(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5575248号
(P5575248)
(45)発行日　平成26年8月20日(2014.8.20)　(24)登録日　平成26年7月11日(2014.7.11)

(51)Int.Cl.　F I
*H04L 9/18 (2006.01)*　H04L 9/00 651

請求項の数 11 (全 19 頁)

(21)出願番号　特願2012-530455(P2012-530455)
(86)(22)出願日　平成22年8月24日(2010.8.24)
(86)国際出願番号　PCT/JP2010/064237
(87)国際公開番号　WO2012/025987
(87)国際公開日　平成24年3月1日(2012.3.1)
審査請求日　平成24年11月27日(2012.11.27)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100151220
弁理士　八巻　満隆
(72)発明者　辻　宏郷
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　柴田　陽一
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】通信端末、通信システム、通信方法及び通信プログラム

(57)【特許請求の範囲】
【請求項１】
ワンタイムパッド暗号用の暗号鍵を、その暗号鍵を所定のビット数毎に複数に分割した暗号鍵ブロックとして記憶する暗号鍵ブロック記憶部と、
前記暗号鍵ブロック記憶部が記憶した複数の暗号鍵ブロックを特定する第１識別情報を、通信の相手先端末へ送信する識別情報送信部と、
前記識別情報送信部が送信した第１識別情報から特定される複数の暗号鍵ブロックのうち、前記相手先端末が保有する暗号鍵ブロックに含まれる暗号鍵ブロックだけを特定する第２識別情報を、前記相手先端末から受信する識別情報受信部と、
前記識別情報受信部が受信した第２識別情報から特定される暗号鍵ブロックを前記暗号鍵ブロック記憶部から揮発性の記憶装置にコピーし、前記コピーの完了と同時に、前記暗号鍵ブロック記憶部に記憶されたコピー元の暗号鍵ブロックを消去し、揮発性の記憶装置にコピーした暗号鍵ブロックを用いて、ワンタイムパッド暗号により前記相手先端末と暗号化通信する暗号化通信部とを備えることを特徴とする通信端末。
【請求項２】
前記暗号化通信部は、前記第２識別情報から複数の暗号鍵ブロックが特定される場合には、予め前記相手先端末と共有した方法によりいずれか１つの暗号鍵ブロックを選択し、選択した暗号鍵ブロックを用いて暗号化通信する
ことを特徴とする請求項１に記載の通信端末。
【請求項３】

前記暗号化通信部は、暗号鍵ブロックのビットを所定の順に用いて暗号化通信し、その暗号鍵ブロックの全てのビットを使用し終わると、前記第２識別情報から特定される他の暗号鍵ブロックを用いて暗号化通信し、
前記通信端末は、さらに、
前記暗号化通信部が全てのビットを使用し終わった暗号鍵ブロックを消去する暗号鍵ブロック消去部
を備えることを特徴とする請求項２に記載の通信端末。
【請求項４】
前記暗号鍵ブロック消去部は、前記暗号化通信部が暗号化通信に用いた暗号鍵ブロックに使用していないビットが残っている場合であっても、前記相手先端末との通信が終了した場合に、前記暗号化通信部が暗号化通信に用いた暗号鍵ブロックを消去する
ことを特徴とする請求項３に記載の通信端末。
【請求項５】
前記暗号鍵ブロック記憶部は、不揮発性の記憶装置である
ことを特徴とする請求項１に記載の通信端末。
【請求項６】
前記通信端末は、さらに、
前記暗号鍵ブロックの残り個数を利用者へ通知する残量通知部
を備えることを特徴とする請求項１から５までのいずれかに記載の通信端末。
【請求項７】
前記暗号化通信部は、暗号鍵ブロックのビットを所定の順に用いて暗号化通信し、その暗号鍵ブロックの全てのビットを使用し終わると、前記第２識別情報から特定される他の暗号鍵ブロックを用いて暗号化通信し、
前記残量通知部は、前記暗号化通信部が暗号化通信に用いる暗号鍵ブロックを変更したことを利用者へ通知する
ことを特徴とする請求項６に記載の通信端末。
【請求項８】
第１通信端末と第２通信端末とを備える通信システムであり、
前記第１通信端末は、
ワンタイムパッド暗号用の暗号鍵を、その暗号鍵を所定のビット数毎に複数に分割した暗号鍵ブロックとして記憶する第１暗号鍵ブロック記憶部と、
前記第１暗号鍵ブロック記憶部が記憶した複数の暗号鍵ブロックを特定する第１識別情報を、前記第２通信端末へ送信する第１識別情報送信部と
を備え、
前記第２通信端末は、
ワンタイムパッド暗号用の暗号鍵を、その暗号鍵を前記所定のビット数毎に複数に分割した暗号鍵ブロックとして記憶する第２暗号鍵ブロック記憶部と、
前記第１識別情報送信部が送信した識別情報から特定される複数の暗号鍵ブロックのうち、前記第２暗号鍵ブロック記憶部が記憶した複数の暗号鍵ブロックに含まれる暗号鍵ブロックだけを特定する第２識別情報を、前記第１通信端末へ送信する第２識別情報送信部と
を備え、
前記第１通信端末は、さらに、
前記第２識別情報送信部が送信した第２識別情報から特定される暗号鍵ブロックを前記第１暗号鍵ブロック記憶部から揮発性の記憶装置にコピーし、前記コピーの完了と同時に、前記第１暗号鍵ブロック記憶部に記憶されたコピー元の暗号鍵ブロックを消去し、揮発性の記憶装置にコピーした暗号鍵ブロックを用いて、ワンタイムパッド暗号により前記第２通信端末と暗号化通信する第１暗号化通信部
を備え、
前記第２通信端末は、さらに、

前記第２識別情報送信部が送信した第２識別情報から特定される暗号鍵ブロックを前記第２暗号鍵ブロック記憶部から揮発性の記憶装置にコピーし、前記コピーの完了と同時に、前記第２暗号鍵ブロック記憶部に記憶されたコピー元の暗号鍵ブロックを消去し、揮発性の記憶装置にコピーした暗号鍵ブロックを用いて、ワンタイムパッド暗号により前記第１通信端末と暗号化通信する第２暗号化通信部
を備えることを特徴とする通信システム。
【請求項９】
通信端末と、ワンタイムパッド暗号用の暗号鍵を前記通信端末へ配布する暗号鍵配布装置とを備える通信システムであり、
前記暗号鍵配布装置は、
ワンタイムパッド暗号用の暗号鍵を、所定のビット数毎に分割して複数の暗号鍵ブロックを生成する暗号鍵ブロック生成部と、
前記暗号鍵ブロック生成部が生成した複数の暗号鍵ブロックを通信端末へ送信する暗号鍵ブロック送信部と
を備え、
前記通信端末は、
前記暗号鍵ブロック送信部が送信した暗号鍵ブロックを記憶する暗号鍵ブロック記憶部と、
前記暗号鍵ブロック記憶部が記憶した複数の暗号鍵ブロックを特定する第１識別情報を、通信の相手先端末へ送信する識別情報送信部と、
前記識別情報送信部が送信した識別情報から特定される複数の暗号鍵ブロックのうち、前記相手先端末が保有する暗号鍵ブロックに含まれる暗号鍵ブロックだけを特定する第２識別情報を、前記相手先端末から受信する識別情報受信部と、
前記識別情報受信部が受信した第２識別情報から特定される暗号鍵ブロックを前記暗号鍵ブロック記憶部から揮発性の記憶装置にコピーし、前記コピーの完了と同時に、前記暗号鍵ブロック記憶部に記憶されたコピー元の暗号鍵ブロックを消去し、揮発性の記憶装置にコピーした暗号鍵ブロックを用いて、通信データをワンタイムパッド暗号により前記相手先端末と暗号化通信する暗号化通信部と
を備えることを特徴とする通信システム。
【請求項１０】
ワンタイムパッド暗号用の暗号鍵を、その暗号鍵を所定のビット数毎に複数に分割した暗号鍵ブロックとして記憶した不揮発性の記憶装置を備える通信端末の通信方法であり、
前記不揮発性の記憶装置に記憶された複数の暗号鍵ブロックを特定する第１識別情報を、通信の相手先端末へ送信する識別情報送信工程と、
前記識別情報送信工程で送信した第１識別情報から特定される複数の暗号鍵ブロックのうち、前記相手先端末が保有する暗号鍵ブロックに含まれる暗号鍵ブロックだけを特定する第２識別情報を、前記相手先端末から受信する識別情報受信工程と、
前記識別情報受信工程で受信した第２識別情報から特定される暗号鍵ブロックを前記不揮発性の記憶装置から揮発性の記憶装置にコピーし、前記コピーの完了と同時に、前記不揮発性の記憶装置に記憶されたコピー元の暗号鍵ブロックを消去し、揮発性の記憶装置にコピーした暗号鍵ブロックを用いて、ワンタイムパッド暗号により前記相手先端末と暗号化通信する暗号化通信工程とを備えることを特徴とする通信方法。
【請求項１１】
ワンタイムパッド暗号用の暗号鍵を、その暗号鍵を所定のビット数毎に複数に分割した暗号鍵ブロックとして記憶した不揮発性の記憶装置を備える通信端末の通信プログラムであり、
前記不揮発性の記憶装置に記憶された複数の暗号鍵ブロックを特定する第１識別情報を、通信の相手先端末へ送信する識別情報送信処理と、
前記識別情報送信処理で送信した第１識別情報から特定される複数の暗号鍵ブロックのうち、前記相手先端末が保有する暗号鍵ブロックに含まれる暗号鍵ブロックだけを特定す

