知能と情報（日本知能情報ファジィ学会誌）Vol.23, No.6, pp.874－881（2011）

ショートノート

時空間情報と動作に基づく認証方法†

角田 雅照 *1・伏田 享平 *1・亀井 靖高 *3・中村 匡秀 *2
三井 康平 *1・後藤 慶多 *1・松本 健一 *1

本稿では，時空間情報(位置，移動時間，移動距離)と動作に基づく認証方法を提案する．ユーザは時空間情報で定義された特定の認証点において，特定の動作を行うことにより認証に成功する．ただし，時空間情報を認証に用いる場合，認証に時間が掛かり，やり直しが容易ではないため，正しいユーザが認証に失敗する確率を抑える必要がある．そこで，認証行為の部分的な誤りを許容する，部分一致認証を提案する．また，時空間文字を用いて安全性の評価方法を定式化するとともに，提案手法が安全性において有効であることを実験により示す．実験により提案方法の安全性を評価した結果，本人拒否率は0.233%，他人受入率は0.010%となった．

キーワード：時空間情報，時空間文字，部分一致認証，認証点マージン，ユビキタスコンピューティング

1．はじめに

近年，安全性が高い方法として，ICカードを用いた認証方法と生体情報を用いた認証方法が普及しつつある．ただし，ICカードを用いた認証方法では，カードが盗難され，ユーザが盗難に気づいてカードを利用不能にする前に，認証に利用される危険性がある[4]．生体情報を用いた認証方法の場合，盗難される可能性はないが，人工物により不正に認証される問題が指摘されている[9]．厳格な場面(機密データ保管室，原子力発電所などの重要施設に入場する際)での認証の安全性を高めるには，これらの問題点を補う必要がある．

そのための最も簡単な方法は，2つの認証方法を併用する，二要素認証を適用することである．二要素認証では，「何を持っているか」(ICカードや生体情報を用いた認証方法)と「何を知っているか」に基づく認証方法を組み合わせるのが通常である[12]．後者として，パスワード入力が最も一般的であるが，のぞき見攻撃(他人に入力を盗み見られること)に脆弱である．

そこで本稿では，(二要素認証に適した)より安全性の高い，時空間情報(ユーザの位置，移動時間，移動距離)と動作に基づく認証方法を提案する．提案方法では，ユーザの時空間情報が特定の認証点と一致するときに，ユーザが特定の動作を行うことにより認証される．図1に位置とボタン押下を組み合わせた認証例を示す．ユーザは，位置(認証点)A，B，C，Dで携帯するボタンを押下することにより認証に成功し，データセンターに入ることができる．

時空間情報を認証に用いる場合，認証に時間が掛かり，やり直しが容易ではないため，正しいユーザが認証に失敗する確率を抑える必要がある．そこで，認証行為の部分的な誤りを許容する，部分一致認証を提案する．また，時空間文字を用いて安全性の評価方法を定式化するとともに，提案手法が安全性において有効であることを実験により示す．

以降，2章で提案方法を詳述し，3章で提案方法に基づく認証システムについて説明する．4章で安全性の評価方法を説明し，5章で安全性の評価実験について述べ，6章で考察を加える．最後に7章でまとめと今後の課題を述べる．

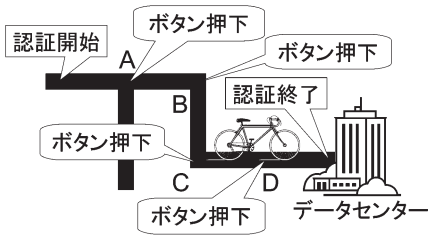

図1　位置情報とボタン押下動作による認証例

† An Authentication Method Based on Spatiotemporal Information and Actions
Masateru TSUNODA, Kyohei FUSHIDA, Yasutaka KAMEI, Masahide NAKAMURA, Kohei MITSUI, Keita GOTO and Kenichi MATSUMOTO

*1 奈良先端科学技術大学院大学 情報科学研究科
Graduate School of Information Science, Nara Institute of Science and Technology
*2 神戸大学大学院 システム情報学研究科
Graduate School of System Informatics, Kobe University
*3 九州大学 大学院システム情報科学研究院
Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University

