(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2005-84822
(P2005-84822A)
(43)公開日　平成17年3月31日(2005.3.31)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/60	G06F 17/60	222	5B085
G06F 15/00	G06F 17/60	224	5J104
H04L 9/32	G06F 17/60	232	
	G06F 17/60	416	
	G06F 15/00	330A	

審査請求 未請求　請求項の数 5　OL　（全 14 頁）　最終頁に続く

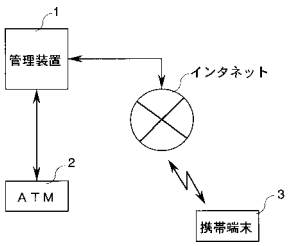
(21)出願番号　特願2003-314420(P2003-314420)
(22)出願日　平成15年9月5日(2003.9.5)

(71)出願人　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町８０１番地
(74)代理人　100084548
弁理士　小森　久夫
(74)代理人　100123940
弁理士　村上　辰一
(72)発明者　野地　英昭
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内

Fターム(参考)　5B085 AA08 AE00 AE02 AE03
5J104 KA01 NA05 PA10

(54)【発明の名称】不正利用通知方法、および不正利用通知プログラム

(57)【要約】
【課題】　正当な利用者が不正利用者の存在を認識したときに、利用停止にかかる手続が迅速に行え、不正利用者による不正利用を十分に防止できる不正利用通知方法を提供する
【解決手段】　管理装置１は、誤ったパスワードが入力された回数が予め設定されている所定回数以上になると、正当な利用者にその旨を電子メールで通知する。この電子メールは、利用停止にかかる要求を受け付けるページをリンクさせたリンクメッセージである。このため、正当な利用者は、不正利用者の存在を認識したとき、簡単且つ迅速に利用停止にかかる要求を受け付けるページにアクセスし、自己の口座を利用停止にできる。したがって、不正利用者の存在を認識した正当な利用者が、利用停止にかかる手続を迅速に行うことができ、不正利用者による不正利用を十分に防止できる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
他の機器から送られてきた、利用者を識別する利用者識別情報、およびパスワードを含む認証要求を受け付ける第１のステップと、
上記第１のステップで受け付けた認証要求に含まれている利用者識別情報をキーにして、利用者毎に利用者識別情報、パスワード、および電子メールアドレスを関連づけて登録した利用者データベースを検索し、この利用者データベースに登録されている該当する利用者のパスワードを取得する第２のステップと、
上記第１のステップで受け付けた認証要求に含まれているパスワードと、上記第２のステップで取得したパスワードと、が一致しているかどうかを判定する第３のステップと、
上記第３のステップの判定結果を、上記第１のステップで受け付けた認証要求を送ってきた機器へ通知する第４のステップと、
上記第３のステップが、２つのパスワードが不一致であると判定した場合、上記データベースから該当する利用者の電子メールアドレスを取得する第５のステップと、
上記第５のステップで取得した電子メールアドレスを宛て先にし、誤ったパスワードで認証要求があったことを通知する電子メールを送信する第６のステップと、を備えた不正利用通知方法であって、
上記第６のステップが送信する電子メールは、利用停止の要求を受け付けるページをリンクさせたリンクメッセージであり、
上記第６のステップが送信した電子メールにリンクさせたページで利用停止の要求を受け付けたとき、該当する利用者について利用停止を上記データベースに登録する第７のステップを備えた不正利用通知方法。
【請求項２】
上記第６のステップは、上記第３のステップで２つのパスワードが不一致であると判定された利用者が、すでに利用停止が登録されている利用者であれば、上記電子メールの送信を中止する請求項１に記載の不正利用通知方法。
【請求項３】
上記第６のステップが電子メールを送信してから所定時間経過後に、この電子メールにリンクさせたページで利用停止の要求を受け付けたとき、この要求を無効とする第８のステップを備えた請求項１または２に記載の不正利用通知方法。
【請求項４】
上記第６のステップが送信する電子メールは、さらにパスワードの変更要求を受け付けるページをリンクさせたリンクメッセージであり、
この電子メールにリンクさせたページでパスワードの変更要求を受け付けたとき、上記データベースに登録されているパスワードを、この変更要求で指示されたパスワードに変更する第９のステップを備えた請求項１～３のいずれかに記載の不正利用通知方法。
【請求項５】
他の機器から送られてきた、利用者を識別する利用者識別情報、およびパスワードを含む認証要求を受け付ける第１のステップと、
上記第１のステップで受け付けた認証要求に含まれている利用者識別情報をキーにして、利用者毎に利用者識別情報、パスワード、および電子メールアドレスを関連づけて登録した利用者データベースを検索し、この利用者データベースに登録されている該当する利用者のパスワードを取得する第２のステップと、
上記第１のステップで受け付けた認証要求に含まれているパスワードと、上記第２のステップで取得したパスワードと、が一致しているかどうかを判定する第３のステップと、
上記第３のステップの判定結果を、上記第１のステップで受け付けた認証要求を送ってきた機器へ通知する第４のステップと、
上記第３のステップが、２つのパスワードが不一致であると判定した場合、上記データベースから該当する利用者の電子メールアドレスを取得する第５のステップと、
上記第５のステップで取得した電子メールアドレスを宛て先にし、誤ったパスワードで

