(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6520004号
(P6520004)
(45)発行日　令和1年5月29日(2019.5.29)　(24)登録日　令和1年5月10日(2019.5.10)

(51)Int.Cl.		F I		
G08B 25/10	(2006.01)	G08B	25/10	D
G08B 25/04	(2006.01)	G08B	25/04	K
G08G 1/09	(2006.01)	G08G	1/09	F

請求項の数 8　(全 27 頁)

(21)出願番号　特願2014-153034(P2014-153034)
(22)出願日　平成26年7月28日(2014.7.28)
(65)公開番号　特開2016-31596(P2016-31596A)
(43)公開日　平成28年3月7日(2016.3.7)
審査請求日　平成29年4月6日(2017.4.6)

(73)特許権者　318012780
富士通コネクテッドテクノロジーズ株式会社
神奈川県川崎市中原区上小田中四丁目１番１号
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(74)代理人　100175190
弁理士　大竹　裕明
(72)発明者　岩渕　裕輝
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】携帯型情報処理装置、情報処理方法、及び情報処理プログラム

(57)【特許請求の範囲】
【請求項１】
ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　ＩＤｅｎｔｉｆｉｃａｔｉｏｎ）リーダ／ライタと、
前記ＲＦＩＤリーダ／ライタに、ＲＦタグを探索させる探索制御部と、
前記ＲＦＩＤリーダ／ライタに、検出されたＲＦタグに対して、自装置の通過記録情報を書き込ませる書込制御部と、
前記ＲＦＩＤリーダ／ライタに、前記検出されたＲＦタグが保持する複数の通過記録情報を読み出させる読出制御部と、
前記複数の通過記録情報から１つを削除し、前記自装置の通過記録情報を追加して、複数の通過記録情報を編集する編集部と、
を備え、
前記書込制御部は、前記ＲＦＩＤリーダ／ライタに、前記編集部によって編集された前記複数の通過記録情報を前記検出されたＲＦタグに対して書き込ませる、
携帯型情報処理装置。
【請求項２】
前記編集部は、前記ＲＦタグから読み出された前記複数の通過記録情報から最も古い通過記録情報の１つを削除する、
請求項１に記載の携帯型情報処理装置。
【請求項３】

前記編集部によって編集された前記複数の通過記録情報をサーバに送信する送信部、
をさらに備える請求項１又は２に記載の携帯型情報処理装置。
【請求項４】
前記通過記録情報は、自装置の識別情報と、通過日時とを含む、
請求項１から３のいずれか一項に記載の携帯型情報処理装置。
【請求項５】
前記通過記録情報を、記録装置内のセキュア領域において暗号化する暗号化処理部をさらに備え、
前記書込制御部は、前記ＲＦＩＤリーダ／ライタに、前記検出されたＲＦタグに対して、暗号化された通過記録情報を書き込ませる、
請求項１から４のいずれか一項に記載の携帯型情報処理装置。
【請求項６】
暗号化された通過記録情報を記憶する記憶部をさらに備え、
前記編集部は、前記検出されたＲＦタグから読み出された暗号化されている複数の通過記録情報に、前記暗号化処理部によって暗号化された自装置の通過記録情報を追加して編集し、
前記記憶部は、前記編集部によって編集された前記複数の通過記録情報を記憶する、
請求項５に記載の携帯型情報処理装置。
【請求項７】
ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　ＩＤｅｎｔｉｆｉｃａｔｉｏｎ）リーダ／ライタを備える携帯型情報処理装置が、
前記ＲＦＩＤリーダ／ライタに、ＲＦタグを探索させ、
前記ＲＦＩＤリーダ／ライタに、検出されたＲＦタグに対して、自装置の通過記録情報を書き込ませ、
前記ＲＦＩＤリーダ／ライタに、前記検出されたＲＦタグが保持する複数の通過記録情報を読み出させ、
前記複数の通過記録情報から１つを削除し、前記自装置の通過記録情報を追加して、複数の通過記録情報を編集し、
前記自装置の通過記録情報の書込みにおいて、前記ＲＦＩＤリーダ／ライタに、前記編集された前記複数の通過記録情報を前記検出されたＲＦタグに対して書き込ませる、
情報処理方法。
【請求項８】
ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　ＩＤｅｎｔｉｆｉｃａｔｉｏｎ）リーダ／ライタを備える携帯型情報処理装置に、
前記ＲＦＩＤリーダ／ライタのＲＦタグの探索を制御させ、
前記ＲＦＩＤリーダ／ライタの、検出されたＲＦタグへの自装置の通過記録情報の書き込みを制御させ、
前記ＲＦＩＤリーダ／ライタの、前記検出されたＲＦタグが保持する複数の通過記録情報の読み出しを制御させ、
前記複数の通過記録情報から１つを削除し、前記自装置の通過記録情報を追加して、複数の通過記録情報を編集させ、
前記自装置の通過記録情報の書込みの制御において、前記ＲＦＩＤリーダ／ライタに、前記編集された前記複数の通過記録情報を前記検出されたＲＦタグに対して書き込ませる、
ための情報処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、携帯型情報処理装置、情報処理方法、及び情報処理プログラムに関する。
【背景技術】

【０００２】
行方不明者の捜索では、目撃情報、キャッシュカードの利用履歴、携帯電話等の位置登録情報、ＧＰＳ（Global Positioning System）の位置情報等の点情報が、捜索者の主観により結び付けられて線情報が取得され、捜索の方向性が決められることが多い。捜索者の主観によって点情報を結び付けて線情報が取得される場合には、点情報が多い場合や捜索者の主観が行方不明者の行動性と合っているという条件下では、発見確率が高くなる。
【０００３】
捜索者の主観と行方不明者との行動性が合うかどうかは、捜索者の経験に依存するところが大きい。一方で、点情報は客観的情報であるため、点情報は多ければ多いほど、行方不明者の発見確率を上げることができる。例えば、行方不明者の携帯電話端末の、携帯電話網の位置登録データベース内の位置情報や、ＧＰＳの位置情報を登録するデータベース内の位置情報等のネットワークを利用して記録された位置情報は、多く存在する場合が多く、有効である。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００１－３３８３８５号公報
【特許文献２】特開２００８－２７６７０３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、携帯電話網の位置登録データベースへの位置情報の記録やＧＰＳの位置情報のデータベースへの記録等のネットワークを利用して位置情報が記録される方法では、例えば、震災等でネットワークが利用できなくなった場合には、位置情報を残すことができない。そのため、行方不明者の捜索に用いられる点情報が少なくなり、行方不明者の発見確率を上げることが難しい場合があった。
【０００６】
本発明の一態様は、ネットワークが利用できない場合でも通過記録情報を残すことができる携帯型情報処理装置、情報処理方法、及び情報処理プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明の態様の一つは、
ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　ＩＤｅｎｔｉｆｉｃａｔｉｏｎ）リーダ／ライタと、
前記ＲＦＩＤリーダ／ライタに、ＲＦタグを探索させる探索制御部と、
前記ＲＦＩＤリーダ／ライタに、検出されたＲＦタグに対して、自装置の通過記録情報を書き込ませる書込制御部と、
を備える携帯型情報処理装置である。
【発明の効果】
【０００８】
開示の携帯型情報処理装置、情報処理方法、及び情報処理プログラムによれば、ネットワークが利用できない場合でも、通過記録情報を残すことができる。
【図面の簡単な説明】
【０００９】
【図１】第１実施形態に係る移動履歴検索システムの構成の一例を示す図である。
【図２】携帯端末とＩＣタグとのハードウェア構成の一例を示す図である。
【図３】サーバのハードウェア構成の一例である。
【図４】携帯端末のメモリのメモリマップの一例である。
【図５】移動履歴検索システム内の各装置の機能構成の一例を示す図である。

【図６】移動履歴検索アプリケーションを実行する場合の携帯端末の機能構成の一例である。
【図７】携帯端末の通過記録アプリケーションの処理のフローチャートの一例である。
【図８】アクセスＩＤ取得処理のフローチャートの一例である。
【図９】通過履歴情報受信処理のフローチャートの一例である。
【図１０】通過履歴ネットワーク送信処理のフローチャートである。
【図１１】格納サーバに対して移動履歴検索処理が行われる場合の移動履歴検索アプリケーションの処理のフローチャートの一例である。
【図１２】ＩＣタグに対して移動履歴検索処理が行われる場合の移動履歴検索アプリケーションの通過履歴情報受信処理のフローチャートの一例である。
【図１３】格納サーバの処理のフローチャートの一例である。
【図１４】格納サーバによる通過履歴情報読出処理のフローチャートの一例である。
【図１５】格納サーバによる通過履歴情報格納処理のフローチャートの一例である。
【図１６】ＩＣタグの処理のフローチャートの一例を示す図である。
【図１７】携帯端末による通過記録アプリケーションの実行時の処理のシーケンスの一例を示す図である。
【図１８】捜索者端末によるサーバに対する移動履歴検索アプリケーションの実行時の処理のシーケンスの一例を示す図である。
【図１９】捜索者端末によるＩＣタグに対する移動履歴検索アプリケーションの実行時の処理のシーケンスの一例を示す図である。
【図２０】第１実施形態における移動履歴検索システムの作用効果の一例を示す図である。
【図２１】ＧＰＳを利用したオートトラッキングによる位置情報の記録処理と、第１実施形態における携帯端末の通過記録アプリケーションによる位置情報の記録処理との消費電流の比較の一例である。
【発明を実施するための形態】
【００１０】
以下、図面に基づいて、本発明の実施の形態を説明する。以下の実施形態の構成は例示であり、本発明は実施形態の構成に限定されない。
【００１１】
＜第１実施形態＞
近年、国土地理院によって設置される基準点には、ＩＣタグが埋め込まれ、位置情報や識別番号等を該ＩＣタグから読み出せるものが増えてきている。基準点は、ある地点での位置情報を記録するためのものであり、石製やコンクリート製の杭状のものである。ＩＣタグが埋め込まれている基準点をインテリジェント基準点とも言う。
【００１２】
第１実施形態では、携帯型情報処理装置は、基準点等に設置されたＩＣタグを利用し、自身の通過記録情報を該ＩＣタグに書き込むことによって、携帯電話網やＧＰＳ等のネットワークが利用できない場合でも移動履歴を残す。通過記録情報は、例えば、自装置の識別情報、通過日時等である。自装置の識別情報には、例えば、電話番号、電子メールアドレス、個体識別番号等がある。
【００１３】
図１は、第１実施形態に係る移動履歴検索システムの構成の一例を示す図である。移動履歴検索システム１００は、携帯端末１と、複数のＩＣタグ２と、サーバ３とを含む。携帯端末１は、ＩＣタグリーダライタを備えているものとする。ＩＣタグ２は、例えば、基準点等の位置識別点、建物のゲート、壁、ドア、アクセスポイント等に設置されている。
【００１４】
携帯端末１は、ＩＣタグ２を検出すると、ＩＣタグ２から通過履歴情報を読み出す。通過履歴情報は、ＩＣタグ２の近傍を通過した携帯端末１の通過記録の履歴情報である。ＩＣタグのメモリ容量は、数キロバイト～数１００キロバイト程度であることが多く、その

場合、ＩＣタグに記録可能な通過履歴情報の件数は、１００～２００件程度である。そのため、第１実施形態では、携帯端末１は、読み出した通過履歴情報のうち、例えば、最も古い一件を削除し、自装置の通過記録情報を追加して、ＩＣタグ２に書き戻す。これによって、ＩＣタグ２のメモリ容量が小さい場合でも、携帯端末１の通過記録情報をＩＣタグ２に残すことができる。

【００１５】

また、第１実施形態では、携帯端末１は、ＩＣタグ２から読み出した通過履歴情報をサーバ３に送信する。これによって、ＩＣタグ２に保持される通過履歴情報がサーバ３に格納されるため、ＩＣタグ２のメモリ容量が少ない場合でも、通過履歴情報が失われずに済む。また、サーバ３に各ＩＣタグ２に保持される通過履歴情報が集約されるので、サーバ３を利用することによって、所望の携帯端末１の移動履歴を効率よく検索するこができる。

