(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2006-295234
(P2006-295234A)
(43)公開日　平成18年10月26日(2006.10.26)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5B058
G06F 21/20	(2006.01)	G06F	15/00	330G	5B285
G06K 17/00	(2006.01)	G06K	17/00	T	5J104
G09C 1/00	(2006.01)	G09C	1/00	640E	
		H04L	9/00	673C	

審査請求 未請求　請求項の数 8　ＯＬ　（全 13 頁）

(21)出願番号　特願2005-108908 (P2005-108908)
(22)出願日　平成17年4月5日 (2005.4.5)

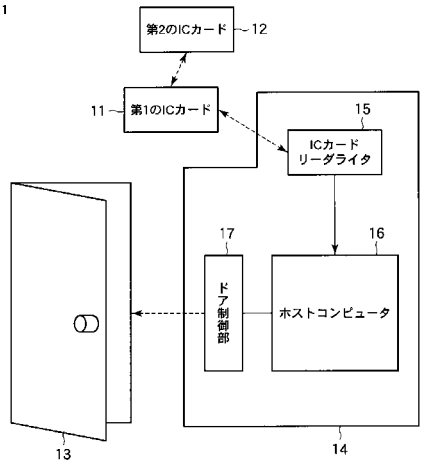
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】認証システム、認証方法および入退場管理システム

(57)【要約】
【課題】認証用情報は１つの認証用媒体に対してだけホスト装置に持てばよいため情報管理がし易くなり、かつ、認証用媒体との通信回数を減らすことができる認証システム、認証方法および入退場管理システムを提供する。
【解決手段】第１のＩＣカードおよび第２のＩＣカードを用いて認証処理を行なう認証システムにおいて、外部と通信を行なう機能を有する第１のＩＣカードおよび第２のＩＣカードと、ＩＣカードと通信を行なう機能を有するホスト装置とを有して構成され、ホスト装置は、第１のＩＣカードに対し限定して通信を実施するよう制御し、第２のＩＣカードは、第１のＩＣカードに対し限定して通信を実施するような制御を行なう。
【選択図】　図１

図１



【特許請求の範囲】
【請求項１】
外部と通信を行なう機能を有する第１の認証用媒体および第２の認証用媒体と、認証用媒体と通信を行なう機能を有するホスト装置とを有して構成され、
前記ホスト装置は、
前記第１の認証用媒体に対し認証用情報要求を送信する第１の送信手段を具備し、
前記第１の認証用媒体は、
前記ホスト装置の第１の送信手段により送信された認証用情報要求を受信する第１の受信手段と、
この第１の受信手段により受信された認証用情報要求に応答し、あらかじめ記憶手段に登録された固有の認証用情報を前記ホスト装置に対し送信する第２の送信手段とを具備し、
前記ホスト装置は、さらに、
前記第１の認証用媒体の第２の送信手段により送信された認証用情報を受信する第２の受信手段と、
この第２の受信手段により受信された認証用情報に基づき当該第１の認証用媒体はあらかじめ登録されている認証用媒体であるか否かを判定する第１の判定手段と、
この第１の判定手段により当該第１の認証用媒体はあらかじめ登録されている認証用媒体であると判定された場合、あらかじめ定められた固有情報を前記第１の認証用媒体に対し送信する第３の送信手段とを具備し、
前記第１の認証用媒体は、さらに、
前記ホスト装置の第３の送信手段により送信された固有情報を受信する第３の受信手段と、
この第３の受信手段により受信された固有情報をあらかじめ定められた第１の鍵情報を用いて暗号化する第１の暗号化手段と、
この第１の暗号化手段により暗号化された固有情報を前記第２の認証用媒体に対し送信する第４の送信手段とを具備し、
前記第２の認証用媒体は、
前記第１の認証用媒体の第４の送信手段により送信された暗号化された固有情報を受信する第４の受信手段と、
この第４の受信手段により受信された固有情報をあらかじめ定められた第２の鍵情報を用いてさらに暗号化する第２の暗号化手段と、
この第２の暗号化手段によりさらに暗号化された固有情報を前記第１の認証用媒体に対し送信する第５の送信手段とを具備し、
前記第１の認証用媒体は、さらに、
前記第２の認証用媒体の第５の送信手段により送信された暗号化された固有情報を受信する第５の受信手段と、
この第５の受信手段により受信された暗号化された固有情報をそのまま前記ホスト装置に対し送信する第６の送信手段とを具備し、
前記ホスト装置は、さらに、
前記第１の認証用媒体の第６の送信手段により送信された暗号化された固有情報を受信する第６の受信手段と、
この第６の受信手段により受信された暗号化された固有情報を前記第１の鍵情報および第２の鍵情報に対応する鍵情報を用いて復号化する復号化手段と、
この復号化手段により復号化された固有情報と前記第３の送信手段により送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否かを判定する第２の判定手段とを具備したことを特徴とする認証システム。
【請求項２】
前記第２の認証用媒体が複数存在する場合、前記第４の受信手段および第２の暗号化手段および第５の送信手段による処理を複数の第２の認証用媒体ごとに順次縦続的に行なう

