(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4533102号
(P4533102)

(45)発行日　平成22年9月1日(2010.9.1)　(24)登録日　平成22年6月18日(2010.6.18)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520F
G06F 21/02	(2006.01)	G06F	12/14	510C
G06K 17/00	(2006.01)	G06F	12/14	530C
H04L 9/32	(2006.01)	G06F	12/14	560D
		G06K	17/00	F

請求項の数 8　(全 18 頁)　最終頁に続く

(21)出願番号　特願2004-334756 (P2004-334756)
(22)出願日　平成16年11月18日 (2004.11.18)
(65)公開番号　特開2005-174315 (P2005-174315A)
(43)公開日　平成17年6月30日 (2005.6.30)
審査請求日　平成19年6月12日 (2007.6.12)
(31)優先権主張番号　特願2003-392377 (P2003-392377)
(32)優先日　平成15年11月21日 (2003.11.21)
(33)優先権主張国　日本国(JP)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100125254
弁理士　別役　重尚
(72)発明者　鈴木　勝也
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　高橋　克

最終頁に続く

(54)【発明の名称】情報処理装置、及び情報処理方法

(57)【特許請求の範囲】

【請求項１】

可搬性記憶媒体から前記可搬性記憶媒体を特定するための第１の特定情報及び前記第１の特定情報とは異なる所定情報を読出す情報読出手段と、

前記可搬性記憶媒体へ前記所定情報を書込む情報書込手段と、

前記情報読出手段が前記可搬性記憶媒体から読出した前記所定情報を記憶する記憶手段と、

前記情報読出手段、前記情報書込手段及び前記記憶手段を制御する制御手段と、

前記情報読出手段により読み出された前記第１の特定情報が前記記憶手段に記憶された第２の特定情報と一致する場合に、前記第１の特定情報に対応するユーザの所定エリアからの退場及び前記所定エリアへの入場を認証する認証手段とを有し、

前記制御手段は、

前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証手段により認証される場合に、前記第１の特定情報と一致した前記第２の特定情報に、前記可搬性記憶媒体から読み出された前記所定情報を対応付けて前記記憶手段に記憶させるとともに前記所定情報を前記可搬性記憶媒体から消去するよう制御し、

前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアへの入場が前記認証手段により認証される場合に、前記記憶手段に前記第２の特定情報と対応付けて記憶された前記所定情報を前記第１の特定情報が読み出された前記可搬

性記憶媒体に書込むよう制御することを特徴とする情報処理装置。
【請求項２】
前記記憶手段は、前記可搬性記憶媒体が前記所定エリアへ入場している入場状態であるか前記所定エリアから退場している退場状態であるかを示す入退場情報を前記第２の特定情報に対応付けて記憶し、
前記認証手段は、前記情報読出手段により読み出された前記第１の特定情報が前記記憶手段に記憶された前記第２の特定情報と一致する場合において、前記入退場情報が前記入場状態を示す場合は前記第２の特定情報に対応するユーザの前記所定エリアからの退場を認証し、前記入退場情報が前記退場状態を示す場合は前記第２の特定情報に対応するユーザの前記所定エリアへの入場を認証し、
前記制御手段は、前記認証手段が前記第２の特定情報に対応するユーザの前記所定エリアへの入場を認証する場合は前記入退場情報を前記退場状態を示す情報から前記入場状態を示す情報に変更し、前記認証手段が前記第２の特定情報に対応するユーザの前記所定エリアからの退場を認証する場合は前記入退場情報を前記入場状態を示す情報から前記退場状態を示す情報に変更するよう前記記憶手段を制御する
ことを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記情報読出手段は、前記所定データを機密にすべきかどうかを示す機密情報を前記可搬性記憶媒体から読出し、
前記制御手段は、前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証手段により認証される場合であって前記機密情報が前記所定情報を機密にすべきことを示す場合に、前記所定情報を前記可搬性記憶媒体から消去するよう制御することを特徴とする請求項１又は２記載の情報処理装置。
【請求項４】
前記可搬性記憶媒体は、非接触にて通信可能な記憶媒体であり、前記情報読出手段は、非接触状態にて前記可搬性記憶媒体から情報を読出し、前記情報書込手段は、非接触状態にて前記可搬性記憶媒体に情報を書込むことを特徴とする請求項１～３の何れか１項に記載の情報処理装置。
【請求項５】
情報処理装置における情報処理方法であって、
可搬性記憶媒体から前記可搬性記憶媒体を特定するための第１の特定情報及び前記第１の特定情報とは異なる所定情報を読出す情報読出ステップと、
前記情報読出ステップにより読み出された前記第１の特定情報が前記情報処理装置が備える記憶手段に記憶された第２の特定情報と一致する場合に、前記第１の特定情報に対応するユーザの所定エリアからの退場及び前記所定エリアへの入場を認証する認証ステップと、
前記情報読出ステップにより読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証ステップにて認証される場合に、前記第１の特定情報と一致した前記第２の特定情報に、前記可搬性記憶媒体から読み出された前記所定情報を対応付けて記憶手段に記憶させる記憶ステップと、
前記情報読出ステップにより読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証ステップにて認証される場合に、前記所定情報を前記可搬性記憶媒体から消去する消去ステップと、
前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアへの入場が前記認証ステップにて認証される場合に、前記記憶手段に前記第２の特定情報と対応付けて記憶された前記所定情報を前記第１の特定情報が読み出された前記可搬性記憶媒体に書込む情報書込ステップとを有することを特徴とする情報処理方法。
【請求項６】
前記記憶手段は、前記可搬性記憶媒体が前記所定エリアへ入場している入場状態であるか前記所定エリアから退場している退場状態であるかを示す入退場情報を前記第２の特定

情報に対応付けて記憶し、
前記認証ステップは、前記情報読出手段により読み出された前記第１の特定情報が前記記憶手段に記憶された前記第２の特定情報と一致する場合において、前記入退場情報が前記入場状態を示す場合は前記第２の特定情報に対応するユーザの前記所定エリアからの退場を認証し、前記入退場情報が前記退場状態を示す場合は前記第２の特定情報に対応するユーザの前記所定エリアへの入場を認証し、
前記情報処理方法は、更に、
前記認証ステップが前記第２の特定情報に対応するユーザの前記所定エリアへの入場を認証する場合は前記入退場情報を前記退場状態を示す情報から前記入場状態を示す情報に変更し、前記認証ステップが前記第２の特定情報に対応するユーザの前記所定エリアからの退場を認証する場合は前記入退場情報を前記入場状態を示す情報から前記退場状態を示す情報に変更する変更ステップを有する
ことを特徴とする請求項５記載の情報処理方法。
【請求項７】
前記情報読出ステップは、前記所定データを機密にすべきかどうかを示す機密情報を前記可搬性記憶媒体から読出し、
前記消去ステップは、前記情報読出ステップにより読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証ステップにて認証される場合であって前記機密情報が前記所定情報を機密にすべきことを示す場合に、前記所定情報を前記可搬性記憶媒体から消去することを特徴とする請求項５又は６記載の情報処理方法。
【請求項８】
前記可搬性記憶媒体は、非接触にて通信可能な記憶媒体であり、非接触状態にて前記可搬性記憶媒体から情報を読出し、非接触状態にて前記可搬性記憶媒体に情報を書込むことを特徴とする請求項５～７の何れか１項に記載の情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、及び情報処理方法に関し、特に、可搬性記憶媒体を用いて入出管理等を行うのに好適な情報処理装置、及び情報処理方法に関する。
【背景技術】
【０００２】
従来、磁気カード等の可搬性のある記憶媒体等を用いて認証を行うことで、部屋（所定エリア）への入退出管理を行うセキュリティシステムが実現されている（特許文献１参照）。
【０００３】
また、非接触ＩＣメモリ［例えば、ＲＦＩＤ（Radio Frequency Identification）タグ］等の可搬性記憶媒体の利用形態として、ＭＦＰ（Multi Function Printer）に可搬性記憶媒体からの情報を読み出す機能を設けることが考えられる。この場合、ＭＦＰは、可搬性記憶媒体から、ＭＦＰ（複合機）が実行すべきジョブ情報を読み出し、この読み出したジョブ情報に基づいてジョブを実行させることが考えられる。なお、ジョブの実行の一例としては、例えば画像データに基づいて用紙に画像をプリントするプリント処理がある。
【特許文献１】特開平１１－３０３４７８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
以上のような利用形態において、可搬性記憶媒体に機密情報（例えば、社外秘、或いは部門外秘等の機密データ）を格納した状態で、この可搬性記憶媒体を入退室が管理される部屋（所定エリア）の外部（社外、或いは部門外等）に持ち出した際には問題となる場合がある。例えば、可搬性記憶媒体を紛失してしまったような場合には、可搬性記憶媒体内に格納された機密情報が第３者により読み出されてしまい、機密情報に関するセキュリテ

