(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2019年3月14日(14.03.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/049711 A1

(51) 国際特許分類:
G06Q 20/40 (2012.01) *G06Q 20/32* (2012.01)

(21) 国際出願番号： PCT/JP2018/031661

(22) 国際出願日： 2018年8月28日(28.08.2018)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
62/556,564 2017年9月11日(11.09.2017) US

(71) 出願人: ソニー株式会社 (**SONY CORPORATION**) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

(72) 発明者: 鈴木 謙治 (**SUZUKI Kenji**); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 王 啓宏 (**Wang QiHong**); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP).

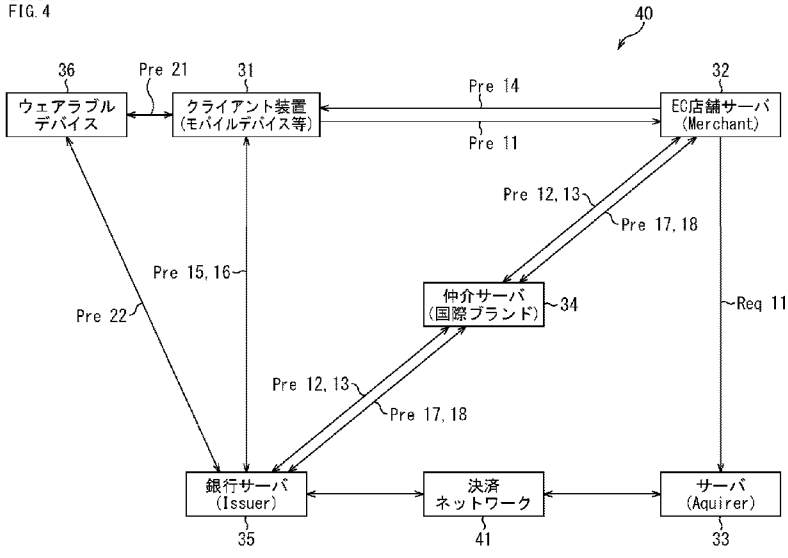
(74) 代理人: 西川 孝，外 (**NISHIKAWA Takashi** et al.); 〒1600023 東京都新宿区西新宿７丁目５番２５号 西新宿プライムスクエア９階 Tokyo (JP).

(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,

(54) **Title:** INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, CLIENT SYSTEM, AND METHOD FOR CONTROLLING CLIENT SYSTEM

(54) 発明の名称： 情報処理装置、および情報処理方法、並びに、クライアントシステム、およびクライアントシステムの制御方法

[図4]
FIG. 4



31 Client device (mobile device or the like)
32 EC store server (Merchant)
33 Server (Aquirer)
34 Mediation server (international brand)
35 Bank server (Issuer)
36 Wearable device
41 Settlement network

(57) **Abstract:** The present disclosure pertains to an information processing apparatus, an information processing method, a client system, and a method for controlling the client system, which are capable of reducing user's time and effort required for authentication without lowering the security level of a settlement process. According to the present invention,

WO 2019/049711 A1

[続葉有]

HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, 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))

a user wears a wearable device that carries out fingerprint authentication and periodically transmits positional information to a bank server. The user carries out a settlement process by operating a client device comprising a smartphone, a PC, or the like. The client device transmits positional information of itself to the bank server when the settlement process is to be performed. The bank server reduces a risk score when the positional information of the wearable device and the positional information of the client device indicate that the wearable device and the client device are at the same position. The information processing apparatus can be applied to a settlement processing system.

(57) 要約:本開示は、決済処理のセキュリティレベルを下げることなく、ユーザによる認証の手間を低減することができるようにする情報処理装置、および情報処理方法、並びに、クライアントシステム、およびクライアントシステムの制御方法に関する。 ユーザが、指紋認証を行うと共に位置情報を定期的に銀行サーバに送信するウェアラブルデバイスを装着する。また、ユーザは、スマートフォンやPCなどからなるクライアント装置を操作して決済処理を行う。クライアント装置は、決済処理がなされる際、自らの位置情報を銀行サーバに送信する。銀行サーバは、ウェアラブルデバイスの位置情報と、クライアント装置の位置情報とから同一の位置に存在すれば、リスクスコアを低減する。決済処理システムに適用することができる。

明　細　書

発明の名称 ：

情報処理装置、および情報処理方法、並びに、クライアントシステム、およびクライアントシステムの制御方法

技術分野

[0001] 本開示は、情報処理装置、および情報処理方法、並びに、クライアントシステム、およびクライアントシステムの制御方法に関し、特に、決済処理におけるセキュリティレベルを下げることなく、ユーザによる認証の手間を低減できるようにした情報処理装置、および情報処理方法、並びに、クライアントシステム、およびクライアントシステムの制御方法に関する。

背景技術

[0002] 電子決済に際して、ユーザの正当性に応じた信頼情報に基づいて、認証処理方法を決定する技術が提案されている（特許文献１参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１５－０７６０４４号公報

発明の概要

発明が解決しようとする課題

[0004] しかしながら、特許文献１に記載の技術においては、ユーザの正当性に応じた信頼情報に基づいて、認証処理方法を決定するのみであり、ユーザの認証処理は必須であるため、ユーザには、面倒な認証処理が強いられていた。

[0005] 本開示は、このような状況に鑑みてなされたものであり、特に、決済処理におけるセキュリティレベルを下げることなく、ユーザによる認証の手間を低減できるようにするものである。

課題を解決するための手段

[0006] 本開示の第１の側面の情報処理装置および情報処理方法は、決済処理にお

いて、ユーザを認証した認証装置と、前記ユーザが前記決済処理を行うクライアント装置との位置関係に基づいて、前記決済処理に係るリスクを判定するリスク判定部を含む情報処理装置および情報処理方法である。

[0007] 本開示の第１の側面においては、決済処理において、ユーザを認証した認証装置と、前記ユーザが前記決済処理を行うクライアント装置との位置関係に基づいて、前記決済処理に係るリスクが判定される。

[0008] 本開示の第２の側面のクライアントシステムおよびクライアントシステムの制御方法は、ユーザを認証する認証装置と、決済処理に係るリスクを判定する情報処理装置に対して前記ユーザによる前記決済処理を実行するクライアント装置とからなるクライアントシステムであって、前記認証装置が、前記ユーザを認証する認証部と、前記認証装置の位置情報を認証装置位置情報として取得する認証装置位置情報取得部と、前記認証部による認証結果と前記認証装置位置情報を前記情報処理装置に送信する認証装置位置情報送信部とを含み、前記クライアント装置は、前記クライアント装置の位置情報をクライアント装置位置情報として取得するクライアント装置位置情報取得部と、前記クライアント装置位置情報を前記情報処理装置に送信するクライアント装置位置情報送信部とを含むクライアントシステムである。

[0009] 本開示の第２の側面においては、前記認証装置により、前記ユーザが認証され、前記認証装置の位置情報が認証装置位置情報として取得され、認証結果と前記認証装置位置情報が前記情報処理装置に送信され、前記クライアント装置により、前記クライアント装置の位置情報がクライアント装置位置情報として取得され、前記クライアント装置位置情報が前記情報処理装置に送信される。

発明の効果

[0010] 本開示の一側面によれば、決済処理におけるセキュリティレベルを下げることなく、ユーザによる認証の手間を低減することが可能となる。

図面の簡単な説明

[0011] [図1]決済処理システムの概要を説明する図である。

[図2]事前与信処理システムの概要を説明する図である。

[図3]本開示の決済処理システムの概要を説明する図である。

[図4]本開示の事前与信処理システムの構成例を説明する図である。

[図5]クライアント装置の構成例を説明する図である。

[図6]EC店舗サーバの構成例を説明する図である。

[図7]アクワイヤラサーバの構成例を説明する図である。

[図8]仲介サーバの構成例を説明する図である。

[図9]銀行サーバの構成例を説明する図である。

[図10]ウェアラブルデバイスの構成例を説明する図である。

[図11]図３の決済処理システムによる決済処理を説明するフローチャートである。

[図12]図４の事前与信処理システムによる登録処理を説明するフローチャートである。

[図13]登録処理における表示画像の表示例を説明する図である。

[図14]登録処理を説明する図である。

[図15]図４の事前与信処理システムによるコンテキスト情報アップロード処理を説明するフローチャートである。

[図16]コンテキスト情報アップロード処理を説明する図である。

[図17]図４の事前与信処理システムによる事前与信処理を説明するフローチャートである。

[図18]クライアント装置とウェアラブルデバイスが同一の居室にいる状態を説明する図である。

[図19]図４の事前与信処理システムによる事前与信処理を説明する図である。

[図20]リスクスコアと閾値に基づいたリスクスコア判定を説明する図である。

[図21]図４の事前与信処理システムによる事前与信処理における表示画像の表示例を説明する図である。

[図22]クライアント装置とウェアラブルデバイスとの相互の位置情報の取得方法のバリエーション（その１）を説明する図である。

[図23]クライアント装置とウェアラブルデバイスとの相互の位置情報の取得方法のバリエーション（その１）を説明する図である。

[図24]クライアント装置とウェアラブルデバイスとの相互の位置情報の取得方法のバリエーション（その２）を説明する図である。

[図25]クライアント装置とウェアラブルデバイスとがほぼ同一の位置であるか否かの判定方法のバリエーション（その１）を説明する図である。

[図26]クライアント装置とウェアラブルデバイスとがほぼ同一の位置であるか否かの判定方法のバリエーション（その２）を説明する図である。

[図27]図４の事前与信処理システムによるコンテキスト情報アップロード処理の変形例を説明するフローチャートである。

[図28]図２７のコンテキスト情報アップロード処理の変形例によるリスクスコアの変移例を説明する図である。

[図29]QRコード決済を説明する図である。

[図30]汎用のパーソナルコンピュータの構成例を説明する図である。

発明を実施するための形態

[0012] 以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0013] 以下、本技術を実施するための形態について説明する。説明は以下の順序で行う。

１．決済処理システムの概要

２．本開示の決済処理システムの構成例

３．本開示の事前与信処理システムの構成例

４．クライアント装置の構成例

５．EC店舗サーバの構成例

[0014] ＜＜１．決済処理システムの概要＞＞

本開示の決済処理システムの説明にあたり、まず、決済処理システムの概要について説明する。

[0015] 一般に、ユーザがクライアント装置（例えば、スマートフォンやPC（Personal Computer））を用いて、電子決済により商品を購入する場合、決済処理システムは、例えば、図１で示されるような構成とされる。

[0016] 図１の決済処理システム１は、クライアント装置１１、EC（電子商取引）店舗サーバ（Merchant）１２、アクワイヤラサーバ（Acquirer）１３、国際ブランド（Payment card brand）業者により管理運営される仲介サーバ１４

、および銀行サーバ（Issuer）１５より構成される。

[0017] クライアント装置１１は、スマートフォンや携帯型のPC（パーソナルコンピュータ）などであり、ユーザにより所持され、ブラウザアプリケーションプログラムなどによりEC店舗サーバ１２にアクセスし商品を選択して、決済処理を行うことで商品の購入を実現する。クライアント装置１１は、ユーザのクレジットカードのカード番号等の情報をEC店舗サーバ１２に送信することにより、決済処理を実行させる。

[0018] EC店舗サーバ（Merchant）１２は、対面決済における店舗に対応する加盟店（Merchant）により管理運営されるサーバであり、商品販売に必要とされるHP（HomePage）などをインターネット等のネットワークを介してクライアント装置１１等に提供する。また、EC店舗サーバ１２は、HP等を介して、クライアント装置１１により選択された商品の販売に際して、クレジットカードによる決済に必要とされる与信処理をアクワイヤラサーバ１３に依頼し、与信結果を取得する。この際、EC店舗サーバ１２は、与信処理に必要とされる情報として、クレジットカードのカード番号や商品の金額の情報を供給して、与信処理をアクワイヤラサーバ１３に依頼する。そして、EC店舗サーバ１２は、アクワイヤラサーバ１３からの与信結果を取得し、与信結果に基づいて商品の販売に係る決済処理を行う。

[0019] アクワイヤラサーバ（Acquirer）１３は、EC店舗サーバ１２に対してクレジットカードによる決済結果に応じた金額を支払うための金融機関である加盟店管理業者（Acquirer）により管理されるサーバである。アクワイヤラサーバ１３は、決済処理において、EC店舗サーバ１２より供給されるクレジットカードのカード番号や金額の情報を取得すると、取得したクレジットカード番号や金額の情報を仲介サーバ１４に供給して、与信処理を依頼し、与信結果を取得して、EC店舗サーバ１２に供給する。

[0020] 仲介サーバ１４は、VISA（登録商標）、Master（登録商標）、およびJCB（登録商標）等の国際ブランド（Payment card brand）を管理する業者により管理されるサーバであり、アクワイヤラサーバ１３と銀行サーバ１５との与

信処理に係る仲介処理を行う。すなわち、仲介サーバ１４は、アクワイヤラサーバ１３よりクレジットカードのカード番号や金額の与信に必要とされる情報を取得して、与信処理の依頼を受け付ける。また、仲介サーバ１４は、取得したカード番号や金額の与信に必要とされる情報を銀行サーバ１５に供給すると共に、与信結果を取得して、アクワイヤラサーバ１３に送信する。

[0021] 銀行サーバ１５は、クレジットカードの発行業者であり、クレジットカード利用者と契約して各種のサービスを提供する銀行により管理運営されるサーバであり、クレジットカードによる決済に係る与信処理を実行する。すなわち、銀行サーバ１５は、仲介サーバ１４より供給される決済に使用されるクレジットカードのカード番号や金額の情報に基づいて与信処理を実行して、与信結果を仲介サーバ１４に供給する。また、銀行サーバ１５は、与信が認められるときに決済される、商品購入に係る金額の情報を記録し、アクワイヤラサーバ１３により管理される口座に振り込む。

[0022] アクワイヤラサーバ１３は、銀行サーバ１５より振り込まれたクレジットカード決済された金額を、加盟店の口座に払い込む。

[0023] 以上のような図１の決済処理システム１による決済処理は以下のような処理となる。

[0024] まず、図１の処理Startで示されるように、クライアント装置１１により商品の購入処理がなされるとき、商品を購入するユーザのクレジットカードのカード番号の情報がEC店舗サーバ１２に供給される。

[0025] 処理Req1において、EC店舗サーバ１２は、クライアント装置１１からクレジットカードのカード番号の情報を取得すると、商品購入に係る金額の情報と共に、アクワイヤラサーバ１３に対して与信処理を依頼する情報を送信する。

[0026] 処理Req２において、アクワイヤラサーバ１３は、EC店舗サーバ１２からクレジットカードのカード番号と金額の情報を取得すると共に、与信処理を依頼する情報を取得すると、カード番号の情報と金額の情報と共に与信処理を依頼する情報を仲介サーバ１４に送信する。

[0027] 処理Req３において、仲介サーバ１４は、アクワイヤラサーバ１３からクレジットカードのカード番号と金額の情報を取得すると共に、与信処理を依頼する情報を取得すると、カード番号と金額の情報と共に、与信処理を依頼する情報を銀行サーバ１５に送信する。

[0028] 処理Resp１において、銀行サーバ１５は、仲介サーバ１４からクレジットカードのカード番号と金額の情報を取得すると、与信処理を実行し、与信結果を仲介サーバ１４に対して送信する。

[0029] 処理Resp２において、仲介サーバ１４は、銀行サーバ１５から与信結果を取得すると、アクワイヤラサーバ１３に対して送信する。

[0030] 処理Resp３において、アクワイヤラサーバ１３は、仲介サーバ１４から与信結果を取得すると、EC店舗サーバ１２に対して送信する。

[0031] 処理Endで示されるように、EC店舗サーバ１２は、与信結果に基づいて、決済処理を完了させて商品の販売処理を終了する。すなわち、与信結果に問題が無ければ、商品販売に係る料金の決済は完了し、与信結果に問題があれば、商品販売は成立しない。

[0032] 以上の処理により、決済処理が実現される。

[0033] ＜図１の決済処理システムにより実現される事前与信システム＞

しかしながら、この一連の処理は、クレジットカードの偽造やなりすましがなされていないことが前提とされる処理であり、現実には、クレジットカードの情報そのものの偽造やなりすまし対策が必要とされる。クレジットカードの情報そのものの偽造対策やなりすまし対策として、例えば、図１の決済処理システム１においては、上述した一連の決済処理の中に、さらに、事前与信処理がなされる。

[0034] 図２は、事前与信処理を実現するための事前与信処理システムの構成例が示されている。ただし、図２の事前与信処理システム１０は、図１におけるクライアント装置１１、EC店舗サーバ（Merchant）１２、仲介サーバ１４、および銀行サーバ（Issuer）１５より構成される。尚、図２において、アクワイヤラサーバ（Acquirer）１３が記載されているが、クライアント装置１

１から通常の決済処理に進む状況を示すために記載されている。また、アクワイヤラサーバ１３と銀行サーバ１５との間に設けられた決済ネットワーク２１は、図１の決済処理における仲介サーバ１４等である。

[0035] 図２の事前与信処理において、クライアント装置１１における機能は、図１における場合と同様である。

[0036] EC店舗サーバ１２は、図１における処理Req1で示される与信の依頼をする前のタイミングにおいて、クライアント装置１１より供給されるクレジットカードのカード番号と商品購入に係る金額の情報を、仲介サーバ１４を介して銀行サーバ１５に供給して、事前与信を要求し、事前与信結果を取得する。また、EC店舗サーバ１２は、事前与信結果が認められない場合、チャレンジフロー（Challenge Flow）と称される、クライアント装置１１に対して直接パスワードを入力させることによる認証処理や、生体情報を直ちに入力させるような認証処理を、仲介サーバ１４を介して銀行サーバ１５に要求する。このチャレンジフローの要求に応じて、銀行サーバ１５は、クライアント装置１１に対して、認証処理を実行させて、認証結果を取得し、チャレンジフローに係る事前与信結果を仲介サーバ１４を介してEC店舗サーバ１２に送信する。尚、事前与信結果に問題が無く、すなわち、チャレンジフローの必要がなく、そのまま決済処理を進めるフローを、フリクションレスフロー（Frictionless Flow）と称する。

[0037] 銀行サーバ１５は、EC店舗サーバ１２より供給されるクレジットカードのカード番号の情報と金額の情報に基づいて、偽造やなりすましに係るリスクに対するリスクスコアを算出する。

[0038] 銀行サーバ１５は、計算されたリスクスコアと所定の閾値との比較により、リスクスコアが所定の閾値より低く、クレジットカードのカード番号の偽造やなりすましがないものとみなしたとき、事前与信として問題が無いことを示す事前与信結果を、仲介サーバ１４を介してEC店舗サーバ１２に送信する。この場合、EC店舗サーバ１２は、図１のReq１を参照して説明した決済処理を進める。

[0039] 一方、銀行サーバ１５は、計算されたリスクスコアと所定の閾値との比較により、リスクスコアが所定の閾値より高く、クレジットカードのカード番号の偽造やなりすましの疑いがあるとみなしたとき、事前与信として問題があることを示す事前与信結果を、仲介サーバ１４を介してEC店舗サーバ１２に送信する。この場合、EC店舗サーバ１２は、事前与信結果を取得すると共に、仲介サーバ１４を介して、クライアント装置１１に対して認証処理を要求する処理であるチャレンジフローを銀行サーバ１５に対して要求する。

[0040] 銀行サーバ１５は、チャレンジフローの要求に応じて、クライアント装置１１に対してパスワードの認証処理を要求して、取得し、適切な認証結果であるか否かを判定し、仲介サーバ１４を介して、EC店舗サーバ１２に送信する。

[0041] このとき、チャレンジフローに基づいてなされた認証処理で取得された認証情報が適切である場合、リスクスコアが所定の閾値よりも高い場合と同様に、EC店舗サーバ１２は、図１の処理Req１で示されるように、決済処理を実行する。

[0042] これに対して、チャレンジフローに基づいた認証処理で取得された認証情報が適切ではない場合、EC店舗サーバ１２は、決済処理を中止する。

[0043] ここで、図２の事前与信システムにより事前与信処理について説明する。

[0044] 図２の処理Pre１において、クライアント装置１１は、決済処理に係るクレジットカードのカード番号と決済処理が求められる金額の情報をEC店舗サーバ１２に送信する。

[0045] 処理Pre２において、EC店舗サーバ１２は、仲介サーバ１４を介して、取得したカード番号の情報と金額の情報を併せて、銀行サーバ１５に対して事前与信処理を要求する。

[0046] 処理Pre３において、銀行サーバ１５は、取得したカード番号の情報と金額の情報に基づいてリスクスコアを算出し、リスクスコアと所定の閾値との比較により事前与信がOKであるか否かを判定し、判定結果に基づいて事前与信結果を、仲介サーバ１４を介して、EC店舗サーバ１２に送信する。

[0047] このとき、EC店舗サーバ１２は、事前与信結果がOKであり、クレジットカードのカード番号や使用限度額等に問題が無い場合、処理Req１により、決済処理を開始する。すなわち、この場合、フリクションレス処理が実現される。

[0048] また、事前与信結果がNGであり、クレジットカードのカード番号から偽造やなりすましである疑いがあった場合、処理Pre４において、EC店舗サーバ１２は、クライアント装置１１に対して、チャレンジフローにより、認証処理を要求する。

[0049] 処理Pre５において、クライアント装置１１は、EC店舗サーバ１２よりチャレンジフローによる認証処理が要求されたことを銀行サーバ１５に対して通知すると共に、チャレンジフローによる認証処理を銀行サーバ１５からクライアント装置１１に向けて要求するように通知する。

[0050] 処理Pre６において、銀行サーバ１５は、クライアント装置１１に対して、ユーザに対してパスワードの入力や生体情報による認証処理を要求する。これに応じて、クライアント装置１１は、入力されたパスワードや生体情報による認証結果を銀行サーバ１５に供給する。そして、銀行サーバ１５は、認証結果を取得すると共に、認証結果が正規のものであるか否かを判定する。

[0051] 処理Pre７において、銀行サーバ１５は、チャレンジフローにおける認証情報が正規のものであるか否かの判定結果を、仲介サーバ１４を介して、EC店舗サーバ１２に送信する。処理Pre８において、EC店舗サーバ１２は、チャレンジフローの認証結果を受信したことを通知する。

[0052] このとき、チャレンジフローにおける認証情報が正規のものである場合、処理Req１に進み、正規のものではない場合、決済処理は終了する。

[0053] 以上の事前与信処理により、クレジットカードの偽造やなりすましによるリスクスコアが求められて、リスクスコアが所定の閾値よりも低い場合にはフリクションレスフローとなり、そのまま決済処理が進められ、リスクスコアが所定の閾値よりも高い場合にはチャレンジフローがなされることで、認証処理がなされ、認証結果に応じて決済処理が進められる。

[0054] 結果として、クレジットカードの偽造やなりすましに対する対策がなされた状態で、決済処理を実現させることができるので、より適切な決済処理を実現することが可能となる。

[0055] しかしながら、正規のユーザが、正規のクレジットカードを使用して決済処理を実行する場合、何らかの原因でリスクスコアが高く求められると、正規のユーザは、正規のクレジットカードを使用しているにもかかわらず、チャレンジフローがなされることになる。

[0056] このような場合、正規のユーザが、正規のクレジットカードを利用する際のチャレンジフローにおける認証情報の入力処理は煩わしい処理となるので、事前与信処理において、チャレンジフローがなされないことが望ましい。

[0057] そこで、本開示においては、クレジットカードの偽造やなりすましに対しての対策を適切に実行しつつ、正規のユーザが、正規のクレジットカードを利用する際のチャレンジフローへと移行する頻度を極力低減できるようにすることで、セキュリティを維持しつつ、ユーザにとって快適な決済処理を実現させるものである。

[0058] ＜＜２．本開示の決済処理システムの構成例＞＞

次に、図３を参照して、本開示の決済処理システムの構成例について説明する。

[0059] 図３の決済処理システム３０は、クライアント装置３１、EC店舗サーバ（Merchant）３２、アクワイヤラサーバ（Acquirer）３３、仲介サーバ３４、銀行サーバ（Issuer）３５、およびウェアラブルデバイス３６より構成される。

[0060] 尚、クライアント装置３１、EC店舗サーバ（Merchant）３２、アクワイヤラサーバ（Acquirer）３３、および国際ブランド（Payment card brand）業者により管理運営される仲介サーバ３４は、基本的な機能において、それぞれ図１のクライアント装置１１、EC店舗サーバ（Merchant）１２、アクワイヤラサーバ（Acquirer）１３、および仲介サーバ１４とほぼ同一である。

[0061] また、図３の決済処理システム３０において、図１の決済処理システム１

と異なる点は、新たにウェアラブルデバイス３６が設けられている点である。

[0062] ウェアラブルデバイス３６は、クライアント装置３１を使用するユーザに装着されるものであり、ユーザの生体情報による認証処理を行うと共に、所定の時間間隔で位置情報を取得して、コンテキスト情報として銀行サーバ３５に送信する。ウェアラブルデバイス３６における認証処理で使用される生体情報は、指紋、静脈パターン、虹彩、および顔画像やそれらの組み合わせなど、ユーザを識別することが可能な生体情報であればいずれでもよい。ただし、以降においては、生体情報として指紋による認証処理がなされる例について説明を進める。

[0063] また、図３の決済処理システム３０の決済処理において、図１の決済処理システム１における決済処理と異なる点は、事前与信処理において、クレジットカードおよび金額の情報に加えて、クライアント装置３１の位置情報を用いる点である。

[0064] すなわち、ウェアラブルデバイス３６は、所定時間間隔で位置情報を銀行サーバ３５に送信する。銀行サーバ３５は、予めクレジットカードのカード番号と対応付けて、そのクレジットカードの利用者であるユーザが使用するウェアラブルデバイス３６と、決済処理に使用されるクライアント装置１１とを対応付けて記憶している。

[0065] また、銀行サーバ３５は、ウェアラブルデバイス３６から定期的に送信されてくる位置情報からなるコンテキスト情報を取得して記憶する。そして、銀行サーバ３５は、決済処理がなされるとき、決済処理が要求されたクライアント装置３１の位置情報と、最新のコンテキスト情報であるウェアラブルデバイス３６の位置情報とを比較し、一致する場合については、クライアント装置３１を利用して決済処理を要求するユーザが、ウェアラブルデバイス３６により生体情報により認証がなされた本人であるものとみなし、リスクスコアを低減させて、事前与信処理を行う。

[0066] この結果、正規のクレジットカードを用いた正規のユーザがクライアント

装置３１を用いた決済処理においては、クレジットカードの利用者が認証された正規のユーザであり、かつ、そのユーザが決済処理を行っていることでリスクスコアが低減されることで、チャレンジフローへと移行する頻度が低減されるので、チャレンジフローに伴った認証処理が不要となるので、セキュリティレベルを低減させることなく、煩わしい認証処理の頻度を低くし、快適な決済処理を実現することが可能となる。

[0067] 尚、事前与信処理についての詳細については、図４の本開示の事前与信処理システムを参照して後述する。

[0068] また、図３の決済処理システム３０における決済処理については、図１の決済処理システム１の決済処理と同一であるので、その説明は省略する。

[0069] ＜＜３．本開示の事前与信処理システムの構成例＞＞

次に、図４を参照して、本開示の事前与信処理システムの構成例について説明する。

[0070] 本開示の事前与信システム４０は、図１におけるクライアント装置３１、EC店舗サーバ（Merchant）３２、仲介サーバ３４、銀行サーバ（Issuer）３５、およびウェアラブルデバイス３６より構成される。

[0071] 尚、ここでも、クライアント装置３１、EC店舗サーバ（Merchant）３２、および仲介サーバ３４は、それぞれクライアント装置１１、EC店舗サーバ（Merchant）１２、および仲介サーバ１４とほぼ同一の機能を備えているので、その説明は適宜省略する。また、図４における処理Pre１１乃至Pre１８の処理については、基本的に図２の処理Pre１１乃至Pre８と同様である。

[0072] 銀行サーバ３５は、基本的な機能において、銀行サーバ１５とほぼ同一であるが、ウェアラブルデバイス３６より所定の時間間隔で、送信されてくるユーザの位置情報と生体情報による認証結果とをコンテキスト情報として取得し記憶する。

[0073] また、銀行サーバ３５は、事前与信処理において、クレジットカードのカード番号と金額の情報に加えて、クライアント装置３１の位置情報を取得すると、直近で取得したウェアラブルデバイス３６より供給されたコンテキス

ト情報に含まれる、位置情報との比較に基づいて、クライアント装置３１とウェアラブルデバイス３６のそれぞれの位置情報がほぼ一致し、かつ、生体情報による認証結果に問題が無い（認証処理において、取得した生体情報と予め登録された正規のユーザの生体情報とが一致する）とき、リスクスコアを所定値だけ低減させる。

[0074] すなわち、銀行サーバ３５は、クライアント装置３１とウェアラブルデバイス３６とのそれぞれの位置情報が一致し、かつ、予め登録した生体情報による認証結果に問題が無い場合、正規のユーザが正規のクレジットカードを用いた決済処理を要求しているものとみなせるので、通常の算出方法で求められるリスクスコアを低減させるようにする。

[0075] このような処理により、位置情報と生体情報により認証結果とを用いた事前与信処理により、クレジットカードの偽造やなりすましを対策しつつ、不要なチャレンジフローの発生を抑制することが可能となり、正規のユーザが正規のクレジットカードを用いる場合においては、不要な認証処理が要求されることがなく、より快適な決済処理を実現させることが可能となる。

[0076] ＜＜４．クライアント装置の構成例＞＞

次に、図５を参照して、クライアント装置３１の構成例について説明する。

[0077] クライアント装置３１は、決済処理により商品を購入するユーザにより使用される端末であり、例えば、スマートフォンやPCなどである。

[0078] より具体的には、クライアント装置３１は、制御部５１、通信部５２、記憶部５３、入力部５４、出力部５５、ドライブ５６、リムーバブル記憶媒体５７、およびGPS５９より構成され、それらが、相互にバス５８を介して電気的に接続された構成とされている。

[0079] 制御部５１は、プロセッサやメモリより構成されており、クライアント装置３１の動作の全体を制御する。

[0080] また、制御部５１は、決済処理部７１、チャレンジ処理部７２、および登録処理部７３を備えている。尚、決済処理部７１、チャレンジ処理部７２、

および登録処理部７３は、例えば、銀行サーバ３５より配信されるアプリケーションプログラムをインストールすることにより実現される機能である。

[0081] 決済処理部７１は、商品を購入する際の決済処理を実行し、GPS５９により取得されるクライアント装置３１の位置情報、および記憶部５３に記憶されているクレジットカードのカード番号の情報を、通信部５２を制御して、EC店舗サーバ１２に送信する。

[0082] チャレンジ処理部７２は、事前認証処理において、リスクスコアが高く、銀行サーバ３５より認証処理が要求されてきた場合、出力部５５を制御して、認証情報の入力を促す画像を表示したり、音声を出力すると共に、入力された認証情報による認証結果を、通信部５２を制御して、EC店舗サーバ１２に送信する。

[0083] 登録処理部７３は、登録処理を実行し、ユーザが装着するウェアラブルデバイス３６とカード番号とを銀行サーバ３５に対応付けて登録させて記憶させる。

[0084] 通信部５２は、制御部５１により制御され、有線（または無線（図示せず））により、LAN（Local Area Network）などに代表される通信ネットワークを介して、EC店舗サーバ３２やウェアラブルデバイス３６との間で各種のデータやプログラムを送受信する。

