社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE

位置と速度を利用した移動体向け認証方式の提案

角田 雅照† 伏田 享平† 三井 康平† 亀井 靖高†
後藤 慶多† 中村 匡秀† 松本 健一†

†奈良先端科学技術大学院大学情報科学研究科 〒630-0192 けいはんな学研都市
E-mail: †{masate-t, kyohei-f, kohei-m, yasuta-k, keita-g, masa-n, matumoto}@is.naist.jp

あらまし 位置と速度を利用した移動体向け認証方式を提案する．これまで，パスワードや暗証番号を用いた認証方式が広く用いられてきたが，他人に入力を盗み見られることによりパスワードや暗証番号を知られ，不正な認証をされる可能性があった．提案方式では，ユーザは複数の地点を特定の速度で順番に通過することにより認証に成功し，通過速度があらかじめ設定された速度と異なる場合，認証に失敗する．本稿では，認証方式を提案するとともに，予備実験により位置と速度が認証に利用可能であることを確かめた．

キーワード 位置に基づく認証，速度，チャレンジアンドレスポンス，入室認証，
ユビキタスコンピューティング

An Authentication Method Using Location and Speed Information for Mobile Users

Masateru TSUNODA† Kyohei FUSHIDA† Kohei MITSUI† Yasutaka KAMEI†
Keita GOTO† Masahide NAKAMURA† and Ken-ichi MATSUMOTO†

†Nara Institute of Science and Technology Kansai Science City, 630-0192 Japan
E-mail: †{masate-t, kyohei-f, kohei-m, yasuta-k, keita-g, masa-n, matumoto}@is.naist.jp

Abstract This paper proposes an authentication method using location and speed information for mobile users. Though passwords or PINs is widely used for authentication, an incorrect user could be authenticated, peeking at a user inputting a password or PIN. With proposed method, users are authenticated when they sequentially pass through some points with specific speed. They are not authenticated when passing speed on the point is different from specific speed. This paper proposes the authentication method and confirms that location and speed information can be used for authentication by exploratory experiment.

Keyword Location-based Authentication, Velocity, Challenge and Response, Door Access Control, Ubiquitous Computing

1. はじめに

これまで，認証方式としてパスワードや暗証番号を用いた方式が広く用いられてきた[12]．パスワードや暗証番号を用いた認証は，安価かつ汎用的に用いることができる方式であるが，他人に入力を盗み見られることによりパスワードや暗証番号を知られ，不正な認証をされる可能性がある．

このため，パスワードや暗証番号に代わる，新たな認証方式が提案されてきている．例として，IC カードなどの所有物による認証方式があげられる[4]．IC カードは偽造される危険性が低いため安全性が高いが，紛失や盗難の可能性がある．盗難に遭った場合，IC カードなどの使用を停止することができるが，使用者が盗難に気づく前に不正使用される危険性がある[7]．また，指紋[6]や虹彩[1]などの生体情報を用いた認証方式も数多く提案されている．生体情報は紛失の心配がないが，認証方式の安全性が充分評価されていない側面があり[13]，また認証装置自体の設置場所の制約が存在する．また，生体情報は個人の特定が容易であることから，他人(認証する側)に生体情報を知られたくないというユーザの心理的抵抗も少なからず存在する[14]．

本稿では新たな認証方式として，位置と速度を利用した手法を提案する．具体的には，ユーザがあらかじめ設定した複数のチェックポイントを特定の順序，かつ特定の速度で通過することにより，認証を試みる．例えば，図 1のようにユーザはチェックポイント A，B，C の順に通過し，かつ A では時速 13km，B では時速 18km ，C では時速 15km で通過すると認証に成功する．チェックポイントの通過順序や速度が設定されたものと異なった場合，認証に失敗する．