【００１６】

図２は、携帯端末１とＩＣタグ２とのハードウェア構成の一例を示す図である。携帯端末１は、例えば、携帯電話端末、スマートフォン、タブレット端末等、ＩＣタグリーダライタを備える装置等である。第１実施形態では、携帯端末１は、携帯電話端末であることを想定する。

【００１７】

携帯端末１は、ＣＰＵ（Central Processing Unit）１０１、メモリ１０２、ＩＣタグアンテナ１０３、ＩＣタグリーダライタ１０４、無線回路１０５、アンテナ１０６を備える。

【００１８】

ＩＣタグリーダライタ１０４及びＩＣタグアンテナ１０３は、電磁誘導方式、電波方式のいずれに対応するものであってもよい。電磁誘導方式では、交信範囲は、数十ｃｍである。電波方式では、交信範囲は、数ｍである。第１実施形態では、ＩＣタグリーダライタ１０４、ＩＣタグアンテナ１０３は、交信範囲の広い電波方式に対応するものであるとする。

【００１９】

ＩＣタグリーダライタ１０４は、所定の周波数の電波を所定周期で所定時間継続して発信し、該周波数の無線信号を受信することにより、該無線信号の発信元であるＩＣタグ２が交信範囲内に存在することを検出する。例えば、ＩＣタグリーダライタ１０４は、７秒に１回の周期で、０．２秒間、所定の周波数の電波を発信する。以降、ＩＣタグリーダライタ１０４がＩＣタグ２を検出するために所定の周波数の電波を発信することを、「電波を照射する」ともいう。

【００２０】

また、ＩＣタグリーダライタ１０４がリーダ又はライタのいずれで動作するのかは、照射される電波によって通知される情報に含まれている。ＩＣタグリーダライタ１０４は、ＩＣタグ２から受信した無線信号を電気信号に変換し、該電気信号を変換してデータを取得する。ＩＣタグリーダライタ１０４によって取得されたデータは、ＣＰＵ　１０１に出力される。

【００２１】

無線回路１０５は、アンテナ１０６と接続しており、アンテナ１０６を通じて受信した無線信号を電気信号に変換してＣＰＵ　１０１に出力したり、ＣＰＵ　１０１から入力される電気信号を無線信号に変換してアンテナ１０６を通じて送信したりする。無線回路１０５は、無線通信に係る処理を行い、例えば、第３世代移動通信システム，第２世代移動通信システム，ＬＴＥ（Long Term Evolution）等の無線通信方式のうちのいずれか１つ又は複数の方式に則った通信の処理を行う。

【００２２】

メモリ１０２は、例えば、ＲＡＭ（Random Access Memory）である。メモリ１０２は、ＲＯＭ（Read Only Memory）を含んでもよい。ＲＡＭには、揮発性のものと不揮発性のも

のと、双方が含まれる。不揮発性のＲＡＭには、ＯＳ（Operating System）や様々なアプリケーションプログラムが格納されている。揮発性のＲＡＭは、例えば、ＳＤＲＡＭ（Synchronous Dynamic RAM）等である。揮発性のＲＡＭは、作業領域、バッファ等の一時的な記憶領域等に用いられる。

【００２３】

ＣＰＵ　１０１は、メモリ１０２に格納されるプログラムをＲＡＭの作業領域に展開し、展開された命令を実行することによって様々な処理を行う。ＣＰＵ　１０１は、例えば、ＩＣタグリーダライタ１０４、無線回路１０５、のいずれかからの入力を受ける。ＣＰＵ　１０１は、入力を受けると、所定プログラム又はアプリケーションに則った処理を実行し、処理の結果を、例えば、メモリ１０２、ＩＣタグリーダライタ１０４、無線回路１０５のいずれかへ出力する。

【００２４】

なお、携帯端末１のハードウェア構成は、図２に示されるものに限定されず、適宜、追加、置換、削除等の変更が可能である。例えば、携帯端末１は、図２に示される構成に加えて、ディスプレイ、タッチパネル、スピーカ、マイクロフォン、カメラ等を備えていてもよい。携帯端末１は、「携帯型情報処理装置」の一例である。

【００２５】

ＩＣタグ２は、携帯端末１のＩＣタグリーダライタ１０４、ＩＣタグアンテナ１０３の方式と同じ方式のものとする。したがって、第１実施形態では、ＩＣタグ２は、電波方式のＩＣタグ２とする。ＩＣタグ２は、ＣＰＵ　２０１、メモリ２０２、アンテナ２０３を含む。ＩＣタグ２は、第１実施形態では、パッシブ型のＩＣタグであって、電源を備えない。ただし、これに限られず、ＩＣタグ２は電源を備えるアクティブ型であってもよい。

【００２６】

アンテナ２０３がＩＣタグアンテナ１０３によって照射された電波を受信すると、アンテナ２０３に磁界が発生して電流が流れ、ＣＰＵ　２０１が起動する。ＣＰＵ　２０１は、アンテナ２０３を通じて受信するデータに従って、メモリ２０２に格納されるデータの読出し又はメモリ２０２へのデータの書き込みを行う。

【００２７】

メモリ２０２は、例えば、ＥＥＰ－ＲＯＭ（Electrically Erasable Programmable-ROM）、Ｆｅ　ＲＡＭ（Ferroelectric Random Access Memory）である。

【００２８】

図３は、サーバ３のハードウェア構成の一例である。サーバ３は、例えば、移動履歴検索システム１００を提供する業者のネットワーク内に設置されている。サーバ３は、例えば、所定のキャリアの無線基地局及びＬＡＮ（Local Area Network）を通じて、携帯端末１からのデータを受信する。サーバ３は、例えば、汎用又は専用のコンピュータである。

【００２９】

サーバ３は、ＣＰＵ　３０１、データストレージ３０２、ＬＡＮ装置３０３を含む。データストレージ３０２は、例えば、ＨＤＤ（Hard Disk Drive）である。ＬＡＮ装置３０３は、ＬＡＮに接続されており、該ＬＡＮを通じて無線基地局に接続している。

【００３０】

図４は、携帯端末１のメモリ１０２のメモリマップの一例である。メモリ１０２は、不揮発性のＲＡＭと揮発性のＲＡＭとを含む。不揮発性のＲＡＭには、セキュアＯＳ、通過記録アプリケーション１１、移動履歴検索アプリケーション１２、通過記録情報１３が格納される。

【００３１】

セキュアＯＳは、情報を保護するための処理を行うＯＳである。セキュアＯＳは、暗号化／復号モジュール１４を含む。暗号化／復号モジュール１４は、後述のセキュアキー１６を用いて暗号化又は復号を行うためのモジュールである。通過履歴情報は、例えば、電話番号等の個人情報を含むため、ユーザがアクセス可能な範囲では、暗号化された状態で保存される。

【００３２】
通過記録アプリケーション１１及び移動履歴検索アプリケーション１２は、カーネル上で動作するアプリケーションである。通過記録アプリケーション１１は、携帯端末１がＩＣタグ２から通過履歴情報を読み出し、通過記録情報を追加し、通過履歴情報をＩＣタグ２に書き込み、通過履歴情報を格納サーバ３に送信するためのアプリケーションである。移動履歴検索アプリケーション１２は、指定される携帯端末１の移動履歴を検索するためのアプリケーションである。通過記録アプリケーション１１は、「情報処理プログラム」の一例である。
【００３３】
なお、携帯端末１は、通過記録アプリケーション１１と移動履歴検索アプリケーション１２との両方を保持していなくてもよい。通過記録アプリケーション１１を保持する装置と、移動履歴検索アプリケーション１２を保持する装置とは、別であってもよい。例えば、通過記録アプリケーション１１は、所定の通信キャリアと契約する携帯端末、又は、所定のメーカの携帯端末に搭載される。例えば、移動履歴検索アプリケーション１２は、警察関係者等の捜索において個人情報を閲覧することを認められている者が使用する携帯端末１やＰＣに搭載される。
【００３４】
通過記録情報１３は、通過記録アプリケーション１１によってＩＣタグ２から読み出されて、編集された、暗号化済みの通過履歴情報である。通過記録情報１３を格納する不揮発性ＲＡＭは、「記憶部」の一例である。
【００３５】
揮発性のＲＡＭは、セキュア領域を含む。セキュア領域は、セキュアＯＳがアクセス可能な領域であって、通常のＯＳやアプリケーションはアクセスできない領域である。そのため、セキュア領域には、ユーザ操作によるアクセスを回避したい、セキュリティ性の高い情報が格納される。
【００３６】
セキュア領域には、固有情報１５、セキュアキー１６が格納されている。固有情報１５は、携帯端末１に固有に割り当てられた識別番号（ＩＭＥＩ：International Mobile Equipment Identity）である。セキュアキー１６は、通過記録情報及び通過履歴情報の暗号化及び復号に用いられるキーである。
【００３７】
固有情報１５、セキュアキー１６は、工場出荷時に暗号化された状態で不揮発性メモリに格納されている。固有情報１５、セキュアキー１６は、携帯端末１の起動処理の一つとして、又は、通過記録アプリケーション１１及び移動履歴検索アプリケーション１２の起動によって、復号されて、セキュア領域に格納される。これによって、通過履歴情報の暗号化又は復号処理をより迅速に行うことができる。セキュア領域には、暗号化及び復号処理のための作業領域１７も設けられる。
【００３８】
図５は、移動履歴検索システム１００内の各装置の機能構成の一例を示す図である。図５に示される例では、移動履歴検索システム１００は、サーバとして、認証サーバ４、格納サーバ３を含む。格納サーバ３は、携帯端末１によってＩＣタグ２から読み出される通過履歴情報を蓄積、格納するサーバである。認証サーバ４は、携帯端末１に対して、アクセスＩＤを発行するサーバである。認証サーバ４のハードウェア構成は、格納サーバ３と同様である。なお、認証サーバ４と格納サーバ３とは、別々の装置であることに限られず、１つの装置が認証サーバ４と格納サーバ３として動作してもよい。
【００３９】
図５に示される例は、携帯端末１が通過記録アプリケーション１１を実行する場合の機能構成の一例を示す。携帯端末１は、ＩＤ取得部１１１、リーダライタ制御部１１２、編集部１１３、送信部１１４、暗号化／復号処理部１４１を機能構成として含む。ＩＤ取得部１１１、リーダライタ制御部１１２、編集部１１３、送信部１１４は、携帯端末１のＣ

ＰＵ　１０１が通過記録アプリケーション１１を実行することによって実現される機能である。暗号化／復号処理部１４１は、携帯端末１のＣＰＵ　１０１がセキュアＯＳの暗号化／復号モジュール１４を実行することによって実現される機能である。

【００４０】

ＩＤ取得部１１１は、認証サーバ４からアクセスＩＤを取得する。アクセスＩＤは、携帯端末１がＩＣタグ２、格納サーバ３等に対してアクセスする場合の認証に用いられるＩＤである。アクセスＩＤを利用することによって、移動履歴検索システム１００内のセキュリティが保たれる。認証サーバ４から取得されたアクセスＩＤは、メモリ１０２の不揮発性ＲＡＭに格納される。

【００４１】

リーダライタ制御部１１２は、ＩＣタグリーダライタ１０４を制御する。具体的には、リーダライタ制御部１１２は、ＩＣタグリーダライタ１０４の、起動及び停止、リーダ／ライタの動作モードの切り替え、探索時の電波の照射の開始及び停止、通過履歴情報のＩＣタグ２からの読出及びＩＣタグ２への書込等を制御する。リーダライタ制御部１１２は、「探索制御部」、「書込制御部」、「読出制御部」の一例である。

