# ハッシュ連鎖を用いた位置証跡方法のアクセスポイントによる改良

村尾亮 †‡　　森田光 †

† 神奈川大学大学院工学研究科　　‡r201170119oq@kanagawa-u.ac.jp
221-8686 横浜市神奈川区六角橋 3-27-1

**あらまし** GPS による位置情報には証拠性がない。位置情報の正しさを検証するためには信頼できる第三者が必要になるが、空間的に第三者を多数配置することはコスト的に不可能である。そこで、著者らは位置情報の軌跡とユーザ同士の通信を活用する方法を提案した。しかし、ユーザの数が少ない場合の証拠性は損なわれる。本研究では、信頼できるアクセスポイントを設置し、ユーザの数や密度に左右され難いシステムを提案する。また、そのようなアクセスポイントを用いた場合の証跡方法を与え、その評価方法について考察した。

# The tracing data-logger method by using trusted access points

Ryo Murao †‡　　Hikaru Morita†

†Graduate School of Engineering, Kanagawa University
3-27-1, Rokkakubashi, Kanagawa-ward, Yokohama-shi,221-8686, Japan.
‡r201170119oq@kanagawa-u.ac.jp

**Abstract** The GPS positional information is the lack of evidence. In order to verify the correctness of the positional information, a trusted third party is necesary, but it costs too high. Therefore, the authors proposed a method to take advantage of communication the users and the tracing of positional information. However, the evidence of a small number of users was impaired. In this study, we use reliable access points so that a system doesn't depend on the density and the number of users. In addition, the trail gives way in the case of using the access points, and the evaluation method is discussed.

## 1　はじめに

GPS(Global Positioning System) による位置情報には証拠性がない。位置情報はただの座標を示すデータに過ぎず、改ざんや偽造といったことが容易に可能である。位置情報に証拠性を与えるために、位置情報が正しいこと責任を負う信頼できる第三者が必要になる。信頼できる第三者は直接 GPS ユーザの存在を確認をする。しかし、信頼できる第三者を空間的に多数配置することはコスト的に不可能である。

そこで、筆者らは位置情報の軌跡とユーザ同士の通信を活用する方法を提案した [1]。 確証が第三者的に持てる地点から位置情報取得を続け、それらをハッシュ連鎖させる。そうすることで位置の軌跡を作り、明らかな偽造を検知することで改ざん可能な範囲を狭める。また、システムユーザ同士で同じ地点にいた際、通信し、互いの軌跡に影響を与え合うことで目撃者のような役割となり検証可能な地点を増やした。しかし、ユーザは信頼できる第三者ではないため、確実な情報とはなり得ない。ユーザ間の結託による偽造なども考えられる。また、ユーザの数が少ない場合、ここでの補償は役に立たなくなる。

本研究では、新たに信頼できる第三者によるアクセスポイントを設置する。アクセスポイントでは、ユーザと同様の通信を行う。即ち、ユーザが近くに居た場合に通信し、軌跡に影響を残すことで、アクセスポイントがその時ユーザが居ることを示す。それによりユーザの数や、場所による密度の違いに左右され難いシステムを提案した。また、そのようなアクセスポイントを用いた場合の証跡方法を与え、その評価方法について考察した。

## 2　提案の概要

### 2.1　位置情報に証拠を与える困難性

位置情報に証拠性を与えるためには、GPS などの位置検出システム自体が証拠性を与える事が望ましい。なぜなら、偽造された位置情報を用いて証拠性を得ようとする可能性があるためである。しかし、例えばGPS では、複数のGPS 衛星からの信号を受信し計算することで位置を検出している。しかし、GPS が位置情報に対して証拠性を与える機能はない。よって、証拠性を与えるためには信頼できる第三者が必要不可欠となる。しかし、その第三者が位置情報に署名するだけならば簡単だが、位置情報に対して検証するには、直接その場にいない限り不可能である。結果として、証拠性を与えるためには、あらゆる場所に信頼できる第三者を配置する必要が生じ、これもコストの点から不可能となる。

