(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4635182号
(P4635182)

(45)発行日　平成23年2月16日(2011.2.16)　(24)登録日　平成22年12月3日(2010.12.3)

(51)Int.Cl.		F I		
H04W 12/04	(2009.01)	H04Q	7/00	182
H04W 64/00	(2009.01)	H04Q	7/00	502
H04W 12/06	(2009.01)	H04Q	7/00	183
H04L 9/32	(2006.01)	H04L	9/00	673A
H04L 9/08	(2006.01)	H04L	9/00	601C

請求項の数 5　(全 11 頁)

(21)出願番号　特願2005-271145(P2005-271145)
(22)出願日　平成17年9月16日(2005.9.16)
(65)公開番号　特開2007-88514(P2007-88514A)
(43)公開日　平成19年4月5日(2007.4.5)
審査請求日　平成20年7月25日(2008.7.25)

(73)特許権者　301022471
独立行政法人情報通信研究機構
東京都小金井市貫井北町４－２－１
(74)代理人　100130111
弁理士　新保　斉
(72)発明者　黒田　正博
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内

審査官　深津　始

最終頁に続く

(54)【発明の名称】無線通信システム

(57)【特許請求の範囲】
【請求項１】
無線の種類に依存しない複数のアクセスポイント間を移動する移動端末と、各アクセスポイントとの間で相互に認証可能な無線通信システムであって、
アクセスポイントが、
移動端末と暗号化通信する暗号化通信手段と、
該移動端末の位置情報を取得する移動端末位置取得手段と、
該移動端末の位置情報に係るデータの履歴を１個格納できる記憶領域が所定の個数集合した位置履歴記憶媒体と、
該位置履歴記憶媒体における任意の記憶領域のポインタを設定するポインタ設定処理手段と、
該位置履歴記憶媒体に含まれるいずれかのデータを少なくとも用いて暗号鍵を生成する暗号鍵生成処理手段と、
移動端末の認証を行う認証処理手段と
を備える一方、
移動端末が、
アクセスポイントと暗号化通信する暗号化通信手段と、
該移動端末の位置情報を取得する移動端末位置取得手段と、
該移動端末の位置情報に係るデータの履歴を１個格納できる記憶領域が所定の個数集合した位置履歴記憶媒体と、

該位置履歴記憶媒体における任意の記憶領域のポインタを設定するポインタ設定処理手段と、
該位置履歴記憶媒体に含まれるいずれかのデータを少なくとも用いて暗号鍵を生成する暗号鍵生成処理手段と、
アクセスポイントの認証を行う認証処理手段と
を備え、
アクセスポイントの暗号鍵生成処理手段が、ポインタ設定処理手段が選択した位置履歴記憶媒体中のデータから暗号鍵を生成すると共に、暗号化通信処理手段において該暗号鍵を用いて暗号化して移動端末にメッセージを送信し、
移動端末において位置履歴記憶媒体中のデータから暗号鍵生成処理手段が順次暗号鍵を生成して該メッセージの復号化を試行し、いずれかのデータから生成した暗号鍵で復号化に成功した場合に、認証処理手段がアクセスポイントの認証を行う
ことを特徴とする無線通信システム。

【請求項２】
前記無線通信システムにおいて、
移動端末の認証処理手段がアクセスポイントの認証を行った後に、
該認証時における移動端末の位置情報に係るデータを、復号化に成功したデータが格納されている記憶領域に書き換えて格納し、
暗号鍵生成処理手段が該データから暗号鍵を生成し、該暗号鍵を用いて少なくともアクセスポイントから受信した情報を含めて暗号化したメッセージを暗号化通信手段がアクセスポイントに送信する一方、
アクセスポイントにおいて先に暗号鍵を生成したデータが格納されていた記憶領域に、該認証時における移動端末の位置情報に係るデータを書き換えて格納し、暗号鍵生成処理手段が該データから暗号鍵を生成し、該暗号鍵を用いて移動端末から受信したメッセージの復号化を試行し、復号化成功すると共に含まれていた情報が先に移動端末に送信した情報と一致する場合に、認証処理手段が移動端末の認証を行う
ことを特徴とする請求項１に記載の無線通信システム。

