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

今澤　貴夫 †　　小池　英樹 †　　高田　哲司 ‡

† 電気通信大学大学院情報システム学研究科
182-8585 東京都調布市調布ヶ丘 1-5-1

imazawa@vogue.is.uec.ac.jp, koike@is.uec.ac.jp

‡ 産業技術総合研究所
100-8921 東京都千代田区霞ヶ関 1-3-1

zetaka@computer.org

あらまし

近年, 個人認証にユーザの位置情報を利用する方法が検討されてきている. 位置情報による個人認証では, ユーザによる自身の行動履歴と時刻情報の関連付け（自分がいつ, どこにいたか）が重要である. 本研究では, この関連付けを行いやすい場面としてユーザが 1 カ所に滞在している場合を想定し, 計測された位置情報の中からユーザが滞在していた場所（停留点）と時刻情報を抽出する手法を考案した. また, 複数のユーザデータから抽出した停留点情報を利用して認証を行うシステムを考案した.

Positional authentication system using GPS data and the stopping point calculation method

Takao Imazawa†　　Hideki Koike†　　Tetsuji Takada‡

†Graduate School of Information System
The University of Electro-Communications
1-5-1, Chofugaoka, Chofu-shi
Tokyo 182-8585, Japan

imazawa@vogue.is.uec.ac.jp, koike@is.uec.ac.jp

‡Advanced Industrial Science and Technology
1-3-1, Kasumigaseki, Chiyoda-ku
Tokyo 100-8921, Japan

zetaka@computer.org

Abstract In late years, the personal authentication method using the location information of the user has been examined. In the method of the personal authentication using the location information, the linkage between the action history and the time information of the user himself (when and where user was) is important.

In this paper, We have developed a new technique to extract the information of the place (stopping point) and the time which user stayed from the measured information of the user location, assuming that the action history and the time are easy to be linked when user stays at one place. We also have developed a new authentication system using the stopping point information extracted from plural user.

1　はじめに

近年, 個人認証にユーザの位置情報を利用する手法が検討されてきている. その背景には, 現在広く利用されている英数字や 4 桁番号によるパスワードでは, ユーザが自身の記憶負担を軽減するために覚えやすいパスワード（誕生日や電話番号など）を設定してしまい, 第三者による推測が容易になってしまうという問題がある.

一方, 位置情報を認証に用いた場合, 認証をするユーザや認証を行う時間帯によって位置情報はめまぐるしく変化し, かつ, 自身の行動履歴であるが故にユーザの記憶負担は比較的小さく済むという利点がある. 位置情報を個人認証に利用する場合, ユーザ自身による行動履歴と時刻情報の関連付け（自分がいつ, どこにいたか）が重要な要素となる.

本研究では, この関連付けを行いやすい場面としてユーザが 1 カ所に滞在している場合を想定し, 携帯電話の GPS 機能を用いて数 10 秒おきに細かく取得した位置情報の中からユーザが滞在していた場所（停留点）と時刻情報を抽出する手法を考案した. また, 複数のユーザデータから抽出した停留点情報を利用して認証を行うシステムを考案した.

2　位置情報を用いた認証

2.1　位置情報を用いた個人認証の概念

本研究では, 石原ら [1] によるユーザの位置情報の変化をパスワードにした認証システム Path-Pass を出発点とした認証システムと, それに伴う停留点の算出方法を提案する.

Path-Pass はユーザの位置情報（行動履歴）をパスワードとした認証である. ユーザの行動履歴を過去に遡ってたどることで認証を行う. 例えば新宿駅から電気通信大学まで来た後に認証を行う場合, 新宿駅→吉祥寺駅→電気通信大学と移動した時（図 1 実線）と, 新宿駅→調布駅→電気通信大学と移動した時（同破線）では経由した駅が異なるため, パスワードが異なる. 行動履歴をパスワードとすることで, 特定のパスワードを覚える必要がない, 覗き見によるなりすましが難しくなるといった利点が生じる.

図 1: Path-Pass の概念図

2.2　携帯電話の GPS 機能を利用した位置情報の取得

位置情報を計測し, その情報の蓄積とリアルタイムでの利用を行うために, 本研究では au の携帯電話の GPS 機能を利用した.

au の携帯電話では所定のリンクにアクセスすることで cdmaOne に基づいた測位が行われ, 結果が cgi に渡される. また, WAP（ Wireless Application Protocol ）の仕様では, 指定した時間が経過した後に指定した URL へ自動的にジャンプさせることが可能である. これらを組み合わせて一定時間毎に自動的に GPS 測位を行った.