### 2.2　位置証跡方法の概要

そこで考えられるのが、現状の GPS を利用し、改ざんや偽造を困難にする方法である。改ざんや偽造を行った際、それらを検知できるようにする。まず、検証可能な地点を最低でも一つ用意し、その地点から位置情報を一定間隔で取得し軌跡を作る。そうすることで、明らかに軌跡から外れている位置情報が偽造か改ざんであることが検知でき、単一の位置情報に比べ偽造か改ざんの余地を減らすことが可能である。また、検証可能である地点を複数用意し、軌跡の途中でも組み込むことでより偽造・改ざん可能範囲を狭めることも可能である。そのため、検証可能地点が多いほど偽造の範囲を狭めることが可能だが、検証可能な地点とは信頼できる第三者を配置することに変わりなく、前述の通りコスト的に限界がある。

そこで、信頼できる第三者を用いない手段で検証可能な地点を作ることで、偽造範囲を狭める。具体的には、ユーザ同士での通信を行う。ユーザ同士が近い地点にいる時に、アドホックで通信を行い、互いに互いの目撃者として証人にする。また、通信した情報も軌跡の中に加えることで、後の検証も可能である。一方で、常にユーザの数が十分にいるとは限らない問題点がある。ユーザの数が十分でないと、数が疎らな地点では偽造可能な範囲が広まってしまい、証拠性として乏しくなってしまう。数が多くとも密度が少ないと同様の問題が生じる。また、ユーザの結託も考えられる。結託には、正当なユーザとの通信があれば、結託の存在を確認可能である。そのため、ユーザの数や密度が十分でない場合では結託も成功しやすくなる。その上、結託したユーザが非常に多い場合、正当なユーザとの通信をしたとしても、どちらが不正なユーザか判断出来ないことが考えられる。

### 2.3　提案

ユーザと同様の通信を行うアクセスポイントを設置する。ユーザがそのアクセスポイントの近くを通る際にユーザ同士と同様の通信を行うことで、そのアクセスポイントと通信できる地点である証拠をユーザの軌跡の中に残す。このようにして、信頼できる第三者が直接配置されていなくとも、アクセスポイントを管理することで検証を可能とする。

アクセスポイントは信頼できる第三者があらゆる場所に設置する。公共的に設置するのであれば電信柱などに設置することを考え。アクセスポイントに関しては、位置を移動しないものとする。

以上をまとめて、構成図にしたものが図 1 である。

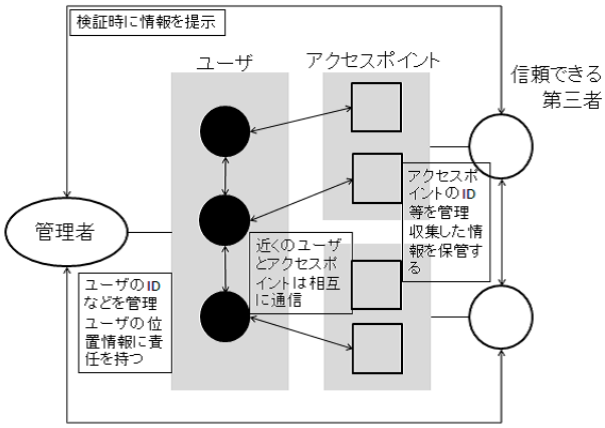


図 1: システム構成図

# 3 提案法

## 3.1 準備

提案をする準備として、位置情報とユーザごとに与えられた乱数、ユーザの ID が必要である。位置情報は GPS から取得可能な情報として、受信機が算出した現在値の座標と現在の時間を含めたものを言う。座標情報と時間情報を合わせていないと、証明する際に意味がないためこのような、一纏めとした扱いをする。乱数はユーザによって違う値を与えられる。またユーザは数値を与えられながら数値自体を知ることができない耐タンパー性をもつものとする。ユーザ ID は利用者個人を示すものである。位置情報だけでは、誰の (何の) ものであるかが不明である。証明する理由として、何者かに示す必要があるため、証明するものの ID が必要である。また、アクセスポイントに関しても、ユーザと同様の通信を行うために ID と乱数を与えておく必要がある。

また、予め、それら ID や乱数を管理するような信頼できる第三者が必要である。これを管理者とする。この時の管理者は、アクセスポイントを管理する第三者と一致する必要は無いが、アクセスポイントを利用するために、第三者同士で利用できるように決めておく必要がある。

