M-068

スケジュールと GPS 情報を利用した認証方法の検討

A Person Authentication System Using Schedule Data and GPS

長谷 容子　青木 輝勝　安田 浩
Yohko Hase　Terumasa Aoki　Hiroshi Yasuda

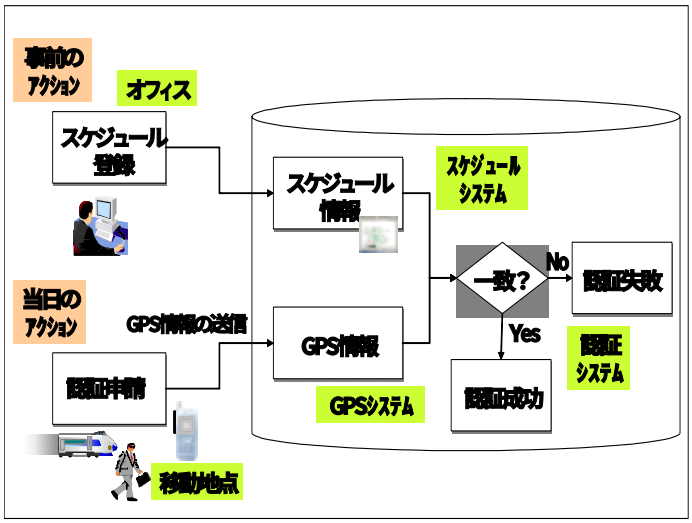
東京大学大学院工学系研究科
Graduate School of Engineering, University of Tokyo

１．はじめに

個人認証技術は、従来よりさまざまな研究がなされてきた。例えば、個人認証の方法として、「パスワード等の個人が持つ秘密情報を利用したもの」、「IC カード等の個人所有物を利用したもの」、「指紋等の個人固有の生体的特徴を利用したもの（バイオメトリクス）」、「手指動等の個人の行動特性を利用したもの」[(1)]等の検討が盛んにおこなわれている。しかしながら、従来の研究の多くは、それぞれ個人の手法の認証精度を向上させることを主眼にしたものが多く、アプリケーションを想定し、ユーザーの利用環境にも考慮した個人認証方法は、ほとんど検討されていない。[(3),(4)]

ユーザーの環境として、これまでの固定デスクトップＰＣを利用する一定の環境だけでなく、ユーザーの移動とともに、認証システムへアクセスするクライアント機器（携帯電話、ＰＤＡ、ノートＰＣ等）自身も移動するモバイル環境が急速に普及してきている。そのため、従来はあまり問題とならなかったユーザーの利用環境の変化（湿度、温度、照度、位置等）によって認証精度が影響を受けるような個人認証方法等は、そのままでは使うことができない。また、モバイル機器の持つ“持ち運ぶ“という最大の特徴を考えると、セキュリティのための付加的装置等を利用した認証の仕組みを考えることは現実的ではない。

そこで本稿では、ユーザーのモバイル環境において有効と考えられる新しい個人認証システムとして「スケジュール及び GPS 情報を利用した個人認証システム」を考え、その特徴について検討する。



［図１］スケジュール及び GPS 情報を利用した個人認証システムの全体イメージ

２．スケジュール及び GPS 情報を利用した個人認証システムの概要

「スケジュール及び GPS 情報を利用した個人認証システム」は、“ユーザー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する“という行為に関する情報を、個人を認証する際の特徴量として利用する個人認証システムである。（図１）

ユーザーにおいては、GPS 機能を持つ携帯電話の所有を前提としており、システムは、主に、電子的にスケジュールを管理することができるスケジュール管理サーバ、ユーザーの位置情報を管理する GPS サーバ、スケジュール情報と GPS 情報を照会して認証を行う認証サーバ、ユーザーの携帯電話とのやりとりを行う CTI サーバから構成される。（図２）

