(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5947358号
(P5947358)

(45)発行日　平成28年7月6日(2016.7.6)　(24)登録日　平成28年6月10日(2016.6.10)

(51)Int.Cl.　F I
G06F 21/31 (2013.01)　G06F 21/31
G06F 21/34 (2013.01)　G06F 21/34

請求項の数 15　(全 17 頁)

(21)出願番号　特願2014-230844(P2014-230844)
(22)出願日　平成26年11月13日(2014.11.13)
(65)公開番号　特開2016-95637(P2016-95637A)
(43)公開日　平成28年5月26日(2016.5.26)
審査請求日　平成26年11月13日(2014.11.13)

(73)特許権者　397077955
株式会社三井住友銀行
東京都千代田区丸の内一丁目１番２号
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　森　滋子
東京都千代田区丸の内一丁目１番２号　株式会社三井住友銀行内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】認証処理装置、方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
認証処理装置であって、
ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含む、第１のデータベースと、
前記ユーザによって入力された前記認証情報を格納する第２のデータベースと、
前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定するように構成されている判定手段であって、前記判定手段は、前記ユーザ端末から受信した前記ユーザの認証情報を前記第２のデータベースに格納するようにさらに構成されている、判定手段と、
前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合するように構成されている照合手段と
を備え、
前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致しない場合に、前記照合手段は、認証情報入力画面を介してユーザ端末から受信した一連の認証情報を前記第２のデータベースに格納されている前記認証情報と照合し、両者が一致するか

どうかを判定するようにさらに構成されている、認証処理装置。
【請求項２】
両者が一致するとの判定に応じて、前記照合手段は、インターネットサービスプロバイダに対して通知メッセージを送信するようにさらに構成されている、請求項１に記載の認証処理装置。
【請求項３】
前記通知メッセージは、不正アクセスが行われていることを示すメッセージであり、
前記第２のデータベースに格納されている認証情報は、不正アクセスが疑われる際の照合用データとして利用される、
請求項２に記載の認証処理装置。
【請求項４】
前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、請求項１に記載の認証処理装置。
【請求項５】
認証処理装置であって、
ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含み、前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、第１のデータベースと、
前記ユーザによって入力された前記認証情報を格納する第２のデータベースと、
前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定するように構成されている判定手段であって、前記判定手段は、前記ユーザ端末から受信した前記ユーザの認証情報を前記第２のデータベースに格納するようにさらに構成されている、判定手段と、
前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合するように構成されている照合手段と
を備えた認証処理装置。
【請求項６】
認証処理装置であって、
ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含み、前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、第１のデータベースと、
前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定するように構成されている判定手段と、
前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合するように構成されている照合手段と
を備えたことを特徴とする認証処理装置。
【請求項７】
認証処理装置において実行される認証処理方法であって、
前記認証処理装置は、
ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含む、第１のデータベースと、

前記ユーザによって入力された前記認証情報を格納する第２のデータベースと
を備え、前記方法は、
前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定することであって、前記ユーザ端末から受信した前記ユーザの認証情報は、前記第２のデータベースに格納される、ことと、
前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合することと、
前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致しない場合に、認証情報入力画面を介してユーザ端末から受信した一連の認証情報を前記第２のデータベースに格納されている前記認証情報と照合し、両者が一致するかどうかを判定することと
を備える認証処理方法。
【請求項８】
両者が一致するとの判定に応じて、インターネットサービスプロバイダに対して通知メッセージを送信することをさらに備える、請求項７に記載の認証処理方法。
【請求項９】
前記通知メッセージは、不正アクセスが行われていることを示すメッセージであり、
前記第２のデータベースに格納されている認証情報は、不正アクセスが疑われる際の照合用データとして利用される、
請求項８に記載の認証処理方法。
【請求項１０】
前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、請求項７に記載の認証処理方法。
【請求項１１】
請求項７乃至１０のいずれか一項に記載の方法をコンピュータに実行させるためのプログラム。
【請求項１２】
認証処理装置において実行される認証処理方法であって、
前記認証処理装置は、
ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含み、前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、第１のデータベースと、
前記ユーザによって入力された前記認証情報を格納する第２のデータベースと
を備え、前記方法は、
前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定することであって、前記ユーザ端末から受信した前記ユーザの認証情報は、前記第２のデータベースに格納される、ことと、
前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合することと
を備える認証処理方法。

【請求項１３】
請求項１２に記載の方法をコンピュータに実行させるためのプログラム。
【請求項１４】
認証処理装置において実行される認証処理方法であって、
前記認証処理装置は、
ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含み、前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、第１のデータベースを備え、
前記方法は、
前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定することと、
前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合することと
を備える認証処理方法。
【請求項１５】
請求項１４に記載の方法をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティ技術に関する。より詳細に言えば、本発明は、ネットバンキングシステムにおける認証情報の盗難に対する認証処理装置、方法およびプログラムに関する。
【背景技術】
【０００２】
従来から、ユーザが、パーソナルコンピュータ（ＰＣ）や携帯電話などを使用してインターネット経由で銀行などの金融機関が提供するネットバンキングシステムにアクセスし、当該システムが提供するサービスを利用することが広まっている。ネットバンキングシステムを利用する際、まず、ユーザ認証のための画面が表示されることが多い。また、ユーザが使用を望むサービスの種類（例えば、送金）によっては、さらなるユーザ認証が必要になることもある。
【０００３】
このようなネットバンキングシステムの利用が拡大する一方で、コンピュータウィルスなどによるユーザのＩＤおよびパスワードの盗難事件が多発するようになってきている。ユーザが使用するパーソナルコンピュータ（ＰＣ）などがウィルス感染すると、認証画面や追加パスワード入力画面の偽画面が表示され、ユーザがその偽画面を本物の画面と信じてＩＤやパスワードを入力したことによりパスワードが盗まれたり、あるいは本物の画面が表示されたとしても、ＩＤやパスワードを入力して所定のボタン押下時に入力したＩＤやパスワードが盗まれたりすることも発生している。
【０００４】
ＩＤやパスワードが盗まれると、本人が気づかないうちに第三者によって口座から不正送金が実行されてしまうなどの重大な被害が発生することもあった。
【０００５】
このような第三者の不正アクセスを防止するために、正規利用者のＩＤおよびパスワードに類似した「おとりパスワード」のリストを予め用意しておき、アクセスしてきた利用者が入力したＩＤおよびパスワードが「おとりパスワード」リストと一致した場合に当該利用者を不正利用者と判断することも行われていた（特許文献１参照）。