認証要求があったことを通知する電子メールを送信する第６のステップと、をコンピュータに実行させる不正利用通知プログラムであって、
上記第６のステップが送信する電子メールは、利用停止の要求を受け付けるページをリンクさせたリンクメッセージであり、
さらに、上記第６のステップが送信した電子メールにリンクさせたページで利用停止の要求を受け付けたとき、該当する利用者について利用停止を上記データベースに登録する第７のステップをコンピュータに実行させる不正利用通知プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、正当な利用者に成りすました不正利用が行われている可能性が高いときに、この正当な利用者に対して不正利用が行われていることを通知する不正利用通知方法、および不正利用通知プログラムに関する。
【背景技術】
【０００２】
従来、正当な利用者に成りすました不正利用を防止するために、利用者にＩＤとパスワードを入力させ、利用者の認証を行っている。例えば、銀行に設置されているＡＴＭでは、口座番号を利用者のＩＤとし、出金時に利用者にパスワード（所謂、暗証番号）を入力させ、正当な利用者であるかどうか認証している。ＩＤ（口座番号）は、本体に投入されたキャッシュカードから読み出される。また、インタネットを利用した業務アプリケーションシステムや、ネットワークバンキングシステム等のシステムにおいても、アクセス時にＩＤとパスワードを入力させ、アクセスを要求している利用者が正当な利用者であるかどうかの認証を行っている。
【０００３】
そして、存在しないＩＤや誤ったパスワードが入力され、正当な利用者であると認証できなかった場合に、今回の利用が正当な利用者に成りすました不正利用者による不正利用の可能性が高いと判断し、該当する正当な利用者や、システムの管理者等に、その旨（誤ったパスワードが入力されたこと）を電子メールで通知することが特許文献１～４で提案されている。これらの特許文献１～４は、不正利用者が存在する可能性が高いことを、正当な利用者やシステムの管理者に電子メールで通知することにより、正当な利用者に成りすました不正利用者による不正利用に対する注意を促し、不正利用者による不正利用を抑えている。また、出金取引や入金取引が行われ、口座残高が変化したときに、その預金口座の所有者である正当な利用者にその旨（口座残高が変化したこと）を電子メールで通知することが特許文献５で提案されている。
【特許文献１】特開２００１－１７５６００号公報
【特許文献２】特開２００１－３５０７２３号公報
【特許文献３】特開２００１－３１９０５９号公報
【特許文献４】特開２００２－２６９６１９号公報
【特許文献５】特開２００３－　９１６４３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、正当な利用者が、送信されてきた電子メールにより不正利用者の存在を認識しても、自己のユーザＩＤによるシステムの利用を停止しなければ、不正利用者による不正利用を防止できない。一方、特許文献１～５では、不正利用者が存在する可能性が高いことを、正当な利用者やシステムの管理者に通知しているだけであった。このため、正当な利用者が不正利用者の存在を認識しても、自己のユーザＩＤによるシステムの利用停止にかかる手続を迅速に行うことができず、不正利用者による不正利用を十分に防止できていなかった。
【０００５】

この発明の目的は、正当な利用者が不正利用者の存在を認識したときに、利用停止にかかる手続を迅速に行うことができ、不正利用者による不正利用を十分に防止できる不正利用通知方法、および不正利用通知プログラムを提供することにある。

【課題を解決するための手段】

【０００６】

この発明にかかる不正利用通知方法は、上記課題を解決するために以下の構成を備えている。

【０００７】

（１）他の機器から送られてきた、利用者を識別する利用者識別情報、およびパスワードを含む認証要求を受け付ける第１のステップと、

上記第１のステップで受け付けた認証要求に含まれている利用者識別情報をキーにして、利用者毎に利用者識別情報、パスワード、および電子メールアドレスを関連づけて登録した利用者データベースを検索し、この利用者データベースに登録されている該当する利用者のパスワードを取得する第２のステップと、

上記第１のステップで受け付けた認証要求に含まれているパスワードと、上記第２のステップで取得したパスワードと、が一致しているかどうかを判定する第３のステップと、

上記第３のステップの判定結果を、上記第１のステップで受け付けた認証要求を送ってきた機器へ通知する第４のステップと、

上記第３のステップが、２つのパスワードが不一致であると判定した場合、上記データベースから該当する利用者の電子メールアドレスを取得する第５のステップと、

上記第５のステップで取得した電子メールアドレスを宛て先にし、誤ったパスワードで認証要求があったことを通知する電子メールを送信する第６のステップと、を備えた不正利用通知方法であって、

上記第６のステップが送信する電子メールは、利用停止の要求を受け付けるページをリンクさせたリンクメッセージであり、

上記第６のステップが送信した電子メールにリンクさせたページで利用停止の要求を受け付けたとき、該当する利用者について利用停止を上記データベースに登録する第７のステップを備えている。

【０００８】

この構成では、誤ったパスワードが入力されたことにより、成りすましによる不正利用者が存在している可能性が高いと判断したときに、正当な利用者に対して誤ったパスワードが入力されたことを電子メールで通知する。この電子メールは、利用停止の要求を受け付けるページをリンクさせたリンクメッセージである。このため、この電子メールを受け取った正当な利用者は、不正利用者の存在を認識したとき、この電子メールにリンクされているページに簡単にアクセスすることができ、利用停止の手続が迅速に行える。

【０００９】

すなわち、不正利用者の存在を認識した正当な利用者が、利用停止にかかる手続を迅速に行うことができ、不正利用者による不正利用を十分に防止できる。

【００１０】

（２）上記第６のステップは、上記第３のステップで２つのパスワードが不一致であると判定された利用者が、すでに利用停止が登録されている利用者であれば、上記電子メールの送信を中止する。

【００１１】

多くの場合、利用停止が登録されている利用者は、先に送信されてきた電子メールにより、すでに不正利用者の存在を認識しているので、このような利用者に誤ったパスワードが入力されたことを通知する電子メールを何度も送信することは、この電子メールを受け取る利用者にとって迷惑な行為であり、利用者を不快にさせ、利用者に対するサービスを低下させてしまう。この構成では、利用停止が登録されている利用者に、誤ったパスワードが入力されたことを通知する電子メールを送信しないので、利用者を不快にさせることがなく、利用者に対するサービスを低下させることがない。

