(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ１）　(11)特許番号
特許第3493024号
(P3493024)
(45)発行日　平成16年２月３日(2004.2.3)　(24)登録日　平成15年11月14日(2003.11.14)

(51)Int.Cl.[7]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　17/60	４１４
Ｇ０６Ｆ　17/60	４１４		５０６
	５０６		５１２
	５１２	Ｈ０４Ｌ　9/00	６７５Ｚ
Ｈ０４Ｌ　9/08			６７５Ａ

請求項の数８(全 20 頁)　最終頁に続く

(21)出願番号　特願2002－263018(P2002－263018)
(22)出願日　平成14年９月９日(2002.9.9)
審査請求日　平成14年11月１日(2002.11.1)
(31)優先権主張番号　特願2002－97941(P2002－97941)
(32)優先日　平成14年３月29日(2002.3.29)
(33)優先権主張国　日本（ＪＰ）
早期審査対象出願

(73)特許権者　502306660
日本テレコム株式会社
東京都中央区八丁堀四丁目７番１号
(72)発明者　鈴木　秀孝
東京都中央区八丁堀四丁目７番１号　日本テレコム株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　(外５名)
審査官　阿波　進

(56)参考文献　特開2002－24730（ＪＰ，Ａ）
特開2001－109835（ＪＰ，Ａ）
国際公開01／009807（WO，Ａ１）
国際公開02／008981（WO，Ａ１）
米国特許6000832（ＵＳ，Ａ）

最終頁に続く

(54)【発明の名称】　情報処理システム及び情報処理方法

(57)【特許請求の範囲】
【請求項１】　携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードとで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信するサーバと、
第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コードとに分離し、当該第３暗証コードと上記第２暗証コードとが一致する場合には上記秘匿情報が有効であると判断し、所定の処理を行う情報読取装置と、を有することを特徴とする情報処理システム。

【請求項２】　携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードと第１時間情報とで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信するサーバと、
第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コード、第２時間情報とに分離し、当該第３暗証コードと上記第２暗証コードとの

比較結果と上記第２時間情報とに基づいて、上記秘匿情報の有効性を判断し、当該秘匿情報が有効であると判断された場合には所定の処理を行う情報読取装置と、を有することを特徴とする情報処理システム。

【請求項３】　上記情報読取装置は、携帯電話機の暗号情報に基づく表示を光学的に読み取る読取手段を更に有し、当該読取手段による光学的な読み取りにより携帯電話機に記憶された暗号情報を得る、ことを更なる特徴とする請求項1又は２のいずれかに記載の情報処理システム。

【請求項４】　上記情報読取装置は、携帯電話機と無線通信を行う無線通信手段を更に有し、当該無線通信手段による無線通信により携帯電話機に記憶された暗号情報を得る、ことを更なる特徴とする請求項1又は２のいずれかに記載の情報処理システム。

【請求項５】　少なくともサーバと情報読取装置とを有する情報処理システムによる情報処理方法において、

サーバが、

携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードとで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信し、

情報読取装置が、

第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コードとに分離し、当該第３暗証コードと上記第２暗証コードとが一致する場合には上記秘匿情報が有効であると判断し、所定の処理を行う、ことを特徴とする情報処理方法。

【請求項６】　少なくともサーバと情報読取装置とを有する情報処理システムによる情報処理方法において、

サーバが、

携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードと第１時間情報とで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信し、

情報読み取り装置が、

第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コード、第２時間情報とに

分離し、当該第３暗証コードと上記第２暗証コードとの比較結果と上記第２時間情報とに基づいて、上記秘匿情報の有効性を判断し、当該秘匿情報が有効であると判断された場合には所定の処理を行う、ことを特徴とする情報処理方法。

【請求項７】　上記情報読取装置の読取手段が携帯電話機の表示を光学的に読み取ることで該携帯電話機に記憶された暗号情報を得るステップを更に有することを特徴とする請求項５又は６のいずれかに記載の情報処理方法。

【請求項８】　上記情報読取装置の無線通信手段が携帯電話機と無線通信を行うことで該携帯電話機に記憶された暗号情報を得るステップを更に有することを特徴とする請求項５又は６のいずれかに記載の情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、決済等の情報処理を行うシステム及び方法に係り、特に利用者が店舗等の加盟店において商品を購入した際、或いはサービスの提供を受けた際に、当該商品等の代金の支払い等に係る決済等を行うとき、当該利用者の個人情報の漏洩を防止し秘匿性を高める情報処理システム及び情報処理方法に関するものである。

【０００２】

【従来の技術】従来、店舗等において商品を購入し、或いはサービスの提供を受けた際に、利用者が保有するクレジットカード等を用いて決済を行うことは一般的になされている。図１０には、従来技術に係る情報処理システムとしての決済システムの構成を示し説明する。この決済システムは、利用者の情報記憶媒体２００と、加盟店に配設された情報読取装置２０１と、信販会社のサーバ２０２からなる。

【０００３】このような構成の下、利用者が店舗等の加盟店においてクレジットカード等の情報記憶媒体２００を提示すると、情報読取装置２０１の情報読取部２０１ａが当該情報記憶媒体２００内の情報記憶部２００ａに記憶された情報Ａを読み出して、送信／受信部２０１ｂを介してサーバ２０２側に送信する。こうして、サーバ２０２では、その内部の送信／受信部２０２ａが当該情報Ａを受信し、更に課金処理部２０２ｂにおいて所定の課金処理を行うことになる。

【０００４】一方、今日では、携帯電話機及びインターネットの普及に伴い、ＥコマースやＭコマースが盛んに行われるようになっており、更にはインターネットのＷｅｂページを通じても様々なサービスが提供されている。かかるサービスの１つに携帯端末を利用した「チケットレスサービス」がある。これは、紙ベースで発券していた従来型のチケットの換わりに、電子メールを携帯端末に送信し、或いはＷｅｂサーバより携帯端末に識別情報を送信し、例えば店舗等の加盟店において当該携帯

端末に表示されている情報に基いた識別を行うものであり、例えば映画や旅行のチケットやクーポン等の用途で利用されている。更に、インターネットを通じてＷｅｂ上でショッピングする「インターネットショッピング」や携帯端末を用いた「モバイルショッピング」の利用も増加の傾向にあるが、このようなサービスでは、インターネットを介して決済が行われることになる。

【０００５】そして、上記の如き決済を行う場合には、デジタル情報の欠点であるコピーや複製を防止するために、インターネットを介して送信される情報を、例えば公開鍵方式やバーコード方式等により暗号化することも一般的になされている。

【０００６】例えば特開２００１－５８８３号公報では、決済システムに係る技術が開示されている。即ち、この決済システムでは、携帯型端末が、認証サーバから送信されたバーコード情報に基づきディスプレイにバーコードパターンを表示する。そして、店舗のＰＯＳレジスタに接続されたバーコードリーダが、当該バーコードパターンを読み取り、取得した情報を決済コントローラに送信する。こうして決済コントローラが、当該情報に基づく決済を行う、というものである。

【０００７】

【発明が解決しようとする課題】しなしながら、上記チケットレスサービスが対象としている映画のチケットや電子クーポン等は、一度使用すると再利用が不可能であることから問題は少ないが、上記インターネットショッピングやモバイルショッピングで入力される利用者のクレジットカードの番号等に係る情報は再利用可能なものであり、当該情報がインターネットを介して送受信される過程で漏洩すると不正使用される可能性もあることから、そのセキュリティの面で更なる改善が嘱望されている。

【０００８】さらに、上記モバイルショッピングでは、そのサービスに加入している加盟店でのみショッピングが可能となるにすぎないことから、利用者の間に広く普及しているクレジットカードによる決済に比べると、その利便性は低い。

【０００９】また、前述した特開２００１－５８８３号公報により開示された決済システム等に係る技術では、情報のセキュリティを高めるべくバーコード方式が採用されているものの、例えばクレジットカードの番号等に係る情報が再利用可能なものである点については考慮されておらず、従って、携帯端末の紛失時等における不正使用対策については、何等示唆も開示もされていない。

【００１０】本発明は、上記問題に鑑みてなされたもので、その目的とするところは、既存のシステムを大きく変更することなく、簡易な構成を付加するだけで、効果的な不正使用防止機能を実現し、セキュリティを向上させつつ、利用者が携帯電話機をカードの代用として店舗等において利用可能とする等、利用者の利便性や利用者の個人情報の秘匿性を向上させることにある。

【００１１】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明は、携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードとで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信するサーバと、第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コードとに分離し、当該第３暗証コードと上記第２暗証コードとが一致する場合には上記秘匿情報が有効であると判断し、所定の処理を行う情報読取装置と、を有することを特徴とする情報処理システムとしたものである。　請求項２の発明は、携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードと第１時間情報とで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信するサーバと、第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コード、第２時間情報とに分離し、当該第３暗証コードと上記第２暗証コードとの比較結果と上記第２時間情報とに基づいて、上記秘匿情報の有効性を判断し、当該秘匿情報が有効であると判断された場合には所定の処理を行う情報読取装置と、を有することを特徴とする情報処理システムとしたものである。　請求項３の発明は、上記情報読取装置は、携帯電話機の暗号情報に基づく表示を光学的に読み取る読取手段を更に有し、当該読取手段による光学的な読み取りにより携帯電話機に記憶された暗号情報を得る、ことを更なる特徴とする請求項1又は２のいずれかに記載の情報処理システムとしたものである。　請求項４の発明は、上記情報読取装置は、携帯電話機と無線通信を行う無線通信手段を更に有し、当該無線通信手段による無線通信により携帯電話機に記憶された暗号情報を得る、ことを更なる特徴とする請求項1又は２のいずれかに記載の情報処理システムとしたものである。　請求項５の発明は、少なくともサーバと情報読取装置とを有する情報処理システムによる情報処理方法において、サーバが、携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードとで可逆

的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信し、情報読取装置が、第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コードとに分離し、当該第３暗証コードと上記第２暗証コードとが一致する場合には上記秘匿情報が有効であると判断し、所定の処理を行う、ことを特徴とする情報処理方法としたものである。　請求項６の発明は、少なくともサーバと情報読取装置とを有する情報処理システムによる情報処理方法において、サーバが、携帯端末からの利用者情報を受信し、当該利用者情報に対応する秘匿情報と第１暗証コードと第１時間情報とで可逆的な演算を実施して付加情報を生成し、予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵を生成し、当該第２共通鍵により上記付加情報を暗号化して暗号情報を生成し、該暗号情報を上記携帯端末に返信し、情報読み取り装置が、第２暗証コードの入力を受け、当該第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成し、上記携帯端末からの暗号情報を受信し、当該暗号情報を上記第３共通鍵により復号化し、更に逆演算により秘匿情報と第３暗証コード、第２時間情報とに分離し、当該第３暗証コードと上記第２暗証コードとの比較結果と上記第２時間情報とに基づいて、上記秘匿情報の有効性を判断し、当該秘匿情報が有効であると判断された場合には所定の処理を行う、ことを特徴とする情報処理方法としたものである。　請求項７の発明は、上記情報読取装置の読取手段が携帯電話機の表示を光学的に読み取ることで該携帯電話機に記憶された暗号情報を得るステップを更に有することを特徴とする請求項５又は６のいずれかに記載の情報処理方法としたものである。　そして、請求項８の発明は、上記情報読取装置の無線通信手段が携帯電話機と無線通信を行うことで該携帯電話機に記憶された暗号情報を得るステップを更に有することを特徴とする請求項５又は６のいずれかに記載の情報処理方法としたものである。

【００１２】

【００１３】

【００１４】

【００１５】

【００１６】

【００１７】

【００１８】

【００１９】

【００２０】

【００２１】

【００２２】

【００２３】

【００２４】

【００２５】

【００２６】

【００２７】

【００２８】

【００２９】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について説明する。

【００３０】先ず、図１には、本発明の実施の形態に係る情報処理システムの概略構成を示し概説する。即ち、ここでは、後述する第１乃至第３の実施の形態に係る情報処理システム及び情報処理方法に共通する構成及び作用を説明する。

【００３１】図１（ａ）に示されるように、携帯電話機１は、インターネット等のネットワーク４を介してサービス提供者のサーバ２と通信自在に接続され、当該サーバ２は、信販会社のサーバ３ａ，３ｂ･･･と専用線５ａ，５ｂ･･･を介して通信自在に接続されている。以上の構成により、携帯電話機１において暗号化されたカード番号を２次元バーコードとして表示するまでの処理が実現される。

