(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
2022年9月22日(22.09.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/196150 A1

(51) 国際特許分類:
G06Q 20/34 (2012.01) *G06F 21/60* (2013.01)
G06F 21/32 (2013.01) *H04L 9/10* (2006.01)
G06F 21/44 (2013.01) *H04L 9/32* (2006.01)

(21) 国際出願番号： PCT/JP2022/004002

(22) 国際出願日： 2022年2月2日(02.02.2022)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

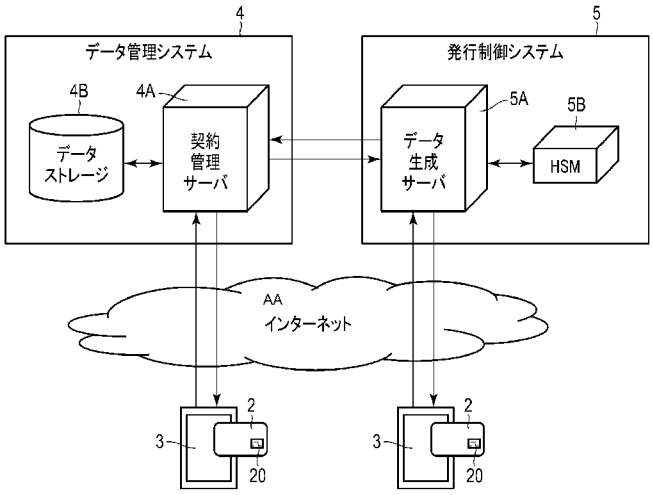
(30) 優先権データ：
特願 2021-044573 2021年3月18日(18.03.2021) JP
特願 2021-044594 2021年3月18日(18.03.2021) JP
特願 2021-146164 2021年9月8日(08.09.2021) JP

(71) 出願人: 株式会社 東芝 (**KABUSHIKI KAISHA TOSHIBA**) [JP/JP]; 〒1050023 東京都港区芝浦一丁目1番1号 Tokyo (JP). 東芝インフラシステムズ株式会社 (**TOSHIBA INFRASTRUCTURE SYSTEMS & SOLUTIONS CORPORATION**) [JP/JP]; 〒2120013 神奈川県川崎市幸区堀川町72番地34 Kanagawa (JP).

(72) 発明者: 三澤 裕人 (**MISAWA, Yuto**); 〒2120013 神奈川県川崎市幸区堀川町72番地34 東芝インフラシステムズ株式会社内 Kanagawa (JP). 宇野 美月 (**UNO, Mizuki**); 〒2120013 神奈川県川崎市幸区堀川町72番地34 東芝インフラシステムズ株式会社内 Kanagawa (JP).

(54) **Title:** REMOTE ISSUING SYSTEM AND DATA-GENERATING SERVER

(54) 発明の名称： リモート発行システムおよびデータ生成サーバ



4 Data management system
4A Contract management server
4B Data storage
5 Issuing control system
5A Data-generating server
5B HSM
AA Internet

(57) **Abstract:** According to the embodiment of the present invention, a remote issuing system includes a portable electronic device and a data-generating server. The portable electronic device includes a biometric sensor, a memory, a communication interface, and a first processor. If biometric authentication is successful, the first processor generates authentication data for performing an issuing process in the portable electronic device, outputs the authentication data to a reader–writer, and executes the issuing process on the basis of issuing data supplied by the reader–writer. The data-generating

WO 2022/196150 A1

[続葉有]

(74) 代理人: 蔵田 昌俊，外 (KURATA, Masatoshi et al.)；〒1050014 東京都港区芝三丁目２３番１号 セレスティン芝三井ビルディング１１階 鈴榮特許綜合事務所内 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一　国際調査報告（条約第21条(3)）

server includes a communication unit and a second processor. The second processor generates issuing data causing the portable electronic device to execute the issuing process on the basis of application data corresponding to a contract ID and the authentication data, and transmits the generated issuing data to a user terminal.

(57) 要約：実施形態によれば、リモート発行システムは、携帯可能電子装置とデータ生成サーバとを有する。携帯可能電子装置は、生体センサとメモリと通信インターフェースと第１プロセッサとを有する。第１プロセッサは、生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、認証データを前記リーダライタへ出力し、リーダライタから供給される発行データに基づいて発行処理を実行する。データ生成サーバは、通信部と第２プロセッサとを有する。第２プロセッサは、契約ＩＤに対応する申請データと認証データとに基づいて携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データをユーザ端末へ送信する。

明　細　書

発明の名称 ： リモート発行システムおよびデータ生成サーバ

技術分野

[0001] 本発明の実施形態は、リモート発行システムおよびデータ生成サーバに関する。

背景技術

[0002] 従来、携帯可能電子装置としてのＩＣカードは、クレジットカード等として運用するための情報を運用機関が書き込んで使用可能とする二次発行という手続きが必要である。また、ＩＣカードに対して、新たな機能を追加する場合も運用機関による所定の手続きが必要である。従来、ＩＣカードに対する二次発行や機能追加は、運用機関又は取扱い店舗の係員が公的な証明書などによってユーザの本人確認を行った後に、専用の発行機を用いて行っている。

[0003] 上述したような従来のＩＣカードに対する二次発行や機能追加などの発行処理の手続きでは、ユーザが運用機関又は店舗などの指定場所へ行ったり、指定場所の係員による人的な本人確認を行ったりする必要がある。また、近年では、指紋などの生体情報を用いて本人確認を行う機能を有するＩＣカードが開発されているが、このような生体認証機能を有するＩＣカードであっても、従来のＩＣカードと同様な手続きで二次発行や機能追加などの発行処理を行う必要があるという問題がある。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開２０１６－１６７２０１号公報

発明の概要

発明が解決しようとする課題

[0005] 上記の課題を解決するために、本発明は、利便性が高い発行処理の手続きを実現できるリモート発行システムおよびデータ生成サーバを提供すること

を目的とする。

課題を解決するための手段

[0006] 実施形態によれば、リモート発行システムは、携帯可能電子装置とデータ生成サーバとを有する。携帯可能電子装置は、生体センサとメモリと通信インターフェースと第１プロセッサとを有する。生体センサは、生体情報を取得する。メモリは、ユーザの生体情報を記憶する記憶領域を含む。通信インターフェースは、ユーザ端末と接続されるリーダライタと通信する。第１プロセッサは、生体センサにより取得する生体情報とメモリに保存する生体情報との照合による生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、認証データを前記リーダライタへ出力し、リーダライタから供給される認証データに対応する発行データに基づいて発行処理を実行する。データ生成サーバは、通信部と第２プロセッサとを有する。通信部は、ユーザ端末と通信する。第２プロセッサは、ユーザ端末から携帯可能電子装置が生成した認証データと契約ＩＤとを含む発行リクエストを受信した場合、契約ＩＤに対応する申請データと認証データとに基づいて携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データをユーザ端末へ送信する。

図面の簡単な説明

[0007] [図1]図１は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムの構成例を概略的に示す図である。

[図2]図２は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムによって発行手続きがなされるＩＣカードの構成例を示すブロック図である。

[図3]図３は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける携帯端末の構成例を示すブロック図である。

[図4]図４は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける契約管理サーバの構成例を示すブロック図である。

[図5]図５は、第１実施形態に係るリモート発行システムとしてのＩＣカード

発行システムにおけるデータ生成サーバの構成例を示すブロック図である。

[図6]図６は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける申請手続きの動作例を説明するためのシーケンスである。

[図7]図７は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンスである。

[図8]図８は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンスである。

[図9]図９は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムの構成例を概略的に示す図である。

[図10]図１０は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムによって発行手続きがなされるＩＣカードの構成例を示すブロック図である。

[図11]図１１は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける携帯端末の構成例を示すブロック図である。

[図12]図１２は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける契約管理サーバの構成例を示すブロック図である。

[図13]図１３は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおけるデータ生成サーバの構成例を示すブロック図である。

[図14]図１４は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける申請手続きの動作例を説明するためのシーケンスである。

[図15]図１５は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンス

である。

[図16]図１６は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンスである。

実施形態

[0008] 以下、第１および第２実施形態について、図面を参照しつつ説明する。

（第１実施形態）

まず、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システム１について説明する。

[0009] 図１は、第１実施形態に係るリモート発行システムとしてのＩＣカード発行システム１の構成例を模式的に示す図である。

図１に示す構成例において、ＩＣカード発行システム１は、ＩＣカード２、ユーザ端末３、データ管理システム４、および、発行制御システム５を有する。

[0010] ＩＣカード２は、生体認証を実行する機能を有する携帯可能電子装置の一例である。第１実施形態に係るＩＣカード２は、人物から取得する認証情報としての生体情報を取得するための生体センサ２０を備える。例えば、ＩＣカード２が具備する生体センサ２０は、生体情報の一例としての指紋を読み取る指紋センサである。生体センサとしての指紋センサ２０を備えるＩＣカード２は、指紋センサが読み取る人物の指紋とＩＣカード２内のメモリに予め登録されている登録者（ユーザ、カードホルダ）の指紋とを照合することにより本人確認としての指紋認証（生体認証）を実行する。

[0011] 第１実施形態において、ＩＣカード２は、生体情報としての指紋を用いて生体認証を行う機能を有する指紋センサカードであるものとして説明するものとする。ただし、第１実施形態に係る携帯可能電子装置としてのＩＣカード２は、生体情報として指紋による指紋（生体）認証を行うものに限定されるものではない。例えば、ＩＣカード２で例示される携帯可能電子装置は、指紋以外の生体情報によって生体認証を行うものであっても良い。

[0012] ユーザ端末３は、ユーザが所持する情報処理装置である。ユーザ端末３は、例えば、スマートフォン、タブレットＰＣ、パソコンなどである。ユーザ端末３は、ユーザ自身が操作するものであって、ＩＣカード２と通信するカードリーダライタおよびインターネットなどのネットワークを介して各サーバ４Ａ、５Ａと通信する通信部とを備えるものであれば良い。また、ユーザ端末３は、ＩＣカード２と通信するカードリーダライタを備えるものに代えて、外部機器としてのカードリーダライタに接続するためのインターフェースを備えるものであっても良い。

[0013] データ管理システム４は、遠隔によってユーザが保持するＩＣカードにおける発行処理（二次発行又は機能追加など）の申請を受け付けるシステムである。データ管理システム４は、契約管理サーバ４Ａとデータストレージ４Ｂとを有する。契約管理サーバ４Ａは、サーバ装置で構成される。データストレージ４Ｂは、契約管理サーバ４Ａからアクセス可能な記憶装置を含む装置である。契約管理サーバ４Ａは、データストレージ４Ｂにアクセスする機能、インターネットを介してユーザ端末３と通信する機能および発行制御システム５のデータ生成サーバ５Ａと通信する機能を有する。

[0014] 契約管理サーバ４Ａは、ユーザが所持するユーザ端末３と通信し、ユーザ端末３からの当該ユーザが保持するＩＣカードに対する発行処理（契約）に関する申請データを取得する。ここで、ＩＣカードに対する発行処理とは、二次発行又は機能追加を含むものとする。ＩＣカードの二次発行とは、発行業者からユーザ（カードホルダ）に渡したＩＣカードに対して個人データなどを書き込む処理（パーソナライズ）を含む処理である。また、機能追加は、ＩＣカードに対してアプリケーションなどを追加する処理である。例えば、機能追加としては、ジャバカード（Ｊａｖａ（登録商標）　Ｃａｒｄ）としてのＩＣカードにアプレットを追加する処理などが含まれる。

[0015] 契約管理サーバ４Ａは、ユーザ端末３から申請データを取得した後、ユーザ端末３からの申請データに基づく申請内容の契約が可能であれば、契約ＩＤを発行する。契約管理サーバ４Ａは、契約ＩＤを発行した場合、発行した

ユーザ端末３を通知し、契約ＩＤに対応づけた申請データ等をデータストレージ４Ｂに記憶する。また、契約管理サーバ４Ａは、発行制御システム５におけるデータ生成サーバ５Ａからの契約ＩＤに基づく申請データの問い合わせに応じて、データストレージ４Ｂに保存している契約ＩＤに対応する申請データを提供する。

[0016] 発行制御システム５は、遠隔によるＩＣカードに対して発行処理（二次発行又は機能追加）を実行させるためのシステムである。発行制御システム５は、データ生成サーバ５ＡとＨＳＭ（ハードウエアセキュリティモジュール：Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）５Ｂとを有する。データ生成サーバ５Ａは、サーバ装置で構成される。ＨＳＭ５Ｂは、セキュアに鍵情報に保存し、鍵情報を用いた暗号処理を行うデバイスである。データ生成サーバ５Ａは、ＨＳＭ５Ｂにアクセスする機能、インターネットを介してユーザ端末３と通信する機能およびデータ管理システム４の契約管理サーバ４Ａと通信する機能を有する。

[0017] データ生成サーバ５Ａは、ＨＳＭ５Ｂに保存する鍵および暗号処理機能を用いてユーザ端末３を介したＩＣカード２とのセキュアな通信を行う。データ生成サーバ５Ａは、ユーザ端末３からＩＣカード２が鍵情報を用いて生成するカード認証データと契約ＩＤとを含む発行リクエストを取得する。

[0018] データ生成サーバ５Ａは、ユーザ端末３からの発行リクエストに応じてデータ管理システム４の契約管理サーバ４Ａが管理する申請データを取得する。データ生成サーバ５Ａは、発行リクエストに応じて取得した申請データに基づいてユーザが所持するＩＣカードに対する発行処理を行うための発行データをＨＳＭ５Ｂが保存する鍵情報を用いて生成し、生成した発行データをユーザ端末３へ供給する。

[0019] 次に、第１実施形態に係る携帯可能電子装置としてのＩＣカード２における制御系の構成について説明する。

図２は、第１実施形態に係る携帯可能電子装置としてのＩＣカード２の構成例を示すブロック図である。

ＩＣカード２は、外部装置から供給される電力により活性化する（動作可能な状態になる）携帯可能電子装置の一例である。ＩＣカード２は、スマートカードとも称される。図２に示すように、ＩＣカード２は、本体Ｃを有する。本体Ｃは、プラスチックなどによりカード状に形成される。ＩＣカード２の本体Ｃ内には、制御モジュールＭが埋設される。制御モジュールＭは、１つ又は複数のＩＣチップに通信インターフェースが接続された状態で一体的に形成される。

[0020] 図２に示す構成例において、制御モジュールＭは、プロセッサ２１、ＲＯＭ２２、ＲＡＭ２３、データメモリ２４および通信インターフェース２５を有する。また、ＩＣカード２の本体Ｃ内において、制御モジュールＭには、表示器２６および生体センサとしての指紋センサ２７が接続される。

[0021] プロセッサ２１は、種々の処理を実行する回路を含む。プロセッサ２１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ２１は、ＩＣカード２全体の制御を司る。プロセッサ２１は、ＲＯＭ２２あるいはデータメモリ２４に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ２１が実行する各種の機能のうちの一部又は全部は、ハードウエア回路により実現されるようにしても良い。

[0022] ＲＯＭ２２は、プログラムメモリとして機能する不揮発性のメモリである。ＲＯＭ２２は、予め制御用のプログラムおよび制御データなどが記憶される。ＲＯＭ２２は、製造段階で制御プログラムや制御データなどが記憶された状態でＩＣカード２内に組み込まれるものである。ＲＯＭ２２に記憶される制御プログラムや制御データは、予め当該ＩＣカード２の仕様に応じて組み込まれる。例えば、ＲＯＭ２２には、外部装置（カードリーダライタ）から受信するコマンドに応じた処理をプロセッサ２１が実行するためのプログラムが記憶される。

[0023] ＲＡＭ２３は、ワーキングメモリとして機能する揮発性のメモリである。また、ＲＡＭ２３は、プロセッサ２１が処理中のデータなどを一時保管する

バッファとしても機能する。例えば、ＲＡＭ２３は、通信インターフェース２５を介して外部装置との間で送受信するデータを一時保管する通信バッファとして機能する。

[0024] データメモリ２４は、データの書き込みおよび書換えが可能な不揮発性のメモリである。データメモリ２４は、例えば、ＥＥＰＲＯＭ（登録商標）（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などで構成する。データメモリ２４には、当該ＩＣカード２の運用用途に応じたプログラムや種々のデータが書き込まれる。データメモリ２４には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルに制御プログラムや種々のデータが書き込まれる。また、データメモリ２４は、一部又は全部の領域が耐タンパー性を有し、セキュアにデータが格納できる。

[0025] データメモリ２４は、鍵情報を記憶する第１の記録領域２４ａおよび生体情報を格納する第２の記憶領域２４ｂを有する。第１の記憶領域２４ａは、セキュアにデータを記憶できる耐タンパー性を有するメモリである。第１の記憶領域２４ａには、当該ＩＣカード２を使用可能な状態とする処理（一次発行）において鍵情報が書き込まれる。本ＩＣカード発行システム１においては、一次発行済みのＩＣカード２における第１の記憶領域２４ａに書き込んだ鍵情報に対応する鍵情報が発行制御システム５におけるＨＳＭ５Ｂに保存されるものとする。

[0026] また、第２の記憶領域２４ｂは、当該ＩＣカード２の所有者であるユーザの生体情報を記憶する。例えば、ＩＣカード２は、生体情報として指紋を用いた生体情報を行う指紋センサカードであることを想定する。ＩＣカード２が指紋センサカードである場合、ＩＣカード２の第２の記憶領域２４ｂには所有者であるユーザの生体情報としての指紋情報が書き込まれる。なお、以下に説明する第１実施形態では、ＩＣカード２は、二次発行又は機能追加を実行する前に、第２の記憶領域にユーザの生体情報としての指紋情報が書き込まれた状態でユーザが所持しているものであることを前提とする。

[0027] 通信インターフェース２５は、通信制御部とインターフェース部とを有し、通信部を構成する。通信インターフェース２５は、ユーザ端末３が備えるカードリーダライタ（ＲＷ）又はユーザ端末３とインターフェースを介して接続されるカードリーダライタと通信接続するためのインターフェースである。通信インターフェース２５は、カードＲＷのインターフェースに対応した通信方式による通信機能を実現する。また、通信インターフェース２５は、複数の通信方式（例えば、接触通信と非接触通信）をサポートするものとして構成しても良い。

[0028] 当該ＩＣカード２が非接触型のＩＣカードとして実現される場合、通信インターフェース２５は、ユーザ端末３が備えるカードＲＷ又はユーザ端末３とインターフェースを介して接続されるカードＲＷと非接触（無線）で通信する通信部を構成する。この場合、通信インターフェース２５は、電波の送受信を行うアンテナを備え、アンテナから送信する電波を生成するための変調回路およびアンテナが受信した電波から信号を生成するための復調回路などにより構成される。

[0029] また、当該ＩＣカード２が接触型のＩＣカードとして実現される場合、通信インターフェース２５は、ユーザ端末３が備えるカードＲＷ又はユーザ端末３とインターフェースを介して接続されるカードＲＷと接触して通信する通信部を構成する。この場合、通信インターフェース２５は、カードＲＷに設けられたコンタクト部と物理的かつ電気的に接触するコンタクト部を備え、コンタクト部を介した信号の送受信を制御する通信制御回路などにより構成される。

[0030] 生体センサ２０は、認証情報を取得する認証情報取得部の一例である。生体センサ２０は、認証処理に用いる認証情報として人物の生体情報を取得するセンサである。第１実施形態において、生体センサ２０は、利用者の指紋情報（指紋画像）を読み取る指紋センサであるものとする。生体センサ２０としての指紋センサは、指紋を読み取るセンサがカード本体Ｃの表面に露出するように設けられ、露出したセンサ部分に翳された人物の指の指紋を読み

取る。生体センサ２０が読み取る指紋情報が、データメモリ２４の第２の記憶領域２４ｂに記憶されている指紋情報と照合されるにで指紋認証が実行される。

[0031] なお、生体センサ２０は、指紋センサに限定されるものではなく、指紋以外の生体情報（例えば、掌紋、静脈、虹彩等）を取得するセンサであっても良い。指紋以外の生体情報を取得するセンサを備える場合、ＩＣカード２は、センサが取得する生体情報に対応した生体認証を行う機能（例えば、掌紋照合、静脈照合、虹彩照合等を実行するＩＣチップ）を備えるようにすれば良い。

[0032] 次に、第１実施形態に係るＩＣカード発行システム１におけるユーザ端末３の構成について説明する。

図３は、第１実施形態に係るＩＣカード発行システム１におけるユーザ端末３の構成例を示すブロック図である。

ユーザ端末３は、オペレーティングシステム（ＯＳ）上で種々のアプリケーションプログラムが実行される電子装置である。ユーザ端末３は、ＩＣカード２を所持するカードホルダとしてのユーザが使用する電子装置であれば良い。例えば、ユーザ端末３は、スマートフォン、タブレット端末、携帯電話などのカードＲＷを備える携帯端末又はカードＲＷを接続するインターフェースを備える携帯端末である。また、ユーザ端末３は、カードＲＷを備えるパーソナルコンピュータ（ＰＣ）又はカードＲＷを接続するインターフェースを備えるＰＣであっても良い。

