

(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
2019年5月9日(09.05.2019)



(10) 国際公開番号

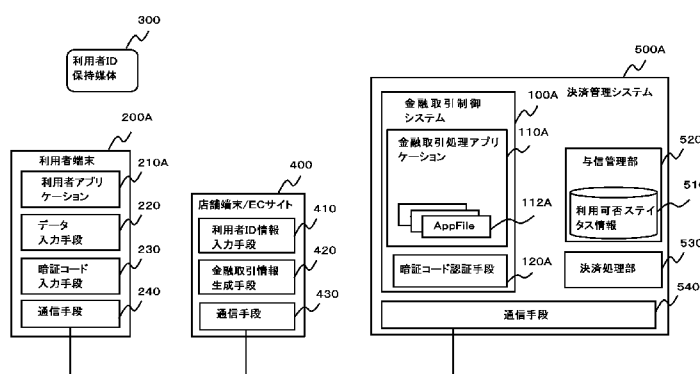
WO 2019/087416 A1

- (51) 国際特許分類:
G06Q 20/34 (2012.01)
- (21) 国際出願番号: PCT/JP2018/004317
- (22) 国際出願日: 2018年2月8日(08.02.2018)
- (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/JP2017/039703 2017年11月2日(02.11.2017) JP
- (71) 出願人: 株式会社 L E I S (LEIS CO.LTD.)
[JP/JP]; 〒6580032 兵庫県神戸市東灘区向洋町中6丁目9番地 神戸ファッションマート10階 Hyogo (JP).
- (72) 発明者: 松 永 力 (MATSUNAGA Chikara);
〒6580032 兵庫県神戸市東灘区向洋町中6丁目9番地 神戸ファッションマート10階 Hyogo (JP).
- (74) 代理人: 永井 道彰(NAGAI,Michiaki); 〒6500044
兵庫県神戸市中央区東川崎町1丁目8番4号 神戸市産業振興センター8階 Hyogo (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, JO, JP, 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,

(54) Title: FINANCIAL TRANSACTION CONTROL SYSTEM, APPLICATION THEREFOR, AND FINANCIAL TRANSACTION CONTROL METHOD

(54) 発明の名称: 金融取引制御システムおよびそのアプリケーションおよび金融取引制御方法

[図1]



- 100A Financial transaction control system
110A Financial transaction processing application
112A Application file
120A Passcode authentication means
200A User terminal
210A User application
220 Data input means
230 Passcode input means
240, 430, 540 Communication means
300 User ID holding medium
400 Store terminal/e-commerce site
410 User ID information input means
420 Financial transaction information generation means
500A Payment management system
510 Availability status information
520 Credit management unit
530 Payment processing unit

(57) Abstract: [Problem] To provide a financial transaction control system that makes it possible to prevent unauthorized use via skimming or identity fraud by a third party in financial transactions such as use of credit and use of debit. [Solution] A financial transaction control system in which an open passcode and a close passcode are set and registered in a financial transaction processing application file generated for each user account. Authentication of an open passcode transmitted by a user terminal is required in processing for opening a financial transaction processing application file, and when financial

[続葉有]

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, 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))

transaction information is subsequently received from a financial transactor and editing processing for editing the financial transaction information in the financial transaction processing application file is performed, an approval request regarding the financial transaction information is transmitted to the user terminal, the financial transaction control system waits for a reply including approval information, and after authentication of a close passcode included in the approval information included in the reply, processing for handing over financial transaction processing data to a payment management system and processing for closing the financial transaction processing application file are performed.

(57) 要約：【課題】 クレジット利用、デビット利用などの金融取引において、第三者の成り済まし使用やスキミングによる不正使用の防止ができる金融取引制御システムを提供する。【解決手段】 利用者のアカウントごとに生成された金融取引処理アプリケーションファイルにオープン暗証コードとクローズ暗証コードを設定登録しておく。金融取引処理アプリケーションファイルのオープン処理には利用者端末より送信されたオープン暗証コードの認証を必要とし、その後、金融取引者からの金融取引情報を受けて金融取引処理アプリケーションファイルに金融取引情報を書き込む編集処理をすれば、利用者端末に対して金融取引情報に対する承認リクエストを送信して承認情報の返信を待ち、返信された承認情報に含まれているクローズ暗証コードの認証後、金融取引処理データの決済管理システムへの引き渡し処理と、金融取引処理アプリケーションファイルのクローズ処理を実行する。

明 細 書

発明の名称：

金融取引制御システムおよびそのアプリケーションおよび金融取引制御方法

技術分野

[0001] 本発明は、クレジット利用、デビット利用を伴う金融取引における不正防止の技術分野に属する。

背景技術

[0002] クレジットカード、キャッシュカード等を利用した金融取引は高い利便性から広く普及している。近年は電子決済システムが普及しつつあり、スマートフォンなどに取り込んだクレジット機能アプリケーションやデビット機能アプリケーションを用いた電子決済も増えてきた。

クレジット機能、デビット機能を利用した金融取引は便利であり、今後ますます普及が見込まれるが、その一方で不正使用に伴う問題もある。カード類を紛失したり盗難にあったりした場合、不正使用されるおそれがある。また、スキミング被害に合う恐れもある。

クレジットカードやキャッシュカードの不正使用を防止するため、従来から様々な対策が採られている。

[0003] クレジットカードの本人認証手段の１つとして本人のサインがある。

伝統的な方法であるが、クレジットカード裏面のサイン欄に記入されている本人サインと、利用伝票にその場で利用者が記入した利用者サインを店員がその場で照合することで行われる。

他のクレジットカードの本人認証手段として暗証番号がある。クレジットカードがＩＣチップ搭載しているＩＣカードである場合、ＩＣカードの記録情報として暗証コードを記憶させておき、上記のサインに代えてまたはサインと併用され、暗証番号が利用されることがある。例えば、店頭設置のクレジットカード決済端末にＰＩＮパッドが接続されており、ＰＩＮパッドを介

して利用者から入力された暗証番号と、そのＩＣチップのメモリに記憶されている暗証番号を照合することで認証処理が行われる。

[0004] 他のクレジットカードの本人認証手段として顔画像確認がある。

クレジットカードに顔写真が貼付されているものは従来から存在するが、例えば、図２５に示すように、特開平１０－２１７６５５号公報には、特殊印刷技術により、平面のプラスチック製のクレジットカードに対して、立体的な視認が可能な疑似３次元顔写真が印刷できる技術も紹介されている。

[0005] 他のクレジットカードの本人認証手段として生体情報による認証がある。

クレジットカードがＩＣチップ搭載しているＩＣカードである場合、ＩＣカードの記録情報として生体情報を記憶させておき、例えば、店頭設置のクレジットカード決済端末に生体情報入力装置が接続されており、生体情報入力装置を介して利用者から入力された生体情報と、そのＩＣチップのメモリに記憶されている生体情報を照合することで行われる。

[0006] 例えば、図２６に示すように、特開２０１２－７３９０２号公報には、クレジットカードなどのＩＤカードのＩＣチップの記憶領域に生体情報を登録しておき、店頭設置のクレジットカード決済端末に生体情報取得用のデバイスが接続されており、デバイスを介して利用者から入力された生体情報と、そのＩＣチップのメモリに記憶されている生体情報を照合することで認証処理が行われる。

[0007] また、例えば、図２７に示すように、特表２０１４－５１２５７９号公報には、生体情報を利用する特殊なＩＣカードタイプのクレジットカードが開示されている。クレジットカードの一部に指紋受容器と呼ばれる特殊なデバイスが設けられており、利用者がその指紋受容器に親指を接触させてクレジットカードを持ち、親指を指紋受容器に接触させて把持したまま、クレジットカード決済端末のカードリーダを通すことにより、クレジットカードのＩＣチップとクレジットカード決済端末とのデータ伝送ができるというものである。

[0008] 特許文献１：特開平１０－２１７６５５号公報

特許文献2：特開 2012-73902 号公報

特許文献3：特表 2014-512579 号公報

発明の開示

発明が解決しようとする課題

[0009] しかしながら、上記した本人認証処理にはそれぞれ問題があった。

クレジットカードの本人認証手段として本人のサインを用いる場合、セキュリティレベルが低い点が問題である。つまり、サインは偽書が可能な場合があり得る。重要な契約書などで書くサインは広いスペースが確保されており、書いたサインはそれなりに個性づけられており、契約社会の現在でもある程度有効性が担保されている。しかし、クレジットカードのサイン欄は小さく、簡略化したサインを使用することも多い。また、店頭のスタッフはかならずしもサイン認証に長けた者ばかりでなく、実質、サインの照合が簡略化されてしまうことも多い。

[0010] 次に、クレジットカードの本人認証手段として暗証番号を用いる場合も、セキュリティレベルが低い点が問題である。暗証番号は使用実態として4桁の番号に過ぎず、類推される場合もあり得るし、ある金融取引での決済端末入力時に第三者に流出してしまい、その後クレジットカードが不正使用される恐れがある。

次に、クレジットカードの本人認証手段として顔画像を用いる場合、セキュリティレベルが十分ではない点が問題である。顔画像は貼り換えられる可能性もあり得るし、本人と年恰好がある程度近い人物であれば店員が気付かずに本人として取り扱う恐れもある。特に女性は化粧によってだいぶ変わり得るため成り済ましが起こり得る。

次に、クレジットカードの本人認証手段として生体情報を用いる場合、セキュリティレベルは比較的高く担保されているが、生体情報を読み取るデバイスの装備が問題となる。クレジットカードは極めて広く普及しているため、クレジットカード決済端末の数は相当数に上る。ほとんどのクレジットカード決済端末はそのような生体情報の読み取りデバイスを装備していないた

め、現実問題としてクレジットカード決済端末に生体情報の読み取りデバイスを装備させることは難しいと言わざるを得ない。

[0011] 特表2014-512579号公報に開示された技術によれば、指紋受容器と呼ばれる特殊なデバイスはクレジットカード側に設けられるので、クレジットカード側の装備変更で済むと言える。しかし、親指を指紋受容器に接触させて把持したままクレジットカード決済端末のカードリーダを通すという使用条件が生じてしまう。つまり、これはカード利用者自身がクレジットカード決済端末を操作することを意味するが、店舗での使用状況は大半のケースにおいて、クレジットカード決済端末がカウンター内に設置されており、クレジットカードを利用者から手渡された店員がクレジットカード決済端末にクレジットカードを通して操作することがルーチン化されており、利用者自らがクレジットカード決済端末を使用することは店頭での混乱を招く。特表2014-512579号公報に開示された技術は、実際にはキャッシュカードを用いたATM操作などが想定されており、利用者自身が端末を操作する場合に限られる。

[0012] 上記のように、クレジットカードの利用について様々なセキュリティレベルの本人認証処理が試行されているが、いずれも問題があり、クレジットカードの不正使用の問題を解決するには至っていない。

ここで、利用者がクレジットカードやキャッシュカードの紛失や不正使用に気付いた場合、クレジットカードやキャッシュカードを無効化して被害を抑制する必要があった。

[0013] 例えば、紛失や盗難に気付いたカードの利用者からカード運営会社またはカード管理受託会社に対して、紛失・盗難にあったクレジットカードやキャッシュカードを無効にしたい旨の通知を電話やウェブサイトを通じて通知する必要があった。通知を受けたカード運営会社自身またはカード管理受託会社が、カード会社の管理ホストコンピュータにおいて該当するクレジットカードやキャッシュカードの停止登録を行って対応することとなる。クレジットカードやキャッシュカードが無効化されると、例えば、クレジットカード

決済端末を介してカード会社の管理ホストコンピュータに対して、該当するカードＩＤ番号を含むカードの利用要求の金融取引データが送信されてきても金融取引の認証をせず、利用不可の取り扱いとしていた。

[0014] クレジットカードの利用停止及び再発行サービスは、カード会員がクレジットカードの紛失或いは不正使用に気付いて利用停止手続きを行うことによって初めて無効化できるものであり、時間が掛かっていた。また、一旦クレジットカードを利用停止すると再発行に時間と手間が掛かり、その間、カード会員はクレジットカードを利用できなくなるという問題がある。

[0015] さらに、多数のクレジットカードを所持しているが、日常的には、それらの内、一部しか利用していない場合、利用していないクレジットカードの紛失或いは不正使用に気が付き難いという問題がある。

現在は、クレジットカード、キャッシュカードは正しく使用されることが大前提となっており、紛失や盗難にあった場合はイレギュラーの事故状態と捉える運用である。この運用である限り、紛失や盗難にあった場合にクレジットカードやキャッシュカードの利用停止手続きが申請され、実際に利用停止処理が完了するまでクレジットカード、キャッシュカードは使用され得る状態に置かれてしまい、幾ばくかの被害が発生してしまう。

[0016] 上記問題点に鑑み、本発明は、クレジット利用、デビット利用などの金融取引において、確実に、第三者の成り済まし使用やスキミングによる不正使用の防止ができる金融取引制御システム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

[0017] 本発明者は、クレジットカード、キャッシュカードの不正使用の問題の解決に向けて、不正使用の防止を管理するアプリケーションおよびアプリケーションファイルの利用を思いついた。

本発明の金融取引制御システムは、利用者のアカウントごとに生成された金融取引処理アプリケーションファイルと、利用者のアカウントに対する金融取引処理を制御する金融取引処理アプリケーションを備えた構成とし、金融取引処理アプリケーションファイルに、オープン処理に対するオープン暗

証コードとクローズ処理に対するクローズ暗証コードが設定登録されており、金融取引処理アプリケーションが、利用者端末から金融取引処理リクエスト情報を受け、当該利用者のアカウントに対する金融取引処理アプリケーションファイルを開く“オープン処理”と、金融取引者から利用者のアカウントへの金融取引情報を受けて、金融取引処理アプリケーションファイルに金融取引情報を書き込む“編集処理”と、利用者端末に対して金融取引情報を承認するか否かを問う承認リクエストを送信し、利用者端末からの承認情報の返信を待つ“承認伺い処理”と、利用者端末からの承認情報の返信を条件として、金融取引処理アプリケーションファイルデータの決済管理システムへの“引き渡し処理”と、金融取引処理アプリケーションファイルの“クローズ処理”を実行することを特徴とするものである。

[0018] このように、本発明の金融取引制御システムは、利用者のアカウントに対応した金融取引処理アプリケーションファイルを用い、当該ファイルを正常に開くオープン処理と、当該ファイルを正常終了するためのクローズ処理にそれぞれ暗証コードが設定されており、オープン暗証コードの照合によって金融取引処理アプリケーションファイルを開く“オープン処理”と、金融取引処理アプリケーションファイルに金融取引情報を書き込む“編集処理”までを行い、その後、利用者端末からの承認情報の返信を待つ“承認伺い処理”を入れることにより、利用者による使用状況の把握、承認を促し、クローズ暗証コードの照合を経て、金融取引処理アプリケーションファイルデータの決済管理システムへの“引き渡し処理”と、金融取引処理アプリケーションファイルの“クローズ処理”を実行することにより、シンプルで簡素な流れの中で、利用者による使用状況の把握、承認を確実に行うことができ、利用者が把握していない不正使用などを有効に防御することができる。

[0019] 金融取引に関する利用者ID情報が利用者媒体に保持されており、金融取引処理に際して利用者媒体を介して利用者ID情報がやり取りされる。

利用者ID情報を保持する手段も多様なものが可能である。

従来型のカード媒体に保持させてカードリーダーを介して利用者ID情報を取得するもの、スマートフォンなどに保持させて端末を介して電子クレジット決済処理において利用者ID情報を取得するものもあり得る。

次に、オープン暗証コード、クローズ暗証コードとして、多様なものが可能である。

例えば、PINコード、パスワード、バーコードなどの1次元コード、QRコードなどの二次元コード、静脈や指紋や虹彩や声紋など利用者の生体情報などがある。

[0020] 本発明では“オープン暗証コード”と“クローズ暗証コード”という2つの暗証コードを設定登録する手法は高いセキュリティを達成する。

従来のアプリケーションにおいて、立ち上げ時のオープン暗証コード（パスワード、生体情報）を設定するものは存在したが、終了時のクローズ暗証コード（パスワード、生体情報）を設定するものは存在しなかった。このようにアプリケーションのオープン時と、金融取引情報の内容確定と終了時の2回にわたって暗証コード入力を求めるという技術は、本発明者がオリジナルに発明した素晴らしい手法である。つまり、利用可否ステータス情報状態制御手段の金融取引処理アプリケーションが、オープン時の金融取引処理アプリケーションファイルオープン処理において、切り替えリクエスト情報に含まれるオープン暗証コードと設定登録にかかるオープン暗証コードとの照合による認証処理を経て金融取引処理アプリケーションのオープン処理を行う。さらに、利用可否ステータス情報状態制御手段の金融取引処理アプリケーションが、終了時にあたる承認確認処理において承認情報に含まれるクローズ暗証コードと設定登録にかかるクローズ暗証コードとの照合による認証処理を経て連続処理を実行して金融取引処理アプリケーションファイルをクローズする。このように、クレジット利用やデビット利用の利用開始直前にも利用者によるオープン暗証コード入力を求め、クレジット利用やデビット利用の利用終了時にも利用者によるクローズ暗証コード入力を求めるものである。

[0021] なお、オープン暗証コード、クローズ暗証コードとして生体情報を用いる構成とすれば、利用者本人を認証することもできる。利用者端末がスマートフォンである場合、スマートフォンに利用者の生体情報読み取りデバイスが搭載されているものとする。店舗据え付けの生体情報読み取りデバイスを利用する構成であれば、悪意の店舗または端末がハッキングされている店舗で生体情報読み取りデバイスを利用すると、重要な生体情報自体が盗用・流出するおそれがあるが、自分が保持しているスマートフォンなどに装備された生体情報読み取りデバイスであれば、他者による盗用・流出するおそれが劇的に減少する。

[0022] 次に、本発明者は、さらに高いセキュリティレベルの運用も思いついた。

クレジットカード、キャッシュカードは1日のうちで実際に使用する時間は極めて限られており、店頭での支払いなどの数十秒程度である。1日に数回使用するとしてもやはりクレジットカード、キャッシュカードを実際に使用する時間はわずかである。現在のシステムの運用は、そのわずかな時間のために、常時クレジットカード、キャッシュカードを有効な状態に固定し、紛失や盗難にあったことが発覚した場合にのみ無効化するものであるが、この考え方を逆転させ、常時クレジットカード、キャッシュカードを無効の状態に固定しておき、店頭などで使用する瞬間だけ動的に有効化する運用とすればもっとも安全である。かつ、クレジットカード、キャッシュカードの有効化の手段として本人自身が保持するスマートフォンなどの携帯端末を介して本人認証付きにて行うものであれば高いセキュリティレベルが達成できる。たとえ、紛失したり盗難にあったりしてもクレジットカード、キャッシュカードの拾得者にとって簡単には不正使用ができないこととなる。

[0023] このように、アカウントがデフォルトとして通常時無効状態においておくという考え方は従来にはなく、利用者が使用する場合にのみ、利用可否ステータス情報を自発的に細かく切り替えられることにより、カードの紛失時、盗難時のなりすまし使用や、スキミングなどの不正使用が有効に防止できる。

[0024] そこで、本発明者は、利用者のクレジットカードやキャッシュカードの利用において、店頭などで使用する直前にアカウントを動的に有効化し、その後かならずクレジットカード、キャッシュカードを常時無効の状態に戻す処理を付加する拡張も行った。

本発明の金融取引制御システムは、上記した基本構成に加えて、金融取引処理アプリケーションが、利用者のアカウントの有効無効状態または金融取引受け入れ可否の状態を示す利用可否ステータス情報の切り替えを制御する利用可否ステータス情報状態制御手段を備え、金融取引処理アプリケーションが、利用可否ステータス情報を通常時は無効状態に維持する利用可否ステータス情報状態制御手段を介した無効デフォルト処理を行い、利用者端末からの承認情報の返信を条件として、利用可否ステータス情報の一時有効状態への切り替え処理と、引き渡し処理と、利用可否ステータス情報の無効デフォルト処理と、クローズ処理を連続処理するものである。

つまり、上記した基本の金融取引制御システムの処理の流れは、オープン処理→編集処理→承認伺い処理→引き渡し処理→クローズ処理の流れであったが、この改良型の金融取引制御システムの処理の流れは、無効デフォルト処理を通常時のデフォルト処理とし、オープン処理→編集処理→承認伺い処理→有効状態切り替え処理→引き渡し処理→無効デフォルト処理→クローズ処理の流れとして、さらにセキュリティレベルを向上させている。

[0025] 上記構成のように、金融取引処理アプリケーションは、利用可否ステータス情報状態制御手段により、利用可否ステータス情報が無効デフォルト処理により通常時無効状態に維持しておき、その通常時無効状態において、利用者端末から送信される情報が金融取引処理を開始する旨の金融取引処理リクエスト情報である場合、金融取引処理アプリケーションが利用者のアカウントに関する金融取引処理アプリケーションファイルをオンデマンドでオープンする「(1)オープン処理」を実行する。つまり『今からクレジット利用、デビット利用を行うので、その処理を受け付けるアプリケーションファイル（金融取引処理アプリケーションファイル）を立ち上げる』という処理を実行

する。その金融取引処理アプリケーションが金融取引者（つまり、クレジット利用を行う店舗やクレジット利用を認めるECサイト）からの利用者のアカウントに対する金融取引情報（つまりクレジットでの代金決済の要求）を受け付けると、金融取引処理アプリケーションファイルにその金融取引情報の内容を書き込む編集を受け付けて処理する「(2)編集処理」を実行する。さらに、利用者端末（スマートフォン）に対して金融取引情報を受け付けて正常終了して良いか否かを問う承認リクエストを送信する“承認リクエスト処理”と、承認リクエストに対する利用者端末からの承認情報の返信を待つ「(3)承認確認の伺い処理および受付処理」（例えば、スマートフォンの画面に取引内容の表示と、承認ボタンを表示し、その承認ボタンの押下または生体情報の入力を待つ処理）と、利用者端末からの承認情報の返信（承認ボタンの押下や生体情報の入力）を受け、承認確認処理で承認情報が確認されたことを条件として、利用可否ステータス情報の一時有効状態へ切り替える「(4)利用可否ステータス情報一時有効状態切り替え処理」と、金融取引処理アプリケーションファイルに書き込まれている金融取引情報を決済管理システムへ引き渡す「(5)金融取引処理の決済管理システムへの引き継ぎ処理」と、利用可否ステータス情報の通常時無効状態へ戻す「(6)利用可否ステータス情報の無効状態切り替え処理」と、金融取引処理アプリケーションファイルを終了してクローズする「(7)クローズ処理」を連続処理する。

[0026] つまり、店舗からの金融取引情報またはECサイトからの金融取引情報が決済管理システムに送信されても、金融取引処理アプリケーションが代理でその金融取引情報を金融取引処理アプリケーションファイルに受け付けておき、利用者からの承認ボタンの押下があるまでは、利用可否ステータス情報の通常時無効状態を維持しておく。利用者からの承認ボタンの押下があると、一気に、(4)利用可否ステータス情報一時有効状態切り替え処理と、(5)金融取引処理の決済管理システムへの引き継ぎ処理と、(6)利用可否ステータス情報の無効状態切り替え処理と、(7)クローズ処理の一連の処理を連続処理する。

[0027] 一方、利用者端末には利用者アプリケーションがインストールまたはASPで利用可能となっている。利用者アプリケーションは金融取引制御システムとやり取りして金融取引制御を実行する。

利用者アプリケーションには、金融取引処理リクエスト情報を作成する金融取引処理リクエスト情報作成処理と、作成した金融取引処理リクエスト情報を金融取引処理アプリケーションに送信する金融取引処理リクエスト情報送信処理と、承認情報を作成する承認情報作成処理と、作成した承認情報を金融取引処理アプリケーションに返信する承認情報返信処理を備えた構成となっている。

単純にアカウントの有効・無効状態の切り替えを可能とする場合に比べ、上記構成では、利用者端末からの承認情報の返信を条件として、利用可否ステータス情報の一時有効状態への切り替え処理と、金融取引処理アプリケーションファイルの決済管理システムへの引き渡し処理と、利用可否ステータス情報の無効デフォルト処理と、金融取引処理アプリケーションファイルのクローズ処理を連続処理とすることにより、金融取引処理時以外は通常時無効状態が維持される。

[0028] 上記のように、連続処理となっていない場合、利用可否ステータス情報の切り替え忘れや利用者がショッピングモールなどで滞留する数時間にわたり、利用者アカウントが有効状態になったまま放置される可能性がある。もし、利用者アカウントの有効状態の時間的制約を設けた場合、実際の店頭での店員とのやり取りや商品の引き渡し準備に時間が掛かったりすると利用者アカウントの有効状態が強制的に切り替わってしまうという不都合がある。もし、利用者アカウントの有効状態の時間的制約を長く設定しすぎると、しばらくは有効状態が継続されてしまい、スキミングによる不正キャッシングなどを完全には防止できない。