【００１２】
（３）上記第６のステップが電子メールを送信してから所定時間経過後に、この電子メールにリンクさせたページで利用停止の要求を受け付けたとき、この要求を無効とする第８のステップを備えている。
【００１３】
この構成では、送信してから所定時間、例えば２～３日、経過後に、この電子メールにリンクさせたページで利用停止の要求を受け付けた場合、この利用停止にかかる要求を無効とする。このため、以前に送信されてきていた電子メールを、最近送信されてきた電子メールであると勘違いした利用者が利用停止の手続を行ったときに、この利用停止の手続が無効にされる。したがって、利用者の勘違いで利用停止が登録されるのを防止でき、利用者に対するサービスの向上が図れる。
【００１４】
（４）上記第６のステップが送信する電子メールは、さらにパスワードの変更要求を受け付けるページをリンクさせたリンクメッセージであり、
この電子メールにリンクさせたページでパスワードの変更要求を受け付けたとき、上記データベースに登録されているパスワードを、この変更要求で指示されたパスワードに変更する第９のステップを備えている。
【００１５】
この構成では、誤ったパスワードが入力されたことを通知する電子メールに、パスワードの変更にかかる要求を行うページもリンクさせたので、利用を停止すると自己の不都合が大きい利用者に、不正利用を防止するためにパスワードを変更するという選択を行わせることができ、またこのパスワードの変更にかかる操作を簡単に行わせることができる。
【発明の効果】
【００１６】
この発明によれば、不正利用者の存在を認識した正当な利用者が、利用停止にかかる手続を迅速に行うことができ、不正利用者による不正利用を十分に防止できる。
【発明を実施するための最良の形態】
【００１７】
図１は、この発明にかかる不正利用通知方法を適用した取引処理システムの構成を示す図である。図１において、１は各利用者の口座を管理する管理装置であり、２は銀行等の金融機関の店舗に設置されたＡＴＭ（現金自動預け払い機）であり、３は利用者が所有し、電子メールを受信する機能を有する携帯電話等の携帯端末である。管理装置１とＡＴＭ２とは、専用回線で接続されており、両装置間でデータ通信可能に構成されている。管理装置１には、この発明にかかる不正利用通知方法が適用されている。ＡＴＭ２は、公知の構成であり、利用者との間で入金取引、出金取引等の取引処理を実行する。管理装置１は、携帯端末３等に電子メールを送信する機能を有し、またインタネット上で口座の利用停止にかかる要求を受け付けるページや、パスワードの変更にかかる要求を受け付けるページを公開している。また、携帯端末３は、インタネットに接続することもでき、上記管理装置１がインタネット上で公開しているページにアクセスできる。
【００１８】
なお、図１では管理装置１に接続されているＡＴＭ２を１台だけ示しているが、実際には多数のＡＴＭ２が接続されている。
【００１９】
図２は、管理装置の構成を示すブロック図である。管理装置１は、本体の動作を制御する制御部１１と、専用回線を介して接続されているＡＴＭ２とのデータ通信を行う第１の通信部１２と、インタネットを介して携帯端末３に電子メールを送信したり、インタネット上で公開しているページにアクセスした利用者が入力した要求を受信する第２の通信部１３と、口座毎に、利用者の氏名、口座番号、現在の口座残高、これまでの取引履歴等を記憶した取引データベース１４と、利用者を管理するための利用者管理データベース１５と、を備えている。利用者管理データベース１５には、図３に示すように利用者毎に利用

者識別番号（ここでは口座番号）、暗証番号、電子メールのアドレス、誤った暗証番号が入力された回数、誤った暗証番号が入力された日時とその時に利用されたＡＴＭの識別番号（１回目～４回目まで）、利用停止の登録の有無、および利用者に送信した電子メールの識別番号を関連づけて記憶している。

【００２０】

なお、取引データベース１４と、利用者管理データベース１５と、は１つのデータベースで構築してもよい。

【００２１】

以下、この実施形態の取引処理システムの動作について説明する。

【００２２】

まず、ＡＴＭ２における取引処理について説明する。図４は、ＡＴＭの出金取引にかかる処理を示すフローチャートである。ＡＴＭ２は、利用者が本体に投入したカード、所謂キャッシュカード、から口座番号（この発明で言う利用者識別情報に相当する。）を読み出すとともに、利用者による暗証番号の入力を受け付ける（ｓ１、ｓ２）。また、ｓ１では、利用者が通帳を挿入した場合、この通帳も受け付ける。また、ＡＴＭ２は出金金額の入力を受け付ける（ｓ３）。ＡＴＭ２は、ｓ１でカードから読み取った口座番号、ｓ２で受け付けた暗証番号、およびｓ３で受け付けた出金金額を含む、取引認証要求を専用回線を介して管理装置１に送信し（ｓ４）、管理装置１から今回の取引認証要求に対する認証結果が送信されてくるのを待つ（ｓ５）。

【００２３】

管理装置１は、ＡＴＭ２から送られてきた取引認証要求に対して取引の可否を判定し、その結果を認証結果としてＡＴＭ２に送信する。管理装置１における認証処理の詳細については後述する。

【００２４】

ＡＴＭ２は、管理装置１からの認証結果が取引可であれば出金処理を行い（ｓ６、ｓ７）、反対に認証結果が取引不可であれば取引中止処理を行う（ｓ６、ｓ８）。そして、ＡＴＭ２はｓ１で受け付けたカードを返却し（ｓ９）、本処理を終了する。また、ＡＴＭ２は、通帳を受け付けていればｓ９で通帳に取引内容を印字して返却し、通帳を受け付けていないければｓ９で取引内容を印字した取引伝票を発行する。

