

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3639811号
(P3639811)

(45) 発行日 平成17年4月20日(2005.4.20)

(24) 登録日 平成17年1月21日(2005.1.21)

(51) Int. Cl.⁷

F I

G06F 17/60

G06F 17/60 414

G06F 15/00

G06F 15/00 330B

H04L 9/32

H04L 9/00 675Z

請求項の数 3 (全 18 頁)

(21) 出願番号	特願2001-327113 (P2001-327113)	(73) 特許権者	000005108 株式会社日立製作所 東京都千代田区丸の内一丁目6番6号
(22) 出願日	平成13年10月25日(2001.10.25)	(73) 特許権者	599175026 株式会社ユーエフジェイ銀行 愛知県名古屋市中区錦三丁目21番24号
(65) 公開番号	特開2003-132290 (P2003-132290A)	(74) 代理人	100075096 弁理士 作田 康夫
(43) 公開日	平成15年5月9日(2003.5.9)	(72) 発明者	江頭 剛雄 神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所 金融システム事業部内
審査請求日	平成13年11月1日(2001.11.1)	(72) 発明者	近藤 博文 神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所 金融システム事業部内

最終頁に続く

(54) 【発明の名称】 本人認証方法。

(57) 【特許請求の範囲】

【請求項1】

認証申請者端末と認証サーバがネットワークにより接続され、認証申請者に予め配布した複数の符号の配列からなる回答ソースデータに基づいて前記認証申請者の本人認証を行う本人認証方法であって、

前記認証サーバは、前記符号それぞれについて、当該符号のコードデータであって当該符号の形状を示す形状コードおよび色を示す色コードを含むシンボルコードデータを格納したシンボルコード対応テーブル、前記認証申請者端末の利用者である認証申請者毎に、前記回答ソースデータに含まれる複数の符号に対応する複数のコードデータからなる利用者シンボルコードを格納した利用者情報テーブルおよび前記利用者シンボルコードに關係する質問であり前記符号の色および形状のうち少なくとも一方を含む所定条件を満たす符号の位置を問合せする質問を示す質問データを複数有する質問情報テーブルを格納した利用者情報テーブルを記憶した記憶装置を有し、

前記認証申請者端末が、前記認証サーバへ前記ネットワークを介して、前記認証申請者を識別する利用者識別情報を含む認証要求を送信し、

前記認証サーバが、前記認証要求を受信して、前記質問情報テーブルから複数の質問データを抽出し、抽出された質問データに対応する質問および当該質問の回答を受け付ける複数のチェックボックスを含む質問画面を作成し、作成された質問画面および前記シンボルコード対応テーブルを、前記認証申請者端末へ前記ネットワークを介して送信し、

前記認証申請者端末が、前記質問画面を表示して、当該質問画面で示される質問に対す

る回答である前記チェックボックスに対する入力を受け付け、送信されたシンボルコード対応テーブルおよびチェックボックスに対して入力が行われた位置を用いて、前記質問に対する回答を示し、入力に対応する色および形状の少なくとも一方を含むシンボルコードデータおよび当該シンボルコードデータの位置を示す回答コードを算出し、算出された回答コードを、前記認証サーバに前記ネットワークを介して送信し、

前記認証サーバが、送信された前記回答コードと前記利用者識別情報で識別される前記認証申請者の利用者シンボルコードを比較して、前記回答データの示す位置において、前記回答コードに含まれるシンボルコードデータと前記利用者シンボルコードに含まれるシンボルコードデータが一致するか否かにより前記認証申請者の本人認証を行うことを特徴とする本人認証方法。

10

【請求項 2】

前記認証サーバは、前記認証要求を受信する毎にランダムな質問データを前記質問情報テーブルから抽出もしくは予め前記記憶装置に記憶されたルールに従った質問データを前記質問情報テーブルから抽出して前記質問画面を作成することを特徴とする請求項 1 に記載の本人認証方法。

【請求項 3】

前記認証申請者端末は、回答コード候補群を生成し、生成された前記回答コード候補群に対して、論理和演算を施すことにより前記回答コードを算出し、算出された前記回答コードを、前記認証サーバに前記ネットワークを介して送信し、

前記認証サーバは、送信された前記回答コードと前記利用者識別情報で識別される前記認証申請者の利用者シンボルコードとを比較することを特徴とする請求項 1 または 2 に記載の本人認証方法。

20

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信網上の決済取引など本人認証を行う分野に係り、特に、認証申請者毎に契約者カード等の利用カードを予め配布し、利用カードに記載されている本人認証データに基づいた、認証用の質問と、それに対する認証申請者から入力された回答データを照合することにより、前記認証申請者の本人認証を行う方法に関する。

【0002】

【従来の技術】

通信網上の決済取引などでは様々な情報を使用した本人認証が行われ、企業による種々のサービス提供を不特定多数の人が利用するようになった。このような場合、例えば前記サービス利用者がコンピュータ上で入力したIDやパスワードを用い、照合作業を行うことで本人認証を実現する必要がある。この本人認証技術にワンタイムパスワードの概念を付加し、認証機会毎に入力要求する情報を変化させて機密性を高めた手法が提供されている。例えば特開平9-305541号公報に示される契約者確認方法の技術がそれにあたる。この技術は、例えばマトリックス表示された乱数表を印字した利用カードを“契約者”に予め配布しておき、この乱数表におけるマトリックスの所定位置に記された数字を前記契約者に入力要求し、この所定位置の数字に関し照合作業を行うことで本人認証を実現している。

30

40

【0003】

【発明が解決しようとする課題】

上記従来技術における本人認証において、照合対象となるのは、例えば乱数表に記された数字であり、その場合は“契約者”に入力要求できる情報の範囲も0～9までの数字の組合せに限定される。また、記契約者が多数にのぼれば、異なる乱数表を多数作成する必要がある為、乱数表自体を大きくする必要があり、しかしバンクカードやクレジットカード等のサイズのカードに大きな乱数表を印字するとなれば、数字が細かく並べたものになる。

【0004】

本発明は必要に応じて利用容易性及び信頼性に優れ、かつ随意的なセキュリティ度を簡便確

50

実に達成することが可能な本人認証方法を提供することを目的とする。

【0005】

【課題を解決するための手段】

上記目的を達成する本発明の本人認証方法は、以下のように構成される。認証申請者端末と認証サーバがネットワークにより接続されたシステムにおける本人認証方法において、認証申請者に予め符号を含む回答ソースデータを配布しておく。

認証サーバには、認証申請者毎に配布される回答ソースデータに含まれる符号の配列をコード化して記録しておく。認証申請者端末から認証サーバへ接続要求があったときに、認証サーバは、特定の符号が何処にあるかをチェックボックス形式で回答する認証用質問を作成して認証申請者端末に送信する。ここで、認証用質問の作成は、接続要求毎にランダムにもしくはルールに従って作成する。また、認証申請端末で実行する回答作成プログラムと、該プログラムが参照するシンボルコード対応テーブルを併せて送信する。認証申請者端末では受信した認証用質問を表示し、認証申請者からの回答を受付けて認証サーバに返信する。認証サーバは、受信した回答を認証データベースに記録されたデータと照合することで認証申請者からの回答の正否を判定し、判定結果が正しければ接続を許可する。

10

【0006】

【発明の実施の形態】

以下に本発明の実施形態について図面を用いて詳細に説明する。

図1は実施形態における利用カードを示す図である。図1において100は利用カードであり、利用カード上には利用者ID101、契約者の名前102、利用者毎に割り当てられた、丸、星、四角及び、菱形などの形状と、それぞれに白または黒といった色彩が加わり視覚により容易に識別できるシンボル103が記載されている。

20

図1では、利用カード100として“ご契約カード”、利用者ID101として“111122223333”、名前102として“山田太郎”、シンボル103として“

”がプリントされている。利用カード100は、例えばクレジットカードサイズのカードであり、素材は、紙、木材、プラスチック、ゴム、金属、ガラス、ビニール、セラミック、あるいはコンピュータで読み取り可能な記録媒体やコンピュータ上のメモリなど様々なもので可能である。媒体の形状としてもカードなど平板状のものから、立方体、球体など種々の立体的なものまで可能である。なお、シンボル103はここで例示しているものに限定されず、他の視覚により識別可能な文字、記号、図形あるいは色彩やこれらの組合せが利用でき、例えば、本例より複雑なシンボルの組合せも可能であり、アニメキャラクタやイラスト図形などを使うことも可能である。また、凹凸など触覚により触って認識できる点字や形状、あるいはこれらの任意の組合せを包含するものでも可能である。

