

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2002年10月24日 (24.10.2002)

PCT

(10) 国際公開番号  
**WO 02/084548 A1**

(51) 国際特許分類?: **G06F 17/60** [JP/JP]; 〒104-0032 東京都 中央区八丁堀 1-7-7 Tokyo (JP).

(21) 国際出願番号: PCT/JP02/02027

(22) 国際出願日: 2002年3月5日 (05.03.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
PCT/JP01/03130 2001年4月11日 (11.04.2001) JP  
PCT/JP01/07108 2001年8月17日 (17.08.2001) JP

(71) 出願人(米国を除く全ての指定国について): イレブン  
ポイントツー株式会社 (ELEVEN POINT TWO INC.)

(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 中島 啓一 (NAKA-JIMA,Keiichi) [JP/JP]; 〒140-0032 東京都 中央区八丁堀 1-7-7 イレブンポイントツー株式会社内 Tokyo (JP).

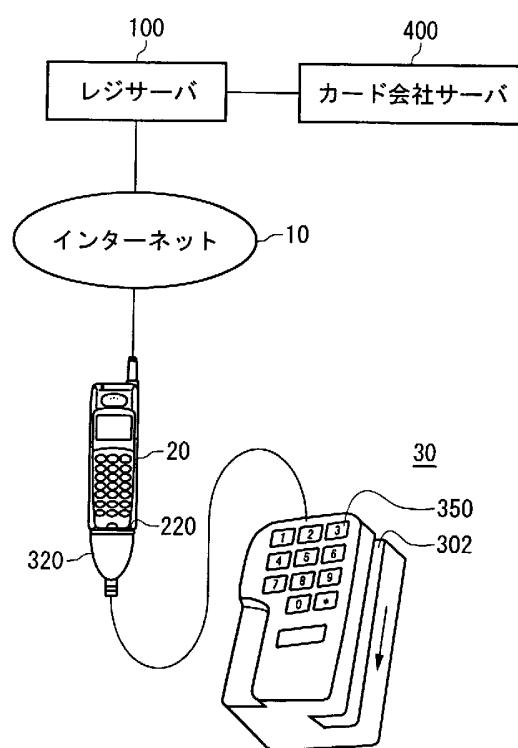
(74) 代理人: 龍華 明裕 (RYUKA,Akihiro); 〒160-0022 東京都 新宿区新宿 1丁目 24番 12号 東信ビル 6階 Tokyo (JP).

(81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,

[続葉有]

(54) Title: ELECTRONIC SETTLING SYSTEM

(54) 発明の名称: 電子決済システム



100...REGISTER SERVER  
400...CREDIT CARD COMPANY SERVER  
10...INTERNET

(57) Abstract: An electronic settling system enhanced in security against a combination of apparatuses, typically comprising a normal credit card-use card reader (30) connected to a mobile phone (20) used as a transaction terminal at a store, the terminal being authenticated by sending a card reader ID to a settling server (100) in addition to a user ID and a terminal ID. When authenticated successfully, servers (100) (400) carry out a credit transaction. A connection-controlling, ID-carrying adapter may be placed between the reader and the terminal. Or, an ID base may be encrypted.

WO 02/084548 A1

[続葉有]



ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:  
— 國際調査報告書

(84) 指定国(広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT,

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

---

(57) 要約:

機器の組み合わせに関してセキュリティを向上させた電子決済システム。典型的には店頭で通常のクレジットカード用のカードリーダ(30)がトランザクション端末としての携帯電話(20)に接続されるような構成であり、そこでは端末の認証がユーザ ID や端末 ID などに加えてカードリーダ ID が決済サーバ(100)に送られることで行われる。認証が成功するとサーバ(100)(400)によってクレジット・トランザクションが実行される。リーダと端末の間に接続をコントロールする ID つきアダプタが挿入されるようにしてもよい。また、ID ベースの暗号化を行ってもよい。

## 明細書

電子決済システム、決済サーバ、カードリーダ、端末システム、接続装置、情報通信システム、情報管理装置、認証システム、認証サーバ、決済方法、通信方法、情  
5 報送信方法、情報管理方法、認証方法、プログラム、及び記録媒体

## 技術分野

本発明は、通信ネットワークを用いて、商取引における決済を電子的に行うことのできる電子決済システム、決済サーバ、カードリーダ、端末システム、及び接続  
10 装置に関する。

## 背景技術

従来、通信ネットワークを介して、商取引における決済を電子的に行う電子決済システムでは、インターネットを経由して、クレジットカード番号などの個人情報をデジタルデータで送信していた。この場合、個人情報の漏洩を防ぐため、セキュリティの向上が望まれている。しかし、セキュリティを向上させると、例えば複雑な認証手続きなどが必要となり、簡便性を犠牲にせざるをえないという問題が生じていた。そこで本発明は、このような問題を解決することを目的とする。

## 20 発明の開示

このような目的を達成するために、本発明の第1の形態によれば、取引の決済を行う決済サーバを含む電子決済システムであって、前記取引の決済を利用するカードからカード情報を読み取るカードリーダと、前記カードリーダに接続し、前記カードリーダから取得した前記カード情報を、前記決済サーバに送信する取引端末とを備える。前記取引端末は、前記取引端末に接続した前記カードリーダを識別するカードリーダ識別情報と、前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報及び前記取引端末を識別する取引端末識別情報の少なくとも一方と、を前記決済サーバに送信し、前記決済サーバは、前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記

カードリーダ識別情報と、の組み合わせに基づいて、前記取引端末の認証を行い、前記認証に成功した場合に、前記通信ネットワークを介して前記取引端末から受信した前記カード情報を利用して決済処理を行う。

前記決済サーバは、前記取引端末の認証に成功した場合に、前記取引端末との通信を要求する通信要求を前記取引端末に送信し、前記取引端末は、前記通信要求を受信すると、当該通信要求に対する返信として、前記カードリーダから取得した前記カード情報を前記決済サーバに送信し、前記決済サーバは、前記通信要求の返信として受信した前記カード情報を利用して決済処理を行ってもよい。

前記取引端末は、携帯電話であってもよく、前記取引端末識別情報は、前記携帯電話の電話番号であってもよい。

本発明の第2の形態によれば、取引の決済を行う決済サーバを含む電子決済システムであって、前記取引の決済に利用するカードからカード情報を読み取るカードリーダと、前記カードリーダから前記カード情報を取得し、前記カード情報を前記決済サーバに送信する取引端末とを備える。前記取引端末は、前記カードリーダを識別するカードリーダ識別情報及び前記取引端末を識別する取引端末識別情報を利用して暗号化された前記カード情報を前記決済サーバに送信し、前記決済サーバは、前記取引端末識別情報及び前記カードリーダ識別情報を利用して、前記カード情報を復号化する。

本発明の第3の形態によれば、取引の決済を行う決済サーバを含む電子決済システムであって、前記取引の決済に利用するカードからカード情報を読み取るカードリーダと、前記カードリーダから前記カード情報を取得し、前記カード情報を前記決済サーバに送信する取引端末とを備える。前記決済サーバは、前記取引を識別する取引識別情報を発行し、前記カードリーダは、前記決済サーバが発行した前記取引識別情報を取得し、取得した前記取引識別情報を利用して、前記カード情報を暗号化し、前記取引端末は、暗号化後の前記カード情報を前記決済サーバに送信し、前記決済サーバは、発行した前記取引識別情報を利用して、前記カード情報を復号化する。

本発明の第4の形態によれば、取引の決済を行う決済サーバを含む電子決済システムであって、前記取引の決済に利用するカードからカード情報を読み取るカード

リーダと、前記カードリーダから取得した前記カード情報を、前記決済サーバに送信する取引端末と、前記カードリーダと前記取引端末とを接続する接続装置とを備える。前記取引端末は、前記カードリーダを識別するカードリーダ識別情報、前記取引端末を識別する取引端末識別情報若しくは前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報、及び前記取引端末に接続した前記接続装置を識別する接続装置識別情報、及びのうち少なくとも2つを前記決済サーバに送信し、前記決済サーバは、前記カードリーダ識別情報、前記取引端末識別情報若しくは前記ユーザ識別情報、及び前記接続装置識別情報のうち少なくとも2つの組み合わせに基づいて、前記取引端末の認証を行い、前記認証に成功した場合に、前記通信ネットワークを介して前記取引端末から受信した前記カード情報を利用して決済処理を行う。

本発明の第5の形態によれば、取引端末における取引の決済を行う決済サーバであって、前記取引端末を識別する取引端末識別情報及び前記取引端末又は前記カードリーダのユーザを識別するユーザ識別情報の少なくとも一方を受信するとともに、前記取引の決済を利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を、前記取引端末を介して受信する受信部と、前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報の組み合わせに基づいて、前記取引端末を認証する認証部と、前記認証に成功した場合に、前記取引端末を介して前記カードリーダから受信した前記カード情報を利20用して、前記決済処理を行う決済部とを備える。

前記認証部が、前記取引端末の認証に成功した場合に、前記受信部は、前記取引端末を介して前記カードリーダが読み取った前記カード情報を受信してもよい。

前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報とを対応付けて格納するカードリーダデータベースをさらに備え、前記認証部は、前記カードリーダデータベースにおいて対応付けられた、前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報との組み合わせを利用して、前記取引端末を認証してもよい。

前記認証部が前記取引端末の認証に成功した場合に、前記取引端末との通信を要する通信要求を前記取引端末に送信する送信部をさらに備えてよい。前記受信

部は、前記通信要求に対する返信として前記カード情報を受信してもよい。

前記受信部は、さらに前記取引の内容を示す取引内容を前記取引端末から受信し、

前記送信部は、前記取引内容を識別可能に、前記取引端末に前記通信要求を送信し、

前記受信部が前記通信要求に対する返信を受信した場合に、前記決済部は、前記取

5 引識別情報に対応する前記取引内容について、決済処理を行ってもよい。

前記決済サーバは、複数の前記取引端末における取引の決済を行い、前記カード

リーダデータベースは、前記取引端末識別情報と、前記カードリーダ識別情報とを

対応付けて格納するとともに、前記取引端末識別情報に対応付けて、前記取引の決

済の支払先を示す支払先識別情報をさらに格納し、前記決済部は、前記カードリー

10 ダデータベースにおいて、前記取引端末識別情報に対応付けて格納される前記支払

先に対して決済処理を行ってもよい。

本発明の第6の形態によれば、取引を行う取引端末における取引を決済する決済

サーバであって、前記取引端末を識別する取引端末識別情報、及び前記取引の決済

に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識

15 別情報をを利用して暗号化されたカード情報を前記取引端末から受信する受信部と、

前記カードリーダと、前記カードリーダが前記カード情報を送信すべき取引端末と

を対応付ける装置管理テーブルと、前記受信部が前記取引端末から前記カード情報

を受信した場合、前記取引端末識別情報、及び前記装置管理テーブルにおいて前記

取引端末に対応付けられた前記カードリーダの前記カードリーダ識別情報を利用し

20 て、前記カード情報を復号化する復号化部とを備える。

本発明の第7の形態によれば、取引の支払に利用するカードのカード情報を読み

取るカードリーダであって、前記カード情報を読み取るカード読取部と、取引端末

に接続する接続部と、前記接続部を介して前記カード情報を前記取引端末に送信す

る送信部とを備える。

25 前記接続部が、前記取引端末に接続した場合に、前記接続部を介して前記取引端

末を識別する取引端末識別情報を読み取る接続先認証部と、前記接続先認証部が読

み取った前記取引端末識別情報と予め定められた取引端末識別情報とが一致した場

合に、前記カード情報を前記取引端末に送信することを許可する許可部とをさらに

備えてもよい。

前記取引端末が通信すべき通信先を指定する通信先情報を保持する通信先保持部と、前記接続先認証部が読み取った前記取引端末識別情報と予め定められた前記取引端末識別情報とが一致した場合に、前記通信先保持部に保持される前記通信先情報をを利用して、前記取引端末と前記通信先との通信を確立する通信確立部とをさらに備えてもよい。

前記送信部は、さらに当該カードリーダを識別するカードリーダ識別情報を前記取引端末に送信してもよい。

前記取引端末は携帯電話であってもよい。前記接続先認証部は、前記携帯電話の電話番号を前記取引端末識別情報として読み取ってもよい。

前記カード讀取部が読み取ったカード情報を、暗号化する暗号化部をさらに備えてもよい。前記送信部は、前記暗号化部が暗号化した後の前記カード情報を前記取引端末に送信してもよい。

前記暗号化部は、当該カードリーダを識別するカードリーダ識別情報を利用して前記カード情報を暗号化してもよい。

前記送信部が前記カード情報を送信した回数を保持する回数保持部をさらに備えてもよい。前記暗号化部は、前記回数保持部に保持される回数を利用して、前記カード情報を暗号化してもよい。

前記回数を減じることを示す情報を受信する受信部をさらに備えてもよい。前記受信部が前記情報を受信した場合に、前記回数保持部は、保持する回数を減じてもよい。

本発明の第8の形態によれば、取引の決済を行う決済サーバと通信ネットワークを介して通信する端末システムであって、前記取引に利用するカードのカード情報を読み取るカードリーダと、前記カード情報を前記決済サーバに送信する取引端末とを備える。前記カードリーダは、前記カード情報を読み取るカード讀取部と、

前記取引端末に接続する前記接続部と、前記接続部を介して前記カード情報を前記取引端末に送信する送信部とを有する。前記取引端末は、前記カードリーダの前記接続部を介して前記カード情報を取得する取得部と、前記カード情報を前記決済サーバに送信する送信部と、前記決済が完了したことを示す決済完了通知を前記決済サーバから受信する受信部と、受信した前記決済完了通知を表示する表示部とを

有する。

前記取引端末は、前記カードの所有者から、前記カードのパスワード入力を受け付ける入力部をさらに備えてもよい。前記送信部は、前記入力部が受け付けた前記パスワードを、対応する前記カードの前記カード情報に対応付けて前記決済サーバ  
5 に送信してもよい。

本発明の第9の形態によれば、取引の決済を行う決済サーバと通信ネットワークを介して通信する端末システムであって、前記取引に利用するカードのカード情報を読み取るカードリーダと、前記カード情報を前記決済サーバに送信する取引端末とを備える。前記カードリーダは、前記カード情報を読み取るカード読取部と、前  
10 記カード情報を前記取引端末に送信する送信部とを有する。前記取引端末は、前記カードリーダの前記接続部を介して前記カード情報を取得する取得部と、前記カード情報を前記決済サーバに送信する送信部とを有し、前記カードリーダ及び前記取  
15 引端末のいずれか一方は、前記カードリーダを識別するカードリーダ識別情報を利用して、前記カード情報を暗号化するリーダ暗号化部を有し、前記カードリーダ及び前記取引端末のいずれか一方は、前記取引端末を識別する取引端末識別情報を利用して、前記カード情報を暗号化する端末暗号化部を有し、前記取引端末の送信部は、前記リーダ暗号化部及び前記端末暗号化部が暗号化した後の、前記カード情報を前記決済サーバに送信してもよい。

本発明の第10の形態によれば、取引の支払に利用するカードのカード情報を読み取るカードリーダと接続し、かつ取引端末と接続する接続装置であって、前記カードリーダに接続し、前記カードリーダから前記カード情報を取得するカードリーダ接続部と、前記取引端末に接続する取引端末接続部と、当該接続装置を識別する接続装置識別情報を保持する接続装置識別情報保持部と、前記取引端末接続部を介して、前記接続装置識別情報及び前記カード情報を前記取引端末に送信する送信部とを備える。

前記取引端末を識別する取引端末識別情報を保持する取引端末識別情報保持部と、前記取引端末接続部が前記取引端末に接続された場合に、前記取引端末接続部を介して、前記取引端末から当該取引端末を識別する取引端末識別情報を取得する接続先認証部と、前記接続先認証部が取得した前記取引端末識別情報と、前記取引端末

識別情報保持部が保持する前記取引端末識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許可する許可部とをさらに備えてもよい。

前記取引端末を識別する取引端末識別情報を保持する取引端末識別情報保持部と、前記取引端末接続部が前記取引端末に接続された場合に、前記取引端末接続部を介して、前記取引端末から当該取引端末を識別する取引端末識別情報を取得する接続先認証部と、前記取引端末接続部に接続された前記取引端末が通信すべき通信先を指定する通信先情報を保持する通信先保持部と、前記接続先認証部が読み取った前記取引端末識別情報と、前記取引端末識別情報保持部が保持する前記取引端末識別情報とが一致した場合に、前記通信先保持部に保持される前記通信先情報を利用して、前記取引端末と前記通信先との通信を確立させる通信確立部とをさらに備えてよい。

前記カードリーダを識別するカードリーダ識別情報を保持するカードリーダ識別情報保持部と、前記カードリーダ接続部が前記カードリーダに接続された場合に、前記カードリーダ接続部を介して、前記カードリーダから当該カードリーダを識別するカードリーダ識別情報を取得する接続先認証部と、前記接続先認証部が読み取った前記カードリーダ識別情報と、前記カードリーダ識別情報保持部が保持する前記カードリーダ識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許可する許可部とをさらに備えてもよい。

前記カードリーダを識別するカードリーダ識別情報を保持するカードリーダ識別情報保持部と、前記カードリーダ接続部が前記カードリーダに接続された場合に、前記カードリーダ接続部を介して、前記カードリーダから当該カードリーダを識別するカードリーダ識別情報を取得する接続先認証部と、前記カードリーダ接続部に接続された前記カードリーダが通信すべき通信先を指定する通信先情報を保持する通信先保持部と、前記接続先認証部が読み取った前記カードリーダ識別情報と、前記カードリーダ識別情報保持部が保持する前記カードリーダ識別情報とが一致した場合に、前記通信先保持部に保持される前記通信先情報を利用して、前記取引端末と前記通信先との通信を確立させる通信確立部とをさらに備えてもよい。

本発明の第11の形態によれば、ネットワークを介して通信を行う第1及び第2の通信装置を含む情報通信システムであって、情報を読み取る情報読み取り装置と、

前記情報読み取り装置から前記情報を取得し、前記読み取り装置を識別する読み取り装置識別情報及び第1の通信装置を識別する通信装置識別情報を利用して暗号化された前記情報を、暗号化情報として第2の通信装置に送信する第1の通信装置と、前記ネットワークを介して前記第1の通信装置から前記暗号化情報を受信し、前記読み取り装置識別情報及び前記第1通信装置識別情報を利用して、前記暗号化情報を復号化する第2の通信装置とを備える。

前記読み取り装置及び前記第1の通信装置と接続し、前記読み取り装置から前記第1の通信装置に情報を送る接続装置をさらに備えてもよい。前記第1の通信装置は、前記読み取り装置識別情報、前記接続装置を識別する接続装置識別情報、及び第1通信装置識別情報のうち少なくとも2つを利用して暗号化された前記暗号化情報を前記第2の通信装置に送信し、前記第2の通信装置は、前記読み取り装置識別情報、前記接続装置識別情報、及び前記第1通信装置識別情報のうち少なくとも2つを利用して前記暗号化情報を復号化してもよい。

本発明の第12の形態によれば、情報を管理する情報管理装置であって、前記情報を読み取る情報読み取り装置を識別する読み取り装置識別情報、及び前記読み取り装置に接続された通信装置を識別する通信装置識別情報を利用して暗号化された前記情報を、前記通信装置から受信する受信部と、前読み取り装置と、前記読み取り装置が前記情報を送信すべき通信装置とを対応付ける装置管理テーブルと、前記受信部が前記通信装置から前記情報を受信した場合に、前記通信装置識別情報及び前記装置管理テーブルにおいて前記通信装置に対応付けられた前記読み取り装置の前記読み取り装置識別情報を利用して、前記カード情報を復号化する復号化部とを備える。

本発明の第13の形態によれば、装置の認証を行う認証サーバを含む認証システムであって、情報を読み取る読み取り装置と、前記読み取り装置から当該読み取り装置を認証する認証要求を受け取り、当該認証要求を、ネットワークを介して前記認証サーバに送信する通信装置と、前記読み取り装置が前記情報を送るべき通信装置を管理し、前記ネットワークを介して、前記通信要求を受信した場合に、前記通信要求に示される前記読み取り装置が読み取った前記情報を送るべき前記通信装置に、前記読み取り装置を認証することを示す読み取り装置認証情報を送信する認証

サーバとを備える。前記読み取り装置は、前記通信装置が受信した前記読み取り装置認証情報と同一の読み取り装置認証情報を取得した場合に、前記情報を前記通信装置に送ることを許可する送信許可部を有する。

前記読み取り装置は、所定の処理が行われた場合に、前記読み取り情報を送信することを禁止する送信禁止部と、前記送信禁止部が前記送信を禁止した場合に、前記認証要求を前記通信端末に送る認証要求送信部とをさらに有してもよい。

前記通信装置は、前記読み取り装置認証情報を受信する受信部と、前記受信部が受信した読み取り装置認証情報を表示する表示部とを有してもよい。前記読み取り装置は、ユーザからの入力により、前記表示部に表示された前記読み取り装置認証情報を取得する取得部をさらに有してもよい。前記取得部が前記読み取り装置認証情報を取得した場合に、前記送信許可部は、前記情報を前記通信装置に送ることを許可してもよい。

前記読み取り装置は、前記認証装置が前記読み取り装置を認証するときに利用する読み取り装置認証情報を保持する読み取り装置認証情報保持部をさらに有してもよい。前記取得部が取得した前記読み取り装置認証情報と、前記読み取り装置認識情報保持部に保持される前記読み取り装置認識情報とが一致した場合に、前記送信許可部は、前記読み取り情報を前記通信装置に送ってもよい。

前記読み取り装置は、カードからカード情報を読み取るカードリーダであってよい。

本発明の第14の形態によれば、装置を認証する認証サーバであって、情報を読み取る読み取り装置が読み取った情報を、当該読み取り装置に接続された通信装置から、ネットワークを介して受信する受信部と、前記通信部から、前記読み取り装置を認証することを要求する認証要求を取得する認証要求取得部と、前記読み取り装置と、当該読み取り装置が読み取った読み取り情報を送るべき通信装置とを対応付ける装置管理テーブルと、装置管理テーブルを利用して、前記認証要求取得部が取得した前記認証要求に示される前記読み取り装置が前記情報を送るべき前記通信装置を選択し、選択された前記通信装置に対して、前記読み取り装置を認証すべき読み取り装置認証情報を送信する送信部とを備える。

なお、上記した各システム又は装置の動作による方法、及び動作させるためのブ

ログラム及びこれを格納した記録媒体も、発明の一形態である。

### 図面の簡単な説明

- 5 図1は、電子決済システム全体を示す図である。  
図2は、レジサーバ100の機能構成を示すブロック図である。  
図3は、カードリーダデータベース122のデータ構成を示す図である。  
図4は、携帯電話20の機能構成を示す図である。  
図5は、カードリーダ30の機能構成を示すブロック図である。
- 10 図6は、レジサーバ100と、携帯電話20の通信シーケンスである。  
図7は、図6のカードリーダ識別情報取得段階(S102)における、カードリーダ30の詳細な動作を示すフローチャートである。  
図8は、図6の携帯電話認証段階(S106)における、レジサーバ100の詳細な動作を示すフローチャートである。
- 15 図9は、図6の商品選択段階(S112)における、携帯電話20の詳細な動作を示すフローチャートである。  
図10は、図6のカード情報及び暗証番号取得段階(S122)における、携帯電話20及びカードリーダ30の詳細な動作を示すフローチャートである。
- 20 図11は、図6の決済処理段階(S134)における、レジサーバ100の詳細な動作を示すフローチャートである。  
図12は、カードリーダ30において不正処理が行われた場合の、カードリーダ30、携帯電話20、及びレジサーバ100の通信シーケンスである。
- 25 図13は、レジサーバ100のハードウェア構成を示す図である。  
図14は、第2実施形態における電子決済システム全体を示す図である。  
図15は、第2実施形態におけるカードリーダ30の機能構成を示す。
- 図16は、接続装置40の機能構成を示すブロック図ある。  
図17は、接続装置40の動作を示すフローチャートである。
- 図18は、第2実施形態におけるカードリーダ30、接続装置40、及び携帯電話20の詳細な動作を示すフローチャートである。

