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

特許第5514780号
(P5514780)

(45)発行日　平成26年6月4日(2014.6.4)　(24)登録日　平成26年4月4日(2014.4.4)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 6　(全 24 頁)

(21)出願番号　特願2011-189004(P2011-189004)
(22)出願日　平成23年8月31日(2011.8.31)
(65)公開番号　特開2013-51577(P2013-51577A)
(43)公開日　平成25年3月14日(2013.3.14)
審査請求日　平成24年6月13日(2012.6.13)

(73)特許権者　000003562
東芝テック株式会社
東京都品川区大崎一丁目１１番１号　ゲートシティ大崎ウエストタワー　東芝テック株式会社内
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100159651
弁理士　高倉　成男
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】通信システム、送信装置及び受信装置

(57)【特許請求の範囲】
【請求項１】
送信装置と、受信装置とを有する通信システムであって、
前記送信装置は、
暗号鍵を記憶する送信側鍵記憶部と、
周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵を送信するモジュールと通信する送信側モジュール通信部と、
前記送信側モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記送信側鍵記憶部を書込み許可状態にするとともに、前記送信側モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信する送信側ＩＤ処理部と、
前記送信側鍵記憶部が書込み許可状態のとき、前記送信側モジュール通信部を介して前記モジュールから受信した暗号鍵を前記送信側鍵記憶部に書き込む送信側書込部と、
前記送信側鍵記憶部に記憶された暗号鍵を用いて情報を暗号化する送信側暗号処理部と、
前記送信側暗号処理部が暗号化した情報を前記受信装置に送信する送信部と、
を備え、
前記受信装置は、
暗号鍵を記憶する受信側鍵記憶部と、
前記モジュールと通信する受信側モジュール通信部と、

前記送信装置から送信される前記暗号化された情報を受信する受信部と、
前記受信側モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記受信側鍵記憶部を書込み許可状態にするとともに、前記受信側モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信する受信側ＩＤ処理部と、
前記受信側鍵記憶部が書込み許可状態のとき、前記受信側モジュール通信部を介して前記モジュールから受信した暗号鍵を前記受信側鍵記憶部に書き込む受信側書込部と、
前記受信側鍵記憶部に記憶された暗号鍵を用いて前記受信部が受信する情報を復号化する受信側暗号処理部と、
を備えることを特徴とする通信システム。

【請求項２】
送信装置と、受信装置と、を有する通信システムであって、
前記送信装置は、
暗号鍵を記憶する送信側鍵記憶部と、
周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵及び所定の条件を示す電子チケットを送信するモジュールと通信する送信側モジュール通信部と、
前記送信側モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記送信側鍵記憶部を書込み許可状態にするとともに、前記送信側モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信する送信側ＩＤ処理部と、
前記送信側鍵記憶部が書込み許可状態のとき、前記送信側モジュール通信部を介して前記モジュールから受信した電子チケットにて示される条件が満たされる場合に、前記モジュールから受信した暗号鍵を前記送信側鍵記憶部に書き込む送信側書込部と、
前記送信側鍵記憶部に記憶された暗号鍵を用いて情報を暗号化する送信側暗号処理部と、
前記送信側暗号処理部が暗号化した情報を前記受信装置に送信する送信部と、
を備え、
前記受信装置は、
暗号鍵を記憶する受信側鍵記憶部と、
前記モジュールと通信する受信側モジュール通信部と、
前記送信装置から送信される前記暗号化された情報を受信する受信部と、
前記受信側モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記受信側鍵記憶部を書込み許可状態にするとともに、前記受信側モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信する受信側ＩＤ処理部と、
前記受信側鍵記憶部が書込み許可状態のとき、前記受信側モジュール通信部を介して前記モジュールから受信した電子チケットにて示される条件が満たされる場合に、前記モジュールから受信した暗号鍵を前記受信側鍵記憶部に書き込む受信側書込部と、
前記受信側鍵記憶部に記憶された暗号鍵を用いて、前記受信部が受信する情報を復号化する受信側暗号処理部と、
を備えることを特徴とする通信システム。

【請求項３】
暗号鍵を記憶する鍵記憶部と、
周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵を送信するモジュールと通信するモジュール通信部と、
前記モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記鍵記憶部を書込み許可状態にするとともに、前記モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信するＩＤ処理部と、
前記鍵記憶部が書込み許可状態のとき、前記モジュール通信部を介して前記モジュールから受信した暗号鍵を前記鍵記憶部に書き込む書込部と、

前記鍵記憶部に記憶された暗号鍵を用いて情報を暗号化する暗号処理部と、
前記暗号処理部が暗号化した情報を受信装置に送信する送信部と、
を備えることを特徴とする送信装置。
【請求項４】
暗号鍵を記憶する鍵記憶部と、
周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵及び所定の条件を示す電子チケットを送信するモジュールと通信するモジュール通信部と、
前記モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記鍵記憶部を書込み許可状態にするとともに、前記モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信するＩＤ処理部と、
前記鍵記憶部が書込み許可状態のとき、前記モジュール通信部を介して前記モジュールから受信した電子チケットにて示される条件が満たされる場合に、前記モジュールから受信した暗号鍵を前記鍵記憶部に書き込む書込部と、
前記鍵記憶部に記憶された暗号鍵を用いて情報を暗号化する暗号処理部と、
前記暗号処理部が暗号化した情報を受信装置に送信する送信部と、
を備えることを特徴とする送信装置。
【請求項５】
暗号鍵を記憶する鍵記憶部と、
周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵を送信するモジュールと通信するモジュール通信部と、
送信装置から送信される暗号化された情報を受信する受信部と、
前記モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記鍵記憶部を書込み許可状態にするとともに、前記モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信するＩＤ処理部と、
前記鍵記憶部が書込み許可状態のとき、前記モジュール通信部を介して前記モジュールから受信した暗号鍵を前記鍵記憶部に書き込む書込部と、
前記鍵記憶部に記憶された暗号鍵を用いて前記受信部が受信する情報を復号化する暗号処理部と、
を備えることを特徴とする受信装置。
【請求項６】
暗号鍵を記憶する鍵記憶部と、
周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵を送信するモジュールと通信するモジュール通信部と、
送信装置から送信される暗号化された情報を受信する受信部と、
前記モジュール通信部を介して前記モジュールから受信した前記ＩＤコードの正当性が確認されると、前記鍵記憶部を書込み許可状態にするとともに、前記モジュール通信部を介して前記モジュールに前記暗号鍵の送信要求データを送信するＩＤ処理部と、
前記鍵記憶部が書込み許可状態のとき、前記モジュール通信部を介して前記モジュールから受信した電子チケットにて示される条件が満たされる場合に、前記モジュールから受信した暗号鍵を前記鍵記憶部に書き込む書込部と、
前記鍵記憶部に記憶された暗号鍵を用いて、前記受信部が受信する情報を復号化する暗号処理部と、
を備えることを特徴とする受信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、情報を暗号化して送受信する通信システム、このシステムで用いられる送信装置及び受信装置に関する。
【背景技術】
【０００２】

従来、暗号鍵で暗号化した情報を送信装置から受信装置に送信し、受信装置で上記暗号鍵を用いて上記暗号化された情報を復号化し、元の情報を得て各種情報処理を行う通信システムがある。

【０００３】

例えば、商品の販売や役務の提供を行う店舗においては、ＰＯＳ（Point Of Sales）端末やカード決済に特化したカード決済端末等の処理端末にクレジットカード等を読み取るためのカード端末を接続し、このカード端末が読み取ったカードデータを暗号鍵で暗号化して上記処理端末に送信し、上記処理端末で暗号化されたカードデータを復号化し、元のカードデータを得て客の買い上げ商品の決済を行う通信システムが利用されている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０００－２９５２０９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

上記のような通信システムにおいて、同じ暗号鍵を恒久的に使用すると、複数の平文と暗号文の組から鍵を推定する既知平文攻撃により暗号鍵が漏洩する虞がある。暗号鍵が漏洩すると、端末間で送受信される情報が漏洩したり改ざんされたりしかねない。

【０００６】

このような事情から、通信システムにて使用される暗号鍵の危殆化を防止して、システムのセキュリティ性を向上させる必要があった。

【課題を解決するための手段】

【０００７】

一実施形態に係る通信システムは、送信装置と、受信装置とを有する。送信装置は、暗号鍵を記憶する送信側鍵記憶部と、周期的にＩＤコードを送信し、暗号鍵の送信要求データを受信すると暗号鍵を送信するモジュールと通信する送信側モジュール通信部と、前記送信側モジュール通信部を介してモジュールから受信したＩＤコードの正当性が確認されると、送信側鍵記憶部を書込み許可状態にするとともに、送信側モジュール通信部を介してモジュールに暗号鍵の送信要求データを送信する送信側ＩＤ処理部と、送信側鍵記憶部が書込み許可状態のとき、送信側モジュール通信部を介してモジュールから受信した暗号鍵を送信側鍵記憶部に書き込む送信側書込部と、送信側鍵記憶部に記憶された暗号鍵を用いて情報を暗号化する送信側暗号処理部と、前記送信側暗号処理部が暗号化した情報を前記受信装置に送信する送信部と、を備える。受信装置は、暗号鍵を記憶する受信側鍵記憶部と、前記モジュールと通信する受信側モジュール通信部と、前記送信装置から送信される前記暗号化された情報を受信する受信部と、前記受信側モジュール通信部を介してモジュールから受信したＩＤコードの正当性が確認されると、受信側鍵記憶部を書込み許可状態にするとともに、受信側モジュール通信部を介してモジュールに暗号鍵の送信要求データを送信する受信側ＩＤ処理部と、受信側鍵記憶部が書込み許可状態のとき、受信側モジュール通信部を介してモジュールから受信した暗号鍵を受信側鍵記憶部に書き込む受信側書込部と、受信側鍵記憶部に記憶された暗号鍵を用いて受信部が受信する情報を復号化する受信側暗号処理部と、を備える。