る第２識別情報を、前記相手先端末から受信する識別情報受信処理と、
前記識別情報受信処理で受信した第２識別情報から特定される暗号鍵ブロックを前記不揮発性の記憶装置から揮発性の記憶装置にコピーし、前記コピーの完了と同時に、前記不揮発性の記憶装置に記憶されたコピー元の暗号鍵ブロックを消去し、揮発性の記憶装置にコピーした暗号鍵ブロックを用いて、ワンタイムパッド暗号により前記相手先端末と暗号化通信する暗号化通信処理とをコンピュータに実行させることを特徴とする通信プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ワンタイムパッド（ＯＴＰ：Ｏｎｅ　Ｔｉｍｅ　Ｐａｄ）暗号を用いた暗号化通信技術に関する。
【背景技術】
【０００２】
複数の通信端末において、暗号アルゴリズムの鍵を共有し、通信端末間の通信内容の暗号化を行うことによって、通信内容の盗聴防止を実現することができる。
この時、暗号アルゴリズムとしてブロック暗号アルゴリズムを用いる場合は、平文データをブロックと呼ばれる単位（通常は固定長）に分割し、ブロック毎に暗号鍵を用いた暗号化処理を繰り返し行う。
また、暗号アルゴリズムとしてストリーム暗号アルゴリズムを用いる場合は、暗号鍵から鍵ストリームと呼ばれる疑似乱数を生成し、鍵ストリームを用いてビット単位で平文データの暗号化処理を繰り返し行う。
いずれの場合も、通信端末間で共有する暗号鍵の長さは１２８ビットや２５６ビット等である。即ち、平文データよりも短い長さの暗号鍵に基づいて通信内容を暗号化する方式である。これらの方式では、暗号鍵として取り得る値の範囲が２の１２８乗～２の２５６乗通りの組合せであり、現在の計算機技術を用いた場合、暗号鍵の全ての組合せで復号を試みる総当たり攻撃は不可能であると考えられている。
【０００３】
一方、平文データと同じ長さの乱数を用意しておき、その乱数を鍵として１回限りの暗号化に使用するワンタイムパッドと呼ばれる暗号方式が存在する。
ワンタイムパッド暗号方式では、暗号鍵として取り得る値の範囲は平文データと等しい巨大な空間となるため、計算機技術が飛躍的に進化したと仮定しても解読が不可能であることが証明可能である。ヴァーナム暗号（Ｖａｒｎａｍ’ｓ　Ｃｉｐｈｅｒ）はワンタイムパッド暗号方式の一種であり、平文データと暗号鍵の排他的論理和（ＸＯＲ）を暗号文とする。
【０００４】
ワンタイムパッド暗号方式を用いて通信内容を暗号化するためには、通信端末間で平文データの長さ以上のワンタイムパッド暗号鍵を事前共有する必要がある。量子暗号鍵配布（ＱＫＤ：Ｑｕａｎｔｕｍ　Ｋｅｙ　Ｄｉｓｔｒｉｂｕｔｉｏｎ）技術は、ワンタイムパッド暗号鍵を共有するための有力な技術と考えられている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００１－７８００号公報
【特許文献２】特開２００１－８６１１０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ワンタイムパッド暗号方式を用いた通信システムでは、ワンタイムパッド暗号を用いて暗号化通信する通信端末の間で、事前共有しておいた長いワンタイムパッド暗号鍵のどの

部分を暗号化に使用するか調整しなければならない。
これまでは、ワンタイムパッド暗号方式を用いた通信システムにおける通信端末は、量子暗号鍵配布技術等を使った鍵共有システムに常時接続された固定端末であることが前提であった。そのため、ワンタイムパッド暗号鍵が通信端末間で完全に一致していることが前提であり、単に先頭のビットから順に暗号化に使用すればよいと考えられてきた。
しかし、例えば、通信端末をモバイル通信端末とした場合、鍵共有システムには不定期に接続されることになり、ワンタイムパッド暗号鍵がモバイル通信端末間で完全に一致していない可能性がある。また、ワンタイムパッド暗号鍵をモバイル通信端末へ転送中に、モバイル通信端末の接続が解除され、一部のワンタイムパッド暗号鍵の転送に失敗する場合も考えられる。このようなことも原因となって、ワンタイムパッド暗号鍵がモバイル通信端末間で完全に一致していない可能性がある。
この発明は、ワンタイムパッド暗号鍵が通信端末間で完全に一致していない可能性がある場合に、ワンタイムパッド暗号鍵のどの部分を使用するかを調整して暗号化通信を実現することを目的とする。
【課題を解決するための手段】
【０００７】
この発明に係る通信端末は、
ワンタイムパッド暗号用の暗号鍵を、その暗号鍵を所定のビット数毎に複数に分割した暗号鍵ブロックとして記憶する暗号鍵ブロック記憶部と、
前記暗号鍵ブロック記憶部が記憶した複数の暗号鍵ブロックを特定する第１識別情報を、通信の相手先端末へ送信する識別情報送信部と、
前記識別情報送信部が送信した第１識別情報から特定される複数の暗号鍵ブロックのうち、前記相手先端末が保有する暗号鍵ブロックに含まれる暗号鍵ブロックだけを特定する第２識別情報を、前記相手先端末から受信する識別情報受信部と、
前記識別情報受信部が受信した第２識別情報から特定される暗号鍵ブロックを用いて、ワンタイムパッド暗号により前記相手先端末と暗号化通信する暗号化通信部と
を備えることを特徴とする。
【発明の効果】
【０００８】
この発明に係る通信端末では、ワンタイムパッド暗号用の暗号鍵を、所定のビット数毎に分割した暗号鍵ブロックとして記憶し、暗号化通信前に通信相手と共有している暗号鍵ブロックを確認した上で、暗号化通信に用いる暗号鍵ブロックを決定する。これにより、ワンタイムパッド暗号鍵のどの部分を使用するか調整することができる。
【図面の簡単な説明】
【０００９】
【図１】実施の形態１における通信システム１の構成図。
【図２】実施の形態１における暗号鍵転送装置１０２の機能を示すブロック図。
【図３】実施の形態１におけるワンタイムパッド暗号鍵カートリッジ１１２のフォーマット及び暗号鍵転送装置１０２におけるカートリッジ化・暗号化処理を示す図。
【図４】実施の形態１におけるモバイル通信端末１０３の機能を示すブロック図。
【図５】実施の形態１におけるワンタイムパッド暗号鍵カートリッジ１１２のフォーマット及びモバイル通信端末１０３における開封処理を示す図。
【図６】モバイル通信端末１０３の暗号化通信開始時のシーケンスを示す図。
【図７】モバイル通信端末１０３の暗号化通信中のシーケンスを示す図。
【図８】モバイル通信端末１０３の暗号化通信終了時のシーケンスを示す図。
【図９】ワンタイムパッド暗号鍵カートリッジ１１２の廃棄の説明図。
【図１０】モバイル通信端末１０３におけるワンタイムパッド暗号鍵カートリッジ１１２の取り扱いを示すフローチャート。
【図１１】モバイル通信端末１０３における画面表示を示す図。
【図１２】モバイル通信端末１０３のハードウェア構成の一例を示す図。

