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

特許第4103465号
(P4103465)

(45)発行日　平成20年6月18日(2008.6.18)　(24)登録日　平成20年4月4日(2008.4.4)

(51)Int.Cl.			F I		
H04Q	7/20	(2006.01)	H04Q	7/04	Z
G01S	5/14	(2006.01)	G01S	5/14	
H04B	7/26	(2006.01)	H04B	7/26	M
H04M	11/00	(2006.01)	H04M	11/00	302
H04Q	7/38	(2006.01)	H04B	7/26	109R

請求項の数 17　(全 42 頁)

(21)出願番号　特願2002-185912(P2002-185912)
(22)出願日　平成14年6月26日(2002.6.26)
(65)公開番号　特開2004-32376(P2004-32376A)
(43)公開日　平成16年1月29日(2004.1.29)
審査請求日　平成17年6月16日(2005.6.16)

前置審査

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(72)発明者　高田　昌幸
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　武藤　隆保
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　吉村　博之

最終頁に続く

(54)【発明の名称】情報端末装置、情報処理装置、及び情報送受信システム

(57)【特許請求の範囲】

【請求項１】

全地球測位システムを構成する人工衛星から送出される衛星信号を受信する受信手段と、

通信ネットワークを介し、認証情報として各情報処理装置を識別する識別情報を送受信する送受信手段と、

上記送受信手段により受信された上記識別情報をユーザに報知し、ユーザによって上記情報処理装置が正当な接続対象であることを認める操作が入力された場合に、上記情報処理装置が正当な接続対象であると認証し、上記衛星信号から算出される自己の現在位置及び現在の時刻に関する位置時刻情報を上記送受信手段により送信することを許可する認証手段と、

を備えることを特徴とする情報端末装置。

【請求項２】

全地球測位システムを構成する人工衛星から送出される衛星信号を受信する受信手段と、

通信ネットワークを介して情報処理装置との間で各種情報を送受信する送受信手段と、

上記衛星信号に基づいて、自己の現在位置及び／又は現在の時刻を算出する演算手段と、

上記演算手段により算出された自己の現在位置及び／又は現在の時刻が、位置及び／又は時刻に関する所定の条件に適合するか否かを判定する条件判定手段と、

上記送受信手段により送受信される認証情報に基づいて上記情報処理装置が正当な接続対象であるか否かを判定する認証手段と、
を備え、
上記送受信手段は、上記情報処理装置が正当な接続対象あると上記認証手段により認証された場合に、上記条件判定手段による判定結果を現在位置及び／又は現在の時刻に関する位置時刻情報として上記情報処理装置に対して送信することを特徴とする、情報端末装置。
【請求項３】
全地球測位システムを構成する人工衛星から送出される衛星信号を受信して、上記衛星信号から自己の現在位置及び／ 又は現在時刻を算出する位置時刻算出手段と、
通信ネットワークを介して情報処理装置との間で各種情報を送受信する送受信手段と、
上記送受信手段により送受信される認証情報に基づいて上記情報処理装置が正当な接続対象であるか否かを認証する認証手段と、
上記認証手段により認証された上記情報処理装置に関する情報と、上記位置時刻算出手段によって算出された現在位置及び／又は現在時刻とに基づいて鍵を生成し、上記送受信手段により送受信される各種情報に対して、上記鍵を用いて暗号化処理及び／又は復号化処理を施す暗号処理手段とを備えること
を特徴とする情報端末装置。
【請求項４】
上記送受信手段は、上記位置時刻情報として、上記衛星信号に含まれ、自己の現在位置及び現在の時刻を上記情報処理装置によって算出するために利用される情報を送信すること
を特徴とする請求項１に記載の情報端末装置。
【請求項５】
上記衛星信号に基づいて、自己の現在位置及びは現在の時刻を算出する演算手段をさらに備え、
上記送受信手段は、上記位置時刻情報として、上記演算手段により算出された自己の現在位置及び現在の時刻を示す情報を送信すること
を特徴とする請求項１に記載の情報端末装置。
【請求項６】
上記衛星信号に基づいて、自己の現在位置及は現在の時刻を算出する演算手段をさらに備え、
上記演算手段により算出された自己の現在位置及び現在の時刻が、位置及び時刻に関する所定の条件に適合するか否かを判定する条件判定手段をさらに備え、
上記送受信手段は、上記条件判定手段による判定結果を上記位置時刻情報として上記情報処理装置に対して送信すること
を特徴とする請求項１に記載の情報端末装置。
【請求項７】
上記送受信手段は、上記条件を示す情報を上記情報処理装置から取得すること
を特徴とする請求項６に記載の情報端末装置。
【請求項８】
上記条件を示す情報を記憶する記憶手段をさらに備え、
上記記憶手段には、上記条件に対応した接続対象となる情報処理装置に関する情報が記憶され、
上記送受信手段は、適合した条件に応じた情報処理装置に対して上記条件判定手段による判定結果を送信すること
を特徴とする請求項６に記載の情報端末装置。
【請求項９】
ユーザからの要求に応じて、或いは接続対象とする情報処理装置に応じて、上記位置時刻情報に含まれる現在位置の精度及び現在時刻の精度を変更とする精度変更手段をさらに

備えること
を特徴とする請求項１に記載の情報端末装置。
【請求項１０】
上記送受信手段は、上記情報処理装置から所定のデータ列を含むデータ列情報をさらに取得し、
上記認証手段は、さらに上記送受信手段により取得した上記データ列情報が予め設定されたデータ列情報と一致する場合に、上記情報処理装置が正当な接続対象であると認証すること
を特徴とする請求項１に記載の情報端末装置。
【請求項１１】
上記送受信手段により送受信する上記識別情報を含む各種情報に対して所定の暗号方式で暗号化処理及び／又は復号化処理を施す暗号処理手段をさらに備えること
を特徴とする請求項１に記載の情報端末装置。
【請求項１２】
上記認証手段は、上記情報処理装置が正当な接続対象であると認証した場合に限って、上記衛星信号を捕捉するために利用されるアシスト情報を上記送受信手段によって上記情報処理装置から取得することを許可すること
を特徴とする請求項１に記載の情報端末装置。
【請求項１３】
全地球測位システムを構成する人工衛星から送出される衛星信号を受信する情報端末装置との間で通信ネットワークを介して各種情報の送受信を行う送受信手段と、
上記衛星信号から算出される上記情報端末装置の現在位置及び現在の時刻に関する位置時刻情報を上記送受信手段により上記情報端末装置から取得するに際して、上記送受信手段によって上記情報端末装置との間で認証情報として各情報処理装置を識別する識別情報を授受することにより、上記位置時刻情報を取得する正当な権限を有することを認証する認証手段とを備えること
を特徴とする情報処理装置。
【請求項１４】
上記送受信手段によって取得した上記位置時刻情報に基づいて、上記情報端末装置の現在位置を算出する演算手段をさらに備えること
を特徴とする請求項１３記載の情報処理装置。
【請求項１５】
上記送受信手段により送受信する各種情報に対して所定の暗号方式で暗号化処理及び／又は復号化処理を施す暗号処理手段をさらに備えること
を特徴とする請求項１３記載の情報処理装置。
【請求項１６】
上記送受信手段は、通信ネットワークを介して接続された他の情報処理装置との間で各種情報の送受信を行うとともに、
上記認証手段は、上記他の情報処理装置から所定の時刻における上記情報端末装置の位置に関する問い合わせがあった場合に、上記他の情報処理装置との間で授受される識別情報に基づいて上記他の情報処理装置が正当な接続対象であるか否かを判定し、正当な接続対象であると認証した場合に限って、上記送受信手段により上記情報端末装置の位置に関する情報を送信することを許可すること
を特徴とする請求項１３記載の情報処理装置。
【請求項１７】
全地球測位システムを構成する人工衛星から送出される衛星信号を受信する情報端末装置と、上記衛星信号から算出される上記情報端末装置の現在位置及び現在の時刻に関する位置時刻情報を上記情報端末装置に対して問い合わせる情報処理装置とが通信ネットワークを介して接続されてなり、
上記情報端末装置と上記情報処理装置との間で認証情報として各情報処理装置を識別す

る識別情報を授受することによって認証を行い、上記情報処理装置が正当な接続対象であると認証した場合に限って、上記情報端末装置から上記情報処理装置に対する上記位置時刻情報の送信を許可すること
を特徴とする情報送受信システム。

【発明の詳細な説明】

【０００１】

【発明の属する分野】

本発明は、全地球測位システムを構成する人工衛星から送出された衛星信号を受信する情報端末装置に関する。また、このような情報端末装置に対して、現在位置及び／又は現在の時刻に関する位置時刻情報の問い合わせを行う情報処理装置、及び情報送受信システムに関する。

【０００２】

【従来の技術】

近年、地球軌道を周回する人工衛星を利用して地上における移動体の位置を測定する全地球測位システム（ＧＮＳＳ：Global Navigation Satellites System）が普及しつつある。このような全地球測位システムとしては、アメリカ合衆国が構築したＧＰＳ（Global Positioning System）、旧ソビエト連邦国が構築したＧＬＯＮＡＳＳ（Global Navigation Satellites System）、欧州の各国が中心となって構築が進められているＧＡＬＩＬＥＯなどがある。

【０００３】

この全地球測位システムにおいて、現在位置を測定するに際しては、移動体に搭載された受信装置によって、少なくとも４つ以上の衛星からの信号を受信する。そして、各衛星からの信号を復調して各衛星の軌道情報を取得し、各衛星の軌道情報及び時間情報と受信信号の遅延時間とに基づいて、自己の３次元位置と現在の正確な時刻とを連立方程式によって算出する。全地球測位システムは、上述のようにして現在位置及び現在時刻を算出する機能（以下、ＧＰＳ機能と称する。）を有する受信装置を各種の車両や航空機などに搭載して、経路を案内したり、各車両や航空機の現在位置を把握するなどの目的で広く利用されている。また、従来から、ＧＰＳ機能を搭載した携帯型の測位装置も利用されている。

【０００４】

ところで、近年では、例えば受信装置の小型化・低消費電力化が進められており、これに伴って、ＧＰＳ機能が各種の情報端末装置に搭載されつつある。特に、高機能化・多機能化が急速に進められている携帯型の電話機（すなわち、いわゆる携帯電話）においては、ＧＰＳ機能を搭載した機種の普及が顕著である。

【０００５】

このような携帯電話は、基本的な通話機能及びＧＰＳ機能の他に、例えばインターネット（The Internet）などの通信ネットワークを介して他の情報処理装置との間で各種情報の授受を可能とするネットワーク機能を備えていることが一般的である。そして、ＧＰＳ機能を利用して得られた現在位置に関する情報を、ネットワーク機能を利用して他の情報処理装置との間で授受することにより、現在位置に関連した様々なサービスを享受することが可能とされている。

【０００６】

このようなサービスの例としては、例えば、ＧＰＳ機能を備えた携帯電話によって取得した現在位置に関する情報を通信ネットワークを介してサーバ装置に送信し、このサーバ装置から現在位置近傍の地図データを取得して表示画面に表示する地図表示サービスを挙げることができる。また、同様にしてサーバ装置との間で情報の授受を行うことにより実現される、現在位置から目的地までの経路を表示するナビゲーションサービス、現在位置に関する情報を他の携帯電話やコンピュータ装置に対して電子メールによって通知するメール送信サービス、現在位置の周辺に存在する各種店舗に関する情報を表示する周辺情報表示サービスなどを挙げることができる。

【０００７】

また、現在、通信ネットワークの広帯域化・低コスト化が進められていることを考慮すると、上述したような携帯電話だけでなく、例えばＰＤＡ（Personal Digital Assistant）機器や小型軽量のパーソナルコンピュータ装置に代表される各種の情報端末装置においても、ＧＰＳ機能とネットワーク機能とを連携させて現在位置に関する各種サービスの提供が一層広まるものと予想される。

【０００８】

【発明が解決しようとする課題】

ところで、近年では、携帯電話を肌身離さず携行する傾向がみられるように、高機能化及び小型軽量化が進む各種の情報端末装置は、その所有者（ユーザ）とほぼ一体に利用される場合が多い。このため、このような情報端末装置の現在位置は、そのユーザの現在位置であるとみなすことが可能であるといった状況になりつつある。

【０００９】

したがって、情報端末装置に備えられたＧＰＳ機能を利用して得られる現在位置及び現在時刻は、そのユーザが「何時何処にいたか」ということを特定する情報である。また、ＧＰＳ機能によって得られる現在位置は、数十メートルから数メートル程度の誤差で極めて高精度で算出されることから、この現在位置に基づいて、特定の時刻にユーザが何処の店舗にいたか、或いは建物内のどの位置にいたかなどといったことを特定し、延いてはユーザが「なにをしていたか」ということまで予想することも困難ではない。このため、情報端末装置に備えられたＧＰＳ機能を利用して得られる現在位置及び現在時刻に関する情報は、ユーザの行動を特定する情報であり、ユーザにとって極めて重要な個人情報としての性質を有している。

【００１０】

しかしながら、ＧＰＳ機能を備える携帯電話を利用した従来のサービスにおいては、特定の時刻に算出された現在位置に関する情報が特別な保護を受けずに通信ネットワーク上を送受信されている。このため、ユーザが意図しない第三者によってこの情報が読み出されてしまい、ユーザの個人情報が漏洩してしまう虞があった。

【００１１】

例えば、ＧＰＳ機能を備える携帯電話を利用したサービスを例に挙げると、従来は、この携帯電話と基地局或いはサーバ装置との間で通信経路を確立するまでの間に、携帯電話又はユーザを特定する識別情報などの授受が行われるものの、一度通信経路が確立された後は、他の雑多なデータと同様にして位置情報が送受信されている。また、インターネットなどのように不特定多数のユーザが利用するオープンな通信ネットワークを介在させて位置情報を送受信する場合には、第三者によって位置情報の漏洩が行われる危険性が高くなる。

【００１２】

そこで、本発明は、上述した従来の実情に鑑みてなされたものであり、全地球測位システムを利用して算出される現在位置や現在時刻に関する情報、すなわち位置時刻情報が、ユーザの意図しない第三者へ漏洩してしまうことを防止し、通信ネットワークを介して情報処理装置との間で安全且つ確実に位置時刻情報を送受信することが可能な情報端末装置を提供することを目的とする。また、このような情報端末装置に対して位置時刻情報の問い合わせを行う情報処理装置、及び情報送受信システムを提供することを目的とする。さらに、全地球測位システムを利用して算出される現在位置や現在時刻に関する情報と、接続に対して認証が行われた情報処理装置に関する情報とを利用して全く新規な暗号処理を行うことが可能な情報処理装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】

上記課題を解決するために、本発明のある観点によれば、全地球測位システムを構成する人工衛星から送出される衛星信号を受信する受信手段と、通信ネットワークを介して情報処理装置との間で各種情報を送受信する送受信手段と、上記送受信手段により送受信される認証情報に基づいて上記情報処理装置が正当な接続対象であるか否かを判定し、正当

な接続対象であると認証した場合に限って、上記衛星信号から算出される自己の現在位置及び現在の時刻に関する位置時刻情報を上記送受信手段により送信することを許可する認証手段とを備えること情報端末装置が提供される。

【００１４】

当該情報端末装置は、位置時刻情報を情報処理装置に対して送信するに際して、この情報処理装置が正当な接続対象であることを認証手段によって認証した場合に限って、位置時刻情報の送信が許可される。したがって、例えば、ユーザが意図しない第三者から位置時刻情報の送信を要求された場合であっても、これを認証手段によって確実に防止することができ、ユーザの行動を特定する個人情報となり得る位置時刻情報がユーザの意図に反する第三者に漏洩してしまうことを防止することができる。

【００１５】

また、上記課題を解決するために、本発明の別の観点によれば、全地球測位システムを構成する人工衛星から送出される衛星信号を受信する受信手段と、通信ネットワークを介して情報処理装置との間で各種情報を送受信する送受信手段と、上記衛星信号に基づいて、自己の現在位置及び／又は現在の時刻を算出する演算手段と、上記演算手段により算出された自己の現在位置及び／又は現在の時刻が、位置及び／又は時刻に関する所定の条件に適合するか否かを判定する条件判定手段と、上記送受信手段により送受信される認証情報に基づいて上記情報処理装置が正当な接続対象であるか否かを判定する認証手段と、を備え、上記送受信手段は、上記情報処理装置が正当な接続対象あると上記認証手段により認証された場合に、上記条件判定手段による判定結果を上記位置時刻情報として上記情報処理装置に対して送信する情報端末装置が提供される。

【００１６】

また、上記課題を解決するために、本発明の別の観点によれば、全地球測位システムを構成する人工衛星から送出される衛星信号を受信して、上記衛星信号から自己の現在位置及び／ 又は現在時刻を算出する位置時刻算出手段と、通信ネットワークを介して情報処理装置との間で各種情報を送受信する送受信手段と、上記送受信手段により送受信される認証情報に基づいて上記情報処理装置が正当な接続対象であるか否かを認証する認証手段と、上記認証手段により認証された上記情報処理装置に関する情報と、上記位置時刻算出手段によって算出された現在位置及び／又は現在時刻とに基づいて鍵を生成し、上記送受信手段により送受信される各種情報に対して、上記鍵を用いて暗号化処理及び／又は復号化処理を施す暗号処理手段とを備える情報端末装置が提供される。

【００１７】

また、上記送受信手段は、上記位置時刻情報として、上記衛星信号に含まれ、自己の現在位置及び／ 又は現在の時刻を上記情報処理装置によって算出するために利用される情報を送信してもよい。この構成は、衛星信号から算出される情報端末装置の現在位置或いは現在時刻を直接示す情報ではなく、衛星信号に含まれる情報のうち、現在位置或いは現在時刻を算出するために必要となる情報を位置時刻情報として情報端末装置から情報処理装置に送信する構成である。以上の構成とすることにより、情報端末装置側で衛星信号から現在位置や現在時刻を算出せずに、これを情報処理装置側で算出することができ、現在位置や現在時刻の算出に要する演算能力を情報端末装置側に備えることが不要となる。したがって、情報端末装置に搭載する演算回路の回路規模や消費電力を低減することができる。なお、この場合に、情報端末装置側で衛星信号から得られた現在位置や現在時刻を表示するなどの必要が生じた場合には、情報処理装置側で算出された現在位置や現在時刻を通信ネットワークを介して取得すればよい。

【００１８】

また、当該情報処理端末は、上記衛星信号に基づいて、自己の現在位置及び／ 又は現在の時刻を算出する演算手段をさらに備え、上記送受信手段は、上記位置時刻情報として、上記演算手段により算出された自己の現在位置及び／
又は現在の時刻を示す情報を送信する。以上の構成とすることにより、演算手段によって情報端末装置自身が衛星信号から現在位置や現在時刻を算出することができる。このため

