(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5962484号
(P5962484)
(45)発行日　平成28年8月3日(2016.8.3)　(24)登録日　平成28年7月8日(2016.7.8)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62

請求項の数 5　(全 17 頁)

(21)出願番号　特願2012-273628(P2012-273628)
(22)出願日　平成24年12月14日(2012.12.14)
(65)公開番号　特開2014-119888(P2014-119888A)
(43)公開日　平成26年6月30日(2014.6.30)
審査請求日　平成27年8月4日(2015.8.4)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４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
(72)発明者　▲高▼野　あゆみ
神奈川県川崎市中原区上小田中４丁目１番１号　株式会社富士通コンピュータテクノロジーズ内

最終頁に続く

(54)【発明の名称】記憶装置、記憶装置のデータ保護方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
地理上のエリアを示すエリア情報を記憶する第１の記憶領域と、
データを記憶する第２の記憶領域と、
前記第２の記憶領域に記憶されるデータに、記憶装置の位置を示すデータ格納情報を付加するデータ処理部と、
前記記憶装置が前記エリア情報によって示されるエリア内にあるときに、前記第２の記憶領域に記憶された各データのうち、前記データ格納情報が示す位置が前記エリア情報によって示されるエリア内にあるデータを使用可能とする制御部と、
を備えることを特徴とする記憶装置。
【請求項２】
前記エリア情報及び前記データ格納情報は、それぞれ緯度及び経度を示す情報を含み、
前記制御部は、前記エリア情報及び前記データ格納情報に含まれる緯度及び経度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定することを特徴とする請求項１に記載の記憶装置。
【請求項３】
前記エリア情報及び前記データ格納情報は、それぞれ高度を示す情報をさらに含み、
前記制御部は、前記エリア情報及び前記データ格納情報に含まれる緯度、経度、高度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定する

ことを特徴とする請求項２に記載の記憶装置。
【請求項４】
記憶装置の第１の記憶領域に地理上のエリアを示すエリア情報を記憶するステップと、
前記記憶装置の第２の記憶領域にデータを記憶する際に、前記記憶装置の位置を示すデータ格納情報を前記データに付加するステップと、
前記記憶装置が前記エリア情報によって示されるエリア内にあるときに、前記第２の記憶領域に記憶された各データのうち、前記データ格納情報が示す位置が前記エリア情報によって示されるエリア内にあるデータを使用可能とするステップと、
を含むことを特徴とする記憶装置のデータ保護方法。
【請求項５】
コンピュータに、記憶装置の第１の記憶領域に地理上のエリアを示すエリア情報を記憶するステップと、
前記記憶装置の第２の記憶領域にデータを記憶する際に、前記記憶装置の位置を示すデータ格納情報を前記データに付加するステップと、
前記記憶装置が前記エリア情報によって示されるエリア内にあるときに、前記第２の記憶領域に記憶された各データのうち、前記データ格納情報が示す位置が前記エリア情報によって示されるエリア内にあるデータを使用可能とするステップと、
を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、記憶装置、記憶装置のデータ保護方法、及びプログラムに関する。
【背景技術】
【０００２】
ＰＣ（Personal Computer）等の保守作業においては、保守作業員が保守契約を結んでいる顧客のＰＣ等も調整することがある。従来、ＰＣ等の現場調整時やメンテナンス作業時に、保守作業員はＰＣ等に記憶された情報を一時的にＵＳＢ（Universal Serial Bus）メモリ等の外部の記憶装置に記憶することもある。そして、このような保守作業終了後、保守作業員は記憶装置に記憶したデータを消去する。
【０００３】
記憶装置のデータ保護においては、データの漏洩を防止するために種々の方法が用いられている。その方法としては、データの暗号化やデータへのパスワード設定、生体認証等が挙げられる。また、例えば特許文献１においては、利用者が、ＵＳＢメモリの利用場所を、物理サーバに事前登録することで、複数の拠点間を移動するＵＳＢメモリ等の記憶媒体を管理する。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１０－２８７００２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、上記文献に開示の技術においても、保守作業員が記憶装置に記憶したデータの消去を忘れることもあり得る。保守作業員がデータの消去を忘れた場合、同じ記憶装置を使用して他の顧客の保守作業を行う際に、保守作業員が誤って消去し忘れたデータを復号化して保守作業を行ってしまう可能性がある。したがって、依然として情報が漏洩する等のおそれがあり、顧客に不都合が生じることも想定される。さらに、ＵＳＢメモリの利用場所を、物理サーバに事前登録する方法では、管理の柔軟性がないため利用者の負担が大きい。
【０００６】

本発明は上記の事情に鑑みてなされたものであり、その目的とするところは、記憶したデータをより安全かつ柔軟に保管及び使用することが可能な記憶装置、記憶装置のデータ保護方法、及びプログラムを提供することである。

【課題を解決するための手段】

【０００７】

一実施形態による記憶装置は、地理上のエリアを示すエリア情報を記憶する第１の記憶領域と、データを記憶する第２の記憶領域と、第２の記憶領域に記憶されるデータに、記憶装置の位置を示すデータ格納情報を付加するデータ処理部と、記憶装置がエリア情報によって示されるエリア内にあるときに、第２の記憶領域に記憶された各データのうち、データ格納情報が示す位置がエリア情報によって示されるエリア内にあるデータを使用可能とする制御部とを有する。