[0029] このように、本発明の金融取引制御システムは、いわば、カード不正使用防止システムとして利用できる。金融取引処理アプリケーションは無効デフォルト処理によって通常時は金融取引が利用できず、利用者のクレジットカ

ードやキャッシュカードの利用時にのみ、店頭やECサイトなどで使用する際に、利用可否ステータス情報の一時有効状態への切り替え処理をし、金融取引を完了した後に引き続き無効デフォルト処理を連続処理するため、カード不正使用が防止できる。

[0030] 上記のように、本発明の金融取引制御システムは、利用者の金融取引開始によって利用可否ステータス情報の有効・無効状態が書き換えられるが、もっとも、金融機関側の与信情報に基づくアカウントの無効設定は書き換え不可とする運用がこのましい。つまり、利用者が与信オーバー状態や、利用者の利用代金の口座引き落としが失敗してクレジット利用が凍結された状態である場合には、金融機関側から与信情報に基づくアカウントの無効設定がされるが、その無効設定まで利用者が自由に書き換えることを許容する訳にはいかないからである。

[0031] そこで、決済管理システム上の与信に基づいて設定される「利用者のアカウントの有効無効状態または利用者のアカウントに対する前記金融取引受け入れの有効無効状態を示す利用可否ステータス情報」の設定が有効状態を示す設定の場合、決済管理システムが、利用可否ステータス情報状態制御手段による利用可否ステータス情報の切り替え制御を優先させて利用可否ステータス情報の切り替えを受け入れ、逆に、決済管理システム上の与信に基づいて設定される「利用者のアカウントの有効無効状態または利用者のアカウントに対する金融取引受け入れの有効無効状態を示す利用可否ステータス情報」の設定が無効状態を示す設定の場合、決済管理システムが利用可否ステータス情報状態制御手段による利用可否ステータス情報の切り替え制御を受け入れず、利用可否ステータス情報の無効状態を維持するという取扱いとする。

なお、上記のように、与信情報に基づく利用可否ステータス情報の無効状態の設定を優先させ、利用者の操作による利用可否ステータス情報の切り替え設定を不可とするか否かも運営主体の運用によって決めれば良い。例えば、与信情報に基づく利用可否ステータス情報の無効状態の設定と、利用者の

操作による利用可否ステータス情報の切り替え設定のいずれを優先するかは運営主体の運用によって選択可能とする取り扱いも可能である。

発明の効果

[0032] 本発明の金融取引制御システムによれば、カード不正使用を防止できる。

本発明の金融取引制御システムは、利用者のアカウントに対応した金融取引処理アプリケーションファイルを用い、当該ファイルを正常に開くオープン処理と、当該ファイルを正常終了するためのクローズ処理にそれぞれ暗証コードが設定されており、オープン暗証コードの照合によって金融取引処理アプリケーションファイルをオープンする“オープン処理”と、金融取引処理アプリケーションファイルに金融取引情報を書き込む“編集処理”までを行い、その後、利用者端末からの承認情報の返信を待つ“承認伺い処理”を入れることにより、利用者による使用状況の把握、承認を促し、クローズ暗証コードの照合を経て、金融取引処理アプリケーションファイルデータの決済管理システムへの“引き渡し処理”と、金融取引処理アプリケーションファイルの“クローズ処理”を実行することにより、シンプルで簡素な流れの中で、利用者による使用状況の把握、承認を確実に行うことができ、利用者が把握していない不正使用などを有効に防御することができる。

図面の簡単な説明

[0033] [図1]実施例1にかかる金融取引制御システム100Aの構成を簡単に示した図である。

[図2]実施例1にかかる金融取引制御システム100Aのクレジット利用の手続の流れを示すシステムブロック図（その1）である。

[図3]実施例1にかかる金融取引制御システム100Aのクレジット利用の手続の流れを示すシステムブロック図（その2）である。

[図4]実施例1にかかる金融取引制御システム100Aのクレジット利用の手続の流れを示すシステムブロック図（その3）である。

[図5]実施例1にかかる金融取引制御システム100Aのクレジット利用の手続の流れを示すシステムブロック図（その4）である。

[図6]実施例1にかかる金融取引制御システム100Aのクレジット利用の手続の流れを示すシステムブロック図（その5）である。

[図7]実施例1にかかる金融取引制御システム100Aの利用者端末200での操作画面の例を示す図（その1）である。

[図8]実施例1にかかる金融取引制御システム100Aの利用者端末200での操作画面の例を示す図（その2）である。

[図9]実施例2にかかる金融取引制御システム100Bの構成を簡単に示した図である。

[図10]実施例2にかかる金融取引制御システム100Bのクレジット利用の手続の流れを示すシステムブロック図（その1）である。

[図11]実施例2にかかる金融取引制御システム100Bのクレジット利用の手続の流れを示すシステムブロック図（その2）である。

[図12]実施例2にかかる金融取引制御システム100Bのクレジット利用の手続の流れを示すシステムブロック図（その3）である。

[図13]実施例2にかかる金融取引制御システム100Bのクレジット利用の手続の流れを示すシステムブロック図（その4）である。

[図14]実施例2にかかる金融取引制御システム100Bのクレジット利用の手続の流れを示すシステムブロック図（その5）である。

[図15]実施例2にかかる金融取引制御システム100Bの利用者端末200Bでの操作画面の例を示す図（その1）である。

[図16]実施例2にかかる金融取引制御システム100Bの利用者端末200Bでの操作画面の例を示す図（その2）である。

[図17]実施例3にかかる金融取引制御システム100Cの構成を簡単に示した図である。

[図18]実施例3にかかる金融取引制御システム100Cのクレジット利用の手続の流れを示すシステムブロック図（その1）である。

[図19]実施例3にかかる金融取引制御システム100Cのクレジット利用の手続の流れを示すシステムブロック図（その2）である。

[図20]実施例3にかかる金融取引制御システム100Cのクレジット利用の手続の流れを示すシステムブロック図（その3）である。

[図21]実施例3にかかる金融取引制御システム100Cのクレジット利用の手続の流れを示すシステムブロック図（その4）である。

[図22]実施例3にかかる金融取引制御システム100Cのクレジット利用の手続の流れを示すシステムブロック図（その5）である。

[図23]実施例3にかかる金融取引制御システム100Cの利用者端末200Aでの操作画面の例を示す図（その1）である。

[図24]実施例3にかかる金融取引制御システム100Cの利用者端末200Aでの操作画面の例を示す図（その2）である。

[図25]特開平10-217655号公報に示す従来技術のクレジットカードを示す図である。

[図26]特開2012-73902号公報に示す従来技術のクレジットカード利用システムを示す図である。

[図27]特表2014-512579号公報に示す従来技術のクレジットカードを示す図である。

発明を実施するための最良の形態

[0034] 以下、本発明を実施するための最良の形態について実施例により具体的に説明する。なお、本発明はこれらの実施例に限定されるものではない。

実施例1として、クレジットカードやキャッシュカードなどの利用者ID保持媒体300を用いて金融取引処理を行う金融取引制御システム100Aの例を示す。金融取引処理アプリケーションファイル112Aには、オープンする際のオープン暗証コードとクローズする際のクローズ暗証コードが設定されている例を示す。

実施例2として、利用者ID保持媒体300を不要とし、スマートフォン200などに金融取引処理に必要な利用者ID情報などが電子化されたいわゆる電子クレジット金融取引処理や電子デビット金融取引処理を行う例を示す。

実施例 3 として、実施例 2 と同様、利用者 ID 保持媒体 300 を不要とした、いわゆる電子クレジット金融取引処理や電子デビット金融取引処理を行う例において、利用可否ステータス情報、利用可否ステータス情報状態制御手段を備え、通常時に無効デフォルト処理を行ってセキュリティレベルを向上させた例を示す。

実施例 1

[0035] 実施例 1 にかかる本発明の金融取引制御システム 100A およびそれを利用する利用者アプリケーション 210A について説明する。

図 1 は実施例 1 にかかる金融取引制御システム 100A および利用者アプリケーション 210A の構成を簡単に示した図である。図 1 には、金融取引制御システム 100A および利用者アプリケーション 210A のほか、利用者端末 200A、利用者媒体 300、店舗端末/EC サイト 400、決済管理システム 500A が示されている。

[0036] 金融取引制御システム 100A は、利用者によるクレジット利用またはデビット利用を伴う金融取引を制御するシステムである。

金融取引制御システム 100A は、利用者端末 200A と決済管理システム 500A との間に介在するものであるが、システムの構築箇所としては、利用者端末 200A 上に装備されていても良いし、決済管理システム 500A に装備されていても良い。この例では、決済管理システム 500A に装備されている例として示す。

金融取引制御システム 100A は、少なくとも金融取引処理アプリケーション 110A を備えており、さらに、本実施例 1 の構成では暗証コード認証手段 120A も備えている。これらは詳しく後述する。

[0037] 利用者端末 200A は、スマートフォンなどの利用者が携帯する端末が好ましい。利用者端末 200A は、利用者アプリケーション 210A、データ入力手段 220、暗証コード入力手段 230、通信手段 240 を備えている。

利用者アプリケーション 210A は、金融取引制御システム 100 との間

でデータのやり取りをするアプリケーションである。この利用者アプリケーション210Aを搭載することにより利用者は利用者端末200Aを介して、クレジット利用、デビット利用のサービスについて本発明の金融取引サービスを利用できる。

データ入力手段220は、一般の携帯型端末が装備するタッチディスプレイや音声入力手段などの利用者インターフェイスを介して利用者よりデータの入力を受け付ける手段である。

暗証コード入力手段230は、利用者から暗証コードの入力を受け付けるデバイスである。

暗証コードがPINコードやパスワードである場合は、PINパッド、キーボード、タッチパネルなどの入力デバイスがある。データ入力手段220が暗証コード入力手段230を兼用する構成でも良い。なお、暗証コードは4桁以上の数字・文字列が好ましい。利用者が入力するPINコードと利用者端末200Aの端末ID番号とを組み合わせるなど一定のアルゴリズムで計算したコードを暗証コードとして送信するものでも良い。

また、暗証コードがバーコードの一次元コードやQRコードなどの二次元コードである場合、当該コードの読み取りリーダーやカメラなどの入力デバイスがある。

暗証コードが生体情報である場合、生体情報としては、指紋情報、指静脈情報、手のひら静脈情報、虹彩情報、顔画像情報、声紋情報などがあり得る。この場合利用者端末200Aの暗証コード入力手段230は、対応する生体情報が読み取れるデバイス（指紋リーダー、静脈リーダー、虹彩リーダー、カメラ、マイクロフォンなどの音声入力装置など）が装備されているものとする。

通信手段240は、利用者端末200Aが装備している通信機能で良い。

[0038] 次に、利用者媒体300を説明する。

利用者媒体300は、クレジット利用時やデビット利用時に用いる媒体であり、典型的には、磁気ストライプカード、ICカード、非カード型のIC

チップ埋設物、人体埋設型のマイクロＩＣチップなどがあり得る。利用者媒体３００には利用者ＩＤ情報、カード情報、金融取引に必要な情報などの各種情報が保持されており、店舗端末／ＥＣサイト４００に対して提示することにより、クレジット利用やデビット利用を伴う金融取引を申し込むことができる。

なお、利用者媒体３００を用いず、スマートフォンなどに金融取引で要求される利用者ＩＤ情報などを電子化した電子クレジット金融取引処理や電子デビット金融取引処理を行う金融取引制御システムについては実施例２において示す。

[0039] 次に、店舗端末／ＥＣサイト４００を説明する。

店舗端末／ＥＣサイト４００は、決済管理システム５００Ａとの間での決済情報をやり取りする機能を備えた店舗に据え付けられた端末や、インターネット上の電子商取引可能なウェブサイトであり、利用者情報入力手段４１０、金融取引情報生成手段４２０、通信手段４３０を備えている。

利用者情報入力手段４１０は、利用者媒体３００に対応したカードリーダーであり、利用者媒体３００からカード情報や利用者ＩＤ情報などを読み取るデバイスである。

金融取引情報生成手段４２０は、利用者が所望するクレジット利用、デビット利用のサービスに伴う金融取引情報を生成する手段である。例えば、カード情報、利用者ＩＤ情報、店舗情報／取引者情報、決済金額、決済管理システム５００ＡのＩＤ情報などを含む金融取引情報を生成し、通信手段４３０を介して、ネットワークを介して決済管理システム５００Ａに対して送信する。

[0040] 次に、決済管理システム５００Ａを説明する。

決済管理システム５００Ａは、金融機関や信販会社などが管理運営しているシステムであり、利用可否ステータス情報５１０、与信管理部５２０、決済処理部５３０を備えている。金融取引制御システム１００とのデータのやり取りができ、さらに、オンライン上で店舗端末／ＥＣサイト４００や利用者

端末２００Ａとデータ通信可能となっている。

[0041] ここで、利用可否ステータス情報５１０とは、決済管理システム５００Ａ上で管理される利用者のアカウントの有効無効状態、または、利用者のアカウントに対する金融取引受け入れの有効無効状態を示す情報である。

この構成例では、利用可否ステータス情報５１０は、与信管理部５２０により管理されている例となっている。この利用可否ステータス情報５１０が有効状態を示す場合、決済管理システム５００Ａは、当該利用者によるクレジット利用またはデビット利用を伴う金融取引を受け入れる取り扱いとなっている。逆に、この利用可否ステータス情報５１０が無効状態を示す場合、決済管理システム５００Ａは、当該利用者によるクレジット利用またはデビット利用を伴う金融取引を拒否する取り扱いとなっている。

本来は、与信に問題がないクレジット利用者、デビット利用者の利用可否ステータス情報５１０は有効状態に維持されている。

[0042] 与信管理部５２０は、金融機関や信販会社などが管理運営している一般の決済管理システムが装備している与信管理部と同様で良い。利用可否ステータス情報５１０の管理を行っている。

[0043] 決済処理部５３０は、金融機関や信販会社などが管理運営している一般の決済管理システムが装備している決済処理部と同様で良く、利用可否ステータス情報が有効状態と確認された条件下、店舗端末／ＥＣサイト４００から受信した金融取引情報を基に決済処理を行うものである。

なお、該当する利用者ＩＤ情報の金融取引情報が店舗端末／ＥＣサイト４００から送信されてくると、そのまま決済処理を行うのではなく、金融取引処理アプリケーション１１０Ａに金融取引情報を一旦引き渡し、金融取引処理アプリケーション１１０Ａでの処理に任せ、後述する金融取引処理アプリケーション１１０Ａの“金融取引情報データ引き渡し処理”により、金融取引処理アプリケーションファイル１１２Ａの金融取引情報のデータ内容が引き渡された後に、通常の決済処理（利用可否ステータス情報の有効状態の確認、金融決済処理など）を実行する。

なお、利用者の与信情報に基づく決済管理システム側による無効設定との優劣については実施例１と同様の処理で良い。

[0044] 次に、金融取引制御システム１００Ａの構成を詳しく述べる。

金融取引制御システム１００Ａは、金融取引処理アプリケーション１１０Ａ、暗証コード認証手段１２０Ａを備えた構成となっている。

[0045] 先に、暗証コード認証手段１２０Ａについて説明する。

金融取引制御システム１００Ａは、暗証コード認証手段１２０Ａを含んでおり、利用者端末２００Ａにも暗証コード入力手段２３０が含まれており、暗証コード認証手段１２０Ａが、利用者が暗証コード入力手段２３０を介して入力されて送信された暗証コードと、決済管理システム５００Ａ上で登録されている暗証コード情報との認証処理を行い、認証処理に成功したことを条件として金融取引処理アプリケーション１１０Ａの所定の処理を実行する取り扱いとする。

[0046] 実施例１では、利用者アプリケーション２１０Ａより“金融取引処理リクエスト情報”の送信に加え、“承認情報”の送信が求められる。前者は金融取引処理アプリケーションファイルのオープン処理に対応し、後者は金融取引処理アプリケーションファイルのクローズ処理に対応するものである。

[0047] 暗証コード認証手段１２０Ａは利用者端末２００Ａから送信されてくる金融取引処理のリクエスト情報や承認情報に含まれる暗証コードを抽出し、真正の利用者により決済管理システム５００Ａ上で事前に登録されている暗証コードデータにアクセスし、暗証コードが正しいものか否かをチェックすることにより利用者を認証する。

[0048] 次に、金融取引処理アプリケーション１１０Ａを説明する。

金融取引処理アプリケーション１１０Ａは、金融取引制御システム１００ＡにインストールまたはＡＳＰで利用可能となっているアプリケーションであり、金融取引処理アプリケーション１１０Ａは常駐型でも良く、利用者端末２００Ａから送信されてくる金融取引処理のリクエスト情報に応じて立ち上げられるものであっても良い。ここでは常駐型とする。

金融取引処理アプリケーション 110Aは、利用者ごとまたは金融取引ごとに用意される利用者アプリケーションファイル 112Aを備えた構成となっている。

金融取引処理アプリケーション 110Aによってクレジット利用/デビット利用時にオンデマンドによる金融取引処理アプリケーションファイル 112Aのオープン処理、金融取引処理アプリケーションファイル 112Aを決済処理部 530に引き渡すデータ引き渡し処理、金融取引処理アプリケーションファイル 112Aのクローズ処理を実行する。

[0049] 金融取引処理アプリケーションファイル 112Aは、金融取引処理アプリケーション 110Aにより処理される利用者ごとまたは金融取引ごとに用意されるアプリケーションファイルである。金融取引処理アプリケーション 110Aは金融取引処理アプリケーションファイル 112Aを用いて以下の処理を実行する。

(1)利用者ごとまたは金融取引ごとに金融取引処理アプリケーションファイル 112Aをオンデマンドでオープンする「オープン処理」、(2)金融取引処理アプリケーションファイル 112Aのデータを編集する「編集処理」、(3)利用者による「承認確認」の伺い処理および受付処理、(4)金融取引処理の決済管理システム 500Aへの引き継ぎ処理、(5)金融取引処理アプリケーションファイル 112Aのクローズ処理の各処理である。

[0050] (1) 金融取引処理アプリケーションファイル 112Aのオープン処理

まず、金融取引処理アプリケーションファイル 112Aのオープン処理について説明する。“金融取引処理アプリケーションファイル 112Aのオープン処理”は金融取引処理の開始に応じてオンデマンドで実行される。ここでは、利用者アプリケーション 210Aからの利用者によるクレジット利用開始などのリクエストがあれば、金融取引処理アプリケーション 110Aは当該利用者のアカウントに対応する金融取引処理アプリケーションファイル 112Aを立ち上げる“金融取引処理アプリケーションファイルオープン処理”を実行する。

[0051] (2) 金融取引処理アプリケーションファイル 1 1 2 A のデータ編集処理
金融取引処理アプリケーションファイル 1 1 2 A は利用者 I D ごとに管理されており、オープンされるとデータの書き込みなどの編集が可能となる。
ここでは、店舗端末/E C サイト 4 0 0 の金融取引情報生成手段 4 2 0 にて生成された金融取引情報が決済管理システム 5 0 0 A に送信されてくると、決済処理部 5 3 0 は、金融取引処理アプリケーション 1 1 0 A に金融取引情報を引き渡す。金融取引処理アプリケーション 1 1 0 A は、利用者 I D 情報に対応する金融取引処理アプリケーションファイル 1 1 2 A に対して金融取引情報のデータを書き込むことで第三者（ここでは店舗端末/E C サイト 4 0 0）による編集を一旦受け入れる扱いとする。

[0052] (3) 利用者に対する承認伺い処理および確認処理

利用者に対する承認確認処理として、まず、利用者端末 2 0 0 A に対して金融取引の受け付けを承認して金融取引を正常終了させる承認終了処理を実行しても良いかを問う“承認リクエスト”を送信し、“承認リクエスト”に対する利用者端末 2 0 0 A からの承認情報の返信を待つ承認確認の伺い処理を行う。

ここでは、この“承認リクエスト”には“クローズ暗証コード”の入力要求が設定されているものとする。つまり、金融取引処理アプリケーションファイル 1 1 2 A に正常にクローズさせるためクローズ用の暗証コードが設定されており、利用者に対して、このクローズ用の暗証コードを入力させる。

この例では、承認用の“クローズ暗証コード”として利用者の生体情報が登録されているものとする。

[0053] 次に、利用者端末 2 0 0 A からの“承認情報”の返信を受けて“承認情報”を確認する“承認確認処理”を行う。

ここでは、この承認情報には利用者が入力した“クローズ暗証コード”が含まれているので、暗証コード認証手段 1 2 0 A を介して承認情報に含まれている“クローズ暗証コード”の認証が行われる。この例では利用者の生体情報がクローズ暗証コードである。

このように、金融取引処理アプリケーションファイル 112A を編集後にファイルを正常にクローズさせるためにクローズ用の暗証コードが設定されており、さらに高いセキュリティレベルが設けられている。

[0054] (4) 金融取引処理の決済管理システム 500A への引き継ぎ処理

金融取引処理アプリケーション 110A は、“金融取引情報データ引き渡し処理”として、金融取引処理アプリケーションファイル 112A に記録された金融取引情報のデータ内容を決済管理システム 530 へ引き渡す。

なお、決済管理システム 530 は金融取引情報の引き渡しを受け、その後は通常の決済処理（利用可否ステータス情報の有効状態の確認、金融決済処理など）が行われる。

[0055] (5) 金融取引処理アプリケーションファイル 112A のクローズ処理

最後に、金融取引処理アプリケーション 110 によって金融取引処理アプリケーションファイル 112 をクローズする“金融取引処理アプリケーションファイル終了処理”が実行される。

ここでは、上記した(3)利用者に対する承認確認処理から(5)金融取引処理アプリケーションファイル 112A のクローズ処理まで、利用者から送信された“承認情報”に含まれるクローズ用の暗証コードが認証されれば、一気に連続処理し、金融取引処理アプリケーションファイルの終了処理まで実行する運用となっている。

[0056] 次に、フローチャートおよび図面を参照しつつ、実施例 1 にかかる金融取引制御システム 100 の処理の流れの概略を示す。

ここでは、利用者媒体 300 は、IC カード型のクレジットカード 300 とする。利用者が店舗に行って商品を購入してクレジット利用により金融取引決済を行うシーンを前提として説明する。なお、利用者が EC サイトにログインして商品を購入してクレジット利用やデビット利用による金融取引決済を行うシーンとしても同様に考えることができる。

[0057] 以下、一連のクレジット利用、デビット利用の手続の流れを図 2～図 5 のシステムブロック図、図 7 および図 8 の金融取引制御システム 100A の利

用者端末200Aでの操作画面の例を示す図を参照しつつ説明する。

- [0058] まず、利用者は、商品を選定し、クレジット利用の決済に先立ち、スマートフォン200Aを操作して利用者アプリケーション210Aを立ち上げる（図2ステップS1）、例えば、利用者端末200Aのディスプレイ上に表示されている利用者アプリケーション210Aのアイコンをタップする（図7（1））。なお、この段階で、利用者アプリケーション210Aの使用権限を確認するため、パスワードを入力する運用も可能である。利用者端末200A上に利用者アプリケーション210Aが立ち上がり、サービスメニューが表示される（図7（2））。この例では“クレジットを利用する”、“デビットを利用する”という2つのメニューが表示されている。
- [0059] このクレジット利用開始ボタン押下（図7（3））により利用者アプリケーション210Aは、利用者に対してオープン暗証コードの入力を要求するガイダンスを表示して入力を要求し（図7（4））、利用者から暗証コード入力手段230を介して入力された“オープン暗証コード”を得る（図2ステップS2）。ここでは生体情報として指紋情報が入力される（図7（5））。
- [0060] 利用者アプリケーション210Aは“金融取引処理リクエスト情報”を生成し（図2ステップS3）、利用者アプリケーション210Aは、通信手段240を介して“金融取引処理リクエスト情報”と指紋情報である“オープン暗証コード”を金融取引制御システム100Aに送信する（図2ステップS4）。なお、実施例2では“金融取引処理リクエスト情報”が送信されたが、ここでは、“金融取引処理リクエスト情報”と“オープン暗証コード”が送信される。
- [0061] 金融取引制御システム100Aは、送信されてきた“金融取引利用リクエスト情報”を受け付けると、“オープン暗証コード”を抽出し、暗証コード認証手段120Aに入力し、オープン暗証コードの認証処理を実行させる（図2ステップS5）。暗証コード認証手段120Aは、利用者アプリケーション210Aから送信されてきた“オープン暗証コード情報”と、決済管理

