(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
2010 年 2 月 11 日(11.02.2010)

PCT

(10) 国際公開番号
WO 2010/016163 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)　*G06Q 20/00* (2006.01)
G06F 21/20 (2006.01)　*H04L 9/32* (2006.01)
G06F 21/24 (2006.01)

(21) 国際出願番号: PCT/JP2009/000517

(22) 国際出願日: 2009 年 2 月 9 日(09.02.2009)

(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 2008-204894 2008 年 8 月 7 日(07.08.2008) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社ＩＣＯＮ (ICON Corp.) [JP/JP]; 〒2210056 神奈川県横浜市神奈川区金港町５番地３６ Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 土屋敏子 (TSUCHIYA, Toshiko) [JP/JP]; 〒2210056 神奈川県横浜市神奈川区金港町５番地３６株式会社ＩＣＯＮ内 Kanagawa (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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

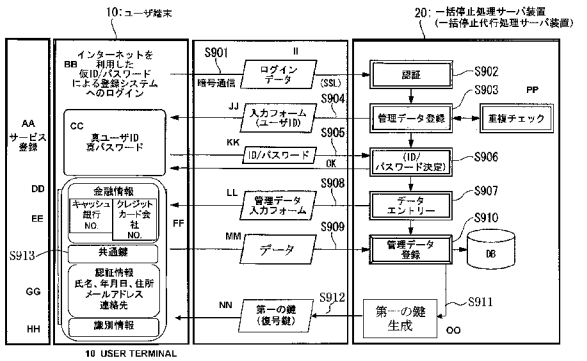
添付公開書類:
— 国際調査報告（条約第 21 条(3)）

[続葉有]

(54) **Title**: COLLECTIVE SUSPENSION/SETTLEMENT REPRESENTATION PROCESSING SERVER DEVICE AND PROGRAM

(54) 発明の名称: 一括停止処理／決済代行処理サーバ装置及びプログラム

[図5]



10 USER TERMINAL
20 COLLECTIVE SUSPENSION PROCESSING SERVER DEVICE (COLLECTIVE SUSPENTION REPRESENTATION PROCESSING SERVER DEVICE)
AA REGISTRATION OF SERVICES
BB LOG IN TO REGISTRATION SYSTEM USING TEMPORARY ID/PASSWORD OVER THE INTERNET
CC ACTUAL USER ID AND PASSWORD
DD FINANCIAL INFORMATION
EE BANK CASH CARD NUMBER
FF CREDIT CARD NUMBER
S913 COMMON KEY
GG AUTHENTICATION INFORMATION
NAME, BIRTH DATE, ADDRESS, MAIL ADDRESS, CONTACT
HH IDENTIFICATION INFORMATION
S901 ENCRYPTED COMMUNICATION
II LOG-IN DATA
JJ INPUT FORM (USER ID)
KK ID/PASSWORD
LL MANAGEMENT DATA INPUT FORM
MM DATA
NN FIRST KEY (DECRYPTION KEY)
S902 AUTHENTICATION
S903 REGISTRATION OF MANAGEMENT DATA
S906 (DETERMINATION OF ID/PASSWORD)
S907 DATA ENTRY
S910 REGISTRATION OF MANAGEMENT DATA
OO GENERATION OF FIRST KEY
PP CHECK FOR DUPLICATE

(57) **Abstract**: Provided is a collective suspension processing server device, collective suspension representation processing server device, settlement representation processing server device, method, and program, wherein there is no chance that the encryption key leaks. Also provided is the implementation of preventing the leakage of any piece of information under management. The collective suspension processing server device, collective suspension representation processing server device, settlement representation processing server device, method, and program does not hold the encryption key and the decryption key which are used to encrypt users' card information in a management database, but instead, dynamically generates the encryption key and the decryption key. Regarding the common key which is used in encryption, the common key is generated and encrypted for each authentication information table without destructing the rank order of strings of characters and numbers which constitute the authentication information, and encrypted strings of characters and numbers are searched using the common key generated and encrypted for each authentication information table. The decryption key which is used to decrypt the encrypted card information is unique to each user.

(57) 要約:

[続葉有]

WO 2010/016163 A1

暗号鍵が漏れる可能性をなくした一括停止処理サーバ装置、一括停止代行処理サーバ装置、決済代行処理サーバ装置、方法及びプログラムを提供する。それとともに管理している全ての情報が漏洩することを防止する。一括停止処理サーバ装置、一括停止代行処理サーバ装置、決済代行処理サーバ装置、方法及びプログラムは、ユーザのカード情報を暗号化する際に用いる暗号鍵及び復号鍵を管理データベースに保持せず、動的に生成するものとする。また、暗号化する際に用いる共通鍵は、認証情報の文字数列の順位を壊さず、当該認証情報テーブル毎に当該共通鍵を生成させ暗号化することで暗号化文字数列を検索するものとする。さらに、暗号化カード情報を復号化する際に用いる当該復号鍵はユーザ毎に固有のものとする。

明　細　書

一括停止処理／決済代行処理サーバ装置及びプログラム

技術分野

[0001] 本発明は、一括停止処理サーバ装置、一括停止代行処理サーバ装置、決済代行処理サーバ装置、一括停止処理、一括停止代行処理、決済代行処理方法及びプログラムに関する。

背景技術

[0002] 従来は、キャッシュカードやクレジットカードを紛失してカードの停止を行う際、利用者が各金融機関やクレジットカード会社に個別に連絡をしてカード停止処理を行っており、多くのユーザはクレジットカード等の紛失することを普段からは想定していないため、所定のカード情報等を紙面や電子情報として記録していることはほとんどない。また、記録していたとしても、紛失して連絡を行う時にカード情報等を記録した記録媒体を持参しているとも限らない。したがって、各金融機関によって各カード毎のクレジットカードと銀行口座紛失連絡先への連絡は時間を要するため、すべてのカードをクレジットカードと銀行口座停止するまでの時間差で第三者によって使用される危険があった。

[0003] さらに、近年ではユーザでは複数の金融機関と契約を結んでいることが多く、各金融機関の契約情報等を個人で管理することは困難である。したがって、契約していること自体を忘れてしまったり、カードを紛失してしまったことに気づかないこともある。これにより、第三者によるカード決済が行われていることを、商品購入の請求書を見て初めて認識する等の問題があった。

[0004] 一方、電子商取引技術の発達に伴い、ユーザはネットワーク上でコンピュータ装置を介して所望の商品を選択して、数日後には実際の商品を入手することができる。したがって、流通が集中する都心部ではない遠隔地に住むユーザや巷の販売店に赴く時間がない多忙なユーザにとって、このような電子商

取引システムは日常生活を過ごすためには必要不可欠となり、ごく当たり前のツール（道具）となっている。

[0005] しかし、電子商取引を行うためにはネットワーク上で決済処理を行うため、ユーザはカード情報等の個人情報の漏洩の危険性があることを示唆している。また、商品購入の際はコンピュータ装置にかかる操作画面上で所定の情報を入力するだけで決済処理が進むため、安易に不本意な商品を購入してしまうこともある。

[0006] そうした中で、個人情報を保護しつつ、クレジットカード等の利用停止や商品購入の処理を円滑に行うために、種々の特許文献がある。

[0007] 特許文献１に開示された代行サービスによれば、ユーザの個人情報及びユーザが契約しているサービス内容等の情報は暗号化され、代行サーバ装置に記憶される。このため、ユーザの個人情報及びユーザが契約しているサービス内容等の情報は第三者に知られることはない。しかしながら、特許文献１に開示されたシステムにおいては、ユーザの個人情報及びユーザが契約しているサービス内容等の情報を暗号化する際に用いた暗号鍵を第三者である代行サーバ装置運用者側に保持しておく必要があり、暗号鍵が第三者に盗み見られる危険性がある。

[0008] また、特許文献２に開示されたネット決済保持装置に関しては、ワンタイムパスワードを用いて、認証サーバが会員登録されている本人と操作者とが一致するか否かを判断し、本人と確認できたら商取引を行うことができるものである。しかしながら、特許文献２に開示された装置においては、当該本人の承諾の有無に関わらず当該ワンタイムパスワードの一致不一致で判断しており、多大なカード消費の抑制することは困難である。

[0009] また、特許文献３に開示された決済システム等に関しては、購買者からの暗号化された取引コードの受信をきっかけに、電話番号等の個人情報をもとにデータベース内を検索して、当該購買者に渡した暗号鍵と対をなす復号鍵を用いて復号化することで商取引を行うことができるものである。しかしながら、特許文献３に開示されたシステムにおいては、復号化するために登録者

本人の承諾を必要としていないため、カード消費の抑制することは困難である。

特許文献1：特開２００２－０５６１９８号公報

特許文献2：特開２００８－０１５９２４号公報

特許文献3：特開２００３－１５０８８５号公報

発明の開示

発明が解決しようとする課題

[0010] 上述したように、従来のカード停止処理等の代行サービスに関する技術は、個人情報の暗号化に際し、暗号鍵或いは復号鍵の管理が不十分であるため、セキュリティの面に関しては脆弱と言える。暗号鍵データの管理は、個人情報固有者自ら管理を行っていない管理方法であり、暗号鍵データの管理者はシステム運用者である第三者が暗号鍵データを流出させる場合には、代行サーバ装置に保持している全てのユーザの情報漏洩する危険性がある。

[0011] また、昨今のカード利用者が利用しているカード枚数も増加傾向にあり、各カードに関する契約情報等を個人が管理しきれなくなってきており、迅速にカードの利用停止や解約等をすることできず、特にカード被害を最小限に食い止めなければいけない紛失の手続に関しても同様に手続が容易ではない。

[0012] さらに、ネットワークユーザーが増大する昨今において、電子商取引を行う年齢層も広がり、コンピューター装置の操作になれていない高齢者や痴呆症等の老人、浪費家の夫婦、決済能力の無い学生等が容易に商品購入することができるため、個人情報の流出が原因となるカード犯罪または返済可能な限度額を超えた購入によるカード破産等の社会問題も勃発している。

[0013] したがって、本発明の目的は、電子商取引を行うにあたり、個人情報の流出の可能性もあるため暗号化した個人情報を復号化させるための復号鍵を個人情報固有者に管理させることで個人情報が漏れる可能性をなくした一括停止処理サーバ装置、一括停止代行処理サーバ装置、決済代行処理サーバ装置、方法及びプログラムを提供することにある。また、それとともに管理してい

る全ての情報が漏洩することを防止することを目的とする。

[0014] また、本発明の別の目的は、銀行やクレジットカード会社等の各金融機関において利用しているカードに関する情報を暗号化して一元管理する一括停止代行処理サーバ装置、方法及びプログラムを提供することにある、また、それとともに、一元解約等の手続を簡単かつ迅速に行うことを目的としている。

[0015] また、本発明のまた別の目的は、決済処理をカード所有者承認によって処理を実行させるため、不本意な電子商取引や振込み詐欺、フィッシング詐欺を未然に防ぐ決済代行処理サーバ装置、方法及びプログラムを提供することにある。また、それとともに、カード犯罪やカード破産を抑制することを目的としている。

課題を解決するための手段

[0016] （１）本発明は上記の課題を解決するためになされたものであり、本発明の一態様は、

一括停止処理サーバ装置に接続された端末装置において、

前記端末装置におけるユーザ操作に応じて、電子的情報を操作入力する入力部、電子的情報を記憶する記憶部、電子的情報を表示する表示部及び電子的情報を受信する受信部、前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報と前記記憶部より受信するユーザ識別情報を用いて暗号化するための共通暗号鍵と復号化するための共通復号鍵を生成する共通鍵処理部を有し、

前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報とユーザが所有している銀行口座とクレジットカードの情報である金融情報に、前記記憶部に記憶されているユーザを識別するための識別情報を加え、金融情報と認証情報と識別情報に基づいて暗号化するための暗号鍵を生成するとともに復号化するための復号鍵をペアーで自動生成する鍵生成処理部と、

前記入力部より情報登録用のユーザ認証情報が入力されると、前記共通鍵処理部より暗号化するための文字数が与えられ、前記ユーザ認証情報の文字

数列に当該暗号共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記端末装置における記憶部よりユーザ識別情報を取得し、前記ユーザ識別情報の文字数列に当該暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成する暗号化処理部と

前記端末装置における暗号化処理部において生成された暗号化認証情報と暗号化識別情報とともに、前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を対応付けて記憶させる記憶部と、前記端末装置における記憶部に記憶された前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報と送信させる送信部と、前記端末装置より送信された前記一括停止処理サーバ装置に受信され記憶される記憶部と、前記端末装置における記憶部より記憶されている暗号化金融情報と、復号鍵を呼び出して金融情報を復号化する復号化処理部と、前記端末装置における表示部に前記復号化処理された金融情報から停止させたい金融情報を特定し、選択した金融情報に紐付けられている暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を記憶部より取得し送信させ、前記一括停止処理サーバ装置に受信される受信部と、受信した暗号化認証情報が登録されている確認をおこなう認証部と、前記端末装置により受信した暗号化認証情報と暗号化識別情報の暗号化文字列に基づいて、前記一括停止処理サーバ装置における記憶部より登録されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した情報の有無を検索する暗号化処理部と、前記暗号化文字数列の完全一致した暗号化認証と暗号化識別情報と前記端末装置より受信した暗号化金融情報と復号化させる復号鍵と復号化共通鍵で復号させる復号化処理部と、前記端末装置より受信された指定金融機関に停止する金融情報発信命令を送信する送信部と、

を具備することを特徴とする一括停止サーバ処理装置である。

[0017] （２）また、本発明の一態様である一括停止処理方法は、

前記端末装置におけるユーザ操作に応じて、電子的情報を操作入力する入力部、電子的情報を記憶する記憶部、電子的情報を表示する表示部及び電子的情報を受信する受信部、前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報と前記記憶部より受信するユーザ識別情報を用いて暗号化するための共通暗号鍵と復号化するための共通復号鍵を生成する共通鍵処理ステップを有し、

前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報とユーザが所有している銀行口座とクレジットカードの情報である金融情報に、前記記憶部に記憶されているユーザを識別するための識別情報を加え、金融情報と認証情報と識別情報に基づいて暗号化するための暗号鍵を生成するとともに復号化するための復号鍵をペアーで自動生成する鍵生成処理ステップと、

前記入力部より情報登録用のユーザ認証情報が入力されると、前記共通鍵処理部より暗号化するための文字数が与えられ、前記ユーザ認証情報の文字数列に当該暗号共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記端末装置における記憶部よりユーザ識別情報を取得し、前記ユーザ識別情報の文字数列に当該暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成する暗号化処理ステップと

前記端末装置における暗号化処理部において生成された暗号化認証情報と暗号化識別情報とともに、前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を対応付けて記憶させる記憶ステップと、前記端末装置における記憶部に記憶された前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報と送信させる

送信ステップと、前記端末装置より送信された前記一括停止処理サーバ装置に受信され記憶される記憶ステップと、前記端末装置における記憶部より記憶されている暗号化金融情報と、復号鍵を呼び出して金融情報を復号化する復号化処理ステップと、前記端末装置における表示部に前記復号化処理された金融情報から停止させたい金融情報を特定し、選択した金融情報に紐付けられている暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を記憶部より取得し送信させ、前記一括停止処理サーバ装置に受信される受信ステップと、受信した暗号化認証情報が登録されている確認をおこなう認証ステップと、前記端末装置により受信した暗号化認証情報と暗号化識別情報の暗号化文字列に基づいて、前記一括停止処理サーバ装置における記憶部より登録されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した情報の有無を検索する暗号化処理ステップと、前記暗号化文字数列の完全一致した暗号化認証と暗号化識別情報と前記端末装置より受信した暗号化金融情報と復号化させる復号鍵と復号化共通鍵で復号させる復号化処理ステップと、前記端末装置より受信された指定金融機関に停止する金融情報発信命令を送信する送信ステップと、を具備することを特徴とする一括停止処理方法である。

[0018] （３）また、本発明の一態様は、一括停止代行処理サーバ装置と前記端末装置からユーザに関連する情報と停止する暗号化金融情報と復号鍵を受信し、当該暗号化金融情報の使用停止のための処理を実行する当該金融機関サーバ装置と、を含んで構成される金融口座停止処理システムである。

[0019] また、本発明の一態様は、一括停止処理サーバ装置は当該金融情報の使用停止のための処理を実行する当該金融機関サーバ装置に備えることを特徴とする一括停止処理サーバ装置である。

[0020] （４）また、本発明の一態様である一括停止代行処理サーバ装置は、

ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情

報登録用のユーザ認証情報とユーザ金融情報と前記端末装置用における記憶部に記憶されているユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記一括停止代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理部と、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理部と、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記一括停止代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザ金融情報を当該第三の鍵を用いて暗号化決済処理用金融情報を生成する鍵生成処理部と、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理金融情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信部と、

で受信し記憶する前記端末装置における記憶部と、

前記端末装置における表示部より停止する金融情報発信命令操作により、前記停止する暗号化処理用金融情報と認証情報と識別情報と第二の鍵が記憶部より取得され、前記端末装置送信部より送信され、前記一括停止代行処理サーバ装置に送信したユーザ認証情報とユーザ識別情報は、前記一括停止代行処理サーバ装置に置ける暗号化処理部により、フィールド単位毎に暗号化するための文字数を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理部と、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置よ

り送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理部と、
前記端末装置より送信された暗号化決済処理用金融情報を第三の鍵で復号化する復号化処理部と、
金融機関に停止する金融情報発信命令を送信する送信部と
を具備することを特徴とする一括停止代行処理サーバ装置である。

[0021] （５）また、本発明の一態様である一括停止代行処理方法は、
ネットワークを介して端末装置に接続されたサーバ装置において、
前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザ金融情報と前記端末装置用における記憶部に記憶されているユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記一括停止代行処理サーバ装置における受信部より受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数列を与える共通鍵処理ステップと、
当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理ステップと、
前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記一括停止代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザ金融情報を当該第三の鍵を用いて暗号化決済処理用金融情報を生成する鍵生成処理ステップと、
当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理金融情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信ステップと、
前記端末装置用で受信し記憶する記憶ステップと、
前記端末装置における表示部より停止する金融情報発信命令操作により、前記停止する暗号化処理用金融情報と認証情報と識別情報と第二の鍵が記憶部

より取得され、前記端末装置送信部より送信され、前記一括停止代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、フィールド単位毎に暗号化するための文字数列を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理ステップと、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理ステップと、

前記端末装置より送信された暗号化決済処理用金融情報を第三の鍵で復号化する復号化処理ステップと、

金融機関に停止する金融情報発信命令を送信する送信ステップと

を具備することを特徴とする一括停止代行処理方法である。

[0022] 本発明の一態様による決済代行処理サーバ装置は、

ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置用における記憶部に記憶されている。前記ユーザ認証情報とユーザクレジットカード情報とユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記決済代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理部と、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理部と、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用

いて第一の鍵を動的に生成し、前記決済代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザクレジットカード情報を当該第三の鍵を用いて暗号化決済処理用クレジットカード情報を生成する鍵生成処理部と、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理用クレジットカード情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信部と、

前記端末装置用で受信し記憶する記憶部と、

前記端末装置における入力部より購入したい商品を依頼する操作が行われると、ユーザ認証情報とユーザ識別情報とユーザクレジットカード情報を記憶部から呼び出し、前記決済代行処理サーバにおける受信部へ送信する。

前記決済代行処理サーバ装置における受信部で受信し、ユーザ認証情報と、ユーザ識別情報にフィールド単位毎に暗号化するため文字数を共通鍵処理部から与え、暗号化処理部で暗号化認証情報と暗号化識別情報を生成し、前記決済代行処理サーバ装置における記憶部に登録用として記憶されている暗号化認証情報と暗号化識別情報と安全一致の情報を検索し、暗号化認証情報のフィールド単位で保管されているメールアドレスのみを復号化処理部で復号化して送信部より決済実行処理確認通知を復号化したメールアドレス宛に送信する。前記端末装置受信部により受信された決済実行処理確認通知を前記端末装置における表示部に表示する。前記表示部に表示された内容から、承認処理依頼操作を行うと前記端末装置における記憶部より、決済処理を行う。記憶部より決済する暗号化決済処理用クレジットカード情報と認証情報と識別情報と第二の鍵が取得され、前記端末装置送信部より送信され、前記決済代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、フィールド単位毎に暗号化するための文字数列を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗

号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理部と、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理部と、

前記端末装置より送信された暗号化決済処理用クレジット情報を第三の鍵で復号化する復号化処理部と、

決済処理を行う金融機関に決済処理に関する金融情報とともに送信する送信部と、

を具備することを特徴とする決済代行処理サーバ装置である。

[0023] 本発明の一態様による決済代行処理方法は、

ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されている。前記ユーザ認証情報とユーザクレジットカード情報とユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記決済代行処理サーバ装置における受信部より受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理ステップと、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理ステップと、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記決済代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザクレジットカード情報を当該第三の鍵を用いて暗号化決済処理用クレジットカード情報を生成する鍵生成処理ステップと、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理用クレジットカード情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信ステップと、

前記端末装置で受信し記憶する記憶ステップと、

前記端末装置における入力部より購入したい商品を依頼する操作が行われると、ユーザ認証情報とユーザ識別情報とユーザクレジットカード情報を記憶部から呼び出し、前記決済代行処理サーバにおける受信部へ送信する。

前記決済代行処理サーバ装置における受信部で受信し、ユーザ認証情報と、ユーザ識別情報にフィールド単位毎に暗号化するため文字数を共通鍵処理部から与え、暗号化処理部で暗号化認証情報と暗号化識別情報を生成し、前記決済代行処理サーバ装置における記憶部に登録用として記憶されている暗号化認証情報と暗号化識別情報と安全一致の情報を検索し、暗号化認証情報のフィールド単位で保管されているメールアドレスのみを復号化処理部で復号化して送信部より決済実行処理確認通知を復号化したメールアドレス宛に送信する。前記端末装置受信部により受信された決済実行処理確認通知を前記端末装置における表示部に表示する。前記表示部に表示された内容から、承認処理依頼操作を行うと前記端末装置における記憶部より、決済処理を行う。記憶部より決済する暗号化決済処理用クレジットカード情報と認証情報と識別情報と第二の鍵が取得され、前記端末装置送信部より送信され、前記決済代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、フィールド単位毎に暗号化するための文字数列を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理部ステップと、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理部ステップ