、情報端末装置は、情報処置装置と接続されていない状況の下であっても、衛星信号から算出された現在位置などの情報を、例えば表示部に現在位置を表示するなどして利用することが可能となる。また、現在位置を連続して表示する場合などであっても、情報処理装置との接続状態を維持する必要がない。

【００１９】

また、当該情報処理端末は、上記衛星信号に基づいて、自己の現在位置及び／ 又は現在の時刻を算出する演算手段をさらに備え、上記演算手段により算出された自己の現在位置及び／
又は現在の時刻が、位置及び／ 又は時刻に関する所定の条件に適合するか否かを判定する条件判定手段をさらに備え、上記送受信手段は、上記条件判定手段による判定結果を上記位置時刻情報として上記情報処理装置に対して送信してもよい。この構成では、衛星信号から算出された現在位置や現在時刻が所定の条件に適合したか否かを示す判定結果のみを、自己の現在位置及び／
又は現在の時刻に関する位置時刻情報として情報処理装置に対して送信する構成である。この場合には、現在位置や現在時刻を示す直接的で高精度な情報ではなく、判定結果のみを情報処理装置に対して送信することから、ユーザの行動を特定する個人情報の秘匿性を向上させることができる。

【００２０】

なお、条件判定手段における判定に用いられる「条件」に関する情報は、情報処理装置から送受信手段によって取得するとしてもよいし、請求項６ に係る情報端末装置の構成とすることによって、情報端末装置に備えられたＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）
やＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ） 等の各種記憶素子に予め記憶しておくとしてもよい。判定に用いる条件を情報処理装置から取得する構成とすることにより、状況に応じて多数の多様な条件に対して判定を行うことができ、条件を保持しておくために必要な記憶領域を低減することができる。一方、判定に用いる条件を情報端末装置に備えられる記憶手段に記憶しておく構成とすることにより、現在位置や時刻が更新される度に情報処理装置から条件を取得することが不要となり、情報処理装置と接続されていない状況の下でも条件に適合するか否かを判定する処理を連続的に行うことができる。

【００２１】

また、当該情報端末装置は、上記条件を示す情報を記憶する記憶手段をさらに備え、上記記憶手段には、上記条件に対応した接続対象となる情報処理装置に関する情報が記憶され、上記送受信手段は、適合した条件に応じた情報処理装置に対して上記条件判定手段による判定結果を送信してもよい。以上の構成とすることにより、例えば、適合した条件に応じた情報処理装置に対して判定結果を送信し、この情報処理装置から現在位置や現在時刻に即したサービスを選択的に享受するなどして、柔軟且つ多彩な情報をユーザに提供することが容易となる。また、当該情報端末装置は、ユーザからの要求に応じて、或いは接続対象とする情報処理装置に応じて、上記位置時刻情報に含まれる現在位置の精度及び／ 又は現在時刻の精度を変更とする精度変更手段をさらに備えてもよい。以上の構成により、例えば、特定の接続対象に対しては高精度な現在位置や現在時刻に関する情報を送信する一方で、他の接続対象に対しては精度を意図的に劣化させた情報を送信することが可能となり、ユーザの行動を特定する個人情報としての位置や時刻に関する情報を不必要に高精度で送信してしまうことを防止することができる。また、上記送受信手段は、上記認証情報として、各情報処理装置を識別する識別情報を上記情報処理装置から取得し、上記認証手段は、上記識別情報をユーザに報知し、ユーザによって上記情報処理装置が正当な接続対象であることを認める操作が入力された場合に、上記情報処理装置が正当な接続対象であると判定してもよい。以上の構成により、情報端末装置は、情報処理装置に対して位置時刻情報を送信しても問題がないか否かをユーザに問い合わせることができ、ユーザの判断に応じて位置時刻情報を送信するか否かを選択することができる。

【００２２】

また、上記送受信手段は、上記情報処理装置から所定のデータ列を含むデータ列情報を取得し、上記認証手段は、上記送受信手段により取得した上記データ列情報が予め設定されたデータ列情報と一致する場合に、上記情報処理装置が正当な接続対象であると判定してもよい。この構成は、認証情報として情報処理装置から取得したデータ列情報が予め設定されたデータ列情報と一致するか否かを判定することによる認証、いわゆるパスワード方式の認証を行う構成である。この構成によれば、最も原始的且つ簡素な手法により認証を行うことができることから、認証を行うに際して高い演算能力を必要とせず、極めて高速且つ簡便に実現することができる。なお、データ列情報としては、英字、数字、ひらがな、漢字等からなる各種の文字の連続した一群を示す文字列情報だけでなく、バイナリデータであってもよい。

【００２３】

また、当該情報端末装置は、上記送受信手段により送受信する各種情報に対して所定の暗号方式で暗号化処理及び／又は復号化処理を施す暗号処理手段をさらに備えてもよい。以上の構成によれば、認証情報を含めて、情報端末装置と情報処理装置との間で送受信する各種情報に対して暗号化を施すことができ、ユーザが意図しない第三者に各種情報が漏洩してしまうことを防止することができる。

【００２４】

また、上記暗号処理手段は、上記位置時刻情報に基づいて鍵を生成し、当該鍵を用いて各種情報に対する暗号化処理及び／又は復号化処理を施してもよい。なお、位置時刻情報から鍵を生成する手順に関する情報は、予め定められて情報端末装置内部に記憶しておくとしてもよいし、鍵を生成するに際して情報処理装置から取得するとしてもよい。以上の構成とすることにより、所定の場所で所定の時刻になったときに初めて解読することが可能な情報を情報処理装置との間で送受信することができる。これにより、ユーザの個人情報となる位置時刻情報の漏洩を防止する一方で、柔軟で多彩なサービスを享受することが可能となる。

【００２５】

なお、情報端末装置と情報処理装置との間で送受信する情報に対して暗号化を施す場合には、本発明の情報端末装置が共通鍵を利用した共通鍵暗号方式により暗号化処理及び／又は復号化処理を施す暗号処理手段を備えるような構成とすることによって、共通鍵を利用した共通鍵暗号方式を採用するとしてもよいし、本発明の情報端末装置が公開鍵と秘密鍵とを利用した公開鍵暗号方式に基づいて暗号化処理及び／又は復号化処理を施す暗号処理手段を備えるような構成とすることによって、公開鍵と秘密鍵とを利用した公開鍵暗号方式を採用するとしてもよい。共通鍵暗号方式を採用する場合には、暗号化・復号化手順が比較的簡便であることから、簡便且つ小規模な演算回路によって、送受信する情報に対する暗号化処理及び復号化処理を高速で施すことができる。また、公開鍵暗号方式を採用する場合には、共通鍵暗号方式と比較してより複雑で計算量を要する処理が必要となるものの、送受信する情報に対してより強固な暗号化を施すことが可能となる。

【００２６】

また、上記暗号処理手段は、共通鍵を利用した共通鍵暗号方式により暗号化処理及び／又は復号化処理を施し、上記認証手段は、上記共通鍵を利用して所定の認証情報を上記情報処理装置との間で授受することによって認証を行ってもよい。具体的には、例えば、情報端末装置側で乱数を生成し、この乱数を情報処理装置側で共通鍵を用いて暗号化した後に情報端末装置側に戻し、情報端末装置側で共通鍵を用いて復号化した乱数と元の乱数とが一致している場合に、この情報処理装置を正しい接続対象と認証するなどの認証手順を行う。このように、認証に用いる認証情報（この場合には、乱数が認証情報に該当する。）を暗号化することによって、ユーザが意図しない第三者による「なりすまし」等を防止して、より確実に認証を行うことができる。

【００２７】

また、上記暗号処理手段は、共通鍵を利用した共通鍵暗号方式により暗号化処理及び／又は復号化処理を施し、上記認証手段は、上記共通鍵を利用して所定の認証情報を上記情

報処理装置との間で授受することによって認証を行う構成に、さらに加えて、上記認証手段は、上記公開鍵暗号方式を利用して上記情報処理装置との間で電子署名を授受することによって認証を行ってもよい。公開鍵暗号方式においては、通常、接続対象毎に異なる秘密鍵を有していることから、電子署名を授受することによって、認証を行うと同時に接続対象となる情報処理装置を特定することができる。なお、認証時に必要となる相手側の公開鍵は、予め情報端末装置内に保持しておくとしてもよいし、必要に応じて通信ネットワークを介して外部から取得するとしてもよい。

【００２８】

また、上記認証手段は、上記情報処理装置が正当な接続対象であると認証した場合に限って、上記衛星信号を捕捉するために利用されるアシスト情報を上記送受信手段によって上記情報処理装置から取得することを許可してもよい。以上の構成とすることにより、認証が正しく行われた場合に限って情報処理装置からアシスト情報を取得することができることから、ユーザの意図しない第三者に対してアシスト情報が漏洩してしまうことを防止して、このアシスト情報に基づいてユーザの現在位置が類推されてしまう虞を低減することができる。

【００２９】

また、上記課題を解決するために、本発明の別の観点によれば、全地球測位システムを構成する人工衛星から送出される衛星信号を受信して、上記衛星信号から自己の現在位置及び／又は現在時刻を算出する位置時刻算出手段と、通信ネットワークを介して情報処理装置との間で各種情報を送受信する送受信手段と、上記送受信手段により送受信される認証情報に基づいて上記情報処理装置が正当な接続対象であるか否かを認証する認証手段と、上記認証手段により認証された上記情報処理装置に関する情報と、上記位置時刻算出手段によって算出された現在位置及び／又は現在時刻とに基づいて鍵を生成し、上記送受信手段により送受信される各種情報に対して、上記鍵を用いて暗号化処理及び／又は復号化処理を施す暗号処理手段とを備える情報端末装置が提供される。

【００３０】

以上のように構成された情報端末装置は、衛星信号から算出された現在位置や現在時刻と、接続に対して認証が行われた情報処理装置に関する情報とに基づいて生成した鍵を用いて暗号処理を行うことができる。このため、情報処理装置に対して正しく接続状態が確立された状態において、所定の位置に存在する場合に限って、又は所定の時刻になった時点に限って、或いは所定の位置に存在し、且つ所定の時刻になった時点に限って、情報の暗号化処理や復号化処理を行うことが可能であるという全く新規な暗号処理を行うことができる。

【００３１】

また、上記課題を解決するために、本発明の別の観点によれば、全地球測位システムを構成する人工衛星から送出される衛星信号を受信する情報端末装置との間で通信ネットワークを介して各種情報の送受信を行う送受信手段と、上記衛星信号から算出される上記情報端末装置の現在位置及び現在の時刻に関する位置時刻情報を上記送受信手段により上記情報端末装置から取得するに際して、上記送受信手段によって上記情報端末装置との間で認証情報を授受することにより、上記位置時刻情報を取得する正当な権限を有することを認証する認証手段とを備える情報処理装置が提供される。

【００３２】

以上のように構成された情報処理装置は、位置時刻情報を情報端末装置から取得するに際して、情報端末装置との間で認証を行う構成とされている。したがって、例えば、ユーザが意図しない第三者に対して位置時刻情報を送信してしまうことを防止する目的で、情報端末装置側から認証を求められた場合であっても、この認証を正しく行って、位置時刻情報を取得することができる。

【００３３】

また、当該情報処理装置は、上記送受信手段によって取得した上記位置時刻情報に基づいて、上記情報端末装置の現在位置を算出する演算手段をさらに備えてもよい。以上の構

成とすることによって、情報端末装置側で衛星信号から現在位置や現在時刻を算出せずに、これを情報処理装置側で算出することができ、現在位置や現在時刻の算出に要する演算能力を情報端末装置側に備えることが不要となる。また、この場合には、情報端末装置と情報処理装置との間で授受される位置時刻情報が現在位置や現在時刻を直接示す情報ではなく、現在位置や現在時刻を算出する元となる情報であることから、ユーザが意図しない第三者により通信ネットワーク上で位置時刻情報が傍受された場合であっても、この位置や時刻の特定を困難とすることができる。

【００３４】

また、当該情報処理装置は、上記送受信手段により送受信する各種情報に対して所定の暗号方式で暗号化処理及び／又は復号化処理を施す暗号処理手段をさらに備えてもよい。以上の構成によれば、認証情報を含めて、情報端末装置と情報処理装置との間で送受信する各種情報に対して暗号化を施すことができ、ユーザが意図しない第三者に各種情報が漏洩してしまうことを防止することができる。

【００３５】

上記送受信手段は、通信ネットワークを介して接続された他の情報処理装置との間で各種情報の送受信を行うとともに、上記認証手段は、上記他の情報処理装置から所定の時刻における上記情報端末装置の位置に関する問い合わせがあった場合に、上記他の情報処理装置との間で授受される認証情報に基づいて上記他の情報処理装置が正当な接続対象であるか否かを判定し、正当な接続対象であると認証した場合に限って、上記送受信手段により上記情報端末装置の位置に関する情報を送信することを許可してもよい。この構成は、情報端末装置から位置時刻情報の送信対象を所定の情報処理装置に限定し、他の情報処理装置は、この所定の情報処理装置に対して問い合わせを行うことによって、携帯端末装置の位置時刻情報を取得する構成としたものである。以上の構成とすることにより、情報端末装置が認証を行う対象の数を最小限に抑えながら、所定の情報処理装置が中継処理を行うことによって、多数の情報処理装置からの問い合わせに対応することができる。これにより、情報端末装置が多数の接続対象との間でそれぞれ認証を行うことが不要となり、認証に要する処理の簡略化を図るとともに、情報端末装置と情報処理装置との間で位置時刻情報などが漏洩してしまう虞を著しく低減することができる。

【００３６】

また、上記課題を解決するために、本発明の別の観点によれば、全地球測位システムを構成する人工衛星から送出される衛星信号を受信する情報端末装置と、上記衛星信号から算出される上記情報端末装置の現在位置及び現在の時刻に関する位置時刻情報を上記情報端末装置に対して問い合わせる情報処理装置とが通信ネットワークを介して接続されてなり、上記情報端末装置と上記情報処理装置との間で認証情報を授受することによって認証を行い、上記情報処理装置が正当な接続対象であると認証した場合に限って、上記情報端末装置から上記情報処理装置に対する上記位置時刻情報の送信を許可する情報送受信システムが提供される。

【００３７】

以上のように構成された情報送受信システムは、情報端末装置と情報処理装置との間で位置時刻情報を授受するに際して、この情報処理装置が正当な接続対象であることを認証手段によって認証した場合に限って、位置時刻情報の送信が許可される。したがって、例えば、ユーザが意図しない第三者に対して位置時刻情報が送信されてしてしまうことを防止することができる。

【００３８】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。以下では、本発明を適用した情報端末装置として、人工衛星を利用した測位機能を備える携帯電話を例に挙げて説明する。

【００３９】

まず、本発明を適用することにより実現される情報提供システムの全体構成について、図

１を参照しながら説明する。

【００４０】

情報提供システム１は、図１に示すように、ＧＰＳを利用した測位機能（以下、ＧＰＳ機能と称する。）を備える携帯電話１０と、ＧＰＳを構成する複数の人工衛星２０（以下、ＧＰＳ衛星２０と称する。）と、携帯電話１０に対して各種の情報を提供するサーバ装置３０と、携帯電話１０との間で無線通信を行うとともに、サーバ装置３０と通信ネットワーク４０を介して接続されてなる通信基地局５０とを備える。なお、情報提供システム１においては、携帯電話１０が接続対象とするサーバ装置３０が１つだけであってもよいし、複数であってもよい。

【００４１】

携帯電話１０は、通信基地局５０との間で無線通信を行い、この通信基地局５０及び電話回線網を介して他の電話機との間で音声通話を行う通話機能を有している。また、携帯電話１０は、通話機能の他に、各ＧＰＳ衛星２０から送出される信号（以下、ＧＰＳ信号と称する。）を受信するＧＰＳ機能と、通信基地局５０及び通信ネットワーク４０を介してサーバ装置３０との間で伝送路を確立し、サーバ装置３０との間で各種の情報を送受信する機能（以下、ネットワーク機能と称する。）とを有している。

【００４２】

つぎに、携帯電話１０の具体的な一構成例について、図２を参照しながら説明する。携帯電話１０は、図２に示すように、スピーカ１００と、マイク１０１と、音声処理部１０３と、ＲＦアンテナ１０４と、ＲＦ信号処理部１０５と、変復調部１０６と、ＣＰＵ（Central Processing Unit）１０７と、入力操作部１０８と、液晶表示部（以下、単にＬＣＤと称する。）１０９と、ＲＯＭ（Read Only Memory）１１０と、ＲＡＭ（Random Access Memory）１１１と、不揮発メモリ１１２と、ＧＰＳアンテナ１１３と、ＧＰＳ信号受信部１１４とを備える。

【００４３】

スピーカ１００は、音声処理部１０３から出力された電気的な音声信号を音声に変換して出力する。ユーザは、このスピーカ１００から出力される音声を聴取する。マイク１０１は、ユーザが発声した音声を電気的な音声信号に変換し、音声処理部１０３に出力する。音声処理部１０３は、マイク１０１から供給される音声信号に対して、増幅、デジタル信号への変換、耐圧圧縮、及び誤り訂正符号の付加などの処理を施し、得られたベースバンド信号を変復調部１０６に出力する。また、音声処理部１０３は、変復調部１０６から出力されたベースバンド信号に対して、帯域圧縮、誤り訂正処理、アナログ信号への変換、及び増幅などの処理を施し、得られた音声信号をスピーカ１００に出力する。

【００４４】

ＲＦアンテナ１０４は、通信基地局５０から送信された無線電波を受信するとともに、ＲＦ信号処理部１０５から出力された信号を無線電波として通信基地局５０に送信する。ＲＦ信号処理部１０５は、ＲＦアンテナ１０４が受信した信号を増幅し、所定の周波数成分の信号であるＲＦ信号に変換する。そして、変換したＲＦ信号に対して各種のフィルタ処理を行った後に、変復調部１０６に出力する。また、ＲＦ信号処理部１０５は、変復調部１０６から出力された変調信号を、図示を省略する周波数シンセサイザからの出力と混合することにより所定の周波数に変換し、さらに増幅処理を行ってＲＦアンテナ１０４に出力する。

