(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2012-169751
(P2012-169751A)
(43)公開日　平成24年9月6日(2012.9.6)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5B017
H04L 9/14	(2006.01)	H04L	9/00	641	5J104
G06F 21/24	(2006.01)	G06F	12/14	540A	

審査請求 有　請求項の数 8　OL　（全 22 頁）

(21)出願番号　特願2011-27286(P2011-27286)
(22)出願日　平成23年2月10日(2011.2.10)

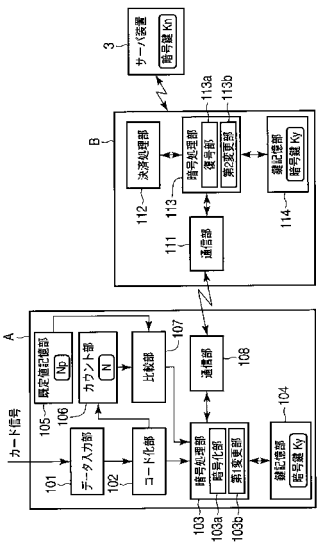
(71)出願人　000003562
東芝テック株式会社
東京都品川区東五反田二丁目１７番２号
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100159651
弁理士　高倉　成男
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】情報処理システム、読取端末および処理端末

(57)【要約】
【課題】暗号鍵や復号鍵が不正取得された場合であっても媒体情報の漏洩を防止し、システムのセキュリティ性を向上させる。
【解決手段】一実施形態の情報処理システムは、記憶媒体から媒体情報を読み取る読取手段を備えた読取端末と媒体情報を用いた処理を実行する処理端末を有する。読取端末は、読み取られた媒体情報を暗号鍵で暗号化して処理端末に送信する暗号化手段、同一の媒体情報が既定回数読み取られたとき処理端末に所定の情報を送信すると共に暗号化手段が使用する暗号鍵を他の暗号鍵に変更する第１変更手段を備える。処理端末は、暗号化された媒体情報を受信したとき同情報を復号鍵で復号する復号手段、読取端末から上記所定の情報を受信したとき復号手段が使用する復号鍵を第1変更手段による変更後の暗号鍵に対応する他の復号鍵に変更する第２変更手段を備える。
【選択図】　図２

図２



【特許請求の範囲】
【請求項１】
記憶媒体に記憶された媒体情報を読み取る読取手段を備えた読取端末と、この読取端末で読み取られた媒体情報を用いた処理を行う処理端末とを通信接続した情報処理システムであって、
前記読取端末は、
前記読取手段で読み取られた媒体情報を所定の暗号鍵で暗号化して前記処理端末に送信する暗号化手段と、
前記読取手段で同一の媒体情報が既定回数読み取られたとき、前記処理端末に所定の情報を送信すると共に、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更する第１変更手段と、を備え、
前記処理端末は、
前記読取端末から送信される暗号化された媒体情報を受信したとき、当該暗号化された媒体情報を所定の復号鍵で復号する復号手段と、
前記読取端末から前記所定の情報を受信したとき、前記復号手段が使用する復号鍵を、前記第１変更手段による変更後の暗号鍵に対応する他の復号鍵に変更する第２変更手段と、を備えていることを特徴とする情報処理システム。
【請求項２】
前記第１変更手段は、前記読取手段で同一の媒体情報が連続して既定回数読み取られたとき、前記処理端末に前記所定の情報を送信すると共に、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更することを特徴とする請求項１に記載の情報処理システム。
【請求項３】
前記第１変更手段は、前記読取手段で既定時間内に同一の媒体情報が既定回数読み取られたとき、前記処理端末に前記所定の情報を送信すると共に、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更することを特徴とする請求項１に記載の情報処理システム。
【請求項４】
前記処理端末からの要求に応じて暗号鍵およびこの暗号鍵に対応する復号鍵を前記処理端末に送信するサーバ装置をさらに備え、
前記第２変更手段は、前記読取端末から前記所定の情報を受信したとき、前記サーバ装置に暗号鍵および復号鍵を要求し、この要求に対して前記サーバ装置から送信される暗号鍵および復号鍵を受信すると、前記復号手段が使用する復号鍵を当該受信した復号鍵に変更すると共に当該受信した暗号鍵を前記読取端末に送信し、
前記第１変更手段は、前記読取手段で同一の媒体情報が既定回数読み取られたとき、前記処理端末に前記所定の情報を送信し、この送信の後に前記処理端末から送信される暗号鍵を受信すると、前記暗号化手段が使用する暗号鍵を当該受信した暗号鍵に変更することを特徴とする請求項１に記載の情報処理システム。
【請求項５】
前記読取端末は、
前記媒体情報を暗号化するための複数の暗号鍵を記憶した第1記憶手段と、
この第１記憶手段に記憶された各暗号鍵からいずれか１つを指定する第1指定手段と、をさらに備え、
前記暗号化手段は、前記第１指定手段が指定する暗号鍵を用いて媒体情報を暗号化し、
前記第１変更手段は、前記第１指定手段が指定する暗号鍵を前記第１記憶手段に記憶された他の暗号鍵に変更することで、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更し、
前記処理端末は、
暗号化された媒体情報を復号するための複数の復号鍵を記憶した第２記憶手段と、
この第２記憶手段に記憶された各復号鍵からいずれか１つを指定する第２指定手段と、をさらに備え、
前記復号手段は、前記読取端末から送信される暗号化された媒体情報を受信したとき、

前記第２指定手段が指定する復号鍵を用いて当該暗号化された媒体情報を復号し、前記第２変更手段は、前記第２指定手段が指定する復号鍵を前記第１指定手段が指定する暗号鍵に対応する前記第２記憶手段に記憶された他の復号鍵に変更することで、前記復号手段が使用する復号鍵を他の復号鍵に変更することを特徴とする請求項１に記載の情報処理システム。

【請求項６】

記憶媒体に記憶された媒体情報を用いた処理を実行する処理端末と通信する通信手段と、

記憶媒体に記憶された媒体情報を読み取る読取手段と、

前記読取手段で読み取られた媒体情報を所定の暗号鍵で暗号化して前記通信手段により前記処理端末に送信する暗号化手段と、

前記読取手段で同一の媒体情報が既定回数読み取られたとき、前記通信手段により前記処理端末に所定の情報を送信すると共に、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更する変更手段と、

を備えたことを特徴とする読取端末。

【請求項７】

記憶媒体に記憶された媒体情報を読み取り、読み取った媒体情報を暗号化して送信する読取端末と通信する通信手段と、

この通信手段により前記読取端末から前記暗号化された媒体情報を受信したとき、当該暗号化された媒体情報を所定の復号鍵で復号する復号手段と、

この復号手段で復号された媒体情報を用いた処理を実行する処理手段と、

前記読取端末が同一の媒体情報を既定回数読み取ったときに送信する所定の情報を前記通信手段により受信したとき、前記復号手段が使用する復号鍵を他の復号鍵に変更する変更手段と、

を備えていることを特徴とする処理端末。

【請求項８】

記憶媒体に記憶された媒体情報を読み取る読取手段を備えた読取端末と、この読取端末で読み取られた媒体情報を用いた処理を行う処理端末とを通信接続した情報処理システムであって、

前記読取端末は、前記読取手段で読み取られた媒体情報を所定の暗号鍵で暗号化して前記処理端末に送信する暗号化手段を備え、

前記処理端末は、前記読取端末から送信される暗号化された媒体情報を受信したとき、当該暗号化された媒体情報を所定の復号鍵で復号する復号手段を備え、

前記読取手段で同一の媒体情報が既定回数読み取られたとき、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更する第１変更手段と、

前記読取手段で同一の媒体情報が既定回数読み取られたとき、前記復号手段が使用する復号鍵を、前記第１変更手段による変更後の暗号鍵に対応する他の復号鍵に変更する第２変更手段と、

を前記読取端末と前記処理端末のいずれか一方が備えていることを特徴とする情報処理システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明の実施形態は、記憶媒体に記憶された媒体情報を読み取り、読み取った媒体情報を用いて所定の処理を行う情報処理システム、記憶媒体に記憶された媒体情報を読み取る読取端末、およびこの読取端末が読み取った媒体情報を用いた処理を行う処理端末に関する。