提案方式の鍵である，認証地点を決められた速度で通過するという行為は，認証行為であることを気づかせにくい．仮

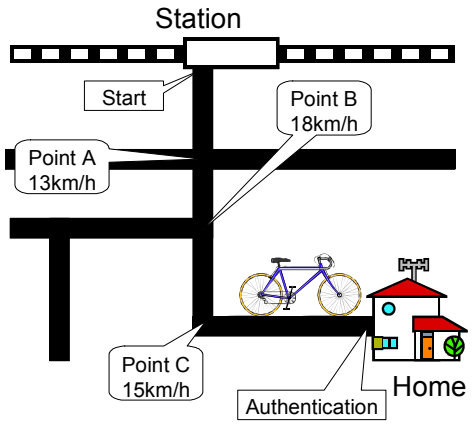

図 1　位置と速度を用いた認証の例

に悪意のある他人が認証行為を見ても，正確な認証速度を割り出すことは難しい．さらに，認証に失敗したときのリトライコストが大きく，総当り的攻撃も防げる．認証開始をユーザに知らせるようにすれば，疑わしい認証が試みられた際，認証完了までにユーザが認証自体を停止することも可能である．

また，認証情報の変更が容易でありバリエーションも増やしやすい．提案方式は認証装置自体の設置場所の制約がないため，他の方式と組み合わせて認証を行うこと(二要素認証[14])にも適している．提案方式は，ユーザが移動先で認証を行う場面に適用すること想定している．例えば，銀行で預金を引き出すときや，自宅など特定の場所に入場するときの認証に用いることができる．

以降，2章で関連研究と用語の定義について述べ，3章では提案方式について説明する．提案方法に基づいた認証システムのアーキテクチャを4章で述べ，5章で提案方式の実現可能性を確認するために行った予備実験について説明する．6章において提案方式のセキュリティ評価を行い，7章でまとめと今後の課題について述べる．

2. 準備

2.1. 関連研究

他人の盗み見や盗難による不正認証の危険性が少なく，認証情報を容易に変更可能である方式がいくつか提案されている．ユーザの手指の動きを近赤外線光によって計測し，認証に利用する方式[9]や，ユーザが携帯端末を動かした軌跡を加速度センサーで計測し，その動きを認証に用いる方式[5]，ユーザが思考した際の脳波を認証に用いる方式[12]，ユーザの視線を計測し，見ている画像の組み合わせにより認証を行う方式[3]などがある．これらの方式は提案方式と異なり，認証専用の装置を必要とする．また，これらの方式は認証のためだけの特殊な行為(行動)を用いるため，提案方式に比べて他人に認証行為を気づかれやすい．

位置情報を認証に利用した研究が少数ではあるが存在する．Denning ら[2]はユーザの現在位置によって，リモートシステムへのアクセス権を決定する方式を提案している．また，Sharma[10]はリモートシステムへのアクセス制御方式として，ユーザの現在位置と特定ポイントとの関係(2 点間の距離など)を，ユーザに答えさせることを提案している．特定ポイントの位置はユーザのみが知っており，ユーザの位置に応じて質問の回答も変化する．これらの認証方式はリモートシステムへのアクセス制御には適しているが，入室時の認証などには適していない．また，これらの方式は認証にユーザの位置情報のみを使っており，速度に関する情報を用いていない．

2.2. 定義

本稿で用いる用語について，以下に定義を述べる．

チェックポイント ：チェックポイント $p_1, p_2, \ldots, p_i, \ldots, p_n$ は，緯度と経度を用いて設定されている地点であり，通過すべき順に n 個設定されている．ユーザは認証を試みる際，チェックポイントを順番に通過しなければならない．

指定速度 ：指定速度 $s_1, s_2, \ldots, s_j, \ldots, s_n$ は，チェックポイント順に n 個設定されている．ユーザは認証を試みる際，指定速度でチェックポイントを通過しなければならない．

