

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5534186号
(P5534186)

(45) 発行日 平成26年6月25日(2014.6.25)

(24) 登録日 平成26年5月9日(2014.5.9)

(51) Int. Cl.	F I	
G06F 21/44 (2013.01)	G06F 21/20	144C
G06F 21/34 (2013.01)	G06F 21/20	134
H04L 9/32 (2006.01)	H04L 9/00	673E
G06K 17/00 (2006.01)	G06K 17/00	F
H04W 84/10 (2009.01)	G06K 17/00	T

請求項の数 6 (全 17 頁) 最終頁に続く

(21) 出願番号 特願2010-81868 (P2010-81868)
 (22) 出願日 平成22年3月31日(2010.3.31)
 (65) 公開番号 特開2011-215764 (P2011-215764A)
 (43) 公開日 平成23年10月27日(2011.10.27)
 審査請求日 平成25年1月31日(2013.1.31)

(73) 特許権者 000002897
 大日本印刷株式会社
 東京都新宿区市谷加賀町一丁目1番1号
 (74) 代理人 110000958
 特許業務法人 インテクト国際特許事務所
 (74) 代理人 100083839
 弁理士 石川 泰男
 (74) 代理人 100120189
 弁理士 奥 和幸
 (72) 発明者 大石 真徳
 東京都新宿区市谷加賀町一丁目1番1号
 大日本印刷株式会社内
 審査官 金木 陽一

最終頁に続く

(54) 【発明の名称】 情報処理システム、情報処理サーバ、情報処理方法及び情報処理プログラム等

(57) 【特許請求の範囲】

【請求項1】

ICチップに記憶され且つ当該ICチップを他のICチップから識別するためのICチップ識別情報に基づいて認証処理を行う情報処理サーバであって、

ネットワークを介して接続される端末装置から、前記ICチップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として受信する受信手段と、

前記受信したICチップ識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶手段と、

前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信手段と、

前記新たな前記認証処理を行う場合において、前記受信した端末装置識別情報に対して前記登録情報において対応付けられている前記ICチップ識別情報に基づいて、前記新たな前記認証処理を行う認証手段と、

を備えることを特徴とする情報処理サーバ。

【請求項2】

請求項1に記載の情報処理サーバであって、

前記端末装置はNFCモジュールを備える携帯電話機であり、

前記ICチップ識別情報を前記NFCモジュールによって取得し、前記情報処理サーバへ送信することを特徴とする情報処理サーバ。

【請求項 3】

請求項 1 又は 2 に記載の情報処理サーバであって、

前記端末装置は SIM カードを備える携帯電話機であり、前記端末装置識別情報は SIM カードに付与される ID であることを特徴とする情報処理サーバ。

【請求項 4】

端末装置と、IC チップに記憶され且つ当該 IC チップを他の IC チップから識別するための IC チップ識別情報に基づいて認証処理を行う情報処理サーバとを備える情報処理システムであって、

前記端末装置は、前記 IC チップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として、ネットワークを介して前記情報処理サーバへ送信する送信手段を備え、

前記情報処理サーバは、

前記端末装置から、前記 IC チップ識別情報と、前記端末装置識別情報と、を一組として受信する受信手段と、

前記受信した IC チップ識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶手段と、

前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信手段と、

前記新たな前記認証処理を行う場合において、前記受信した端末装置識別情報に対して前記登録情報において対応付けられている前記 IC チップ識別情報に基づいて、前記新たな前記認証処理を行う認証手段と、

を備えることを特徴とする情報処理システム。

【請求項 5】

IC チップに記憶され且つ当該 IC チップを他の IC チップから識別するための IC チップ識別情報に基づいて認証処理を行う情報処理サーバにおける情報処理方法であって、

ネットワークを介して接続される端末装置から、前記 IC チップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として受信する受信ステップと、

前記受信した IC チップ識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶ステップと、

前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信ステップと、

前記新たな前記認証処理を行う場合において、前記受信した端末装置の識別情報に対して前記登録情報において対応付けられている前記 IC チップ識別情報に基づいて、前記新たな前記認証処理を行う認証ステップと、

を含むことを特徴とする情報処理方法。

【請求項 6】

IC チップに記憶され且つ当該 IC チップを他の IC チップから識別するための IC チップ識別情報に基づいて認証処理を行う情報処理サーバに含まれるコンピュータを、

ネットワークを介して接続される端末装置から、前記 IC チップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として受信する受信手段、

前記受信した IC チップ識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶手段、

前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信手段、

前記新たな前記認証処理を行う場合において、前記受信した端末装置識別情報に対して前記登録情報において対応付けられている前記 IC チップ識別情報に基づいて、前記新たな前記認証処理を行う認証手段、

として機能させることを特徴とする情報処理プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理システム、情報処理サーバ、情報処理方法及び情報処理プログラム等に関するものであり、より詳細には、例えば、ＩＣカードを用いて認証処理を行う情報処理システム、情報処理サーバ、情報処理方法及び情報処理プログラム等の技術分野に関する。

【背景技術】

【0002】

近年、ＩＣカード関連技術の発達に伴い、かかるＩＣカードを用いたシステムの信頼性、可用性及び保守性が確立された結果、様々なシステムにおいてＩＣカードが採用されるようになってきている。当該ＩＣカードは、採用されるシステムに応じて様々な機能を備えている。このようなＩＣカードの一例として、例えば、Felica（登録商標）の技術を用いた乗車券や電子マネーとしての機能を備えたSuica（登録商標）、所定の場所における入退出時間を記憶する機能を備えた入退出を管理するＩＣカード、店舗等において商品を購入する毎に付与されるポイントを顧客情報とともに記憶する機能を備えた所謂ポイントカードとしてのＩＣカード、又は所定の情報処理サーバとの間で決算処理が行われるクレジット機能を備えたＩＣカード等が挙げられる。

10

【0003】

また、特許文献１及び２では、ＩＣカードを用いたシステムを利用する者が携行する物品に当該ＩＣカードの機能を具備させ、当該システムの円滑な運用を図るべく、携帯電話端末にＩＣカードの機能を具備させる技術が開示されている。

20

【先行技術文献】

【特許文献】

【0004】

【特許文献１】特開２００８－３０５３８８号公報

【特許文献２】特開２００８－２１１８４９号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

30

しかしながら、上記ＩＣカードは、採用されるシステムに応じて異なる機能を備えた個別のＩＣカードが用意されているため、当該システムを利用する者は、かかるシステムに応じた個別のカードを所有する必要がある。換言すれば、上記システムのうち複数の異なるシステムを利用する場合には、かかる利用者は、システム毎に複数毎ＩＣカードを所持する必要があり、当該ＩＣカードの管理が煩雑となる。

【0006】

また、特許文献１及び２に記載の技術では、上記ＩＣカードの機能を携帯電話端末に付与することは可能であるが、現在所有するＩＣカードとは全く別のＩＣカードを新たに発行（作り出す）することとなるため、使用中のデータを引き継げない等、サービスによっては新たに個人情報を登録しなければならない等の手間が必要になる。

