ユーザの生活履歴を用いた認証方式—電子メール履歴認証システム

西垣正勝[†] 小池誠[††]

パスワード認証には，「長くランダムなパスワードは覚えにくい/短く意味のあるパスワードは推測されやすい」という利便性と安全性のトレードオフが存在する．近年はセキュリティに対する関心も高まり，利便性と安全性の両者を満足する認証方式の必要性が叫ばれている．そこで本論文では，本人のみが覚えやすく，他人に推測されにくいパスワードの実現に向けて，「パスワードを覚える」から「覚えていることをパスワードとして使用する」というコンセプトの転換を提唱し，ユーザの生活履歴（本人が経験し覚えている情報）をパスワードに用いた認証方式を提案する．本方式のプロトタイプである電子メールの履歴情報を用いた認証システムにおいて，基礎的な評価実験を行った結果，本認証システムの実現の可能性が確認できた．

A User Authentication Based On Personal History — A User Authentication System Using E-mail History

Masakatsu Nishigaki[†] and Makoto Koike[††]

It is very difficult for users to memorize secure passwords (long and random strings). This paper proposes a user authentication using personal history of each user. Here, authentication is done by giving answers to questions about the history of user's daily life. Users do not have to memorize any password, since the passwords are what users already know by experience. In addition, everyday-life experience increases day by day, and thus the question could change on every authentication trial. In this paper, a user authentication system using users' e-mail history is shown as a prototype of our proposal, and some basic experiments to evaluate the availability of the system are carried out.

1. はじめに

パスワードによる認証方式は非常に簡素で汎用性にも富むため，様々なシステムで採用されている．しかし，パスワード認証には長くランダムなパスワードは覚えにくい/短いパスワードまたは意味のあるパスワードは推測されやすいという「記憶の量」に関しての利便性と安全性におけるトレードオフが存在する．また，同じパスワードを使用し続けるといつかは総当たり攻撃によりパスワードが見つけられてしまう/パスワードを頻繁に変更する（覚えなおす）ことは難しいという「記憶の頻度」に関しての利便性と安全性におけるトレードオフも存在する[1)]．

しかし，近年はセキュリティに対する関心も高まり，利便性と安全性の両者を満足する認証方式の必要性が叫ばれている．それを実現するにあたっての１つの有効なアプローチと考えられるのが，人間が比較的得意とされる画像の記憶や個人的体験の記憶を利用する認証方式[2),3)] である．これらは，人間の記憶特性を活用することにより，パスワードの記憶負荷を減少させることを目的としている．本論文では，この考えをさらに発展させ，パスワードを記憶する必要すらない認証方式の実現を目指す．具体的には，「パスワードを覚える」から「覚えていることをパスワードとして使う」というコンセプトの転換を提唱し，これを「人間の行動履歴に基づくユーザ認証方式」として実装する．

以下，利便性と安全性の両立が可能なパスワードとして用いるに適した情報とは何であるかを２章で考察したうえで，３章でユーザの生活履歴をパスワードとして用いる認証方式を提案する．４章では，本方式のプロトタイプとしてメールの送受信履歴を用いた認証システムを作成し，その安全性の評価のための基礎的な実験を行う．５章では，メール履歴認証システムの改良とその評価実験の結果を報告する．そして，６章で本論文をまとめる．

† 静岡大学情報学部
Faculty of Informatics, Shizuoka University
†† デンソーテクノ株式会社電子１事業部
Electronic Div.I, DENSO TECHNO CO., LTD.

2. 本人がすでに知っている情報

人間は基本的にランダムな情報を覚えることが苦手である．よって，新たなパスワードを機械的に覚えるという方法は得策ではない．パスワードの記憶負荷を減少させるために，人間が比較的得意とされる画像の記憶や個人的体験の記憶を利用する認証方式[2),3)]が提案されているが，パスワードの記憶負荷を単に「減少」させるアプローチには限界がある．たとえば，文献 2) の方式においては，画像をパスワードとして使用することによって確かにそれを覚える際の記憶負荷は軽減されると思われるが，覚えなければならない画像が増えてくれば記憶負荷も相応のものとなるため，文献 2) の方式によってある程度のタイムスパンでパスワードを更新する（頻繁に新たなパスワード画像を覚えさせる）ような認証システムを実現することは難しいだろう．

複雑なパスワードを頻繁に更新するような認証方式を実現するにあたっては，パスワードの記憶負荷を「ゼロ」にするアプローチが不可欠だと思われる．その方法として，本論文では，「パスワードを覚える」から「覚えていることをパスワードとして使う」というコンセプトの転換を提案する．すなわち，「本人に関連のあること/本人がすでに知っていること」をパスワードとして使用するというアプローチを採る．

「本人に関連のあること/本人がすでに知っていること」とは，次の 2 つの情報に大別されるものと思われる．1 つは生年月日や趣味などの情報（本人固有の情報）で，もう 1 つは本人の経験に基づく情報（本人の履歴情報）である．以下，これらをパスワードとして用いるにあたっての利便性と安全性を各々検討する．

2.1 本人固有の情報

本人固有の情報としては，たとえば，以下のような情報があげられる．

- 生年月日，住所や職業などといった情報
- 好きな食べ物・色など趣味についての情報

本人固有の情報は，確かに，本人にとって改めて覚える必要のない情報である．しかし，これらの情報は，1 度決まるとそれ以降はほぼ不変である．そのため，これらをそのままパスワードとして用いると，いずれ他人に知られてしまう可能性がある．特に，生年月日，住所や職業などの情報は，ある程度一般に公開されていて他人が知ることができる情報である．また，趣味や趣向に関する情報は本人の周りに居る人や知人にはすでに知られている情報であるといえる．

以上より，本人固有の情報をパスワードとして用いるのはあまり適当ではないと判断される．

2.2 本人の履歴情報

本人の履歴情報としては，たとえば，以下のような情報があげられる．

- 昨日の夕食のメニュー
- 昨晩見た TV 番組

本人の履歴情報は本人がすでに体験・経験した事柄であるため，記憶に新しい出来事や記憶に残る出来事を適切に選ぶことで，（すでに知っているため）覚える必要のないパスワードとして使用できる可能性がある．さらに，これらの情報は，たとえば「今日の夕食」は翌日になると「昨日の夕食」となるように，生活していく中でつねに変化していく情報であるといえる．すなわち，このような情報をパスワードとして使用した場合，パスワードがある程度のタイムスパンでつねに変化していくパスワードと見なすことができる．また，一般に人間はだれしも 1 人きりの時間やプライベートな世界を持つため，本人の履歴情報の中には「本人以外には（家族や知人にも）知られていない，推測も容易ではない情報」も少なくないと思われる．

以上より，本人の履歴情報をパスワードとして用いることにより，「記憶の量」および「記憶の頻度」の双方に関して利便性と安全性をあわせ持つ認証方式が実現できるのではないかと考えられる☆．