[0033] 図３に示す構成例において、ユーザ端末３は、プロセッサ３１、ＲＯＭ３２、ＲＡＭ３３、データメモリ３４、ネットワーク（ＮＷ）通信部３５、カードリーダライタ（ＲＷ）３６、表示部３７、および、入力部３８などを有する。

[0034] プロセッサ３１は、プログラムを実行することにより各種の処理を実行する。プロセッサ３１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ３１は、システムバスを介してユー

ザ端末３内の各部と接続され、各部との間でデータを送受信する。プロセッサ３１は、ＲＯＭ３２およびＲＡＭ３３と協働してユーザ端末３における制御およびデータ処理などの動作を実行する。例えば、プロセッサ３１は、ＲＯＭ３２あるいはデータメモリ３４に記憶されているアプリケーションプログラムを実行することにより種々の処理機能を実現する。ただし、後述するプロセッサ３１が実行する各種の機能のうちの一部又は全部は、ハードウエア回路により実現されるようにしても良い。

[0035] ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）３２は、ユーザ端末３の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。例えば、ＲＯＭ３２は、オペレーティングシステム（ＯＳ）などの基本動作を司るプログラムを記憶する。また、ＲＯＭ３２は、ユーザ端末３が具備する機能を実現するためのアプリケーションプログラムなどを記憶しても良い。ＲＯＭ３２は、書き換え可能な不揮発性のメモリで構成しても良い。例えば、書き換え可能なＲＯＭ３２としては、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）又はフラッシュＲＯＭなどで実現される。

[0036] ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）３３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ３３は、プロセッサ３１がプログラムを実行する場合にワーキングメモリとして機能する。

[0037] データメモリ３４は、各種のデータを記憶する記憶部である。データメモリ３４は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ３４は、フラッシュＲＯＭ、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）などの半導体素子メモリ、あるいは、ＨＤＤ（Ｈａｒｄ Ｄｉｓｃ Ｄｒｉｖｅ）などの記憶装置が用いられる。データメモリ３４は、アプリケーションプログラム、動作設定値、個人情報などを記憶する。また、データメモリ３４は、ＯＳプログラムを記憶するようにしても良い。

[0038] ＮＷ通信部３５は、外部装置と通信するための通信インターフェースである。ＮＷ通信部３５は、無線で通信を行うものであって良いし、有線で通信

を行うものであっても良い。ＩＣカード発行システム１において、ＮＷ通信部３５は、インターフェースを介して、契約管理サーバ４Ａおよびデータ生成サーバ５Ａと通信するものであれば良い。

[0039] カードリーダライタ３６は、ＩＣカード２と通信する機能を有する。カードリーダライタ３６は、ＩＣカード２に対して、電源供給、クロック供給、リセット制御、データの送受信を行う。カードリーダライタ３６は、ＩＣカード２を活性化（起動）させた後、プロセッサ３１による制御に基づいて種々のコマンドを送信したり送信したコマンドに対する応答を受信したりする。なお、ユーザ端末３は、外部機器としてのカードリーダライタに接続するためのインターフェースを備える構成としても良い。

[0040] カードリーダライタ３６は、ＩＣカード２が備える通信方式に対応する構成を備える。例えば、ＩＣカード２が非接触型のＩＣカードとして実現される場合、カードリーダライタ３６は、非接触型のＩＣカードの通信方式に準拠する通信プロトコルで、非接触（無線）でＩＣカード２と通信する。また、ＩＣカード２が接触型のＩＣカードとして実現される場合、カードリーダライタ３６は、ＩＣカード２のコンタクト部（インターフェース）と物理的かつ電気的に接触するコンタクト部を有し、コンタクト部を介してデータの送受信を行う。

[0041] 表示部３７は、液晶パネル等の表示デバイスである。入力部３８は、ユーザ端末３に対して操作指示を入力する操作デバイスである。入力部３８は、例えば、タッチパネルを含む。表示部３７と入力部３８とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部３８は、ボタンスイッチで構成する操作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。

[0042] 次に、第１実施形態に係るＩＣカード発行システム１における契約管理サーバ４Ａの構成について説明する。

図４は、第１実施形態に係るＩＣカード発行システム１における契約管理

サーバ４Ａの構成例を示すブロック図である。

図４に示すように、契約管理サーバ４Ａは、プロセッサ４１、ＲＯＭ４２、ＲＡＭ４３、データメモリ４４、インターフェース４５、ネットワーク（ＮＷ）通信部４６、および、通信部４７を有する。

[0043] プロセッサ４１は、プログラムを実行することにより各種の処理を実行する。プロセッサ４１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ４１は、システムバスを介してサーバ４Ａ内の各部と接続され、各部との間でデータを送受信する。プロセッサ４１は、ＲＯＭ４２およびＲＡＭ４３と協働して契約管理サーバ４Ａにおける制御およびデータ処理などの動作を実行する。

[0044] ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）４２は、契約管理サーバ４Ａの基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）４３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ４３は、プロセッサ４１がプログラムを実行する場合にワーキングメモリとして機能する。

データメモリ４４は、各種のデータを記憶する記憶部である。データメモリ４４は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ４４は、ＯＳプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0045] インターフェース４５は、データストレージ４Ｂにアクセスするためのインターフェースである。データストレージ４Ｂが外部デバイスとしての記憶装置である場合、インターフェース４５は、データストレージ４Ｂとしての記憶装置が備えるインターフェース規格に対応したものであれば良い。また、データストレージ４Ｂがデータサーバ等である場合、インターフェースは、データストレージ４Ｂとしてのサーバと通信するための通信インターフェースで構成すれば良い。

[0046] ネットワーク（ＮＷ）通信部４６は、外部装置と通信するための通信イン

ターフェースである。ＮＷ通信部４６は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第１実施形態に係るＩＣカード発行システム１において、ＮＷ通信部４６は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末３と通信するものであれば良い。

[0047] 通信部４７は、データ生成サーバと通信するための通信インターフェースである。通信部４７は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第１実施形態に係るＩＣカード発行システム１において、通信部４７は、データ生成サーバ５Ａとの通信がセキュアに行えるものであれば良い。

なお、ＮＷ通信部４６および通信部４７は、１つの通信インターフェースで実現する構成しても良い。さらに、インターフェース４５についても、ＮＷ通信部４６又は通信部４７と共通化した通信インターフェースとする構成としても良い。

[0048] 次に、第１実施形態に係るＩＣカード発行システム１におけるデータ生成サーバ５Ａの構成について説明する。

図５は、第１実施形態に係るＩＣカード発行システム１におけるデータ生成サーバ５Ａの構成例を示すブロック図である。

図５に示すように、データ生成サーバ５Ａは、プロセッサ５１、ＲＯＭ５２、ＲＡＭ５３、データメモリ５４、インターフェース５５、ネットワーク（ＮＷ）通信部５６、および、通信部５７を有する。

[0049] プロセッサ５１は、プログラムを実行することにより各種の処理を実行する。プロセッサ５１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ５１は、システムバスを介してサーバ５Ａ内の各部と接続され、各部との間でデータを送受信する。プロセッサ５１は、ＲＯＭ５２およびＲＡＭ５３と協働してデータ生成サーバ５Ａにおける制御およびデータ処理などの動作を実行する。

[0050] ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）５２は、データ生成サーバ

５Ａの基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）５３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ５３は、プロセッサ５１がプログラムを実行する場合にワーキングメモリとして機能する。

データメモリ５４は、各種のデータを記憶する記憶部である。データメモリ５４は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ５４は、ＯＳプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0051] インターフェース５５は、ＨＳＭ５Ｂにアクセスするためのインターフェースである。インターフェース５５は、ＨＳＭ５Ｂが備えるインターフェース規格に対応したものであれば良い。

ネットワーク（ＮＷ）通信部５６は、外部装置と通信するための通信インターフェースである。ＮＷ通信部５６は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第１実施形態に係るＩＣカード発行システム１において、ＮＷ通信部５６は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末３と通信するものであれば良い。

[0052] 通信部５７は、契約管理サーバ４Ａと通信するための通信インターフェースである。通信部５７は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第１実施形態に係るＩＣカード発行システム１において、通信部５７は、契約管理サーバ４Ａとの通信がセキュアに行えるものであれば良い。

なお、ＮＷ通信部５６および通信部５７は、１つの通信インターフェースで実現する構成しても良い。

[0053] 次に、第１実施形態に係るＩＣカード発行システム１におけるＩＣカード２に対する発行処理の申請手続きおよび発行手続きについて説明する。

以下に説明する動作の前提条件として、ＩＣカード２は、一次発行（カー

ド製造と初期化）の処理がなされた後にユーザ（カードホルダ）に渡されるものとする。また、ユーザに渡されるＩＣカード２には、一次発行においてカード認証データの生成に関する鍵（鍵情報）が書き込まれているものとする。ＩＣカード２に書き込まれた鍵情報は、発行制御システム５におけるＨＳＭ５Ｂに保存されている。さらに、ユーザ（カードホルダ）が所持するＩＣカード２には、当該ユーザの本人認証が行われた上で当該ユーザ（本人）の指紋情報が書き込まれているものとする。

[0054] まず、第１実施形態に係るＩＣカード発行システム１におけるＩＣカード２に対する発行処理の申請手続きについて説明する。

図６は、ＩＣカード発行システム１におけるＩＣカード２に対する発行処理の申請手続きの動作例を説明するためのシーケンスである。

カードホルダは、ユーザ端末３のプロセッサ３１は、カードホルダとしてのユーザの操作に応じて入力部３８による申請データの入力を受け付ける（ＳＴ２１）。申請データとしては、例えば、発行処理（二次発行又は機能追加）に必要な情報、カードホルダであるユーザ自身の個人情報、および、カードホルダ（ユーザ）が所持するＩＣカード２に関する情報などが含まれることが想定される。

[0055] また、ユーザ端末３は、申請用のプログラムにより申請データが入力されるようにしても良いし、インターネット上に提供される申請データの入力用のＷｅｂサイトで申請データが入力されるようにしても良い。前者の場合、ユーザ端末３は、データメモリ３４に申請用のプログラムをインストールしておく。ユーザ端末３のプロセッサ３１は、ユーザの操作に応じて申請用のプログラムを起動し、申請用のプログラムで提示される申請データの入力フォーマットに従って申請データを入力する。また、後者の場合、ユーザ端末３のプロセッサ３１は、ＮＷ通信部３５によりインターネット上で提供される申請データの入力用のサイトにアクセスし、入力用のサイトで提示される申請データの入力フォーマットに沿って申請データを入力する。

[0056] また、ユーザ端末３は、カードホルダ（ユーザ）が所持するＩＣカード２

に関する情報を当該ＩＣカード２から読み取るようにしても良い。当該ＩＣカード２に関する情報（カードデータ）は、例えば、当該ＩＣカード２を識別するための固有な識別情報（ＩＤ）などを含む。また、カードホルダであるユーザ自身の個人情報がＩＣカード２に保存されている場合、ユーザ端末３は、ユーザの個人情報をＩＣカード２から読み取るようにしても良い。図６に示す動作例において、ＩＣカード２は、ユーザ端末３のカードリーダライタ３６からの要求に応じて、生体（指紋）認証で本人確認が成功した後にカードデータを出力するものとする。

[0057] すなわち、ユーザ端末３のプロセッサ３１は、カードＲＷ３６により生体認証としての指紋認証の要求とカードデータの要求とをＩＣカード２へ送信する（ＳＴ２２）。ＩＣカード２のプロセッサ２１は、ユーザ端末３からの要求に応じてデータメモリ２４に記憶されている指紋データを用いて指紋認証を実行する（ＳＴ１１）。ＩＣカード２のプロセッサ２１は、指紋認証による本人確認が成功した後に当該ＩＣカード２の情報をユーザ端末３へ出力する（ＳＴ１２）。

[0058] 申請データの入力が完了すると、ユーザ端末３のプロセッサ３１は、入力された申請データによる発行処理（契約）に関する審査を要求する審査リクエストを作成する（ＳＴ２３）。審査リクエストは、申請データとして入力された申請内容によって、カードホルダが所持するＩＣカード２に対する発行処理（二次発行又は機能追加）を実行すること（契約）が可能であるか否かの審査を要求するものである。

[0059] 審査リクエストを作成すると、ユーザ端末３のプロセッサ３１は、データ管理システム４の契約管理サーバ４Ａへ審査リクエストを送信する（ＳＴ２４）。プロセッサ３１は、ＮＷ通信部３５によりインターネットを介して契約管理サーバ４Ａにアクセスし、審査リクエストを契約管理サーバ４Ａへ送信する。

[0060] 契約管理サーバ４Ａは、ＮＷ通信部４６によりユーザ端末３からの審査リクエストを受け付ける（ＳＴ３１）。ユーザ端末３からの審査リクエストを

受信すると、契約管理サーバ４Ａのプロセッサ４１は、受信した審査リクエストに応じて申請された発行処理を許可するか否かを審査する。例えば、契約管理サーバ４Ａは、申請データが示す申請内容に問題がないか、および、申請者であるカードホルダに関して発行処理を行うための契約上の問題がないかを審査する。審査の内容および手続きは、運用形態に準じたものであれば特定の形態に限定されるものではない。審査リクエストに応じた審査結果が契約管理サーバ４Ａに入力されるものであれば良い。

[0061] 審査リクエストに対する審査結果が契約不可（発行処理が不可）であった場合、契約管理サーバ４Ａのプロセッサ４１は、審査結果として契約不可となった旨を審査リクエストの送信元であるユーザ端末３へ通知する（ＳＴ３４）。また、プロセッサ４１は、申請データでカードホルダが指定した連絡先に審査結果を通知するようにしても良い。

[0062] ユーザ端末３のプロセッサ３１は、契約管理サーバ４Ａから審査リクエストに対する審査結果が契約不可である旨の通知を受けると、審査結果が契約不可であった旨を表示部３７に表示することによりカードホルダに報知する（ＳＴ２５）。

[0063] 審査リクエストに対する審査結果が契約可（発行処理が可）であった場合、契約管理サーバ４Ａのプロセッサ４１は、契約ＩＤを発行する（ＳＴ３２）。契約ＩＤを発行すると、プロセッサ４１は、審査結果が契約可となった審査リクエストに含まれる申請データを発行した契約ＩＤに対応づけてデータストレージ４Ｂに登録する（ＳＴ３３）。データストレージ４Ｂは、契約管理サーバ４Ａからの申請データと契約ＩＤとを契約情報として保存する（ＳＴ４１）。

[0064] 申請データと契約ＩＤとをデータストレージ４Ｂに登録すると、契約管理サーバ４Ａのプロセッサ４１は、審査結果および契約ＩＤを審査リクエストの送信元であるユーザ端末３へ通知する（ＳＴ３４）。

[0065] ユーザ端末３のプロセッサ３１は、契約管理サーバ４Ａから審査リクエストに対する審査結果が契約可である旨の通知を受けると、審査結果として契

約可であった旨の案内とともに、契約ＩＤを表示部３７に表示する（ＳＴ２５）。また、審査結果が可であった場合、ユーザ端末３のプロセッサ３１は、表示部３７に発行処理の手続きに関する案内などを表示するようにしても良い。

[0066] 以上のような申請手続きによって、契約管理サーバは、ユーザ端末からの審査リクエストが契約可となった場合、当該審査リクエストを行ったカードホルダからの申請データと契約ＩＤと対応づけてデータストレージに保存することができる。この結果、カードホルダが所持するＩＣカード２は、後述するような動作によるリモートでの発行処理が可能な状態となる。これにより、カードホルダは、発行処理が可能な状態となった後、つまり、契約ＩＤの通知を受けた後、ユーザ端末３を用いてＩＣカード２に対してリモートで発行処理を行うための後述するような発行手続きを実行する。

[0067] 次に、第１実施形態に係るＩＣカード発行システム１におけるＩＣカード２に対する発行処理を行うための発行手続きについて説明する。

図７および図８は、ＩＣカード発行システム１におけるＩＣカード２に対する発行処理を行うための発行手続きの動作例を説明するためのシーケンスである。

カードホルダとしてのユーザは、ユーザ端末３においてＩＣカード２に対する発行処理用のアプリケーションプログラム（以下、発行アプリと称する）を起動させる。発行アプリは、予めデータメモリ２４に記憶しておくようにしても良いし、契約管理サーバ４Ａ又はデータ生成サーバ５Ａからダウンロードするようにしても良い。

[0068] ユーザ端末３のプロセッサ３１は、カードホルダが入力部３８に入力する発行アプリの起動指示に応じて発行アプリを起動させる（ＳＴ１２０）。発行アプリが起動すると、プロセッサ３１は、カードホルダに対して契約ＩＤの入力を要求する（ＳＴ１２１）。カードホルダは、申請データに対する審査結果と共に取得した契約ＩＤを入力部３８により入力する。プロセッサ３１は、入力部３８に契約ＩＤが入力されると、カードＲＷ３６によりＩＣカ

ード２にアクセスし、本人確認のための生体認証としての指紋認証をＩＣカード２に要求する（ＳＴ１２２）。

[0069] ＩＣカード２は、カードＲＷ３６から供給される電力により起動する。ＩＣカード２が起動すると、プロセッサ２１は、カードＲＷ３６から供給される指紋認証の要求に応じて指紋認証処理を実行する（ＳＴ１１１）。プロセッサ２１は、指紋センサ２０によりユーザの指紋を取得する。プロセッサ２１は、指紋センサ２０が取得した指紋情報とデータメモリ２４に記憶している指紋データとを比較することにより指紋認証を行う。

[0070] 指紋センサ２０が取得した指紋情報とデータメモリ２４に記憶している指紋データとが同一人物の指紋であると判定された場合、プロセッサ２１は、指紋認証が成功したものとする。指紋センサ２０が取得した指紋情報とデータメモリ２４に記憶している指紋データとが同一人物の指紋であると判定できなかった場合、プロセッサ２１は、指紋認証が失敗したものとする。

[0071] ＩＣカード２における指紋認証が失敗した場合、プロセッサ２１は、指紋認証が失敗したことをカードＲＷ３６へ通知する。カードＲＷ３６によりＩＣカード２から指紋認証が失敗した旨の通知を受けた場合、ユーザ端末３のプロセッサ３１は、ＩＣカード２に対する発行処理を実行するための発行手続きを中止する。この場合、プロセッサ３１は、表示部３７に本人確認が失敗したためにＩＣカード２に対する発行処理で不可となった旨を表示することによりユーザに発行手続きの中止を報知する。

[0072] ＩＣカード２における指紋認証が成功した場合、プロセッサ２１は、指紋認証が成功したことをカードＲＷ３６へ通知する。カードＲＷ３６によりＩＣカード２から指紋認証が成功した旨の通知を受けた場合、ユーザ端末３のプロセッサ３１は、カードＲＷ３６を介してＩＣカード２に発行処理を実行するためのカード認証データを要求する。これに対して、ＩＣカード２のプロセッサ２１は、カード認証データを生成し、生成したカード認証データをカードＲＷ３６へ供給する。

[0073] すなわち、ＩＣカード２のプロセッサ２１は、指紋認証が成功した場合、

カード認証データ（認証データ）を生成する（ＳＴ１１２）。カード認証データは、当該ＩＣカード２における生体認証が成功した場合に生成される認証データであり、当該ＩＣカード２に機能追加（例えば、アプレットの追加）あるいは二次発行などの発行処理を実施するための情報を含む。

[0074] カード認証データは、セキュアメモリであるデータメモリ２４の記憶領域２４ａに記憶されている鍵情報を用いて生成される。また、カード認証データには、発行処理を実施するための情報として、例えば、ＣＰＬＣ（当該ＩＣカードのプロダクトサイクルを示す情報）、ＩＮＩＴＩＡＬＩＺＥ　ＵＰＤＡＴＥコマンドおよびレスポンスデータなどが含まれる。

[0075] 指紋認証が成功した後にカード認証データを生成すると、ＩＣカード２のプロセッサ２１は、生成したカード認証データをユーザ端末３のカードＲＷ３６へ出力する（ＳＴ１１３）。カード認証データを出力した後、ＩＣカード２のプロセッサ２１は、当該カード認証データに対応してデータ生成サーバ５Ａが生成する発行データに基づく発行処理が実行可能な状態とする。

[0076] ユーザ端末３のプロセッサ３１は、カードＲＷ３６により指紋認証が成功したＩＣカード２からカード認証データを取得すると、ＩＣカード２に対する発行処理を要求する発行リクエストを生成し、生成した発行リクエストをデータ生成サーバ５Ａへ送信する（ＳＴ１２４）。

[0077] 例えば、プロセッサ３１は、カード認証データおよび契約ＩＤを含む発行リクエストを生成する。発行リクエストを生成すると、プロセッサ３１は、ＮＷ通信部３５によりインターネットを介して発行制御システム５におけるデータ生成サーバ５Ａにアクセスする。データ生成サーバ５Ａにアクセスすると、プロセッサ３１は、カード認証データおよび契約ＩＤを含む発行リクエストをデータ生成サーバ５Ａへ送信する。