2．時空間情報と動作を用いた認証方法

2.1 諸定義

提案方法では，時空間情報と動作による認証行為を，パスワードの文字列入力と見なして定式化する．時空間情報と動作の組を**時空間文字**と定義し，時空間文字の系列により，システムパスワードとユーザが入力したパスワードを表現する．前者を**規定文字列**，後者を**入力文字列**と呼ぶ．ただし，規定文字列中の時空間文字は**認証点**と**規定動作**の組であり，入力文字列中の時空間文字は**時空間情報**と**入力動作**の組である．以降それぞれの詳細について述べる．

(1)時空間情報

時空間情報とは，あるユーザUのある時点における**位置**(緯度，経度，高度で定義される)，認証開始時点(認証開始はユーザが明示的に指示する)からの**移動距離**，または認証開始時点からの**移動時間**のいずれかを指す．

(2)認証点

認証点とは，ユーザを認証するために用いられる以下の3種類の点である(各認証点を特に区別する必要がない場合，単に認証点と呼ぶ)．

位置認証点 l を任意の位置とし，l で定義される認証点を位置認証点と呼ぶ．

時間認証点 t を任意の移動時間とし，t で定義される認証点を時間認証点と呼ぶ．例えばある時間認証点 p が15秒とは，認証開始時点から15秒経過した時点を表す．

距離認証点 d を任意の移動距離とし，d で定義される認証点を距離認証点と呼ぶ．例えばある距離認証点 p が100mとは，認証開始時の位置から100m移動した地点を表す．

(3)認証動作

認証動作とは，ユーザが認証のために行うべき動作である．認証動作として，例えば移動速度などの動作の状態に基づく認証動作，ボタンを押すなどの機器の操作に基づく認証動作，クラッチなどの乗り物の操作に基づく認証動作などを用いることができる．システムであらかじめ規定された動作を**規定動作**，ユーザが実際に行った動作を**入力動作**と呼ぶ．

(4)時空間文字，規定文字列，入力文字列

時空間文字　ある認証点 p と規定動作 s のペア$\langle p, s\rangle$，及びある時空間情報 c と入力動作 e のペア$\langle c, e\rangle$を時空間文字(あるいは単純に文字)と呼ぶ．

規定文字列　ある認証点 p_i と規定動作 s_i の k 個のペアによる時空間文字の系列$\langle p_1, s_1\rangle\cdots\langle p_i, s_i\rangle\cdots\langle p_k, s_k\rangle$を規定文字列と呼ぶ．図1の例を規定文字列として表すと〈A，“ボタンを押す”〉〈B，“ボタンを押す”〉〈C，“ボタンを押す”〉〈D，“ボタンを押す”〉となる．

入力文字列　あるユーザUが k 回の入力動作 e_1，…，e_i，…，e_k を行い，e_i を実行した時のUの時空間情報が c_i であるとする．このとき，c_i と e_i をペアとする時空間文字の系列$\langle c_1, e_1\rangle\cdots\langle c_i, e_i\rangle\cdots\langle c_k, e_k\rangle$を入力文字列という．

2.2 部分一致認証

部分一致認証では，規定文字列と入力文字列で一致しない文字が，ある値 δ 個以下ならば，認証に成功していると判定する．規定文字列中のある文字$\langle p, s\rangle$と，入力文字列中の文字$\langle c, e\rangle$が不一致とは，規定動作 s と入力動作 e が不一致，または時空間情報 c が認証点 p 上にないときである

δ を**不一致許容数**と呼ぶ．部分一致認証では文字列の並びは考慮しない(考慮しても，安全性を高める効果は低い)．また，未入力文字が存在してもよいが，入力文字列の文字列長は規定文字列の文字列長を超えてはいけない(大量の文字入力により，規定文字列と入力文字列の文字が一致する確率が高まることを防ぐため)．

パスワード入力に例えると，システムパスワードが n 文字の場合，ユーザの入力文字列が $n-\delta$ 個以上一致していれば(タイプミスが δ 文字以下ならば)，認証成功となる．例えばシステムパスワードが“ABCD”，δ が1の場合，ユーザの入力文字列が“ABCE”，“BCD”などの場合，認証に成功する．

2.3 認証点マージン

ユーザの入力動作が認証点から少しずれる可能性を考慮して(入力動作を行った時空間情報と認証点との微小なズレを吸収するため)，また，位置情報の測定誤差を吸収するため，**認証点マージン**を定義する．ユーザのある時空間情報を c，認証点を p，ϕ，φ を p からの時空間上の距離とする．このとき，$p-\phi \leq c < p+\varphi$(位置認証点の場合，ある認証点 l から半径 ϕ 以内に c が含まれる)ならば，c は p 上にあると判定する．ϕ を前方マージン，φ を後方マージンと呼ぶ．例えば，ある時間認証点 m を認証開始30秒後とし，ϕ を1秒，φ を2秒とした場合，c が29秒以上32秒未満に含まれるならば，m 上にあると判定する．

