(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-15107
(P2016-15107A)
(43)公開日　平成28年1月28日(2016.1.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 20/40	(2012.01)	G06Q	20/40	100	5L055
G06Q 20/10	(2012.01)	G06Q	20/10	110	
G06F 21/36	(2013.01)	G06F	21/20	136	

審査請求 未請求　請求項の数 18　ＯＬ　（全 31 頁）

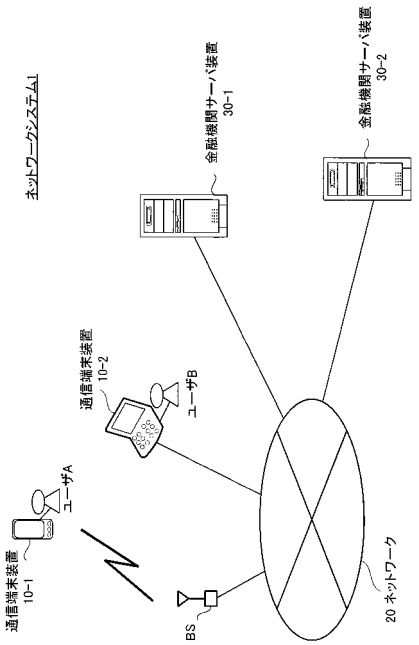
(21)出願番号　特願2014-177578 (P2014-177578)
(22)出願日　平成26年9月1日 (2014.9.1)
(31)優先権主張番号　特願2014-104705 (P2014-104705)
(32)優先日　平成26年5月1日 (2014.5.1)
(33)優先権主張国　日本国 (JP)
(31)優先権主張番号　特願2014-135075 (P2014-135075)
(32)優先日　平成26年6月12日 (2014.6.12)
(33)優先権主張国　日本国 (JP)

(71)出願人　514126430
バンクガード株式会社
東京都武蔵野市吉祥寺本町二丁目１５番１５－１０４号アルクス
(74)代理人　100134809
弁理士　庄司　亮
(72)発明者　藤井　治彦
東京都武蔵野市吉祥寺本町２－１５－１５
(72)発明者　松田　修一
千葉県柏市布施新町４丁目８－３

Ｆターム(参考)　5L055 AA25　AA73

(54)【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

(57)【要約】
【課題】インターネットバンクサービス等のサービス提供時におけるセキュリティーを向上させ、不正使用を防止するネットワークシステムなどを提供すること。
【解決手段】ユーザの入力すべき文字を当該文字とは無関係な写真等の形象と対応付けた乱数表ＲＭＴを予めユーザに発行するとともに、金融機関サーバ装置３０は、当該乱数表ＲＭＴに対応する乱数表データを管理し、情報入力時に乱数表データの一部を含む入力用データを通信端末装置１０に配信して、入力用データと乱数表ＲＭＴとを照らし合わせつつ、特定すべき情報の特定を実行する構成を有している。
【選択図】図１



【特許請求の範囲】
【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の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。

【発明の詳細な説明】
【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（ｗｏｒｌｄ　ｗｉｄｅ　ｗｅｂ）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ー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ーを向上させ、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。
【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、セキュリティー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。
【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。

【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、セキュリティー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、セキュリティー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。
【発明の効果】
【００２５】
本発明に係るサーバシステムなどは、セキュリティー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。
【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、特許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、セキュリティー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ー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ーを向上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的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ので、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、的確な生態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に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１０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サービス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ようになっている。

【００５６】

また、本実施形態のネットワークサービス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サービス１は、セキュリティー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」が一列に配置され、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（プラスティック製又は紙製）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、暗唱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こうせいしてもよい。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に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、通信制御部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１００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、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「○○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、ＪＰＥＧ（Ｊｏｉｎｔ　Ｐｈｏｔｏｇｒａｐｈｉｃ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）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、ＧＩＦ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ＲＭＴ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ＤＢ３３３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ＤＢ３３３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。

【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、記録された場合の例が示されている。

【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ＤＢ３３２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ＤＢ３３２を検索し、該当する乱数表データを乱数表データ管理ＤＢ３３２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行目及ぶ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Ｓａ３０３）。

【０１３８】

なお、ステップＳａ３０２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Ｓａ１０１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Ｓａ１０３）、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Ｓａ１０４）。

【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と（ステップＳａ１０５）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Ｓａ１０６）。

【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Ｓａ３１１）、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列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数桁分（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Ｓａ１１１）、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Ｓａ１１２）。