30

【0007】

図2は本実施形態における認証申請端末及び取引システムを示す構成図である。図2において110は取引システムを利用しようとする利用者らが備える認証申請端末であり、この端末の例としてパーソナルコンピュータ111、携帯電話機112、デジタルTV113を用いることができる。

130は取引システムを示しており、この取引システム130は、本人認証を実施する認証サーバ140、本人認証後の取引業務を実施する取引サーバ160、顧客マスター情報など基幹系の情報を管理するホストコンピュータ190と、認証サーバ140や取引サーバ160へホストコンピュータとの接続インターフェースを提供するホスト接続サーバ180から構成される。また、認証サーバ140、取引サーバ160は各々ハードディスクなどの記憶装置上にデータベースを所有しており、認証サーバ140は認証時に使用する各データを記憶した認証データベース150、取引サーバ160は取引業務で使用する各データを記憶した取引データベース170を所有している。

40

【0008】

認証データベース150内には、認証申請端末110に送信する各種画面データを記憶する画面情報テーブル151、認証用の質問データを記憶する質問情報テーブル152、シ

50

ンボルとコードの対応を記憶するシンボルコード対応テーブル153、契約者の利用者ID、パスワード、利用者シンボルコード等の情報を記憶する利用者情報テーブル154、利用者の回答から回答コードを作成する回答作成プログラム155が記憶される。

【0009】

図2では、認証申請端末110と取引システム130は、通信網120を介して接続されることを示しており、認証申請端末110と通信網120の間はそれぞれ回線及び無線等で接続され、通信網120と取引システム130の間は回線で接続される事を一例として示している。なお、通信網120は、専用回線、電話回線、LAN、無線通信など様々な通信方式を採用することが可能である。通信網120がオープンな通信網の場合には、認証申請端末110と取引システム130間で送受信するデータは暗号化を行う事が望ましい。また、認証申請端末110は、本図で示した以外に、PDA(Personal Digital Assistance)端末、ゲーム機、ファックス機などいずれのマイコンを備える機器でもよい。

10

【0010】

次に本実施例における、認証申請端末110、取引システム130間でのデータの流れを以下に述べる。取引システム130は、利用者が操作する認証申請端末110から通信網120を介してアクセスされると、まず利用者が本システムに登録され、アクセスが許可されている本人かどうかを判定するため、認証サーバ140にてアクセスを受付ける。認証申請端末110からのアクセスを受付けた認証サーバ140は、認証データベース150からケーブルを介し必要なデータを参照し、必要に応じて認証申請端末110とデータを送受信して本人認証を行う。利用者が本システムに登録され、アクセス許可されている本人と認証された場合にのみ利用者は取引が可能となり、以降、認証申請端末110は取引サーバ160へアクセスして取引を行う。取引サーバ160は利用者からの取引の要求があった場合、必要に応じてケーブルを介し取引データベース170を使用し、またホスト接続サーバ180を介して、ホスト接続サーバ180とチャンネル接続されたホストコンピュータ190が管理する利用者情報を使用し取引に応じる。なお、認証サーバ140及び取引サーバ160は、それぞれ認証申請端末からのアクセス要求を受付けるWebサーバ、各要求に関する処理プログラムを備え、必要に応じてプログラムを実行させるアプリケーションサーバ、データベースとのアクセスを行うデータベースサーバと複数のコンピュータに各々分割させてもよい。また、認証データベース150と取引データベース170は1体のデータベース上で存在する場合であっても、適宜組み合わせさせたものでもよい。

20

30

【0011】

図3は本人認証方法の処理手順を、認証申請端末110側と認証サーバ140側の流れ図で示したものである。図3においてステップ2000(以下、s2000と略す。以下同じ)~s2060は認証申請端末110側における本人認証の処理ステップを示し、s2200~s2270は認証サーバ140側における本人認証の処理ステップを示す。なおステップ中、認証申請端末110と認証サーバ140間の通信はインターネット等の通信網を使用しており、また認証サーバ140と認証データベース150間の通信はデータベースアクセス通信を使用している。これらの各ステップは、コンピュータのプログラムにより実現することができ、そのプログラムはHDD、FD、CD-ROM等の記録媒体に格納できるものである。

40

【0012】

取引開始時、まず認証申請端末110は利用者からの入力を受付け、認証サーバ140にアクセスする(s2000)。認証申請端末110の入力手段は、パーソナルコンピュータ111であればキーボードやマウスを、携帯電話機であればダイヤルボタンを、デジタルTVであればリモコンを利用できる。

【0013】

認証サーバ140は認証申請端末110からのアクセスを受付けると(s2200)、画面情報テーブル151から端末の種類に合わせたLogon画面データを取得し、認証申請端末110へ送信する(s2210)。認証申請端末は認証サーバ140からLogon

50

n画面データを受信すると出力装置にLogon画面を出力する(s2010)。認証申請端末110の出力装置は、パーソナルコンピュータ111であればCRTや液晶ディスプレイを、携帯電話機112であれば液晶表示部を、デジタルTVであればブラウン管やプラズマ表示機器、液晶表示機器を利用できる。これらの入出力装置は端末機器上、分離した構成あっても、一体になった構成であってもよい。

【0014】

続けて、利用者が利用カード100の利用者ID101を参照しながら利用者ID、パスワードを入力すると、認証申請端末110は受付けた利用者ID、パスワードを認証サーバ140へ送信する(s2020)。認証サーバ140は認証申請端末110から利用者ID及びパスワードを受信すると、受信した利用者ID、利用者IDに対するパスワードが利用者情報テーブル154上にあるか検索し、本システムに登録されている利用者か否か判定する(s2220)。判定の結果、認証申請端末110から受信した利用者IDが利用者情報テーブル154に存在しない場合、あるいは利用者IDは存在するが、利用者IDに対応するパスワードが間違っている場合は、認証申請端末110に認証結果を送信するステップs2270に遷移する(s2230)。

10

【0015】

利用者情報テーブル154上に受信した利用者IDが存在し、かつ利用者IDに対応するパスワードが合っている場合、認証サーバ140は認証申請端末110の種類に合わせた認証画面データを画面情報テーブル151より取得し、利用者の利用者シンボルコードに關係する質問データを質問情報テーブル152よりランダムに複数個、例えば3個取得し、認証画面データと組合せて質問入り認証画面データを作成する(s2240)。次に認証サーバ140は回答作成プログラム155、シンボルコード対応テーブル153を取得し、回答作成プログラム155と、シンボルコード対応テーブル153及び、質問入り認証画面データを認証申請端末110へ送信する(s2250)。なお、回答作成プログラム155は、あらかじめ認証申請端末110側に備えられている場合でもよく、またプログラムのアルゴリズムが容易に解読できないよう、アプレット等の小規模なアプリケーションである事が望ましい。

20

【0016】

認証申請端末110は認証サーバ140からの回答作成プログラム、シンボルコード対応テーブル及び、質問入り認証画面データを受信すると、質問入り認証画面を出力装置へ出力する(s2030)。その後認証申請端末110は、利用者からの質問に対する回答を受付け、回答作成プログラムが質問に対する回答(チェックボックスの位置)と、シンボルコード対応テーブルから導出したシンボルコードから、回答コードを作成する(s2040)。回答コードが完成すると認証申請端末110は、回答コードを認証サーバ140へ送信する(s2050)。認証サーバ140は認証申請端末110からの回答コードを受信すると、受信した回答コードと利用者情報テーブル154内の利用者シンボルコードが、一致しているかどうか照合して判定する。なお、一致している場合は本人である(認証結果OK)と判定し、不一致の場合は本人でない(認証結果NG)と判定する(s2260)。判定が終了すると、画面情報テーブル151から認証結果に伴う認証結果画面データを取得し、認証申請端末110に認証結果画面データを送信する(s2270)。認証申請端末110は認証サーバ140からの認証結果画面データを受信すると、受信した認証結果画面を出力装置へ出力し(s2060)、処理を終了する。