[0078] データ生成サーバ５Ａは、ＮＷ通信部５６によりユーザ端末３からの発行リクエストを受信する。発行リクエストを受信した場合、データ生成サーバ５Ａのプロセッサ５１は、発行リクエストに含まれる契約ＩＤを抽出する。発行リクエストに含まれる契約ＩＤを抽出すると、プロセッサ５１は、通信

部５７を介して契約管理サーバ４Ａにアクセスする。契約管理サーバ４Ａにアクセスすると、プロセッサ５１は、発行リクエストに含まれる契約ＩＤに対応する申請データの要求（リクエスト）を契約管理サーバ４Ａへ送信する（ＳＴ１３１）。

[0079] 契約管理サーバ４Ａは、通信部４７を介してデータ生成サーバ５Ａと通信する。契約管理サーバ４Ａのプロセッサ４１は、データ生成サーバ５Ａから契約ＩＤに対応する申請データを要求するリクエストを受信した場合、データストレージ４Ｂにおいて当該契約ＩＤに対応する申請データを検索する（ＳＴ１４１）。データ生成サーバ５Ａから要求された契約ＩＤに対応する申請データを検出すると、プロセッサ４１は、通信部４７を介して当該契約ＩＤに対応する申請データをデータ生成サーバ５Ａへ送信する（ＳＴ１４２）。

[0080] 発行リクエストに含まれる契約ＩＤに対応する申請データを契約管理サーバ４Ａから受信すると、データ生成サーバ５Ａのプロセッサ５１は、ＩＣカード２において申請データに基づく発行処理を実行するための発行データを生成する（ＳＴ１３２）。発行データは、申請データに基づく一連の発行処理においてＩＣカード２に実行させるべきコマンドと一連の発行処理においてＩＣカード２に書き込むべきデータとを含む。

[0081] 例えば、発行処理としてＩＣカード２にアプレットを追加する場合、発行データには、ＩＣカード２に実行させるべきコマンドとしてインストール（ＩＮＳＴＡＬＬ）コマンドが含まれる。また、あるクレジットカードの規格でアプレットを追加する場合、発行データには、ＩＣカード２に実行させるべきコマンドとして外部認証（ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ）コマンド、および、ストアデータ（ＳＴＯＲＥ　ＤＡＴＡ）コマンドが含まれる。

[0082] また、プロセッサ５１は、発行データをセキュアにＩＣカード２に供給するためにＨＳＭ５Ｂが保管する鍵情報を用いて発行データを処理する（ＳＴ１３３）。ここで、ＨＳＭ５Ｂには、ＩＣカード２内に保持する鍵情報に対

応する鍵情報が保存されている。これにより、ＨＳＭ５Ｂを用いた暗号化によって安全に発行データをＩＣカード２へ供給できる。例えば、プロセッサ５１は、ＨＳＭ５Ｂにおいて当該ＩＣカード２内の保存される鍵情報と共有する鍵情報を用いて発行データに含まれるデータを暗号化する。

[0083] 発行データをＨＳＭ５Ｂが保存する鍵情報で暗号化処理した後、プロセッサ５１は、発行リクエストの送信元であるユーザ端末３へＨＳＭ５Ｂで暗号化処理した発行データを送信する（ＳＴ１３４）。

[0084] ユーザ端末３は、データ生成サーバ５Ａへ発行リクエストを送信した後、発行リクエストに対する応答としての発行データの受信待ちとなる。この状態において、ユーザ端末３は、ＮＷ通信部３５４によりデータ生成サーバ５Ａから送信される発行データを受信する（ＳＴ１２５）。発行データを受信した場合、ユーザ端末３のプロセッサ３１は、カードＲＷ３６によりＩＣカード２に対して発行データを出力する（ＳＴ１２６）。

[0085] ＩＣカード２のプロセッサ２１は、生体認証が成功した後に生成したカード認証データに対応する発行データをユーザ端末３のカードＲＷ３６から取得する。発行データを取得すると、プロセッサ２１は、取得した発行データに従って発行処理を実行する（ＳＴ１１３）。

[0086] 例えば、プロセッサ２１は、発行データに含まれるコマンドを実行することにより発行処理として書き込むべきデータをデータメモリ２４に書き込む。また、プロセッサ２１は、発行処理において供給される発行データに含まれる暗号化データをデータメモリ２４におけるセキュアメモリである第１の記憶領域２４ａに記憶している鍵情報を用いて復号化する。

[0087] ＩＣカード２のプロセッサ２１は、供給された発行データに基づく発行処理が完了すると、発行処理の完了をユーザ端末３のカードＲＷ３６へ通知する（ＳＴ１１４）。

ユーザ端末３は、カードＲＷ３６によりＩＣカード２へ発行データを出力した後にＩＣカード２から発行処理が完了した旨の通知を受信する。ユーザ端末３のプロセッサ３１は、カードＲＷ３６によりＩＣカード２から発行処

理の完了通知を受けると、ＩＣカード２における発行処理（機能追加あるいは二次発行）が完了した旨の案内を表示部３７に表示する（ＳＴ１２７）。

[0088] また、発行データに基づくＩＣカード２における発行処理が完了した旨の通知を受けると、プロセッサ３１は、ＮＷ通信部３５により発行データの送信元であるデータ生成サーバ５Ａへ発行処理の完了を通知する（ＳＴ１２８）。

データ生成サーバ５Ａのプロセッサ５１は、ユーザ端末３からのＩＣカード２における発行処理の完了通知をＮＷ通信部５６により受信すると、通信部５７によりＩＣカード２における発行処理の完了通知を契約管理サーバ４Ａへ転送（送信）する。

[0089] 契約管理サーバ４Ａは、通信部４７によりデータ生成サーバ５Ａを介してＩＣカード２における発行処理の完了通知を受信する。契約管理サーバ４Ａのプロセッサ４１は、データ生成サーバ５Ａを経由してＩＣカード２における発行処理の完了通知を受信すると、データストレージ４Ｂにおいて申請データに対応して発行処理の完了を記録する（ＳＴ１４３）。

[0090] 以上のような発行手続きによって、第１実施形態に係るＩＣカード発行システムは、生体センサとしての指紋センサを有するＩＣカード２において生体認証による本人認証が成功した後に、セキュアにリモートでＩＣカードに対して機能追加あるいは二次発行などの発行処理を行うことができる。

[0091] （第２実施形態）

以下、第２実施形態について、図面を参照しつつ説明する。

まず、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システム２０１について説明する。

[0092] 図９は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システム２０１の構成例を模式的に示す図である。

図９に示す構成例において、ＩＣカード発行システム２０１は、ＩＣカード２０２、ユーザ端末２０３、データ管理システム２０４、および、発行制御システム２０５を有する。

[0093] ＩＣカード２０２は、生体認証を実行する機能を有する携帯可能電子装置の一例である。第２実施形態に係るＩＣカード２０２は、人物から取得する認証情報としての生体情報を取得するための生体センサ２２０を備える。例えば、ＩＣカード２０２が具備する生体センサ２２０は、生体情報の一例としての指紋を読み取る指紋センサである。生体センサとしての指紋センサ２２０を備えるＩＣカード２０２は、指紋センサが読み取る人物の指紋とＩＣカード２０２内のメモリに予め登録されている登録者（ユーザ、カードホルダ）の指紋とを照合することにより本人確認としての指紋認証（生体認証）を実行する。

[0094] また、本実施形態に係る携帯可能電子装置としてのＩＣカード２０２は、固有な個体機別情報としてＰＵＦ（Ｐｈｙｓｉｃａｌｌｙ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎ：物理複製困難関数）データを出力する機能を有する。ＰＵＦは、例えば、半導体チップのシリコン結晶パターンのばらつきなど、物体の物理的な特徴のばらつきからその物体に固有な情報（ＩＤ）を示すものである。ＰＵＦデータは、ＩＣチップなどのＩＣカード２０２に含まれる電子回路から得られるものとする。ＰＵＦは、電子回路を構成する個々のデバイスのばらつきによるものであるため、たとえ回路パターンが不正に複製されたとしても、ＰＵＦ自体は、複製困難である。ＰＵＦデータは、個々のＩＣカード２０２ごとに固有な情報となる。

[0095] 第２実施形態において、ＩＣカード２０２は、生体情報としての指紋を用いて生体認証を行う機能を有する指紋センサカードであるものとして説明するものとする。ただし、第２実施形態に係る携帯可能電子装置としてのＩＣカード２０２は、生体情報として指紋による指紋（生体）認証を行うものに限定されるものではない。例えば、ＩＣカード２０２で例示される携帯可能電子装置は、指紋以外の生体情報によって生体認証を行うものであっても良い。

[0096] ユーザ端末２０３は、ユーザが所持する情報処理装置である。ユーザ端末２０３は、例えば、スマートフォン、タブレットＰＣ、パソコンなどである

。ユーザ端末２０３は、ユーザ自身が操作するものであって、ＩＣカード２０２と通信するカードリーダライタおよびインターネットなどのネットワークを介して各サーバ４Ａ、５Ａと通信する通信部とを備えるものであれば良い。また、ユーザ端末２０３は、ＩＣカード２０２と通信するカードリーダライタを備えるものに代えて、外部機器としてのカードリーダライタに接続するためのインターフェースを備えるものであっても良い。

[0097] データ管理システム２０４は、遠隔によってユーザが保持するＩＣカードにおける発行処理（二次発行又は機能追加など）の申請を受け付けるシステムである。データ管理システム２０４は、契約管理サーバ２０４Ａとデータストレージ２０４Ｂとを有する。契約管理サーバ２０４Ａは、サーバ装置で構成される。データストレージ２０４Ｂは、契約管理サーバ２０４Ａからアクセス可能な記憶装置を含む装置である。契約管理サーバ２０４Ａは、データストレージ２０４Ｂにアクセスする機能、インターネットを介してユーザ端末２０３と通信する機能および発行制御システム２０５のデータ生成サーバ２０５Ａと通信する機能を有する。

[0098] 契約管理サーバ２０４Ａは、ユーザが所持するユーザ端末２０３と通信し、ユーザ端末２０３からの当該ユーザが保持するＩＣカードに対する発行処理（契約）に関する申請データを取得する。ここで、ＩＣカードに対する発行処理とは、二次発行又は機能追加を含むものとする。ＩＣカードの二次発行とは、発行業者からユーザ（カードホルダ）に渡したＩＣカードに対して個人データなどを書き込む処理（パーソナライズ）を含む処理である。また、機能追加は、ＩＣカードに対してアプリケーションなどを追加する処理である。例えば、機能追加としては、ジャバカード（Ｊａｖａ　Ｃａｒｄ）（登録商標）としてのＩＣカードにアプレットを追加する処理などが含まれる。

[0099] 契約管理サーバ２０４Ａは、ユーザ端末２０３から申請データを取得した後、ユーザ端末２０３からの申請データに基づく申請内容の契約が可能であれば、契約ＩＤを発行する。契約管理サーバ２０４Ａは、契約ＩＤを発行し

た場合、発行したユーザ端末２０３を通知し、契約ＩＤに対応づけた申請データとカードホルダが所持するＩＣカード２０２のＰＵＦデータとをデータストレージ２０４Ｂに記憶する。また、契約管理サーバ２０４Ａは、発行制御システム２０５におけるデータ生成サーバ２０５Ａからの契約ＩＤに基づく申請データの問い合わせに応じて、データストレージ２０４Ｂに保存している契約ＩＤに対応する申請データとＰＵＦデータとを提供する。

[0100] 発行制御システム２０５は、遠隔によるＩＣカードに対して発行処理（二次発行又は機能追加）を実行させるためのシステムである。発行制御システム２０５は、データ生成サーバ２０５ＡとＨＳＭ（ハードウエアセキュリティモジュール：Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）２０５ＢとＰＵＦストレージ２０５Ｃとを有する。

[0101] データ生成サーバ２０５Ａは、サーバ装置で構成される。ＨＳＭ２０５Ｂは、セキュアに鍵情報に保存し、鍵情報を用いた暗号処理を行うデバイスである。ＨＳＭ２０５Ｂには、本ＩＣカード発行システム２０１においてリモートでの発行処理を実行可能とするＩＣカード２０２が保持する鍵情報に対応する鍵情報を保存する。また、ＰＵＦストレージ２０５Ｃは、本ＩＣカード発行システム２０１においてリモートでの発行処理を実行可能とするＩＣカードのＰＵＦデータを保持する記憶装置である。ＰＵＦストレージ２０５Ｃには、例えば、ＩＣカード発行システム２０１での発行処理に実行対象となるＩＣカードの正規の製造者が発行（製造）したＩＣカード２０２のＰＵＦデータが登録される。

[0102] データ生成サーバ２０５Ａは、ＨＳＭ２０５Ｂにアクセスする機能、ＰＵＦストレージ２０５Ｃにアクセスする機能、インターネットを介してユーザ端末２０３と通信する機能およびデータ管理システム２０４の契約管理サーバ２０４Ａと通信する機能を有する。

[0103] データ生成サーバ２０５Ａは、ＨＳＭ２０５Ｂに保存する鍵および暗号処理機能を用いてユーザ端末２０３を介したＩＣカード２０２とのセキュアな通信を行う。データ生成サーバ２０５Ａは、ユーザ端末２０３からＩＣカー

ド２０２が鍵情報を用いて生成するカード認証データと契約ＩＤとを含む発行リクエストを取得する。

[0104] データ生成サーバ２０５Ａは、ユーザ端末２０３からの発行リクエストに応じてデータ管理システム２０４の契約管理サーバ２０４Ａが管理する申請データとＰＵＦデータとを取得する。データ生成サーバ２０５Ａは、発行リクエストに含まれるＰＵＦデータがＰＵＦストレージに登録されているか、および、発行リクエストに含まれるＰＵＦデータが契約管理サーバ２０４Ａから申請データとともに取得するＰＵＦデータと一致するかをチェックする。

[0105] データ生成サーバ２０５Ａは、発行リクエストに含まれるＰＵＦデータがＰＵＦストレージに登録され、かつ、申請時に取得したＰＵＦデータと一致することを確認した後、申請データに基づいてＩＣカードに対する発行処理を行うための発行データを生成する。データ生成サーバは、申請データに基づく発行データをＨＳＭ２０５Ｂが保存する鍵情報を用いて処理した後にユーザ端末２０３へ供給する。

[0106] 次に、第２実施形態に係る携帯可能電子装置としてのＩＣカード２０２における制御系の構成について説明する。

図１０は、第２実施形態に係る携帯可能電子装置としてのＩＣカード２０２の構成例を示すブロック図である。

ＩＣカード２０２は、外部装置から供給される電力により活性化する（動作可能な状態になる）携帯可能電子装置の一例である。ＩＣカード２０２は、スマートカードとも称される。図１０に示すように、ＩＣカード２０２は、本体Ｃを有する。本体Ｃは、プラスチックなどによりカード状に形成される。ＩＣカード２０２の本体Ｃ内には、制御モジュールＭが埋設される。制御モジュールＭは、１つ又は複数のＩＣチップに通信インターフェースが接続された状態で一体的に形成される。

[0107] 図１０に示す構成例において、制御モジュールＭは、プロセッサ２２１、ＲＯＭ２２２、ＲＡＭ２２３、データメモリ２２４および通信インターフェ

ース２２５を有する。また、ＩＣカード２０２の本体Ｃ内において、制御モジュールＭには、表示器２６および生体センサとしての指紋センサ２２０が接続される。

[0108] プロセッサ２２１は、種々の処理を実行する回路を含む。プロセッサ２２１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。プロセッサ２２１は、ＩＣカード２０２全体の制御を司る。プロセッサ２２１は、ＲＯＭ２２２あるいはデータメモリ２２４に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ２２１が実行する各種の機能のうちの一部又は全部は、ハードウエア回路により実現されるようにしても良い。

[0109] ＲＯＭ２２２は、プログラムメモリとして機能する不揮発性のメモリである。ＲＯＭ２２２は、予め制御用のプログラムおよび制御データなどが記憶される。ＲＯＭ２２２は、製造段階で制御プログラムや制御データなどが記憶された状態でＩＣカード２０２内に組み込まれるものである。ＲＯＭ２２２に記憶される制御プログラムや制御データは、予め当該ＩＣカード２０２の仕様に応じて組み込まれる。例えば、ＲＯＭ２２２には、外部装置（カードリーダライタ）から受信するコマンドに応じた処理をプロセッサ２２１が実行するためのプログラムが記憶される。

[0110] ＲＡＭ２２３は、ワーキングメモリとして機能する揮発性のメモリである。また、ＲＡＭ２２３は、プロセッサ２２１が処理中のデータなどを一時保管するバッファとしても機能する。例えば、ＲＡＭ２２３は、通信インターフェース２２５を介して外部装置との間で送受信するデータを一時保管する通信バッファとして機能する。

[0111] データメモリ２２４は、データの書き込みおよび書換えが可能な不揮発性のメモリである。データメモリ２２４は、例えば、ＥＥＰＲＯＭ（登録商標）（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などで構成する。データメモリ２２４には、当該ＩＣカード２０２の運用用途に応じたプログラムや種々の

データが書き込まれる。データメモリ２２４には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルに制御プログラムや種々のデータが書き込まれる。また、データメモリ２２４は、一部又は全部の領域が耐タンパー性を有し、セキュアにデータが格納できる。

[0112] データメモリ２２４は、鍵情報を記憶する第１の記憶領域２２４ａ、生体情報を記憶する第２の記憶領域２２４ｂ、および、ＰＵＦデータを保持する第３の記憶領域２２４ｃを有する。第１の記憶領域２２４ａは、セキュアにデータを記憶できる耐タンパー性を有するメモリである。第１の記憶領域２２４ａには、当該ＩＣカード２０２を使用可能な状態とする処理（一次発行）において鍵情報が書き込まれる。本ＩＣカード発行システム２０１においては、一次発行済みのＩＣカード２０２における第１の記憶領域２２４ａに書き込んだ鍵情報に対応する鍵情報が発行制御システム２０５におけるＨＳＭ２０５Ｂに保存されるものとする。

[0113] また、第２の記憶領域２２４ｂは、当該ＩＣカード２０２の所有者であるユーザの生体情報を記憶する。例えば、ＩＣカード２０２は、生体情報として指紋を用いた生体情報を行う指紋センサカードであることを想定する。ＩＣカード２０２が指紋センサカードである場合、ＩＣカード２０２の第２の記憶領域２２４ｂには所有者であるユーザの生体情報としての指紋情報が書き込まれる。なお、以下に説明する第２実施形態では、ＩＣカード２０２は、二次発行又は機能追加を実行する前に、第２の記憶領域にユーザの生体情報としての指紋情報が書き込まれた状態でユーザが所持しているものであることを前提とする。

[0114] 第３の記憶領域２２４ｃは、ＰＵＦデータが記憶される。第３の記憶領域２２４ｃに記憶されるＰＵＦデータは、当該ＩＣカード２０２に固有な識別情報の一例である。第３の記憶領域２２４ｃに記憶されるＰＵＦデータは、当該ＩＣカード２０２内に存在する電子回路（ＩＣチップなど）から得られる情報である。例えば、ＰＵＦデータは、当該ＩＣカード２０２の製造時などに第３の記憶領域に記憶されるものとする。

[0115] なお、ＰＵＦデータは、データメモリ２２４に予め記憶しておくものに限定されず、申請手続きおよび発行手続きにおいてプロセッサ２２１が取得できるようにすれば良い。例えば、ＩＣカード２０２は、データメモリ２２４にＰＵＦデータを記憶するのに代えて、ＰＵＦデータを出力するハードウエアとしてのＰＵＦ回路を設けても良い。この場合、プロセッサ２２１は、ＰＵＦ回路からＰＵＦデータを取得するようにすれば良い。

[0116] 通信インターフェース２２５は、通信制御部とインターフェース部とを有し、通信部を構成する。通信インターフェース２２５は、ユーザ端末２０３が備えるカードリーダライタ（ＲＷ）又はユーザ端末２０３とインターフェースを介して接続されるカードリーダライタと通信接続するためのインターフェースである。通信インターフェース２２５は、カードＲＷのインターフェースに対応した通信方式による通信機能を実現する。また、通信インターフェース２２５は、複数の通信方式（例えば、接触通信と非接触通信）をサポートするものとして構成しても良い。

[0117] 当該ＩＣカード２０２が非接触型のＩＣカードとして実現される場合、通信インターフェース２２５は、ユーザ端末２０３が備えるカードＲＷ又はユーザ端末２０３とインターフェースを介して接続されるカードＲＷと非接触（無線）で通信する通信部を構成する。この場合、通信インターフェース２２５は、電波の送受信を行うアンテナを備え、アンテナから送信する電波を生成するための変調回路およびアンテナが受信した電波から信号を生成するための復調回路などにより構成される。

[0118] また、当該ＩＣカード２０２が接触型のＩＣカードとして実現される場合、通信インターフェース２２５は、ユーザ端末２０３が備えるカードＲＷ又はユーザ端末２０３とインターフェースを介して接続されるカードＲＷと接触して通信する通信部を構成する。この場合、通信インターフェース２２５は、カードＲＷに設けられたコンタクト部と物理的かつ電気的に接触するコンタクト部を備え、コンタクト部を介した信号の送受信を制御する通信制御回路などにより構成される。