【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Ｓａ１１３）。

【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Ｓａ１１４）、当該入力口座情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Ｓａ１１５）。

【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Ｓａ１１３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Ｓａ３２１）、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Ｓａ３２２）。

【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て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Ｓａ３１０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Ｓａ３２３）。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Ｓａ３２４）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Ｓａ１２１）、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Ｓａ１２２）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Ｓａ１０４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。

【０１６３】

また、本実施形態のネットワークサービス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サービス１は、セキュリティー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。

【０１６５】

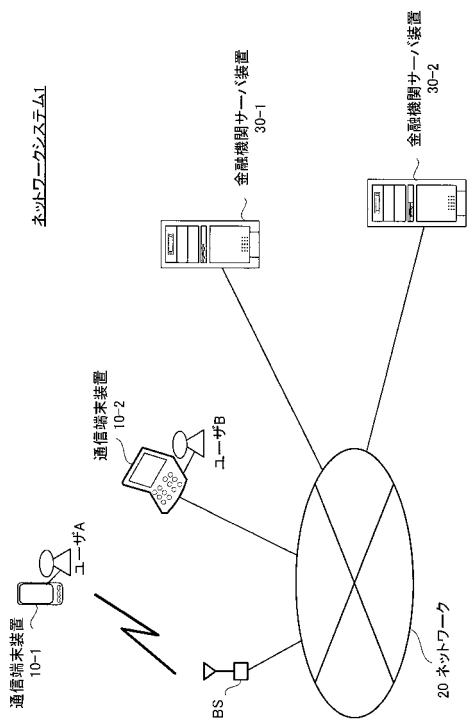
［６］変形例

［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が、
【０１６８】
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ー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ＤＢ３３１～３３４を設け、管理する構成を採用したが、各ＤＢ３３１～３３４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。

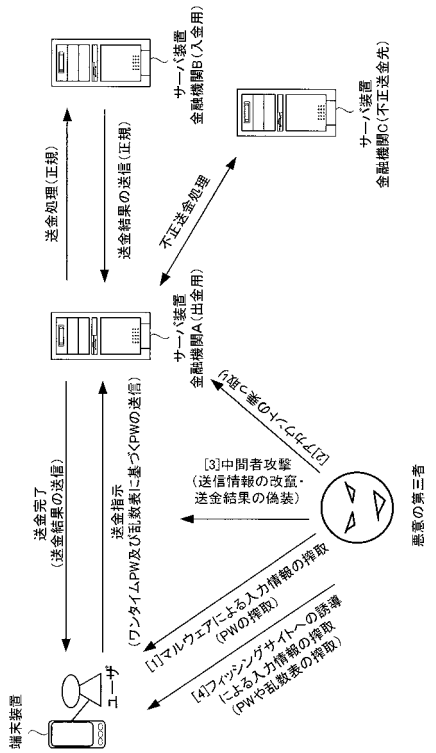
【０１７５】
［６．７］変形例７
また、上記実施形態においては、金融機関サーバ装置３０を複数のコンピュータにより構成されるサーバシステムとして、構成してもよい。
【０１７６】
［６．８］変形例８
また、上記実施形態においては、金融機関毎に金融機関サーバ装置３０を設け、異なる金融機関の金融機関サーバ装置３０間で、入出金を行う例について説明したが、同一の金融機関内で入出金を行う場合には、金融機関サーバ装置３０は、一台あれば、入出金を管理することができる。
【０１７７】
［６．９］変形例９
また、上記の実施形態においては、金融機関サーバ装置３０は、上述の「０」～「９」の数字を有する乱数表ＲＭＴにおい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を対応付けておけば、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
３４０　…　サーバ管理制御部
３５０　…　データ処理部
３５１　…　管理制御部
３５２　…　形象抽出部