続いて、利用する仕組みとして、ハッシュ連鎖を挙げる。ハッシュ連鎖とは、ある数値に対してハッシュ関数を用いて出した値に対して再びハッシュしていく仕組みである。ハッシュ関数はどのような値でも入力可能であり、同じ入力に対しては常に同じ出力を返す。また出力は一定のビット長であり、入力とは無関係の乱数のような値となる。そのため一方向性を持ち、出力からなんら情報を引き出すことができない。また、ハッシュ関数の出力をハッシュ値と呼ぶ。

### 3.1.1 記号の表記

以上を踏まえ、概要を説明する。利用する記号はそれぞれ以下の通り

- $H_i$:ハッシュ値
- $H_0$:ユーザごとに与えられた乱数
- $x_i$:GPS 位置情報（座標と時刻）
- $ID$:ユーザの ID
- $h()$:ハッシュ関数
- $\|$:連結

であるとする。

## 3.2 位置証跡のプロトコル

**step 1.** $i = 0$ とし、開始する

**step 2.** $x_i$ を取得する

**step 3.** 他のユーザかアクセスポイントと通信可能であれば通信する。通信のプロトコルに関しては後述する

**step 4.** $H_i$ と $x_i$ を連結させて、ハッシュ化し $H_{i+1}$ を得るとともに、$x_i$ を蓄積する

$$H_{i+1} = h(x_i \| H_i)$$

**step 5.** 予め決めた間隔で、$x_i$ と $H_i$ と $ID$ を管理者に送信する

**step 6.** $i$ に $i + 1$ を代入する

**step 7.** 必要に応じて、step 2. へ

**step 8.** 蓄積した $x_i \quad (i = 0, 1, \cdots\cdots)$ すべてに対し、管理者の回収に応じ、管理者は確認をする

### 3.2.1 ユーザ通信のプロトコル

ユーザとの通信を行い、ハッシュ値の更新を行う。即ち、通信が発生した場合、位置証跡プロトコルの step.4 における $H_i$ に変化を与える。

この時の通信プロトコルを示すため、通信相手の情報を表記が必要である場合には、

- $H_A$:ハッシュ値
- $x_A$:位置情報
- $ID_A$:ユーザの ID

と表記する。

まず、$x_i$ と $H_i$ と利用者 $ID$ を相互に送信する。このとき、互いの位置情報を確認し、近くに存在していることが間違いないかを確認する。確認できたならば、相手の $ID_A$ と $H_{A_i}$ を保存する。

以上を終えた後、ハッシュ値を更新する。更新には、自分のハッシュ値と相手のハッシュ値を連結し、ハッシュする。式にして示すと

$$H_i = h(H_i \parallel H_{A_i})$$

となり、step.4 における $H_i$ として扱う

### 3.2.2 信頼できるアクセスポイントの導入プロトコル

ユーザがアクセスポイントに代わっても同様の通信を行う。ただし、アクセスポイントは移動しないため、GPS を用いる必要が無い。そのため、アクセスポイントにおける位置情報 $(x_{AP_i})$ では、時刻のみが変化するユーザとは異なるものを利用する。

そのため、アクセスポイントは位置情報を用いてハッシュ値の更新を行えない。ただし、ユーザはそれを利用して偽造をすることができない。ユーザとの通信範囲が定まっているため、通信した段階でユーザの位置情報がその範囲の中であると判明する。即ち、その位置であるという証拠になるため、ユーザは偽造にアクセスポイントを利用することができない。

