

明 細 書

発明の名称：

サーバシステム、通信システム、通信端末装置、プログラム、記録媒体及び通信方法

技術分野

[0001] 本発明は、秘匿性を確保しつつ、各種情報の送受信を行うサーバシステム、通信システム、プログラム、通信端末装置、記録媒体及び通信方法に関する。

背景技術

[0002] 近年、WWW (w o r l d w i d e w e b) を介したインターネットバンクサービス又はオンラインストア等のサービスにおいて、所謂、なりすましに代表される不正使用が急増している。

[0003] 例えば、インターネットバンクサービスの場合には、金融機関によって発行された、ユーザ毎のユニークな乱数表を用いてユーザ認証を行うシステムの他に、例えば、当該金融機関によって発行された暗号トークンが発生するワンタイムパスワードを用いて、ユーザを認証するシステム（例えば、特許文献1）が実用化されている。

先行技術文献

特許文献

[0004] 特許文献1：特開2010-049554号公報

発明の概要

発明が解決しようとする課題

[0005] しかしながら、上記のシステムでは、サービス提供時における通信のセキュリティを十分に確保できておらず、不正使用の温床になっている。

[0006] 本発明は、上記課題を解決するためになされたものであり、その目的は、各種のサービス提供時におけるセキュリティを向上させ、不正使用を防止

することが可能なサーバシステム等を提供することにある。

課題を解決するための手段

- [0007] (1) 上述した課題を解決するため、本発明のサーバシステムなどは、
- ネットワークを介して、通信接続される通信端末装置からデータを受信する受信手段と、
- 前記通信端末装置のユーザ毎に予め定められた表データであって、前記通信端末装置にて入力される入力対象文字と、当該入力対象文字の各々に対して予め割り当てられた形象と、を対応付けた表データが、前記ユーザを識別するための識別情報と対応付けて記録される記録手段を制御する制御手段と、
- 前記受信手段によって前記通信端末装置からユーザを指定した所与の要求が受信された場合に、当該ユーザに対応する表データを特定するデータ特定手段と、
- 前記特定された表データに基づき、前記ユーザによって特定すべき入力対象文字に対応する前記形象を抽出する抽出手段と、
- 前記抽出された形象の各々に対応付けられ、かつ、該当する通信端末装置にて該当する形象が表示される際に用いる標識情報を含む入力用データを生成し、当該生成した入力用データを前記通信端末装置に配信する配信手段と、
- 前記配信された入力用データに基づき前記通信端末装置にて前記形象が表示された際に、ユーザが入力した前記形象に対応する前記標識情報を当該通信端末装置から取得する取得手段と、
- 前記取得された標識情報に基づき、該当する前記形象を決定する決定手段と、
- 前記決定された形象に基づき、前記特定すべき入力対象文字を特定し、当該特定した入力対象文字に基づき、所与の処理を実行する処理手段と、
- を備える構成を有している。

- [0008] この構成により、本発明のサーバシステムなどは、ユーザによって入力対

象文字を入力させる際に形象を用いているので、口座情報（口座番号や送金金額）や認証情報（ログイン情報）その他のユーザによって特定すべき情報をキーボードなどの入力デバイスによって直接入力させることなく、当該特定すべき情報を特定することができる。

[0009] したがって、本発明のサーバシステムなどは、予めユーザに発行された乱数表等に記載された情報の全てをフィッシングサイトにおいて一度に全部入力するなど、ユーザの不注意に起因するセキュリティに関する情報（例えば、パスワード）の漏洩、及び、不正ログインする第三者への情報の譲渡を防止することができる。

[0010] また、本発明のサーバシステムなどは、通信端末装置とサーバシステム間におけるデータ通信には形象の表示位置などの標識情報を用いており、入力対象文字やそれを特定する形象を用いていないので、通信端末装置とサーバシステム間においてユーザによって特定すべき情報が第三者により盗み取られ、又は、改竄されることを防止することができる。

[0011] したがって、本発明のサーバシステムは、ユーザに提供しているサービスへの第三者による不正ログインや中間者攻撃を有効に防止することができる。

[0012] この結果、本発明のサーバシステムは、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止し、インターネットバンクサービス等の各種のサービス提供時におけるセキュリティを向上させることができる。

[0013] （２）また、上記課題を解決するため、本発明の通信端末装置などは、各種の処理を実行するサーバシステムとネットワークを介して接続され、当該サーバシステムとデータの授受を行いつつ、ユーザに各種のサービスの提供をするための通信端末装置であって、

ユーザ毎に予め定められた表データであって、ユーザによって入力される入力対象文字と、当該入力対象文字の各々に対して予め割り当てられた形象と、を対応付けた表データの一部を、各形象を表示手段に表示する表示位置を少なくとも制御する制御情報とともに、前記サーバシステムから取得する

取得手段と、

前記取得された表データに基づいて表示された画像に従って、ユーザの入力操作を受け付ける受付手段と、

前記入力操作に応じ、ユーザの指定した前記形象に対応する表示位置を特定する特定手段と、

前記特定された形象に対応する表示位置を示す情報を前記サーバシステムに送信する送信手段と、

を備える構成を有している。

[0014] この構成により、本発明の通信端末装置は、ユーザによって入力対象文字を入力させる際に形象を用いているので、口座情報（口座番号や送金金額）や認証情報（ログイン情報）その他のユーザによって特定すべき情報をキーボードなどの入力デバイスによって直接入力させることなく、当該特定すべき情報を特定することができる。

[0015] したがって、本発明のサーバシステムなどは、予めユーザに発行された乱数表等に記載された情報の全てをフィッシングサイトにおいて一度に全部入力するなど、ユーザの不注意に起因するセキュリティに関する情報（例えば、パスワード）の漏洩、及び、不正ログインする第三者への情報の譲渡を防止することができる。

[0016] また、本発明のサーバシステムなどは、通信端末装置とサーバシステム間におけるデータ通信には形象の表示位置などの標識情報を用いており、入力対象文字やそれを特定する形象を用いていないので、通信端末装置とサーバシステム間においてユーザによって特定すべき情報が第三者により盗み取られ、又は、改竄されることを防止することができる。

[0017] したがって、本発明のサーバシステムは、ユーザに提供しているサービスへの第三者による不正ログインや中間者攻撃を有効に防止することができる。

[0018] この結果、本発明のサーバシステムは、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止し、インターネットバンクサービス等の

各種のサービス提供時におけるセキュリティーを向上させることができる。

- [0019] (3) また、上記課題を解決するため、本発明の記憶媒体は、
- ユーザが通信端末装置を用いて、各種のサービスを提供するサーバシステムにアクセスする際に、当該ユーザが入力する入力対象文字を前記サーバシステムにて特定するための形象が視認可能に形成された記憶媒体であって、
- 一の行又は一の列に複数の異なる入力対象文字と、
- 前記入力対象文字毎に異なる複数の形象と、
- が配置された複数の行及び複数の列により形成された表を有し、
- 各形象が、ユーザによって所定の情報を入力するために用いられる入力デバイスに基づくユーザの操作入力時に用いられる文字コードによって変換不能な形状を有している構成をしている。

- [0020] この構成により、本発明の記憶媒体は、例えば、当該入力対象文字を直接推定不能な記号、図柄、絵柄又は画像（例えば、写真を含む静止画像、動画又は手書き文字）などの形象（すなわち、ユーザによって所定の情報を入力するために用いられる入力デバイスに基づくユーザの操作入力時に用いられる文字コードによって変換不能な形状）と、が対応付けられた乱数表が形成されているので、入力対象文字を入力する際に、当該入力対象文字を使うことなく当該入力対象文字を特定することができる。

- [0021] したがって、本発明の記憶媒体は、予めユーザに発行された乱数表等に記載された情報の全てをフィッシングサイトにおいて一度に全部入力するなど、ユーザの不注意に起因するセキュリティーに関する情報（例えば、パスワード）の漏洩、及び、不正ログインする第三者への情報の譲渡を防止することができる。

- [0022] また、本発明の記憶媒体は、入力対象文字やそれを特定する形象を用いることなく、通信端末装置とサーバシステム間におけるデータ通信には形象の表示位置などの標識情報を用いることが可能となるので、通信端末装置とサーバシステム間においてユーザによって特定すべき情報が第三者により盗み取られ、又は、改竄されることを防止することができる。

[0023] したがって、本発明の記憶媒体は、ユーザに提供しているサービスへの第三者による不正ログインや中間者攻撃を有効に防止することができる。

[0024] この結果、本発明の記憶媒体は、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止し、インターネットバンクサービス等の各種のサービス提供時におけるセキュリティを向上させることができる。

発明の効果

[0025] 本発明に係るサーバシステムなどは、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止し、インターネットバンクサービス等の各種のサービス提供時におけるセキュリティを向上させることができる。