【発明の効果】

【０００８】

上記の実施形態により、記憶したデータをより安全かつ柔軟に保管及び使用することが可能な記憶装置、記憶装置のデータ保護方法、及びプログラムが実現する。

【図面の簡単な説明】

【０００９】

【図１】図１（ａ）は、第１の実施形態に係る可搬媒体を示す概略構成図であり、図１（ｂ）は、第１の実施形態に係る可搬媒体のデータ保護システムを示す概略構成図である。

【図２】図２は、第１の実施形態に係る可搬媒体のデータ構成を示す概略図である。

【図３】図３は、第１の実施形態においてエリア情報設定時に使用するダイアログを示す概略図である。

【図４】図４は、第１の実施形態におけるエリア情報設定を説明するための平面地図である。

【図５】図５は、第１の実施形態に係る可搬媒体のデータ記憶処理のフローチャートである。

【図６】図６は、第１の実施形態に係る可搬媒体のデータ保護方法を実現する処理のフローチャートである。

【図７】図７は、第１の実施形態に係る可搬媒体のデータ保護方法を実現する処理のサブルーチンを示すフローチャートである。

【図８】図８は、第１の実施形態に係る可搬媒体のデータ表示を示す概略図である。

【図９】図９は、第２の実施形態にけるエリア情報設定を説明するための立体地図である。

【発明を実施するための形態】

【００１０】

以下に、一実施形態に係る記憶装置、記憶装置のデータ保護方法、及びプログラムの詳細について、図面を参照しながら説明する。

【００１１】

図１（ａ）は、第１の実施形態に係る可搬媒体１００を示す概略構成図である。本実施形態では、記憶装置の一例として可搬媒体１００を挙げる。図１（ａ）に示すように、可搬媒体１００は、インターフェイス１０、制御部２０、メモリ３０を備える。インターフェイス１０は、外部装置であるホストとの接続部分である。制御部２０は、可搬媒体１００内の各部を制御して種々の処理を実行する。制御部２０は、例えば、ＣＰＵ（Central Processing Unit）、プログラムコントローラ、プログラム記憶部を備えたワンチップマイコン等である。メモリ３０は、可搬媒体１００に保存するためにホストから送られるデータを記憶する記憶領域である。さらに、メモリ３０は、可搬媒体１００の種々の処理における各種データを記憶する。各部や各処理の詳細については後述する。可搬媒体１００の一例としては、ＵＳＢコントローラを内蔵するＵＳＢ機器が挙げられる。このＵＳＢコントローラの一例として、メモリを有するワンチップマイコンを備えたＵＳＢターゲットコントローラが挙げられる。

【００１２】
次に、図１（ｂ）は、第１の実施形態に係る可搬媒体１００のデータ保護方法を実行するためのデータ保護システム１を示す概略構成図である。
【００１３】
データ保護システム１は、可搬媒体１００と、可搬媒体１００と接続可能なＰＣ２００を備える。ＰＣ２００はホストの一例である。なお、保守作業員（ユーザ）が保守作業を行う際に可搬媒体１００を接続するホストとしては任意のＰＣを選択することができる。ただし、説明の便宜上、本実施形態では、ユーザは、保守契約を結んだ顧客先に、可搬媒体１００及びＰＣ２００を持ち込み、可搬媒体１００をＰＣ２００に接続して保守作業を行うものとする。可搬媒体１００の一例としてはＵＳＢメモリ等が、ＰＣ２００の一例としてはノートＰＣ等がそれぞれ想定される。
【００１４】
図１（ｂ）に示すように、可搬媒体１００は、メイン制御部１１０、認証部１２０、データ管理部１３０を有する。メイン制御部１１０は、エリア判定部１１１とリクエスト処理部１１２を有する。認証部１２０は、ＧＰＳ情報取得部１２１、座標変換部１２２、ホスト接続検出部１２３を有する。データ管理部１３０は、データ処理部１３１、データ記憶領域１３２、設定エリア情報記憶領域１３３を有する。各部及び各領域の詳細については後述する。
【００１５】
メイン制御部１１０は、可搬媒体１００をＰＣ２００に接続したときに、認証部１２０やデータ管理部１３０と連携して、可搬媒体１００内で実行されるデータ保護に関する種々の処理の実行を制御する。エリア判定部１１１は、ＧＰＳ情報取得部１２１が取得したＧＰＳ情報のデータを座標に変換する。さらに、エリア判定部１１１は、当該座標に基づいて、データ記憶領域１３２に記憶されているデータを使用できるエリア内に可搬媒体１００があるか否かを判定する。リクエスト処理部１１２は、ＰＣ２００から可搬媒体１００に対して送信されたリクエストを受信する。そして、リクエスト処理部１１２は、データ記憶領域１３２に記憶されているデータに対する読み取りや書き込み等のリクエストに応じた処理を行う。
【００１６】
認証部１２０は、メイン制御部１１０による制御に基づいて、ＧＰＳ衛星からのＧＰＳ情報の取得、取得したＧＰＳ情報に基づく可搬媒体１００の現在地の座標変換、可搬媒体１００とＰＣ２００との接続を検出する。ＧＰＳ情報取得部１２１は、複数のＧＰＳ衛星から測位情報を取得する。取得された測位情報は、エリア判定部１１１や座標変換部１２２に送られる。座標変換部１２２は、ＧＰＳ情報取得部１２１から送られた測位情報を緯度、経度、高度からなる座標に変換する。変換された座標は、現在地情報としてデータ管理部１３０に送られる。ホスト接続検出部１２３は、可搬媒体１００がホストであるＰＣ２００と接続されているか否かを検出する。
【００１７】
データ管理部１３０は、ＰＣ２００から受信したデータを暗号化したり復号化したりする。また、データ管理部１３０は、座標変換部１２２から送られる現在地情報をデータに付加する。さらに、データ管理部１３０は、ＰＣ２００から受信したエリア情報を記憶する。データ処理部１３１は、ＰＣ２００から受信したデータを暗号化したり復号化したりする。なお、後述するように、データの暗号化及び復号化に使用される暗号化キー及び復号化キーは、ファイル／フォルダ管理情報に記憶される。データ記憶領域１３２は、ＰＣ２００から受信したデータ等を記憶する領域である。設定エリア情報記憶領域１３３は、設定エリア情報を記憶する領域である。この設定エリア情報は、データ記憶領域１３２に記憶されたデータが使用可能となるエリアに関するエリア情報の一例である。本実施形態においては、設定エリア情報記憶領域１３３が第１の記憶領域に対応する。また、データ記憶領域１３２が第２の記憶領域に対応する。
【００１８】

図２に、本実施形態において可搬媒体１００のデータ記憶領域１３２に記憶されるデータの一例としてのファイル又はフォルダの管理情報の構成内容を示す。ユーザが可搬媒体１００にファイル又はフォルダを保存する際に、各ファイル及び各フォルダには、図２に示すファイル／フォルダ管理情報４００が作成されて管理される。ファイル／フォルダ管理情報４００は、ファイルやフォルダに関する基本情報を有する。この基本情報は、ファイル／フォルダ名４００ａと、ファイルやフォルダが格納されるクラスタ番号であるファイル／フォルダ格納クラスタ番号４００ｂである。さらに、ファイル／フォルダ管理情報４００は、ファイルやフォルダの暗号化及び復号化に使用するデータ暗号化キー４００ｃ及びデータ復号化キー４００ｄ、データ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇを有する。データ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇは、本実施形態におけるデータ格納情報の一例である。本実施形態においては、ファイル／フォルダ管理情報４００とは別にファイル又はフォルダの実体５００がデータ記憶領域１３２に記憶されている。ファイル又はフォルダの実体５００は、ファイル／フォルダ管理情報４００の基本情報であるファイル／フォルダ名４００ａとファイル／フォルダ格納クラスタ番号４００ｂに基づいて参照される。

【００１９】

データ処理部１３１は、暗号化キー及び復号化キーを作成する。また、データを暗号化する際にＧＰＳ情報取得部１２１が測位情報を取得する。さらに、座標変換部１２２が当該測位情報を緯度、経度、高度を示す座標に変換する。そして、データ処理部１３１は、変換された座標を取得して、データ格納緯度、データ格納経度、データ格納高度としてファイル／フォルダ管理情報４００に追加する。

