

(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
2017 年 7 月 6 日(06.07.2017)



(10) 国際公開番号
WO 2017/115557 A1

- (51) 国際特許分類:
G06Q 20/40 (2012.01) G07G 1/12 (2006.01)
- (21) 国際出願番号: PCT/JP2016/082873
- (22) 国際出願日: 2016 年 11 月 4 日(04.11.2016)
- (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 2015-256028 2015 年 12 月 28 日(28.12.2015) JP
- (71) 出願人: 株式会社エヌティーアイ(NTI, INC.)
[JP/JP]; 〒5108021 三重県四日市市松寺三丁目 7 番 4 号 Mie (JP).
- (72) 発明者: 中村 貴利(NAKAMURA, Takatoshi); 〒5108021 三重県四日市市松寺三丁目 7 番 4 号 株式会社エヌティーアイ内 Mie (JP).
- (74) 代理人: 村松 義人(MURAMATSU, Yoshihito); 〒1050003 東京都港区西新橋二丁目 8 番 1 1 号 第 7 東洋海事ビル 2 階 村松国際特許事務所 Tokyo (JP).

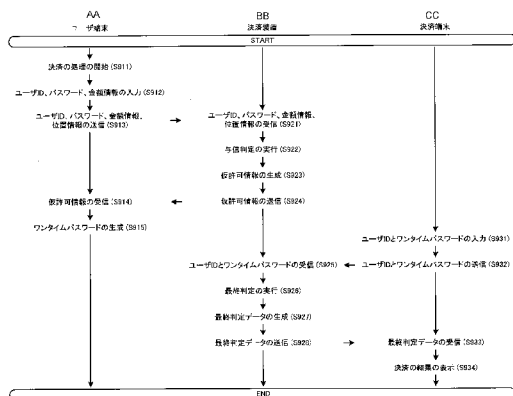
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, 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:

— 国際調査報告 (条約第 21 条(3))

(54) Title: SETTLEMENT SYSTEM, USER TERMINAL AND METHOD EXECUTED BY SAME, SETTLEMENT DEVICE AND METHOD EXECUTED BY SAME, AND PROGRAM

(54) 発明の名称: 決済システム、ユーザ端末及びそれで行われる方法、決済装置及びそれで行われる方法、並びにプログラム



S911 Begin settlement processing
S912 Input user ID, password, amount information
S913 Transmit user ID, password, amount information, location information
S914 Receive provisional authorization information
S915 Generate one-time password
S921 Receive user ID, password, amount information, location information
S922 Execute credit determination
S923 Generate provisional authorization information
S924 Transmit provisional authorization information
S925 Receive user ID and one-time password
S926 Execute final determination
S927 Generate final determination data
S928 Transmit final determination data
S931 Input user ID and one-time password
S932 Transmit user ID and one-time password
S933 Receive final determination data
S934 Display settlement result
AA User terminal
BB Settlement device
CC Settlement terminal

(57) Abstract: In order to provide a safer settlement system as an alternative to a settlement system that uses credit cards, this settlement system has a user terminal, a settlement device, and a settlement terminal. Amount information specifying a user ID, a password, and an amount is input at the user terminal (S912), and that information is transmitted to the settlement device (S913). The settlement device makes a credit determination (S922), generates provisional authorization information (S923) if crediting is possible, and transmits that information to the user terminal (S924). The user terminal generates a one-time password (S915). The one-time password is input to the settlement terminal (S931). If the one-time password transmitted from the settlement terminal to the settlement device is the same as the one-time password created at the settlement device (S926), the settlement device confirms the user's payment (S927).

(57) 要約: クレジットカードを用いた決済システムに代わるより安全性の高い決済システムを提供する。決済システムは、ユーザ端末、決済装置、決済端末を持つ。まず、ユーザ端末でユーザIDとパスワードと金額を特定する金額情報を入力 (S912) し、それを決済装置に送る (S913)。決済装置は、与信判定 (S922) を行い、与信が可能なら仮許可情報を生成し (S923)、それをユーザ端末に送る (S924)。ユーザ端末はワンタイムパスワードを生成する (S915)。ワンタイムパスワードは、決済端末に入力される (S931)。決済端末から決済装置に送られたワンタイムパスワードが決済装置で作られたワンタイムパスワードと同じなら (S926)、決済装置はユーザの支払いを認める (S927)。

WO 2017/115557 A1

明 細 書

発明の名称：

決済システム、ユーザ端末及びそれで行われる方法、決済装置及びそれで行われる方法、並びにプログラム

技術分野

[0001] 本発明は、決済システムに関する。

背景技術

[0002] 例えば、店舗、飲食店等での支払いに、インターネット上での商品の売買の際の支払いに、クレジットカードによる決済が広く用いられている。かかる決済（金銭の支払い）は現在、インターネットその他のネットワークを介して行われる。

より詳細には、クレジットカードでの決済は、以下のようにして行われる。

現在普及しているクレジットカードでは、ユーザがクレジットカードで支払いを行なう場合、ユーザがクレジットカードを実店舗で用いた場合にはその実店舗のカードリーダ等で読込まれたデータを、ユーザがクレジットカードをウェブ上の仮想店舗で用いた場合には、ユーザが例えば暗号化通信で仮想店舗に送ったデータを、実店舗又は仮想店舗からインターネット等のネットワークを介して、クレジットカード会社のコンピュータ（或いはクレジットカード会社が管理するコンピュータ）である決済装置に送る。決済装置は、受取ったそのデータに基づいてユーザに対して与信が可能か否かの判定を行ない、与信を行なえた場合には決済を行なうという手法が一般的に採られている。かかる与信は、クレジットカード会社が負うリスクを軽減するためのものであるが、クレジットカード会社のコンピュータは、与信を行うに先立ってユーザの認証（例えば、クレジットカードナンバーとクレジットカードホルダの名称との組み合わせの正当性を見ることによる認証）を行なうことによって、第三者のなりすましによるクレジットカードの不正利用による

リスクの軽減を図っている。以上のようなユーザに対する認証は、基本的には、クレジットカードに物理的に刻印された、或いは電磁氣的に記録された情報であるクレジットカードナンバーとクレジットカードホルダとによってなされる。

発明の概要

発明が解決しようとする課題

[0003] 上述のように、クレジットカードにおけるクレジットカードナンバーは、一つのクレジットカードに対して、固定された1つのみである。したがって、クレジットカードナンバーを用いての認証は、第三者によるなりすましを完全に排除することが難しい。

クレジットカード自体を悪意の第三者により盗難された場合のみならず、クレジットカードナンバーが、データとして、例えば、決済装置が持つ顧客のクレジットカードのナンバーを記録したデータベースから流出した場合などには、悪意の第三者はクレジットカードの所有者に容易になりすますことができる。

ユーザの認証の精度を上げることにより、第三者のなりすましによるクレジットカードの不正利用を減じる目的で、様々な工夫がなされている。クレジットカードが実店舗で利用される場合には、ユーザの署名を必須とするのもその工夫の1つである。また、最近では、CVC (Card Verification Code)、CVC2などの様々な技術も実用されている。しかしながら、これらの技術は、クレジットカードナンバーとは別の桁数の数字をクレジットカードナンバーと共に認証に用いることにより認証の精度を上げるものに過ぎない。クレジットカードナンバーと共に用いられる桁数の数字は、クレジットカードナンバーと同じく、常に固定されているから、これらの技術は、クレジットカードナンバーの桁数を幾らか増やした程度の効果しか無く、ユーザの認証の精度を上げるというその効果も極めて限定的である。

他方、デビットカードを用いた決済システムも実用されている。デビット

カードを用いた決済システムは、クレジットカードを用いた決済システムが、クレジットカード、決済装置、カードリーダーを備えるのと同様に、デビットカード、決済装置、カードリーダを備えるのが一般である。デビットカードを用いた決済システムは、ユーザが他人に支払いを行った金額分の金銭が、ユーザの預金残高（例えば、ユーザが銀行口座を持つ銀行における当該ユーザの銀行口座における預金残高）から即時にその支払先の他人の口座に移されるという支払いの即時性を実現している点で、クレジットカードを用いた決済システムとは異なっている。しかしながら、デビットカードを用いた即時決済の場合においても、クレジットカードによる決済システムにおいて使用されるクレジットカードナンバーと同様の固定のデビットカードナンバーが用いられる点ではクレジットカードを用いた決済システムと同様であり、それ故にクレジットカードナンバーを盗まれたときに生じうる、クレジットカードを用いた決済システムに起こりうる上述の課題はデビットカードを用いた決済システムにも存在する。

[0004] 本願発明は、クレジットカード又はデビットカードを用いた決済技術に変わる、第三者のなりすましによる不正の生じにくい新規な決済技術を提案することをその課題とする。

課題を解決するための手段

[0005] かかる課題を解決するため、本願発明者は、以下に説明する発明を提案する。

本願発明は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支

払いを受ける者が管理する決済端末と、を含んで構成されている決済システムである。

かかる決済システムにおける前記ユーザ端末は、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力できるようになっており、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信するようになっているとともに、前記ユーザ端末情報処理手段は、ワンタイムパスワードを生成するユーザ端末OTP生成部を備えている。

また、決済システムにおける前記決済装置は、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部を備えているとともに、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取るようになっており、前記決済装置情報処理手段は、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する与信判定部と、決済の最終判定を行う最終判定部と、前記ユーザ端末と同じワンタイムパスワードを生成する決済装置OTP生成部とを備えており、前記決済装置送受信手段は、前記与信判定部が生成した仮許可情報を前記ネットワークを介して前記ユーザ端末に送信するようになっている。

そして、この決済システムでは、前記仮許可情報を前記決済装置から前記ユーザ端末が前記ユーザ端末送受信手段にて受け取ると、前記ユーザ端末OTP生成部が、ワンタイムパスワードを生成するようになっており、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決

済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記与信判定部で前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置OTP生成部で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記最終判定部が、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するとともに、前記決済装置情報処理手段は、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている。

[0006] 本願発明の大まかな理解を助けるために例示すると、本願発明の決済システムにおけるユーザ端末は、ユーザによって使用、管理等がなされるものであり、従来のクレジットカードを用いた決済システムにおけるクレジットカードに、従来のデビットカードを用いた決済システムにおけるデビットカードに相当する。また、本願発明の決済装置は、クレジットカードによる決済システムにおける、クレジットカード会社等によって管理等される決済装置に、デビットカードを用いた決済システムにおけるデビットカード会社等によって管理等される決済装置に、相当する。また、本願発明の決済端末は、クレジットカードによる決済システムにおける、実店舗に置かれたカードリーダーを有する装置に相当し、或いはインターネット上の仮想店舗での決済に決済システムが応用される場合であれば、ユーザが用いるコンピュータそれ自体、或いはユーザが用いるコンピュータからワンタイムパスワードを受取る、その仮想店舗の管理者が管理するコンピュータ、又はそれらを併せたものに相当する。また、本願発明の決済端末は、デビットカードを用いた決済システムにおけるカードリーダー等を有する装置等に相当する。もっとも、以上の例示はあくまでも例示であり、本願発明がまったく新規な決済システムであることもあるため、必ずしも正確ではない場合もあり得る。なお、冗長になるので、以下の説明ではクレジットカードを用いた決済システムのみを

例示に用いる。

本願発明のユーザ端末は、コンピュータ、例えば可搬のコンピュータであり、携帯電話、スマートフォン、タブレット等である。これらの機器を持ち歩くことは最早一般人にとっても極日常的なことである。これらの機器をユーザ端末として利用することで、ユーザはクレジットカードという嵩張るものを持ち歩く必要がなくなる。この決済システムにおいて、従来の決済システムにおけるクレジットカードに相当するものがユーザ端末であるとすれば、この決済システムにおいて、従来の決済システムにおけるクレジットカードナンバーに相当するものはユーザ端末で発生させられるワンタイムパスワードである。ワンタイムパスワードは、周知のように、次々と異なるものが発生させられる。したがって、ワンタイムパスワードが悪意のある第三者に盗まれたとしても、そのいわば使い捨てのワンタイムパスワードを悪用するのは難しく、しかも後述するようにしてワンタイムパスワードの有効期限を、通常のクレジットカードの有効期限に比して極めて短く（例えば、これより長くてもよいが、数日以内から数十分程度、場合によっては１０分程度）決めておくことにより、その悪用は殆ど不可能となる。つまり、この決済システムでは、そのとき限りしか有効でないワンタイムパスワードをクレジットカードナンバーの代わりに用いることにより、悪意のある第三者のなりすましを防止することになっている。

他方、本願発明による決済システムには更なる利点がある。従来のクレジットカードを用いた決済システムにおいて、クレジットカードナンバーを盗みそれを悪用する者が、ユーザからクレジットカードナンバーを知らされる立場にあるクレジットカードリーダの操作者等である、という場合があることが広く知られている。つまり、クレジットカードによる決済システムにおいては、構造的にクレジットカードナンバーを扱う者自体が悪意ある第三者となることがあり、それを完全に排除することは不可欠である。そのような者が行うクレジットカードナンバーの悪用に備え、クレジットカードを発行するクレジットカード会社等は、クレジットカードリーダを設置する者に対

する与信管理を行い、その信用の程度に合せてクレジットカードにより支払いを行う場合における手数料を上下させるなどの変更に手間のかかることを行っている。しかも、上述の与信管理において、手数料を幾ら上げたとしてもクレジットカード会社等が負うリスクと釣り合わないと判断されるような、最低限の信用も持ちあわせていない者は、クレジットカード会社等が行う与信管理から漏れ、クレジットカードによる支払いを受けることができないというのが、クレジットカードによる決済システムが普及している今日における現実である。しかしながら、クレジットカードナンバーの第三者による悪用が殆ど想定できない本願発明の決済システムによれば、クレジットカード会社等が行う上述の与信管理が必要なくなる。また、クレジットカードナンバーをユーザから受取る、クレジットカードを用いた決済システムでユーザからの支払いを受取る者に対する与信管理が不要になるということは、本願発明の決済システムによりユーザからの支払いを受ける者を従来よりも増やせるということを意味する。これは、当然、大きな利点である。支払いを受ける者に対する与信管理が必要であるというのは、デビットカードを用いた決済システムの場合も同様である。本願発明の決済システムによれば、クレジットカードによる決済システムよりもユーザからの支払いを受ける者を従来よりも増やせるのみならず、デビットカードによる決済システムよりもユーザからの支払いを受ける者を従来よりも増やせる。

[0007] この決済システムにおける処理の大まかな流れは、以下のとおりである。

まず、ユーザが、ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力する。金額情報は、金額情報により決済を行うユーザを特定する情報であるユーザ情報とともに、ユーザ端末から、決済装置に送信される。

この決済装置は、ユーザ情報と金額情報とを用いて、与信判定部により、ユーザの認証及び与信の判断を行う。ここで行われるユーザの認証は、ユーザ情報によって行われる。ユーザ情報は、例えば、ユーザが、前記ユーザ端末入力手段を用いて入力を行うユーザIDと、前記ユーザ端末のそれぞれに

対して割り振られたユニークな端末情報の少なくとも一方を含むものとする
ことができ、また、それらの双方を含むものとされていても良い。ユーザIDは、例えばユーザが決定した、数字、文字、記号等の羅列であり、基本的に正当なユーザしか知らないものであるため、ユーザ端末が第三者に盗まれた場合であっても、第三者のなりすましを防止することができる可能性が高い。端末情報の例としては、ユーザ端末がスマートフォンである場合における当該スマートフォンに組込まれたSIMカード（Subscriber Identity Module Card）に記録されたID番号や、スマートフォンの製造番号等の個体識別番号を挙げることができる。端末情報をユーザの認証に用いることとすれば、ユーザ端末自体が悪意の第三者に盗まれない限り、悪意の第三者によるなりすましを防げる可能性が高くなる。もちろん、ユーザIDと端末情報の双方をユーザの認証に用いることにより、ユーザの認証の精度は高くなり、且つなりすましを防げる可能性も高くなる。

与信判定部で行われる与信判定自体は、従来のクレジットカードを用いる場合における与信判定と同様に行うことも可能であるが、本願発明ではむしろデビットカードにおける与信判定と同様に、ユーザが支払いを行おうとしている金額と、ユーザの預金残高とのどちらが大きいかを基準に与信判定を行うこととしている。つまり、この決済システムは、ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部を備えているとともに、与信判定部は、決済装置が金額情報と、ユーザ情報とを受取った場合に、与信判定部が預金残高記録部から読みだした預金残高情報が金額情報で特定される金額以上であるか否かにより、与信判定を行うようになっている。つまり、本願発明の決済システムの与信判定部は、預金残高がユーザの支払おうとしている金額情報で特定される金額以上である場合には、仮許可情報を生成することとしている。このような預金残高に基づいた決済方法を本願発明で採用しているのは、かかる決済システムであれば、支払いを受ける者がより確実に支払いを受けられるようになるからである。この場合、決済装置の預金残高記録部にユーザの預金残高情報が記録されている状態というの

は、ユーザの少なくとも1つの預金口座を決済装置の管理者が管理している状態である。そのような状態は、例えば、ユーザが決済装置の管理者に対して予め幾らかの金銭を支払っている場合、つまりいわゆるプリペイドによる決済システムが採用されている場合に実現可能である。さもなくば、決済装置の管理者が預金の管理を事業として行っている銀行等である場合、或いは決済装置の管理者が銀行等と提携している場合（これらの場合には、デビットカードによる決済システムにより近いものになる。）にも、決済装置の預金残高記録部にユーザの預金残高を記録することが可能となろう。なお、プリペイドによる決済システムと、デビットカードによる決済システムの相違は、概ねユーザの預金口座からの支払いがそのプリペイドによる決済システムにしか使われないか、他の支払いにも使われるかというものである。後者がデビットカードによる決済システムに相当するが、本願発明はその両者を含む。

与信判定で決済を行えるということになったら、その旨を示す仮許可情報が、決済装置からユーザ端末へと送られる。

仮許可情報を受取ったユーザ端末では、そのユーザ端末OTP生成部で、ワンタイムパスワードが生成される。ワンタイムパスワードは、数字、文字、記号等の羅列とすることができ、少なくともユーザが決済装置で認証を受ける度に生成されるようにされ、また、生成される度に異なるようなものとなるようにされている。また、各ユーザ端末で生成されるワンタイムパスワードは、複数回生成されるワンタイムパスワードの全体を見た場合には、異なるものとなるようにされている。ワンタイムパスワードは、例えば、公知の手法で生成することができる。ユーザ端末で生成されたワンタイムパスワードは、決済端末の決済端末入力手段を用いて、決済端末に渡される。

ユーザ端末は通常、ディスプレイを備えている。ユーザ端末OTP生成部で生成されたワンタイムパスワードは例えば、ディスプレイに表示されるようになっている。ワンタイムパスワードが数字の羅列の場合には、決済端末入力手段をテンキー等とすることにより、ユーザ或いは決済端末の管理者は

、ディスプレイに表示されたワンタイムパスワードを、テンキー等を入力することにより決済端末に入力することができる。ワンタイムパスワードが、数字と文字の組合せであり、且つ決済端末入力手段がキーボードである場合には、ユーザ或いは決済端末の管理者は、ディスプレイに表示されたワンタイムパスワードを、キーボードを入力することにより決済端末に入力することができる。ワンタイムパスワードの決済端末への受渡しの方法は、これには限られない。例えば、ワンタイムパスワードが表示されたユーザ端末のディスプレイを、決済端末入力手段としてのカメラで撮影し、ディスプレイに表示されたワンタイムパスワードを画像処理によって決済端末に入力する、或いはユーザ端末のディスプレイにバーコードとして表示されたワンタイムパスワードを、決済端末入力手段としてのバーコードリーダで読み取ることによって、ワンタイムパスワードを決済端末に受け渡すことも可能である。或いは、Bluetooth（商標）、赤外線通信などの無線通信によって（もちろん、有線の通信でも構わないが若干不便である。）、ユーザ端末から決済端末にワンタイムパスワードをデータとして受け渡すことも可能である。なお、この場合には必ずしも、ユーザ端末のディスプレイにワンタイムパスワードを表示する必要はない。

ユーザが、インターネット上の仮想店舗に対する支払いを行う場合には、ユーザがワンタイムパスワードを仮想店舗に渡すために、ユーザ端末、或いはユーザが使用するインターネットによる通信が可能な他の端末に、ユーザが、ワンタイムパスワードを入力することになる。この場合の入力には一般に、ユーザ端末或いは他の端末が備えたテンキー或いはキーボードが用いられるが、かかる入力においても、上述の場合と同様に、カメラ、バーコードリーダ、或いは無線通信が利用されても良いのは自明であろう。

いずれにせよ、ユーザ端末から決済端末に受渡されたワンタイムパスワードは、決済端末から、決済装置に送られる。

決済装置は、決済装置OTP生成部を有している。決済装置OTP生成部は、ユーザ端末OTP生成部と同じワンタイムパスワードを生成することが

できるようになっている。公知のように、ユーザ端末OTP生成部で生成されるワンタイムパスワードと、決済装置OTP生成部で生成されるワンタイムパスワードとは、同期されたものとされる。決済装置は、多数のユーザ端末の決済を行うので、各ユーザ端末のユーザ端末OTP生成部で生成されるワンタイムパスワードと同期したワンタイムパスワードを生成できるようになっている。決済端末からワンタイムパスワードを受取ると、決済装置では、最終判定部が、決済装置OTP生成部が生成したワンタイムパスワードと、決済端末から送られて来たワンタイムパスワードとを比較することにより、決済を認めて良いか否かの最終判定がなされる。両ワンタイムパスワードが一致したのであれば、最終判定部は、そのワンタイムパスワードによるユーザ端末のユーザから、決済端末の管理者への支払いを許可する。決済が許可された後、決済装置情報処理手段は、預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じる。これは、基本的には即時に行われるが、その金額に相当する金銭を、決済装置が即座に支払いを受けるべき者に支払うか否か（つまり、一旦決済装置或いはその管理者が預かるか）は、適宜決定すればよい。

この決済システムによれば、上述したように、決済装置で行われる最終的な決済の許可は、ユーザ端末で生成されたワンタイムパスワードを用いて行われる。

ユーザ端末で使用されるワンタイムパスワードは、1回の決済の許可にしか用いられない。したがって、ワンタイムパスワードを第三者に盗まれたところで、それにより被害が生じる可能性は低く、被害が生じたとしてもクレジットカード又はデビットカードを用いた決済システムの場合に比べれば遥かに小さい。

なお、本願発明において、決済端末の管理者とは、決済端末を管理する者に限られず、決済端末を設置、所有、専有又は占有し或いは管理、操作する者、及びユーザから支払いを受ける者をすべて含み、いずれにせよユーザからの支払いを受ける組織自体、或いは当該組織に属するか、少なくともその

組織に関連する者を意味する。

また、本願発明の決済システムにおいて、決済装置とユーザ端末の間の通信と、決済装置と決済端末との間の通信は、暗号化通信であっても構わない。

なお、本願の決済システムを用いて、ユーザが支払いを行う相手方が特に実店舗である場合であって、ユーザ端末を用いてワンタイムパスワードを発生させてからある程度の時間を経た（例えば、数時間から数ヶ月を経てから）後に、ユーザが相手方に対して支払いを行うことが想定される場合には、ユーザ端末で生成されたワンタイムパスワードを紙に印刷するのが便利である場合もある。本願発明におけるワンタイムパスワードは、物理的な実体を持たないデータ（或いは単なる情報）であるが、それはそのデータ或いは情報を用いて第三者に支払いを行うことができるという性質を持つ。かかる性質をより強調するのであれば、本願の決済システムにおいてユーザ端末で生成されるワンタイムパスワードは、貨幣の代替物であると考えることができる。フィンテック関連の技術が話題に上っている昨今の流れを考えれば、貨幣はやがて実体を失っていくのかもしれないが、しかしながら物理的な実体を持つ貨幣に少なくとも現状の一般人は慣れ親しんでいる。ワンタイムパスワードを印刷した紙である金券を、ユーザはあたかも貨幣（紙幣）のように用いることにより、支払いの相手方への支払いを行うことが可能となる。言い換えれば、かかる金券は、ワンタイムパスワードをユーザ端末から決済端末に引渡すためのバリエーションの1つであるといえる。かかる金券を受取った支払いを受ける者は、それに印刷されたワンタイムパスワードを何らかの方法で、例えばテンキーやキーボードを用いて入力することで、決済端末に入力することができる。

もっとも、かかる金券をユーザが落としたり、或いは第三者に盗まれたりした場合には、通常の紙幣をユーザが落としたり、或いは第三者に盗まれたりしたときと同様に、その金券を第三者に使用されてしまうおそれがある。とはいえ、その金券には、ワンタイムパスワードに設けられた使用可能な期

間に応じた使用期限があるから、悪意の第三者に使用されるリスクは通常の貨幣よりは小さいといえる。しかしながら、それとは別種の問題として、かかる金券には、それに印刷されたワンタイムパスワードを第三者に知られた場合には、金券自体はユーザの手元に存在するのに、そのワンタイムパスワードを第三者に使用されてしまい、その金券或いは、その金券に印刷されていたワンタイムパスワードが本来持っていた金銭的な価値が失われてしまう可能性があるという、通常の紙幣にはないリスクがある。金券に印刷されたワンタイムパスワードを第三者に盗まれたということは、手元に金券が残っているユーザには知得するのが難しいから、仮にかかる問題が生じたとしてもその発見、及び解決は難しい。そこで、そのような状況の発生を防止するための技術として、本願発明者は、前記ワンタイムパスワードの一部は、前記紙の一方の面に、前記ワンタイムパスワードの残部は、前記紙の他方の面に、それぞれ印刷されている、という金券を提案する。かかる金券であれば、悪意の第三者が金券に印刷されたワンタイムパスワードを盗もうとした場合には、その金券の両面を見る（或いは、写真に撮る）ことが必要となるから、ワンタイムパスワードを盗まれる可能性は、ワンタイムパスワードが紙の一方の面のみに印刷されている場合に比して格段に小さくなる。

また、本願の決済システムにおけるユーザ端末で生成された前記ワンタイムパスワードを特定するための情報を、紙に印刷してなる、金券をも本願発明者は、本願発明の一態様として提案する。かかる金券も、従来からの伝統的貨幣と同様の態様でユーザが使用することができる。ワンタイムパスワードを特定するための情報とは、例えば、バーコードである。ユーザからかかる金券を受取ったユーザから支払いを受けるべき相手方は、その情報（例えば、バーコード）を読取りそれを決済端末に入力することによって、ユーザ端末で生成されたワンタイムパスワードを決済端末に入力することができる。これも、ワンタイムパスワードをユーザ端末から決済端末に引渡すためのバリエーションの1つであるといえる。ワンタイムパスワード自体を金券に印刷する場合と同じく、前記ワンタイムパスワードの一部を特定するための