通過速度 ：ユーザがチェックポイントを通過したときの速度を指す．

チャレンジ ：チャレンジ-レスポンスにおいて，認証時に被認証者が受ける質問を指す．チャレンジ-レスポンスはインターネット･バンキングで用いられている認証方式である[8]．ユーザは銀行から乱数表をあらかじめ渡されており，重要な取引の際に，乱数表の特定の位置にある数値を入力するように求められる(チャレンジ)．それに対し，ユーザが乱数表の指定された位置にある数値を入力する(レスポンス)ことにより，取引が成立する．チャレンジの内容，すなわち指定される乱数表の位置は毎回変わるため，レスポンスすべき内容も変わる．これにより，万が一キーロガーなどによりレスポンスの内容が漏れたとしても，漏れたレスポンスに対応するチャレンジが出現する確率は低いため，不正な取引を高い確率で防ぐことができる．

攻撃者 ：認証を認められていないにもかかわらず，不正に認証を試みる者を指す．

3. 位置と速度を利用した移動体向け認証方式

3.1. 認証シナリオ

認証方式をシナリオとユースケースを用いて説明する．シナリオは「自宅の最寄り駅にいるユーザが，自宅に入るための認証を試みるために，チェックポイントを指定速度で通過することを繰り返す．ユーザが自宅到着後，システムは認証が成功しているか判定し，成功している場合自宅の入口を開錠する.」とする．このときのユースケースは以下のようになる．

目的 ：ユーザは自宅の入口の鍵を開けるために認証を受ける．

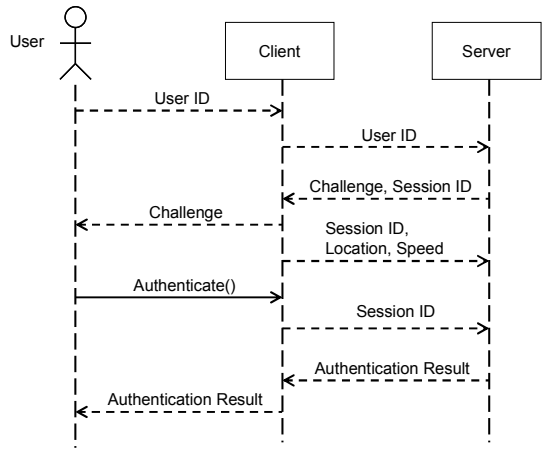

図 2　提案手法に基づく認証手順

事前条件：ユーザはチェックポイントの位置，チェックポイントの通過順序，及びチェックポイントの通過速度を知っている．ユーザは自転車，もしくは徒歩で移動しており，自分の現在位置と速度をシステムに伝えることができる．

基本系列：

1. ユーザは認証を開始することをシステムに知らせる．
2. ユーザはチェックポイントを指定速度で通過する．
3. システムはユーザの位置と速度の情報を受信する．
4. ユーザは自宅到着をシステムに知らせる．
5. システムは認証が成功しているか判定する．
6. ユーザが認証に成功している場合
   6.1. システムは入口の鍵を開ける．

例外系列：

2a. ユーザがあるチェックポイントを指定速度で通過することに失敗した場合
   2a.1. ユーザはそのチェックポイントの通過をやり直す

6a. ユーザが認証に失敗している場合
   6a.1. システムは入口の鍵を開けない．

事後条件：ユーザは認証に成功し，自宅の入口の鍵を開けることができている．

3.2. 提案認証方式

位置と速度を利用した認証の安全性を高めるために，チャレンジ-レスポンス方式の考えに基づく 3 つの認証方式を提案する．以下に詳細を述べる．

3.2.1. チェックポイント通過順序可変方式

チェックポイントを通過する順序を認証ごとに変更する方式である．すなわち，$p_1, p_2, \ldots, p_i, \ldots, p_n$ から作成した順列をチャレンジとする．例えば，チェックポイントとして p_1, p_2, p_3, p_4 が設定されているときに，「p_4, p_3, p_1, p_2 の順に通過する」ことや「p_3, p_4, p_2, p_1 の順に通過する」ことをチャレンジとする．チェックポイントと指定速度の組み合わせは変更しない．同じチャレンジが出現する事象 C が起こる確率 $P\{C\}$ は，n 個のチェックポイントが存在し，全てのチェックポイントを 1 度だけ通るとすると $P\{C\}=\frac{1}{n!}$ となり，安全性が高まる．例えば，チェックポイントが 5 箇所の場合，$P\{C\}=\frac{1}{120}$ となる．ただし，ユーザにかなりの遠回りを強いる可能性が高いため，利便性は低くなる．