図19は、変更例におけるカードリーダ30の機能構成を示すブロック図である。

図20は、変更例における接続装置40の機能構成を示すブロック図である。

5 図面に用いた主な符号の凡例を以下に示す。

10 インターネット

20 携帯電話

30 カードリーダ

40 接続装置

10 100 レジサーバ

400 カード会社サーバ

724 データベース

## 発明を実施するための最良の形態

15

以下、図面を参照して本発明の実施の形態の一例を説明する。以下の実施形態はクレームにかかる発明を限定するものではなく、又実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

なお、詳細な説明中に記載の「レジサーバ」は、特許請求の範囲に記載の「決済サーバ」の一例である。また、詳細な説明中に記載の「インターネット通信部」は、特許請求の範囲に記載の「送信部」及び「受信部」の一例である。

詳細な説明中に記載の「携帯電話」は、特許請求の範囲に記載の「取引端末」の一例である。詳細な説明中に記載の「リーダ通信部」は、特許請求の範囲に記載の「取得部」の一例である。

25 図1は、電子決済システムを示す。電子決済システムは、レジサーバ100と、カード会社サーバ400と、携帯電話20と、カードリーダ30とを備える。

カードリーダ30は、カード読取部302、テンキー330、及び接続部320を有する。カード読取部302は、クレジットカードなど決済用カードに格納されているカード情報を読み取る。テンキー330は、ユーザからの入力を受け付ける。

接続部320は、携帯電話20の接続部220と接続する。カードリーダ30は、カード読み取部302が読み取ったカード情報を、接続部320を介して携帯電話20に送る。

携帯電話20は、カードを利用した取引の取引対象となる商品及び取引金額などを示す取引内容と、カードリーダ30から受け取ったカード情報を、インターネット10を介してレジサーバ100に送る。

レジサーバ100は、携帯電話20及びカードリーダ30を認証する。レジサーバ100は、認証に成功すると、携帯電話20から受け取ったカード情報を利用して、取引の決済を行う。レジサーバ100は、取引内容及びカード情報をカード会社サーバ400へ送信する。レジサーバ100は、カード会社サーバ400へ送信した取引内容に対し、取引内容についての決済が完了したことを示す決済完了通知をカード会社サーバ400から受信する。

このように本電子決済システムでは、インターネット10を介して、ユーザが所有するクレジットカードやデビットカードなど決済用カードを利用した決済を行うことができる。従って、商品を販売する販売者は、携帯電話20及びカードリーダ30を用いて、ユーザの所有するカードのカード情報をレジサーバ100に送信することができるので、例えば、宅配サービスなど、店頭以外の場所でも、カードによる取引を行うことができる。

図2は、レジサーバ100の機能構成を示すブロック図である。レジサーバ100の一連の動作は、主にCPUとROM及びRAMに格納されたプログラムの共働によって実現される。但し、それ以外の構成要素によってレジサーバ100が実現されてもよく、その設計の自由度は高い。レジサーバ100は、インターネット通信部102と、商品情報抽出部104と、決済部106と、認証部108と、位置検出部出力部112と、認証要求取得部114と、復号化部130と、カード会社サーバ通信部110と、商品データベース120と、及びカードリーダデータベース122とを有する。

インターネット通信部102は、インターネット10を介して携帯電話20と各種情報を送受信する。インターネット通信部102は、例えば携帯電話20から暗号化されたカード情報を受信する。

商品データベース 120 は、取引の対象となる商品に関する情報を格納する。商品に関する情報とは、例えば、商品の品名、単価などである。商品情報抽出部 104 は、インターネット通信部 102 を介して携帯電話 20 から取引内容を受け取り、取引内容に示される商品に関する情報を商品情報データベース 120 から抽出する。

5 カードリーダデータベース 122 は、携帯電話 20 を識別する取引端末識別情報及びカードリーダ 30 を識別するカードリーダ識別情報を対応付けて格納する。ここで、さらに携帯電話 20 のユーザ、若しくはカードリーダのユーザを識別するユーザ識別情報を対応付けて格納してもよい。

位置検出部 132 は、携帯電話 20 の位置を検出する。位置検出部 132 は、例 10 えば GPS (Global Positioning System) を利用して緯度及び経度を示す位置情報を検出してもよい。

認証要求取得部 114 は、インターネット通信部 102 を介して、カードリーダ 30 を認証することを要求する認証要求を取得する。認証要求は、送信元であるカードリーダ 30 を識別するカードリーダ識別情報を含む。認証要求取得部 114 は、15 取得した認証要求を認証部 108 に送る。

認証部 108 は、携帯電話 20 を識別する携帯電話識別情報、及び携帯電話 20 又はカードリーダ 30 のユーザを識別するユーザ識別情報、の少なくとも一方をインターネット通信部 102 を介して携帯電話 20 から受け取ると共に、カードリーダ 30 を識別するカードリーダ識別情報を、インターネット通信部 102 を介して 20 携帯電話 20 から受け取る。認証部 108 はまた、携帯電話 20 の位置を示す位置情報を、位置検出部 132 から受け取る。認証部 108 は、カードリーダデータベース 122 に格納される携帯電話識別情報及びユーザ識別情報の少なくとも一方と、カードリーダ識別情報と、の組み合わせを、及びインターネット通信部 102 を介して受け取った、携帯電話識別情報及びユーザ識別情報の少なくとも一方とカード 25 リーダ識別情報との組み合わせに対して比較して、携帯電話 20 及びカードリーダ 30 を携帯する販売者を認証する。すなわち、認証部 108 は、インターネット通信部 102 を介して、携帯電話 20 から受信した、携帯電話識別情報及びユーザ識別情報の少なくとも一方とカードリーダ識別情報の組み合わせと、及びカードリーダデータベース 122 に格納される携帯電話識別情報及びユーザ識別情報の少なく

とも一方とカードリーダ識別情報の組み合わせと、が一致した場合に、携帯電話20を携帯する販売者の認証に成功したと判断する。認証部108は、このときさらに位置情報をを利用して販売者を認証する。なお、認証部108は、系炭田和式別情報とユーザ識別情報の組合せに基づいて認証を行ってもよい。

5 認証部108はまた、認証要求取得部114から認証要求を受け取る。認証部108は、カードリーダデータベース122を利用して、受け取った認証要求が示すカードリーダ30を認証することを示す認証情報を選択し、かつこの認証情報を送信すべき携帯電話20を選択する。認証部108は、インターネット通信部102に対して、選択した認証情報を、選択した携帯電話20に送信させる。

10 認証部108が、販売者の認証に成功した場合、決済部106は、インターネット通信部102を介して、携帯電話20から受け取った取引内容に示される取引についての決済を行う。決済部106はまた、取引毎に取引を識別する取引識別情報を発行する。

15 復号化部130は、インターネット通信部102が受信したカード情報を、カードリーダデータベース122に格納される情報及びこの取引に対して発行された取引識別情報を利用して、復号化する。カード会社サーバ通信部110は、カード会社サーバ400と通信し、各種情報を送受信する。レジサーバ100は、例えばLAN (Local Area Net Work) などの専用回線を介して、カード会社サーバ400と通信する。他の例としては、レジサーバ100は、カード会社サーバ400とインターネット10などの通信回線を介して通信してもよい。

20 図3は、カードリーダデータベース122のデータ構成を示す。カードリーダデータベース122は、携帯電話フィールドと、カードリーダフィールドと、ユーザフィールドと、パスワードフィールドと、販売者名フィールドと、支払先フィールドと、許可地域フィールドと、取引回数フィールドと、カードリーダ認証情報フィールドとを有する。

25 携帯電話フィールドは、販売者が携帯する携帯電話20を識別する携帯電話識別情報を確認する。携帯電話20が携帯電話の場合、携帯電話識別情報は、携帯電話の電話番号であってもよい。カードリーダフィールドは、カードリーダを識別するカードリーダ識別情報を格納する。ユーザフィールドは、携帯電話20のユーザ又

はカードリーダのユーザを識別するユーザ識別情報を格納する。

このようにカードリーダデータベース122は、携帯電話識別情報、ユーザ識別情報、及びカードリーダ識別情報を対応付けて格納する。従って、認証部108は、カードリーダデータベース122において対応付けられている携帯電話識別情報及びユーザ識別情報の少なくとも一方と、カードリーダ識別情報との組み合わせに基づいて、携帯電話20を認証することができる。すなわち、携帯電話20を携帯する販売者を認証することができる。

パスワードフィールドは、販売者が入力すべきパスワードを格納する。販売者名フィールドは、携帯電話20及びカードリーダ30を携帯する販売者の氏名を格納する。支払先フィールドは、決済における取引金を支払う支払先を格納する。支払先は、例えば商品の販売元である販売会社などである。許可地域フィールドは、携帯電話20を利用した取引が許可される地域を示す許可地域情報を格納する。許可地域情報は、例えば東京都・神奈川県など都道府県を示す情報であってもよく、また他の例としては、日本やアメリカなど国を示す情報であってもよい。取引回数フィールドは、対応する携帯電話20と取引を行った回数を格納する。すなわち、インターネット通信部102が受信したカード情報を、復号化部130が復号化できた場合に、1回とカウントされる。カードリーダ認証情報フィールドは、カードリーダを認証することを示す認証情報を格納する。認証情報は、カードリーダ30に登録された認証番号などであってもよい。また、カードリーダ認証情報フィールドは、複数の認証情報を格納してもよい。なお、本実施の形態における「カードリーダデータベース122」は、特許請求の範囲に記載の「装置管理テーブル」の一例である。

このように、本実施の形態におけるカードリーダデータベース122は、携帯電話識別情報に対応付けて、ユーザ識別情報、カードリーダ識別情報及びカードリーダ認証情報を格納している。従って、許可部108は、カードリーダデータベース122を利用して、認証要求に対する認証情報を選択することができる。許可部108はさらに、カードリーダデータベース122を利用して、カードリーダ認証情報を送信すべき携帯電話20を選択することができる。

また、復号化部130は、カードリーダデータベース122において対応付けら

れている携帯電話識別情報、ユーザ識別情報、カードリーダ識別情報、及び取引回数などをを利用して、カード情報を復号化することができる。なお、カードリーダデータベース 122 は、復号化部 130 がカード情報を復号化できた場合に、取引回数が 1 回とカウントされる。しかし、携帯電話 20 とレジサーバ 100 との通信に 5 障害が生じた場合、取引回数を正しくカウントすることができない。従って、復号化部 130 は、カードリーダデータベース 122 に格納される取引回数を利用して、カード情報を復号化できない場合に、取引回数から所定の範囲の回数を利用して、カード情報の復号化を試みてもよい。

図 4 及び図 5 は、携帯電話 20 及びカードリーダ 30 の機能構成を示すブロック 10 図である。携帯電話 20 及びカードリーダ 30 の一連の動作は、主に CPU と ROM 及び RAM に格納されたプログラムの共働によって実現される。但し、それ以外の構成によって、携帯電話 20 及びカードリーダ 30 が実現されてもよく、その設計の自由度は高い。

図 4 は、携帯電話 20 の機能構成を示すブロック図である。携帯電話 20 は、接続部 220 と、リーダ通信部 202 と、インターネット通信部 210 と、入力部 204 と、表示部 206 と、端末暗号化部 230 と、携帯電話識別情報保持部 232 とを有する。

リーダ通信部 202 は、接続部 220 を介してカードリーダ 30 と各種情報を送受信する。リーダ通信部 202 は、カードリーダ 30 からカードリーダ識別情報及びカード情報を受け取る。

入力部 204 は、例えば携帯電話のプッシュボタン等であり、販売者からパスワードの入力を受け付ける。入力部 204 は、さらにカード所有者からカードの暗証番号等の入力を受け付ける。

携帯電話識別情報保持部 232 は、本携帯電話を識別する携帯電話識別情報を保 25 持する。

端末暗号化部 230 は、リーダ通信部 202 からカード情報を受け取り、入力部 204 から暗証番号を受け取る。端末暗号化部 230 はさらに、インターネット通信部 210 から取引番号を受け取る。端末暗号化部 230 は、携帯電話識別情報保持部 232 から携帯電話識別情報を受け取る。端末暗号化部 230 は、携帯電話識

別情報及び取引番号を利用してカード情報及び暗証番号を暗号化する。端末暗号化部230は、例えば、携帯電話識別情報をカード情報に織り交ぜ、さらに、取引番号をキーとしてハッシュ関数などを用いてカード情報にスクランブルをかけてよい。

5 また、入力部204は、携帯電話20のユーザ識別情報又はカードリーダ30のユーザ識別情報を取得してもよい。この場合、端末暗号株230は、ユーザ識別情報を、カード番号及び暗証番号を暗号化する際に用いてよい。

また、インターネット通信部210は、カードリーダ30から取得したユーザ識別情報、又は入力部204が取得したユーザ識別情報を、インターネット10に接続している他の機器に送信してもよい。

なお、レジサーバ100の復号化部130は、携帯端末20及びカードリーダ30の暗号化ロジックに対応する復号化を行う。

インターネット通信部210は、インターネット10を介してレジサーバ100と各種情報を送受信する。インターネット通信部210は、端末暗号化部230からカード情報及び暗証番号を受け取り、これらをレジサーバ100に送信する。

インターネット通信部210は、レジサーバ100から各種情報を受け取り、表示部210へ送る。表示部210は、例えば携帯電話の液晶画面であってもよく、受信部208から受け取った情報等を表示する。

20 このように、携帯電話20は、カードリーダ識別情報、取引回数、及び携帯電話識別情報を利用して暗号化した後にカード情報をレジサーバ100に送信するので、インターネット10において、カード情報が漏洩するのを防ぐことができる。

図5は、カードリーダ30の機能構成を示す。カードリーダ30は、カード読取部302と、リーダ暗号化部330と、リーダ識別情報保持部332と、回数保持部324と、不正処理監視部360と、送信禁止部362と、許可部306と、接続先認証部308と、接続先保持部310と、通信部340と、認証情報保持部364と、カードリーダ認証部366と、接続部320と、テンキー350とを有する。

カード読取部302は、挿入されたカードからカード情報を読み取る。ここで読みとるカード情報には、ユーザを識別するユーザ識別情報を含んでいてよい。

リーダ識別情報保持部332は、本カードリーダ30を識別するリーダ識別情報を保持する。回数保持部324は、通信部340がカード情報を送信した回数を取り回数として保持する。

リーダ暗号化部330は、カード読み取り部302からカード情報を受け取る。

- 5 リーダ暗号化部330は、またリーダ識別情報保持部332からリーダ識別情報を受け取り、回数保持部324から取引回数を受け取る。リーダ暗号化部330はさらに、テンキー350から入力された取引識別情報を受け取る。リーダ暗号化部330は、リーダ識別情報、取引回数、及び取引識別情報をを利用して、カード情報を暗号化する。リーダ暗号化部330は、例えばリーダ識別情報、取引回数、及び取  
10 引識別情報を、カード情報に織り交ぜることによってカード情報を暗号化してもよい。

通信部340は、接続部320を介して携帯電話20と各種情報を送受信する。

- 通信部340は、リーダ暗号化部330からカード情報を受け取り、携帯電話20に送信する。通信部340は、また携帯電話20から携帯電話識別情報、及び取引  
15 が完了したことを示す取引完了通知を受信する。接続部320は、例えばソケットなど、携帯電話20と接続可能な構造であって、携帯電話20と接続する。

このように、カードリーダ20は、カードリーダ読取部302が読み取ったカード情報を暗号化した後に、携帯電話20に送信する。従って、カードリーダ30は、カード情報が携帯電話20から漏洩するのを防止することができる。

- 20 なお、カードリーダ20は、カード読取部302が読みとったカード情報がユーザ識別情報である場合、読みとったカード情報を、リーダ暗号化部330を介さず  
に、直接通信部340及び接続部320を介して携帯電話20に送信してもよい。

- 接続先保持部310は、接続部320が接続すべき携帯電話20の携帯電話識別情報を、接続先携帯電話識別情報として保持する。すなわち、各カードリーダ30  
25 は、それぞれに予め設定された接続先携帯電話識別情報を格納する。

なお、接続先保持部310は、予め定められている接続先携帯電話識別情報を保持してもよく、また他の例としては、保持する接続先携帯電話識別情報を適宜更新してもよい。接続先保持部310は、さらにこの場合、カードリーダ30は、接続部320を介して、携帯電話識別情報を取得してもよい。接続先保持部310は、

取得した携帯電話識別情報を保持してもよい。また他の例としては、接続先保持部310は、複数の接続先携帯電話識別情報を保持してもよい。

不正処理監視部360は、本カードリーダ20において不正な処理が行われていないか監視する。不正処理監視部360は、例えば、リーダ暗号化部330が、同一の取引識別情報を利用して暗号化を行っていた場合に、不正処理と判断してもよい。レジサーバ100は、各取引毎に取引識別情報を発生させる。従って、異なる取引に同一の取引識別情報が割り当てられることはない。そこで、不正処理監視部360は、このように、同一の取引識別情報を利用した暗号化を不正処理と判断する。不正処理監視部360はまた、異なる取引に対して、テンキー350から同一の取引識別情報を受け付けた場合に、不正処理と判断してもよい。不正処理監視部360は、不正処理が検出された場合に、送信禁止部362に通知する。

送信禁止部362は、不正処理監視部360から通知を受けると、通信部340に対して、カード情報の送信を禁止する。このように、送信禁止部362は、カードリーダ30において不正処理が行われた場合に、カード情報の送信を禁止することができる。これによって、第三者が本カードリーダ30を不正に利用した場合に、カードリーダ30から読み出されたカード情報がインターネット10に送信されるのを防ぐことができる。

接続先認証部308は、通信部340から携帯電話20の携帯電話識別情報を受け取る。接続先認証部308は、さらに接続先保持部310から接続先携帯電話識別情報を受け取る。接続先認証部308は、携帯電話識別情報と、接続先携帯電話識別情報とを照合し、接続先を認証する。

認証情報保持部364は、本カードリーダ30を認証する認証情報を保持する。人情報保持部364が保持する認証情報は、レジサーバ100のカードリーダデータベース122に保持される本カードリーダ30の認証情報と同一の認証情報である。

カードリーダ認証部366は、テンキー350を利用してユーザが入力した認証情報を受け取る。カードリーダ認証部366は、受け取った認証情報と、認証情報保持部364に保持される認証情報とを利用して、本カードリーダ30を認証する。すなわち、カードリーダ認証部366は、認証部正式なユーザが利用していること

を認証する。なお、「テンキー 350」は、特許請求の範囲に記載の「取得部」の一例である。

許可部 306 は、接続先認証部 308 が接続先の認証に成功した場合に、通信部 340 に対し、カードリーダ識別情報及びカード情報を送信することを許可する。

- 5 許可部 306 はまた、カードリーダ認証部 366 が本カードリーダ 30 のユーザの認証に成功した場合に、通信部 340 に対して、カード情報を送信することを許可する。

このように、本実施の形態のカードリーダ 30 は、携帯電話 20 と接続できるので、販売者が携帯する携帯電話 20 を利用して、カード情報をレジサーバ 100 へ 10 送信することができる。また、カードリーダ 30 の接続先認証部 308 は、接続先保持部 310 に予め保持されている携帯電話識別情報をを利用して、携帯電話 20 を認証する。従って、第三者が、他人の携帯電話 20 またはカードリーダ 30 を用いて、不正な取引を行うのを防ぐことができる。

また、テンキー 350 は、外部からカードリーダのユーザを識別するユーザ識別情報若しくは携帯電話 20 のユーザを識別するユーザ識別情報を取得し、通信部 3 15 40 、接続部 320 、及び携帯電話 20 を介して、インターネット 10 に接続している他の機器に送信してもよい。

図 6 は、レジサーバ 100 と携帯電話 20 の通信を示す通信シーケンスである。販売者は、携帯する携帯電話 20 とカードリーダ 30 とを接続し、カードリーダ 3 20 0 を用いた取引の準備をする (S100)。携帯電話 20 がカードリーダ 30 に接続されると、携帯電話 20 のリーダ通信部 202 は、カードリーダ 30 からカードリーダ識別情報を取得する (S102)。次に、携帯電話 20 のインターネット通信部 210 は、レジサーバ 100 に対し、取引を行うことを要求する取引要求を送信する (S104)。

25 レジサーバ 100 のインターネット通信部 102 は、携帯電話 20 から取引要求を受け取る。次に、認証部 108 は、取引要求を送信した携帯電話 20 を認証する (S106)。認証部 108 は、携帯電話 20 の認証に成功すると、携帯電話 20 から商品データベース 120 へのアクセスを許可する (S108)。次に、インターネット通信部 102 は、商品データベース 120 へのアクセスを許可した旨を示す許

可通知を携帯電話 20 へ送信する (S 110)。

携帯電話 20 のインターネット通信部 210 は、レジサーバ 100 から許可通知を受信する。次に、インターネット通信部 210 は、レジサーバ 100 の商品データベース 120 にアクセスし、取引の対象となる商品に関する情報を選択する (S 5 112)。次に、携帯電話 20 の表示部 206 は、取引の対象となる商品に関する情報などを含む取引内容を表示する。従って、販売者は、表示部 206 に表示された取引内容を確認することができる。携帯電話 20 のインターネット通信部 210 は、販売者が確認した取引内容をレジサーバ 100 に送信する (S 114)。

レジサーバ 100 のインターネット通信部 102 は、取引内容を受信する。次に、  
10 決済部 106 は、受信した取引内容に対し、取引内容を識別する取引番号を発行する (S 116)。このように、レジサーバ 100 は、取引内容を受信する毎に、受信した取引内容に対して異なる取引番号を発行する。すなわち、1 取引につき、1 つ  
15 の仮想的なレジ端末が発生する。従って、レジサーバ 100 は、各取引毎に取引番号を割り当てることによって、仮想的なレジ端末を発生させ、これによって、各取引についての処理を行うことができる。

次に、レジサーバ 100 の決済部 106 は、取引番号を含む通信要求を作成する (S 118)。インターネット通信部 102 は、通信要求を携帯電話 20 に送信する (S 120)。決済部 106 は、例えば、電子メールに通信要求を埋め込み、インターネット通信部 102 は、決済部 106 が作成した電子メールを送信してもよい。

20 携帯電話 20 は、レジサーバ 100 から通信要求を受け取ると、通信要求に基づいてレジサーバ 100 との通信を確立する。通信要求には、例えば、Java で記載された、レジサーバ 100 との通信を確立するためのプログラムが埋め込まれていてもよい。この場合、携帯電話 20 は、プログラムによって、自動的にレジサーバ 100 との通信を確立する。

25 このように、レジサーバ 100 は、携帯電話 20 からのアクセスによって確立した通信を一旦切断する。レジサーバ 100 は、切断した後に、改めて、認証に利用した情報を用いて携帯電話 20 にアクセスする。レジサーバ 100 は、こうして確立した通信回線を利用して取引を行う。従って、レジサーバ 100 は、不正なアクセスによってレジサーバ 100 との通信を確立した携帯電話 20 との通信を行うこ