【００２０】

図５に、本実施形態におけるデータ記憶領域１３２へのデータの記憶処理のフローチャートを示す。説明の便宜上、データはデータ記憶領域１３２に新規に記憶されるものとする。また、本フローチャートの実行に先立って、可搬媒体１００とＰＣ２００が接続されており、認証処理等の処理が完了して可搬媒体１００は、データを記憶することができる状態になっているものとする。なお、認証処理等の処理の詳細については後述する。

【００２１】

本フローチャートは、データがデータ記憶領域１３２に記憶される際に、メイン制御部１１０によって開始される。そして、メイン制御部１１０が可搬媒体１００内の各部を制御して本フローチャートの処理を進める。まず、Ｓ１０１において、データ処理部１３１によって、記憶するデータのファイル／フォルダ管理情報４００が作成される。Ｓ１０１において作成されるファイル／フォルダ管理情報４００は、基本情報であるファイル／フォルダ名４００ａとファイル／フォルダ格納クラスタ番号４００ｂを有する。次いで、処理はＳ１０３に進む。

【００２２】

Ｓ１０３では、データ処理部１３１が、記憶されるデータの暗号化及び復号化に使用する暗号化キー及び復号化キーを作成する。そして、データ処理部１３１は、作成した暗号化キー及び復号化キーを、Ｓ１０１において作成されたファイル／フォルダ管理情報４００に、それぞれデータ暗号化キー４００ｃ及びデータ復号化キー４００ｄとして付加する。後述するように、データは、設定エリア情報記憶領域１３３に記憶された設定エリア情報に基づいて使用可能あるいは使用不可となる。そこで、Ｓ１０３において、データ処理部１３１は、データが使用可能になる設定エリア情報に基づいて暗号化キー及び復号化キーを作成してもよい。次いで、処理はＳ１０５に進む。

【００２３】

Ｓ１０５では、ＧＰＳ情報取得部１２１が複数のＧＰＳ衛星から測位情報を取得する。また、座標変換部１２２が当該測位情報を緯度、経度、高度を示す座標に変換する。そして、データ処理部１３１は、変換された座標を取得し、座標が示す緯度、経度、高度を、データ格納情報としてそれぞれファイル／フォルダ管理情報４００のデータ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇに付加する。次いで、処理はＳ

１０７に進む。Ｓ１０７では、データ処理部１３１がデータ暗号化キー４００ｃに格納された暗号化キーを使用してデータを暗号化する。データの暗号化が完了すると、メイン制御部１１０はデータの記憶処理を終了する。

【００２４】

なお、データ記憶領域１３２に新規にデータを記憶する場合について説明したが、データ記憶領域１３２の既存のデータを上書きする場合も同様の処理が実行される。この場合、Ｓ１０１においてファイル／フォルダ管理情報４００が既に基本情報、暗号化・復号化キー、データ格納緯度・経度・高度の情報を有している点が異なる。さらに、各情報がＳ１０３やＳ１０５で作成された情報で更新される点が異なる。

【００２５】

次に、本実施形態においてデータが使用可能となる範囲を規定するエリア情報の設定について説明する。本実施形態においては、ユーザは、保守作業に先立って可搬媒体１００に記憶されるデータの使用可能エリアを設定する。図３は、本実施形態におけるエリア情報設定時に使用するエリア情報設定ダイアログ３００である。エリア情報設定ダイアログ３００に関するデータは、データ管理部１３０内の図示しないメモリに記憶されている。可搬媒体１００をＰＣ２００に接続しているときに、メイン制御部１１０は、ＰＣ２００からエリア情報設定のリクエストを受信する。そして、メイン制御部１１０は、エリア情報設定ダイアログ３００に関するデータをデータ管理部１３０から取得してＰＣ２００に送信する。ＰＣ２００は、受信したデータに基づいてエリア情報設定ダイアログ３００を表示部２０１に表示する。

【００２６】

図３に示すように、エリア情報設定ダイアログ３００は、設定するエリア情報の名称を入力するエリア名称入力ボックス３０１と、設定するエリアを規定するためのエリア情報入力ボックス３０２～３０７を有する。設定するエリアは、開始緯度、終了緯度、開始経度、終了経度、開始高度、終了高度によって規定される。ユーザは、エリア情報入力ボックス３０２～３０７にそれぞれの値を入力する。これにより、入力値に基づく所定の範囲の空間を規定する設定エリアが定まる。ユーザは、エリア情報設定ダイアログ３００で各情報の入力を完了して「保存」ボタンを押す。すると、各ボックス３０１～３０７に入力されたデータが設定エリア情報として可搬媒体１００に送信される。可搬媒体１００が設定エリア情報のデータを受信すると、リクエスト処理部１１２が受信したデータを設定エリア情報記憶領域１３３に記憶する。リクエスト処理部１１２が設定エリア情報記憶領域１３３に設定エリア情報を記憶する際は、データはデータ処理部１３１により暗号化される。

【００２７】

ここで、本実施形態におけるエリア情報設定の詳細について具体例を挙げて説明する。図４に、本実施形態において可搬媒体１００を使用して保守作業を行う作業現場の一例としての平面地図の概略図を示す。図４に示すように、ユーザは所在地がそれぞれ異なるＡ、Ｂ、Ｃ、Ｄの各社で保守作業を行うものとする。本実施形態では、ユーザは、図４に示すように、互いに直交するＸ軸及びＹ軸からなる座標を設定するものとする。なお、Ｘ座標は当該平面地図における経度を示し、Ｙ軸は同じく緯度を示す。また、Ａ、Ｂ、Ｃ、Ｄの各社をそれぞれ１社ずつ囲むようにＸ座標Ｘ１～Ｘ３及びＹ座標Ｙ１～Ｙ３を用いた矩形のエリアが設定されるものとする。

【００２８】

例えば、ユーザが、可搬媒体１００を使用して、１日目にＡ社で、２日目にＤ社で保守作業を行うものとする。ユーザは、Ａ社に出向く前にエリア情報設定を行うため、任意の場所で可搬媒体１００をＰＣ２００に接続する。そして、ユーザは、例えばＰＣ２００でエリア情報設定用のアプリケーションを起動する等して、エリア情報設定のリクエストを可搬媒体１００に送る。ＰＣ２００では、可搬媒体１００からエリア情報設定ダイアログ３００に関するデータが受信される。そして、エリア情報設定ダイアログ３００が表示部２０１に表示される。

