2008－GN－67 (13)
2008／3／21

OpenID を用いたユーザ指向型ホワイトリスト作成手法の提案

阪本裕介[†1] 中山雅哉[†1]

現在，様々なコミュニケーションツールが広く利用されるようになる中で，それぞれのツールにおいてスパムが発生し問題となっている．スパムが増加する中で意図した相手からの通信を守る重要性が増している．そのために通信に用いられている ID などからその通信が意図した相手からのものかを判別するホワイトリスト方式が広く利用されている．しかし，既存のホワイトリスト方式では，1人のユーザが複数の ID を持ち，状況によってそれらを使い分けるというコミュニケーションツールの利用形態において，十分な効果を発揮できない可能性がある．本稿では，OpenID 認証機構を用いて Web 上で各ユーザが自身の ID 情報を管理することにより，事前にコミュニケーションツールの ID を交換していない場合でも通信を保護することが可能となる，ユーザ指向型のホワイトリストを作成する手法を提案する．

A Proposal to Create User-oriented White Lists Based on OpenID

Yusuke Sakamoto [†1] and Masaya Nakayama[†1]

Recently various communication tools are widely used, but many of them have problems of spam messages. In the context of increasing spam messages, it will be more important to protect messages sent by valid users. To achive this goal, white list methods, which select messages from valid users based on IDs, are used. However, it is usual for users to own plural IDs and use different IDs depending on commucation partners, and existing white list methods are not effective. In this paper, we propose a method to store ID information on the Web and create user-oriented white lists, which is effective even if communication tools' IDs are not exchanged beforehand, by using OpenID authentication mechanism.

1. はじめに

現在，インターネット上で電子メールやインスタントメッセンジャー，IP 電話などといったコミュニケーションツールが利用されている．これらのツールは多くのユーザに利用される一方で，受信者の意向を無視して一方的にメッセージを送りつけるスパムに悩まされている[2]．スパムメールは，全電子メールの内 40%を占め，すでに大きな問題となっている[4]．インスタントメッセンジャーでのスパム（SPIM）や IP 電話でのスパム（SPIT）は，増加が予想されている．そのため，全体の通信の中からスパムでない，意図した相手からの通信を判別し，守ることが重要になってくる．

電子メールにおいては，その配送の仕様に基づいてスパム判別を行ったり[11]，電子メールの本文を解析してスパム判別を行ったり[9]することが可能である．しかし，スパムメールや SPIM, SPIT に対して統一的な対策を行う際には，通信に用いられる ID から，その通信が意図した相手からのものかどうかを判別するホワイトリスト方式を取ることが有効である．インスタントメッセンジャーや IP 電話においても ID を用いてユーザを識別しており，ID を用いた判別が可能となるからである．

このホワイトリスト方式の課題として，現在のコミュニケーションツールの利用形態への対応が挙げられる．現在，1 人のユーザが 1 つのコミュニケーションツールにおいて複数の ID を所有することはよくみられるようになってきている．その中で，ユーザは自分の所有する ID を相手に合わせて部分的に交換し，それを用いてコミュニケーションを行っている．また，それらの ID はユーザの所属組織の変更や，恣意的な理由により変更されることがしばしばある．よって，事前に交換していた ID が何らかの理由で使用不可能な際に別の ID を用いて通信を試みるといったことや，ID が変更になった際にその旨を事前に相手に通知せずに変更後の ID を用いて通信を試みるといったことが想定される．その際，その通信に用いられた ID がホワイトリストに登録されていないために，同一ユーザの別の ID がホワイトリストにあったとしても，受信を拒否する可能性がある．結果，そのユーザからの

†1 東京大学大学院新領域創成科学研究科基盤情報学専攻
Department of Frontier Informatics, Graduate School of Frontier Sciences, The University of Tokyo

通信をホワイトリストによって守ろうとしているにも関わらず，その目的が達成できなくなる．この点において，従来のホワイトリストでは，ID の使い分けや変更といった利用形態への対応がなされていないと言える．

本稿では，この問題を解決するために，ユーザ指向型ホワイトリストを提案する．ユーザ指向型ホワイトリストとは，コミュニケーションツールで現在用いられているような ID を記載していくホワイトリストではなく，相手のユーザを記載していきそのユーザからの通信であればその ID に関わらず守ることを目的とするホワイトリストである．これにより，ID の使い分けや，ID の変更といったコミュニケーションの利用形態に合致したホワイトリストの作成，管理を実現する．