以下に、出張を予定しているユーザーを想定して、本システムを利用した認証までの流れを説明する。

＜事前の流れ＞

出張に先立って、ユーザー、及び、システムが事前に行う処理は、以下のようである（図２の①～⑤）。

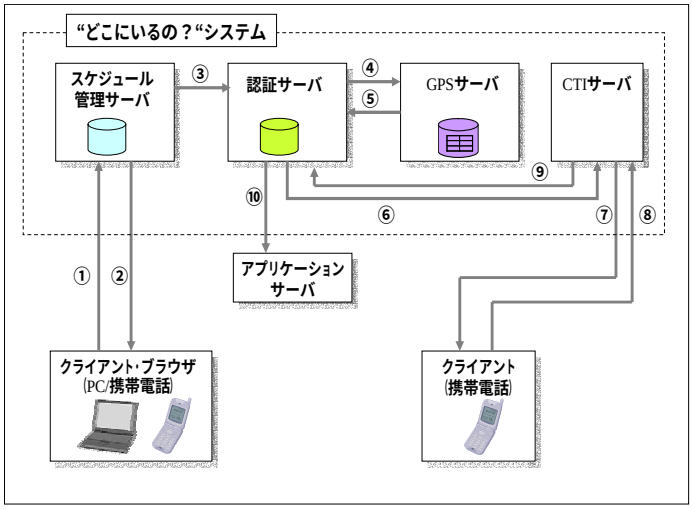
１．ユーザーは、オフィス等からあらかじめ予定している出張スケジュール（行き先、経路、移動のための交通手段、到着時間等）を社内のスケジュール管理サーバに登録する。
２．スケジュール管理サーバに登録された予定出張先の場所から、GPS サーバにおいて GPS 情報を換算し、ユーザー情報やその他のスケジュール情報とともに、認証サーバにおいて情報を管理する。
３．認証サーバは、ユーザーの出張スケジュールデータ（行き先、経路、移動のための交通手段、到着時間等）を用いて、認証を行うチェックポイント（時間、ユーザーの目的地までの途中到着場所の GPS データ等）を複数決定し管理する。（図３）

＜当日の流れ＞

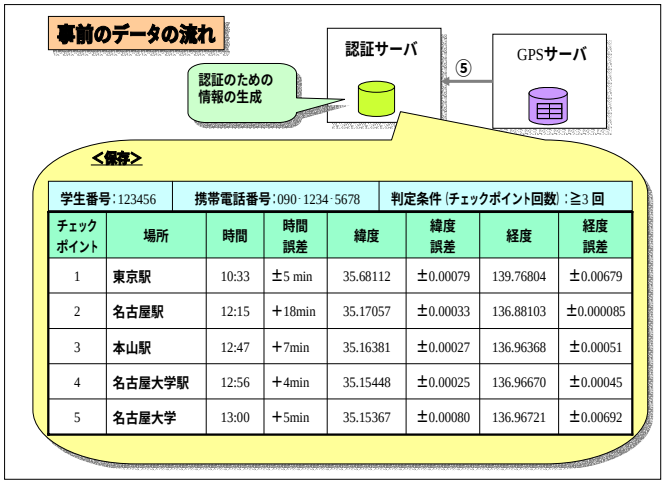
出張当日のユーザー、及び、システムが事前に行う処理は、以下のようである（図２の⑥～⑩）。

１．認証サーバは、あらかじめ管理していたチェックポイントの時間が来た際に、CTI サーバから移動中のユーザーに電話をかけるよう指示する。
２．ユーザーは、CTI サーバからの電話がかかってきたことを合図に、その場所から GPS データを送信する。
３．認証サーバは、ユーザーから送られてきた GPS データと予定到着場所の GPS データを比較する。

4．１～３を複数のチェックポイントで行い、最終的にユーザーが出張目的地に到達した時点を最終のチェックポイントとして、GPS データを比較する。
5．４～５における比較の結果から、予定通りの移動を行ったとみなされた場合、本人と判定され、アプリケーションサーバへのアクセスが許可される。