【図面の簡単な説明】

【０００８】

【図１】第１の実施形態に係るカード処理システムの全体構成図。

【図２】同実施形態に係るカード端末，ＰＯＳ端末の構成を示すブロック図。

【図３】同実施形態に係る無線ＩＤモジュールの構成を示すブロック図。

【図４】同実施形態に係る無線ＩＤモジュールの動作を示すフローチャート。

【図５】同実施形態に係るＩＤ信号データの構造例を示す図。

【図６】同実施形態に係る受信確認信号データの構造例を示す図。

【図７】同実施形態に係る暗号鍵信号データの構造例を示す図。
【図８】同実施形態に係るカード端末の動作を示すフローチャート。
【図９】同実施形態に係るＰＯＳ端末の動作を示すフローチャート。
【図１０】第２の実施形態に係るカード処理システムの全体構成図。
【図１１】同実施形態に係るカード端末，ＰＯＳ端末の構成を示すブロック図。
【図１２】同実施形態に係る無線ＩＤモジュールの構成を示すブロック図。
【図１３】同実施形態に係る従業員予定ＤＢの構造例を示す図。
【図１４】同実施形態に係る端末鍵ＤＢの構造例を示す図。
【図１５】同実施形態に係る入場管理装置の構成を示すブロック図。
【図１６】同実施形態に係る入場管理装置の動作を示すフローチャート。
【図１７】同実施形態に係るＩＤモジュールデータの構造例を示す図。
【図１８】同実施形態に係る受信確認信号データの構造例を示す図。
【図１９】同実施形態に係る無線ＩＤモジュールの動作を示すフローチャート。
【図２０】同実施形態に係るチケット信号データの構造例を示す図。
【図２１】同実施形態に係るカード端末の動作を示すフローチャート。
【図２２】同実施形態に係るＰＯＳ端末の動作を示すフローチャート。
【発明を実施するための形態】
【０００９】
以下、いくつかの実施形態について図面を参照しながら説明する。
なお、以下に説明する第１，第２の実施形態においては、通信システムの一例として、小売店にてカード決済に使用されるカード処理システムを例示し、カードデータの暗号化方式として、暗号鍵と復号鍵が同一である共通鍵方式を採用した場合について述べる。
【００１０】
（第１の実施形態）
［システム構成］
図１は、第１の実施形態に係るカード処理システムの全体構成図である。
このカード処理システムは、店舗１に配置されたカード端末Ａ及びＰＯＳ端末Ｂと、インターネット等のネットワーク２と、カード決済事業の運営センタ等に設置された決済サーバ３とを備えている。このうち、カード端末ＡとＰＯＳ端末Ｂとが有線又は無線にて相互通信可能に接続され、ＰＯＳ端末Ｂと、決済サーバ３とがネットワーク２を介して相互通信可能に接続されている。
【００１１】
カード端末Ａは、本実施形態に係る送信装置として機能するものであり、磁気タイプあるいはＩＣタイプのクレジットカード等のカードＣからカード信号を取り込むリーダユニット４を備え、このリーダユニット４が取り込んだカード信号に基づいてカードデータを生成してＰＯＳ端末Ｂに送信する。なお、カード端末Ａは、リーダユニット４に加え、暗証番号等入力用のテンキーやディスプレイを備えたピンパッドであってもよい。
【００１２】
ＰＯＳ端末Ｂは、本実施形態に係る受信装置として機能するものであり、各種情報を表示する表示部や客が購入しようとする商品に関する情報（以下、商品情報と称す）を入力するための入力部等を備えており、上記入力部の操作により入力された商品情報と、カード端末Ａから受信したカードデータとを用いて、商品の代金をカード決済する装置である。
【００１３】
決済サーバ３は、カードＣの名義人に関する情報等を管理すると共に、ＰＯＳ端末Ｂがカード決済に用いるカードデータに含まれる暗証番号の認証やオーソリゼーション（与信照会）等の決済に関わる処理を行う。
【００１４】
本実施形態に係るカード端末Ａ及びＰＯＳ端末Ｂは、無線ＩＤモジュール５と通信する機能を備える。無線ＩＤモジュール５は、例えば従業員毎に用意され、従業員の名札に取

り付けられる。
【００１５】
［カード端末Ａ、ＰＯＳ端末Ｂ、無線ＩＤモジュールの要部構成］
カード端末Ａ、ＰＯＳ端末Ｂ、及び無線ＩＤモジュール５の要部構成について説明する。図２はカード端末Ａ及びＰＯＳ端末Ｂの要部構成を示すブロック図であり、図３は無線ＩＤモジュール５の要部構成を示すブロック図である。
【００１６】
図２に示すように、カード端末Ａは、ＣＰＵ（Central Processing Unit）１００、データ入力部１０１、コード化部１０２、暗号処理部１０３、通信鍵記憶部１０４、ＲＦ（Radio Frequency）送受信部１０５、ＩＤ検査部１０６、鍵抽出書込部１０７、端末通信部１０８、及びアンテナ１０９等を備えている。暗号処理部１０３は、本実施形態に係る送信側暗号処理部として機能し、ＲＦ送受信部１０５は、本実施形態に係る送信側モジュール通信部として機能し、端末通信部１０８は、本実施形態に係る送信部として機能する。
【００１７】
ＰＯＳ端末Ｂは、ＣＰＵ２００、カード決済処理部２０２、暗号処理部２０３、通信鍵記憶部２０４、ＲＦ送受信部２０５、ＩＤ検査部２０６、鍵抽出書込部２０７、端末通信部２０８、及びアンテナ２０９等を備えている。暗号処理部２０３は、本実施形態に係る受信側暗号処理部として機能し、ＲＦ送受信部２０５は、本実施形態に係る受信側モジュール通信部として機能し、端末通信部２０８は、本実施形態に係る受信部として機能する。
【００１８】
図３に示すように、無線ＩＤモジュール５は、ＣＰＵ３００、ＲＦ送受信部３０１、ＩＤ記憶部３０２、暗号鍵記憶部３０３、及びアンテナ３０４等を備えている。無線ＩＤモジュール５のＩＤ記憶部３０２は、無線ＩＤモジュール５の所持者である従業員に割り当てられた利用者ＩＤを記憶し、暗号鍵記憶部３０３は、無線ＩＤモジュール５の所持者である従業員に割り当てられた暗号鍵Ｋｙを記憶している。
【００１９】
なお、カード端末Ａ、ＰＯＳ端末Ｂ、及び無線ＩＤモジュール５が備える各部やＣＰＵ１００，２００，３００の動作は、それぞれＣＰＵ１００，２００，３００がカード端末Ａ、ＰＯＳ端末Ｂ、及び無線ＩＤモジュール５が備えるＲＯＭ等に記憶されたコンピュータプログラムを実行することでソフトウェア的に実現されてもよいし、回路等によってハードウェア的に実現されてもよい。また、ソフトウェアとハードウェアとを協動させることで実現されてもよい。
【００２０】
カード端末Ａの端末通信部１０８とＰＯＳ端末Ｂの端末通信部２０８は、有線又は無線にて相互に通信する。各ＲＦ送受信部１０５，２０５，３０１は、それぞれに接続されたアンテナ１０９，２０９，３０４が送受信する電波を介して相互に無線通信する。
【００２１】
無線ＩＤモジュール５のＲＦ送受信部３０１の送信出力（送信電力）は、カード端末Ａ及びＰＯＳ端末Ｂの近辺に無線ＩＤモジュール５が所在する場合に、アンテナ３０４から送信される電波がカード端末Ａ及びＰＯＳ端末Ｂのアンテナ１０９，２０９で受信できる程度の値に設定されている。カード端末Ａ及びＰＯＳ端末ＢのＲＦ送受信部１０５，２０５の送信出力は、上記従業員の立ち位置付近に所在する無線ＩＤモジュール５と良好な通信ができるように十分大きな値に設定されている。
【００２２】
さて、本実施形態においては、無線ＩＤモジュール５を所持する従業員がカード端末Ａ及びＰＯＳ端末Ｂの近辺に所在するときに限り、カード端末ＡとＰＯＳ端末Ｂとの間でカードデータの送受信が可能となる。このような機能を実現すべく、図２，図３に示した各部によって行われる動作の詳細を、図４～図９を用いて説明する。

【００２３】
［無線ＩＤモジュール５の動作］
無線ＩＤモジュール５は、例えば所持者である従業員がカード端末Ａ及びＰＯＳ端末Ｂの操作を担当すべく各端末Ａ，Ｂの設置場所に移動した際に当該従業員の手動で電源がオンされ、図４のフローチャートに示す処理を開始する。
【００２４】
すなわち、先ず無線ＩＤモジュール５のＲＦ送受信部３０１がＩＤ記憶部３０２に記憶された利用者ＩＤを含むＩＤ信号データをアンテナ３０４から送信するとともに（ステップＳ１０１）、後述のステップＳ２０４，Ｓ３０４においてカード端末ＡやＰＯＳ端末Ｂから返信される受信確認信号データの受信処理を実行する（ステップＳ１０２）。この受信処理において、ＲＦ送受信部３０１は、アンテナ３０４にて受信される信号を復調してＣＰＵ３００に出力する。
【００２５】
ＩＤ信号データは、例えば図５に示すように、スタートビット“０ｘ０００００”と、ＩＤ記憶部３０２に記憶された利用者ＩＤを示すビット列と、ストップビット“０ｘＦ０Ｆ０”とを有する。受信確認信号データは、図６に示すように、スタートビット“０ｘＦＦ００”と、フラグデータを示すビット列と、ストップビット“０ｘＦ０Ｆ０”とを有する。本実施形態に係るフラグデータは、通常確認を示す“０”、暗号鍵要求を示す“１”のいずれかにセットされる。
【００２６】
ＣＰＵ３００は、ＲＦ送受信部３０１からの入力データに基づき、受信確認信号データを正常に受信できたかどうかを判定する（ステップＳ１０３）。具体的には、入力データから図６に示した受信確認信号データのスタートビットとストップビットの検出を試み、各ビットが検出されたならばその間に在るデータをフラグデータとして抽出する。そして、スタートビットとストップビットを検出できない場合や、検出できたがフラグデータが“０”又は“１”のいずれでもない場合には、受信確認信号データを正常に受信できていないと判定し、“０”又は“１”のフラグデータが抽出できた場合には受信確認信号データを正常に受信できたと判定する。
【００２７】
受信確認信号データを正常に受信できていないと判定した場合（ステップＳ１０３のＮｏ）、ステップＳ１０１に戻る。このようにステップＳ１０１～Ｓ１０３が繰り返されることで、無線ＩＤモジュール５から周期的にＩＤ信号データが送信される。
【００２８】
一方、受信確認信号データを正常に受信できている場合（ステップＳ１０３のＹｅｓ）、ＣＰＵ３００は、当該受信確認信号データから抽出したフラグデータに基づき、暗号鍵送信の要求の有無を検査し（ステップＳ１０４）、その結果を判定する（ステップＳ１０５）。
【００２９】
フラグデータが“１”以外を示すならば、ＣＰＵ３００は、暗号鍵の送信が要求されていないと判定し（ステップＳ１０５のＮｏ）、ステップＳ１０１に戻る。フラグデータが“１”を示すならば、ＣＰＵ３００は、暗号鍵の送信が要求されていると判定する（ステップＳ１０５のＹｅｓ）。この場合、ＲＦ送受信部３０１が暗号鍵記憶部３０３に記憶された暗号鍵Ｋｙを含む暗号鍵信号データをアンテナ３０４から返信するとともに（ステップＳ１０６）、後述のステップＳ２０７，Ｓ３０７においてカード端末ＡやＰＯＳ端末Ｂから返信される受信確認信号データの受信処理を実行する（ステップＳ１０７）。この受信処理において、ＲＦ送受信部３０１は、アンテナ３０４にて受信される信号を復調してＣＰＵ３００に出力する。
【００３０】
暗号鍵信号データは、例えば図７に示すように、スタートビット“０ｘ００００”と、暗号鍵記憶部３０３に記憶された暗号鍵Ｋｙを示すビット列と、ストップビット“０ｘＦ