【００２９】
ユーザは、表示されたエリア情報設定ダイアログ３００のエリア名称入力ボックス３０１に、例えば「Ａ社様用データ格納領域」等、Ａ社用のエリア設定情報であることを示す名称を入力する。また、ユーザは、各入力ボックス３０２～３０５にＡ社が含まれる緯度及び経度の範囲を指定する。例えば、図４に示すように、開始緯度をＸ１、終了緯度Ｘ２、開始経度をＹ２、終了経度をＹ３として、各値をエリア情報設定ダイアログ３００の入力ボックス３０２～３０５にそれぞれ入力する。なお、Ａ社が含まれるように範囲を指定できれば、開始緯度と終了緯度、あるいは開始経度と終了経度を入れ替えて入力してもよい。この例では、Ａ社が含まれるエリアは緯度と経度で指定することができる。このため、ユーザは入力ボックス３０６、３０７に高度を入力しなくてもよい。ユーザは、各入力ボックス３０１～３０５の入力を完了し、「保存」ボタンを押す。なお、ユーザは、エリア情報設定を中止する場合は「キャンセル」ボタンを押す。また、ユーザは、入力ボックスの入力内容を空欄にする場合は「クリア」ボタンを押す。

【００３０】
「保存」ボタンが押されると、各入力ボックスに入力された設定エリア情報のデータが可搬媒体１００のデータ処理部１３１に送られる。データ処理部１３１は、受信した設定エリア情報のデータを暗号化する。そして、データ処理部１３１は、暗号化されたデータを設定エリア情報記憶領域１３３に記憶する。これによりＡ社のエリア情報設定が完了する。なお、ユーザは、Ａ社と同様にＤ社のエリア情報設定を行うことができる。Ｄ社のエリア情報設定については、Ａ社と同様であるため説明は省略する。

【００３１】
ユーザは、Ａ社のエリア情報設定を行った後、Ａ社に出向き、可搬媒体１００を使用して保守作業を行う。ここで、フローチャートを参照しながら本実施形態における可搬媒体のデータ保護を実現する各処理について説明する。便宜上、以下の説明では、各ステップをＳと略記する。図６は、可搬媒体１００で実行されるデータ保護に係る処理の全体フローである。可搬媒体１００がＰＣ２００に接続されると、可搬媒体１００に電源が投入される。さらに、可搬媒体１００のメイン制御部１１０が本フローチャートを開始する。本フローチャートの開始後、処理はＳ２０１に進む。

【００３２】
Ｓ２０１では、メイン制御部１１０により認証処理が実行される。図７に、Ｓ２０１においてメイン制御部１１０により実行される認証処理のサブルーチンのフローチャートを示す。まずＳ３０１において、メイン制御部１１０は、設定エリア情報記憶領域１３３に記憶されている設定エリア情報を取得する。設定エリア情報記憶領域１３３に複数の設定エリア情報が記憶されている場合は、いずれかの設定エリア情報を取得する。次いで、処理はＳ３０３に進む。

【００３３】
Ｓ３０３では、ＧＰＳ情報取得部１２１が、複数のＧＰＳ衛星から測位情報を取得するためのデータを受信する。ＧＰＳ衛星からのデータ受信は、周知の技術を用いて行うため、詳細な説明は省略する。次いで、処理はＳ３０５に進む。Ｓ３０５では、メイン制御部１１０は、Ｓ３０３で各ＧＰＳ衛星からのデータ受信を行った結果、測位情報を取得できたか否かを判定する。測位情報を取得できなかった場合は（Ｓ３０５：Ｎｏ）、Ｓ３０３に戻り、ＧＰＳ衛星からのデータ受信を再試行して測位情報を取得する。測位情報を取得できた場合は（Ｓ３０５：Ｙｅｓ）、処理がＳ３０７に進む。

【００３４】
Ｓ３０７では、座標変換部１２２がＧＰＳ情報取得部１２１から取得した測位情報に基づいて現在地の緯度、経度、高度を示す座標への変換を行う。次いで、処理はＳ３０９に進む。Ｓ３０９では、エリア判定部１１１が、変換された座標がＳ３０１において取得した設定エリア情報が示すエリア内にあるか否かを判定する。そして、エリア判定部は、判定した結果を示すフラグを生成する。生成されたフラグは、設定エリア情報記憶領域１３３のエリア判定テーブル１３３ａに格納される。このフラグは、例えば、座標がエリア内

にある場合は「１」や「ｔｒｕｅ」であり、エリア内にない場合は「０」や「ｆａｌｓｅ」である。なお、判定結果を記憶しておくことができれば、テーブルやフラグを使用する以外に任意の構成を採用すればよい。次いで、処理はＳ３１１に進む。

【００３５】

Ｓ３１１では、Ｓ３０１においてまだ取得していない設定エリア情報が設定エリア情報記憶領域１３３に記憶されているか否かが判定される。他に設定エリア情報が存在する場合は（Ｓ３１１：Ｙｅｓ）、Ｓ３０１に戻り、当該他の設定エリア情報に基づいてＳ３０３～Ｓ３０９の処理を行う。複数の設定エリア情報が設定エリア情報記憶領域１３３に記憶されている場合、Ｓ３０９の処理によって追加される各フラグは、それぞれ別のレコードとしてエリア判定テーブル１３３ａに追加される。したがって、エリア判定テーブル１３３ａには、設定エリア情報ごとの判定結果が格納される。一方、他に設定エリア情報が存在しない場合は（Ｓ３１１：Ｎｏ）、認証処理のサブルーチンが終了し、処理は図６に示すＳ２０３に進む。

【００３６】

Ｓ２０３では、メイン制御部１１０が、Ｓ２０１の認証処理サブルーチンを実行した結果、エリア判定テーブル１３３ａのエリア判定フラグのいずれかが設定エリア内であることを示すか否かを判定する。いずれかのエリア判定フラグが設定エリア内であることを示す場合は（Ｓ２０３：Ｙｅｓ）、処理はＳ２０５に進む。また、いずれのエリア判定フラグも設定エリア内にないことを示す場合は（Ｓ２０３：Ｎｏ）、後述するＳ２０５のホストへの接続検出やＳ２０７のデータの復号化を実行せずに、処理がＳ２０９に進む。

【００３７】

Ｓ２０５では、メイン制御部１１０が、認証部１２０のホスト接続検出部１２３によって可搬媒体１００とホストであるＰＣ２００との接続が確立したことが検出されたか否かを判定する。可搬媒体１００とＰＣ２００との接続が確立したことが検出されている場合は（Ｓ２０５：Ｙｅｓ）、処理はＳ２０７に進む。可搬媒体１００とＰＣ２００との接続が確立されていない場合は（Ｓ２０５：Ｎｏ）、Ｓ２０１に戻り、現在位置に基づく上述の認証処理が再度実行される。

