社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－CSEC－41（20）
2008／5／23

サービス利用者を介したユーザ認証方式

市川 幸宏† 坂上 勉† 宮崎 一哉†

†三菱電機株式会社 情報総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1

E-mail: †Ichikawa.Sachihiro@dp.MitsubishiElectric.co.jp, Sakagami.Tsutomu@bp.MitsubishiElectric.co.jp, Miyazaki.Kazuya@dh.MitsubishiElectric.co.jp

あらまし 本稿では，IBE に適用することを考慮した，外部ユーザが特別なソフトウェアを端末にインストールする必要がなく，ユーザの認証情報をサーバに登録する必要もない，内部ユーザを介してコミュニティに参加できる仕組みを提案する．提案方式を用いることで，社内などで展開されている IBE を用いたメールシステムに社外ユーザを容易に参加させることができる．

キーワード 認証，IBE，メールシステム

Authentic Method using a Service Agent

Sachihiro Ichikawa† Tsutomu Sakagami† Kazuya Miyazaki

†Mitsubishi Electric Corporation, Information Technology R & D Center,

5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan

E-mail: †Ichikawa.Sachihiro@dp.MitsubishiElectric.co.jp, Sakagami.Tsutomu@bp.MitsubishiElectric.co.jp, Miyazaki.Kazuya@dh.MitsubishiElectric.co.jp

Abstract In this paper, We study how to use ID-Based Encryption and Our suggestion can be joined an external user in the safe community using an internal user. An external user doesn't need to install any special softwares on his computer and register any user's authentication informations on the server computer when he joins it. Our suggestion is easy to join him in the Internal Secure Mail Service using ID-Based Encryption.

Keyword authentication, IBE, Mail System

1. はじめに

公開鍵証明書を必要としないため，従来の Public Key Infrastructure（以下，PKI）よりも低コストで管理・運用可能な ID-Based Encryption（以下，IBE）が注目されている．IBE は，1 対多の暗号化通信を考えた場合，個々のユーザの証明書を必要としないため，ユーザの証明書のダウンロードや Certification Authority（以下，CA）の証明書の登録を不要とできる利点がある．ただし，IBE にも欠点がある．IBE は，Private Key Generator（以下，PKG）と呼ばれる秘密鍵生成機がすべてのユーザ秘密鍵を生成できる．そのため，PKI と異なり，ユーザ自身が秘密鍵と公開鍵のペアを作成し，CA に公開鍵だけを登録することができない．PKG の管理者は，すべての暗号化データを復号できるため，第三者が運用する CA のようなシステムを構築しづらい．よって，PKG は，CA より社外を含め 2 社間で行う通信や課や部単位など比較的小さなグループで，PKG を運用するのが好ましいと言われている．また，このように内向きに運用することを考慮しているためか，IBE システムにおいて，社外ユーザを容易に認証および登録する方法について，提案が今までなされなかった．OCN は IBE を適用したメールシステムのサービスを展開しており，社外ユーザを登録する方法として以下のような登録システムを採用している．[1]サーバに登録済みかつ，閉じられた環境のサービスをそのサーバから受けられるユーザ（以下，内部ユーザ）が一度も登録されていないユーザ（以下，外部ユーザ）をメールアドレスだけサーバに登録し，登録後，サーバは外部ユーザにメールを送信し，外部ユーザは，そのメールにあるリンクの指示に従い，パスワードを設定することで，外部ユーザを登録する方式である．しかし，この方式では，パスワードを設定するメールを盗聴できれば，なりすましが可能となるため，安全なシステムといえない．

提案方式は，なりすまし不可能な外部ユーザの登録方式について述べる．また，外部ユーザに特別なソフトをインストールさせる必要がなく，

鍵やパスワードといった情報の共有も不要とする特徴がある．さらに近年，社会問題となっている情報漏えいを考慮し，サーバに外部ユーザの情報を登録不要とする．本方式では社内適用するIBEメールシステムに社外ユーザの参加を考慮するものであり，社外ユーザが負担なく，サーバのサービスに参加することができる．

2. 従来方式

外部ユーザをサーバに登録する方法は以前から研究されている．ここでは，それら研究がIBEメールシステムに適用できないか検討した．

通常，コンピュータネットワーク上のリソースへのアクセス制御として，Basic認証やDigest認証と呼ばれるパスワードによるユーザ認証が知られている．[2]この認証はサーバとユーザが1対1で行い，サーバがユーザを信頼するための情報を必要とするため，あらかじめ，なんらかの方法でサーバにそれら情報を登録する必要がある．しかし，その登録や登録するユーザの証明が困難であり，ユーザやサーバに膨大なコストがかかる．そこで，すでにサーバに登録されている情報を利用して，柔軟に認証を行う方式を適用できないか検討した．