［図２］システムの主な全体構成と処理の流れ



チェックポイント	場所	時間	時間誤差	緯度	緯度誤差	経度	経度誤差
1	東京駅	10:33	±5 min	35.68112	±0.00079	139.76804	±0.00679
2	名古屋駅	12:15	＋18min	35.17057	±0.00033	136.88103	±0.000085
3	本山駅	12:47	＋7min	35.16381	±0.00027	136.96368	±0.00051
4	名古屋大学駅	12:56	＋4min	35.15448	±0.00025	136.96670	±0.00045
5	名古屋大学	13:00	＋5min	35.15367	±0.00080	136.96721	±0.00692

［図３］認証のために管理する情報の例

３．考察

本システムの実現に際して、以下の状況について検討する必要があることがわかった。

１）ユーザーの移動途中において、電話や GPS データを送信できない地点が存在しうる。
２）ユーザーが予定の場所に、正確に立たない場合がある。
３）ユーザーが予定の時間に到着しない場合がある。

１）は、例えば、ユーザーが建物の中や地下に入ってしまった場合等が該当する。この場合、ユーザーの移動出発地点から出張先地点までの複数（N 箇所）のチェックポイントのうち、ある数（M 箇所（N≧M））以上のチェックポイントにおいて GPS データを認証システムが取得できた場合のみを認証対象とするように設定することにより、本システムの有効範囲を広げることができる。当然ながら、認証対象となるチェックポイントの数が多いほど、認証精度は高いと考えられる。もし、M 箇所以上のチェックポイントから GPS データを取得できなかった（あるいは、できそうにない）場合は、認証サーバがあらかじめ想定していたチェックポイントの変更（追加等）を行う設定も有効である。

２）については、認証に利用する GPS データの有効範囲の設定を考慮することによって、本システムの有効範囲を広げることができる。GPS データの有効範囲内において、誤差が小さいほど認証精度は高いわけであるが、装備している GPS センサーの誤差や人間の行動範囲を見込んだ誤差範囲に設定することが重要である。

３）は、２）と同様に、時刻データの有効範囲の設定の考慮が必要となるが、それ以外に、移動手段（鉄道、飛行機等）の遅延等による誤差や利用者の行動特性（いつも遅れがちの性質な人等）も考慮することによって、本システムの有効範囲を広げることができる。

４．まとめ

本稿では、スケジュール及び GPS 情報を利用した個人認証システムについて、概要、及び、実現に向けて検討が必要となる事項について述べた。

本システムによれば、ユーザーが秘密情報（パスワード等）を意識的に記憶したり、入力したりする負担がなく、指紋等のバイオメトリクスを利用した認証システムと異なり、湿度や温度等の気象に影響されることもない。また、スケジュール情報を管理するスケジュールサーバの事前の盗聴、及び、ユーザーの持つ携帯電話の盗難という２つの悪意をもった行為が連携してなされない限り、なりすましの危険性もかなり低いと考えられ、セキュリティレベルの観点からも有効である。

［参考文献］

（１） 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誌 D-II, Vol.J84-D-II, No.2, pp.258-265, 2001.
（２） 坂野鋭, “バイオメトリクス個人認証技術の動向と課題“ ,信学技法, PRMU99-29,pp.75-82,June 1999.
（３） 長谷容子, 青木輝勝, 安田浩, “多重インタラクティブ個人認証システムの提案”電子情報通信学会 2002 年総合大会 A-7-14, 2002.
（４） 長谷容子, 青木輝勝, 安田浩, “モバイル端末における多重インタラクティブ個人認証システムの提案” 電子化知的財産・社会基盤研究報告, No.16 16-6 2002.
（５） 長谷容子, 青木輝勝, 安田浩, “スケジュールと GPS 情報を利用した認証方法の提案” 情報処理学会第 66 回全国大会 5J-1, 2004.