3．提案方法に基づく認証システム

提案方法に基づく認証システムは，ユーザが時空間文字を入力する端末と，ユーザを認証するサーバから構成される．各ユーザUはユーザIDを持ち，ユーザID

ごとに規定文字列r_uが設定されている．安全性を高めるためには，(文献[6]で用いられているような)耐タンパ性の高い機器を端末に用いるべきである．認証手順を以下に記す．

ステップ1 Uは任意の位置で，端末に対し認証開始を指示する．
ステップ2 Uは目的地に移動しながら，端末に時空間文字を入力する．
ステップ3 目的地に到着後，Uは端末に対し認証終了を指示する．
ステップ4 端末はUから認証終了の指示を受け，入力文字列q_uとユーザIDをサーバに送る．
ステップ5 サーバは端末から送られたq_uとr_uを照合してUを認証し，結果を端末に送る．

必要な装置 時間認証点や距離認証点を用いる場合，ユーザに移動時間や移動距離を通知する装置が必要である．位置認証点を用いて屋外で認証を行う場合，GPSを利用する必要がある(準天頂衛星システム[11]が稼働すれば，より高精度な位置計測が可能となる)．屋内で認証を行う場合は，専用の(UWB(Ultra Wide Band)などを用いた[1])位置計測装置が必要となる．移動距離は位置情報に基づいて求めるか，車輪の回転数によって求める(移動手段が自動車などの場合)．

4．安全性評価

本章では安全性の評価方法について説明する．数式導出を容易にするために，ある規定文字列rに含まれる認証点は，時間認証点，距離認証点，位置認証点のいずれか1種類であり，rに重複する認証点が含まれないとする．これは提案方法に不利となる(安全性が低下する)条件であるが，それでも充分な安全性が確保できることを示す．

以降において，**試行可能回数**とは，認証に連続して失敗し，アカウントがロックされるまでの回数とする．パスワード入力に例えると，入力を何回まで試みることができるかを表す．

4.1 攻撃者が認証に成功する確率

攻撃者とは，認証が認められていないにもかかわらず，(不正な)認証を試みる者を指す．攻撃者は認証に必要な端末とユーザIDを入手しており，規定文字列の文字列長と認証点の候補，認証動作の候補を知っている(その他には規定文字列の手がかりを持っていない)とする．

他人受入率(FAR) 攻撃者が入力文字列の入力を試行可能回数γまで繰り返し，偶然認証に成功する確率を他人受入率(False Acceptance Rate；FAR)と呼ぶ．FARは以下の式により求められる．

$$\mathrm{FAR} = 1 - \prod_{i=1}^{\gamma}(1 - z_i) \tag{1}$$

ここで，z_iはi回目の認証試行における**入力文字列一致率**であり，規定文字列を知らない攻撃者がランダムに入力文字列を作成し，認証に成功する確率に基づく．$(1-z_i)$はi回目において認証に失敗する確率，$\Pi_{i=1}^{\gamma}(1-z_i)$は$\gamma$回連続で認証に失敗する確率を表す．FARはその余事象として求められる．

入力文字列一致率 攻撃者が入力する可能性のある入力文字列の全組合せ数wと，認証に成功する入力文字列の組合せ数vを用いた以下の式により求められる．ここで，攻撃者はi回目の認証試行において，それ以前に試みた入力文字列は試みないと仮定し，wから$i-1$を減じている．

$$z_i = \frac{v}{w - i + 1} \tag{2}$$

なお，攻撃者の入力文字列の文字列長が規定文字列よりも短い場合は考慮しなくてよい(文字列長nの入力文字列の方が，n未満の入力文字列よりも認証に成功する可能性が高いため)．

以降のwとvの導出方法の説明において，理解を容易にするため，まず具体例を用いて説明し，その後一般化した数式を示す．具体例では認証点の候補をAからZの26種類，認証動作の候補を0から9の10種類とし，規定文字列は〈A0〉〈B0〉〈C0〉〈D0〉とした．