【００４５】

変復調部１０６は、ＲＦ信号処理部１０５から出力された信号をベースバンド信号に変調し、得られた音声信号を音声処理部１０３に出力するとともに、変調して得られた信号に音声以外の情報が含まれている場合には、この情報をＣＰＵ１０７に出力する。また、音声処理部１０３から出力されたベースバンド信号で高周波信号を変調し、変調して得られた信号をＲＦ信号処理部１０５に出力する。また、変復調部１０６は、ＣＰＵ１０７から音声以外の情報を通信基地局５０を介してサーバ装置３０などに送信する要求が入力された場合には、この情報に対して符号化処理、変調処理などを施して、得られた信号をＲＦ

信号処理部１０５に出力する。

【００４６】

ＣＰＵ１０７は、ＲＯＭ１１０に記憶されたソフトウエアプログラムに記述された処理手順に従って動作することにより、携帯電話１０を構成する各部との間で各種の信号及び情報の授受を行い、各部の動作を制御するとともに、各部から得られた情報に対して各種の演算処理を行う。

【００４７】

入力操作部１０８は、携帯電話１０の本体に配設された複数の入力ボタンを有している。ユーザは、この入力操作部１０８を操作することによって、例えば架電する相手の電話番号の入力操作、サーバ装置３０から情報を取得する要求操作など、携帯電話１０の動作に関する各種の入力操作を行う。入力操作部１０８は、ユーザにより入力された操作を電気信号に変換してＣＰＵ１０７に供給する。ＬＣＤ１０９は、ＣＰＵ１０７から出力される情報に基づいて、図示を省略する駆動回路の制御の下に、各種情報を表示する。

【００４８】

ＲＯＭ１１０には、ＣＰＵ１０７の動作を記述したソフトウェアプログラムなどの各種情報が予め書き込まれている。ＲＯＭ１１０に書き込まれている各種情報は、ＣＰＵ１０７の制御の下に読み出される。なお、携帯電話１０の電源を切断した場合であっても、ＲＯＭ１１０に書き込まれている情報は消失しない。ＲＡＭ１１１は、ＣＰＵ１０７において各種処理を実行する際に必要となる一時記憶領域としての機能を有しており、例えば入力操作部１０８により入力された電話番号などの情報を一時記憶する。不揮発メモリ１１２は、例えば、電話番号と相手氏名との関係を示す電話帳や、サーバ装置３０との間で接続を確立するために必要となる情報など、主としてユーザが携帯電話を利用するに即して必要となるユーザ特有の情報を記憶する目的で備えられている。そして、ＣＰＵ１０７からの要求に応じて、情報の書き込み及び読み出しが自由に行われる。また、不揮発メモリ１１２に記憶された情報は、携帯電話１０の電源を切断した場合であっても消失しない。

【００４９】

ＧＰＳアンテナ１１３は、ＧＰＳ衛星２０から送信されたＧＰＳ信号を受信してＧＰＳ信号受信部１１４に出力する。ＧＰＳ信号受信部１１４は、ＧＰＳアンテナ１１３によって受信したＧＰＳ信号に対して捕捉処理、復調処理などを施すことにより、ＧＰＳ信号に含まれる情報を取り出し、得られた情報に基づいて現在時刻と携帯電話１０の現在位置とを算出する。また、ＧＰＳ信号受信部１１４は、算出された現在位置及び現在時刻をＣＰＵ１０７に出力する。なお、携帯電話１０においては、ＧＰＳ信号処理部１１４においてＧＰＳ信号から情報の取り出しのみを行い、現在位置及び現在時刻を算出する演算処理はＣＰＵ１０７によって行うとしてもよい。

【００５０】

なお、携帯電話１０の構成例は、図２に示す回路構成に限定されるものではなく、例えば着信をユーザに報知するためのバイブレータや発光素子などを備えるとしてもよい。また、本例においては、後述する暗号処理及び認証処理をＣＰＵ１０７において実行される演算処理により実現されるものとするが、これらの処理を専ら行う回路をさらに備えるとしてもよい。携帯電話１０は、暗号処理及び認証処理を実行するための専用回路をそれぞれ備えることにより、ＣＰＵ１０７で必要となる演算能力を低減する一方で、効率的且つ高速に暗号処理及び認証処理を行うことが可能となる。

【００５１】

つぎに、サーバ装置３０の具体的な一構成例について、図３を参照しながら説明する。サーバ装置３０は、図３に示すように、ＣＰＵ２００と、ＲＡＭ２０１と、ＲＯＭ２０２と、ハードディスク装置（以下、ＨＤＤと称する。）２０３と、ネットワークインターフェース２０４とを備えている。

【００５２】

ＣＰＵ２００は、ＨＤＤ２０３に記憶されたソフトウェアプログラムに記述された処理手順に従って動作することにより、サーバ装置３０を構成する各部との間で各種情報の授受

を行い、各種の演算処理を行うとともに、各部の動作を制御する。ＲＡＭ２０１は、ＣＰＵ２００において各種処理を実行する際に必要となる一時記憶領域としての機能を有している。また、ＲＯＭ２０２は、サーバ装置３０の起動時に必要となる情報などが予め書き換え不能な状態で記憶されている。ＨＤＤ２０３には、ＣＰＵ２００の動作を記述したソフトウェアプログラム、接続要求がなされる携帯電話１０を特定するための情報、携帯電話１０に対して各種サービスを提供するに際して必要となる各種の情報などが記憶されている。

【００５３】

ネットワークインターフェース２０４は、通信ネットワーク４０に接続されており、この通信ネットワーク４０を介して、携帯電話１０を含む他の情報処理装置とサーバ装置３０との間で各種情報の授受を行う機能を有している。

【００５４】

なお、サーバ装置３０は、上述した構成に限定されるものではなく、ユーザが各種操作を入力するための入力部や、ＣＰＵ２００によって処理された情報やサーバ装置３０の動作状況をユーザに報知するための表示部などをさらに備えるとしてもよい。

【００５５】

以上のように構成された情報提供システム１においては、携帯電話１０のネットワーク機能を利用して、携帯電話１０とサーバ装置３０との間で伝送路を確立し、携帯電話１０のユーザからなされた要求に応じて、サーバ装置３０から携帯電話１０に対して各種の情報が提供される。このとき、携帯電話１０の現在位置に関連した情報をサーバ装置３０に対して提供する場合、例えば、現在位置周辺を示す地図を提供するサービス、現在位置周辺に存在する各種の店舗に関する情報を提供するサービス、現在位置から所定の場所までの経路に関する情報を提供するサービス、或いは携帯電話１０の現在位置を他の情報処理装置に通知するサービスなどが利用される場合には、携帯電話１０のＧＰＳ機能を利用して取得される位置時刻情報、すなわち現在時刻における携帯電話１０の現在位置を示す情報がサーバ装置３０に送出される。そして、例えば、現在位置周辺の地図や店舗などに関する情報をサーバ装置３０から携帯電話１０に対して送信し、この情報を携帯電話１０のＬＣＤ１０９に表示したり、携帯電話１０の現在位置に関する情報がサーバ装置３０から他の情報処理装置に対して送信されるなどの処理が行われる。

【００５６】

ここで、携帯電話１０における通話機能及びネットワーク機能のについては、従来から広く利用されているものと同等であるため、その詳細な説明を割愛し、以下では、携帯電話１０のＧＰＳ機能について、サーバ装置３０が携帯電話１０から位置時刻情報を取得するまでの処理に注目して図４を参照しながら説明することとする。

【００５７】

携帯電話１０は、ユーザから現在位置に関するサービスを利用する要求がなされた場合、或いはサーバ装置３０から現在位置を送信する要求がなされた場合に、図４に示すように、ＧＰＳ衛星２０から送出されたＧＰＳ信号を受信する（Ｓ１０）。そして、携帯電話１０は、受信したＧＰＳ信号を復調して、ＧＰＳ信号に含まれる当該ＧＰＳ衛星の軌道情報及び時間情報を取得し、この軌道情報及び時間情報と受信したＧＰＳ信号の遅延時間とに基づいて、自己の３次元位置及び正確な現在時刻を連立方程式を解くことによって算出する（Ｓ１１）。次に、携帯電話１０は、得られた現在位置及び現在時刻を示す情報を、図４中において矢印Ｓ１２で示すように、サーバ装置３０に送信する。

【００５８】

なお、ＧＰＳ信号から現在位置及び現在時刻を算出するに際しては、携帯電話１０により少なくとも４つ以上のＧＰＳ衛星２０からＧＰＳ信号を受信することが必要となるが、これは以下の理由による。すなわち、携帯電話１０が備える時計の内部時刻と各ＧＰＳ衛星２０が備える原子時計による時刻との間には誤差があり、この誤差の影響を除去した正確な現在時刻と３次元位置との４つの未知パラメータを算出するためには、少なくとも４つのＧＰＳ衛星２０からの疑似距離が必要となることによる。

【００５９】
また、図４に示す例においては、ＧＰＳ信号を受信して現在位置及び現在時刻を算出するまでの処理が携帯電話１０の内部で完結している場合の例を示しているが、例えば図５に示すように、ＧＰＳ信号を高速に且つ効率よく捕捉するために利用される各種の情報（以下、アシスト情報と称する。）をサーバ装置３０から取得し（Ｓ２０）、このアシスト情報を利用してＧＰＳ信号を受信するとしてもよい。
【００６０】
このアシスト情報は、例えば、携帯電話１０が存在すると推定される地域において現在時刻にＧＰＳ信号を受信することが可能なＧＰＳ衛星２０を示す情報、これら各ＧＰＳ衛星２０についての軌道情報、これら各ＧＰＳ衛星２０のＧＰＳ信号に含まれる情報を補正する情報などである。
【００６１】
なお、アシスト情報は、現在位置及び現在時刻を算出する度に毎回サーバ装置３０から取得する必要はなく、例えば、一度取得したアシスト情報を携帯電話１０に備えられる記憶部に所定の期間だけ保持しておき、この期間内では記憶部に保持されたアシスト情報を利用し得ＧＰＳ信号を捕捉するとしてもよい。また、図５においては、携帯電話１０がアシスト情報を取得するサーバ装置と、現在位置及び現在時刻を送出するサーバ装置とを同一の装置として図示しているが、これらは互いに異なる別個の装置であってもよい。
【００６２】
また、図４及び図５に示す例においては、受信したＧＰＳ信号に基づいて現在位置及び現在時刻を算出する処理が携帯電話１０自身によって行われる場合の例を示しているが、例えば図６に示すように、携帯電話１０によってＧＰＳ信号を捕捉・復調して得られる情報、すなわち現在位置及び現在時刻を算出する前のＧＰＳ捕捉情報を携帯電話１０からサーバ装置３０に対して送信し（Ｓ３０）、このＧＰＳ捕捉情報に基づいて、サーバ装置３０側で現在位置及び現在時刻を算出するとしてもよい。
【００６３】
このように、サーバ装置３０側で現在位置及び現在時刻を算出する構成とすることにより、これらの算出に要する演算能力を携帯電話１０側に備えることが不要となり、携帯電話１０に搭載する演算回路の回路規模や消費電力を低減することができる。なお、図６においては、携帯電話１０がアシスト情報を取得するサーバ装置と、ＧＰＳ捕捉情報を送信するサーバ装置とを同一の装置として図示しているが、これらは互いに異なる別個の装置であってもよい。
【００６４】
ところで、情報提供サービス１においては、サーバ装置３０が携帯電話１０から位置時刻情報を取得するに際して、上述のように、現在位置及び現在時刻を示す情報、アシスト情報、ＧＰＳ捕捉情報などが携帯電話１０とサーバ装置３０との間で授受される。これらの情報は、所定の時刻における携帯電話１０の現在位置を特定し得る情報であり、携帯電話１０がユーザによって携行されることを考慮すると、ユーザの行動を特定することが可能なユーザの重要な個人情報としての性質を有している。したがって、これらの情報がユーザの意図しない第三者によって傍受され、漏洩してしまうことを防止することが重要となる。
【００６５】
そこで、情報提供サービス１においては、携帯電話１０とサーバ装置３０との間で現在位置及び現在時刻を示す情報、アシスト情報、或いはＧＰＳ捕捉情報など、携帯電話１０によって受信したＧＰＳ信号から算出される現在位置及び現在時刻に関連した情報、或いはＧＰＳ信号から現在位置及び現在時刻を算出するために用いられる情報を授受するに際して、携帯電話１０とサーバ装置３０との間で認証を行い、この認証が正しく行われた場合に限って位置や時刻に関する情報の授受を行う構成とされている。
【００６６】
以下では、携帯電話１０とサーバ装置３０との間で行われる処理について、主として上述

した認証処理に注目し、その様々な処理の例について、図面を参照しながら順次説明する。

【００６７】

＜第１の処理例＞

まず、最も基本的な認証を行う第１の処理例について、図７に示すフロー図、及び図８に示す模式図を参照しながら説明する。なお、図８に示す模式図は、図７に示す一連の処理について、携帯電話１０における処理に注目して模式的に図示したものである。また、以下では、通信基地局５０及び通信ネットワーク４０を介して携帯電話１０とサーバ装置３０との間に通信経路が確立され、携帯電話１０とサーバ装置３０との間で各種情報の授受が可能な状態とされていることを前提とする。

【００６８】

この状態において、携帯電話１０のユーザによって現在位置に関連したサービスを利用することが要求され、サーバ装置３０が携帯電話１０から現在位置に関する情報の取得処理が開始されると、携帯電話１０及びサーバ装置３０は以下のように動作する。

【００６９】

先ずステップＳ１００において、サーバ装置３０は、携帯電話１０における認証処理を行うための認証情報を携帯電話１０に送信する。次に携帯電話１０は、サーバ装置３０から送信された認証情報をステップＳ１０１において受信する。次に携帯電話１０は、ステップＳ１０２において、この認証情報を利用して所定の認証アルゴリズムに基づいた認証処理を行い、その認証結果をサーバ装置３０に送信する。この認証処理は、携帯電話１０に備えられたＣＰＵ１０７が各種の演算処理を行うことによって実現される。また、認証処理に特化した認証回路を携帯電話１０に備え、この認証回路によって認証処理を行うとしてもよい。

【００７０】

次にサーバ装置３０は、ステップＳ１０３において、携帯電話１０から送信された認証結果を受信し、ステップＳ１０４において、携帯電話１０によって認証が正しく行われたか否かを判定する。この判定の結果、認証が許可されなかった場合には、携帯電話１０から現在位置を取得する一連の処理を終了する。認証が許可された場合には、ステップＳ１０５において、アシスト情報を携帯電話１０に対して送信する。

【００７１】

次に携帯電話１０は、ステップＳ１０６において、アシスト情報を受信する。そして、ステップＳ１０７において、ＧＰＳアンテナ１１３によってＧＰＳ信号を受信し、アシスト情報に基づいてＧＰＳ信号受信部１１４によりＧＰＳ信号を捕捉する。次に携帯電話１０は、ステップＳ１０８において、ＧＰＳ信号受信部１１４によって捕捉されたＧＰＳ信号に対して変調処理などを施すことにより現在位置及び現在時刻を算出する。なお、この算出処理は、ＧＰＳ信号受信部によって行うとしてもよいし、ＧＰＳ信号受信部からＧＰＳ捕捉情報を出力し、このＧＰＳ捕捉情報に基づいてＣＰＵ１０７により行うとしてもよい。

【００７２】

次に携帯電話１０は、ステップＳ１０９において、算出された現在位置及び現在時刻をサーバ装置３０に対して送信する。そして、サーバ装置３０は、ステップＳ１１０において、携帯電話１０から送信された現在位置及び現在時刻を受信する。

【００７３】

上述した一連の処理により、携帯電話１０からサーバ装置３０に対する現在位置及び現在時刻の送信処理が完了する。これ以後、サーバ装置３０は、携帯電話１０からなされた要求に応じて、現在位置に関する各種情報を携帯電話１０に送信するなどの処理を行う。

【００７４】

携帯電話１０及びサーバ装置３０は、上述のような一連の処理を行うことにより、認証情報を利用して認証処理を行った後にアシスト情報や現在位置及び現在時刻が授受される。したがって、携帯電話１０のユーザは、サーバ装置３０が正当な接続対象であることを保

証された状態で、行動を特定する重要な個人情報となる現在位置及び現在時刻を示す情報をサーバ装置３０に対して送信することができ、安心して現在位置に関する各種のサービスを享受することができる。

【００７５】

また、上述とは反対に携帯電話１０からサーバ装置３０に対して認証情報を送信し、サーバ装置３０側で受信した認証情報に基づいて認証処理を行うことによって、いわゆる相互認証を実現することができ、サーバ装置３０によってサービスを提供する事業者としても、上述の認証処理を行うことによって、携帯電話１０が正当なサービス提供対象であることを確認することができることから、現在位置に関する情報を安心して提供することができる。この点は、情報を提供するサービスに対して課金を行う場合などには、特に有効となる。

【００７６】

なお、図７に示す例においては、携帯電話１０側で認証処理を行った後に、サーバ装置３０から携帯電話１０に対してアシスト情報を送信する場合について図示している。ただし、例えば携帯電話１０が備えるＲＡＭ１１１や不揮発メモリ１１２などに最新のアシスト情報が予め登録されている場合などにおいて、携帯電話１０がサーバ装置３０からアシスト情報を取得する必要がない場合には、ステップＳ１０３乃至ステップＳ１０６の処理を省略して、ステップＳ１０２における認証処理の結果、認証が許可された場合にステップＳ１０７以降の処理を行うとすればよい。

【００７７】

また、アシスト情報は、認証が行われる以前にサーバ装置３０から携帯電話１０に対して送信するとしてもよい。ただし、アシスト情報に基づいて携帯電話１０の現在位置を大まかに特定し得る可能性を考慮すると、認証を行った後にアシスト情報を送信することが望ましい。

【００７８】

＜第２の処理例＞

つぎに、第１の処理例に基づいて、ステップＳ１０２における認証処理の一例を具体的に示す第２の処理例について、図９に示す模式図を参照して説明する。この第２の処理例は、ステップＳ１０２における認証処理として、携帯電話１０のユーザに正当な接続対象であるか否かを問い合わせることによって認証を行う場合の例であり、他の一連の処理については第１の処理例と同等である。このため、本例においては、第１の処理例と同等の処理については説明を省略し、図中においても同一の符号を付すこととする。なお、第２の処理例の説明以降、他の処理例についても説明するが、これら他の処理例についても同様にして特徴的な相違点のみについて説明することとし、図中においては他と同様の処理について同一の符号を付すこととする。