情報が、前記紙の一方の面に、前記ワントタイムパスワードの残部を特定するための情報が、前記紙の他方の面に、それぞれ印刷されていても構わない。

また、以上の金券を構成する前記紙には、その金券を使用することが予定された者の顔が印刷されていても良い。ユーザから支払いを受けるべき者が金券を受取った場合に、その金券に印刷された顔とその金券を差出したユーザの顔との一致を確認し、その確認が行えた場合にのみ、その金券による決済に必要な処理（例えば、決済端末に対する金券に記載されていたワントタイムパスワードの入力）を行うことにすれば、金券を落したり第三者に盗まれた場合においても、そのワントタイムパスワードの不正使用（不正な決済）を防止することができるようになる。

[0008] 本願発明の決済システムにおける前記ユーザ端末は、前記ユーザ端末が存在する位置を特定するための情報である位置情報を生成する位置情報生成手段を備えており、前記ユーザ端末送受信手段は、前記位置情報を前記決済装置に送信するようになっていてもよい。ユーザ端末がそのようなものである場合、前記決済装置の前記最終判定部は、前記ユーザ端末から前記ワントタイムパスワードをその前記決済端末送受信手段で送って来た前記決済端末の位置が、前記ユーザ端末の前記位置情報生成手段で生成された位置情報で特定される位置から、所定の距離以内の場合に限り、そのワントタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するようになっていてもよい。

この限りではないが、この決済システムは、決済端末が実店舗に存在する場合に特に有用である。この決済システムであれば、ユーザ端末と、ユーザ端末からワントタイムパスワードを受渡される決済端末の位置とが所定の距離以内でない限り、決済装置の最終判定部は決済の許可を行わない。これにより、第三者がなりすましを行うおそれをより小さくすることができる。

ユーザ端末から、決済装置に位置情報を送信するタイミングは、金額情報とユーザ情報とを決済装置に送信するタイミングとは別に決定することができる。例えば、前記ユーザ端末送受信手段は、前記位置情報を、前記金額情

報、及び前記ユーザ情報と一緒に、前記決済装置に送信するようになっていてもよい。或いは、仮許可情報をユーザ端末が受取った後の所定のタイミングで、ユーザ端末が決済装置に位置情報を送るようになっていても良い。

位置情報生成手段は、例えばGPS（Global Positioning System）である。GPSの機能は、ユーザ端末の一例となるスマートフォン等には一般的に内蔵されるように既になっているので、位置情報生成手段としてGPSを用いるのにハードウェア的な面からの負担は大きくない。

最終判定部は、上述のように、ユーザ端末からワンタイムパスワードを送って来た決済端末の位置が、ユーザ端末の位置情報で特定される位置から、所定の距離以内か否かの判定を行う。かかる判定を行うには、最終判定部は、決済端末の位置を知ることが必要となる。それを可能とするには、以下のように幾つかのアプローチがある。

その1つ目は、決済装置にワンタイムパスワードを送る可能性のある決済端末の位置を、予め決済装置が把握しておくというものである。例えば、各決済端末を特定するための決済端末のIDと、各決済端末の位置とを紐付けて記録したデータベースを、決済装置が有していれば、決済装置はどの決済端末からワンタイムパスワードが送られてきたかを把握することにより、ワンタイムパスワードを送ってきた決済端末の位置を把握することができる。

その2つ目は、決済端末に、ユーザ端末が備える位置情報生成手段と同様の位置情報生成手段を持たせておき、決済端末が、ワンタイムパスワードを決済装置に送る度に（ワンタイムパスワードを送るのと同時か否かは問わない）、決済端末の位置情報を決済端末から決済装置に送るというものである。これによっても、決済装置は、ワンタイムパスワードを送ってきた決済端末の位置を把握することができる。

[0009] 本願発明の決済システムにおける決済装置が有する前記最終判定部は、ユーザが、前記ユーザ端末入力手段によって、前記金額情報を入力するための処理を開始してから、前記最終判定部が決済の最終判定を行う前までのうちの所定の時点から、前記最終判定部が決済の最終判定を行うまでの時間が、

予め定められた時間間隔よりも短い場合にのみ、決済を許可するようになっていてもよい。

これは、要するに、ユーザ端末で生成されたワンタイムパスワードに有効期限を設けるものである。これにより、クレジットカードを用いた決済システムにおけるクレジットカードナンバーに相当する、本願発明による決済システムにおけるワンタイムパスワードが不正利用される可能性がより小さくなる。

所定の時点は、上述のように、ユーザが、ユーザ端末入力手段によって、金額情報を入力するための処理を開始してから、最終判定部が決済の最終判定を行う前までのうちの所定の時点である。「ユーザが、ユーザ端末入力手段によって、金額情報を入力するための処理を開始したとき」というのは、ユーザが金額情報の入力そのものを始めたときではなく、ユーザが金額情報の入力を開始するに必要な何らかの処理を開始したとき、を意味する。例えば、金額情報を入力するために、この決済に必要なソフトウェアをユーザ端末で立ち上げることが必要なのであれば、その処理を行った時という意味である。

所定の時点は例えば、ユーザが、ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力した（例えば、入力を開始した時点、或いは入力をし終えた）時点、ユーザ端末送受信手段が、金額情報と、ユーザ情報とを、ユーザ端末送受信手段によって、ネットワークを介して決済装置に送信した時点、決済装置送受信手段が、金額情報と、ユーザ情報とを、ユーザ端末送受信手段から受取った時点、決済装置の与信判定部が仮許可情報を生成した時点、仮許可情報が決済装置の決済装置送受信手段から送信された時点、仮許可情報がユーザ端末のユーザ端末送受信手段で受取られた時点、である。

[0010] 本願発明者は、以上で説明した決済システムに用いられるユーザ端末をも、本願発明の一態様として提案する。これにより得られる効果は、上述の決済システムで得られる効果に同じである。

一例となるユーザ端末は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、を含んで構成されている決済システム、を構成するためのユーザ端末である。

このユーザ端末は、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力できるようになっており、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信するようになっており、前記ユーザ端末情報処理手段は、ワンタイムパスワードを生成するユーザ端末OTP生成部を備えている。

そして、このユーザ端末を含む決済システムに含まれる前記決済装置は、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部を備えているとともに、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取るようになっており、前記決済装置情報処理手段は、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読み出した前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情

報である仮許可情報を生成する与信判定部と、決済の最終判定を行う最終判定部と、前記ユーザ端末と同じワンタイムパスワードを生成する決済装置OTP生成部とを備えており、前記決済装置送受信手段は、前記与信判定部が生成した仮許可情報を前記ネットワークを介して前記ユーザ端末に送信するようになっている。

そして、このユーザ端末を含む決済システムは、前記仮許可情報を前記決済装置から前記ユーザ端末が前記ユーザ端末送受信手段にて受けると、前記ユーザ端末OTP生成部が、ワンタイムパスワードを生成するようになっていることにより、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記与信判定部で前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置OTP生成部で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記最終判定部が、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するようになっているとともに、前記決済装置情報処理手段は、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている。

[0011] 本願発明者は、ユーザ端末で実行される以下の方法も本願発明の一態様として提案する。これにより得られる効果は、上述の決済システムで得られる効果に同じである。

その方法の一例は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受け付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預

金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、を含んで構成されている決済システム、を構成するためのユーザ端末に含まれるユーザ端末情報処理手段にて実行される方法である。

この方法は、前記ユーザ端末情報処理手段が実行する。

具体的には、この方法は、ユーザ端末情報処理手段が実行する、前記ユーザ端末入力手段により、決済の対象となる金額を特定する情報である金額情報の入力を受付ける過程と、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信する過程と、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取った前記決済装置において、前記決済装置情報処理手段が、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合にその旨を示す情報である仮許可情報を生成し、その仮許可情報を前記決済装置送受信手段が、前記ネットワークを介して前記ユーザ端末に送信した場合に、それを前記ユーザ端末送受信手段により受付ける過程と、前記仮許可情報を前記決済装置から前記ユーザ端末が受付けた場合に、ワンタイムパスワードを生成する過程と、を含んでいる。

それにより、この決済システムは、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して

前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記決済装置情報処理手段で、前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記決済装置情報処理手段が、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを許可するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じる、ようになっている。

[0012] 本願発明者は、所定のコンピュータを、本願発明の決済システムに含まれるユーザ端末として機能させるためのコンピュータプログラムも本願発明の一態様として提案する。これにより得られる効果は、上述の決済システムで得られる効果に同じである。

そのコンピュータプログラムの一例は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、を含んで構成されている決済システム、を構成するためのユーザ端末としてコンピュータを機能させるためのコンピュータプログラムである。

そして、このコンピュータプログラムは、前記コンピュータに、前記ユーザ端末入力手段により、決済の対象となる金額を特定する情報である金額情報の入力を受付ける過程と、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユ

一ザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信する過程と、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取った前記決済装置において、前記決済装置情報処理手段が、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合にその旨を示す情報である仮許可情報を生成し、その仮許可情報を前記決済装置送受信手段が、前記ネットワークを介して前記ユーザ端末に送信した場合に、それを前記ユーザ端末送受信手段により受付ける過程と、前記仮許可情報を前記決済装置から前記ユーザ端末が受付けた場合に、ワンタイムパスワードを生成する過程と、を実行させる。

それにより、この決済システムは、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記決済装置情報処理手段で、前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記決済装置情報処理手段が、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを許可するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている。

[0013] 本願発明者は、以上で説明した決済システムに用いられる決済装置をも、本願発明の一態様として提案する。これにより得られる効果は、上述の決済システムで得られる効果に同じである。

その決済装置の一例は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、を含んで構成されている決済システム、を構成するための決済装置である。

この決済装置を含む決済システムに含まれる前記ユーザ端末は、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力できるようになっており、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信するようになっており、前記ユーザ端末情報処理手段は、ワンタイムパスワードを生成するユーザ端末OTP生成部を備えている。

そして、この決済装置は、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取るようになっており、前記決済装置情報処理手段は、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読み出した前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する与信判定部と、決済の最終判定を行う最終判定

部と、前記ユーザ端末と同じワンタイムパスワードを生成する決済装置OTP生成部とを備えており、前記決済装置送受信手段は、前記与信判定部が生成した仮許可情報を前記ネットワークを介して前記ユーザ端末に送信するようになっている。

そして、この決済システムは、前記仮許可情報を前記決済装置から前記ユーザ端末が前記ユーザ端末送受信手段にて受けると、前記ユーザ端末OTP生成部が、ワンタイムパスワードを生成するようになっており、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記与信判定部で前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置OTP生成部で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記最終判定部が、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するとともに、前記決済装置情報処理手段は、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている。

[0014] 本願発明のユーザ端末における前記ユーザ端末入力手段は、ユーザからの支払いを受ける者が管理する決済端末を特定する情報である決済端末特定情報を入力できるようになっているとともに、前記ユーザ端末送受信手段は、前記決済端末特定情報を前記ネットワークを介して前記決済装置に送るようになっているもよい。

この場合、決済装置の前記最終判定部は、前記決済装置に前記ワンタイムパスワードを送ってきた前記決済端末が、前記ユーザ端末から送られてきた前記決済端末特定情報で特定される前記決済端末と一致した場合にのみ決済を許可するようになっていてもよい。

ユーザ端末から決済装置には上述のように、金額情報と、ユーザ情報とが

送られるようになっている。これら情報によれば、どのユーザが幾ら支払いを行おうとしているかを特定することは可能であるが、ユーザが誰に支払いを行おうとしているかは特定することはできない。他方、金額情報と、ユーザ情報とに加えて、決済端末特定情報がユーザ端末から決済装置に送られるのであれば、どのユーザが誰に幾らの支払いを行おうとしているかを特定することができる。最終判定部が、決済装置にワンタイムパスワードを送ってきた決済端末が、ユーザ端末から送られてきた決済端末特定情報で特定される決済端末と一致した場合にのみ決済を許可するようにすることで、ユーザが支払いを行おうとする相手方と、支払いを受けようとする決済端末の管理者との一致をも確認できるようになる。これにより、決済の正当性をより確実にすることが可能となる。

ユーザ端末から決済装置に送られる決済端末特定情報は、各決済端末を特定するための決済端末のID自体であっても良いし、決済端末のIDと一対一対応をした情報（例えば決済端末が置かれた店舗名、或いは店舗名とその店舗の住所又は電話番号を加えた情報）であっても良い。ユーザ端末から決済装置に送られる決済端末特定情報が決済端末のID自体である場合には、決済装置は、各決済端末を区別するための情報として、決済端末のIDを記録したデータベースを備えていれば良い。それにより、決済装置の最終判定部は、決済装置にワンタイムパスワードを送ってきた決済端末が、ユーザ端末から送られてきた決済端末特定情報で特定される決済端末と一致するか否かを判定することができる。他方、ユーザ端末から決済装置に送られる決済端末特定情報が決済端末のID自体ではなく、決済端末のIDと一対一対応をした情報である場合には、決済装置は、各決済端末を区別するための情報として、ユーザ端末から送られてくることが予定された情報及びそれら情報と対応付けられた決済端末のIDとを記録したデータベースを備えていれば良い。それにより、決済装置の最終判定部は、決済装置にワンタイムパスワードを送ってきた決済端末が、ユーザ端末から送られてきた決済端末特定情報で特定される決済端末と一致するか否かを判定することができる。

ユーザ端末で決済端末特定情報を入力する場合、ユーザ端末においては、予め準備されている、例えば幾つかの決済端末特定情報から、ユーザが、自らが支払いを行おうとしている者の決済端末を特定するための決済端末特定情報を選択することができるようになっており、便利である。例えば、ユーザ端末がディスプレイを備えているのであれば、そのディスプレイに、ユーザが選択可能な決済端末特定情報が例えば幾つか例示されるようにし、ユーザがその一つを選択することにより、ユーザが、ユーザ端末に決済端末特定情報を入力することができるようにすることができる。上述したように、ユーザ端末には、ユーザ端末が存在する位置を特定するための情報である位置情報を生成する位置情報生成手段が備えられている場合がある。かかる位置情報生成手段でその位置が特定されたユーザ端末の近くにある決済端末についての決済端末特定情報を、ユーザ端末のディスプレイに選択可能な決済端末特定情報の例として表示することとすれば、ユーザが支払いを行おうとしている決済端末の例として適切であろう。

[0015] ユーザ端末の前記ユーザ端末入力手段は、前記決済装置の前記最終判定部が決済を許可した後において、そのユーザ端末を用いて過去に行われた決済の一つを特定しそれを取消するためのユーザ端末取消情報を入力できるようになっているとともに、前記ユーザ端末送受信手段は、前記ユーザ端末取消情報を前記ネットワークを介して前記決済装置に送るようになっていてもよい。この場合、決済装置の前記決済装置情報処理手段は、前記ユーザ端末取消情報を受付けたときに、前記ユーザ端末取消情報で特定された決済を取消す、取消手段を備えていてもよい。

このようにすることにより、ユーザは自分の意志で、既に認められた決済を取消することができるようになり、例えば、決済に誤りがあったときの訂正が可能となる。

同様の効果は、以下の発明によっても得ることができる。

決済端末の前記決済端末入力手段は、前記決済装置の前記最終判定部が決済を許可した後において、その決済端末を用いて過去に行われた決済の一つ

を特定しそれを取り消すための決済端末取消情報を入力できるようになっているとともに、前記決済端末送受信手段は、前記決済端末取消情報を前記ネットワークを介して前記決済装置に送るようになっていてもよい。この場合、前記決済装置情報処理手段は、前記決済端末取消情報を受付けたときに、前記決済端末取消情報で特定された決済を取り消す、取消手段を備えていてもよい。

この場合には、決済端末の管理者は、自分の意志で、既に認められた決済を取り消すことができるようになる。

ユーザ端末からは上述の場合と同様にユーザ端末取消情報が、決済端末からはこれも上述の場合と同様に決済端末取消情報がそれぞれ、決済端末に送られるようにすることもできる。この場合、前記取消手段は、前記ユーザ端末取消情報と、前記決済端末取消情報とを受付け且つそれらが特定する決済が一致したときに当該決済を取り消すようになっていても良い。

この場合には、決済端末の管理者とユーザ端末を持つユーザとの意志の合致があった場合のみ、既に認められた決済を取り消すことができるようになる。

なお、以上3つの場合のいずれの場合においても、決済の取消を認めることのできる時間を制限することが可能である。例えば、決済装置で決済が認められてから10分以内であれば決済の取消が可能、というのが如きである。

以上の決済の取消を可能とする機能は、特に以下の場合に有用である。これまでに述べたように、従来のクレジットカードにおけるクレジットカードナンバーの如くに用いられる本願発明におけるワンタイムパスワードは、基本的に一度しか使われないいわば使い捨てのものであるから、その盗用の可能性は極めて低くほとんど想定することができない。ただし、例えば、ユーザがスマートフォン等の自らのユーザ端末のディスプレイ等に表示させたワンタイムパスワードを何者かに盗み見され、そのユーザが自らの支払いにそのワンタイムパスワードを使用する前に、つまりユーザが、そのワンタイムパスワードを、ある店舗の決済端末から決済装置に送る前に、そのワンタイム

ムパスワードを知った第三者が、例えば他店舗の決済端末から決済装置に送ってしまうことがあり得る。本願発明の決済装置では基本的に、仮許可情報を生成する場合には、ユーザが本人であることの認証を行うが、決済端末から送られてきたワンタイムパスワードにより決済を行う場合には、そのワンタイムパスワードを決済端末の管理者に渡したのがユーザ本人であるか否かの確認を必ずしも行う必要がない。したがって、正規のユーザのユーザ端末に表示されたワンタイムパスワードを盗み見た悪意の第三者が、正規のユーザよりも先にそのワンタイムパスワードを使用した場合には、決済装置はその不正を見破ることができないおそれがある。

このような不正を防止するために、決済装置の前記最終判定部は、決済を許可しなかったときに、どの決済を許可しなかったかを特定して決済を許可しなかったことを示す不許可情報を生成して前記決済装置送受信手段に送るようになっており、前記決済装置送受信手段は、前記不許可情報を前記ネットワークを介して前記決済端末に送信するようになっていてもよい。この場合、前記不許可情報を受付けた前記決済端末は、どの決済が許可されなかったかを前記決済端末の管理者に通知するようになっていてもよい。このような決済装置と決済端末を有する決済システムにおいては、決済端末を操作するものは、自分がユーザから受取って、決済端末から決済装置に自分が送ったワンタイムパスワードで決済が行えたかどうかを知ることが、例えば不許可情報に基づいて決済端末のディスプレイに表示された内容により知ることができる。決済端末の管理者が、それをユーザに例えば口頭で知らせたのであれば、ユーザは、自らのユーザ端末を操作して上述のユーザ端末取消情報をユーザ端末に生成させ、それを決済装置に送れば良い。そうすることにより、第三者に不正に知得されたワンタイムパスワードにより決済装置で認められた決済を取消することができる。

なお、この場合、決済装置が不許可情報を送信する相手方は、決済端末のみで良い。なぜなら、本願発明の決済システムにおいて、第三者によりワンタイムパスワードが不正に使用されるのは、正規のユーザよりも先に第三者

が正規のユーザが自らのユーザ端末で発生させたワンタイムパスワードを使用した場合のみであり、正規のユーザよりも先に悪意の第三者が使用したワンタイムパスワードによる決済は、決済装置で認められてしまうからである。つまり、悪意の第三者によるワンタイムパスワードの使用があった場合においても、決済ができたかできなかったかでいえば、ワンタイムパスワードによる決済はできてしまっているのであるから、ユーザ端末に不許可情報を送るのはそもそも不可能である。したがって、決済装置は、不許可情報を決済端末のみに送るようになっていけば良い。もっとも、決済装置は、不許可情報を決済端末に送るだけでなく、不許可情報又は同じワンタイムパスワードが2回使用されたことを示す情報（即ち、ワンタイムパスワードが不正使用されたことを示す情報）を、ユーザ端末に送るようになっていても構わない。

これらの処理は、単に、決済装置が、決済端末から送られてきたワンタイムパスワードにより決済を行えたかどうかを、決済端末と、場合によってはユーザ端末とに通知する処理、とすることができる。決済端末の管理者は、その通知の内容により、決済が許可されたことを知ったのであれば、その旨、つまり支払いが終わったことをユーザに伝えれば良い。これは、クレジットカードを用いた決済システムでユーザが支払いを行う場合と何も変わらない。他方、通知の内容により、決済が許可されなかったことを知ったのであれば、ユーザにその旨を伝え、決済の取消と、再度のワンタイムパスワードの生成を促せば良い。これは、クレジットカードを用いた決済システムでユーザが支払いを行う場合と多少異なる手続きとなるが、かかる手続きこそが、本願の決済システムによる決済の確実性をより高める。

[0016] 本願発明者は、決済装置で実行される以下の方法も本願発明の一態様として提案する。これにより得られる効果は、上述の決済システムで得られる効果に同じである。

その方法の一例は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介し

てデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、を含んで構成されている決済システム、を構成するための決済装置に含まれる決済装置情報処理手段にて実行される方法である。

この方法は、前記決済装置情報処理手段が実行する。

具体的には、この方法は、前記決済装置情報処理手段が、前記ユーザ端末において、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報が入力された後に、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とが、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信された際に、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取る過程、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する過程、生成した仮許可情報を、前記決済装置送受信手段により、前記ネットワークを介して前記ユーザ端末に送信する過程、前記仮許可情報を前記決済装置から前記ユーザ端末送受信手段にて受付けた前記ユーザ端末において、前記ユーザ端

末情報処理手段が生成したワнтаイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置送受信手段で受取る過程、前記決済装置が前記決済端末から受取ったワнтаイムパスワードが、前記決済装置で前記仮許可情報が生成されたのと同様かその後に、前記ユーザ端末と同じワнтаイムパスワードを生成することのできるようにされた前記決済装置の前記決済装置情報処理手段で生成されたワнтаイムパスワードと一致したことを条件に、そのワнтаイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを決済するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じる過程、を含む。

[0017] 本願発明者は、所定のコンピュータを、本願発明の決済システムに含まれる決済装置として機能させるためのコンピュータプログラムも本願発明の一態様として提案する。これにより得られる効果は、上述の決済システムで得られる効果に同じである。

そのコンピュータプログラムの一例は、所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、を含んで構成されている決済システム、を構成するための決済装置としてコンピュータを機能させるためのコンピュータプログラムである。

そして、このコンピュータプログラムは、前記コンピュータに、前記ユー

ザ端末において、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報が入力された後に、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とが、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信された際に、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取る過程、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する過程、生成した仮許可情報を、前記決済装置送受信手段により、前記ネットワークを介して前記ユーザ端末に送信する過程、前記仮許可情報を前記決済装置から前記ユーザ端末送受信手段にて受付けた前記ユーザ端末において、前記ユーザ端末情報処理手段が生成したワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置送受信手段で受取る過程、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置で前記仮許可情報が生成されたのと同様かその後に、前記ユーザ端末と同じワンタイムパスワードを生成することのできるようにされた前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを決済する過程、を実行させるとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている。

図面の簡単な説明

[0018] [図1]第1実施形態による決済システムの全体構成を示す図。

[図2]図1に示した決済システムに含まれるユーザ端末の外観を示す図。

[図3]図1に示した決済システムに含まれるユーザ端末のハードウェア構成を示す図。

[図4]図1に示した決済システムに含まれるユーザ端末の内部に生成される機能ブロックを示すブロック図。

[図5]図1に示した決済システムに含まれる決済装置のハードウェア構成を示す図。

[図6]図1に示した決済システムに含まれる決済装置の内部に生成される機能ブロックを示すブロック図。

[図7]図6に示した与信情報記録部に記録されているデータの例を示す図。

[図8]図6に示した位置情報記録部に記録されているデータの例を示す図。

[図9]図6に示したOTP情報記録部に記録されているデータの例を示す図。

[図10]図1に示した決済システムに含まれる決済端末のハードウェア構成を示す図。

[図11]図1に示した決済システムに含まれる決済端末の内部に生成される機能ブロックを示すブロック図。

[図12]図1に示した決済システムに含まれるユーザ端末のディスプレイに表示される画像の一例を示す図。

[図13]図1に示した決済システムに含まれるユーザ端末のディスプレイに表示される画像の他の例を示す図。

[図14]図1に示した決済システムに含まれる決済端末のディスプレイに表示される画像の一例を示す図。

[図15]図1に示した決済システムで決済が行われるときに実行される処理の流れを示す図。

[図16]図1に示した決済システムで決済の取消が行われるときにユーザ端末のディスプレイに表示される画像の一例を示す図。

[図17]第2実施形態の決済システムに含まれるユーザ端末のディスプレイに表示される画像の一例を示す図。

[図18]第2実施形態の決済システムに含まれるユーザ端末の内部に生成される機能ブロックを示すブロック図。

[図19]第2実施形態の決済システムに含まれるユーザ端末のディスプレイに表示される画像の一例を示す図。

[図20]第1実施形態で用いられる金券の一例を示す図。

[図21]第1実施形態で用いられる金券の他の例を示す図。

発明を実施するための形態

[0019] 以下、本発明の第1～第2実施形態について説明する。各実施形態、変形例の説明で同じ対象には同一の符号を付すものとし、重複する説明は場合により省略するものとする。

[0020] 《第1実施形態》

図1に、第1実施形態の決済システムの全体構成を概略で示す。

決済システムは、複数のユーザ端末100-1～100-N（以後、単に、「ユーザ端末100」と記載する場合もある。）、決済装置200及び決済端末300-1～300-n（以後、単に、「決済端末300」と記載する場合もある。）を含んで構成されている。これらはすべて、ネットワーク400に接続可能とされている。

ネットワーク400は、これには限られないが、この実施形態ではインターネットである。

[0021] ユーザ端末100は、本願でいうユーザ端末に相当するものであり、コンピュータを含んでいる。より詳細には、この実施形態におけるユーザ端末100は、汎用のコンピュータにより構成されている。この実施形態では、各ユーザがユーザ端末100をそれぞれ1つずつ所有するものとして説明を行うが、一人のユーザが複数のユーザ端末100を所有しても構わない。クレジットカード又はデビットカードを用いた決済システムで例えるのであれば、1人で複数のクレジットカード又はデビットカードを所有するようなもの

