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

特許第4829697号
(P4829697)

(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月22日(2011.9.22)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330B
H04L 9/32	(2006.01)	G06F	15/00	330E
G06F 3/12	(2006.01)	H04L	9/00	673A
B41J 29/00	(2006.01)	G06F	3/12	K
B41J 29/38	(2006.01)	B41J	29/00	Z

請求項の数 12　(全 15 頁)　最終頁に続く

(21)出願番号　特願2006-170247 (P2006-170247)
(22)出願日　平成18年6月20日 (2006.6.20)
(65)公開番号　特開2008-3697 (P2008-3697A)
(43)公開日　平成20年1月10日 (2008.1.10)
審査請求日　平成21年6月19日 (2009.6.19)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　岸本　浩明
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法、コンピュータプログラム及び記録媒体

(57)【特許請求の範囲】

【請求項１】

情報処理装置であって、

暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信手段と、

前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信手段とを有し、

前記送信手段は、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする情報処理装置。

【請求項２】

前記送信手段は、前記暗号化通信が使用される場合に、外部の認証装置による認証処理で必要な認証情報をユーザに入力可能にし、外部の認証装置による認証処理をユーザに選択可能にする画面をウェブブラウザに表示させる情報を送信することを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記送信手段は、前記暗号化通信が使用されない場合に、前記情報処理装置による認証処理で必要な認証情報をユーザに入力可能にし、前記情報処理装置による認証処理をユーザに選択可能にする画面をウェブブラウザに表示させる情報を送信することを特徴とする請求項１或いは２に記載の情報処理装置。

【請求項４】
暗号化された情報を通信する暗号化通信の使用または不使用をユーザに選択可能にする設定手段を有することを特徴とする請求項１乃至３のいずれかに記載の情報処理装置。
【請求項５】
外部の認証装置をユーザに登録可能にする登録手段を有し、
前記送信手段は、前記暗号化通信が使用される場合に、前記登録手段によって登録された複数の認証装置の一覧を示す情報を送信することを特徴とする請求項１乃至４のいずれかに記載の情報処理装置。
【請求項６】
暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信ステップと、
前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信ステップとを有し、
前記送信ステップでは、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする情報処理方法。
【請求項７】
前記送信ステップでは、前記暗号化通信が使用される場合に、外部の認証装置による認証処理で必要な認証情報をユーザに入力可能にし、外部の認証装置による認証処理をユーザに選択可能にする画面をウェブブラウザに表示させる情報を送信することを特徴とする請求項６に記載の情報処理方法。
【請求項８】
前記送信ステップでは、前記暗号化通信が使用されない場合に、前記情報処理装置による認証処理で必要な認証情報をユーザに入力可能にし、前記情報処理装置による認証処理をユーザに選択可能にする画面をウェブブラウザに表示させる情報を送信することを特徴とする請求項６或いは７に記載の情報処理方法。
【請求項９】
暗号化された情報を通信する暗号化通信の使用または不使用をユーザに選択可能にする設定ステップを有することを特徴とする請求項６乃至８のいずれかに記載の情報処理方法。
【請求項１０】
外部の認証装置をユーザに登録可能にする登録ステップを有し、
前記送信ステップでは、前記暗号化通信が使用される場合に、前記登録ステップによって登録された複数の認証装置の一覧を示す情報を送信することを特徴とする請求項６乃至９のいずれかに記載の情報処理方法。
【請求項１１】
コンピュータによって実行されるコンピュータプログラムであって、
暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信ステップと、
前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信ステップとをコンピュータに実行させ、
前記送信ステップでは、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とするコンピュータプログラム。
【請求項１２】
コンピュータによって実行されるコンピュータプログラムを格納し、前記コンピュータによって読み取り可能な記録媒体であって、
暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信ステップと、

前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信ステップとをコンピュータに実行させるコンピュータプログラムを格納し、

前記送信ステップでは、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

外部の認証装置と通信可能な情報処理装置に関するものである。

【背景技術】

【０００２】

認証機能を備えた情報処理装置では、ユーザがネットワークを介して情報処理装置を操作するに当たって認証処理を行う。例えば、ユーザがウェブブラウザを使ってユーザモードへの移行を印刷装置に指示すると、印刷装置は暗証番号の入力をウェブブラウザに要求し、ユーザによって入力された暗証番号に基づいて認証処理を行う（例えば、特許文献１）。

【０００３】

暗証番号に基づく認証が成功した場合には、印刷装置はユーザモードのウェブページをウェブブラウザに送信する。これにより、ユーザはユーザモードのウェブページで印刷装置を操作することができる。

【特許文献１】特開２００２－３５９７１８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

ネットワーク環境においては、認証処理で用いられる認証情報を複数の情報処理装置のそれぞれが管理することなく、外部の認証装置（以下、認証サーバ）が一元的に管理する場合がある。