と、

前記端末装置より送信された暗号化決済処理用クレジット情報を第三の鍵で復号化する復号化処理部ステップと、

決済処理を行う金融機関に決済処理に関する金融情報とともに送信する送信ステップと

を具備することを特徴とする決済代行処理方法である。

[0024] また、本発明の一態様による金融機関決済処理システムは、

決済代行処理サーバ装置と、前記金融機関決済処理サーバ装置に前記端末装置より決済依頼処理情報と復号鍵と識別情報と認証情報を受信し、当該決済依頼処理を実行する当該金融機関サーバ装置とを含んで構成される。

[0025] また、本発明の一態様による決済システムは、 端末装置と決済代行処理サーバ装置がインターネットを介して接続された決済依頼情報提供装置において、 前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されているユーザ識別するための識別情報を取得し、送信部より前記決済代行処理サーバ装置に受信される受信部と、前記受信部より受信されたユーザ認証情報とユーザ識別情報とクレジットカード情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理部と、当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字列の暗号化認証情報と暗号化識別情報と暗号化クレジットカード情報を生成させる暗号化処理部と、前記決済代行処理サーバ装置に外部の商品決済依頼情報提供装置から商品をクレジットガードによる決済処理依頼情報が与えられると、当該決済依頼情報に含まれているクレジットカード情報と認証情報を、前記共通鍵処理部によりクレジットカード情報と認証情報をフィールド単位毎に暗号化するための文字数を与える。暗号化するための文字数を、当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化クレジット情報と暗号化認証情報を動的に生成させる暗号化処理部と、 前記決済代行処理サーバ装置

における記憶部の記憶されている暗号化クレジット情報と暗号化認証情報の暗号化文字数列と完全一致するか否かを判断し、及び／もしくは完全一致しない場合、処理を停止させる制御処理部と、　当該外部の商品決算依頼情報提供装置に決済処理停止命令を送信する送信部を有する決済代行処理サーバ装置である。

[0026] また、本発明の一態様による決済システムは、　端末装置と決済代行処理サーバ装置がインターネットを介して接続された決済依頼情報提供装置において、　前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されているユーザ識別するための識別情報を取得し、送信部より前記決済代行処理サーバ装置に受信される受信ステップと、前記受信部より受信されたユーザ認証情報とユーザ識別情報とクレジットカード情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理ステップと、当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字列の暗号化認証情報と暗号化識別情報と暗号化クレジットカード情報を生成させる暗号化処理ステップと、前記決済代行処理サーバ装置に外部の商品決済依頼情報提供装置から商品をクレジットガードによる決済処理依頼情報が与えられると、当該決済依頼情報に含まれているクレジットカード情報と認証情報を、前記共通鍵処理部によりクレジットカード情報と認証情報をフィールド単位毎に暗号化するための文字数を与える。暗号化するための文字数を、当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化クレジット情報と暗号化認証情報を動的に生成させる暗号化処理ステップと、　前記決済代行処理サーバ装置における記憶部の記憶されている暗号化クレジット情報と暗号化認証情報の暗号化文字数列と完全一致するか否かを判断し、及び／もしくは完全一致しない場合、処理を停止させる制御処理ステップと、　当該外部の商品決算依頼情報提供装置に決済処理停止命令を送信する送信部を有する決済代行処理方法である。

[0027] 本発明の一態様は、端末装置に接続された一括停止処理サーバ装置において、端末装置におけるユーザ操作に応じて、電子的情報を操作入力する入力部、電子的情報を記憶する記憶部、電子的情報を表示する表示部及び電子的情報を受信する受信部、暗号鍵情報を生成する共通鍵処理部を有し、前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報とユーザが所有している銀行口座とクレジットカードの情報である金融情報に、前記記憶部に記憶されているユーザを識別するための識別情報を加え、金融情報と認証情報と識別情報に基づいて暗号化するための暗号鍵を生成するとともに復号化するための復号鍵をペアーで自動生成し、前記入力部より情報登録用のユーザ金融情報が入力されると当該暗号鍵で暗号化したユーザ金融情報を自動生成する鍵生成処理部と、前記入力部より情報登録用のユーザ認証情報が入力されると、暗号化するための暗号鍵を生成し、前記ユーザ認証情報の文字数列に当該暗号鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記端末装置における記憶部よりユーザ識別情報を取得し、前記ユーザ識別情報の文字数列に当該暗号鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成する暗号化処理部とを具備する端末装置と接続し、前記端末装置における共通鍵処理部において生成された暗号鍵情報と復号化させる復号鍵を対とした共通鍵情報と、前記共通鍵処理で生成された暗号化認証情報と暗号化識別情報とともに、前記端末装置における鍵生成処理部で生成された暗号化金融情報を前記端末装置における送信部より送信される情報を受信する受信部と、前記暗号化認証情報を暗号化識別情報と、前記暗号化認証情報と暗号化識別情報を暗号化させた暗号鍵情報と復号化させる復号鍵の対である共通鍵情報と、前記端末装置用における鍵生成処理部で生成された暗号化金融情報を受信し、前記端末装置用における送信部より送られた前記暗号化された暗号化認証情報と暗号化識別情報と共通鍵情報と暗号化金融情報とを対応付けて記憶させる記憶部と、前記端末装置における表示部より、停止する金融情報発信命令を選択し操作が行われると停止する金融情報を復号化させる特定の復号鍵と共通鍵処理部におい

て暗号化されて記憶されている暗号化認証情報と暗号化識別情報を呼び出し、前記端末装置における送信部より送信させ、前記端末装置より受信した暗号化認証情報と暗号化識別情報に基づいて、前記記憶部から暗号化されている暗号化認証情報と暗号化識別情報の文字数列が完全一致した暗号化認証情報と暗号化識別情報を呼び出し、対応付けて記憶されている暗号化金融情報と前記暗号化金融情報を復号化させる復号鍵で復号化する復号化処理部と、金融機関に停止する金融情報発信命令を送信する送信部とを具備することを特徴とする。

[0028] また、本発明の一態様である一括停止処理方法は、端末装置における入力部よりユーザの入力操作に応じて入力されたユーザ認証情報とユーザが所有している銀行口座とクレジットカードの情報である金融情報に、記憶部に記憶されているユーザを識別するための識別情報を加え、金融情報と認証情報と識別情報に基づいて暗号化するための暗号鍵を生成するとともに復号化するための復号鍵をペアーで自動生成し、情報登録用のユーザ金融情報が入力されると当該暗号鍵で暗号化したユーザ金融情報を自動生成する鍵生成処理するステップと、前記端末装置における入力部より情報登録用のユーザ認証情報が入力されると、暗号化するための暗号鍵を生成し、前記ユーザ認証情報の文字数列に当該暗号鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記端末装置における記憶部よりユーザ識別情報を取得し、前記ユーザ識別情報の文字数列に当該暗号鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成する暗号化処理するステップと

を具備する処理を行う端末装置に接続するステップを有し、前記端末装置における共通鍵処理部において生成された暗号鍵情報と復号化させる復号鍵を対とした共通鍵情報と、前記共通鍵処理で生成された暗号化認証情報と暗号化識別情報とともに、前記端末装置における鍵生成処理部で生成された暗号化金融情報を前記端末装置における送信部よりされる情報を受信するステップと、前記暗号化認証情報を暗号化識別情報と、前記暗号化認証情報と暗号

化識別情報を暗号化させた暗号鍵情報と復号化させる復号鍵の対である共通鍵情報と、前記端末装置用における鍵生成処理部で生成された暗号化金融情報を受信し、前記端末装置用における送信部より送られた前記暗号化された暗号化認証情報と暗号化識別情報と共通鍵情報と暗号化金融情報とを対応付けて記憶させる記憶するステップと、前記端末装置における表示部より、停止する金融情報発信命令を選択し操作が行われると停止する金融情報を復号化させる特定の復号鍵と共通鍵処理部において暗号化されて記憶されている暗号化認証情報と暗号化識別情報を呼び出し、前記端末装置における送信部より送信させ、前記端末装置より受信した暗号化認証情報と暗号化識別情報に基づいて、前記記憶部から暗号化されている暗号化認証情報と暗号化識別情報の文字数列が完全一致した暗号化認証情報と暗号化識別情報を呼び出し、対応付けて記憶されている暗号化金融情報と前記暗号化金融情報を復号化させる復号鍵で復号化する復号化処理するステップと、機関に停止する金融情報発信命令を送信する送信するステップと
を備えて処理することを特徴とする。

[0029] また、本発明の一態様である一括停止代行処理サーバ装置は、ネットワークを介して端末装置に接続されたサーバ装置において、前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザ金融情報と前記端末装置用における記憶部に記憶されているユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、受信したユーザ認証情報とユーザ識別情報に暗号化するための暗号鍵を生成し、当該情報の文字数列に前記暗号鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成させる暗号化処理部と、前記端末装置における送信部より送信されたユーザ認証情報を用いて第一の暗号鍵を動的に生成し、前記ユーザ識別情報を用いて第二の暗号鍵を動的に生成し、当該第一の暗号鍵と当該第二の暗号鍵から第三の暗号鍵を動的に生成し、前記ユーザ金融情報を当該第三の暗号鍵を用いて暗号化金融情報を生成する鍵生成処理部と、当該鍵生成処理部において、前記第一の暗号鍵を復

号化させる復号鍵を動的に生成し、送信部より前記端末装置へ送信し、前記端末装置用における記憶部と前記端末装置における表示部より停止する金融情報発信命令操作により、前記停止する金融情報復号鍵と認証情報と識別情報が記憶部より取得され、前記端末装置より送信され、受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、暗号化するための共通暗号鍵を当該情報の文字数列に埋め込まれ、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列から完全一致した暗号化認証情報と暗号化識別情報を呼び出し、前記鍵生成処理部から対応付けて記憶されている暗号化金融情報と前記停止する金融情報発信命令とともに、送信された前記復号鍵とともに復号化する処理を行う復号化処理部と、金融機関に停止する金融情報発信命令を送信する送信部と
を具備することを特徴とする。

[0030] また、本発明の一態様である一括停止代行処理方法は、ネットワークを介して端末装置と接続し、前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザ金融情報と前記端末装置における記憶部に記憶されているユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、受信したユーザ認証情報とユーザ識別情報に暗号化するための暗号鍵を生成し、当該情報の文字数列に前記暗号鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成させる暗号化処理するステップと、前記端末装置用における送信部より送信されたユーザ認証情報を用いて第一の暗号鍵を動的に生成し、前記ユーザ識別情報を用いて第二の暗号鍵を動的に生成し、当該第一の暗号鍵と当該第二の暗号鍵から第三の暗号鍵を動的に生成し、前記ユーザ金融情報を当該第三の暗号鍵を用いて暗号化金融情報を生成する鍵生成処理するステップと、当該鍵生成処理部において、前記第一の暗号鍵を復号化させる復号鍵を動的に生成し、送信部より前記端末装置へ送信し、前記端末装置用における記憶部と前記端末装置における表示部より停止する金融情報発信

命令操作により、前記停止する金融情報復号鍵と認証情報と識別情報が記憶部より取得され、前記端末装置より送信され、受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、暗号化するための共通暗号鍵を当該情報の文字数列に埋め込まれ、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列から完全一致した暗号化認証情報と暗号化識別情報を呼び出し、前記鍵生成処理部から対応付けて記憶されている暗号化金融情報と前記停止する金融情報発信命令とともに、送信された前記復号鍵とともに復号化する処理を行う復号化処理するステップと、金融機関に停止する金融情報発信命令を送信する送信するステップと、を具備することを特徴とする。

[0031] 本発明の一態様による決済代行処理サーバ装置は、ネットワークに接続した決済代行処理サーバ装置において、電子的情報を操作入力する入力部、電子的情報を記憶する記憶部、電子的情報を表示する表示部及び電子的情報を受信する受信部を有し、前記入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記記憶部に記憶されているユーザ識別するための識別情報を取得し、前記入力部より購入したい商品依頼する操作が行われると、前記記憶部からユーザ認証情報とユーザ識別情報を取得し電子的情報として送信するための送信部とを具備する端末装置と接続し、電子的情報を記憶する記憶部、電子的情報を受信する受信部、電子的情報を暗号化する暗号化処理部を有し、前記受信部より受信したユーザ認証情報とユーザ識別情報を前記暗号化処理部により暗号化するための共通暗号鍵を当該情報の文字数列に埋め込まれ、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化認証情報と暗号化識別情報を生成し、前記記憶部に記憶されている暗号化認証情報と、暗号化識別情報の暗号化文字数列から完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための復号化処理部と、前記記憶部より呼び出された暗号化認証情報と暗号化識別情報を前記復号化処理部により復号化し、復号化した認証情

報の一つである決済実行処理確認通知情報を前記端末装置における受信部に送信する送信部と、前記端末装置における記憶部に記憶されている登録用情報であるユーザ認証情報とユーザ識別情報と復号鍵を前記端末装置における記憶部から呼び出し、前記端末装置における表示部に表示された内容と前記端末装置における記憶部から呼び出す情報を、前記端末装置における送信部より送信し、前記受信部に受信したユーザ認証情報とユーザ識別情報と復号鍵は、暗号化処理部で暗号化され、暗号化認証情報と暗号化識別情報と復号鍵を与える鍵生成処理部とを具備し、前記記憶部に記憶されている暗号化金融情報を呼び出し、前記鍵生成処理部に与え、復号鍵によりユーザ情報を復号化させ、決済処理を行う金融機関に決済処理に関する金融情報とともに送信することを特徴とする。

[0032] また、本発明の一態様による決済代行処理方法は、電子的情報を操作入力する入力し、電子的情報を記憶する記憶し、電子的情報を表示し及び電子的情報を受信する受信するステップを有し、前記入力するステップよりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記記憶するステップより記憶されているユーザ識別するための識別情報を取得し、前記入力するステップより購入したい商品依頼する操作が行われると、前記記憶するステップよりユーザ認証情報とユーザ識別情報を取得し電子的情報として送信するステップと、を具備する端末装置と接続し、電子的情報を記憶する記憶し、電子的情報を受信し、電子的情報を暗号するステップを有し、前記受信するステップにより受信したユーザ認証情報とユーザ識別情報を前記暗号するステップにより暗号化するための共通暗号鍵を当該情報の文字数列に埋め込まれ、元文字数列の順位を壊さず5倍以下の暗号化文字数列で暗号化認証情報と暗号化識別情報を生成し、前記記憶するステップにより記憶されている暗号化認証情報と、暗号化識別情報の暗号化文字数列から完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための復号化処理するステップと、前記記憶するステップにより呼び出された暗号化認証情報と暗号化識別情報を前記復号化処理するステッ

プにより復号化し、復号化した認証情報の一つである決済実行処理確認通知情報を送信する送信ステップと、前記端末装置における記憶するステップにより記憶されている登録用情報であるユーザ認証情報とユーザ識別情報と復号鍵を前記端末装置から呼び出し、前記端末装置における表示するステップにより表示された内容と前記端末装置から呼び出す情報を、前記端末装置における送信するステップにより送信し、前記受信するステップで受信したユーザ認証情報とユーザ識別情報と復号鍵は、暗号化処理部で暗号化され、暗号化認証情報と暗号化識別情報と復号鍵を与える鍵生成処理するステップとを具備し、前記記憶するステップにより記憶されている暗号化金融情報を呼び出し、前記鍵生成処理鍵生成処理するステップに与え、復号鍵によりユーザ情報を復号化させ、決済処理を行う金融機関に決済処理に関する金融情報とともに送信するステップを備えることを特徴とする。

[0033] また、本発明の一態様による決済システムは、端末装置と決済代行処理サーバ装置が接続された決済システムにおいて、前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されているユーザ識別するための識別情報を取得し、前記決済代行処理サーバ装置に外部の商品決済依頼情報提供装置から商品をクレジットガードによる決済処理依頼情報が与えられると、当該決済依頼情報に含まれているクレジットカード情報と認証情報を、暗号化するための共通暗号鍵を当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化クレジット情報と暗号化認証情報を動的に生成させる暗号化処理部と、前記決済代行処理サーバ装置における記憶部の記憶されている暗号化クレジット情報と暗号化認証情報の暗号化文字数列と完全一致するか否かを判断し、及び／もしくは完全一致しない場合、処理を停止させる制御処理部と、当該外部の商品決算依頼情報提供装置に決済処理停止命令を送信する送信部を有する決済代行処理サーバ装置を有する。

[0034] また、本発明の一態様による決済代行処理方法は、端末装置と決済代行処

理サーバ装置が接続された決済代行処理方法において、前記端末装置における入力するステップよりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置用記憶部に記憶するステップにより記憶されているユーザ識別するための識別情報を取得し、前記決済代行処理サーバ装置に外部の商品決済依頼情報提供装置から商品をクレジットガードによる決済処理依頼情報が与えられると、当該決済依頼情報に含まれているクレジットカード情報と認証情報を、前記暗号化処理部により暗号化するステップにより暗号化するための共通暗号鍵を当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化クレジット情報と暗号化認証情報を動的に生成させる前記サーバ装置用暗号化処理するステップと、前記サーバ装置における記憶部の記憶されている暗号化クレジット情報と暗号化認証情報の暗号化文字数列と完全一致するか否かを判断する処理ステップと、完全一致しない場合、処理を停止させる制御ステップと、当該外部の商品決算依頼情報提供装置に決済処理停止命令を送信する送信ステップを有する。

[0035] また、本発明の一態様に係る決済処理サーバ装置は、クレジットカード決済をおこなう金融機関サーバ装置に備えることを特徴とする。

[0036] また、本発明の一態様に係る決済処理システムは、決済代行処理サーバ装置における送信部から暗号化金融情報を送信し、ネットワークを介して金融機関サーバ装置に暗号化されたまま当該暗号化金融情報を受信し、ユーザ端末装置における送信部から暗号化金融情報を復号化させる第二の鍵と暗号化決済処理用金融情報を前記金融機関サーバ装置に直接送信し、当該決済処理を実行する当該金融機関サーバ装置と、を含んで構成される。

発明の効果

[0037] 本発明によれば、一括停止処理サーバ装置、一括停止代行処理サーバ装置により複数の異なる金融機関やクレジットカード会社のカードを一括して停止するため、ユーザーの手間が減少する。また、本発明によれば、一括停止代行処理サーバ装置、決済代行処理サーバ装置により、ユーザのカード情報を

暗号化する際に用いる第一の鍵と第二の鍵から第三の鍵を自動生成により暗号化する。よって、暗号鍵自体の安全性が高まる。また、第三の鍵を自動生成に用いる第二の鍵は、管理データベースに保持せずユーザ毎に固有で保持させるので、全てのユーザーのカード情報が一度に漏洩する事を防止できる。また、本発明によれば、暗号化した情報を復号化する際に用いる第二の鍵をユーザ毎に固有のものとするので、暗号化情報の強度が高まる。

図面の簡単な説明

[0038] [図1]本発明の一本実施形態による一括停止処理システム（一括停止代行処理システム）の構成図である。

[図2]本発明の一実施形態に係るユーザの識別情報を記憶する際のテーブル構造である。

[図3A]本発明の一実施形態に係る別のユーザの認証情報を記憶する際のテーブル構造である。

[図3B]サーバ装置における受信情報がフィールド単位ごとで動的に生成された共通鍵により暗号化された暗号化データとして記憶するテーブル例である。

[図4A]本実施形態におけるユーザ識別情報とユーザ認証情報を暗号化および復号化する処理を示す図である。

[図4B]本実施形態におけるユーザ金融情報を暗号化する処理を示す図である。

[図4C]本実施形態におけるユーザ識別情報とユーザ認証情報を復号化する処理を示す図である。

[図4D]本実施形態におけるユーザ端末装置１０に係る置鍵生成処理部（図示しない）を示す図である。

[図4E]本実施形態における一括停止代行処理サーバ装置２０に係る暗号化処理部（図示しない）を示す図である。

[図4F]本実施形態における一括停止代行処理サーバ装置２０に係る復号化処理部（図示しない）を示す図である。

[図5]本実施形態におけるサービス登録の手順を示すシーケンス図である。

[図6]本実施形態における停止処理の依頼の手順を示すシーケンス図である。

[図7]本実施形態における本実施形態における一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０の上記ステップＳ１１６の処理に基づきユーザ端末装置１０が表示する実行認証画面の例である。

[図8]本発明に係る他の実施の形態による決済システム１００の構成を示す。

[図9]本実施形態における同決済システムにおける端末装置１０ａの構成を示すブロック図である。

[図10]本実施形態における同決済システムにおけるサーバ装置２０ａの構成を示すブロック図である。

[図11]本実施の形態による決済処理手順ＲＴ２０を示す。

[図12]本実施形態における一括停止代行処理システムまたは決済代行処理システムの情報登録時処理フローを示す図である。

[図13]本実施形態における一括停止代行処理フローを示す図である。

[図14]本実施形態における一括停止処理システムに係る情報登録時処理フローを示す図である。

[図15]本実施形態における一括停止処理フローを示す図である。

[図16]本実施形態における決済代行処理フローを示す図である。

発明を実施するための最良の形態

[0039] 以下、図面を参照しながら本発明の実施形態について詳しく説明する。

[0040] 図１は、本実施形態による一括停止処理システム（一括停止代行処理システム）の構成図である。一括停止処理システムは、ユーザ端末１０と、一括停止処理サーバ装置２０（一括停止代行処理サーバ装置）と、金融機関サーバ装置３０と、を含んで構成される。

[0041] 一括停止処理サービスを提供する業者は、一括停止処理サーバ装置２０を設け、金融機関サーバ装置３０を設けた複数の金融機関やクレジットカード会社と提携する。一括停止処理を利用するユーザの操作によりユーザ端末１０は、停止したい銀行カードやクレジットカードを複数選択して停止要求を一

括停止処理サーバ装置２０へ送信する。当該停止要求を受け取った一括停止処理サーバ装置２０は、各金融機関やクレジットカード会社の金融機関サーバ装置３０へ選択されたカードの停止要求を送信する。当該停止要求を受け取った金融機関サーバ装置３０は、該当するカードの停止処理を行う。これによりユーザは複数の異なる金融機関やクレジットカード会社の銀行カードやクレジットカードを一括して停止することができる。

