(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-249507
(P2007-249507A)
(43)公開日　平成19年9月27日(2007.9.27)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	510F	5B017
H04Q 7/38	(2006.01)	G06F	12/14	560D	5K067
		G06F	12/14	540P	
		H04B	7/26	109R	

審査請求 未請求　請求項の数 8　OL　（全 15 頁）

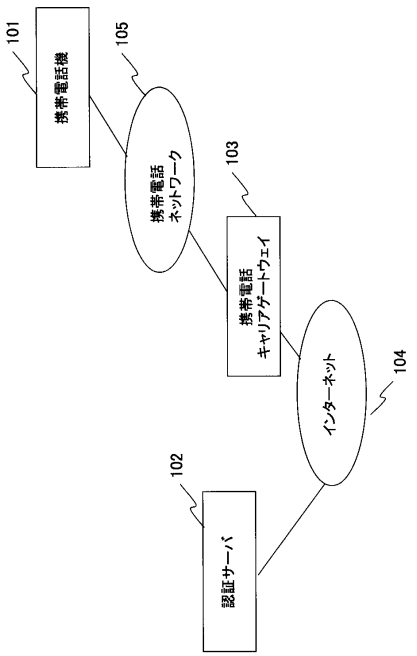
(21)出願番号　特願2006-71015(P2006-71015)
(22)出願日　平成18年3月15日(2006.3.15)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市鶴見区末広町一丁目１番４３
(74)代理人　110000442
特許業務法人　武和国際特許事務所
(72)発明者　堤　俊之
東京都品川区東品川４丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

Fターム(参考)　5B017 AA03 BA05 BA07 BA08 BA10
5K067 AA32 BB04 BB21 EE02 EE10 EE16 HH22 HH23 HH24 HH36 KK15

(54)【発明の名称】情報漏洩防止方法、情報漏洩防止システム及び情報端末

(57)【要約】
【課題】携帯電話機等の通信可能な端末を紛失したり、盗まれたりした場合にも、内部の個人情報や機密情報等の情報の漏洩を確実に防止する。
【解決手段】携帯電話機101とインターネットに接続している認証サーバ102とが、接続されて構成される。携帯電話機は、自身で分割した機密情報の一方とPIN情報とを認証サーバに登録し、PIN情報で利用者認証して、機密情報を認証サーバから取得する。認証サーバは、PIN情報、機密情報を携帯電話テーブルに登録し、PIN情報を携帯電話機から受信して利用者認証を行い機密情報を返送する。携帯電話機内の機密情報は、PIN情報による利用者認証が規定回数以上失敗した場合に削除される。認証サーバから取得した機密情報は、揮発性メモリに保持され、電源断、リセット時に消去される。分割された他方の機密情報は、携帯電話自身が保持し、両情報が揃ったとき機密情報全体が復元できる。
【選択図】図１



【特許請求の範囲】
【請求項１】
情報端末内の機密情報の漏洩を防止する情報漏洩防止方法において、前記情報端末は、ネットワークを介して認証サーバと接続する通信手段を備え、情報端末内で前記機密情報を暗号化して分割し、分割した一方のデータを前記認証サーバに送信して保持させると共に分割した他方のデータを自端末内に保持し、前記機密情報の利用時、前記認証サーバから前記分割した一方のデータを取得し、このデータと、自端末内に保持していた前記他方のデータとから前記機密情報を復元することを特徴とする情報漏洩防止方法。
【請求項２】
前記情報端末は、分割した他方のデータを自端末内に不揮発性の記憶部に保持し、前記認証サーバから機密情報の暗号化のために取得した暗号鍵、復元した機密情報を揮発性メモリに保持することにより、電源が切断され、あるいは、リセットされた場合に前記揮発性メモリ内に保持している情報を消去することを特徴とする請求項１記載の情報漏洩防止方法。
【請求項３】
前記情報端末は、情報端末の利用時に必要な認証データであるローカルＰＩＮと認証サーバの利用時に必要な認証データであるネットワークＰＩＮとを予め認証サーバに登録し、前記機密情報の利用時、前記ローカルＰＩＮ、ネットワークＰＩＮを認証サーバに送信して認証を受け、認証成功時に、前記認証サーバから前記分割した一方のデータと復号用の暗号鍵とを受け取ることを特徴とする請求項１または２記載の情報漏洩防止方法。
【請求項４】
前記情報端末は、ローカルＰＩＮによる利用者認証が規定回数以上失敗した場合に、前記情報端末内に保持している機密情報を削除することを特徴とする請求項３記載の情報漏洩防止方法。
【請求項５】
情報端末内の機密情報の漏洩を防止する情報漏洩防止システムにおいて、前記情報端末は、ネットワークを介して認証サーバと接続する通信手段と、情報端末内で前記機密情報を暗号化し分割する手段と、分割した一方のデータを前記認証サーバに送信する手段と、分割した他方のデータを自端末内に保持する手段と、前記機密情報の利用時、前記認証サーバから前記分割した一方のデータを取得する手段と、認証サーバから取得した一方のデータ及び自端末内に保持していた前記他方のデータとから前記機密情報を復元する手段とを備え、前記認証サーバは、情報端末から送信されてきた前記分割した一方のデータを保持する手段と、情報端末からの要求により前記一方のデータを返送する手段とを備えることを特徴とする情報漏洩防止システム。
【請求項６】
前記情報端末は、情報端末の利用時に必要な認証データであるローカルＰＩＮと認証サーバの利用時に必要な認証データであるネットワークＰＩＮとを予め前記認証サーバに登録する手段と、前記機密情報の利用時、前記ローカルＰＩＮ、ネットワークＰＩＮを認証サーバに送信して認証を受ける手段と、認証成功時に、前記認証サーバから前記分割した一方のデータと復号用の暗号鍵とを受け取る手段とをさらに備え、前記認証サーバは、前記情報端末からの前記ローカルＰＩＮとネットワークＰＩＮとを登録して保持する手段と、前記情報端末からの機密情報の要求時に、要求と共に送信されてくる前記ローカルＰＩＮ、ネットワークＰＩＮにより情報端末の認証を行う手段と、認証の成功時に保持していた前記一方のデータと共に復号化のための暗号鍵を返送する手段とをさらに備えることを特徴とする請求項５記載の情報漏洩防止システム。
【請求項７】
機密情報の漏洩を防止することができる情報端末において、ネットワークを介して認証サーバと接続する通信手段と、情報端末内で前記機密情報を暗号化し分割する手段と、分割した一方のデータを前記認証サーバに送信する手段と、分割した他方のデータを自端末内に保持する手段と、前記機密情報の利用時、前記認証サーバから前記分割した一方のデ