30

40

【0017】

図4はホストコンピュータ190が認証データベース内の各テーブルを更新する処理手順を示す流れ図である。図4において、s2300~s2320はホストコンピュータにおけるシンボルコード対応テーブル153及び利用者情報テーブル154への更新処理ステップを示す。なおステップ中、ホストコンピュータ190と認証データベース150間の通信は、ホスト接続サーバを介して行う。

【0018】

ホストコンピュータ190は、一定間隔毎(例えば数日毎~1年毎など、間隔は任意)に

50

各シンボルに対する新たなシンボルコード値（更新値）を決める（s 2 3 0 0）。次に前ステップにて決まった更新値を認証データベース150に一括ダウンロードし、シンボルコード対応テーブル153内のシンボルコード値を更新する（s 2 3 1 0）。続いて利用者情報テーブル154内にある利用者シンボルコード値を更新して（s 2 3 2 0）処理を終了する。

【0019】

図5は、本発明の実施例である本人認証方法に関し、認証データベース150内の各種テーブルのデータ構造を示す図である。図5において、画面情報テーブル300は認証申請端末110の種類毎及び、操作画面毎の画面データを記憶したテーブルであり、画面情報テーブル151のデータ構造を示している。質問情報テーブル310は本人認証用の質問データを記憶したテーブルであり、質問情報テーブル152のデータ構造を示している。シンボルコード対応テーブル320は本人認証で使用する“ ”等のシンボルデータとシンボルコードの対応を記憶したテーブルであり、シンボルコード対応テーブル153のデータ構造を示している。利用者情報テーブル330は利用者の個人情報記憶したテーブルであり、利用者情報テーブル154のデータ構造を示している。なお、各々のテーブルは認証データベース150に記憶されている。

10

【0020】

図5では、画面情報テーブル300は、認証申請端末110に送信する画面データの情報として画面毎の画面ID、画面データを記憶しており、画面IDとして“001”、“002”、・・・、“023”、・・・、画像データとして“インターネット用Logon画面データ”、“モバイル用Logon画面データ”・・・“モバイル用認証成功画面データ”・・・が記憶されていることを例示している。なお、これらの画面データは、例えばインターネット上で使用されるのであればHTML(HyperText Markup Language)等で記述されたデータ、携帯電話等に使用されるのであればC-HTML(Compact-HTML)等で記述されたデータを利用できる。

20

【0021】

質問情報テーブル310は、利用者に提示する質問として、質問毎の質問ID、及び質問データを記憶しており、質問IDとして“001”、“002”、・・・“020”・・・、質問データとして“白色シンボルの位置はどこですか？”、“黒色シンボルの位置はどこですか？”・・・“シンボルの位置はどこですか？”・・・が記憶されていることを例示している。なお、これらの質問データも画面データ同様、HTML等で記述されたデータである。シンボルコード対応テーブル320は、シンボルデータ毎に対応するシンボルコード値の情報として、シンボル毎のシンボルID、シンボルデータ、形状データ、色データ、またシンボルコードとして形状コード、色コードを記憶している。本例ではシンボルIDとして“001”、“002”、・・・“901”・・・、シンボルデータとして“ ”、“ ”、・・・“星”・・・、形状データとして“丸”、“星”、“四角”、“菱形”・・・、色データとして“白”、“黒”・・・、シンボルコードとして“aa01”、“bb01”、・・・“bb-”・・・が記憶されていることを例示している。シンボルデータは形状データと色データの組合せで構成されており、これと同様にシンボルコードも形状コードと色コードの組合せにより構成されている。例えばシンボルコード対応テーブル320中シンボルID“001”のシンボルデータ“ ”を例にあげると、形状データ“丸”と色データ“白”の組合せで構成されている。これに伴い“ ”に対応するシンボルコードも“丸”に対応する形状コード“aa”と、“白”に対応する色コード“01”を組合せたシンボルコード“aa01”で示すことができる。なお、色のみを示すシンボル、例えばシンボルID“800”のシンボルデータ“白色”は、形状データが“任意”を意味する“-”であり、色データは“白”、である。この為シンボルデータ“白色”のシンボルコードは、形状コードが“任意”を示す“-”であり、色コードが“白”を示す“01”を組合せたシンボルコード“-01”となる。同様に形状のみのシンボルを示す、シンボルID“900”のシンボルデータ“丸”も、形状コードは“丸”を示す“aa”と、色コードが“任意”を示す“-”を組合せたシンボルコード“aa-

30

40

50

”となる。なお、本例においてシンボルコードは最大4桁の英数字で例示しているが、より多数の桁でもよい。利用者情報テーブル330では、利用者毎に利用者ID、パスワード、利用者名、利用者シンボルコードを記憶しており、利用者IDとして“111122223333”、“444455556666”・・・、パスワードとして“password”、“ws23568rt”・・・、利用者名として“山田太郎”、“鈴木花子”・・・、利用者シンボルコードとして“aa01:aa02:dd02:cc01:dd01:bb01:cc02:bb02”、“aa01:bb01:cc01:dd01:aa02:bb02:cc02:dd02”・・・が記憶されていることを例示している。また、図中に示す通り、利用者が所有する利用カード100は、利用者情報テーブル330の内容を示しており、利用カード100中、利用者ID101、名前102、シンボル103はそれぞれ、利用者情報テーブル330内の利用者ID、利用者名、利用者シンボルコードの内容を示している。また、利用者情報テーブル330内の利用者シンボルコードは、シンボルコード対応テーブル320に示すようなコード表に基づきシンボル自身(シンボルデータ)ではなくシンボルコードで記録される。例えば、利用カード100に示すシンボル103“ ”の左から1番目の“ ”は、シンボルコード対応テーブル320中で参照するとシンボルコードは“aa01”というコード値なる。以下同様に各々のシンボル“ ”、“ ”、“ ”、“ ”、“ ”、“ ”、“ ”に対するシンボルコードを求め、各々のシンボルを“:”の記号で区切ると、一番右端が“ ”を示す“bb02”のコード値となる、“aa01:aa02:dd02:cc01:dd01:bb01:cc02:bb02”となる図中に示すような利用者シンボルコードとなる。

10

20

【0022】

図6は認証申請端末110で表示されるLogon画面と、画面情報テーブルとのデータ関連及び、Logon画面への入力例を示した図である。400はインターネット用Logon画面であり、401は利用者IDを入力する欄、402はパスワードを入力する欄である。

【0023】

図6では、画面情報テーブル300から画面ID“001”、画面データとして“インターネット用Logon画面データ”が選択されていることを例示している。インターネット用Logon画面400は画面情報テーブル300内に記憶されており、利用者が認証申請端末110を通して取引システムへアクセスした際に、認証サーバ140により画面情報テーブル300から選択される。認証サーバ140がLogon画面データを選択する際には、アクセスされた認証申請端末110の種類に応じて画面を選択する。Logon画面が認証申請端末110で表示されると利用者は、利用カード100に記されている利用者ID101を参照しながら、利用者ID入力欄401へ利用者IDを入力し、パスワード入力欄402には利用者のパスワードを入力する。なお、認証申請端末110はパスワードが入力されると、パスワード入力欄上に“*****”といった表記で示す。図では利用者IDとして“111122223333”、パスワードとして“password”が入力された状態を示している。

30

【0024】

図7は認証申請端末110で表示される質問入り認証画面と、画面情報テーブル及び質問情報テーブルとのデータ関連、また質問入り認証画面への入力例を示した図である。図7において500は質問入り認証画面であり、510～512は各質問501～503に対する回答チェックボックス群である。

40

【0025】

図7では、質問入り認証画面500の構成例として、画面情報テーブル300から画面ID“011”の画面データ“インターネット用認証画面データ”が選択され(矢印501)、質問情報テーブル310から質問ID“001”の質問データ“白色シンボルの位置はどこですか?”と質問ID“010”の質問データ“星(と)シンボルの位置はどこですか?”、質問ID“020”の質問データ“シンボルの位置はどこですか?”がランダムに選択されていることを示している(502～504)。なお認証画面データは

50

、各認証申請端末の種類に応じた画面データとして画面情報テーブル300から認証サーバ140にて選択され、また質問データは、質問情報テーブル310から利用者シンボルコードに関する質問データとして、認証サーバ140がランダムに複数（本例では3つ選択されたものを示す）選択する。