【００３２】尚、以下では、図１（ａ）のサーバ３ａ，３ｂ･･･を符号３により総称し、専用線５ａ，５ｂを符号５により総称し、説明を更に進める。

【００３３】このような構成において、携帯電話機１は、ネットワーク４を介して、利用者情報をサーバ２に送信する。サーバ２は、この利用者情報を受信すると、ユーザ情報蓄積データベース１８を参照して、当該利用者情報に対応するカード番号情報を取得する。尚、上記サーバ２が、ユーザ情報蓄積データベース１８を具備していない場合には、信販会社のサーバ３と専用線５を介して通信を行うことで利用者のカード番号情報を取得する。続いて、サーバ２は、このカード番号情報に時間情報を付加した上で暗号化し、暗号情報を生成する。さらに、この暗号情報を２次元データに変換し、当該２次元データをネットワーク４を介して携帯電話機１側に返送する。この携帯電話機１は、この２次元データ受信すると、２次元バーコード等の態様で表示する。或いは、暗号化情報を記憶し、後述するように情報読取装置８と無線通信を行う。尚、上述のように時間情報を付加せずに、別途記憶手段に記憶し、有効性確認に用いる方法を採用することもできる。

【００３４】一方、図１（ｂ）に示されるように、加盟店の情報読取装置８には変換部７を介してバーコードリーダ６が接続されている。この情報読取装置８は、専用線１０ａ，１０ｂ･･･を介して、信販会社のサーバ３ｘ，３ｙ･･･と通信自在に接続されている。尚、上記バ

ーコードリーダ６及び変換部７の構成に換えて、或いは当該構成と共に、携帯電話機１との間で無線通信を実現する無線通信部９を採用することも可能である。そして、このような無線通信部９を採用する場合には、携帯電話機１側にも同種の構成が必要となる。以上の構成により、携帯電話１において表示された２次元バーコードに基づく決済等の情報処理が実現される。

【００３５】尚、以下では、図１（ｂ）のサーバ３ｘ，３ｙ･･･も符号３により総称し、専用線１０ａ，１０ｂを符号１０により総称し、説明を更に進める。但し、サーバ３ｘ，３ｙは、上記サーバ３ａ，３ｂとは別のサーバであってもよい。

【００３６】このような構成において、店舗等の加盟店において、利用者が２次元バーコードを表示した携帯電話機１を提示すると、バーコードリーダ６が当該２次元バーコードを読み取り、変換部７が当該２次元バーコードを暗号情報、更にはカード番号情報と時間情報に変換し、当該時間情報が有効であるか否かを判断する。そして、変換部７は、時間情報が有効であると判断した場合には、カード番号情報を情報読取装置８側に送信する。すると、情報読取装置８は、カード番号情報を専用線１０を介して信販会社のサーバ３に送信する。こうして、サーバ３は、当該カード番号等に係る情報に基づいて所定の課金処理を行う。

【００３７】尚、上記無線通信部９を採用する場合、携帯電話機１は無線通信により暗号情報を無線通信部９に送信する。無線通信部９は、当該暗号情報を受信すると、当該暗号情報をカード番号情報と時間情報とに復号し、時間情報が有効であるか否かを判断する。以降、上記同様の処理がなされることになる。

【００３８】このように、実施の形態に係る情報処理システム及び方法では、カード番号情報に時間情報を付加した上で暗号化し、更に２次元データに変換することで、情報の秘匿性を高めている。また、決済時には、上記時間情報に基づいて情報の有効性を判断しているので、紛失時等における不正使用も防止される。

【００３９】

【００４０】また、秘匿情報とは、上記カード番号情報等に相当するものである。また、読取手段とはバーコードリーダ６及び変換器７等に相当し、無線通信手段とは無線通信部９等に相当する。但し、これらには限定されない。

【００４１】以下、このような特徴点をふまえつつ、本発明の第１の実施の形態に係る情報処理システム及び情報処理方法について更に詳細に説明する。

【００４２】先ず、図２には第１の実施の形態に係る情報処理システムの構成を示し説明する。図２に示されるように、この情報処理システムは、サービスの利用者の携帯電話機１、サービス提供者のサーバ２、店舗等の加盟店の２次元情報読取装置５４及び情報読取装置８、信

販会社のサーバ３からなる。ここでは、先に示した図１と同一構成については同一構成を付しているが、２次元情報読取装置５４は図１（ｂ）におけるバーコードリーダ６及び変換機７を含む構成要素である。

【００４３】以下、これら各構成要素について更に詳細に説明する。

【００４４】先ず、利用者の携帯電話機１は、全体の制御を司る制御部１５、ＩＤ／ＰＷ入力部１１、サービス選択部１２、２次元データ蓄積部１３、２次元データ表示部１４、送受信部１６が通信自在に接続され、構成されている。

【００４５】このような構成において、制御部１５は、ＣＰＵ等からなる。ＩＤ／ＰＷ入力部１１は、利用者が自己のＩＤやＰＷ等を入力するためのものであり、サービス選択部１２は、利用者が所望とするサービスを選択枝の中から選択するためのものである。このＩＤ／ＰＷ入力部１１及びサービス選択部１２としては、例えば操作キー等を採用することができる。２次元データ蓄積部１３は、サービス提供者のサーバ２から送信された２次元データを蓄積するためのものであり、メモリ等からなる。２次元データ表示部１４は、上記２次元データ蓄積部１３に蓄積された２次元データを表示するためのものであり、液晶表示ユニット等を採用することができる。そして、送受信部１６はサービス提供者のサーバ２等との間での無線通信を実現するためのものである。尚、ここでは、携帯電話機１を例に挙げているが、これに限定されずＰＤＡ(Personal Digital Assistant)やノート型パーソナルコンピュータ等の携帯端末を採用することもできる。

【００４６】一方、サービス提供者のサーバ２は、認証部２０、サービス選択部２１、時間情報付加部２２、暗号化部２３、２次元データ化部２４を少なくとも有した制御部１９と、２次元データ蓄積部２５と、送受信部１７と、ユーザ情報蓄積ＤＢ１８と、が通信自在に接続され、構成されている。

【００４７】このような構成において、送受信部１７は、利用者の携帯電話機１等と通信を行うためのものである。ユーザ情報蓄積ＤＢ１８は、利用者のＩＤやＰＷ、携帯電話番号、更にはこれらに対応したカード番号等を蓄積するためのデータベースである（図５参照）。ここでは、これら各種情報は、利用者により事前に登録されているものとする。認証部２０は、利用者について所定の認証を行うためのものである。サービス選択部２１は、携帯電話機１のサービス選択部１２により入力された情報に基づき、利用者のカード番号情報Ａをユーザ情報蓄積ＤＢ１８より読み出すためのものである。そして、時間情報付加部２２は、上記情報Ａに時間情報Ｔを付加するためのものである。暗号化部２３は、公開鍵方式等により上記付加後の情報を暗号鍵により暗号化して暗号情報（Ａ＋Ｔ）を生成するためのものである。そし

て、２次元データ化部２４は、上記暗号情報（Ａ＋Ｔ）を更に２次元データ[Ａ＋Ｔ]に変換するためのものであり、２次元データ蓄積部２５は当該２次元データ[Ａ＋Ｔ]を蓄積するためのものであり、メモリ等からなる。

【００４８】一方、加盟店の２次元情報読取装置５４は、２次元データ読取部２６、２次元データ解析部２７、復号部２８、時間情報判定部２９からなる。この２次元データ読取部２６と２次元データ解析部２７は、図１（ｂ）のバーコードリーダ６に相当し、復号化部２８と時間情報判定部２９は変換部７に相当する。

【００４９】また、加盟店の情報読取装置８は、情報読取部３０と送受信部３１を有している。情報読取装置８としては、ＰＯＳ端末等を採用することができる。

【００５０】このような構成において、２次元データ読取部２６は、携帯電話機１の２次元データ表示部１４に表示された２次元データ[Ａ＋Ｔ]を、例えば光学的な手段により読み取るためのものである。２次元データ解析部２７は、この２次元データ[Ａ＋Ｔ]を暗号情報（Ａ＋Ｔ）に変換するためのものである。

【００５１】そして、復号化部２８は暗号情報（Ａ＋Ｔ）を復号鍵により暗号化前の情報に復号するためのものである。さらに、時間情報判定部２９は、この暗号化前の情報より時間情報を読み出し、当該情報が有効であるか否かを判定するためのものである。また、情報読取部３０は、上記暗号化前の情報よりカード番号情報Ａを抽出するためのものである。そして、送受信部３１は、当該カード番号情報Ａを信販会社のサーバ３に送信するためのものである。

【００５２】一方、信販会社のサーバ３は、決済システムとしての機能も備えたものであって、送受信部３２と課金処理部３３とで構成されている。

【００５３】このサーバ３としては、公知の技術を採用することができるので、詳細な説明は省略するが、送受信部３２は加盟店の情報読取装置８から送信されたカード番号情報Ａを受信するためのものである。課金処理部３３は、このカード番号情報Ａに基づいて利用者に対する課金処理を行うためのものである。

【００５４】以下、図３のフローチャートを参照して、上述したような構成の第１の実施の形態に係る情報処理システムによる処理を詳細に説明する。尚、この処理は、本発明の第１の実施の形態に係る情報処理方法にも相当するものである。

【００５５】この情報処理システムによる一連の処理が開始されると、先ず、利用者により携帯電話機１のＩＤ／ＰＷ入力部１１やサービス選択部１２が操作され、サービス提供者のＷｅｂサイトのＵＲＬが入力されると、携帯電話機１は、制御部１５による制御の下、送受信部１６及びネットワーク４を介して、サービス提供者のサーバ２（上記ＵＲＬ）にアクセスを行うことになる（ステップＳ１）。

【００５６】サービス提供者のサーバ２は、この携帯電話機１からのアクセスを送受信部１７を介して受けると、制御部１９による制御の下、ＰＷ入力画面に係るファイルを不図示のＤＢより読み出し、送受信部１７及びネットワーク４を介して、携帯電話機１に送信する（ステップＳ２）。携帯電話機１は、送受信部１６にてＰＷ入力画面に係るファイルを受信すると、制御部１５による制御の下、２次元データ表示部１４においてＰＷ入力画面を表示する（ステップＳ３）。

【００５７】このＰＷ入力画面の様子は、例えば図４（ａ）に示される通りである。

【００５８】即ち、このＰＷ入力画面１００では、利用者に認証情報の入力を促す「認証情報を入力してください。」とのコメントと、ＰＷを入力すべきＰＷ入力領域１００ａ、送信を指示するための送信指示ボタン１００ｂが表示されている。尚、ＰＷ入力画面１００は、これに限定されるものでないことは勿論である。即ち、例えばＩＤ入力領域等をＰＷ入力画面１００に適宜組み込むことも可能である。

【００５９】こうして、利用者により、ＩＤ／ＰＷ入力部１１が操作され、ＰＷ入力領域１００ａにＰＷが入力され、送信ボタン１００ｂが選択されると、この携帯電話機１は、制御部１５による制御の下、ＰＷ情報を、送受信部１６及びネットワーク４を介して、サービス提供者のサーバ２に送信する（ステップＳ４）。

【００６０】サービス提供者のサーバ２は、送受信部１７がＰＷ情報を受信すると、認証部２０が当該ＰＷ情報に基づく所定の認証処理を行い（ステップＳ５）、この認証が成立すると判断した場合には、続いて、カード選択画面に係るファイルを不図示のＤＢより読み出して、制御部１９による制御の下、送受信部１７及びネットワーク４を介して、携帯電話機１に送信する（ステップＳ６）。

【００６１】こうして、携帯電話機１では、送受信部１６が上記サーバ２からのカード選択画面に係るファイルを受信すると、制御部１５による制御の下、２次元データ表示部１４においてカード選択画面を表示する（ステップＳ７）。

【００６２】このカード選択画面の様子は、例えば図４（ｂ）に示される通りである。

【００６３】即ち、このカード選択画面１０１では、利用者に対してカードの種類の選択を促す「カードの種類を選択してください。」とのコメントと、カードを実際に選択する選択肢（この例では３つの選択肢）を示したカード選択領域１０１ａ、送信を指示するための送信指示ボタン１０１ｂが表示されている。尚、このカード選択画面１０１は、これに限定されるものでないことは勿論である。