従来方式では，大きく分けて二つある．一つは登録済のユーザを中継し，新規サーバに登録する方式[3][5]と，もう一つは，登録済のサーバを中継し，新規サーバに登録する方式である．[4]

方式[3]は，あらかじめCAで登録された公開鍵および秘密鍵を用いてコミュニティ参加を実現している．そのため，外部ユーザがCAの登録および鍵の生成などを行わなければならず，前提条件のコストが大幅にかかる．方式[4]はクライアントとの認証が成功している情報を，認証が成功していない他のサーバに渡す方法で，コミュニティの参加を実現している．そのため，信頼できるサーバ同士で認証情報を交換しなければならないかつ，サーバは外部ユーザの認証情報を保存しなければならないため，登録するコストがかかる．さらに近年流行しているmixi[5]などSocial Networking Serviceのユーザ登録方法やWebの会員登録では，サーバから送信される登録許可メールが暗号化されていないため，盗聴およびなりすましが容易に可能である．

これら従来方式を考慮した結果，どの方式もIBEを適用したメールシステムにふさわしくないと判断し，提案方式を考えた．

3. 提案方式

提案方式では，外部ユーザに特別なソフトのインストールを不要とし，鍵やパスワードといった情報の共有も不要とすることで，前提条件のコストを大幅に下げる手法を実現し，盗聴やなりすましを防ぎ，IBEメールシステムに外部ユーザを参加させることを可能とする．

3.1. 前提条件

提案方式の前提条件は以下である．

1. 内部ユーザはサーバに登録を希望している外部ユーザを知っている．
2. 内部ユーザは外部ユーザの名刺程度の情報（名前，メールアドレスなど）を知っている．
3. 内部ユーザはサービス発行サーバに自身の個人情報やパスワード，秘密鍵，公開鍵を登録している．
4. 本方式はIBEを用いることを前提としている．ただし，通常の公開鍵暗号方式を用いても実装可能である．
5. サービス発行サーバはPKGの機能を持つ．

3.2. 提案方式

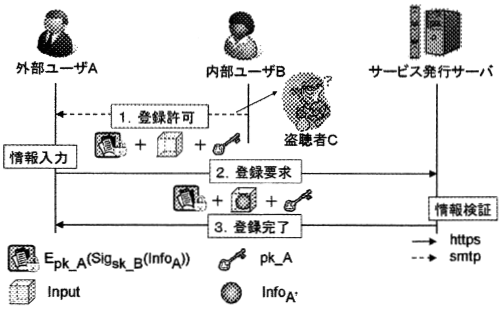

図 1　提案方式のフロー

提案方式の手順を図 1に示す．

1. 内部ユーザBはあらかじめ決定している外部ユーザ情報 $Info_A$ (メールアドレスやユーザ名など)を内部ユーザBの秘密鍵 sk_B で署名する．

$$Sig_{sk\_B}(Info_A) \quad (1)$$

内部ユーザBは外部ユーザAに登録許可メールを送信する．登録許可メールに添付されるデータは情報(1)を外部ユーザ A の公開鍵 pk_A で，IBEを用いて暗号化したデ

ータ $E_{pk\_A}[(1)]$，pk_A と入力フォーム Input である．
このとき，内部ユーザ B は pk_A を外部ユーザ A のメールアドレスなどを用いて暗号化できる．

$$(E_{pk\_A}[(1)],\ pk\_A,\ Input) \quad (2)$$

2. 外部ユーザは，入力フォーム Input にあらかじめ決定している自身の情報 InfoA'を入力し，サービス発行サーバに登録要求を送信する．送信するデータは，情報(1)に外部ユーザ情報を入力したものとなる．

$$(E_{pk\_A}[(1)],\ pk\_A,\ Input_{InfoA'}) \quad (3)$$

3. サービス発行サーバは，PKG の機能も持ち合わせているため，pk_A からユーザ秘密鍵 sk_A を生成できる．データ $E_{pk\_A}[(1)]$ を復号し，情報(1)を取得し，この署名を検証する．検証に成功した場合，チケットから取り出した外部ユーザ情報 $Info_A$ と外部ユーザ入力情報 $Input_{InfoA'}$を比較し，一致していた場合，外部ユーザに登録完了通知を行う．