【請求項３】
前記移動端末が固有の乱数を備え、
暗号化通信手段から送信するメッセージが、該乱数を含めて暗号化される
請求項１又は２に記載の無線通信システム。

【請求項４】
前記アクセスポイントが送信したメッセージに含まれる情報が、
アクセスポイントに備えた固有の乱数である
請求項２又は３に記載の無線通信システム。

【請求項５】
前記移動端末及びアクセスポイントに演算処理手段を備え、
前記位置情報に係るデータが、移動端末位置取得手段において取得された位置情報と、前記各々の乱数を用い、鍵付ハッシュ関数による演算処理された値である
請求項３又は４に記載の無線通信システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は移動端末と無線の種類に依存しない複数のアクセスポイント（基地局）からなる無線通信システムに関し、特に移動端末とアクセスポイント間の認証方法に係る技術である。

【背景技術】
【０００２】
モバイルネットワークでの移動端末の認証方式は、基本的には有線ネットワークの認証方式と何ら変わりはなく、お互いにしか知りえない情報を共有し、お互いが、相手がその

情報を知っているということを確認することにより、実現されている。
例えばIEEE802.11（非特許文献１参照）では、MDとネットワーク(AP)が事前に鍵を共有する手段をとる。しかしこの方式では、事前のネゴシエーション時に鍵が漏洩する可能性がある。
【０００３】
【非特許文献１】"IEEE 802.11 Wireless LANMedium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE, 1999
【０００４】
より高度なIEEE802.1X*ではEAPによる認証が提案されている。EAPの認証はTLS、PEAP、TTLSなどの様々な方法が提案されているが、それらは公開鍵認証基盤を用いている。これには認証局(CA)の構築・管理が必要となると共に、移動端末のユーザにも余計な手続きを要求することになる。
【０００５】
事前鍵共有を用いない方式としてDH鍵共有方式がある。移動端末とネットワーク間で、DH方式により共通鍵を共有しておき、それを用いてID等を交換することで認証が可能である。しかしながら、DH方式は大きな計算量を必要とする。この認証方式では認証の成否に関らず膨大なDH計算を実施する必要があるため、移動端末ないしはネットワークの負荷を増大することになる。
【０００６】
また別な認証方法として、ユーザの位置により認証を行う方法が知られている。特許文献１に開示される技術は、端末の位置を認証データベースに記録しておき、端末がその記録された範囲内に存在する場合に認証を行う構成である。
しかし、この方法ではその範囲内にさえ入れば端末の認証が行えるのであるから、端末の固有性を確認できるほどに十分な認証を行っているとはいえない。
【０００７】
【特許文献１】特開2005-050150号公報
【発明の開示】
【発明が解決しようとする課題】
【０００８】
本発明は、上記従来技術の有する問題点に鑑みて創出されたものであり、簡便かつ強固なセキュリティを有する無線通信システムにおける認証方法を提供することを目的とする。
【課題を解決するための手段】
【０００９】
本発明は、上記の課題を解決するために、次のような無線通信システムを提供する。
すなわち、本発明は無線の種類に依存しない複数のアクセスポイント間を移動する移動端末と、各アクセスポイントとの間で相互に認証可能な無線通信システムを構成する。
該システムにおけるアクセスポイントが、移動端末と暗号化通信する暗号化通信手段と、該移動端末の位置情報を取得する移動端末位置取得手段と、該移動端末の位置情報に係るデータの履歴を１個格納できる記憶領域が所定の個数集合した位置履歴記憶媒体と、該位置履歴記憶媒体における任意の記憶領域のポインタを設定するポインタ設定処理手段と、該位置履歴記憶媒体に含まれるいずれかのデータを少なくとも用いて暗号鍵を生成する暗号鍵生成処理手段と、移動端末の認証を行う認証処理手段とを備える。
【００１０】
一方、移動端末が、アクセスポイントと暗号化通信する暗号化通信手段と、該移動端末の位置情報を取得する移動端末位置取得手段と、該移動端末の位置情報に係るデータの履歴を１個格納できる記憶領域が所定の個数集合した位置履歴記憶媒体と、該位置履歴記憶媒体における任意の記憶領域のポインタを設定するポインタ設定処理手段と、該位置履歴記憶媒体に含まれるいずれかのデータを少なくとも用いて暗号鍵を生成する暗号鍵生成処理手段と、アクセスポイントの認証を行う認証処理手段とを備える。

