(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2010-34911
(P2010-34911A)
(43)公開日　平成22年2月12日(2010.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
H04W 12/04	(2009.01)	H04L	9/00	601E	5K067
		H04Q	7/00	182	

審査請求 未請求　請求項の数 6　OL　（全 17 頁）

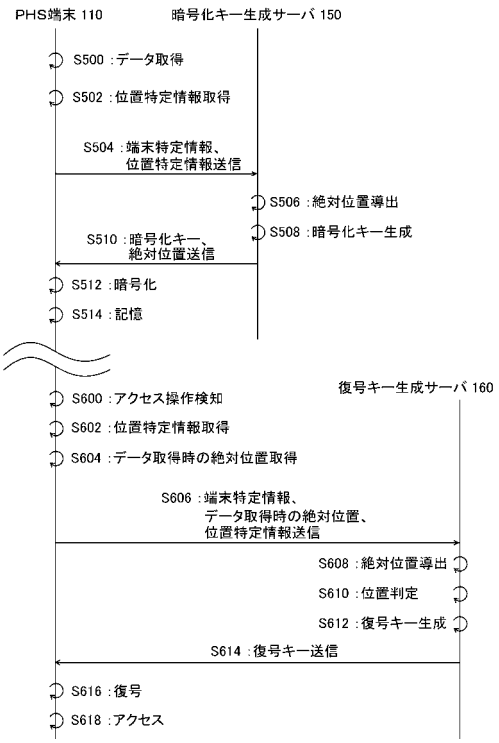
(21)出願番号　特願2008-195542 (P2008-195542)
(22)出願日　平成20年7月29日 (2008.7.29)

(71)出願人　000006633
京セラ株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　110000349
特許業務法人　アクア特許事務所
(72)発明者　是枝　稔明
神奈川県横浜市都筑区加賀原２丁目１番１号　京セラ株式会社横浜事業所内

Fターム(参考)　5J104 AA16　EA16　KA20　MA07　PA02
5K067 AA35　EE02　EE10

(54)【発明の名称】暗号化システム、携帯端末、復号キー生成サーバ、および暗号化方法

(57)【要約】　（修正有）
【課題】正規のユーザの利便性を確保しつつ、機密情報の保全をより容易かつ確実に遂行することが可能な暗号化システム、携帯端末、暗号化キー生成サーバ、復号キー生成サーバ、および暗号化方法を提供する。
【解決手段】暗号化システムでは、ＰＨＳ端末１１０がデータを取得すると、そのときの位置情報を取得して暗号化キー生成サーバ１５０から受信した端末固有の暗号化キーでデータを暗号化し、復号する際は、データを取得した際の位置情報と、復号するときの位置情報を復号キー生成サーバ１６０に送信し、２地点が所定の距離内であるときに復号キーを生成し復号できる。
【選択図】図８



【特許請求の範囲】
【請求項１】
携帯端末と、該携帯端末と通信可能な暗号化キー生成サーバと、該携帯端末と通信可能な復号キー生成サーバと、を含む暗号化システムであって、
前記携帯端末は、
テキスト、音声、または画像のうち少なくとも１つを含むデータを取得するデータ取得部と、
前記データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得する記憶位置取得部と、
当該携帯端末を特定する端末特定情報を前記暗号化キー生成サーバに送信する端末特定情報送信部と、
前記暗号化キー生成サーバから受信した暗号化キーを用いて前記取得されたデータを暗号化する暗号化部と、
暗号化したデータを前記位置特定情報に関連付けて記憶する端末記憶部と、
前記端末記憶部の前記データへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得するアクセス位置取得部と、
前記データ取得時およびアクセス時の位置特定情報と前記端末特定情報とを前記復号キー生成サーバに送信する位置特定情報送信部と、
前記復号キー生成サーバから受信した復号キーを用いて前記取得されたデータを復号する復号部と、
前記復号されたデータへのアクセスを実行させるアクセス実行部と、
を備え、
前記暗号化キー生成サーバは、
受信した前記端末特定情報から暗号化キーを生成する暗号化キー生成部と、
前記生成された暗号化キーを前記携帯端末に送信する暗号化キー送信部と、
を備え、
前記復号キー生成サーバは、
受信した前記データ取得時の位置情報とアクセス時の位置特定情報との距離が所定範囲以内である場合、復号キーを生成する復号キー生成部と、
前記生成された復号キーを前記携帯端末に送信する復号キー送信部と、
を備えることを特徴とする暗号化システム。
【請求項２】
前記位置特定情報は、ＧＰＳを用いた絶対位置であることを特徴とする請求項１に記載の暗号化システム。
【請求項３】
携帯端末と、該携帯端末と通信可能な暗号化キー生成サーバと、該携帯端末と通信可能な復号キー生成サーバと、を含む暗号化システムであって、
前記携帯端末は、
テキスト、音声、または画像のうち少なくとも１つを含むデータを取得するデータ取得部と、
前記データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得する記憶位置取得部と、
当該携帯端末を特定する端末特定情報とデータ取得時の位置特定情報とを前記暗号化キー生成サーバに送信する端末特定情報送信部と、
前記暗号化キー生成サーバから受信した暗号化キーを用いて前記取得されたデータを暗号化する暗号化部と、
前記暗号化したデータを前記暗号化キー生成サーバから受信したデータ取得時の絶対位置に関連付けて記憶する端末記憶部と、
前記端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得するアクセス位置取得部と、

前記データ取得時の絶対位置と前記アクセス時の位置特定情報と前記端末特定情報とを前記復号キー生成サーバに送信する位置特定情報送信部と、
前記復号キー生成サーバから受信した復号キーを用いて前記取得されたデータを復号する復号部と、
前記復号されたデータへのアクセスを実行させるアクセス実行部と、
を備え、
前記暗号化キー生成サーバは、
前記データ取得時の位置特定情報からデータ取得時の絶対位置を導出する暗号化位置導出部と、
受信した前記端末特定情報から暗号化キーを生成する暗号化キー生成部と、
前記生成された暗号化キーと前記絶対位置とを前記携帯端末に送信する暗号化キー送信部と、
を備え、
前記復号キー生成サーバは、
前記アクセス時の位置特定情報からアクセス時の絶対位置を導出する復号位置導出部と、
受信した前記データ取得時の絶対位置と前記復号位置導出部が導出したアクセス時の絶対位置との距離が所定範囲以内である場合、復号キーを生成する復号キー生成部と、
前記生成された復号キーを前記携帯端末に送信する復号キー送信部と、
を備えることを特徴とする暗号化システム。

【請求項４】
テキスト、音声、または画像のうち少なくとも１つを含むデータを取得するデータ取得部と、
前記データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得する記憶位置取得部と、
当該携帯端末を特定する端末特定情報を前記暗号化キー生成サーバに送信する端末特定情報送信部と、
暗号化キー生成サーバで前記端末特定情報に基づいて生成された暗号化キーを用いて前記取得されたデータを暗号化する暗号化部と、
暗号化したデータを前記位置特定情報に関連付けて記憶する端末記憶部と、
前記端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得するアクセス位置取得部と、
前記データ取得時およびアクセス時の位置特定情報と前記端末特定情報とを前記復号キー生成サーバに送信する位置特定情報送信部と、
前記復号キー生成サーバで前記データ取得時およびアクセス時の位置特定情報と前記端末特定情報とに基づいて生成された復号キーを用いて前記取得されたデータを復号する復号部と、
前記復号されたデータへのアクセスを実行させるアクセス実行部と、
を備えることを特徴とする携帯端末。