そのために，本稿では各ユーザが自分のコミュニケーションツールの ID を Web 上で管理する手法を提案する．ユーザは，通信を受信する際に相手の Web サイトから情報を取得し，その通信が意図した相手からのものかを判別する．各ユーザが自身の Web サイト上の ID 情報を最新に保つようにすれば，受信の際にそこから情報を取得することで，相手の ID が変更になっていてもその相手からの通信を守ることができる．ID の使い分けという課題には，OpenID による認証[8] を用いてユーザを識別し，ユーザごとに異なる ID の組を見せることにより対応する．これにより，コミュニケーションツールの利用形態に合致したホワイトリストの作成が可能になる．

また，本稿では，Web サイト上で ID 管理機構を実装し，それについての報告も合わせて行う．相手に合わせて異なる ID の組を表示する機能を実装した．これにより，ユーザ指向型ホワイトリストの実現に必要な ID 管理機構を実現できた．

2. 背　　景

2.1 コミュニケーションツールの利用形態とそれに付随する問題

現在，インターネット上で様々なコミュニケーションツールが利用されている．電子メールや各種インスタントメッセンジャー，IP 電話などが例として挙げられる．

それらのツールを利用する際には，各ツールごとに ID が必要となる．電子メールであれば，電子メールアドレスが必要となり，インスタントメッセンジャーではその種類に応じた ID が必要となる．IP 電話を利用するためには，電話番号，もしくは SIP-URI と呼ばれる ID が必要となる．

ユーザがこれらの ID を複数所有し，状況に応じて使い分けるということが一般的に見られる．仕事の連絡には職場の電子メールアドレスを用い，趣味のコミュニケーションには個人の電子メールアドレスを使うといった例が挙げられる．インスタントメッセジャーにおいても，相手に応じて異なるインスタントメッセンジャー，異なる ID を利用するということがみられる．そのため，**図 1** のように，複数所有している ID 群の中から相手に合わせて部分的に ID を交換するということがある．

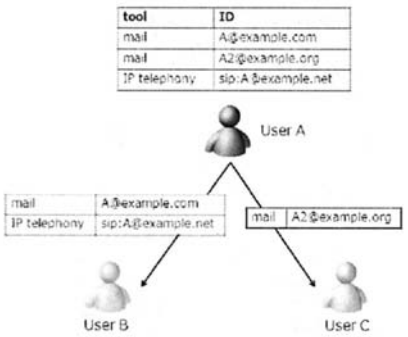

図 1 ユーザに合わせた ID の交換例
Fig. 1 Exchanging different partial IDs depending on communication partners

複数のツール，ID を使い分けることは用途に応じたコミュニケーション手段の使い分けが可能になり，ユーザの利便性を向上させる．しかし，その一方で，各 ID 間には関連が見えないという問題がある．そのため，コミュニケーションに用いた ID が異なれば，送信者が同一ユーザであったとしても受信者にとってそれを知ることが困難となる．よって，事前に交換していない ID を用いて通信を行った場合，相手のことは知っているにも関わらず ID を知らないために，両者間でコミュニケーションが成立しなくなる可能性がある．

この問題は，ID を使い分ける時だけでなく，ID が変更になったときにも生じる．ID が変更になったときそのことを相手のユーザに適切に通知しておかなければ，新しい ID を用いてコミュニケーションを図った際に受信者にはその ID が誰のものかわからない．そのため，この場合も両者間のコミュニケーションに支障をきたしてしまう．

2.2 スパムの現状とその対策

電子メールにおいて，一方的に広告などを相手に送りつけるスパムメールが，2006 年には全電子メールの内 40%を占めるなど大きな問題となっている[4]．インスタントメッセンジャーにおいても，同様に広告などを一方的に送りつける SPIM が存在する．また，IP 電話においても，一方的に電話をかけ，録音された広告メッセージなどを流す SPIT が存在する．現在，SPIM や SPIT は存在が確認されている程度であるが，2004 年から 2005 年にかけてインスタントメッセンジャーのネットワークに対する攻撃が 4 倍に急増し，今後