【背景技術】

【０００２】

従来、カード等の記憶媒体に記憶された媒体情報を読み取り、読み取った媒体情報を用

いた処理を行う情報処理システムが種々の分野で利用されている。
【０００３】
例えば、各種店舗においては、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情報を上記処理端末に送信して客の買い上げ商品の決済を行わせるカード決済システムが使用されている。
【０００４】
上記カード端末から上記処理端末に送信されるカード情報には、カードの持ち主の会員番号や暗証番号等の個人情報が含まれている。したがって、このカード情報が悪意のある者に漏洩すれば、同カード情報が悪用され、カードの持ち主やカード事業者等が金銭的な損害を受けかねない。
【０００５】
このような事態に鑑み、従来、カード端末においてカード情報を暗号鍵で暗号化して処理端末に送信し、処理端末において当該暗号化されたカード情報を復号鍵で復号して、復号後のカード情報を用いて処理を行う方法が採られている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００８－２６９１８０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
上記のように暗号鍵および復号鍵を用いてカード端末と処理端末との間でカード情報を通信する場合であっても、いわゆる既知平文攻撃等により暗号鍵や復号鍵が悪意のある者に知られかねない。なお、既知平文攻撃とは、複数の平文と暗号文の組から鍵を推定する攻撃方法である。この攻撃方法においては、通常、同一のカードをカード端末に複数回読み取らせて処理端末に送信される暗号文が不正に取得される。
【０００８】
このように悪意のある者に暗号鍵および復号鍵が知られると、不正取得された暗号文からカード情報の復号が可能となる。
【０００９】
このような事情から、カード処理システム等の情報処理システムにて使用される暗号鍵や復号鍵が不正取得された場合であってもカード情報等の媒体情報の漏洩を防止するための手段を講じ、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】
【００１０】
上記課題を解決すべく、一実施形態における情報処理システムは、記憶媒体に記憶された媒体情報を読み取る読取手段を備えた読取端末と、この読取端末で読み取られた媒体情報を用いた処理を実行する処理端末とを通信接続して構成され、前記読取端末は、前記読取手段で読み取られた媒体情報を所定の暗号鍵で暗号化して前記処理端末に送信する暗号化手段と、前記読取手段で同一の媒体情報が既定回数読み取られたとき、前記処理端末に所定の情報を送信すると共に、前記暗号化手段が使用する暗号鍵を他の暗号鍵に変更する第１変更手段とを備える。
また、前記処理端末は、前記読取端末から送信される暗号化された媒体情報を受信したとき、当該暗号化された媒体情報を所定の復号鍵で復号する復号手段と、前記読取端末から前記所定の情報を受信したとき、前記復号手段が使用する復号鍵を、前記第1変更手段による変更後の暗号鍵に対応する他の復号鍵に変更する第２変更手段とを備える。
【図面の簡単な説明】
【００１１】
【図１】第１の実施形態におけるカード処理システムの全体構成図。

【図２】同実施形態におけるカード端末、ＰＯＳ端末、サーバ装置の構成を示すブロック図。
【図３】同実施形態におけるカウント部を説明するための図。
【図４】同実施形態におけるカード端末の動作を説明するためのフローチャート。
【図５】同実施形態におけるＰＯＳ端末の動作を説明するためのフローチャート。
【図６】第２の実施形態におけるカード端末、ＰＯＳ端末、サーバ装置の構成を示すブロック図。
【図７】同実施形態におけるカウント部を説明するための図。
【図８】同実施形態におけるカード端末の動作を説明するためのフローチャート。
【図９】第３の実施形態におけるカード端末、ＰＯＳ端末、サーバ装置の構成を示すブロック図。
【図１０】同実施形態における鍵記憶部および鍵リスト部を説明するための図。
【図１１】同実施形態におけるカード端末の動作を説明するためのフローチャート。
【図１２】同実施形態におけるＰＯＳ端末の動作を説明するためのフローチャート。
【図１３】変形例におけるカード処理システムを説明するための図。
【発明を実施するための形態】
【００１２】
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３の実施形態においては、情報処理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、カード情報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。
【００１３】
（第１の実施形態）
［システム構成］
図１は、第１の実施形態におけ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と、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サーバ装置３とを備えている。このうち、カード端末ＡとＰＯＳ端末Ｂとが有線または無線にて相互通信可能に接続され、ＰＯＳ端末Ｂと、サーバ装置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。
【００１４】
カード端末Ａは、本実施形態における読取端末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（記憶媒体）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情報（媒体情報）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表示部を備えたピンパッドであってもよい。
【００１５】
ＰＯＳ端末Ｂは、本実施形態における処理端末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情報とを用いて商品の代金をカード決済する装置である。
【００１６】
サーバ装置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情報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。また、サーバ装置３は、カード端末ＡおよびＰＯＳ端末Ｂがカード情報の暗号化および復号に用いる暗号鍵をＰＯＳ端末Ｂに送信する機能を備える。
【００１７】
カード端末Ａ、ＰＯＳ端末Ｂ、およびサーバ装置３の詳細な構成につき、図２のブロッ

ク図を用いて説明する。
カード端末Ａは、データ入力部１０１、コード化部１０２、暗号処理部１０３、鍵記憶部１０４、既定値記憶部１０５、カウント部１０６、比較部１０７、および通信部１０８を備えている。これら各部１０１～１０８の全てまたはいずれかは、例えばカード端末Ａに設けられたＣＰＵ（Central Processing Unit）等のプロセッサが同じくカード端末Ａに設けられたＲＯＭ（Read Only Memory）等に記憶されたプログラムを実行することで実現される。
【００１８】
上記リーダユニット４で取り込まれたカード信号は、データ入力部１０１に出力される。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情報を生成し、暗号処理部１０３およびカウント部１０６に出力する。
鍵記憶部１０４は、カード情報の暗号化に用いられる暗号鍵Ｋｙを記憶する。通信部１０８は、ＰＯＳ端末Ｂとの間で各種データを送受信する。
【００１９】
暗号処理部１０３は、暗号化部１０３ａと第１変更部１０３ｂとを有している。暗号化部１０３ａは、コード化部１０２から入力されたカード情報を鍵記憶部１０４に記憶された暗号鍵Ｋｙで暗号化し、暗号化した後のカード情報を通信部１０８を介してＰＯＳ端末Ｂに送信する。
【００２０】
カウント部１０６は、図３に示すように、コード化部１０２から入力されるカード情報を記憶するメモリ１０６ａと、メモリ１０６ａに記憶されたカード情報の直前にコード化部１０２から入力されたカード情報を記憶するメモリ１０６ｂと、カウント値Ｎを記憶するメモリ１０６ｃとを有している。カウント部１０６は、メモリ１０６ａ，１０６ｂに記憶された両カード情報を比較し、一致する場合にはカウント値Ｎを１つインクリメントし、一致しないならばカウント値Ｎを０にリセットする。カウント値Ｎをインクリメントあるいはリセットした後、カウント部１０６は、メモリ１０６ｂのカード情報をメモリ１０６ａのカード情報で書き換え、メモリ１０６ａのカード情報を消去する。
【００２１】
既定値記憶部１０５には、上記カウント値Ｎとの比較に用いられる既定カウント値Ｎｐが予め記憶されている。既定カウント値Ｎｐの具体的な値は、種々の事情を考慮して定めればよい。
比較部１０７は、既定値記憶部１０５およびカウント部１０６からそれぞれ既定カウント値Ｎｐおよびカウント値Ｎを読み込み、読み込んだ既定カウント値Ｎｐとカウント値Ｎとを比較し、その比較の結果を暗号処理部１０３に通知する。
【００２２】
暗号処理部１０３の第１変更部１０３ｂは、比較部１０７から入力される比較結果に基づき、ＰＯＳ端末Ｂに暗号鍵Ｋｙの危殆化を通知し、鍵記憶部１０４に記憶された暗号鍵Ｋｙを他の暗号鍵に変更する。なお、上記危殆化の通知は、予め定められた危殆化を示す情報を通信部１０８から送信することで行われる。
【００２３】
ＰＯＳ端末Ｂは、通信部１１１、決済処理部１１２、暗号処理部１１３、および鍵記憶部１１４を備えている。これら各部１１１～１１４の全てまたはいずれかは、例えばＰＯＳ端末Ｂに設けられたＣＰＵ等のプロセッサが同じくＰＯＳ端末Ｂに設けられたＲＯＭ等に記憶されたプログラムを実行することで実現される。
【００２４】
通信部１１１は、カード端末Ａとの間で各種データを送受信する。鍵記憶部１１４は、カード情報の復号に用いられる復号鍵を記憶する。なお、本実施形態においては共通鍵方式を採用しているため、鍵記憶部１１４にはカード端末Ａの鍵記憶部１０４に記憶された

