

平成 25 年度 卒業論文

Twitter を用いた携帯端末における個人認証プ
ロセスの多要素化に関する提案

電気通信大学 情報理工学部 総合情報学科

高田研究室

1010086 高浪悟

指導教官 高田 哲司 准教授

提出日 平成 26 年 1 月 31 日

概要

目次

第 1 章	序論	5
1.1	背景	5
1.2	研究目的	6
1.3	論文の構成	7
第 2 章	個人認証の多要素化への流れ	8
2.1	既存の認証技術	8
2.1.1	知識認証	8
2.1.2	所有物認証	9
2.1.3	生体認証	10
2.2	多要素認証	10
2.3	スマートフォン/タブレットの普及	11
2.4	Social Networking Service の普及	11
第 3 章	関連研究/製品	12
3.1	ライフログによる認証	12
3.2	Web サービスを利用した認証	12
3.3	多要素認証/既存認証の多要素化	12
第 4 章	Twitter 上の情報を用いた提案認証システム	13
4.1	採用手法の概要	13
4.2	システムの詳細	13
4.3	具体的特徴	13

第 5 章	検証実験	15
5.1	概要	15
5.2	SNS の情報を利用することに関する評価実験	15
5.3	時系列における期間を秘密として用いることに関する評価実験	15
5.4	時系列における周期を秘密として用いることに関する評価実験	15
第 6 章	考察	17
6.1	安全性に関する考察	17
6.1.1	憶えやすさに関する考察	17
6.2	使用継続性に関する考察	17
6.3	他環境における応用に関する考察	17
第 7 章	結論	18
謝辞		19
参考文献		20

図 目 次

4.1	リサーチ図形	14
5.1	our lab's web page	16

.....

表 目 次

6.1 なんのかんの表	17
-------------------	----

第 1 章

序論

1.1 背景

通信網の高速化・大容量化，電子機器の小型化・高性能化などにより，Web サービスで可能なことが多くなった．また，高性能な携帯端末の普及により，個人や決済にかかわる重要な情報を持ち歩くことが一般化しつつあり，必然的に個人認証を行う場面が増えてきている．こういった場面における個人認証では，パスワードや，PIN^{*1}を用いた例をよく見かける．

特にパスワードを用いた認証では，安全性と記憶持続性・利便性に関してはトレードオフの関係が存在する．例えば，辞書攻撃に強い安全なパスワードを用いようとする際には，意味のない文字列にすることが望ましい．しかし，意味のない文字列というのは憶えることが難しく，ユーザがパスワードを他のサービスにおいても使い回してしまう可能性を生じさせる．そうすると，どれか一つのサービスからパスワードが流出した際，かえって脆弱になってしまう恐れがある．現在，こういった問題を防ぐものとして，多要素認証を自由意志で利用できる Web サービスが増加しつつある．例えば，パスワードの入力が完了し，それが正しいものだ

^{*1}Personal Identification Number，暗証番号．本論文においてこれを用いた認証という場合には，特に指定がない限り 4 桁の数字を秘密情報としたものを想定する．

と判断された後に、あらかじめ登録された電話番号に SMS^{*2}を利用して乱数を送信し、その乱数をそのまま入力させるといった方式をとることができる。これにより、覗き見、推測や総当り攻撃によってパスワードが漏洩した際の不正利用のリスクを減少させることができるというメリットがある。

また、SNS^{*3}の形態を持つ Web サービスが近年増えてきている。これにより、コミュニケーションの道具やライフログとして自分自身の情報を公開することが多くのユーザ間で一般的になりつつある。SNS においては、その情報が公開される範囲が最も広いもので完全なパブリック、最も狭いもので自分自身のみ閲覧可 (非公開) の範囲で、それをある程度任意に指定できるサービスが多いという特徴がある。

1.2 研究目的

現在行われている個人認証の多要素化は、セキュリティトークンや E メールを用いたものが一般的であり、それにより大きく認証の安全性を高めている。しかし、利便性という点においては、一度認証のための画面から目を逸らす必要がある、特別なハードウェアを持ち歩く必要があるなど、今後の普及に際して改善の余地があると考えられる。

