個人認証のパーソナライズ化を目指した規則ベース個人認証の提案

高浪 悟 †*　　高田 哲司 †

† 電気通信大学
182-8585 東京都調布市調布が丘 1-5-1
satorutakanami @ gmail.com, zetaka @ computer.org

あらまし 我々は日常生活を通じて多様な情報を能動的/受動的を問わず日々生成している．本論文ではこのような情報のことを「情報流データ」と定義する．移動履歴や電子メール，Twitter での” つぶやき” はその一例である．本研究では，この情報流データを対象に規則に基づく秘密情報を用いた個人認証を提案し，この認証手法を用いることでサービスの利用者が画一的な認証手法の利用を強制させられるかわりに，利用者毎に好きな認証手法を利用可能にする枠組みについて説明する．これにより，画一的な認証手法を大勢の利用者が利用することを前提とした攻撃手法に対する対策となることを目指す．

Personalized User Authentication by a Rule-based Secret with Fluid-data

Satoru Takanami†　　Tetsuji Takada†

†The University of Electro-Communications.
1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, JAPAN
satorutakanami @ gmail.com, zetaka @ computer.org

Abstract We have generated various information through dairy lives. We call such data set as “fluid data”. A various kind of history information, such as moving, receiving emails and tweets, are included in the fluid data. In this work, we proposed a user authentication with a rule-based secret, and we discuss about personalized user authentication using the proposed authentication. A rule-based secret with fluid data enables users to use various kind of secrets in a user authentication. We expect that this becomes a measure against a mass attack using leaked information.

1　はじめに

既存の知識照合型個人認証は，利用者から 2 つの自由を奪っている，という見方もできると考える．1 つは (i) 秘密情報の母集団として何を使用するかを既定している点，もう 1 つは (ii) 秘密情報の決定方法を既定している点である．暗証番号認証を例にとると，秘密情報は数字のみを使用すると決定している点が (i) にあたり，秘密情報は特定桁数の数値と決定していることが，(ii) に該当する．これらの制約のうち (i) の制約を数字のみから，英数字と記号の使用も認めると変更するとパスワード認証になり，特定桁数と同等の文字数利用を認めるならば安全性は向上することになる．また (ii) の制約を特定桁の数値に限定せず好きな桁数の数値を利用可能にすると秘密情報の選択肢が増加し，結果としてこの変更も個人認証の安全性を向上させることになる．

これらの制約は，利用者が細かな点を気にせず個人認証を利用可能にするための配慮としてサービス運用側が既定しているといえる．しかしこのように既定されてしまうと「4 桁暗証番号ではなく，パスワードを使いたい」という利用者の希望は叶えられない．つまり利用者に選択の余地を与える事ができないという点で制約であるという見方もできる．

* 現在，KLab(株) 勤務

ここで知識照合型個人認証の秘密情報について再考すると，以下の３つのプロセスで示せると考えた．

a) 情報種 (母集団)
b) 決定規則
c) 利用者選択

つまり，a) 秘密情報の母集団としてどのような情報を利用するのかを決定し，b) その母集団に対して決定規則を適用して秘密情報の候補集合を生成する．c) 利用者は生成された秘密情報の候補集合から必要な数だけ秘密情報を選択する．というプロセスで個人認証の秘密情報は決定されるという意味である．

上記のプロセスが妥当であると仮定した場合，我々は以下の２点が可能になれば知識照合型個人認証を改善できるのではないかと考えた．

a) 秘密情報の母集団を利用者が決定
秘密情報とする情報種 (母集団) を利用者が自由に決定できるようにする．情報種は数字，文字，記号，音声，音楽，画像，動画などなんでもよい．ただし個人認証を仮定するならば，理想的には個々のユーザ毎に母集団が異なっていることが望ましいと考える．

b) 秘密情報の決定規則を利用者が決定
上記 a) で決定された秘密情報の母集団を利用し，秘密情報の決定規則を利用者が決定する．既存のパスワードポリシー (例：8 文字以上で英大文字/小文字と記号を 1 つ以上含むこと) も決定規則の１つである．しかし既存の方法にとらわれず，より多種多様な秘密情報決定規則を決定 (利用) 可能にすることが望ましい．また，この決定規則そのものが，個人認証における秘密情報となる．