ものと同一の暗号鍵Ｋｙが記憶される。
【００２５】
暗号処理部１１３は、復号部１１３ａと第２変更部１１３ｂとを有している。復号部１１３ａは、通信部１１１がカード端末Ａから受信した暗号化されたカード情報を、鍵記憶部１１４に記憶された暗号鍵Ｋｙで復号し、決済処理部１１２に出力する。
【００２６】
決済処理部１１２は、暗号処理部１１３から入力されたカード情報と、上記入力部の操作によって入力された商品情報とを用いて商品の代金を決済する。
暗号処理部１１３の第２変更部１１３ｂは、カード端末Ａから暗号鍵の危殆化が通知されたとき、すなわち、上記危殆化を示す情報が通信部１１１で受信されたときに、鍵記憶部１１４に記憶された暗号鍵Ｋｙを第1変更部１０３ｂによる変更後の暗号鍵に対応する他の復号鍵、すなわちカード端末Ａの鍵記憶部１０４に記憶されたものと同一の暗号鍵Ｋｙに変更する。
【００２７】
サーバ装置３は、ＰＯＳ端末Ｂからの要求に応じて各鍵記憶部１０４，１１４に記憶された暗号鍵Ｋｙと異なる暗号鍵Ｋｎを生成し、ＰＯＳ端末Ｂに送信する。
【００２８】
［動作］
次に、当該カード処理システムにて実行されるカード決済の流れについて説明する。
ＰＯＳ端末Ｂに客が購入しようとする商品の商品情報が入力され、カード決済が選択されると、ＰＯＳ端末Ｂからカード端末Ａにカードの読み取りが指示される。
【００２９】
その後、カード端末Ａの各部は、図４のフローチャート沿って動作する。すなわち、リーダユニット４がカードＣの挿入を待ち、挿入されたカードＣからカード信号を取り込み、データ入力部１０１に入力する（ステップＳ１０１）。このときデータ入力部１０１は、リーダユニット４から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。
【００３０】
続いてコード化部１０２がデータ入力部１０１から入力されたカード信号をコード化してカード情報を生成し、暗号処理部１０３およびカウント部１０６に出力する（ステップＳ１０２）。カウント部１０６は、入力されたカード情報をメモリ１０６ａに記憶し（ステップＳ１０３）、この記憶したカード情報とメモリ１０６ｂに記憶された前回のカード情報とが同一であるかを判定する（ステップＳ１０４）。その結果、両カード情報が一致するならば（ステップＳ１０４のＹｅｓ）、カウント部１０６は、メモリ１０６ｃのカウント値Ｎを１つインクリメントする（ステップＳ１０５）。このようにカウント値Ｎがインクリメントされた後、比較部１０７が既定値記憶部１０５およびカウント部１０６からそれぞれ既定カウント値Ｎｐおよびカウント値Ｎを読み込み（ステップＳ１０６）、読み込んだ既定カウント値Ｎｐとカウント値Ｎとを比較する（ステップＳ１０７）。
【００３１】
上記比較の結果、カウント値Ｎが既定カウント値Ｎｐ未満（Ｎ＜Ｎｐ）である場合（ステップＳ１０７のＹｅｓ）、その旨が暗号処理部１０３に通知される。このとき、暗号化部１０３ａは、ステップＳ１０２にてコード化部１０２から入力されたカード情報を鍵記憶部１０４に記憶された暗号鍵Ｋｙで暗号化する（ステップＳ１０８）。そして、暗号化部１０３ａは、暗号化した後のカード情報を通信部１０８を介してＰＯＳ端末Ｂに送信する（ステップＳ１０９）。
【００３２】
ステップＳ１０４において両カード情報が一致しない場合（ステップＳ１０４のＮｏ）、カウント部１０６は、メモリ１０６ｃのカウント値Ｎを０にリセットする（ステップＳ１１０）。そして、暗号化部１０３ａがステップＳ１０２にてコード化部１０２から入力されたカード情報を鍵記憶部１０４に記憶された暗号鍵Ｋｙで暗号化し（ステップＳ１０

８）、暗号化した後のカード情報を通信部１０８を介してＰＯＳ端末Ｂに送信する（ステップＳ１０９）。

【００３３】

ステップＳ１０７の比較の結果、カウント値Ｎが既定カウント値Ｎｐ以上（Ｎ≧Ｎｐ）である場合（ステップＳ１０７のＮｏ）、その旨が暗号処理部１０３に通知される。このとき、暗号化部１０３ａによる暗号化および送信は行われず、第１変更部１０３ｂが鍵記憶部１０４に記憶された暗号鍵Ｋｙを削除する（ステップＳ１１１）。さらに、第１変更部１０３ｂは、通信部１０８を介して暗号鍵の危殆化をＰＯＳ端末Ｂに通知し（ステップＳ１１２）、ＰＯＳ端末Ｂからの暗号鍵Ｋｎの返信を待つ（ステップＳ１１３）。

【００３４】

やがてＰＯＳ端末Ｂから後述のステップＳ２０８において返信される暗号鍵Ｋｎを通信部１０８が受信すると、第１変更部１０３ｂは、当該受信した暗号鍵Ｋｎを新たな暗号鍵Ｋｙとして鍵記憶部１０４に記憶する（ステップＳ１１４）。

【００３５】

ステップＳ１０９またはステップＳ１１４を以って一連の処理が終了する。なお、ステップＳ１１４を以って処理が終了した場合には、カード決済が完了しない。したがって、再びステップＳ１０１から各部が動作する。

【００３６】

次に、ＰＯＳ端末Ｂの各部が実行する処理について説明する。

カード端末Ａにカード Ｃの読み取りを指示した後、ＰＯＳ端末Ｂの各部は、図５のフローチャートに沿って動作する。すなわち、暗号処理部１１３がカード端末Ａから送信されるデータの受信を待ち、通信部１１１がカード端末Ａからデータを受信すると（ステップＳ２０１）、そのデータの種別を判定する（ステップＳ２０２）。

【００３７】

この判定の結果、カード端末Ａから受信したデータがステップＳ１０９で送信された暗号化されたカード情報である場合（ステップＳ２０２の「カード情報」）、復号部１１３ａが鍵記憶部１１４に記憶された暗号鍵Ｋｙを用いて当該暗号化されたカード情報を復号する（ステップＳ２０３）。復号後のカード情報は、決済処理部１１２に出力される。決済処理部１１２は、入力されたカード情報と、客が購入しようとする商品の商品情報とを用いて決済処理を実行する（ステップＳ２０４）。

【００３８】

具体的には、決済処理部１１２は、入力されたカード情報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を介してサーバ装置３に送信する。サーバ装置３は、ＰＯＳ端末Ｂから受信した暗号化されたカード情報を復号し、カード情報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。ＰＯＳ端末Ｂは、サーバ装置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を介してサーバ装置３に送信するなどして決済処理を完了させる。

【００３９】

ステップＳ２０２の判定の結果、カード端末Ａから受信したデータが暗号鍵の危殆化の通知である場合（ステップＳ２０２の「危殆化通知」）、第２変更部１１３ｂがネットワーク２を介してサーバ装置３に暗号鍵の交換を要求し（ステップＳ２０５）、サーバ装置３からの返信を待つ（ステップＳ２０６）。この要求を受信したサーバ装置３は、例えば複数用意された暗号鍵の中からランダムに１つの暗号鍵Ｋｎを選定し、ネットワーク２を介してＰＯＳ端末Ｂに返信する。このように返信される暗号鍵Ｋｎを受信すると、第２変更部１１３ｂは、鍵記憶部１１４に記憶された暗号鍵Ｋｙを削除し、当該受信した暗号鍵Ｋｎを新たな暗号鍵Ｋｙとして鍵記憶部１１４に記憶する（ステップＳ２０７）。さらに第２変更部１１３ｂは、通信部１１１を介してカード端末Ａにサーバ装置３から受信した暗号鍵Ｋｎを送信する（ステップＳ２０８）。

【００４０】
上記ステップＳ１１４においては、このようにＰＯＳ端末Ｂから送信された暗号鍵Ｋｎが新たな暗号鍵Ｋｙとして鍵記憶部１０４に記憶される。すなわち、第１変更部１０３ｂによる変更後の暗号鍵Ｋｙと、第２変更部１１３ｂによる変更後の暗号鍵Ｋｙとは常に同一となる。
【００４１】
ステップＳ２０４またはステップＳ２０８を以って一連の処理が終了する。なお、ステップＳ２０８を以って処理が終了した場合には、カード決済が完了しない。したがって、再びステップＳ２０１から各部が動作する。
【００４２】
このように、本実施形態においてはカード端末Ａで同一のカード情報が連続して既定回数Ｎｐだけ読み取られたとき、暗号化部１０３ａが使用する暗号鍵Ｋｙを第１変更部１０３ｂが他の暗号鍵に変更する。また、復号部１１３ａが使用する暗号鍵Ｋｙを第２変更部１１３ｂが第1変更部１０３ｂによる変更後の暗号鍵Ｋｙと同一の暗号鍵に変更する。
【００４３】
（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のみ行う。
【００４４】
［システム構成］
図６は、第２の実施形態におけるカード端末Ａ、ＰＯＳ端末Ｂ、およびサーバ装置３の詳細な構成を示すブロック図である。カード端末Ａは、データ入力部１０１、コード化部１０２、暗号処理部１０３、鍵記憶部１０４、比較部１０７、通信部１０８、カウント部２０１、計時部２０２、および既定値記憶部２０３を備えている。このうちデータ入力部１０１、コード化部１０２、暗号処理部１０３、鍵記憶部１０４、比較部１０７、通信部１０８と、ＰＯＳ端末Ｂおよびサーバ装置３は、第１の実施形態で説明したものと同一である。また、各部１０１～１０４，１０７，１０８，２０１～２０３の全てあるいはいずれかは、例えばカード端末Ａに設けられたＣＰＵ等のプロセッサが同じくカード端末Ａに設けられたＲＯＭ等に記憶されたプログラムを実行することで実現される。
【００４５】
計時部２０２は、例えば年、月、日、時、分、秒の単位で日時を計時する。
本実施形態における既定値記憶部２０３には、上記既定カウント値Ｎｐと、既定時間Ｔｐとが予め記憶されている。既定時間Ｔｐの具体的な値は、種々の事情を考慮して定めればよい。
【００４６】
本実施形態におけるカウント部２０１は、図７に示すように、コード化部１０２から入力されるカード情報を計時部２０２で計時される時間と共に記憶するメモリ２０１ａと、カウント値Ｎを記憶するメモリ２０１ｂとを有している。
メモリ２０１ａは、コード化部１０２から入力されるカード情報および計時部２０２で計時される時間の組に、その時間が新しいものから昇順のナンバ（Ｎｏ．）を付して蓄積して記憶する。すなわち、ナンバ「１」が付されたものが、常に最直近の組となる。メモリ２０１ａに蓄積されるカード情報および時間の組は、例えば１日の店舗の営業が終了した際に消去される。
【００４７】
カウント部２０１は、ナンバ「１」が付された組のカード情報と同一のカード情報を有する組であって、かつその時間とナンバ「１」が付された組の時間との差分Δｔが既定時間Ｔｐ未満である組をメモリ２０１ａから検索し、この条件に合致する組の数をカウント値Ｎに代入する。
例えば、図７に示すように既定時間Ｔｐが「１０min」（１０分）である場合、ナンバ