【００２５】

なお、ここでは出金処理について説明したが、ＡＴＭ２は公知のＡＴＭと同様に入金処理、振込処理、残高照会等の他の取引についても処理できる。

【００２６】

次に、管理装置１の動作について説明する。図５は、管理装置の動作を示すフローチャートである。管理装置１は、ＡＴＭ２から取引認証要求が送られてくると（ｓ１１）、この取引についての認証処理を行う（ｓ１２）。また、インタネット上で公開している、口座の利用停止にかかる要求を受け付けるページにおいて利用停止にかかるアクセスがあると（ｓ１３）、利用停止処理を行い（ｓ１４）、さらにパスワードの変更にかかる要求を受け付けるページにおいてパスワードの変更にかかるアクセスがあると（ｓ１５）、パスワード変更処理を行う（ｓ１６）。

【００２７】

まず、ｓ１２にかかる取引の認証処理について説明する。図６は、取引の認証処理を示すフローチャートである。管理装置１は、今回送信されてきた取引認証要求に含まれている口座番号をキーにして、利用者管理データベース１５を検索し、この口座番号に対応する暗証番号を読み出す（ｓ２１）。そして、ｓ２１で読み出した暗証番号と、今回送信されてきた取引認証要求に含まれている暗証番号と、が一致しているかどうかを判定する（ｓ２２）。管理装置１は、ｓ２２で２つの暗証番号が一致していると判定すると、この口座について利用停止が登録されているかどうかを判定する（ｓ２３）。上述したように、利用者管理データベース１５に口座毎に利用停止の有無が登録されている。また、利用停止の登録にかかる処理については後述する。

【００２８】
管理装置１は、ｓ２３で利用停止が登録されていないと判定すると（利用が停止されていない口座であると判定すると）、今回送信されてきた取引認証要求に含まれている出金額等の取引データを基に、取引の可否を判定する（ｓ２４）。ｓ２４では、例えば今回の取引が出金取引である場合、現在の口座残高が出金金額以上であるかどうかを判定し、出金金額以上であれば取引可と判定し、出金金額未満であれば取引不可と判定する。そして、管理装置１は、今回取引の認証要求を送信してきたＡＴＭ２に対して、ｓ２４における判定結果を認証結果として送信する（ｓ２５）。また、今回取引が行われた口座について、誤った暗証番号が入力された回数を「０」にリセットし、且つ誤った暗証番号が入力された日時および使用されたＡＴＭ２の識別番号を削除する、利用者管理データベース１５の更新を行う（ｓ２６）。

【００２９】
利用者管理データベース１５で管理している、誤った暗証番号が入力された回数は、上記の説明から明らかなように、誤った暗証番号が入力された連続回数であり、正当な利用者が暗証番号を誤って入力しても、次に正しい暗証番号を入力することにより、「０」に戻る。

【００３０】
また、管理装置１は、ｓ２５でＡＴＭ２に対して取引可を送信しているときには、取引データベース１４で管理している口座残高や取引履歴を、今回の取引の内容に基づいて更新する（ｓ２７）。

【００３１】
管理装置１は、ｓ２３で利用停止が登録されていると判定すると、認証結果として取引不可をＡＴＭ２に送信するとともに（ｓ２８）、利用者管理データベース１５で管理している誤った暗証番号が入力された日時および使用されたＡＴＭ２の識別番号の欄に、現在の日時、および今回取引認証要求を送信してきたＡＴＭ２の識別番号を追加する（ｓ２９）。ここでは、入力された暗証番号は適正であったが、正当な利用者が既に利用停止の登録を行っていることから、不正利用者による利用である可能性が高いと判断し、ｓ２９にかかる処理を行うようにしている。この情報は、この不正利用者の追跡に利用できる。また、この場合には、誤った暗証番号の回数を「０」にしないが、正当な利用者が利用停止を登録していることから、何らの問題も生じない。

【００３２】
また、管理装置１は、ｓ２２で２つの暗証番号が一致していないと判定すると、認証結果として取引不可をＡＴＭ２に送信するとともに（ｓ３０）、利用者管理データベース１５で管理している誤った暗証番号が入力された回数を１カウントアップするとともに（ｓ３１）、誤った暗証番号が入力された日時および使用されたＡＴＭ２の識別番号の欄に、現在の日時、および今回取引認証要求を送信してきたＡＴＭ２の識別番号を追加する（ｓ３２）。そして、利用者管理データベース１５で管理している誤った暗証番号が入力された回数が、予め設定されている所定回数、例えば３回、以上であるかどうかを判定し（ｓ３３）、所定回数未満であれば本処理を終了する。

【００３３】
これにより、正当な利用者が、たまたま暗証番号を誤った入力した場合に、正当な利用者に対して以下に示すｓ３４以降の処理が行われることがなく、正当な利用者を不快にさせる等、利用者に対するサービスの低下を招くことがない。

【００３４】
管理装置１は、ｓ３３で誤った暗証番号が入力された回数が所定回数以上であると判定すると、既に利用停止が登録されている口座であるかどうかを判定する（ｓ３４）。ｓ３４で利用停止が登録されていない口座であると判定すると、利用者管理データベース１５から該当する口座の正当な利用者のメールアドレスを読み出し（ｓ３５）、ｓ３５で読み出したメールアドレスを宛て先にして、口座の利用停止にかかる要求を受け付けるページ、およびパスワードの変更にかかる要求を受け付けるページをリンク付けしたリンクメッ

セージを電子メールで送信する（ｓ３６）。管理装置１は、ｓ３６で送信した電子メールに識別番号（電子メール識別番号）を付けており、この電子メール識別番号を利用者管理データベース１５に登録し（ｓ３７）、本処理を終了する。