【００７９】

第２の処理例では、サーバ装置３０から送信された認証情報を携帯電話１０がステップＳ１０１において受信した後に、図９に示すステップＳ１５０において、この認証情報を携帯電話１０に備えられたＬＣＤ１０９に表示する。そして、表示された認証情報を携帯電話１０のユーザが確認し、サーバ装置３０が正当な接続対象であるか否かを判断して、入力操作部１０８に対する判断結果の入力操作を促す。そして携帯電話１０は、ステップＳ１５１において、入力操作部１０８により入力されたユーザによる操作に応じて、サーバ装置３０が正当な接続対象であるか否かを示す認証結果をサーバ装置３０に対して送信する。

【００８０】

すなわち、第２の処理例においては、携帯電話１０に備えられたＬＣＤ１０９によってサーバ装置３０からの認証情報をユーザに対して報知し、この認証情報に基づくユーザからの操作が入力操作部１０８によって入力されることにより、認証を許可するか否かが決定される。したがって、本例においては、サーバ装置３０に対して位置時刻情報を送信しても問題がないか否かをユーザに問い合わせることができ、ユーザの判断に応じて位置時刻

情報を送信するか否かを選択することができる。

【００８１】

なお、本例における認証情報としては、ユーザがサーバ装置３０を識別することが可能な情報であれば特に限定されるものではないが、例えば、サーバ装置３０の名称、電話番号、ＩＰアドレスなどを用いればよい。

【００８２】

また、本例においては、認証情報を携帯電話１０のＬＣＤ１０９に表示することによってユーザに対して報知しているが、認証情報の送信元であるサーバ装置３０をユーザが確認することが可能であれば特に報知するデバイスや方法に限定されるものでなく、例えば、ＬＣＤ１０９に限らず他の表示デバイスに表示するとしてもよいし、接続対象に対応した音声を出力したり、接続対象に対応してバイブレータを動作させることなどによってユーザに対する報知を行うとしてもよい。

【００８３】

＜第３の処理例＞

つぎに、第１の処理例に基づいて、ステップＳ１０２における認証処理の別の一例を具体的に示す第３の処理例として、図１０に示す模式図を参照して説明する。この第３の処理例は、認証情報として所定のデータ列情報、いわゆるパスワードを用いて、サーバ装置３０から送信されたパスワードと携帯電話１０の内部に予め記憶されたパスワードとを比較することにより認証を行う場合の例である。

【００８４】

第３の処理例では、図１０に示すように、携帯電話１０が認証情報としてのパスワードをサーバ装置３０から取得する。そして、ステップＳ２００において、サーバ装置３０から取得したパスワードと、携帯電話１０のＲＯＭ１１０、ＲＡＭ１１１、或いは不揮発メモリ１１２などに予め記憶されたパスワードとを比較し、これらが一致するか否かをＣＰＵ１０７によって判定する。この判定の結果、一致する場合には認証が許可されたものとし、一致しない場合には認証が許可されなかったものとして、この認証結果をサーバ装置３０に送信する。

【００８５】

なお、パスワードとしては、ユーザが意図しない第三者に知られておらず、認証処理に利用できる情報であれば特に限定されるものではない。また、接続対象となるサーバ装置３０が複数存在する場合には、各接続対象にそれぞれ対応した複数のパスワードを予め携帯電話１０内部に記憶しておけばよい。

【００８６】

また、パスワードをサーバ装置３０から携帯電話１０に対して送信するに際しては、このパスワードに対して暗号化処理を施すことが望ましい。具体的には、図１１に示すように、サーバ装置３０から送信するパスワードに対してサーバ装置３０側で暗号化処理を施した（ステップＳ２１０）後に携帯電話１０に対して送信し、暗号化されたパスワードを携帯電話１０により受信した後に、これに対して復号化処理を施し（ステップＳ２１１）、この後にステップＳ２００における認証処理を行う。

【００８７】

このように、暗号化処理を施すことにより、サーバ装置３０から携帯電話１０に対して送信されたパスワードが、ユーザの意図しない第三者によって例えば通信ネットワーク４０の途中で傍受され、漏洩してしまうことを防止することができる。

【００８８】

なお、上述した暗号化処理及び復号化処理は、携帯電話１０及びサーバ装置３０にそれぞれ備えられたＣＰＵ１０７及びＣＰＵ２００において所定の演算処理を行うことにより実現することができる。また、暗号化処理及び復号化処理は、ＣＰＵ１０７及びＣＰＵ２００によって実現するとせずに、これらの処理を専ら行う暗号回路を携帯電話１０及びサーバ装置３０に備え、この暗号回路によって実現するとしてもよい。

【００８９】

また、上述した暗号化処理及び復号化処理で採用する暗号方式としては、特に限定されるものではなく、携帯電話１０とサーバ装置３０との間で予め設定された任意の暗号方式を用いることができる。具体的な暗号方式の例としては、携帯電話１０とサーバ装置３０とのあいだで予め定められた共通の鍵を用いて暗号化・復号化を行う共通鍵暗号方式、通信相手に公開しない秘密鍵と通信相手に公開する公開鍵とを用いて暗号化・復号化を行う公開鍵暗号方式などを挙げることができる。また、各種の暗号方式を組み合わせて暗号化処理及び復号化処理を行うとしてもよい。

【００９０】

また、上述した暗号化処理及び復号化処理は、第２の処理例においてパスワードを送信する際のみに限定して有効なものではなく、携帯電話１０とサーバ装置３０との間で他の各種の情報を送受信するに際しても、これらの情報に対して暗号化を施すとしてもよい。これにより、携帯電話１０の現在位置に関する情報だけでなく、他の情報についても第三者による傍受或いは漏洩を防止することができる。

【００９１】

＜第４の処理例＞

ここで、認証情報としてのパスワードを授受する場合だけでなく、他の情報を送受信する場合にも暗号化を施す場合の一例について、図１２に模式的に示す第４の処理例について説明する。なお、図１２に示す例においては、携帯電話１０とサーバ装置３０との間で授受された認証情報としてのパスワードを用いて、他の情報、すなわちアシスト情報と現在位置及び現在時刻を示す情報とを授受する際に暗号化を施す場合について図示している。

【００９２】

この場合には、携帯電話１０とサーバ装置３０との間で認証処理が完了して認証が許可された後に、図７に示すステップＳ１０５においてアシスト情報を送信する際に、図１２に示すように、このアシスト情報に対してサーバ装置３０側で暗号化処理を施した後に送信する（Ｓ２２０）。そして、図７に示すステップＳ１０６において、暗号化されたアシスト情報を携帯電話１０により受信した後に、この暗号化されたアシスト情報に対して復号化処理を施し、このアシスト情報を取り出す（Ｓ２２１）。また、図７に示すステップＳ１０９において位置及び時刻を示す情報を送信する際に、図１２に示すように、この位置及び時刻を示す情報に対して携帯電話１０側で暗号化処理を施した後に送信する（Ｓ２２２）。そして、図７に示すステップＳ１１０において、暗号化された情報をサーバ装置３０により受信した後に、この暗号化された情報に対して復号化処理を施し、位置及び時刻を示す情報を取り出す（Ｓ２２３）。

【００９３】

上述のように、本例においては、認証を行う際に用いられる認証情報（本例ではパスワードが認証情報に相当する。）だけでなく、携帯電話１０とサーバ装置３０との間で授受される他の情報に対しても暗号化を施した状態で送受信している。このため、これらの情報がユーザの意図しない第三者によって傍受され、漏洩してしまうことを防止することができ、より安全に情報を送受信することができる。

【００９４】

なお、図１２に示す例においては、認証情報としてのパスワードをそのまま暗号化処理及び復号化処理する際の鍵として利用しているが、携帯電話１０及びサーバ装置３０の間で予め定められた所定の手順によってパスワードから生成された情報を鍵として用いることもできる。

【００９５】

＜第５の処理例＞

つぎに、共通鍵暗号方式を利用して携帯電話１０とサーバ装置３０との間で認証を行う場合の一例について、図１３に示す第５の処理例について説明する。本例の説明においては、認証処理の手順が特徴的であり、他の処理については第１の処理例と同等であることから、第１の処理例と同等の処理についての説明を省略するとともに、図１３においては図８と同一の符号を付すこととする。

【００９６】
第５の処理例では、図１３に示すように、サーバ装置３０から認証を開始する要求（認証要求）が携帯電話１０に対して送信されると、この認証要求を受信した携帯電話１０によって乱数を生成し、この乱数をサーバ装置３０に対して送信する（Ｓ２３０）。次に、サーバ装置３０は、携帯電話１０から送信された乱数を受信した後に、この乱数に対して、携帯電話１０との間で予め定められた共通の鍵、すなわち共通鍵を用いて暗号化を施すとともに、暗号化された乱数を携帯電話１０に送信する（Ｓ２３１）。
【００９７】
次に、携帯電話１０は、サーバ装置３０によって暗号化された乱数を受信して、これに対して共通鍵を用いた復号化処理を施す（Ｓ２３２）。次に、携帯電話１０は、サーバ装置３０から送信された乱数と、ステップＳ２３０において生成した元の乱数とが一致するか否かを判定する。この判定の結果、一致する場合には認証が許可されたものとし、一致しない場合には認証が許可されなかったものとして、この認証結果をサーバ装置３０に送信する（Ｓ２３３）。
【００９８】
上述のように、本例においては、携帯電話１０側で生成した乱数と、この乱数をサーバ装置３０側で暗号化したものとを比較することによって、携帯電話１０が有する共通鍵と同一の共通鍵をサーバ装置３０が有しているか否かを判断し、これによってサーバ装置３０が接続対象であるか否かという正当性を認証している。なお、共通鍵は、携帯電話１０に備えられたＲＯＭ１１０、ＲＡＭ１１１、或いは不揮発メモリ１１２に予め記憶しておくことができる。また、サーバ装置３０側においては、携帯電話１０が有する共通鍵と同一の共通鍵をＲＡＭ２０１、ＲＯＭ２０２、或いはＨＤＤ２０３に予め記憶しておくことができる。
【００９９】
なお、本例においては、携帯電話１０側で乱数を生成する処理と、暗号化された乱数が元の乱数と一致するか否かを判定することによる認証処理とを携帯電話１０側で行っているが、これらの処理をサーバ装置３０側で行うようにすることによって、携帯電話１０が接続対象であるか否かという正当性をサーバ装置３０側から認証することもできる。また、携帯電話１０側からの認証と、サーバ装置３０側からの認証との双方を行うことにより、いわゆる相互認証を容易に実現することができる。
【０１００】
＜第６の処理例＞
つぎに、上述した第５の処理例で説明した共通鍵暗号方式を利用して、認証を行う他に、アシスト情報と、位置及び時刻を示す情報とを授受する際に暗号化を施す場合について、図１４に示す第６の処理例について説明する。なお、本例においては、図１３に示す第５の処理例と比較して、ステップＳ２３２における復号化処理以降が特徴的である。
【０１０１】
第６の処理例では、ステップＳ２３２における復号化処理の後に、図１４に示すステップＳ２４０において、サーバ装置３０から送信された乱数と、ステップＳ２３０において生成した元の乱数とが一致するか否かを携帯電話１０側で判定する。そして、この判定の結果、一致しない場合には認証が許可されなかったものとして、この旨を示すメッセージ「認証エラー」をサーバ装置３０に送信する。また、判定の結果が一致する場合には、例えば携帯電話１０に備えられるＣＰＵ１０７、或いは認証回路、暗号回路などによって通信鍵を生成する（Ｓ２４１）。この通信鍵としては、携帯電話１０とサーバ装置３０との間で送受信する情報に対して暗号化を行う際に用いることができれば任意であるが、例えば、先に生成した乱数に基づいて、予め定められた所定の手順により生成されるものであってもよい。
【０１０２】
次に携帯電話１０は、ステップＳ２４２において、通信鍵を共通鍵によって暗号化した後に、暗号化された通信鍵をサーバ装置３０に送信する。次に、サーバ装置３０は、ステッ

プＳ２４３において、暗号化された通信鍵を携帯電話１０から受信して共通鍵を用いて復号化し、通信鍵を取得する。そして、サーバ装置３０は、アシスト情報を携帯電話１０に対して送信するに際して、ステップＳ２４４において、このアシスト情報を通信鍵で暗号化する。

【０１０３】

一方、携帯電話１０は、暗号化されたアシスト情報を受信すると、これを通信鍵を用いて復号化してアシスト情報を取り出す（Ｓ２４５）。そして、携帯電話１０におけるステップＳ１０６以降においては、取り出した平文のアシスト情報を利用する。

【０１０４】

また、ステップＳ１０９において携帯電話１０から位置及び時刻に関する情報を送信するに際しては、ステップＳ２４１において生成した通信鍵を用いて暗号化を施し、暗号化された情報をサーバ装置３０に対して送信する（Ｓ２４６）。そして、サーバ装置３０は、暗号化された位置及び時刻に関する情報を受信すると、この情報をステップＳ２４３により得られた通信鍵を用いて復号化し、携帯電話１０の位置及び時刻に関する情報を取り出す（Ｓ２４７）。

【０１０５】

上述のように、本例においては、携帯電話１０側でサーバ装置３０の認証を行うだけでなく、携帯電話１０とサーバ装置３０との間で授受される情報に対して暗号化を施した状態で送受信している。このため、これらの情報がユーザの意図しない第三者によって傍受され、漏洩してしまうことを防止することができ、より安全に情報を送受信することができる。

【０１０６】

＜第７の処理例＞

つぎに、公開鍵暗号方式を利用して携帯電話１０とサーバ装置３０との間で認証を行う場合の一例について、図１５に示す第７の処理例について説明する。本例の説明においては、認証処理の手順が特徴的であり、他の処理については第１の処理例と同等であることから、第１の処理例と同等の処理についての説明を省略するとともに、図１５においては図８と同一の符号を付すこととする。

【０１０７】

第７の処理例では、図１５に示すように、サーバ装置３０が携帯電話１０から現在位置に関する情報を取得するに際しての認証処理が開始されると、例えばサーバ装置３０を識別する所定の識別情報に対して、サーバ装置３０自身の秘密鍵を利用して暗号化処理を施すことにより電子署名を生成し、この電子署名を元の識別情報とともに携帯電話１０に対して送信される（Ｓ２５０）。

【０１０８】

次に、携帯電話１０は、サーバ装置３０から送信された情報を受信し、受信した情報に含まれる識別情報に基づいて、サーバ装置３０の公開鍵を取得する。そして、サーバ装置３０の公開鍵を用いて電子署名を検証し、元の識別情報を確認する。そして、電子署名が正しく検証できた場合には、受信した情報が間違いなくサーバ装置３０から送信されたものであると認証する。また、サーバ装置３０の公開鍵を用いて電子署名が正しく検証できなかった場合には、受信した情報の送信元がサーバ装置３０ではないと判断して、認証を許可しない。そして、携帯電話１０は、この認証結果をサーバ装置３０に送信する（Ｓ２５１）。

【０１０９】

以上のようにして、公開鍵暗号方式を利用して電子署名を授受することにより、携帯電話１０とサーバ装置３０との間で認証を行うことができる。

【０１１０】

なお、携帯電話１０がサーバ装置３０の公開鍵を取得するに際しては、例えば、接続対象となる複数のサーバ装置に対応した公開鍵を携帯電話１０の内部に保持しておき、受信した識別情報に応じて、保持された公開鍵の中から電子署名の検証に用いる公開鍵を選出す

る構成とすることができる。また、例えば、携帯電話１０のネットワーク機能を利用して、通信ネットワーク４０に接続された他の情報処理装置に対してサーバ措置３０の公開鍵を問い合わせることにより、この情報処理装置から公開鍵を取得するとしてもよい。

【０１１１】

公開鍵を携帯電話１０の内部に保持しておく場合には、接続対象となるサーバ装置の数が増大するに従って、公開鍵を記憶しておくために要するメモリ領域が増大してしまうが、他の情報処理装置に対して公開鍵の問い合わせを行う必要がないことから、比較的高速に認証処理を行うことができる。また、他の情報処理装置に対して公開鍵の問い合わせを行う場合には、問い合わせを行う分だけ時間を要するが、携帯電話１０内に多数の公開鍵を保持しておく必要がないことから、少ないメモリ容量で多数の接続対象との間での認証処理を行うことができる。なお、これらを組み合わせて、使用頻度が高い公開鍵のみ携帯電話１０の内部に保持しておき、必要に応じて外部の情報処理装置に対して問い合わせを行う構成としてもよい。

【０１１２】

＜第８の処理例＞

つぎに、第７の処理例の構成を発展させて、より強固な暗号化を図るとともに、より確実に認証を行うことが可能な第８の処理例について、図１６を参照しながら説明する。

【０１１３】

第８の処理例では、図１６に示すように、サーバ装置３０が携帯電話１０から現在位置に関する情報を取得するに際しての認証処理が開始されると、例えばサーバ装置３０を識別する所定の識別情報に対して、サーバ装置３０自身の秘密鍵を利用して暗号化処理を施すことにより電子署名を生成し、この電子署名を元の識別情報に付加する（Ｓ２６０）。次にサーバ装置３０は、ステップＳ２６０での処理により生成された情報に対して、接続対象となる携帯電話１０の公開鍵を利用して暗号化処理を施した後に、これを携帯電話１０に対して送信する（Ｓ２６１）。

【０１１４】

携帯電話１０は、サーバ装置３０から暗号化された情報を受信すると、この情報を携帯電話１０自身の秘密鍵を用いて復号化する（Ｓ２６２）。次に携帯電話１０は、ステップＳ２６２での処理により復号化された情報に含まれる識別情報に基づいて、サーバ装置３０の公開鍵を取得する。そして、サーバ装置３０の公開鍵を用いて電子署名を検証後、元の識別情報を一致するか否かを確認する。そして、電子署名が正しく検証できた場合には、受信した情報が間違いなくサーバ装置３０から送信されたものであると認証する。また、サーバ装置３０の公開鍵を用いて電子署名が正しく検証できなかった場合には、受信した情報の送信元がサーバ装置３０ではないと判断して、認証を許可しない。そして、携帯電話１０は、この認証結果をサーバ装置３０に送信する（Ｓ２６３）。

【０１１５】

本例においては、サーバ装置３０の電子署名も含めて携帯電話１０の公開鍵によって暗号化されていることから、携帯電話１０とサーバ装置３０との間の通信経路が第三者に傍受された場合であっても、サーバ装置３０の電子署名を検出することができない。したがって、第三者に対して、サーバ装置３０から携帯電話１０に対する認証要求が行われたことが漏洩してしまうことがない。

【０１１６】

また、本例においては、公開鍵暗号方式の暗号化が２重に行われており、非常に強固な暗号化を施すことができる。また、携帯電話１０及びサーバ装置３０の双方の秘密鍵を用いて認証が行われており、携帯電話１０とサーバ装置３０とがそれぞれ互いに接続対象を特定することが可能であり、いわゆる相互認証を実現することができる。