【0026】

認証申請端末140にて質問入り認証画面500が表示されると、利用者はまず利用カード100のシンボル103“ ”を参照しながら、認証用質問1である“白色シンボルの位置はどこですか？”に対する回答を入力する。本例のシンボル103“ ”での白色シンボルの位置は、左から1、4、5、6番目である為、利用者は入力装置を通じ、図示のように回答チェックボックス510の1、4、5、6番目をチェックする。質問2“星（ と ）シンボルの位置はどこですか？”に対する回答についてはシンボル103の左から6、8番目の2つが該当する為、図示のように回答チェックボックス511中の6、8番目のチェックボックスをチェックする。質問3“シンボルの位置はどこですか？”に対してはシンボル103の左から2番目のみが該当する為、図示のように回答チェックボックス512中の2番目のチェックボックスのみをチェックする。このように、チェック形式での認証申請者の回答入力を促すとすれば、回答入力作業が至極簡単で間違いも生じにくく好適である。また、マウスや矢印キーなどの入力装置によってチェックボックスをチェックするだけなので、キーボード等（図示せず）から文字をタイプするといった煩雑さは伴わない。なお、目の不自由な人は、音声にて質問を出して、点字や浮きだし加工されたシンボルに触れて前記認証用質問に何らかの入力装置から回答するようにしても良い。また、このように認証機会毎に認証用質問が変化すれば、該認証用質問に対応する回答について第三者が盗み見やなりすましを働こうにも困難である一方で、いくら認証用質問が変化しても認証申請者としては比較的単純で認識性が良好な記号等が数桁並ぶだけの利用者シンボルをもとに視覚的に回答するだけで済むので本人認証に関する利便性は確保されつづける。

【0027】

図8は本人認証の質問に対する回答から、回答作成プログラム155が回答コードを作成することを示す図である。この回答作成プログラム155は、図3のs2040で示したように認証申請端末110側で実行される。

600は回答作成プログラム155が回答コード610を作成する段階を示すものであり、601は回答チェックボックス510中のチェック位置、およびシンボルコード対応テーブル154のコード情報から作成された回答コードである。602は回答チェックボックス511中のチェック位置、およびシンボルコード対応テーブル154のコード情報から作成された回答コードである。603は回答チェックボックス512中のチェック位置、およびシンボルコード対応テーブル154のコード情報から作成された回答コードである。また、610は回答コード601～603を論理和（OR）演算にて算出し、最終的に認証サーバに送信される回答コードである。

【0028】

最終的に作成される回答コード610“-01：aa02：- -：-01：-01：bb01：- -：bb-”は、各回答コード601～603中の各シンボルコードを構成する形状コード、色コード単位の和（OR）演算にて導き出される。本例に示す通り回答コード601“-01：- -：- -：-01：-01：-01：- -：- -”と、回答コード602“- -：- -：- -：- -：bb-：- -：bb-”と、回答コード603“- -：aa02：- -：- -：- -：- -：- -”を和（OR）演算した場合、まず回答コード601～603各々のコード左から1番目のシンボルコードに着目し、“-01”+“- -”+“- -”の和（OR）演算を実施する。シンボルコードを構成する形状コード、色コード単位で和（OR）演算を実施すると左から1番目の結果は回答コード610の左から1番目に示す通り“-01”になる。詳細を述べると、まず各シンボルコード中の形状コードの和（OR）演算にて“-”+“-”+“-”を実施し、結果“-”を導き出し、次に色コードの和（OR）演算にて“01”+“-”+“-”を実施し、

10

20

30

40

50

その結果“01”を導き出す、最後に形状コードの結果、色コードの結果を結合しシンボルコード“-01”の結果を得る。同様に601～603の各々の回答コード中、左から2番目のシンボルコードの和(OR)演算を例とすると、“-”+“-”+“aa02”が実施され、その結果“aa02”が算出される。以下同様にして各シンボルコードの形状コード、色コード単位で各々を和(OR)演算すると回答コード610に示す“-01:a a 0 2:- :-: - 0 1:- 0 1:b b 0 1:- :-: b b -”が算出される。なお、OR演算式にて算出する際、任意を意味する“-”以外の異なるコード同士を結合しようとした場合はエラーとなり、本人認証をNGと判定する。例を述べると“01”+“01”のパターンや、“-”+“aa”は、同じコード値である“01”同士で和(OR)演算を行っており、また任意を意味する“-”と“aa”による和(OR)演算のためエラーにならない。しかし、“02”+“01”のパターンや“aa”+“bb”は“-”以外のコード同士、かつ異なるコード同士で演算を行っているためエラーとなる。

10

【0029】

尚、演算とは別に、回答作成プログラム155が回答コード601～603を作成する際に参照するシンボルコード対応テーブル154は、認証申請端末110側でなく認証サーバ側にあり、回答コードを作成する度に回答作成プログラム155が認証サーバ140側へ参照するという方式でもよい。また、回答データの形式は、本図で示した以外にコード化せず、シンボル自身(シンボルデータ)例えば“-”などを用いて“- - - -”等の形式でもよい。シンボル自身を使用する場合、シンボルをコードに変換する必要が無い為回答作成プログラム155は不要となる。しかし、回答に使用できる情報がシンボル自身に限定されることから、“白色シンボルの位置はどこですか?”、“星(と)シンボルの位置はどこですか?”などの色データ、形状データのみに関する質問ができないため(質問に対する回答がシンボル化できない)質問が限定されることになり、またシンボル自身を用いて回答を行うため、利用者シンボルを解読され易い。

20

【0030】

図9は、回答作成プログラム155による、質問1に対する回答コードの作成手順を示した図である。図9では、回答作成プログラム155が、質問1“白色シンボルの位置はどこですか?”に対する回答チェックボックス510中のチェック位置と、シンボルコード対応テーブル320を用い、回答コード601として“-01:- :-: - :-: - 0 1:- 0 1:- 0 1:- :-: - -”を作成することを例示している。以下に回答コード601の作成手順を述べる。始めに回答作成プログラム155は、質問ID001“白色シンボルの位置はどこですか?”を参照し、何のシンボルに対する質問かを識別する。本例の場合“白色シンボル”に対する質問であるため、回答作成プログラム155がシンボルコード対応テーブル320からシンボルデータ“白色”を検索し、“白色シンボル”に対応するシンボルコード“-01”を導き出す。質問に対するシンボルコードを導出すると、次に回答作成プログラム155は回答チェックボックス510を参照し、チェックが付いている箇所を検索する。本例では回答チェックボックス510中の左から1、4、5、6番目にチェックが付いている為、チェックが付いた箇所、つまり回答コード601の左から1、4、5、6番目に“白色シンボル”を意味するシンボルコード“-01”を設定する。なお、回答コード中何も設定されなかった箇所(本例では左から2、3、7、8番目)はデフォルト(標準値)として任意を意味する“-”が設定される。以上の手順で完成したものが、質問ID001“白色シンボルの位置はどこですか?”と、回答チェックボックス510に対する回答コード601“-01:- :-: - :-: - 0 1:- 0 1:- 0 1:- :-: - -”である。

30

40

【0031】

図10は、回答作成プログラムによる、質問2に対する回答コードの作成手順を示した図である。図10では、回答作成プログラム155が、質問ID010“星(と)シンボルの位置はどこですか?”に対する回答チェックボックス511中のチェック位置と、シンボルコード対応テーブル320を用い、回答コード602として“- :-: - :-: - :-: - :-: - :-: b b - :-: - :-: b b -”を作成することを例示している。以下に回答コー

50

ド602の作成手順を述べる。始めに回答作成プログラム155は、質問データ502“星(と)シンボルの位置はどこですか?”を参照し、何のシンボルに対する質問かを識別する。本例の場合“星シンボル”に対する質問であるため、回答作成プログラム155がシンボルコード対応テーブル320からシンボルデータ“星”を検索し、“星シンボル”に対応するシンボルコード“bb-”を導き出す。質問に対するシンボルコードを導出すると、次に回答作成プログラム155は回答チェックボックス511を参照し、チェックが付いている箇所を検索する。本例では回答チェックボックス中511の左から6、8番目にチェックが付いている為、チェックが付いた箇所、つまり回答コード602の左から6、8番目に“星シンボル”を意味するシンボルコード“bb-”を設定する。なお、回答コード中何も設定されなかった箇所(本例では左から1、2、3、4、5、7番目)はデフォルト(標準値)として任意を意味する“- -”が設定される。以上の手順で完成したものが、質問ID010“星(と)シンボルの位置はどこですか?”と、回答チェックボックス511に対する回答コード602“- - : - - : - - : - - : bb - : - - : bb -”である。