3. ホームコンピューティングと履歴情報

3.1 ホームコンピュータのログ

最近の IT の発展にともない，ほとんどの家電製品にはマイコンが搭載され，電子制御されるようになっている．また，IPv6 環境では様々な機器に IP アドレスを割り当てることが可能となる[4)]．近未来のユビキタス社会においては，ゴマ粒大のコンピュータがありとあらゆるものに搭載され，それらすべてが機器間通信を行い，巨大なネットワークが構成されることになるだろう[5),6)]．

居住環境も格段にインテリジェント化され，家庭内のあらゆる家電がホームコンピュータと接続されて自律的，またはホームコンピュータの管理の下に協調して人間をバックアップするというホームコンピューティ

☆ 近年のバイオメトリクス認証の普及にともない，たとえば文献 11) のように，「人間の体が覚えている情報（文献 11) ではキーボード入力のリズム）」を認証に使用するアイデアも提案されている．しかし，これらの方式は基本的に「時間的に不変なユーザの特徴量」を利用してアノマリ検知によりユーザ認証を行うものである．本論文では時間的に不変な情報は「本人固有な情報」に分類されることになるため，そのような認証方式は本論文のスコープから外している．

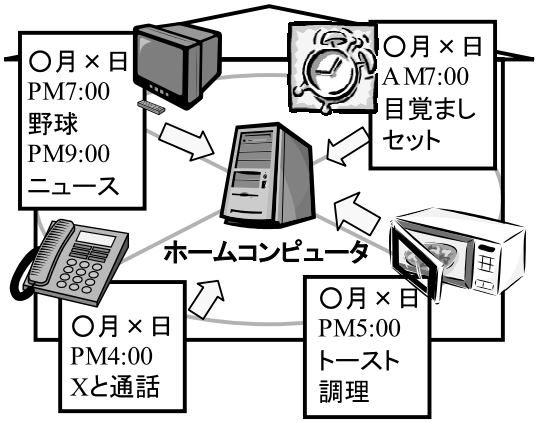

図 1 ホームコンピュータに蓄積されるログ
Fig. 1 Log data stored in home computer.

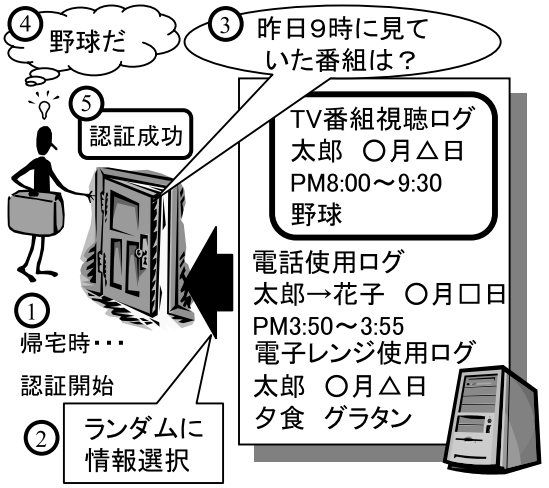

図 2 生活履歴を用いた認証システムの適用例（ホームセキュリティ）
Fig. 2 An application to home security.

ングの時代がやってくる[7]．すでに，電子メールの送受信機能を持つ電話機[8]，インターネットに接続して情報を取得することができる機能を備えたテレビ[7]や冷蔵庫，電子レンジ[9]などが実用化されている．

ホームコンピューティング環境では，様々な家電の状態や使用に関するログがホームコンピュータに残されていくことになると考えられる．すなわち，**図 1** で示すように，ビデオデッキから「昨日の×時から○○の TV 番組を録画した」という情報や，冷蔵庫や電子レンジから「今日の夕食に△△を作った」といった情報が絶え間なくホームコンピュータに蓄積されていく．

このように取得される家電の状態や使用によるログは，その家庭で生活している人間が家電を使用することで生じる情報であり，まさに「その人の生活の履歴」であるということができるだろう．すなわち，2.2 節で示した本人の履歴情報としてこのログ情報を使用することができるのではないかと期待できる．

3.2 ホームコンピュータのログを用いた認証システム

ホームコンピュータに残る各種のログをパスワードとして用いることにより，

(1) パスワードを覚える負荷がない（すでに知っている），
(2) 他人にとって，ユーザのパスワード（すなわち，そのユーザの個人の経験）を知ることは難しい，
(3) ログ情報は時々刻々と変化するために，ある程度のタイムスパンでパスワードの更新が行われる，

といった利便性と安全性の両者を満たす新しいパスワード認証方式を実現することが可能であると期待される．

例として，ホームセキュリティ（防犯システム）への適用として，玄関の鍵を本認証方式により開閉するシステムを**図 2** に示す．認証手順は以下のとおりになる．なお，その家の住人の生活履歴はすでにホームコンピュータに保存されているものとする．

(1) 玄関を開ける際には，玄関先に設置されている認証システムの端末を用いて認証を開始する．
(2) 認証システムは，ホームコンピュータに保存されている対象者（認証を要求しているユーザ）に関する生活履歴の中から 1 つをランダムに選択する．
(3) 認証システムの端末に，手順 (2) で選択された生活履歴に対する問合せとなる質問を呈示する．
(4) 認証を要求しているユーザはその質問に対する回答を端末に入力する．
(5) 正答であった場合，認証成功となり鍵が開く（必要ならば，手順 (2)～(4) を繰り返し，正答率が閾値以上であれば認証成功とする）．

3.3 考　　察

ログ情報の取扱い：

本方式では，ホームコンピュータに保存されているログは住人のプライバシに深く関わる情報であるため，ログ情報をホームコンピュータ以外の場所へ置くような運用形態は望ましくない．よって，3.2 節で示したホームセキュリティのような家庭内の認証は，本方式と相性が良い．本方式を家庭外での認証に使用する場合には，リバティ・アライアンス[10]との結合により，外部からホームコンピュータに認証の問合せを行

うといった運用☆が必要になると思われる．

また，一人暮らしをしているユーザを除くと，家族共用の情報家電におけるログ情報は各個人の認証に利用することが難しいという問題もあるだろう．これに対しては，(i) 目覚まし時計や携帯電話など，「一家に 1 台」ではなく「1 人 1 台」の情報家電のログ情報を使用する，(ii) 一家でパソコンを共用していたとしても，電子メールは（Web メールなどを利用して）各自が自分のメールアドレスを取得して個別に利用することが普通だと思われるので，メールアドレスごとのログ情報を利用する，などの対応が必要だと考える．

質問の形式：

本方式では，ホームコンピュータに保存されているログ情報より，どのような質問をいかに生成するのかという大きな問題が存在する．具体的には，

(a) それぞれのログ情報から適当な質問を自動生成するには，ある程度のインテリジェンスが必要になる（さもなければ，質問はすべて「○日前の×時に何をしていましたか？」という形式に固定せざるをえない），