【発明を実施するための形態】
【００１０】
以下、図に基づき、発明の実施の形態を説明する。
以下の説明において、処理装置は後述するＣＰＵ９１１等である。不揮発性メモリは後述する磁気ディスク９２０等である。また、揮発性メモリは後述するＲＡＭ９１４等である。
【００１１】
実施の形態１．
図１は、実施の形態１における通信システム１の構成図である。
通信システム１は、鍵共有システム１０１、複数の暗号鍵転送装置１０２、複数のモバイル通信端末１０３、ネットワーク１０４を備える。
【００１２】
鍵共有システム１０１は、拠点間でワンタイムパッド暗号鍵１１１を共有する手段を提供するシステムである。ここでは、鍵共有システム１０１は、量子暗号鍵配布技術を用いたシステムであるとするが、他の方式によるシステムであってもよい。
鍵共有システム１０１は拠点毎に鍵共有装置１０５を備え、鍵共有装置１０５間は光ファイバリンク１０６で接続される。そして、鍵共有装置１０５間では、例えば、毎秒２０，０００ビットのワンタイムパッド暗号鍵１１１が光ファイバリンク１０６を介して共有される。
【００１３】
暗号鍵転送装置１０２は、鍵共有システム１０１で共有されたワンタイムパッド暗号鍵１１１をモバイル通信端末１０３へ転送する装置である。
暗号鍵転送装置１０２は、拠点毎に設置され、その拠点に設置された鍵共有装置１０５と接続される。暗号鍵転送装置１０２は、接続された鍵共有装置１０５からワンタイムパッド暗号鍵１１１を取得する。そして、暗号鍵転送装置１０２は、取得したワンタイムパッド暗号鍵１１１を分割し、デバイス鍵１１３を用いて暗号化してワンタイムパッド暗号鍵カートリッジ１１２の形式に変換した上で、モバイル通信端末１０３に転送する。
【００１４】
モバイル通信端末１０３は、暗号鍵転送装置１０２から転送されたワンタイムパッド暗号鍵カートリッジ１１２を用い、ネットワーク１０４を介して他のモバイル通信端末１０３と暗号化通信する端末である。
例えば、モバイル通信端末１０３は、ワンタイムパッド暗号鍵カートリッジ１１２を用いて、他のモバイル通信端末１０３と通話データ（音声データ）を暗号化して通信する。
【００１５】
ネットワーク１０４は、モバイル通信端末１０３間の通信路として用いられるネットワークである。
【００１６】
ワンタイムパッド暗号鍵１１１は、鍵共有システム１０１によって拠点間で共有されるワンタイムパッド用の暗号鍵であり、例えば真性乱数である。ワンタイムパッド暗号鍵１１１は、上述したように鍵共有装置１０５間で、毎秒２０，０００ビット共有されるため、非常に大きなビット列のデータとなる。
【００１７】
ワンタイムパッド暗号鍵カートリッジ１１２は、一定量の通信データの暗号化通信に必要となる量毎にワンタイムパッド暗号鍵１１１を分割し、デバイス鍵１１３を用いて暗号化することによって作成されたワンタイムパッド用の暗号鍵である。
例えば、ワンタイムパッド暗号鍵カートリッジ１１２は、通話データを暗号化して通信する場合、所定の時間（例えば、１０分）分の通話データを暗号化できるだけのワンタイムパッド暗号用の暗号鍵である。この場合、通話データのビットレートが８０００ｂｐｓ（ｂｉｔ　ｐｅｒ　ｓｅｃｏｎｄ）であるとき、ワンタイムパッド暗号鍵カートリッジ１１２は、８０００ｂｐｓ×６００秒（１０分）×２＝９，６００，０００ビットである。

なお、上記式で最後に２倍しているのは、通話は双方向通信であるためである。

【００１８】

デバイス鍵１１３は、暗号鍵転送装置１０２とモバイル通信端末１０３との間の事前共有鍵である。デバイス鍵１１３は、ワンタイムパッド暗号鍵カートリッジ１１２の暗号化処理に用いられる。

【００１９】

次に、実施の形態１における暗号鍵転送装置１０２の機能について説明する。

図２は、実施の形態１における暗号鍵転送装置１０２の機能を示すブロック図である。

暗号鍵転送装置１０２は、主記憶装置２０１、補助記憶装置２０２、デバイス鍵管理部２０３、暗号鍵取得部２０４、暗号鍵カートリッジ生成部２０５（暗号鍵ブロック生成部）、ブロック暗号化部２０６、暗号鍵カートリッジ転送部２０７、インタフェース部２０８、有線通信部２０９を備える。

【００２０】

主記憶装置２０１は、暗号鍵転送装置１０２の電源投入中のみデータを保持可能な揮発性メモリである。補助記憶装置２０２は、暗号鍵転送装置１０２の電源投入中であるか否かにかかわらずデータを保持可能な不揮発性メモリである。デバイス鍵管理部２０３は、モバイル通信端末１０３との間の事前共有鍵であるデバイス鍵１１３を耐タンパ装置等により管理する。

インタフェース部２０８は、鍵共有システム１０１と接続するためのインタフェースである。例えば、暗号鍵転送装置１０２は、インタフェース部２０８を介して、常時鍵共有システム１０１と接続されている。有線通信部２０９は、モバイル通信端末１０３と接続するためのインタフェースである。例えば、暗号鍵転送装置１０２は、有線通信部２０９を介して、不定期にモバイル通信端末１０３と接続される。

他の機能については、暗号鍵転送装置１０２の動作の説明において、詳しく説明する。

【００２１】

次に、暗号鍵転送装置１０２の動作について説明する。

まず、ワンタイムパッド暗号鍵１１１の取得時の動作について説明する。

暗号鍵取得部２０４は、鍵共有システム１０１の鍵共有装置１０５間で共有されたワンタイムパッド暗号鍵１１１を、インタフェース部２０８を介して接続された鍵共有装置１０５から所定の時間毎に取得する。取得したワンタイムパッド暗号鍵１１１は、主記憶装置２０１に一旦格納される。

次に、暗号鍵カートリッジ生成部２０５は、処理装置により、ワンタイムパッド暗号鍵１１１を一定量の通信データの暗号化通信に必要となる量毎に分割する。そして、暗号鍵カートリッジ生成部２０５は、デバイス鍵管理部２０３によって管理されるデバイス鍵１１３を用いて、分割したワンタイムパッド暗号鍵１１１それぞれをブロック暗号化部２０６に暗号化させる。これにより、暗号鍵カートリッジ生成部２０５は、複数のワンタイムパッド暗号鍵カートリッジ１１２を生成する。生成されたワンタイムパッド暗号鍵カートリッジ１１２は、補助記憶装置２０２に格納される。暗号鍵カートリッジ生成部２０５は、ワンタイムパッド暗号鍵カートリッジ１１２を生成した後、主記憶装置２０１からワンタイムパッド暗号鍵１１１を消去する。

【００２２】

次に、ワンタイムパッド暗号鍵１１１からワンタイムパッド暗号鍵カートリッジ１１２への変換処理の詳細について説明する。

図３は、実施の形態１におけるワンタイムパッド暗号鍵カートリッジ１１２のフォーマット及び暗号鍵転送装置１０２におけるカートリッジ化・暗号化処理を示す図である。

【００２３】

ワンタイムパッド暗号鍵ブロック３０１は、一定量の通信データの暗号化通信に必要となる量毎にワンタイムパッド暗号鍵１１１が分割されたブロックである。デバイス鍵ＩＤ３０２は、デバイス鍵１１３を一意に識別するための識別子である。暗号化パラメータ３０３は、ブロック暗号アルゴリズムを用いて暗号化を行う際に指定するアルゴリズムパラ

メータ（例えば、暗号モードの指定やＩＶ（Ｉｎｉｔｉａｌｉｚａｔｉｏｎ Ｖｅｃｔｏｒ）値）である。

暗号化したワンタイムパッド暗号鍵ブロック３１１は、ワンタイムパッド暗号鍵ブロック３０１の１つを平文、デバイス鍵１１３を暗号鍵、暗号化パラメータ３０３をアルゴリズムパラメータとして、ブロック暗号化部２０６によりブロック暗号アルゴリズムで暗号化された暗号文である。ワンタイムパッド暗号鍵カートリッジＩＤ３１２は、ワンタイムパッド暗号鍵カートリッジ１１２を一意に識別するための識別子である。端末ＩＤ（＃１）３１３及び端末ＩＤ（＃２）３１４は、ワンタイムパッド暗号鍵カートリッジ１１２を用いて暗号化通信を行う二台のモバイル通信端末１０３を識別するための識別子である。

【００２４】

暗号鍵カートリッジ生成部２０５は、各ワンタイムパッド暗号鍵ブロック３０１について、デバイス鍵１１３と暗号化パラメータ３０３とを用いて、ブロック暗号化部２０６にブロック暗号アルゴリズムで暗号化させる。これにより、暗号化したワンタイムパッド暗号鍵ブロック３１１が生成される。

そして、暗号鍵カートリッジ生成部２０５は、ワンタイムパッド暗号鍵カートリッジカートリッジＩＤ３１２、端末ＩＤ（＃１）３１３、端末ＩＤ（＃２）３１４、デバイス鍵ＩＤ３０２、暗号化パラメータ３０３と、暗号化したワンタイムパッド暗号鍵ブロック３１１とを組み合わせて、１個のワンタイムパッド暗号鍵カートリッジ１１２とする。

【００２５】

次に、ワンタイムパッド暗号鍵カートリッジ１１２の転送時の動作について説明する。

暗号鍵カートリッジ転送部２０７は、有線通信部２０９を介してモバイル通信端末１０３の接続を検出する。すると、暗号鍵カートリッジ転送部２０７は、補助記憶装置２０２に保管していたワンタイムパッド暗号鍵カートリッジ１１２を有線通信部２０９経由でモバイル通信端末１０３へ転送する。暗号鍵カートリッジ転送部２０７は、正常に転送されたことを確認した後、補助記憶装置２０２からワンタイムパッド暗号鍵カートリッジ１１２を消去する。

【００２６】

なお、鍵共有装置１０５間では常に同一のワンタイムパッド暗号鍵１１１が共有される。また、暗号鍵転送装置１０２は鍵共有装置１０５に常時接続されているため、暗号鍵転送装置１０２間では原則として同一のワンタイムパッド暗号鍵１１１が共有される。

しかし、モバイル通信端末１０３は、不定期に暗号鍵転送装置１０２に接続され、接続されたタイミングで暗号鍵転送装置１０２からワンタイムパッド暗号鍵カートリッジ１１２を取得する。そのため、モバイル通信端末１０３間では、持っているワンタイムパッド暗号鍵カートリッジ１１２が異なる場合がある。