【００４２】

編集部１１３は、ＩＣタグ２から読み出された通過履歴情報を編集する。通過履歴情報には、ＩＣタグ２の近傍を通過した携帯端末１の履歴が格納されている。より具体的には、第１実施形態では、通過履歴情報は、ＩＣタグ２の識別情報、ＩＣタグ２の位置情報、携帯端末１の電話番号、携帯端末１の通過日時を１エントリとして、通過日時の古い順に並べられたリストである。また、通過履歴情報は、第１実施形態では、１エントリ単位で暗号化されている。編集部１１３は、「編集部」の一例である。

【００４３】

編集部１１３は、携帯端末１の電話番号と、通過日時としての現在日時とを取得し、これらと、ＩＣタグ２から取得されるＩＣタグ２の識別情報及び位置情報と、を合わせて、通過履歴情報のエントリを作成する。編集部１１３は、暗号化／復号処理部１４１に作成したエントリの暗号化を依頼し、暗号化してもらう。編集部１１３は、通過履歴情報の先頭のエントリを削除し、最後尾に作成したエントリを追加して、通過履歴情報の編集を完了する。追加するエントリの分古いエントリを削除することによって、ＩＣタグ２のメモリ容量が小さくても、自装置の通過記録情報を残すことができる。なお、通過履歴情報の編集の方法は、これに限られない。

【００４４】

送信部１１４は、格納サーバ３に、編集部１１３によって編集された通過履歴情報を送信する。編集部１１３による通過履歴情報の編集が完了した際に、格納サーバ３にアクセスできない場合には、送信部１１４は、通過履歴情報をメモリ１０２の不揮発性ＲＡＭに格納する。送信部１１４は、格納サーバ３にアクセス可能になった際に、不揮発性ＲＡＭから通過履歴情報を読み出して格納サーバ３に送信する。送信部１１４は、「送信部」の一例である。

【００４５】

暗号化／復号処理部１４１は、他の処理部からの依頼に応じて、セキュアキー１６を用いて、暗号化又は復号を行う。暗号化／復号処理部１４１が行う暗号化方式は、例えば、ＤＥＳ（Data Encryption Standard）である。暗号化／復号処理部１４１は、「暗号化処理部」の一例である。

【００４６】

認証サーバ４は、機能構成として、認証部４１を含む。認証部４１は、例えば、認証サーバ４のＣＰＵが所定のプログラムを実行することによって実現される機能の一つである。認証部４１は、携帯端末１からの要求に応じて、固有情報１５によって携帯端末１を認証し、アクセスＩＤを発行する。

【００４７】

例えば、認証部４１は、１つのアクセスＩＤを保持し、該１つのアクセスＩＤが移動履

歴検索システム１００内で全携帯端末１によって共有されてもよい。または、認証部４１は、移動履歴検索システム１００内で予め定められた複数のアクセスＩＤのプールを保持し、該プールからアクセスＩＤを払い出してもよい。又は、認証部４１は、所定の演算方法に則って、例えば、要求元の携帯端末１の識別情報等に応じて、アクセスＩＤを作成してもよい。いずれの場合でも、アクセスＩＤは、認証サーバ４、ＩＣタグ２、格納サーバ３との間で共通のルールの下作成されるものとする。

【００４８】

また、第１実施形態では、携帯端末１は、取得したアクセスＩＤを継続して使用することとする。すなわち、第１実施形態では、携帯端末１が、認証サーバ４に対して、アクセスＩＤの取得処理を行うのは、ＩＣタグ２や格納サーバ３へのアクセスの初回時に限定される。ただし、アクセスＩＤの使用方法は、取得したものを継続的に使用することに限られず、例えば、ワンタイムパスワードのように、携帯端末１がＩＣタグ２や格納サーバ３にアクセスする度に、認証サーバ３からアクセスＩＤを取得するのでもよい。

【００４９】

ＩＣタグ２は、機能構成として、認証部２１、読出書込処理部２２を含む。認証部２１、読出書込処理部２２は、それぞれ、メモリ２０２のプログラム領域に格納される所定のプログラムをＣＰＵ　２０１が実行することによって実現される機能である。

【００５０】

認証部２１は、携帯端末１の認証を行う。認証部２１が行う認証は、携帯端末１から受信するアクセスＩＤが、認証サーバ４と共通のルールに従ったものであるか否かで行われる。

【００５１】

読出書込処理部２２は、メモリ２０２内の暗号化領域に対する通過履歴情報の読み出し又は書き込みを行う。

【００５２】

ＩＣタグ２のメモリ２０２は、暗号化領域を含む。暗号化領域には、通過履歴情報が暗号化されて格納されている。また、ＩＣタグ２の識別情報及び位置情報は、予めＩＣタグ２のメモリ２０２の暗号化領域以外の領域に格納されている（図示せず）。ＩＣタグ２の位置情報は、例えば、緯度経度、住所、建物内の設置個所の識別情報等である。

【００５３】

格納サーバ３は、機能構成として、認証部３１、暗号化／復号処理部３２、格納部３３、検索部３４、通過履歴情報データベース３５を含む。認証部３１は、アクセスＩＤによる携帯端末１の認証を行う。暗号化／復号処理部３２は、通過履歴情報の暗号化又は復号を行う。なお、格納サーバ３も携帯端末１が有するセキュアキーを不揮発性メモリに有している。

【００５４】

格納部３３は、携帯端末１からの通過履歴情報を通過履歴情報データベース３５に格納する。なお、通過履歴情報は、暗号化／復号処理部３２によって復号されてから通過履歴情報データベース３５に格納される。

【００５５】

検索部３４は、携帯端末１からの履歴検索要求の受信に応じて、通過履歴情報データベース３５の検索を行う。検索の結果、通過履歴情報データベース３５から抽出された通過履歴情報のエントリは、暗号化／復号処理部３２によって暗号化されてから、検索部３４によって、履歴検索要求の送信元である携帯端末１に送信される。

【００５６】

通過履歴情報データベース３５には、各携帯端末１から送信された通信履歴情報が格納されている。通過履歴情報データベース３５は、暗号化されていない状態で通信履歴情報が格納されている。

【００５７】

図６は、移動履歴検索アプリケーション１２を実行する場合の携帯端末１の機能構成の

一例である。移動履歴検索アプリケーション１２は、２つの移動履歴検索処理を含む。１つ目の移動履歴検索処理は、格納サーバ３の通過履歴情報データベース３５を検索する方法である。２つ目の移動履歴検索処理は、各ＩＣタグ２から通過履歴情報を読み出して、所望の通過履歴情報を収集する方法である。いずれの移動履歴検索処理を行うかは、ユーザ操作によって選択される。

【００５８】

携帯端末１は、機能構成として、ＩＤ取得部１２１、検索制御部１２２、表示処理部１２３、リーダライタ制御部１２４、暗号化／復号処理部１４１を含む。ＩＤ取得部１２１、検索制御部１２２、表示処理部１２３は、携帯端末１のＣＰＵ　１０１が移動履歴検索アプリケーション１２を実行することによって実現される機能である。暗号化／復号処理部１４１は、携帯端末１のＣＰＵ　１０１がセキュアＯＳの暗号化／復号モジュール１４を実行することによって実現される機能である。

【００５９】

ＩＤ取得部１２１、リーダライタ制御部１２４は、通過記録アプリケーション１１が実行された場合の機能構成である、ＩＤ取得部１１１、リーダライタ制御部１１２と同様の機能である。

【００６０】

検索制御部１２２は、格納サーバ３に対して移動履歴検索処理を行う場合には、格納サーバ３に通過履歴情報の検索を要求するための読出要求を送信し、ＩＣタグ２に対して移動履歴検索処理を行う場合には、リーダライタ制御部１２４を通じＩＣタグ２に通過履歴情報の読出要求を送信する。通過履歴情報の検索のための読出要求には、捜索対象の携帯端末１の電話番号が含まれる。捜索対象の電話番号は、ユーザによって入力される。表示処理部１２３は、検索結果である通過履歴情報を、例えば、ディスプレイに出力する。

【００６１】

＜携帯端末１の処理の流れ＞

図７は、携帯端末１の通過記録アプリケーション１１の処理のフローチャートの一例である。図７に示される処理は、例えば、携帯端末１の起動、所定アプリケーションの起動、ユーザ操作による起動指示の入力等を契機として、開始される。所定のアプリケーションは、例えば、電子メールアプリケーション、ユーザ設定のアプリケーションである。または、通過記録アプリケーションは、電子メールアプリケーションによって災害発生予測の緊急通報の電子メールが受信された場合に起動してもよい。以降、ＩＣタグリーダライタ１０４がリーダとして動作する場合には、ＩＣタグリーダ１０４と表記する。また、ＩＣタグリーダライタ１０４がライタとして動作する場合には、ＩＣタグライタ１０４と表記する。

【００６２】

ＯＰ１では、ＣＰＵ　１０１は、アクセスＩＤ取得処理を行う。アクセスＩＤ取得処理は、サーバ３からアクセスＩＤを取得するための処理である。アクセスＩＤ取得処理の詳細は、後述される。アクセスＩＤが取得されると、次に処理がＯＰ２に進む。

【００６３】

ＯＰ２では、ＣＰＵ　１０１は、ＩＣタグリーダライタ１０４を起動させる。これによって、ＩＣタグリーダライタ１０４が起動する。なお、ＣＰＵ　１０１は、ＩＣタグリーダライタ１０４をリーダとして起動させる。次に処理がＯＰ３に進む。

【００６４】

ＯＰ３では、ＣＰＵ　１０１は、ユーザ操作によるＩＣタグ２の探索停止要求の入力の有無を判定する。ユーザ操作によるＩＣタグ２の探索停止要求の入力がある場合には（ＯＰ３：ＹＥＳ）、図７に示される処理が終了する。ユーザ操作によるＩＣタグ２の探索停止要求が入力されない場合には（ＯＰ３：ＮＯ）、処理がＯＰ４に進む。

【００６５】

ＯＰ４では、ＣＰＵ　１０１は、第１のタイマを起動する。第１のタイマは、ＩＣタグリーダライタ１０４が電波を照射するタイミングを計るためのタイマであって、例えば、

７秒である。次に処理がＯＰ５に進む。

【００６６】

ＯＰ５では、ＣＰＵ　１０１は、電波の照射の開始をＩＣタグリーダ１０４に指示する。指示を受けて、ＩＣタグリーダ１０４は所定の周波数で電波の照射を開始する。照射される電波には、例えば、アクセスＩＤが含まれている。次に処理がＯＰ６に進む。

【００６７】

ＯＰ６では、ＣＰＵ　１０１は、第２のタイマを起動する。第２のタイマは、電波の照射の継続時間を規定するタイマである。第２のタイマは、例えば、０．２秒である。次に処理がＯＰ７に進む。

【００６８】

ＯＰ７では、ＣＰＵ　１０１は、ＩＣタグ２の検出の有無を判定する。ＩＣタグ２から、照射電波と同じ周波数の電波を受信すると、ＩＣタグリーダ１０４はＣＰＵ　１０１に通知し、ＣＰＵ　１０１はＩＣタグ２を検出する。ＩＣタグ２が検出された場合には（ＯＰ７：ＹＥＳ）、処理がＯＰ１０に進む。ＩＣタグが検出されない場合には（ＯＰ７：ＮＯ）、処理がＯＰ８に進む。

【００６９】

ＯＰ８では、ＣＰＵ　１０１は、第２のタイマのタイムアウトであるか否かを判定する。第２のタイマのタイムアウトである場合には（ＯＰ８：ＹＥＳ）、ＯＰ９に処理が進む。第２のタイマのタイムアウトでない場合には（ＯＰ８：ＮＯ）、処理がＯＰ７に戻る。

【００７０】

ＯＰ９では、第２のタイマのタイムアウトであるため、ＣＰＵ　１０１は、ＩＣタグリーダ１０４の電波の照射の停止を指示する。指示を受けて、ＩＣタグリーダ１０４は、電波の照射を停止する。次に処理がＯＰ３に戻り、再度、ＯＰ３以降の処理が行われる。

