(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2007-265018
(P2007-265018A)
(43)公開日　平成19年10月11日(2007.10.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	H04L	9/00	673D	5J104

審査請求 未請求　請求項の数 11　ＯＬ　（全 12 頁）

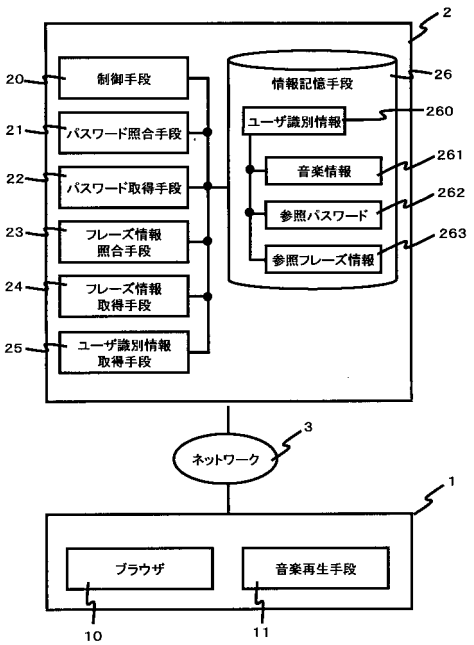
(21)出願番号　特願2006-89098(P2006-89098)
(22)出願日　平成18年3月28日(2006.3.28)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(72)発明者　本多　康太郎
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　矢野　義博
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　山谷　学
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

最終頁に続く

(54)【発明の名称】ユーザ認証システムおよび方法

(57)【要約】
【課題】パスワードを用いてユーザを認証するシステムにおいて、フィッシングによってパスワードの搾取を防止できるシステムを提供する。
【解決手段】サーバ２は、パスワードを用いたユーザ認証を実施する前に、クライアント１に音楽情報を送信し、送信した音楽情報はクライアント１で再生される。サーバ２は、クライアント１で再生される音楽情報の任意の一部の区間をユーザに指定させ、ユーザが指定した区間を認証フレーズ情報として取得し、取得した認証フレーズ情報を照合する。そして、サーバ２は、認証フレーズ情報の照合に成功した場合のみ、パスワードによるユーザ認証を実施する。パスワードを用いてユーザを認証する前には、クライアント２には必ず音楽情報が送信されるため、ユーザごとに配信する音楽情報を変更すれば、正規のサーバ２を装ったフィッシング行為の実施が困難になる。
【選択図】図２



【特許請求の範囲】
【請求項１】
パスワードを用いたユーザ認証方法であって、前記ユーザ認証方法は、パスワードを用いたユーザ認証を実行する前に、認証するユーザに対して予め設定された音楽情報を再生するステップａ、前記ユーザのパスワードを用いてユーザ認証するステップｂが順に実行されることを特徴とするユーザ認証方法。
【請求項２】
請求項１に記載のユーザ認証方法であって、前記ユーザ認証方法は、前記ステップａの後に、前記ユーザによって指定された前記音楽情報の任意の区間を示す認証フレーズ情報を取得するステップａ１、予め設定された前記音楽情報の任意の区間を示す参照フレーズ情報と前記認証フレーズ情報とを照合するステップａ２を実行し、前記フレーズ情報の照合に成功した場合のみ、前記ステップｂが実行されることを特徴とするユーザ認証方法。
【請求項３】
請求項２に記載のユーザ認証方法であって、予め設定された回数だけ、前記参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した場合は、前記ステップａ１および前記ステップａ２は実行されないことを特徴とするユーザ認証方法。
【請求項４】
請求項１から請求項３のいずれかに記載のユーザ認証方法であって、前記ステップａで再生される前記音楽情報は前記ユーザごとに設定されることを特徴とするユーザ認証方法。
【請求項５】
パスワードを用いてユーザを認証するユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記ユーザを識別するための情報であるユーザ識別情報に関連付けて音楽情報、予め設定された前記ユーザのパスワードである参照パスワードを記憶し、更に、前記ユーザ認証システムは、認証する前記ユーザの前記ユーザ識別情報に関連付けられた前記音楽情報を再生する音楽再生手段、前記参照パスワードと照合するためのパスワードである認証パスワードを前記ユーザから取得するパスワード取得手段、前記参照パスワードと前記認証パスワードを照合するパスワード照合手段を備え、前記ユーザ認証システムは、前記音楽再生手段を用いて前記音楽情報を再生してから、前記パスワード照合手段を作動させることを特徴とするユーザ認証システム。
【請求項６】
請求項５に記載のユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記ユーザが操作するクライアントと、前記クライアントとネットワークを介して接続されたサーバとから構成され、前記クライアントは前記音楽再生手段を備え、前記パスワード取得手段および前記パスワード照合手段は前記サーバに備えられていることを特徴とするユーザ認証システム。
【請求項７】
請求項５に記載のユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記音楽情報および前記参照パスワードに加え、前記ユーザ識別情報に関連付けて、前記音楽情報の一部の区間を示す参照フレーズ情報を記憶し、更に、前記ユーザ認証システムは、前記音楽再生手段を用いて前記音楽情報を再生している間に、再生されている前記音楽情報の一部の区間を示す認証フレーズ情報を取得するフレーズ情報取得手段、前記認証フレーズ情報と前記参照フレーズ情報とを照合するフレーズ情報照合手段を備え、前記ユーザ認証システムは、前記フレーズ情報照合手段が前記認証フレーズ情報の照合に成功した後に、前記パスワード照合手段を作動させることを特徴とするユーザ認証システム。
【請求項８】
請求項７に記載のユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記ユーザが操作するクライアントと、前記クライアントとネットワークを介して接続されたサーバとから構成され、前記クライアントは前記音楽再生手段を備え、前記フレ