[0119] 生体センサ２２０は、認証情報を取得する認証情報取得部の一例である。生体センサ２２０は、認証処理に用いる認証情報として人物の生体情報を取得するセンサである。第２実施形態において、生体センサ２２０は、利用者の指紋情報（指紋画像）を読み取る指紋センサであるものとする。生体センサ２２０としての指紋センサは、指紋を読み取るセンサがカード本体Ｃの表面に露出するように設けられ、露出したセンサ部分に翳された人物の指の指紋を読み取る。生体センサ２２０が読み取る指紋情報が、データメモリ２２４の第２の記憶領域２２４ｂに記憶されている指紋情報と照合されることで指紋認証が実行される。

[0120] なお、生体センサ２２０は、指紋センサに限定されるものではなく、指紋以外の生体情報（例えば、掌紋、静脈、虹彩等）を取得するセンサであっても良い。指紋以外の生体情報を取得するセンサを備える場合、ＩＣカード２０２は、センサが取得する生体情報に対応した生体認証を行う機能（例えば、掌紋照合、静脈照合、虹彩照合等を実行するＩＣチップ）を備えるようにすれば良い。

[0121] 次に、第２実施形態に係るＩＣカード発行システム２０１におけるユーザ端末２０３の構成について説明する。

図１１は、第２実施形態に係るＩＣカード発行システム２０１におけるユーザ端末２０３の構成例を示すブロック図である。

ユーザ端末２０３は、オペレーティングシステム（ＯＳ）上で種々のアプリケーションプログラムが実行される電子装置である。ユーザ端末２０３は、ＩＣカード２０２を所持するカードホルダとしてのユーザが使用する電子装置であれば良い。例えば、ユーザ端末２０３は、スマートフォン、タブレット端末、携帯電話などのカードＲＷを備える携帯端末又はカードＲＷを接続するインターフェースを備える携帯端末である。また、ユーザ端末２０３は、カードＲＷを備えるパーソナルコンピュータ（ＰＣ）又はカードＲＷを接続するインターフェースを備えるＰＣであっても良い。

[0122] 図１１に示す構成例において、ユーザ端末２０３は、プロセッサ２３１、

ＲＯＭ２３２、ＲＡＭ２３３、データメモリ２３４、ネットワーク（ＮＷ）通信部２３５、カードリーダライタ（ＲＷ）２３６、表示部２３７、および、入力部２３８などを有する。

[0123] プロセッサ２３１は、プログラムを実行することにより各種の処理を実行する。プロセッサ２３１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。プロセッサ２３１は、システムバスを介してユーザ端末２０３内の各部と接続され、各部との間でデータを送受信する。プロセッサ２３１は、ＲＯＭ２３２およびＲＡＭ２３３と協働してユーザ端末２０３における制御およびデータ処理などの動作を実行する。例えば、プロセッサ２３１は、ＲＯＭ２３２あるいはデータメモリ２３４に記憶されているアプリケーションプログラムを実行することにより種々の処理機能を実現する。ただし、後述するプロセッサ２３１が実行する各種の機能のうちの一部又は全部は、ハードウエア回路により実現されるようにしても良い。

[0124] ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２３２は、ユーザ端末２０３の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。例えば、ＲＯＭ２３２は、オペレーティングシステム（ＯＳ）などの基本動作を司るプログラムを記憶する。また、ＲＯＭ２３２は、ユーザ端末２０３が具備する機能を実現するためのアプリケーションプログラムなどを記憶しても良い。ＲＯＭ２３２は、書き換え可能な不揮発性のメモリで構成しても良い。例えば、書き換え可能なＲＯＭ２３２としては、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）又はフラッシュＲＯＭなどで実現される。

[0125] ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２３３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ２３３は、プロセッサ２３１がプログラムを実行する場合にワーキングメモリとして機能する。

[0126] データメモリ２３４は、各種のデータを記憶する記憶部である。データメモリ２３４は、データの書き換えが可能な不揮発性のメモリで構成される。

例えば、データメモリ２３４は、フラッシュＲＯＭ、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）などの半導体素子メモリ、あるいは、ＨＤＤ（Ｈａｒｄ Ｄｉｓｃ Ｄｒｉｖｅ）などの記憶装置が用いられる。データメモリ２３４は、アプリケーションプログラム、動作設定値、個人情報などを記憶する。また、データメモリ２３４は、ＯＳプログラムを記憶するようにしても良い。

[0127] ＮＷ通信部２３５は、外部装置と通信するための通信インターフェースである。ＮＷ通信部２３５は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。ＩＣカード発行システム２０１において、ＮＷ通信部２３５は、インターフェースを介して、契約管理サーバ２０４Ａおよびデータ生成サーバ２０５Ａと通信するものであれば良い。

[0128] カードリーダライタ２３６は、ＩＣカード２０２と通信する機能を有する。カードリーダライタ２３６は、ＩＣカード２０２に対して、電源供給、クロック供給、リセット制御、データの送受信を行う。カードリーダライタ２３６は、ＩＣカード２０２を活性化（起動）させた後、プロセッサ２３１による制御に基づいて種々のコマンドを送信したり送信したコマンドに対する応答を受信したりする。なお、ユーザ端末２０３は、外部機器としてのカードリーダライタに接続するためのインターフェースを備える構成としても良い。

[0129] カードリーダライタ２３６は、ＩＣカード２０２が備える通信方式に対応する構成を備える。例えば、ＩＣカード２０２が非接触型のＩＣカードとして実現される場合、カードリーダライタ２３６は、非接触型のＩＣカードの通信方式に準拠する通信プロトコルで、非接触（無線）でＩＣカード２０２と通信する。また、ＩＣカード２０２が接触型のＩＣカードとして実現される場合、カードリーダライタ２３６は、ＩＣカード２０２のコンタクト部（インターフェース）と物理的かつ電気的に接触するコンタクト部を有し、コンタクト部を介してデータの送受信を行う。

[0130] 表示部２３７は、液晶パネル等の表示デバイスである。入力部２３８は、

ユーザ端末２０３に対して操作指示を入力する操作デバイスである。入力部２３８は、例えば、タッチパネルを含む。表示部２３７と入力部２３８とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部２３８は、ボタンスイッチで構成する操作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。

[0131] 次に、第２実施形態に係るＩＣカード発行システム２０１における契約管理サーバ２０４Ａの構成について説明する。

図１２は、第２実施形態に係るＩＣカード発行システム２０１における契約管理サーバ２０４Ａの構成例を示すブロック図である。

図１２に示すように、契約管理サーバ２０４Ａは、プロセッサ２４１、ＲＯＭ２４２、ＲＡＭ２４３、データメモリ２４４、インターフェース２４５、ネットワーク（ＮＷ）通信部２４６、および、通信部２４７を有する。

[0132] プロセッサ２４１は、プログラムを実行することにより各種の処理を実行する。プロセッサ２４１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ２４１は、システムバスを介してサーバ４Ａ内の各部と接続され、各部との間でデータを送受信する。プロセッサ２４１は、ＲＯＭ２４２およびＲＡＭ２４３と協働して契約管理サーバ２０４Ａにおける制御およびデータ処理などの動作を実行する。

[0133] ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２４２は、契約管理サーバ２０４Ａの基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２４３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ２４３は、プロセッサ２４１がプログラムを実行する場合にワーキングメモリとして機能する。

データメモリ２４４は、各種のデータを記憶する記憶部である。データメモリ２４４は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ２４４は、ＯＳプログラム、アプリケーションプログ

ラム、動作設定情報などを記憶する。

[0134] インターフェース２４５は、データストレージ２０４Ｂにアクセスするためのインターフェースである。データストレージ２０４Ｂが外部デバイスとしての記憶装置である場合、インターフェース２４５は、データストレージ２０４Ｂとしての記憶装置が備えるインターフェース規格に対応したものであれば良い。また、データストレージ２０４Ｂがデータサーバ等である場合、インターフェースは、データストレージ２０４Ｂとしてのサーバと通信するための通信インターフェースで構成すれば良い。

[0135] ネットワーク（ＮＷ）通信部２４６は、外部装置と通信するための通信インターフェースである。ＮＷ通信部２４６は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第２実施形態に係るＩＣカード発行システム２０１において、ＮＷ通信部２４６は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末２０３と通信するものであれば良い。

[0136] 通信部２４７は、データ生成サーバ２０５Ａと通信するための通信インターフェースである。通信部２４７は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第２実施形態に係るＩＣカード発行システム２０１において、通信部２４７は、データ生成サーバ２０５Ａとの通信がセキュアに行えるものであれば良い。

なお、ＮＷ通信部２４６および通信部２４７は、１つの通信インターフェースで実現する構成しても良い。さらに、インターフェース２４５についても、ＮＷ通信部２４６又は通信部２４７と共通化した通信インターフェースとする構成としても良い。

[0137] 次に、第２実施形態に係るＩＣカード発行システム２０１におけるデータ生成サーバ２０５Ａの構成について説明する。

図１３は、第２実施形態に係るＩＣカード発行システム２０１におけるデータ生成サーバ２０５Ａの構成例を示すブロック図である。

図１３に示すように、データ生成サーバ２０５Ａは、プロセッサ２５１、

ＲＯＭ２５２、ＲＡＭ２５３、データメモリ２５４、インターフェース２５５、ネットワーク（ＮＷ）通信部２５６、通信部２５７、および、インターフェース２５８を有する。

[0138] プロセッサ２５１は、プログラムを実行することにより各種の処理を実行する。プロセッサ２５１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ２５１は、システムバスを介してサーバ５Ａ内の各部と接続され、各部との間でデータを送受信する。プロセッサ２５１は、ＲＯＭ２５２およびＲＡＭ２５３と協働してデータ生成サーバ２０５Ａにおける制御およびデータ処理などの動作を実行する。

[0139] ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２５２は、データ生成サーバ２０５Ａの基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２５３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ２５３は、プロセッサ２５１がプログラムを実行する場合にワーキングメモリとして機能する。

データメモリ２５４は、各種のデータを記憶する記憶部である。データメモリ２５４は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ２５４は、ＯＳプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0140] インターフェース２５５は、ＨＳＭ２０５Ｂにアクセスするためのインターフェースである。インターフェース２５５は、ＨＳＭ２０５Ｂが備えるインターフェース規格に対応したものであれば良い。

ネットワーク（ＮＷ）通信部２５６は、外部装置と通信するための通信インターフェースである。ＮＷ通信部２５６は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第２実施形態に係るＩＣカード発行システム２０１において、ＮＷ通信部２５６は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末２０３と通信するものであれば良い。

[0141] 通信部２５７は、契約管理サーバ２０４Ａと通信するための通信インターフェースである。通信部２５７は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第２実施形態に係るＩＣカード発行システム２０１において、通信部２５７は、契約管理サーバ２０４Ａとの通信がセキュアに行えるものであれば良い。

なお、ＮＷ通信部２５６および通信部２５７は、１つの通信インターフェースで実現する構成しても良い。

[0142] インターフェース２５８は、ＰＵＦストレージ２０５Ｃにアクセスするためのインターフェースである。インターフェース２５８は、ＰＵＦストレージ２０５Ｃが備えるインターフェース規格に対応したものであれば良い。プロセッサ２５１は、インターフェース２５８を介してＰＵＦストレージ２０５Ｃに登録されているＰＵＦデータを確認する。

[0143] 次に、第２実施形態に係るＩＣカード発行システム２０１におけるＩＣカード２０２に対する発行処理の申請手続きおよび発行手続きについて説明する。

以下に説明する動作の前提条件として、ＩＣカード２０２は、一次発行（カード製造と初期化）の処理がなされた後にユーザ（カードホルダ）に渡されるものとする。また、ユーザに渡されるＩＣカード２０２には、一次発行においてカード認証データの生成に関する鍵（鍵情報）が書き込まれているものとする。ＩＣカード２０２に書き込まれた鍵情報は、発行制御システム２０５におけるＨＳＭ２０５Ｂに保存されている。さらに、ユーザ（カードホルダ）が所持するＩＣカード２０２には、当該ユーザの本人認証が行われた上で当該ユーザ（本人）の指紋情報が書き込まれているものとする。

[0144] まず、第２実施形態に係るＩＣカード発行システム２０１におけるＩＣカード２０２に対する発行処理の申請手続きについて説明する。

図１４は、ＩＣカード発行システム２０１におけるＩＣカード２０２に対する発行処理の申請手続きの動作例を説明するためのシーケンスである。

カードホルダは、ユーザ端末２０３のプロセッサ２３１は、カードホルダ

としてのユーザの操作に応じて入力部２３８による申請データの入力を受け付ける（ＳＴ２２１）。申請データとしては、例えば、発行処理（二次発行又は機能追加）に必要な情報、カードホルダであるユーザ自身の個人情報、および、カードホルダ（ユーザ）が所持するＩＣカード２０２に関する情報などが含まれることが想定される。

[0145] また、ユーザ端末２０３は、申請用のプログラムにより申請データが入力されるようにしても良いし、インターネット上に提供される申請データの入力用のＷｅｂサイトで申請データが入力されるようにしても良い。前者の場合、ユーザ端末２０３は、データメモリ２３４に申請用のプログラムをインストールしておく。ユーザ端末２０３のプロセッサ２３１は、ユーザの操作に応じて申請用のプログラムを起動し、申請用のプログラムで提示される申請データの入力フォーマットに従って申請データを入力する。また、後者の場合、ユーザ端末２０３のプロセッサ２３１は、ＮＷ通信部２３５によりインターネット上で提供される申請データの入力用のサイドにアクセスし、入力用のサイトで提示される申請データの入力フォーマットに沿って申請データを入力する。

[0146] また、ユーザ端末２０３のプロセッサ２３１は、入力部２３８で入力される申請データの情報に加えて、カードホルダ（ユーザ）が所持するＩＣカード２０２に関する情報を当該ＩＣカード２０２から読み取る。ここでは、当該ＩＣカード２０２に関する情報には、当該ＩＣカード２０２を識別するための固有な識別情報（ＩＤ）としてＰＵＦデータが含まれるものとする。

[0147] また、カードホルダであるユーザ自身の個人情報がＩＣカード２０２に保存されている場合、ユーザ端末２０３のプロセッサ２３１は、ユーザの個人情報をＩＣカード２０２から読み取るようにしても良い。

[0148] 図１４に示す動作例において、ＩＣカード２０２は、ユーザ端末２０３のカードＲＷ２３６からの要求に応じて、生体認証で本人確認が成功した後にＰＵＦデータを含むＩＣカードに関する情報を出力するものとする。

[0149] この場合、ユーザ端末２０３のプロセッサ２３１は、カードＲＷ２３６に

より生体認証としての指紋認証の要求とＰＵＦデータの出力要求とＩＣカード２０２へ送信する（ＳＴ２２２）。ＩＣカード２０２のプロセッサ２２１は、ユーザ端末２０３からの要求に応じてデータメモリ２２４に記憶されている指紋データを用いて指紋認証を実行する（ＳＴ２１１）。ＩＣカード２０２のプロセッサ２２１は、指紋認証による本人確認が成功した後に当該ＩＣカード２０２の０ＰＵＦデータを含むカードデータをユーザ端末２０３へ出力する（ＳＴ２１２）。

[0150] 申請データの入力およびＰＵＦデータの取得が完了すると、ユーザ端末２０３のプロセッサ２３１は、入力された申請データによる発行処理（契約）に関する審査を要求する審査リクエストを作成する（ＳＴ２２３）。審査リクエストは、申請データとして入力された申請内容によって、カードホルダが所持するＩＣカード２０２に対する発行処理（二次発行又は機能追加）を実行すること（契約）が可能であるか否かの審査を要求するものである。また、審査リクエストには、ＩＣカード２０２から取得したＰＵＦデータも含まれるものとする。

[0151] 申請データとＰＵＦデータとを含む審査リクエストを作成すると、ユーザ端末２０３のプロセッサ２３１は、データ管理システム２０４の契約管理サーバ２０４Ａへ審査リクエストを送信する（ＳＴ２２４）。プロセッサ２３１は、ＮＷ通信部２３５によりインターネットを介して契約管理サーバ２０４Ａにアクセスし、審査リクエストを契約管理サーバ２０４Ａへ送信する。

[0152] 契約管理サーバ２０４Ａは、ＮＷ通信部２４６によりユーザ端末２０３からの審査リクエストを受け付ける（ＳＴ２３１）。ユーザ端末２０３からの審査リクエストを受信すると、契約管理サーバ２０４Ａのプロセッサ２４１は、受信した審査リクエストに応じて申請された発行処理を許可するか否かを審査する。

[0153] 例えば、契約管理サーバ２０４Ａは、申請データが示す申請内容に問題がないか、および、申請者であるカードホルダに関して発行処理を行うための契約上の問題がないかを審査する。審査の内容および手続きは、運用形態に

準じたものであれば良く、特定の形態に限定されるものではない。つまり、審査手続きは、契約管理サーバ２０４Ａに審査リクエストに対する審査結果が入力されるものであれば良い。

[0154] 審査リクエストに対する審査結果が契約不可（発行処理が不可）であった場合、契約管理サーバ２０４Ａのプロセッサ２４１は、審査結果として契約不可となった旨を審査リクエストの送信元であるユーザ端末２０３へ通知する（ＳＴ２３４）。また、プロセッサ２４１は、申請データでカードホルダが指定した連絡先に審査結果を通知するようにしても良い。

[0155] ユーザ端末２０３のプロセッサ２３１は、契約管理サーバ２０４Ａから審査リクエストに対する審査結果が契約不可である旨の通知を受けると、審査結果が契約不可であった旨を表示部２３７に表示することによりカードホルダに報知する（ＳＴ２２５）。

[0156] 審査リクエストに対する審査結果が契約可（発行処理が可）であった場合、契約管理サーバ２０４Ａのプロセッサ２４１は、契約ＩＤを発行する（ＳＴ２３２）。契約ＩＤを発行すると、プロセッサ２４１は、審査結果が契約可となった審査リクエストに含まれる申請データとＰＵＦデータとを発行した契約ＩＤに対応づけてデータストレージ２０４Ｂに登録する（ＳＴ２３３）。これにより、データストレージ２０４Ｂは、契約管理サーバ２０４Ａからの申請データとＰＵＦデータと契約ＩＤとを対応づけた情報を保存する（ＳＴ２４１）。

[0157] 申請データとＰＵＦデータと契約ＩＤとをデータストレージ２０４Ｂに登録すると、契約管理サーバ２０４Ａのプロセッサ２４１は、審査結果とともに契約ＩＤを審査リクエストの送信元であるユーザ端末２０３へ通知する（ＳＴ２３４）。

[0158] ユーザ端末２０３のプロセッサ２３１は、契約管理サーバ２０４Ａから審査リクエストに対する審査結果が契約可である旨の通知を受けると、審査結果として契約可であった旨の案内とともに、契約ＩＤを表示部２３７に表示する（ＳＴ２２５）。ここで、審査結果が可であった場合、ユーザ端末２０

３のプロセッサ２３１は、表示部２３７に発行処理の手続きに関する案内などを表示するようにしても良い。なお、契約ＩＤは、審査結果が契約可であった場合にカードホルダとなるユーザに報知されるものであれば良い。例えば、契約管理サーバ２０４Ａは、申請データに含まるカードホルダの連絡先（例えば、メールアドレス）に契約ＩＤを通知するようにしても良い。

[0159] 以上のような申請手続きによって、契約管理サーバは、ユーザ端末からの審査リクエストが契約可となった場合、当該審査リクエストを行ったカードホルダからの申請データと発行処理の対象とするＩＣカードのＰＵＦデータと契約ＩＤとをデータストレージに保存することができる。この結果、カードホルダが所持するＩＣカード２０２は、後述するような動作によるリモートでの発行処理が可能な状態となる。つまり、カードホルダは、発行処理が可能な状態となった後、ユーザ端末２０３を用いてＩＣカード２０２に対してリモートで発行処理を行うための後述するような発行手続きを実行する。

[0160] 次に、第２実施形態に係るＩＣカード発行システム２０１におけるＩＣカード２０２に対する発行処理を行うための発行手続きについて説明する。

図１５および図１６は、ＩＣカード発行システム２０１におけるＩＣカード２０２に対する発行処理を行うための発行手続きの動作例を説明するためのシーケンスである。

カードホルダとしてのユーザは、ユーザ端末２０３においてＩＣカード２０２に対する発行処理用のアプリケーションプログラム（以下、発行アプリと称する）を起動させる。発行アプリは、予めデータメモリ２２４に記憶しておくようにしても良いし、契約管理サーバ２０４Ａ又はデータ生成サーバ２０５Ａからダウンロードするようにしても良い。

[0161] ユーザ端末２０３のプロセッサ２３１は、カードホルダが入力部２３８に入力する発行アプリの起動指示に応じて発行アプリを起動させる（ＳＴ３２０）。発行アプリが起動すると、プロセッサ２３１は、カードホルダに対して契約ＩＤの入力を要求する（ＳＴ３２１）。カードホルダは、申請データに対する審査結果と共に取得した契約ＩＤを入力部２３８により入力する。