以上で外部ユーザ登録完了となる．外部ユーザは名刺程度の情報を入力するだけで，特別なソフトウェアをインストールすることなく，鍵やパスワードといった情報の共有も必要ない．また，外部ユーザおよび内部ユーザが，サーバに対して，住所やメールアドレスのような個人情報を登録する必要がない．このため，外部ユーザの登録における内部ユーザおよび外部ユーザの利便性を高めることができ，また，外部ユーザの登録において内部ユーザ，外部ユーザおよびサーバのリソースを消費しない．さらに，暗号化および電子署名を用いているため，盗聴やなりすましといった悪意ある第三者からの攻撃を防ぐことができ，悪意ある第三者はあらかじめ決定している外部ユーザ情報を推測できない．

ただし，盗聴者 C が内部ユーザと外部ユーザのあらかじめ任意に決定している情報を知りえた場合，それら情報が名詞程度の情報であるため，なりすましが可能となる．また，上の提案方式では外部ユーザと内部ユーザがあらかじめ入力する情報を共有しなければならない．そこで運用として外部ユーザ情報を入力するのではなく，質問文の回答を入力する内部不正者対応型について述べる．手順としては図 1と変わらない．以下に質問文の回答を行う方式について述べる．

1. 内部ユーザ B が外部ユーザ A に登録許可メールを送信する．送信データは情報(2)と質問文 Question を送信する．

$$(E_{pk\_A}[(1)],\ pk\_A,\ Input,\ Question) \quad (4)$$

2. 外部ユーザは質問の回答を入力し，サービス発行サーバに送信する．

$$(E_{pk\_A}[(1)],\ pk\_A,\ Input_{InfoA'},\ Question) \quad (5)$$

3. サービス発行サーバは情報(5)を検証する．提案方式の手順同様，$Info_A = Input_{InfoA'}$の場合，外部ユーザに登録完了通知を行う．

以上で外部ユーザ登録完了となる．会議の内容など外部ユーザと内部ユーザしか知りえない質問と回答を作成することで，悪意ある内部ユーザのなりすましを防ぐことができる．また，外部ユーザがあらかじめ決定する情報を知らない場合にも対処可能となる．このように提案方式は質問に回答することで，外部ユーザと内部ユーザだけの既知情報を任意に変更でき，悪意ある第三者の攻撃を困難にすることができる．

4. 提案システム

提案システムでは，提案方式を用いて運用を考慮して，３つのシステムを構築した．

1. 登録要求の受付時間制限システム
2. 不正サーバ誘導防止システム
3. 内部ユーザ承認システム

１は内部ユーザが登録許可情報に時間情報をつけ，サービス発行サーバに時間を送信することで，生成した登録要求受付のタイムアウト処理を行うシステムである．２は内部ユーザが登録許可情報に URI などのサーバ情報をつけることで，外部ユーザが登録完了後，サーバ情報を検証できるシステムである．３はサービス発行サーバが情報を検証した結果，不一致であった場合に，内部ユーザに検証した情報を確認させることで，外部ユーザを登録するものである．それぞれの手順については以下に述べる．以下の手順は内部不正者を考慮しない手順となっているが，３章の提案方式の後半部で示した内部不正者対応型についても以

下の手順は問題なくシステム構築できる.

4.1. 登録要求の受付時間制限システム

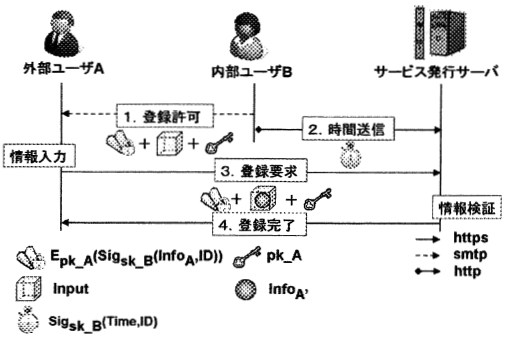

図 2 登録要求の受付時間制限システム

登録要求の受付タイムアウト処理の手順について図 2に示す.

1. 内部ユーザはあらかじめ任意に決定している外部ユーザ情報 $Info_A$ (メールアドレスやユーザ名など)と登録許可データ識別子 ID を sk_B で署名する.

$$Sig_{sk\_B}(Info_A,\ ID) \qquad (6)$$

内部ユーザ B は外部ユーザ A に登録許可メールを送信する. 登録許可メールに添付されるデータは情報(6)を pk_A で暗号化し, pk_A と Input を送付する.

$$(E_{pk\_A}[(6)],\ pk\_A,\ Input) \qquad (7)$$

2. 内部ユーザは現在の時間 Time と ID を sk_B で署名し, サービス発行サーバに登録要求を送信する. Time については内部ユーザのローカル時間またはタイムスタンプサーバなどどのような手段を用いてもよい.

