

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5950345号  
(P5950345)

(45) 発行日 平成28年7月13日(2016.7.13)

(24) 登録日 平成28年6月17日(2016.6.17)

(51) Int.Cl. F1  
G06F 21/31 (2013.01) G06F 21/31

請求項の数 6 (全 11 頁)

<p>(21) 出願番号 特願2012-189186 (P2012-189186)                  (22) 出願日 平成24年8月29日 (2012.8.29)                  (65) 公開番号 特開2014-48747 (P2014-48747A)                  (43) 公開日 平成26年3月17日 (2014.3.17)                  審査請求日 平成27年7月28日 (2015.7.28)</p>	<p>(73) 特許権者 899000057                  学校法人日本大学                  東京都千代田区九段南四丁目8番24号                  (74) 代理人 100119677                  弁理士 岡田 賢治                  (74) 代理人 100115794                  弁理士 今下 勝博                  (72) 発明者 木原 雅巳                  東京都千代田区九段南四丁目8番24号                  学校法人日本大学内                    審査官 宮司 卓佳</p>
--	--

最終頁に続く

(54) 【発明の名称】 位置認証システム

(57) 【特許請求の範囲】

【請求項1】

端末装置に搭載され、当該端末装置の位置を取得する位置情報取得部と、  
 前記端末装置に搭載され、前記位置情報取得部の取得した位置を当該端末装置の位置のオフセット情報に基づいて移動させて認証位置を求める認証位置演算部と、  
 前記端末装置に搭載され、前記認証位置演算部の求めた前記認証位置を送信する位置情報送信部と、  
 認証サーバに搭載され、予め登録されている前記端末装置の位置と前記位置情報送信部から送信された前記認証位置とが一致している場合に認証成功と判定する認証部と、  
 を備える位置認証システム。

【請求項2】

端末装置に搭載され、当該端末装置の位置を取得する位置情報取得部と、  
 前記端末装置に搭載され、当該端末装置の位置のオフセット情報を、前記位置情報取得部の取得した位置と共に送信する位置情報送信部と、  
 認証サーバに搭載され、前記位置情報送信部から送信された位置を前記位置情報送信部から送信されたオフセット情報に基づいて移動させて認証位置を求める認証位置演算部と、  
 前記認証サーバに搭載され、予め登録されている前記端末装置の位置と前記認証位置演算部の求めた認証位置とが一致している場合に認証成功と判定する認証部と、  
 を備える位置認証システム。

**【請求項 3】**

前記オフセット情報は、複数桁の数値であり、

前記認証位置演算部は、前記オフセット情報として取得した数値を用いて予め定められた方法で演算することで前記端末装置の位置の移動量を算出し、当該移動量に応じて前記位置情報取得部の取得した位置を移動させることを特徴とする請求項 1 又は 2 に記載の位置認証システム。

**【請求項 4】**

端末装置の現在位置を取得する位置取得手順と、

前記位置取得手順で取得した前記端末装置の位置を、当該端末装置の位置のオフセット情報に基づいて移動させて認証位置を求める認証位置演算手順と、

前記認証位置演算手順で求めた前記認証位置を送信する認証位置送信手順と、

予め登録されている前記端末装置の位置と前記位置情報送信手順で送信された前記認証位置とが一致している場合に認証成功と判定する認証手順と、

を順に有する位置認証方法。

10

**【請求項 5】**

端末装置の現在位置を取得する位置取得手順と、

端末装置の位置のオフセット情報を、前記位置取得手順で取得した位置と共に送信する位置情報送信手順と、

前記位置情報送信手順で送信した前記端末装置の位置を前記オフセット情報に基づいて移動させて認証位置を求める認証位置演算手順と、

予め登録されている前記端末装置の位置と前記認証位置演算手順で求めた認証位置とが一致している場合に認証成功と判定する認証手順と、

を順に有する位置認証方法。

20

**【請求項 6】**

前記オフセット情報は、複数桁の数値であり、

前記認証位置演算手順において、前記オフセット情報として取得した数値を用いて予め定められた方法で演算することで前記端末装置の位置の移動量を算出し、当該移動量に応じて前記端末装置の位置を移動させることを特徴とする請求項 4 又は 5 に記載の位置認証方法。