【０１１７】

＜第９の処理例＞

つぎに、上述した第７の処理例で説明した公開鍵暗号方式を利用して、認証を行う他に、アシスト情報と、位置及び時刻を示す情報とを授受する際に暗号化を施す場合について、

図１７に示す第９の処理例について説明する。なお、本例においては、図１５に示す第７の処理例と比較して、ステップＳ２５１における電子署名の検証処理以降が特徴的である。

【０１１８】

第９の処理例では、ステップＳ２５１における電子署名の検証処理の後に、図１７に示すステップＳ２７０において、サーバ装置３０から取得した電子署名が正しいものであるか否かを判定する。そして、この判定の結果、正しくない場合には認証が許可されなかったものとして、この旨を示すメッセージ「認証エラー」をサーバ装置３０に送信する。また、判定の結果、電子署名が正しいものであった場合には、例えば携帯電話１０に備えられるＣＰＵ１０７、或いは認証回路、暗号回路などによって通信鍵を生成する（Ｓ２７１）。この通信鍵としては、携帯電話１０とサーバ装置３０との間で送受信する情報に対して暗号化を行う際に用いることができれば任意であるが、例えば、予め定められた所定の手順に基づいて、接続対象との通信経路が確立される度に（すなわちセッション毎に）生成されるものであってもよい。

【０１１９】

次に携帯電話１０は、ステップＳ２７２において、通信鍵をサーバ装置３０の公開鍵によって暗号化した後に、暗号化された通信鍵をサーバ装置３０に送信する。次に、サーバ装置３０は、ステップＳ２７３において、暗号化された通信鍵を携帯電話１０から受信して、サーバ装置３０自身の秘密鍵を用いて復号化し、通信鍵を取得する。そして、サーバ装置３０は、アシスト情報を携帯電話１０に対して送信するに際して、ステップＳ２７４において、このアシスト情報を通信鍵で暗号化する。

【０１２０】

一方、携帯電話１０は、暗号化されたアシスト情報を受信すると、これを通信鍵を用いて復号化してアシスト情報を取り出す（Ｓ２７５）。そして、携帯電話１０におけるステップＳ１０６以降においては、取り出した平文のアシスト情報を利用する。

【０１２１】

また、ステップＳ１０９において携帯電話１０から位置及び時刻に関する情報を送信するに際しては、ステップＳ２７１において生成した通信鍵を用いて暗号化を施し、暗号化された情報をサーバ装置３０に対して送信する（Ｓ２７６）。そして、サーバ装置３０は、暗号化された位置及び時刻に関する情報を受信すると、この情報をステップＳ２７３により得られた通信鍵を用いて復号化し、携帯電話１０の位置及び時刻に関する情報を取り出す（Ｓ２７７）。

【０１２２】

上述のように、本例においては、認証を行う際に授受される情報に対してだけでなく、携帯電話１０とサーバ装置３０との間で授受される他の情報に対しても暗号化を施した状態で送受信している。このため、これらの情報がユーザの意図しない第三者によって傍受され、漏洩してしまうことを防止することができ、より安全に情報を送受信することができる。

【０１２３】

＜第１０の処理例＞

つぎに、第１の処理例に基づいて、携帯電話１０からサーバ装置３０に対して、現在位置及び現在時刻を直接示す情報を送信せずに、サーバ装置３０から送信された所定の条件について判定した結果のみを送信する場合の一例について、図１８に示すフロー図を参照して説明する。この第１０の処理例では、所定の条件についての判定結果をサーバ装置３０に対して送信する点のみ第１の処理例と異なるので、第１の処理例と同等の処理については説明を省略し、図中においても同一の符号を付すこととする。

【０１２４】

第１０の処理例では、図１８に示すようにステップＳ１００乃至ステップＳ１０４の処理によって認証が許可されると、ステップＳ１０５において、サーバ装置３０からアシスト情報とともに、位置及び時刻に関する所定の条件を示す条件情報が携帯電話１０に対して

送信される。そして、携帯電話１０は、ステップＳ１０６乃至ステップＳ１０８の処理により、携帯電話１０の現在位置及び現在時刻を算出した後に、ステップＳ２８０において、サーバ装置３０から取得した条件情報に基づいて、例えばＣＰＵ１０７によって条件の判定を行う。

【０１２５】

ここで、「位置及び時刻に関する所定の条件」を示す条件情報とは、以下のようなものである。すなわち、例えば、「所定の緯度及び経度を中心として所定の半径以内の範囲」、「所定の緯度及び経度により表される２点を直径とする円の内部」などのように所定の位置範囲を示す位置情報、所定の年月日或いは時刻を示す時刻情報、或いはこれら位置情報と時刻情報を組み合わせた情報である。

【０１２６】

そして、ステップＳ２８０においては、ＧＰＳ信号から算出された位置及び時刻が、サーバ装置３０から取得した条件情報に含まれる条件に適合するか否かを判定する。次に携帯電話１０は、ステップＳ１０９において、ステップＳ２８０における判定結果、すなわち現在位置或いは現在時刻が条件に適合しているか否かを示す情報をサーバ装置３０に送信する。そして、サーバ装置３０は、この情報（判定結果）をステップＳ１１０で受信し、携帯電話１０が、条件情報を満足する状態であるか否か、すなわち所定の時刻に所定の位置範囲に存在するか否かを知る。

【０１２７】

上述のように、本例においては、携帯電話１０の現在位置及び現在時刻を直接示す情報をサーバ装置３０に送信せずに、サーバ装置３０から位置及び時刻に関する条件についての判定結果を示す情報のみを送信している。したがって、本例では、認証処理を行うことにより第三者に対する情報の漏洩を防止した上で、ユーザの行動を詳細に特定し得る高精度な現在位置や現在時刻をサーバ装置３０に送信することなく、サーバ装置３０からの問い合わせに応答することができる。

【０１２８】

したがって、本例によれば、携帯電話１０の現在位置及び現在時刻を不必要に高い精度でサーバ装置３０側に特定されてしまうことを防止することができる。このため、携帯電話１０のユーザのプライバシーを効果的に保護することができる。

【０１２９】

以下、本例に係る情報提供サービス１を利用した場合の具体的な一例について説明する。例えば、携帯電話１０を携行している社員の所在を、この社員の上司がサーバ装置３０によって問い合わせを行う場合を想定する。この場合、例えば、「会社付近」を示す位置範囲を条件情報としてサーバ装置３０から携帯電話１０に対して送信すると、携帯電話１０を携行する社員が条件に適合する位置に存在すれば、この旨を示す結果をサーバ装置３０側で取得を得ることができ、上司は社員が会社に出社しているものと推察することができる。一方、社員が会社付近に存在しない場合には、条件に適合しなかったことを示す結果がサーバ装置３０側で得られるものの、この社員が現在何処にいるのかといったことを上司に知られることがない。したがって、会社に出社していない社員のプライバシーを保護することができる。

【０１３０】

＜第１１の処理例＞

つぎに、上述した第１０の処理例で説明した条件情報が予め携帯電話１０の内部に保持されている場合に可能な処理の一例として示す第１１の処理例について、図１９に示すフロー図を参照して説明する。

【０１３１】

この第１１の処理例では、図１９に示すように、ＧＰＳ信号を受信して現在位置及び現在時刻を算出する処理を携帯電話１０によって所定の時間間隔で繰り返し行うことを想定する。また、本例では、図２０に示すような条件情報が予め携帯電話１０の内部に保持されているものとする。この条件情報は、図２０に示すように、所定の位置範囲を示す位置情

報、所定の年月日或いは時刻を示す時刻情報、或いはこれら位置情報と時刻情報を組み合わせた情報からなる位置時刻条件と、各位置時刻条件に対応した接続対象との間で行われる認証処理に必要となる認証情報との組み合わせを１つの情報として、この情報を１つ又は複数備える形で携帯電話１０の内部に保持される。条件情報は、例えば、携帯電話１０に備えられるＲＯＭ１１０、ＲＡＭ１１１、或いは不揮発メモリ１１２などに記憶される。

【０１３２】

第１１の処理例において、携帯電話１０は、ステップＳ２９０において、ＧＰＳアンテナ１１３によってＧＰＳ信号を受信し、アシスト情報に基づいてＧＰＳ信号受信部１１４によってＧＰＳ信号を捕捉する。なお、本例においては、アシスト情報が予め携帯電話１０の内部に保持されているものとする。次に携帯電話１０は、ステップＳ２９１において、ＧＰＳ信号受信部１１４によって捕捉されたＧＰＳ信号に対して変調処理などを施すことにより現在位置及び現在時刻を算出する。

【０１３３】

次にステップＳ２９２において、携帯電話１０は、例えばＣＰＵ１０７によって条件情報を参照することにより、現在位置及び現在時刻に適合する条件が存在するか否かを判定する。この判定の結果、適合する条件が存在しない場合には、所定の時間だけ待機した後に、ステップＳ２９０に処理を戻し、ＧＰＳ信号の受信処理と位置及び時刻の算出処理とを所定の時間間隔で繰り返し行う。一方、適合する条件が存在する場合には、処理をステップＳ２９３に進める。

【０１３４】

ステップＳ２９３において、携帯電話１０は、条件情報を参照することにより、ステップＳ２９２における判定処理で適合した条件に対応した認証情報を取得し、この認証情報を用いてサーバ装置３０との間で認証処理を行う。

【０１３５】

なお、この認証処理に対応したサーバ装置３０側での処理を図１９においてステップＳ２９４として示す。このステップＳ２９３及びステップＳ２９４における携帯電話１０とサーバ装置３０との間で行われる認証処理は、特にその手順について限定されるものではなく、先に説明した処理例におけるいずれかの認証処理を行ったり、或いは先に説明した処理例における認証処理を組み合わせて行うなどとすればよい。

【０１３６】

また、携帯電話１０における認証処理は、携帯電話１０に備えられたＣＰＵ１０７が各種の演算処理を行うことによって実現される。また、認証処理に特化した認証回路やＤＳＰ（Digital Signal Processor）などを携帯電話１０に備え、この認証回路やＤＳＰによって認証処理を行うとしてもよい。同様にして、サーバ装置３０における認証処理は、サーバ装置３０に備えられたＣＰＵ２００が各種の演算処理を行うことによって実現される。また、認証処理に特化した認証回路やＤＳＰ（Digital Signal Processor）などをサーバ装置３０に備え、この認証回路やＤＳＰによって認証処理を行うとしてもよい。

【０１３７】

サーバ装置３０との間での認証処理が許可されると、ステップＳ２９５において、携帯電話１０は、ステップＳ２９２での判定処理で適合した条件を識別する条件識別情報をサーバ装置３０に送信する。次にステップＳ２９６において、サーバ装置３０は、携帯電話１０から送信された条件識別情報を受信し、この条件識別情報に含まれる情報に基づいて、いずれの条件に適合したかを知る。

【０１３８】

上述のように、本例では、携帯電話１０が位置及び時刻に関する所定の条件に適合したことをサーバ装置３０に対して通知するに際して、携帯電話１０の内部に保持された条件情報が参照されている。このため、携帯電話１０のユーザは、この条件情報を例えばＬＣＤ１０９に表示させるなどして容易に確認することができる。また、ユーザ自身が所望とする条件のみを条件情報として登録したり、ユーザが望まない条件を条件情報から削除する

などの操作を実現することも容易である。

【０１３９】

したがって、本例では、位置及び時刻に関する情報がユーザの意図に反してサーバ装置３０に送信されてしまうことを防止することができ、ユーザの行動を特定し得る個人情報を保護するとともに、位置及び時刻に関連したサービスの利用に際してユーザの安心感を獲得することができる。

【０１４０】

以下、本例に係る情報提供サービス１を利用した場合の具体的な一例について説明する。例えば、携帯電話１０のユーザが、所定の店舗Ａについての特売情報を取得するサービスを享受する場合を想定する。

【０１４１】

この場合、例えば、「店舗Ａを中心として半径１０ｍ以内」という位置範囲と、店舗Ａの特売情報を提供するサーバ装置との間で認証を行うための認証情報との組み合わせを、条件情報として携帯電話１０の内部に予め登録しておく。この状態の下で、携帯電話１０を携行するユーザが店舗Ａの近辺まで移動すると、携帯電話１０は、店舗Ａに関する条件が適合したと判定して、認証情報に基づいて所定のサーバ装置との間で認証を行い、店舗Ａに関する条件が適合したことを示す条件識別情報をサーバ装置に対して送信する。

【０１４２】

そして、サーバ装置は、受信した条件識別情報に基づいて、店舗Ａに関する特売情報を携帯電話１０に対して送信する。これにより、携帯電話１０のユーザは、店舗Ａに近づくだけで、この店舗Ａに関する情報を携帯電話１０によって知ることができる。また、例えば、サーバ装置から店舗Ａで利用可能な割引チケットに関する情報を携帯電話１０に対して送信し、携帯電話１０でこの割引チケットを表示した状態で店舗Ａの店員に提示することにより、店舗Ａにて割引サービスを享受することが可能なサービスの提供を行うとしてもよい。

【０１４３】

＜第１２の処理例＞

つぎに、図２０に示すような条件情報が予め携帯電話１０の内部に保持されている場合に可能な処理の別の一例として示す第１２の処理例について、図２１に示すフロー図を参照して説明する。この第１２の処理例では、図２１に示すように、ＧＰＳ信号を受信して現在位置及び現在時刻を算出する処理を携帯電話１０によって所定の時間間隔で繰り返し行うことを想定する。

【０１４４】

第１２の処理例において、携帯電話１０は、ステップＳ３００において、ＧＰＳアンテナ１１３によってＧＰＳ信号を受信し、アシスト情報に基づいてＧＰＳ信号受信部１１４によってＧＰＳ信号を捕捉する。なお、本例においては、アシスト情報が予め携帯電話１０の内部に保持されているものとする。次に携帯電話１０は、ステップＳ３０１において、ＧＰＳ信号受信部１１４によって捕捉されたＧＰＳ信号に対して変調処理などを施すことにより現在位置及び現在時刻を算出する。

【０１４５】

ここで、サーバ装置３０において、携帯電話１０から位置及び時刻に関する情報を取得する処理が開始され、ステップＳ３０２で示すように認証情報を携帯電話１０に対して送信された場合を想定すると、携帯電話１０は、ステップＳ３０３において認証情報を受信する。

【０１４６】

次に、ステップＳ３０４において、携帯電話１０は、例えばＣＰＵ１０７によって認証情報を受信したか否かを判定する。この判定の結果、受信していない場合には、所定の時間だけ待機した後に、ステップＳ３００に処理を戻し、ＧＰＳ信号の受信処理と位置及び時刻の算出処理とを所定の時間間隔で繰り返し行う。また、受信している場合には、処理をステップＳ３０５に進める。

【０１４７】
ステップＳ３０５において、携帯電話１０は、受信した認証情報に基づいて、サーバ装置３０との間で認証処理を行う。なお、この認証処理に対応したサーバ装置３０側での処理を図２１においてステップＳ３０６で示す。このステップＳ３０５及びステップＳ３０６における携帯電話１０とサーバ装置３０との間で行われる認証処理は、特にその手順に限定されるものではなく、先に説明した処理例におけるいずれかの認証処理、或いは先に説明した処理例における認証処理を組み合わせて行うとすればよい。
【０１４８】
サーバ装置３０との間での認証処理が許可されると、ステップＳ３０７において、携帯電話１０は、例えばＣＰＵ１０７によって条件情報を参照することにより、受信した認証情報に対応した位置及び時刻に関する条件を取得するとともに、現在位置及び現在時刻が条件に適合するか否かを判定する。
【０１４９】
次に携帯電話１０は、ステップＳ３０８において、ステップＳ３０７における判定結果、すなわち現在位置或いは現在時刻が条件に適合しているか否かを示す情報をサーバ装置３０に送信する。そして、サーバ装置３０は、この情報（判定結果）をステップＳ３０９で受信し、携帯電話１０が、条件情報を満足する状態であるか否か、すなわち所定の時刻に所定の位置範囲に存在するか否かを知る。
【０１５０】
上述のように、本例においては、携帯電話１０の現在位置及び現在時刻を直接示す情報をサーバ装置３０に送信せずに、サーバ装置３０から位置及び時刻に関する条件についての判定結果を示す情報のみを送信している。したがって、本例では、認証処理を行うことにより第三者に対する情報の漏洩を防止した上で、ユーザの行動を詳細に特定し得る高精度な現在位置や現在時刻をサーバ装置３０に送信することなく、サーバ装置３０からの問い合わせに応答することができる。
【０１５１】
したがって、本例によれば、携帯電話１０の現在位置及び現在時刻を不必要に高い精度でサーバ装置３０側に特定されてしまうことを防止することができる。このため、携帯電話１０のユーザのプライバシーを効果的に保護することができる。
【０１５２】
また、本例では、携帯電話１０が位置及び時刻に関する所定の条件に適合したことをサーバ装置３０に対して通知するに際して、携帯電話１０の内部に保持された条件情報が参照されている。このため、携帯電話１０のユーザは、この条件情報を例えばＬＣＤ１０９に表示させるなどして容易に確認することができる。また、ユーザ自身が所望とする条件のみを条件情報として登録したり、ユーザが望まない条件を条件情報から削除するなどの操作を実現することも容易である。
【０１５３】
したがって、本例では、位置及び時刻に関する情報がユーザの意図に反してサーバ装置３０に送信されてしまうことを防止することができ、ユーザの行動を特定し得る個人情報を保護するとともに、位置及び時刻に関連したサービスの利用に際してユーザの安心感を獲得することができる。
【０１５４】
＜第１３の処理例＞
つぎに、携帯電話１０からサーバ装置３０に対して送信する位置及び時刻に関する情報の精度を変更する場合の処理の一例として示す第１３の処理例について、図２２に示すフロー図を参照して説明する。
【０１５５】
この第１３の処理例では、図２２に示すように、ＧＰＳ信号を受信して現在位置及び現在時刻を算出する処理を携帯電話１０によって所定の時間間隔で繰り返し行うことを想定する。また、本例では、図２３に示すような精度変更情報が予め携帯電話１０の内部に保持

されているものとする。この精度変更情報は、図２３に示すように、接続対象となるサーバ装置との間で認証を行う際に必要となる認証情報と、接続対象毎に設定された精度情報との組み合わせを１つの情報として、この情報を１つ又は複数備える形で携帯電話１０の内部に保持される。精度情報は、位置及び時刻に関する情報を送信する際に、この情報の精度を指定する情報である。また、精度変更情報は、例えば、携帯電話１０に備えられるＲＯＭ１１０、ＲＡＭ１１１、或いは不揮発メモリ１１２などに記憶される。