[0042] ユーザ端末装置１０は、ユーザが使用するパーソナルコンピュータ、携帯電話端末、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などの端末であって、インターネットや携帯電話網などのネットワークにより一括停止処理サーバ装置２０と接続される。

[0043] 所定のコンピュータ処理にて一括停止処理システムへの初期登録を行ったユーザの操作によりユーザ端末装置１０はユーザＩＤとパスワードを一括停止処理サーバ装置２０へ送信し、一括停止処理システムへログインする。ユーザ端末装置１０は、ログインすると以下に記す操作が可能になる。

[0044] ユーザの操作によりユーザ端末装置１０は一括停止処理システムを利用したい銀行カードやクレジットカードのカード情報を暗号鍵を用いて暗号化した暗号化金融情報を一括停止処理サーバ装置２０へ送信し、登録を行う。

[0045] ユーザが銀行カードやクレジットカードを紛失して、そのカードを停止したい場合には、ユーザの操作によりユーザ端末装置１０は予め登録してある銀行カードやクレジットカードを選択して停止要求と当該暗号化金融情報を復号化するための復号鍵とを一括停止処理サーバ装置２０へ送信し、一括停止処理システムを利用する。

[0046] 金融機関サーバ装置３０は、ユーザに対してカードを発行する金融機関やクレジットカード会社などが設けるサーバ装置である。金融機関サーバ装置３０は、インターネットなどのネットワークにより一括停止処理サーバ装置２０と接続される。

[0047] また、金融機関サーバ装置３０は、一括停止処理サーバ装置２０から停止要求と共に受信した後述する金融情報（復号化済み）を取得する。復号化され

た金融情報を基にカードの停止処理を行う。

[0048] 一括停止処理サーバ装置２０は、一括処理停止サービスを提供するサーバ装置である。

[0049] 図２は、本発明の一実施形態に係るユーザの識別情報を記憶する際のテーブル構造である。同図に示すとおり、当該テーブル構造は、ユーザＩＤと識別番号を一意に関連付けて記憶するものである。

[0050] 図３、本発明の一実施形態に係る別のユーザの認証情報を記憶する際のテーブル構造である。同図に示すとおり、当該テーブル構造は、住所、氏名、パスワード、生年月日、メールアドレス、連絡先（たとえば、電話番号等）をユーザＩＤ毎に関連付けて保持する。ここで、ユーザＩＤはユーザを一意に特定する番号である。住所はユーザの住所である。氏名はユーザの氏名である。パスワードは後述する認証部２０－９にて行われるユーザ認証に使用されるパスワードである。図示するデータ例では、たとえば、一行目は、ユーザＩＤが「０００１」、住所が「〇〇県××市」、氏名が「Ｙ田Ｔ郎」、パスワードが「＊＊＊＊＊」、生年月日「１９６０／０１／０１」、メールアドレス「ｘｘ＠ｘｘ．ｃｏ．ｊｐ」、連絡先「０３ｘｘｘｘｘｘｘｘ」となっている。なお、認証テーブル内では、ユーザＩＤ、住所、氏名、パスワード等は、暗号化されて保持されている。

[0051] 図３Ｂは、本発明の一実施形態に係るサーバ装置における受信情報が動的に生成された共通鍵により暗号化された暗号化データとして記憶するテーブル例である。共通鍵はフィールド単位ごとに動的に共通鍵を生成し、受信情報の文字数列に当該共通鍵を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成させる。なお、当該共通鍵はフィールド単位で共通であるため、同じフィールドに登録される情報は当該暗号化文字数列となり、暗号化のまま完全一致検索する。認証情報に当該共通鍵を用いて暗号化し、識別情報テーブルのユーザＩＤが「ｂｉｂｉ１３５ａｊ」、住所が「ｔｏ６８ｘｏｏ８ｓｉｄ」、氏名が「１２３ａｂｃ４５６ｏｘｉｓｅ」、パスワードが「&%#？／／」、生年月日が「ｅｔｕｈｉ９８・・・」、メール

アドレスが「＆ｚ＠ｉ－１２３４・・・」、連絡先が「５８７ａｂｃ・・・」となっている。

[0052] 図４Ａは、本実施形態におけるユーザ識別情報とユーザ認証情報を暗号化および復号化する処理を示す図である。同図に示すとおり、ユーザ端末装置１０からユーザ識別情報とユーザ認証情報が一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０に送信されると、関数処理により、暗号鍵と復号鍵に係る共通鍵が生成され、これら共通鍵を用いて復号化処理或いは暗号化処理が行われる。

[0053] 図４Ｂは、本実施形態におけるユーザ金融情報を暗号化する処理を示す図である。同図に示すとおり、ユーザ端末装置１０から金融情報（データ用）が一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０に送信されると、上記記載の暗号化共通鍵で暗号化処理された暗号化ユーザ識別情報と暗号化ユーザ認証情報を基に鍵生成処理が行われ、当該金融情報（データ用）は暗号鍵にて暗号化処理された暗号鍵（暗号化金融情報データ）となる。

[0054] 図４Ｃは、本実施形態におけるユーザ識別情報とユーザ認証情報を復号化する処理を示す図である。同図に示すとおり、上記記載の暗号化された暗号化ユーザ識別情報と暗号化ユーザ認証情報は、共通鍵に係る共通の復号鍵を用いて復号化し、ユーザ識別情報と暗号化ユーザ認証情報を取得することができる。

[0055] 図４Ｄは、本実施形態におけるユーザ端末装置１０に係る置鍵生成処理部（図示しない）を示す図である。同図に示すとおり、上記記載の暗号化された暗号化金融情報データは、金融情報用の復号鍵を用いて鍵生成処理を行い、復号鍵（復号化された金融情報）を取得することができる。

[0056] 図４Ｅは、本実施形態における一括停止代行処理サーバ装置２０に係る暗号化処理部（図示しない）を示す図である。同図に示すとおり、上記記載の暗号化された暗号化ユーザ識別情報と暗号化ユーザ認証情報による自動生成された第一の鍵及びランダム数文字により自動生成された第二の鍵をもちいて第三の鍵を生成し決済処理用金融情報を暗号化し、第二の鍵とともに暗号化

決済処理用金融情報をユーザ端末装置１０で保持する。

[0057] 図４Ｆは、本実施形態における一括停止代行処理サーバ装置２０の復号化処理部を示す図である。同図に示すとおり、上記記載の暗号化された暗号化ユーザ識別情報と暗号化ユーザ認証情報による復号化するための基になる第一の鍵とユーザ端末装置１０から受信した第二の鍵に基づいて自動生成された復号化するための第三の鍵と暗号化決済処理用金融情報により復号化処理することで、復号化された金融情報を取得することができる。

[0058] 図５は、本実施形態におけるサービス登録の手順を示すシーケンス図である。ユーザ端末１０は、コンピュータ装置の操作によりネットワークを介して発行された仮ユーザＩＤ及び仮パスワードを一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０へ送信する（ステップＳ９０１）。当該データを受信した停止一括停止処理サーバ装置（一括停止代行処理サーバ装置）は、認証部（２０－９）にてユーザ認証を行い（ステップＳ９０２）、ユーザ認証が成功すると、管理データ登録部（２０－９）にてユーザの属性情報を管理データベース（２０－９）へ記憶する（ステップＳ９０３）。その際、ユーザの属性情報が既に記憶されていないかをチェックする。次に一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は、ユーザＩＤ及びパスワードの入力フォームをユーザ端末装置１０へ送信する（ステップＳ９０４）。ユーザ端末装置１０は、入力フォームへ入力されたユーザＩＤとパスワードを一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０へ送信する。一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は、ユーザ端末装置１０から受信したユーザＩＤとパスワードをユーザ固有のユーザＩＤとパスワードとして決定する（ステップＳ９０６）。一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は、当該ユーザＩＤと当該パスワードを属性情報テーブルへ記憶し（ステップＳ９０７）、管理データ入力フォームをユーザ端末装置１０へ送信する（ステップＳ９０８）。

[0059] ユーザ端末装置１０は、この管理データ入力フォームに入力されたカード情報一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０へ送信する

（ステップＳ９０９）。

[0060] 一括停止代行処理サーバ装置２０は、受信した金融情報から鍵生成処理部が生成した暗号鍵により所定の乱数演算を含み得る演算処理で当該金融情報を暗号化し、所定の記憶部に記憶する（ステップＳ９１０）。これと同時に、第二の鍵（以下、「復号鍵」ともいう。）を生成し（ステップＳ９１１）、ユーザ端末１０に送信する（ステップＳ９１２）。

[0061] このとき、一括停止処理においては、金融情報のみ公開鍵で暗号化して当該情報を一括停止処理サーバ装置２０に送り、ユーザの認証情報及び識別情報は、共通鍵で暗号化して一括停止処理サーバ装置２０に送信する。共通鍵で暗号化するのは、当該情報を検索可能とするためである。なお、秘密鍵は検索を実行するに際して不都合が生じるとも考えられる。したがって、当該共通鍵も一括停止処理サーバ装置２０に送信し、金融情報の暗号鍵・秘密鍵（復号鍵）はユーザ端末装置１０に記録する。一方、一括停止代行処理においては、共通鍵を使用して暗号化させ、復号鍵として一括停止代行処理サーバ装置２０から第二の鍵（復号鍵）をユーザ端末１０に送信し、ユーザ端末１０に記録する。

[0062] 図６は、本実施形態における停止処理の依頼の手順を示すシーケンス図である。ユーザ端末装置１０は、ユーザＩＤとパスワードを一括停止処理サーバ装置２０へ送信する（ステップＳ１１０）。このデータを受信した一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は認証部（２０－９）でユーザ認証を行い（ステップＳ１１１）、ユーザ認証が成功するとサービス選択フォームをユーザ端末装置１０へ送信する（ステップＳ１１２）。ユーザは、サービス選択フォームでは、停止サービスかデータメンテナンスかを選択可能である。ユーザ端末装置１０は、選択した情報を一括停止処理サーバ装置２０へ送信する（ステップＳ１１３）。一括停止処理サーバ装置２０は、データメンテナンスが選択された場合には、上述したサービス登録を行う（ステップＳ１１９）。ストップサービスが選択された場合は、一括停止処理サーバ装置２０は、実行認証画面をユーザ端末装置１０へ送信する（

ステップＳ１１６）。ユーザ端末装置１０は、実行認証画面に入力したデータとなる停止依頼情報と併せて復号鍵を一括停止処理サーバ装置２０へ送信する（ステップＳ１１７）。一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は、停止サービス処理部（図示しない）にて選択された金融機関の金融情報を取り出し、該当する提携会社の金融機関サーバ装置３０へ送信する（ステップＳ１１８）。

[0063] 図７は、

本実施形態における一括停止処理サーバ装置２０の上記ステップＳ１１６の処理に基づきユーザ端末装置１０が表示する実行認証画面の例である。実行認証画面には、ユーザＩＤと、停止を実行するボタンと、カード停止操作と登録したカードが複数選択できるチェックボックスと、が表示される。情報カード停止操作を選択した場合には、登録済みの全てのカードの停止をする。また、個別に停止をするカードを複数選択することもできる。停止を実行するボタンを押すと、ユーザ端末装置１０は、入力したデータ復号鍵を一括停止処理サーバ装置２０へ送信する。

[0064] なお、詳細な説明及び図示はしないが、一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は停止処理を行う金融情報を金融機関サーバ装置３０に送信する。カード管理サーバ装置３０は、所定の手順によりカード停止処理が終了したら、終了した旨を一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０する。一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０は、終了を確認すると、ユーザ端末１０へ停止処理終了がしたことを通知する。

[0065] このように、本実施形態によれば一括停止処理サーバ装置（一括停止代行処理サーバ装置）により複数の異なる金融機関やクレジットカード会社のカードを一括して停止することができる。また、カード情報を暗号化する暗号鍵及び復号化する復号鍵はは、ユーザ認証情報とユーザ識別情報を使用して動的に生成しているため、ユーザに固有であり、当該復号鍵はユーザーごとで保持するためサーバー装置内で保持する必要はない。これにより、全てのユ

ーザのカード情報が一度に漏洩することを防止できる。

[0066] また、ユーザ端末１０と一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０と金融機関サーバ装置３０の各部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより、停止処理を行ってもよい。なお、ここでいう「コンピュータシステム」とはＯＳや周辺機器等のハードウェアを含むものであってもよい。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、フラッシュメモリ等の書き込み可能な不揮発性メモリ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

[0067] さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（例えばＤＲＡＭ（Dynamic Random Access Memory））のように、一定時間プログラムを保持しているものも含むものとする。　また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

[0068] また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

[0069] 以上、図面を参照してこの発明の一実施形態について詳しく説明してきたが

、具体的な構成は上述のものに限られることはなく、この発明の要旨を逸脱しない範囲内において様々な設計変更等をすることが可能である。例えば、ガス、電気、水道、予約などのシステムの代行サービスにおけるデータ管理にも適用が可能である。

[0070] （他の実施の形態）

ここで図８に、本発明に係る他の実施の形態による決済システム１００の構成を示す。この決済システム１００は、登録されているユーザのカード情報などの金融情報を用いて、例えばインターネットを介して商品購入の注文が行われた際、決済の確認を促す情報をユーザに通知し、ユーザの承認を得た上で決済を行う決済サービスを実現するためのシステムである。

[0071] この決済システム１００は、例えばパーソナルコンピュータや携帯電話機など、ユーザが保有する端末装置１０ａと、上述の決済サービスを提供するためのサーバ装置２０ａと、商品の情報を提供する商品情報提供装置１３０と、カード情報を用いて決済を行う決済装置１４０とを有する。

[0072] 図９は、本実施形態における同決済システムにおける端末装置１０ａの構成を示すブロック図である。同図に示すように、当該端末装置１０ａは、制御処理部１０－１、受信部１０－２、送信部１０－３、共通鍵処理部１０－４、鍵生成処理部１０－５、記憶部１０－６、入力部１０－７、表示部１０－８、暗号化処理部１０－９、復号化処理部１０－１０で構成される。

[0073] 図１０は、本実施形態における同決済システムにおけるサーバ装置２０ａの構成を示すブロック図である。同図に示すように、当該サーバ装置２０ａは、制御処理部２０－１、受信部２０－２、送信部２０－３、共通鍵処理部２０－４、鍵生成処理部２０－５、記憶部２０－６、暗号化処理部２０－７、復号化処理部２０－８、認証部２０－９で構成される。

[0074] 図９及び図１０を用いて、端末装置１０ａとサーバ装置２０ａとの関係を説明する。

[0075] 始めに、ユーザが、端末装置１０ａの入力部１０－７を操作することにより、パスワードと、クレジットカードのカード番号や有効期限などに関する

カード情報とを入力すると、制御処理部１０－１は、送信部１０－３を介してサーバ装置２０ａ送信する。

[0076] その際、ユーザは、入力部１０－７を操作することにより、当該端末装置１０ａを保有するユーザの識別情報とユーザ認証情報をも入力し、制御処理部１０－１は、当該金融情報をサーバ装置２０ａに送信する際には、このユーザ識別情報とユーザ認証情報をもサーバ装置２０ａに送信する。

[0077] サーバ装置２０ａの受信部２０－２は、端末装置１０ａから送られてきたユーザ識別情報とユーザ認証情報と金融情報を受信すると、これらユーザ識別情報とユーザ認証情報と金融情報とを共通処理部２０－４で文字数を与えられ暗号化処理部２０－７で生成した暗号鍵で所定の乱数演算を含み得る演算処理で暗号化し、対応付けてサーバ装置用記憶部としての記憶部２０－６に記憶する。また、当該鍵生成処理部２０－５で生成した第二の鍵と暗号化金融情報を送信部２０－３を介して端末装置１０ａに送信する。当該第二の鍵と暗号化金融情報は端末装置１０ａの受信部１０－２を介して制御処理部１０－１に渡され、記憶部１０－６に記憶する。

[0078] これにより、サーバ装置２０ａは、金融情報を、フィールド単位で暗号化し、記憶部２０－６に記憶し管理する。また、カード情報は複数でもよく、たとえば、カード会社や銀行毎、カードの種類や保有数毎、またはユーザの任意の組み合わせ毎に暗号化し、暗号化された暗号化カード情報を記憶部２０－６に記憶して管理してもよい。

[0079] この状態において、ユーザは、端末装置１０ａの入力部１０－７を操作し、インターネットを介して商品情報提供装置１３０との間で通信を行うことにより、商品情報提供装置１３０が提供する商品を購入するための注文を行う。

[0080] この場合、ユーザは、入力部１０－７を操作することにより、ユーザ識別情報と、クレジットカードのカード番号などのカード情報と、購入対象の商品などの商品情報とを入力する。

[0081] これにより、制御処理部１０－１は、これらユーザ識別情報とユーザ認証

情報、金融情報及び商品情報を注文情報として、送信部１０－３を介して商品情報提供装置１３０に送信する。

[0082] 商品情報提供装置１３０は、端末装置１０ａから送られてきた注文情報を受信すると、これをサーバ装置２０ａに送信する。サーバ装置２０ａの受信部２０－２は、この注文情報を受信すると、これを暗号化処理部２０－７に出力する。また、注文情報は、商品情報提供装置１３０に含まれる所定のコンピュータ装置（たとえば、パーソナルコンピュータやカードリーダーを含む。）により入力・読込されてもよい。

[0083] 暗号化処理部２０－７は、当該注文情報を共通鍵処理部２０－４で文字数を与え、暗号化処理部２０－７で所定の乱数演算を含み得る演算処理で暗号化し、制御処理部２０－１に出力する。

[0084] 制御処理部２０－１は、記憶部２０－６に記憶されている暗号化ユーザ識別情報と暗号化ユーザ認証情報の中から、対応付けて記憶されている暗号化金融情報を検索し、さらに当該検索された暗号化金融情報の中から、商品情報提供装置１３０から送信され暗号化処理部２０－７で暗号化された暗号化ユーザ認証情報及び／または暗号化ユーザ識別情報と完全一致するものを検索する。たとえば、暗号化金融情報に含まれる文字数列化した氏名とメールアドレス及び／または識別情報に含まれる文字数列化した識別番号とを照合して、一致するか否かを判定する。これらは共通の暗号鍵で暗号化されているため、同一の識別番号ならば、暗号化により文字数列化したカード番号も完全に一致するため、このような判定方法が実現する。

[0085] 制御処理部２０－１は、記憶部２０－６に暗号化ユーザ識別情報と暗号化ユーザ認証情報に対応付けて記憶されている暗号化金融情報の中から、商品情報提供装置１３０から送信され暗号化処理部２０－７で暗号化された暗号化金融情報及び／または暗号化認証情報と完全に一致するものを検索できた場合には、ユーザ本人が決済しようとしているとして、決済の確認をユーザに行わせるための決済確認情報を生成し、これを送信部１０－３に出力する。たとえば、決済確認情報は、ユーザ認証情報に含まれる電子メールアドレ

スに、電子メールとして送信されてもよい。送信部１０－３は、この決済確認情報を端末装置１０ａに送信する。この場合、制御処理部２０－１及び送信部２０－３は、第１のサーバ装置用送信部として動作する。

[0086] 端末装置１０ａの受信部１０－２は、この決済確認情報を受信すると、これを制御処理部１０－１に出力する。この場合、制御処理部１０－１は、決済確認画面を表示部１０－８に表示することにより、決済の確認をユーザに促す。たとえば、決済確認情報が電子メールとして受信した場合、ユーザは表示部１０－８を介して当該電子メール本文或いは当該電子メール本文に含まれるURL（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）からサーバ装置２０ａにアクセスして決済確認フォームを画面で確認してもよい。これらの場合、表示部１０－８を介してユーザは、「あなたは○○円の買い物をしましたか？」というメッセージを確認することができる。

[0087] ユーザは、この決済確認画面を目視しつつ、入力部１０－７を操作することにより、当該決済を承認すると、制御処理部１０－１は、決済承認情報を生成すると共に、記憶部１０－６から第２の鍵と暗号化決済処理用金融情報を読み出し、これら決済承認情報と併せて第２の鍵を送信部１０－３を介してサーバ装置２０ａに送信する。なお、この場合、制御処理部１０－１及び送信部１０－３は、端末装置用送信部として動作する。

[0088] サーバ装置２０ａの受信部２０－２は、決済承認情報と併せて第２の鍵と暗号化決済処理用金融情報を受信すると、決済承認情報を記憶部２０－６に出力し、第２の鍵と暗号化決済処理用金融情報を復号化処理部２０－８に出力する。記憶部２０－６は、決済承認情報が与えられると、第３の鍵を生成し当該決済承認情報に対応する暗号化金融情報を読み出し、共通鍵処理部２０－４より数文字が与えられると第１の鍵と第２の鍵から第３の鍵を生成し、これを復号化処理部２０－８に出力する。

[0089] 復号化処理部２０－８は、暗号化金融情報を復号化し、復元化された金融情報を送信部２０－３に送信する。送信部２０－３は、この金融情報を決済装置１４０に送信することにより、決済を行わせる。また、送信部２０－３

は、決済承認情報を商品情報提供装置１３０に送信して、決済の手続を行ったことを通知し、商品の発送を行わせる。なお、この場合、暗号化処理部２０－７、復号化処理部２０－８及び送信部２０－３は、第２のサーバ装置用送信部として動作する。

[0090] これに対して、ユーザは、入力部１０－７を操作することにより、当該決済を拒否すると、制御処理部１０－１は、決済拒否情報を生成し、これを送信部１０－３を介してサーバ装置２０ａに送信する。この場合、制御部１０－１は、復号鍵をサーバ装置２０ａに送信しない。

[0091] サーバ装置２０ａの受信部２０－２は、この決済拒否情報を受信すると、これを送信部２０－３に送信する。送信部２０－３は、この決済拒否情報を商品情報提供装置１３０に送信して、注文をキャンセルさせると共に、この決済拒否情報を決済装置１４０に送信して、決済を行うことを停止させる。

[0092] なお、認証部２０－９は、ユーザの認証を行い、ユーザ端末１０から通知されたユーザＩＤとパスワード等を取得する。次に認証部２０－９は、当該ユーザＩＤと属性情報テーブルに記憶されたユーザＩＤを照合し、一致したユーザＩＤに関連付けて記憶されるパスワードと通知されたパスワードとを照合し、一致するか否かの判定を行う。認証部２０－９は、一致すると判定された場合、ユーザ認証成功とする。認証部２０－９は、通知されたユーザＩＤと一致したユーザＩＤがない場合あるいはパスワードが一致しない場合は、ユーザ認証失敗とする。