【００７１】

ＯＰ１０では、ＣＰＵ　１０１は、ＩＣタグ２を検出したので、通過履歴情報の読出要求をＩＣタグリーダ１０４に発信させる。通過履歴情報の読出要求には、アクセスＩＤが含まれる。ＣＰＵ　１０１は、第２のタイマを起動させる。次に処理がＯＰ１１に進む。

【００７２】

ＯＰ１１では、ＣＰＵ　１０１は、第２のタイマのタイムアウトであるか否かを判定する。第２のタイマのタイムアウトである場合には（ＯＰ１１：ＹＥＳ）、処理がＯＰ９に進み、ＩＣタグリーダ１０４の電波の照射が停止される。第２のタイマのタイムアウトでない場合には（ＯＰ１１：ＮＯ）、処理がＯＰ１２に進む。

【００７３】

ＯＰ１２では、ＣＰＵ　１０１は、データを受信したか否かを判定する。受信されるデータは、ＩＣタグ２が保持する通過履歴情報とＩＣタグ２の識別情報及び位置情報である。通過履歴情報を受信した場合には（ＯＰ１２：ＹＥＳ）、処理がＯＰ１３に進む。なお、通過履歴情報は、暗号化された状態である。次に、処理がＯＰ１３に進む。通過履歴情報を受信していない場合には（ＯＰ１２：ＮＯ）、処理がＯＰ１１に戻る。

【００７４】

ＯＰ１３では、ＣＰＵ　１０１は、通過履歴情報受信処理を行う。通過履歴情報受信処理は、ＩＣタグ２から通過履歴情報を受信した場合に実行される処理である。通過履歴情報受信処理の詳細は、後述される。通過履歴情報受信処理が終了すると、処理がＯＰ３に戻り、再度ＯＰ３以降の処理が行われる。

【００７５】

ＯＰ２～ＯＰ１２の処理は、リーダライタ制御部１１２の処理である。なお、ＯＰ１のアクセスＩＤ取得処理は、既にアクセスＩＤを取得している場合には、実施されない。

【００７６】

図８は、アクセスＩＤ取得処理のフローチャートの一例である。図８に示される処理は、ＩＤ取得部１１１、又は、ＩＤ取得部１２１の処理である。

【００７７】

ＯＰ２１では、ＣＰＵ　１０１は、セキュア領域から固有情報１５を読み出す。次に処理がＯＰ２２に進む。

【００７８】

ＯＰ２２では、ＣＰＵ　１０１は、暗号化通信で認証サーバ４に認証要求を送信する。認証要求には、固有情報が含まれている。携帯端末１と認証サーバ４との間の暗号化通信は、例えば、ＳＳＬ（Secure Sockets Layer）である。次に処理がＯＰ２３に進む。

【００７９】

ＯＰ２３では、ＣＰＵ　１０１は、認証サーバ４から認証要求に対する応答を受信したか否かを判定する。認証サーバ４から認証要求に対する応答を受信した場合には（ＯＰ２３：ＹＥＳ）、処理がＯＰ２４に進む。認証サーバ４から認証要求に対する応答が所定時間経過しても受信されない場合には（ＯＰ２３：ＮＯ）、図８に示される処理が終了する。

【００８０】

ＯＰ２４では、ＣＰＵ　１０１は、受信した認証要求に対する応答からアクセスＩＤを抽出する。アクセスＩＤは、例えば、メモリ１０２の不揮発性ＲＡＭに格納される。その後、処理が図７のＯＰ２に進む。

【００８１】

図９は、通過履歴情報受信処理のフローチャートの一例である。ＯＰ３１では、ＣＰＵ　１０１は、ＩＣタグリーダ１０４に対して、電波の照射を停止させる。次に処理がＯＰ３２に進む。

【００８２】

ＯＰ３２では、ＣＰＵ　１０１は、現在日時を取得する。現在日時は、携帯端末１内の内蔵時計（図示せず）から取得される。次に処理がＯＰ３３に進む。

【００８３】

ＯＰ３３では、ＣＰＵ　１０１は、携帯端末１の電話番号を取得する。電話番号は、例えば、メモリ１０２の不揮発性ＲＡＭに格納されている。次に処理がＯＰ３４に進む。

【００８４】

ＯＰ３４では、ＣＰＵ　１０１は、ＩＣタグ２から読み出された通過履歴情報を編集する。より具体的には、以下の通りである。通過履歴情報は、例えば、１エントリごとに暗号化処理が施されており、エントリは、古いものの順番で並んでいる。ＣＰＵ　１０１は、セキュア領域において、ＯＰ３２で取得した現在時刻、ＯＰ３３で取得した電話番号、ＩＣタグ２の識別情報及び位置情報を通過履歴情報の１エントリとして、暗号化する。ＣＰＵ　１０１は、暗号化した通過履歴情報の１エントリを、不揮発性ＲＡＭから読み出した暗号化されている通過履歴情報の最後尾に追加し、通過履歴情報の先頭のエントリを削除する。次に処理がＯＰ３５に進む。

【００８５】

ＯＰ３５では、ＣＰＵ　１０１は、ＩＣタグライタ１０４に電波を照射させる。次に処理がＯＰ３６に進む。ＯＰ３６では、ＣＰＵ　１０１は、ＩＣタグライタ１０４に、通過履歴情報の書込要求を発信させる。通過履歴情報の書込要求には、アクセスＩＤと、編集後の通過履歴情報とが含まれる。該通過履歴情報はＩＣタグ２に受信され、ＩＣタグ２内のメモリ２０２に格納される。なお、通過履歴受信処理が行われる際には、既にＩＣタグ２は検出済みであり、図７～図９の処理が完了するまでの時間（１秒未満）に、携帯端末１のユーザが該ＩＣタグ２の交信範囲（７～１０メートル）から出ることは考えにくい。そのため、ＣＰＵ　１０１は、ＯＰ３５の処理の後、ＩＣタグ２からの応答を待たずに、ＯＰ３６の処理を実行する。次に処理がＯＰ３７に進む。

【００８６】

ＯＰ３７では、ＣＰＵ　１０１は、ＩＣタグライタ１０４に電波の照射を停止させる。次に処理がＯＰ３８に進む。

【００８７】

ＯＰ３８では、ＣＰＵ　１０１は、携帯端末１が格納サーバ３にアクセス可能であるか

否かを判定する。携帯端末１がサーバ３にアクセス可能か否かは、携帯端末１が無線回路１０５の通信可能圏内にいるか否かによって、判定される。携帯端末１が格納サーバ３にアクセス可能な場合には（ＯＰ３８：ＹＥＳ）、処理がＯＰ３９に進む。携帯端末１が格納サーバ３にアクセス可能でない場合には（ＯＰ３８：ＮＯ）、処理がＯＰ４０に進む。

【００８８】

ＯＰ３９では、携帯端末１が格納サーバ３にアクセス可能であるため、ＣＰＵ　１０１は、通過履歴ネットワーク送信処理を行う。通過履歴ネットワーク送信処理は、通過履歴を格納サーバ３に送信する処理であり、詳細は後述される。その後、処理が図７のＯＰ３に戻る。

【００８９】

ＯＰ４０では、携帯端末１が格納サーバ３にアクセス可能でないため、ＣＰＵ　１０１は、編集後の通過履歴情報を不揮発性ＲＡＭに格納する。その後、処理が図７のＯＰ３に戻る。なお、携帯端末１が格納サーバ３にアクセス可能になった場合に、ＣＰＵ　１０１は、不揮発性ＲＡＭに格納されている通過履歴情報を送信する。

【００９０】

ＯＰ３１、ＯＰ３５～ＯＰ３７の処理は、リーダライタ制御部１１１の処理である。ＯＰ３２、ＯＰ３３、ＯＰ３４の処理は、編集部１１３の処理である。ＯＰ３５の暗号化処理は、暗号化／復号処理部１４１の処理である。ＯＰ３８、ＯＰ４０の処理は、送信部１１４の処理である。

【００９１】

図１０は、通過履歴ネットワーク送信処理のフローチャートである。図１０に示される処理は、送信部１１４の処理である。

【００９２】

ＯＰ４１では、ＣＰＵ　１０１は、格納サーバ３に送信するアクセスＩＤと通過履歴情報とを設定する。通過履歴情報は、編集後のものである。次に処理がＯＰ４２に進む。

【００９３】

ＯＰ４２では、ＣＰＵ　１０１は、格納サーバ３に履歴保存要求を暗号化通信で送信する。履歴保存要求には、アクセスＩＤと、通過履歴情報とが含まれる。次に処理がＯＰ４３に進む。

【００９４】

ＯＰ４３では、ＣＰＵ　１０１は、通過履歴情報の送信完了を判定する。通過履歴情報の送信完了は、例えば、格納サーバ３から履歴保存要求に対する応答を受信することによって判定する。通過履歴情報の送信が完了した場合には（ＯＰ４３：ＹＥＳ）、処理が図７のＯＰ３に戻る。通過履歴情報の送信が完了しない場合には（ＯＰ４３：ＮＯ）、通過履歴情報の送信が完了するまでＣＰＵ　１０１は、待機状態となる。例えば、所定時間経過しても通信履歴情報の送信が完了しない場合には、エラーとなり、図１０に示される処理が終了する。

【００９５】

図１１は、格納サーバ３に対して移動履歴検索処理が行われる場合の移動履歴検索アプリケーション１２の処理のフローチャートの一例である。図１１に示される処理は、ユーザ操作によって開始される。なお、捜索対象の携帯端末１の電話番号は、開始の指示とともにユーザ操作によって入力される。

【００９６】

ＯＰ５１では、ＣＰＵ　１０１は、アクセスＩＤ取得処理を実行する。ＯＰ５１で行われるアクセスＩＤ処理は、図８で示された通りである。アクセスＩＤが取得されると、処理がＯＰ５２に進む。なお、アクセスＩＤを既に取得している場合には、ＯＰ５１の処理は実施されない。

【００９７】

ＯＰ５２では、ＣＰＵ　１０１は、アクセスＩＤと、電話番号とを読出して設定する。次に処理がＯＰ５３に進む。

【００９８】
ＯＰ５３では、ＣＰＵ　１０１は、格納サーバ３に履歴読出要求を暗号化通信で送信する。履歴読出要求には、アクセスＩＤと電話番号とが含まれる。次に処理がＯＰ５４に進む。
【００９９】
ＯＰ５４では、ＣＰＵ　１０１は、格納サーバ３から履歴読出要求に対する応答を受信したか否かを判定する。履歴読出要求の応答には、格納サーバ３の通過履歴情報データベース３５の検索結果である通過履歴情報が含まれる。履歴読出要求に対する応答を受信した場合には（ＯＰ５４：ＹＥＳ）、処理がＯＰ５５に進む。履歴読出要求に対する応答を受信しない場合には（ＯＰ５４：ＮＯ）、応答を受信するまでＣＰＵ　１０１は、待機状態となる。例えば、所定時間経過しても履歴読出要求に対する応答が受信されない場合には、エラーとなり、図１１に示される処理が終了する。
【０１００】
ＯＰ５５では、ＣＰＵ　１０１は、受信した検索結果である通過履歴情報を復号する。次に処理がＯＰ５６に進む。
【０１０１】
ＯＰ５６では、ＣＰＵ　１０１は、受信した検索結果である通過履歴情報を、例えば、ディスプレイに表示する。その後、図１１に示される処理が終了する。
【０１０２】
ＯＰ５１の処理は、ＩＤ取得部１２１の処理である。ＯＰ５２、ＯＰ５３、ＯＰ５４の処理は、検索制御部１２２の処理である。ＯＰ５５の処理は、暗号化／復号処理部１４１の処理である。ＯＰ５６の処理は、表示処理部１２３の処理である。
【０１０３】
図１２は、ＩＣタグ２に対して移動履歴検索処理が行われる場合の移動履歴検索アプリケーション１２の通過履歴情報受信処理のフローチャートの一例である。ＩＣタグ２に対して移動履歴検索処理が行われる場合には、図７に示される、通過記録アプリケーション１１の処理と同様の処理が行われる。ただし、移動履歴検索アプリケーション１２の場合には、ユーザ操作による起動の指示の入力によって開始される。
【０１０４】
また、通過履歴情報受信処理も、通過記録アプリケーション１１の場合と異なる。図１２に示される処理は、移動履歴検索アプリケーション１２の実行において、ＩＣタグ２から通信履歴情報を受信した後の処理である。
【０１０５】
ＯＰ６１では、ＣＰＵ　１０１はＩＣタグリーダ１０４に電波の照射を停止させる。次に処理がＯＰ６２に進む。
【０１０６】
ＯＰ６２では、ＣＰＵ　１０１は、ＩＣタグ２から受信した通過履歴情報を復号する。次に処理がＯＰ６３に進む。
【０１０７】
ＯＰ６３では、ＣＰＵ　１０１は、捜索対象の電話番号をキーとして、ＩＣタグ２から受信した通過履歴情報を検索する。次に処理がＯＰ６４に進む。
【０１０８】
ＯＰ６４では、ＣＰＵ　１０１は、検索結果の通過履歴情報を、例えば、ディスプレイに表示する。その後、図１２に示される処理が終了する。
【０１０９】
ＯＰ６１の処理は、リーダライタ制御部１２４の処理である。ＯＰ６２の処理は、暗号化／復号処理部１４１の処理である。ＯＰ６３の処理は、検索制御部１２２の処理である。ＯＰ６４の処理は、表示処理部１２３の処理である。
【０１１０】
＜格納サーバ３の処理＞