０Ｆ０”とを有する。
【００３１】
ＣＰＵ３００は、ＲＦ送受信部３０１からの入力データに基づき、受信確認信号データを正常に受信できたかどうかを判定する（ステップＳ１０８）。具体的には、ステップＳ１０３と同様にスタートビットとストップビットの検出を試み、各ビットが検出されたならばその間に在るデータをフラグデータとして抽出し、各ビットを検出できない場合や、検出できたがフラグデータが“１”である場合には、受信確認信号データを正常に受信できていないと判定し、“０”のフラグデータが抽出できた場合には受信確認信号データを正常に受信できたと判定する。
【００３２】
受信確認信号データを正常に受信できていないと判定した場合（ステップＳ１０８のＮｏ）、ステップＳ１０６に戻る。一方、受信確認信号データを正常に受信できていると判定した場合（ステップＳ１０８のＹｅｓ）、ステップＳ１０１に戻る。
以上で無線ＩＤモジュール５の動作の説明を終える。
【００３３】
［カード端末Ａの動作］
カード端末Ａは、例えば店舗の営業が開始された際に電源がオンされ、図８のフローチャートに示す処理を開始する。なお、処理開始当初においては、通信鍵記憶部１０４に暗号鍵Ｋｙが記憶されておらず、ＰＯＳ端末Ｂへのカードデータの送信が不可能な状態にある。
【００３４】
このフローチャートにおいて、先ずＲＦ送受信部１０５が上述のステップＳ１０１にて無線ＩＤモジュール５から送信されるＩＤ信号データの受信処理を実行する（ステップＳ２０１）。この受信処理において、ＲＦ送受信部１０５は、アンテナ１０９にて受信される信号を復調してＩＤ検査部１０６に出力する。
【００３５】
ＩＤ検査部１０６は、ＲＦ送受信部１０５からの入力データに基づき利用者ＩＤの正当性を確認する（ステップＳ２０２）。具体的には、ＩＤ検査部１０６は、入力データから図５に示したＩＤ信号データのスタートビットとストップビットの検出を試み、各ビットが検出されたならばその間に在るデータを利用者ＩＤとして抽出する。さらに、ＩＤ検査部１０６は、複数の従業員の正当な利用者ＩＤからなるリストを予め記憶しており、これらの利用者ＩＤに上記抽出した利用者ＩＤが含まれるかどうかを検査する。ＩＤ信号データのスタートビットとストップビットを検出できない場合や、検出できたが抽出した利用者ＩＤが上記リストに含まれていない場合には（ステップＳ２０２のＮｏ）、ステップＳ２０１に戻る。
【００３６】
一方、上記リストに含まれる利用者ＩＤを抽出できた場合（ステップＳ２０２のＹｅｓ）、ＩＤ検査部１０６は、カード読取機能を有効化する（ステップＳ２０３）。具体的には、通信鍵記憶部１０４を暗号鍵の書き込みを許可する状態に移行させる。
【００３７】
ステップＳ２０３の後、ＲＦ送受信部１０５がフラグデータを“１”とした受信確認信号データをアンテナ１０９から送信し（ステップＳ２０４）、暗号鍵信号データの受信処理を実行する（ステップＳ２０５）。この受信処理において、ＲＦ送受信部１０５は、アンテナ１０９にて受信される信号を復調して鍵抽出書込部１０７に出力する。フラグデータが“１”の受信確認信号データを無線ＩＤモジュール５が受信すると、上述のステップＳ１０６の通り該モジュール５から暗号鍵Ｋｙを含む暗号鍵信号データが返信される。
【００３８】
鍵抽出書込部１０７は、ＲＦ送受信部１０５からの入力データから図７に示した暗号鍵信号データのスタートビットとストップビットの検出を試み、各ビットが検出されたならばその間に在るデータを暗号鍵Ｋｙとして抽出する（ステップＳ２０６）。

【００３９】
暗号鍵Ｋｙを抽出したならば、ＲＦ送受信部１０５がフラグデータを“０”とした受信確認信号データをアンテナ１０９から返信し（ステップＳ２０７）、鍵抽出書込部１０７が抽出した暗号鍵Ｋｙを通信鍵記憶部１０４に記憶する（ステップＳ２０８）。
【００４０】
ステップＳ２０７にて送信された受信確認信号データを無線ＩＤモジュール５が受信すると、該モジュール５では上述の通りステップＳ１０１からの処理が再び実行され、無線ＩＤモジュール５から周期的にＩＤ信号データが送信される。
【００４１】
ステップＳ２０８の後、暗号処理部１０３がＰＯＳ端末Ｂでカードデータ受信の準備が整っているか否かを確認する（ステップＳ２０９）。具体的には、暗号処理部１０３が予め定められた確認メッセージを通信鍵記憶部１０４に記憶された暗号鍵Ｋｙにて暗号化し、暗号化された後の確認メッセージを端末通信部１０８がＰＯＳ端末Ｂに送信し、ＰＯＳ端末Ｂから返信されるデータの受信処理を実行する。上記確認メッセージは、カード端末Ａ及びＰＯＳ端末Ｂの双方で既知であるとする。暗号化された確認メッセージをＰＯＳ端末Ｂの端末通信部２０８が受信すると、暗号処理部２０３が通信鍵記憶部２０４に記憶された暗号鍵Ｋｙを用いて当該メッセージの復号化を試みる。その結果、元の確認メッセージを復元できたならば、暗号処理部２０３は、端末通信部２０８を介して準備完了を示すメッセージを返信する。一方、通信鍵記憶部２０４に暗号鍵Ｋｙが記憶されていない場合や、記憶されているが元の確認メッセージを復元できない場合には、端末通信部２０８が準備未完を示すメッセージを返信する。
【００４２】
ステップＳ２０９の後、暗号処理部１０３は、確認結果を判定する（ステップＳ２１０）。端末通信部１０８が受信したＰＯＳ端末Ｂからのメッセージが準備未完を示すならば（ステップＳ２１０のＮｏ）、ステップＳ２０９に戻る。
【００４３】
一方、ＰＯＳ端末Ｂからのメッセージが準備完了を示すならば（ステップＳ２１０のＹｅｓ）、ＲＦ送受信部１０５が上述のステップＳ１０１にて無線ＩＤモジュール５から送信されるＩＤ信号データの受信処理を実行する（ステップＳ２１１）。この受信処理において、ＲＦ送受信部１０５は、アンテナ１０９にて受信される信号を復調してＩＤ検査部１０６に出力する。
【００４４】
ＩＤ検査部１０６は、ＲＦ送受信部１０５からの入力データに基づき利用者ＩＤの正当性を確認する（ステップＳ２１２）。具体的には、ＩＤ検査部１０６は、入力データから図５に示したＩＤ信号データのスタートビットとストップビットの検出を試み、各ビットが検出されたならばその間に在るデータを利用者ＩＤとして抽出する。さらに、ＩＤ検査部１０６は、抽出した利用者ＩＤがステップＳ２０１にて受信した利用者ＩＤと同一であるかどうかを判定する。
【００４５】
ＩＤ検査部１０６がステップＳ２０１にて受信したものと同一の利用者ＩＤを抽出できた場合（ステップＳ２１２のＹｅｓ）、カード読取処理が実行される（ステップＳ２１３）。この処理が実行された際にリーダユニット４にカードが挿入されていると、リーダユニット４が当該カードに記憶された情報を読み取ってカード信号を生成し、データ入力部１０１に出力する。データ入力部１０１は、入力されたカード信号をデジタル信号に整形し、コード化部１０２に出力する。コード化部１０２は、データ入力部１０１から入力されたカード信号をコード化してカードデータを生成し、暗号処理部１０３に出力する。
【００４６】
カード読取処理にてカードデータが入力されると、暗号処理部１０３が通信鍵記憶部１０４に記憶された暗号鍵Ｋｙで当該カードデータを暗号化し、端末通信部１０８が暗号化後のカードデータをＰＯＳ端末Ｂに送信する（ステップＳ２１４）。

【００４７】
その後、ステップＳ２１１に戻る。なお、カード読取処理の実行時にリーダユニット４にカードが挿入されていないならば、ステップＳ２１３，Ｓ２１４で実質的な処理は行われず、ステップＳ２１１に戻る。
【００４８】
このように、通信鍵記憶部１０４に暗号鍵Ｋｙが一旦記憶された後には、その暗号鍵Ｋｙの送信元である無線ＩＤモジュール５から送信される利用者ＩＤが受信できる限り、カードの読み取り、読み取ったカードデータの暗号化、及び、暗号化したカードデータのＰＯＳ端末Ｂへの送信が可能となる。
【００４９】
一方、ステップＳ２１２において、ＩＤ信号データのスタートビットとストップビットを検出できない場合や、検出できたが抽出された利用者ＩＤがステップＳ２０１にて受信した利用者ＩＤと同一でない場合には（ステップＳ２１２のＮｏ）、それまでカード端末Ａの近辺にいた従業員がレジから離れたことになる。この場合、暗号処理部１０３は、通信鍵記憶部１０４に記憶された暗号鍵Ｋｙを消去することで、カード読取機能を無効化する（ステップＳ２１５）。その後、ステップＳ２０１からの処理が再び実行される。
【００５０】
以上でカード端末Ａの動作の説明を終える。
【００５１】
［ＰＯＳ端末Ｂの動作］
ＰＯＳ端末Ｂは、例えば店舗の営業が開始された際にカード端末Ａとともに電源がオンされ、図９のフローチャートに示す処理を開始する。なお、処理開始当初においては、通信鍵記憶部２０４に暗号鍵Ｋｙが記憶されておらず、カード端末Ａからのカードデータの受信が不可能な状態にある。
【００５２】
このフローチャートにおいて、ステップＳ３０１～Ｓ３１２の処理は、ステップＳ２０１～Ｓ２１２の処理と同様である。
すなわち、ＲＦ送受信部２０５が上述のステップＳ１０１にて無線ＩＤモジュール５から送信されるＩＤ信号データの受信処理を実行し（ステップＳ３０１）、ＩＤ検査部２０６がＲＦ送受信部２０５からの入力データに基づき利用者ＩＤの正当性を確認し（ステップＳ３０２）、ＩＤ信号データのスタートビットとストップビットを検出できない場合や、検出できたがＩＤ検査部２０６が予め記憶したリストに抽出された利用者ＩＤが含まれていない場合には（ステップＳ３０２のＮｏ）、ステップＳ３０１に戻る。
【００５３】
一方、上記リストに含まれる利用者ＩＤを抽出できた場合（ステップＳ３０２のＹｅｓ）、ＩＤ検査部２０６がカード読取機能を有効化し（ステップＳ３０３）、ＲＦ送受信部２０５がフラグデータを“１”とした受信確認信号データをアンテナ２０９から返信し（ステップＳ３０４）、暗号鍵信号データの受信処理を実行する（ステップＳ３０５）。そして、鍵抽出書込部２０７がＲＦ送受信部２０５からの入力データから暗号鍵信号データのスタートビットとストップビットの検出を試み、各ビットが検出されたならばその間に在るデータを暗号鍵Ｋｙとして抽出し（ステップＳ３０６）、ＲＦ送受信部２０５がフラグデータを“０”とした受信確認信号データをアンテナ２０９から返信し（ステップＳ３０７）、鍵抽出書込部２０７が抽出した暗号鍵Ｋｙを通信鍵記憶部２０４に記憶する（ステップＳ３０８）。
【００５４】
ステップＳ３０８の後、カード端末Ａでカードデータ送信の準備が整っているか否かを、ステップＳ２０９と同様の手法で確認する（ステップＳ３０９）。すなわち、暗号処理部２０３が上記確認メッセージを通信鍵記憶部２０４に記憶された暗号鍵Ｋｙにて暗号化し、端末通信部２０８が暗号化後の確認メッセージをカード端末Ａに送信し、カード端末Ａから返信されるデータの受信処理を実行する。暗号化された確認メッセージをカード端