10

【0032】

図11は、回答作成プログラムによる、質問3に対する回答コードの作成手順を示した図である。図11では、回答作成プログラム155が、質問ID020“シンボルの位置はどこですか?”に対する回答チェックボックス512中のチェック位置と、シンボルコード対応テーブル320を用い、回答コード603として“- - : aa02 : - - : - - : - - : - - : - - : - -”を作成することを例示している。以下に回答コード603の作成手順を述べる。始めに回答作成プログラム155は、質問データ503“シンボルの位置はどこですか?”を参照し、何のシンボルに対する質問かを識別する。本例の場合“シンボル”に対する質問であるため、回答作成プログラム155がシンボルコード対応テーブル320からシンボルデータ“ ”を検索し、“シンボル”に対応するシンボルコード“aa02”を導き出す。質問に対するシンボルコードを導出すると、次に回答作成プログラム155は回答チェックボックス512を参照し、チェックが付いている箇所を検索する。本例では回答チェックボックス512中の左から2番目のみにチェックが付いている為、チェックが付いた箇所、つまり回答コード601の左から2番目のみに“シンボル”を意味するシンボルコード“aa02”を設定する。なお、回答コード中何も設定されなかった箇所(本例では左から1、3、4、5、6、7、8番目)はデフォルト(標準値)として任意を意味する“- -”が設定される。以上の手順で完成したものが、質問ID020“シンボルの位置はどこですか?”と、回答チェックボックス512に対する回答コード603“- - : aa02 : - - : - - : - - : - - : - - : - -”である。

20

30

【0033】

図12は、認証申請端末から送信された回答コードと、利用者情報テーブル内の利用者シンボルコードを照合した際の、本人認証が成功した例と失敗した例を示す図である。図12において、620は本人認証が失敗する場合の回答コード例であり、1000は本人認証が成功した場合の認証結果画面、また、1010は本人認証が失敗した場合の認証結果画面である。

40

【0034】

図12では、本人認証が成功した例として、画面情報テーブル300から画面ID“021”の画面データ“インターネット用認証成功画面データ”が選択され、利用者情報テーブル330からは認証された利用者の利用者IDとして“111122223333”、利用者名として“山田太郎”が選択されてインターネット用認証成功画面1000が成り立つことを例示している。また、本人認証が失敗した例として、画面情報テーブル300から画面ID“022”の画面データ“インターネット用認証失敗画面データ”が選択されることを例示している。

【0035】

まず本人認証が成功した例(a)を基に、本人認証を行う際の手順を以下に述べる。認証

50

サーバは、認証申請端末から回答コード610を受信すると、利用者情報テーブル330の利用者シンボルコードと照合を行い、本人認証を行う。認証の手順としては、回答コード610中のシンボルコード1つと、利用者情報テーブル330内の利用者シンボルコード1つを左から1つずつに順に照合していく。なお、回答コード610中“-”は任意を意味する為、照合の対象とせず、“-”以外の箇所で認証を行う。その結果、“-”以外の値が全て利用者シンボルコードと一致した場合にのみ本人と判定する。本人と判定した場合、画面情報テーブル300から本人認証が成功した場合の認証結果画面1000として“インターネット用認証結果成功画面データ”を取得し、利用者情報テーブル330内の照合対象になっている利用者ID、利用者名を埋め込み認証申請端末へ送信する。

【0036】

次に本人認証が失敗した例(b)について以下に述べる。認証サーバは、認証申請端末から回答コード620を受信すると、前記成功した例と同様に回答コード620と利用者情報テーブル330内の利用者シンボルコードを照合し、本人認証を行う。回答コード620中、“-”以外の箇所で1箇所でも利用者情報テーブル330の利用者シンボルコードと一致していない箇所がある場合は、本人でないと判定し、画面情報テーブル300から本人認証が失敗した場合の認証結果画面画面1010として“インターネット用認証結果失敗画面データ”を取得し、認証申請端末へ送信する。なお、本例では回答コード620中、左から3つ目のコード“-01”が利用者シンボルコードと異なっているため、本人ではないと判定される。

【0037】

図13では、これまでに述べてきた本人認証の各処理における、インターネット用の各画面400~1010の遷移関係を例示している。利用者は認証サーバにアクセスした後、認証申請端末の出力装置にインターネットLogon画面400が表示されると、利用者IDおよびパスワードを画面400に入力し、認証サーバにLogonを行う。その結果、Logonが成功した場合は、認証サーバから画面データ500が返されインターネット用本人認証画面500に遷移する。なお、Logonが失敗した場合は、認証サーバから画面1010が返されインターネット用認証結果画面1010に遷移する。Logonが成功した際に、インターネット本人認証画面500が表示されると、利用者は認証用の各質問に対する回答を画面500中に入力する。回答入力が完了すると認証サーバ側で本人認証が実施され、認証が成功した場合、認証サーバから認証成功を意味するインターネット認証結果画面1000が返され、その後各種取引画面が表示される。また本人認証が失敗した場合はLogonが失敗した場合と同様、認証サーバから画面1010が返されインターネット用認証結果画面1010に遷移する。

【0038】

図14は携帯電話機112(モバイル機器)にて本人認証を実施した際の画面遷移を示す図である。1100はモバイル機器用のLogon画面であり、1110~1130はモバイル用本人認証画面である。なお、1140は認証成功時のモバイル用認証結果画面であり、1150は認証失敗時のモバイル用認証結果画面である。モバイル用認証画面形式1100~1130と、インターネット用認証画面形式500の表示形式が異なるのは、認証申請端末における出力装置の表示領域大きさ、解像度等の性能が異なるためである。本例ではインターネット用では一画面で表示している本人認証画面が、モバイル用では1110~1130と質問No毎に分割して表示される様子を示している。

【0039】

図15はホストコンピュータ190からの指示にて一定間隔で変化する、シンボルコード対応テーブル、利用者情報テーブル及び、それに関連して変化する回答コードを示した図である。

【0040】

325は一定間隔後のシンボルコードが変化したシンボルコード対応テーブルであり、335も同様に利用者シンボルコードが変化した利用者情報テーブルである。また、615は一定間隔後のコード値が変化した回答コードである。図15では、ホストコンピュータ

10

20

30

40

50

190が制御している一定間隔で新しいシンボルコードがダウンロードされ、シンボルコード対応テーブル320のシンボルコードが“aa01”、“bb01”、・・・“bb-”・・・から325に示す通り“ed97”、“ca97”、・・・“ca-”・・・に更新され、また利用者情報テーブル330中の利用者シンボルコードが“aa01:aa02:dd02:cc01:dd01:bb01:cc02:bb02”から335に示す通り“ed97:ed81:bc81:ee97:bc97:ca97:ee81:ca81”に変更されることを例示している。またその結果、回答コード610が“-01:aa02:-:-01:-01:bb01:-:bb-”から615に示す“-97:ed81:-:-97:-97:ca97:-:ca-”に変化することも例示している。

10

【0041】

図15に示すようにシンボルコードを一定間隔で変更させる目的は、通信網上を流れる回答コード610を一定間隔で変更させ、第三者からの盗み取り、及び情報漏洩による成り済まし等を行難くするためである。例えば図に示すように、シンボルコード対応テーブル320が一定間隔後には325に変更され、それに伴い利用者情報テーブル330が335に変更した場合、作成される回答コードも610や615に示すように値が異なる。なお、回答コードの値が一定間隔で異なっても、回答コードの値と、利用者情報テーブル内の利用者シンボルコードの間で同期がとれている為、本人認証におけるコードの照合時に問題は生じない。具体的に例を述べると、変更前のシンボルコード対応テーブル320内に示すシンボルデータ“ ”に対するシンボルコードが“aa01”から325に示す通り“ed97”に変更された場合、利用者情報テーブル330の利用者ID“111122223333”の利用者シンボルコードも、“aa01”(左から1番目に示す)から、335に示す通り“ed97”に変更される。同様にして他のシンボルコードも、シンボルコード対応テーブル内で変化した値が、利用者情報テーブルにも反映されテーブル間におけるシンボルコードの同期を保つ。このため、回答作成プログラムが作成する回答コードと利用者情報テーブル内の利用者シンボルコードの同期が保たれ、問題なく本人認証が実施できる。

