(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4599791号
(P4599791)
(45)発行日　平成22年12月15日(2010.12.15)　(24)登録日　平成22年10月8日(2010.10.8)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B

請求項の数 13　(全 33 頁)

(21)出願番号　特願2002-234385(P2002-234385)
(22)出願日　平成14年8月12日(2002.8.12)
(65)公開番号　特開2004-80125(P2004-80125A)
(43)公開日　平成16年3月11日(2004.3.11)
審査請求日　平成17年7月28日(2005.7.28)

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

審査官　速水　雄太

最終頁に続く

(54)【発明の名称】情報機器

(57)【特許請求の範囲】
【請求項１】
装置ごとに異なる秘密鍵を保持する秘密鍵保持部と、
装置の識別情報あるいは装置の使用者の識別情報を保持する識別情報保持部と、
測位用衛星から受信した電波に基づき測定された、前記電波の受信位置および時刻を示す位置・時刻情報を、前記秘密鍵保持部に保持された前記秘密鍵を用いてデジタル署名するデジタル署名手段と、
前記識別情報保持部に保持された前記識別情報と、前記デジタル署名が付加された前記位置・時刻情報とを、通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信するための通信手段と、
前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、
前記位置・時刻情報を、前記デジタル署名の前に、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、
を備える通信装置。
【請求項２】
請求項１に記載の通信装置において、
前記通信相手先の公開鍵を保持する公開鍵保持部と、
前記デジタル署名手段により生成された前記デジタル署名が付加された前記位置・時刻情報を、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号

化手段と、
を備える通信装置。
【請求項３】
機器ごとに異なる秘密鍵を保持する秘密鍵保持部と、
機器の識別情報あるいは機器の使用者の識別情報を保持する識別情報保持部と、
測位用衛星から受信した電波に基づき測定された、前記電波の受信位置および時刻を示す位置・時刻情報を、前記秘密鍵保持部に保持された前記秘密鍵を用いてデジタル署名するデジタル署名手段と、
前記デジタル署名が付加された前記位置・時刻情報を、外部から読み出し可能な状態で記憶する記憶手段と、
前記識別情報保持部に保持された前記識別情報と、前記デジタル署名が付加された前記位置・時刻情報とを、通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される機器を検索して送信した送信情報を受信するための通信手段と、
前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、
前記位置・時刻情報を、前記デジタル署名の前に、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、
を備える情報機器。
【請求項４】
請求項３に記載の情報機器において、
前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、
前記デジタル署名手段により生成された前記デジタル署名が付加された前記位置・時刻情報を、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、
を備える情報機器。
【請求項５】
ＩＣカードの装着部と、
測位用衛星から受信した電波に基づき測定された、前記電波の受信位置および時刻を示す位置・時刻情報を、前記ＩＣカードに供給するようにする手段と、
前記ＩＣカードに保持されたＩＣカードのユーザを識別するための識別情報と、前記ＩＣカードからの、デジタル署名が付加された前記位置・時刻情報とを、前記通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信するための通信手段と、
前記ＩＣカードからは、前記通信相手先の公開鍵を用いて、前記位置・時刻情報を暗号化した情報に、前記デジタル署名が付加されたデータが出力され、
前記通信手段は、前記デジタル署名が付加された前記暗号化された前記位置・時刻情報を前記通信相手先に送信する
通信装置。
【請求項６】
請求項５に記載の通信装置において、
前記ＩＣカードからは、前記デジタル署名が付加された前記位置・時刻情報を、前記通信相手先の公開鍵を用いて暗号化した情報が出力され、
前記通信手段は、前記ＩＣカードからの前記暗号化された情報を前記通信相手先に送信する
通信装置。
【請求項７】
ＩＣカードの装着部と、
測位用衛星からの電波に基づき測定された、前記電波の受信機器の位置および時刻を示す位置・時刻情報を、前記ＩＣカードに供給するようにする手段と、

前記ＩＣカードに保持されたＩＣカードのユーザを識別するための識別情報と、前記ＩＣカードからの、デジタル署名が付加された前記位置・時刻情報を、外部から読み出し可能な状態で記憶する記憶部と、

前記識別情報保持部に保持された前記識別情報と、前記デジタル署名が付加された前記位置・時刻情報とを、通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信するための通信手段と、

前記ＩＣカードからは、前記通信相手先の公開鍵を用いて、前記位置・時刻情報を暗号化した情報に、前記デジタル署名が付加されたデータが出力され、

前記ＩＣカードからの、前記デジタル署名が付加された前記暗号化された前記位置・時刻情報を前記記憶部に記憶する

情報機器。

【請求項８】

請求項７に記載の情報機器において、

前記ＩＣカードからは、前記デジタル署名が付加された前記位置・時刻情報を、前記通信相手先の公開鍵を用いて暗号化した情報が出力され、

前記ＩＣカードからの前記暗号化された情報を、前記記憶部に記憶する

情報機器。

【請求項９】

ＩＣカードの装着部と、

測位用衛星から受信した電波に基づき測定された、前記電波の受信位置および時刻を示す位置・時刻情報を、前記ＩＣカードに供給するようにする手段と、

前記ＩＣカードに保持されたＩＣカードのユーザを識別するための識別情報と、前記ＩＣカードからの、デジタル署名が付加された前記位置・時刻情報とを、前記通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信するための通信手段と、

を備える通信装置の前記ＩＣカードの装着部に装着されるＩＣカードであって、

ＩＣカード毎に異なる秘密鍵を保持する秘密鍵保持部と、

自ＩＣカードのユーザの識別情報を保持する識別情報保持部と、

前記位置・時刻情報を、前記秘密鍵保持部に保持された前記秘密鍵を用いてデジタル書名して、出力するデジタル署名手段と、

前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、

前記位置・時刻情報を、前記デジタル署名の前に、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、

を備えるＩＣカード。

【請求項１０】

ＩＣカードの装着部と、

測位用衛星からの電波に基づき測定された、前記電波の受信機器の位置および時刻を示す位置・時刻情報を、前記ＩＣカードに供給するようにする手段と、

前記ＩＣカードに保持されたＩＣカードのユーザを識別するための識別情報と、前記ＩＣカードからの、デジタル署名が付加された前記位置・時刻情報を、外部から読み出し可能な状態で記憶する記憶部と、

前記識別情報保持部に保持された前記識別情報と、前記デジタル署名が付加された前記位置・時刻情報とを、通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される機器を検索して送信した送信情報を受信するための通信手段と、

を備える情報機器の前記ＩＣカードの装着部に装着されるＩＣカードであって、

ＩＣカード毎に異なる秘密鍵を保持する秘密鍵保持部と、

自ＩＣカードのユーザの識別情報を保持する識別情報保持部と、

前記位置・時刻情報を、前記秘密鍵保持部に保持された前記秘密鍵を用いてデジタル書名して、出力するデジタル署名手段と、
前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、
前記位置・時刻情報を、前記デジタル署名の前に、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、
を備えるＩＣカード。
【請求項１１】
請求項９または請求項１０に記載のＩＣカードにおいて、
前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、
前記デジタル署名手段により生成された前記デジタル署名が付加された前記位置・時刻情報を、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、
を備えるＩＣカード。
【請求項１２】
測位手段と、デジタル署名手段と、位置・時刻情報通信手段と、通信手段とを備える通信装置における送受信方法であって、
前記測位手段が、測位用衛星からの電波を受信して、受信位置および時刻を測定する測位工程と、
前記デジタル署名手段が、前記測位工程で得られた前記受信位置および時刻を示す位置・時刻情報について、予め保持されている秘密鍵を用いてデジタル署名するデジタル署名工程と、
前記位置・時刻情報通信手段が、前記デジタル署名が付加された前記位置・時刻情報を、通信相手先に送信する位置・時刻情報通信工程と、
前記通信手段が、自装置の識別情報あるいは自装置の使用者の識別情報を、前記位置・時刻情報の送信に先立ち、または、前記位置・時刻情報の送信の後に、または、前記位置・時刻情報の送信と同時に、前記通信相手先に送信する工程と、
前記通信手段が、前記通信相手先がメモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信する工程と、
前記通信装置が備える前記暗号化手段が、前記デジタル署名工程の前に、通信相手先の公開鍵を用いて、前記位置・時刻情報を暗号化する暗号化工程を有し、
前記通信工程で前記通信相手先に送られる前記位置・時刻情報は、暗号化されている
送受信方法。
【請求項１３】
請求項１２に記載の送受信方法において、
前記通信装置が備える暗号化手段が、前記デジタル署名工程と、前記通信工程との間に、前記デジタル署名が付加された前記位置・時刻情報を、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化工程を有する
送受信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、位置・時刻の測位機能を備える、例えば携帯電話機やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ；携帯情報機器）などの通信装置や情報機器に関する。
【０００２】
【従来の技術】
人工衛星を利用して移動体の位置を測定するＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）受信機が普及しつつある。ＧＰＳ受信機は、４個以上の人工衛星（ＧＰＳ衛星）からの信号を受信し、その受信信号から受信機の位置と時刻を計算すること

ができ、カーナビゲーションシステムやハンディＧＰＳシステムなどに広く利用されている。

【０００３】

そして、近年では、携帯電話などネットワークに接続される携帯型電子機器とＧＰＳ受信機の機能とが一体化された携帯機器やサービスが登場し始めている。そこで、この種の携帯機器からの位置・時刻情報を利用したネットワークサービスが考えられている。例えば、ＧＰＳ受信機の機能とが一体化された携帯機器からの位置・時刻情報を収集し、決まった時刻に限定された場所にいる人（当該携帯機器の所持者）にだけ、特定の情報や広告などを配信するサービスが考えられている。

【０００４】

今後、安価なネットワークが構築されると、この種の、ネットワークに接続される前記のＧＰＳ受信機の機能が一体化された携帯機器からの位置・時刻情報を利用したネットワークサービスが、ますます増加することが予想される。

【０００５】

また、このようなサービス用途の他に、移動する人々に携帯機器を所持させ、その携帯機器からの位置・時刻情報を収集して、前記移動する人々の現在位置を管理して、それらの移動する人々に、その存在位置や時刻に適合する指示を送るようにするネットワークシステムも考えられている。

【０００６】

【発明が解決しようとする課題】

ところで、上述のようなネットワークサービスやネットワークシステムにおいては、携帯機器から送られてくる位置・時刻情報が当該携帯機器から送られてきた正しいデータであることが重要である。情報提供者や、管理者の意図する通りの情報伝達ができなくなる等の問題が発生するためである。

【０００７】

しかしながら、携帯機器の利用者からの位置・時刻の情報の従来の収集方法では、送られてきた位置・時刻の情報が、本当に、使用者が使用するＧＰＳ受信機能付きの携帯機器で測定が行なわれた正当な情報であるかどうかを確認することができなかった。

【０００８】

例えば、悪意の者が、前記ＧＰＳ受信機能付きの携帯機器以外の他の機器から、実際とは異なった位置・時刻の情報を、あたかも、前記ＧＰＳ受信機能付きの携帯機器から送ったように偽装しても、それを見破る手立てがなかった。

【０００９】

また、逆に、位置・時刻の情報が、本当に、使用者が使用するＧＰＳ受信機能付きの携帯機器で測定が行なわれた正当な情報であっても、それを証明する方法が従来は無かった。

【００１０】

この発明は、以上の問題点を解消することができる通信装置および情報機器を提供することを目的とする。

【００１１】

【課題を解決するための手段】

前記課題を解決するため、請求項１の発明による通信装置は、

装置ごとに異なる秘密鍵を保持する秘密鍵保持部と、

装置の識別情報あるいは機器の使用者の識別情報を保持する識別情報保持部と、

測位用衛星から受信した電波に基づき測定された、前記電波の受信位置および時刻を示す位置・時刻情報を、前記秘密鍵保持部に保持された前記秘密鍵を用いてデジタル署名するデジタル署名手段と、

前記識別情報保持部に保持された前記識別情報と、前記デジタル署名が付加された前記位置・時刻情報とを、通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信するための通信手段と、

を備えることを特徴とする。

【００１２】

上記の構成の請求項１の発明によれば、通信装置に秘密裏に保持されている秘密鍵が用いられてデジタル署名がなされ、当該デジタル署名が付加された位置・時刻情報が通信相手先に送られる。

【００１３】

通信相手先では、通信装置から通信手段により送られてくる識別情報に基づき、デジタル署名を検証するための、当該識別情報に対応する公開鍵を取得する。そして、取得した公開鍵を用いて、通信装置から通信手段により送られてくる位置・時刻情報に付加されているデジタル署名を検証する。この検証の結果、通信相手先では、検証できたときには、正当な位置・時刻情報と認識し、検証できなかったときには、改ざん等が行なわれた不正な位置・時刻情報と認識することができる。

【００１４】

また、請求項２の発明は、請求項１に記載の通信装置において、

前記位置・時刻情報を通知したい相手の公開鍵を保持する公開鍵保持部と、

前記位置・時刻情報を、前記デジタル署名の前に、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、

を備えることを特徴とする。

【００１５】

この請求項２の発明によれば、位置・時刻情報は、位置・時刻情報を通知したい相手の公開鍵が用いられて、デジタル署名前に暗号化されている。そこで、通信相手先では、通信装置から通信手段により送られてくる暗号化されている位置・時刻情報に付加されているデジタル署名を検証して、暗号化されている位置・時刻情報が正当な情報か不正な情報であるかを判定することができる。

【００１６】

しかし、請求項２の発明の場合には、位置・時刻情報は暗号化されているので、その暗号化に使用された公開鍵が通信相手先に対応するものであれば、復号化することができるが、他の者に対応する公開鍵であれば、暗号は復号できず、位置・時刻情報は、通信相手先では秘匿される。そして、例えば通信相手先から、位置・時刻情報を通知したい相手に、当該暗号化された位置・時刻情報が渡されたときに、当該相手により、その秘密鍵が用いられて位置・時刻情報が復号される。

【００１７】

したがって、この請求項２の発明の場合には、特定の相手にのみ、位置・時刻情報を渡すようにしたい場合に便利である。

【００１８】

また、請求項３の発明は、請求項１に記載の通信装置において、

前記通信相手先の公開鍵を保持する公開鍵保持部と、

前記デジタル署名手段により生成された前記デジタル署名が付加された前記位置・時刻情報を、前記公開鍵保持部に保持された前記通信相手先の公開鍵を用いて暗号化する暗号化手段と、

を備えることを特徴とする。

【００１９】

この請求項３の発明の場合には、通信相手先に送られる情報は、当該通信相手先の公開鍵により暗号化されている。したがって、通信相手先では、受信した情報を先ず秘密鍵を用いて復号する。復号できれば、自分宛ての情報であるとすることができる。