【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開平６－１５２７４７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、このような対策が採られていたとしても、パスワード盗難による被害は毎年のように報告されている。上述のようなコンピュータウィルスによりパスワードが盗まれた場合、本人が気づかないうちに見ず知らずの第三者宛ての不正送金が行われることがあった。
【０００８】
また、パスワードの盗難がしづらくなるための対策が採られたとしても、その対策を破る新手のコンピュータウィルスなどが出現することにより、新たな対策を採る必要が生じるといった、いたちごっこの状況となっていた。
【０００９】
本願発明は、このような課題に鑑みてなされたものであり、盗まれても構わない「おとりパスワード」および「正規のパスワード」の入力条件を定めておき、当該入力条件を満たす操作をユーザが行った場合にのみ処理を続行させ、当該入力条件を満たす操作が行われなかった場合には後続の処理を行わないことにより、パスワード盗難による不正送金などの被害を減らす装置および方法を提供することを目的とする。
【００１０】
また、本願発明は、パスワード盗難による不正アクセスが疑われる時には、インターネットサービスプロバイダ（ＩＳＰ）などに必要な情報を通知することにより、不正アクセスを行った者を特定しやすくする装置および方法を提供することを目的とする。
【課題を解決するための手段】
【００１１】
上記の課題を解決するための一態様としての認証処理装置は、ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含む、第１のデータベースと、前記ユーザによって入力された前記認証情報を格納する第２のデータベースと、前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定するように構成されている判定手段であって、前記判定手段は、前記ユーザ端末から受信した前記ユーザの認証情報を前記第２のデータベースに格納するようにさらに構成されている、判定手段と、前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合するように構成されている照合手段とを備え、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致しない場合に、前記照合手段は、認証情報入力画面を介してユーザ端末から受信した一連の認証情報を前記第２のデータベースに格納されている前記認証情報と照合し、両者が一致するかどうかを判定するようにさらに構成されている、ことを特徴とする。
【００１２】
本発明の他の態様としての認証処理装置は、ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含み、前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、第１のデータベースと、前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す

場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定するように構成されている判定手段と、前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合するように構成されている照合手段とを備えたことを特徴とする。

【００１３】

また、他の態様としての認証処理装置において実行される認証処理方法は、前記認証処理装置が、ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含む、第１のデータベースと、前記ユーザによって入力された前記認証情報を格納する第２のデータベースとを備え、前記方法は、前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定することであって、前記ユーザ端末から受信した前記ユーザの認証情報は、前記第２のデータベースに格納される、ことと、前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合することと、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致しない場合に、認証情報入力画面を介してユーザ端末から受信した一連の認証情報を前記第２のデータベースに格納されている前記認証情報と照合し、両者が一致するかどうかを判定することを備えることを特徴とする。

【００１４】

本発明の他の態様としての認証処理装置において実行される認証処理方法は、前記認証処理装置が、ユーザの管理情報を格納する第１のデータベースであって、前記管理情報は、前記ユーザの認証情報、契約情報、および認証時回数情報を含み、前記認証時回数情報は、前記ユーザに関連付けられているワンタイムパスワードの値に基づいて動的に決定される、第１のデータベースを備え、前記方法は、前記第１のデータベースから前記管理情報を読み出し、前記読み出した管理情報の前記契約情報が契約有りを示す場合に、認証情報入力画面を介してユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上であるかを判定することと、前記ユーザ端末から受信した認証情報の数が前記認証時回数情報に示される数以上の場合に、前記ユーザ端末から受信した認証情報のうち前記認証時回数情報に示される数の時に入力された認証情報と、前記読み出した管理情報の前記ユーザの認証情報とが一致するかどうかを照合することとを備えることを特徴とする。

【発明の効果】

【００１５】

本発明によれば、盗まれても構わない「おとりパスワード」および「正規のパスワード」の入力条件を定めておき、当該入力条件を満たす操作をユーザが行った場合にのみ処理を続行させ、当該入力条件を満たす操作が行われなかった場合には後続の処理を行わないことにより、パスワード盗難による不正送金などの被害を減らすことが可能となる。

【００１６】

また、本発明によれば、パスワード盗難による不正アクセスが疑われる時には、インターネットサービスプロバイダ（ＩＳＰ）などに必要な情報を通知することにより、不正アクセスを行った者を特定しやすくすることが可能となる。