2.3　取得されるデータの種類と形式

携帯電話の GPS 機能を用いて得られる情報は表 1 の形式で記録される.

記録される情報は, 緯度経度, 測定日時の他に, 測位方法を表す値である測位モードがある. 通常の GPS と異なり, 携帯電話の GPS 機能は GPS 衛星との通信状況によって測位方法を自動的に切り替えて測位を行う. 測位モードは 3 を除く 0 から 5 までの値をとり, 数字が大きいほど位置計測の精度は低下する. それぞれの値と測定精度は表 2 の通りである [6].

測位モード 0 は屋外で, 1 は屋外の屋根の下や屋内の窓際での計測で記録される. 同様に 2

表 1: 取得データの形式

```
+35.65697,+139.54180,2008/04/15,00:33:17,1
+35.65724,+139.54249,2008/04/15,00:33:31,1
+35.65714,+139.54245,2008/04/15,00:33:46,2
+35.65711,+139.54255,2008/04/15,00:34:00,2
+35.65702,+139.54038,2008/04/15,00:34:16,2
+35.65728,+139.54147,2008/04/15,00:34:31,0
+35.65750,+139.54177,2008/04/15,00:34:46,0
```

表 2: 各測位モード値の誤差

測位モード値	最小値 [m]	最大値 [m]
0	7	240
1	38	1087
2	28	734
4	53	2138
5	115	115

は主に屋内, 4は主に地下やトンネル内などで記録される. 5は記録されること自体が稀であるが, 主に電波状況が著しく悪いときに記録される.

誤差の値について, 測位モード0～4に関しては複数回記録されたうちの最大誤差と最小誤差の値である. 測位モード5に関しては1回しか記録されなかったため, その時の誤差の値である.

3 停留点の算出

3.1 停留点の必要性

Path-Pass では, ４０分前までの行動履歴を１０分毎に質問するという形式であったため, 質問された時刻に移動中であったなどの理由から, ユーザによる自身の行動履歴と時刻情報の関連付けができずに認証失敗となる場合があった. このような事態を避けるためには, ユーザが行動履歴と時刻情報の関連付け（自分がいつ, どこにいたか）を行いやすい場所, あるいは時刻を質問する必要がある.

本研究では, この関連付けを行いやすい場面としてユーザが1カ所に滞在している場合を想定し, 連続的に取得した位置情報の中からユーザが長時間滞在していたと思われる場所（＝停留点）を算出し, その場所をパスワードとすることで関連付けの簡便化を図った.

3.2 測定データの処理

測定されたデータのうち, 測位モードの値が４と５であるものを削除する. これは測定精度が低いためである. 次に, 各計測地点間の座標と計測時刻の差から2点間の移動速度を求め, 一定速度以上のデータを削除する. このとき, 測位モードの値から屋内データと屋外データの区別をつけ, それぞれ別々の速度閾値を設定する. これは屋内データの方が測定精度が低いため, 測定地点が分散し, その結果2点間の計算上の移動速度が上昇してしまい, 停留点と判断されなくなることを防ぐためである. また, 緯度・経度・時刻の情報は, 2点間の平均値を求め, その値を移動速度と対応させた.

3.3 近隣点の統合

速度閾値以下の点を地図上に表示すると, 滞在していたと思われる地点付近には点が密集する. この点が密集している地域を停留点として１点に定めるために, 近隣の点の統合を行う.

統合点は, 近隣と判定された点の緯度と経度を平均した点とする. 近隣の判定には, 時系列順に並んだ2点間の距離と時刻の間隔に閾値を設定し, 両方の条件を満たした場合を近隣点とした.

測定データと速度閾値以下の点, 近隣の点を統合した後の停留点をそれぞれ地図上に表示したものが, 図 2, 図 3, 図 4 である.

測定データ（図 2）ではマーカーが密集している地点が, 最終的には停留点として1点に定められた（図 4）.

図 2: 測定データ

図 3: 速度閾値以下の点

図 4: 停留点

4　認証システム

4.1　認証方法

石原ら [1] による Path-Pass システムに, 停留点を適用した認証システムを考案した.