ィが低下する可能性がある。

【０００５】

そこで、本発明は、可搬性記憶媒体が所定エリアから持ち出される場合の情報の漏洩を防止するとともに、可搬性記憶媒体に記憶された情報の所定エリア内での利用を可能とする情報処理装置及び情報処理方法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】

【０００６】

上記課題を解決するため、本発明に係る情報処理装置は、可搬性記憶媒体から前記可搬性記憶媒体を特定するための第１の特定情報及び前記第１の特定情報とは異なる所定情報を読出す情報読出手段と、前記可搬性記憶媒体へ前記所定情報を書込む情報書込手段と、前記情報読出手段が前記可搬性記憶媒体から読出した前記所定情報を記憶する記憶手段と、前記情報読出手段、前記情報書込手段及び前記記憶手段を制御する制御手段と、前記情報読出手段により読み出された前記第１の特定情報が前記記憶手段に記憶された第２の特定情報と一致する場合に、前記第１の特定情報に対応するユーザの所定エリアからの退場及び前記所定エリアへの入場を認証する認証手段とを有し、前記制御手段は、前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証手段により認証される場合に、前記第１の特定情報と一致した前記第２の特定情報に、前記可搬性記憶媒体から読み出された前記所定情報を対応付けて前記記憶手段に記憶させるとともに前記所定情報を前記可搬性記憶媒体から消去するよう制御し、前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアへの入場が前記認証手段により認証される場合に、前記記憶手段に前記第２の特定情報と対応付けて記憶された前記所定情報を前記第１の特定情報が読み出された前記可搬性記憶媒体に書込むよう制御することを特徴とする。

【０００７】

また、本発明に係る情報処理方法は、情報処理装置における情報処理方法であって、可搬性記憶媒体から前記可搬性記憶媒体を特定するための第１の特定情報及び前記第１の特定情報とは異なる所定情報を読出す情報読出ステップと、前記情報読出ステップにより読み出された前記第１の特定情報が前記情報処理装置が備える記憶手段に記憶された第２の特定情報と一致する場合に、前記第１の特定情報に対応するユーザの所定エリアからの退場及び前記所定エリアへの入場を認証する認証ステップと、前記情報読出ステップにより読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証ステップにて認証される場合に、前記第１の特定情報と一致した前記第２の特定情報に、前記可搬性記憶媒体から読み出された前記所定情報を対応付けて記憶手段に記憶させる記憶ステップと、前記情報読出ステップにより読み出された前記第１の特定情報に対応するユーザの前記所定エリアからの退場が前記認証ステップにて認証される場合に、前記所定情報を前記可搬性記憶媒体から消去する消去ステップと、前記情報読出手段により読み出された前記第１の特定情報に対応するユーザの前記所定エリアへの入場が前記認証ステップにて認証される場合に、前記記憶手段に前記第２の特定情報と対応付けて記憶された前記所定情報を前記第１の特定情報が読み出された前記可搬性記憶媒体に書込む情報書込ステップとを有することを特徴とする。

【発明の効果】

【０００８】

本発明によれば、可搬性記憶媒体に対応するユーザの所定エリアからの退場が認証される場合に可搬性記憶媒体に記憶された所定情報を消去し、退場が認証されたユーザの所定エリアへの入場が認証される場合に当該ユーザに対応する可搬性記憶媒体に、消去された所定情報を書込むので、所定情報が所定エリア外に漏れるのを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】

【０００９】

以下、本発明を実施するための一形態を、図面に基づいて詳細に説明する。

【００１０】

図１は、本発明の一形態に係る情報処理装置を適用したセキュリティシステムのシステム構成図である。本システムにおいては、門、ドア等の物理的な複数のゲートや物理的な壁（不図示）等によって外界から区分された部屋であるセキュリティエリア（機密エリアとも言う）１００を想定しており、このセキュリティエリア１００内には、セキュリティサーバ１０３、ＭＦＰ（複合機）１０５、文書サーバ１０６、清算装置１０８が配備されている。なお、門、ドア等の物理的な複数ゲートには、これらゲートを開閉制御するゲート制御部１０１が設けられている。そして、ゲートが閉じられた状態ではセキュリティエリア１００への入退室が禁止され、ゲートが開けられた状態ではセキュリティエリア１００への入退室が許可される。

【００１１】

また、複数のゲートの各々には、ＲＦＩＤタグ（非接触ＩＣ）１０４内の不揮発性メモリ２０１（図２参照）にアクセスするためのリーダ／ライタ１０９も設置されている。また、各ゲートに設置された各リーダ／ライタ１０９は、第１のネットワーク１０２によって相互に接続されており、この第１のネットワーク１０２には、ゲート制御部１０１、セキュリティサーバ１０３も接続されている。

【００１２】

図８に示したように、セキュリティサーバ１０３は、リーダ／ライタ１０９と情報（データ）の入出力をするためのＩ／Ｆ部８０１と、セキュリティサーバ１０３を制御するための制御部８０２と、制御部８０２により制御され、後述するテーブルデータ８０４等を記憶するハードディスク等の記憶部８０３とを有する。なお、この記憶部８０３には、図５のフローチャートにおけるステップＳ５０３～Ｓ５０５、図６のフローチャートにおけるステップＳ６０３，Ｓ６０４に対応するアプリケーションプログラムも格納されている。

【００１３】

このようなネットワーク構成の下で、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１に格納されたユーザＩＤ４０１（図４参照）をリーダ／ライタ１０９で読み出してセキュリティサーバ１０３に転送し、このセキュリティサーバ１０３にて当該ユーザの入退出を管理すると共に、ゲート制御部１０１を介してゲートを開閉することにより、セキュリティエリア１００を形成している。