20

【0042】

以上、本発明に係る実施の形態にあっては、次の効果を奏する。本人認証にあたって入力(回答)要求できる情報の範囲が限定されないため、セキュリティ面での機能も制限されることがなくなる。また、前記顧客が多数にのぼるとしても、配列するシンボルの形状や色彩等をいかようにも変化させることで、各顧客間で重複の無い利用者シンボルを作成して入力要求を行うことが簡便に出来る。加えて、例えばカード表面などの限られた面積においても、数桁のシンボルを例えば一列だけ配列表示することで利用者シンボルを提示することも可能であるから、回答作業が容易になる。

30

【0043】

また、通信網上を流れる回答コードが一定間隔で変化する為、第三者から盗み取り難くなり、安全及び信頼性の向上につながる。

【0044】

以上、実施の一形態についての例を説明したが、本発明の本人認証方法はインターネットバンキングのLogon時だけに限られず、入館チェックやネットデビットなどの本人認証が必要とされる状況等で利用可能である。

40

【0045】

【発明の効果】

本発明によれば、利用容易性及び信頼性に優れ、かつ必要に応じて随意的なセキュリティ度を簡便確実に達成することが可能な本人認証方法を提供可能となる。また、今後のブラウザ機器の発展に伴いあらゆる機器に対応し、ユーザビリティを維持、且つ高信頼性である。特に次世代携帯、TVバンキング等などに向いている。

【図面の簡単な説明】

【図1】実施形態における利用カードを示す図である。

50

【図2】実施形態における取引システム及び認証申請端末を示す構成図である。

【図3】本人認証方法の処理手順を示す流れ図である。

【図4】図4はホストコンピュータが認証データベース内の各テーブルを更新する処理手順を示す流れ図である。

【図5】本発明の実施例である本人認証方法に関し、認証データベース内の各種テーブルのデータ構造を示す図である。

【図6】認証申請端末で表示されるLogon画面と、画面情報テーブルとのデータ関連及び、Logon画面への入力例を示した図である。

【図7】認証申請端末で表示される質問入り認証画面と、画面情報テーブル及び質問情報テーブルとのデータ関連、また質問入り認証画面への入力例を示した図である。

10

【図8】本人認証の質問に対する回答から、回答作成プログラムが回答コードを作成することを示した図である。

【図9】回答作成プログラムによる、質問1に対する回答コードの作成手順を示した図である。

【図10】回答作成プログラムによる、質問2に対する回答コードの作成手順を示した図である。

【図11】回答作成プログラムによる、質問3に対する回答コードの作成手順を示した図である。

【図12】認証申請端末から送信された回答コードと、利用者情報テーブル内の利用者シンボルコードを照合した際の、本人認証が成功した例と失敗した例を示す図である。

20

【図13】インターネットにて本人認証を実施した際の画面遷移を示す図である。

【図14】携帯電話機（モバイル機器）にて本人認証を実施した際の画面遷移を示す図である。

【図15】ホストコンピュータからの指示にて一定間隔で変化する、シンボルコード対応テーブル、利用者情報テーブル及び、それに関連して変化する回答コードを示した図である。