【図面の簡単な説明】

【００１７】

【図１】本発明に係るネットバンキングシステムを含む、システム全体の概要を説明する図である。

【図２】本発明に係るネットバンキングシステムのシステム構成の概要を説明する図である。
【図３】本発明に係るネットバンキングシステムにおいて実行される認証処理を説明するフロー図である。
【図４】認証情報入力画面の一例としてのログイン画面である。
【図５】管理ＤＢに格納される管理情報のデータ項目の一例を説明する図である。
【図６】入力情報ＤＢに格納される入力認証情報のデータ項目の一例を説明する図である。
【図７】本発明に係るネットバンキングシステムの機能ブロック図である。
【図８】第三者が盗んだユーザＩＤやＰＷなどの認証情報を利用してシステムにアクセスした際の処理を説明する図である。
【発明を実施するための形態】
【００１８】
まず、本明細書で説明する「おとりパスワード」のサービスについて説明する。従来のネットバンキングシステムを利用する際の認証情報としては「正規のユーザＩＤ」および「正規のパスワード」が利用されていた。本発明では、このような認証情報がコンピュータウィルスなどにより盗まれることを想定し、常に複数回のＩＤとパスワードを入力するようにしておき、「正規のユーザＩＤ」と「正規のパスワード」を何回目に入力するかを本発明に係るネットバンキングシステムに登録しておき、登録された回数時以外は任意のパスワード（これを本明細書では「おとりパスワード」と呼ぶことにする）をユーザに入力してもらい、認証要求実行後、当該回数時に入力した、正規の認証情報をもって認証処理を行うこととした。具体的に言えば、当該回数が３回の時、少なくとも３回は入力を促すメッセージとともに認証情報（ＩＤおよびパスワード）を入力する画面が表示され、３回以上認証情報を入力した後に認証要求を実行して始めて認証処理が行われる。例えば、認証情報を入力する画面を１０回表示させて認証情報（ＩＤおよびパスワード）を１０回入力した上で、認証要求を実行（例えば、ログインボタンを押下）してもよい。かかる場合、登録された回数が３回なので、３回目に入力された認証情報に基づいて認証処理が行われることになる。
【００１９】
本発明の一実施形態では、どんなパスワードを入力したとしても認証要求を実行するまで何度でも認証情報入力画面が表示されるので、ユーザは、任意の回数だけ認証情報を入力することが可能である。入力されるパスワードは、指定された回数時だけは正規のパスワードを入力する必要があるが、それ以外の回数時は、正規のパスワードを入力するようにしてもよいし、正規ではないパスワードを入力するようにしてもよく、いずれでも構わない。
【００２０】
また、本発明の一実施形態では、何回目に正規のパスワードを入力するのかを表す回数は、動的に変更可能である。本実施形態では、上述したように、ユーザによって予め設定された回数（静的な値）を登録しておくことも可能であるが、本発明の一実施形態では、ワンタイムパスワードのサービスを使用し、動的に当該回数を設定可能にすることも可能である。
【００２１】
既知のワンタイムパスワードのサービスでは、トークンと呼ばれることもある、ワンタイムパスワードを表示するデバイスがユーザに配布され、ユーザは認証情報を入力する際、当該デバイスに表示されている値を使用していた。後述するように、本発明では、ユーザがシステムに認証情報を入力する際に当該デバイスに表示されているワンタイムパスワードの任意の桁（例えば、１の位）の値を回数として動的に設定することが可能である。本発明に係るネットバンキングシステムでは、認証情報を入力する画面が開かれた時などに、ワンタイムパスワードの任意の桁の値を回数として動的に設定可能なように構成することができる。このような構成により、ユーザ側とシステム側で、何回目に正規の認証情

報を入力しなければならないのかの情報が同期されるので、ユーザはトークンに示される数値にしたがって正規の認証情報を入力すればよい。なお、本実施形態の前提として、ユーザが銀行に対して、ワンタイムパスワードの任意の桁のうち、どの桁の数値を使用するかは知らせておく必要がある。

【００２２】

上述のような実施形態によれば、仮に、認証情報の盗難があったとしても、第三者は、システムにアクセスできないユーザＩＤおよびパスワードの組合せを多数保持してしまうので、不正アクセスをするまでに時間がかかり、また、故意にパスワード入力を誤る回数が動的に変更されうるので、盗んだ一連のユーザＩＤおよびパスワードを順番に全て使用したとしても、不正アクセスをすることが非常に困難となる。例えば、ワンタイムパスワードを使用する実施形態では、ユーザＩＤおよびパスワードの盗難時には３回目の入力時に正規のユーザＩＤおよび正規のパスワードが使用されていたが、盗難者が不正アクセスを試みるときには３回目ではない回数（例えば、２回目や５回目）の入力時に正規のユーザＩＤおよび正規のパスワードを使用しなくてはならなくなる可能性が高いので、不正アクセスに成功する可能性が著しく減少することになる。

【００２３】

さらに、上述した実施形態を組み合わせて使用することも可能である。例えば、トークンに表示された任意の桁の数値が「３」である時には、３回目の認証情報の入力時に正規のユーザＩＤとパスワードを入力すればよく、４回以上ユーザＩＤとパスワードを入力した上で任意のタイミングで認証要求を実行すればよい。このようにすることにより同じユーザのＩＤとパスワードが何度盗まれたとしても、毎回、何回目に正規の認証情報を入力しなければならないのかの情報が異なってくるので、盗難者は、不正を働くことが著しく困難となる。

【００２４】

以下、本発明の実施形態について詳細に説明するが、本発明の要旨を逸脱することなく、構成および細部において変更される様々な実施形態を実現可能であることを当業者は理解するだろう。

【００２５】

図１は、本発明に係るネットバンキングシステム１２０を含む、システム全体の概要を説明する図である。図１に示されるように、ユーザ端末１００ａ、１００ｂ、１００ｃ、１００ｄ、・・・（説明の便宜上、以後、「ユーザ端末１００」とする）は、インターネットサービスプロバイダ（ＩＳＰ）１１０ａ、１１０ｂ（同様に、「ＩＳＰ１１０」とする）経由でネットバンキングシステム１２０にアクセスすることができる。

【００２６】

本明細書において「ユーザ端末」という用語には、例えば、パーソナルコンピュータ（ＰＣ）、ラップトップ、タブレット型コンピュータ、携帯情報端末（ＰＤＡ）、ユーザ機器（ＵＥ）、移動局、セルラ電話機、スマートフォン、あるいは有線または無線環境において動作可能な他の任意のタイプのデバイスが含まれ得るが、これらには限定されない。すなわち、ユーザ端末１００は、ＩＳＰ１１０を介してネットバンキングシステム１２０に有線および／または無線でアクセスすることが可能な任意の種類のデバイスとすることができる。