3.2.2. チェックポイント組み合わせ可変方式

通過すべきチェックポイントと通過してはならないチェックポイントの組み合わせを認証ごとに変更する方式である．すなわち，$p_1, p_2, \ldots, p_i, \ldots, p_n$ から r 個のチェックポイントを取り出した組み合わせをチャレンジとする．例えば，チェックポイントとして p_1, p_2, p_3, p_4 が設定されているときに，「p_1, p_3 の順に通過し，かつ p_2, p_4 を通過しない」ことや「p_2, p_3 の順に通過し，かつ p_1, p_4 を通過しない」ことをチャレンジとする．チェックポイントと指定速度の組み合わせは変更しない．この方法の場合，ユーザは場合によっては遠回りをしなければならない可能性があるが，チェックポイント通過順序可変方式に比べれば利便性は高くなる．ただし，チェックポイント通過順序可変方式と比べると安全性が低くなる．n 個のチェックポイントが存在するとき，r 個のチェックポイントを通過し，かつ n-r 個のチェックポイントを通過してはならないとすると，$P\{C\}=\frac{1}{{}_nC_r}$ となる．例えば，5 箇所のチェックポイントのうち 3 箇所を通過し，残りを通過しない場合，$P\{C\}=\frac{1}{10}$ となる．

3.2.3. 指定速度可変方式

各チェックポイントの指定速度を認証ごとに変更する方式である．すなわち，$p_1, p_2, \ldots, p_i, \ldots, p_n$ における指定速度を $s_1, s_2, \ldots, s_j, \ldots, s_m$ から作成した重複順列とし，これをチャレンジとする．例えば，チェックポイントとして p_1, p_2, p_3, p_4 が設定されており，s_1, s_2, s_3 が設定されているときに，「p_1, p_2, p_3, p_4 の順に s_1, s_2, s_1, s_2 の速度で通過する」ことや「p_1, p_2, p_3, p_4 の順に s_3, s_2, s_1, s_3 の速度で通過する」ことをチャレンジとする．この方法の場合，ユーザは遠回りをする必要が全くなくなり，その他の方式よりも利便性が高くなる． さらに，安全性についてもこの方式が最も高い．n 個のチェックポイントが存在するとき，m 個の速度から作成した重複順列を指定速度の列とするとき，$P\{C\}=\frac{1}{{}_m\Pi_n}$ となる．例えば，チェックポイントが 5 箇所で速度が 3 つの場合，$P\{C\}=\frac{1}{243}$ となる．なお，安全性を高めるために，n 個の指定速度が全て同じとなるような組み合わせはチャレンジから除外したほうがよい．

それぞれの方法を組み合わせることも可能であるが，認証方式を複雑にするとユーザの利便性が低下してしまうので注意が必要である．本稿では紙面の都合上，安全性が最も高く，