**【発明の詳細な説明】**

30

**【技術分野】****【0001】**

本発明は、携帯端末を用いて個人認証を行う位置認証システムに関する。

**【背景技術】****【0002】**

ネットワークを介したサービスでは、個人認証は必須である。ID、パスワードなどのほかに、指紋や静脈パターンなどの技術も実用化されている。複数の認証要素を使用する多要素認証では、これらの認証技術を組み合わせて使用している。例えば、銀行のATMでは、近年、カード、暗証番号、指紋という組み合わせで利用者を特定するシステムが実用化されている。

40

**【0003】**

多要素認証では、通常、カテゴリーが異なる認証技術を組み合わせることで、より高い信頼性を実現している。ID、パスワードは知識型、指紋や静脈パターンは生体型である。さらに、利用者の位置も、認証要素として使用することができる（例えば、特許文献 1 乃至 4 参照。）。

**【0004】**

位置認証に使用される情報は、地理的な位置、ビル内などの限られたエリアでの位置情報、ネットワークの位置情報などである。地理的な位置、特に限られた位置は、場所そのものと結びついている。これに対し、ネットワークの位置は、IPアドレスで特定されることが多い。

50

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2005-216210号公報

【特許文献2】特開2006-267024号公報

【特許文献3】特開2008-293399号公報

【特許文献4】特開2011-138488号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

位置情報は認証情報のひとつとして有効な情報であるが、個人の行動記録をサービス側に提供することになるため、個人情報漏洩や、自分の位置が知られるという利用者の嫌悪感が問題となっていた。また、IPアドレスでのネットワーク位置認証は、携帯電話のようなモバイル機器では、場所や時刻により変化してしまうため、使用することができない問題がある。

10

【0007】

そこで、本発明は、個人の行動記録をサービス側に提供することなく地理的な認証を行うことが可能な位置認証システムの提供を目的とする。

【課題を解決するための手段】

【0008】

上記目的を達成するために、本願発明の位置認証システムは、位置情報をサービス側に送信するときに、利用者が指定した量（オフセット量）だけ、位置情報をオフセットする。

20

【0009】

本願発明の位置認証システムは、端末装置に搭載され、当該端末装置の位置を取得する位置情報取得部と、前記端末装置に搭載され、前記位置情報取得部の取得した位置を当該端末装置の位置のオフセット情報に基づいて移動させて認証位置を求める認証位置演算部と、前記端末装置に搭載され、前記認証位置演算部の求めた前記認証位置を送信する位置情報送信部と、認証サーバに搭載され、予め登録されている前記端末装置の位置と前記位置情報送信部から送信された前記認証位置とが一致している場合に認証成功と判定する認証部と、を備える。

30

【0010】

本願発明の位置認証システムは、端末装置に搭載され、当該端末装置の位置を取得する位置情報取得部と、前記端末装置に搭載され、当該端末装置の位置のオフセット情報を、前記位置情報取得部の取得した位置と共に送信する位置情報送信部と、認証サーバに搭載され、前記位置情報送信部から送信された位置を前記位置情報送信部から送信されたオフセット情報に基づいて移動させて認証位置を求める認証位置演算部と、前記認証サーバに搭載され、予め登録されている前記端末装置の位置と前記認証位置演算部の求めた認証位置とが一致している場合に認証成功と判定する認証部と、を備える。

【0011】

本願発明の位置認証システムでは、前記オフセット情報は、複数桁の数値であり、前記認証位置演算部は、前記オフセット情報として取得した数値を用いて予め定められた方法で演算することで前記端末装置の位置の移動量を算出し、当該移動量に応じて前記位置情報取得部の取得した位置を移動させてもよい。

40

【0012】

本願発明の位置認証方法は、端末装置の現在位置を取得する位置取得手順と、前記位置取得手順で取得した前記端末装置の位置を、当該端末装置の位置のオフセット情報に基づいて移動させて認証位置を求める認証位置演算手順と、前記認証位置演算手順で求めた前記認証位置を送信する認証位置送信手順と、予め登録されている前記端末装置の位置と前記位置情報送信手順で送信された前記認証位置とが一致している場合に認証成功と判定す