(b) 人間の記憶というものは曖昧であるため「何日の何時に何をしていたか」という情報をすべて正確に記憶しているということはありえない，

(c) 正規ユーザをよく知る者ほど不正を行いやすい，

(d) 回答は選択式か記入式か，質問数は何問か，などによって，認証の安全性と利便性が変わってくる，

(e) 選択式の回答の場合には，成りすましを試みる不正者にも質問と回答の選択肢が呈示される．選択肢の中には正答が表示されるため，不正者が認証にパスしなかったとしても，プライバシ情報が少なからず漏洩する，

などの未解決問題が残る．十分な認証精度と利便性を保つための適切なログの選択方法，質問の生成方法，回答形式，質問回数などについては，今後の検討課題である．

☆ さらには，ログ情報を各情報家電の外に出さない（ホームコンピュータで集中管理しない）ようにしておき，認証の際にはホームコンピュータから各情報家電に問合せをするという方法も可能であろう．

4. 電子メールの履歴を用いた認証システム

本章以降で，本認証方式を利用したユーザ認証のプロトタイプを実装し，その実現可能性の評価を目的とした基礎実験を行う．ただし，現時点ではまだホームコンピューティング環境は現実のものとなっていない．また本方式には，3.3 節で述べたような質問形式に関する 5 つの未解決問題が残る．そこで本論文では，まずは単一の PC における電子メールの送受信履歴を用いることとし，かつ，主に 3.3 節の問題 (b) に注力して，システムの実装と実験を行うこととした．また 5 章では，本人認証率の向上およびプライバシの問題（3.3 節の問題 (e)）に対するアイデアを示し，これに関する追実験を行う．

なお，本方式のシステム化においては質問の自動生成が必須となるが，3.3 節の問題 (a) に示したようにメールの内容に関して問う記入回答式の質問を自動生成することは難しいため，本プロトタイプシステムでは「メールの本文を呈示して，その新旧を問う」という選択式の質問形態を採用することとした．この結果，本プロトタイプシステムでは 1 回の回答で認証判断をすることができず（新旧の回答の場合は成りすまし者も正答率が 50%となる），1 回の認証において複数回の質問を繰り返さざるをえなくなる．加えて，認証時にメールの本文が呈示されるため，成りすまし者がメールの内容を読むことができるというプライバシの問題も発生する．しかし，プロトタイプシステムでの実験を行う現時点では，これらの問題が含まれてしまうことはやむをえないとした（ただし，プライバシの問題に関しては 5 章でその対策について触れる．質問を繰り返さざるをえないことに関しては今後の課題としたい）．

4.1 電子メールの履歴を用いた認証システム

電子メールの履歴を用いた認証システムを**図 3** に示す．そして，その認証手順を以下に示す．

(1) ユーザが保持している送受信メールの中で，最近 n 日以内に送受信したメールを「最近のメール」とし，m 日前よりも以前に送受信したメールを「過去のメール」とする．ここで，$n < m$ である．

(2) ユーザが認証を要求すると，認証システムは当該ユーザの最近のメールと過去のメールを取り込む☆☆．

☆☆ 特に過去のメールは非常に多数となることが多いと考えられるため，現システムではとりあえず，それぞれ新しい順に最大 100 通までを取り込むようにしている．

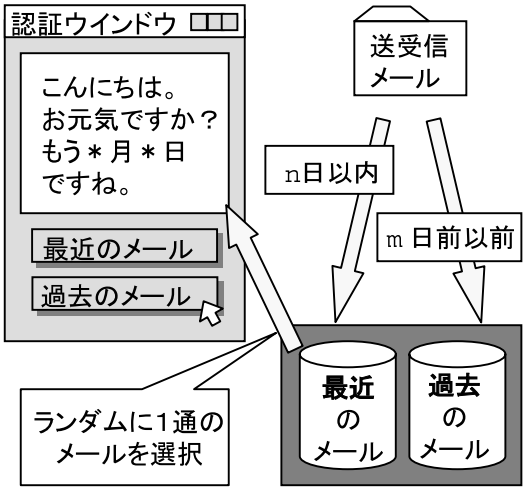

図 3 電子メールの履歴を用いた認証システム
Fig. 3 User authentication system using e-mail history.

(3) 認証システムは取り込んだメールの中から，ランダムに 1 通のメールを選択し，そのメールの本文のみを呈示する（From，To，Subject などのヘッダ情報は呈示しない）．
(4) ユーザは呈示されたメールを見て，そのメールが最近のメールか過去のメールかを答える．
(5) 手順 3〜4 を i 回繰り返す．
(6) i 回行ったうち，正答数が j 以上ならば認証成功とする．

ここで重要なのは，人間は「自分が経験したことの中でも記憶の残りやすさには差がある」ということである．このため，何らかの方法で，鮮明な記憶のみを取り出す（曖昧な記憶を排除する）という工夫が重要となる．そこで本システムでは，「$(n+1)$ 日前から $(m-1)$ 日前までのメールは認証に使用しない」というアイデアを導入した．人間の記憶は曖昧なため，そのメールが何日前に届いたメールであるかを特定することはまず不可能である．このため，たとえば 6 日前に届いたメールに対してここ 1 週間のうちに届いたメールか否かを問われても，確実な回答を返すことができない．本システムでは，人間の感覚の中で「最近と過去」の狭間に位置する期間を取り除くことにより，記憶の曖昧性を排除している．6 日前に届いたメールの例においては，たとえば $n=7$，$m=30$ とし，認証の際にユーザに「8 日前から 29 日前までのメールは質問の中に出てきません」と明示することにより，ユーザは「何日前のメールかは思い出せないが，さすがに 30 日以上も前のメールではないということは覚えている．8 日前から 29 日前までのメールは出てこないのであれば，このメールはここ 1 週間のうちに届いたメールに違いない」という判断を下すことができ，直感的に新旧の返答をすることが可能である．

また，「ユーザがその内容を自然に記憶しているメール」とは，自分にとって必要または有用な内容が記されているメールである．スパムメールやジャンクメールなどを記憶しているユーザは皆無であろう．そこで本システムでは，ユーザが送受信メールを複数のメールフォルダに振り分けて管理している場合，そのメールを認証に使用するか否かをフォルダ単位で選択できるようにした．すなわち，たとえばゴミ箱フォルダのメールは認証に使わないなどというように，ユーザがその内容を自然に記憶しているメールのみを認証に用いることができるように配慮されている☆．

なお，成りすましに対する耐性を考え，メール本文に日付や月を示す英単語そのものが含まれている場合には，それを自動的に削除する（‘∗’ で上書きする）ようにしている☆☆．