【０１５６】

第１３の処理例において、携帯電話１０は、ステップＳ３１０において、ＧＰＳアンテナ１１３によってＧＰＳ信号を受信し、アシスト情報に基づいてＧＰＳ信号受信部１１４によってＧＰＳ信号を捕捉する。なお、本例においては、アシスト情報が予め携帯電話１０の内部に保持されているものとする。次に携帯電話１０は、ステップＳ３１１において、ＧＰＳ信号受信部１１４によって捕捉されたＧＰＳ信号に対して変調処理などを施すことにより現在位置及び現在時刻を算出する。

【０１５７】

ここで、サーバ装置３０において、携帯電話１０から位置及び時刻に関する情報を取得する処理が開始され、ステップＳ３１２で示すように認証情報を携帯電話１０に対して送信された場合を想定すると、携帯電話１０は、ステップＳ３１３において認証情報を受信する。

【０１５８】

次に、ステップＳ３１４において、携帯電話１０は、例えばＣＰＵ１０７によって認証情報を受信したか否かを判定する。この判定の結果、受信していない場合には、所定の時間だけ待機した後に、ステップＳ３１０に処理を戻し、ＧＰＳ信号の受信処理と位置及び時刻の算出処理とを所定の時間間隔で繰り返し行う。また、受信している場合には、処理をステップＳ３１５に進める。

【０１５９】

ステップＳ３１５において、携帯電話１０は、受信した認証情報に基づいて、サーバ装置３０との間で認証処理を行う。なお、この認証処理に対応したサーバ装置３０側での処理を図２２においてステップＳ３１６で示す。このステップＳ３１５及びステップＳ３１６における携帯電話１０とサーバ装置３０との間で行われる認証処理は、特にその手順に限定されるものではなく、先に説明した処理例におけるいずれかの認証処理、或いは先に説明した処理例における認証処理を組み合わせて行うとすればよい。

【０１６０】

サーバ装置３０との間での認証処理が許可されると、ステップＳ３１７において、携帯電話１０は、例えばＣＰＵ１０７によって精度変更情報を参照することにより、受信した認証情報に対応した精度情報を取得する。次にステップＳ３１８において、携帯電話１０は、例えばＣＰＵ１０７によって、ステップＳ３１１で算出された現在位置及び現在時刻に対して、精度を変更する処理を行う。

【０１６１】

次に携帯電話１０は、ステップＳ３１９において、ステップＳ３１８において精度を変更した位置及び時刻をサーバ装置３０に送信する。そしてステップＳ３２０において、サーバ装置３０は、携帯電話１０の位置及び時刻を受信する。

【０１６２】

上述のように、本例では、サーバ装置３０が正当な接続対象であるか否かを認証するとともに、ＧＰＳ信号に基づいて算出された位置及び時刻の精度を、精度変更情報を参照することにより接続対象となるサーバ装置毎に変更した後に、このサーバ装置に対して送信している。

【０１６３】

現在では、ＧＰＳ機能を利用することにより、数十メートルから数メートル程度の誤差で極めて高精度に現在位置を算出することが可能。このため、算出された高精度の位置情報をそのままの状態でサーバ装置３０に対して送信してしまうと、携帯電話１０を携行する

ユーザの行動が不必要に高い精度で特定されてしまうという点で問題が生じる場合がある。

【０１６４】

しかしながら、本例では、上述のように、接続対象となるサーバ装置毎に精度を変更して送信することができ、例えば、利用するサービス、或いは接続対象となるサーバ装置の信頼度などに応じて、高い精度のままで位置及び時刻に関する情報を送信したり、精度を劣化させて位置及び時刻に関する情報を送信することなどが可能である。

【０１６５】

なお、本例においては、精度変更情報を参照することによって、受信した認証情報に応じて精度を変更する場合の処理例について説明したが、ユーザからの要求に応じて、或いは接続対象とするサーバ装置に応じて位置及び時刻の精度を変更した後に、これをサーバ装置に送信することが可能であれば、特に処理の手順について限定されるものではない。

【０１６６】

また、本例においては、ＣＰＵ１０７が精度を変更するものとして説明したが、例えば、ＧＰＳ信号受信部１１４によってＧＰＳ信号から位置及び時刻を算出する際に精度を変更するとしてもよいし、位置及び時刻の精度を変更する演算処理を専ら行う回路を携帯電話１０に備えるとしてもよい。

【０１６７】

また、精度を変更する具体的な手法としては、例えば、位置や時刻を示す情報の値に対して、いわゆる切り捨て処理や丸め込み処理を施すとしてもよいし、無意味な値を加減するなどして誤差を拡大する処理などを施すとしてもよい。

【０１６８】

＜第１４の処理例＞

つぎに、携帯電話１０とサーバ装置３０との間で授受される情報に対して、全く新規な方式で暗号化処理又は復号化処理を施す第１４の処理例について、図２４に示す模式図を参照しながら説明する。なお、図２４に示す模式図は、携帯電話１０で行われる処理に注目して模式的に図示したものである。以下では、通信基地局５０及び通信ネットワーク４０を介して携帯電話１０とサーバ装置３０との間に通信経路が確立され、携帯電話１０とサーバ装置３０との間で各種情報の授受が可能な状態とされていることを前提とする。また、以下では、暗号化処理及び復号化処理を行うに際して特徴的な点のみについて説明及び図示する。

【０１６９】

この状態において、携帯電話１０は、図２４に示すステップＳ３３０において、ＧＰＳアンテナ１１３によってＧＰＳ信号を受信し、アシスト情報に基づいてＧＰＳ信号受信部１１４によりＧＰＳ信号を捕捉する。なお、本例においては、アシスト情報が予め携帯電話１０の内部に保持されているものとするが、このアシスト情報を先に説明した処理例と同様にしてサーバ装置３０から取得するとしてもよい。

【０１７０】

次に携帯電話１０は、ステップＳ３３１において、ＧＰＳ信号受信部１１４によって捕捉されたＧＰＳ信号に対して変調処理などを施すことにより現在位置及び現在時刻を算出する。なお、この算出処理は、ＧＰＳ信号受信部１１４によって行うとしてもよいし、ＧＰＳ信号受信部１１４からＧＰＳ捕捉情報を出力し、このＧＰＳ捕捉情報に基づいてＣＰＵ１０７により行うとしてもよい。

【０１７１】

以上のようにして、携帯電話１０がＧＰＳ機能を利用して現在位置及び現在時刻を取得した状態の下で、暗号処理を行うサービスを享受することをユーザによって要求された場合、或いは、サーバ装置３０から暗号処理を行うことを要求された場合に、携帯電話１０は、ステップＳ３３２において、サーバ装置３０との間で認証処理を行う。なお、この認証処理に対応したサーバ装置３０側での処理を図２４においてステップＳ３３３として示す。

【０１７２】
このステップＳ３３２及びステップＳ３３３における携帯電話１０とサーバ装置３０との間で行われる認証処理は、特にその手順について限定されるものではなく、先に説明した処理例におけるいずれかの認証処理を行ったり、或いは先に説明した処理例における認証処理を組み合わせて行うなどとすればよい。
【０１７３】
サーバ装置３０との間での認証処理が許可されると、ステップＳ３３４において、携帯電話１０は、ステップＳ３３１において算出された現在位置及び現在時刻のうちのいずれか一方又は双方と、認証されたサーバ装置３０に関する情報とに基づいて、以降の暗号処理で用いる鍵を生成する。
【０１７４】
このステップＳ３３４における鍵の生成処理は、ＣＰＵ１０７によって行うとしてもよいし、暗号処理を専ら行う暗号回路が携帯電話１０に備えられている場合には、この暗号回路によって行うとしてもよい。また、認証されたサーバ装置３０に関する情報と、現在位置及び現在時刻のうちのいずれか一方又は双方とに基づいて鍵を生成する手順は、サーバ装置３０側との間で予め定められていてもよいし、サーバ装置３０側から通信ネットワーク４０を介して取得するとしてもよい。鍵の生成手順が予め定められている場合には、この生成手順を携帯電話１０の内部に保持しておく必要があるが、例えば、ＲＯＭ１１０、ＲＡＭ１１１、不揮発メモリ１１２に予め生成手順を記憶しておき、この生成手順をＣＰＵ１０７によって読み出すなどすればよい。
【０１７５】
また、鍵を生成する際に用いる情報のうち、「認証が行われたサーバ装置３０に関する情報」は、認証結果に応じて特定される情報であれば任意であるが、例えば、ステップＳ３３２における認証処理で用いられる認証情報であってもよいし、携帯電話１０の内部に予め保持された情報の中から認証処理の結果特定されたサーバ装置に応じて選出される情報であってもよい。
【０１７６】
以上のようにして鍵が生成された状態の下で、サーバ装置３０から所定の平文と、この平文に対して暗号化を施す要求とを受信すると、携帯電話１０は、ステップＳ３３５において、受信した平文に対して当該鍵を用いて暗号化処理を施して暗号文を生成し、この暗号文をサーバ装置３０に対して送信する。
【０１７７】
また、サーバ装置３０から所定の暗号文と、この暗号文に対して復号化を施す要求とを受信すると、携帯電話１０は、ステップＳ３３６において、受信した暗号文に対して当該鍵を用いて復号化処理を施して平文を生成し、この平文をサーバ装置３０に対して送信する。なお、このステップＳ３３６においては、平文をサーバ装置３０に送信せずに、例えば携帯電話１０のＬＣＤ１０９に表示するのみであってもよい。
【０１７８】
なお、ステップＳ３３５及びステップＳ３３６における暗号化処理及び復号化処理は、ＣＰＵ１０７によって行うとしてもよいし、携帯電話１０が暗号処理を専ら行う暗号回路を備えている場合には、この暗号回路によって行うとしてもよい。
【０１７９】
携帯電話１０は、以上のような処理を行うことによって、所定のサーバ装置３０との間で正しく接続状態が確立され、認証が行われた状態の下で、所定の位置に存在する場合に限って、又は所定の時刻になった時点に限って、或いは所定の位置に存在し、且つ所定の時刻になった時点に限って、情報の暗号化処理や復号化処理を行うことが可能であるという全く新規な暗号処理を行うことができる。このような暗号処理を行うことが可能な装置は、従来存在していない。
【０１８０】
上述の暗号処理においては、現在位置や現在時刻を用いるだけでなく、認証が行われたサ

ーバ装置３０に関する情報をも用いて暗号化処理を行っていることから、情報を暗号化又は復号化するに際して、サーバ装置３０との間で正しく認証が許可されていることが必要となる。この認証処理は、携帯電話１０側がサーバ装置３０を認証する場合、サーバ装置３０側が携帯電話１０を認証する場合、携帯電話１０及びサーバ装置３０が相互に認証する場合のいずれであってもよい。ただし、サーバ装置３０側からの認証を含む形での認証処理を行うことによって、例えば、上述の暗号処理を用いたサービスをサーバ装置３０によって提供する場合に、このサービスを利用する携帯電話１０を特定し、利用に際して課金を施すことなどが容易となる。

【０１８１】

なお、上述の暗号処理を用いたサービスの具体的な例としては、以下のようなサービスを挙げることができる。例えば、携帯電話１０を携行した状態で所定の扉の前に行き、この携帯電話１０で所定のサーバ装置３０に対してアクセスした場合にのみ、この扉が開くサービス、携帯電話１０によって所定の時刻に所定のサーバ装置３０に対してアクセスした場合にのみメッセージを解読することが可能なサービス、或いは携帯電話１０を携行した状態で所定の場所に行き、この携帯電話１０によって所定のサーバ装置３０に対してアクセスした場合のみメッセージを解読することが可能なサービスなどを容易に実現することができる。

【０１８２】

＜第１５の処理例＞

つぎに、携帯電話１０から位置及び時刻を取得するサーバ装置３０を、いわゆる認証サーバとして用いる場合の一例を示す第１５の処理例について、図２５に示す概略構成図及び図２６に示すフロー図を参照しながら説明する。

【０１８３】

本例に係る情報提供システム２は、図２５に示すように、携帯電話１０と、複数のＧＰＳ衛星２０と、認証サーバとしての機能を備えるサーバ装置３０と、通信ネットワーク４０と、通信基地局５０と、通信ネットワーク４０を介してサーバ装置３０に接続され、サーバ装置３０との間で各種情報の送受信を行う複数のコンピュータ装置６０とを備える。

【０１８４】

本例においては、コンピュータ装置６０を複数備える他は、図１に示した構成と同等であることから、同等な各部についての説明を割愛し、図中において同一の符号を付すこととする。また、コンピュータ装置６０は、図３に示すサーバ装置３０の構成と同等であり、通信ネットワーク４０を介してサーバ装置３０との間で通信経路を確立し、サーバ装置３０との間で各種情報を送受信する機能を有している。

【０１８５】

以上のように構成された情報提供システム２において、携帯電話１０は、予め設定された所定のサーバ装置３０に対してのみ認証を行い、ＧＰＳ機能を利用して得られた位置及び時刻に関する情報（位置時刻情報）を送信する。そして、各コンピュータ装置６０が携帯電話１０の位置時刻情報を取得するに際しては、サーバ装置３０に対して認証を行い、サーバ装置３０で認証が許可された場合にのみ、サーバ装置３０からコンピュータ装置６０に対して携帯電話１０の位置時刻情報が提供される。

【０１８６】

すなわち、情報提供システム２におけるサーバ装置３０は、コンピュータ装置６０が携帯電話１０の位置時刻情報を取得するに際しての中継を行う中継サーバとしての機能、或いは、コンピュータ装置６０と携帯電話１０との間での認証を代理する認証サーバとしての機能を有している。以下では、コンピュータ装置６０が携帯電話１０から位置時刻情報を取得するまでの手順の概略について、サーバ装置３０の上述した機能に注目し、図２６に示すフロー図を参照しながら説明する。

【０１８７】

情報提供システム２におけるサーバ装置３０は、携帯電話１０から位置時刻情報を取得するに際して、携帯電話１０との間で認証を行う（Ｓ３４０，Ｓ３４１）。なお、図２６中

においてステップＳ３４０及びステップＳ３４１として示す携帯電話１０とサーバ装置３０との間で行われる認証処理は、特にその手順について限定されるものではなく、先に説明した処理例におけるいずれかの認証処理を行ったり、或いは先に説明した処理例における認証処理を組み合わせて行うなどとすればよい。

【０１８８】

そして携帯電話１０は、サーバ装置３０との間での認証処理が許可されると、ステップＳ３４２において、ＧＰＳ機能を用いて得られた現在位置及び現在時刻に関する情報（位置時刻情報）をサーバ装置３０に対して送信する。次にステップＳ３４３において、サーバ装置３０は、携帯電話１０から送信された位置時刻情報を受信する。そして、サーバ装置３０は、受信した位置時刻情報を、例えば、ＲＡＭ２０１やＨＤＤ２０３などに記憶・保持する。なお、位置時刻情報の取得対象としての携帯電話１０が複数存在する場合には、例えば、各携帯電話１０を識別する情報と、それぞれの携帯電話１０から取得した位置時刻情報とを関連付けて、データベースに登録する形で保持しておけばよい。

【０１８９】

サーバ装置３０は、上述のようにして携帯電話１０から位置時刻情報を取得した状態で、コンピュータ装置６０から位置時刻情報の取得要求がなされると、このコンピュータ装置６０との間で認証を行う（Ｓ３４４，Ｓ３４５）。なお、図２６中においてステップＳ３４４及びステップＳ３４５として示すサーバ装置３０とコンピュータ装置６０との間で行われる認証処理は、特にその手順について限定されるものではなく、先に説明した処理例におけるいずれかの認証処理を行ったり、或いは先に説明した処理例における認証処理を組み合わせて行うなどとすればよい。

【０１９０】

そしてサーバ装置３０は、コンピュータ装置６０との間での認証処理が許可されると、ステップＳ３４６において、コンピュータ装置６０からの要求に応じて、携帯電話１０の位置時刻情報を送信する。次にステップＳ３４７において、コンピュータ装置６０は、サーバ装置３０から送信された位置時刻情報を受信する。これにより、コンピュータ装置６０は、携帯電話１０の位置時刻情報を取得することができる。そして、コンピュータ装置６０は、取得した位置時刻情報に基づいて、携帯電話１０に対して位置や時刻に関する各種のサービスを提供する処理、複数の携帯電話１０の位置時刻情報を同様にしてサーバ装置３０から取得することによって、各携帯電話１０の現在位置を把握する処理などを行う。

【０１９１】

なお、携帯電話１０、サーバ装置３０、コンピュータ装置６０における認証処理は、各装置に備えられるＣＰＵが各種の演算処理を行うことによって実現される。また、認証処理に特化した認証回路やＤＳＰ（Digital Signal Processor）などを各装置に備え、この認証回路やＤＳＰによって認証処理を行うとしてもよい。

【０１９２】

上述のように、情報提供システム２においては、携帯電話１０から位置時刻情報を送信する送信対象を所定のサーバ装置３０に限定している。そして、他のコンピュータ装置は、サーバ装置３０に対して問い合わせを行うことによって、携帯電話１０の位置時刻情報を取得するよう構成されている。このため、携帯電話１０が認証を行う対象の数を最小限に抑えながら、サーバ装置３０が認証サーバとして機能して中継処理を行うことによって、多数のコンピュータ装置６０からの問い合わせに対応することができる。

【０１９３】

したがって、携帯電話１０が多数の接続対象との間でそれぞれ認証を行うことが不要となり、携帯電話１０における認証に要する処理の簡略化を図ることができる。また、これに伴って、携帯電話１０に必要となる演算能力やメモリ容量を低減することができる。さらに、携帯電話１０が位置時刻情報を送信する対象を最小限に限定することができることから、位置時刻情報が漏洩してしまう虞を著しく低減することができる。

【０１９４】

なお、本例における情報提供システム２においては、携帯電話１０、サーバ装置３０、及

びコンピュータ装置６０の間で情報を送受信するに際して、先に説明した他の処理例と同様にして、この情報に対して暗号化を施すとしてもよい。これにより、これら装置の間で送受信する情報の秘匿性を向上させることができ、ユーザの個人情報に関わる位置時刻情報の漏洩を一層強固に防止することができる。

【０１９５】

また、本例における情報提供システム２では、サーバ装置３０によって携帯電話１０の位置時刻情報を予め取得しておき、コンピュータ装置６０からの要求に従って、サーバ装置３０に保持された携帯電話１０の位置時刻情報をコンピュータ装置６０に対して送信する構成とされている。しかしながら、情報提供システム２においては、携帯電話１０、サーバ装置３０、及びコンピュータ装置６０における処理の手順について、システム全体に要求される機能に応じて改変することも可能である。