ーズ情報取得手段、前記フレーズ情報照合手段、前記パスワード取得手段および前記パスワード照合手段は前記サーバに備えられていることを特徴とするユーザ認証システム。
【請求項９】
請求項７または請求項８に記載のユーザ認証システムにおいて、前記サーバは、参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した回数を記憶し、前記回数を超えて参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した場合、ユーザ認証を実施しないことを特徴とするユーザ認証システム。
【請求項１０】
請求項７から請求項９のいずれかに記載のユーザ認証システムにおいて、前記パスワード取得手段は、前記認証パスワードを入力する画面を前記クライアントに送信することで、前記クライアントから前記認証パスワードを取得する手段であることを特徴とするユーザ認証システム。
【請求項１１】
請求項７から請求項９のいずれかに記載のユーザ認証システムにおいて、前記認証パスワードは前記クライアントに予め記憶され、前記サーバに備えられた前記パスワード照合手段は、記憶された前記認証パスワードを前記クライアントから取得する手段であることを特徴とするユーザ認証システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パスワードを利用したユーザ認証システムおよび方法に関し、更に詳しくは、音楽情報を用いたユーザ認証システムおよび方法に関する。
【背景技術】
【０００２】
不正なユーザのアクセスを防止すべく、パーソナルコンピュータ（以下、ＰＣ）やネットワークにログインする際に、ログインする各ユーザの認証を必要とするケースが増えている。ユーザ認証としては、パスワードベースのユーザ認証が用いられることが一般的である。
【０００３】
図６は、パスワードが用いてユーザ認証するときに表示されるパスワード入力画面の一例で、ユーザ認証時には、図６のパスワード入力画面でユーザの識別情報であるユーザＩＤ（図６では、ＡＢＣＤＥＦ）とパスワード（図６では、０１２３４５６７）が入力され、図６のパスワード入力画面に入力されたパスワードと予めＰＣやサーバなどに記憶されたユーザのパスワードとが照合され、ユーザは認証される。
【０００４】
しかし、上述したパスワードベースのユーザ認証では、パスワードを簡単なもの（例えば、ユーザの誕生日）にすると、パスワードが他人から容易に推測される危険性が高くなるし、複雑なものにすると、パスワード入力が面倒になるばかりかユーザがパスワードを忘れる危険性が高くなる。
【０００５】
特許文献１では、ユーザにとって暗記し易く且つ改良されたパスワードベースのユーザ認証方式が開示されている。特許文献１で開示されているユーザ認証方式は、音楽を利用した認証方式で、パスワードを入力キーの順序に合わせてメロディを記憶しておき、ユーザがパスワードをキー入力するときのメロディから、キー入力の正否を判断する発明である。特許文献１の技術を用いることで、ユーザは長いパスワードを暗記し易くかつ第三者に盗用し難くなる。
【特許文献１】特開平１０－２８３３２１号公報
【発明の開示】
【発明が解決しようとする課題】