入力文字列の全組合せ数w〈J0〉〈K1〉〈L2〉〈M1〉などが入力文字列となりうる．認証点の重複はなく，文字列の並びを考慮しないため，入力文字列に含まれる認証点の組合せ数は，26文字から4文字を取り出す組み合わせの総数${}_{26}\mathrm{C}_4$となる．それぞれの場合について4つの認証点において10種類の認証動作のうちの1つが入力可能なので，入力文字列の組合せ数は${}_{26}\mathrm{C}_4 \times 10^4$となる．これを一般化すると，攻撃者が入力する可能性がある入力文字列の組合せ数wは，以下の式により求められる．

$$w = {}_b\mathrm{C}_n\, a^n \tag{3}$$

ここで，nは規定文字列の文字列長，bは認証点の候補数，aは認証動作の候補数である．

認証に成功する入力文字列の組合せ数v例として，不一致許容数δが2であり，入力文字列と規定文字列の不一致の文字数が2文字であるとする．うち1文字

は認証点が一致しているが入力動作が不一致(〈C1〉など．正規表現では〈[A-D][1-9]〉となる．動作不一致文字と呼ぶ)，もう1文字は認証点が不一致で，入力動作は一致または不一致(〈E0〉など．正規表現では〈[E-Z][0-9]〉となる．点不一致文字と呼ぶ)であるとする．該当する入力文字列として，〈A0〉〈B0〉〈C1〉〈E0〉などが挙げられる．

(1)動作不一致文字の候補の組合せ数：入力文字列のうち，3文字は規定文字列と認証点が一致している．よって(規定文字列の〈A0〉〈B0〉〈C0〉〈D0〉から)3文字を選ぶ場合の数であり，組合せ数は${}_4\mathrm{C}_3$となる．

(2)動作不一致文字の組合せ数：(1)の3文字うち，1文字の入力動作が不一致なので，この組合せ数は${}_3\mathrm{C}_1 \times 9^1$となる．さらに入力動作が不一致なので，(0を除いた)9種類の認証動作のうちの1つを入力することになり，組合せ数は${}_3\mathrm{C}_1 \times 9^1$となる．

(3)点不一致文字の組合せ数：認証点[E-Z]([A-D]を除いた22通り)から1文字を選び，10種類の認証動作のうちの1つを入力するので，${}_{22}\mathrm{C}_1 \times 10^1$となる．

(1)～(3)は独立の事象なので，認証に成功する入力文字列の組合せ数はそれぞれを乗じた${}_4\mathrm{C}_3 \times {}_3\mathrm{C}_1 \times 9^1 \times {}_{22}\mathrm{C}_1 \times 10^1$となる．

ここで，不一致文字数をg，動作不一致文字数をhとおく(点不一致文字数は$g-h$となる)．規定文字列の文字列長をn，不一致許容数をδ，認証点の候補数をb，認証動作の候補数をaとおくと，表1より(1)は${}_n\mathrm{C}_{n-g+h}$，(2)は${}_{n-g+h}\mathrm{C}_h \times (a-1)^h$，(3)は${}_{b-n}\mathrm{C}_{g-h} \times a^{g-h}$の組合せ数となることがわかる．(1)～(3)の組合せ数を乗じると各行の組合せ数となる．

表の各行は独立の事象であり，認証に成功する入力文字列の組合せ数vは，各行の組合せ数を合計した，以下の式より求められる(便宜上$0^0=1$とする)．

表1 認証に成功する入力文字列の組合せ数

δ	$g-h$	h	組合せ数(1)	組合せ数(2)	組合せ数(3)
0	0	0	${}_4\mathrm{C}_4$	${}_4\mathrm{C}_0 \times 9^0$	${}_{22}\mathrm{C}_0 \times 10^0$
1	1	0	${}_4\mathrm{C}_3$	${}_3\mathrm{C}_0 \times 9^0$	${}_{22}\mathrm{C}_1 \times 10^1$
	0	1	${}_4\mathrm{C}_4$	${}_4\mathrm{C}_1 \times 9^1$	${}_{22}\mathrm{C}_0 \times 10^0$
2	2	0	${}_4\mathrm{C}_2$	${}_2\mathrm{C}_0 \times 9^0$	${}_{22}\mathrm{C}_2 \times 10^2$
	1	1	${}_4\mathrm{C}_3$	${}_3\mathrm{C}_1 \times 9^1$	${}_{22}\mathrm{C}_1 \times 10^1$
	0	2	${}_4\mathrm{C}_4$	${}_4\mathrm{C}_2 \times 9^2$	${}_{22}\mathrm{C}_0 \times 10^0$
3	3	0	${}_4\mathrm{C}_1$	${}_1\mathrm{C}_0 \times 9^0$	${}_{22}\mathrm{C}_3 \times 10^3$
	2	1	${}_4\mathrm{C}_2$	${}_2\mathrm{C}_1 \times 9^1$	${}_{22}\mathrm{C}_2 \times 10^2$
	1	2	${}_4\mathrm{C}_3$	${}_3\mathrm{C}_2 \times 9^2$	${}_{22}\mathrm{C}_1 \times 10^1$
	0	3	${}_4\mathrm{C}_4$	${}_4\mathrm{C}_3 \times 9^3$	${}_{22}\mathrm{C}_0 \times 10^0$