本提案による改善点は，現実に発生している一部の攻撃手法への安全性である．今日，1 つのサービスを多数のユーザが利用することは珍しいことではない．そこで利用者は，サービス運営側が指定する個人認証の利用を強制される．利用者が認証手法を選択する自由はない．この事実は利用者にとって制約になっている可能性については前述した．しかしそれに加えて攻撃者にとって好都合な状況を生んでいる可能性もある．決められた母集団と決定規則はその前提に基づく辞書の作成を可能にする．またなんらかの形で漏えいしたと推測されるパスワードを悪用して replay 攻撃 (アカウントリスト攻撃) を可能にしているのは複数のサービスで同一手法の認証手法を採用しているため，と見ることも可能だと考える．もしここでサービス利用者が利用者毎に認証手法を選択できるとした場合，上記の２攻撃手法による攻撃成功率は下がると推測する．理由は利用者毎に利用している認証手法が何かを攻撃者は特定する必要が生じるからであり，認証手法が画一であることを前提とした攻撃が困難になるからである．また攻撃者が特定認証手法の攻撃用に辞書を作成したとしても，認証手法がユーザ毎に異なる状況になれば，その辞書を用いた辞書攻撃をサービス利用者に一様に適用できなくなるからである．ただし誤解を招かないように言及するが，認証手法における理論的な安全性，つまりランダムに入力した値が偶然正解となる確率が向上するわけではない．これは多くの場合，認証手法の秘密情報と認証回答のための User interface によって規定される．本提案は秘密情報について言及しているが，User interface については言及していないため，理論的安全性が向上するとは限らない．

また現状の個人認証は，母集団と決定規則の間に一定の関連性があると言える．例えば暗証番号認証の場合は母集団が数字なので，決定規則は特定桁の数値という具合である．もしこの２者の関連性を可能な限り少なくし，理想として互いに独立な状況が作り出せたとするならば，以下のような秘密情報の変更方法も考えられる．

1) 決定規則を変更せずに母集団を変更
2) 母集団を変更せずに決定規則を変更

これらは秘密情報の変更における負担を減らす可能性もあるかと思慮する．またそれだけではなくサービス運営側と利用者側が協調して認証方法を組み上げるという運用方法も考えられる．サービス運営側が母集団 (情報種) を決定し，利用者が決定規則を決めれば，認証に利用する情報種は限定されるものの，その決定方法は利用者が自由に決定できるので，利用者の望むセキュリティレベルに応じて決定規則を決めることも可能になる．また決定規則が利用者によって異なるため，前述の２攻撃手法に対する安全性向上の可能性も残ることになる．

以降本論文では，このアイデアを基にした個人認証手法として，情報流と本論文で規定する時間とともに生成されるデータ群を情報種とし，時間に基づく決定規則を用いた個人認証手法を提案する．またそ

のアイデアに基づくプロトタイプとして notifAuth を提案し，その利用可能性について評価を行ったので報告する．

2　提案手法

前章のアイデアを基に要件を満たしうる実現方法について議論を行った．そこで我々は，情報種 (母集団) として「情報流データ」決定規則として「時間帯」とする認証手法に行きついた．この選択の理由は，情報種ならびに決定規則の双方において複数の選択肢がありうることと，両者の関連性は低いという要件を満たしうる選択肢だと考えたからである．

ここで情報流データについて説明する．情報流データとは「一定の手法で生成されるデータで，時間経過とともに新たなデータが生成される」と定義する．同様の定義に Lifelog があるが，生活に起因しないデータであっても一定の方法で時間とともに情報が生成されるものであれば該当するものとする．計算機サーバーのログ，センサーにより一定間隔ごとに生成されるデータ等も情報流データである．つまり情報種としては時刻情報と “なんらかの値” の組み情報で時間経過とともに情報が継続して生成されうるならば「情報流データ」であるとする．

秘密情報の決定規則は「時間帯」とした．つまり始点と終点の２つの時刻で規定される期間を利用者が任意に規定し，これ自体を秘密とする．前述の情報流データに対してこの規則を適用すると，この規定時間帯内に生成された情報 (群) が抽出できる．この情報 (群) を個人認証における秘密情報とするのである．