である。もっとも、一つのユーザ端末１００に、例えば異なる決済装置２００の管理者が配布した異なるコンピュータプログラム（これについては、後述する。）を複数インストールすること等により、ユーザは、１つのユーザ端末１００を所有するだけで、ユーザが、複数の決済装置２００における決済を一つのユーザ端末１００で行えるようにすることも可能である。これは、従来のクレジットカードを用いた決済システムにおいて、ユーザが複数のクレジットカードを所持しているのと同様の状態である。しかしながら、本願発明によればユーザは、物理的に嵩張るクレジットカードを、複数枚所持する必要はない。

[0022] 次に、ユーザ端末１００の構成を説明する。各ユーザ端末１００－１～１００－Ｎの構成は、本願発明との関連でいえば同じである。

ユーザ端末１００は、携帯電話、スマートフォン、タブレット、ノート型パソコン、デスクトップ型パソコン等である。可搬であり、且つ後述するプログラムをインストールするのに向いているという点を考慮すれば、これらのうち、特に、スマートフォンかタブレットが、ユーザ端末１００として用いるのに好ましい。スマートフォンは例えば、Apple Japan 合同会社が製造、販売を行うiPhone（商標）である。タブレットの例はApple Japan 合同会社が製造、販売を行うiPad（商標）である。以下、これには限られないが、ユーザ端末がスマートフォンであることとして話を進める。

[0023] ユーザ端末１００の外観の一例を図２に示す。

ユーザ端末１００は、ディスプレイ１０１を備えている。ディスプレイ１０１は、静止画又は動画を表示するためのものであり、公知、或いは周知のものをを用いることができる。ディスプレイ１０１は例えば、液晶ディスプレイである。ユーザ端末１００は、また入力装置１０２を備えている。入力装置１０２は、ユーザが所望の入力をユーザ端末１００に対して行うためのものである。入力装置１０２は、公知或いは周知のものをを用いることができる。この実施形態におけるユーザ端末１００の入力装置１０２はボタン式のも

のとなっているが、これには限られず、テンキー、キーボード、トラックボール、マウスなどを用いることも可能である。また、ディスプレイ 101 がタッチパネルである場合、ディスプレイ 101 は入力装置 102 の機能を兼ねることになり、この実施形態ではそうされている。

[0024] ユーザ端末 100 のハードウェア構成を、図 3 に示す。

ハードウェアには、CPU (central processing unit) 111、ROM (read only memory) 112、RAM (random access memory) 113、インターフェイス 114 が含まれており、これらはバス 116 によって相互に接続されている。

CPU 111 は、演算を行う演算装置である。CPU 111 は、例えば、ROM 112 に記録されたコンピュータプログラムを実行することにより、後述する処理を実行する。なお、ここでいうコンピュータプログラムには、本願発明のユーザ端末としてこのユーザ端末 100 を機能させるためのコンピュータプログラムが少なくとも含まれる。このコンピュータプログラムは、ユーザ端末 100 にプリインストールされていたものであっても良いし、事後的にインストールされたものであっても良い。このコンピュータプログラムのユーザ端末 100 へのインストールは、メモリカード等の所定の記録媒体を介して行なわれても良いし、LAN 或いはインターネットなどのネットワークを介して行なわれても構わない。

ROM 112 は、CPU 111 が後述する処理を実行するために必要なコンピュータプログラムやデータを記録している。ROM 112 に記録されたコンピュータプログラムは、これに限られず、ユーザ端末 100 がスマートフォンであれば、ユーザ端末をスマートフォンとして機能させるために必要な、例えば、通話や電子メールを実行するためのコンピュータプログラムやデータが記録されている。ユーザ端末 100 は、また、ネットワーク 400 を介して受取ったデータに基づいて、ホームページを閲覧することも可能とされており、それを可能とするための公知の web ブラウザを実装している。

RAM 113は、CPU 111が処理を行うために必要なワーク領域を提供する。

インターフェイス 114は、バス 116で接続されたCPU 111やRAM 113等と外部との間でデータのやり取りを行うものである。インターフェイス 114には、上述のディスプレイ 101と、入力装置 102とが接続されている。入力装置 102から入力された操作内容は、インターフェイス 114からバス 116に入力されるようになっているとともに、後述する画像データは、インターフェイス 114から、ディスプレイ 101に出力されるようになっている。インターフェイス 114は、また、いずれも図示を省略する、GPS機構と、送受信部とに接続されている。

GPS機構は、地球上におけるユーザ端末 100が存在する位置を検出するものである。GPS機構は、検出したユーザ端末 100の位置を特定する位置情報を生成するようになっている。GPS機構は、公知又は周知のものであり、例えば静止衛星からの電波を受取ることにより、ユーザ端末 100の位置を検出するようになっている。位置情報は、インターフェイス 114により受取られるようになっている。

送受信部は、インターネットであるネットワーク 400を介してのデータの送受信を行うものである。かかる通信は、有線で行われる場合もあるが、ユーザ端末 100がスマートフォンである場合には、かかる通信は無線で行われる。それが可能な限り、送受信部の構成は、公知或いは周知のものとすることができる。送受信部がネットワーク 400から受取ったデータは、インターフェイス 114により受取られるようになっており、インターフェイス 114から送受信部にわたされたデータは、送受信部によって、ネットワーク 400を介して外部、例えば、決済装置 200に送られるようになっている。

[0025] CPU 111がコンピュータプログラムを実行することにより、ユーザ端末 100内部には、図4で示されたような機能ブロックが生成される。なお、以下の機能ブロックは、ユーザ端末 100を本願発明のユーザ端末として

機能させるための上述のコンピュータプログラム単体の機能により生成されていても良いが、上述のコンピュータプログラムと、ユーザ端末１００にインストールされたＯＳその他のコンピュータプログラムとの協働により生成されても良い。

ユーザ端末１００内には、本願発明の機能との関係で、以下のような制御部１２０が生成され、制御部１２０内に、主制御部１２１、表示制御部１２２、データ入出力部１２３、ＯＴＰ生成部１２４が生成される。

[0026] 制御部１２０は、以下に説明するような情報処理を実行する。

主制御部１２１は、制御部１２０内の全体的な制御を行う。例えば、主制御部１２１は、追って詳述するデータ入出力部１２３から受取ったデータに基づいて表示制御部１２２の制御を行う。

主制御部１２１は、追って説明するデータ入出力部１２３から、これも追って説明する仮許可情報を受取った場合に、その旨をＯＴＰ生成部１２４に通知するようになっている。主制御部１２１は、また、データ入出力部１２３から、後述するユーザＩＤとパスワードと金額情報とを受取るようになっている。主制御部１２１は、また、データ入出力部１２３から、後述するユーザ端末取消情報を受取る場合がある。また、主制御部１２１は、図示を省略のメモリ等からなる記録手段を内蔵しており、そこに、端末情報を記録している。端末情報の例としては、ユーザ端末１００がスマートフォンである場合における当該スマートフォンに組込まれたＳＩＭカード（Subscriber Identity Module Card）に記録されたＩＤ番号や、スマートフォンの製造番号等の個体識別番号を挙げることができる。主制御部１２１は、これら端末情報のうちの少なくとも一つを、ユーザ端末１００から予め取得しておく。なお、主制御部１２１は、端末情報を、ユーザが支払いの処理を行う都度、ユーザ端末１００から取得するようになっていても構わない。いずれにせよ、主制御部１２１は、後述するタイミングで、ユーザＩＤとパスワードと金額情報とそして端末情報とを、データ入出力部１２３に送るようになっている。

主制御部 121 は、また、OTP 生成部 124 から、ワンタイムパスワードを受取るようになっている。

表示制御部 122 は、主制御部 121 の制御を受けつつ、ディスプレイ 101 に表示される画像の制御を行う。ディスプレイ 101 には、表示制御部 122 から送られたデータに基づく画像が表示される。主制御部 121 は、表示制御部 122 に対して、ディスプレイ 101 にどのような画像を表示させるべきかという指示を送る。

[0027] データ入出力部 123 は、制御部 120 へのデータの入出力を行うものである。具体的には、データ入出力部 123 は、入力装置 102 からの入力を受取るようになっている。入力装置 102 からデータ入出力部 123 へ入力されるのは、例えば、決済の開始の指示、ユーザ ID、パスワード、金額情報、ユーザ ID とパスワードと金額情報との送信の指示、ユーザ端末取消情報である。これらはいずれも主制御部 121 に送られるようになっている。

また、データ入出力部 123 は、送受信部から、追って説明する、決済装置 200 からネットワーク 400 を介して送られて来た仮許可情報を受取るようになっている。データ入出力部 123 は、受取った仮許可情報を、主制御部 121 に送るようになっている。

また、データ入出力部 123 は、GPS 機構から、位置情報を受取るようになっている。データ入出力部 123 は、受取った位置情報を主制御部 121 に送るようになっている。

また、データ入出力部 123 は主制御部 121 から、ユーザ ID、パスワード、端末情報、及び金額情報を受取るようになっている。ユーザ ID は、ユーザを特定するための各ユーザにユニークな情報であり、これには限られないがこの実施形態では、後述するように所定の文字数の英数字の羅列とされている。パスワードは、ユーザの認証をより確実にするための情報であり、これには限られないがこの実施形態では、後述するように所定の文字数の英数字の羅列とされている。端末情報は、ユーザ端末 100 を特定するための情報であり、これもユーザの認証をより確実にすることを目的とする。こ

れには限られないがこの実施形態における端末情報は、後述するように所定の文字数の数字の羅列とされている。金額情報は、ユーザが、決済端末300の管理者に支払いを行おうとする金額を特定するための情報であり、所定の単位（円、ドル、ユーロ等）の金額を表す数字である。データ入出力部123には、また、主制御部121から、位置情報と、ワンタイムパスワードとが送られるようになっている。なお、位置情報は、データ入出力部123から主制御部121を経てデータ入出力部123に戻されるのではなく、GPS機構からデータ入出力部123に入力された状態のまま、データ入出力部123にて保持されていても構わない。また、ワンタイムパスワードは、主制御部121を経ずに、OTP生成部124から直接データ入出力部123に送られるようになっているても構わない。ユーザ端末取消情報は、後述するようにして既に終了した過去の決済の一つを取消するためのユーザの意思表示を示す情報であり、入力装置102を用いてユーザが入力するものである。ユーザ端末取消情報には、ユーザが取消を望む過去の決済の一つを特定する情報が少なくとも含まれている。

ユーザID、パスワード、端末情報、金額情報、位置情報、ワンタイムパスワード、ユーザ端末取消情報等は、それぞれについて適切な後述するタイミングで、データ入出力部123から、送受信部に送られるようになっており、これらのうちワンタイムパスワードを除いたものは、送受信部からネットワーク400を介して、決済装置200に送られるようになっている。

[0028] OTP生成部124は、上述したように、主制御部121が仮許可情報を受取った場合、主制御部121からその旨を通知されるようになっている。その通知を受けた場合に、OTP生成部124はワンタイムパスワードを生成するようになっている。ワンタイムパスワードの生成の仕方は従来技術に倣うことができる。ワンタイムパスワードの生成の仕方の具体例については、後述する。

[0029] 次に、決済装置200について説明する。

決済装置200は一般的なコンピュータである。ハードウェア構成として

は、従来の決済システムにおける決済装置と同等のもので良い。

[0030] 決済装置200のハードウェア構成の一例を、図5に示す。

ハードウェアには、CPU211、ROM212、RAM213、インターフェイス214が含まれており、これらはバス216によって相互に接続されている。

CPU211は、演算を行う演算装置である。CPU211は、例えば、ROM212に記録されたコンピュータプログラムを実行することにより、後述する処理を実行する。なお、ここでいうコンピュータプログラムには、本願発明の決済装置としてこの決済装置200を機能させるためのコンピュータプログラムが少なくとも含まれる。このコンピュータプログラムは、決済装置200にプリインストールされていたものであっても良いし、事後的にインストールされたものであっても良い。このコンピュータプログラムの決済装置200へのインストールは、メモリカード等の所定の記録媒体を介して行なわれても良いし、LAN或いはインターネットなどのネットワークを介して行なわれても構わない。

ROM212は、CPU211が後述する処理を実行するために必要なコンピュータプログラムやデータを記録している。ROM212に記録されたコンピュータプログラムは、これに限られず、他の必要なコンピュータプログラムが記録されていても良い。

RAM213は、CPU211が処理を行うために必要なワーク領域を提供する。

ROM212、RAM213に加えて、その他の記録媒体、例えば、HDD (Hard Disk Drive) やSSD (Solid State Drive) を設けて、それらにROM212、RAM213の機能の一部を賄わせることができるのは当然である。

インターフェイス214は、バス216で接続されたCPU211やRAM213等と外部との間でデータのやり取りを行うものである。インターフェイス214は、少なくとも送受信部に接続されている。送受信部がネット

ワーク４００から受取ったデータは、インターフェイス２１４により受取られるようになっており、インターフェイス２１４から送受信部にわたされたデータは、送受信部によって、ネットワーク４００を介して外部、例えば、ユーザ端末１００に送られるようになっている。

[0031] CPU 211がコンピュータプログラムを実行することにより、決済装置２００内部には、図６で示されたような機能ブロックが生成される。なお、以下の機能ブロックは、決済装置２００を本願発明の決済装置として機能させるための上述のコンピュータプログラム単体の機能により生成されていても良いが、上述のコンピュータプログラムと、決済装置２００にインストールされたOSその他のコンピュータプログラムとの協働により生成されても良い。

決済装置２００内には、本願発明の機能との関係で、以下のような制御部２２０が生成される。制御部２２０内には、データ入出力部２２１、主制御部２２２、与信判定部２２３、与信情報記録部２２４、最終判定部２２５、位置情報記録部２２６、OTP生成部２２７、OTP情報記録部２２８が生成される。

[0032] データ入出力部２２１は、制御部２２０へのデータの入出力を行うものである。具体的には、データ入出力部２２１は、主制御部２２２から後述する種々のデータを受付けるようになっている。主制御部２２２から受付けた種々のデータを、データ入出力部２２１は、送受信部に渡すようになっており、送受信部はそれらデータを、ネットワーク４００を介してユーザ端末１００又は決済端末３００に送るようになっている。

データ入出力部２２１は、また、ネットワーク４００を介してユーザ端末１００又は決済端末３００から送受信部が受取った後述する種々のデータを送受信部から受取り、受取ったそれらデータを主制御部２２２に送るようになっている。

[0033] 主制御部２２２は、制御部２２０内の全体的な制御を行う。

主制御部２２２は、データ入出力部２２１から、ユーザIDとパスワード

と端末情報とそして金額情報とを受取る場合がある。主制御部２２２がそれらを受取った場合、主制御部２２２は、それらと与信判定部２２３へと送るようになっている。

主制御部２２２は、データ入出力部２２１から、ユーザ端末１００から送られてきた位置情報を受取る場合がある。主制御部２２２は、この位置情報を受取った場合には、それを最終判定部２２５に送るようになっている。

主制御部２２２は、また、与信判定部２２３から、後述する仮許可情報を受取る場合がある。主制御部２２２がそれを受取った場合、主制御部２２２は、それをデータ入出力部２２１へと送るようになっている。主制御部２２２は、また、データ入出力部２２１から、それらのいずれもが決済端末３００から送られてきたものである、共に後述する決済申込情報と、ワンタイムパスワードと、ユーザＩＤとを受取る場合がある。主制御部２２２がそれらを受取った場合、主制御部２２２は、それらと最終判定部２２５へと送るとともに、ワンタイムパスワードを生成せよとの指示をＯＴＰ生成部２２７へと送るようになっている。

主制御部２２２は、また、ＯＴＰ生成部２２７からワンタイムパスワードを受取る場合がある。主制御部２２２がそれを受取った場合、主制御部２２２は、それを最終判定部２２５へと送るようになっている。なお、ワンタイムパスワードは、必ずしも主制御部２２２を介して最終判定部２２５へと送られる必要はなく、例えばＯＴＰ生成部２２７から直接最終判定部２２５へと送られるようになっていても構わない。

主制御部２２２は、また、最終判定部２２５から、後述する最終判定データを受取る場合がある。主制御部２２２は、それを受取った場合、決済処理を行うようになっている。決済処理は、あるユーザから、そのユーザへの支払いを求めるための仮許可情報を送信してきた決済端末３００の管理者への決済を認めるための処理である。主制御部２２２は、どのような決済を行ったかというデータを保持するようになっている。例えば、主制御部２２２は、誰から誰への幾らの支払いを最終的に許可したのかという情報を、各ユー

が毎に図示せぬ記録媒体に記録するようになっている。また、決済の処理の一環として主制御部２２２は、与信情報記録部２２４の内容を書換えるが、これについては後述する。

主制御部２２２は、データ入出力部２２１から、ユーザ端末取消情報と、後述する決済端末取消情報とを受取る場合がある。主制御部２２２がそれらを受取った場合であって、且つそれらユーザ端末取消情報と、決済端末取消情報とによって特定される過去の決済が同一の場合には、主制御部２２２は当該過去の決済を取消するための処理を行うようになっている。もっとも、かかる決済の取消の処理は、必ずしも必須のものではなく、決済の取消の処理が不要なのであれば、ユーザ端末１００、決済装置２００、決済端末３００からかかる処理にのみ必要な機能を削除することも可能である。なお、この実施形態においては、主制御部２２２は、ユーザ端末取消情報と、後述する決済端末取消情報との双方を受取り、且つそれらユーザ端末取消情報と、決済端末取消情報とによって特定される過去の決済が同一の場合にのみ過去の決済を取消することとしていたが、これに代えて、主制御部２２２は、ユーザ端末取消情報と決済端末取消情報のいずれか一方のみを受付けたときに、そのユーザ端末取消情報又は決済端末取消情報で特定される過去の決済を取消するようになっていても構わない。また、主制御部２２２は、過去の決済のうち、比較的新しいものについてのみ決済の取消を行うようになっていても良い。例えば、主制御部２２２は、上述の決済の処理が終了してから１０分以内のものに限り、決済の取消を認めるようになっていても良い。

[0034] 与信判定部２２３は、上述したように、主制御部２２２からユーザＩＤとパスワードとそして端末情報とを受取るようになっている。与信判定部２２３は、それらを受取った場合、与信判定を行うようになっている。与信判定は、ユーザＩＤとパスワードとそして端末情報で特定されるユーザについての、上記金額情報で特定される金額の支払いの決済が可能か否かの判定である。かかる与信判定には、ユーザが正当なものであるか否かのいわゆる認証の処理も含まれる。

与信判定部２２３は、与信情報記録部２２４に記録されているデータを、認証の処理を含む与信判定のために利用する。

[0035] 与信情報記録部２２４には、図７に示したようなデータが記録されている。

これには限られないが、この実施形態で与信情報記録部２２４に記録されているのは、ユーザＩＤ、パスワード、端末情報、及び預金残高である。これらは、各ユーザ毎に紐付けられている。なお、これらに加えて、ユーザそれぞれの本名や、電話番号、電子メールアドレス等が記録されていても構わないのは当然である。

ユーザＩＤは、各ユーザを特定するための情報である。これには限られないが、この実施形態におけるユーザＩＤは、所定の文字数の英数字の羅列となっている。ユーザＩＤは、各ユーザが決定するか、さもなくば決済装置２００の管理者が決定する。ユーザＩＤがユーザにより決定される場合には、公知又は周知の方法によって、ユーザＩＤはユーザから決済装置２００の管理者に通知され、通知されたユーザＩＤが与信情報記録部２２４に記録される。

パスワードは、各ユーザの正当性を確認するための情報である。これには限られないが、この実施形態におけるパスワードは、所定の文字数の英数字の羅列となっている。パスワードは、各ユーザが決定する。パスワードは、公知又は周知の方法によって、ユーザから決済装置２００の管理者に通知され、通知されたパスワードが与信情報記録部２２４に記録される。

端末情報は、各ユーザの正当性を更に強固に確認するための情報である。その具体例がＳＩＭカードに記録されたＩＤ番号や、スマートフォンの製造番号等であることは、既に述べた通りである。端末情報は、ユーザ端末１００毎にユニークに決定されている。端末情報は、公知又は周知の方法によって、例えばユーザから、決済装置２００の管理者に通知され、通知された端末情報が与信情報記録部２２４に記録される。

預金残高は、各ユーザの預金の額であり、各ユーザの口座に入っている金

銭の金額を示すものである。預金残高は、それを特定する預金残高情報として、与信情報記録部２２４に記録されている。預金残高は、ユーザが決済装置２００の管理者に対して予め幾らかの金銭を支払っている場合、における決済装置２００の管理者が管理するユーザの口座に入っている金銭の金額である場合がある。このような場合、この決済システムは、いわゆるプリペイド方式による決済システムとなる。或いは、預金残高は、決済装置２００の管理者が預金の管理を事業として行っている銀行等である場合、或いは決済装置２００の管理者が銀行等と提携している場合における、当該銀行にユーザが持つ口座に入っている金銭の金額である場合がある。この実施形態では、どちらの場合も、あり得る。

[0036] 与信判定部２２３は、主制御部２２２からユーザＩＤとパスワードと端末情報とそして金額情報とを受取ると、受取ったユーザＩＤと同じユーザＩＤと対応付けられた、パスワード、端末情報、及び預金残高を、与信情報記録部２２４から読み出す。与信判定部２２３が受取ったユーザＩＤと同じユーザＩＤが与信情報記録部２２４に存在しない場合には、パスワード等の情報を与信判定部２２３は、与信情報記録部２２４から読み出さない。この場合には、与信判定部２２３は、与信判定の処理を中止する。

与信判定部２２３が主制御部２２２から受取ったユーザＩＤと同じユーザＩＤが与信情報記録部２２４に記録されており、受取ったユーザＩＤと同じユーザＩＤと対応付けられた、パスワード、端末情報、及び預金残高が与信情報記録部２２４から読み出された場合には、与信判定部２２３は、主制御部２２２から受取ったパスワード及び端末情報が、与信情報記録部２２４から読み出されたパスワード及び端末情報と同じか否か判定するようになっている。それらが共に一致したのであれば、与信判定部２２３は、そのユーザＩＤ等を送って来たユーザが正当なユーザであると認証し、パスワード及び端末情報の少なくとも一方が一致しなかったのであれば、そのユーザＩＤ等を送って来たユーザが正当なユーザでないと判定して、与信判定の処理を中止する。ここまでが、認証の処理である。つまり、この実施形態の与信判定

における認証の処理でユーザが正当であると認められるには、ユーザが送ってきたユーザIDとパスワードと端末情報とのすべてが、与信情報記録部224に記録されていたそれらと完全に一致することが条件とされる。認証の処理で、そのパスワードを送って来たユーザが正当なユーザであると認証された場合には、与信判定部223は、ユーザの求める決済を認めて良いか否かについての与信の判定を行う。

与信の判定は、ユーザ端末100から送信されてきた金額情報と、その金額情報と紐付けられていたユーザIDと紐付けられていた、上記与信情報記録部224から読み出された預金残高とを比較することにより行われる。これには限られないが、この実施形態では、預金残高の方が、金額情報で特定される金額と同じかそれよりも大きい場合に、ユーザの求める決済が認められる。その場合には、与信判定部223は、仮許可情報を生成する。他方、預金残高が、金額情報で特定される金額よりも小さい場合には、ユーザの求める決済は認められない。この場合には、与信判定部223は仮許可情報を生成しない。与信判定部223が仮許可情報を生成した場合には、その仮許可情報は主制御部222に送られるようになっている。

また、与信判定部223は時刻を特定する機能を有しており（通常のコンピュータが有する時計の機能を利用しても良い。）、与信判定を行った時刻を特定するための時刻情報を主制御部222に通知するようになっている。かかる時刻情報は、主制御部222から最終判定部225に送られるようになっている。

[0037] 最終判定部225は、上述したように、主制御部222から、ユーザ端末100から送られてきた位置情報を受取る場合がある。主制御部222は、また、データ入出力部221から、それらのいずれもが決済端末300から送られてきたものである、決済申込情報と、ユーザIDと、ワンタイムパスワードとを受取る場合がある。これには限られないがこの実施形態では、決済申込情報と、ユーザIDと、ワンタイムパスワードは、決済端末300から決済装置200にまとめて送られ、それら3つの情報は、最終判定部22

５にまとめて受取られる。最終判定部２２５は、決済申込情報、ユーザＩＤ、及びワンタイムパスワードを受取った場合に、最終判定の処理を行う機能を有する。最終判定は、ユーザが希望した、決済端末３００の管理者への支払いを最終的に認めるか否かについての判定である。

最終判定部２２５は、位置情報記録部２２６に記録されている情報を、最終判定を行うために利用する。また、ＯＴＰ生成部２２７から主制御部２２２を経て提供されるワンタイムパスワードも、最終判定に利用する。

[0038] 位置情報記録部２２６には、図８に示したように、決済端末ＩＤと、位置情報とが互いに紐付けた状態で記録されている。

決済端末ＩＤは、各決済端末３００を区別し、特定するためのものである。この実施形態における決済端末３００は n 個であるので、もちろんこれには限られないが、この実施形態では、自然数である $1 \sim n$ の連番を、各決済端末３００を特定するための決済端末ＩＤとして用いることとしている。

位置情報は、それと紐付けられた決済端末３００が存在する位置を特定するための情報である。この実施形態における位置情報は、緯度と経度とで、決済端末３００の位置を特定することとしている。図８において、「N」又は「S」の文字が付された左側に位置する数字は、前者が北緯、後者が南緯である緯度を、「E」又は「W」の文字が付された右側に位置する数字は、前者が東経、後者が西経である経度を、それぞれ特定するものとなっている。もっとも、位置情報の形式は、緯度と経度の組合せに限らない。なお、ユーザ端末１００のGPS機構で生成される位置情報も、この実施形態では同様の形式となっている。

なお、図８において、決済端末ＩＤが４のものには、位置情報が設定されていない。例えば、決済端末３００がインターネット上の仮想店舗の決済に用いられるものである場合には、後述する理由で、決済端末３００の位置を特定することにあまり意味が無い。そのような決済端末３００については位置情報の設定がなされないこともあり得る。

位置情報は、例えば、決済端末３００の管理者が、決済端末３００を設置

する際に決済装置 200 の管理者に、電子メールや書簡等の適当な手段で通知することにより決済装置 200 の管理者に知らせることが可能である。決済装置 200 の管理者は、通知された位置情報を各決済端末 300 の決済端末 ID に紐づけて位置情報記録部 226 に記録すれば良い。

上述した決済申込情報には、その決済申込情報を送信した決済端末 300 の決済端末 ID が付されている。最終判定部 225 は、決済申込情報とワンタイムパスワードとを受取ったときに、その決済申込情報に付された決済端末 ID と一致する決済端末 ID に紐付けられた位置情報を、位置情報記録部 226 から読み出すようになっている。