また、例えば、暗号鍵転送装置１０２からモバイル通信端末１０３へのワンタイムパッド暗号鍵カートリッジ１１２の転送中に、暗号鍵転送装置１０２とモバイル通信端末１０３とを繋ぐケーブルを抜いてしまい、暗号鍵転送装置１０２とモバイル通信端末１０３との接続が解除されてしまうことも考えられる。この場合、一部のワンタイムパッド暗号鍵カートリッジ１１２の転送に失敗し、そのワンタイムパッド暗号鍵カートリッジ１１２はモバイル通信端末１０３へ転送されない場合もある。このようなことも原因となって、モバイル通信端末１０３間では、持っているワンタイムパッド暗号鍵カートリッジ１１２が異なる場合がある。

【００２７】

次に、実施の形態１におけるモバイル通信端末１０３の機能について説明する。

図４は、実施の形態１におけるモバイル通信端末１０３の機能を示すブロック図である。

モバイル通信端末１０３は、主記憶装置４０１、補助記憶装置４０２（暗号鍵ブロック記憶部）、デバイス鍵管理部４０３、暗号鍵カートリッジ受信部４０４、ブロック復号部４０５、識別情報送信部４０６、識別情報受信部４０７、暗号化通信部４０８、ワンタイムパッド暗号化・復号部４０９、暗号鍵ブロック消去部４１０、残量通知部４１１、液晶

表示画面４１２、バイブレータ４１３、スピーカー４１４、マイク４１５、無線通信部４１６、有線通信部４１７を備える。

【００２８】

主記憶装置４０１は、モバイル通信端末１０３の電源投入中のみデータを保持可能な揮発性メモリである。補助記憶装置４０２は、モバイル通信端末１０３の電源投入中であるか否かにかかわらずデータを保持可能な不揮発性メモリである。デバイス鍵管理部４０３は、暗号鍵転送装置１０２との間の事前共有鍵であるデバイス鍵１１３を管理する。

液晶表示画面４１２は、テキスト情報やグラフィックス情報を出力する表示装置である。バイブレータ４１３は、振動を発生する装置である。スピーカー４１４は、音声を出力する装置である。マイク４１５は、音声を入力する装置である。

無線通信部４１６は、ネットワーク１０４を介して他のモバイル通信端末１０３と通信するためのインタフェースである。有線通信部４１７は、暗号鍵転送装置１０２と接続するためのインタフェースである。

他の機能については、モバイル通信端末１０３の動作の説明において、詳しく説明する。

【００２９】

次に、モバイル通信端末１０３の動作について説明する。

まず、ワンタイムパッド暗号鍵カートリッジ１１２の補充時の動作について説明する。

暗号鍵カートリッジ受信部４０４は、暗号鍵転送装置１０２が転送したワンタイムパッド暗号鍵カートリッジ１１２を有線通信部４１７を介して受信し、補助記憶装置４０２に格納する。

【００３０】

次に、ワンタイムパッド暗号鍵カートリッジ１１２を用いた暗号化通信時の動作について説明する。

まず、暗号化通信部４０８は、通信内容を暗号化するために、補助記憶装置４０２に格納されたワンタイムパッド暗号鍵カートリッジ１１２からワンタイムパッド暗号鍵ブロック３０１を抽出し、主記憶装置４０１に記憶する。ワンタイムパッド暗号鍵ブロック３０１の抽出が完了した後、暗号鍵ブロック消去部４１０は、補助記憶装置４０２からワンタイムパッド暗号鍵カートリッジ１１２を消去する。

そして、暗号化通信部４０８は、主記憶装置４０１に記憶したワンタイムパッド暗号鍵ブロック３０１の各ビットを先頭から順に用いて、無線通信部４１６を介して他のモバイル通信端末１０３との間で暗号化通信する。暗号化通信終了後、暗号鍵ブロック消去部４１０は、主記憶装置４０１からワンタイムパッド暗号鍵ブロック３０１を消去する。

【００３１】

次に、ワンタイムパッド暗号鍵カートリッジ１１２からワンタイムパッド暗号鍵ブロック３０１への抽出処理（ワンタイムパッド暗号鍵カートリッジ１１２の開封処理）の詳細について説明する。

図５は、実施の形態１におけるワンタイムパッド暗号鍵カートリッジ１１２のフォーマット及びモバイル通信端末１０３における開封処理を示す図である。

なお、図５において、ワンタイムパッド暗号鍵カートリッジ１１２及びその構成要素は図３と同一である。

【００３２】

暗号化通信部４０８は、ワンタイムパッド暗号鍵カートリッジ１１２に含まれる端末ＩＤ（＃１）３１３及び端末ＩＤ（＃２）３１４が自端末及び通信相手のモバイル通信端末１０３の端末ＩＤであることを確認する。また、暗号化通信部４０８は、デバイス鍵管理部４０３で管理するデバイス鍵ＩＤ３０２がワンタイムパッド暗号鍵カートリッジ１１２に含まれるデバイス鍵ＩＤ３０２と一致することを確認する。

以上の条件を満たしていた場合、暗号化通信部４０８は、ワンタイムパッド暗号鍵カートリッジ１１２に含まれる、暗号化したワンタイムパッド暗号鍵ブロック３１１を、ブロック復号部４０５に復号させる。この際、ブロック復号部４０５は、デバイス鍵管理部４

０３で管理するデバイス鍵１１３とワンタイムパッド暗号鍵カートリッジ１１２に含まれる暗号化パラメータ３０３とを用いて、ブロック暗号アルゴリズムにより、暗号化したワンタイムパッド暗号鍵ブロック３１１を復号する。これにより、ワンタイムパッド暗号鍵ブロック３０１が抽出される。

【００３３】

次に、モバイル通信端末１０３間で暗号化に用いるワンタイムパッド暗号鍵カートリッジ１１２の調整方法や使用済みワンタイムパッド暗号鍵カートリッジ１１２の消去方法について説明する。

【００３４】

まず、暗号化通信開始時、モバイル通信端末１０３間で使用するワンタイムパッド暗号鍵カートリッジ１１２を決定するためのネゴシエーションについて説明する。

図６は、モバイル通信端末１０３の暗号化通信開始時のシーケンスを示す図である。

なお、通信開始時点において、発信側のモバイル通信端末１０３は、ＩＤ＝１０１～３００のワンタイムパッド暗号鍵カートリッジ１１２を持っている。また、着信側のモバイル通信端末１０３は、ＩＤ＝２０１～４００のワンタイムパッド暗号鍵カートリッジ１１２を持っている。

発信側のモバイル通信端末１０３の識別情報送信部４０６は、ＩＤ＝１０１～３００のワンタイムパッド暗号鍵カートリッジ１１２を持っていることを示す暗号化通信要求（Ｐｒｏｐｏｓｅｄ　ＩＤ＝１０１－３００）（第１識別情報の例）を着信側のモバイル通信端末１０３へ送信する（Ｓ５０１）。

着信側のモバイル通信端末１０３の識別情報受信部４０７は、暗号化通信要求（Ｐｒｏｐｏｓｅｄ　ＩＤ＝１０１－３００）を受信する。すると、暗号化通信部４０８は、処理装置により、受信した暗号化通信要求が示すＩＤ（＝１０１～３００）と、着信側のモバイル通信端末１０３が持っているワンタイムパッド暗号鍵カートリッジ１１２のＩＤ（＝２０１～４００）とを比較する。これにより、暗号化通信部４０８は、発信側と着信側との双方のモバイル通信端末１０３が共有するワンタイムパッド暗号鍵カートリッジ１１２のＩＤを特定する。ここでは、双方のモバイル通信端末１０３は、ＩＤ＝２０１～３００のワンタイムパッド暗号鍵カートリッジ１１２を共有している。そこで、着信側のモバイル通信端末１０３の識別情報送信部４０６は、双方のモバイル通信端末１０３がＩＤ＝２０１～３００のワンタイムパッド暗号鍵カートリッジ１１２を共有していることを示す暗号化通信開始応答（Ａｃｃｅｐｔ　ＩＤ＝２０１－３００）（第２識別情報の例）を、発信側のモバイル通信端末１０３へ返信する（Ｓ５０２）。

発信側のモバイル通信端末１０３の識別情報受信部４０７は、暗号化通信開始応答（Ａｃｃｅｐｔ　ＩＤ＝２０１－３００）を受信する。これにより、双方のモバイル通信端末１０３は、双方のモバイル通信端末１０３が共有するワンタイムパッド暗号鍵カートリッジ１１２のＩＤを知ることができる。

そこで、双方のモバイル通信端末１０３の暗号化通信部４０８は、処理装置により、共有しているワンタイムパッド暗号鍵カートリッジ１１２のＩＤから、使用するワンタイムパッド暗号鍵カートリッジ１１２を予め共有した方法で決定する。例えば、暗号化通信部４０８は、最も値の小さいＩＤを選択する。ここでは、ＩＤ＝２０１が選択される。そして、双方のモバイル通信端末１０３の暗号化通信部４０８は、ＩＤ＝２０１のワンタイムパッド暗号鍵カートリッジ１１２の開封処理（図５参照）を行う（Ｓ５１１）。