【０１９６】

例えば、サーバ装置３０がコンピュータ装置６０から特定の携帯電話１０の現在位置についての問い合わせを受けた時点で、サーバ装置３０が携帯電話１０から位置時刻情報を取得する処理を行い、取得した位置時刻情報をコンピュータ装置６０に対して送信する構成とすることもできる。このような構成とすることにより、コンピュータ装置６０は、特定の携帯電話１０についての現在位置をリアルタイムで取得することが可能となる。

【０１９７】

＜他の実施の形態＞

以上の説明においては、本発明を適用した情報提供サービスについて、種々の具体的な処理例を述べたが、上述した処理例を適宜組み合わせてなる形態で本発明を実施するとしてもよい。

【０１９８】

また、以上の説明においては、全地球測位システムとして、日本国で広く利用されているＧＰＳ（Global Positioning System）を想定したが、他の各種方式の全地球測位システムを利用するとしてもよい。

【０１９９】

また、本発明は、携帯電話への適用に限定されるものではなく、人工衛星を利用した測位機能を備え、通信ネットワークを介して他の情報処理装置との間で情報を送受信することが可能な移動体端末に対して広く適用することが可能である。このような移動体端末としては、例えば、いわゆるノート型パーソナルコンピュータ、携帯型の測位端末、各種ＰＤＡ機器、車載用のナビゲーション装置などを挙げることができる。

【０２００】

また、例えば、各種の宅配サービス、物流システム、郵便システムなどに対して本発明を適用するとしてもよい。この場合には、運搬される荷物や手紙の各々に対して、ＧＰＳ機能及びネットワーク機能を有する情報端末装置を備え付ける。そして、この情報端末装置に対して現在位置を問い合わせることによって、荷物や手紙の現在位置を正確に把握することが可能となる。

【０２０１】

【発明の効果】

本発明に係る情報端末装置は、位置時刻情報を情報処理装置に対して送信するに際して、この情報処理装置が正当な接続対象であることを認証手段によって認証した場合に限って、位置時刻情報の送信が許可される。したがって、例えば、ユーザが意図しない第三者から位置時刻情報の送信を要求された場合であっても、これを認証手段によって確実に防止することができ、ユーザの行動を特定する個人情報となり得る位置時刻情報がユーザの意図に反する第三者に漏洩してしまうことを防止することができる。

【０２０２】

また、本発明に係る情報端末装置は、衛星信号から算出された現在位置や現在時刻と、接続に対して認証が行われた情報処理装置に関する情報とに基づいて生成した鍵を用いて暗号処理を行うことができる。このため、情報処理装置に対して正しく接続状態が確立され

た状態において、所定の位置に存在する場合に限って、又は所定の時刻になった時点に限って、或いは所定の位置に存在し、且つ所定の時刻になった時点に限って、情報の暗号化処理や復号化処理を行うことが可能であるという全く新規な暗号処理を行うことができる。したがって、このような情報端末装置を用いることにより、情報処理装置によって全く新規なサービスを提供することができる。

【０２０３】

また、本発明に係る情報処理装置は、位置時刻情報を情報端末装置から取得するに際して、情報端末装置との間で認証を行う構成とされている。したがって、例えば、ユーザが意図しない第三者に対して位置時刻情報を送信してしまうことを防止する目的で、情報端末装置側から認証を求められた場合であっても、この認証を正しく行って、位置時刻情報を取得することができる。

【０２０４】

さらに、本発明に係る情報送受信システムは、情報端末装置と情報処理装置との間で位置時刻情報を授受するに際して、この情報処理装置が正当な接続対象であることを認証手段によって認証した場合に限って、位置時刻情報の送信が許可される。したがって、例えば、ユーザが意図しない第三者に対して位置時刻情報が送信されてしてしまうことを防止することができる。

【０２０５】

したがって、本発明によれば、全地球測位システムを利用して算出される現在位置や現在時刻に関する情報、すなわち位置時刻情報が、ユーザの意図しない第三者へ漏洩してしまうことを防止し、通信ネットワークを介して情報端末装置と情報処理装置との間で安全且つ確実に位置時刻情報を送受信することができる。したがって、この位置時刻情報を利用した種々のサービスを、個人情報の漏洩を防止して安全に実現することができる。

【図面の簡単な説明】

【図１】本発明を適用して実現される情報提供システムの一例を示す概略構成図である。

【図２】同情報提供システムに備えられる携帯電話の一構成例を示す概略図である。

【図３】同情報提供システムに備えられるサーバ装置の一構成例を示す概略図である。

【図４】同情報提供システムに備えられる携帯電話におけるＧＰＳ機能を説明するための模式図である。

【図５】同情報提供システムに備えられる携帯電話におけるＧＰＳ機能を説明するための別の模式図である。

【図６】同情報提供システムに備えられる携帯電話におけるＧＰＳ機能を説明するためのさらに別の模式図である。

【図７】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１の処理例について説明するためのフロー図である。

【図８】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１の処理例について説明するための模式図である。

【図９】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第２の処理例について説明するための模式図である。

【図１０】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第３の処理例について説明するための模式図である。

【図１１】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第３の処理例において、暗号化を施す場合について説明するための模式図である。

【図１２】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第４の処理例について説明するための模式図である。

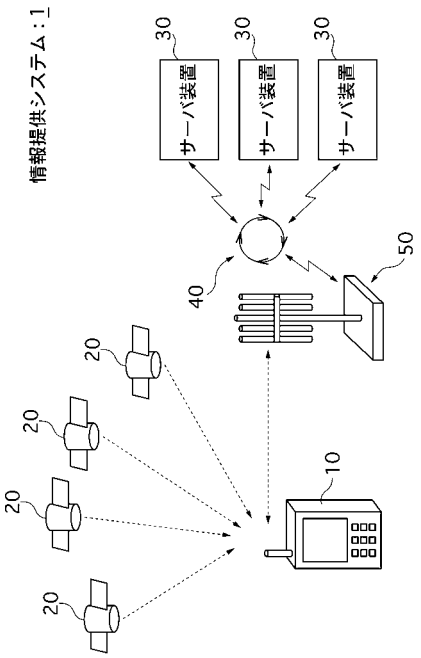
【図１３】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第５の処理例について説明するための模式図である。

【図１４】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第６の処理例について説明するための模式図である。

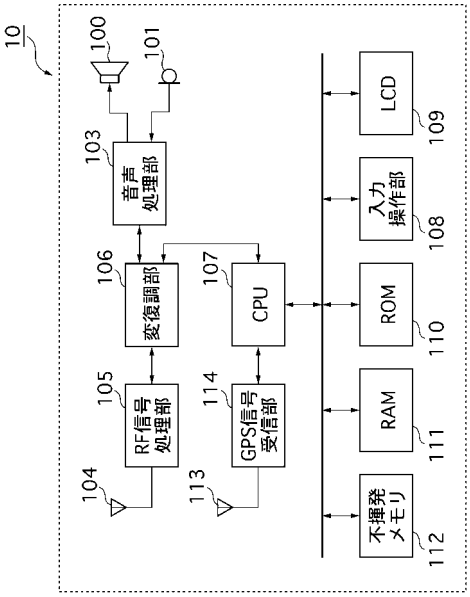
【図１５】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第７の処

理例について説明するための模式図である。
【図１６】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第８の処理例について説明するための模式図である。
【図１７】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第９の処理例について説明するための模式図である。
【図１８】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１０の処理例について説明するためのフロー図である。
【図１９】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１１の処理例について説明するためのフロー図である。
【図２０】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１１の処理例で用いられる条件情報について説明するための模式図である。
【図２１】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１２の処理例について説明するためのフロー図である。
【図２２】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１３の処理例について説明するためのフロー図である。
【図２３】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１３の処理例で用いられる精度変更情報について説明するための模式図である。
【図２４】同情報提供システムにおいて携帯電話とサーバ装置との間で行われる第１４の処理例について説明するための模式図である。
【図２５】本発明を適用して実現される情報提供システムの別の一例を示す概略構成図である。
【図２６】同情報提供システムにおいて携帯電話、サーバ装置、及びコンピュータ装置の間で行われる処理の例について説明するためのフロー図である。
【符号の説明】
１，２　情報提供システム、１０　携帯電話、２０　ＧＰＳ衛星、３０　サーバ装置、４０　通信ネットワーク、５０　通信基地局、６０　コンピュータ装置、１０３　音声処理部、１０４　ＲＦアンテナ、１０５　ＲＦ信号処理部、１０６　変復調部、１０７　ＣＰＵ、１０８　入力操作部、１０９　ＬＣＤ、１１０ＲＡＭ、１１１　ＲＡＭ、１１２　不揮発メモリ、１１３　ＧＰＳアンテナ、１１４　ＧＰＳ信号受信部、２００　ＣＰＵ、２０１　ＲＡＭ、２０２　ＲＯＭ、２０３　ＨＤＤ、２０４　ネットワークインターフェース

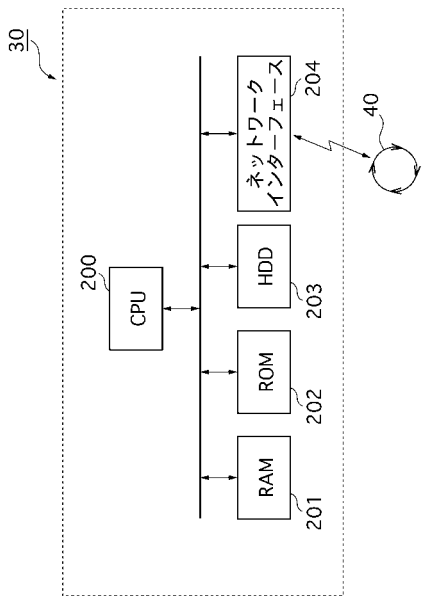
【図１】


情報提供システム：1
サーバ装置
30
40
50
20
10

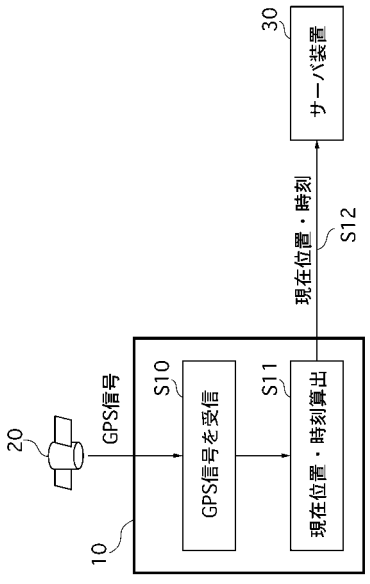
【図２】


10
100
101
103
音声処理部
106
変復調部
107
CPU
105
RF信号処理部
104
114
GPS信号受信部
113
LCD
109
入力操作部
108
ROM
110
RAM
111
不揮発メモリ
112

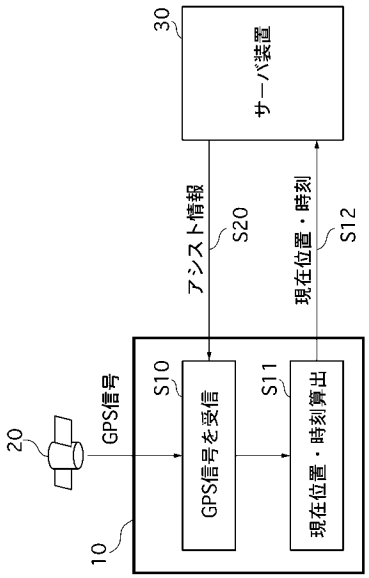
【図３】


30
CPU
200
RAM
201
ROM
202
HDD
203
ネットワークインターフェース
204
40

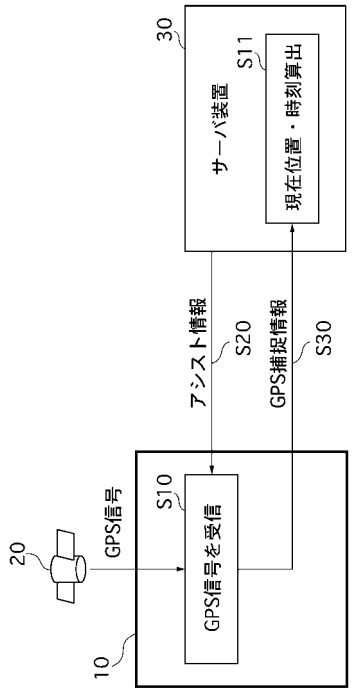
【図４】


30
サーバ装置
現在位置・時刻
S12
20
GPS信号
S10
GPS信号を受信
S11
現在位置・時刻算出
10

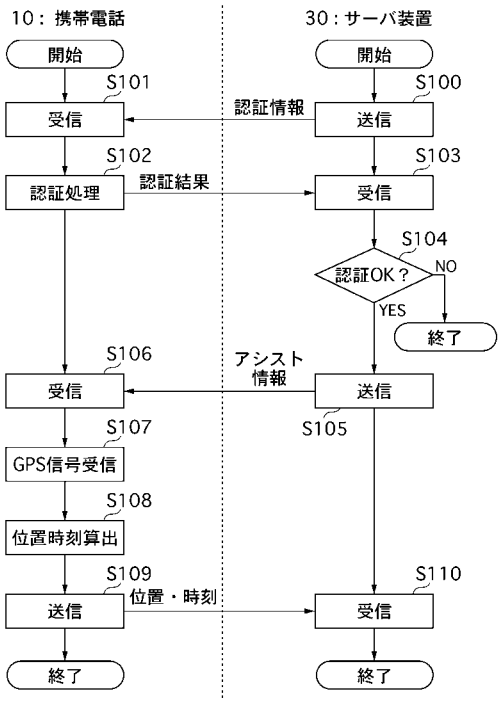
【図５】


30
サーバ装置
アシスト情報
S20
現在位置・時刻
S12
GPS信号
S10
GPS信号を受信
S11
現在位置・時刻算出
20
10

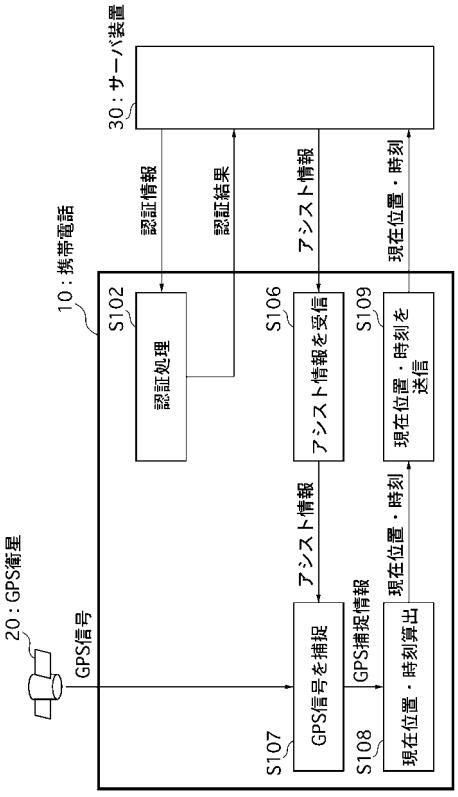
【図６】


30
サーバ装置
S11
現在位置・時刻算出
アシスト情報
S20
GPS捕捉情報
S30
GPS信号
S10
GPS信号を受信
20
10

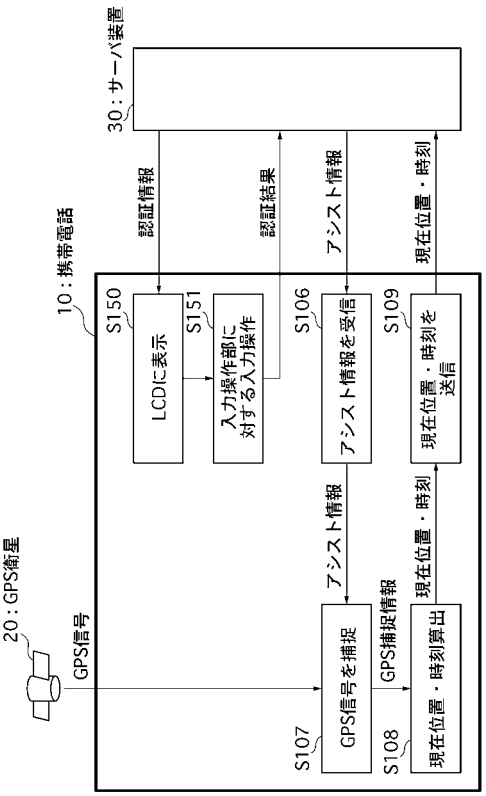
【図７】


10：携帯電話
30：サーバ装置
開始
開始
S101
S100
送信
認証情報
受信
S102
S103
認証処理
認証結果
受信
S104
認証OK？
NO
YES
終了
S106
アシスト情報
受信
送信
S105
S107
GPS信号受信
S108
位置時刻算出
S109
位置・時刻
送信
S110
受信
終了
終了

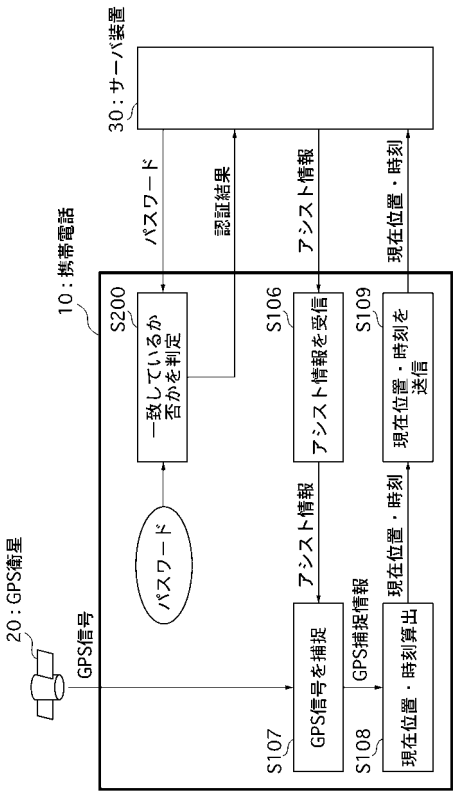
【図８】


30：サーバ装置
認証情報
認証結果
アシスト情報
現在位置・時刻
10：携帯電話
S102
認証処理
S106
アシスト情報を受信
S109
現在位置・時刻を送信
アシスト情報
現在位置・時刻
20：GPS衛星
GPS信号
GPS信号を捕捉
GPS捕捉情報
S107
S108
現在位置・時刻算出