ータを取得する手段と、認証サーバから取得した一方のデータ及び自端末内に保持していた前記他方のデータとから前記機密情報を復元する手段とを備えることを特徴とする情報端末。

【請求項８】

情報端末の利用時に必要な認証データであるローカルＰＩＮと認証サーバの利用時に必要な認証データであるネットワークＰＩＮとを予め認証サーバに登録する手段と、前記機密情報の利用時、前記ローカルＰＩＮ、ネットワークＰＩＮを認証サーバに送信して認証を受け、認証成功時に、前記認証サーバから前記分割した一方のデータと復号用の暗号鍵とを受け取る手段とをさらに備えることを特徴とする請求項７記載の情報端末。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報漏洩防止方法、情報漏洩防止システム及び情報端末に係り、特に、携帯電話機等の通信可能な情報端末を紛失したり、盗まれたりした場合、端末内に格納されている個人情報や機密情報等の情報の漏洩を防止することを可能にした情報漏洩防止方法、情報漏洩防止システム及び情報端末に関する。

【背景技術】

【０００２】

近年、携帯電話機等の携帯可能で通信をも行うことができる情報端末の高機能化により、従来、ノートＰＣ等で行われていた業務作業を携帯端末で行うことができるようになってきている。これに伴い、取引先の顧客情報や卸価格等の機密情報を携帯端末に格納して利用する場面が増加してきている。

【０００３】

一方、個人情報保護法の施行により、個人の氏名や住所、電話番号等の個人を特定できる情報の漏洩防止は、重要な課題となっており、これらの情報が漏洩した場合には、組織の存亡を左右する大きな問題となってしまう。また、個人情報以外の情報に対しても、厳格な管理を行い、情報を漏洩させない体制を整備することが重要となってきている。

【０００４】

このため、携帯端末を紛失したり、盗難されたりした場合にも、携帯端末に格納されている個人情報や機密情報を漏洩させない仕組みが要求されている。

【０００５】

機密情報の漏洩防止に関する従来技術として、例えば、特許文献１等に記載された技術が知られている。この従来技術は、携帯電話機に格納されている特定のプログラムや特定のデータの漏洩を防止するものであり、フラッシュメモリ等の不揮発性メモリに格納されているこれらのデータを、サーバからの要求に従って削除するというものである。

【０００６】

また、他の従来技術として、非特許文献１等に記載された技術が知られている。この従来技術は、携帯電話機がサーバから個人情報等を取得して保持した場合、その受信データを特定時刻や一定時間経過後に削除するというものである。

【特許文献１】特願２００２－５８９９７０号公報　（第３１頁）

【非特許文献１】「ａｕ携帯電話による高い個人情報漏洩防止機能を備えた「渉外支援システム」を開発」ＫＤＤＩ（株）、日本ヒューレット・パッカード（株））、２００５年３月１１日発表http://www.kddi.com/corporate/news_release/2005/0311/

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかし、前述した特許文献１に記載の従来技術は、携帯電話機の電波が到達しない場所に携帯電話機が移動させられた場合、サーバからの命令を受信することができず、個人情報や機密情報を消去することができず、また、携帯電話機のハードウェア改造により、不揮発性メモリ上のデータを抽出する攻撃を防御することができないため、機密情報が盗ま

れてしまうという問題点を有している。

【０００８】

また、非特許文献１に記載の従来技術は、一定時間の経過で携帯電話機のデータを消去する場合、安全性を保つために、短い間隔でデータを消去を行う必要があるが、短い間隔でのデータの消去は利用者の利便性を低下させるという問題点を生じさせ、また、インターネット等の公衆通信網を介してアクセスするサーバにデータが保持されているため、サーバが攻撃されることにより個人情報や機密情報が盗まれてしまうという問題点を有している。

【０００９】

本発明の目的は、前述した従来技術の問題点を解決し、携帯電話機等の通信可能な情報端末を紛失したり、盗まれたりした場合に、個人情報や機密情報等の情報の漏洩を確実に防止することを可能にした情報漏洩防止方法、情報漏洩防止システム及び情報端末を提供することにある。

【課題を解決するための手段】

【００１０】

本発明によれば前記目的は、情報端末内の機密情報の漏洩を防止する情報漏洩防止方法において、前記情報端末が、ネットワークを介して認証サーバと接続する通信手段を備え、情報端末内で前記機密情報を暗号化して分割し、分割した一方のデータを前記認証サーバに送信して保持させると共に分割した他方のデータを自端末内に保持し、前記機密情報の利用時、前記認証サーバから前記分割した一方のデータを取得し、このデータと、自端末内に保持していた前記他方のデータとから前記機密情報を復元することにより達成される。

【００１１】

また、前記目的は、情報端末内の機密情報の漏洩を防止する情報漏洩防止システムにおいて、前記情報端末が、ネットワークを介して認証サーバと接続する通信手段と、情報端末内で前記機密情報を暗号化し分割する手段と、分割した一方のデータを前記認証サーバに送信する手段と、分割した他方のデータを自端末内に保持する手段と、前記機密情報の利用時、前記認証サーバから前記分割した一方のデータを取得する手段と、認証サーバから取得した一方のデータ及び自端末内に保持していた前記他方のデータとから前記機密情報を復元する手段とを備え、前記認証サーバが、情報端末から送信されてきた前記分割した一方のデータを保持する手段と、情報端末からの要求により前記一方のデータを返送する手段とを備えることにより達成される。