【請求項５】
携帯端末から受信した、該携帯端末におけるデータ取得時の位置情報とアクセス時の位置特定情報との距離が所定範囲以内である場合、復号キーを生成する復号キー生成部と、
前記生成された復号キーを前記携帯端末に送信する復号キー送信部と、
を備えることを特徴とする復号キー生成サーバ。

【請求項６】
携帯端末と、該携帯端末と通信可能な暗号化キー生成サーバと、該携帯端末と通信可能な復号キー生成サーバと、を含む暗号化方法であって、
前記携帯端末は、
テキスト、音声、または画像のうち少なくとも１つを含むデータを取得し、
前記データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得

し、
当該携帯端末を特定する端末特定情報を前記暗号化キー生成サーバに送信し、
前記暗号化キー生成サーバは、
受信した前記端末特定情報から暗号化キーを生成し、
前記生成された暗号化キーを前記携帯端末に送信し、
前記携帯端末は、
前記暗号化キー生成サーバから受信した暗号化キーを用いて前記取得されたデータを暗号化し、
暗号化したデータを前記位置特定情報に関連付けて記憶し、
前記端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得し、
前記データ取得時およびアクセス時の位置特定情報と前記端末特定情報とを前記復号キー生成サーバに送信し、
前記復号キー生成サーバは、
受信した前記データ取得時の位置情報とアクセス時の位置特定情報との距離が所定範囲に収まる場合、復号キーを生成し、
前記生成された復号キーを前記携帯端末に送信し、
前記携帯端末は、
前記復号キー生成サーバから受信した復号キーを用いて前記取得されたデータを復号し、
前記復号されたデータへのアクセスを実行させることを特徴とする暗号化方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、携帯端末内で暗号化されたデータを保持する暗号化システム、携帯端末、復号キー生成サーバ、および暗号化方法に関する。

【背景技術】

【０００２】

現在普及しているＰＨＳ（Personal Handyphone System）や携帯電話等の携帯端末は高機能化、小型化が進み、ほとんどの携帯端末には、静止画や動画等画像の撮像機能と撮像したデータを送受信する機能が設けられている。このため特別な別体の装置を用いることなく、だれもが画像や音声を記憶してその画像や音声を無線経由で送受信することが可能である。

【０００３】

さらに、ＵＳＢ（Universal Serial Bus）メモリやメモリカードなどの半導体記憶媒体やＨＤＤ（Hard Disk Drive）などの小型化、大容量化が進み、容量の大きな高画質の画像や動画も比較的小さな記憶媒体に保存できるようになった。

【０００４】

ところで製造会社の工場や研究施設などでは、生産ラインの品質管理や先端技術の研究結果などを記憶しておく必要があり、簡便な記憶装置として携帯性の高い上述した携帯端末が利用されることもある。また、このような施設では機密情報を扱うことが多く、機密漏えいを防止するため、機密情報が記憶されたこれらの携帯端末や、その携帯端末からデータを取り出し得る記憶媒体の管理が重要となっている。

【０００５】

そこで、不正利用を防止する為のデータの管理技術として、指定した期間を経過すると対象となるデータへアクセスできないようにして、デジタルコンテンツなどの使用期限を設定できる技術が公開されている（特許文献１）。

【０００６】

また、デジタルデータの制御技術として、複製元のデジタルコンテンツなどの情報に更新があると、通信網を介して自動的あるいは任意に差分データなどを送受信して自体の情

報を更新するシステムを低負荷で実現する技術も公開されている（特許文献２）。
【特許文献１】特開２００１－２６５６６２号公報
【特許文献２】特開２０００－３４７９６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかし、携帯端末に一旦生成および保存されてしまったデータを後からアクセス制限することはその実現性に乏しい。また、携帯端末の持ち出しを制限したとしても、アクセス制限される前にデータを記憶媒体へ複製すれば簡単に外部へ持ち出すことができる。さらに携帯端末は無線通信が可能なので、撮像後すぐにデータを送信してしまうと機密情報の漏洩先を特定することすらできなくなってしまう。
【０００８】
ここで、機密保持を徹底し携帯端末の機能を制限すると、不正目的ではない正規の業務で利便性が悪くなってしまう。
【０００９】
さらに、特許文献１にあるアクセス制限を行った場合、データへのアクセスを所定の期間内に制限することは可能であるが、工場や研究施設などの機密情報は永続的に保存する必要があるものも多く、所定の期間経過後にデータを参照したい正規のユーザがいても、アクセスすることができなくなってしまう。また所定の期間内であれば不正なアクセスも制限されず、そのデータを外部に持ち出すことが可能となる。従って、データの機密性を有効に保つことができない。
【００１０】
このような無体物である電子データは、一旦アクセス可能な状態になってしまうと、上述した従来技術を含め、その後の状態を完全に管理するのは困難を極める。そこで、アクセス可能な状態になる前に、何かしらの制限を加えることが望まれる。
【００１１】
本発明は、このような課題に鑑み、正規のユーザの利便性を確保しつつ、機密情報の保全をより容易かつ確実に遂行することが可能な暗号化システム、携帯端末、復号キー生成サーバ、および暗号化方法を提供することを目的としている。
【課題を解決するための手段】
【００１２】
上記課題を解決するために、本発明の代表的な構成は、携帯端末と、携帯端末と通信可能な暗号化キー生成サーバと、携帯端末と通信可能な復号キー生成サーバと、を含む暗号化システムであって、携帯端末は、テキスト、音声、または画像のうち少なくとも１つを含むデータを取得するデータ取得部と、データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得する記憶位置取得部と、携帯端末を特定する端末特定情報を暗号化キー生成サーバに送信する端末特定情報送信部と、暗号化キー生成サーバから受信した暗号化キーを用いて取得されたデータを暗号化する暗号化部と、暗号化したデータを位置特定情報に関連付けて記憶する端末記憶部と、端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得するアクセス位置取得部と、データ取得時およびアクセス時の位置特定情報と端末特定情報とを復号キー生成サーバに送信する位置特定情報送信部と、復号キー生成サーバから受信した復号キーを用いて取得されたデータを復号する復号部と、復号されたデータへのアクセスを実行させるアクセス実行部と、を備え、暗号化キー生成サーバは、受信した端末特定情報から暗号化キーを生成する暗号化キー生成部と、生成された暗号化キーを携帯端末に送信する暗号化キー送信部と、を備え、復号キー生成サーバは、受信したデータ取得時の位置情報とアクセス時の位置特定情報との距離が所定範囲以内である場合、復号キーを生成する復号キー生成部と、生成された復号キーを携帯端末に送信する復号キー送信部と、を備えることを特徴とする。
【００１３】

本発明において携帯端末は、暗号化キー生成サーバに暗号化キーを生成させ、その暗号化キーを使って取得したデータを暗号化してからはじめてそのデータを記憶する。従って、ユーザは、暗号化後のデータしか認識することができず、復号キーが無い限りそのデータを参照することができない。

