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

特許第5569284号
(P5569284)

(45)発行日　平成26年8月13日(2014.8.13)　(24)登録日　平成26年7月4日(2014.7.4)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131E
G06F 21/34	(2013.01)	G06F	21/20	134
G06F 3/12	(2006.01)	G06F	3/12	K
G06F 1/00	(2006.01)	G06F	1/00	370E
B41J 29/00	(2006.01)	B41J	29/00	Z

請求項の数 7　(全 16 頁)　最終頁に続く

(21)出願番号　特願2010-205882(P2010-205882)
(22)出願日　平成22年9月14日(2010.9.14)
(65)公開番号　特開2012-63863(P2012-63863A)
(43)公開日　平成24年3月29日(2012.3.29)
審査請求日　平成25年7月18日(2013.7.18)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　杉山　真良
東京都中央区勝どき３丁目１２番１号　リコーＩＴソリューションズ株式会社内
(72)発明者　阿部　修二
東京都中央区勝どき３丁目１２番１号　リコーＩＴソリューションズ株式会社内

審査官　石田　信行

最終頁に続く

(54)【発明の名称】情報処理装置、認証制御方法、及び認証制御プログラム

(57)【特許請求の範囲】

【請求項１】

ユーザ識別情報をクライアント装置より受信し、ユーザごとにパスワードを記憶するユーザ情報記憶手段に記憶されている全てのパスワードと異なる第一の文字列を前記クライアント装置に送信する文字列送信手段と、

前記クライアント装置よりパスワードとして受信される第二の文字列に、前記第一の文字列の少なくとも一部が含まれているかを判定する照合手段と、

前記照合手段による判定結果が肯定的な場合に、前記ユーザ識別情報に関連付けて記憶されているパスワードを認証に用いるパスワードとして選択する選択手段とを有する情報処理装置。

【請求項２】

前記照合手段は、前記第二の文字列と前記第一の文字列とが所定の文字数以上の共通の文字列を含むかを判定する請求項１記載の情報処理装置。

【請求項３】

前記文字列送信手段は、前記クライアント装置が表示させる認証画面において入力が制限されている文字を含む前記第一の文字列を前記クライアント装置に送信する請求項１又は２記載の情報処理装置。

【請求項４】

前記文字列送信手段は、前記認証画面において入力が制限されている文字のみによって構成される前記第一の文字列を前記クライアント装置に送信する請求項３記載の情報処理

装置。
【請求項５】
前記文字列送信手段は、前記クライアント装置が表示させる認証画面において入力可能な最大文字数を有する前記第一の文字列を該クライアント装置に送信し、
前記照合手段は、前記第二の文字列と前記第一の文字列とが一致するかを判定する請求項１乃至４いずれか一項記載の情報処理装置。
【請求項６】
ユーザ識別情報をクライアント装置より受信し、ユーザごとにパスワードを記憶するユーザ情報記憶手段に記憶されている全てのパスワードと異なる第一の文字列を前記クライアント装置に送信する文字列送信手順と、
前記クライアント装置よりパスワードとして受信される第二の文字列に、前記第一の文字列の少なくとも一部が含まれているかを判定する照合手順と、
前記照合手順による判定結果が肯定的な場合に、前記ユーザ識別情報に関連付けて記憶されているパスワードを認証に用いるパスワードとして選択する選択手順とをコンピュータが実行する認証制御方法。
【請求項７】
ユーザ識別情報をクライアント装置より受信し、ユーザごとにパスワードを記憶するユーザ情報記憶手段に記憶されている全てのパスワードと異なる第一の文字列を前記クライアント装置に送信する文字列送信手順と、
前記クライアント装置よりパスワードとして受信される第二の文字列に、前記第一の文字列の少なくとも一部が含まれているかを判定する照合手順と、
前記照合手順による判定結果が肯定的な場合に、前記ユーザ識別情報に関連付けて記憶されているパスワードを認証に用いるパスワードとして選択する選択手順とをコンピュータに実行させる認証制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、認証制御方法、及び認証制御プログラムに関し、特にパスワードの入力の省略が可能な認証処理を制御する情報処理装置、認証制御方法、及び認証制御プログラムに関する。
【背景技術】
【０００２】
従来、各種のコンピュータシステムは認証機能を有し、認証されたユーザにのみ利用権限を与えるように構成されている。具体的には、最初に認証画面が表示される。認証画面において、ユーザは、ユーザ名（又はユーザＩＤ）及びパスワードの入力を行う。当該画面に入力されたユーザ名及びパスワードが、予め保持されているユーザ名及びパスワードに合致する場合、ユーザに利用権限が与えられる。認証機能によれば、利用権限を付与するユーザを予め限定することができ、コンピュータシステムの安全性を向上させることができる。
【０００３】
他方において、近年では、一台のＰＣ（Personal Computer）等が、複数のユーザによって共用されることが少なくなっている。換言すれば、各ユーザは、自らに専用のＰＣを有することが多い。そして、各ＰＣでは、ＯＳ（Operating System）へのログイン時に、認証が行われる。そうすると、ＯＳにログインできているということによって、ＰＣの操作者が当該ＰＣの正当なユーザであることは或る程度担保されている。それにも拘わらず、インターネット上のサイトや他のコンピュータシステムを利用する際に、改めてユーザ名及びパスワードの入力を要求されるのは、ユーザにとって煩わしい場合がある。
【０００４】
そこで、従来、認証画面に予めユーザ名及びマスクされたパスワードを表示させることによって、ユーザ名及びパスワードの入力操作の省略が可能とされている。

