることにより、容易な設定変更を可能にする。また、アドレス変換の内容とその時間を記録することで、後で任意のアドレスの使用者が特定できるようになる。

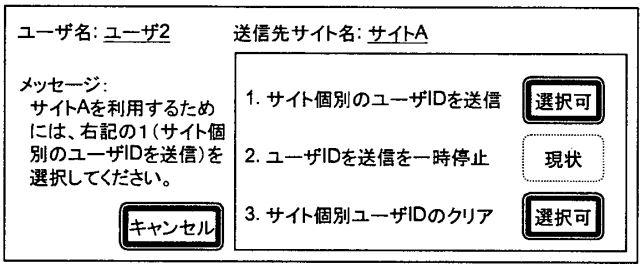

図3. ユーザ情報送信設定インタフェイスの例

5. まとめと今後の課題

本稿では、SSOにおけるプライバシ確保のために、(1)相手サイトへのユーザIDの送信および停止を指定可能にし、かつユーザIDの送信を停止した場合でもアクセス制御を可能にし、(2)サイト毎に個別のユーザIDを利用し、(3)送信元情報を隠蔽しつつ、後で利用者の追跡を可能にするように記録する、という機能が必要であることを明らかにし、筆者らが提案するVPN-exchange方式にこれらの機能を追加する方法を示した。

本稿で述べたとおり、アドレス変換は、消費するグローバルアドレス数を抑えるためだけでなく、プライバシ保護の観点から必要であるといえる。これは、潤沢なアドレス空間を持つIPv6を利用する環境においてもアドレス変換が必要であることを意味する。アドレス変換にはアプリケーション毎の個別対応が必要になるという問題があるが、この問題をRSIP[9]やUPnP[10]等の方法で解決する方法が提案されており、これらを本稿で述べた方式へ導入する方法について、今後検討をすすめる予定である。

参考文献

[1] Microsoft .NET passport, http://www.passport.com/
[2] Liberty Alliance Project, http://www.projectliberty.org/
[3] 岡田・冨士, "スター型End-to-end-VPNを提供するVPN-exchange方式のスケーラビリティ向上", コンピュータセキュリティ研究会(CSEC-16), 情報処理学会, 2002.
[4] 岡田・冨士, "安全かつスケーラビリティが高いシングルサインオン方式", SCIS2002, 電子情報通信学会, 2002.
[5] Novell Single Sign-on 2.0, http://www.novell.co.jp/products/sso/
[6] 飯田他, "ユーザを識別しない認証方式の実装と評価", 情報処理学会第62回全国大会, 3-301, 2001.
[7] Kohl 他, The Kerberos Network Authentication Service (V5), RFC1510, 1993.
[8] Soliton Webgate, http://net.soliton.co.jp/products/soliton/webgate/webgate.html
[9] Borella 他, Realm Specific IP: A Framework, RFC 3102, 2001.
[10] Universal Plug and Play, http://www.upnp.org/