プロセッサ２３１は、入力部２３８に契約ＩＤが入力されると、カードＲＷ２３６によりＩＣカード２０２にアクセスし、本人確認のための生体認証としての指紋認証をＩＣカード２０２に要求する（ＳＴ３２２）。

[0162] ＩＣカード２０２は、カードＲＷ２３６から供給される電力により起動する。ＩＣカード２０２が起動すると、プロセッサ２２１は、カードＲＷ２３６から供給される生体（指紋）認証の要求に応じて指紋認証処理を実行する（ＳＴ３１１）。指紋認証を実行する場合、プロセッサ２２１は、指紋センサ２２０によってユーザ（カードホルダ）の指紋を取得する。プロセッサ２２１は、指紋センサ２２０が取得した指紋情報とデータメモリ２２４の第２の記憶領域２２４ｂに記憶している指紋データとを比較することにより指紋認証を行う。

[0163] 指紋センサ２２０が取得した指紋情報とデータメモリ２２４の第２の記憶領域２２４ｂに記憶している指紋データとが同一人物の指紋であると判定された場合、プロセッサ２２１は、指紋認証が成功したものとする。指紋センサ２２０が取得した指紋情報と第２の記憶領域２２４ｂに記憶している指紋データとが同一人物の指紋であると判定できなかった場合、プロセッサ２２１は、指紋認証が失敗したものとする。

[0164] ＩＣカード２０２における指紋認証が失敗した場合、プロセッサ２２１は、指紋認証が失敗したことをカードＲＷ２３６へ通知する。カードＲＷ２３６によりＩＣカード２０２から指紋認証が失敗した旨の通知を受けた場合、ユーザ端末２０３のプロセッサ２３１は、ＩＣカード２０２に対する発行処理を実行するための発行手続きを中止する。この場合、プロセッサ２３１は、表示部２３７に本人確認が失敗したためにＩＣカード２０２に対する発行処理で不可となった旨を表示することによりユーザに発行手続きの中止を報知する。

[0165] ＩＣカード２０２における指紋認証が成功した場合、プロセッサ２２１は、指紋認証が成功したことをカードＲＷ２３６へ通知する。カードＲＷ２３６によりＩＣカード２０２から指紋認証が成功した旨の通知を受けた場合、

ユーザ端末２０３のプロセッサ２３１は、カードＲＷ２３６を介してＩＣカード２０２に発行処理を実行するためのカード認証データとＰＵＦデータとを要求する。これに対して、ＩＣカード２０２のプロセッサ２２１は、カード認証データを生成するとともにＰＵＦデータを取得し、生成したカード認証データとＰＵＦデータとをカードＲＷ２３６へ供給する。

[0166] すなわち、ＩＣカード２０２のプロセッサ２２１は、指紋認証が成功した場合、カード認証データ（認証データ）を生成する（ＳＴ３１２）。カード認証データは、当該ＩＣカード２０２における生体認証が成功した場合に生成される認証データであり、当該ＩＣカード２０２に機能追加（例えば、アプレットの追加）あるいは二次発行などの発行処理を実施するための情報を含む。

[0167] カード認証データは、セキュアメモリであるデータメモリ２２４の記憶領域２２４ａに記憶されている鍵情報を用いて生成される。また、カード認証データには、発行処理を実施するための情報として、例えば、ＣＰＬＣ（当該ＩＣカードのプロダクトサイクルを示す情報）、ＩＮＩＴＩＡＬＩＺＥＵＰＤＡＴＥコマンドおよびレスポンスデータなどが含まれる。

[0168] また、ＩＣカード２０２のプロセッサ２２１は、指紋認証が成功した場合、当該ＩＣカード２０２に固有な情報であるＰＵＦデータを取得する。図１０に示すようにＰＵＦデータがデータメモリ２２４の第３の記憶領域２２４ｃに保持される場合、プロセッサ２２１は、データメモリ２２４における第３の記憶領域からＰＵＦデータを取得する。ただし、ＩＣカード２０２がＰＵＦデータを出力するデバイスとしてのＰＵＦ回路を備える構成である場合、プロセッサ２２１は、ＰＵＦ回路からＰＵＦデータを取得するようにすれば良い。

[0169] 指紋認証が成功した後にカード認証データを生成し、ＰＵＦデータを取得すると、ＩＣカード２０２のプロセッサ２２１は、生成したカード認証データとＰＵＦデータとをユーザ端末２０３のカードＲＷ２３６へ出力する（ＳＴ３１３）。カード認証データとＰＵＦデータとを出力した後、ＩＣカード

２０２のプロセッサ２２１は、当該カード認証データに対応してデータ生成サーバ２０５Ａが生成する発行データに基づく発行処理が実行可能な状態とする。

[0170] ユーザ端末２０３のプロセッサ２３１は、カードＲＷ２３６により指紋認証が成功したＩＣカード２０２からカード認証データとＰＵＦデータとを取得すると、ＩＣカード２０２に対する発行処理を要求する発行リクエストを生成し、生成した発行リクエストをデータ生成サーバ２０５Ａへ送信する（ＳＴ３２４）。

[0171] 例えば、プロセッサ２３１は、ＩＣカード２０２から取得するカード認証データとＰＵＦデータとに加えて入力部２３８で入力された契約ＩＤを含む発行リクエストを生成する。カード認証データとＰＵＦデータと契約ＩＤとを含む発行リクエストを生成すると、プロセッサ２３１は、ＮＷ通信部２３５によりインターネットを介して発行制御システム２０５におけるデータ生成サーバ２０５Ａにアクセスする。データ生成サーバ２０５Ａにアクセスすると、プロセッサ２３１は、カード認証データ、ＰＵＦデータおよび契約ＩＤを含む発行リクエストをデータ生成サーバ２０５Ａへ送信する。

[0172] データ生成サーバ２０５Ａは、ＮＷ通信部２５６によりユーザ端末２０３からの発行リクエストを受信する。発行リクエストを受信した場合、データ生成サーバ２０５Ａのプロセッサ２５１は、発行リクエストに含まれる契約ＩＤを抽出する。発行リクエストに含まれる契約ＩＤを抽出すると、プロセッサ２５１は、通信部２５７を介して契約管理サーバ２０４Ａにアクセスする。契約管理サーバ２０４Ａにアクセスすると、プロセッサ２５１は、発行リクエストに含まれる契約ＩＤに対応する申請データの要求（リクエスト）を契約管理サーバ２０４Ａへ送信する（ＳＴ３３１）。

[0173] 契約管理サーバ２０４Ａは、通信部２４７を介してデータ生成サーバ２０５Ａと通信する。契約管理サーバ２０４Ａのプロセッサ２４１は、データ生成サーバ２０５Ａから契約ＩＤに対応する申請データを要求するリクエストを受信した場合、データストレージ２０４Ｂにおいて当該契約ＩＤに対応す

る申請データを検索する（ＳＴ３４１）。データ生成サーバ２０５Ａから要求された契約ＩＤに対応する申請データを検出すると、プロセッサ２４１は、通信部２４７を介して当該契約ＩＤに対応する申請データとＰＵＦデータとをデータ生成サーバ２０５Ａへ送信する（ＳＴ３４２）。

[0174] 契約管理サーバ２０４Ａから契約ＩＤに対応する申請データとＰＵＦデータとを受信すると、データ生成サーバ２０５Ａのプロセッサ２５１は、ユーザ端末２０３からの発行リクエストに含まれるＰＵＦデータが、ＰＵＦストレージ２０５Ｃに登録され、かつ、申請データに対応するＰＵＦデータと一致するかを確認する（ＳＴ３３２）。

[0175] 例えば、プロセッサ２５１は、発行リクエストに含まれるＰＵＦデータがＰＵＦストレージ２０５Ｃに登録されているかを確認する。つまり、プロセッサ２５１は、発行リクエストに含まれるＰＵＦデータ（発行処理を要求するＩＣカードのＰＵＦデータ）がＰＵＦストレージ２０５Ｃに登録されているか正規品のＩＣカードのＰＵＦデータであるかを確認（真偽判定）する。これにより、プロセッサ２５１は、発行処理を要求するＩＣカードが正規品であることを確認できる。

[0176] 発行リクエストに含まれるＰＵＦデータがＰＵＦストレージ２０５Ｃに登録されている場合、プロセッサ２５１は、さらに、発行リクエストに含まれるＰＵＦデータが契約管理サーバ２０４Ａから取得したＰＵＦデータと一致するかを確認する。つまり、プロセッサ２５１は、発行リクエストに含まれるＰＵＦデータ（発行処理を要求するＩＣカードのＰＵＦデータ）が発行処理の申請を行ったＩＣカードのＰＵＦデータと一致するかを確認する。これにより、プロセッサ２５１は、発行処理を要求するＩＣカードが発行処理の申請を行ったＩＣカードと同一であることを確認できる。

なお、データ生成サーバ２０５Ａのプロセッサ２５１は、ユーザ端末２０３から発行リクエストを受けた場合に、発行リクエストに含まれるＰＵＦデータがＰＵＦストレージに登録されているかをチェックするようにしても良い。すなわち、プロセッサ２５１は、発行リクエストに含まれるＰＵＦデー

タがＰＵＦストレージに登録されていることを確認した後に、契約管理サーバ２０４Ａから申請データとＰＵＦデータとを取得するようにしても良い。

[0177] ＰＵＦデータのチェックにより発行処理の対象とするＩＣカード２０２が正規品で、かつ、申請を行ったＩＣカードと一致することを確認した場合、データ生成サーバ２０５Ａのプロセッサ２５１は、ＩＣカード２０２において申請データに基づく発行処理を実行するための発行データを生成する（ＳＴ３３３）。発行データは、申請データに基づく一連の発行処理においてＩＣカード２０２に実行させるべきコマンドと一連の発行処理においてＩＣカード２０２に書き込むべきデータとを含む。

[0178] 例えば、発行処理としてＩＣカード２０２にアプレットを追加する場合、発行データには、ＩＣカード２０２に実行させるべきコマンドとしてインストール（ＩＮＳＴＡＬＬ）コマンドが含まれる。また、あるクレジットカードの規格でアプレットを追加する場合、発行データには、ＩＣカード２０２に実行させるべきコマンドとして外部認証（ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ）コマンド、および、ストアデータ（ＳＴＯＲＥ　ＤＡＴＡ）コマンドが含まれる。

[0179] また、プロセッサ２５１は、発行データをセキュアにＩＣカード２０２に供給するためにＨＳＭ２０５Ｂが保管する鍵情報を用いて発行データを処理する（ＳＴ３３４）。ここで、ＨＳＭ２０５Ｂには、ＩＣカード２０２内に保持する鍵情報に対応する鍵情報が保存されている。これにより、ＨＳＭ２０５Ｂを用いた暗号化によって安全に発行データをＩＣカード２０２へ供給できる。例えば、プロセッサ２５１は、ＨＳＭ２０５Ｂにおいて当該ＩＣカード２０２内の保存される鍵情報と共有する鍵情報を用いて発行データに含まれるデータを暗号化する。

[0180] 発行データをＨＳＭ２０５Ｂが保存する鍵情報で暗号化処理した後、プロセッサ２５１は、発行リクエストの送信元であるユーザ端末２０３へＨＳＭ２０５Ｂで暗号化処理した発行データを送信する（ＳＴ３３５）。

[0181] ユーザ端末２０３は、データ生成サーバ２０５Ａへ発行リクエストを送信

した後、発行リクエストに対する応答としての発行データの受信待ちとなる。この状態において、ユーザ端末２０３は、ＮＷ通信部２３５４によりデータ生成サーバ２０５Ａから送信される発行データを受信する（ＳＴ３２５）。発行データを受信した場合、ユーザ端末２０３のプロセッサ２３１は、カードＲＷ２３６によりＩＣカード２０２に対して発行データを出力する（ＳＴ３２６）。

[0182] これにより、ＩＣカード２０２のプロセッサ２２１は、生体認証が成功した後に生成したカード認証データに対応する発行データをユーザ端末２０３のカードＲＷ２３６から取得することとなる。発行データを取得すると、プロセッサ２２１は、取得した発行データに従って発行処理を実行する（ＳＴ３１４）。

[0183] 例えば、プロセッサ２２１は、発行データに含まれるコマンドを実行することにより発行処理として書き込むべきデータをデータメモリ２２４に書き込む。また、プロセッサ２２１は、発行処理において供給される発行データに含まれる暗号化データをデータメモリ２２４におけるセキュアメモリである第１の記憶領域２２４ａに記憶している鍵情報を用いて復号化する。

[0184] ＩＣカード２０２のプロセッサ２２１は、供給された発行データに基づく発行処理が完了すると、発行処理の完了をユーザ端末２０３のカードＲＷ２３６へ通知する（ＳＴ３１５）。

ユーザ端末２０３は、カードＲＷ２３６によりＩＣカード２０２へ発行データを出力した後にＩＣカード２０２から発行処理が完了した旨の通知を受信する。ユーザ端末２０３のプロセッサ２３１は、カードＲＷ２３６によりＩＣカード２０２から発行処理の完了通知を受けると、ＩＣカード２０２における発行処理（機能追加あるいは二次発行）が完了した旨の案内を表示部２３７に表示する（ＳＴ３２７）。

[0185] また、発行データに基づくＩＣカード２０２における発行処理が完了した旨の通知を受けると、プロセッサ２３１は、ＮＷ通信部２３５により発行データの送信元であるデータ生成サーバ２０５Ａへ発行処理の完了を通知する

（ＳＴ３２８）。

データ生成サーバ２０５Ａのプロセッサ２５１は、ユーザ端末２０３からのＩＣカード２０２における発行処理の完了通知をＮＷ通信部２５６により受信すると、通信部２５７によりＩＣカード２０２における発行処理の完了通知を契約管理サーバ２０４Ａへ転送（送信）する。

[0186] 契約管理サーバ２０４Ａは、通信部２４７によりデータ生成サーバ２０５Ａを介してＩＣカード２０２における発行処理の完了通知を受信する。契約管理サーバ２０４Ａのプロセッサ２４１は、データ生成サーバ２０５Ａを経由してＩＣカード２０２における発行処理の完了通知を受信すると、データストレージ２０４Ｂにおいて申請データに対応して発行処理の完了を記録する（ＳＴ３４３）。

[0187] 以上のような発行手続きによって、第２実施形態に係るＩＣカード発行システムは、生体センサとしての指紋センサを有するＩＣカードにおける生体認証による本人認証が成功した後、当該ＩＣカードが正規品で、かつ、申請時のＩＣカードと一致するかについてＰＵＦデータを用いて確認できる。この結果、第２実施形態に係るＩＣカード発行システムは、正規品で、かつ、申請時と一致するＩＣカードに対してリモートで機能追加あるいは二次発行などの発行処理を行うことができる。

[0188] 第２実施形態に係るＩＣカード発行システムは、ＰＵＦデータを用いたが、これにより、従来のようにＩＣカードを生成する際に人為的に個々のＬＳＩに対する固有のデータを生成し、それをＬＳＩに書き込むという作業が不要となる。ＰＵＦは、電子回路や半導体の結晶パターンなどの物理的な固有のばらつきを利用して、特定のアルゴリズムにより、自動的に生成させることができるからである。

[0189] また、ＩＣカードに個別に付される識別符号のような固有データが必要となる場合、過去に発行してきたデータと必ず異なるデータとなることが必要となる。その点、ＰＵＦは、必ず固有のデータとなり、重複することがないため、ＩＤとして、この第２実施形態に係る発明に好適となる。

[0190] さらに、ＬＳＩに固有のデータを作成するには、ＬＳＩベンダーによって、作成する様式又は形式が異なるのが一般的である。その点、第２実施形態に係る発明によれば、ＰＵＦを使用することで、固有のデータの生成や形式を統一することができる。

[0191] 上述の各実施形態で説明した機能は、ハードウエアを用いて構成するに留まらず、ソフトウエアを用いて各機能を記載したプログラムをコンピュータに読み込ませて実現することもできる。また、各機能は、適宜ソフトウエア、ハードウエアのいずれかを選択して構成するものであっても良い。

[0192] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

[請求項1] 携帯可能電子装置とデータ生成サーバとを有するリモート発行システムであって、

前記携帯可能電子装置は、

生体情報を取得する生体センサと、

ユーザの生体情報を記憶する記憶領域を含むメモリと、

ユーザ端末と接続されるリーダライタと通信する通信インターフェースと、

前記生体センサにより取得する生体情報と前記メモリに保存する生体情報との照合による生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、前記認証データを前記リーダライタへ出力し、前記リーダライタから供給される前記認証データに対応する発行データに基づいて発行処理を実行する第１プロセッサと、を有し、

前記データ生成サーバは、

前記ユーザ端末と通信する通信部と、

前記ユーザ端末から前記携帯可能電子装置が生成した前記認証データと契約ＩＤとを含む発行リクエストを受信した場合、前記契約ＩＤに対応する申請データと前記認証データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信する第２プロセッサと、を有する、

リモート発行システム。

[請求項2] 前記携帯可能電子装置は、前記生体センサ、前記メモリ、前記第１プロセッサ、および、前記通信インターフェースを有するモジュールと、前記モジュールを格納する本体と、を備えるＩＣカードである、

請求項１に記載のリモート発行システム。

[請求項3] 前記生体センサは、指紋情報を取得する指紋センサである、

請求項１又は２のいずれか１項に記載のリモート発行システム。

[請求項4] 前記携帯可能電子装置は、

前記メモリは、さらに、鍵情報を記憶するセキュアメモリを含み、

前記第１プロセッサは、前記セキュアメモリに記憶する鍵情報を用いて前記認証データを生成し、

前記データ生成サーバは、

さらに、前記携帯可能電子装置が備える前記セキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウエアセキュリティモジュールに接続するインターフェースを有し、

前記第２プロセッサは、前記ハードウエアセキュリティモジュールが保存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項１に記載のリモート発行システム。

[請求項5] 契約管理サーバとデータ生成サーバとを有するリモート発行システムであって、

前記契約管理サーバは、

ユーザ端末と通信する第１通信部と、

前記第１通信部によりユーザ端末から携帯可能電子装置に対する発行処理を申請する申請データを含む審査リクエストを受信し、前記審査リクエストに応じた審査で前記申請データで申請される発行処理が許可された場合に契約ＩＤを発行する第１プロセッサと、　前記契約ＩＤと前記申請データとを対応づけて保存するデータストレージにアクセスするためのインターフェースと、と有し、

前記データ生成サーバは、

前記ユーザ端末と通信する第２通信部と、

携帯可能電子装置における生体認証が成功した場合に当該携帯可能電子装置が生成する認証データと前記契約管理サーバが発行した前記契約ＩＤとを含む発行リクエストを前記ユーザ端末から受信し、

前記発行リクエストに含まれる契約ＩＤに対応する申請データを

前記契約管理サーバから取得し、

前記契約管理サーバから取得した申請データに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記携帯可能電子装置と通信するリーダライタを備える前記ユーザ端末へ送信する、第２プロセッサと、を有する、

リモート発行システム。

[請求項6] 前記データ生成サーバは、

さらに、前記携帯可能電子装置が備えるセキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウエアセキュリティモジュールに接続するインターフェースを有し、

前記第２プロセッサは、前記ハードウエアセキュリティモジュールが保存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項５に記載のリモート発行システム。

[請求項7] 生体認証を行う機能を備える携帯可能電子装置と通信するリーダライタを接続するユーザ端末と通信する通信部と、

前記携帯可能電子装置における生体認証が成功した場合に当該携帯可能電子装置が生成する認証データと契約ＩＤとを含む発行リクエストを前記ユーザ端末から受信し、

前記発行リクエストに含まれる前記認証データと前記契約ＩＤに対応する申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信するプロセッサと、

を有するデータ生成サーバ。

[請求項8] さらに、前記携帯可能電子装置が備えるセキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウエアセキュリティモジュールと接続するインターフェースを有し、

前記プロセッサは、前記ハードウエアセキュリティモジュールが保

存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項７に記載のデータ生成サーバ。

[請求項9] 携帯可能電子装置とデータ生成サーバとを有するリモート発行システムであって、

前記携帯可能電子装置は、

生体情報を取得する生体センサと、

ユーザの生体情報を記憶する記憶領域を含むメモリと、

リーダライタと通信する通信インターフェースと、

前記生体センサにより取得する生体情報と前記メモリに保存する生体情報との照合による生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、前記認証データと当該携帯可能電子装置に固有なＰＵＦデータとを前記リーダライタへ出力し、前記リーダライタから供給される前記認証データに対応する発行データに基づいて発行処理を実行する第１プロセッサと、を有し、

前記データ生成サーバは、

発行処理が可能な携帯可能電子装置のＰＵＦデータを保存するＰＵＦストレージに接続するインターフェースと、

前記携帯可能電子装置が生成した認証データとＰＵＦデータとを含む発行リクエストが入力された場合、前記発行リクエストに含まれるＰＵＦデータが前記ＰＵＦストレージに登録されていれば、前記携帯可能電子装置に対する発行処理に関する申請データと前記認証データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成する第２プロセッサと、を有する、