[0085] より具体的には、通信部５２は、WiFi通信部（WiFi）９１、LTE通信部（LTE）９２、Bluetooth通信部（Bluetooth）９３、およびNFC通信部（NFC）９４からなる各種の通信機能を備えており、EC店舗サーバ１２およびウェアラブルデバイス３６と通信する。尚、WiFi通信部（WiFi）９１、LTE通信部（LTE）９２、Bluetooth通信部（Bluetooth）９３、およびNFC通信部（NFC）９４は、そのいずれかが設けられていればよいものであり、または、この他の通信方式の通信部が含まれていてもよい。

[0086] WiFi通信部（WiFi）９１は、制御部５１により制御され、WiFiによる通信により他の装置とデータやプログラムを授受する。

[0087] LTE通信部（LTE）９２は、制御部５１により制御され、LTE（Long Term Ev

olution）による通信により他の装置とデータやプログラムを授受する。尚、LTEは、携帯電話通信技術の１つであり、携帯電話通信の他の通信方式であってもよい。

[0088] Bluetooth通信部（Bluetooth）９３は、制御部５１により制御され、Bluetooth（登録商標）による通信により他の装置とデータやプログラムを授受する。

[0089] NFC通信部（NFC）９３は、制御部５１により制御され、NFC（Near Field Communication）による通信により他の装置とデータやプログラムを授受する。

[0090] 記憶部５３は、制御部５１により制御され、HDD（Hard Disk Drive）、SSD（Solid State Drive）、または、半導体メモリなどからなり、各種のデータおよびプログラムを書き込む、または、読み出す。また、記憶部５３には、クレジットカードのカード番号の情報が記憶されている。

[0091] 入力部５４は、キーボードや操作ボタンなどから構成され、ユーザの操作入力を受け付ける。

[0092] 出力部５５は、画像を表示する例えば、LCD（Liquid Crystal Display）や有機EL（Electro Luminescence）などからなるディスプレイなどである表示部、音声を出力するスピーカなどからなる音声出力部を備えており、必要に応じて、画像や音声を出力する。

[0093] ドライブ５６は、磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体５７に対してデータを読み書きする。

[0094] GPS（Global Positioning System）５９は、図示せぬ複数の衛星からの信号を受信して、クライアント装置１１の位置情報を算出し、算出した位置情報を制御部５１に出力する。

[0095] ＜＜５．EC店舗サーバの構成例＞＞

次に、図６を参照して、EC店舗サーバ３２の構成例について説明する。

[0096] EC店舗サーバ３２は、決済処理により商品を販売する店舗により管理運営されるサーバであり、例えば、PCなどである。

[0097] より具体的には、EC店舗サーバ３２は、制御部１０１、通信部１０２、記憶部１０３、入力部１０４、出力部１０５、ドライブ１０６、およびリムーバブル記憶媒体１０７より構成され、それらが、相互にバス１０８を介して電気的に接続された構成とされている。

[0098] 制御部１０１は、プロセッサやメモリより構成されており、EC店舗サーバ３２の動作の全体を制御する。

[0099] また、制御部１０１は、事前与信処理部１２１、および決済処理部１２２を備えている。

[0100] 事前与信処理部１２１は、決済処理に際して、事前にクレジットカードの偽造やなりすましの対策処理である事前与信処理を実行する。より具体的には、事前与信処理部１２１は、仲介サーバ３４を介して、銀行サーバ３５に対して、クレジットカードのカード番号、および金額、並びに、決済処理を要求したクライアント装置３１の位置情報を供給して事前与信処理を要求する。

[0101] 事前与信処理部１２１は、事前与信がNGであった場合、チャレンジフローによりクライアント装置３１から認証結果を取得するように要求する。

[0102] 決済処理部１２２は、チャレンジフローによる認証結果に問題がない場合、クレジットカードのカード番号と金額の情報に基づいて、アクワイヤラサーバ３３に対して決済処理に関わる与信処理（処理Req１）を要求する。

[0103] 一方、チャレンジフローによる認証処理において、認証結果に問題がある場合については、決済処理が中止される。

[0104] 通信部１０２は、制御部１０１により制御され、有線（または無線（図示せず））により、LAN（Local Area Network）などに代表される通信ネットワークを介して、クライアント装置３１、アクワイヤラサーバ３３、および仲介サーバ３４との間で各種のデータやプログラムを送受信する。

[0105] 記憶部１０３は、制御部１０１により制御され、HDD（Hard Disk Drive）

、SSD（Solid State Drive）、または、半導体メモリなどからなり、各種のデータおよびプログラムを書き込む、または、読み出す。

[0106] 入力部１０４は、キーボードや操作ボタンなどから構成され、ユーザの操作入力を受け付ける。

[0107] 出力部１０５は、画像を表示する例えば、LCD（Liquid Crystal Display）や有機EL（Electro Luminescence）などからなるディスプレイなどである表示部、音声を出力するスピーカなどからなる音声出力部を備えており、必要に応じて、画像や音声を出力する。

[0108] ドライブ１０６は、磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体１０７に対してデータを読み書きする。

[0109] ＜＜６．アクワイヤラサーバの構成例＞＞

次に、図７を参照して、アクワイヤラサーバ３３の構成例について説明する。

[0110] アクワイヤラサーバ３３は、EC店舗サーバ１２に対してクレジットカードによる決済結果に応じた金額を支払うための金融機関である加盟店管理業者により管理されるサーバであり、例えば、PCなどである。

[0111] より具体的には、アクワイヤラサーバ３３は、制御部１４１、通信部１４２、記憶部１４３、入力部１４４、出力部１４５、ドライブ１４６、およびリムーバブル記憶媒体１４７より構成され、それらが、相互にバス１０８を介して電気的に接続された構成とされている。

[0112] 制御部１４１は、プロセッサやメモリより構成されており、アクワイヤラサーバ３３の動作の全体を制御する。

[0113] また、制御部１４１は、決済処理部１５１を備えている。

[0114] 決済処理部１５１は、事前与信処理において、フリクションレスフローである場合、または、チャレンジフローによる認証処理が認められた場合、ク

レジットカードのカード番号と金額の情報に基づいて、仲介サーバ３４に対して決済処理に関わる与信処理を要求する。

[0115] 通信部１４２は、制御部１４１により制御され、有線（または無線（図示せず））により、LAN（Local Area Network）などに代表される通信ネットワークを介して、EC店舗サーバ３２、および仲介サーバ３４との間で各種のデータやプログラムを送受信する。

[0116] 記憶部１４３は、制御部１４１により制御され、HDD（Hard Disk Drive）、SSD（Solid State Drive）、または、半導体メモリなどからなり、各種のデータおよびプログラムを書き込む、または、読み出す。

[0117] 入力部１４４は、キーボードや操作ボタンなどから構成され、ユーザの操作入力を受け付ける。

[0118] 出力部１４５は、画像を表示する例えば、LCD（Liquid Crystal Display）や有機EL（Electro Luminescence）などからなるディスプレイなどである表示部、音声を出力するスピーカなどからなる音声出力部を備えており、必要に応じて、画像や音声を出力する。

[0119] ドライブ１４６は、磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体１４７に対してデータを読み書きする。

[0120] ＜＜７．仲介サーバの構成例＞＞

次に、図８を参照して、仲介サーバ３４の構成例について説明する。

[0121] 仲介サーバ３４は、国際ブランド（Payment card brand）を管理する業者により管理運営されるサーバであり、決済処理においては、アクワイヤラサーバ１３と銀行サーバ１５との与信処理に係る仲介処理を実行し、事前与信処理においては、EC店舗サーバ３２と銀行サーバ１５との事前与信処理に係る仲介処理を実行する。

[0122] より具体的には、仲介サーバ３４は、制御部１６１、通信部１６２、記憶

部１６３、入力部１６４、出力部１６５、ドライブ１６６、およびリムーバブル記憶媒体１６７より構成され、それらが、相互にバス１６８を介して電気的に接続された構成とされている。

[0123] 制御部１６１は、プロセッサやメモリより構成されており、仲介サーバ３４の動作の全体を制御する。

[0124] また、制御部１６１は、事前与信仲介処理部１８１、および決済仲介処理部１８２を備えている。

[0125] 事前与信仲介処理部１８１は、事前与信処理において、EC店舗サーバ３２と銀行サーバ１５との事前与信処理に係る仲介処理を実行する。

[0126] 決済仲介処理部１８２は、決済処理において、アクワイヤラサーバ１３と銀行サーバ１５との与信処理に係る仲介処理を実行する。

[0127] 通信部１６２は、制御部１６１により制御され、有線（または無線（図示せず））により、LAN（Local Area Network）などに代表される通信ネットワークを介して、EC店舗サーバ３２、アクワイヤラサーバ３３、および銀行サーバ３５との間で各種のデータやプログラムを送受信する。

[0128] 記憶部１６３は、制御部１６１により制御され、HDD（Hard Disk Drive）、SSD（Solid State Drive）、または、半導体メモリなどからなり、各種のデータおよびプログラムを書き込む、または、読み出す。

[0129] 入力部１６４は、キーボードや操作ボタンなどから構成され、ユーザの操作入力を受け付ける。

[0130] 出力部１６５は、画像を表示する例えば、LCD（Liquid Crystal Display）や有機EL（Electro Luminescence）などからなるディスプレイなどである表示部、音声を出力するスピーカなどからなる音声出力部を備えており、必要に応じて、画像や音声を出力する。

[0131] ドライブ１６６は、磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体１６７に対してデータを読み書きする

。

[0132] ＜＜８．銀行サーバの構成例＞＞

次に、図９を参照して、銀行サーバ３５の構成例について説明する。

[0133] 銀行サーバ３５は、クレジットカードの発行業者であり、クレジットカード利用者と契約して各種のサービスを提供する銀行により管理運営されるサーバであり、クレジットカードによる決済に係る与信処理を実行する。

[0134] より具体的には、銀行サーバ３５は、制御部２０１、通信部２０２、記憶部２０３、入力部２０４、出力部２０５、ドライブ２０６、およびリムーバブル記憶媒体２０７より構成され、それらが、相互にバス２０８を介して電気的に接続された構成とされている。

[0135] 制御部２０１は、プロセッサやメモリより構成されており、銀行サーバ３５の動作の全体を制御する。

[0136] また、制御部２０１は、登録処理部２２１、コンテキスト受信処理部２２２、チャレンジ処理部２２３、リスクスコア判定部２２４、および決済処理部２２５を備えている。

[0137] 登録処理部２２１は、クライアント装置３１とウェアラブルデバイス３６とをクレジットカードのカード番号に対応付けて登録する登録処理を実行する。

[0138] コンテキスト受信処理部２２２は、登録したウェアラブルデバイス３６より所定の時間間隔で送信されてくる位置情報と生体情報とをコンテキスト情報として受信して、コンテキストDB２０３ａとして記憶部２０３に記憶させる。

[0139] チャレンジ処理部２２３は、リスクスコア判定部２２４によりリスクスコアが所定の閾値よりも大きく、チャレンジフローに移行する必要がある場合、クライアント装置３１に対して認証処理を要求して、認証結果を取得し、認証結果に問題があるか否かを判定する。

[0140] リスクスコア判定部２２４は、クレジットカードのカード番号、金額、およびクライアント装置３１の位置情報、並びに、直近のコンテキスト情報で

あるウェアラブルデバイス３６の位置情報に基づいてリスクスコアを算出する。そして、リスクスコア判定部２２４は、算出したリスクスコアと所定の閾値とを比較して、チャレンジフローとするか、または、フリクションレスフローとするかを判定する。

[0141] 決済処理部２２５は、決済処理において仲介サーバ３４を介して、アクワイヤラサーバ３３より供給されたクレジットカードのカード番号に基づいて、決済に係る与信処理を実行する。

[0142] 通信部２０２は、制御部２０１により制御され、有線（または無線（図示せず））により、LAN（Local Area Network）などに代表される通信ネットワークを介して、アクワイヤラサーバ３３、および仲介サーバ３４との間で各種のデータやプログラムを送受信する。

[0143] 記憶部２０３は、制御部２０１により制御され、HDD（Hard Disk Drive）、SSD（Solid State Drive）、または、半導体メモリなどからなり、各種のデータおよびプログラムを書き込む、または、読み出す。

[0144] 入力部２０４は、キーボードや操作ボタンなどから構成され、ユーザの操作入力を受け付ける。

[0145] 出力部２０５は、画像を表示する例えば、LCD（Liquid Crystal Display）や有機EL（Electro Luminescence）などからなるディスプレイなどである表示部、音声を出力するスピーカなどからなる音声出力部を備えており、必要に応じて、画像や音声を出力する。

[0146] ドライブ２０６は、磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体２０７に対してデータを読み書きする。

[0147] ＜＜９．ウェアラブルデバイスの構成例＞＞

次に、図１０を参照して、ウェアラブルデバイス３６の構成例について説明する。

[0148] ウェアラブルデバイス３６は、ユーザに装着されるものであり、生体情報として指紋を用いた認証処理を実行すると共に、所定の時間間隔で位置情報を取得して、コンテキスト情報として銀行サーバ３５に送信する。

[0149] より具体的には、ウェアラブルデバイス３６は、制御部２４１、通信部２４２、記憶部２４３、入力部２４４、出力部２４５、ドライブ２４６、リムーバブル記憶媒体２４７、GPS２４９、装着センサ２５０、および指紋センサ２５１より構成され、それらが、相互にバス２４８を介して電気的に接続された構成とされている。

[0150] 制御部２４１は、プロセッサやメモリより構成されており、ウェアラブルデバイス３６の動作の全体を制御する。

[0151] また、制御部２４１は、登録処理部２７１、コンテキスト送信処理部２７２、およびチャレンジ処理部２７３を備えている。

[0152] 登録処理部２７１は、登録処理を実行し、ウェアラブルデバイス３６とクライアント装置１１とをクレジットカードのカード番号と対応付けて銀行サーバ３５に登録して記憶させる。

[0153] コンテキスト送信処理部２７２は、ウェアラブルデバイス３６がユーザに装着されて、指紋センサ２５１により指紋からなる生体情報による認証処理がなされ、認証結果に問題がない場合、所定の時間間隔で、GPS２４９を制御して、位置情報を取得し、コンテキスト情報として通信部２４２を制御して銀行サーバ３５に送信する。また、コンテキスト送信処理部２７２は、装着センサ２５０を制御して、ウェアラブルデバイス３６の本体がユーザに対して装着されたタイミング、または、脱着されたタイミングを検出し、装着および脱着のタイミングにおいて、通信部２４２を制御して、銀行サーバ３５に装着および脱着が発生したことを通知する情報を送信する。

[0154] チャレンジ処理部２７３は、事前与信処理において、銀行サーバ３５からクライアント装置３１に対して認証処理が要求された場合、クライアント装置３１からの認証処理の要求に応じて、指紋センサ２５１を制御して、生体情報である指紋を用いた認証処理を実行し、認証結果をクライアント装置３

１に送信する。

[0155] 通信部２４２は、制御部２４１により制御され、有線（または無線（図示せず））により、LAN（Local Area Network）などに代表される通信ネットワークを介して、仲介サーバ３４や銀行サーバ３５との間で各種のデータやプログラムを送受信する。

[0156] より具体的には、通信部２４２は、WiFi２８１、LTE２８２、Bluetooth２８３、およびNFC２８４からなる各種の通信機能を備えており、クライアント装置３１および銀行サーバ３５と通信する。尚、WiFi通信部（WiFi）２８１、LTE通信部（LTE）２８２、Bluetooth通信部（Bluetooth）２８３、およびNFC通信部（NFC）２８４は、そのいずれかが設けられていればよいものであり、または、この他の通信方式の通信部が含まれていてもよい。

[0157] WiFi通信部（WiFi）２８１は、制御部２４１により制御され、WiFiによる通信により他の装置とデータやプログラムを授受する。

[0158] LTE通信部（LTE）２８２は、制御部２４１により制御され、LTE（Long Term Evolution）による通信により他の装置とデータやプログラムを授受する。尚、LTEは、携帯電話通信技術の１つであり、携帯電話通信の他の通信方式であってもよい。

[0159] Bluetooth通信部（Bluetooth）２８３は、制御部２４１により制御され、Bluetoothによる通信により他の装置とデータやプログラムを授受する。

[0160] NFC通信部（NFC）２８３は、制御部２４１により制御され、NFC（Near Field Communication）による通信により他の装置とデータやプログラムを授受する。

[0161] 記憶部２４３は、制御部２４１により制御され、HDD（Hard Disk Drive）、SSD（Solid State Drive）、または、半導体メモリなどからなり、各種のデータおよびプログラムを書き込む、または、読み出す。また、記憶部２４３には、予め指紋センサ２５１により読み取られた正規のユーザの指紋の情報が記憶されるようにしてもよい。

[0162] 入力部２４４は、キーボードや操作ボタンなどから構成され、ユーザの操

作入力を受け付ける。

[0163] 出力部２４５は、画像を表示する例えば、LCD（Liquid Crystal Display）や有機EL（Electro Luminescence）などからなるディスプレイなどである表示部、音声を出力するスピーカなどからなる音声出力部を備えており、必要に応じて、画像や音声を出力する。

[0164] ドライブ２４６は、磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体２４７に対してデータを読み書きする。

[0165] GPS（Global Positioning System）２４９は、図示せぬ複数の衛星からの信号を受信して、ウェアラブルデバイス３６の位置情報を算出し、算出した位置情報を制御部２４１に出力する。

[0166] 装着センサ２５０は、ウェアラブルデバイス３６がユーザにより装着されているか否かを検出し、検出結果を制御部２４１に出力する。

[0167] 指紋センサ２５１は、ウェアラブルデバイス３６のユーザの指紋を検出し、検出した指紋の情報と、記憶部２４３に記憶されている、予め登録されている正規のユーザの指紋の情報とを比較して、指紋による認証処理を実行し、認証結果を出力する。

[0168] ＜＜１０．図３の決済処理システムにおける決済処理＞＞

次に、図１１のフローチャートを参照して、図３の決済処理システムにおける決済処理について説明する。尚、以降の処理においては、クライアント装置３１をユーザが操作して所望とする購入を希望する商品を決定した後、購入に係る決済処理の操作をしていることが前提となる。

[0169] ステップＳ１１において、クライアント装置の制御部５１における決済処理部７１は、GPS５９を制御して、現在の位置情報を取得する。

[0170] ステップＳ１２において、決済処理部７１は、記憶部５３に記憶されているユーザが保有するクレジットカードのカード番号の情報を読み出すと共に

、クライアント装置３１の位置情報と併せて、通信部５２を制御して、EC店舗サーバ３２に送信し、決済を要求する。尚、ステップＳ１１，Ｓ１２の処理が、図３における処理Start（図４の処理Pre１１）に対応する処理となる。

[0171] ステップＳ３１において、EC店舗サーバ３２における制御部１０１の事前与信処理部１２１は、通信部１０２を制御して、送信されてきたカード番号、およびクライアント装置３１の位置情報を受信する。

[0172] ステップＳ３２において、事前与信処理部１２１は、仲介サーバ３４を介して銀行サーバ３５に対して、カード番号、購入に係る金額、およびクライアント装置３１の位置情報事前与信処理を実行し、ユーザのクレジットカードの事前与信結果に問題が無い場合、処理は、ステップＳ３３に進む。

[0173] 尚、事前与信結果に問題がある場合については、決済処理は不能とされ、処理が終了する。また、事前与信処理は、ステップＳ３２の処理に加えて、クライアント装置１１におけるステップＳ１３、仲介サーバ３４におけるステップＳ７１、および、銀行サーバ３５におけるステップＳ９１を含めた処理により実現される。さらに、事前与信処理については、図１６のフローチャートを参照して、詳細を後述する。

[0174] ステップＳ３３において、決済処理部１２２は、通信部１０２を制御して、カード番号、および、購入に係る金額の情報をアクワイヤラサーバ３３に送信し、与信処理を要求する。尚、ステップＳ３３の処理が、図３の処理Req１に対応する。

[0175] ステップＳ５１において、アクワイヤラサーバ３３の制御部１４１における決済処理部１５１は、通信部１４２を制御して、EC店舗サーバ３２からのカード番号と金額の情報を受信する。

[0176] ステップＳ５２において、決済処理部１５１は、通信部１４２を制御して、カード番号と金額の情報を仲介サーバ３４に送信し、与信処理を要求する。尚、ステップＳ５２の処理が、図３の処理Req１２に対応する。

[0177] ステップＳ７２において、仲介サーバ３４の制御部１６１における決済仲

介処理部１８２は、通信部１６２を制御して、カード番号と金額の情報を受信する。

[0178] ステップＳ７３において、決済仲介処理部１８２は、通信部１６２を制御して、カード番号と金額の情報を銀行サーバ３５に送信し、与信処理を要求する。尚、ステップＳ７３の処理が、図３の処理Req１３に対応する。

[0179] ステップＳ９２において、銀行サーバ３５の制御部２０１における決済処理部２２５は、通信部２０２を制御して、カード番号と金額の情報を受信する。

[0180] ステップＳ９３において、決済処理部２２５は、カード番号と金額の情報に基づいて、カード番号に対応付けて登録されているクレジットカードの与信判定を実行する。

[0181] ステップＳ９４において、決済処理部２２５は、通信部２０２を制御して、与信判定結果を仲介サーバ３４に送信する。尚、ステップＳ９４の処理が、図３の処理Resp１１の処理に対応する。

[0182] ステップＳ７４において、仲介サーバ３４の決済仲介処理部１８２は、通信部１６２を制御して、銀行サーバ３５からの与信判定結果を受信する。

[0183] ステップＳ７５において、決済仲介処理部１８２は、通信部１６２を制御して、アクワイヤラサーバ３３に与信判定結果を送信する。尚、ステップＳ７５の処理が、図３の処理Resp１２の処理に対応する。

[0184] ステップＳ５３において、アクワイヤラサーバ３３の決済処理部１５１は、通信部１４２を制御して、仲介サーバ３４からの与信判定結果を受信する。

[0185] ステップＳ５４において、決済処理部１５１は、通信部１４２を制御して、EC店舗サーバ３２に与信判定結果を送信する。尚、ステップＳ５４の処理が、図３の処理Resp１３の処理に対応する。

[0186] ステップＳ３４において、EC店舗サーバ３２の決済処理部１２２は、通信部１０２を制御して、アクワイヤラサーバ３３からの与信判定結果を受信する。

[0187] ステップＳ３５において、決済処理部１２２は、与信判定結果に基づいて、与信判定結果に問題がない場合、クライアント装置３１より購入処理がなされた料金の支払いを決済する。尚、ここでは決済判定結果に問題がある場合、決済処理がなされない。

[0188] ステップＳ３６において、決済処理部１２２は、通信部１０２を制御して、クライアント装置３１に決済結果を送信する。尚、ステップＳ３６の処理が、図３の処理Endに対応する。

[0189] ステップＳ１４において、クライアント装置３１の決済処理部７１は、通信部５２を制御して、EC店舗サーバ３２より送信されてくる決済結果を受信する。

[0190] ステップＳ１５において、決済処理部７１は、出力部５５のディスプレイに決済結果を表示する。

[0191] 以上の処理により、決済処理が実現される。

[0192] すなわち、図１１の決済処理においては、事前与信処理において、カード番号と金額に加えて、位置情報が用いられる点以外については、図１，図２を参照して説明した処理と基本的には同様である。

[0193] ＜＜１１．登録処理＞＞

次に、図１２のフローチャートを参照して、事前与信処理の前処理となる、クライアント装置３１を操作して商品を購入するユーザが生体情報を用いた認証処理に使用するウェアラブルデバイス３６を、銀行サーバ３５に登録する登録処理について説明する。尚、図１２を参照して説明する登録処理は、図４の処理Pre２１の処理に対応する。

[0194] ステップＳ１１１において、クライアント装置３１の制御部５１における登録処理部７３は、アプリケーションプログラムを起動させて、登録処理画像を生成し、出力部５５のディスプレイに表示させる。

[0195] ステップＳ１１２において、登録処理部７３は、選択可能な通信方式の選択画像を生成し、出力部５５のディスプレイに表示する。

[0196] ここで、表示される選択画像は、例えば、図１３の右上部で示されるよう

な表示画像Ｄ１である。表示画像Ｄ１においては、上から「XXX Bank　認証するデバイスと接続してください」と表記されており、この表示画像Ｄ１が、銀行サーバ３５を管理運営するXXX Bankのアプリケーションプログラムによるものであり、認証処理に必要とされるウェアラブルデバイス３６と通信するための通信方式を選択する画像が表示されている。また、その下には、上から選択可能な通信方式として「Bluetooth」と表示されたボタンＢ１と、「NFC」と表示されたボタンＢ２が表示されている。

[0197] クライアント装置３１においては、通信部５２の通信方式として、WiFi通信部９１、LTE通信部９２、Bluetooth通信部９３、およびNFC通信部９４が選択可能であるが、図１３においては、このうちのBluetooth通信部９３、およびNFC通信部９４が選択可能な通信方式として表示されている。したがって、さらに、WiFi通信部９１、およびLTE通信部９２を選択可能な通信方式として表示させてもよい。

[0198] 表示画像Ｄ１においては、選択可能な通信方式を選択するためのボタンＢ１，Ｂ２が設けられており、表記されている「Bluetooth」を選択する場合、ボタンＢ１が操作され、「NFC」を選択する場合、ボタンＢ２が選択される。

[0199] ステップＳ１１３において、登録処理部７３は、通信部５２を制御して、選択された通信方式により、選択可能なウェアラブルデバイスを検索するため、ポーリング信号を送信する。すなわち、図１３の場合、ボタンＢ１が操作されたとき、登録処理部７３が、Bluetooth通信部９３を制御して、ポーリング信号を送信する。また、図１３の場合、ボタンＢ２が操作されたとき、登録処理部７３が、NFC通信部９４を制御して、ポーリング信号を送信する。

[0200] ステップＳ１２１において、ウェアラブルデバイス３６の登録処理部２７１は、通信部２４２を制御して、送信されてくるポーリング信号を受信する。より詳細には、登録処理部２７１は、通信部２４２のWiFi通信部２８１、LTE通信部２８２、Bluetooth通信部２８３、およびNFC通信部２８４のそれぞれを制御して、ポーリング信号の有無を検出させ、ポーリング信号が検出された場合、送信されてきたポーリング信号を受信するように制御する。ここ

では、ステップＳ１１３の処理により、ボタンＢ１またはＢ２が操作されて、「Bluetooth」、または、「NFC」のいずれかのポーリング信号が受信される。

[0201] ステップＳ１２２において、登録処理部２７１は、通信部２４２のうち、ポーリング信号を受信した通信方式で、自らを識別する情報と共にポーリング信号の応答信号を送信させる。

[0202] ステップＳ１１４において、クライアント装置３１の登録処理部７３は、送信されてきたポーリング信号の応答信号と、送信元であるウェアラブルデバイス３６を識別する情報を受信し、受信したウェアラブルデバイス３６の情報に基づいて検索された認証用デバイスの選択画像を生成して出力部５５に表示させる。

[0203] すなわち、例えば、ステップＳ１１３の処理により、ボタンＢ１が押下されることにより、Bluetoothのポーリング信号が送信される場合、図１４で示されるように、クライアント装置３１の付近にBluetoothにより通信可能なウェアラブルデバイス３６－１，３６－２が存在するとき、クライアント装置３１には、ウェアラブルデバイス３６－１，３６－２のそれぞれからポーリング信号の応答信号と、それぞれのウェアラブルデバイス３６を識別する情報がクライアント装置３１に送信される。

[0204] これにより、クライアント装置３１は、図１３の右下部で示されるように、選択可能なウェアラブルデバイス３６の選択を促す表示画像Ｄ２を表示する。

[0205] 表示画像Ｄ２には、上から「XXX Bank　下記デバイスがBluetoothで検出されました。認証デバイスとして登録しますか？」と表示され、その下に、「ウェアラブルデバイス１」と表記されたボタンＢ１１と、「ウェアラブルデバイス２」と表記されたボタンＢ１２とが表示されている。

[0206] すなわち、通信方式がBluetoothのうち、クライアント装置３１の近傍に存在する、認証デバイスとして選択可能なウェアラブルデバイス３６－１，３６－２に対応するウェアラブルデバイス１，２が、それぞれボタンＢ１１，

Ｂ１２として表記され、ボタンＢ１１，Ｂ１２は、それぞれを選択するとき押下される。

[0207] 一方、例えば、図１３の右上部で示される表示画像Ｄ１のうち、ボタンＢ２が押下されて、通信方式としてNFCが選択された場合、例えば、図１３の左下部で示されるような表示画像Ｄ３が表示される。

[0208] 表示画像Ｄ３には、上から「XXX Bank　下記デバイスがNFCで検出されました。認証デバイスとして登録しますか？」と表示され、その下に、「ウェアラブルデバイス」と表記されたボタンＢ２１が表示されている。

[0209] すなわち、通信方式がNFCのうち、クライアント装置３１の近傍に存在する、認証デバイスとして選択可能なウェアラブルデバイス３６に対応するウェアラブルデバイス１が、ボタンＢ２１として表記され、ウェアラブルデバイス１に対応するウェアラブルデバイス３６が選択されるとき押下される。

[0210] ステップＳ１１５において、登録処理部７３は、表示画像Ｄ２またはＤ３に基づいて、認証デバイスとしてボタンＢ１１，Ｂ１２のいずれか、または、ボタンＢ２１が押下されることにより、選択された認証用デバイスであるウェアラブルデバイス３６の情報と共に、カード番号、および、自らであるクライアント装置３１を特定する情報を、通信部５２を制御して、銀行サーバ３５に送信させる。

[0211] ステップＳ１３１において、銀行サーバ３５の登録処理部２２１は、通信部２０２を制御して、クライアント装置３１より送信されてくる認証用デバイスとして選択されたウェアラブルデバイス３６の情報に加えて、カード番号、およびクライアント装置３１を識別する情報を受信する。

[0212] ステップＳ１３２において、登録処理部２２１は、クライアント装置３１より送信されてくる認証用デバイスとして選択されたウェアラブルデバイス３６の情報に加えて、カード番号、およびクライアント装置３１を識別する情報を対応付けてコンテキストDB２０３ａとして記憶部２０３に記憶させる。

[0213] 以上の処理により、図１４で示されるように、クレジットカードのカード

番号の情報に対応付けて、ユーザが商品の購入に使用するクライアント装置３１、および認証用デバイスとしてのウェアラブルデバイス３６がコンテキストＤＢ２０３ａに登録される。

[0214] これにより、後述するコンテキスト情報アップロード処理において、ウェアラブルデバイス３６より供給されてくるコンテキスト情報が、コンテキスト情報を送信してくるウェアラブルデバイス３６に対応付けて登録されているクレジットカードのカード番号に対応付けてコンテキストＤＢ２０３ａに蓄積される。

[0215] ＜＜１２．コンテキスト情報アップロード処理＞＞

次に、図１５のフローチャートを参照して、コンテキスト情報アップロード処理について説明する。尚、図１５を参照して説明するコンテキスト情報アップロード処理は、図４の処理Pre２２の処理に対応する。