【０００５】

例えば、ユーザ名及びパスワードなどの認証情報は認証サーバに保持されていて、情報処理装置は、ユーザによって入力された認証情報に基づく認証処理を認証サーバに行ってもらう。ユーザがユーザ端末からネットワークを介して情報処理装置を操作する場合には、情報処理装置はユーザ端末からネットワークを介して認証情報を受信し、受信した認証情報に基づく認証処理を認証サーバに行ってもらう。

【０００６】

このとき、情報処理装置は、ユーザによって入力された認証情報そのものをユーザ端末から受信する必要がある。情報処理装置が認証情報を保持して認証処理を行う場合には、認証方法によっては、ユーザによって入力された認証情報そのものがネットワークを介して情報処理装置に送信されなくても良い場合がある。一方、情報処理装置がユーザ端末に代わって、認証サーバへの認証処理の依頼を代行・仲介する場合には、ユーザによって入力された認証情報そのものを必要とする。

【０００７】

ただし、認証サーバでの認証処理に必要な認証情報がそのままネットワークを介してユーザ端末から情報処理装置に送信されると、第三者によって盗聴されやすく、認証情報が漏洩しやすい。

【０００８】

ユーザ端末と情報処理装置との間で暗号化通信が行われることにより、認証情報が盗聴されるのを防ぐことができる。しかし、情報処理装置が必ずしも暗号化通信を行えるとは限らず、例えば、暗号化通信の使用がユーザによって設定されていない場合には、情報処理装置は暗号化通信を行えない。

【０００９】
情報処理装置が暗号化通信を行えない状態で、認証サーバによる認証処理が選択可能になると、認証情報が安全でないままユーザ端末から情報処理装置に送信されてしまう。
【００１０】
そこで、本発明では、認証サーバによる認証処理に必要な認証情報が安全でないままユーザ端末から情報処理装置に送信されてしまうのを防止することを目的とする。
【課題を解決するための手段】
【００１１】
本発明に係る情報処理装置は、暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信手段と、前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信手段とを有し、前記送信手段は、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする。
【００１２】
また、本発明に係る情報処理方法は、暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信ステップと、前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信ステップとを有し、前記送信ステップでは、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする。
【００１３】
また、本発明に係るコンピュータプログラムは、暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信ステップと、前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信ステップとをコンピュータに実行させ、前記送信ステップでは、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする。
【００１４】
また、本発明に係る記録媒体は、暗号化された情報を通信する暗号化通信が使用される場合に、外部の認証装置による認証処理をユーザに選択可能にする情報をユーザ端末に送信する送信ステップと、前記ユーザによって入力された、外部の認証装置による認証処理で必要な認証情報を、前記暗号化通信を用いて前記ユーザ端末から受信する受信ステップとをコンピュータに実行させるコンピュータプログラムを格納し、前記送信ステップでは、前記暗号化通信が使用されない場合に、外部の認証装置による認証処理をユーザに選択可能にする情報を前記ユーザ端末に送信しないことを特徴とする。
【発明の効果】
【００１５】
本発明によれば、暗号化された情報を通信する暗号化通信が使用されない場合には、外部の認証装置による認証処理がユーザに選択されないようにできる。
【００１６】
また、暗号化通信が使用されない場合には、報処理装置による認証処理をユーザに選択可能にすることにより、認証サーバによる認証処理に必要な認証情報がユーザ端末から情報処理装置に送信されてしまうのを防止できる。
【発明を実施するための最良の形態】
【００１７】
以下、図面を参照して本発明の好適な実施形態を説明する。
【００１８】

図１はネットワークシステムの構成を示す図である。このネットワークシステムでは、情報処理装置１０１、ユーザ端末１０２、認証サーバ１０３及び認証サーバ１０４がネットワーク１００を介して相互に通信可能である。ネットワークは有線であっても無線であっても良い。

【００１９】

認証サーバ１０３及び認証サーバ１０４は、ユーザ名とパスワードとに基づく認証処理を行う認証装置である。また、情報処理装置１０１は、ユーザ名とパスワードとに基づく認証処理を自身で行うことができるとともに、認証処理の実行を認証サーバ１０３及び認証サーバ１０４に要求することもできる。なお、認証処理に必要な認証情報はユーザ名及びパスワードに限られるものではない。

【００２０】

情報処理装置１０１、認証サーバ１０３及び認証サーバ１０４のそれぞれを識別する識別情報として名称が付けられている。情報処理装置１０１の名称は「Ｐｒｉｎｔｅｒ０００」、認証サーバ１０３の名称は「Ａｕｔｈ１．ｄｏｍａｉｎ．ｎｅｔ」、認証サーバ１０３の名称は「Ａｕｔｈ２．ｄｏｍａｉｎ．ｎｅｔ」である。