【００６４】続いて、利用者によりＩＤ／ＰＷ入力部１１が操作され、カード選択領域１０１ａにて所望とする

カードが選択され、送信ボタン１０１ｂが選択されると、携帯電話機１は、制御部１５による制御の下、カード選択に係る情報（以下、利用者情報と称する）を、送受信部１６及びネットワーク４を介してサービス提供者のサーバ２に送信することになる（ステップＳ８）。

【００６５】そして、サービス提供者のサーバ２は、送受信部１７が利用者情報を受信すると、ユーザ情報蓄積ＤＢ１８より当該利用者情報に対応するカード番号情報Ａを読み出す。ここで、サーバ２がユーザ情報蓄積ＤＢ１８を有しない場合には、以下の手法を採る。即ち、サーバ２は、専用線５を介して信販会社のサーバ３に利用者情報を送信する（ステップＳ９）。すると、サーバ３は、利用者情報に対応するカード番号情報Ａを読み出し、専用線５を介してサーバ２側に返信する（ステップＳ１０）。この第１の実施の形態では、このいずれの手法によっても、利用者情報に対応したカード番号情報Ａが取得されることになる。

【００６６】続いて、サービス提供者のサーバ２では、時間情報付加部２２が、上記カード番号情報Ａに時間情報Ｔを付加し付加情報Ａ＋Ｔを生成し、暗号化部２３が、公開鍵方式等により上記付加情報Ａ＋Ｔを暗号鍵により暗号化して暗号情報（Ａ＋Ｔ）を生成する。そして、２次元データ化部２４が、上記暗号情報（Ａ＋Ｔ）を更に２次元データ[Ａ＋Ｔ]に変換し、２次元データ蓄積部２５が、この２次元データ[Ａ＋Ｔ]を蓄積する（ステップＳ１１）。こうして、サーバ２は、制御部１９による制御の下、この生成された２次元データ[Ａ＋Ｔ]を、送受信部１７及びネットワーク４を介して、利用者の携帯電話機１に送信する（ステップＳ１２）。

【００６７】そして、携帯電話機１は、この２次元データ[Ａ＋Ｔ]を送受信部１６が受信すると、２次元データ蓄積部１３に当該２次元データ[Ａ＋Ｔ]を蓄積する。そして、制御部１５が、当該２次元データ[Ａ＋Ｔ]を読み出し、２次元データ表示部１４に２次元データ表示画面を表示する（ステップＳ１３）。

【００６８】ここで、この２次元データ表示画面は、図４（ｃ）に示される通りである。

【００６９】即ち、この表示例では、２次元データ表示画面１０２には、例えば、認証完了後の動作を示唆する「認証できました。下記の２次元バーコードを加盟店に提示してください。」とのコメントと、２次元バーコード１０２ａとが表示される。この２次元データ表示画面１０２は、この例に限定されるものでない。

【００７０】即ち、例えば上記認証完了の動作を示唆するコメントは上記例に限定されるものではなく、また、表示させないようにすることも可能である。

【００７１】こうして、利用者が店舗等の加盟店に出向き、当該加盟店において携帯電話機１を提示すると（ステップＳ１４）、加盟店の２次元情報読取装置５４の２次元データ読取部２６は、携帯電話機１の２次元データ表示部１４に表示された２次元データ[Ａ＋Ｔ]を読み取る（ステップＳ１５）。２次元データ解析部２７は、この２次元データ[Ａ＋Ｔ]を暗号情報（Ａ＋Ｔ）に変換し、更に復号部２８は当該暗号情報（Ａ＋Ｔ）を復号鍵により暗号化前の付加情報Ａ＋Ｔに復号する。そして、時間情報判定部２９は、この情報Ａ＋Ｔに含まれる時間情報Ｔに基づいて情報の有効性を判断する（ステップＳ１６）。尚、この第１の実施の形態に係る情報処理システム及び方法では、時間情報判定部２９は、復号部２８による復号のタイミング（時間）が時間情報Ｔに係る時間よりも先であれば当該情報が有効なものと判断する。但し、判断の手法は、これに限定されないことは勿論である。

【００７２】こうして、時間情報判定部２９が情報が有効なものであると判断すると、情報読取部３０は、カード番号情報Ａを送受信部３１を介して信販会社のサーバ３に送信する（ステップＳ１７）。サーバ３では、送受信部３２がカード番号情報Ａを受信し、課金処理部３３にて所定の課金処理がなされる（ステップＳ１８）。この課金処理については、公知の技術を採用することができるので、詳細な説明は省略する。以上で、決済処理に係る一連の処理を終了する。

【００７３】ここで、サービス提供者のサーバ２内のユーザ情報蓄積ＤＢ１８の記憶内容は図５に示される。図５に示されるように、同ＤＢ１０３には、利用者の携帯電話番号とＰＷ、複数のカード１、２，３…のカード番号情報及びポイント等が関連付けられて記憶されている。このカード番号情報に係る入力に基づき、図４（ｂ）で先に示したカード選択画面１０１の表示態様は、変更される。即ち、例えば図６に示されるようにカード番号情報が入力された場合には、同図の如くカード選択領域１０４ａに「ＡＡＡＡ」、「ＢＢＢＢ」、「ＣＣＣＣ」が表示されたカード選択画面１０４となる。このようなカスタマイズは、利用者が携帯電話機１とサーバ２との通信を行い、予め設定することになる。尚、サービス提供者のサーバ２により利用者の携帯電話機１からの要求に応じてカスタマイズされる画面は上記カード選択画面１０１に限られるものではなく、種々のサービスに係る選択画面を提供することができることは勿論である。この場合、サービス提供者は、当該選択に係る情報をユーザ情報蓄積ＤＢ１８に適宜蓄積することになる。

【００７４】以上説明したように、本発明の第１の実施の形態に係る情報処理システム及び方法では、携帯電話機１からインターネット等のネットワーク４を介してサービス提供者のサーバ２に送信されるのは、利用者の携帯電話番号等に係る情報のみであり、カード番号情報はそのままの態様でやりとりされることはなく、暗号化され更に２次元データに変換された態様でのみサーバ２から携帯電話機１に送信されるに過ぎないので、カード番

号情報の秘匿性が保持される。また、カード番号情報に時間情報が付加された後に暗号化（ワンタイム化）、更には２次元データ化されていることから、再利用可能な特質を有するカード番号情報を再利用不可能な態様で通信し、保持することができることから、セキュリティがより向上される。即ち、２次元データは、ＯＴＣＮ（One Time Card Number）とされていることから、不正コピーも防止され、偽バーコードの生成も不可能とされることになる。さらに、加盟店においては、従来から備えているＰＯＳレジスタ等の情報読取装置８にバーコードリーダ６及び変換器７を付加するだけで本サービスを行うことが可能となることから、既存のインフラを継続して使用することも可能であり、設備投資負担も軽減され、幅広い分野の店舗等がサービスに加入することが予想される。そして、利用者にすれば、複数のクレジットカード等を携帯する必要がなくなり、携帯電話機のみで複数のクレジットカード等によるサービスを享受できるようになることから、利便性、利用率も高まる。

【００７５】次に、前述した特徴点をふまえつつ、本発明の第２の実施の形態に係る情報処理システム及び情報処理方法について更に詳細に説明する。

【００７６】先ず、図７には第２の実施の形態に係る情報処理システムの構成を示し説明する。図７に示されるように、この情報処理システムは、サービスの利用者の携帯電話機５１、サービス提供者のサーバ５２、店舗等の加盟店の無線通信装置５３及び情報読取装置８、信販会社のサーバ３からなる。ここでは、図１及び図２と同一構成については同一構成を付しているが、無線通信装置５３は、図１（ｂ）における無線通信部９に相当する構成要素である。

【００７７】以下、これら各構成要素について更に詳細に説明する。

【００７８】先ず、利用者の携帯電話機５１は、制御部１５とＩＤ／ＰＷ入力部１１、サービス選択部１２、データ蓄積部４０、近距離データ通信部４１、そして近距離データ通信指示部４２が通信自在に接続され、構成されている。

【００７９】このような構成において、制御部１５は、全体の制御を司るものであり、ＣＰＵ等からなる。ＩＤ／ＰＷ入力部１１は利用者が自己のＩＤやＰＷ等を入力するためのものであり、サービス選択部１２は利用者が所望とするサービスを選択枝の中から選択するためのものである。このＩＤ／ＰＷ入力部１１及びサービス選択部１２としては、例えば操作キー等を採用することができる。データ蓄積部４０は、サービス提供者のサーバ２から送信された暗号情報等を蓄積するものであり、メモリ等からなる。近距離データ通信部４１は、加盟店の無線通信装置５３内の近距離データ通信部４３との間で無線通信を行うものであり、例えばBluetooth、IrDA、RFID等からなる。近距離データ通信指示部４２は、上記近距離データ通信部４１による通信を指示するためのものである。尚、ここでは、携帯電話機１を例に挙げているが、これに限定されずＰＤＡ(Personal Digital Assistant)、ノートパソコン等を採用することもできることは勿論である。

【００８０】一方、サービス提供者のサーバ５２は、送受信部１７とユーザ情報蓄積ＤＢ１８、認証部２０、サービス選択部２１、時間情報付加部２２、暗号化部２３等を有している。そして、これら認証部２０、サービス選択部２１、時間情報付加部２２、暗号化部２３は、全て制御部１９に含まれている。

【００８１】このような構成において、上記送受信部１７は、利用者の携帯電話機５１等との通信を行うためのものである。ユーザ情報蓄積ＤＢ１８は、利用者のＩＤやＰＷ、携帯電話番号、更にはこれらに対応したカード番号等を蓄積するためのデータベースである（図５参照）。そして、認証部２０は、利用者について所定の認証を行うためのものである。サービス選択部２１は、携帯電話機１のサービス選択部１２により入力された情報に基づき、利用者のカード番号情報Ａをユーザ情報蓄積ＤＢ１８より読み出すためのものである。時間情報付加部２２は、上記情報Ａに時間情報Ｔを付加するためのものである。そして、暗号化部２３は、例えば公開鍵方式等により上記時間情報Ｔが付加された後の情報Ａ＋Ｔを、暗号鍵により暗号化して、暗号情報（Ａ＋Ｔ）を生成するものである。

【００８２】一方、加盟店の無線通信装置５３は、近距離データ通信部４３、復号化部２８、時間情報判定部２９からなる。情報読取装置８は、情報読取部３０と送受信部３１を有している。尚、この情報読取装置８としては、ＰＯＳ端末等を採用することができるが、これに限定されないことは勿論である。

【００８３】このような構成において、近距離データ通信部４３は、携帯電話機５１の近距離データ通信部４１との間で無線通信を行うためのものであり、例えばBluetooth、IrDA、RFID等からなる。復号化部２８は暗号情報（Ａ＋Ｔ）を復号鍵により暗号化前の情報に復号するためのものである。そして、時間情報判定部２９は、この暗号化前の情報より時間情報を読み出し、当該情報が有効であるか否かを判定するためのものである。情報読取部３０は、暗号化前の情報よりカード番号情報Ａを抽出するためのものである。そして、送受信部３１は、当該カード番号情報Ａを信販会社のサーバ３に送信するためのものである。

【００８４】また、信販会社のサーバ３は、決済システムとしての機能も備えたものであって、送受信部３２と課金処理部３３とで構成されている。

【００８５】このサーバ３としては、公知の技術を採用することができるので、詳細な説明は省略するが、送受信部３２は加盟店の情報読取装置８から送信されたカー

ド番号情報Ａを受信するためのものである。課金処理部３３は、このカード番号情報Ａに基づいて利用者に対する課金処理を行うためのものである。

【００８６】以下、図８のフローチャートを参照して、上述したような構成の第２の実施の形態に係る情報処理システムによる処理を詳細に説明する。尚、この処理は、本発明の第２の実施の形態に係る情報処理方法にも相当するものである。

【００８７】利用者により、携帯電話機５１のＩＤ／ＰＷ入力部１１やサービス選択部１２が操作され、サービス提供者のＷｅｂサイトのＵＲＬが入力されると、携帯電話機５１は、制御部１５による制御の下、送受信部１６及びネットワーク４を介して、サービス提供者のサーバ５２にアクセスする（ステップＳ２１）。

【００８８】サービス提供者のサーバ５２は、この携帯電話機５１によるアクセスを送受信部１７にて受信すると、制御部１９による制御の下、ＰＷ入力画面に係るファイルを不図示のＤＢより読み出し、送受信部１７及びネットワーク４を介して、携帯電話機５１に送信することになる（ステップＳ２２）。