[0093] ところで、第３者がユーザになりすまして決済しようとした場合、たとえば、カードを紛失した場合、当該第３者が有する端末装置等により紛失したカード情報の入力がされ、商品情報提供装置１３０に送信し、商品を購入するための注文が行われる。したがって当該商品情報提供装置１３０は、当該カード情報をサーバ装置２０ａに送信し、上記記載と同様の所定の処理を行って決済承認情報を送信する。

[0094] しかし、決済承認情報の送信先はユーザが予め登録しているユーザ識別情報とユーザ認証情報のうち、たとえば、ＰＣ（パーソナルコンピュータ）や

携帯電話の電子メールアドレスであり、ユーザは身に覚えのない決済確認情報の通知を受けることとなる。そして当該ユーザが決済承認情報と併せて復号鍵をサーバ装置２０ａに送信されない。

[0095] したがって、なりすましを装う第３者は、ユーザが紛失したカードを入手して商品購入等の電子商取引を行おうとしても、決済認証情報を受け取ることができないため、復号鍵を送信することができず、決済処理を行うことができない。

[0096] また、ユーザ認証情報として、ユーザとは異なる者（たとえば、父、母、息子、娘、夫、嫁等）の認証情報（たとえば、電子メールアドレス等）を登録することで、その者にもユーザに通知される決済確認情報と同じ情報を送信することができる（送信のタイミングに限定はないが、好適には同時に送信されるのがよい。）。したがって、たとえば、コンピュータ装置になれていない父親が故意或いは不本意に商品購入をした場合、登録してある父親と息子の電子メールアドレスに決済確認情が送信される。息子は決済確認情報の通知を視認し、父親が決済を迫られていることを認識する。したがって息子は父親に決済をするか否かを確認し、当該父親が取引をした覚えがなかったり、安易に商品購入をするに至ってしまったりしたときは、息子から決済拒否情報を返信することができる。なお、このようなユーザ以外の者の承認やユーザを含む複数人の承認を決済処理の条件とすることは、任意に設定・変更することができる。

[0097] なお、図４Ａ乃至Ｆに示す各種情報の暗号化或いは復号化及び暗号鍵生成或いは復号鍵生成に係る一連の処理は、本決済システム１００における端末装置１０ａ及びサーバ装置２０ａにおいても利用することができるものとし、詳細な説明は上記記載の内容を同様とするため省略する。

[0098] 図１１に、本実施の形態による決済処理手順ＲＴ２０を示す。この図１８において、商品情報提供装置１３０が、注文情報をサーバ装置１２０に送信することにより、決済処理手順ＲＴ２０に入ると、ステップＳＰ５０において、サーバ装置１２０の受信処理部２００は、この商品情報提供装置１３０

から送られてきた注文情報を受信する。

[0099] ステップＳＰ６０において、サーバ装置１２０の受信処理部２００は、注文情報を共通の暗号鍵で暗号化し、暗号化した注文情報を制御部２４０に受け渡す。

[0100] ステップＳＰ７０において、制御部２４０は、記憶部２１０に記憶されている暗号化カード情報の中から、商品情報提供装置１３０から送信され暗号化されたカード情報と一致するものを検索する。検索した結果、一致するものが無い場合は、決済処理が終了する（図示しない。）

[0101] 一方、ステップＳＰ８０において、一致するものが有る場合は、登録しているユーザの電子メールアドレス等に決済確認情報を送信する。このとき、事前の設定により、ユーザ以外の他の者の電子メールアドレス等を登録し、決済確認情報を当該他の者の電子メールアドレス宛に送信するようにしてもよい。これにより、ユーザ等は端末装置１００の送受信処理部１８０を介して決済確認情報を受信する。

[0102] ステップＳＰ９０において、ユーザ及び／または他の者が端末装置１００の表示部１９０で当該決済確認情報を視認する。ここで、決済処理を行うことを承認しなかった場合、ステップＳＰ１３０において操作部１６０を操作して制御部１５０により決済拒否情報を生成し、送受信処理部１８０より当該決済拒否情報をサーバ措置１２０を経由して商品情報提供装置１３０に通知して、ステップＳＰ１４０において決済処理手順ＲＴ２０を終了する。

[0103] 一方、決済処理を行うことを承認した場合、ステップＳＰ１００において操作部１６０を操作して制御部１５０により決済承認情報を生成するとともに、制御部１５０により記憶部１７０から復号鍵を読出し、当該決済認証情報と併せて復号鍵を送受信処理部１８０よりサーバ装置１２０に送信する。

[0104] ステップＳＰ１１０において、サーバ装置１２０の受信処理部２００は決済承認情報と併せて及復号鍵を受信すると、決済承認情報を記憶部２１０に出力し、復号鍵を暗号化復号化処理部２２０に出力する。記憶部２１０は、決済承認情報が与えられると、当該決済承認情報に対応する暗号化カード情

報を読み出し、これを暗号化復号化処理部２２０に出力する。　暗号化復号化処理部２２０は、復号鍵を用いて、暗号化カード情報を復号化し、復元化されたカード情報を送信処理部２３０に送信する。

[0105] ステップＳＰ１２０において、送信処理部２３０は、このカード情報を決済装置１４０に送信することにより、決済を行わせる。また、送信処理部２３０は、決済承認情報を商品情報提供装置１３０に送信して、決済の手続を行ったことを通知し、商品の発送を行わせる。これら一連の動作を行った後、ステップＳＰ１４０において決済処理手順ＲＴ２０を終了する。

[0106] 図１２は、本実施形態における一括停止代行処理システムまたは決済代行処理システムの情報登録時処理フローを示す図である。同図に示すように、端末装置として機能するユーザ端末装置１０或いは端末装置１０ａから情報処理実行指示がされ（ステップＳＰ１０－１）、所定の入力部より入力された「ユーザ認証情報」を取得し（ステップＳＰ１０－２）、当該入力部より入力された「金融情報」を取得し（ステップＳＰ１０－３）、「ユーザ識別情報」を取得し（ステップＳＰ１０－４）、これらの取得した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」をサーバ装置に送信する（ステップＳＰ１０－５）。

[0107] その後、サーバ装置として機能する一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａは、端末装置から「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」を受信し（ステップＳＰ１０－６）、受信した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」を共通鍵で暗号化する（ステップＳＰ１０－７）。なおこのとき、暗号化した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」を所定の記憶部に記録する（ステップＳＰ１０－８）。そして、暗号化した「ユーザ識別情報」と「ユーザ認証情報」を用いて第１の鍵を自動生成し（ステップＳＰ１０－９）、「第２の鍵」をランダム数文字により自動生成し（ステップＳＰ１０－１０）、自動生成した「第１の鍵」と「第２の鍵」のセットから「第３の鍵」を自動生成し（ステップＳＰ１０－１１）、生成した「第３の

鍵」を用いて、受信した暗号化された「金融情報」を暗号化し、「暗号化決済処理用金融情報」に再暗号化し（ステップＳＰ１０－１２）、先に自動生成された「第２の鍵」と第３の鍵で暗号化された「暗号化決済処理用金融情報」をユーザ端末装置１０或いは端末装置１０ａに送信する（ステップＳＰ１０－１３）。

[0108] ユーザ端末装置１０あるいは端末装置１０ａは、一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａより「第２の鍵」を受信すると、第３の鍵で暗号化された「決済処理用金融情報」と「第２の鍵」を所定の記憶部に記録する（ステップＳＰ１０－１４）。

[0109] 図１３は、本実施形態における一括停止代行処理フローを示す図である。同図に示すとおり、端末装置として機能するユーザ端末装置１０或いは端末装置１０ａとしての第一処理が開始し、一括停止処理実行指示をし（ステップＳＰ２０－１）、所定の記憶部に記録されている「ユーザ認証情報」を取得し（ステップＳＰ２０－２）、当該記憶部に記録されている「金融情報」を取得し（ステップＳＰ２０－３）、「ユーザ識別情報」を取得し（ステップＳＰ２０－４）、取得した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」をサーバ装置に送信し（ステップＳＰ２０－５）、当該第一処理が終了する。

[0110] その後、サーバ装置として機能する一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａの第一処理が開始し、ユーザ端末装置１０或いは端末装置１０ａから「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を受信し（ステップＳＰ２０－６）、受信した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を共通暗号鍵で暗号化し（ステップＳＰ２０－７）、暗号化した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を用いて所定の記憶部に記録されている共通鍵で暗号化されている「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」と紐づく情報を検索し、完全一致した暗号情報から、紐づく情報の暗号化されたユーザ認証情報を取得し（ステップＳＰ２０－８）、暗号化された「ユー

ザ認証情報」と紐づく情報の内からメールアドレスを探し出し、メールアドレスのみを復号化して「一括停止処理確認通知」を当該端末装置に送信し（ステップＳＰ２０－９）、当該第一処理が終了する。

[0111] その後、ユーザ端末装置１０或いは端末装置１０ａとしての第二処理が開始し、一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０より送られてくる「一括停止処理確認通知」を受信して所定の表示部に表示し（ステップＳＰ２０－１０）、当該表示部に表示された内容から承認処理を行うと、所定の記憶部より第２の復号鍵を取得し（ステップＳＰ２０－１１）、「第２の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットを当該サーバ装置に送信し（ステップＳＰ２０－１２）、当該第二処理が終了する。

[0112] その後、一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａの第二処理が開始し、ユーザ端末装置１０或いは端末装置１０ａから「第２の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットを受信し（ステップＳＰ２０－１３）、受信した「ユーザ認証情報」と「ユーザ識別情報」を共通暗号鍵で暗号化し（ステップＳＰ２０－１４）、暗号化された「ユーザ認証情報」と「ユーザ識別情報」を用いて記憶部に記録されている暗号化された「ユーザ認証情報」と「ユーザ識別情報」と完全一致した情報を検索し（ステップＳＰ２０－１５）、暗号化した「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索できると、共通暗号鍵を用いて復号化し（ステップＳＰ２０－１６）、復号化した「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報の内から第１の復号鍵を生成し（ステップＳＰ２０－１７）、「第１の復号鍵」とユーザ端末装置より受信した「第２の復号鍵」のセットから「第３の復号鍵」を自動生成し（ステップＳＰ２０－１８）、生成した「第３の復号鍵」をもちいて、先に受信した、一括停止処理に関する暗号化した「決済処理用金融情報」を復号化し（ステップＳＰ２０－１９）、復号化した「一括停止に対する金融機関情報」を各金融機関情報をもとに金融機関へ

送信し（ステップＳＰ２０－２０）、当該第二処理が終了する。

[0113] 図１４は、本実施形態における一括停止処理システムに係る情報登録時処理フローを示す図である。同図に示すとおり、端末装置として機能するユーザ端末装置１０或いは端末装置１０ａとしての処理が開始し、情報処理実行指示がされ（ステップＳ３０－１）、所定の入力部より入力された「ユーザ認証情報」を取得し（ステップＳＰ３０－２）、当該入力部より入力された「金融情報」を取得し（ステップＳＰ３０－３）、「ユーザ識別情報」を取得し（ステップＳＰ３０－４）、取得した「ユーザ識別情報」と「ユーザ認証情報」を用いて暗号鍵と復号鍵を自動生成し（ステップＳＰ３０－５）、取得した「ユーザ識別情報」と「ユーザ認証情報」を共通暗号鍵で暗号化し（ステップＳＰ３０－６）、生成した「暗号鍵」を用いて取得した「金融情報」を暗号化し（ステップＳＰ３０－７）、暗号化した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」をサーバ装置に送信し（ステップＳＰ３０－８）、当該端末装置は待機状態となる。

[0114] その後、サーバ装置として機能する一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａの処理が開始し、暗号化された「ユーザ識別情報」と「ユーザ認証情報」とに紐付けて暗号化された「金融情報」を所定の記憶部に記録し（ステップＳＰ３０－９）、暗号化された「ユーザ識別情報」と「ユーザ認証情報」を当該記憶部に記録し（ステップＳＰ３０－１０）、「登録処理結果」をユーザ端末装置１０或いは端末装置１０ａに送信し（ステップＳＰ３０－１１）、当該サーバ装置の処理は終了する。

[0115] その後、待機状態であったユーザ端末装置１０或いは端末装置１０ａは、一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａから「登録処理結果」を受信し、その内容を所定の表示部に表示し（ステップＳＰ３０－１２）、当該端末装置の処理は終了する。

[0116] 図１５は、本実施形態における一括停止処理フローを示す図である。同図に示すとおり、端末装置として機能するユーザ端末装置１０或いは端末装置

１０ａとしての処理が開始し、

一括停止処理実行指示をし（ステップＳＰ４０－１）、「ユーザ識別情報」を取得し（ステップＳＰ４０－２）、所定の入力部より入力された「ユーザ認証情報」を取得し（ステップＳＰ４０－３）、当該入力部より入力された「金融情報」を取得し（ステップＳＰ４０－４）、所定の記憶部より「復号鍵」と暗号化「ユーザ認証情報」と暗号化「ユーザ識別情報」と復号化させるための復号「共通鍵」と暗号化された「金融情報」を一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａに送信し（ステップＳＰ４０－５）、当該端末装置は待機状態となる。

[0117] その後、サーバ装置として機能する一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａの処理が開始し、端末装置として機能するユーザ端末装置１０或いは端末装置１０ａから暗号化「ユーザ認証情報」と暗号化「ユーザ識別情報」と暗号化「金融情報」と「復号鍵」を受信し（ステップＳＰ４０－６）、暗号化「ユーザ認証情報」と暗号化「ユーザ識別情報」を用いて所定の記憶部に暗号化されて記録されている「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索し（ステップＳＰ４０－７）、「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索できると共通鍵を用いて復号化し（ステップＳＰ４０－８）、復号化した「復号鍵」をもちいて先に取得した「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報の中から一括停止処理に関する金融機関情報を復号化し（ステップＳＰ４０－９）、復号化した「一括停止に対する金融機関情報」を各金融機関情報をもとに所定の金融機関へ送信し（ステップＳＰ４０－１０）、「一括停止処理結果」を当該端末装置に送信し（ステップＳＰ４０－１１）、当該サーバ装置の処理は終了する。

[0118] その後、待機状態であったユーザ端末装置１０或いは端末装置１０ａは、一括停止処理サーバ装置（一括停止代行処理サーバ装置）２０或いはサーバ装置２０ａから「一括停止処理結果」を受信してその内容を所定の表示部に表示し（ステップＳＰ４０－１２）、当該端末装置の処理は終了する。

[0119] 図１６は、本実施形態における決済代行処理フローを示す図である。同図に示すとおり、端末装置として機能する端末装置１０ａの処理が開始し、決済依頼処理実行指示をし（ステップＳＰ５０－１）、所定の入力装置から入力された「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」をサーバ装置として機能するサーバ装置２０ａに送信し（ステップＳＰ５０－２）、当該端末装置は待機状態となる。

[0120] その後、サーバ装置として機能するサーバ装置２０ａの第一の処理が開始し、端末装置から「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を受信し（ステップＳＰ５０－３）、受信した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を共通暗号鍵で暗号化し（ステップＳＰ５０－４）、暗号化した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を用いて所定の記憶部に記録されている暗号化された「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」と紐づく情報が完全一致した情報を検索し（ステップＳＰ５０－５）、「ユーザ認証情報」を検索し、共通暗号鍵を用いて、メールアドレスのみ復号化し（ステップＳＰ５０－６）、復号化したメールアドレスにより「決済実行処理確認通知」を端末装置として機能する端末装置１０ａに送信し（ステップＳＰ５０－７）、第一の処理が終了する。

[0121] その後、端末装置１０ａの処理として、当該サーバ装置より送られてくる「決済実行処理確認通知」を受信して所定の表示部に表示し（ステップＳＰ５０－８）、当該表示部に表示された内容から承認処理を行うと、所定の記憶部より「第２の復号鍵」と暗号化された「決済処理用金融情報」を取得し（ステップＳＰ５０－９）、「第２の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットを当該サーバ装置２０ａに送信し（ステップＳＰ５０－１０）、処理が終了する。

[0122] その後、当該サーバ装置２０ａの第二の処理が開始し、当該端末装置から「第２の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットを受信し（ステップＳＰ５０－１１）、

共通暗号鍵で暗号化された「ユーザ認証情報」と「ユーザ識別情報」を用いて記憶部に記録されている暗号化された「ユーザ認証情報」と「ユーザ識別情報」と完全一致した紐づく情報を検索し（ステップＳＰ５０－１２）、暗号化された「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索できると、共通鍵を用いて、第１の鍵を生成し（ステップＳＰ５０－１３）、「第１の復号鍵」と先に受信した「第２の復号鍵」のセットから「第３の復号鍵」を自動生成し（ステップＳＰ５０－１４）、生成した「第３の復号鍵」を用いて、先に受信した暗号化された「決済処理用金融情報」を復号化し（ステップＳＰ５０－１５）、復号化した「決済処理に関する金融機関情報」を各金融機関情報をもとに所定の金融機関へ送信し（ステップＳＰ５０－１６）、第二の処理が終了する。

[0123] このように本実施の形態によれば、登録されているユーザのカード情報を用いて、商品購入の注文が行われた際、決済確認情報をユーザに通知し、ユーザの承認を得た上で決済を行うことにより、ユーザにとってより安全な決済システムを提供することができる。

[0124] また、利用者（ユーザ）は暗号化が必要な特定の部分のみを暗号化して管理することができる。したがって、暗号化する情報量の軽減を図ることができる。

[0125] 尚、本発明は上述した実施形態に限定されるものではなく、本発明の主旨を逸脱しない範囲内で種々変更して実施することが可能である。また、上述したものは本願に係る技術思想を具現化するための実施形態の一例を示したにすぎないものであり、他の実施形態でも本願に係る技術思想を適用することが可能である。

[0126] さらにまた、本願発明を用いて生産される装置、方法、システムが、その２次的生産品に登載されて商品化された場合であっても、本願発明の価値は何ら減ずるものではない。

産業上の利用可能性

[0127] 本発明の情報管理システム及びその方法によれば、ユーザの使い勝手を向

上させながら、ユーザ関連情報を安全な状態で記憶及び管理することができることから、産業別を問わず、各種産業に従事する人間のあらゆる局面において非常な有意性を実現するものであるため、情報産業はいうまでもなく、建設業、飲食業、各種製造業、流通業等あらゆる分野において利用可能であり、有用性が高い。

請求の範囲

[1] 一括停止処理サーバ装置に接続された端末装置において、

前記端末装置におけるユーザ操作に応じて、電子的情報を操作入力する入力部、電子的情報を記憶する記憶部、電子的情報を表示する表示部及び電子的情報を受信する受信部、前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報と前記記憶部より受信するユーザ識別情報を用いて暗号化するための共通暗号鍵と復号化するための共通復号鍵を生成する共通鍵処理部を有し、

前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報とユーザが所有している銀行口座とクレジットカードの情報である金融情報に、前記記憶部に記憶されているユーザを識別するための識別情報を加え、金融情報と認証情報と識別情報に基づいて暗号化するための暗号鍵を生成するとともに復号化するための復号鍵をペアーで自動生成する鍵生成処理部と、

前記入力部より情報登録用のユーザ認証情報が入力されると、前記共通鍵処理部より暗号化するための文字数が与えられ、前記ユーザ認証情報の文字数列に当該暗号共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記端末装置における記憶部よりユーザ識別情報を取得し、前記ユーザ識別情報の文字数列に当該暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成する暗号化処理部と

前記端末装置における暗号化処理部において生成された暗号化認証情報と暗号化識別情報とともに、前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を対応付けて記憶させる記憶部と、前記端末装置における記憶部に記憶された前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報と送信させる送信部と、前記端末装置より送信された前記一括停止処理サーバ装置に受信され記

憶される記憶部と、前記端末装置における記憶部より記憶されている暗号化金融情報と、復号鍵を呼び出して金融情報を復号化する復号化処理部と、前記端末装置における表示部に前記復号化処理された金融情報から停止させたい金融情報を特定し、選択した金融情報に紐付けられている暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を記憶部より取得し送信させ、前記一括停止処理サーバ装置に受信される受信部と、受信した暗号化認証情報が登録されている確認をおこなう認証部と、前記端末装置により受信した暗号化認証情報と暗号化識別情報の暗号化文字列に基づいて、前記一括停止処理サーバ装置における記憶部より登録されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した情報の有無を検索する暗号化処理部と、前記暗号化文字数列の完全一致した暗号化認証と暗号化識別情報と前記端末装置より受信した暗号化金融情報と復号化させる復号鍵と復号化共通鍵で復号させる復号化処理部と、前記端末装置より受信された指定金融機関に停止する金融情報発信命令を送信する送信部とを具備することを特徴とする一括停止サーバ処理装置。

[2] 一括停止処理サーバ装置に接続された端末装置における一括停止処理方法において、

前記端末装置におけるユーザ操作に応じて、電子的情報を操作入力する入力部、電子的情報を記憶する記憶部、電子的情報を表示する表示部及び電子的情報を受信する受信部、前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報と前記記憶部より受信するユーザ識別情報を用いて暗号化するための共通暗号鍵と復号化するための共通復号鍵を生成する共通鍵処理ステップを有し、

前記入力部よりユーザの入力操作に応じて入力されたユーザ認証情報とユーザが所有している銀行口座とクレジットカードの情報である金融情報に、前記記憶部に記憶されているユーザを識別するための識別情報を加え、金融情報と認証情報と識別情報に基づいて暗号化するための暗号鍵を生成すると

ともに復号化するための復号鍵をペアーで自動生成する鍵生成処理ステップと、

前記入力部より情報登録用のユーザ認証情報が入力されると、前記共通鍵処理部より暗号化するための文字数が与えられ、前記ユーザ認証情報の文字数列に当該暗号共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記端末装置における記憶部よりユーザ識別情報を取得し、前記ユーザ識別情報の文字数列に当該暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成する暗号化処理ステップと、