【００２１】

図２は、情報処理装置１０１とユーザ端末１０２とのハードウェア構成を示す図である。ここでは、情報処理装置１０１の一例として印刷装置を説明する。この他、情報処理装置１０１は、スキャナ、デジタル複合機、複写機などであっても良い。情報処理装置１０１はプリンタ部２０１、演算処理装置（以下、ＣＰＵ）２０２、ＲＡＭ２０３、ネットワークインターフェース部２０４、Ｉ／Ｏ制御部２０５、ＨＤＤ２０６、操作部２０７を備えている。

【００２２】

ＣＰＵ２０２はＨＤＤ２０６に格納されたプログラムを読み出して、そのプログラムをＲＡＭ２０３に格納する。そして、ＣＰＵ２０２は、ＲＡＭ２０３格納されたプログラムを実行して、情報処理装置１０１全体の動作を制御する。プリンタ部２０１は印刷データに基づく印刷を用紙に印刷する。ＲＡＭ２０３はＣＰＵ２０２によって実行されるプログラムを格納したり、プログラムの実行に必要な様々な変数の値を格納したり、或いは印刷データを格納したりする。ネットワークインターフェース部２０４は、ネットワーク１００を介して情報の送受信を行う。Ｉ／Ｏ制御部２０５はＨＤＤ２０６からの情報の読み出しや、ＨＤＤ２０６への情報の書き込みを制御する。ＨＤＤ２０６は大容量の記憶装置であって、プログラム、印刷データ、様々な種類の情報を格納する。操作部２０６は操作パネルや操作キーを有する。ユーザは、操作パネルに表示された様々な情報を閲覧し、操作キーを使って様々な情報を入力する。

【００２３】

ユーザ端末１０２の一例としてはパーソナルコンピュータを説明する。ユーザ端末１０２は、ワークステーション、携帯端末などであっても良い。ユーザ端末１０２は演算処理装置（以下、ＣＰＵ）２１０、ネットワークインターフェース部２１１、入出力ポート２１２、Ｉ／Ｏ制御部２１４、ＨＤＤ２１５、ＲＡＭ２１６、ビデオインターフェース部２１７を備えている。また、ユーザ端末１０２は、入出力ポート２１２を介してキーボード２１３とマウス２１９とに接続し、ビデオインターフェース部２１７を介してディスプレイ２１８に接続している。

【００２４】

ＣＰＵ２１０はＨＤＤ２１５に格納されたプログラムを読み出して、そのプログラムをＲＡＭ２１６に格納する。そして、ＣＰＵ２１０はＲＡＭ２１６に格納されたプログラムを実行して、ユーザ端末１０２全体の動作を制御する。ネットワークインターフェース部２１１はネットワーク１００を介して情報の送受信を行う。入出力ポート２１２は、キーボード２１３やマウス２１９などの入力デバイスと接続したり、入力デバイス以外の外部デバイスと接続したりする。そして、入出力ポート２１２は入力デバイスや外部デバイスとの間で情報の送受信を行う。ユーザはキーボード２１３やマウス２１９を使って様々な

情報を入力する。Ｉ／Ｏ制御部２１４はＨＤＤ２１５からの情報の読み出しや、ＨＤＤ２１５への情報の書き込みを制御する。ＨＤＤ２１５は大容量の記憶装置であって、プログラムや様々な種類の情報を格納する。ＲＡＭ２１６はＣＰＵ２１０によって実行されるプログラムを格納したり、プログラムの実行に必要な様々な変数の値を格納したりする。ビデオインターフェース部２１７はディスプレイ２１８に表示されるべき情報をディスプレイ２１８に送信する。ディスプレイ２１８は様々な情報を表示する表示装置であり、ユーザはディスプレイ２１８に表示された情報を閲覧する。

【００２５】

認証サーバ１０３及び認証サーバ１０４のハードウェア構成はユーザ端末１０２のハードウェア構成と同様である。

【００２６】

ユーザ端末１０２において、WWWブラウザのプログラムはＨＤＤ２１５に格納されている。ユーザからの指示に従って、WWWブラウザのプログラムがＲＡＭ２１６に読み出されて、ＣＰＵ２１０によって実行されることにより、WWWブラウザは起動する。情報処理装置１０１においては、WWWサーバのプログラムがＨＤＤ２０６に格納されている。情報処理装置１０１の電力が投入された後しばらくして、WWWサーバのプログラムがＲＡＭ２０３に読み出されて、ＣＰＵ２０２によって実行されることにより、WWWサーバは起動する。

【００２７】

WWWブラウザは、ユーザが指定するアドレス、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）或いは名称に基づいてWWWサーバと接続し、WWWサーバとの通信を開始する。このときの通信プロトコルとしてはＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）が用いられる。WWWブラウザはＨＴＴＰを使ってWWWサーバにアクセスし、コマンドの実行をWWWサーバに要求する。WWWサーバはコマンドを実行し、その結果を示す文書情報をWWWブラウザに送信する。このときの文書情報はＨＴＭＬ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）などによって記述されている。WWWブラウザは文書情報に基づいて画面を描画し、その画面をディスプレイ２１８に表示させる。