【０００６】
しかしながら、特許文献１の発明を用いて、長いパスワードを利用することでセキュリティのレベルを向上させたとしても、正規のＷｅｂサイトを装いパスワードなどの情報を搾取するフィッシング（phishing）によって被害を受ける可能性がある。
【０００７】
そこで、本発明は、パスワードベースのユーザ認証システムにおいて、フィッシングによってパスワードの搾取を防止でき、更に、長いパスワードも利用できるユーザ認証方法およびユーザ認証システム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】
【０００８】
上述した課題を解決する第１の発明は、パスワードを用いたユーザ認証方法であって、前記ユーザ認証方法は、パスワードを用いたユーザ認証を実行する前に、認証するユーザに対して予め設定された音楽情報を再生するステップａ、前記ユーザのパスワードを用いてユーザ認証するステップｂが順に実行されることを特徴とする。
【０００９】
上述した課題を解決する第２の発明は、第１の発明に記載のユーザ認証方法であって、前記ユーザ認証方法は、前記ステップａの後に、前記ユーザによって指定された前記音楽情報の任意の区間を示す認証フレーズ情報を取得するステップａ１、予め設定された前記音楽情報の任意の区間を示す参照フレーズ情報と前記認証フレーズ情報とを照合するステップａ２を実行し、前記フレーズ情報の照合に成功した場合のみ、前記ステップｂが実行されることを特徴とする。
【００１０】
更に、第３の発明は、第２の発明に記載のユーザ認証方法であって、予め設定された回数だけ、前記参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した場合は、前記ステップａ１および前記ステップａ２は実行されないことを特徴とする。
【００１１】
更に、第４の発明は、第１の発明から第３の発明のいずれかに記載のユーザ認証方法であって、前記ステップａで再生される前記音楽情報は前記ユーザごとに設定されることを特徴とする。
【００１２】
更に、第５の発明は、パスワードを用いてユーザを認証するユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記ユーザを識別するための情報であるユーザ識別情報に関連付けて音楽情報、予め設定された前記ユーザのパスワードである参照パスワードを記憶し、更に、前記ユーザ認証システムは、認証する前記ユーザの前記ユーザ識別情報に関連付けられた前記音楽情報を再生する音楽再生手段、前記参照パスワードと照合するためのパスワードである認証パスワードを前記ユーザから取得するパスワード取得手段、前記参照パスワードと前記認証パスワードを照合するパスワード照合手段を備え、前記ユーザ認証システムは、前記音楽再生手段を用いて前記音楽情報を再生してから、前記パスワード照合手段を作動させることを特徴とする。
【００１３】
更に、第６発明は、第５の発明に記載のユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記ユーザが操作するクライアントと、前記クライアントとネットワークを介して接続されたサーバとから構成され、前記クライアントは前記音楽再生手段を備え、前記パスワード取得手段および前記パスワード照合手段は前記サーバに備えられていることを特徴とする。
【００１４】
更に、第７の発明は、第５の発明に記載のユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記音楽情報および前記参照パスワードに加え、前記ユーザ識別情報に関連付けて、前記音楽情報の一部の区間を示す参照フレーズ情報を記憶し、更に、前記ユーザ認証システムは、前記音楽再生手段を用いて前記音楽情報を再生している

間に、再生されている前記音楽情報の一部の区間を示す認証フレーズ情報を取得するフレーズ情報取得手段、前記認証フレーズ情報と前記参照フレーズ情報とを照合するフレーズ情報照合手段を備え、前記ユーザ認証システムは、前記フレーズ情報照合手段が前記認証フレーズ情報の照合に成功した後に、前記パスワード照合手段を作動させることを特徴とする。

【００１５】

更に、第８発明は、第７の発明に記載のユーザ認証システムであって、前記ユーザ認証システムは、少なくとも、前記ユーザが操作するクライアントと、前記クライアントとネットワークを介して接続されたサーバとから構成され、前記クライアントは前記音楽再生手段を備え、前記フレーズ情報取得手段、前記フレーズ情報照合手段、前記パスワード取得手段および前記パスワード照合手段は前記サーバに備えられていることを特徴とする。

【００１６】

更に、第９の発明は、第７の発明または第８の発明に記載のユーザ認証システムにおいて、前記サーバは、参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した回数を記憶し、前記回数を超えて参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した場合、ユーザ認証を実施しないことを特徴とする。

【００１７】

更に、第１０の発明は、第７の発明から第９の発明のいずれかに記載のユーザ認証システムにおいて、前記パスワード取得手段は、前記認証パスワードを入力する画面を前記クライアントに送信することで、前記クライアントから前記認証パスワードを取得する手段であることを特徴とする。