[0216] ステップＳ１５１において、ウェアラブルデバイス３６の制御部２４１におけるコンテキスト送信処理部２７２は、装着センサ２５０を制御して、装着が検出されたか否かを判定する。

[0217] ステップＳ１５１において、ユーザがウェアラブルデバイス３６を装着することにより、装着センサ２５０により装着が検出されると、処理は、ステップＳ１５２に進む。

[0218] ステップＳ１５２において、コンテキスト送信処理部２７２は、出力部２４５のディスプレイに表示画像を表示したり、スピーカから音声を出力するなどして、生体情報の認証処理を要求する。ここでは、生体情報は、指紋センサ２５１により認証される指紋を用いる例で説明を進めるものとするが、生体情報であれば、指紋以外の生体情報であってもよく、顔認証、虹彩認証、または静脈認証などであってもよい。

[0219] ステップＳ１５３において、コンテキスト送信処理部２７２は、指紋センサ２５１を制御して、生体情報としてのユーザの指紋が提示され、予め登録された正規のユーザの指紋との比較により、認証が認められるか否かを判定する。ステップＳ１５３において、生体情報としての指紋による認証が認め

られる場合、処理は、ステップＳ１５４に進む。

[0220] ステップＳ１５４において、コンテキスト送信処理部２７２は、所定時間Ｔが経過したか否かを判定し、所定時間Ｔが経過するまで、同様の処理を繰り返す。そして、ステップＳ１５４において、所定時間Ｔが経過したとみなされた場合、処理は、ステップＳ１５５に進む。

[0221] ステップＳ１５５において、コンテキスト送信処理部２７２は、GPS２４９を制御して、ウェアラブルデバイス３６の現在の位置情報を取得する。

[0222] ステップＳ１５６において、コンテキスト送信処理部２７２は、通信部２４２を制御して、銀行サーバ３５に対して、取得した現在の位置情報をコンテキスト情報としてアップロードさせる。この際、コンテキスト送信処理部２７２は、コンテキスト情報である位置情報と併せて、生体情報を用いた認証処理による認証結果が認められていることを示す情報や、ウェアラブルデバイス３６を識別する情報もアップロードさせる。尚、ステップＳ１５６の処理が、図４における処理Pre２２に対応する。

[0223] ステップＳ１５７において、コンテキスト送信処理部２７２は、コンテキスト情報アップロード処理の終了が指示されたか否かを判定し、終了が指示された場合、処理は、終了する。また、ステップＳ１５７において、処理の終了が指示されない場合、処理は、ステップＳ１５８に進む。

[0224] ステップＳ１５８において、コンテキスト送信処理部２７２は、装着センサ２５０を制御して、ウェアラブルデバイス３６が脱着されたか否かを判定する。ステップＳ１５８において、ウェアラブルデバイス３６の脱着が検出されない場合、処理は、ステップＳ１５４に戻る。

[0225] また、ステップＳ１５８において、例えば、ユーザによりウェアラブルデバイス３６が外された場合、装着センサ２５０によりウェアラブルデバイス３６の脱着が検出されて、処理は、ステップＳ１５９に進む。

[0226] ステップＳ１５９において、コンテキスト送信処理部２７２は、通信部２４２を制御して、ウェアラブルデバイス３６が脱着されたことを銀行サーバ３５に通知し、処理は、ステップＳ１５１に戻る。

[0227] 一方、ステップＳ１５１において、ウェアラブルデバイス３６の装着が検出されない場合、または、ステップＳ１５３において、生体情報である指紋を用いた認証処理により認証が認められない場合、処理は、ステップＳ１６０に進み、処理の終了が指示されているか否かが判定される。そして、ステップＳ１６０において、処理の終了が指示されていない場合、処理は、ステップＳ１５１に戻り、同様の処理が繰り返され、ステップＳ１６０において、処理の終了が指示されている場合、処理は、終了する。

[0228] すなわち、上述したウェアラブルデバイス３６によるコンテキスト情報アップロード処理により、ウェアラブルデバイス３６の装着が検出された後、生体情報を用いた認証処理が認められると、脱着が確認されるまで、所定時間Ｔの間隔で位置情報が検出されて、生体情報の認証結果と共に、銀行サーバ３５に送信される処理が繰り返される。そして、ウェアラブルデバイス３６の脱着が検出されると、脱着が銀行サーバ３５に通知されて、ウェアラブルデバイス３６が装着されて、生体情報が認証されるまでは、位置情報は銀行サーバ３５には通知されない。

[0229] 一方、銀行サーバ３５によるコンテキスト情報アップロード処理は、図１５の右部のフローチャートで示される処理となる。

[0230] すなわち、ステップＳ１７１において、銀行サーバ３５の制御部２０１におけるコンテキスト受信処理部２２２は、リスクスコアを、チャレンジフローが必要な値に設定し、記憶部２０３に記憶させる。

[0231] そして、ステップＳ１７２において、コンテキスト受信処理部２２２は、通信部２０２を制御して、ウェアラブルデバイス３６からコンテキスト情報である位置情報が送信されてきたか否かを判定する。

[0232] ステップＳ１７２において、コンテキスト情報が送信されてきた場合、処理は、ステップＳ１７３に進む。

[0233] ステップＳ１７３において、コンテキスト受信処理部２２２は、送信されてきたコンテキスト情報である位置情報を、送信してきたウェアラブルデバイス３６を識別する情報に対応付けられたカード番号に対応付けて、コンテ

キストＤＢ２０３ａに記憶させる。

[0234] ステップＳ１７４において、コンテキスト受信処理部２２２は、コンテキスト情報を送信してきたウェアラブルデバイス３６に対応付けられて登録されているクライアント装置３１のユーザが使用するクレジットカードのカード番号で特定されるクレジットカードのリスクスコアを所定値Ａだけ減算して、リスクスコアを低減させる。

[0235] すなわち、コンテキスト情報を送信してきたウェアラブルデバイス３６の利用者であるユーザが使用するクレジットカードのリスクスコアは、低減されることになるので、後述する事前与信処理において、リスクスコアが高く、ユーザに対して認証処理が要求されるチャレンジフローへの移行頻度を低減させ、フリクションレスフローへと移行する頻度を高めることが可能となる。

[0236] 尚、ステップＳ１７２において、コンテキスト情報が送信されてこない場合、ステップＳ１７３，Ｓ１７４の処理はスキップされる。

[0237] ステップＳ１７５において、コンテキスト受信処理部２２２は、時間をカウントするカウンタ（図示せず）に基づいて、所定時間ｔだけ時間が経過したか否かを判定し、所定時間ｔだけ時間が経過している場合、処理は、ステップＳ１７６に進む。

[0238] ステップＳ１７６において、コンテキスト受信処理部２２２は、リスクスコアを所定値ａだけ加算し、経過時間をカウントするカウンタをリセットする。

[0239] 尚、ステップＳ１７５において、所定時間ｔが経過していない場合、ステップＳ１７６の処理はスキップされる。

[0240] すなわち、リスクスコアは、所定時間ｔの間隔で所定値ａだけ徐々に高くなる。すなわち、リスクスコアは、コンテキスト情報が受信されたタイミングにおいて、所定値Ａだけ小さくされるが、時間の経過に伴って徐々に高くなっていく。従って、コンテキスト情報が受信されたタイミングにおいて、リスクスコアは低減されることで、チャレンジフローへと移行する頻度が低

下するが、その後、時間の経過に伴ってリスクスコアは増大することになるので、徐々にチャレンジフローへと移行する頻度が高くなる。

[0241] ステップＳ１７７において、コンテキスト受信処理部２２２は、通信部２０２を制御して、ウェアラブルデバイス３６より脱着が検出されたことを示す通知が送信されてきたか否かを判定する。ステップＳ１７７において、脱着が検出されたことを示す通知が送信されてきた場合、処理は、ステップＳ１７８に進む。

[0242] ステップＳ１７８において、コンテキスト受信処理部２２２は、リスクスコアをチャレンジフローが必要な値に設定する。

[0243] 尚、ステップＳ１７７において、脱着が検出されたことを示す通知が送信されてこない場合、ステップＳ１７８の処理はスキップされる。

[0244] ステップＳ１７９において、コンテキスト受信処理部２２２は、処理の終了が指示されたか否かを判定し、処理の終了が指示されていない場合、処理は、ステップＳ１７２に戻り、それ以降の処理が繰り返される。

[0245] そして、ステップＳ１７９において、処理の終了が指示された場合、処理は、終了する。

[0246] すなわち、脱着が検出されたことを示す通知が送信されてきた場合、ウェアラブルデバイス３６を装着したユーザの位置情報が取得できない状態となるので、クライアント装置３１の位置情報との比較により、なりすましの有無を判断することができないので、リスクスコアに基づいた判定処理において、常に、チャレンジフローが選択されるように高い値に設定される。

[0247] 以上の処理により、例えば、図１６で示されるように、ユーザが生体情報による認証が認められた状態でウェアラブルデバイス３６を装着している限り、ウェアラブルデバイス３６から所定の時間間隔で、ウェアラブルデバイス３６の位置情報からなるコンテキスト情報が所定の時間間隔で銀行サーバ３５に送信されることになる。

[0248] 図１６においては、上段が、ウェアラブルデバイス３６よりコンテキスト情報が送信されるタイミングを示しており、下段が銀行サーバ３５において

、コンテキスト情報が受信されるタイミングが示されている。

[0249] すなわち、図１６においては、時刻ｔ１１，ｔ１２，１３・・・ｔ１６において、ウェアラブルデバイス３６から銀行サーバ３５にコンテキスト情報が送信されており、各タイミングにおいて、リスクスコアが所定値Ａだけ低減される処理が繰り返される。また、リスクスコアは、時間の経過に伴って所定時間ｔの時間間隔で所定値ａだけ増大する。

[0250] ここで、時刻ｔ１１，ｔ１２，１３・・・ｔ１６は、等時間間隔である。また、直近のタイミングである時刻ｔ１６においては、位置Ｎの位置情報がコンテキスト情報として送信されている。さらに、その前のタイミングである、時刻ｔ１５においては、位置Ｎ－１の位置情報がコンテキスト情報として送信されている。さらにまた、その前のタイミングである、時刻ｔ１４においては、位置Ｎ－２の位置情報がコンテキスト情報として送信されている。

[0251] 以上の処理により、コンテキスト情報が送信される度にリスクスコアが低減されつつも、時間の経過に伴ってリスクスコアが高くされることにより、ウェアラブルデバイス３６を装着したユーザの位置情報が最新であるほど、なりすましに対する信頼性を高くすることができ、後述する事前与信処理においてチャレンジフローが選択される頻度を下げることが可能となる。また、コンテキスト情報が送信されない状態が長く続いたり、ウェアラブルデバイス３６が装着されていない状態になるとリスクスコアを高くして、チャレンジフローが選択され易くなることで、なりすましのリスクを回避することが可能となる。

[0252] ＜＜１３．図３の決済処理システムによる事前与信処理＞＞

次に、図１７のフローチャートを参照して、図３の決済処理システムによる事前与信処理について説明する。

[0253] ステップＳ２０１において、EC店舗サーバ３２の制御部１０１における事前与信処理部１２１は、通信部１０２を制御して、カード番号、およびクライアント装置３１の位置情報を、仲介サーバ１４に対して送信し、銀行サー

バ１５に対して事前与信を要求する。尚、ステップＳ２０１の処理は、図４における処理Pre１２に対応する。

[0254] ステップＳ２２１において、仲介サーバ１４の制御部１６１の事前与信仲介処理部１８１は、通信部１６２を制御して、カード番号、およびクライアント装置３１の位置情報と共に、事前与信の要求を受信する。

[0255] ステップＳ２２２において、事前与信仲介処理部１８１は、通信部１６２を制御して、カード番号、決済処理に係る金額、およびクライアント装置３１の位置情報と共に、事前与信の要求を銀行サーバ３５に送信する。尚、ステップＳ２２２の処理は、図４における処理Pre１２に対応する。

[0256] ステップＳ２４１において、銀行サーバ３５の制御部２０１におけるリスクスコア判定部２２４は、通信部２０２を制御して、仲介サーバ３４を介して、EC店舗サーバ３２より送信されてきたカード番号、金額、およびクライアント装置３１の位置情報を受信する。

[0257] ステップＳ２４２において、リスクスコア判定部２２４は、コンテキストDB２０３ａにアクセスし、最新のコンテキスト情報として登録されている、クレジットカードのカード番号に対応付けて登録されているウェアラブルデバイス３６の位置情報とクライアント装置３１の位置情報とが一致するか否かを判定する。

[0258] 例えば、図１８で示されるように、クライアント装置３１とウェアラブルデバイス３６とが同一の位置（同一の居室）Ｈに存在するような場合、クレジットカードのカード番号に対応付けて登録されているウェアラブルデバイス３６の位置情報とクライアント装置３１の位置情報とが一致することになり、ウェアラブルデバイス３６を装着したユーザが、クライアント装置３１を使用しているものと認識することができる。

[0259] また、ウェアラブルデバイス３６の位置情報であるコンテキスト情報は、図１９で示されるように、所定の時間間隔でウェアラブルデバイス３６から銀行サーバ３５に供給されている。このため、例えば、時刻ｔ２１のタイミングにおいて、EC店舗サーバ３２が決済処理を開始して、事前与信を要求す

るような場合、図１９の時刻ｔ１６における最新のコンテキスト情報における位置Ｎの位置情報が取得されたタイミングである時刻ｔ１６との差分である時間αは、図１５のフローチャートを参照して説明したコンテキスト情報アップロード処理における所定時間Ｔよりも短い時間となる。

[0260] 従って、時刻ｔ１６において、ウェアラブルデバイス３６の位置情報と、クライアント装置１１の位置情報とが一致している場合、所定時間Ｔが、例えば、30秒程度であれば、時刻ｔ２１において決済がなされるタイミングにおいてもほぼ同一の位置であるとみなすことができる。

[0261] これらのことから、カード番号により特定されるクレジットカードの利用に際して、ユーザのなりすましはないとみなすことが可能となる。

[0262] 尚、図１９においては、中段および下段においては、図１６におけるコンテキスト情報が、ウェアラブルデバイス３６から銀行サーバ３５に送信されるタイミングを示しており、上段においては、EC店舗サーバ３２による決済処理が開始されるタイミングが示されている。

[0263] また、ウェアラブルデバイス３６の位置情報については、直近のコンテキスト情報における位置情報のみを用いるのみならず、例えば、直近の複数のコンテキスト情報の位置情報における平均値をウェアラブルデバイス３６の位置情報として用いるようにしてもよい。このようにすることで、ゆらぎや誤差を修正することが可能となる。

[0264] ステップＳ２４２において、コンテキストDB２０３ａにアクセスし、クライアント装置３１の位置情報と、クレジットカードのカード番号に対応付けて登録されているウェアラブルデバイス３６の位置情報とが一致すると判定された場合、クレジットカードの利用者がクライアント装置３１を使用しており、なりすましはないものとみなして処理は、ステップＳ２４３に進む。

[0265] ステップＳ２４３において、リスクスコア判定部２２４は、コンテキストDB２０３ａにアクセスし、クレジットカードのカード番号に対応付けて登録されているリスクスコアが所定の閾値よりも低いか否か、すなわち、チャレンジフローによる認証が必要であるか否かを判定する。

[0266] 例えば、時系列のリスクスコアが、図２０の実線で示されるように変移し、閾値ｔｈが点線で示されるように設定される場合、時刻ｔ１０１においては、リスクスコアが、閾値ｔｈよりも高くなるため、リスクスコア判定部２２４は、チャレンジフローによる認証が必要であるとみなす。

[0267] 一方、図２０の場合、時刻ｔ１０２においては、リスクスコアが、閾値ｔｈよりも低くなるため、リスクスコア判定部２２４は、チャレンジフローによる認証が不要であるとみなし、フリクションレスフローを選択する。

[0268] ステップＳ２４３において、例えば、図２０の時刻ｔ１０２で示されるように、リスクスコアが所定の閾値よりも低く、事前与信に問題が無くフリクションレスフローによる処理でよいとみなされる場合、処理は、ステップＳ２４４に進む。

[0269] ステップＳ２４４において、リスクスコア判定部２２４は、通信部１６２を制御して、事前与信に問題が無いことを示す情報を、事前与信結果として仲介サーバ３４に送信させる。尚、ステップＳ２４４の処理は、図４における処理Pre１３に対応する。

[0270] 一方、ステップＳ２４２において、コンテキストDB２０３ａにアクセスし、クライアント装置３１の位置情報と、クレジットカードのカード番号に対応付けて登録されているウェアラブルデバイス３６の位置情報とが一致しないとみなされた場合、または、リスクスコアが所定の閾値よりも高く、事前与信に問題がありチャレンジフローによる処理が必要であるとみなされる場合、処理は、ステップＳ２４５に進む。

[0271] ステップＳ２４５において、リスクスコア判定部２２４は、チャレンジ処理部２２３に対してチャレンジフローによる認証情報の取得を要求する。チャレンジ処理部２２３は、通信部２０２を制御して、クライアント装置３１に対して認証情報を要求する。

[0272] 尚、ステップＳ２４５の処理は、図４における処理Pre１５，１６に対応する。厳密な処理としては、チャレンジフローが必要となる場合、図４においては、処理Pre１３により事前与信が認められず、チャレンジフローが必要と

なったことがEC店舗サーバ３２に通知される。そして、処理Pre１４によりEC店舗サーバ３２からクライアント装置３１に対してチャレンジフローを要求する情報が送信され、さらに、クライアント装置３１から銀行サーバ３５へとチャレンジフローが要求される。この一連の処理により、処理Pre１５，１６のチャレンジフローへと移行し、銀行サーバ３５のチャレンジ処理部２２３が、通信部２０２を制御して、クライアント装置３１に対してチャレンジフローに必要な認証情報を要求することになるが、図１７のフローチャートにおいては省略している。

[0273] ステップＳ２６１において、クライアント装置３１の制御部５１におけるチャレンジ処理部７２は、通信部５２を制御して、認証情報の要求があったか否か、すなわち、チャレンジフローであったか否かを判定し、認証情報の要求があった場合、すなわち、チャレンジフローである場合、処理は、ステップＳ２６２に進む。

[0274] ステップＳ２６２において、チャレンジ処理部７２は、通信部５２を制御して、認証情報の要求を受信する。

[0275] ステップＳ２６３において、チャレンジ処理部７２は、通信部５２を制御して、認証用デバイスとして登録しているウェアラブルデバイス３６に対して認証情報の入力を要求する情報を送信すると共に、出力部５５を制御して、ウェアラブルデバイス３６の指紋センサ２５１に対して認証情報である指紋の入力を促すような情報を画像や音声により提示する。

[0276] ステップＳ２８１において、ウェアラブルデバイス３６の制御部２４１におけるチャレンジ処理部２７３は、通信部２４２を制御して、認証用デバイスとして登録しているウェアラブルデバイス３６に対して認証情報の入力を要求する情報を受信する。

[0277] ステップＳ２８２において、チャレンジ処理部２７３は、出力部２４５を制御して、ユーザに対して指紋による認証を要求する画像や音声をディスプレイやスピーカから出力し、指紋センサ２５１を制御して、ユーザの指紋による生体情報の入力を受け付ける。

[0278] ステップＳ２８３において、チャレンジ処理部２７３は、指紋センサ２５１により入力された生体情報である指紋情報と、予め登録されている正規のユーザの指紋情報とを比較し、認証処理を実行する。

[0279] ステップＳ２８４において、チャレンジ処理部２７３は、通信部２４２を制御して、認証結果を認証情報としてクライアント装置３１に送信する。

[0280] ステップＳ２６４において、クライアント装置３１の制御部５１におけるチャレンジ処理部７２は、通信部５２を制御して、認証情報を取得する。

[0281] ステップＳ２６５において、チャレンジ処理部７２は、通信部５２を制御して、ウェアラブルデバイス３６より取得した認証情報を銀行サーバ３５に送信する。

[0282] 尚、ステップＳ２６１において、認証情報の要求がなく、チャレンジフローではない場合、ステップＳ２６２乃至Ｓ２６５の処理はスキップされる。

[0283] ステップＳ２４６において、銀行サーバ３５の制御部２０１におけるチャレンジ処理部２２３は、通信部２０２を制御して、認証情報を取得し、リスクスコア判定部２２４に供給する。

[0284] ステップＳ２４７において、リスクスコア判定部２２４は、認証情報における認証結果はＯＫである（生体情報による認証が認められた）か否か、すなわち、入力された生体情報である指紋が、予め登録されている正規の指紋の情報と一致するか否かを判定する。

[0285] ステップＳ２４７において、認証情報がＯＫである場合、処理は、ステップＳ２４４に進む。

[0286] また、ステップＳ２４７において、認証情報がＯＫではない場合、処理は、ステップＳ２４８に進む。

[0287] ステップＳ２４８において、リスクスコア判定部２２４は、通信部２０２を制御して、事前与信がＮＧであること（事前与信が認められないこと）を示す事前与信結果を仲介サーバ３４に送信させる。尚、ステップＳ２４８の処理は、図４における処理Pre１７に対応する。

[0288] ステップＳ２２３において、仲介サーバ３４の制御部１６１の事前与信仲

介処理部１８１は、通信部１６２を制御して、銀行サーバ３５からの事前与信結果を受信する。

[0289] ステップＳ２２４において、仲介サーバ３４の制御部１６１の事前与信仲介処理部１８１は、通信部１６２を制御して、事前与信結果をEC店舗サーバ３２に送信する。

[0290] ステップＳ２０２において、EC店舗サーバ３２の制御部１０１における事前与信処理部１２１は、通信部１０２を制御して、仲介サーバ３４を介して送信されてくる事前与信結果を受信する。

[0291] ステップＳ２０３において、事前与信処理部１２１は、通信部１０２を制御して、事前与信結果をクライアント装置３１に送信する。

[0292] ステップＳ２６６において、クライアント装置３１の制御部５１における決済処理部７１は、通信部５２を制御して、事前与信結果を受信して、出力部５５を制御して、事前与信結果を画像および音声などにより提示する。

[0293] 例えば、図２１の左部で示されるように、クライアント装置３１において、上段に「XXX Shop　カート・USB充電器・USBケーブル、合計¥1080-」と表示され、下段に決済を要求するとき押下される「お支払い」と表記されたボタンＢ５１が表示されている表示画像Ｄ２１が表示される場合について考える。

[0294] 図２１の表示画像Ｄ２１におけるボタンＢ５１が押下されることにより、図１１を参照して説明した決済処理は開始されることになる。

[0295] 図２１の場合、図１１のステップＳ３２に対応する事前与信処理がなされることにより、EC店舗であるXXX Shopにおいて、カートの中にUSB充電器とUSBケーブルとが入れられており、合計が1080円の決済処理がなされる。

[0296] このとき、事前与信処理において、事前与信結果がＯＫである場合、ステップＳ２６６の処理により、例えば、図２１の中央左上部で示されるように、上から「XXX BANK　認証デバイスにより認証されました」といったコメントと、「OK」と表記されたボタンＢ５２から構成される表示画像Ｄ２２が表示され、事前与信結果がＯＫであったことが表示される。尚、表示画像Ｄ２

２の表示は、ボタンＢ５２が押下されることにより終了する。

[0297] 一方、事前与信処理において、リスクスコアが閾値よりも高く、チャレンジフローによる認証情報が必要な場合、例えば、ステップＳ２６３の処理により、図２１の中央左下部で示されるように認証情報である指紋の入力を促す表示画像Ｄ２３が表示される。

[0298] 表示画像Ｄ２３においては、上から「XXX Bank　認証デバイスにより再度認証を行ってください」といったコメントと、「OK」と表記されたボタンＢ５２から構成される。尚、表示画像Ｄ２３の表示は、ボタンＢ５３が押下されることにより終了する。

[0299] この表示画像Ｄ２３の示唆に従って、図２１の中央右下部で示されるようにユーザの指Ｆがウェアラブルデバイス３６の指紋センサ２５１にかざされることで指紋が検出され、さらに、検出された指紋が予め登録されている正規のユーザの指紋と一致すると、図２１の中央右部で示されるような事前与信結果がＯＫであることを示す表示画像Ｄ２４が、クライアント装置３１において表示される。

[0300] 表示画像Ｄ２４は、図２１の中央右部で示されるように、上から「XXX BANK　認証デバイスにより認証されました」といったコメントと、「OK」と表記されたボタンＢ５４から構成される。尚、表示画像Ｄ２４の表示は、ボタンＢ５４が押下されることにより終了する。

[0301] そして、図１１のフローチャートを参照して説明した決済処理が完了すると、図２１の右部で示されるような決済が完了したことを示す表示画像Ｄ２５が表示される。

[0302] 表示画像Ｄ２５においては、「XXX Shop　カート・USB充電器・USBケーブル、合計¥1080-　お買い上げありがとうございました」と表示され、決済が完了したことが表示されている。

[0303] 以上の処理により、ユーザが、生体情報による認証がなされたウェアラブルデバイス３６を装着し、クライアント装置３１を操作することにより決済処理がなされる場合、ウェアラブルデバイス３６を装着するユーザと、ウェ

アラブルデバイス３６と対応付けて登録されたクレジットカードを用いて、クライアント装置３１を操作して商品を購入するユーザとが一致することを確認することが可能となり、クレジットカードのなりすまし利用であるか否かを適切に判定することができるので、事前与信処理におけるチャレンジフローがなされる頻度を低減させることが可能となる。

[0304] 結果として、チャレンジフローによる認証処理の手間を低減させることができるので、決済処理におけるクレジットカードのなりすましに対するセキュリティレベルを低減させることなく、クレジットカードを利用した快適な決済処理を実現することが可能となる。

[0305] 尚、以上の処理においては、チャレンジフローに移行した場合、ウェアラブルデバイス３６による指紋認証を用いる例について説明してきたが、クライアント装置３１を利用するユーザを認証できればよいので、その他の手法で認証処理を実施するようにしてもよく、例えば、クライアント装置３１に対してパスワードを入力させるような認証処理であってもよい。

[0306] 以上においては、リスクスコアを用いた事前与信処理における与信判定は、銀行サーバ３５により実施される例について説明してきたが、銀行サーバ３５により実施される与信判定に係る処理を他の装置で実施するようにしてもよく、例えば、EC店舗サーバ３２により実施するようにしてもよい。

[0307] また、図２１を参照して説明した表示画像Ｄ２１乃至Ｄ２５のうち、表示画像Ｄ２２，Ｄ２４については、認証が認められたことを確認するだけの表示画像であるため、表示する処理をスキップし、表示しないようにしてもよい。

[0308] ＜＜１４．クライアント装置とウェアラブルデバイスとの相互の位置情報の取得方法のバリエーション（その１）＞＞

以上においては、クライアント装置３１およびウェアラブルデバイス３６のそれぞれの位置情報については、図２２で示されるように、衛星Ｓａｔ１乃至Ｓａｔｎより取得される信号よりGPS５９，２５１により算出される位置情報に基づいて、クライアント装置３１およびウェアラブルデバイス３６の

位置情報が一致するか否か、すなわち、クライアント装置３１およびウェアラブルデバイス３６が、相互に略同一の位置に存在するか否かに基づいて、チャレンジフローへと移行するか否かが判定されていた。

[0309] しかしながら、クライアント装置３１およびウェアラブルデバイス３６の位置が所定の状態よりも近い状態であることが確認できれば、他の方法により位置情報を求めるようにしてもよい。

[0310] 例えば、クライアント装置３１およびウェアラブルデバイス３６のそれぞれにおいて、受信可能なWiFiアクセスポイントのSSIDと、それぞれのWiFiアクセスポイントにおける受信強度とを比較して、クライアント装置３１およびウェアラブルデバイス３６の位置がほぼ同一であるか否かが判定されるようにしてもよい。

[0311] すなわち、例えば、図２３で示されるように、クライアント装置３１およびウェアラブルデバイス３６がほぼ同一の位置に存在する場合、受信可能なWiFiアクセスポイントＡＰ１乃至ＡＰ４が存在するとき、クライアント装置３１およびウェアラブルデバイス３６のそれぞれのWiFiアクセスポイントＡＰ１乃至ＡＰ４に対する位置関係は同一になる。このように位置関係が一致すると、クライアント装置３１およびウェアラブルデバイス３６のそれぞれの通信部５２，２４２におけるそれぞれのWiFi通信部９１，２８１においてはアクセスポイントＡＰ１乃至ＡＰ４との通信が可能な状態とされ、さらに、それぞれのアクセスポイントＡＰ１乃至ＡＰ４からの受信強度もほぼ同一になる。

[0312] 換言すれば、アクセスポイントＡＰ１乃至ＡＰ４のような、周囲に存在するものに対する位置関係が同一であれば、クライアント装置３１およびウェアラブルデバイス３６は同一の位置に存在するとみなすことができる。従って、クライアント装置３１およびウェアラブルデバイス３６の周辺情報（例えば、気圧、温度、および、周囲の環境音声など）を測定し、周辺情報の類似性が所定レベル以上であれば同一の位置であるとみなすことができる。

[0313] そこで、ウェアラブルデバイス３６は、銀行サーバ３５に対して、コンテ

キスト情報として、通信部２４２におけるWiFi通信部２８１において受信されるアクセスポイントＡＰ１乃至ＡＰ４のSSIDと、それぞれの受信強度の情報を、位置情報として所定の時間間隔で送信する。

[0314] そして、事前与信処理においては、銀行サーバ３５が、決済処理を要求するクライアント装置３１の通信部５２におけるWiFi通信部９１により受信されるアクセスポイントＡＰ１乃至ＡＰ４のSSIDと、それぞれの受信強度の情報を取得して、最新のコンテキストDB２０３ａの情報と比較して、所定のレベル以上に類似している場合については、クライアント装置３１およびウェアラブルデバイス３６が同一の位置に存在するものとみなすようにしてもよい。

[0315] すなわち、クライアント装置３１とウェアラブルデバイス３６のそれぞれにおいて受信可能なアクセスポイントのSSIDと、それぞれの受信強度の情報は、それぞれの位置情報として扱うことができる。

[0316] ＜＜１５．クライアント装置とウェアラブルデバイスとの相互の位置情報の取得方法のバリエーション（その２）＞＞

図２４で示されるように、クライアント装置３１およびウェアラブルデバイス３６が、相互にBluetoothによりペアリングされており、相互に通信可能であるか否かに基づいて、相互に略同一の位置に存在するものみなすようにしてもよい。

[0317] すなわち、Bluetoothによる通信は、数十メートル程度の近距離でのみ通信可能であるため、相互にペアリングされていれば、ほぼ同一の位置に存在するものとみなすことができる。

[0318] そこで、ウェアラブルデバイス３６は、コンテキスト情報として、通信部２４２のBluetooth通信部２８３が、Bluetooth通信においてペアリングしているクライアント装置３１の情報を、所定の時間間隔で銀行サーバ３５を送信する。

[0319] そして、事前与信処理においては、銀行サーバ３５が、決済処理を要求するクライアント装置３１の通信部５２におけるBluetooth通信部９３がBlueto

oth通信においてペアリングしているウェアラブルデバイス３６の情報と、最新のコンテキストDB２０３ａの情報と比較して、クライアント装置３１およびウェアラブルデバイス３６の相互がペアリングしているときには、双方が同一の位置に存在するものとみなすようにしてもよい。