ことで、前の第２の認証用媒体から送信される固有情報を暗号化して次の第２の認証用媒体へ送信し、最後の第２の認証用媒体は暗号化した固有情報を前記第１の認証用媒体へ送信することを特徴とする請求項１記載の認証システム。

【請求項３】

前記第２の認証用媒体が複数存在する場合、複数の第２の認証用媒体が前記第４の受信手段および第２の暗号化手段および第５の送信手段による処理を並列的に行なうことで、複数の第２の認証用媒体はそれぞれ第１の認証用媒体から送信される固有情報を暗号化して第１の認証用媒体へ送信することを特徴とする請求項１記載の認証システム。

【請求項４】

前記第１の認証用媒体および第２の認証用媒体は、無線通信により外部と通信を行なう非接触形ＩＣカードであることを特徴とする請求項１記載の認証システム。

【請求項５】

外部と通信を行なう機能を有する第１の認証用媒体および第２の認証用媒体と、認証用媒体と通信を行なう機能を有するホスト装置とを有し、

前記ホスト装置において、前記第１の認証用媒体に対し認証用情報要求を送信する第１の送信ステップと、

前記第１の認証用媒体において、前記第１の送信ステップにより送信された認証用情報要求を受信する第１の受信ステップと、

前記第１の認証用媒体において、前記第１の受信ステップにより受信された認証用情報要求に応答し、あらかじめ記憶手段に登録された固有の認証用情報を前記ホスト装置に対し送信する第２の送信ステップと、

前記ホスト装置において、前記第２の送信ステップにより送信された認証用情報を受信する第２の受信ステップと、

前記ホスト装置において、前記第２の受信ステップにより受信された認証用情報に基づき当該第１の認証用媒体はあらかじめ登録されている認証用媒体であるか否かを判定する第１の判定ステップと、

前記ホスト装置において、前記第１の判定ステップにより当該第１の認証用媒体はあらかじめ登録されている認証用媒体であると判定された場合、あらかじめ定められた固有情報を前記第１の認証用媒体に対し送信する第３の送信ステップと、

前記第１の認証用媒体において、前記第３の送信ステップにより送信された固有情報を受信する第３の受信ステップと、

前記第１の認証用媒体において、前記第３の受信ステップにより受信された固有情報をあらかじめ定められた第１の鍵情報を用いて暗号化する第１の暗号化ステップと、

前記第１の認証用媒体において、前記第１の暗号化ステップにより暗号化された固有情報を前記第２の認証用媒体に対し送信する第４の送信ステップと、

前記第２の認証用媒体において、前記第４の送信ステップにより送信された暗号化された固有情報を受信する第４の受信ステップと、

前記第２の認証用媒体において、前記第４の受信ステップにより受信された固有情報をあらかじめ定められた第２の鍵情報を用いてさらに暗号化する第２の暗号化ステップと、

前記第２の認証用媒体において、前記第２の暗号化ステップによりさらに暗号化された固有情報を前記第１の認証用媒体に対し送信する第５の送信ステップと、

前記第１の認証用媒体において、前記第５の送信ステップにより送信された暗号化された固有情報を受信する第５の受信ステップと、

前記第１の認証用媒体において、前記第５の受信ステップにより受信された暗号化された固有情報をそのまま前記ホスト装置に対し送信する第６の送信ステップと、

前記ホスト装置において、前記第６の送信ステップにより送信された暗号化された固有情報を受信する第６の受信ステップと、

前記ホスト装置において、前記第６の受信ステップにより受信された暗号化された固有情報を前記第１の鍵情報および第２の鍵情報に対応する鍵情報を用いて復号化する復号化ステップと、