40

【0007】

そこで、本発明は上記各問題点に鑑みてなされたもので、その目的の一例は、ＩＣカードが備える機能を簡便な手続で実行することができる情報処理サーバ、情報処理方法及び情報処理プログラムを提供することを課題とする。

【課題を解決するための手段】

【0008】

上記の問題を解決するために、請求項１に記載の発明は、Cチップに記憶され且つ当該ＩＣチップを他のＩＣチップから識別するためのＩＣチップ識別情報に基づいて認証処理を行う情報処理サーバであって、ネットワークを介して接続される端末装置から、前記ＩＣチップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報

50

と、を一組として受信する受信手段と、前記受信したＩＣチップ識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶手段と、前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信手段と、前記新たな前記認証処理を行う場合において、前記受信した端末装置識別情報に対して前記登録情報において対応付けられている前記ＩＣチップ識別情報に基づいて、前記新たな前記認証処理を行う認証手段と、を備える。

【 0 0 0 9 】

この発明によれば、ＩＣカードが備える機能を簡便な手続で実行することができる。

【 0 0 1 0 】

請求項 2 に記載の発明は、請求項 1 に記載の情報処理サーバであって、前記端末装置は N F C モジュールを備える携帯電話機であり、前記 I C チップ識別情報を前記 N F C モジュールによって取得し、前記情報処理サーバへ送信する。

10

【 0 0 1 1 】

この発明によれば、種々の I C カードが備える機能を簡便な手続で実行することができる。

【 0 0 1 2 】

請求項 3 に記載の発明は、請求項 1 又は 2 に記載の情報処理サーバであって、前記端末装置は S I M カードを備える携帯電話機であり、前記端末装置識別情報は S I M カードに付与される I D であることを特徴とする。

【 0 0 1 3 】

この発明によれば、ＩＣカードが備える機能をより簡便な手続で、更に安全に実行することができる。

20

【 0 0 1 4 】

請求項 4 に記載の発明は、端末装置と、ＩＣチップに記憶され且つ当該 I C チップを他の I C チップから識別するための I C チップ識別情報に基づいて認証処理を行う情報処理サーバとを備える情報処理システムであって、前記端末装置は、前記 I C チップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として、ネットワークを介して前記情報処理サーバへ送信する送信手段を備え、前記情報処理サーバは、前記端末装置から、前記 I C チップ識別情報と、前記端末装置識別情報と、を一組として受信する受信手段と、前記受信した I C チップ識別情報と端末装置識別情報とを
対応付けて登録情報として記憶する記憶手段と、前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信手段と、前記新たな前記認証処理を行う場合において、前記受信した端末装置識別情報に対して前記登録情報において対応付けられている前記 I C チップ識別情報に基づいて、前記新たな前記認証処理を行う認証手段と、を備えることを特徴とする。

30

【 0 0 1 5 】

請求項 5 に記載の発明は、ＩＣチップに記憶され且つ当該 I C チップを他の I C チップから識別するための I C チップ識別情報に基づいて認証処理を行う情報処理サーバにおける情報処理方法であって、ネットワークを介して接続される端末装置から、前記 I C チップ識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として受信する受信ステップと、前記受信した I C チップ識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶ステップと、前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信ステップと、前記新たな前記認証処理を行う場合において、前記受信した端末装置の識別情報に対して前記登録情報において対応付けられている前記 I C チップ識別情報に基づいて、前記新たな前記認証処理を行う認証ステップと、を含むことを特徴とする。

40

【 0 0 1 6 】

請求項 6 に記載の発明は、ＩＣチップに記憶され且つ当該 I C チップを他の I C チップから識別するための I C チップ識別情報に基づいて認証処理を行う情報処理サーバに含

50

れるコンピュータを、ネットワークを介して接続される端末装置から、前記 I C チップ 識別情報と、前記端末装置を他の端末装置から識別するための端末装置識別情報と、を一組として受信する受信手段、前記受信した I C チップ 識別情報と端末装置識別情報とを対応付けて登録情報として記憶する記憶手段、前記登録情報が記憶された後に、新たな前記認証処理を行う場合において、前記端末装置から前記端末装置識別情報を受信する識別情報受信手段、前記新たな前記認証処理を行う場合において、前記受信した端末装置識別情報に対して前記登録情報において対応付けられている前記 I C チップ 識別情報に基づいて、前記新たな前記認証処理を行う認証手段、として機能させることを特徴とする。

【発明の効果】

【 0 0 1 7 】

以上のように、本発明によれば、受信した端末装置識別情報に対応付けられた I C チップ 識別情報に基づいて認証処理を行うため、I C カードが備える機能を簡便な手続で実行することができる。

【図面の簡単な説明】

【 0 0 1 8 】

【図 1】本実施形態に係る情報処理システム S の概要構成の一例を示す図である。

【図 2】本実施形態に係る情報処理サーバ 1 の概要構成の一例を示すブロック図である。

【図 3】記憶部 1 3 に構築される、契約者情報 DB 1 3 1 及び登録情報 DB 1 3 2 に記憶される情報を示すテーブルである。

【図 4】携帯電話機 2 内の機能ブロックの一例を示す概念図である。

【図 5】本実施形態における情報処理システム S の上記登録情報が記憶されるまでの処理及び情報の流れ等を示すシーケンス図である。

【図 6】本実施形態における上記登録情報が記憶されるまでについての動作例を示す概念図である。

【図 7】本実施形態における情報処理システム S の本実施形態における S I M 番号を用いた認証処理についての処理及び情報の流れ等を示すシーケンス図である。

【図 8】複数の I C カードの上記認証処理を受ける機能を取り込んで、各 I C カードとして振舞う携帯電話機 2 を示す概念図である。

【図 9】本実施形態における効果を示す概念図である。

【発明を実施するための形態】

【 0 0 1 9 】

以下、図面を参照して本発明の実施形態について説明する。なお、以下に説明する実施の形態は、情報処理システムに対して本発明を適用した場合の実施形態である。

【 0 0 2 0 】

まず、本発明の一実施形態に係る情報処理システム S の構成及び概要機能について、図 1 を用いて説明する。

【 0 0 2 1 】

図 1 は、本実施形態に係る情報処理システム S の概要構成の一例を示す図である。

【 0 0 2 2 】

図 1 に示すように、情報処理システム S は、I C カード 3 を用いたシステムを運用する企業側に備えられる情報処理サーバ 1 と、このシステムを利用する契約を結んだ者（以下、単に「契約者」とする。）側に備えられる携帯電話機 2（端末装置の一例）と、企業側から契約者に付与（貸与又は譲渡等を含む）される図示しない I C チップを備える I C カード 3 と、を含んで構成される。

【 0 0 2 3 】

また、情報処理サーバ 1 と携帯電話機 2 は、ネットワーク NW を介して、相互にデータの送受信が可能になっている。なお、ネットワーク NW は、インターネット、専用通信回線（例えば、C A T V（Community Antenna Television）回線）、移動体通信網（基地局等を含む）、及びゲートウェイ等により構築されている（通信プロトコルに T C P / I P（Transmission Control Protocol/Internet Protocol）等を採用）。また、I C カード