SPIM の増加が予想されている[6]．また，SPIT も IP 電話網の利用者急増が見込まれる中で脅威となることが予想されている．

これらの複数種のスパムに対して統一的な対策をとる際には，サーバ側での対策は難しい．スパムメールの判別については，電子メールの仕様が公開され統一されているため，電子メールの配送に関わるサーバ側で対策をとることが比較的容易であり，一定の効果も期待できる[11]．しかしながら，インスタントメッセンジャーは，MSN メッセンジャーや Yahoo メッセンジャーを始めとして多くの種類があり，その仕様が公開されているものが少なく，また，統一もされていない．そのため，メッセージの配送に関わるサーバ側で SPIM 対策を行うことは難しく，また効果も各アプリケーションに限定されたものとなる．よって，クライアントアプリケーション側で対策をとる方が，有利であると言える．

スパム対策の例として受信したメッセージの本文を解析してそれがスパムかどうかを判別する方式[9]が存在し，これはクライアントアプリケーション側でも行うことができる．しかし，本文を解析する方式では，意図した相手からの通信であっても内容によってはスパムと判定してしまう誤判別の問題が存在する．そのような誤判定が生じる確率は数%以下と低いが，重要な通信がスパムとして拒否されてしまうことによる問題は大きい[5]．短文がやりとりされることの多いインスタントメッセンジャーにおいては誤判定の起きる確率が上昇し[7]，この問題がさらに顕著になる．また，リアルタイムな音声通信を行う IP 電話においては，通信の内容を解析して SPIT かどうかを判別することが難しい．このため，この手法を SPIM や SPIT の判別に使用することは難しい．

他に，ブラックリスト・ホワイトリスト方式もクライアントアプリケーション側でとることのできる対策である．スパムを送信していると思われるユーザの ID や IP アドレス，スパムの送信に関わっているサーバ名などをリストに記載し，それらを用いてスパム判別を行うものがブラックリスト方式である．逆に，スパムを送信しないと信頼しているユーザに関しては，そのユーザの ID や IP アドレス，サーバ名などを記載し，そのユーザからの通信はスパムと判別しないようにするものがホワイトリスト方式である．

意図した相手の ID からの通信を許可するホワイトリスト方式は，スパムを排除することはできないが，正常な通信をスパムと誤判別されないようにするのに有効である．しかし，2.1 章で述べたように，ユーザが複数の ID を使い分けており，その ID 間の関連はわからないという背景がある．そのため，ホワイトリストに記載されている ID の所有者からの通信であっても，その通信に他の ID が用いられていれば，その通信はホワイトリストによって守られない．ユーザの ID に変更が起きた場合も同様で，事前に新しい ID を相手に教えてホワイトリストに追加するように頼んでおかなければ，新しい ID を用いた通信をホワイトリストによって守ることはできない．よって，現在のコミュニケーションツールの利用形態を考慮すると，意図した相手からの通信であってもホワイトリストによって守られないという事態が増加するという問題がある．ホワイトリストの有効性を発揮させるためには，この問題を解決し，ホワイトリストを適切に作成，維持する必要がある．

3. 関連研究

ホワイトリストを作成，維持する関連研究としては，電子メールアドレスごとに信頼度を割り振りそれをホワイトリスト作成に利用する手法[3]，通話時間を用いて IP 電話で用いる電話番号や SIP-URI に信頼度を割り振りホワイトリスト作成に利用する手法[1]，SNS での関係をホワイトリスト作成に利用する手法[10] などが挙げられる．

Chirita らの研究では，電子メールアドレスごとに信頼度を割り振る MailRank というシステムが提案されている[3]．MailRank では，各ユーザのアドレス帳や電子メールの送信先履歴などを参考にして各電子メールアドレスに信頼度を割り振っていく．電子メールを送信するばかりで受信することの少ないスパム送信者の電子メールアドレスには低い信頼度しか割り振られない．このため，ある閾値を設け，その閾値以上の信頼度をもつ電子メールアドレスをホワイトリストに追加すれば，適切なホワイトリストの作成，維持が期待できる．ユーザが複数の電子メールをもつ場合でも，両方の電子メールアドレスを同頻度で使用していて同程度の信頼度が割り振られていれば，一方の電子メールアドレスしか知らない相手に他方の電子メールアドレスから電子メールを送信したとしても，送信された電子メールはホワイトリストによって守られることが期待できる．しかし，ユーザが電子メールアドレスを変更した場合に，以前所有していた電子メールアドレスの信頼度を引き継ぐことはできず，それを用いた通信はホワイトリストによって守られなくなる．ID の使い分けの問題に関しては，普段から全 ID を同頻度で使っている場合は解決されるが，それ以外の場合は解決されない可能性が高く，また，ID の変更には対応できていない．