とがない。すなわち、レジサーバ100は、不正にアクセスしてきた携帯電話20との通信を避けることができる。

次に、携帯電話20は、カード情報及びカードの暗証番号を取得し(S122)、暗号化されたカード情報及び暗号化された暗証番号をレジサーバ100に送信する5(S126)。このとき、ユーザは、カードに対応する暗証番号を、携帯電話20のプッシュボタンを利用して入力してもよい。

このように、カード情報及び暗証番号は暗号化された後にレジサーバ100に送信されるのでインターネット10上で情報が漏洩するのを防ぐことができる。

またこのとき、携帯端末20は、取引識別情報とともにカード情報を送信しても10よい。これによって、レジサーバ100は、対応する取引を認識することができる。

レジサーバ100のインターネット通信部102は、携帯電話20に送信した通信要求に対する返信としてカード情報及び暗証番号を、携帯電話20から受信する。復号化部130は、カードリーダデータベース122に格納される情報を利用して、カード情報及び暗証番号を復号化する。なお、復号化部130が、レジサーバ1015が有する暗号ロジックを利用して、カード情報を復号化できない場合、レジサーバ100は、カード情報に対する処理を中断し復号化できない旨を携帯電話20に通知してもよい。

このように、復号化部130がカード情報の復号化に成功しない場合、レジサーバ100は、カード情報を利用した決済を中断する。従って、レジサーバ100は、20不正に送信されたカード情報を利用して決済するのを避けることができる。

次に、カード会社サーバ通信部110は、取引内容及びカード情報をカード会社サーバ400に送信する。このとき、カード会社サーバ通信部110は、さらにカードリーダデータベース122において、携帯電話に対応付けて格納される支払先を示す情報をカード会社サーバ400に送信する。このように、カードリーダデータベース122は、携帯電話に対応付けて、支払先を格納するので、レジサーバ100は、携帯電話20から取引内容を受信した場合に、取引内容に示される支払金を支払うべき支払先を特定することができる。

次に、カード会社サーバ通信部110は、送信した取引内容に対し、取引内容の決済に関する内容を示す会計情報を、カード会社サーバ400から受信する。イン

ターネット通信部 102 は、カード会社サーバ 400 から受信した会計情報を、携帯電話 20 に送信する (S128)。

携帯電話 20 は、会計情報を受信し、表示部 210 に表示させる (S130)。販売者及び購入者は、表示部 210 に表示された会計情報を確認すると、入力部 20  
5 6 を介して確認した旨を入力する。確認した旨が入力されると、送信部 204 は、確認通知を送信する (S132)。

レジサーバ 100 のインターネット通信部 102 が確認通知を受信すると、決済処理部 106 は、取引内容に関しての実際の決済処理を行う (S134)。決済が終了すると、レジサーバ 100 は携帯電話 20 に対し決済が完了したことを示す決済  
10 完了通知を送信する (S136)。

携帯電話 20 は、決済完了通知を受信し、決済完了通知を表示部 210 に表示させる (S138)。このように、携帯電話 20 の表示部 210 は、会計情報及び決済完了通知を表示するので、購入者及び販売者は、これによって、会計情報及び決済完了情報を確認することができる。以上で電子決済を行うときのレジサーバ 100  
15 及び携帯電話 20 の動作は終了する。

図 7 は、カードリーダ識別情報取得段階 (S102) における、カードリーダ 30 の動作を示すフローチャートである。カードリーダ 30 は、接続部 320 を介して携帯電話 20 と接続する (S200)。次に、通信部 340 は、携帯電話 20 から携帯電話識別情報を受け取る (S202)。接続先認証部 308 は、携帯電話識別情報と携帯電話識別情報が接続先保持部 310 に格納されている接続先携帯電話識別情報とを照合する。携帯電話識別情報と、接続先携帯電話識別情報が一致する場合  
20 (S204)、許可部 306 は、カードリーダ識別情報及びカード情報を携帯電話 20 に送信することを許可する (S206)。次に、通信部 340 は、カードリーダ識別情報を携帯電話 20 に送信する (S208)。

25 なお、通信部 340 は、さらにカード取得部 302 から取得したカード情報を、図 6 を用いて説明したカード情報取得段階 (S122) において携帯電話 20 に送信したが、これにかえて、カードリーダ識別情報送信段階 (S206) において、カードリーダ識別情報と共に携帯電話 20 に送信してもよい。

S204において、通信部 340 から取得した携帯電話識別情報が接続先保持部

310に保持される接続先携帯電話識別情報と異なる場合、許可部306は、カードリーダ識別情報を送信することを禁止する(S210)。この場合、カードリーダ30の動作は終了する(S212)。このように、カードリーダ30は、接続先保持部310に保持される接続先携帯電話識別情報で識別される携帯電話20以外の携帯電話20には、カード情報を送信しない。従って、第三者は、自己の携帯する携帯電話20を利用して、カードリーダ30を不正に利用するのを防ぐことができる。

図8は、図6におけるレジサーバ100の携帯電話認証段階(S106)におけるレジサーバ100の詳細な動作を示すフローチャートである。レジサーバ100は、携帯電話20からインターネット10を介して携帯電話識別情報及び／又はユーザ識別情報を取得し(S300)、かつ携帯電話20からカードリーダ識別情報を取得する(S302)。さらに、レジサーバ100は、さらに携帯電話20の位置を検出する(S304)。

次に、レジサーバ100の認証部108は、携帯電話データベース120を利用し、インターネット通信部102を介して受信した携帯電話識別情報及び／又はユーザ識別情報、カードリーダ識別情報、及び位置情報の組み合わせを認証する(S306)。ここでの組合せは、これらの項目のうちの任意の組合せであってもよい。認証部108が認証に成功した場合(S308)、認証部108は、携帯電話20から商品データベース120のアクセスを許可する。S308において、認証部108が認証に成功しない場合は、取引は中止し、動作は終了する(S310)。このように、レジサーバ100は、携帯電話識別情報及び／又はユーザ識別情報、カードリーダ識別情報、及び位置情報の組み合わせに基づいて、販売者を認証するので、より精度の高い認証を行うことができる。

図9は、図6において説明した商品選択段階(S112)における携帯電話20の詳細な動作を示すフローチャートである。携帯電話20は、商品データベース120へのアクセスが許可されると、インターネット10を介して取引の対象となる商品に関する情報をレジサーバ100から受信する(S400)。次に、所定の取引内容をレジサーバ100に送信する(S402)。次に、取引に対する購入金額をレジサーバ100から受信する(S406)。このように、レジサーバ100において、携帯電話20及びカードリーダ30の認証が成功すると、携帯電話20は、レジサ

ーバ100の商品データベース120にアクセスすることができる。

図10は、図6において説明したカード情報及び暗証番号取得段階(S122)における携帯電話20及びカードリーダ30の詳細な動作を示すフローチャートである。カードリーダ30は、カード情報を読み取る(S500)。次に、リーダ暗号化部330は、リーダ識別情報を利用してカード情報を暗号化し(S502)、さらに取引回数を利用して、カード情報を暗号化する(S504)。

このように、カードリーダ20は、暗号化した後のカード情報を携帯電話20に送信するので、携帯電話20は、カード情報を復号化することができない。従って、カード情報が漏洩するのを防ぐことができる。

10 次に、通信部340は、暗号化されたカード情報を携帯電話20に送信する(S506)。携帯電話20のリーダ通信部202は、暗号化されたカード情報を受け取る。次に、携帯電話20の入力部204は、ユーザからカードの暗証番号を受け付ける(S508)。このように、携帯電話20を利用して、暗証番号を取得することができる。

15 次に、端末暗号化部230は、携帯電話識別情報を利用して、リーダ通信部202から受け取ったカード情報、及び入力部204から受け取った暗証番号を暗号化する(S510)。次に、インターネット通信部210から受け取った取引番号を利用して、カード情報及び暗証番号を暗号化する。

20 このように、携帯電話20から送信されるカード情報は、カードリーダ20及び携帯端末30で、各装置固有の情報などを利用して暗号化されるので、不正に情報を取得した第三者に解読される可能性が少ない。

一方、カードリーダ30は、S506においてカード情報を送信すると、回数保持部324に保持される取引回数を1増加する(S520)。回数保持部324は、その後通信部340を介して、レジサーバ100がカード情報の受取を拒否したことと示す受け取り拒否情報を受け取った場合(S522)、保持される取引回数を1減じる。

このように、取引回数は、カード情報を送信する毎に変更される情報である。従って、取引回数を利用して暗号化することによって、より安全にカード情報を暗号化することができる。

図11は、図6において説明した決済処理段階(S134)におけるレジサーバ100の詳細な動作を示すフローチャートである。レジサーバ100は、携帯電話20から取引内容を受信すると(S600)、受信したカード情報及び会計情報をカード会社サーバ400へ送信する(S602)。次に、レジサーバ100は、送信に対する返信として、取引内容についての決済が完了したことを示す決済確認情報を受信する(S604)。

図12は、カードリーダ20において不正処理が行われた場合の、カードリーダ30、携帯電話20、及びレジサーバ100の通信シーケンスを示す。カードリーダ30の不正処理監視部360は、常に不正処理を監視する。不正処理監視部360が不正処理を検出した場合に(S900)、送信部362は、通信部340に対して、カード情報の送信を禁止する(S902)。次に、通信部340は、本カードリーダ30を認証する認証要求を接続されている携帯電話20に送る(S904)。次に、携帯電話20は、受け取った認証要求をレジサーバ100に送信する(S906)。すなわち、カードリーダ20は、カード情報の送信が禁止された場合に、カード情報の送信を許可するために必要な情報をレジサーバ100に要求する。

次に、レジサーバ100は、認証要求を受信する。認証要求取得部114は、認証要求に含まれるカードリーダ識別情報を利用して認証要求の送信元であるカードリーダ30を特定する。

次に、認証部108は、カードリーダデータベース122を利用して、認証要求の送信元であるカードリーダ30の認証情報を選択する(S912)。次に、認証部108は、カードリーダデータベース122を利用して、認証要求の送信元であるカードリーダ30に対応付けられている携帯電話20を選択する(S914)。次に、インターネット通信部102は、カードリーダ20の認証情報を、選択した携帯電話20に送る(S916)。

次に、携帯電話20のリーダ通信部202は、認証情報を受信する。次に、表示部206は、受信した認証情報を表示する(S920)。

次に、カードリーダ30の利用者は、携帯電話20の表示部206に表示された認証情報をテンキー350から入力する(S930)。認証情報が入力されると、カードリーダ30のカードリーダ認証部366は、入力された認証情報と、認証情報

保持部 364 に保持される認証情報と比較し、一致した場合に、認証成功と判断する (S932)。この場合、許可部 306 は、通信部 340 に対してカード情報の送信を許可する (S934)。なお、S932において、カードリーダ認証部 366 がカードリーダ 30 の認証に成功しない場合、カード情報の送信は禁止されたままである。以上で、カードリーダ 30 において不正処理が行われた場合の、各装置の動作は終了する。

10 このように、レジサーバ 100 は、カードリーダ 30 の認証情報を、カードリーダ 30 に対応付けられた携帯電話 20 に送る。従って、カードリーダ 30 を不正に取得した第三者が利用していた場合、カードリーダ 30 に対応付けられた携帯電話 20 を所有していない限り、認証情報を取得することができない。従って、第三者が不正に利用するのを防ぐことができる。

またこのように、カードリーダ 30 が、一方向通信しか行えなくとも、ユーザは、携帯電話 20 に送信された認証情報をカードリーダ 30 のテンキー 350 を介して入力するので、カードリーダ 30 の認証を行うことができる。

15 また他の例としては、レジサーバ 100 及びカードリーダ 30 がそれぞれ複数の認証情報を保持している場合、カードリーダ 30 は、複数のうちの任意の 1 つの認証情報をを利用して認証してもよい。

なお、認証情報は、カードリーダ 30 をレジサーバ 100 に登録するとき、すなわち、カードリーダ 30 の情報を、カードリーダデータベース 122 に登録するときに、設定してもよい。また、カードリーダ 30 のユーザは、カードリーダ 30 の認証情報保持部 364 に保持される認証情報を知ることができない。

図 13 は、レジサーバ 100 のハードウェア構成を示す図である。レジサーバ 100 は、CPU 700 と、ROM 702 と、RAM 704 と、通信インターフェース 706 と、ハードディスクドライブ 708 と、データベースインターフェース 710 と、フロッピーディスクドライブ 712 と、CD-ROM ドライブ 714 とを備える。CPU 700 は、ROM 702 及び RAM 704 に格納されたプログラムに基づいて動作する。通信インターフェース 706 は、インターネット 10 を介して外部と通信する。データベースインターフェース 710 は、データベースへのデータの書込、及びデータベースの内容の更新を行う。格納装置の一例としてのハードディス

クドライブ 708 は、設定情報及び CPU 700 が動作するプログラムを格納する。

フロッピーディスクドライブ 712 はフロッピーディスク 720 からデータまたはプログラムを読み取り CPU 700 に提供する。CD-ROM ドライブ 714 は

CD-ROM 722 からデータまたはプログラムを読み取り CPU 700 に提供す

る。通信インターフェース 706 は、インターネット 10 に接続してデータを送受信する。データベースインターフェース 710 は、各種データベース 724 と接続してデータを送受信する。

CPU 700 が実行するソフトウェアは、フロッピーディスク 720 または CD

– ROM 722 等の記録媒体に格納されて利用者に提供される。記録媒体に格納さ

れたソフトウェアは圧縮されていても非圧縮であってもよい。ソフトウェアは記録媒体からハードディスクドライブ 708 にインストールされ、RAM 704 に読み出されて CPU 700 により実行される。

記録媒体に格納されて提供されるソフトウェア、即ちハードディスクドライブ 7

08 にインストールされるソフトウェアは、機能構成として、インターネット通信

モジュールと、商品情報抽出モジュールと、決済モジュールと、認証モジュールと、  
カード会社通信モジュールとを有する。前記各モジュールがコンピュータに働きかけて、CPU 700 に行わせる処理は、それぞれ本実施形態のレジサーバ 100 における、対応する部材の機能及び動作と同一であるから、説明を省略する。

図 13 に示した、記録媒体の一例としてのフロッピーディスク 720 または CD

– ROM 722 には、本出願で説明した全ての実施形態におけるレジサーバ 100 の動作の一部または全ての機能を格納することができる。

これらのプログラムは記録媒体から直接 RAM に読み出されて実行されても、一旦ハードディスクドライブにインストールされた後に RAM に読み出されて実行さ

れても良い。更に、上記プログラムは单一の記録媒体に格納されても複数の記録媒

体に格納されても良い。又、符号化した形態で格納されていてもよい。

記録媒体としては、フロッピーディスク、CD-ROM の他にも、DVD 等の光

光学記録媒体、MD 等の磁気記録媒体、PD 等の光磁気記録媒体、テープ媒体、磁気

記録媒体、IC カードやミニチュアーカードなどの半導体メモリー等を用いること

ができる。又、専用通信ネットワークやインターネットに接続されたサーバシステ

ムに設けたハードディスクまたはRAM等の格納装置を記録媒体として使用し、通信網を介してプログラムをレジサーバ100に提供してもよい。このような記録媒体は、レジサーバ100を製造するためのみに使用されるものであり、そのような記録媒体の業としての製造および販売等が本出願に基づく特許権の侵害を構成する  
5 ことは明らかである。

なお、携帯電話20において、記録媒体に格納されて提供されるソフトウェア、即ちハードディスクドライブ708にインストールされるソフトウェアは、機能構成として、取得モジュールと、送信モジュールと、入力モジュールと、受信モジュールと、表示モジュールとを有する。カードリーダ30において、記録媒体に格納  
10 されて提供されるソフトウェア、即ちハードディスクドライブ708にインストールされるソフトウェアは、機能構成として、カード読み取りモジュールと、送信モジュールと、許可モジュールと、接続モジュールとを有する。各モジュールがコンピュータに働きかけて、CPU700に行わせる処理は、それぞれ本実施形態の携帯電話20及びカードリーダ30における、対応する部材の機能及び動作と同一である  
15 から、説明を省略する。

図13に示した、記録媒体の一例としてのフロッピーディスク720またはCD-ROM722には、本出願で説明した全ての実施形態における携帯電話20及びカードリーダ30それぞれの動作の一部または全ての機能を格納することができる。

図14は、第2実施形態における電子決済システム全体を示す図である。本実施  
20 の形態の電子決済システムは、レジサーバ100、携帯電話20、カードリーダ30に加えて、さらに携帯電話20及びカードリーダ30を接続する接続装置40を備える。この点で、本実施の形態の電子決済システムは、第1実施形態における電子決済システムと異なる。接続装置40は、カードリーダ接続部402を介してカードリーダ30に接続し、携帯電話接続部404を介して携帯電話20に接続する。  
25 接続装置40は、カードリーダ接続部402を介してカードリーダ30と各種情報を送受信する。接続装置40はまた、携帯電話接続部404を介して、携帯電話20と各種情報を送受信する。以下、本実施形態の接続装置40について詳述する。

図15及び図16は、本実施の形態におけるカードリーダ30及び接続装置40の機能構成を示すブロック図である。図15は、カードリーダ30の機能構成を示

すブロック図である。図16は、接続装置40の機能構成を示すブロック図である。

カードリーダ30は、カード読取部302と、通信部340と、接続部320とを備える。なお、カードリーダ30のこれらの構成及び動作は、図5を用いて説明した第1実施形態におけるカードリーダ30における同一名の部分の構成及び動作と同様なので説明を省略する。このように、本実施の形態におけるカードリーダ30は、第1実施形態におけるカードリーダ30に比べて簡易な機能を有する。

接続装置40は、カードリーダ接続部402と、カードリーダ通信部420と、携帯電話接続部404と、携帯電話通信部422と、接続装置暗号化部430と、接続装置識別情報保持部432と、回数保持部434と、接続先認証部406と、接続先識別情報保持部408と、許可部410とを備える。

なお、本実施の形態における「カードリーダ通信部420及び携帯電話通信部422」は、特許請求の範囲に記載の「転送部」の一例である。

カードリーダ接続部402は、カードリーダ30と接続する。カードリーダ通信部420は、カードリーダ接続部402を介してカードリーダ30と各種情報を送受信する。カードリーダ通信部420は、カード情報を受け取り、接続装置暗号化部430に送る。カードリーダ通信部420はまた、カードリーダ識別情報をカードリーダ30から受信する。

接続装置識別情報保持部432は、本接続装置40を識別する接続装置識別情報を保持する。回数保持部424は、携帯電話通信部422がカード情報を送信した回数を取引回数として保持する。接続装置暗号化部430は、カードリーダ通信部420から受け取ったカード情報を暗号化する。接続装置暗号化部430及び回数保持部424の構成及び動作は、それぞれ図4を用いて説明した第1実施形態におけるカードリーダ30におけるリーダ暗号化部330及び回数保持部324の構成及び動作と同様である。

携帯電話接続部404は、携帯電話20と接続する。携帯電話通信部422は、携帯電話接続部404を介して、各種情報を送受信する。携帯電話通信部422は、接続装置暗号化部430から暗号化後のカード情報を受け取り、携帯電話20に送信する。携帯電話通信部422は、さらに、カードリーダ通信部420からカードリーダ識別情報を受け取り、これを送信する。

接続先保持部 408 は、カードリーダ接続部 402 が接続すべきカードリーダ 30 のカードリーダ識別情報を保持する。接続先保持部 408 は、さらに携帯電話接続部 404 が接続すべき携帯電話 20 の携帯電話識別情報を保持する。

接続先認証部 406 は、携帯電話接続部 404 が携帯電話 20 に接続された場合 5 に、携帯電話接続部 404 を介して、携帯電話 20 から携帯電話識別情報を取得する。接続先認証部 406 は、取得した携帯電話識別情報と、接続先保持部 408 に保持される携帯電話識別情報を照合し、接続された携帯電話 20 を認証する。

接続先認証部 406 は、さらにカードリーダ接続部 402 が携帯電話 20 に接続された場合に、カードリーダ接続部 402 を介して、カードリーダ 40 からカードリ 10 ーダ識別情報を取得する。接続先認証部 406 は、取得したカードリーダ 30 からカードリーダ識別情報と、接続先保持部 408 に保持されるカードリーダ識別情報とを照合し、接続されたカードリーダ 30 を認証する。

許可部 410 は、接続先認証部 406 が、接続先の認証に成功した場合に、携帯電話通信部 422 に対して、カードリーダ識別情報及びカード情報を携帯電話 20 15 に転送することを許可する。

このように、本実施の形態における接続装置 40 は、携帯電話 20 及びカードリーダ 30 の認証に成功した場合に、カード情報を転送を信許可するので、カード情報の漏洩を防止することができる。また、本実施の形態においては、接続装置暗号化部 430 がカード情報を暗号化する。従って、接続装置 40 は、第 1 実施形態におけるカードリーダ 30 と同様に、携帯電話 20 に対して、暗号化した後のカード情報を探信することができる。

また、携帯電話 20 の入力部 204 は、第 1 の実施形態と同様に、携帯電話 20 のユーザ識別情報又はカードリーダ 30 のユーザ識別情報を取得し、インターネット通信部 210 を介して、インターネット 10 に接続している他の機器に送信して 25 もよい。

図 17 は、本実施の形態における接続装置 40 の動作を示すフローチャートである。本図は、第 1 実施形態において説明した、通信シーケンスにおけるカードリーダ識別情報取得段階 (S102) における接続装置 40 の動作を示す。

接続装置 40 のカードリーダ接続部 402 に、カードリーダ 30 が接続されると

(S 700)、接続先認証部406は、カードリーダ接続部402を介して、接続されたカードリーダ30のカードリーダ識別情報を取得する。接続先認証部406は、接続先識別情報保持部408に格納されるカードリーダ識別情報と、カードリーダ30から取得したカードリーダ識別情報とを照合する。カードリーダ30から取得したカードリーダ識別情報が、接続先識別情報保持部408に保持されるカードリーダ識別情報と一致しない場合(S 702)、カードリーダ識別情報及びカード情報の、携帯電話20への送信が禁止される(S 720)。次に、カードリーダ30を利用した取引は中止する(S 722)。

S 702において、接続先認証部406が、カードリーダ30の認証に成功した場合は、さらに携帯電話20が接続されるまで待機する。携帯電話接続部404に携帯電話20が接続されると(S 704)、接続先認証部406は、携帯電話接続部404を介して携帯電話識別情報を取得する。接続先認証部406は、接続先識別情報保持部408に格納される携帯電話識別情報と、携帯電話20から取得した携帯電話識別情報を照合する。携帯電話20から取得した携帯電話識別情報が、接続先識別情報保持部408に保持される携帯電話識別情報と一致しない場合(S 706)、S 720へジャンプする。

S 706において、接続先認証部406が、携帯電話20の認証に成功した場合は、許可部410は、携帯電話通信部422に対して、カード情報及びカードリーダ識別情報を、携帯電話20に送信することを許可する(S 708)。次に、転送部414は、カード識別情報を、携帯電話20に送信する(S 710)。以上で、接続装置40の動作は終了する。

そして、携帯電話20は、ユーザ識別情報を取得して、接続装置40から受信した情報と共に、レジサーバ100に送信する。

このように、許可部410は、接続装置40に接続されたカードリーダ30及び携帯電話20の認証に成功した場合に、カード情報の送信を許可する。従って、第三者が、不正にカードリーダ30及び携帯電話20を利用するのを防ぐことができる。