【００１４】

なお、本実施形態では、セキュリティサーバ１０３によるユーザの入退出管理に応じて、物理的なゲートをゲート制御部１０１により開閉制御しているが、必ずしも物理的なゲートをゲート制御部１０１により開閉制御する必要はない。

【００１５】

また、後で詳細に説明するように、機密データ（ジョブ情報、コマンドを含む）が格納されＲＦＩＤタグ１０４をセキュリティエリア１００の外に持ち出す場合は、ＲＦＩＤタグ１０４内の機密データをリーダ／ライタ１０９で読み出してセキュリティサーバ１０３に退避すると共に、ＲＦＩＤタグ１０４内の機密データを消去することにより、セキュリティエリア１００外で機密データが第３者に漏洩するのを防止している。

【００１６】

また、ＲＦＩＤタグ１０４をセキュリティエリア１００の中に再度持ち込む場合に、セキュリティサーバ１０３に退避した機密データをリーダ／ライタ１０９を介してＲＦＩＤタグ１０４に書き戻すことにより、セキュリティエリア１００内で機密データを自由に利用できるようにしている。

【００１７】

セキュリティエリア１００内のＭＦＰ（複合機）１０５、清算装置１０８には、それぞれ、リーダ／ライタ１０５ａ、１０８ａが搭載されており、後述するように、セキュリティエリア１００内では、ＭＦＰ（複合機）１０５、清算装置１０８は、それぞれリーダ／ライタ１０５ａ、１０８ａを介して、ＲＦＩＤタグ１０４内のメモリに対して自由にアクセスできるように構成されている。

【００１８】
なお、第１のネットワーク１０２は、機密性を向上させるため、外界のネットワーク（インターネット等）とは物理的に分離されていることが望ましいが、物理的に分離することなく、ゲートウェイ等により情報的に分離するようにしてもよい。
【００１９】
ＭＦＰ１０５と文書サーバ１０６は、第２のネットワーク１０７を介して接続されている。この第２のネットワーク１０７は、ＬＡＮ、ＳＡＮ（Ｓｔｏｒａｇｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）等により構成されているが、必ずしも第１のネットワーク１０２と物理的に接続されている必要はない。
【００２０】
ＭＦＰ１０５に対するＲＦＩＤタグ１０４の利用形態としては、ＭＦＰ１０５に搭載されたリーダ／ライタ１０５ａにＲＦＩＤタグ１０４をかざすことで、このＲＦＩＤタグ１０４に格納されたＦＡＸ送信先情報、電子メールアドレス、文書サーバ１０６に格納された文書データの位置情報等を非接触にてＭＦＰ１０５にダウンロードし、それぞれＦＡＸ送信、電子メール送信、文書印刷出力を実行させること等が可能である。また、ＭＦＰ１０５に搭載されたリーダ／ライタ１０５ａにＲＦＩＤタグ１０４を近づけた状態で、ＭＦＰ１０５の操作部（不図示）からＦＡＸ送信先情報、メールアドレス、文書サーバ１０６に格納された文書データの位置情報等を入力し、リーダ／ライタ１０５ａを介して非接触にてＲＦＩＤタグ１０４に格納することも可能である。
【００２１】
清算装置１０８は、例えば食堂等に設置されており、この清算装置１０８に対するＲＦＩＤタグ１０４の利用形態としては、例えば清算装置１０８がＲＦＩＤタグ１０４に格納されたユーザＩＤ等に基づいて清算処理を行うことが可能である。この際、清算処理としては、予めプリペイドカード方式で入金を行っておくことで、ＲＦＩＤタグ１０４に格納された残高情報を元に清算する方式でも、或いは清算装置１０８に接続された清算用サーバ（不図示）によって、ユーザ毎の代金情報を上記清算サーバ内に積算・記憶し、１ヶ月等の間隔で清算を行うような構成でもよい。また、毎回の食事の内容等を上記清算サーバ又はＲＦＩＤタグ１０４に格納し、後から履歴を参照できる構成にしてもよい。
【００２２】
上記ＭＦＰ１０５及び、清算装置１０８に対するＲＦＩＤタグ１０４の利用形態は、あくまでも一例であり、上記に説明した形態以外にも種々の形態に適用できる。なお、ＲＦＩＤタグ１０４は、上記ＭＦＰ１０５、清算装置１０８以外のセキュリティエリア１００内の各種の電子情報機器で利用することができる。
【００２３】
［ＲＦＩＤタグ］
図２は、ＲＦＩＤタグ１０４の構成を示すブロック図である。ＲＦＩＤタグ１０４は、非接触ＩＣチップ、或いはデータキャリアとも呼ばれ、リーダ／ライタと無線で（すなわち非接触で）交信することが可能となっている。本実施形態では、カード型のＲＦＩＤタグを想定しており、このカード型ＲＦＩＤタグ内には、以下のデバイスを内蔵した非接触ＩＣチップが内包されている。
【００２４】
すなわち、ＲＦＩＤタグ（非接触ＩＣチップ）１０４には、不揮発性メモリ２０１、電波を送受信するためのアンテナ部２０２、共振コンデンサ部２０３、電流の整流・平滑を行うための電力生成部２０４、電波の復調・変調を行うための復変調回路２０５、及び制御部２０６が形成されている。このＲＦＩＤタグ１０４は、バッテリ等の電源を内蔵しておらず、リーダ／ライタから供給される電波に基づいて電力を誘電している。
【００２５】
すなわち、アンテナ部２０２は、共振コンデンサ部２０３との組み合わせで共振回路を形成している。一方、リーダ／ライタは、後述するように、常時、電力生成用の電波（交流磁界）を発している。このリーダ／ライタにＲＦＩＤタグ１０４をかざすと、ＲＦＩＤ

タグ１０４内の上記共振回路には電磁誘導作用により誘導電流が発生する。この誘導電流は、電力生成部２０４に出力され、電力生成部２０４は、入力された誘導電流を整流・平滑して所定電圧の電力を生成し、不揮発性メモリ２０１、制御部２０６、復変調回路２０５に供給する。制御部２０６は、ＲＦＩＤタグ１０４を全体的に制御するものである。

【００２６】

リーダ／ライタは、電力生成用の電波信号の他に各種のデータに係る電波信号も同時に送信しており、このデータに係る電波信号は、復変調回路２０５によって復調され、制御部２０６の制御の下に不揮発性メモリ２０１に書き込まれる。また、制御部２０６は、不揮発性メモリ２０１からデータを読み出し、復変調回路２０５によって変調してアンテナ部２０２を介して電波信号として送信する。

【００２７】

なお、制御部２０６は、ＲＯＭ（図示省略）を内蔵しており、このＲＯＭには、図５のフローチャートにおけるステップＳ５０１～Ｓ５０２、Ｓ５０６,Ｓ５０９、図６のフローチャートにおけるステップＳ６０１～Ｓ６０２、Ｓ６０６～Ｓ６０７に対応するアプリケーションプログラムが格納されている。ただし、このアプリケーションプログラムは、不揮発性メモリ２０１に格納してもよい。