前記端末装置における暗号化処理部において生成された暗号化認証情報と暗号化識別情報とともに、前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を対応付けて記憶させる記憶ステップと、前記端末装置における記憶部に記憶された前記暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報と送信させる送信ステップと、前記端末装置より送信された前記一括停止処理サーバ装置に受信され記憶される記憶ステップと、前記端末装置における記憶部より記憶されている暗号化金融情報と、復号鍵を呼び出して金融情報を復号化する復号化処理ステップと、前記端末装置における表示部に前記復号化処理された金融情報から停止させたい金融情報を特定し、選択した金融情報に紐付けられている暗号化認証情報と暗号化識別情報を復号化させる復号化共通鍵情報と前記鍵生成処理部で生成された復号鍵と暗号化金融情報と暗号化認証情報と暗号化識別情報を記憶部より取得し送信させ、前記一括停止処理サーバ装置に受信される受信ステップと、受信した暗号化認証情報が登録されている確認をおこなう認証ステップと、前記端末装置により受信した暗号化認証情報と暗号化識別情報の暗号化文字列に基づいて、前記一括停止処理サーバ装置における記憶部より登録されている暗号化認証情報と暗号化識別情報の

暗号化文字数列と完全一致した情報の有無を検索する暗号化処理ステップと、前記暗号化文字数列の完全一致した暗号化認証と暗号化識別情報と前記端末装置より受信した暗号化金融情報と復号化させる復号鍵と復号化共通鍵で復号させる復号化処理ステップと、前記端末装置より受信された指定金融機関に停止する金融情報発信命令を送信する送信ステップとを具備することを特徴とする一括停止処理方法。

[3] 請求項１記載の一括停止代行処理サーバ装置と前記端末装置からユーザに関連する情報と停止する暗号化金融情報と復号鍵を受信し、当該暗号化金融情報の使用停止のための処理を実行する当該金融機関サーバ装置と、を含んで構成される金融口座停止処理システム。

[4] 前記一括停止処理サーバ装置は当該金融情報の使用停止のための処理を実行する当該金融機関サーバ装置に備えることを特徴とする請求項１記載の一括停止処理サーバ装置。

[5] ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザ金融情報と前記端末装置用における記憶部に記憶されているユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記一括停止代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理部と、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理部と、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記一括停止代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザ金融情報を当該第三の鍵を用いて暗号化決済処理用金融情報を生成する鍵生成処理部と、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理金融情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信部と、

で受信し記憶する前記端末装置における記憶部と、

前記端末装置における表示部より停止する金融情報発信命令操作により、前記停止する暗号化処理用金融情報と認証情報と識別情報と第二の鍵が記憶部より取得され、前記端末装置送信部より送信され、前記一括停止代行処理サーバ装置に送信したユーザ認証情報とユーザ識別情報は、前記一括停止代行処理サーバ装置に置ける暗号化処理部により、フィールド単位毎に暗号化するための文字数を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、

前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理部と、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理部と、

前記端末装置より送信された暗号化決済処理用金融情報を第三の鍵で復号化する復号化処理部と、

金融機関に停止する金融情報発信命令を送信する送信部と

を具備することを特徴とする一括停止代行処理サーバ装置。

[6] ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザ金融情報と前記端末装置用における記憶部に記憶されているユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記一括停止代行処理サーバ装置における受信部より受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数列を与える共通鍵処理ステップと、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順

位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理ステップと、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記一括停止代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザ金融情報を当該第三の鍵を用いて暗号化決済処理用金融情報を生成する鍵生成処理ステップと、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理金融情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信ステップと、

前記端末装置用で受信し記憶する記憶ステップと、

前記端末装置における表示部より停止する金融情報発信命令操作により、前記停止する暗号化処理用金融情報と認証情報と識別情報と第二の鍵が記憶部より取得され、前記端末装置送信部より送信され、前記一括停止代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、フィールド単位毎に暗号化するための文字数列を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理ステップと、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理ステップと、

前記端末装置より送信された暗号化決済処理用金融情報を第三の鍵で復号化する復号化処理ステップと、

金融機関に停止する金融情報発信命令を送信する送信ステップと

を具備することを特徴とする一括停止代行処理方法。

[7] ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されている。前記ユーザ認証情報とユーザクレジットカード情報とユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記決済代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理部と、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理部と、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記決済代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザクレジットカード情報を当該第三の鍵を用いて暗号化決済処理用クレジットカード情報を生成する鍵生成処理部と、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理用クレジットカード情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信部と、

前記端末装置で受信し記憶する記憶部と、

前記端末装置における入力部より購入したい商品を依頼する操作が行われると、ユーザ認証情報とユーザ識別情報とユーザクレジットカード情報を記憶部から呼び出し、前記決済代行処理サーバにおける受信部へ送信する送信部と、

前記決済代行処理サーバ装置における受信部で受信し、ユーザ認証情報と、ユーザ識別情報にフィールド単位毎に暗号化するため文字数を共通鍵処理部

から与え、暗号化処理部で暗号化認証情報と暗号化識別情報を生成し、前記決済代行処理サーバ装置における記憶部に登録用として記憶されている暗号化認証情報と暗号化識別情報と安全一致の情報を検索し、暗号化認証情報のフィールド単位で保管されているメールアドレスのみを復号化処理部で復号化して送信部より決済実行処理確認通知を復号化したメールアドレス宛に送信する。前記端末装置受信部により受信された決済実行処理確認通知を前記端末装置における表示部に表示する。前記表示部に表示された内容から、承認処理依頼操作を行うと前記端末装置における記憶部より、決済処理を行い記憶部より決済する暗号化決済処理用クレジットカード情報と認証情報と識別情報と第二の鍵が取得され、前記端末装置送信部より送信され、前記決済代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、フィールド単位毎に暗号化するための文字数列を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理部と、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理部と、

前記端末装置より送信された暗号化決済処理用クレジット情報を第三の鍵で復号化する復号化処理部と、

決済処理を行う金融機関に決済処理に関する金融情報とともに送信する送信部と

を具備することを特徴とする決済代行処理サーバ装置。

[8] ネットワークを介して端末装置に接続されたサーバ装置において、

前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されている。前記ユーザ認証情報とユーザクレジットカ

ード情報とユーザ識別するための識別情報を取得し、ともに前記端末装置における送信部より送信され、前記決済代行処理サーバ装置における受信部より受信したユーザ認証情報とユーザ識別情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理ステップと、

当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列の暗号化認証情報と暗号化識別情報を生成させる暗号化処理ステップと、

前記暗号化処理部より暗号化された暗号化認証情報と暗号化識別情報を用いて第一の鍵を動的に生成し、前記決済代行処理サーバ装置における鍵生成処理部よりランダム数文字を用いて第二の鍵を動的に生成し、当該第一の鍵と当該第二の鍵から第三の鍵を動的に生成し、前記ユーザクレジットカード情報を当該第三の鍵を用いて暗号化決済処理用クレジットカード情報を生成する鍵生成処理ステップと、

当該鍵生成処理部において生成された、前記第二の鍵と前記暗号化決済処理用クレジットカード情報を前記一括停止代行処理サーバ装置における送信部より前記端末装置へ送信する送信ステップと、

前記端末装置で受信し記憶する記憶ステップと、

前記端末装置における入力部より購入したい商品を依頼する操作が行われると、ユーザ認証情報とユーザ識別情報とユーザクレジットカード情報を記憶部から呼び出し、前記決済代行処理サーバにおける受信部へ送信するステップと、

前記決済代行処理サーバ装置における受信部で受信し、ユーザ認証情報と、ユーザ識別情報にフィールド単位毎に暗号化するため文字数を共通鍵処理部から与え、暗号化処理部で暗号化認証情報と暗号化識別情報を生成し、前記決済代行処理サーバ装置における記憶部に登録用として記憶されている暗号化認証情報と暗号化識別情報と安全一致の情報を検索し、暗号化認証情報のフィールド単位で保管されているメールアドレスのみを復号化処理部で復号化して送信部より決済実行処理確認通知を復号化したメールアドレス宛に送

信する。前記端末装置受信部により受信された決済実行処理確認通知を前記端末装置における表示部に表示する。前記表示部に表示された内容から、承認処理依頼操作を行うと前記端末装置における記憶部より、決済処理を行い記憶部より決済する暗号化決済処理用クレジットカード情報と認証情報と識別情報と第二の鍵が取得され、前記端末装置送信部より送信され、前記決済代行処理サーバ装置に受信したユーザ認証情報とユーザ識別情報は、前記暗号化処理部により、フィールド単位毎に暗号化するための文字数列を与えられ当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列を生成し、前記記憶部に記憶されている暗号化認証情報と暗号化識別情報の暗号化文字数列と完全一致した暗号化認証情報と暗号化識別情報を呼び出し復号化するための第一の鍵を生成し、前記暗号化認証情報と暗号化識別情報を復号化させる復号化処理ステップと、

前記復号化処理部で復号化するために生成された第一の鍵と前記端末装置より送信された第二の鍵を用いて第三の鍵を生成される鍵生成処理ステップと、

前記端末装置より送信された暗号化決済処理用クレジット情報を第三の鍵で復号化する復号化処理ステップと、

決済処理を行う金融機関に決済処理に関する金融情報とともに送信する送信ステップと

を具備することを特徴とする決済代行処理方法。

[9] 請求項７記載のサーバ装置に前記端末装置より決済依頼処理情報と復号鍵と識別情報と認証情報を受信し、当該決済依頼処理を実行する当該金融機関サーバ装置とを含んで構成されることを特徴とする金融機関決済処理システム。

[10] 端末装置と決済代行処理サーバ装置がインターネットを介して接続された決済依頼情報提供装置において、 前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されているユーザ識別

するための識別情報を取得し、送信部より前記決済代行処理サーバ装置に受信される受信部と、前記受信部より受信されたユーザ認証情報とユーザ識別情報とクレジットカード情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理部と、当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字列の暗号化認証情報と暗号化識別情報と暗号化クレジットカード情報を生成させる暗号化処理部と、前記決済代行処理サーバ装置に外部の商品決済依頼情報提供装置から商品をクレジットガードによる決済処理依頼情報が与えられると、当該決済依頼情報に含まれているクレジットカード情報と認証情報を、前記共通鍵処理部によりクレジットカード情報と認証情報をフィールド単位毎に暗号化するための文字数を与える。暗号化するための文字数を、当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化クレジット情報と暗号化認証情報を動的に生成させる暗号化処理部と、
前記決済代行処理サーバ装置における記憶部の記憶されている暗号化クレジット情報と暗号化認証情報の暗号化文字数列と完全一致するか否かを判断し、及び／もしくは完全一致しない場合、処理を停止させる制御処理部と、
当該外部の商品決算依頼情報提供装置に決済処理停止命令を送信する送信部を有する決済代行処理サーバ装置。

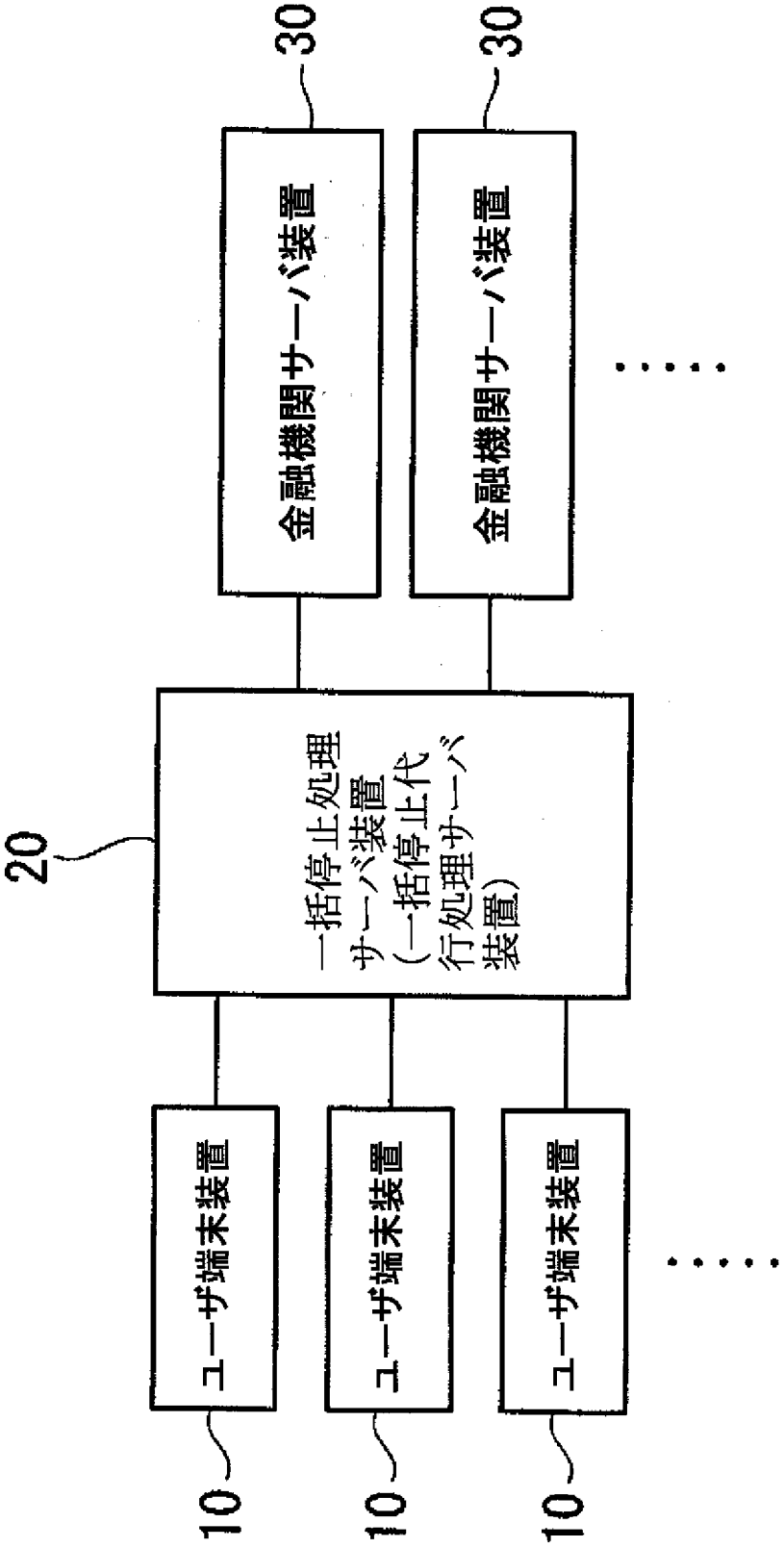
[11] 端末装置と決済代行処理サーバ装置がインターネットを介して接続された決済依頼情報提供装置において、 前記端末装置における入力部よりユーザの入力操作に応じて入力された情報登録用のユーザ認証情報とユーザクレジットカード情報と前記端末装置における記憶部に記憶されているユーザ識別するための識別情報を取得し、送信部より前記決済代行処理サーバ装置に受信される受信ステップと、前記受信部より受信されたユーザ認証情報とユーザ識別情報とクレジットカード情報にフィールド単位毎に暗号化するための文字数を与える共通鍵処理ステップと、当該情報の文字数列に前記暗号化共通鍵文字数を埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字列の暗号化認証情報と暗号化識別情報と暗号化クレジットカード情報を生成さ

せる暗号化処理ステップと、前記決済代行処理サーバ装置に外部の商品決済依頼情報提供装置から商品をクレジットガードによる決済処理依頼情報が与えられると、当該決済依頼情報に含まれているクレジットカード情報と認証情報を、前記共通鍵処理部によりクレジットカード情報と認証情報をフィールド単位毎に暗号化するための文字数を与える。暗号化するための文字数を、当該情報の文字数列に埋め込み、元文字数列の順位を壊さず５倍以下の暗号化文字数列で暗号化クレジット情報と暗号化認証情報を動的に生成させる暗号化処理ステップと、　前記決済代行処理サーバ装置における記憶部の記憶されている暗号化クレジット情報と暗号化認証情報の暗号化文字数列と完全一致するか否かを判断し、及び／もしくは完全一致しない場合、処理を停止させる制御処理ステップと、　当該外部の商品決算依頼情報提供装置に決済処理停止命令を送信する送信部を有する決済代行処理方法。

[12] 前記決済代行処理サーバ装置はクレジットカード決済をおこなう金融機関サーバ装置に備えることを特徴とする請求項１０記載の決済処理サーバ装置。

[13] 請求項１０記載の決済代行処理サーバ装置における送信部から暗号化金融情報を送信し、ネットワークを介して金融機関サーバ装置に暗号化されたまま当該暗号化金融情報を受信し、ユーザ端末装置における送信部から暗号化金融情報を復号化させる第二の鍵と暗号化決済処理用金融情報を前記金融機関サーバ装置に直接送信し、当該決済処理を実行する当該金融機関サーバ装置と、　を含んで構成される決済処理システム。

[図1]


30
30
金融機関サーバ装置
金融機関サーバ装置
・・・・
20
一括停止処理サーバ装置（一括停止代行処理サーバ装置）
ユーザ端末装置
ユーザ端末装置
ユーザ端末装置
・・・・
10
10
10

[図2]

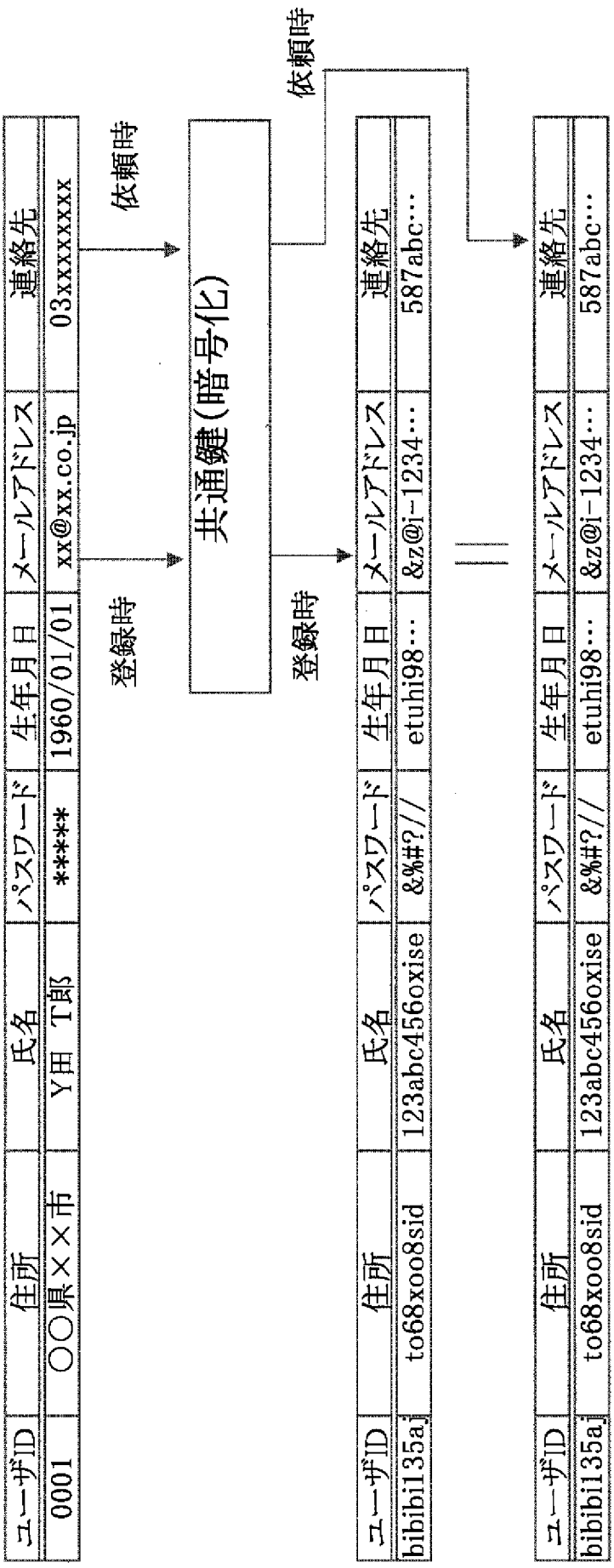
識別情報

ユーザID	識別情報
0001	24692・・・・
0002	13578・・・・
・・・	・・・

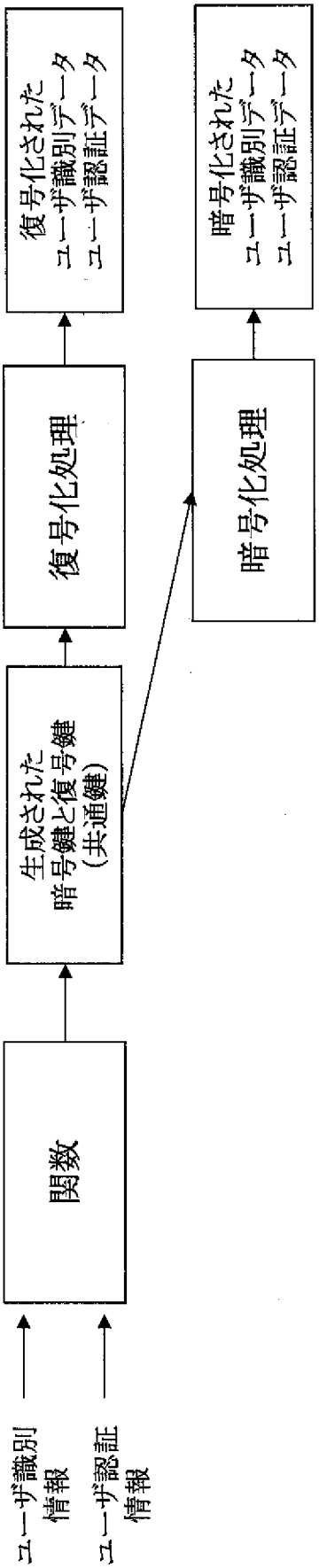
[図3A]

ユーザID	住所	氏名	パスワード	生年月日	メールアドレス	連絡先
0001	○○県××市	Y田 T郎	******	1960/01/01	xx@xx.co.jp	03xxxxxxxx
0002	△△県□□市	U田 S子	******	1987/10/07	boku@…	045xxxxxxx
…	…	…	…	…	…	…