【００１４】

また、復号キーは、復号キー生成サーバが、データ取得時とアクセス時の位置が近くであると判断した場合、すなわち、データを取得した位置の近くでデータにアクセスしようとしている場合にのみ発行されるので、そのデータを取得した位置を知らないまたはその位置に居ない不正な第三者は、暗号化されたデータを復号することができず、正規のユーザの利便性を確保しつつ、機密情報の保全をより容易かつ確実に遂行することが可能となる。

【００１５】

また、上記の位置特定情報は、ＧＰＳ（Global Positioning System）を用いた絶対位置であってもよい。

【００１６】

本発明では、データを復号するのに位置特定情報を要する。かかるＧＰＳを用いる構成により、新たな追加回路を伴うことなく、携帯端末に予め設けられているＧＰＳ機能を用いて低コストで容易に暗号化システムを構築することができる。

【００１７】

本発明の代表的な他の構成は、携帯端末と、携帯端末と通信可能な暗号化キー生成サーバと、携帯端末と通信可能な復号キー生成サーバと、を含む暗号化システムであって、携帯端末は、テキスト、音声、または画像のうち少なくとも１つを含むデータを取得するデータ取得部と、データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得する記憶位置取得部と、当該携帯端末を特定する端末特定情報とデータ取得時の位置特定情報とを暗号化キー生成サーバに送信する端末特定情報送信部と、暗号化キー生成サーバから受信した暗号化キーを用いて取得されたデータを暗号化する暗号化部と、暗号化したデータを暗号化キー生成サーバから受信したデータ取得時の絶対位置に関連付けて記憶する端末記憶部と、端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得するアクセス位置取得部と、データ取得時の絶対位置とアクセス時の位置特定情報と端末特定情報とを復号キー生成サーバに送信する位置特定情報送信部と、復号キー生成サーバから受信した復号キーを用いて取得されたデータを復号する復号部と、復号されたデータへのアクセスを実行させるアクセス実行部と、を備え、暗号化キー生成サーバは、データ取得時の位置特定情報からデータ取得時の絶対位置を導出する暗号化位置導出部と、受信した端末特定情報から暗号化キーを生成する暗号化キー生成部と、生成された暗号化キーと絶対位置とを携帯端末に送信する暗号化キー送信部と、を備え、復号キー生成サーバは、アクセス時の位置特定情報からアクセス時の絶対位置を導出する復号位置導出部と、受信したデータ取得時の絶対位置と復号位置導出部が導出したアクセス時の絶対位置との距離が所定範囲以内である場合、復号キーを生成する復号キー生成部と、生成された復号キーを携帯端末に送信する復号キー送信部と、を備えもよい。

【００１８】

本発明において、携帯端末が、データを記憶した時の絶対位置の導出を暗号化キー生成サーバが行う。またそのデータにアクセスしようとしたときの携帯端末の絶対位置の導出を、復号キー生成サーバが行う。かかる構成により、例えば携帯端末にデータを記憶したときの絶対位置を暗号化キー生成サーバで暗号化（または符号化）してから携帯端末に記憶させることができ、携帯端末の端末記憶部に記憶されているデータ取得時の絶対位置の不正な改竄を防止することが可能となる。また、データ取得時の絶対位置を不正に取得され、その場所へ直接訪れデータにアクセスされる危険を回避できる。

【００１９】

本発明の携帯端末の代表的な構成は、テキスト、音声、または画像のうち少なくとも１

つを含むデータを取得するデータ取得部と、データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得する記憶位置取得部と、当該携帯端末を特定する端末特定情報を暗号化キー生成サーバに送信する端末特定情報送信部と、暗号化キー生成サーバで端末特定情報に基づいて生成された暗号化キーを用いて取得されたデータを暗号化する暗号化部と、暗号化したデータを位置特定情報に関連付けて記憶する端末記憶部と、端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得するアクセス位置取得部と、データ取得時およびアクセス時の位置特定情報と端末特定情報とを復号キー生成サーバに送信する位置特定情報送信部と、復号キー生成サーバでデータ取得時およびアクセス時の位置特定情報と端末特定情報とに基づいて生成された復号キーを用いて取得されたデータを復号する復号部と、復号されたデータへのアクセスを実行させるアクセス実行部と、を備えてもよい。

【００２０】

本発明の復号キー生成サーバの代表的な構成は、携帯端末から受信した、携帯端末におけるデータ取得時の位置情報とアクセス時の位置特定情報との距離が所定範囲以内である場合、復号キーを生成する復号キー生成部と、生成された復号キーを携帯端末に送信する復号キー送信部と、を備えることを特徴とする。

【００２１】

本発明にかかる代表的な他の構成は、携帯端末と、携帯端末と通信可能な暗号化キー生成サーバと、携帯端末と通信可能な復号キー生成サーバと、を含む暗号化方法であって、携帯端末は、テキスト、音声、または画像のうち少なくとも１つを含むデータを取得し、データを取得したときの当該携帯端末の位置を特定するための位置特定情報を取得し、当該携帯端末を特定する端末特定情報を暗号化キー生成サーバに送信し、暗号化キー生成サーバは、受信した端末特定情報から暗号化キーを生成し、生成された暗号化キーを携帯端末に送信し、携帯端末は、暗号化キー生成サーバから受信した暗号化キーを用いて取得されたデータを暗号化し、暗号化したデータを位置特定情報に関連付けて記憶し、端末記憶部のデータへのアクセスを検知すると、当該携帯端末の位置を特定するための位置特定情報を取得し、データ取得時およびアクセス時の位置特定情報と端末特定情報とを復号キー生成サーバに送信し、復号キー生成サーバは、受信したデータ取得時の位置情報とアクセス時の位置特定情報との距離が所定範囲以内である場合、復号キーを生成し、生成された復号キーを携帯端末に送信し、携帯端末は、復号キー生成サーバから受信した復号キーを用いて取得されたデータを復号し、復号されたデータへのアクセスを実行させることを特徴とする。

【００２２】

上述した暗号化システムにおける技術的思想に対応する構成要素やその説明は、当該携帯端末、復号キー生成サーバ、および暗号化方法にも適用可能である。

【発明の効果】

【００２３】

以上説明したように本発明によれば、ユーザの利便性を確保しつつ、機密情報の保全をより容易かつ確実に遂行することが可能となる。

【発明を実施するための最良の形態】

【００２４】

以下に添付図面を参照しながら、本発明の好適な実施形態について詳細に説明する。かかる実施形態に示す寸法、材料、その他具体的な数値などは、発明の理解を容易とするための例示にすぎず、特に断る場合を除き、本発明を限定するものではない。なお、本明細書及び図面において、実質的に同一の機能、構成を有する要素については、同一の符号を付することにより重複説明を省略し、また本発明に直接関係のない要素は図示を省略する。