4.2 本認証システムを用いた基礎実験

本認証システムを評価するため，まず初めに 3 つの基礎実験を行った．

基礎実験 1：n と m の値の正答率への影響を調べるための実験
基礎実験 2：本人のメールを使用した認証実験
基礎実験 3：他人のメールを使用した成りすましの実験

基礎実験では，大学の研究室の学生を被験者として，本認証システムに関する基本的な知見を得ることを目的としている．残念ながら 1 日の送受信メール数が 10 通に満たないという学生がほとんどであったが，実験の初期においては試行錯誤的に多くの実験を試すことになるため，被験者の依頼が容易である学生を対象に実験を重ねることとした☆☆☆．また，読む行為だけの受信メールに対し，読む行為と書く行為が重なる送信メールの方が人間の記憶に残りやすいと考えられるため，本認証方式においては送信メールを使用するほうが理に適っていると考えられる．しかし，ほとんどの学生がメールの送信頻度が非常に少ないという状況

☆ すべてのメールに目を通さないユーザや，重要度の低いメールは読み飛ばすというユーザなどに対しても，既読メールもしくは重要メールのフォルダのみを認証に使用することにより，高い本人認証率が維持できると期待される．
☆☆ 時候の挨拶や時事の記事などから日時が推測されることも往々にしてあるが，これについては，今のところ現システムでは未対応である．
☆☆☆ 受信メール数が少ないため，基礎実験においては，すべてのメールフォルダを認証に使用してもらうこととした．

表 1 n と m を変化させた場合の正答率
Table 1 Correct answer rate on each values of (n, m).

期間	正答数							平均回答	正答数
$(n{:}m)$	A	B	C	D	E	F	計	時間 (秒)	(%)
3:30	7	9	10	10	9	8	53	6.4	88
7:30	8	9	10	9	10	8	54	6.0	90
14:30	8	9	10	9	9	8	53	6.3	88
3:14	9	10	8	9	10	7	53	6.1	88
7:14	10	9	9	10	8	8	54	6.5	90

であった．このため，以降の実験では送信メールは使用せず，受信メールのみを使用することとした．さらに，本論文は本システムの実現可能性を判断するうえでの基礎データを収集することを目的としているため，以降の実験では，4.1 節の手順 (5) および (6) における質問の繰返し回数 i を 1 として，メール 1 通 1 通に対する正答率を測ることにする．

4.2.1 基礎実験 1：n と m の値の正答率への影響を調べる実験

n と m の値が本システムの正答率にどのように影響するかを調べるため，n を 3，7，14，m を 14，30 と変えて，被験者のメールの新旧を被験者本人に答えてもらい，正答数を計測した．

被験者は本学情報科学科の男子学生 6 名（A〜F）である．n と m のそれぞれの組合せに対して，すべての被験者に各自の受信メール（最近のメールと過去のメール）の中よりランダムに 10 通のメールの本文のみを呈示し，メール 1 通 1 通における正答率を調べた．なお，各被験者に対して，実験初日に $(n, m) = (3, 30)$，$(7, 30)$，$(14, 30)$ に対する実験を行った後，5 日後に $(n, m) = (3, 14)$，$(7, 14)$ に対する実験を行っている．初日の 3 通りの実験において，各被験者に同じメールが呈示されることはない．5 日後の 2 通りの実験においても同様である．ただし，初日の実験と同じメール（の一部）が 5 日後の実験に使用されている．本来ならば，被験者が経験した過去の実験の影響が現れないように，すべての実験において同じメールを使用しないようにすべきだが，ここではおおよその傾向を知るための基礎実験であること鑑み，5 日間のインターバルを空けるだけとした．実験結果を**表 1** に示す．

表 1 より，すべての n と m の組合せにおいて，どの被験者も約 9 割の確率で自分の受信メールの新旧を正しく答えることができているのが分かる．n と m の値による有意差は認められず，「ここ 1 カ月のスパン（$n < m \leq 30$）においては，n と m の絶対的な値によらず，n と m に 1 週間程度以上の開きがあれば，人間はメールの新旧を直感的に判断できる」という結果が得られた．

表 2 本人のメールを用いた場合の正答率
Table 2 Correct answer rate for their own e-mails.

	A	B	C	D	E	F	G	計
呈示メール数	80	80	80	80	80	80	80	560
正答数	73	78	75	63	74	67	76	506
正答率 (%)	91	98	94	79	93	84	95	90

よって，以後の実験では，基礎実験 1 の結果で最も正答率が高く，平均回答時間が短かった $(n, m) = (7, 30)$ を採用することにする．

4.2.2 基礎実験 2：本人のメールを使用した認証実験

本認証システムの本人拒否率を調べるため，被験者本人のメールを使用し，1 カ月にわたって認証行為を行ってもらい，正答率を調べた．

被験者は，本学情報科学科の男子学生 7 名（A〜G）である．各被験者の受信メールにおいて最近 7 日以内に受信したメールを「最近のメール」，30 日前以前に受信したメールを「過去のメール」とした．すべての被験者に対して，最近のメールと過去のメールの中からランダムに 20 通のメールを選び，メール本文のみを呈示し，メールの新旧を判断してもらう．これを，1 週間以上の間隔をあけて 4 回（計 80 通）行い，メール 1 通 1 通における正答率を調べた．実験結果を**表 2** に示す．

表 2 より，被験者のメール 1 通 1 通に対する平均正答率は 90%という結果が得られた．実験後，被験者へ新旧の判断を誤ったメールについて尋ねたところ，特に定期的に配信される同じような内容のメール（メーリングリストによる定期的な連絡メールなど）などは記憶が曖昧で，それがどれくらい前のメールか思い出すことが難しいということであった．

4.2.3 基礎実験 3：他人のメールを使用した成りすましの実験

成りすましに対する耐性を調べるため，学生 A のメールを使用し，他人に学生 A のメールの新旧を判断してもらって，その正答率を調べた．

被験者は本学情報科学科の男子学生 5 名（B〜F）と 25 歳〜27 歳の本学情報科学科卒業の OB 3 名（H〜J）である．B〜F は学生 A と同じ研究室に所属している同期の学生であり，研究室内のメーリングリストや CC などにより学生 A と同じ内容のメールを受信するため，認証に使用された学生 A の受信メールの中には B〜F にとっても既知のメールが存在する．一方 OB 3 名は，在学中に学生 A と同じ研究室に所属しており，学生 A の人となりについてはよく知っている．しかし，現在は研究室を卒業しているため，認証に使用

表 3 他人のメールを用いた場合の正答率
Table 3 Correct answer rate for other's e-mails.