Balasubramaniyan らの研究では，過去の通話時間を用いて IP 電話番号や SIP-URI といった ID に信頼度を割り振る CallRank というシステムが提案されている[1]．CallRank は，MailRank 同様，複数の ID をもつ場合に対しては問題が解決されることが期待できる．しかしながら，新しい ID に対しては，過去の通話がないため低い信頼度しか割り当てられず，その ID

を用いた通信がホワイトリストによって守られなくなる．この研究もMailRank同様，IDの変更に対応できないという問題が残る．

横山らの研究では，SNSから趣味などの近さを取得するAPIが提案されている[10]．このAPIを用いて趣味の近い相手の電子メールアドレスなどを取得し，それらを登録したホワイトリストを作成するということも合わせて提案されている．このAPIを利用すれば，あるユーザの電子メールアドレスが変更になったとしても，そのユーザがSNS上にそれを記載しておけば，その変更状況が相手に取得され，ホワイトリストに追加される．しかし，横山らの研究で用いているSNSはmixi[*1]であり，ユーザごとに異なるIDの組を公開することができない．相手によって公開するIDを変更できるなど，コミュニケーションツールの利用形態に合った管理のできる機構から情報取得することが必要だと考えられる．IDの変更による問題は解決されることが期待されるが，IDの使い分けという問題に対しては効果が期待されない．

4. 提案手法

4.1 Webサイトの URL を用いたユーザ指向型ホワイトリスト

本稿では，IDの変更が生じた際に相手のユーザのホワイトリストを自動的にそれに対応させるために，Webを用いたID管理機構を用いることを提案する．各ユーザが自身のWebサイトを1つ持ち，そこに電子メールアドレスなどのIDを記載し，そのサイトのURLを，すでに何らかのコミュニケーションツールを用いて連絡をとりあっているユーザ，あるいは今後そうしたいユーザと交換する．ユーザは交換したURLを自身のホワイトリストに記載していく．ユーザは交換後にそのURLを用いてホワイトリストを作成する．URLはユーザと1対1に対応しているため，この作業を繰り返すことでユーザ指向型のホワイトリストを作成することができる．

URLの交換を行ったら，各ユーザは自身のWebサイト上の情報をIDの変更に合わせて最新の状態に保つようにする．ホワイトリスト作成後に，あるコミュニケーションツールを介して通信を受け取ったとする．このとき，ホワイトリストを見て，これまでにURLを交換したユーザのWebサイトを参照し，各ユーザのID情報を取得する．取得したID情報の中にこの通信で用いられているIDが存在すれば，その通信はホワイトリストによって守られることとする．

このようにすることで，事前に交換したIDとは別のIDから通信を図ったとしても，そのIDを自身のWebサイトに記載していて，かつ相手のホワイトリストにそのWebサイトのURLが存在すれば，ホワイトリストによって通信を守ることができる．これにより，複数のIDを使い分けるコミュニケーションツールの利用形態にあったホワイトリストの利用が可能になると考えられる．

また，あるユーザがコミュニケーションツールのIDを変更しても，そのユーザのURLが相手のホワイトリストに登録されていれば，自身のWebサイトに記載するID情報を変更するだけで，新しいIDを用いた通信もホワイトリストによって守られるようになる．

本提案手法により，IDに変更が生じてもユーザ間のコミュニケーションに支障をきたさないようにすることができる．

4.2 ID公開制限のための認証機構

相手に応じたIDの使い分けを実現するためには，ユーザごとに異なるIDを公開することが必要となる．横山らの研究[10]では既存のSNSを用いていたためIDの使い分けのための新機能を追加することは困難であった．より一般的な情報基盤であるWebを用いることで，ID使い分けの機能を追加することが比較的容易となる．

Webでその機能を実現するには，各ユーザを識別するための認証機構が必要となる．認証を行い，交換したURLによってアクセスできるWebサイトにおいて，ユーザによって異なるIDの組を公開できるようにしなければならない．

そこで，本稿では，認証機構としてOpenID認証[8]を用いることを提案する．OpenIDは仕様が公開されているシングルサインオン認証機構であり，Webでの利用を想定して作られたものである．OpenIDの認証においては，各ユーザがもつURLを認証の際のユーザ識別子として利用できる．