「１」が付された組のカード情報「４９８８　９９９８　８８７７　７６６６」と同一のカード情報を有する組は、ナンバ「４」「５」の組となる。さらにこの２組のうち、ナンバ「１」が付された組の時間「２１：２５：１０：４５」（２１時２５分１０秒４５）とナンバ「４」が付された組の時間「２１：１６：２０：１９」（２１時１６分２０秒１９）との差分Δｔは Ｔｐ（＝１０min）未満であり、ナンバ「１」が付された組の時間「２１：２５：１０：４５」（２１時２５分１０秒４５）とナンバ「５」が付された組の時間「２１：１１：５８：３９」（２１時１１分５８秒３９）との差分Δｔは Ｔｐ（＝１０min）以上である。したがって、条件に合致する組の数は１であるため、カウント値Ｎに「１」が代入される。

【００４８】

［動作］

次に、第２の実施形態におけるカード処理システムにて実行されるカード決済の流れについて説明する。なお、ＰＯＳ端末Ｂの動作は、第１の実施形態において図５を用いて説明したものと同様であるため、その説明を省略する。

ＰＯＳ端末Ｂに客が購入しようとする商品の商品情報が入力され、カード決済が選択されると、ＰＯＳ端末Ｂからカード端末Ａにカードの読み取りが指示される。

【００４９】

その後、カード端末Ａの各部は、図８のフローチャートに沿って動作する。すなわち、リーダユニット４がカードＣの挿入を待ち、挿入されたカードＣからカード信号を取り込み、データ入力部１０１に入力する（ステップＳ３０１）。このときデータ入力部１０１は、リーダユニット４から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。

【００５０】

続いてコード化部１０２がデータ入力部１０１から入力されたカード信号をコード化してカード情報を生成し、暗号処理部１０３およびカウント部１０６に出力する（ステップＳ３０２）。カウント部２０１は、入力されたカード情報を計時部２０２で計時される時間と共にメモリ２０１ａに記憶する（ステップＳ３０３）。

【００５１】

さらに、カウント部２０１は、図７を用いて説明したように、ナンバ「１」が付された組のカード情報と同一のカード情報を有する組であって、かつその時間とナンバ「１」が付された組の時間との差分Δｔが既定時間Ｔｐ未満である組をメモリ２０１ａから検索し、この条件に合致する組の数をカウントする（ステップＳ３０４）。そして、カウント結果をメモリ２０１ｂのカウント値Ｎに代入する（ステップＳ３０５）。

【００５２】

このようにカウント値Ｎが更新された後、比較部１０７が既定値記憶部２０３およびカウント部２０１からそれぞれ既定カウント値ＮｐおよびカウントＮを読み込み（ステップＳ３０６）、読み込んだ既定カウント値Ｎｐとカウント値Ｎとを比較する（ステップＳ３０７）。

【００５３】

上記比較の結果、カウント値Ｎが既定カウント値Ｎｐ未満（Ｎ＜Ｎｐ）である場合（ステップＳ３０７のＹｅｓ）、その旨が暗号処理部１０３に通知される。このとき、暗号化部１０３ａは、ステップＳ３０２にてコード化部１０２から入力されたカード情報を鍵記憶部１０４に記憶された暗号鍵Ｋｙで暗号化する（ステップＳ３０８）。そして、暗号化部１０３ａは、暗号化した後のカード情報を通信部１０８を介してＰＯＳ端末Ｂに送信する（ステップＳ３０９）。

【００５４】

ステップＳ３０７の比較の結果、カウント値Ｎが既定カウント値Ｎｐ以上（Ｎ≧Ｎｐ）である場合（ステップＳ３０７のＮｏ）、その旨が暗号処理部１０３に通知される。このとき、暗号化部１０３ａによる暗号化および送信は行われず、第１変更部１０３ｂが鍵記憶部１０４に記憶された暗号鍵Ｋｙを削除する（ステップＳ３１０）。さらに、第１変更

部１０３ｂは、通信部１０８を介して暗号鍵の危殆化をＰＯＳ端末Ｂに通知し（ステップＳ３１１）、ＰＯＳ端末Ｂからの暗号鍵Ｋｎの返信を待つ（ステップＳ３１２）。

【００５５】

やがてＰＯＳ端末Ｂから上記ステップＳ２０８において返信される暗号鍵Ｋｎを通信部１０８が受信すると、第１変更部１０３ｂは、当該受信した暗号鍵Ｋｎを新たな暗号鍵Ｋｙとして鍵記憶部１０４に記憶する（ステップＳ３１３）。

【００５６】

ステップＳ３０９またはステップＳ３１３を以って一連の処理が終了する。なお、ステップＳ３１３を以って処理が終了した場合には、カード決済が完了しない。したがって、再びステップＳ３０１から各部が動作する。

【００５７】

このように、本実施形態においてはカード端末Ａで同一のカード情報が既定時間Ｔｐ内に既定回数Ｎｐだけ読み取られたとき、暗号化部１０３ａが使用する暗号鍵Ｋｙが第１変更部１０３ｂによって他の暗号鍵に変更される。また、復号部１１３ａが使用する暗号鍵Ｋｙが第２変更部１１３ｂによって第1変更部１０３ｂによる変更後の暗号鍵Ｋｙと同一の暗号鍵に変更される。

【００５８】

（第３の実施形態）

次に、第３の実施形態について説明する。

第１，第２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のみ行う。

【００５９】

［システム構成］

図９は、第３の実施形態におけるカード端末Ａ、ＰＯＳ端末Ｂ、およびサーバ装置３の詳細な構成を示すブロック図である。

【００６０】

カード端末Ａは、データ入力部１０１、コード化部１０２、暗号処理部１０３、鍵記憶部１０４、既定値記憶部１０５、カウント部１０６、比較部１０７、通信部１０８、鍵リスト部３０１、およびアドレスカウンタ３０２を備えている。

このうちデータ入力部１０１、コード化部１０２、暗号処理部１０３、鍵記憶部１０４、既定値記憶部１０５、カウント部１０６、比較部１０７、および通信部１０８は、第１の実施形態で説明したものと同一である。また、各部１０１～１０８，３０１，３０２の全てまたはいずれかは、例えばカード端末Ａに設けられたＣＰＵ等のプロセッサが同じくカード端末Ａに設けられたＲＯＭ等に記憶されたプログラムを実行することで実現される。

【００６１】

図１０に示すように、鍵リスト部３０１は、暗号鍵リストＲを有している。暗号鍵リストＲには、「０」～「ｎ」（ｎ：自然数）のアドレス（ＡＤＲ）が設定されたエリアが設けられており、各エリアにはそれぞれ暗号鍵Ｋ１～Ｋｎが記述されている。

【００６２】

アドレスカウンタ３０２は、暗号鍵リストＲのアドレス「０」～「ｎ」に対応するカウント値ＡＤＲを記憶する。アドレスカウンタ３０２に記憶されたカウント値ＡＤＲは、カード端末Ａのシステム起動時や予め定められたタイミング等に初期値「０」に設定される。

【００６３】

鍵リスト部３０１は、アドレスカウンタ３０２のカウント値ＡＤＲが示す暗号鍵リストＲのアドレスに記述された暗号鍵にて鍵記憶部１０４に記憶された暗号鍵Ｋｙを更新する。

【００６４】

本実施形態における第１変更部１０３ｂは、アドレスカウンタ３０２のカウント値ＡＤ

Ｒの値を変更することで、鍵記憶部１０４に記憶された暗号鍵Ｋｙを、暗号鍵リストＲの当該変更後のカウント値ＡＤＲが示すアドレスに記憶された暗号鍵に変更する。

【００６５】

ＰＯＳ端末Ｂは、通信部１１１、決済処理部１１２、暗号処理部１１３、鍵記憶部１１４、鍵リスト部３１１、およびアドレスカウンタ３１２を備えている。

【００６６】

このうち通信部１１１、決済処理部１１２、暗号処理部１１３、鍵記憶部１１４は、第１の実施形態で説明したものと同一である。また、各部１１１～１１４，３１１，３１２の全てまたはいずれかは、例えばＰＯＳ端末Ｂに設けられたＣＰＵ等のプロセッサが同じくＰＯＳ端末Ｂに設けられたＲＯＭ等に記憶されたプログラムを実行することで実現される。