なお定義方法だと秘密情報は以下の２点の特徴を持つことになる．その理由を図１を使って説明する．

- 秘密情報は時間経過とともに変化する
- 秘密情報が１つとは限らない

ここで秘密情報を抽出する時間帯を次のように定義したと仮定する．

1) 現在時刻から指定時間分過去に戻る (図１中 (a))
2) その時刻を基準に時間幅を決定する (図１中 (b))

図の横軸は時間軸を表しており，上から下に向かって時間が経過していることを示している．図中の吹き出しは生成されたデータとその生成時刻を表している．図中で secret period と記載しているグレーで塗りつぶされた四角形が秘密情報となる時間帯であり，これは上記の定義に基づき決定されたものである．ここで秘密情報の時間帯は「現在時刻」という時間経過とともに変化する値を基準に決定しているため，秘密情報は時間経過とともに変化することになる．また秘密時間抽出の時間幅と情報流データにおけるデータ生成状況に依存するが，図中中段の時間軸に表されるように時間枠内に複数の生成情報が含まれる可能性もある．したがって秘密情報が複数，つまり正解回答が１つのみとは限らないことになる．

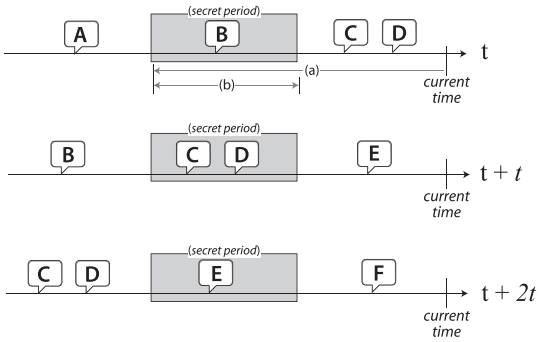

図 1: Rule-based secret with fluid information data

3　関連研究

本提案と関連があると思われる研究について言及する．今澤らの研究 [2] では，ライフログの１種といえる人の移動履歴情報を利用した個人認証手法を提案している．その手法では，人の移動履歴情報から一定時間以上同一場所に滞在した位置を抽出し，それを秘密情報とすることで個人認証を行う手法である．この手法では，我々の提案でいうところの決定規則にあたる滞在時間を変更することは可能である．しかし，それをあまりに短くすると正解回答数が増えてしまい，また長くすると移動履歴によっては容易に推測される懸念が生じる．したがって決定規則の選択肢が制約されるのではと考える．移動履歴を用いた個人認証の提案については，複数地点を特定の速度で順番に通過する認証 [3] や, 移動してきた経路を順に回答する認証 [4]，そして現在位置に応じて認証手法を変更する，つまりコンテキストに応じて認証手法を変更する手法 [8] などが提案されている．

西垣らの研究 [5] でもライフログを個人認証に応用する提案を行っている．この研究ではユーザが受信した電子メールの本文を利用者に提示し，そのメールの受信時刻を秘密情報として回答する認証手法で

ある．ただし，回答正答率を改善するため，最近受信したメールか指定期間よりも過去に受信したものかを判定する二択回答となっている．この手法でも最近および過去のメール判定の基準となる指定期間を変更することは可能である．しかし，これらは回答対象外とする期間を決めるものであり，大幅な変更は可能なものの，しにくいのではと推測する．

ライフログで時刻情報を応用する以外の認証方法としては FeliCa の利用履歴を用いた個人認証が提案されている [1]．これは鉄道駅改札の通過履歴と物販購入履歴を応用し，駅名や利用時刻を回答させる認証手法を提案している．この手法では秘密情報の決定規則は変更可能なものの，そのバリエーションは多くないと推測される．また情報種と決定規則の関連性が強く，情報種の変更は容易ではないと考える．

これらの手法は，情報種やその決定規則について変更可能性を残しているものがある．しかし，基本的には利用可能性に配慮した結果それぞれ規定された手法になったものと推測する．これに対して本研究では，あらためてこの 2 点の決定を利用者にゆだねうる自由度を持つ認証手法の実現を目指すという点で異なる試みであると考えている．