【００３８】

Ｓ２０７では、メイン制御部１１０が、エリア判定テーブル１３３ａに格納されているエリア判定フラグを参照する。そして、メイン制御部１１０は、エリア内にあることを示すフラグを有する設定エリア情報を特定する。さらに、メイン制御部１１０は、特定した設定エリア情報に基づいて、データ記憶領域１３２に記憶された各ファイルや各フォルダを復号化する。具体的には、メイン制御部１１０は、各ファイルや各フォルダのうち、ファイル／フォルダ管理情報４００のデータ格納緯度４００ｅ、経度４００ｆ、高度４００ｇが、上記特定された設定エリア情報が示すエリア内にあるか否かを判定する。そして、ファイル／フォルダ管理情報４００のデータ格納緯度４００ｅ、経度４００ｆ、高度４００ｇが、上記特定された設定エリア情報が示すエリア内にある場合に、メイン制御部１１０は、ファイルやフォルダを復号化する。メイン制御部１１０によるデータの復号化が完了したら、処理がＳ２０９に進む。

【００３９】

Ｓ２０９では、ユーザは、ＰＣ２００を操作して、復号化されたデータに対して読み取りや書き込み等の種々の処理を実行する。ＰＣ２００は、実行される各処理に基づいてメイン制御部１１０のリクエスト処理部１１２にリクエストを送信する。リクエスト処理部１１２は、受信したリクエストに応じた処理を実行する。

【００４０】

リクエスト処理部１１２がＰＣ２００から受信したリクエストに応じてデータを作成したり保存したりする際は、ＧＰＳ情報取得部１２１がＧＰＳ衛星から測位情報を取得する。さらに、座標変換部１２２が取得した測位情報に基づいて現在地の座標に変換する。ＧＰＳ情報取得部１２１及び座標変換部１２２における処理は、上記のＳ３０３～Ｓ３０７における処理と同じであるため、説明は省略する。そして、リクエスト処理部１１２は、

座標変換部１２２により変換された座標を取得する。次いで、リクエスト処理部１１２は、取得した座標に基づいて処理対象のデータのファイル／フォルダ管理情報４００のデータ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇを更新する。なお、データの作成や保存に限らず、データに対して何らかの処理が発生する度に当該更新処理を行う構成としてもよい。

【００４１】

リクエスト処理部１１２によるデータの処理やファイル／フォルダ管理情報４００の更新処理が完了すると、処理はＳ２１１に進む。Ｓ２１１では、メイン制御部１１０が、Ｓ２０７において復号化されたデータやＳ２０９において新たに作成されたデータに対して暗号化キー及び復号化キーを作成した上で暗号化する。作成された暗号化キー及び復号化キーは、暗号化対象のデータのファイル／フォルダ管理情報４００のデータ暗号化キー４００ｃ及びデータ復号化キー４００ｄとして保存される。あるいは、既にデータ暗号化キー４００ｃ及びデータ復号化キー４００ｄの情報が存在する場合は、作成された暗号化キー及び復号化キーで情報が更新される。

【００４２】

Ｓ２１１におけるデータの暗号化が完了すると、処理はＳ２０１に戻り、上記の認証処理やデータの復号化等が再び実行される。このため、例えばユーザがＡ社での保守作業を完了した後で、可搬媒体１００をＰＣ２００に接続したままＡ社から離れた場合でも、図４に示すようにＸ１、Ｘ２、Ｙ２、Ｙ３で規定されるＡ社用の設定エリアの外に出ると、Ｓ２０１の認証処理サブルーチンにより、エリア判定テーブル１３３ａのＡ社用の設定エリア情報に対するエリア判定フラグが「０」や「ｆａｌｓｅ」になる。このため、Ａ社用の設定エリア内で使用可能であったデータは、Ｓ２０７において復号化の対象とはならなくなり使用できなくなる。

【００４３】

ここで、復号化されたデータをＰＣ２００の表示部２０１に表示したときの一例を図８に示す。ここでは、以前ユーザがＡ社、Ｂ社、Ｃ社で保守作業を行っているものとする。このため、データ記憶領域１３２にＡ社用、Ｂ社用、Ｃ社用のフォルダが既に記憶されている。すなわち、図８において、「Ａ社様用データ格納領域」はＡ社内で作成されたフォルダである。ここで、Ａ社内とは、より正確にはＸ１、Ｘ２、Ｙ２、Ｙ３で規定されるエリア内を意味する。また、Ａ社外とは、当該エリア外を意味する。以下、他社についても同様とする。そして、「Ｂ社様用データ格納領域」はＢ社内で、「Ｃ社様用データ格納領域」はＣ社内で、それぞれ作成されたフォルダである。便宜上、図８では、これら２つのフォルダを点線で示す。ただし、これら２つのフォルダは、実際は表示部２０１には表示されないか、表示されてもフォルダを開く等の操作を行うことはできないものとする。

【００４４】

ユーザは、再びＡ社において保守作業を行うためにＡ社に出向く。そして、ユーザが可搬媒体１００をＰＣ２００に接続すると、上記のＳ２０１、Ｓ２０３、Ｓ２０５、Ｓ２０７の処理が実行される。図８には、上記のＳ２０９に進んだときの表示部２０１の表示状態を示す。図８に示すように、Ｓ２０７では、上述の通りＡ社内で作成されたファイルやフォルダが復号化される。このため、ユーザは「Ａ社様用データ格納領域」フォルダ及びフォルダ内のファイルに対して読み取りや書き込み等の作業を行うことができる。一方、ユーザは、Ｂ社用やＣ社用のデータを使用することはできない。

【００４５】

また、ユーザは、「Ａ社様用データ格納領域」フォルダ内あるいはフォルダ外に、新しいフォルダやファイルを作成することができる。上述の通り、作成されたフォルダやファイルのファイル／フォルダ管理情報４００には現在地の座標に基づくデータ格納緯度、経度、高度の各情報が付加される。したがって、「Ａ社様用データ格納領域」フォルダと同様、新たに作成されたフォルダやファイルもＡ社内で使用可能となる。また同様に、新たに作成されたフォルダやファイルはＡ社外では使用できない。

【００４６】

このように、本実施形態においては、ユーザはＡ社内で作成したファイルやフォルダを可搬媒体１００に保存する。これにより当該ファイルやフォルダはＡ社内で使用可能となる。そして、Ａ社外では、これらのファイルやフォルダは使用できない。したがって、Ｂ社内やＣ社内等Ａ社外においてこれらのファイルやフォルダの漏洩を防止することができる。また、本実施形態において、ユーザは、従来の可搬媒体を扱う感覚で可搬媒体１００に対してデータの作業を行うことができる。つまり、本実施形態の処理では、Ｓ１０５の処理により、データ処理部１３１は、ＧＰＳ衛星から取得された測位情報を基に変換された緯度、経度、高度をファイル／フォルダ管理情報４００のデータ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇに付加する。そして、Ｓ２０７の処理により、メイン制御部１１０は、各ファイルや各フォルダのうち、ファイル／フォルダ管理情報４００のデータ格納緯度４００ｅ、経度４００ｆ、高度４００ｇが特定されたエリア内にある場合に、メイン制御部１１０は、ファイルやフォルダを復号化する。このため、ユーザは、データ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇを各ファイルや各フォルダへ付加する処理の実行を意識しない。また、ユーザは、各ファイルや各フォルダへ付加されたデータ格納緯度４００ｅ、データ格納経度４００ｆ、データ格納高度４００ｇがエリア内にあるか否かを判定する処理の実行を意識しない。したがって、ユーザが本実施形態のエリアの判定処理を意識することなく、可搬媒体のデータ保護が実現できる。