図面の簡単な説明

[0026] [図1]本発明に係るネットワークシステムの一実施形態におけるシステム構成を示すシステム構成図である。

[図2]従来から問題となっている不正攻撃の手口を説明するための図である。

[図3]一実施形態の乱数表の一例を示す図である。

[図4]一実施形態における通信端末装置の機能ブロックを示す図である。

[図5]一実施形態における金融機関サーバ装置の機能ブロックを示す図である。

[図6]一実施形態の金融機関サーバ装置内に設けられたユーザ管理データベースに記録されるデータの一例を示す図である。

[図7]一実施形態の金融機関サーバ装置内に設けられた乱数表データ管理データベースに記録されるデータの一例を示す図である。

[図8]一実施形態の金融機関サーバ装置内に設けられた金融機関管理データベースに記録されるデータの一例を示す図である。

[図9]一実施形態の金融機関サーバ装置内に設けられた口座管理データベースに記録されるデータの一例を示す図である。

[図10]一実施形態のネットワークシステムにおいて実行される決済処理の動作を示すフローチャートである。

[図11]一実施形態の通信端末装置において表示されるサービスログイン画面

の一例を示す図である。

[図12]一実施形態の通信端末装置において表示される入力画面の一例を示す図である。

[図13]一実施形態の通信端末装置において表示される確認画面の一例を示す図である。

発明を実施するための形態

[0027] 以下、図面を参照しつつ、本発明の実施形態について説明する。なお、以下の実施形態は、ユーザに対してインターネットを介してバンクサービス（以下、「インターネットバンクサービス」という。）の提供を受けるユーザ（すなわち、口座開設者）の利用する通信端末装置と、当該通信端末装置にネットワークを介して通信接続される金融機関サーバ装置と、を有するネットワークシステムに対し、本発明に係る、サーバシステム、サーバシステム用プログラム、通信端末装置、通信端末用プログラム、記憶媒体、文字入力方法及び情報暗号化方法を適用した場合の実施形態である。

[0028] なお、以下に説明する本実施形態は、請求の範囲に記載された本発明の内容を不当に限定するものではない。また本実施形態で説明される構成の全てが、本発明の必須構成要件であるとは限らない。

[0029] [1] ネットワークシステムの概要

まず、図1又は2を用いて本実施形態におけるネットワークシステム1の構成及び概要について説明する。

[0030] なお、図1は、本実施形態のネットワークシステム1のシステム構成を示す図であり、図2は、従来、インターネットバンクサービスにおいて生じている悪意の第三者による攻撃を説明するための図である。

[0031] 上記の各図においては、図が煩雑になることを防止するために、一部のユーザ、通信端末装置10、金融機関、金融機関サーバ装置30及び悪意の第三者のみを表示している。すなわち、実際のネットワークシステム1においては、図面に表示されるよりも多数のユーザ、通信端末装置10、金融機関及び金融機関サーバ装置30などが存在している。

[0032] 本実施形態のネットワークシステム 1 は、各ユーザに対して個々にインターネットバンクサービスを提供するための構成を有し、かつ、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止することが可能な所与の乱数表 RMT を用いることによって、口座や送金先の銀行などの送金先の情報又は送金金額などのインターネットバンクサービスにおける各種の処理を実行するための必要な入力対象文字を特定し、当該インターネットバンクサービスのセキュリティを向上させることが可能なシステムである。

[0033] 特に、本実施形態のネットワークシステム 1 は、図 1 に示すように、各ユーザが所有する複数の通信端末装置 10 と、各金融機関によって管理運営されるとともに、ネットワーク 20 を介して通信端末装置 10 と接続され、第三者の口座に送金する送金処理その他の決済処理を実行する複数の金融機関サーバ装置 30 と、を有している。

[0034] そして、本実施形態のネットワークシステム 1 は、所与の乱数表 RMT としては、特定のユーザによって特定されるべき数字、アルファベット、ひらがな、カタカナや漢字その他の入力対象文字（例えば、キーボードなどの入力デバイスによって一般的に入力可能な文字）と、当該入力対象文字を直接推定不能な記号、図柄、絵柄又は画像（例えば、写真を含む静止画像、動画画像又は手書き文字）などの形象（すなわち、ユーザによって所定の情報を入力するために用いられる入力デバイスに基づくユーザの操作入力時に用いられる文字コードによって変換不能な形状）と、が対応付けられた乱数表 RMT を用いることによって、上記のインターネットバンクサービスにおけるセキュリティの向上を実現することができるようになっている。

[0035] 従来のインターネットバンクサービスにおいては、例えば、図 2 に示すように、ユーザの指示に基づく端末装置からの送金指示に基づいて金融機関 A（出金用）のサーバ装置から金融機関 B（入金用）のサーバ装置に送金を行う場合に、大別して、以下のようなタイプの攻撃や詐欺が横行し、不正送金、振り込め詐欺等の被害が頻発している。

[0036] （1）タイプ 1（図 2 の [1]）

ユーザが使用するパーソナルコンピュータなどの端末装置に何らかの方法により、当該端末装置をキーロガー等のマルウェアに感染させるとともに、ユーザによって入力されたパスワード（以下、「PW」ともいう。）等の入力情報を詐取するタイプ。この場合には、不正に搾取したパスワード等を用いて金融機関A（出金用）のサーバ装置に不正にログインして正規のユーザになりすまして送金指示をし、悪意の第三者の口座など金融機関C（不正送金先）のサーバ装置に不正送金する不正送金処理を実行する。

[0037] （２）タイプ２（図２の〔２〕）

悪意の第三者が乱数発生器等を利用しつつ、金融機関A（出金用）のサーバ装置に対して全ての数字及び英文字の組み合わせを総当たりに送信する攻撃を実施し、ユーザのアカウントを乗っ取るタイプ。この場合には、金融機関A（出金用）のサーバ装置に対して正規のユーザになりすまして送金指示をし、悪意の第三者の口座など金融機関C（不正送金先）のサーバ装置に不正送金する不正送金処理を実行する。

[0038] （３）タイプ３（図２の〔３〕）

ユーザの端末装置から金融機関のサーバ装置に送信される情報をネットワーク上にて改竄し、入金先や金額等を変更して本来の入金先とは異なる入金先に入金させる中間者攻撃タイプ。例えば、ユーザの指示に基づいて端末装置から金融機関A（出金用）のサーバ装置に金融機関B（出金用）のサーバ装置への送金指示をした場合に、当該送信指示を解析した上で、当該指示を金融機関C（不正送金先）のサーバ装置に送信する指示に改竄して当該不正送金先への不正送金処理を実行するとともに、不正送金先からの送金結果をさらに金融機関B（入金用）のサーバ装置からの送金結果に偽装し、金融機関A（出金用）のサーバ装置からの送金完了として通知させる。

[0039] （４）タイプ３（図２の〔４〕）

ユーザの端末装置にメール等にて本来のサービス提供サイトとは異なるサイト（すなわち、フィッシングサイト）のURLを送信し、フィッシングサイトにユーザを誘導しつつ、当該フィッシングサイト上にてパスワードや乱

数表などの各種の情報を入力させてそれらを詐取するフィッシング詐欺タイプ（図2の〔4〕）。この場合には、不正に搾取したパスワード等を用いて金融機関A（出金用）のサーバ装置に不正にログインして正規のユーザになりすまして送金指示をし、悪意の第三者の口座など金融機関C（不正送金先）のサーバ装置に不正送金する不正送金処理を実行する。

[0040] したがって、インターネットバンクサービスの安全性を確保するためには、上記の各種の攻撃や詐欺の全てのタイプに対策を施してこれらの防止をすることが必要となる。

[0041] 一方、従来、上述の各種の攻撃を回避する方法としては、
（A）クライアント証明書を使う方法、
（B）ワンタイムパスワードを発生する暗号トークンを使う方法、
（C）ユーザの端末装置における固有情報（加入者番号、製造番号等）や指紋や静脈などの生体情報により認証する方法
などが挙げられる。

[0042] しかしながら、クライアント証明書は、容易に乗っ取られるため、有効な攻撃防止手段とはならない上に、国により、証明書のタイプが異なるため、国際的な商取引に利用できない。また、暗号トークンを利用する場合には、暗号トークンの専用機の製造に多くのコストを要するため、その普及が進んでいない。さらに、ユーザの端末装置の固有情報は、マルウェアにより抜き取られる可能性があるため、攻撃の防止方法としては、有効性を確保できない場合も多い。そして、生体情報を使う場合もそれらのデバイスの導入によるコスト高、容易に情報を入力することができなくなるなどの利便性の低下、又は、的確な生体情報の取得の困難性などにより、その普及が進んでいない。

[0043] 他方、上記の（A）～（C）の各方法に加えて、金融機関によってユーザ毎にユーザの入力するための乱数表（行列にランダムに数字が配列された表）を別途発行し、当該乱数表RMTを用いた入力を行うことによって本人確認を行う方法もある。

[0044] しかしながら、このような場合には、ユーザから金融機関に送信される情報の内容が、ASCIIコードなどの他の一般的な端末装置において特定可能なキャラクターコードにより表現されてしまう。したがって、悪意の第三者は、送受信される情報により表現される文字列を容易に特定することができるとともに、通信中の情報の改竄及び偽装を行う中間者攻撃を防止することが難しい。

[0045] また、このような乱数表RMTを用いる場合には、ユーザがフィッシングサイトに誘導され、不注意により、当該フィッシングサイト上で乱数表の全ての情報をユーザが入力してしまうことも多く、乱数表RMTの全ての情報を入力してしまうと当該乱数表RMTに基づいて本人になりすまされ、不正送金が実施されてしまう。