【００１８】

更に、第１１の発明は、第７の発明から第９の発明のいずれかに記載のユーザ認証システムにおいて、前記認証パスワードは前記クライアントに予め記憶され、前記サーバに備えられた前記パスワード照合手段は、記憶された前記認証パスワードを前記クライアントから取得する手段であることを特徴とする。

【発明の効果】

【００１９】

上述した本発明によれば、パスワードを用いてユーザを認証する前には、ユーザには必ず前記音楽情報が配信されるため、正規のサーバ２を装ったフィッシング行為の実施が困難になる。また、再生されている前記音楽情報の一部の区間を前記認証フレーズ情報として取得し、前記認証フレーズ情報を照合することでユーザ認証システムのセキュリティをより高めることができる。

【００２０】

更に、参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した回数を記憶し、前記回数を超えて前記参照フレーズ情報と前記認証フレーズ情報との照合に連続して失敗した場合、ユーザ認証を実施しないことで、なりすまし行為による不正アクセスを防止できる。

【００２１】

更に、前記クライアントに前記認証パスワードを記憶することで、前記ユーザは前記認証パスワードを入力する必要がなくなるため、長い前記認証パスワードを利用できるようになる。

【発明を実施するための最良の形態】

【００２２】

ここから、本発明に係るユーザ認証システムについて、図を参照しながら詳細に説明する。図１は、本発明が適用されたクライアントサーバシステムを説明する図である。図１に示したように、クライアントサーバシステムは、情報資源を記憶・管理するサーバ２と、ネットワーク３を介してサーバ２に接続し、サーバ２に記憶された情報資源を利用するクライアント１とから、少なくとも構成されている。

【００２３】

図１では、本発明を分かり易く説明するために、クライアント１を１台としている。実際には、ネットワーク３を介して複数のクライアント１がサーバ２に接続される。また、図１ではサーバ２を１台のサーバで構成されているかのように図示しているが、サーバ２はアプリケーションサーバなどを備えた複数台のサーバで構成されていてもよい。更に、図１では、ＨＵＢやルータなど、本発明の説明に必要とされない装置は省略している。

【００２４】

サーバ２は、正当なユーザに対してのみアクセスを許可するために、クライアント１がネットワーク３を介してサーバ２にログインする際は、パスワードを用いたユーザ認証を実施し、このユーザ認証に本発明は適用されている。

【００２５】

サーバ２には、パスワードを用いたユーザ認証を実施する前に、クライアント１に音楽情報を送信し、送信した音楽情報はクライアント１で再生される。なお、クライアント１に送信する音楽情報はユーザごとに設定されている。

【００２６】

また、サーバ２には、クライアント１に送信する音楽情報の任意の一部の区間が参照フレーズ情報として記憶され、サーバ２は、クライアント１で再生される音楽情報の任意の一部の区間をユーザに指定させ、ユーザが指定した区間を認証フレーズ情報として取得し、取得した認証フレーズ情報と参照フレーズ情報とを照合する。そして、サーバ２は、認証フレーズ情報と参照フレーズ情報との照合に成功した場合のみ、パスワードによるユーザ認証を実施する。

【００２７】

このように、本実施の形態によれば、パスワードを用いてユーザを認証する前には、クライアント２に必ず音楽情報が配信されるため、ユーザごとに配信する音楽情報を変更すれば、正規のサーバ２を装ったフィッシング行為の実施が困難になる。

【００２８】

また、クライアント２で再生されている音楽情報の一部の区間を認証フレーズ情報として取得し、認証フレーズ情報と参照フレーズ情報とを照合することでユーザ認証システムのセキュリティをより高めることができる。

【００２９】

図２は、図１で示したクライアントサーバシステムのブロック図である。図２に示したように、クライアント１には、Ｗｅｂページを表示するためのプログラムであるブラウザ１０と、音楽を再生するための手段である音楽再生手段１１が備えられている。

【００３０】

クライアント１のブラウザ１０は、ＨＴＭＬなどの構造化文書を解釈し表示する機能に加え、ＨＴＭＬのＳＣＲＩＰＴタグなどによって埋め込まれたプログラムコード、例えば、Ｊａｖａ（登録商標）のコードを実行する機能を備えている。また、クライアント１の音楽再生手段１１とは、スピーカなどのハードウェアとスピーカを作動させるプログラムとから構成される。