10

20

30

40

50

3と情報処理サーバ1は、図示しないリーダライタ装置を介して非接触で相互にデータの送受信が可能となっている。かかるリーダライタ装置は、例えば、非接触ICカード技術である公知のFeliCa技術を採用したRFIDリーダライタが適用され、当該FeliCa技術を採用したICチップからのデータの読み取り及び当該ICチップへのデータの書き込みを所定周波数の電波により非接触で（非接触通信により）行うことが可能になっている。更に、ICカード3と携帯電話機2は、詳しくは後述するが、携帯電話機2に備えられるリーダライタ機能によって相互にデータの送受信が可能となっている。

【0024】

なお、図1の例では、説明の便宜上、情報処理サーバ1及びICカード3は一つずつ示されているが、システムを運用する企業側毎に多数存在するようにしてもよい。また、携帯電話機2は、契約者毎に多数存在する。

10

【0025】

[1-1.情報処理サーバ1の構成及び機能]

次に、情報処理サーバ1の構成及び機能について、図2を用いて説明する。

【0026】

図2は、本実施形態に係る情報処理サーバ1の概要構成の一例を示すブロック図である。

【0027】

図2に示すように、情報提供サーバ1は、通信部11と、操作部12と、記憶部13と、入出力インターフェース部16と、システム制御部14（受信手段、記憶手段、登録情報送信手段、識別情報受信手段、認証手段の一例）とを備えている。そして、システム制御部14と入出力インターフェース部16とは、システムバス15を介して接続されている。

20

【0028】

通信部11は、ネットワークNWに接続して、携帯電話機2との通信を制御する。また、通信部11は、図示しないリーダライタ装置を介して、ICカード3との通信を制御する。

【0029】

操作部12は、例えば、キーボード及びマウス等を備える。

【0030】

記憶部13は、例えば、ハードディスクドライブ等により構成されており、オペレーティングシステム及びデータ抽出プログラム等の各種プログラムを記憶する。

30

【0031】

また、記憶部13には、契約者情報DB（データベース）131、及び登録情報DB132が構築されている。

【0032】

なお、これらのデータベースは、データベースを管理するデータベースサーバに構築されるようにしてもよい。この場合、情報提供サーバ1は、上記データベースサーバ、その他のサーバから構成されるサーバ群として構成するようにしてもよい。

【0033】

ここで、記憶部13に構築される契約者情報DB131、及び登録情報DB132について、図3と対応付けて説明する。

40

【0034】

図3は、記憶部13に構築される契約者情報DB131及び登録情報DB132に記憶される情報を示すテーブルである。

【0035】

図3(A)に示す契約者情報データベース(DB)131には、契約者情報として、契約者（後述するクレジットカードの契約者）のユーザID、後述するICカード識別情報（ICチップ識別情報の一例）、パスワード、名称、住所、電話番号、メールアドレス等の属性情報が登録されている。かかる契約者情報は、契約者のユーザIDによって契約者

50

毎に判別可能になっている。ここで、契約者のユーザIDは、ユーザを識別するための識別子である。またICカード識別情報は、契約者情報として登録されているため、契約者を識別するための識別情報として用いることができる。

【0036】

図3(B)に示す登録情報データベース(DB)132には、登録情報として、契約者のユーザID、ICカード識別情報、及び後述するSIM番号(端末装置識別情報の一例)が登録されている。このSIM番号は、登録情報として登録されているため、契約者を識別するための識別情報として用いることができる。さらに、登録情報として登録されているユーザIDから、契約者情報DB131を参照して、契約者情報をユーザ毎に識別することができる。

10

【0037】

入出力インターフェース部16は、通信部11及び記憶部13とシステム制御部14との間のインターフェース処理を行うようになっている。

【0038】

システム制御部14は、CPU(Central Processing Unit)14a、ROM(Read Only Memory)14b、RAM(Random Access Memory)14c等により構成されている。

【0039】

そして、システム制御部14は、CPU14aが、ROM14bや記憶部13に記憶された各種プログラムを読み出し実行することにより、上記各手段として機能するようになっている。

20

【0040】

また、本実施形態における情報処理サーバ1は、ICカード3を用いたシステムを運用する企業側、例えばクレジットカードの契約者との間で決算処理を行う信販会社等に備えられ、契約者が例えば店舗における商品の購入又はサービスの提供を受ける際に、その代金を信販会社等に事後的に支払う信用取引を行うようになっている。

【0041】

かかる信用取引を行うために、システム制御部14は、契約者が所有するICカード3のICチップに記憶されたICカード識別情報を参照して認証処理を行い、認証結果に基づいて決算処理を行い、上記信用取引を成立させるようになっている。

【0042】

ここで、認証処理とは、信用取引を行う者が契約者本人であり、当該契約者が信用取引を行う権利を有することを確認するための処理(本人確認)である。この認証処理は公知の手法であるため詳しい説明は省略するが、その一例として、上記信用取引時に、情報処理システム1は、契約者が所有するICカードに記憶されたICカード識別情報の送信を要求する。そして、情報処理システム1は、送信されたICカード識別情報と、契約者情報DB131に登録されたICカード識別情報を照合して、本人確認を行うようになっている。

30

【0043】

具体的には、システム制御部14は、図示しないリーダライタ装置から送信されるICカード識別情報と、契約者情報DB131に記憶されるICカード識別情報を照合することにより契約者情報を検索し、当該契約者情報に登録されたICカード識別情報を照合して認証処理を行うようになっている。

40

【0044】

更に、システム制御部14は、携帯電話機2から送信されるICカード識別情報と携帯電話機2のSIM番号を受信すると、契約者情報DB131を参照して、受信したICカード識別情報が契約者情報として記憶されているか否かを確認する。そして、受信したICカード識別情報が契約者情報として記憶されていた場合には、システム制御部14は、当該ICカード識別情報と受信したSIM番号とを対応付けて登録情報として登録情報DB132に記憶するようになっている。

【0045】

50

すなわち、受信したICカード識別情報が契約者情報として記憶されていた場合には、かかるICカード識別情報を送信した者は、上記契約者であり、上記システムを利用する権利を有する者であることを示している。

【0046】

そこで、システム制御部14は、かかる契約者が新たに前記認証処理を行う場合には、携帯電話機2の操作によりSIM番号を送信することによって上記認証処理を可能とするために、当該ICカード識別情報と受信したSIM番号とを対応付けて登録情報として登録情報DB132に記憶するようになっている。

【0047】

以後、上記ICカード識別情報と受信したSIM番号とを対応付けて登録情報として記憶された場合の当該ICカード識別情報が示すICカードを、単に「登録情報が記憶されたICカード」とする。

【0048】

そして、システム制御部14は、この登録情報が記憶されると、新たに認証処理を行う場合には、登録情報DB132を参照して、携帯電話機2から送信されるSIM番号と対応付けられたICカード識別情報を検索し、検索されたICカード識別情報が契約者情報として記憶されていた場合には、当該契約者情報に登録されたICカード識別情報を用いて上記認証処理を行うようになっている。