【００８９】こうして、携帯電話機５１は、送受信部１６にてＰＷ入力画面に係るファイルを受信すると、制御部１５による制御の下、不図示の表示部においてＰＷ入力画面（図４（ａ）で前述）を表示する（ステップＳ２３）。

【００９０】続いて、利用者によりＩＤ／ＰＷ入力部１１が操作され、ＰＷ入力領域１００ａにパスワードが入力され、送信ボタン１００ｂが選択されると、携帯電話機５１は、制御部１５による制御の下、ＰＷ情報を、送受信部１６及びネットワーク４を介して、サービス提供者のサーバ５２に送信する（ステップＳ２４）。

【００９１】サービス提供者のサーバ５２は、送受信部１７がＰＷ情報を受信すると、認証部２０が当該ＰＷ情報に基づく所定の認証処理を行い（ステップＳ２５）、この認証が成立するものと判断した場合には、カード選択画面に係るファイルを不図示のＤＢより読み出し、制御部１９による制御の下、送受信部１７及びネットワーク４を介して、携帯電話機５１に送信することになる（ステップＳ２６）。

【００９２】こうして、携帯電話機１では、送受信部１６がカード選択画面に係るファイルを受信すると、制御部１５による制御の下、不図示の表示部においてカード選択画面（図４（ｂ）で前述）を表示することになる（ステップＳ２７）。

【００９３】続いて、利用者によりＩＤ／ＰＷ入力部１１が操作され、カード選択領域１０１ａにて所望とするカードが選択され、送信ボタン１０１ｂが選択されると、携帯電話機５１は、制御部１５による制御の下、利用者情報を、送受信部１６及びネットワーク４を介してサービス提供者のサーバ５２に送信する（ステップＳ２８）。そして、サービス利用者のサーバ５２は、送受信部１７が利用者情報を受信すると、ユーザ情報蓄積ＤＢ１８より当該利用者情報に対応するカード番号情報Ａを読み出す。尚、ユーザ情報蓄積ＤＢ１８を有していない場合には、以下の手法を採る。即ち、サーバ５２は、専用線５を介して信販会社のサーバ３に利用者情報を送信する（ステップＳ２９）。そして、サーバ３は、この利用者情報を受信すると、当該利用者情報に対応するカード番号情報Ａを読み出し、専用線５を介してサーバ５２側に返信する（ステップＳ３０）。このいずれの手法によっても利用者情報に対応したカード番号情報Ａが取得されることになる。

【００９４】続いて、サービス提供者のサーバ５２では、時間情報付加部２２が上記カード番号情報Ａに時間情報Ｔを付加し付加情報Ａ＋Ｔを生成し、暗号化部２３が公開鍵方式等により上記付加情報Ａ＋Ｔを暗号鍵により暗号化して暗号情報（Ａ＋Ｔ）を生成する（ステップＳ３１）。そして、サーバ５２は、制御部１９による制御の下で、この暗号情報Ａ＋Ｔを、送受信部１７及びネットワーク４を介して、利用者の携帯電話機５１に送信することになる（ステップＳ３２）。そして、携帯電話機５１では、この暗号情報Ａ＋Ｔを送受信部１６が受信すると、データ蓄積部４０に当該暗号情報（Ａ＋Ｔ）を蓄積する。尚、このとき、不図示の表示部に「カード情報を受信しました。」との確認表示をしてもよい（ステップＳ３３）。続いて、制御部１５が当該暗号情報（Ａ＋Ｔ）を読み出し、近距離データ通信指示部４２の指示に基づき近距離データ通信部４１が当該暗号情報（Ａ＋Ｔ）を加盟店の情報読取装置５２に無線で送信する（ステップＳ３４，Ｓ３５）。

【００９５】加盟店の情報読取装置５３の近距離データ通信部４３は、この暗号情報（Ａ＋Ｔ）を受信し、更に復号部２８は当該暗号情報（Ａ＋Ｔ）を復号鍵により暗号化前の付加情報Ａ＋Ｔに復号する。そして、時間情報判定部２９は、この情報Ａ＋Ｔに含まれる時間情報Ｔに基づいて情報の有効性を判断する（ステップＳ３６）。

【００９６】尚、この第２の実施の形態に係る情報処理システム及び方法では、時間情報判定部２９では、復号部２８により暗号情報Ａ＋Ｔを復号した時間が時間情報Ｔに係る時間よりも先であれば当該情報が有効なものと判断している。但し、有効性判断の手法は、これに限定されるものではないことは勿論である。

【００９７】こうして、情報の有効性が確認されると、情報読取部３０がカード番号情報Ａを送受信部３１を介して信販会社のサーバ３に送信する（ステップＳ３７）。サーバ３では、送受信部３２がカード番号情報Ａを受信し、課金処理部３３にて所定の情報処理、例えば課金処理等を行う（ステップＳ３８）。

【００９８】尚、この課金処理については、公知の技術を採用することができるので、ここでは詳細な説明は省

略する。

【００９９】ここで、サービス提供者のサーバ５２内のユーザ情報蓄積ＤＢ１８の記憶内容は、先に図５に示した通りであり、これについての詳細は前述した通りであるので、ここでは重複した説明は省略する。

【０１００】以上説明したように、本発明の第２の実施の形態に係る情報処理システム及び情報処理方法では、携帯電話機５１からインターネット等のネットワーク４を介してサービス提供者のサーバ５２に送信されるのは、利用者の携帯電話番号等に係る情報のみであり、カード番号情報はそのままの態様でやりとりされることはなく、暗号化された態様でのみサーバ５２から携帯電話機５１に送信されるに過ぎないので、カード番号情報の秘匿性が保持される。また、カード番号情報に時間情報が付加された後に暗号化されていることから、再利用可能な特質を有するカード番号情報を再利用不可能な態様で通信、保持することができセキュリティがより向上される。即ち、暗号情報は、ＯＴＣＮ（One Time Card Number）とされていることから、不正コピーも防止され、偽バーコードの生成も不可能とされることになる。さらに、加盟店においては、従来から備えているＰＯＳレジスタ等の情報読取装置８に無線通信装置５３を付加するだけで本サービスを行うことが可能となることから、既存のインフラが可能であり、設備投資負担も軽減され、幅広い分野の店舗等がサービスに加入することが予想される。

【０１０１】そして、利用者にすれば、複数のクレジットカード等を携帯する必要がなくなり、携帯電話機のみで複数のクレジットカード等によるサービスを享受できるようになることから、利便性、利用率も高まることとなる。

【０１０２】次に、前述した特徴点をふまえつつ、本発明の第３の実施の形態に係る情報処理システム及び情報処理方法について更に詳細に説明する。

【０１０３】第３の実施の形態に係る情報処理システムは、先に示した図２の構成において時間情報付加部２２を構成上省略し、サービス提供者のサーバ２から利用者情報が信販会社等のサーバ３に送信され、その応答としてカード番号情報を当該サーバ２に返信した際に、発行時間をサーバ３が別途保持し、加盟店からの要求に応じて、適宜、情報の有効性判断をサーバ３が行うようにしたものである。

【０１０４】このように、第３の実施の形態は、図２の構成と略同一であることから、これらと同一構成については同一符号をもって説明を進める。尚、第３の実施の形態は、図７と同様の構成によっても実現されることは勿論である。

【０１０５】以下、図９のフローチャートを参照して、第３の実施の形態に係る情報処理システムによる処理を詳細に説明する。尚、この処理は、本発明の第３の実施の形態に係る情報処理方法にも相当するものである。

【０１０６】この情報処理システムによる一連の処理が開始されると、先ず、利用者により携帯電話機１のＩＤ／ＰＷ入力部１１やサービス選択部１２が操作され、サービス提供者のＷｅｂサイトのＵＲＬが入力されると、携帯電話機１は、制御部１５による制御の下、送受信部１６及びネットワーク４を介して、サービス提供者のサーバ２（上記ＵＲＬ）にアクセスを行うことになる（ステップＳ５１）。

【０１０７】サービス提供者のサーバ２は、この携帯電話機１からのアクセスを送受信部１７を介して受けると、制御部１９による制御の下、ＰＷ入力画面に係るファイルを不図示のＤＢより読み出し、送受信部１７及びネットワーク４を介して、携帯電話機１に送信する（ステップＳ５２）。携帯電話機１は、送受信部１６にてＰＷ入力画面に係るファイルを受信すると、制御部１５による制御の下、２次元データ表示部１４においてＰＷ入力画面を表示する（ステップＳ５３）。

【０１０８】このＰＷ入力画面の様子は、先に図４（ａ）に示した通りである。

【０１０９】こうして、利用者により、ＩＤ／ＰＷ入力部１１が操作され、ＰＷ入力領域１００ａにＰＷが入力され、送信ボタン１００ｂが選択されると、この携帯電話機１は、制御部１５による制御の下、ＰＷ情報を、送受信部１６及びネットワーク４を介して、サービス提供者のサーバ２に送信する（ステップＳ５４）。

【０１１０】サービス提供者のサーバ２は、送受信部１７がＰＷ情報を受信すると、認証部２０が当該ＰＷ情報に基づく所定の認証処理を行い（ステップＳ５５）、この認証が成立すると判断した場合には、続いて、カード選択画面に係るファイルを不図示のＤＢより読み出して、制御部１９による制御の下、送受信部１７及びネットワーク４を介して、携帯電話機１に送信する（ステップＳ５６）。

【０１１１】こうして、携帯電話機１では、送受信部１６が上記サーバ２からのカード選択画面に係るファイルを受信すると、制御部１５による制御の下、２次元データ表示部１４においてカード選択画面を表示する（ステップＳ５７）。

【０１１２】このカード選択画面の様子は、先に図４（ｂ）に示した通りである。

【０１１３】続いて、利用者によりＩＤ／ＰＷ入力部１１が操作され、カード選択領域１０１ａにて所望とするカードが選択され、送信ボタン１０１ｂが選択されると、携帯電話機１は、制御部１５による制御の下、カード選択に係る情報（以下、利用者情報と称する）を、送受信部１６及びネットワーク４を介してサービス提供者のサーバ２に送信することになる（ステップＳ５８）。

【０１１４】そして、サービス提供者のサーバ２は、送受信部１７が利用者情報を受信すると、サーバ２は、専

用線５を介して信販会社のサーバ３に利用者情報を送信する（ステップＳ５９）。すると、サーバ３は、利用者情報に対応するカード番号情報Ａを読み出し、専用線５を介してサーバ２側に返信する（ステップＳ６０）。このとき、信販会社等のサーバ３は、サーバ２にカード番号情報を返信した時間（以下、発行時間と称する）を記録又は記憶する（ステップＳ６２）。

【０１１５】続いて、サービス提供者のサーバ２では、暗号化部２３が公開鍵方式等により上記カード番号情報Ａを暗号鍵により暗号化して暗号情報（Ａ）を生成する。そして、２次元データ化部２４が、上記暗号情報（Ａ）を更に２次元データ[Ａ]に変換し、２次元データ蓄積部２５が、この２次元データ[Ａ]を蓄積する（ステップＳ６１）。こうして、サーバ２は、制御部１９による制御の下、この生成された２次元データ[Ａ]を、送受信部１７及びネットワーク４を介して、利用者の携帯電話機１に送信する（ステップＳ６３）。

【０１１６】そして、携帯電話機１は、２次元データ[Ａ]を送受信部１６が受信すると、２次元データ蓄積部１３に２次元データ[Ａ]を蓄積する。そして、携帯電話機１では、制御部１５が、２次元データ[Ａ]を読み出し、２次元データ表示部１４に２次元データ表示画面を表示することになる（ステップＳ６４）。

【０１１７】尚、この２次元データ表示画面は、先に図４（ｃ）に示した通りである。

【０１１８】こうして、利用者が店舗等の加盟店に出向き、当該加盟店において携帯電話機１を提示すると（ステップＳ６５）、加盟店の２次元情報読取装置５４の２次元データ読取部２６は、携帯電話機１の２次元データ表示部１４に表示された２次元データ[Ａ]を読み取る（ステップＳ６６）。２次元データ解析部２７は、この２次元データ[Ａ]を暗号情報（Ａ）に変換し、更に復号部２８は当該暗号情報（Ａ）を復号鍵により暗号化前のカード番号情報Ａに復号する（ステップＳ６７）。

【０１１９】次いで、加盟店の情報読取装置８は、信販会社等のサーバ３に上記カード番号情報Ａの有効性判断を依頼する（ステップＳ６８）。

【０１２０】この依頼を受けた信販会社等のサーバ３は、先にステップＳ６２で記録又は記憶した発行時間に係る情報に基づいて、カード番号情報Ａの有効性を判断することになる（ステップＳ６９）。ここでは、例えば発行時間から所定時間経過している場合には当該情報を無効とし、発行時間経過前であれば有効とするといった判断を行うことになるが、その手法はこれに限定されるものではない。