【００３１】

サーバ２には、クライアント２から認証フレーズ情報を取得するフレーズ情報取得手段２４と、クライアント２から認証パスワードを取得するパスワード取得手段２２と、認証フレーズ情報を照合するフレーズ情報照合手段２３と、認証パスワードを照合するパスワード照合手段２１と、クライアント１に送信する音楽情報２６１などが記憶される情報記憶手段２６と、クライアント１を操作しているユーザ識別情報２６０を取得するユーザ識別情報取得手段２５、サーバ２の全体を制御する制御手段２０とを備えている。

【００３２】

サーバ２の情報記憶手段２６はハードディスクなどの情報記憶装置で実現され、ユーザを識別するユーザ識別情報２６０に関連付けて、クライアント１に送信する音楽情報２６１と、予めユーザによって選択された音楽情報２６１の一部の区間を示す情報が参照フレーズ情報２６３として記憶され、更には、図４のパスワード入力画面などによって、ユー

ザによって予め設定されたパスワードが参照パスワード２６２として記憶されている。

【００３３】

図３は、クライアント１からサーバ２に送信される音楽情報２６１を説明する図である。クライアント１からサーバに送信される音楽情報２６１は、管理者もしくはユーザによって予めサーバ２に登録された音楽情報２６１で、MP3やATRACなどのデータ形式で記述されている。

【００３４】

図３に示したように、音楽情報２６１は、一組のヘッダ２６１ａとフッタ２６１ｂに加え、数多くのフレーム２６１ｃとから構成され、それぞれのフレームにはフレームを識別するためのフレーム番号が付与されている。

【００３５】

図２で示した情報記憶手段２６には、予め、クライアント１を操作するユーザによって、この音楽情報２６１の一部の区間がユーザによって選択され、選択された区間を示す情報が参照フレーズ情報２６３として記憶されている。

【００３６】

例えば、音楽情報２６１の一部の区間を示す情報として、音楽情報２６１に含まれるフレーム番号を利用するときは、一つの参照フレーズ情報２６３は、区間の開始のフレーム番号と区間の最後のフレーム番号とで示される。

【００３７】

サーバ２のユーザ識別情報取得手段２５、フレーズ情報取得手段２４およびパスワード取得手段２２はそれぞれ、クライアント１のブラウザ１０上で動作するアプリケーションで、クライアント１のブラウザ１０に対応したプログラムコードで記述されている。

【００３８】

サーバ２のユーザ識別情報取得手段２５とは、クライアント１を操作しているユーザを識別するための情報であるユーザ識別情報２６０を取得する手段で、図４は、ユーザ識別情報取得手段２５が動作したときにブラウザ１０に表示される画面の一例で、ユーザ識別情報取得手段２５は、図４の入力欄２５ａに入力された情報をユーザ識別情報２６０としてクライアント１からサーバ２に送信する。

【００３９】

サーバ２のフレーズ情報取得手段２４は、ユーザ識別情報取得手段２５が取得したユーザ識別情報２６０に関連付けられ情報記憶手段２６に記憶された音楽情報２６１を、クライアント１に備えられた音楽再生手段１１を利用してブラウザ１０上で再生する機能と、再生した音楽情報２６１の一部の区間をユーザが選択する機能を備えている。

【００４０】

図５は、フレーズ情報取得手段２４が動作したときにブラウザ１０に表示される画面の一例である。図５では、ユーザが音楽情報２６１の一部の区間をを選択するときの目安になるように、音楽情報２６１の再生状況を示すインジケータ２４ａと、音楽情報２６１の一部の区間を選択するためのボタン２４ｂを備えている。音楽情報２６１が再生されると、再生状況がインジケータ２４ａに表示される。

【００４１】

そして、音楽情報２６１の再生中に、ユーザがボタン２４ｂをクリックしてから再度クリックされるまでに再生された区間が認証フレーズ情報として取得される。例えば、音楽情報２６１の一部の区間を示す情報として、音楽情報２６１に含まれるフレーム番号を利用するときは、一つの認証フレーズ情報は、区間の開始のフレーム番号と区間の最後のフレーム番号とで示される。そして、取得した認証フレーズ情報はクライアント１からサーバ２に送信される。

【００４２】

サーバ２のフレーズ情報照合手段２３とは、フレーズ情報取得手段２４が取得した認証フレーズ情報と、情報記憶手段２６に記憶された参照フレーズ情報２６３とを照合する手段である。上述しているように、認証フレーズ情報はユーザによって指定されるため、フ