4　プロトタイプ実装: NotifAuth

これまでの検討を基にプロトタイプシステムの実装を行った．使用した情報種は，時刻情報付きの情報流データとして API 経由で取得可能な Twitter の Tweet を選択した．また実装対象としては iOS version 7 が稼働する Apple の携帯端末を対象とし，モバイルアプリケーションとして実装した．以降，本論文ではこの認証システムを “NotifAuth” と呼ぶ．図 2 は実装したシステムのシステム概要である．

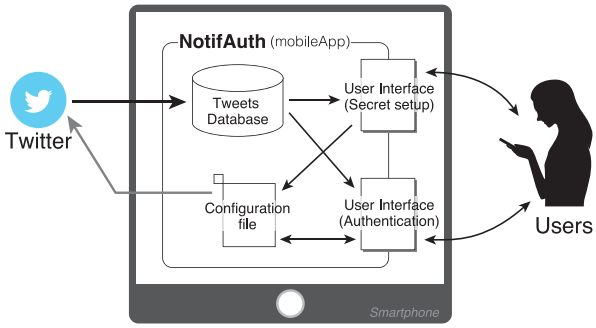

図 2: System Overview of the notifAuth

NotifAuth の利用手順は以下の順となる．

1) Tweet 情報の取得 - NotifAuth は tweet を秘密情報および不正解回答選択肢として利用するため，秘密情報の候補となる tweet を twitter API を通じて取得する．twitter とのアプリ連携のため，ユーザは Twitter の認証情報をアプリを通じて入力し，それを Configuration file に保存する．その後アプリは Twitter から最新 1,000 件分の tweet を取得し，それをアプリ内の Tweet Database に格納する．

2) 秘密情報設定 - 次に秘密情報を設定する．NotifAuth には 3 種類の秘密情報が利用可能になっており，それぞれ秘密情報設定用 UI を通じて設定を行う．この詳細については，次節で述べる．設定された秘密情報はアプリ内の Configuration file に記録される．

3) 認証操作 - 認証操作用 UI を通じて秘密情報を入力し認証を行う．認証操作用 UI の画面例を図 3 に示す．

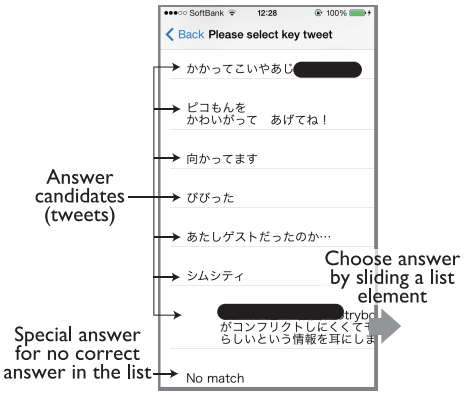

図 3: Authentication screen of the NotifAuth

認証操作用画面は，回答候補である tweet 10 個と正解回答 (秘密情報) が存在しない場合の回答 “No match” の計 11 個の回答選択肢がリスト形式で提示される画面構成となっている．利用者はこのリストの中から正解回答を見つけ出し，該当 tweet を横スライドすることで回答する．回答後，認証結果と認証時間が画面上に表示される．

4.1　3 種の秘密情報と設定方法

NotifAuth では 3 種の秘密情報が利用可能である．それらの定義法と実際の設定方法について説明する．

1) **fixed mode** - この fixed mode は，最新 200 件の tweet の中から任意の 1 つを秘密情報とする手法である．秘密設定画面には 200 個の tweet がリストとして提示されるので，利用者はこの中から秘密情報として使用したい tweet を 1 つ選択する．

2) **span mode** - このモードでは秘密情報として，時間軸上に一定の期間を定め，その期間内に生成された tweet 群を秘密情報とするモードである．この期間設定は 2 章で図 1 を用いて説明した通り，現在時刻を基準として定義する．したがって，時間経過とともに秘密情報が変化する仕組みとなっている．秘密情報の設定画面を図 4 中左に示す．利用者は最古時間を示す “From” と期間を示す “Term” の 2 つの値をスライダーで決定することで秘密情報となる tweet 群の生成期間を決定する．“From” を 30 日，“Term” を 7 日とした場合，現在時刻から 30 日前を最古側の時間とし，それより 7 日間の期間が秘密情報期間となる．