【０１２１】尚、上記「発行時間」とは、発行時刻を示す場合と許容経過時間そのものを示す場合の双方が含まれる広い概念であることは勿論である。

【０１２２】こうして、サーバ３がカード番号情報Ａが有効であると判断した場合には、当該サーバ３は通常のカード処理依頼（オーソリゼーション）用の選択情報を加盟店の情報読取装置８側に送信し（ステップＳ７０）、以降、サーバ３の課金処理部３３にて所定の情報処理、例えば課金処理等がなされる（ステップＳ７１）。この課金処理については、公知の技術を採用することができるので、詳細な説明は省略する。以上で、決済処理に係る一連の処理を終了する。

【０１２３】以上説明したように、本発明の第３の実施の形態に係る情報処理システム及び情報処理方法では、携帯電話機５１からインターネット等のネットワーク４を介してサービス提供者のサーバ５２に送信されるのは、利用者の携帯電話番号等に係る情報のみであり、カード番号情報はそのままの態様でやりとりされることはなく、暗号化された態様でのみサーバ５２から携帯電話機５１に送信されるに過ぎないので、カード番号情報の秘匿性が保持される。また、カード番号情報を発行した時間を信販会社等のサーバ３が保持しており、適宜、加盟店の情報読取装置８からの要求に応じてカード番号情報の有効性を判断するので、再利用可能な特質を有するカード番号情報を再利用不可能な態様で通信、保持することができセキュリティがより向上される。さらに、加盟店においては、従来から備えているＰＯＳレジスタ等の情報読取装置８に簡易な構成ををを付加するだけで本サービスを行うことが可能となることから、既存のインフラが可能であり、設備投資負担も軽減され、幅広い分野の店舗等がサービスに加入することが予想される。

【０１２４】そして、利用者にすれば、複数のクレジットカード等を携帯する必要がなくなり、携帯電話機のみで複数のクレジットカード等によるサービスを享受できるようになることから、利便性、利用率も高まることとなる。

【０１２５】次に、本発明の第４の実施の形態について説明する。

【０１２６】図１１，１２には、本発明の第４の実施の形態に係る情報処理システムの構成を示し説明する。先ず、図１１に示されるように、サーバ３００は、ユーザ情報蓄積ＤＢ３０１、認証部３０２、サービス選択部３０３、共通キーＫ１蓄積部３０４、第１演算部３０５、第２共通キーＫ２生成部３０６、暗号化部３０７、バーコード生成部３０８、そして送受信部３０９からなる。ユーザ情報蓄積ＤＢ３０１は、利用者のＩＤやＰＷ、携帯電話番号、これらに対応したカード番号、更にはＰＩＮコードＰ等を蓄積するためのものである。第４の実施の形態では、これら各種情報は、利用者により事前に登録されているものとする。ここで、ＰＩＮコードとは、個人認証用の数字及び文字列である所謂暗証番号を意味している。

【０１２７】一方、図１１、図１２に示されるように、利用者の携帯電話機４００は、ＣＰＵ等からなる携帯電話機４００全体の制御を司る制御部４０６、ＩＤ／ＰＷ

入力部４０２、サービス選択部４０３、２次元データ蓄積部４０４、液晶表示ユニット等の２次元データ表示部４０５、そして送受信部４０１からなる。

【０１２８】尚、第４の実施の形態では、携帯電話機１を例に挙げているが、これに限定されることなく、例えばＰＤＡやノート型パーソナルコンピュータ等の携帯端末を採用することもできることは勿論である。

【０１２９】さらに、図１２に示されるように、加盟店の２次元情報読取装置５００は、２次元データ読取部５０１、２次元データ解析部５０２、復号化部５０３、逆演算部５０７、認証部５０８、共通キー蓄積部５０４、ＰＩＮ入力部５０５、第２共通キー生成部５０６からなる。加盟店の情報読取装置６００は情報読取部６０１と送受信部６０２からなり、サーバ７００は課金処理部７０１と送受信部７０２からなる。情報読取装置６００には、ＰＯＳ端末等を採用できる。サーバ７００は、決済システムとしての機能も備えたものであり、公知の技術を採用することができるので、詳細な説明は省略する。

【０１３０】そして、図１１に示されるように、サーバ３００と携帯電話機４００とは、それぞれの送受信部３０９，４０１を介して通信自在に構成されている。更に、図１２に示されるように、携帯電話機４００と２次元情報読取装置は通信自在に構成されており、２次元情報読取装置５００と情報読取装置６００、サーバ７００は通信自在に構成されている。

【０１３１】以下、図１１、図１２を参照しつつ、この第４の実施の形態に係る情報処理システムによる特徴のある動作について詳細に説明する。

【０１３２】この情報処理システムによる一連の処理が開始されると、利用者により携帯電話機４００のＩＤ／ＰＷ入力部４０２やサービス選択部４０３が操作され、サービス提供者のＷｅｂサイトのＵＲＬが入力されると、携帯電話機４００は、制御部４０６による制御の下、送受信部４０１及びネットワークを介して、サービス提供者のサーバ３００（上記ＵＲＬ）にアクセスを行う。

【０１３３】このサービス提供者のサーバ３００は、この携帯電話機４００からのアクセスを送受信部３０９を介して受けると、不図示の制御部による制御の下、ＰＷ入力画面に係るファイルを不図示のＤＢより読み出し、送受信部３０９及びネットワークを介して、携帯電話機４００に送信する。携帯電話機４００は、送受信部４０１にてＰＷ入力画面に係るファイルを受信すると、制御部４０６による制御の下、２次元データ表示部４０５においてＰＷ入力画面を表示する。このＰＷ入力画面の様子は、例えば先に図４（ａ）に示した通りである。こうして、利用者により、ＩＤ／ＰＷ入力部４０２が操作され、ＰＷが入力されると、この携帯電話機４００は、制御部４０６による制御の下、ＰＷ情報を、送受信部４０１及びネットワークを介して、サービス提供者のサーバ３００に送信する。

【０１３４】このサービス提供者のサーバ３００は、送受信部３０９がＰＷ情報を受信すると、認証部３０２が当該ＰＷ情報に基づく所定の認証処理を行い、この認証が成立すると判断した場合には、続いて、カード選択画面に係るファイルを不図示のＤＢより読み出して、不図示の制御部による制御の下、送受信部３０９及びネットワークを介して、携帯電話機４００に送信する。

【０１３５】こうして、携帯電話機４００では、送受信部４０１が上記サーバ３００からのカード選択画面に係るファイルを受信すると、制御部４０６による制御の下、２次元データ表示部４０５においてカード選択画面を表示する。このカード選択画面の様子は、例えば先に図４（ｂ）に示した通りである。

【０１３６】続いて、利用者によりＩＤ／ＰＷ入力部４０２が操作され、所望とするカードが選択されると、携帯電話機４００は、制御部４０６による制御の下、選択情報を、送受信部４０１及びネットワークを介してサービス提供者のサーバ３００に送信することになる。サービス提供者のサーバ３００は、送受信部３０９が選択情報を受信すると、サービス選択部３０３がユーザ情報蓄積ＤＢ３０１より当該利用者情報に対応するカード番号情報Ａを読み出す。尚、サーバ３００がユーザ情報蓄積ＤＢ３０１を有していない場合には、専用線を介して信販会社のサーバに利用者情報を送信し、当該信販会社のサーバから送られる、利用者情報に対応するカード番号情報Ａを、専用線を介して受信する。

【０１３７】続いて、サービス提供者のサーバ３００では、共通キーＫ１蓄積部３０４に予め蓄積されている共通キーＫ１とユーザ情報蓄積ＤＢ３０１内のＰＩＮコードＰとに基づいて、第２共通キー生成部３０６にて共通キーＫ２を生成する。このＰＩＮコードＰは、請求項記載の第１暗証コードの一例に相当する。

【０１３８】第１演算部３０５は、カード番号情報ＡとＰＩＮコードＰとに基づいて、新たなデータＡ１を生成する。このデータＡ１は、請求項記載の付加情報の一例に相当する。この演算は、可逆的な演算であれば、種々の方法を採用するこができることは勿論である。暗号化部３０７では、上記データＡ１を共通キーＫ２を用いて暗号化し、暗号化データＡ２を生成する。この共通キーＫ２は、請求項記載の第２共通鍵情報の一例に相当する。また、暗号化データＡ２は、請求項記載の暗号情報の一例に相当する。バーコード生成部３０８では、この生成された暗号化データＡ２を２次元バーコード化し、２次元データＡ３を生成して、送受信部３０９を介して携帯電話機４００に送信することになる。

【０１３９】携帯電話機４００は、２次元データＡ３を送受信部４０１にて受信すると、２次元データ蓄積部４０４に当該２次元データＡ３を蓄積する。そして、制御部４０６が、当該２次元データＡ３を読み出し、２次元

データ表示部４０５に２次元データ表示画面を表示する。ここで、この２次元データ表示画面は、例えば先に図４（ｃ）に示した通りであるが、これには限定されない。

【０１４０】こうして、利用者が店舗等の加盟店に出向き、当該加盟店において携帯電話機４００を提示すると、加盟店の２次元情報読取装置５００の２次元データ読取部５０１は、携帯電話機４００の２次元データ表示部４０５に表示された２次元データＡ３を読み取る。２次元データ解析部５０２は、この２次元データＡ３を暗号化データＡ２に変換する。第２共通キー生成部５０６は、ＰＩＮ入力部５０５にて入力されたＰＩＮコードＰ’と共通キー蓄積部５０４に蓄積されている共通キーＫ１とに基づいて共通キーＫ２’を生成する。このＰＩＮコードＰ’は、請求項記載の第２暗証コードの一例に相当する。また、共通キーＫ２’は、請求項記載の第３暗証コードの一例に相当する。ここで、ＰＩＮ入力部５０５より入力されたＰＩＮコードＰ’が正しければ、Ｐ＝Ｐ’、Ｋ２＝Ｋ２’となる。

【０１４１】次いで、復号化部５０３は、暗号化データＡ２を共通キーＫ２’によりデータＡ１’に復号する。ここで、上記Ｐ＝Ｐ’であれば、Ａ１’＝Ａ１となる。

【０１４２】そして、逆演算部５０７にて、当該データＡ１’を逆演算してカード番号情報ＡとＰＩＮコードＰ”に分離抽出する。このＰＩＮコードＰ”は、請求項記載の第３暗証コードの一例に相当する。そして、認証部５０８では、所定の逆演算により生成されたＰ”とＰＩＮ入力部５０５にて入力されたＰ’とを比較し、両者が一致していれば、カード番号情報Ａを読み読取装置６００に送信することになる。そして、情報読取部６０１は、カード番号情報Ａを送受信部６０２を介して信販会社のサーバ７００に送信する。

【０１４３】サーバ７００では、送受信部７０２がカード番号情報Ａを受信し、課金処理部７０１にて所定の課金処理がなされる。この課金処理については、公知の技術を採用することができる。以上で、一連の処理を終了する。

【０１４４】以上説明した第４の実施の形態に係る情報処理システム及び方法では、ＰＩＮコードＰ’を共通キーＫ１の一部として新たな共通キーＫ２’を生成し、当該共通キーＫ２’で復号化する構成としたため、従来方式に比して高いセキュリティを実現することができる。更に、時間情報の要素がなくなるため、バーコード情報を携帯端末機４００内に蓄積しても使用可能となる。即ち、携帯電話機４００が圏外であっても利用可能な状況をつくれる。この場合、利用の度にサーバ３００と通信する必要がなくなるため、通信費用が低減される。

【０１４５】尚、この第４の実施の形態では、上記暗号化、復号化処理中の中間演算結果等は不図示の揮発性メモリ等に一時的に最小限の期間保存するものとし、演算終了後は速やかに消去している。更に、共通キーＫ１の不図示のデコーダユニットへの保存は、当該デコーダユニットが盗難等にあってメモリ解析されても、当該共通キーＫ１の記憶領域が見出せないような工夫がされている。また、ＰＩＮ入力部５０５からの入力は、人間が行う通常操作以上の速度で入力された場合には受け付けないものとし、不正アクセスを防止している。また、連続して所定回数以上のＰＩＮコードの入力エラーが起きた場合には、当該入力を所定期間受け付けないようにして、不正を防止している。