[0320] また、この他にも、携帯電話の通信網を利用して、例えば、クライアント装置３１およびウェアラブルデバイス３６のそれぞれの通信部５２，２４２のLTE通信部９２，２８２が通信に利用しているセルが同一であるか否かに基づいて、クライアント装置３１およびウェアラブルデバイス３６がほぼ同一の位置に存在するか否かを判定するようにしてもよい。

[0321] さらに、クライアント装置３１およびウェアラブルデバイス３６の通信部５２，２４２のNFC９４，２８４により相互通信が可能であるか否かに基づいて、クライアント装置３１およびウェアラブルデバイス３６がほぼ同一の位置に存在するか否かを判定するようにしてもよい。

[0322] ＜＜１６．クライアント装置とウェアラブルデバイスとがほぼ同一の位置であるか否かの判定方法のバリエーション（その１）＞＞

[0323] クライアント装置３１およびウェアラブルデバイス３６において、それぞれ受信可能なアクセスポイントＡＰ１乃至ＡＰ４のSSIDと、それぞれの受信強度などから得られる位置情報、GPS５９，２４９により求められる位置情報等、様々な方法で得られる位置情報を利用して、双方の距離を直接求め、その距離が所定の距離よりも近い場合は、双方がほぼ同一の位置に存在するものとみなすようにしてもよい。

[0324] すなわち、図２５のウェアラブルデバイス３６－３１で示されるように、クライアント装置３１との距離が所定の距離ｒ（例えば、30mなど）よりも近い場合については、相互にほぼ同一の位置に存在するものみなすようにする。

[0325] 一方、ウェアラブルデバイス３６－３２で示されるように、クライアント装置３１との距離が所定の距離ｒ（例えば、30mなど）よりも遠い場合については、相互にほぼ同一の位置に存在しないものとみなすようにしてもよい。

[0326] ＜＜１７．クライアント装置とウェアラブルデバイスとがほぼ同一の位置であるか否かの判定方法のバリエーション（その２）＞＞

以上においては、決済処理が開始された後に、クライアント装置３１の位置とウェアラブルデバイス３６との距離を用いて実測して所定の距離との比較により同一の位置であるか否かを判定する例について説明してきたが、例えば、ウェアラブルデバイス３６の位置情報である直近のコンテキスト情報が、過去に何度か、決済を行った場所であれば、クライアント装置３１の位置情報がない状態であっても、クライアント装置３１とほぼ同一の位置であるものとみなすようにしてもよい。

[0327] すなわち、以上においては、決済処理が開始された後のクライアント装置３１の位置情報を用いて、ウェアラブルデバイス３６の位置と同一の位置であるか否かが判定された後、同一の位置である時、所定値Ａだけリスクスコアが低減される例について説明してきた。

[0328] しかしながら、リスクスコアが高過ぎる場合、何度か所定値Ａだけ繰り返し低減させなければ、チャレンジフローに移行させるための閾値よりもリスクスコアを低減できない可能性がある。この場合、リスクスコアが閾値よりも小さくなる前に決済処理がなされるとチャレンジフローへと移行される可能性がある。

[0329] そこで、図２６で示されるように、決済処理が要求される前の段階で、すなわち、クライアント装置３１の位置情報が供給される前の段階で、ウェアラブルデバイス３６の位置が、過去に所定回数以上決済処理がなされた位置Ｈより所定の距離ｒだけ近い位置であることが認識された段階で、クライアント装置３１とほぼ同一の位置であるものとみなし、事前にリスクスコアを低減させるようにする。

[0330] すなわち、図２６のウェアラブルデバイス３６－３１で示されるように、クライアント装置３１により過去に決済処理がなされた位置Ｈとの距離が所定の距離ｒ（例えば、30mなど）よりも近い場合については、相互にほぼ同一の位置に存在するものみなすようにする。一方、ウェアラブルデバイス３６

－３２で示されるように、クライアント装置３１により過去に決済処理がなされた位置Ｈとの距離が所定の距離ｒ（例えば、30mなど）よりも遠い場合については、相互にほぼ同一の位置に存在しないものとみなすようにしてもよい。

[0331] このような処理により、リスクスコアの低減が間に合わずにチャレンジフローへと移行してしまうようなことを防止させることが可能となる。

[0332] ＜＜１８．コンテキスト情報アップロード処理の変形例＞＞

以上においては、コンテキスト情報は、所定時間間隔でウェアラブルデバイス３６から一方的に銀行サーバ３５に送信する例について説明してきたが、銀行サーバ３５からの要求に応じて送信するようにしてもよい。

[0333] 例えば、リスクスコアは、所定時間ｔ毎に所定値ａだけ増大することになるので、銀行サーバ３５が、現在のリスクスコアとチャレンジフローへと移行する閾値とを比較し、リスクスコアが閾値を超えそうになる近い値になったとき（または、リスクスコアが閾値を超えたとき）に、ウェアラブルデバイス３６にコンテキスト情報を要求し、この要求に応じて、ウェアラブルデバイス３６がコンテキスト情報を送信するようにしてもよい。

[0334] ここで、図２７のフローチャートを参照して、銀行サーバ３５からウェアラブルデバイス３６に対してコンテキスト情報を要求するようにしたコンテキスト情報アップロード処理について説明する。

[0335] 尚、図２７のフローチャートにおいて、ステップＳ３０１乃至Ｓ３０３，Ｓ３０５乃至Ｓ３１０の処理、およびステップＳ３２１乃至Ｓ３２８，Ｓ３３１の処理は、図１５のステップＳ１５１乃至Ｓ１５３，Ｓ１５５乃至Ｓ１６０の処理、およびステップＳ１７１乃至Ｓ１７９の処理と同様であるので、その説明は適宜省略する。

[0336] すなわち、ステップＳ３２９において、銀行サーバ３５の制御部２０１におけるリスクスコア判定部２２４は、コンテキストDB２０３ａにアクセスし、リスクスコアがチャレンジフローに移行させるための閾値よりも低いが、閾値を超える兆候がある（閾値に近付きつつある）か、または、閾値を既に

超えているか否かを判定する。

[0337] ステップＳ３２９において、リスクスコア判定部２２４は、リスクスコアが閾値よりも低いが、閾値を超える兆候がある、または、閾値を既に超えていると判定した場合、処理は、ステップＳ３３０に進む。

[0338] ステップＳ３３０において、リスクスコア判定部２２４は、通信部２０２を制御して、ウェアラブルデバイス３６に対してコンテキスト情報を要求する。

[0339] 尚、ステップＳ３２９において、リスクスコアが閾値を超えておらず、また、閾値に近い値でもない場合、ステップＳ３３１の処理はスキップされる。

[0340] ステップＳ３０４において、ウェアラブルデバイス３６の制御部２４１におけるコンテキスト送信処理部２７２は、通信部２４２を制御して、銀行サーバ３５よりコンテキスト情報が要求されたか否かを判定し、送信されてくるまで、同様の処理が繰り返される。

[0341] そして、ステップＳ３０４において、コンテキスト情報を要求する情報が送信されてくると、処理は、ステップＳ３０５に進む。

[0342] すなわち、ウェアラブルデバイス３６は、銀行サーバ３５からコンテキスト情報が要求されるときに、コンテキスト情報を供給する。

[0343] この結果、リスクスコアは、例えば、図２８の実線で示されるように時系列に変化する。尚、この時系列の変化は、ウェアラブルデバイス３６が装着されていない状態から、装着し、脱着されるまでのリスクスコアの変化を示している。また、図２８の最上段における双方向の矢印の範囲内がユーザがウェアラブルデバイス３６を装着しているタイミングである。

[0344] すなわち、時刻ｔ１００において、ウェアラブルデバイス３６は、ユーザに装着されていない状態であるが、実線で示されるリスクスコアは、リスクスコア閾値ｔｈよりも低い値である。

[0345] しかしながら、リスクスコアは、時間の経過に伴って、徐々に増大し、時刻ｔ１０１において閾値ｔｈを超える。

[0346] そして、ウェアラブルデバイス３６は、ユーザに装着されることがないため、リスクスコアは増大し続ける。

[0347] ここで、時刻ｔ１０２において、生体認証である指紋が検出されて登録された正規の生体情報であることが認識されて、ウェアラブルデバイス３６がユーザに装着されると、装着に伴って、リスクスコアが低減され、閾値ｔｈよりも低い値となる。

[0348] その後、時間の経過に伴って、徐々にリスクスコアが増大し、時刻ｔ１０３において、閾値ｔｈに近い値となる。そこで、この時刻ｔ１０３において、銀行サーバ３５からウェアラブルデバイス３６に対してコンテキスト情報が要求される。

[0349] このコンテキスト情報の要求に応じて、時刻ｔ１０４において、ウェアラブルデバイス３６は、コンテキスト情報を銀行サーバ３５に送信する。

[0350] この結果、リスクスコアは低減されて閾値ｔｈよりも小さな値となり、その後、時間の経過に伴って増大し、再び、時刻ｔ１０５において、閾値ｔｈに近い値となる。そこで、この時刻ｔ１０５において、銀行サーバ３５からウェアラブルデバイス３６に対してコンテキスト情報が要求される。

[0351] このコンテキスト情報の要求に応じて、時刻ｔ１０６において、ウェアラブルデバイス３６は、コンテキスト情報を銀行サーバ３５に送信する。

[0352] この結果、リスクスコアは低減されて閾値ｔｈよりも小さな値となり、その後、時間の経過に伴って増大し、再び、時刻ｔ１０７において、閾値ｔｈに近い値となる。そこで、この時刻ｔ１０７において、銀行サーバ３５からウェアラブルデバイス３６に対してコンテキスト情報が要求される。

[0353] このコンテキスト情報の要求に応じて、時刻ｔ１０８において、ウェアラブルデバイス３６は、コンテキスト情報を銀行サーバ３５に送信する。

[0354] この後、時刻ｔ１０９において、ウェアラブルデバイス３６の脱着が検出されると、リスクスコアは、チャレンジフローが必要な閾値よりも大きな値に調整される。

[0355] このような一連の動作により、リスクスコアは、ウェアラブルデバイス３

６がユーザにより装着されている期間においては、閾値ｔｈよりも低い値を維持することが可能となり、なりすましに対するセキュリティのレベルを低減させることなく、チャレンジフローへの移行の頻度を低減させることが可能となる。

[0356] 結果として、チャレンジフローによる認証処理の手間を低減させることができるので、決済処理におけるクレジットカードのなりすましに対するセキュリティレベルを低減させることなく、クレジットカードを利用した快適な決済処理を実現することが可能となる。

[0357] ＜＜１９．対面決済への応用＞＞

以上においては、電子決済に係る決済処理を例にして説明してきたが、店頭における、いわゆる、対面決済においても応用させることが可能である。

[0358] 対面決済においては、クライアント装置３１は、クレジットカードのカードリーダなどに対応することになり、EC店舗サーバ３２が、ネットワークに接続された店頭の精算機などに対応する。以降においては、精算機はEC店舗サーバ３２と対応するものとして精算機３２とも称する。

[0359] また、対面決済においては、QRコード決済であってもよい。

[0360] QRコード決済とは、専用のアプリケーションプログラムがインストールされたクライアント装置３１を用いて、QRコード（登録商標）を用いた決済方法であり、コード決済と読取決済とがある。

[0361] コード決済とは、例えば、図２９の左部で示されるように、専用のアプリケーションプログラムがインストールされたクライアント装置３１を用いて、支払い金額に対応するQRコードを提示して、店頭の精算機３２などがリーダ（入力部１０４に相当）により読み取ることで行う決済である。

[0362] 読取決済とは、例えば、図２９の右部で示されるように、専用のアプリケーションプログラムがインストールされたクライアント装置３１を用いて、店頭の精算機などに接続されたディスプレイ等（出力部部１０５に相当）により支払い金額に対応するQRコードをクライアント装置３１が読み取ることで行う決済である。

[0363] いずれにおいても、クライアント装置３１によりクレジットカードを用いた場合と同様に決済することが可能である。

[0364] ＜＜２０．ソフトウェアにより実行させる例＞＞

ところで、上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のコンピュータなどに、記録媒体からインストールされる。

[0365] 図３０は、汎用のコンピュータの構成例を示している。このパーソナルコンピュータは、CPU(Central Processing Unit)１００１を内蔵している。CPU１００１にはバス１００４を介して、入出力インタフェース１００５が接続されている。バス１００４には、ROM(Read Only Memory)１００２およびRAM(Random Access Memory)１００３が接続されている。

[0366] 入出力インタフェース１００５には、ユーザが操作コマンドを入力するキーボード、マウスなどの入力デバイスよりなる入力部１００６、処理操作画面や処理結果の画像を表示デバイスに出力する出力部１００７、プログラムや各種データを格納するハードディスクドライブなどよりなる記憶部１００８、LAN (Local Area Network) アダプタなどよりなり、インターネットに代表されるネットワークを介した通信処理を実行する通信部１００９が接続されている。また、磁気ディスク（フレキシブルディスクを含む）、光ディスク (CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク（ＭＤ(Mini Disc)を含む）、もしくは半導体メモリなどのリムーバブル記憶媒体１０１１に対してデータを読み書きするドライブ１０１０が接続されている。

[0367] CPU１００１は、ROM１００２に記憶されているプログラム、または磁気ディスク、光ディスク、光磁気ディスク、もしくは半導体メモリ等のリムーバブル記憶媒体１０１１ら読み出されて記憶部１００８にインストールされ、

記憶部１００８からRAM１００３にロードされたプログラムに従って各種の処理を実行する。RAM１００３にはまた、CPU１００１が各種の処理を実行する上において必要なデータなども適宜記憶される。

[0368] 以上のように構成されるコンピュータでは、CPU１００１が、例えば、記憶部１００８に記憶されているプログラムを、入出力インタフェース１００５及びバス１００４を介して、RAM１００３にロードして実行することにより、上述した一連の処理が行われる。

[0369] コンピュータ（CPU１００１）が実行するプログラムは、例えば、パッケージメディア等としてのリムーバブル記憶媒体１０１１に記録して提供することができる。また、プログラムは、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の伝送媒体を介して提供することができる。

[0370] コンピュータでは、プログラムは、リムーバブル記憶媒体１０１１をドライブ１０１０に装着することにより、入出力インタフェース１００５を介して、記憶部１００８にインストールすることができる。また、プログラムは、有線または無線の伝送媒体を介して、通信部１００９で受信し、記憶部１００８にインストールすることができる。その他、プログラムは、ROM１００２や記憶部１００８に、あらかじめインストールしておくことができる。

[0371] なお、コンピュータが実行するプログラムは、本明細書で説明する順序に沿って時系列に処理が行われるプログラムであっても良いし、並列に、あるいは呼び出しが行われたとき等の必要なタイミングで処理が行われるプログラムであっても良い。

[0372] 尚、図３０におけるCPU１００１が、図５乃至図１０のそれぞれの制御部５１，１０１，１４１，１６１，２０１，２４１の機能を実現させる。

[0373] また、本明細書において、システムとは、複数の構成要素（装置、モジュール（部品）等）の集合を意味し、すべての構成要素が同一筐体中にあるか否かは問わない。したがって、別個の筐体に収納され、ネットワークを介して接続されている複数の装置、及び、１つの筐体の中に複数のモジュールが

収納されている１つの装置は、いずれも、システムである。

[0374] なお、本開示の実施の形態は、上述した実施の形態に限定されるものではなく、本開示の要旨を逸脱しない範囲において種々の変更が可能である。

[0375] 例えば、本開示は、１つの機能をネットワークを介して複数の装置で分担、共同して処理するクラウドコンピューティングの構成をとることができる。

[0376] また、上述のフローチャートで説明した各ステップは、１つの装置で実行する他、複数の装置で分担して実行することができる。

[0377] さらに、１つのステップに複数の処理が含まれる場合には、その１つのステップに含まれる複数の処理は、１つの装置で実行する他、複数の装置で分担して実行することができる。

[0378] 尚、本開示は、以下のような構成も取ることができる。

[0379] ＜１＞ 決済処理において、ユーザを認証した認証装置と、前記ユーザが前記決済処理を行うクライアント装置との位置関係に基づいて、前記決済処理に係るリスクを判定するリスク判定部を含む

情報処理装置。

＜２＞ 前記リスク判定部は、前記決済処理に係るリスクに係るスコアをリスクスコアとして設定し、設定した前記リスクスコアと所定の閾値との比較によりリスクを判定する

＜１＞に記載の情報処理装置。

＜３＞ 前記リスク判定部により、前記リスクスコアが所定の閾値よりも高いと判定された場合、前記クライアント装置に対して、認証処理を要求する認証処理要求を送信する認証処理要求部をさらに含み、

前記リスク判定部は、前記認証処理要求に応じた前記クライアント装置からの認証結果に基づいて、前記決済処理に係るリスクを判定する

＜２＞に記載の情報処理装置。

＜４＞ 前記認証装置から所定の時間間隔で送信される、前記ユーザの認証結果と、前記認証装置の位置情報である認証装置位置情報とをコンテキスト

情報として受信するコンテキスト情報受信部をさらに含み、

前記リスク判定部は、前記コンテキスト情報受信部により、前記コンテキスト情報が受信されるとき、前記リスクスコアを所定値だけ低減させる

＜３＞に記載の情報処理装置。

＜５＞　前記リスク判定部は、所定の時間間隔で、前記リスクスコアを所定値だけ増大させる

＜４＞に記載の情報処理装置。

＜６＞　前記認証装置は、前記ユーザにより装着されるものであり、前記ユーザにより装着されるとき、前記コンテキスト情報受信部は、前記コンテキスト情報を受信する

＜４＞に記載の情報処理装置。

＜７＞　前記認証装置が前記ユーザにより脱着されるとき、前記コンテキスト情報受信部は、前記認証装置が脱着されたことを示す情報を受信し、

前記リスク判定部は、前記コンテキスト情報受信部により、前記認証装置が脱着されたことを示す情報が受信されたとき、前記リスクスコアを前記所定の閾値よりも大きな値に設定する

＜５＞に記載の情報処理装置。

＜８＞　前記コンテキスト情報受信部は、前記リスクスコアが前記所定の閾値よりも低いが、前記所定の閾値を超えるような兆候を見せたとき、または、前記リスクスコアが前記所定の閾値を超えたとき、前記認証装置に対して前記コンテキスト情報を要求し、受信する

＜４＞に記載の情報処理装置。

＜９＞　前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が同一の位置であるか否かに基づいて、前記決済処理に係るリスクを判定する

＜１＞乃至＜８＞のいずれかに記載の情報処理装置。

＜１０＞　前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が、所定の距離内であるか否かに基づいて、前記決済処理に係るリ

スクを判定する

＜１＞乃至＜８＞のいずれかに記載の情報処理装置。

＜１１＞　前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が、双方で受信可能なアクセスポイントのSSIDと、それぞれの受信強度が所定のレベルより大きく類似しているか否かに基づいて、前記決済処理に係るリスクを判定する

＜１＞乃至＜８＞のいずれかに記載の情報処理装置。

＜１２＞　前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が、双方でBluetoothによりペアリングできるか否かに基づいて、前記決済処理に係るリスクを判定する

＜１＞乃至＜８＞のいずれかに記載の情報処理装置。

＜１３＞　決済処理において、ユーザを認証した認証装置と、前記ユーザが前記決済処理を行うクライアント装置の位置情報との位置関係に基づいて、前記決済処理に係るリスクを判定する

情報処理方法。

＜１４＞　ユーザを認証する認証装置と、決済処理に係るリスクを判定する情報処理装置に対して前記ユーザによる前記決済処理を実行するクライアント装置とからなるクライアントシステムにおいて、

前記認証装置は、

前記ユーザを認証する認証部と、

前記認証装置の位置情報を認証装置位置情報として取得する認証装置位置情報取得部と、

前記認証部による認証結果と前記認証装置位置情報を前記情報処理装置に送信する認証装置位置情報送信部とを含み、

前記クライアント装置は、

前記クライアント装置の位置情報をクライアント装置位置情報として取得するクライアント装置位置情報取得部と、

前記クライアント装置位置情報を前記情報処理装置に送信するクライア

ント装置位置情報送信部とを含む

クライアントシステム。

＜１５＞　前記認証装置位置情報送信部は、所定の時間間隔で、前記認証結果と前記認証装置の位置情報をコンテキスト情報として前記情報処理装置に送信する

＜１４＞に記載のクライアントシステム。

＜１６＞　前記認証装置は、前記ユーザにより装着されるものであり、

前記認証装置位置情報送信部は、前記認証装置が前記ユーザにより装着されるとき、前記コンテキスト情報を前記情報処理装置に送信する

＜１５＞に記載のクライアントシステム。

＜１７＞　前記認証装置位置情報送信部は、前記認証装置が前記ユーザにより脱着されるとき、前記認証装置が脱着されたことを示す情報を前記情報処理装置に送信する

＜１６＞に記載のクライアントシステム。

＜１８＞　前記認証装置位置情報送信部は、前記情報処理装置より前記コンテキスト情報の要求があった場合、前記コンテキスト情報を前記情報処理装置に送信する

＜１５＞に記載のクライアントシステム。

＜１９＞　前記情報処理装置の前記決済処理に係るリスクの判定結果に基づいて、前記ユーザの認証情報が要求された場合、前記ユーザの認証情報を、前記情報処理装置に送信する認証情報送信部をさらに含む

＜１４＞に記載のクライアントシステム。

＜２０＞　ユーザを認証する認証装置と、決済処理に係るリスクを判定する情報処理装置に対して前記ユーザによる前記決済処理を実行するクライアント装置とからなるクライアントシステムの制御方法において、

前記認証装置の制御方法は、

前記ユーザを認証する認証処理と、

前記認証装置の位置情報を認証装置位置情報として取得する認証装置位

置情報取得処理と、

前記認証処理の認証結果と前記認証装置位置情報を前記情報処理装置に送信する認証装置位置情報送信処理とを含み、

前記クライアント装置の制御方法は、

前記クライアント装置の位置情報をクライアント装置位置情報として取得するクライアント装置位置情報取得処理と、

前記クライアント装置位置情報を前記情報処理装置に送信するクライアント装置位置情報送信処理とを含む

クライアントシステムの制御方法。

符号の説明

[0380] ３０　決済処理システム，　３１　クライアント装置，　３２　EC店舗サーバ，　３３　アクワイヤラサーバ，　３４　仲介サーバ，　３５　銀行サーバ，　３６　ウェアラブルデバイス，　５１　制御部，　５９　GPS，　７１　決済処理部，　７２　チャレンジ処理部，　７３　登録処理部，　１０１　制御部，　１２１　事前与信処理部，　１２２　決済処理部，　１４１　制御部，　１５１　決済処理部，　１６１　制御部，　１８１　事前与信仲介処理部，　１８２　決済仲介処理部，　２０１　制御部，　２０３ａ　コンテキストDB，　２２１　登録処理部，　２２２　コンテキスト受信処理部，　２２３　チャレンジ処理部，　２２４　リスクスコア判定部，　２２５　決済処理部，　２４１　制御部，　２４９　GPS，　２５０　装着センサ，　２５１　指紋センサ，　２７１　登録処理部，　２７２　コンテキスト送信部，　２７３　チャレンジ処理部

請求の範囲

[請求項1] 決済処理において、ユーザを認証した認証装置と、前記ユーザが前記決済処理を行うクライアント装置との位置関係に基づいて、前記決済処理に係るリスクを判定するリスク判定部を含む

情報処理装置。

[請求項2] 前記リスク判定部は、前記決済処理に係るリスクに係るスコアをリスクスコアとして設定し、設定した前記リスクスコアと所定の閾値との比較によりリスクを判定する

請求項１に記載の情報処理装置。

[請求項3] 前記リスク判定部により、前記リスクスコアが所定の閾値よりも高いと判定された場合、前記クライアント装置に対して、認証処理を要求する認証処理要求を送信する認証処理要求部をさらに含み、

前記リスク判定部は、前記認証処理要求に応じた前記クライアント装置からの認証結果に基づいて、前記決済処理に係るリスクを判定する

請求項２に記載の情報処理装置。

[請求項4] 前記認証装置から所定の時間間隔で送信される、前記ユーザの認証結果と、前記認証装置の位置情報である認証装置位置情報とをコンテキスト情報として受信するコンテキスト情報受信部をさらに含み、

前記リスク判定部は、前記コンテキスト情報受信部により、前記コンテキスト情報が受信されるとき、前記リスクスコアを所定値だけ低減させる

請求項３に記載の情報処理装置。

[請求項5] 前記リスク判定部は、所定の時間間隔で、前記リスクスコアを所定値だけ増大させる

請求項４に記載の情報処理装置。

[請求項6] 前記認証装置は、前記ユーザにより装着されるものであり、前記ユーザにより装着されるとき、前記コンテキスト情報受信部は、前記コ

ンテキスト情報を受信する

請求項４に記載の情報処理装置。

[請求項7] 前記認証装置が前記ユーザにより脱着されるとき、前記コンテキスト情報受信部は、前記認証装置が脱着されたことを示す情報を受信し、

前記リスク判定部は、前記コンテキスト情報受信部により、前記認証装置が脱着されたことを示す情報が受信されたとき、前記リスクスコアを前記所定の閾値よりも大きな値に設定する

請求項５に記載の情報処理装置。

[請求項8] 前記コンテキスト情報受信部は、前記リスクスコアが前記所定の閾値よりも低いが、前記所定の閾値を超えるような兆候を見せたとき、または、前記リスクスコアが前記所定の閾値を超えたとき、前記認証装置に対して前記コンテキスト情報を要求し、受信する

請求項４に記載の情報処理装置。

[請求項9] 前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が同一の位置であるか否かに基づいて、前記決済処理に係るリスクを判定する

請求項１に記載の情報処理装置。

[請求項10] 前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が、所定の距離内であるか否かに基づいて、前記決済処理に係るリスクを判定する

請求項１に記載の情報処理装置。

[請求項11] 前記リスク判定部は、前記認証装置と前記クライアント装置との位置関係が、双方で受信可能なアクセスポイントのSSIDと、それぞれの受信強度が所定のレベルより大きく類似しているか否かに基づいて、前記決済処理に係るリスクを判定する

請求項１に記載の情報処理装置。

[請求項12] 前記リスク判定部は、前記認証装置と前記クライアント装置との位

置関係が、双方でBluetoothによりペアリングできるか否かに基づいて、前記決済処理に係るリスクを判定する

請求項１に記載の情報処理装置。

[請求項13] 決済処理において、ユーザを認証した認証装置と、前記ユーザが前記決済処理を行うクライアント装置の位置情報との位置関係に基づいて、前記決済処理に係るリスクを判定する

情報処理方法。

[請求項14] ユーザを認証する認証装置と、決済処理に係るリスクを判定する情報処理装置に対して前記ユーザによる前記決済処理を実行するクライアント装置とからなるクライアントシステムにおいて、

前記認証装置は、

前記ユーザを認証する認証部と、

前記認証装置の位置情報を認証装置位置情報として取得する認証装置位置情報取得部と、

前記認証部による認証結果と前記認証装置位置情報を前記情報処理装置に送信する認証装置位置情報送信部とを含み、

前記クライアント装置は、

前記クライアント装置の位置情報をクライアント装置位置情報として取得するクライアント装置位置情報取得部と、

前記クライアント装置位置情報を前記情報処理装置に送信するクライアント装置位置情報送信部とを含む

クライアントシステム。

[請求項15] 前記認証装置位置情報送信部は、所定の時間間隔で、前記認証結果と前記認証装置の位置情報をコンテキスト情報として前記情報処理装置に送信する

請求項１４に記載のクライアントシステム。

[請求項16] 前記認証装置は、前記ユーザにより装着されるものであり、

前記認証装置位置情報送信部は、前記認証装置が前記ユーザにより

装着されるとき、前記コンテキスト情報を前記情報処理装置に送信する

請求項１５に記載のクライアントシステム。

[請求項17] 前記認証装置位置情報送信部は、前記認証装置が前記ユーザにより脱着されるとき、前記認証装置が脱着されたことを示す情報を前記情報処理装置に送信する

請求項１６に記載のクライアントシステム。

[請求項18] 前記認証装置位置情報送信部は、前記情報処理装置より前記コンテキスト情報の要求があった場合、前記コンテキスト情報を前記情報処理装置に送信する

請求項１５に記載のクライアントシステム。

[請求項19] 前記情報処理装置の前記決済処理に係るリスクの判定結果に基づいて、前記ユーザの認証情報が要求された場合、前記ユーザの認証情報を、前記情報処理装置に送信する認証情報送信部をさらに含む

請求項１４に記載のクライアントシステム。

[請求項20] ユーザを認証する認証装置と、決済処理に係るリスクを判定する情報処理装置に対して前記ユーザによる前記決済処理を実行するクライアント装置とからなるクライアントシステムの制御方法において、

前記認証装置の制御方法は、

前記ユーザを認証する認証処理と、

前記認証装置の位置情報を認証装置位置情報として取得する認証装置位置情報取得処理と、

前記認証処理の認証結果と前記認証装置位置情報を前記情報処理装置に送信する認証装置位置情報送信処理とを含み、

前記クライアント装置の制御方法は、

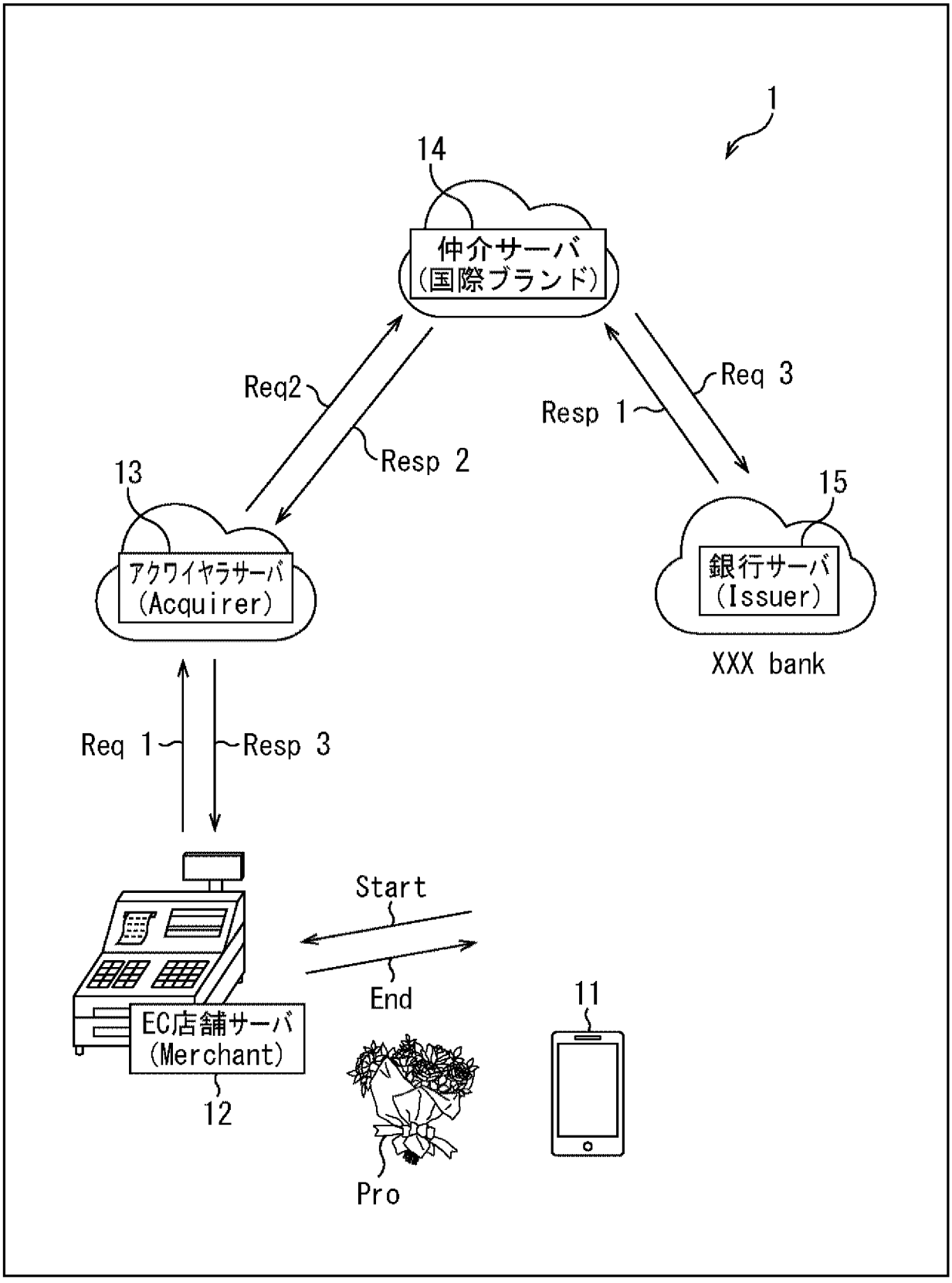
前記クライアント装置の位置情報をクライアント装置位置情報として取得するクライアント装置位置情報取得処理と、