[0039] OTP 生成部 227 は、ワンタイムパスワードを生成する機能を有している。

上述したように、主制御部 222 は、データ入出力部 221 から、決済申込情報と、ワンタイムパスワードとを受取ると、ワンタイムパスワードを生成せよとの指示を OTP 生成部 227 へと送る。この指示を受取ると OTP 生成部 227 は、ワンタイムパスワードを生成する。なお、この実施形態では、決済装置 200 でワンタイムパスワードが生成されるタイミングは、決済申込情報と、ユーザ端末 100 で生成されたワンタイムパスワードとを決済装置 200 が受取った後であるが、これはこの限りではない。決済装置 200 は例えば、仮許可情報が生成されると同時かそれ以降であって、最終判定部 225 が最終判定を行うよりは前の適当なタイミングで、OTP 生成部 227 にワンタイムパスワードを作らせるようになっていれば良い。

ワンタイムパスワードの生成の仕方は従来技術に倣えばよいが、その具体例は、例えば以下の通りである。

ワンタイムパスワードを生成するには、ある初期値（2 つ以上の場合もある）を用い、過去の値を所定の関数に代入することにより、新しい値を順次作るという方法をワンタイムパスワードが必要となる度に実行すれば良い。そうすることにより、上記「値」であるワンタイムパスワードを連続して生成することができる。このようなワンタイムパスワードは、初期値依存性の

ある擬似乱数となる。

上述の「値」を作るのに使われる関数の例として、以下の (a) ~ (c) を挙げる。以下の (a) ~ (c) はいずれも、N 番目の「値」である X_N を作るための式である。また、P、Q、R、S は自然数である。

$$(a) \quad (X_N) = (X_{N-1})^P + (X_{N-2})^Q$$

$$(b) \quad (X_N) = (X_{N-1})^P$$

$$(c) \quad (X_N) = (X_{N-1})^P (X_{N-2})^Q (X_{N-3})^R (X_{N-4})^S$$

(a) は、過去の「値」2つを用い、それらをそれぞれP乗とQ乗したものを足し合わせるにより、新しい「値」を生成する。なお、正確には、過去の「値」2つを用い、それらをP乗とQ乗したものを足し合わせると、桁数が増えるため、実際には得られた値のうちの頭から適当な桁数を抜き出す、末尾から適当な桁数を抜き出す、或いはその値のうちの適当な部分から適当な桁数を抜き出すこと等により、新しい「値」を生成する。

(b) は、過去の「値」1つを用い、それをP乗したものの桁数を上述のように整理したものを新しい「値」とするものである。

(c) は、過去の「値」4つを用い、それらをそれぞれP乗、Q乗、R乗、S乗したものの積を取り、その後上述したように桁数を整理したものを新しい「値」とするものである。

上述の (a) ~ (c) はワンタイムパスワードを生成するためのアルゴリズムの一例であり、ワンタイムパスワードを生成する際にアルゴリズムに変化を加える、例えば、上述の (a) ~ (c) を順番に用いる等の変化を加えることも可能である。

OTP生成部227は、ワンタイムパスワードを生成するにあたって、OTP情報記録部228に記録されているデータを利用する。OTP情報記録部228には、例えば、図9に記載したようなデータが記録されている。OTP情報記録部228に記録されているのは、ユーザID、初期値、生成回数である。これらのうち、必須のものは初期値のみである。

OTP情報記録部228に記録されているユーザIDは、与信情報記録部

224に記録されているユーザIDと同じものであり、各ユーザを特定するためのものである。

初期値は、ワンタイムパスワードを生成する場合に用いられる初期値である。

初期値は、各ユーザ端末100毎に異なるものとなっている。各ユーザ端末100のOTP生成部124で生成されるワンタイムパスワードと同じワンタイムパスワードを、決済装置200のOTP生成部227で生成できるようにするため、各ユーザ端末100に与えられた初期値と同じ初期値が、OTP情報記録部228に記録されている。上述したように、ワンタイムパスワードは初期値依存性のある擬似乱数となる。言い換えれば、あるユーザ端末100用のワンタイムパスワードは、同じ順番のもの同士を比較すれば、常に同じものとなるようになっている。したがって、各ユーザ端末100に持たせた初期値と同じワンタイムパスワードを決済装置200において準備しておけば、決済装置200は、どのユーザ端末100におけるワンタイムパスワードをも再現できることになる。この実施形態では、OTP情報記録部228に記録されている初期値は、各ユーザ端末100について2つである。これは、これには限られないがこの実施形態では、過去の2つの「値」を利用して新しい「値」を生成する、上述した(a)の数式を用いてワンタイムパスワードを生成するからである。OTP情報記録部228には、新しい「値」を生成するのに必要なだけの過去の値、即ちワンタイムパスワードを記録しておけば足りる。

生成回数は、そのユーザ端末100用のワンタイムパスワードを何回生成したかを示す数値である。上述したように、ワンタイムパスワードは乱数ではあるが、擬似乱数である。生成回数0回の場合は、初期値を用いて1番目に生成されるワンタイムパスワードが後述する最終判定に用いられ、生成回数が1回のときは、上述の初期値を用いて2番目に生成されるワンタイムパスワードが最終判定に用いられ、生成回数がN回のときは、上述の初期値を用いてN-1番目に生成されるワンタイムパスワードが最終判定に用いられ

るようになっている。

OTP生成部227は、主制御部222から、ワンタイムパスワードを生成せよとの指示を受けると、ワンタイムパスワードとともに受取ったユーザIDと紐付けられている初期値と、生成回数とを、OTP情報記録部228から読み出す。OTP生成部227は、上述した数式(a)に初期値を代入して、読み出した生成回数がNのときに、N-1番目までの値を生成する。それが、最終判定に使用されるワンタイムパスワードとなる。

なお、ユーザ端末100のOTP生成部124でも、同様の方法でワンタイムパスワードが生成される。上述したようにユーザ端末100のOTP生成部124は、決済装置200のOTP情報記録部228に記録されたのと同じ初期値を持っており、また決済装置200のOTP生成部227で 사용되는のと同じ数式(この実施形態の場合であれば、数式(a))を使用できるようになっており、且つOTP情報記録部228に記録されるのと同じように、過去に何回「値」を生成したかということを特定する生成回数の記録を行えるようになっている。それにより、ユーザ端末100と決済装置200とで生成されるワンタイムパスワードは、常に同期させることができる。

このように、ワンタイムパスワードを生成する2つの装置で同じワンタイムパスワードを生成する、或いはワンタイムパスワードを同期させるために、2つの装置で同じ順番で生成されたワンタイムパスワードを用いる方法を一般に、イベント同期と呼ぶ。上述の方法は、イベント同期を用いたワンタイムパスワードの手法を採用したものである。他方、ワンタイムパスワードを同期させるために、時刻の情報をを用いることもできる。このようなワンタイムパスワードの同期方法を一般に、時刻同期と呼ぶ。イベント同期も、時刻同期も公知の技術であり、いずれかを用いることにより、ワンタイムパスワードを同期させることも可能である。

いずれにせよ、OTP生成部227は、生成したワンタイムパスワードを、主制御部222を介して、最終判定部225に送る。また、OTP生成部

227は、OTP情報記録部228に記録されていた、そのユーザ端末100用のワンタイムパスワードが作られたユーザ端末100のユーザIDと紐付けられていた、生成回数を+1するように書き換える。

[0040] なお、OTP情報記録部228に記録されるべき情報のうち、必須なのは初期値のみであると上述した。その場合、ユーザ端末100で生成されるワンタイムパスワードと、決済装置200で生成されるワンタイムパスワードとは以下のようにして同期される。

まず、生成回数の情報がない場合である。この場合、決済装置200のOTP生成部227は、新しい「値」を生成するたびに、古いものから「値」を消去して、それを一つ新しい「値」で上書きするという処理を繰り返す。同様の処理をユーザ端末100でも繰り返すことにより、過去何回「値」を生成したかという生成回数の情報を用いずとも、ユーザ端末100で生成されるワンタイムパスワードと、決済装置200で生成されるワンタイムパスワードとを同期させることが可能となる。

次にユーザIDがない場合である。ユーザIDが存在しない場合には、ユーザIDの代わりとなる、ユーザを特定するための情報でユーザを特定する。ユーザを特定するための情報が原則として必要となるのは、決済装置200がワンタイムパスワードを生成するための条件はユーザ毎に異なるため（例えば、この実施形態ではユーザ毎に割当てられた初期値が異なるが、用いる数式つまりアルゴリズムをユーザ毎に変えることも可能である。）、決済装置200においてユーザ毎に異なる条件のうちのどの条件でワンタイムパスワードを生成させるかを確定するために、ユーザを特定するための情報が必要となる。例えば、ユーザは、ユーザIDでなく、後述する決済端末300が備えるタッチパネル式のディスプレイに対して署名を行うことにより、決済端末300からその署名を電子データとして、決済装置200に送信することが可能である。或いは、ユーザの指紋や静脈の性状等の生体情報を読み取り装置を決済端末300に設けることにより、読み取り装置で読取った指紋や静脈の性状等を電子データとして、決済装置200に送信すること

が可能である。これらの場合、OTP情報記録部228には、ユーザIDの代わりに、或いはそれに加えて、署名、指紋や静脈の性状等が記録されることになる。

[0041] 最終判定部225は、上述したように、主制御部222から、決済申込情報及びワンタイムパスワードを受取る。また、その前に、最終判定部225は、主制御部222から、ユーザ端末100から送られてきた位置情報と、与信判定部223で生成された時刻情報とを受取っている。

他方、最終判定部225は、位置情報記録部226から、決済申込情報を決済装置200に送って来た決済端末300の位置を示す位置情報を受取るとともに、OTP生成部227から、ワンタイムパスワードを受取る。

最終判定部225は、主制御部222を介して受取った決済端末300からのワンタイムパスワードと、これも主制御部222を介して受取ったOTP生成部227からのワンタイムパスワードとを比較するとともに、主制御部222を介して受取ったユーザ端末100の位置を示す位置情報と、位置情報記録部226から受取った位置情報とを比較する。その結果、比較した上記2つのワンタイムパスワードが一致する、比較した2つの上記位置情報により特定される位置が、所定の距離、例えば20m以内の場合である、そしてこの比較が行われた時刻が与信判定部223から主制御部222を介して受付けた時刻情報で特定される時刻から所定の時間、例えば5分、或いは30分以内である、という3つの条件がすべて満たされたときのみ、最終判定部225は、ユーザ端末100のユーザからの決済端末300の管理者への支払いを認める決定を最終的に行う。最終判定部225は、3つの条件のいずれかが充足されない場合には、上記支払を認めないとの決定を最終的に行う。これら両決定を、最終判定と称する。

最終判定部225が最終判定を行った場合、最終判定部225は、主制御部222に、最終判定の結果を示すデータである最終判定データを送る。これを受取った主制御部222は、最終判定で支払いが認められた場合には、当該最終判定をなすために使用されたワンタイムパスワードを生成したユー

ザ端末１００のユーザから、そのワンタイムパスワードの生成のきっかけとなった金額情報で特定される金額の金銭の、最終判定をなすために使用されたワンタイムパスワードを送って来た決済端末３００の管理者への支払いを認めるための処理を行う。この処理の結果は、例えば、主制御部２２２に内蔵された、図示を省略の記録媒体に記録され、その支払の処理を実現するために必要であれば、関係する金融機関等へと通知されるようになっている。また、主制御部２２２は、最終判定で支払いが認められなかった場合には、上述の処理を行わない。他方、主制御部２２２は、最終判定データに基づく内容を、データ入出力部２２１に送り、送受信部及びネットワーク４００を介して、その最終判定の基礎となる決済申込情報を送信してきた決済端末３００に送るようになっている。

[0042] 次に、決済端末３００について説明する。

決済端末３００は、クレジットカードを用いた決済システムで用いられていた決済端末と略同じものであり、一般的なコンピュータである。ハードウェア構成としては、従来の決済システムにおける決済端末と同等のもので良く、この実施形態ではユーザ端末１００と同等のものとされている。

なお、決済端末３００は、図示を省略のタッチパネル式のディスプレイを備えている。結果として、決済端末３００は、ディスプレイと、入力装置を備えることになる。もっとも、これに代えて、決済端末３００は、タッチパネル式でないディスプレイと、テンキー、キーボード、マウス、トラックボール等の公知又は周知の入力装置のうちから必要なものを選択してなる入力装置とを、ディスプレイと入力装置とを別個のものとして備えていても良いが、この実施形態の決済システムはタッチパネル式のキーボードを備えるものとして以下、話を進める。

[0043] 決済端末３００のハードウェア構成を、図１０に示す。

ハードウェアには、CPU 311、ROM 312、RAM 313、インターフェイス 314 が含まれており、これらはバス 316 によって相互に接続されている。

CPU 311は、演算を行う演算装置である。CPU 311は、例えば、ROM 312に記録されたコンピュータプログラムを実行することにより、後述する処理を実行する。このコンピュータプログラムは、決済端末300にプリインストールされていたものであっても良いし、事後的にインストールされたものであっても良い。このコンピュータプログラムの決済端末300へのインストールは、メモリカード等の所定の記録媒体を介して行われても良いし、LAN或いはインターネットなどのネットワークを介して行われても構わない。

ROM 312は、CPU 311が後述する処理を実行するために必要なコンピュータプログラムやデータを記録している。ROM 312に記録されたコンピュータプログラムは、これに限られず、他の必要なコンピュータプログラムが記録されていても良い。

RAM 313は、CPU 311が処理を行うために必要なワーク領域を提供する。

インターフェイス314は、バス316で接続されたCPU 311やRAM 313等と外部との間でデータのやり取りを行うものである。インターフェイス314は、少なくとも図示を省略の送受信部に接続されている。送受信部がネットワーク400から受取ったデータは、インターフェイス314により受取られるようになっており、インターフェイス314から送受信部にわたされたデータは、送受信部によって、ネットワーク400を介して外部、例えば、決済装置200に送られるようになっている。

インターフェイス314は、また、タッチパネル式ディスプレイに設けられた入力装置に接続されており、入力装置からの入力を受付けるようになっている。インターフェイス314は、タッチパネル式ディスプレイに接続されており、タッチパネル式のディスプレイに後述する画像を表示するためのデータを送るようになっている。

[0044] CPU 311がコンピュータプログラムを実行することにより、決済端末300内部には、図11で示されたような機能ブロックが生成される。なお

、以下の機能ブロックは、決済端末３００を本願発明の決済端末として機能させるための上述のコンピュータプログラム単体の機能により生成されていても良いが、上述のコンピュータプログラムと、決済端末３００にインストールされたＯＳその他のコンピュータプログラムとの協働により生成されても良い。

決済端末３００内には、本願発明の機能との関係で、以下のような制御部３２０が生成され、制御部３２０内に、主制御部３２１、表示制御部３２２、データ入出力部３２３が生成される。

[0045] 制御部３２０は、以下に説明するような情報処理を実行する。

主制御部３２１は、制御部３２０内の全体的な制御を行う。例えば、主制御部３２１は、追って詳述するデータ入出力部３２３から受取ったデータに基づいて表示制御部３２２の制御を行う。

主制御部３２１は、追って説明するデータ入出力部３２３から、ユーザＩＤと、ユーザ端末１００で生成されたワンタイムパスワードと、決済申込情報とを受取るようになっている。そして、それらをすべて受取ったときに、それらをデータ入出力部３２３に送るようになっている。主制御部３２１は、後述する決済端末取消情報をデータ入出力部３２３から受取る場合がある。決済端末取消情報を受取った場合、主制御部３２１は、それを適当なタイミングでデータ入出力部３２３に送るようになっている。また、主制御部３２１は、各決済端末３００を区別するための、各決済端末３００にユニークな決済端末ＩＤを保持している。決済端末ＩＤは、主制御部３２１によって、決済申込情報に含められるようになっている。

表示制御部３２２は、主制御部３２１の制御を受けつつ、タッチパネル式とされたディスプレイに表示される画像の制御を行う。ディスプレイには、表示制御部３２２から送られたデータに基づく画像が表示される。主制御部３２１は、表示制御部３２２に対して、ディスプレイにどのような画像を表示させるべきかという指示を送る。

[0046] データ入出力部３２３は、制御部３２０へのデータの入出力を行うもので

ある。具体的には、データ入出力部 323 は、入力装置からの入力を受取るようになっている。入力装置からデータ入出力部 323 へ入力されるデータの例は、上述の通りであり、ユーザ ID、ワンタイムパスワード、決済申込情報である。それらは主制御部 321 に送られるようになっている。また、入力装置からは、決済端末取消情報が入力される場合がある。

また、データ入出力部 323 は、図示を省略の送受信部に対して、データを出力するようになっている。送受信部に対して出力されるデータは例えば、ユーザ ID、ワンタイムパスワード、決済申込情報、決済端末取消情報であり、それらは送受信部から、ネットワーク 400 を介して、決済装置 200 に送られるようになっている。なお、ユーザ ID と、ワンタイムパスワードは既に説明した通りのものである。決済申込情報は、決済の最終判定を決済装置 200 に依頼する情報である。また、決済端末取消情報は、既に終了した過去の決済の一つを取消するための決済端末 300 の管理者の意思表示を示す情報であり、入力装置を用いて決済端末 300 の管理者が入力するものである。決済端末取消情報には、管理者が取消を望む過去の決済の一つを特定する情報が少なくとも含まれている。

[0047] 次に以上のような決済システムの使用方法、及び動作について図 15 を参照しながら説明する。

かかるシステムを用いて決済を行う際には、まず、ユーザが自らの、ユーザ端末 100 を操作して、決済の処理を開始する (S911)。そのためにユーザは、決済の処理を開始することを示す情報を入力する。例えば、ユーザ端末 100 のディスプレイ 101 に表示されている、図示を省略のアイコンにタッチすることにより、かかる情報の入力を行える。

その情報は、データ入出力部 123 から、主制御部 121 に送られる。主制御部 121 は、その情報を受付けると、表示制御部 122 に対して、ユーザ ID 等の入力をユーザに促すような画像をディスプレイ 101 に表示せよとの指示を送る。この指示を受付けた表示制御部 122 は、ディスプレイ 101 に、例えば、図 12 (A) の如き、ユーザにユーザ ID と、パスワード

と、ユーザが支払いを行おうとする金額の入力を促す画像を表示する。ユーザは、ユーザIDと示された部分の右側にユーザIDを、パスワードと示された部分の右側にパスワードを、金額（円）と示された部分の右側に自分が支払おうとする金額をそれぞれ入力する（S912）。ユーザが入力したユーザIDとパスワードについてのデータは、入力装置102からデータ入出力部123に入力され、主制御部121に送られる。金額を特定する情報は金額情報であるが、この金額情報も同様に主制御部121に送られる。ユーザが入力したユーザIDとパスワードと金額は、入力中も含めて、主制御部121に制御された表示制御部122の制御によってディスプレイ101に表示されるから、ユーザは、ディスプレイ101を確認しながら、ユーザIDとパスワードと金額との入力を行うことができる。図12（B）に示した例によれば、ユーザは、この決済システムを用いて、25000円の支払いを行おうとしている。

なお、ユーザ端末100における金額情報の入力は、支払いを行おうとする金額を直に入力するには限られない。例えば、ユーザが支払いを行おうとする店舗で販売されている商品を特定するための表示（例えば商品名、商品の写真又はイラスト、或いは商品を特定するためのアイコンの如き識別子）がユーザ端末100のディスプレイ101に複数表示されるとする。ユーザが、それらの表示から自分が購入したいものを選択することにより、その選択された商品の合計金額が、ユーザが支払おうとしている金額である金額情報になるように、例えば主制御部121が自動的に演算を行うような構成も採用可能である。例えば、ユーザが支払いを行おうとしている店舗がコーヒーチェーンの店舗である場合には、コーヒーと、サンドイッチと、ヨーグルトの3つの商品を選択した場合には、それらの合計額を特定する情報が自動的に金額情報となるようになっている、というのがその例である。

ユーザIDとパスワードと金額情報の入力が終わったら、ユーザは、ディスプレイ101に表示された「決定」と書かれたボタンをクリックする。

[0048] 「決定」と書かれたボタンをユーザがクリックすると、GPS機構が、ユ

ユーザ端末100が存在する位置を特定する情報であるユーザ端末の位置情報を生成する。位置情報は、データ入出力部123から主制御部121に送られる。主制御部121は、ユーザIDとパスワードと金額情報とに加えて、位置情報と、主制御部121の図示を省略された記録手段に記録された端末情報とをすべて一纏めにして、それらをデータ入出力部123に送る。データ入出力部123は、それらデータをまとめて送受信部に送り、送受信部は、それらデータをまとめてネットワーク400を介して決済装置200に送る(S913)。「決定」と書かれたボタンをユーザがクリックしてから、上記5つのデータの決済装置200への送信は略実時間で、少なくとも例えば数秒のうちに実行される。

[0049] 決済装置200は、その送受信部でそれらデータを受付ける(S921)。送受信部はそれらデータをすべてデータ入出力部221に送り、データ入出力部221はそれらデータをすべて主制御部222に送る。主制御部222は、ユーザIDと、パスワードと、端末情報と、金額情報とを与信判定部223に、ユーザ端末100の位置情報を最終判定部225にそれぞれ送る。

与信判定部223は、与信判定を実行する(S922)。与信判定は具体的には、以下のように実行される。

与信判定部223は、主制御部222からユーザID、パスワード、及び端末情報を受取ると、受取ったユーザIDと同じユーザIDと対応付けられた、パスワード、端末情報、及び預金残高を、与信情報記録部224から読み出す。与信判定部223が受取ったユーザIDと同じユーザIDが与信情報記録部224に存在しない場合には、パスワード等の情報を与信判定部223は、与信情報記録部224から読み出さない。この場合には、与信判定部223は、与信判定の処理を中止する。

この実施形態では、図12(B)に示したように、ユーザがユーザ端末100に入力したユーザIDは、「d2af1apfa」であり、それと同じユーザIDが、与信情報記録部224の上から2番目に存在しているから、与信判定部

２２３は、与信情報記録部２２４から、そのユーザＩＤと紐付けられたパスワード（aofau554）と、端末情報（012457854）と、預金残高（２９５６００２円）を読み出す。

与信判定部２２３が主制御部２２２から受取ったユーザＩＤと同じユーザＩＤが与信情報記録部２２４に記録されており、主制御部２２２から受取ったユーザＩＤと同じユーザＩＤと対応付けられた、パスワード、端末情報、及び預金残高が与信情報記録部２２４から読み出された場合には、与信判定部２２３は、主制御部２２２から受取ったパスワード及び端末情報が、与信情報記録部２２４から読み出されたパスワード及び端末情報と同じか否か判定する。それらが共に一致したのであれば、与信判定部２２３は、そのユーザＩＤ等を送って来たユーザが正当なユーザであると認証する。他方、パスワード及び端末情報の少なくとも一方が一致しなかったのであれば、そのユーザＩＤ等を送って来たユーザが正当なユーザでないと判定して、与信判定の処理を中止する。

次いで、認証されたユーザの与信の判定が実行される。与信判定部２２３は、そのユーザが送ってきた金額情報と、そのユーザのユーザＩＤと紐付けられていた、上記与信情報記録部２２４から読み出された預金残高とを比較する。この実施形態では、預金残高の方が、金額情報で特定される金額と同じかそれよりも大きい場合に、ユーザの求める決済が、仮にはあるが、認められる。他方、預金残高が、金額情報で特定される金額よりも小さい場合には、ユーザの求める決済は認められない。この例では、預金残高（２９５６００２円）の方が、金額情報で特定される金額（２５０００円）よりも大きいため、ユーザの求める決済が認められる。かかる決済が認められるのであれば、与信判定部２２３は、仮許可情報を生成する（Ｓ９２３）。与信判定部２２３が仮許可情報を生成した場合には、その仮許可情報は主制御部２２２に送られるようになっている。

なお、与信判定部２２３が仮許可情報を生成した場合には、与信判定部２２３は与信判定を行った時刻を特定するための時刻情報を主制御部２２２に

通知する。かかる時刻情報は、その仮許可情報で決済が一応認められたユーザが誰であるかを特定するために、ユーザIDとともに、主制御部222から最終判定部225に送られる。

主制御部222は仮許可情報を、データ入出力部221に送る。データ入出力部221は、仮許可情報を、送受信部、及びネットワーク400を介してユーザ端末100に送信する（S924）。

[0050] ユーザ端末100の送受信部は、決済装置200から送られてきた仮許可情報を受取る（S914）。受取られた仮許可情報は、データ入出力部123から、主制御部121に送られる。仮許可情報を受取った主制御部121は、仮許可情報を受取った旨を、OTP生成部124に通知する。

この通知を受けたOTP生成部124は、ワンタイムパスワードを生成する（S915）。OTP生成部124は、ワンタイムパスワードを生成するための初期値を有しており、且つ過去に何回ワンタイムパスワードを生成したかということを示す生成回数を記録している。また、OTP生成部124は、ワンタイムパスワードを生成するための数式（これはつまり、アルゴリズムである。）を使用できるようになっている。OTP生成部124は、初期値を上述の数式に代入して得た値を再び数式に代入して次の値を得る、という処理を繰り返すことにより次々と値を生成する。生成回数で示された数字よりも1多い順番に作られた値を、OTP生成部124は、そのとき使用するワンタイムパスワードとするようになっている。

生成されたワンタイムパスワードは、主制御部121に送られる。主制御部121は、表示制御部122に対してワンタイムパスワードをディスプレイ101に表示せよとの指示を送る。表示制御部122には、例えば、図13（A）に示されたような画像が表示される。

このワンタイムパスワードは従来のクレジットカードを用いた決済システムにおけるクレジットカードナンバーの如くに利用されるものではあるが、後述するようにそれが有効である（決済に用いることができる）時間に制限がある。ユーザの注意を促す側面から、図13（A）に示したように、『こ

のワンタイムパスワードは今から5分間有効です』といった表示を、ワンタイムパスワードと一緒にかどうかはさておき、適当なタイミングでディスプレイ101に行うようにするのが好ましい。

[0051] なお、上述したように、決済装置200の与信判定部223は、与信判定を中止した場合やそのユーザについての預金残高が不足していた場合等、仮許可情報を生成しない場合もある。この場合には、当然にユーザ端末100には仮許可情報が送信されない。もっともこの場合においても、決済装置200からユーザ端末100に対して何らかのデータを送信し、決済装置200で仮許可情報が生成されなかったこと（ユーザの視点では、決済の手続きが継続できないこと。）、及び必要であればその理由をユーザ端末100のディスプレイ101に表示するようにしても良い。