【００２７】

ＩＳＰ１１０は、企業や家庭に設置されているユーザ端末１００に対して通信回線を通じてインターネット接続サービスを提供することができる既知のプロバイダである。ＩＳＰ１１０は、ネットバンキングシステム１２０から所定の通知メッセージを受信し、およびネットバンキングシステム１２０に対する特定のアクセスに関わったユーザ端末１００の情報を格納するように構成されることができる。特定のアクセスに関わったユーザ端末１００の情報は、不正アクセスの対象者を識別するために用いることができる。

【００２８】

本実施形態では、インターネットサービスプロバイダ（ＩＳＰ）を利用する実施形態を

説明するが、本発明の適用範囲はこれに限定されることはなく、ユーザ端末１００がインターネットなどのネットワークに接続するための機能を提供するものであれば構わない。

【００２９】

ネットバンキングシステム１２０は、ユーザ端末１００に対して既知のサービス（例えば、預金残高照会、入出金照会、口座振込や振替などの送金処理、など）を提供することができる。ネットバンキングシステム１２０は、ＩＳＰ１１０に対して所定の通知メッセージを送信することができる。所定の通知メッセージの送信に関する処理およびそのための構成については図８を参照しながら後述する。

【００３０】

図２は、本発明に係るネットバンキングシステム１２０のシステム構成の概要を説明する図である。ネットバンキングシステム１２０は、一般的なコンピュータと同様に、バス２１０などによって相互に接続された制御部２０１、主記憶部２０２、補助記憶部２０３、インターフェース（ＩＦ）部２０４および出力部２０５を備える。また、ネットバンキングシステム１２０は、管理データベース（ＤＢ）２０６および入力情報ＤＢ２０７を備えることができる。

【００３１】

制御部２０１は、中央処理装置（ＣＰＵ）とも呼ばれ、ネットバンキングシステム１２０内の各構成要素の制御やデータの演算を行い、また、補助記憶部２０３に格納されている各種プログラムを主記憶部２０２に読み出して実行することができる。主記憶部２０２は、メインメモリとも呼ばれ、受信した各種データ、コンピュータ実行可能な命令および当該命令による演算処理後のデータなどを記憶することができる。補助記憶部２０３は、ハードディスク（ＨＤＤ）などに代表される記憶装置であり、データやプログラムを長期的に保存する際に使用される。

【００３２】

図２の実施形態では、制御部２０１、主記憶部２０２および補助記憶部２０３を同一のサーバコンピュータ内に設ける実施形態について説明したが、他の実施形態として、ネットバンキングシステム１２０は、制御部２０１、主記憶部２０２および補助記憶部２０３を複数個使用することにより、複数のサーバコンピュータによる並列分散処理を実現するように構成されることもできる。また、他の実施形態として、ネットバンキングシステム１２０用の複数のサーバを設置し、複数サーバが一つの補助記憶部２０３を共有する実施形態にすることも可能である。

【００３３】

ＩＦ部２０４は、他のシステムや装置との間でデータを送受信する際のインターフェースの役割を果たし、また、システムオペレータから各種コマンドや入力データ（各種マスタ、テーブルなど）を受け付けるインターフェースを提供することができる。出力部２０５は、処理されたデータを表示する表示画面などを提供することができる。

【００３４】

管理ＤＢ２０６は、ネットバンキングシステム１２０の利用者（ユーザ）の管理情報を格納するデータベースである。当該管理情報には、ユーザのＩＤやパスワード（ＰＷ）などの認証情報、本明細書で上述した「おとりパスワード」のサービス契約の締結有無、何回目に正規の認証情報を入力しなければならないのかの情報（図５の認証時回数５０６）、ワンタイムパスワード使用時に利用される任意の桁情報などが含まれるが、これらのデータ項目に限定されることはない。

【００３５】

入力情報ＤＢ２０７は、ユーザによって実際に入力された認証情報（ユーザＩＤとパスワード）を格納するデータベースである。格納されている認証情報は、ユーザにより入力された認証情報のログ情報であり、不正アクセスが疑われる際の照合用データとして利用されることが可能である。

【００３６】

図３は、本発明の一実施形態に係るネットバンキングシステム１２０において実行され

る認証処理を説明するフロー図である。以降の説明では、ユーザがワンタイムパスワードを使用する実施形態および使用しない実施形態の両方に適用可能な実施形態について説明するが、本発明の要旨は、いずれかの実施形態のみに適用することも可能であることを理解されたい。

【００３７】

本処理フローは、Ｓ３０１からスタートする。Ｓ３０１にて、ユーザはユーザ端末１００を使用してＩＳＰ１１０経由でネットバンキングシステム１２０にアクセスする。ネットバンキングシステム１２０にアクセスすると、図４に例示されるような認証情報入力画面（ログイン画面）４００がユーザ端末１００のディスプレイ等に表示される。なお、図４ではログイン画面４００を認証情報入力画面４００の一例として示したが、本発明はこれに限定されることはなく、ユーザＩＤおよびパスワード（ＰＷ）などの認証情報を入力可能な入力画面であれば、他の用途（例えば、送金）の操作画面であってもよい。

【００３８】

図４のログイン画面４００には、ユーザＩＤおよびパスワードの入力欄、これらの認証情報をさらに入力可能にするためのＯＫボタン、および認証要求を実行するためのログインボタンが含まれている。より詳細に説明すれば、ログイン画面４００においてユーザＩＤおよびパスワードを入力してＯＫボタンを押下すれば、ユーザが所望の回数だけユーザＩＤおよびパスワードを入力可能となる。すなわち、ユーザＩＤおよびパスワードの入力とＯＫボタンの押下を５回繰り返せば、５回分の認証情報が蓄積されることとなり、ログインボタンが押下されて始めて認証処理が行われる（ただし、認証時回数５０６に示される回数以上の入力は必要）。なお、ボタンの名称は例示であって、同様の機能を果たすものであれば他の名称であっても構わない。