本研究では SNS の情報を用いた個人認証というものがあまり提案されていないことに着目し、応用可能な典型例として携帯端末に搭載することを想定したシステムを考案した。本研究における目的は、SNS の情報を用いて記憶持続性と利便性に考慮しつつ個人認証の安全性を向上させることである。

^{*2}Short Message Service, 電話番号を利用して短いメッセージを送受信できるサービス

^{*3}Social Networking Service, 社会的ネットワークをインターネット上で構築するサービス。

1.3 論文の構成

本論文は以下の章により構成される．

第 1 章 序論：ここでは，本研究を行うに至った背景と主たる目的に関する解説を行う．

第 2 章 個人認証の多要素化への流れ：ここでは，認証技術の現状や，近年普及した技術が個人認証へ及ぼすと考えられる影響について述べる．

第 3 章 関連研究/製品：この章では，前章で述べた内容に関連する，既存の製品や研究の取り組みを紹介する．

第 4 章 Twitter 上の情報を用いた提案認証システム：ここでは，本研究で開発したシステムに関する原理と詳細説明を行う．

第 5 章 検証実験：この章では，本研究で開発したシステムを用いた実験についての内容と結果の説明を行う．

第 6 章 考察：ここでは，これまでの取り組みと得られた結果から，本研究の成果と各結果に対する考察，ならびに今後の課題について考察する．

第 7 章 結論：ここで本研究について総括する．

第 2 章

個人認証の多要素化への流れ

2.1 既存の認証技術

一般に認証手法は以下の 3 つに大別できる。

2.1.1 知識認証

本人のみが記憶している情報を秘密情報として認証を行う手法。主にキーボードやタッチパネルなどの入力インターフェースを用いてアウトプットを行う。この手法は他の認証方式と比較して以下のようなメリットから、一般の Web サービスやモバイル端末などにおける認証に多く普及している。

- 多くの端末に搭載される汎用的な入力インターフェースを利用できるため、実装される環境への依存が少ない
- 新たなハードウェアを必要とする場面が少ないため、低コストで導入できる
- 秘密情報の伝達や保管が容易

秘密情報として、パスワードや PIN が用いられることが多い。そのため、以下のような欠点が存在する

- ユーザへ強い記憶負担が大きい
- 認証のための秘密情報入力に際して負担が大きい
- 情報量が少なく、総当り攻撃や辞書攻撃に対して脆弱

推測が難しいパスワードにするには意味を持たせないほうがよい。記憶するのが難しくなりがちである。しかし、ユーザにそういったパスワードを使用させることは難しく、Ashlee Vance[1]によれば、パスワードの20%がわずか5000個のリストで網羅可能である。

2.1.2 所有物認証

本人のみが所有している物の情報を秘密情報として認証を行う手法。他の認証手法に対して、

- 入力においてユーザの負担が少ない
- 所有物を交換することで秘密情報を容易に変更可能
- 秘密情報の情報量を増やしやすいため、比較的容易に安全性を高められる
- 貸与が可能

などの利点がある。しかしながら、

- 認証に際してその場に所有していることが求められるため、ユーザの負担が大きい
- 認証に特殊な機器を必要とするため、導入のコストが高い
- 盗難・紛失した場合、容易になりすましされる恐れがある

といった欠点も抱えている．具体例としては，IC カードや USB キー，ハードウェアトークンを用いたワンタイムパスワードによる認証などが挙げられる．

2.1.3 生体認証

本人の生体情報を秘密情報として認証を行う手法．

- 所有物認証のように何かを持ち歩く必要がなく，盗難・紛失の恐れも少ないため，ユーザへの管理負担が少ない
- 入力においてユーザの負担が少ない
- 秘密情報の情報量が大きい

などの利点を持つ反面，

- 秘密情報の変更が困難
- 認証に特殊な機器を必要とするため，導入のコストが高い
- 盗難・紛失した場合，容易になりすましされる恐れがある
- 体質や外部からの影響により認証操作を行うことが困難な場合がある．