[0046] さらに、キーロガー等のマルウェアにユーザの端末装置などが感染した場合には、ユーザが乱数表RMTに従って入力された情報の全てが、第三者に盗み取られてしまう。

[0047] そこで、本実施形態のネットワークシステム1は、

(1) 金融機関において予めユーザ毎に発行された乱数表RMTであって、図3に例示するような数字及びアルファベットなどの入力対象文字と、記号、写真、図形又は絵柄などの当該入力対象文字を直接推定不能な形象と、が対応付けられた乱数表RMTを用いるとともに、

(2) ユーザ毎の乱数表RMTがデータ化された乱数表データと、該当ユーザを識別するためのユーザIDと、を対応付けて管理し、

(3) ユーザがインターネットバンクサービスを利用する際に、各ユーザに対応する乱数表データに基づいて該当するユーザに入力対象文字に対応する形象を含む複数の形象を表示するためのデータであって、当該入力対象文字を形象によって入力させるためのデータ（以下、「入力用データ」という。）を配信し、

(4) 入力用データに基づいて複数の形象がユーザに提供（表示）された際に、ユーザが選択した形象を特定するための表示位置を示す位置情報や当該

表示位置を特定するための情報（以下、「標識情報」という。）を特定し、
（５）特定した標識情報に基づいて形象を決定しつつ、最終的に入力対象文字を特定する、
構成を採用している。

[0048] 特に、本実施形態においては、上述のような乱数表RMTを用いることによって特定すべき入力対象文字を標識情報として通信し、通信中に第三者によって入力対象文字を特定することが不能である一方、金融機関サーバ装置30においては各ユーザの特定すべき入力対象文字を特定することが可能な構成を有している。

[0049] 具体的には、通信端末装置10は、ユーザによって使用されるパーソナルコンピュータ（PC）又はスマートフォン等の通信端末装置であり、直接、又は、基地局BSを介して、ネットワーク20に接続され、金融機関サーバ装置30とデータ通信を実行するようになっている。

[0050] また、通信端末装置10は、使用者等の入力操作に応じて、XML（eXtensible Markup Language）等のマークアップ言語によって記述されているリソースデータをURLに基づいて取得し、当該リソースデータに基づき、画像の表示及びデータ通信を行うブラウジング機能を有している。

[0051] 特に、通信端末装置10は、ブラウジング機能を利用してインターネットバンクサービスの利用時に、金融機関サーバ装置30にログインするとともに、入力用データを取得し、乱数表RMTに基づいて入力された形象における標識情報を金融機関サーバ装置30に送信するようになっている。

[0052] 一方、金融機関サーバ装置30は、各金融機関によって管理運営されるコンピュータシステムであり、各種のデータベース（以下、「DB」という。）を有し、インターネットバンクサービスを提供するための各種処理を実行する。

[0053] 特に、本実施形態の金融機関サーバ装置30は、
（A）インターネットバンクサービスのサービス提供時に、通信端末装置1

０と連動し、ユーザを特定しつつ、当該ユーザ毎に発行された乱数表ＲＭＴに対応する乱数表データに基づいて入力用データを生成し、生成した入力用データを通信端末装置１０に配信する入力用データ配信処理と、

（Ｂ）通信端末装置１０から送信された、入力用データ及び乱数表ＲＭＴに基づいてユーザによって入力された標識情報を受信し、受信した標識情報に基づいて入力対象文字を特定する入力対象文字特定処理と、

（Ｃ）特定した入力対象文字に基づいて所定のインターネットバンクサービスを実行するサービス処理と、

を実行することが可能なことが可能な構成を有している。

[0054] 具体的には、本実施形態の金融機関サーバ装置３０は、

（１）通信端末装置１０のユーザ毎に予め定められた乱数表データであって、通信端末装置１０にて入力される入力対象文字と、当該入力対象文字の各々に対して予め割り当てられた形象と、を対応付けた乱数表データが、ユーザを識別するための識別情報（すなわち、ユーザＩＤ）と対応付けて記録されるデータベースを制御し、

（２）通信端末装置１０からユーザを指定した所与の要求（例えば、決済処理の要求）が受信された場合に、当該ユーザに対応する乱数表データを特定し、

（３）特定した乱数表データに基づき、ユーザによって特定すべき入力対象文字に対応する形象を抽出し、

（４）抽出した形象の各々に対応付けられ、かつ、該当する通信端末装置１０にて該当する形象が表示される際に用いる標識情報を含む入力用データを生成し、当該生成した入力用データを通信端末装置１０に配信し、

（５）配信した入力用データに基づき通信端末装置１０にて形象が表示された際に、ユーザが入力した形象に対応する標識情報を当該通信端末装置１０から取得し、

（６）取得した標識情報に基づき、該当する形象を決定し、

（７）決定した形象に基づき、特定すべき入力対象文字を特定し、当該特定

した入力対象文字に基づき、決済処理などの所与の処理を実行する、構成を有している。

[0055] このような構成により、本実施形態のネットワークシステム1は、予めユーザに発行された乱数表RMT等に記載された情報の全てをフィッシングサイトにおいて一度に全部入力するなど、ユーザの不注意に起因するセキュリティに関する情報（例えば、パスワード）の漏洩、及び、不正ログインする第三者への情報の譲渡を防止することができるようになっている。

[0056] また、本実施形態のネットワークシステム1は、ユーザに提供しているサービスへの第三者による不正ログインや中間者攻撃を有効に防止することができるようになっている。

[0057] したがって、本実施形態のネットワークシステム1は、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止し、インターネットバンクサービス等の各種のサービス提供時におけるセキュリティを向上させることができるようになっている。

[0058] なお、本実施形態においては、入力用データには、
（1）通信端末装置10において各形象を選択させるための画像データ、
（2）当該画像データが通信端末装置10において表示される際の表示位置を示す位置情報、及び、
（3）各形象の画像データを各表示位置に表示させるための表示制御データが含まれる。

[0059] また、入力用データを生成する際に用いられるユーザに選択させるための複数の形象には、入力される可能性のある入力対象文字に対応する全ての形象が含まれることが好ましく、本実施形態においては、当該入力用データを生成する際に用いられる形象には、入力される可能性のある入力対象文字に対応する全ての形象が含まれた場合を用いて説明する。

[0060] ただし、生成された入力用データには対象入力文字に該当する形象の画像データが含まれていない場合には、当該入力用データを再発行するなどの所定の処理を実施すれば、特定すべき入力対象文字の数Nに対して（N+1）

の数の形象の画像データを用いればよい。

[0061] また、本実施形態においては、標識情報としては、各形象における通信端末装置 10 において表示される際の表示位置情報を用いて説明するが、各形象が通信端末装置 10 において例えば行列を伴って表示される場合には、行番号及び列番号の情報など、ユーザによって選択された各形象を特定するための情報であればよい。

[0062] [2] 乱数表

次に、図 3 を用いつつ、本実施形態の乱数表 RMT について説明する。なお、図 3 は、本実施形態において利用される乱数表 RMT の一例を示す図である。

[0063] 本実施形態の乱数表 RMT は、ユーザが通信端末装置 10 を用いて、各種のサービスを提供する金融機関サーバ装置 30 にアクセスする際に、当該ユーザが入力する入力対象文字を金融機関サーバ装置 30 において特定するための形象が視認可能に形成された記憶媒体であって、一の行又は一の列に複数の異なる入力対象文字と、入力対象文字毎に異なる形象と、が配置された複数の行及び複数の列により形成された表を有し、各形象が、ユーザによって所定の情報を入力するために用いられる入力デバイスに基づくユーザの操作入力時に用いられる文字コードによって変換不能な形状を有している。

[0064] 例えば、本実施形態の乱数表 RMT は、図 3 に示すように、先頭行に入力対象文字として数字「0」～「9」が一行に配置され、複数行（すなわち、6 行）から構成される乱数表（すなわち、6 行 10 列の行列状の乱数表 RMT）であって、各入力対象文字としての各数字のそれぞれに割り当てられた異なる形象（すなわち、10 個の記号、図形又は絵柄のいずれか）を有し、行毎に形象の配置が異なる特徴を有している。

[0065] そして、本実施形態の乱数表 RMT は、金融機関がユーザに発行するキャッシュカード（プラスチック製）の裏面に印刷してユーザに提供され、又は、専用の暗証カード（プラスチック製又は紙製）に印刷してユーザに提供される。