その後、双方のモバイル通信端末１０３の暗号化通信部４０８は、ワンタイムパッド暗号化・復号部４０９に、ＩＤ＝２０１のワンタイムパッド暗号鍵カートリッジ１１２におけるワンタイムパッド暗号鍵ブロック３０１を前のビットから順に用いて通信データを暗号化させる。そして、双方のモバイル通信端末１０３の暗号化通信部４０８は、暗号化された通信データを送受信することにより、暗号化通信を行う（Ｓ５０３）。なお、通信データとは、例えば、マイク４１５から入力された通話データである。

【００３５】

次に、１個分のワンタイムパッド暗号鍵カートリッジ１１２の通信データ量を超えて暗

号化通信を継続したため、ワンタイムパッド暗号鍵カートリッジ１１２を使い切ってしまった場合の動作について説明する。

図７は、モバイル通信端末１０３の暗号化通信中のシーケンスを示す図である。

なお、双方のモバイル通信端末１０３は、ＩＤ＝２０１～３００のワンタイムパッド暗号鍵カートリッジ１１２を持っている。

図７において、ＩＤ＝２０１のワンタイムパッド暗号鍵カートリッジ１１２の開封処理（Ｓ５１１）及びＩＤ＝２０１のワンタイムパッド暗号鍵カートリッジ１１２を用いた暗号化通信（Ｓ５０３）は、図６のシーケンスと同様である。

カートリッジ１個分の通信データ量の通信後、双方のモバイル通信端末１０３の暗号鍵ブロック消去部４１０は、ＩＤ＝２０１のワンタイムパッド暗号鍵カートリッジ１１２の廃棄処理を行う（Ｓ５２１）。また、双方のモバイル通信端末１０３の暗号化通信部４０８は、残りのワンタイムパッド暗号鍵カートリッジ１１２の中で最も値の小さいＩＤ（ここでは、ＩＤ＝２０２）を選択して、選択したワンタイムパッド暗号鍵カートリッジ１１２の開封処理を行う（Ｓ５１２）。その後、双方のモバイル通信端末１０３の暗号化通信部４０８は、ＩＤ＝２０２のワンタイムパッド暗号鍵カートリッジ１１２におけるワンタイムパッド暗号鍵ブロック３０１を前のビットから順に用いて、ワンタイムパッド暗号化・復号部４０９に通信データを暗号化させる。そして、双方のモバイル通信端末１０３の暗号化通信部４０８は、暗号化された通信データを送受信することにより、暗号化通信を行う（Ｓ５０４）。

【００３６】

次に、暗号化通信終了時、モバイル通信端末１０３におけるワンタイムパッド暗号鍵カートリッジ１１２の廃棄について説明する。

図８は、モバイル通信端末１０３の暗号化通信終了時のシーケンスを示す図である。

なお、双方のモバイル通信端末１０３はＩＤ＝２０３～３００のワンタイムパッド暗号鍵カートリッジ１１２を持っており、ＩＤ＝２０３のワンタイムパッド暗号鍵カートリッジ１１２を用いた暗号化通信を行っている（Ｓ５０５）。

一方のモバイル通信端末１０３の暗号化通信部４０８は、暗号化通信終了要求を他方のモバイル通信端末１０３へ送信する（Ｓ５０６）。すると、他方のモバイル通信端末１０３の暗号化通信部４０８は、暗号化通信終了応答を返信する（Ｓ５０７）。その後、双方のモバイル通信端末１０３の暗号鍵ブロック消去部４１０は、ＩＤ＝２０３のワンタイムパッド暗号鍵カートリッジ１１２の廃棄処理を行う（Ｓ５２３）。

【００３７】

図９は、ワンタイムパッド暗号鍵カートリッジ１１２の廃棄の説明図である。なお、図９では、１つのワンタイムパッド暗号鍵カートリッジ１１２が１０分の通話データを暗号化できるだけのワンタイムパッド暗号用の暗号鍵であり、モバイル通信端末１０３間で２４分間通話を行った場合の例を示す。

まず、ＩＤ＝２０１のワンタイムパッド暗号鍵カートリッジ１１２は、最初の１０分間の通話に使用され、最初の１０分間の通話が終わった時点で消去される。次に、ＩＤ＝２０２のワンタイムパッド暗号鍵カートリッジ１１２は、１１分から２０分の通話に使用され、１１分から２０分の通話が終わった時点で消去される。そして、ＩＤ＝２０３のワンタイムパッド暗号鍵カートリッジ１１２は、２１分から２４分の通話に使用され、通話終了となった時点で消去される。

つまり、ＩＤ＝２０３のワンタイムパッド暗号鍵カートリッジ１１２は、通話終了時点で残りがあるが、残りの部分は使用されることなく、消去される。すなわち、ワンタイムパッド暗号鍵カートリッジ１１２は、２４分間の通話により、３０分間の通話分消費される。

【００３８】

次に、１台のモバイル通信端末１０３に着目したワンタイムパッド暗号鍵カートリッジ１１２の取り扱いについて説明する。

図１０は、モバイル通信端末１０３におけるワンタイムパッド暗号鍵カートリッジ１１

２の取り扱いを示すフローチャートである。
まず、モバイル通信端末１０３の識別情報送信部４０６、識別情報受信部４０７は、通信相手のモバイル通信端末１０３との通信開始時のネゴシエーションを行う。これにより、最初に使用するワンタイムパッド暗号鍵カートリッジ１１２のワンタイムパッド暗号鍵カートリッジＩＤ３１２の値が決定され、決定した値が変数Ｘに設定され主記憶装置４０１に保存される（Ｓ６０１）。
暗号化通信部４０８は、補助記憶装置４０２におけるＩＤ＝Ｘのワンタイムパッド暗号鍵カートリッジ１１２からワンタイムパッド暗号鍵ブロック３０１を抽出し、主記憶装置４０１に展開して記憶する（Ｓ６０２）。また、暗号鍵ブロック消去部４１０は、補助記憶装置４０２からＩＤ＝Ｘのワンタイムパッド暗号鍵カートリッジ１１２を消去する（Ｓ６０３）。
【００３９】
続いて、暗号化通信部４０８は、抽出したワンタイムパッド暗号鍵ブロック３０１を用いた暗号化通信を行う（Ｓ６０４）。
暗号化通信が終了した場合（Ｓ６０５でＹＥＳ）、暗号鍵ブロック消去部４１０は、主記憶装置４０１からワンタイムパッド暗号鍵ブロック３０１を消去する（Ｓ６０９）。
一方、暗号化通信が継続中であり、かつワンタイムパッド暗号鍵ブロック３０１が残っている場合（Ｓ６０５、Ｓ６０６共にＮＯ）、暗号化通信部４０８は（Ｓ６０４）へ処理を戻し、使用中のワンタイムパッド暗号鍵ブロック３０１を用いた暗号化通信を行う。
また、暗号化通信が継続中であるが、ワンタイムパッド暗号鍵ブロック３０１を使い切った場合（Ｓ６０５でＮＯ、Ｓ６０６でＹＥＳ）、暗号鍵ブロック消去部４１０は主記憶装置４０１からワンタイムパッド暗号鍵ブロック３０１を消去する（Ｓ６０７）。続いて、暗号化通信部４０８は、次に暗号化に用いるワンタイムパッド暗号鍵カートリッジ１１２のワンタイムパッド暗号鍵カートリッジＩＤ３１２の値を変数Ｘに設定した後、（Ｓ６０２）へ処理を戻す。そして、暗号化通信部４０８は、新しいワンタイムパッド暗号鍵カートリッジ１１２からワンタイムパッド暗号鍵ブロック３０１を抽出する。
【００４０】
次に、モバイル通信端末１０３におけるワンタイムパッド暗号鍵カートリッジ１１２の残量を利用者に通知する方法について説明する。
図１１は、モバイル通信端末１０３における画面表示を示す図である。なお、図１１は、モバイル通信端末１０３間で音声通話する場合を例として示す。
残量通知部４１１は、暗号化通信をしている場合には、暗号化通信中であることを示す情報７０１を液晶表示画面４１２に表示する。また、残量通知部４１１は、残っているワンタイムパッド暗号鍵カートリッジ１１２を全て用いた場合の暗号化通信可能時間を示す情報７０２を液晶表示画面４１２に表示する。なお、暗号化通信可能時間は、ワンタイムパッド暗号鍵カートリッジ１１２の残りのビット数を、通信のビットレート×２で割ることにより計算できる。また、残量通知部４１１は、ワンタイムパッド暗号鍵カートリッジ１１２の総残量を示す情報７０３を液晶表示画面４１２に表示する。また、残量通知部４１１は、現在使用中のワンタイムパッド暗号鍵カートリッジ１１２における暗号鍵の残量を示す情報７０４を液晶表示画面４１２に表示する。
残量通知部４１１は、これらの情報７０１～７０４を液晶表示画面４１２に表示することにより、ワンタイムパッド暗号鍵カートリッジ１１２の残量を利用者に通知する。
【００４１】
また、残量通知部４１１は、暗号化通信可能時間が一定の値以下となった場合やワンタイムパッド暗号鍵カートリッジ１１２の残量が１個減少した場合等において、バイブレータ４１３を用いた振動やスピーカー４１４を用いた効果音や音声ガイダンスを出力する。
これにより、残量通知部４１１は、利用者が液晶表示画面４１２を見ることができない場合であっても、利用者にワンタイムパッド暗号鍵カートリッジ１１２の減少を通知することができる。
【００４２】