図１３は、格納サーバ３の処理のフローチャートの一例である。図１３に示される処理は、格納サーバ３の起動とともに開始される。

【０１１１】

ＯＰ７１では、認証部３１は、携帯端末１からの要求の受信を判定する。携帯端末１からの要求を受信した場合には（ＯＰ７１：ＹＥＳ）、処理がＯＰ７２に進む。携帯端末１からの要求を受信していない場合には（ＯＰ７１：ＮＯ）、携帯端末１からの要求を受信するまで待機状態となる。

【０１１２】

ＯＰ７２では、認証部３１は、携帯端末１からの要求に含まれるアクセスＩＤを用いて認証を行う。認証が成功した場合には（ＯＰ７２：ＹＥＳ）、処理がＯＰ７３に進む。認証が失敗した場合には（ＯＰ７２：ＮＯ）、認証部３１は、認証失敗を携帯端末１に通知し、図１３に示される処理が終了する。

【０１１３】

ＯＰ７３では、認証部３１は、要求内容を判定する。要求内容が履歴読出要求である場合には、処理がＯＰ７４に進み、ＯＰ７４では、通過履歴情報読出処理が行われる。要求内容が履歴保存要求である場合には、処理がＯＰ７５に進み、通過履歴情報格納処理が行われる。通過履歴情報読出処理、通過履歴情報格納処理の詳細は後述される。

【０１１４】

ＯＰ７４において通過履歴情報読出処理が終了すると、図１３に示される処理が終了する。また、ＯＰ７５において、通過履歴情報格納処理が終了すると、図１３に示される処理が終了する。

【０１１５】

図１４は、格納サーバ３による通過履歴情報読出処理のフローチャートの一例である。ＯＰ８１では、検索部３４は、通過履歴情報データベース３５を、履歴読出要求に含まれる電話番号をキーとして検索する。次に処理がＯＰ８２に進む。

【０１１６】

ＯＰ８２では、検索部３４による検索の結果として得られた通過履歴情報を、暗号化／復号処理部３２が暗号化する。次に処理がＯＰ８３に進む。

【０１１７】

ＯＰ８３では、検索部３４は、暗号化通信で、携帯端末１に検索結果である通過履歴情報を送信する。次に処理がＯＰ８４に進む。

【０１１８】

ＯＰ８４では、検索部３４は、通信履歴情報の送信完了を判定する。通信履歴情報の送信が完了した場合には（ＯＰ８４：ＹＥＳ）、図１４に示される処理が終了し、これに伴い、図１３に示される処理も終了する。例えば、所定時間経過しても通過履歴情報の送信が完了しない場合には（ＯＰ８４：ＮＯ）、エラーとなり、図１４に示される処理が終了する。

【０１１９】

図１５は、格納サーバ３による通過履歴情報格納処理のフローチャートの一例である。ＯＰ９１では、暗号化／復号処理部３２は、履歴保存要求で受信した通過履歴情報を復号する。復号された通過履歴情報は、格納部３４に出力される。次に処理がＯＰ９２に進む。

【０１２０】

ＯＰ９２では、格納部３４は、復号された通過履歴情報を通過履歴情報データベース３５に追加する。復号された通過履歴情報は、例えば、通過履歴情報データベース３５に格納されている通過履歴情報のエントリの最後尾に追加される。次に処理がＯＰ９３に進む。

【０１２１】

ＯＰ９３では、格納部３４は、暗号化通信を通じて、履歴保存要求の送信元である携帯端末１に、格納結果を送信する。その後、図１５に示される処理が終了し、これとともに

図１３に示される処理も終了する。

【０１２２】

＜ＩＣタグの処理の流れ＞

図１６は、ＩＣタグ２の処理のフローチャートの一例を示す図である。図１６に示されるフローチャートは、ＩＣタグ２が携帯端末１のＩＣタグリーダライタ１０４によって照射された電波を受信すると開始される。

【０１２３】

ＯＰ１０１では、携帯端末１のＩＣタグリーダライタ１０４からの電波を受けることによって、電源が起動し、ＣＰＵ　２０１が起動する。次に処理がＯＰ１０２に進む。

【０１２４】

ＯＰ１０２では、認証部２１は、受信した電波と同じ周波数で電波を発信する。次に処理がＯＰ１０３に進む。

【０１２５】

ＯＰ１０３では、認証部２１は、要求を受信する。次に処理がＯＰ１０４に進む。ＯＰ１０４では、認証部２１は、受信した要求に含まれるアクセスＩＤを抽出して、認証を行う。次に処理がＯＰ１０５に進む。

【０１２６】

ＯＰ１０５では、認証部２１は、認証の成功又は失敗を判定する。認証が成功した場合には（ＯＰ１０５：ＹＥＳ）、処理がＯＰ１０６に進む。認証が失敗した場合には（ＯＰ１０５：ＮＯ）、図１６に示される処理が終了する。

【０１２７】

ＯＰ１０６では、読出書込処理部２２は、要求内容を判定する。要求内容が書込要求である場合には、処理がＯＰ１０７に進む。要求内容が読出要求である場合には、処理がＯＰ１０８に進む。

【０１２８】

ＯＰ１０７では、要求内容が書込要求であるので、読出書込処理部２２は、要求に含まれるデータをメモリ２０２に書き込む。なお、書込要求は通過履歴情報の書込要求であって、要求に含まれるデータは、携帯端末１によって編集された暗号化された通過履歴情報である。次に処理がＯＰ１１０に進む。

【０１２９】

ＯＰ１０８では、要求内容が読出要求であるので、読出書込処理部２２は、メモリ２０２から通過履歴情報、ＩＣタグ２の識別情報及び位置情報を読み出す。なお、読出要求は、通過履歴情報の読出要求である。また、読み出された通過履歴情報は、暗号化されている。次に処理がＯＰ１０９に進む。

【０１３０】

ＯＰ１０９では、読出書込処理部２２は、読み出した通過履歴情報、ＩＣタグ２の識別情及び位置情報を電波に乗せて発信する。次に処理がＯＰ１１０に進む。

【０１３１】

ＯＰ１１０では、携帯端末１のＩＣタグリーダライタ１０４からの電波受信が停止し、ＩＣタグ２は、電波を受信せずに所定時間経過すると、電源を停止する。その後、図１６に示される処理が終了する。

【０１３２】

なお、ＯＰ１０２で発信される電波に、移動履歴検索システム１００のサービスに対応するＩＣタグであるか否かを示す情報を含めて送信してもよい。該情報を含む電波を携帯端末１が受信した場合には、携帯端末１は、要求を送信する等の処理を行わずに、通過記録アプリケーション１１や移動履歴検索アプリケーション１２の処理を終了する。

【０１３３】

＜装置間の処理の流れ＞

図１７は、携帯端末１による通過記録アプリケーション１１の実行時の処理のシーケンスの一例を示す図である。図５では、認証サーバ４と格納サーバ３とが同じサーバであり

、単にサーバ３と称する。
【０１３４】
Ｓ１では、携帯端末１は、通過記録アプリケーション１１を起動し、ＩＣタグ２の探索を開始する。
【０１３５】
Ｓ２では、携帯端末１は、インターネット経由の暗号化通信で、サーバ３に対して、認証要求を送信する（図８、ＯＰ２２）。認証要求には、携帯端末１の固有情報１５が含まれている。
【０１３６】
Ｓ３では、サーバ３は、携帯端末１からの認証要求を受信し、該認証要求から携帯端末１の固有情報１５を抽出し、認証を行う。サーバ３は、サービスに加入している携帯端末１の固有情報を予め保持しており、認証要求から抽出した携帯端末１の固有情報１５に合致する固有情報を保持している場合に、認証成功とし、アクセスＩＤを発行する。
【０１３７】
Ｓ４では、サーバ３は、携帯端末１に認証成功の応答と、アクセスＩＤとを送信する。携帯端末１は、該応答とアクセスＩＤを受信する（図８、ＯＰ２３：ＹＥＳ、ＯＰ２４）。なお、アクセスＩＤは一旦取得すると、継続して使用可能なため、Ｓ２～Ｓ３の処理は、通過記録アプリケーション１１の初回起動時に実行され、２回目以降は実行されないことが多い。
【０１３８】
Ｓ５では、携帯端末１は、所定の周波数の電波を照射して、ＩＣタグ２の探索を行う（図７、ＯＰ５）。周波数の値は、ＩＣタグリーダライタ１０４の種類等に応じて予め決定されている。携帯端末１によるＩＣタグ２の探索のための電波の照射は、例えば、７秒間に１回の周期で、０．２秒間継続して行われる。
【０１３９】
Ｓ６では、携帯端末１から照射された電波の到達範囲内に設置されているＩＣタグ２において、ＩＣタグ２内のアンテナ２０３に電界が発生し、電圧が発生することによってＣＰＵ　２０１が起動する（図１６、ＯＰ１０１）。起動したＩＣタグ２は、携帯端末１から照射された電波と同じ周波数で電波を発信する（図１６、ＯＰ１０２）。
【０１４０】
Ｓ７では、携帯端末１は、ＩＣタグ２から発信された電波を受信したので、ＩＣタグ２内の通過履歴情報の読出要求を発信する（図７、ＯＰ１０）。読出要求には、アクセスＩＤも含まれる。
【０１４１】
Ｓ８では、ＩＣタグ２は、携帯端末１からの通過履歴情報の読出要求を受信し、携帯端末１の認証を行う（図１６、ＯＰ１０３、ＯＰ１０４）。認証は、携帯端末１からの読出要求に含まれるアクセスＩＤが、サーバ３との間で共通のルールの下作成されている場合には、成功となる。ＩＣタグ２は、認証が成功すると、メモリ２０２から通過履歴情報、ＩＣタグ２の識別情報及び位置情報を読み出し、発信する（図１６、ＯＰ１０８、ＯＰ１０９）。
【０１４２】
Ｓ９では、携帯端末１は、ＩＣタグ２から通過履歴情報を受信し、受信した通過履歴情報を編集する（図９、ＯＰ３２～ＯＰ３４）。具体的には、携帯端末１は、自装置の電話番号と現在時刻を含むエントリを通過履歴情報の最後尾に追加し、通過履歴情報の先頭の最も古いエントリを削除する。
【０１４３】
Ｓ１０では、携帯端末１は、編集後の通過履歴情報の書込要求を発信する（図９、ＯＰ３６）。Ｓ１１では、ＩＣタグ２は、通過履歴情報の書込要求を受信し、メモリ２０２に受信した通過履歴情報を書き込む（図１６、ＯＰ１０３～ＯＰ１０７）
【０１４４】