【００２０】

次に、通信相手先では、通信装置から通信手段により送られてくる識別情報に基づき、デジタル署名を検証するための、当該識別情報に対応する公開鍵を取得する。そして、取得した公開鍵を用いて、通信装置から通信手段により送られてくる位置・時刻情報に付加されているデジタル署名を検証する。この検証の結果、通信相手先では、検証できたとき

には、正当な位置・時刻情報と認識し、検証できなかったときには、改ざん等が行なわれた不正な位置・時刻情報と認識することができる。

【００２１】

この請求項３の発明の場合には、通信装置から通信相手先への通信の際に、通信データが傍受されてしまったとしても、暗号化されているため、情報の秘匿ができるという特徴がある。

【００２２】

また、請求項４の発明は、

機器ごとに異なる秘密鍵を保持する秘密鍵保持部と、

機器の識別情報あるいは機器の使用者の識別情報を保持する識別情報保持部と、

測位用衛星から受信した電波に基づき測定された、前記電波の受信位置および時刻を示す位置・時刻情報を、前記秘密鍵保持部に保持された前記秘密鍵を用いてデジタル署名するデジタル署名手段と、

前記デジタル署名が付加された前記位置・時刻情報を、外部から読み出し可能な状態で記憶する記憶手段と、

前記識別情報保持部に保持された前記識別情報と、前記デジタル署名が付加された前記位置・時刻情報とを、通信相手先に送信すると共に、前記通信相手先が、メモリに記憶した前記位置・時刻情報に基づき、特定の場所において、特定の時間帯に存在すると推定される装置を検索して送信した送信情報を受信するための通信手段と、

を備えることを特徴とする。

【００２３】

この請求項４の発明においては、デジタル署名が付加された位置・時刻情報が、外部から読み出し可能な状態で記憶部に記憶されているので、必要なときに記憶されたデータを取り出すことができる。そして、取り出された情報は、デジタル署名を検証することにより、位置・時刻情報が正当な情報であるかどうかを判定することができる。

【００２４】

【発明の実施の形態】

以下、この発明による通信装置の実施形態を、通信装置が測位機能付きの携帯電話端末の場合について、図を参照しながら説明する。そして、以下においては、通信装置の実施形態である携帯電話端末を、位置・時刻情報の送受信システムに用いた場合について主として説明する。この例では、測位システムとしては、ＧＰＳシステムが用いられる。

【００２５】

図１は、実施形態の通信装置である携帯電話端末１０を含む位置・時刻情報の送受信システムの概要を説明するための図である。この図１の例のシステムは、測位用衛星、この例ではＧＰＳ衛星１の複数個からの電波を受信して、当該電波受信時の自機の位置および時刻を測定する機能を備える携帯電話端末１０と、この携帯電話端末１０と無線基地局２および通信ネットワーク３を通じて接続される情報収集サーバ装置２０とからなる。

【００２６】

携帯電話端末１０は、ＧＰＳ衛星１からの電波を受信して、この受信電波に基づいて測定して得た、衛星電波受信時の自機の位置および時刻を示す情報（この情報を、以下、位置・時刻情報と略称する）をサーバ装置２０に対して送信する。図１では、携帯電話端末１０は、１台のみを示したが、実際的には、システム上には、複数台の携帯電話端末１０がサーバ装置２０に対して接続される。

【００２７】

この場合に、いずれの携帯電話端末１０からの位置・時刻情報であるかをサーバ装置２０では判別する必要があるが、そのために、携帯電話端末１０からは、何等かの識別情報（この明細書では、この識別情報をユーザＩＤと呼ぶこととする）をサーバ装置２０に送るようにする。このユーザＩＤには、携帯電話端末１０の使用者個人を特定する識別情報と、携帯電話端末１０を特定する識別情報とが含まれる。

【００２８】

ユーザＩＤとしては、例えば、携帯電話端末１０のそれぞれの機器に割り当てられている機器識別信号（機器ＩＤ）を用いることができる。また、携帯電話端末１０のそれぞれに割り当てられている電話番号を、ユーザＩＤとして用いても良い。また、予め、サーバ装置２０に対して、携帯電話端末１０の使用者が、特定の番号や記号からなり他の使用者と区別することができる識別情報を登録しておき、その登録した識別情報をユーザＩＤとして用いることもできる。以下に説明する第１の実施形態～第３の実施形態では、ユーザＩＤとしては、携帯電話端末１０のそれぞれの機器に割り当てられている機器ＩＤを用いるものである。

【００２９】

なお、この場合に、携帯電話端末１０のそれぞれは、ＧＰＳ測位機能を備えると共に、サーバ装置２０に対して、位置・時刻情報を送信する機能を有するものであれば、全く同一の構成を備えるものでなくとも良いことは言うまでもない。

【００３０】

また、位置・時刻情報を携帯電話端末１０からサーバ装置へ送るためのアプリケーションは、予め携帯電話端末に格納しておくようにしても良いが、例えば、携帯電話端末が、サーバ装置２０から、インターネットを通じてダウンロードなどして、取得するようにすることもできる。

【００３１】

サーバ装置２０は、１または複数個の携帯電話端末１０から収集した位置・時刻情報に基づき、例えば、特定の時刻に、特定の場所にいる人にだけ、情報を提供するなどのサービスをするようにする。あるいは、サーバ装置２０に登録された特定の転送先に、収集した情報を転送するようにするサービスを提供するようにすることもできる。

【００３２】

[通信装置の第１の実施形態の構成]

図２は、通信装置の例としての携帯電話端末１０の第１の実施形態の構成例を示すものである。

【００３３】

携帯電話端末１０は、電話通信部３０と、ＧＰＳ信号受信部４０と、位置・時刻計算機能やサーバ装置２０への送信データの生成機能を含む制御部１００とからなる。

【００３４】

電話通信部３０においては、通話用マイクロホン３１からの音声信号は、アンプ３２を通じて信号処理部３３に供給され、この信号処理部３３においてデジタル信号処理や所定の変調処理などが行なわれ、送信用信号に変換される。この送信用信号は、送信部３４を通じ、分配器３５を通じてアンテナ３６に供給され、無線基地局２に送信される。そして、無線基地局２を経由した送信用信号は、通信ネットワーク３を通じて、携帯電話端末３０において指定された相手方に送られるようにされる。

【００３５】

また、無線基地局２を経由して相手方から送られてきた信号の電波は、アンテナ３６で受信され、アンテナ分配器３５、受信部３７を通じて信号処理部３３に供給され、この信号受信部３３において、変調されていた信号が復調される。そして、復調された信号が音声信号であれば、アナログ音声信号に戻され、アンプ３８を通じてスピーカ３９に供給され、音声再生される。

【００３６】

ＧＰＳ信号受信部４０は、ＧＰＳアンテナ４１により受信したＧＰＳ衛星からの電波について、同期捕捉処理を行い、同期捕捉ができたＧＰＳ衛星についてのスペクトラム拡散符号の位相と、キャリア周波数の情報を、制御部１００に供給する。後述するように、制御部１００は、この例では、測位機能を備え、ＧＰＳ信号受信部４０において、４個以上のＧＰＳ衛星からの電波の同期捕捉ができたときに、自機の位置を測定することが可能となる。

【００３７】

なお、このＧＰＳ信号受信部４０は、携帯電話端末１０内に一体不可分に内蔵されていてもよいし、また、アダプタ的に携帯電話端末１０に対して装着可能な構成とされてもよい。ただし、位置・時刻情報の正当性をできるだけ確保するためには、ＧＰＳ信号受信部４０は、携帯電話端末１０内に一体不可分に内蔵されていた方が良い。

【００３８】

制御部１００は、マイクロコンピュータを用いて構成され、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０１に対して、システムバス１０２を介して、プログラムやデータが保持されたＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１０３と、ワークエリア用のＲＡＭ（Ｒａｎｄｏｍ ＡｃｃｅｓｓＭｅｍｏｒｙ）１０４と、Ｉ／Ｏポート１０５～１０８と、キー入力操作部１１０を接続するためのインターフェース１０９と、ＬＣＤ（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）１１２を接続するためのディスプレイインターフェース１１１と、地図メモリ１１３と、時計回路１１４と、機器ＩＤ保持部１１５と、相手先メモリ１１６と、位置・時刻計算部１１７と、位置・時刻情報メモリ１１８と、送信データ生成部１２０とが接続されている。

【００３９】

Ｉ／Ｏポート１０５および１０６を介して、受信部３７および送信部３４に制御部１００から制御信号が供給されて、通信制御がなされる。また、Ｉ／Ｏポート１０７を通じて制御信号が信号処理部３３に供給されて、この信号処理部３３が制御される。

【００４０】

さらに、受信部３７を通じてこの信号処理部３３に供給された信号のうち、音声信号以外のデータや、通信制御用の信号が、この信号処理部３３から制御部１００に供給される。また、制御部１００からの後述する位置・時刻データなどの送信すべきデータや通信制御用の信号が、Ｉ／Ｏポート１０７を通じて信号処理部３３に供給され、送信部３４、アンテナ３６を通じて送信される。

【００４１】

また、ＧＰＳ信号受信部４０からの同期捕捉ができたＧＰＳ衛星についてのスペクトラム拡散符号の位相と、キャリア周波数の情報は、Ｉ／Ｏポート１０８を通じて制御部１００に供給される。また、制御部１００から、制御信号がＧＰＳ信号受信部４０に供給される。

【００４２】

地図メモリ１１３には、予め所定の地区の地図データが格納されていると共に、通信ネットワークを通じて、所定のサーバから現在位置周辺の地図データなど必要な地図データがダウンロードされて格納される。この地図メモリ１１３の地図データは、ＲＯＭ１０３のプログラムやデータにしたがってＣＰＵ１０１により読み出されて地図表示データとされ、ディスプレイインターフェース１１１を通じてＬＣＤ１１２に供給されて、ＬＣＤ１１２の画面に地図表示される。

【００４３】

機器ＩＤ保持部１１５には、携帯電話端末１０のそれぞれ毎に異なる機器ＩＤが格納されて保持されている。この例の機器ＩＤとしては、例えば機器ごとに異なるように一元管理されたシリアル番号が用いられている。前述したように、機器ＩＤは、この第１の実施の形態では、ユーザＩＤとして用いられ、この機器ＩＤがサーバ装置２０に伝えられることにより、サーバ装置２０は、どの携帯電話端末あるいはどのユーザからの情報の受信であるかを認識することができる。

【００４４】

相手先メモリ１１６には、情報収集サーバ装置２０の電話番号のほか、ユーザにより登録された電話の相手先の電話番号が記憶されている。サーバ装置２０の電話番号は、後述するように、自機の位置・時刻情報をサーバ装置２０に通知するタイミングの時に自動的に読み出されて、自動ダイヤル用として用いられる。

【００４５】

位置・時刻計算部１１７は、ＧＰＳ信号受信部４０からの同期捕捉ができた、４個以上の

ＧＰＳ衛星についてのスペクトラム拡散符号の位相と、キャリア周波数の情報を用いて、自機の位置と、そのときの時刻を計算する。位置・時刻計算部１１７で計算された結果得られる位置・時刻情報は、送信データ生成部１２０に送られる。

【００４６】

送信データ生成部１２０は、この第１の実施形態では、デジタル署名生成部１２１と、秘密鍵保持部１２２とを備える。秘密鍵保持部１２２には、機器ＩＤ保持部１１５に保持される機器ＩＤに一意に対応する秘密鍵が、秘密裏に格納されて保持される。

【００４７】

デジタル署名生成部１２１では、ＣＰＵ１０１の指令の下に、システムバス１０２を通じて位置・時刻計算部１１７から送られてくる位置・時刻情報について、秘密鍵保持部１２２に保持されている秘密鍵を用いてデジタル署名を行なう。そして、デジタル署名生成部１２１で生成されたデジタル署名が付加された位置・時刻情報は、送信データとされ、Ｉ／Ｏポート１０７を通じて信号処理部３３に送出され、サーバ装置２０に送られる。

【００４８】

送信データ生成部１２０で生成されたデジタル署名が付加された位置・時刻情報は、また、位置・時刻情報メモリ１１８に記憶される。このメモリ１１８に格納された位置・時刻情報は、キー入力操作部１１０等を用いた送出要求に応じて、後の時点において、任意にサーバ装置２０やその他の必要な相手先に送ることが可能とされている。

【００４９】

また、図示は省略したが、この例の携帯電話端末１０は、アダプタを介してパーソナルコンピュータに接続可能とされており、パーソナルコンピュータからの指示により、位置・時刻情報メモリ１１８に格納されている位置・時刻情報が、適宜のタイミングで、パーソナルコンピュータに吸い上げ可能とされている。

【００５０】

［第１の実施形態におけるサーバ装置２０の構成例］

図３は、第１の実施形態における情報収集サーバ装置２０の構成例を示すもので、マイクロコンピュータで構成されている。すなわち、情報収集サーバ装置２０は、ＣＰＵ２０１に対して、システムバス２０２を介して、プログラムやデータが保持されたＲＯＭ２０３と、ワークエリア用のＲＡＭ２０４と、通信ネットワーク３に接続するための通信インターフェース２０５と、携帯電話端末１０から送られてくる位置・時刻情報を格納するための位置・時刻情報メモリ２０６と、携帯電話端末１０の機器ＩＤを保持する相手機器ＩＤ保持部２０７と、機器ＩＤのそれぞれに一意に対応する公開鍵を保持する公開鍵保持部２０８と、デジタル署名検証部２０９と、相手端末メモリ２１０と、提供情報データベース２１１とからなる。

【００５１】

相手機器ＩＤ保持部２０７には、サーバ装置２０に予め登録された携帯電話端末１０の機器ＩＤが保持されている。なお、ユーザＩＤとして、携帯電話端末１０に割り当てられた電話番号や、ユーザが設定した番号、記号からなる識別情報を用いる場合には、この相手機器ＩＤ保持部２０７には、それぞれの機器ＩＤと、対応する電話番号や識別情報との対応付けも保持されている。この第１の実施形態では、ユーザＩＤとして機器ＩＤを用いているので、相手機器ＩＤ保持部２０７には、それらの対応付けを保持しておく必要はない。

【００５２】

公開鍵保持部２０８には、位置・時刻情報を送ってくると想定される全ての携帯電話端末１０についての公開鍵が、予めダウンロードされる等して、格納されて保持されている。そして、ＣＰＵ２０１からの指令により、機器ＩＤを検索子として、対応する公開鍵が、この公開鍵保持部２０８から読み出される。