【０００５】
図１は、ユーザ名及びパスワードの入力操作を省略するための仕組みを説明するための図である。同図において、認証サーバ５１０は、認証機能を有するコンピュータである。認証画面６１０は、認証サーバ５１０とネットワークを介して接続されるコンピュータにおいて表示される画面である。
【０００６】
ステップＳ１において、認証画面６１０は、ユーザ識別情報を認証サーバ５１０に送信する。例えば、認証サーバ５１０がＷｅｂサイトを提供するコンピュータであれば、ユーザ識別情報は、当該Ｗｅｂサイトに対するクッキー情報に相当する。
【０００７】
続いて、認証サーバ５１０は、ユーザ識別情報に関連付けられているユーザ名及びパスワードを認証画面６１０に返信する（Ｓ２）。認証画面６１０は、受信されたユーザ名及びパスワードを表示させる。この際、認証画面６１０は、パスワードに関しては「＊＊＊＊＊＊」といったように、マスクされた結果を表示する。認証画面６１０において、ＯＫボタン６１１が押下されると、認証画面６１０は、自らが表示させているユーザ名及びパスワードを認証サーバ５１０に送信する（Ｓ３）。認証サーバ５１０は、受信されたユーザ名及びパスワードを、データベースに登録されているユーザ名及びパスワードと照合することにより、ユーザの認証を行う。
【０００８】
図１に示されるような仕組みによれば、ユーザは、ＯＫボタン６１１を押下するのみで、簡易に認証を受けることができる。
【発明の概要】
【発明が解決しようとする課題】
【０００９】
しかしながら、従来の仕組みには、セキュリティ上の観点から不都合な点がある。一例として、ユーザ名及びパスワードがネットワーク上を流通する機会が増加することが挙げられる。すなわち、認証サーバ５１０から認証画面６１０へのユーザ名及びパスワードの転送が必要となる。その結果、ユーザ名及びパスワードが盗聴される可能性が増加することが考えられる。
【００１０】
本発明は、上記の点に鑑みてなされたものであって、パスワードの入力を省略させることによるセキュリティの劣化を改善することのできる情報処理装置、認証制御方法、及び認証制御プログラムの提供を目的とする。
【課題を解決するための手段】
【００１１】
そこで上記課題を解決するため、本発明は、ユーザ識別情報をクライアント装置より受信し、ユーザごとにパスワードを記憶するユーザ情報記憶手段に記憶されている全てのパスワードと異なる第一の文字列を前記クライアント装置に送信する文字列送信手段と、前記クライアント装置よりパスワードとして受信される第二の文字列に、前記第一の文字列の少なくとも一部が含まれているかを判定する照合手段と、前記照合手段による判定結果が肯定的な場合に、前記ユーザ識別情報に関連付けて記憶されているパスワードを認証に用いるパスワードとして選択する選択手段とを有する。
【００１２】
このような情報処理装置では、パスワードの入力を省略させることによるセキュリティの劣化を改善することができる。
【発明の効果】
【００１３】
本発明によれば、パスワードの入力を省略させることによるセキュリティの劣化を改善することができる。
【図面の簡単な説明】

【００１４】
【図１】ユーザ名及びパスワードの入力操作を省略するための仕組みを説明するための図である。
【図２】第一の実施の形態における情報処理システムの構成例を示す図である。
【図３】本発明の実施の形態における情報処理サーバのハードウェア構成例を示す図である。
【図４】第一の形態の情報処理システムにおける認証処理の処理手順の一例を説明するための図である。
【図５】第一の実施の形態におけるキャッシュ情報記憶部の構成例を示す図である。
【図６】認証画面の表示例を示す図である。
【図７】第二の実施の形態における情報処理システムの構成例を示す図である。
【図８】第二の形態の情報処理システムにおける認証処理の処理手順の一例を説明するための図である。
【図９】第三の実施の形態における情報処理システムの構成例及びその処理手順を説明するための図である。
【発明を実施するための形態】
【００１５】
以下、図面に基づいて本発明の実施の形態を説明する。図２は、第一の実施の形態における情報処理システムの構成例を示す図である。同図の情報処理システム１において、情報処理サーバ１０と認証サーバ２０とは、ＬＡＮ（Local Area Network）又はインターネット等のネットワークを介して通信可能とされている。また、情報処理サーバ１０とクライアント装置３０とは、ＬＡＮ又はインターネット等のネットワークを介して通信可能とされている。
【００１６】
クライアント装置３０は、情報処理サーバ１０がネットワークを介して提供するサービスを受けるためにユーザが利用するＰＣ（Personal Computer）等のコンピュータである。携帯電話、ＰＤＡ（Personal Digital Assistance）、又はスマートフォン等が、クライアント装置３０として用いられてもよい。
【００１７】
情報処理サーバ１０は、ネットワークを介して所定のサービスを提供するコンピュータである。情報処理サーバ１０の一形態として、Ｗｅｂサーバが挙げられる。但し、情報処理サーバ１０によって提供されるサービスは、専用のクライアントアプリケーションが必要とされるサーバプログラムによって実現されてもよい。
【００１８】
認証サーバ２０は、クライアント装置３０を介して情報処理サーバ１０が提供するサービスを受けようとするユーザを認証するコンピュータである。
【００１９】
同図において、クライアント装置３０は、ＵＩ制御部３１を有する。ＵＩ制御部３１は、情報処理サーバ１０が提供するサービスを受けるための画面の表示制御等を行う。ＵＩ制御部３１が表示させる画面の一つとして認証画面が挙げられる。認証画面は、一般的にログイン画面等とも呼ばれ、ユーザ名（ユーザＩＤとも呼ばれる。）及びパスワード等をユーザに入力させるための画面である。なお、情報処理サーバ１０がＷｅｂサーバである場合、ＵＩ制御部３１は、Ｗｅｂブラウザに相当する。
【００２０】
情報処理サーバ１０は、文字列送信部１１、照合部１２、選択部１３、認証制御部１４、キャッシュ情報記憶部１５、及びサービス提供部１６等を有する。これら各部は、情報処理サーバ１０にインストールされたプログラム（認証制御プログラム）が、情報処理サーバ１０のＣＰＵに実行させる処理によって実現される。
【００２１】
文字列送信部１１は、認証画面においてユーザ名及びパスワードとして表示される文字

列をクライアント装置３０に送信する。認証画面に対するユーザ名及びパスワードの入力の省略を可能とするためのである。但し、文字列送信部１１は、パスワードに関しては、真のパスワードではなく、ダミーのパスワード（以下、「ダミーパスワード」という。）を送信する。

【００２２】

照合部１２は、クライアント装置３０より受信される認証要求に含まれているパスワード（以下、「受信パスワード」という。）と、ダミーパスワードとを照合し、受信パスワードにダミーパスワードの一部が含まれているか否かを判定する。