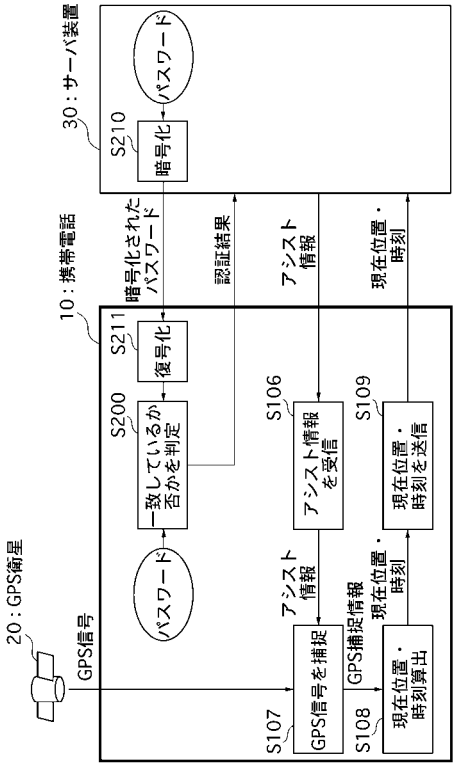
【図９】



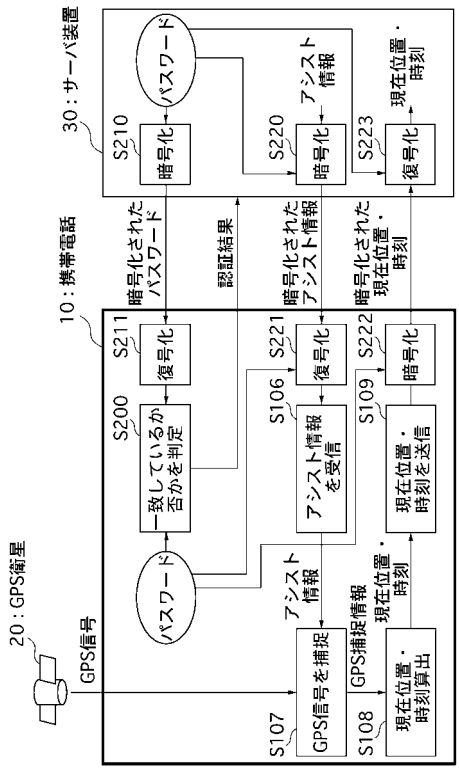
【図１０】



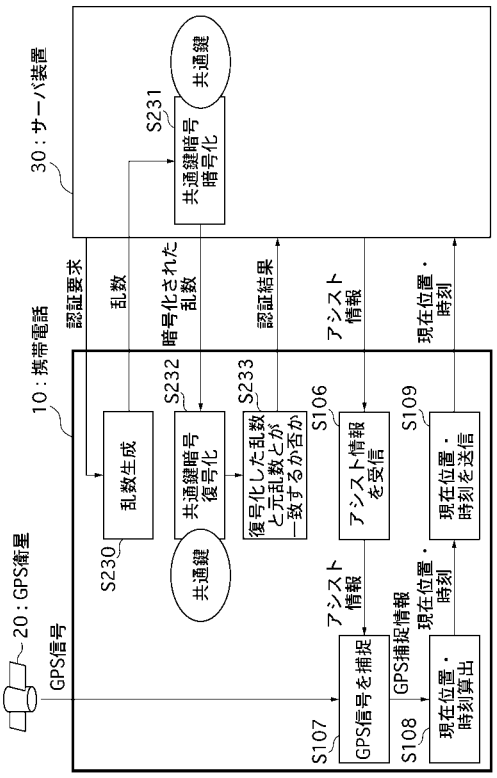
【図１１】



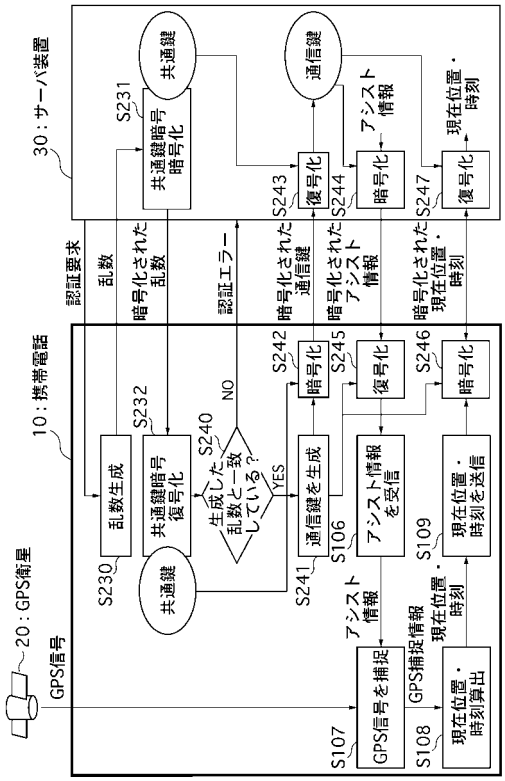
【図１２】



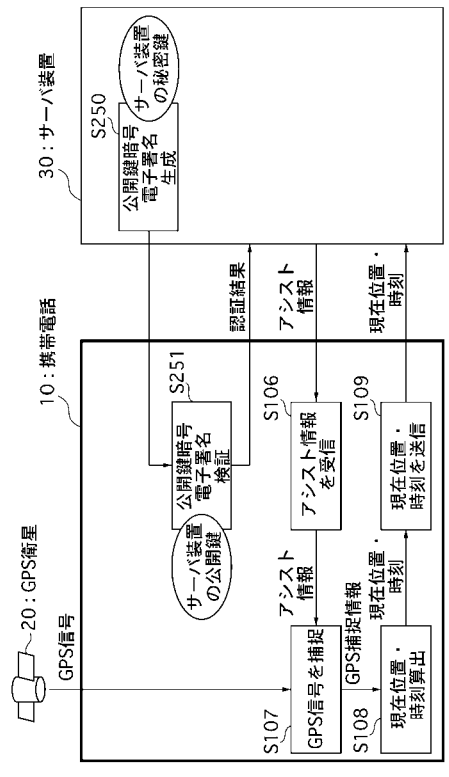
【図１３】



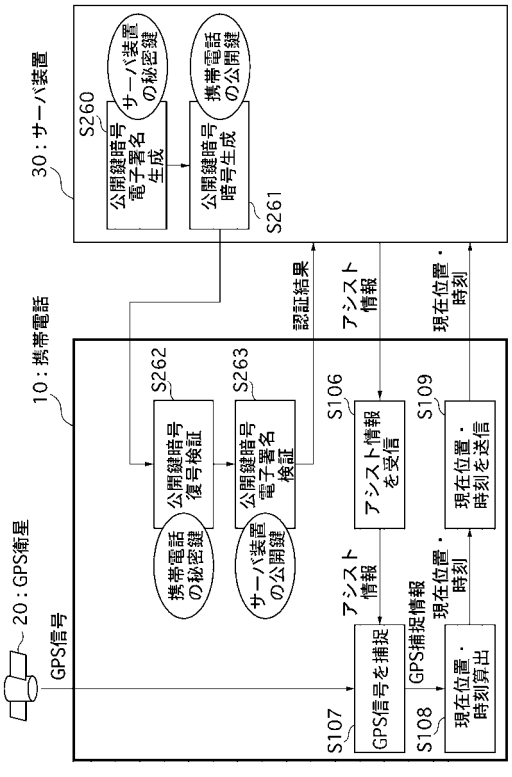
【図１４】



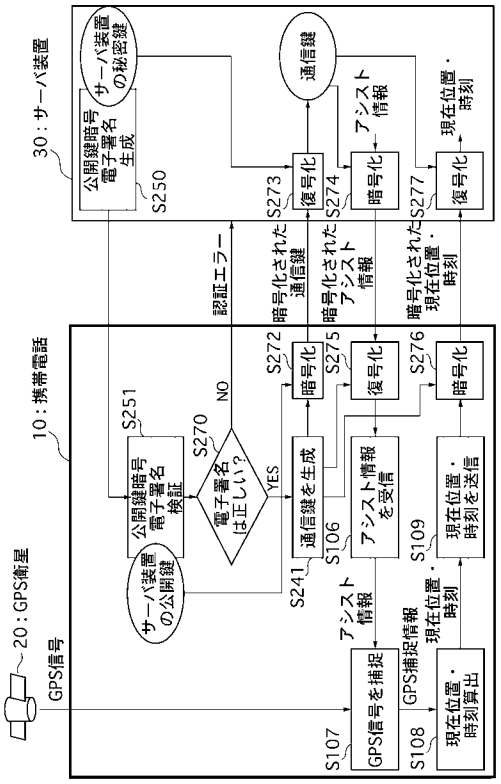
【図１５】



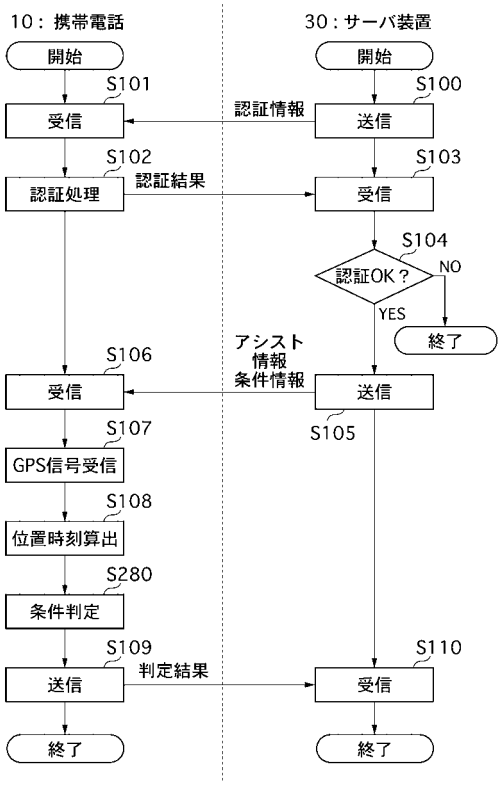
【図１６】



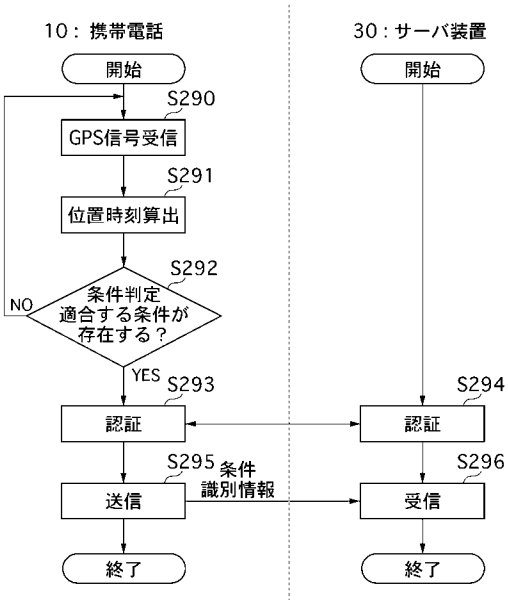
【図１７】



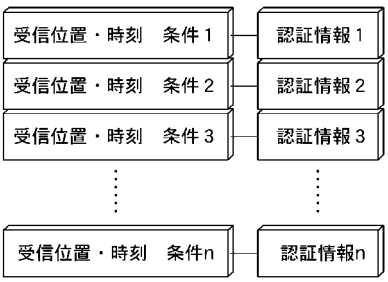
【図１８】



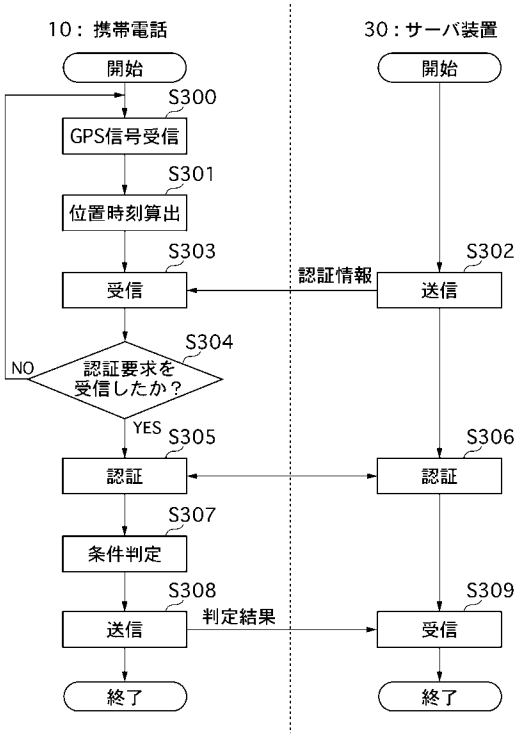
【図１９】



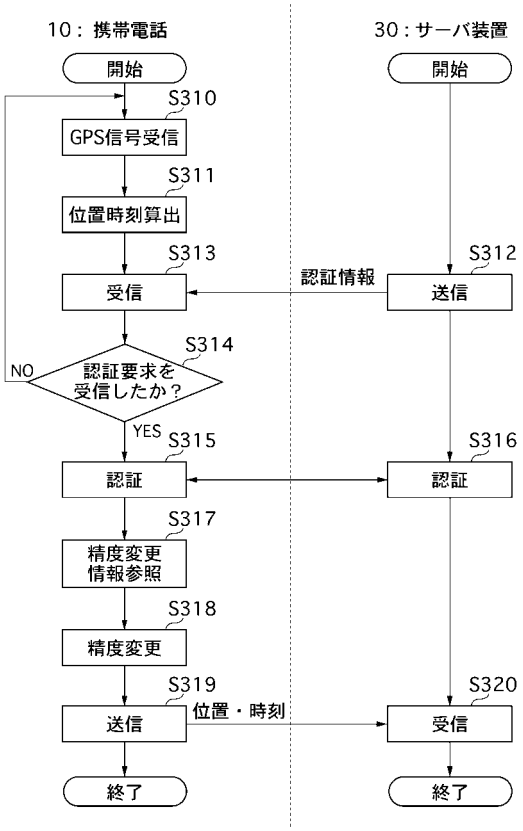
【図２０】



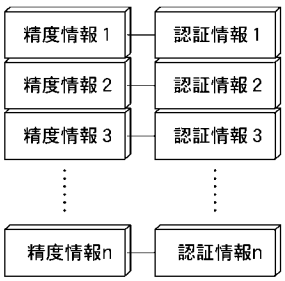
【図２１】



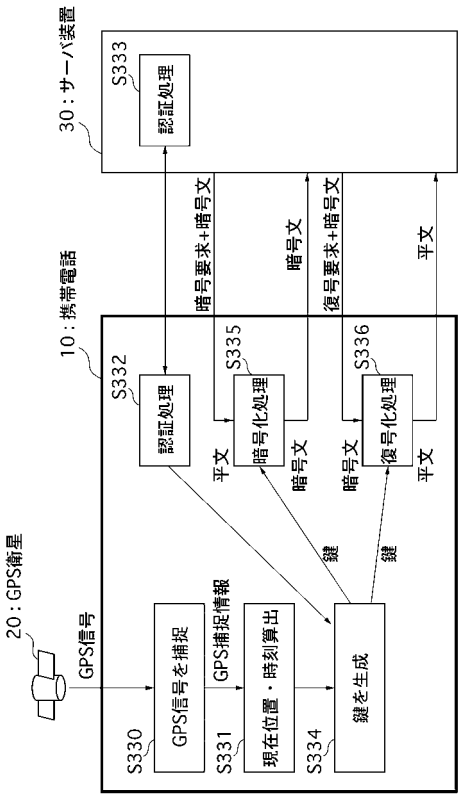
【図２２】



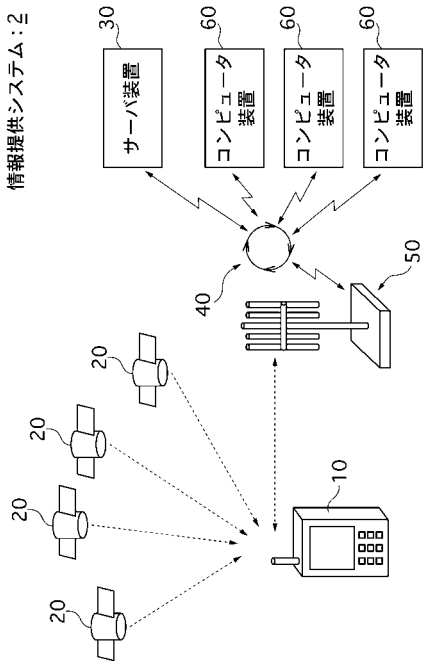
【図２３】



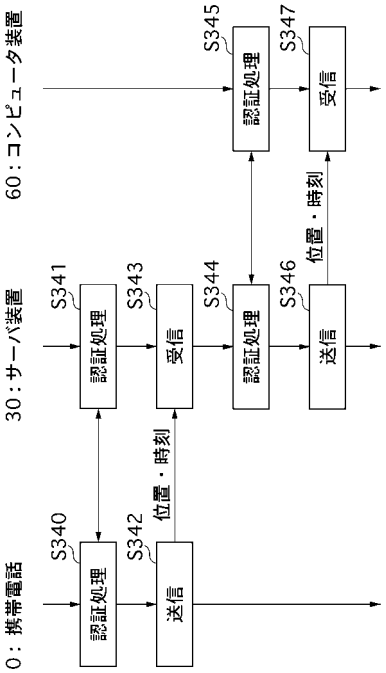
【図２４】



【図２５】


情報提供システム：2
30
サーバ装置
60
コンピュータ装置
60
コンピュータ装置
60
コンピュータ装置
40
50
20
20
20
20
10

【図２６】


10：携帯電話
30：サーバ装置
60：コンピュータ装置
S340
認証処理
S341
認証処理
S342
送信
位置・時刻
S343
受信
S344
認証処理
S345
認証処理
S346
送信
位置・時刻
S347
受信

フロントページの続き

(56)参考文献 特開２０００－２９８６３０（ＪＰ，Ａ）
特開２００１－０１４５９２（ＪＰ，Ａ）
特開平１０－１７０６２５（ＪＰ，Ａ）
特開２０００－００４４８２（ＪＰ，Ａ）
特開２０００－１５６８８２（ＪＰ，Ａ）
特開２００２－０５１３７３（ＪＰ，Ａ）
特開２００１－１４８７４２（ＪＰ，Ａ）
特開２００１－２３８２７４（ＪＰ，Ａ）
特開２００１－１７７８６３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24- 7/26
H04Q 7/00- 7/38