システム５００Ａ上で登録されている“オープン暗証コード情報”との認証処理を行い、認証処理に成功した場合は、金融取引処理アプリケーション１１０Ａに認証成功を通知し、金融取引処理アプリケーション１１０Ａは、該当する利用者ＩＤ情報に関連付けられた金融取引処理アプリケーションファイル１１２Ａのオープン処理を実行する（図２ステップＳ６）。

なお、認証処理に失敗した場合は（図２ステップＳ５：Ｎ、図中には図示せず）、金融取引処理アプリケーション１１０Ａに認証不成立を通知し、金融取引処理を打ち切る。

[0062] 金融取引制御システム１００Ａ側において金融取引処理アプリケーションファイル１１２Ａのオープン処理が完了すれば、“金融取引利用開始ＯＫ”を示す情報を生成し（図１０ステップＳ６）、通信手段５４０を介して利用者端末２００Ａに返信され（図２ステップＳ７）、利用者端末２００Ａ上において“クレジット利用できます”という表示がなされ（図７（６））、クレジット利用を開始する（図２ステップＳ８）。

[0063] 次に、店舗やＥＣサイトでの利用に移る。

利用者は、上記のように、利用者端末２００Ａにおいて、“クレジット利用できます。”という表示があれば、クレジット利用を開始する。

利用者が店舗などで商品購入時にクレジットカード３００を提示し、店舗会計スタッフが、カードのタイプに応じて磁気ストライプリーダ、ＩＣカードリーダなどの利用者情報入力手段４１０から利用者ＩＤ情報を入力し（図３ステップＳ９）、店舗端末／ＥＣサイト４００の金融取引情報生成手段４２０を介してクレジットカードから利用者ＩＤ情報などクレジット利用に必要な諸情報および決済代金情報などを入力し、それら情報を基に金融取引情報を生成し（図３ステップＳ１０）、店舗端末／ＥＣサイト４００の通信手段４３０を介してそれら金融取引情報が決済管理システム５００Ａに送信する（図３ステップＳ１１）。

なお、ＥＣサイトの利用の場合、決済用の入力画面を表示してクレジットカード番号や有効期限や暗証番号などの諸情報を入力すれば、ＥＣサイトに

において金融取引情報が生成され、店舗端末/E Cサイト400の通信手段430を介してそれら金融取引情報が決済管理システム500Aに送信される。

[0064] 本実施例1では、この段階ではまだ決済管理システム500Aは通常のクレジット処理を行わない。まず、決済処理部530は、金融取引情報を金融取引処理アプリケーション110Aに渡す（図3ステップS12）。

なお、後述するように、決済処理部530は、金融取引処理アプリケーション110Aから決済処理開始OKの旨の情報を受け取った後は、通常の決済処理を実行する。

[0065] 金融取引処理アプリケーション110Aは、受け取った金融取引情報の中から利用者ID情報を抽出して、オープン処理されている金融取引処理アプリケーションファイル112Aと関連付けられている利用者ID情報が否かをチェックする（図3ステップS13）。

[0066] オープン処理されている金融取引処理アプリケーションファイル112Aがある利用者ID情報である場合は（図3ステップS13：Y）、本発明の金融取引制御システム100Aの利用者であり、クレジット利用の金融取引処理中を意味するので、受け取った金融取引情報を該当する金融取引処理アプリケーションファイル112Aに書き込む（図3ステップS14）。

[0067] 次に、金融取引処理アプリケーションファイル112Aの承認処理に進む。

金融取引制御システム100Aは“承認伺い処理”を実行する。

金融取引制御システム100Aは、利用者アプリケーション210Aに対して金融取引を承認して金融取引を正常終了させる承認終了処理を実行しても良いかを問う“承認リクエスト”を送信し（図4ステップS15）、“承認リクエスト”に対する利用者アプリケーション210Aからの“承認情報”の返信を待つ。

なお、この“承認伺い処理”は、金融取引制御システム100Aが自律的に利用者アプリケーション210Aに対して送信して“承認情報”の入力を待つ形でも良いし、利用者アプリケーション210A側が金融取引制御シス

テム１００Ａに自発的にアクセスして“承認情報”の入力を行う形であっても良い。

[0068] 利用者端末２００Ａは、“承認リクエスト”を受信すると、ディスプレイ上に「ご利用の取引内容をご確認ください」というメッセージと、商品購入代金、クレジット支払回数などのクレジット利用内容を表示し、“承認ボタン”を表示して押下を促す（図８（１））。この例では“承認する”というボタンと“承認しない”というボタンが表示される。

利用者が“承認ボタン”を押下すると（図４ステップＳ１６、図８（２））、利用者アプリケーション２１０Ａは、利用者に対してクローズ暗証コードの入力を要求するガイダンスを表示し（図８（３））、利用者から暗証コード入力手段２３０を介して入力された“クローズ暗証コード”を得る（図４ステップＳ１７）。ここでは生体情報として指紋情報が入力されるものとする（図８（４））。

なお、“承認しない”ボタンを押下した場合の運用は限定されないが、例えば、利用者アプリケーション２１０Ａはこの金融取引が利用者による正当な取引ではないとして（例えば、不正使用者による不正取引とみなして）、決済処理部５３０には決済処理ＮＧの旨を通知し、金融取引処理を強制終了する。

[0069] 金融取引制御システム１００Ａは、利用者端末２００Ａからの“承認情報”の返信（図４ステップＳ１８）を受けて“承認確認処理”を実行する。ここでは、この承認情報には“クローズ暗証コード”が設定されているので、“クローズ暗証コード”を抽出し、暗証コード認証手段１２０Ａに入力し、クローズ暗証コードの認証処理を実行させる（図４ステップＳ１９）。

暗証コード認証手段１２０Ａは、利用者アプリケーション２１０Ａから送信されてきた“クローズ暗証コード情報”と、決済管理システム５００Ａ上で登録されている“クローズ暗証コード情報”との認証処理を行う。

認証処理に成功した場合は（図４ステップＳ１９：Ｙ）、金融取引処理アプリケーション１１０Ａに認証成功を通知（図４ステップＳ２０）する。金

金融取引処理アプリケーション 110A は決済処理 OK の旨の情報とともに金融取引情報のデータ内容を決済管理システム 530A へ引き渡す（図 5 ステップ S21）。

なお、認証処理に失敗した場合は（図中には図示せず）、金融取引処理アプリケーション 110A に認証不成立を通知する。金融取引処理アプリケーション 110A は決済処理 NG の旨の情報を決済管理システム 530 へ引き渡す（図中には図示せず）。

[0070] 承認確認処理で“承認情報”が確認されたこと、つまり、クローズ用の暗証コードの入力を条件として、金融取引処理アプリケーション 110A は決済処理 OK の旨の情報とともに、金融取引処理アプリケーションファイル 112A の金融取引情報のデータ内容を決済管理システム 530 へ引き渡す（図 5 ステップ S21）。

[0071] 決済管理システム 530 は金融取引情報の引き渡しを受け、その後は通常の決済処理を開始する。

与信管理部 520 が与信に基づいた場合の利用可否ステータス情報 510 の設定が“有効状態”つまり“無効状態の設定ではない”か否かをチェックし（図 5 ステップ S22）、与信管理部 520 の与信情報に基づく設定が“無効状態の設定ではない”場合には、決済処理部 530 に与信情報が有効である旨を通知し（図 5 ステップ S23）、金融取引情報から利用者 ID 情報などクレジット利用に必要な諸情報および決済代金情報を抽出し、クレジット決済処理が実行され（図 5 ステップ S24）、店舗端末/EC サイト 400 にクレジット利用が成立した旨を示す情報が返信される（図 5 ステップ S25）。

もし、与信情報に基づく与信管理部 520 による利用可否ステータス情報 510 の設定が“無効状態”を示す設定の場合は（図中には図示せず）、金融取引処理アプリケーション 110A は、利用者端末 200A から送信された承認終了処理にかかわらず、金融取引処理アプリケーション 110A は決済処理 NG の旨の情報を決済管理システム 530 へ引き渡す。結局クレジット

ト処理が不成立となる。

決済処理部 530 から店舗端末/E C サイト 400 にクレジット利用が不成立である旨を示す情報が返信される（図中には図示せず）。

[0072] 金融取引処理アプリケーション 110A は、“金融取引処理アプリケーションファイル終了処理”を実行し、金融取引処理アプリケーションファイル 112A をクローズする（図 6 ステップ S26）。

利用者アプリケーション 210A には、クレジット処理が完了した旨が表示され（図 8（5））、必要に応じて、利用者アプリケーション 210A を終了し（図 8（6））、利用者アプリケーション 210A が閉じられる（図 8（7））。さらに、利用者アプリケーション 210A のアイコン選択を解除する（図 8（8））。

なお、上記したステップ S13 において、オープン処理されている金融取引処理アプリケーションファイル 112A がある利用者 ID 情報ではない場合は（図中には図示せず）、本発明の金融取引制御システム 100A の利用者とは異なる他者の利用（つまり、本発明の利用者ではない一般の利用者）であるため、決済処理部 530 に対して、決済処理開始 OK の情報とともに金融取引情報を返し、決済処理部 530A は、金融取引情報を基に、通常の決済処理を開始する。

実施例 2

[0073] 実施例 2 として、利用者 ID 保持媒体 300 を不要とし、スマートフォン 200 などに金融取引処理に必要な利用者 ID 情報などが電子化されたいわゆる電子クレジット金融取引処理や電子デビット金融取引処理を行う例を示す。

なお、以下、一例として、利用者端末 200B の電子決済アプリケーション 260B および利用者媒体アカウント情報 270B と、決済処理部 530 の利用者媒体アカウント情報 560B を用いた電子決済の例を説明するが、本発明は、このような電子決済に用いる利用者端末 200B の電子決済アプリケーション 260B および利用者媒体アカウント情報 270B や、決済処

理部 530 の利用者媒体アカウント情報 560 B 自体には限定されずそれらが何であっても良く、利用者端末 200 B の利用者アプリケーション 210 B と金融取引制御システム 100 B の金融取引処理アプリケーション 110 B および金融取引処理アプリケーションファイル 112 B の働きにより不正使用防止の用に供するものである。

[0074] 実施例 2 にかかる金融取引制御システム 100 B の構成は、少なくとも金融取引処理アプリケーション 110 B、暗証コード認証手段 120 B を備えており、実施例 1 で示した図 1 の構成と同様であるのでここでは説明を省略する。

[0075] 実施例 2 にかかる利用者端末 200 B は、少なくとも利用者アプリケーション 210 B、データ入力手段 220、暗証コード入力手段 230、通信手段 240 に加え、カメラ 250 B、電子決済アプリケーション 260 B、利用者媒体アカウント情報 270 B を備えている。

利用者アプリケーション 210 B は、実施例 1 と同様、金融取引制御システム 100 B との間でやり取りし、実施例 1 で示した (1) 金融取引処理アプリケーションファイル 112 A のオープン処理、(3) 利用者に対する承認伺い処理および確認処理を行う機能を備えている。

データ入力手段 220、暗証コード入力手段 230、通信手段 240 は、実施例 1 に示したものと同様で良く、ここでの詳しい説明は省略する。

[0076] 電子決済アプリケーション 260 B は、電子クレジット決済や電子デビット決済のために使用するアプリケーションである。利用者端末 200 B を用いて金融機関などが提供する多様な電子決済を行うためのアプリケーションである。近年、同様の電子決済アプリケーションが提供されているが、本発明では、電子決済アプリケーション 260 B として、普及しつつある公知のアプリケーションを含めることができる。例えば、アップルペイ (TM)、アマゾンペイ (TM) など多様なものが提供され始めている。

[0077] 利用者媒体アカウント情報 270 B は、電子決済アプリケーション 260 B において利用される利用者媒体のアカウント情報である。名称は、利用す

る電子決済アプリケーション２６０Ｂにおいて異なる場合があるが、それら電子決済アプリケーション２６０Ｂにおいて、従来の利用者ＩＤ情報の保持においてカード媒体を必要としたものが電子化された情報として保持されるものである。

[0078] カメラ２５０Ｂは、スマートフォンなどの利用者端末が装備しているカメラでも良い。例えば、クレジットカード媒体をカメラ２５０Ｂで撮影して画像認識することにより、保持されている利用者ＩＤ情報を利用者媒体アカウント情報２７０Ｂとして電子決済アプリケーション２６０Ｂに登録する際に使用する。セキュリティコードなどは手入力する場合もある。

[0079] なお、利用する電子決済アプリケーション２６０Ｂにおいて、利用者媒体アカウント情報２７０Ｂの登録手順や、登録に要する本人認証のやり方などは異なることはあり得るが、本発明では、電子決済アプリケーション２６０Ｂおよび利用者媒体アカウント情報２７０Ｂの登録や利用手順などには限定されず、各種の電子決済アプリケーション２６０Ｂおよび利用者媒体アカウント情報２７０Ｂが正常に登録されているものとする。

[0080] 次に、実施例２にかかる決済管理システム５００Ｂについて説明する。

決済管理システム５００Ｂは、実施例１と同様、金融機関や信販会社などが管理運営しているシステムであり、金融取引制御システム１００Ｂとのデータのやり取りができ、さらに、オンライン上で店舗端末／ＥＣサイト４００や利用者端末２００Ｂとデータ通信可能となっている。この例では、金融取引制御システム１００Ｂは、決済管理システム５００Ｂに含まれている例であるが、別のコンピュータリソースにインストールされている構成も可能であることは言うまでもない。

[0081] 決済管理システム５００Ｂは、実施例１と同様、利用可否ステータス情報５１０、与信管理部５２０、決済処理部５３０、通信手段５４０を備え、本実施例２では、さらに利用者媒体アカウント情報５６０Ｂを備えている。

利用者媒体アカウント情報５６０Ｂは、利用者端末２００Ｂ上で作成された利用者媒体アカウント情報２７０Ｂに対応するものであり、電子決済アプ

リケーション260Bと決済処理部530とのやり取りにおいて利用される利用者媒体のアカウント情報である。この利用者媒体アカウント情報560Bと利用者媒体アカウント情報270Bとの連動によって、電子クレジット処理、電子デビット処理などが進められる。

[0082] 次に、フローチャートおよび図面を参照しつつ、実施例2にかかる金融取引制御システム100Bの処理の流れの概略を示す。なお、実施例1に示した金融取引制御システム100Aの処理の流れの概略と同様の部分については詳しい説明は省略することとする。

[0083] 図10に示した流れは実施例の図2に示した流れと同様で良い。つまり、クレジット利用の決済に先立つ利用者アプリケーション210Bの立ち上げ処理（図10ステップS31）、暗証コード入力手段230を介した“オープン暗証コード”の入力処理（図10ステップS32）、利用者アプリケーション210Bを用いた“金融取引処理リクエスト情報”の生成処理（図10ステップS33）、利用者アプリケーション210Bによる“金融取引処理リクエスト情報”と“オープン暗証コード”の金融取引制御システム100Bへの送信処理（図10ステップS34）、暗証コード認証手段120Bによるオープン暗証コードの認証処理（図10ステップS35）、利用者アプリケーション210Bによる金融取引処理アプリケーションファイルのオープン処理（図10ステップS36）、金融取引処理開始の準備完了の旨の利用者端末200Bへの返信処理（図10ステップS37）、クレジット利用開始OKの表示処理（図10ステップS38）までは実施例1の図2のステップS1からS8までと同様で良い。

[0084] 次に、店舗やECサイトでの金融取引利用に移る。

本実施例2では、利用者端末200Bにインストールされている電子決済アプリケーション260Bが利用される。

利用者は電子決済アプリケーション260Bを用いて、店舗やECサイトで電子クレジット決済利用などを通じて商品購入などの金融取引処理を開始する。電子クレジット決済利用の手順などは、利用する電子決済アプリケー

ション 260B の手順に従って行うものとする。

ここでは、電子決済アプリケーション 260B から利用者媒体アカウント情報 270B が、店舗や EC サイトでの電子決済の仕組みに応じて取り込まれる（図 11 ステップ S39）。ここでは、利用者媒体情報入力手段 410 を通じて利用者媒体アカウント情報 270B が取り込まれる。

[0085] 次に、店舗端末/EC サイト 400 の金融取引情報生成手段 420 を介してクレジット利用に必要な諸情報および決済代金情報などを入力し、それら情報を基に金融取引情報を生成し（図 11 ステップ S40）、店舗端末/EC サイト 400 の通信手段 430 を介してそれら金融取引情報が決済管理システム 500B に送信される（図 11 ステップ S41）。

[0086] ここでは、金融取引情報は決済処理部 530 の利用者媒体アカウント情報 560B に渡され、利用者媒体アカウント情報 270B と利用者媒体アカウント情報 560B が対応し合うものであるか確認されるものとする。確認されなければ、電子決済運用主体により電子決済ができない扱いとなる。ここでは確認されたものとする。

この段階ではまだ決済管理システム 500B は通常のクレジット処理を行わない。まず、決済処理部 530 は、金融取引情報を金融取引処理アプリケーション 110B に渡す（図 11 ステップ S42）。

[0087] 金融取引処理アプリケーション 110B は、受け取った金融取引情報の中から利用者 ID 情報を抽出して、オープン処理されている金融取引処理アプリケーションファイル 112B と関連付けられている利用者 ID 情報か否かをチェックする（図 11 ステップ S43）。

[0088] オープン処理されている金融取引処理アプリケーションファイル 112B がある利用者 ID 情報である場合は（図 11 ステップ S43：Y）、本発明の金融取引制御システム 100B の利用者であり、クレジット利用の金融取引処理中を意味するので、受け取った金融取引情報を該当する金融取引処理アプリケーションファイル 112B に書き込む（図 11 ステップ S44）。

[0089] 次に、金融取引処理アプリケーションファイル 112B の承認処理に進む

。

金融取引制御システム１００Ｂは“承認伺い処理”および“承認処理”を実行する。

図１２に示す“承認リクエスト”の送信処理（図１２ステップＳ４５）、利用者による“承認ボタン”処理（図１２ステップＳ４６、図１６（１）（２））、利用者に対するクローズ暗証コードの入力処理（図１２ステップＳ４７、図１６（３）（４））、利用者端末２００Ｂからの“承認情報”の返信処理（図１２ステップＳ４８）、金融取引制御システム１００Ｂにおけるクローズ暗証コードの認証処理（図１２ステップＳ４９）は、実施例１の図４で示したステップＳ４５からステップＳ４９までと同様で良い。

[0090] 承認確認処理で“承認情報”が確認されたこと、つまり、クローズ用の暗証コードの入力を条件として、金融取引処理アプリケーション１１０Ｂは決済処理ＯＫの旨の情報とともに、金融取引処理アプリケーションファイル１１２Ｂの金融取引情報のデータ内容を決済管理システム５３０へ引き渡す（図１３ステップＳ５０）。

この例では図１６（１）に示すように、“承認する”というボタンと“承認しない”というボタンが表示されるが、“承認しない”ボタンを押下した場合の運用は限定されないが、例えば、実施例１と同様、利用者アプリケーション２１０Ｂはこの金融取引が利用者による正当な取引ではないとして（例えば、不正使用者による不正取引とみなして）、決済処理部５３０Ｂには決済処理ＮＧの旨を通知し、金融取引処理を強制終了する。

[0091] 決済処理部５３０Ｂの利用者媒体アカウント情報５６０Ｂは、金融取引情報の引き渡しを受け、その後は所定の決済処理を開始する。

与信管理部５２０の利用可否ステータス情報５１０の設定の確認処理（図１３ステップＳ５２）、（図１３ステップＳ５３）、決済処理部５３０Ｂによる金融取引情報を基にしたクレジット決済処理の実行（図１３ステップＳ５４）、店舗端末／ＥＣサイト４００にクレジット利用が成立した旨を示す情報の返信（図１３ステップＳ５５）が実行される。

[0092] 最後に、金融取引処理アプリケーション 110Bは、“金融取引処理アプリケーションファイル終了処理”を実行し、金融取引処理アプリケーションファイル 112Bをクローズする（図14ステップS56）。

利用者アプリケーション 210Bには、クレジット処理が完了した旨が表示され（図16（5））、必要に応じて、利用者アプリケーション 210Bを終了し（図16（6））、利用者アプリケーション 210Bが閉じられる（図16（7））。さらに、利用者アプリケーション 210Bのアイコン選択を解除する（図16（8））。

[0093] このように、本実施例2の金融取引制御システム 100Bの場合、カード媒体を伴わない電子クレジット利用や電子デビット利用のシステム構成においても、金融取引制御システム 100B、金融取引処理アプリケーション 110B、金融取引処理アプリケーションファイル 112B、暗証コード認証手段 120Bを用いて、金融取引処理に対する、ファイルオープン用の暗証コード、ファイルクローズ用の暗証コードを用いた認証処理を取り入れることができ、高いセキュリティレベルを獲得することができる。従来技術には、本願発明のように、利用者ごとのアプリケーションファイルを用いて、アプリケーションファイルを開く処理と、閉じる処理の2回にわたって暗証コードを要求する電子決済システムはない。高いセキュリティ処理の確実な実行が担保される。

なお、上記したステップS43において、オープン処理されている金融取引処理アプリケーションファイル 112Bがある利用者ID情報ではない場合は（図中には図示せず）、本発明の金融取引制御システム 100Bの利用者とは異なる他者の利用（つまり、本発明の利用者ではない一般の利用者）であるため、決済処理部 530に対して、決済処理開始OKの情報とともに金融取引情報を返し、決済処理部 530は、金融取引情報を基に、通常の決済処理を開始する。

実施例 3

[0094] 実施例3として、利用可否ステータス情報、利用可否ステータス情報状態

制御手段を備え、通常時に無効デフォルト処理を行ってセキュリティレベルを向上させた例を示す。ここでは、実施例2と同様、利用者ID保持媒体300を不要とした、いわゆる電子クレジット金融取引処理や電子デビット金融取引処理を行う例として示す。

[0095] 図17は実施例3にかかる金融取引制御システム100Cの構成例を示す図である。図17に示すように、実施例3にかかる金融取引制御システム100Cは少なくとも金融取引処理アプリケーション110C、暗証コード認証手段120Cを備えている。

ここで、本実施例3では、金融取引処理アプリケーション110Cが、利用可否ステータス情報状態制御手段111Cと、利用者ごとまたは金融取引ごとに用意される利用者アプリケーションファイル112Cを備えた構成となっている。

[0096] 利用可否ステータス情報状態制御手段111Cは、金融取引処理アプリケーション110Cが利用者端末200Cの利用者アプリケーション210Cから受け取った金融取引情報のリクエストに基づいて、決済管理システム500Cで管理されている利用可否ステータス情報510Cの有効／無効の状態の切り替えを制御する手段である。

[0097] ここで、利用可否ステータス情報510Cとは、決済管理システム500C上で管理される利用者のアカウントの有効無効状態、または、利用者のアカウントに対する金融取引受け入れの有効無効状態を示す情報である。

利用可否ステータス情報510Cは、与信管理部520により管理されており、この利用可否ステータス情報510Cが有効状態を示す場合、決済管理システム500Cは、当該利用者によるクレジット利用またはデビット利用を伴う金融取引を受け入れる取り扱いとなっている。逆に、この利用可否ステータス情報510Cが無効状態を示す場合、決済管理システム500Cは、当該利用者によるクレジット利用またはデビット利用を伴う金融取引を拒否する取り扱いとなっている。

本来は、与信に問題がないクレジット利用者、デビット利用者の利用可否

ステータス情報 510C は有効状態に維持するが、本発明では、金融取引制御システム 100C の利用可否ステータス情報状態制御手段 111C により、利用可否ステータス情報 510C の状態制御がなされる仕組みとなっている。

[0098] 利用可否ステータス情報状態制御手段 111C は、「無効デフォルト処理」と「ステータス情報切り替え処理」を備えている。

「無効デフォルト処理」は、利用可否ステータス情報状態制御手段 111C が決済管理システム 500C の利用可否ステータス情報 510C の状態をデフォルト（通常時状態）として無効状態にするものであり、この無効デフォルト処理により、利用可否ステータス情報 510C の状態がデフォルト設定として“無効状態”に制御される。

[0099] 「ステータス情報切り替え処理」は、利用者が保持する利用者端末 200C の利用者アプリケーション 210C から送信される金融取引のリクエスト情報や承認情報を受けて、利用可否ステータス情報 510C の無効状態/有効状態をオンデマンドで切り替える処理である。つまり、金融取引処理アプリケーション 110C は、利用可否ステータス情報状態制御手段 111C の「ステータス情報切り替え処理」によって、利用可否ステータス情報 510C のデフォルト設定である無効状態をオンデマンドで一時的に有効状態に切り替えたり、一時的に有効状態になったものを「無効デフォルト処理」によってデフォルト設定である無効状態に切り戻したりすることができる。