【００１２】

さらに、前記目的は、機密情報の漏洩を防止することができる情報端末において、ネットワークを介して認証サーバと接続する通信手段と、情報端末内で前記機密情報を暗号化し分割する手段と、分割した一方のデータを前記認証サーバに送信する手段と、分割した他方のデータを自端末内に保持する手段と、前記機密情報の利用時、前記認証サーバから前記分割した一方のデータを取得する手段と、認証サーバから取得した一方のデータ及び自端末内に保持していた前記他方のデータとから前記機密情報を復元する手段とを備えることにより達成される。

【発明の効果】

【００１３】

本発明によれば、携帯電話機等の通信可能な情報端末を紛失したり、盗まれたりした場合に、個人情報や機密情報等の情報の漏洩を確実に防止することができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明による情報漏洩防止方法及び情報漏洩防止システムの実施形態を図面により詳細に説明する。

【００１５】

図１は本発明の一実施形態による情報漏洩防止システムを構築するネットワークシステ

ムの構成を示す図である。なお、以下に説明する本発明の実施形態は、端末として携帯電話機を例に挙げて説明するが、本発明は、通信機能を持つものであれば、どのような情報端末に対しても適用することができる。図１において、１０１は携帯電話機、１０２は認証サーバ、１０３は携帯電話キャリアゲートウェイ、１０４はインターネット、１０５は携帯電話ネットワークである。

【００１６】

図１に示すネットワークシステムは、機密データを利用するアプリケーションが稼働する通信機器である携帯電話機１０１と、携帯電話機１０１と連携して、機密データの安全性を確保する通信機器である認証サーバ１０２と、携帯電話キャリアが自社の携帯電話機向けに構築した携帯電話ネットワーク１０５とインターネット１０４とを接続する通信機器である携帯電話キャリアゲートウェイ１０３とにより構成されている。そして、携帯電話機１０１は、携帯電話キャリアゲートウェイ１０３を介してインターネット１０４に接続し、認証サーバ１０１と通信を行うことができる。

【００１７】

図２は携帯電話機１０１の構成を示すブロック図である。図２において、２０１はＣＰＵ、２０２はメモリ、２０３は通信部、２０４は入力部、２０５は出力部、２０６はデータ登録プログラム、２０７はデータ利用プログラム、２０８は分散暗号データＢ、２０９は記憶部、２１０は端末識別子番号、２１１はバス、２１２は分散暗号データＡ、２１３はローカルＰＩＮ情報、２１４は暗号鍵、２１５は機密データである。

【００１８】

携帯電話機１０１は、プログラムの実行を行うＣＰＵ２０１と、プログラムやデータをロードするメモリ２０２と、他の端末とコネクションを確立する通信部２０３と、命令やデータの入力を行う入力部２０４と、システムの状態などを出力する出力部２０５と、端末識別子番号２１０と、データ登録プログラム２０６、データ利用プログラム２０７、分散暗号データＢ２０８を記憶している不揮発性メモリ等による記憶部２０９とがバス２１１により接続されて構成されている。

【００１９】

通信部２０３は、インターネットの標準プロトコルであるＴＣＰ等を用いて、他の端末との間でコネクションを確立してデータ通信を行う機能を持ち、入力部２０４は、キーボード、マウス、ペン入力、音声入力、ボタン、ジョグダイヤル、十字キー等による入力手段である。出力部２０５は、ディスプレイ、音声等の出力手段であり、端末識別番号２１０は、携帯電話のキャリアがそれぞれの携帯電話機１０１を一意に識別できるように割り当てた番号である。

【００２０】

また、データ登録プログラム２０６は、携帯電話機１０１からのＰＩＮ情報や機密データの認証サーバへの登録を行うプログラム、データ利用プログラム２０７は、携帯端末１０１で実際に機密データを利用する際に、利用者認証とアクセス制御とを行うプログラムであり、分散暗号データＢ２０８は、携帯電話機１０１で利用される機密データを作成するために必要なデータである。

【００２１】

メモリ２０２上には、一時的に保持される、分散暗号データＡ２１２、ローカルＰＩＮ情報２１３、暗号鍵２１４、機密データ２１５等がロードされる。分散暗号データＡ２１２は、携帯電話機１０１で利用される機密データを作成するために必要な、認証サーバ１０２から取得したデータであり、ローカルＰＩＮ情報２１３は、携帯電話機１０１での利用者認証に利用するデータである。暗号鍵２１４は、機密データを暗号化、復号化するために利用するデータであり、機密データ２１５は、携帯電話機１０１に保持されている平文形式の個人情報や機密情報等である。

【００２２】

図３は認証サーバ１０２の構成を示すブロック図である。図３において、３０１はＣＰＵ、３０２はメモリ、３０３は通信部、３０４は入力部、３０５は出力部、３０６はデー

タ設定プログラム、３０７はデータ認証プログラム、３０８は携帯電話テーブル、３０９はキャリアＧＷテーブル、３１０は記憶部、３１１はバスである。

【００２３】

認証サーバ１０２は、プログラムの実行を行うＣＰＵ３０１と、プログラムやデータをロードするメモリ３０２と、他の端末とコネクションを確立する通信部３０３と、命令やデータの入力を行う入力部３０４と、システムの状態などを出力する出力部３０５と、データ設定プログラム３０６、データ認証プログラム３０７、携帯電話テーブル３０８、キャリアＧＷテーブル３０９を記憶している記憶部３１０がバス３１１により接続されて構成されている。

【００２４】

データ設定プログラム３０６は、携帯端末１０１から受信したＰＩＮ情報や機密データを携帯電話テーブル３０８に設定するプログラムであり、データ認証プログラム３０７は、携帯端末１０１からの認証要求を対して、利用者認証を行うプログラムである。また、携帯電話テーブル３０８は、登録している携帯電話機１０１の情報を管理するテーブルであり、キャリアＧＷテーブル３０９は、携帯電話機１０１がインターネット１０４に接続する際に、携帯電話会社が利用するキャリアゲートウェイ１０３のネットワークアドレスを管理するテーブルである。

【００２５】

図４は携帯電話テーブル３０８の構成を示す図である。このテーブル３０８は、項番４０１、登録端末番号４０２、携帯電話キャリア４０３、ローカルＰＩＮ４０４、ネットワークＰＩＮ４０５、暗号鍵４０６、分散暗号データ４０７、ロックアウトフラグ４０８により構成される。