- [0066] なお、乱数表RMTは、暗証カードを電子的に提供してもよい。この場合には、例えば、暗証カードを電子ペーパーにより構成し、電子インクにより視認可能に構成してもよいし、パーソナルコンピュータやスマートフォンによって表示可能に構成してもよい。この場合には、暗号トークンとは異なり、乱数表RMTの発行におけるコストを抑えることができるので、その普及を促進することができるようになっている。
- [0067] 一方、図3においては、入力対象文字をデータ通信中に推定不能な形象によって構成する場合について例示しているが、当該形象は、一般的な入力デバイスによって一意的に推定不能なものであればよく、上述のように、例えば、写真等の静止画であってもよく、事前にユーザに記載させた手書き文字により形成された形象であってもよい。
- [0068] 特に、ユーザによる手書きの文字を形象として用いる場合には、口座開設時又は暗証カードの発行申込時などの所定のタイミングに、ユーザに0～9の数字と、A～Zの英字を申込書に記入させるようにして、その記入された文字を用いて乱数表RMTの形象を構築するようにすればよい。
- [0069] 他方、本実施形態の乱数表RMTは、数字を入力対象文字として用いる場合には、少なくとも「0」～「9」の数字を先頭行に記載する必要があるとともに、英字、ひらがな、カタカナ、漢字、又はその他の文字による入力に用いる場合には、「A」～「Z」又は入力すべき文字を先頭行に記載する必要がある。ただし、いずれの文字を入力対象文字として用いる場合には、各行においてそれぞれ異なる形象を配置するとともに、複数行において当該形象の配置が異なるように、各形象を各文字に対応付けて配置することが必要となる。
- [0070] なお、図3においては、乱数表RMTの先頭行に入力対象文字を配置してあるが、本実施形態においては、乱数表RMTの末行に配置するようにしてもよく、先頭列又は末列に配置するようにしてもよい。いずれの場合においても図3の例と同様に、各行や各列においてそれぞれ異なる形象を配置するとともに、複数行又は複数列において当該形象の配置が異なるように、各形

象を各文字に対応付けて配置することが必要となる。

[0071] [3] 通信端末装置

次に、図4を用いて本実施形態の通信端末装置10について説明する。なお、図4は、本実施形態の通信端末装置10の構成を示すブロック図である。

[0072] 本実施形態の通信端末装置10は、図4に示すように、ネットワーク通信部110と、記録部120と、表示制御部130と、表示部140と、操作部150と、端末管理制御部160と、アプリケーション実行部170と、を有している。

[0073] なお、上記の各部は、バスBによって相互に接続され、各構成要素間におけるデータの転送が実行される。

[0074] ネットワーク通信部110は、基地局BSを介して、又は、直接、ネットワーク20に通信接続され、ネットワーク20を介して、金融機関サーバ装置30と、各種データの授受を行う。

[0075] 記録部120は、例えば、ハードディスクドライブ（以下、「HDD」と略す。）、或いは、NAND型、NOR型等の不揮発性フラッシュメモリによって構成される。

[0076] また、記録部120は、アプリケーション記録部121と、バッファ122と、を有し、アプリケーション記録部121には、ブラウジング機能を実現するためのブラウザが記録される。

[0077] なお、インターネットバンクサービス専用のアプリケーションを用いて、サービスを提供する場合には、専用アプリケーションが、アプリケーション記録部121に記録される。バッファ122は、ネットワーク通信部110、端末管理制御部160及びアプリケーション実行部170のワークエリアとして用いられる。

[0078] 表示制御部130は、表示部140に表示させるために必要な表示データを生成するようになっており、生成された表示データを当該表示部140に出力する。

- [0079] 具体的には、金融機関サーバ装置30から受信した入力用データに基づき、入力対象文字列と、を対応付けつつ、各形象に対応する画像データを表示部140に表示させるための表示データを生成し、表示部140に供給する。
- [0080] 表示部140は、例えば、液晶素子または有機EL (Electro Luminescence) 素子のパネルによって構成され、表示制御部130において生成された表示データに基づいて所定の画像を表示する。
- [0081] 操作部150は、各種の確認ボタン、マウス、ポインティングデバイス、テンキーなどの多数のキー及びタッチパネルにより構成され、ユーザが入力用データに基づき、各種情報を入力するとともに形象を選択するために用いられるようになっている。例えば、操作部150は、入力用データに基づいて表示された複数の形象の中から一の形象を選択する際に用いられ、特定の表示位置にタッチされた場合に、タッチされた位置に表示された形象の位置情報をアプリケーション実行部170に提供する。
- [0082] 端末管理制御部160は、主に中央演算処理装置(CPU)によって構成されるとともに、キー入力ポート、表示制御ポート等の各種入出力ポートを含み、記録部120に記録された各種のアプリケーションを実行することにより、通信端末装置10の全般的な機能を総括的に制御する。
- [0083] アプリケーション実行部170は、端末管理制御部160と同一又は独立したCPUにより構成され、端末管理制御部160による制御の下、アプリケーション記録部121に記録された各種のアプリケーションを実行することによりインターネットバンクサービスのサービスを受けるための処理を実行する。
- [0084] [4] 金融機関サーバ装置
- 次に、図5～図9を用いて本実施形態の金融機関サーバ装置30の構成について説明する。
- [0085] なお、図5は本実施形態の金融機関サーバ装置30の機能ブロックの一例を示す図であり、図6～図9は、本実施形態の金融機関サーバ装置30内に

設けられたユーザ管理DB331、乱数表データ管理DB332、金融機関管理DB333、口座管理DB334、に記録されるデータの一例を示す図である。

[0086] 本実施形態の金融機関サーバ装置30は、図5に示すように、ネットワーク20に通信接続される通信制御部310と、各種のメモリとして機能するROM/RAM320と、各種のDBが構築される記録装置330と、装置全体を制御するサーバ管理制御部340と、インターネットバンクサービスの提供時に各種の処理を実行するデータ処理部350と、を有し、上記の各部は、バスBによって相互に接続されている。

[0087] 通信制御部310は、所定のネットワークインターフェースであり、ネットワーク20を介して通信端末装置10と通信チャネルを構築し、各種データの授受を行う。

[0088] ROM/RAM320には、金融機関サーバ装置30の駆動に必要な各種のプログラムが記録されている。また、ROM/RAM320は、各種の処理が実行される際のワークエリアとして用いられる。

[0089] 記録装置330は、例えば、HDD (Hard Disc Drive)、又は、SSD (Solid State Drive) により構成される。そして、記録装置330は、少なくとも、ユーザ管理DB331と、乱数表データ管理DB332と、金融機関管理DB333と、口座管理DB334と、を有している。なお、本実施形態の記録装置330は、例えば、本発明の「記録手段」を構成する。

[0090] ユーザ管理DB331は、該当する金融機関に口座を開設済みのユーザを管理するための各種情報がデータとして登録されるデータベースである。例えば、ユーザ管理DB331には、図6に示すように、各ユーザに対応するユーザIDと対応付けて、ユーザ属性情報が記録される。

[0091] 特に、ユーザ属性情報は、
(1) 対応するユーザの氏名、
(2) 住所、

(3) アカウント名、及び、

(4) 第1暗証（ログインパスワード）

を含み、インターネットバンクサービスに対するユーザのログインを管理するために用いられる。

[0092] 例えば、図6には、ユーザID「user001」に対応するユーザ属性情報として、氏名「〇〇太郎」、住所「東京都北区***」アカウント名「2351000」、第1暗証「****」なるユーザ属性情報が記録された状態が示されている。

[0093] なお、アカウント名は、口座番号又はお客様番号等であってもよく、ユーザIDと同一のものを用いてもよい。

[0094] 乱数表データ管理DB332は、各ユーザに予め発行される乱数表RMTに対応した乱数表データを管理するためのデータベースである。例えば、乱数表データ管理DB332には、図7に示すように、各ユーザに対応するユーザIDと、当該ユーザに発行された乱数表RMTの内容を示す乱数表データと、が各々対応付けて記録される。

[0095] 例えば、図7には、「user001」～「user004」の各々に対して、乱数表データ、「DATA001」～「DATA004」が対応付けて記録された状態が示されている。

[0096] 特に、乱数表データ管理DB332に記録される乱数表データは、図3に例示するように、乱数表RMTに含まれる入力対象文字と、各入力対象文字に割り当てられた形象を通信端末装置10にてアイコン表示させるための画像データと、乱数表RMTと同様の行列形式にて配置されたデータ構成となっている。

[0097] なお、各形象に対応する画像データには、例えば、

(1) 学術記号（例えば、微分積分等の数学記号や地図記号、音楽記号等）を含む各種記号を示す絵柄又は図形に対応するビットマップ

(2) 写真等の静止画

(3) 動画

(4) 手書き文字の画像

のいずれの形式にて構成することも可能である。

[0098] 特に、形象の画像データとして、静止画を用いる場合には、画像データを、例えば、J P E G (J o i n t P h o t o g r a p h i c E x p e r t s G r o u p) 等のデータ形式により構成すればよい。

[0099] また、形象の画像データを動画により構成する場合には、画像データを、例えば、G I F 等の形式にて構成することにより、通信端末装置 10 にて、徐々に形象が浮かび上がるように形象を表示させ、又は、形象が順次入れ替わって表示されるとともに、所定時間経過後に形象を表示させるような表示方法を実現するデータ形式によって構成すればよい。

[0100] そして、形象を動画として表示する場合には、通信端末装置 10 に配信する入力用データに含まれる形象の特定を困難にして、悪意の第三者による、各種攻撃を更に困難にすることが可能となる。ただし、発行される乱数表 R M T においても、動画の形象が再生可能な電子ペーパー又は携帯端末装置などによって提供される必要がある。