Time	Latitude	Longitude	Speed (km/h)	
12:33:00	[Lat. of Check Point A]-a-b	[Long. of Check Point A]-a-b	9	Moving Speed on Check Point A (Canceled)
12:33:01	[Lat. of Check Point A]-a	[Long. of Check Point A]-a	10	
12:33:02	[Lat. of Check Point A]+a	[Long. of Check Point A]+a	10	
12:33:03	[Lat. of Check Point A]+a+b	[Long. of Check Point A]+a+b	9	
12:34:01	[Lat. of Check Point A]-a-b	[Long. of Check Point A]-a-b	12	Moving Speed on Check Point A
12:34:02	[Lat. of Check Point A]-a	[Long. of Check Point A]-a	13	
12:34:03	[Lat. of Check Point A]+a	[Long. of Check Point A]+a	13	
12:34:04	[Lat. of Check Point A]+a+b	[Long. of Check Point A]+a+b	12	
12:40:00	[Lat. of Check Point B]-a-b	[Long. of Check Point B]-a-b	17	Moving Speed on Check Point B
12:40:01	[Lat. of Check Point B]-a	[Long. of Check Point B]-a	18	
12:40:02	[Lat. of Check Point B]+a	[Long. of Check Point B]+a	18	
12:40:03	[Lat. of Check Point B]+a+b	[Long. of Check Point B]+a+b	17	

図 3 チェックポイントの通過速度の計算例

利便性も高い指定速度可変方式を採用する．

3.3. チャレンジのユーザへの提示

提案方式では，ユーザが認証を試みる際にチャレンジを提示する必要がある．ただし，指定速度可変方式の場合，チャレンジとして各チェックポイントの指定速度をそのまま提示すると，攻撃者に盗み見られると指定速度を知られてしまう．そこで指定速度を順序のない記号(○や□など)や色(記号は同じで色を赤や青にする)で表すこととする．指定速度 $s_1, s_2, \ldots, s_j, \ldots, s_m$ を順序のない記号や色で表した場合，各速度との組み合わせの数は $m!$通りとなり，安全性が高まる．

4. 認証システムのアーキテクチャ

4.1. 認証手順

提案方式をシステムとして実現した際の認証手順について説明する．まず，システムの仕様を下記のように決定した．

- 各ユーザはユーザ ID を持つ．
  ユーザごとにチェックポイントや指定速度を別々に設定できるようにするため．
- 認証ごとにセッション ID を生成する．
  セッションごとにチャレンジが異なるため，各セッションを区別する必要がある．
- クライアントは認証のためのチェックポイントや指定速度を知らない．
  攻撃者にクライアントを盗まれて，認証に必要な情報を取得されるのを防ぐため．

上記仕様に基づき，認証手順を以下のように設計した(図 2)．

(Step 1) クライアントはサーバにユーザ ID を送る．
(Step 2) クライアントはサーバからセッション ID とチャレンジを受け取る．
(Step 3) クライアントはユーザにチャレンジを提示する．
(Step 4) クライアントはサーバにユーザの現在位置と速度をセッション ID と共に送る．
(Step 5) 目的地に到着後，クライアントはセッション ID をサーバに送り，認証を完了する．

通信の傍受を防ぐため，(Step 1)から(Step 5)は暗号化しておく必要がある．(Step 1)におけるユーザ ID は機器固有の ID を用いてもよい．

必要とする機器について述べる．ユーザの位置と速度は GPS によって取得する．よってクライアントは GPS が利用可能である必要がある．また，サーバとの通信を行うために，クライアントは移動体データ通信を行える必要がある．想定されるクライアントとしては，PDA に GPS ユニットと PHS データ通信カードを接続したものが考えられる．サーバについては，クライアントと通信可能(インターネットに接続している)であればよく，特別な機器を必要としない．

提案方式を実際に適用する際に考慮すべき事項について述べる．チェックポイントの数は，ユーザの利便性を考慮すれば 5 個程度が適切であると考えられる．ユーザの移動手段が自動車の場合，チェックポイント近辺で渋滞に巻き込まれると速度調整が困難になる．また，後続車両がいる場合，減速して速度調整を行いにくいと考えられる．敷地内の道路を自動車で走る場合には提案方式を適用可能であると考えられるが，一般道を走る車には不適であると考えられる．

