メールアドレスを利用したWeb認証の自動化に関する提案

川人 彰文† 酒徳 哲† 北形 元‡ 木下 哲男§
東北大学 大学院情報科学研究科† 東北大学 電気通信研究所‡
東北大学 サイバーサイエンスセンター§

1. 序論

本稿では、メールアドレスを利用したWeb認証の自動化を提案する。

近年，ネット通販やブログ，SNSといった様々なWebサービスが展開されている．これらのサービスでは，サイト毎にアカウントを作成・登録して利用するという方式が一般的であるため，ユーザーIDやパスワードを，ユーザー自身が管理する必要がある．そのため複数のサイトを利用する場合，パスワードの管理が煩雑化したり、またサイト毎に認証をおこなう必要があり、ユーザーの負担となっている．

こうしたユーザーの負担を軽減するためのシステムとして，シングルサインオンという仕組みがある．これは1回の認証で複数のサービスへアクセス可能にする仕組みのことで、この仕組みの利用により，ユーザーの使用するIDとパスワードは1組だけで済む．この仕組みは主に企業の社内システム向けで普及してきたが，近年の認証を必要とするWebサービスの増加に伴い，提供者の異なるWebサービス間でのシングルサインオンの実現への期待が高まっている．

そこで本稿では，アカウント作成時やパスワード紛失時に従来から用いられてきたメールアドレスによる本人確認を自動化し，通常のログイン時にも利用可能とする手法を提案する．これによりサイト毎のユーザーIDやパスワードの管理を不要とし，ユーザーの負担を大幅に軽減する．提案手法について述べた後，提案に基づいたシステムの設計について述べる．

2. 関連研究

2.1 ローカルディスクに情報を保持

Webサービス利用時におけるユーザーの負担を軽減するためのアプローチとしては，ローカルディスクにユーザーIDとパスワードの情報を保持しておいて，ログインページにアクセスする度に自動的に入力するという方式が挙げられる [1, 2, 3]．これはWebブラウザの機能として採用されている例や，アプリケーションとして実現されている例も多く，サーバー側の機能追加や変更は必要ないため，導入が簡単で運用コストも発生しない．その一方で，セキュリティに関する情報をローカルに保持するという性質上，完全にパーソナルな計算機上でしか使用することはできない．共有パソコンに個人情報を入力しておくことは，セキュリティ的に問題がある．

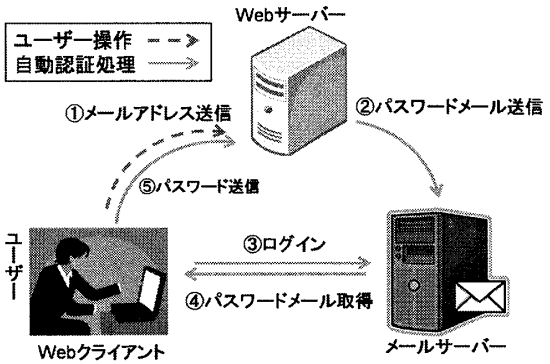

図 1: 提案手法の概要

2.2 第三者による認証

元来Webサービスにおけるユーザー認証は，サービス提供者とユーザーの間のやりとりだけであったが，前節の方針とは逆に，Webサーバー上に認証用の情報を保持しておくというアプローチも存在している．サービス提供者，およびユーザーとは異なる第三者のサーバー等を利用して認証をおこなうことで，シングルサインオンを実現する仕組みが提案されている [4, 5]．OpenID [5] では，URL形式の共通IDを発行・認証するための専用サーバーを用いて，対応しているWebサービスへのログイン時に認証処理を代行する．

こうした第三者を介した認証手法では，サービス提供者とID提供をおこなう第三者との信頼関係が不可欠であるため，導入の際は対応作業が必要となる．また，情報を集中管理するためのサーバーを新たに設置・運用する必要があるため，導入や運用にはコストがかかる．

3. メールアドレスを利用したWeb認証の自動化

3.1 概要

本研究では，メールアドレスを利用したWeb認証を自動化し，通常のログイン時にも利用可能とする手法を提案する．

まずメールアドレスを利用したWeb認証について述べる．この認証方法は，Webサービスの利用に際して，従来から一般的に用いられてきた本人確認手段である．例として，アカウント作成時には以下の手順が取られてきた．

1. ユーザーは特定のページでメールアドレスを入力．

Automating Web Authentication using Mail Address
Akifumi Kawato , Akira Sakatoku , Gen Kitagata , Tetsuo Kinoshita
†Graduate School of Information Sciences , Tohoku University
‡Research Institute of Electrical Communication , Tohoku University
§Cyberscience Center, Tohoku University