同期生	B	C	D	E	F	計
呈示メール数	80	80	80	80	80	400
正答数	52	52	56	52	53	265
正答率 (%)	66	65	70	65	66	66
既知のメール数	27	25	33	36	35	156
OB	H	I	J			計
呈示メール数	80	80	80			240
正答数	45	51	41			137
正答率 (%)	56	64	51			57
既知のメール数	0	0	0			0

された学生 A の受信メールと同じメールは 1 通も受信していない．

学生 A の最近のメール（7 日以内に受信したメール）と過去のメール（30 日前以前に受信したメール）の中からランダムに 20 通のメールを選び，これら被験者 8 名に対し，メール本文のみを呈示しメールの新旧を判断してもらう．これを，1 週間以上の間隔をあけて 4 回（計 80 通）行い，メール 1 通 1 通における正答率を調べた．実験結果を**表 3** に示す．

表 3 より，既知のメールがない OB の平均正答率は 57%という結果であった．本認証システムは 2 択であるため，新旧の判断をランダムに行った場合，平均正答率は約 50%となる．OB の平均正答率が 50%に近い値だった（有意差が示されなかった）ことから，OB は知らないメールに対してほとんど「あてずっぽう」で答えることしかできなかったということが確かめられた．しかしながら，実験後の OB への聞き取り調査より，メール本文に日付を表すような言葉や時事的な話題などが含まれている場合には，比較的容易に新旧の判断が可能だったことが分かった．

同期生の平均正答率は 66%という結果であった．調べたところ，呈示されたメール数の約 40%が同期生にも同報されていたメールであった．また，基礎実験 2 の結果より本人のメールに対して，ユーザは約 90%で正しく答えることができることが分かっている．以上より，同報メールではない残りの約 60%のメールに対する同期生の平均正答率を X とすると，$0.40 \times 0.90 + 0.60 \times X = 0.66$ が成立することから，X は約 0.5 であると求まる．つまり，同期生も，自分が知らないメールに対してはほとんど「あてずっぽう」で答えることしかできなかったということが分かる．

本実験より，攻撃者が知らないメール（正規ユーザのプライベートなメール）を認証に使用することで，成りすまし成功率を低く抑えることができる可能性が示された．ただし，本システムがメールの新旧を問う 2 択のシステムである以上，たとえば質問を 10 回繰り返したとしても，回答の組合せは $2^{10} = 1{,}024$ 通りしか存在しない．そのため，完答を要求したとしても，1/1,024 の確率（約 0.1%）で成りすましを許してしまうことになる．

4.3 基礎実験の考察

基礎実験の結果より，「$(n+1)$ 日前から $(m-1)$ 日前までのメールは認証に使用しない」という工夫を加えることにより，受信メールの履歴を用いた認証方式が正常に機能する可能性が確認できた．しかし，これだけでは記憶の曖昧なメールをすべて排除することができず，認証精度は 90%程度にとどまるという結果であった．

成りすましを防ぐためには，認証の際の質問に攻撃者が知らないメールを呈示する必要がある．このためには，(i) 正規ユーザのプライベートなメールのみを使用する，または，(ii) 攻撃者の知らないメールをダミーとして混入させる（正規ユーザならば自分のメールでないものを見分けることが可能），などの方策が有効であろう．特に，本認証システムは認証に使用するメールをフォルダ単位で指定できるので，ユーザのプライベートなメールが多く含まれるメールフォルダを指定して認証を行うことは容易に実施可能である．ただし，プライベートなメールは数が限られてくるという問題がある．また，成りすましの際に不正者があてずっぽうで答えることを考えると，選択肢を増やすことだけでもある程度の成りすまし対策となると思われる．

本認証方式では，認証時に正規ユーザの受信メールの内容が呈示される．すなわち，成りすましを試みる攻撃者が正規ユーザのメールを読むことができてしまう．これはプライバシの観点からは大きな問題となる．

5. 電子メールの履歴を用いた認証システムの改良

4 章において示した本認証システムの基礎実験からは，本認証方式の実用の可能性が示唆される結果が得られた．しかし，基礎実験では 1 日の平均受信メール数が 10 通未満の被験者を対象としており，正答率も 90%程度にとどまっている．

本認証システムでは「最近と過去」の狭間に位置する期間のメールを除くことにより記憶の曖昧性を排除することを試みているが，これだけでは人間の感覚における曖昧性を完全に排除することができていない．

加えて，本認証システムでは認証の際にメール本文が呈示されるため，他人があるユーザに成りすまして

認証を受ける時点ですでに当該ユーザのメールの内容を読むことができる（認証にパスしなくても当該ユーザのメールを読める）というプライバシの問題がある．

これらの問題点をまとめると次のようになる．

問題点 1)：日常的に大量のメールを受信しているユーザに対する評価が不十分である．

問題点 2)：新旧の判断が困難である曖昧なメールを完全に排除しきれていないため，本人拒否率が増加している．

問題点 3)：認証時にメール本文が呈示されるため，他人がメールの内容を簡単に知ることができるというプライバシの問題がある．

本章では，問題点 2）と問題点 3）の改善を試みるための改良方式を提案する．そして，問題点 1）を鑑み，改良方式に対して，情報系企業に勤める社会人を被験者とした評価実験を行う．

5.1 認証システムの改良方式

本節では，問題点 2）の改善を試みるための改良方式と，問題点 3）の軽減を試みるための改良方式を提案する．

問題点 2）に対する提案は，認証時の選択肢を細粒度化することである．認証時の選択肢を「最近のメール」,「過去のメール」の 2 択から,「確実に最近のメール」,「曖昧だが最近のメール」,「確実に過去のメール」,「曖昧だが過去のメール」の 4 択に変更する．そして，ユーザ自身が，確実だと判断したメールだけを認証に使用することで，記憶の曖昧なメール（定期的に配信されるメールや定期的な書式を持つメール，よく読まなかったメールなど）をさらに排除することが可能になると期待される．これを改良方式 α とする．

問題点 3）に対する提案は，認証に使用するメールの中に，当該ユーザが受信していないダミーメールを含める方式である．これにより，たとえ他人にメールを読まれたとしても，そのメールが正規ユーザのメールなのかダミーメールなのかの判断が困難となり，プライバシの問題が軽減されると考えられる．これを改良方式 β とする．

問題点 1）を鑑み，これら改良方式に対して，情報系企業に勤める社会人を被験者とした評価実験を行う．被験者は 26〜45 歳の情報系企業の社会人 8 名（O〜V）である．各被験者のメールの受信状況について**表 4** に示す．なお，表 4 においては，スパムメールやウィルスメールなどを「不要なメール」，それ以外を「必要なメール」と定義しており，1 行目に「1 日の平均受信メール数」，2 行目に「受信するメールのうちで不要メールの割合」が記されている．表 4 の 3 行目は「受信メールをカテゴリごとに各メールフォルダに振り分けて管理しているか否か」が YES/NO で示されており，YES の被験者に対しては，4 行目に「不要メールのメールフォルダ（ゴミ箱フォルダ）内のメールを認証に使用したか否か」が，5 行目に「すべてのメールフォルダのうち，何割のメールフォルダの中のメールを認証に使用するように設定したか」が記されている．

表 4 被験者のメール受信状況
Table 4 Average number of e-mails received.