【００２６】

このテーブル３０８において、項番４０１は、テーブル内のレコードを一意に決定する識別子であり、登録端末番号４０２は、登録している携帯電話機１０１を一意に識別することができる番号、例えば、製造番号やネットワーク番号等である。また、携帯電話キャリア４０３は、利用している携帯電話会社の識別子であり、ローカルＰＩＮ４０４は、携帯電話機１０１の内部だけで利用者認証を行う場合に利用するデータである。

【００２７】

さらに、ネットワークＰＩＮ４０５は、携帯電話機１０１からの認証要求を処理する場合に、利用するデータであり、暗号鍵４０６は、携帯電話機１０１が機密データを暗号化、復号化する際に利用するデータである。また、分散暗号データＡ４０７は、携帯電話機１０１により暗号化された機密データの分割した一方のデータであり、ロックアウトフラグ４０８は、携帯電話機が利用者認証を受付けないロックアウト状態にあるか否かを判断するフラグである。

【００２８】

図５はキャリアＧＷテーブル３０９の構成を示す図である。このテーブル３０９は、項番５０１、ゲートウェイアドレス５０２、携帯電話アドレス５０３により構成される。

【００２９】

このテーブル３０９において、項番５０１は、テーブル内のレコードを一意に決定する識別子であり、ゲートウェイアドレス５０２は、携帯電話会社が公表しているキャリアゲートウェイ１０３のネットワークアドレスを表している。また、携帯電話キャリア５０３は、ゲートウェイアドレス５０２に対応する携帯電話会社の識別子である。

【００３０】

次に、利用者による機密データの登録の処理と、利用者による機密データの利用の処理とについて説明するが、利用者による機密データの登録の処理では、携帯電話機１０１のデータ登録プログラム２０６と認証サーバ１０２のデータ設定プログラム３０６とが利用され、利用者による機密データの利用の処理では、携帯電話機１０１のデータ利用プログラム２０７と認証サーバ１０２のデータ認証プログラム３０７とが利用される。従って、以下では、それぞれのプログラムの処理動作について説明する。

【００３１】
図６は利用者が機密データの登録を行う際の携帯電話機１０１内のデータ登録プログラム２０６の処理動作を説明するフローチャートであり、次に、これについて説明する。
【００３２】
（１）携帯電話機１０１の利用者は、ローカルＰＩＮとネットワークＰＩＮとを入力部２０４のキー等を利用して入力すると共に、保存したい機密データを入力して、データ登録プログラム２０６に取得させる。機密データは、利用者が直接入力してもよいが、携帯電話機１０１に接続されるメモリカードからのデータ、インターネットを介して得たデータであってよい（ステップ６０１）。
【００３３】
（２）次に、データ登録プログラム２０６は、ステップ６０１の処理で取得した機密データを暗号化するため、認証サーバ１０２に暗号鍵の取得要求を送信して、暗号鍵を取得する。このとき、認証サーバ１０２へ送信する取得要求には、端末識別番号２１０が含まれる（ステップ６０２）。
【００３４】
（３）ステップ６０１の処理で取得した機密データを、ステップ６０２の処理で取得した暗号鍵を用いてＡＥＳ暗号方式等により暗号化し、暗号化した機密データを、偶数バイトのデータ列と奇数バイトのデータ列とに分割する。分割したそれぞれのデータ列を、分割暗号データＡ、分割暗号データＢと呼ぶ（ステップ６０３、６０４）。
【００３５】
（４）ステップ６０４の処理で分割した分割暗号データＡと、ステップ６０１の処理で利用者により入力されたローカルＰＩＮ及びネットワークＰＩＮの情報とを認証サーバ１０２に登録するために、認証サーバ１０２に送信する（ステップ６０５）。
【００３６】
図７は図６に示すステップ６０４の処理で暗号化した機密データを分割するイメージを説明する図である。いま、ステップ６０３の処理で機密データを暗号化したとき、暗号データ７０１として示す１０バイトの暗号データ列が得られたものとする。そして、ステップ６０４の処理では、暗号化データ７０１の奇数バイトだけを集めて分散暗号データＢ７０２を生成すると共に、暗号化データ７０１の偶数バイトだけを集めて分散暗号データＡ７０３を生成する。
【００３７】
図８は図６のステップ６０２の処理で暗号鍵の取得要求を受信した場合の認証サーバ１０２のデータ設定プログラム３０６の処理動作を説明するフローチャートであり、次に、これについて説明する。
【００３８】
（１）認証サーバ１０２は、携帯電話機１０１のデータ登録プログラム２０６から暗号鍵の取得要求を受信する。要求を受信すると、その暗号鍵の取得要求元が携帯電話機であることを確認する。この確認の処理については、図９を参照して後述する（ステップ８０１、８０２）。
【００３９】
（２）ステップ８０２の処理で、暗号鍵の取得要求元が携帯電話機であることが確認できた場合、ステップ８０２の処理で取得した端末識別番号が携帯電話テーブル３０８に登録されているかを確認する（ステップ８０３）。
【００４０】
（３）ステップ８０３の確認で、端末識別番号が携帯電話テーブル３０８に登録されていなかった場合、携帯電話テーブル３０８に新たなレコードを登録する。その際、ステップ８０２で取得した端末識別番号４０２、携帯電話キャリア４０３を登録すると共に、新たに暗号鍵を設定する（ステップ８１０）。
【００４１】
（４）ステップ８０３の確認で、端末識別番号が携帯電話テーブル３０８に登録されてい

た場合、また、ステップ８１０の処理後、携帯電話テーブル３０８から暗号鍵４０６を取得して、携帯電話機１０１へ返信する（ステップ８０４）。

【００４２】

（５）その後、図６に示すステップ６０５の処理で携帯電話機１０１からの登録要求として送信されてくる分散暗号データＡと、ローカルＰＩＮ及びネットワークＰＩＮとを受信する（ステップ８０５）。