その場合には、例えば、図13（B）に示したような画像がユーザ端末100のディスプレイ101に表示される。この画像も、主制御部121の指示に従い、表示制御部122がディスプレイ101に表示する。この図の場合であれば、左側の四角いチェックボックスの中にチェックが入っていることから明らかなように、パスワードが正しくないということが決済の手続きが継続できない理由であるということが、ユーザに示されている。

[0052] ユーザ端末100のディスプレイ101にワンタイムパスワードが表示されると、ユーザが、それを決済端末300に入力することにより決済端末300に渡す（S931）。予めワンタイムパスワードを生成しておけば、ワンタイムパスワードを決済端末300に渡すにあたって手間取ることもないであろう。

上述したように、決済端末300は、図示を省略のタッチパネル式のディスプレイを備えている。タッチパネル式のディスプレイには、例えば図14（A）に示したような、ユーザ等にユーザIDとワンタイムパスワードとの入力を促す表示を行う。かかる表示は、決済端末300の主制御部321の制御下で、表示制御部322が行う。ユーザは、ユーザIDと表示された部分の右側にユーザIDを、OTPと表示された部分の右側にワンタイムパス

ワードを、タッチパネル式のディスプレイを手で操作することにより入力する。

ユーザは、決済端末300のディスプレイを操作して、ユーザIDとワンタイムパスワードとを入力する(図14(B))。ユーザが入力したユーザIDとワンタイムパスワードとは、入力中も含めて、主制御部321に制御された表示制御部322の制御によってディスプレイに表示されるから、ユーザは、ディスプレイを確認しながら、ユーザIDとワンタイムパスワードとの入力を行うことができる。

なお、この実施形態では、ユーザの手入力によって、ユーザ端末100で生成されたワンタイムパスワードを決済端末300に渡すこととしているが、これには限られず、例えば決済端末300が備えた、あるいは決済端末300に接続されたカメラによりユーザ端末100のディスプレイ101を撮像した後、そのディスプレイ101を含む画像に対して決済端末300で所定の画像処理を行うことにより、ディスプレイ101に表示されているワンタイムパスワードを決済端末300が特定するようにすることもできる。或いは、ユーザ端末100のディスプレイ101に、一次元或いは二次元バーコードとして表示されたワンタイムパスワードを、決済端末300が備えるバーコードリーダで読み取ることにより、ユーザ端末100で生成されたワンタイムパスワードを決済端末300に渡すことも可能である。また、Bluetooth、赤外線通信などの無線通信によって、ユーザ端末100から決済端末300にワンタイムパスワードをデータとして渡すことも可能である。なお、ユーザ端末100から決済端末300に無線通信によってワンタイムパスワードを渡す場合には必ずしも、ユーザ端末100のディスプレイ101にワンタイムパスワードを表示する必要はない。

なお、ユーザ端末100から決済端末300にワンタイムパスワードを引渡す方法は、これには限られない。ユーザは、ユーザ端末100で発生させたワンタイムパスワード、或いはワンタイムパスワードを特定する情報を、例えば自らが所有する公知或いは周知のプリンタで紙に印刷することができ

る。この場合にはユーザは、ワンタイムパスワードを、支払いを行おうとしている場所（店舗内、或いはその付近）で発生させる必要はなく、自宅或いはプリンタが存在する場所でそれを行えば良い。ワンタイムパスワードが印刷された紙は、金券として貨幣（或いは紙幣）と同様に、その引渡しによる支払いのためのツールとして使用することが可能になる。ユーザはその金券を、決済端末300の管理者に引渡すことにより、決済を行うことが可能となる。かかる金券の一例を、図20と、図21とに示す。

図20は、ワンタイムパスワードを印刷した金券の一例であり、図20（A）は、ある金券の表面、同（B）は、その金券の裏面を示す。金券には、ワンタイムパスワードが印刷されている。この実施形態では、一例としてワンタイムパスワードとして、ユーザ端末100で、01563894451という数字が発生させられたものとしているが、金券の表面にはワンタイムパスワードの一部（OTP1）として、その前半が、金券の裏面にはワンタイムパスワードの残部（OTP2）として、その後半が、印刷されている。ワンタイムパスワードは、その全部が金券の表面又は裏面のいずれかに印刷されても良いが、このようにワンタイムパスワードが金券の両面に渡って印刷されることにより、悪意の第三者がワンタイムパスワードの全体を盗み見たり、盗撮したりすることが難しくなる。また、図20の金券には、この金券を用いて支払いを行うことが想定された者（ワンタイムパスワードを発生させたユーザとは限らない。）の顔Fが印刷されている。このような金券であれば、決済端末300の管理者に金券を渡した者の顔と、金券に印刷された顔とが一致した場合にのみ決済端末300の管理者が決済に関する以後の処理を行うというルールを作ることが可能となり、そのようなルールを実行することにより、金券を不正に取得した者による金券Fの不正使用（不正な支払い）が行われるリスクを低減できる。なお、この例ではユーザ等の顔Fは金券の表裏両面に印刷されているが、顔Fは金券のいずれか一方の面に印刷されていれば足りる。このような金券を受取った決済端末300の管理者は、金券の表裏に記載のワンタイムパスワードの一部と残部を、テンキーそ

他の入力装置を用いて、或いはカメラで撮像することにより、決済端末300に入力可能である。顔Fをユーザ以外の者とした場合には、ユーザからその金券を正当に譲渡された者が、その金券を用いて決済を行うことが可能となる。

図21の金券は、ワンタイムパスワードではなく、ワンタイムパスワードを特定するための情報を紙に印刷したものである。ワンタイムパスワードを特定するための情報の例として、この実施形態では、二次元バーコードを採用している。図21に示した金券の場合でも、金券の表面にワンタイムパスワードの一部が、金券の裏面にワンタイムパスワードの残部が印刷されている。図21(A)で示された面に印刷された二次元バーコードは、図20(A)に記載のOTP1に、また、図21(B)で示された面に印刷された二次元バーコードは、図20(B)に記載のOTP2に対応しており、それら二次元バーコードを所定の二次元バーコードリーダで読取ると、OTP1、OTP2にそれぞれ対応した値が読み出されるようになっている。また、図20に示した金券の場合でもそうであったが、図21に示した金券でも、その表裏両面にその金券を使用することが予定された者の顔Fが印刷されている。このような金券を受取った決済端末300の管理者は、その金券の表裏に印刷された二次元バーコードを、例えばバーコードリーダを用いて読取らせることにより、ワンタイムパスワードを決済端末300に入力することが可能となる。

いずれにせよ、ユーザIDとパスワードと金額情報の入力が終わったら、ユーザ或いは決済端末300の管理者は、ディスプレイに表示された「決定」と書かれたボタンをクリックする。

[0053] ユーザが、「決定」と書かれたボタンをクリックすると、その入力内容はデータ入出力部323から主制御部321に送られる。主制御部321は、その入力内容を受取ると、決済申込情報を生成する。決済申込情報は、決済端末300の管理者が決済の最終判定を決済装置200に依頼する情報である。決済申込情報には、また、その決済端末300を特定するための、決済

端末 1 D が含まれる。主制御部 3 2 1 は、決済申込情報とユーザ 1 D とワンタイムパスワードとを一纏めにしてデータ入出力部 3 2 3 を介して決済端末 3 0 0 の送受信部に送り、送受信部からネットワーク 4 0 0 を介して決済装置 2 0 0 に送る（S 9 3 2）。

[0054] 決済装置 2 0 0 は、その送受信部で、決済端末 3 0 0 から送られてきたそれら 3 つのデータを受取る（S 9 2 5）。決済端末 3 0 0 から送られてきた決済申込情報とユーザ 1 D とワンタイムパスワードは、データ入出力部 2 2 1 を介して主制御部 2 2 2 に送られる。

主制御部 2 2 2 は、決済端末 3 0 0 から送られてきた決済申込情報とユーザ 1 D とワンタイムパスワードのデータを、最終判定部 2 2 5 に送る。これらデータを受取った最終判定部 2 2 5 は、決済申込情報に含まれていた決済端末 1 D と紐付けられている位置情報を、位置情報記録部 2 2 6 から読み出す。

[0055] 他方、主制御部 2 2 2 は、決済申込情報等を受取ると、ワンタイムパスワードを生成せよとの指示を、OTP 生成部 2 2 7 に送る。

ワンタイムパスワードを生成せよとの指示には、主制御部 2 2 2 が受取ったユーザ 1 D が付されている。OTP 生成部 2 2 7 は、そのユーザ 1 D に対応するユーザ 1 D と紐付けられている初期値と、生成回数とを、OTP 情報記録部 2 2 8 から読み出す。

OTP 情報記録部 2 2 8 に記録されていた、それら初期値と生成回数についての情報を用いて OTP 生成部 2 2 7 によって行われるワンタイムパスワードの生成の処理は、ワンタイムパスワードを生成せよとの指示を出すきっかけとなった決済申込情報と共に送られてきたユーザ 1 D によって特定されるユーザ端末 1 0 0 の OTP 生成部 1 2 4 で実行された処理とまったく同じものとなる。したがって、ユーザ端末 1 0 0 で行われたワンタイムパスワードの生成や、決済端末 3 0 0 から決済装置 2 0 0 へのワンタイムパスワードの送信等のどこかに、第三者による不正がない限り、ユーザ端末 1 0 0 でなされるワンタイムパスワードの生成の処理と、決済装置 2 0 0 で行われるワ

ンタイムパスワードの生成の処理とは、完全に同期したものとなる。

ワンタイムパスワードを生成したら、OTP生成部227は、それを、主制御部222を介して最終判定部225に送る。

[0056] 最終判定部225が、位置情報記録部226から位置情報を読み出し、また、OTP生成部227からOTP生成部227が生成したワンタイムパスワードを受取る前に、既に、最終判定部225には、主制御部222からユーザ端末100で生成され決済端末300から送られてきたワンタイムパスワードと、これもユーザ端末100で生成され、ユーザ端末100から送られてきた位置情報と、与信判定部223で生成され主制御部222を介して送られてきた時刻情報とが存在している。

最終判定部225は、これらの情報を用いて、最終判定を行う（S926）。

[0057] 最終判定は、以下のように行われる。

この実施形態における最終判定では、最終判定部225は、ユーザ端末100が生成し、決済端末300から送られてきたワンタイムパスワードと、OTP生成部227が生成したワンタイムパスワードとを比較してこれらが一致するか否かを判定する。両ワンタイムパスワードが一致することが、最終判定で決済が可能と判定されるための条件の一つとなる。これを条件とするのが有効なのは、両ワンタイムパスワードが一致するのであれば、ユーザ端末100を使用してワンタイムパスワードを生成した者や、ワンタイムパスワードを送って来た決済端末300の管理者に悪意の第三者によるなりすましが無く、また、ワンタイムパスワードを決済端末300から決済装置200に送信する間にも、悪意の第三者の攻撃が無い等、決済の全過程に不正がないと想定することが可能であるからである。

また、この実施形態における最終判定では、最終判定部225は、ユーザ端末100が生成し、ユーザ端末100から送られてきた位置情報と、位置情報記録部226から読み出された位置情報とを比較して、両位置情報により特定される位置が、所定の距離よりも近いかな否かを判定する。両位置情報

により特定される位置が所定の距離、例えば20mよりも近いことが、必ずしもこの限りではないがこの実施形態では、最終判定で決済が可能と判定されるための条件の一つとなる。これを条件とするのが有効なのは、以下の理由による。ユーザ端末100から送られて来た位置情報は、端的に言えば、ユーザ端末100がどこにあるかということを示すものである。位置情報記録部226から読み出された位置情報は、端的に言えば、決済端末300がどこにあるかを示すものである。そして、両位置情報により特定される位置が近いということは、ユーザ端末100を操作するユーザと、決済端末300の管理者が近くにいるということを示している。ユーザと、ユーザから支払いを受ける決済端末300の管理者は、多くの場合、支払いが行われるとき近くにいる。例えば、レストランその他の飲食店や、実店舗の商店等での支払いの場合、そのような状況は普通に生じるというよりも、そうでないことがまず無い。ユーザと決済端末300との距離が近いという状況が生じているか否かを、上述の如き2つの位置情報の比較により確認することにより、第三者が、ユーザ又は決済端末300の管理者になりすますことを防止できる可能性が高まる。しかも、決済端末300の位置はある程度固定されているが、ユーザは移動するため、ユーザがどこにいるかを知らない第三者はユーザになりすますことは難しい。したがって、2つの位置情報を対比した結果を、決済を認める条件とすることには大きな意味がある。なお、両位置情報により特定される位置が「近い」と判断されるか、されないかの基準となる距離（例えば、上述の場合であれば20m）が小さければ小さい程、この決済システムを用いての決済の安全性は高まるが、この基準となる距離は、ユーザ端末100に含まれるGPS機構の性能（位置情報により特定されるユーザ端末100の位置の精度）等に応じて適切に決定すれば良い。

他方、決済端末300が、実店舗に存在しない場合がある。例えば、インターネット上に存在する仮想店舗での支払いの場合には、広く知られているようにオンライン決済が行われる。その場合には、ユーザと決済端末300の距離は、決済を認めるための条件としたところで大した意味を持たない。

必ずしもこの限りではないが、この実施形態では、決済端末300が実店舗に存在しない場合には、図8の決済端末104の場合のように、その決済端末300についての位置情報は位置情報記録部226に記録されていない。この場合には、決済装置200は、最終判定を行うにあたり、上述の如き2つの位置情報の比較を行わない（或いは、省略する）ようにすることができる。この決済システムの全体で、位置情報を用いないようにすることも可能である。

この実施形態における最終判定では、最終判定部225は、与信判定部223が生成した時刻情報により特定される時刻と、最終判定が行われた時刻とを対比し、その時間間隔が所定の時間間隔以内であるか否かを判定する。その時間間隔が所定の時間間隔（この実施形態では、図13（A）を用いて説明したように、その時間間隔は5分である。）以内であることが、必ずしもこの限りではないがこの実施形態では、最終判定で決済が可能と判定されるための条件の一つとなる。これを条件とするのが有効なのは、その時間間隔を短くすることによって、ユーザ端末100で生成されたワンタイムパスワードが第三者に盗まれて不正に使用されることが可能な時間を短くすることができ、それにより決済の安全性をより高めることができるからである。なお、この実施形態では、与信判定部223で与信判定が行われた時刻を、上述の時間間隔を計測するための始点として用い、最終判定部225で最終判定が行われる時刻を、上述の時間間隔を計測するための終点として用いることとしている。しかしながら、上述の時間間隔を計測するための特に始点は、上述のタイミングには限られない。上述の時間間隔を計測するための始点は、ユーザが、ユーザ端末100の入力装置102を操作することによって、この決済のための処理に必要な最初の入力を行って以降、最終判定部225が最終判定を行う前の適当なタイミングとすることができる。つまり、S911が開始された後、最終判定部225で最終判定が行われる前の任意のタイミング、特に、決済装置200からユーザ端末100に仮許可情報が届くその瞬間までの任意の時点を、上述の時間間隔を計測するための始点

とすることができる。例えば、ユーザ端末１００で金額情報が入力されたタイミング、ユーザ端末１００でディスプレイ１０１に表示された「決定」という文字が表示されたボタンがクリックされたタイミング、ユーザ端末１００から送信された金額情報等が決済装置２００に受取られたタイミング、与信判定部２２３で与信判定が開始されたタイミング、決済装置２００からユーザ端末１００への仮許可情報の送信が開始されたタイミング等が、採用可能な始点の例となる。なお、この決済システムで、ユーザ端末１００で生成されたワンタイムパスワードに有効期限を設けないことも可能である。

この実施形態では、決済装置２００の最終判定部２２５は、上述の３つの条件がすべて充足されたと判定したときにのみ、ユーザ端末１００を持つユーザからの決済端末３００の管理者への支払いを認める決定を最終的に行う。最終判定部２２５は、３つの条件のいずれかが充足されない場合には、上記支払を認めないとの決定を最終的に行う。これら両決定を、最終判定と称する。

最終判定部２２５は、最終判定を行った場合、最終判定の結果を示すデータである最終判定データを生成（Ｓ９２７）し、それを例えばユーザＩＤとともに主制御部２２２に送る。これを受取った主制御部２２２は、最終判定で支払いが認められた場合には、当該最終判定をなすために使用されたワンタイムパスワードを生成したユーザ端末１００を持つユーザから、そのワンタイムパスワードの生成のきっかけとなった金額情報で特定される金額の金銭の、最終判定をなすために使用されたワンタイムパスワードを送って来た決済端末３００の管理者への支払いを認めるための処理を行う。この処理の結果は、例えば、主制御部２２２に内蔵された、或いは決済装置２００の内部、或いは外部にある図示を省略の記録媒体に記録され、その支払の処理を実現するために必要であれば、関係する金融機関等へと通知される。記録媒体に記録される内容は、少なくとも支払いを行ったユーザを特定するための情報、支払いを受ける者を特定するための情報、及び支払いに使用されたワンタイムパスワードである。ワンタイムパスワードを記録するのは、同じワ

ンタイムパスワードで2回の支払いを認めないようにするためである。また、最終判定データを受取った主制御部222は、支払いの処理の一環として、ユーザから、決済端末300の管理者への支払いが認められた金銭に相当する金額を、減じる。減じられた額に相当する金銭は、即時に支払いを受ける決済端末300の管理者に送金されても良いし、決済装置200或いはその管理者が一旦預かってよい。与情報記録部224の上から2番目に記載されたユーザが、25000円の支払いをしたのであれば、主制御部222は、その預金残高2956002円から25000円を減じて、その預金残高を2931002円に書換える。

また、主制御部222は、最終判定で支払いが認められなかった場合には、上述の処理を行わない。

他方、主制御部222は、最終判定データの内容を、データ入出力部221に送り、送受信部及びネットワーク400を介して、その最終判定の基礎となる決済申込情報を送信してきた決済端末300に送るようになっている(S928)。

[0058] 最終判定データを、決済装置200から決済端末300は受取る(S933)。決済端末300は、このデータをその送受信部で受取る。送受信部が受取ったそのデータは、送受信部からデータ入出力部323に送られ、データ入出力部323から主制御部321に送られる。

主制御部321は、最終判定データに基づく内容をそのディスプレイに表示させるべく表示制御部322を制御する。表示制御部322の制御により決済端末300のディスプレイには、適当な表示がなされる(S934)。その表示は、最終判定データの内容が支払いを認めるものであればその旨を示すものとなり、最終判定データの内容が支払いを認めないものであればその旨を示すものとなる。

なお、決済装置200は、最終判定データの内容を、決済端末300のみならずユーザ端末100にも送信するようになっていても良い。この場合には、ユーザ端末100のディスプレイ101に、決済端末300のディスプ

レイに表示されたのと同様の、最終判定データに基づく内容が表示される。

[0059] 以上が、この実施形態の決済システムで行われる決済の流れである。

ただし、以上のように行われた決済が、取消される場合がある。それは次のような流れで実行される。

ユーザと決済端末300の管理者が、何らかの事情により過去に行った決済を取消したいと考えたとする。そのときユーザは、ユーザ端末100の入力装置102を操作して、決済の取消しの画面をディスプレイ101上に呼出す。そのときのディスプレイ101上の表示の一例を、図16に示す。なお、この例では、ユーザIDがd2af1apfaであるユーザが行った25000円の上記決済を取消すものとする。

図16に示したように、ディスプレイ101には、取消が可能な過去の決済の一覧が表示される。過去の決済のうち取消を行えるものは、この実施形態では、決済装置200で決済が終了してから例えば10分以内のものに制限されているから、ここで表示される過去の決済は多くはないであろう。図16(A)では、2015年9月15日の19時21分になされた25000円の支払いと、同19時18分に行われた2600円の支払いの2つが、取消を行える対象としてディスプレイ101に表示されている。ユーザは、入力装置102を使用して、それらのうちから一つを選択する。図16(B)では、取消の対象となっている2つの支払いのうちの前者が選択された状態を示している。ユーザが、決定と記載されているボタンをクリックすると、取消の対象として2015年9月15日の19時21分になされた25000円の支払いを特定した情報を含む、ユーザ端末取消情報が生成される。ユーザ端末取消情報は、入力装置102からの入力をデータ入出力部123を介して受付けた主制御部121が生成する。ユーザ端末取消情報は、主制御部121からデータ入出力部123を介して送受信部へ送られ、送受信部からネットワーク400を介して決済装置200に送られる。

他方、決済端末300の管理者も、同様の処理を行い、決済端末取消情報を生成する。決済端末300の管理者は、決済端末300の入力装置を操作

して決済端末300のディスプレイ上に、図16に示したのと同様の画面を表示させる。ディスプレイには、取消が可能な過去の決済の一覧が表示される。過去の決済のうち取消を行えるものは、この実施形態では、決済装置200で決済が終了してから例えば10分以内のものに制限されているけれども、一般に一つの決済端末300を用いて行われる決済は、一つのユーザ端末100を用いて行われる決済よりも数が多いから、決済端末300のディスプレイには、図16に示したものよりもより多くの決済が表示されることになるであろう。決済端末300の管理者は、決済端末300の入力装置を操作して、そのうちの一つを選択する。決済端末300の管理者が選択を誤らないようにするには、図16で示した例では、過去の決済を特定するための情報として、決済の日時と金額のみが表示されていたが、それに加えて決済を行ったユーザを特定するための情報、例えばユーザIDをもディスプレイ上に表示されるようになっているのが便利であろう。決済端末300の管理者が入力装置を操作することにより、ユーザIDがd2af1apfaであるユーザが2015年9月15日の19時21分に行った25000円の支払いを特定した情報を含む、決済端末取消情報が生成される。決済端末取消情報は、入力装置からの入力をデータ入出力部323を介して受付けた主制御部321が生成する。決済端末取消情報は、主制御部321からデータ入出力部323を介して送受信部へ送られ、送受信部からネットワーク400を介して決済装置200に送られる。

決済装置200は、その送受信部で、ユーザ端末取消情報と決済端末取消情報とを受取る。これらは、データ入出力部221を介して、主制御部222へと送られる。主制御部222は、それら2つの情報を受取った場合、それらユーザ端末取消情報と、決済端末取消情報とによって特定される過去の決済が同一であるか否かを判定する。その結果、両者が同一である場合には、主制御部222は当該過去の決済を取消するための処理を行う。ユーザ端末取消情報と決済端末取消情報との一方しか受取らなかった場合、或いはこれら2つの情報を受取ったけれどもユーザ端末取消情報と、決済端末取消情報

とによって特定される過去の決済が同一でない場合には、過去の決済を取消す処理を主制御部２２２は行わない。主制御部２２２は、決済の取消の結果を、例えば、主制御部２２２に内蔵された、図示を省略の記録媒体に記録し、また、その取消の処理を実現するために必要であれば、関係する金融機関等へと通知する。また、主制御部２２２は、与情報記録部２２４においてした上述した預金残高の書換を取消し、その預金残高を支払い前の残高に戻す。

[0060] 上述した取消の処理は、例えば、以下のように用いればより実用的になる。

従来のクレジットカードにおけるクレジットカードナンバーの如くに用いられる本願発明におけるワンタイムパスワードは、基本的に一度しか使われないいわば使い捨てのものであるから、その盗用の可能性は極めて低くほとんど想定することができない。しかしながら、ユーザ端末１００で生成されたワンタイムパスワードを、ユーザが、決済端末３００を介して決済装置２００に送るまでの間に第三者に盗まれ、第三者に使用されてしまう可能性がないわけではない。

上述の実施形態では、決済端末３００から決済装置２００にユーザＩＤか、或いはユーザを特定するための他の情報である署名、指紋や静脈の性状等の情報を送信することとしていた。これらのうち、決済端末３００から送られるワンタイムパスワードを用いて支払いを行おうとするユーザを特定する材料として、指紋や静脈の性状等のバイオ情報を用いるのであれば、ワンタイムパスワードを盗んだ第三者が正規のユーザになりすますのは極めて難しいであろう。しかしながら、ユーザを特定するために決済端末３００から決済装置２００にワンタイムパスワードとともに送られる材料がユーザＩＤのみである場合には、ユーザＩＤは通常変化させない固定のものであるから、ワンタイムパスワードのみならずユーザＩＤまで盗まれた場合には、第三者によるなりすましを防止することができないという事態も生じうる。また、追って本願発明の変形例で述べるように、決済端末３００から決済装置２０

０にワンタイムパスワードを送る場合に、ユーザＩＤ等の、そのワンタイムパスワードを自らのユーザ端末１００で生成したユーザを特定するための如何なる情報をも添付しないことも可能である。そのような場合においては、ユーザが本人であるという確認と、そのユーザの支払い能力についての与信の判定をパスして仮許可情報が生成された上で発生させられたワンタイムパスワードは、それを用いれば、そのワンタイムパスワードを自らのユーザ端末１００を用いて発生させたユーザのみならず、誰でもが、そのワンタイムパスワードを相手に引き渡すことで支払いを行える、現金、小切手等の如き性格を持つことになる。決済システムが、そのようなワンタイムパスワードを扱うものである場合には、ワンタイムパスワードを盗み出した第三者は、そのワンタイムパスワードをそのワンタイムパスワードを自らのユーザ端末１００で発生させたユーザになり変わって使用することができる。

そのような第三者によるワンタイムパスワードの不正使用を上述した取消の処理により防止することができる。

[0061] 上述したように、この実施形態の決済システムでは、最終判定データが、決済装置２００から決済端末３００に送られるようになっており、最終判定データが示す内容が、決済端末３００が備えるディスプレイに表示されるようになっている。

ここで、第三者にワンタイムパスワードが不正に使用されてしまったと仮定する。例えば、ユーザが、自分が支払いを行うために、自らのユーザ端末１００で発生させたワンタイムパスワードを渡そうと思っていた相手以外の者が管理する決済端末３００から、盗まれたワンタイムパスワードが、決済装置２００に対して送信されてしまったとする。この場合、そのワンタイムパスワードによる支払いは、決済端末装置２００の最終判定部２２５により承認されてしまう場合がある。もっとも、上述したように、最終判定部２２５が、決済端末３００から送られてきたワンタイムパスワードによる支払いに対して肯定的な判定を行うためには、ワンタイムパスワードの一致と、ユーザ端末１００と決済端末３００との距離が近いことと、そしてワンタイム

パスワードの有効期限が切れていないこと、の3つの要件がすべて充足されることがこの実施形態では必要である。したがって、ユーザが盗まれて決済装置200に送られたワンタイムパスワードが決済装置200のOTP生成部227で作られたワンタイムパスワードと一致したとしても、他の2つの要件が充足されなければ、最終判定部225が決済を認めることはない。しかしながら、その2つの条件が充足される場合もあるし、またそもそもこれら2つの条件は、この実施形態における決済システムにおいて必ずしも必須のものではないため、これら2つの条件がそもそも最終判定部225において考慮されない場合もあり得る。そのような場合には、上述のワンタイムパスワードの一致の条件が満足されたのであれば、決済装置200の最終判定部225は、そのワンタイムパスワードによる支払いを承認する。