前記ホスト装置において、前記復号化ステップにより復号化された固有情報と前記第３の送信ステップにより送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否かを判定する第２の判定ステップと、
を具備したことを特徴とする認証方法。
【請求項６】
施設を利用する利用者が所持し、外部と通信を行なう機能を有する第１の認証用媒体および第２の認証用媒体と、認証用媒体と通信を行ない、その通信結果に基づき前記施設の入口に設けられた入退場用のゲートを開閉制御するホスト装置とを有して構成され、
前記ホスト装置は、
前記第１の認証用媒体に対し認証用情報要求を送信する第１の送信手段を具備し、
前記第１の認証用媒体は、
前記ホスト装置の第１の送信手段により送信された認証用情報要求を受信する第１の受信手段と、
この第１の受信手段により受信された認証用情報要求に応答し、あらかじめ記憶手段に登録された固有の認証用情報を前記ホスト装置に対し送信する第２の送信手段とを具備し、
前記ホスト装置は、さらに、
前記第１の認証用媒体の第２の送信手段により送信された認証用情報を受信する第２の受信手段と、
この第２の受信手段により受信された認証用情報に基づき当該第１の認証用媒体はあらかじめ登録されている認証用媒体であるか否かを判定する第１の判定手段と、
この第１の判定手段により当該第１の認証用媒体はあらかじめ登録されている認証用媒体であると判定された場合、あらかじめ定められた固有情報を前記第１の認証用媒体に対し送信する第３の送信手段とを具備し、
前記第１の認証用媒体は、さらに、
前記ホスト装置の第３の送信手段により送信された固有情報を受信する第３の受信手段と、
この第３の受信手段により受信された固有情報をあらかじめ定められた第１の鍵情報を用いて暗号化する第１の暗号化手段と、
この第１の暗号化手段により暗号化された固有情報を前記第２の認証用媒体に対し送信する第４の送信手段とを具備し、
前記第２の認証用媒体は、
前記第１の認証用媒体の第４の送信手段により送信された暗号化された固有情報を受信する第４の受信手段と、
この第４の受信手段により受信された固有情報をあらかじめ定められた第２の鍵情報を用いてさらに暗号化する第２の暗号化手段と、
この第２の暗号化手段によりさらに暗号化された固有情報を前記第１の認証用媒体に対し送信する第５の送信手段とを具備し、
前記第１の認証用媒体は、さらに、
前記第２の認証用媒体の第５の送信手段により送信された暗号化された固有情報を受信する第５の受信手段と、
この第５の受信手段により受信された暗号化された固有情報をそのまま前記ホスト装置に対し送信する第６の送信手段とを具備し、
前記ホスト装置は、さらに、
前記第１の認証用媒体の第６の送信手段により送信された暗号化された固有情報を受信する第６の受信手段と、
この第６の受信手段により受信された暗号化された固有情報を前記第１の鍵情報および第２の鍵情報に対応する鍵情報を用いて復号化する復号化手段と、
この復号化手段により復号化された固有情報と前記第３の送信手段により送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否かを判定する第２の判定手段

と、
この第２の判定手段の判定結果に基づき前記施設の入口に設けられた入退場用のゲートを開閉制御するゲート制御手段とを具備したことを特徴とする入退場管理システム。
【請求項７】
前記第２の認証用媒体が複数存在する場合、前記第４の受信手段および第２の暗号化手段および第５の送信手段による処理を複数の第２の認証用媒体ごとに順次縦続的に行なうことで、前の第２の認証用媒体から送信される固有情報を暗号化して次の第２の認証用媒体へ送信し、最後の第２の認証用媒体は暗号化した固有情報を前記第１の認証用媒体へ送信することを特徴とする請求項６記載の入退場管理システム。
【請求項８】
前記第２の認証用媒体が複数存在する場合、複数の第２の認証用媒体が前記第４の受信手段および第２の暗号化手段および第５の送信手段による処理を並列的に行なうことで、複数の第２の認証用媒体はそれぞれ第１の認証用媒体から送信される固有情報を暗号化して第１の認証用媒体へ送信することを特徴とする請求項６記載の入退場管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、たとえば、複数人が同意することが条件となる入退場管理システムなどにおいて、複数の非接触形ＩＣカード（認証用媒体）を用いて認証を行なう認証システムおよび認証方法に関する。
また、本発明は、認証システムおよび認証方法を用いて高度なセキュリティが求められている部屋やエリアなどの施設に対する入退場を管理する入退場管理システムに関する。
【背景技術】
【０００２】
たとえば、コンピュータネットワークにおいて、複数のＩＣカードを用い、それぞれが端末装置との間で認証処理を実施することで、高度なセキュリティを維持可能とする認証システムが提案されている（特許文献１参照）。
【特許文献１】特開２００３－１５０５５３
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、特許文献１の技術では、複数のＩＣカードを用いてロック解除等を実施する場合、使用する全てのＩＣカードの情報を端末装置側で持つことになる。したがってＩＣカードの枚数が増えると、組合せは枚数の掛け算となり、情報管理が非常に煩雑になるという問題がある。
【０００４】
そこで、本発明は、認証用情報は１つの認証用媒体に対してだけホスト装置に持てばよいため情報管理がし易くなり、かつ、認証用媒体との通信回数を減らすことができる認証システム、認証方法および入退場管理システ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】
【０００５】
本発明の認証システムは、外部と通信を行なう機能を有する第１の認証用媒体および第２の認証用媒体と、認証用媒体と通信を行なう機能を有するホスト装置とを有して構成され、前記ホスト装置は、前記第１の認証用媒体に対し認証用情報要求を送信する第１の送信手段を具備し、前記第１の認証用媒体は、前記ホスト装置の第１の送信手段により送信された認証用情報要求を受信する第１の受信手段と、この第１の受信手段により受信された認証用情報要求に応答し、あらかじめ記憶手段に登録された固有の認証用情報を前記ホスト装置に対し送信する第２の送信手段とを具備し、前記ホスト装置は、さらに、前記第１の認証用媒体の第２の送信手段により送信された認証用情報を受信する第２の受信手段と、この第２の受信手段により受信された認証用情報に基づき当該第１の認証用媒体はあ