図18は、本実施の形態におけるカードリーダ30、接続装置40、及び携帯電話20の詳細な動作を示すフローチャートである。本図は、第1実施形態において

図5を用いて説明した、通信シーケンスにおけるカードリーダ識別情報取得段階(S 102)におけるカードリーダ30、接続装置40、及び携帯電話20の動作を示す。

はじめに、カードリーダ30のカード読取部302は、カード情報を読み取る(S 800)。次に、通信部320は、カード情報を接続装置40に送信する(S 802)。接続装置40のカードリーダ通信部420は、カード情報を受信する。以下、接続装置40のS 814からS 822における動作は、第1実施形態において図9を用いて説明したカードリーダ30のS 502からS 522における動作と同様である。また、携帯電話20のS 810からS 814における動作は、第1実施形態において図9を用いて説明した携帯電話20のS 508からS 512における動作とと同様である。

本実施の形態における電子決済システムにおけるレジサーバ100、携帯電話20、及びカードリーダ30のこれ以外の構成及び動作は、第1実施形態におけるレジサーバ100、携帯電話20、及びカードリーダ30の構成及び動作と同様なので説明を省略する。

このように、本実施の形態においては、接続装置40及び携帯電話20がそれぞれカード情報を暗号化することができる。

なお、第1実施形態において説明した携帯電話20及びカードリーダ30は、販売者が携帯し、例えば、購入者の自宅において取引を行う場合に利用されるが、これにかえて、携帯電話20及びカードリーダ30は、各購入者が所持してもよい。この場合、レジサーバ100のカードリーダデータベース122の販売者名フィールドは、販売者の名前にかえて、購入者の名前を格納する。また、パスワードフィールドは、購入者が入力すべきパスワードを格納する。これによって、購入者は、所持する携帯電話20及びカードリーダ30を利用して、容易にカードによる取引を行うことができる。さらに他の例としては、電子決済システムは、販売者が所持する携帯電話20と購入者が所持するカードリーダ30とを利用した取引を行ってもよい。

同様に、第2実施形態において説明した携帯電話20、カードリーダ30、及び接続装置40は、販売者が所持してもよく、また他の例としては、例えば購入者が

所持してもよい。さらに他の例としては、電子決済システムは、購入者が所持する携帯電話20と、販売者が所持する接続装置40及びカードリーダ30を利用した取引を行ってもよい。このように、携帯電話20、カードリーダ30、及び接続装置40は、販売者及び購入者のいずれが所持してもよく、予め、設定された組み合  
5 わせが満たされればよい。

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることができる。その様な変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

10 こうした第1の変更例を説明する。図19は、第1実施形態におけるカードリーダ30の変更例である。本例におけるカードリーダ30は、第1実施形態におけるカードリーダ30の構成に加えて、通信先保持部350及び通信確立部352をさらに備える。通信先保持部350は、接続すべき携帯電話20が通信すべき通信先を指定する通信先情報を含み、通信先情報が示す通信先と携帯電話20との通信を確立させるプログラムを保持する。すなわち、通信先保持部312は、レジサーバ100と携帯電話20との通信を確立させるプログラムを保持する。通信確立部352は、通信先保持部が保持するプログラムを起動し、接続部320に接続される携帯電話20と、レジサーバ100との通信を確立する。  
15

本例における許可部306は、接続先認証部308が接続先の認証に成功した場合に、通信確立部352に対して、通信確立プログラムの実行を許可する。このように、本例においても、携帯電話20の認証に成功した場合に、携帯電話20とレジサーバ100との通信が確立する。従って、携帯電話20からレジサーバ100への不正なアクセスを防ぐことができる。

本例においては、第1実施形態で図7を用いて説明した送信許可段階(S206)で、カードリーダ識別情報及びカード情報の送信が許可されると、通信確立部352は、通信先保持部350に保持されるプログラムを利用して、携帯電話20とレジサーバ100との通信を確立する。すなわち、接続先認証部308が、携帯電話識別情報と、接続先保持部310に保持される接続先携帯電話識別情報の照合に成功した場合に、携帯電話20とレジサーバ100との通信が自動的に確立される。

このように、認証に成功した場合、携帯電話 20 とレジサーバ 100 との通信が自動的に確立する。従って、購入者及び販売員は、レジサーバ 100 の通信アドレスを知る必要がない。従って、携帯電話 20 からレジサーバ 100 へ不正にアクセスするのを防ぐことができる。なお、この場合、レジサーバ 100 は、携帯電話 20  
5 に対して、通信要求を送信しなくともよい。

図 20 は、第 2 実施形態における接続装置 40 の変更例である。本実施の形態における第 2 実施形態の接続装置 40 は、通信先保持部 450 及び通信確立部 452 をさらに備える。なお、通信先保持部 450 及び通信確立部 452 の構成及び動作は、それぞれ第 1 実施形態におけるカードリーダ 30 の第 1 の変更例における通信  
10 先保持部 350 及び通信確立部 352 の構成及び動作と同様なので説明を省略する。

第 2 の変更例としては、本実施の形態における電子決済システムは、レジサーバ 100 及びカード会社サーバ 400 と専用回線を介して通信するシンクロサーバをさらに備えてもよい。この場合、レジサーバ 100 は、シンクロサーバを介してカード会社サーバ 400 と通信する。これによって、カード会社サーバ 400 と送受  
15 信する、カード所有者の個人情報が漏洩するのを防ぐことができる。また、この場合、シンクロサーバは、カード情報をうけとり、カード情報に基づいて、通信要求を作成してもよい。このように、レジサーバ 100 の機能の一部をシンクロサーバに持たせてもよい。

第 3 の変更例としては、本実施の形態におけるカードリーダデータベース 122  
20 は、1 つの携帯電話識別情報に、1 つのカードリーダ識別情報が対応付けて格納されていたが、これにかえて、1 つの携帯電話識別情報に、複数のカードリーダ識別情報が対応付けられていてもよい。これによって、1 カ所の店舗から配布されている複数のカードリーダを、一人の販売者が利用する場合において一人の販売者は販売元の店舗で配布されたすべてのカードリーダを利用することができる。

25 また他の例としては、カードリーダデータベース 122 は、1 つのカードリーダ識別情報に、複数の携帯電話識別情報を対応付けて格納してもよい。また他の例としては、カードリーダデータベース 122 は、複数の携帯電話識別情報に、複数のカードリーダ識別情報をそれぞれ対応付けて格納してもよい。

この場合、カードリーダ 30 の接続先保持部 310 は、それぞれ、レジサーバ 1

00のカードリーダデータベース122において、カードリーダ30に対応付けられている携帯電話20の携帯電話識別情報を格納する。従って、接続先保持部310は、1つまたは複数の携帯電話識別情報を格納する。

第4の変更例としては、本実施の形態においては、カードリーダ30は、接続部5320に接続された携帯電話20の携帯電話識別情報が、予め指定された携帯電話識別情報と一致しない場合に、カード情報の送信を禁止したが、カード情報の送信を禁止するのにかえて、カード情報の読み取りを禁止してもよい。いずれにせよカードリー30は、カード情報を不正に送信するのを防ぐことができる。

第5の変更例としては、第2実施形態においては、接続装置40の接続先認証部10406が、カードリーダ30及び携帯電話20の認証に成功した場合に、許可部410は、カードリーダ識別情報及びカード情報の送信を許可した。これにかえて、接続先認証部406が、携帯電話20の認証に成功した場合に、許可部410は、カードリーダ識別情報及びカード情報の携帯電話20への送信を許可してもよい。これによって、例えば第三者が、所持する携帯電話20を利用して、他人の接続装置40を利用して、取引を行うのを防ぐことができる。

また例えば、購入者が、携帯電話20及び接続装置40を所持し、販売員がカードリーダ30を所持している場合、接続装置40は、次のような認証を行ってもよい。すなわち、接続先認証部406が、カードリーダ20の認証に成功した場合に、許可部410は、カードリーダ識別情報及びカード情報の携帯電話20への送信を許可してもよい。これによって、接続装置40は、予め登録された販売員の所持するカードリーダ30のみ認証するので、不正に販売を行う第三者との取引を防止することができる。

第6の変更例としては、本実施の形態においては、カードの暗証番号は、携帯電話20のプッシュボタンを介して入力されたが、これにかえて、カードリーダ30から入力されてもよい。入力された、暗証番号は、接続部320を介して携帯電話20に送られてもよい。

第7の変更例としては、本実施の形態においては、カードリーダ30は、カードリーダ識別情報を利用してカード情報を暗号化し、携帯電話20は、携帯電話識別情報を利用してカード情報を暗号化したが、これにかえて、カードリーダ30が、

カードリーダ識別情報及び携帯電話識別情報をを利用してカード情報を暗号化してもよい。なお、この場合、カードリーダ30は、通信部340を介して携帯電話20から取得した携帯電話識別情報をを利用して、カード情報を暗号化する。このように、カード情報の暗号化を担当する装置は、本実施の形態に限定されるものではない。

5 また他の例としては、本実施の形態においては、携帯電話20が取引識別情報を利用して、カード情報を暗号化したが、これにかえて、カードリーダ30は、テンキー350を介して取得した取引識別情報をを利用してカード情報を暗号化してもよい。

10 また他の例としては、第2実施形態におけるカード情報は、接続装置識別情報及び携帯電話識別情報をを利用して暗号化されたが、カード情報は、接続装置識別情報及び携帯電話識別情報に加えて、携帯電話識別情報をを利用して暗号化されてもよい。このように、カード情報は、カードリーダ識別情報、接続装置識別情報、及び携帯電話識別情報の少なくとも2つの情報をを利用して暗号化されてもよい。

15 第8の変更例としては、本実施の形態における取引端末は、携帯電話20であつたが、これにかえて取引端末は、パーソナルコンピュータや、PDA（Personal Digital Assistant）であつてもよい。

20 第9の変更例としては、本実施の形態においては、レジサーバ100は、取引識別情報をインターネット10を介して携帯端末20に送信したが、これにかえて、レジサーバ100は、取引識別情報を含むレシートを発行してもよい。この場合、カードリーダ30を利用する販売員は、レシートに含まれる取引識別情報をテンキー350から入力する。さらにこの場合、カードリーダ30は取引識別情報をを利用してカード情報を暗号化してもよい。すなわち、取引識別情報を携帯端末20に通知しない。これによって、カードリーダ30は、携帯端末20に知られていない情報をを利用してカード情報を暗号化することができる。すなわち、携帯端末20にカード情報を復号化させる情報が残らないので、カード情報の漏洩を避けることができる。

## 産業上の利用可能性

以上の説明から明らかなように、本発明によれば、商品の取引における決済を、

ネットワークを介して、安全かつ簡便に行うことができる。

## 請求の範囲

1. 取引の決済を行う決済サーバを含む電子決済システムであって、

前記取引の決済に利用するカードからカード情報を読み取るカードリーダと、

5 前記カードリーダに接続し、前記カードリーダから取得した前記カード情報を、

前記決済サーバに送信する取引端末と

を備え、

前記取引端末は、前記取引端末に接続した前記カードリーダを識別するカードリーダ識別情報と、前記取引端末のユーザを識別するユーザ識別情報若しくは前記カ

10 ラードリーダのユーザを識別するユーザ識別情報及び前記取引端末を識別する取引端末識別情報の少なくとも一方と、を前記決済サーバに送信し、

前記決済サーバは、前記カードリーダ識別情報と、及び前記ユーザ識別情報及び前記取引端末識別情報の少なくとも一方と、の組み合わせに基づいて、前記取引端末の認証を行い、前記認証に成功した場合に、前記通信ネットワークを介して前記取引端末から受信した前記カード情報をを利用して決済処理を行うことを特徴とする電子決済システム。

2. 前記決済サーバは、前記取引端末の認証に成功した場合に、前記取引端末との通信を要求する通信要求を前記取引端末に送信し、

前記取引端末は、前記通信要求を受信すると、当該通信要求に対する返信として、

20 前記カードリーダから取得した前記カード情報を前記決済サーバに送信し、

前記決済サーバは、前記通信要求の返信として受信した前記カード情報を利用して決済処理を行うことを特徴とする請求項1に記載の電子決済システム。

3. 前記取引端末は、携帯電話であって、

前記取引端末識別情報は、前記携帯電話の電話番号であることを特徴とする請求

25 項1に記載の電子決済システム。

4. 取引の決済を行う決済サーバを含む電子決済システムであって、

前記取引の決済に利用するカードからカード情報を読み取るカードリーダと、

前記カードリーダから前記カード情報を取得し、前記カード情報を前記決済サーバに送信する取引端末と

を備え、

前記取引端末は、前記カードリーダを識別するカードリーダ識別情報及び前記取引端末を識別する取引端末識別情報を利用して暗号化された前記カード情報を前記決済サーバに送信し、

5 前記決済サーバは、前記取引端末識別情報及び前記カードリーダ識別情報を利用して、前記カード情報を復号化することを特徴とする電子決済システム。

5. 取引の決済を行う決済サーバを含む電子決済システムであって、

前記取引の決済を利用するカードからカード情報を読み取るカードリーダと、

前記カードリーダから前記カード情報を取得し、前記カード情報を前記決済サーバに送信する取引端末と

を備え、

前記決済サーバは、前記取引を識別する取引識別情報を発行し、

前記カードリーダは、前記決済サーバが発行した前記取引識別情報を取得し、取得した前記取引識別情報をを利用して、前記カード情報を暗号化し、

15 前記取引端末は、暗号化後の前記カード情報を前記決済サーバに送信し、

前記決済サーバは、発行した前記取引識別情報をを利用して、前記カード情報を復号化することを特徴とする電子決済システム。

6. 取引の決済を行う決済サーバを含む電子決済システムであって、

前記取引の決済を利用するカードからカード情報を読み取るカードリーダと、

20 前記カードリーダから取得した前記カード情報を、前記決済サーバに送信する取引端末と、

前記カードリーダと前記取引端末とを接続する接続装置と

を備え、

前記取引端末は、前記カードリーダを識別するカードリーダ識別情報、前記取引端末を識別する取引端末識別情報若しくは前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報、及び前記取引端末に接続した前記接続装置を識別する接続装置識別情報、及びのうち少なくとも2つを前記決済サーバに送信し、

前記決済サーバは、前記カードリーダ識別情報、前記取引端末識別情報若しくは

前記ユーザ識別情報、及び前記接続装置識別情報のうち少なくとも2つの組み合わせに基づいて、前記取引端末の認証を行い、前記認証に成功した場合に、前記通信ネットワークを介して前記取引端末から受信した前記カード情報をを利用して決済処理を行うことを特徴とする電子決済システム。

- 5 7. 取引端末における取引の決済を行う決済サーバであって、  
前記取引端末を識別する取引端末識別情報及び前記取引端末又は前記カードリーダのユーザを識別するユーザ識別情報の少なくとも一方を受信とともに、前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を、前記取引端末を介して受信する受信部と、
- 10 10. 前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報の組み合わせに基づいて、前記取引端末を認証する認証部と、  
前記認証に成功した場合に、前記取引端末を介して前記カードリーダから受信した前記カード情報をを利用して、前記決済処理を行う決済部と  
を備えることを特徴とする決済サーバ。
- 15 8. 前記認証部が、前記取引端末の認証に成功した場合に、前記受信部は、前記取引端末を介して前記カードリーダが読み取った前記カード情報を受信することを特徴とする請求項7に記載の決済サーバ。
9. 前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報とを対応付けて格納するカードリーダデータベースをさらに備  
20 え、  
前記認証部は、前記カードリーダデータベースにおいて対応付けられた、前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報との組み合わせを利用して、前記取引端末を認証することを特徴とする請求項7記載の決済サーバ。
- 25 10. 前記認証部が前記取引端末の認証に成功した場合に、前記取引端末との通信を要求する通信要求を前記取引端末に送信する送信部をさらに備え、  
前記受信部は、前記通信要求に対する返信として前記カード情報を受信することを特徴とする請求項7に記載の決済サーバ。  
11. 前記受信部は、さらに前記取引の内容を示す取引内容を前記取引端末から

受信し、

前記送信部は、前記取引内容を識別可能に、前記取引端末に前記通信要求を送信し、

前記受信部が前記通信要求に対する返信を受信した場合に、前記決済部は、前記  
5 取引識別情報に対応する前記取引内容について、決済処理を行うことを特徴とする  
請求項 10 に記載の決済サーバ。

12. 前記決済サーバは、複数の前記取引端末における取引の決済を行い、

前記認証部は、前記取引端末識別情報及び前記カードリーダ識別情報の組合せに基づいて前記取引端末を認証し、

10 前記カードリーダデータベースは、前記取引端末識別情報と、前記カードリーダ識別情報とを対応付けて格納するとともに、前記取引端末識別情報に対応付けて、前記取引の決済の支払先を示す支払先識別情報をさらに格納し、

前記決済部は、前記カードリーダデータベースにおいて、前記取引端末識別情報に対応付けて格納される前記支払先に対して決済処理を行うことを特徴とする請求  
15 項 9 に記載の決済サーバ。

13. 取引を行う取引端末における取引を決済する決済サーバであって、

前記取引端末を識別する取引端末識別情報、及び前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を利用して暗号化されたカード情報を前記取引端末から受信する受信部と、

20 前記カードリーダと、前記カードリーダが前記カード情報を送信すべき取引端末とを対応付ける装置管理テーブルと、

前記受信部が前記取引端末から前記カード情報を受信した場合、前記取引端末識別情報、及び前記装置管理テーブルにおいて前記取引端末に対応付けられた前記カードリーダの前記カードリーダ識別情報を利用して、前記カード情報を復号化する  
25 復号化部と

を備えることを特徴とする決済サーバ。

14. 取引の支払に利用するカードのカード情報を読み取るカードリーダであつて、

前記カード情報を読み取るカード読取部と、

取引端末に接続する接続部と、

前記接続部を介して前記カード情報を前記取引端末に送信する送信部と  
を備えることを特徴とするカードリーダ。

15. 前記接続部が、前記取引端末に接続した場合に、前記接続部を介して前記  
5 取引端末を識別する取引端末識別情報を読み取る接続先認証部と、

前記接続先認証部が読み取った前記取引端末識別情報と予め定められた取引端末  
識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許  
可する許可部と

をさらに備えることを特徴とする請求項14に記載のカードリーダ。

10 16. 前記取引端末が通信すべき通信先を指定する通信先情報を保持する通信先  
保持部と、

前記接続先認証部が読み取った前記取引端末識別情報と予め定められた前記取引  
端末識別情報とが一致した場合に、前記通信先保持部に保持される前記通信先情報  
を利用して、前記取引端末と前記通信先との通信を確立する通信確立部と

15 をさらに備えることを特徴とする請求項15に記載のカードリーダ。

17. 前記送信部は、さらに当該カードリーダを識別するカードリーダ識別情報を  
前記取引端末に送信することを特徴とする請求項14に記載のカードリーダ。

18. 前記取引端末は携帯電話であって、

前記接続先認証部は、前記携帯電話の電話番号を前記取引端末識別情報として読  
み取ることを特徴とする請求項15に記載のカードリーダ。

19. 前記カード読取部が読み取ったカード情報を、暗号化する暗号化部をさら  
に備え、

前記送信部は、前記暗号化部が暗号化した後の前記カード情報を前記取引端末に  
送信することを特徴とする請求項14に記載のカードリーダ。

20. 前記暗号化部は、当該カードリーダを識別するカードリーダ識別情報を利  
用して、前記カード情報を暗号化することを特徴とする請求項19に記載のカード  
リーダ。

21. 前記送信部が前記カード情報を送信した回数を保持する回数保持部をさら  
に備え、

前記暗号化部は、前記回数保持部に保持される回数を利用して、前記カード情報を暗号化することを特徴とする請求項 20 に記載のカードリーダ。

22. 前記回数を減じることを示す情報を受信する受信部をさらに備え、

前記受信部が前記情報を受信した場合に、前記回数保持部は、保持する回数を減

5 じることを特徴とする請求項 21 に記載のカードリーダ。

23. 取引の決済を行う決済サーバと通信ネットワークを介して通信する端末システムであって、

前記取引を利用するカードのカード情報を読み取るカードリーダと、

前記カード情報を前記決済サーバに送信する取引端末と

10 を備え、

前記カードリーダは、

前記カード情報を読み取るカード読取部と、

前記取引端末に接続する前記接続部と、

前記接続部を介して前記カード情報を前記取引端末に送信する送信部と

15 を有し、

前記取引端末は、

前記カードリーダの前記接続部を介して前記カード情報を取得する取得部と、

前記カード情報を前記決済サーバに送信する送信部と、

前記決済が完了したことを示す決済完了通知を前記決済サーバから受信する受信

20 部と、

受信した前記決済完了通知を表示する表示部と

を有することを特徴とする端末システム。

24. 前記取引端末は、前記カードの所有者から、前記カードのパスワード入力を受け付ける入力部をさらに備え、

25 前記送信部は、前記入力部が受け付けた前記パスワードを、対応する前記カードの前記カード情報に対応付けて前記決済サーバに送信することを特徴とする請求項 23 に記載の端末システム。

25. 取引の決済を行う決済サーバと通信ネットワークを介して通信する端末システムであって、

前記取引に利用するカードのカード情報を読み取るカードリーダと、  
前記カード情報を前記決済サーバに送信する取引端末と  
を備え、

前記カードリーダは、

5 前記カード情報を読み取るカード讀取部と、

前記カード情報を前記取引端末に送信する送信部と

を有し、

前記取引端末は、

前記カードリーダの前記接続部を介して前記カード情報を取得する取得部と、

10 前記カード情報を前記決済サーバに送信する送信部と

を有し、

前記カードリーダ及び前記取引端末のいずれか一方は、前記カードリーダを識別するカードリーダ識別情報をを利用して、前記カード情報を暗号化するリーダ暗号化部を有し、

15 前記カードリーダ及び前記取引端末のいずれか一方は、前記取引端末を識別する取引端末識別情報をを利用して、前記カード情報を暗号化する端末暗号化部を有し、

前記取引端末の送信部は、前記リーダ暗号化部及び前記端末暗号化部が暗号化した後の、前記カード情報を前記決済サーバに送信することを特徴とする端末システム。

20 26. 取引の支払に利用するカードのカード情報を読み取るカードリーダと接続し、かつ取引端末と接続する接続装置であって、

前記カードリーダに接続し、前記カードリーダから前記カード情報を取得するカードリーダ接続部と、

前記取引端末に接続する取引端末接続部と、

25 当該接続装置を識別する接続装置識別情報を保持する接続装置識別情報保持部と、  
前記取引端末接続部を介して、前記接続装置識別情報及び前記カード情報を前記取引端末に送信する送信部と  
を備えることを特徴とする接続装置。

27. 前記取引端末を識別する取引端末識別情報を保持する取引端末識別情報保

持部と、

前記取引端末接続部が前記取引端末に接続された場合に、前記取引端末接続部を介して、前記取引端末から当該取引端末を識別する取引端末識別情報を取得する接続先認証部と、

- 5 前記接続先認証部が取得した前記取引端末識別情報と、前記取引端末識別情報保持部が保持する前記取引端末識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許可する許可部と  
をさらに備えることを特徴とする請求項 2 6 に記載の接続装置。