【００３５】

管理装置１がｓ３６で送信した電子メールは、インタネットを介して正当な利用者の携帯端末３に送信される。管理装置１が送信したリンクメッセージを受信した携帯端末３における、このリンクメッセージの表示例を図７に示す。この電子メールには、誤った暗証番号が入力された日時や、そのときに使用されたＡＴＭ２の識別番号が含まれている。正当な利用者は、この電子メールを確認することにより、不正利用者の存在を認識できる。具体的には、正当な利用者は、自分自身が誤った暗証番号を入力していた場合、自分自信の誤操作であって、不正利用者については存在していないと判断し、自分自身が誤った暗証番号を入力していない場合、不正利用者が存在していることを認識する。

【００３６】

なお、ここでは誤った暗証番号が入力されたときに使用されたＡＴＭ２の識別番号を利用者管理データベース１５に記憶させたり、電子メールで正当な利用者に通知するとしたが、ＡＴＭ２の識別番号にかえて、このＡＴＭ２が設置されている店舗名（支店名）等にしてもよい。

【００３７】

利用者は、この電子メールに、口座の利用停止にかかる要求を受け付けるページ、およびパスワードの変更にかかる要求を受け付けるページがリンク付けされているので、これらのページに簡単にアクセスすることができ、口座の利用停止や、パスワードの変更にかｋる操作を簡単且つ迅速に行える。

【００３８】

また、管理装置１は、ｓ３４で既に利用停止が登録されている口座であると判定すると、ｓ３５以降の処理を行うことなく、本処理を終了する。既に利用停止の登録を行っている利用者は、以前に送られてきた電子メールにより不正利用者の存在を認識しているので、ｓ３６で電子メールを送信し、正当な利用者に不正利用者の存在を認識させなくても何ら問題は生じない。一方、不正利用者の存在を認識している利用者にとっては、不正利用者が存在を認識させるための電子メールが何度も送信されてくることは迷惑であり、不快である。この取引処理システムでは、ｓ３４で既に利用停止中であるかを判定し、利用停止中であれば、ｓ３６で電子メールの送信を行わないので、利用者を不快にさせることがなく、利用者に対するサービスの低下を防止できる。

【００３９】

次に、ｓ１４にかかる利用停止処理について説明する。図８は、利用停止処理を示すフローチャートである。利用者は、不正利用者の存在を認識し、口座の利用を停止する場合、管理装置１が上記ｓ３６で送信してきた電子メールに、口座の利用停止にかかる要求を受け付けるページがリンク付けされているので、このページに簡単にアクセスすることができる。図９は、口座の利用停止にかかる要求を受け付けるページにアクセスした携帯端末の画面例を示す図である。利用者は、携帯端末３において、口座番号、暗証番号、および電子メール識別番号を入力し、送信する。

【００４０】

なお、携帯端末３で口座の利用停止にかかる要求を受け付けるページにアクセスしたときに、口座番号、および電子メール識別番号については自動的に入力されるようにしてもよいが、暗証番号については今回の口座の利用停止にかかる操作を行う者を認証するために、利用者本人に入力させる。

【００４１】

管理装置１は、口座の利用停止にかかる要求を受け付けるページで、口座番号、暗証番号、電子メール識別番号を受け付けると、今回受け付けた口座番号をキーにして、利用者管理データベース１５を検索し、この口座番号に対応する暗証番号を読み出す（ｓ４１）。そして、ｓ４１で読み出した暗証番号と、今回受け付けた暗証番号と、が一致している

かどうかを判定する（ｓ４２）。管理装置１は、ｓ４２で２つの暗証番号が一致していると判定すると、今回受け付けた電子メール識別番号で識別される電子メールが送信してから所定時間以上、例えば２日（４８時間）以上、経過しているかどうかを判定する（ｓ４３）。ｓ４３で、所定期間以上経過していないと判定すると、利用者管理データベース１５に対して今回受け付けた口座番号の口座について利用停止を登録し（ｓ４４）、利用者の携帯端末３に利用停止の登録完了を通知して本処理を終了する（ｓ４５）。

【００４２】

また、管理装置１は、ｓ４２で２つの暗証番号が一致していないと判定すると、利用者の携帯端末３に暗証番号の不一致を通知し（ｓ４６）、本処理を終了する。これにより、正当な利用者の口座が、他人に勝手に利用停止にされるのを防止できる。

【００４３】

さらに、管理装置１は、ｓ４３で電子メールの送信から所定時間以上経過していると判定すると、利用者管理データベース１５に対して今回受け付けた口座番号の口座の利用停止を登録することなく、利用者に対して以前に送信した電子メールを、最近送信されてきた電子メールであると勘違いしていないかどうかの確認メッセージを送信し（ｓ４７）、本処理を終了する。これにより、利用者が以前に送信されていた電子メールを、最近送信されてきた電子メールであると勘違いして、口座を利用停止にするのを防止でき、利用者に対するサービスの向上が図れる。

【００４４】

なお、ｓ４７で通知したメッセージで利用者に確認の入力を要求し、利用者が勘違いしていない旨の入力を行ったときに、上記ｓ４４、ｓ４５にかかる処理を行うようにしてもよい。

【００４５】

次に、ｓ１６にかかるパスワード変更処理について説明する。図１０は、パスワード変更処理を示すフローチャートである。利用者は、不正利用者の存在を認識し、パスワードを変更する場合、管理装置１が上記ｓ３６で送信してきた電子メールに、パスワードの変更にかかる要求を受け付けるページがリンク付けされているので、このページに簡単にアクセスすることができる。図１１は、パスワードの変更にかかる要求を受け付けるページにアクセスした携帯端末の画面例を示す図である。利用者は、携帯端末３において、口座番号、現在の暗証番号、変更する暗証番号、および電子メール識別番号を入力し、送信する。