[0100] 従来技術では、一般的にはこの利用可否ステータス情報 510C は有効状態であることが通常状態であり、無効状態である場合は何らかの異常状態や事故状態に陥っているものであった。例えば、クレジットカードやデビットカードなどが盗難や紛失したため利用者から金融機関や信販会社の決済センターに対して、それらカード類を使用できないように使用停止の要求が出されている場合や、利用者のクレジット利用やデビット利用を伴う過去の金融取引の口座引き落としが不能で当該利用者の与信がなくなった場合など何らかの異常状態に陥っている場合が想定されている。

しかし、本発明では、金融取引制御システム１００Ｃは、金融取引処理アプリケーション１１０Ｃを装備し、利用可否ステータス情報状態制御手段１１１Ｃにより、決済管理システム５００Ｃ上で管理されている利用可否ステータス情報５１０Ｃの有効無効状態を利用者の金融取引処理の間だけ細かく切り替え制御を認めることで、クレジット利用またはデビット利用を伴う金融取引のセキュリティを向上せしめるものである。

[0101] 従来の決済管理システム５００Ｃの管理では、利用可否ステータス情報５１０Ｃは通常時（デフォルト設定時）は“有効状態”が維持され、何らかの不都合が発生した場合にのみ例外的に“無効状態”に切り替えられるものであった。

しかし、本発明では、従来とは発想を逆転させ、利用可否ステータス情報状態制御手段１１１Ｃは、利用可否ステータス情報５１０Ｃのデフォルト設定を“無効状態”として制御する「無効デフォルト処理」を行う。つまり、利用可否ステータス情報５１０Ｃは通常時（デフォルト設定時）は、利用可否ステータス情報状態制御手段１１１Ｃにより“無効状態”に維持される。これにより、利用者が気付かないうちに第三者が不正使用を試みようとしてもクレジット利用やデビット利用ができず高いセキュリティが維持できる。

[0102] 金融取引処理アプリケーション１１０Ｃは金融取引処理の開始の際に利用者アプリケーション２１０Ｃから金融取引処理のリクエストを受け、金融取引処理の実行に伴い、一時的に利用可否ステータス情報５１０Ｃを有効状態に切り替え、金融取引処理が完了すれば、自動的に通常時無効状態に戻すものである。

[0103] 次に、利用者の与信情報に基づく決済管理システム側による無効設定との優劣について述べる。

上記のように、金融取引制御システム１００Ｃの利用可否ステータス情報状態制御手段１１１Ｃは、決済管理システム５００Ｃの利用可否ステータス情報５１０Ｃの有効／無効の状態の切り替えを制御する機能を備えているが、利用者の与信情報に基づく決済管理システム側による無効設定は書き換え

不可とすることが好ましい。与信情報に基づく無効設定は、利用者自身の支払い能力欠如が判明した状況や、利用者に与えられた決済の信用枠を超える取引がなされようとしている状況に基づいて、それ以上の金融取引の成立を阻止するための決済管理システム側からのいわば強制的措置であるので、この措置を利用者が自由に切り替えられる機能まで付与することは明らかに行き過ぎである。

そこで、決済管理システム500Cは、与信に基づく利用可否ステータス情報510Cの無効設定を優先するという原則で制御を実行する。

[0104] つまり、決済管理システム500C上の与信管理部520が管理する与信情報に基づいて設定される利用可否ステータス情報510Cの設定が“有効状態”を示す設定の場合には、決済管理システム500Cは、利用可否ステータス情報状態制御手段111Cによる利用可否ステータス情報510Cの切り替え制御を優先させて利用可否ステータス情報510Cの切り替えを受け入れる。一方、利用可否ステータス情報510Cの設定が“無効状態”を示す設定の場合、決済管理システム500Cが、当該“無効設定”を優先し、利用可否ステータス情報状態制御手段111Cによる利用可否ステータス情報510Cによる切り替え制御（つまり、有効状態への切り替え処理）を受け入れず、利用可否ステータス情報510Cの“無効状態”を維持する取り扱いとする。

[0105] 次に、金融取引処理アプリケーションファイル112Cを説明する。

金融取引処理アプリケーションファイル112Cは、金融取引処理アプリケーション110Cにより処理される利用者ごとまたは金融取引ごとに用意されるアプリケーションファイルである。金融取引処理アプリケーション110Cは金融取引処理アプリケーションファイル112Cを用いて以下の処理を実行する。

(11)利用者ごとまたは金融取引ごとに金融取引処理アプリケーションファイル112Cをオンデマンドでオープンする「オープン処理」、(12)金融取引処理アプリケーションファイル112Cのデータを編集する「編集処理」

、(13)利用者による「承認確認」の伺い処理および受付処理、(14)利用可否ステータス情報510Cの一時有効状態切り替え処理、(15)金融取引処理の決済管理システム500Cへの引き継ぎ処理、(16)利用可否ステータス情報510Cの無効状態切り替え処理、(17)金融取引処理アプリケーションファイル112Cのクローズ処理の各処理である。

[0106] (11) 金融取引処理アプリケーションファイル112Cのオープン処理
金融取引処理アプリケーションファイル112Cのオープン処理については、実施例1で示した(1)金融取引処理アプリケーションファイル112Aのオープン処理と同様であり、ここでは省略する。

[0107] (12) 金融取引処理アプリケーションファイル112Cのデータ編集処理

金融取引処理アプリケーションファイル112Cのデータ編集処理については実施例1で示した(2)金融取引処理アプリケーションファイル112Aのデータ編集処理と同様であり、ここでは省略する。

[0108] (13) 利用者に対する承認伺い処理および確認処理

利用者に対する承認伺い処理、承認確認処理とも、実施例1で示した(3)利用者に対する承認伺い処理、承認確認処理と同様でありここでは省略する。

[0109] (14) 利用可否ステータス情報510Cの一時有効状態切り替え処理

なお、承認確認処理で“承認情報”が確認されたこと、つまり、クローズ用の暗証コードが認証されたことを条件として、金融取引処理アプリケーション110Cは、利用可否ステータス情報状態制御手段111Cを介して、既に説明した利用可否ステータス情報510Cをデフォルト無効状態から一時有効状態へ切り替える“一時有効状態切り替え処理”を実行させる。

[0110] (15) 金融取引処理の決済管理システム500Cへの引き継ぎ処理

金融取引処理アプリケーション110Cは、“金融取引情報データ引き渡し処理”として、金融取引処理アプリケーションファイル112Cに記録された金融取引情報のデータ内容を決済管理システム530へ引き渡す。

なお、決済管理システム530は金融取引情報の引き渡しを受け、その後は通常の決済処理（利用可否ステータス情報の有効状態の確認、金融決済処理など）が行われる。

[0111] （16）利用可否ステータス情報510Cの無効状態切り替え処理

上記した金融取引処理の決済管理システム500Cへの引き継ぎ処理を実行した後、金融取引処理アプリケーション110Cは、利用可否ステータス情報状態制御手段111Cを介して、利用可否ステータス情報状態制御手段110Cによる、利用可否ステータス情報510Cのデフォルト無効状態へ切り戻す“デフォルト無効状態切り替え処理”が行われる。

[0112] （17）金融取引処理アプリケーションファイル112Cのクローズ処理

最後に、金融取引処理アプリケーション110Cによって金融取引処理アプリケーションファイル112Cをクローズする“金融取引処理アプリケーションファイル終了処理”が実行される。

ここでは、上記した（13）利用者に対する承認確認処理から（17）金融取引処理アプリケーションファイル112Cのクローズ処理まで、利用者から送信された“承認情報”に含まれるクローズ用の暗証コードが認証されれば、一気に連続処理し、金融取引処理アプリケーションファイルの終了処理まで実行する運用となっている。

[0113] 次に、フローチャートおよび図面を参照しつつ、実施例3にかかる金融取引制御システム100Cの処理の流れの概略を示す。なお、実施例1に示した金融取引制御システム100Aの処理の流れの概略と同様の部分、実施例2に示した金融取引制御システム100Bの処理の流れの概略と同様の部分については詳しい説明は省略することとする。

[0114] 以下、一連のクレジット利用、デビット利用の手続の流れを図18～図22のシステムブロック図を参照しつつ説明する。なお、図23と図24は実施例3にかかる金融取引制御システム100Cの利用者端末200Cでの操作画面の例を示す図である。それら図中には、適宜利用可否ステータス情報510Cの有効状態、無効状態の切り替えの様子が併せて図示されている。

[0115] 図18に示した流れは実施例1の図2に示した流れと同様で良い。つまり、クレジット利用の決済に先立つ利用者アプリケーション210Cの立ち上げ処理（図18ステップS51）、暗証コード入力手段230を介した“オープン暗証コード”の入力処理（図18ステップS52）、利用者アプリケーション210Cを用いた“金融取引処理リクエスト情報”の生成処理（図18ステップS53）、利用者アプリケーション210Cによる“金融取引処理リクエスト情報”と“オープン暗証コード”の金融取引制御システム100Cへの送信処理（図18ステップS54）、暗証コード認証手段120Cによるオープン暗証コードの認証処理（図18ステップS55）、利用者アプリケーション210Cによる金融取引処理アプリケーションファイルのオープン処理（図18ステップS56）、金融取引処理開始の準備完了の旨の利用者端末200Cへの返信処理（図18ステップS57）、クレジット利用開始OKの表示処理（図18ステップS58）までは実施例1の図2のステップS1からS8までと同様で良い。

[0116] 次に、店舗やECサイトでの金融取引利用に移る。

利用者は、上記のように、クレジット利用開始ボタン押下した後、“クレジット利用できます。”という表示があれば、クレジット利用を開始する。

図19に示した流れは実施例2の図11に示した流れと同様で良い。つまり、電子決済アプリケーション260Cから利用者媒体アカウント情報270Cの取り込み処理（図19ステップS59）、店舗端末/ECサイト400の金融取引情報生成手段420を介した金融取引情報の生成処理（図19ステップS60）、金融取引情報の決済管理システム500Cへの送信処理（図19ステップS61）、決済処理部530Cから金融取引情報の金融取引処理アプリケーション110Cへの引き渡し処理（図19ステップS62）、オープン処理されている金融取引処理アプリケーションファイル112Cと関連付けられている利用者ID情報が否かのチェック処理（図19ステップS63）、金融取引情報の金融取引処理アプリケーションファイル112Bへの編集・書き込み処理（図19ステップS64）は、実施例2の図11

に示したステップS 3 9からステップS 4 4までと同様で良い。

[0117] 次に、金融取引処理アプリケーションファイル1 1 2 Cの承認処理に進む。

まず、金融取引制御システム1 0 0 Cは“承認伺い処理”を実行する。

利用者アプリケーション2 1 0 Cに対して金融取引を承認して金融取引を正常終了させる承認終了処理を実行しても良いかを問う“承認リクエスト”を送信し、“承認リクエスト”に対する利用者アプリケーション2 1 0 Cからの“承認情報”の返信を待つ(図2 0ステップS 6 6)。

なお、この“承認伺い処理”は、金融取引制御システム1 0 0 Cが自律的に利用者アプリケーション2 1 0 Cに対して送信して“承認情報”の入力を待つ形でも良いし、利用者アプリケーション2 1 0 C側が金融取引制御システム1 0 0 Cに自発的にアクセスして“承認情報”の入力を行う形であっても良い。

[0118] 利用者端末2 0 0 Cは、“承認リクエスト”を受信すると、ディスプレイ上に「ご利用の取引内容をご確認ください」というメッセージと、商品購入代金、クレジット支払回数などのクレジット利用内容を表示し、“承認ボタン”を表示して押下を促す(図2 4 (1))。この例では“承認する”というボタンと“承認しない”というボタンが表示される。

利用者が“承認ボタン”を押下すると(図2 0ステップS 6 6、図2 4 (2))、利用者アプリケーション2 1 0 Cは、利用者に対してクローズ暗証コードの入力を要求するガイダンスを表示し(図2 4 (3))、利用者から暗証コード入力手段2 3 0を介して入力された“クローズ暗証コード”を得る(図2 0ステップS 6 7)。ここでは生体情報として指紋情報が入力されるものとする(図2 4 (4))。

なお、“承認しない”ボタンを押下した場合の運用は限定されないが、例えば、実施例1と同様、利用者アプリケーション2 1 0 Bはこの金融取引が利用者による正当な取引ではないとして(例えば、不正使用者による不正取引とみなして)、決済処理部5 3 0 Cには決済処理NGの旨を通知し、金融

取引処理を強制終了する。

[0119] なお、上記の図 18 の金融取引処理アプリケーションファイルのオープン処理から、図 19 の各処理を経て、図 20 の金融取引処理アプリケーションファイルのクローズ処理の流れは、利用者端末 200C と金融取引制御システム 100C との間でアクセスを維持したままでも良い。つまり、図 18 で説明した利用者アプリケーション 210C による金融取引処理アプリケーションファイル 112C のオープン処理において確立した利用者アプリケーション 210C と金融取引処理アプリケーション 112C とのアクセスが維持されたままとし、図 19 で説明した各処理を経て、図 20 および図 21 で説明する上記の金融取引処理アプリケーションファイル 112C のクローズ処理を開始し、“承認伺い処理”の段階に進んだことをもって利用者が利用者端末 200C を介して“承認情報”の入力、“クローズ暗証コード”の入力に進む形でも良い。

[0120] 金融取引制御システム 100C は、利用者端末 200C からの“承認情報”の返信（図 20 ステップ S68）を受けて“承認確認処理”を実行する。ここでは、この承認情報には“クローズ暗証コード”が設定されているので、“クローズ暗証コード”を抽出し、暗証コード認証手段 120C に入力し、クローズ暗証コードの認証処理を実行させる（図 20 ステップ S69）。暗証コード認証手段 120C は、利用者アプリケーション 210C から送信されてきた“クローズ暗証コード情報”と、決済管理システム 500C 上で登録されている“クローズ暗証コード情報”との認証処理を行い、認証処理に成功した場合は（図 20 ステップ S69：Y）、金融取引処理アプリケーション 110C に認証成功を通知し、認証処理に失敗した場合は（図中には図示せず）、利用可否ステータス情報状態制御手段 110C に認証不成立を通知し、利用可否ステータス情報状態制御手段 110C は金融取引情報のデータ内容を決済管理システム 530 へ引き渡す（図中には図示せず）。なお、ここでは利用可否ステータス情報 510C は一度も書き換えられることなく“デフォルト無効状態”のままであり、決済管理システム 530 が通常の

クレジット処理を実行するため、結局クレジット処理が不成立となる。

[0121] 認証に成功した場合、金融取引処理アプリケーション 110C は、与信管理部 520 が与信に基づいた場合の利用可否ステータス情報 510C の設定が“有効状態”つまり“無効状態の設定ではない”か否かをチェックし（図 20 ステップ S70）、与信管理部 520 の与信情報に基づく設定が“無効状態の設定ではない”場合には、決済管理システム 500C は、利用可否ステータス情報状態制御手段 111C による利用可否ステータス情報 510C の切り替え制御を実行する（図 20 ステップ S71）。

[0122] なお、切り替え制御は、利用可否ステータス情報状態制御手段 111C が利用可否ステータス情報 510C の状態を直接切り替えるプログラムでも良く、利用可否ステータス情報状態制御手段 111C が決済管理システム 500C の与信管理部 520 に利用可否ステータス情報 510C の状態の切り替えを依頼し、与信管理部 520 が利用可否ステータス情報 510C を切り替えるプログラムでも良い。

図 20 のステップ S70 の結果、利用可否ステータス情報 510C の状態は一時的に有効状態に切り替わる。

[0123] なお、与信情報に基づく与信管理部 520 による利用可否ステータス情報 510C の設定が“無効状態”を示す設定の場合は（図中には図示せず）、利用可否ステータス情報状態制御手段 110C は、当該与信管理部 520 による“無効設定”を優先し、利用者端末 200C から送信された承認終了処理にかかわらず、利用可否ステータス情報 510C の“無効状態”を維持する取り扱いとし、利用可否ステータス情報状態制御手段 111C は金融取引情報のデータ内容を決済管理システム 530 へ引き渡す（図示せず）。なお、ここでは利用可否ステータス情報 510C は一度も書き換えられることなく無効状態のままであるので、決済管理システム 530 が通常のクレジット処理を実行することはできず、結局クレジット処理が不成立となる。

[0124] 承認確認処理で“承認情報”が確認されたこと、つまり、クローズ用の暗証コードの入力を条件として、金融取引処理アプリケーション 110C は決

済処理OKの旨の情報とともに、金融取引処理アプリケーションファイル112Cの金融取引情報のデータ内容を決済管理システム530へ引き渡す（図21ステップS72）。

決済管理システム530は金融取引情報の引き渡しを受け、その後は通常の決済処理（利用可否ステータス情報の有効状態の確認、金融決済処理など）を開始する（図21ステップS73）。

[0125] 決済処理部530は、金融取引情報から利用者ID情報などクレジット利用に必要な諸情報および決済代金情報を抽出し、利用可否ステータス情報510Cの状態が有効状態であるか否かをチェックし（図21ステップS74）、利用可否ステータス情報510Cの状態が“有効状態”であれば、クレジット決済処理が実行され（図21ステップS75）、店舗端末/ECサイト400にクレジット利用が成立した旨を示す情報が返信される（図21ステップS76）。なお、決済処理部530において、利用可否ステータス情報510Cの状態が“無効状態”であれば（図中には図示せず）、クレジット決済処理が拒絶され、決済処理部530Cから店舗端末/ECサイト400にクレジット利用が不成立である旨を示す情報が返信される（図中には図示せず）。

[0126] 利用可否ステータス情報状態制御手段110Cは、利用可否ステータス情報510Cの通常時無効状態へ切り戻す“通常時無効状態切り替え処理”を自動的に実行する（図22ステップS77）。

金融取引処理アプリケーション110Cは、“金融取引処理アプリケーションファイル終了処理”を実行し、金融取引処理アプリケーションファイル112Cをクローズする（図22ステップS78）。

[0127] ここでは、図20のステップS69から図22のステップS78まで、利用者からの“承認情報”が確認されたこと、つまり、クローズ用の暗証コードの入力があれば、一気に連続処理し、金融取引処理アプリケーションファイルのクローズ処理まで実行する運用となっている。

このように、実施例3の金融取引制御システム100Cでは、クレジット

利用を実行すると、一連の処理として利用可否ステータス情報が無効状態に切り戻される。利用可否ステータス情報が無効状態に切り戻された旨の表示がされる（図 24（5））。

[0128] 必要に応じて、利用者アプリケーション 210C を終了し（図 24（6））、利用者アプリケーション 210C が閉じられる（図 24（7））。さらに、利用者アプリケーション 210C のアイコン選択を解除する（図 24（8））。

[0129] 以上、本発明の金融取引制御システム 100、その利用者アプリケーション 210 の構成例における好ましい実施形態を図示して説明してきたが、本発明の技術的範囲を逸脱することなく種々の変更が可能であることは理解されるであろう。

産業上の利用可能性

[0130] 本発明の金融取引制御システムは、種々のクレジット利用システム、種々のデビット利用システムに広く適用することができる。

符号の説明

- [0131]
- 100 金融取引制御システム
 - 110 金融取引処理アプリケーション
 - 111 利用可否ステータス情報状態制御手段
 - 112 金融取引処理アプリケーションファイル
 - 120 暗証コード認証手段
 - 200 利用者端末
 - 210 利用者アプリケーション
 - 220 データ入力手段
 - 230 暗証コード入力手段
 - 240 通信手段
 - 250 カメラ
 - 260 電子決済アプリケーション
 - 270 利用者媒体アカウント情報

- 3 0 0 利用者 I D 保持媒体
- 4 0 0 店舗端末/E C サイト
- 4 1 0 利用者情報入力手段
- 4 2 0 金融取引情報生成手段
- 4 3 0 通信手段
- 5 0 0 決済管理システム
- 5 1 0 利用可否ステータス情報
- 5 2 0 与信管理部
- 5 3 0 決済処理部
- 5 4 0 通信手段
- 5 6 0 利用者媒体アカウント情報

請求の範囲

[請求項1]

クレジット利用またはデビット利用の決済管理システムに適用される金融取引制御システムであって、

利用者のアカウントごとに生成された金融取引処理アプリケーションファイルと、前記利用者のアカウントに対する金融取引処理を制御する金融取引処理アプリケーションを備え、

前記金融取引処理アプリケーションファイルに、オープン処理に対するオープン暗証コードとクローズ処理に対するクローズ暗証コードが設定登録されており、

前記金融取引処理アプリケーションが、前記利用者端末より送信された前記金融取引処理リクエスト情報に含まれているオープン暗証コードを認証した後、当該利用者のアカウントに対する前記金融取引処理アプリケーションファイルをオープンするオープン処理と、

金融取引者から前記利用者のアカウントへの金融取引情報を受けて、前記金融取引処理アプリケーションファイルに前記金融取引情報を書き込む編集処理と、

前記利用者端末に対して前記金融取引情報を承認するか否かを問う承認リクエストを送信し、前記利用者端末からの承認情報の返信を待つ承認伺い処理と、

前記利用者端末より返信された前記承認情報に含まれているクローズ暗証コードを認証した後、前記金融取引処理アプリケーションファイルデータの前記決済管理システムへの引き渡し処理と、前記金融取引処理アプリケーションファイルのクローズ処理を実行することを特徴とする金融取引制御システム。

[請求項2]

前記オープン暗証コードが前記利用者の生体情報を含むものであり、

前記クローズ暗証コードが前記利用者の生体情報を含むものであることを特徴とする請求項1に記載の金融取引制御システム。

[請求項3] 前記金融取引に関する前記利用者ID情報が利用者媒体に保持されており、前記金融取引処理に際して前記利用者媒体を介して前記利用者ID情報がやり取りされる請求項1または2に記載の金融取引制御システム。

[請求項4] 前記金融取引に関する前記利用者ID情報が前記利用者端末に保持されており、前記金融取引処理に際して前記利用者端末を介して前記利用者ID情報がやり取りされる請求項1または2に記載の金融取引制御システム。

[請求項5] 前記金融取引処理アプリケーションが、前記利用者のアカウントの有効無効状態または金融取引受け入れ可否の状態を示す利用可否ステータス情報の切り替えを制御する利用可否ステータス情報状態制御手段を備え、

前記金融取引処理アプリケーションが、前記利用可否ステータス情報を通常時は無効状態に維持する前記利用可否ステータス情報状態制御手段を介した無効デフォルト処理を行い、

前記利用者端末からの前記承認情報の返信を条件として、前記利用可否ステータス情報の一時有効状態への切り替え処理と、前記引き渡し処理と、前記利用可否ステータス情報の前記無効デフォルト処理と、前記クローズ処理を連続処理することを特徴とする1から4のいずれかに記載の金融取引制御システム。

[請求項6] 前記決済管理システム上の与信情報に基づいて設定される前記利用者のアカウントの有効無効状態または前記利用者の前記アカウントに対する前記金融取引受け入れの有効無効状態を示す前記利用可否ステータス情報の設定が有効状態を示す設定の場合、前記決済管理システムが、前記利用可否ステータス情報状態制御手段による前記利用可否ステータス情報の切り替え制御を優先させて前記利用可否ステータス情報の切り替えを受け入れ、

前記決済管理システム上の前記与信情報に基づいて設定される前記

利用者のアカウントの有効無効状態または前記利用者の前記アカウントに対する前記金融取引受け入れの有効無効状態を示す前記利用可否ステータス情報の設定が無効状態を示す設定の場合、前記決済管理システムが、前記利用可否ステータス情報状態制御手段による前記利用可否ステータス情報の切り替え制御を受け入れず、前記利用可否ステータス情報の無効状態を維持することを特徴とする請求項5に記載の金融取引制御システム。

[請求項7]

前記決済管理システム上の与信情報に基づいて設定される前記利用者のアカウントの有効無効状態または前記利用者の前記アカウントに対する前記金融取引受け入れの有効無効状態を示す前記利用可否ステータス情報の設定が有効状態を示す設定の場合、前記決済管理システムが、前記利用可否ステータス情報状態制御手段による前記利用可否ステータス情報の切り替え制御を優先させて前記利用可否ステータス情報の切り替えを受け入れ、

前記決済管理システム上の前記与信情報に基づいて設定される前記利用者のアカウントの有効無効状態または前記利用者の前記アカウントに対する前記金融取引受け入れの有効無効状態を示す前記利用可否ステータス情報の設定が無効状態を示す設定の場合、前記決済管理システムが、前記与信情報に基づく前記利用可否ステータス情報の無効状態の設定を優先するか、前記利用可否ステータス情報状態制御手段による前記利用可否ステータス情報の切り替え制御を優先するかを選択可能としたことを特徴とする請求項5に記載の金融取引制御システム。

[請求項8]