位置証跡と通信のプロトコルをまとめて、フローチャートにしたものが図 2 である。またユーザのデータのやりとりを示したシーケンス図を図 3 に示す。

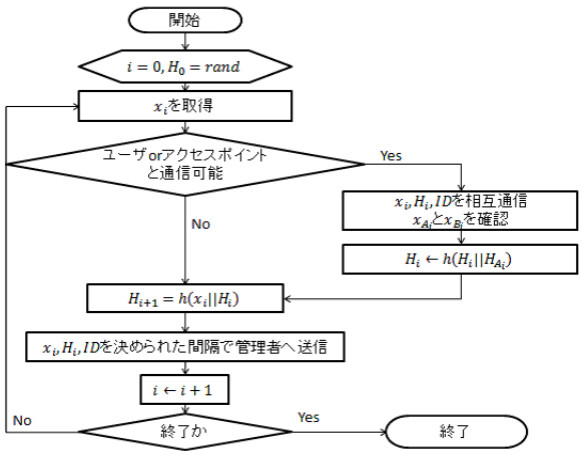


図 2: 提案法のフローチャート

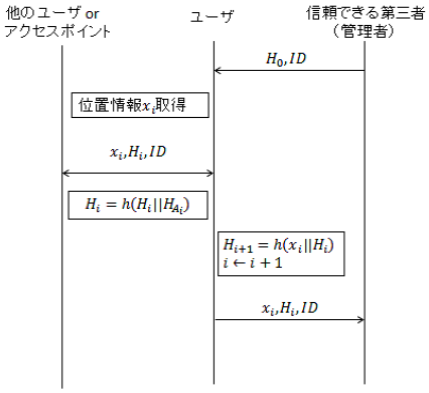


図 3: 提案法のデータシーケンス図

## 4 考察

### 4.1 偽造検知

扱っている位置情報自体は GPS を用いて得たものであり、偽造は容易である。提案法では、偽造した位置情報を検知することで偽造を防ぐ。軌跡を用いることで、明らかに軌跡と外れた位置が検出されれば、それは偽造だと判断出来る。ただし、軌跡の中に確実に検証可能な場所が必要である。加えて、検証可能な地点を経過して

から時間が経つほど改ざん可能な範囲が広がるため、軌跡だけでは検知できなくなる。

ユーザやアクセスポイントを用いることで、検証可能な地点を増やし、偽造可能範囲を狭めることができる。他のユーザやアクセスポイントから送られてくる情報のハッシュ値は、その時までの位置情報を全てハッシュ連鎖したものである。偽造するために都合の良いユーザの情報を作ることは、偽造パターンを増やす事でしかなく、一人で行うことで偽造をしやすくすることはできない。また、複数人で結託した上で偽造をすることは、一人で偽造をするより、偽造しやすくする。そのような場合には、正当なユーザとの通信で位置情報の異常が検知できるためユーザとアクセスポイントを多数用意することで、結託した場合でも偽造可能とはならない。

また、予め理想的な軌跡を用意することは出来ない。まず、交通状況は常に一定ではなく、毎日変わるものである。仮に偽造できたとしても、アクセスポイントから常に同じ値で通信する訳では無く、通信の内容次第で次回の出力も変わるため予測不可能である。

## 4.2 評価法

偽造可能な範囲を狭めることにより、偽造を困難とさせることが、本研究における位置情報に証拠性を与えることである。即ち、偽造可能な範囲を算出し、従来と比べてどの程度狭められたか比較する。図 4 は算出方法を示したもの

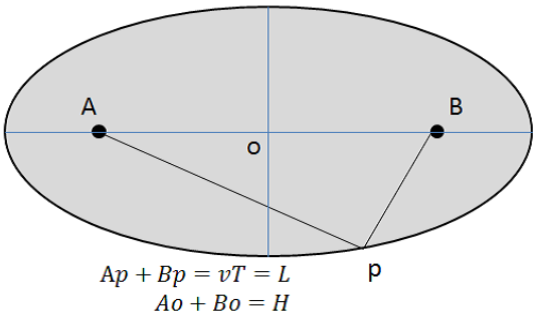


図 4: 偽造可能範囲の評価法

である。点 A と点 B は共に検証可能地点であり、その距離を $H$ とし、A から B へ向かうと考える。出発から到着までに掛かる時間を $T$ とし、ユーザの平均の早さを $v$ すると、ユーザの移動した距離を $L = vt$ と示すことができ、$vt \geq H$ となる。このとき、$vt$ の両端をそれぞれ A,B とし、点 p のみを角とする二本の直線であるとすると、p の取り得る点を結ぶことで A,B を焦点とした楕円が作図でき、その楕円の中がユーザの行きうる範囲であり、証跡の曖昧さである。