【００４６】

なお、携帯端末３でパスワードの変更にかかる要求を受け付けるページにアクセスしたときに、口座番号、および電子メール識別番号については自動的に入力されるようにしてもよいが、現在の暗証番号、および変更する暗証番号については今回のパスワードの変更にかかる操作を行う者を認証するために、利用者本人に入力させる。

【００４７】

管理装置１は、パスワードの変更にかかる要求を受け付けるページで、口座番号、現在の暗証番号、変更する暗証番号、および電子メール識別番号を受け付けると、今回受け付けた口座番号をキーにして、利用者管理データベース１５を検索し、この口座番号に対応する暗証番号を読み出す（ｓ５１）。そして、ｓ５１で読み出した暗証番号と、今回受け付けた現在の暗証番号と、が一致しているかどうかを判定する（ｓ５２）。管理装置１は、ｓ５２で２つの暗証番号が一致していると判定すると、利用者管理データベース１５に対して今回受け付けた口座番号の口座の暗証番号を今回受け付けた変更する暗証番号に更新し（ｓ５３）、利用者の携帯端末３に暗証番号の変更完了を通知して本処理を終了する（ｓ５４）。

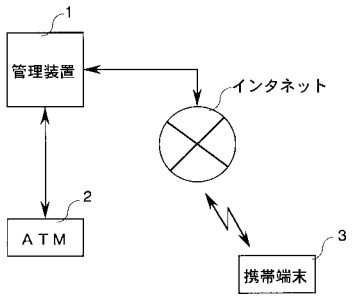
【００４８】

また、管理装置１は、ｓ５２で２つの暗証番号が一致していないと判定すると、利用者の携帯端末３に暗証番号の不一致を通知し（ｓ５５）、本処理を終了する。これにより、正当な利用者の口座の暗証番号が、他人に勝手に変更されるのを防止できる。

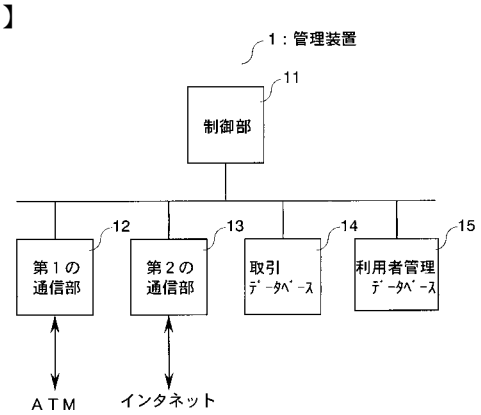
【００４９】
このように、この実施形態の取引処理システムでは、誤った暗証番号が入力されたことを正当な利用者に通知する電子メールを、利用停止にかかる要求を受け付けるページをリンク付けしたリンクメッセージとしたので、正当な利用者が簡単且つ迅速に利用停止にかかる要求を受け付けるページにアクセスし、自己の口座を利用停止にできる。したがって、不正利用者の存在を認識した正当な利用者が、利用停止にかかる手続を迅速に行うことができ、不正利用者による不正利用を十分に防止できる。
【００５０】
また、多くの場合、利用停止が登録されている利用者は、先に送信されてきた電子メールにより、すでに不正利用者の存在を認識しているので、このような利用者に誤ったパスワードが入力されたことを通知する電子メールを何度も送信すると、この電子メールを受け取る利用者にとっては迷惑であり、また利用者を不快にさせ、利用者に対するサービスを低下させてしまう。そこで、利用停止が登録されている利用者については、誤ったパスワードが入力されたことを通知する電子メールを送信しないので、利用者を不快にさせることがなく、利用者に対するサービスの低下を防止できる。
【００５１】
また、送信してから所定時間以上経過した後に、この電子メールにリンクさせたページで利用停止の要求を受け付けた場合、この利用停止にかかる要求を無効とするようにしたので、以前に送信されてきていた電子メールを、最近送信されてきた電子メールであると勘違いした利用者が口座を利用停止にするのを防止でき、利用者に対するサービスの向上が図れる。
【００５２】
さらに、誤ったパスワードが入力されたことを通知する電子メールに、パスワードの変更にかかる要求を行うページもリンクさせたので、利用を停止すると自己の不都合が大きい利用者に、不正利用を防止するためにパスワードを変更するという選択を行わせることができ、またこのパスワードの変更にかかる操作を簡単に行わせることができる。
【００５３】
なお、上記実施形態では、口座を利用停止にするとしたが、取引におけるキャッシュカードの利用を停止し、通帳と印鑑による口座取引については利用可能にしてもよい。
【００５４】
また、ｓ３６では正当な利用者の携帯端末３に電子メールを送信するとしたが、電子メールの送信先は据え置き型のパーソナルコンピュータ等であってもよい。
【００５５】
また、本願発明は、上記実施形態の取引処理システムだけでなく、インタネットを利用した業務アプリケーションシステムや、ネットワークバンキングシステム等、利用者がＩＤとパスワードを入力する様々なシステムに適用できる。
【図面の簡単な説明】
【００５６】
【図１】この発明にかかる不正利用通知方法を適用した取引処理システムの構成を示す図である。
【図２】管理装置の構成を示すブロック図である。
【図３】利用者管理データベースの構成を示す図である。
【図４】ＡＴＭの出金取引にかかる処理を示すフローチャートである。
【図５】管理装置の動作を示すフローチャートである。
【図６】認証処理を示すフローチャートである。
【図７】管理装置が送信したリンクメッセージを受信した携帯端末における、このリンクメッセージの表示例を示す図である。。
【図８】利用停止処理を示すフローチャートである。
【図９】口座の利用停止にかかる要求を受け付けるページにアクセスした携帯端末の画面例を示す図である。

