(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4964338号
(P4964338)
(45)発行日　平成24年6月27日(2012.6.27)　(24)登録日　平成24年4月6日(2012.4.6)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 21/20　144C
H04L 9/32 (2006.01)　　H04L 9/00　673A

請求項の数 4　(全 25 頁)

(21)出願番号　特願2011-22895(P2011-22895)
(22)出願日　平成23年2月4日(2011.2.4)
(62)分割の表示　特願2010-212465(P2010-212465)の分割
原出願日　平成18年3月29日(2006.3.29)
(65)公開番号　特開2011-100489(P2011-100489A)
(43)公開日　平成23年5月19日(2011.5.19)
審査請求日　平成23年2月18日(2011.2.18)

前置審査

(73)特許権者　598049322
株式会社三菱東京ＵＦＪ銀行
東京都千代田区丸の内２丁目７番１号
(74)代理人　110000408
特許業務法人高橋・林アンドパートナーズ
(72)発明者　嘉藤　隆也
東京都千代田区丸の内２－７－１　株式会社三菱東京ＵＦＪ銀行内

審査官　和田　財太

(56)参考文献　特開２００５－０４４２７７（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】ユーザ確認装置、方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
個々のユーザに対して一定の端末装置からのアクセスを許可するユーザ確認装置であって、
インターネット層のプロトコルとしてIPが適用され、アプリケーション層のプロトコルとしてHTTPが適用されて端末装置より受信したパケットから、当該パケットのHTTPヘッダに設定されているユーザエージェント情報を抽出する抽出手段と、
個々のユーザが操作する端末装置より受信したパケットから前記抽出手段によって各々抽出されたユーザエージェント情報を、前記個々のユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させる情報管理手段と、
認証されたユーザの使用する端末装置より受信したパケットから前記抽出手段によって抽出されたユーザエージェント情報を、前記ユーザのユーザ識別情報と対応付けて前記記憶手段に記憶されているユーザエージェント情報と照合し、前記記憶手段に記憶されているユーザエージェント情報と対応していることにより前記ユーザが一定の端末装置からアクセスしているか否かを判定することで、前記ユーザが正当なユーザか否かを判断する判断手段と、
を含むユーザ確認装置。
【請求項２】
前記個々のユーザが使用している電子メールアドレスを前記個々のユーザのユーザ識別情報と対応付けて各々管理する電子メールアドレス記憶手段と、

前記判断手段により、前記ユーザが正当なユーザでないと判断された場合に、前記判断手段と異なる方法によって前記ユーザが正当なユーザか否かを確認するための所定のウェブページへのリンクが付加された電子メールを、前記ユーザのユーザ識別情報と対応付けて前記電子メールアドレス記憶手段に記憶されている電子メールアドレスへ送信する送信手段と、

を含む請求項１に記載のユーザ確認装置。

【請求項３】

請求項１または２に記載のユーザ確認装置にネットワーク回線を介して接続された端末装置を含むユーザ認証システムであって、

前記端末装置は、該端末装置にインストールされているユーザエージェント情報を、前記ユーザ確認装置に対してパケット送信する際、HTTPヘッダに設定することを特徴とするユーザ認証システム。

【請求項４】

個々のユーザに対して一定の端末装置からのアクセスを許可するユーザ確認装置を用いるユーザ確認方法であって、

インターネット層のプロトコルとしてIPが適用され、アプリケーション層のプロトコルとしてHTTPが適用されて端末装置より受信したパケットから、当該パケットのHTTPヘッダに設定されているユーザエージェント情報をサーバが抽出し、

個々のユーザが操作する端末装置より受信したパケットから前記抽出されたユーザエージェント情報を、前記個々のユーザのユーザ識別情報と対応付けて前記サーバの記憶手段に前記サーバが各々記憶し、

認証されたユーザの使用する端末装置より受信したパケットから前記抽出されたユーザエージェント情報を、前記ユーザのユーザ識別情報と対応付けて前記記憶手段に記憶されているユーザエージェント情報と照合し、前記記憶手段に記憶されているユーザエージェント情報と対応していることにより前記ユーザが一定の端末装置からアクセスしているか否かを判定することで、前記ユーザが正当なユーザか否かを前記サーバが判断すること、

を含むユーザ確認方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はユーザ確認装置、方法及びプログラムに係り、特に、端末装置を操作しているユーザが正当なユーザか否かを確認するユーザ確認装置、該ユーザ確認装置に適用可能なユーザ確認方法、及び、コンピュータを前記ユーザ確認装置として機能させるためのユーザ確認プログラムに関する。

【背景技術】

【０００２】

予め登録したユーザに対してオンラインで所定のサービスを提供するウェブサイトでは、端末装置を介してウェブサイトにアクセスしてきた利用者にユーザＩＤ及びパスワードを入力させ、入力されたユーザＩＤとパスワードの組合わせが登録されているか否かに基づいて、アクセスしてきた利用者が正当なユーザか否かを確認するユーザ確認方法が採用されることが一般的である。しかし、上記のユーザ確認方法は、仮にユーザＩＤとパスワードが他者へ漏洩してしまった場合に、ユーザＩＤとパスワードを知った者が正当なユーザになりすまして不正にアクセスすることが可能になってしまうという欠点がある。

【０００３】

上記に関連して特許文献１には、ユーザＩＤ及びパスワードに加え、電話交換機から通知された発信者の電話番号が登録ユーザが使用する電話回線の電話番号と一致しているか否かも判定することで、ユーザの認証を行う技術が開示されている。

【０００４】

また特許文献２には、サービスの利用を許容するＩＰアドレス（及びリンク元ＵＲＬ）

をＩＤ・パスワードと共にデータベースに保存しておき、ＩＤ・パスワードによる認証に加え、アクセス元ＩＰアドレスがデータベースに登録されているか否か（及び、アクセス信号中にリンク元ＵＲＬが存在している場合は、当該リンク元ＵＲＬがデータベースに登録されているか否か）を判断することで、サービスの利用を許容するか否かを判断する技術が開示されている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開平２０００－２０９２８４号公報

【特許文献２】特開平２００１－３２５２２９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

特許文献１，２に記載の技術は、電話番号やＩＰアドレスを利用してアクセス元の端末装置が正当な端末装置か否かを判断することで、アクセス元の端末装置を操作しているユーザが正当なユーザか否か（第三者が正当なユーザになりすましていないか否か）を確認している。しかしながら、特許文献１に記載の技術は、電話番号を用いることで端末装置を一意に特定できるという利点を有しているものの、電話交換機を介してネットワークに接続された端末装置以外には適用できないという問題がある。

【０００７】

また、特許文献２に記載の技術で用いられているＩＰアドレスは、グローバルＩＰアドレスが固定的に付与された端末装置であれば常に一定であるものの、このような端末装置はごく少数であり、殆どの端末装置は、例えばインターネットへのアクセス時に、インターネット・サービス・プロバイダ（Internet service provider：インターネット接続業者、以下単に「プロバイダ」という）が保有している多数のグローバルＩＰアドレスの中から任意のＩＰアドレスが自動的に割り当てされるので、アクセスの都度ＩＰアドレスが相違する。このため、特許文献２に記載の技術のように、ＩＰアドレスが一致しているか否かに基づいてユーザの確認や認証を行った場合、正当なユーザによるアクセスを不正アクセスと誤判断したり、正当でないユーザを正当なユーザと誤判断する恐れがある。

【０００８】

また、なりすましを防止してセキュリティ性を向上させる技術として、ユーザＩＤとパスワードに基づくユーザ認証に先立ち、電子証明書を利用して端末装置の認証を行う技術も知られている。この技術を適用すれば、仮にユーザＩＤとパスワードが他者へ漏洩してしまったとしても、ユーザＩＤとパスワードを知った者が正規の電子証明書がインストールされた端末装置を操作しない限りは不正を防止できる。但し、この技術を適用するためには、端末装置に電子証明書をインストールするという煩雑な作業を行う必要があり、ユーザの負担が大きいという問題がある。

【０００９】

本発明は上記事実を考慮して成されたもので、ユーザの利便性を損なうことなくユーザ確認の精度を向上させることができるユーザ確認装置、ユーザ確認方法及びユーザ確認プログラムを得ることが目的である。

【課題を解決するための手段】

【００１０】

端末装置との通信におけるアプリケーション層のプロトコルとしてＨＴＴＰ(HyperText Transfer Protocol)を適用した場合、端末装置から受信するパケットにはＨＴＴＰヘッダが付加されるが、このＨＴＴＰヘッダにはユーザエージェント（User-Agent）情報が含まれている。ユーザエージェント情報は、ＨＴＴＰプロトコル上でフォーマット等が規定されておらず、任意の文字列を設定可能とされている。例えば端末装置がＰＣ（Personal Computer：パーソナル・コンピュータ）等のコンピュータであり、当該コンピュータからパケットを送信するアプリケーションがブラウザ（browser：閲覧ソフト）である場合

、ブラウザのデフォルトの設定では、ユーザエージェント情報として、当該コンピュータ上で動作しているＯＳ（オペレーティング・システム：Operating System）のバージョン等を表す情報と、ブラウザのバージョン等を表す情報を含む情報が設定される。また、コンピュータを操作するユーザによっては、ユーザエージェント情報として所望の文字列が送信されるように、ブラウザ等の設定が予め変更される場合もある。

【００１１】

デフォルトの設定のブラウザによって設定されるユーザエージェント情報には、ＯＳやブラウザのバージョン以外に、ＯＳやブラウザにパッチがどこまで当たっているかといった情報も含まれているので、デフォルトの設定のブラウザによってユーザエージェント情報が設定される場合、同一のユーザエージェント情報を送信する端末装置は存在するものの、個々の端末装置が送信するユーザエージェント情報の相違度は高い。また、ユーザエージェント情報は、ＯＳやブラウザに新たなパッチが当てられたり、バージョンアップや入れ替えが行われれば内容が変更されるが、ＯＳやブラウザに新たなパッチを当てられたり、ＯＳやブラウザのバージョンアップや入れ替えが行われて内容が変更される頻度は非常に低いので、個々の端末装置から送信されるユーザエージェント情報はおよそ一定とみなすことができる。また、ユーザエージェント情報として所望の文字列が送信されるようにユーザによって予め設定された場合、個々の端末装置が送信するユーザエージェント情報の相違度は更に高くなる。