OpenIDの認証と利用の流れは**図2**のとおりである．図2において，OpenID Providerは，ユーザからの要求に対してOpenIDの発行と，その後の認証を行う機関である．Serviceは，OpenID Providerによる認証結果に応じて，ユーザに対し何らかのサービスを提供する機関である．Serviceは，ユーザにOpenIDを入力させるためのフォームを自身のWebサイトにもつ．ユーザは，あらかじめOpenID ProviderからOpenIDの発行を受けており，その発行の際にパスワードや公開鍵といった，今後そのOpenIDの認証に必要な情報をOpenID Providerに登録しているものとする．このOpenIDはURLの形式をとっており，ユーザはそのURLを用いてアクセスできるWebサイト下の文書に自身のOpenID Providerがどこであるかという情報を記載しているものとする．あるユーザがServiceにアクセスし，フォームに自身のOpenIDを入力すると，Serviceはその OpenID下の文書を解析してその OpenIDの認証を担う OpenID Providerの情報を取得し，OpenIDの情報とともにOpenID ProviderのURLへとユーザを転送する（Step.1）．OpenID

*1 http://mixi.jp/

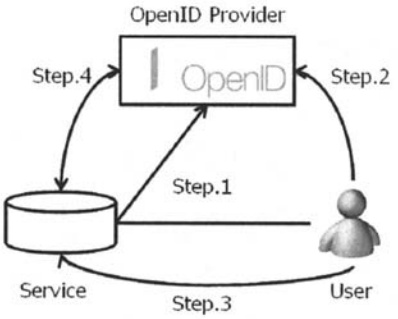

図 2 OpenID 認証機構
Fig. 2 OpenID Authentication Mechanism

Provider は，転送されてきたユーザに対し，同じく転送されてきた OpenID の認証に必要な情報の入力を要求する．その要求に対し，ユーザは OpenID の発行の際に決めた，認証に必要な情報を OpenID Provider に対し入力する（Step.2）．入力を受けた OpenID Provider はそのユーザを元の Service の URL に転送する（Step.3）．ユーザに再度アクセスされた Service は，OpenID Provider に対してそのユーザの認証結果を問い合わせる（Step.4）．認証結果に応じて，Service はユーザに対してサービスを提供する．一般に，認証結果が真であればサービスが提供され，偽であれば提供されない．

本提案手法では，どのユーザが Web サイトにアクセスしていて，そのユーザにはどの ID の組を公開すべきかを判断するために，この OpenID 認証機構を用いる．OpenID の利点として，各ユーザが自身の ID を記載する Web サイトの URL をそのまま利用できる点が挙げられる．そのため，ユーザ間で交換した URL を用いて，どの ID の組をそのユーザに公開するかを考えることができる．

提案手法を用いることで，ユーザごとに異なる ID の組を公開できるようになる．これにより，相手ごとに異なる ID を使い分けてコミュニケーションを行うという，コミュニケーションツールの利用形態にあった ID の使用が可能になる．

5. 実　　装

提案手法で述べた Web サイトでの ID 管理機構を実装したので，報告する．

本稿では，Web サイト上で HTML ドキュメントと CGI として実装した．ユーザ A が http://A.example.com/という Web サイトを持っていてそれを OpenID として利用しており，ユーザ B が http://B.example.com/という Web サイトを持っていてそれを OpenID として利用しているとする．

あるユーザが http://A.example.com/にアクセスすると，http://A.example.com/index.html が表示される．ここには，**図 3** のように，OpenID 入力フォームが用意されている，

図 3 OpenID 入力フォーム
Fig. 3 OpenID input form

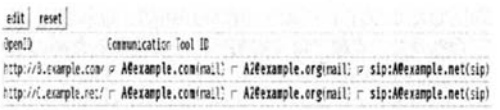

図 4 ID 公開設定画面
Fig. 4 ID release configuration

図 3 のフォームにユーザが OpenID を入力すると，4.2 章で述べた流れに従い，OpenID の認証が行われる．認証に成功した場合，入力された OpenID に応じて機能が提供される．

入力された OpenID がサイトの URL と同一だった場合，つまり http://A.example.com/だった場合，そのユーザは自身のもつコミュニケーションツールの ID をその Web サイト上に記載し，どのユーザに対してその ID を公開するかを相手の OpenID を用いて指定できる（**図 4**）．図 4 は，http://B.example.com/を OpenID として持つユーザ B に対しては，電子メールアドレス A@example.com と IP 電話で用いる SIP-URI である sip:A@example.net を公開する例である．