	O	P	Q	R	S	T	U	V
1 日の平均受信数	50	50	80	150	70	100	30	40
不要メールの割合 (%)	60	0	70	60	1	30	1	30
フォルダを分けて管理	○	○	×	○	○	○	○	○
不要メールの使用	×	×	–	×	○	○	○	×
認証に使用した割合 (%)	50	30	–	50	20	70	80	50

5.2 4 択認証システム（改良方式 α）の評価

5.2.1 本人拒否率の評価

改良方式 α の本人拒否率を調べるため，被験者本人のメールを使用し，1 カ月にわたって認証行為を行ってもらい，正答率を調べた．

被験者は表 4 の 8 名（O〜V）である．各被験者の最近（7 日以内）の受信メールと過去（30 日前以前）の受信メールの中からランダムに 30 通のメールを選び，各被験者にメール本文のみを呈示し，メールの新旧を「確実に最近のメール」,「確実に過去のメール」,「曖昧だが最近のメール」,「曖昧だが過去のメール」の 4 択で回答してもらう．これを，1 週間以上の間隔をあけて 4 回（計 120 通）行い，メール 1 通 1 通における正答率を調べた．

改良方式 α に関する本実験は，選択肢を 2 択から 4 択に細粒化したことによる認証率の変化を調べることが目的である．そこで，今回実施した 4 択システムの実験結果に関しては，これを擬似 2 択システムとして見た場合の正答率についても算出し，擬似 2 択システムの正答率と 4 択システムの正答率を比較することにする．

まず，被験者が「確実に最近のメール」,「曖昧だが最近のメール」と答えた場合を「最近と判断した」と分類し，被験者が「確実に過去のメール」,「曖昧だが過去のメール」と答えた場合を「過去と判断した」と分類したうえで，その回答の正答数，正答率を示したのが**表 5** である．表 5 は，4 択の認証システムを擬似的に 2 択の認証システムと見なした場合の認証率であると考えることができる．

表 5 より，1 日の平均受信メール数が 30〜150 通のユーザであっても，平均 85%の確率でメールの新旧に対する 2 択の判断ができていることが確認できる．

表 5 社会人における疑似 2 択認証システムの正答率
Table 5 Correct answer rate for their own e-mails on two-alternative question system.

	O	P	Q	R	S	T	U	V	計
呈示メール数	120	120	120	120	120	120	120	120	960
正答数	108	108	84	106	101	105	88	112	812
正答率 (%)	90	90	70	88	84	88	73	93	85

表 6 社会人における 4 択認証システムの正答率
Table 6 Correct answer rate for their own e-mails on four-alternative question system.

	O	P	Q	R	S	T	U	V	計
呈示メール数	120	120	120	120	120	120	120	120	960
確実と判断	83	104	52	86	60	86	38	101	610
正答数	83	100	49	85	60	86	38	101	602
正答率 (%)	100	96	94	99	100	100	100	100	99
曖昧と判断	37	16	68	34	60	34	82	19	350
正答数	25	8	35	21	41	19	50	11	210
正答率 (%)	68	50	51	62	68	56	61	58	60

次に，被験者が「確実に最近のメール」,「確実に過去のメール」と答えた場合を「確実と判断した」と分類し，被験者が「曖昧だが最近のメール」,「曖昧だが過去のメール」と答えた場合を「曖昧と判断した」と分類したうえで，それぞれのメールの数，正答数，正答率を示したのが**表 6** である．表 6 は 4 択の認証システムにおける認証率であり，表 5 と表 6 の差が選択肢を 2 択から 4 択に改良したことによって得られる効果であると考えることができる．

表 6 より，4 択の認証システムにおいて，ユーザが確実と判断した場合のみの回答を見れば，正答率は約 99%に達することが確かめられる．

5.2.2 成りすまし成功率の評価

1 日の平均受信メール数が比較的多いユーザのメールに対し，改良方式 α の成りすまし成功率を調べる．

5.2.1 項の被験者 O を正規ユーザと仮定し，25〜27 歳の本学情報科学科卒業の OB 7 名（H〜N）に成りすまし行為を行ってもらう．O の最近（7 日以内）の受信メールと過去（30 日前以前）の受信メールの中からランダムにメールを選び，H〜N にメール本文のみを呈示する．H〜N は，メールの新旧を「確実に最近のメール」,「確実に過去のメール」,「曖昧だが最近のメール」,「曖昧だが過去のメール」の 4 択で回答する．60 通のメールに対して，メール 1 通 1 通における正答率を調べた．

なお，O は H〜N の在学時の卒業研究指導教員であり，H〜N は O という人物をよく知っている．また，H〜N の 1 日の平均受信メール数を**表 7** に示す．成りすましの実験においては，攻撃者自身が受信しているメールの記憶が成りすましにあたってのノイズになる可能性があると考えたため，5.2.1 項の O 以外の被験者 P〜V ではなく，1 日の受信メール数が少ない H〜N を攻撃者として採用した．

表 7 攻撃者の 1 日の平均受信メール数
Table 7 Average number of e-mails that adversaries receive.

	H	I	J	K	L	M	N
1 日の平均受信数	30	40	5	40	3	2	15

表 8 他人のメールに対する疑似 2 択認証システムでの正答率
Table 8 Correct answer rate for other's e-mails on two-alternative question system.

	H	I	J	K	L	M	N	計
呈示メール数	60	60	60	60	60	60	60	420
正答数	35	25	28	37	33	31	27	216
正答率 (%)	58	42	47	62	55	52	45	51

表 9 他人のメールに対する 4 択認証システムでの正答率
Table 9 Correct answer rate for other's e-mails on four-alternative question system.

	H	I	J	K	L	M	N	計
呈示メール数	60	60	60	60	60	60	60	420
確実と判断	16	1	40	60	48	35	29	229
正答数	13	1	18	37	28	18	13	128
正答率 (%)	81	100	45	62	58	51	45	56
曖昧と判断	44	59	20	0	12	25	31	191
正答数	22	24	10	0	5	13	14	88
正答率 (%)	50	41	50	—	42	52	45	46

本実験は，本人認証率の実験と同様，選択肢を 2 択から 4 択に細粒化したことによる成りすまし成功率の変化を調べることが目的である．そこで，まず，擬似 2 択システムと見なした場合の攻撃者の正答率を算出した．これを**表 8** に示す．表 8 より，O のメールに対する平均正答率は 51%であった．よって，攻撃者 H〜N は O のメールの新旧を「あてずっぽう」で答えることしかできなかったといえる．