$$v = \sum_{g=0}^{\delta} \sum_{h=0}^{g} {}_n\mathrm{C}_{n-g+h}\ {}_{n-g+h}\mathrm{C}_h (a-1)^h\ {}_{b-n}\mathrm{C}_{g-h} a^{g-h} \tag{4}$$

4.2 ユーザが認証に失敗する確率

ユーザが認証に失敗する確率について説明する．ユーザは，自分のユーザIDに対応した規定文字列を知っているとする．

本人拒否率(FRR) ユーザが，試行可能回数γ以内に入力文字列の入力を成功させることができない確率を本人拒否率(False Rejection Rate；FRR)と呼ぶ．FRRは以下の式により計算される．

$$\mathrm{FRR} = y^{\gamma} \tag{5}$$

ここで，yは**文字列入力失敗率**であり，1回の試行において，ユーザが入力文字列を正しく入力できなかったために，認証に失敗する確率を指す．パスワード入力に例えると，システムパスワードを知っているユーザが，入力時にタイプミスがあったために，認証に失敗する確率となる．yとFRRは**要素入力失敗率**に基づく．以下にそれぞれの詳細を述べる．

要素入力失敗率 ユーザが，時空間文字1文字を入力失敗する確率．パスワード入力に例えると，システムパスワードを知っているユーザが，1文字タイプミスする確率を指す．

文字列入力失敗率 要素入力失敗率をx，規定文字列の文字列長をn，不一致許容数をδとすると，文字列入力失敗率yは，時空間文字n個のうち$\delta+1$文字以上，入力に失敗する確率であり，以下のように表される．

$$y = \sum_{i=\delta+1}^{n} {}_n\mathrm{C}_i\, x^i (1-x)^{n-i} \tag{6}$$

ここで${}_n\mathrm{C}_i x^i (1-x)^{n-i}$は$n$文字のうち$i$文字入力に失敗する確率であり，二項分布に従う．$y$は$\delta+1$文字以上入力に失敗する場合の，それぞれの確率を合計したものである．

4.3 認証点の候補数

認証点の候補数bは，以下の式により求められる．

$$b = \left[\frac{\sigma}{\phi + \varphi} + 1 \right] - 2 \tag{7}$$

σは(システムが想定する)総移動時間，または総移動距離を表し，ϕは前方マージン，φは後方マージンを表す．認証開始時と終了時は入力動作を行えないとみなし，bから2を減算している．

位置認証点を用いる場合，マージンの設定時に測定誤差を考慮する必要があるが，距離認証点を用いる場合には考慮する必要はない．これは，ユーザ，システムとも，誤差を含んだ移動距離を用いるためである．例えば，実際の移動距離が90mであり，測定された距離が誤差を含む100mであっても，ユーザとシステムが移動距離として認識するのは通知（測定）された100mである．

5．評価実験

5.1 概要

実験の目的は，ボタン押下に基づく認証動作を用いた場合の他人受入率（FAR）と本人拒否率（FRR）を求めることである．まず，要素入力失敗率，認証点候補数と認証点マージンとの関係を確かめた．実験では，測定誤差が最も小さい時間認証点を用いた．距離認証点と位置認証点を用いた場合でも，移動しながら特定のタイミングで動作をすることには違いがなく，要素入力失敗率の差は小さい（認証点の種類の違いよりも，動作の違いのほうが影響が大きい）と考えられるため，これらを用いた実験は省略した．