【0049】

なお、情報処理サーバ1は、例えば、パーソナルコンピュータ、ワークステーション、PDA(Personal Digital Assistant)、STB(Set Top Box)、等を適用することができる。

【0050】

[1-2.携帯電話機2の構成及び機能]

携帯電話機2は、アンテナ、スピーカ、マイク、操作キー、ディスプレイ、及び電子回路基板(CPU、RAM、ROM(各種データ及び携帯電話機2の動作を担うプログラムを予め記憶)等が実装)により構成されている。

【0051】

図4は、携帯電話機2内の機能ブロックの一例を示す概念図である。

【0052】

図4に示すように、携帯電話機2は、一般的な通信制御機能(例えば、W-CDMA又はCDMA2000の通信方式による。本願の送信手段の一例。)、ブラウザ機能(URLを指定することで所定のサーバにアクセスして所定の情報を受ける(例えば、http(Hyper Text Transfer Protocol)による))、メーラ機能(例えば、メーラをユーザインターフェースとして、他の携帯電話機又はサーバ等との間でネットワークNWを介したデータの送受信を行う。)、携帯アプリ(携帯電話機の利用者が携帯電話機上で実行したい作業を実施する機能を直接的に有するソフトウェア)等を有している。なお、携帯電話機2におけるこれらの機能は公知であるため詳しい説明を省略する。

【0053】

また、携帯電話機2には、上述したSIM番号が記憶された図示しないSIMカードが備えられている。このSIM番号は、契約者の携帯電話機2に備えられるSIMカード(Subscriber Identity Module Card)に記憶される固有の識別番号であり、IMSI(International Mobile Subscriber Identity)とも呼ばれている。SIMカードについては公知の技術であるため詳しい説明は省略するが、携帯電話会社が発行する、固有の番号及び携帯電話番号等の契約者情報を記録したICカードであり、GSM(Global System for Mobile Communications)やW-CDMA(Wideband Code Division Multiple Access)などの方式の携帯電話機に差し込んで利用者の識別に用いられている。

【0054】

更に、本実施形態の携帯電話機2は、アンテナ及びNFC通信制御部(当該携帯電話機2におけるCPUと電氣的に接続されている)等を備えるNFCモジュールを搭載し、上

10

20

30

40

50

述したICカード3との間でデータ通信を可能とするリーダライタ機能を実現している。

【0055】

このリーダライタ機能は、例えば、非接触ICカード技術である公知のNFC(Near Field Communication)(登録商標)技術を採用しており、Mifare(登録商標)(ISO/IEC14443 TypeA)、ISO/IEC14443 TypeB、Felica及びISO/IEC15693技術を採用したICチップ(以下、「非接触ICチップ」という)が備えられたICカードから、データの読取り及びデータの書込みを非接触で行うことができる。

【0056】

NFCについては公知の技術であるため詳しい説明は省略するが、非接触ICカードとして機能し対応するMifare、ISO/IEC14443 TypeB、Felica及びISO/IEC15693として振る舞うことができるカードエミュレーション機能、リーダライタとして機能しMifare、ISO/IEC14443 TypeB、Felica及びISO/IEC15693に対応するICカード及びICチップの読み書きを可能とするリーダライタ(R/W)エミュレーション機能、そして、NFCを搭載した機器間で通信を行うことができる端末間通信機能の各種機能を備えている。

【0057】

更に、本実施形態における携帯電話機2は、上記携帯アプリの一例として認証処理用アプリを有している。この認証処理用アプリは、契約者が、ICカード3の代わりに携帯電話機2を用いて、上記企業との間で信用取引を成立させることを実現するためのソフトウェアである。

【0058】

具体的には、契約者の操作に基づき認証処理用アプリが起動されると、当該アプリの制御のもと、携帯電話機2のCPUは、携帯電話機2をICカード3として振る舞うべく、上記NFCのカードエミュレーション機能を起動させ、ICカード3のICチップに記憶されたICカード識別情報を読み取る。そして、携帯電話機2のCPUは、読み取ったICカード識別情報と、携帯電話機2のSIM番号とを、情報処理サーバ1へ送信するようになっている。

【0059】

更に、携帯電話機2のCPUは、情報処理サーバ1から上記登録情報を受信すると、新たに上記信用取引を成立させようとする際には、上記アプリの制御のもと上記NFCのリーダライタエミュレーション機能によって、SIM番号を情報処理サーバ1へ送信するようになっている。

【0060】

従って、携帯電話機2のCPUは、上記アプリの制御のもと、情報処理サーバ1へSIM番号を送信することによって、上記認証処理を受けることができる。換言すれば、本実施形態の携帯電話機2のCPUは、ICカード3の上記認証処理を受ける機能を取り込んで、ICカード3として振る舞うことを可能としている。

【0061】

なお、携帯機器としては、例えば、携帯電話機、PDA、ポータブルプレイヤー等を適用可能であるが、本実施形態においては、携帯電話機2を適用する。

【0062】

[1-3.ICカード3の構成及び機能]

ICカード3は、ICチップをICカード基体に備えている。

【0063】

ICチップは、図示しないインターフェース、ROM(Read Only Memory)、RAM(Random Access Memory)、EEPROM、CPU(Central Processing Unit)等を備えて構成されている。インターフェースは、上述したデータ等を送受信するための入出力ポート(port)であり、CPUは、インターフェースを介して、上述したリーダライタ装置や携帯電話機2等と交信する。EEPROMは、不揮発性半導体メモリの一種であり、記憶領域

10

20

30

40

50

に記憶されているデータを消去し、何度でも再記憶ができる P R O M (Programmable Rom) である。更に、E E P R O M は、上述した I C カード識別情報等の契約者の情報を格納 (記憶) する。この I C カード識別情報は、契約者に付与される I C カード自体を他の I C カードから識別するための識別情報であり、例えば、I C チップの製造業者等によって、製造時点に予め記憶されている。

【 0 0 6 4 】

[2 . 情報処理システムの動作]

次に、図 5 を用いて、本実施形態における上記登録情報が記憶されるまでについての動作例 (図 6) と、本実施形態における情報処理システム S の上記登録情報が記憶されるまでの処理及び情報の流れ等を示すシーケンス図とを対応付けて説明する。

10

【 0 0 6 5 】

図 5 は本実施形態における情報処理システム S の上記登録情報が記憶されるまでの処理及び情報の流れ等を示すシーケンス図であり、図 6 は本実施形態における上記登録情報が記憶されるまでについての動作例を示す概念図である。

【 0 0 6 6 】

図 5 において、I C カード 3 の代わりに携帯電話機 2 を用いて上記企業との間で信用取引を成立させるために、契約者の携帯電話機 2 の操作により認証処理用アプリケーションが起動されると (ステップ S 1)、携帯電話機 2 の C P U は、上記 N F C のカードエミュレーション機能を起動させ、I C カード 3 に対して I C カード識別情報の送信を要求する (ステップ S 2、図 6 (A))。