【００１２】

本願発明者は上記事実に着目し、或るユーザが操作する端末装置から以前に受信したパケットのＨＴＴＰヘッダに設定されているユーザエージェント情報全体を記憶しておき、同一と推定されるユーザが操作する端末装置から受信したパケットのＨＴＴＰヘッダに設定されているユーザエージェント情報全体を、記憶しているユーザエージェント情報全体と照合することで、ユーザエージェント情報のフォーマットや内容が事前に変更設定されていたとしても、これを検知することなく、今回受信したパケットを送信した端末装置が、以前受信したパケットを送信した端末装置と同一か否かを判定することができ、ユーザ確認の精度を向上させることができることに想到して本発明を成すに至った。

【００１３】

上記に基づき第１の発明に係るユーザ確認装置は、インターネット層のプロトコルとしてＩＰが適用され、アプリケーション層のプロトコルとしてＨＴＴＰが適用されて端末装置より受信したパケットから、当該パケットのＨＴＴＰヘッダに設定されているユーザエージェント情報全体を抽出すると共に、前記パケットからアクセス元ＩＰアドレスを抽出する抽出手段と、個々のユーザが操作する端末装置より受信したパケットから前記抽出手段によって各々抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、前記個々のユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させる情報管理手段と、任意の端末装置より受信したパケットから前記抽出手段によって抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、前記任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて前記記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合し、前記記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを各々判定することで、前記任意の端末装置を操作しているユーザが正当なユーザか否かを判断する判断手段と、を含み、前記判断手段は、前記受信したパケットから抽出されたアクセス元ＩＰアドレスについては、前記記憶手段に記憶されているアクセス元ＩＰアドレスとの所定ビット単位の一致率が閾値以上か否かを判定することで、前記受信したパケットから抽出されたアクセス元ＩＰアドレスが前記記憶手段に記憶されているアクセス元ＩＰアドレスと対応しているか否かを判定し、前記受信したパケットから抽出されたユーザエージェント情報全体については、前記記憶手段に記憶されているユーザエージェント情報全体と同一か否かを判定することで、前記受信したパケットから抽出されたユーザエージェント情報全体が前記記憶手段に記憶されているユーザエージェント情報と対応しているか否かを判定することを特徴としている。

【００１４】
第１の発明は、インターネット層のプロトコルとしてＩＰ（Internet Protocol）が適用され、アプリケーション層のプロトコルとしてＨＴＴＰが適用されて端末装置より受信したパケットから、当該パケットのＨＴＴＰヘッダに設定されているユーザエージェント情報全体を抽出すると共に、前記パケットからアクセス元ＩＰアドレスを抽出する抽出手段を備えており、情報管理手段は、個々のユーザが操作する端末装置より受信したパケットから抽出手段によって各々抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、個々のユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させる。なお、ユーザ識別情報としては、例えば端末装置を操作する個々のユーザによって入力されたユーザＩＤや、このユーザＩＤから一意に定まる他の識別情報を適用することができる。また、ユーザエージェント情報全体は記憶手段にそのまま記憶させてもよいが、ハッシュ関数を用いる方法等の公知の暗号化方法を適用して暗号化した後に記憶手段に記憶させるようにした方がセキュリティ上好ましい。
【００１５】
また、第１の発明に係る判断手段は、任意の端末装置より受信したパケットから抽出手段によって抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合し、記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを各々判定することで、任意の端末装置を操作しているユーザが正当なユーザか否かを判断する。
【００１６】
前述のように、個々の端末装置から送信されるユーザエージェント情報はおよそ一定とみなすことができる。アプリケーション層のプロトコルとしてＨＴＴＰが適用された場合、端末装置より受信したパケットのＨＴＴＰヘッダには必ずユーザエージェント情報が設定されているので、ユーザエージェント情報全体を利用したユーザ（端末装置）の確認は、電話交換機を介してネットワークに接続された端末装置以外には適用できない特許文献１に記載の技術よりも汎用性が高く、アクセスの都度変化する可能性があるＩＰアドレスのみを用いる技術よりも確認の精度が高く、端末装置に電子証明書をインストールする等の煩雑な作業も不要である。また、ユーザエージェント情報全体を照合することで、例えば、ユーザエージェント情報として所望の文字列が送信されるようにユーザによってユーザエージェント情報が変更設定された等のように、ユーザエージェント情報のフォーマットや内容が事前に変更設定されていたとしても、これを検知することなく、任意の端末装置を操作しているユーザが正当なユーザか否かを判断することができる。
【００１７】
また、個々の端末装置に割り当てされるＩＰアドレスはアクセスの都度相違する可能性があるものの、個々のプロバイダが端末への割り当て用に保有しているＩＰアドレス（グローバルＩＰアドレス）は一定の範囲内でかつ個々のプロバイダ毎に相違しており、個々の端末装置は各々一定のプロバイダを経由してアクセスするので、個々の端末装置がアクセスの都度割り当てされるＩＰアドレスは常に同一ではないものの、例えば上位数ビットは常に一定等のように一致度が高い。
【００１８】
上記に基づき第１の発明では、端末装置より受信したパケットからユーザエージェント情報全体に及びアクセス元ＩＰアドレスを各々抽出し、抽出したアクセス元ＩＰアドレス及びユーザエージェント情報全体をユーザ識別情報と対応付けて記憶手段に各々記憶させておき、任意の端末装置より受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が、任意の端末装置を操作しているユーザのユーザ識別情報全体と対応付けて記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを各々判定することで、任意の端末装置を操作しているユーザが正当なユーザか否かを判断している。更に、判断手段は、受信したパケット

から抽出されたアクセス元ＩＰアドレスについては、記憶手段に記憶されているアクセス元ＩＰアドレスとの所定ビット単位の一致率が閾値以上か否かを判定することで、受信したパケットから抽出されたアクセス元ＩＰアドレスが記憶手段に記憶されているアクセス元ＩＰアドレスと対応しているか否かを判定し、受信したパケットから抽出されたユーザエージェント情報全体については、記憶手段に記憶されているユーザエージェント情報全体と同一か否かを判定することで、受信したパケットから抽出されたユーザエージェント情報全体が記憶手段に記憶されているユーザエージェント情報全体と対応しているか否かを判定するように構成されている。これにより、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が、記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを正確に判定することができ、今回パケットを受信した端末装置が、同一のユーザによって過去に使用された端末装置か否かに基づいて、今回パケットを受信した端末装置を操作しているユーザが正当なユーザか否かを判断することができ、ユーザの利便性を損なうことなくユーザ確認の精度を向上させることができる。

【００１９】

また、第２の発明は、第１の発明において、個々のユーザが各々不定の端末装置からアクセスすることを許容するために、情報管理手段は、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合された結果、判断手段により、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応していないと判定された場合に、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体をユーザ識別情報と対応付けて記憶手段に追加記憶させ、判断手段は、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けられたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されている場合、任意の端末装置より受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々照合することで、任意の端末装置を操作しているユーザが正当なユーザか否かを判断することを特徴としている。

【００２０】

第２の発明では、個々のユーザが過去に使用していない新たな端末装置を介してアクセスしてきた場合、判断手段により、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が、記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と判定され、正当なユーザでないと判断されることになるが、この場合、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が、情報管理手段によってユーザ識別情報と対応付けて記憶手段に追加記憶される。そして判断手段は、端末装置を操作しているユーザのユーザ識別情報と対応付けられたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されている場合に、任意の端末装置より受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々照合することで、任意の端末装置を操作しているユーザが正当なユーザか否かを判断するので、上記の新たな端末装置を介しての次回以降のアクセスでは正当なユーザと判断されることになる。

【００２１】

このように、第２の発明では、個々のユーザが、例えば自宅に設置された端末装置や職場に設置された端末装置等の複数の端末装置のうちの所望の端末装置を用いてアクセスすることも可能となる。なお、個々のユーザが各々不定の端末装置からアクセスすることを許容した場合であっても、個々のユーザが使用する端末装置の数は限られていることが殆どであるので、毎回新たな端末装置を介してアクセスが行われることで、正当なユーザでないと毎回判断されることは極めて稀である。

【００２２】
なお、第２の発明において、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応していないと判定された場合、情報管理手段は、パケット送信元の端末装置を操作しているユーザが、判断手段と異なる方法によって正当なユーザであることが確認されたときにのみ、アクセス元ＩＰアドレス及びユーザエージェント情報全体を記憶手段に追加記憶させるようにしてもよい。
【００２３】
また、第２の発明において、判断手段は、例えば第３の発明として記載したように、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けられたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されている場合、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が、記憶手段に記憶されている複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体のうちの少なくとも１組のアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々対応していると判定した場合に、任意の端末装置を操作しているユーザが正当なユーザであると判断するように構成することができる。これにより、正当なユーザが複数台の端末装置を選択的に用いてアクセスを行う等の場合にも、正当なユーザを精度良く判断することができる。
【００２４】
また、第２の発明において、判断手段は、例えば第４の発明として記載したように、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けられたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されている場合、複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体の中に、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が存在していなかった場合に、任意の端末装置を操作しているユーザが正当なユーザでないと判断するように構成することができる。これにより、正当なユーザでない第三者がアクセスしてきた場合にも、過去のアクセスと比較してアクセス元ＩＰアドレス及びユーザエージェント情報全体の少なくとも一方が各々異なることに基づいて正当なユーザでないと判断することができ、正当なユーザでない第三者を精度良く判断することができる。
【００２５】
なお、第４の発明において、パケット送信元の端末装置を操作しているユーザが正当なユーザであっても、例えば多数台の端末装置の中から毎回異なる端末装置を用いてアクセスしている場合や、一定の端末装置を用いてアクセスしているものの、アクセスに用いている端末装置がノート型ＰＣ等の携帯型の端末装置であり、毎回異なるホットスポット（HOTSPOT：公衆無線ＬＡＮを利用可能な場所）を利用してアクセスしている場合等のように、利用環境が特殊である場合には、記憶手段に記憶されている複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体の中に、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が存在していないことで、正当なユーザでないと判断されるという不都合が生ずる。
【００２６】
上記を考慮すると、第４の発明において、例えば第５の発明として記載したように、情報管理手段は、判断手段によって正当なユーザでないと判断されたユーザが、判断手段によるユーザ確認と異なる確認方法によって正当なユーザであると判断されたことが通知された場合、所定の識別情報をユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させ、判断手段は、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けられて記憶手段に所定の識別情報が記憶されており、かつ、複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体の中に、受信したパケットから抽出されたアクセス元ＩＰアドレスと対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情