【００２５】

ＰＨＳ端末や携帯電話等に代表される携帯端末は、所定の場所に設置されている基地局と無線により通信を実行する無線通信システムを構築する。このような無線通信システム

において、携帯端末は、静止画や動画等画像の撮像機能と撮像したデータを基地局を通じて様々なサーバに送受信する機能が設けられている。

【００２６】

携帯端末は、その優れた携帯性から機密情報等データの取得に用いられることもあるが、その取得されたデータの漏洩を防ぐのは容易ではない。そこで本実施形態では、正規のユーザの利便性を確保しつつ、機密情報の保全をより容易かつ確実に遂行する暗号化システムを提供する。ここでは、理解を容易にするため暗号化システム全体を説明し、その後、携帯端末、暗号化キー生成サーバ、および復号キー生成サーバの具体的構成、暗号化方法と、復号方法を説明する。

【００２７】

また、ここでは、携帯端末としてＰＨＳ端末を挙げているが、かかる場合に限らず、携帯電話、ノート型パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）、デジタルカメラ、音楽プレイヤー、カーナビゲーション、ポータブルテレビ、ゲーム機器、ＤＶＤプレイヤー、リモートコントローラ等無線通信可能な様々な電子機器を携帯端末として用いることもできる。

【００２８】

（暗号化システム１００）

図１は、暗号化システム１００の概略的な接続関係を示した説明図である。当該暗号化システム１００は、ＰＨＳ端末１１０と、基地局１２０と、ＩＳＤＮ(Integrated Services Digital Network)回線、インターネット、専用回線等で構成される通信網１３０と、中継サーバ１４０と、暗号化キー生成サーバ１５０と、復号キー生成サーバ１６０を含んで構成される。

【００２９】

本実施形態の暗号化システム１００では、例えばユーザが自身のＰＨＳ端末１１０を用いてデータを取得すると、その取得したデータはそのまま保持されず、暗号化を通じて初めてデータとして認識することができる。従って、ユーザは、復号キーが無い限りそのデータを参照することができない。また、復号キーは、復号する位置に関する所定の条件を満足した場合にのみ提供される。従って、その条件を知らないまたはその条件を満足できない不正な第三者は、暗号化されたデータを復号することができない。

【００３０】

当該暗号化システム１００において暗号化キーを生成するのが暗号化キー生成サーバ１５０であり、復号キーを生成するのが復号キー生成サーバ１６０である。ＰＨＳ端末１１０は、基地局１２０および通信網１３０を通じて、かかる暗号化キー生成サーバ１５０と、復号キー生成サーバ１６０にアクセスし、自体が取得したデータを保全する。

【００３１】

（ＰＨＳ端末１１０）

このような暗号化システム１００におけるＰＨＳ端末１１０の具体的な構成について以下に記述する。

【００３２】

図２は、ＰＨＳ端末１１０のハードウェア構成を示したブロック図であり、図３はＰＨＳ端末１１０の外観を示した斜視図である。ＰＨＳ端末１１０は端末制御部２００、端末記憶部２０２、表示部２０４、操作部２０６、音声入力部２０８、音声出力部２１０、撮像部２１２、端末無線通信部２１４とを含んで構成される。

【００３３】

端末制御部２００は中央処理装置（ＣＰＵ）を含む半導体集積回路によりＰＨＳ端末１１０全体を管理および制御する。また、端末制御部２００は、端末記憶部２０２のプログラムを用いて、通話機能、メール送受信機能、撮像機能、音楽再生機能、Ｗｅｂ閲覧機能、ＴＶ視聴機能も遂行する。

【００３４】

さらに、端末制御部２００は、データ取得部２５０、暗号化部２５２、復号部２５４、

アクセス実行部２５６としても機能する。

【００３５】

データ取得部２５０は、操作部２０６から入力されたテキストやメモ、音声入力部２０８から入力された音声信号、または撮像部２１２から入力された画像信号などのデータを取得する。また、データ取得部２５０のデータ取得手段は、上述した操作部２０６、音声入力部２０８、撮像部２１２に限らず、例えば、デジタルカメラ、デジタルビデオカメラ、ボイスレコーダ等の外部装置を用いて生成されたデータをＵＳＢ接続等を介して取得することもできる。

【００３６】

暗号化部２５２は、データ取得部２５０が取得したデータを、暗号化キー生成サーバ１５０から取得した暗号化キーを用いて暗号化する。かかる暗号化が完了するまで、ユーザは取得したデータにアクセスすることができない。なお、本実施形態においては、暗号化方式は限定せず、様々な暗号化方式を適用することができる。

【００３７】

復号部２５４は、復号キー生成サーバ１６０から取得した復号キーを用いて、アクセス要求のあった、暗号化されたデータを復号する。

【００３８】

アクセス実行部２５６は、復号部２５４によって復号されたデータへのアクセスを実行する。例えば画像データへのアクセスであれば、復号された画像データを表示部２０４に表示させ、ユーザはその画像データの編集や削除が可能となる。

【００３９】

端末記憶部２０２は、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、不揮発性ＲＡＭ、フラッシュメモリ、ＨＤＤ等で構成され、端末制御部２００で処理されるプログラムや音声データ、さらには暗号化部２５２で暗号化されたデータや、取得位置テーブル２５８も記憶する。

【００４０】

図４は、取得位置テーブル２５８を説明するための説明図である。

【００４１】

取得位置テーブル２５８において、暗号化部２５２で暗号化されたデータＡ、Ｂはそれぞれデータ取得時の絶対位置（緯度Ｘ１、経度Ｙ１）、（Ｘ２、Ｙ２）に関連付けられて記憶されている。

【００４２】

また、データ取得時の絶対位置は、データと同様暗号化された状態で記憶しておくこともできる。そうすることで、不正な第三者が、ＰＨＳ端末１１０を入手した際に端末記憶部２０２に記憶されている取得位置テーブル２５８を参照して、その絶対位置でデータを取得したり、その絶対位置を改竄して不正な位置でデータを取得したりするのを回避できる。

【００４３】

また、端末記憶部２０２は、一時記憶部２６０としても機能する。一時記憶部２６０は、データ取得部２５０が取得したデータをアクセス不能な状態で一時的に記憶し、データが正常に暗号化された後、その暗号化されたデータを正式に端末記憶部２０２に記憶する。そして、一時記憶部２６０は、暗号化前のデータを自体の保存領域から削除する。また、暗号化途中で電源が切られるなど、暗号化が正しく行われないような動作が検知されると、自動的に取得したデータを消去する。かかる構成により、不正にデータを取得しようとするユーザが、暗号化前のデータを取り出す事態を回避できる。

【００４４】

表示部２０４は、液晶ディスプレイ、有機ＥＬ(Electro Luminescence)ディスプレイ等で構成され、端末記憶部２０２に記憶された、または通信網１３０を介してサーバ（図示せず）から提供される、ＷｅｂコンテンツやアプリケーションのＧＵＩ（Graphical User Interface）を表示することができる。

【００４５】

操作部２０６は、キーボード、十字キー、ジョイスティック等から構成され、ユーザの操作入力を受け付ける。また、当該ＰＨＳ端末１１０がテキスト、音声、または画像などのデータの記憶装置として機能する場合、記憶操作を、操作部２０６を通じて直接行うことができる。

【００４６】

音声入力部２０８は、マイク等の音声認識手段で構成され、通話時等に入力されたユーザの音声をＰＨＳ端末１１０内で処理可能な電気信号に変換する。

【００４７】

音声出力部２１０は、スピーカで構成され、ＰＨＳ端末１１０で受信した通話相手の音声信号を音声に変えて出力する。また、着信音や、操作部２０６の操作音、アラーム音等も出力できる。