【００１１】
そして、アクセスポイントの暗号鍵生成処理手段が、ポインタ設定処理手段が選択した位置履歴記憶媒体中のデータから暗号鍵を生成すると共に、暗号化通信処理手段において該暗号鍵を用いて暗号化して移動端末にメッセージを送信する。
移動端末においては、位置履歴記憶媒体中のデータから暗号鍵生成処理手段が順次暗号鍵を生成して該メッセージの復号化を試行し、いずれかのデータから生成した暗号鍵で復号化に成功した場合に、認証処理手段がアクセスポイントの認証を行う。
【００１２】
請求項２に記載の発明は、前記の無線通信システムにおいて、移動端末の認証処理手段がアクセスポイントの認証を行った後に、該認証時における移動端末の位置情報に係るデータを、復号化に成功したデータが格納されている記憶領域に書き換えて格納し、暗号鍵生成処理手段が該データから暗号鍵を生成する。該暗号鍵を用いて少なくともアクセスポイントから受信した情報を含めて暗号化したメッセージを暗号化通信手段がアクセスポイントに送信する。
【００１３】
一方、アクセスポイントにおいて先に暗号鍵を生成したデータが格納されていた記憶領域に、該認証時における移動端末の位置情報に係るデータを書き換えて格納し、暗号鍵生成処理手段が該データから暗号鍵を生成し、該暗号鍵を用いて移動端末から受信したメッセージの復号化を試行し、復号化成功すると共に含まれていた情報が先に移動端末に送信した情報と一致する場合に、認証処理手段が移動端末の認証を行う。
【００１４】
請求項３に記載の発明は、移動端末が固有の乱数を備え、暗号化通信手段から送信するメッセージが、該乱数を含めて暗号化されることを特徴とするものである。
請求項４に記載の発明は、アクセスポイントが送信したメッセージに含まれる情報が、アクセスポイントに備えた固有の乱数であることを特徴とする。
【００１５】
請求項５に記載の発明は、移動端末及びアクセスポイントに演算処理手段を備え、位置情報に係るデータが、移動端末位置取得手段において取得された位置情報と、前記各々の乱数を用い、鍵付ハッシュ関数による演算処理された値である構成を提供する。
【発明の効果】
【００２１】
本発明は、端末の位置情報を認証時の共通鍵として利用することを提案するものである。端末の位置情報は複数のアクセスポイント間を通過する間にその履歴を位置履歴記憶媒体内に格納し、他人が全く同じ位置履歴を持つようにすることは困難である。
このような特徴を活かして、限られたデータ容量でも従来方式と同等以上の暗号強度を持たせる事ができる。位置情報を利用することで簡便に共通鍵を持つことができ、その履歴の中から選択するだけの処理であるため、鍵の変換に要する計算量を極めて低く抑えることができる。
【発明を実施するための最良の形態】
【００２２】
以下、本発明の実施形態を、図面に示す実施例を基に説明する。なお、実施形態は下記に限定されるものではない。
図１は本発明システムの全体概要を説明する図である。ネットワーク（１）には複数のアクセスポイント（２）が接続され、移動端末（３）はさまざまな経路で移動しながらいくつかのアクセスポイント（２）と通信を行う。
通信するアクセスポイント（２）は移動の経路や電波状況によって異なり、全く同じ経路を通ったとしても変化することがある。
なお、本発明のアクセスポイントは、一般に基地局と呼ばれることがあり、同義で用いている。
【００２３】

図２は本発明に係るアクセスポイントの構成図である。アクセスポイントとしては、ネットワークとの接続に特化したアクセスポイント装置の他、公知のパーソナルコンピュータを用いることができる。