【００３９】

Ｓ３０２にて、ユーザ端末１００のディスプレイ等に表示された認証情報入力画面４００にユーザＩＤおよびパスワード（ＰＷ）などの認証情報が入力される。入力された認証情報は、図４に例示した「ＯＫ」ボタンの押下時にネットバンキングシステム１２０に送信されて主記憶部２０２上に記憶される。また、入力された認証情報は、図４に例示した「ログイン」ボタンの押下時にも、ユーザ端末１００からネットバンキングシステム１２０に送信され、かかる場合には、送信された認証情報は、主記憶部２０２に格納されている認証情報とともに入力情報ＤＢ２０７に格納される。

【００４０】

入力情報ＤＢ２０７には、図６に例示するような入力認証情報６００を格納可能である。入力認証情報６００は、ユーザが認証情報入力画面４００に実際に入力したユーザＩＤおよびパスワード（ＰＷ）などの履歴情報（ログ情報）であり、第三者がこのユーザの認証情報を盗んで使用した場合に盗難情報であるかどうかを判定するための情報として活用することができる。

【００４１】

図６に例示するように、入力認証情報６００は、契約者名６０１、ユーザＩＤ６０２、日時６０３および入力ＰＷ６０４を備えるが、これ以外のデータ項目を含めるようにしても構わない。契約者名６０１は、ネットバンキングシステム１２０にアクセスしてきたユーザの契約者名であり、後述する契約者名５０１と同様のデータである。ユーザＩＤ６０２、日時６０３および入力ＰＷ６０４は、それぞれ、認証情報入力画面４００に実際に入力されたユーザＩＤ、ＯＫボタンやログインボタンなどの所定のボタンを押下するといったイベントが発生した日時、および実際に入力されたＰＷである。

【００４２】

再び図３に戻って説明すると、Ｓ３０３にて、ユーザによって図４に例示した「ログイン」ボタンが押下されると、認証要求実行指示がユーザ端末１００からネットバンキングシステム１２０に送信される。ネットバンキングシステム１２０は、ユーザ端末１００から認証要求実行指示を受信したことに応答して、ユーザによってそれまでに入力された認証情報に含まれるユーザ識別情報（例えば、ユーザＩＤ）を検索キーにして管理ＤＢ２０

６にアクセスし、管理ＤＢ２０６に格納されている、図５に例示されるような管理情報５００を読み出す。読み出された管理情報５００は、主記憶部２０２上に記憶される。仮に、ユーザＩＤが複数存在する場合には、複数のユーザＩＤが存在する旨のエラーメッセージを表示するようにしてもよいし、あるいは、最も数が多いユーザＩＤを検索キーとして利用してもよい。

【００４３】

図５は、管理ＤＢ２０６に格納されている管理情報５００のデータ項目を説明する図である。管理情報５００は、契約者名５０１、口座情報５０２、契約有無５０３、ユーザＩＤ５０４、パスワード（ＰＷ）５０５および認証時回数５０６を備えることができる。図５に示した管理情報５００のデータ項目は一例であり、その他のデータ項目が含まれてもよい。

【００４４】

契約者名５０１、口座情報５０２、ユーザＩＤ５０４およびパスワード（ＰＷ）５０５は、それぞれ、ネットバンキングシステム１２０のサービスを契約しているユーザのユーザ名、当該ユーザの口座情報（店番号、科目、口座番号）、当該サービスを利用する際のユーザＩＤおよびパスワードである。

【００４５】

契約有無５０３は、本明細書で説明する「おとりパスワード」を使用する契約を締結しているか否かを示す情報である。認証時回数５０６は、何回目に正規の認証情報を入力しなければならないのかを示す回数情報を格納する。認証時回数５０６に格納される数値は、ワンタイムパスワード用トークンに表示される数値の任意の桁（例えば、１の位）の数値と同じ数値が当該ユーザのシステムアクセス時や所望の機能（例えば、送金）を実行しようとする時に動的に格納されるように構成されることができる。ワンタイムパスワードを利用する実施形態の利点として挙げられるのは、ワンタイムパスワード用トークンに表示される数値は、配布されるユーザごとに異なる（換言すれば、ユーザごとに異なる表示となる）ことである。このため、第三者が他のトークンを入手したとしても被盗難者のトークンと同じ数値を把握することは困難である。本発明においてワンタイムパスワードを使用しない実施形態も可能であるが、その場合には、ユーザによって設定された回数が認証時回数５０６に格納される。

【００４６】

再び図３に戻って説明すると、Ｓ３０４にて、ネットバンキングシステム１２０は、読み出した管理情報５００内の契約有無５０３が「契約有り」を示す場合に、認証情報入力画面４００を介してユーザ端末１００から受信した認証情報の数が認証時回数５０６に示される回数以上であるかを判定する。認証時回数５０６に示される回数以上であればＳ３０６に処理が進み、一方、認証時回数５０６に示される回数未満であればＳ３０５に処理が進んで、入力された認証情報の数が少ない旨のエラー表示がユーザ端末１００のディスプレイ等に表示され、本処理フローが終了する。

【００４７】

具体的に言えば、認証時回数５０６に「２」という情報が示されていれば、認証情報（ＩＤ、ＰＷ）が何回入力されたとしても２回目に入力された認証情報を使用して認証処理が行われることとなり、１回目に入力された認証情報および３回目以降に入力された認証情報は、認証処理には使用されない。仮に、１回しか認証情報が入力されなければＳ３０５のエラー処理が行われる。この「２」という数値は、ワンタイムパスワード用のトークンに表示されているか、あるいはユーザが設定した数値であるので、第三者はどの認証情報を使用したらよいのか特定することが非常に困難となる。