末Ａの端末通信部１０８が受信すると、暗号処理部１０３が通信鍵記憶部１０４に記憶された暗号鍵Ｋｙを用いて当該メッセージの復号化を試みる。その結果、元の確認メッセージを復元できたならば、端末通信部１０８が準備完了を示すメッセージを返信する。一方、通信鍵記憶部１０４に暗号鍵Ｋｙが記憶されていない場合や、記憶されているが元の確認メッセージを復元できない場合には、端末通信部１０８が準備未完を示すメッセージを返信する。

【００５５】

ステップＳ３０９の後、暗号処理部２０３は、確認結果を判定し（ステップＳ３１０）、カード端末Ａから返信されたメッセージが準備未完を示すならば（ステップＳ３１０のＮｏ）、ステップＳ３０９に戻り、カード端末Ａから返信されたメッセージが準備完了を示すならば（ステップＳ３１０のＹｅｓ）、ＲＦ送受信部２０５が上述のステップＳ１０１にて無線ＩＤモジュール５から送信されるＩＤ信号データの受信処理を実行する（ステップＳ３１１）。そして、ＩＤ検査部２０６がＲＦ送受信部２０５からの入力データに基づき利用者ＩＤの正当性を確認する（ステップＳ３１２）。

【００５６】

以降の処理はカード端末Ａと異なる。すなわち、ＩＤ検査部２０６がステップＳ３０１で受信したものと同一の利用者ＩＤを抽出できた場合（ステップＳ３１２のＹｅｓ）、カードデータの受信処理が実行される（ステップＳ３１３）。この処理の実行中に、端末通信部２０８がカード端末Ａから暗号化されたカードデータを受信したならば、暗号処理部２０３が通信鍵記憶部２０４に記憶された暗号鍵Ｋｙにて当該受信したカードデータを復号化する（ステップＳ３１４）。復号化されたカードデータは、カード決済処理部２０２に出力される。

【００５７】

カード決済処理部２０２は、暗号処理部２０３から入力されたカードデータと、客が購入しようとする商品の商品情報とを用いて、当該商品の代金を決済処理する（ステップＳ３１５）。商品情報は、このフローチャートに示す処理と平行して実行される商品登録処理において、ＰＯＳ端末Ｂが備える入力部の操作等により入力される。

【００５８】

ステップＳ３１５の処理において、カード決済処理部２０２は、入力されたカードデータや客が購入しようとする商品の商品情報をカード決済事業の運営センタが定めた暗号鍵にて暗号化し、ネットワーク２を介して決済サーバ３に送信する。決済サーバ３は、ＰＯＳ端末Ｂから受信した暗号化されたカードデータを復号化し、カードデータに含まれる暗証番号の認証やオーソリゼーションを行い、その結果をネットワーク２を介してＰＯＳ端末Ｂに返信する。カード決済処理部２０２は、決済サーバ３からカード決済を許可する旨の結果を得たならば、図示せぬプリンタから取引の伝票を発行し、客が購入しようとする商品の商品情報や当該店舗の情報等をネットワーク２を介して決済サーバ３に送信するなどして決済処理を完了させる。

【００５９】

ステップＳ３１５の後、ステップＳ３１１に戻る。なお、カードデータの受信処理の実行時にカード端末Ａからカードデータが受信されないならば、ステップＳ３１３～Ｓ３１５で実質的な処理は行われず、ステップＳ３１１に戻る。

【００６０】

このように、通信鍵記憶部２０４に暗号鍵Ｋｙが一旦記憶された後には、その暗号鍵Ｋｙの送信元である無線ＩＤモジュール５から送信される利用者ＩＤが受信できる限り、カードデータの受信、受信したカードデータの復号化、及び、復号化したカードデータを用いた決済処理の実行が可能となる。

【００６１】

一方、ステップＳ３１２において、ＩＤ信号データのスタートビットとストップビットを検出できない場合や、検出できたが抽出された利用者ＩＤがステップＳ３０１で受信した利用者ＩＤと同一でない場合には（ステップＳ３１２のＮｏ）、それまでＰＯＳ端末Ｂ

の近辺にいた従業員がレジから離れたことになる。この場合、暗号処理部２０３は、通信鍵記憶部２０４に記憶された暗号鍵Ｋｙを消去することで、カードデータ読取機能を無効化する（ステップＳ３１６）。その後、ステップＳ３０１からの処理が再び実行される。

【００６２】

以上でＰＯＳ端末Ｂの動作の説明を終える。

【００６３】

以上説明したように、第１の実施形態では、カード端末Ａ及びＰＯＳ端末Ｂの双方において、カード端末Ａ及びＰＯＳ端末Ｂが無線ＩＤモジュール５から正当な利用者ＩＤを受信できる間、該モジュール５に記憶された暗号鍵Ｋｙを用いたカードデータの暗号文通信が可能となる。このような構成であれば、カード端末Ａ及びＰＯＳ端末Ｂを操作しようとする者が正当な利用者である場合に限り、カードデータの暗号文通信が行われるので、第３者の不正な操作によってカードデータや暗号鍵が漏洩するような事態を防止できる。

【００６４】

さらに、暗号鍵は無線ＩＤモジュール５からカード端末Ａ及びＰＯＳ端末Ｂに供給されるので、各端末を利用する従業員が変更される毎に暗号鍵も変更されることになる。したがって、既知平文攻撃への耐性が高まり、通信システムのセキュリティ性が格段に向上する。しかも、面倒なメンテナンス作業を要することなく、暗号鍵を変更できる。

【００６５】

また、カード端末Ａ及びＰＯＳ端末Ｂに記憶される暗号鍵は、無線ＩＤモジュール５から利用者ＩＤを受信できなくなったときに消去されるので、カード端末Ａ及びＰＯＳ端末Ｂから不正に暗号鍵が取得されることもない。

【００６６】

その他にも、第１の実施形態の構成からは、種々の好適な効果が得られる。

（第２の実施形態）

次に、第２の実施形態について説明する。第１の実施形態と同一の構成要素には同一の符号を付し、重複説明は必要な場合に限り行う。

【００６７】

［システム構成］

図１０は、本実施形態に係るカード処理システムの全体構成図である。なお、当該システムは、第１の実施形態と同様に、カード端末Ａ、ＰＯＳ端末Ｂ、及び決済サーバ３等を備えるが、図示を省略している。本実施形態に係るカード処理システムは、複数組のカード端末Ａ及びＰＯＳ端末Ｂを備えている。

【００６８】

図示したように、本実施形態に係るカード処理システムは、第１の実施形態にて説明した構成に加え、例えば店舗１の従業員入口に配置された入場管理装置６、生体情報読取装置７、及び無線リーダライタ８と、店舗１の事務室等に配置された従業員管理サーバ９とを備えている。入場管理装置６と従業員管理サーバ９は、店舗１内に設置されたＬＡＮ回線１０を介して接続されている。生体情報読取装置７及び無線リーダライタ８は、入場管理装置６に接続されている。

【００６９】

生体情報読取装置７は、人体から生体情報（バイオメトリクス情報）を読み取る装置である。読み取り対象の生体情報は、指紋や虹彩・網膜、又は静脈のパターン等、どのようなものであってもよい。

【００７０】

無線リーダライタ８は、電波を介して無線ＩＤモジュール５と無線通信し、無線ＩＤモジュール５からのデータの読み出しや、無線ＩＤモジュール５へのデータの書き込みを行う。

【００７１】

従業員管理サーバ９は、従業員に関する情報を管理する従業員予定ＤＢ１１（図１３参照）と、各ＰＯＳ端末Ｂに割り当てられた端末鍵ＳＫを記憶した端末鍵ＤＢ１２（図１４

参照）とを備えている。
【００７２】
［カード端末Ａ、ＰＯＳ端末Ｂ、無線ＩＤモジュールの要部構成］
本実施形態に係るカード端末Ａ、ＰＯＳ端末Ｂ、及び無線ＩＤモジュール５の要部構成について説明する。図１１はカード端末Ａ及びＰＯＳ端末Ｂの要部構成を示すブロック図であり、図１２は無線ＩＤモジュール５の要部構成を示すブロック図である。
【００７３】
図１１に示すように、カード端末Ａは、第１の実施形態にて説明した構成に加えて端末鍵記憶部１１０を備え、ＩＤ検査部１０６に代えてＩＤ・チケット検査部１１１を備えている。また、ＰＯＳ端末Ｂは、第１の実施形態にて説明した構成に加えて端末鍵記憶部２１０を備え、ＩＤ検査部２０６に代えてＩＤ・チケット検査部２１１を備えている。
【００７４】
各ＰＯＳ端末Ｂの端末鍵記憶部２１０には、自身に割り当てられた暗号鍵である端末鍵ＳＫが記憶されている。さらに、各カード端末Ａの端末鍵記憶部１１０には、自身に接続されたＰＯＳ端末Ｂに割り当てられた端末鍵ＳＫが記憶されている。
【００７５】
図１２に示すように、無線ＩＤモジュール５は、第１の実施形態にて説明した構成に加えて電子チケットＥＣを記憶するチケット記憶部３０５を備えている。
【００７６】
本実施形態にて追加又は変更した各部は、それぞれＣＰＵ１００，２００，３００がカード端末Ａ、ＰＯＳ端末Ｂ、及び無線ＩＤモジュール５が備えるＲＯＭ等に記憶されたコンピュータプログラムを実行することでソフトウェア的に実現されてもよいし、回路等によってハードウェア的に実現されてもよい。また、ソフトウェアとハードウェアとを協動させることで実現されてもよい。
【００７７】
［各ＤＢの構造］
図１３に示すように、従業員予定ＤＢ１１は、利用者ＩＤ、このＩＤで示される従業員に使用が許可されたＰＯＳ端末Ｂの識別子である利用端末ＩＤ、このＩＤで示されるＰＯＳ端末Ｂの利用が許可された時間帯を示す利用時間、及び、予め取得された当該従業員の生体情報を含む複数のレコードによって構成される。レコードは、従業員の数だけ用意される。
【００７８】
図１４に示すように、端末鍵ＤＢ１２は、利用端末ＩＤ、及びこのＩＤで示されるＰＯＳ端末Ｂに割り当てられた端末鍵ＳＫを含む複数のレコードによって構成される。レコードは、当該カード処理システムに含まれるＰＯＳ端末Ｂの数だけ用意される。
【００７９】
［入場管理装置６の要部構成］
図１５は、入場管理装置６の要部構成を示すブロック図である。
図１５に示すように、入場管理装置６は、ＣＰＵ６００、時刻処理部６０１、利用者認証処理部６０２、チケット生成部６０３、暗号鍵生成部６０４、及びＩＤモジュールデータ生成部６０５等を備えている。
【００８０】
入場管理装置６が備える各部は、ＣＰＵ６００が入場管理装置６に設けられたＲＯＭ等に記憶されたコンピュータプログラムを実行することでソフトウェア的に実現されてもよいし、回路等によってハードウェア的に実現されてもよい。また、ソフトウェアとハードウェアとを協動させることで実現されてもよい。
【００８１】
［入場管理装置６の動作］
本実施形態においては、従業員が店舗１に出勤した際に、入場管理装置６にて電子チケットＥＣ及び暗号鍵Ｋｙの発行を受け、電子チケットＥＣで規定された範囲内でカード端