50

る認証手順と、を順に有する。

【0013】

本願発明の位置認証方法は、端末装置の現在位置を取得する位置取得手順と、端末装置の位置のオフセット情報を、前記位置取得手順で取得した位置と共に送信する位置情報送信手順と、前記位置情報送信手順で送信した前記端末装置の位置を前記オフセット情報に基づいて移動させて認証位置を求める認証位置演算手順と、予め登録されている前記端末装置の位置と前記認証位置演算手順で求めた認証位置とが一致している場合に認証成功と判定する認証手順と、を順に有する。

【0014】

本願発明の位置認証方法では、前記オフセット情報は、複数桁の数値であり、前記認証位置演算手順において、前記オフセット情報として取得した数値を用いて予め定められた方法で演算することで前記端末装置の位置の移動量を算出し、当該移動量に応じて前記端末装置の位置を移動させてもよい。

【発明の効果】

【0015】

本発明によれば、個人の行動記録をサービス側に提供することなく地理的な認証を行うことが可能な位置認証システムを提供することができる。

【図面の簡単な説明】

【0016】

【図1】本実施形態に係る位置認証システムの概要を示す。

【図2】本実施形態に係る位置認証の説明図を示す。

【図3】実施形態1に係る位置認証システムの機能ブロックの一例を示す。

【図4】実施形態2に係る位置認証システムの機能ブロックの一例を示す。

【発明を実施するための形態】

【0017】

添付の図面を参照して本発明の実施形態を説明する。以下に説明する実施形態は本発明の実施の例であり、本発明は、以下の実施形態に制限されるものではない。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。

【0018】

図1に、本実施形態に係る位置認証システムの概要を示す。端末装置10は、携帯電話やスマートフォンなどの個人が携帯する移動端末装置である。本発明は、コンテンツサーバ30が端末装置10に提供するインターネットサービスにおいて、サービス利用者の個人認証を行う際に、サービス利用者の端末装置10の位置情報と登録された利用者の位置情報が一致するか否かを用いて認証を行う。端末装置10の位置測定機能を使用して、サービス側の認証サーバ20に端末装置10の位置情報を転送し、認証サーバ20において認証が成功した場合に、コンテンツサーバ30からのサービスを受けることを可能にする。

【0019】

図2に、本実施形態に係る位置認証の説明図を示す。

本実施形態に係る位置認証では、初期登録時に実際の位置 $PP(Rx, Ry)$ とオフセット量 $OS(x, y)$ から求まる認証用の位置情報である認証位置 $PC(Sx, Sy)$ を決めておく。認証位置 $PC(Sx, Sy)$ は、実際の位置 $PP(Rx, Ry)$ からオフセット量 $OS(x, y)$ 移動させた $PC((Rx + x), (Ry + y))$ である。そして、認証サーバ20には、位置 $PP(Rx, Ry)$ は登録せずに、認証位置 $PC(Sx, Sy)$ を参照用の位置 $PR(Sx, Sy)$ として登録する。

【0020】

認証時には、端末装置10は、端末装置10の現在位置 $PP(Rx, Ry)$ を測定するとともに、オフセット量 $OS(x, y)$ を指定する。これにより、端末装置10又は認証サーバ20において認証位置 $PC(Sx, Sy)$ を生成する。このとき、認証位置 $PC(Sx, Sy)$ の生成と同時に現在位置 $PP(Rx, Ry)$ 及びオフセット量 $OS(x, y)$

10

20

30

40

50

$x$  ,  $y$  )を消去する。そして、認証サーバ20は、参照用の位置PR ( $S_x$  ,  $S_y$  )と認証位置PC ( $S_x$  ,  $S_y$  )を照合し、一致していれば認証成功と判定し、一致していなければ認証失敗と判定する。認証サーバ20は、判定結果を端末装置10又はコンテンツサーバ30に通知する。コンテンツサーバ30は、認証サーバ20の判定結果に応じた動作を行う。例えば、認証成功の場合はサービスを提供し、認証失敗の場合はサービスを提供しない。

#### 【0021】

ここで、オフセット量OS ( $x$  ,  $y$  )は、端末装置10の利用者が任意に決定することができることが好ましい。これにより、端末装置10の利用者が指定する任意の位置に認証位置PC ( $(R_x + x)$  ,  $(R_y + y)$  )を設定することができる。