らかじめ登録されている認証用媒体であるか否かを判定する第１の判定手段と、この第１の判定手段により当該第１の認証用媒体はあらかじめ登録されている認証用媒体であると判定された場合、あらかじめ定められた固有情報を前記第１の認証用媒体に対し送信する第３の送信手段とを具備し、前記第１の認証用媒体は、さらに、前記ホスト装置の第３の送信手段により送信された固有情報を受信する第３の受信手段と、この第３の受信手段により受信された固有情報をあらかじめ定められた第１の鍵情報を用いて暗号化する第１の暗号化手段と、この第１の暗号化手段により暗号化された固有情報を前記第２の認証用媒体に対し送信する第４の送信手段とを具備し、前記第２の認証用媒体は、前記第１の認証用媒体の第４の送信手段により送信された暗号化された固有情報を受信する第４の受信手段と、この第４の受信手段により受信された固有情報をあらかじめ定められた第２の鍵情報を用いてさらに暗号化する第２の暗号化手段と、この第２の暗号化手段によりさらに暗号化された固有情報を前記第１の認証用媒体に対し送信する第５の送信手段とを具備し、前記第１の認証用媒体は、さらに、前記第２の認証用媒体の第５の送信手段により送信された暗号化された固有情報を受信する第５の受信手段と、この第５の受信手段により受信された暗号化された固有情報をそのまま前記ホスト装置に対し送信する第６の送信手段とを具備し、前記ホスト装置は、さらに、前記第１の認証用媒体の第６の送信手段により送信された暗号化された固有情報を受信する第６の受信手段と、この第６の受信手段により受信された暗号化された固有情報を前記第１の鍵情報および第２の鍵情報に対応する鍵情報を用いて復号化する復号化手段と、この復号化手段により復号化された固有情報と前記第３の送信手段により送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否かを判定する第２の判定手段とを具備している。

【０００６】

また、本発明の認証方法は、外部と通信を行なう機能を有する第１の認証用媒体および第２の認証用媒体と、認証用媒体と通信を行なう機能を有するホスト装置とを有し、前記ホスト装置において、前記第１の認証用媒体に対し認証用情報要求を送信する第１の送信ステップと、前記第１の認証用媒体において、前記第１の送信ステップにより送信された認証用情報要求を受信する第１の受信ステップと、前記第１の認証用媒体において、前記第１の受信ステップにより受信された認証用情報要求に応答し、あらかじめ記憶手段に登録された固有の認証用情報を前記ホスト装置に対し送信する第２の送信ステップと、前記ホスト装置において、前記第２の送信ステップにより送信された認証用情報を受信する第２の受信ステップと、前記ホスト装置において、前記第２の受信ステップにより受信された認証用情報に基づき当該第１の認証用媒体はあらかじめ登録されている認証用媒体であるか否かを判定する第１の判定ステップと、前記ホスト装置において、前記第１の判定ステップにより当該第１の認証用媒体はあらかじめ登録されている認証用媒体であると判定された場合、あらかじめ定められた固有情報を前記第１の認証用媒体に対し送信する第３の送信ステップと、前記第１の認証用媒体において、前記第３の送信ステップにより送信された固有情報を受信する第３の受信ステップと、前記第１の認証用媒体において、前記第３の受信ステップにより受信された固有情報をあらかじめ定められた第１の鍵情報を用いて暗号化する第１の暗号化ステップと、前記第１の認証用媒体において、前記第１の暗号化ステップにより暗号化された固有情報を前記第２の認証用媒体に対し送信する第４の送信ステップと、前記第２の認証用媒体において、前記第４の送信ステップにより送信された暗号化された固有情報を受信する第４の受信ステップと、前記第２の認証用媒体において、前記第４の受信ステップにより受信された固有情報をあらかじめ定められた第２の鍵情報を用いてさらに暗号化する第２の暗号化ステップと、前記第２の認証用媒体において、前記第２の暗号化ステップによりさらに暗号化された固有情報を前記第１の認証用媒体に対し送信する第５の送信ステップと、前記第１の認証用媒体において、前記第５の送信ステップにより送信された暗号化された固有情報を受信する第５の受信ステップと、前記第１の認証用媒体において、前記第５の受信ステップにより受信された暗号化された固有情報をそのまま前記ホスト装置に対し送信する第６の送信ステップと、前記ホスト装置において、前記第６の送信ステップにより送信された暗号化された固有情報を受信する第

６の受信ステップと、前記ホスト装置において、前記第６の受信ステップにより受信された暗号化された固有情報を前記第１の鍵情報および第２の鍵情報に対応する鍵情報を用いて復号化する復号化ステップと、前記ホスト装置において、前記復号化ステップにより復号化された固有情報と前記第３の送信ステップにより送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否かを判定する第２の判定ステップとを具備している。