【００４８】

撮像部２１２は、ＣＣＤ（Charge Coupled Device）やＣＭＯＳ（Complementary Metal Oxide Semiconductor）等の映像素子で構成されており、静止画や動画等画像を撮像できる。

【００４９】

端末無線通信部２１４は、基地局１２０との無線通信を行う。このような無線通信としては、基地局１２０内でフレームを時分割した複数のタイムスロットをそれぞれのＰＨＳ端末１１０のチャネルに割り当てて通信を行う時分割多重方式（ＴＤＭＡ：Time Division Multiple Access）等が採用されている。

【００５０】

また、端末無線通信部２１４は、記憶位置取得部２６２、端末特定情報送信部２６４、アクセス位置取得部２６６、位置特定情報送信部２６８としても機能する。

【００５１】

記憶位置取得部２６２は、データ取得部２５０がデータを取得した際、当該ＰＨＳ端末１１０の位置を特定するための位置特定情報を取得する。具体的には、オープンサーチで近辺の基地局のＣＳＩＤ（基地局識別番号：Cell Station IDentifier）や基地局毎のＲＳＳＩ（受信信号強度：Received Signal Strength Indicator）などを取得する。

【００５２】

端末特定情報送信部２６４は、ＰＨＳ端末１１０を特定する端末特定情報と、記憶位置取得部２６２が取得したデータ取得時の位置特定情報とを暗号化キー生成サーバ１５０に送信する。

【００５３】

アクセス位置取得部２６６は、ユーザがＰＨＳ端末１１０のデータにアクセスしようとした際、当該ＰＨＳ端末１１０の位置を特定するための位置特定情報を取得する。記憶位置取得部２６２と同様、オープンサーチで付近の基地局のＣＳＩＤや基地局毎のＲＳＳＩなどを取得する。かかるアクセス位置取得部２６６は、記憶位置取得部２６２と機能が等しいので一体的に構成することもできる。

【００５４】

位置特定情報送信部２６８は、暗号化されたデータに関連付けられているデータ取得時の絶対位置と、アクセス位置取得部２６６が取得したアクセス時の位置特定情報と、ＰＨＳ端末１１０の端末特定情報とを復号キー生成サーバ１６０に送信する。

【００５５】

（暗号化キー生成サーバ１５０）

続いて暗号化キー生成サーバ１５０の構成について記述する。

【００５６】

図５は、暗号化キー生成サーバ１５０のハードウェア構成を示したブロック図である。暗号化キー生成サーバ１５０は、暗号化記憶部３００と、暗号化制御部３０２と、暗号化有線通信部３０４とを含んで構成される。

【００５７】

暗号化記憶部３００は、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、不揮発性ＲＡＭ、フラッシュメモリ、ＨＤＤ等で構成され、暗号化キー生成サーバ１５０で処理されるプログラムや基地局位置テーブル３５０を記憶している。

【００５８】

図６は、基地局位置テーブル３５０の説明図である。基地局位置テーブル３５０では、基地局１２０固有のＣＳＩＤ　Ｃ、Ｄと、基地局１２０の絶対位置（緯度Ｘ３、経度Ｙ３）、（Ｘ４、Ｙ４）とが対応付けられている。このテーブルを参照することで、当該暗号化キー生成サーバ１５０は、ＰＨＳ端末１１０がオープンサーチで取得したＣＳＩＤの基地局１２０の絶対位置を特定することが可能となる。

【００５９】

当該基地局位置テーブル３５０は、基地局１２０の新設、撤去に対応して、常に最新の情報を有していることが望ましいが、後述する理由により、必ずしも常に最新でなくともよい。

【００６０】

暗号化制御部３０２は、中央処理装置（ＣＰＵ）を含む半導体集積回路により暗号化キー生成サーバ１５０全体を管理および制御する。さらに、暗号化制御部３０２は、暗号化位置導出部３５２と、暗号化キー生成部３５４としても機能する。

【００６１】

暗号化位置導出部３５２は、ＰＨＳ端末１１０から送信された位置特定情報（ＣＳＩＤとＲＳＳＩ）から、ＰＨＳ端末１１０がデータを取得した絶対位置を導出する。暗号化位置導出部３５２は、上述の基地局位置テーブル３５０を参照し、ＰＨＳ端末１１０から送られてきたＣＳＩＤの基地局１２０の絶対位置を特定する。さらに、ＲＳＳＩの強さは概ね基地局１２０からの距離に比例するため、基地局１２０の絶対位置を中心とした同心円上にＰＨＳ端末１１０があることとなり、ＰＨＳ端末１１０のデータ取得時の位置を推定できる。

【００６２】

また、ＰＨＳ端末１１０はオープンサーチで複数のＣＳＩＤ、ＲＳＳＩを取得し送信するため、暗号化位置導出部３５２は基地局１２０を中心とした複数の同心円を導出でき、その同心円同士の交点がもっとも集中した位置を、ＰＨＳ端末１１０のデータ取得時の絶対位置とすることで、絶対位置導出の精度を高めることができる。

【００６３】

このように、絶対位置の導出には複数のＣＳＩＤを用いるため、仮に基地局位置テーブル３５０が最新のデータに更新されておらず、基地局位置テーブル３５０に記憶されていない基地局１２０のＣＳＩＤが送信されてきても、暗号化位置導出部３５２は、そのＣＳＩＤを参考にせず他のＣＳＩＤとＲＳＳＩから絶対位置を導出することで、暗号化システム１００を正常に機能させることができる。

【００６４】

同様に、基地局位置テーブル３５０に記載されているＣＳＩＤの基地局１２０が撤去されたとしても、ＰＨＳ端末１１０から同ＣＳＩＤが送信されてくることはなく、その基地局１２０の位置情報は参照されることはないため、暗号化システム１００には影響が無い。

【００６５】

かかる構成により、複数のＣＳＩＤとＲＳＳＩを用いてデータ取得時のＰＨＳ端末１１０の絶対位置を導出する方法を用いることで、暗号化キー生成サーバ１５０と後述する復号キー生成サーバ１６０の基地局位置テーブル３５０は常に最新情報である必要は無く、管理が容易である。

【００６６】

さらに、暗号化キー生成サーバ１５０において、データ取得時の絶対位置を導出させずに、ＰＨＳ端末１１０から送信されてきたＣＳＩＤとＲＳＳＩのデータの組み合わせをそのまま位置の照合に利用してもよい。暗号化キー生成サーバ１５０には絶対位置導出のた

めのプログラムや回路などを搭載する必要が無く、より簡便で高速なシステムを実現できる。

【００６７】

暗号化有線通信部３０４は、通信網１３０と接続し、ＰＨＳ端末１１０から位置特定情報と、端末特定情報を受信する。また、暗号化有線通信部３０４は、暗号化キー送信部３５６としても機能し、暗号化キー生成部が生成した暗号化キーをＰＨＳ端末１１０へ送信する。

【００６８】

（復号キー生成サーバ１６０）

続いて復号キー生成サーバ１６０の構成について記述する。

【００６９】

図７は、復号キー生成サーバ１６０のハードウェア構成を示したブロック図である。復号キー生成サーバ１６０は、復号記憶部４００と、復号制御部４０２と、復号有線通信部４０４とを含んで構成される。