【００４３】

（６）ステップ８０４の処理とステップ８０５との処理との間でネットワークが一旦切断される場合もあるので、次に、再度、ステップ８０２の処理と同一の処理を実行して、送信元が携帯電話機であることを確認する。この確認の処理も、図９を参照して後述する場合と同様に行われる（ステップ８０６）。

【００４４】

（７）ステップ８０６の確認の処理で、送信元が携帯電話機であることが確認できれば、処理を継続し、ステップ８０６の処理で取得した端末識別番号に対応した携帯電話テーブル３０８の項目にネットワークＰＩＮが設定されているか否かを確認する（ステップ８０７）。

【００４５】

（８）ステップ８０７の確認で、端末識別番号に対応したネットワークＰＩＮが携帯電話テーブル３０８の項目に設定されていた場合、ステップ８０６の処理で取得した端末識別番号に対応した携帯電話テーブル３０８の項目のネットワークＰＩＮとステップ８０５の処理で受信したネットワークＰＩＮとが同一であるか否かを確認し、同一でなかった場合、何もせずに、ここでの処理を終了する（ステップ８０８）。

【００４６】

（９）ステップ８０８の確認で、２つのネットワークＰＩＮが同一であった場合、ステップ８０６の処理で取得した端末識別番号に対応した携帯電話テーブル３０８の項目にステップ８０５の処理で受信した分散暗号データＡを登録し、ここでの処理を終了する（ステップ８０９）。なお、携帯電話テーブル３０８で同一端末識別番号、同一ネットワークＰＩＮに対する別の分散暗号データＡ４０７が既に登録されていた場合であっても、同一端末識別番号、同一ネットワークＰＩＮに対して複数の分散暗号データＡ４０７を重ねて登録できるものとする。

【００４７】

（10）ステップ８０７の確認で、端末識別番号に対応したネットワークＰＩＮが携帯電話テーブル３０８の項目に設定されていなかった場合、ステップ８０６の処理で取得した端末識別番号に対応した携帯電話テーブル３０８の項目にステップ８０５で受信した分散暗号データＡとローカルＰＩＮとネットワークＰＩＮとを登録して、ここでの処理を終了する（ステップ８１１）。

【００４８】

図９は図８に示すステップ８０２の処理における暗号鍵の取得要求元が携帯電話機であることを確認する処理の動作を説明するフローチャートであり、次に、これについて説明する。

【００４９】

（１）はじめに、データ設定プログラム３０６、受信した要求から携帯電話機１０１の持つ端末識別番号２１０を取得できるか否かを確認し、取得することができなかった場合、ここでの処理を中止する（ステップ９０１、９０４）。

【００５０】

（２）ステップ９０１の確認で、受信した要求から携帯電話機１０１の持つ端末識別番号２１０を取得できた場合、暗号鍵の取得要求が携帯電話機より発信された可能性があるので、受信した要求の接続元のネットワークアドレスがキャリアＧＷテーブル３０９に登録されているか否かを確認し、登録されていなかった場合、ここでの処理を中止する（ステップ９０２、９０４）。

【００５１】
（３）ステップ９０２のに確認で、要求の接続元のネットワークアドレスがキャリアＧＷテーブル３０９に登録されていた場合、携帯電話会社からの接続であると判るので、処理を継続することとして、ステップ８０３の処理に進む（ステップ９０３）。
【００５２】
図１０は利用者が機密データの利用を行う際の携帯電話機１０１内のデータ利用プログラム２０７の処理動作を説明するフローチャートであり、次に、これについて説明する。
【００５３】
（１）携帯電話機１０１の利用者あるいはアプリケーションによる機密データへのアクセス要求が発生すると、データ利用プログラム２０７は、ローカルＰＩＮ情報２１３がメモリ２０２上にあるか否かを確認する（ステップ１００１、１００２）。
【００５４】
（２）ステップステップ１００２の確認で、ローカルＰＩＮ情報２１３がメモリ２０２上にあった場合、入力画面を表示して、利用者に、登録してあるローカルＰＩＮの情報を入力させて、入力させたＰＩＮ情報を取得する（ステップ１００３）。
【００５５】
（３）ステップ１００３の処理で取得したローカルＰＩＮとメモリ２０２内のローカルＰＩＮ情報２１３とが同一であるか否かを確認し、同一であった場合、メモリ２０２内の機密データ２１５へのアクセスを許可する（ステップ１００４、１００５）。
【００５６】
（４）ステップ１００２の確認で、ローカルＰＩＮ情報２１３がメモリ２０２上になかった場合、入力画面を表示して、利用者に、登録されているネットワークＰＩＮと新規ローカルＰＩＮとの情報を入力させて、入力させたこれらのＰＩＮ情報を取得する（ステップ１００６）。
【００５７】
（５）次に、ステップ１００６の処理で取得したネットワークＰＩＮとローカルＰＩＮとを認証サーバ１０２に送信して、ローカルＰＩＮの再設定と一時的に保持する情報の取得要求を行う（ステップ１００７）。
【００５８】
（６）ステップ１００７の処理での情報取得要求に対して、認証サーバ１０２から分散暗号データＡとローカルＰＩＮ情報と暗号鍵とが送信されてくるので、これらのデータを受信して、メモリ２０２上に保持する（ステップ１００８）。
【００５９】
（７）ステップ１００８の処理で受信した分散暗号データＡ２１２と、記憶部２０９に格納されている分散暗号データＢ２０８とから暗号化データを合成し、受信した暗号鍵２１４を利用して復号化し、平文形式の機密データ２１５を復元してメモリ２０２に格納し、メモリ２０２内の機密データ２１５へのアクセスを許可する（ステップ１００９、１００５）。
【００６０】
（８）ステップ１００４の確認で、入力されて取得したローカルＰＩＮとメモリ２０２内のローカルＰＩＮ情報２１３とが同一でなかった場合、ステップ１００４の確認の処理であるローカルＰＩＮの比較が、予め定めた回数以上、例えば、連続して４回以上失敗したか否かを確認する。なお、失敗した回数は、データ利用プログラム２０７によりカウントされ、メモリ２０２内に保持されている（ステップ１０１０）。
【００６１】
（９）ステップ１０１０の確認で、予め定めた回数以上失敗していなかった場合、ステップ１００３からの処理に戻り、再び、利用者にローカルＰＩＮの入力を要求して処理を繰り返し、予め定めた回数以上失敗していた場合、メモリ２０２内の分散暗号データＡ２１２とローカルＰＩＮ情報２１３と暗号鍵２１４と機密データ２１５を削除し、ステップ１００２からの処理に戻って処理を続ける（ステップ１０１１）。