[0101] さらに、ユーザが事前に登録済みの入金先に関する入金先情報（金融機関、支店入金先口座番号、名義人）が入力対象文字に割り当てられている場合、又は、所定の定型文又は定型フォーマットが入力対象文字に割り当てられている場合には、当該入力対象文字に対応付けて入金先情報又は所定の定型文なども対応付けて登録されている。

[0102] 金融機関管理 D B 3 3 3 は、各金融機関を管理するための情報がデータとして記録されるデータベースである。例えば、金融機関管理 D B 3 3 3 には、図 8 に示すように、各金融機関を識別するための金融機関コードと対応付けて、

- (1) 当該金融機関の金融機関名、
- (2) 当該金融機関が運営している各支店の支店名、
- (3) 当該支店の支店コード、及び、
- (4) 当該支店の住所、

が記録される。

[0103] 例えば、図8には、金融機関コード「B001」の「大江戸銀行」が、「新宿支店」と、「渋谷支店」と、「日本橋本店」と、を運営しており、各支店の支店コード等が記録された状態が示されている。

[0104] なお、金融機関コードは、各金融機関に対して一つずつ割り当てられる一方、支店コードは、金融機関毎に独自に割り当てられるものである。また、金融機関コードに代えて、S W I F Tコードなどの銀行コード、国名、所在地コード及び支店コードなどの他のコードを含むものであってもよい。

[0105] 口座管理DB334は、各ユーザが開設している口座を管理するための情報に対応するデータが、記録されるデータベースである。例えば、口座管理DB334には、図9に示すように、

- (1) 各ユーザのユーザID、及び、
- (2) 口座情報、

が対応付けて記録される。

[0106] 特に、口座情報には、

- (2A) 該当する口座の口座番号、
- (2B) 該当する口座の開設された銀行名及び支店名、
- (2C) 該当する口座の口座残高、及び、
- (2D) 登録済みの振込先を示す情報、

が含まれ、これらの情報は、ユーザの口座を管理するために用いられる。

[0107] 例えば、図9には、「user001」の口座情報として口座番号「1234567」、金融機関名「大江戸銀行」、支店名「新宿支店」、残高「¥*****」登録済み振り込み先「大江戸銀行日本橋本店*****」及び「△銀行渋谷支店*****」なる口座情報が、記録された場合が示されている。

[0108] なお、本実施形態においては、登録済み振り込み情報は、上記入金先情報として利用することができる。

[0109] サーバ管理制御部340は、主に中央演算処理装置(CPU)によって構

成され、プログラムを実行することによって、金融機関サーバ装置 30 の各部を統合制御する。

[0110] データ処理部 350 は、サーバ管理制御部 340 と同一又は異なる CPU により構成され、サーバ管理制御部 340 による制御の下、アプリケーションを実行することにより、通信端末装置 10 から所定の口座への送金処理その他の決済処理におけるインターネットバンクサービスを提供する際に、入力用データを通信端末装置 10 に配信する入力用データ配信処理と、入力用データ及び乱数表 RMT に基づく入力に応じて通信端末装置 10 から送信された標識情報に基づいて入力対象文字を特定する入力対象文字特定処理と、特定した入力対象文字に基づいて所定のインターネットバンクサービスを実行するサービス処理と、を実行する。

[0111] 具体的には、データ処理部 350 は、通信制御部 310 及び記録装置 330 と連動し、各 DB へのデータの記録及び更新その他のインターネットバンクサービスの管理を行う管理制御部 351 と、インターネットバンクサービスを提供する際に、該当するユーザの乱数表データを特定し、当該特定した乱数表データから一部の形象を抽出する形象抽出部 352 と、抽出した形象に基づいて入力用データ配信処理を実行する入力用データ生成配信部 353 と、入力対象文字特定処理を実行する特定処理部 354 と、決済処理などの特定した入力対象文字に基づくインターネットバンクサービス（以下、「特定のバンクサービス」という。）を実行する決済処理部 355 と、を実現する。

[0112] なお、例えば、本実施形態の管理制御部 351 は、本発明の「制御手段」を構成し、形象抽出部 352 は、本発明の「特定手段」及び「抽出手段」を構成する。また、例えば、本実施形態の入力用データ生成配信部 353 は、本発明の「配信手段」を構成し、特定処理部 354 は、本発明の「取得手段」を構成する。さらに、例えば、本実施形態の決済処理部 355 は、本発明の「処理手段」を構成する。

[0113] 管理制御部 351 は、各 DB に対するデータの読み出し及び書き込みを管

理する。また、管理制御部 351 は、図示せぬスキャナー等又は手動によって予め取り込まれた乱数表 RMT に基づいて乱数表データを生成し、対応するユーザ ID と対応付けて乱数表データ管理 DB 332 に記録させる。

[0114] なお、管理制御部 351 において乱数表データが生成される方法は、任意であり、例えば、乱数表 RMT に含まれる各形象を分離し、入力対象文字と対応付けつつ、行列状に形象を配置して、図 3 に例示するような乱数表 RMT に対応する乱数表データを生成するようにしてもよい。

[0115] また、管理制御部 351 は、通信端末装置 10 からのインターネットバンクサービスの実行要求に応じて、当該インターネットバンクサービスのログインページに対応するデータを、該当する通信端末装置 10 に配信し、当該データに基づきユーザが入力したアカウント名及び第 1 暗証（パスワード）と、ユーザ属性情報に基づき、ユーザ認証を実行する。

[0116] そして、管理制御部 351 は、ログイン後において、通信端末装置 10 と連動し、ユーザの操作に基づいて、決済処理などの特定のバンクサービスを除き、口座における残高照会又はローンの申し込みなどの各種のインターネットバンクサービスに関する処理を実行する。

[0117] 形象抽出部 352 は、決済処理などの特定のバンクサービスにおける処理要求を受信した場合に、管理制御部 351 の制御の下、ログインした際のユーザ ID に基づいて乱数表データ管理 DB 332 を検索し、該当する乱数表データを乱数表データ管理 DB 332 から読み出す。そして、形象抽出部 352 は、読み出した乱数表データから、例えば、ランダムに選択された 2 つの行に属する複数の形象に対応する画像データを抽出する。

[0118] 例えば、図 3 に示す乱数表 RMT に対応する乱数表データを読み出した場合には、形象抽出部 352 は、読み出した乱数表データから入力対象文字を特定するための形象として、B 行目及び E 行目に配置される各形象に対応するそれぞれの画像データを抽出する。

[0119] 入力用データ生成配信部 353 は、決済処理などの特定のバンクサービスにおける処理要求を受信した場合であって、形象抽出部 352 により複数の

形象の画像データが読み出された場合に、管理制御部 351 の制御の下、通信制御部 310 と連動しつつ、入力用データの生成及びその配信を実行する。

[0120] 具体的には、入力用データ生成配信部 353 は、形象抽出部 352 によって抽出された各形象の画像データに基づいて、入力用データを生成し、生成した入力用データを該当する通信端末装置 10 に配信する。

[0121] 特に、入力用データ生成配信部 353 は、抽出された各形象の画像データの表示位置を特定しつつ、特定した各形象の表示位置を示す位置情報（すなわち、標識情報）を決定し、各形象の画像データと、各形象の表示位置を示す位置情報と、当該各形象の画像データを各表示位置に表示させるための表示制御データと、ユーザに入力を指示するための指示データと、を含む入力用データを生成し、生成した入力用データを該当する通信端末装置 10 に配信する。

[0122] 例えば、図 3 に示す乱数表 RMT に対応する乱数表データにおいて、B 行目及び E 行目に配置される各形象の画像データが読み出されている場合を想定する。この場合においては、入力用データ生成配信部 353 は、例えば、B 行を表示するための列表示に基づいて、一番右に B 行 2 列の形象、そして、その次の列の表示位置に B 行 5 列の形象が表示されるように、一列にかつランダムに各形象を通信端末装置 10 において表示するための表示位置（例えば、通信端末装置 10 の画面上に各形象の画像データを表示するためのピクセル座標であって、画像データの中心を示す中心座標（ x 、 y ））を決定する。そして、入力用データ生成配信部 353 は、決定した各形象の表示位置を示す位置情報を有する入力用データを生成する。

[0123] なお、入力用データ生成配信部 353 は、E 行を表示するための列表示に基づいて、一列にかつランダムに各形象を通信端末装置 10 において表示するための表示位置を決定する。

[0124] また、例えば、ユーザに選択させるべき形象を指示するための指示データとしては、例えば、「乱数表 RMT の B 行目から入力したい文字に対応する

形象を選択してください」等の文字列（テキスト）のデータが含まれる。

[0125] 特定処理部 354 は、通信端末装置 10 において入力用データに基づいてユーザによって形象が入力された場合に取得した位置情報（すなわち、入力用データ及び乱数表 RMT に基づいて入力された形象に対応する標識情報）を受信すると、当該受信した位置情報と、該当する乱数表データと、形象抽出部 352 によって入力用データの生成に用いられた情報であって、形象を抽出した際の乱数表 RMT の行を示す情報（以下、「抽出情報」という。）と、に基づいて、ユーザの選択した形象に対応する入力対象文字を特定する。