前記クライアント装置位置情報を前記情報処理装置に送信するク

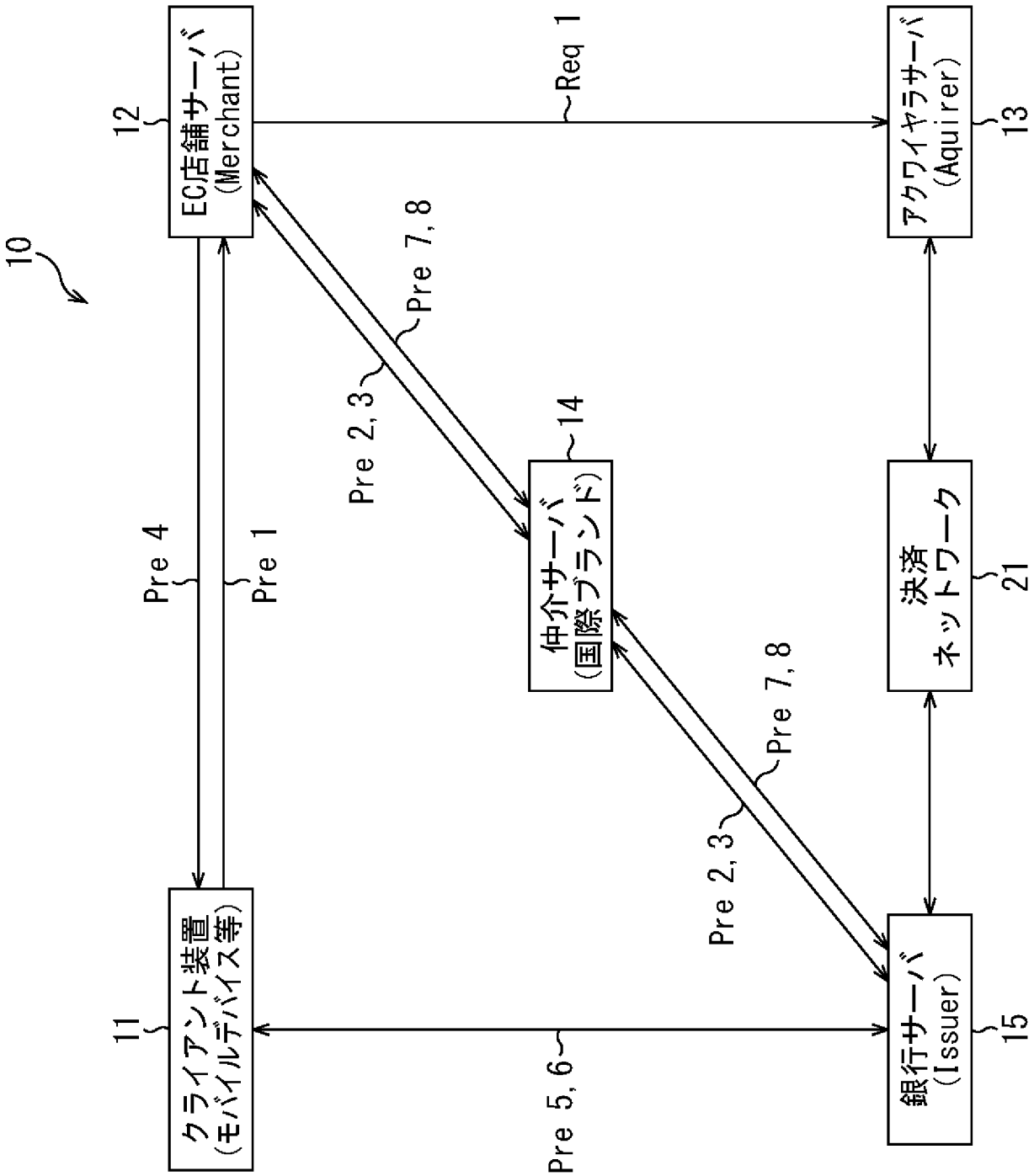
ライアント装置位置情報送信処理とを含む

クライアントシステムの制御方法。

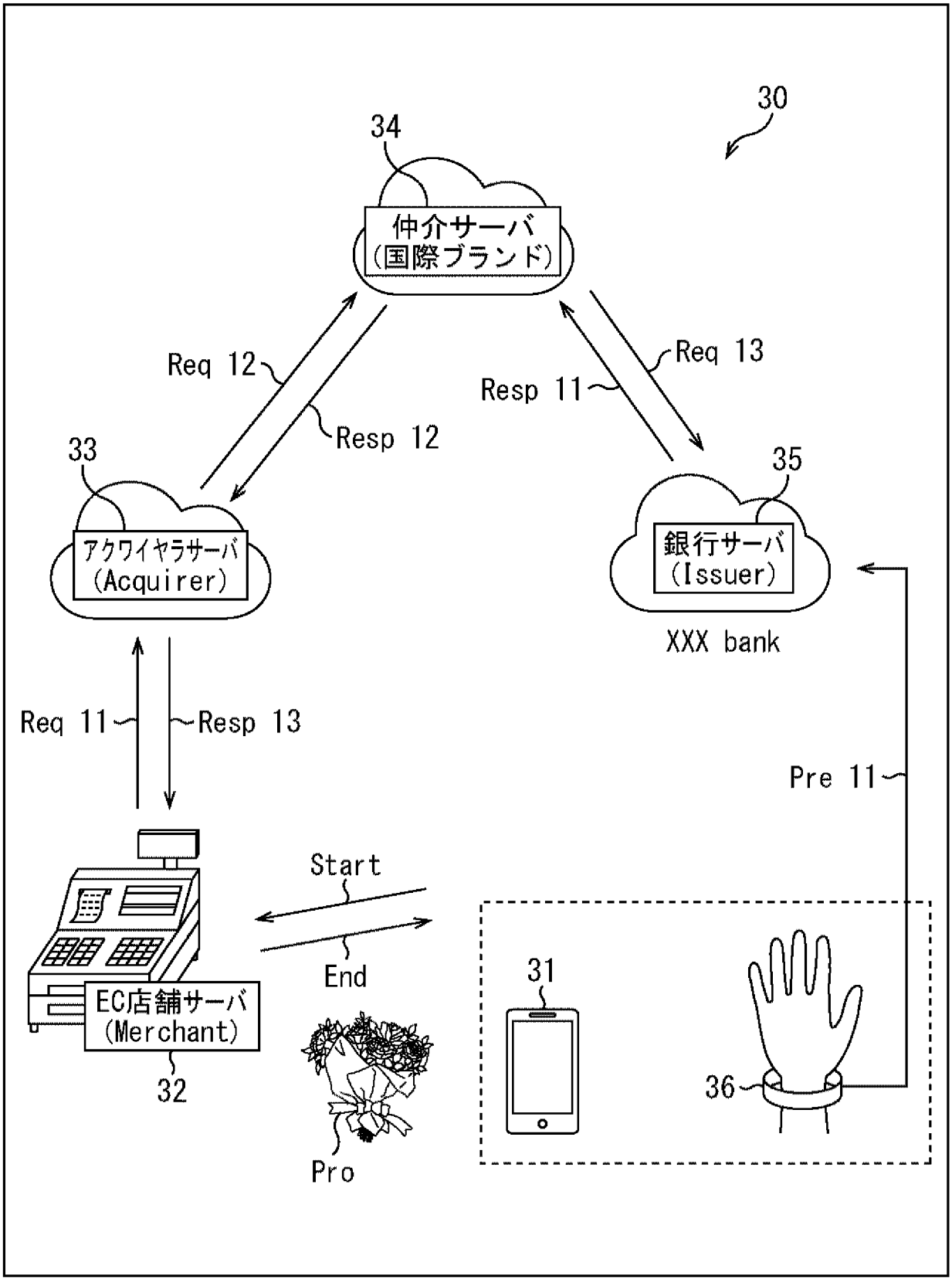
[図1]
FIG. 1


1
14
仲介サーバ
(国際ブランド)
Req2
Resp 2
Req 3
Resp 1
13
アクワイヤラサーバ
(Acquirer)
15
銀行サーバ
(Issuer)
XXX bank
Req 1
Resp 3
Start
End
EC店舗サーバ
(Merchant)
12
11
Pro

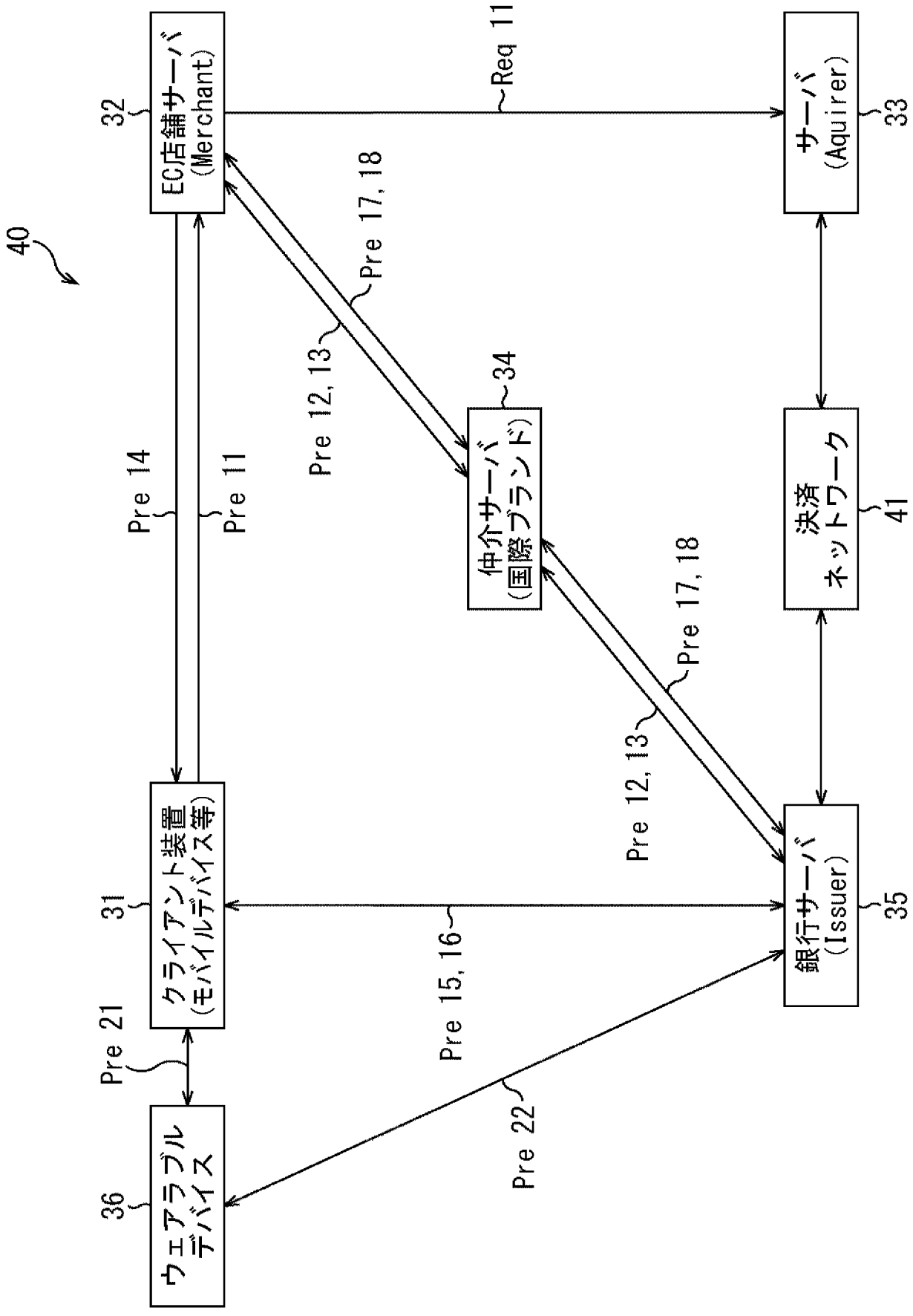
[図2]
FIG. 2


10
EC店舗サーバ
(Merchant)
12
Req 1
アクワイヤラサーバ
(Aquirer)
13
Pre 7, 8
Pre 2, 3
14
仲介サーバ
(国際ブランド)
Pre 4
Pre 1
決済
ネットワーク
21
Pre 7, 8
Pre 2, 3
クライアント装置
(モバイルデバイス等)
11
Pre 5, 6
銀行サーバ
(Issuer)
15

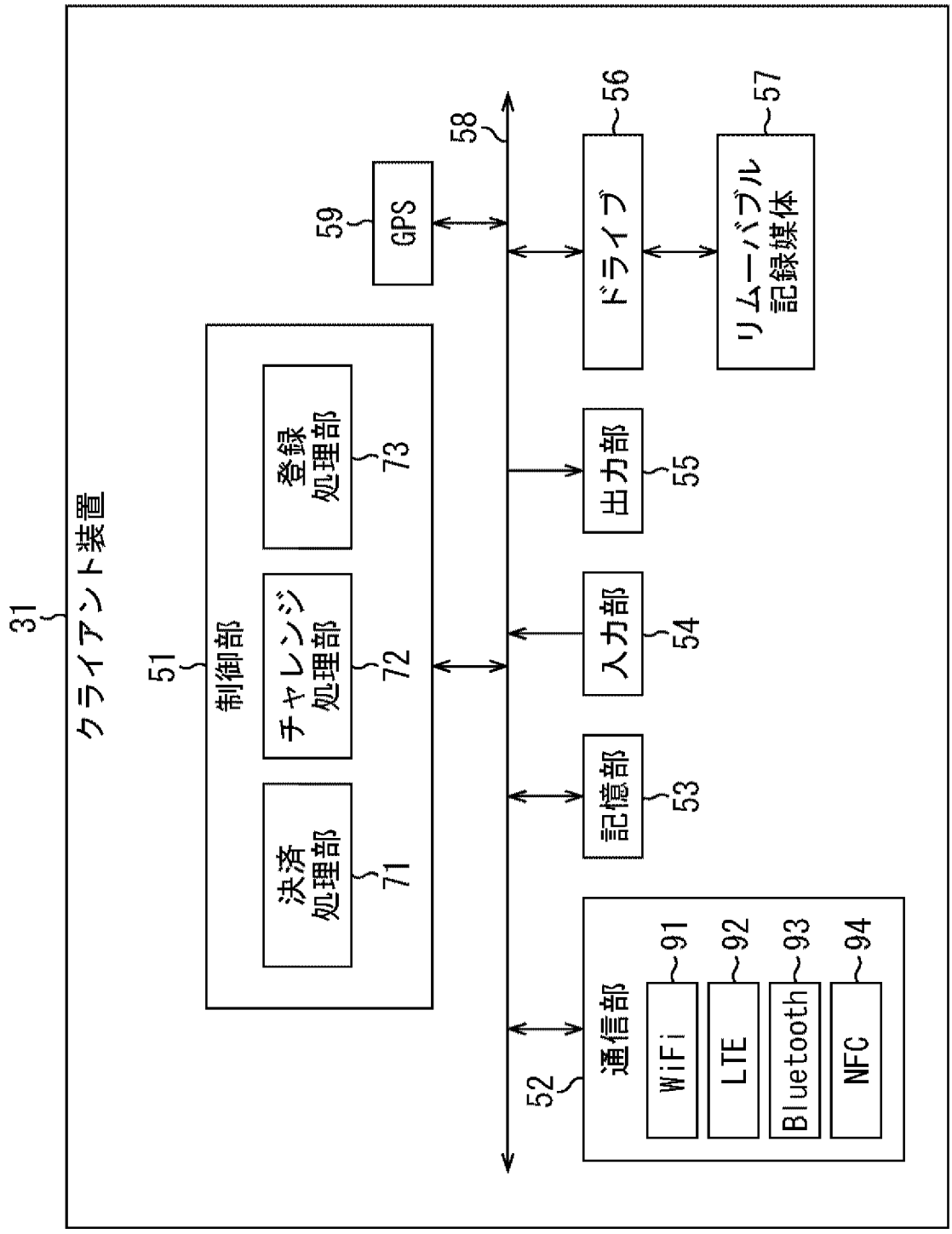
[図3]
FIG. 3


30
34
仲介サーバ
(国際ブランド)
Req 12
Resp 12
Req 13
Resp 11
33
アクワイヤラサーバ
(Acquirer)
35
銀行サーバ
(Issuer)
XXX bank
Req 11
Resp 13
Pre 11
Start
End
EC店舗サーバ
(Merchant)
32
Pro
31
36

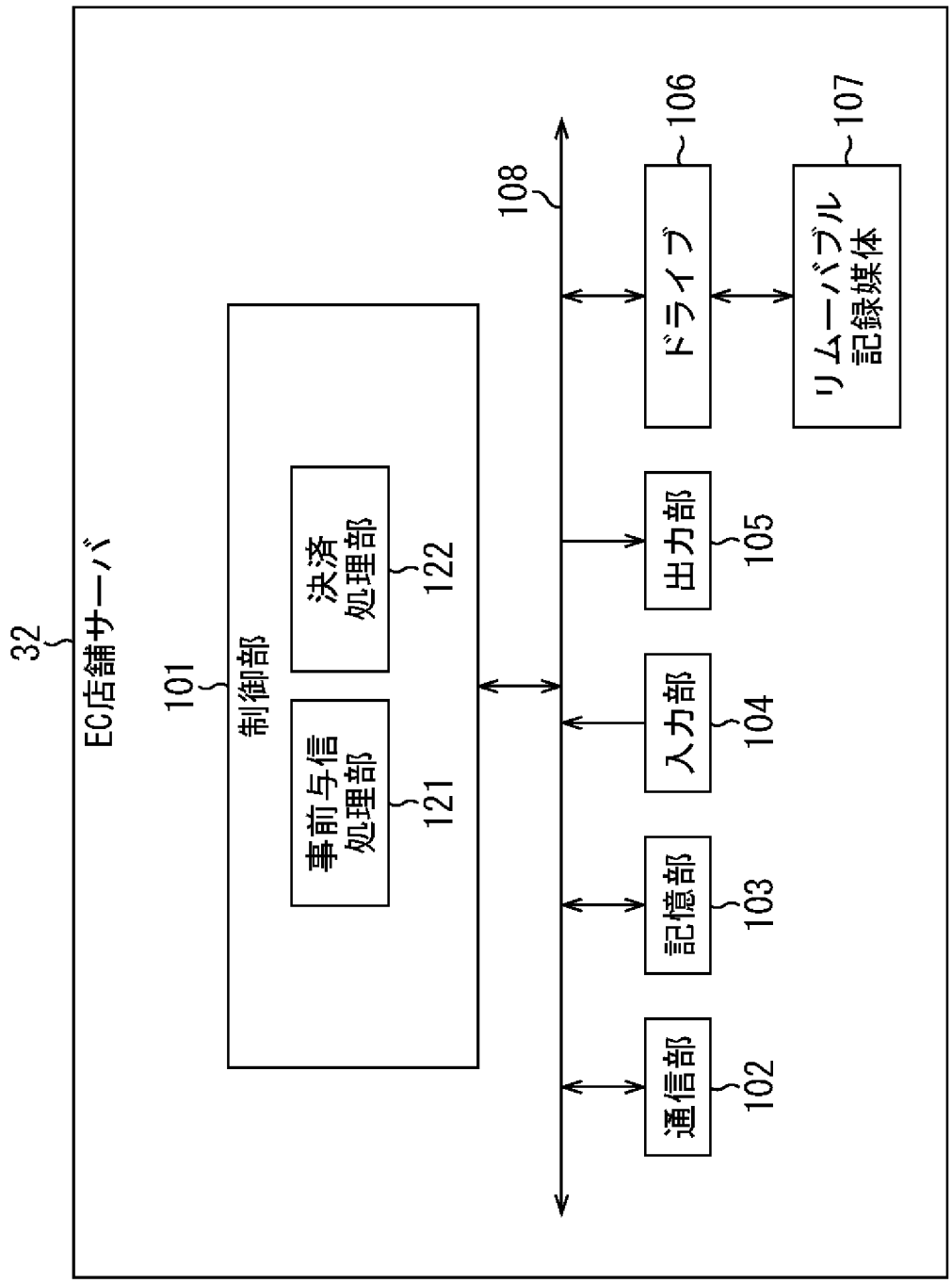
[図4]
FIG. 4


40
EC店舗サーバ
(Merchant)
32
Req 11
サーバ
(Aquirer)
33
Pre 17, 18
Pre 12, 13
34
仲介サーバ
(国際ブランド)
Pre 14
Pre 11
決済
ネットワーク
41
Pre 17, 18
Pre 12, 13
クライアント装置
(モバイルデバイス等)
31
銀行サーバ
(Issuer)
35
Pre 15, 16
Pre 21
Pre 22
ウェアラブル
デバイス
36

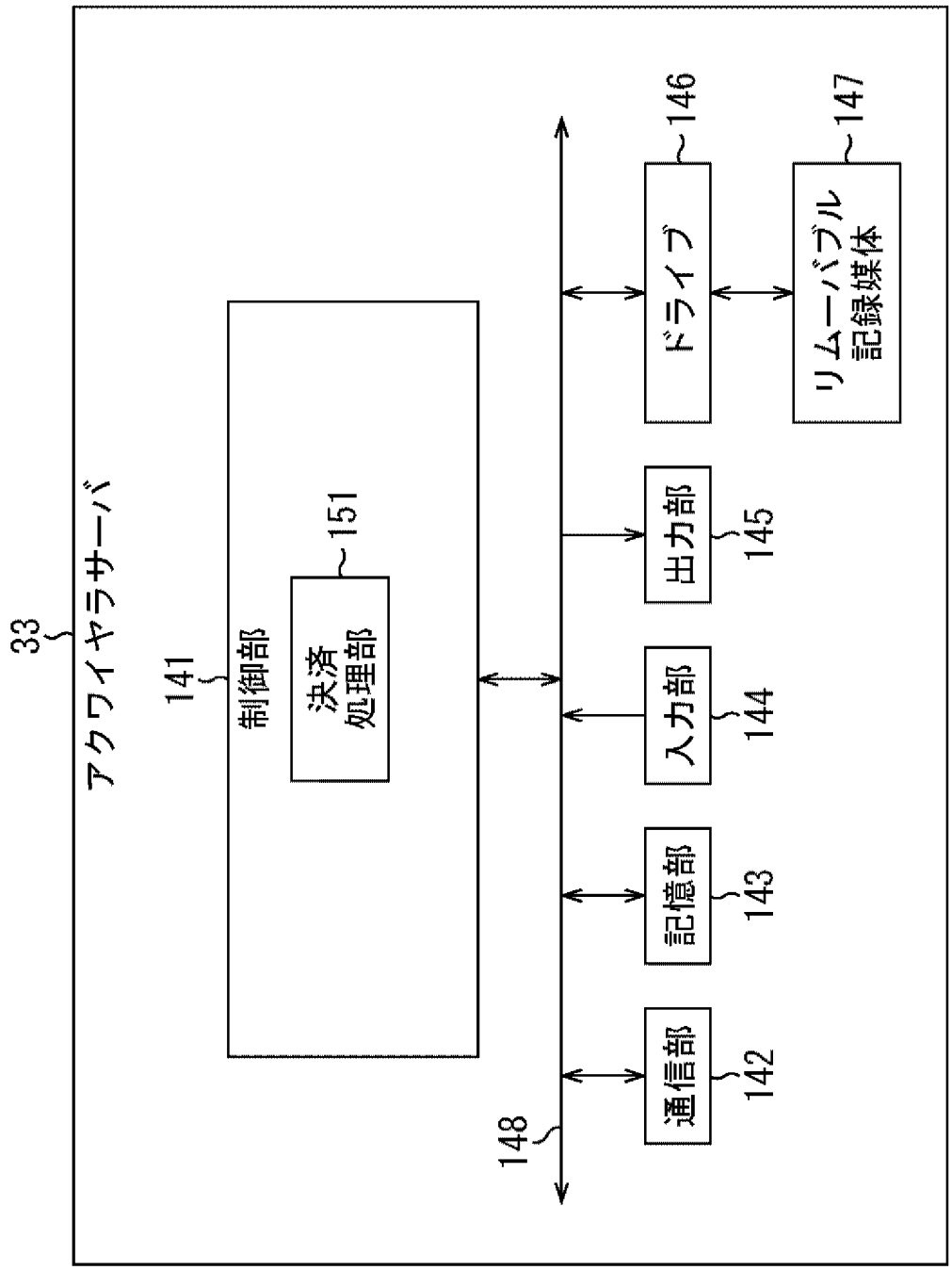
[図5]
FIG. 5


31
クライアント装置
51
制御部
決済処理部
71
チャレンジ処理部
72
登録処理部
73
59
GPS
58
56
ドライブ
57
リムーバブル記録媒体
出力部
55
入力部
54
記憶部
53
52
通信部
91
WiFi
92
LTE
93
Bluetooth
94
NFC

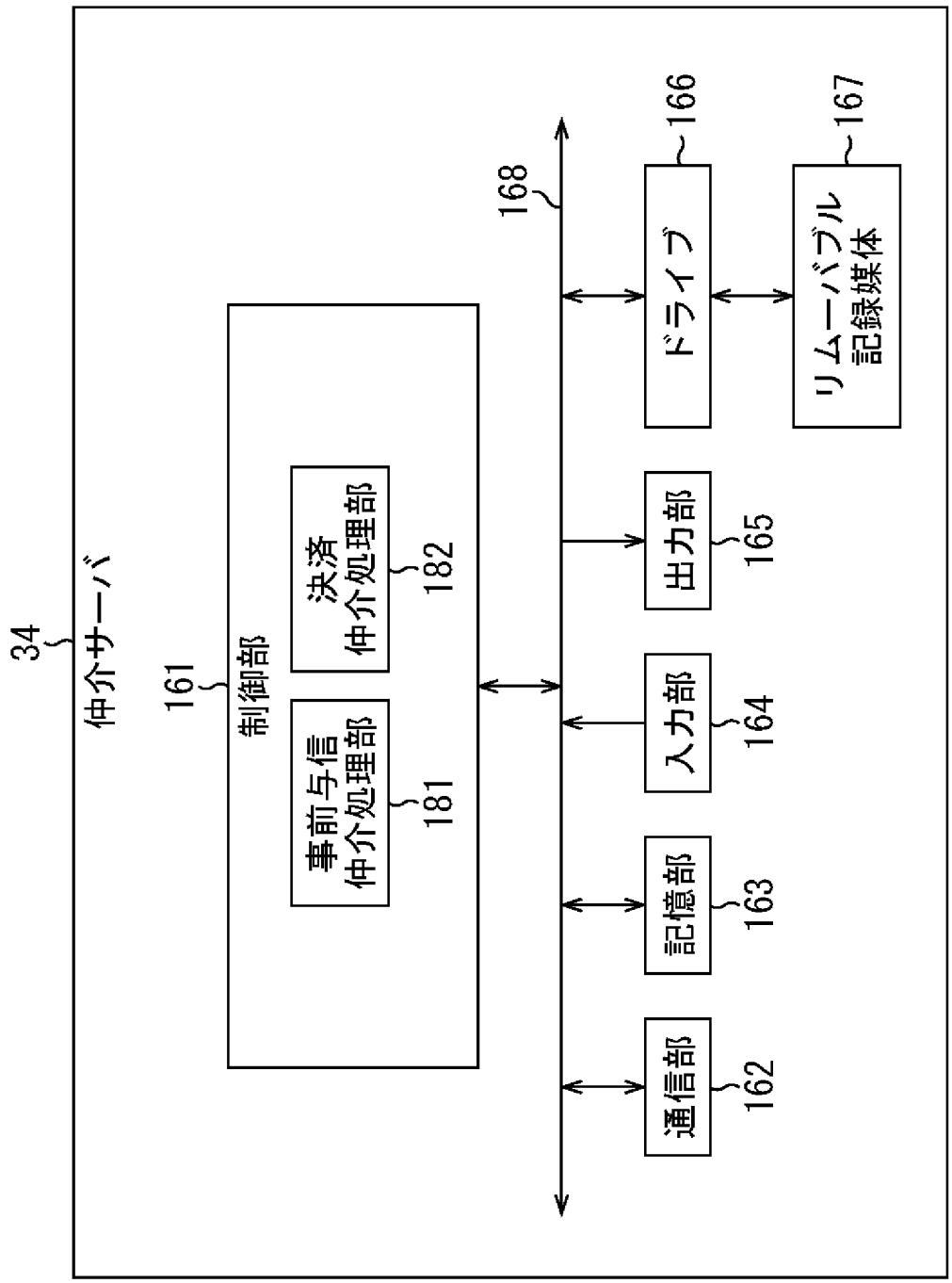
[図6]
FIG. 6


32
EC店舗サーバ
101
制御部
事前与信
処理部
121
決済
処理部
122
108
通信部
102
記憶部
103
入力部
104
出力部
105
ドライブ
106
リムーバブル
記録媒体
107

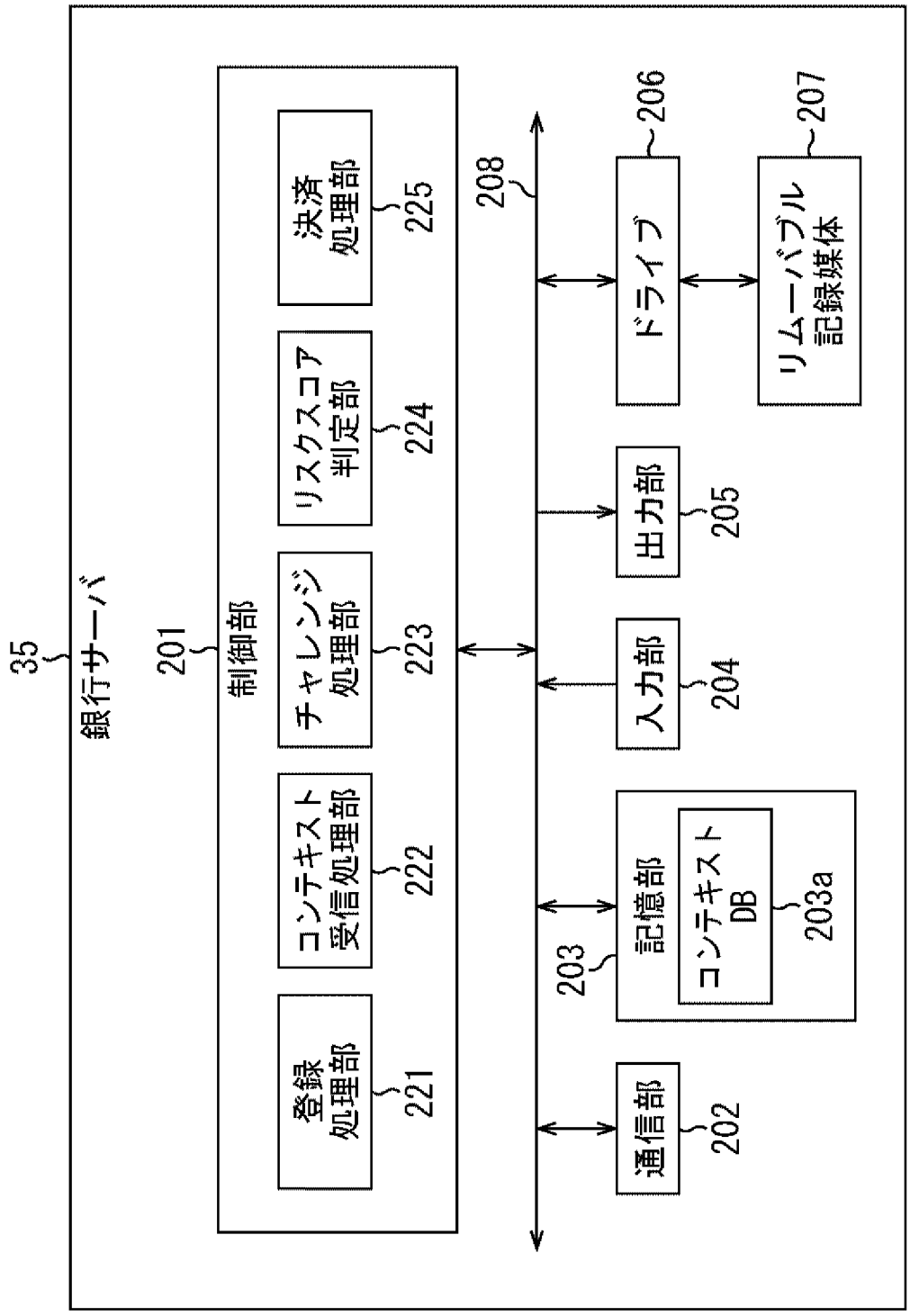
[図7]
FIG. 7


33
アクワイヤラサーバ
141
制御部
151
決済
処理部
148
通信部
142
記憶部
143
入力部
144
出力部
145
ドライブ
146
リムーバブル
記録媒体
147