【００４７】

また、データが使用可能になるエリアは緯度及び経度により規定されるため、本実施形態におけるデータ保護方法にＧＰＳの測位情報を簡易に利用することができる。さらに、ＧＰＳの測位情報を利用することにより、データが使用可能になるエリアを精確に区分けすることができる。

【００４８】

さらに、データはエリア情報という地理情報に基づいて保護されるため、設定されたエリア内でデータを使用する限り、日を跨いだ作業を行っても支障がない。すなわち、例えば、保守作業員は、交換部品の不良等が原因でＰＣの修理が当日中に終わらず日を改めて作業を行う場合、従来は退避したデータを格納した可搬媒体を保守作業場所の外部に持ち出す際にデータを消去する必要がある。しかし、本実施形態により、その場所で可搬媒体に退避したデータはその場所でしか参照することができない。これにより、保守作業員は、保守作業場所から離れる際に、可搬媒体に退避したデータを削除する必要がない。

【００４９】

また、従来は保守作業完了後に当該保守作業に係るすべてのデータを可搬媒体から消去する運用方法を採るケースが多い。しかし、本実施形態により、可搬媒体に保存したデータを安全に保管することができる。これにより、保守作業後も可搬媒体にデータを残しておき、後日ユーザが解析作業等で保守作業に使用したデータを再度使用することになった場合にも柔軟に対応することが可能となる。

【００５０】

以上が本実施形態に関する説明であるが、データ保護システム１の構成は、上記の実施形態に限定されるものではなく、本発明の技術的思想と同一性を失わない範囲内において種々の変更が可能である。例えば、上記の実施形態では、可搬媒体１００への電力供給は接続先のホストであるＰＣ２００が行う構成としている。しかし、可搬媒体１００が内部電源を有し、ＰＣ２００から取り外した場合でも内部電源により可搬媒体１００内の各部が動作する構成としてもよい。これにより、上記の認証処理をＰＣ２００への接続前に完了しておくことで、可搬媒体１００をＰＣ２００に接続してからデータが使用可能になるまでの時間を短縮することができる。

【００５１】

また、上記の説明では、可搬媒体１００の現在位置を示す情報を、ＧＰＳ衛星から取得した測位情報を座標変換した情報としている。しかし、ＧＰＳを利用する代わりにあるいは加えて、携帯電話の基地局との通信に基づいて現在位置を特定する機構を可搬媒体１０

０に設ける構成としてもよい。これにより、ＧＰＳ衛星との通信を確立できない環境下で保守作業を行う場合でも、可搬媒体１００の現在位置を示す情報を取得することができる。

【００５２】

さらに、例えば、上記の説明では、図４に示すようにエリア情報の設定において２次元の直交座標を用いてエリアを規定した。しかし、２次元のエリアを規定できれば任意の方法及び座標を用いることができる。また、エリアは高度を加味して設定することもできる。図９に、第２の実施形態における、ＸＹＺ座標を用いた３次元の直交座標によるエリア情報の設定例を示す。図９に示すように、互いに直交するＸ軸、Ｙ軸、Ｚ軸を設定する。ここでは、Ｘ座標が経度、Ｙ座標が緯度、Ｚ座標が高度を表す。図９に示すように、１階～４階にそれぞれＥ社～Ｈ社の各社が入っているビルを想定する。そして、ユーザはＥ社とＧ社で保守作業を行うものとする。なお、本実施形態については、エリア設定において第１の実施形態と異なる点を説明する。その他の点については、第１の実施形態と同様であるため、説明は省略する。

【００５３】

本実施形態において、ユーザは、エリア情報設定ダイアログ３００を使用してＥ、Ｇ各社用のエリア設定を行う。図９において、Ｅ社が占有する空間は、Ｘ１とＸ２により規定される経度範囲、Ｙ１とＹ２により規定される緯度範囲、Ｚ１とＺ２により規定される高度範囲によって特定される。そこで、ユーザは、エリア情報設定ダイアログ３００において、エリア名称入力ボックス３０１に、例えば「Ｅ社様用データ格納領域」等の設定エリアがＥ社用であることを示すエリア名称を入力する。さらに、ユーザは、エリア情報入力ボックス３０２～３０７に、開始緯度をＹ１、終了緯度をＹ２、開始経度をＸ１、終了経度をＸ２、開始高度をＺ１、終了高度をＺ２としてそれぞれ値を入力する。なお、Ｘ１とＸ２、Ｙ１とＹ２、Ｚ１とＺ２は互いに入れ替えて入力してもよい。ユーザは、各入力ボックス３０１～３０７の入力を完了したら「保存」ボタンを押す。これにより、Ｅ社用の設定エリア情報が設定エリア情報記憶領域１３３に記憶される。

【００５４】

次いで、ユーザはＧ社用のエリア設定を行う。図９において、Ｇ社が占有する空間は、Ｘ１とＸ２により規定される経度範囲、Ｙ１とＹ２により規定される緯度範囲、Ｚ３とＺ４により規定される高度範囲によって特定される。そこで、ユーザは、各入力ボックスに、設定エリアがＧ社用であることを示すエリア名称や各座標の値を入力し、「保存」ボタンを押す。これにより、Ｇ社用の設定エリア情報が設定エリア情報記憶領域１３３に記憶される。

【００５５】

第１の実施形態において説明したように、Ｓ３０５で取得される測位情報には高度に関する情報も含まれている。そして、Ｓ３０７において変換される座標は、緯度、経度、高度を示す。したがって、本実施形態において、Ｓ３０９では緯度及び経度の他に高度を加味して現在地が設定済みのエリア内に含まれるか否かが判定される。これにより、緯度及び経度が同じであり高度が異なるＥ社及びＧ社を精確に区別して判定することができる。そして、Ｅ社内で作成されたデータはＥ社内で使用可能となり、Ｅ社外では使用できなくなる。また、Ｇ社内で作成されたデータはＧ社内で使用可能となり、Ｇ社外では使用できなくなる。なお、Ｅ、Ｇ各社用に作成したファイルやフォルダの表示は、図８と同様であるため、図示及び説明は省略する。