【符号の説明】

100 利用カード、101 利用者ID、

102 名前、103 シンボル、

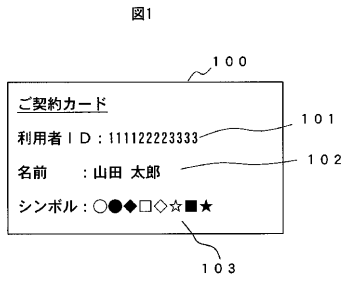
300 画面情報テーブル、310 質問情報テーブル、

30

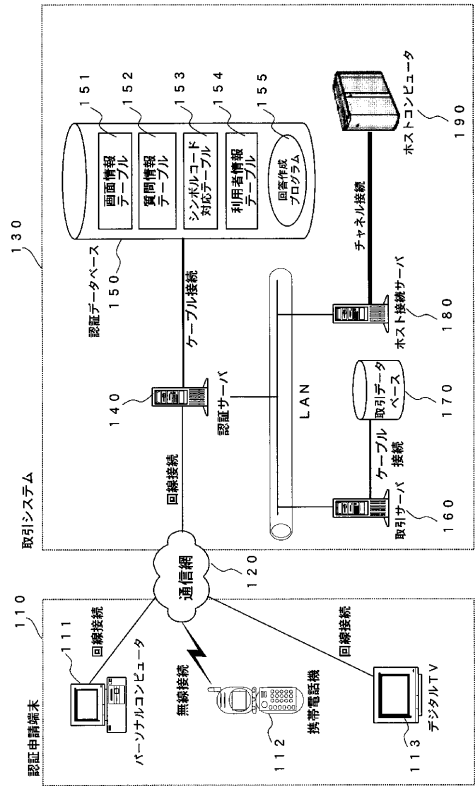
500 質問入り認証画面、

510, 511, 512 回答チェックボックス

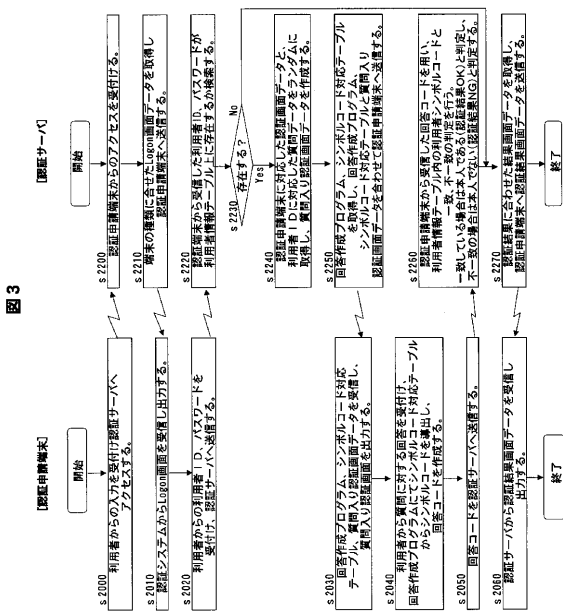
【 図 1 】



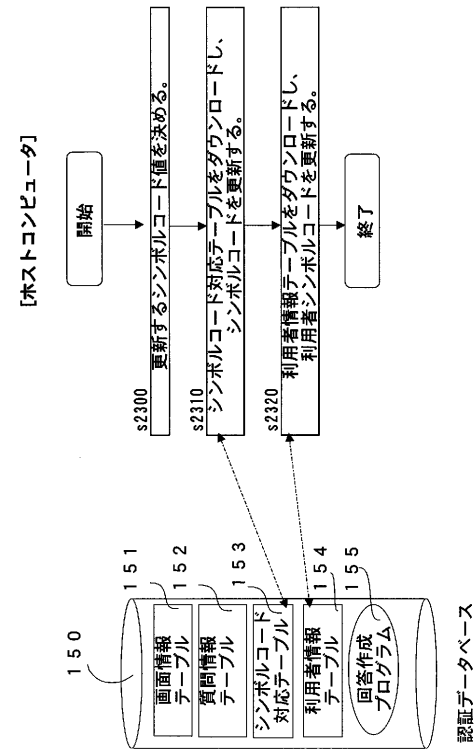
【 図 2 】



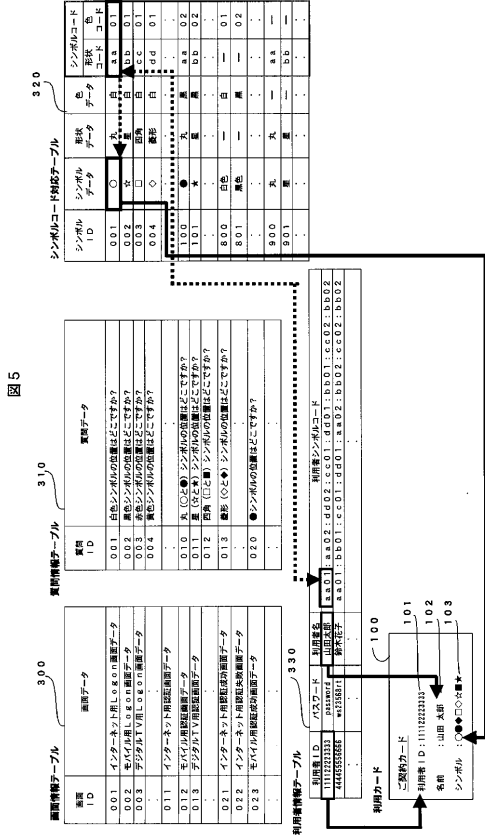
【 図 3 】



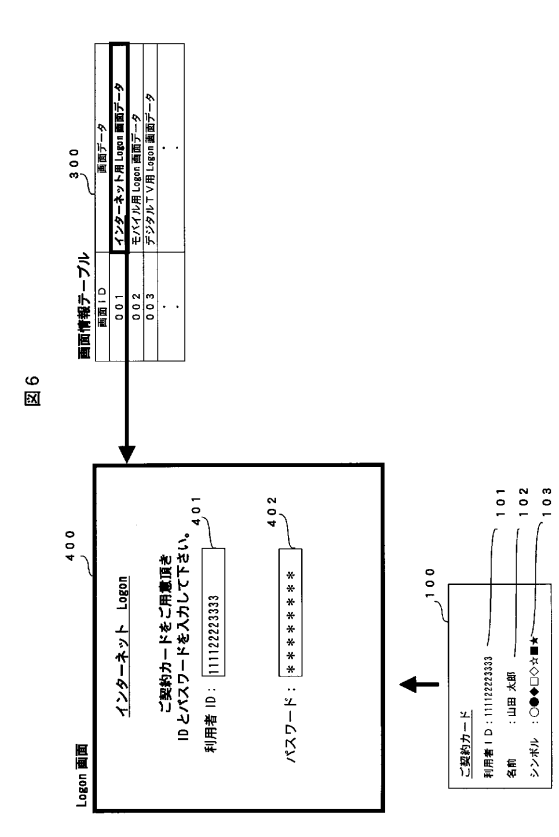
【 図 4 】



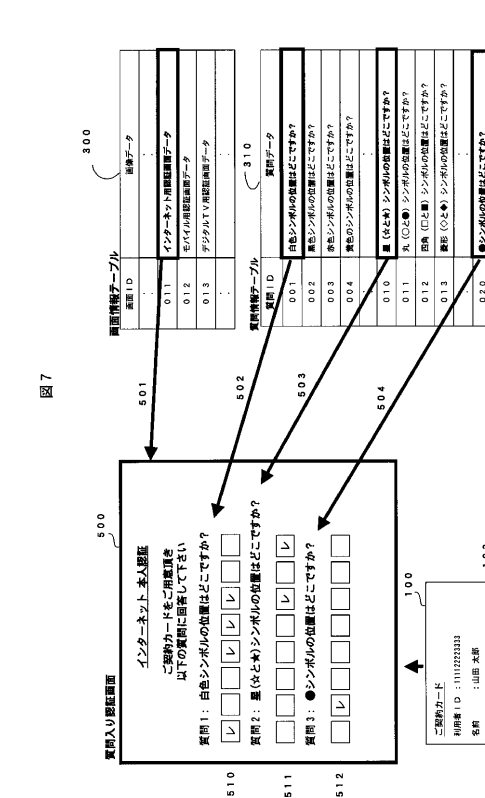
【 図 5 】



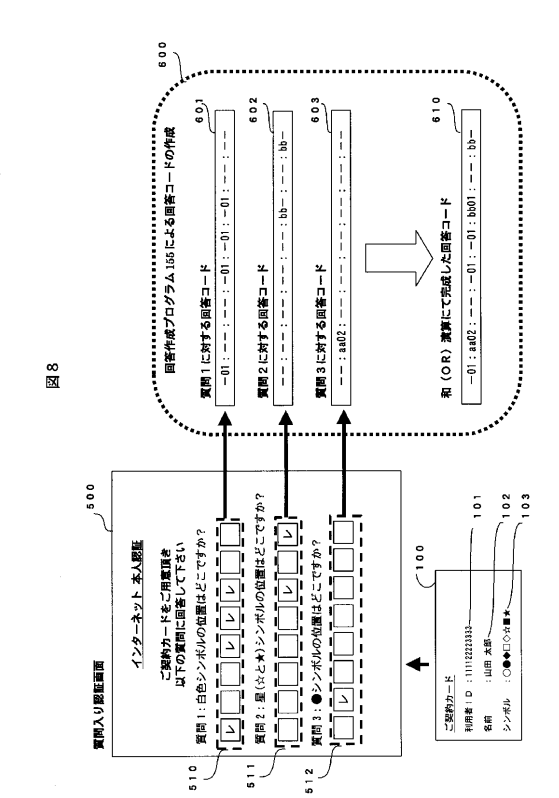
【 図 6 】



【 図 7 】



【 図 8 】



【 図 9 】

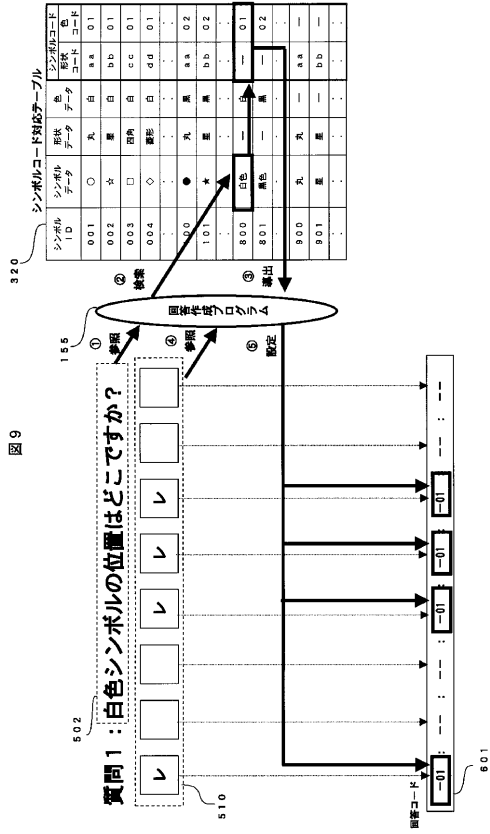


図 9

【 図 10 】

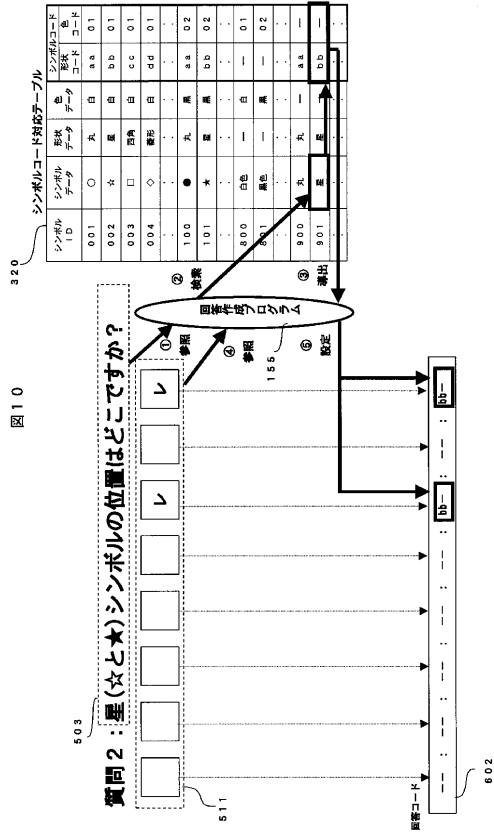


図 10

【 図 11 】

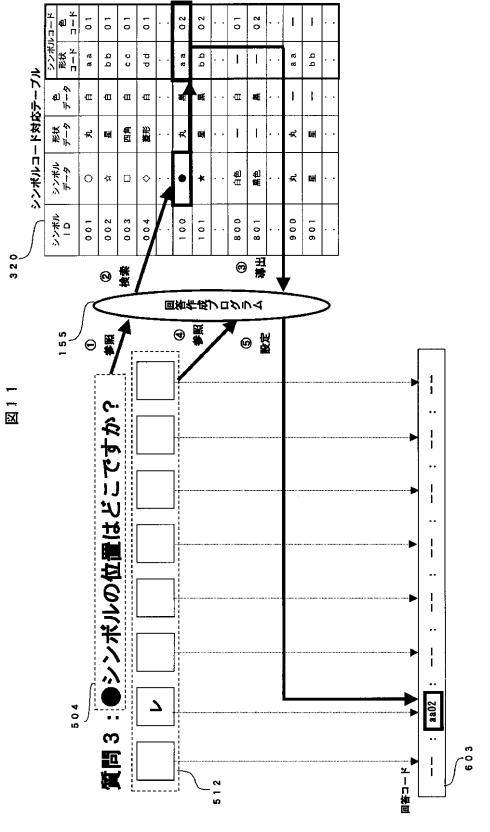


図 11

【 図 12 】

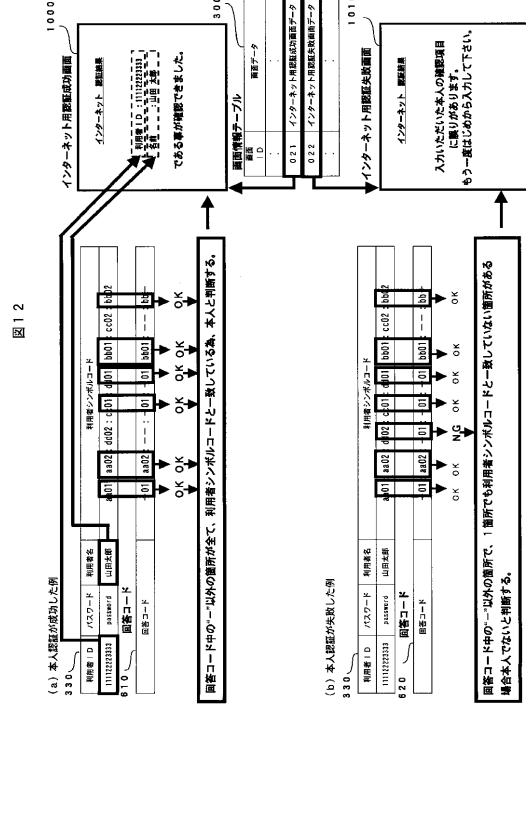
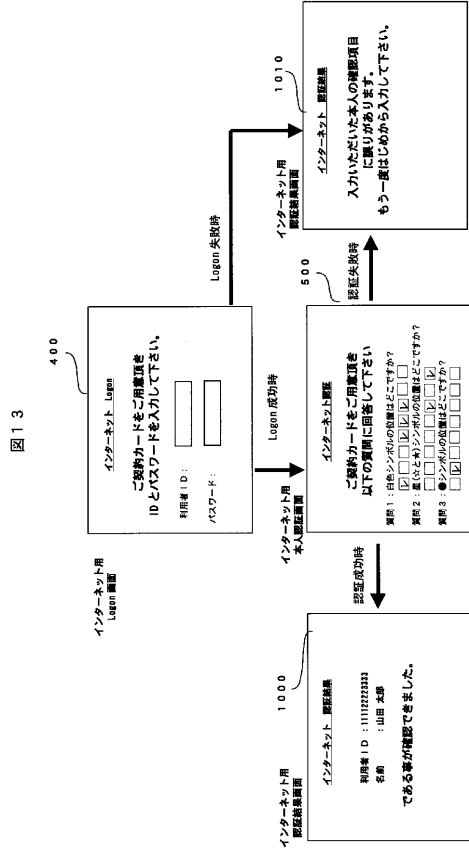