そして、ＣＰＵ（２０）には、暗号化通信部（２０１）、鍵生成処理部（２０２）、ハッシュ関数演算処理部（２０３）、ポインタ設定処理部（２０４）、位置情報取得部（２０５）、認証処理部（２０６）の各処理部が設けられる。

【００２４】

ＣＰＵ（２０）とはネットワークカード（２１）が接続されて移動端末（３）との通信を行う他、メモリ領域あるいはハードディスク内の記憶領域として、本発明に係るキャロセル型記憶領域（２２）が設けられている。

【００２５】

図２は本発明に係るアクセスポイントの構成図である。移動端末には公知の携帯電話端末やＰＤＡ、パーソナルコンピュータを用いることができる。

ＣＰＵ（３０）には、暗号化通信部（３０１）、鍵生成処理部（３０２）、ハッシュ関数演算処理部（３０３）、ポインタ設定処理部（３０４）、位置情報取得部（３０５）、認証処理部（３０６）の各処理部が設けられる。

【００２６】

ＣＰＵ（３０）とはネットワークアダプタ（３１）が接続されてアクセスポイント（２）との通信を行う他、メモリ領域あるいはハードディスク内の記憶領域として、本発明に係るキャロセル型記憶領域（３２）が設けられている。

【００２７】

キャロセル型記憶領域（２２）（３２）の構成について図４を用いて説述する。キャロセルとは空港などに設けられている荷物を循環的に運搬する装置である。本発明では記憶領域を概念的にはキャロセルのように利用することからキャロセル型記憶領域と呼んでいる。

【００２８】

全体しては環状（４０）にデータが配置されていると理解することができ、環状の中を複数の記憶領域であるセル（４１）（４２）（４３）・・に分割されている。各セルには移動端末（３）の位置情報に係るデータが１個ずつ格納される。

環状であるためにセル（４２）からセル（４３）方向に１つずつデータを確認して行ったとき、最後にセル（４１）に到達し、１周して全てのデータを確認することができる。

【００２９】

実際には、メモリ内の物理的アドレスの終点から始点に戻るような処理を行うことでこのような概念が実現される。本処理は単にアドレスを示すポインタを移動させるだけであるから、計算処理上極めて単純な処理である。

ＣＰＵのポインタ設定処理部（２０４）（３０４）はランダムに、あるいは順に次のセルを示すようにポインタを設定することができる。

【００３０】

このようなキャロセル型記憶領域の内容は、アクセスポイント（２）と移動端末（３）の間で常に一致させている。基本的には後述する処理の中でアクセスポイント（２）と移動端末（３）のデータは一致するが、アクセスポイントの移動に伴って相違した場合には、暗号化通信が確立した状態で移動端末（３）からアクセスポイント（２）に対して同期を行う。

また、ネットワーク（１）に接続されたアクセスポイント（２）間では、周知のデータ交換技術により、当該移動端末に関するデータはすべて同期されている。

従って移動端末と、全てのアクセスポイントにおけるキャロセル型記憶領域（２２）（３２）内のデータは一致している状態である。

【００３１】

キャロセル型記憶領域にはポインタ設定処理部（３０４）により一つのエントリポイント（４４）を持ち、エントリポイントがさしているセルに対してのみ位置情報を格納する

操作が可能である。位置情報を格納する前には、ポインタ設定処理部（３０４）がエントリポイント（４４）を自由に移動することができる。新しい位置情報を格納する場合、もしそのセルに古い位置情報が格納されていればその情報は廃棄され新しい位置情報で置き換えられる。

【００３２】

１基の移動端末には１つのキャロセル型記憶領域を持つ。このキャロセル型記憶領域の中の各セルには、そのモバイル端末が移動してきた位置情報が入っているので、キャロセル型記憶領域全体（４０）でその移動端末の移動履歴情報と考えることが出来る。

【００３３】

次に、移動端末及びアクセスポイントのＣＰＵにおける各処理部の作用を説述する。

まず鍵生成処理部（２０２）（３０２）における鍵生成機能は、１つのセルに含まれるデータから暗号鍵を生成する機能である。同じキャロセルからは同じ暗号鍵が生成される。

暗号化通信部（２０１）（３０１）における暗号化通信機能は、鍵生成処理部位（２０２）（３０２）で生成された暗号鍵を利用して、互いに暗号化通信を実施するための機能である。