フォームに入力された OpenID がサイトの URL と異なる場合，そのサイトの所有者がそのユーザに公開すると決めた ID が表示される．入力された OpenID が http://B.example.com/である場合，mailto:A@example.com，sip:A@example.net が表示される．

6. 結　　論

本稿では，従来のホワイトリストでは対応できない ID の使い分けや変更といった問題を解決するために，ユーザ指向型ホワイトリストを提案した．具体的には，Web で各ユーザが自身の ID を管理し，そこに他のユーザが OpenID 認証を通じてアクセスして ID 情報を取得し，通信が意図した相手からのものかを判別することのできるホワイトリストを提案した．

ユーザ指向型ホワイトリストの実現に向けて，ID を使い分けるという利用形態に適した ID 管理を実現するために，Web 上で OpenID を用いて認証を行い，相手によって異なる ID を公開する手法を提案した．また，各ユーザが 1 つの Web サイトを持つことで Web サイトの URL とユーザとを 1 対 1 に対応させ，その Web サイトの URL を用いてホワイトリストを作成

することを提案した．提案手法を用いることで，事前に交換していない ID を用いて通信を試みたとしても，その ID を Web サイト上で相手に公開するようになっていれば，その通信が誰からのものかが相手にわかるようになった．これにより，ID の使い分けと変更に対応したホワイトリストの作成が可能となった．

合わせて，本稿では，提案手法を実現するための ID 管理機構を Web サイト上に実装した．OpenID を用いて認証を行い，相手ごとに異なる ID を公開できることを確認した．

7. 今後の課題

本稿では，URL を用いたユーザ指向型ホワイトリストを提案し，Web 上での ID 管理機構を実装したが，その ID 管理機構へのアクセスと OpenID の認証は Web ブラウザ経由のものであった．各コミュニケーションツールがこの ID 管理機構から情報を取得し，通信が意図した相手からのものかどうかを判別するためには，情報を取得する機構をミドルウェアの形で実装し，それを各アプリケーションから利用できるようにするのがよいと考えられる．そのミドルウェアのデザインおよび実装が今後の課題として挙げられる．また，そのミドルウェアが，過去に URL を交換した相手の Web サイトを訪れて ID 情報を取得し通信が意図した相手からのものかを判別するのに必要な時間を見積り，それを実用的な時間に短縮していくことも今後の課題である．

参 考 文 献

1) Balasubramaniyan, V., Ahamad, M. and Park, H.: CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation, *Conference on Email and Anti-Spam* (2007).
2) Cerf, V.G.: Spam, spim, and spit, *Commun. ACM*, Vol.48, No.4, pp.39–43 (2005).
3) Chirita, P., Diederich, J. and Nejdl, W.: MailRank: using ranking for spam detection, *Proceedings of the 14th ACM international conference on Information and knowledge management*, pp.373–380 (2005).
4) Evett, D.: Spam Statistics 2006, *TopTenREVIEWS http://spam-filterreview. toptenreviews. com/spam-statistics. html (2006).*
5) Hershkop, S. and Stolfo, S. J.: Combining email models for false positive reduction, *KDD '05: Proceeding of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*, New York, NY, USA, ACM, pp.98–107 (2005).
6) Leavitt, N.: Instant Messaging: A New Target for Hackers, *Computer*, Vol.38, No.7, pp.20–23 (2005).
7) Liu, Z., Lin, W., Li, N. and Lee, D.: Detecting and filtering instant messaging spam - a global and personalized approach, pp.19–24 (6 Nov. 2005).
8) Recordon, D. and Reed, D.: OpenID 2.0: a platform for user-centric identity management, *DIM '06: Proceedings of the second ACM workshop on Digital identity management*, New York, NY, USA, ACM, pp.11–16 (2006).
9) Sahami, M., Dumais, S., Heckerman, D. and Horvitz, E.: A Bayesian Approach to Filtering Junk E-Mail, *Learning for Text Categorization: Papers from the 1998 Workshop*, Madison, Wisconsin, AAAI Technical Report WS-98-05 (1998).
10) Yokoyama, T., Kashihara, S., Okuda, T., Kadobayashi, Y. and Yamaguchi, S.: A Generic API for Retrieving Human-Oriented Information from Social Network Services, *Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on*, pp.33–33 (15-19 Jan. 2007).
11) 陳 春祥, 佐々木宣介, 田中稔次朗：SMTP セッションフィルタとグレイリストを併用した迷惑メール対策, 情報処理学会論文誌, Vol.47, No.4, pp. 1000–1009 (20060415).