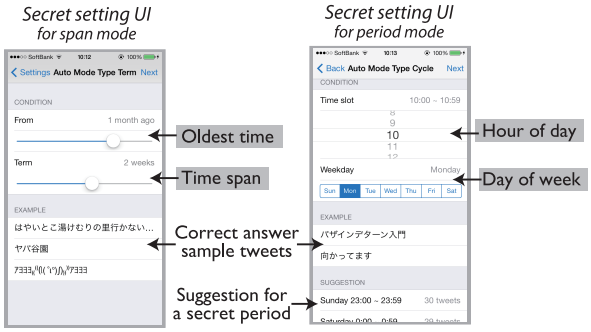

図 4: Secret set up UI for span and period mode

3) **period mode** - このモードは span mode と同様に時間軸上に一定の期間を定めることで秘密情報を定義する手法である．ただし span mode との違いは一時間帯として定義するかわりに，周期的情報を用いて時間枠として定義する方法となっている点にある．本モードにおける秘密情報の設定画面を図 4 中右に示す．画面からわかる通り，周期的情報による時間枠の定義は「曜日」と「何時台」の 2 つによって定義する．例えば毎週土曜日の 19 時台という定義になる．なお画面中央部には，その時間枠に生成されている tweet の一例が画面に表示され，画面下部には tweet 数の多い時間枠を提示する仕組みを備えている．これらは秘密情報設定の参考情報となることを意図したものである．

5 評価実験

NotifAuth の利用可能性について評価実験を行った．本章では評価実験とその結果について述べる．

本実験では，4 桁暗証番号によるスクリーンロックが必要な携帯電話のロック解除を二要素認証化することを想定し，(NotifAuth の 3 手法 + 4 桁暗証番号) による二要素認証を仮定した．なお比較のため，上記 3 つの組み合わせによる二要素認証のほかに 5 桁の暗証番号のみによる認証手法を加え，計 4 種の認証手法により比較実験を行うこととした．図 5 は，4 種の認証手法のフロー図である．なお以降本論文では，便宜上 4 認証手法をそれぞれ span&4pin, period&4pin, fixed&4pin, 5pin と呼ぶこととする．

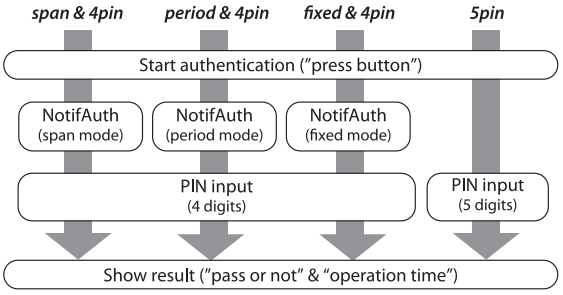

図 5: Operation Flow of Four Authentication Schemes

実験手順は 1 認証手法あたり 8 日間で 4 回の認証試行を実施させた．実験手順のタイムラインを図 6 に示す．実験初日に認証手法と実験概要について説明を行い，秘密情報を自由に決定させた．秘密情報設定直後に 1 回目の認証実験を実施し，以降 1, 3, 8 日後に認証実験を依頼した．また実験終了後にアンケートを依頼した．この実験手順を上記の 4 種の認証手法で繰り返して頂いた (計 32 日間)．4 種の認証手法の実施順序は被験者毎にランダムに設定した．なお本実験は被験者の所有する携帯端末に我々が実装したモバイルアプリをインストールし，それを利用してもらう形態で実施した．認証実験日には電子メールで被験者に対し実験実施を依頼する通知を行ったが，諸般の事情で指定した日に実験を実施できず，実験実施日が前後しているデータがある．またアンケートは 2 種の認証手法を完了するたびに実施した (計 2 回)．また残念ながら認証実験および

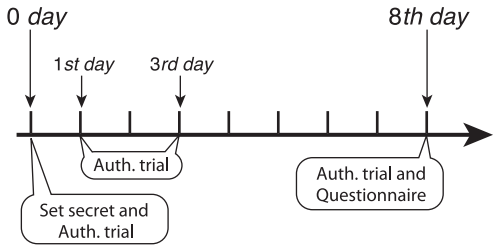

図 6: Experiment timeline

アンケートの双方について，全被験者が完了したわけではないこともここに述べておく．

被験者は著者の友人/知人を中心に男性 12 名，女性 3 名の合計 15 名に参加頂いた．被験者の年齢分布と Twitter の利用状況は表 1,2 に示す通りである．