３５３　…　入力用データ生成配信部
３５４　…　特定処理部
３５５　…　決済処理部

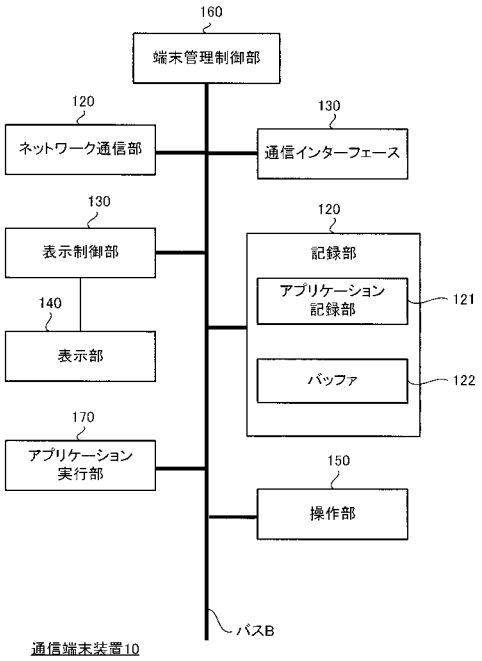
【図１】



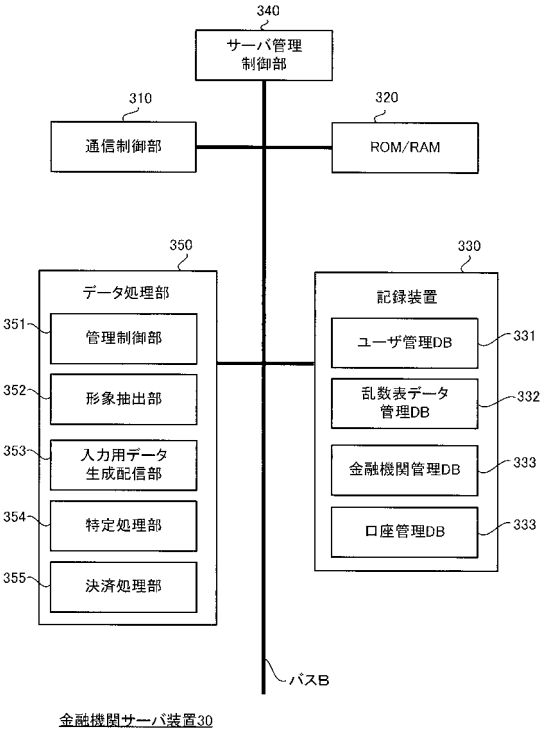
【図２】



【図４】



【図５】



【図６】

ユーザID	ユーザ属性情報			
	氏名	住所	アカウント名	第1暗証
user001	○○太郎	東京都北区***	235i1000	****
user002	△花子	大阪市北区***	222222	*****
user003	×△四朗	大阪市中央区***	333333	****
…	…	…	…	…

【図７】

ユーザID	乱数表データ
user001	DATA001
user002	DATA002
user003	DATA003
user004	DATA002
⋮	⋮

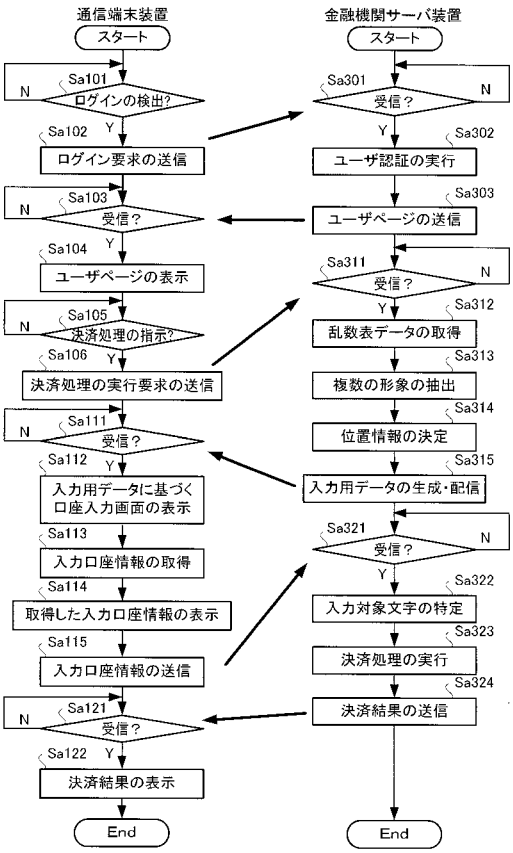
【図８】

金融機関コード	金融機関名	支店名	支店コード	支店住所
B101	大江戸銀行	新宿支店	456	東京都新宿区***
		渋谷支店	321	東京都渋谷区***
		日本橋本店	1	東京都中央区***
B102	△△銀行	名古屋本店	1	愛知県名古屋市***
		静岡支店	110	静岡県静岡市***
B200	○○信用金庫	仙台本店	1	宮城県仙台市***
		盛岡支店	3	岩手県盛岡市***
：	：	：	：	：