4.2. チェックポイントの通過速度の計算

チェックポイントの通過速度の計算方法について説明する(認証方式としては指定速度可変方式を適用することを想定している)．認証処理には，クライアントから送信されるユーザの位置と速度のデータを用いる．認証には以下のような制約を設ける．

- GPS の位置計測精度には 10m 程度の誤差があるため，チェックポイント p_i の近辺(緯度・経度$\pm a$)における速度の平均値を，ユーザの p_i における通過速度とする．
- p_i を指定速度で通過できなかったなどの理由で p_i の通過をやり直す場合，p_i の近辺外(緯度・経度$+a+b$，もしくは緯度・経度$-a-b$)から通過し直す．
- p_{i-1} と p_i の緯度・経度は $a+b$ よりも離れているものとする．
- $p_1, p_2, \ldots, p_i, \ldots, p_n$ に同じ位置のチェックポイントが含まれていてもよいが，p_{i-1} と p_i とは別々のチェックポイントとする(同じ位置のチェックポイントを連続させない)．なお，p_i の通過やり直しを認めない場合は，この制約は

表 1　GPS による計測速度と実際の速度との差の絶対値

指定速度	平均値	最大値
20km/h	0.3	0.7
15km/h	0.3	0.8
10km/h	0.2	0.4

不要である．

- チェックポイントの通過順序を間違えた場合，p_i からやり直す．

具体的には以下のような計算方法が考えられる(図 3)．なお，クライアントから送信された位置(緯度・経度)と速度が，セッション ID，データの受信時刻ともにサーバに記録されているとする．

(Step 1) 記録されたデータから，認証対象のセッション ID と一致するデータで，かつチェックポイント p_i の近辺 $\pm b$(緯度・経度+a+b，もしくは緯度・経度-a-b)のデータを抽出する．

(Step 2) データを受信時刻順に並べ替える．

(Step 3) データを順に読み，p_i の近辺(緯度・経度$\pm a$)のデータならば，速度の集計を開始する．

(Step 4) p_i の近辺外(緯度・経度+a+b，もしくは緯度・経度-a-b のデータならば，速度の集計を終了し，集計した速度の平均値を求め，p_i における通過速度とする．

(Step 5) 次に見つかった p_i の近辺(緯度・経度$\pm a$)のデータが，直前に集計したチェックポイントと同じならば，認証処理の対象外データとみなす(ユーザによってキャンセルされた通過速度とみなす． p_i の通過やり直しを認めない場合，この処理は不要である)．

5. 予備実験

5.1. 概要

提案方式が実現可能であることを確かめるため，予備実験を行った．提案方式が実現できるためには，以下に示す誤差が小さい必要がある．

- チェックポイントの位置の誤差(GPS の位置誤差)
- チェックポイント近辺における GPS の計測結果に基づく平均通過速度と，実際のチェックポイント通過速度との誤差(GPS の速度誤差)
- チェックポイントにおけるユーザの通過速度と指定速度との誤差(ユーザの速度誤差)．

そこで，ある地点(チェックポイント)を指定した速度で被験者に移動してもらい，上記誤差を調べる実験を行った．実験は堤防上にある直線の歩道で行い，被験者は自転車に乗って移動することとした．被験者はチェックポイントの手前約 100m から出発し，チェックポイントの前後約 10m の区間を指定速度で通過し，チェックポイント通過後約 100m で停止する．指定速度は時速 10km，15km，20km とし，被験者は指定速度ごとに 10 回走行することを繰り返した．なお予備実験のため，被験者は 1 人とした．

表 2　指定速度と通過速度との差の絶対値

指定速度	平均値	最大値
20km/h	0.6	1.1
15km/h	0.3	0.6
10km/h	0.5	0.9

5.2. 使用した機材

自転車の実際の速度を計測するために，自転車の車輪の回転数に基づいて速度を計算する速度計を用いた．被験者にチェックポイント通過時の速度計の速度を報告してもらい，この速度を実際の通過速度とみなした．使用した GPS ユニットは GlobalSat 社の BT-338 を用いた．この GPS ユニットは SiRF 社の SiRFstarIII チップセットを搭載しており，仕様上の位置誤差は 10m，速度誤差は 0.1m/s である．GPS ユニットから 1 秒間隔で出力される NMEA 形式のデータを移動ログとして記録した．自転車は 24 段変速を装備しているものを使用した．