被験者は10人，移動手段は徒歩とし，被験者はPDAを手に持ちながら直線の道路上で移動を繰り返した．道路は歩道と車道が分離した，起伏がなく見通しのよい舗装路であり，車や歩行者が通ることは少なく，被験者の認証動作に支障をきたすことはなかった．実験では，手よりも少し大きい程度（幅77mm，高さ131mm）の長方形のPDA（Hewlett-Packard社iPAQ hx4700 Pocket PC）を用い，移動時間はPDAにより被験者に提示した．認証動作はタッチパネル機能を持つ液晶画面に表示されているGUIボタンを押すこととした．被験者は1秒から30秒のうちの任意の時点2つを認証点として設定し，その後，移動しながら2つの認証点それぞれでボタンを押すことを10回繰り返した．

5.2 結果

表2に認証点マージン，要素入力失敗率，認証時間を60秒とした場合の認証点候補数の関係を示す．認証点よりも手前でボタンを押した被験者はいなかったため，前方マージンは0秒とした．ここで，結果の信頼性を評価するために，ブートストラップ法[5]を用いて要素入力失敗率の95%信頼区間を算出した．信頼区間とは，直感的には試行を無限に繰り返した場合に想定されうる最悪と最良の値を示す．結果を表2に示す．例えば，後方マージンが1秒の場合，要素入力失敗率は最悪でも11.0%，最良では3.5%となる．液晶画面上のGUIボタンは押しにくいという被験者が複数人いたことから，ボタンをクリック感のあるものにすれば，要素入力失敗率はより低下する可能性がある．

次に後方マージンを1秒，試行可能回数を2回とし，文字列入力失敗率（式6より），FRR（式5より），FAR（式1，式2より）を求めた．さらに要素入力失敗率の信頼区間に基づいて（下側信頼限界と上側信頼限界を式6に代入して），文字列入力失敗率の95%信頼区間を計算した．結果を表3に示す．規定文字列長を5，不一致許容数を1とすると，文字列入力失敗率は4.8%（下側信頼限界は1.1%，上側信頼限界は9.7%），FARは0.010%となり，ユーザの利便性（記憶の負担や認証をやり直す確率）はやや低くなるが，高い安全性を実現できる．規定文字列長を4，不一致許容数を1とすると，文字列入力失敗率は3.0%，FARは0.092%（下側信頼限界は0.7%，上側信頼限界は6.2%）となり，安全性は少し低下するが，利便性をより高めることができる．

表2 認証点マージン（後方）φと，要素入力失敗率，認証点候補数との関係

φ (秒)	要素入力失敗率 (%)	信頼区間 (%)	認証点候補数
1	7.5	[3.5, 11.0]	59
2	4.5	[1.5, 7.0]	29
3	4	[1.0, 6.5]	19
4	2.5	[0.0, 4.5]	14

表3 規定文字列長n，不一致許容数δと，文字列入力失敗率，FRR，FARとの関係

n	4					5				
δ	文字列入力失敗率 (%)	信頼区間 (%)	FRR (%)	信頼区間 (%)	FAR (%)	文字列入力失敗率 (%)	信頼区間 (%)	FRR (%)	信頼区間 (%)	FAR (%)
0	26.791	[13.318, 37.258]	7.177	[1.774, 13.881]	0	32.281	[16.360, 44.159]	10.421	[2.677, 19.501]	0
1	3.047	[0.705, 6.239]	0.093	[0.005, 0.389]	0.092	4.828	[1.148, 9.651]	0.233	[0.013, 0.931]	0.01
2	0.159	[0.017, 0.488]	0	[0.000, 0.002]	3.833	0.376	[0.041, 1.121]	0.001	[0.000, 0.013]	0.55
3	0.003	[0.000, 0.015]	0	[0.000, 0.000]	43.204	0.015	[0.001, 0.067]	0	[0.000, 0.000]	9.862
4						0	[0.000, 0.002]	0	[0.000, 0.000]	59.325

6．考察

厳格な認証に適用可能である，指紋や静脈を用いた認証方法は，どちらも本人拒否率(FRR)が１％，他人受入率(FAR)が0.01％である[7]．これらと提案方法は，FRR，FAR計算時の前提(想定する攻撃方法など)が多少異なるため，数値の大小のみで優劣を決めることは避けるべきであるが，前提の違いを考慮しても，提案方法はこれらの認証方法と(安全性の面で)大きな差はないと考えられる．よって提案方法は，厳格な場面での認証に(二要素認証の１つとして)適用することが可能であると考えられる．