【００５６】

《コンピュータが読み取り可能な記録媒体》

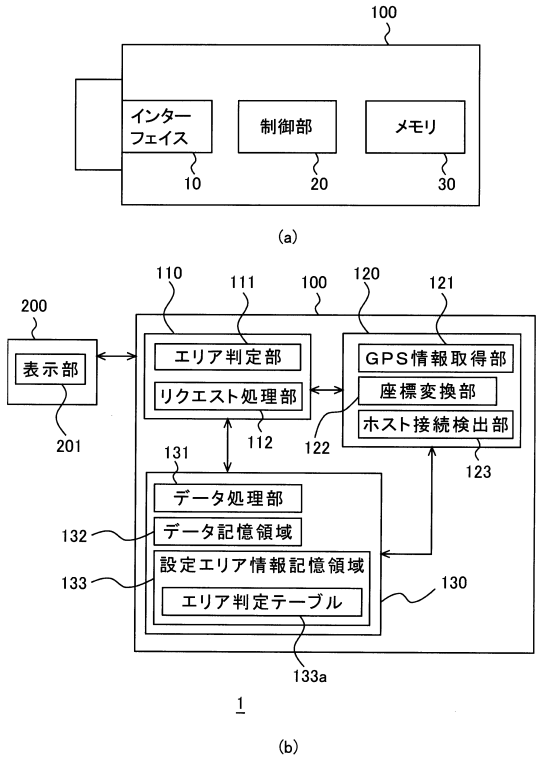
コンピュータその他の機械、装置（以下、コンピュータ等）に上記いずれかの機能を実現させるプログラムをコンピュータ等が読み取り可能な記録媒体に記録することができる。そして、コンピュータ等に、この記録媒体のプログラムを読み込ませて実行させることにより、その機能を提供させることができる。ここで、コンピュータは、例えば、可搬媒体１００の制御部２０等である。

【００５７】
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、フラッシュメモリ等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やＲＯＭ等がある。
【００５８】
以上の実施形態に関し、さらに以下の付記を開示する。
【００５９】
（付記１）
地理上のエリアを示すエリア情報を記憶する第１の記憶領域と、
データを記憶する第２の記憶領域と、
前記第２の記憶領域に記憶されるデータに、記憶装置の位置を示すデータ格納情報を付加するデータ処理部と、
前記記憶装置が前記エリア情報によって示されるエリア内にあるときに、前記第２の記憶領域に記憶された各データのうち、前記データ格納情報が示す位置が前記エリア情報によって示されるエリア内にあるデータを使用可能とする制御部と、
を備えることを特徴とする記憶装置。
【００６０】
（付記２）
前記エリア情報及び前記データ格納情報は、それぞれ緯度及び経度を示す情報を含み、
前記制御部は、前記エリア情報及び前記データ格納情報に含まれる緯度及び経度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定することを特徴とする付記１に記載の記憶装置。
【００６１】
（付記３）
前記エリア情報及び前記データ格納情報は、それぞれ高度を示す情報をさらに含み、
前記制御部は、前記エリア情報及び前記データ格納情報に含まれる緯度、経度、高度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定する
ことを特徴とする付記２に記載の記憶装置。
【００６２】
（付記４）
記憶装置の第１の記憶領域に地理上のエリアを示すエリア情報を記憶するステップと、
前記記憶装置の第２の記憶領域にデータを記憶する際に、前記記憶装置の位置を示すデータ格納情報を前記データに付加するステップと、
前記記憶装置が前記エリア情報によって示されるエリア内にあるときに、前記第２の記憶領域に記憶された各データのうち、前記データ格納情報が示す位置が前記エリア情報によって示されるエリア内にあるデータを使用可能とするステップと、
を含むことを特徴とする記憶装置のデータ保護方法。
【００６３】
（付記５）
前記エリア情報及び前記データ格納情報は、
それぞれ高度を示す情報をさらに含み、
前記データを使用可能とするステップは、前記エリア情報及び前記データ格納情報に含まれる緯度、経度、高度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定する
ことを特徴とする付記４に記載の記憶装置のデータ保護方法。

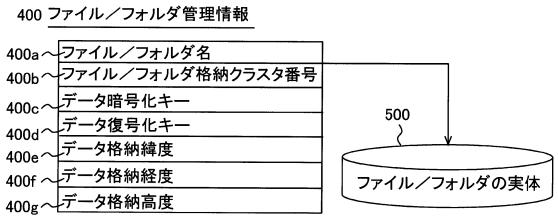
【００６４】
（付記６）
前記エリア情報及び前記データ格納情報は、それぞれ高度を示す情報をさらに含み、
前記データを使用可能とするステップは、前記エリア情報及び前記データ格納情報に含まれる緯度、経度、高度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定する
ことを特徴とする付記５に記載の記憶装置のデータ保護方法。
【００６５】
（付記７）
コンピュータに、記憶装置の第１の記憶領域に地理上のエリアを示すエリア情報を記憶するステップと、
前記記憶装置の第２の記憶領域にデータを記憶する際に、前記記憶装置の位置を示すデータ格納情報を前記データに付加するステップと、
前記記憶装置が前記エリア情報によって示されるエリア内にあるときに、前記第２の記憶領域に記憶された各データのうち、前記データ格納情報が示す位置が前記エリア情報によって示されるエリア内にあるデータを使用可能とするステップと、
を実行させるためのプログラム。
【００６６】
（付記８）
前記エリア情報及び前記データ格納情報は、それぞれ高度を示す情報をさらに含み、
前記データを使用可能とするステップは、前記エリア情報及び前記データ格納情報に含まれる緯度、経度、高度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定する
ことを特徴とする付記７に記載のプログラム。
【００６７】
（付記９）
前記エリア情報及び前記データ格納情報は、それぞれ高度を示す情報をさらに含み、
前記データを使用可能とするステップは、前記エリア情報及び前記データ格納情報に含まれる緯度、経度、高度に基づいて、前記記憶装置が前記エリア情報によって示されるエリア内にあるか否かを決定する
ことを特徴とする付記７に記載の記憶装置のプログラム。
【産業上の利用可能性】
【００６８】
上記の実施形態に係る記憶装置、記憶装置のデータ保護方法、及びプログラムは、顧客の情報処理装置等の保守作業を行う際に、ＰＣ等に記憶されたデータを一時的に退避したり、退避したデータを復元したりする場合に利用することができる。
【符号の説明】
【００６９】
１　データ保護システム
１０　インターフェイス
２０　ＣＰＵ
３０　メモリ
１００　可搬媒体
１１０　メイン制御部
１１１　エリア判定部
１１２　リクエスト処理部
１２０　認証部
１２１　ＧＰＳ情報取得部
１２２　座標変換部
１２３　ホスト接続検出部