前記利用者端末にインストールまたはA S Pで利用可能であり、請求項1から7のいずれかに記載の金融取引制御システムとやり取りする利用者アプリケーションであって、

前記金融取引処理リクエスト情報を作成する金融取引処理リクエスト情報作成処理と、作成した前記金融取引処理リクエスト情報を前記

金融取引処理アプリケーションに送信する金融取引処理リクエスト情報送信処理と、

前記承認情報を作成する承認情報作成処理と、作成した前記承認情報を前記金融取引処理アプリケーションに返信する承認情報返信処理を備えたことを特徴とする利用者アプリケーション。

[請求項9] 前記クレジット利用または前記デビット利用が、クレジットカードまたはキャッシュカードを用いて行われる金融取引であることを特徴とする請求項8に記載の利用者アプリケーション。

[請求項10] 前記クレジット利用または前記デビット利用が、非カード型のICデバイスまたは人体埋設型のマイクロICデバイスを用いて行われる金融取引であることを特徴とする請求項8に記載の利用者アプリケーション。

[請求項11] クレジット利用またはデビット利用の決済管理システムに適用される金融取引制御方法であって、

利用者のアカウントごとに生成された金融取引処理アプリケーションファイルと、前記利用者のアカウントに対する金融取引処理を制御する金融取引処理アプリケーションを用い、

前記金融取引処理アプリケーションファイルに、オープン処理に対するオープン暗証コードとクローズ処理に対するクローズ暗証コードが設定登録されており、

前記金融取引処理アプリケーションが、前記利用者端末より送信された前記金融取引処理リクエスト情報に含まれているオープン暗証コードを認証した後、当該利用者のアカウントに対する前記金融取引処理アプリケーションファイルをオープンするオープン処理と、

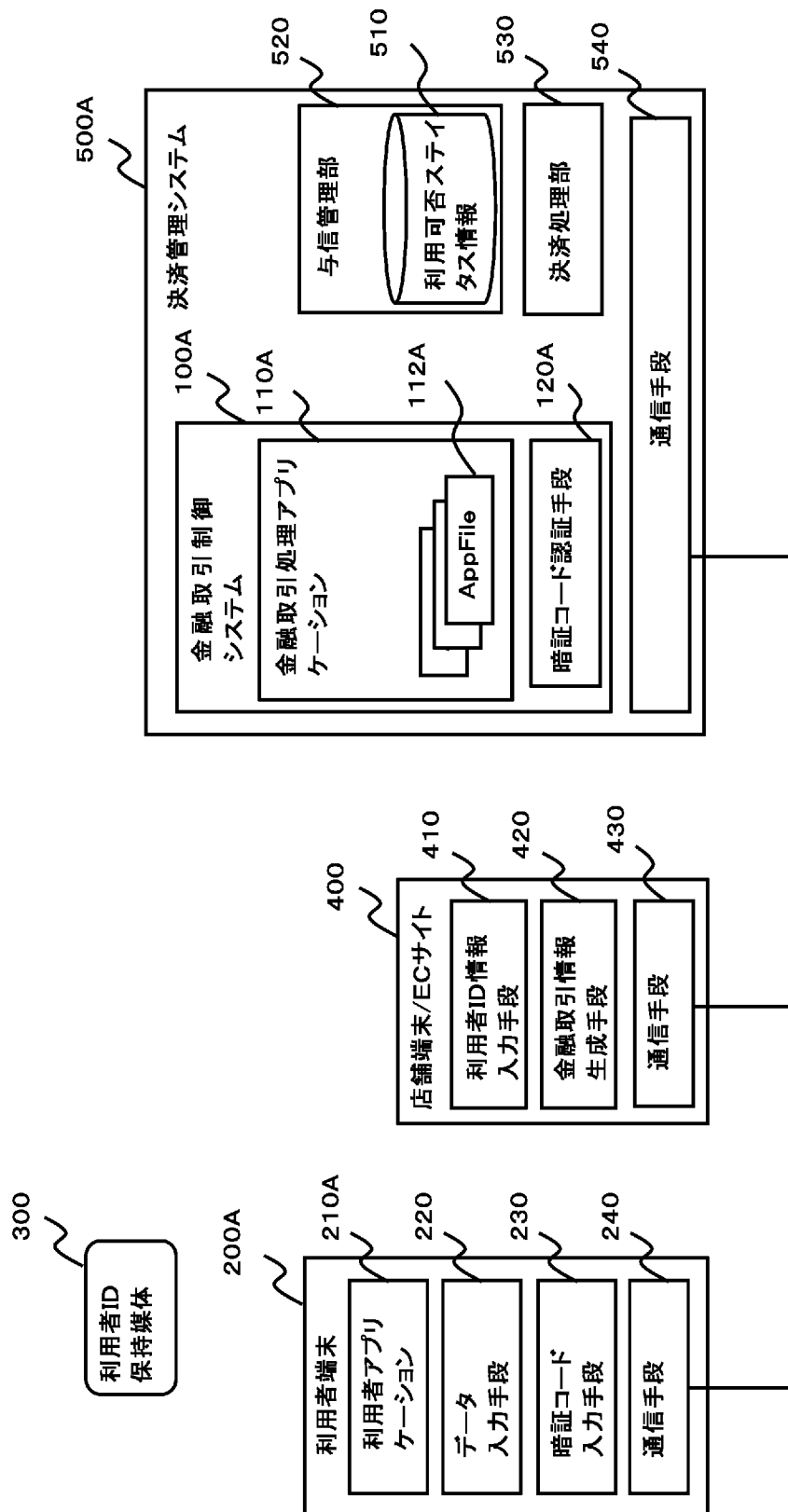
金融取引者から前記利用者のアカウントへの金融取引情報を受けて、前記金融取引処理アプリケーションファイルに前記金融取引情報を書き込む編集処理と、

前記利用者端末に対して前記金融取引情報を承認するか否かを問う

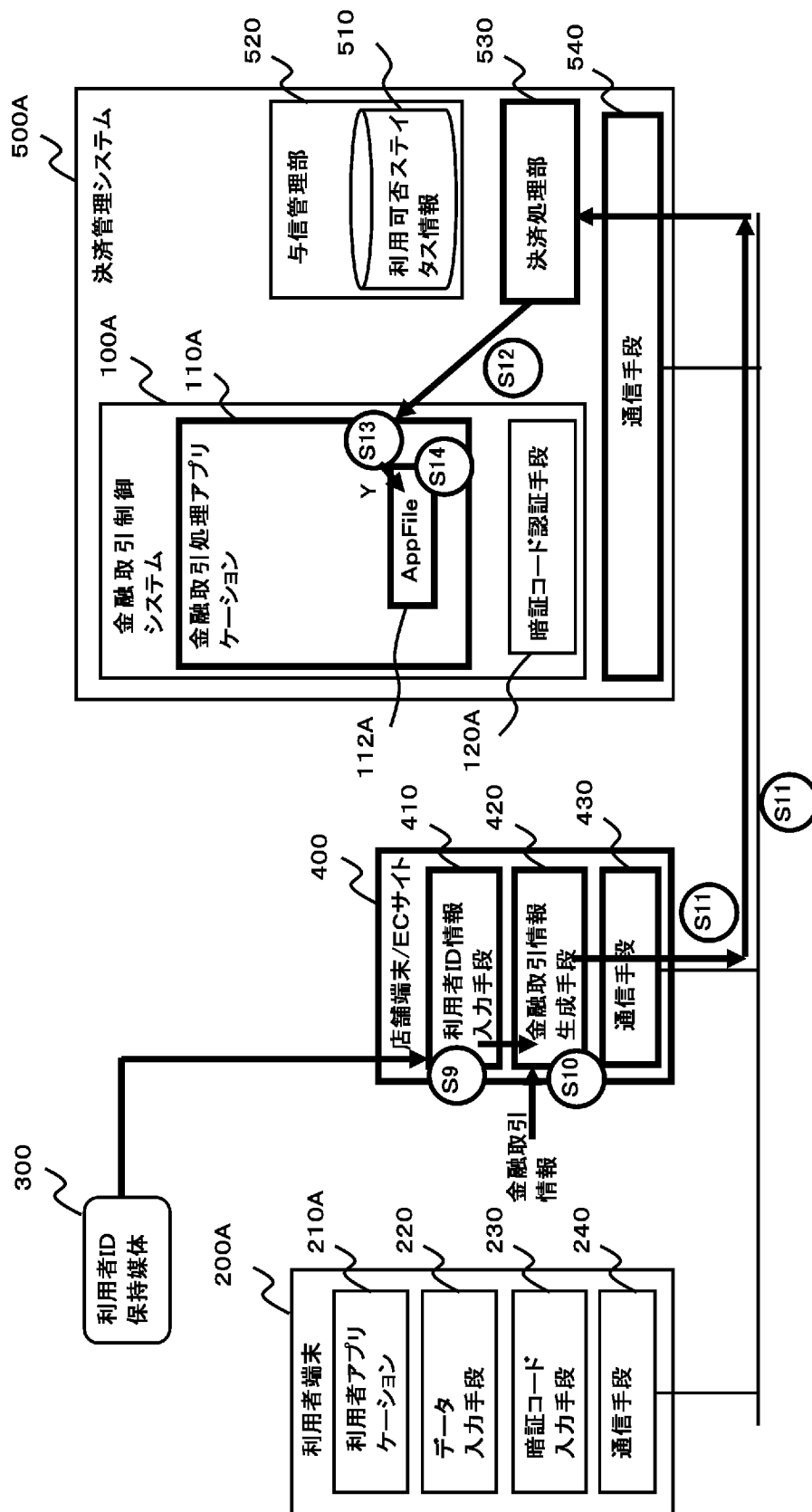
承認リクエストを送信し、前記利用者端末からの承認情報の返信を待つ承認伺い処理と、

前記利用者端末より返信された前記承認情報に含まれているクローズ暗証コードを認証した後、前記金融取引処理アプリケーションファイルデータの前記決済管理システムへの引き渡し処理と、前記金融取引処理アプリケーションファイルのクローズ処理を実行することを特徴とする金融取引制御方法。

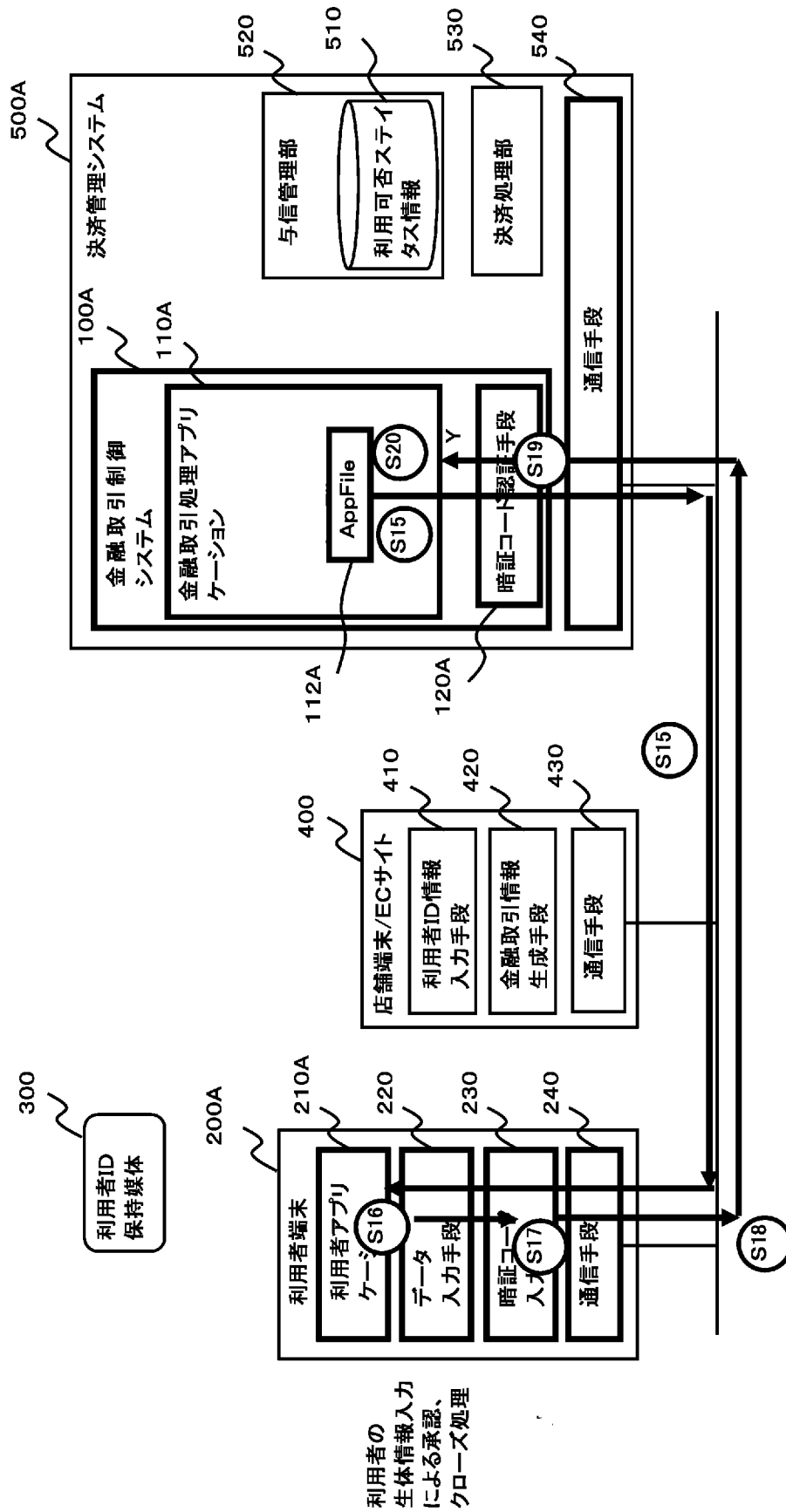
[図1]



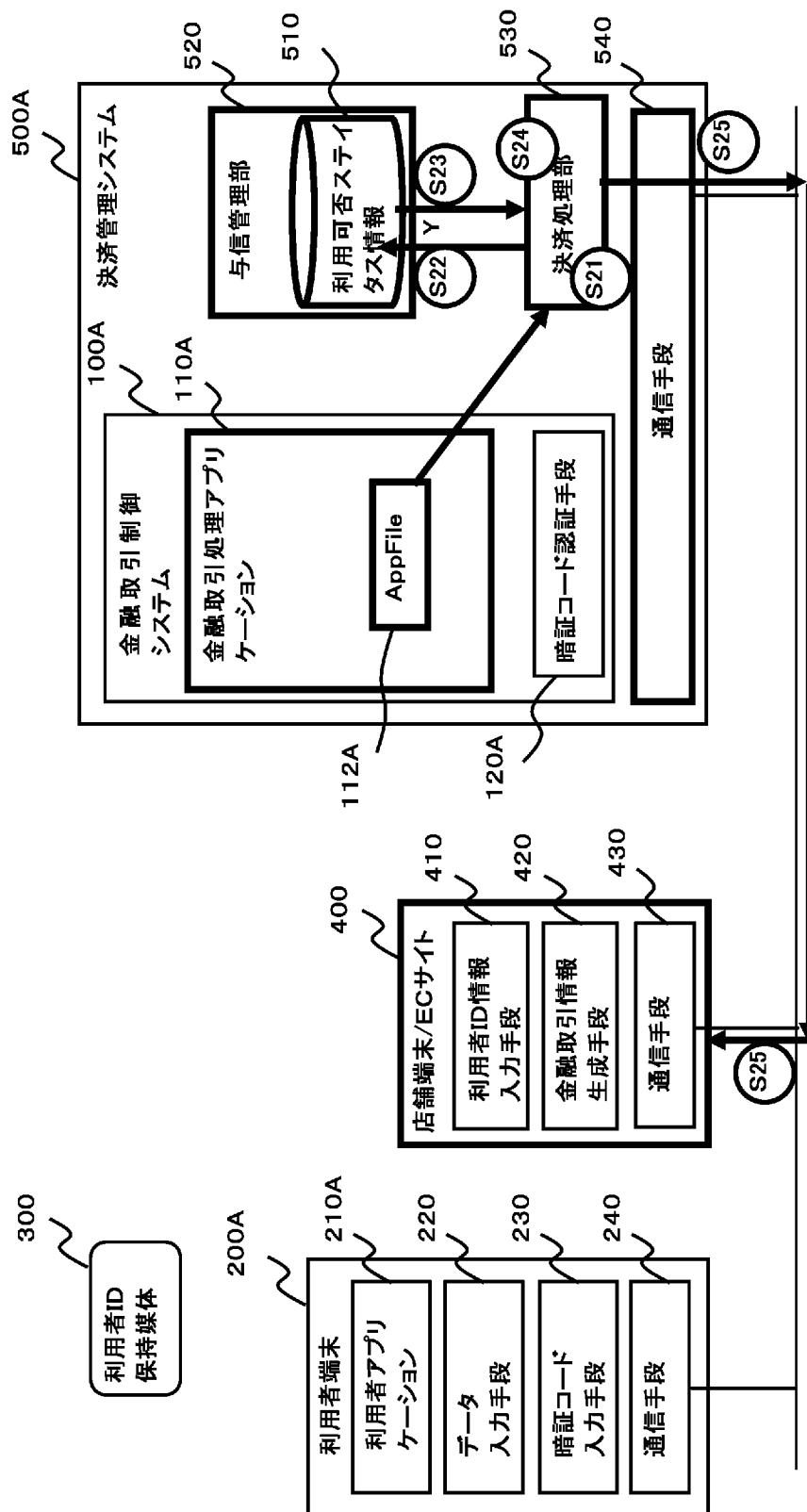
[図3]



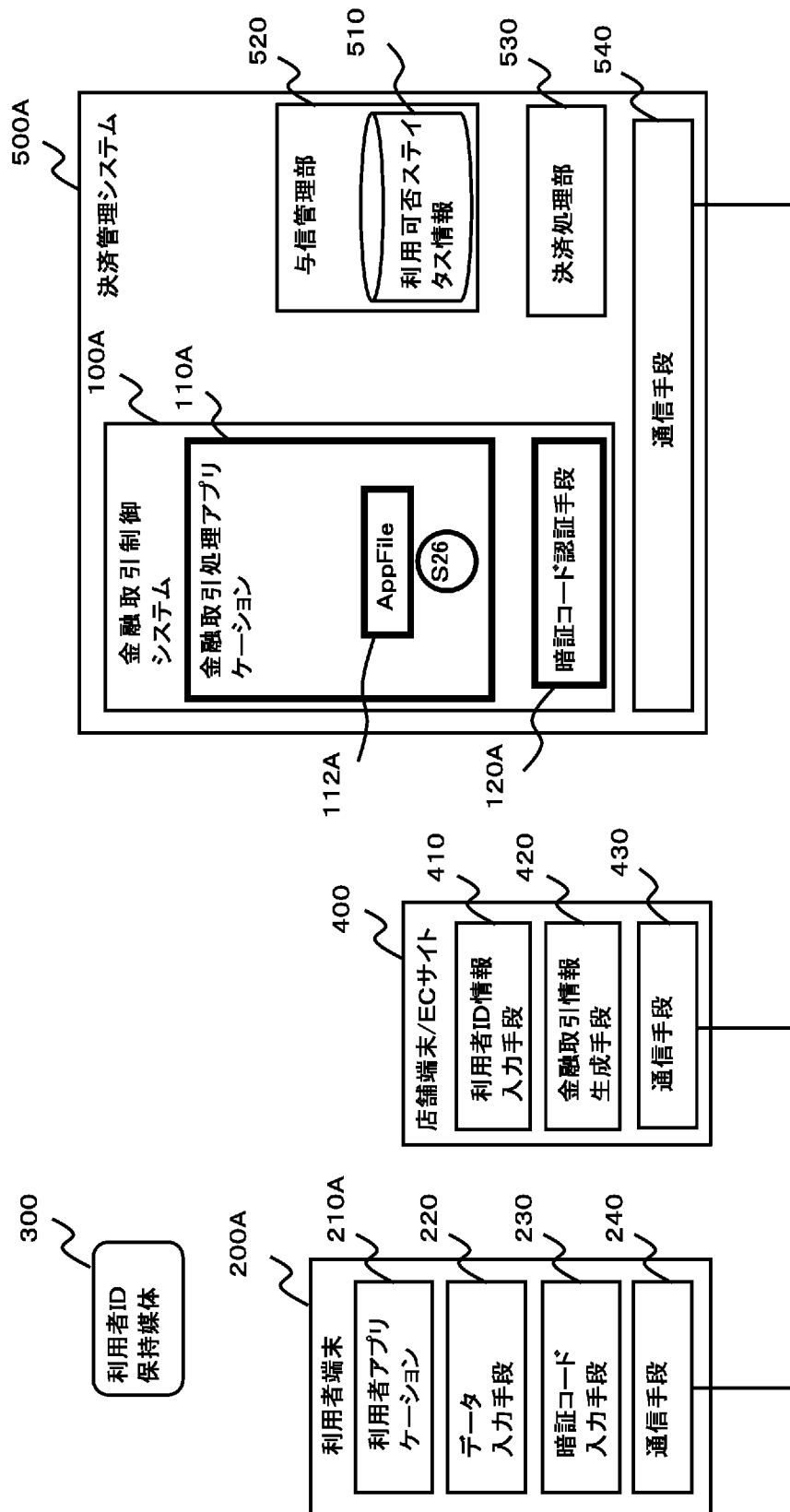
[図4]



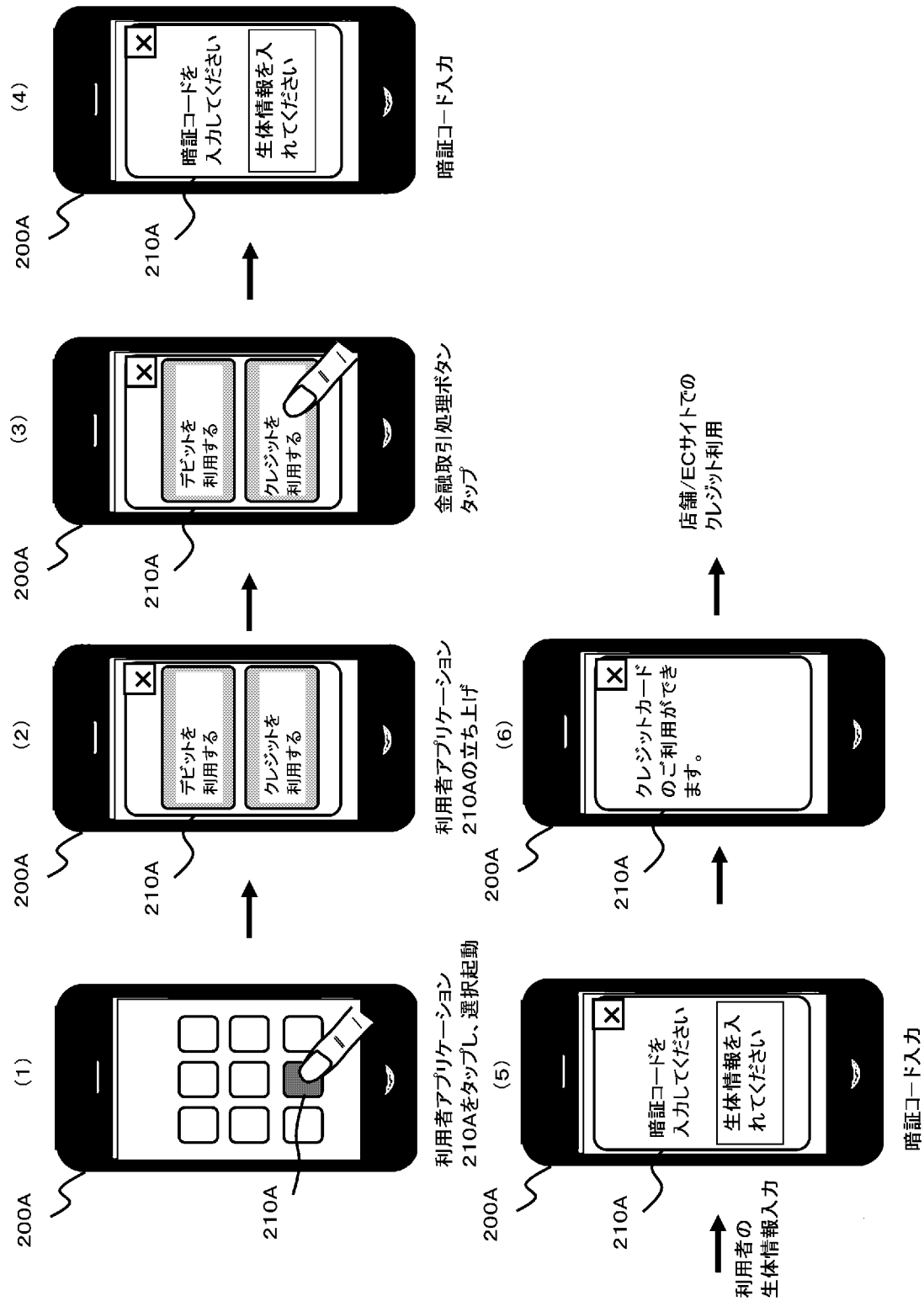
[図5]