リモート発行システム。

[請求項10] 前記携帯可能電子装置の前記メモリは、さらに、当該携帯可能電子装置に固有なＰＵＦデータを記憶し、

前記携帯可能電子装置の前記第１プロセッサは、生体認証が成功した場合に前記メモリに記憶された前記ＰＵＦデータを取得する、

請求項９に記載のリモート発行システム。

[請求項11] 前記携帯可能電子装置は、さらに、固有なＰＵＦデータを出力するＰＵＦ回路を有し、　前記携帯可能電子装置の前記第１プロセッサは、生体認証が成功した場合に前記ＰＵＦ回路が出力するＰＵＦデータを取得する、

請求項９に記載のリモート発行システム。

[請求項12] 前記携帯可能電子装置は、前記生体センサ、前記メモリ、前記第１プロセッサおよび前記通信インターフェースを有するモジュールと、前記モジュールを格納する本体と、を備えるＩＣカードである、

請求項９乃至１１のいずれか１項に記載のリモート発行システム。

[請求項13] 前記生体センサは、指紋情報を取得する指紋センサである、

請求項９乃至１２のいずれか１項に記載のリモート発行システム。

[請求項14] 前記携帯可能電子装置の前記通信インターフェースは、ユーザ端末と接続されるリーダライタと通信し、

前記データ生成サーバは、

さらに、前記ユーザ端末と通信する通信部を有し、

前記データ生成サーバの前記第２プロセッサは、前記ユーザ端末から前記携帯可能電子装置が生成した認証データとＰＵＦデータとを含む発行リクエストを受信した場合、前記発行リクエストに含まれるＰＵＦデータが前記ＰＵＦストレージに登録されていれば、前記携帯可能電子装置に対する発行処理に関する申請データと前記認証データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信する、

請求項９乃至１３のいずれか１項に記載のリモート発行システム。

[請求項15] 前記携帯可能電子装置の前記メモリは、さらに、鍵情報を記憶するセキュアメモリを含み、

前記携帯可能電子装置の前記第１プロセッサは、前記セキュアメモリに記憶する鍵情報を用いて前記認証データを生成し、

前記データ生成サーバは、

さらに、前記携帯可能電子装置が備える前記セキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウエアセキュリティモジュールに接続する第２のインターフェースを有し、

前記データ生成サーバの前記第２プロセッサは、前記ハードウエアセキュリティモジュールが保存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項１４に記載のリモート発行システム。

[請求項16] 契約管理サーバとデータ生成サーバとを有するリモート発行システムであって、

前記契約管理サーバは、

ユーザ端末と通信する第１通信部と、

前記第１通信部によりユーザ端末から携帯可能電子装置に対する発行処理を申請する申請データを含む審査リクエストを受信し、前記審査リクエストに応じた審査で前記申請データで申請される発行処理が許可された場合に契約ＩＤを発行する第１プロセッサと、　前記契約ＩＤと前記申請データとを対応づけて保存するデータストレージにアクセスするための第１インターフェースと、と有し、

前記データ生成サーバは、

前記ユーザ端末と通信する第２通信部と、

発行処理が可能な携帯可能電子装置のＰＵＦデータを保存するＰＵＦストレージに接続する第２インターフェースと、

生体認証が成功した携帯可能電子装置が生成する認証データと当該携帯可能電子装置のＰＵＦデータと契約ＩＤとを含む発行リクエストを前記ユーザ端末から受信した場合、前記発行リクエストに含まれ

るＰＵＦデータが前記ＰＵＦストレージに登録されていれば、前記発行リクエストに含まれる契約ＩＤに対応する申請データを前記契約管理サーバから取得し、

前記発行リクエストに含まれる認証データと前記契約管理サーバから取得した申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記携帯可能電子装置と通信するリーダライタを備える前記ユーザ端末へ送信する、第２プロセッサと、を有する、

リモート発行システム。

[請求項17] 前記契約管理サーバは、

前記第１プロセッサは、前記第１通信部によりユーザ端末から携帯可能電子装置に対する発行処理を申請する申請データとＰＵＦデータとを含む審査リクエストを受信し、

前記データストレージには、前記契約ＩＤと前記申請データと前記ＰＵＦデータとを対応づけて保存し、

前記第２プロセッサは、

前記発行リクエストに含まれるＰＵＦデータが前記ＰＵＦストレージに登録されていれば、前記発行リクエストに含まれる契約ＩＤに対応する申請データとＰＵＦデータとを前記契約管理サーバから取得し、

前記発行リクエストに含まれる認証データと前記契約管理サーバから取得したＰＵＦデータと一致すれば、前記発行リクエストに含まれる認証データと前記契約管理サーバから取得した申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成する、

請求項１６に記載のリモート発行システム。

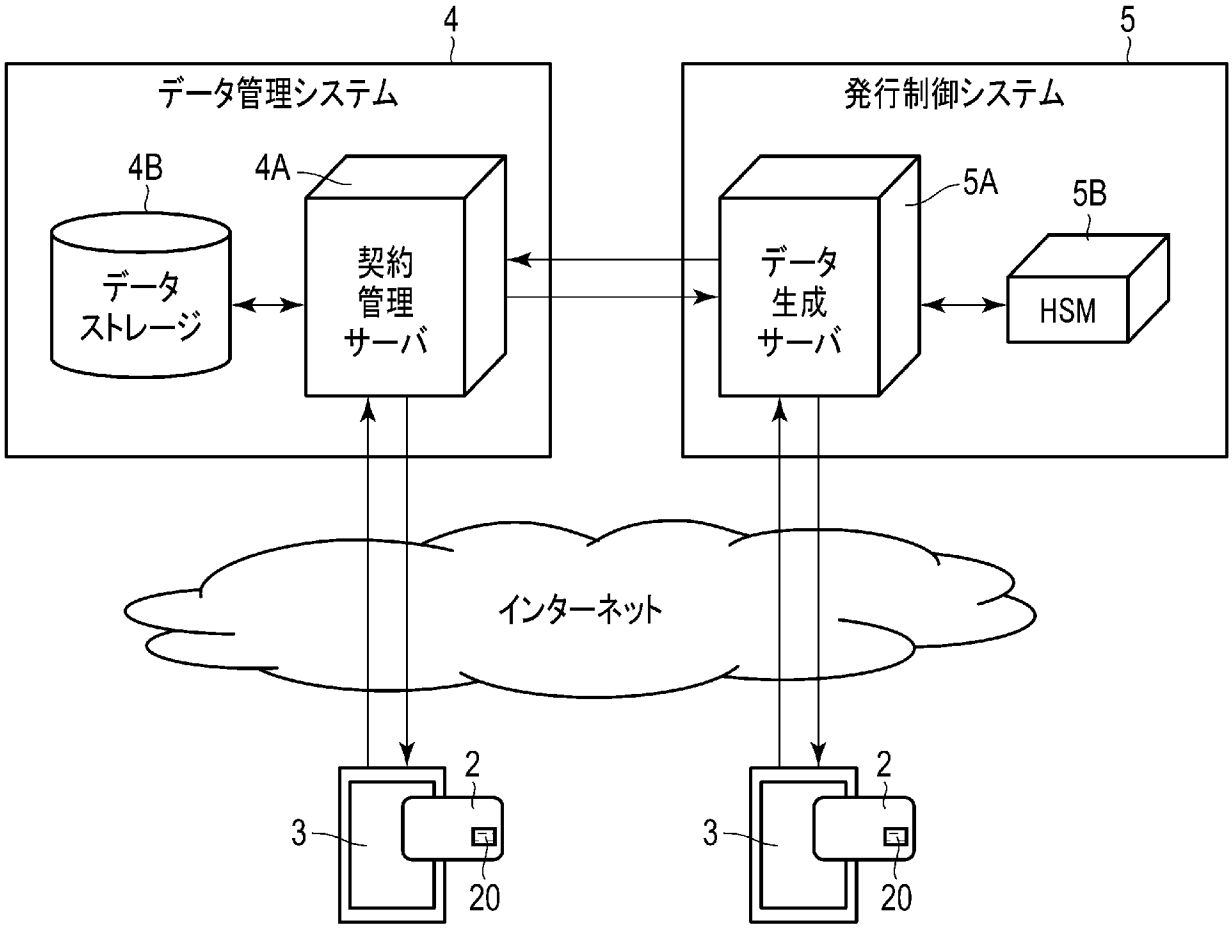
[請求項18] 生体認証を行う機能を備える携帯可能電子装置と通信するリーダライタを接続するユーザ端末と通信する通信部と、

発行処理が可能な携帯可能電子装置のＰＵＦデータを保存するＰＵＦストレージに接続するインターフェースと、

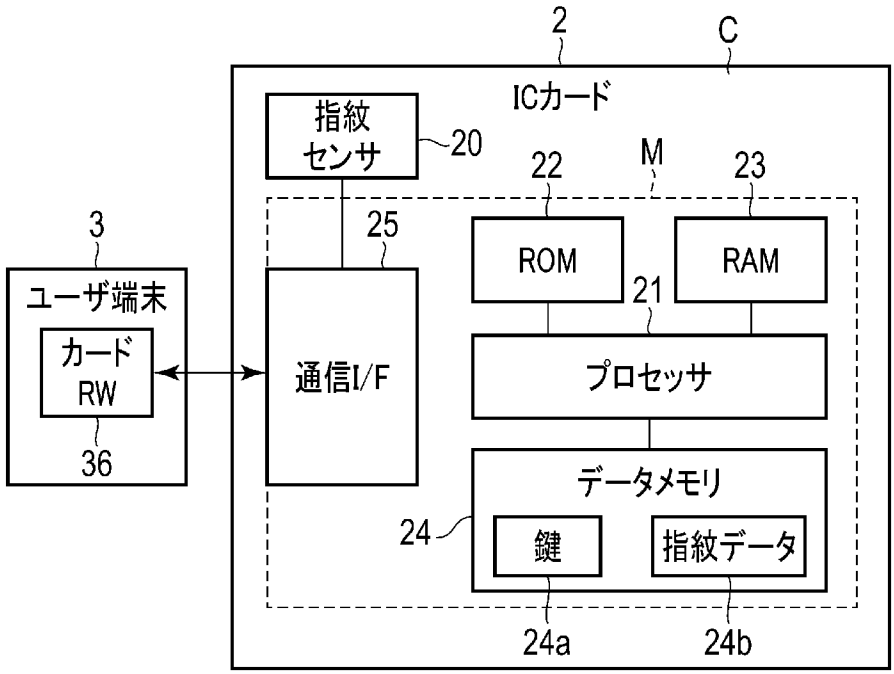
生体認証が成功した携帯可能電子装置が生成する認証データとＰＵＦデータと契約ＩＤとを含む発行リクエストを前記ユーザ端末から受信した場合、前記発行リクエストに含まれるＰＵＦデータが前記ＰＵＦストレージに登録されていれば、前記発行リクエストに含まれる前記認証データと前記契約ＩＤに対応する申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信するプロセッサと、

を有するデータ生成サーバ。

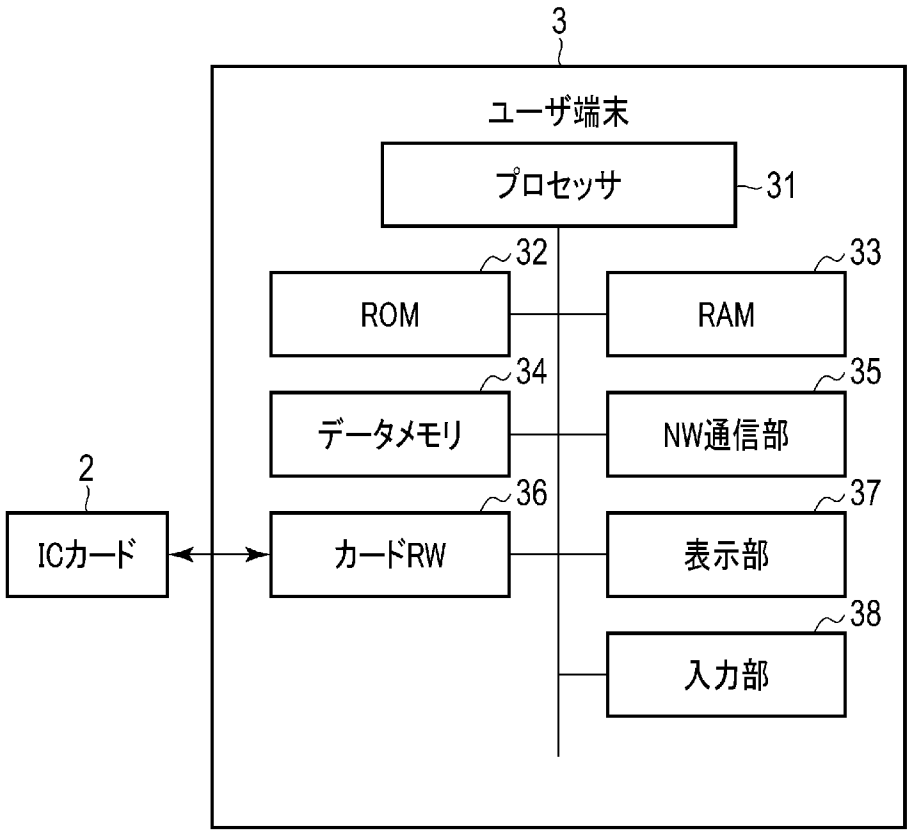
[図1]


4
5
データ管理システム
発行制御システム
4B
4A
5A
5B
データ
ストレージ
契約
管理
サーバ
データ
生成
サーバ
HSM
インターネット
2
3
20
2
3
20

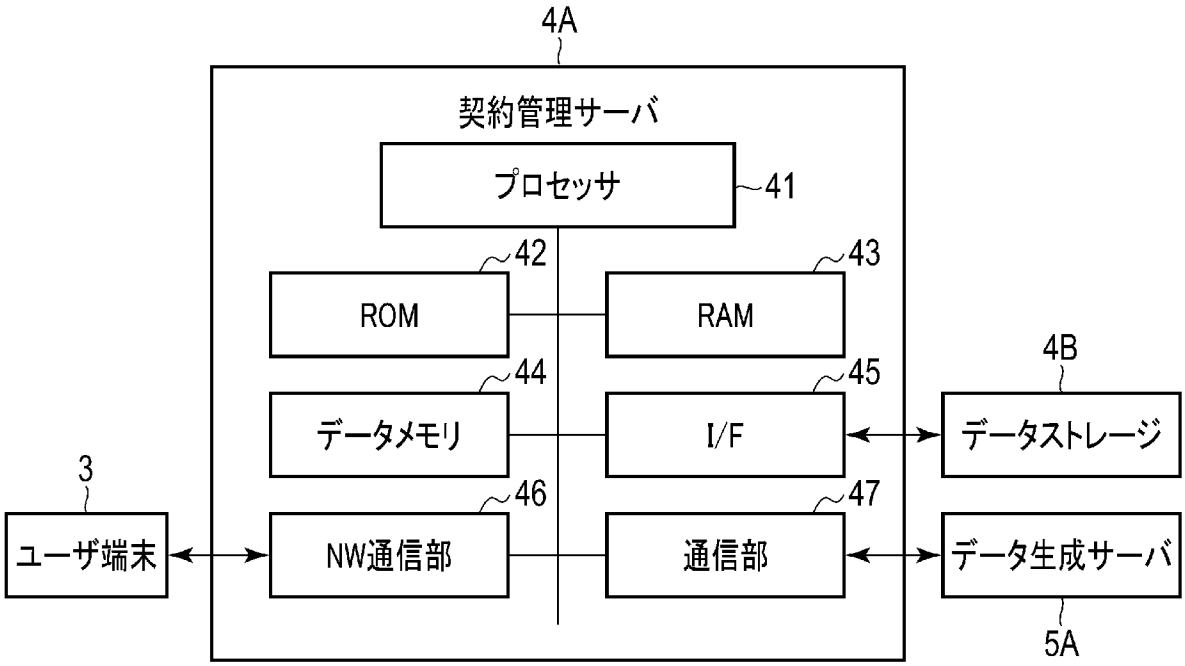
[図2]


2
C
ICカード
指紋
センサ
20
22
M
23
3
25
ROM
RAM
21
ユーザ端末
カード
RW
通信I/F
プロセッサ
データメモリ
24
鍵
指紋データ
36
24a
24b

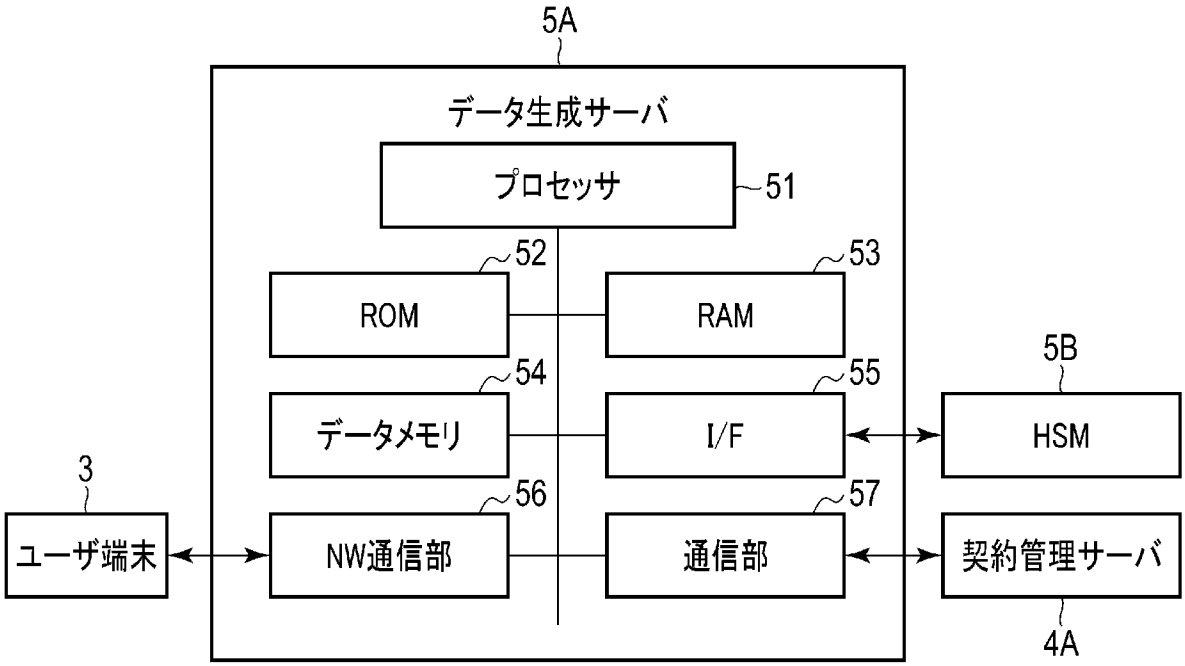
[図3]


3
ユーザ端末
プロセッサ
31
32
33
ROM
RAM
34
35
データメモリ
NW通信部
2
36
37
ICカード
カードRW
表示部
38
入力部

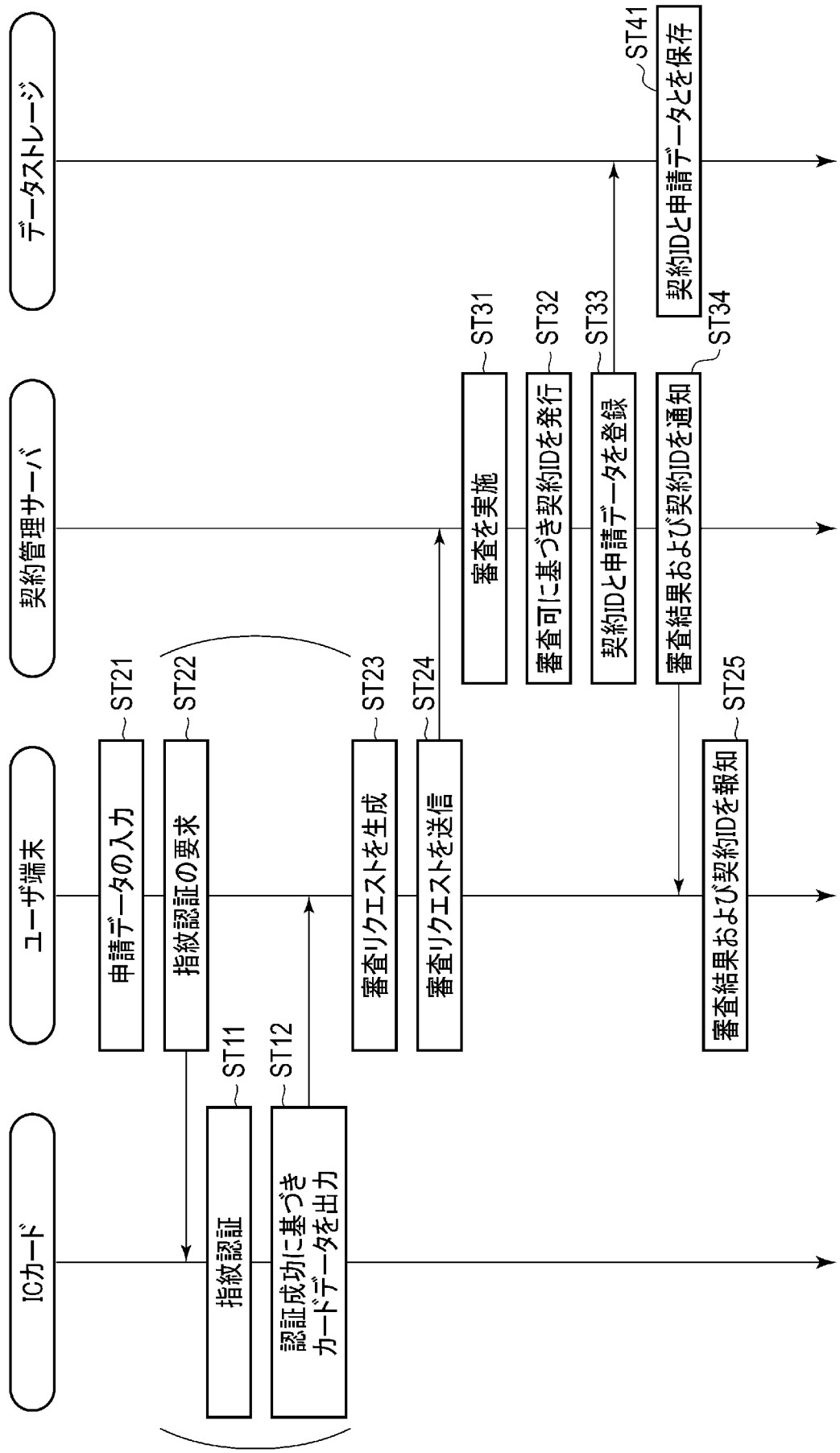
[図4]