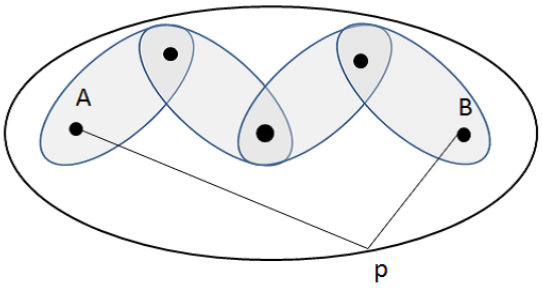


図 5: 偽造可能範囲の比較

図 5 は、アクセスポイントを用いた場合、偽造可能範囲がどの程度狭められるかを図示したものである。アクセスポイントは検証可能地点であるため、区間ごとに図 4 と同様の形で偽造可能範囲を示すことが可能である。図 5 では、アクセスポイントとの通信が二度あった場合の図である。外側の楕円はアクセスポイントを用いない場合の範囲、内側の楕円がアクセスポイントを利用した場合の範囲であり、内側の範囲の総和から、アクセスポイントを利用することで範囲を狭めていることが解る。

ここで、どの程度曖昧さがなくなったのかを面積の比較を用いて示す。また、その時、アクセスポイントの数がいくつなのかを $n$、二点の距離と実際に通った長さを比較し数値化したものを $R = \frac{L}{H}$ であるとする。

まず、楕円の面積を求めるためには、長軸と短軸の半分の長さが必要であり、それぞれ $x, y$ で示す。$x$ は $L$ の半分であるため、$x = \frac{L}{2}$ である。また $x^2 - y^2 = (\frac{H}{2})^2$ が成り立つため、$y = \frac{1}{2}L\sqrt{1 - \frac{1}{R^2}}$ である。ここで楕円の面積を

$S$ とすると $S = \pi xy$ であるため

$$S = \frac{\pi}{4} L^2 \sqrt{1 - \frac{1}{R^2}} \tag{1}$$

である。

内側の楕円は $H$ を $h_i$、$L$ を $l_i$ とおき、それぞれ平均であると考える。即ち $L = \sum_{i=1}^{d} l_i = dl_i$ であることが解る。なお、$d$ は分割された数である。$h_i$ の総和は、二点 AB 間の距離より長くなるのは、図 5 などからも明らかである。そのため $h_i$ に関しては別途定義をする。仮に、アクセスポイントを網目状に配置するとする。その時アクセスポイント一つあたりの面積は $\frac{s}{n}$ である。網目状に配置しているため、その面積は正方形とみなして考えると、$h_i$ は正方形の辺である。よって、$h = \sqrt{\frac{s}{n}}$ として考えることができる。

また、$R = \frac{l_i}{h_i}$ であると仮定する。このとき、内側の楕円ひとつの面積を $s_i$ であらわし、その面積の総和は

$$ds_i = \frac{\pi}{4} {l_i}^2 \sqrt{1 - \frac{1}{R^2}} \tag{2}$$

で表すことができる。

面積の比を $\frac{ds_i}{S}$ で表すと、(1)(2) から共通部分を約分して $\frac{ds_i}{S} = d(\frac{l}{L})^2$ となる。また $L = dl_i$ であったため、$L$ に代入することで $\frac{ds_i}{S} = \frac{1}{d}$ となり、これを $R$ と $n$ の式に直すと

$$\frac{ds_i}{S} = R \frac{\sqrt{\pi}}{2\sqrt{n}} (1 - \frac{1}{R^2})^{\frac{1}{4}} \tag{3}$$

となり、$n, R$ を用いて評価可能である。また、その時のグラフを図 6 に示す。

グラフより $R = 1$ の時、曖昧さが 0 になることが解る。$R = 1$ であるということは $R = \frac{L}{H} = 1$ であるため、二点間の距離とユーザが通る軌跡が一致することを示し、一切の曖昧さがないことは間違いない。また、$R$ の値が大きくなるほど曖昧さが大きくなることが解る。$R$ は実際の長さと距離との比になるため、$R = 2$ であれば、距離の二倍を示し、それだけ遠回りをしていることになり、区間の曖昧さが広まると考えられる。

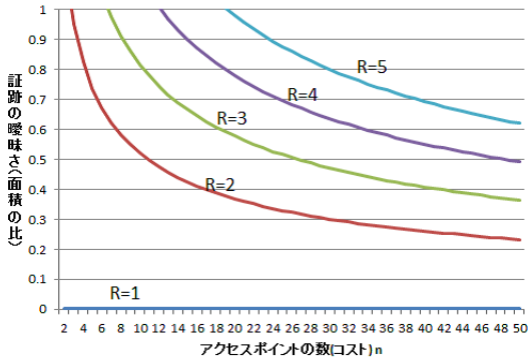


図 6: アクセスポイントの数と曖昧さの関係

$n$ においては式 (3) からも明らかであるが、ルートで縮減することがグラフより読み取れる。$n$ は全体のアクセスポイントの数であり、必ずしも通るわけではない。空間に網目状で等間隔に配置されているとしているため、このようなルートの減り方にも不自然ではない。