報全体の組が複数存在しているか、又は、受信したパケットから抽出されたユーザエージェント情報全体と対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が複数存在している場合に、任意の端末装置を操作しているユーザが正当なユーザであると判断するように構成することが好ましい。

【００２７】

第５の発明では、判断手段によって正当なユーザでないと判断されたユーザが、判断手段によるユーザ確認と異なる確認方法によって正当なユーザであると判断されたことが通知された場合、当該ユーザの利用環境が特殊であるとみなして、所定の識別情報をユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させる。そして、記憶手段に所定の識別情報が記憶されているユーザについては、複数組のアクセス元ＩＰアドレス及びユーザエージェント情報の中に、受信したパケットから抽出されたアクセス元ＩＰアドレスと対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が複数存在しているか、又は、受信したパケットから抽出されたユーザエージェント情報全体と対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が複数存在している場合に、任意の端末装置を操作しているユーザが正当なユーザであると判断している。

【００２８】

これにより、例えば正当なユーザが多数台の端末装置の中から毎回異なる端末装置を用いてアクセスしている等の場合には、記憶されている複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体の中に、受信したパケットから抽出されたアクセス元ＩＰアドレスと対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が複数存在していることに基づいて、正当なユーザであると判断することができる。また、正当なユーザが携帯型の端末装置を用い、毎回異なるホットスポットを利用してアクセスしている等の場合には、記憶されている複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体の中に、受信したパケットから抽出されたユーザエージェント情報全体と対応していると判定したアクセス元ＩＰアドレス及びユーザエージェント情報全体の組が複数存在していることに基づいて、正当なユーザであると判断することができる。従って、第５の発明によれば、ユーザの利用環境が特殊である場合にもユーザ確認を精度良く行うことができる。

【００２９】

また、第１の発明において、例えば第６の発明として記載したように、個々のユーザが使用している電子メールアドレスを個々のユーザのユーザ識別情報と対応付けて各々記憶する電子メールアドレス記憶手段と、判断手段により、任意の端末装置を操作しているユーザが正当なユーザでないと判断された場合に、判断手段と異なる方法によって前記ユーザが正当なユーザか否かを確認するための所定のウェブページへのリンクが付加された電子メールを、前記ユーザのユーザ識別情報と対応付けて電子メールアドレス記憶手段に記憶されている電子メールアドレスへ送信する送信手段と、を更に設けることが好ましい。これにより、判断手段によって正当なユーザでないと判断されたユーザが、判断手段と異なる方法によって正当なユーザか否かの確認を受けるための操作が簡単になり、正当なユーザでないと判断されたユーザの負担を軽減することができる。

【００３０】

また、第２の発明において、情報管理手段を、例えば第７の発明として記載したように、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々照合された結果、判断手段により、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体の何れとも対応していないと判定され、かつ、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体の組の数が所定の上限値に達している場合に、前記受信したパケットから抽出されたアクセス元Ｉ

Ｐアドレス及びユーザエージェント情報全体を、記憶手段に記憶されている複数組のアクセス元ＩＰアドレス及びユーザエージェント情報全体のうち、記憶手段へ記憶させた時期が最も古いアクセス元ＩＰアドレス及びユーザエージェント情報全体の組に上書きして記憶手段に記憶させるように構成してもよい。

【００３１】

これにより、個々のユーザについて、アクセス元ＩＰアドレス及びユーザエージェント情報全体の組が上限値を越えて記憶手段に記憶されることが防止され、記憶手段の記憶容量を節減できると共に、判断手段が、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合するアクセス元ＩＰアドレス及びユーザエージェント情報全体の組の数も上限値以下になるので、判断手段に多大な負荷が加わることも防止することができる。

【００３２】

なお、第７の発明において、判断手段により、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体の何れとも対応していないと判定され、かつ、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体の組の数が所定の上限値に達している場合、情報管理手段は、パケット送信元の端末装置を操作しているユーザが、判断手段と異なる方法によって正当なユーザであることが確認されたときにのみ、受信したパケットから抽出された新たなアクセス元ＩＰアドレス及びユーザエージェント情報全体を記憶手段に上書き記憶させるようにしてもよい。

【００３３】

一方、第７の発明において、判断手段により、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体の何れとも対応していないと判定され、かつ、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体の組の数が所定の上限値に達している場合に、情報管理手段が、新たなアクセス元ＩＰアドレス及びユーザエージェント情報全体を無条件に（前述のように、判断手段と異なる方法によって正当なユーザであることが確認されたか否かに拘わらず）上書き記憶させた場合、新たなアクセス元ＩＰアドレス及びユーザエージェント情報全体が不正アクセスに対応する情報であったときには、正当なユーザに対応する情報が上書きされて消去される可能性があるが、この場合、正当なユーザからのアクセスで「正当なユーザでない」と判断されることで、不正アクセスがあったことを検知できるという効果が得られる。

【００３４】

また、第２の発明において、情報管理手段は、例えば第８の発明として記載したように、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と各々照合された結果、判断手段により、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体が記憶手段に複数組記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体のうちアクセス元ＩＰアドレス及びユーザエージェント情報全体の特定の組に対応していると判定された場合に、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体のうちの少なくともユーザエージェント情報全体を、アクセス元ＩＰアドレス及びユーザエージェント情報全体の特定の組に上書きして記憶手段に記憶させることが好ましい。

【００３５】

前述のように、ユーザエージェント情報は、ブラウザ等のアプリケーションのデフォルトの設定が用いられている場合は、ＯＳやブラウザに新たなパッチが当てられたりバージョンアップや入れ替えが行われた場合に内容が変更され、所望の文字列がユーザエージェント情報として送信されるようにユーザによって設定されている場合は、ユーザエージェ

ント情報として送信する文字列を変更する操作がユーザによって行われると内容が変更されるが、内容が一旦変更された後は当分の間内容は変更されない。このため、上記のように、受信したパケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体のうちの少なくともユーザエージェント情報全体を、対応していると判断されたアクセス元ＩＰアドレス及びユーザエージェント情報全体の特定の組に上書きして記憶手段に記憶させることで、少なくともユーザエージェント情報全体については最新の情報が記憶手段に記憶されることになり、以降のユーザ確認の精度を向上させることができる。なお、第８の発明において、受信したパケットから抽出されたアクセス元ＩＰアドレスについても、ユーザエージェント情報全体と共に上書きして記憶させるようにしてもよいことは言うまでもない。

【００３６】

第９の発明に係るユーザ確認方法は、抽出手段が、インターネット層のプロトコルとしてＩＰが適用され、アプリケーション層のプロトコルとしてＨＴＴＰが適用されて端末装置より受信したパケットから、当該パケットのＨＴＴＰヘッダに設定されているユーザエージェント情報全体を抽出すると共に、前記パケットからアクセス元ＩＰアドレスを抽出し、情報管理手段が、個々のユーザが操作する端末装置より受信したパケットから前記抽出手段によって各々抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、前記個々のユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させ、判断手段が、任意の端末装置より受信したパケットから前記抽出手段によって抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、前記任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて前記記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合し、前記記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを各々判定することで、前記任意の端末装置を操作しているユーザが正当なユーザか否かを判断すると共に、前記判断手段が、前記受信したパケットから抽出されたアクセス元ＩＰアドレスについては、前記記憶手段に記憶されているアクセス元ＩＰアドレスとの所定ビット単位の一致率が閾値以上か否かを判定することで、前記受信したパケットから抽出されたアクセス元ＩＰアドレスが前記記憶手段に記憶されているアクセス元ＩＰアドレスと対応しているか否かを判定し、前記受信したパケットから抽出されたユーザエージェント情報全体については、前記記憶手段に記憶されているユーザエージェント情報全体と同一か否かを判定することで、前記受信したパケットから抽出されたユーザエージェント情報全体が前記記憶手段に記憶されているユーザエージェント情報と対応しているか否かを判定することを特徴としているので、第１の発明と同様に、ユーザの利便性を損なうことなくユーザ確認の精度を向上させることができる。

【００３７】

第１０の発明に係るユーザ確認プログラムは、記憶手段を備えたコンピュータを、インターネット層のプロトコルとしてＩＰが適用され、アプリケーション層のプロトコルとしてＨＴＴＰが適用されて端末装置より受信したパケットから、当該パケットのＨＴＴＰヘッダに設定されているユーザエージェント情報全体を抽出すると共に、前記パケットからアクセス元ＩＰアドレスを抽出する抽出手段、個々のユーザが操作する端末装置より受信したパケットから前記抽出手段によって各々抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、前記個々のユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させる情報管理手段、及び、任意の端末装置より受信したパケットから前記抽出手段によって抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報全体を、前記任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて前記記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合し、前記記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを各々判定することで、前記任意の端末装置を操作しているユーザが正当なユーザか否かを判断する判断手段として機能させ、前記判断手段は、前記受信したパケットから抽出されたアクセス元ＩＰアドレスについては、前記記憶手段に記憶されている

アクセス元ＩＰアドレスとの所定ビット単位の一致率が閾値以上か否かを判定することで、前記受信したパケットから抽出されたアクセス元ＩＰアドレスが前記記憶手段に記憶されているアクセス元ＩＰアドレスと対応しているか否かを判定し、前記受信したパケットから抽出されたユーザエージェント情報全体については、前記記憶手段に記憶されているユーザエージェント情報全体と同一か否かを判定することで、前記受信したパケットから抽出されたユーザエージェント情報全体が前記記憶手段に記憶されているユーザエージェント情報と対応しているか否かを判定することを特徴としている。

【００３８】

第１０の発明に係るユーザ確認プログラムは、記憶手段を備えたコンピュータを、上記の抽出手段、情報管理手段及び判断手段として機能させるためのプログラムであるので、コンピュータが第１０の発明に係るユーザ確認プログラムを実行することで、前記コンピュータが第１の発明のユーザ確認装置として機能することになり、第１の発明と同様に、ユーザの利便性を損なうことなくユーザ確認の精度を向上させることができる。