【００２８】

［リーダ／ライタ］

図３は、リーダ／ライタ１０９、１０５ａ、１０８ａの構成を示すブロック図である。リーダ／ライタ１０９、１０５ａ、１０８ａは、電波信号を送信するための送信アンテナ部３０１と、Ｉ／Ｆ部３０６から入力される信号を送信アンテナ部３０１から送信するデータ信号へ変調する変調回路３０２と、電波信号を受信する受信アンテナ部３０３、受信アンテナ部３０３より受信した電波信号をＩ／Ｆ部３０６から出力するための信号へ復調する復調回路３０４、上位機器（本実施形態では、セキュリティサーバ１０３）との通信を行うＩ／Ｆ部３０６、及び制御部３０５を有する。そして、制御部３０５は、送信アンテナ部３０１、変調回路３０２、受信アンテナ部３０３、復調回路３０４、及びＩ／Ｆ部３０６を制御する。なお、送信アンテナ部３０１には、電波信号を発するため電力を生成する交流電源３０７が接続されている。

【００２９】

制御部３０５は、セキュリティサーバ１０３からの指示により、変調回路３０２を用いて電力を供給するための電波、及び送信するデータを変調して、送信アンテナ部３０１を介して電波を発信させる。また、制御部３０５は、受信アンテナ部３０３で受信した電波信号を、復調回路３０４により復調させた後、データ信号として扱えるように変換することができる。つまり、制御部３０５は、送信アンテナ部３０１から電波信号を発信させることで送信アンテナ部３０１の送信範囲内に存在するＲＦＩＤタグ１０４の不揮発性メモリ２０１へ情報（データ）を書き込むことができる。制御部３０５は、受信アンテナ部３０３で受信された電波信号を復調回路３０４にて復調させることで受信アンテナ部３０３の受信範囲内に存在するＲＦＩＤタグ１０４の不揮発性メモリ２０１から情報（データ）を読み込むことができる。

【００３０】

なお、制御部３０５は、ＲＯＭ（図示省略）を内蔵しており、このＲＯＭには、図５のフローチャートにおけるステップＳ５０１～Ｓ５０２，Ｓ５０５～Ｓ５１１、図６のフローチャートにおけるステップＳ６０１～Ｓ６０２，Ｓ６０５～Ｓ６０８に対応するアプリケーションプログラムが格納されている。

【００３１】

［ＲＦＩＤタグの格納データ］

図４は、ＲＦＩＤタグ１０４の不揮発性メモリ２０１に格納されたデータを示す概念図である。

【００３２】

ＲＦＩＤタグ１０４内の不揮発性メモリ２０１には、当該ＲＦＩＤタグ１０４の所有権

者のユーザＩＤ４０１と個別データ４０２が格納されている。このユーザＩＤ４０１としては、各ＲＦＩＤタグ１０４に対してそれぞれに固有の値（数値、記号等）が割り振られており、このユーザＩＤ４０１に基づいて当該ＲＦＩＤタグ１０４を所有するユーザを認証することができる。すなわち、各ＲＦＩＤタグ１０４内の不揮発性メモリ２０１に格納された各ユーザＩＤ４０１は、本システムの運用前に予めセキュリティサーバ１０３に登録されており、例えばゲートを通過する際に、リーダ／ライタ１０９によりＲＦＩＤタグ１０４からユーザＩＤ４０１を読み取り、セキュリティサーバ１０３に登録されたユーザＩＤ等と照合することで、当該ユーザがゲートを通過しても良いか否かを判断し（これを認証と呼ぶ）、入場／退出した旨がセキュリティサーバ１０３に記録される。

【００３３】

個別データ４０２は、１つのＲＦＩＤタグ１０４内に１つ又は複数の個別データ４０２が格納されている。各個別データ４０２は、それぞれ個別データＩＤ４０３、データ本体４０４、機密フラグ４０５によって構成されている。

【００３４】

個別データＩＤ４０３は、各個別データ４０２（すなわち、データ本体４０４）を識別するためのＩＤであり、電力生成用の電波信号個別データ４０２毎に固有の値（数値、記号等）が割り振られており、ユーザＩＤ４０１と組み合わせることで、ＭＦＰ１０５や清算装置１０８に対して、データ本体４０４の各種データを授受することができる。

【００３５】

データ本体４０４は、実際に読み書きされて各種処理に用いられる個別データ４０２の実体をなすデータであり、前述のように、ＭＦＰ１０５に関するデータとしては、ＦＡＸ送信先情報、電子メールアドレス、文書サーバ１０６に格納された文書データの位置情報等が読み書きされ。なお、ＭＦＰ１０５操作部から入力された情報を追加、或いは上書きすることも可能である。

【００３６】

また、清算装置１０８に関するデータとしては、予め入金された金銭データや、食事の履歴情報が読み書きされる。なお、金銭データは清算装置１０８に接続された清算サーバ（不図示）によってのみ書き換えられる情報である。食事の履歴情報は、清算装置１０８によって書き換えられる情報である。

【００３７】

機密フラグ４０５は、個別データ４０２毎に設定される情報であり、当該個別データ４０２が機密情報を含むのか否かを表している。本実施形態では、機密フラグ４０５がＯＮ（１）の場合は機密情報を含み、ＯＦＦ（０）の場合は機密情報を含まないものと定義している。この機密フラグ４０５は、セキュリティサーバ１０３に接続されるリーダ／ライタ１０９でのみ書き込みが可能となっている。

【００３８】

なお、本明細書では、機密フラグ４０５がＯＮとなっている個別データ４０２については、その個別データ４０２の全部が機密事項ではなく一部だけが機密事項となっている場合も、当該個別データ４０２全体を機密データと呼んでいる（特許請求の範囲も同趣旨）。

【００３９】

［退場処理］

次に、セキュリティエリア１００の内部から外部に退出する場合の処理を、図５のフローチャートに基づいて説明する。なお、図５は、少なくともセキュリティサーバ１０３とリーダ／ライタ１０９で構成される情報処理装置が実行する動作である。

【００４０】

ステップＳ５０１：リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグタグ１０４と通信可能か否かを判定する。ＲＦＩＤタグ１０４には、リーダ／ライタ１０９から発せられた電波により電力が誘電されるので、リーダ／ライタ１０９の通信可能範囲にユーザがＲＦＩＤタグ１０４を近づけると、リーダ／ライタ１０９はＲＦＩＤタグ１０４との通

信が可能となる。なお、リーダ／ライタ１０９にＲＦＩＤタグ１０４を近づけて、後述する所定の認証処理を実行しないとゲートが開かないようにしているので、ユーザはセキュリティエリア１００から退場するためにはＲＦＩＤタグ１０４をリーダ／ライタ１０９に近づける必要がある。

【００４１】

ステップＳ５０２：リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１から、ユーザＩＤ４０１を読み出してセキュリティサーバ１０３に送信する。

【００４２】

ステップＳ５０３：セキュリティサーバ１０３は、リーダ／ライタ１０９から受信したユーザＩＤ４０１が、当該セキュリティサーバ１０３に登録されており、かつ、そのユーザＩＤ４０１に係るユーザの入退出の状況が「入場」となっているか否かを判別することにより、当該ユーザの退出を認証するか否かを判別する。