この場合、最終判定データが、決済装置200から決済端末300に送られることになる。かかる最終判定データは、決済が認められたということを示すものとされている。ただし、ここで問題なのは、支払いが受けられることになった決済端末300の管理者は、ユーザが本来支払いを行おうと意図していた相手とは別である、ということである。この段階では、ユーザが本来支払いを行おうとしていた相手が管理者となっている決済端末300には、最終判定データが届いていない。他方、上述したように、最終判定データは、ユーザ端末100にも送られる場合がある。しかしながら、仮にこの段階でユーザ端末100に最終判定データが送られて来たとしても、それはそのユーザから、ユーザが本来支払いを行うつもりがなかった相手への支払いを決済装置200が認めた、という内容になる。ユーザ端末100のディスプレイに表示される情報の程度にもよるが、ユーザはその内容からは、自己のユーザ端末100にて発生させたワンタイムパスワードが第三者に不正に使用されたことに気づかない可能性がある。

他方、ユーザが自己のユーザ端末100にて発生させたワンタイムパスワードを第三者に既に使用されてしまった後に、つまりそのワンタイムパスワードによって誰かへの支払いが成立してしまった後に、ユーザがそのワンタ

タイムパスワードを、ユーザが本来支払いをしようとした相手に対して渡したとする。この場合そのワンタイムパスワードは、その相手が管理者となっている決済端末300から、決済装置200に送られる。しかしながら、そのワンタイムパスワードは既に、過去の支払いに使用されてしまっているから、決済装置200の最終判定部225は、そのワンタイムパスワードによる支払いを再び認めることはない。例えば、そのワンタイムパスワードが過去（例えば、一定の時間の範囲内）に利用されたものであることは、最終判定部225が上述した記録媒体に記録されているワンタイムパスワードの中に今最終判定の対象となっているワンタイムパスワードと同じものが存在するか否かを検索し、同じものが存在するのであれば、そのワンタイムパスワードが過去に利用されたものであると判定することができる。

かくして、この場合に決済装置200から、決済端末300へ送られる最終判定データは、決済が認められないということを示すものとなる。本来支払いを受けるべき者であったその決済端末300を管理者は、決済装置200で決済が認められなかったことをワンタイムパスワードを渡してきたユーザに告げる。

これを聞いたユーザは、過去にワンタイムパスワードの不正利用があったことを認識し、上述の取消の処理を実行すればよい。これにより、ワンタイムパスワードの不正利用を防ぐことが可能となる。なお、2回目のワンタイムパスワードの使用の試みがあったことを、上述のように決済装置200は把握することが可能である。その旨を、或いはワンタイムパスワードの不正利用を行おうとする者がいることを、決済装置200はユーザ端末100に通知するようになっていても良い。

[0062] [変形例]

変形例の決済システムについて説明する。この変形例における決済システムは基本的に、第1実施形態の決済システムと同様に構成され、それが実行する決済の流れも、第1実施形態の決済システムの場合と同様である。

第1実施形態と変形例の決済システムで異なるのは、決済装置200の最

最終判定部 225 における、ワンタイムパスワードの生成のタイミング及びその方法と、最終判定の行い方であり、また、それに付随して、決済端末 300 から決済装置 200 に送られるデータにも変更がある。

[0063] 第 1 実施形態では、上述したように、決済端末 300 から決済装置 200 に対して、決済申込情報と、ワンタイムパスワードとを送信する場合には、それらと共にユーザ ID もが送信されるようになっていた。

決済端末 300 から送信された、ユーザ端末 100 で生成されたワンタイムパスワードは、決済装置 200 の OTP 生成部 227 で生成されたワンタイムパスワードと最終判定部 225 で対比されるものであるから、決済申込情報と共に、決済端末 300 から決済装置 200 に送られることが必要となる。他方、決済申込情報とワンタイムパスワードとを決済端末 300 から決済装置 200 に送信するにあたって、ユーザ ID の送信が必要な理由として、第 1 実施形態では、『決済装置 200 がワンタイムパスワードを生成するための条件はユーザ毎に異なるため（例えば、この実施形態ではユーザ毎に割当てられた初期値が異なるが、用いる数式つまりアルゴリズムをユーザ毎に変えることも可能である。）、決済装置 200 においてユーザ毎に異なる条件のうちのどの条件でワンタイムパスワードを生成させるかを確定するために、ユーザを特定するための情報が必要となる。』と説明した。つまり、決済端末 300 から送信された、ユーザ端末 100 で生成されたワンタイムパスワードは、決済装置 200 の OTP 生成部 227 で生成されたワンタイムパスワードと最終判定部 225 で対比されるものであるところ、決済の処理の間に両ワンタイムパスワードが一致するようにするためには、決済装置 200 で、その決済を求めているユーザについてのワンタイムパスワードを生成する必要があるが、その決済を求めているユーザが誰か特定できない限り、正しいワンタイムパスワードを生成することができないから、第 1 実施形態では、決済申込情報及びワンタイムパスワードと共に、ユーザを特定するためのユーザ ID をも決済端末 300 から決済装置 200 に送るようにする、というのが第 1 実施形態における理屈である。したがって、第 1 実施形

態では、決済申込情報及びワンタイムパスワードと共に、ユーザIDか、或いはユーザを特定するための他の情報である署名、指紋や静脈の性状等の情報を、決済端末300から決済装置200に送信することとしていた。

しかしながら、決済申込情報及びワンタイムパスワードに加えて、ユーザID、署名、指紋や静脈の性状等の情報の如きユーザを特定するための情報を決済端末300から決済装置200に対して送らなくとも、決済装置200の最終判定部225で、ユーザ端末100で生成されたワンタイムパスワードと、決済装置200で生成されたワンタイムパスワードとを正しく比較することは可能である。

この変形例は、そのような決済システムに関する。

[0064] 変形例の決済システムでは、上述したように、決済端末300から決済装置200に、決済申込情報が送信される際に、決済申込情報にユーザ端末100で生成されたワンタイムパスワードは付加されるが、ユーザIDを始めとするその決済を行おうとしているユーザを特定するための情報は付加されない。

[0065] 他方、変形例の決済システムでは、OTP生成部227がワンタイムパスワードを生成するタイミングが第1実施形態とは異なる。第1実施形態では、主制御部222からワンタイムパスワードを生成せよとの指示を受けるとワンタイムパスワードを生成するようになっていたが、かかる指示は主制御部222が、データ入出力部221から、決済端末300から送られてきた決済申込情報とワンタイムパスワードとを受取った後に出されていた。

しかし、この変形例では、与信判定部223が仮許可情報を生成すると同時に、或いはその後遅滞なく、少なくとも決済端末300から決済申込情報及びワンタイムパスワードが送られてくるよりも前に、OTP生成部227はワンタイムパスワードを生成する。これには限られないが、この変形例では、与信判定部223が生成した仮許可情報が与信判定部223から主制御部222に送られると、主制御部222は、ワンタイムパスワードを生成せよとの指示を、その仮許可情報の対象となっているユーザIDと共に、O

ＴＰ生成部２２７に送る。この指示を受取ったＯＴＰ生成部２２７は、主制御部２２２から受取ったユーザＩＤを用いて、より正確にはそのユーザＩＤと紐付けられていた初期値を用いて、そのユーザＩＤを持つユーザ用のワンタイムパスワードを生成する。ワンタイムパスワードの生成方法自体は、第１実施形態の場合と同じで良い。ＯＴＰ生成部２２７は、生成したワンタイムパスワードを、遅滞なく最終判定部２２５に送る。ここまでの処理を、この変形例では、与信判定部２２３が仮許可情報を生成するのと同時に、或いはその後遅滞なく、少なくとも決済端末３００から決済申込情報及びワンタイムパスワードが送られてくるよりも前に終わらせる。

最終判定部２２５は、ＯＴＰ生成部２２７から送られたワンタイムパスワードを保持する。この場合、最終判定部２２５には、各ユーザ端末１００を保持するユーザが支払いを行おうとしたことにより、ＯＴＰ生成部２２７によって生成された多数のユーザ用の多数のワンタイムパスワードが保持されることになる。

[0066] そのような状態が生じているときに、あるユーザが、決済端末３００を通して、決済申込情報と共に、そのユーザが持つユーザ端末１００で生成したワンタイムパスワードを、決済装置２００に送信してきたとする。その決済申込情報及びワンタイムパスワードは、決済装置２００の送受信部で受取られ、データ入出力部２２１を介して、主制御部２２２へと送られる。主制御部２２２は、受取った決済申込情報とワンタイムパスワードとを、最終判定部２２５へと送る。

最終判定部２２５は、このとき、主制御部２２２から受取ったワンタイムパスワードと、ＯＴＰ生成部２２７から既に受取っているＯＴＰ生成部２２７が生成した多数のワンタイムパスワードとを保持している。最終判定部２２５は、主制御部２２２から受取ったワンタイムパスワードと、ＯＴＰ生成部２２７から既に受取っているＯＴＰ生成部２２７が生成した多数のワンタイムパスワードとを比較する。最終判定部２２５は、主制御部２２２から受取ったワンタイムパスワードが、ＯＴＰ生成部２２７から既に受取っている

OTP生成部227が生成した多数のワンタイムパスワードの一つと一致した場合には、ユーザから、その決済申込情報及びワンタイムパスワードを送ってきた決済端末300の管理者への支払いを認め、主制御部222から受取ったワンタイムパスワードが、OTP生成部227から既に受取っているOTP生成部227が生成した多数のワンタイムパスワードのいずれとも一致しない場合には、その支払を認めない。最終判定部225は、ユーザ端末100で生成されたワンタイムパスワードと、OTP生成部227が生成した多数のワンタイムパスワードとを比較することになるが、あるユーザ端末100を用いての決済の処理が開始され、仮許可情報が生成された後に、その同じユーザの支払いについての決済申込情報が決済端末300から決済装置200に送られてくるまでの間に決済装置200のOTP生成部227で生成されるワンタイムパスワードの数は、特にユーザ端末100で生成されたワンタイムパスワードに有効期限がある場合には、多数ではあるものの莫大な数とはならず、また、その間にOTP生成部227で作られる複数のユーザ用のワンタイムパスワードに同じものが生じる可能性はまずない。

したがって、最終判定部225は、この変形例の方法によっても、第1実施形態の場合と同様に、正しく最終判定データを生成することができる。

最終判定部225が最終判定を行うにあたり、位置情報を利用することができること、及び時刻情報を利用することができることについては、第1実施形態の場合と変わらない。

ただし、変形例の場合には、ユーザ端末100で生成され、決済端末300を介して送られてきたワンタイムパスワードと、決済装置200のOTP生成部227で生成された多数のワンタイムパスワードとの対比を先に行い、OTP生成部227で生成された多数のワンタイムパスワードの中に、決済端末300から送られてきたワンタイムパスワードと一致するものが存在した場合には、OTP生成部227で生成された多数のワンタイムパスワードのうちの、決済端末300から送られてきたワンタイムパスワードと一致したそのワンタイムパスワードを生成する際に用いられたユーザIDと紐付

けられたユーザ端末１００の位置情報を、他のユーザ端末１００から送られてきた位置情報とは区別して、その最終判定に用いるユーザ端末１００側の位置情報として特定するようにすればよい。

同様に、ＯＴＰ生成部２２７で生成された多数のワンタイムパスワードのうちの、決済端末３００から送られてきたワンタイムパスワードと一致したそのワンタイムパスワードを生成する際に用いられたユーザＩＤと紐付けられた時刻情報を、他のユーザ端末１００を用いて決済を行うために作られた仮許可情報が作られたときの時刻情報とは区別して、その最終判定に用いる時刻情報として特定するようにすればよい。

このようにすることで、最終判定データは正しく生成することが可能となる。

[0067] ≪第２実施形態≫

第２実施形態の決済システムについて説明する。

第２実施形態の決済システムは、概ね第１実施形態の決済システムに同じであり、その決済の処理の流れも概ね第１実施形態の場合と同じである。

第２実施形態の決済システムも、第１実施形態の場合と同じく、そのいずれもがネットワーク４００に対して接続可能とされている、多数のユーザ端末１００、一つの決済装置２００、及び多数の決済端末３００を含んで構成されている。

[0068] 第２実施形態の決済システムの第１実施形態の決済システムと異なる点は、端的に言えば、第１実施形態の決済システムでは、ユーザは、誰に対して支払いを行うかという意思表示を決済装置２００に対して行わなかったのに対して、第２実施形態の決済システムでは、ユーザが、誰に対して支払いを行うかという意思表示を決済装置２００に対して行う、という点である。

それを実現するために、第２実施形態の決済システムは以下のように構成されている。第２実施形態で行われる処理の流れを交えつつ、第２実施形態の決済システムの構成について説明する。

[0069] まず、第２実施形態のユーザ端末１００について説明する。

第2実施形態でもユーザ端末100は、第1実施形態の場合と同様に情報処理を行う制御部120を有している。制御部120は、第1実施形態のユーザ端末100における制御部120と同様のものとされているが、第2実施形態の制御部120には、第1実施形態の場合には存在しなかった決済端末データ記録部125が含まれている。

決済端末データ記録部125は、決済端末300についてのデータを記録するものである。具体的には、決済端末データ記録部125には、第1実施形態における決済装置200の位置情報記録部226に記録されている、図8に示したようなデータが記録されている。つまり、決済端末データ記録部125には、決済端末IDと、各決済端末200の位置情報とが互いに紐付けた状態で記録されている。決済端末IDと、決済装置200の位置情報の意義は、第1実施形態におけるそれらと同じである。また、決済端末データ記録部125に記録されている決済端末ID及び位置情報は、決済装置200の位置情報記録部226に記録されているそれらと完全に一致している。ただし、決済端末データ記録部125には、決済端末IDと各決済端末200の位置情報とに加えて、各決済端末200が置かれている飲食店や店舗の名称、電話番号、住所、及び飲食店や店舗をユーザが認識するのに役立つロゴ等が、それぞれの決済端末IDと紐付けた状態で記録されていても構わない。

[0070] 第1実施形態の決済システムでは、ユーザがS911の決済の処理を開始した場合には、ユーザは続けて、自らのユーザ端末100に、ユーザIDと、パスワードと、決済金額とを入力することになっていた。

これに対して、第2実施形態の決済システムでは、ユーザは、自らのユーザ端末100に、ユーザIDと、パスワードと、決済金額とに加えて、支払いを行う対象となる支払先を特定する情報を入力することになっている。支払先を特定する情報は事実上、その支払先となる店舗等に置かれている決済端末300を特定する情報である。

第2実施形態では、決済の処理が開始されると、ユーザ端末100のディ

スプレイ 101 に、図 17 (A) に示したような画像が表示される。第 1 実施形態の場合と異なり、第 2 実施形態の場合におけるかかる画像は、ユーザ ID と、パスワードと、決済金額との入力に加えて、支払先を特定する情報の入力をもユーザに促すものとなっている。かかる画像は、第 1 実施形態の場合と同様、主制御部 121 の制御下で、表示制御部 122 が生成し、表示制御部 122 がディスプレイ 101 に表示させる。

ユーザは、第 1 実施形態の場合と同様に、ユーザ ID と、パスワードと、決済金額とを入力装置 102 を用いて入力する。また、ユーザは、支払先を特定するための情報を入力する。支払先の情報は、ユーザが支払先の店舗等を打込むことによって入力するようにすることもできるが、ユーザの負担を減らし、またユーザによる入力の誤りを減らすことを重視するのであれば、支払先の店舗等を所定の候補からユーザに選択させるようになっているのが好ましい。この実施形態では、必ずしもその限りではないがそうされている。

ユーザが支払先の入力をしようとする、この実施形態では、図 19 に示したようなウィンドウがポップアップするようになっている。そのウィンドウの中には、★で示されたユーザの現在位置の近くに存在する、決済端末 300 が置かれている店舗等の候補が、例えば、丸で囲まれた 9、19、22 の数字として、ユーザの現在地の近辺を示す地図上に表示される。9、19、22 の丸で囲まれた数字は、これには限られないが、この実施形態では、決済端末 ID に等しい。また、地図の外側、この例では、地図の右側に、それぞれの店舗等の名称と電話番号が、ユーザが正しく店舗等を選択することの助けとなるようにして、地図上に示された上述の 9、19、22 の符号と紐付けられた状態で表示される。

表示される地図の範囲の選択、及び地図上に表示されるユーザの現在位置の特定と、支払先の候補となる店舗等の選択は、ユーザ端末 100 の GPS 機構からデータ入出力部 123 を介して主制御部 121 に送られた、ユーザ端末 100 の現在の位置を示す位置情報を用いて、主制御部 121 が決定す

るようになっている。この実施形態では、この時点で、GPS機構がユーザ端末100が存在する位置についての位置情報を生成する。また、地図の外側に表示される、店舗等に関する情報の作成も、主制御部121が行うようになっている。なお、主制御部121は、かかる処理の一部を、ネットワーク400を介して接続された外部のクラウドに記録されたソフトウェアを利用して行っても構わない。その場合には例えば、決済端末データ記録部125は、ユーザ端末100の外部に存在することもあり得る。

具体的には、主制御部121は、上述の表示をディスプレイ101上に行うにあたって、ユーザ端末100の現在の位置を示す位置情報に基づいて、例えばGoogle Inc. が提供しているグーグルマップ（商標）などで用いられている周知又は公知の手法でディスプレイ101に表示すべき地図の範囲を選択する。また主制御部121は、位置情報によりユーザ端末100の現在位置を特定することが可能となり、地図上におけるその現在位置に★のマークを表示するようにする。また主制御部121は、ユーザ端末100の現在の位置を示す位置情報により特定される位置から近い位置を特定する位置情報を持つ決済端末300の決済端末IDに加え、当該位置情報と紐付けられた、それら店舗等の名称、電話番号等のデータを決済端末データ記録部125から読み出す。それぞれの位置情報に店舗等の位置情報が示す地図上の位置に○で囲んだ決済端末IDを表示することで、地図上に、ユーザがいる位置の近くにある店舗等であってユーザが支払いを行おうとする候補となりうるものを表示することができる。また、決済端末IDと紐付けられたそれら店舗等の名称、電話番号等を、地図の外側に表示することができる。もちろん、表示される店舗等の候補は3つだけとは限らない。主制御部121はこれら情報を表示制御部122に送り、表示制御部122に、図19に示したような画像をディスプレイ101に表示させる。

ユーザは、入力装置102を操作して、9、19、22の候補の中から一つを選択し、決定と書かれたボタンをクリックする。そうすると、ポップアップされた図19に示したウィンドウが閉じ、図17（B）に示したように

、支払先と書かれた部分の右側の枠の中に、ユーザが選択した店舗等の決済端末IDと名称が自動的に書き込まれる。この例では、決済端末IDが19である決済端末300がその店舗等に設置された「〇〇C A F E」が、ユーザが支払いを行おうとする相手側として選択された。これらディスプレイ101上の表示も、主制御部121の制御下で、表示制御部122が制御する。これにより、ユーザ端末100には、ユーザIDと、パスワードと、決済金額と、支払先を特定する情報とが、入力された状態となる。これら4つの情報は、データ入出力部123から主制御部121に送られる。

ユーザIDとパスワードと金額情報と、そして支払先を特定するための情報の入力が終わったら、ユーザは、ディスプレイ101に表示された「決定」と書かれたボタンをクリックする。

[0071] 「決定」と書かれたボタンをユーザがクリックすると、主制御部121は、ユーザIDとパスワードと金額情報と支払先を特定する情報に加えて、位置情報と、主制御部121の図示を省略された記録手段に記録された端末情報とをすべて一纏めにして、それらをデータ入出力部123に送る。データ入出力部123は、それらデータをまとめて送受信部に送り、送受信部は、それらデータをまとめてネットワーク400を介して決済装置200に送るようになっている。これは第1実施形態におけるS913の処理に相当する。

[0072] 決済装置200は、第1実施形態におけるS921の処理と同様に、それらデータを受取り、第1実施形態におけるS922の処理と同様に、与信の判定を実行する。第2実施形態における支払先を特定するための情報以外のユーザ端末100から決済装置200に送られた各情報の取扱いは、第1実施形態の場合と変わらない。また、与信の判定の処理には、第2実施形態ではユーザ端末100から決済装置200に送られる支払先を特定するための情報は用いられないため、第2実施形態の場合でも第1実施形態のときと変わらない。

支払先を特定するための情報は、第2実施形態では、データ入出力部22

1 から主制御部 2 2 2 を介して最終判定部 2 5 5 に送られる。最終判定部 2 5 5 には、最終判定部 2 5 5 が最終判定を行う際に支払先を特定するための情報が届いていれば良い。

[0073] 第 1 実施形態で説明した、決済装置 2 0 0 で実行される、仮許可情報の生成 (S 9 2 3) 及び仮許可情報の送信 (S 9 2 4)、ユーザ端末 1 0 0 で実行される、仮許可情報の受信 (S 9 1 4) 及びワンタイムパスワードの生成 (S 9 1 5)、決済端末 3 0 0 で行われる、ユーザ ID とワンタイムパスワードの入力 (S 9 3 1)、ユーザ ID とワンタイムパスワードの送信 (S 9 3 2) の各処理、及び決済装置 2 0 0 で行われるユーザ ID とワンタイムパスワードの受信 (S 9 2 5) の処理は、第 2 実施形態でも同様に実行される。

[0074] 次いで、第 1 実施形態と同様に、最終判定の実行 (S 9 2 6) がなされる。

第 1 実施形態の最終判定では、ユーザ端末 1 0 0 が生成し、決済端末 3 0 0 から送られてきたワンタイムパスワードと、OTP 生成部 2 2 7 が生成したワンタイムパスワードとを比較してこれらが一致すること、が最終判定で決済が肯定されるための一つ目の条件となった。また、ユーザ端末 1 0 0 が生成し、ユーザ端末 1 0 0 から送られてきた位置情報と、位置情報記録部 2 2 6 から読み出された位置情報とを比較して、両位置情報により特定される位置が、所定の距離よりも近いこと、が最終判定で決済が肯定されるための二つ目の条件となった。そして、与信判定部 2 2 3 が生成した時刻情報により特定される時刻と、最終判定が行われた時刻とを対比し、その時間間隔が所定の時間間隔以内であること、が最終判定で決済が肯定されるための三つ目の条件となった。そして、これら 3 つの条件がすべて満足されたときのみ、最終判定部 2 2 5 は、その決済を認めるという肯定的な最終判定データを生成することとしていた。

これに対して、第 2 実施形態では、ユーザ端末 1 0 0 が生成し、ユーザ端末 1 0 0 から送られてきた決済端末 ID と、決済申込情報等の送信元となっ

た決済端末300の決済端末IDとを比較して、それらが一致すること、を最終判定で決済が肯定されるための四つ目の条件とする。つまり、この実施形態では、以上4つの条件がすべて満足されたときにのみ、最終判定部225は、その決済を認めることになる。なお、上記条件のうち、二つ目と三つ目の条件を省略することができるのは、第1実施形態の場合と同様である。

[0075] 第2実施形態の決済システムにおいて実行される、最終判定データが生成された後の処理は、第1実施形態の場合と同様である。

請求の範囲

[請求項1]

所定のネットワークにそのそれぞれが接続可能とされた、

情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システムであって、

前記ユーザ端末は、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力できるようになっており、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信するようになっているとともに、前記ユーザ端末情報処理手段は、ワンタイムパスワードを生成するユーザ端末OTP生成部を備えており、

前記決済装置は、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部を備えているとともに、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取るようになっており、前記決済装置情報処理手段は、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信

判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記与信判定で前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり、前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する与信判定部と、決済の最終判定を行う最終判定部と、前記ユーザ端末と同じワンタイムパスワードを生成する決済装置OTP生成部とを備えており、前記決済装置送受信手段は、前記与信判定部が生成した仮許可情報を前記ネットワークを介して前記ユーザ端末に送信するようになっているとともに、

前記仮許可情報を前記決済装置から前記ユーザ端末が前記ユーザ端末送受信手段にて受けると、前記ユーザ端末OTP生成部が、ワンタイムパスワードを生成するようになっており、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記与信判定部で前記仮許可情報が生成されたのと同様かその後前記決済装置の前記決済装置OTP生成部で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記最終判定部が、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するとともに、前記決済装置情報処理手段は、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている、

決済システム。

[請求項2]

所定のネットワークにそのそれぞれが接続可能とされた、

情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを

介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システム、を構成するためのユーザ端末であって、

前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力できるようになっており、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信するようになっており、前記ユーザ端末情報処理手段は、ワンタイムパスワードを生成するユーザ端末OTP生成部を備えており、

前記決済装置は、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部を備えているとともに、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取るようになっており、前記決済装置情報処理手段は、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報

で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する与信判定部と、決済の最終判定を行う最終判定部と、前記ユーザ端末と同じワンタイムパスワードを生成する決済装置OTP生成部とを備えており、前記決済装置送受信手段は、前記与信判定部が生成した仮許可情報を前記ネットワークを介して前記ユーザ端末に送信するようになっているとともに、

前記仮許可情報を前記決済装置から前記ユーザ端末が前記ユーザ端末送受信手段にて受けると、前記ユーザ端末OTP生成部が、ワンタイムパスワードを生成するようになっていることにより、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記与信判定部で前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置OTP生成部で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記最終判定部が、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するとともに、前記決済装置情報処理手段は、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている、

ユーザ端末。

[請求項3]

前記ユーザ情報は、ユーザが、前記ユーザ端末入力手段を用いて入力を行うユーザIDと、前記ユーザ端末のそれぞれに対して割り振られたユニークな端末情報の双方を含む、

請求項2記載のユーザ端末。

[請求項4]

前記ユーザ端末は、前記ユーザ端末が存在する位置を特定するため

の情報である位置情報を生成する位置情報生成手段を備えており、前記ユーザ端末送受信手段は、前記位置情報を前記決済装置に送信するようになっており、

前記決済装置の前記最終判定部は、前記ユーザ端末から前記ワンタイムパスワードをその前記決済端末送受信手段で送って来た前記決済端末の位置が、前記ユーザ端末の前記位置情報生成手段で生成された位置情報で特定される位置から、所定の距離以内の場合に限り、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するようになっている、