20

【 0 0 6 7 】

具体的には、例えば、携帯電話機 2 の C P U は、携帯電話機 2 のアンテナ部を介して、I C カード 3 の I C チップへ、I C カード 3 の動作に必要な電力及び I C カード識別情報の送信を要求するコマンドを送信する。

【 0 0 6 8 】

かかる電力及びコマンドを受信した I C チップは、携帯電話機 2 へ、I C カード識別情報を送信する (ステップ S 3)。

【 0 0 6 9 】

携帯電話機 2 の C P U は、I C カード識別情報を受信すると (ステップ S 4)、情報処理サーバ 1 へ、携帯電話機 2 の S I M 番号と受信した I C カード識別情報を送信する (ステップ S 5、図 6 (B))。

30

【 0 0 7 0 】

なお、携帯電話機 2 は、上記 S I M 番号と I C カード識別情報を、ネットワークを介して情報処理サーバ 1 へ送信するようにしてもよいし、図示しないリーダライタ装置を介して情報処理サーバ 1 へ送信するようにしてもよい。この場合、リーダライタ装置は、携帯電話機 2 の C P U から送信される上記 S I M 番号と I C カード識別情報を受信し、受信した S I M 番号と I C カード識別情報を、上記ネットワークを介して、情報処理サーバ 1 へ送信するようになっている。

【 0 0 7 1 】

情報処理サーバ 1 のシステム制御部 1 4 は、携帯電話機 2 から送信される S I M 番号と I C カード識別情報を受信すると (ステップ S 6)、契約者情報 D B 1 3 1 を参照して、受信した I C カード識別情報が契約者情報として記憶されているか否かを確認する。そして、受信した I C カード識別情報が契約者情報として記憶されていた場合には、システム制御部 1 4 は、当該 I C カード識別情報と受信した S I M 番号とを対応付けて登録情報として登録情報 D B 1 3 2 に記憶する (ステップ S 7、図 6 (C))。

40

【 0 0 7 2 】

なお、上記アプリは、I C カード識別情報と併せて、契約者に付与されているパスワードを合わせて送信させるようにしてもよい。これにより、真の契約者のみ以外は上記登録情報の記憶に関する処理を行うことができないため、セキュリティ性が向上する。

【 0 0 7 3 】

50

そして、システム制御部 14 は、登録情報を携帯電話機 2 の CPU へ送信する（ステップ S 8）。

【0074】

以上の動作により、上述したように上記 NFC のリーダライタエミュレーション機能によって IC カード 3 を取り込んだ携帯電話機 2 は、情報処理サーバ 1 に、SIM 番号を送信することによって、上記認証処理

IC カード 3 として振舞うことができる。

【0075】

次に、図 7 を用いて、本実施形態における情報処理システム S の本実施形態における SIM 番号を用いた認証処理についての処理及び情報の流れ等を説明する。

10

【0076】

図 7 は本実施形態における情報処理システム S の本実施形態における SIM 番号を用いた認証処理についての処理及び情報の流れ等を示すシーケンス図である。

【0077】

図 7 では、例えば、登録情報が記憶された IC カードの所有者である契約者が、店舗における商品の購入又はサービスの提供を受ける際にその代金を信販会社等に事後的に支払う信用取引を、携帯電話機 2 を用いて行うための処理及び情報の流れ等が示されている。

【0078】

具体的には、契約者が店舗において上記信用取引を行うため、かかる契約者の携帯電話機 2 の操作により、携帯電話機 2 の CPU は、認証処理用アプリを起動する（ステップ S 11）。

20

【0079】

ついで、例えば店舗の経営者の操作に基づき店舗に備えられたリーダライタ装置から、IC カードの情報の送信要求がなされると（ステップ S 12）、携帯電話機 2 の CPU は、かかる送信要求を受信した上記認証処理用アプリの制御により、上記リーダライタ装置へ、携帯電話機 2 の SIM 番号を送信する（ステップ S 13）。

【0080】

上記 SIM 番号を受信したリーダライタ装置は、かかる SIM 番号を、情報処理サーバ 1 へ送信する（ステップ S 15）。

【0081】

30

リーダライタ装置から送信される SIM 番号を受信した情報処理サーバ 1 のシステム制御部 14 は、登録情報を検索する（ステップ S 16）。

【0082】

具体的には、システム制御部 14 は、登録情報 DB 132 を参照して、上記 SIM 番号と対応付けられた IC カード識別情報を検索し、検索された IC カード識別情報が契約者情報として記憶されていた場合には、この検索結果をリーダライタ装置へ送信する（ステップ S 17）。

【0083】

かかる検索結果を受信したリーダライタ装置は、上記認証処理を行う（ステップ S 18）。

40

【0084】

なお、かかる認証処理は、上述したようにシステム制御部 14 が行うようにしてもよい。

【0085】

そして、リーダライタ装置は、上記認証処理の結果を携帯電話機 2 へ送信し（ステップ S 19）、携帯電話機 2 の CPU は、受信した認証処理の結果を記憶（更新）した旨をリーダライタ装置へ送信する（ステップ S 20）。

【0086】

なお、以上説明した本実施形態の携帯電話機 2 の CPU は、IC カード 3 の上記認証処理を受ける機能を取り込んで IC カード 3 として振舞うことを可能としているが、携帯電

50

話機 2 の CPU は、複数の IC カードの上記認証処理を受ける機能を取り込んで、各 IC カードとして振る舞うようにしてもよい。

【 0 0 8 7 】

ここで、図 8 を用いて、複数の IC カードの上記認証処理を受ける機能を取り込んで、各 IC カードとして振る舞う他の実施例について説明する。

【 0 0 8 8 】

図 8 は、複数の IC カードの上記認証処理を受ける機能を取り込んで、各 IC カードとして振る舞う携帯電話機 2 を示す概念図である。

【 0 0 8 9 】

IC カードを用いたシステムでは、当該システム毎に、異なる種類の IC カードが存在し、各システムにおいて上記認証処理が行われている。

【 0 0 9 0 】

具体的には、所定の場所における入退出時間を管理するシステムでは入退出管理用の IC カードに記憶された IC カード識別情報を用いて上記認証処理が行われ、IC カードが付与された者の入退出時間が管理されている。また、店舗等において商品を購入する毎に付与されるポイントを顧客情報とともに管理するシステムでは、ポイント管理用の IC カードに記憶された IC カード識別情報を用いて上記認証処理が行われ、IC カードが付与された者のポイントが管理されている。

【 0 0 9 1 】

そこで、各システムに応じた上記認証処理用アプリを用意し、かかるアプリを用いて、本実施形態の携帯電話機 2 に、各システムの IC カードの上記認証処理を受ける機能を取り込ませて、携帯電話機 2 を、各 IC カードとして振る舞わせるようにしてもよい。