【０００７】

さらに、本発明の入退場管理システムは、施設を利用する利用者が所持し、外部と通信を行なう機能を有する第１の認証用媒体および第２の認証用媒体と、認証用媒体と通信を行ない、その通信結果に基づき前記施設の入口に設けられた入退場用のゲートを開閉制御するホスト装置とを有して構成され、前記ホスト装置は、前記第１の認証用媒体に対し認証用情報要求を送信する第１の送信手段を具備し、前記第１の認証用媒体は、前記ホスト装置の第１の送信手段により送信された認証用情報要求を受信する第１の受信手段と、この第１の受信手段により受信された認証用情報要求に応答し、あらかじめ記憶手段に登録された固有の認証用情報を前記ホスト装置に対し送信する第２の送信手段とを具備し、前記ホスト装置は、さらに、前記第１の認証用媒体の第２の送信手段により送信された認証用情報を受信する第２の受信手段と、この第２の受信手段により受信された認証用情報に基づき当該第１の認証用媒体はあらかじめ登録されている認証用媒体であるか否かを判定する第１の判定手段と、この第１の判定手段により当該第１の認証用媒体はあらかじめ登録されている認証用媒体であると判定された場合、あらかじめ定められた固有情報を前記第１の認証用媒体に対し送信する第３の送信手段とを具備し、前記第１の認証用媒体は、さらに、前記ホスト装置の第３の送信手段により送信された固有情報を受信する第３の受信手段と、この第３の受信手段により受信された固有情報をあらかじめ定められた第１の鍵情報を用いて暗号化する第１の暗号化手段と、この第１の暗号化手段により暗号化された固有情報を前記第２の認証用媒体に対し送信する第４の送信手段とを具備し、前記第２の認証用媒体は、前記第１の認証用媒体の第４の送信手段により送信された暗号化された固有情報を受信する第４の受信手段と、この第４の受信手段により受信された固有情報をあらかじめ定められた第２の鍵情報を用いてさらに暗号化する第２の暗号化手段と、この第２の暗号化手段によりさらに暗号化された固有情報を前記第１の認証用媒体に対し送信する第５の送信手段とを具備し、前記第１の認証用媒体は、さらに、前記第２の認証用媒体の第５の送信手段により送信された暗号化された固有情報を受信する第５の受信手段と、この第５の受信手段により受信された暗号化された固有情報をそのまま前記ホスト装置に対し送信する第６の送信手段とを具備し、前記ホスト装置は、さらに、前記第１の認証用媒体の第６の送信手段により送信された暗号化された固有情報を受信する第６の受信手段と、この第６の受信手段により受信された暗号化された固有情報を前記第１の鍵情報および第２の鍵情報に対応する鍵情報を用いて復号化する復号化手段と、この復号化手段により復号化された固有情報と前記第３の送信手段により送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否かを判定する第２の判定手段と、この第２の判定手段の判定結果に基づき前記施設の入口に設けられた入退場用のゲートを開閉制御するゲート制御手段とを具備している。

【発明の効果】

【０００８】

本発明によれば、認証用情報は１つの認証用媒体に対してだけホスト装置に持てばよいため情報管理がし易くなり、かつ、認証用媒体との通信回数を減らすことができる認証システム、認証方法および入退場管理システムを提供できる。

【発明を実施するための最良の形態】

【０００９】

以下、本発明の実施の形態について図面を参照して説明する。

図１は、本発明に係る認証システムおよび認証方法が適用される入退場管理システムの構成を概略的に示すものである。図１において、この入退場管理システムは、たとえば、

複数人が同意することが条件となり、高度なセキュリティが求められている部屋やエリアなどの施設に対する入退場を管理するもので、たとえば施設を利用する利用者が所持し、外部と通信を行なう機能を有する第１の認証用媒体としての非接触形ＩＣカード（以降、単に第１のＩＣカードと称す）１１、たとえば施設を利用する別の利用者が所持し、外部と通信を行なう機能を有する第２の認証用媒体としての非接触形ＩＣカード（以降、単に第２のＩＣカードと称す）１２、第１のＩＣカード１１と通信を行ない、その通信結果に基づき施設の入口に設けられた入退場用のゲート例えばドア１３を開閉制御するホスト装置１４とを有して構成される。

【００１０】

ホスト装置１４は、第１のＩＣカード１１に対し無線通信によりデータの読出しや書込みを行なう非接触形のＩＣカードリーダライタ（以降、単にリーダライタと称す）１５、リーダライタ１５に接続され通信情報の制御や各種処理を行なうホストコンピュータ１６、および、ホストコンピュータ１６からの制御信号に応じて施設の入口に設けられた入退場用のドア１７を開閉制御するゲート制御手段としてのドア制御部１８により構成されている。

なお、この実施の形態では、ホスト装置１４がドア１７を開く条件として、第１のＩＣカード１１および第２のＩＣカード１２との認証成功が必要である。

【００１１】

第１、第２のＩＣカード１１，１２は、たとえば、いわゆる無線カードと称される非接触形ＩＣカードで、図２に示すように、リーダライタ１５や他のＩＣカードに対し電波を送受信する送受信アンテナ部２１、送受信アンテナ部２１で受信した電波から電力に変換し各部に供給するする電源部２２、送受信アンテナ部２１で受信した電波からデータに変換または送信データから電波に変換する変復調回路部２３、データの解析や記憶の制御等を行なう制御部２４、および、データを記憶する消去可能なメモリ部２５により構成されている。

【００１２】

リーダライタ１５は、たとえば、図３に示すように、ＩＣカードに対し電波を送受信する送受信アンテナ部３１、送受信アンテナ部３１で受信した電波からデータに変換または送信データから電波に変換する変復調回路部３２、および、データの解析や送信の制御等を行なう制御部３３により構成されている。