【００６７】

鍵リスト部３１１は、カード端末Ａの鍵リスト部３０１が有するものと同じ暗号鍵リストＲを有している。

アドレスカウンタ３１２は、暗号鍵リストＲのアドレス「０」～「ｎ」に対応するカウント値ＡＤＲを記憶する。アドレスカウンタ３１２に記憶されたカウント値ＡＤＲは、ＰＯＳ端末Ｂのシステム起動時や予め定められたタイミング等に初期値として「０」に設定される。

【００６８】

鍵リスト部３１１は、アドレスカウンタ３１２のカウント値ＡＤＲが示す暗号鍵リストＲのアドレスに記述された暗号鍵にて鍵記憶部１１４に記憶された暗号鍵Ｋｙを更新する。

【００６９】

本実施形態における第２変更部１１３ｂは、アドレスカウンタ３１２のカウント値ＡＤＲの値を変更することで、鍵記憶部１１４に記憶された暗号鍵Ｋｙを、暗号鍵リストＲの当該変更後のカウント値ＡＤＲが示すアドレスに記述された暗号鍵に変更する。

【００７０】

［動作］

次に、第３の実施形態におけるカード処理システムにて実行されるカード決済の流れについて説明する。

ＰＯＳ端末Ｂに客が購入しようとする商品の商品情報が入力され、カード決済が選択されると、ＰＯＳ端末Ｂからカード端末Ａにカードの読み取りが指示される。

【００７１】

その後、カード端末Ａの各部は、図１１のフローチャートに沿って動作する。すなわち、鍵リスト部３０１がアドレスカウンタ３０２のカウント値ＡＤＲで示されるアドレスに記述された暗号鍵を暗号鍵リストＲから読み出し、読み出した暗号鍵を暗号鍵Ｋｙとして鍵記憶部１０４に記憶させる（ステップＳ４０１）。

【００７２】

その後、リーダユニット４がカードＣの挿入を待ち、挿入されたカードＣからカード信号を取り込み、データ入力部１０１に入力する（ステップＳ４０２）。このときデータ入力部１０１は、リーダユニット４から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。

【００７３】

続いてコード化部１０２がデータ入力部１０１から入力されたカード信号をコード化してカード情報を生成し、暗号処理部１０３およびカウント部１０６に出力する（ステップＳ４０３）。

【００７４】

カウント部１０６は、入力されたカード情報をメモリ１０６ａに記憶する（ステップＳ４０４）。さらに、カウント部１０６は、メモリ１０６ａに記憶したカード情報とメモリ１０６ｂに記憶された前回のカード情報とが同一であるかを判定する（ステップＳ４０５

）。その結果、両カード情報が一致するならば（ステップＳ４０５のＹｅｓ）、カウント部１０６は、メモリ１０６ｃのカウント値Ｎを１つインクリメントする（ステップＳ４０６）。

【００７５】

このようにカウント値Ｎがインクリメントされた後、比較部１０７が既定値記憶部１０５およびカウント部１０６からそれぞれ既定カウント値Ｎｐおよびカウント値Ｎを読み込み（ステップＳ４０７）、読み込んだ既定カウント値Ｎｐとカウント値Ｎとを比較する（ステップＳ４０８）。

【００７６】

上記比較の結果、カウント値Ｎが既定カウント値Ｎｐ未満（Ｎ＜Ｎｐ）である場合（ステップＳ４０８のＹｅｓ）、その旨が暗号処理部１０３に通知される。このとき、暗号化部１０３ａは、ステップＳ４０２にてコード化部１０２から入力されたカード情報を鍵記憶部１０４に記憶された暗号鍵Ｋｙで暗号化する（ステップＳ４０９）。そして、暗号化部１０３ａは、暗号化した後のカード情報を通信部１０８を介してＰＯＳ端末Ｂに送信する（ステップＳ４１０）。

【００７７】

ステップＳ４０５において両カード情報が一致しない場合（ステップＳ４０５のＮｏ）、カウント部１０６は、メモリ１０６ｃのカウント値Ｎを０にリセットする（ステップＳ４１１）。そして、暗号化部１０３ａがステップＳ４０２にてコード化部１０２から入力されたカード情報を鍵記憶部１０４に記憶された暗号鍵Ｋｙで暗号化し（ステップＳ４０９）、暗号化した後のカード情報を通信部１０８を介してＰＯＳ端末Ｂに送信する（ステップＳ４１０）。

【００７８】

ステップＳ４０８の比較の結果、カウント値Ｎが既定カウント値Ｎｐ以上（Ｎ≧Ｎｐ）である場合（ステップＳ４０８のＮｏ）、その旨が暗号処理部１０３に通知される。このとき、暗号化部１０３ａによる暗号化および送信は行われず、第１変更部１０３ｂが通信部１０８を介して暗号鍵の危殆化をＰＯＳ端末Ｂに通知し（ステップＳ４１２）、ＰＯＳ端末Ｂからの鍵交換指示の返信を待つ（ステップＳ４１３）。

【００７９】

やがてＰＯＳ端末Ｂから後述のステップＳ５０９において返信される鍵交換指示を通信部１０８が受信すると、第１変更部１０３ｂは、アドレスカウンタ３０２のカウント値ＡＤＲを１つインクリメントする（ステップＳ４１４）。さらに、第１変更部１０３ｂは、カウント値Ｎのリセットをカウント部１０６に指令する。この指令を受けたことに応じて、カウント部１０６がカウント値Ｎを０にリセットする（ステップＳ４１５）。

【００８０】

ステップＳ４１０またはステップＳ４１５を以って一連の処理が終了する。なお、ステップＳ４１５を以って処理が終了した場合には、カード決済が完了しない。したがって、再びステップＳ４０１から各部が動作する。その結果、ステップＳ４１４でインクリメントされた後のカウント値ＡＤＲで示されるアドレスに記述された暗号鍵が暗号鍵リストＲから読み出され、暗号鍵Ｋｙとして鍵記憶部１０４に記憶される（ステップＳ４０１）。そして、この暗号鍵Ｋｙを用いてカード情報が暗号化され（ステップＳ４０９）、ＰＯＳ端末Ｂに送信される（ステップＳ４１０）。

【００８１】

次に、第３の実施形態におけるＰＯＳ端末Ｂの動作について説明する。

カード端末Ａにカード Ｃの読み取りを指示した後、ＰＯＳ端末Ｂの各部は、図１２のフローチャートに沿って動作する。すなわち、鍵リスト部３１１がアドレスカウンタ３１２のカウント値ＡＤＲで示されるアドレスに記述された暗号鍵を暗号鍵リストＲから読み出し、読み出した暗号鍵を暗号鍵Ｋｙとして鍵記憶部１０４に記憶させる（ステップＳ５０１）。

【００８２】

その後、暗号処理部１１３がカード端末Ａから送信されるデータの受信を待ち、通信部１１１がカード端末Ａからデータを受信すると（ステップＳ５０２）、そのデータの種別を判定する（ステップＳ５０３）。

【００８３】

この判定の結果、カード端末Ａから受信したデータがステップＳ４１０で送信された暗号化されたカード情報である場合（ステップＳ５０３の「カード情報」）、復号部１１３ａが鍵記憶部１１４に記憶された暗号鍵Ｋｙを用いて当該暗号化されたカード情報を復号する（ステップＳ５０４）。復号後のカード情報は、決済処理部１１２に出力される。

【００８４】

決済処理部１１２は、復号部１１３ａから入力されたカード情報と、客が購入しようとする商品の商品情報とを用いて第１の実施形態にて説明した決済処理を実行する（ステップＳ５０５）。

【００８５】

ステップＳ５０３の判定の結果、カード端末Ａから受信したデータが暗号鍵の危殆化の通知である場合（ステップＳ５０３の「危殆化通知」）、第２変更部１１３ｂがネットワーク２を介してサーバ装置３に暗号鍵の交換を要求し（ステップＳ５０６）、サーバ装置３からの鍵交換指示の返信を待つ（ステップＳ５０７）。この要求を受信したサーバ装置３は、鍵交換指示をＰＯＳ端末Ｂに返信する。このとき、サーバ装置３にて鍵交換指示をＰＯＳ端末Ｂに送信した履歴を残すようにしてもよい。このようにすれば、サーバ装置３にて暗号鍵交換の頻度等を把握できる。

【００８６】

サーバ装置３から返信される暗号鍵Ｋｎを受信すると、第２変更部１１３ｂは、アドレスカウンタ３１２のカウント値ＡＤＲを１つインクリメントする（ステップＳ５０８）。さらに第２変更部１１３ｂは、通信部１１１を介してカード端末Ａに鍵交換指示を送信する（ステップＳ５０９）。