【 0 0 9 2 】

この認証用アプリの動作は、上述した動作と同様であるため、詳しい説明は省略する。

【 0 0 9 3 】

次に、図 9 を用いて、本実施形態における効果について説明する。

【 0 0 9 4 】

図 9 は、本実施形態における効果を示す概念図である。

【 0 0 9 5 】

図 9 に示すように、携帯電話機 2 が、IC カード 3 の上記認証処理を受ける機能を取り込むことにより、携帯電話機 2 のディスプレイ機能に IC カードの中身、例えば、契約者が上記信用取引によって消費した金額や、上記ポイントの合計等を確認することも可能となる。

【 0 0 9 6 】

なお、以上説明した実施形態は特許請求の範囲にかかる発明を限定するものではない。そして、上記実施形態の中で説明されている構成の組み合わせ全てが発明の課題解決に必須の手段であるとは限らない。

【 0 0 9 7 】

以上説明したように、本実施形態によれば、システム制御部 1 4 は、ネットワークを介して接続される携帯電話機 2 から、IC カード識別情報と、SIM 番号を受信し、受信した IC カード識別情報と、SIM 番号とを対応付けて登録情報として記憶し、前記登録情報が記憶された後に、新たに上記認証処理を行う場合には、受信した SIM 番号に対応付けられた IC カード識別情報に基づいて認証処理を行うように構成したため、IC カード 3 が備える機能を簡便な手続で実行することができる。

【 0 0 9 8 】

なお、上記実施形態においては、本願を IC カード取引システムに対して適用した場合の例を示したが、その他にも例えば、IC カードを用いた入退出管理システム等、IC カードを用いた各種認証システム等に対しても適用することができる。

【 0 0 9 9 】

また、本願の IC チップは、IC カードのみならず、携帯電話機、PDA 等の携帯型情

10

20

30

40

50

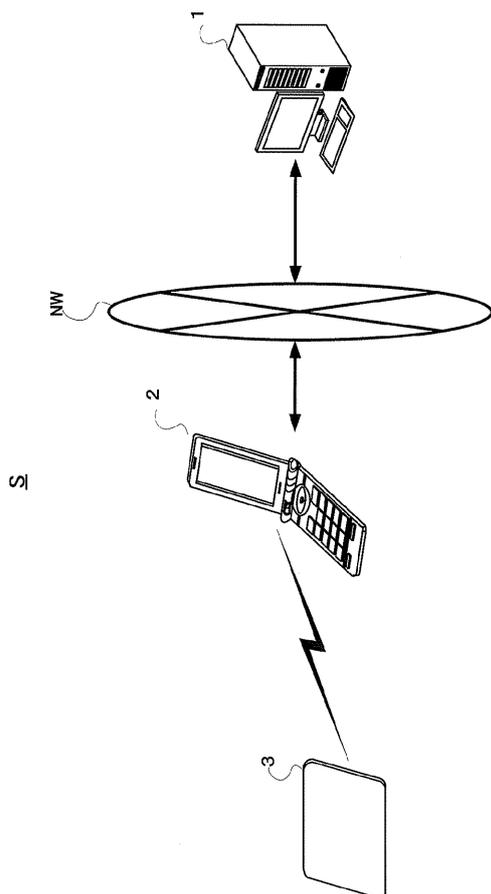
報端末に対しても適用可能である。

【符号の説明】

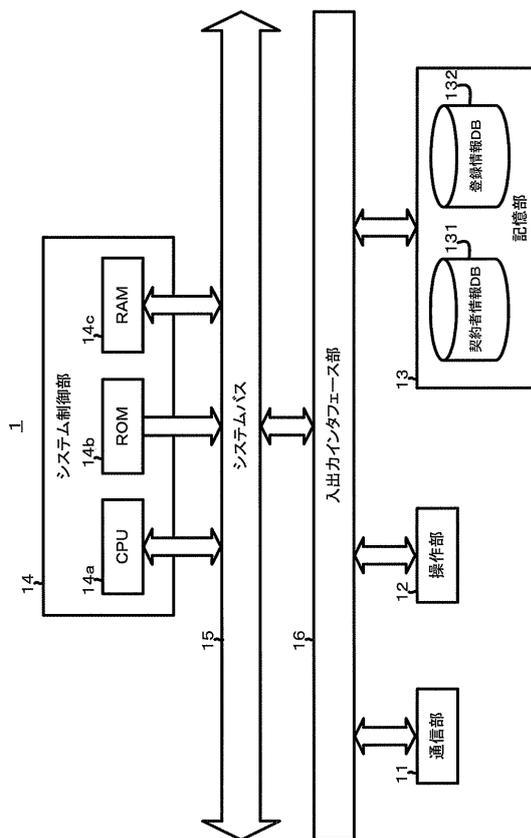
【0100】

- 1 情報処理サーバ
- 2 携帯電話機
- 3 ICカード
- 11 通信部
- 12 操作部
- 13 記憶部
- 14 システム制御部
- 15 システムバス
- 16 入出インターフェース部
- NW ネットワーク
- S 情報処理システム