【００２３】

選択部１３は、照合部１２による判定結果に基づいて、認証に用いるパスワードを選択する。具体的には、照合部１２による判定結果が肯定的な場合（受信パスワードにダミーパスワードの少なくとも一部が含まれている場合）、選択部１３は、キャッシュ情報記憶部１５にキャッシュされているパスワードを認証に用いるパスワードとして選択する。一方、照合部１２による判定結果が否定的な場合（受信パスワードにダミーパスワードの少なくとも一部が含まれていない場合）、選択部１３は、受信パスワードを認証に用いるパスワードとして選択する。

【００２４】

認証制御部１４は、クライアント装置３０より受信される認証要求に含まれているユーザ名又はキャッシュ情報記憶部１５に記憶されているユーザ名と、選択部１３によって選択されたパスワードとに基づく認証を認証サーバ２０に実行させる。キャッシュ情報記憶部１５は、認証サーバ２０において管理されているユーザ名及びパスワードを、例えば、情報処理サーバ１０の補助記憶装置を用いてキャッシュする。サービス提供部１６は、クライアント装置３０を利用するユーザが認証された場合に、所定のサービスを提供する。

【００２５】

認証サーバ２０は、認証処理部２１及びユーザ情報記憶部２２等を有する。認証処理部２１は、情報処理サーバ１０の認証制御部１４からの認証要求に含まれているユーザ名及びパスワードを、ユーザ情報記憶部２２に記録されているユーザ名及びパスワードと照合することにより認証を行う。ユーザ情報記憶部２２は、情報処理サーバ１０が提供するサービスの利用を許可されたユーザごとに、ユーザ名及びパスワード等を記憶する。

【００２６】

図３は、本発明の実施の形態における情報処理サーバのハードウェア構成例を示す図である。図３の情報処理サーバ１０は、それぞれバスBで相互に接続されているドライブ装置１００と、補助記憶装置１０２と、メモリ装置１０３と、ＣＰＵ１０４と、インタフェース装置１０５とを有する。

【００２７】

情報処理サーバ１０での処理を実現するプログラムは、ＣＤ－ＲＯＭ等の記録媒体１０１によって提供される。プログラムを記録した記録媒体１０１がドライブ装置１００にセットされると、プログラムが記録媒体１０１からドライブ装置１００を介して補助記憶装置１０２にインストールされる。但し、プログラムのインストールは必ずしも記録媒体１０１より行う必要はなく、ネットワークを介して他のコンピュータよりダウンロードするようにしてもよい。補助記憶装置１０２は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

【００２８】

メモリ装置１０３は、プログラムの起動指示があった場合に、補助記憶装置１０２からプログラムを読み出して格納する。ＣＰＵ１０４は、メモリ装置１０３に格納されたプログラムに従って情報処理サーバ１０に係る機能を実行する。インタフェース装置１０５は、ネットワークに接続するためのインタフェースとして用いられる。

【００２９】

以下、情報処理システム１の処理手順について説明する。図４は、第一の形態の情報処理システムにおける認証処理の処理手順の一例を説明するための図である。

【００３０】
クライアント装置３０におけるＵＩ制御部３１に対するユーザによる所定の入力に応じ、ＵＩ制御部３１は、情報処理サーバ１０に対し、アクセス要求を送信する（Ｓ１０１）。当該アクセス要求には、クライアント装置３０のユーザを識別するためのユーザ識別情報が含まれている。ユーザ識別情報は、予め補助記憶装置１０２に記憶されている。ユーザ識別情報は、例えば、情報処理サーバ１０がＷｅｂサーバである場合、当該Ｗｅｂサーバに対するクッキー情報であってもよい。ユーザ識別情報は、ユーザ名と同じ値でもよいし、異なっていてもよい。
【００３１】
または、ＵＩ制御部３１は、ユーザ名を入力させるための画面を表示させ、当該画面を介してユーザ名を入力させてもよい。この場合、ＵＩ制御部３１は、入力されたユーザ名をユーザ識別情報として情報処理サーバ１０に送信する。
【００３２】
情報処理サーバ１０において、アクセス要求が受信されると、文字列送信部１１は、当該アクセス要求に含まれているユーザ識別情報に基づいて、ユーザ名をキャッシュ情報記憶部１５より検索する（Ｓ１０２）。
【００３３】
図５は、第一の実施の形態におけるキャッシュ情報記憶部の構成例を示す図である。同図に示されるように、キャッシュ情報記憶部１５は、ユーザごとに、ユーザ識別情報、ユーザ名、及びパスワード等を関連付けて記憶している。
【００３４】
したがって、ステップＳ１０２において、文字列送信部１１は、アクセス要求に含まれているユーザ識別情報に関連付けられているユーザ名を検索する。なお、ユーザ名がユーザ識別情報としても用いられている場合、ステップＳ１０２は、必ずしも実行されなくてもよい。
【００３５】
続いて、文字列送信部１１は、ダミーパスワードを生成する（Ｓ１０３）。文字列送信部１１は、ダミーパスワードを、ステップＳ１０２において検索されたユーザ名に関連付けて、例えば、メモリ装置１０３に記録しておく。
【００３６】
ダミーパスワードは、ユーザ情報記憶部２２に記憶されている全てのユーザのパスワードと異なる任意の文字列であればよい。例えば、文字列送信部１１は、ランダムに又は所定の命名規則に基づいて文字列を生成する。文字列送信部１１は、当該文字列がパスワードとして登録されているか否かを、認証サーバ２０の認証処理部２１に問い合わせる。認証処理部２１は、当該文字列がパスワードとしてユーザ情報記憶部２２に記憶されているか否かを確認し、確認結果を返信する。
【００３７】
または、当該文字列は、予め固定的に決められていてもよい。ユーザごとに固定的であってもよいし、全ユーザに共通な値であってもよい。更に、当該文字列は、定期的に認証サーバ２０から転送されてもよい。すなわち、認証処理部２１が、ユーザ情報記憶部２２にパスワードとして記憶されていない文字列を生成し、情報処理サーバ１０に転送してもよい。
【００３８】
なお、ダミーパスワードの文字数は、真のパスワードの文字数と異なることが望ましい。後述される認証画面３１０において、ダミーパスワードが表示される際に、ＵＩ制御部３１の実装内容によっては、マスクされた文字列がダミーパスワードと同じ文字数で表示される場合がある。そうすると、真のパスワードの文字数が特定され、真のパスワードが看破される可能性が高まってしまからである。
【００３９】
続いて、文字列送信部１１は、ユーザ名及びダミーパスワードを、アクセス要求に対す