$$Sig_{sk\_B}(Time,\ ID) \qquad (8)$$

3. 外部ユーザは入力フォーム Input に InfoA' を入力し, サービス発行サーバに登録要求を送信する.

$$(E_{pk\_A}[(6)],\ pk\_A,\ Input_{InfoA'}) \qquad (9)$$

4. サービス発行サーバは, データ $E_{pk\_A}((8))$ を復号し, 情報(6)の署名と情報(8)の署名を検証する. 検証に成功し, ID が一致している場合, 検証終了後の時刻と Time の差を計算する. その差が閾値以下である場合, チケットから取り出した外部ユーザ情報 $Info_A$ と外部ユーザ入力情報 $Input_{InfoA'}$を比較する. $Info_A$ と $Input_{InfoA'}$ が一致していた場合, 外部ユーザに登録完了通知を行う. 検証終了後の時刻はサーバのローカル時間またはタイムスタンプサーバなどどのような手段を用いてもよい. 閾値より大きい場合, ユーザ認証を行わない.

4.2. 不正サーバ誘導防止システム

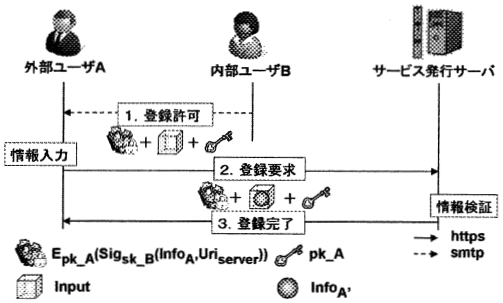

図 3 不正サーバ誘導防止システム

不正サーバ誘導防止の手順について図 3に示す.

1. 内部ユーザは外部ユーザ情報 $Info_A$ とサービス発行サーバの特定できる情報(URI や IP など)を sk_B で署名する.

$$Sig_{sk\_B}(Info_A,\ Uri_{server}) \qquad (10)$$

内部ユーザ B は外部ユーザ A に登録許可メールを送信する. 登録許可メールに添付されるデータは情報(10)を pk_A で暗号化し, pk_A と Input を送付する.

$$(E_{pk\_A}[(10)],\ pk\_A,\ Input) \qquad (11)$$

2. 外部ユーザは入力フォーム Input に InfoA' を入力し, サービス発行サーバに登録要求を送信する.

$$(E_{pk\_A}[(10)],\ pk\_A,\ Input_{InfoA'}) \qquad (12)$$

3. サービス発行サーバは，データ $E_{pk\_A}[(10)]$ を復号し，情報(10)の署名を検証する．検証に成功した場合，チケットから取り出した外部ユーザ情報 $Info_A$ と外部ユーザ入力情報 $Input_{InfoA'}$ を比較し，一致していた場合，外部ユーザに登録完了通知を行う．

登録完了通知に外部ユーザの秘密鍵 sk_A が添付されていた場合，sk_A を用いて情報(11)を復号し，情報(10)を取得する．取得した情報(10)を検証し，検証に成功した場合，Uri_{server} を取得し，その情報を元にサービス発行サーバが不正サーバであるかどうか確認できる．

4.3. 内部ユーザ承認システム

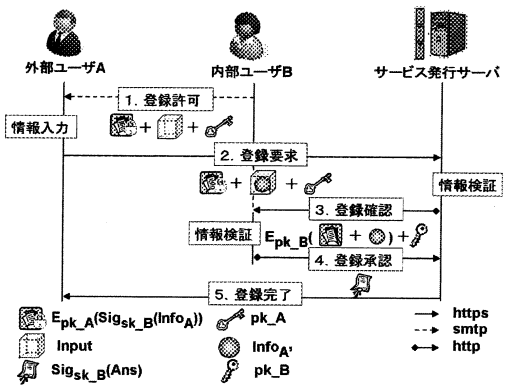

図 4　内部ユーザ承認システム

内部ユーザ承認方式の手順について図 4に示す．

1. 内部ユーザは外部ユーザ情報 $Info_A$ を sk_B で署名する．
   内部ユーザ B は外部ユーザ A に登録許可メールを送信する．登録許可メールに添付されるデータは情報(2)を送付する．

2. 外部ユーザはサービス発行サーバに登録要求として情報(3)を送信する．

3. サービス発行サーバは，情報(3)を復号し，情報(1)の署名を検証する．検証に成功した場合，チケットから取り出した外部ユーザ情報 $Info_A$ と外部ユーザ入力情報 $Input_{InfoA'}$ を比較し，一致していた場合，外部ユーザに登録完了通知を行う．一致していない場合，登録確認として情報(1)と $Input_{InfoA'}$ を内部ユーザの公開鍵 pk_B で暗号化したデータと pk_B を内部ユーザに送信する．