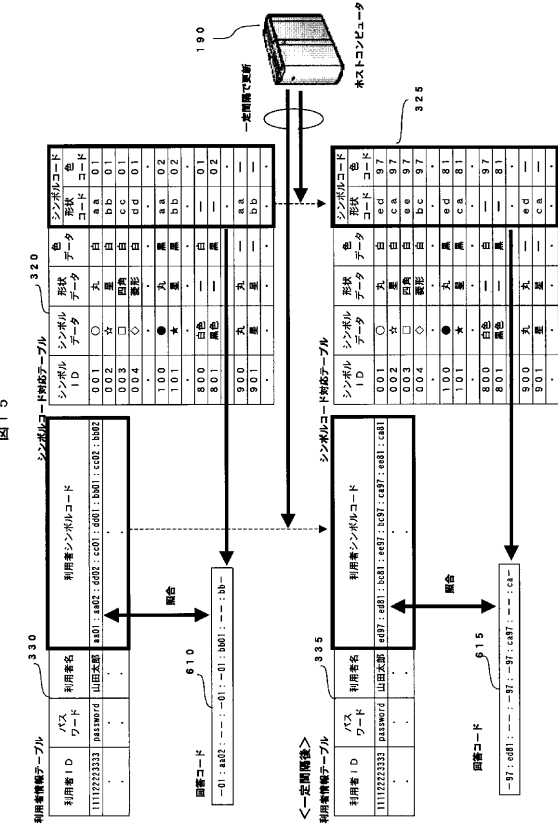


図 12

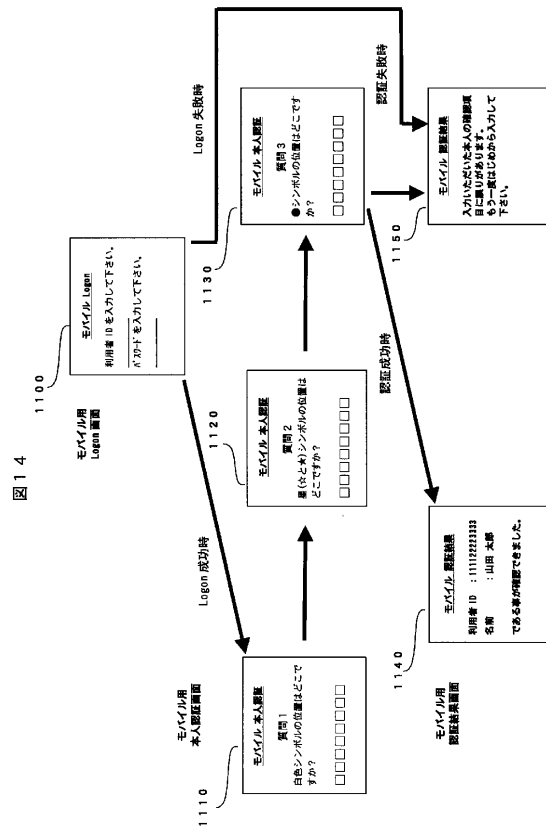
【 図 1 3 】



【 図 1 5 】



【 図 1 4 】



フロントページの続き

- (72)発明者 立野 直樹
神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 金融システム事業部内
- (72)発明者 深日 剛
東京都千代田区大手町 1 丁目 1 番 1 号 株式会社三和銀行内
- (72)発明者 竹本 達治
東京都千代田区大手町 1 丁目 1 番 1 号 株式会社三和銀行内
- (72)発明者 広瀬 義行
東京都千代田区大手町 1 丁目 1 番 1 号 株式会社三和銀行内
- (72)発明者 山元 孝之
東京都千代田区大手町 1 丁目 1 番 1 号 株式会社三和銀行内
- (72)発明者 野村 耕一
東京都千代田区大手町 1 丁目 1 番 1 号 株式会社三和銀行内

審査官 関 博文

- (56)参考文献 特開平 0 9 - 3 0 5 5 4 1 (J P , A)
特開 2 0 0 0 - 0 9 9 4 7 1 (J P , A)
特開平 0 9 - 1 5 2 9 9 1 (J P , A)
特開平 1 0 - 0 9 7 5 0 0 (J P , A)
特開平 0 9 - 0 8 3 5 0 6 (J P , A)
特開平 1 1 - 2 7 4 9 9 9 (J P , A)
特開 2 0 0 0 - 1 5 1 5 7 8 (J P , A)

- (58)調査した分野(Int.Cl.⁷, D B名)
G06F 17/60 414
G06F 15/00 330
H04L 9/32
JICSTファイル(JOIS)