【００８７】

ステップＳ５０５またはステップＳ５０９を以って一連の処理が終了する。なお、ステップＳ５０９を以って処理が終了した場合には、カード決済が完了しない。したがって、再びステップＳ５０１から各部が動作する。その結果、ステップＳ５０８にてインクリメントされた後のカウント値ＡＤＲで示されるアドレスに記述された暗号鍵が暗号鍵リストＲから読み出され、暗号鍵Ｋｙとして鍵記憶部３１４に記憶される（ステップＳ５０１）。そして、この暗号鍵Ｋｙを用いてカード端末Ａから送信される暗号化されたカード情報が復号され（ステップＳ５０４）、決済処理が行われる（ステップＳ５０５）。

【００８８】

このように、本実施形態のカード端末Ａにおいては、アドレスカウンタ３０２のカウント値ＡＤＲによって暗号鍵リストＲから指定された暗号鍵を暗号化部１０３ａが使用する暗号鍵Ｋｙに設定する。そして、このように設定された暗号鍵Ｋｙを用いて暗号化部１０３ａがカード情報を暗号化し、暗号鍵Ｋｙが危殆化した場合には第１変更部１０３ｂがアドレスカウンタ３０２のカウント値ＡＤＲの値を変更することで、暗号化に用いる暗号鍵Ｋｙを変更する。

【００８９】

また、ＰＯＳ端末Ｂにおいては、アドレスカウンタ３１２のカウント値ＡＤＲによって暗号鍵リストＲから指定された暗号鍵を復号部１１３ａが復号に使用する暗号鍵Ｋｙに設定する。そして、このように設定された暗号鍵Ｋｙを用いて復号部１１３ａが暗号化されたカード情報を復号し、暗号鍵Ｋｙが危殆化した場合には第２変更部１１３ｂがアドレスカウンタ３１２のカウント値ＡＤＲの値を変更することで、復号に用いる暗号鍵Ｋｙを変更する。

【００９０】

以上説明したように、第１～第３の実施形態におけるカード処理システムは、カード端末Ａで同一のカード情報が既定回数読み取られたとき、カード端末ＡおよびＰＯＳ端末Ｂ

でカード情報の暗号化および復号に使用される暗号鍵を他の暗号鍵に変更する。このような構成であれば、悪意のある者が暗号鍵を特定すべく同一のカードＣを用いて複数回のカード決済を行った場合等に、自動的にカード端末ＡおよびＰＯＳ端末Ｂで使用される暗号鍵が変更されるので、使用中の暗号鍵の特定が困難となり、システムのセキュリティ性が大幅に向上する。また、使用中の暗号鍵Ｋｙが危殆化した場合に限って暗号鍵Ｋｙを他の暗号鍵に変更するので、不必要に暗号鍵が変更されることがなく、システムの処理負担が軽減され、暗号鍵を変更する処理によるパフォーマンスの低下を防止できる。さらに、暗号鍵の変更が自動的に実行されるので、手間がかからず、システムのメンテナンスコストを低く抑えることができる。

【００９１】

また、第１の実施形態におけるカード処理システムは、カード端末Ａで同一のカード情報が連続して既定回数Ｎｐだけ読み取られたときにカード端末ＡおよびＰＯＳ端末Ｂで使用する暗号鍵Ｋｙを他の暗号鍵に変更する。このような構成であれば、同一のカードＣを用いたカード決済が複数回行われた場合であっても、それらの決済が連続していなければ暗号鍵Ｋｙが変更されない。したがって、悪意のない通常の客が頻繁に同一のカードＣでカード決済を行ったときのように不必要な場合にまで暗号鍵Ｋｙが変更されないので、システムの処理負担をより軽減できる。

【００９２】

また、第２の実施形態におけるカード処理システムは、カード端末Ａで同一のカード情報が既定時間Ｔｐ内に既定回数Ｎｐだけ読み取られたときにカード端末ＡおよびＰＯＳ端末Ｂで使用する暗号鍵Ｋｙを他の暗号鍵に変更する。このような構成であれば、同一のカードＣを使用したカード決済が連続していない場合であっても、それらの決済が既定時間Ｔｐ内に行われていればカード端末ＡおよびＰＯＳ端末Ｂで使用される暗号鍵Ｋｙが変更される。したがって、悪意のある者が暗号鍵を特定すべく複数のカードＣを交互に使用してカード情報の連続性をなくしつつカード決済を行った場合であっても暗号鍵Ｋｙが変更され、暗号鍵Ｋｙの特定が困難となる。

【００９３】

また、第３の実施形態におけるカード処理システムは、カード端末ＡおよびＰＯＳ端末Ｂで使用する暗号鍵Ｋｙを、カード端末ＡおよびＰＯＳ端末Ｂのそれぞれに設けられた暗号鍵リストＲを用いて変更する。このような構成であれば、サーバ装置３が暗号鍵を選定してＰＯＳ端末Ｂに送信する必要がなくなるので、サーバ装置３の処理負担やメンテナンスコストをより軽減できる。

【００９４】

（変形例）

上記各実施形態にて開示した構成は、種々変形実施可能である。具体的な変形例としては、例えば次のようなものがある。

【００９５】

（１）上記各実施形態では、カード端末ＡおよびＰＯＳ端末Ｂを有するカード処理システムを例示した。しかしながら、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鍵の変更に関わる構成を他のカード処理システムに適用してもよい。他のカード処理システムとしては、例えばカードにて各種ポイントを管理するポイント管理システムや、カードにて個人認証を行い、特定の場所への入退室を管理するセキュリティシステム等が想定される。

【００９６】

さらに、カード以外の記憶媒体、例えば携帯電話装置や携帯情報端末（ＰＤＡ）から電波や赤外線等を介した無線通信にて媒体情報を読み取る読取端末と、この読取端末にて読み取られた媒体情報を用いた処理を行う処理端末とを有する情報処理システムに対して、上記各実施形態にて開示した構成を適用してもよい。この場合には、カード端末Ａが備え

るとしたカードの読み取りに関する構成を携帯電話装置や携帯情報端末から媒体情報を読み取る構成に変更して読取端末を構成すればよい。

【００９７】

（２）上記各実施形態では、暗号鍵と復号鍵が同一である共通鍵方式を採用したカード処理システムを例示した。しかしながら、暗号鍵と復号鍵が異なる暗号化方式を採用してもよい。この場合、上記各実施形態におけるＰＯＳ端末Ｂの鍵記憶部１１４にカード端末Ａの鍵記憶部１０４に記憶された暗号鍵Ｋｙに対応する復号鍵を記憶する。そして、第１，第２の実施形態の場合にあってはＰＯＳ端末Ｂからサーバ装置３に暗号鍵の交換が要求された際に、サーバ装置３に暗号鍵Ｋｎとそれに対応する復号鍵とをＰＯＳ端末Ｂに返信させ、第２変更部１１３ｂに鍵記憶部１１４の復号鍵を当該返信された復号鍵に変更させると共に、当該返信された暗号鍵をカード端末Ａに送信させる。また、第３の実施形態の場合にあっては、カード端末Ａの暗号鍵リストＲの各アドレスに記述された暗号鍵に対応する復号鍵を、ＰＯＳ端末Ｂの暗号鍵リストＲの各アドレスに記述しておけばよい。

【００９８】

（３）上記各実施形態では、同一のカード情報が連続してあるいは既定時間内に既定回数読み取られたときに、暗号鍵が危殆化したとして暗号化および復号に用いる暗号鍵を変更する場合を例示した。しかしながら、どのような場合に暗号鍵が危殆化したと扱うかについては、店舗の運営等に合せて適宜変形すればよい。例えば、単に同一のカード情報が既定回数読み取られたときに暗号鍵が危殆化したとして扱ってもよい。

【００９９】

（４）また、上記各実施形態においてカード端末Ａが備えるとした構成の一部をＰＯＳ端末Ｂに設け、ＰＯＳ端末Ｂが備えるとした構成の一部をカード端末Ａに設けてもよい。例えば第３の実施形態のように暗号鍵リストＲを用いて暗号化および復号に使用する暗号鍵を変更する場合に各変更部１０３ｂ，１１３ｂをカード端末Ａの暗号処理部１０３に設けてもよい。この場合、同一のカード情報が連続して既定回数Ｎｐだけ読み取られたならば、第１変更部１０３ｂによって既述の通り鍵記憶部１０４の暗号鍵Ｋｙを変更させる。さらに、変更後の暗号鍵Ｋｙと同一の暗号鍵を第２変更部１１３ｂによってＰＯＳ端末Ｂに送信させ、鍵記憶部１１４に記憶させる。また、第３の実施形態のように暗号鍵リストＲを用いて暗号化および復号に使用する暗号鍵を変更する場合に各変更部１０３ｂ，１１３ｂをＰＯＳ端末Ｂの暗号処理部１１３に設けてもよい。この場合、カード端末Ａにて同一のカード情報が連続して既定回数Ｎｐだけ読み取られたならば、その旨をＰＯＳ端末Ｂに通知させる。そして、この通知を受けたことに応じて、ＰＯＳ端末Ｂの第２変更部１１３ｂに既述の通り鍵記憶部１１４の暗号鍵Ｋｙを変更させる。さらに変更後の暗号鍵Ｋｙと同一の暗号鍵を第１変更部１０３ｂによってカード端末Ａに送信させ、鍵記憶部１０４に記憶させる。