末Ａ及びＰＯＳ端末Ｂを使用する。

【００８２】

電子チケットＥＣ及び暗号鍵Ｋｙの発行に関して、入場管理装置６、生体情報読取装置７、及び無線リーダライタ８は、図１６のフローチャートに示す処理を実行する。

すなわち、先ず利用者認証処理部６０２が無線リーダライタ８を介して無線ＩＤモジュール５と通信し、無線ＩＤモジュール５のＩＤ記憶部３０２に記憶された利用者ＩＤを受信する（ステップＳ４０１）。

【００８３】

続いて、生体情報読取装置７が従業員から生態情報を読み取り、利用者認証処理部６０２が当該生体情報に基づいて生体認証を行い（ステップＳ４０２）、従業員が正規の利用者であるかどうかを判定する（ステップＳ４０３）。具体的には、利用者認証処理部６０２は、ステップＳ４０１で受信した利用者ＩＤを含むレコードに記憶された生体情報を従業員予定ＤＢ１１から取得し、取得した生体情報と、生体情報読取装置７が読み取った生体情報との一致／不一致を判定する。利用者ＩＤに対応する生体情報が従業員予定ＤＢ１１から取得できない場合や、取得できたが生体情報が一致しない場合には従業員が正規の利用者でないと判定し（ステップＳ４０３のＮｏ）、ステップＳ４０１に戻る。

【００８４】

一方、生体情報が一致する場合には従業員が正規の利用者であると判定し（ステップＳ４０３のＹｅｓ）、時刻処理部６０１がステップＳ４０１で受信した利用者ＩＤを含む従業員予定ＤＢ１１のレコードから操作予定（利用時間、利用端末ＩＤ）を取得する（ステップＳ４０４）。

【００８５】

ステップＳ４０４の後、時刻処理部６０１は、時刻認証を行う（ステップＳ４０５）。具体的には、時刻処理部６０１は、現在時刻を図示せぬ時計回路から取得し、取得した時刻と、ステップＳ４０４で取得した利用時間とを比較する。取得した時刻が利用時間外であるならば時刻認証失敗と判定し（ステップＳ４０５のＮｏ）、ステップＳ４０１に戻る。

【００８６】

一方、取得した時刻が利用時間内であるならば時刻認証成功と判定する（ステップＳ４０５のＹｅｓ）。この場合、チケット生成部６０３がステップＳ４０１で取得した利用端末ＩＤを含む端末鍵ＤＢ１２のレコードから端末鍵ＳＫを取得する（ステップＳ４０６）。

【００８７】

続いて、チケット生成部６０３は、ステップＳ４０１で受信した利用者ＩＤと、ステップＳ４０４で取得した利用時間及び利用端末ＩＤとを、ステップＳ４０６で取得した端末鍵ＳＫで暗号化して電子チケットＥＣを生成する（ステップＳ４０７）。

【００８８】

さらに、暗号鍵生成部６０４が、チケット生成部６０３によって生成された電子チケットＥＣを暗号鍵生成アルゴリズムにて変換処理し、暗号鍵Ｋｙを生成する（ステップＳ４０８）。上記暗号鍵生成アルゴリズムは、例えばガロア体を用いた演算により変換元の情報から暗号鍵を生成するものなど、どのようなものを用いてもよい。

【００８９】

ステップＳ４０８の後、ＩＤモジュールデータ生成部６０５が、チケット生成部６０３によって生成された電子チケットＥＣと、暗号鍵生成部６０４によって生成された暗号鍵Ｋｙとを含むＩＤモジュールデータを生成し（ステップＳ４０９）、生成したＩＤモジュールデータと書き込みコマンドとを、無線リーダライタ８を介して無線ＩＤモジュール４１０に送信する（ステップＳ４１０）。

【００９０】

ＩＤモジュールデータは、例えば図１７に示すように、スタートビット“０ｘ０００００”と、利用者ＩＤを示すビット列と、データの区切りを示すセパレートビット“０ｘＦ３

Ｆ３”と、電子チケットＥＣを示すビット列と、セパレートビット“０ｘＦ３Ｆ３”と、暗号鍵Ｋｙを示すビット列と、ストップビット“０ｘＦ０Ｆ０”とを有する。

【００９１】

書き込みコマンドとともに上記のような構成のＩＤモジュールデータをアンテナ３０４及びＲＦ送受信部３０１を介して受信すると、無線ＩＤモジュール５のＣＰＵ３００は、スタートビットと最初のセパレートビットの間のビット列を利用者ＩＤとして認識し、セパレートビット間のビット列を電子チケットＥＣとして認識し、最後のセパレートビットとストップビットの間のビット列を暗号鍵Ｋｙとして認識する。そして、認識した利用者ＩＤと自身のＩＤ記憶部３０２に記憶された利用者ＩＤと比較し、両ＩＤが一致するならば認識した暗号鍵Ｋｙを暗号鍵記憶部３０３に、認識した電子チケットＥＣをチケット記憶部３０５にそれぞれ記憶する。このとき、既に記憶された暗号鍵Ｋｙや電子チケットＥＣがあるならば、上記認識した暗号鍵Ｋｙや電子チケットＥＣにてそれらを上書きする。

【００９２】

書き込みが正常に終了したならば、ＲＦ送受信部３０１がフラグデータを“０”とした受信確認信号データをアンテナ３０４から送信し、書き込みが正常に終了しなかったならば、ＲＦ送受信部３０１がフラグデータを“１”とした受信確認信号データをアンテナ３０４から送信する。ここでのフラグデータは、カード端末Ａ及びＰＯＳ端末Ｂとの通信で用いられるものと異なり、図１８に示すように“０”が書き込みの正常終了を示し、“１”が書き込みのエラー終了を示す。

【００９３】

ステップＳ４１０の後、無線リーダライタ８が受信確認信号データの受信処理を実行する（ステップＳ４１１）。この受信処理では、無線リーダライタ８が受信信号を復調してＩＤモジュールデータ生成部６０５に出力する。ＩＤモジュールデータ生成部６０５は、無線リーダライタ８からの入力データに基づき、書き込みが正常に完了したかどうかを判定する（ステップＳ４１２）。この処理では、ステップＳ１０３等と同様に、スタートビットとストップビットの検出が試行され、検出できたならば各ビットの間に在るデータをフラグデータとして抽出する。フラグデータが検出できない場合や、検出したフラグデータが“１”である場合には、書き込みが正常に完了していないと判定し（ステップＳ４１２のＮｏ）、ステップＳ４１０に戻る。

【００９４】

一方、“０”であるフラグデータが検出できた場合、ＩＤモジュールデータ生成部６０５は、書き込みが正常に完了したと判定する（ステップＳ４１２のＹｅｓ）。この場合、１つの無線ＩＤモジュール５に電子チケットＥＣ及び暗号鍵Ｋｙを書き込むための一連の処理が完了する。

【００９５】

正常に電子チケットＥＣ及び暗号鍵Ｋｙが書き込まれると、入場管理装置６に設けられたスピーカから音声を発するなどして従業員に報知する。この報知を受けた従業員は、例えば自身に割り当てられたカード端末Ａ及びＰＯＳ端末Ｂの設置場所に移動して、業務を開始する。

【００９６】

［無線ＩＤモジュール５の動作］

電子チケットＥＣ及び暗号鍵Ｋｙの書き込みを終えた無線ＩＤモジュール５は、図１９に示すフローチャートに沿って動作する。

ステップＳ１０１～１０５，Ｓ１０７，Ｓ１０８の処理は、第１の実施形態にて説明した処理と同じである。但し、本実施形態においては、ステップＳ１０６の処理に代えて、ステップＳ１０６ａの処理が実行される。

【００９７】

すなわち、暗号鍵の送信が要求されている場合（ステップＳ１０５のＹｅｓ）、ＲＦ送受信部３０１が暗号鍵記憶部３０３に記憶された暗号鍵Ｋｙ及びチケット記憶部３０５に記憶された電子チケットＥＣを含むチケット信号データをアンテナ３０４から送信する（

ステップＳ１０６ａ）。
【００９８】
チケット信号データは、例えば図２０に示すように、スタートビット“０ｘ００００”と、電子チケットＥＣを示すビット列と、セパレートビット“０ｘＦ３Ｆ３”と、暗号鍵Ｋｙを示すビット列と、ストップビット“０ｘＦ０Ｆ０”とを有する。
【００９９】
［カード端末Ａの動作］
本実施形態に係るカード端末Ａは、図２１に示すフローチャートに沿って動作する。
ステップＳ２０１～２０４，Ｓ２０７～Ｓ２１５の処理は、第１の実施形態にて説明した処理と同じである。但し、ステップＳ２０２，Ｓ２１２における利用者ＩＤの確認は、ＩＤ検査部１０６に代えてＩＤ・チケット検査部１１１が実行する。
【０１００】
本実施形態においては、ステップＳ２０５，Ｓ２０６の処理に代えてステップＳ２０５ａ，Ｓ２０５ｂ，Ｓ２０５ｃ，Ｓ２０６ａの処理が実行される。
すなわち、ステップＳ２０４にてフラグデータを“１”とした受信確認信号データをアンテナ１０９から送信した後、ＲＦ送受信部１０５がチケット信号データの受信処理を実行する（ステップＳ２０５ａ）。この受信処理において、ＲＦ送受信部１０５は、アンテナ１０９にて受信される信号を復調して鍵抽出書込部１０７及びＩＤ・チケット検査部１１１に出力する。フラグデータが“１”の受信確認信号データを無線ＩＤモジュール５が受信すると、上述のステップＳ１０６ａの通り電子チケットＥＣ及び暗号鍵Ｋｙを含むチケット信号データが返信される。
【０１０１】
ＩＤ・チケット検査部１１１は、ＲＦ送受信部１０５からの入力データから図２０に示したチケット信号データのスタートビットと最初のセパレートビットの検出を試み、各ビットが検出されたならばその間に在るデータを電子チケットＥＣとして抽出する（ステップＳ２０５ｂ）。
【０１０２】
そして、ＩＤ・チケット検査部１１１は、当該電子チケットＥＣで示される条件が満たされているかどうかを判定する（ステップＳ２０５ｃ）。具体的には、先ずＩＤ・チケット検査部１１１は、端末鍵記憶部１１０に記憶された端末鍵ＳＫで当該電子チケットＥＣを復号化する。そして、復号化した電子チケットＥＣに含まれる利用者ＩＤとステップＳ２０１で受信した利用者ＩＤとを比較し、電子チケットＥＣに含まれる利用時間と図示せぬ時計回路が計時する現在の時刻とを比較し、電子チケットＥＣに含まれる利用端末ＩＤと当該カード端末Ａの接続先であるＰＯＳ端末Ｂに割り当てられた利用端末ＩＤとを比較する。その結果、両利用者ＩＤが一致し、現在の時刻が利用時間に含まれ、両利用端末ＩＤが一致するならば、当該電子チケットＥＣで示される条件が満たされていると判定する。一方、これら３つの条件のうち、いずれか１つでも満たされないならば、当該電子チケットＥＣで示される条件が満たされていないと判定する。
【０１０３】
電子チケットＥＣで示される条件が満たされていないと判定した場合（ステップＳ２０５ｃのＮｏ）、ステップＳ２０１に戻る。
【０１０４】
一方、電子チケットＥＣで示される条件が満たされていると判定した場合（ステップＳ２０５ｃのＹｅｓ）、鍵抽出書込部１０７がＲＦ送受信部１０５から入力されたチケット信号データから暗号鍵Ｋｙを抽出する（ステップＳ２０６ａ）。このように抽出された暗号鍵ＫｙがステップＳ２０８にて通信鍵記憶部１０４に記憶され、ステップＳ２１４ではカードデータが当該暗号鍵Ｋｙを用いて暗号化され、ＰＯＳ端末Ｂに送信される。
【０１０５】
［ＰＯＳ端末Ｂの動作］
本実施形態に係るＰＯＳ端末Ｂは、図２２に示すフローチャートに沿って動作する。