【発明の効果】

【００３９】

以上説明したように本発明は、端末装置より受信したパケットからユーザエージェント情報全体及びアクセス元ＩＰアドレスを抽出し、抽出したアクセス元ＩＰアドレス及びユーザエージェント情報全体を個々のユーザのユーザ識別情報と対応付けて記憶手段に各々記憶させ、任意の端末装置より受信したパケットから抽出したアクセス元ＩＰアドレス及びユーザエージェント情報全体を、任意の端末装置を操作しているユーザのユーザ識別情報と対応付けて記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と照合し、記憶手段に記憶されているアクセス元ＩＰアドレス及びユーザエージェント情報全体と対応しているか否かを各々判定することで、任意の端末装置を操作しているユーザが正当なユーザか否かを判断すると共に、受信したパケットから抽出されたアクセス元ＩＰアドレスについては、記憶手段に記憶されているアクセス元ＩＰアドレスとの所定ビット単位の一致率が閾値以上か否かを判定することで、受信したパケットから抽出されたアクセス元ＩＰアドレスが前記記憶手段に記憶されているアクセス元ＩＰアドレスと対応しているか否かを判定し、受信したパケットから抽出されたユーザエージェント情報全体については、記憶手段に記憶されているユーザエージェント情報全体と同一か否かを判定することで、受信したパケットから抽出されたユーザエージェント情報全体が前記記憶手段に記憶されているユーザエージェント情報全体と対応しているか否かを判定するので、ユーザの利便性を損なうことなくユーザ確認の精度を向上させることができる、という優れた効果を有する。

【図面の簡単な説明】

【００４０】

【図１】本実施形態に係るコンピュータ・システムの概略構成を示すブロック図である。

【図２】クライアント端末からサーバへのＨＴＴＰデータの送信において、各レイヤでのヘッダの付加及び除去を説明する概念図である。

【図３】アプリケーション・サーバによって行われるユーザ認証処理の内容を示すフローチャートである。

【図４】使用履歴情報の内容を示す概略図である。

【図５】使用履歴情報に基づく認証ＯＫ／ＮＧの判定条件を示す図表である。

【図６】再認証要請メールの一例を示すイメージ図である。

【図７】使用履歴テーブル更新処理の内容を示すフローチャートである。

【図８】確認メールの一例を示すイメージ図である。

【発明を実施するための形態】

【００４１】

以下、図面を参照して本発明の実施形態の一例を詳細に説明する。図１には本実施形態に係るコンピュータ・システム１０が示されている。本実施形態に係るコンピュータ・システム１０は、特定金融機関に設置されたウェブサーバ１２を含んで構成されている。ウ

ェブサーバ１２は、ＣＰＵ１２Ａ、ＲＡＭ等から成るメモリ１２Ｂ、ハードディスクドライブ（ＨＤＤ）１２Ｃ、ネットワークインタフェース（Ｉ／Ｆ）部１２Ｄを備えている。ＨＤＤ１２Ｃには認証情報データベース（ＤＢ）及び使用履歴テーブル（何れも詳細は後述）が記憶されており、本発明に係る記憶手段に対応している。また、ＨＤＤ１２ＣにはＣＰＵ１２Ａが後述するユーザ認証処理を行うためのユーザ認証プログラムがインストールされている。なお、ユーザ認証プログラムは第１０の発明のユーザ確認プログラムに対応しており、ＣＰＵ１２Ａがユーザ認証プログラムを実行することで、ウェブサーバ１２は本発明に係るユーザ確認装置として機能する。

【００４２】

また、ウェブサーバ１２のネットワークＩ／Ｆ部１２Ｄは、多数台のウェブサーバが通信回線を介して相互に接続されて成るコンピュータ・ネットワーク（インターネット）１６に直接接続されており、更に特定金融機関内に設置されたイントラネット（ＬＡＮ）２６にも接続されている。イントラネット２６には勘定系システム２８が接続されている。インターネット１６には、各々ＰＣ等から成る多数台のクライアント端末１８が接続されている。個々のクライアント端末１８にはブラウザがインストールされており、本発明に係る端末装置に対応している。なお、個々のクライアント端末１８のインターネット１６への接続形態は、符号「１８Ａ」を付したクライアント端末のように、インターネット１６に直接接続される（詳しくは図示しないプロバイダを介して接続される）場合もあれば、符号「１８Ｂ」を付したクライアント端末のように、企業内に設置されプロクシサーバ２２を介してインターネット１６に接続される場合もある。

【００４３】

次に本実施形態の作用を説明する。本実施形態に係る特定金融機関は、特定金融機関に口座を開設しているユーザがオンラインで金融取引を行うことを可能とするサービスとして、ウェブサーバ１２によって運営されるオンライン金融取引用ウェブサイトを利用してユーザからのオンラインでの金融取引の実行指示を受け付けるオンライン金融取引受付サービスを提供している。このオンライン金融取引受付サービスを利用した金融取引では、ユーザがクライアント端末１８を介してオンライン金融取引用ウェブサイトのウェブページを閲覧し、該ウェブページ上で必要な情報を入力することで、ユーザが所望している金融取引の実行を指示するための情報（金融取引指示情報）がクライアント端末１８からウェブサーバ１２へ送信される。そして、この金融取引指示情報がウェブサーバ１２からイントラネット２６に接続された勘定系システム２８等へ転送されることで、金融取引指示情報に基づいてユーザから指示された金融取引が勘定系システム２８等によって実行されるようになっている。

【００４４】

オンライン金融取引受付サービスを利用するユーザは、事前に前記サービスの利用を特定金融機関へ申請する。特定金融機関は、ユーザから前記サービスの利用が申請される毎に前記ユーザへユーザＩＤ（本発明に係るユーザ識別情報に相当）を付与し、付与したユーザＩＤを、ユーザが設定したパスワード（本発明に係る認証情報に相当）及びユーザから通知された電子メールアドレス（ユーザが使用している電子メールアドレス）と共に、ウェブサーバ１２のＨＤＤ１２Ｃに記憶されている認証情報ＤＢに登録する。このように、ＨＤＤ１２Ｃは第６の発明の電子メールアドレス記憶手段に対応している。

【００４５】

次に、ユーザがクライアント端末１８を介してオンライン金融取引用ウェブサイトへのアクセスを指示した際に、クライアント端末１８からウェブサーバ１２へ送信されるパケットについて説明する。なお、インターネット１６経由でのクライアント端末１８とウェブサーバ１２との間の通信では、インターネット層のプロトコルとしてＩＰが適用され、トランスポート層のプロトコルとしてＴＣＰ（Transmission Control Protocol）が適用され、アプリケーション層のプロトコルとしてＨＴＴＰが適用される。オンライン金融取引用ウェブサイトへのアクセスの指示は、クライアント端末１８上でブラウザが起動されている状態で、ユーザがクライアント端末１８の入力装置を操作してオンライン金融取引

用ウェブサイトのＵＲＬ(Uniform Resource Locator)を指定する等の操作を行うことによって為される。

【００４６】

オンライン金融取引用ウェブサイトへのアクセスが指示されると、アプリケーション層に対応する処理を行うアプリケーション・プログラムであるブラウザは、指定されたＵＲＬに対応するウェブページの配信をウェブサーバ１２に要求するために必要な情報を設定したＨＴＴＰデータを生成すると共に、当該ＨＴＴＰデータの先頭に、アプリケーション層に対応する情報を設定したＨＴＴＰヘッダを付加する（図２参照）。なお、クライアント端末１８からウェブサーバ１２へ後述する認証要求パケットが送信される場合、ＨＴＴＰデータには、ユーザがクライアント端末１８を介して入力したユーザＩＤやパスワードを含む情報が設定される。また、ＨＴＴＰヘッダに設定される情報にはユーザエージェント情報が含まれており、ブラウザのデフォルトの設定では、このユーザエージェント情報として、クライアント端末１８上で動作しているＯＳやブラウザ自身のバージョン、パッチがどこまで当たっているか等を表す情報が設定される。また、ユーザエージェント情報として任意の文字列を固定的に設定するようにブラウザの設定を変更することも可能であり、このような設定変更が行われていた場合、事前に指定された文字列がユーザエージェント情報として設定される。

【００４７】

また、クライアント端末１８上では、トランスポート層、インターネット層及びネットワークインタフェース層の各レイヤに対応する処理を行う処理モジュールも各々動作しており、図２に示すように、ブラウザによって生成された情報（ＨＴＴＰヘッダを付加したＨＴＴＰデータ）は上位レイヤの処理モジュールから下位レイヤの処理モジュールへ順に引き渡され、各レイヤの処理モジュールは各レイヤに対応する処理を行うと共に、引き渡された情報の先頭に、各レイヤに対応する情報を設定したヘッダを付加する処理を順次行う。これにより、クライアント端末１８からは、ネットワークインタフェース層に対応するネットワークヘッダ、インターネット層に対応するＩＰヘッダ、トランスポート層に対応するＴＣＰヘッダ及びアプリケーション層に対応するＨＴＴＰヘッダが各々付加されたＨＴＴＰデータがウェブサーバ１２へパケットとして送信される。

【００４８】

なお、ＩＰヘッダには、インターネット層に対応する処理モジュールにより、インターネット層に対応する情報としてパケットの宛先を示す宛先ＩＰアドレスや送信元ＩＰアドレス（クライアント端末１８に付与されたＩＰアドレス）等の情報が設定され、ＴＣＰヘッダには、トランスポート層に対応する処理モジュールにより、トランスポート層に対応する情報としてＴＣＰポート番号等の情報が設定される。

【００４９】

また、ウェブサーバ１２上でも各レイヤの処理モジュールが各々動作しており、クライアント端末１８からのパケットは下位レイヤの処理モジュールから上位レイヤの処理モジュールへ順に引き渡され、各レイヤの処理モジュールは、引き渡されたパケットの先頭に付加されている各レイヤに対応するヘッダを参照し、当該ヘッダに設定されている情報に基づいて各レイヤに対応する処理を行った後に前記ヘッダを除去する処理を順次行う。これにより、ウェブサーバ１２上で動作するアプリケーション層の処理モジュール（この処理モジュールには、後述するユーザ認証処理を行う処理モジュールも含まれる）には、先頭にＨＴＴＰヘッダのみが付加されたＨＴＴＰデータが引き渡される。

【００５０】

なお、後述するユーザ認証処理では、ウェブサーバ１２がクライアント端末１８から受信したパケットのＩＰヘッダに設定されている送信元ＩＰアドレス（アクセス元ＩＰアドレス）を用いて処理を行うが、ユーザ認証処理を行う処理モジュールがパケットを受け取る時点では既にＩＰヘッダが除去されているので、そのままでは送信元ＩＰアドレスを検知できない。このため、ウェブサーバ１２上で動作するインターネット層の処理モジュールは、クライアント端末１８から受信したパケットのＩＰヘッダに設定されている送信元