【００２８】

以下、本発明に係る情報処理を説明する。図３は情報処理装置１０１で行われる情報処理を示すフローチャートである。図３のフローチャートに基づくプログラムがＣＰＵ２０２によって実行されることにより、この情報処理が行われる。

【００２９】

情報処理装置１０１はユーザ端末１０２のWWWブラウザからのアクセスを受信する（ステップＳ３０１）。すると、情報処理装置１０１はＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）の設定が有効であるか無効であるかを判断する（ステップＳ３０２）。

【００３０】

図４は、ＳＳＬの設定を有効または無効にするための管理画面を示す図である。管理者の権限を有するユーザがWWWブラウザを使って情報処理装置１０１にアクセスし、管理者としての認証が成功した場合に、管理画面がWWWブラウザによって表示される。また、管理画面が操作部２０７によって表示されても良い。

【００３１】

図４において、オプションスイッチ４０１は、ＳＳＬの設定を有効または無効にするためのものである。ＳＳＬの設定が有効である場合には、ＳＳＬに基づく暗号化通信が使用可能であり、ＳＳＬの設定が無効である場合には、ＳＳＬに基づく暗号化通信が使用できない。ＳＳＬは、WWWブラウザとWWWサーバとの間のＨＴＴＰによる通信を暗号化技術によって保護するために用いられるプロトコルである。ＳＳＬを用いた暗号化通信が行われるためには、WWWサーバ（ここでは情報処理装置１０１）においてＳＳＬの設定が有効になっていなければならず、WWWブラウザがＳＳＬによる暗号化通信をできなければならない。情報処理装置１０１の初期値としては、ＳＳＬの設定は無効になっている。

【００３２】
情報処理装置１０１自身は独自のユーザ認証方式をサポートすることにより、情報処理装置１０１での認証処理に必要なパスワードが保護され、必ずしもＳＳＬによる暗号化通信は必要ではない。そのため、ＳＳＬの設定を無効にすることも可能である。
【００３３】
オプションスイッチ４０２は、ＳＳＬの設定が有効な場合に認証サーバによる認証処理を許可するか、またはＳＳＬの設定が有効であっても認証サーバによる認証処理を禁止するためのものである。
【００３４】
本来ならば、ＳＳＬを用いた暗号化通信では、送受信される情報は暗号化され、安全である。つまり、ＳＳＬの設定が有効であれば、認証サーバでの認証処理に必要なパスワードがユーザ端末１０２から情報処理装置１０１に送信されても安全であり、盗聴されにくい。ただし、認証サーバでの認証処理に用いられる認証情報がより厳重に管理されている環境では、その認証情報がネットワークを介して送信されること自体を防ぐために、認証サーバによる認証処理を許可したくない場合がある。そのために、オプションスイッチ４０２が設けられている。
【００３５】
フィールド４０３は認証サーバを登録するためのものである。管理者は、認証サーバの名称を入力することにより、複数の認証サーバを登録することができる。図４の例では、認証サーバ１０３及び認証サーバ１０４がそれぞれ登録されている。
【００３６】
図４の例では、認証サーバの名称が入力されるようにしたが、認証サーバを識別するその他の識別情報が入力されるようにしても良い。例えば、ネットワークがドメインと呼ばれる単位で管理されている環境では、ドメインごとに認証サーバが存在する。従って、各ドメインの名称（以下、ドメイン名）が認証サーバを識別する識別情報として用いられても良い。
【００３７】
また、ユーザが認証サーバの名称を入力するだけでなく、情報処理装置１０１がネットワーク上に存在する管理サーバから認証サーバの一覧を示す情報を自動的に取得し、その一覧に含まれている認証サーバの名称を登録しても良い。例えば、ネットワークに存在する機器の名称から機器のＩＰアドレスを検索するＤＮＳサーバが、複数の認証サーバの名称をＳＲＶレコードとして格納する。情報処理装置１０１は、ＤＮＳサーバのＳＲＶレコードから複数の認証サーバの名称を自動的に取得して、それらをフィールド４０３に表示する。
【００３８】
ＳＳＬの設定が無効であると図３のステップＳ３０２において判断された場合には、ＳＳＬを使わずに通信を継続する。情報処理装置１０１は、ログイン先として情報処理装置１０１のみを列挙して、ログイン画面を示す文書情報を生成する（ステップＳ３０３）。そして、情報処理装置１０１はログイン画面を示す文書情報をユーザ端末１０２に対して送信する（ステップＳ３０４）。
【００３９】
ＳＳＬの設定が無効である場合には、情報処理装置１０１による認証処理のみが許可される。認証サーバによる認証処理では、情報処理装置１０１がユーザ端末１０２に代わって認証サーバに対して認証処理の実行を要求する。そのため、情報処理装置１０１はユーザが入力したパスワードそのものを必要とし、ユーザによって入力されたパスワードそのものがユーザ端末１０２から情報処理装置１０１へ送信されなければならい。ＳＳＬを用いた暗号化通信が行われる場合には、パスワードが暗号化されるため、パスワードが盗聴されにくくなるが、ＳＳＬを用いた暗号化通信が行われない場合には、パスワードが盗聴されやすくなる。そのため、ＳＳＬの設定が無効である場合には、認証サーバによる認証処理は行われないようにした。