【００５３】

デジタル署名検証部２０９は、公開鍵保持部２０８から機器ＩＤを検索子として読み出された公開鍵を用いて、受信した位置・時刻情報に付加されているデジタル署名の検証を行

なう。この例では、後述するように、デジタル署名の検証ができたときには、正当な位置・時刻情報であると判定して、機器ＩＤに対応を付けて位置・時刻情報メモリ２０６に書き込んで、保存するようにするが、デジタル署名の検証ができなかったときには、不正な位置・時刻情報であると判定して、その位置・時刻情報は、廃棄してしまうようにする。

【００５４】

相手端末メモリ２１０には、位置・時刻情報を送ってくる携帯電話端末１０の電話番号や個人情報等を格納するメモリである。前述したように、この実施形態においては、携帯電話端末１０のユーザは、サーバ装置２０にアクセスして、位置・時刻情報を通知するアプリケーションプログラムをダウンロードするが、その際に、サーバ装置２０からの有用な情報の提供を受けるための各端末の電話番号や、各ユーザのプロフィールなどが登録され、このメモリ２１０に格納されるものである。各ユーザのプロフィールは、サーバ装置２０から提供情報を絞り込むときに使用することが可能である。

【００５５】

提供情報データベース２１１には、携帯電話端末１０に対して提供しようとする情報を格納している。この提供情報データベース２１１には、提供元から、適宜のタイミングで提供情報がアップロードされて格納される。あるいは、提供元から提供された記録メディアから読み出された提供情報が格納される。

【００５６】

この例では、サーバ装置２０は、位置・時刻情報メモリ２０６に記憶されている位置・時刻情報を基にして、特定の範囲内の場所に、当該時間帯に存在するであろう携帯電話端末１０を検索し、その検索結果として検出された携帯電話端末１０に対して、その電話番号を相手端末メモリ２１０から読み出して、当該携帯電話端末１０を呼び出し、提供情報データベース２１１から取り出された適宜の情報を、それらの携帯電話端末１０に対して送信するようにする。

【００５７】

次に、この第１の実施形態のシステムにおける携帯電話端末１０からの位置・時刻情報の送信動作およびそれに対するサーバ装置２０における受信動作を、図４および図５のフローチャートを参照しながら説明する。

【００５８】

［携帯電話端末１０からの送信動作（第１の実施形態）、図４］

この実施形態では、携帯電話端末１０が備えるサーバ装置２０へ位置・時刻情報を送るためのアプリケーションは、一定時間間隔ごとに自機の位置・時刻情報をサーバ装置２０に通知するようにするものである。ＣＰＵ１０１は、時計回路１１４の時刻情報を、位置・時刻情報の通知タイミングの計測タイマーとして用いる。なお、図４の各ステップＳの動作は、ＣＰＵ１０１の動作を主として記述したものである。

【００５９】

すなわち、携帯電話端末１０では、先ず、待機状態において（ステップＳ１）、通信（通話）のための操作入力がなされたか否か判別し（ステップＳ２）、操作がなされたと判別したときには、通信（通話）のための処理を実行する（ステップＳ３）。そして、通信（通話）が終了したと判別したときには（ステップＳ４）、ステップＳ１の待機状態に戻る。ステップＳ２～ステップＳ４の処理は、位置・時刻情報のサーバ装置２０への通知に優先して、通信（通話）を行なうようにするためである。

【００６０】

ステップＳ２で、通信（通話）のための操作入力が無かったと判別したときには、位置・時刻情報の通知タイミングとなったかどうか、時計回路１１４の時刻を参照して判別する（ステップＳ５）。位置・時刻情報の通知タイミングでなかったときには、ステップＳ１の待機状態に戻る。

【００６１】

そして、ステップＳ５で、位置・時刻情報の通知タイミングとなったと判別したときには、ＧＰＳ信号受信部４０にＧＰＳ衛星信号の捕捉を指示する（ステップＳ６）。そして、

ＧＰＳ信号受信部４０から、４個以上のＧＰＳ衛星についての捕捉結果がＩ／Ｏポート１０７を通じて取り込まれたときには、ＣＰＵ１０１は、位置・時刻計算部１１７に、自機の受信位置および時刻の計算を指示する（ステップＳ７）。

【００６２】

次に、位置・時刻情報が求められると、ＣＰＵ１０１は、送信データ生成部１２０にデジタル署名の生成・付加処理を指示する（ステップＳ８）。送信データ生成部１２０では、デジタル署名生成部１２１が、秘密鍵保持部１２２からの秘密鍵を用いて、位置・時刻計算部１１７からの位置・時刻情報を暗号化して、デジタル署名を行なう。

【００６３】

次に、ＣＰＵ１０１は、デジタル署名生成部１２１からのデジタル署名が付加された位置・時刻情報を、位置・時刻情報メモリ１１８に書き込むと共に、ＲＡＭ１０４の一部で構成される送信バッファに格納する（ステップＳ９）。

【００６４】

そして、ＣＰＵ１０１は、相手先メモリ１１６から情報収集サーバ装置２０の電話番号を読み出し、自動ダイヤル発信する（ステップＳ１０）。そして、これに対して情報収集サーバ装置２０が応答したか否か判別し（ステップＳ１１）、応答しないと判別したときには、通信中であるか否か判別し（ステップＳ１２）、通信中でなければ、ステップＳ１１に戻って応答を待ち、通信中であれば、ステップＳ１０に戻って、情報収集サーバ装置２０へのダイヤル発信をやり直す。

【００６５】

また、ステップＳ１１で情報収集サーバ装置２０で応答があったと判別したときには、まず、ユーザＩＤとしての機器ＩＤを情報収集サーバ装置２０に送る（ステップＳ１３）。次いで、送信バッファに一次保持されているデジタル署名が付加されている位置・時刻情報を情報収集サーバ装置２０に送信する（ステップＳ１４）。送信が終了したら、サーバ装置２０との通信路を切断する（ステップＳ１５）。

【００６６】

なお、上述の説明は、一定時間間隔で携帯電話端末１０からサーバ装置２０に対して自動的に位置・時刻情報の通知が行なわれる場合であるが、この実施形態の携帯電話端末１０においては、キー入力操作部１１０を操作することにより、ユーザは任意のタイミングで、サーバ装置２０への位置・時刻情報の通知を行なうように指示することが可能なように構成されている。そのための処理ルーチンは、サーバ装置２０への送信の起動がタイマー時間であったものが、ユーザによりキー入力操作指示である点が異なるのみで、図４に示したフローチャートのステップＳ６以降は、全く同様となるものである。

【００６７】

[サーバ装置２０での受信動作（第１の実施の形態）、図５]

次に、携帯電話端末１０からの位置・時刻情報を受信したときのサーバ装置２０の動作を、図５のフローチャートを参照しながら説明する。この図５の各ステップＳの処理は、ＣＰＵ２０１が実行する処理を中心として示したものである。

【００６８】

先ず、携帯電話端末１０からの着信があったか否か判別し（ステップＳ２１）、着信があったときには、それに自動応答する（ステップＳ２２）。すると、前述したように、位置・時刻情報を送信してくる携帯電話端末１０であれば、送信者のユーザＩＤとして機器ＩＤを送ってくるのでそれを確認する（ステップＳ２３）。そして、確認の結果、ＯＫであるか、ＮＧであるかを判別する（ステップＳ２４）。

【００６９】

すなわち、機器ＩＤの受信を確認できなかったとき、また、機器ＩＤは受信したが、相手機器ＩＤ保持部２０７に登録されていない機器ＩＤであったときには、確認ＮＧであるとして、この実施形態では、回線を切断する（ステップＳ２５）。また、受信した機器ＩＤが相手機器ＩＤ保持部２０７に登録されている機器ＩＤであると判別したときには確認ＯＫとして、次に携帯電話端末１０から送られてくるデジタル署名付きの位置・時刻情報を

受信する（ステップＳ２６）。
【００７０】
次に、受信した機器ＩＤを検索子として、公開鍵保持部２０８から、位置・時刻情報を送信してきたユーザ（携帯電話端末）についての公開鍵を読み出し、この公開鍵をデジタル署名検証部２０９に渡し、受信した位置・時刻情報についてのデジタル署名の検証を指示する（ステップＳ２７）。そして、ＣＰＵ２０１は、検証がＯＫであるか否か判別する（ステップＳ２８）。
【００７１】
ＣＰＵ２０１は、デジタル署名の検証ができたと判別したときには、受信した位置・時刻情報は、送信ユーザが当該時刻に当該位置にいたことの証明用データとして、例えば機器ＩＤなどのユーザＩＤと対応付けて位置・時刻情報メモリ２０６に格納する（ステップＳ３０）。
【００７２】
また、デジタル署名の検証ができなかったと判別したときには、受信した位置・時刻情報は、不正な情報であるので、送信ユーザが当該時刻に当該位置にいたことの証明用データとしては使用することができないため、当該位置・時刻情報はメモリ２０６には格納せずに廃棄する（ステップＳ２９）。その後、携帯電話端末１０との間の通信路の切断処理をし（ステップＳ３１）、この受信処理ルーチンを終了する。
【００７３】
以上のようにして、第１の実施形態によれば、通信装置から送信される位置・時刻情報には、通信装置に秘密裏に保持されている秘密鍵が用いられてデジタル署名が付加されるので、当該位置・時刻情報は、少なくとも当該携帯電話端末１０から送信されたものであることが証明可能となる。
【００７４】
このため、例えば当該通信装置以外の機器から、当該通信装置の位置や時刻を偽装した位置・時刻情報をサーバ装置に送信しても、当該偽装は即座に検知され、サーバ装置２０の位置・時刻情報メモリ２０６には、正当な位置・時刻情報のみが蓄積されるものである。
【００７５】
そして、携帯電話端末１０の位置・時刻情報メモリ１１８には、デジタル署名された位置・時刻情報が格納されており、キー入力操作部１１０からの読み出し指示に従って読み出し可能とされるので、この位置・時刻情報メモリ１１８に格納されている情報を、いわゆるアリバイ情報として用いることができる可能性がある。同様に、サーバ装置２０の位置・時刻情報メモリ２０６に格納されている情報も、ユーザＩＤと対応付けられて記録されているので、当該ユーザのアリバイ情報として用いることができる可能性がある。
【００７６】
なお、上述の説明では、ユーザＩＤ（機器ＩＤ）は、位置・時刻情報の伝送に先立ち、サーバ装置２０に送るようにしたが、デジタル署名付きの位置・時刻情報の後に送ることもできる。
【００７７】
また、ユーザＩＤ（機器ＩＤ）は、位置・時刻情報とは別に送るのではなく、位置・時刻情報に含めて送ることもできる。その場合には、サーバ装置２０では、デジタル署名の前に、位置・時刻情報に含まれるユーザＩＤ（機器ＩＤ）を取り出し、それに基づきデジタル署名検証のための公開鍵を公開鍵保持部２０８から読み出すようにする。
【００７８】
なお、上述の第１の実施形態では、サーバ装置２０にのみ、位置・時刻情報を送るようにしたが、携帯電話端末１０のユーザが指定した任意の相手先にも同様にして送ることができる。その場合、当該相手先では、送り手の公開鍵を取得してデジタル署名することができるものである。
【００７９】

なお、サーバ装置は、特定の相手先にさらに位置・時刻情報を転送するようにすることができる。その場合には、位置・時刻情報は暗号化されていた方がよい。特定の相手先のみで位置・時刻情報を解読できるようにして、サーバ装置では、単に情報の中継を行なうだけという使い方ができる。情報の秘匿性を高くし、また、情報の使用対象を特定の機関のみに制限することが容易になる。

【００８０】

[通信装置の第２の実施形態の構成]

図６は、通信装置の例としての携帯電話端末１０の第２の実施形態の構成例を示すものである。この第２の実施形態は、前述の図２に示した第１の実施形態とは、送信データ生成部１２０の構成が異なるのみで、他は全く第１の実施形態と同様に構成される。

【００８１】

この第２の実施形態においては、携帯電話端末１０からサーバ装置２０の送る情報は、暗号化して、情報伝送時の秘匿性を高めるようにしている。これにより、暗号を復号（解読）することができる相手先のみが、位置・時刻情報のデジタル署名の検証をすることができることになり、位置・時刻情報が、それを傍受した任意の第３者によって安易に利用される事態を防止することができる。

【００８２】

そして、この第２の実施形態の携帯電話端末では、この利点を利用して、前述と同様にしてサーバ装置２０に位置・時刻情報を送信する機能を備えるほか、予め暗号化のための公開鍵が保持されている相手先をユーザが発信先として指定して、位置・時刻情報を送信することができるように構成されている。

【００８３】

すなわち、図６に示すように、この第２の実施形態における送信データ生成部１２０は、デジタル署名生成部１２１および秘密鍵保持部１２２に加えて、暗号／復号部１２３と、公開鍵保持部１２４とを備える。

【００８４】

公開鍵保持部１２４には、サーバ装置２０の公開鍵の他、位置・時刻情報の送信を行なう可能性のある相手についての公開鍵が保持されている。暗号／復号部１２３は、位置・時刻情報の送信時には、送信相手の公開鍵を公開鍵保持部１２４から取り出された公開鍵を用いて、デジタル署名付きの位置・時刻情報を暗号化する。

【００８５】

また、暗号／復号部１２３は、位置・時刻情報の受信時には、秘密鍵保持部１２２に保持されている秘密鍵を用いて暗号化されている情報を復号（解読）し、送り手の公開鍵を公開鍵保持部１２４から読み出して、デジタル署名の検証を行なうものである。

【００８６】

[第２の実施形態におけるサーバ装置２０の構成例]

図７は、第２の実施形態における情報収集サーバ装置２０の構成例を示すもので、図３に示した第１の実施形態のサーバ装置２０に、秘密鍵保持部２１２と、復号化部２１３とが追加された構成とされている。

【００８７】

秘密鍵保持部２１２には、サーバ装置２０についての秘密鍵が、秘密裏に格納されて保持されている。復号化部２１３は、携帯電話端末１０から送られてきた暗号化されている情報を、秘密鍵保持部２１２に保持されている秘密鍵を用いて復号（解読）する。そして、復号（解読）したデジタル署名付きの位置・時刻情報をデジタル署名検証部２０９に渡すようにする。

【００８８】

［携帯電話端末１０からサーバ装置２０への送信動作（第２の実施形態）、図８］

図８は、第２の実施形態において、携帯電話端末１０からサーバ装置２０への位置・時刻情報の送信処理動作を示すフローチャートである。この例の場合も、前述の図４の場合と同様に、携帯電話端末１０は、サーバ装置２０へは、一定時間間隔ごとに位置・時刻情報