る応答に含めてクライアント装置３０に返信する（Ｓ１０４）。クライアント装置３０においてユーザ名及びダミーパスワードが受信されると、ＵＩ制御部３１は、当該ユーザ名及びダミーパスワードが入力された（設定された）状態の認証画面を、クライアント装置３０の表示装置に表示させる（Ｓ１０５）。

【００４０】

図６は、認証画面の表示例を示す図である。同図において、認証画面３１０は、ユーザ名入力領域３１１、パスワード入力領域３１２、及びＯＫボタン３１３等を有する。ユーザ名入力領域３１１は、ユーザ名を入力させるための領域である。パスワード入力領域３１２は、パスワードを入力させるための領域である。但し、本実施の形態の認証画面３１０には、表示された初期状態において、ユーザ名入力領域３１１には、情報処理サーバ１０より返信されたユーザ名が設定されている。また、パスワード入力領域３１２には、情報処理サーバ１０より返信されたダミーパスワードがパスワードとして設定されている。

【００４１】

したがって、ユーザは、ユーザ名及びパスワードの入力操作を省略することができる。なお、同図では、パスワード入力領域３１２において、パスワードがマスクされて表示された状態が示されている。但し、パスワード入力領域３１２に設定されているパスワードは、ダミーパスワードである。したがって、マスクされずに表示されてしまってもよい。

【００４２】

なお、ユーザは、必要に応じてユーザ名入力領域３１１又はパスワード入力領域３１２において、ユーザ名又はパスワードを編集することができる。その場合、認証画面３１０に設定されているユーザ名及びパスワードの値は更新される。

【００４３】

続いて、ユーザによってＯＫボタン３１３がクリックされると、ＵＩ制御部３１は、認証画面３１０に設定されているユーザ名及びパスワードを含む認証要求を情報処理サーバ１０に送信する（Ｓ１０６）。

【００４４】

情報処理サーバ１０において認証要求が受信されると、照合部１２は、認証要求に含まれているユーザ名（受信ユーザ名）に関連付けられてメモリ装置１０３に記録されているダミーパスワードを取得し、当該ダミーパスワードと認証要求に含まれているパスワード（受信パスワード）とを照合（又は比較）する（Ｓ１０７）。具体的には、照合部１２は、受信パスワードに、ダミーパスワードの少なくとも一部が含まれているか否かを判定する。これは、ユーザの意図を判断するための処理である。すなわち、ユーザが、認証画面３１０のパスワード入力領域３１２においてパスワードを入力し直した場合、ユーザは、入力したパスワードに基づく認証を希望していると考えられる。一方、ユーザが、パスワード入力領域３１２においてパスワードを編集せずにＯＫボタン３１３をクリックした場合、ユーザは、キャッシュされているパスワードに基づく認証を希望していると考えられる。そうすると、照合部１２は、受信パスワードがダミーパスワードに完全に一致するか否かを判定すればよいとも考えられる。

【００４５】

但し、ユーザが、パスワード入力領域３１２において、数文字削除した後、やはりキャッシュされているパスワードに基づく認証を希望する場合も考えられる。したがって、本実施の形態において、照合部１２は、受信パスワードに、ダミーパスワードの少なくとも一部が含まれているか否かを判定する。

【００４６】

但し、ユーザが、新たに入力したパスワードによる認証を希望し、パスワードを入力し直した場合、受信パスワードにダミーパスワードの一部が偶然含まれてしまう可能性もある。そうすると、新たに入力されたパスワードが有効なものとして扱われる可能性が低くなってしまう。特に、ダミーパスワードの文字数が大きくなればなるほど、ダミーパスワードに含まれる文字の種類は多くなり、新たに入力されたパスワードにダミーパスワードの一部が偶然含まれてしまう可能性は高くなる。