レーズ情報照合手段２３は、認証フレーズ情報の指定誤差を考慮して照合することが望ましい。

【００４３】

例えば、音楽情報２６１が１秒間に４４Ｋ回でサンプリングされているときは、音楽情報２６１に含まれる一つのフレームのサンプリング間隔は２２．６μｓｅｃになる。認証フレーズ情報の指定誤差の許容値を０．５ｓｅｃとすると、０．５ｓｅｃは約２２０００フレームになり、この約２２０００フレームを考慮して照合するとよい。

【００４４】

サーバ２のパスワード取得手段２２とは、例えば、図６で示したパスワード入力画面をブラウザ１０に表示し、図６の入力欄２２ａにユーザが入力した情報を認証パスワード２６２として取得する手段である。

【００４５】

サーバ２のパスワード照合手段２１は、パスワード取得手段２２が取得した認証パスワードと情報記憶手段２６に記憶されている参照パスワード２６２とを照合する手段で、この手段は一般的な手段であるため、詳細は省く。

【００４６】

ここから、サーバ２の制御手段２０が、サーバ２に備えられた手段を利用してユーザ認証する手順について説明する。図７は、サーバ２がユーザ認証する手順を示したフロー図である。この手順の最初のステップＳ１は、クライアント１からユーザ識別情報２６０を取得するステップである。

【００４７】

クライアント１からサーバ２にアクセス要求があると、制御手段２０はユーザ識別情報取得手段２５をクライアント１に送信し、ユーザ識別情報取得手段２５はブラウザ１０上で動作する。ユーザ識別情報取得手段２５がブラウザ１０上で動作すると、例えば、図４の画面がクライアント２に表示され、ユーザ識別情報取得手段２５は、図４の入力欄２５ａに入力された情報をユーザ識別情報２６０としてサーバ２に送信する。

【００４８】

次のステップＳ２は、サーバ２が認証フレーズ情報を取得するステップである。サーバ２がユーザ識別情報２６０を取得すると、制御手段２０は、取得したユーザ識別情報２６０に関連付けられて情報記憶手段２６に記憶されている音楽情報２６１とフレーズ情報取得手段２４とを、クライアント１に送信する。

【００４９】

クライアント１に送信されたフレーズ情報取得手段２４はブラウザ１０上で動作し、例えば、図５の画面をブラウザ１０に表示するとともに音楽情報２６１を再生する。そして、例えば、図５のボタン２４ｂなどによって認証フレーズ情報が選択されると、フレーズ情報取得手段２４は認証フレーズ情報をサーバ２に送信する。

【００５０】

次のステップＳ３は、認証フレーズ情報を照合するステップである。制御手段２０は、認証フレーズ情報を取得すると、ステップＳ１で取得したユーザ識別情報２６０に関連付けられて記憶している参照フレーズ情報２６３と認証フレーズ情報とを照合する。このステップにおいて、照合に失敗した場合はこの手順を終了し、照合に成功した場合はステップＳ４に進む。

【００５１】

認証フレーズ情報の照合に成功した場合に実行されるステップＳ４は、認証パスワードを取得するステップである。制御手段２０は、認証フレーズ情報と参照フレーズ情報２６３との照合に成功すると、パスワード取得手段２２をクライアント１に送信し、パスワード取得手段２２はクライアント１のブラウザ１０上で動作する。

【００５２】

パスワード取得手段２２がクライアント１のブラウザ１０上で動作すると、例えば、図６の画面がブラウザ１０上に表示され、図６の入力欄２２ａに入力された情報が認証パス

ワードと取得され、取得したパスワードはサーバ２に送信される。

【００５３】

次のステップＳ５は、認証パスワードを照合するステップである。制御手段２０は、ステップＳ１で取得したユーザ識別情報２６０に関連付けられて記憶している参照パスワード２６２と認証パスワードとを照合する。このステップにおいて、照合に失敗した場合はこの手順を終了し、照合に成功した場合はステップＳ６に進み、ステップＳ６ではクライアント１のサーバへのアクセスが許可される。

【００５４】

なお、上述した実施の形態において、サーバ２の制御手段２０は、連続して認証フレーズ情報の照合に失敗できる回数を示すリトライ回数を記憶し、リトライ回数を超えて認証フレーズ情報の照合に失敗した場合、制御手段２０はフレーズ情報照合手段２３を作動させないことが望ましい。