を通知するようにする。

【００８９】

すなわち、携帯電話端末１０では、先ず、待機状態において（ステップＳ４１）、通信（通話）のための操作入力がなされたか否か判別し（ステップＳ４２）、操作がなされたと判別したときには、通信（通話）のための処理を実行する（ステップＳ４３）。そして、通信（通話）が終了したと判別したときには（ステップＳ４４）、ステップＳ４１の待機状態に戻る。ステップＳ４２～ステップＳ４４の処理は、位置・時刻情報のサーバ装置２０への通知に優先して、通信（通話）を行なうようにするためである。

【００９０】

ステップＳ４２で、通信（通話）のための操作入力が無かったと判別したときには、位置・時刻情報の通知タイミングとなったかどうか、時計回路１１４の時刻を参照して判別する（ステップＳ４５）。位置・時刻情報の通知タイミングでなかったときには、ステップＳ４１の待機状態に戻る。

【００９１】

そして、ステップＳ４５で、位置・時刻情報の通知タイミングとなったと判別したときには、ＧＰＳ信号受信部４０にＧＰＳ衛星信号の捕捉を指示する（ステップＳ４６）。そして、ＧＰＳ信号受信部４０から、４個以上のＧＰＳ衛星についての捕捉結果がＩ／Ｏポート１０７を通じて取り込まれたときには、ＣＰＵ１０１は、位置・時刻計算部１１７に、自機の受信位置および時刻の計算を指示する（ステップＳ４７）。

【００９２】

次に、位置・時刻情報が求められると、ＣＰＵ１０１は、送信データ生成部１２０にデジタル署名の生成・付加処理を指示する。送信データ生成部１２０では、デジタル署名生成部１２１が、秘密鍵保持部１２２からの秘密鍵を用いて、位置・時刻計算部１１７からの位置・時刻情報を暗号化して、デジタル署名を行なう（ステップＳ４８）。

【００９３】

次に、ＣＰＵ１０２は、デジタル署名付きの位置・時刻情報を、位置・時刻情報メモリ１１８に書き込むと共に、ＲＡＭ１０４の一部で構成される送信バッファに格納する（ステップＳ４９）。

【００９４】

そして、ＣＰＵ１０１は、相手先メモリ１１６から情報収集サーバ装置２０の電話番号を読み出し、自動ダイヤル発信する（ステップＳ５０）。そして、これに対して情報収集サーバ装置２０が応答したか否か判別し（ステップＳ５１）、応答しないと判別したときには、通信中であるか否か判別し（ステップＳ５２）、通信中でなければ、ステップＳ５１に戻って応答を待ち、通信中であれば、ステップＳ５０に戻って、情報収集サーバ装置２０へのダイヤル発信をやり直す。

【００９５】

また、ステップＳ５２で、情報収集サーバ装置２０で応答があったと判別したときには、ＣＰＵ１０１は、まず、ユーザＩＤとしての機器ＩＤを情報収集サーバ装置２０に送る（ステップＳ５３）。

【００９６】

次いで、送信バッファに一次保持されている暗号化されているデジタル署名付きの位置・時刻情報と、公開鍵保持部１２４に保持されているサーバ装置２０の公開鍵とを、暗号／復号部１２３に渡し、暗号化指示を行なう。暗号／復号部１２３では、サーバ装置２０の公開鍵を用いて、送信バッファからのデジタル署名が付加された位置・時刻情報を暗号化する（ステップＳ５４）。そして、情報収集サーバ装置２０に送信する（ステップＳ５５）。送信が終了したら、サーバ装置２０との通信路を切断する（ステップＳ５６）。

【００９７】

なお、上述の説明は、一定時間間隔で携帯電話端末１０からサーバ装置２０に対して自動的に位置・時刻情報の通知が行なわれる場合であるが、この実施形態の携帯電話端末１０においては、キー入力操作部１１０を操作することにより、ユーザは任意のタイミングで

、サーバ装置２０への位置・時刻情報の通知を行なうように指示することが可能なように構成されている。そのための処理ルーチンは、サーバ装置２０への送信の起動がタイマー時間であったものが、ユーザによりキー入力操作指示である点が異なるのみで、図８に示したフローチャートのステップＳ６６以降は、全く同様となるものである。

【００９８】

[サーバ装置２０での受信動作（第２の実施の形態）、図９]

次に、携帯電話端末１０からの暗号化されている、デジタル署名付きの位置・時刻情報を受信したときのサーバ装置２０の動作を、図９のフローチャートを参照しながら説明する。この図９の各ステップＳの処理は、ＣＰＵ２０１が実行する処理を中心として示したものである。

【００９９】

先ず、携帯電話端末１０からの着信があったか否か判別し（ステップＳ６１）、着信があったときには、それに自動応答する（ステップＳ６２）。すると、前述したように、位置・時刻情報を送信してくる携帯電話端末１０であれば、送信者のユーザＩＤとして機器ＩＤを送ってくるのでそれを確認する（ステップＳ６３）。そして、確認の結果、ＯＫであるか、ＮＧであるかを判別する（ステップＳ６４）。

【０１００】

すなわち、機器ＩＤの受信を確認できなかったとき、また、機器ＩＤは受信したが、相手機器ＩＤ保持部２０７に登録されていない機器ＩＤであったときには、確認ＮＧであるとして、この実施形態では、回線を切断する（ステップＳ６５）。また、受信した機器ＩＤが相手機器ＩＤ保持部２０７に登録されている機器ＩＤであると判別したときには確認ＯＫとして、次に携帯電話端末１０から送られてくる暗号化されているデジタル署名付きの位置・時刻情報を受信する（ステップＳ６６）。

【０１０１】

次に、ＣＰＵ２０１は、秘密鍵保持部２１２に保持されている秘密鍵を読み出して復号化部２１３に渡し、暗号の復号（解読）処理を指示する。これを受けて、復号化部２１３は、受信情報の復号化処理を実行する（ステップＳ６７）。復号後のデジタル署名付きの位置・時刻情報は、デジタル署名検証部２０９に渡される。

【０１０２】

ＣＰＵ２０１は、次に、受信した機器ＩＤを検索子として、公開鍵保持部２０８から、位置・時刻情報を送信してきたユーザ（携帯電話端末）についての公開鍵を読み出し、この公開鍵をデジタル署名検証部２０９に渡し、受信した位置・時刻情報についてのデジタル署名の検証を指示する（ステップＳ６８）。そして、ＣＰＵ２０１は、検証がＯＫであるか否か判別する（ステップＳ６９）。

【０１０３】

ＣＰＵ２０１は、デジタル署名の検証ができたと判別したときには、受信した位置・時刻情報は、送信ユーザが当該時刻に当該位置にいたことの証明用データとして、例えば機器ＩＤなどのユーザＩＤと対応付けて位置・時刻情報メモリ２０６に格納する（ステップＳ７１）。

【０１０４】

また、デジタル署名の検証ができなかったと判別したときには、受信した位置・時刻情報は、不正な情報であるので、送信ユーザが当該時刻に当該位置にいたことの証明用データとしては使用することができないため、当該位置・時刻情報はメモリ２０６には格納せずに廃棄する（ステップＳ７０）。その後、携帯電話端末１０との間の通信路の切断処理をし（ステップＳ７２）、この受信処理ルーチンを終了する。

【０１０５】

なお、図９においては説明の簡単のため省略したが、ステップＳ６７において暗号の復号ができなかったときには、検証がＮＧであった場合と同様に、ステップＳ７０に進んで、不正なデータとして廃棄処理するようにする。

【０１０６】

［携帯電話端末１０から他の携帯電話端末１０への送信動作（第２の実施形態）、図１０］

この第２の実施形態の携帯電話端末１０においては、前述したようにサーバ装置のみではなく、ユーザが指定したときには、通信の相手先の携帯電話端末１０に対しても、暗号化したデジタル署名付きの位置・時刻情報の送信ができるようにしている。この場合において、第２の実施形態においては、携帯電話端末１０同士においては、互いの公開鍵は、相手方の電話番号を検索子としてそれぞれの公開鍵保持部１２４に保持しているものである。

【０１０７】

携帯電話端末１０においては、ＣＰＵ１０１は、まず、発呼操作が行われたか否か判別する（ステップＳ１２１）。発呼操作が行われなかったときには、その他の処理を行なう（ステップＳ１２２）。ステップＳ１２１で発呼操作が行われたと判別したときには、ＣＰＵ１０１は、発呼処理を実行する（ステップＳ１２３）。

【０１０８】

そして、相手応答を待ち（ステップＳ１２４）、相手応答がないままオンフック操作されたか否か判別し（ステップＳ１２５）、オンフックされたときには、発呼中止されたとしてこの処理ルーチンを終了する。オンフックされなかったときには、ステップＳ１２４において相手応答を待つ。

【０１０９】

そして、ステップＳ１２４で相手応答を確認したときには、通信路を形成して、相手との間で通信中となる（ステップＳ１２６）。この通信中において、位置・時刻情報の送信操作がなされたか否か判別し（ステップＳ１２７）、前記送信操作がなされないと判別したときには、通信終了操作がなされたか否か判別する（ステップＳ１３１）。そして、通信終了操作がなされたと判別したときには、この処理ルーチンを終了する。また、通信終了操作がなされなかったと判別したときにはステップＳ１２６に戻る。

【０１１０】

そして、ステップＳ１２７において、位置・時刻情報の送信操作がなされたと判別したときには、位置・時刻計算部１１７で計算された位置・時刻情報をデジタル署名生成部１２１に送り、秘密鍵保持部１２２の秘密鍵を用いてデジタル署名を実行させる。そして、デジタル署名付きの位置・時刻情報を位置・時刻情報メモリ１１８に格納する（ステップＳ１２８）。

【０１１１】

また、デジタル署名付きの位置・時刻情報を暗号／復号部１２３に送り、通信相手先の公開鍵を公開鍵保持部１２４から得て、暗号／復号部１２３において、デジタル署名付きの位置・時刻情報を当該公開鍵により暗号化するようにする（ステップＳ１２９）。そして、その暗号化した情報を通信の相手方に送信する（ステップＳ１３０）。そして、ステップＳ１３１に戻る。

【０１１２】

［他の携帯電話端末１０からの位置・時刻情報の受信動作（第２の実施形態）、図１１］

図１０のようにして他の携帯電話端末１０に送信された位置・時刻情報は、受信側の携帯電話端末１０において、図１１に示すようにして受信処理される。

【０１１３】

すなわち、携帯電話端末１０では、着信があったか否か判別し（ステップＳ１４１）、着信があったと判別したときには応答操作がなされたか否か判別する（ステップＳ１４２）。そして、応答操作なされる前に、相手が切断したか否か判別し（ステップＳ１４３）、相手切断を確認したら、着信処理を終了する。相手切断がなされなかったときにはステップＳ１４２に戻って応答操作を待ち、応答操作を確認すると通信中状態になる（ステップＳ１４４）。なお、どの相手からの着信であるかは、発呼メッセージに含まれる電話番号によりＣＰＵ１０１は、認識するものである。

【０１１４】

そして、この通信中状態において、位置・時刻情報を受信したか否か判別し（ステップＳ１４５）、位置・時刻情報を受信しないと判別したときには、通信終了操作がなされたか否か判別する（ステップＳ１５４）。そして、通信終了操作がなされたと判別したときには、この処理ルーチンを終了する。また、通信終了操作がなされなかったと判別したときにはステップＳ１４４に戻る。

【０１１５】

そして、ステップＳ１４５において、位置・時刻情報を受信したと判別したときには、ＣＰＵ１０１は、秘密鍵保持部１２２に保持されている秘密鍵を用いて、暗号／復号部１２３において、復号処理を行なうように制御する（ステップＳ１４６）。

【０１１６】

このステップＳ１４６での復号処理により、復号ができなかったときには、その旨を示すＮＧメッセージをＬＣＤ１１２に表示するとともに、送信してきた相手にもＮＧメッセージを送るようにする（ステップＳ１４８）。そして、ステップＳ１５４に進む。

【０１１７】

また、ステップＳ１４６での復号処理により、復号ができたときには、デジタル署名を、送信者の公開鍵を公開鍵保持部１２４から取り出して、デジタル署名の検証を行なう（ステップＳ１４９）。なお、図６では、デジタル署名検証部の図示を省略してある。

【０１１８】

このデジタル署名の検証の結果を判別し（ステップＳ１５０）、検証がＮＧであれば、ステップＳ１４８に進み、ＮＧメッセージをＬＣＤ１１２の画面に表示すると共に、ＮＧメッセージを相手端末へも送信する。

【０１１９】

また、デジタル署名の検証の結果、検証がＯＫであれば、ＯＫメッセージをＬＣＤ１１２の画面に表示すると共に、ＯＫメッセージを相手端末へも送信する（ステップＳ１５１）。その後、ＯＫであった、相手の位置・時刻情報を、当該相手のユーザＩＤと対応付けて位置・時刻情報メモリ１１８に格納する（ステップＳ１５２）。これは、後日、相手の位置・時刻の証明のために用いられる場合があることを考慮したものである。

【０１２０】

その後、相手の位置を、ＬＣＤ１１２の地図上に、相手の名前など識別可能な表示と共に表示するようにする（ステップＳ１５３）。そして、ステップＳ１５４に戻る。なお、このステップＳ１５３の処理は、位置・時刻情報の利用形態の一態様である。

【０１２１】

以上説明したように、この第２の実施形態によれば、第１の実施形態と同様の作用効果に加えて、暗号化により、携帯電話端末１０からサーバ装置２０また携帯電話端末１０間での通信において、伝送情報の秘匿性を高めることができるという効果がある。

【０１２２】

[携帯機器の第３の実施形態および第３の実施形態の場合のサーバ装置]

携帯機器の第３の実施形態は、デジタル署名する前に、位置・時刻情報を、特定の相手の公開鍵を用いて暗号化することにより、デジタル署名は、受信者が行なうようにするが、位置・時刻情報は、受信者には秘匿して他の相手にのみ通知することができるようにする場合である。

【０１２３】

[通信装置の第３の実施形態および第３の実施形態の場合のサーバ装置]

通信装置の第３の実施形態は、デジタル署名する前に、位置・時刻情報を、特定の相手の公開鍵を用いて暗号化することにより、デジタル署名は、受信者が行なうようにするが、位置・時刻情報は、受信者には秘匿して他の相手にのみ通知することができるようにする場合である。