以上のように、実施の形態１における通信システム１では、鍵共有システム１０１を用いて拠点間で共有したワンタイムパッド暗号鍵１１１をワンタイムパッド暗号鍵カートリッジ１１２に変換した上でモバイル通信端末１０３に転送する。そして、モバイル通信端末１０３は、ワンタイムパッド暗号鍵カートリッジ１１２を持ち出し、モバイル通信端末１０３間でワンタイムパッド暗号鍵カートリッジ１１２を用いた暗号化通信を行う。これにより、モバイル通信端末１０３間でワンタイムパッド暗号方式を用いた暗号化通信を実現する。

特に、実施の形態１における通信システム１では、暗号化通信開始時にワンタイムパッド暗号鍵カートリッジ１１２に含まれるワンタイムパッド暗号鍵カートリッジＩＤ３１２の情報を交換する。そのため、モバイル通信端末１０３に転送されたワンタイムパッド暗号鍵カートリッジ１１２が完全に一致していない場合であっても、モバイル通信端末１０３間でどのワンタイムパッド暗号鍵カートリッジ１１２を使用するかを調整して暗号化通信を実現することができる。

なお、量子暗号鍵配布技術により鍵の共有をする場合、鍵共有システム１０１における鍵共有装置１０５間の距離は、５０～１００キロメートル程度が限界であるとされている。したがって、通信端末を固定端末とした場合、ワンタイムパッド暗号による暗号化通信を行えるのは、５０～１００キロメートル程度の範囲内になる通信端末間に限定されていた。しかし、実施の形態１における通信システム１では、モバイル通信端末１０３間でワンタイムパッド暗号方式を用いた暗号化通信を実現できるため、距離の制約がなくなる。

【００４３】

また、実施の形態１における通信システム１では、使用済みのワンタイムパッド暗号鍵カートリッジ１１２は不要になった時点で即消去している。そのため、モバイル通信端末１０３からワンタイムパッド暗号鍵カートリッジ１１２を抜き出して、過去の暗号化通信内容の復号を防止することができる。

特に、ワンタイムパッド暗号鍵カートリッジ１１２を開封し、主記憶装置４０１へ展開した時点で、補助記憶装置４０２からワンタイムパッド暗号鍵カートリッジ１１２を消去する。主記憶装置４０１は、モバイル通信端末１０３の電源が入っている場合のみデータを保持可能であり、電源が入っていなければデータを保持できない。そのため、暗号化した通信データを送信した後、ワンタイムパッド暗号鍵カートリッジ１１２を消去する前に、モバイル通信端末１０３の電源が落ちた場合には、展開されたワンタイムパッド暗号鍵カートリッジ１１２は主記憶装置４０１から自動的に消去される。したがって、このような場合であっても、モバイル通信端末１０３からワンタイムパッド暗号鍵を抜き出して、過去の暗号化通信内容の復号を防止することができる。

【００４４】

また、実施の形態１における通信システム１では、モバイル通信端末１０３の液晶表示画面４１２、バイブレータ４１３、スピーカー４１４を通して各種残量及びその変化を通知する。これにより、利用者は、ワンタイムパッド暗号鍵カートリッジ１１２の減少や、暗号化通信可能時間の残りを知ることができる。

【００４５】

以上の実施の形態におけるモバイル通信端末１０３のハードウェア構成について説明する。

図１２は、モバイル通信端末１０３のハードウェア構成の一例を示す図である。

図１２に示すように、モバイル通信端末１０３は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４（主記憶装置４０１の一例）、液晶表示画面４１２、キーボード９０２（Ｋ／Ｂ）、バイブレータ４１３、スピーカー４１４、マイク４１５、無線通信ボード９１５（無線通信部４１６の一例）、有線通信ボード９１６（有線通信部４１７の一例）、磁気ディスク装置９２０（補助記憶装置４０２の一例）と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装

置９２０の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。磁気ディスク装置９２０は、所定の固定ディスクインタフェースを介して接続される。

【００４６】

磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

【００４７】

プログラム群９２３には、上記の説明において「暗号鍵カートリッジ受信部４０４」、「ブロック復号部４０５」、「識別情報送信部４０６」、「識別情報受信部４０７」、「暗号化通信部４０８」、「ワンタイムパッド暗号化・復号部４０９」、「暗号鍵ブロック消去部４１０」、「残量通知部４１１」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、上記の説明において「ワンタイムパッド暗号鍵カートリッジ１１２」、「ワンタイムパッド暗号鍵ブロック３０１」、「デバイス鍵１１３」等の情報やデータや信号値や変数値やパラメータが、「データベース」の各項目として記憶される。「データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１の動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

【００４８】

なお、暗号鍵転送装置１０２も、モバイル通信端末１０３と同様に、プログラムを実行するＣＰＵ９１１を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４（主記憶装置２０１の一例）、ＬＣＤ９０１、キーボード９０２（Ｋ／Ｂ）、通信ボード９１５、磁気ディスク装置９２０（補助記憶装置２０２の一例）と接続され、これらのハードウェアデバイスを制御する。

【００４９】

磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

【００５０】

プログラム群９２３には、上記の説明において「暗号鍵取得部２０４」、「暗号鍵カートリッジ生成部２０５」、「ブロック暗号化部２０６」、「暗号鍵カートリッジ転送部２０７」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。

ファイル群９２４には、上記の説明において「ワンタイムパッド暗号鍵１１１」、「ワンタイムパッド暗号鍵カートリッジ１１２」、「デバイス鍵１１３」等の情報やデータや信号値や変数値やパラメータが、「データベース」の各項目として記憶される。

【００５１】

また、上記の説明におけるフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、その他光ディスク等の記録媒体やＩＣチップに記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体や電波によりオンライン伝送される。

また、上記の説明において「～部」として説明するものは、「～回路」、「～装置」、

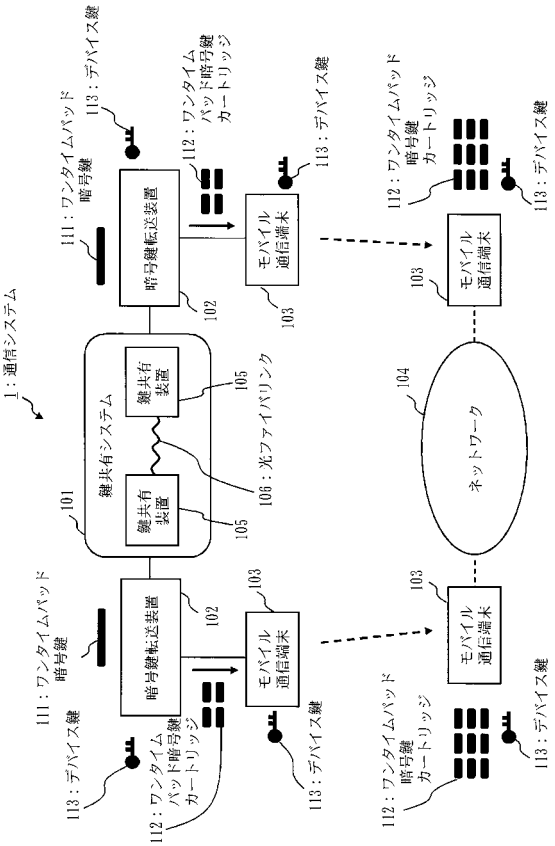
「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。また、「～装置」、「～端末」として説明するものは、「～回路」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組合せ、さらには、ファームウェアとの組合せで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、ＲＯＭ９１３等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、上記で述べた「～部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた「～部」の手順や方法をコンピュータ等に実行させるものである。