【００３４】

認証処理部（２０６）（３０６）における認証機能は、これら鍵生成機能と暗号化通信機能を用いて相互認証を行うための機能である。暗号化通信機能によって互いにやりとりしたパケットが互いの持つ暗号鍵で暗号化・復号が可能であれば、それはお互いが同じ暗号鍵を持っていることを示している。これによって相互認証を行う。

【００３５】

位置情報取得部（２０５）（３０５）における位置情報取得機能は、移動端末がアクセスポイントと相互認証を開始した時点の位置情報を取得する機能である。本実施例においては位置情報としてアクセスポイントのＭＡＣアドレスを用いることができ、その場合移動端末（３）はアクセスポイントとの通信により位置情報を取得する。アクセスポイント（２）は通信中の移動端末（３）の位置情報につき、自己のＭＡＣアドレスを位置情報として取得すればよい。

【００３６】

近年、移動端末（３）にＧＰＳ機能を備えたものがあり、衛星測位による移動端末の位置情報を移動端末が直接取得してもよい。本構成のためにはＧＰＳレシーバ等の公知の受信機が必要である。取得した測位情報は、暗号化通信によりアクセスポイントに伝達される。

【００３７】

ハッシュ関数演算処理部（２０３）（３０３）は、図示しない乱数発生部により発生した移動端末又はアクセスポイント固有の乱数を用い、上記位置情報と共にハッシュ関数を用いた演算を行う。数１に示されるように、ハッシュ関数に対して鍵生成処理部で生成された鍵、位置情報、乱数を入力し、格納するデータPOSDATAを得る。

一方向ハッシュ関数については公知であり、演算方法も既存の方法を用いることができる。

【００３８】

（数１）

$$POSDATA = h(K, POS \,||\, Rand_{ap})$$

上記の式においてｈ（）はハッシュ関数、Kは鍵、POSは位置情報取得部（２０５）（３０５）で取得した位置情報、$Rand_{ap}$はアクセスポイントにおける乱数（移動端末の乱数は異なる）である。

【００３９】

次に、通信端末（３）とアクセスポイント（２）の認証プロトコルにつき、説述する。図５は本発明にかかる認証プロトコルのシーケンス図である。

まず、移動端末（３）が通信中のアクセスポイント（２）と異なるアクセスポイント（２）と通信を開始するとき、認証要求（Ｓ１）を送出する。

【００４０】

認証要求（Ｓ１）を受信したアクセスポイントは、位置情報取得部（２０５）で通信端末（３）の位置情報を取得し、次いでポインタ設定処理部（２０４）がランダムにキャロセル型記憶領域のいずれかのセルを選択する。概念的には、ルーレットのようにキャロセルを適当に回転させ、停止した位置にポインタを設定することになる。

そして、当該ポインタの位置に格納されたデータを用いて鍵を生成する。

【００４１】

次の回転要求Ｓ２では、ハッシュ関数演算で用いたアクセスポイントの乱数R_NとMAC_N（メッセージから生成されたメッセージ認証コード）を暗号化して回転要求メッセージを作成し移動端末（３）に送付する。

より具体的には次式によりメッセージを送付する。

【００４２】

（数２）

$N \rightarrow M$： $RotateREQ([R_n||MAC_N]K_N)$

ここで、M をモバイル端末、Nをアクセスポイントとする。R_M と R_N はそれぞれMとNによって選定された乱数値。$[X]_K$は平分Xを鍵Kで暗号化したもの。MAC はメッセージから生成されたメッセージ認証コード。T(B) はBをボディにもつメッセージT。以下同じ。

【００４３】

回転要求Ｓ２を受け取った移動端末は、まず位置情報取得部（３０５）で自端末の位置情報を取得し、キャロセル型記憶領域（３２）の現在のポインタのセルからデータを読み出し、鍵生成処理部（３０２）で鍵を生成し、受信したメッセージの復号化を試みる。復号した平文からの認証コードとMAC_Nが合致すれば、その鍵は正しい、すなわちキャロセルが同期していることを示す。