【０１２４】

［携帯電話端末１０からサーバ装置２０への送信動作（第３の実施形態）、図１２］

図１２は、第３の実施形態において、携帯電話端末１０からサーバ装置２０への位置・時

刻情報の送信処理動作を示すフローチャートである。この例の場合も、前述の図４や図８の場合と同様に、携帯電話端末１０は、サーバ装置２０へは、一定時間間隔ごとに位置・時刻情報を通知するようにする。

【０１２５】

すなわち、携帯電話端末１０では、先ず、待機状態において（ステップＳ８１）、通信（通話）のための操作入力がなされたか否か判別し（ステップＳ８２）、操作がなされたと判別したときには、通信（通話）のための処理を実行する（ステップＳ８３）。そして、通信（通話）が終了したと判別したときには（ステップＳ８４）、ステップＳ８１の待機状態に戻る。ステップＳ８２～ステップＳ８４の処理は、位置・時刻情報のサーバ装置２０への通知に優先して、通信（通話）を行なうようにするためである。

【０１２６】

ステップＳ８２で、通信（通話）のための操作入力が無かったと判別したときには、位置・時刻情報の通知タイミングとなったかどうか、時計回路１１４の時刻を参照して判別する（ステップＳ８５）。位置・時刻情報の通知タイミングでなかったときには、ステップＳ８１の待機状態に戻る。

【０１２７】

そして、ステップＳ８５で、位置・時刻情報の通知タイミングとなったと判別したときには、ＧＰＳ信号受信部４０にＧＰＳ衛星信号の捕捉を指示する（ステップＳ８６）。そして、ＧＰＳ信号受信部４０から、４個以上のＧＰＳ衛星についての捕捉結果がＩ／Ｏポート１０７を通じて取り込まれたときには、ＣＰＵ１０１は、位置・時刻計算部１１７に、自機の受信位置および時刻の計算を指示する（ステップＳ８７）。

【０１２８】

次に、位置・時刻情報が求められると、ＣＰＵ１０１は、送信データ生成部１２０に暗号化指示する。すなわち、ユーザにより指定された位置・時刻情報を通知したい相手の公開鍵を公開鍵保持部１２４から取り出し、暗号／復号部１２３に渡す。また、暗号／復号部１２３に位置・時刻計算部１１７からの位置・時刻情報も渡す。そして、暗号／復号部１２３に対して、公開鍵を用いて、位置・時刻情報を暗号化するように指示する（ステップＳ８８）。ここで、位置・時刻情報を通知したい相手は、通信の相手、ここではサーバ装置２０であってもよいし、通信の相手と異なる他の相手であってもよい。

【０１２９】

次いで、ＣＰＵ１０１は、送信データ生成部１２０にデジタル署名の生成・付加処理を指示する。送信データ生成部１２０では、デジタル署名生成部１２１が、秘密鍵保持部１２２からの秘密鍵を用いて、暗号／復号部１２３で暗号化された位置・時刻情報を暗号化して、デジタル署名を行なう（ステップＳ８９）。

【０１３０】

次に、ＣＰＵ１０２は、デジタル署名付きの位置・時刻情報を、位置・時刻情報メモリ１１８に書き込むと共に、ＲＡＭ１０４の一部で構成される送信バッファに格納する（ステップＳ９０）。

【０１３１】

そして、ＣＰＵ１０１は、相手先メモリ１１６から情報収集サーバ装置２０の電話番号を読み出し、自動ダイヤル発信する（ステップＳ９１）。そして、これに対して情報収集サーバ装置２０が応答したか否か判別し（ステップＳ９２）、応答しないと判別したときには、通信中であるか否か判別し（ステップＳ９３）、通信中でなければ、ステップＳ９２に戻って応答を待ち、通信中であれば、ステップＳ９１に戻って、情報収集サーバ装置２０へのダイヤル発信をやり直す。

【０１３２】

また、ステップＳ９２で、情報収集サーバ装置２０で応答があったと判別したときには、ＣＰＵ１０１は、まず、ユーザＩＤとしての機器ＩＤを情報収集サーバ装置２０に送る（ステップＳ９４）。

【０１３３】

次いで、送信バッファに一次保持されているデジタル署名付きの暗号化されている位置・時刻情報を、情報収集サーバ装置２０に送信する（ステップＳ９５）。送信が終了したら、サーバ装置２０との通信路を切断する（ステップＳ９６）。

【０１３４】

なお、上述の説明は、一定時間間隔で携帯電話端末１０からサーバ装置２０に対して自動的に位置・時刻情報の通知が行なわれる場合であるが、この実施形態の携帯電話端末１０においては、キー入力操作部１１０を操作することにより、ユーザは任意のタイミングで、サーバ装置２０への位置・時刻情報の通知を行なうように指示することが可能なように構成されている。そのための処理ルーチンは、サーバ装置２０への送信の起動がタイマー時間であったものが、ユーザによりキー入力操作指示である点が異なるのみで、図１２に示したフローチャートのステップＳ８６以降は、全く同様となるものである。

【０１３５】

[サーバ装置２０での受信動作（第３の実施の形態）、図１３]

次に、携帯電話端末１０からの暗号化されている、デジタル署名付きの位置・時刻情報を受信したときのサーバ装置２０の動作を、図１３のフローチャートを参照しながら説明する。この図１３の各ステップＳの処理は、ＣＰＵ２０１が実行する処理を中心として示したものである。

【０１３６】

先ず、携帯電話端末１０からの着信があったか否か判別し（ステップＳ１０１）、着信があったときには、それに自動応答する（ステップＳ１０２）。すると、前述したように、位置・時刻情報を送信してくる携帯電話端末１０であれば、送信者のユーザＩＤとして機器ＩＤを送ってくるのでそれを確認する（ステップＳ１０３）。そして、確認の結果、ＯＫであるか、ＮＧであるかを判別する（ステップＳ１０４）。

【０１３７】

すなわち、機器ＩＤの受信を確認できなかったとき、また、機器ＩＤは受信したが、相手機器ＩＤ保持部２０７に登録されていない機器ＩＤであったときには、確認ＮＧであるとして、この実施形態では、回線を切断する（ステップＳ１０５）。また、受信した機器ＩＤが相手機器ＩＤ保持部２０７に登録されている機器ＩＤであると判別したときには確認ＯＫとして、次に携帯電話端末１０から送られてくるデジタル署名付きの暗号化されている位置・時刻情報を受信する（ステップＳ１０６）。

【０１３８】

次に、ＣＰＵ２０１は、受信した機器ＩＤを検索子として、公開鍵保持部２０８から、位置・時刻情報を送信してきたユーザ（携帯電話端末）についての公開鍵を読み出し、この公開鍵をデジタル署名検証部２０９に渡し、受信した位置・時刻情報についてのデジタル署名の検証を指示する（ステップＳ１０７）。そして、ＣＰＵ２０１は、検証がＯＫであるか否か判別する（ステップＳ１０８）。

【０１３９】

ＣＰＵ２０１は、デジタル署名の検証ができなかったと判別したときには、受信した位置・時刻情報は、不正な情報であるので、送信ユーザが当該時刻に当該位置にいたことの証明用データとしては使用することができないため、当該位置・時刻情報はメモリ２０６には格納せずに廃棄する（ステップＳ１０９）。その後、携帯電話端末１０との間の通信路の切断処理をし（ステップＳ１１２）、この受信処理ルーチンを終了する。

【０１４０】

また、ＣＰＵ２０１は、デジタル署名の検証ができたと判別したときには、秘密鍵保持部２１２に保持されている秘密鍵を読み出して復号化部２１３に渡し、暗号の復号（解読）処理を指示する。これを受けて、復号化部２１３は、位置・時刻情報の復号化処理を実行する（ステップＳ１１０）。

【０１４１】

そして、ＣＰＵ２０１は、受信した位置・時刻情報は、送信ユーザが当該時刻に当該位置にいたことの証明用データとして、例えば機器ＩＤなどのユーザＩＤと対応付けて位置・

時刻情報メモリ２０６に格納する（ステップＳ１１１）。そして、ステップＳ１１２に進み、通信路の切断処理をし、この受信処理ルーチンを終了する。

【０１４２】

なお、図１３においては説明の簡単のため省略したが、ステップＳ１１１において暗号の復号ができなかったときには、検証がＮＧであった場合と同様に、ステップＳ１０９に進んで、不正なデータとして廃棄処理するようにする。

【０１４３】

以上説明した第３の実施形態の場合には、デジタル署名を行なう前の位置・時刻情報を暗号化するようにしたので、当該暗号化に用いる公開鍵を通信の相手ではない他の者とすることできるので、個人の位置・時刻情報についての秘密を保持して、特定の通信相手に送ることができるようになるという効果がある。

【０１４４】

例えば、デジタル署名は特定の受け付け人が行ない、位置・時刻情報は、その受け付け人以外の特定の者が暗号解読して見ることができるようにするという用い方が可能となる。

【０１４５】

[通信装置の第４の実施形態の構成例]

以上の例では、機器ＩＤをユーザＩＤとして用いたが、いわゆるＳＩＭカードやＰＫＩカードなどの個人用のＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ；集積回路）カードを用いることにより、各個人のＩＤをユーザＩＤとして用いることができる。つまり、同じ携帯電話端末を用いる場合であっても使用者を区別して、使用者毎の位置・時刻情報の通信が可能となる。

【０１４６】

図１４は、この第４の実施形態における携帯電話端末１０の構成例を示すものである。この図１４の例においては、送信データ生成部１２０は設けられず、その代わりに、ＩＣカードインターフェース１３１を介してＩＣカード装填機構１３２がシステムバス１０２に接続される。そして、ＩＣカード装填機構１３２に対しては、ＩＣカード５０が装填可能とされている。

【０１４７】

また、この第４の実施形態においては、ユーザＩＤとしては、ＩＣカード５０内に保持される個人識別情報からなるユーザＩＤが用いられる。また、位置・時刻情報メモリは、ＩＣカード５０内に設けられるため、携帯電話端末１０には、位置・時刻情報メモリ１１８を設ける必要はない。その他は、図２の携帯電話端末１０とほぼ同様の構成である。

【０１４８】

次に、ＩＣカード５０の構成例を図１５に示す。すなわち、ＩＣカード５０は、ＣＰＵ５０１に対して、システムバス５０２を通じて、プログラムやデータが格納されているＲＯＭ５０３と、ワークエリア用のＲＡＭ５０４と、携帯電話端末１０のＩＣカード装填機構１３２に装填されたときに、携帯電話端末１０に接続するためのインターフェース５０５と、ユーザＩＤ保持部５０６と、位置・時刻情報メモリ５０７と、秘密裏にＩＣカードごとに異なる秘密鍵が書き込まれている秘密鍵保持部５０８と、デジタル署名生成部５０９と、自分および通信等の相手の公開鍵を保持する公開鍵保持部５１０と、暗号／復号部５１１とが接続されて構成されている。

【０１４９】

図１６にＩＣカード５０の発行手順と、相手との通信の際に必要な手順について説明する。

【０１５０】

例えばユーザＡは、ＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ；認証）局をも兼ねるＩＣカード発行会社に対してユーザ登録して、ＩＣカードを購入する。この購入の際に、ＩＣカードには、ＣＡ局により次のような情報が書き込まれる。まず、登録されたユーザＩＤがユーザＩＤ保持部５０６に格納されると共に、登録されたユーザＡについての秘密鍵が秘密裏に秘密鍵保持部５０８に格納される。また、ＣＡ局のデジタル署名

付きのユーザＡの公開鍵からなるユーザＡの証明書Ａが公開鍵保持部５１０に格納されると共に、ＣＡ局の公開鍵が公開鍵保持部５１０に格納される。

【０１５１】

他のユーザＢについても同様にして、ユーザ登録および購入要求に応じて、ユーザＢのＩＣカードが発行される。そのＩＣカードには、同様にして、ユーザＢの秘密鍵が秘密鍵保持部５０８に格納され、また、ＣＡ局のデジタル署名付きのユーザＢの公開鍵からなるユーザＢの証明書Ｂと、ＣＡ局の公開鍵が公開鍵保持部５１０に格納される。

【０１５２】

ＣＡ局は、登録された全てのユーザの証明書を、ディレクトリサーバに公開する。ユーザＡと、ユーザＢとの間で通信を行うとする場合には、予め、ユーザＡは、ユーザＢの証明書Ｂを、ディレクトリサーバからダウンロードし、また、ユーザＢは、ユーザＡの証明書Ａを、ディレクトリサーバからダウンロードして、それぞれ公開鍵保持部５１０に格納しておく。

【０１５３】

そして、この第４の実施形態において、前述した第１の実施形態を適用して位置・時刻情報を、例えばユーザＡからユーザＢに送る場合には、ユーザＡは、自己のＩＣカード５０をＩＣカード装填機構１３２に装填し、ユーザＢを通信相手として指定して、位置・時刻情報の送信操作を行なう。

【０１５４】

すると、ＣＰＵ１０１は、まず、ＩＣカード５０のユーザＩＤ保持部５０６に保持されているユーザＩＤを取得して、ユーザＢに送る。そして、位置・時刻計算部１１７で計算した結果の位置・時刻情報を、ＩＣカード５０に送る。すると、ＩＣカード５０では、ＣＰＵ５０１の制御の下に、デジタル署名生成部５０９でデジタル署名を行ない、その結果としてのデジタル署名付きの位置・時刻情報を位置・時刻情報メモリ５０７に記憶すると共に、インターフェース５０５を通じて携帯電話端末１０に送出する。

【０１５５】

携帯電話端末１０は、このデジタル署名付きの位置・時刻情報をＩＣカードインターフェース部１３１を通じて受け取り、Ｉ／Ｏポート１１７を通じて信号処理部３３および送信部３４を通じて、アンテナ３６に送り出し、ユーザＢに送信するようにする。

【０１５６】

また、この第４の実施形態において、前述した第２の実施形態を適用して、位置・時刻情報を、例えばユーザＡからユーザＢに送る場合には、ＩＣカード５０では、携帯電話端末１０から受け取った位置・時刻情報をデジタル署名生成部５０９において、デジタル署名を生成・付加した後、デジタル署名付きの位置・時刻情報を位置・時刻情報メモリ５０７に記憶すると共に、暗号／復号部５１１において、公開鍵保持部５１０に保持されているユーザＢの公開鍵を用いて、デジタル署名付きの位置・時刻情報を暗号化する。そして、暗号化したデジタル署名付きの位置・時刻情報を、インターフェース５０５を通じて携帯電話端末１０に送出するようにする。

【０１５７】

なお、この場合には、ＩＣカード５０には、位置・時刻情報に加えて、通信相手となるユーザＢの情報の伝達される。ＩＣカード５０内において、ユーザＢの公開鍵を検索するためである。