【００５５】

更に、上述した実施の形態において、認証パスワードがクライアント１に記憶されていてもよい。このときは、パスワード取得手段２２がブラウザ１０から認証パスワードを取得する手段になる。図８は、パスワード取得手段２２が作動したときにブラウザ１０に表示され、クライアントに記憶したパスワードを送信する画面の一例で、図８の送信ボタン２２ｂが選択されたときに、クライアント２に記憶された認証パスワードがサーバ２に送信される。

【図面の簡単な説明】

【００５６】

【図１】クライアントサーバシステムを説明する図。

【図２】クライアントサーバシステムのブロック図。

【図３】音楽情報を説明する図。

【図４】ユーザ識別情報取得手段が動作したときにブラウザに表示される画面の一例。

【図５】フレーズ情報取得手段が動作したときにブラウザに表示される画面の一例。

【図６】パスワード入力画面の一例。

【図７】サーバがユーザ認証する手順を示したフロー図。

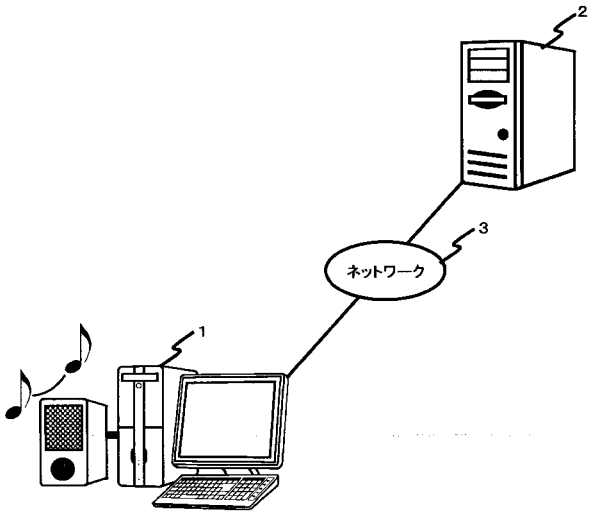
【図８】クライアントに記憶したパスワードを送信する画面の一例。

【符号の説明】

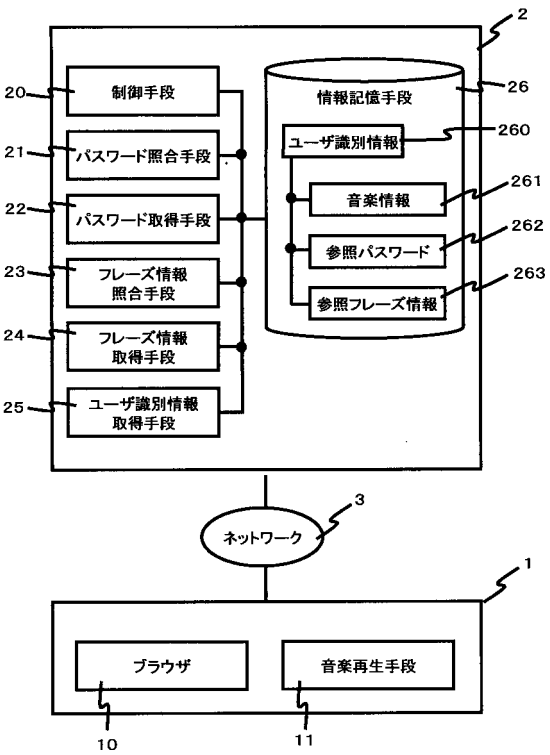
【００５７】

１　クライアント
　１０　ブラウザ
　１１　音楽再生手段
２　サーバ
　２０　制御手段
　２１　パスワード照合手段
　２２　パスワード取得手段
　２３　フレーズ情報照合手段
　２４　フレーズ情報取得手段
　２５　ユーザ識別情報取得手段
　２６　情報記憶手段
　２６０　ユーザ識別情報
　２６１　音楽情報
　２６２　参照パスワード
　２６３　参照フレーズ情報
３　ネットワーク