【００７０】

復号記憶部４００は、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、不揮発性ＲＡＭ、フラッシュメモリ、ＨＤＤ等で構成され、復号キー生成サーバ１６０で処理されるプログラムや基地局位置テーブル３５０を記憶する。かかる基地局位置テーブル３５０は、暗号化キー生成サーバ１５０の基地局位置テーブル３５０と所定の頻度で同期がとられている。

【００７１】

復号制御部４０２は、中央処理装置（ＣＰＵ）を含む半導体集積回路により復号キー生成サーバ１６０全体を管理および制御する。さらに、復号制御部４０２は、復号位置導出部４５２と、復号キー生成部４５４としても機能する。

【００７２】

復号位置導出部４５２は、前述上述の暗号化位置導出部３５２と同様の方法で、上述の基地局位置テーブル３５０を参照し、ＰＨＳ端末１１０から送られてきたＣＳＩＤやＲＳＳＩなどの位置特定情報を元にＰＨＳ端末１１０がデータにアクセスしようとしている絶対位置を導出する。

【００７３】

復号キー生成部４５４は、復号位置導出部４５２が導出した、データへのアクセス時の絶対位置とＰＨＳ端末１１０が送信してきたデータ取得時の絶対位置とを比較し、２地点が所定の距離内にある場合、例えば、同一の会社内であると判断できる場合に、ＰＨＳ端末１１０が送信してきた端末特定情報を元に復号キーを生成する。このとき、２地点が所定の距離よりも離れていた場合、不正なアクセスとみなして復号キー生成部４５４は復号キーを生成しない。こうして、ユーザはデータを取得した位置に行かない限りデータへはアクセスできない。

【００７４】

復号有線通信部４０４は、通信網１３０と接続し、ＰＨＳ端末１１０からデータ取得時の絶対位置と、データアクセス時の位置特定情報と、端末特定情報を受信する。また、復号有線通信部４０４は、復号キー送信部４５６としても機能し、復号キー生成部が生成した復号キーをＰＨＳ端末１１０へ送信する。

【００７５】

（暗号化および復号化方法）

図８は、本実施形態にかかる暗号化および復号化方法の流れを示したシーケンス図である。

【００７６】

ＰＨＳ端末１１０のデータ取得部２５０がデータを取得すると（Ｓ５００）、記憶位置取得部２６２がオープンサーチを行い位置特定情報（ＣＳＩＤやＲＳＳＩ）を取得する（Ｓ５０２）。そして取得した位置特定情報と、端末特定情報とを暗号化キー生成サーバ１５０に送信する（Ｓ５０４）。

【００７７】
暗号化キー生成サーバ１５０の暗号化位置導出部３５２は、受信した位置特定情報からデータを取得した絶対位置を導出し（Ｓ５０６）、端末特定情報から暗号化キーを生成する（Ｓ５０８）。そして生成した暗号化キーとデータ取得時の絶対位置をＰＨＳ端末１１０に送信する（Ｓ５１０）。
【００７８】
ＰＨＳ端末１１０の暗号化部２５２は、受信した暗号化キーを用いて取得したデータを暗号化する（Ｓ５１２）。そして、暗号化したデータを、データ取得時の絶対位置に関連付けて端末記憶部２０２に記憶する（Ｓ５１４）。
【００７９】
このように、ＰＨＳ端末１１０は、暗号化キー生成サーバ１５０にＰＨＳ端末１１０を特定する端末特定情報を元に暗号化キーを生成させ、その暗号化キーを使って対象の情報を暗号化してから記憶する。従って、ユーザは、暗号化後のデータしか認識することができず、復号キーが無い限りそのデータを参照することができない。
【００８０】
続いて復号方法について記述する。ＰＨＳ端末１１０は、暗号化されたデータへのアクセスを検知すると（Ｓ６００）、オープンサーチして位置特定情報（ＣＳＩＤやＲＳＳＩ）を取得し（Ｓ６０２）、さらに取得位置テーブル２５８を参照してアクセスされたデータに対応するデータ取得時の絶対位置を取得し（Ｓ６０４）、端末特定情報や位置特定情報と共に復号キー生成サーバ１６０に送信する（Ｓ６０６）。
【００８１】
復号キー生成サーバ１６０は、受信した位置特定情報からデータへのアクセス時の絶対位置を導出し（Ｓ６０８）、受信したデータ取得時の絶対位置と比較して２地点が所定の距離内に位置しているかどうか判定する（Ｓ６１０）。所定の距離内であれば、端末特定情報から復号キーを生成し（Ｓ６１２）、ＰＨＳ端末１１０へ送信する（Ｓ６１４）。
【００８２】
ＰＨＳ端末１１０の復号部２５４は、受信した復号キーを用いてアクセス対象の暗号化されたデータを復号し（Ｓ６１６）、アクセス実行部２５６がデータへアクセスする（Ｓ６１８）。
【００８３】
この復号方法を用いることで、復号キーは、復号キー生成サーバ１６０が、データ取得時とアクセス時の位置が近くであると判断した場合、すなわち、データを取得した位置の近くでデータにアクセスしようとしていると判断した場合にのみ発行されるので、そのデータを取得した位置を知らないまたは位置に居ない不正な第三者は、暗号化されたデータを復号することができず、正規のユーザの利便性を確保しつつ、機密情報の保全をより容易かつ確実に遂行することが可能となる。
【００８４】
上述したＣＳＩＤとＲＳＳＩを用いた絶対位置の導出方法は、後述するＧＰＳを用いた導出方法とは異なり、建物に遮られても電波を受信可能なため屋内でも利用可能である。そのため本実施形態は、例えば、工場や研究所など機密情報を扱う施設で効果的に利用できる。
【００８５】
（他の実施形態）
上述した実施形態では、データ取得時の位置や暗号化データへのアクセス時の位置を特定するために、位置特定情報としてＣＳＩＤやＲＳＳＩを用いた。しかし、ＧＰＳを使ってデータ取得時の絶対位置や、暗号化されたデータへのアクセス時の絶対位置を特定してもよい。
【００８６】
図９は、他の実施形態におけるＰＨＳ端末７１０のハードウェア構成を示したブロック図である。図２と異なり、ＰＨＳ端末７１０はＧＰＳアンテナ部７１２を備えている。Ｇ

ＰＳアンテナ部７１２は、ＧＰＳ衛星７５０から放出されるＧＰＳ信号を受信する。

【００８７】

記憶位置取得部２６２は、データ取得時に位置特定情報として上述のＣＳＩＤやＲＳＳＩを取得する代わりにＧＰＳアンテナ部７１２からＧＰＳ信号を取得し絶対位置を導出する。

【００８８】

また、暗号化キー生成サーバ１５０における暗号化位置導出部３５２と、復号キー生成サーバ１６０における復号位置導出部４５２は、本実施形態においては不要となる。

【００８９】

以下に、本実施形態における暗号化および復号化方法を記述する。上述の実施形態との相違点について主に説明する。

【００９０】

ＰＨＳ端末７１０は、データ取得時にＧＰＳアンテナ部７１２においてＧＰＳ信号を受信し、記憶位置取得部２６２はその信号を元にデータ取得時の絶対位置を導出する。導出した絶対位置は、暗号化キー生成サーバ１５０へ送信せず、暗号化されたデータに関連付けられる。