【００４８】

Ｓ３０６にて、ネットバンキングシステム１２０は、認証情報入力画面４００を通じて入力された認証情報のうち認証時回数５０６に示される回数の時に入力された認証情報と、読み出された管理情報５００のユーザＩＤ５０４およびＰＷ５０５とが一致するかどうかを照合する。上述したように、認証時回数５０６に示される回数の時以外に入力された

認証情報は、照合処理には使用されない。

【００４９】

Ｓ３０７にて、Ｓ３０６の照合の結果、正規のユーザであると判定された場合にはＳ３０８に処理が進み、一方、正規のユーザではないと判定された場合にはＳ３０９に処理が進む。

【００５０】

Ｓ３０８にて、ネットバンキングシステム１２０は、ユーザの所望の画面（例えば、メニュー画面、送金画面、など）をユーザ端末１００のディスプレイ等に表示させる。これにより、ユーザは所望の画面を利用して望む操作を行うことができるようになる。

【００５１】

Ｓ３０９にて、ネットバンキングシステム１２０は、画面上にＩＤやＰＷが誤っていることを示すエラーメッセージを表示するなどのエラー処理を行う。エラー処理の一実施形態としては、エラーメッセージの画面表示を行うだけでも構わないし、他の実施形態としては、図８を参照しながら後述するプロバイダ通知機能を実行するようにしてもよい。

【００５２】

図３を参照しながら説明した上記実施形態では、ユーザ端末１００から送信された認証情報が入力情報ＤＢ２０７に格納される実施形態について説明したが、本発明の実施形態はこれに限定されることはない。本発明の他の実施形態では、ユーザによって入力されたユーザＩＤおよびパスワードを入力情報ＤＢ２０７に格納することなく、認証を行うことが可能である。かかる場合、ユーザ端末１００から受信した認証情報は、主記憶部２０２上に記憶される。Ｓ３０３にて、ネットバンキングシステム１２０は、ユーザ端末１００から認証要求実行指示を受信したことに応答して、ユーザによってそれまでに入力された認証情報に含まれるユーザ識別情報（例えば、ユーザＩＤ）を検索キーにして管理ＤＢ２０６にアクセスし、管理ＤＢ２０６に格納されている管理情報５００を読み出す。その後、Ｓ３０４以後の処理が行われる。本発明の他の実施形態では、主記憶部２０２上に記憶されている認証情報は、入力情報ＤＢ２０７に格納されないので、その後破棄される。

【００５３】

図７は、本発明に係るネットバンキングシステム１２０の機能ブロック図の一例である。図７に示すように、ネットバンキングシステム１２０は、ＩＦ制御部７０１、判定部７０２、照合部７０３、エラー処理部７０４、管理ＤＢ２０６および入力情報ＤＢ２０７を備えている。

【００５４】

ＩＦ制御部７０１は、ユーザ端末１００によって行われた操作に応じて、または予め定められた条件が満たされる時に、予め定められた画面インターフェース（例えば、認証情報入力画面４００）をユーザ端末１００のディスプレイ等に表示させることができる。また、ＩＦ制御部７０１は、ユーザによって入力された認証情報を、所定のイベント発生時（例えば、画面上のボタン押下時、など）にユーザ端末１００からネットバンキングシステム１２０に送信することができる。

【００５５】

判定部７０２は、管理ＤＢ２０６に格納されている管理情報５００を読み出し、読み出した管理情報５００内の契約有無５０３が「契約有り」を示す場合に、認証情報入力画面４００を介してユーザ端末１００から受信した認証情報の数が認証時回数５０６に示される回数以上であるかを判定する。なお、認証時回数５０６の数値は、当該ユーザに割り当てられているワンタイムパスワード用トークンに表示される数値の任意の桁（例えば、１の位）の数値と同じ数値になるように動的に構成されてもよいし、あるいは、ユーザによって設定された数値が格納されるように構成されてもよい。

【００５６】

また、判定部７０２は、入力情報ＤＢ２０７に入力認証情報６００を格納することができる。入力認証情報６００は、ユーザが認証情報入力画面４００に実際に入力したユーザＩＤおよびＰＷの履歴情報であり、第三者がこれらの認証情報を盗んで利用した場合に利

用された情報が盗難情報であるかどうかを判定するための情報として活用することができる。

【００５７】

照合部７０３は、認証情報入力画面４００に入力された認証情報（ユーザＩＤおよびＰＷ）のうち認証時回数５０６に示される回数の時に入力された認証情報と、読み出された管理情報５００のユーザＩＤ５０４およびＰＷ５０５とが一致するかどうかを照合する。

【００５８】

また、照合部７０３は、入力されたユーザＩＤおよびＰＷの組合せが間違っているなどのエラーが発生した後に、入力された一連の認証情報を、入力情報ＤＢ２０７に格納されている過去に入力された入力認証情報６００と照合し、両者が一致するかどうかを判定することができる。当該判定の結果、一致していると判定された場合には、照合部７０３は、ＩＳＰ１１０に対して当該アクセスしてきたユーザが不正を行っている可能性が高い旨の通知メッセージを送信することができる。過去に入力された入力認証情報６００には、正規ユーザが出鱈目に入力したパスワードが含まれている可能性があり、そのようなパスワードまでが一致するということは、パスワード盗難があったと推定することが可能だからである。

【００５９】

エラー処理部７０４は、入力されたＩＤおよびＰＷの組合せが間違っている、といったエラー発生時にエラーメッセージやエラー表示をユーザ端末１００のディスプレイ等に表示させることができる。

【００６０】

管理ＤＢ２０６および入力情報ＤＢ２０７は、図２を参照しながら説明したように、それぞれ、ネットバンキングシステム１２０の利用ユーザの管理情報およびユーザによって入力された認証情報を格納するデータベースである。