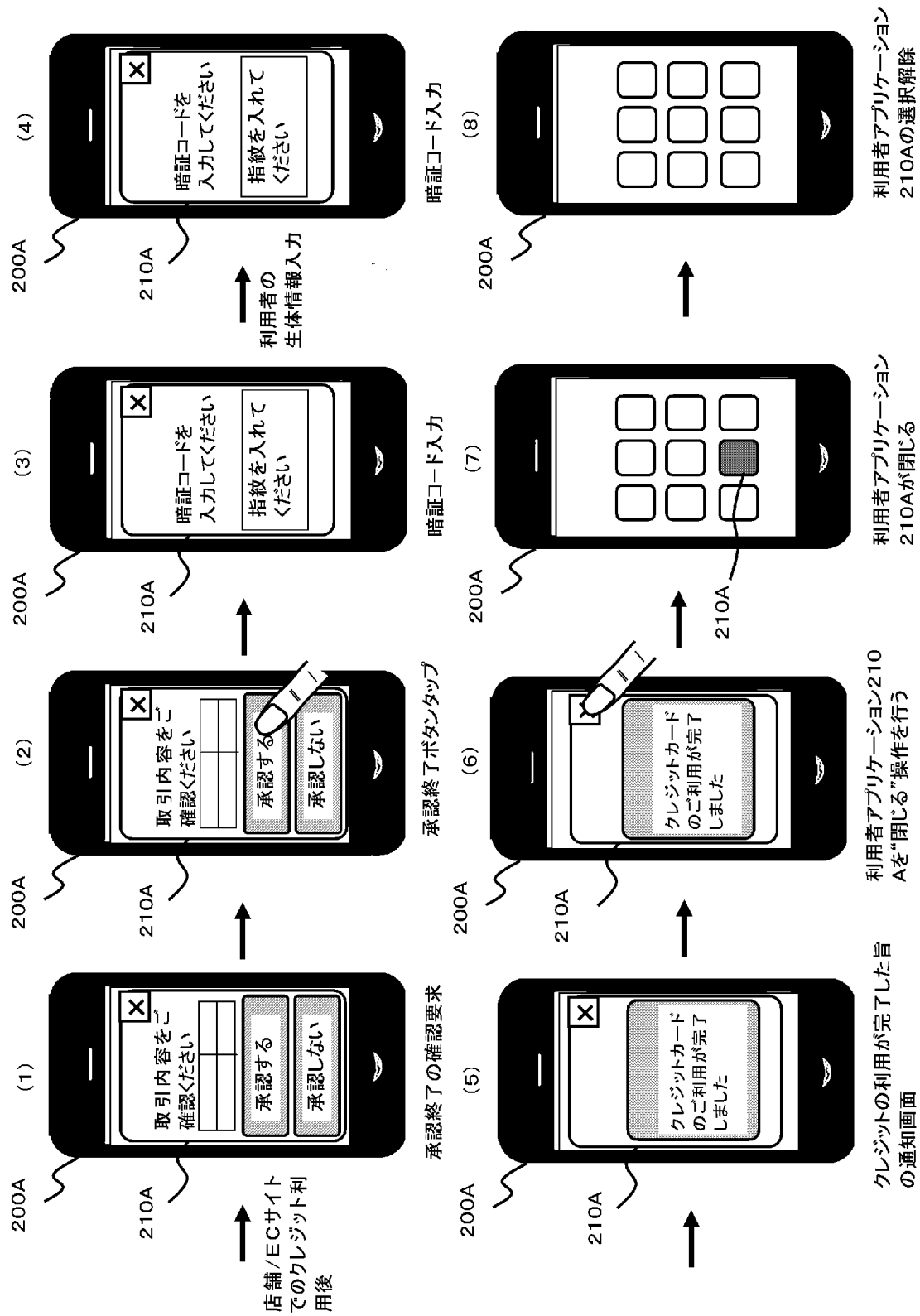
[図6]



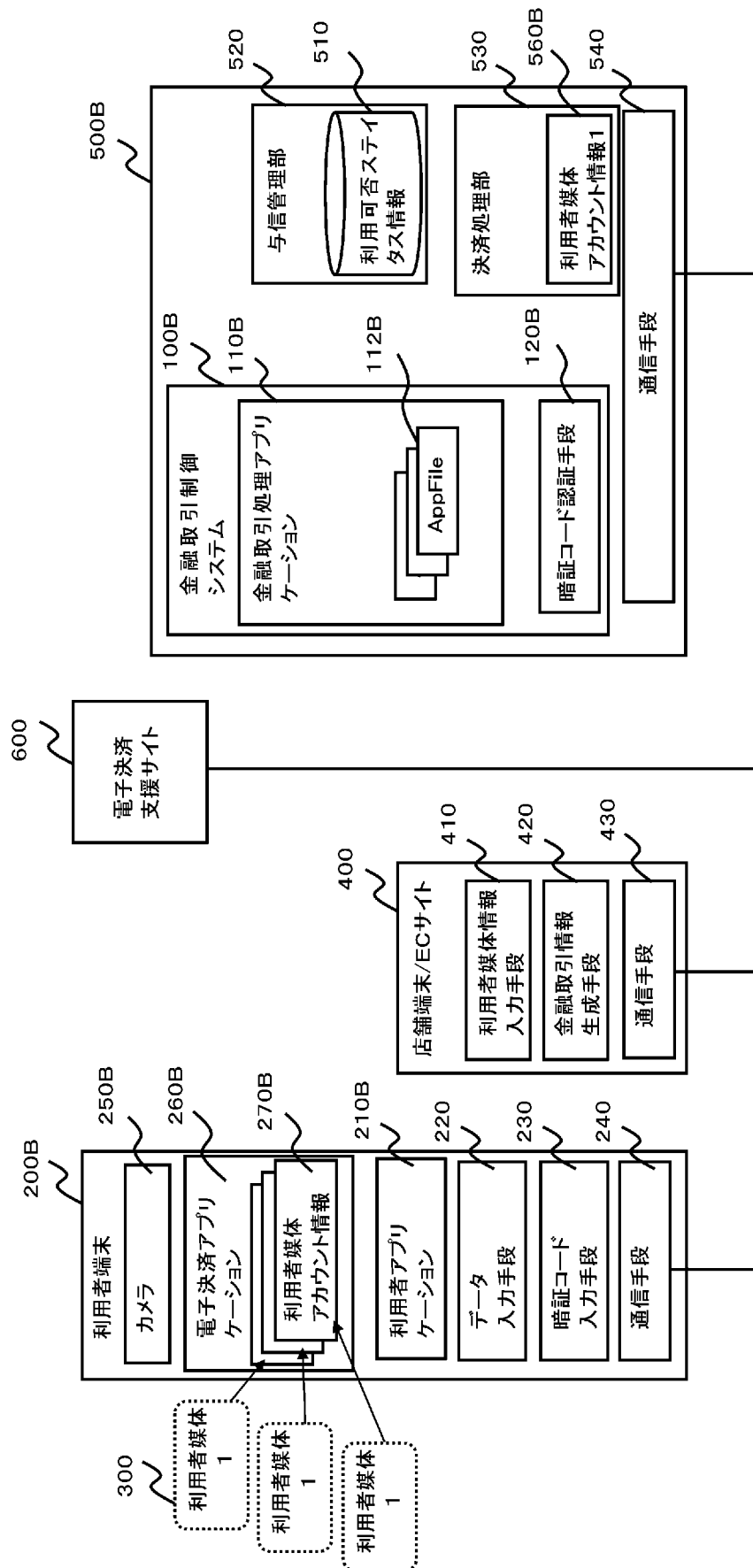
[図7]



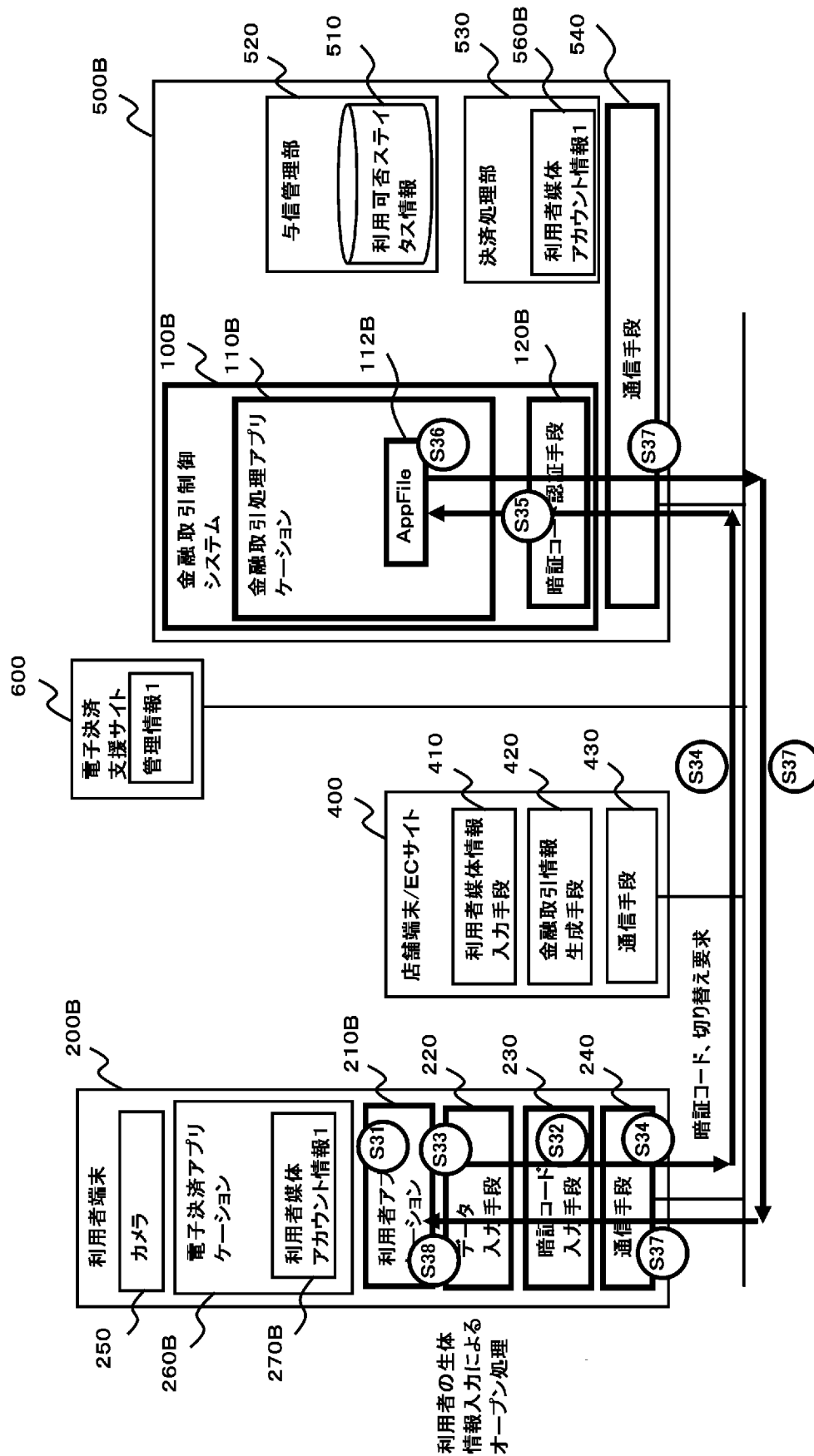
[図8]



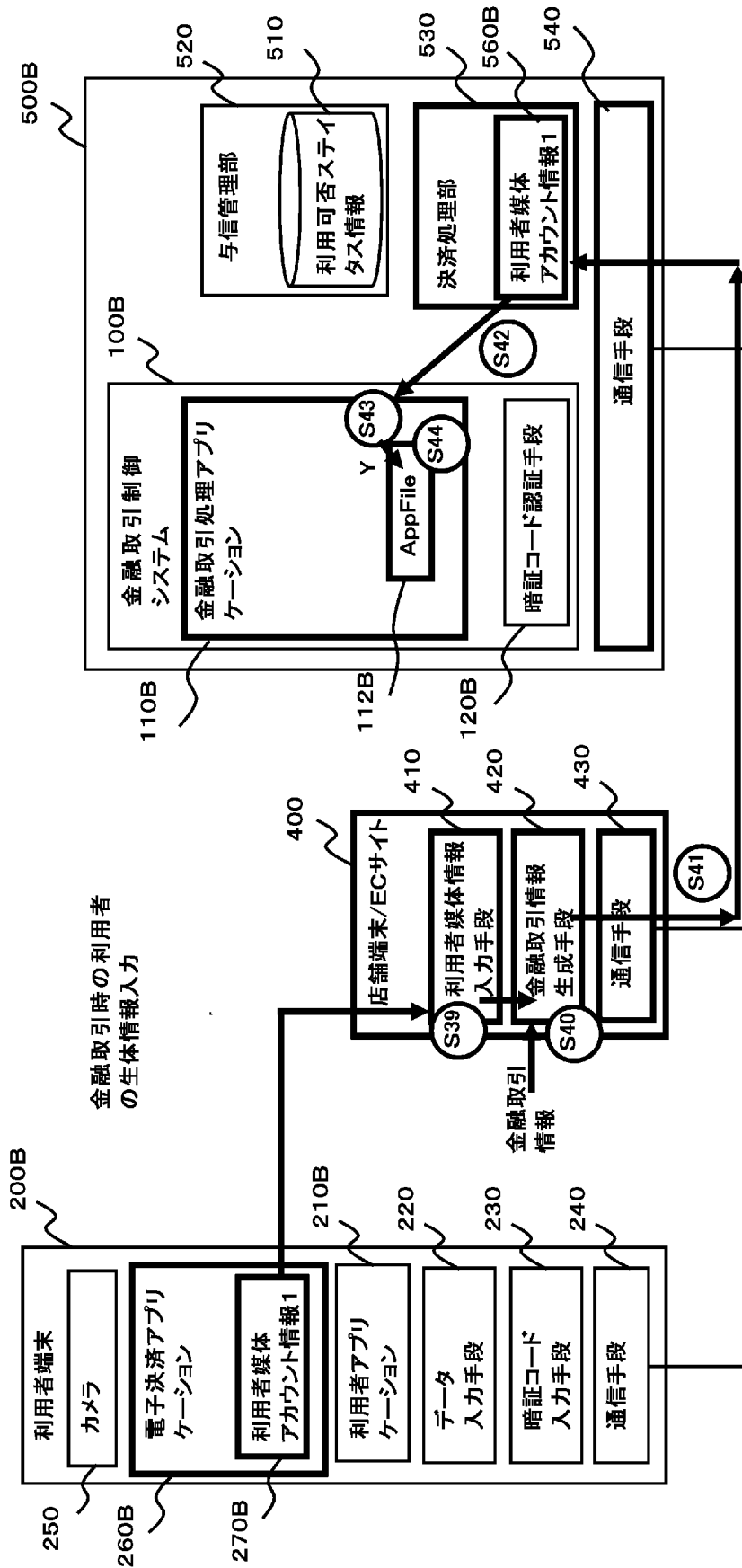
[図9]



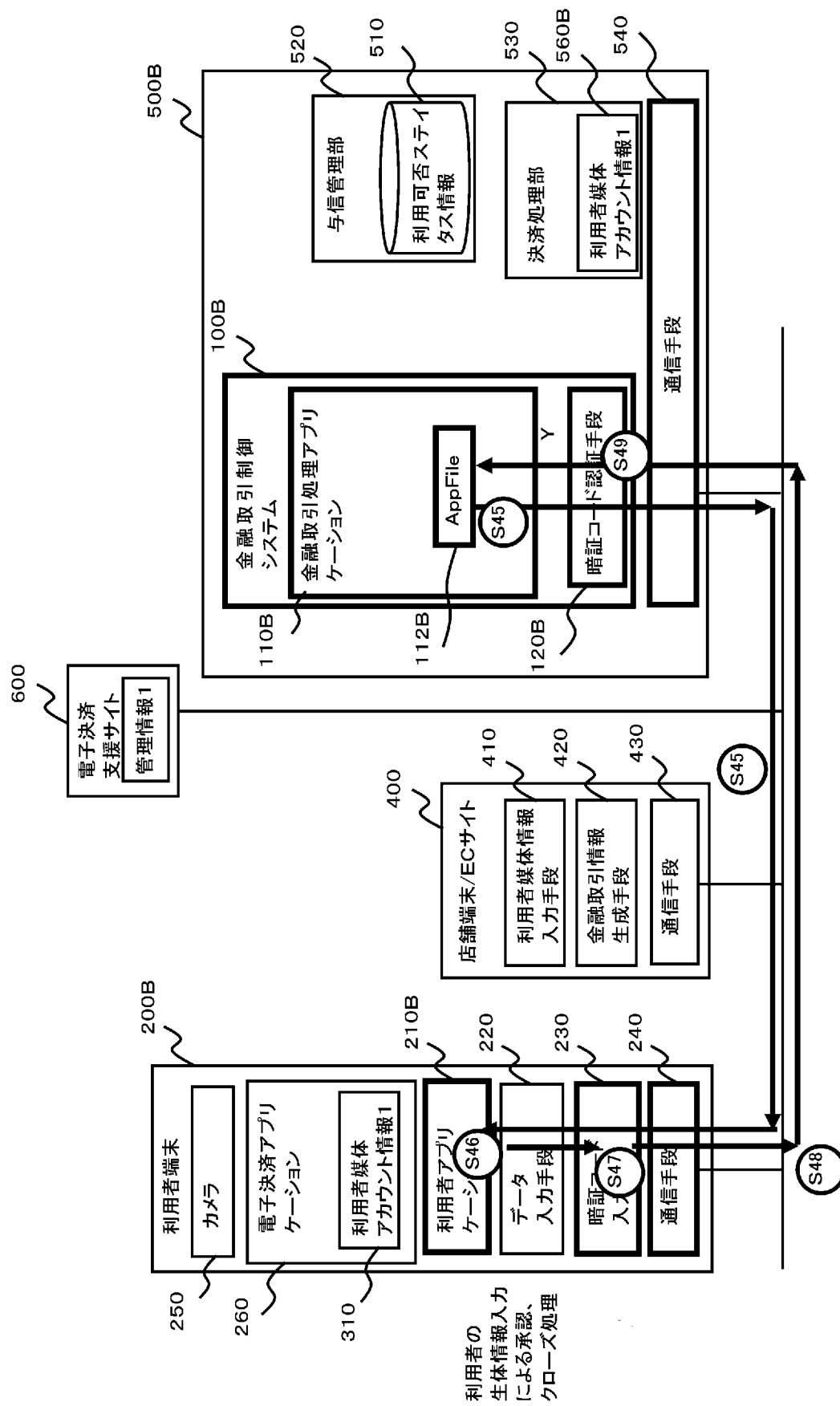
[図10]



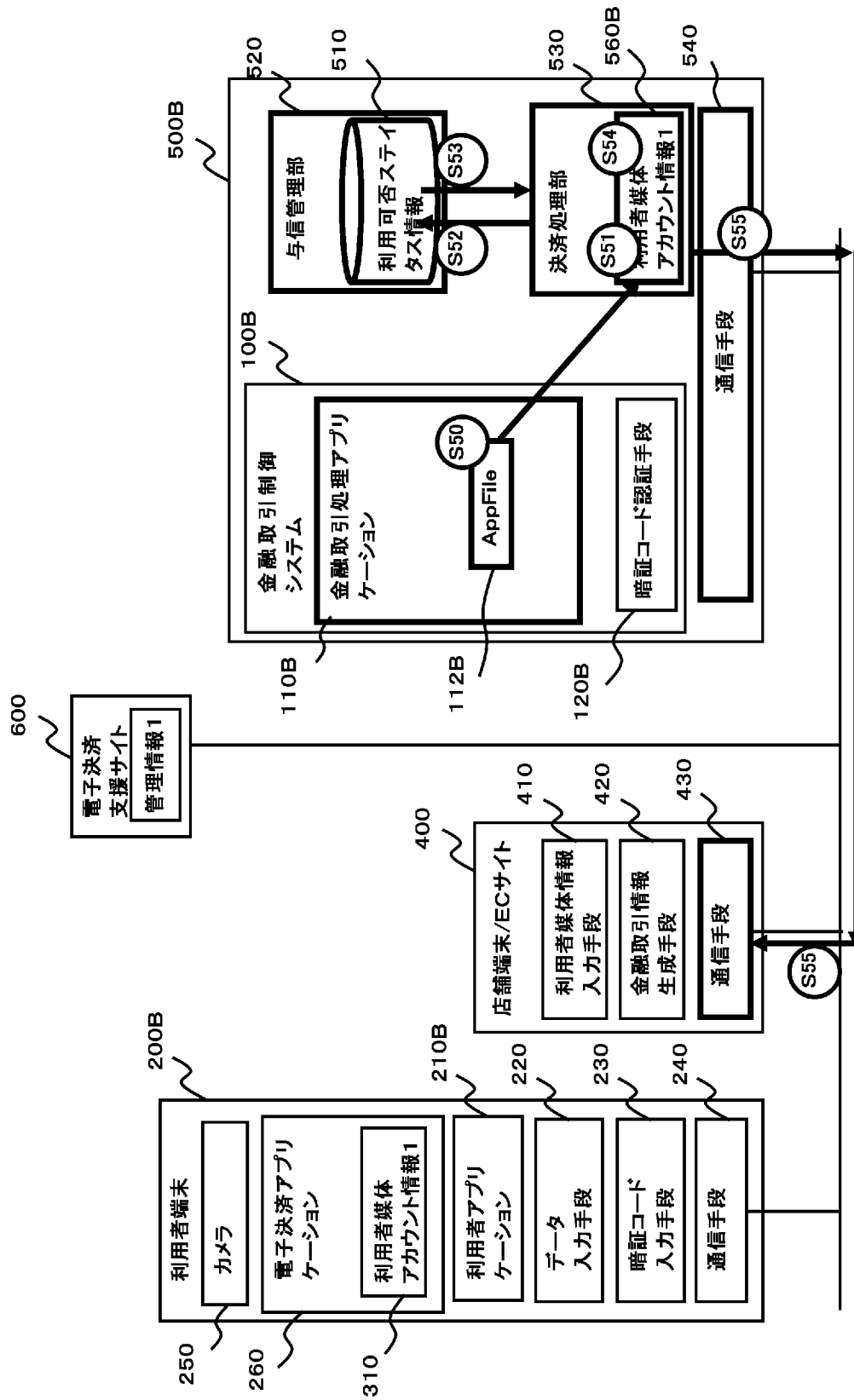
[図11]