【００４０】
一方、情報処理装置１０１による認証処理では、下記に説明する方法により、ユーザが入力したパスワードそのものは送信されない。
【００４１】
図５は、ステップＳ３０４で送信された文書情報に基づいてＷＷＷブラウザによって表示されるログイン画面を示す図である。入力エリア５０１はユーザ名を入力するためのものであり、入力エリア５０２はパスワードを入力するためのものである。プルダウンメニュー５０３はログイン先を選択するためのものである。ユーザ名及びパスワードに基づく認証処理はログイン先によって行われる。図５のログイン画面では、ログイン先として情報処理装置１０１のみが選択可能になっている。
【００４２】
ユーザがユーザ名とパスワードとを入力し、ログイン先を選択し、ＯＫボタンを押下すると、ユーザ端末１０２は、認証処理の実行を要求するためのコマンド（以下、認証要求コマンド）を情報処理装置１０１に送信する。
【００４３】
情報処理装置１０１による認証処理では、ユーザによって入力されたパスワードそのものが情報処理装置１０１に送信される必要はない。ＷＷＷブラウザは、ユーザによって入力されたパスワードを一方向性を有する特定の関数（例えばハッシュ関数）で処理する。その特定の関数によって生成された値は元のパスワードへの逆変換が不可能になっている。
【００４４】
認証要求コマンドは、ユーザによって入力されたユーザ名と、特定の関数によって生成された値（以下、第２のパスワード）と、ユーザによって選択されたログイン先とを示す。
【００４５】
情報処理装置１０１はその認証要求コマンドをユーザ端末１０２から受信する（ステップＳ３０５）。ここで受信される認証要求コマンドが示すログイン先は必ず情報処理装置１０１である。そこで、情報処理装置１０１での認証処理が行われる（ステップＳ３０６）。
【００４６】
図６は、情報処理装置１０１で行われる認証処理を示すフローチャートである。図６のフローチャートに基づくプログラムがＣＰＵ２０２によって実行されることにより、この認証処理が行われる。
【００４７】
情報処理装置１０１のＨＤＤ２０６は、ユーザデータベース（以下、ユーザＤＢ）を保持している。ユーザＤＢは、情報処理装置１０１へのログインが許されているユーザに関し、ユーザ名及びパスワードの組を少なくとも１つ格納している。
【００４８】
そこで、情報処理装置１０１は、認証要求コマンドが示すユーザ名をユーザＤＢから検索する（ステップＳ６０１）。情報処理装置１０１は、検索の結果に基づいて、認証要求コマンドが示すユーザ名がユーザＤＢ内に存在するかどうかを判断する（ステップＳ６０２）。
【００４９】
認証要求コマンドが示すユーザ名がユーザＤＢ内に存在しない場合には、情報処理装置１０１は、認証が失敗した旨を示す文書情報をユーザ端末１０２に送信する（ステップＳ６０３）。ＷＷＷブラウザはその文書情報に基づいて、認証が失敗した旨をディスプレイ２１８に表示させる。
【００５０】
一方、認証要求コマンドが示すユーザ名がユーザＤＢ内に存在する場合には、情報処理装置１０１は、認証要求コマンドが示す第２のパスワードとユーザＤＢ内のパスワードと

を照合して、それらがお互いに対応するものかどうかを判断する（ステップＳ６０４）。ステップＳ６０４では、情報処理装置１０１はまず、ユーザＤＢ内から見つかったパスワードを先ほどの特定の関数で処理して、第２のパスワードを生成する。そして、情報処理装置１０１は、認証要求コマンドが示す第２のパスワードと、ユーザＤＢ内のパスワードから生成された第２のパスワードとが一致するかどうかを判断する。

【００５１】

２つの第２のパスワードが一致しなかった場合には、情報処理装置１０１は、認証が失敗した旨を示す文書情報をユーザ端末１０２に送信する（ステップＳ６０３）。２つの第２のパスワードが一致した場合には、情報処理装置１０１は、認証が成功した場合に限り送信されるべき文書情報をユーザ端末１０２に送信する（ステップＳ６０５）。例えば、図５のログイン画面を示す文書情報や、ユーザが情報処理装置１０１での印刷処理を操作するための操作画面を示す文書情報などがステップＳ６０５で送信される。