【００６２】
図１１は図１０のステップ１００７での処理で送信されてきたＰＩＮ再設定と情報取得要求を認証サーバ１０２が受信したときのデータ認証プログラム３０７の処理動作を説明するフローチャートであり、次に、これについて説明する。
【００６３】
（１）認証サーバ１０２が携帯電話機１０１からネットワークＰＩＮとローカルＰＩＮとを含んだＰＩＮ再設定と情報要求を受信すると、データ認証プログラム３０７は、取得要求元が携帯電話機であることを確認する。この処理は、図９により説明した場合と同様に行われる（ステップ１１０１、１１０２）。
【００６４】
（２）ステップ１１０２の確認で、取得要求元が携帯電話機であることが確認できた場合、ステップ１１０２の処理で取得した端末識別番号に対応した携帯電話テーブル３０８の項目のロックアウトフラグ４０８が設定されていないか否かを確認し、ロックアウトフラグ４０８が設定されていた場合、ここでの処理を終了する（ステップ１１０３）。
【００６５】
（３）ステップ１１０３の確認で、ロックアウトフラグ４０８が設定されていなかった場合、ステップ１１０１の処理で受信したネットワークＰＩＮと、ステップ１１０２で取得した端末識別番号に対応した携帯電話テーブル３０８の項目のネットワークＰＩＮ４０５とが同一であるか否かを確認する（ステップ１１０４）。
【００６６】
（４）ステップ１１０４の確認で、ネットワークＰＩＮが同一であった場合、ステップ１１０１の処理で受信したローカルＰＩＮで、ステップ１１０２で取得した端末識別番号に対応した携帯電話テーブル３０８のローカルＰＩＮ４０４を書き換える（ステップ１１０５）。
【００６７】
（５）その後、ステップ１１０２の処理で取得した端末識別番号に対応した携帯電話テーブル３０８の分散暗号データＡ４０７とローカルＰＩＮ４０４とネットワークＰＩＮ４０５とを携帯電話機１０１に返信して、ここでの処理を終了する（１１０６）。
【００６８】
（６）ステップ１１０４の確認で、ネットワークＰＩＮが同一でなかった場合、ネットワークＰＩＮの比較を予め定めた所定の回数以上、例えば、連続１１回以上失敗したか否かを確認し、所定の回数以上失敗していた場合、ステップ１１０２で取得した端末識別番号に対応した携帯電話テーブル３０８のロックアウトフラグ４０８を設定する。なお、失敗した回数は、データ認証プログラム３０７によりカウントされ、メモリ３０２内に格納される。また、一旦、ロックアウトフラグ４０８が設定されると、このフラグ４０８は、認証サーバ１０２の管理者でなければ解除することができない（ステップ１１０７、１１０９）。
【００６９】
（７）ステップ１１０７の確認で、所定の回数以上失敗していなかった場合、または、ステップ１１０９の処理の後、携帯電話機１０１へエラーメッセージを返信して、ここでの処理を終了する（ステップ１１０８）。
【００７０】
前述した本発明の実施形態は、認証サーバの情報と携帯端末の情報との両方のデータを入手することができたときに、はじめて個人情報や機密情報を復元することができるようにしているので、機密情報を攻撃者に盗まれることがないように防御することができる。
【００７１】
前述した本発明の実施形態によれば、携帯電話機を紛失したり盗難にあったりした場合に、携帯電話機内部の個人情報や機密情報等を、携帯電話機利用者の認証のロックアウトのタイミングで消去することができ、また、携帯電話機のハードウェアを改造して、携帯電話機内部の個人情報や機密情報を取り出す攻撃に対しても、携帯電話機の電源ＯＦＦや

リセットのタイミングでこれら情報を消去して対応することができる。

【００７２】

前述した本発明の実施形態での各処理は、プログラムにより構成し、情報端末、認証サーバが備えるＣＰＵに実行させることができ、また、それらのプログラムは、ＦＤ、ＣＤ－ＲＯＭ、ＤＶＤ等の記録媒体に格納して提供することができ、また、ネットワークを介してディジタル情報により提供することができる。

【図面の簡単な説明】

【００７３】

【図１】本発明の一実施形態による情報漏洩防止システムを構築するネットワークシステムの構成を示す図である。

【図２】携帯電話機の構成を示すブロック図である。

【図３】認証サーバの構成を示すブロック図である。

【図４】携帯電話テーブルの構成を示す図である。

【図５】キャリアＧＷテーブルの構成を示す図である。

【図６】利用者が機密データの登録を行う際の携帯電話内のデータ登録プログラムの処理動作を説明するフローチャートである。

【図７】図６に示すステップ６０４の処理で暗号化した機密データを分割するイメージを説明する図である。

【図８】図６のステップ６０２の処理で暗号鍵の取得要求を受信した場合の認証サーバのデータ設定プログラムの処理動作を説明するフローチャートである。

【図９】図８に示すステップ８０２の処理における暗号鍵の取得要求元が携帯電話であることを確認する処理の動作を説明するフローチャートである。

【図１０】利用者が機密データの利用を行う際の携帯電話内のデータ利用プログラムの処理動作を説明するフローチャートである。

【図１１】図１０のステップ１００７での処理で送信されてきたＰＩＮ再設定と情報取得要求を認証サーバが受信したときのデータ認証プログラムの処理動作を説明するフローチャートである。