Ｓ１２では、携帯端末１は、編集後の通過履歴情報をサーバ３に送信する（図９、ＯＰ３９、図１０）。このとき、携帯端末１のアクセスＩＤもサーバ３に送信される。なお、サーバ３への接続が不可能な場合には、Ｓ１２の処理は、サーバ３への接続が可能になった時点で行われる。サーバ３への接続が可能か否かは、例えば、基地局からの電波を検知できるか否かで判定される。

【０１４５】

Ｓ１３では、サーバ３は、受信した通信履歴情報を通過履歴情報データベース３５に格納する（図１５、ＯＰ９２）。Ｓ１４では、サーバ３は、携帯端末１に対して受信応答を返信する（図１５、ＯＰ９３）。なお、認証サーバと検索サーバとが異なる場合には、Ｓ１３の前に、サーバ３は、携帯端末１のアクセスＩＤにより認証を行う。

【０１４６】

通過記録アプリケーション１１が常時起動でない場合には、携帯端末１がＳ１４のサーバ３からの受信応答を受信すると、通過記録アプリケーション１１は停止する。通過記録アプリケーション１１が常時起動である場合には、Ｓ５のＩＣタグ２の探索が所定周期で実行される。

【０１４７】

図１８は、捜索者端末５によるサーバ３に対する移動履歴検索アプリケーション１１の実行時の処理のシーケンスの一例を示す図である。捜索者端末５は、例えば、携帯電話端末、スマートフォン、タグレット端末、ＰＣ（Personal Computer）であって、ハードウェア構成、及び、機能構成は、携帯端末１と同様又はほぼ同様であるとする。また、捜索者端末５と携帯端末１とが同じであってもよい。また、図１８では、図１７と同様に、認証サーバ４と格納サーバ３とが同じサーバ３であることとする。

【０１４８】

Ｓ２１では、捜索者端末５は、移動履歴検索アプリケーション１２を起動し、サーバ３に対して認証要求を送信する。認証要求には、捜索者端末５の固有情報１５が含まれている。移動履歴検索アプリケーション１２は、例えば、ユーザ操作によって起動される。

【０１４９】

Ｓ２２では、サーバ３は、捜索者端末５からの認証要求を受信し、該認証要求から捜索者端末５の固有情報１５を抽出し、認証を行う。サーバ３は、認証要求から抽出した創作者端末５の固有情報１５に合致する固有情報を保持している場合に、認証成功とし、アクセスＩＤを発行する。

【０１５０】

Ｓ２３では、サーバ３は、捜索者端末５に認証成功の応答と、アクセスＩＤとを送信する。なお、アクセスＩＤは一旦取得すると、継続して使用可能なため、捜索者端末５が既にアクセスＩＤを取得している場合には、Ｓ２１～Ｓ２３の処理は実行されない。

【０１５１】

Ｓ２４では、捜索者端末５は、サーバ３に対して、履歴読出要求を送信する（図１１、ＯＰ５２、ＯＰ５３）。履歴読出要求には、捜索対象の携帯端末１の電話番号と、捜索者端末５のアクセスＩＤとが含まれる。捜索対象の携帯端末１の電話番号は、例えば、捜索者端末５のユーザによって入力される。

【０１５２】

Ｓ２５では、サーバ３は、履歴読出要求から捜索対象の電話番号を抽出し、該電話番号をキーとして通過履歴情報データベース３５を検索する（図１４、ＯＰ８１）。Ｓ２６では、サーバ３は、検索結果として検出した通過履歴情報を暗号化する（図１４、ＯＰ８２）。Ｓ２７では、サーバ３は、検索結果としての通過履歴情報を捜索者端末５に送信する（図１４、ＯＰ８３）。

【０１５３】

Ｓ２８では、捜索者端末５は、サーバ３から検索結果としての通過履歴情報を受信し、該通過履歴情報を復号する（図１１、ＯＰ５４：ＹＥＳ、ＯＰ５５）。Ｓ２９では、捜索者

端末５は、検索結果としての通過履歴情報を、例えばディスプレイに表示する（図１１、ＯＰ５６）。

【０１５４】

なお、サーバ３の通過履歴情報データベースの検索は、電話番号をキーとするものに限られない。例えば、地理的範囲、日時範囲等の捜索対象の通過履歴情報の限定条件を捜索者端末５のユーザが指定し、サーバ３は指定された限定条件を満たす通過履歴情報に対して検索を行ってもよい。

【０１５５】

図１９は、捜索者端末５によるＩＣタグ２に対する移動履歴検索アプリケーション１１の実行時の処理のシーケンスの一例を示す図である。図１９における前提は、図１８と同様とする。

【０１５６】

Ｓ３１～Ｓ３３は、図１８のＳ２１～Ｓ２３と同様のアクセスＩＤ取得処理であり、捜索者端末５はサーバ３からアクセスＩＤを取得する。詳細な説明は省略する。

【０１５７】

Ｓ３４～Ｓ３７は、図１７のＳ５～Ｓ８で行われる、携帯端末１とＩＣタグ２との間の処理と同様であり、捜索者端末５は、ＩＣタグ２から通過履歴情報を取得する。詳細な説明は省略する。

【０１５８】

Ｓ３８では、捜索者端末５は、ＩＣタグ２から読み出した通過履歴情報は暗号化されているので、該通過履歴情報を復号する（図１２、ＯＰ６２）。Ｓ３９では、捜索者端末５は、復号した通過履歴情報から、捜索対象の電話番号に合致する通過履歴情報を検索する（図１２、ＯＰ６３）。Ｓ４０では、携帯端末１は、検索結果としての通過履歴情報を、例えばディスプレイに表示する（図１２、ＯＰ６４）。

【０１５９】

Ｓ３４～Ｓ３８の処理は、捜索対象範囲内に複数のＩＣタグ２が存在する場合には、該複数のＩＣタグ２のそれぞれに対して実行される。

【０１６０】

＜第１実施形態の作用効果＞

図２０は、第１実施形態における移動履歴検索システム１００の作用効果の一例を示す図である。第１実施形態では、携帯端末１がＩＣタグ２の交信範囲内を通過すると、携帯端末１は自身の通過記録情報（電話番号、通過日時）をＩＣタグ２に書き込むので、携帯端末１の移動軌跡の近傍の各地点に設置されたＩＣタグ２に携帯端末１の通過記録情報が残る。また、各ＩＣタグ２の通過履歴情報は、サーバ３に集約され、一括管理される。

【０１６１】

例えば、捜索者は、行方不明者の存在が確認できた最終地点から所定範囲内に存在する複数のＩＣタグ２を特定する。図２０では、顔マークを行方不明者の存在が確認できた最終地点とする。また、図２０では、所定範囲が、該最終地点を中心とする円５００で示されている。

【０１６２】

捜索者は、特定された、円５００内に存在する複数のＩＣタグ２の通過履歴情報の中から、行方不明者の電話番号に合致し、最も新しい通過日時を有するエントリに対応するＩＣタグ２－１を特定する。

【０１６３】

次に、捜索者は、特定されたＩＣタグ２－１を中心とする所定範囲である円５０１内に存在する複数のＩＣタグ２を特定し、行方不明者の電話番号に合致し、最も新しい通過日時を有するエントリに対応するＩＣタグ２－２を特定する。これを繰り返すことによって、ＩＣタグ２－３も特定され、行方不明者の移動軌跡が、ＩＣタグ２－１→ＩＣタグ２－２→ＩＣタグ２－３であることが特定される。したがって、第１実施形態によれば、特定されたＩＣタグ２の位置情報という点情報から線情報を取得することができ、行方不明者

の移動軌跡をより正確に取得することができる。また、サーバ３を利用する場合には、捜索者は、より少ない労力で、効率よく行方不明者の移動軌跡を特定することができる。

【０１６４】

図２１は、ＧＰＳを利用したオートトラッキングによる位置情報の記録処理と、第１実施形態における携帯端末１の通過記録アプリケーション１１による位置情報の記録処理との消費電流の比較の一例である。図２１に示される例では、ＧＰＳを利用したオートトラッキングは、６０秒に１回の間隔で位置情報を測位し、１回の測位には５．３秒を要するものとする。通過記録アプリケーションは、７秒に一回の間隔でＩＣタグ２の探索処理を行い、１回の探索処理では０．２秒間電波を照射するものとする。

【０１６５】

１回の処理の消費電流は、ＧＰＳのオートトラッキングが０．６ｍＡｈ、通過記録アプリケーション１１が０．０２２ｍＡｈである。また、１時間における消費電流は、ＧＰＳのオートトラッキングが３５．６ｍＡｈ、通過記録アプリケーション１１が１１．３１ｍＡｈである。

【０１６６】

したがって、第１実施形態によれば、位置情報の記録に係る消費電力をより少なくすることができ、電池を電源とする携帯端末１をより長く起動させることができる。

【０１６７】

また、ＩＣタグ２は、パッシブ型のものでよく、電源を用意しなくてもよいため、災害等の影響を受けることが少なく、電源が確保できない状況でも、携帯端末１が近傍を通過することによって、該携帯端末１の通過記録情報を残すことができる。また、ＩＣタグ２は、設置が容易で、第１実施形態の移動履歴検索システム１００は導入に係る初期費用を抑えることができる。

【０１６８】

また、ＩＣタグ２は電源を有するアクティブ型、電源を有しないパッシブ型に依らず、ＧＰＳや携帯電話網等のネットワークが使用できない状況でも、ＩＣタグ２の近傍を通過することによって、ＩＣタグ２に通過記録情報を残すことができる。

【０１６９】

第１実施形態では、通過履歴情報は、携帯端末１のセキュア領域やサーバ３の通過履歴情報データベース３５内以外では、暗号化された状態である。また、携帯端末１においてもセキュアＯＳを経由しないと通過履歴情報を復号することができない。これによって、他者の電話番号の漏えいの可能性を低減することができる。

【０１７０】

＜その他＞

第１実施形態では、携帯端末１は、ＩＣタグ２から読み出した通過履歴情報の先頭のエントリを削除し、自装置のエントリを最後尾に追加する編集を行う。これに代えて、ＩＣタグ２が通過履歴情報とともに自装置のメモリの空き容量を携帯端末１に通知し、携帯端末１は空き容量に応じて、エントリの削除を行うようにしてもよい。

【０１７１】

また、第１実施形態では、ＩＣタグ２とＩＣタグリーダライタ４を備える携帯端末１を例として説明されたが、第１実施形態で説明された技術は、これらに限られず、ＲＦＩＤ（Radio Frequency Identification）テクノロジ全般に適用可能である。

【０１７２】

＜記録媒体＞

コンピュータその他の機械、装置（以下、コンピュータ等）に上記いずれかの機能を実現させるプログラムをコンピュータ等が読み取り可能な記録媒体に記録することができる。コンピュータ等に、この記録媒体のプログラムを読み込ませて実行させることにより、その機能を提供させることができる。