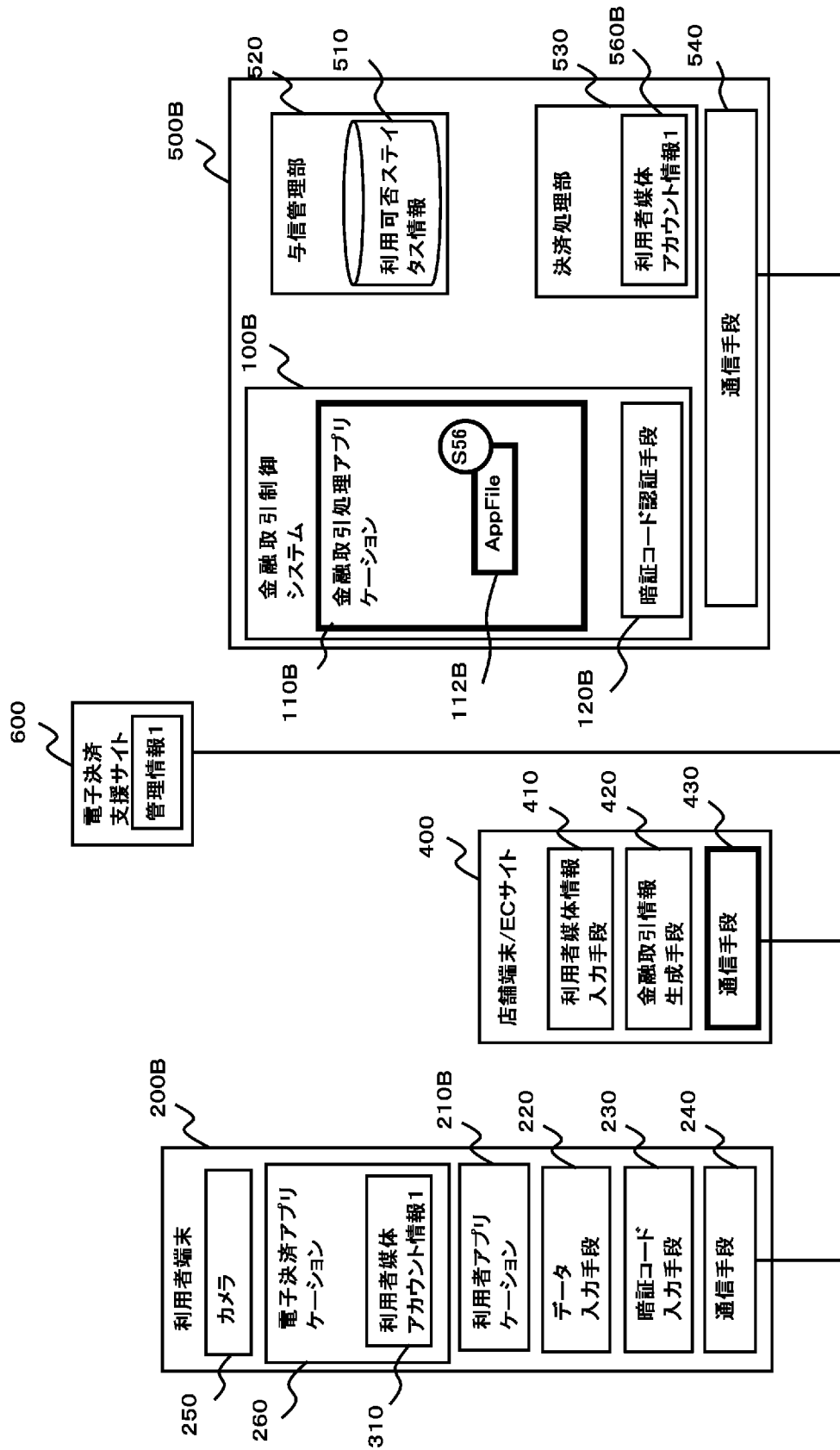
[図12]



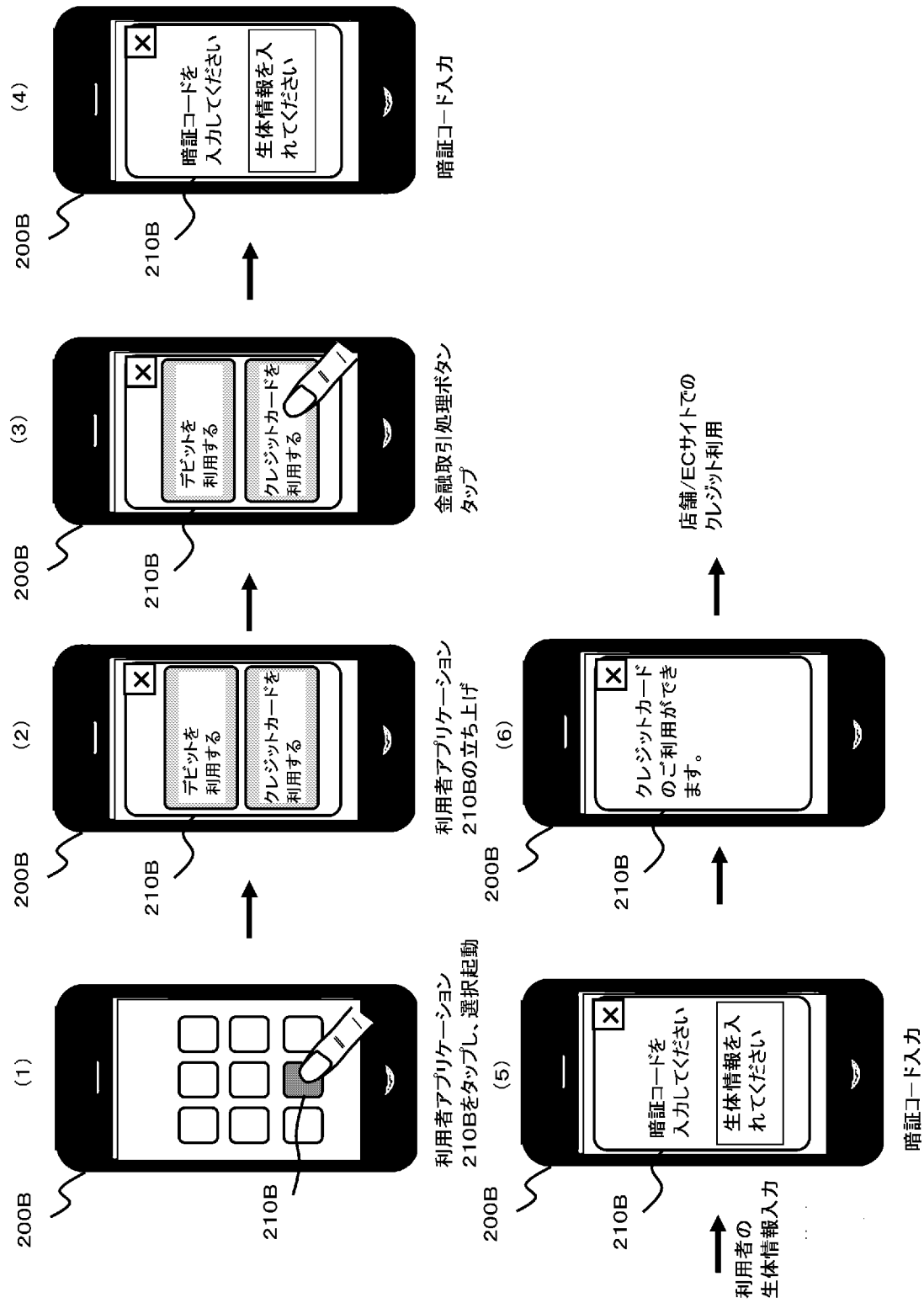
[図13]



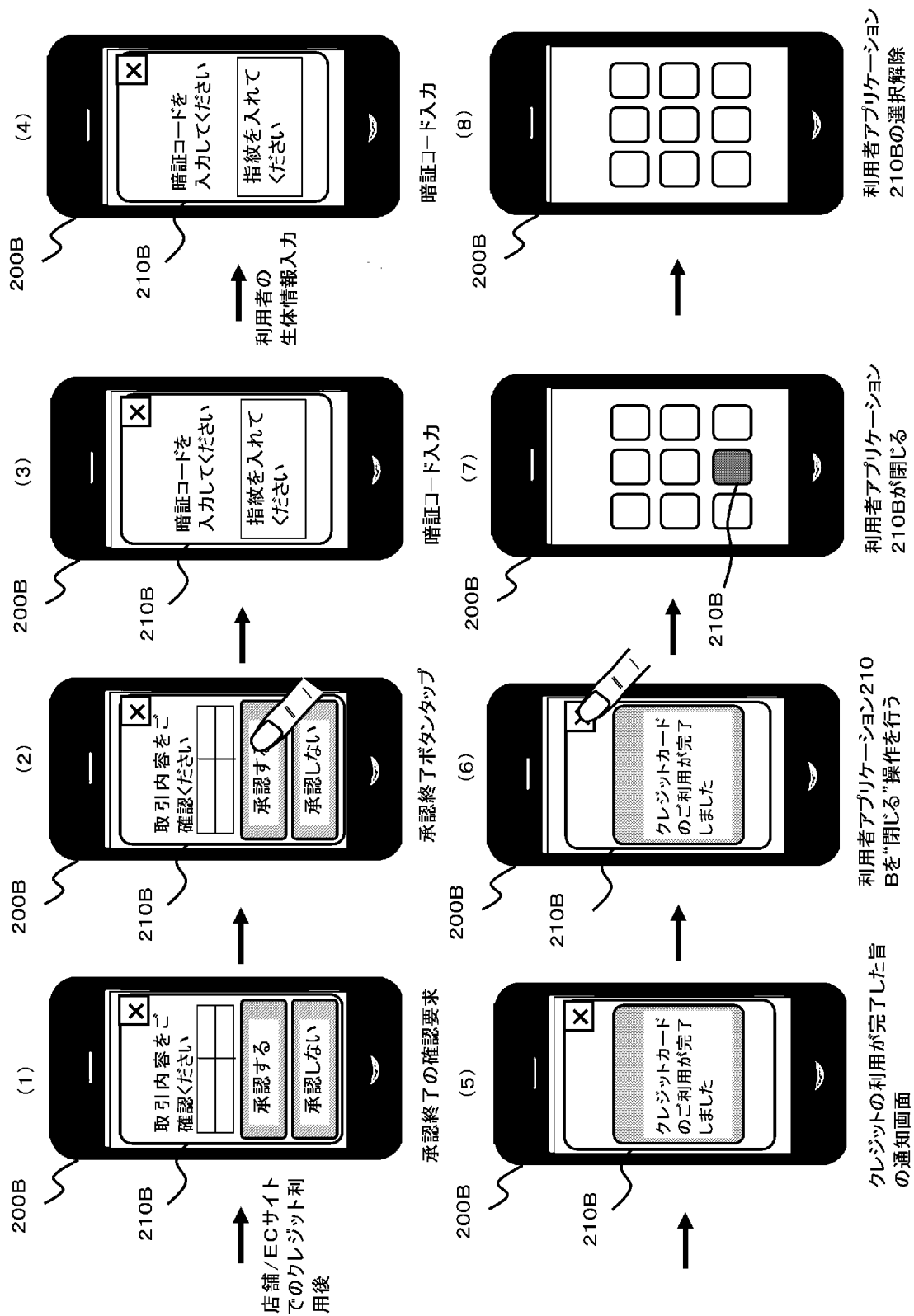
[図14]



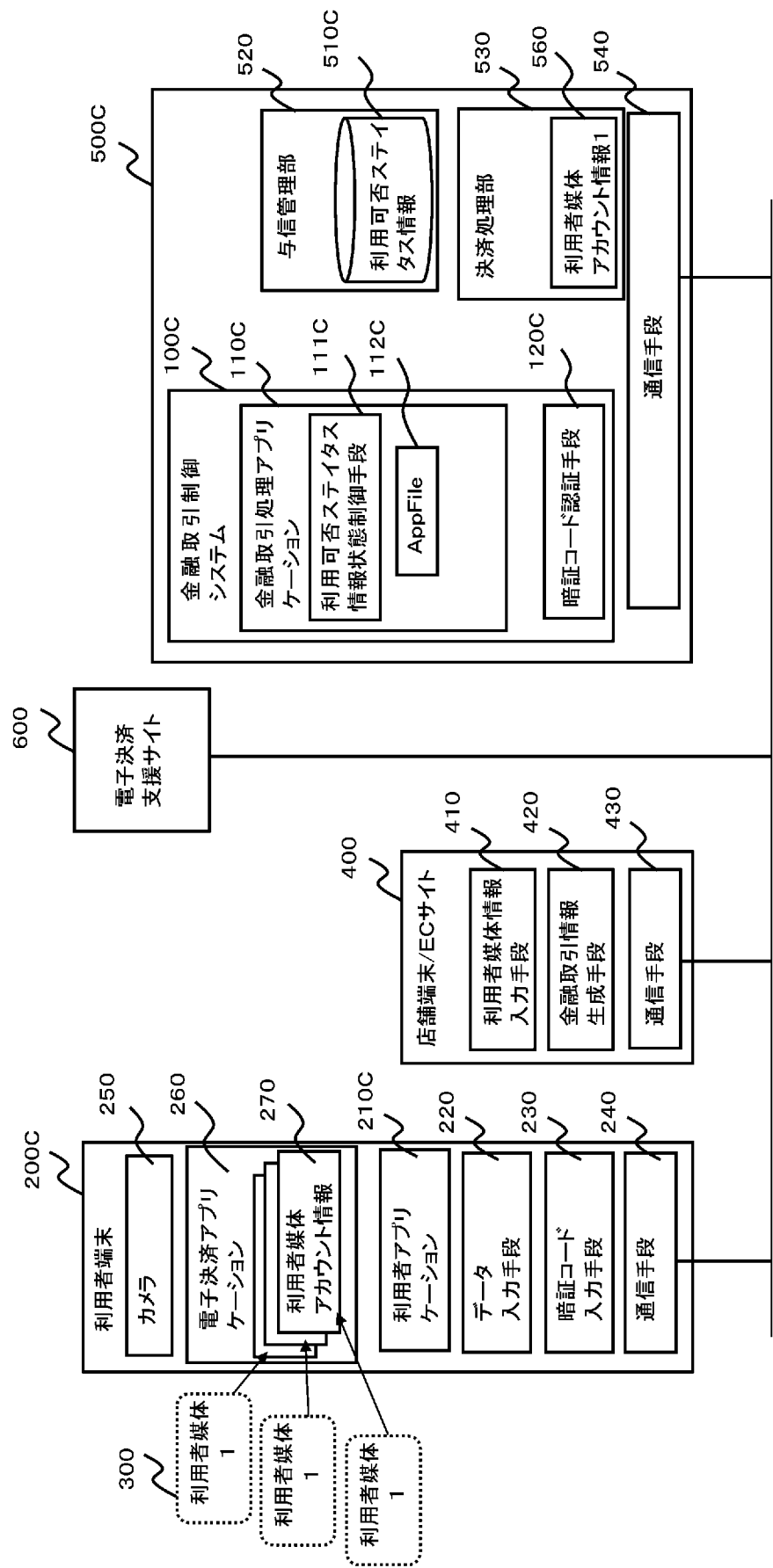
[図15]

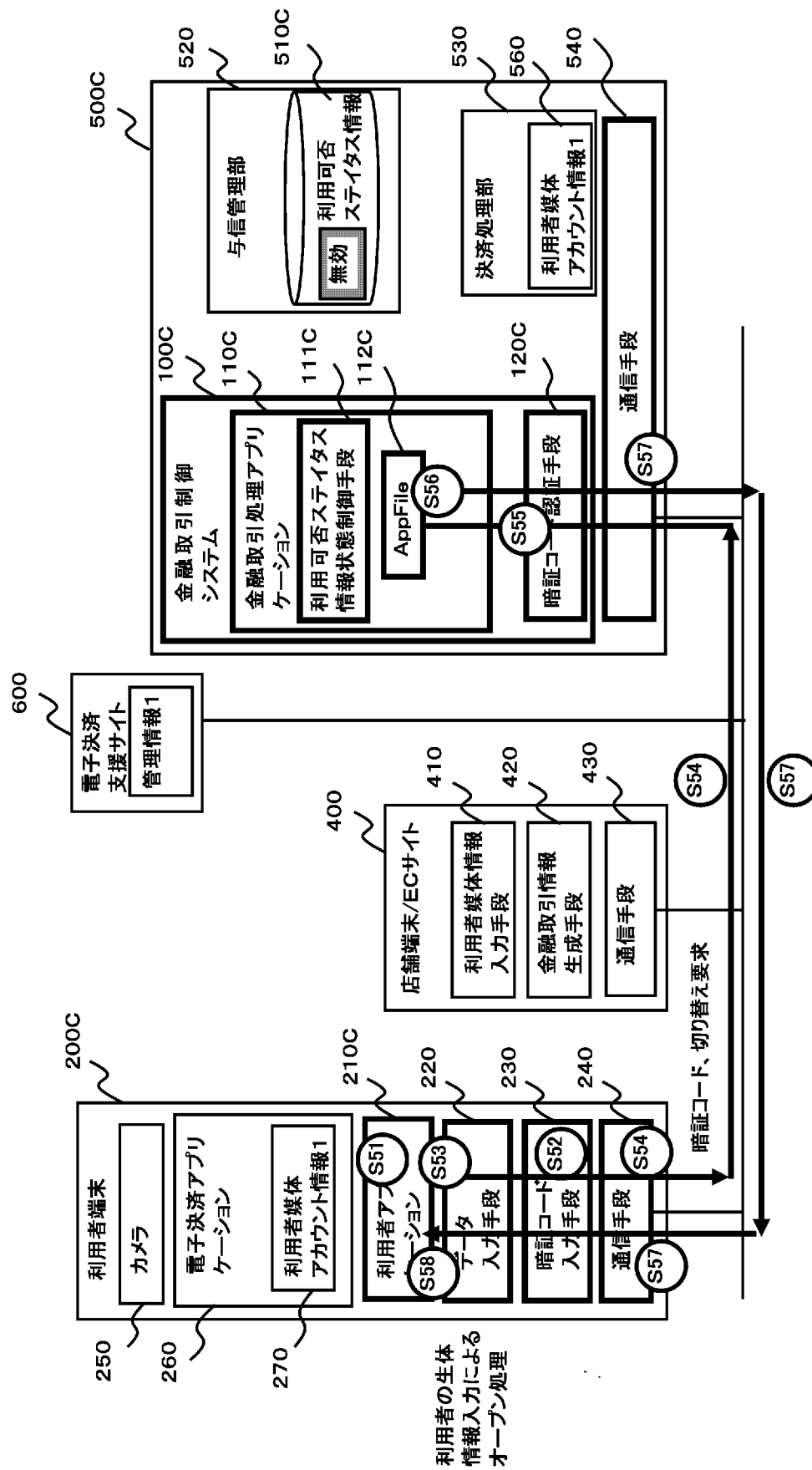


[図16]

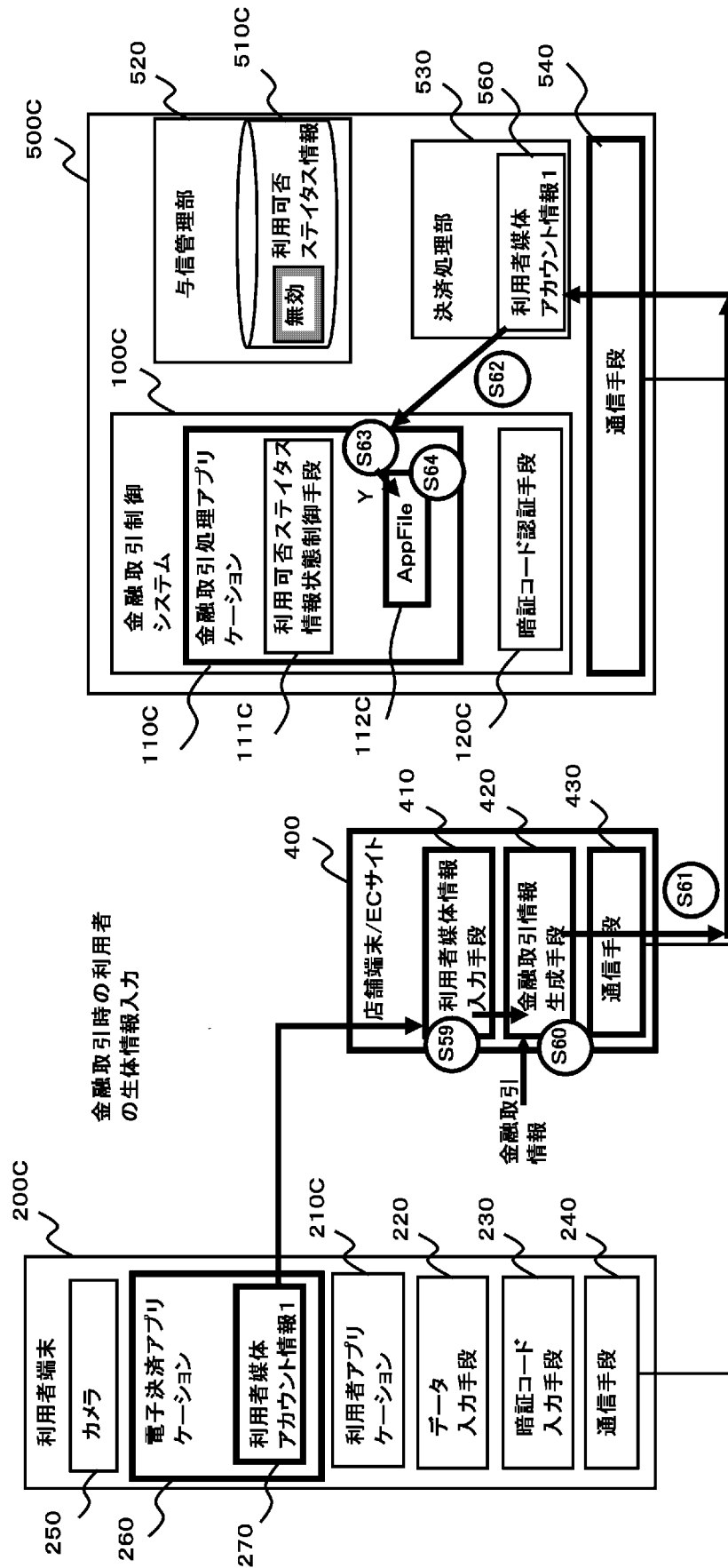


[図17]

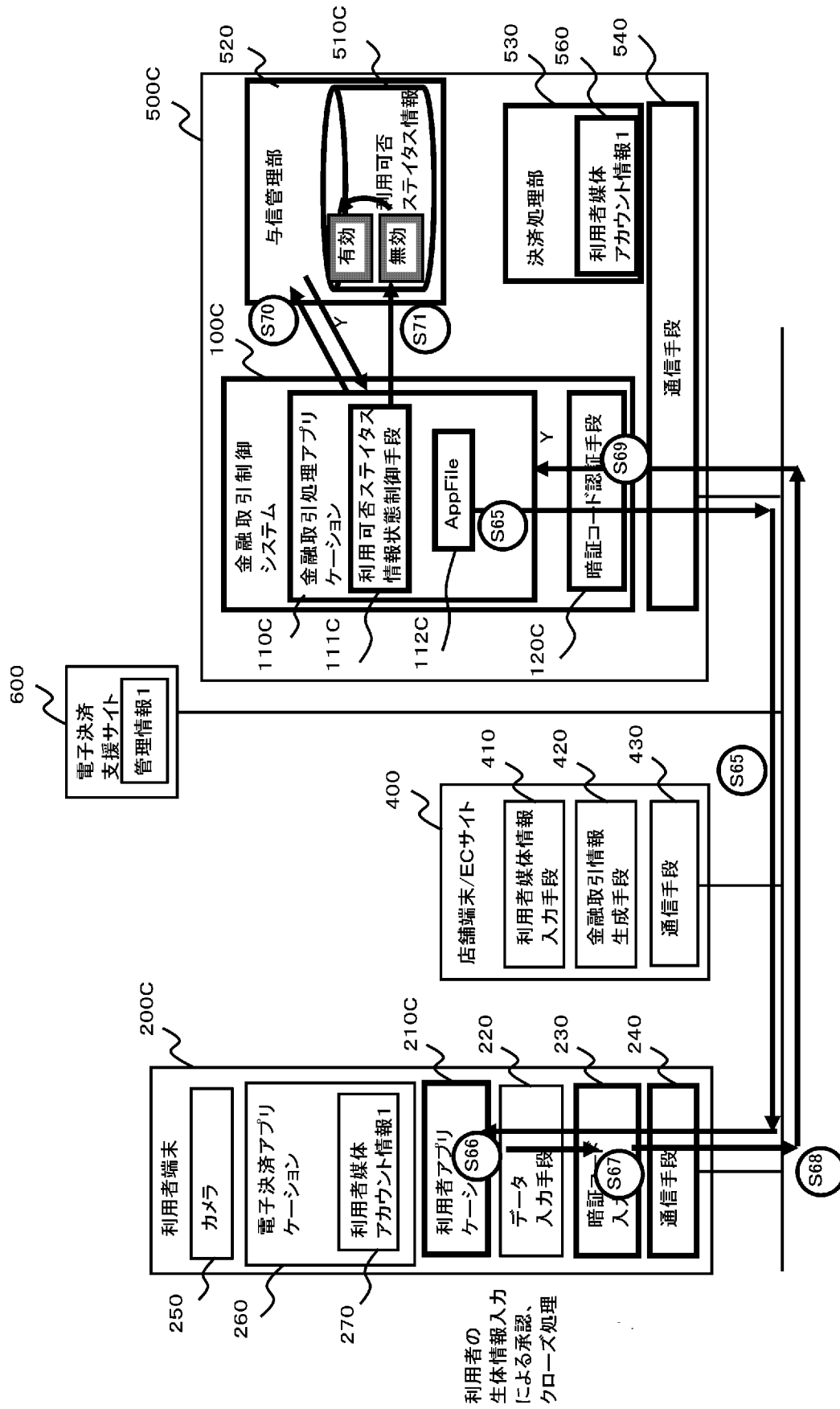




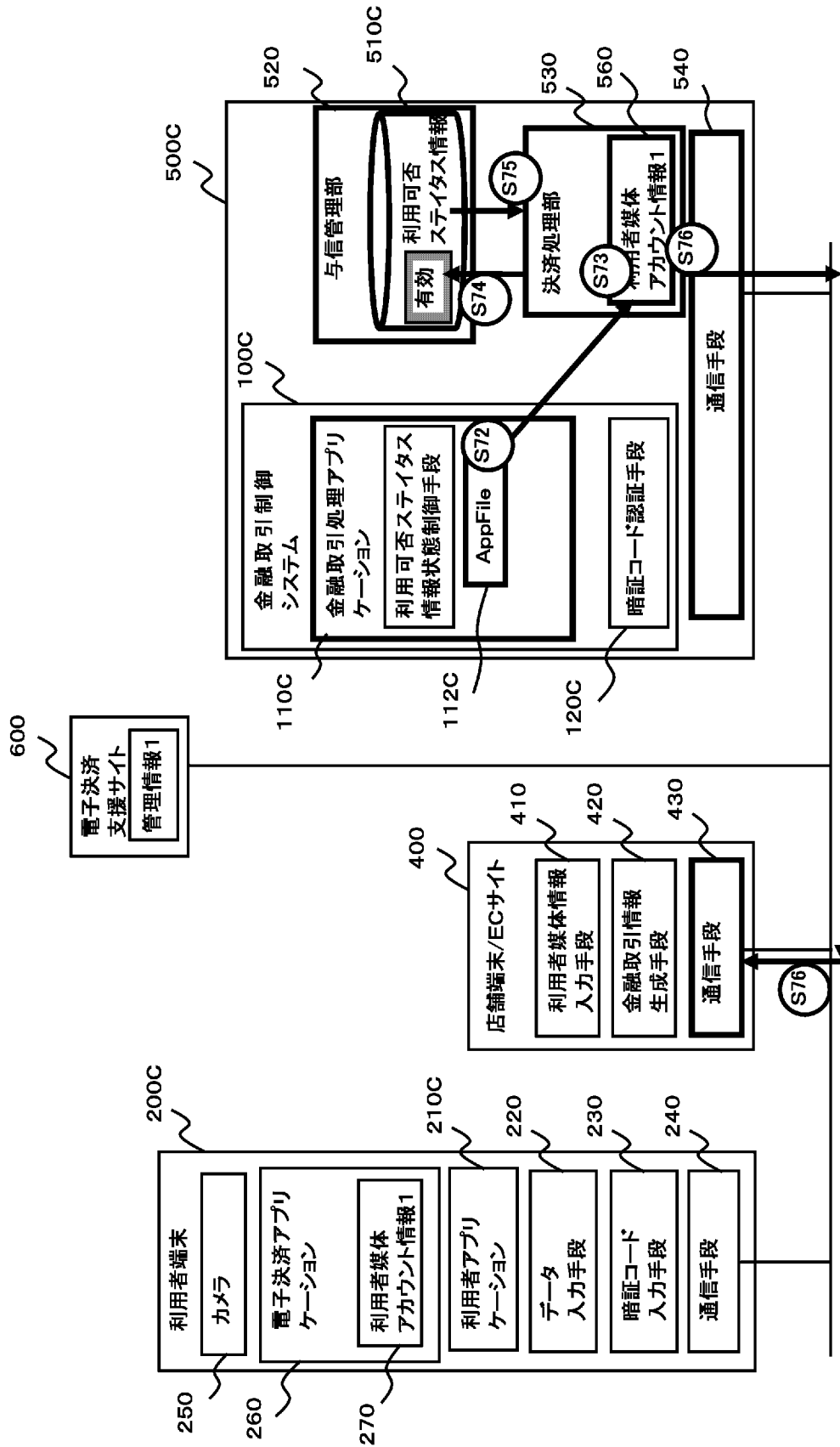
[図19]