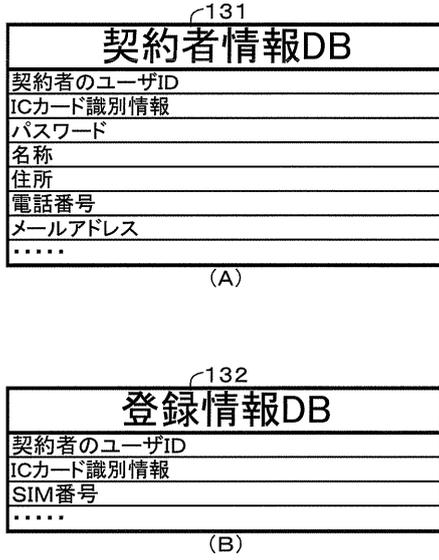
【図1】



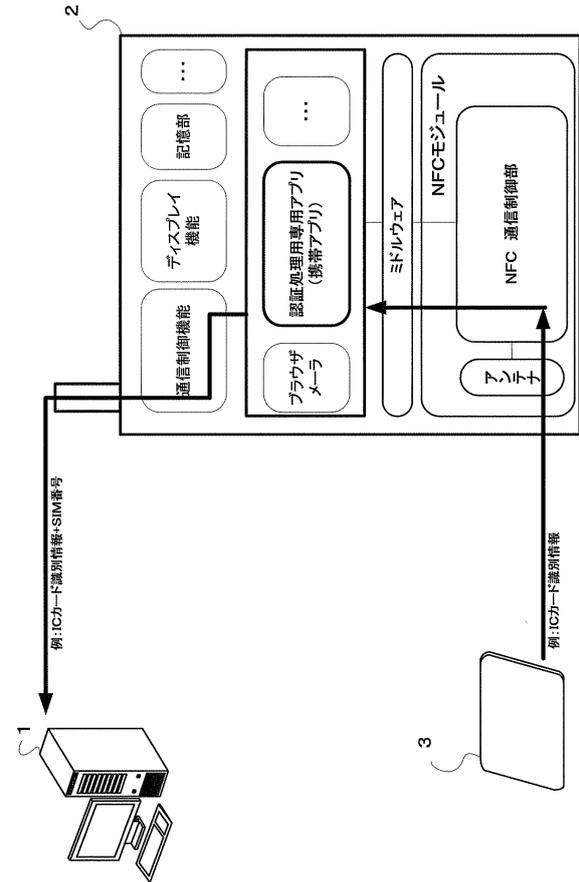
【図2】



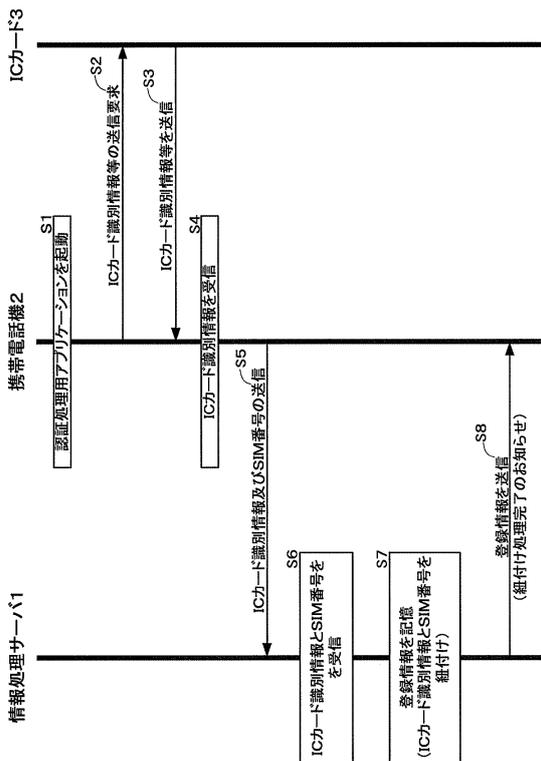
【図3】



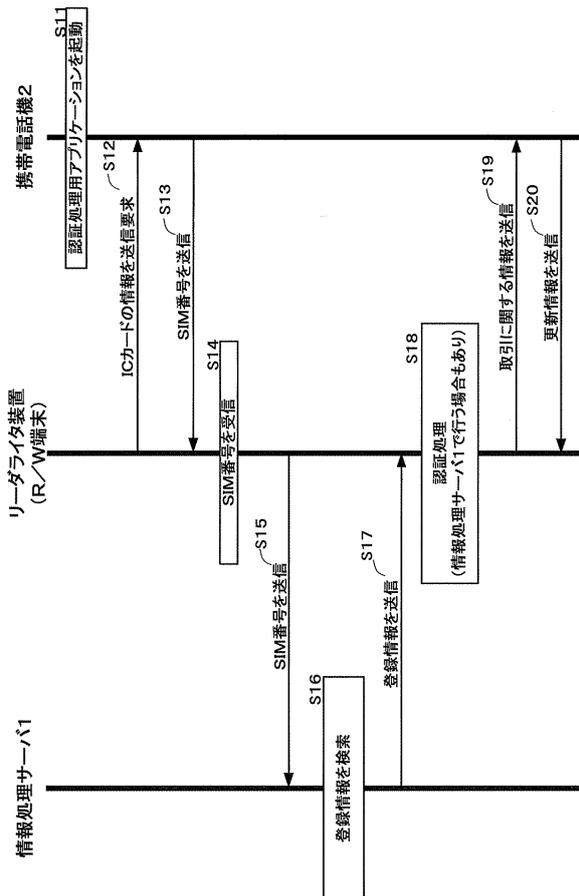
【図4】



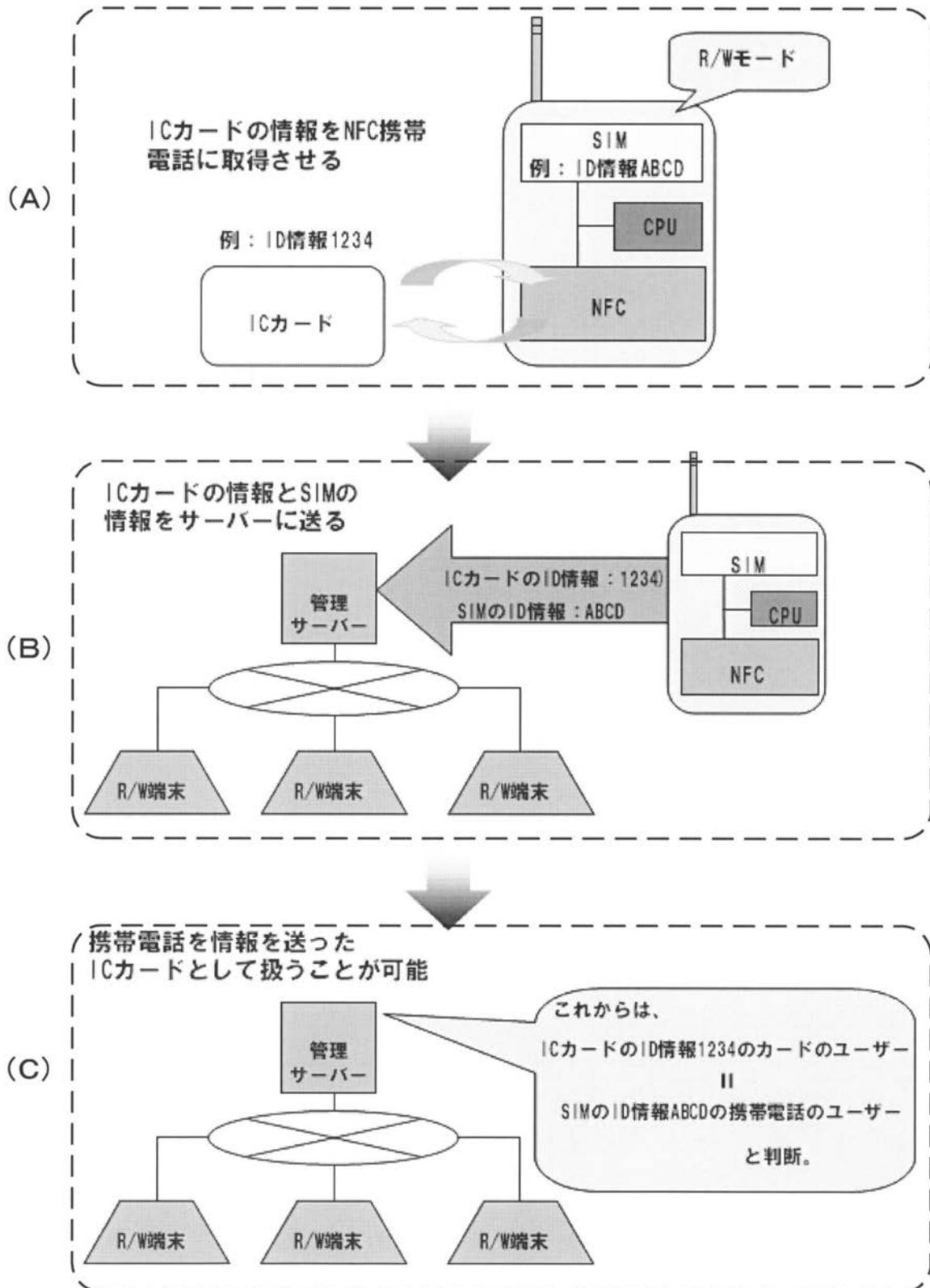
【図5】



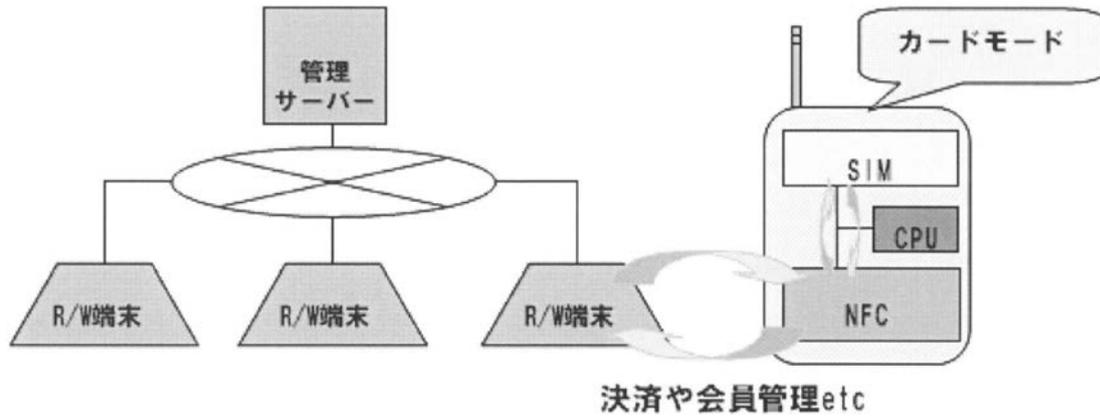
【図7】



【図6】

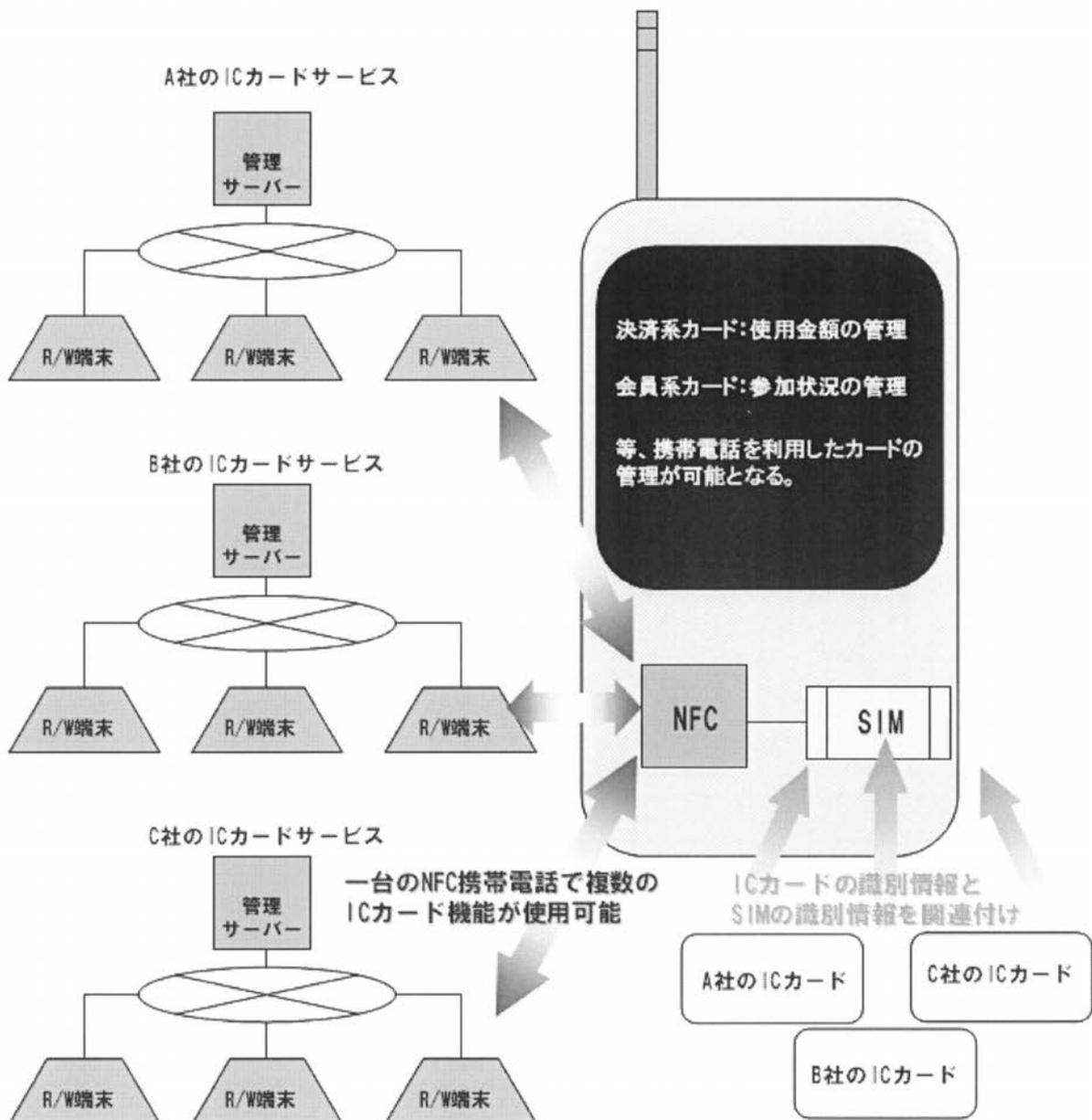


【図8】



以上のプロセスを他のICカードにも行うことで、ICカードの機能を携帯電話に集約することが可能

【図9】



 フロントページの続き

(51) Int.Cl.			F I		
<i>H 0 4 M</i>	<i>1/727</i>	<i>(2006.01)</i>	<i>H 0 4 W</i>	84/10	1 1 0
<i>H 0 4 M</i>	<i>3/42</i>	<i>(2006.01)</i>	<i>H 0 4 M</i>	1/727	
			<i>H 0 4 M</i>	3/42	D

(56) 参考文献 特開 2 0 0 3 - 2 9 6 6 4 9 (J P , A)
 特開 2 0 0 6 - 1 0 7 3 1 6 (J P , A)
 特開 2 0 0 6 - 0 6 7 5 0 9 (J P , A)
 特開 2 0 0 7 - 0 8 0 0 0 6 (J P , A)
 特開 2 0 1 0 - 1 8 1 9 8 8 (J P , A)

(58) 調査した分野(Int.Cl. , DB名)

G 0 6 F	2 1 / 4 4
G 0 6 F	2 1 / 3 4
G 0 6 K	1 7 / 0 0
H 0 4 L	9 / 3 2
H 0 4 M	1 / 7 2 7
H 0 4 M	3 / 4 2
H 0 4 W	8 4 / 1 0