マルチパスワードのランダム問いかけによる本人認証方式の研究

高橋　一生　藤澤　公也†
東京工科大学メディア学部‡

1. はじめに

現在のネットワーク社会の中でいくつかの脅威がセキュリティにおいて問題とされている．その脅威として挙げられている一つとして，「なりすまし」の問題がある．しかし，多くの場所で問題とされているのは「当事者が意図しないところで行われる，第三者によるなりすまし」であり，「当事者と第三者によって行われる意図的ななりすまし」の問題については軽視されている．後者の問題は具体的には商業用データベースのパスワードを多人数で共有する，認証を用いた授業の出席確認において代返を行うなどが挙げられる．

本研究では多くの場所で用いられているパスワード認証を，ハードウェアを交換することなくソフトウェアによって「当事者と第三者によって行われる意図的ななりすまし」（以下，「意図的ななりすまし」とする）を抑制することを目的とした．

2. 提案する認証方法

2.1 基本となるパスワード認証の定義

本研究で提案する，認証方法の基本となるパスワード認証として，電子商取引推進協議会による「本人認証技術の評価基準（第 1 版）」の本人認証の基本モデルを用いた[1].

この基本モデルに基づき，以下認証される側を認証請求者，認証を行う側を認証者と呼ぶ.

2.2 パスワード認証の変更点の仕様

一般的なパスワード認証で意図的ななりすましが起こる原因は認証請求者がパスワードを管理（記録や記憶）していることである．認証請求者が管理している情報を他者に渡せば簡単に代理が成り立ってしまう．つまり，認証請求者に対してどんなパスワードが認証者に登録されているかを思い出しにくくすれば，パスワードを他者に渡すことは困難になると考えられる.

そのため，本研究では基本となるパスワード認証から以下のように変更した.

- パスワード管理者を認証者のみとする
- 登録パスワード数を複数にする
- 要求するパスワードをランダムに変化させる
- 認証のたびに新規パスワードを登録していく
- 認証通過に必要なパスワード正解数を複数とする

2.3 変更に伴い追加する仕様

しかし変更点がこれだけでは，例え本人が認証を行ったとしても設定されているパスワードを答えることができず，認証が成り立たない．そのため，それを補うためパスワードを個人情報とする．個人情報であれば，認証請求者がどんな登録パスワードをわからないとしても，パスワードを問われれば答えられることが期待できる．認証を行うときは，個人情報を尋ねる文字列である「問いかけ」を用いてパスワード入力の要求を行う．本研究では，意図的ななりすましを抑制するため，前節と本節の変更点を持つパスワード認証方法を提案する.

3. 検証実験

3.1 検証方法

本研究では提案する認証方法を評価するための検証方法として実験を行った．本研究で問題とする意図的ななりすましの具体例としては，学校の授業での出席確認にパスワードを用いる場合での代返を対象とした．実際に実験で比較対象とするパスワード認証は，東京工科大学における授業での出席確認で使用される ASSIT システムの認証部分とした.

提案するパスワード認証は，本実験用に必要な機能のみを実装したシステムを用いた．具体的には，認証サーバとネットワークを用いた仕組みを持たず，提案する認証方法とユーザーインターフェースのみを実装している.

Person authentication system using random question of multi password
†Kazuki TAKAHASHI Kimiya FUJISAWA
‡School of Media Science, Tokyo University of Technology

表 1:代返成功率と認証にかかった時間の比較

被験者	代返失敗率(%)	認証段階で認証にかかった時間の平均(秒)	代返段階で認証にかかった時間(秒)
A	0	71	135
B	40	40	168
C	50	39	120
D	50	23	90
E	25	37	55
F	0	42	54
平均	27.5	42	103.7

3.2 実験の手順

実験は提案する認証方法が運用され，代返が行われたことを想定して行い，その流れごとに 3 段階に分けて行った．その段階は，提案する認証方法を使用するにあたっての準備として認証者にパスワード登録を行う「実験準備段階」，本人として数回の認証を行う「認証段階」，擬似的に代返を行う「代返段階」の 3 段階とした．

4. 評価

4.1 記憶している問いかけ数の比率

実験の評価として，提案する認証方法が，認証者に登録しているパスワードに関する情報の再生を困難にしているかを評価した．認証者に登録している問いかけ数と再生できた問いかけ数の比率を求めた結果，平均 68.3 パーセントの再生率であった．

4.2 代返を行う際の失敗率と労力

代返の失敗率は平均 27.5 パーセントと低い値をつけた．しかし，値としては低いが，ある程度の失敗するリスクを上げることには成功していることがわかる．また，代返を行う際の労力として，実験では本人認証が終了するまでの時間を取得した．その結果，代返をしない状態で 42 秒，代返を行った状態で 103.7 秒と，代返をすることで倍以上の時間がかかることがわかった(表 1)．

4.3 代返に対する抑制効果

代返を行う際の心理的な抑制効果の評価として，実験の中で被験者に 5 段階評定のアンケートを実施した．アンケートの質問は，代返のしにくさを代返が行われる段階ごとに尋ねる(1)～(7)の 7 項目を使用した．その計 7 つの質問を，ASSIT システムの認証と提案する認証方法の 2 つのそれぞれの場合で尋ねた．

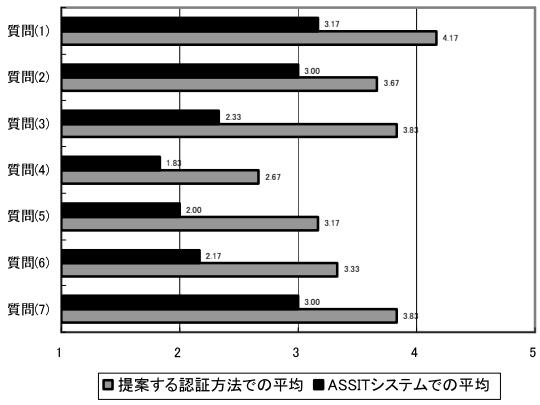

図 1:アンケート結果の比較

その結果の平均を求めたところ，全ての場合で提案する認証方法の方が代返を行いにくいという結果になった(図 1)．

4.4 正当なユーザのみ認証を通過できるか

認証請求者が本人であった場合は認証を通過できるかどうかの評価を行った．実験の結果，本人であるのに認証に失敗した被験者は 0 であった．

また，本人でないユーザが認証を行おうとした場合，パスワード情報を全く持たない状態では認証を通過できないかを実験した．この実験結果も，本人でないにもかかわらず認証を通過できた被験者は 0 であった．

5. まとめ

本研究では，問題として扱われることが少ない「当事者と第三者による意図的ななりすまし」に対して問題解決を目指した．問題解決の方法として，一般的なパスワード認証を改変した新しいパスワード認証方法を提案した．

効果の検証としては，東京工科大学の ASSIT システムの認証部分を比較対象とし，授業での代返を問題として実験を行った．実験の結果，代返の抑制効果で高い評価を得ることができた．

本研究で提案する認証方法の今後の課題は，個人情報を用いることによる情報漏洩の危険に対する対策と，大学の代返以外の状況での効果の確認である．

参考文献

[1] 電子商取引推進協議会　本人認証技術検討WG：本人認証技術の評価基準(第 1 版)，1998