【図１０】パスワード変更処理を示すフローチャートである。
【図１１】パスワードの変更にかかる要求を受け付けるページにアクセスした携帯端末の画面例を示す図である。
【符号の説明】
【００５７】
１－管理装置
２－ＡＴＭ
３－携帯端末
１１－制御部
１２－第１の通信部
１３－第２の通信部
１４－取引データベース
１５－利用者管理データベース

【図１】



【図２】

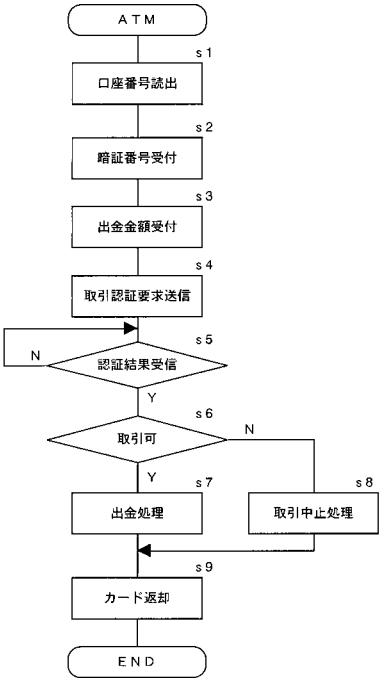


【図３】

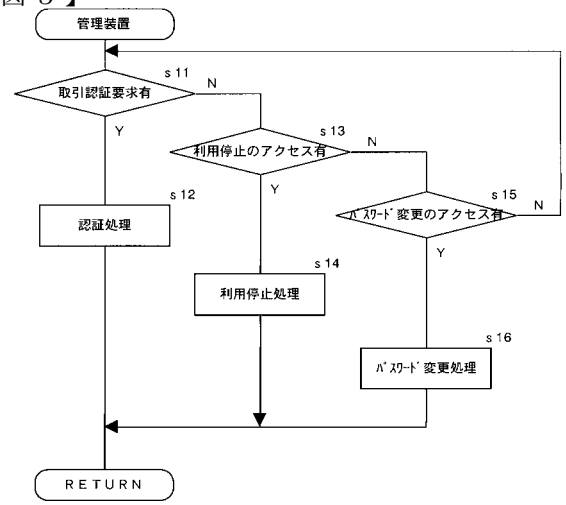
15:利用者管理ﾃﾞｰﾀﾍﾞｰｽ

利用者識別番号	暗証番号	ﾒｰﾙｱﾄﾞﾚｽ	誤った暗証番号が入力された回数	誤った暗証番号および使用されたATMの識別番号				利用停止の登録	電子ﾒｰﾙ識別番号
				1回目	2回目	3回目	4回目		
100001	2365	taro@pp.jpn	2	2003/3/1 15:00 A001	2003/3/3 16:00 A002	なし	なし	利用可	なし
100002	4521	jiro@good.jpn	0	なし	なし	なし	なし	利用可	なし
100003	6523	smith@ahf.jpn	3	2003/3/3 16:00 A003	2003/3/3 16:00 A003	2003/3/5 14:00 A004	なし	利用可	B002
100004	5623	kate@ju.jpn	3	2003/3/4 11:00 A002	2003/3/4 15:00 A002	2003/3/4 16:00 A002	なし	利用停止	B001
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○
○	○	○	○	○	○	○	○	○	○

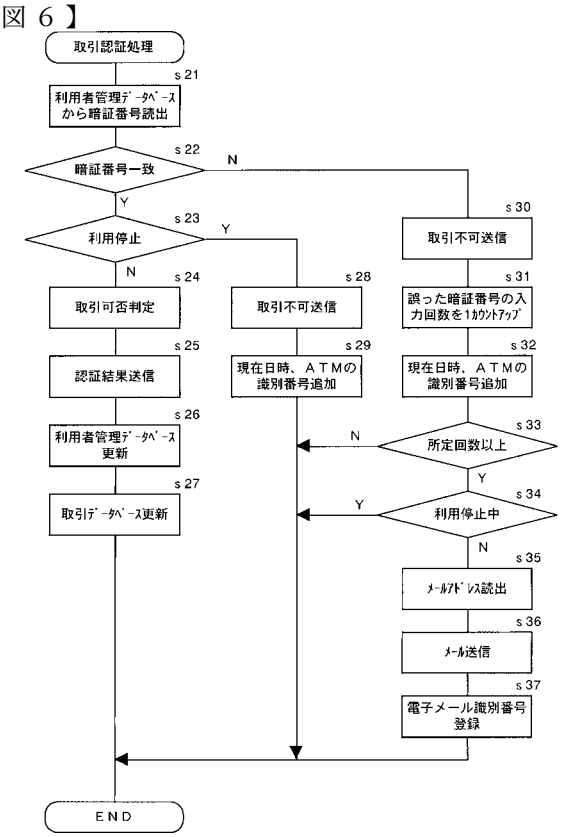
【図４】


ＡＴＭ
s 1
口座番号読出
s 2
暗証番号受付
s 3
出金金額受付
s 4
取引認証要求送信
s 5
認証結果受信
N
Y
s 6
取引可
N
Y
s 7
出金処理
s 8
取引中止処理
s 9
カード返却
ＥＮＤ