【０１７３】

ここで、コンピュータ等が読み取り可能な記録媒体とは、データやプログラム等の情報

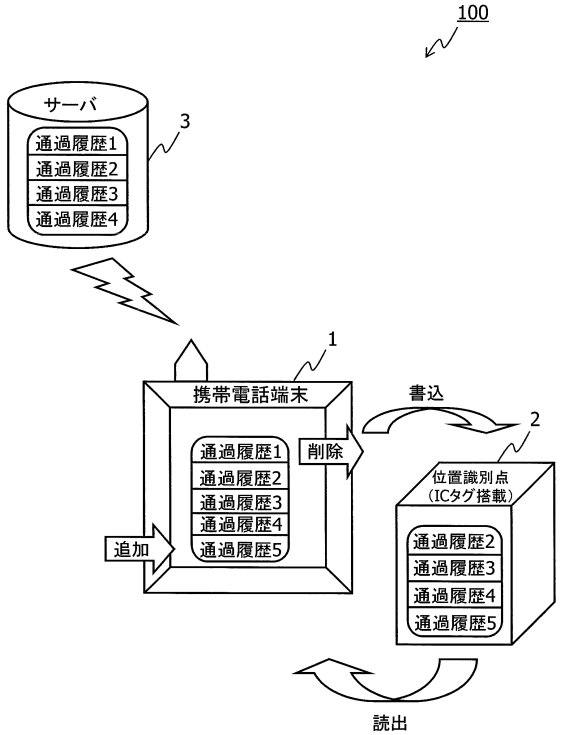
を電気的、磁気的、光学的、機械的、または化学的作用によって蓄積し、コンピュータ等から読み取ることができる記録媒体をいう。このような記録媒体のうちコンピュータ等から取り外し可能なものとしては、例えばフレキシブルディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ／Ｗ、ＤＶＤ、ブルーレイディスク、ＤＡＴ、８ｍｍテープ、フラッシュメモリなどのメモリカード等がある。また、コンピュータ等に固定された記録媒体としてハードディスク、ＲＯＭ（リードオンリーメモリ）等がある。さらに、ＳＳＤ（Solid State Drive）は、コンピュータ等から取り外し可能な記録媒体としても、コンピュータ等に固定された記録媒体としても利用可能である。

【符号の説明】

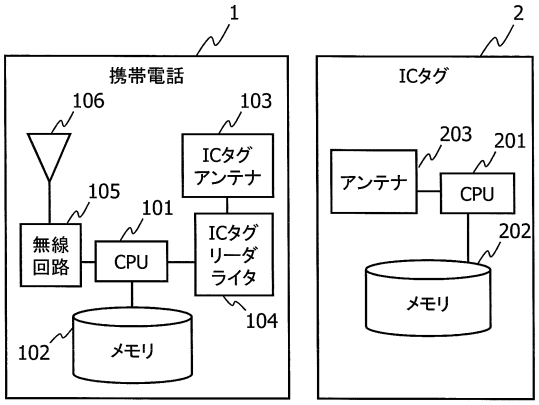
【０１７４】

１　　携帯端末
２　　ＩＣタグ
３　　サーバ
１１　　通過記録アプリケーション
１２　　移動履歴検索アプリケーション
１０１　　ＣＰＵ
１０２　　メモリ
１０４　　ＩＣタグリーダライタ
１１１、１２１　　ＩＤ取得部
１１２、１２４　　リーダライタ制御部
１１３　　編集部
１１４　　送信部
１２２　　検索部
１２３　　表示処理部
１４１　　暗号化／復号処理部

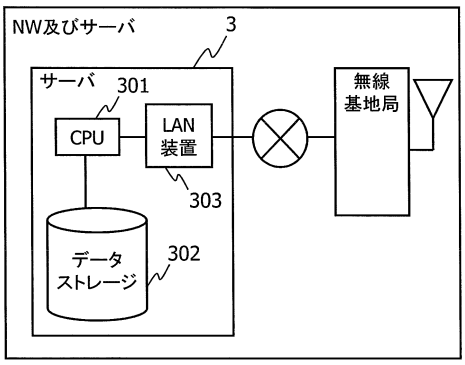
【図１】



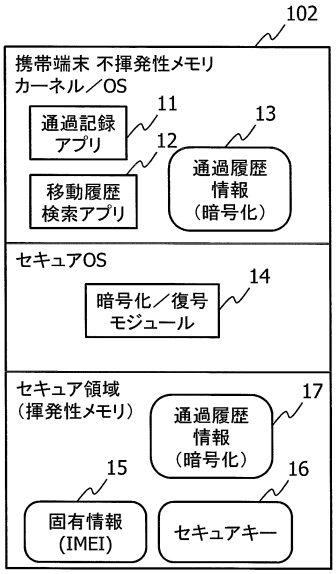
【図２】



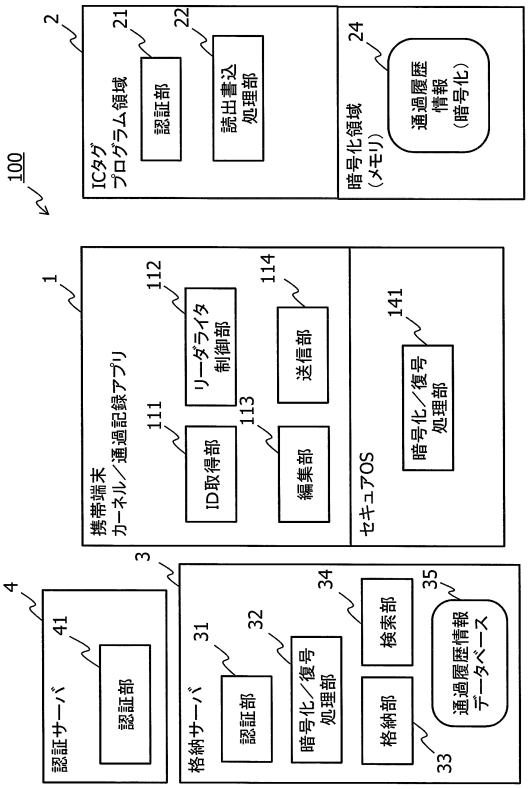
【図３】


NW及びサーバ
3
サーバ
301
CPU
LAN
装置
303
データ
ストレージ
302
無線
基地局

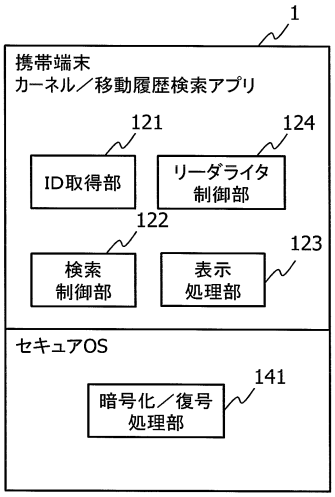
【図４】


102
携帯端末 不揮発性メモリ
カーネル／OS
11
通過記録
アプリ
12
移動履歴
検索アプリ
13
通過履歴
情報
（暗号化）
セキュアOS
14
暗号化／復号
モジュール
セキュア領域
（揮発性メモリ）
17
通過履歴
情報
（暗号化）
15
固有情報
(IMEI)
16
セキュアキー

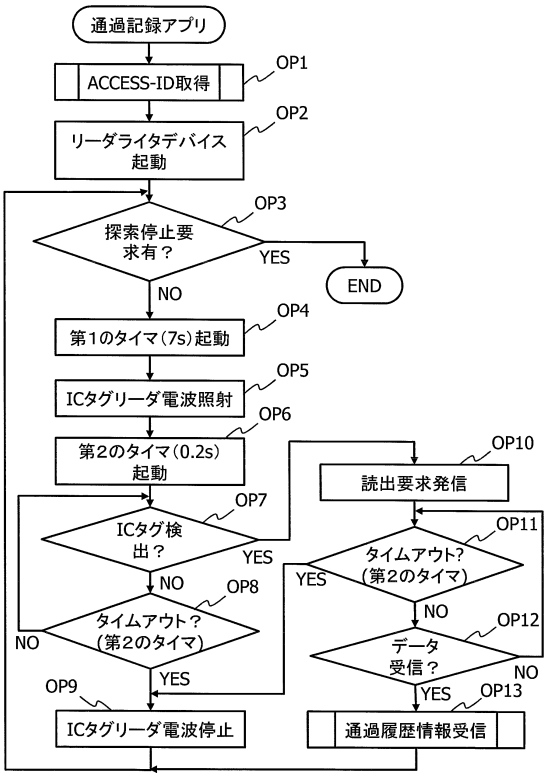
【図５】


100
2
ICタグ
プログラム領域
21
認証部
22
読出書込
処理部
暗号化領域
（メモリ）
24
通過履歴
情報
（暗号化）
1
携帯端末
カーネル／通過記録アプリ
112
リーダライタ
制御部
114
送信部
111
ID取得部
113
編集部
セキュアOS
141
暗号化／復号
処理部
3
4
認証サーバ
41
認証部
格納サーバ
31
認証部
32
暗号化／復号
処理部
34
検索部
格納部
33
35
通過履歴情報
データベース

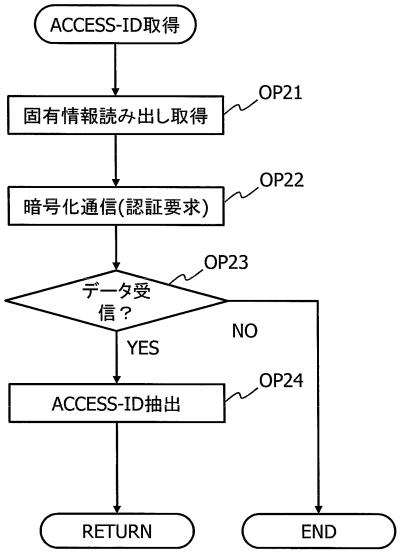
【図６】


1
携帯端末
カーネル／移動履歴検索アプリ
121
ID取得部
124
リーダライタ
制御部
122
検索
制御部
123
表示
処理部
セキュアOS
141
暗号化／復号
処理部

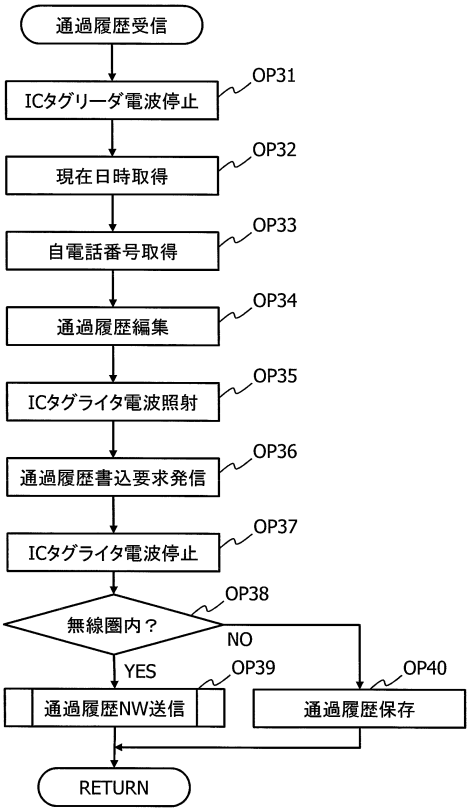
【図７】


通過記録アプリ
ACCESS-ID取得
OP1
リーダライタデバイス起動
OP2
探索停止要求有？
OP3
YES
END
NO
第1のタイマ(7s)起動
OP4
ICタグリーダ電波照射
OP5
第2のタイマ(0.2s)起動
OP6
ICタグ検出？
OP7
YES
NO
タイムアウト？(第2のタイマ)
OP8
NO
YES
ICタグリーダ電波停止
OP9
読出要求発信
OP10
タイムアウト?(第2のタイマ)
OP11
YES
NO
データ受信？
OP12
NO
YES
通過履歴情報受信
OP13

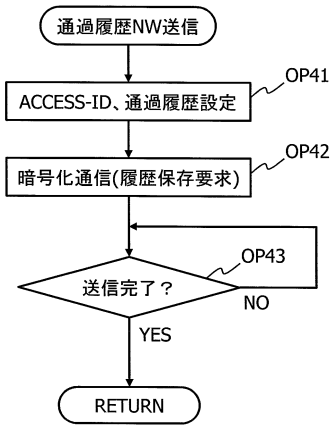
【図８】


ACCESS-ID取得
固有情報読み出し取得
OP21
暗号化通信(認証要求)
OP22
データ受信？
OP23
NO
YES
ACCESS-ID抽出
OP24
RETURN
END