【０１４６】次に、本発明の第５の実施の形態について説明する。

【０１４７】図１３，１４には、本発明の第５の実施の形態に係る情報処理システムの構成を示し説明する。ここでは、先に説明した第４の実施の形態と同一構成ついては同一符号を付し、共通する構成、作用については重複した説明を省略し、特徴ある部分を中心に説明する。図１３に示されるように、サーバ３５０には、時間情報生成部３１０が組み込まれている点で、図１１のサーバ３００と構成上の相違がある。更に、図１４に示されるように、２次元情報読取装置５５０には、認証部５０８に代えて認証および時間情報判定部５０９が組み込まれている点で、図１２の２次元情報読取装置５００と構成上の相違がある。

【０１４８】以下、図１３，図１４を参照しつつ、この第５の実施の形態に係る情報処理システムによる特徴のある動作について詳細に説明する。

【０１４９】この第５の実施の形態では、次の点で第４の実施の形態と相違する。

【０１５０】即ち、図１３において、サービス提供者のサーバ３５０では、共通キーＫ１蓄積部３０４に予め蓄積されている共通キーＫ１とユーザ情報蓄積ＤＢ３０１内のＰＩＮコードＰとに基づいて、第２共通キー生成部３０６にて共通キーＫ２を生成する。そして、第１演算部３０５は、カード番号情報ＡとＰＩＮコードＰ、時間情報生成部位３１０が生成する時間情報Ｔとに基づいて、新たなデータＡ１を生成する。この時間情報Ｔは、請求項記載の第１時間情報の一例に相当する。このように、時間情報生成部位３１０が生成する時間情報Ｔを含めてデータＡ１を生成している点が第５の実施の形態と相違する。暗号化部３０７では、上記データＡ１を共通キーＫ２を用いて暗号化し、暗号化データＡ２を生成する。バーコード生成部３０８では、この生成された暗号化データＡ２を２次元バーコード化し、２次元データＡ３を生成して、送受信部３０９を介して、携帯電話機４００に送信する。これ以降は、第４の実施の形態と同様である。

【０１５１】一方、図１４において、逆演算部５０７にて、当該データＡ１を逆演算してカード番号情報ＡとＰＩＮコードＰ、時間情報Ｔ’に分離抽出する。この時間

情報Ｔ’は、請求項記載の第２時間情報に相当する。Ｐ＝Ｐ’である場合には、Ｔ＝Ｔ’となる。そして、認証および時間情報判定部５０９では、所定の逆演算により生成されたＰ”とＰＩＮ入力部５０５にて入力されたＰ’とを比較して両者が一致しているか否かを判断することで認証を行うと共に、この時間情報Ｔ’（Ｐ＝Ｐ’であれば、Ｔ’＝Ｔとなる）に基づいて情報の有効性を判断する。

【０１５２】即ち、この第５の実施の形態に係る情報処理システム及び方法では、認証および時間情報判定部５０９は、時間情報判定については、復号化部５０３による復号のタイミング（時間）が時間情報Ｔ’（＝Ｔ）に係る時間よりも先であれば当該情報が有効なものと判断する。或いは、認証および時間情報判定部５０９での判定のタイミング、つまり現在時刻が時間情報Ｔ’（＝Ｔ）を経過していなければ当該情報が有効なものと判断する。

【０１５３】但し、判断の手法は、これに限定されない。

【０１５４】以上説明したように、第５の実施の形態では、例えば抽出された時間情報Ｔを本サービスの有効期限や更新期限とする事で、従来方式よりも高いセキュリティを実現することができる。即ち、正規のＰＩＮコードが入力されれば、センタに問い合わせることなく、当該サービスの有効期限をチェックすることが可能となり、不正使用を効率的に防止することができる。また、二次元バーコードに埋め込む時間情報Ｔを２次元コード生成時刻の数分後（例えば１０分後）にしておくことで、携帯電話機４００を紛失し且つＰＩＮコードが見出されてしまった場合でも、時間経過により二次元バーコードの読み取りが不可能になることから、より高いセキュリティを実現できる。

【０１５５】尚、この発明には、以下の内容も含まれることは勿論である。

【０１５６】即ち、第１に、少なくともサーバ（３００）と情報読取装置（５００）が通信自在に接続された情報処理システムにおいて、上記サーバ（３００）は、利用者情報と秘匿情報、暗証コードを記憶している記憶手段（３０１）と、上記携帯端末からの利用者情報に対応する秘匿情報、第１暗証コードを上記記憶手段から読み出し、当該秘匿情報に第１暗証コードを付加して第１付加情報を生成する演算手段（３０５）と、上記予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵情報を生成する第２共通鍵情報生成手段（３０６）と、この第２共通鍵情報により上記第１付加情報を暗号化して暗号情報を生成する暗号化手段（３０７）と、この暗号化情報を携帯電話機（４００）に送信する送受信手段（３０９）と、を有し、上記情報読取装置（５００）は、第２暗証コードの入力を受け付ける第２暗証コード入力手段（５０５）と、この第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成する第３共通鍵情報生成手段（５０６）と、上記携帯端末（４００）からの暗号情報を上記第３共通鍵情報により復号して第２付加情報を生成する復号化手段（５０３）部と、この第２付加情報を逆演算して秘匿情報と第３暗証コードとに分離する逆演算手段（５０７）と、この第３暗証コードと上記第２暗証コードとを比較し、両者が一致する場合には上記秘匿情報が有効であるものと判断する認証手段（５０８）と、を有する、ことを特徴とする情報処理システム、である。

【０１５７】第２に、少なくともサーバ（３５０）と情報読取装置（５５０）が通信自在に接続された情報処理システムにおいて、上記サーバ（３５０）は、利用者情報と秘匿情報、暗証コードを記憶している記憶手段（３０１）と、上記携帯端末からの利用者情報に対応する秘匿情報、第１暗証コードを上記記憶手段から読み出し、当該秘匿情報に第１暗証コード及び第１時間情報を付加して第１付加情報を生成する演算手段（３０５）と、上記予め蓄積された第１共通鍵情報と上記第１暗証コードとに基づいて第２共通鍵情報を生成する第２共通鍵情報生成手段（３０６）と、この第２共通鍵情報により上記第１付加情報を暗号化して暗号情報を生成する暗号化手段（３０７）と、この暗号化情報を携帯電話機（４００）に送信する送受信手段（３０９）と、を有し、上記情報読取装置（５５０）は、第２暗証コードの入力を受け付ける第２暗証コード入力手段（５０５）と、この第２暗証コードと予め蓄積された第１共通鍵情報とに基づいて第３共通鍵情報を生成する第３共通鍵情報生成手段（５０６）と、上記携帯端末（４００）からの暗号情報を上記第３共通鍵情報により復号して第２付加情報を生成する復号化手段（５０３）部と、この第２付加情報を逆演算して秘匿情報と第３暗証コード、第２時間情報とに分離する逆演算手段（５０７）と、この第３暗証コードと上記第２暗証コードとの比較結果、及び上記第２時間情報とに基づいて、上記秘匿情報が有効であるか否かを判断する認証および時間情報判定手段（５０９）と、を有する、ことを特徴とする情報処理システム、である。

【０１５８】なお、上記第２の態様では、一例ではあるが、認証および時間情報判定手段（５０９）は、第３認証コードと第２認証コードとが一致し、且つ第２時間情報が現在時刻を越えていない場合に、秘匿情報が有効なものと判断する。

【０１５９】以上、本発明の実施の形態について説明したが、本発明はこれに限定されることなく、その趣旨を逸脱しない範囲で種々の改良・変更が可能であることは勿論である。例えば、上記第１乃至５の実施の形態では、暗号化の方式として公開鍵方式を採用することを前提としているが、暗号鍵、復号鍵のいずれを公開することとしてもよい。更に詳細には、ＲＳＡ暗号、エルガマ

ル暗号、だ円曲曲線暗号等、種々の方式を採用することが可能である。さらに、上記第１、２、５の実施の形態では、時間情報Ｔを付加することとしていたが、付加される情報は時間情報Ｔに限定されるものではなく、セキュリティを高める上で好適なものであれば、種々のものを採用できることは勿論である。また、上記第１乃至５の実施の形態では、カード番号情報を暗号化の対象、２次元データ化の対象としていたが、これらに限定されることなく、高い秘匿性が要求される「秘匿情報」たる種々の情報に適用可能であることは勿論である。

【０１６０】

【発明の効果】以上詳述したように本発明によれば、既存のシステムを大きく変更することなく、簡易な構成により、効果的な不正使用防止機能を実現することによって、セキュリティを向上させつつ、利用者が携帯電話をカードの代用として店舗等において利用可能とする等、利用者の利便性、更には利用者の個人情報の秘匿性を向上させた情報処理システム及び情報処理方法を提供することができる。

【図面の簡単な説明】

【図１】（ａ）は本発明の実施の形態に係る情報処理システムにおける携帯電話機１とサービス提供者のサーバ２、信販会社等のサーバ３の関係を示す図であり、（ｂ）は、本発明の実施の形態に係る情報処理システムにおける携帯電話機１と加盟店の情報読取装置８、信販会社等のサーバ３の関係を示す図である。

【図２】本発明の第１の実施の形態に係る情報処理システムの構成を示すブロック図である。

【図３】本発明の第１の実施の形態に係る情報処理システムによる処理の流れをデータフローと共に説明するためのフローチャートである。

【図４】（ａ）はＰＷ入力画面１００の様子を示し、（ｂ）はカード選択画面１０１の様子を示し、（ｃ）は２次元データ表示画面１０２の様子を示す図である。

【図５】ユーザ情報蓄積ＤＢ１８の記憶内容を示す図である。

【図６】カード選択画面１０１のカスタマイズを説明する為の図である。

【図７】本発明の第２の実施の形態に係る情報処理システムの構成を示すブロック図である。

【図８】本発明の第２の実施の形態に係る情報処理システムによる処理の流れをデータフローと共に説明するためのフローチャートである。

【図９】本発明の第３の実施の形態に係る情報処理システムによる処理の流れをデータフローと共に説明するためのフローチャートである。

【図１０】従来技術に係る情報処理システムの構成を示す図である。

【図１１】本発明の第４の実施の形態に係る情報処理システムの構成を示し説明する。

【図１２】本発明の第５の実施の形態に係る情報処理システムの構成を示し説明する。

【図１３】本発明の第５の実施の形態に係る情報処理システムの構成を示し説明する。

【図１４】本発明の第５の実施の形態に係る情報処理システムの構成を示し説明する。

【符号の説明】

１　携帯電話機
２　サーバ
３　サーバ
４　ネットワーク
５　専用線
６　バーコードリーダ
７　変換器
８　情報読取装置
９　無線通信部
１０　専用線
１１　ＩＤ／ＰＷ入力部
１２　サービス選択部
１３　２次元データ蓄積部
１４　２次元データ表示部
１５　制御部
１６　送受信部
１７　送受信部
１８　ユーザ情報蓄積ＤＢ
１９　制御部
２０　認証部
２１　サービス選択部
２２　時間情報付加部
２３　暗号化部
２４　２次元データ化部
２５　２次元データ蓄積部
２６　２次元データ読取部
２７　２次元データ解析部
２８　復号化部
２９　時間情報判定部
３０　情報読取部
３１　送受信部
３２　送受信部
３３　課金処理部
４０　データ蓄積部
４１　近距離データ通信部
４２　近距離データ通信指示部
４３　近距離データ通信部
５１　携帯電話機
５２　サーバ
５３　無線通信装置
５４　２次元情報読取装置

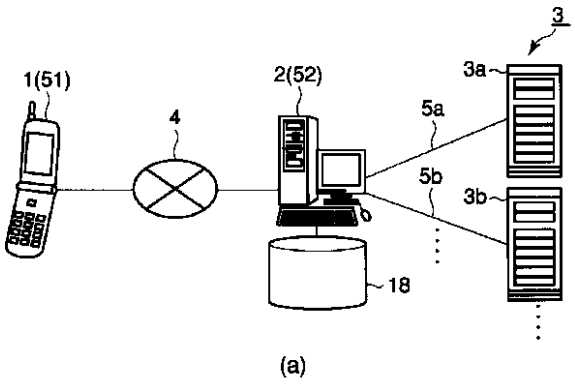
【要約】

【課題】既存のシステムを大きく変更することなく、簡

易な構成により、効果的な不正使用防止機能を実現することによって、セキュリティを向上させつつ、利用者が携帯電話をカードの代用として店舗等において利用可能とする等、利用者の利便性、更には利用者の個人情報の秘匿性を向上させることにある。