ＩＰアドレスをＨＴＴＰデータに付加する等の処理を行うことで、アプリケーション層の処理モジュール（ユーザ認証処理を行う処理モジュール）へ送信元ＩＰアドレスを伝達する。

【００５１】

ウェブサーバ１２では、インターネット１６経由でクライアント端末１８から何らかのパケットを受信した場合、ウェブサーバ１２上で動作する所定の処理モジュール（この処理モジュールもアプリケーション層に対応する処理モジュールである）により、ＨＴＴＰデータに所定の情報が設定されているか否か等に基づいて、クライアント端末１８から受信したパケットが認証要求パケットか否かが判定される。

【００５２】

オンライン金融取引用ウェブサイトは、リンクによって互いに関連付けられた多数のウェブページの集合体であり、上記ウェブサイトのホームページからリンクを辿っていくことで、ユーザが実行を所望している金融取引の条件を指定して実行を指示することが可能な金融取引実行指示ページが表示されるが、オンライン金融取引用ウェブサイトのホームページには、ユーザＩＤやパスワードを入力するための入力欄が設けられており、ユーザに対してログイン操作（ユーザＩＤやパスワードの入力）を促すメッセージも表示されている。そして、ユーザがホームページの対応する入力欄にユーザＩＤ及びパスワードを入力して送信を指示すると、ユーザが操作しているクライアント端末１８からＨＴＴＰデータに所定の情報が設定された認証要求パケットが送信される。

【００５３】

所定の処理モジュールは、クライアント端末１８から受信したパケットが認証要求パケットでないと判定した場合、受信したパケットに応じた処理、例えばオンライン金融取引用ウェブサイトのホームページのデータを要求元のクライアント端末１８へ配信するためのＨＴＴＰデータを生成し、生成したＨＴＴＰデータにＨＴＴＰヘッダを付加する等の処理を行う。このＨＴＴＰデータ及びＨＴＴＰヘッダは、図２に示すプロセスと逆のプロセスを経てクライアント端末１８へパケットとして送信される。これにより、クライアント端末１８のディスプレイには、クライアント端末１８を介してユーザが配信を要求したウェブページが表示される。

【００５４】

一方、クライアント端末１８から受信したパケットが認証要求パケットであると判定した場合、所定の処理モジュールはユーザ認証処理を行う処理モジュールを起動する。これにより、ＣＰＵ１２Ａによってユーザ認証プログラムが実行され、図３に示すユーザ認証処理が行われる。

【００５５】

このユーザ認証処理では、まずステップ３０において、受信した認証要求パケットのＨＴＴＰデータからユーザＩＤ及びパスワードを抽出し、次のステップ３２において、ステップ３０で抽出したユーザＩＤとパスワードの組合わせが認証情報ＤＢに登録されているか否を検索する認証処理を行う。ステップ３４では、ステップ３２の検索によってユーザＩＤとパスワードの組合わせが認証情報ＤＢから抽出されたか否かに基づいて、ステップ３２の認証処理で認証に成功したか否か判定する。判定が否定された場合はステップ７４へ移行し、起動元の所定の処理モジュールへ認証失敗を通知してユーザ認証処理を終了する。この場合、所定の処理モジュールにより、認証要求パケット送信元のクライアント端末１８のディスプレイに、入力されたユーザＩＤ又はパスワードが誤っている旨を通知するメッセージを表示させる等のエラー処理が行われる。

【００５６】

一方、ステップ３２の認証処理で認証に成功した場合には、ステップ３４の判定が肯定されてステップ３６へ移行し、受信した認証要求パケットのＨＴＴＰデータからアクセス元ＩＰアドレス（送信元ＩＰアドレス）を抽出すると共に、認証要求パケットのＨＴＴＰヘッダからユーザエージェント情報を抽出する。なお、このステップ３６は本発明に係る抽出手段に対応している。また、次のステップ３８では、ＨＤＤ１２Ｃに記憶されている

使用履歴テーブルから、先のステップ３０で抽出されたユーザＩＤに対応する使用履歴情報を抽出し、抽出した使用履歴情報をメモリ１２Ｂに記憶させる。

【００５７】

本実施形態に係る使用履歴テーブルは、オンライン金融取引受付サービスの利用を事前に申請しユーザＩＤが付与されている個々のユーザ（正当なユーザ）について、図４に示すような使用履歴情報を記憶するための領域が各々設けられて構成されており、個々のユーザに対応する使用履歴情報記憶領域には、顧客ＩＤ、取引停止フラグ、特殊環境フラグ、照合判定用閾値、インデックスの各情報を設定／登録するための領域が設けられ、更にアクセス元ＩＰアドレス及びユーザエージェント情報を２組登録可能な領域が設けられている。

【００５８】

顧客ＩＤ領域には顧客マスタに登録されている口座番号からハッシュ関数を用いて生成された顧客ＩＤが事前に登録される。また、取引停止フラグは通常ルートでの認証（アクセス元ＩＰアドレス及びユーザエージェント情報に基づく認証）を停止するか否かを表すフラグであり、取引停止フラグ領域には当初、取引停止フラグの初期値である０（通常ルートでの認証有効を意味する）が設定される。また、特殊環境フラグはユーザの利用環境が特殊か否かを表すフラグであり、特殊環境フラグ領域には当初、特殊環境フラグの初期値である０（通常環境を意味する）が設定される。またインデックスidは、使用履歴情報として登録された２組のアクセス元ＩＰアドレス及びユーザエージェント情報(IP0,UA0及びIP1,UA1)のうちの何れが最新かを表す情報であり、インデックス領域には当初、初期値０(IP0,UA0が最新であることを表す)が設定される。また、個々のアクセス元ＩＰアドレス領域及びユーザエージェント情報領域には初期値として空白（情報無し）が各々設定される。

【００５９】

前述のステップ３８では、先のステップ３０で抽出されたユーザＩＤをキーに顧客マスタ（図示省略）を検索することで、前記ユーザＩＤが付与されたユーザが保有している口座の口座番号を抽出し、抽出した口座番号からハッシュ関数を用いて顧客ＩＤを求め、求めた顧客ＩＤをキーにして使用履歴テーブルを検索することで、ユーザＩＤに対応する使用履歴情報を抽出する。次のステップ４０では、抽出した使用履歴情報のうちの取引停止フラグが１か否か判定する。判定が否定された場合はステップ４２へ移行し、抽出した使用履歴情報にアクセス元ＩＰアドレス及びユーザエージェント情報が１組以上登録されているか否か判定する。

【００６０】

前述のように、使用履歴情報領域のうちのアクセス元ＩＰアドレス領域及びユーザエージェント情報領域には初期値として空白が設定されるが、オンライン金融取引受付サービスの利用を申請したユーザによって、オンライン金融取引用ウェブサイトへのアクセスが１回以上行われると、ステップ３６で認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報が使用履歴情報として登録される（詳細は後述）。使用履歴情報としてアクセス元ＩＰアドレス及びユーザエージェント情報が既に登録されている場合はステップ４２の判定が肯定されてステップ４４へ移行し、ステップ３６で認証要求パケットから抽出したアクセス元ＩＰアドレス及びユーザエージェント情報を、使用履歴情報として登録されているアクセス元ＩＰアドレス及びユーザエージェント情報と照合する。

【００６１】

なお、ＩＰアドレスの照合は以下のようにして行われる。すなわち、ＩＰアドレスは４バイトのデータであるが、本実施形態では、アクセス元ＩＰアドレス領域へのアクセス元ＩＰアドレスの登録に際し、１バイト毎にハッシュ関数を用いてハッシュ値が演算され、４個のハッシュ値がアクセス元ＩＰアドレスとして登録される。このため、ステップ３６で抽出したアクセス元ＩＰアドレスについても１バイト毎にハッシュ値を演算し、得られた４個のハッシュ値をアクセス元ＩＰアドレス領域に登録されている４個のハッシュ値と

比較し、ハッシュ値単位での一致率を求める。そして、求めた一致率を使用履歴情報として設定されている照合判定用閾値と比較し、一致率が閾値以上の場合は、今回のアクセス元ＩＰアドレスが登録されているＩＰアドレスと「対応している」と判定し、一致率が閾値未満の場合は、今回のアクセス元ＩＰアドレスが登録されているＩＰアドレスと「対応していない」と判定する。

【００６２】

図１に示すクライアント端末１８Ａのように、インターネット１６に直接接続される形態において、クライアント端末１８ＡのＩＰアドレス（グローバルＩＰアドレス）は、プロバイダとの契約により予め固定されている場合と、インターネット１６へ接続する度にプロバイダによって不定のＩＰアドレス（プロバイダが割り当て用に事前に確保している一定範囲内のＩＰアドレスのうちの何れか）が割り当てされる場合がある。また、図１に示すクライアント端末１８Ｂのように、企業内に設置されプロクシサーバ２２を介してインターネット１６に接続される接続形態において、例えば前記企業が独自ドメインを取得し、割り当て用に一定範囲内のＩＰアドレスを事前に確保している場合、クライアント端末１８Ｂから送信されたパケットは、ＩＰヘッダに設定されている送信元ＩＰアドレスが、プロクシサーバ２２によって割り当て用に前記企業が事前に確保している一定範囲内のＩＰアドレスのうちの何れかのＩＰアドレスで上書きされた後にインターネット１６へ送出される。

【００６３】

従って、割り当てされるＩＰアドレスが不定のクライアント端末１８であっても、割り当てされるＩＰアドレスは一定の範囲内に収まっている（上位数バイトは同一である）ので、上記のようにＩＰアドレスの一致率が閾値以上か否かに基づいて、ＩＰアドレスが対応しているか否かを判定することで、オンライン金融取引用ウェブサイトが以前にアクセスされた際と同一のアクセス元（インターネット１６上でのクライアント端末１８の所在）からオンライン金融取引用ウェブサイトがアクセスされた場合に、ＩＰアドレスが対応していると判定することができる。

【００６４】

なお、ユーザエージェント情報については、今回のユーザエージェント情報が登録されているユーザエージェント情報と同一であれば「対応している」と判定し、今回のユーザエージェント情報が登録されているユーザエージェント情報と同一でなければ「対応していない」と判定する。アクセス元ＩＰアドレス及びユーザエージェント情報の照合で上記の判定を行うことは第１の発明に対応している。また、使用履歴情報としてアクセス元ＩＰアドレス及びユーザエージェント情報が２組登録されている場合には、認証要求パケットから抽出したアクセス元ＩＰアドレス及びユーザエージェント情報を、登録されている２組のアクセス元ＩＰアドレス及びユーザエージェント情報と各々照合する。