5.3. 結果

実験の結果，GPS により計測した位置の誤差は小さいことが確認できた．移動ログからチェックポイント通過時のデータを取得するためには，GPS の誤差を考慮し，チェックポイントの地点から半径 α m の範囲をチェックポイントとする必要がある．実験では，チェックポイントにおいて約 3 分間静止した状態で位置を記録し，計測された緯度と経度の平均値をチェックポイントの位置とした．そして α を変化させ，実験で得た移動ログからチェックポイント通過時のデータを取得できるかどうかを確かめた． α<5m の場合，チェックポイントを通過しているにもかかわらず，移動ログ上では通過していないことになった．よって，この予備実験においては，α=5m とみなし，チェックポイントの位置から半径 5m の範囲における平均速度をチェックポイントの通過速度とした．

また，GPS により計測した速度の誤差も小さいことが確認できた．GPS で計測した速度を基に，チェックポイントの位置から半径 5m の範囲における平均速度を計算し，チェックポイント時点における実際の通過速度(被験者がチェックポイント通過時に確認した速度計の速度)との差の絶対値を，GPS で計測した速度の誤差とした．各指定速度における GPS の速度誤差の平均値と最大値を表 1に示す．計測した速度の誤差の最大値は時速 0.8km であった．

さらに，ユーザ(被験者)が通過速度をかなり正確にコントロールできることが確認できた．チェックポイント時点における通過速度(速度計の速度)と指定速度との差の絶対値を被験者の速度誤差とした．各指定速度における被験者の速度誤差の平均値と最大値を表 2に示す．計測した速度の誤差の最大値は時速 1.1km であった．

予備実験の結果より，GPS の受信状況が良好な場合，提案方法は実現可能であると考えられる．チェックポイントの位

置誤差は半径 5m 程度であり，速度誤差はユーザと GPS の誤差を加えても時速 2km 程度であり，充分誤差が小さいといえる．ただし，今回の予備実験は上空の遮蔽物が少ない堤防上で行っており，建造物の多い街中で実験を行った場合，誤差が大きくなるものと考えられる．また，ユーザによって通過速度の誤差も異なるものと考えられるため，さらに実験を行うことが必要である．

6. 評価

提案する認証方式のセキュリティを評価するために，移動と速度の履歴を攻撃者に取得される可能性と，取得された場合に不正な認証が成功する可能性について考察する．

実験によって確かめる必要があるが，攻撃者がユーザを尾行するだけでは，チェックポイントやチェックポイントの通過速度を知る可能性は低いと考えられる．また，サーバとクライアントとの通信を暗号化するため，通信経路で移動と速度の履歴を傍受される可能性も低い．ただし，[11]のような小型のデータロガーによって，位置と速度の履歴を攻撃者に取得される可能性がある．特にユーザが自転車に乗って認証を行う場合，攻撃者によって駐輪中の自転車に装置を取り付けられる可能性がより高まる．