次に，4 択の認証システムにおける成りすまし成功率を示したのが**表 9** である．表 9 より，攻撃者が確実と判断した場合の平均正答率は 56%となり，2 択システムとほぼ同様に，攻撃者 H〜N は O のメールの新旧を「あてずっぽう」で答えることしかできなかったということが分かる．なお，攻撃者 I の正答率が 100%であるが，呈示された 60 通のメールに対し，確実に判断できたメールの数がたった 1 通であるため，成りすまし耐性が弱いということを意味するものではない．

以上の結果より，4 択の認証システム（改良方式 α）は成りすまし成功率の向上を低く抑えながら，本人拒否率の改善をすることが可能であることが確認できた．

5.3 ダミーメールを含める方式（改良方式 β）の評価

改良方式 β は，他人にメールを読まれたとしても，他人にはそのメールが正規ユーザのメールなのかダミーメールなのかが分からないということを利用して，本認証方式におけるプライバシの問題の軽減を試みる方式である．その評価を行うにあたっては，(i) 攻撃者が呈示されるメール本文を見て，それが正規ユーザのメールかダミーメールかを判断することがどの程度困難であるかを調べることと，(ii) ダミーメールの混入により，正規ユーザ本人の認証成功率が低下するような弊害が生じないかを調べることが必要である．

5.3.1 攻撃者によるダミーメールの判別実験

攻撃者は 5.2.2 項の H〜N の 7 名である．この 7 名に，5.2.1 項の被験者 O のメールとダミーメールをランダムな順で呈示し，それらが「正規ユーザ O のメール」であるか「ダミーメール」であるか 2 択で答えてもらう．なお，5.2.2 項でも述べたが，被験者 O は攻撃者 H〜N の在学時の卒業研究指導教員であり，H〜N は O という人物をよく知っている．

O の正規の受信メールの内容は，

- 仕事関連のメール（O は情報セキュリティ関連の研究者である）
- IT 関連のニュースメール

である．ここに以下のようなダミーメールを加えることとした．

- Web で公開されている情報セキュリティ関連のメーリングリスト，メールマガジンにおける任意のメール（O はこれらのメーリングリスト，メールマガジンを購読していない）

ダミーメールの混合率は 50%とした．被験者 H〜N には，ダミーメールが 50%含まれているという情報と，ダミーメールは Web で公開されている任意のメーリングリスト，メールマガジンのメールを利用しているという情報を与えた．

まず，O の最近（7 日以内）の受信メールの中から 15 通，過去（30 日前以前）の受信メールの中から 15 通をランダムに選択した．次に，上述のメーリングリスト，メールマガジンから前もって多量のメールをダミーメールとして採集しておき，その中からランダムに 30 通のメールを選択した．そして，計 60 通のメールをランダムな順序で攻撃者に呈示し，攻撃者に「正規ユーザのメール（過去のメール，または最近のメール)」,「ダミーメール」の 2 択で答えてもらい，メール 1 通 1 通に対する正答率を調べた．結果を**表 10** に示す．

表 10 攻撃者によるダミーメール判別の正答率
Table 10 Detection rate of dummy mails by adversaries.

	H	I	J	K	L	M	N	計
呈示メール数	60	60	60	60	60	60	60	420
正答数	29	27	39	40	52	27	26	240
正答率 (%)	48	45	65	67	87	45	43	57

表 11 本人によるダミーメール判別の正答率
Table 11 Detection rate of dummy mails by themselves.

	O	P	Q	R	S	T	U	計
呈示メール数	60	60	60	60	60	60	60	420
正答数	60	60	58	60	60	59	60	417
正答率 (%)	100	100	97	100	100	98	100	99

表 10 より，攻撃者 L が約 90%の高い確率で O のメールを見破っているという結果が得られた．実験後，L に聞き取り調査を行ったところ，本実験でダミーメールとして使用したメーリングリスト，メールマガジンを L も購読したことがあり，メール本文の内容や書式などからそのメールがダミーメールであることが判断可能であったとのことだった．

しかしながら，被験者 7 名の平均正答率は 57%であることから，一般的には（ダミーメールの出所を適切に設定できれば），呈示されたメールが正規ユーザのメールかダミーメールか判断することはある程度困難であるということが確かめられた．

5.3.2 ダミーメールの本人認証率に対する弊害

被験者は，5.2.1 項の被験者 O〜U の計 7 名である．本実験では被験者が情報系企業の社会人であることから，ダミーメールとしては

- Web で公開されている IT 関連のメーリングリスト，メールマガジンにおける任意のメール（各被験者はこれらのメーリングリスト，メールマガジンを購読していない）

を利用した．

まず，各被験者の最近（7 日以内）の受信メールの中から 15 通，過去（30 日前以前）のメールの中から 15 通をランダムに選択した．次に，上述のメーリングリスト，メールマガジンから前もって多量のメールをダミーメールとして採集しておき，その中からランダムに 30 通のメールを選択した．そして，計 60 通のメールをランダムな順序で本人に呈示し，各被験者に「自身のメール（過去のメール，または最近のメール)」,「ダミーメール」の 2 択で答えてもらい，メール 1 通 1 通に対する正答率を調べた．実験結果を**表 11** に示す．

表 11 より，ほとんどの被験者の正答率が 100%であり，100%の正答率とならなかった被験者 Q，T に対

しもほぼ 100%に近い正答率であることが確かめられる．この結果より，正規ユーザならば本人の正規メールとダミーメールの判断はほぼ確実に行うことができるため，ダミーメールを含める方法（改良方式 β）を採用したとしても，本人認証率を低下させることはほとんどないだろうということが期待できる．

5.4 考　　察

5.4.1 情報系企業・情報系研究機関の社会人を対象とした認証実験について

5.2 節の実験を通じ，本方式が一般の社会人の認証にも利用可能であるという可能性を示すことができた．

ただし，5.2.1 項で行った実験では，各被験者は 1 週間に 1 度の認証行為を 4 週間行っただけである．特に，短時間のうちに頻繁に認証を繰り返す必要がある場合などには，認証を繰り返すうちに過去のメールを何度も見ることにより，最近と過去の記憶の混乱が引き起こされる可能性がある．これについては，追実験を行い，本方式の評価をする必要があるだろう．

5.4.2 改良方式 α について

5.2.1 項で行った実験より，認証時の選択肢を 4 択にし，ユーザ自身が確実と判断したメールのみを認証に使用することで，記憶の曖昧なメールをさらに排除し，本人拒否率を格段に減少させることができた．

ただし，改良方式 α においては，ユーザが「曖昧だが最近」,「曖昧だが過去」と答えた場合の取扱いが問題となる．たとえば，この質問を i 回繰り返すシステムの場合においては，呈示される i 通のメールの中にユーザが「確実に最近」,「確実に過去」と判断できるメールが少なかった際には，認証の成否の判断に使用されるメールが少なくなり認証精度が下がることになる．逆に，「確実に最近」,「確実に過去」と答えた回数が i 回に達するまで試行を繰り返すようなシステムとした場合，確実に判断できるメールが i 回呈示されるまで認証が終了しないことになる．