   $(E_{pk\_B}[(1),\ Input_{InfoA'}],\ pk\_B)$　　(13)

4. 情報(13)を受信した内部ユーザは sk_B で復号し，$Info_A$ と $Input_{InfoA'}$ を取得する．これらを比較した結果，内部ユーザの判断で外部ユーザを承認することができる．承認する場合は，承認許可 Ans=true でサービス発行サーバに送信する．承認しない場合は，承認許可 Ans=false でサービス発行サーバに送信する．

   $Sig_{sk\_B}(Ans)$　　(14)

5. サービス発行サーバは情報(14)の署名を検証する．検証に成功した場合は，承認許可 Ans=true で，外部ユーザに登録完了を送信し，承認許可 Ans=false で外部ユーザに登録失敗を送信する．

5. 考察

【登録許可フローの追跡】

情報(3)や情報(5)の署名値と外部ユーザ公開鍵情報から登録許可フローの追跡を行うことが可能である．サービス発行サーバは，電子署名つき情報(1)の電子署名を抽出し，抽出した電子署名を用いて情報(1)の生成元を特定することが可能である．そして，外部ユーザの秘密鍵が漏洩した場合などなんらかの問題が発生した場合，内部ユーザに責任を負わせてもよい．この機能を用いることで，内部ユーザの不正外部ユーザ登録を防ぐことができ，システムとして全体の安全性が高まる．

【安全性の評価】

提案方式の安全性は，運用で決定した外部ユーザ情報の秘匿性もしくは，質問に対する回答の秘匿性に帰着する．当然ながら安全性を意識しないユーザであれば，秘匿情報に外部ユーザのメールアドレスなどを用い，悪意ある第三者の推測を容易にする．ただし，危険性を意識しているユーザである場合，外部ユーザ情報に用いる値は様々で，仮に会議の主題とした場合，第三者にとっては推測することは不可能である．

全数探索のみを考慮した鍵長の安全強度は

65-70 ビットのものであれば，1 年以内では解読されないと予想されている．また，Diceware[6]とよばれるパスフレーズを作るための方法でも $\log 2^{65}$ と程度の安全強度を持たせていることから，外部ユーザの秘密情報には $\log 2^{65}$ 程度の安全性強度が必要であると考える．仮に会議の主題を外部ユーザの秘密情報とした場合，使用言語として英数字，仮名および漢字が考えられる．１文字あたりエントロピー値約 $\log 2^{11}$ あるので，安全な文字長としては６文字から１０文字あれば十分ではないかと考えている．ただし，これはもちろんすべての文字が同じ確率で使用された場合によるもので，今後，より厳密な安全性の評価を行う必要がある．

【運用上の問題】

未実装であるため，推測される事柄となるが，質問に対する回答であると，様々な回答が予測でき，一致する確率が低くなる可能性が高い．4．3 の提案システムを用いることによって不一致の問題は多少軽減されると考えるが，根本的な解決となっていない．よって，質問をあらかじめ固定もしくは有限の情報から選択するという形式をとることを考慮する．

また，質問から回答自体が悪意ある第三者に推測されてしまう場合があるため，運用方法として，ユーザに安全性を選択させ，高い安全性を持たせたい場合には，システムで会議の主題や会議の結論などの比較的回答が困難である質問を選択するようにし，低い安全性の場合は，会議の日時などを選択するように運用すべきと考えている．これらは今後，実装して明らかにする．

6. まとめ

外部ユーザが特別なソフトウェアを端末にインストールする必要がなく，ユーザの認証情報をサーバに登録する不要もない，内部ユーザを介してコミュニティに参加できる仕組みを実現する提案方式を示した．提案方式を用いることで，なりすましを防ぎつつ，外部ユーザが容易に登録することができ，IBE のメールシステムを展開した場合，社外のユーザに対してシームレスでシステムを使用することができる．

文　献

[1] NTT Communications.
http://www.ocn.ne.jp/business/security/encryption/

[2] RFC 2617.　http://tools.ietf.org/html/rfc2617

[3] 千葉健司，山田敏哉，倉林則之，“アクセス制御装置および方法” 特開 2004-287784，2004-10-14.

[4] 平川俊治，”コンテンツサービス提供システム，コンテンツサービス用サーバおよび会員用クライアント”特開 2004-86510，　2004-3-18.

[5] 株式会社ミクシィ．http://mixi.jp/

[6] Arnold G．Reinhold.
”The Diceware Passphrase Home Page”.
http://world.std.com/~reinhold/diceware.html