のぞき見攻撃に強い認証方法として，携帯端末を動かした軌跡[2]や歩き方[8]などのユーザの動作を用いた認証方法があげられるが，これらはFARが１～５％程度である．前述のように単純な数値比較は避けるべきであるが，少なくとも，提案方法よりも安全性が高いとはいえない．

提案方法と同様に，ユーザの位置履歴を利用した認証方法(自分が過去にいた場所を答えることにより認証する[3]など)が提案されているが，尾行やGPSロガー[10]による位置情報の履歴取得に脆弱である．提案方法では，尾行やGPSロガーだけでは規定文字列を得られず，より安全性が高い．

厳格な認証に従来のパスワード認証を用いる場合，パスワードを入力する場所がある程度安全である可能性があり，その場合は覗き見攻撃される可能性が低下する．ただし，提案方法も安全な屋内などで適用可能であり，同様に安全性を高められる．パスワードの場合，１箇所にカメラなどを設置することにより，容易に多数のユーザのパスワードの手掛かりを取ることができるが，提案方法の場合，攻撃者が規定文字列を得るためには，１人のユーザの尾行を繰り返し，かつ詳細に行動を観察することを繰り返す必要があり，不正認証は容易ではない．

提案方法は，認証途中に攻撃者に行動を妨害される可能性があるが，これはパスワード認証も同様である．例えば，どんな認証方法でも，ユーザが攻撃者に拉致されれば認証に失敗する．また，重要施設に入場するための認証の場合，入口に認証のための装置が設置されることが多いが，これを破壊すれば認証を妨害できる．これらは認証方法の安全性とは別の議論である．

7．まとめ

本稿では，時空間情報(位置，移動距離，移動時間)と動作に基づく認証方法を提案した．提案方法では，時空間情報で定義される認証点において，特定の認証動作を行うことにより認証に成功する．また，時空間情報と認証動作の組を時空間文字と定義し，時空間文字に基づく部分一致認証と，安全性の評価方法について提案した．実験では，ボタン押下を認証動作として用いた場合の安全性を確かめた．今後は，本稿で取り上げていない認証動作について，利便性や安全性を評価することを予定している．

謝辞

本研究の一部は，文部科学省科学研究補助費(若手B：課題番号21700077)による助成を受けた．

参 考 文 献

[1] 日立製作所：日立AirSense UWBエントリーモデル，http://www.hitachi.co.jp/wirelessinfo/as_entrymodel_uwb.html
[2] 石原進，太田雅敏，行方エリキ，水野忠則：端末自体の動きを用いた携帯端末向け個人認証，情報処理学会論文誌，Vol.46，No.12，pp.2997-3007（2005）．
[3] 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（CSS）予稿集（2006）．
[4] Just, M. and Oorschot, P.: Addressing the Problem of Undetected Signature Key Compromise, *Proc. Network and Distributed System Security Symposium* (1999).
[5] 金明哲：Rとブートストラップ，ESTRELA，統計情報研究開発センター，No.156，pp.58-63（2007）．
[6] 佐藤直之，鈴木英明：耐タンパ個人端末を利用し個人情報の保護を可能とした認証方式，情報処理学会論文誌，Vol.41，No.8，pp.2129-2137（2000）．
[7] 瀬戸洋一：バイオメトリックセキュリティ認証技術の動向と展望，情報処理，Vol.47，No.6，pp.571-576（2006）．
[8] 杉浦一成，槇原靖，八木康史：全方位カメラを用いた複数方向の観測による歩容認証，情報処理学会論文誌：コンピュータビジョンとイメージメディア，Vol.1，No.2，pp.76-85（2008）．
[9] 鈴木雅貴，宇根正志：生体認証システムの脆弱性の分析と生体検知技術の研究動向，金融研究，Vol.28，No.3，pp.69-106（2009）．
[10] Telespial Systems, Inc.: TrackStick, http://www.trackstick.com/
[11] 宇宙航空研究開発機構：準天頂衛星初号機「みちびき」，http://www.jaxa.jp/projects/sat/qzss/index_j.html
[12] Weaver, A.: Biometric Authentication, *IEEE Computer*, Vol.39, No.2, pp.96-97（2006）．

（2011年２月７日　受付）
（2011年７月６日　採録）

［問い合わせ先］
〒630-0192　奈良県生駒市高山町8916-5
奈良先端科学技術大学院大学 情報科学研究科
角田　雅照
TEL：0743-72-5318
FAX：0743-72-5319
E-mail： masate-t@is.naist.jp