【００４７】
そこで、照合部１２による判定が肯定的となる条件に更なる制限を設けてもよい。例えば、ダミーパスワードと受信パスワードとが、所定の文字数以上の共通の文字列を含むことを条件として追加してもよい。更に、一致する文字列の位置（例えば、先頭からの位置）が一致することを条件として追加してもよい。例えば、先頭からの所定の文字数の文字列が一致することを条件としてもよい。
【００４８】
なお、ユーザが、新たに入力されたパスワードによる認証を希望する場合とは、例えば、キャッシュ情報記憶部１５に記憶されているパスワードが、ユーザ情報記憶部２２に記憶されているパスワードとが一致していないことをユーザが知っている場合である。具体的には、セキュリティ上の観点より、認証サーバ２０において定期的かつ強制的にユーザ情報記憶部２２におけるパスワードが変更され、電子メール等によって新たなパスワードがユーザに通知されている場合が一例として挙げられる。または、情報処理サーバ１０を介さずに、ユーザの操作に基づくクライアント装置３０からの要求に応じて、認証サーバ２０においてユーザ情報記憶部２２におけるパスワードが変更された場合も当てはまる。
【００４９】
または、ユーザが、パスワード入力領域３１２において、数文字削除した後、やはりキャッシュされているパスワードに基づく認証を希望する場合、ユーザの取り得る行動として、削除した分について、真のパスワードを入力することが考えられる。ダミーパスワードがマスクされて表示されている場合、ユーザは、真のパスワードが認証画面３１０に設定されているものと考えるからである。
【００５０】
そこで、受信パスワードに、ダミーパスワードの少なくとも一部が含まれており、両者が相違する部分については、キャッシュ情報記憶部１５にキャッシュされているパスワード（すなわち、真のパスワード）に一致することを、照合部１２による判定結果が肯定的となる条件としてもよい。なお、キャッシュされているパスワードは、認証要求に含まれているユーザ名に基づいて、キャッシュ情報記憶部１５を用いて特定されればよい。
【００５１】
または、ダミーパスワードに、パスワード入力領域３１２には入力できない（入力が制限されている）文字（以下、「禁止文字」という。）が含まれるようにしてもよい。換言すれば、ステップＳ１０３において、文字列送信部１１は、ダミーパスワードに禁止文字を含めるようにしてもよい。すなわち、一般的にパスワードに使用できる文字には制限がある。そして、ＵＩ制御部３１は、パスワード入力領域３１２に対する禁止文字の入力を拒否するように実装されている場合が多い。そうすると、受信パスワードに、ダミーパスワードの少なくとも一部が含まれており、かつ、その一部に禁止文字が含まれている場合、当該禁止文字は、ユーザによって入力されたものでないことが保証される。したがって、この場合、照合部１２の判定結果を肯定的なものとすることについて、妥当性が認められる。なお、禁止文字によってのみ（禁止文字の集合によって）ダミーパスワードが構成されるようにしてもよい。そうすることにより、受信パスワードにダミーパスワードの少なくとも一部が含まれているか否かの判定結果の正確性（確からしさ）を向上させることができる。この場合、パスワード入力領域３１２において全てのダミーパスワードが削除されない限り、受信パスワードには、ユーザには入力できない可能性の高い禁止文字が含まれるからである。
【００５２】
なお、照合部１２による判定結果が肯定的となるのは、受信ユーザ名に関連付けられているダミーパスワードがメモリ装置１０３に記録されていることが前提となる。すなわち、認証画面３１０のユーザ名入力領域３１１において、ユーザ名が変更されていないことが前提となる。したがって、受信ユーザ名に関連付けられているダミーパスワードがメモリ装置１０３に記録されていない場合、照合部１２による判定結果は否定的なものとなる。

【００５３】
続いて、選択部１３は、照合部１２による判定結果に基づいて認証に用いるパスワード等を選択する（Ｓ１０８）。具体的には、照合部１２による判定結果が肯定的な場合、選択部１３は、キャッシュされているパスワードを選択する。この場合、選択部１３は、受信ユーザ名に係るパスワードをキャッシュ情報記憶部１５より取得し、当該受信ユーザ名（又はキャッシュ情報記憶部１５に記憶されている当該受信ユーザ名と同じユーザ名）と、当該パスワードとを認証に用いるユーザ名及びパスワードとして選択する。一方、照合部１２による判定結果が否定的な場合、選択部１３は、受信ユーザ名及び受信パスワードを認証に用いるユーザ名及びパスワードとして選択する。
【００５４】
続いて、認証制御部１４は、選択部１３によって選択されたユーザ名及びパスワードを含む認証要求を認証サーバ２０に送信する（Ｓ１０９）。認証サーバ２０において認証要求が受信されると、認証サーバ２０の認証処理部２１は、当該認証要求に含まれているユーザ名及びパスワードと、ユーザ情報記憶部２２に記憶されているユーザ名及びパスワードとを照合することにより、認証を行う（Ｓ１１０）。続いて、認証処理部２１は、認証結果を情報処理サーバ１０に返信する（Ｓ１１１）。
【００５５】
情報処理サーバ１０において認証結果が受信されると、サービス提供部１６は、認証結果に応じてサービスの提供の許否を判定する。
【００５６】
なお、上記においては、情報処理サーバ１０と認証サーバ２０とが別の装置である例を示したが、情報処理サーバ１０が認証サーバ２０を兼ねてもよい。具体的には、情報処理サーバ１０が、認証処理部２１及びユーザ情報記憶部２２を有していてもよい。この場合、キャッシュ情報記憶部１５は、必ずしも必要ではない。キャッシュ情報記憶部１５の機能は、ユーザ情報記憶部２２によって代替されればよいからである。但し、この場合、ユーザ情報記憶部２２の各レコードと、ユーザ識別情報との関連付け情報が補助記憶装置１０２に記憶される必要がある。
【００５７】
上述したように、本実施の形態によれば、真のパスワードがネットワーク上を流通する機会を減少させることができる。具体的には、ステップＳ１０４においては、真のパスワードではなくダミーパスワードが転送される。また、ユーザが、キャッシュされているパスワードによる認証を望む場合、ステップＳ１０６においてもダミーパスワードが転送される。したがって、パスワードの入力を省略させることによるセキュリティの劣化を改善することができる。
【００５８】
また、本実施の形態の実施に際し、クライアント装置３０側（すなわち、ＵＩ制御部３１）に関して基本的に改変は必要とされない点も、本実施の形態の利点として挙げられる。すなわち、ＵＩ制御部３１から見れば、真のパスワードの代わりにダミーパスワードが送信されてくる点が相違するが、両者は単なる文字列である。したがって、ＵＩ制御部３１にとって、斯かる相違点による影響は無い。よって、ユーザに対しても、基本的に従来の方式（例えば、図１において説明した方式）との差異は露出されない。その結果、ユーザが知らない間（又は、ユーザに気付かれることなく）に、セキュリティを向上させることができる。
【００５９】
また、本実施の形態によれば、パスワードが看破される危険性を著しく低下させることもできる。すなわち、従来の方式（図１において説明した方式）は、真のパスワードが看破される可能性があるという問題を有する。例えば、認証画面６１０に表示されているパスワードは、マスクされているものの、実際の値である。したがって、最後の一文字を削除し、削除した分の一文字を適当に入力する。この状態で認証を受ける。認証に失敗したら同じことを繰り返す。この際、入力する一文字は、前回と異なるものとする。いずれ認

証に成功したら、パスワードの最後の一文字が判明したことになる。続いて、最後から２番目、３番目と、一文字ずつ同じことを繰り返すことにより、最終的にはパスワードの全ての文字列が看破されてしまう可能性がある。