10

#### 【0022】

また、オフセット量OS ( $x$  ,  $y$  )は、 $x$  および  $y$  を直接入力する必要はない。例えば、端末装置10にオフセット量OS ( $x$  ,  $y$  )を導き出すためのパスワードを入力すると、端末装置10がオフセット量OSの具体的な数値である  $x$  及び  $y$  を指定するようにしてもよい。これにより、端末装置10の利用者が  $x$  及び  $y$  を直接覚える必要がないため、利用者の負荷を減らすことができる。このように、端末装置10に指定するオフセット量OS ( $x$  ,  $y$  )は数値に限らないため、以下の説明においては、オフセット量OS ( $x$  ,  $y$  )をオフセット情報OSと呼ぶ。

#### 【0023】

このように、本発明は、利用者の現実の位置とは異なる認証位置を用いて位置認証を行うため、位置情報という個人情報漏洩せず、かつ自分の位置が知られるという利用者の嫌悪感も低減することが可能である。また、本発明は、現実の位置を用いた位置認証であるため、ある限られたエリアにいる利用者に対してサービスを提供する場合の位置認証にも用いることができる。

20

#### 【0024】

なお、認証サーバ20側において、オフセットされた位置情報しか保存できない構成をとることが好ましい。これにより、利用者の位置情報漏洩への嫌悪感を和らげ、さらにオフセット量は利用者しか知りえないパスワードのような情報とすることができる。

#### 【0025】

また、サービス側において、オフセット情報を保存してもよい。この場合は、オフセット情報を用いて現在位置PPを逆算できないよう、オフセット情報からオフセット量への変換に利用者ごとに異なる演算方法を用いたり、参照用の位置PRをぼかしたりすることが好ましい。

30

オフセット情報からオフセット量への変換に利用者ごとに異なる演算方法を用いる場合、認証サーバ20はオフセット情報及び演算方法を記憶する。演算方法の詳細については実施形態4において説明する。オフセット量の秘匿性を維持するために、演算方法は認証サーバ20が自動的に決定し、オフセット情報とは別に記憶しておくことが好ましい。

参照用の位置PRをぼかす場合、認証サーバ20はオフセット情報及びぼかし量を記憶する。参照用の位置PRのぼかしは、例えば、ランダムな誤差を位置に付加したり、四捨五入、切捨て又は切り上げを行うことで、丸め誤差を位置に付加したりする。ぼかし量は認証サーバ20が自動的に決定してもよいし、利用者が決定してもよい。ぼかし量についても、オフセット量の秘匿性を維持するために、オフセット情報とは別に記憶しておくことが好ましい。

40

#### 【0026】

本実施形態では、発明の把握が容易になるように、位置認証の位置が1つの場合についてのみ説明するが、位置認証の位置は2以上であってもよい。2以上にすることで、認証精度を高めることができる。この場合は、全てのオフセット情報OSを利用者が記憶しておくことは利用者の負担となるため、認証サーバ20側においてオフセット情報OSを保管することが好ましい。この場合は、共通のパスワードを用いて、位置情報ごとに異なる演算を用いてオフセット情報を算出するようにする。これにより、認証位置を実際の位置

50

とは異なるランダムな位置にしつつ、利用者の入力すべきパスワードとしてのオフセット情報を共通化することができる。

【 0 0 2 7 】

非常に価値のあるコンテンツや限られた利用者には公開されないようなコンテンツを、ネットワークを介して提供するようなサービスでは、利用者の厳密な認証が不可欠である。このような認証では、複数の要素を使用する多要素認証が使用される。パスワードのような知識認証に加えて、コンテンツを閲覧、利用できる場所を限定することは、違法なコピーや改ざんを防止するために非常に有効である。例えば、病院でのカルテ管理、大学内に限定されているアプリケーションの実行など、IDやパスワードを盗まれても、登録された場所以外では、コンテンツを利用できないようなシステムを構築することができる。

10

【 0 0 2 8 】

(実施形態1)

図3に、本実施形態に係る位置認証システムの一例を示す。本実施形態では、端末装置10が位置情報送信部11、位置情報取得部12、オフセット取得部13及び認証位置演算部14を備え、認証サーバ20が位置情報受信部21及び認証部22を備える。