本システムは, web ブラウザで利用可能な web アプリケーションとして実装した. ユーザはユーザ ID を入力し, 現在位置を地図上から選択して認証を開始する. 地図上には直前に選択した地点１カ所（青点）と選択肢８カ所（赤点）が表示されるので, ユーザは停留点を過去に遡って４カ所回答する（図 5）. ４カ所全て正解すれば認証成功となる.

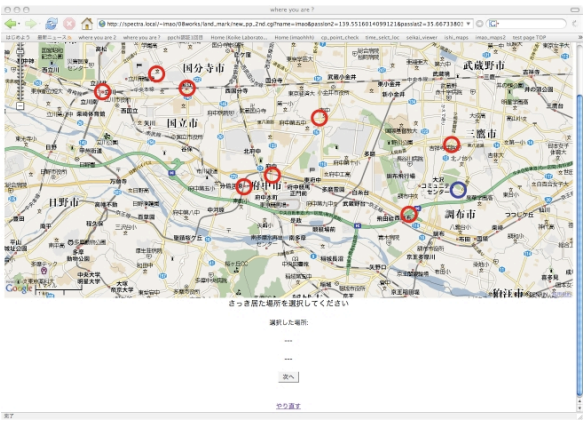

図 5: 認証画面

4.2　生活圏の設定

ユーザの停留点情報のうち, 認証に用いるものは最新の４点である. その最新４点を除いた過去１週間分の停留点情報から, 東西南北端の値のバウンディングボックスを設定し, ユーザの生活圏とした. 図 6 において地図上のマーカーは１週間以内の停留点を表し, 四角で囲まれた地域はこのユーザの生活圏を表す.

図 6: 生活圏の設定

4.3　ダミーの選出方法

画面上に表示される地点は, 基本的にダミー選択肢７つと正解選択肢１つ, そして前回選択した地点１つの計９地点である. 前回の選択地点が不正解であった場合は, 正解選択肢を表示せずダミー選択肢を１つ増やす. ダミー選択肢は, ユーザの過去１週間の停留点情報または他ユーザの停留点情報から選出される. 前回選択した地点が, 先に述べたユーザの生活圏内であっ

た場合, ダミー選択肢はユーザの過去の停留点情報から選出される. ただし認証に用いる情報は除かれる. 生活圏外であった場合は, 他ユーザの停留点情報の中から条件に一致するものを選出する. この条件とは, 「『前回選択した地点と次の正解地点との距離』と『前回選択した地点とダミー選択肢との距離』の差が小さいものから順に７点選択する」ことである.

ユーザが生活圏内にいる場合の認証画面では, ユーザが普段立ち寄る場所ばかりが選択肢として表示されるため, ユーザの普段の行動範囲を知らない攻撃者はもちろん, 知る攻撃者でも推測によるなりすましが難しくなる. 一方, 生活圏外にいる場合の認証画面では, 選択肢は行動範囲の外の地点であるため普段の行動範囲からの推測は成立しない. また, 似たような距離にある他ユーザの情報を利用しているため, どの選択肢も立ち寄る可能性があるように見える.

このように, ダミー選択肢の選出方法を選択地点によって変えることで, ユーザに関する情報を持つ攻撃者と持たない攻撃者両方に対する推測によるなりすまし対策を講じることができる.

5　関連研究

Denning ら [2] は, 位置情報を利用してリモートシステムへのアクセス権を決定するシステムを提案している. また Sharma ら [3] はアクセス制御の方式として, 特定の地点とユーザの現在位置に関する質問に回答することで認証を行うシステムを提案している. これらのシステムはリモートログインの制御には適しているが, 入室管理には適していない. 一方, 角田ら [4] は入室時の認証として, 位置情報と速度情報を利用した認証システムを提案している. これは特定の地点を特定の速度で通過することによって認証を行うシステムであり, 遠隔地にあるシステムにリモートログインするといった用途には適さない.

本研究では位置情報を利用し, かつ場所や用途を問わない汎用性の高い認証システムを目指した.

6　考察

6.1　安全性

ユーザの１週間の停留点数が１１点以上の場合は, 生活圏内での認証においてダミー７点と正解１点, 選択済み地点１点が正常に表示される. しかし, ユーザの１週間の停留点数が１０点以下であった場合ダミー選択肢の数が減ってしまう. その結果選択肢数が減少し, 安全性が損なわれてしまうという問題が生じた.