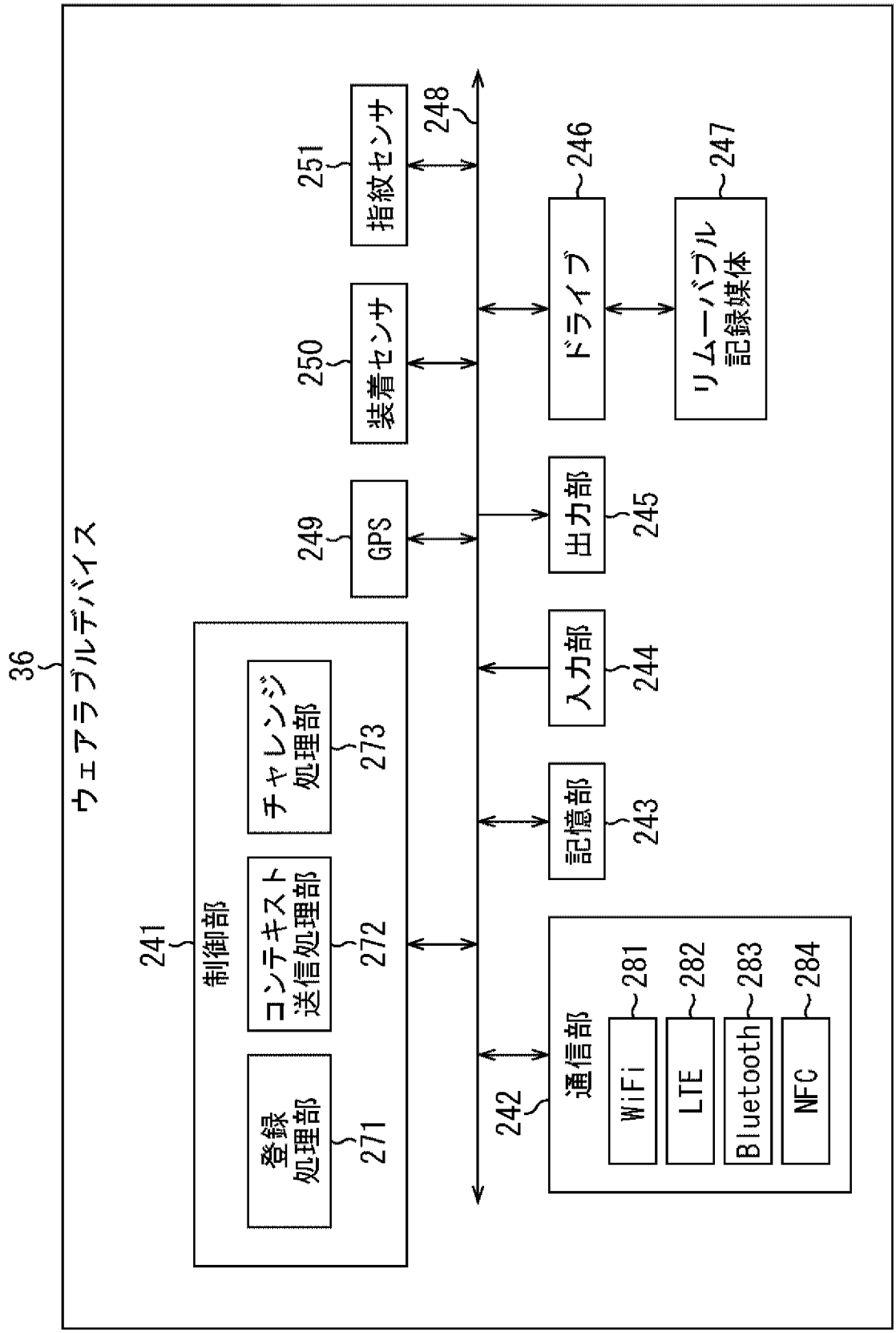
[図8]
FIG. 8


34
仲介サーバ
161
制御部
事前与信
仲介処理部
181
決済
仲介処理部
182
168
通信部
162
記憶部
163
入力部
164
出力部
165
ドライブ
166
リムーバブル
記録媒体
167

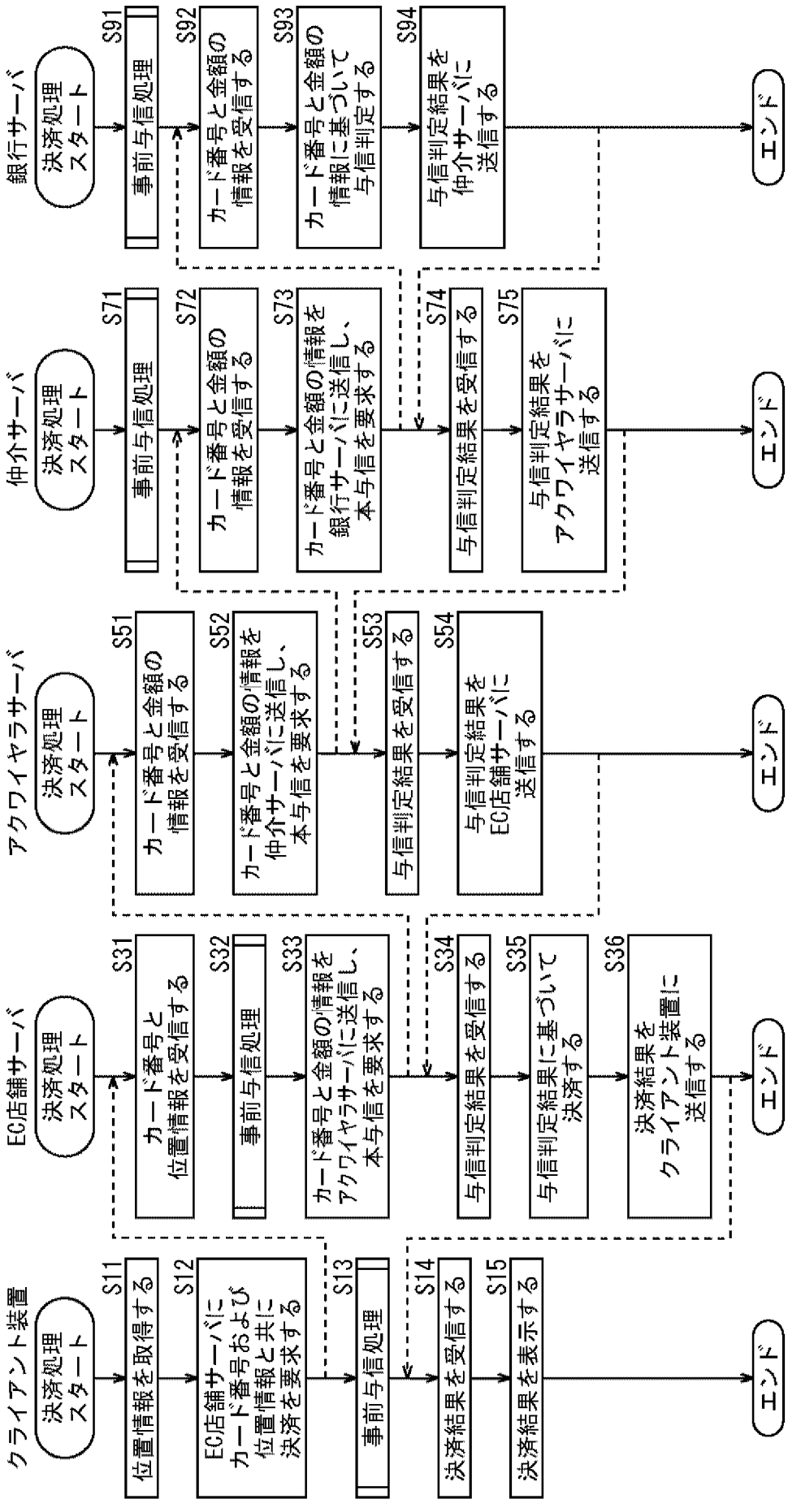
[図9]
FIG. 9


35
銀行サーバ
201
制御部
登録処理部
221
コンテキスト受信処理部
222
チャレンジ処理部
223
リスクスコア判定部
224
決済処理部
225
208
通信部
202
203
記憶部
コンテキストDB
203a
入力部
204
出力部
205
ドライブ
206
リムーバブル記録媒体
207

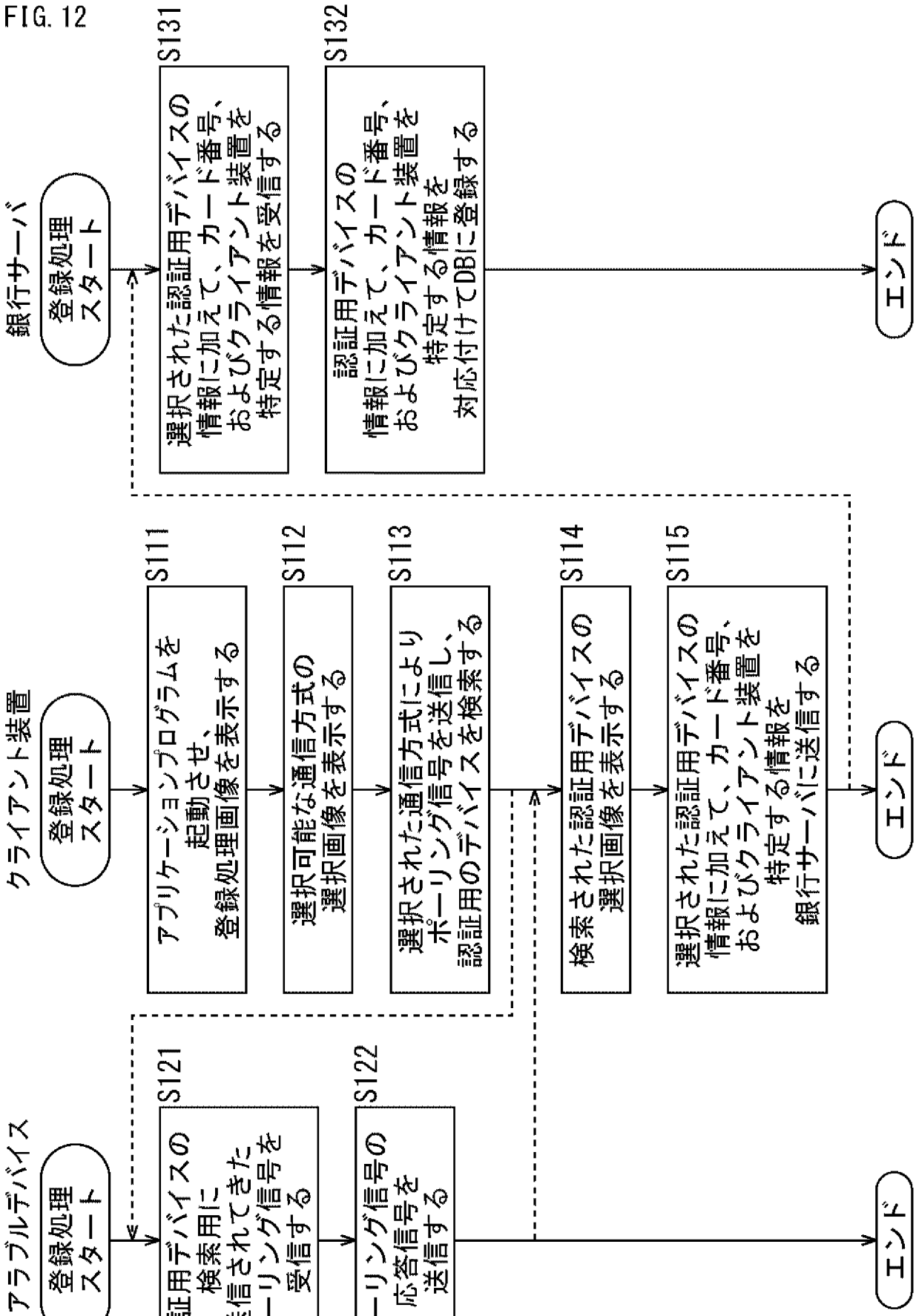
[図10]
FIG. 10


36
ウェアラブルデバイス
241
制御部
登録処理部
271
コンテキスト送信処理部
272
チャレンジ処理部
273
242
通信部
WiFi
281
LTE
282
Bluetooth
283
NFC
284
243
記憶部
244
入力部
245
出力部
249
GPS
250
装着センサ
251
指紋センサ
248
246
ドライブ
247
リムーバブル記録媒体

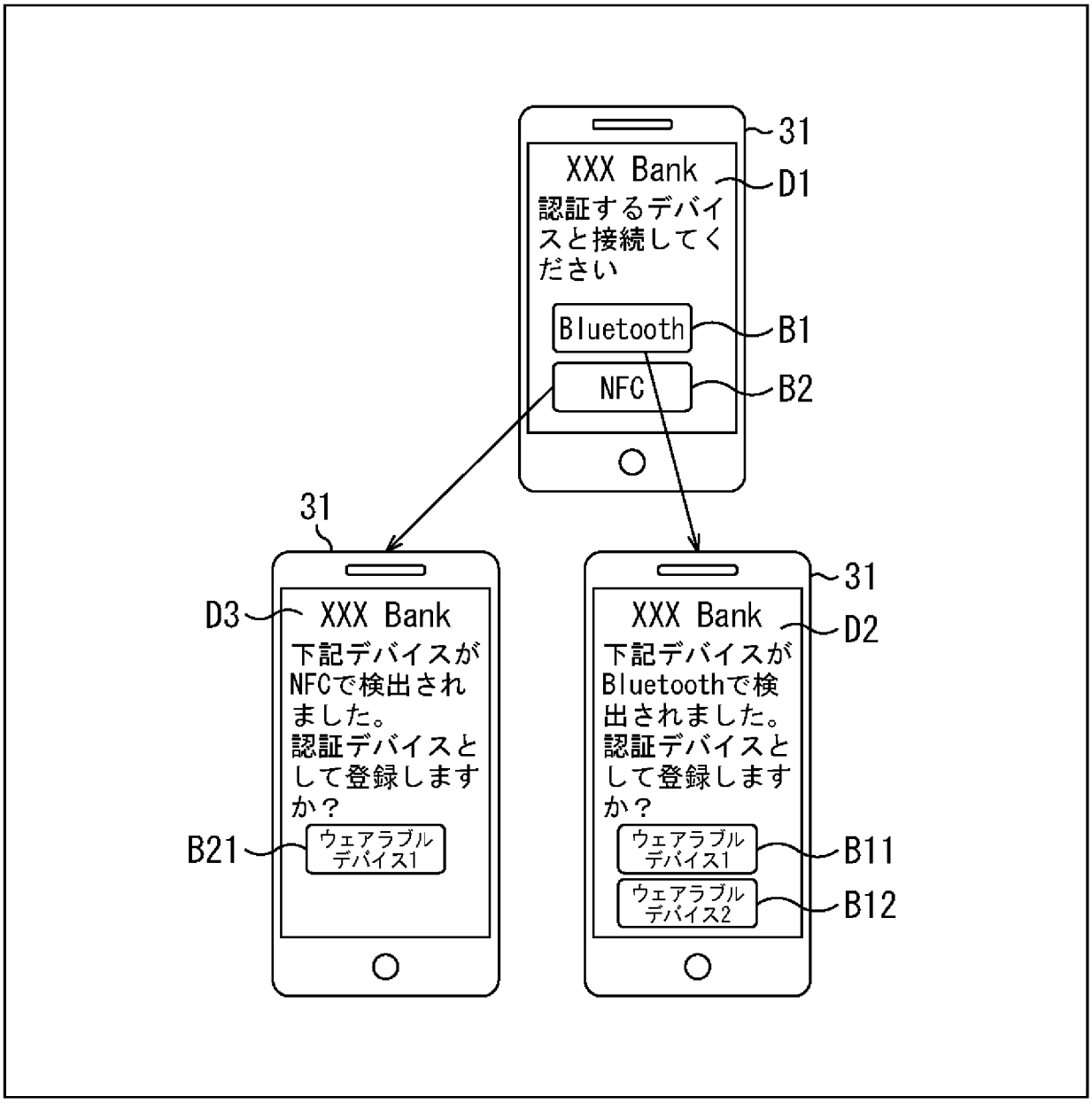
[図11]
FIG. 11


クライアント装置
決済処理スタート
S11
位置情報を取得する
S12
EC店舗サーバにカード番号および位置情報と共に決済を要求する
S13
事前与信処理
S14
決済結果を受信する
S15
決済結果を表示する
エンド
EC店舗サーバ
決済処理スタート
S31
カード番号と位置情報を受信する
S32
事前与信処理
S33
カード番号と金額の情報をアクワイヤラサーバに送信し、本与信を要求する
S34
与信判定結果を受信する
S35
与信判定結果に基づいて決済する
S36
決済結果をクライアント装置に送信する
エンド
アクワイヤラサーバ
決済処理スタート
S51
カード番号と金額の情報を受信する
S52
カード番号と金額の情報を仲介サーバに送信し、本与信を要求する
S53
与信判定結果を受信する
S54
与信判定結果をEC店舗サーバに送信する
エンド
仲介サーバ
決済処理スタート
S71
事前与信処理
S72
カード番号と金額の情報を受信する
S73
カード番号と金額の情報を銀行サーバに送信し、本与信を要求する
S74
与信判定結果を受信する
S75
与信判定結果をアクワイヤラサーバに送信する
エンド
銀行サーバ
決済処理スタート
S91
事前与信処理
S92
カード番号と金額の情報を受信する
S93
カード番号と金額の情報に基づいて与信判定する
S94
与信判定結果を仲介サーバに送信する
エンド

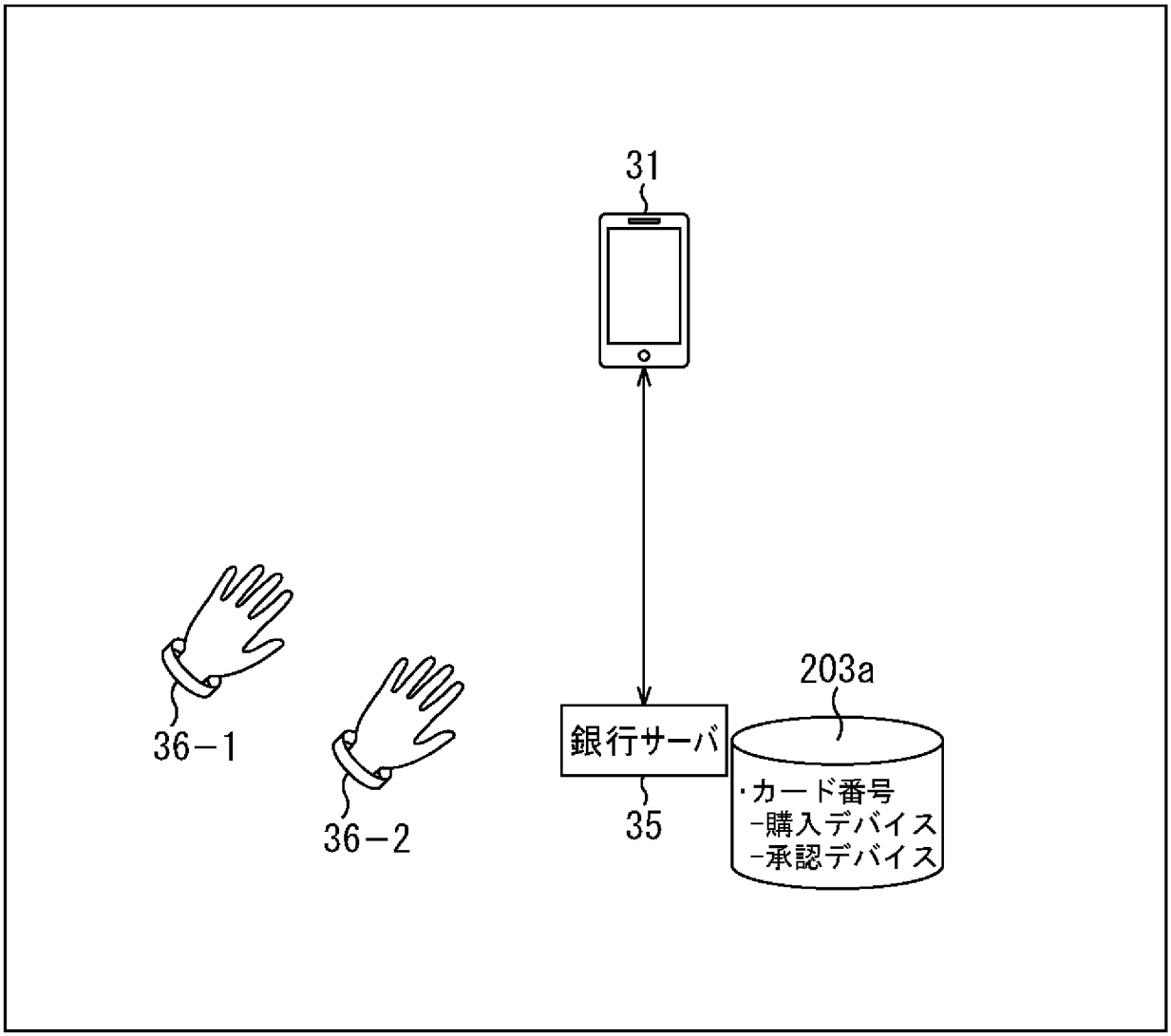
[図12]
FIG. 12


銀行サーバ
登録処理スタート
S131
選択された認証用デバイスの情報に加えて、カード番号、およびクライアント装置を特定する情報を受信する
S132
認証用デバイスの情報に加えて、カード番号、およびクライアント装置を特定する情報を対応付けてDBに登録する
エンド
クライアント装置
登録処理スタート
S111
アプリケーションプログラムを起動させ、登録処理画像を表示する
S112
選択可能な通信方式の選択画像を表示する
S113
選択された通信方式によりポーリング信号を送信し、認証用のデバイスを検索する
S114
検索された認証用デバイスの選択画像を表示する
S115
選択された認証用デバイスの情報に加えて、カード番号、およびクライアント装置を特定する情報を銀行サーバに送信する
エンド
ウェアラブルデバイス
登録処理スタート
S121
認証用デバイスの検索用に送信されてきたポーリング信号を受信する
S122
ポーリング信号の応答信号を送信する
エンド

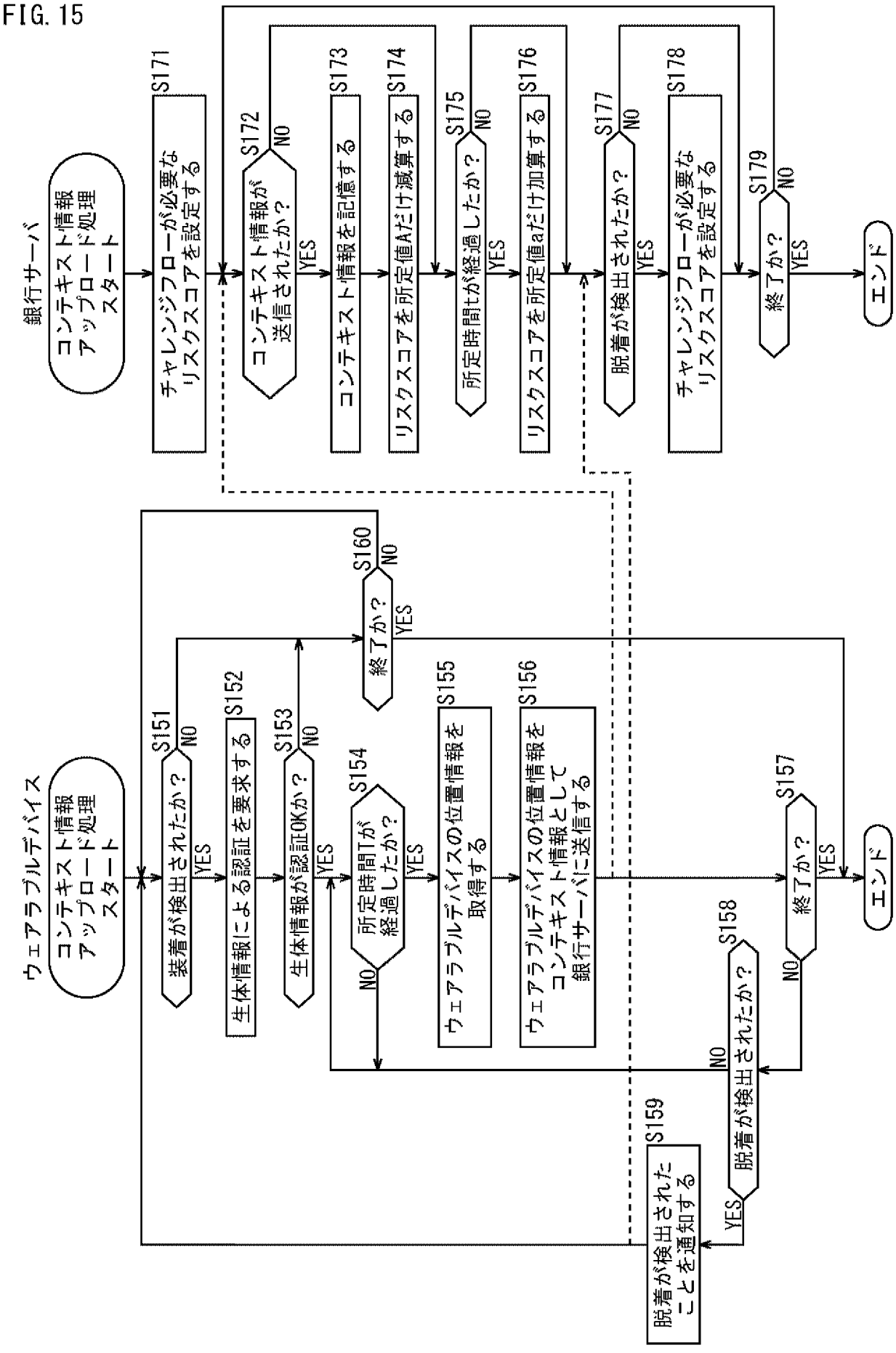
[図13]
FIG. 13


31
XXX Bank
D1
認証するデバイスと接続してください
Bluetooth
B1
NFC
B2
31
D3
XXX Bank
下記デバイスがNFCで検出されました。
認証デバイスとして登録しますか？
B21
ウェアラブルデバイス1
31
XXX Bank
D2
下記デバイスがBluetoothで検出されました。
認証デバイスとして登録しますか？
ウェアラブルデバイス1
B11
ウェアラブルデバイス2
B12