請求項 2 記載のユーザ端末。

[請求項5] 前記ユーザ端末送受信手段は、前記位置情報を、前記金額情報、及び前記ユーザ情報と一緒に、前記決済装置に送信するようになっている、

請求項 4 記載のユーザ端末。

[請求項6] 前記ユーザ端末入力手段は、前記決済装置の前記最終判定部が決済を許可した後において、そのユーザ端末を用いて過去に行われた決済の一つを特定しそれを取り消すためのユーザ端末取消情報を入力できるようになっているとともに、前記ユーザ端末送受信手段は、前記ユーザ端末取消情報を前記ネットワークを介して前記決済装置に送るようになっている、

前記決済装置情報処理手段は、前記ユーザ端末取消情報を受付けたときに、前記ユーザ端末取消情報で特定された決済を取り消す、取消手段を備えている、

請求項 2 記載のユーザ端末。

[請求項7] 所定のネットワークにそのそれぞれが接続可能とされた、情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ

端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システム、を構成するためのユーザ端末に含まれるユーザ端末情報処理手段にて実行される方法であって、

前記ユーザ端末情報処理手段が、

前記ユーザ端末入力手段により、決済の対象となる金額を特定する情報である金額情報の入力を受付ける過程と、

前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信する過程と、

前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取った前記決済装置において、前記決済装置情報処理手段が、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合にその旨を示す情報である仮許可情報を生成し、その仮許可情報を前記決済装置送受信手段が、前記ネットワークを介して前記ユーザ端末に送信した場合に、それを前記ユーザ端末送受信手段により受付

ける過程と、

前記仮許可情報を前記決済装置から前記ユーザ端末が受付けた場合に、ワンタイムパスワードを生成する過程と、

を含んでいることにより、

前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記決済装置情報処理手段で、前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記決済装置情報処理手段が、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを許可するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じる、

方法。

[請求項8]

所定のネットワークにそのそれぞれが接続可能とされた、

情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユー

ザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システム、を構成するためのユーザ端末としてコンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

前記ユーザ端末入力手段により、決済の対象となる金額を特定する情報である金額情報の入力を受付ける過程と、

前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信する過程と、

前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取った前記決済装置において、前記決済装置情報処理手段が、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合にその旨を示す情報である仮許可情報を生成し、その仮許可情報を前記決済装置送受信手段が、前記ネットワークを介して前記ユーザ端末に送信した場合に、それを前記ユーザ端末送受信手段により受付ける過程と、

前記仮許可情報を前記決済装置から前記ユーザ端末が受付けた場合に、ワンタイムパスワードを生成する過程と、

を実行させることにより、

前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前

記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記決済装置情報処理手段で、前記仮許可情報が生成されたのと同様かその後に前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記決済装置情報処理手段が、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを許可するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている、

コンピュータプログラム。

[請求項9]

所定のネットワークにそのそれぞれが接続可能とされた、

情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システム、を構成するための決済装置であって、

前記ユーザ端末は、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報を入力できるようになっており、前記金額情報と、前記金額情報により特定される金額の支払い

を行うユーザを特定する情報であるユーザ情報とを、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信するようになっているとともに、前記ユーザ端末情報処理手段は、ワンタイムパスワードを生成するユーザ端末OTP生成部を備えており、

前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取るようになっており、前記決済装置情報処理手段は、前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する与信判定部と、決済の最終判定を行う最終判定部と、前記ユーザ端末と同じワンタイムパスワードを生成する決済装置OTP生成部とを備えており、前記決済装置送受信手段は、前記与信判定部が生成した仮許可情報を前記ネットワークを介して前記ユーザ端末に送信するようになっているとともに、

前記仮許可情報を前記決済装置から前記ユーザ端末が前記ユーザ端末送受信手段にて受け取ると、前記ユーザ端末OTP生成部が、ワンタイムパスワードを生成するようになっており、前記ユーザ端末で生成されたそのワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置の前記与信判定部で前記仮許可情報が生成されたのと同様かそ

の後に前記決済装置の前記決済装置OTP生成部で生成されたワンタイムパスワードと一致したことを条件に、前記決済装置の前記最終判定部が、そのワンタイムパスワードによる前記ユーザ端末のユーザから、前記決済端末の管理者への支払いを許可するとともに、前記決済装置情報処理手段は、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じるようになっている、

決済装置。

[請求項10] 前記最終判定部は、ユーザが、前記ユーザ端末入力手段によって、前記金額情報を入力するための処理を開始してから、前記最終判定部が決済の最終判定を行う前までのうちの所定の時点から、前記最終判定部が決済の最終判定を行うまでの時間が、予め定められた時間間隔よりも短い場合にのみ、決済を許可するようになっている、

請求項9記載の決済装置。

[請求項11] 前記ユーザ端末入力手段は、ユーザからの支払いを受ける者が管理する決済端末を特定する情報である決済端末特定情報を入力できるようになっているとともに、前記ユーザ端末送受信手段は、前記決済端末特定情報を前記ネットワークを介して前記決済装置に送るようになっている、

前記最終判定部は、前記決済装置に前記ワンタイムパスワードを送ってきた前記決済端末が、前記ユーザ端末から送られてきた前記決済端末特定情報で特定される前記決済端末と一致した場合にのみ決済を許可するようになっている、

請求項9記載の決済装置。

[請求項12] 前記ユーザ端末入力手段は、前記決済装置の前記最終判定部が決済を許可した後において、そのユーザ端末を用いて過去に行われた決済の一つを特定しそれを取り消すためのユーザ端末取消情報を入力できるようになっているとともに、前記ユーザ端末送受信手段は、前記ユー

が端末取消情報を前記ネットワークを介して前記決済装置に送るよう
になっており、

前記決済装置情報処理手段は、前記ユーザ端末取消情報を受付けた
ときに、前記ユーザ端末取消情報で特定された決済を取消す、取消手
段を備えている、

請求項 9 記載の決済装置。

[請求項13] 前記決済端末入力手段は、前記決済装置の前記最終判定部が決済を
許可した後において、その決済端末を用いて過去に行われた決済の一
つを特定しそれを取消するための決済端末取消情報を入力できるよう
になっているとともに、前記決済端末送受信手段は、前記決済端末取消
情報を前記ネットワークを介して前記決済装置に送るようになってお
り、

前記決済装置情報処理手段は、前記決済端末取消情報を受付けたと
きに、前記決済端末取消情報で特定された決済を取消す、取消手段を
備えている、

請求項 9 記載の決済装置。

[請求項14] 前記決済端末入力手段は、前記決済装置の前記最終判定部が決済を
許可した後において、その決済端末を用いて過去に行われた決済の一
つを特定しそれを取消するための決済端末取消情報を入力できるよう
になっているとともに、前記決済端末送受信手段は、前記決済端末取消
情報を前記ネットワークを介して前記決済装置に送るようになってお
り、

前記取消手段は、前記ユーザ端末取消情報と、前記決済端末取消情
報とを受付け且つそれらが特定する決済が一致したときに当該決済を
取消すようになっている、

請求項 1 2 記載の決済装置。

[請求項15] 前記最終判定部は、決済を許可しなかったときに、どの決済を許可
しなかったかを特定して決済を許可しなかったことを示す不許可情報

を生成して前記決済装置送受信手段に送るようになっており、前記決済装置送受信手段は、前記不許可情報を前記ネットワークを介して前記決済端末に送信するようになっており、

前記不許可情報を受付けた前記決済端末は、どの決済が許可されなかったかを前記決済端末の管理者に通知するようになっている、

請求項 12～14 のいずれかに記載の決済装置。

[請求項16]

所定のネットワークにそのそれぞれが接続可能とされた、

情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システム、を構成するための決済装置に含まれる決済装置情報処理手段にて実行される方法であって、

前記決済装置情報処理手段が、

前記ユーザ端末において、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報が入力された後に、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とが、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信された際に、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取る過程、

前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である受信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合に、その旨を示す情報である仮許可情報を生成する過程、

生成した仮許可情報を、前記決済装置送受信手段により、前記ネットワークを介して前記ユーザ端末に送信する過程、

前記仮許可情報を前記決済装置から前記ユーザ端末送受信手段にて受付けた前記ユーザ端末において、前記ユーザ端末情報処理手段が生成したワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置送受信手段で受取る過程、

前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置で前記仮許可情報が生成されたのと同様かその後に、前記ユーザ端末と同じワンタイムパスワードを生成することのできるようにされた前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを決済するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じる過程、

を含む、方法。

[請求項17]

所定のネットワークにそのそれぞれが接続可能とされた、

情報の入力を受付けるユーザ端末入力手段と、前記ネットワークを

介してデータの送受信を行うユーザ端末送受信手段と、情報処理を行うユーザ端末情報処理手段とを備えている、ユーザが使用するユーザ端末と、

前記ネットワークを介してデータの送受信を行う決済装置送受信手段と、情報処理を行う決済装置情報処理手段と、前記ユーザそれぞれの預金残高を特定する預金残高情報を記録する預金残高記録部とを備えている、ユーザの支払いの決済を行う決済装置と、

情報の入力を受付ける決済端末入力手段と、前記ネットワークを介してデータの送受信を行う決済端末送受信手段とを備えている、ユーザからの支払いを受ける者が管理する決済端末と、

を含んで構成されている決済システム、を構成するための決済装置としてコンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

前記ユーザ端末において、前記ユーザ端末入力手段によって、決済の対象となる金額を特定する情報である金額情報が入力された後に、前記金額情報と、前記金額情報により特定される金額の支払いを行うユーザを特定する情報であるユーザ情報とが、前記ユーザ端末送受信手段によって、前記ネットワークを介して前記決済装置に送信された際に、前記金額情報と、前記ユーザ情報とを前記ユーザ端末から前記決済装置送受信手段によって受取る過程、

前記決済装置送受信手段が前記金額情報と、前記ユーザ情報とを受取った場合に、前記ユーザ情報で特定されるユーザについての前記金額情報で特定される金額の支払いの決済が可能か否かの判定である与信判定を、前記預金残高記録部から読みだした前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であるか否かにより実行し、前記預金残高情報で特定される預金残高が前記金額情報で特定される金額以上であり前記決済が可能であると判定した場合

に、その旨を示す情報である仮許可情報を生成する過程、

生成した仮許可情報を、前記決済装置送受信手段により、前記ネットワークを介して前記ユーザ端末に送信する過程、

前記仮許可情報を前記決済装置から前記ユーザ端末送受信手段にて受付けた前記ユーザ端末において、前記ユーザ端末情報処理手段が生成したワンタイムパスワードを、前記決済端末の前記決済端末入力手段から入力し、それを前記決済端末が前記決済端末送受信手段から前記ネットワークを介して前記決済装置に送った場合に、前記決済装置送受信手段で受取る過程、

前記決済装置が前記決済端末から受取ったワンタイムパスワードが、前記決済装置で前記仮許可情報が生成されたのと同様かその後に、前記ユーザ端末と同じワンタイムパスワードを生成することのできるようにされた前記決済装置の前記決済装置情報処理手段で生成されたワンタイムパスワードと一致したことを条件に、そのワンタイムパスワードによる前記ユーザ端末のユーザから前記決済端末の管理者への支払いを決済するとともに、前記預金残高記録部に記録された当該ユーザの預金残高から許可された前記支払いに用いられた金額を減じる過程、

を実行させるようになっている、コンピュータプログラム。

[請求項18] 請求項2記載のユーザ端末で生成された前記ワンタイムパスワードを、紙に印刷してなる、
金券。

[請求項19] 前記ワンタイムパスワードの一部は、前記紙の一方の面に、前記ワンタイムパスワードの残部は、前記紙の他方の面に、それぞれ印刷されている、

請求項18記載の金券。

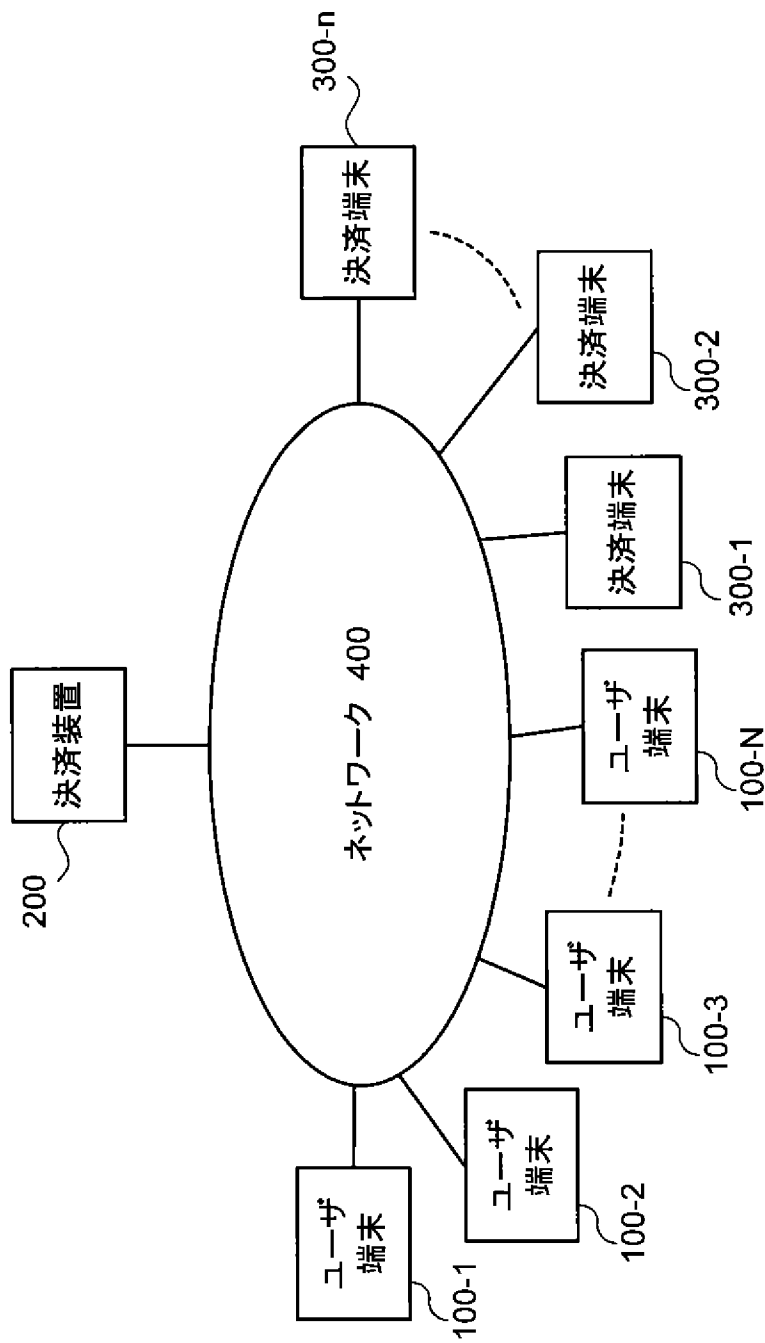
[請求項20] 請求項2記載のユーザ端末で生成された前記ワンタイムパスワードを特定するための情報を、紙に印刷してなる、

金券。

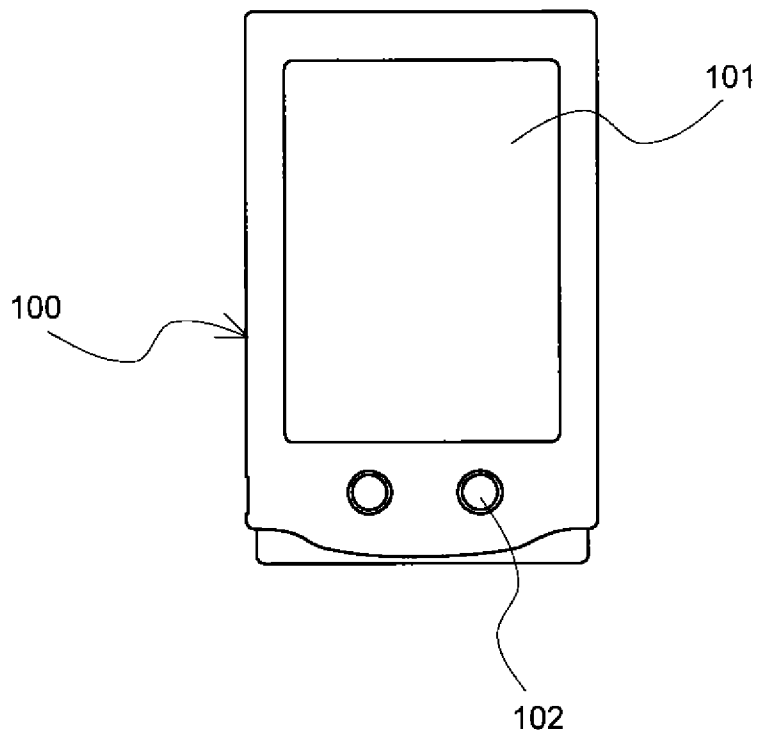
[請求項21] 前記ワンタイムパスワードの一部を特定するための情報が、前記紙の一方の面に、前記ワンタイムパスワードの残部を特定するための情報が、前記紙の他方の面に、それぞれ印刷されている、
請求項20記載の金券。

[請求項22] 前記紙には、その金券を使用することが予定された者の顔が印刷されている、
請求項18～21のいずれかに記載の金券。

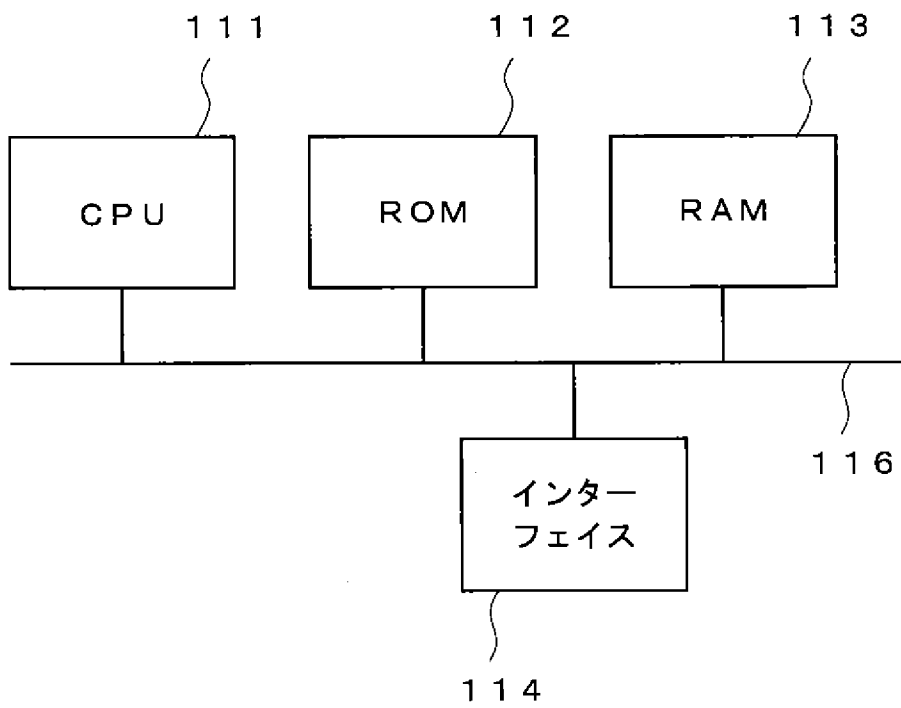
[図1]



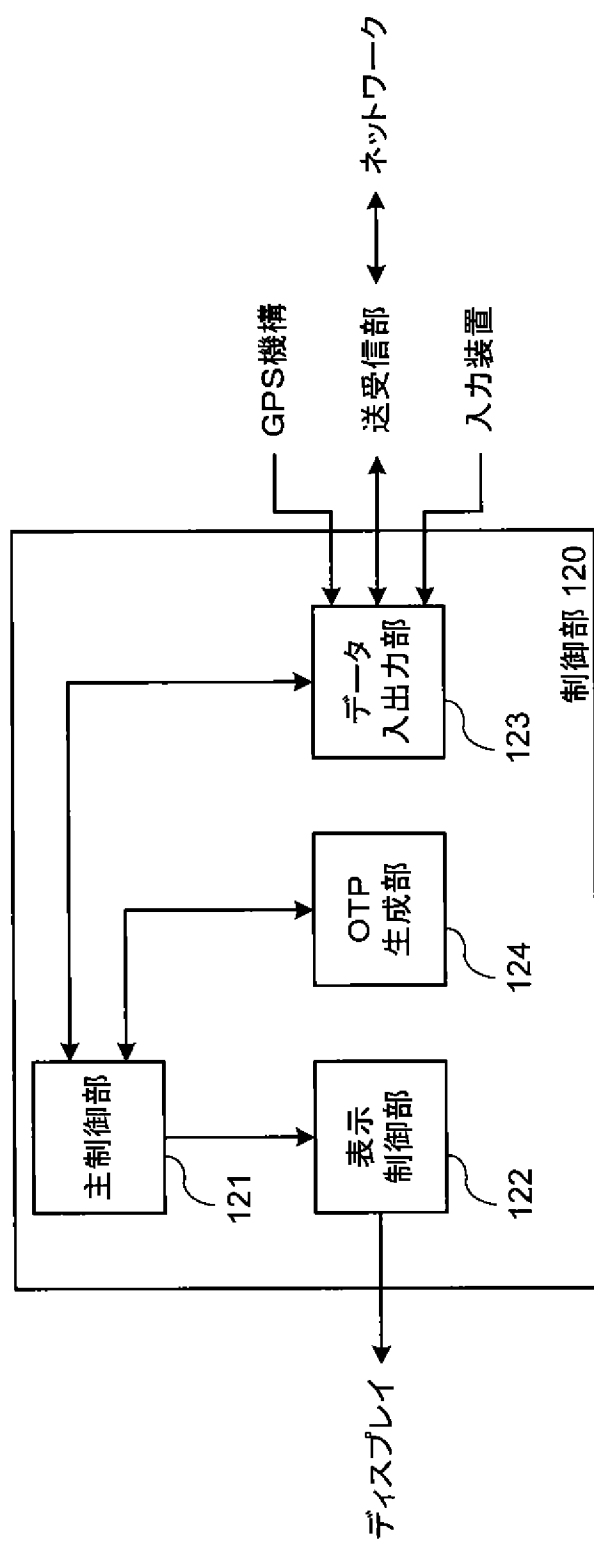
[図2]



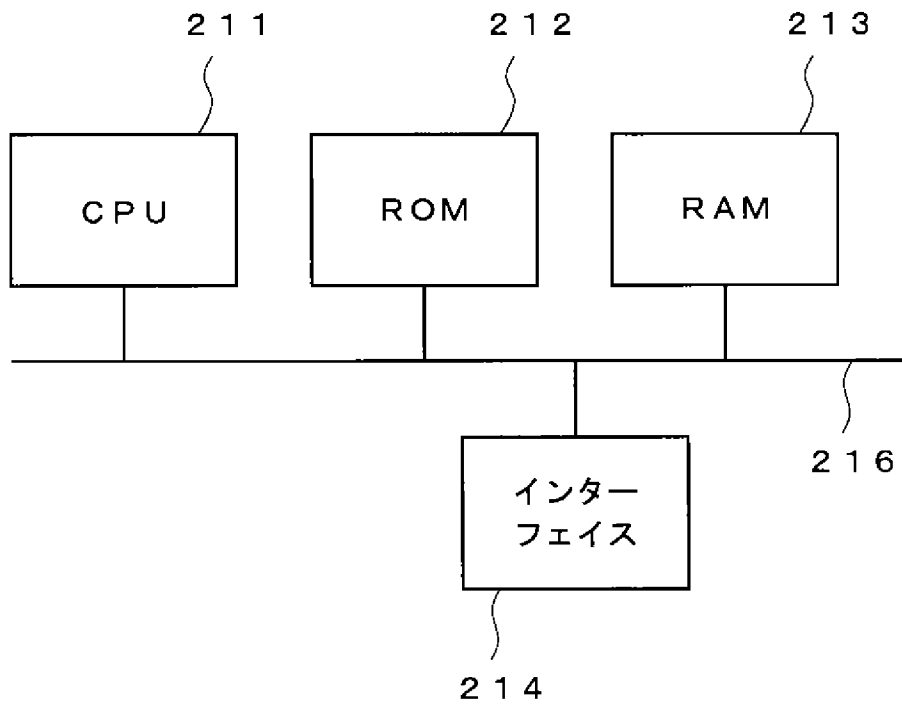
[図3]



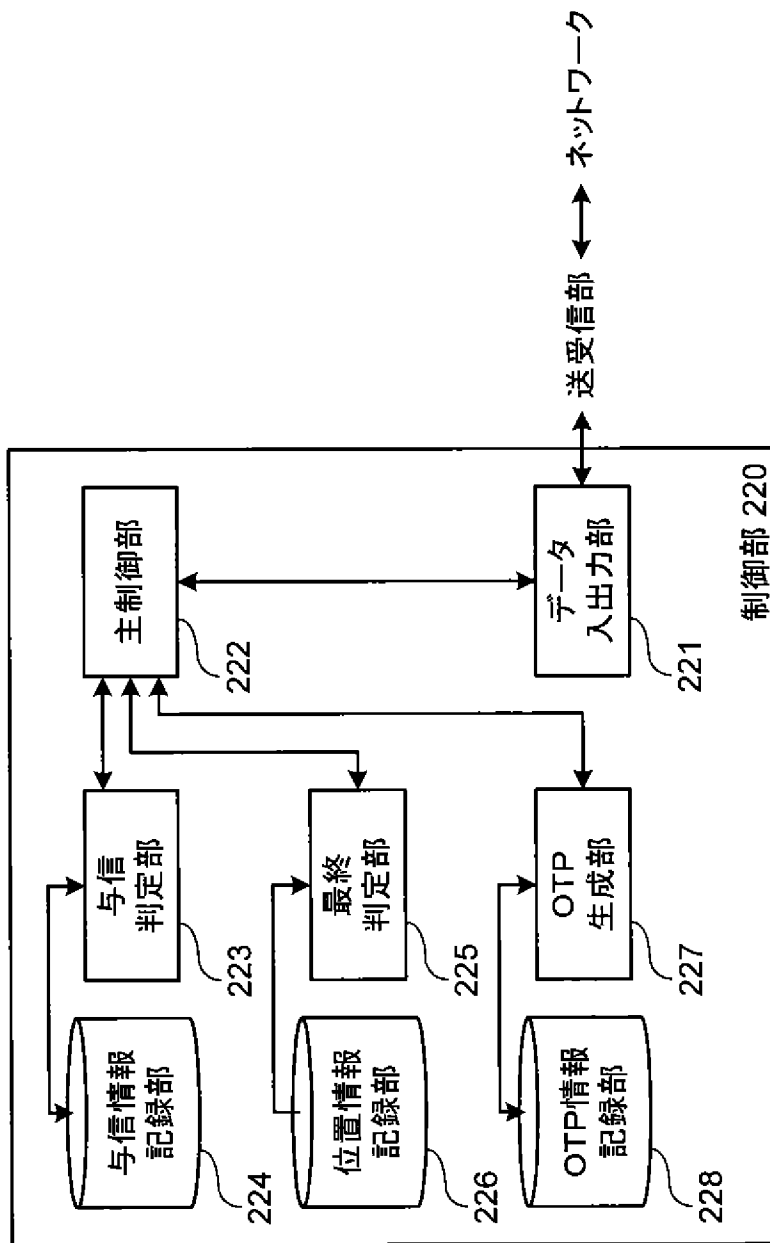
[図4]