著 者 紹 介

角田（つのだ）　雅照（まさてる） ［非会員］

1997年和歌山大・経済卒．2007年奈良先端大・情報科学・博士後期課程修了．同年同大学同研究科特任助教．博士（工学）．ソフトウェアメトリクス，ユビキタスコンピューテング等の研究に従事．IEICE，IPSJ，HIS，JSiSE，IEEE各会員．

亀井（かめい）　靖高（やすたか） ［非会員］

2005年関西大・総合情報卒．2009年同大学院博士後期課程修了．同年日本学術振興会・特別研究員（PD）．2010年カナダ・Queen's大・博士研究員．2011年九大院・システム情報科学・助教．博士（工学）．ソフトウェアメトリクス，マイニングソフトウェアリポジトリ等の研究に従事．ＩＥＥＥ，IEICE，IPSJ各会員．

三井（みつい）　康平（こうへい） ［非会員］

2005年岩手県立大・ソフトウェア情報・ソフトウェア情報卒．2008年奈良先端大・情報科学・博士前期課程修了．同年株式会社インターネットイニシアティブ入社．在学時，ホームネットワークシステム等の研究に従事．

松本（まつもと）　健一（けんいち） ［非会員］

1985年阪大・基礎工・情報卒．1989年同大学大学院博士課程中退．同年同大学・基礎工・情報・助手．1993年奈良先端大・情報科学・助教授．2001年同大学同研究科教授．工学博士．エンピリカルソフトウェア工学，特に，プロジェクトデータ収集／利用支援の研究に従事．IPSJ，IEICE，JSSST，ACM各会員，IEEE Senior Member．

伏田（ふしだ）　享平（きょうへい） ［非会員］

2005年大阪府立大・工・電気電子システム工中退．2010年奈良先端大・情報科学・博士後期課程修了．同年同大学同研究科博士研究員．2011年同大学同研究科特任助教．博士（工学）．ソフトウェア工学，特にソフトウェアプロセス，ソフトウェアデザイン，リポジトリマイニングの研究に従事．IEEE，IEICE，IPSJ，JSSST各会員．

中村（なかむら）　匡秀（まさひで） ［非会員］

1994年阪大・基礎工・情報卒．1996年同大学院博士前期課程修了．1999年同大学院博士後期課程修了．同年カナダ・オタワ大・ポスドクフェロー．2000年阪大・サイバーメディアセンター・助手，2002年奈良先端大・情報科学・助手，2007年神戸大・情報知能・准教授．2010年同大大学院・システム情報学・准教授．博士（工学）．サービス指向アーキテクチャ，ホームネットワークシステム，ライフログ，ソフトウェア工学等の研究に従事．IEEE，IEICE，IPSJ，HIS各会員．

後藤（ごとう）　慶多（けいた） ［非会員］

2005年阪南大・経営情報卒．2007年奈良先端大・情報科学・博士前期課程修了．同年日本電子計算株式会社入社．在学時，ソフトウェア開発プロセス等の研究に従事．

An Authentication Method Based on Spatiotemporal Information and Actions

by

Masateru TSUNODA, Kyohei FUSHIDA, Yasutaka KAMEI, Masahide NAKAMURA, Kohei MITSUI, Keita GOTO and Kenichi MATSUMOTO

Abstract：

We propose a new authentication method based on actions and spatiotemporal information such as location, elapsed time, and travel distance of a user. To be authenticated, a user performs certain actions at certain points defined with spatiotemporal information. To apply spatiotemporal information to authentication, it is needed that suppressing probability of authentication failure of regular user, for it is not easy to retry authentication. So we propose partial matching authentication which allows partial mistake of user's authentication procedure. Also, we define combination of spatiotemporal information and action as spatiotemporal character, and formalize security evaluation of our method based on it. In addition, we show security effectiveness of our method with an experiment. The experiment showed that false rejection rate of our method is 0.233% and false acceptance rate is 0.010%.

Keywords：spatiotemporal information, spatiotemporal character, partial match authentication, authentication point margin, ubiquitous computing

Contact Address：**Masateru TSUNODA**

Graduate School of Information Science, Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, Nara, 630-0192, JAPAN
TEL ：0743-72-5318
FAX ：0743-72-5319
E-mail ：masate-t@is.naist.jp