【００４３】

具体的には、セキュリティサーバ１０３の制御部８０２は、リーダ／ライタ１０９の制御部３０５を介して入力されるユーザＩＤが、セキュリティサーバ１０３内のテーブルデータ８０４に記憶されているユーザＩＤと一致し、かつそのユーザＩＤに対応付けられた入退場状況が「入場」となっている場合には、ユーザの退出を認証することとし、認証する旨の情報をＩ／Ｆ部８０１を介してリーダ／ライタ１０９へ送信する。そして、セキュリティサーバ１０３は、ユーザの退出を認証する場合はステップＳ５０５へ処理を進め、ユーザの退出を認証しない場合はステップＳ５０４へ処理を進める。

【００４４】

ここで、ＲＦＩＤタグ１０４には、そのＲＦＩＤタグ１０４を特定するための情報としてＲＦＩＤタグ１０４の所有者であるユーザＩＤが予め不揮発性メモリ２０１の記憶領域の一部に記憶されているものとする。また、セキュリティサーバ１０３には、ユーザＩＤを管理するためのテーブルデータ８０４（例えば、図７に示す内容を記憶する）が記憶されており、テーブルデータ８０４には、ＲＦＩＤタグ１０４を特定するためのユーザＩＤと対応付けて、ユーザ（言い換えれば、ユーザＩＤで特定されるＲＦＩＤタグ１０４）の入退室状況、及び後述する機密情報が記憶されているものとする。なお、機密情報等を含むテーブルデータ８０４は、セキュリティサーバ１０３内のハードディスク等の記憶部８０３に記憶させておくものとする。

【００４５】

ステップＳ５０４：セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録されていない、或いは登録されていても当該ユーザＩＤ４０１に係るユーザの入退出の状況が「退出」となっている場合（この場合は、過去に不正にセキュリティエリア１００内に入場したことを意味する）は、当該ユーザの退出を認証せずに、所定の警告処理を行う。この警告処理としては、例えば、ゲートに設置された表示装置（図示省略）に警告メッセージを表示する、ゲートに設置されたスピーカ（図示省略）により警告音を鳴らす、或いはゲート制御部１０１によりゲートを一時的に閉鎖状態にロックさせること等が考えられる。

【００４６】

ステップＳ５０５：セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録され、かつ当該ユーザＩＤ４０１に係るユーザの入退出の状況が「入場」となっている場合は、当該ユーザの退出を認証し、当該ユーザＩＤ４０１に係るユーザの入退出の状況を「退場」に変更し、当該ユーザの退出を認証した旨の情報をリーダ／ライタ１０９に通知する。

【００４７】

なお、リーダ／ライタ１０９の制御部３０５は、セキュリティサーバ１０３からユーザの退出を認証した旨の情報を受信すると、ユーザが退出したことを示す情報（言い換えれば、ＲＦＩＤタグ１０４がセキュリティエリア１００に存在しない「退場」状態にあるこ

とを示す情報）をＲＦＩＤタグ１０４の不揮発性メモリ２０１に書き込むよう変調回路３０２を制御する。

【００４８】

なお、本実施形態では、テーブルデータ８０４が使用する記憶部８０３の記憶容量を削減するため、セキュリティサーバ１０３の記憶部８０３は、最新の入退出状況だけを記憶しているが、過去の全て、或いは複数の入退出状況（履歴）を記憶するようにしてもよい。

【００４９】

ステップＳ５０６：リーダ／ライタ１０９の制御部３０５は、当該ユーザの退出を認証した旨の情報をセキュリティサーバ１０３から受信すると、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１から、１つの個別データ４０２に係る個別データＩＤ４０３と機密フラグ４０５を読み出して、セキュリティサーバ１０３へ送信する。

【００５０】

ステップＳ５０７：セキュリティサーバ１０３の制御部８０２は、個別データ４０２に対応する機密フラグ４０５がＯＮとなっているか否かを判別する。

【００５１】

ステップＳ５０８：セキュリティサーバ１０３の制御部８０２は、機密フラグ４０５がＯＮとなっていると判断した場合は、リーダ／ライタ１０９の制御部３０５とＲＦＩＤタグ１０４の制御部２０６とを協働させて、対応する個別データ４０２（データ本体４０４）をＲＦＩＤタグ１０４内の不揮発性メモリ２０１から読み出して、セキュリティサーバ１０３に送信させる。

【００５２】

ここで、ＲＦＩＤタグ１０４の不揮発性メモリ２０１から個別データ４０２を受信したセキュリティサーバ１０３の制御部８０２は、受信した個別データ４０２をステップＳ５０３にて認証したユーザＩＤと対応付けてテーブルデータ８０４として記憶部８０３に記憶（退避）させる。

【００５３】

ステップＳ５０９：リーダ／ライタ１０９の制御部３０５は、ステップＳ５０８でセキュリティサーバ１０３の記憶部８０３に退避させた個別データ４０２を、不揮発性メモリ２０１から消去して、ステップＳ５１０に進む。一方、ステップＳ５０７で機密フラグ４０５がＯＦＦとなっていると制御部８０２が判断した場合、セキュリティサーバ１０３の制御部８０２及びリーダ／ライタ１０９の制御部３０５は、ステップＳ５０８の退避処理、ステップＳ５０９の消去処理を行うことなく、ステップＳ５１０に進む。

【００５４】

ステップＳ５１０：リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１を参照し、機密フラグ４０５のチェック等を行っていない次の個別データ４０２が存在するか否かを判別する。

【００５５】

その結果、機密フラグ４０５のチェック等を行っていない次の個別データ４０２が存在すれば、リーダ／ライタ１０９の制御部３０５は、ステップＳ５０６に戻り、当該次の個別データ４０２に対して同様の処理を行う。一方、全ての個別データ４０２に対する機密フラグ４０５のチェック等の処理が完了した場合はステップＳ５１１へ進み、リーダ／ライタ１０９の制御部３０５は、例えばゲート制御部１０１によりゲートをオープンさせる等の退場処理を行い、本処理を終了する。

【００５６】

以上説明したように、リーダ／ライタ１０９の制御部３０５は、復調回路３０４がＲＦＩＤタグ１０４から読み出した入退場の情報が「入場」を示す場合であってＲＦＩＤタグ１０４に記憶された個別データ４０２の機密フラグがＯＮとなっている場合は、ＲＦＩＤ

タグ１０４に記憶された個別データ４０２を読み出し不可能とするように、個別データ４０２の退避及び削除を行う。また、リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４に、入退場の情報として「退場」を示す情報を書き込むように変調回路３０２を制御する。

【００５７】

なお、セキュリティサーバ１０３の制御部８０２は、ＲＦＩＤタグ１０４の不揮発性メモリ２０１に記憶されている複数の個別データ（図４の４０２、４０６、４０７、４０８）の各々について機密フラグが設定されているかをステップＳ５０７にて判断するので、複数の個別データのうち機密にすべきデータを不揮発性メモリ２０１から確実に消去するとともに、機密にする必要のないデータを不揮発性メモリ２０１に記憶させたままとすることができる。

【００５８】

［入場処理］

次に、ＲＦＩＤタグ１０４を携帯するユーザが、セキュリティエリア１００の外部からセキュリティエリアの内部に入場する場合の処理を、図６のフローチャートに基づいて説明する。なお、図６は、少なくともセキュリティサーバ１０３とリーダライタ１０９で構成される情報処理装置が実行する動作である。