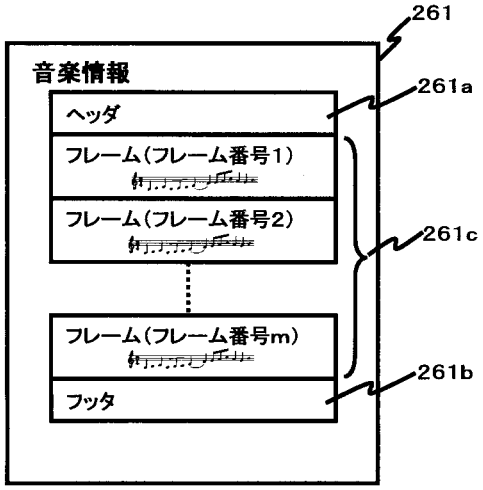
【図１】


2
ネットワーク
3
1

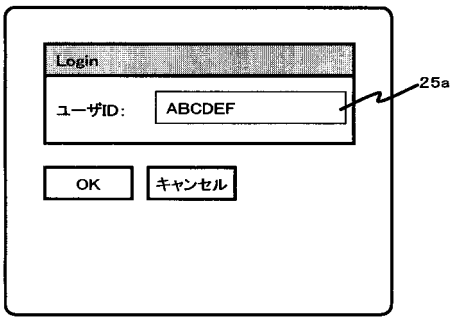
【図２】


2
20
制御手段
21
パスワード照合手段
22
パスワード取得手段
23
フレーズ情報
照合手段
24
フレーズ情報
取得手段
25
ユーザ識別情報
取得手段
情報記憶手段
26
ユーザ識別情報
260
音楽情報
261
参照パスワード
262
参照フレーズ情報
263
3
ネットワーク
1
ブラウザ
音楽再生手段
10
11

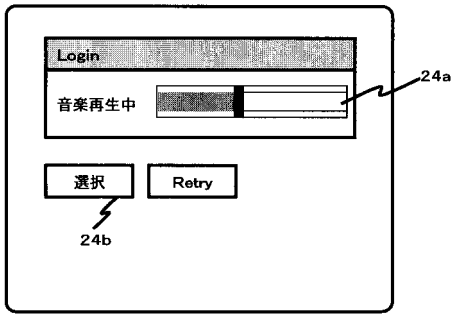
【図３】


261
音楽情報
261a
ヘッダ
フレーム(フレーム番号1)
フレーム(フレーム番号2)
261c
フレーム(フレーム番号m)
261b
フッタ

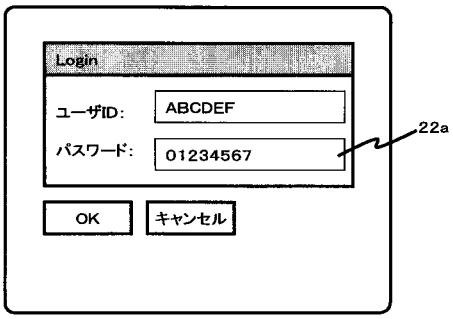
【図４】


Login
ユーザID:
ABCDEF
25a
OK
キャンセル

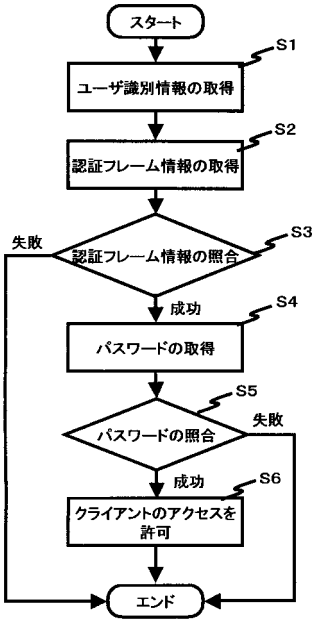
【図５】


Login
音楽再生中
24a
選択
Retry
24b

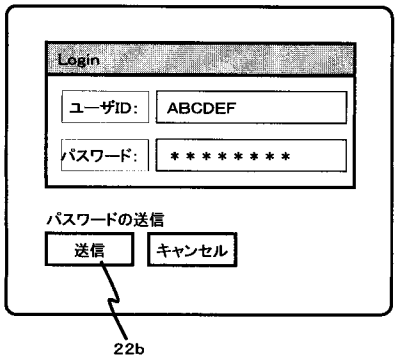
【図６】


Login
ユーザID:
ABCDEF
パスワード:
01234567
22a
OK
キャンセル

【図７】


スタート
S1
ユーザ識別情報の取得
S2
認証フレーム情報の取得
S3
失敗
認証フレーム情報の照合
成功
S4
パスワードの取得
S5
パスワードの照合
失敗
成功
S6
クライアントのアクセスを許可
エンド

【図８】


Login
ユーザID:
ABCDEF
パスワード:
＊＊＊＊＊＊＊＊
パスワードの送信
送信
キャンセル
22b

フロントページの続き

Ｆターム(参考) 5B285 AA01 BA01 CA02 CB02 CB53 CB62 CB72 CB85
5J104 KA01 KA06 KA21 NA05