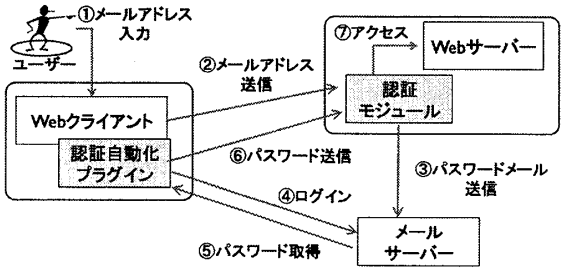

図 2: 提案する認証システムの概要と処理の流れ

2. Web サーバーは入力されたメールアドレス宛に，必要な情報を含んだメールを送信する．
3. ユーザーはメールの指示に従いアカウントを作成する．

以上の手順を踏むことにより，サーバー側は入力されたメールアドレスが，入力したユーザーによって確かに使用されていることを確認することが出来る．ネット通販サイト，ブログサービスといったサービスの種類を問わず，基本的にサービス提供者はメールアドレスを介してユーザーを信頼し，サービスを提供してきた．

本稿で提案する手法では，以上に述べたメールアドレスを利用した Web 認証の手順を自動化することにより，通常のログイン時にも利用可能とする．図 1 に提案手法の概要を示す．ユーザーがログインしたいサイトにメールアドレスを入力すると、Web サーバーはアクセス時刻に基づいたワンタイムパスワードを生成し，入力されたメールアドレス宛に送信する．そして Web クライアントが自動的にメールアドレスにログイン，パスワードメールを取得し，Web サーバーにパスワードを送信することにより，認証をおこなう．Web サーバーは認証されたメールアドレスに対応するアカウントに，ユーザーをログインさせる．

3.2 効果

提案手法を用いることにより，ユーザーが使用する ID とパスワードはメールアカウントのものに限られるため，複数のサイトを利用する場合のパスワードの管理負担は発生しなくなる．そのため共有パソコンでも利用しやすい方式であると言える．

また，複数のサイト間で共有する ID を新たに作成する必要がないため，それを管理する専用サーバーも不要である．認証手順に参加するのは従来通りサービス提供者とユーザーだけなので，低コストで導入が可能である．ユーザー自身がパスワードを入力する必要がないため，フィッシング被害を防げるといった効果も期待できる．

4. 設計

図 2 に提案手法を用いた認証システムの概要と，認証処理の流れを示す．実現のためには Web クライアント，Web サーバーの両方に新しい機能を追加する必要がある．本研究では Web クライアントの認証自動化プラグイン，Web サーバーに対しては認証モジュールを新たに開発する．

Web サーバーの認証モジュールの機能を以下に示す．

(Fs-1) パスワード生成・送信機能

(Fs-2) パスワード認証機能

(Fs-3) アカウント管理機能

次に Web クライアントの認証自動化プラグインの機能を以下に示す．

(Fc-1) パスワードメール取得機能

(Fc-2) パスワード送信機能

以上のような機能を持ったコンポーネントの連携によって，自動的な認証を実現する．具体的には，ユーザーのメールアドレス入力 (図 2①-②) に対応して，機能 (Fs-1) によりワンタイムパスワードを生成し，受け取ったメールアドレスに送信する (③)．次に (Fc-1) によりパスワードメールを取得 (④-⑤) し，(Fc-2) で Web サーバーにパスワードを送信 (⑥)，(Fs-2) により Web クライアントからパスワードを受け取り認証をおこなう．その後，(Fs-3) のアカウント管理機能によって，認証したメールアドレスに対応するアカウントにユーザーをログインさせる．

実装に当たっては，1 つのアカウントに対して，認証のためのメールアドレスを複数設定することを許可し，一方のメールサーバーに障害が発生している場合でも，他方のメールアドレスを用いてログインすることができるようにする．

5. 結論

本稿では，Web サービス利用時におけるユーザーの負担を軽減することを目的として，アカウント作成時やパスワード紛失時に従来から用いられてきたメールアドレスによる本人確認を自動化し，通常のログイン時にも利用可能とする手法を提案した．加えて，提案手法の効果について述べ，提案手法を用いたシステムの設計と，実現のために必要な機能と処理手順について述べた．今後はシステムの実装を進めて，認証にメールアドレスを利用することによる遅延等の測定実験を予定している．

参考文献

[1] Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J., “Stronger Password Authentication Using Browser Extensions”, 14th Usenix Security Symposium, 2005.

[2] Herzberg, A. and Jbara, A., “Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks”. Cryptology ePrint Archive, Report 2004/155.

[3] Yee, K., Sitaker, K., “Passpet: Convenient password management and phishing protection, Proceedings of the second symposium on Usable privacy and security (SOUPS), 2006.

[4] Perlman, R., Kaufman, C., “User-centric PKI”, IDtrust; Vol. 283 Proceedings of the 7th symposium on Identity and trust on the Internet.

[5] “OpenID”, http://openid.net/