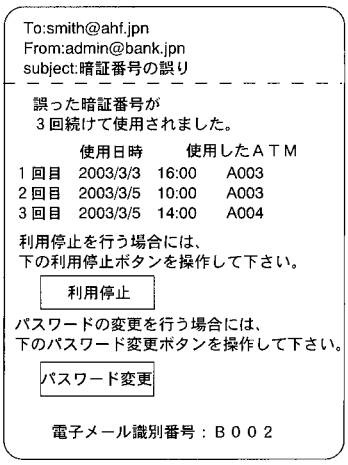
【図５】


管理装置
s 11
取引認証要求有
N
Y
s 13
利用停止のアクセス有
N
Y
s 15
ﾊﾟｽﾜｰﾄﾞ変更のアクセス有
N
Y
s 12
認証処理
s 14
利用停止処理
s 16
ﾊﾟｽﾜｰﾄﾞ変更処理
ＲＥＴＵＲＮ

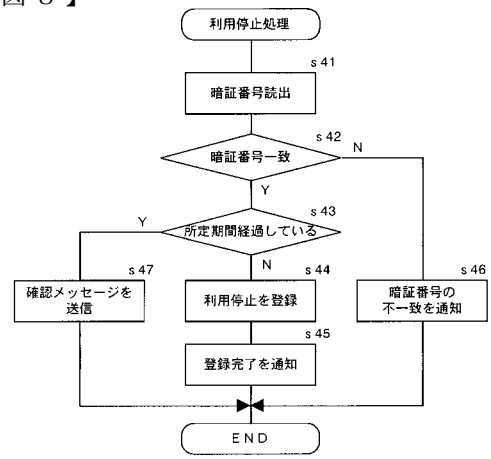
【図６】


取引認証処理
s 21
利用者管理ﾃﾞｰﾀﾍﾞｰｽから暗証番号読出
s 22
暗証番号一致
N
Y
s 23
利用停止
Y
N
s 24
取引可否判定
s 25
認証結果送信
s 26
利用者管理ﾃﾞｰﾀﾍﾞｰｽ更新
s 27
取引ﾃﾞｰﾀﾍﾞｰｽ更新
s 28
取引不可送信
s 29
現在日時、ＡＴＭの識別番号追加
s 30
取引不可送信
s 31
誤った暗証番号の入力回数を1ｶｳﾝﾄｱｯﾌﾟ
s 32
現在日時、ＡＴＭの識別番号追加
s 33
所定回数以上
N
Y
s 34
利用停止中
Y
N
s 35
ﾒｰﾙｱﾄﾞﾚｽ読出
s 36
ﾒｰﾙ送信
s 37
電子メール識別番号登録
ＥＮＤ

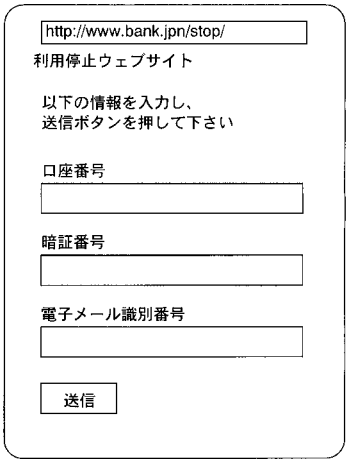
【図７】


To:smith@ahf.jpn
From:admin@bank.jpn
subject:暗証番号の誤り
誤った暗証番号が
３回続けて使用されました。
使用日時 使用したＡＴＭ
1回目 2003/3/3 16:00 A003
2回目 2003/3/5 10:00 A003
3回目 2003/3/5 14:00 A004
利用停止を行う場合には、
下の利用停止ボタンを操作して下さい。
利用停止
パスワードの変更を行う場合には、
下のパスワード変更ボタンを操作して下さい。
パスワード変更
電子メール識別番号：Ｂ００２

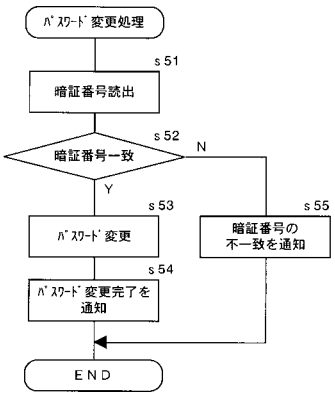
【図８】


利用停止処理
s41
暗証番号読出
s42
暗証番号一致
N
Y
s43
所定期間経過している
Y
N
s47
確認メッセージを送信
s44
利用停止を登録
s46
暗証番号の不一致を通知
s45
登録完了を通知
END

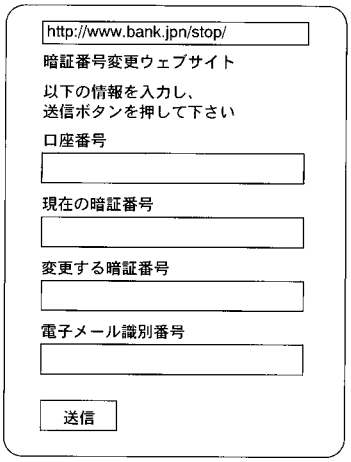
【図９】


http://www.bank.jpn/stop/
利用停止ウェブサイト
以下の情報を入力し、
送信ボタンを押して下さい
口座番号
暗証番号
電子メール識別番号
送信

【図１０】


ﾊﾟｽﾜｰﾄﾞ変更処理
s51
暗証番号読出
s52
暗証番号一致
N
Y
s53
ﾊﾟｽﾜｰﾄﾞ変更
s55
暗証番号の不一致を通知
s54
ﾊﾟｽﾜｰﾄﾞ変更完了を通知
END

【図１１】


http://www.bank.jpn/stop/
暗証番号変更ウェブサイト
以下の情報を入力し、
送信ボタンを押して下さい
口座番号
現在の暗証番号
変更する暗証番号
電子メール識別番号
送信

フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
	H04L 9/00 673A	