[0126] 例えば、図 3 に示す乱数表 RMT に対応する乱数表データにおいて、B 行目に配置される各形象の画像データが読み出されている場合であって、最右側に B 行 2 列目の形象が配置されており、その位置を示す位置情報（標識情報）を受信した場合には、特定処理部 354 は、入力対象文字として「B 行 2 列目」に対応する入力対象文字「2」を特定する。

[0127] なお、特定処理部 354 は、例えば、複数の入力対象文字を入力した順番に応じて特定する。すなわち、特定処理部 354 は、2 桁の入力対象文字を特定する場合には、最初に特定した入力対象文字を上位の桁に、また、その次に特定した入力対象文字を下位の桁に対応させて特定する。

[0128] 決済処理部 355 は、特定された入力対象文字に従って、入金先の口座や入金額等の所定の情報を決定し、決定した情報に基づいて決済処理を実行する。

[0129] 例えば、決済処理部 355 は、特定された入力対象文字に従って入金先の金融機関を特定し、該当するユーザの口座情報から入金額相当分の残高を減算しつつ、入金先の口座に特定された入金額を送信するための決済処理を実行する。

[0130] なお、本実施形態における決済処理は、従来のインターネットバンクサービスと同様であるため、詳細を省略する。

[0131] [5] ネットワークシステムの動作（決済処理）

次に、図１０～図１３を用いて本実施形態のネットワークシステム１において実行される決済処理の動作について説明する。

[0132] なお、図１０は、本実施形態のネットワークシステム１にて実行される処理の流れを示すフローチャートであり、図１１は、本実施形態のネットワークシステム１において、インターネットバンクサービスにログインする際のログインページの一例を示す図である。また、図１２は、本実施形態のネットワークシステム１において入力用データに基づき、ユーザが各種情報を入力する際の入力画面の一例を示す図であり、図１３は、本実施形態のネットワークシステム１において入力用データに基づき、ユーザが各種情報を入力した後に表示される確認画面の一例を示す図である。

[0133] 本動作においては、金融機関サーバ装置３０の各ＤＢ３３１～３３４には、図６～図９の情報が予め記憶されているものとし、通信端末装置１０においては、例えば、図１１に示す所定のログイン画面表示を表示しつつ、ユーザが、操作部１５０にインターネットバンクサービスを行う旨の指示を入力するのを待機する状態になっているものとする。

[0134] なお、本動作においては、第三者の口座に対して送金処理を行う決済処理（特定のバンクサービス）を実行するものとして説明する。

[0135] まず、通信端末装置１０において、アプリケーション実行部１７０は、操作部１５０を介してアカウント名及び第１暗証と、「ログイン」ボタンを選択する旨の入力操作と、を検出すると（ステップＳａ１０１）、アプリケーション記録部１２１に記録されたアプリケーションに従って、入力されたアカウント名及び第１暗証を含むログイン要求を金融機関サーバ装置３０に送信し、受信待機状態に移行する（ステップＳａ１０２）。

[0136] 次いで、金融機関サーバ装置３０においては、通信制御部３１０が通信端末装置１０から送信されたログイン要求を受信すると（ステップＳａ３０１）、管理制御部３５１は、ログイン要求に含まれているアカウント名及び第１暗証に基づいてユーザ管理ＤＢ３３１を検索し、ユーザＩＤを特定してユーザ認証を実行する（ステップＳａ３０２）。

[0137] 次いで、管理制御部 351 は、ユーザ認証を適切に実行してログインが実行されると、通信制御部 310 を介して、該当する通信端末装置 10 に、該当するユーザにおける各種のネットバンクサービスを実行するための Web ページ（以下、「ユーザページ」という。）に対応するデータを該当する通信端末装置 10 に送信し、受信待機状態に移行する（ステップ S a 303）。

[0138] なお、ステップ S a 302 において、ログインが適切にできない場合には、管理制御部 351 は、その旨を該当する通信端末装置 10 に送信して本動作を終了させる。また、通信端末装置 10 は、ログインが適切にできなかった旨を受信した場合には、ステップ S a 101 の処理に戻る。さらに、管理制御部 351 は、ログイン状態中に通信端末装置 10 からログアウト指示を受信した場合には、本動作の各処理に無関係に本動作を終了させる。

[0139] 次いで、通信端末装置 10 においては、ネットワーク通信部 110 がユーザページのデータを受信すると（ステップ S a 103）、アプリケーション実行部 170 は、表示制御部 130 と連動しつつ、表示部 140 にユーザページの画像を表示させ、第三者の口座に対して送金を実行する決済処理の操作入力を待機する（ステップ S a 104）。

[0140] なお、アプリケーション実行部 170 は、ログイン状態中に操作部 150 を介してログアウト指示を検出した場合には、本動作の各処理に無関係に金融機関サーバ装置 30 にログアウト指示を送信して本動作を終了させる。

[0141] 次いで、アプリケーション実行部 170 は、操作部 150 を介して決済処理の実行指示を検出する（ステップ S a 105）と、当該決済処理の実行要求を金融機関サーバ装置 30 に送信し、受信待機状態に移行する（ステップ S a 106）。

[0142] 次いで、金融機関サーバ装置 30 において、管理制御部 351 は、決済処理を実行するための実行要求を受信すると（ステップ S a 311）、形象抽出部 352 に該当するユーザ（すなわち、ログイン状態のユーザであって決済処理の要求を行ったユーザ）に対応する乱数表データを乱数表データ管理

DB332から読み出させて取得する（ステップSa312）。

[0143] 次いで、形象抽出部352は、当該読み出された乱数表データから、複数の入力対象文字を選択するためにランダムに任意の一行に属する複数の形象を抽出する（ステップSa313）。

[0144] 次いで、入力用データ生成配信部353は、乱数表データ管理DB332から抽出された形象に対応する画像データを読み出しつつ、抽出された各形象の画像データの表示位置を特定し、特定した各形象の表示位置を示す位置情報（すなわち、標識情報）を決定する（ステップSa314）。

[0145] 次いで、入力用データ生成配信部353は、読み出した各形象の画像データと、各形象の表示位置を示す位置情報（標識情報）と、当該各形象の画像データを各表示位置に表示させるための表示制御データと、ユーザに入力を指示するための指示データと、を含む入力用データを生成し、生成した入力用データを該当する通信端末装置10に配信する（ステップSa315）。

[0146] 例えば、入力用データ生成配信部353は、図12に例示するように、

- (1) 入金先の金融機関名、
- (2) 入金額、
- (3) 入金先の支店名、
- (4) 口座種別（普通、当座等）を選択するためのプルボックス、及び、
- (5) 入金先の口座番号の先頭から所定の桁分（例えば、先頭5桁分）を入力させるためのテキストボックスを通信端末装置10にて表示させるためのデータと、
- (6) 形象により入力させる入力対象文字（例えば、口座番号の下2桁分）を選択させるため、「（下2桁目）に該当する形象をB行から選択して下さい」等の文字列及びB行目の形象に対応する画像データ、及び、
- (7) 「最後の桁に対応する形象をE行目から選択して下さい」等の文字列と、E行目の形象に対応する画像データ、

を含む入力用データを生成する。

[0147] なお、各テキストボックスは、プルダウンボックスにより代替するように

してもよい。

[0148] 次いで、通信端末装置 10 において、ネットワーク通信部 110 が金融機関サーバ装置 30 から配信された入力用データを受信すると、（ステップ S a 111）、アプリケーション実行部 170 は、受信された入力用データに基づき、図 13 に例示するような入力画面（以下、「口座情報入力画面」ともいう。）を表示させる（ステップ S a 112）。

[0149] 次いで、アプリケーション実行部 170 は、操作部 150 と連動して、口座情報入力画面に従って、入力された送金金額、送金先の銀行名、支店名、口座種別、及び、口座番号の一部を取得するとともに、該当する乱数表 RMT と照らし合わせて入力された口座番号の他の部分（すなわち、入力対象文字）を特定するための形象の位置情報を含む入力口座情報を取得する（ステップ S a 113）。

[0150] 特に、本実施形態のアプリケーション実行部 170 は、入力対象文字を形象によって特定するための情報として、座番号の下二桁の番号に対応する形象の位置を検出すると、当該検出した形象の位置を示す位置情報を特定する。

[0151] 例えば、入力対象文字となる口座番号の下二桁が「21」の場合であって操作部 150 によって乱数表 RMT の B 行 2 列の形象、及び、E 行 1 列の形象が選択された場合には（該当する形象の表示位置がタッチされた場合には）、アプリケーション実行部 170 は、上位桁の形象の位置情報として画像データの紙面に向かって左から 8 番目の位置を示す位置情報、及び、下位桁の形象の位置情報として画像データの紙面に向かって左から 5 番目の位置情報を特定する。

[0152] 次いで、アプリケーション実行部 170 は、標識情報としての位置情報を含む入力口座情報を表示部 140 に表示するとともに（ステップ S a 114）、当該入力口座情報を金融機関サーバ装置 30 に送信し、送金結果を示す情報の受信を待機する（ステップ S a 115）。

[0153] なお、アプリケーション実行部 170 は、表示制御部 130 と連動し、例

例えば、図 14 に示すように、標識情報としての位置情報を含むステップ S a 113 によって取得した情報（バンクサービス特定情報）を表示部 140 に表示する。ただし、アプリケーション実行部 170 は、バンクサービス特定情報を取得した後に、金融機関サーバ装置 30 と連動し、当該金融機関サーバ装置 30 において口座の確認が為された場合に、バンクサービス特定情報を表示部 140 に表示してもよい。