【００６５】

次のステップ４６では、ステップ４４におけるアクセス元ＩＰアドレス及びユーザエージェント情報の照合結果に基づいて、認証要求パケット送信元のクライアント端末１８を操作しているユーザに対する認証が「成功」「条件付き成功」「失敗」の何れかに該当するかを判定し、判定結果に応じて分岐する。上記判定は図５に示す判定表に従って行われる。なお、図５における「○」はステップ４４の照合で「対応している」と判定された場合に、「×」は「対応していない」と判定された場合に各々対応している。また、図５における「最新」のアクセス元ＩＰアドレス及びユーザエージェント情報は、使用履歴情報として登録されている２組のアクセス元ＩＰアドレス及びユーザエージェント情報のうち、使用履歴情報のインデックスidが指し示しているアクセス元ＩＰアドレス及びユーザエージェント情報を表し、「以前」のアクセス元ＩＰアドレス及びユーザエージェント情報は、他方のアクセス元ＩＰアドレス及びユーザエージェント情報を表している。また、使用履歴情報として１組のアクセス元ＩＰアドレス及びユーザエージェント情報（「最新」の情報）のみが登録されている場合には、「以前」のアクセス元ＩＰアドレス及びユーザエージェント情報との照合結果が何れも「対応していない」と判定されたものとしてステ

ップ４６の判定が行われる。なお、上記のステップ４４，４６は、後述するステップ６４と共に本発明に係る判断手段（詳しくは第１～５の発明の判断手段）に対応している。

【００６６】

先のステップ４４における照合結果が、「認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報が、使用履歴情報として登録されている２組のアクセス元ＩＰアドレス及びユーザエージェント情報のうち、少なくとも１組のアクセス元ＩＰアドレス及びユーザエージェント情報と各々対応している」という条件（便宜上、第１の条件と称する）を満たす結果であった場合、今回のアクセスは、同一のユーザが過去にオンライン金融取引用ウェブサイトをアクセスした際と、アクセス元が同一でかつクライアント端末１８も同一とみなすことができるので、認証要求パケット送信元のクライアント端末１８を操作しているユーザも正当なユーザである可能性が極めて高い。このため、ステップ４６では上記場合に、図５に「認証ＯＫ」と表記して示すように認証が「成功」と判定する。

【００６７】

一方、先のステップ４４における照合結果が、「使用履歴情報として登録されているアクセス元ＩＰアドレス及びユーザエージェント情報の組の中に、認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報と各々対応していると判定された組が存在していない」という条件（便宜上、第２の条件と称する）を満たす結果であった場合、今回のアクセスは、同一のユーザが過去にオンライン金融取引用ウェブサイトをアクセスした際と、アクセス元及びクライアント端末１８の少なくとも一方が各々相違しているので、認証要求パケット送信元のクライアント端末１８を操作しているユーザは正当なユーザでない可能性が高い。

【００６８】

但し、多数のユーザの中には、例えばオンライン金融取引用ウェブサイトのアクセスに利用可能なクライアント端末１８を多数台保有しており、多数台のクライアント端末１８の中から不定のクライアント端末１８を介してオンライン金融取引用ウェブサイトにアクセスしたり（この場合、各回のアクセスでユーザエージェント情報が互いに相違する可能性が高い）、ノート型ＰＣ等の携帯型のクライアント端末１８を用い、毎回異なるホットスポットを利用してオンライン金融取引用ウェブサイトへアクセスする（この場合、各回のアクセスでアクセス元ＩＰアドレスが大きく相違する可能性が高い）等のように、利用環境が特殊なユーザが存在している可能性があり、この種の利用環境が特殊なユーザも上記第２の条件に該当する。

【００６９】

このため、ステップ４６では、ステップ４４における照合結果が「使用履歴情報として登録されている２組のアクセス元ＩＰアドレス及びユーザエージェント情報の両方が、認証要求パケットから抽出されたアクセス元ＩＰアドレスと対応していると判定されるか、又は、認証要求パケットから抽出されたユーザエージェント情報と対応していると判定された」という条件（便宜上、第３の条件と称する）を満たす結果であった場合に、図５に「条件付き認証ＯＫ」と表記して示すように、認証を「条件付き成功」と判定し、ステップ４４における照合結果が前述の第２の条件を満たしかつ上記の第３の条件を満たさない場合に、図５に「認証ＮＧ」と表記して示すように、認証を「失敗」と判定する。

【００７０】

ステップ４６で認証「成功」と判定された場合はステップ４８へ移行し、使用履歴情報の特殊環境フラグが１か否か判定する。判定が否定された場合はステップ５２へ移行し、起動元の所定の処理モジュールへ認証成功を通知する。この場合、所定の処理モジュールにより、正当なユーザであることが確認されたユーザに対してのみ配信する所定のウェブページを、認証要求パケット送信元のクライアント端末１８へ配信する等の処理が行われる。次のステップ５４では、認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報が、使用履歴情報として登録されているアクセス元ＩＰアドレス及びユーザエージェント情報のうち、インデックスidが指し示している「最新」のアク

セス元ＩＰアドレス及びユーザエージェント情報に各々対応していると判定されたか否か判定する。

【００７１】

判定が肯定された場合はステップ６０へ移行し、認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報を、使用履歴情報として登録されている「最新」のアクセス元ＩＰアドレス及びユーザエージェント情報に上書きして登録し、ステップ６２へ移行する。また、ステップ５４の判定が否定された場合はステップ５６へ移行し、認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報を、使用履歴情報として登録されている「以前」のアクセス元ＩＰアドレス及びユーザエージェント情報（インデックスidが指し示していないアクセス元ＩＰアドレス及びユーザエージェント情報）に上書きして登録する（なお、上書きされるアクセス元ＩＰアドレス及びユーザエージェント情報が「空白」の場合、ステップ５６における上書き登録は第２の発明の「追加記憶」に相当する）。また、次のステップ５８ではインデックスidのビットを反転させることで、ステップ５６で上書きして登録したアクセス元ＩＰアドレス及びユーザエージェント情報を「最新」へ変更する。

【００７２】

そしてステップ６２では、メモリ１２Ｂ上に記憶している使用履歴情報を使用履歴テーブルに書き戻すことで、使用履歴テーブル上の使用履歴情報を更新し、ユーザ認証処理を終了する。なお、上記のステップ６０，５６のように、認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報を、使用履歴情報として登録されているアクセス元ＩＰアドレス及びユーザエージェント情報に上書きして登録することで、同一ユーザについて再度ユーザ認証処理が行われた際の、ステップ４４の照合及びステップ４６の判定の精度を向上させることができる。なお、上述したステップ５４～ステップ６２は本発明に係る情報管理手段（詳しくは第８の発明の情報管理手段）に対応している。

【００７３】

一方、先のステップ４６で認証が「失敗」と判定された場合はステップ６８へ移行し、使用履歴情報のうちの取引停止フラグに１を設定する。また、ステップ４６で認証が「失敗」と判定された場合にも、認証要求パケット送信元のクライアント端末１８を操作しているユーザが正当なユーザである可能性があり、これを考慮して次のステップ７０では、ステップ３２で抽出したユーザＩＤと対応付けて認証情報ＤＢに記憶されている電子メールアドレスを読み出し、読み出した電子メールアドレスへ再認証要請メールを送信する。例として図６に示すように、この再認証要請メールには、認証要求パケット送信元のクライアント端末１８を操作しているユーザを、通常ルートと異なる認証方法によって正当なユーザか否かを確認するための再認証専用のウェブページへのリンク１００が付加されている。なお、ステップ７０は第６の発明の送信手段に対応している。

【００７４】

次のステップ７２では起動元の所定の処理モジュールへ認証失敗を通知し、ステップ５４へ移行する。これにより、前述のように、認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報の使用履歴情報への上書き登録・使用履歴テーブルへの使用履歴情報の書き戻しが行われてユーザ認証処理を終了する。

【００７５】

上記のように、ステップ４６で認証が「失敗」と判定されると取引停止フラグに１が設定されるので、同一ユーザに対してユーザ認証処理が再度実行された場合、ステップ４０の判定が肯定されてステップ７０へ移行することで、通常ルートでの認証（アクセス元ＩＰアドレス及びユーザエージェント情報に基づく認証）は行われず、再認証要請メールが再度送信され（ステップ６８）、起動元の所定の処理モジュールへ認証失敗が再度通知される（ステップ７２）。従って、ステップ４６で認証が「失敗」と判定された前回のユーザ認証処理が、ユーザＩＤ及びパスワードを不正に取得した第三者による不正アクセスによって実行されていた場合、その後、正当なユーザがオンライン金融取引用ウェブサイト

にアクセスして認証を受けようとしても認証が「失敗」となってしまうことになるが、その代わりに不正アクセスがあったことを検知することができる。

【００７６】

また、認証要求パケット送信元のクライアント端末１８を操作しているユーザが正当なユーザであるにも拘わらず、前述のようにステップ４６で認証が「失敗」と判定された場合、当該ユーザは先のステップ７０で送信された再認証要請メールを受信し、受信した再認証要請メールに付加されているリンク１００から再認証専用のウェブページにアクセスする操作を行い、クライアント端末１８のディスプレイに表示された再認証専用のウェブページを介して所定の再認証手続きを受ける。この再認証手続きで正当なユーザであることが確認された場合、ユーザ認証処理を行う処理モジュールへ再認証成功が通知される。なお、再認証専用のウェブページにアクセスするためには、再認証要請メールを受信できる環境を有している必要があり、再認証専用のウェブページにアクセスして再認証手続きを受ける人は、その時点で正当なユーザである可能性が非常に高いとみなすことができるので、再認証手続きを比較的簡素な手続きとすることでユーザの負担を軽減することが可能である。