【解決手段】この発明の情報処理システムは、携帯電話機１からの利用者情報を受信し、当該利用者情報に対応＊するカード番号情報に時間情報を付加した後に暗号化して暗号情報を生成し上記携帯電話機１に返信するサーバ２と、上記携帯電話機１の暗号情報を得て当該暗号情報を復号化し、上記時間情報に基づいて上記カード番号情報の有効性を判断し、当該カード番号情報が有効であると判断した場合には所定の決済処理を進める情報読取装置８と、を有する。

【図１】

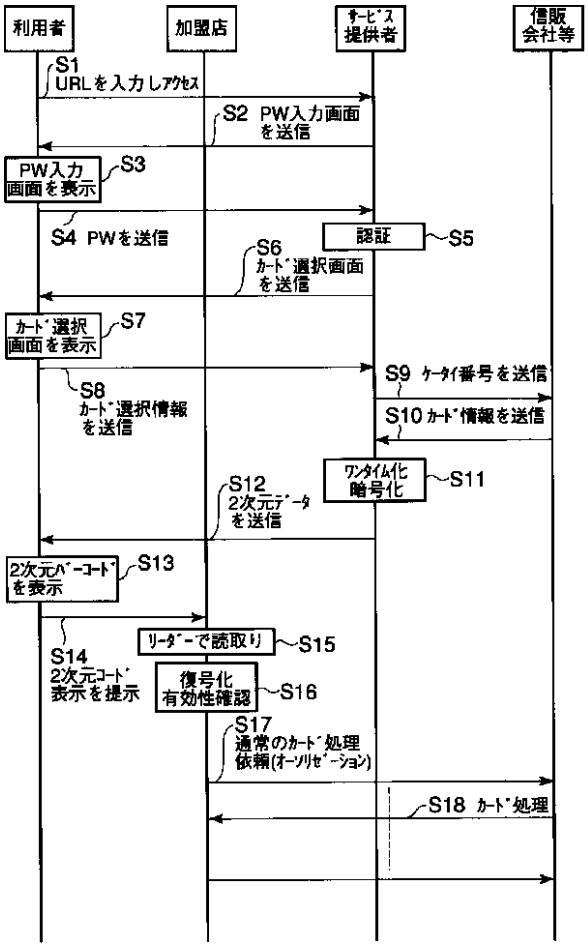


【図５】

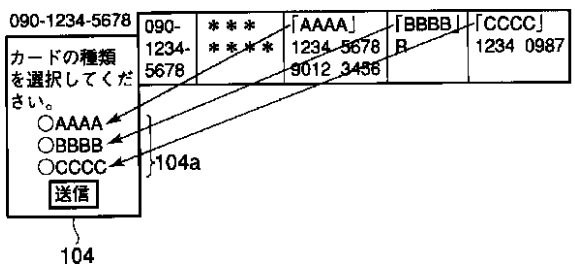
103

ケータイ	password	カード1	カード2	カード3	……
090-1234-5678	＊＊＊＊＊＊	「AAAA」 1234 5678 9012 3456 321点	「BBBB」 R	「CCCC」 1234 0987 21点	
090-9876-1234	＊＊＊＊＊＊＊＊	「DDDD」 R	「EEEE」 R	「FFFF」 1234 5678 9012 3456 123点	
⋮	⋮	⋮	⋮	⋮	⋮

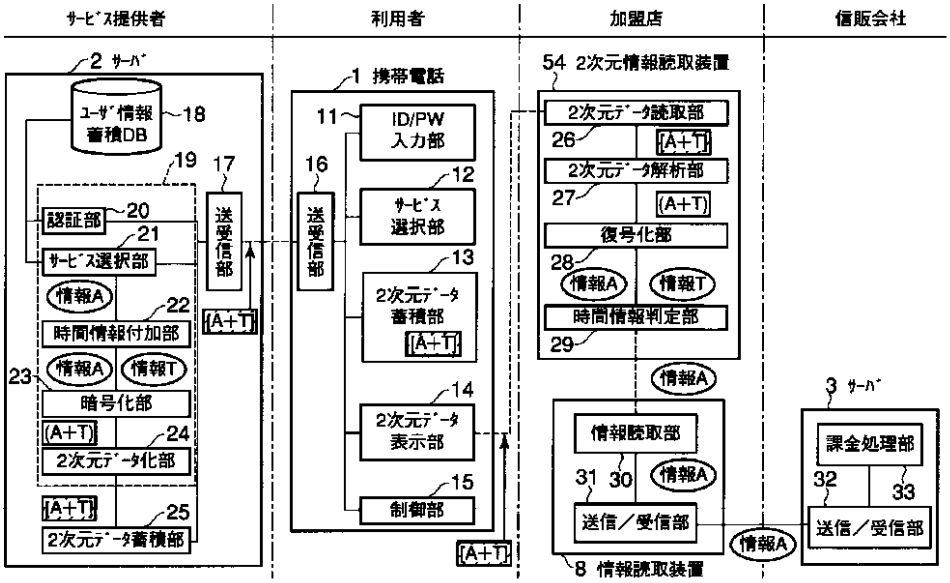
【図３】



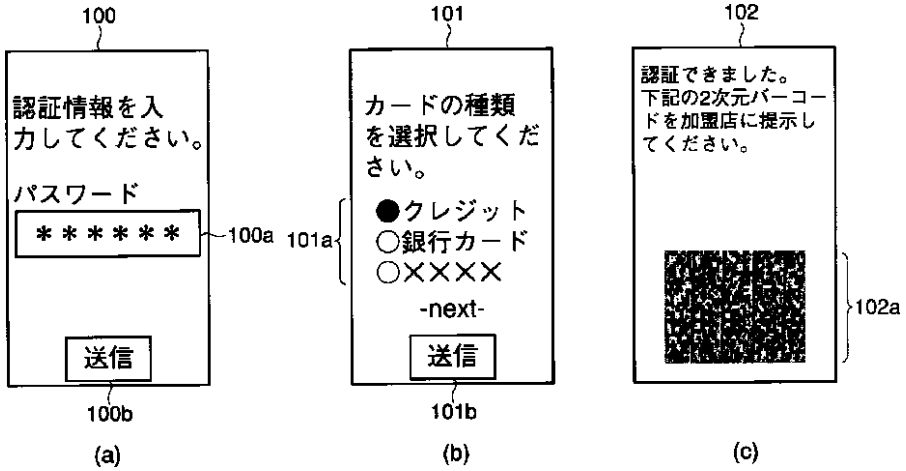
【図６】



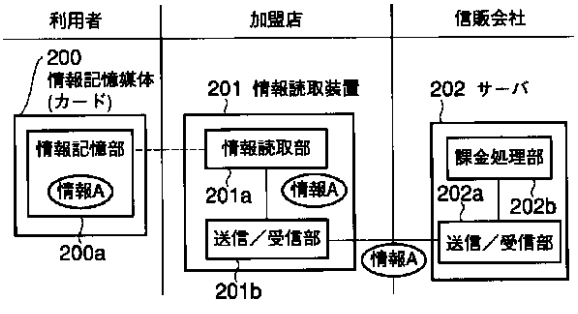
【図２】


ｻｰﾋﾞｽ提供者
利用者
加盟店
信販会社
2 ｻｰﾊﾞ
ﾕｰｻﾞ情報蓄積DB
18
19
17
認証部
20
ｻｰﾋﾞｽ選択部
21
情報A
22
時間情報付加部
23
情報A
情報T
暗号化部
(A+T)
24
2次元ﾃﾞｰﾀ化部
(A+T)
25
2次元ﾃﾞｰﾀ蓄積部
送受信部
(A+T)
1 携帯電話
11
ID/PW入力部
16
送受信部
12
ｻｰﾋﾞｽ選択部
13
2次元ﾃﾞｰﾀ蓄積部
(A+T)
14
2次元ﾃﾞｰﾀ表示部
15
制御部
(A+T)
54 2次元情報読取装置
2次元ﾃﾞｰﾀ読取部
26
(A+T)
2次元ﾃﾞｰﾀ解析部
27
(A+T)
復号化部
28
情報A
情報T
時間情報判定部
29
情報A
情報読取部
31
30
情報A
送信／受信部
8 情報読取装置
情報A
3 ｻｰﾊﾞ
課金処理部
32
33
送信／受信部

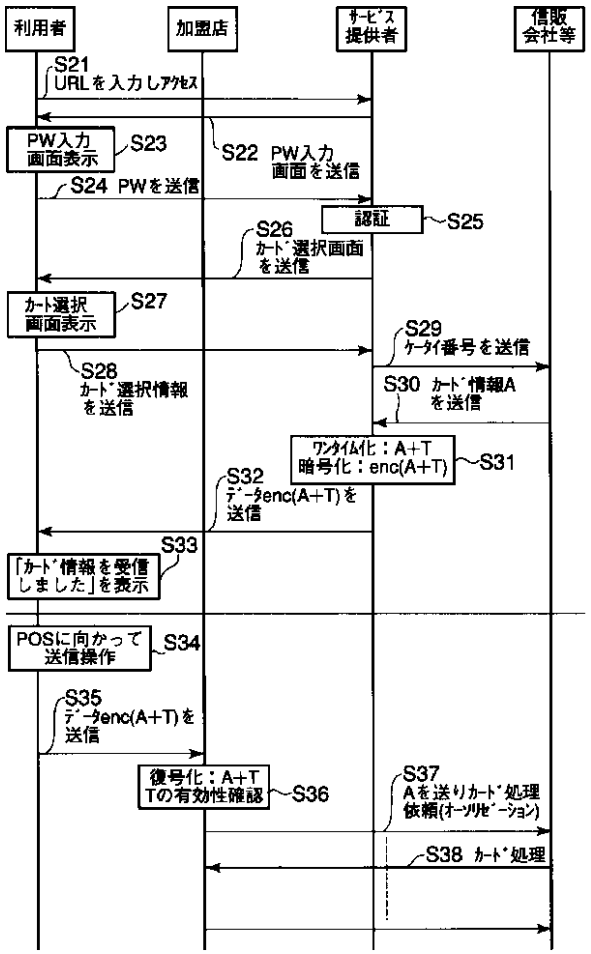
【図４】


100
認証情報を入力してください。
パスワード
＊＊＊＊＊＊
100a
送信
100b
(a)
101
カードの種類を選択してください。
●クレジット
○銀行カード
○××××
-next-
101a
送信
101b
(b)
102
認証できました。
下記の2次元バーコードを加盟店に提示してください。
102a
(c)

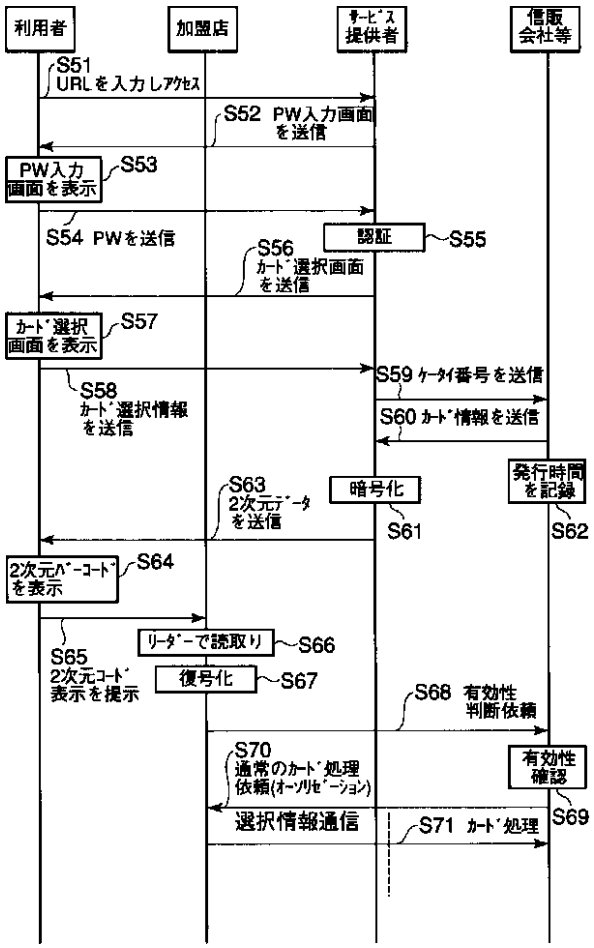
【図１０】


利用者
加盟店
信販会社
200
情報記憶媒体(カード)
情報記憶部
情報A
200a
201 情報読取装置
情報読取部
201a
情報A
送信／受信部
201b
情報A
202 サーバ
課金処理部
202a
202b
送信／受信部