【００６１】

図８は、第三者が盗んだユーザＩＤやＰＷなどの認証情報を利用してシステムにアクセスした際の処理を説明する図である。ワンタイムパスワード用トークンに表示される数値の任意の桁（例えば、１の位）の数値と同じ数値が認証時回数５０６に格納される実施形態の場合には、一連の「おとりパスワード」および「正規のパスワード」が盗まれたとしても、盗難者がシステムにアクセスして盗んだ認証情報を使用した場合には、そのアクセス時の認証時回数５０６の値は、盗難時の認証時回数５０６の値とは異なっている可能性が高い。例えば、ワンタイムパスワード用トークンに表示される数値の任意の桁の数値が０～９のいずれかであるとすると、盗難時と不正アクセス時の数値が一致する確率は１０分の１となる。このため、図３のフローに従って、盗難者がネットバンキングシステム１２０にアクセスしたとしても、Ｓ３０９のエラー処理に進む可能性が高い。

【００６２】

かかる場合に、Ｓ８０１にて、ネットバンキングシステム１２０（照合部７０３）は、入力された一連の認証情報が入力情報ＤＢ２０７に格納されている過去に入力された認証情報と一致するかどうかを判定する。一致しない場合には盗難者ではない可能性が高いので、画面上にエラー表示（例えば、「ＩＤおよびＰＷの組合せが間違っています。再度、入力をして下さい。」など）をして処理を終了する。一方、一致する場合には、盗難者が盗んだ認証情報を利用してアクセスしてきた可能性が高いので、ネットバンキングシステム１２０（照合部７０３）は、ＩＳＰ１１０に対して当該アクセスしてきたユーザが不正を行っている可能性が高い旨の通知メッセージを送信することができる。これにより、ＩＳＰ１１０では、どのアクセスユーザが不正な行為を行っているかを容易に特定することが可能となる。

【００６３】

本発明の他の実施形態として、認証時回数５０６によって示される回数時以外には、正規のパスワードの入力を不可とする実施形態も可能である。このような実施形態によれば、不正アクセスを試みようとする者（盗難者）が正規のＩＤおよび正規のパスワードの組

合せのみを使用してシステムへのアクセスを試みた場合でも不正アクセスを防止することが可能となる。

【００６４】

上記の実施形態では、図４に例示したような認証情報入力画面（ログイン画面）４００にユーザＩＤおよびパスワードを１回入力してＯＫボタンやログインボタンを１回押下する実施形態について説明した。しかしながら、本発明の他の実施形態として、認証情報入力画面（ログイン画面）４００にユーザＩＤおよびパスワードを入力するエリアを複数表示させて、ユーザＩＤおよびパスワードを複数の入力エリアにそれぞれ入力してからＯＫボタンやログインボタンを１回押下するように構成することも可能である。このような実施形態によれば、認証情報入力画面（ログイン画面）４００上で、例えば、５つのユーザＩＤおよびパスワードを入力しておき、その上でＯＫボタンやログインボタンを１回押下することになるので、盗難者はどのユーザＩＤおよびパスワードが正規のものであるのかが分かりにくくなる。

【００６５】

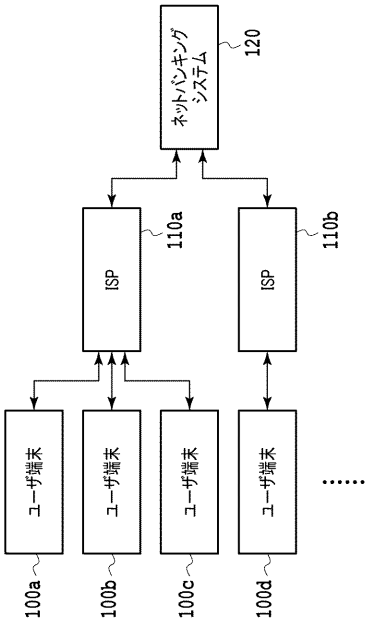
以上、例示的な実施形態を参照しながら本発明の原理を説明したが、本発明の要旨を逸脱することなく、構成および細部において変更する様々な実施形態を実現可能であることを当業者は理解するだろう。すなわち、本発明は、例えば、システム、装置、方法、プログラムもしくは記憶媒体等としての実施態様を採ることが可能である。

【符号の説明】

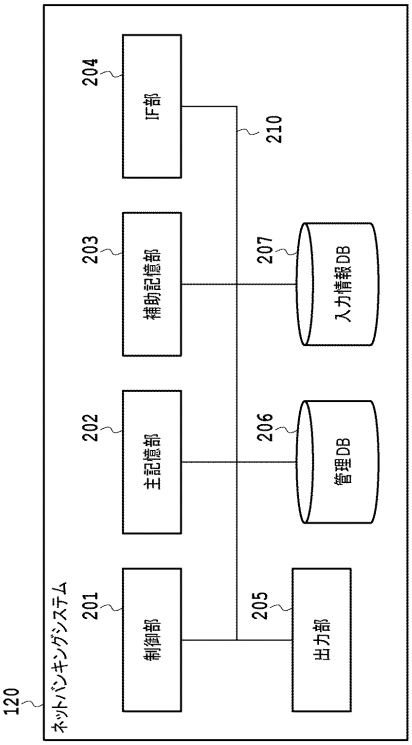
【００６６】

１００　ユーザ端末
１０１　インターネットサービスプロバイダ（ＩＳＰ）
１０２　ネットバンキングシステム
２０１　制御部
２０２　主記憶部
２０３　補助記憶部
２０４　インターフェース（ＩＦ）部
２０５　出力部
２０６　管理データベース（ＤＢ）
２０７　入力情報データベース（ＤＢ）
４００　認証情報入力画面（ログイン画面）
５００　管理情報
５０１、６０１　契約者名
５０２　口座情報
５０３　契約有無
５０４、６０２　ユーザＩＤ
５０５、６０４　パスワード（ＰＷ）
５０６　認証時回数
６００　入力認証情報
６０３　日時
７０１　ＩＦ制御部
７０２　判定部
７０３　照合部
７０４　エラー処理部