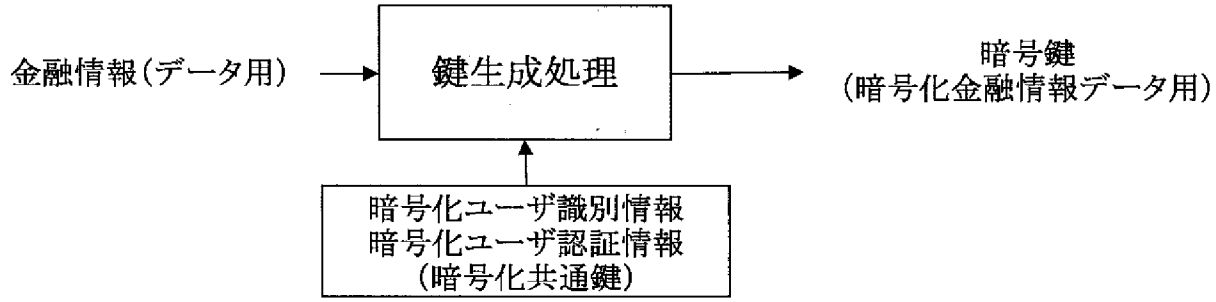
[図3B]


ユーザID
住所
氏名
パスワード
生年月日
メールアドレス
連絡先
0001
○○県××市
Y田 T郎
******
1960/01/01
xx@xx.co.jp
03xxxxxxxx
依頼時
登録時
共通鍵(暗号化)
依頼時
登録時
ユーザID
住所
氏名
パスワード
生年月日
メールアドレス
連絡先
bibibi135aj
to68xoo8sid
123abc456oxise
&%#?//
etuhi98…
&z@i-1234…
587abc…
ユーザID
住所
氏名
パスワード
生年月日
メールアドレス
連絡先
bibibi135aj
to68xoo8sid
123abc456oxise
&%#?//
etuhi98…
&z@i-1234…
587abc…

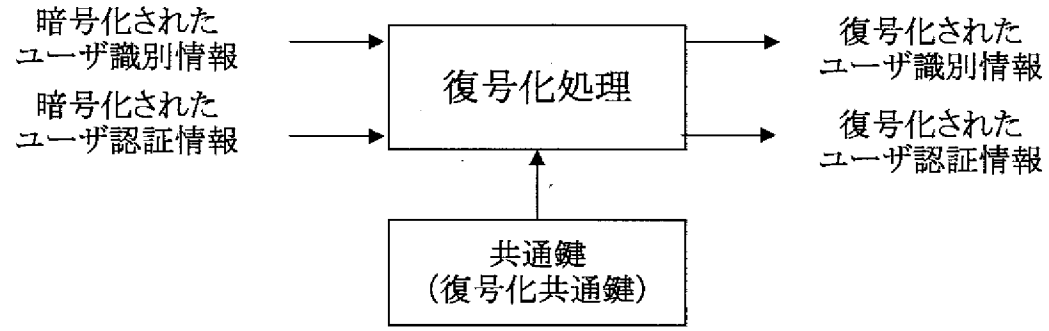
[図4A]


ユーザ識別情報
ユーザ認証情報
関数
生成された暗号鍵と復号鍵(共通鍵)
復号化処理
復号化されたユーザ識別データユーザ認証データ
暗号化処理
暗号化されたユーザ識別データユーザ認証データ

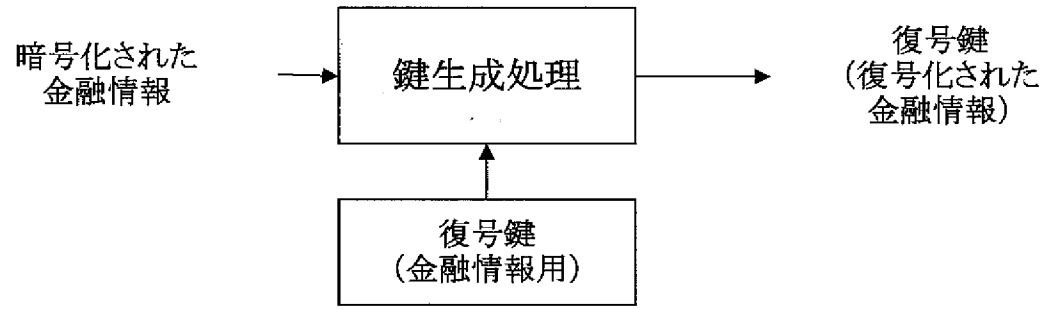
[図4B]


金融情報(データ用)
鍵生成処理
暗号鍵
(暗号化金融情報データ用)
暗号化ユーザ識別情報
暗号化ユーザ認証情報
(暗号化共通鍵)

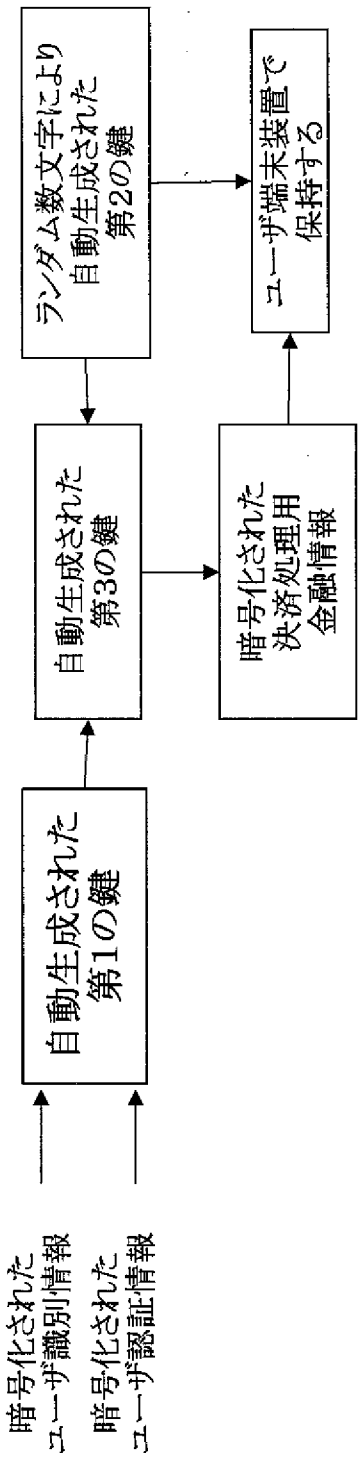
[図4C]


暗号化された
ユーザ識別情報
暗号化された
ユーザ認証情報
復号化処理
復号化された
ユーザ識別情報
復号化された
ユーザ認証情報
共通鍵
(復号化共通鍵)

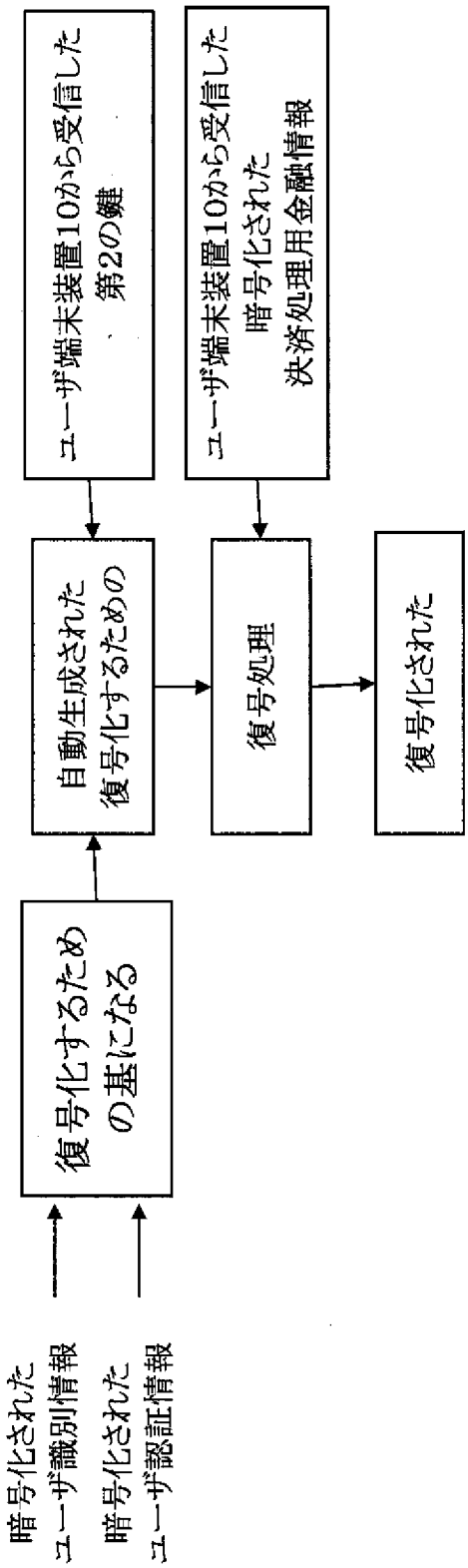
[図4D]


暗号化された
金融情報
鍵生成処理
復号鍵
(復号化された
金融情報)
復号鍵
(金融情報用)

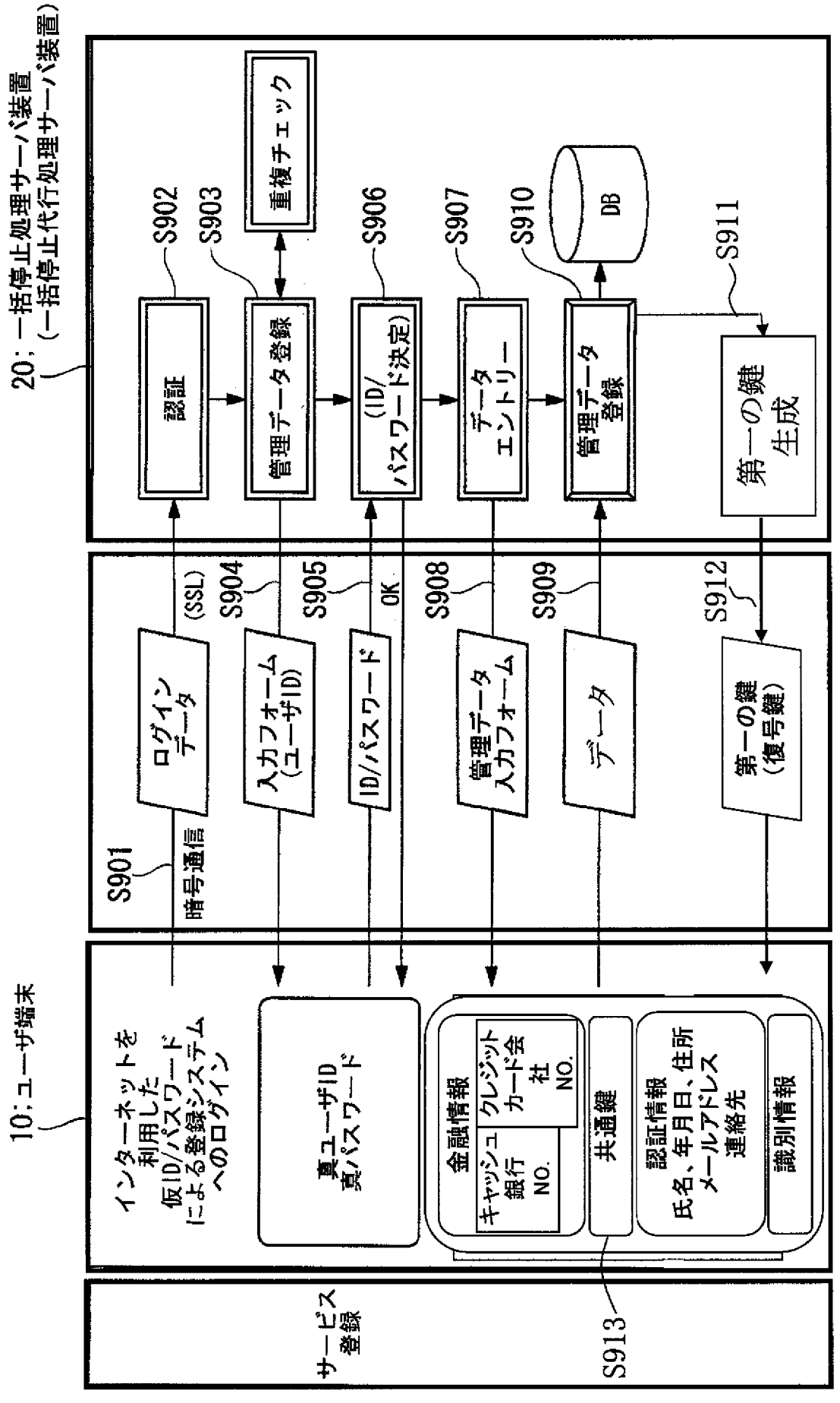
[図4E]


暗号化された
ユーザ識別情報
暗号化された
ユーザ認証情報
自動生成された
第1の鍵
自動生成された
第3の鍵
ランダム数文字により
自動生成された
第2の鍵
暗号化された
決済処理用
金融情報
ユーザ端末装置で
保持する

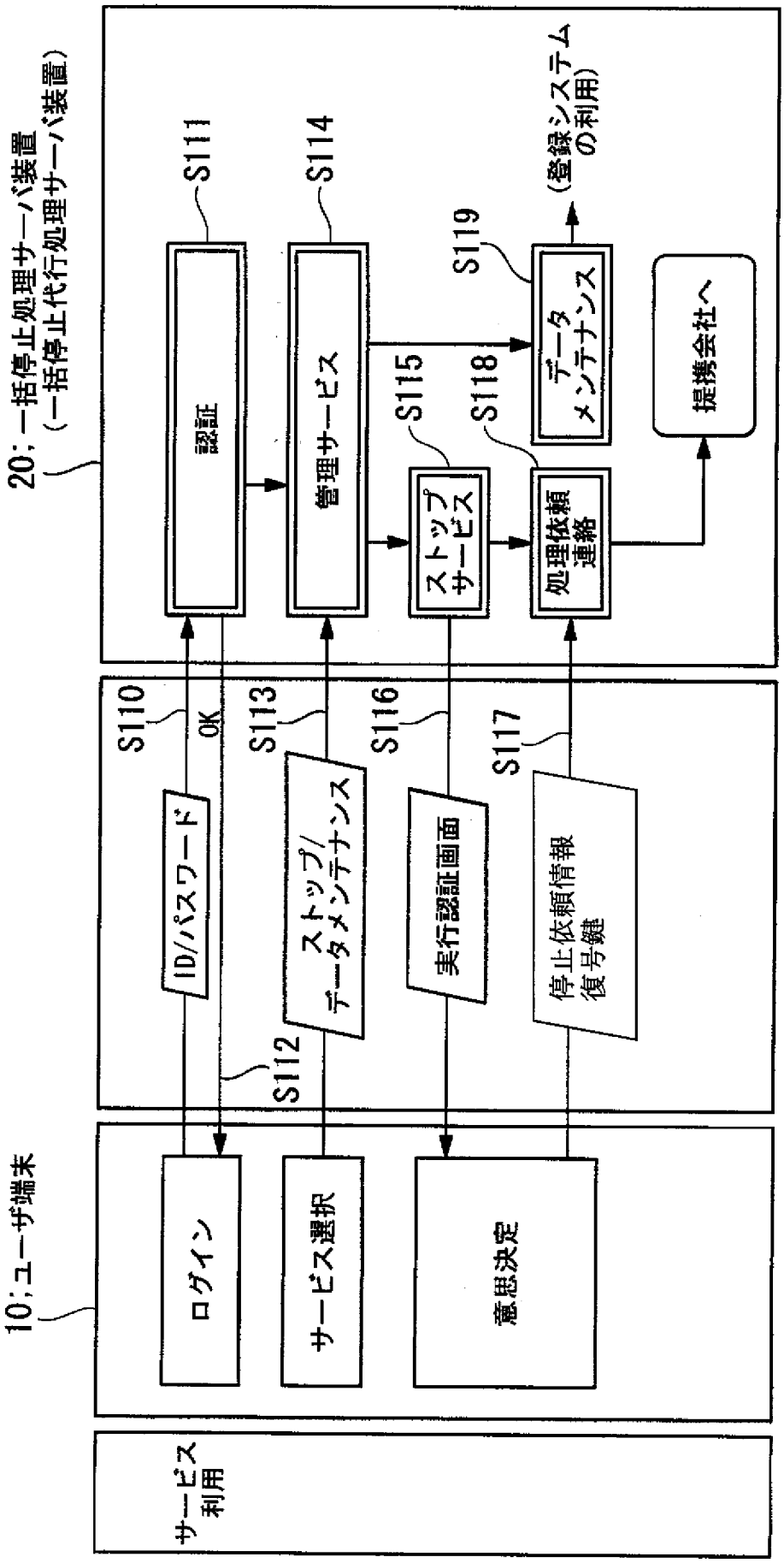
[図4F]


暗号化された
ユーザ識別情報
暗号化された
ユーザ認証情報
復号化するための
の基になる
自動生成された
復号化するための
ユーザ端末装置10から受信した
第2の鍵
復号処理
ユーザ端末装置10から受信した
暗号化された
決済処理用金融情報
復号化された

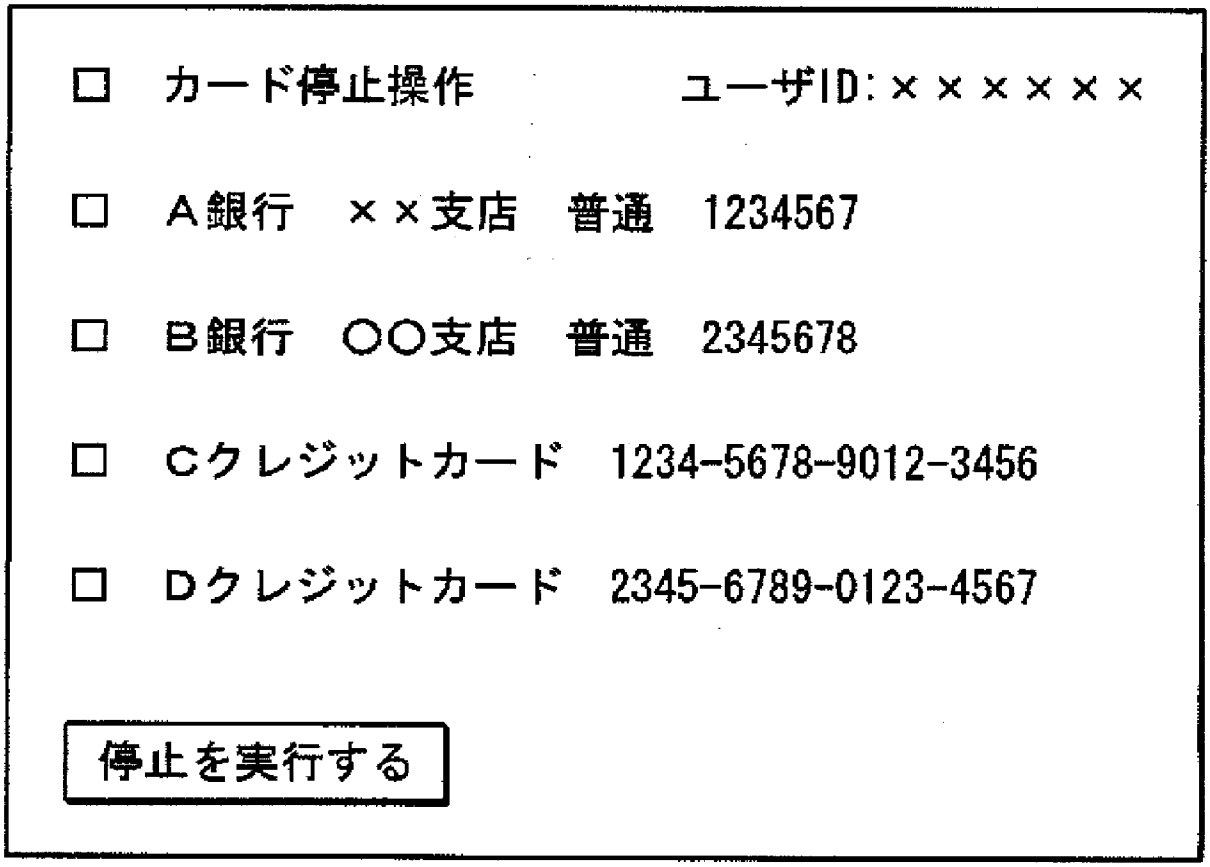
[図5]


20;一括停止処理サーバ装置
(一括停止代行処理サーバ装置)
10;ユーザ端末
認証
管理データ登録
重複チェック
(ID/
パスワード決定)
データ
エントリー
管理データ
登録
DB
第一の鍵
生成
S902
S903
S906
S907
S910
S911
S901
S904
S905
S908
S909
S912
暗号通信
(SSL)
ログイン
データ
入力フォーム
(ユーザID)
ID/パスワード
OK
管理データ
入力フォーム
データ
第一の鍵
(復号鍵)
インターネットを
利用した
仮ID/パスワード
による登録システム
へのログイン
真ユーザID
真パスワード
金融情報
キャッシュ
銀行
NO.
クレジット
カード会
社
NO.
共通鍵
認証情報
氏名、年月日、住所
メールアドレス
連絡先
識別情報
サービス
登録
S913