28. 前記取引端末を識別する取引端末識別情報を保持する取引端末識別情報保持部と、

前記取引端末接続部が前記取引端末に接続された場合に、前記取引端末接続部を介して、前記取引端末から当該取引端末を識別する取引端末識別情報を取得する接続先認証部と、

- 前記取引端末接続部に接続された前記取引端末が通信すべき通信先を指定する通信先情報を保持する通信先保持部と、

前記接続先認証部が読み取った前記取引端末識別情報と、前記取引端末識別情報保持部が保持する前記取引端末識別情報とが一致した場合に、前記通信先保持部に保持される前記通信先情報をを利用して、前記取引端末と前記通信先との通信を確立させる通信確立部と

- 20 をさらに備えることを特徴とする請求項 2 6 に記載の接続装置。

29. 前記カードリーダを識別するカードリーダ識別情報を保持するカードリーダ識別情報保持部と、

- 前記カードリーダ接続部が前記カードリーダに接続された場合に、前記カードリーダ接続部を介して、前記カードリーダから当該カードリーダを識別するカードリーダ識別情報を取得する接続先認証部と、

前記接続先認証部が読み取った前記カードリーダ識別情報と、前記カードリーダ識別情報保持部が保持する前記カードリーダ識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許可する許可部と  
をさらに備えることを特徴とする請求項 2 6 に記載の接続装置。

30. 前記カードリーダを識別するカードリーダ識別情報を保持するカードリーダ識別情報保持部と、

前記カードリーダ接続部が前記カードリーダに接続された場合に、前記カードリーダ接続部を介して、前記カードリーダから当該カードリーダを識別するカードリーダ識別情報を取得する接続先認証部と、

前記カードリーダ接続部に接続された前記カードリーダが通信すべき通信先を指定する通信先情報を保持する通信先保持部と、

前記接続先認証部が読み取った前記カードリーダ識別情報と、前記カードリーダ識別情報保持部が保持する前記カードリーダ識別情報とが一致した場合に、前記通信

10 通信先保持部に保持される前記通信先情報をを利用して、前記取引端末と前記通信先との通信を確立させる通信確立部と

をさらに備えることを特徴とする請求項26に記載の接続装置。

31. ネットワークを介して通信を行う第1及び第2の通信装置を含む情報通信システムであって、

15 情報を読み取る情報読み取り装置と、

前記情報読み取り装置から前記情報を取得し、前記読み取り装置を識別する読み取り装置識別情報及び第1の通信装置を識別する通信装置識別情報をを利用して暗号化された前記情報を、暗号化情報として第2の通信装置に送信する第1の通信装置と、

20 前記ネットワークを介して前記第1の通信装置から前記暗号化情報を受信し、前記読み取り装置識別情報及び前記第1通信装置識別情報をを利用して、前記暗号化情報を復号化する第2の通信装置と

を備えることを特徴とする情報通信システム。

32. 前記読み取り装置及び前記第1の通信装置と接続し、前記読み取り装置から前記第1の通信装置に情報を送る接続装置をさらに備え、

前記第1の通信装置は、前記読み取り装置識別情報、前記接続装置を識別する接続装置識別情報、及び第1通信装置識別情報のうち少なくとも2つを利用して暗号化された前記暗号化情報を前記第2の通信装置に送信し、

前記第2の通信装置は、前記読み取り装置識別情報、前記接続装置識別情報、及

び前記第1通信装置識別情報のうち少なくとも2つを利用して前記暗号化情報を復号化することを特徴とする請求項3-1に記載の情報通信システム。

3-3. 情報を管理する情報管理装置であって、

前記情報を読み取る情報読み取り装置を識別する読み取り装置識別情報と、前記読み取り装置に接続された通信装置を識別する通信装置識別情報をを利用して暗号化された前記情報と、を前記通信装置から受信する受信部と、

前読み取り装置と、前記読み取り装置が前記情報を送信すべき通信装置とを対応付ける装置管理テーブルと、

前記受信部が前記通信装置から、前記読み取り装置識別情報及び前記情報を受信した場合に、前記通信装置識別情報及び前記装置管理テーブルにおいて前記通信装置に対応付けられた前記読み取り装置の前記読み取り装置識別情報を利用して、前記情報を復号化する復号化部と

を備えることを特徴とする情報管理装置。

3-4. 装置の認証を行う認証サーバを含む認証システムであって、

15 情報を読み取る読み取り装置と、

前記読み取り装置から当該読み取り装置を認証する認証要求を受け取り、当該認証要求を、前記通信装置を識別する情報と共に、ネットワークを介して前記認証サーバに送信する通信装置とを備え、

前記認証サーバは、前記読み取り装置が前記情報を送るべき通信装置を管理し、  
20 前記ネットワークを介して、前記認証要求及び前記通信装置を識別する情報を受信した場合に、当該通信装置を識別する情報により識別される前記通信装置に、前記読み取り装置を認証することを示す読み取り装置認証情報を送信し、

前記読み取り装置は、前記通信装置が受信した前記読み取り装置認証情報と同一の読み取り装置認証情報を外部から取得した場合に、前記情報を前記通信装置に送ることを許可する送信許可部を有することを特徴とする認証システム。

3-5. 前記読み取り装置は、

所定の処理が行われた場合に、前記読み取り情報を送信することを禁止する送信禁止部と、

前記送信禁止部が前記送信を禁止した場合に、前記認証要求を前記通信端末に送

る認証要求送信部と  
をさらに有することを特徴とする請求項 3 4 に記載の認証システム。

3 6 . 前記通信装置は、

前記読み取り装置認証情報を受信する受信部と、

5 前記受信部が受信した読み取り装置認証情報を表示する表示部と  
を有し、

前記読み取り装置は、

ユーザからの入力により、前記表示部に表示された前記読み取り装置認証情報を  
取得する取得部をさらに有し、

10 前記取得部が前記読み取り装置認証情報を取得した場合に、前記送信許可部は、  
前記情報を前記通信装置に送ることを許可することを特徴とする請求項 3 4 に記載  
の認証システム。

3 7 . 前記読み取り装置は、前記認証装置が前記読み取り装置を認証するときに  
利用する読み取り装置認証情報を保持する読み取り装置認証情報保持部をさらに有  
15 し、

前記取得部が取得した前記読み取り装置認証情報と、前記読み取り装置認識情報  
保持部に保持される前記読み取り装置認識情報とが一致した場合に、前記送信許可  
部は、前記読み取り情報を前記通信装置に送ることを特徴とする請求項 3 6 に記載  
の認証システム。

20 3 8 . 前記読み取り装置は、カードからカード情報を読み取るカードリーダである  
ことを特徴とする請求項 3 4 に記載の認証システム。

3 9 . 装置を認証する認証サーバであって、

情報を読み取る読み取り装置が読み取った情報を、当該読み取り装置に接続され  
た通信装置から、ネットワークを介して受信する受信部と、

25 前記通信部から、前記読み取り装置を認証することを要求する認証要求を取得す  
る認証要求取得部と、

前記読み取り装置と、当該読み取り装置が読み取った読み取り情報を送るべき通  
信装置とを対応付ける装置管理テーブルと、

装置管理テーブルを利用して、前記認証要求取得部が取得した前記認証要求に示

される前記読み取り装置が前記情報を送るべき前記通信装置を選択し、選択された前記通信装置に対して、前記読み取り装置を認証すべき読み取り装置認証情報を送信する送信部と

を備えることを特徴とする認証サーバ。

5 40. 取引の決済を利用するカードからカード情報を読み取るカードリーダと、取引を行う取引端末と、取引の決済を行う決済サーバを含む決済システムにおける決済方法であって、

前記取引端末が、前記カードリーダに接続し、前記カードリーダから取得した前記カード情報を、前記取引端末に接続した前記カードリーダを識別するカードリーダ識別情報と、前記取引端末を識別する取引端末識別情報及び前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報の少なくとも一方と、とともに前記決済サーバに送信する段階と、

前記決済サーバが、前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報の組み合わせに基づいて、前記取引端末の認証を行う段階と、

前記決済サーバが、前記認証に成功した場合に、前記通信ネットワークを介して前記取引端末から受信した前記カード情報をを利用して決済処理を行う段階とを有することを特徴とする決済方法。

41. 取引の決済を利用するカードからカード情報を読み取るカードリーダと、前記取引を行う取引端末と、前記取引の決済を行う決済サーバを含む決済システムにおける決済方法であって、

前記取引端末が、前記カードリーダから前記カード情報を取得し、前記カード情報を前記決済サーバに送信する段階と、

前記取引端末が、前記カードリーダを識別するカードリーダ識別情報と、前記取引端末を識別する取引端末識別情報と、を利用して暗号化された前記カード情報を前記決済サーバに送信する段階と、

前記決済サーバが、前記取引端末識別情報と、前記カードリーダ識別情報とを利用して、前記カード情報を復号化する段階とを有することを特徴とする決済方法。

4 2. 取引の決済に利用するカードからカード情報を読み取るカードリーダと、前記取引を行う取引端末と、前記取引の決済を行う決済サーバを含む決済システムにおける決済方法であって、

前記取引端末が、前記カードリーダから前記カード情報を取得し、前記カード情報 5 を前記決済サーバに送信する段階と、

前記決済サーバが、前記取引を識別する取引識別情報を発行する段階と、

前記カードリーダが、前記決済サーバが発行した前記取引識別情報を取得し、取得した前記取引識別情報をを利用して、前記カード情報を暗号化する段階と、

前記取引端末が、暗号化後の前記カード情報を前記決済サーバに送信する段階と、

10 前記決済サーバが、発行した前記取引識別情報をを利用して、前記カード情報を復号化する段階と

を有することを特徴とする決済方法。

4 3. 取引の決済に利用するカードからカード情報を読み取るカードリーダと、前記取引を行う取引端末と、前記カードリーダと前記取引端末とを接続する接続装置 15 と、前記取引の決済を行う決済サーバを含む決済システムにおける決済方法であって、

前記取引端末が、前記カードリーダから取得した前記カード情報を、前記決済サーバに送信する段階と、

20 前記取引端末が、前記カードリーダを識別するカードリーダ識別情報と、前記取引端末に接続した前記接続装置を識別する接続装置識別情報と、前記取引端末を識別する取引端末識別情報及び前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報の一方と、のうち少なくとも 2 つを前記決済サーバに送信する段階と、

25 前記決済サーバが、前記カードリーダ識別情報、前記取引端末識別情報及び前記ユーザ識別情報の一方、及び前記接続装置識別情報のうち少なくとも 2 つの組み合わせに基づいて、前記取引端末の認証を行い、前記認証に成功した場合に、前記通信ネットワークを介して前記取引端末から受信した前記カード情報をを利用して決済処理を行う段階と

を有することを特徴とする決済方法。

4 4 . 取引端末における取引の決済を行う決済方法あって、

前記取引端末を識別する取引端末識別情報及び前記取引端末又は前記カードリーダのユーザを識別するユーザ識別情報の少なくとも一方を受信とともに、前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を、前記取引端末を介して受信する段階と、

前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報と、の組み合わせに基づいて、前記取引端末を認証する段階と、

前記認証に成功した場合に、前記取引端末を介して前記カードリーダから受信した前記カード情報をを利用して、前記決済処理を行う段階と

10 を有することを特徴とする決済方法。

4 5 . 取引を行う取引端末における取引を決済する決済方法であって、

前記取引端末を識別する取引端末識別情報と、前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報と、を利用して暗号化されたカード情報を、前記取引端末から受信する段階と、

15 前記取引端末から前記カード情報を受信した場合、前記取引端末識別情報と、前記カードリーダと、前記カードリーダが前記カード情報を送信すべき取引端末とを対応付ける装置管理テーブルにおいて、前記取引端末識別情報及び前記カードリーダ識別情報をを利用して、前記カード情報を復号化する段階と  
を有することを特徴とする決済方法。

20 4 6 . カードからカード情報を読み取るカードリーダと取引を行う取引端末と、取引の決済を行う決済サーバとを含む端末システムにおける通信方法であって、前記カードリーダが、前記カード情報を読み取る段階と、

前記取引端末に接続された前記カードリーダが、前記カード情報を前記取引端末に送信する段階と、

25 前記取引端末が、前記カードリーダの接続部を介して取得した前記カード情報を前記決済サーバに送信する段階と、  
前記取引端末が、前記決済が完了したことを示す決済完了通知を受信する段階と、  
前記取引端末が、受信した前記決済完了通知を表示部に表示させる段階と  
を有することを特徴とする通信方法。

4 7. 取引に利用するカードのカード情報を読み取るカードリーダと、前記カード情報を前記決済サーバに送信する取引端末とを含み、取引の決済を行う決済サーバと通信ネットワークを介して通信する端末システムにおける通信方法であって、前記カードリーダが、前記カード情報を読み取る段階と、

- 5 前記カードリーダ及び前記取引端末のいずれか一方が、前記カードリーダを識別するカードリーダ識別情報をを利用して、前記カード情報を暗号化する段階と、前記カードリーダ及び前記取引端末のいずれか一方が、前記取引端末を識別する取引端末識別情報をを利用して、前記カード情報を暗号化する段階と、
- 前記取引端末が、前記リーダ暗号化部及び前記端末暗号化部が暗号化した後の、

- 10 前記カード情報を前記決済サーバに送信する段階と  
を有することを特徴とする通信方法。

4 8. 取引の支払に利用するカードのカード情報を読み取るカードリーダ及び取引端末と接続する接続装置の情報送信方法であって、

- 前記接続装置が、前記カードリーダに接続し、前記カードリーダから前記カード情報を取得するカードリーダ接続段階と、

前記接続装置が前記取引端末に接続された場合に、前記取引端末から当該取引端末を識別する取引端末識別情報を取得する接続先認証段階と、

- 前記接続先認証段階で取得した前記取引端末識別情報と、前記接続装置が保持する前記取引端末識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許可する許可段階と、

前記許可段階において前記送信が許可された場合に、前記カード情報を前記取引端末に送信する送信段階と  
を有することを特徴とする情報送信方法。

- 4 9. ネットワークを介して通信を行う第1及び第2の通信装置を含む情報通信システムにおける通信方法であって、

前記第1の通信装置が、情報を読み取る情報読み取り装置から前記情報を取得し、前記読み取り装置を識別する読み取り装置識別情報及び第1の通信装置を識別する通信装置識別情報をを利用して暗号化された前記情報を、暗号化情報として第2の通信装置に送信する段階と、

前記第2の通信装置が、前記ネットワークを介して前記第1の通信装置から前記暗号化情報を受信し、前記読み取り装置識別情報及び前記第1通信装置識別情報を利用して、前記暗号化情報を復号化する段階と  
を有することを特徴とする通信方法。

5 50. 情報を管理する情報管理方法であって、

前記情報を読み取る情報読み取り装置を識別する読み取り装置識別情報、及び前記読み取り装置に接続された通信装置を識別する通信装置識別情報をを利用して暗号化された前記情報を、前記通信装置から受信する段階と、

前記通信装置から前記情報を受信した場合に、前記通信装置識別情報及び、前読み取り装置と、前記読み取り装置が前記情報を送信すべき通信装置とを対応付ける装置管理テーブルにおいて前記通信装置に対応付けられた前記読み取り装置の前記読み取り装置識別情報をを利用して、前記カード情報を復号化する段階と  
を有することを特徴とする情報管理方法。

5 51. 装置の認証を行う認証サーバを含む認証システムにおける認証方法であつて、

通信装置が、情報を読み取る読み取り装置から当該読み取り装置を認証する認証要求を受け取り、当該認証要求を、ネットワークを介して前記認証サーバに送信する段階と、

前記認証サーバが、前記ネットワークを介して前記通信要求を受信した場合に、  
前記通信要求に示される前記読み取り装置が読み取った前記情報を送るべき前記通信装置に、前記読み取り装置を認証することを示す読み取り装置認証情報を送信する段階と、

前記読み取り装置が、前記通信装置が受信した前記読み取り装置認証情報と同一の読み取り装置認証情報を取得した場合に、前記情報を前記通信装置に送ることを許可する段階と  
を有することを特徴とする認証方法。

5 52. 装置を認証する認証方法であって、

情報を読み取る読み取り装置が読み取った情報を、当該読み取り装置に接続された通信装置から、ネットワークを介して受信する段階と、

前記通信装置から、前記読み取り装置を認証することを要求する認証要求を取得する段階と、

前記読み取り装置と、当該読み取り装置が読み取った読み取り情報を送るべき通信装置とを対応付ける装置管理テーブルを利用して、前記通信装置から取得した前記認証要求に示される前記読み取り装置が前記情報を送るべき前記通信装置を選択し、選択された前記通信装置に対して、前記読み取り装置を認証すべき読み取り装置認証情報を送信する段階と

を有することを特徴とする認証方法。

5 3. 取引端末における取引の決済を行うコンピュータ用プログラムであって、

10 前記プログラムが前記コンピュータに対して、

前記取引端末を識別する取引端末識別情報及び前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報の少なくとも一方を受信させるとともに、前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を、前記取引端末を介して受信させる受信モジュールと、

前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報の組み合わせに基づいて、前記取引端末を認証させる認証モジュールと、

前記認証に成功した場合に、前記取引端末を介して前記カードリーダから受信した前記カード情報を利用して、前記決済処理を行わせる決済モジュールとを備えることを特徴とするプログラム。

5 4. 取引を行う取引端末における取引を決済するコンピュータ用プログラムであって、

前記プログラムが、前記コンピュータに対して、

25 前記取引端末を識別する取引端末識別情報、及び前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を利用して暗号化されたカード情報を前記取引端末から受信させる受信モジュールと、

前記受信モジュールが前記取引端末から前記カード情報を受信した場合、前記取引端末識別情報、及び前記カードリーダと、前記カードリーダが前記カード情報を

送信すべき取引端末とを対応付ける装置管理テーブルと、装置管理テーブルにおいて前記取引端末に対応付けられた前記カードリーダの前記カードリーダ識別情報を利用して、前記カード情報を復号化させる復号化モジュールとを有することを特徴とするプログラム。

5 55. 取引の支払に利用するカードのカード情報を読み取るコンピュータ用プログラムであって、

前記プログラムが、前記コンピュータに対して、

前記カード情報を読み取らせるカード読取モジュールと、

取引端末に接続した場合に、前記取引端末から前記取引端末を識別する取引端末  
10 識別情報を読み取らせる接続先認証モジュールと、

前記接続先認証モジュールで読み取った前記取引端末識別情報と、予め定められた取引端末識別情報とが一致した場合に、前記カード情報を前記取引端末に送信することを許可させる許可モジュールと

前記送信することが許可された場合に、前記カード情報を前記取引端末に送信さ  
15 せる送信モジュールと

を有することを特徴とするプログラム。

56. 取引の支払に利用するカードのカード情報を読み取るカードリーダ及び取  
引端末と接続するコンピュータ用プログラムであって、

前記プログラムが、前記コンピュータに対して、

20 前記接続装置と前記取引端末とを接続させる取引端末接続モジュールと、

前記接続装置が前記取引端末に接続された場合に、前記取引端末から当該取引端  
末を識別する取引端末識別情報を取得させる接続先認証モジュールと、

前記接続先認証モジュールが取得させた前記取引端末識別情報と、前記接続装置  
が保持する前記取引端末識別情報とが一致した場合に、前記カードリーダから取得  
25 した前記カード情報を前記取引端末に送信することを許可させる許可モジュールと、

前記許可段階において前記送信が許可された場合に、前記カード情報を前記取引  
端末に送信させる送信モジュールと

を有することを特徴とするプログラム。

57. 情報を管理するコンピュータ用プログラムであって、

前記プログラムが前記コンピュータに対して、

前記情報を読み取る情報読み取り装置を識別する読み取り装置識別情報と、前記読み取り装置に接続された通信装置を識別する通信装置識別情報をを利用して暗号化された前記情報と、を前記通信装置から受信させる受信モジュールと、

- 5 前記受信モジュールが前記通信装置から前記装置識別情報及び前記情報を受信させた場合に、前記通信装置識別情報と、前記読み取り装置と当該読み取り装置が前記情報を送信すべき通信装置とを対応付ける装置管理テーブルにおいて前記通信装置に対応付けられた前記読み取り装置の前記読み取り装置識別情報と、を利用して前記情報を復号化させる復号化モジュールと

- 10 を有することを特徴とするプログラム。

5 8. 装置を認証するコンピュータ用プログラムであって、

前記プログラムが、前記コンピュータに対して、

情報を読み取る読み取り装置が読み取った情報を、当該読み取り装置に接続された通信装置から、ネットワークを介して受信させる受信モジュールと、

- 15 前記通信装置から、前記読み取り装置を認証することを要求する認証要求を取得させる取得モジュールと、

前記読み取り装置と、当該読み取り装置が読み取った読み取り情報を送るべき通信装置とを対応付ける装置管理テーブルを利用して、前記通信装置から取得した前記認証要求に示される前記読み取り装置が前記情報を送るべき前記通信装置を選択

- 20 させ、選択された前記通信装置に対して、前記読み取り装置を認証すべき読み取り装置認証情報を送信させる送信モジュールと

を有することを特徴とするプログラム。

5 9. 取引端末における取引の決済を行うコンピュータ用プログラムを格納する記録媒体であって、前記プログラムが、前記コンピュータに対して、

- 25 前記取引端末を識別する取引端末識別情報及び前記取引端末のユーザを識別するユーザ識別情報若しくは前記カードリーダのユーザを識別するユーザ識別情報の少なくとも一方を受信するとともに、前記取引の決済に利用するカードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を、前記取引端末を介して受信させる受信モジュールと、

前記取引端末識別情報及び前記ユーザ識別情報の少なくとも一方と、前記カードリーダ識別情報と、の組み合わせに基づいて、前記取引端末を認証させる認証モジュールと、

前記認証に成功した場合に、前記取引端末を介して前記カードリーダから受信し  
5 前記カード情報をを利用して、前記決済処理を行わせる決済モジュールと  
を有することを特徴とする記録媒体。

6 0. 取引を行う取引端末における取引を決済するコンピュータ用プログラムを  
格納する記録媒体であって、

前記プログラムが、前記コンピュータに対して、

10 前記取引端末を識別する取引端末識別情報、及び前記取引の決済に利用するカ  
ードのカード情報を読み取るカードリーダを識別するカードリーダ識別情報を利用し  
て暗号化されたカード情報を前記取引端末から受信させる受信モジュールと、

前記受信モジュールが前記取引端末から前記カード情報を受信した場合、前記取  
引端末識別情報、及び前記カードリーダと、前記カードリーダが前記カード情報を  
15 送信すべき取引端末とを対応付ける装置管理テーブルと、装置管理テーブルにおいて前記取引端末に対応付けられた前記カードリーダの前記カードリーダ識別情報を  
利用して、前記カード情報を復号化させる復号化モジュールと  
を有することを特徴とする記録媒体。

6 1. 取引の支払に利用するカードのカード情報を読み取るコンピュータ用プロ  
20 グラムを格納する記録媒体であって、前記プログラムがコンピュータに対して、

前記カード情報を読み取らせるカード読取モジュールと、

取引端末に接続した場合に、前記取引端末から前記取引端末を識別する取引端末  
識別情報を読み取らせる接続先認証モジュールと、

前記接続先認証段階で読み取った前記取引端末識別情報と、予め定められた取引  
25 端末識別情報とが一致した場合に、前記カード情報を前記取引端末に送信すること  
を許可させる許可モジュールと

前記送信することが許可された場合に、前記カード情報を前記取引端末に送信さ  
せる送信モジュールと  
を有することを特徴とする記録媒体。

6 2. 取引の支払に利用するカードのカード情報を読み取るカードリーダ及び取引端末と接続する接続装置のコンピュータ用プログラムを格納する記録媒体であつて、前記プログラムがコンピュータに対して、