表 1: Ages of the Subjects

Ages	20-29	30-39	40-49
# of subjects	12	2	1

表 2: Average # of Tweets per day of the Subjects

Tweets/day	0-1	2-10	11-50	51-100	over 100
# of subjects	1	6	6	1	1

5.1 実験結果

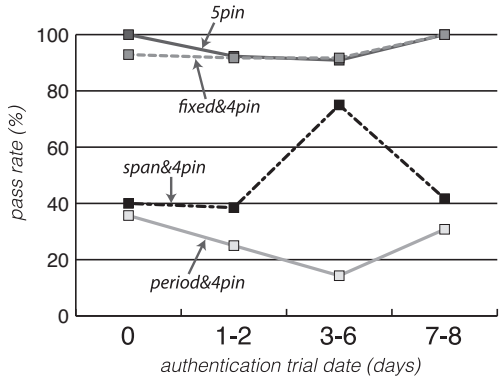

図 7: Pass Rates in four schemes in Eight Days

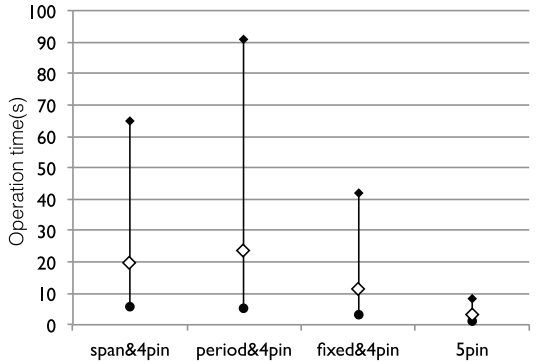

図 8: Operation times of four Auth. schemes

評価実験結果を認証成功率と認証時間として示す．図 7 は，4 種の認証手法における認証成功率の推移を表すグラフである．5pin と fixed&4pin の 2 つの認証手法は 8 日間にわたって 90%以上の認証成功率を維持していた．一方，span&4pin, period&4pin の 2 手法は秘密設定直後であっても認証成功率が 50%に届かないという結果となった．

図 8 は，4 種の認証手法における認証時間を示している．白抜き四角形は平均値を，黒四角と黒丸はそれぞれ最大値，最小値を表している．NotifAuth との組み合わせによる認証時間は平均でも 10〜22 秒ほど必要になる結果となった．なお認証時間の中央値は，全 4 手法において平均認証時間 (白抜き四角) を下回る結果となったことをあわせて述べておく．

図 9 はアンケート結果を示したグラフである．アンケートでは 4 種の認証手法について秘密保持負担，認証操作負担，認証操作時間，フラストレーションの 4 項目について 5 段階評価で回答させた．各評価値は 1 が最も良い印象，5 が最も悪い印象という割り当てになっており，グラフの値は各評価項目への評価結果を認証手法毎に集約し，平均値として示したものである．これらの評価値は被験者の各評価項目に対する主観的評価になっていると理解する．

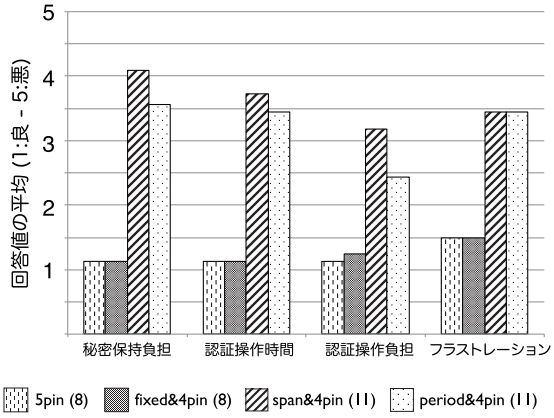

図 9: Impression to the four Auth. schemes

6 考察

本章では，NotifAuth の安全性，利用可能性および今後の課題について述べる．

6.1 安全性

NotifAuth の理論的安全性は認証操作画面内 (図 3) のリストに表示される回答候補の数に依存し，現在の画面設計では 1/11 である．ただし，この回答候補数は変更可能であり，その数を増やすことで安全性は向上可能である．しかしリスト内回答候補数の変更は回答探索時間に影響を及ぶため，無配慮に行うことはできない．リスト内候補数と回答探索時間の関係については評価実験を通じて妥当な回答候補数を見いだす必要がある．またリスト以外の認証操作画面の可能性についても検討する．また今回は検討外としたが，回答検証回数を 1 回から複数回に