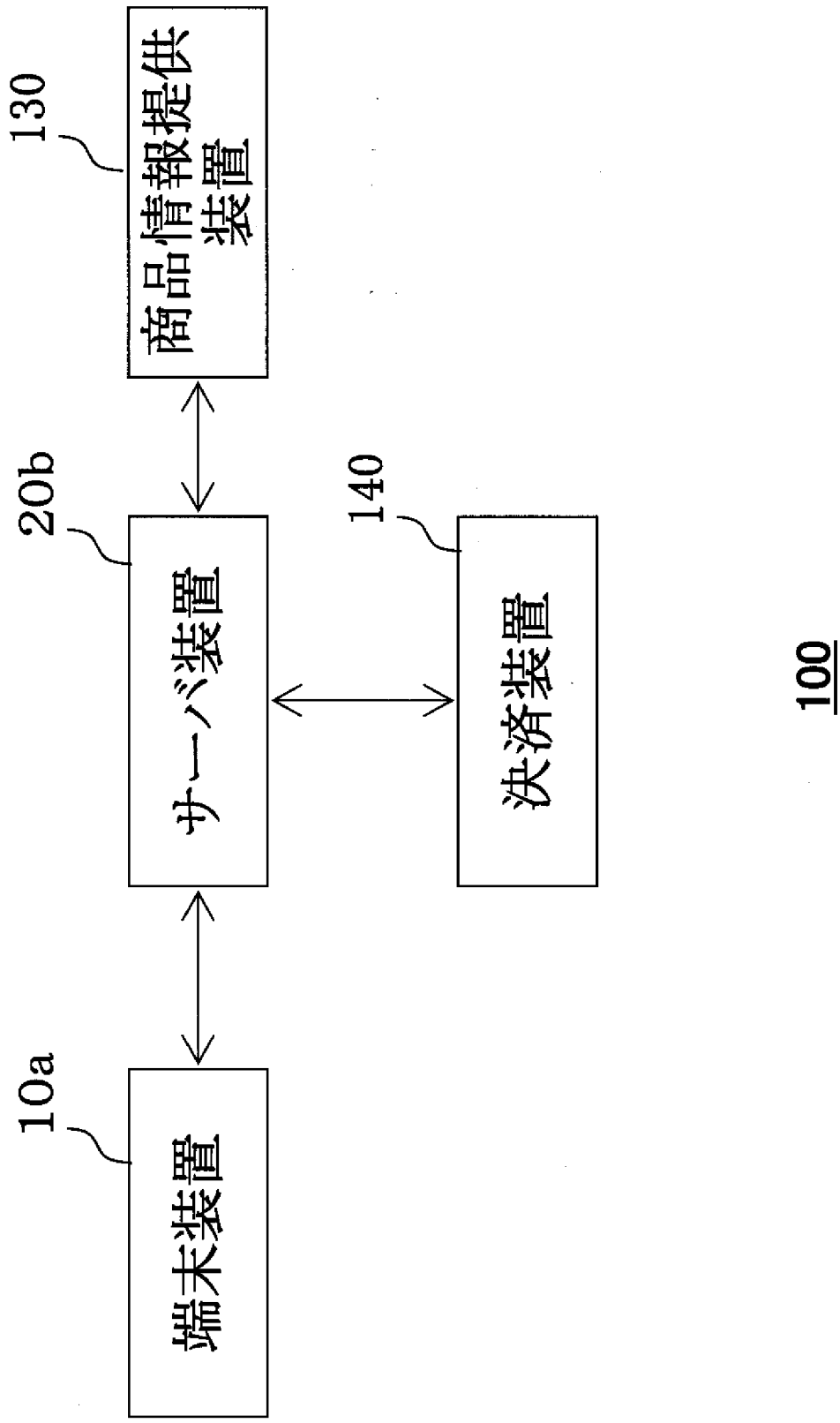
[図6]


20;一括停止処理サーバ装置
(一括停止代行処理サーバ装置)
10;ユーザ端末
サービス利用
認証
管理サービス
ストップサービス
処理依頼連絡
データメンテナンス
(登録システムの利用)
提携会社へ
S111
S114
S115
S118
S119
S110
S113
S116
S117
S112
OK
ID/パスワード
ストップ/データメンテナンス
実行認証画面
停止依頼情報復号鍵
ログイン
サービス選択
意思決定

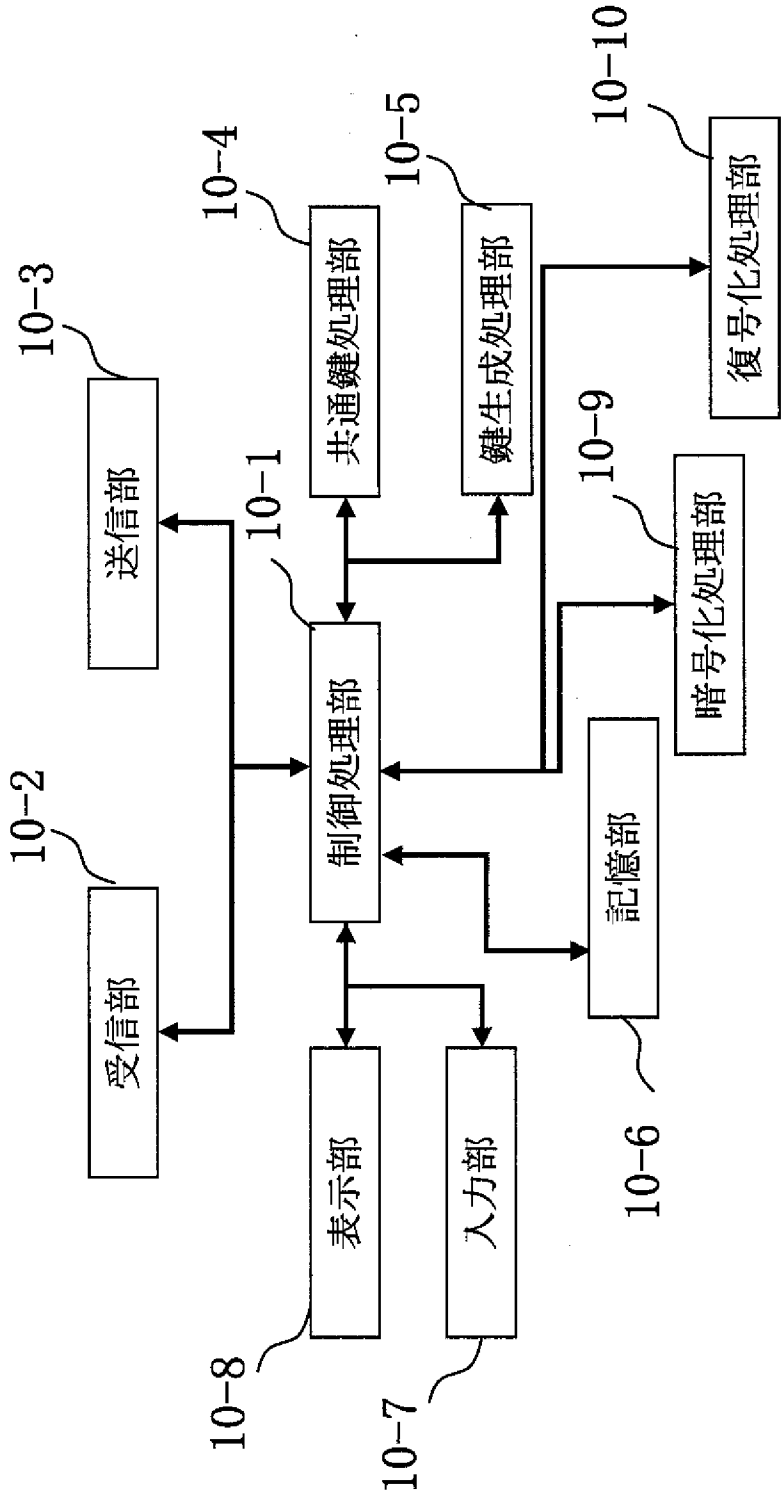
[図7]


□ カード停止操作 ユーザID:××××××
□ A銀行 ××支店 普通 1234567
□ B銀行 ○○支店 普通 2345678
□ Cクレジットカード 1234-5678-9012-3456
□ Dクレジットカード 2345-6789-0123-4567
停止を実行する

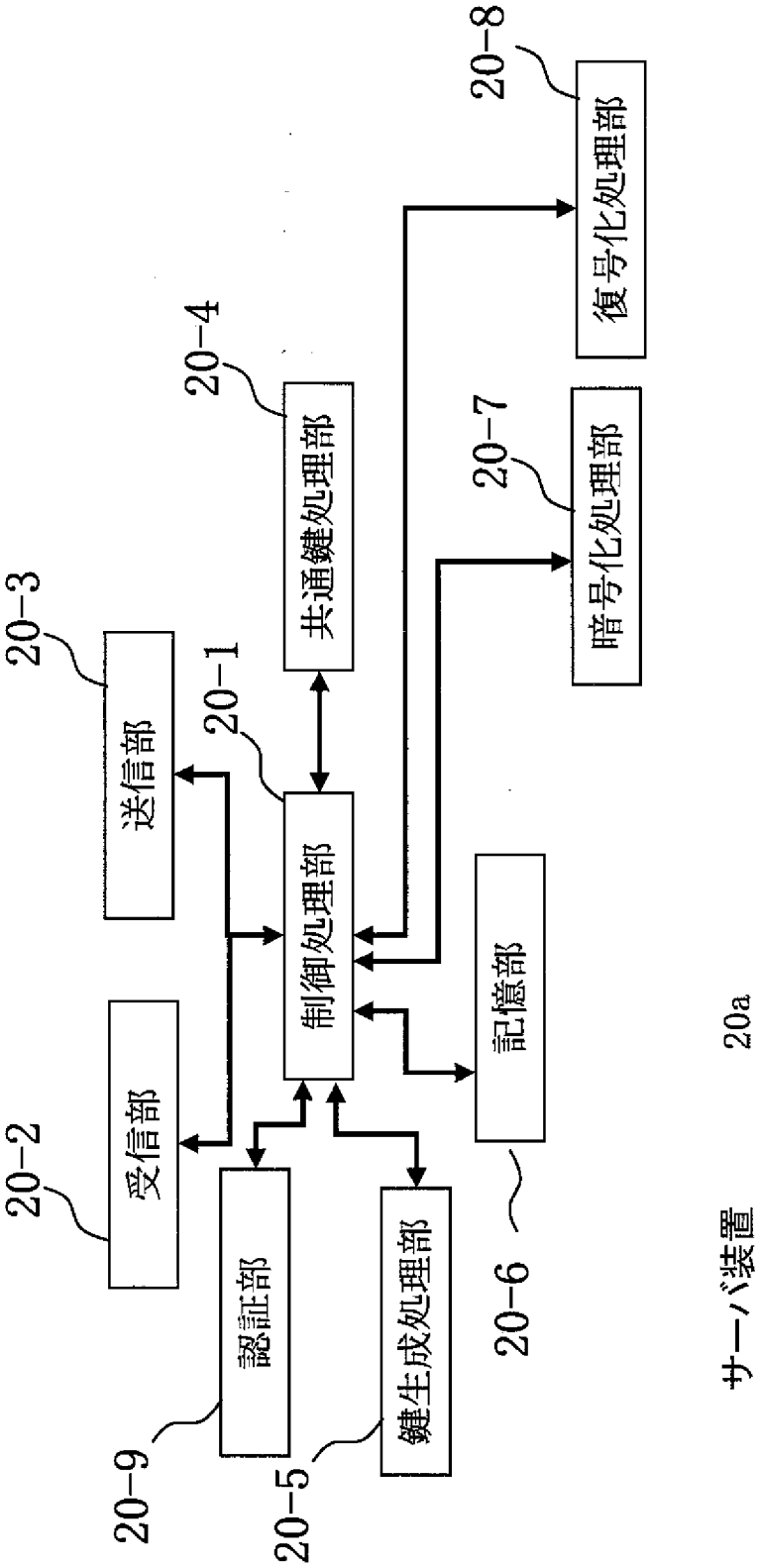
[図8]



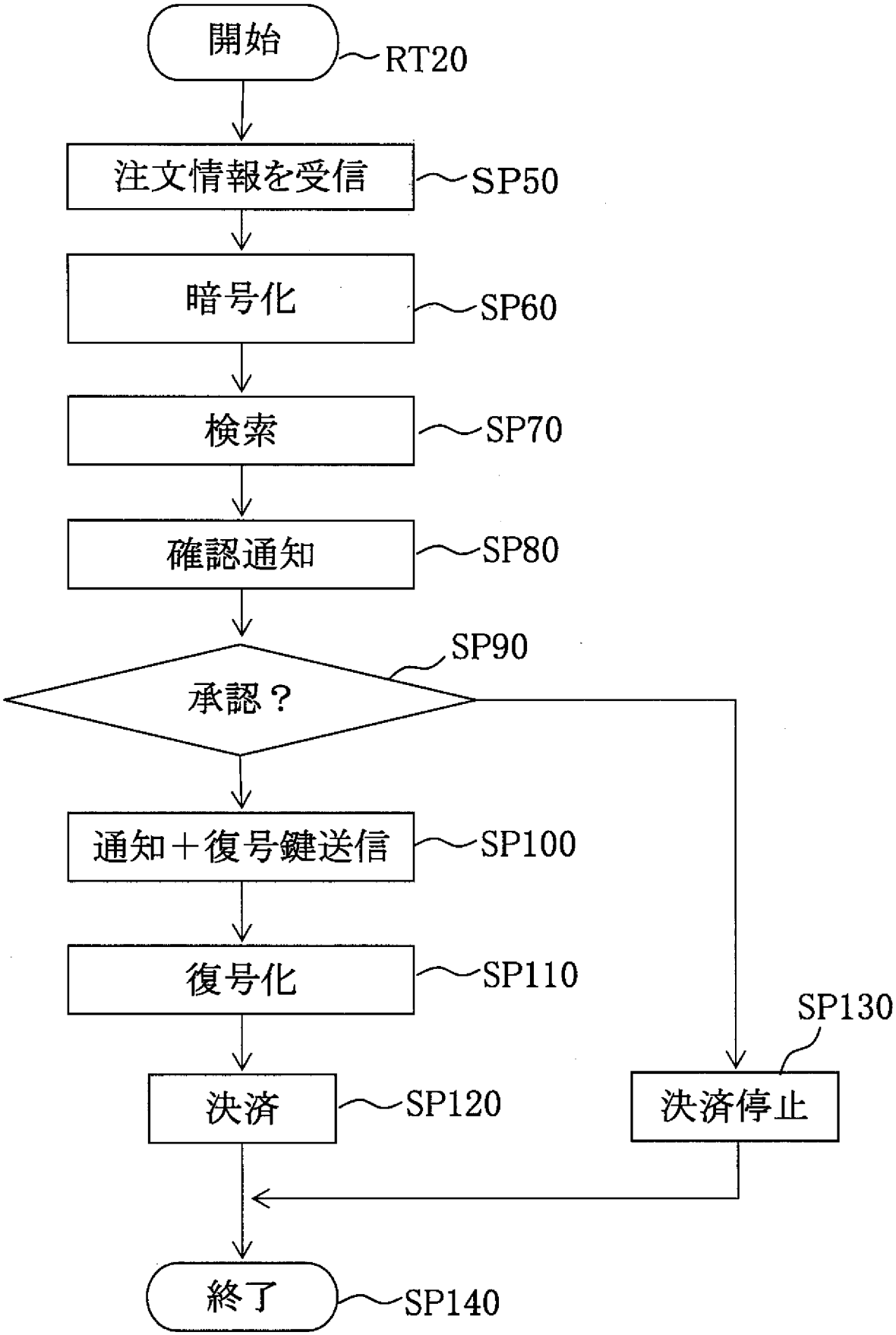
[図9]


10-10
10-4
10-5
10-3
共通鍵処理部
鍵生成処理部
復号化処理部
送信部
10-1
10-9
制御処理部
暗号化処理部
10-2
記憶部
受信部
10-6
表示部
入力部
10-8
10-7
端末装置 10a

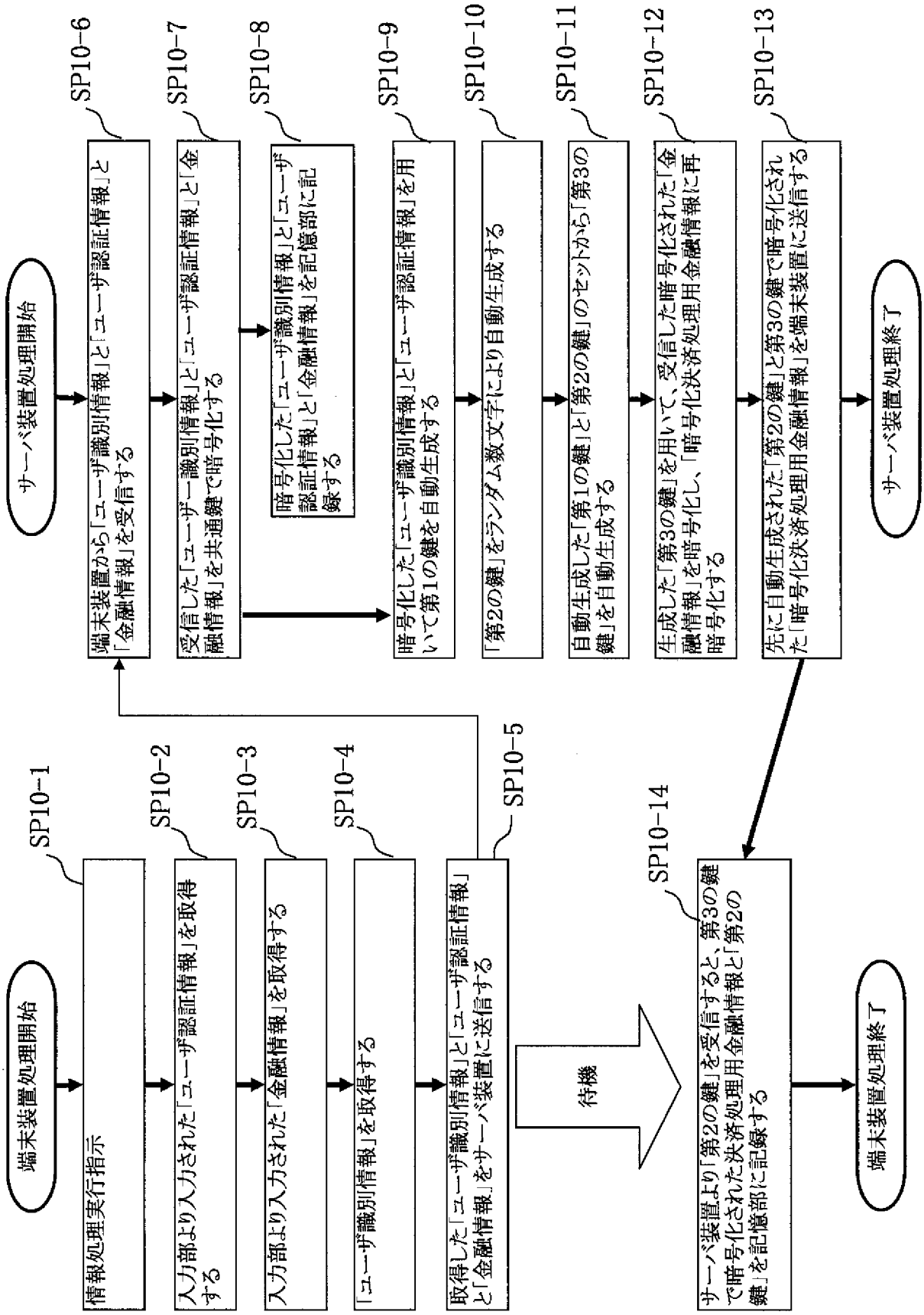
[図10]


20-8
復号化処理部
20-4
共通鍵処理部
20-7
暗号化処理部
20-3
送信部
20-1
制御処理部
20-2
受信部
記憶部
20-6
認証部
20-9
鍵生成処理部
20-5
サーバ装置
20a

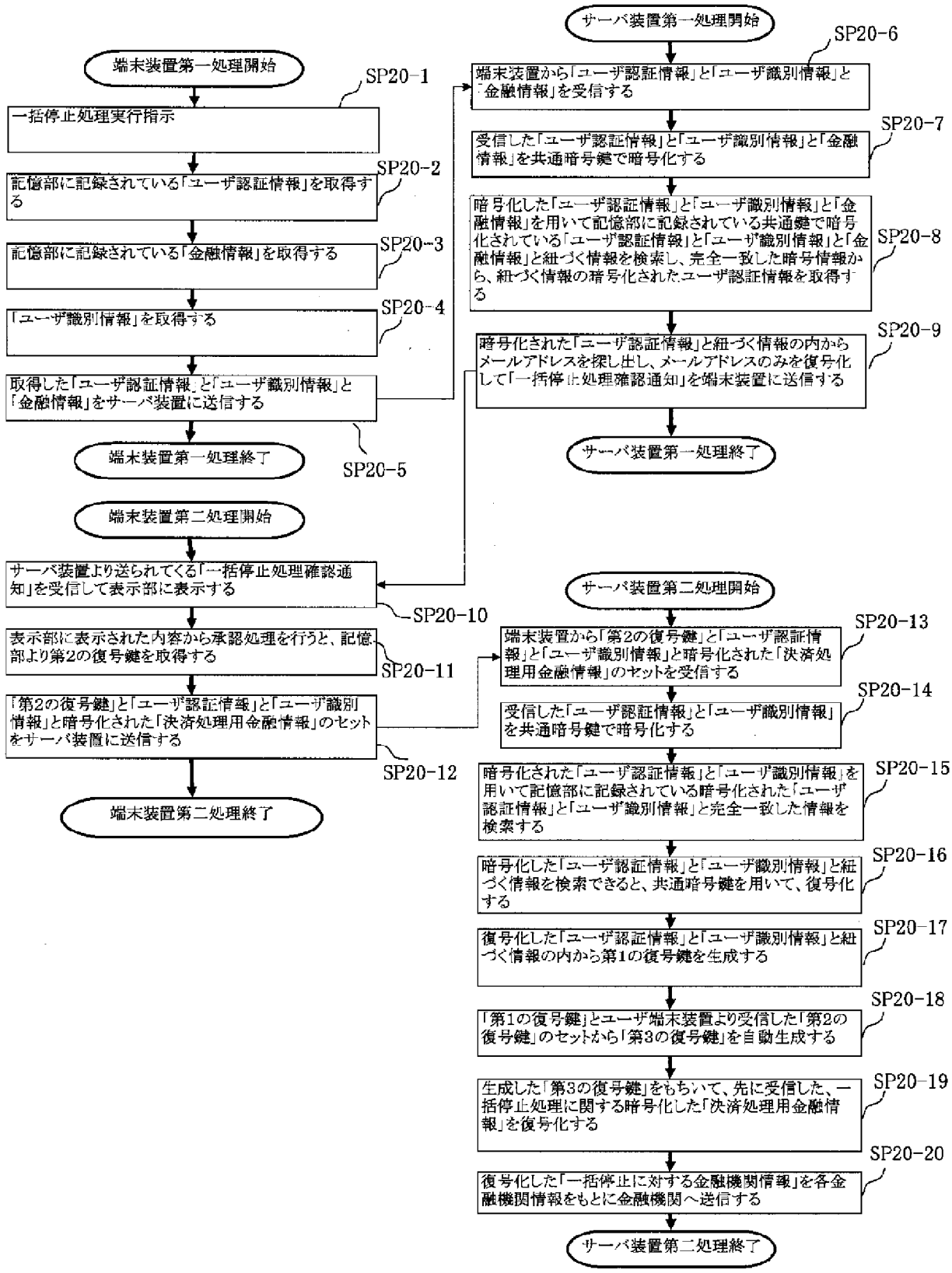
[図11]