【００９１】

ユーザが暗号化されたデータへアクセスしたとき、アクセス位置取得部２６６は、同様にＧＰＳアンテナ部７１２からＧＰＳ信号を取得してアクセス時の絶対位置を導出する。復号キー生成サーバ１６０は、ＰＨＳ端末７１０から受信したデータ取得時とアクセス時の絶対位置を比較して、所定の距離内にある場合のみ復号キーを生成してＰＨＳ端末７１０へ送信する。

【００９２】

かかる構成により、ＰＨＳ端末１１０に予め設けられたＧＰＳを使うことで低コスト化を図ることができ、さらに、絶対位置を導出するための暗号化キー生成サーバ１５０および復号キー生成サーバ１６０とＰＨＳ端末７１０と間の通信を要さないため、高速な暗号化システムを構築することができる。

【００９３】

さらに、セキュリティを高めるために、データ取得時の絶対位置を取得位置テーブル２５８に記憶する際、暗号化（符号化）してもよい。そうすることで、不正な第三者が、データ取得時の絶対位置を端末記憶部から抽出して、その場所へ直接訪れデータにアクセスしてしまう事態を回避できる。

【００９４】

以上、添付図面を参照しながら本発明の好適な実施形態について説明したが、本発明はかかる実施形態に限定されないことは言うまでもない。当業者であれば、特許請求の範囲に記載された範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【００９５】

例えば、上述した実施形態においては、暗号化キー生成サーバ１５０がデータ取得時の絶対位置導出を行わず、ＰＨＳ端末１１０は位置特定情報のままデータに関連付けて記憶しておいてもよい。この場合、データへのアクセス時には、絶対位置に変換されていない位置特定情報を送信し、復号キー生成サーバ１６０がデータ取得時およびアクセス時の両絶対位置を導出し、上述の位置判定を行う。かかる構成により、暗号化キー生成サーバ１５０は暗号化位置導出部を設けないで済む。

【００９６】

また、暗号化キー生成サーバ１５０と復号キー生成サーバ１６０を一体形成し、両サーバの機能を同一のサーバに実現させることもできる。かかる構成により、共通の回路やデータを共有化できるので、コストの低減を図ることができる。

【００９７】

なお、本明細書の暗号化方法における各工程は、必ずしもシーケンス図として記載され

た順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むとしても良い。

【産業上の利用可能性】

【００９８】

本発明は、携帯端末内で暗号化されたデータを保持する暗号化システム、携帯端末、復号キー生成サーバ、および暗号化方法に利用することができる。

【図面の簡単な説明】

【００９９】

【図１】暗号化システムの概略的な接続関係を示した説明図である。

【図２】ＰＨＳ端末のハードウェア構成を示したブロック図である。

【図３】ＰＨＳ端末の外観を示した斜視図である。

【図４】暗号化したデータとそのデータ取得時の絶対位置を関連付けた取得位置テーブルの説明図である。

【図５】暗号化キー生成サーバのハードウェア構成を示したブロック図である。

【図６】基地局位置テーブルの説明図である。

【図７】復号キー生成サーバのハードウェア構成を示したブロック図である。

【図８】本実施形態にかかる暗号化および復号化方法の流れを示したシーケンス図である。

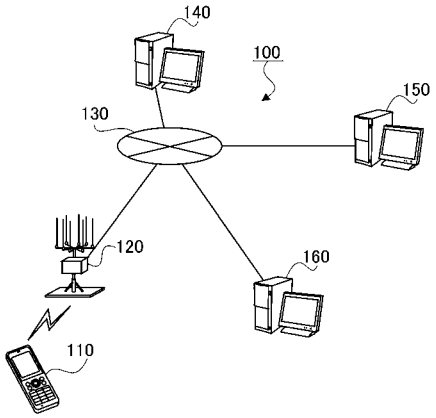
【図９】他の実施形態におけるＰＨＳ端末のハードウェア構成を示したブロック図である。

【符号の説明】

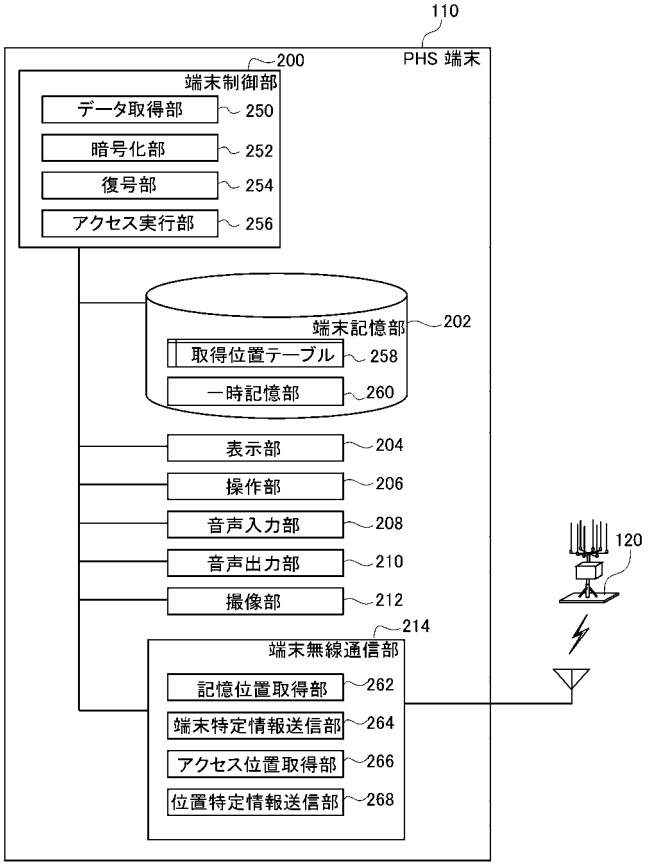
【０１００】

１００　…暗号化システム
１１０　…ＰＨＳ端末
１５０　…暗号化キー生成サーバ
１６０　…復号キー生成サーバ
２０２　…端末記憶部
２５０　…データ取得部
２５２　…暗号化部
２５４　…復号部
２５６　…アクセス実行部
２５８　…取得位置テーブル
２６２　…記憶位置取得部
２６４　…端末特定情報送信部
２６６　…アクセス位置取得部
２６８　…位置特定情報送信部
３５２　…暗号化位置導出部
３５４　…暗号化キー生成部
３５６　…暗号化キー送信部
４５２　…復号位置導出部
４５４　…復号キー生成部
４５６　…復号キー送信部