する方法もある．一方，span mode と period mode ではリスト内に複数の正解が含まれる可能性がある．この状況はリスト長を固定と仮定するならば，理論的安全性を低下させることになる．しかし複数の正解候補を活用することで，リスト長を長くしつつも探索時間の拡大を一定範囲に抑えたり，リストは一定長だが正解回答が認証試行の毎に異なるようにすることで Intersection 攻撃への安全性を向上させることも可能となる [7].

6.2 利用可能性

実験結果から，認証時間は平均値で fixed&4pin が 10 秒台，span&4pin と period&4pin が 20 秒台という結果となり，5pin よりも大幅に時間がかかる結果となった．この理由は 2 つあると考える．1 つは回答探索時間が必要な点である．NotifAuth の認証操作ではリスト内の複数の回答候補から正解を探し出す時間 (回答探索時間) が必要になる．秘密情報が記憶内に保持されていて，即座に入力操作を可能な 5pin の認証手法とは異なるためである．もう 1 つは正解回答抽出時間が必要なためである．span mode と period mode に特有の処理だが，記憶している正解回答時間帯 (決定規則) からその時間帯に生成された tweet を抽出/判定する時間が必要なためである．前者の回答探索時間は NotifAuth が関与する 5pin 以外の 3 種の認証手法に影響してくるが，後者の正解回答抽出時間は span mode および period mode の認証のみで必要となる処理であり，それはアンケート結果 (図 9 の認証操作時間からも 5pin, fixed&4pin と span&4pin, period&4pin で値がはっきり異なることから負担になっていることが見てとれる．

認証操作負担に対する被験者の印象も図 9 から 5pin, fixed&4pin とそれ以外の 2 手法で評価結果が大きく分かれた．NotifAuth が関係する 3 手法の見た目上での認証操作は同一である．それにもかかわらずこのような評価が分かれた理由は，上記の正解回答抽出処理が認証操作の一環と被験者に受け止められたためと推測される．

秘密情報の記憶保持ならびにフラストレーションに関する被験者の印象も認証操作負担への印象と同じく評価が 2 分した．これらも正解回答抽出にまつわる負担が評価に影響した結果だと考える．span mode と oeriod mode を実施した被験者のうち認証に失敗した被験者を対象に秘密情報の記憶保持に関して追加ヒアリングを実施した．その結果，span mode で認証に失敗した 7 名のうち正解回答時間帯は記憶していたが tweet の選択肢に失敗した人が 4 名，period mode では 7 名中 5 名が同様の状況であったことがわかった．なお fixed&4pin モードは 5pin とほぼ同等の利用可能性が期待できると考える．認証時間は 5pin よりかかるものの，操作に対する慣れの問題と回答探索時間を考慮すると妥当な差であると考える．また認証成功率はほぼ同等であり，秘密情報の保持に対する印象も肯定的であった．

6.3 Twitter の認証応用について

今回の提案において情報流データとして Twitter を選択した理由は 4 つある:

1) 能動的行為による生成情報,
2) 1 情報あたりの情報量 (文字数) が限られる
3) 一定の情報数が期待できる,
4) 情報生成時の時刻情報が利用可能.

一番大きな理由は 1) である．span mode と period mode で NotifAuth を利用するには各情報の生成時刻を推測できる必要がある．そのため受動的に生成されるデータでは生成時刻の類推が難しいと考え，利用者の能動的行為による生成情報である tweet 情報を活用した．また上記 2),3),4) も twitter の特徴によるものだが，これらも今回の応用には都合のよい条件であった．