ステップＳ３０１～３０４，Ｓ３０７～Ｓ３１６の処理は、第１の実施形態にて説明した処理と同じである。但し、ステップＳ３０２，Ｓ３１２における利用者ＩＤの確認は、ＩＤ検査部２０６に代えてＩＤ・チケット検査部２１１が実行する。

【０１０６】

本実施形態においては、ステップＳ３０５，Ｓ３０６の処理に代えてステップＳ３０５ａ，Ｓ３０５ｂ，Ｓ３０５ｃ，Ｓ３０６ａの処理が実行される。これらの処理は、ステップＳ２０５ａ，Ｓ２０５ｂ，Ｓ２０５ｃ，Ｓ２０６ａの処理と同様である。

すなわち、ステップＳ３０４にてフラグデータを“１”とした受信確認信号データをアンテナ２０９から送信した後、ＲＦ送受信部２０５がチケット信号データの受信処理を実行する（ステップＳ３０５ａ）。この受信処理において、ＲＦ送受信部２０５は、アンテナ２０９にて受信される信号を復調して鍵抽出書込部２０７及びＩＤ・チケット検査部２１１に出力する。フラグデータが“１”の受信確認信号データを無線ＩＤモジュール５が受信すると、上述のステップＳ１０６ａの通り電子チケットＥＣ及び暗号鍵Ｋｙを含むチケット信号データが返信される。

【０１０７】

ＩＤ・チケット検査部２１１は、ＲＦ送受信部２０５からの入力データから図２０に示したチケット信号データのスタートビットと最初のセパレートビットの検出を試み、各ビットが検出されたならばその間に在るデータを電子チケットＥＣとして抽出する（ステップＳ３０５ｂ）。

【０１０８】

そして、ＩＤ・チケット検査部２１１は、当該電子チケットＥＣで示される条件が満たされるかどうかを判定する（ステップＳ３０５ｃ）。具体的には、先ずＩＤ・チケット検査部２１１は、端末鍵記憶部２１０に記憶された端末鍵ＳＫで当該電子チケットＥＣを復号化する。そして、復号化した電子チケットＥＣに含まれる利用者ＩＤとステップＳ３０１で受信した利用者ＩＤとを比較し、電子チケットＥＣに含まれる利用時間と図示せぬ時計回路が計時する現在の時刻とを比較し、電子チケットＥＣに含まれる利用端末ＩＤと当該ＰＯＳ端末Ｂに割り当てられた利用端末ＩＤとを比較する。その結果、両利用者ＩＤが一致し、現在の時刻が利用時間に含まれ、両利用端末ＩＤが一致するならば、当該電子チケットＥＣで示される条件が満たされていると判定する。一方、これら３つの条件のうち、いずれか１つでも満たされないならば、当該電子チケットＥＣで示される条件が満たされていないと判定する。

【０１０９】

電子チケットＥＣで示される条件が満たされていないと判定した場合（ステップＳ３０５ｃのＮｏ）、ステップＳ３０１に戻る。

【０１１０】

一方、電子チケットＥＣで示される条件が満たされていると判定した場合（ステップＳ３０５ｃのＹｅｓ）、鍵抽出書込部２０７がＲＦ送受信部２０５から入力されたチケット信号データから暗号鍵Ｋｙを抽出する（ステップＳ３０６ａ）。このように抽出された暗号鍵ＫｙがステップＳ３０８にて通信鍵記憶部２０４に記憶され、ステップＳ３１５ではカード端末Ａから受信したカードデータが当該暗号鍵Ｋｙを用いて復号化される。

【０１１１】

以上説明したように、第２の実施形態では、カード端末Ａ及びＰＯＳ端末Ｂの双方において、無線ＩＤモジュール５から正当な利用者ＩＤを受信でき、かつ、該モジュール５に記憶された電子チケットＥＣが表す利用時間・利用端末ＩＤ等の条件が満たされるとき、該モジュール５に記憶された暗号鍵Ｋｙを用いたカードデータの暗号文通信が可能となる。このように電子チケットＥＣを導入すれば、通信システムのセキュリティ性が第１の実施形態に開示した構成よりも、更に向上する。

【０１１２】

また、無線ＩＤモジュール５に記憶される暗号鍵Ｋｙは、利用者ＩＤや利用時間等の従業員毎に異なる情報を含む電子チケットＥＣに基づいて生成される。このような構成であ

れば、従業員毎に異なる暗号鍵Ｋｙが生成されるので、暗号鍵Ｋｙが危殆化しにくくなる。この点からも、セキュリティ性の向上が期待できる。

【０１１３】

その他にも、第２の実施形態の構成からは、種々の好適な効果が得られる。

（変形例）

上記各実施形態に開示された構成は、実施段階において各構成要素を適宜変形して具体化できる。

【０１１４】

例えば、上記各実施形態では、カード端末Ａ及びＰＯＳ端末Ｂを有するカード処理システムを例示したが、ＰＯＳ端末Ｂに代えてＥＣＲ（Electric Cash Register）やカード決済に特化したカード決済端末を接続し、これらＥＣＲやカード決済端末にＰＯＳ端末Ｂが備えるとした構成要素を設けてカード処理システムを構成してもよい。また、上記各実施形態にて開示した暗号文通信に関わる構成を、他の通信システムに適用してもよい。

【０１１５】

また、上記各実施形態では、利用者ＩＤを用いて暗号文通信の許否を決める各処理を行う場合を例示したが、利用者ＩＤに代えて他種のＩＤコードを用いて各処理を行ってもよい。

【０１１６】

また、第２の実施形態では、利用者ＩＤ、利用時間、及び利用端末ＩＤを表す電子チケットＥＣを生成する場合を例示したが、利用者ＩＤ、利用時間、及び利用端末ＩＤに代えて、あるいはこれらと共に他の条件を採用し、その条件を含む電子チケットＥＣを生成してもよい。

【０１１７】

また、図４，図８，図９，図１６，図１９，図２１，図２２のフローチャートに示した処理を実現させるためのコンピュータプログラムを、ＣＤ－ＲＯＭやＵＳＢメモリ等の非一時的（non-transitory）な記録媒体に記憶して提供してもよい。あるいは、インターネット等のネットワークを介して提供してもよい。

【０１１８】

また、カード端末Ａ、ＰＯＳ端末Ｂ、及び入場管理装置６が備えるとした構成や、これら端末及び装置が実行するとした処理の一部又は全てを他のコンピュータ、例えば従業員管理サーバ９等にて実現してもよい。また、上記各部や処理の一部又は全ては、クラウドコンピューティングシステムに含まれるサーバから、カード端末Ａ、ＰＯＳ端末Ｂ、及び入場管理装置６に提供されてもよい。このような場合、例えばＳａａＳ（software as a service）と称されるソフトウェア提供形態を利用できる。

【０１１９】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

以下に、本願出願の当初の特許請求の範囲に記載された発明を付記する。

［１］送信装置と、受信装置とを有する通信システムであって、前記送信装置は、ＩＤコード及び暗号鍵を送信するモジュールと通信する送信側モジュール通信部と、この送信側モジュール通信部が前記モジュールから送信されるＩＤコードを受信可能なとき、前記送信側モジュール通信部が前記モジュールから受信する暗号鍵を用いて情報を暗号化する送信側暗号処理部と、この送信側暗号処理部が暗号化した情報を前記受信装置に送信する送信部と、を備え、前記受信装置は、前記モジュールと通信する受信側モジュール通信部と、前記送信装置から送信される前記暗号化された情報を受信する受信部と、前記受信側モジュール通信部が前記モジュールから送信されるＩＤコードを受信可能なとき、前記受

信側モジュール通信部が前記モジュールから受信する暗号鍵を用いて、前記受信部が受信する情報を復号化する受信側暗号処理部と、を備えていることを特徴とする通信システム。

［２］送信装置と、受信装置と、を有する通信システムであって、前記送信装置は、ＩＤコード、暗号鍵、及び所定の条件を示す電子チケットを送信するモジュールと通信する送信側モジュール通信部と、この送信側モジュール通信部が前記モジュールから送信される前記ＩＤコードを受信可能であり、かつ、前記送信側モジュール通信部が前記モジュールから受信する電子チケットにて示される条件が満たされるとき、前記送信側モジュール通信部が前記モジュールから受信する暗号鍵を用いて情報を暗号化する送信側暗号処理部と、この送信側暗号処理部が暗号化した情報を前記受信装置に送信する送信部と、を備え、前記受信装置は、前記モジュールと通信する受信側モジュール通信部と、前記送信装置から送信される前記暗号化された情報を受信する受信部と、前記受信側モジュール通信部が前記モジュールから送信される前記ＩＤコードを受信可能であり、かつ、前記受信側モジュール通信部が前記モジュールから受信する電子チケットにて示される条件が満たされるとき、前記受信側モジュール通信部が前記モジュールから受信する暗号鍵を用いて、前記受信部が受信する情報を復号化する受信側暗号処理部と、を備えていることを特徴とする通信システム。

［３］ＩＤコード及び暗号鍵を送信するモジュールと通信するモジュール通信部と、このモジュール通信部が前記モジュールから送信されるＩＤコードを受信可能なとき、前記モジュール通信部が前記モジュールから受信する暗号鍵を用いて情報を暗号化する暗号処理部と、この暗号処理部が暗号化した情報を受信装置に送信する送信部と、を備えていることを特徴とする送信装置。