【符号の説明】

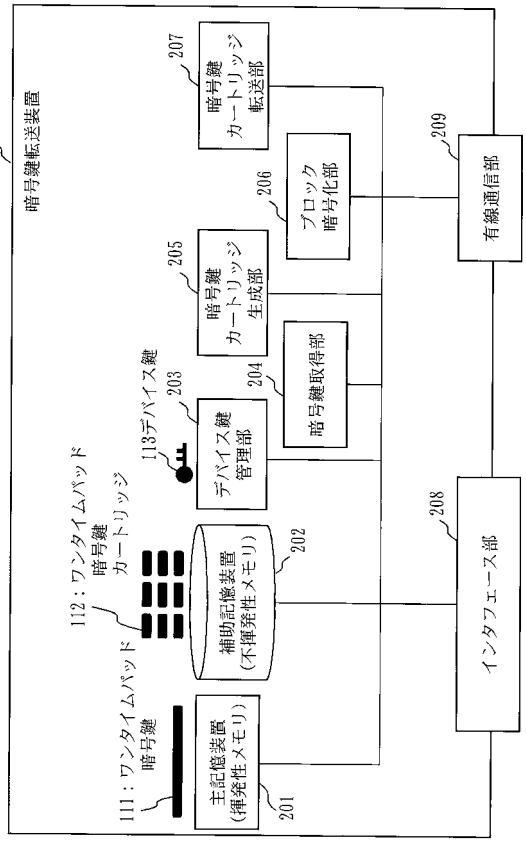
【００５２】

１　通信システム、１０１　鍵共有システム、１０２　暗号鍵転送装置、１０３　モバイル通信端末、１０４　ネットワーク、１０５　鍵共有装置、１０６　光ファイバリンク、１１１　ワンタイムパッド暗号鍵、１１２　ワンタイムパッド暗号鍵カートリッジ、１１３　デバイス鍵、２０１　主記憶装置、２０２　補助記憶装置、２０３　デバイス鍵管理部、２０４　暗号鍵取得部、２０５　暗号鍵カートリッジ生成部、２０６　ブロック暗号化部、２０７　暗号鍵カートリッジ転送部、２０８　インタフェース部、２０９　有線通信部、３０１　ワンタイムパッド暗号鍵ブロック、３０２　デバイス鍵ＩＤ、３０３　暗号化パラメータ、３１１　暗号化したワンタイムパッド暗号鍵ブロック、３１２　ワンタイムパッド暗号鍵カートリッジＩＤ、３１３　端末ＩＤ（＃１）、３１４　端末ＩＤ（＃２）、４０１　主記憶装置、４０２　補助記憶装置、４０３　デバイス鍵管理部、４０４　暗号鍵カートリッジ受信部、４０５　ブロック復号部、４０６　識別情報送信部、４０７　識別情報受信部、４０８　暗号化通信部、４０９　ワンタイムパッド暗号化・復号部、４１０　暗号鍵ブロック消去部、４１１　残量通知部、４１２　液晶表示画面、４１３　バイブレータ、４１４　スピーカー、４１５　マイク、４１６　無線通信部、４１７　有線通信部。

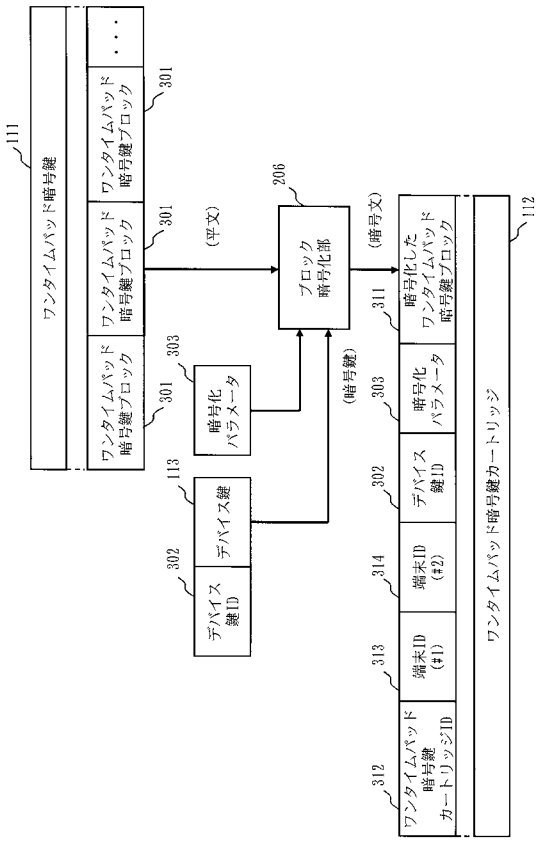
【図１】


1：通信システム
111：ワンタイムパッド暗号鍵
113：デバイス鍵
112：ワンタイムパッド暗号鍵カートリッジ
101
鍵共有システム
鍵共有装置
105
106：光ファイバリンク
暗号鍵転送装置
102
モバイル通信端末
103
ネットワーク
104

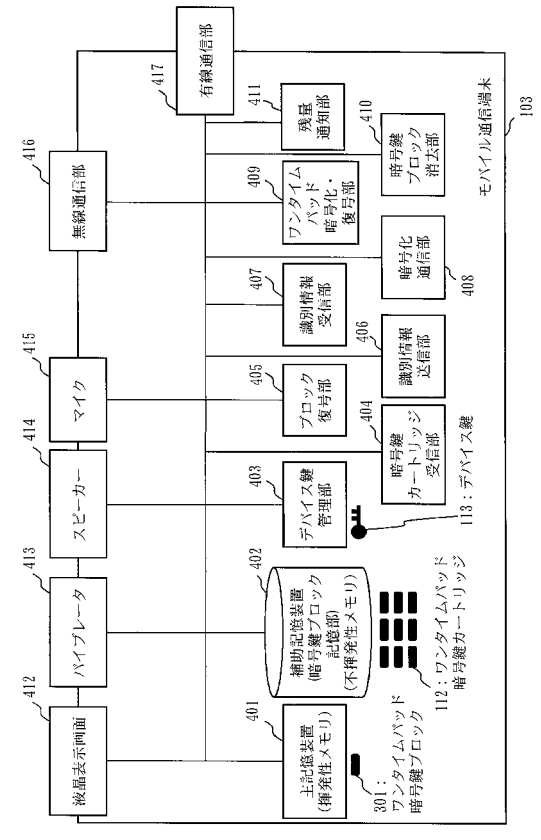
【図２】


102
暗号鍵転送装置
112：ワンタイムパッド暗号鍵カートリッジ
111：ワンタイムパッド暗号鍵
113デバイス鍵
主記憶装置（揮発性メモリ）
補助記憶装置（不揮発性メモリ）
デバイス鍵管理部
暗号鍵取得部
暗号鍵カートリッジ生成部
ブロック暗号化部
暗号鍵カートリッジ転送部
有線通信部
インタフェース部
201
202
203
204
205
206
207
208
209

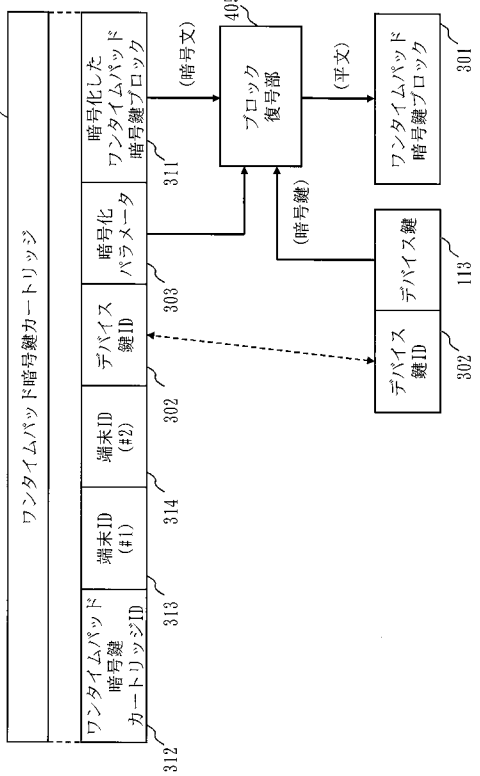
【図３】


111
ワンタイムパッド暗号鍵
ワンタイムパッド暗号鍵ブロック
301
（平文）
（暗号文）
（暗号鍵）
206
ブロック暗号化部
暗号化パラメータ
303
デバイス鍵ID
302
デバイス鍵
113
端末ID（#1）
313
端末ID（#2）
314
デバイス鍵ID
302
暗号化パラメータ
303
暗号化したワンタイムパッド暗号鍵ブロック
311
ワンタイムパッド暗号鍵カートリッジID
312
ワンタイムパッド暗号鍵カートリッジ
112

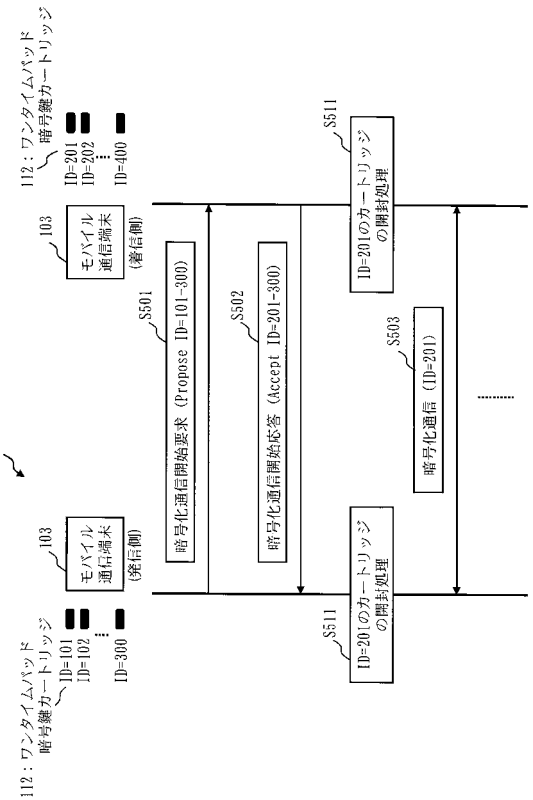
【図４】


液晶表示画面
412
バイブレータ
413
スピーカー
414
マイク
415
無線通信部
416
有線通信部
417
主記憶装置（揮発性メモリ）
401
補助記憶装置（暗号鍵ブロック記憶部）（不揮発性メモリ）
402
デバイス鍵管理部
403
ブロック復号部
405
識別情報受信部
407
ワンタイムパッド暗号化・復号部
409
残量通知部
411
暗号鍵ブロック消去部
410
暗号鍵カートリッジ受信部
404
識別情報送信部
406
暗号化通信部
408
301：ワンタイムパッド暗号鍵ブロック
112：ワンタイムパッド暗号鍵カートリッジ
113：デバイス鍵
モバイル通信端末
103