前記接続装置が前記取引端末に接続された場合に、前記取引端末から当該取引端

5 末を識別する取引端末識別情報を取得させる接続先認証モジュールと、

前記接続先認証モジュールが取得させた前記取引端末識別情報と、前記接続装置が保持する前記取引端末識別情報とが一致した場合に、前記カードリーダから取得した前記カード情報を前記取引端末に送信することを許可させる許可モジュールと、

前記許可段階において前記送信が許可された場合に、前記カード情報を前記取引

10 端末に送信させる送信モジュールと

を有することを特徴とする記録媒体。

6 3. 情報を管理するコンピュータ用プログラムを格納する記録媒体であつて、

前記プログラムが前記コンピュータに対して、

前記情報を読み取る情報読み取り装置を識別する読み取り装置識別情報、及び前

15 記読み取り装置に接続された通信装置を識別する通信装置識別情報を利用して暗号化された前記情報を、前記通信装置から受信させる受信モジュールと、

前記受信モジュールが前記通信装置から前記情報を受信させた場合に、前記通信装置識別情報と、前読み取り装置と前記読み取り装置が前記情報を送信すべき通信装置とを対応付ける装置管理テーブルにおいて前記通信装置に対応付けられた前記

20 読み取り装置の前記読み取り装置識別情報と、を利用して、前記カード情報を復号化させる復号化モジュールと

を有することを特徴とする記録媒体。

6 4. 装置を認証するコンピュータ用プログラムを格納する記録媒体であつて、

前記プログラムが、前記コンピュータに対して、

25 情報を読み取る読み取り装置が読み取った情報を、当該読み取り装置に接続された通信装置から、ネットワークを介して受信させる受信モジュールと、

前記通信装置から、前記読み取り装置を認証することを要求する認証要求を取得させる取得モジュールと、

前記読み取り装置と、当該読み取り装置が読み取った読み取り情報を送るべき通

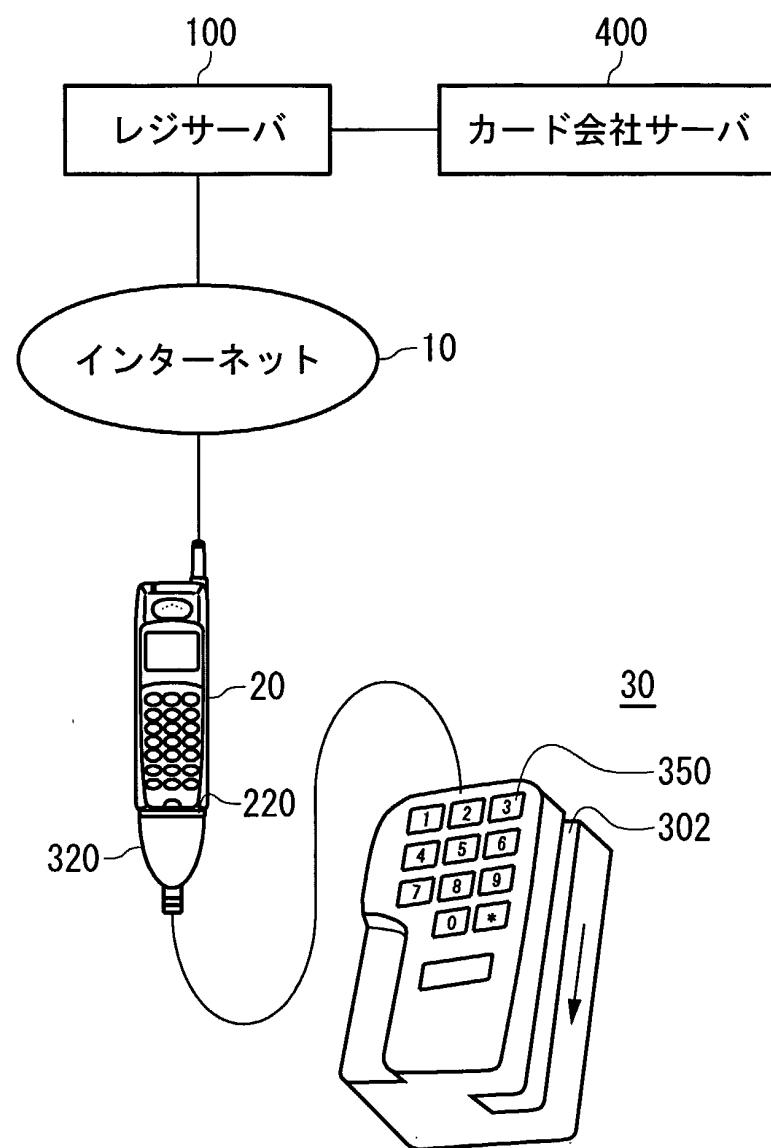
60

信装置とを対応付ける装置管理テーブルを利用して、前記通信装置から取得した前記認証要求に示される前記読み取り装置が前記情報を送るべき前記通信装置を選択させ、選択された前記通信装置に対して、前記読み取り装置を認証すべき読み取り装置認証情報を送信させる送信モジュールと