【 0 0 2 9 】

本実施形態に係る位置認証方法は、位置取得手順と、認証位置演算手順と、位置情報送信手順と、認証手順と、を順に有する。位置取得手順の前に、参照用の位置PRを認証サーバ20に登録する。

20

【 0 0 3 0 】

位置取得手順では、位置情報取得部12が、端末装置10の現在位置PPを取得する。このとき、オフセット取得部13が、オフセット情報OSを取得する。

認証位置演算手順では、認証位置演算部14が、位置情報取得部12の取得した位置Pをオフセット情報OSに基づいて移動させて認証位置PCを求める。

位置情報送信手順では、位置情報送信部11が、認証位置演算部14の求めた認証位置PCを送信する。すると、位置情報受信部21が、位置情報送信部11の送信した認証位置PCを受信する。

認証手順では、認証部22が、予め登録されている端末装置10の位置PRと位置情報送信部11から送信された認証位置PCとが一致しているか否かを判定し、判定結果を端末装置10又はコンテンツサーバ30に通知する。コンテンツサーバ30は、認証サーバ20の判定結果に応じた動作を行う。

30

【 0 0 3 1 】

位置情報取得部12の測位方法は任意であり、GPS(Global Positioning System)を用いてもよいし、無線基地局を用いた測位方法であってもよい。

【 0 0 3 2 】

オフセット取得部13は、端末装置10の利用者によって入力された情報を取得してもよいし、予め定められた記憶部(不図示)からオフセット情報OSを読み出してもよいし、端末装置10の利用者によって入力された情報を予め定められた方法で算出することによって求めてもよい。

40

【 0 0 3 3 】

本実施形態では、端末装置10において認証位置PCを求めるため、認証サーバ20に対して端末装置10の実際の位置を完全に秘匿にすることができる。このため、認証サーバ20から利用者の行動記録が漏洩することに対する利用者の安心感を得ることができる。

【 0 0 3 4 】

(実施形態2)

図4に、本実施形態に係る位置認証システムの一例を示す。本実施形態では、端末装置10が位置情報送信部11、位置情報取得部12及びオフセット取得部13を備え、認証

50

サーバ 20 が位置情報受信部 21、認証位置演算部 24 及び認証部 22 を備える。

【0035】

本実施形態に係る位置認証方法は、位置取得手順と、位置情報送信手順と、認証位置演算手順と、認証手順と、を順に有する。位置取得手順の前に、参照用の位置 PR を認証サーバ 20 に登録する。

【0036】

位置取得手順では、位置情報取得部 12 が、端末装置 10 の現在位置 PP を取得する。このとき、オフセット取得部 13 が、オフセット情報 OS を取得する。

位置情報送信手順では、位置情報送信部 11 が、オフセット取得部 13 の取得したオフセット情報 OS と位置情報取得部 12 の取得した位置 PP を、認証サーバ 10 に送信する。すると、位置情報受信部 21 が、位置情報送信部 11 の送信したオフセット情報 OS 及び位置 PP を受信する。

認証位置演算手順では、認証位置演算部 24 が、位置情報受信部 21 の受信したオフセット情報 OS 及び位置 PP を用いて認証位置 PC を求め、オフセット情報 OS 及び位置 PP を即座に消去する。

認証手順では、認証部 22 が、予め登録されている端末装置 10 の位置 PR と認証位置演算部 24 の求めた認証位置 PC とが一致しているか否かを判定し、判定結果を端末装置 10 又はコンテンツサーバ 30 に通知する。コンテンツサーバ 30 は、認証サーバ 20 の判定結果に応じた動作を行う。

【0037】

本実施形態では、認証サーバ 20 において認証位置 PC を求めるため、端末装置 10 における処理負荷を軽減することができる。また、利用者は端末装置 10 にオフセット量である  $x$  及び  $y$  を求めるためのオフセット情報 OS を入力すればよいため、利用者の負荷も軽減することができる。

【0038】

(実施形態 3)