【００５９】

ステップＳ６０１：リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４と通信可能か否かを判定する。ＲＦＩＤタグ１０４には、リーダ／ライタ１０９から発せられた電波により電力が誘電されるので、リーダ／ライタ１０９の通信可能範囲にユーザがＲＦＩＤタグ１０４を近づけると、リーダ／ライタ１０９はＲＦＩＤタグ１０４との通信が可能となる。なお、リーダ／ライタ１０９にＲＦＩＤタグ１０４を近づけて、後述する所定の認証処理を実行しないとゲートが開かないようにしているので、ユーザはセキュリティエリア１００へ入場するためにはＲＦＩＤタグ１０４をリーダ／ライタ１０９に近づける必要がある。

【００６０】

ステップＳ６０２：リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１から、ユーザＩＤ４０１を読み出してセキュリティサーバ１０３に送信する。

【００６１】

ステップＳ６０３：セキュリティサーバ１０３は、リーダ／ライタ１０９から受信したユーザＩＤ４０１が、当該セキュリティサーバ１０３に登録されており、かつ、そのユーザＩＤ４０１に係るユーザの入退出の状況が「退場」となっているか否かを判別することにより、当該ユーザの入場を認証するか否かを判別する。

【００６２】

具体的には、セキュリティサーバ１０３の制御部８０２は、リーダ／ライタ１０９の制御部３０５を介して入力されるユーザＩＤが、セキュリティサーバ１０３内のテーブルデータ８０４に記憶されているユーザＩＤと一致し、かつそのユーザＩＤに対応付けられた入退場状況が「退場」となっている場合には、ユーザの入場を認証することとし、認証する旨の情報をＩ／Ｆ部８０１を介してリーダ／ライタ１０９へ送信する。

【００６３】

そして、セキュリティサーバ１０３は、ユーザの入場を認証する場合はステップＳ６０５へ処理を進め、ユーザの入場を認証しない場合はステップＳ６０４へ処理を進める。

【００６４】

ステップＳ６０４：セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録されていない、或いは登録されていても当該ユーザＩＤ４０１に係るユーザの入退出の状況が「入場」となっている場合（この場合は、過去に不正にセキュリティエリア１００の外に退出したことを意味する）は、当該ユーザの入場を認証せずに、所定の警告処理を行う。

【００６５】
この警告処理としては、例えば、ゲートに設置された表示装置に警告メッセージを表示する、ゲートに設置されたスピーカにより警告音を鳴らす、或いはゲート制御部１０１によりゲートを一時的に閉鎖状態にロックさせること等が考えられる。
【００６６】
ステップＳ６０５：セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録され、かつ当該ユーザＩＤ４０１に係るユーザの入退出の状況が「退出」となっている場合は、当該ユーザの入場を認証し、当該ユーザＩＤ４０１に係るユーザの入退出の状況を「入場」に変更し、当該ユーザの入場を認証した旨の情報をリーダ／ライタ１０９に通知する。
【００６７】
なお、リーダ／ライタ１０９の制御部３０５は、セキュリティサーバ１０３からユーザの入場を認証した旨の情報を受信すると、ユーザが入場したことを示す情報（言い換えれば、ＲＦＩＤタグ１０４がセキュリティエリア１００に存在する「入場」状態にあることを示す情報）をＲＦＩＤタグ１０４の不揮発性メモリ２０１に書き込むよう変調回路３０２を制御する。
【００６８】
ステップＳ６０６：リーダ／ライタ１０９の制御部３０５は、当該ユーザＩＤ４０１に係るユーザの入場を認証した旨の情報をセキュリティサーバ１０３から受信すると、当該ユーザＩＤ４０１に係る退避された個別データ４０２をセキュリティサーバ１０３に照会して送信してもらい、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１に書き戻す。
【００６９】
例えば、セキュリティサーバ１０３の制御部８０２は、当該ユーザＩＤ４０１がテーブルデータ８０４に示される「１３１１４０３９」（その入退場情報は「退場」）であり、ステップＳ６０３にて不揮発性メモリ２０１から読み出した入退場情報が「退場」状態を示す場合であれば（図７参照）、退場した際に機密データであるとして記憶部８０３へ退避させた情報（ａａａ．ｔｘｔ）をＲＦＩＤタグ１０４の不揮発性メモリ２０１へ書き戻すよう、当該情報（ａａａ．ｔｘｔ）をリーダ／ライタ１０９へ送信する。セキュリティサーバ１０３から情報（ａａａ．ｔｘｔ）を受信したＲＦＩＤタグ１０４の制御部３０５は、情報（ａａａ．ｔｘｔ）をＲＦＩＤタグ１０４の不揮発性メモリ１０４へ書き込むよう、変調回路３０２を制御する。
【００７０】
ステップＳ６０７：リーダ／ライタ１０９の制御部３０５は、当該ユーザＩＤ４０１に係る退避された他の個別データ（図４における４０６、４０７、４０８）が存在するか否かをセキュリティサーバ１０３に問合せ、退避された他の個別データが存在する場合は、ステップＳ６０６に戻ることにより、当該他の個別データ４０２をＲＦＩＤタグ１０４内の不揮発性メモリ２０１に書き戻す。
【００７１】
なお、セキュリティサーバ１０３の制御部８０２は、セキュリティサーバ１０３内の記憶部８０３の記憶領域を有効利用するため、不揮発性メモリ２０１に書き戻した個別データ４０２を記憶部８０３から消去する。また、セキュリティサーバ１０３の制御部８０２は、上記のように、リーダ／ライタ１０９の制御部３０５からの照会や問合せに応答して、退避に係る個別データ４０２をリーダ／ライタ１０９に送信するのではなく、ステップＳ６０２でリーダ／ライタ１０９から受信したユーザＩＤ４０１に基づいて、能動的に退避に係る個別データ４０２を検索してリーダ／ライタ１０９に送信するようにしてもよい。
【００７２】
ステップＳ６０８：一方、退避された他の個別データ４０２が存在しない場合は、リーダ／ライタ１０９の制御部３０５は、例えばゲート制御部１０１によりゲートをオープン

させる等の入場処理を行い本処理を終了する。

【００７３】

このように、本実施形態では、セキュリティエリア１００の外部にＲＦＩＤタグ１０４を持ち出す場合に、ＲＦＩＤタグ１０４から機密データを読み出してセキュリティサーバ１０３に退避した後に、ＲＦＩＤタグ１０４上の退避に係る機密データを消去するとともに、セキュリティエリア１００の中にＲＦＩＤタグ１０４を持ち込む場合に、退避に係る機密データをＲＦＩＤタグ１０４に書き戻して復元している。

【００７４】

従って、本実施形態によれば、機密データがセキュリティエリア１００の外で第３者に漏れて悪用されるのを回避することが可能となる。また、機密データの退避、消去、書戻し処理は、ＲＦＩＤタグ１０４をリーダ／ライタ１０９にかざした際に自動的に行われるので、ユーザの負担が増大することはない。

【００７５】

また、ＲＦＩＤタグ１０４にはバッテリを搭載する必要がないので、ＲＦＩＤタグ１０４の小型化が可能になると共に、セキュリティシステムを安価に構築することが可能となる。さらに、ユーザ認証を受けないと機密データの復元は行われないので、万一、ユーザ認証を受けずに不正にセキュリティエリア１００の中に入場したとしても、機密データを利用できなくなり、セキュリティ機能が更に向上する。