- 5 を有することを特徴とする記録媒体。

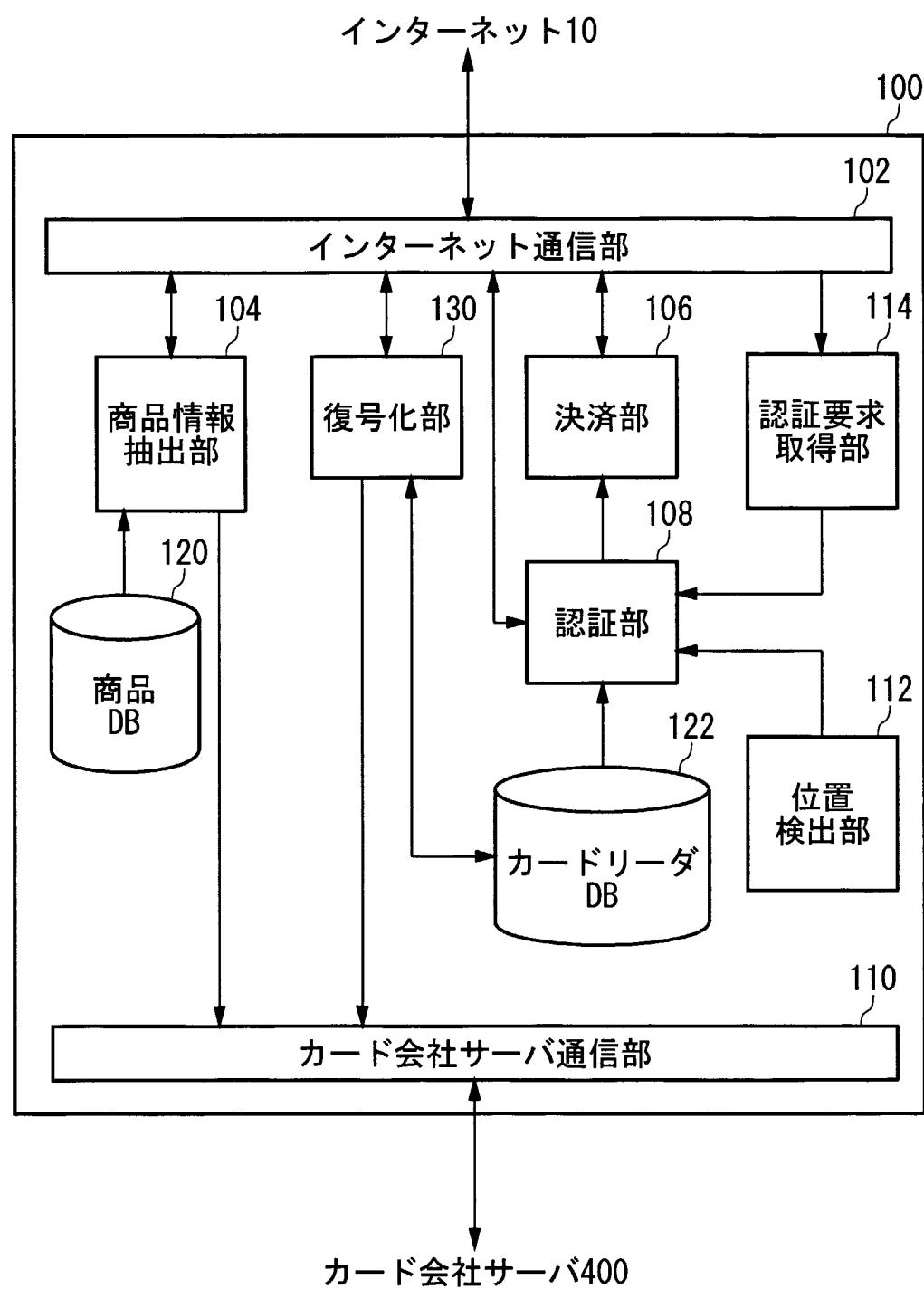
1/20

図 1



2/20

図 2



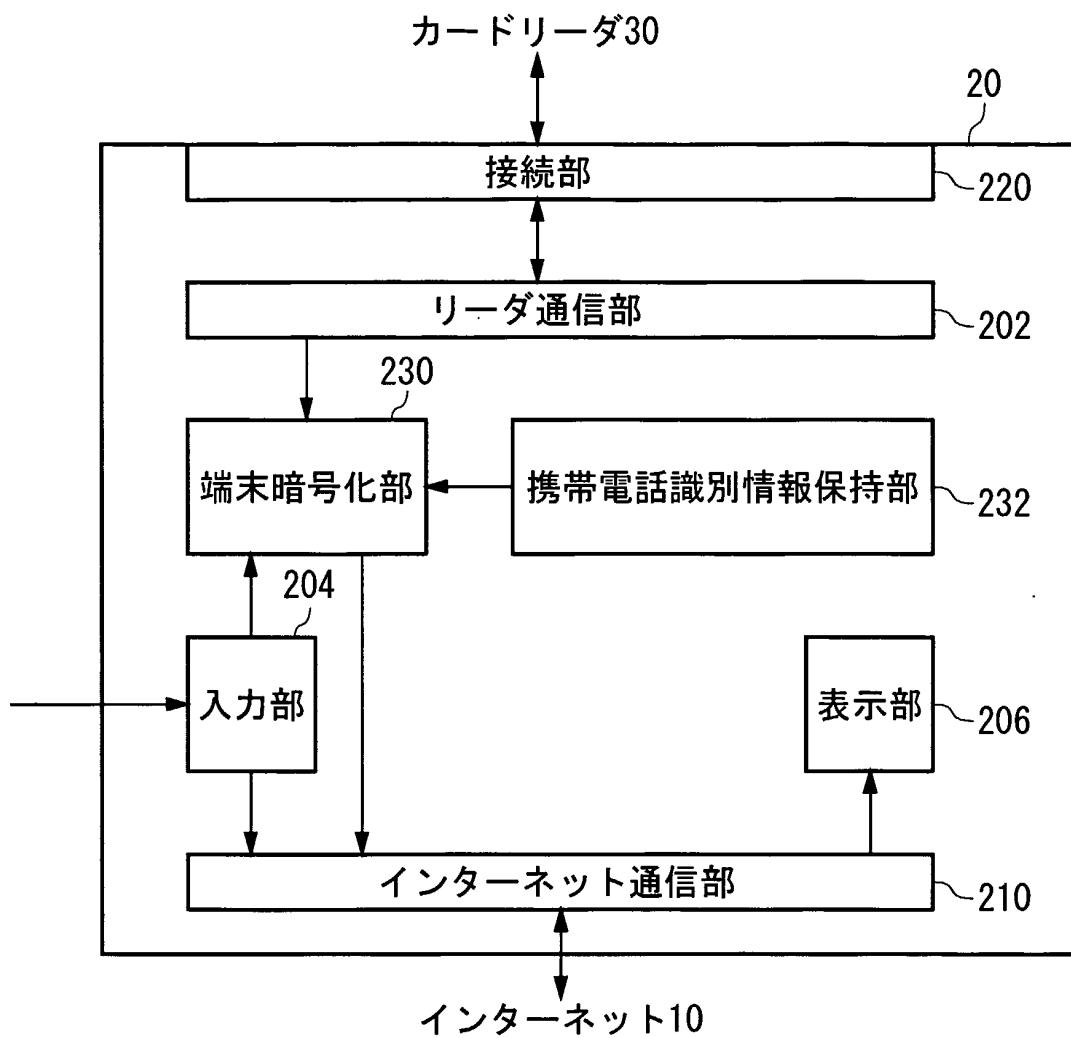
3/20

图 3

122

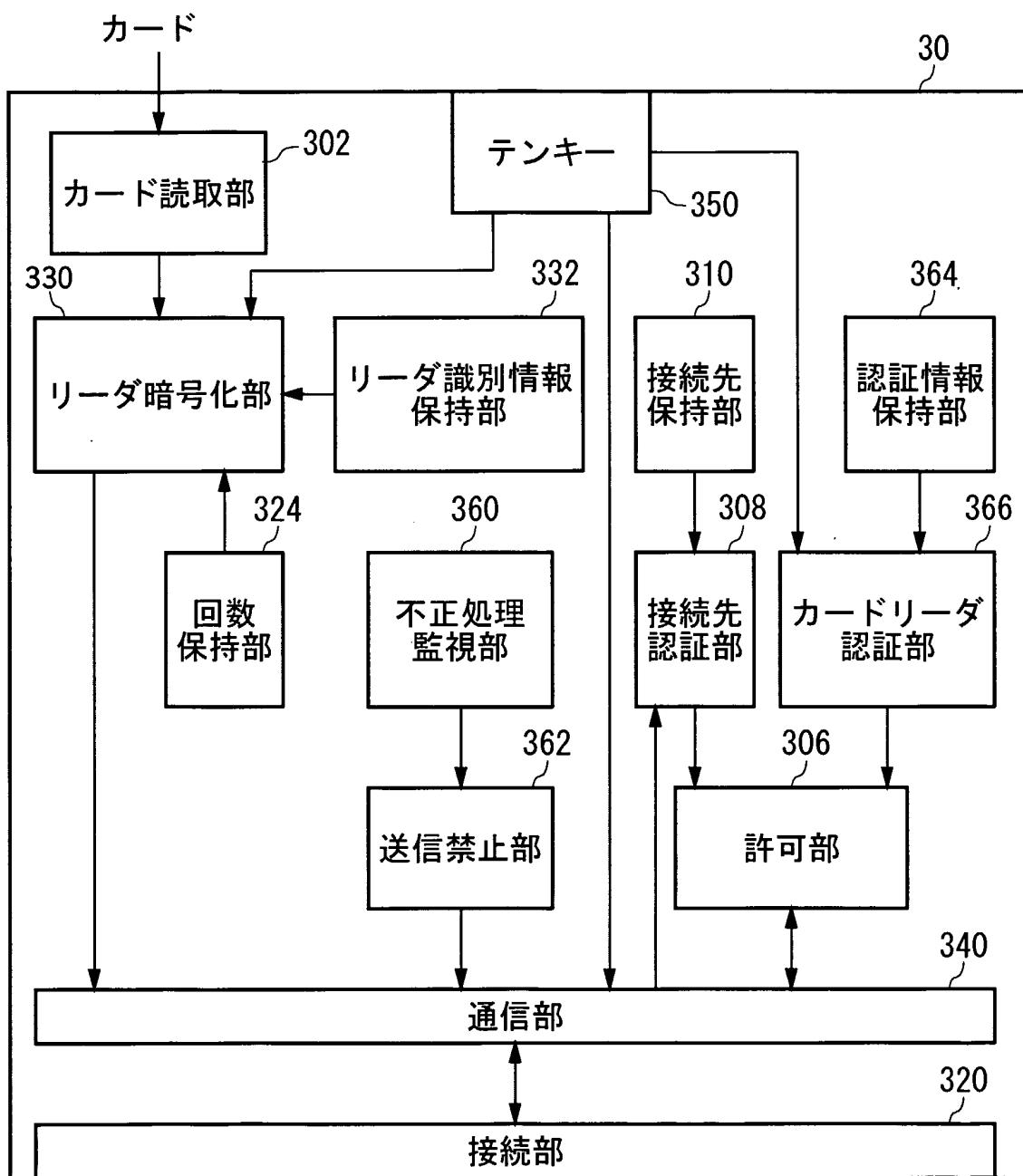
4/20

図 4



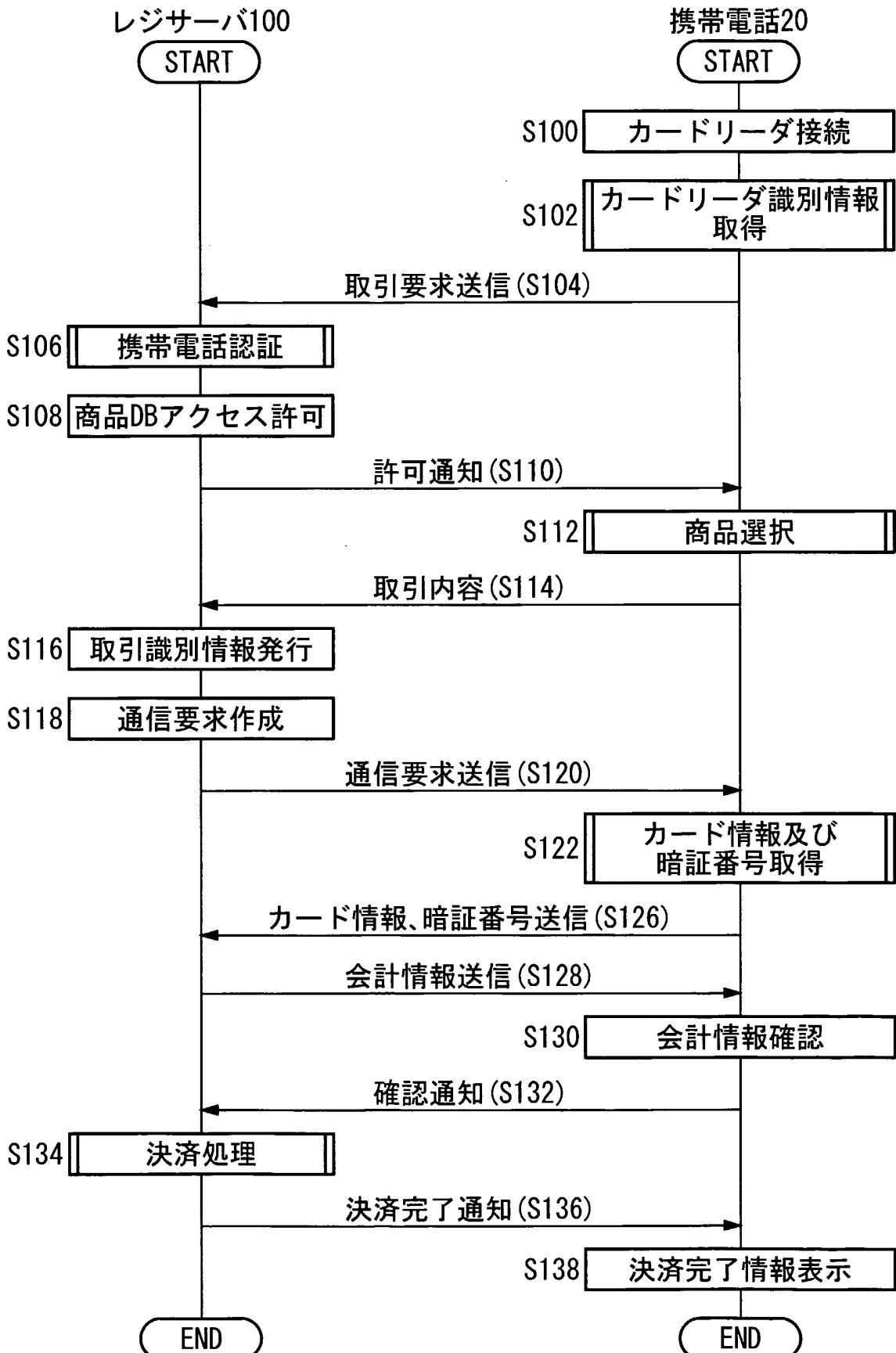
5/20

図 5



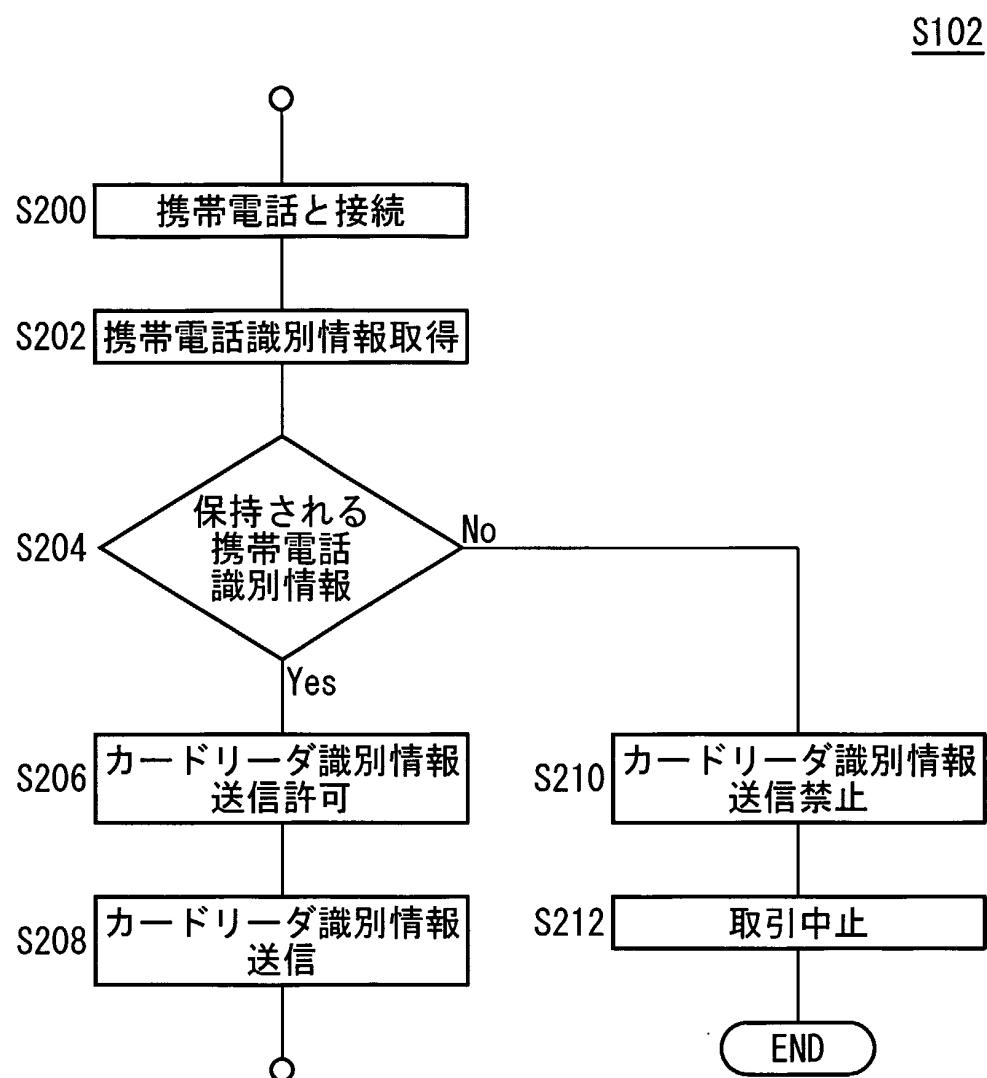
6/20

図 6



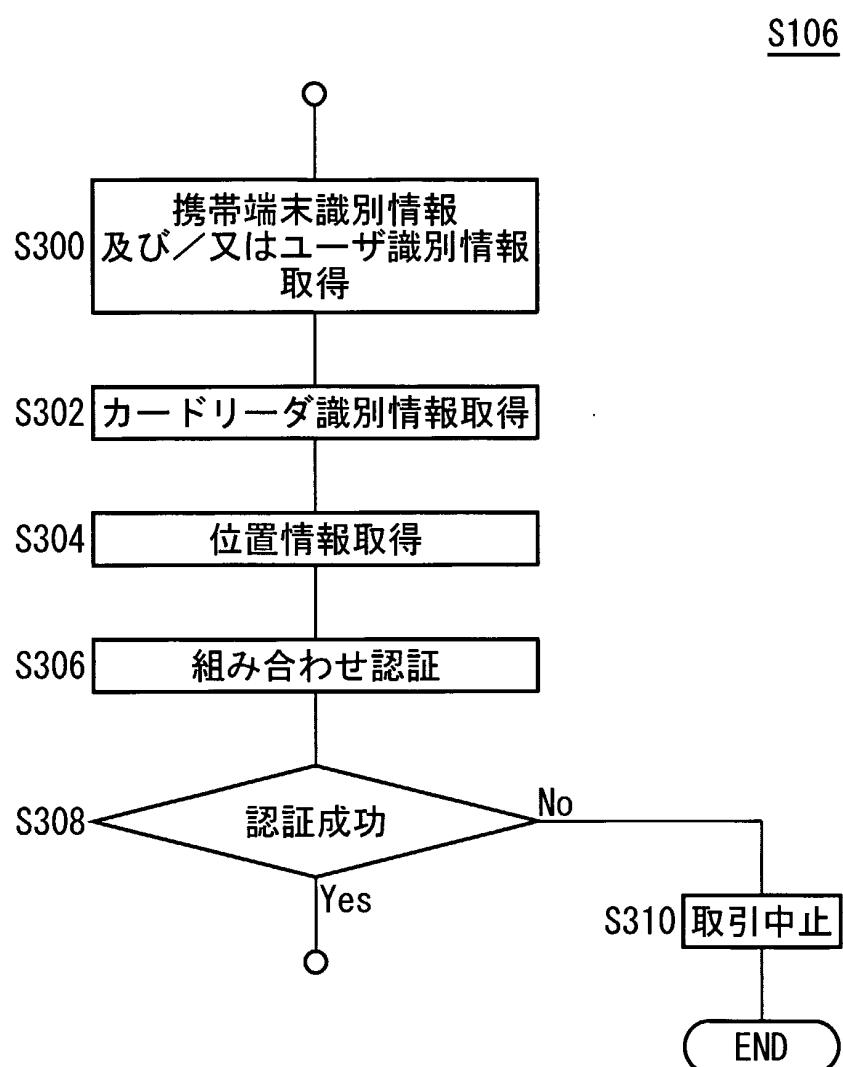
7/20

図 7



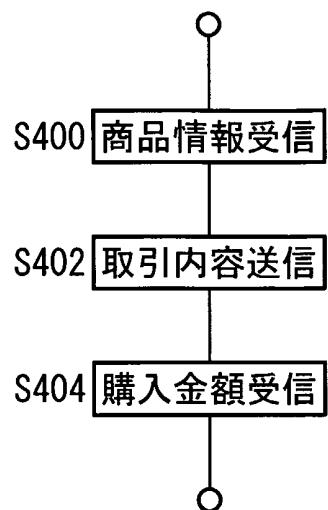
8/20

図 8



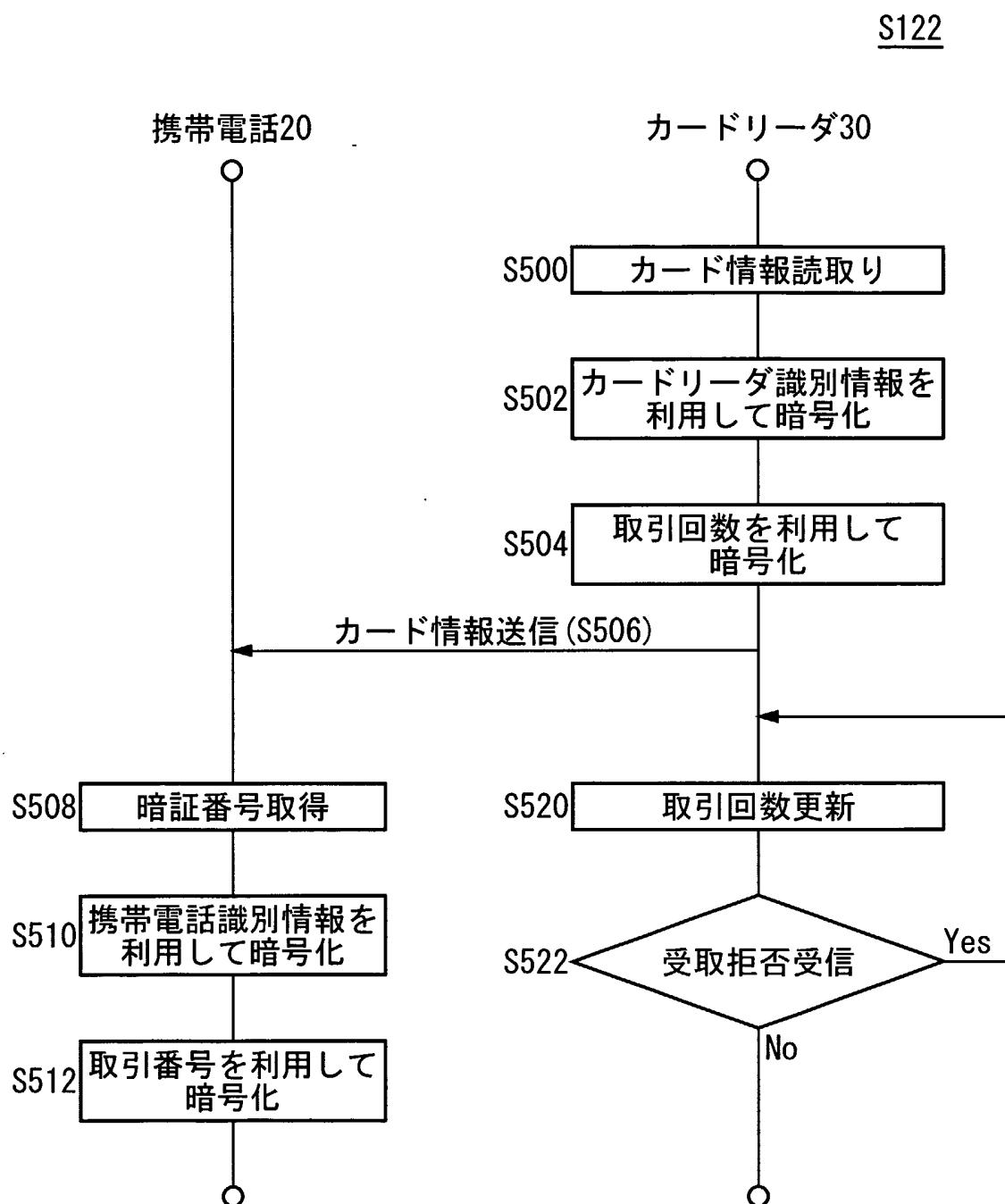
9/20

図 9

S112

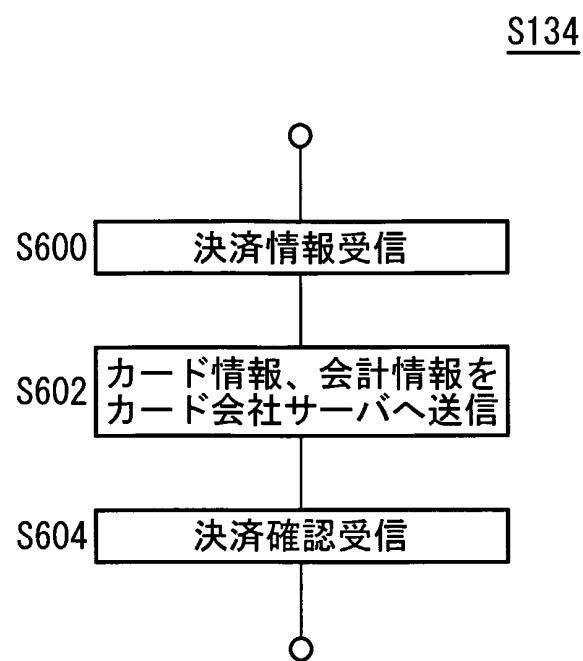
10/20

図 10



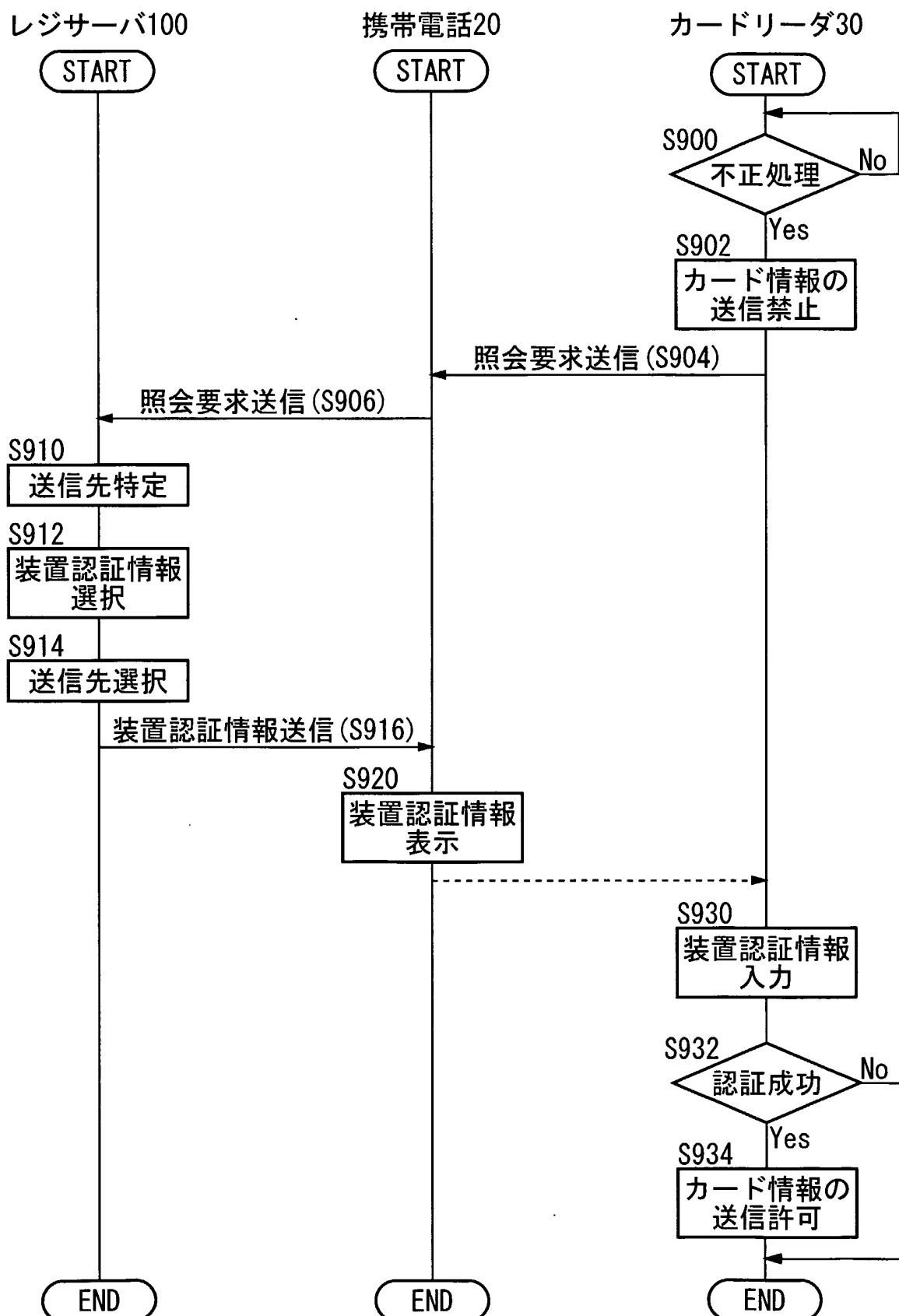
11/20

図 1 1



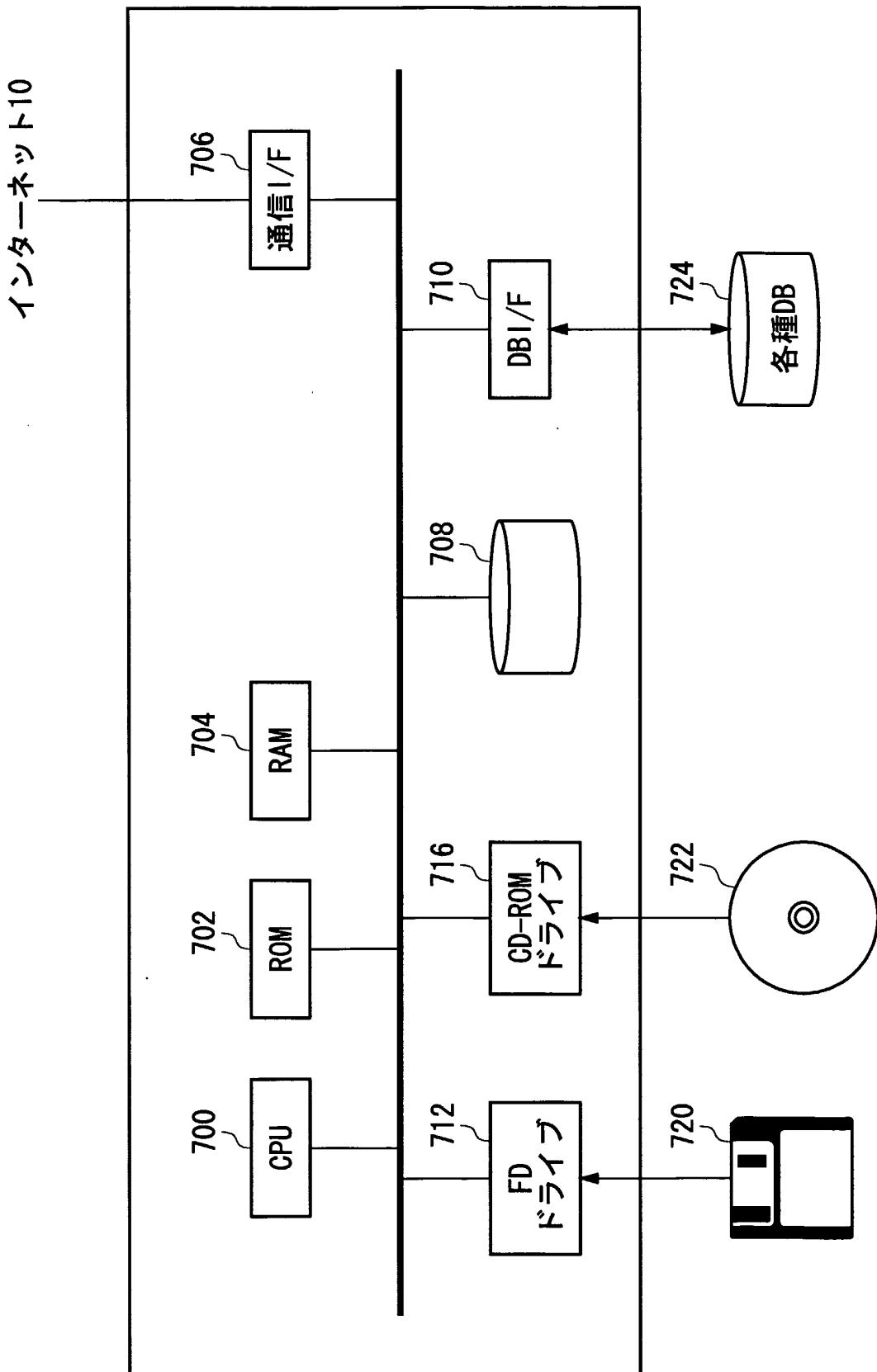
12/20

図 12



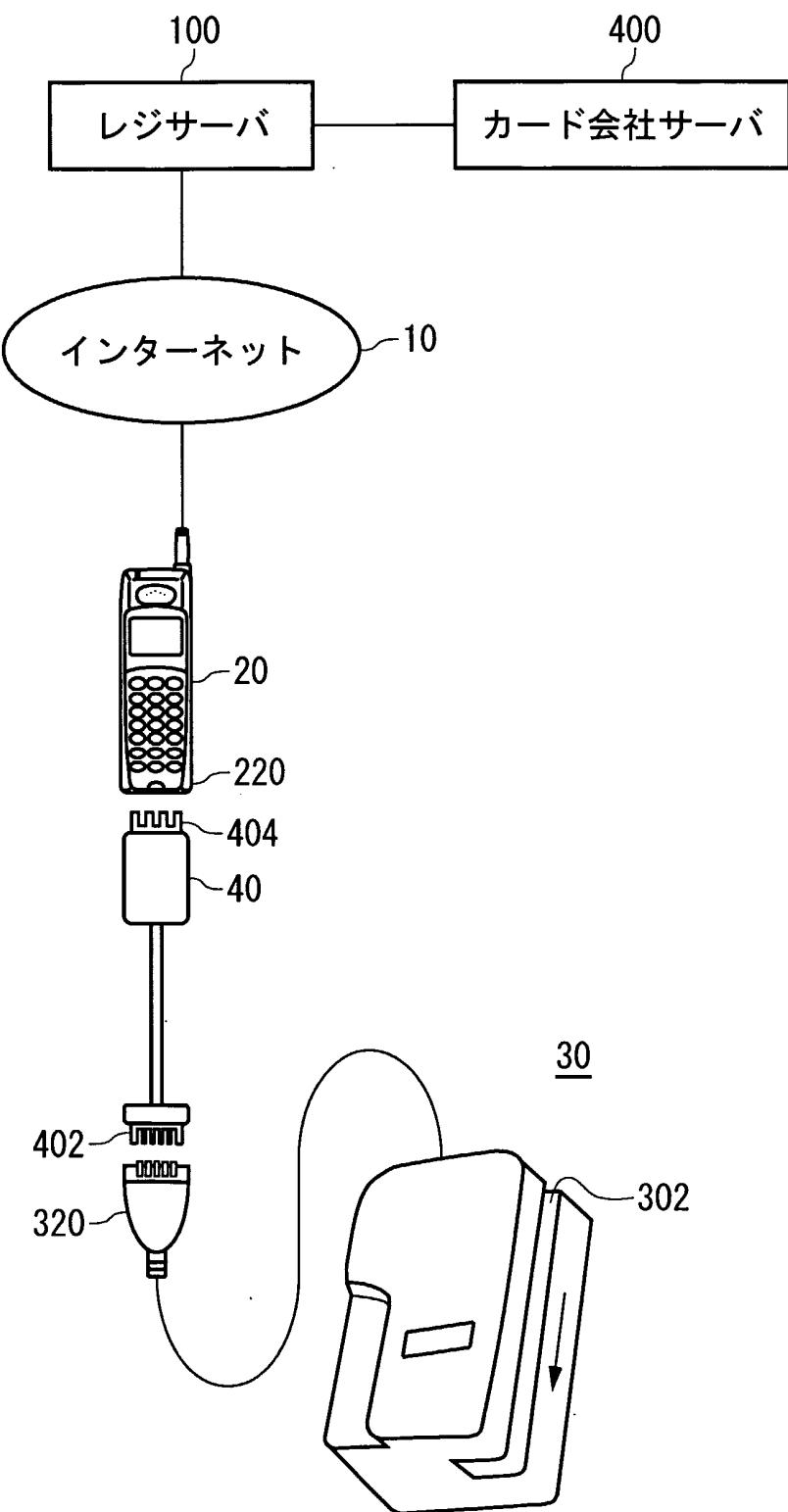
13/20

図 13



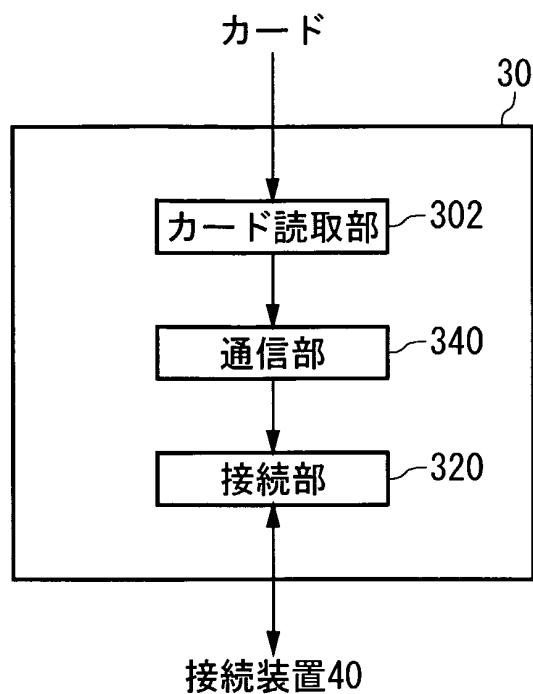
14/20

図 14



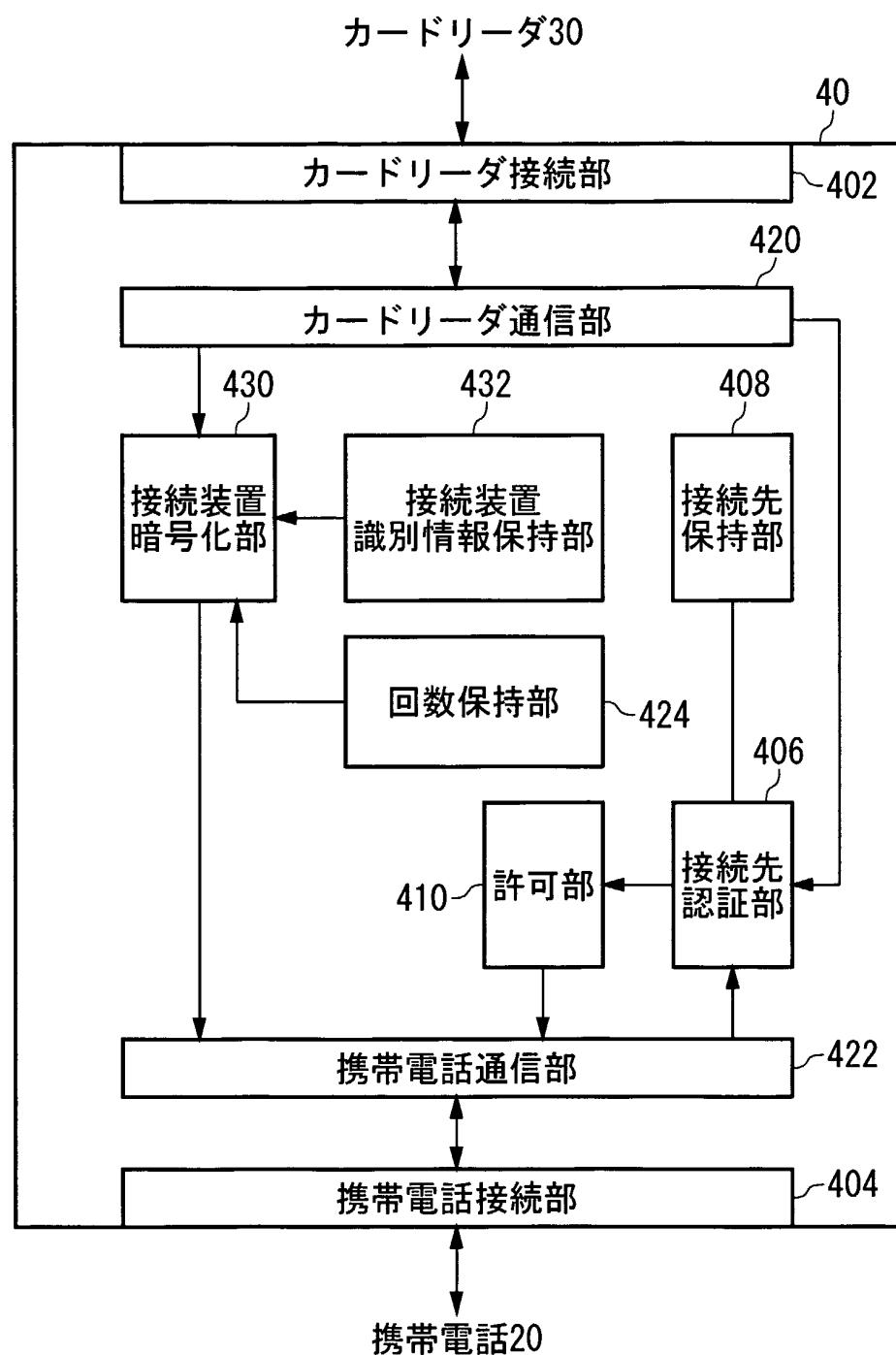
15/20

図 15



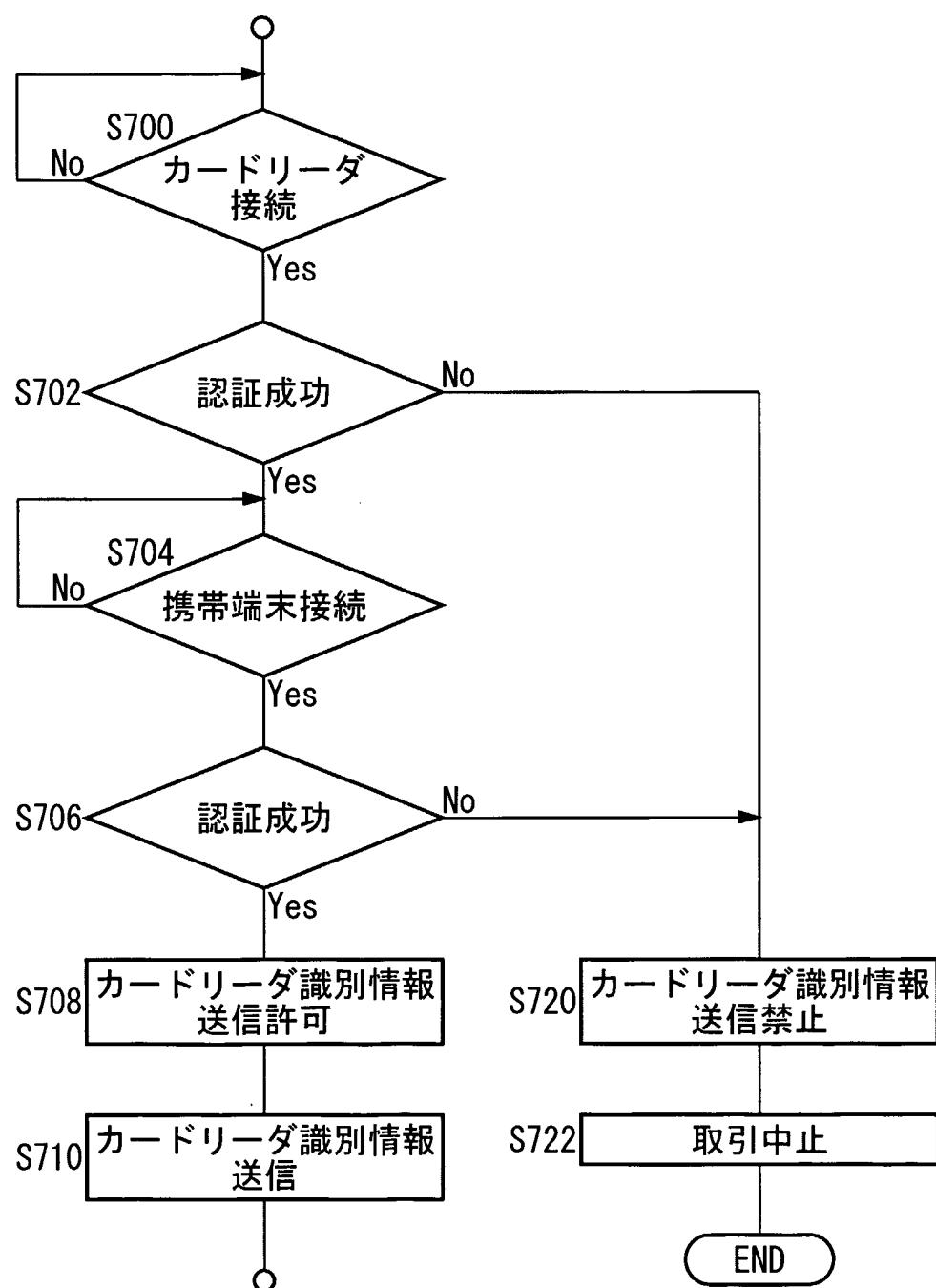
16/20

図 16



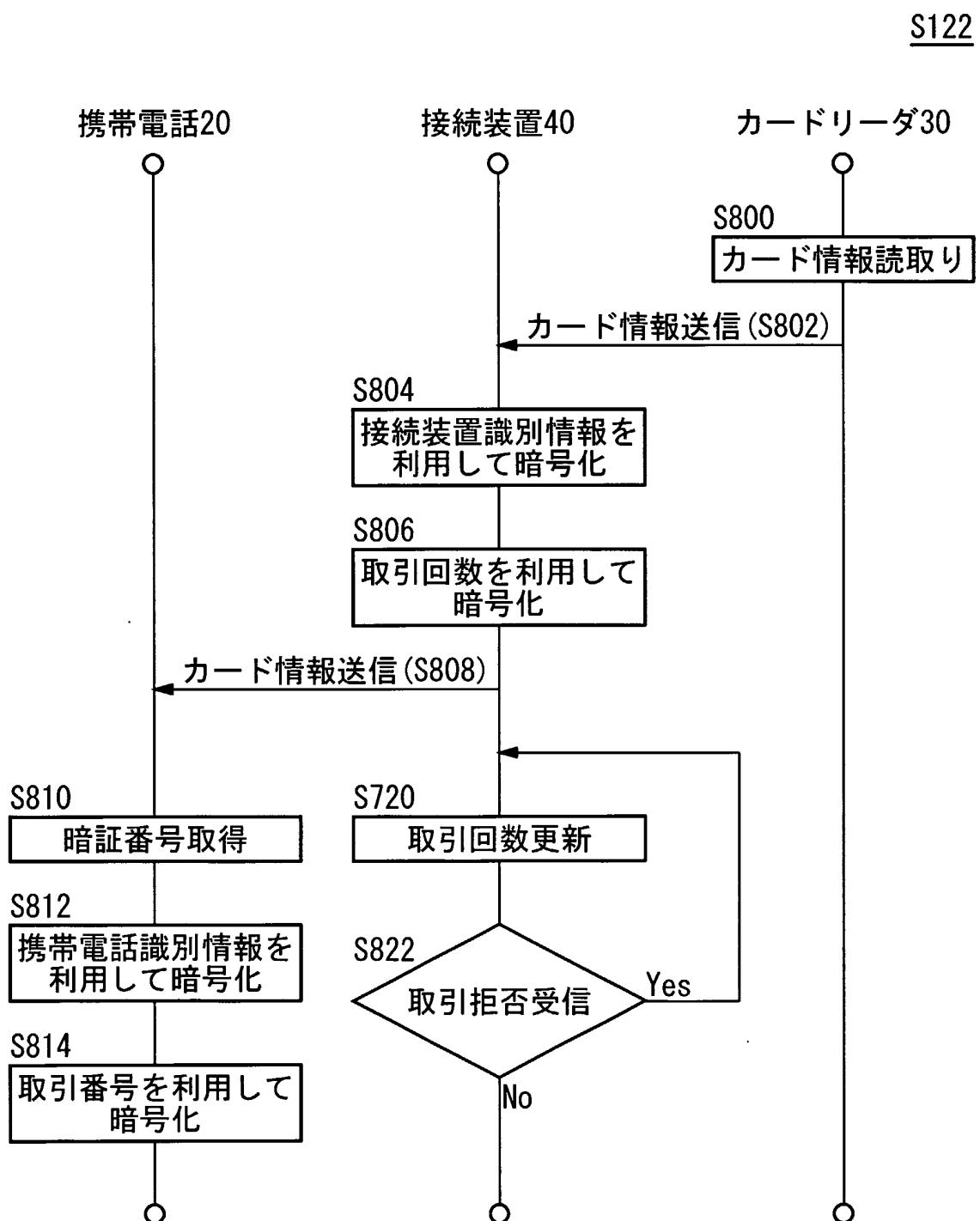
17/20

図 17

S102

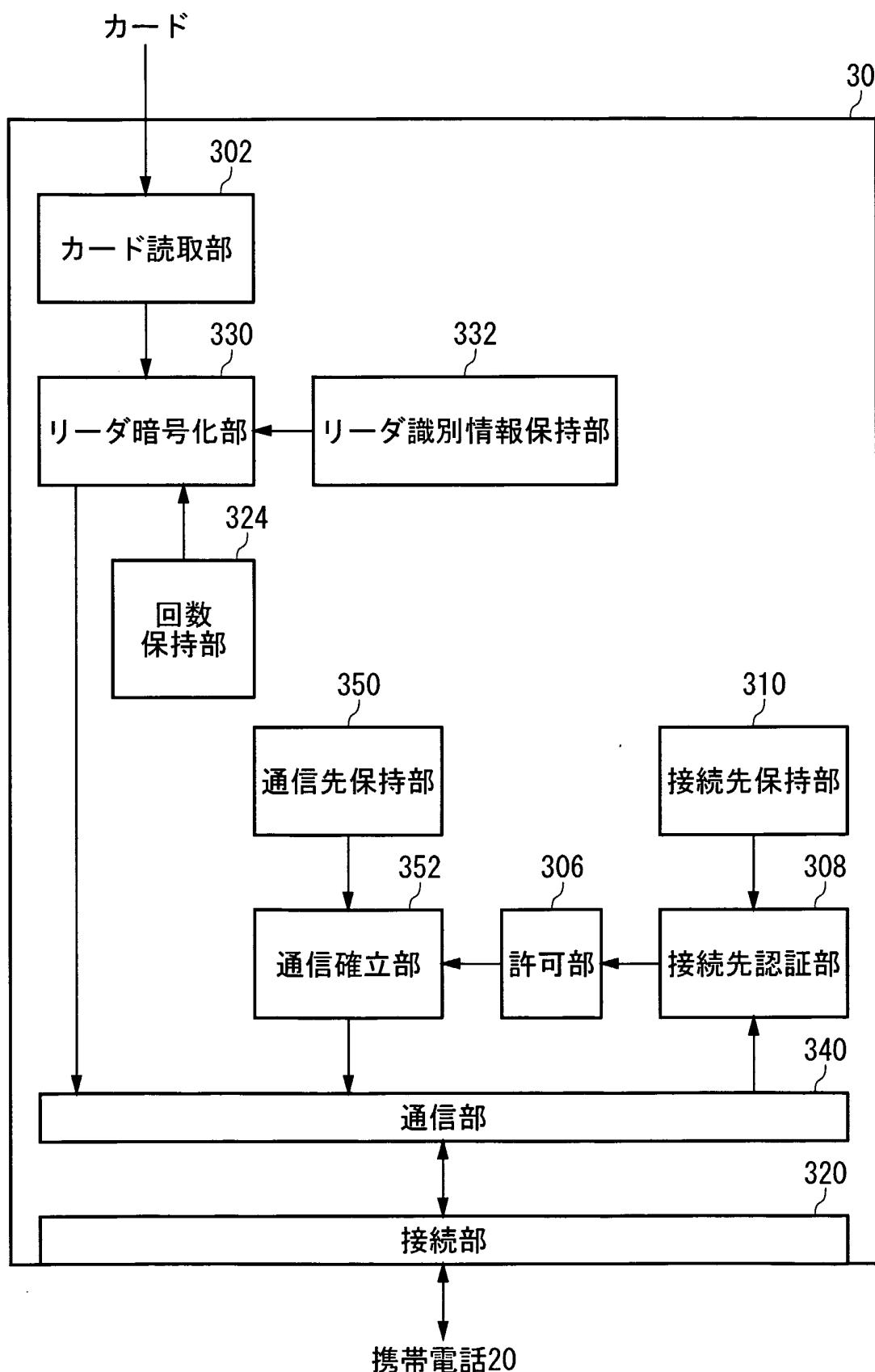
18/20

図18



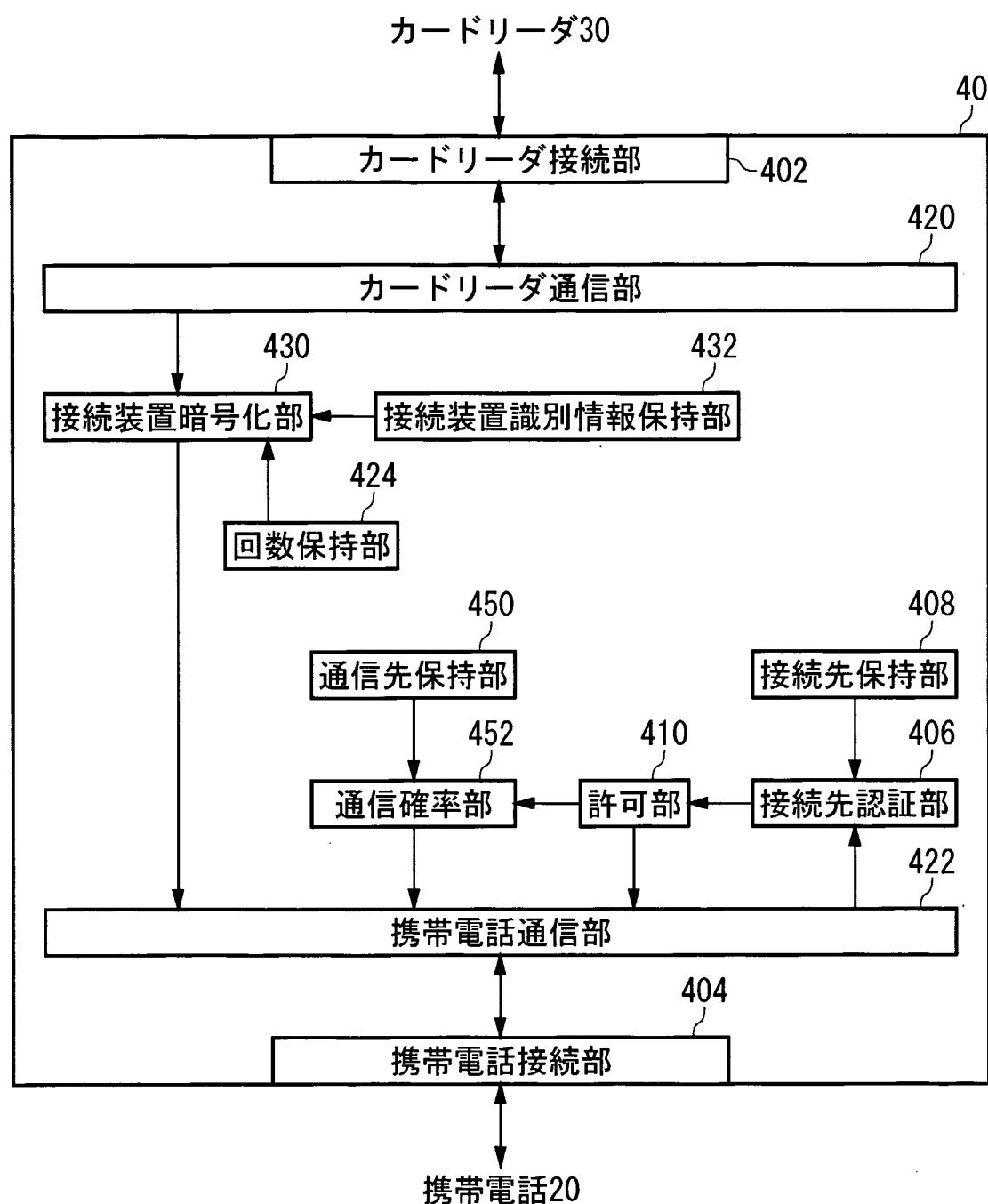
19/20

义 19



20/20

図 20



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/02027

**A. CLASSIFICATION OF SUBJECT MATTER**

Int.C1<sup>7</sup> G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

Int.C1<sup>7</sup> G06F17/60, G06F19/00, G06F15/00, G06K17/00, G07F7/08,  
G07G1/12, H04L9/00, H04M1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Toroku Jitsuyo Shinan Koho	1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5907801 A (AT&T Wireless Services, Inc.), 25 May, 1999 (25.05.99), Fig. 3 (See "Terminal Number" and "Merchant ID"); Fig. 7 (See "Adapter ID"); column 10, lines 62 to 67 (Family: none)	1-3, 6-12, 14, 17, 18, 23, 24, 26, 40, 43, 44, 46, 48, 53, 59
X	US 5991410 A (AT&T Wireless Services, Inc.), 23 November, 1999 (23.11.99), Fig. 5 (See 203) (Family: none)	5, 14, 18, 19, 23, 24, 42, 46
X	WO 95/20195 A1 (Dynamic Data Systems Pty. Ltd.), 27 July, 1995 (27.07.95), Fig. 1; page 8 (Paragraph "An initial swipe of...") & AU 8321798 A1 & CA 2181999 A & CN 1142871 A & EP 0741884 A1 & JP 9-507719 A & NZ 265896 A & RU 2124231 C1 & US 6010067 A	14, 18, 19, 23, 24, 46

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 28 May, 2002 (28.05.02)	Date of mailing of the international search report 18 June, 2002 (18.06.02)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP02/02027

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 999678 A2 (Citibank, N.A.), 10 May, 2000 (10.05.00), Figs. 2, 4, 5; Par. Nos. [0044], [0049] & AU 58280/99 A & CN 1259822 A & JP 2000-232528 A	14, 18, 46
X	LUKE, Rob. "You've Got C@sh!", Banking Strategies, Vol.76, No.5 (September/October 2000), 2000.09.ISSN:1091-6385. Paragraph "Meanwhile, e-mail payment companies face..."	14, 18, 46
X	JP 2000-252978 A (Rohm Co., Ltd.), 14 September, 2000 (14.09.00), Figs. 1, 4; Par. No. [0028] & AU 1957500 A GB 2347537 A	26, 29, 48
Y	JP 2000-057278 A (Nippon LSI Card Kabushiki Kaisha), 25 February, 2000 (25.02.00), Par. Nos. [0025] to [0029] (Family: none)	31, 33, 49, 50