4A
契約管理サーバ
プロセッサ
41
42
ROM
43
RAM
44
データメモリ
45
I/F
4B
データストレージ
3
ユーザ端末
46
NW通信部
47
通信部
データ生成サーバ
5A

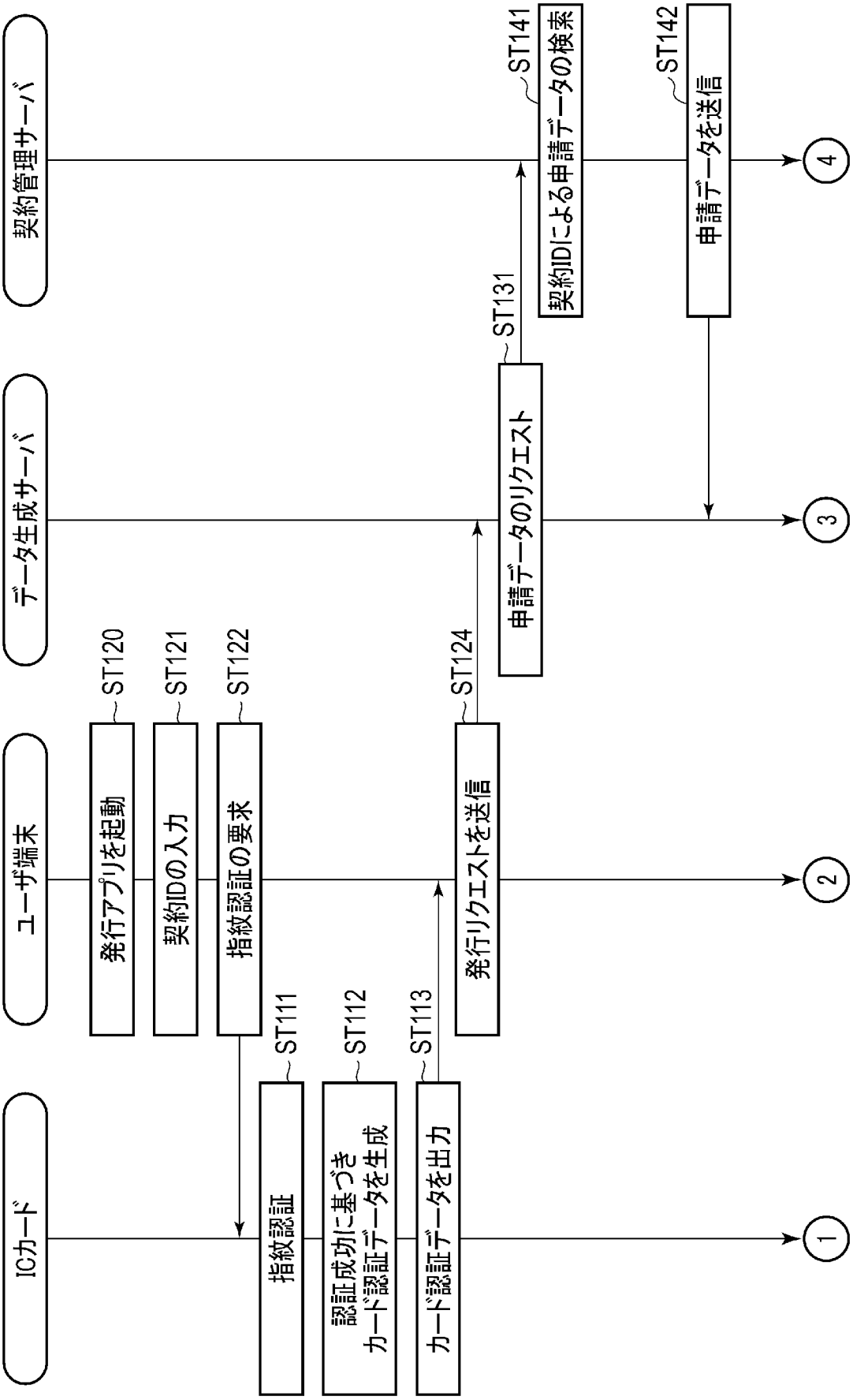
[図5]


5A
データ生成サーバ
プロセッサ
51
52
ROM
53
RAM
54
データメモリ
55
I/F
5B
HSM
3
ユーザ端末
56
NW通信部
57
通信部
契約管理サーバ
4A

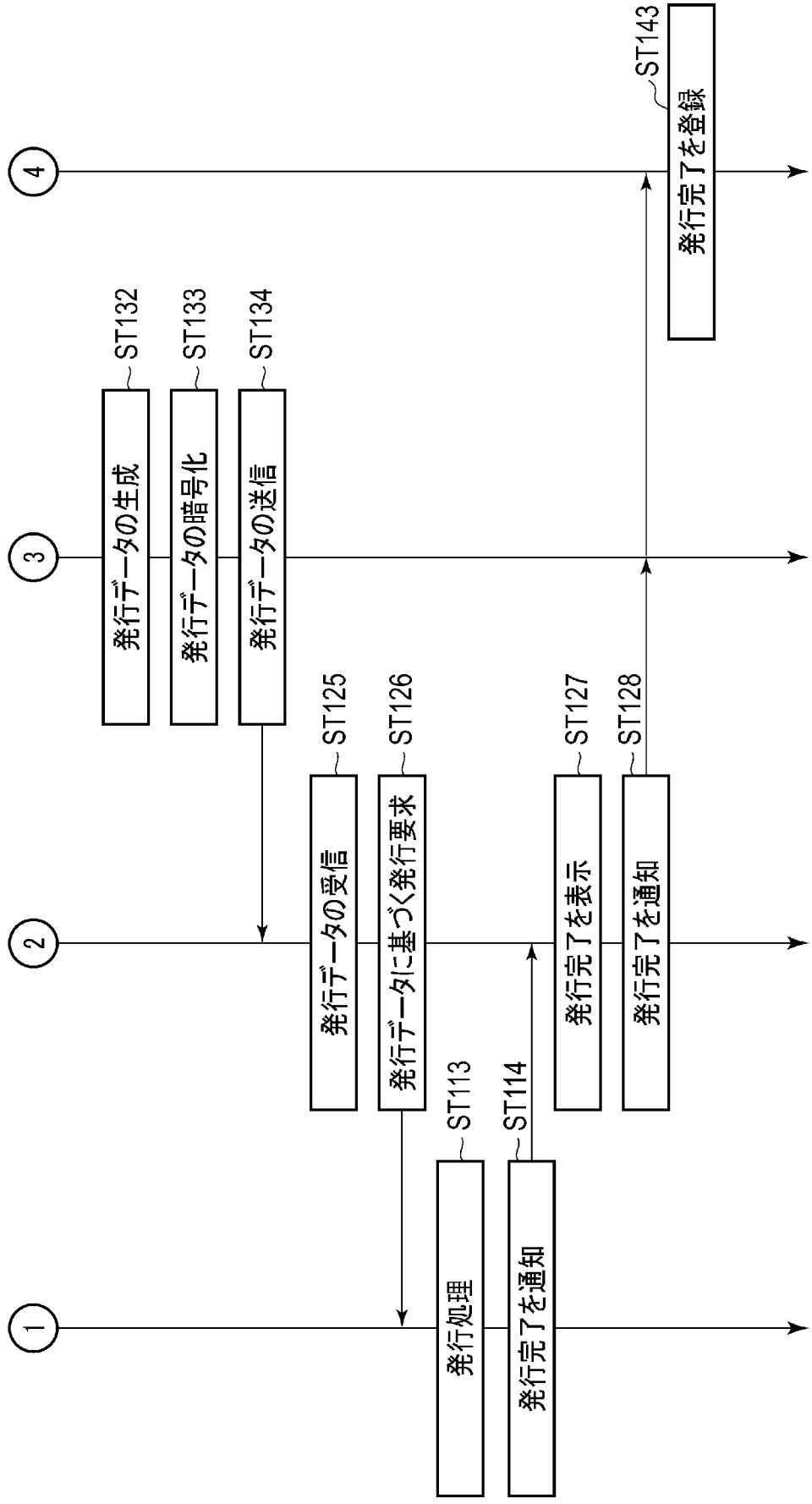
[図6]


ICカード
ユーザ端末
契約管理サーバ
データストレージ
ST11
指紋認証
ST12
認証成功に基づき
カードデータを出力
ST21
申請データの入力
ST22
指紋認証の要求
ST23
審査リクエストを生成
ST24
審査リクエストを送信
ST31
審査を実施
ST32
審査可に基づき契約IDを発行
ST33
契約IDと申請データを登録
ST34
審査結果および契約IDを通知
ST25
審査結果および契約IDを報知
ST41
契約IDと申請データとを保存

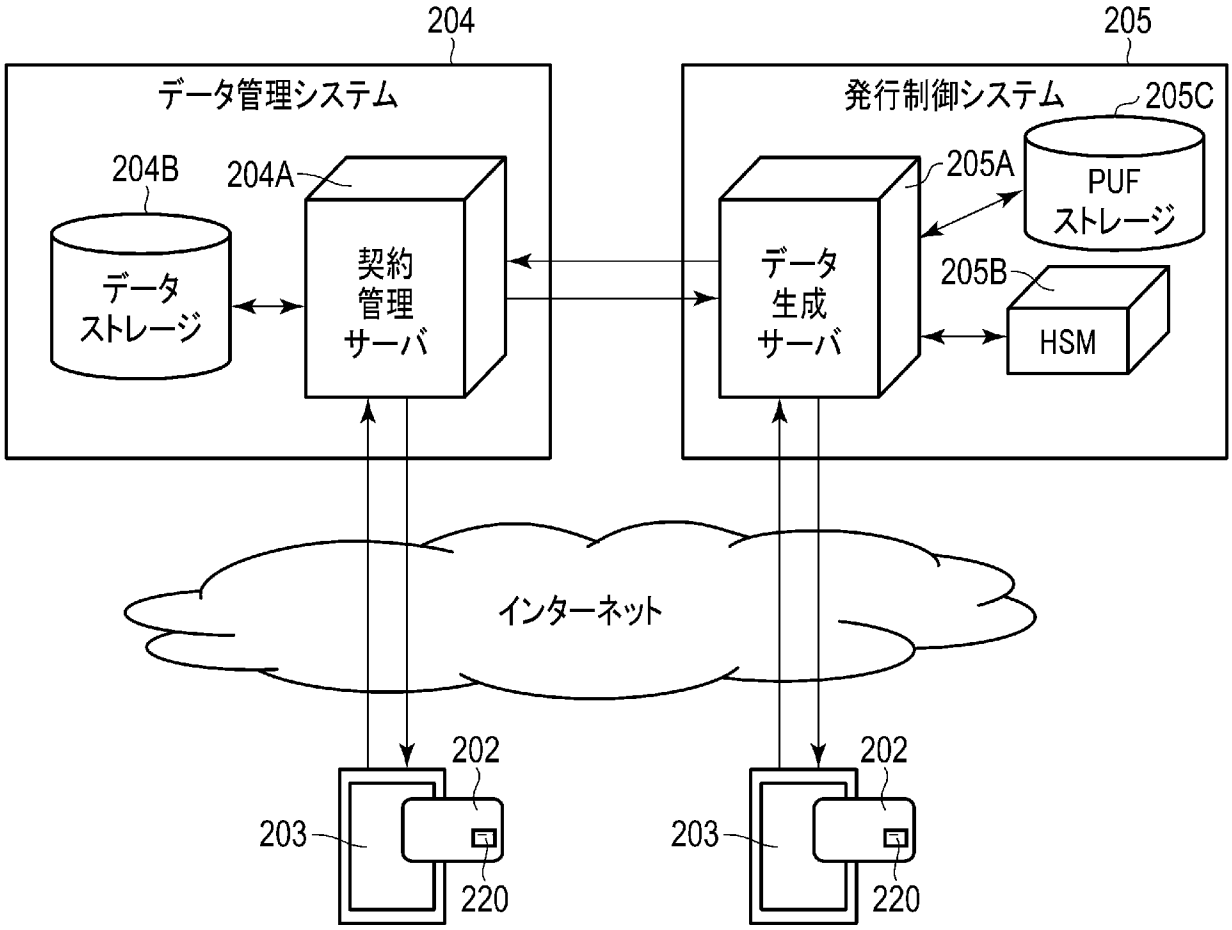
[図7]


契約管理サーバ
データ生成サーバ
ユーザ端末
ICカード
ST120
発行アプリを起動
ST121
契約IDの入力
ST122
指紋認証の要求
ST111
指紋認証
ST112
認証成功に基づき
カード認証データを生成
ST113
カード認証データを出力
ST124
発行リクエストを送信
申請データのリクエスト
ST131
ST141
契約IDによる申請データの検索
ST142
申請データを送信
1
2
3
4

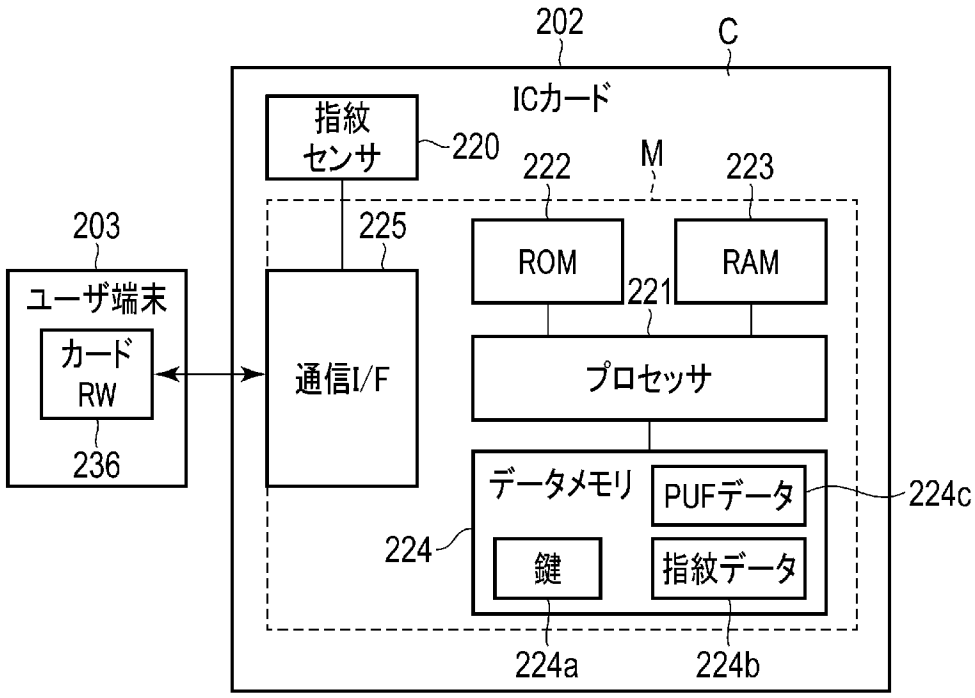
[図8]


ST143
発行完了を登録
4
ST132
ST133
ST134
発行データの生成
発行データの暗号化
発行データの送信
3
ST125
ST126
ST127
ST128
発行データの受信
発行データに基づく発行要求
発行完了を表示
発行完了を通知
2
ST113
ST114
発行処理
発行完了を通知
1

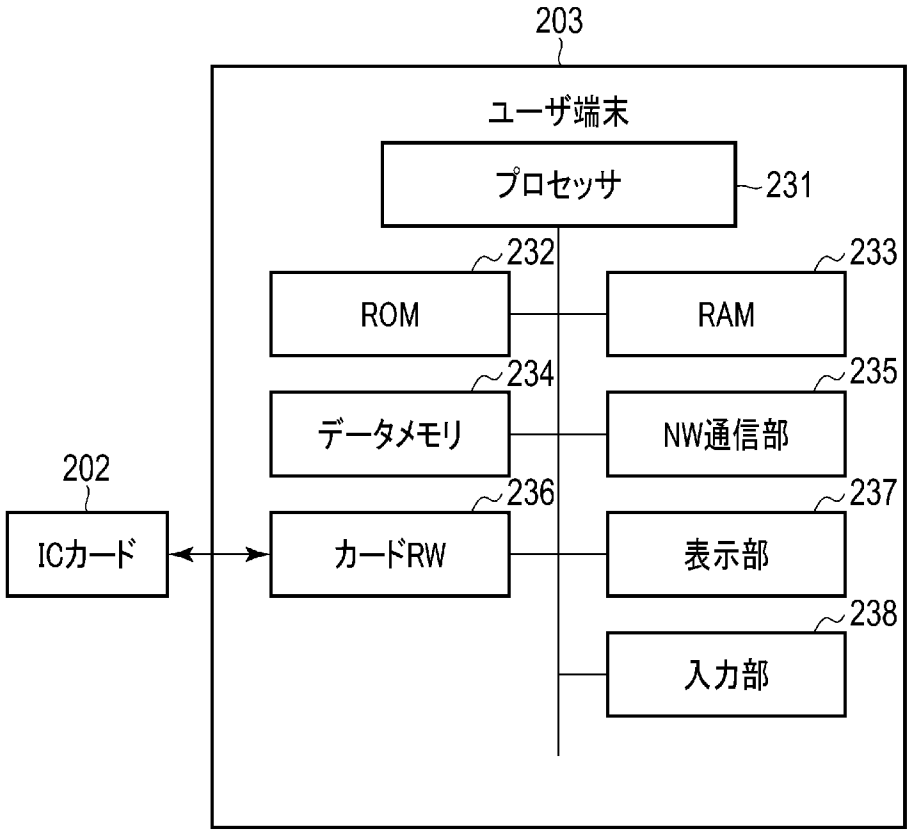
[図9]


204
データ管理システム
204B
204A
データ
ストレージ
契約
管理
サーバ
205
発行制御システム
205C
205A
PUF
ストレージ
データ
生成
サーバ
205B
HSM
インターネット
202
203
220
202
203
220