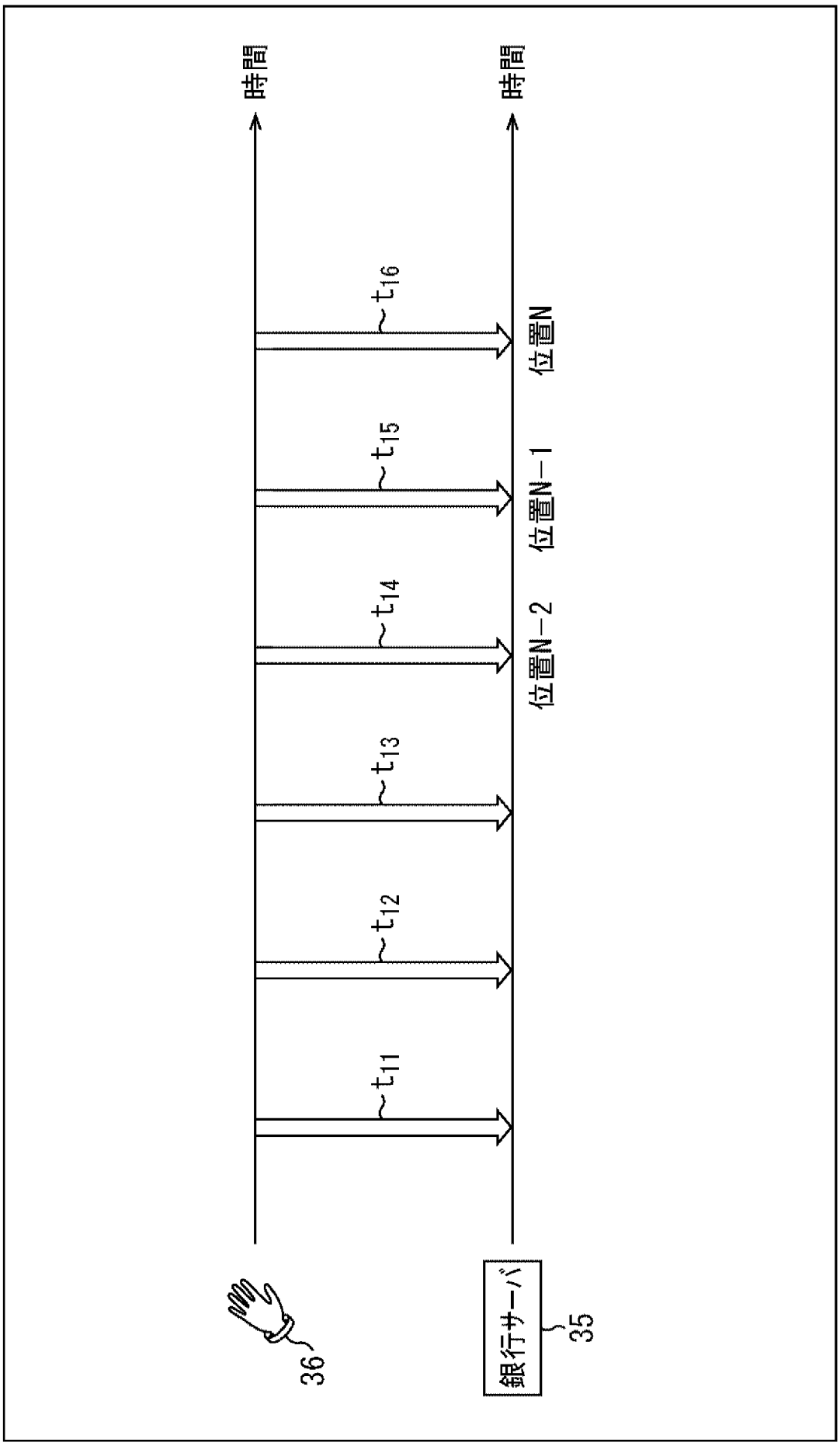
[図14]
FIG. 14



[図15]
FIG. 15

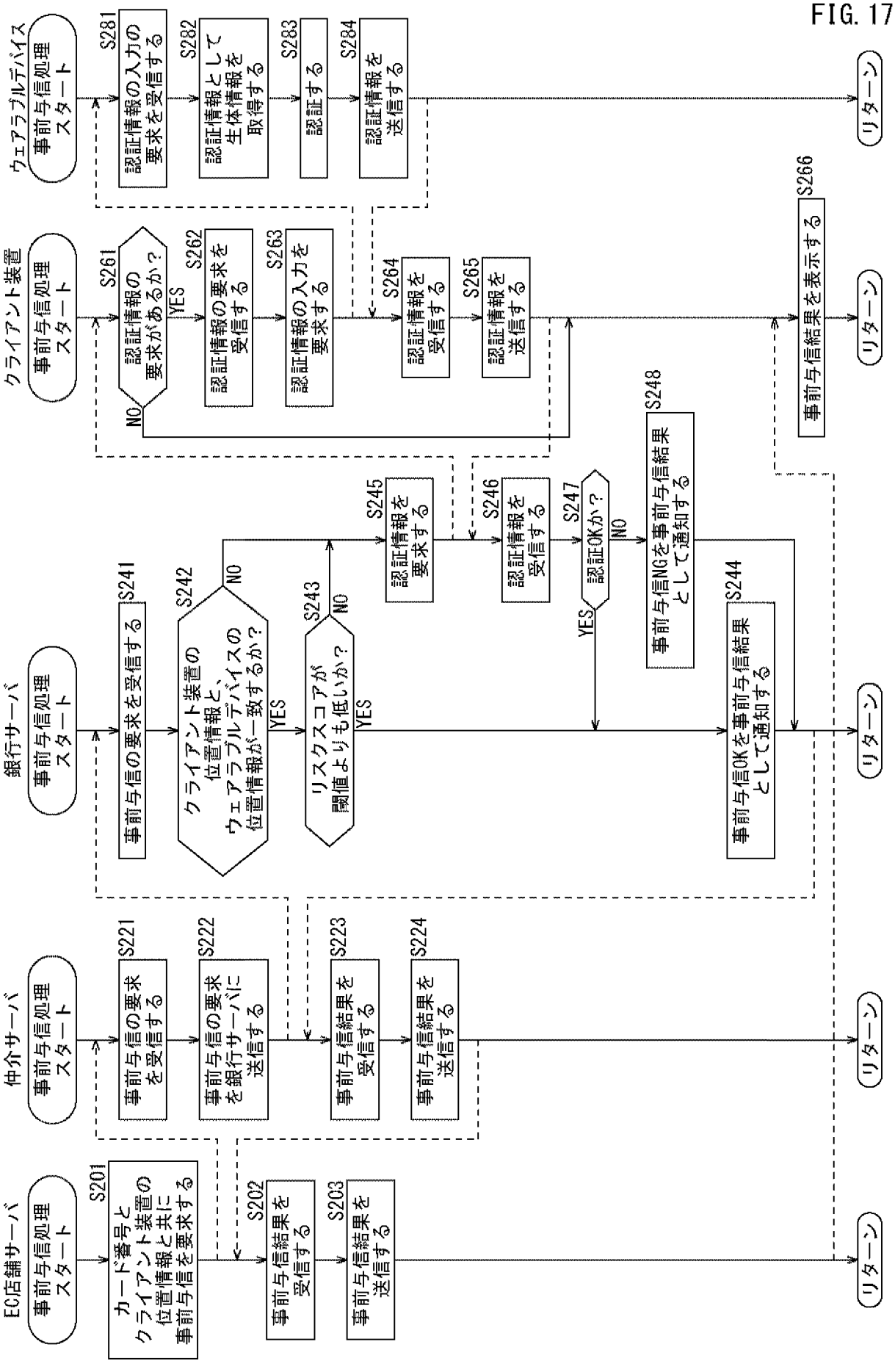

銀行サーバ
コンテキスト情報アップロード処理スタート
チャレンジフローが必要なリスクスコアを設定する
S171
コンテキスト情報が送信されたか？
S172
NO
YES
コンテキスト情報を記憶する
S173
リスクスコアを所定値Aだけ減算する
S174
所定時間tが経過したか？
S175
NO
YES
リスクスコアを所定値aだけ加算する
S176
脱着が検出されたか？
S177
NO
YES
チャレンジフローが必要なリスクスコアを設定する
S178
終了か？
S179
NO
YES
エンド
ウェアラブルデバイス
コンテキスト情報アップロード処理スタート
装着が検出されたか？
S151
NO
YES
生体情報による認証を要求する
S152
生体情報が認証OKか？
S153
NO
YES
所定時間Tが経過したか？
S154
NO
YES
ウェアラブルデバイスの位置情報を取得する
S155
ウェアラブルデバイスの位置情報をコンテキスト情報として銀行サーバに送信する
S156
終了か？
S157
NO
YES
エンド
脱着が検出されたか？
S158
NO
YES
脱着が検出されたことを通知する
S159
終了か？
S160
NO
YES

[図16]
FIG. 16

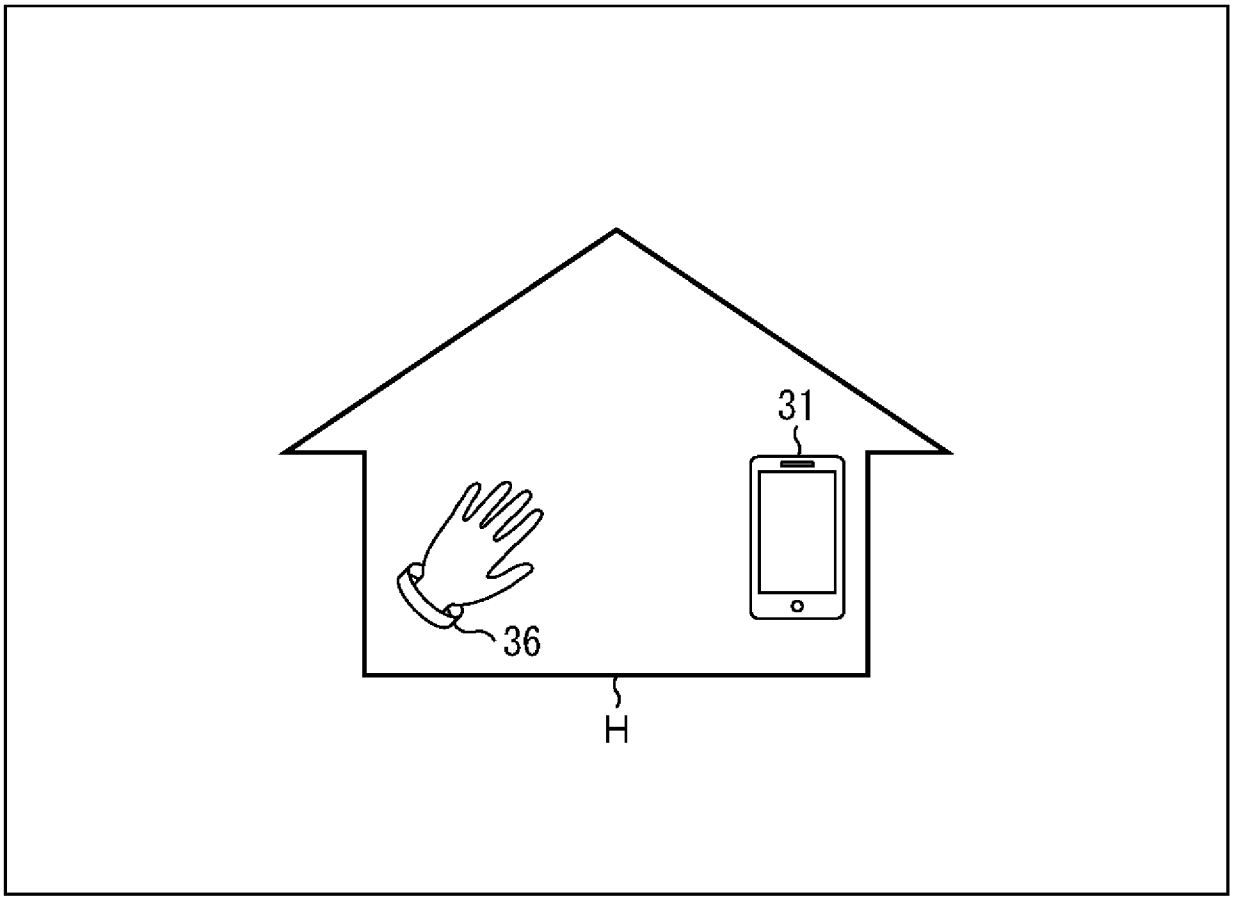


[図17]

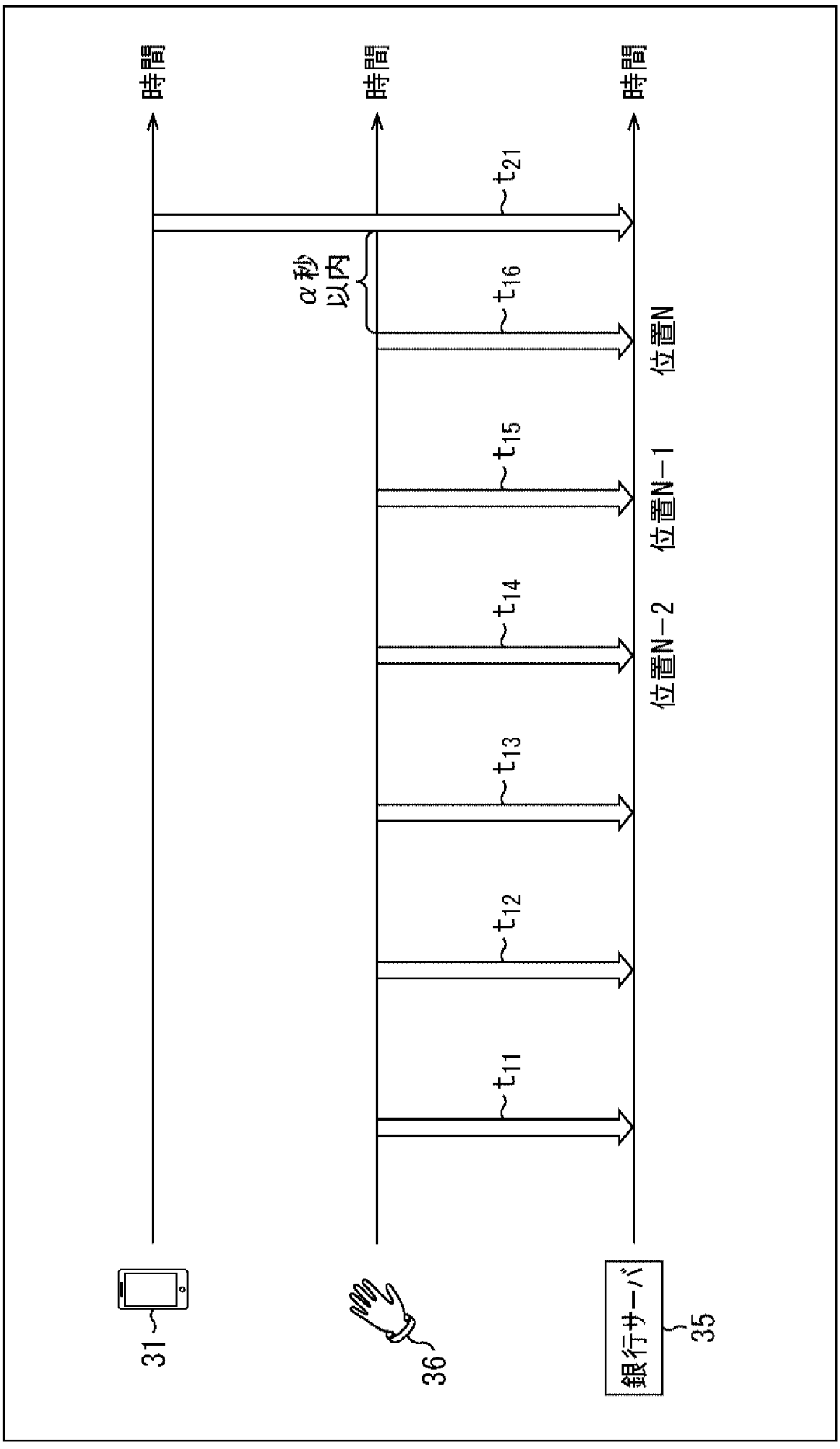
FIG. 17


EC店舗サーバ
事前与信処理スタート
S201
カード番号とクライアント装置の位置情報と共に事前与信を要求する
S202
事前与信結果を受信する
S203
事前与信結果を送信する
リターン
仲介サーバ
事前与信処理スタート
S221
事前与信の要求を受信する
S222
事前与信の要求を銀行サーバに送信する
S223
事前与信結果を受信する
S224
事前与信結果を送信する
リターン
銀行サーバ
事前与信処理スタート
S241
事前与信の要求を受信する
S242
クライアント装置の位置情報と、ウェアラブルデバイスの位置情報が一致するか？
NO
YES
S243
リスクスコアが閾値よりも低いか？
NO
YES
S244
事前与信OKを事前与信結果として通知する
S245
認証情報を要求する
S246
認証情報を受信する
S247
認証OKか？
NO
YES
S248
事前与信NGを事前与信結果として通知する
リターン
クライアント装置
事前与信処理スタート
S261
認証情報の要求があるか？
NO
YES
S262
認証情報の要求を受信する
S263
認証情報の入力を要求する
S264
認証情報を受信する
S265
認証情報を送信する
S266
事前与信結果を表示する
リターン
ウェアラブルデバイス
事前与信処理スタート
S281
認証情報の入力の要求を受信する
S282
認証情報として生体情報を取得する
S283
認証する
S284
認証情報を送信する
リターン

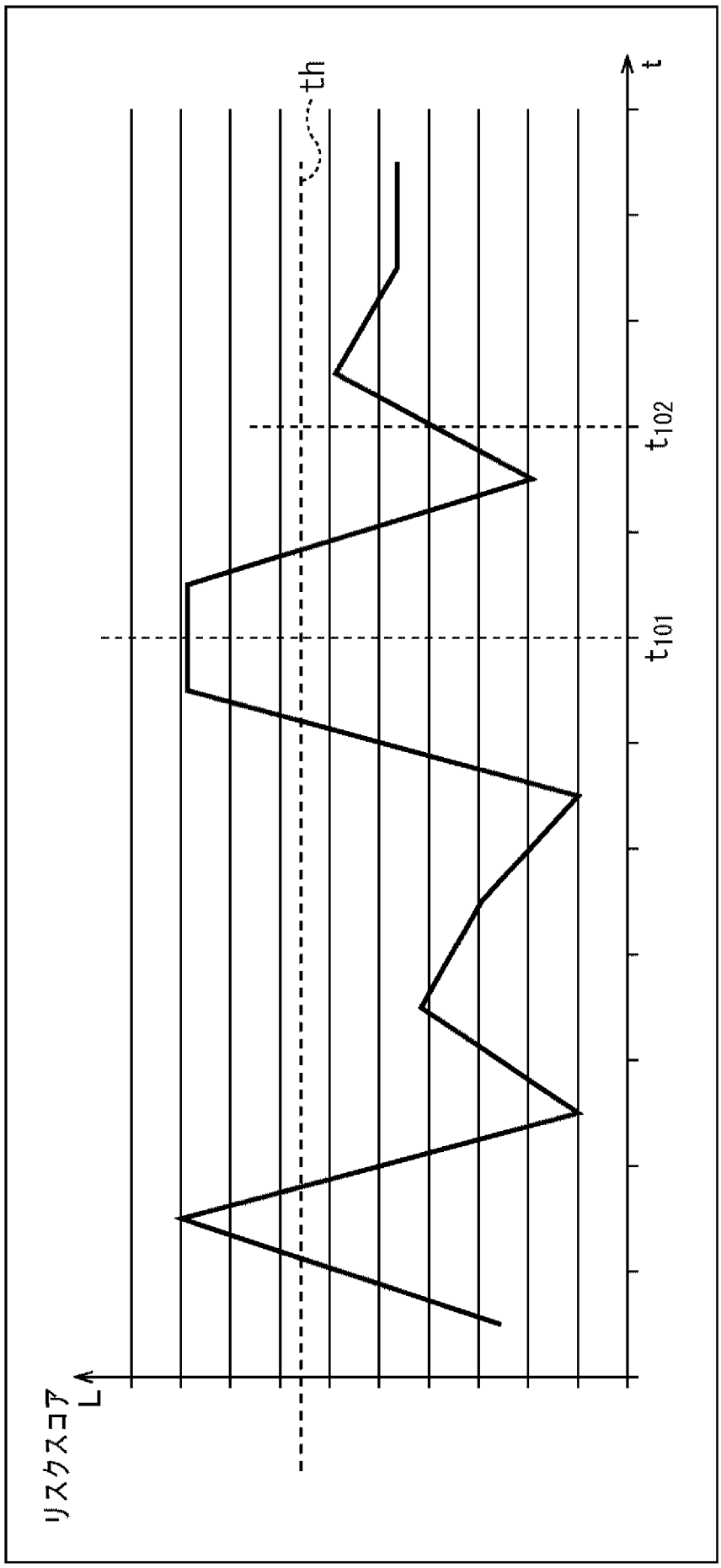
[図18]
FIG. 18



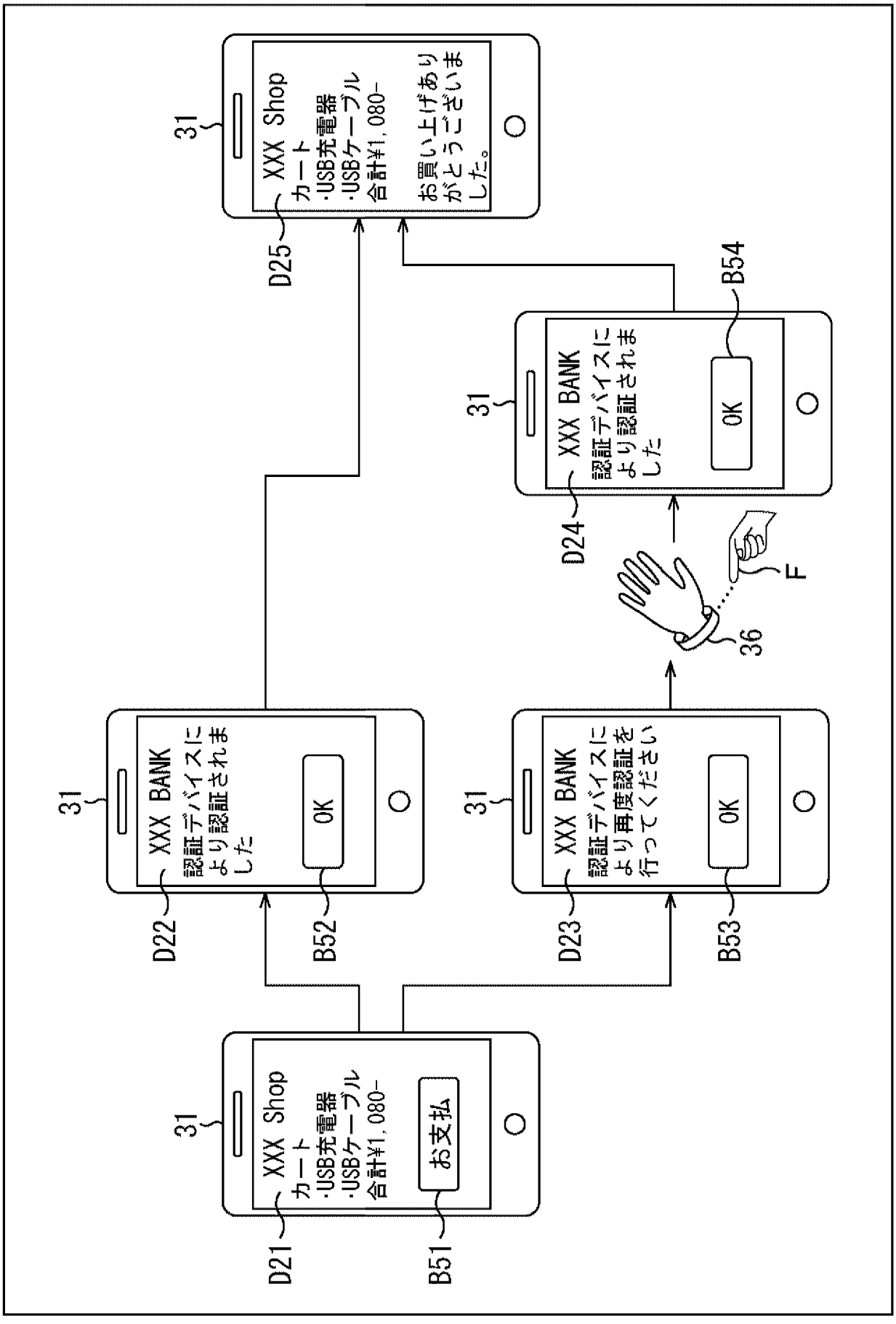
[図19]
FIG. 19


時間
時間
時間
t_{21}
α秒以内
t_{16}
位置N
t_{15}
位置N−1
t_{14}
位置N−2
t_{13}
t_{12}
t_{11}
31
36
銀行サーバ
35

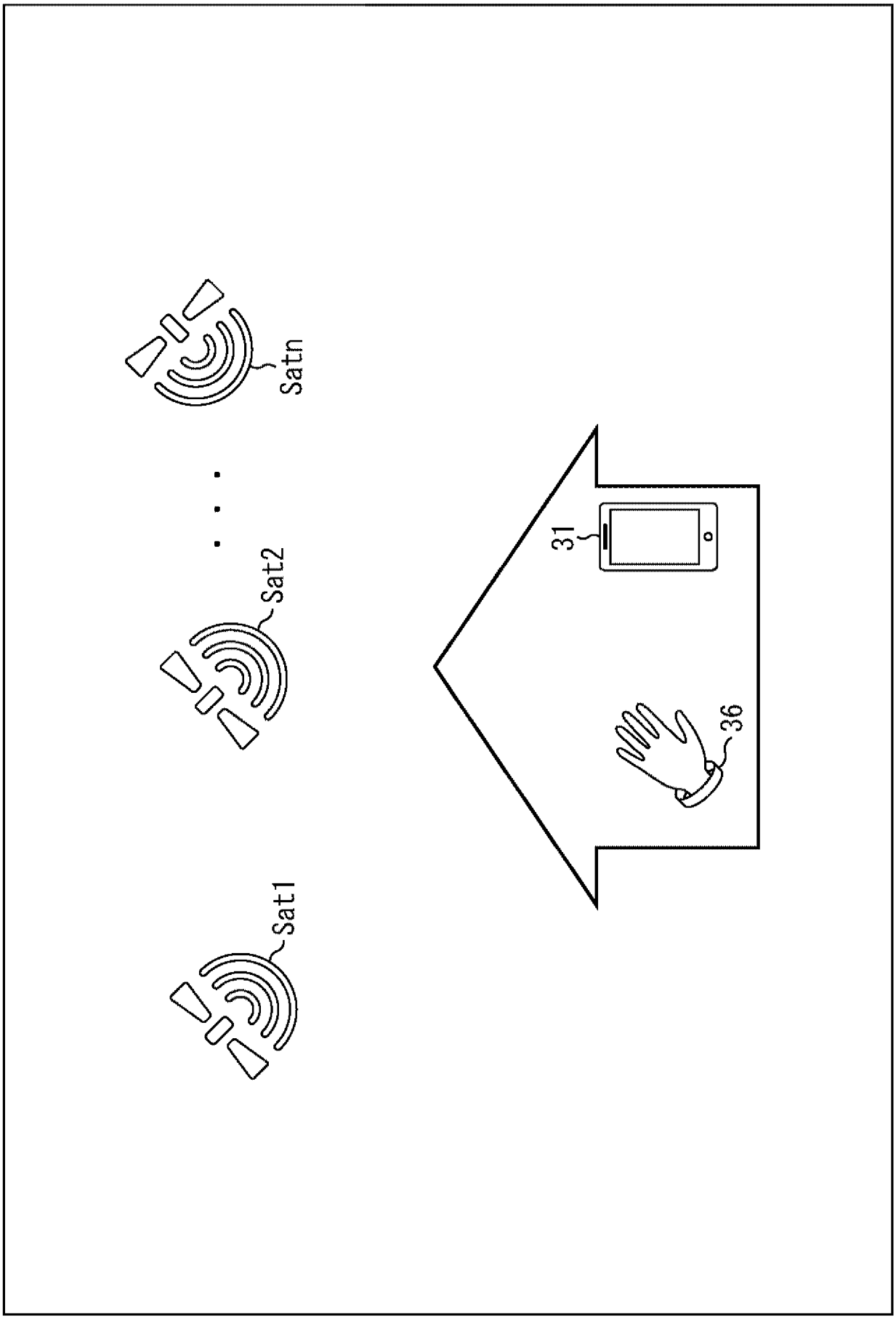
[図20]
FIG. 20



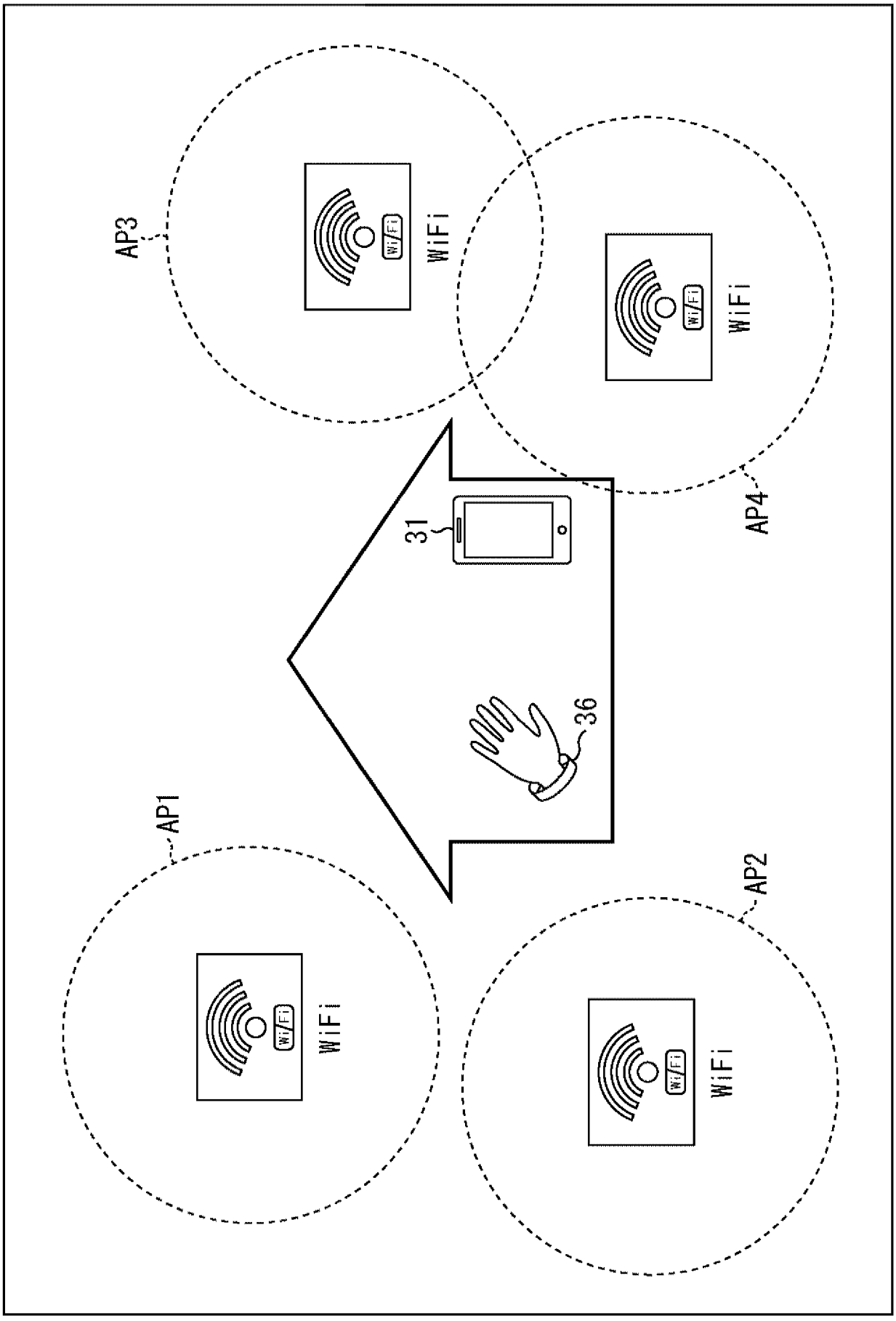
[図21]
FIG. 21


31
XXX Shop
カート
・USB充電器
・USBケーブル
合計¥1,080-
お支払
D21
B51
31
XXX BANK
認証デバイスにより認証されました
OK
D22
B52
31
XXX BANK
認証デバイスにより再度認証を行ってください
OK
D23
B53
31
XXX BANK
認証デバイスにより認証されました
OK
D24
B54
31
XXX Shop
カート
・USB充電器
・USBケーブル
合計¥1,080-
お買い上げありがとうございました。
D25
F
36