【００５２】

もちろん、ここで説明したユーザ名とパスワードとに基づく認証方法は一例に過ぎず、その他の方法によって認証が行われても良い。

【００５３】

ＳＳＬの設定が有効であると図３のステップＳ３０２において判断された場合には、情報処理装置１０１は、ＳＳＬによる暗号化通信が行われるようにするべく、ＳＳＬによるアクセスをリダイレクトする指示をユーザ端末１０２に送信する（ステップＳ３０６）。このリダイレクトの指示に従って、ＷＷＷブラウザは、ＷＷＷサーバへのアクセスで用いるポートを、ＨＴＴＰ通信で一般的に使用されているポートから、ＳＳＬで保護されたＨＴＴＰ通信で使用されるポートへ切り換える。ＨＴＴＰ通信で一般的に使用されているポートは例えば８０番のポートであり、ＳＳＬで保護されたＨＴＴＰ通信で使用されるポートは例えば４４３番のポートである。そして、ＷＷＷブラウザはＳＳＬを用いて４４３番のポートへアクセスしなおす。

【００５４】

情報処理装置１０１は、ユーザ端末１０２のＷＷＷブラウザからのアクセス（４４３番のポートへのアクセス）を受信する（ステップＳ３０７）。ステップＳ３０７での通信ではＳＳＬが用いられる。

【００５５】

つぎに、情報処理装置１０１は、認証サーバによる認証処理が許可されているか、禁止されているかを判断する（ステップＳ３０８）。認証サーバによる認証処理の許可または禁止は管理画面のオプションスイッチ４０２によって設定される。

【００５６】

ＳＳＬの設定が有効であっても認証サーバによる認証処理が禁止されている場合には、情報処理装置１０１はステップＳ３０３に進む。この場合には、情報処理装置１０１での認証処理のみが行われる。

【００５７】

認証サーバによる認証処理が許可されている場合には、情報処理装置１０１は、登録されている認証サーバが存在するかどうかを判断する（ステップＳ３０９）。登録されている認証サーバが存在しない場合には、情報処理装置１０１はステップＳ３０３に進む。

【００５８】

登録されている認証サーバが存在する場合には、情報処理装置１０１は、登録されている認証サーバを情報処理装置１０１と共にログイン先として列挙し、ログイン画面を示す文書情報を生成する（ステップＳ３１０）。そして、情報処理装置１０１はログイン画面を示す文書情報をユーザ端末１０２に対して送信する（ステップＳ３１１）。

【００５９】

図７は、ステップＳ３１１で送信された文書情報に基づいてＷＷＷブラウザによって表示されるログイン画面を示す図である。入力エリア７０１はユーザ名を入力するためのものであり、入力エリア７０２はパスワードを入力するためのものである。プルダウンメニ

ュー７０３はログイン先を選択するためのものである。図７のログイン画面では、ログイン先として情報処理装置１０１だけではなく、認証サーバ１０３や認証サーバ１０４も選択可能になっている。

【００６０】

ユーザがユーザ名とパスワードとを入力し、ログイン先を選択し、ＯＫボタンを押下すると、ユーザ端末１０２は認証要求コマンドを情報処理装置１０１に送信する。

【００６１】

ユーザがログイン先として情報処理装置１０１を選択した場合には、認証要求コマンドは、ユーザによって入力されたユーザ名と、ユーザによって入力されたパスワードから生成される第２のパスワードと、ユーザによって選択されたログイン先とを示す。ユーザがログイン先として認証サーバを選択した場合には、認証要求コマンドは、ユーザによって入力されたユーザ名と、ユーザによって入力されたパスワードと、ユーザによって選択されたログイン先とを示す。

【００６２】

情報処理装置１０１はその認証要求コマンドをユーザ端末１０２から受信する（ステップＳ３１２）。つぎに、情報処理装置１０１は、認証要求コマンドが示すログイン先が情報処理装置１０１であるか認証サーバであるかを判断する（ステップＳ３１３）。ログイン先が情報処理装置１０１である場合には、情報処理装置１０１はステップＳ３０６に進む。この場合には、情報処理装置１０１による認証処理が行われる。ログイン先が認証サーバである場合には、認証サーバによる認証処理が行われる（ステップＳ３１４）。

【００６３】

図８は、認証処理の実行を認証サーバに要求するための情報処理を示すフローチャートである。図８のフローチャートに基づくプログラムがＣＰＵ２０２によって実行されることにより、この情報処理が行われる。

【００６４】

情報処理装置１０１は、ユーザ端末１０２から受信した認証要求コマンドが示すユーザ名とパスワードとに基づいて、ログイン先として選択された認証サーバに対して所定のプロトコルで認証処理の実行を要求する（ステップＳ８０１）。所定のプロトコルとは、ログイン先として選択された認証サーバがサポートしているプロトコルである。例えば、ＮＴＬＭやＫｅｒｂｅｒｏｓなどのプロトコルがある。これらのプロトコルでは、ユーザ名やパスワードがそのまま情報処理装置１０１から認証サーバに送信されるのではなく、一連の安全な手順によって認証処理が行われる。