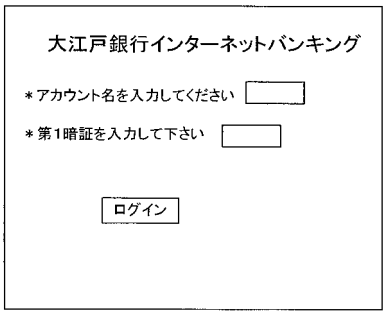
【図９】

口座情報						
ユーザID	口座番号	銀行名	支店名	口座残高	登録済みの振込先
user001	1234567	大江戸銀行	新宿支店	￥*******	大江戸銀行日本橋本店****
					△銀行渋谷支店****
user002	2345678	△△銀行	名古屋本店	￥*****	大江戸銀行新宿支店****
					△△銀行静岡支店****
user003	3456789	○○銀行	日本橋本店	￥*****	大江戸銀行渋谷支店****
					△銀行日本橋支店****
：	：	：	：	：	：

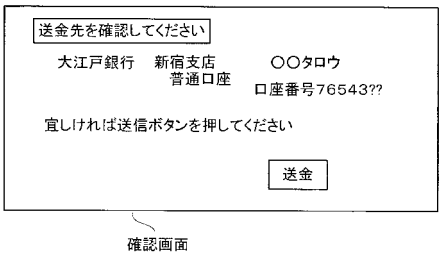
【図１０】



【図１１】



【図１３】


送金先を確認してください
大江戸銀行　新宿支店
普通口座
○○タロウ
口座番号76543??
宜しければ送信ボタンを押してください
送金

確認画面

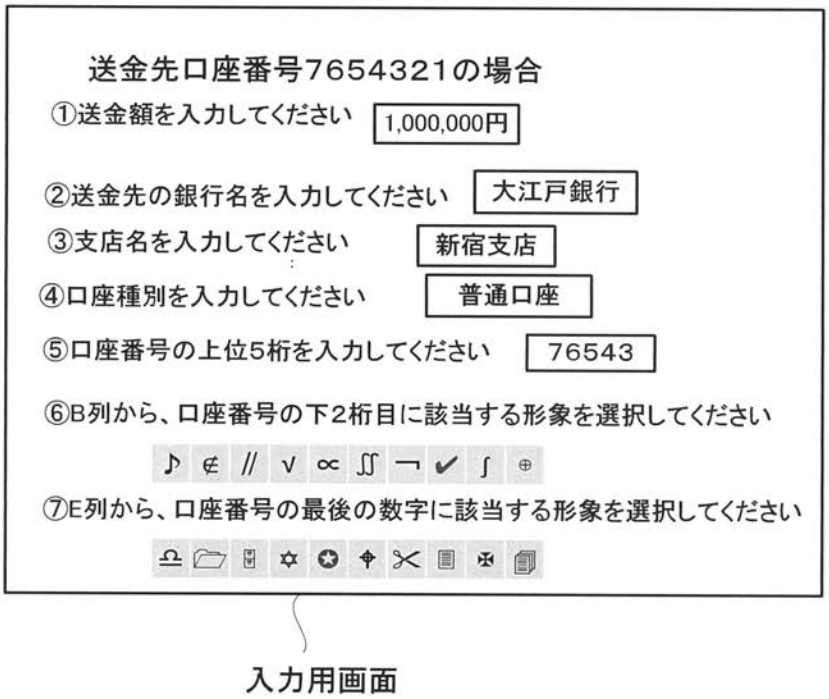
【図３】


【キャッシュカードの裏面】
大江戸銀行　送金先口座番号指定用乱数表
※コピーや写真撮影をしないでください。銀行等がこれらを要求することはありません
1 2 3 4 5 6 7 8 9 0
A
B
C
D
E
（資料作成の便宜上、特殊文字フォントを利用していますが、本来は特殊文字フォントにない画像を利用します）
乱数表RMT

【図１２】


【キャッシュカードの裏面】
大江戸銀行　送金先口座番号指定用乱数表
※コピーや写真撮影をしないでください。銀行等がこれらを要求することはありません
1 2 3 4 5 6 7 8 9 0
A
B
C
D
E
（資料作成の便宜上、特殊文字フォントを利用していますが、本来は特殊文字フォントにない画像を利用します）
乱数表RMT

(A)


送金先口座番号7654321の場合
①送金額を入力してください
1,000,000円
②送金先の銀行名を入力してください
大江戸銀行
③支店名を入力してください
新宿支店
④口座種別を入力してください
普通口座
⑤口座番号の上位5桁を入力してください
76543
⑥B列から、口座番号の下2桁目に該当する形象を選択してください
⑦E列から、口座番号の最後の数字に該当する形象を選択してください
入力用画面

(B)