【００７７】

一方、ユーザ認証処理を行う処理モジュールは、再認証成功が通知されると、図７に示す使用履歴テーブル更新処理を行う。すなわち、上記の再認証通知には、再認証手続きによって正当なユーザであることが確認されたユーザのユーザＩＤが情報として付加されており、まずステップ８０では、正当なユーザであることが確認されたユーザのユーザＩＤを抽出・取得する。次のステップ８２では、ステップ８０で取得したユーザＩＤに対応する使用履歴情報を使用履歴テーブルから抽出し、抽出した使用履歴情報をメモリ１２Ｂに記憶させる。またステップ８４では、抽出した使用履歴情報のうち、取引停止フラグを０に戻すと共に、特殊環境フラグに１を設定する。そして、次のステップ８６で使用履歴情報を使用履歴テーブルへ書き戻し、使用履歴テーブル更新処理を終了する。上記のように取引停止フラグを０に戻すことで、同一ユーザに対してユーザ認証処理が再度実行された場合に、ステップ４０の判定が否定されることで通常ルートでの認証が再開されることになる。なお、ステップ８４は第５の発明の情報管理手段に対応している。

【００７８】

また、先のステップ４６で認証が「条件付き成功」と判定された場合はステップ６４へ移行し、使用履歴情報のうちの特殊環境フラグが１か否か設定する。認証が「条件付き成功」の場合、先に説明したように、認証要求パケット送信元のクライアント端末１８を操作しているユーザは利用環境が特殊なユーザである可能性が高いが、第三者による不正アクセスである可能性も否定できない。このため、本実施形態における「条件付き成功」は、前述の再認証手続きで認証に成功していることを認証成功の条件としており、ステップ６４の判定が否定された場合、すなわち再認証成功が通知されていない場合にはステップ６８へ移行し、前述の再認証要請メールの送信等の処理を行う。

【００７９】

また、ステップ６４の判定が肯定された場合、すなわち再認証成功が通知されて使用履歴テーブル更新処理（図７）を行っている場合にはステップ６６へ移行し、ステップ３２で抽出したユーザＩＤと対応付けて認証情報ＤＢに記憶されている電子メールアドレスを読み出し、読み出した電子メールアドレスへ例として図８に示すような確認メールを送信する。この確認メールには日時等が記載されており、今回のアクセスが万一不正アクセスであった場合にも、正当なユーザが上記の確認メールを受信・参照することで、不正アクセスがあったことを検知することができる。ステップ６６の処理を行うとステップ５２へ移行し、起動元の所定の処理モジュールへ認証成功を通知した後に、ステップ５４以降で認証要求パケットから抽出されたアクセス元ＩＰアドレス及びユーザエージェント情報の使用履歴情報への上書き登録・使用履歴テーブルへの使用履歴情報の書き戻しを行ってユーザ認証処理を終了する。これにより、使用環境が特殊なユーザであっても、正当なユーザと判定することができる。

【００８０】
なお、特殊環境フラグに１が設定されていると、ステップ４６の判定で前述の第３の条件を満足すると認証が「成功」と判定されるので、セキュリティ性が若干低下するという欠点がある。このため、ステップ４６の判定で第１の条件を満足して認証が「成功」と判定された場合、ステップ４８で特殊環境フラグに１が設定されているか否かを判定しており、判定が肯定された場合はステップ５０で特殊環境フラグを０に戻した後にステップ５２へ移行する。これにより、上記の欠点を解消することができる。
【００８１】
最後に、オンライン金融取引受付サービスの利用を申請したユーザが、オンライン金融取引用ウェブサイトへ最初にアクセスした場合について説明する。この場合、使用履歴情報にアクセス元ＩＰアドレス及びユーザエージェント情報が登録されておらず、この状態では通常ルートでの認証が困難であるので、ステップ４２の判定が否定されてステップ６８へ移行し、前述のように取引停止フラグに１を設定すると共に、再認証要請メールの送信等の処理を行うことで、再認証専用のウェブページを介して所定の再認証手続きを受けさせる。この場合も、ステップ６０で使用履歴情報にアクセス元ＩＰアドレス及びユーザエージェント情報が登録されると共に、再認証が成功すれば取引停止フラグが０に戻されるので、次回以降のアクセスでは通常ルートでの認証が行われることになる。
【００８２】
なお、上記では個々のユーザについてアクセス元ＩＰアドレス及びユーザエージェント情報を最大２組登録する場合を説明したが、これに限定されるものではなく、アクセス元ＩＰアドレス及びユーザエージェント情報の組の登録数の上限値を３以上としてもよい。この場合、既に登録されているアクセス元ＩＰアドレス及びユーザエージェント情報の組の中に、認証要求パケットから抽出された新たなアクセス元ＩＰアドレス及びユーザエージェント情報と各々対応していると判定された組が存在していなければ、アクセス元ＩＰアドレス及びユーザエージェント情報の組の登録数が上限値に達する迄の間は、新たなアクセス元ＩＰアドレス及びユーザエージェント情報の組を追加登録し、アクセス元ＩＰアドレス及びユーザエージェント情報の登録数が上限値に達した以降は、新たなアクセス元ＩＰアドレス及びユーザエージェント情報の組を、登録した時期が最も古いアクセス元ＩＰアドレス及びユーザエージェント情報の組に上書きして登録するようにすればよい。上記事項は第７の発明に対応している。
【００８３】
また、アクセス元ＩＰアドレス及びユーザエージェント情報の組の登録数に上限を設けなくてもよい。例えば多数台のクライアント端末１８又は多数種のアクセス元（例えば多数箇所のホットスポット）を選択的に用いてアクセスを行う等の特殊な利用環境を考慮し、アクセス元ＩＰアドレス及びユーザエージェント情報の組を上限を設けずに登録する（既に登録されているアクセス元ＩＰアドレス及びユーザエージェント情報の組の中に、認証要求パケットから抽出された新たなアクセス元ＩＰアドレス及びユーザエージェント情報と各々対応していると判定された組があれば、新たなアクセス元ＩＰアドレス及びユーザエージェント情報を前記対応していると判定された組に上書きして登録し、それ以外の場合は新たなアクセス元ＩＰアドレス及びユーザエージェント情報を追加登録する）と共に、登録してからの経過期間の長さが閾値を越えるか、又は、新たなアクセス元ＩＰアドレス及びユーザエージェント情報と対応していないと判定された回数が閾値を越えたアクセス元ＩＰアドレス及びユーザエージェント情報の組を削除するようにしてもよい。この態様では、使用履歴情報が肥大化する可能性があるという欠点がある一方、利用環境が特殊なユーザであってもステップ４６で認証が「成功」と判定することができるので、認証の「条件付き成功」を設ける必要がなくなり、セキュリティ性を更に向上させることができる。
【００８４】
また、上記では本発明に係る端末装置として、ＰＣ等から成るクライアント端末１８を例に説明したが、これに限定されるものではなく、インターネットにアクセスする機能を

備えたＰＤＡや携帯電話機等の携帯端末であってもよい。この種の携帯端末は無線通信網に設けられたゲートウェイサーバを介してインターネットに接続されるが、詳しくは、任意のウェブサイトにアクセスするために携帯端末から送信された情報はゲートウェイサーバで一旦受信され、インターネット１６経由での通信に適用されるプロトコル（インターネット層のプロトコル：ＩＰ、トランスポート層のプロトコル：ＴＣＰ、アプリケーション層のプロトコル：ＨＴＴＰ）に準拠したパケットへ変換されると共に、無線通信事業者が割り当て用に事前に確保している一定範囲内のＩＰアドレスのうちの何れかのＩＰアドレスがＩＰヘッダに送信元ＩＰアドレスとして設定され、無線通信事業者名や携帯端末の機種、型番、ブラウザのバージョン等を含む情報がユーザエージェント情報としてＨＴＴＰヘッダに設定された後にインターネット１６へ送出される。なお、無線通信事業者との契約形態によっては、ゲートウェイサーバと特定のウェブサーバとの間が専用線で接続され、特定のウェブサーバ宛のパケットがインターネットを経由せずに専用線経由でゲートウェイサーバから送信される場合もあるが、このような通信形態でもパケットには上記と同様に送信元ＩＰアドレスやユーザエージェント情報が設定される。そして、割り当て用に確保しているＩＰアドレスの範囲は個々の無線通信事業者毎に相違している。従って、端末装置が携帯端末であったとしても、本発明を適用して携帯端末を操作しているユーザが正当なユーザか否かを確認することは可能である。

【００８５】

更に、上記ではオンライン金融取引受付サービスを提供するオンライン金融取引用ウェブサイトにおけるユーザ認証に本発明を適用した態様を説明したが、これに限定されるものではなく、任意のサイトにおけるユーザ認証やユーザ確認に適用可能である。また、上記では、本発明を適用したユーザ認証を、ユーザＩＤ及びパスワードを用いたユーザ認証と併用していたが、電子メールアドレス等の簡単なユーザ識別情報を事前に登録したユーザから請求がある毎に、一定の情報を配信する情報発信型サービスを提供するウェブサイトであれば、高精度なユーザ確認（認証）は不要であるので、パスワードに基づくユーザ認証を省略し、ユーザによって入力された電子メールアドレス等のユーザ識別情報に基づいて、本発明を適用したユーザ確認（認証）のみを行うようにしてもよい。

【００８６】

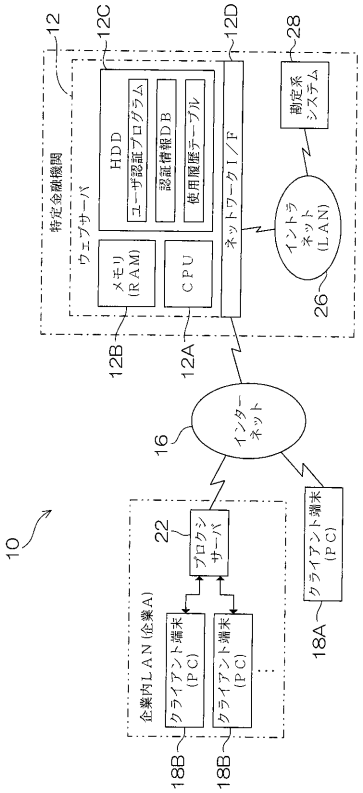
また、上記ではアクセス元ＩＰアドレスとユーザエージェント情報を各々用いてユーザ確認（認証）を行う態様を説明したが、これに限定されるものではなく、例えば個々のユーザに対して電子証明書をインストールしたクライアント端末からのアクセスのみを許可しているウェブサイトのように、個々のユーザに対して一定の端末装置からのアクセスのみを許可している場合には、ユーザエージェント情報のみをユーザ識別情報と対応付けて記憶し、ユーザエージェント情報が登録されているユーザエージェント情報と一致しているか否かに基づいてユーザ確認（認証）を行うようにしてもよい。