１３０　データ管理部
１３１　データ処理部
１３２　データ記憶領域
１３３　設定エリア情報記憶領域
１３３ａ　エリア判定テーブル
２００　ＰＣ
２０１　表示部

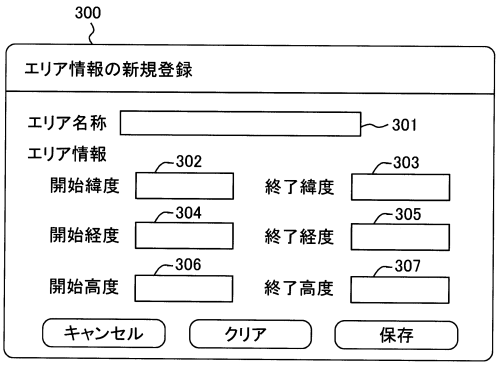
【図１】



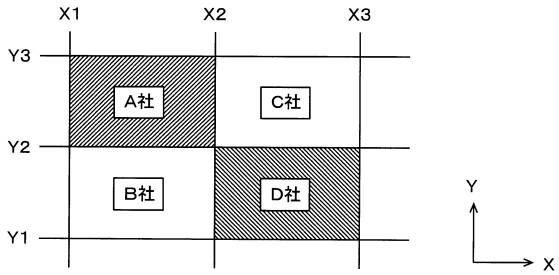
【図２】



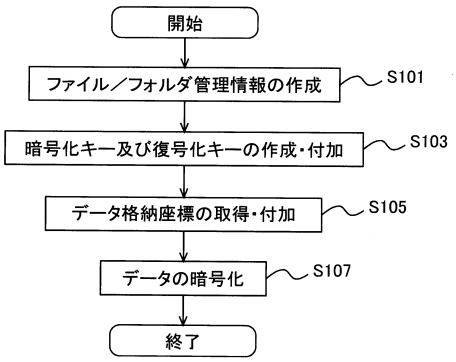
【図３】



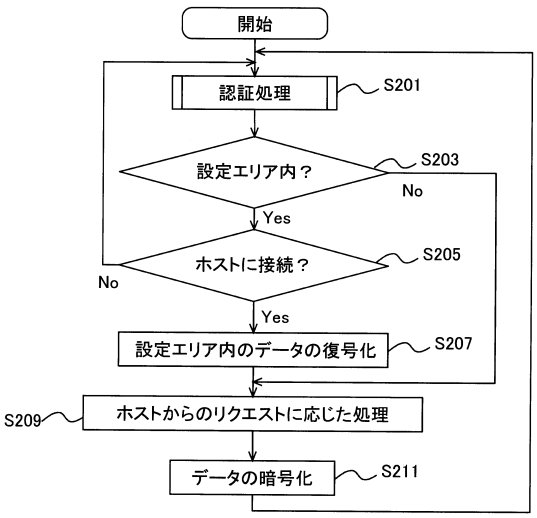
【図４】


X1
X2
X3
Y3
Y2
Y1
A社
C社
B社
D社
Y
X

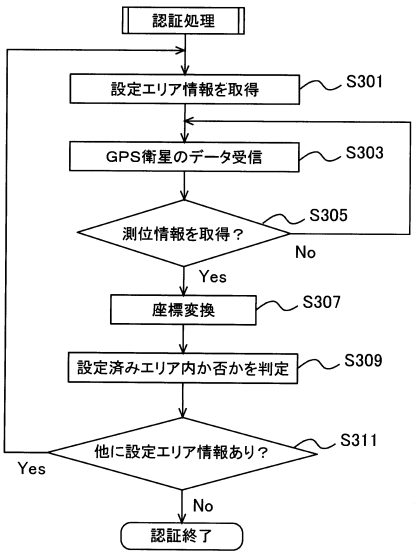
【図５】


開始
ファイル／フォルダ管理情報の作成
S101
暗号化キー及び復号化キーの作成・付加
S103
データ格納座標の取得・付加
S105
データの暗号化
S107
終了

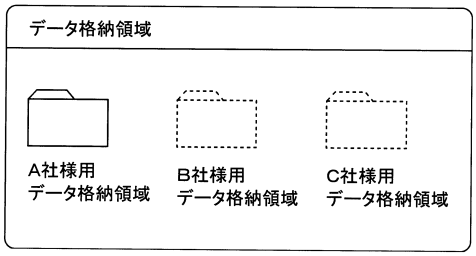
【図６】


開始
認証処理
S201
設定エリア内？
S203
No
Yes
ホストに接続？
S205
No
Yes
設定エリア内のデータの復号化
S207
S209
ホストからのリクエストに応じた処理
データの暗号化
S211

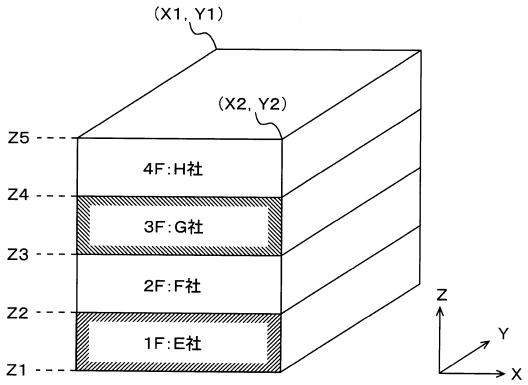
【図７】


認証処理
設定エリア情報を取得
S301
GPS衛星のデータ受信
S303
測位情報を取得？
S305
No
Yes
座標変換
S307
設定済みエリア内か否かを判定
S309
他に設定エリア情報あり？
S311
Yes
No
認証終了

【図８】


データ格納領域
A社様用
データ格納領域
B社様用
データ格納領域
C社様用
データ格納領域

【図９】


(X1, Y1)
(X2, Y2)
Z5
Z4
Z3
Z2
Z1
4F:H社
3F:G社
2F:F社
1F:E社
Z
Y
X

フロントページの続き

(72)発明者　入澤　亨
神奈川県川崎市中原区上小田中４丁目１番１号　株式会社富士通コンピュータテクノロジーズ内
(72)発明者　生島　茂
神奈川県川崎市中原区上小田中４丁目１番１号　株式会社富士通コンピュータテクノロジーズ内
(72)発明者　山田　琢磨
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

審査官　平井　誠

(56)参考文献　特開２００９－０８７２４１（ＪＰ，Ａ）
特開２００８－１９１７３２（ＪＰ，Ａ）
特表２００４－５２８６１６（ＪＰ，Ａ）
特開２００６－１５５２８３（ＪＰ，Ａ）
特開２００３－２５６２８７（ＪＰ，Ａ）
特開平０９－１９０２３６（ＪＰ，Ａ）
特開２００９－２３７６２５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０－６２