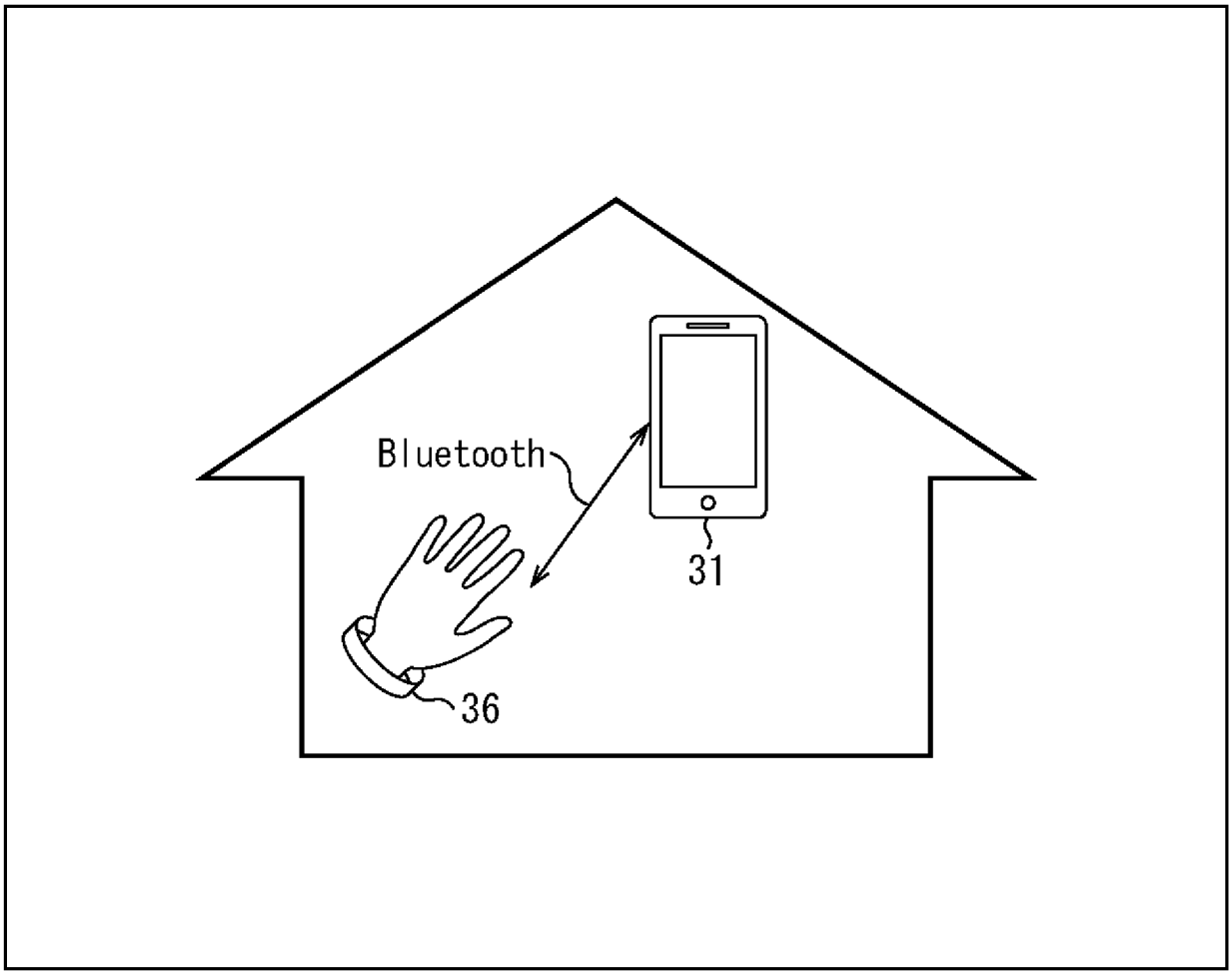
[図22]
FIG. 22



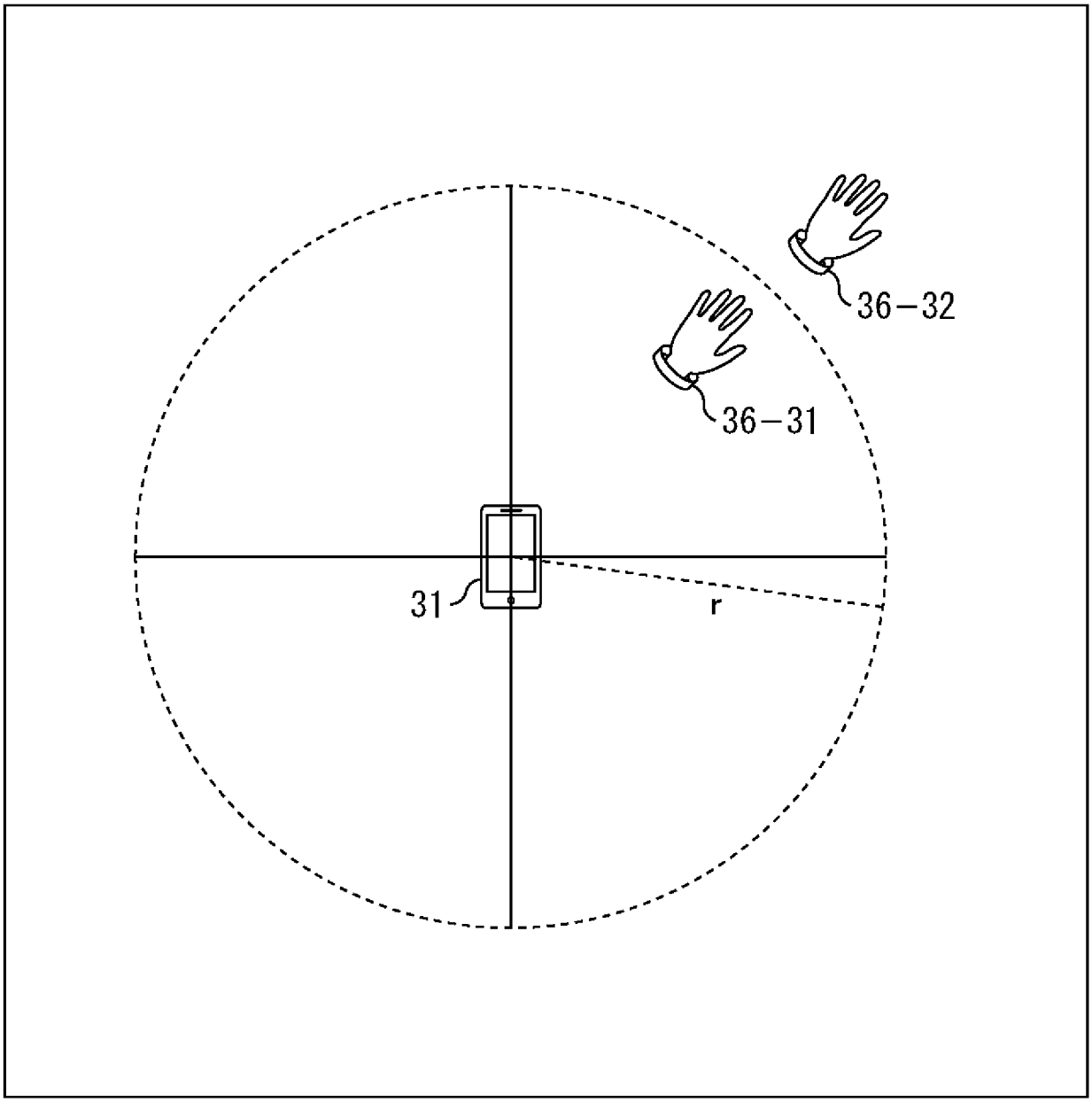
[図23]
FIG. 23



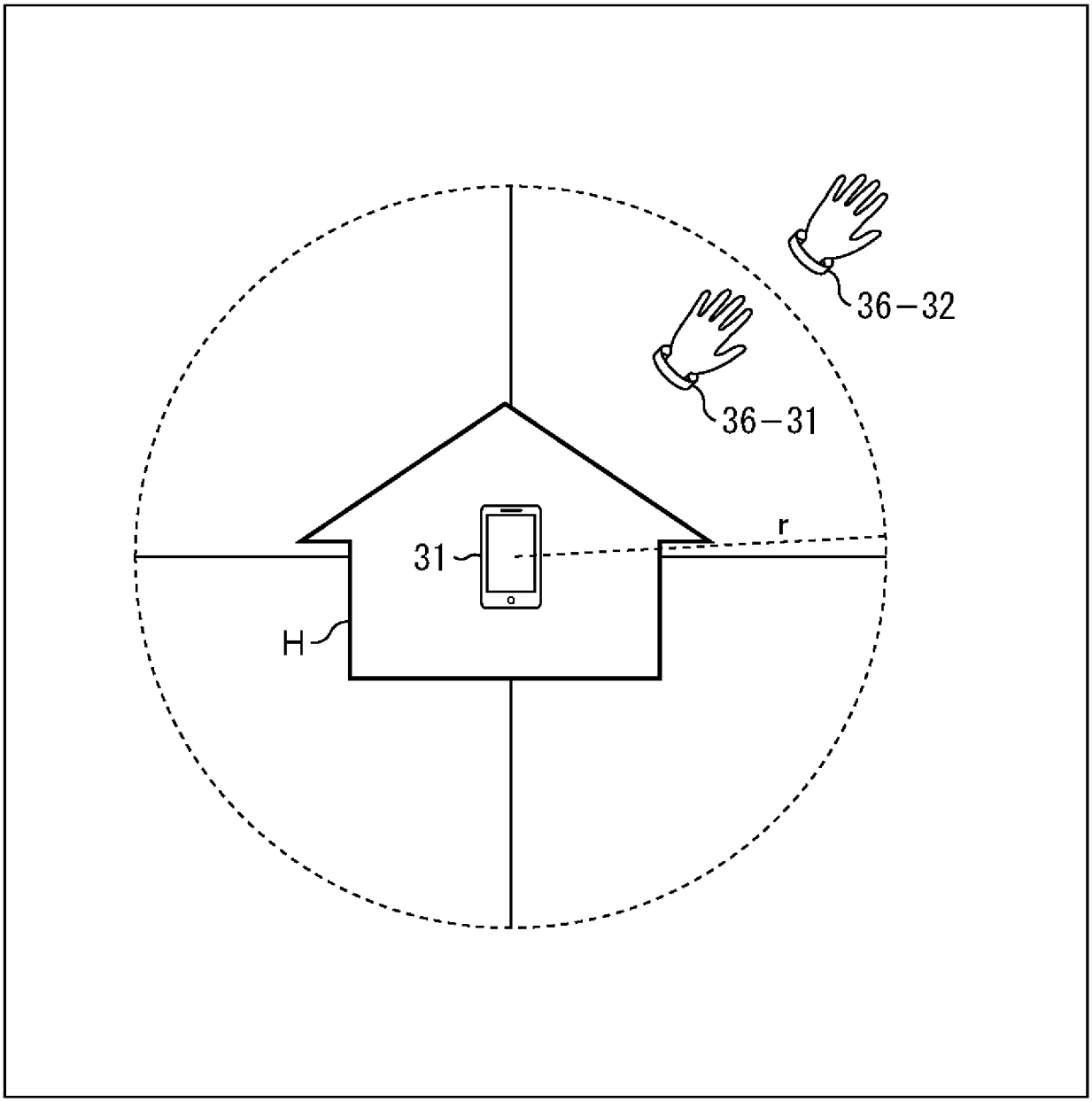
[図24]
FIG. 24



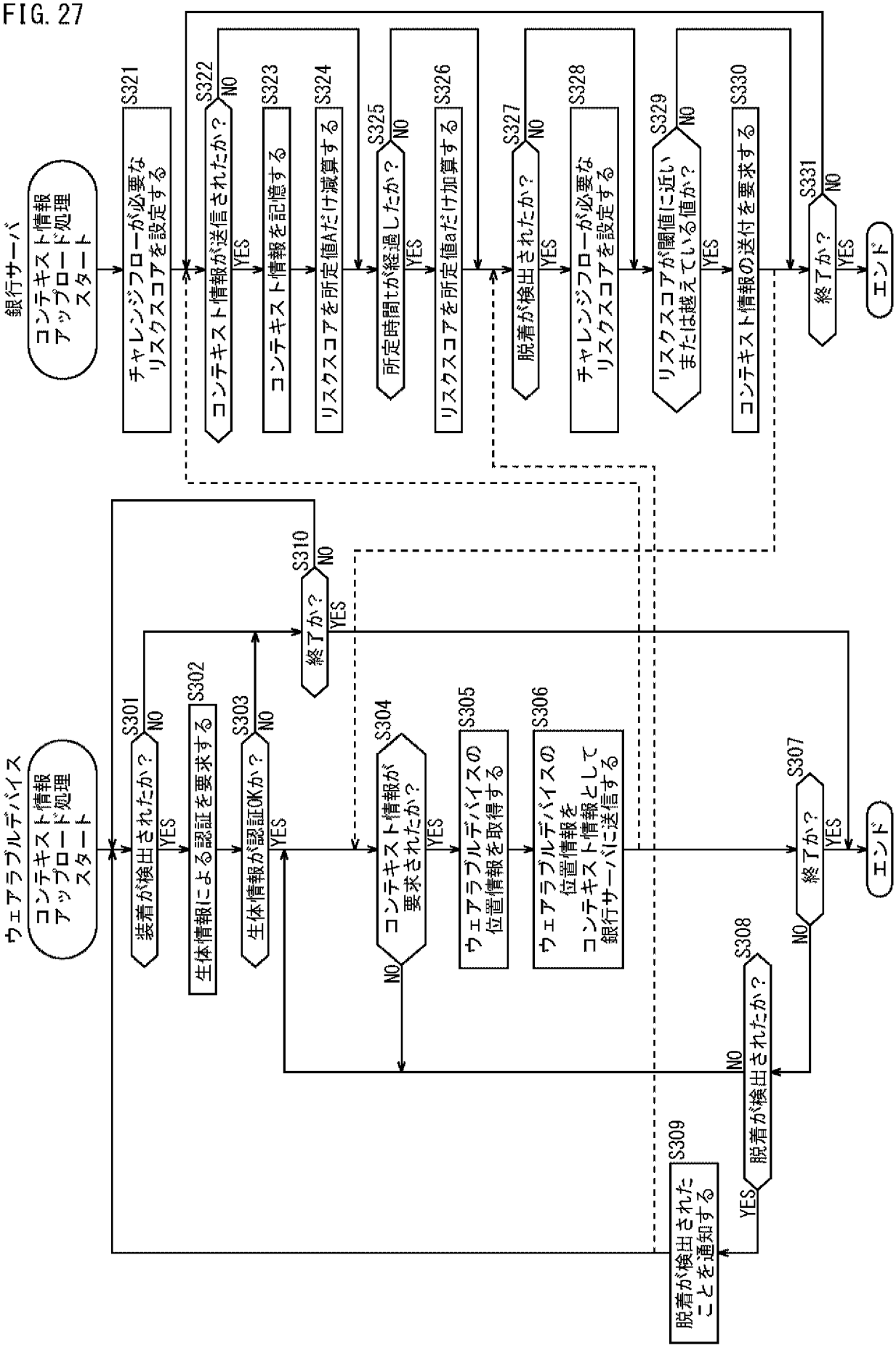
[図25]
FIG. 25



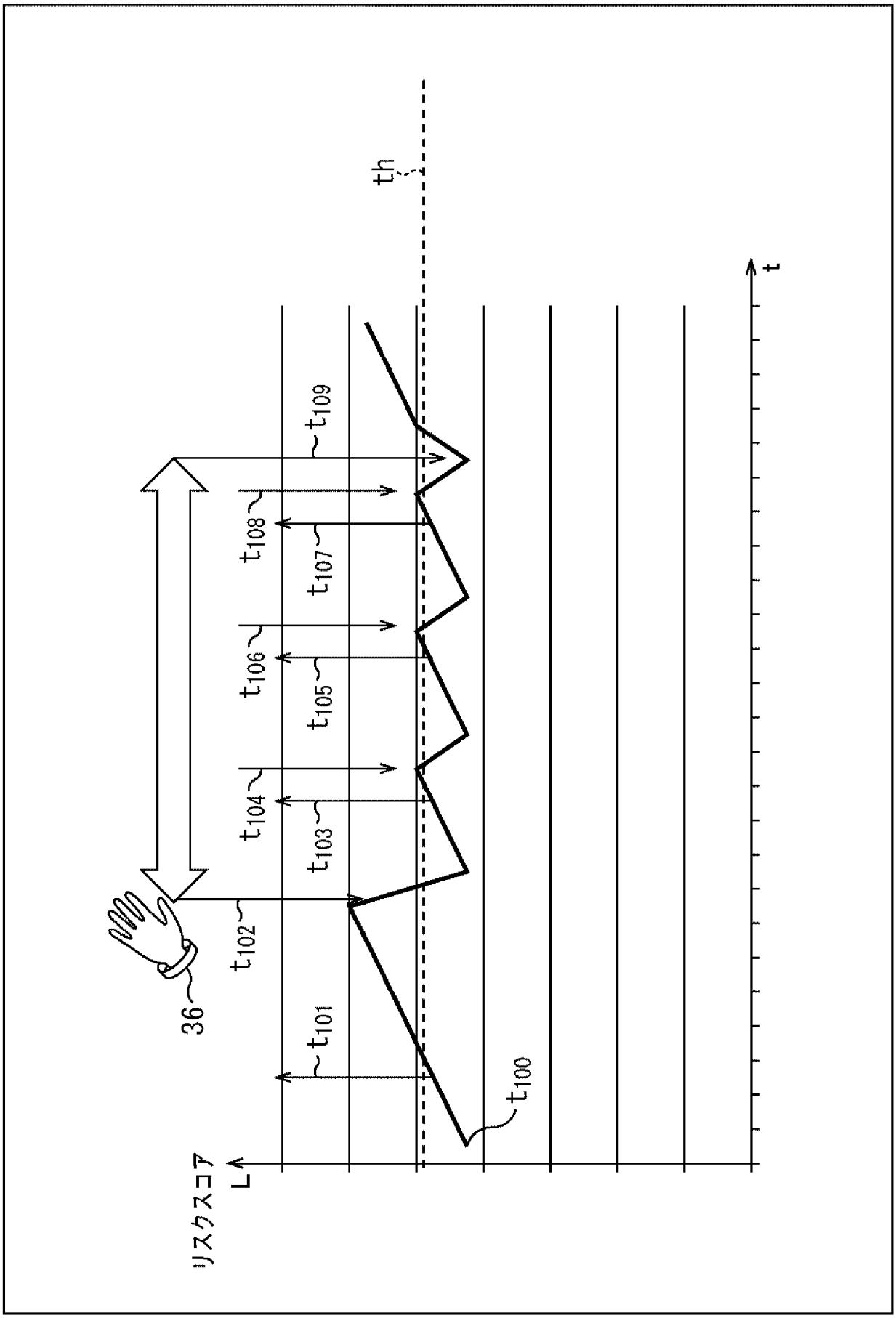
[図26]
FIG. 26



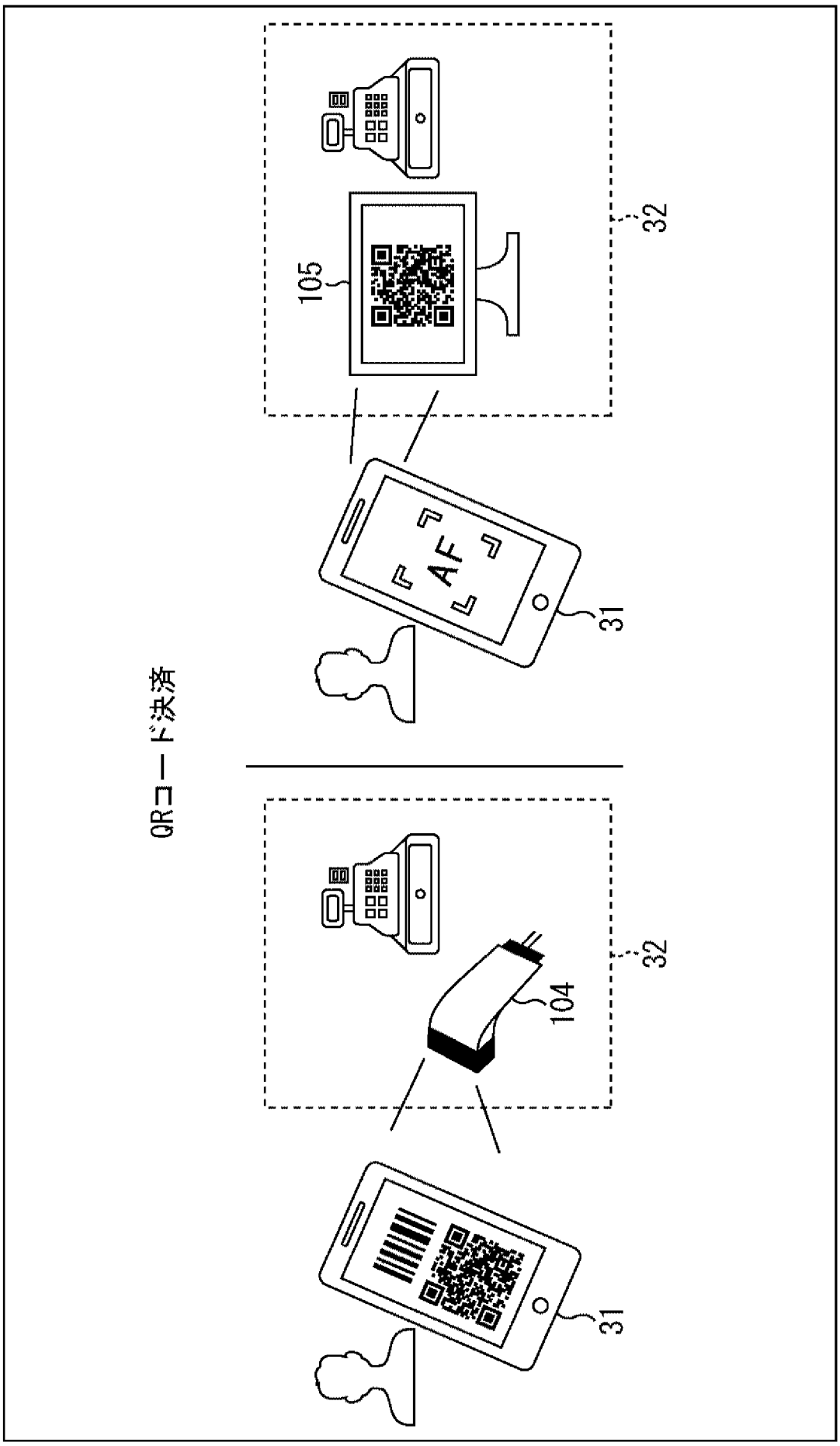
[図27]
FIG. 27


銀行サーバ
コンテキスト情報アップロード処理スタート
S321
チャレンジフローが必要なリスクスコアを設定する
S322
コンテキスト情報が送信されたか？
NO
YES
S323
コンテキスト情報を記憶する
S324
リスクスコアを所定値Aだけ減算する
S325
所定時間tが経過したか？
NO
YES
S326
リスクスコアを所定値aだけ加算する
S327
脱着が検出されたか？
NO
YES
S328
チャレンジフローが必要なリスクスコアを設定する
S329
リスクスコアが閾値に近いまたは越えている値か？
NO
YES
S330
コンテキスト情報の送付を要求する
S331
終了か？
NO
YES
エンド
ウェアラブルデバイス
コンテキスト情報アップロード処理スタート
S301
装着が検出されたか？
NO
YES
S302
生体情報による認証を要求する
S303
生体情報が認証OKか？
NO
YES
S304
コンテキスト情報が要求されたか？
NO
YES
S305
ウェアラブルデバイスの位置情報を取得する
S306
ウェアラブルデバイスの位置情報をコンテキスト情報として銀行サーバに送信する
S307
終了か？
NO
YES
エンド
S308
脱着が検出されたか？
NO
YES
S309
脱着が検出されたことを通知する
S310
終了か？
NO
YES

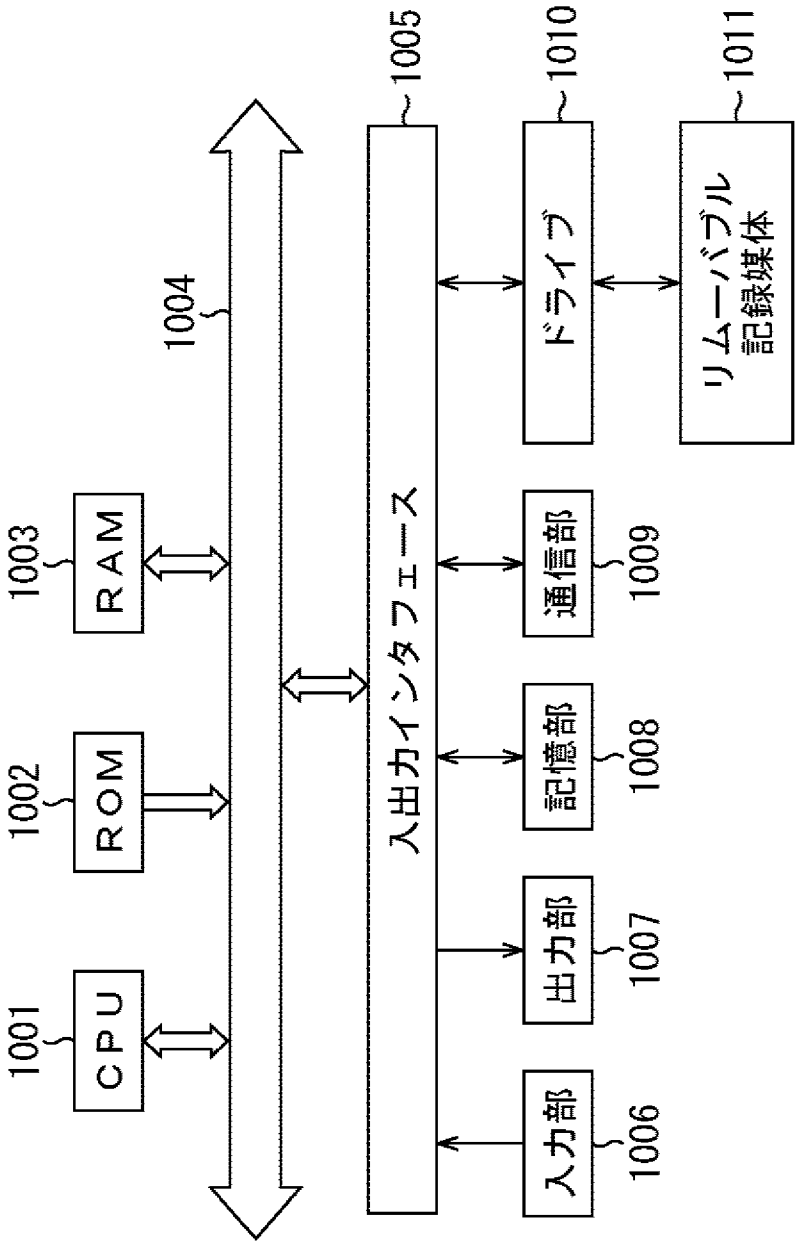
[図28]
FIG. 28


th
t
t109
t108
t107
t106
t105
t104
t103
t102
t101
t100
36
リスクスコア
L

[図29]
FIG. 29



[図30]
FIG. 30


1001
CPU
1002
ROM
1003
RAM
1004
1005
入出力インタフェース
1006
入力部
1007
出力部
1008
記憶部
1009
通信部
1010
ドライブ
1011
リムーバブル
記録媒体

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/031661

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G06Q20/40(2012.01)i, G06Q20/32(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl. G06Q20/40, G06Q20/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2018
Registered utility model specifications of Japan 1996-2018
Published registered utility model applications of Japan 1994-2018

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2015-121910 A (HITACHI, LTD.) 02 July 2015, abstract, paragraphs [0002]-[0013], [0018], [0045]-[0049], [0056]-[0062] & US 2016/0224779 A1, abstract, paragraphs [0002]-[0013], [0027], [0054]-[0058], [0065]-[0071] & WO 2015/098384 A1 & EP 3089062 A1	1, 13 2-12, 15-19
Y	JP 2007-514333 A (RSA SECURITY, INC.) 31 May 2007, claim 1, paragraphs [0028], [0031], [0054] & US 2005/0097320 A1, claim 1, paragraphs [0034], [0037], [0060] & WO 2005/025292 A2 & CN 101073219 A	2-12, 15-19

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
11.10.2018	23.10.2018
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/031661

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 2015-121840 A (TOSHIBA CORP.) 02 July 2015, paragraphs [0019]-[0021] & US 2015/0181368 A1, paragraphs [0022]-[0024]	8-12
X Y	US 2017/0185103 A1 (IRITECH, INC.) 29 June 2017, claims 41-43, paragraphs [0146], [0153], [0154], [0232]-[0234], [0247]-[0249] & JP 2017-531843 A & WO 2016/006927 A1 & KR 10-2016-0006912 A & CN 107077597 A	14, 20 11-12, 18-19
Y	JP 2017-134689 A (KDDI CORP.) 03 August 2017, paragraph [0034] (Family: none)	11-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０３１６６１

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, G06Q20/32(2012.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06Q20/40, G06Q20/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８年

国際調査で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
X	JP 2015-121910 A（株式会社日立製作所）2015.07.02,　［要約］、段落［０００２］～［００１３］、［００１８］、	1,13
Y	［００４５］～［００４９］、［００５６］～［００６２］ & US 2016/0224779 A1,[要約],段落[0002]～[0013],[0027],[0054]～[0058],[0065]～[0071] & WO 2015/098384 A1 & EP 3089062 A1	2-12,15-19

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

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１１．１０．２０１８	２３．１０．２０１８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｌ　３７８６
山本　雅士
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 2007-514333 A (アールエスエイ　セキュリティー　インコーポレーテッド) 2007.05.31, ［請求項１］、段落［００２８］、［００３１］、［００５４］ & US 2005/0097320 A1,[請求項１],段落[0034],[0037],[0060] & WO 2005/025292 A2 & CN 101073219 A	2-12,15-19
Y	JP 2015-121840 A (株式会社東芝) 2015.07.02, 段落［００１９］～［００２１］ & US 2015/0181368 A1,段落[0022]～[0024]	8-12
X	US 2017/0185103 A1 (IRITECH, INC.) 2017.06.29, ［請求項４１］-[請求項４３],段落[０１４６]、	14,20
Y	[０１５３]～[０１５４]、[０２３２]～[０２３４]、[０２４７]～[０２４９] & JP 2017-531843 A & WO 2016/006927 A1 & KR 10-2016-0006912 A & CN 107077597 A	11-12,18-19
Y	JP 2017-134689 A (ＫＤＤＩ株式会社) 2017.08.03, 段落［００３４］（ファミリーなし）	11-12