[図5]



[図6]



[図7]

ユーザ I D	パスワード	端末情報	預金残高 (¥)
12385adf0	fai2fa60	123456789	10000000
d2af1apfa	aofau554	012457854	2956002
fd8a4op44	mauoa365	658799365	1505612
nm465fai3	009afaoi	709658456	204550
faio897a8	pl36a7uf	325778456	5002230
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
90afa45a5	5f0a65ak	201147775	700445
21orz4651	a4awktk0	123388440	0

[図8]

決済端末 I D

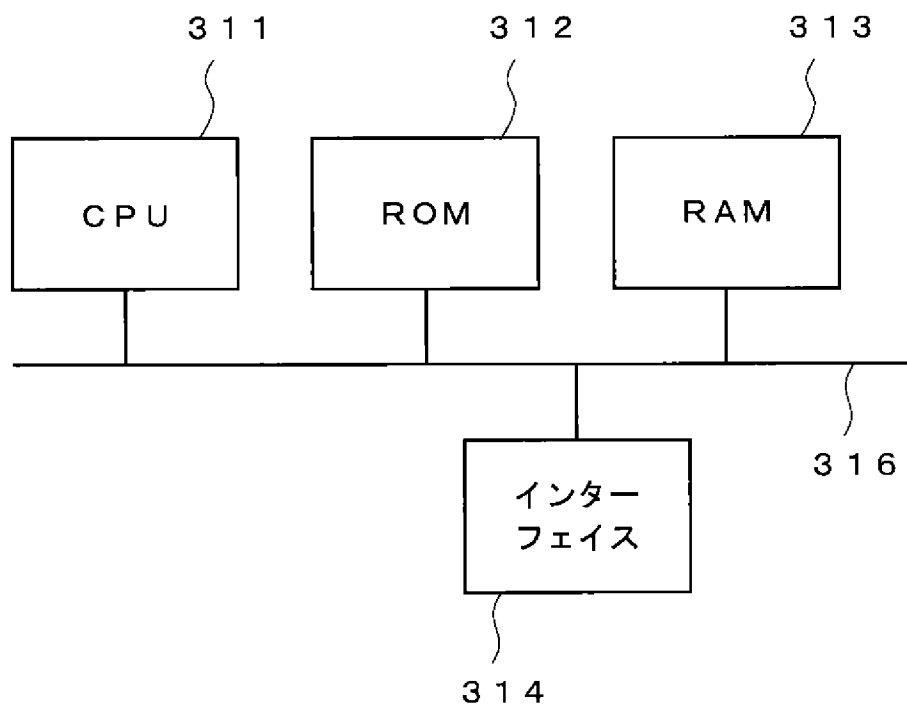
位置情報

1	36° 18' 48.3"N	139° 21' 17.5"E
2	48° 34' 25.3"N	13° 24' 56.8"E
3	40° 44' 33.2"N	73° 59' 36.1"W
4	-----	
5	33° 56' 41.4"S	151° 14' 46.7"E
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.
n — 1	41° 24' 14.2"N	2° 11' 09.1"E
n	22° 54' 37.7"S	43° 14' 27.6"W

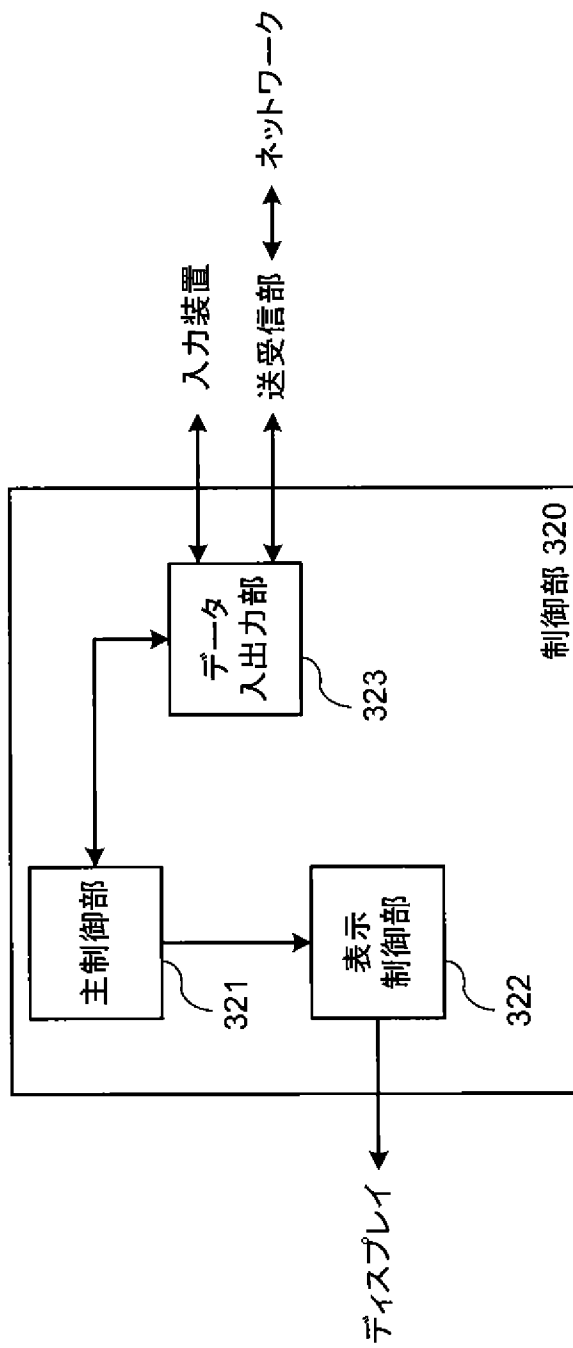
[図9]

ユーザ I D	初期値		生成回数
12385adf0	001245533	123458899	12
d2af1apfa	178655336	458752225	233
fd8a4op44	398756899	157846355	0
nm465fai3	569869896	700002321	4501
faio897a8	755003665	923658855	990
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
90afa45a5	4577778123	6356899677	9455
21orz4651	6898100021	3236955441	214651

[図10]



[図11]



[図12]

(A)

決済開始	決定
ユーザID :	
パスワード :	
金額 (円) :	

(B)

決済開始	決定
ユーザID :	d2af1apfa
パスワード :	aofau554
金額 (円) :	25,000

[図13]

(A)

ワンタイムパスワードは以下の通りです
このワンタイムパスワードは今から5分間有効です

0 1 5 6 3 8 9 4 4 5 1

(B)

あなたの依頼した決済は、
以下の理由でできません

- ☐ ユーザIDが誤っています
- ☒ パスワードが正しくありません
- ☐ 登録された端末ではありません
- ☐ 残高不足です

[図14]

(A)

最終確認

決定

ユーザID :

O T P :

(B)

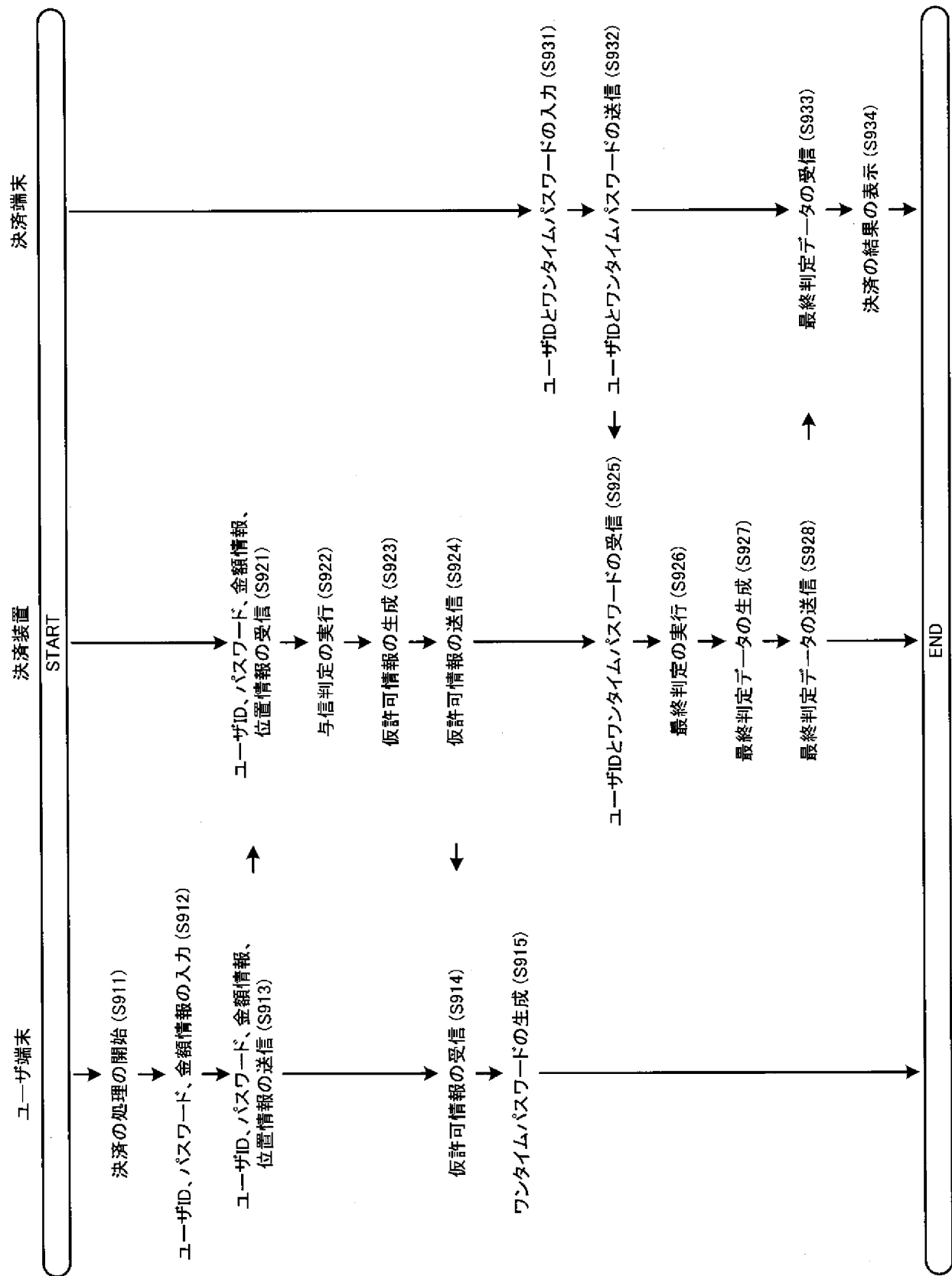
最終確認

決定

ユーザID :

O T P :

[図15]



[図16]

(A)

取消し可能な決済	決定
☐ 2015/9/15 19:21	¥25,000
☐ 2015/9/15 19:18	¥2,600

(B)

取消し可能な決済	決定
☒ 2015/9/15 19:21	¥25,000
☐ 2015/9/15 19:18	¥2,600

[図17]

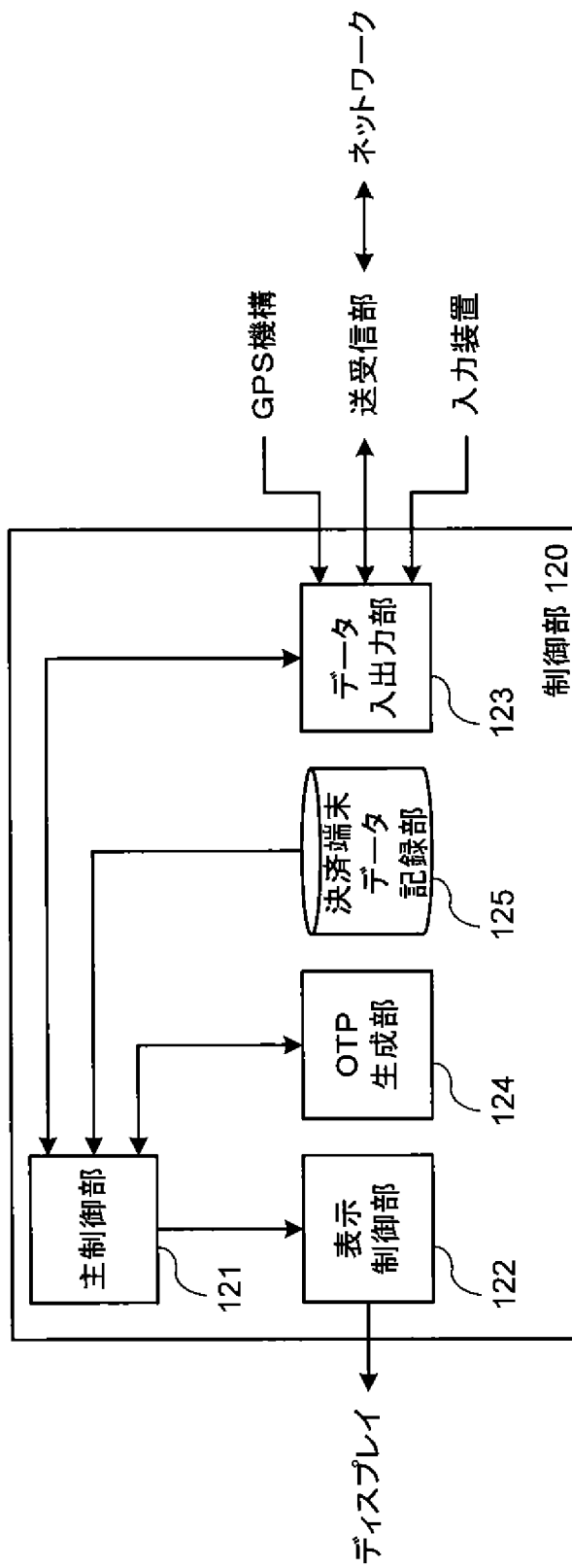
(A)

決済開始	決定
ユーザID :	
パスワード :	
金額 (円) :	
支払先 :	

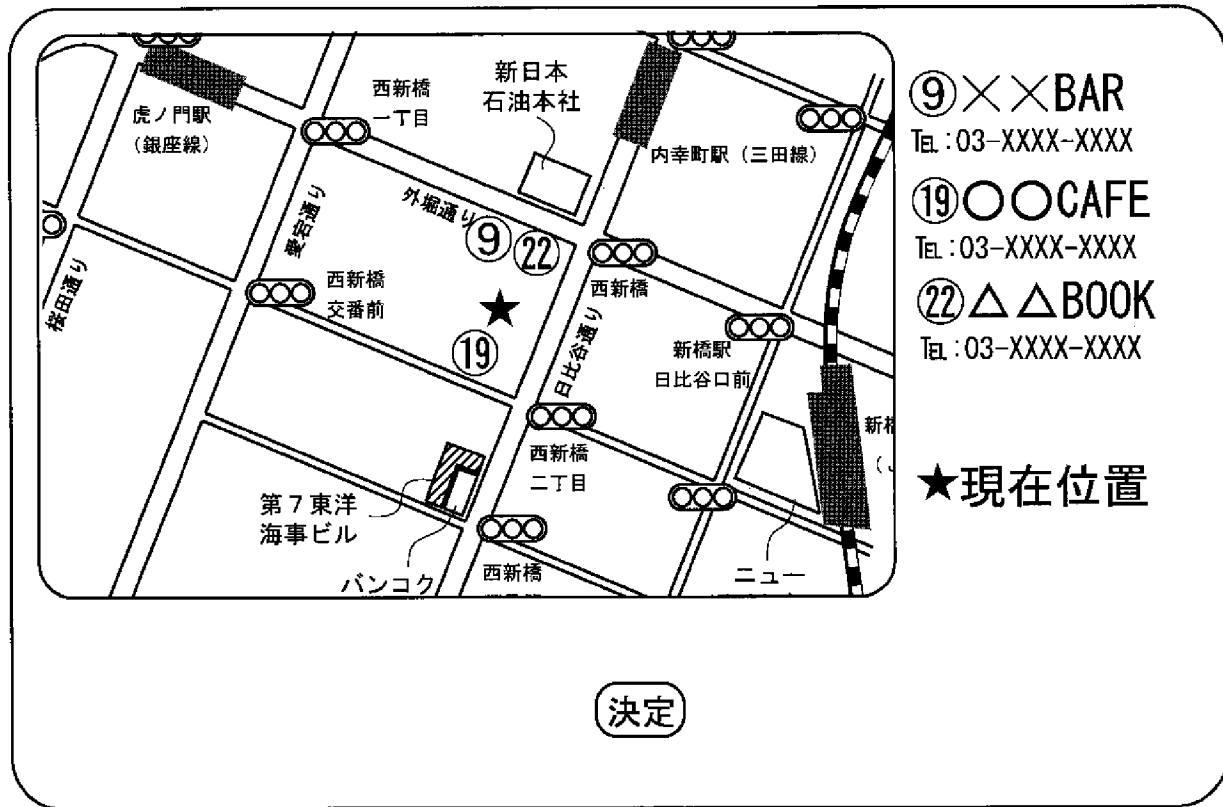
(B)

決済開始	決定
ユーザID :	d2af1apfa
パスワード :	aofau554
金額 (円) :	25,000
支払先 :	①9 ○○CAFE

[図18]



[図19]

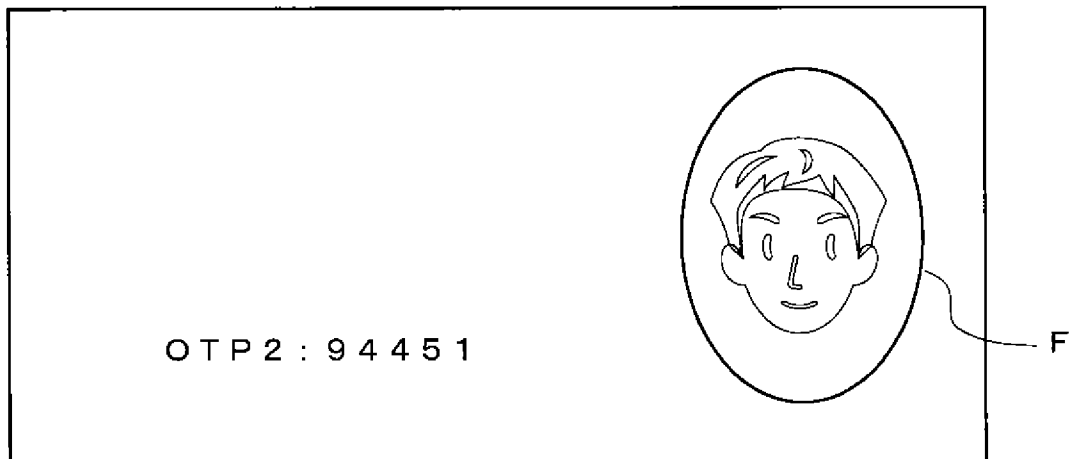


[図20]

(A)

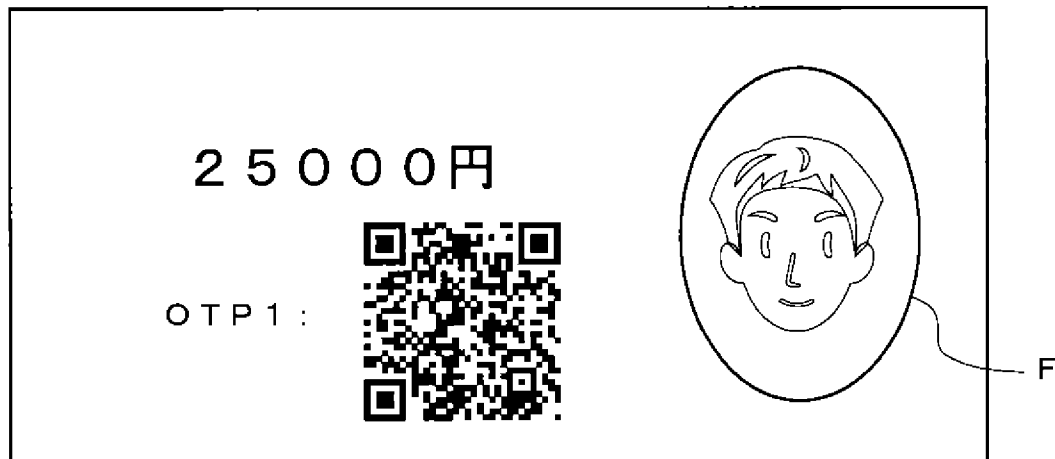


(B)

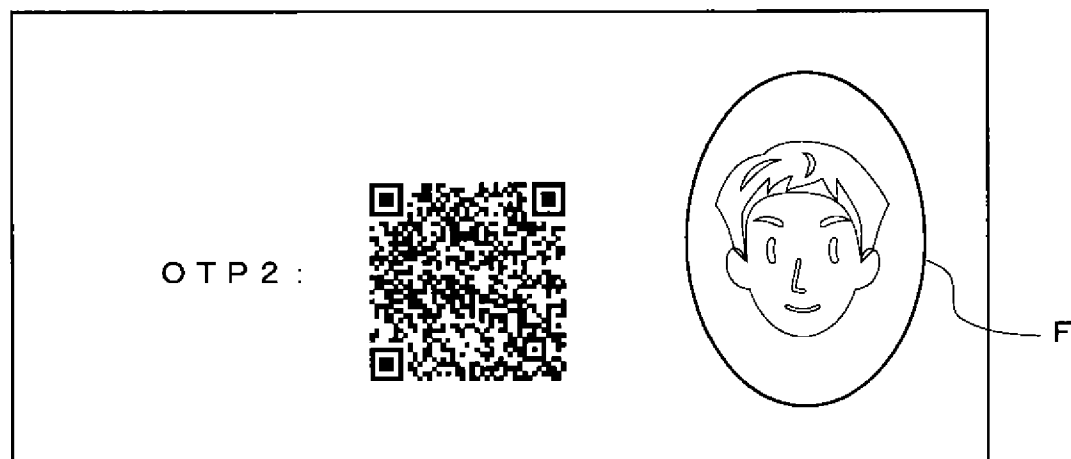


[図21]

(A)



(B)



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/082873

A. CLASSIFICATION OF SUBJECT MATTER

G06Q20/40(2012.01)i, G07G1/12(2006.01)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)

G06Q20/40, G07G1/12

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

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.
Y	JP 2010-61318 A (N-Crypt Lab., Inc.), 18 March 2010 (18.03.2010), paragraphs [0004] to [0062] (Family: none)	1-17
Y	JP 2012-48694 A (Kabushiki Kaisha ZYBOX), 08 March 2012 (08.03.2012), paragraphs [0014] to [0016], [0020] (Family: none)	1-17
Y	JP 2015-152952 A (Sumitomo Mitsui Card Co., Ltd.), 24 August 2015 (24.08.2015), paragraphs [0057] to [0059] (Family: none)	1-17

☒ 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
18 January 2017 (18.01.17)

Date of mailing of the international search report
31 January 2017 (31.01.17)

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/JP2016/082873

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-209616 A (Nippon Seigyo Kabushiki Kaisha), 03 August 2001 (03.08.2001), paragraph [0015] (Family: none)	10
Y	JP 2008-102914 A (Yahoo Japan Corp.), 01 May 2008 (01.05.2008), paragraph [0029] (Family: none)	10
X Y	JP 2005-313438 A (Dainippon Printing Co., Ltd.), 10 November 2005 (10.11.2005), paragraphs [0017], [0019]; fig. 1 (Family: none)	18, 20, 22 19, 21
Y	JP 2001-331731 A (Toppan Printing Co., Ltd.), 30 November 2001 (30.11.2001), paragraph [0079] (Family: none)	19, 21
Y	JP 2002-41472 A (Asahi Business Assist Ltd.), 08 February 2002 (08.02.2002), paragraph [0012] & US 2004/0053654 A1 paragraph [0009] & US 2009/0328162 A1 & WO 2002/008921 A1 & EP 1313027 A1 & AU 7278401 A & CN 1455899 A & CN 101025778 A	19, 21
A	US 2003/0028439 A1 (COX, Christopher Robert), 06 February 2003 (06.02.2003), entire text & WO 2003/008202 A1 & CA 2353283 A1	1-22

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06Q20/40(2012.01)i, G07G1/12(2006.01)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（IPC））

Int.Cl. G06Q20/40, G07G1/12

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	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017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
Y	JP 2010-61318 A（株式会社エヌクリプトラボ）2010.03.18, 段落0004-0062（ファミリーなし）	1-17
Y	JP 2012-48694 A（株式会社ZYBOX）2012.03.08, 段落0014-0016、0020（ファミリーなし）	1-17
Y	JP 2015-152952 A（三井住友カード株式会社）2015.08.24, 段落0057-0059（ファミリーなし）	1-17

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	「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
「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	「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
「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）	「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
「O」 口頭による開示、使用、展示等に言及する文献	「&」 同一パテントファミリー文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日

18.01.2017

国際調査報告の発送日

31.01.2017

国際調査機関の名称及びあて先

日本国特許庁（ISA/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）

塩田 徳彦

5 L

4533

電話番号 03-3581-1101 内線 3562

C (続き) . 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
Y	JP 2001-209616 A (日本制御株式会社) 2001. 08. 03, 段落 0015 (ファミリーなし)	10
Y	JP 2008-102914 A (ヤフー株式会社) 2008. 05. 01, 段落 0029 (ファミリーなし)	10
X Y	JP 2005-313438 A (大日本印刷株式会社) 2005. 11. 10, 段落 0017、0019、図 1 (ファミリーなし)	18, 20, 22 19, 21
Y	JP 2001-331731 A (凸版印刷株式会社) 2001. 11. 30, 段落 0079 (ファミリーなし)	19, 21
Y	JP 2002-41472 A (有限会社旭ビジネスアシスト) 2002. 02. 08, 段落 0012 & US 2004/0053654 A1 段落 0009 & US 2009/0328162 A1 & WO 2002/008921 A1 & EP 1313027 A1 & AU 7278401 A & CN 1455899 A & CN 101025778 A	19, 21
A	US 2003/0028439 A1 (COX, Christopher Robert) 2003. 02. 06, 全文 & WO 2003/008202 A1 & CA 2353283 A1	1-22