【０１００】

（５）また、カード端末ＡおよびＰＯＳ端末Ｂで実行されるとした処理の一部を、サーバ装置３や、カード処理システムに通信接続された他のサーバ装置に実行させてもよい。

このようにしてシステムを構築する場合、例えばクラウドコンピューティングを利用できる。より具体的には、ＳａａＳ（software as a service）と称されるソフトウェア提供形態が適する。

【０１０１】

図１３はクラウドシステムを利用するカード処理システムの構成図である。

このカード処理システム５００は、クラウド５０１、複数の端末装置５０２および複数の通信ネットワーク５０３、および互いに通信接続された複数のサーバ装置５０４を有する。なお、端末装置５０２、通信ネットワーク５０３、およびサーバ装置５０４は、それぞれ１つのみでもよい。

【０１０２】

端末装置５０２は、通信ネットワーク５０３を介してクラウド５０１と通信可能である。端末装置５０２としては、上記各実施形態にて説明したＰＯＳ端末や、デスクトップタ

イプやノートブックタイプなどの種々のコンピュータ、携帯電話装置、携帯情報端末（ＰＤＡ）、あるいはスマートフォンなどを適宜に利用できる。

【０１０３】

通信ネットワーク５０３としては、インターネット、プライベートネットワーク、次世代ネットワーク（ＮＧＮ）、あるいはモバイルネットワークなどを適宜に利用できる。なお、図示を省略しているが、端末装置５０２にはカードに記憶されたカード情報を読み取るカード端末が接続される。

【０１０４】

このような構成のカード処理システム５００において、上記各実施形態でカード端末ＡおよびＰＯＳ端末Ｂが実行するとした処理の少なくとも一部をサーバ装置５０４に実行させ、残りの処理を端末装置５０２に実行させる。なお、複数のサーバ装置５０４にて処理を分担させてもよい。さらに、サーバ装置５０４で実行させない処理のうち、上記各実施形態にてカード端末Ａが実行するとしたものの一部を端末装置５０２で実行させ、ＰＯＳ端末Ｂで実行するとしたものの一部を端末装置５０２に接続されたカード端末で実行させてもよい。

【０１０５】

例えば、上記各実施形態においてＰＯＳ端末Ｂの決済処理部１１２が実行するとした決済処理（ステップＳ２０４，Ｓ５０５）、第１変更部１０３ｂが実行するとした処理（ステップＳ１１１～Ｓ１１４，Ｓ３１０～Ｓ３１３，Ｓ４１２～Ｓ４１４）、および第２変更部１１３ｂが実行するとした処理（ステップＳ２０５～Ｓ２０８，Ｓ５０６～Ｓ５０９）の一部あるいは全てをサーバ装置５０４に実行させる。

【０１０６】

この場合、例えば決済処理部１１２が実行するとした決済処理をサーバ装置５０４で実行させるならば、端末装置５０２からサーバ装置５０４に客が購入しようとする商品の商品情報および端末装置５０２に接続されたカード端末で読み取られたカード情報を送信させ、これらの情報を用いてサーバ装置５０４に決済処理を実行させる。また、サーバ装置５０４に各変更部１０３ｂ，１１３ｂの処理を実行させるならば、端末装置５０２に接続されたカード端末にて同一のカード情報が既定回数Ｎｐだけ読み取られた場合等にカードの危殆化をサーバ装置５０４に端末装置５０２を介して通知させ、この通知を受けたサーバ装置５０４に端末装置５０２およびこれに接続されたカード端末の鍵記憶部に記憶された暗号鍵および復号鍵を他の暗号鍵およびこれに対応する復号鍵に変更させる。

【０１０７】

また、端末装置５０２で実行される処理を端末装置５０２が有するプロセッサに実現させるためのプログラムを予め端末装置５０２が有するメモリに記憶させておいてもよいし、同プログラムをクラウド５０１が有するメモリに記憶しておき、必要に応じてクラウド５０１から端末装置５０２へと与えるようにしてもよい。上記プログラムをクラウド５０１から端末装置５０２へと与える場合には、サーバ装置５０４のうちの少なくとも１つに、上記プログラムを端末装置５０２へと送信する機能を設ける。

【０１０８】

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。

【符号の説明】

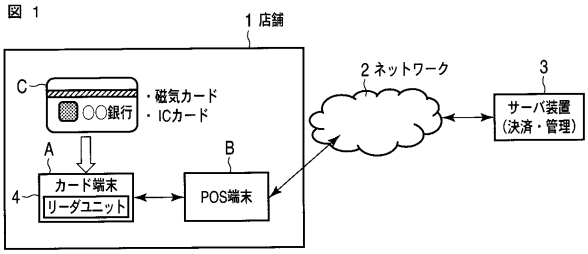
【０１０９】

Ａ…カード端末、Ｂ…ＰＯＳ端末、３…サーバ装置、１０１…データ入力部、１０２…コード化部、１０３…暗号処理部、１０３ａ…暗号化部、１０３ｂ…第１変更部、１０４，１１４…鍵記憶部、１０５…既定値記憶部、１０６…カウント部、１０７…比較部、１