【００７６】

［実施形態の変形例］

上記のように、ＲＦＩＤタグ１０４に格納された機密データを退避、消去、書戻しを行うことなく、以下のようにして、機密データの漏洩を防止するようにしてもよい。

【００７７】

すなわち、個別データ４０２に対応付けた読出可能フラグをＲＦＩＤタグ１０４の不揮発性メモリ２０１に記憶させ、セキュリティエリア１００の外にＲＦＩＤタグ１０４を持ち出す際には、機密データに係る読出可能フラグを読出不可状態に設定し、且つセキュリティエリア１００の中にＲＦＩＤタグ１０４を持ち込む際には、機密データに係る読出可能フラグを読出可能状態に設定することで、セキュリティエリア１００の外では、機密データの漏洩を防止すると共に、セキュリティエリア１００の中では、機密データを自由に利用できるようにしてもよい。

【００７８】

この場合、上記読出可能フラグは、上記セキュリティサーバ１０３によって当該ＲＦＩＤタグ１０４のユーザが認証された場合にのみ、例えばリーダ／ライタ１０９によりフラグ値を変更できるようにする必要がある。また、ＲＦＩＤタグ１０４においては、制御部２０６、又はメモリコントローラ（不図示）内に、上記読出可能フラグが読出不可状態に設定された個別データ（機密データ）を読出せないようにする制御機構を設け、ＲＦＩＤタグ用の市販のリーダ／ライタ等では、この機密データを読出せないようにする必要がある。

【００７９】

なお、上記実施形態例では、機密データの退避、消去、或いは書戻しの処理を行う必要があるため、入退出管理に要する時間が長くなる可能性が考えられる。一方、変形例では、機密データを直接処理することはないので、入退出管理に要する時間は短くなるが、機密データが形式上セキュリティエリア１００の外に持ち出されてしまい、セキュリティの点では多少の不安が残る。上記実施形態例と変形例の何れを選択するかは、セキュリティ性と入退出管理の所要時間との何れを重要視するかで決定すればよい。

【００８０】

なお、個別データ４０２，４０６，４０７，４０８の構成データとして、上記読出可能フラグの代わりに、アクセス可能フラグを定義することにより、機密データの上に他のデータが上書きされる等して機密データが破壊されるのを防止することも可能である。

【００８１】

また、上記のようにＲＦＩＤタグを入退出管理に利用せず、各種の装置で使用するデータを記録するだけの目的で利用する場合にも、本発明を適用することが可能である。この場合は、機密エリアに対するＲＦＩＤタグの持出し／持込みを検知する手段としては、ＲＦＩＤタグ用のリーダ／ライタを用いる必要はなく、例えば、パチンコ店、ゲームセンタ等の遊技場でＲＦＩＤタグを遊戯代金の清算媒体として利用するような場合において、所定の装置により遊技場に磁場（すなわち、機密エリア）を形成し、ＲＤＩＤタグには磁場を検知するデバイスを搭載し、このデバイスにより機密エリアに対するＲＦＩＤタグの持出し／持込みを検知することも可能である。

【００８２】

なお、上記の遊戯場でＲＦＩＤタグを遊戯代金の清算媒体として利用する例では、上記実施形態、又は変形例に係る機密データの漏洩防止処理は、ＲＦＩＤタグに格納されたプリペード情報が他の経営者に係る遊技場で使用されるのを回避するために行われる。

【００８３】

また、ＲＦＩＤタグにバッテリを搭載することも可能である。この場合は、ＲＦＩＤタグの制御部は、リーダ／ライタの制御部と協働することなく、主体的に上記実施形態、又は変形例に係る機密データの漏洩防止処理を実行するように構成することも可能である。

【００８４】

さらに、機密データの漏洩防止処理として、機密エリアの外にＲＦＩＤタグを持出す際に、当該ＲＦＩＤタグ内の機密データを暗号化し、機密エリアの中にＲＦＩＤタグを持込む際に（必要に応じてユーザ認証も行って）、当該ＲＦＩＤタグ内の暗号化された機密データを復号化することも可能である。

【００８５】

また、ＲＦＩＤタグの通信方式は、電波、又は電磁波を用いることなく、例えば、赤外線等の光を用いた通信方式でもよい。また、ＲＦＩＤタグの形状は、カード型でなく、ラベル型、コイン型、箱型、スティック型等であってもよい。

【００８６】

また、本発明は、厳密な意味では機密データと言えないようなデータ、例えば、プライバシーに係るデータ、青少年に有害なデータ等に適用することも可能である。

【００８７】

さらに、本発明の目的は、上記実施形態、変形例等の機能を実現するソフトウェアのプログラムコードをＲＦＩＤタグ、リーダ／ライタに無線通信等により非接触でダウンロードし、ＲＦＩＤタグ、リーダ／ライタの制御部がダウンロードに係るプログラムコードを実行することによっても、達成されることは言うまでもない。

【００８８】

この場合、上記プログラムコード自体が前述した実施形態、変形例等の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、上記プログラムコードを実行することにより、前述した実施形態、変形例等の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、ＲＦＩＤタグ、リーダ／ライタ上で稼動しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態、変形例等の機能が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

【００８９】

【図１】本発明の一形態に係る情報処理装置を適用したセキュリティシステムのシステム構成図である。

【図２】上記セキュリティシステムのＲＦＩＤタグの概略構成を示すブロック図である。

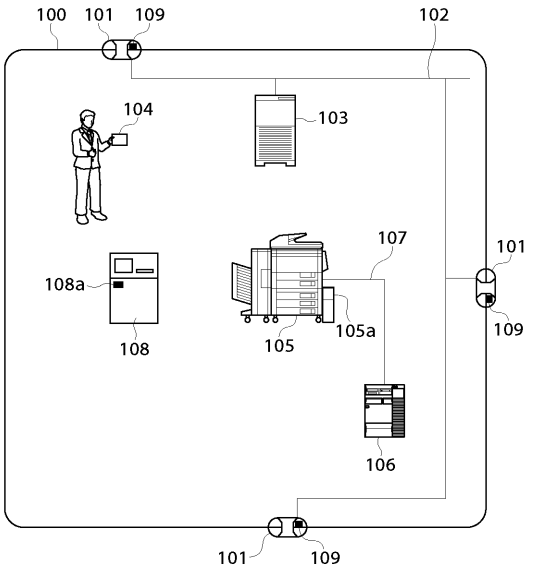
【図３】上記セキュリティシステムのリーダ／ライタの概略構成を示すブロック図である。

【図４】上記ＲＦＩＤタグの不揮発性メモリ内のデータの構成を示す概念図である。

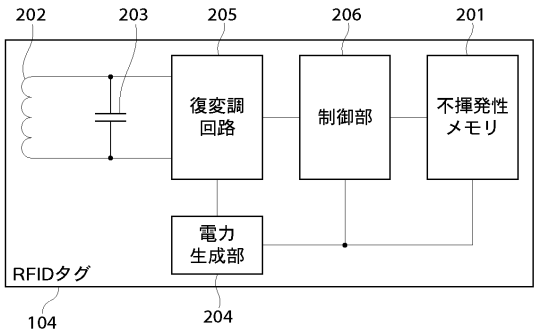
【図５】セキュリティエリアからＲＦＩＤタグを持ち出す場合のセキュリティシステムの