【００６５】

認証処理が認証サーバで行われた後、情報処理装置１０１は認証結果を認証サーバから受信する（ステップＳ８０２）。そして、情報処理装置１０１は、受信した認証結果に基づいて、認証が成功したか否かを判断する（ステップＳ８０３）。

【００６６】

認証が失敗したと判断された場合には、情報処理装置１０１は、認証が失敗した旨を示す文書情報をユーザ端末１０２に送信する（ステップＳ８０４）。ＷＷＷブラウザはその文書情報に基づいて、認証が失敗した旨をディスプレイ２１８に表示させる。

【００６７】

認証が成功したと判断された場合には、情報処理装置１０１は、認証が成功した場合に限り送信されるべき文書情報をユーザ端末１０２に送信する（ステップＳ８０５）。

【００６８】

（他の実施形態）

以上、本発明の実施形態について詳述したが、本発明は、複数の機器から構成されるシステムに適用しても良いし、また一つの機器からなる装置に適用しても良い。

【００６９】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムを、システム或いは装置に直接或いは遠隔から供給し、そのシステム或いは装置のコンピュータ

が該供給されたプログラムを読み出して実行することによっても達成され得る。その場合、プログラムの機能を有していれば、形態は、プログラムである必要はない。

【００７０】

従って、本発明の機能処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明のクレームでは、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。

【００７１】

プログラムを供給するための記録媒体としては、様々なものが使用できる。例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などである。

【００７２】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページからハードディスク等の記録媒体にダウンロードすることによっても供給できる。その場合、ダウンロードされるのは、本発明のコンピュータプログラムそのもの、もしくは圧縮され自動インストール機能を含むファイルであってもよい。

【００７３】

また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明のクレームに含まれるものである。

【００７４】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布する形態としても良い。その場合、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせ、その鍵情報を使用することにより暗号化されたプログラムが実行可能な形式でコンピュータにインストールされるようにする。

【００７５】

また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される形態以外の形態でも実現可能である。例えば、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現され得る。

【００７６】

更に、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれるようにしてもよい。この場合、その後で、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される。

【図面の簡単な説明】

【００７７】

【図１】ネットワークシステムの構成を示す図である。

【図２】情報処理装置１０１とユーザ端末１０２とのハードウェア構成を示す図である。

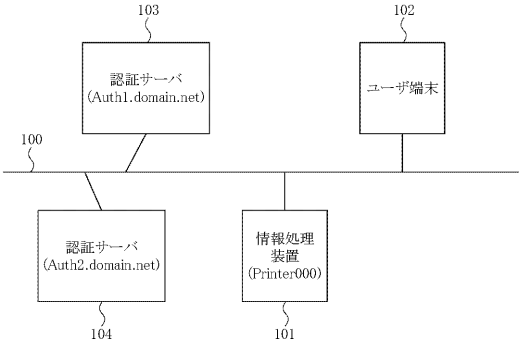
【図３】情報処理装置１０１で行われる情報処理を示すフローチャートである。

【図４】ＳＳＬの設定を有効または無効にするための管理画面を示す図である。

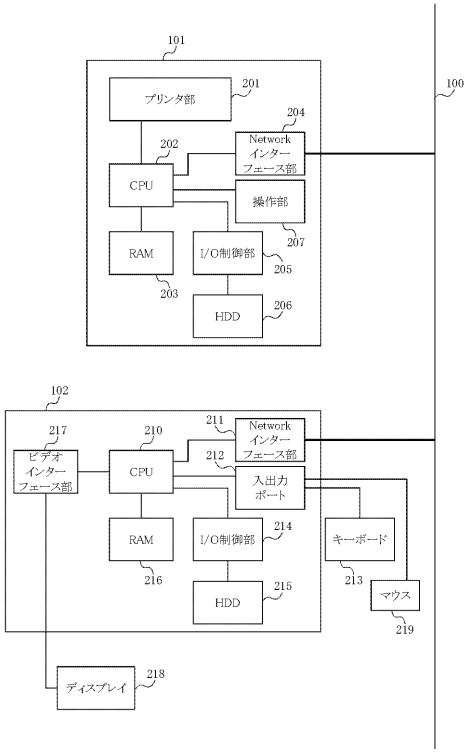
【図５】ＷＷＷブラウザによって表示されるログイン画面を示す図である。

【図６】情報処理装置１０１で行われる認証処理を示すフローチャートである。
【図７】ＷＷＷブラウザによって表示されるログイン画面を示す図である。
【図８】認証処理の実行を認証サーバに要求するための情報処理を示すフローチャートである。
【符号の説明】
【００７８】
１００　ネットワーク
１０１　情報処理装置
１０２　ユーザ端末
１０３　認証サーバ
１０４　認証サーバ
２０１　プリンタ部
２０２　ＣＰＵ
２０３　ＲＡＭ
２０４　ネットワークインターフェース部
２０５　Ｉ／Ｏ制御部
２０６　ＨＤＤ
２０７　操作部
２１０　ＣＰＵ
２１１　ネットワークインターフェース部
２１２　入出力ポート
２１３　キーボード
２１４　Ｉ／Ｏ制御部
２１５　ＨＤＤ
２１６　ＲＡＭ
２１７　ビデオインターフェース部
２１８　ディスプレイ
２１９　マウス