などの欠点が存在する．この認証方式の具体例として，指紋・静脈・虹彩を用いたものが挙げられる．

2.2 多要素認証

既存の認証手法を複数提供し組み合わせることで，欠点を補い，安全性を高めることができる．これが多要素認証である．個人認証の多要素化の実現においては，ワンタイムパスワードを要素の一つとして利用している方式が主流である．[2]

銀行/オンラインゲームなどで多く見られるのが、ハードウェアトークンと呼ばれる、ワンタイムパスワード生成器を用いた方式である。

さらに近年、Google や Facebook、Apple など多くの Web サービスで利用される方式として、SMS/E メールやスマートフォン用アプリケーションを用いたものがある。SMS/E メールを用いた際は、手持ちの携帯端末に乱数が記載されたメッセージが送信され、アプリケーションを用いた場合は、アプリケーション上に乱数が表示される。この方式のメリットとして、新たなハードウェアを持ち歩く必要がなくなることによる利便性の向上と、併せて紛失の危険性も減少するということが挙げられる。

実例としての多要素化手法やワンタイムパスワードの生成方式については、第3章で述べる。

2.3 スマートフォン/タブレットの普及

2013年6月に行われた IDC Japan の調査 [3] によれば、家庭市場におけるスマートフォン^{*1}の所有率は 49.8%、タブレット^{*2}の所有率は 20.1%であった。

2.4 Social Networking Service の普及

^{*1} インターネットの利用を前提とした高機能携帯電話。統一された定義はないが、一般社団法人情報通信ネットワーク産業協会によれば「携帯電話・PHS に携帯情報端末 (PDA) を融合させた端末で、音声通話機能・ウェブ閲覧機能を有し、仕様が公開された OS を搭載し、利用者が自由にアプリケーションソフトを追加して機能拡張やカスタマイズが可能な製品。」(出展：通信機器中期需要予測 2010 年度 CIAJ)

^{*2} 板状のオールインワン・コンピュータやコンピュータ周辺機器の総称。本論文では、特に断りがなければ携帯端末としてのタブレットを指す。

第 3 章

関連研究/製品

- 3.1 ライフログによる認証
- 3.2 Web サービスを利用した認証
- 3.3 多要素認証/既存認証の多要素化

第 4 章

Twitter 上の情報を用いた提案認証システム

4.1 採用手法の概要

4.2 システムの詳細

4.3 具体的特徴

[4].

.....

図 4.1: リサージュ図形

第 5 章

検証実験

5.1 概要

5.2 SNS の情報を利用することに関する評価実験

5.3 時系列における期間を秘密として用いることに関する評価実験

5.4 時系列における周期を秘密として用いることに関する評価実験

図 5.1 は、国分君作のシンボルマーク

図 5.1: our lab's web page

第 6 章

考察

6.1 安全性に関する考察

6.1.1 覚えやすさに関する考察

表 6.1: なんのかんの表

品目	たて	よこ
あれ	1cm	2cm
これ	1.22cm	2.87cm

6.2 使用継続性に関する考察

で、これまでの考察をまとめたのが表 6.1 である。

6.3 他環境における応用に関する考察

第 7 章

結論

謝辞

感謝します。父上，母上，家族のみんなー先生、研究室の諸先輩方、そして同期のみんなー

参考文献

- [1] Ashlee Vance. If your password is 123456, just make it hackme. <http://www.nytimes.com/2010/01/21/technology/21password.html>, 2010.
- [2] Julien Freudiger Emiliano De Cristofaro, Honglu Du and Greg Norcie. Two-factor or not two-factor? a comparative usability study of two-factor authentication. <http://arxiv.org/pdf/1309.5344v1.pdf>, 2013-09-20.
- [3] 木村 融人 浅野 浩寿. 2013 年国内モバイル/クライアントコンピューティング市場家庭ユーザー利用実態調査：ブランド認知度と購買行動の変化. <http://www.idcjapan.co.jp/Report/Pc/j13180103.html>, 2013.
- [4] 情報処理学会の誰か. 情報処理学会論文誌 (ipsj journal) 原稿執筆案内. <http://www.ipsj.or.jp/08edit/journal/shippitsu/ronbunJ-prms.pdf>, 2008-09-01.