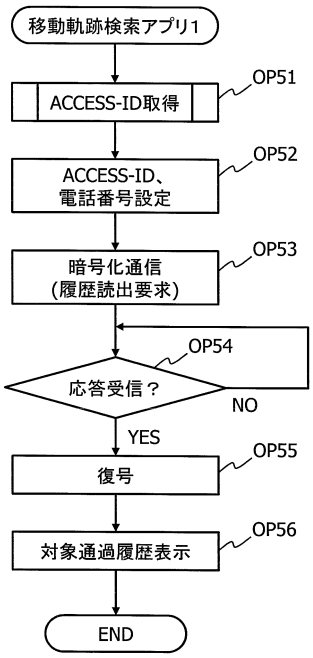
【図９】


通過履歴受信
ICタグリーダ電波停止
OP31
現在日時取得
OP32
自電話番号取得
OP33
通過履歴編集
OP34
ICタグライタ電波照射
OP35
通過履歴書込要求発信
OP36
ICタグライタ電波停止
OP37
無線圏内？
OP38
NO
YES
通過履歴NW送信
OP39
通過履歴保存
OP40
RETURN

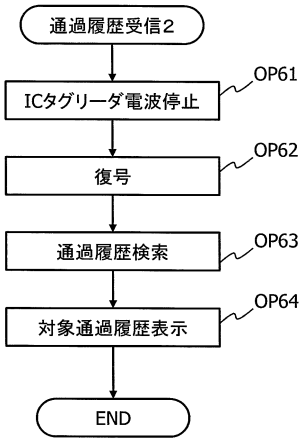
【図１０】


通過履歴NW送信
ACCESS-ID、通過履歴設定
OP41
暗号化通信(履歴保存要求)
OP42
送信完了？
OP43
NO
YES
RETURN

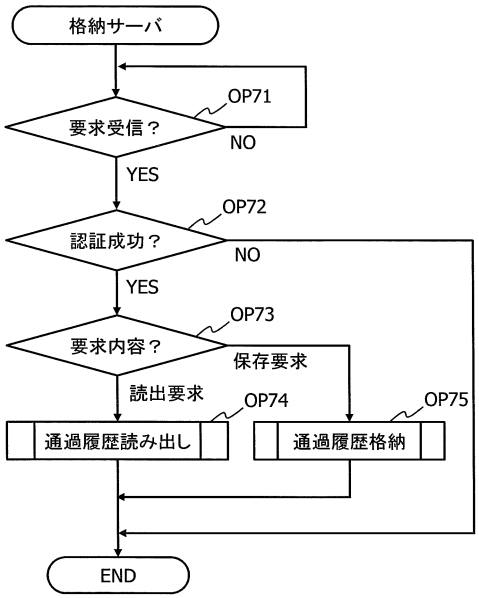
【図１１】



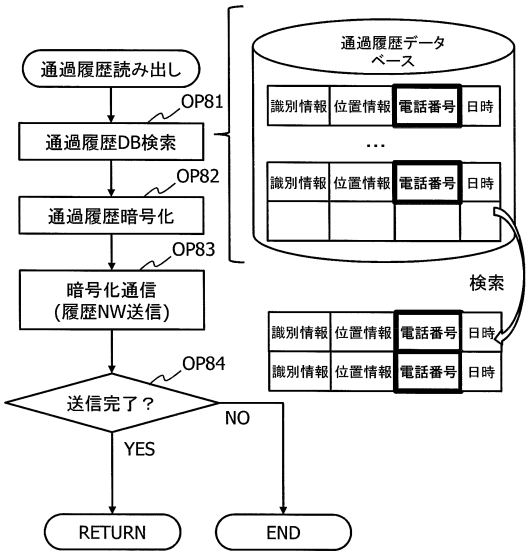
【図１２】



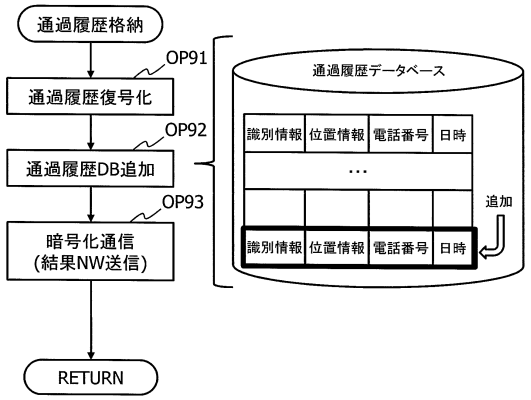
【図１３】



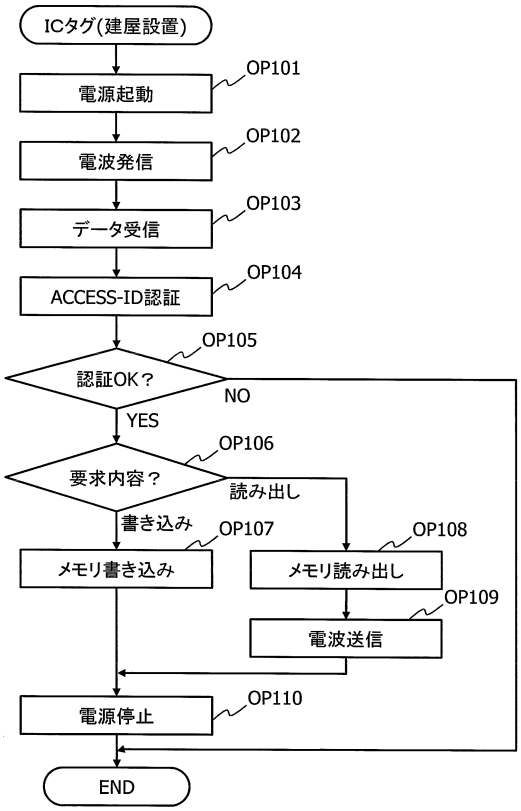
【図１４】



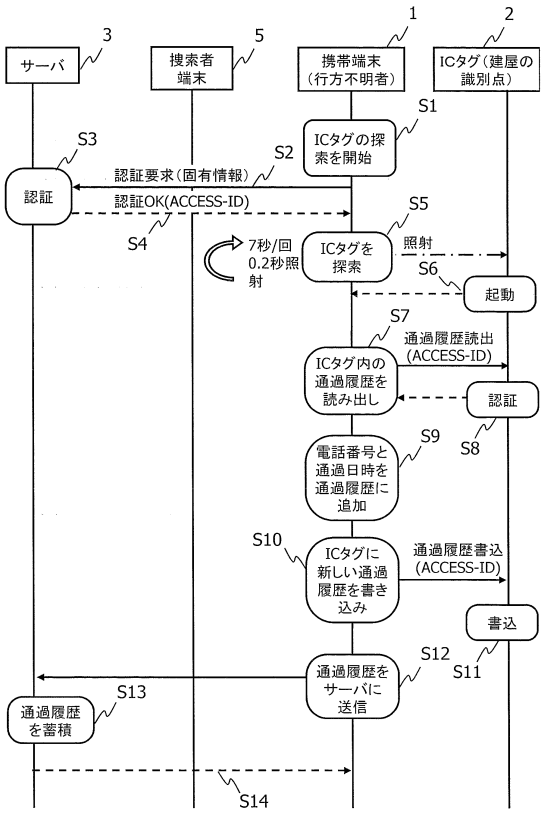
【図１５】



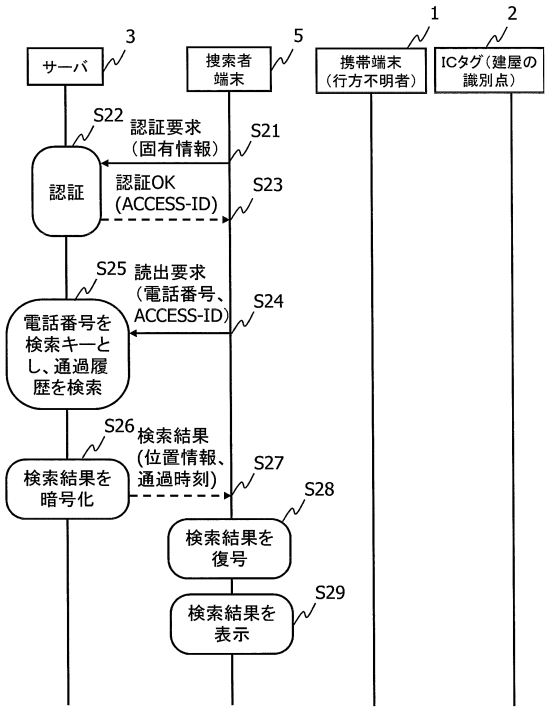
【図１６】



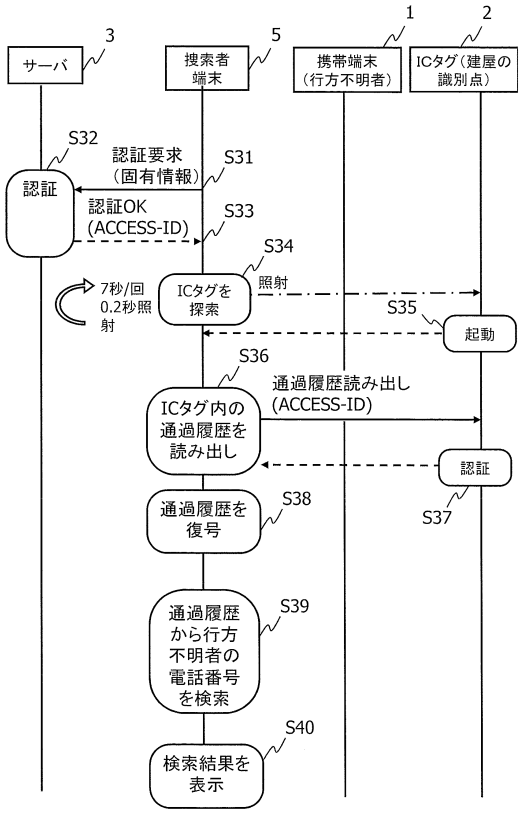
【図１７】



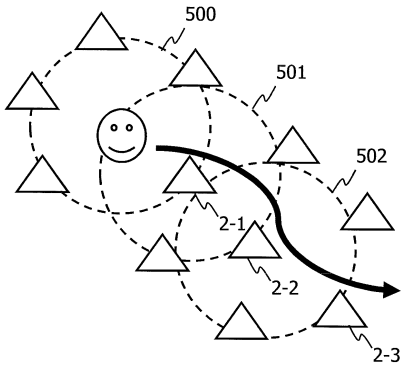
【図１８】



【図１９】



【図２０】



【図２１】

方式	間隔	測位/検出時間	消費電流(1回)	消費電流(1時間)	備考
オートGPS	60秒/回	5.3秒	0.6mAh	35.6mAh	60回/時間
第1実施形態	7秒/回	0.2秒	0.022mAh	11.31mAh	514回/時間

フロントページの続き

審査官　永田　義仁

(56)参考文献　特開２００５－１３５３０２（ＪＰ，Ａ）
特開２０１０－１４０４６４（ＪＰ，Ａ）
特開２００８－１３５０００（ＪＰ，Ａ）
特開２０１０－２３１５７７（ＪＰ，Ａ）
特開２００５－１３５２５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０１Ｃ　２１／００－２１／３６
Ｇ０１Ｃ　２３／００－２５／００
Ｇ０６Ｋ　　７／００－　７／１４
Ｇ０６Ｋ　１７／００－１９／１８
Ｇ０８Ｂ　１９／００－３１／００
Ｇ０８Ｇ　　１／００－９９／００
Ｈ０４Ｂ　　７／２４－　７／２６
Ｈ０４Ｍ　　１／００
Ｈ０４Ｍ　　１／２４－　３／００
Ｈ０４Ｍ　　３／１６－　３／２０
Ｈ０４Ｍ　　３／３８－　３／５８
Ｈ０４Ｍ　　７／００－　７／１６
Ｈ０４Ｍ　１１／００－１１／１０
Ｈ０４Ｍ　９９／００
Ｈ０４Ｗ　　４／００－９９／００