【００４４】

その場合には、認証処理部（３０６）がアクセスポイントを認証し、次のステップに進む。

合致しなければ、ポインタ設定処理部（３０４）が１つ隣のセルにポインタを移動させ、そのデータを用いて試行を繰り返す。１周してもいずれも一致しなければキャロセルが同期していないことになり、認証処理部（３０６）は認証失敗と判断し、通信を切断する。

【００４５】

アクセスポイントの認証が成功すると、まず現在のポインタ位置、すなわち復号化に成功した時のセルに対して、現在の位置情報をハッシュ関数演算処理部（３０３）で演算した結果を書き込む。この処理により、アクセスポイントのキャロセル型記憶領域と内容が一致するように更新される。

そして、回転応答をアクセスポイントに対して返す（Ｓ３）。

【００４６】

その際、書き込んだデータから鍵生成処理部（３０２）が新しい鍵を作成し、受信したR_Nとハッシュ関数演算処理部（３０３）で用いた乱数R_M、そこから作成したMAC_M（メッセージから生成されたメッセージ認証コード）を暗号化し、RotateREPメッセージとして返す。

本処理は次式により表される

【００４７】

（数３）

$M \rightarrow N$： $RotateREP([R_N||R_M||MAC_M]K_{M'})$

【００４８】

アクセスポイント（３）は回転応答（Ｓ３）を受信すると、まず先ほど位置情報取得部

（２０５）で得られた位置情報をハッシュ関数演算処理部（２０３）で演算し、その結果をポインタのあるセルに対して書き込みする。すでに先ほど用いた前のデータがあるのでそれを書き換えする。

さらに、鍵生成処理部においてその書き込んだデータを用いて鍵を生成する。

【００４９】

生成された鍵を用いると、それは移動端末で暗号化に用いた鍵と共通であるから、回転応答（Ｓ３）のメッセージが復号化できる。平文から生成した認証コードとMAC_Mが合致し、かつR_Nが正しければ、通信端末の認証は成功となる。

通信端末に対して、R_MとMAC_Mをその鍵で暗号化したメッセージAuthREPを認証応答Ｓ４として送信する。

【００５０】

本発明は以上により終了してもよいが、認証応答Ｓ４において新たな乱数を加えて暗号化し、通信端末に送信してもよい。通信端末では再び現在のポインタのデータから鍵を生成し、その新しい乱数を抽出した上で認証応答Ｓ５として返信することもできる。

【００５１】

最後に、図６は本発明におけるキャロセル型記憶領域のセル数と、暗号強度の関係をシミュレーションした結果である。

グラフによると、１２８ビットの暗号化と同等以上の暗号強度を得るために、する数が３５個以上を用いればよいことがわかり、同時に３５個ないし４０個程度のセル数で十分であることが分かる。セル数が多いと認証処理に時間を要するため、上記範囲程度とするのが適当である。