[0154] 次いで、金融機関サーバ装置 30 において、通信制御部 310 が通信端末装置 10 により送信された入力口座情報を受信すると（ステップ S a 321）、特定処理部 354 は、受信された入力口座情報に含まれる位置情報と、該当するユーザに配信した入力用データ及び当該ユーザの乱数表データと、に基づき、ユーザの選択した形象に対応する入力対象文字を特定する（ステップ S a 322）。

[0155] 特に、本実施形態においては、特定処理部 354 は、ユーザが入力画面にて入力した口座番号の先頭 5 桁分に対して、位置情報に基づいて特定された下 2 桁分の文字を組み合わせる 7 桁から構成される送金先口座番号を決定する。

[0156] 次いで、決済処理部 355 は、ステップ S a 310 にて特定された入力対象文字と、受信された入力口座情報に含まれる各情報と、に基づいて送金処理を行う決済処理を実行する（ステップ S a 323）。具体的には、決済処理部 355 は、特定された送金先口座番号と、入力口座情報に含まれる送金先の金融機関名及び支店名等と、に基づいて、送金処理を行う。

[0157] なお、このとき、送金先の金融機関サーバ装置 30 は、適切に口座情報等が特定されている場合には、口座管理 DB の入金先口座に対応する口座情報の残高に送金額相当の金額を加算し、送金が適切に実行された旨を送金元の金融機関サーバ装置 30 に通知する。

[0158] 最後に、決済処理部 355 は、決済の結果を示す決済結果情報を該当する通信端末装置 10 に送信して（ステップ S a 324）本動作を終了させる。

[0159] なお、管理制御部 351 は、決済結果情報においては、送金先の金融機関

サーバ装置 30 からの通知の受領後に送信する。また、管理制御部 351 は、決済結果情報の送信後に、本動作を終了させずに、決済処理の終了後にログイン状態を維持し、更に該当する通信端末装置 10 からの入力操作を待機してもよい。

[0160] 一方、通信端末装置 10 においては、アプリケーション実行部 170 は、ネットワーク通信部 110 を介して決済結果情報を受信すると（ステップ S a 1 2 1）、表示制御部 130 と連動して受信した決済結果を表示部 140 に表示して（ステップ S a 1 2 2）本動作を終了させる。

[0161] なお、アプリケーション実行部 170 は、金融機関サーバ装置 30 と同様に、決済結果情報の表示後に、本動作を終了させずに、ログイン状態を維持し、ステップ S a 1 0 4 の処理に移行してもよい。

[0162] 以上説明したように、本実施形態のネットワークシステム 1 は、予めユーザに発行された乱数表 RMT 等に記載された情報の全てをフィッシングサイトにおいて一度に全部入力するなど、ユーザの不注意に起因するセキュリティに関する情報（例えば、パスワード）の漏洩、及び、不正ログインする第三者への情報の譲渡を防止することができる。

[0163] また、本実施形態のネットワークシステム 1 は、ユーザに提供しているサービスへの第三者による不正ログインや中間者攻撃を有効に防止することができる。

[0164] したがって、本実施形態のネットワークシステム 1 は、セキュリティに関する情報の漏洩、不正使用及び中間者攻撃を防止し、インターネットバンクサービス等の各種のサービス提供時におけるセキュリティを向上させることができる。

[0165] [6] 変形例

[6. 1] 変形例 1

上記実施形態においては、入金先の口座番号の一部を入力用データに基づいて入力させる構成としたが、金融機関名、入金額等の一部を入力用データに基づき入力させるようにしてもよい。

[0166] この方法を採用した場合にも、第三者による各種攻撃を防止して、インターネットバンクサービスにおけるセキュリティーを向上させ、不正使用等を防止することが可能となる。

[0167] [6. 2] 変形例2

また、上記実施形態においては、パスワード（第1暗証）を利用して、第一段階のユーザ認証を行った後に、入力用データと乱数表RMTによる入力を行うことにより、セキュリティーを向上させる構成を採用した。

[0168] しかしながら、例えば、ネットワークを用いたオンラインストアのように、ユーザのアカウント名及びパスワードのみで、決済が実行されるようなサービスの場合には、アカウントの一部、パスワードの一部又は双方を乱数表データ及び乱数表RMTを用いて入力させるようにしてもよい。

[0169] この場合には、通信端末装置10は、例えば、アカウント名のみを送信するとともに、金融機関サーバ装置30は、当該送信されたアカウント名に応じてユーザID及び乱数表データを特定し、パスワード入力用の入力用データを生成し、当該生成した入力用データを通信端末装置10に配信するようにすればよい。

[0170] [6. 3] 変形例3

また、上記実施形態においては、ユーザの入力すべき情報の一部を乱数表データ及び乱数表RMTに基づき、入力させる構成を採用したが、ユーザの入力すべき情報の全てを乱数表データ及び乱数表RMTにより入力させるようにしてもよい。

[0171] [6. 4] 変形例4

また、上記実施形態においては、口座番号の下2桁分に対応する全ての形象を含む入力用データを金融機関サーバ装置30から通信端末装置10に配信し、一度に2文字分の形象をユーザに選択させる構成を採用したが、一文字ずつ入力させるようにしてもよい。

[0172] この場合には、金融機関サーバ装置30は、一文字分の入力用データを通信端末装置10に配信するとともに、通信端末装置10は、当該入力用デー

タに基づき、選択された標識情報を金融機関サーバ装置 30 に送信する手順を繰り返して実行することにより、順次文字を特定していくようにすればよい。

[0173] [6. 5] 変形例 5

また、上記実施形態においては、オンラインストア等のサービスにおいては、クレジットカードを登録することがあるが、このクレジットカード登録に際して、本実施形態と同様に、入力用データと乱数表 RMT を用いることにより、クレジットカード番号やセキュリティコードが漏洩することを有効に防止し、クレジットカードの安全な利用を実現することができる。

[0174] [6. 6] 変形例 6

また、上記実施形態においては、金融機関サーバ装置 30 に、各 DB 331 ~ 334 を設け、管理する構成を採用したが、各 DB 331 ~ 334 は、各々、別個のコンピュータにより管理する構成を採用してもよい。

[0175] [6. 7] 変形例 7

また、上記実施形態においては、金融機関サーバ装置 30 を複数のコンピュータにより構成されるサーバシステムとして、構成してもよい。

[0176] [6. 8] 変形例 8

また、上記実施形態においては、金融機関毎に金融機関サーバ装置 30 を設け、異なる金融機関の金融機関サーバ装置 30 間で、入出金を行う例について説明したが、同一の金融機関内で入出金を行う場合には、金融機関サーバ装置 30 は、一台あれば、入出金を管理することができる。

[0177] [6. 9] 変形例 9

また、上記の実施形態においては、金融機関サーバ装置 30 は、上述の「0」～「9」の数字を有する乱数表 RMT において送金を含む決済処理を実行しているが、本変形例においては、例えば、ユーザが事前に登録済みの入金先に関する送信先情報（金融機関、支店入金先口座番号、名義人）を数字その他の入力対象文字に割り当て、当該送信先情報を取得する構成としてもよい。

[0178] この場合には、金融機関サーバ装置 30 は、ユーザが当該入力対象文字を形象を介して選択した場合に、ユーザの選択した入力対象文字に対応する送金先情報を一意に特定し、特定した送金先情報に基づいて決済処理を実行する。

[0179] なお、本実施形態の乱数表 RMT は、予めユーザに所定の定型文又は定型フォーマットを作成させておき、各数字に当該定型文等に対応付けておけば、ユーザの選択した形象から数字を特定し、更に、定型文等を特定することも可能である。

符号の説明

- [0180] 1 … ネットワークシステム
- 10 … 通信端末装置
- 110 … ネットワーク通信部
- 120 … 記憶部
- 121 … アプリケーション記憶部
- 122 … バッファ
- 130 … 表示制御部
- 140 … 表示部
- 150 … 操作部
- 160 … 端末管理制御部
- 170 … アプリケーション実行部
- 30 … 金融機関サーバ装置
- 310 … 通信制御部
- 320 … ROM／RAM
- 330 … 記録装置
- 331 … ユーザ管理DB
- 332 … 乱数表データ管理DB
- 333 … 金融機関管理DB
- 334 … 口座管理DB

- 3 4 0 ... サーバ管理制御部
- 3 5 0 ... データ処理部
- 3 5 1 ... 管理制御部
- 3 5 2 ... 形象抽出部
- 3 5 3 ... 入力用データ生成配信部
- 3 5 4 ... 特定処理部
- 3 5 5 ... 決済処理部