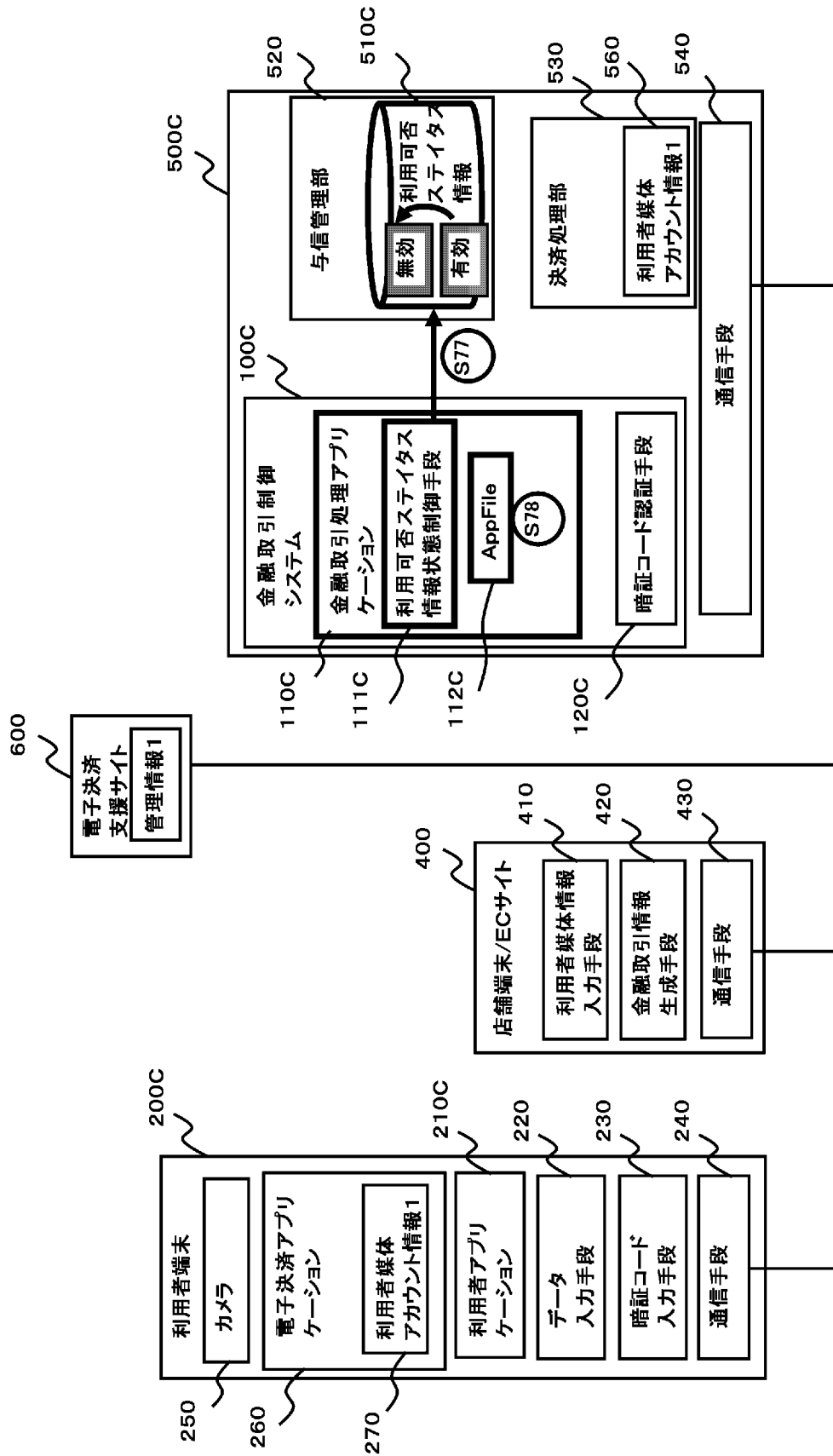
[図20]



[図21]



[図22]



[図23]

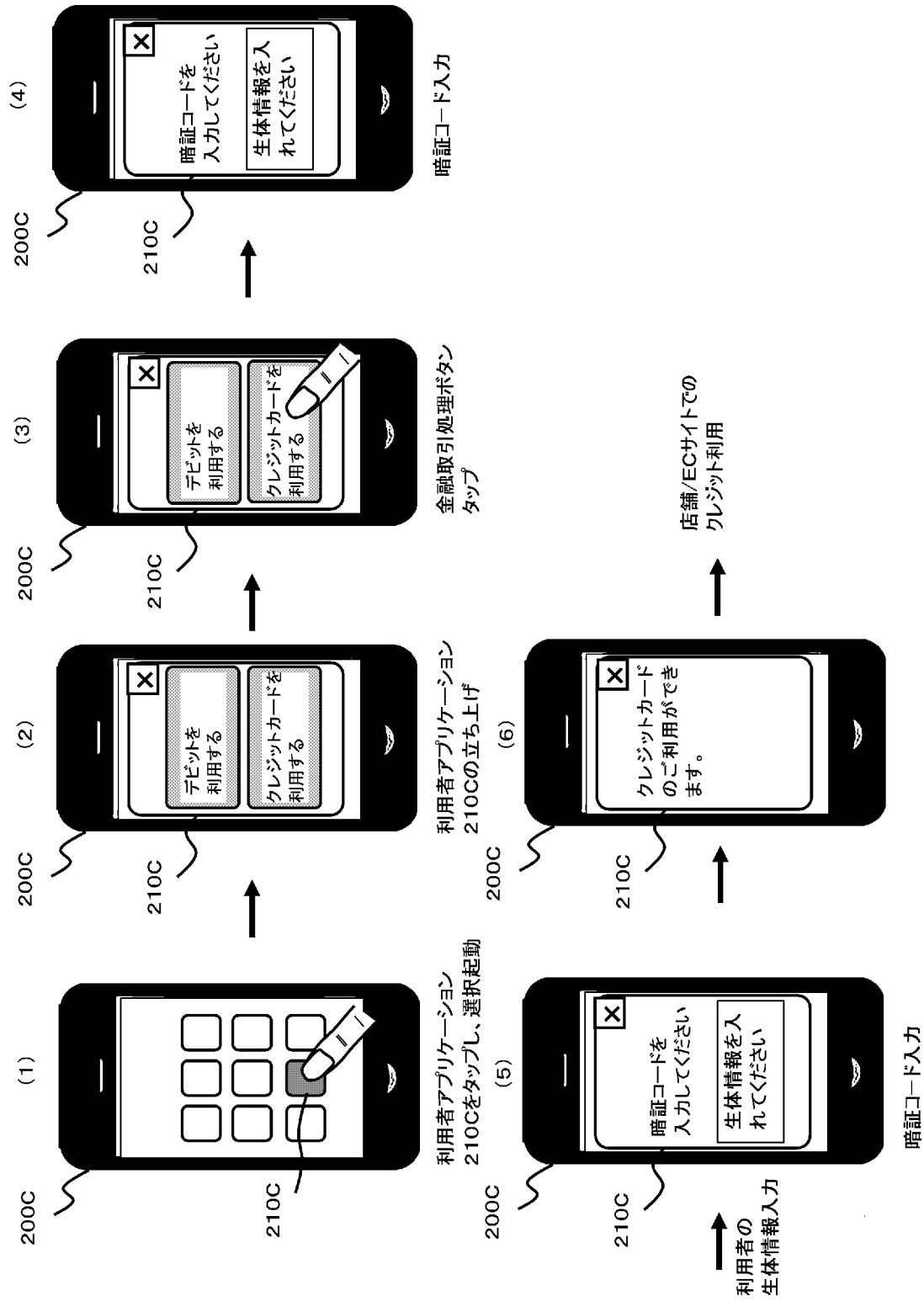


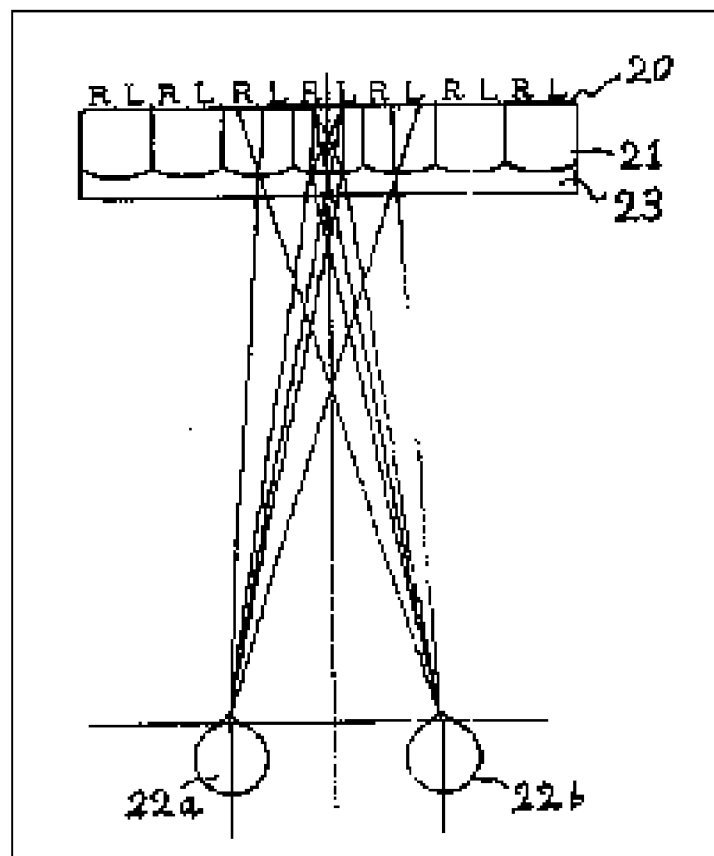
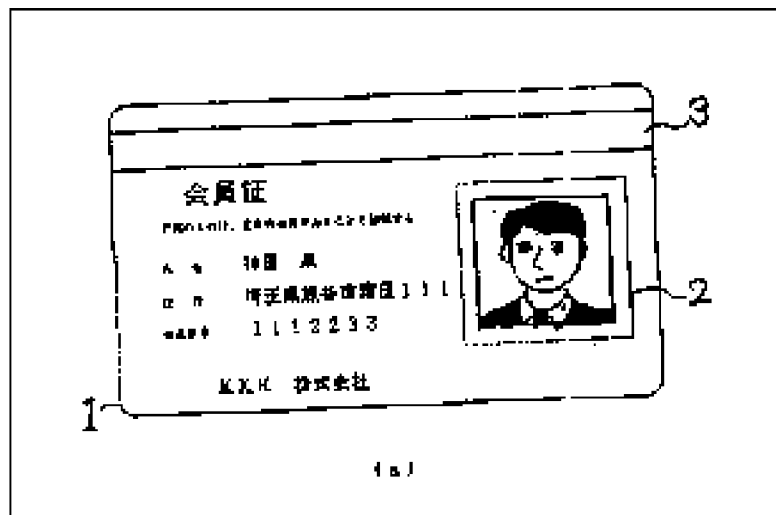
Figure 1 illustrates the sequence of screens for credit card payment confirmation, showing the flow from the initial confirmation request to the final confirmation completion.

The sequence consists of eight steps:

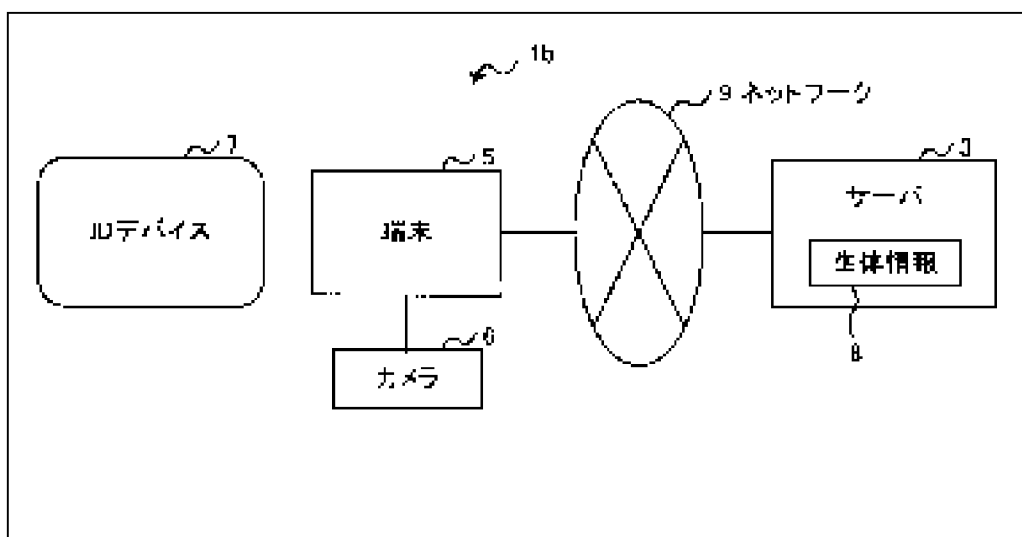
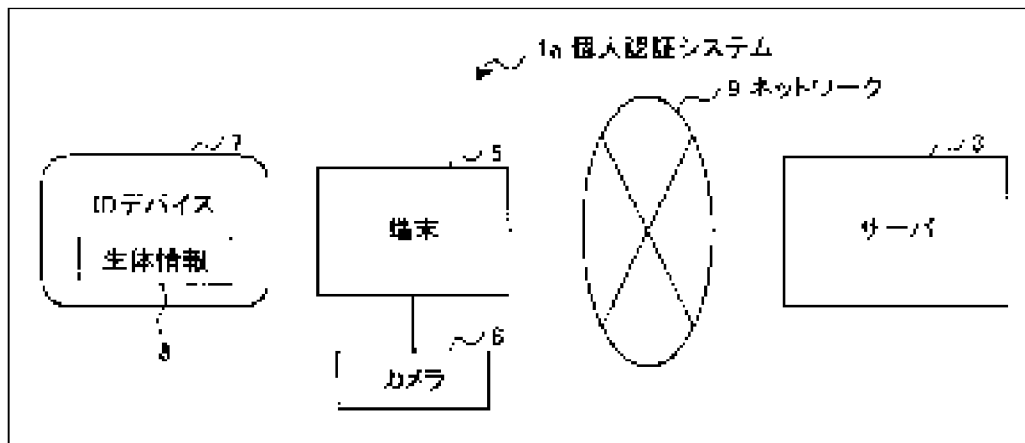
- (1) Confirmation request screen:** The screen displays a confirmation request with input fields for card number, expiration date, and amount. It includes buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (2) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (3) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (4) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (5) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (6) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (7) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).
- (8) Confirmation completion screen:** The screen displays a confirmation completion message with a message box and buttons for "承認する" (Confirm) and "承認しない" (Do not confirm).

The sequence is labeled with "200C" and "210C" indicating the screen type and the specific screen being displayed.

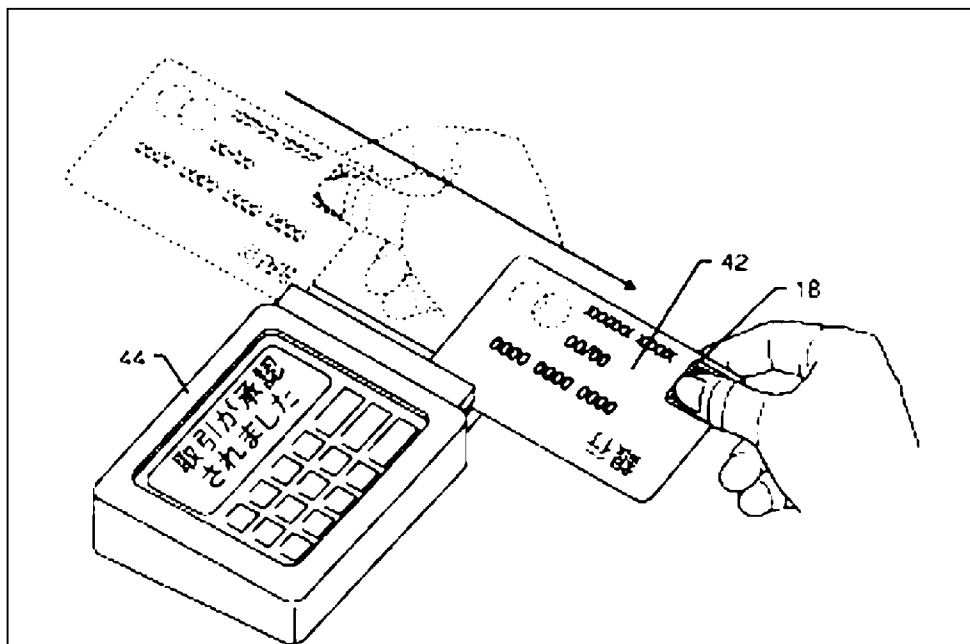
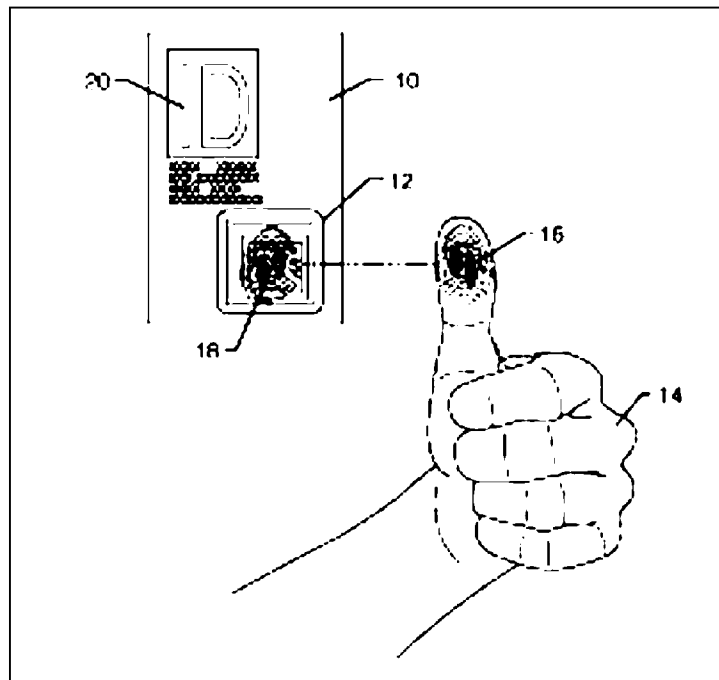
[図25]



[図26]



[図27]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/004317

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl. G06Q20/34 (2012.01) i		
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.Cl. G06Q20/34		
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 1971-2018 Registered utility model specifications of Japan 1996-2018 Published registered utility model applications of Japan 1994-2018		
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 2008-176435 A (HITACHI, LTD.) 31 July 2008, entire text, all drawings & US 2008/0180212 A1 & EP 1947611 A2 & KR 10-2008-0067967 A & CN 101226657 A & TW 200844880 A	1-11
A	JP 2015-500529 A (ROZEN, L.) 05 January 2015, entire text, all drawings & US 2014/0337231 A1 & WO 2013/084145 A2 & EP 2788937 A2	1-11
☒ 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 01.05.2018		Date of mailing of the international search report 15.05.2018
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/004317

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2017-508203 A (EINNOVATIONS HOLDINGS PTE. LTD.) 23 March 2017, entire text, all drawings & WO 2015/119578 A1 & US 2017/0178131 A1 & EP 3103082 A1 & CN 107077669 A & KR 10-2016-0119137 A & CA 2938399 A & AU 2015214646 A & TW 201539339 A & MX 2016010026 A	1-11
A	JP 2004-110352 A (HITACHI SOFTWARE ENG) 08 April 2004, entire text, all drawings (Family: none)	1-11
A	JP 2017-167859 A (SUMITOMO MITSUI BANKING CORP.) 21 September 2017, entire text, all drawings (Family: none)	1-11

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06Q20/34 (2012. 01) i

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（I P C））

Int.Cl. G06Q20/34

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	1971-2018年
日本国実用新案登録公報	1996-2018年
日本国登録実用新案公報	1994-2018年

国際調査で利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 2008-176435 A（株式会社日立製作所） 2008. 07. 31, 全文, 全図 & US 2008/0180212 A1 & EP 1947611 A2 & KR 10-2008-0067967 A & CN 101226657 A & TW 200844880 A	1-11
A	JP 2015-500529 A（ロゼン、リモール） 2015. 01. 05, 全文, 全図 & US 2014/0337231 A1 & WO 2013/084145 A2 & EP 2788937 A2	1-11

☒ 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

01. 05. 2018

国際調査報告の発送日

15. 05. 2018

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

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）

貝塚 涼

電話番号 03-3581-1101 内線 3562

5 L

3043

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	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 2017-508203 A (イーイノベーションズ ホールディングス ピー ティーイー リミテッド) 2017.03.23, 全文, 全図 & WO 2015/119578 A1 & US 2017/0178131 A1 & EP 3103082 A1 & CN 107077669 A & KR 10-2016-0119137 A & CA 2938399 A & AU 2015214646 A & TW 201539339 A & MX 2016010026 A	1-11
A	JP 2004-110352 A (日立ソフトウェアエンジニアリング株式会社) 2004.04.08, 全文, 全図 (ファミリーなし)	1-11
A	JP 2017-167859 A (株式会社三井住友銀行) 2017.09.21, 全文, 全図 (ファミリーなし)	1-11