【０１５８】

さらに、この第４の実施形態において、前述した第３の実施形態を適用して、位置・時刻情報を、例えばユーザＡからユーザＢに送る場合には、ＩＣカード５０では、携帯電話端末１０から受け取った位置・時刻情報を、暗号／復号部５１１において、公開鍵保持部５１０に保持されているユーザＢの公開鍵を用いて暗号化する。その後、デジタル署名生成部５０９において、暗号化されている位置・時刻情報について、デジタル署名を生成・付加した後、デジタル署名付きの位置・時刻情報を位置・時刻情報メモリ５０７に記憶すると共に、デジタル署名付きの暗号化した位置・時刻情報を、インターフェース５０５を通

じて携帯電話端末１０に送出するようにする。
【０１５９】
なお、この場合にも、ＩＣカード５０には、位置・時刻情報に加えて、通信相手となるユーザＢの情報の伝達される。ＩＣカード５０内において、ユーザＢの公開鍵を検索するためである。
【０１６０】
［携帯電話端末１０からサーバ装置２０への送信動作（第４の実施形態）、図１７～図２０］
この第４の実施形態において、前述の第１～第３の実施形態と同様に、位置・時刻情報が情報収集サーバ装置２０の場合に収集される場合には、サーバ装置２０の公開鍵保持部２０８には、機器ＩＤの代わりに、ＩＣカード５０のユーザＩＤ保持部５０６に保持されるユーザＩＤを検索子として、検索可能な状態で、各ユーザの公開鍵が格納されるものである。
【０１６１】
次に、ＩＣカード５０を用いた場合における携帯電話端末１０からサーバ装置２０に位置・時刻情報を送信する動作について、図１７を参照して説明する。なお、この例においても、前述の図４、図８や図１２の場合と同様に、携帯電話端末１０は、サーバ装置２０へは、一定時間間隔ごとに位置・時刻情報を通知するようにする。
【０１６２】
すなわち、携帯電話端末１０では、先ず、待機状態において（ステップＳ１６１）、通信（通話）のための操作入力がなされたか否か判別し（ステップＳ１６２）、操作がなされたと判別したときには、通信（通話）のための処理を実行する（ステップＳ１６３）。そして、通信（通話）が終了したと判別したときには（ステップＳ１６４）、ステップＳ１６１の待機状態に戻る。ステップＳ１６２～ステップＳ１６４の処理は、位置・時刻情報のサーバ装置２０への通知に優先して、通信（通話）を行なうようにするためである。
【０１６３】
ステップＳ１６２で、通信（通話）のための操作入力が無かったと判別したときには、位置・時刻情報の通知タイミングとなったかどうか、時計回路１１４の時刻を参照して判別する（ステップＳ１６５）。位置・時刻情報の通知タイミングでなかったときには、ステップＳ１６１の待機状態に戻る。
【０１６４】
そして、ステップＳ１６５で、位置・時刻情報の通知タイミングとなったと判別したときには、ＧＰＳ信号受信部４０にＧＰＳ衛星信号の捕捉を指示する（ステップＳ１６６）。そして、ＧＰＳ信号受信部４０から、４個以上のＧＰＳ衛星についての捕捉結果がＩ／Ｏポート１０７を通じて取り込まれたときには、ＣＰＵ１０１は、位置・時刻計算部１１７に、自機の受信位置および時刻の計算を指示する（ステップＳ１６７）。
【０１６５】
次に、位置・時刻情報が求められると、ＣＰＵ１０１は、位置・時刻計算部１１７から位置・時刻情報をＩＣカード５０に転送するように指示する（ステップＳ１６８）。
【０１６６】
前述の第１の実施形態のように、位置・時刻情報にデジタル署名を生成・付加してサーバ装置２０に送る場合であれば、ＩＣカード５０では、図１８に示すような処理を実行する。なお、この図１８の処理は、ＣＰＵ５０１の処理を中心として記述したものである。
【０１６７】
すなわち、まず、インターフェース５０５を通じて、位置・時刻情報を取得する（ステップＳ１８１）。次に、ＣＰＵ５０１は、取得した位置・時刻情報をデジタル署名生成部５０９に転送する。デジタル署名生成部５０９では、秘密鍵保持部５０８に保持されている秘密鍵を用いて、位置・時刻情報についてのデジタル署名を生成し、付加する（ステップＳ１８２）。
【０１６８】

次に、ＣＰＵ５０１は、デジタル署名が付加された位置・時刻情報を位置・時刻情報メモリ５０７に格納する（ステップＳ１８３）。さらに、デジタル署名が付加された位置・時刻情報を、インターフェース５０５を通じて携帯電話端末１０に返すようにする（ステップＳ１８４）。

【０１６９】

携帯電話端末１０のＣＰＵ１０１は、このＩＣカード５０からの出力データを、ＩＣカードインターフェース部１３１を通じて取得し、ＲＡＭ１０４の一部で構成される送信バッファに格納する（図１７のステップＳ１６９）。

【０１７０】

そして、ＣＰＵ１０１は、相手先メモリ１１６から情報収集サーバ装置２０の電話番号を読み出し、自動ダイヤル発信する（ステップＳ１７０）。そして、これに対して情報収集サーバ装置２０が応答したか否か判別し（ステップＳ１７１）、応答しないと判別したときには、通信中であるか否か判別し（ステップＳ１７２）、通信中でなければ、ステップＳ１７１に戻って応答を待ち、通信中であれば、ステップＳ１７０に戻って、情報収集サーバ装置２０へのダイヤル発信をやり直す。

【０１７１】

また、ステップＳ１７１で情報収集サーバ装置２０で応答があったと判別したときには、まず、ＩＣカード５０のユーザＩＤ保持部５０６から取得したユーザＩＤを情報収集サーバ装置２０に送る（ステップＳ１７３）。次いで、送信バッファに一次保持されているデジタル署名が付加されている位置・時刻情報を情報収集サーバ装置２０に送信する（ステップＳ１７４）。送信が終了したら、サーバ装置２０との通信路を切断する（ステップＳ１７５）。

【０１７２】

以上は、サーバ装置２０に送る情報の態様が第１の実施形態の場合であるが、サーバ装置２０に送る情報の態様が第２の実施形態の場合であれば、ＩＣカード５０では、図１９に示すようにして、送信データを生成する。また、サーバ装置２０に送る情報の態様が第３の実施形態の場合であれば、ＩＣカード５０では、図２０に示すようにして、送信データを生成する。

【０１７３】

先ず、第２の実施形態の場合におけるＩＣカード５０での処理を図１９のフローチャートを参照して説明する。

【０１７４】

すなわち、まず、インターフェース５０５を通じて、位置・時刻情報を取得する（ステップＳ１９１）。次に、ＣＰＵ５０１は、取得した位置・時刻情報をデジタル署名生成部５０９に転送する。デジタル署名生成部５０９では、秘密鍵保持部５０８に保持されている秘密鍵を用いて、位置・時刻情報についてデジタル署名を生成し、付加する（ステップＳ１９２）。

【０１７５】

次に、ＣＰＵ５０１は、デジタル署名が付加された位置・時刻情報を位置・時刻情報メモリ５０７に格納する（ステップＳ１９３）。さらに、ＣＰＵ５０１は、デジタル署名が付加された位置・時刻情報を、暗号／復号部５１１に送る。暗号／復号部５１１では、携帯電話端末１０からの通信相手の情報を基にして、サーバ装置２０の公開鍵を公開鍵保持部５１０から取得し、取得した公開鍵を用いてデジタル署名付きの位置・時刻情報を暗号化する（ステップＳ１９４）。そして、暗号化したデジタル署名付きの位置・時刻情報を、インターフェース５０５を通じて携帯電話端末１０に返すようにする（ステップＳ１９５）。

【０１７６】

次に、第３の実施形態の場合におけるＩＣカード５０での処理を図２０のフローチャートを参照して説明する。

【０１７７】

すなわち、まず、インターフェース５０５を通じて、位置・時刻情報を取得する（ステップＳ２０１）。次に、ＣＰＵ５０１は、取得した位置・時刻情報を暗号／復号部５１１に転送する。暗号／復号部５１１では、ユーザが指定した位置・時刻情報を通知したい相手の情報を基にして、当該位置・時刻情報を通知したい相手の公開鍵を公開鍵保持部５１０から取得し、取得した公開鍵を用いてデジタル署名付きの位置・時刻情報を暗号化する（ステップＳ２０２）。

【０１７８】

次に、ＣＰＵ５０１は、暗号化した位置・時刻情報をデジタル署名生成部５０９に転送する。デジタル署名生成部５０９では、秘密鍵保持部５０８に保持されている秘密鍵を用いて、暗号化された位置・時刻情報についてデジタル署名を生成し、付加する（ステップＳ２０３）。

【０１７９】

次に、ＣＰＵ５０１は、デジタル署名が付加された暗号化された位置・時刻情報を位置・時刻情報メモリ５０７に格納する（ステップＳ２０４）。さらに、ＣＰＵ５０１は、デジタル署名付きの暗号化された位置・時刻情報を、インターフェース５０５を通じて携帯電話端末１０に返すようにする（ステップＳ２０５）。

【０１８０】

なお、上述の説明は、一定時間間隔で携帯電話端末１０からサーバ装置２０に対して自動的に位置・時刻情報の通知が行なわれる場合であるが、この第４の実施形態の携帯電話端末１０においても、キー入力操作部１１０を操作することにより、ユーザは任意のタイミングで、サーバ装置２０への位置・時刻情報の通知を行なうように指示することが可能なように構成されている。そのための処理ルーチンは、サーバ装置２０への送信の起動がタイマー時間であったものが、ユーザによりキー入力操作指示である点が異なるのみで、図１７に示したフローチャートのステップＳ１６６以降は、全く同様となるものである。

【０１８１】

以上説明した第４の実施形態においては、位置・時刻情報には、ＩＣカード５０の秘密鍵により、デジタル署名がなされるので、携帯電話端末ごとの証明ではなく、ＩＣカード５０を所持するユーザごとの位置・時刻の証明が可能となるものである。

【０１８２】

なお、上述の第４の実施形態の説明においては、通信装置として、携帯電話端末にＩＣカードを装填して使用する場合を説明したが、位置・時刻情報を送信するだけでなく、ＩＣカード内のメモリに記憶する用途をも考慮すると、ＧＰＳ受信機能付きのＰＤＡ、ＧＰＳ受信機能付きのモバイルパーソナルコンピュータ、ＧＰＳ受信機能付きのデジタルカメラ、ＧＰＳ機能付きのカーナビゲーションシステム、ＧＰＳ受信機能付きの時計などにも適用可能である。

【０１８３】

この場合において、ＧＰＳ受信機能は、アダプタとして、それぞれの通信装置に接続される態様であっても良いことは前述した通りである。

【０１８４】

[実施形態の変形例]

なお、上述の図４、図８、図１０、図１７の説明では、サーバ装置２０に発呼をする前に、ＧＰＳ信号受信部４０にＧＰＳ衛星信号の捕捉指示を出して、４個以上のＧＰＳ衛星からの電波の捕捉を行ない、位置・時刻の計算が終了するようにしたが、これは、サーバ装置２０に位置・時刻情報を通知するタイミングのときに、ＧＰＳ信号受信部４０が非動作であって、測位までに時間がかかることを考慮したものである。

【０１８５】

サーバ装置２０に位置・時刻情報を通知するタイミングのときに、ＧＰＳ信号受信部４０が動作中であって、携帯電話端末１０において、既に位置・時刻情報が得られていた場合には、ステップＳ６およびステップＳ７、ステップＳ４６およびステップＳ４７、ステップＳ８６およびステップＳ８７、ステップＳ１６６およびステップＳ１６７は不要となる

。そして、その場合には、サーバ装置２０に発呼を行なって、サーバ装置２０の応答を確認したら、既に求められている位置・時刻情報についてデジタル署名を行ない、位置・時刻情報メモリ１１８に格納するとともに、サーバ装置２０に送信するようにするものである。

【０１８６】

また、上述の実施形態では、通信装置として携帯電話端末の場合を例に説明したが、通信装置としては、携帯電話端末に限られるものではなく、前述したような、ＰＤＡ、モバイルパーソナルコンピュータ、デジタルカメラ等にも適用できるものである。

【０１８７】

また、上述の実施形態では、測位用衛星としてＧＰＳ衛星を用いた場合について説明したが、ＧＰＳ衛星にかぎらず、他の測位用衛星からの電波を受信して測位する場合にも、この発明が適用できることは勿論である。

【０１８８】

【発明の効果】

以上説明したように、この発明によれば、通信装置においてデジタル署名を位置・時刻情報に付加するようにするので、このデジタル署名を検証することにより、他の通信装置などからの偽装の位置・時刻情報を容易に検知することができ、位置・時刻情報の改ざんを防止することができる。

【０１８９】

また、デジタル署名により、位置・時刻情報の正当性を高めることができるという効果がある。

【０１９０】

また、位置・時刻情報を、特定の相手の公開鍵で暗号化するようにしたことにより、当該特定の相手以外に、位置・時刻情報を秘匿することが可能になる。

【図面の簡単な説明】

【図１】　この発明による通信装置の実施形態が適用されたシステムの概要を説明するための図である。

【図２】　第１の実施形態の通信装置としての携帯電話端末の構成例を示す図である。

【図３】　第１の実施形態の携帯電話端末に対する情報収集サーバ装置の構成例を示す図である。

【図４】　第１の実施形態の通信装置からの位置・時刻情報の送信動作を説明するためのフローチャートを示す図である。

【図５】　第１の実施形態の通信装置からの位置・時刻情報を受信するサーバ装置の位置・時刻情報の受信動作を説明するためのフローチャートを示す図である。

【図６】　第２の実施形態の通信装置としての携帯電話端末の構成例を示す図である。

【図７】　第２の実施形態の携帯電話端末に対する情報収集サーバ装置の構成例を示す図である。

【図８】　第２の実施形態の通信装置からの位置・時刻情報の送信動作を説明するためのフローチャートを示す図である。

【図９】　第２の実施形態の通信装置からの位置・時刻情報を受信するサーバ装置の位置・時刻情報の受信動作を説明するためのフローチャートを示す図である。

【図１０】　第２の実施形態の通信装置からの位置・時刻情報の送信動作を説明するためのフローチャートを示す図である。

【図１１】　第２の実施形態の通信装置からの位置・時刻情報を受信する相手の通信装置の位置・時刻情報の受信動作を説明するためのフローチャートを示す図である。

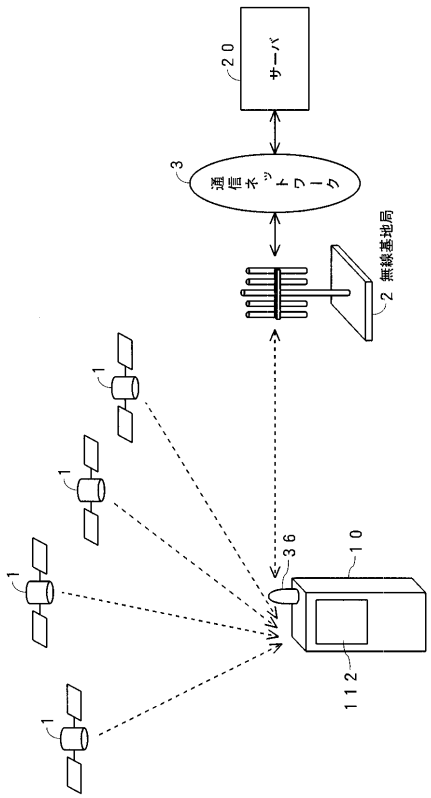
【図１２】　第３の実施形態の通信装置からの位置・時刻情報の送信動作を説明するためのフローチャートを示す図である。