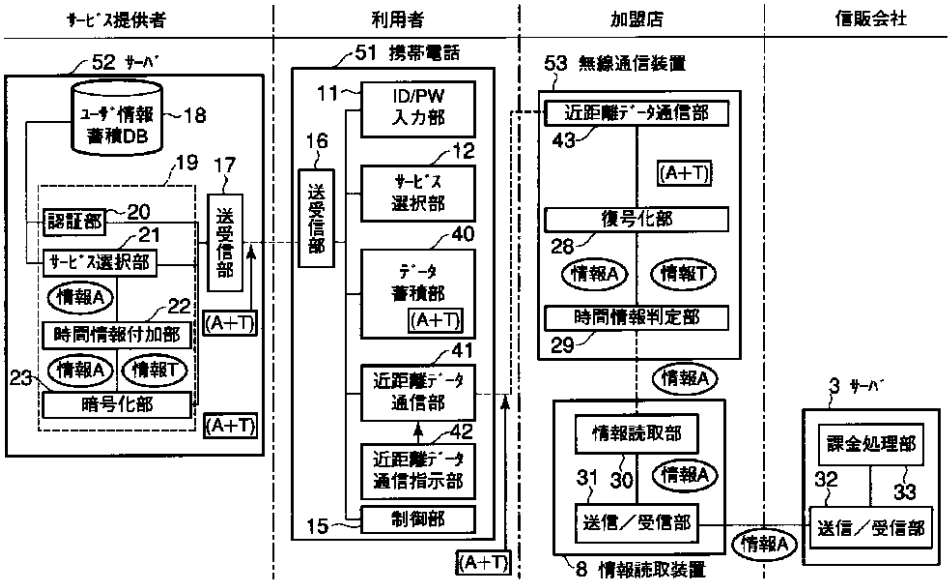
【図８】


利用者
加盟店
ｻｰﾋﾞｽ提供者
信販会社等
S21 URLを入力しｱｸｾｽ
S22 PW入力画面を送信
PW入力画面表示 S23
S24 PWを送信
認証 S25
S26 ｶｰﾄﾞ選択画面を送信
ｶｰﾄﾞ選択画面表示 S27
S28 ｶｰﾄﾞ選択情報を送信
S29 ｹｰﾀｲ番号を送信
S30 ｶｰﾄﾞ情報Aを送信
ﾜﾝﾀｲﾑ化：A+T 暗号化：enc(A+T) S31
S32 ﾃﾞｰﾀenc(A+T)を送信
S33 「ｶｰﾄﾞ情報を受信しました」を表示
POSに向かって送信操作 S34
S35 ﾃﾞｰﾀenc(A+T)を送信
復号化：A+T Tの有効性確認 S36
S37 Aを送りｶｰﾄﾞ処理依頼(ｵｰｿﾘｾﾞｰｼｮﾝ)
S38 ｶｰﾄﾞ処理

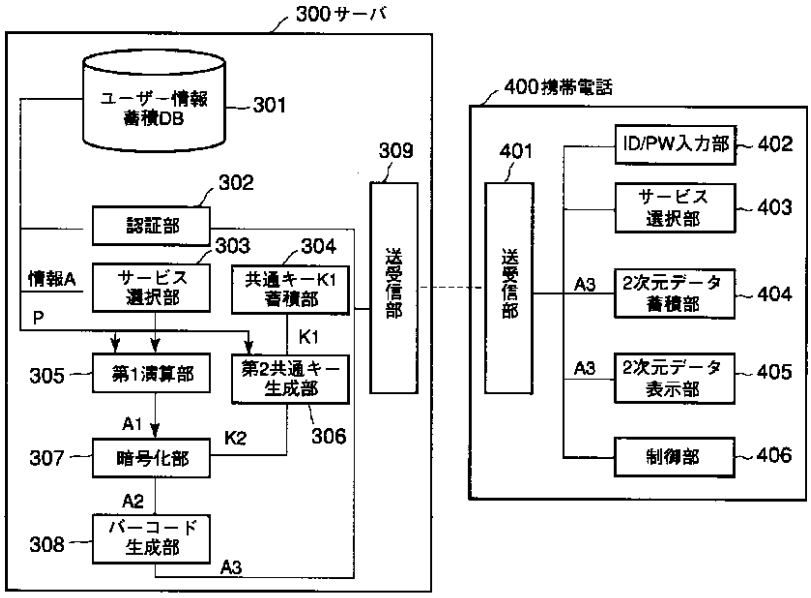
【図９】


利用者
加盟店
ｻｰﾋﾞｽ提供者
信販会社等
S51 URLを入力しｱｸｾｽ
S52 PW入力画面を送信
PW入力画面を表示 S53
S54 PWを送信
認証 S55
S56 ｶｰﾄﾞ選択画面を送信
ｶｰﾄﾞ選択画面を表示 S57
S58 ｶｰﾄﾞ選択情報を送信
S59 ｹｰﾀｲ番号を送信
S60 ｶｰﾄﾞ情報を送信
発行時間を記録 S62
暗号化 S61
S63 2次元ﾃﾞｰﾀを送信
2次元ﾊﾞｰｺｰﾄﾞを表示 S64
S65 2次元ｺｰﾄﾞ表示を提示
ﾘｰﾀﾞｰで読取り S66
復号化 S67
S68 有効性判断依頼
S70 通常のｶｰﾄﾞ処理依頼(ｵｰｿﾘｾﾞｰｼｮﾝ)
有効性確認 S69
選択情報通信
S71 ｶｰﾄﾞ処理

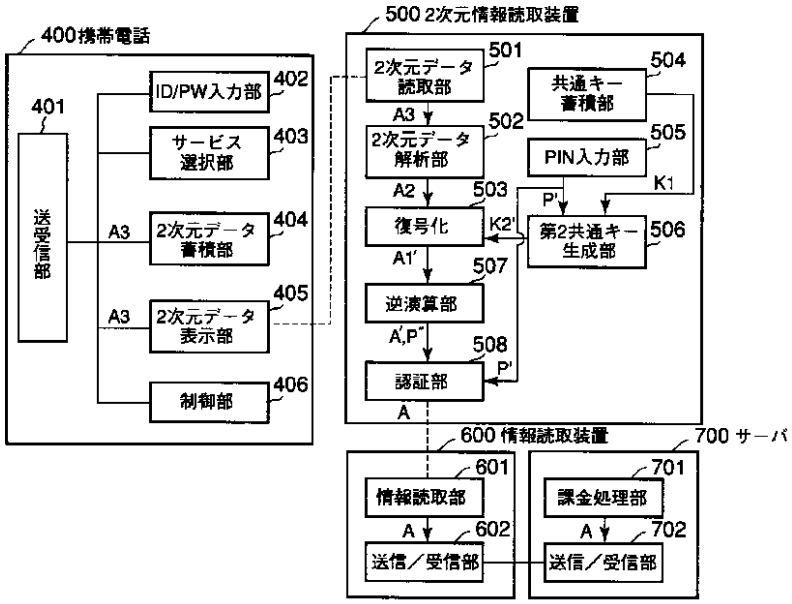
【図７】


ｻｰﾋﾞｽ提供者
利用者
加盟店
信販会社
52 ｻｰﾊﾞ
ﾕｰｻﾞ情報蓄積DB 18
19
17
認証部 20
ｻｰﾋﾞｽ選択部 21
情報A
時間情報付加部 22
情報A 情報T
暗号化部 23
送受信部
(A+T)
(A+T)
51 携帯電話
11
ID/PW入力部
16
送受信部
12
ｻｰﾋﾞｽ選択部
40
ﾃﾞｰﾀ蓄積部
(A+T)
41
近距離ﾃﾞｰﾀ通信部
42
近距離ﾃﾞｰﾀ通信指示部
制御部 15
(A+T)
53 無線通信装置
近距離ﾃﾞｰﾀ通信部 43
(A+T)
復号化部 28
情報A 情報T
時間情報判定部 29
情報A
情報読取部
31 30 情報A
送信／受信部
8 情報読取装置
情報A
3 ｻｰﾊﾞ
課金処理部 32 33
送信／受信部

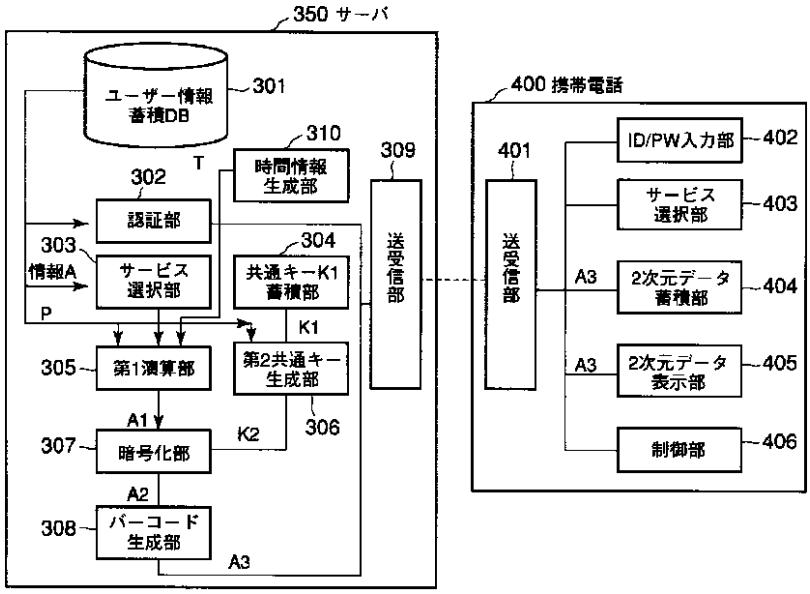
【図１１】


300サーバ
ユーザー情報蓄積DB
301
309
302
認証部
303
304
情報A
サービス選択部
共通キーK1蓄積部
送受信部
P
K1
305
第1演算部
第2共通キー生成部
A1
K2
306
307
暗号化部
A2
308
バーコード生成部
A3
400携帯電話
401
ID/PW入力部
402
サービス選択部
403
送受信部
A3
2次元データ蓄積部
404
A3
2次元データ表示部
405
制御部
406

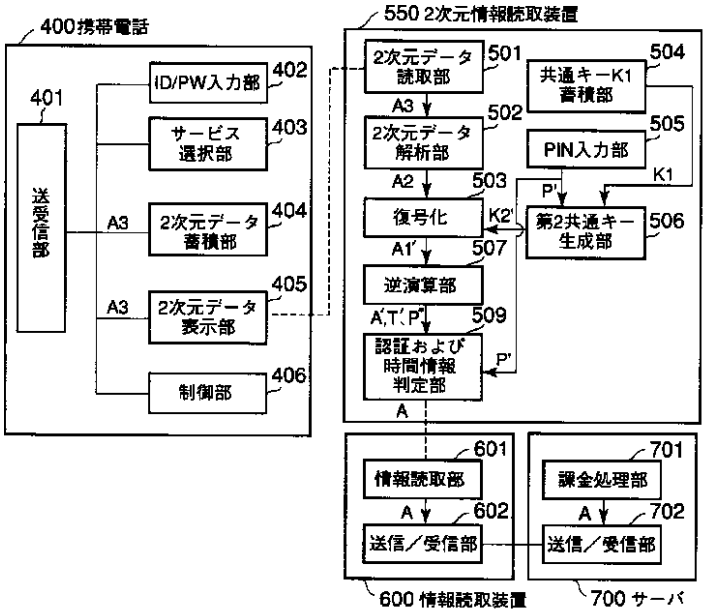
【図１２】


400携帯電話
401
送受信部
ID/PW入力部
402
サービス選択部
403
A3
2次元データ蓄積部
404
A3
2次元データ表示部
405
制御部
406
500 2次元情報読取装置
2次元データ読取部
501
A3
2次元データ解析部
502
A2
復号化
503
A1'
逆演算部
507
A',P''
認証部
508
A
共通キー蓄積部
504
PIN入力部
505
K1
P'
K2'
第2共通キー生成部
506
600 情報読取装置
情報読取部
601
A
送信／受信部
602
700 サーバ
課金処理部
701
A
送信／受信部
702

【図１３】



【図１４】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６０１Ｃ

(58)調査した分野(Int.Cl.[7]，ＤＢ名)

G06F　17/60
G07F　7/10
G07G　1/12
H04L　9/32