なお組合せ論的には，2 択方式の質問を 10 回繰り返した場合の回答の組合せが $2^{10} = 1{,}024$ 通りであるのに対し，4 択方式の場合は $4^{10} = 1{,}048{,}576$ 通りとなる．

5.4.3 改良方式 β について

5.3 節で行った実験より，認証時に呈示するメールにダミーメールを含めると，攻撃者に対しては呈示されたメールが本当に正規ユーザのものであるか否かの判断をある程度困難にする効果があり，正規ユーザに対しては本人認証にあたっての弊害にならないということが確認できた．

ただし，改良方式 β を実用に供するには，どういうメールをダミーメールとして選べばよいのか，そのダミーメールを自動的に収集したり，定期的に更新するにはどうすればよいのか，などの課題を解決していく必要がある．

また，正規ユーザのメールにおいては，末尾に署名をつけたり，冒頭で自分の名前を名乗ることが一般的である．これに対し，ダミーメールには本人の署名や名前は現れない．よって攻撃者は，少なくとも，正規ユーザが発信したメールについては，これを簡単に見分けることが可能であろう．これに対処するためには，メールの本文を呈示するにあたって，正規ユーザの名前や署名部分に対しても ‘∗’ で上書きするような工夫が必要となると思われる．

ダミーメールを含める方法は，正規ユーザのメールをダミーメールの中に隠すという「木を森に隠す」タイプのアプローチである．正規ユーザのメールが認証時に呈示されること自体を阻止したい場合には，たとえば，「記憶負荷の負担が無視できる程度のユーザの覚えやすい 4 桁の PIN（暗証番号）を設定することにより，まずは第一次認証を実施し，これにパスしたユーザに対して，本方式の認証を行う」という 2 段階の認証方式などを採用する必要があるだろう．

6. ま と め

本論文では，「パスワードを覚える」から「覚えていることをパスワードにする」というコンセプトの転換により，利便性と安全性の両者を満足するパスワード認証方式として，ユーザの生活履歴を用いた認証方式を提案した．近未来に実現されるホームコンピューティング環境では，あらゆる家電の状態や使用履歴のログがパスワードとして利用できる．これらのログをパスワードとして用いることで，1）パスワードを覚える負荷がない（すでに知っている），2）他人にとっては，ユーザのパスワード（すなわち，そのユーザの個人の経験）を知ることは難しい，3）行動履歴は時々刻々と変化するために，ある程度のタイムスパンでパスワードの更新が行われるなどの特長を有し，記憶の量と頻度において利便性と安全性をあわせ持つ本人認証が実現できると期待される．

また，本方式のプロトタイプとして，PC におけるユーザの電子メールの送受信履歴を用いたユーザ認証システムを構築し，基礎実験を通じて，その実用の可能性を示した．さらに，基礎実験で明らかとなった本電子メール型認証システムにおける問題に対し，記憶の曖昧なメールをさらに排除するための改良方式と，プライバシの問題を軽減するための改良方式を提案し

た．そして，それぞれの改良方式について追実験を行い，その効果を確認した．

今後の発展として，電子メールの送受信履歴を用いた認証システムについては，受信メールだけでなく送信メールも使用した場合，また，頻繁に認証を行った場合など，より実用を考慮した評価実験を行う必要があるだろう．一方，電子メールの送受信履歴を用いた認証システムは，ここでの提案方式の一例を示したにすぎない．将来的には，電子メール以外の情報家電の使用履歴を用いた認証システム，および，複数の家電の履歴情報による認証システムなどの実現を目指したい．おそらく，利用する情報家電の履歴情報ごとに，人間の記憶の曖昧性を除くためのアプローチはまったく異なってくることが推測される．今後，様々な情報家電の使用履歴による認証方式に対する知見を 1 つずつ蓄積していき，最終的に，履歴型認証方式全般に対する評価へつなげていきたいと考える．

謝辞 本研究の評価実験にご協力いただきました（株）日立製作所システム開発研究所高橋健太氏，NTT データ（株）技術開発本部の皆様，静岡大学情報学部西垣研究室 OB の皆様，その他被験者の皆様に深く感謝いたします．また，本研究の成果の一部は，応用セキュリティフォーラムの研究プロジェクトとして推進されたものである．

参 考 文 献

1) 増井俊之：インターフェイスの街角（42）—明るい認証システム，*UNIX MAGAZIN*, Vol.16, No.7, pp.185–189 (2001).
2) Dhamija, R. and Perrig, A.: DèjáVu: A User Study Using Images for Authentication, *9th Usenix Security Symposium*, pp.45–58 (2002).
3) 高田哲司，小池英樹：あわせ絵：画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法，情報処理学会論文誌，Vol.44, No.8, pp.2002–2012 (2002).
4) BroadbandWatch：パネルディスカッション「家庭 IPv6 ネットワークおよび IPv6 家電の展望」(2002). http://bb.watch.impress.co.jp/cda/news/355.html
5) japan.internet.com：「総務省，ユビキタス技術の将来像に関する報告書を発表」(2002). http://japan.internet.com/public/news/20020617/2.html
6) 高橋史忠：ごま粒チップがめぐる 2 つの「センサー」がもたらすもの，日経エレクトロニクス，Vol.2003-3-2-17 (2003).
7) 総務省：情報通信審議会/情報通信政策部会インターネット利用高度化委員会（第 12 回）配布資料 3 (2002). http://www.soumu.go.jp/joho_tsusin/policyreports/joho_tsusin/joho_bukai/pdf/020412_1_3.pdf
8) NTT 東日本：L モード電話機のウェブページ. http://www.ntt-east.co.jp/Lmode/01_3_kiki/index.html
9) CEATEC JAPAN 2002：エコーネット規格対応製品のウェブページ (2002). http://www.echonet.gr.jp/ceatec2002/ceatec.htm
10) LIBERTY ALLIANCE PROJECT: LIBERTY ALLIANCE PROJECT. http://www.projectliberty.org/jp/index.html
11) 前田 剛，富永洋平，小泉寿男：パスワード入力にリズムを取り入れた個人認証方式の開発，マルチメディア，分散，協調とモーバイル（DICOMO'99）シンポジウム論文集，pp.351–356 (1999).

(平成 17 年 3 月 25 日受付)
(平成 17 年 12 月 2 日採録)

西垣 正勝（正会員）

平成 2 年静岡大学工学部光電機械工学科卒業．平成 4 年同大学大学院修士課程修了．平成 7 年同大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，平成 8 年静岡大学情報学部助手．平成 11 年同講師，平成 13 年同助教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シュミレーション等に関する研究に従事．

小池 誠

平成 15 年鳥取大学工学部知能情報工学科卒業．平成 17 年静岡大学大学院修士課程修了．同年デンソーテクノ株式会社入社．在学中，情報セキュリティに関する研究に従事．