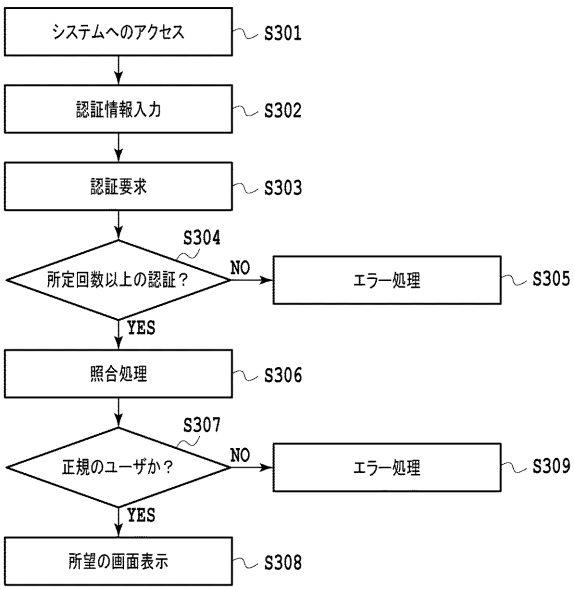
【図１】


ネットバンキングシステム
120
ISP
110a
ISP
110b
ユーザ端末
ユーザ端末
ユーザ端末
ユーザ端末
.....
100a
100b
100c
100d

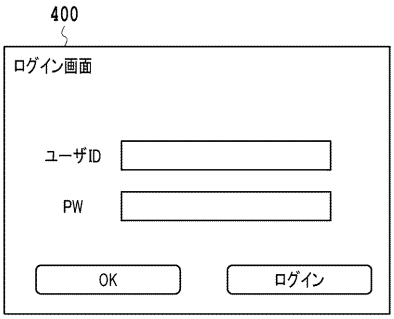
【図２】


204
IF部
210
203
補助記憶部
207
入力情報DB
202
主記憶部
206
管理DB
201
制御部
205
出力部
120
ネットバンキングシステム

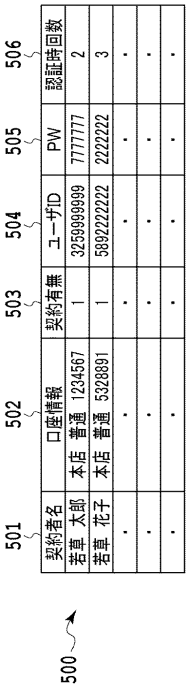
【図３】


システムへのアクセス
S301
認証情報入力
S302
認証要求
S303
S304
所定回数以上の認証？
NO
エラー処理
S305
YES
照合処理
S306
S307
正規のユーザか？
NO
エラー処理
S309
YES
所望の画面表示
S308

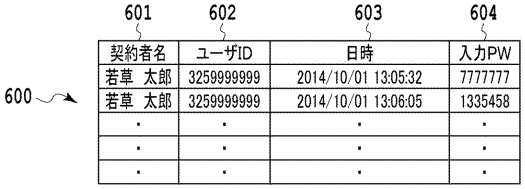
【図４】


400
ログイン画面
ユーザID
PW
OK
ログイン

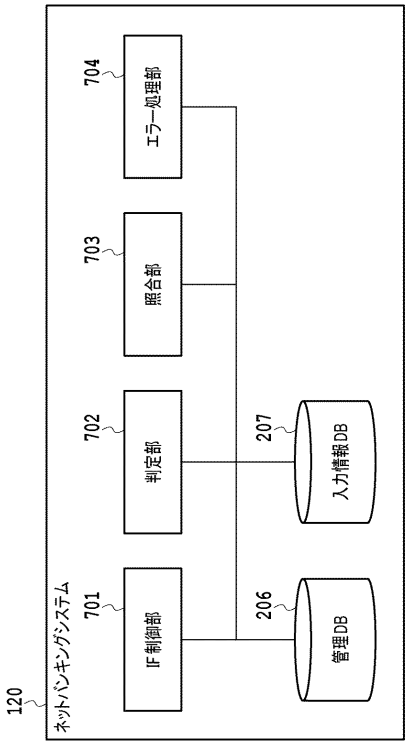
【図５】


501
502
503
504
505
506
契約者名
口座情報
契約有無
ユーザID
PW
認証時回数
若草 太郎
本店 普通 1234567
1
3259999999
7777777
2
若草 花子
本店 普通 5328891
1
5892222222
2222222
3
500

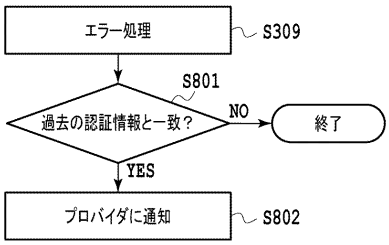
【図６】


601
602
603
604
契約者名
ユーザID
日時
入力PW
若草 太郎
3259999999
2014/10/01 13:05:32
7777777
若草 太郎
3259999999
2014/10/01 13:06:05
1335458
600

【図７】


120
ネットバンキングシステム
701
IF制御部
702
判定部
703
照合部
704
エラー処理部
206
管理DB
207
入力情報DB

【図８】


エラー処理
S309
S801
過去の認証情報と一致？
NO
終了
YES
プロバイダに通知
S802

フロントページの続き

(56)参考文献 特表２００９－５０５５９３（ＪＰ，Ａ）
特開２００２－１５０２４２（ＪＰ，Ａ）
特開２０００－０１０７７３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／３４