【００６０】

一方、本実施の形態において、認証画面３１０に表示されるパスワードは、ダミーパスワードである。したがって、上記のようなパスワードの看破を防止することができる。

【００６１】

なお、上記のようなパスワードの看破方法に鑑みると、パスワードが編集された場合は、キャッシュされているパスワードを用いた認証を回避した方が、セキュリティ上の観点上好ましいと考えられる。特に、パスワードの一部について編集が行われた場合、上記のようなパスワードの看破が試みられている可能性も考えられるからである。

【００６２】

そこで、ダミーパスワードと受信パスワードとが完全に一致することを、照合部１２による判定が肯定的となる条件としてもよい。但し、これでもパスワードの編集が行われていないことを完全には保証できない。パスワードの最後の一部が削除され、改めて追加された一部が、偶然にダミーパスワードと一致する可能性も有るからである。そこで、斯かる観点からも、禁止文字によってのみダミーパスワードを構成することの利点が認められる。ダミーパスワードの全てが禁止文字である場合は、改めて追加された一部が、偶然にダミーパスワードと一致する可能性を低下させることができるからである。すなわち、認証画面３１０では、禁止文字の入力が不可能である場合が多いからである。

【００６３】

但し、禁止文字によってのみダミーパスワードを構成したとしても、ダミーパスワードの後に何らかの文字を追加し、削除するといった行為（編集）を検知することは困難である。

【００６４】

そこで、ダミーパスワードの文字数を、認証画面３１０のパスワード入力領域３１２において入力可能な最大文字数としてもよい。そうすることにより、ダミーパスワードの後に何らかの文字を追加し、削除するといった行為を防止することができる。これは、ダミーパスワードが禁止文字のみで構成されていない場合にも有効である。

【００６５】

次に、第二の実施の形態について説明する。図７は、第二の実施の形態における情報処理システムの構成例を示す図である。図７中、図２と同一部分には同一符号を付し、その説明は省略する。また、第二の実施の形態では第一の実施の形態と異なる点について説明する。したがって、特に言及されない点については、第一の実施の形態と同様でよい。

【００６６】

同図の情報処理システム２において、クライアント装置３０ａは、キャッシュ情報記憶部３２を有している。一方、情報処理サーバ１０ａは、キャッシュ情報記憶部１５を有していない。すなわち、第二の実施の形態は、ユーザ名及びパスワードをキャッシュする位置が情報処理サーバ１０に限定されないことを説明するための実施形態である。

【００６７】

キャッシュ情報記憶部３２の内容は、図５に示されるものと同様でよい。但し、必ずしもユーザ識別情報の列は必要ではない。また、キャッシュ情報記憶部３２は、基本的に、クライアント装置３０のログインユーザに関するユーザ名及びパスワードのみを記憶する。

【００６８】

以下、情報処理システム２の処理手順について説明する。図８は、第二の形態の情報処理システムにおける認証処理の処理手順の一例を説明するための図である。クライアント装置３０におけるＵＩ制御部３１に対するユーザによる所定の入力に応じ、ＵＩ制御部３１は、情報処理サーバ１０に対し、アクセス要求を送信する（Ｓ２０１）。当該アクセス要求には、キャッシュ情報記憶部３２に記憶されているユーザ名及びパスワードがユーザ

識別情報として含まれる。情報処理サーバ１０がＷｅｂサーバである場合、キャッシュ情報記憶部３２は、当該ＷｅｂサーバのＷｅｂサイトに対するクッキー情報を記憶する記憶部であってもよい。

【００６９】

情報処理サーバ１０において、アクセス要求が受信されると、情報処理サーバ１０の文字列送信部１１は、当該アクセス要求に含まれているユーザ識別情報よりユーザ名及びパスワードを抽出する（Ｓ２０２）。

【００７０】

ステップＳ２０３以降は、図４のステップＳ１０３以降と同様でよい。但し、図４においてキャッシュ情報記憶部１５に記憶されているユーザ名又はパスワードの代わりに、ステップＳ２０２において抽出されたユーザ名パスワードが利用されればよい。

【００７１】

上述したように、ユーザ名及びパスワードは、クライアント装置３０にキャッシュされていてもよい。

【００７２】

なお、情報処理サーバ１０等は、必ずしも汎用的なコンピュータでなくてもよい。近年では、複合機、コピー機、プリンタ、ファクシミリ等の機器も、Ｗｅｂサーバ等のサーバとして機能することが可能となっている。したがって、このような機器が情報処理サーバ１０等として用いられてもよい。

【００７３】

ここでは、複合機が、情報処理サーバ１０若しくは１０ａ及びクライアント装置３０若しくは３０ａの機能を有する例を第三の実施の形態として説明する。

【００７４】

図９は、第三の実施の形態における情報処理システムの構成例及びその処理手順を説明するための図である。図９中、図２又は図７と同一部分には同一符号を付し、その説明は省略する。

【００７５】

同図の情報処理システム３において、複合機４０及び認証サーバ２０は、ＬＡＮ（Local Area Network）又はインターネット等のネットワークを介して通信可能とされている。

【００７６】

複合機は４０、図３に示されるようなハードウェア及び画像形成手段としてのハードウェア（プリンタ及びスキャナ等）の他に、タッチパネル４１を有する。タッチパネル４１は、操作画面を表示させ、操作画面を介してユーザより入力を受け付けるタッチ式の液晶パネルである。複合機４０には、また、ＩＣカードリーダ４２が接続されている。ＩＣカードリーダ４２は、ＩＣカード５０に記録された情報を読み取るハードウェアである。ＩＣカード５０は、各ユーザに複数枚ずつ配布されており、当該ユーザのユーザ名及びパスワードが記録されている。ＩＣカード５０内のユーザ名及びパスワードは、専用のツールを用いないと修正することはできない。