請求の範囲

- [請求項1] ネットワークを介して、通信接続される通信端末装置からデータを受信する受信手段と、
- 前記通信端末装置のユーザ毎に予め定められた表データであって、前記通信端末装置にて入力される入力対象文字と、当該入力対象文字の各々に対して予め割り当てられた形象と、を対応付けた表データが、前記ユーザを識別するための識別情報と対応付けて記録される記録手段を制御する制御手段と、
- 前記受信手段によって前記通信端末装置からユーザを指定した所与の要求が受信された場合に、当該ユーザに対応する表データを特定するデータ特定手段と、
- 前記特定された表データに基づき、前記ユーザによって特定すべき入力対象文字に対応する前記形象を抽出する抽出手段と、
- 前記抽出された形象の各々に対応付けられ、かつ、該当する通信端末装置にて該当する形象が表示される際に用いる標識情報を含む入力用データを生成し、当該生成した入力用データを前記通信端末装置に配信する配信手段と、
- 前記配信された入力用データに基づき前記通信端末装置にて前記形象が表示された際に、ユーザが入力した前記形象に対応する前記標識情報を当該通信端末装置から取得する取得手段と、
- 前記取得された標識情報に基づき、該当する前記形象を決定する決定手段と、
- 前記決定された形象に基づき、前記特定すべき入力対象文字を特定し、当該特定した入力対象文字に基づき、所与の処理を実行する処理手段と、
- を備えることを特徴とするサーバシステム。
- [請求項2] 請求項1に記載のサーバシステムであって、
- 前記処理手段が、

前記特定した入力対象文字に基づき、前記所与の処理を実行するために用いられる文字列を特定し、

前記特定した文字列に基づき、前記所与の処理を実行する、サーバシステム。

[請求項3] 請求項2に記載のサーバシステムであって、
前記抽出手段が、前記特定すべき入力対象文字以上の数の形象を抽出する、サーバシステム。

[請求項4] 請求項2又は3に記載のサーバシステムであって、
前記取得手段が、前記通信端末装置からユーザが直接入力した1以上の文字列を取得し、
前記処理手段が、前記特定した入力対象文字と、前記取得されたユーザが直接入力した文字列とを組み合わせることによって前記所与の処理を実行するために用いられる文字列を特定する、サーバシステム。

[請求項5] 請求項1～3のいずれか1項に記載のサーバシステムであって、
前記形象が、前記ユーザによって所定の情報を入力するために用いられる入力デバイスに基づくユーザの操作入力時に用いられる文字コードによって変換不能な形状を有する、サーバシステム。

[請求項6] 請求項5に記載のサーバシステムであって、
前記形象が、記号、図柄、絵柄及び画像の少なくとも一以上を示すものである、サーバシステム。

[請求項7] 請求項1～6のいずれか1項に記載のサーバシステムであって、
前記標識情報が、対応する前記形象が前記通信端末装置によって表示される際の位置を示す位置情報である、サーバシステム。

[請求項8] 請求項1～7のいずれか1項に記載のサーバシステムであって、
行と列とで定まる位置に複数の異なる形象がユーザによって視認可能に配列された表がユーザ毎に予め提供されており、
前記抽出手段が、前記表における特定の行又は列に配列された複数

の形象を抽出する、サーバシステム。

- [請求項9] 請求項1～8のいずれか1項に記載のサーバシステムであって、
前記抽出手段が、前記所与の処理毎又は前記決定すべき形象毎に、
前記入力用データを生成する際に抽出する行又は列を変化させ、前記
ユーザによって特定すべき入力対象文字に対応する前記形象を抽出す
る、サーバシステム。
- [請求項10] 請求項1～9のいずれか1項に記載のサーバシステムであって、
前記入力対象文字には、0～9の数字が含まれる、サーバシステム
。
- [請求項11] 請求項1～9のいずれか1項に記載のサーバシステムであって、
前記入力対象文字には、A～Zの英字が含まれる、サーバシステム
。
- [請求項12] 請求項1～11のいずれか1項に記載のサーバシステムであって、
前記処理手段が、前記特定した入力対象文字に基づいて、口座番号
、送金額、銀行番号、及び、銀行における支店番号の少なくとも一以
上の口座情報を特定し、特定した口座情報に基づいて、所与の処理と
して決済処理を実行する、サーバシステム。
- [請求項13] 請求項1～12のいずれか1項に記載のサーバシステムと、
前記サーバシステムにネットワークを介して通信接続される複数の
通信端末装置と、
を具備することを特徴とする通信システム。
- [請求項14] サーバシステムとして機能するコンピュータを、
ネットワークを介して通信接続される通信端末装置からデータを受
信する受信手段、
前記通信端末装置のユーザ毎に予め定められた表データであって、
前記通信端末装置にて入力される入力対象文字と、当該入力対象文字
の各々に対して予め割り当てられた形象と、を対応付けた表データが
、前記ユーザを識別するための識別情報と対応付けて記録される記録

手段を制御する制御手段、

前記受信手段によって前記通信端末装置からユーザを指定した所与の要求が受信された場合に、当該ユーザに対応する表データを特定するデータ特定手段、

前記特定された表データに基づき、前記ユーザによって特定すべき入力対象文字に対応する前記形象を抽出する抽出手段、

前記抽出された形象の各々に対応付けられ、かつ、該当する通信端末装置にて該当する形象が表示される際に用いる標識情報を含む入力用データを生成し、当該生成した入力用データを前記通信端末装置に配信する配信手段、

前記配信された入力用データに基づき前記通信端末装置にて前記形象が表示された際に、ユーザが入力した前記形象に対応する前記標識情報を当該通信端末装置から取得する取得手段、

前記取得された標識情報に基づき、該当する前記形象を決定する決定手段と、及び、

前記決定された形象に基づき、前記特定すべき入力対象文字を特定し、当該特定した入力対象文字に基づき、所与の処理を実行する処理手段、

として機能させることを特徴とするプログラム。

[請求項15]

各種の処理を実行するサーバシステムとネットワークを介して接続され、当該サーバシステムとデータの授受を行いつつ、ユーザに各種のサービスの提供をするための通信端末装置であって、

ユーザ毎に予め定められた表データであって、ユーザによって入力される入力対象文字と、当該入力対象文字の各々に対して予め割り当てられた形象と、を対応付けた表データの一部を、各形象を表示手段に表示する表示位置を少なくとも制御する制御情報とともに、前記サーバシステムから取得する取得手段と、

前記取得された表データに基づいて表示された画像に従って、ユー

ザの入力操作を受け付ける受付手段と、

前記入力操作に応じ、ユーザの指定した前記形象に対応する表示位置を特定する特定手段と、

前記特定された形象に対応する表示位置を示す情報を前記サーバシステムに送信する送信手段と、

を備えることを特徴とする通信端末装置。

[請求項16]

各種の処理を実行するサーバシステムとネットワークを介して接続され、当該サーバシステムとデータの授受を行いつつ、ユーザに各種のサービスの提供をするための通信端末装置を駆動するためのプログラムであって、

ユーザ毎に予め定められた表データであって、ユーザによって入力される入力対象文字と、当該入力対象文字の各々に対して予め割り当てられた形象と、を対応付けた表データの一部を、各形象を表示手段に表示する表示位置を少なくとも制御する制御情報とともに、前記サーバシステムから取得する取得手段、

前記取得された表データに基づいて表示された画像に従って、ユーザの入力操作を受け付ける受付手段、

前記入力操作に応じ、ユーザの指定した前記形象に対応する表示位置を特定する特定手段、及び、

前記特定された形象に対応する表示位置を示す情報を前記サーバシステムに送信する送信手段、

として機能させることを特徴とするプログラム。

[請求項17]

ユーザが通信端末装置を用いて、各種のサービスを提供するサーバシステムにアクセスする際に、当該ユーザが入力する入力対象文字を前記サーバシステムにて特定するための形象が視認可能に形成された記憶媒体であって、

一の行又は一の列に複数の異なる入力対象文字と、

前記入力対象文字毎に異なる複数の形象と、

が配置された複数の行及び複数の列により形成された表を有し、
各形象が、ユーザによって所定の情報を入力するために用いられる
入力デバイスに基づくユーザの操作入力時に用いられる文字コードに
よって変換不能な形状を有していることを特徴とする記録媒体。

[請求項18]

ネットワークを介して通信接続される通信端末装置からデータを受
信し、

前記通信端末装置のユーザ毎に予め定められた表データであって、
前記通信端末装置にて入力される入力対象文字と、当該入力対象文字
の各々に対して予め割り当てられた形象と、を対応付けた表データが
、前記ユーザを識別するための識別情報と対応付けて記録される記録
手段を制御し、

前記受信手段によって前記通信端末装置からユーザを指定した所与
の要求が受信された場合に、当該ユーザに対応する表データを特定す
るデータ特定手段、

前記特定された表データに基づき、前記ユーザによって特定すべき
入力対象文字に対応する前記形象を抽出し、

前記抽出された形象の各々に対応付けられ、かつ、該当する通信端
末装置にて該当する形象が表示される際に用いる標識情報を含む入力
用データを生成し、当該生成した入力用データを前記通信端末装置に
配信し、

前記配信された入力用データに基づき前記通信端末装置にて前記形
象が表示された際に、ユーザが入力した前記形象に対応する前記標識
情報を当該通信端末装置から取得し、

前記取得された標識情報に基づき、該当する前記形象を決定し、

前記決定された形象に基づき、前記特定すべき入力対象文字を特定
し、当該特定した入力対象文字に基づき、所与の処理を実行する、こ
とを特徴とする通信方法。