【００１３】

次に、図４および図５に示すフローチャートを参照して処理の流れを説明する。

まず、ホスト装置１４は、第１のＩＣカード１１との通信を実施するために、ＩＤ情報要求（認証用情報要求）を変調した電波を放出する（以降、これを送信と表現する。ステップＳ１）。ここに、このステップＳ１の処理が本発明における第１の送信手段に対応している。

【００１４】

第１のＩＣカード１１は、ホスト装置１４のリーダライタ１５からの電波到達エリア内に入ると、ホスト装置１４から送信された電波を受信しＩＤ情報要求を復調する（以降、これを受信と表現する。ステップＳ２）。ここに、このステップＳ２の処理が本発明における第１の受信手段に対応している。

【００１５】

第１のＩＣカード１１は、ホスト装置１４からのＩＤ情報要求を受信すると、メモリ部２５から、それにあらかじめ記憶（登録）されている固有のＩＤ情報（認証用情報）を読出し、この読出したＩＤ情報をホスト装置１４に対し送信する（ステップＳ３）。ここに、このステップＳ３の処理が本発明における第２の送信手段に対応している。

【００１６】

ホスト装置１４は、第１のＩＣカード１１から送信されたＩＤ情報を受信する（ステップＳ４）。ここに、このステップＳ４の処理が本発明における第２の受信手段に対応している。

【００１７】
ホスト装置１４は、第１のＩＣカード１１からのＩＤ情報を受信すると、当該ＩＤ情報を図示しないメモリにあらかじめ記憶（登録）されているＩＤ情報（認証用情報）と照合し、一致するＩＤ情報が存在するか否かにより、当該第１のＩＣカード１１があらかじめ登録されているＩＣカードであるかを判定する（ステップＳ５）。ここに、このステップＳ５の処理が本発明における第１の判定手段に対応している。
【００１８】
ステップＳ５における判定の結果、当該第１のＩＣカード１１はあらかじめ登録されているＩＣカードでないと判定された場合、ホスト装置１４は、ドア１３は閉じた状態のままとし（ステップＳ６）、当該処理を終了して、ステップＳ１のＩＤ情報要求状態に戻る。
【００１９】
ステップＳ５における判定の結果、当該第１のＩＣカード１１はあらかじめ登録されているＩＣカードであると判定された場合、ホスト装置１４は、あらかじめ定められた固有情報（たとえば、乱数）を生成し、この生成した固有情報を第１のＩＣカード１１に対して送信する（ステップＳ７）。ここに、このステップＳ７の処理が本発明における第３の送信手段に対応している。
【００２０】
第１のＩＣカード１１は、ホスト装置１４から送信された固有情報を受信する（ステップＳ８）。ここに、このステップＳ８の処理が本発明における第３の受信手段に対応している。
【００２１】
次に、第１のＩＣカード１１は、受信した固有情報をメモリ部２５にあらかじめ記憶されている第１の鍵情報を用いて暗号化する（ステップＳ９）。ここに、このステップＳ９の処理が本発明における第１の暗号化手段に対応している。
【００２２】
次に、第１のＩＣカード１１は、暗号化した固有情報を第２のＩＣカード１２に対し送信する（ステップＳ１０）。ここに、このステップＳ１０の処理が本発明における第４の送信手段に対応している。
【００２３】
第２のＩＣカード１２は、第１のＩＣカード１１から送信された暗号化された固有情報を受信する（ステップＳ１１）。ここに、このステップＳ１１の処理が本発明における第４の受信手段に対応している。
【００２４】
次に、第２のＩＣカード１２は、受信した暗号化された固有情報をメモリ部２５にあらかじめ記憶されている第２の鍵情報を用いてさらに暗号化する（ステップＳ１２）。ここに、このステップＳ１２の処理が本発明における第２の暗号化手段に対応している。
【００２５】
次に、第２のＩＣカード１１は、さらに暗号化した固有情報を第１のＩＣカード１１に対し送信する（ステップＳ１３）。ここに、このステップＳ１３の処理が本発明における第５の送信手段に対応している。
【００２６】
第１のＩＣカード１１は、第２のＩＣカード１２から送信されたさらに暗号化された固有情報を受信する（ステップＳ１４）。ここに、このステップＳ１４の処理が本発明における第５の受信手段に対応している。
【００２７】
次に、第１のＩＣカード１１は、受信したさらに暗号化された固有情報をそのままホスト装置１４に対し送信する（ステップＳ１５）。ここに、このステップＳ１５の処理が本発明における第６の送信手段に対応している。
【００２８】

ホスト装置１４は、第１のＩＣカード１１から送信されたさらに暗号化された固有情報を受信する（ステップＳ１６）。ここに、このステップＳ１６の処理が本発明における第６の受信手段に対応している。

【００２９】

次に、ホスト装置１４は、受信したさらに暗号化された固有情報を、図示しないメモリにあらかじめ記憶されている第１の鍵情報および第２の鍵情報を用いて復号化する（ステップＳ１７）。ここに、このステップＳ１７の処理が本発明における復号化手段に対応している。

【００３０】

次に、ホスト装置１４は、復号化した固有情報とステップＳ７で送信した固有情報とを照合し、両固有情報間に所定の関係が成立するか否か、この例では両固有情報が一致するか否かにより受信した固有情報が正常か否かを判定する（ステップＳ１８）。ここに、このステップＳ１８の処理が本発明における第２の判定手段に対応している。