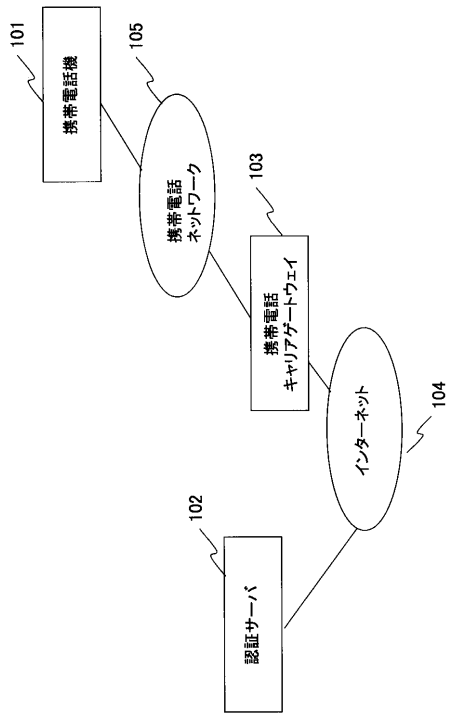
【符号の説明】

【００７４】

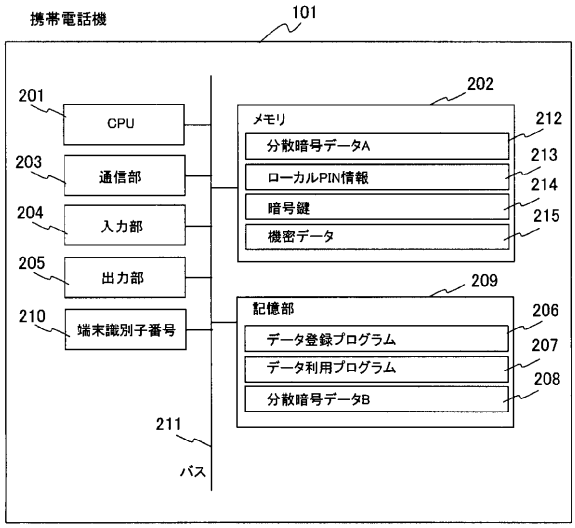
１０１　携帯電話機
１０２　認証サーバ
１０３　携帯電話キャリアゲートウェイ
１０４　インターネット
１０５　携帯電話ネットワーク
２０１、３０１　ＣＰＵ
２０２、３０２　メモリ
２０３、３０３　通信部
２０４、３０４　入力部
２０５、３０５　出力部
２０６　データ登録プログラム
２０７　データ利用プログラム
２０８　分散暗号データＢ
２０９、３１０　記憶部
２１０　端末識別子番号
２１１、３１１　バス
２１２　分散暗号データＡ
２１３　ローカルＰＩＮ情報
２１４　暗号鍵
２１５　機密データ
３０６　データ設定プログラム

３０７　データ認証プログラム
３０８　携帯電話機テーブル
３０９　キャリアＧＷテーブル

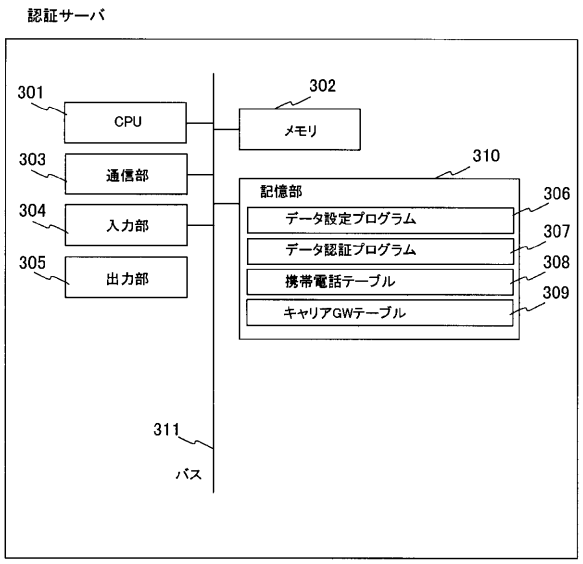
【図１】



【図２】



【図３】



【図４】

携帯電話テーブル 303

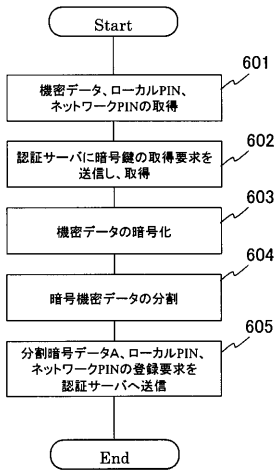
項番	登録端末番号	携帯電話キャリア	ローカルPIN	ネットワークPIN	暗号鍵	分散暗号データA	ロックアウト
1	12345678abcd	Docomo	1234	1234567890	aabbccddeeffgghh	8ay948qyd4i…	○
2	9876fedc5432	AU	5678	0123456789	aaabbbcccdddeeef	Ajha4 5qpaf8…	－
3	3579cccc2468	Vodafone	9012	1357902468	aaaabbbbccccdddd	9l48ka4jaq9d…	－

【図５】

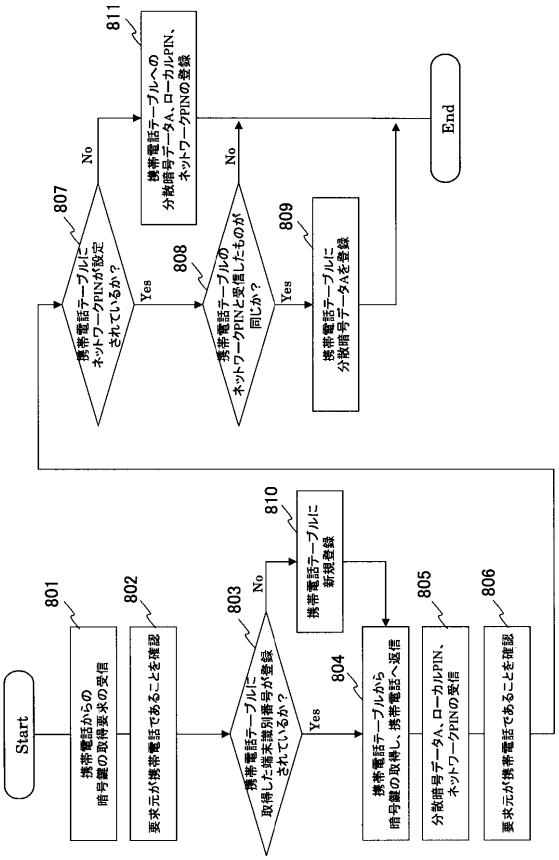
キャリアGWテーブル 304

項番	ゲートウェアアドレス	携帯電話キャリア
1	200.123.4.1	Docomo
2	230.98.7.1	AU
3	240.55.66.1	Vodafone