【図面の簡単な説明】

【００５２】

【図１】本発明の無線通信システムの全体構成図である。

【図２】本発明のアクセスポイントの構成図である。

【図３】本発明の移動端末の構成図である。

【図４】本発明に係るキャロセル型記憶領域の概念を説明する図である。

【図５】本発明に係る認証処理のシーケンス図である。

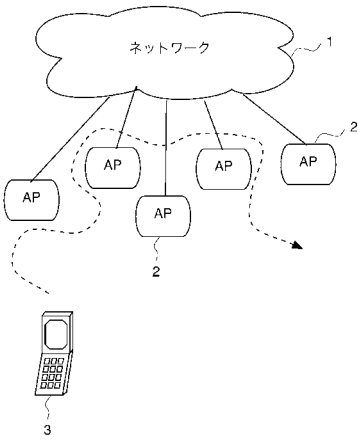
【図６】本発明の技術に係るシミュレーション結果である。

【符号の説明】

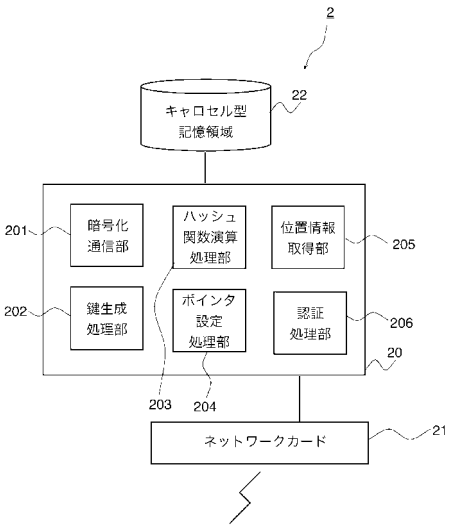
【００５３】

３　　移動端末
３０　　ＣＰＵ
３０１　　暗号化通信部
３０２　　鍵生成処理部
３０３　　ハッシュ関数演算処理部
３０４　　ポインタ設定処理部
３０５　　位置情報取得部
３０６　　認証処理部

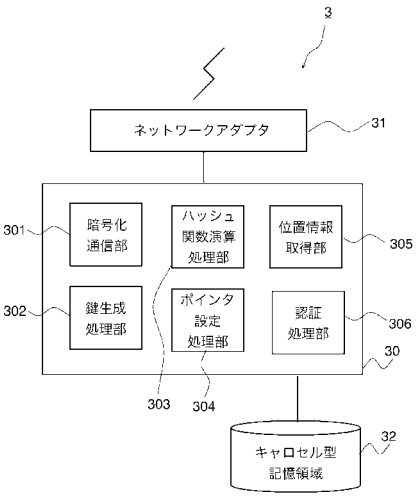
【図１】


ネットワーク
1
AP
AP
AP
AP
AP
2
2
3

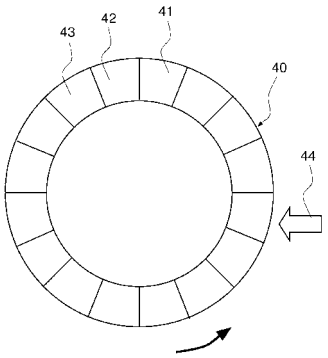
【図２】


2
キャロセル型
記憶領域
22
暗号化
通信部
ハッシュ
関数演算
処理部
位置情報
取得部
201
205
鍵生成
処理部
ポインタ
設定
処理部
認証
処理部
202
206
20
203
204
ネットワークカード
21

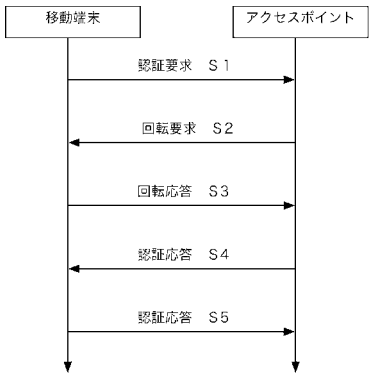
【図３】


3
ネットワークアダプタ
31
暗号化
通信部
ハッシュ
関数演算
処理部
位置情報
取得部
301
305
鍵生成
処理部
ポインタ
設定
処理部
認証
処理部
302
306
30
303
304
キャロセル型
記憶領域
32

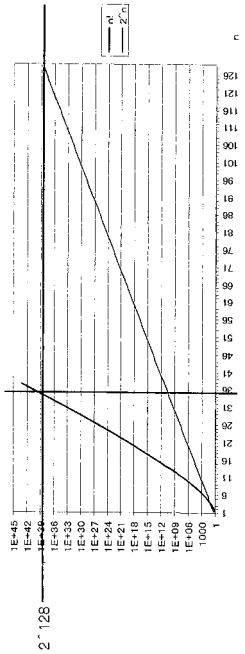
【図４】


43
42
41
40
44

【図５】



【図６】



フロントページの続き

(56)参考文献 特開平１０－１６４６５６（ＪＰ，Ａ）
特開２００４－２４８１６７（ＪＰ，Ａ）
特開２００７－０５８４６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｈ０４Ｗ	４／００	－Ｈ０４Ｗ	９９／００
Ｈ０４Ｌ	９／００	－Ｈ０４Ｌ	９／３８