生活圏外でのダミーは他ユーザの停留点情報を利用するため, 選択肢が減少するという問題は無い. しかし, 「『前回選択した地点と次の正解地点との距離』と『前回選択した地点とダミー選択肢との距離』の差」を基準にしてダミーを選出するため, 表示される地域に偏りが生じてしまう場合があった. その結果表示される点が, 「前回選択した地点」と「正解地点」と「ダミー選択肢群」となりダミーの役割を果たさないという問題が生じた.

6.2　有用性

ユーザが直前に立ち寄った場所を４カ所回答するという方式なので, 長期間同じ場所にいた後での認証の場合, パスワードとなる地点を覚えていない可能性が考えられる. また, 先に述べたように安全性の面から考えても長期間同じ場所に居続けた後の認証行為は好ましくないと考えられる.

また, 本学の学生１６人に対して実際に位置情報の取得と停留点の算出を行い、自身の停留点をどの程度過去のものまで記憶しているかというアンケートを行った. 表 3 に日付と１人あたりの平均停留点数を, 図 7 に測定した日付と正確に記憶していた割合を示した.

この結果, １人の１日あたりの平均停留点数はおよそ４～５点であった. 本システムではおよそ１日分の停留点を回答することになる. また, 停留点の記憶は日を追う毎に薄れていくので, 記憶に新しい直前１日分の情報を質問することは妥当だと考えられる.

表 3: 平均停留点数

日付	合計停留点数	平均停留点数
1 日前	62	3.9
2 日前	65	4.1
3 日前	80	5.0
4 日前	72	4.5
5 日前	82	5.1
6 日前	83	5.2
7 日前	78	4.9

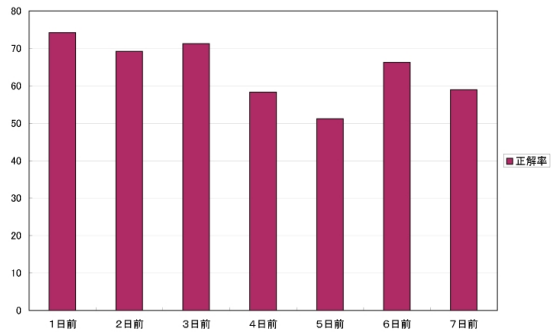

図 7: アンケート結果

6.3 利用場面

ユーザが適度に移動をし, ダミー機能が正常に作動すると仮定した場合, 本システムの利用場面は多岐にわたると考えられる.

必要な環境は web ブラウザのみ, 必要な操作は自分の移動経路の入力のみというシンプルさから, 入室時の認証管理や遠隔地にあるシステムへのリモートログインはもちろん, 電子マネーやクレジットカードでの支払い時の本人確認など, 現在日常生活で行われている認証行為のほぼ全てに利用できると考えられる.

7 まとめ

本研究では, 携帯電話の GPS 機能を用いて取得した位置情報の中からユーザが滞在していた場所（停留点）と時刻情報を抽出する手法を考案した. また, 複数のユーザデータから抽出した停留点情報を利用して認証を行うシステムを考案した. 今後は安全性と有用性の向上と同時に様々な場面での応用を目指す.

参考文献

[1] 石原雄貴, 小池英樹, Path-Pass:位置情報を用いた認証システム, Computer Security Symposium 2006 (CSS2006), 情報処理学会, pp.537-542, 2006.

[2] D.E. Denning, P.F. MacDoran, Location-Based Authentication: Grounding Cyberspace for Better Security, Computer Fraud and Security, Feb. 1996.

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

[4] 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, 位置と速度を利用した移動体向け認証方式の提案, 電子情報通信学会技術研究報告. MoMuC, モバイルマルチメディア通信 (IEICE technical report) Vol.106, No.359(20061109) pp. 11-16.

[5] google maps API
http://www.google.com/apis/maps/

[6] おこめ的技術総合資料館しいしせねっと
http://siisise.net/gps.html

[7] 増井俊之, インターフェイスの街角 (87) - 携帯から位置情報を活用, UNIX MAGAZINE, Vol.20, No7, (株) アスキー ,(2005).

[8] 田口浩平, 小池英樹, PHS を用いた個人認証に関する研究, マルチメディア, 分散, 協調とモバイル (DICOMO2001) シンポジウム, 情報処理学会, pp.458-465,2001.