【００３１】

ステップＳ１８における判定の結果、受信した固有情報が正常の場合（両固有情報が一致する場合）、ホスト装置１４は、ドア制御部１７に対しドア開の制御信号を送ることで、ドア１３を開く（ステップＳ１９）。

ステップＳ１８における判定の結果、受信した固有情報が異常の場合（両固有情報が不一致の場合）、ホスト装置１４は、ドア制御部１７に対しドア閉の制御信号を送ることで、ドア１３は閉じたままの状態のままとし（ステップＳ６）、当該処理を終了して、ステップＳ１のＩＤ情報要求状態に戻る。ここに、このステップＳ１９，Ｓ６の処理が本発明におけるゲート制御手段に対応している。

【００３２】

このように、第１、第２のＩＣカード１１，１２を使用することで、高いセキュリティを持たせた認証処理が可能となることは勿論のこと、従来のように複数のＩＣカードそれぞれが端末装置との間で認証処理を実施する方法に比して、ＩＤ情報（認証用情報）を用いた認証処理は１つの第１のＩＣカード１１とのやり取りとなるため、通信回数を著しく減らすことができ、認証処理の高速化が図れる。また、ＩＤ情報（認証用情報）は第１のＩＣカード１１に対してだけホスト装置１４に持てばよいため、情報管理がし易くなる（対象カードは増えるが、管理するカードの情報は増えない）。

【００３３】

なお、前記実施の形態では、ＩＣカードが２つの場合、すなわち、第１のＩＣカード１１が１つで、第２のＩＣカード１２が１つの場合を例にとって説明したが、第１のＩＣカード１１は１つのままで、第２のＩＣカード１２が複数になっても同様な考えにより実施できる。

【００３４】

まず、第２のＩＣカード１２を２つ以上に増やした場合の第１の方法として、複数の第２のＩＣカード１２が縦続的（直列的）に順次処理を行なう方法が考えられる。すなわち、ステップＳ１３で行なう暗号化された固有情報の送信を増えた第２のＩＣカード１２に対し行ない、暗号化を実施させる、といったように、ステップＳ８～Ｓ１３の処理を増えた第２のＩＣカード１２に対して順次続けていくものである。この場合、最後の第２のＩＣカード１２は暗号化した固有情報を第１のＩＣカード１１へ送信することになる。これにより、複数の第２のＩＣカード１２が縦続的（直列的）に順次処理を行なうことになる。

【００３５】

次に、第２のＩＣカード１２を２つ以上に増やした場合の第２の方法として、複数の第２のＩＣカード１２が並列的に処理を行なう方法が考えられる。すなわち、ステップＳ１４の処理まできたら、その暗号化された固有情報をそのまま増えた第２のＩＣカード１２に対し送信する、といったように、ステップＳ１０～Ｓ１３の処理を増えた第２のＩＣカード１２に対して実施していくものである。この場合、最後の第２のＩＣカード１２から

送信された暗号化された固有情報をステップＳ１５でホスト装置１４へ送信することになる。これにより、複数の第２のＩＣカード１２は並列的に処理を行なうことになる。

【００３６】

また、上記第２の方法の場合に、第１のＩＣカード１１は複数の第２のＩＣカード１２をそれぞれ認識していて、順番にステップＳ１０～Ｓ１３の処理を実施しているが、その順番をランダムに実行していく方法も考えられる。

【００３７】

さらに、前記実施の形態では、第１、第２の認証用媒体として非接触形ＩＣカード（無線カード）を用いた場合について説明したが、本発明はこれに限定されるものではなく、たとえば、接触形ＩＣカードあるいは携帯電話機やＰＤＡなどの携帯端末装置を用いた場合にも同様に適用可能である。

【図面の簡単な説明】

【００３８】

【図１】本発明に係る認証システムおよび認証方法が適用される入退場管理システムの構成を概略的に示すブロック図。

【図２】第１、第２のＩＣカードの構成を概略的に示すブロック図。

【図３】リーダライタの構成を概略的に示すブロック図。

【図４】処理の流れを説明するフローチャート。

【図５】処理の流れを説明するフローチャート。

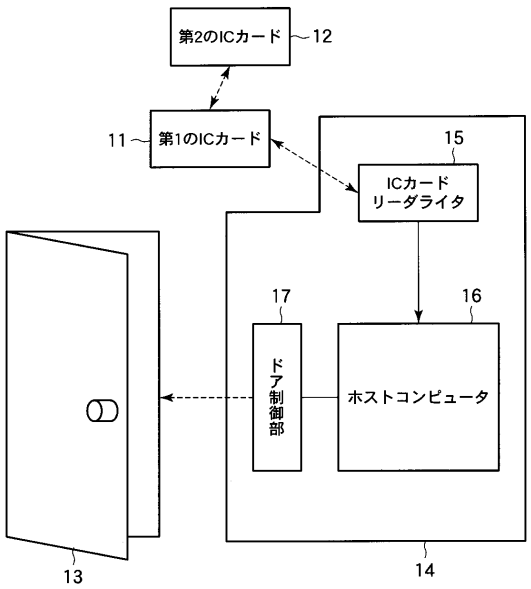
【符号の説明】

【００３９】

１１…第１のＩＣカード（第１の認証用媒体）、１２…第２のＩＣカード（第２の認証用媒体）、１３…ドア（入退場用のゲート）、１４…ホスト装置、１５…ＩＣカードリーダライタ、１６…ホストコンピュータ、１７…ドア制御部（ゲート制御手段）。