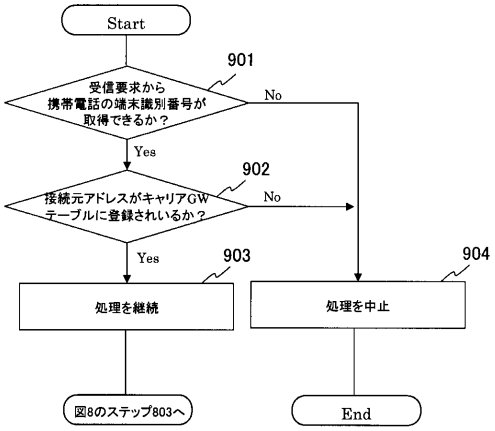
【図６】



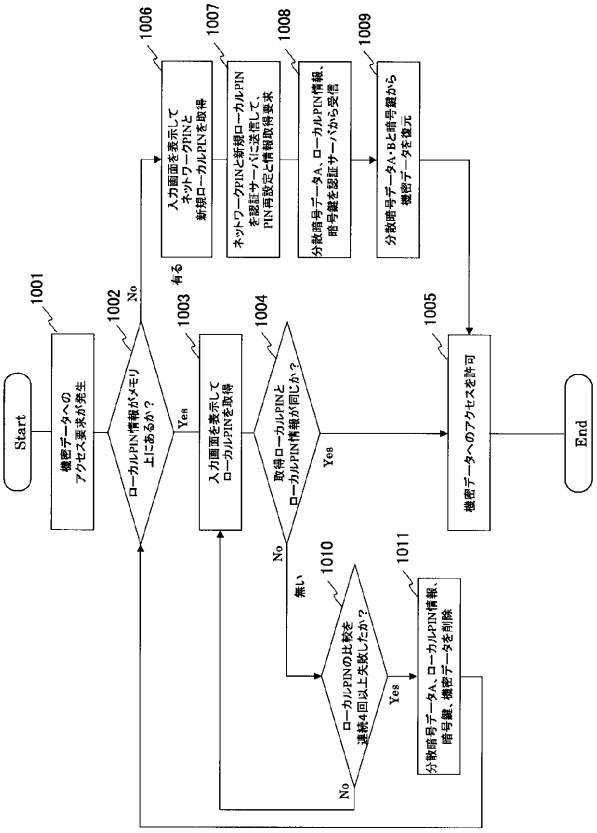
【図８】



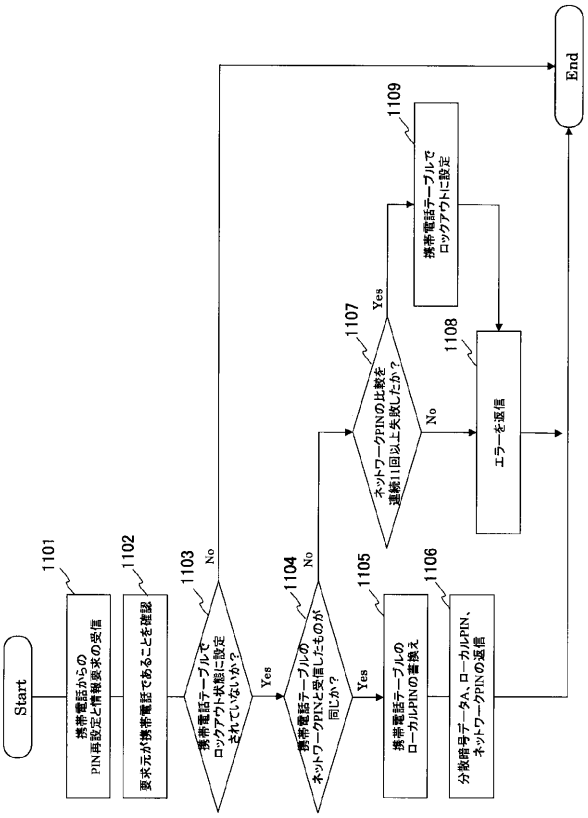
【図９】


Start
901
受信要求から
携帯電話の端末識別番号が
取得できるか？
No
Yes
902
接続元アドレスがキャリアGW
テーブルに登録されいるか？
No
Yes
903
処理を継続
904
処理を中止
図8のステップ803へ
End

【図１０】


Start
1001
機密データへの
アクセス要求が発生
1002
ローカルPIN情報がメモリ
上にあるか？
No
有る
1003
入力画面を表示して
ローカルPINを取得
Yes
1004
取得ローカルPINと
ローカルPIN情報が同じか？
Yes
No
無い
1005
機密データへのアクセスを許可
End
1006
入力画面を表示して
ネットワークPINと
新規ローカルPINを取得
1007
ネットワークPINと新規ローカルPIN
を認証サーバに送信して、
PIN再設定と情報取得要求
1008
分散暗号データA、ローカルPIN情報、
暗号鍵を認証サーバから受信
1009
分散暗号データA・Bと暗号鍵から
機密データを復元
1010
ローカルPINの比較を
連続4回以上失敗したか？
No
Yes
1011
分散暗号データA、ローカルPIN情報、
暗号鍵、機密データを削除

【図１１】


Start
1101
携帯電話からの
PIN再設定と情報要求の受信
1102
要求元が携帯電話であることを確認
1103
携帯電話テーブルで
ロックアウト状態に設定
されていないか？
No
Yes
1104
携帯電話テーブルの
ネットワークPINと受信したものが
同じか？
No
Yes
1105
携帯電話テーブルの
ローカルPINの書換え
1106
分散暗号データA、ローカルPIN、
ネットワークPINの返信
1107
ネットワークPINの比較を
連続11回以上失敗したか？
Yes
No
1108
エラーを返信
1109
携帯電話テーブルで
ロックアウトに設定
End

【図７】