Y	JP 2-075062 A (NTT Data Communications Systems Corp. et al.), 14 March, 1990 (14.03.90), Fig. 1; page 3, upper right column, lines 11 to 16 & JP 2877316 B2	31, 33, 49, 50
A	EP 586081 A1 (Nokia Mobile Phones Ltd.), 27 July, 1993 (27.07.93), Column 7, lines 3 to 15 & AU 4435393 A & CN 1086367 A & DE 69317830 T2 & GB 2269512 A & JP 7-312630 A & US 6223052 A	1-64
A	JP 11-175668 A (Denso Corp.), 02 July, 1999 (02.07.99), Figs. 1 to 3 (Family: none)	1-64
A	JP 2001-043329 A (Matsushita Electric Industrial Co., Ltd.), 16 February, 2001 (16.02.01), Figs. 1, 2 (Family: none)	1-64

## A. 発明の属する分野の分類(国際特許分類(IPC))

*Int. Cl.*<sup>7</sup> G06F17/60

## B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

*Int. Cl.*<sup>7</sup> G06F17/60, G06F19/00, G06F15/00, G06K17/00, G07F7/08, G07G1/12, H04L9/00, H04M1/00

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922 - 1996年

日本国公開実用新案公報 1971 - 2002年

日本国実用新案登録公報 1996 - 2002年

日本国登録実用新案公報 1994 - 2002年

## 国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	US 5907801 A (AT&T WIRELESS SERVICES, INC.) 1999.05.25 <i>図3 ("terminal number" と "merchant ID" を見よ); 図7 ("adapter ID" を見よ); コラム10, 62-67行 (ファミリーなし)</i>	1-3, 6-12, 14, 17, 18, 23, 24, 26, 40, 43, 44, 46, 48, 53, 59
X	US 5991410 A (AT&T WIRELESS SERVICES, INC.) 1999.11.23 <i>図5 (203 を見よ) (ファミリーなし)</i>	5, 14, 18, 19, 23, 24, 42, 46

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示すもの
- 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

- 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日  
28.05.02国際調査報告の発送日  
**18.06.02**国際調査機関の名称及びあて先  
日本国特許庁 (ISA/JP)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号特許庁審査官(権限のある職員)  
阿波 進  
電話番号 03-3581-1101 内線 3561  
5 L 9168

C (続き) 関連すると認められる文献		関連する請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
X	WO 95/20195 A1 (DYNAMIC DATA SYSTEMS PTY. LTD.) 1995.07.27 図1; 8 ページ( "An initial swipe of ..." の段落) & AU 8321798 A1 & CA 2181999 A & CN 1142871 A & EP 0741884 A1 & JP 9-507719 A & NZ 265896 A & RU 2124231 C1 & US 6010067 A	14, 18, 19, 23, 24, 46
X	EP 999678 A2 (CITIBANK, N.A.) 2000.05.10 図2, 4, 5; 段落 0044, 0049 & AU 58280/99 A & CN 1259822 A & JP 2000-232528 A	14, 18, 46
X	LUKE, Rob. "You've Got C@sh!" <i>Banking Strategies</i> , vol. 76, no. 5 (September/October 2000), 2000.09. ISSN: 1091-6385. "Meanwhile, e-mail payment companies face ..." の段落	14, 18, 46
X	JP 2000-252978 A (ローム株式会社) 2000.09.14 図1, 4; 段落 0028 & AU 1957500 A & GB 2347537 A	26, 29, 48
Y	JP 2000-057278 A (日本エルエスアイカード株式会社) 2000.02.25 段落 0025-0029 (ファミリーなし)	31, 33, 49, 50
Y	JP 2-075062 A (エヌ・ティ・ティ・データ通信株式会社ほか) 1990.03.14 図1; 3 ページ, 右上欄, 11-16 行 & JP 2877316 B2	31, 33, 49, 50
A	EP 586081 A1 (NOKIA MOBILE PHONES LTD.) 1993.07.27 コラム7, 3-15 行 & AU 4435393 A & CN 1086367 A & DE 69317830 T2 & GB 2269512 A & JP 7-312630 A & US 6223052 A	1-64
A	JP 11-175668 A (株式会社デンソー) 1999.07.02	1-64

C(続き)	関連すると認められる文献	関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
A	図1-3 (ファミリーなし)  JP 2001-043329 A (松下電器産業株式会社) 2001.02.16 図1, 2 (ファミリーなし)	1-64