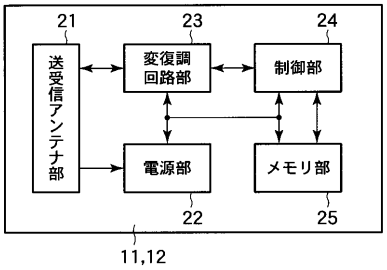
【図１】

図1



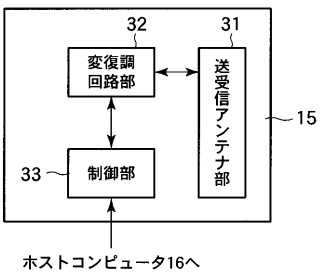
【図２】

図2



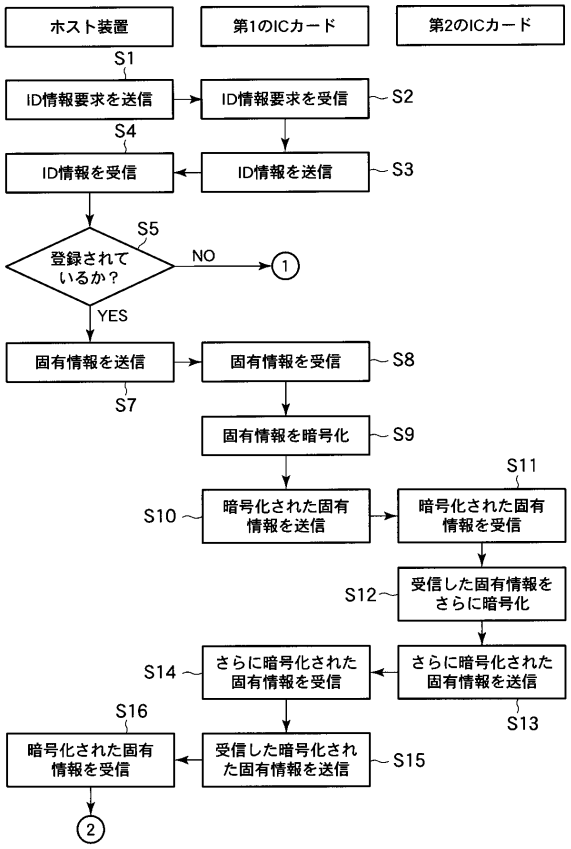
【図３】

図3



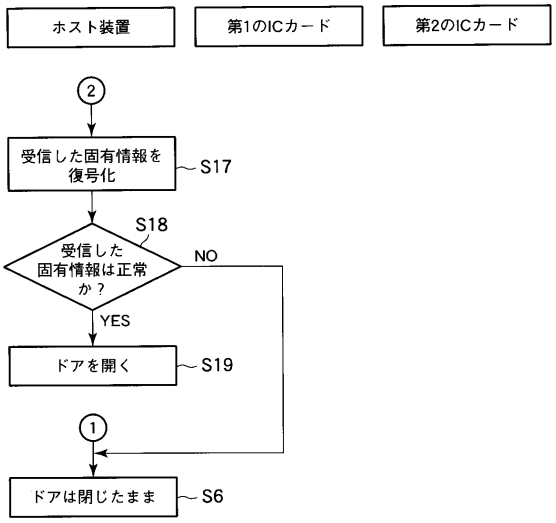
【図４】

図４


ホスト装置
第1のICカード
第2のICカード
S1
ID情報要求を送信
ID情報要求を受信
S2
S4
ID情報を受信
ID情報を送信
S3
S5
登録されているか？
NO
1
YES
固有情報を送信
固有情報を受信
S8
S7
固有情報を暗号化
S9
S11
S10
暗号化された固有情報を送信
暗号化された固有情報を受信
S12
受信した固有情報をさらに暗号化
S14
さらに暗号化された固有情報を受信
さらに暗号化された固有情報を送信
S13
S16
暗号化された固有情報を受信
受信した暗号化された固有情報を送信
S15
2

【図５】

図５


ホスト装置
第1のICカード
第2のICカード
2
受信した固有情報を復号化
S17
S18
受信した固有情報は正常か？
NO
YES
ドアを開く
S19
1
ドアは閉じたまま
S6

フロントページの続き

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 小松 仁
東京都青梅市新町３丁目３番地の１ 東芝デジタルメディアエンジニアリング株式会社内

Ｆターム(参考) 5B058 CA17 KA13 KA31 KA35 YA11
5B285 AA04 CA41 CB08 CB62 CB64 CB72
5J104 AA07 KA01 KA04 PA07 PA16