移動と速度の履歴を得ても，攻撃者がユーザ ID を知らなければ不正な認証が成功する可能性は低い．攻撃者がユーザ ID を知っている場合，攻撃者は取得した位置と速度の履歴をそのままサーバに送るものと考えられる．ただし，チャレンジ-レスポンス方式を採用しているため，不正な認証が成功するためには，攻撃者が位置と速度の履歴を取得したときのチャレンジと同じチャレンジが認証時に出現する必要がある．指定速度可変方式の場合，同じチャレンジが出現する確率は $\frac{1}{{}_m\Pi_n}$ であり，認証のやり直しを k 回まで認める場合，不正な認証に成功する確率は $\frac{k+1}{{}_m\Pi_n}$ となる．例えば，ユーザの利便性を重視し，チェックポイントが 5 箇所，速度域が 3 つ，認証のやり直しを 2 回まで認めるとすると，不正な認証に成功する確率は $\frac{2+1}{{}_3\Pi_5}=\frac{3}{243}=\frac{1}{81}$ となる．安全性を重視し，チェックポイントが 8 箇所，速度域が 4 つ，認証のやり直しを 2 回まで認めるとすると，不正な認証に成功する確率は $\frac{2+1}{{}_4\Pi_8}=\frac{3}{65536}=\frac{1}{21845.333...}$ となる．認証開始時にユーザ ID を入力・表示させない場合，クライアントを盗まれない限り，攻撃者にユーザ ID を知られることはない．従って，攻撃者が移動と速度の履歴を取得し，クライアントを盗み，かつ一致するチャレンジが偶然出現して不正な認証が成功する可能性は低いと考えられる．

7. まとめ

本稿では，位置と速度を利用した移動体向け認証方式を提案し，提案方式に基づく認証システムについて説明した．また，予備実験により位置と速度が認証に利用可能であることを確かめ，セキュリティについて評価した．

今後の予定として，実験の被験者を増やすとともに，被験者の移動手段や移動経路を変化させ，提案方法の有効性を確かめることを考えている．また，チェックポイントや速度の設定方法の違いによる安全性や利便性の差を評価する予定である．

謝　辞

この研究は，文部科学省・21 世紀ＣＯＥプログラム「ユビキタス統合メディアコンピューティング」・若手研究者育成（提案公募型研究）事業経費の助成を受けて行われている．

文　献

[1] J. Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.15, no.11, pp.1148-1161, 1993.

[2] D. Denning, and P. MacDoran, Location-based authentication: grounding cyberspace for better security, In Internet besieged: countering cyberspace scofflaws, pp.167-174, ACM Press/Addison-Wesley Publishing Co., 1997.

[3] B. Hoanca, and K. Mock, “Secure graphical password system for high traffic public areas,” Eye Tracking Research and Applications Symposium, pp.27-29, San Diego, California, Mar. 2006.

[4] M. S. Hwang, and L. H. Li, “A new remote user authentication scheme using smart cards,” IEEE Transaction on Consumer Electronics, vol.46, no.1, pp.28–30, 2000.

[5] 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.

[6] A. Jain, L. Hong, and R. Bolle, “On-Line Fingerprint Verification,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, no.4, pp.302-314, 1997.

[7] M. Just, and P. Oorschot, “Addressing the problem of undetected signature key compromise,” Proc. Network and Distributed System Security Symposium, San Diego, California, Feb. 1999.

[8] 松本勉, 岩下直行, “インターネットを利用した金融サービスの安全性について,” 金融研究, vol.21, 別冊 1, pp.207-226, 2002.

[9] 長田礼子, 尾崎哲, 青木輝勝, 安田浩, “手指動からの特徴抽出によるリアルタイム個人認証,” 電子情報通信学会論文, vol.J84-D2, no.2, pp.258-265, 2001.

[10] S. Sharma, “Location based authentication,” Masters Thesis, University of New Orleans, 2005.

[11] Telespial Systems, Inc., TrackStick : http://www.trackstick.com/

[12] J. Thorpe, P. Oorschot, and A. Somayaji, “Pass-thoughts: authenticating with our minds,” Proc. the 2005 workshop on New security paradigms, pp.45-56, Lake Arrowhead, California, Sep. 2005.

[13] 宇根正志, 松本勉, “生体認証システムにおける脆弱性について : 身体的特徴の偽造に関する脆弱性を中心に,” 金融研究, vol.24, no.2, pp.207-226, 2005.

[14] A. Weaver, “Biometric Authentication,” Computer, vol.39, no.2, pp.96-97, 2006.