【００７７】

更に、複合機４０は、図２又は図７において、情報処理サーバ１０若しくは１０ａ、及びクライアント装置３０若しくは３０ａが有する各部のソフトウェアを有する。

【００７８】

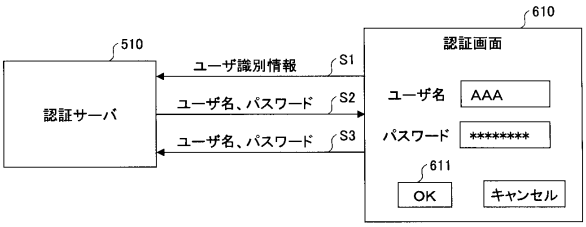
複合機４０の一部又は全部の機能を利用する際に、ユーザは、ＩＣカード５０の提示を要求される。ユーザによって、ＩＣカード５０がＩＣカードリーダ４２にセットされると、ＩＣカードリーダ４２によって、ＩＣカード５０に記録されているユーザ名及びパスワードが読み取られる（Ｓ３０１）。複合機４０の文字列送信部１１は、ダミーパスワードを生成し、ＩＣカード５０より読み取られたユーザ名と当該ダミーパスワードとをタッチパネル４１に送信する（Ｓ３０２）。タッチパネル４１のＵＩ制御部３１は、当該ユーザ名及びダミーパスワードが設定された認証画面３１０（図６参照）をタッチパネル４１に表示させる。

【００７９】
ユーザは、必要に応じてユーザ名又はパスワードの編集を行う。ユーザによってＯＫボタン３１３がクリックされると、ＵＩ制御部３１は、認証画面３１０に設定されているユーザ名及びパスワードを含む認証要求を複合機４０に送信する（Ｓ３０３）。その後、複合機４０内において、ステップＳ１０７及びＳ１０８と同様の処理が実行され、認証サーバ２０に対して認証要求が送信される（Ｓ３０４）。認証サーバ２０の認証処理部２１は認証を行い、認証結果を複合機４０に返信する（Ｓ３０５）。複合機４０は、認証結果に応じて、機能の提供の可否を判定する。
【００８０】
このように、複合機４０に関しても、第一又は第二の実施の形態と同様の処理手順を適用することができる。また、ＩＣカード５０に関して、特別な機能を追加することなく、セキュリティを向上させることができる。
【００８１】
なお、第三の実施の形態において、正当なユーザがログイン画面３１０においてパスワードを編集するケースとしては、例えば、ユーザが、複数枚所有するＩＣカード５０のうちの一枚を紛失した場合が考えられる。ここで、複数枚のＩＣカード５０には、全て同じユーザ名及びパスワードが記録されている。この場合、ユーザは、紛失したＩＣカードの不正利用を防止するため、認証サーバ２０のユーザ情報記憶部２２に記憶されているパスワードを更新させる。但し、手持ちの残りのＩＣカード５０については、パスワードの更新が直ちに行われるとは限らない。専用のツールを用いたＩＣカード５０内のパスワードの更新は、迅速な対応が困難だからである。
【００８２】
斯かるユーザが複合機４０を利用する場合、ユーザは、手持ちのＩＣカード５０をＩＣカードリーダ４２にセットする。ユーザは、ＩＣカード５０に記録されているパスワードは有効で無いことを知っているため、ログイン画面３１０においてパスワードを編集する。
【００８３】
以上、本発明の実施例について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。
【符号の説明】
【００８４】
１、２、３　情報処理システム
１０、１０ａ　情報処理サーバ
１１　文字列送信部
１２　照合部
１３　選択部
１４　認証制御部
１５　キャッシュ情報記憶部
１６　サービス提供部
２０　認証サーバ
２１　認証処理部
２２　ユーザ情報記憶部
３０、３０ａ　クライアント装置
３１　ＵＩ制御部
３２　キャッシュ情報記憶部
４０　複合機
４１　タッチパネル
４２　ＩＣカードリーダ
５０　ＩＣカード

１００　　ドライブ装置
１０１　　記録媒体
１０２　　補助記憶装置
１０３　　メモリ装置
１０４　　ＣＰＵ
１０５　　インタフェース装置
Ｂ　　バス
【先行技術文献】
【特許文献】
【００８５】
【特許文献１】特開平７－０９３０７３号公報