【図１３】　第３の実施形態の通信装置からの位置・時刻情報を受信するサーバ装置の位置・時刻情報の受信動作を説明するためのフローチャートを示す図である。

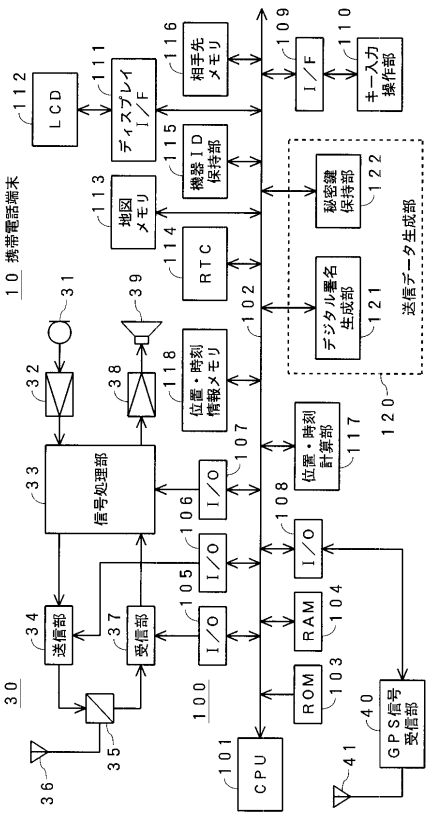
【図１４】　第４の実施形態の通信装置としての携帯電話端末の構成例を示す図である。

【図１５】　第４の実施形態の携帯電話端末に装填するＩＣカードの構成例を示す図である。
【図１６】　ＩＣカードの発行手順を説明するための図である。
【図１７】　第４の実施形態の通信装置からの位置・時刻情報の送信動作を説明するためのフローチャートを示す図である。
【図１８】　第４の実施形態の携帯電話端末に装填するＩＣカードの信号処理動作を説明するためのフローチャートである。
【図１９】　第４の実施形態の携帯電話端末に装填するＩＣカードの信号処理動作を説明するためのフローチャートである。
【図２０】　第４の実施形態の携帯電話端末に装填するＩＣカードの信号処理動作を説明するためのフローチャートである。
【符号の説明】
　１０…携帯電話端末、２０…情報収集サーバ装置、４０…ＧＰＳ信号受信部、１１７…位置・時刻計算部、１１８…位置・時刻情報メモリ、１２０…送信データ生成部、１２１…デジタル署名生成部、１２２…秘密鍵保持部、１２３…暗号／復号部、１２４…公開鍵保持部

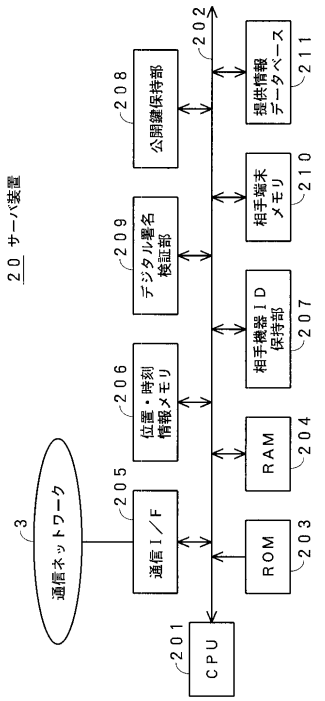
【図１】



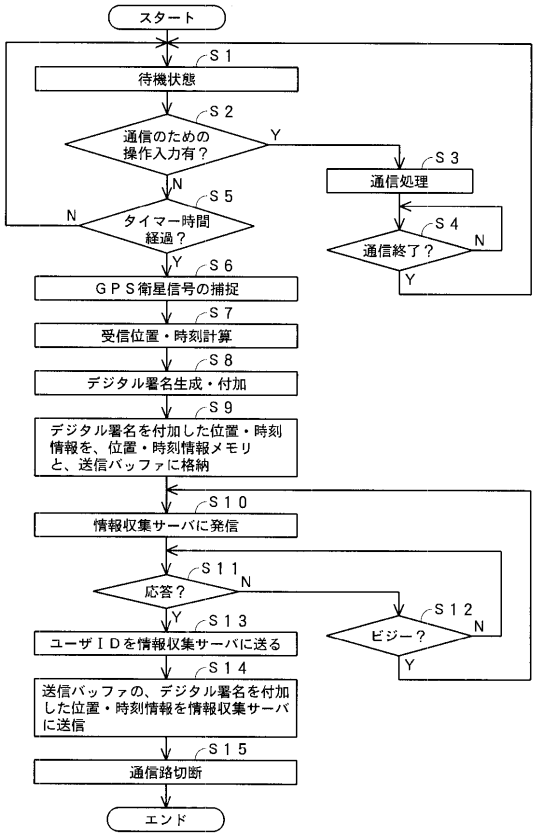
【図２】



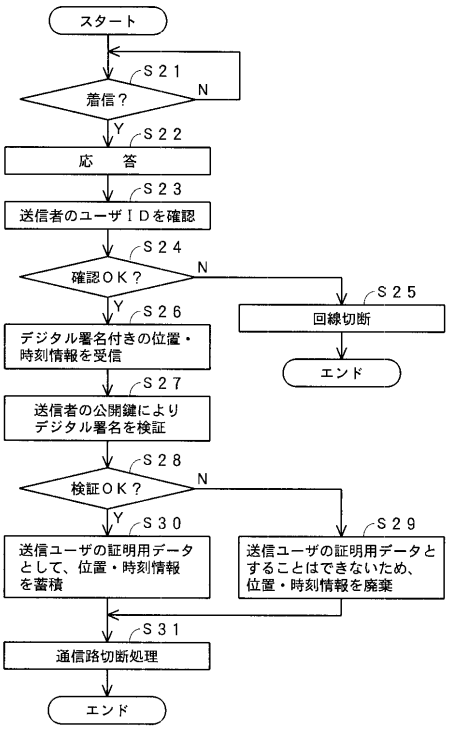
【図３】


20 サーバ装置
3 通信ネットワーク
CPU 201
ROM 203
RAM 204
通信Ｉ／Ｆ 205
位置・時刻情報メモリ 206
デジタル署名検証部 209
公開鍵保持部 208
202
提供情報データベース 211
相手端末メモリ 210
相手機器ＩＤ保持部 207

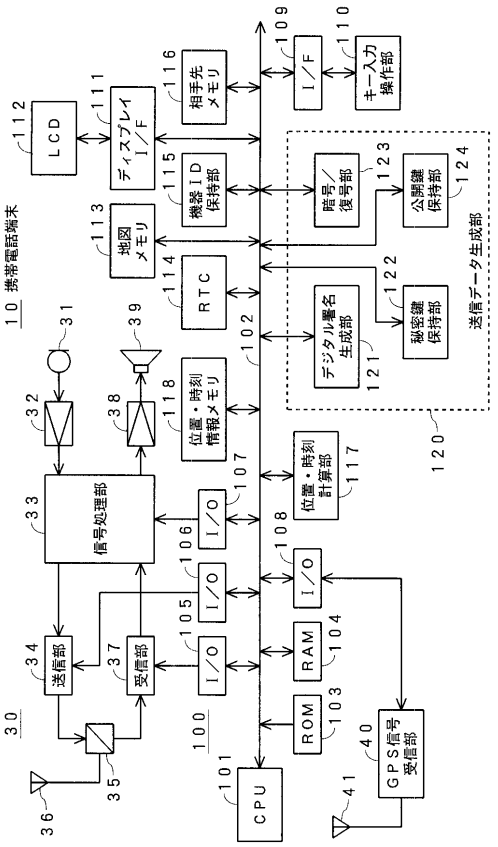
【図４】


スタート
S1 待機状態
S2 通信のための操作入力有？ Y N
S3 通信処理
S4 通信終了？ N Y
S5 タイマー時間経過？ N Y
S6 ＧＰＳ衛星信号の捕捉
S7 受信位置・時刻計算
S8 デジタル署名生成・付加
S9 デジタル署名を付加した位置・時刻情報を、位置・時刻情報メモリと、送信バッファに格納
S10 情報収集サーバに発信
S11 応答？ N Y
S12 ビジー？ N Y
S13 ユーザＩＤを情報収集サーバに送る
S14 送信バッファの、デジタル署名を付加した位置・時刻情報を情報収集サーバに送信
S15 通信路切断
エンド

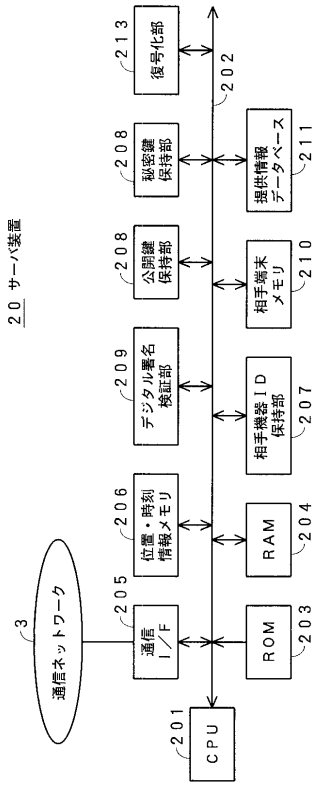
【図５】


スタート
S21 着信？ N Y
S22 応　答
S23 送信者のユーザＩＤを確認
S24 確認ＯＫ？ N Y
S25 回線切断
エンド
S26 デジタル署名付きの位置・時刻情報を受信
S27 送信者の公開鍵によりデジタル署名を検証
S28 検証ＯＫ？ N Y
S29 送信ユーザの証明用データとすることはできないため、位置・時刻情報を廃棄
S30 送信ユーザの証明用データとして、位置・時刻情報を蓄積
S31 通信路切断処理
エンド

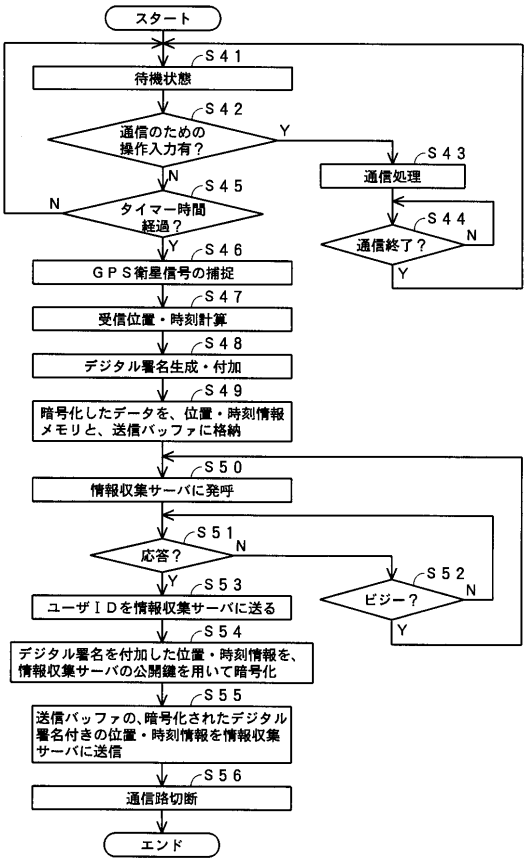
【図６】


10 携帯電話端末
CPU 101
ROM 103
RAM 104
I／O 105
I／O 106
I／O 107
I／O 108
I／Ｆ 109
キー入力操作部 110
ディスプレイＩ／Ｆ 111
LCD 112
地図メモリ 113
RTC 114
機器ＩＤ保持部 115
相手先メモリ 116
位置・時刻計算部 117
位置・時刻情報メモリ 118
信号処理部 33
送信部 34
受信部 37
GPS信号受信部 40
暗号／復号部 123
公開鍵保持部 124
デジタル署名生成部 121
秘密鍵保持部 122
送信データ生成部 120

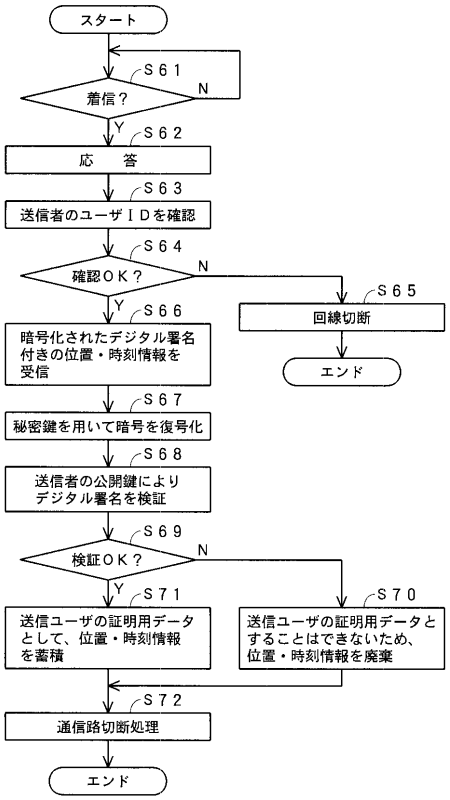
【図７】


20 サーバ装置
復号化部
213
202
秘密鍵保持部
208
提供情報データベース
211
公開鍵保持部
208
相手端末メモリ
210
デジタル署名検証部
209
相手機器ＩＤ保持部
207
位置・時刻情報メモリ
206
RAM
204
通信ＩＦ
205
ROM
203
3
通信ネットワーク
CPU
201