０８，１１１…通信部、１１２…決済処理部、１１３…暗号処理部、１１３ａ…復号部、１１３ｂ…第２変更部、Ｋｙ…暗号鍵

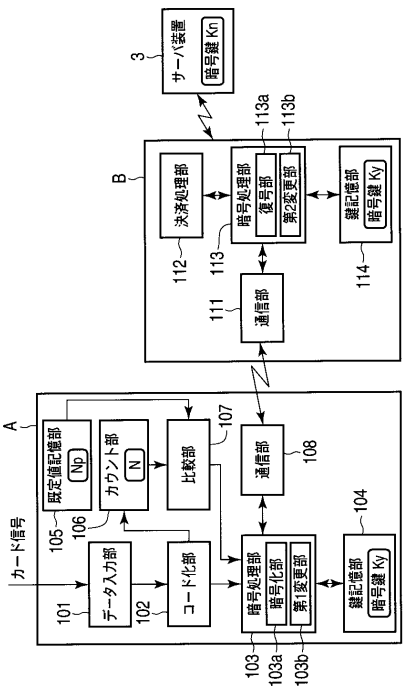
【図１】

図 1



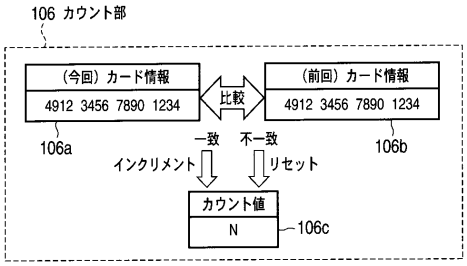
【図２】

図 2



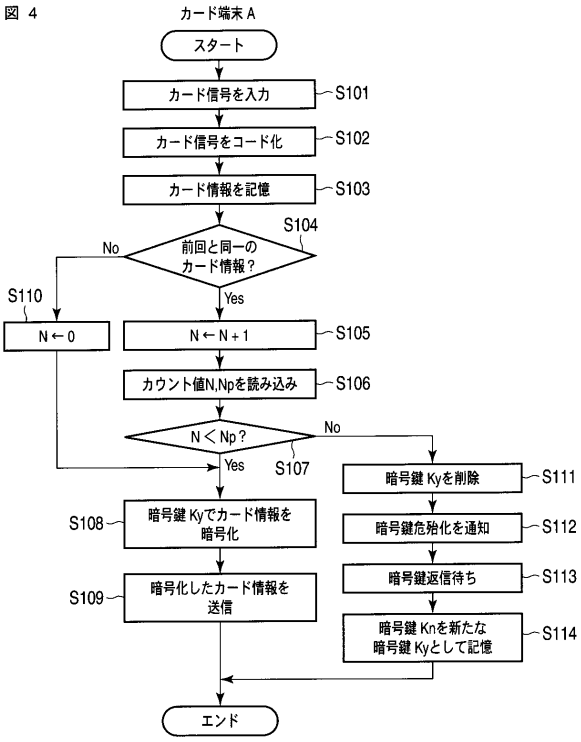
【図３】

図 3



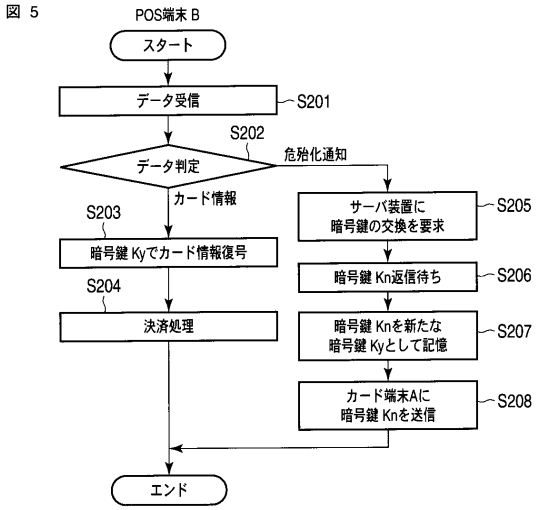
【図４】

図 4



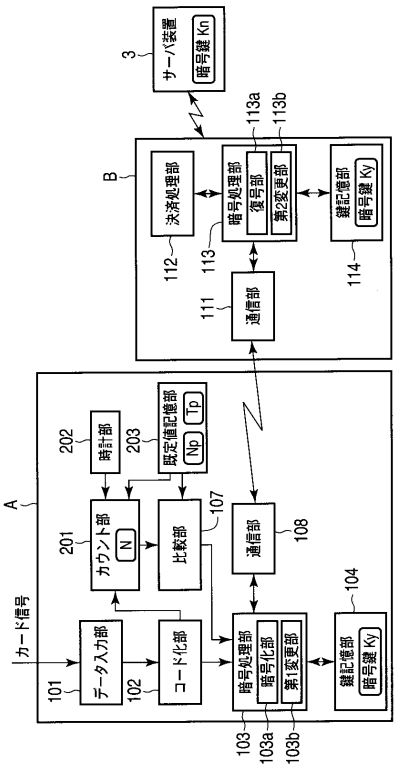
【図５】

図 5



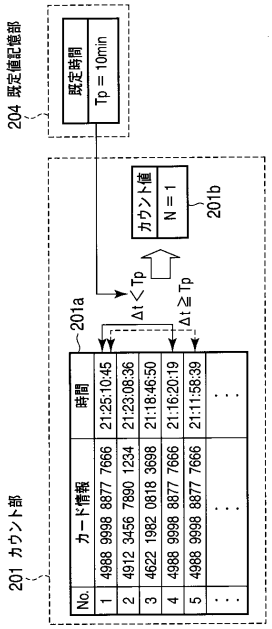
【図６】

図 6



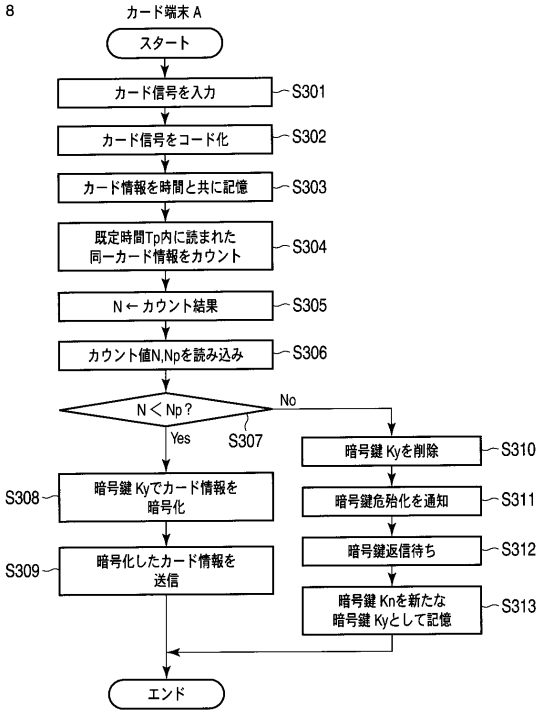
【図７】

図 7



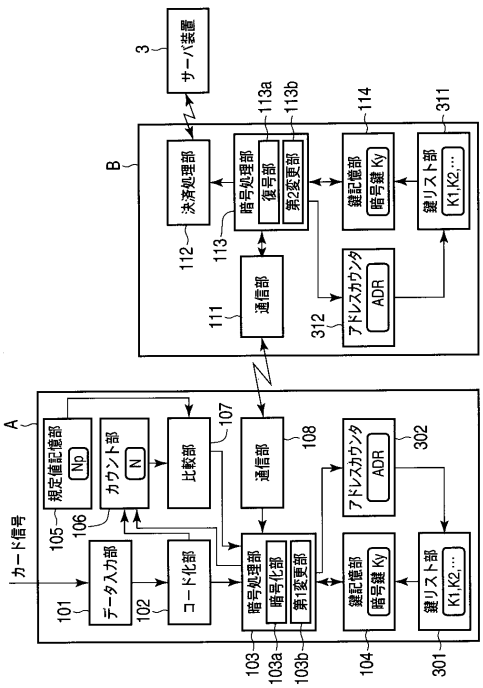
【図８】

図 8



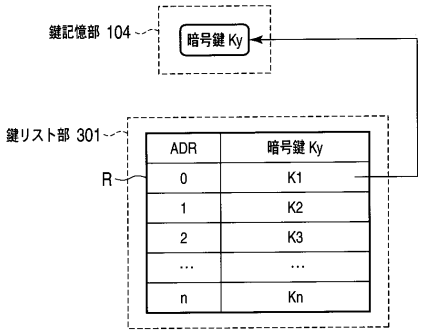
【図９】

図 9



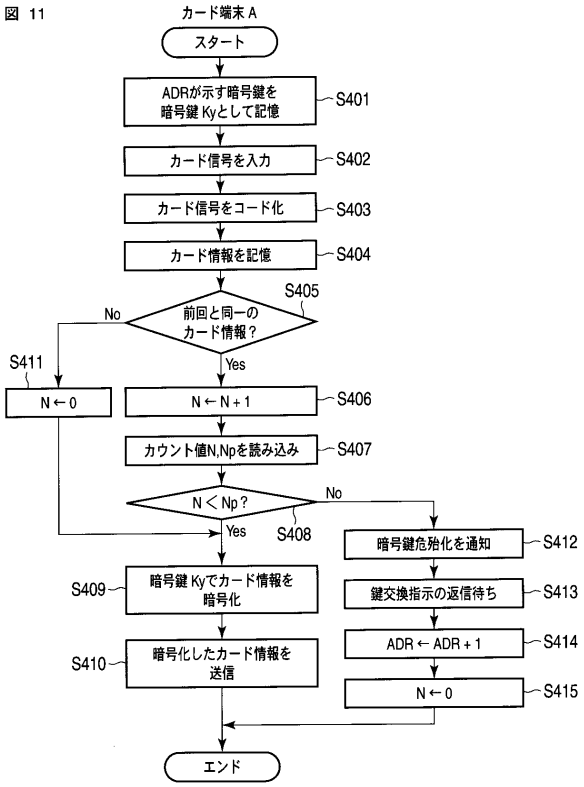
【図１０】

図 10



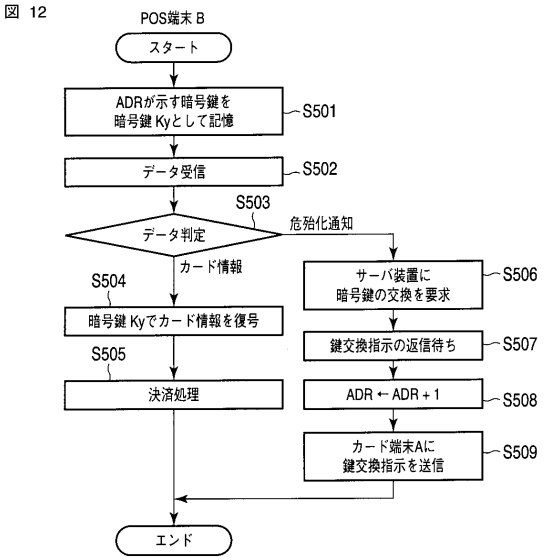
【図１１】

図 11



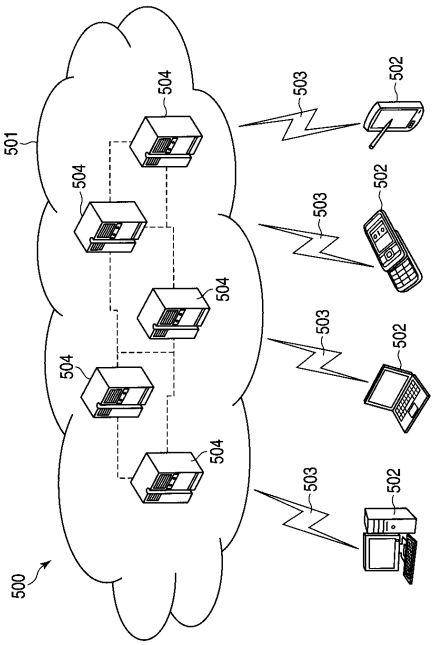
【図１２】

図 12



【図１３】

図 13



フロントページの続き

(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(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
(74)代理人 100134290
弁理士 竹内 将訓
(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

Ｆターム(参考) 5B017 AA01 BA07 BB02 CA16
5J104 AA16 AA34 AA41 EA04 EA08 EA18 JA03 NA02 NA27 NA37
PA14