処理を示すフローチャートである。
【図６】セキュリティエリアにＲＦＩＤタグを持ち込む場合のセキュリティシステムの処理を示すフローチャートである。
【図７】セキュリティサーバの記憶部に記憶されるテーブルデータを示す図である。
【図８】セキュリティサーバの構成を示すブロック図である。
【符号の説明】
【００９０】
１００…セキュリティエリア、１０１…ゲート制御部、１０３…セキュリティサーバ、１０４…ＲＦＩＤタグ、１０９，１０５ａ，１０８ａ…リーダ／ライタ、２０１…不揮発性メモリ、２０５…ＲＦＩＤタグの制御部、３０５…リーダ／ライタの制御部、４０１…ユーザＩＤ、４０２，４０６，４０７，４０８…個別データ、４０５…機密フラグ

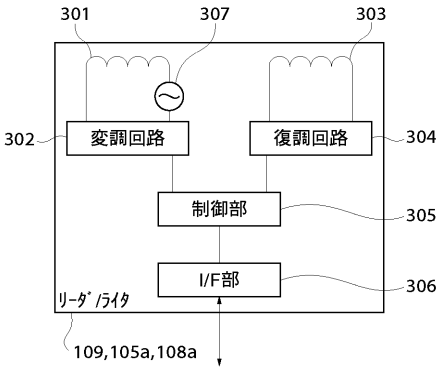
【図１】



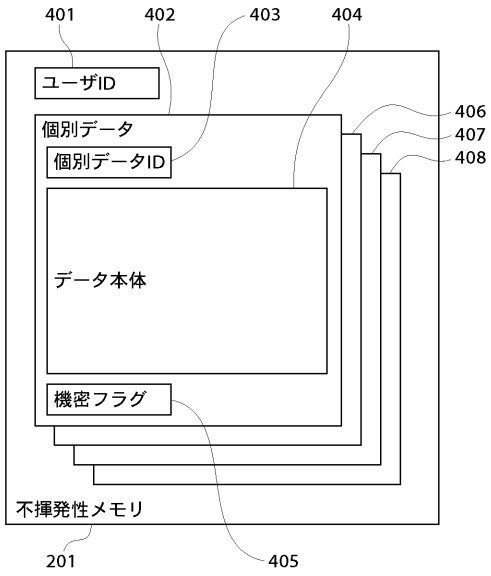
【図２】



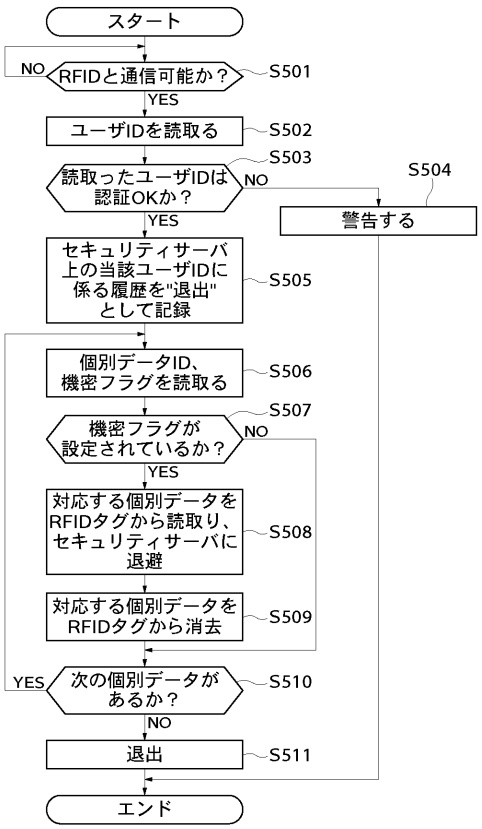
【図３】


301
307
303
302
変調回路
復調回路
304
制御部
305
I/F部
306
ﾘｰﾀﾞ/ﾗｲﾀ
109,105a,108a

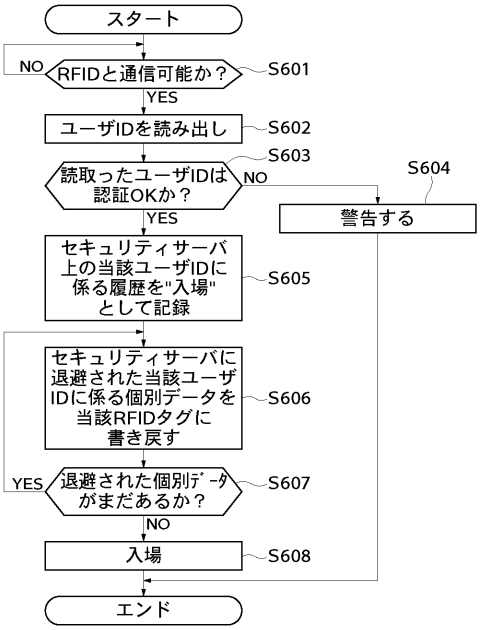
【図４】


401
402
403
404
ユーザID
個別データ
個別データID
406
407
408
データ本体
機密フラグ
不揮発性メモリ
201
405

【図５】


スタート
NO
RFIDと通信可能か？
S501
YES
ユーザIDを読取る
S502
S503
読取ったユーザIDは認証OKか？
NO
S504
警告する
YES
セキュリティサーバ上の当該ユーザIDに係る履歴を"退出"として記録
S505
個別データID、機密フラグを読取る
S506
S507
機密フラグが設定されているか？
NO
YES
対応する個別データをRFIDタグから読取り、セキュリティサーバに退避
S508
対応する個別データをRFIDタグから消去
S509
YES
次の個別データがあるか？
S510
NO
退出
S511
エンド

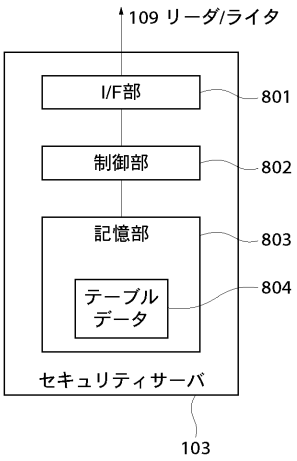
【図６】


スタート
NO
RFIDと通信可能か？
S601
YES
ユーザIDを読み出し
S602
S603
読取ったユーザIDは認証OKか？
NO
S604
警告する
YES
セキュリティサーバ上の当該ユーザIDに係る履歴を"入場"として記録
S605
セキュリティサーバに退避された当該ユーザIDに係る個別データを当該RFIDタグに書き戻す
S606
YES
退避された個別ﾃﾞｰﾀがまだあるか？
S607
NO
入場
S608
エンド

【図７】

NO.	USER ID	入退場状況	退避させた機密情報
1	13114032	入場	—
2	13114039	退場	aaa.txt
⋮	⋮	⋮	⋮

【図８】



フロントページの続き

(51)Int.Cl.	FI		
	G06K	17/00	L
	G06K	17/00	S
	H04L	9/00	673E

(56)参考文献 特開2001－344369（JP, A）
特開2003－110490（JP, A）
特開2003－242285（JP, A）
特開2003－288275（JP, A）
特開2004－078808（JP, A）

(58)調査した分野(Int.Cl., DB名)
G06F 21／24
G06F 21／02
G06K 17／00
H04L 9／32