## 4.3 適用

### 4.3.1 アクセスポイントの配置

アクセスポイントを増やすことで、位置証跡の曖昧さを少なくすることができるのは明らかであるが、アクセスポイントの個数が直接コストに繋がる。そのため、単純に個数を増やす以外に、配置を工夫することによって曖昧さを減らす。

評価では楕円を作り範囲を面で示したが、実際にユーザが通るのは道である。つまり、ユーザはあらゆる方向に行き来できる訳ではなく、決まった幾つかの方向にしか移動できない。そのため、例えば距離に関係なく、交差点ごとにアクセスポイントを配置することなどで、実際の移動した長さと距離を一致させて $R = 1$ となるような状況を目指すことができる。

またアクセスポイントと通信を行う際、どの程度の距離で通信可能であるかによって、曖昧さにも変化がある。例えば PHS では、基地局と通信可能範囲が 50 メートルと考えると、25 メートルごとに基地局があると考えられる。同程度の能力がアクセスポイントにあるとして、

この程度の距離であれば、人の歩く速度や車の速度などを鑑みても十分だと考えられる。

以上のような特性を考えて、ランダムに配置するのではなく、距離や場所を検討した上で配置することで、評価における図 6 よりも曖昧さをなくせる。

#### 4.3.2 応用

本稿では、一般のユーザと信頼できる第三者と一対一の関係で考えてきたが、実際とは異なることが予測される。

ユーザは広く一般人であっても利用可能であるが、細かく位置情報を証拠付きで残す利用は、業務における従業員の管理であったり、フォレンジクスという用途が考えられる。その時、ユーザは従業員、信頼できる第三者は業務管理者となる。業務管理者が検証可能な位置は社内だけとすると、事業場外労働をする時、軌跡を用いて位置の証跡を行う。その場合、業種にもよるが、従業員同士が近くにいるとは限らない。そこで、アクセスポイントの活用が考えられるが、一企業の業務管理のみにアクセスポイントの設置管理はコスト過剰になる懸念がある。そのため、アクセスポイントに関しては別途管理する。即ち、複数の会社が軌跡を用いた証跡を行い、補助的にアクセスポイントの管理会社を用いることが考えられる。

また、タクシー会社など、主だった業務が事業場外労働である場合では、一企業が第三者としてアクセスポイントの役割を果たすことも考えられる。そのような場合であれば、タクシー会社のサービスとして位置に証拠性を持たせるようなサービスを一般向けに行う事も可能である。

## 5 まとめ

位置情報には証拠性がなく、位置情報の軌跡を用いた証跡方法によって証拠性を与えた。しかし、ユーザの密度や数に左右されていた為、曖昧さの残る方法であった。そこで、本稿では、信頼できるアクセスポイントを設置し、証跡の曖昧さを減らした。また、曖昧さを面積で示し、アクセスポイントの有無で比を出すことで、曖昧さがどの程度なくせるかという評価法を示した。評価法によって、アクセスポイント間の距離より遠く回ることで曖昧さが増えてしまうこと、アクセスポイントの数にルートで割る数だけ曖昧さを減らせることから、従来法と比べて曖昧さがなくなったことを示した。

その他では、曖昧さを減らすためにどの様にアクセスポイントを配置するのが良いかを検討し、アクセスポイントの通信距離がそのまま曖昧さに繋がることを示した。また、個人利用以外の場合についても検討を行い、企業で証跡方法を利用する場合や、そのような企業に関してもアクセスポイントとして利用することについてを検討した。

## 参考文献

[1] 村尾亮, 長谷川哲臣, 内田優輝, 奥野祥二, 森田光,“ハッシュ連鎖を用いた改ざんを困難とする位置の証跡方法,” SCIS2012

[2] Stuart Haber,W. Scott Stornetta,“How to Time-Stamp a Digital Document,” Journal of Cryptology, Vol.3,No.2,pp.99-111,1991