［４］ＩＤコード、暗号鍵、及び所定の条件を示す電子チケットを送信するモジュールと通信するモジュール通信部と、このモジュール通信部が前記モジュールからＩＤコードを受信可能であり、かつ、前記モジュール通信部が前記モジュールから受信する電子チケットにて示される条件が満たされるとき、前記モジュール通信部が前記モジュールから受信する暗号鍵を用いて情報を暗号化する暗号処理部と、この暗号処理部が暗号化した情報を受信装置に送信する送信部と、を備えていることを特徴とする送信装置。

［５］ＩＤコード及び暗号鍵を送信するモジュールと通信するモジュール通信部と、送信装置から送信される暗号化された情報を受信する受信部と、前記モジュール通信部が前記モジュールからＩＤコードを受信可能なとき、前記モジュール通信部が前記モジュールから受信する暗号鍵を用いて、前記受信部が受信する情報を復号化する暗号処理部と、を備えていることを特徴とする受信装置。

［６］ＩＤコード、暗号鍵、及び所定の条件を示す電子チケットを送信するモジュールと通信するモジュール通信部と、送信装置から送信される暗号化された情報を受信する受信部と、前記モジュール通信部が前記モジュールからＩＤコードを受信可能であり、かつ、前記モジュール通信部が前記モジュールから受信する電子チケットにて示される条件が満たされるとき、前記モジュール通信部が前記モジュールから受信する暗号鍵を用いて、前記受信部が受信する情報を復号化する暗号処理部と、を備えていることを特徴とする受信装置。

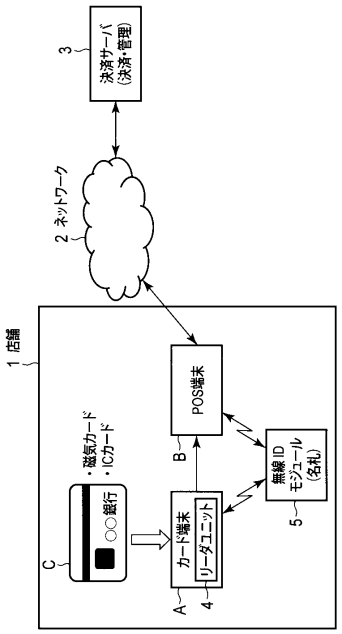
【符号の説明】

【０１２０】

Ａ…カード端末、Ｂ…ＰＯＳ端末、５…無線ＩＤモジュール、７…生体情報読取装置、８…無線リーダライタ、１００，２００…ＣＰＵ、１０１…データ入力部、１０２…コード化部、１０３，２０３…暗号処理部、１０４，２０４…通信鍵記憶部、１０５，２０５…ＲＦ送受信部、１０６，２０６…ＩＤ検査部、１０７，２０７…鍵抽出書込部、１０８，２０８…端末通信部、１０９，２０９…アンテナ、２０２…カード決済処理部

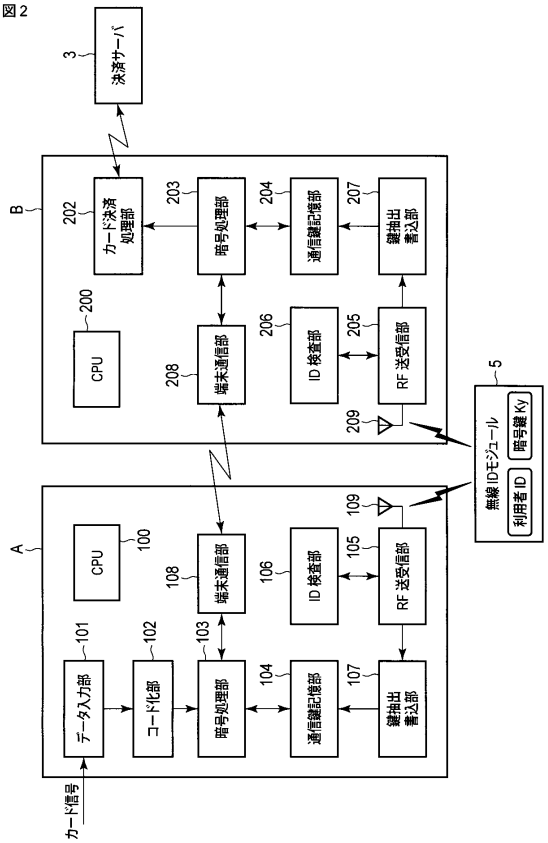
【図１】

図1



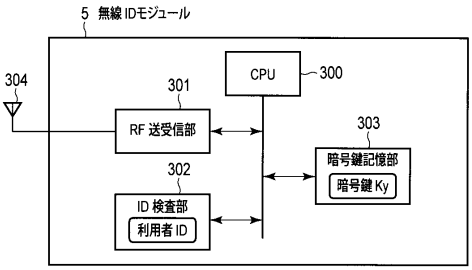
【図２】

図2



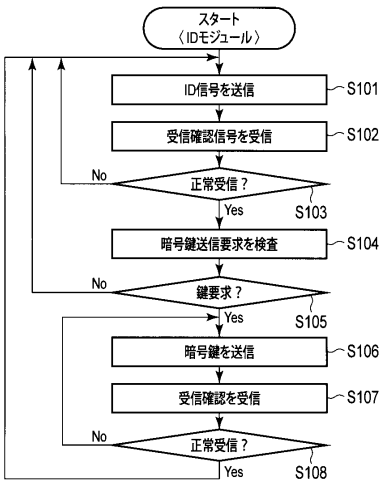
【図３】

図3



【図４】

図4



【図５】

図5

ID 信号データ例

スタート	利用者 ID (8桁)	ストップ
0x0000	A0000165	0xF0F0

【図６】

図6

受信確認信号データ例

スタート	フラグデータ	ストップ
0xFF00	0 : 通常確認 1 : 暗号鍵要求 2 : 予備 3 : 予備	0xF0F0

【図７】

図7

暗号鍵信号データ例

スタート	暗号鍵 (256bit)	ストップ
0x0000	0xC27f6288a7b89be9eea4a9c78812e3cd7b8f2197e3aa9fdda97a5012f31422ed	0xF0F0

【図８】

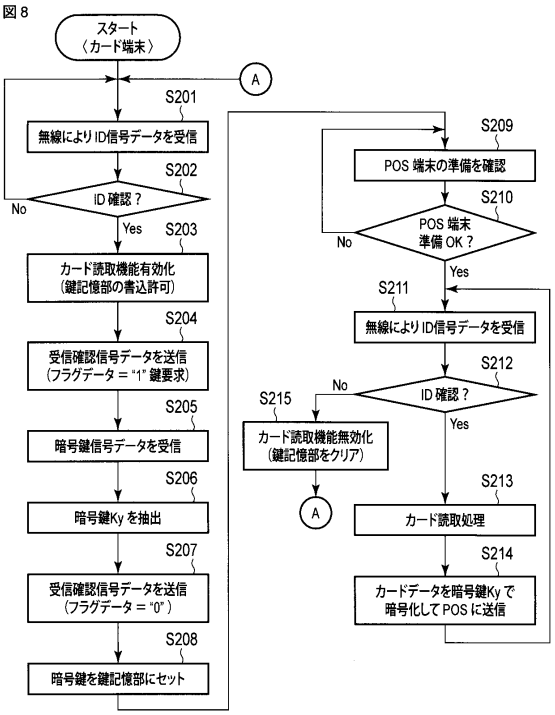


図8
スタート
（カード端末）
A
S201
無線によりID信号データを受信
S202
ID確認？
No
Yes
S203
カード読取機能有効化
（鍵記憶部の書込許可）
S204
受信確認信号データを送信
（フラグデータ＝"1" 鍵要求）
S205
暗号鍵信号データを受信
S206
暗号鍵Ky を抽出
S207
受信確認信号データを送信
（フラグデータ＝"0"）
S208
暗号鍵を鍵記憶部にセット
S209
POS 端末の準備を確認
S210
POS 端末
準備 OK？
No
Yes
S211
無線によりID信号データを受信
S212
ID 確認？
No
Yes
S215
カード読取機能無効化
（鍵記憶部をクリア）
A
S213
カード読取処理
S214
カードデータを暗号鍵Kyで
暗号化してPOSに送信

【図９】

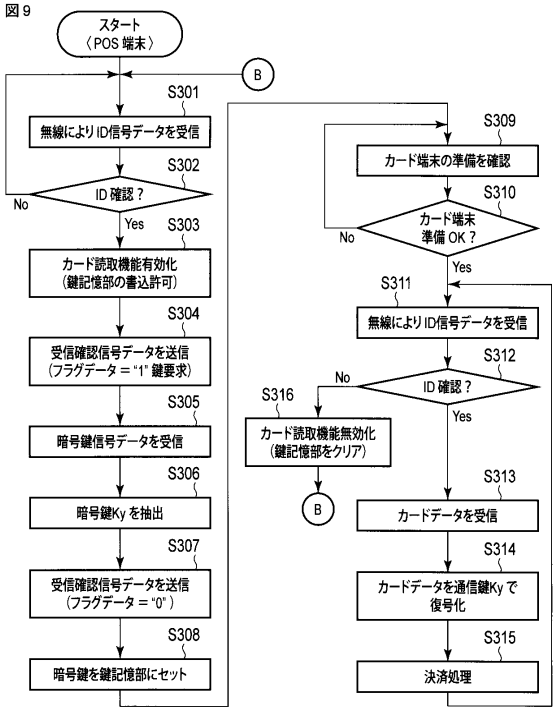


図9
スタート
（POS 端末）
B
S301
無線によりID信号データを受信
S302
ID 確認？
No
Yes
S303
カード読取機能有効化
（鍵記憶部の書込許可）
S304
受信確認信号データを送信
（フラグデータ＝"1" 鍵要求）
S305
暗号鍵信号データを受信
S306
暗号鍵Ky を抽出
S307
受信確認信号データを送信
（フラグデータ＝"0"）
S308
暗号鍵を鍵記憶部にセット
S309
カード端末の準備を確認
S310
カード端末
準備 OK？
No
Yes
S311
無線によりID信号データを受信
S312
ID 確認？
No
Yes
S316
カード読取機能無効化
（鍵記憶部をクリア）
B
S313
カードデータを受信
S314
カードデータを通信鍵Kyで
復号化
S315
決済処理

【図１０】

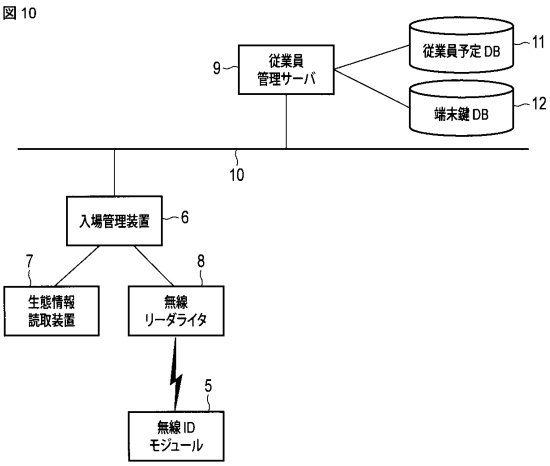


図10
9
従業員
管理サーバ
従業員予定 DB
11
端末鍵 DB
12
10
入場管理装置
6
7
8
生態情報
読取装置
無線
リーダライタ
5
無線 ID
モジュール