開始
RT20
注文情報を受信
SP50
暗号化
SP60
検索
SP70
確認通知
SP80
SP90
承認？
通知＋復号鍵送信
SP100
復号化
SP110
SP130
決済
SP120
決済停止
終了
SP140

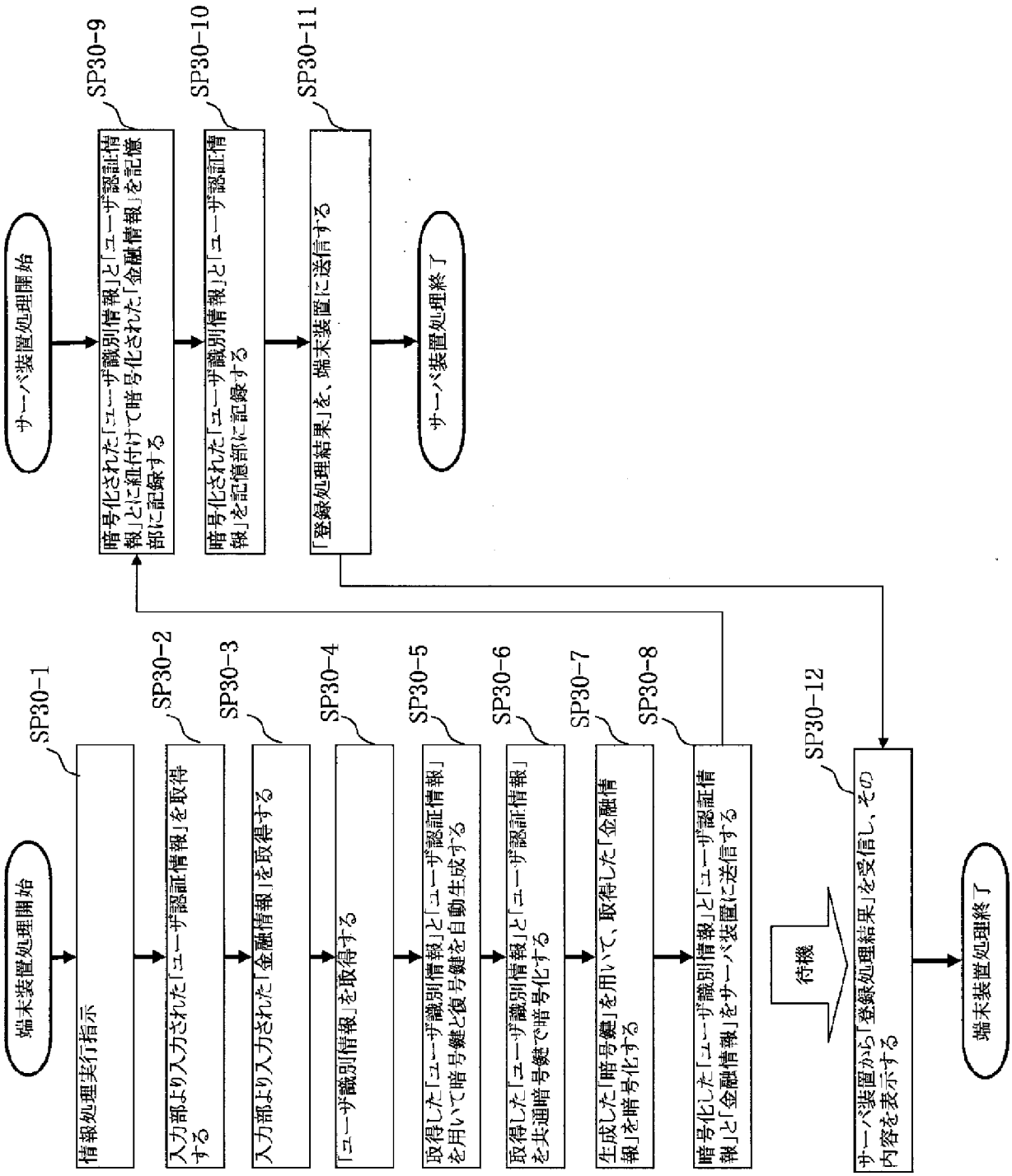
[図12]


端末装置処理開始
SP10-1
情報処理実行指示
SP10-2
入力部より入力された「ユーザ認証情報」を取得する
SP10-3
入力部より入力された「金融情報」を取得する
SP10-4
「ユーザ識別情報」を取得する
SP10-5
取得した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」をサーバ装置に送信する
待機
SP10-14
サーバ装置より「第2の鍵」を受信すると、第3の鍵で暗号化された決済処理用金融情報と「第2の鍵」を記憶部に記録する
端末装置処理終了
サーバ装置処理開始
SP10-6
端末装置から「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」を受信する
SP10-7
受信した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」を共通鍵で暗号化する
SP10-8
暗号化した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」を記憶部に記録する
SP10-9
暗号化した「ユーザ識別情報」と「ユーザ認証情報」を用いて第1の鍵を自動生成する
SP10-10
「第2の鍵」をランダム数文字により自動生成する
SP10-11
自動生成した「第1の鍵」と「第2の鍵」のセットから「第3の鍵」を自動生成する
SP10-12
生成した「第3の鍵」を用いて、受信した暗号化された「金融情報」を暗号化し、「暗号化決済処理用金融情報に再暗号化する
SP10-13
先に自動生成された「第2の鍵」と第3の鍵で暗号化された「暗号化決済処理用金融情報」を端末装置に送信する
サーバ装置処理終了

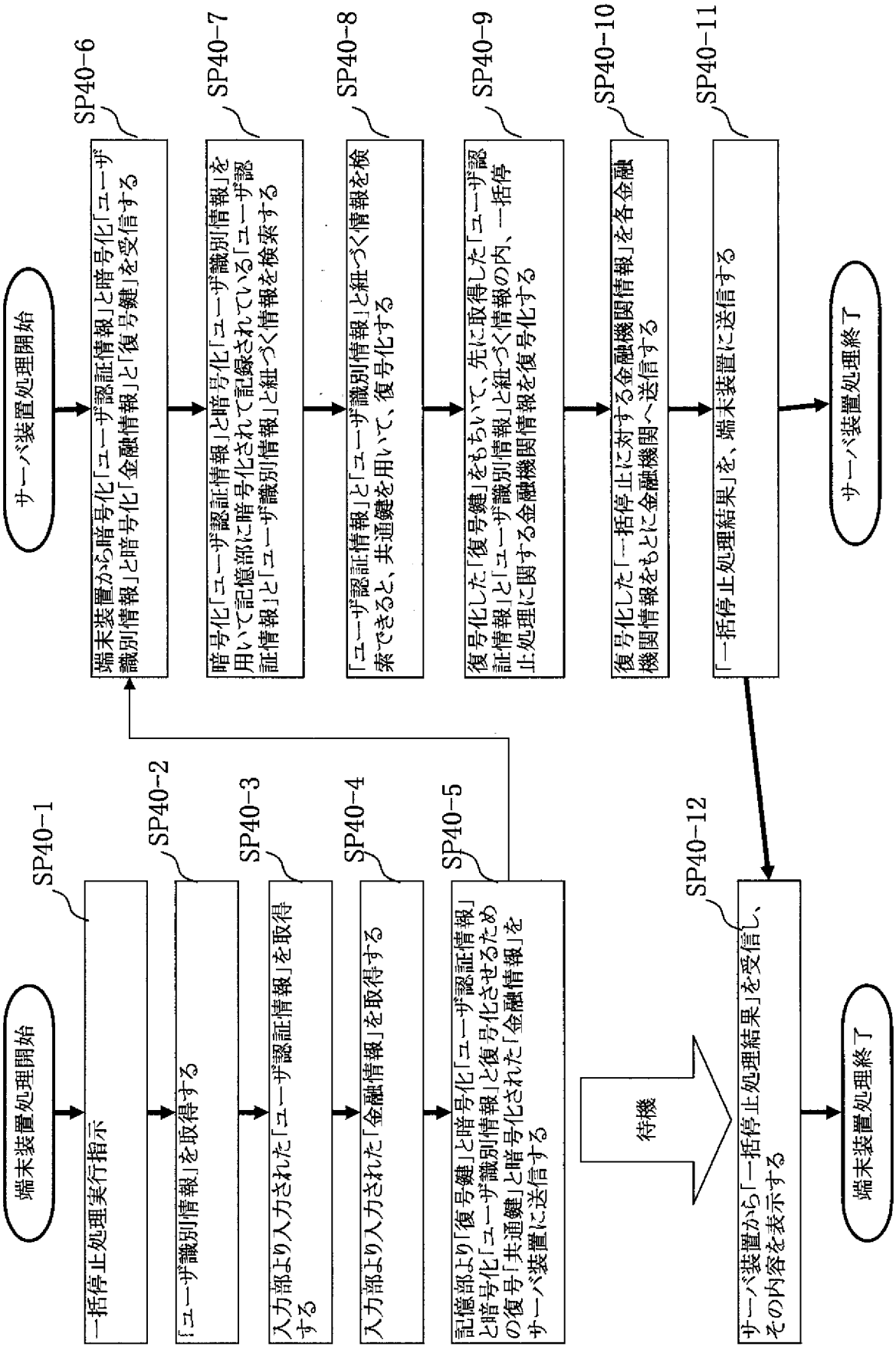
[図13]


端末装置第一処理開始
SP20-1
一括停止処理実行指示
SP20-2
記憶部に記録されている「ユーザ認証情報」を取得する
SP20-3
記憶部に記録されている「金融情報」を取得する
SP20-4
「ユーザ識別情報」を取得する
取得した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」をサーバ装置に送信する
SP20-5
端末装置第一処理終了
端末装置第二処理開始
サーバ装置より送られてくる「一括停止処理確認通知」を受信して表示部に表示する
SP20-10
表示部に表示された内容から承認処理を行うと、記憶部より第2の復号鍵を取得する
SP20-11
「第2の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットをサーバ装置に送信する
SP20-12
端末装置第二処理終了
サーバ装置第一処理開始
SP20-6
端末装置から「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を受信する
SP20-7
受信した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を共通暗号鍵で暗号化する
SP20-8
暗号化した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を用いて記憶部に記録されている共通鍵で暗号化されている「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」と紐づく情報を検索し、完全一致した暗号情報から、紐づく情報の暗号化されたユーザ認証情報を取得する
SP20-9
暗号化された「ユーザ認証情報」と紐づく情報の内からメールアドレスを探し出し、メールアドレスのみを復号化して「一括停止処理確認通知」を端末装置に送信する
サーバ装置第一処理終了
サーバ装置第二処理開始
SP20-13
端末装置から「第2の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットを受信する
SP20-14
受信した「ユーザ認証情報」と「ユーザ識別情報」を共通暗号鍵で暗号化する
SP20-15
暗号化された「ユーザ認証情報」と「ユーザ識別情報」を用いて記憶部に記録されている暗号化された「ユーザ認証情報」と「ユーザ識別情報」と完全一致した情報を検索する
SP20-16
暗号化した「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索できると、共通暗号鍵を用いて、復号化する
SP20-17
復号化した「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報の内から第1の復号鍵を生成する
SP20-18
「第1の復号鍵」とユーザ端末装置より受信した「第2の復号鍵」のセットから「第3の復号鍵」を自動生成する
SP20-19
生成した「第3の復号鍵」をもちいて、先に受信した、一括停止処理に関する暗号化した「決済処理用金融情報」を復号化する
SP20-20
復号化した「一括停止に対する金融機関情報」を各金融機関情報をもとに金融機関へ送信する
サーバ装置第二処理終了

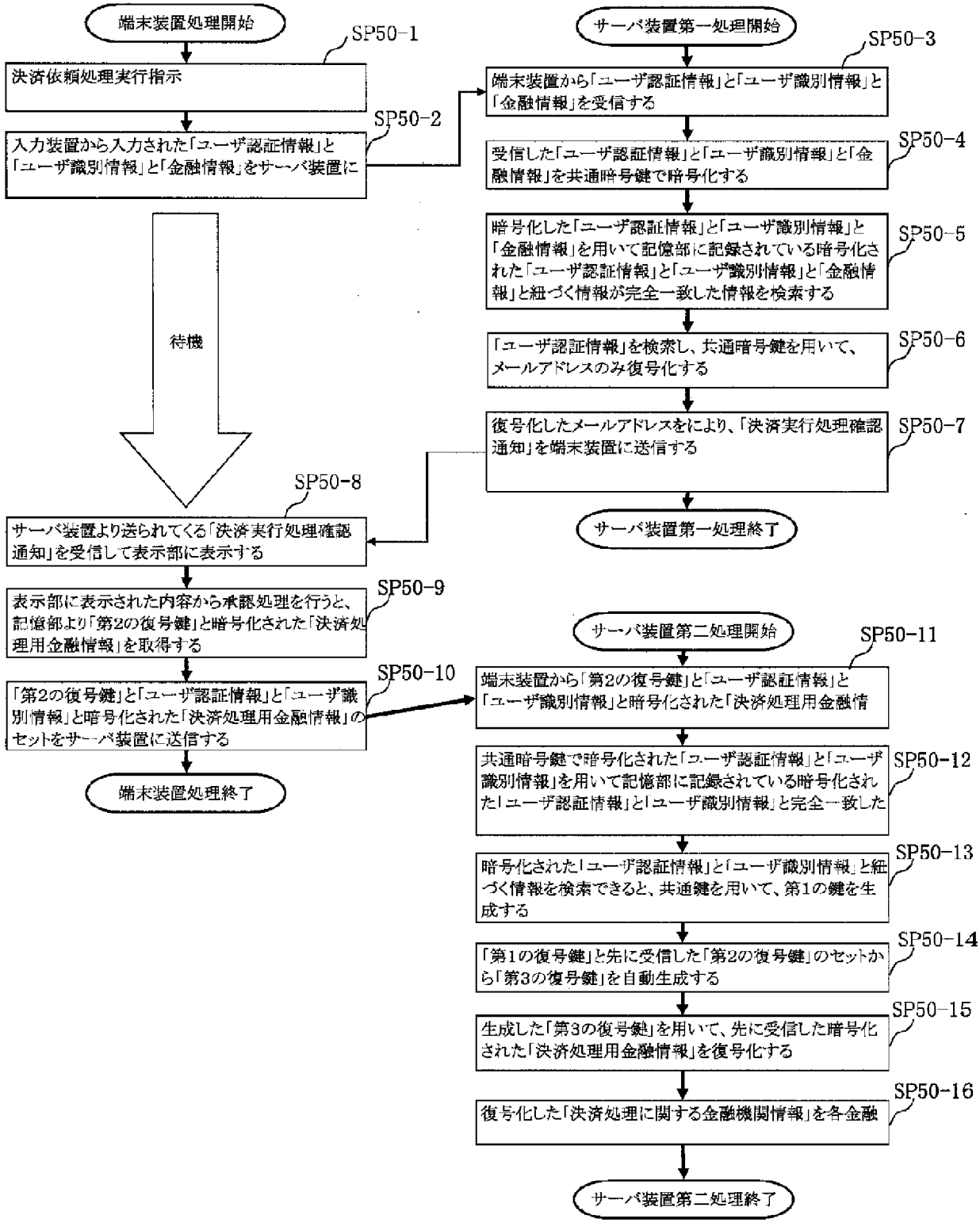
[図14]


端末装置処理開始
SP30-1
情報処理実行指示
SP30-2
入力部より入力された「ユーザ認証情報」を取得する
SP30-3
入力部より入力された「金融情報」を取得する
SP30-4
「ユーザ識別情報」を取得する
SP30-5
取得した「ユーザ識別情報」と「ユーザ認証情報」を用いて暗号鍵と復号鍵を自動生成する
SP30-6
取得した「ユーザ識別情報」と「ユーザ認証情報」を共通暗号鍵で暗号化する
SP30-7
生成した「暗号鍵」を用いて、取得した「金融情報」を暗号化する
SP30-8
暗号化した「ユーザ識別情報」と「ユーザ認証情報」と「金融情報」をサーバ装置に送信する
待機
SP30-12
サーバ装置から「登録処理結果」を受信し、その内容を表示する
端末装置処理終了
サーバ装置処理開始
SP30-9
暗号化された「ユーザ識別情報」と「ユーザ認証情報」とに紐付けて暗号化された「金融情報」を記憶部に記録する
SP30-10
暗号化された「ユーザ識別情報」と「ユーザ認証情報」を記憶部に記録する
SP30-11
「登録処理結果」を、端末装置に送信する
サーバ装置処理終了

[図15]


端末装置処理開始
SP40-1
一括停止処理実行指示
SP40-2
「ユーザ識別情報」を取得する
SP40-3
入力部より入力された「ユーザ認証情報」を取得する
SP40-4
入力部より入力された「金融情報」を取得する
SP40-5
記憶部より「復号鍵」と暗号化「ユーザ認証情報」と暗号化「ユーザ識別情報」と復号化させるための復号「共通鍵」と暗号化された「金融情報」をサーバ装置に送信する
待機
SP40-12
サーバ装置から「一括停止処理結果」を受信し、その内容を表示する
端末装置処理終了
サーバ装置処理開始
SP40-6
端末装置から暗号化「ユーザ認証情報」と暗号化「ユーザ識別情報」と暗号化「金融情報」と「復号鍵」を受信する
SP40-7
暗号化「ユーザ認証情報」と暗号化「ユーザ識別情報」を用いて記憶部に暗号化されて記録されている「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索する
SP40-8
「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索できると、共通鍵を用いて、復号化する
SP40-9
復号化した「復号鍵」をもちいて、先に取得した「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報の内、一括停止処理に関する金融機関情報を復号化する
SP40-10
復号化した「一括停止に対する金融機関情報」を各金融機関情報をもとに金融機関へ送信する
SP40-11
「一括停止処理結果」を、端末装置に送信する
サーバ装置処理終了

[図16]


端末装置処理開始
SP50-1
決済依頼処理実行指示
SP50-2
入力装置から入力された「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」をサーバ装置に
待機
SP50-8
サーバ装置より送られてくる「決済実行処理確認通知」を受信して表示部に表示する
SP50-9
表示部に表示された内容から承認処理を行うと、記憶部より「第2の復号鍵」と暗号化された「決済処理用金融情報」を取得する
SP50-10
「第2の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情報」のセットをサーバ装置に送信する
端末装置処理終了
サーバ装置第一処理開始
SP50-3
端末装置から「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を受信する
SP50-4
受信した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を共通暗号鍵で暗号化する
SP50-5
暗号化した「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」を用いて記憶部に記録されている暗号化された「ユーザ認証情報」と「ユーザ識別情報」と「金融情報」と紐づく情報が完全一致した情報を検索する
SP50-6
「ユーザ認証情報」を検索し、共通暗号鍵を用いて、メールアドレスのみ復号化する
SP50-7
復号化したメールアドレスをにより、「決済実行処理確認通知」を端末装置に送信する
サーバ装置第一処理終了
サーバ装置第二処理開始
SP50-11
端末装置から「第2の復号鍵」と「ユーザ認証情報」と「ユーザ識別情報」と暗号化された「決済処理用金融情
SP50-12
共通暗号鍵で暗号化された「ユーザ認証情報」と「ユーザ識別情報」を用いて記憶部に記録されている暗号化された「ユーザ認証情報」と「ユーザ識別情報」と完全一致した
SP50-13
暗号化された「ユーザ認証情報」と「ユーザ識別情報」と紐づく情報を検索できると、共通鍵を用いて、第1の鍵を生成する
SP50-14
「第1の復号鍵」と先に受信した「第2の復号鍵」のセットから「第3の復号鍵」を自動生成する
SP50-15
生成した「第3の復号鍵」を用いて、先に受信した暗号化された「決済処理用金融情報」を復号化する
SP50-16
復号化した「決済処理に関する金融機関情報」を各金融
サーバ装置第二処理終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/000517

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F21/20*(2006.01)i, *G06F21/24*(2006.01)i, *G06Q20/00*(2006.01)i, *H04L9/32*(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)
H04L9/08, G06F21/20, G06F21/24, G06Q20/00, H04L9/32

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 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 7-303104 A (Nippon Telegraph And Telephone Corp.), 14 November, 1995 (14.11.95), Full text; all drawings (Family: none)	1-13
A	JP 2003-69552 A (Koji AMANO), 07 March, 2003 (07.03.03), Par. Nos. [0010] to [0012]; Figs. 1 to 3 (Family: none)	1-13
A	JP 3-203432 A (Fujitsu Ltd.), 05 September, 1991 (05.09.91), Page 3, lower right column, line 9 to page 4, lower left column, line 17; Fig. 1 (Family: none)	1-13

☒ 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
22 April, 2009 (22.04.09)	12 May, 2009 (12.05.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/000517

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-339732 A (ICON Corp.), 14 December, 2006 (14.12.06), Full text; all drawings & WO 2006/129699 A1	1-13
T,X	JP 2009-43196 A (ICON Corp.), 26 February, 2009 (26.02.09), Full text; all drawings (Family: none)	1-13

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０００５１７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/20(2006.01)i, G06F21/24(2006.01)i, G06Q20/00(2006.01)i, H04L9/32(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.　H04L9/08, G06F21/20, G06F21/24, G06Q20/00, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 7-303104 A (日本電信電話株式会社) 1995.11.14, 全文, 全図（ファミリーなし）	１－１３
A	JP 2003-69552 A (天野　光司) 2003.03.07, 段落【００１０】－【００１２】.【図１】－【図３】（ファミリーなし）	１－１３
A	JP 3-203432 A (富士通株式会社) 1991.09.05, 第３頁右下欄第９行－第４頁左下欄第１７行, 第１図（ファミリーなし）	１－１３

☑　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 ２２．０４．２００９	国際調査報告の発送日 １２．０５．２００９
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）　５Ｓ　４２２９ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６

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
Ａ	JP 2006-339732 A (株式会社ＩＣＯＮ) 2006.12.14, 全文, 全図 &WO 2006/129699 A1	１－１３
Ｔ，Ｘ	JP 2009-43196 A (株式会社ＩＣＯＮ) 2009.02.26, 全文, 全図（ファミリーなし）	１－１３