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

目 次 3

図 目 次

表 目 次

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．そうなると，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 (図 2.1) や PIN(図 2.2) 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

- ユーザへ強いる記憶負担が大きい
- 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ため，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．

図 2.1: Google における ID とパスワードの入力画面

図 2.2: Aplle iOS におけるタッチパネルによる PIN の入力画面

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，ID カードや USB キー (図 2.3)，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．

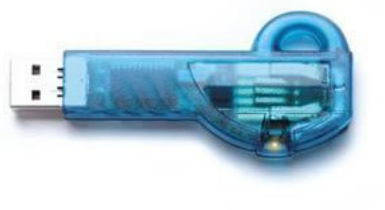

図 2.3: USB キーの例

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 (図 2.4)・虹彩を用いたものが挙げられる．

図 2.4: 静脈を用いた認証のための装置

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，多くの金融にかかわらない Web サービスでは，パスワードを保持するデータベースの増加とその認証情報の流出による，パスワードリスト型攻撃へのリスクを緩和するために多要素認証を用意している．そういった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[*1] 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．

多要素認証のデメリットとしては，

- 中間者攻撃やトロイの木馬を用いた攻撃，フィッシングに対して弱い
- サービスプロバイダが負担するコストが大きい

などが挙げられる．

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．

[*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）

2.3 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の所有率は 49.8%，タブレット[*2]の所有率は 20.1%であった．これらの携帯端末の普及により，外出先などからも様々なサービスにアクセスすることが可能になった．しかしその反面，様々なサービスの認証情報や個人情報などのデータを外に持ち出している状態であるため，携帯端末のセキュリティをいかに強化するかが重要になってきている．

スマートフォン/タブレットでは，携帯端末専用又はタッチパネルなどによる操作に特化した OS[*3]が搭載されていることが多く，Web サービスなどにおいても，ブラウザ上からだけでなく，専用のアプリケーションソフトウェアが用意されている場合がある．そういった場面では，認証情報は端末内に保存され，毎回の個人認証操作を行う必要が省かれていることもあり，端末の画面ロック[*4]が解除されてしまえば，従来の携帯電話などと比較して多くの操作が可能になってしまう．

携帯端末は，2.2 章や 3.3 章で述べられているように，多要素認証における認証要素の一つとしても扱われている現状が存在する．

[*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．

[*3] Operating System，基本ソフトとも．ハードウェアを抽象化しインターフェースを提供するソフトウェア

[*4] 操作を大きく制限されている状態．PIN 認証などを行わない限り解除できないことが一般的である．

2.4 Social Networking Service の普及

2011 年の総務省の調査 [4] では，成人における Social Networking Service(以下 SNS) の利用率は 15.0%であり，この数字は年々増加傾向にある．SNS では，多くのユーザがコミュニケーションやライフログを行うために投稿を行っている．そのため，個人を特定するための情報が多く存在するといえる．

SNS 上の情報は公開範囲を定めることができるという特徴を持つ．全世界に公開されるパブリックなものから友人のみが閲覧可能な情報や，自分のみが見ることができるプライベートな情報を発信できる．

SNS の一つに Twitter というサービスがある．これはユーザが個人で短文 (140 字以内) を投稿する，ミニブログやマイクロブログといったカテゴリーに分類されるのものである．Twitter 上の情報はほとんどがタイムライン[*5]に表示される短文の投稿 (「ツイート」と呼ばれる) であり，それら自体に単独で公開範囲を定めることはできないが，アカウントが protected(一般非公開の状態) に設定されていれば，フォロー[*6]を許可された人物 (フォロワー[*7]) のみが閲覧できる状態になる．アカウントがパブリックであれば，自分の投稿は他のユーザが自由に閲覧できる．しかし，他人への返信は自分と相手の共通のフォロワーでないとタイムライン上には表示されない．Twitter では以上のようにパブリックと protected の 2 つの公開範囲が存在する．

[*5] 投稿が時系列によって表示される画面
[*6] 他ユーザの投稿を自分のタイムラインで表示できるよう登録すること
[*7] 自分のことをフォローしている他のユーザ

第 3 章

関連研究/製品

3.1 ライフログやコミュニケーションツールによる認証

3.1.1 Web 履歴を用いた認証

田村ら [5] は，Web に頻繁に接続するユーザである場合，閲覧履歴を用いてユーザの特徴を抽出できる可能性があるとした．その際は本人認証を Web 閲覧履歴のみによって行えるが，Web に頻繁に接続しないユーザの場合は，ユーザを識別できるほどの特徴が見いだせないという結果が得られている．また，複数のライフログを用いた多要素化についても述べられている．

3.1.2 GPS を用いた認証

長谷ら [6] は，ユーザがあらかじめ予定していた時間に，予定していた場所へ移動したかどうかの情報を個人認証のための特徴量として扱う検討を行った．これによれば，複数のチェックポイントを設け，その場所で送信された GPS データを到着予定場所のものと比較することで，個人認証を行える可能性があるとしたが，GPS データの送信が不可能な場所や，予定時刻へ間に合わない場合が存在するなどの問題点が存在することも示した．

3.1.3 電子メールを用いた認証

3.2 Web サービスを利用した認証

3.2.1 Twitter の Direct Message を用いた認証

3.2.2 Facebook 社による友人の顔写真を用いた認証

3.3 多要素認証/既存認証の多要素化

3.3.1 Google

3.3.2 PassBan

3.3.3 Authy

3.3.4 オンラインゲームにおける多要素化例

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

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

第 6 章

考察

6.1 安全性に関する考察

6.2 憶えやすさに関する考察

6.3 使用継続性に関する考察

6.4 他環境における応用に関する考察

第 7 章

結論

謝辞

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] 総務省. 情報通信白書平成24年版. http://www.soumu.go.jp/johotsusintokei/whitepaper/h24.html, 2013.

[5] 田村 健範，鶴丸 和宏，市野 将嗣 and 小松 尚久. Web 閲覧履歴情報に着目したライフログによる本人認証に関する一考察. **電子情報通信学会技術研究報告**, 111:19–24, 2011-07-14.

[6] 長谷 容子，青木 輝勝 and 安田 浩. スケジュールと gps 情報を利用した認証方法の検討. **情報科学技術フォーラム一般講演論文集**, 3:235–236, 2004-08-20.