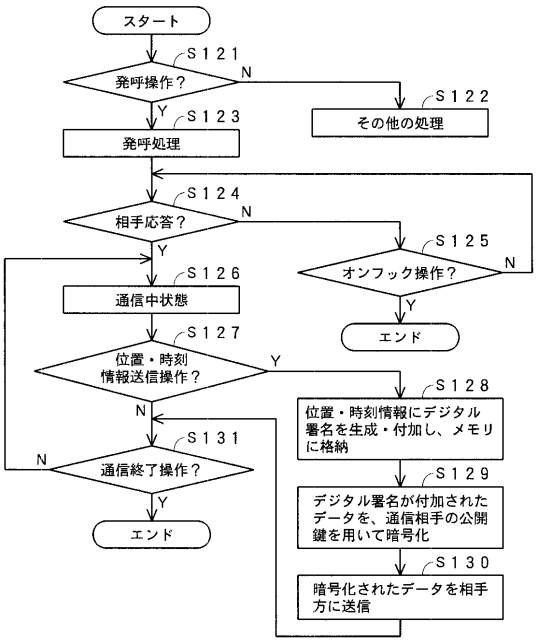
【図８】


スタート
S41
待機状態
S42
通信のための操作入力有？
Y
N
S43
通信処理
S45
タイマー時間経過？
N
S44
通信終了？
N
Y
Y
S46
ＧＰＳ衛星信号の捕捉
S47
受信位置・時刻計算
S48
デジタル署名生成・付加
S49
暗号化したデータを、位置・時刻情報メモリと、送信バッファに格納
S50
情報収集サーバに発呼
S51
応答？
N
S52
ビジー？
N
Y
Y
S53
ユーザＩＤを情報収集サーバに送る
S54
デジタル署名を付加した位置・時刻情報を、情報収集サーバの公開鍵を用いて暗号化
S55
送信バッファの、暗号化されたデジタル署名付きの位置・時刻情報を情報収集サーバに送信
S56
通信路切断
エンド

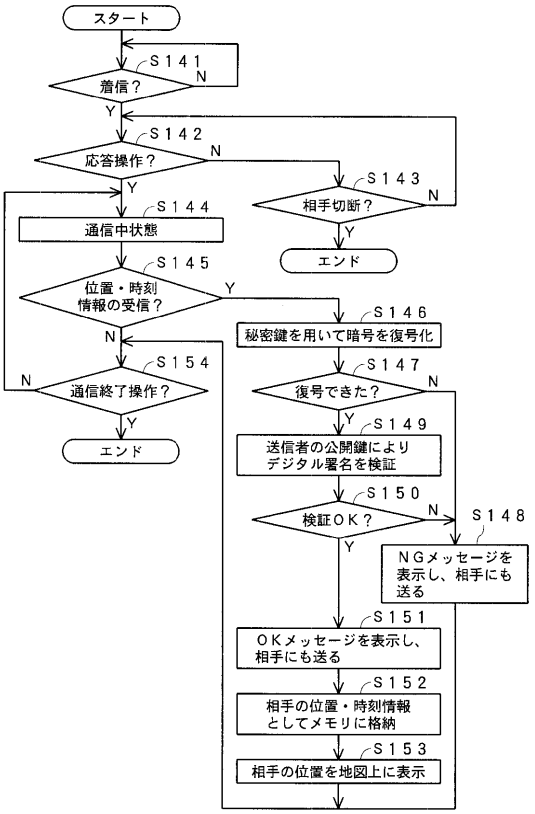
【図９】


スタート
S61
着信？
N
Y
S62
応　答
S63
送信者のユーザＩＤを確認
S64
確認ＯＫ？
N
Y
S65
回線切断
エンド
S66
暗号化されたデジタル署名付きの位置・時刻情報を受信
S67
秘密鍵を用いて暗号を復号化
S68
送信者の公開鍵によりデジタル署名を検証
S69
検証ＯＫ？
N
Y
S70
送信ユーザの証明用データとすることはできないため、位置・時刻情報を廃棄
S71
送信ユーザの証明用データとして、位置・時刻情報を蓄積
S72
通信路切断処理
エンド

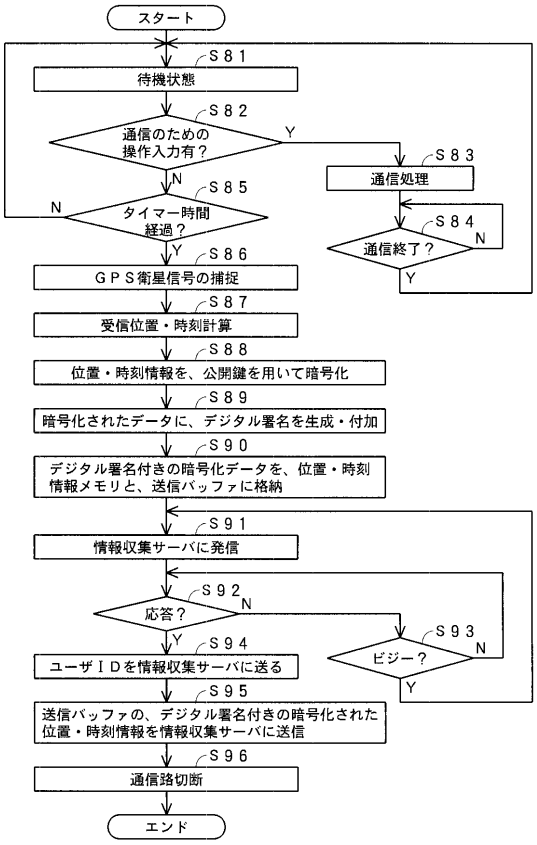
【図１０】


スタート
S121
発呼操作？
N
Y
S122
その他の処理
S123
発呼処理
S124
相手応答？
N
Y
S125
オンフック操作？
N
Y
エンド
S126
通信中状態
S127
位置・時刻情報送信操作？
Y
N
S128
位置・時刻情報にデジタル署名を生成・付加し、メモリに格納
S129
デジタル署名が付加されたデータを、通信相手の公開鍵を用いて暗号化
S130
暗号化されたデータを相手方に送信
S131
通信終了操作？
N
Y
エンド

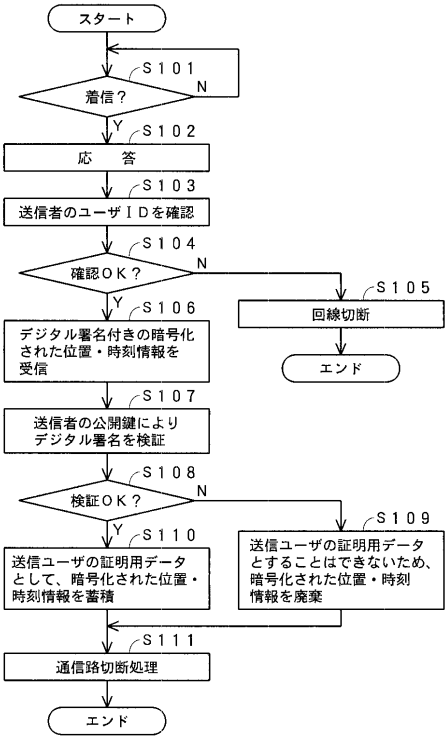
【図１１】



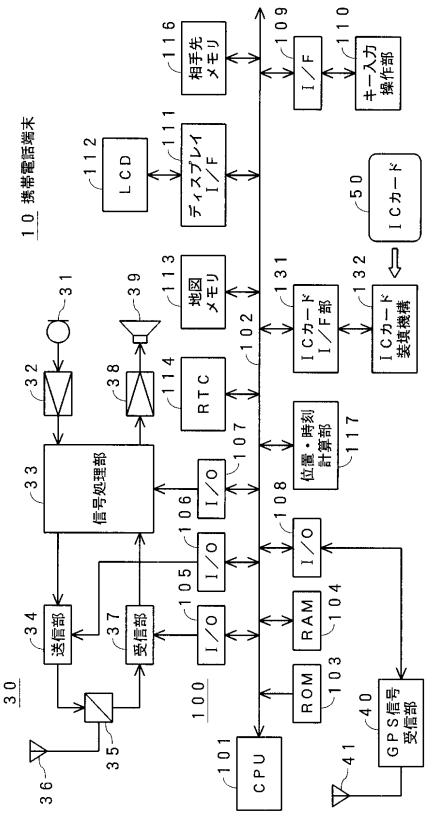
【図１２】



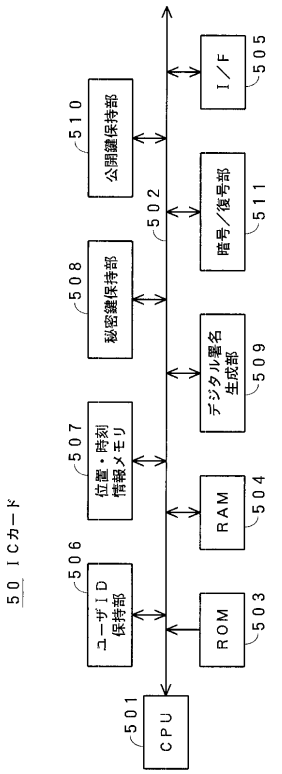
【図１３】



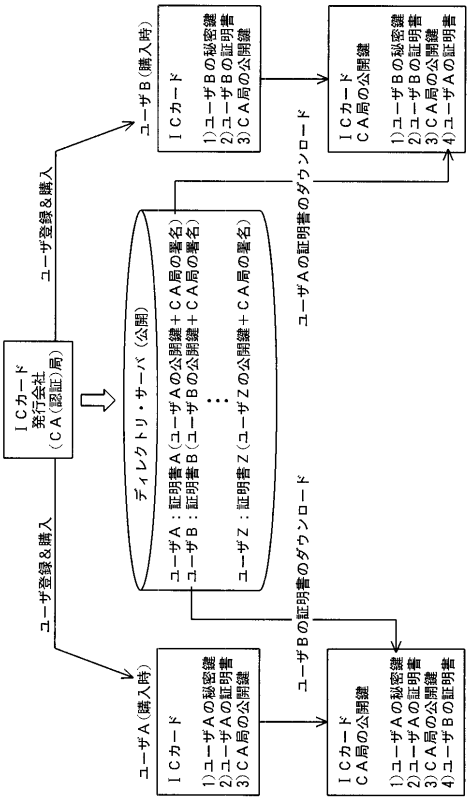
【図１４】



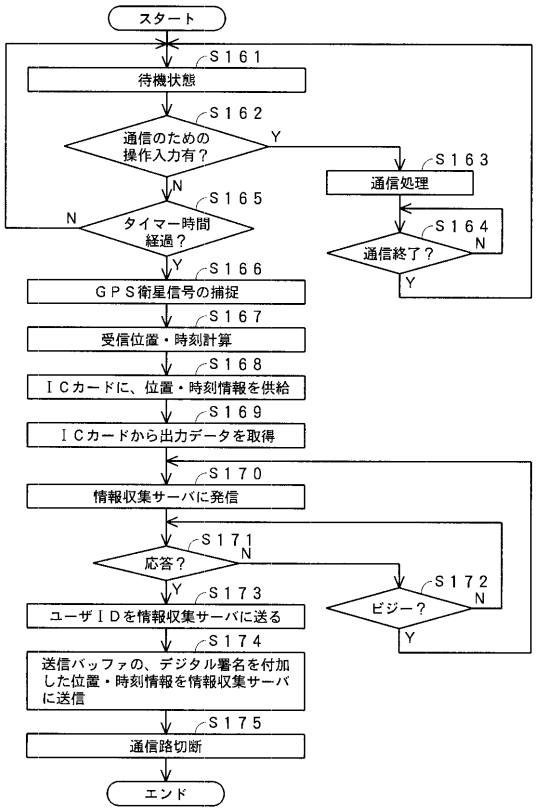
【図１５】



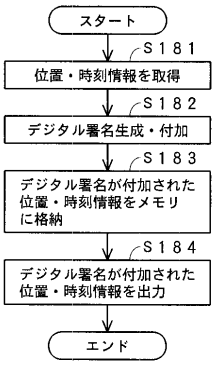
【図１６】



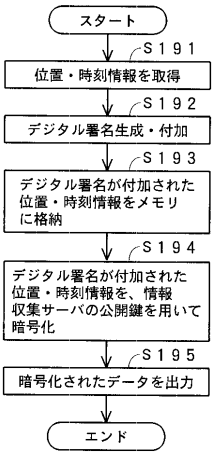
【図１７】



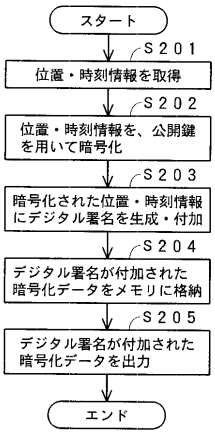
【図１８】



【図１９】


スタート
S191
位置・時刻情報を取得
S192
デジタル署名生成・付加
S193
デジタル署名が付加された位置・時刻情報をメモリに格納
S194
デジタル署名が付加された位置・時刻情報を、情報収集サーバの公開鍵を用いて暗号化
S195
暗号化されたデータを出力
エンド

【図２０】


スタート
S201
位置・時刻情報を取得
S202
位置・時刻情報を、公開鍵を用いて暗号化
S203
暗号化された位置・時刻情報にデジタル署名を生成・付加
S204
デジタル署名が付加された暗号化データをメモリに格納
S205
デジタル署名が付加された暗号化データを出力
エンド

フロントページの続き

(56)参考文献 特開２００２－２０７８９５（ＪＰ，Ａ）
特開２０００－１６３３７９（ＪＰ，Ａ）
特開２００２－１０１４６７（ＪＰ，Ａ）
特開２０００－１２３０２７（ＪＰ，Ａ）
特開２００１－１０３００３（ＪＰ，Ａ）
特開平１１－２５１６５（ＪＰ，Ａ）
山本和彦，転ばぬ先のセキュリティ（１６） ＰＧＰ（２），ＵＮＩＸ ＭＡＧＡＺＩＮＥ，株式会社アスキー，１９９５年 ８月 １日，第１０巻，第８号，第７６－８６頁
Matthias Kabatnik and Alf Zugenmaier , Location Stamps for Digital Signatures: A New Service for Mobile Telephone Networks, ICN2001, LNCS 2094 , ２００１年，pp. 20-30
西村裕，盗み見、のぞき見からプライバシーを守るだれでも使える暗号化メール，日経パソコン，日経ＢＰ社，１９９９年 ９月 ６日，第３４４号，第１５０－１５９頁
J.H. An, Authenticated Encryption in the Public-Key Setting: Security Notions and Analyses, Cryptology ePrint Archive: Report 2001/079, ２００１年，ＵＲＬ，http://eprint.iacr.org/2001/079

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32