ただし Twitter の応用には問題もある．特に考えられるのは可用性とプライバシーへの懸念である．可用性の問題は，Twitter になんらかの不具合が発生し利用できなくなると NotifAuth も利用不能になる可能性がある．NotifAuth は tweet のダウンロード時のみ network 接続が必要となり，それ以外ではオフラインでも実行可能である．ただし span mode と period mode では最新の tweet を随時ダウンロードすることが前提になっており，特に span mode はオフライン状態が長期間にわたると秘密情報数がゼロになる．これはセキュリティ上での問題になるため対応策を検討する必要がある．

プライバシー上の懸念とは認証画面に tweet 群が表示されるため，意図せず第三者に tweet を閲覧されてしまう．またそれを契機として Twitter のアカウントが特定される懸念もある．この問題に対する対応の 1 つとして，アプリ内 tweet database から個人認証の回答候補に利用したくない tweet を削除可能にすることが考えられる．

6.4 今後の課題

喫緊の課題は本論文で述べた基本的なアイデアを維持しつつ，既存の認証手法と同程度の認証成功率を持つ認証手法を実現することにある．アプローチとしては 2 つある．1 つは本研究で実装したプロトタイプを改良する方法である．今回の評価実験で認証成功率が低かった理由は，決定規則から正解回答抽出ができなかったためである．その要因は回答候補に時刻情報を全く提示しなかった認証操作 UI にあると考えている．どの程度の情報を認証操作 UI で開示すれば，決定規則の第三者による推測を困難にしつつ，認証成功率を改善することができるかを見極めていく必要がある．

もう 1 つのアプローチとは，今回とは別の情報源と決定規則による秘密情報を用いた個人認証を検討し，実装・評価を行う方法である．時間による決定規則ではなく他の決定規則でも基本的には問題ない．回答候補がリスト形式で提示されると仮定するならば，リストの最後尾から n 番目が秘密情報という規則も一つの案であり，今後検討していきたい．

7 おわりに

我々は，個人認証に対する攻撃の一因が画一的な秘密情報を強制されている点にあるのではと考えた．そこで本研究では個人認証における秘密情報の定義に関する自由を利用者に提供することを目的として様々な秘密情報を検討した．その結果として時間の経過とともに継続して情報が生成される「情報流データ」に着目し，そのデータに規則を適用することで決定される情報を秘密情報とする個人認証手法を提案した．

上記のアイデアに基づき Twitter の tweet 情報を情報源とし，時間に基づく規則で定義される秘密情報を用いた個人認証を携帯電話端末で動作するアプリケーションとして実装し，被験者による評価実験を行った．その結果は，既存の認証手法と比較して認証操作時間が長くなり，また認証成功率も望ましい結果とならなかった．今後の課題として，基本アイデアはそのままとしつつも別の実装方法を検討し，既存の認証手法と同程度の認証成功率が実現できる個人認証手法の実現を目指して今後も研究を進めていく．

謝辞

本研究は JSPS 科研費 26540055 の助成を受けて実施されたものである．ここに謝意を表する．

参考文献

[1] 松村智彰，小池英樹: Felica の利用履歴を用いた個人認証，コンピュータセキュリティシンポジウム (CSS2010), (2010).

[2] 今澤貴夫，小池英樹，高田哲司: GPS データを用いた位置認証システムとその停留点算出方式，コンピュータセキュリティシンポジウム (CSS2008), pp.707-712, (2008).

[3] 角田雅照, 伏田享平, 三井康平, et al.: 位置と速度を利用した移動体向け認証方式の提案, 信学技報, MoMuC, モバイルマルチメディア通信 Vol 106, pp.11-16, (2006).

[4] 石原雄貴, 小池英樹: Path-Pass:位置情報を用いた認証システム, コンピュータセキュリティシンポジウム (CSS2006), (2006).

[5] 西垣正勝，小池誠: 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，情報処理学会論文誌，Vol.47, No.3, pp.945-956, (2006).

[6] 増井俊之，塚田浩二，高田哲司: マイ認証，インタラクション 2006, pp.25-26, (2006).

[7] 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, (2003).

[8] E. Hayashi, S. Das, S. Amini, et al.: CASA: context-aware scalable authentication, In Proc. of 9th Symp. on Usable Privacy and Security (SOUPS '13), 10 pages, ACM, (2013).

[9] T. Nemoto, K. Furukawa and M. Okamoto: Poster: Knowledge Based Authentication using Twitter, Symp. on Usable Privacy and Security (SOUPS '11), (2011).