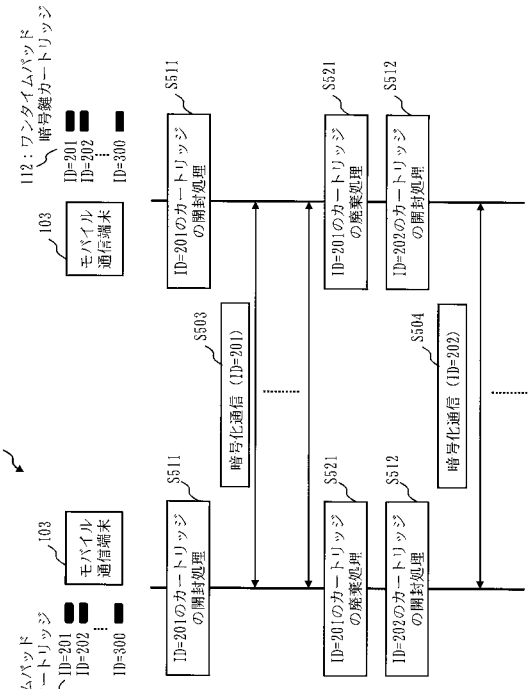
【図５】


112
ワンタイムパッド暗号鍵カートリッジ
ワンタイムパッド暗号鍵カートリッジID
端末ID (#1)
端末ID (#2)
デバイス鍵ID
暗号化パラメータ
暗号化したワンタイムパッド暗号鍵ブロック
312
313
314
302
303
311
405
ブロック復号部
(暗号文)
(平文)
(暗号鍵)
デバイス鍵ID
デバイス鍵
302
113
ワンタイムパッド暗号鍵ブロック
301

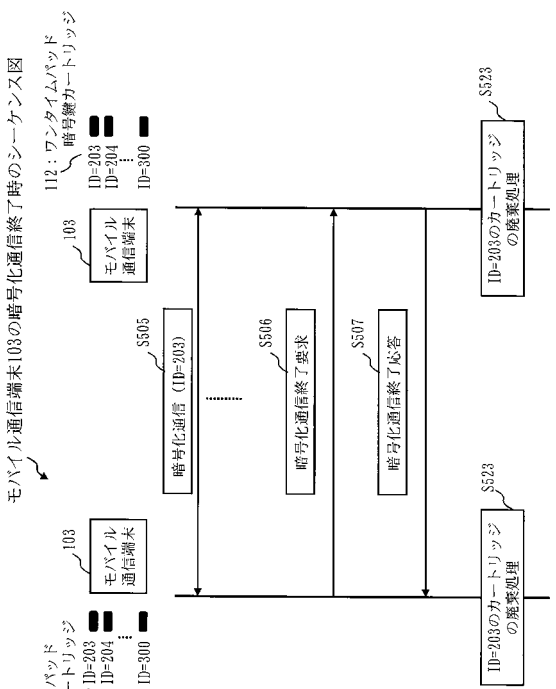
【図６】


モバイル通信端末103間の暗号化通信開始時のシーケンス図
112：ワンタイムパッド暗号鍵カートリッジ
ID=101
ID=102
ID=300
103
モバイル通信端末
(発信側)
暗号化通信開始要求 (Propose ID=101-300)
暗号化通信開始応答 (Accept ID=201-300)
暗号化通信 (ID=201)
S501
S502
S503
S511
ID=201のカートリッジの開封処理
ID=201のカートリッジの開封処理
112：ワンタイムパッド暗号鍵カートリッジ
ID=201
ID=202
ID=400
103
モバイル通信端末
(着信側)
S511
ID=201のカートリッジの開封処理

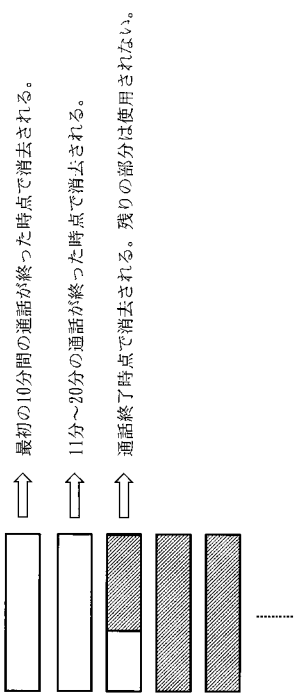
【図７】


モバイル通信端末103の暗号化通信中のシーケンス図
112：ワンタイムパッド暗号鍵カートリッジ
ID=201
ID=202
ID=300
103
モバイル通信端末
S511
ID=201のカートリッジの開封処理
暗号化通信 (ID=201)
S503
S521
ID=201のカートリッジの廃棄処理
S512
ID=202のカートリッジの開封処理
暗号化通信 (ID=202)
S504
112：ワンタイムパッド暗号鍵カートリッジ
ID=201
ID=202
ID=300
103
モバイル通信端末
S511
ID=201のカートリッジの開封処理
S521
ID=201のカートリッジの廃棄処理
S512
ID=202のカートリッジの開封処理

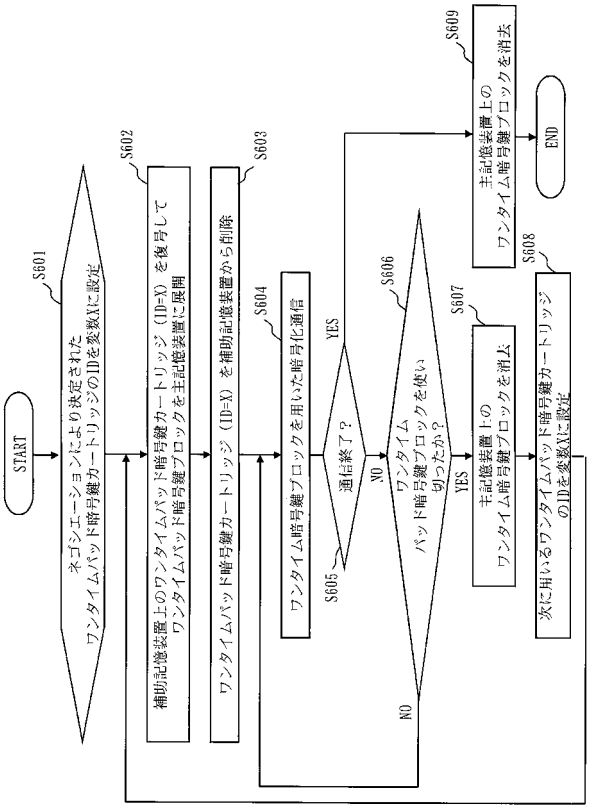
【図８】


モバイル通信端末103の暗号化通信終了時のシーケンス図
112：ワンタイムパッド暗号鍵カートリッジ
ID=203
ID=204
ID=300
103
モバイル通信端末
暗号化通信 (ID=203)
S505
暗号化通信終了要求
S506
暗号化通信終了応答
S507
S523
ID=203のカートリッジの廃棄処理
112：ワンタイムパッド暗号鍵カートリッジ
ID=203
ID=204
ID=300
103
モバイル通信端末
S523
ID=203のカートリッジの廃棄処理

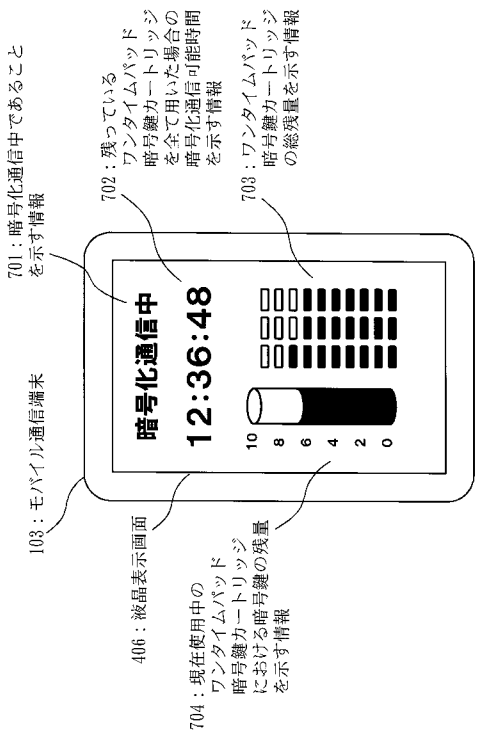
【図９】




【図１０】




【図１１】




【図１２】

フロントページの続き

(56)参考文献 特開２００８－１５４０１９（ＪＰ，Ａ）
特開２００５－３１８２８１（ＪＰ，Ａ）
特開２００４－８０６６３（ＪＰ，Ａ）
特開２００２－２５９２１８（ＪＰ，Ａ）
特表平８－５０４０６７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１８