【符号の説明】

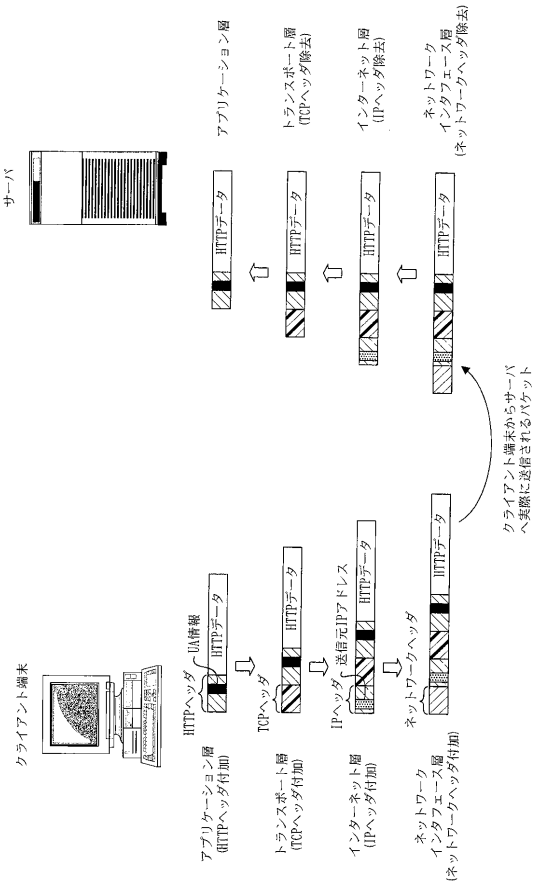
【００８７】

１０ コンピュータ・システム
１２ ウェブサーバ
１２Ｃ ＨＤＤ
１６ インターネット
１８ クライアント端末

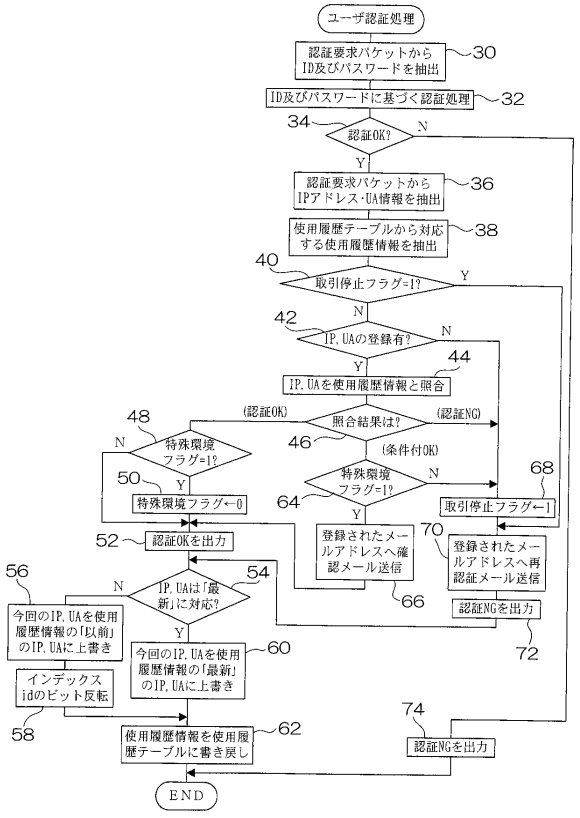
【図１】



【図２】



【図３】



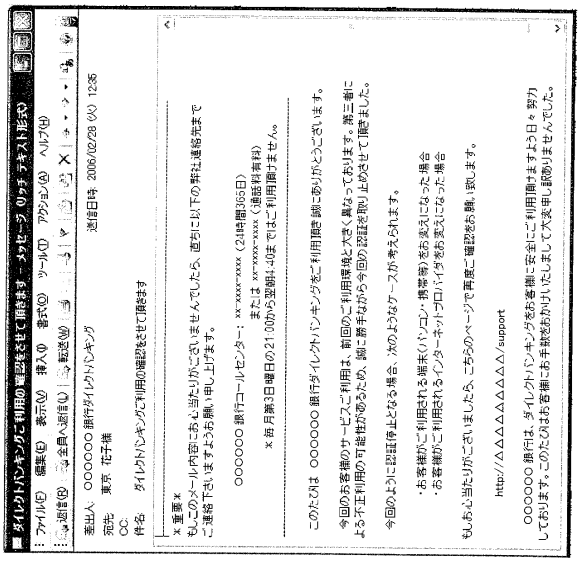
【図４】

〈 使用履歴情報の内容 〉

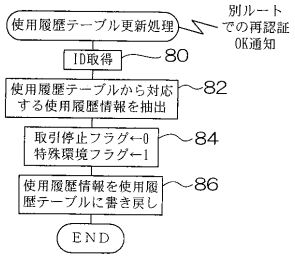
顧客ID	取引停止フラグ	特殊環境フラグ	照合判定用閾値	id	IP0	UA0	IP1	UA1

顧客ＩＤ　　：顧客マスタからハッシュ関数により生成（固定値）
取引停止フラグ　：認証失敗時に1無効(1)とし、通常ルートでの認証をNGとする
特殊環境フラグ　：別ルートでの再認証成時セット(1)し、(条件付き)OK)での認証をOKとする
照合判定用閾値　：IPアドレス照合時に使用する一致度の閾値(デフォルトは例えば80%)
インデックス(id)　：IP0, UA0とIP1, UA1の何れが最新かを1ビットで表す
IP/UA　　：IPアドレス／ユーザエージェント情報、「最新」と「以前」の2組記憶

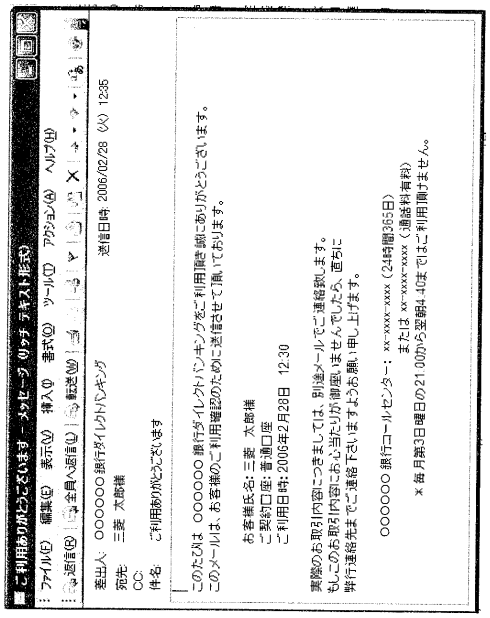
【図６】


ダイレクトバンキングご利用の確認をさせて頂きます - メッセージ (リッチ テキスト形式)
ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) アクション(A) ヘルプ(H)
送信(S) 全員へ返信(L) 転送(W)
差出人: ○○○○○○ 銀行ダイレクトバンキング 送信日時: 2006/02/28 (火) 12:35
宛先: 東京 花子様
CC:
件名: ダイレクトバンキングご利用の確認をさせて頂きます
※重要※
もしこのメール内容にお心当たりがございませんでしたら、直ちに以下の弊社連絡先まで
ご連絡下さいますようお願い申し上げます。
○○○○○○ 銀行コールセンター: xx-xxxx-xxxx (24時間365日)
または xx-xxxx-xxxx (通話料有料)
※毎月第3日曜日の21:00から翌朝4:40までは ご利用頂けません。
このたびは ○○○○○○ 銀行ダイレクトバンキングをご利用頂き誠にありがとうございます。
今回のお客様のサービスご利用は、前回のご利用環境と大きく異なっております。第三者に
よる不正利用の可能性があるため、誠に勝手ながら当行の認証を取り止めさせて頂きました。
今回のように認証停止となる場合、次のようなケースが考えられます。
・お客様がご利用される端末(パソコン・携帯等)をお変えになった場合
・お客様がご利用されるインターネットプロバイダをお変えになった場合
もしお心当たりがございましたら、こちらのページで再度ご確認をお願い致します。
http://△△△△△△△△△△/support
○○○○○○ 銀行は、ダイレクトバンキングをお客様に安全にご利用頂けますよう日々努力
しております。このたびはお客様にお手数をおかけいたしまして大変申し訳ありませんでした。

【図７】


使用履歴テーブル更新処理
別ルートでの再認証OK通知
ID取得
80
使用履歴テーブルから対応する使用履歴情報を抽出
82
取引停止フラグ←0
特殊環境フラグ←1
84
使用履歴情報を使用履歴テーブルに書き戻し
86
END

【図８】


ご利用誠にありがとうございます - メッセージ (リッチ テキスト形式)
ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) アクション(A) ヘルプ(H)
送信(S) 全員へ返信(L) 転送(W)
差出人: ○○○○○○ 銀行ダイレクトバンキング 送信日時: 2006/02/28 (火) 12:35
宛先: 三菱 太郎様
CC:
件名: ご利用誠にありがとうございます
このたびは ○○○○○○ 銀行ダイレクトバンキングをご利用頂き誠にありがとうございます。
このメールは、お客様のご利用確認のために送信させて頂いております。
お客様氏名: 三菱 太郎様
ご契約口座: 普通口座
ご利用日時: 2006年2月28日 12:30
実際のお取引内容につきましては、別途メールでご連絡致します。
もしこのお取引内容にお心当たりが御座いませんでしたら、直ちに
弊行連絡先までご連絡下さいますようお願い申し上げます。
○○○○○○ 銀行コールセンター: xx-xxxx-xxxx (24時間365日)
または xx-xxxx-xxxx (通話料有料)
※毎月第3日曜日の21:00から翌朝4:40までは ご利用頂けません。

【図５】

〈 使用履歴情報に基づく認証OK/NG判定表 〉

		「以前」のIP, UAとの照合結果			
		IP=○, UA=○	IP=○, UA=×	IP=×, UA=○	IP=×, UA=×
「最新」のIP, UAとの照合結果	IP=○, UA=○	認証OK	認証OK	認証OK	認証OK
	IP=○, UA=×	認証OK	条件付き認証OK	認証NG	認証NG
	IP=×, UA=○	認証OK	認証NG	条件付き認証OK	認証NG
	IP=×, UA=×	認証OK	認証NG	認証NG	認証NG

但し、IP=○：IPアドレスの一致度が所定値以上
IP=×：IPアドレスの一致度が所定値未満
UA=○：UA情報が一致
UA=×：UA情報が不一致

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２