【図１１】

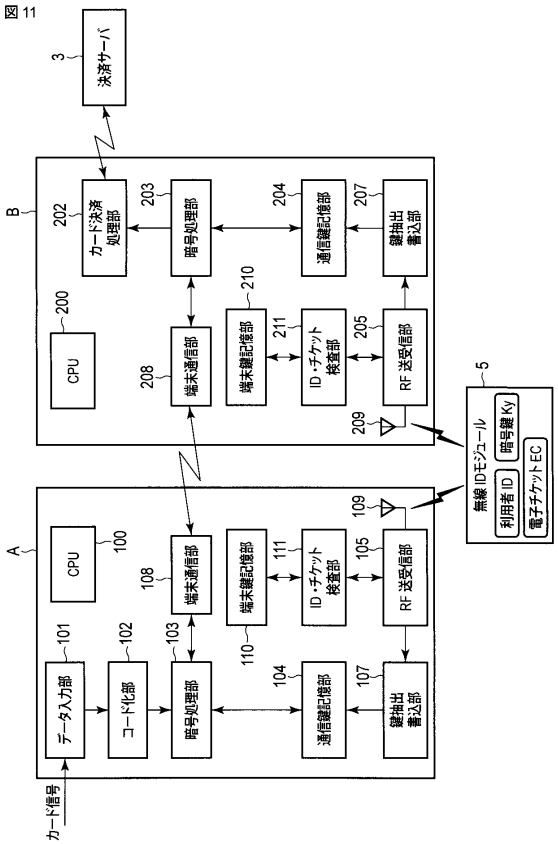
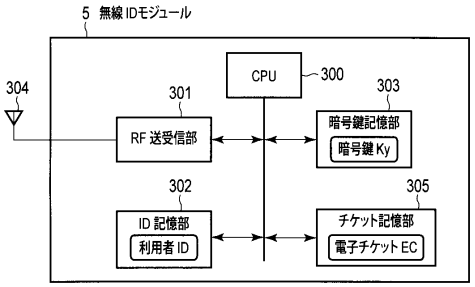


図11
3
決済サーバ
B
202
カード決済
処理部
203
暗号処理部
204
通信鍵記憶部
207
鍵抽出
書込部
200
CPU
208
端末通信部
210
端末鍵記憶部
211
ID・チケット
検査部
205
RF 送受信部
209
5
無線 IDモジュール
利用者 ID
暗号鍵 Ky
電子チケット EC
A
CPU
100
108
端末通信部
端末鍵記憶部
110
ID・チケット
検査部
111
105
RF 送受信部
109
101
データ入力部
102
コード化部
103
暗号処理部
104
通信鍵記憶部
107
鍵抽出
書込部
カード信号

【図１２】

図 12



【図１３】

図 13

従業員予定 DB 内容例

利用者 ID	利用端末 ID	利用時間	生体情報
A0000001	POS_01	09:00 ~ 15:00	生体情報 001
A0000002	POS_02	09:00 ~ 17:00	生体情報 002
A0000165	POS_03	13:00 ~ 20:00	生体情報 165
...	...		
nnnnmmm	POS_nn	17:00 ~ 21:00	生体情報 mmm

【図１４】

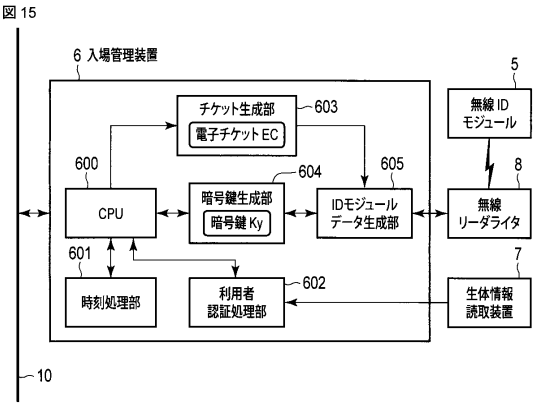
図 14

端末鍵 DB 内容例

利用端末 ID	端末鍵 SK
POS_01	SK01
POS_02	SK02
POS_03	SK03
...	
POS_nn	SKnn

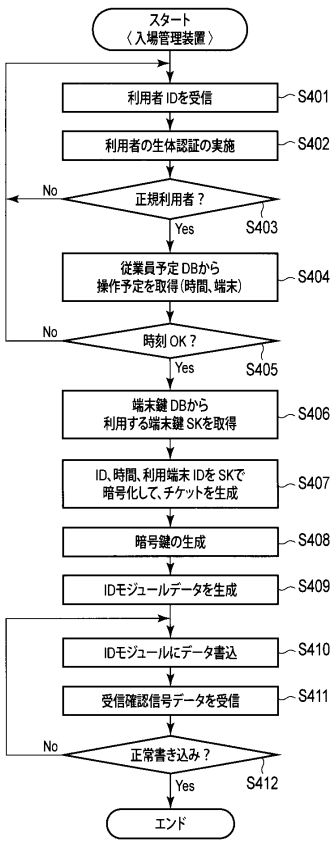
【図１５】

図 15



【図１６】

図 16



【図１７】

図 17

IDモジュールデータ例

スタート	利用者 ID	区切	電子チケット	区切	暗号鍵	ストップ
0x0000	A0000165	0xF3F3	0xc78a7a6c3ce6789a7b3b0a1a9113ac7c29e55a1ef9ace3bd428ed413a4cc98	0xF3F3	0xC27f6288a7b89be9eea4a9c78812e3cd7b8f2197e3aa8fdda97a5012f31422ed	0xF0F0

【図１８】

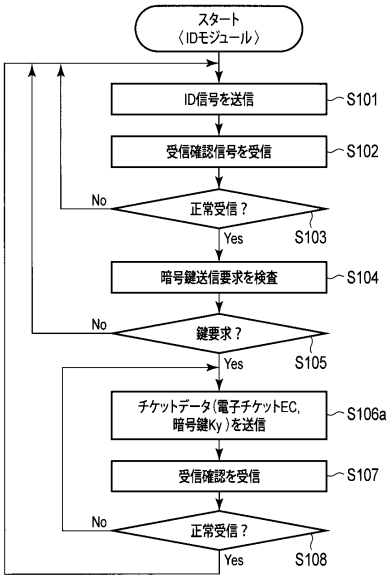
図 18

受信確認信号データ例

スタート	フラグデータ	ストップ
0xFF00	0：正常終了 1：エラー終了	0xF0F0

【図１９】

図 19



【図２０】

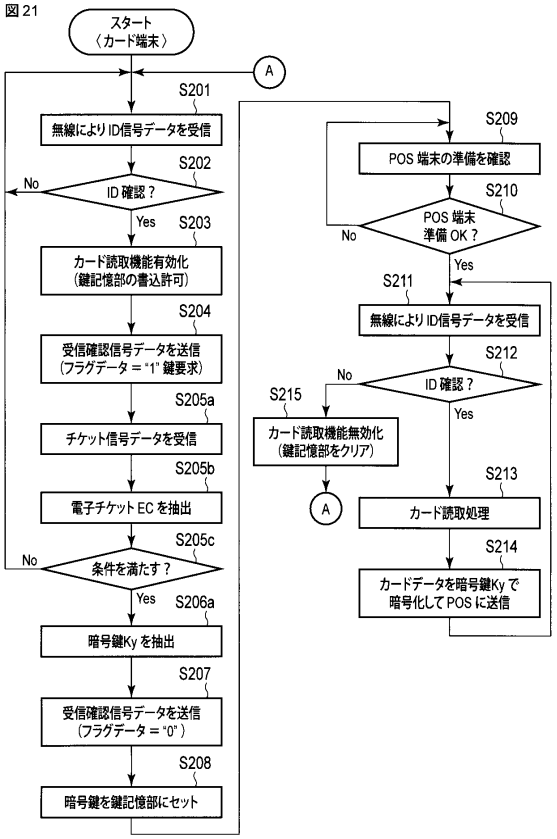
図 20

チケット信号データ例

スタート	電子チケット EC	区切	暗号鍵 Ky	ストップ
0x0000	0xc78a7a6c3ce67898a7b3b0a1a911 3ac7c29e55a1ef9ace3bd428ed413 a4cc98	0xF3F3	0xC27f6288a7b89be9eea4a9c78812 e3cd7b8f2197e3aa9fdda97a5012f314 22ed	0xF0F0

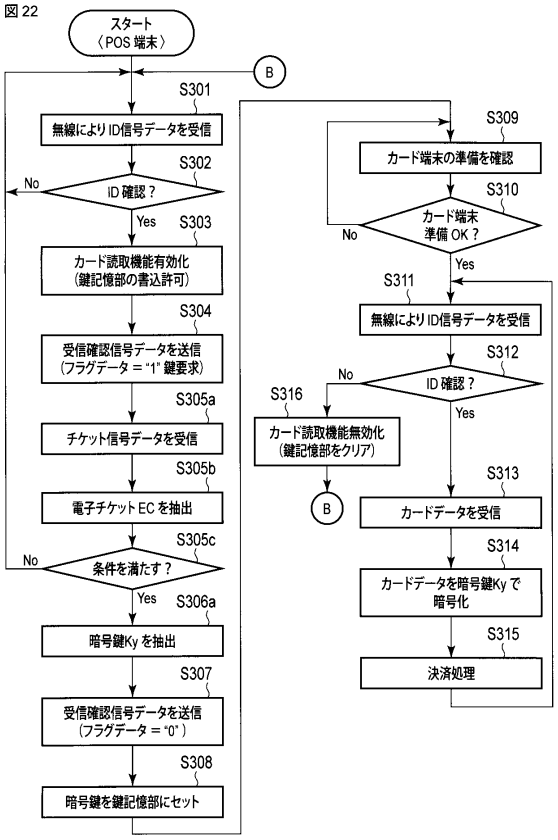
【図２１】

図 21



【図２２】

図 22



フロントページの続き

(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(72)発明者 福島 孝文
東京都品川区東五反田二丁目１７番２号 東芝テック株式会社内
(72)発明者 村上 和則
東京都品川区東五反田二丁目１７番２号 東芝テック株式会社内

審査官 松平 英

(56)参考文献 特開２００４－０６４３３３（ＪＰ，Ａ）
特開２００３－１１５８３３（ＪＰ，Ａ）
特開２００１－２８３３２０（ＪＰ，Ａ）
特開２００３－１３４０９９（ＪＰ，Ａ）
特開２００４－２００８８７（ＪＰ，Ａ）
特開２００４－２６５１３９（ＪＰ，Ａ）
特開２００１－９２７１８（ＪＰ，Ａ）
特開２００７－９４９９２（ＪＰ，Ａ）
特開２００７－１２９３２０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／００
Ｇ０９Ｃ １／００
Ｈ０４Ｗ ４／００
Ｇ０６Ｆ ２１／２４
Ｇ０６Ｋ １７／００
Ｇ０６Ｋ １９／００