本実施形態では、オフセット量  $x$  及び  $y$  について説明する。

位置情報取得部 12 の測定した位置 PP は誤差を有するため、認証部 22 は、認証位置 PC と予め定められた位置 PR とが誤差の範囲で一致している場合に「一致」と判定する。このため、実際の位置 PP からの誤差  $\Delta$  を求め、実際の位置情報 PP と差別化できるように、オフセット量である  $x$  及び  $y$  は、位置 PP の誤差よりも大きい必要がある。すなわち、

$$x > \Delta \quad \text{かつ} \quad y > \Delta$$

にする。

【0039】

ここで、従来であれば、認証部 22 において一致と判定する誤差を小さくしてしまうと、利用者の詳細な現在位置を認証サーバ 20 に登録することになってしまっていた。しかし、本発明では、認証部 22 において一致と判定する誤差を小さくしても、利用者の実際の現在位置を認証サーバ 20 に登録することにはならない。このため、本発明では、認証部 22 において一致と判定する誤差を、位置情報取得部 12 で用いる測位方法の精度と同程度にまで小さくすることができる。これにより、本発明は、従来の位置認証に比べて、認証精度を高めることができる。

【0040】

実際の位置 PP の誤差  $\Delta$  は、住所と比較することで得られる。例えば、位置認証を行う現在位置 PP を自宅にする場合、自宅における緯度及び経度を位置情報取得部 12 で取得し、自宅住所の緯度及び経度を調べる。位置情報取得部 12 で取得した緯度及び経度と自宅住所の緯度及び経度を用いて、実際の位置 PP からの誤差  $\Delta$  を求めることができる。同様の誤差  $\Delta$  の測定を、位置認証を行いたい各位置において行う。

【0041】

また、実際の位置 PP の誤差  $\Delta$  は、現在位置 PP を複数回測定し、ばらつきの分散  $\sigma$  を

10

20

30

40

50

求めてもよい。この場合、オフセット量  $x$  及び  $y$  をばらつき よりも十分に大きい値にする。すなわち、

$$x \gg \quad \text{かつ} \quad y \gg$$

にする。

#### 【0042】

(実施形態4)

本実施形態では、オフセット情報OSとして、位置情報認証用のパスワードを用いる例について説明する。位置情報認証用のパスワードは、数字、文字若しくは記号又はこれらの組み合わせを用いることができる。これらのパスワードを用いて、オフセット量の  $x$  と  $y$  を求める。

10

#### 【0043】

パスワードは、例えば、4桁などの複数桁の数値を使用することができる。この場合、パスワードの数値を、加算、減算、積算又は除算などの演算処理することによって、オフセット量の  $x$  と  $y$  を求める。例えば、パスワードとして「 $e_1 e_2 e_3 e_4$ 」の4桁の十進数を用いた場合、上位2桁「 $e_1 e_2$ 」をオフセット  $x$  に用い、下位2桁「 $e_3 e_4$ 」をオフセット  $y$  に用いる。「 $e_1 e_2$ 」と「 $e_3 e_4$ 」は、それぞれ00~99までの2桁の数値をとりうる。 $x$  と  $y$  は、「 $e_1 e_2$ 」と「 $e_3 e_4$ 」をそのまま利用してもよいが、さらに演算を行ってもよい。例えば、「 $e_1 e_2$ 」から49を引いた数値を  $x$  にし、「 $e_3 e_4$ 」から49を引いた数値を  $y$  にして、 $x$  と  $y$  を  $-49 \sim +10$  までの数値にする。

20

#### 【0044】

位置情報が、緯度及び経度のそれぞれについて、度( $d_1 d_2$ )、分( $m_1 m_2$ )、秒( $s_1 s_2$ )で表されているとする。この場合、位置情報の精度を考慮して、分の10の位( $m_1$ )をオフセットしないと、実際の位置PPと差別化できないので、分( $m_1 m_2$ )にオフセットを行う。そのため、 $x$  と  $y$  は、 $-49 \sim +10$  までの数値のうち、 $-09 \sim +09$  を禁止する。 $x$  と  $y$  が  $-09 \sim +09$  になる場合、認証位置演算部14又は24は、別のパスワードの再入力を要求する。