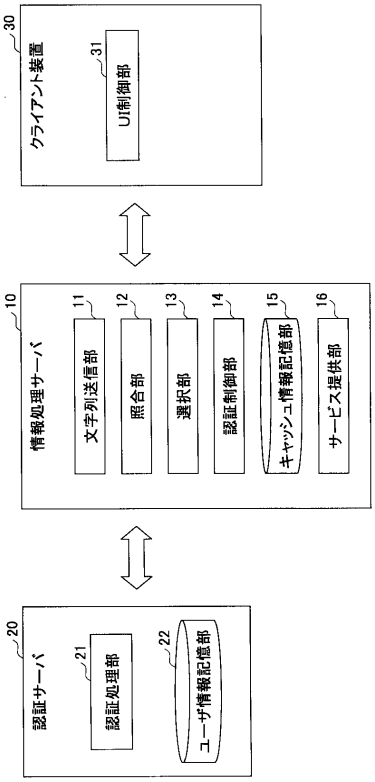
【図１】

ユーザ名及びパスワードの入力操作を省略するための仕組みを説明するための図



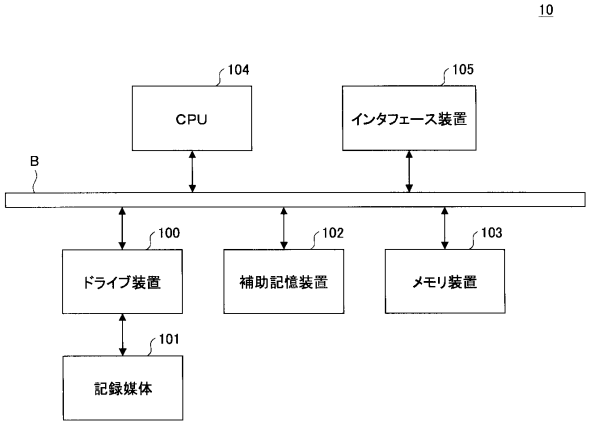
【図２】

第一の実施の形態における情報処理システムの構成例を示す図



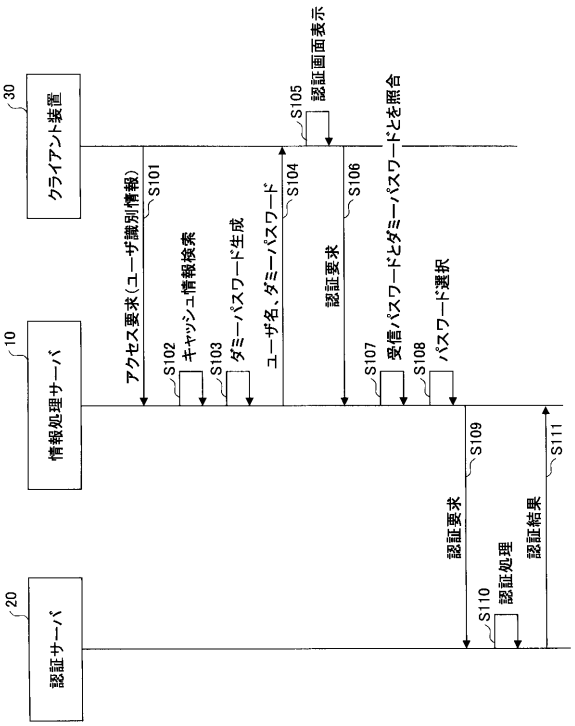
【図３】

本発明の実施の形態における情報処理サーバのハードウェア構成例を示す図



【図４】

第一の形態の情報処理システムにおける
認証処理の処理手順の一例を説明するための図



【図５】

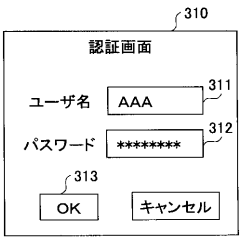
第一の実施の形態におけるキャッシュ情報記憶部の構成例を示す図

15

ユーザ識別情報	ユーザ名	パスワード
12345467	AAA	xxxxxxx
7777790	BBB	yyyyyyyy
32355321	CCC	zzzzzzz
:	:	:

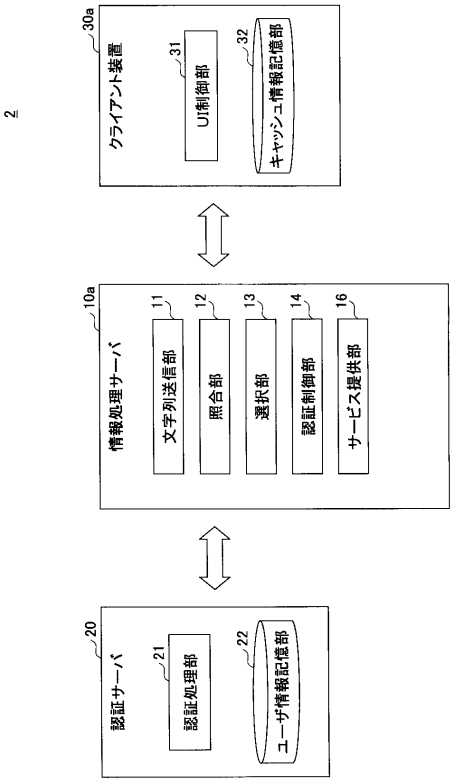
【図６】

認証画面の表示例を示す図



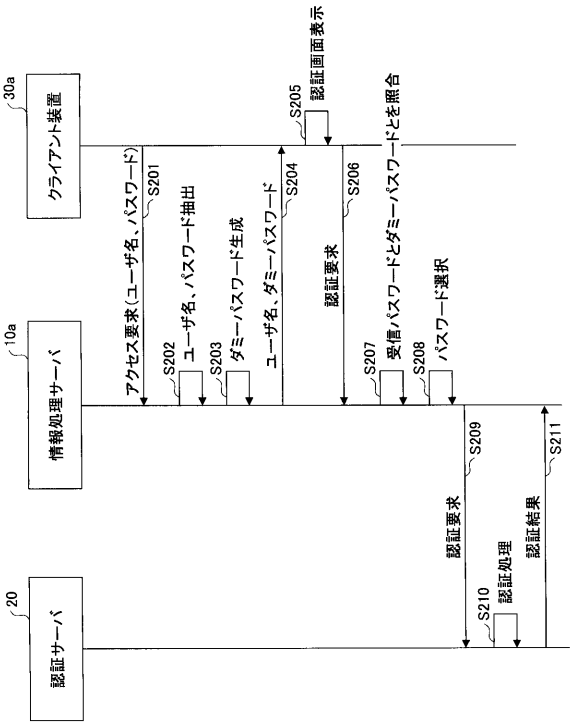
【図７】

第二の実施の形態における情報処理システムの構成例を示す図



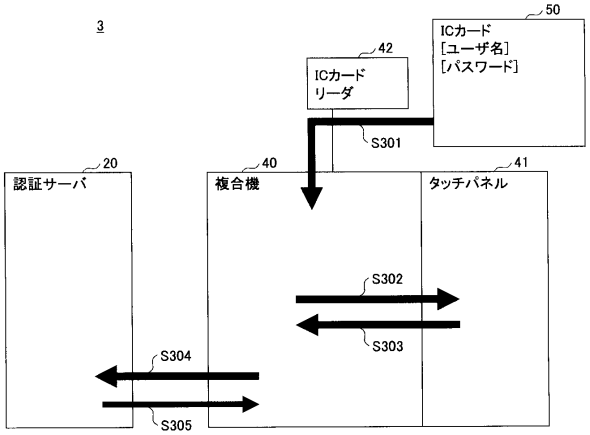
【図８】

第二の形態の情報処理システムにおける
認証処理の処理手順の一例を説明するための図



【図９】

第三の実施の形態における
情報処理システムの構成例及びその処理手順を説明するための図



フロントページの続き

(51)Int.Cl. F I
B41J 29/38 (2006.01) B41J 29/38 Z

(56)参考文献 特開２００６－０１１９４０（ＪＰ，Ａ）
特開２００７－１２２５９９（ＪＰ，Ａ）
特開２００５－０４４０５４（ＪＰ，Ａ）
特開昭６３－２８９１８１（ＪＰ，Ａ）
米国特許出願公開第２００９／０１６５１０４（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３１
Ｇ０６Ｆ ２１／３４
Ｇ０６Ｆ １／００
Ｇ０６Ｆ ３／１２
Ｂ４１Ｊ ２９／００
Ｂ４１Ｊ ２９／３８