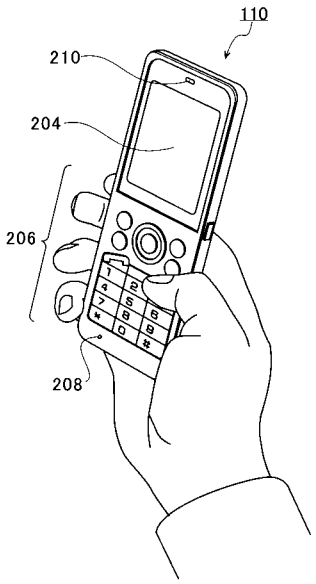
【図１】



【図２】



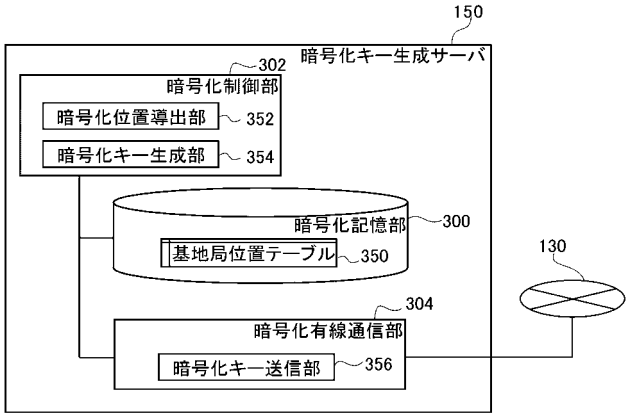
【図３】



【図４】

データ	データ取得時の絶対位置（緯度，経度）
A	X1，Y1
B	X2，Y2
⋮	⋮

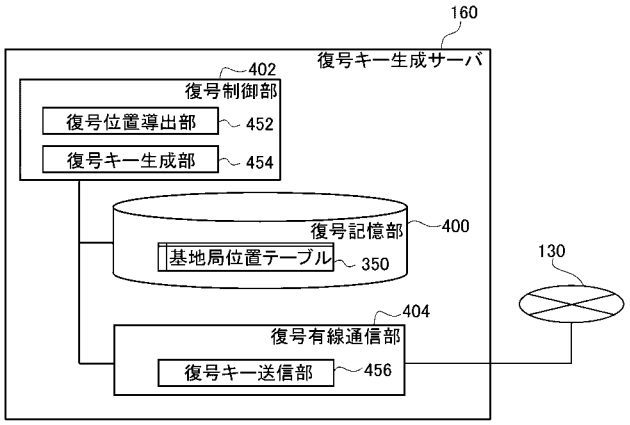
【図５】



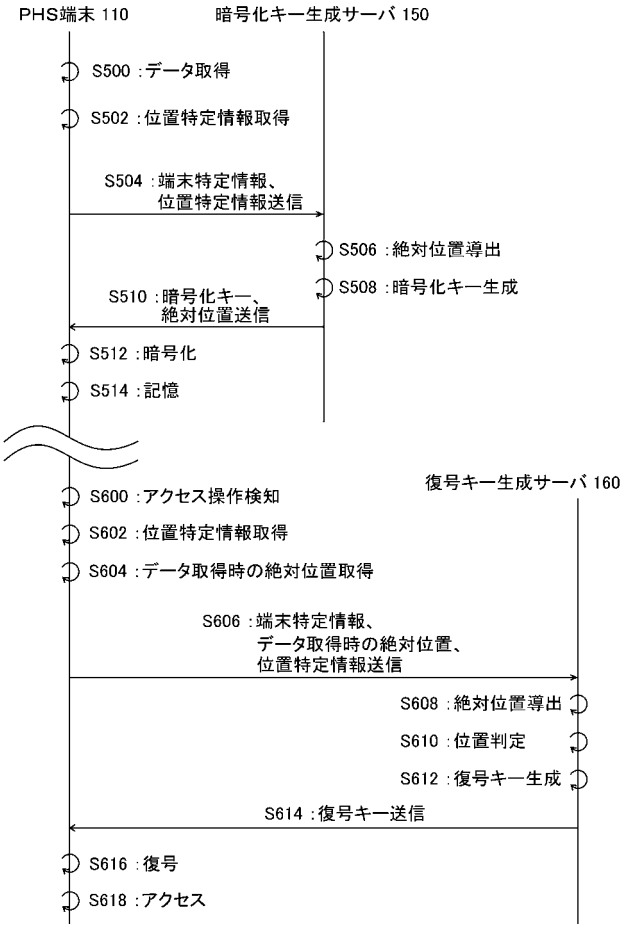
【図６】

CSID	絶対位置（緯度，経度）
C	X3，Y3
D	X4，Y4
⋮	⋮

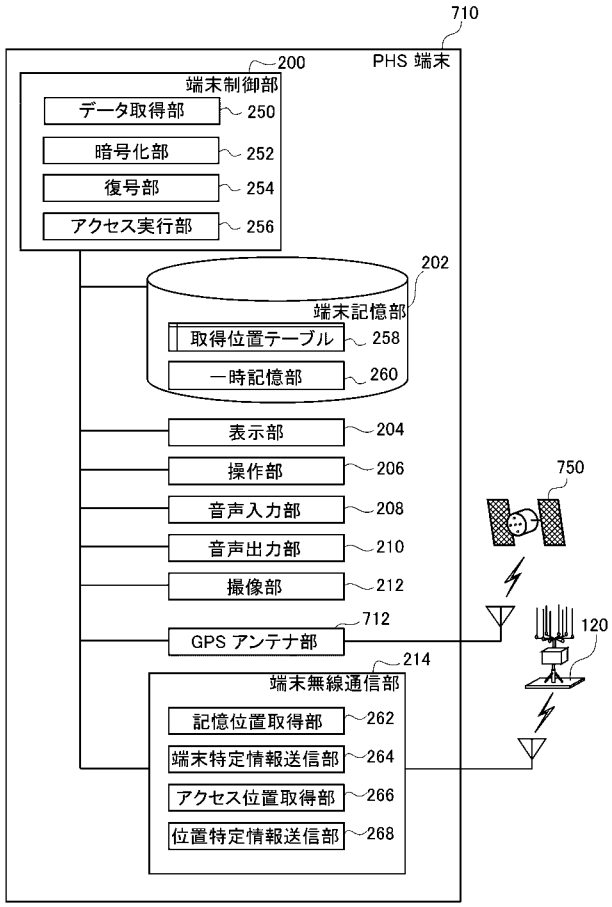
【図７】


160
復号キー生成サーバ
402
復号制御部
復号位置導出部
452
復号キー生成部
454
復号記憶部
400
基地局位置テーブル
350
130
404
復号有線通信部
復号キー送信部
456

【図８】


PHS端末 110
暗号化キー生成サーバ 150
S500 :データ取得
S502 :位置特定情報取得
S504 :端末特定情報、
位置特定情報送信
S506 :絶対位置導出
S508 :暗号化キー生成
S510 :暗号化キー、
絶対位置送信
S512 :暗号化
S514 :記憶
復号キー生成サーバ 160
S600 :アクセス操作検知
S602 :位置特定情報取得
S604 :データ取得時の絶対位置取得
S606 :端末特定情報、
データ取得時の絶対位置、
位置特定情報送信
S608 :絶対位置導出
S610 :位置判定
S612 :復号キー生成
S614 :復号キー送信
S616 :復号
S618 :アクセス

【図９】


710
PHS 端末
200
端末制御部
データ取得部
250
暗号化部
252
復号部
254
アクセス実行部
256
202
端末記憶部
取得位置テーブル
258
一時記憶部
260
表示部
204
操作部
206
音声入力部
208
音声出力部
210
撮像部
212
712
GPS アンテナ部
214
端末無線通信部
記憶位置取得部
262
端末特定情報送信部
264
アクセス位置取得部
266
位置特定情報送信部
268
750
120