#### 【0045】

パスワードとして、MD5のようなハッシュ関数を使用してもよい。MD5の場合、16バイトのデータが得られる。16バイトのデータを8バイトずつに分け、それぞれを緯度のオフセット  $x$  及び経度のオフセット  $y$  にする。例えば、パスワードが「1234」の場合、MD5の値は「81dc9bdb52d04dc20036dbd8313ed055」となる。このうちの先頭の8バイト「81dc9bdb52d04dc2」を  $x$  に用い、後半の8バイト「0036dbd8313ed055」を  $y$  に用いる。 $x$  のうちの上位4バイト「81dc9bdb」を10進数に変換すると「2178718683」となるので、この数値の上位2桁「21」を  $x$  とする。 $y$  のうちの上位4バイト「0036dbd8」を10進数に変換すると「3595224」となるので、この数値の上位2桁「35」を  $y$  とする。

30

#### 【0046】

ここで、上位2桁の数値が「00」~「09」のように「0」から始まるときは、上位2桁目と3桁目をういたり、上位3桁目と4桁目をういたりするなど、使用する桁を変更してもよい。それでも連続する2桁が「00」~「09」になる場合は、パスワードの再入力を要求することが好ましい。使用する桁を変更する場合は、認証位置演算部14又は24は、使用する桁を記憶する。

40

#### 【産業上の利用可能性】

#### 【0047】

本発明は情報通信産業に適用することができる。

#### 【符号の説明】

#### 【0048】

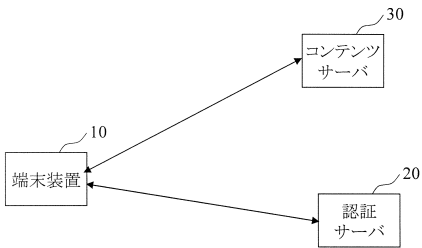
10：端末装置

50

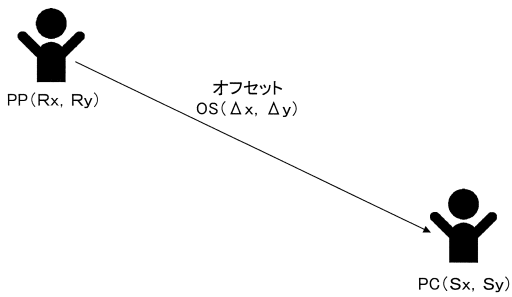


- 1 1 : 位置情報送信部
- 1 2 : 位置情報取得部
- 1 3 : オフセット取得部
- 1 4 : 認証位置演算部
- 2 0 : 認証サーバ
- 2 1 : 位置情報受信部
- 2 2 : 認証部
- 2 4 : 認証位置演算部
- 3 0 : コンテンツサーバ

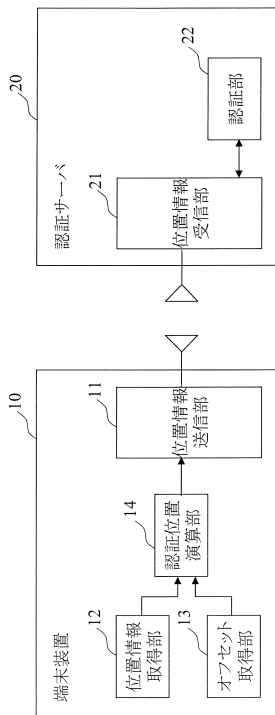
【図 1】



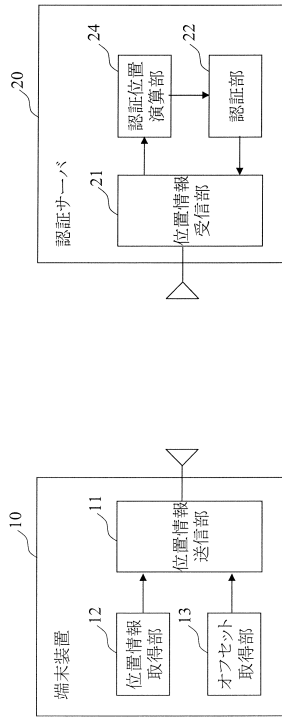
【図 2】



【図 3】



【図4】



---

フロントページの続き

- (56)参考文献 特開2007-286879(JP,A)  
特開2002-314477(JP,A)  
特開2002-007931(JP,A)  
特開2000-163379(JP,A)

- (58)調査した分野(Int.Cl., DB名)  
G06F21/30 - G06F21/46