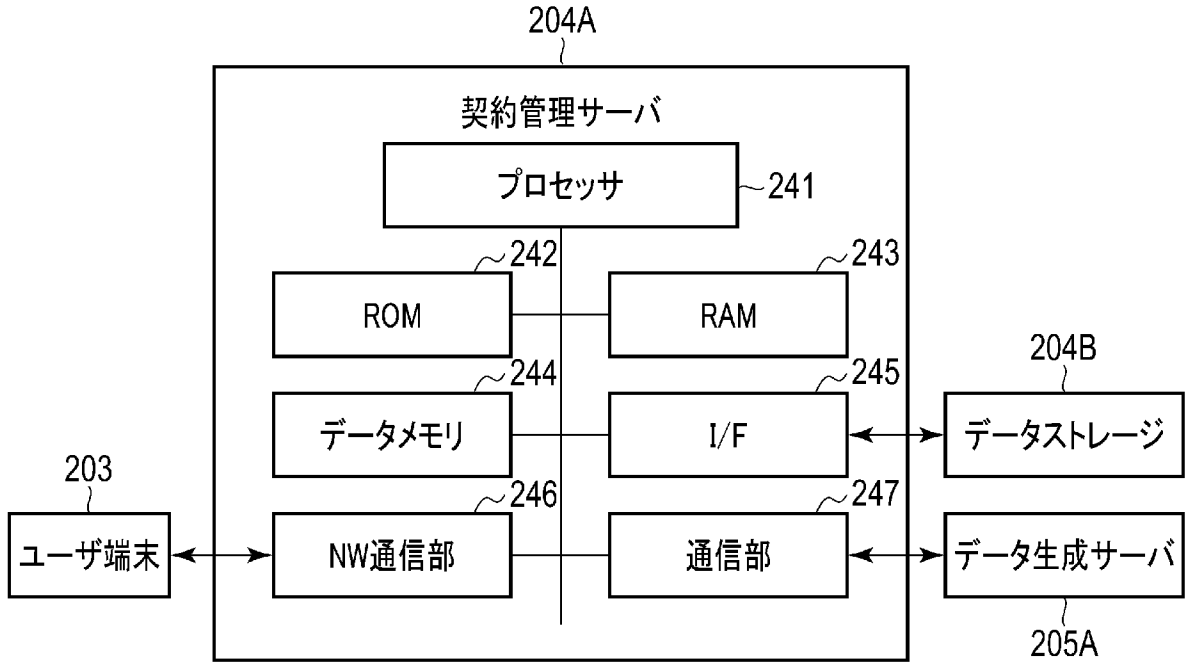
[図10]


202
C
ICカード
指紋
センサ
220
222
M
223
203
225
ROM
RAM
ユーザ端末
221
カード
RW
通信I/F
プロセッサ
データメモリ
PUFデータ
224c
224
鍵
指紋データ
236
224a
224b

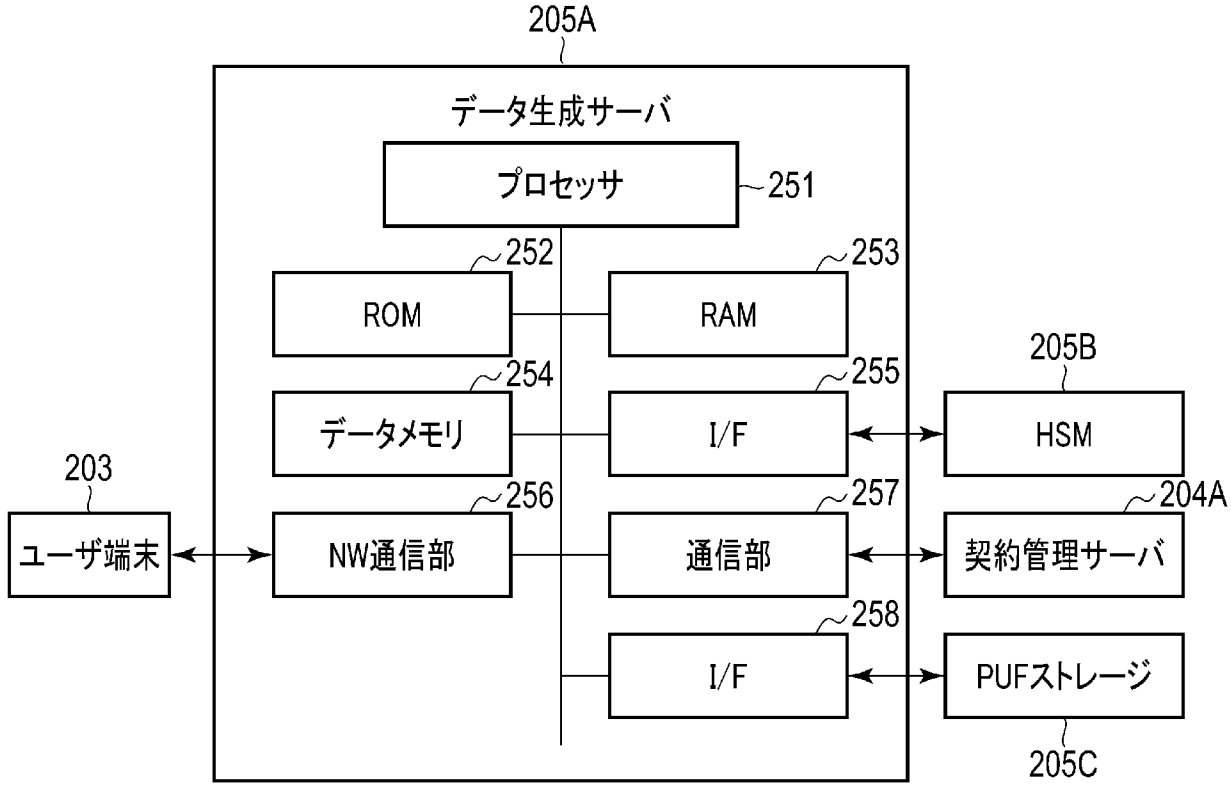
[図11]


203
ユーザ端末
プロセッサ
231
232
233
ROM
RAM
234
235
データメモリ
NW通信部
202
236
237
ICカード
カードRW
表示部
238
入力部

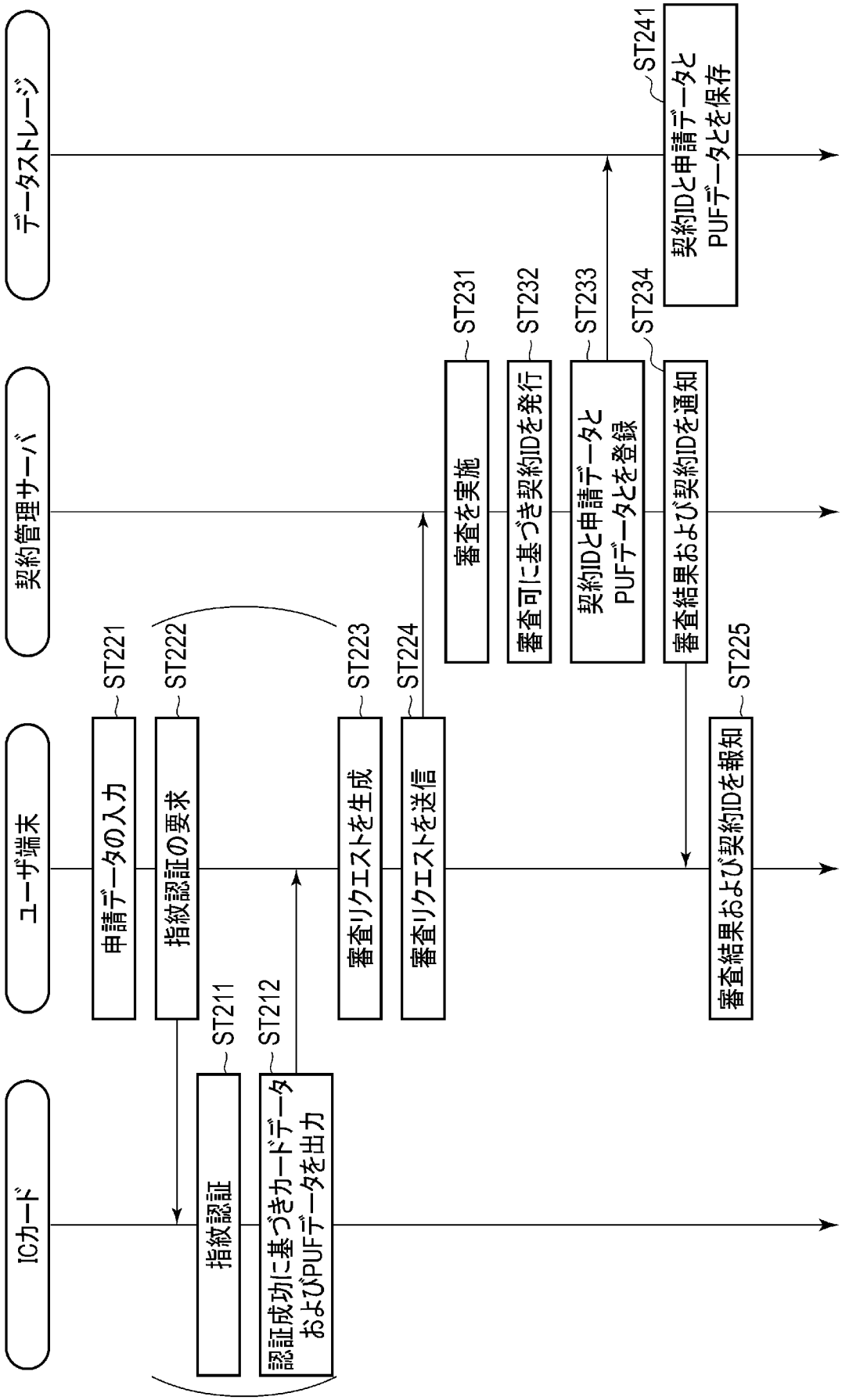
[図12]


204A
契約管理サーバ
プロセッサ
241
242
ROM
243
RAM
244
データメモリ
245
I/F
204B
データストレージ
203
ユーザ端末
246
NW通信部
247
通信部
データ生成サーバ
205A

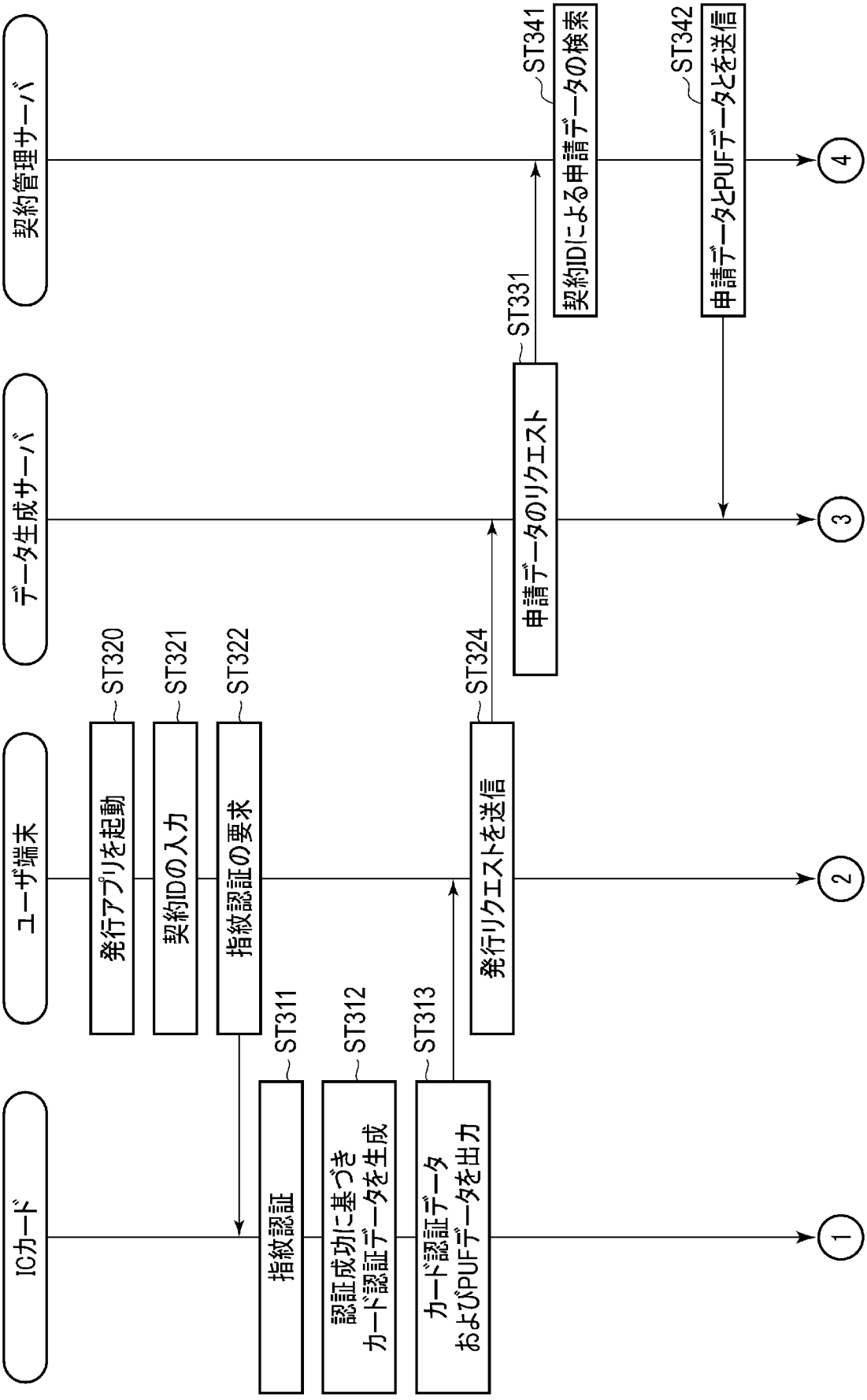
[図13]


205A
データ生成サーバ
プロセッサ
251
252
ROM
253
RAM
254
データメモリ
255
I/F
205B
HSM
203
ユーザ端末
256
NW通信部
257
通信部
204A
契約管理サーバ
258
I/F
PUFストレージ
205C

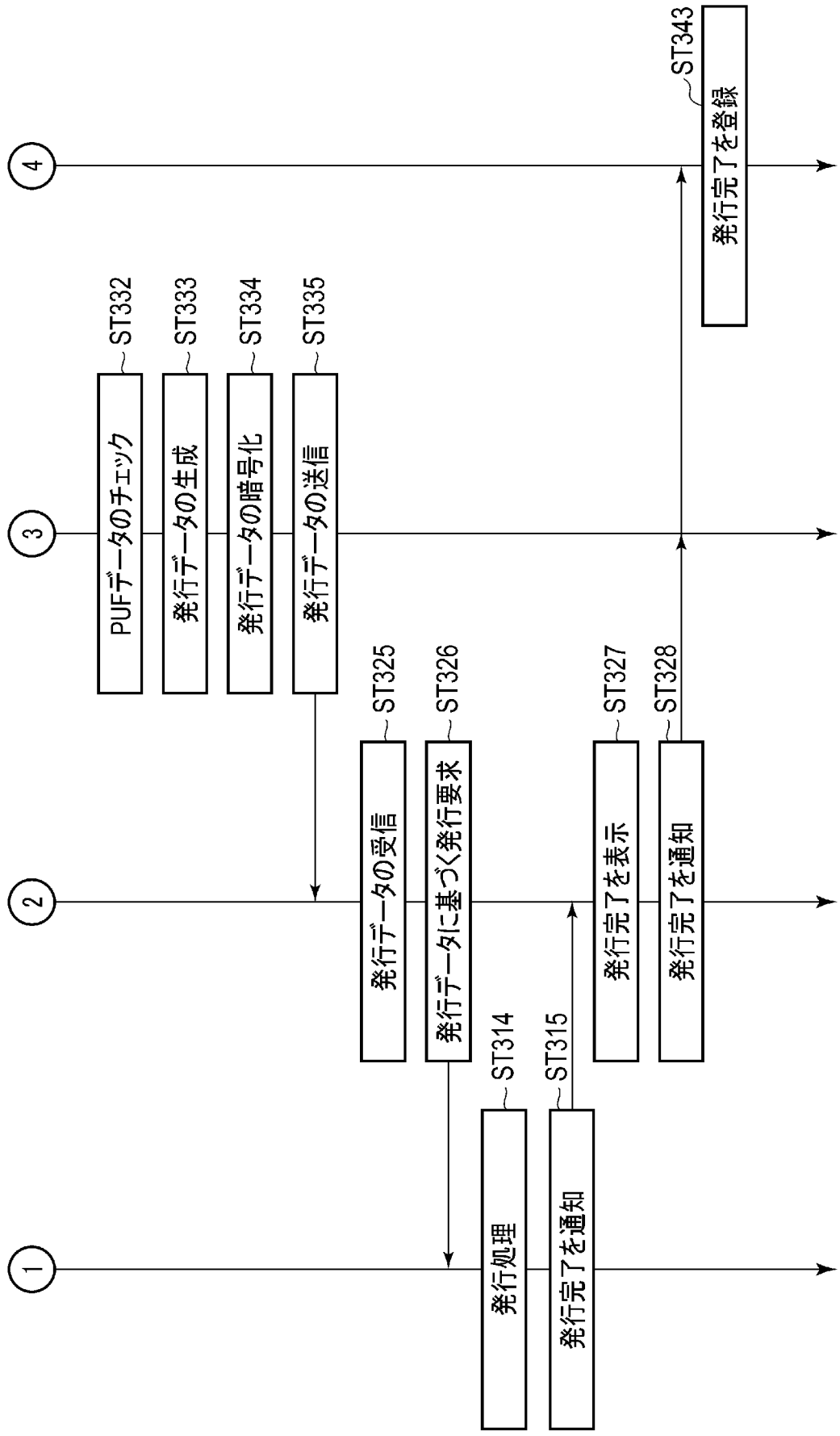
[図14]


ICカード
ユーザ端末
契約管理サーバ
データストレージ
ST211
指紋認証
ST212
認証成功に基づきカードデータおよびPUFデータを出力
ST221
申請データの入力
ST222
指紋認証の要求
ST223
審査リクエストを生成
ST224
審査リクエストを送信
ST231
審査を実施
ST232
審査可に基づき契約IDを発行
ST233
契約IDと申請データとPUFデータとを登録
ST234
審査結果および契約IDを通知
ST225
審査結果および契約IDを報知
ST241
契約IDと申請データとPUFデータとを保存

[図15]


ICカード
ユーザ端末
データ生成サーバ
契約管理サーバ
ST320
発行アプリを起動
ST321
契約IDの入力
ST322
指紋認証の要求
ST311
指紋認証
ST312
認証成功に基づき
カード認証データを生成
ST313
カード認証データ
およびPUFデータを出力
ST324
発行リクエストを送信
ST331
申請データのリクエスト
ST341
契約IDによる申請データの検索
ST342
申請データとPUFデータと送信
1
2
3
4

[図16]


1
2
3
4
PUFデータのチェック
発行データの生成
発行データの暗号化
発行データの送信
発行データの受信
発行データに基づく発行要求
発行処理
発行完了を通知
発行完了を表示
発行完了を通知
発行完了を登録
ST332
ST333
ST334
ST335
ST325
ST326
ST314
ST315
ST327
ST328
ST343

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/004002

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/34(2012.01)i; ***G06F 21/32***(2013.01)i; ***G06F 21/44***(2013.01)i; ***G06F 21/60***(2013.01)i; ***H04L 9/10***(2006.01)i; ***H04L 9/32***(2006.01)i
FI: G06Q20/34 300; G06F21/32; G06F21/44; G06F21/60 360; H04L9/10 Z; H04L9/32 100D

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)

G06Q20/34; G06F21/32; G06F21/44; G06F21/60; H04L9/10; H04L9/32

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2022
Registered utility model specifications of Japan 1996-2022
Published registered utility model applications of Japan 1994-2022

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.
A	JP 2018-5271 A (TOSHIBA CORP.) 11 January 2018 (2018-01-11) entire text, all drawings	1-18
A	JP 2007-128468 A (DAINIPPON PRINTING CO., LTD.) 24 May 2007 (2007-05-24) entire text, all drawings	1-18
A	JP 2019-200683 A (TOSHIBA CORP.) 21 November 2019 (2019-11-21) entire text, all drawings	1-18

☐ 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
"E" earlier application or patent but published on or after the international filing date
"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)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 May 2022	**17 May 2022**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/004002

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2018-5271 A	11 January 2018	US 2017/0374066 A1	
		EP 3264717 A1	
JP 2007-128468 A	24 May 2007	(Family: none)	
JP 2019-200683 A	21 November 2019	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2022/004002

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06Q 20/34(2012.01)i; G06F 21/32(2013.01)i; G06F 21/44(2013.01)i; G06F 21/60(2013.01)i; H04L 9/10(2006.01)i; H04L 9/32(2006.01)i
FI: G06Q20/34 300; G06F21/32; G06F21/44; G06F21/60 360; H04L9/10 Z; H04L9/32 100D

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））

G06Q20/34; G06F21/32; G06F21/44; G06F21/60; H04L9/10; H04L9/32

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	１９７１－２０２２年
日本国実用新案登録公報	１９９６－２０２２年
日本国登録実用新案公報	１９９４－２０２２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	関連する請求項の番号
A	JP 2018-5271 A (株式会社東芝) 11.01.2018 (2018-01-11) 全文，全図	1-18
A	JP 2007-128468 A (大日本印刷株式会社) 24.05.2007 (2007-05-24) 全文，全図	1-18
A	JP 2019-200683 A (株式会社東芝) 21.11.2019 (2019-11-21) 全文，全図	1-18

☐ 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抵触するものではなく、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	国際調査報告の発送日
02.05.2022	17.05.2022

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
田中　秀樹 5R 3246
電話番号 03-3581-1101 内線 3502

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/004002

引用文献	公表日	パテントファミリー文献	公表日
JP 2018-5271 A	11.01.2018	US 2017/0374066 A1	
		EP 3264717 A1	
JP 2007-128468 A	24.05.2007	（ファミリーなし）	
JP 2019-200683 A	21.11.2019	（ファミリーなし）	