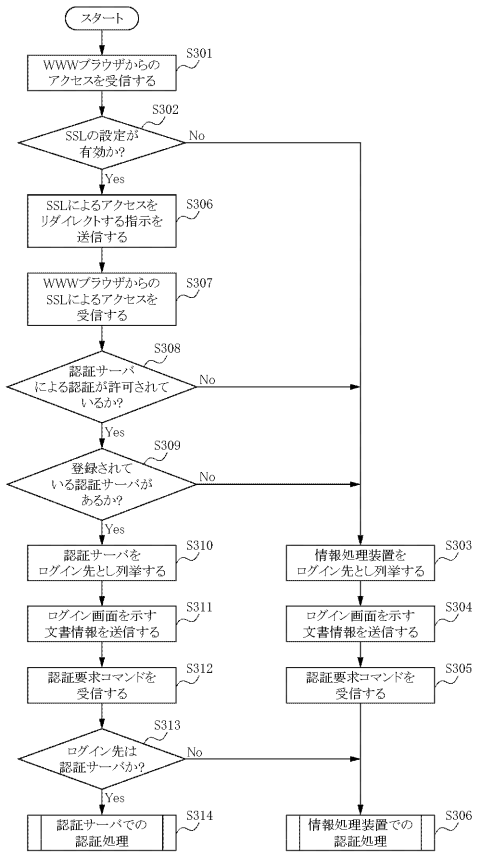
【図１】


103
認証サーバ
(Auth1.domain.net)
102
ユーザ端末
100
認証サーバ
(Auth2.domain.net)
104
情報処理
装置
(Printer000)
101

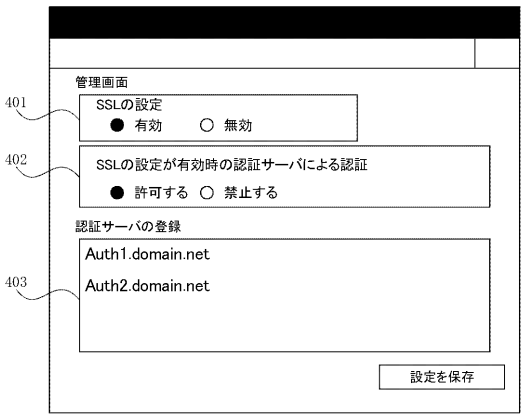
【図２】


101
プリンタ部
201
100
204
Network
インター
フェース部
202
CPU
操作部
207
RAM
I/O制御部
205
203
HDD
206
102
217
210
211
Network
インター
フェース部
ビデオ
インター
フェース部
CPU
212
入出力
ポート
RAM
I/O制御部
214
キーボード
216
213
HDD
215
マウス
219
ディスプレイ
218

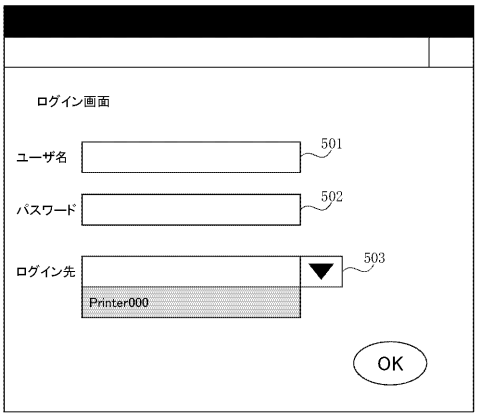
【図３】


スタート
WWWブラウザからの
アクセスを受信する
S301
SSLの設定が
有効か?
S302
No
Yes
SSLによるアクセスを
リダイレクトする指示を
送信する
S306
WWWブラウザからの
SSLによるアクセスを
受信する
S307
認証サーバ
による認証が許可されて
いるか?
S308
No
Yes
登録されて
いる認証サーバが
あるか?
S309
No
Yes
認証サーバを
ログイン先とし列挙する
S310
ログイン画面を示す
文書情報を送信する
S311
認証要求コマンドを
受信する
S312
ログイン先は
認証サーバか?
S313
No
Yes
認証サーバでの
認証処理
S314
情報処理装置を
ログイン先とし列挙する
S303
ログイン画面を示す
文書情報を送信する
S304
認証要求コマンドを
受信する
S305
情報処理装置での
認証処理
S306

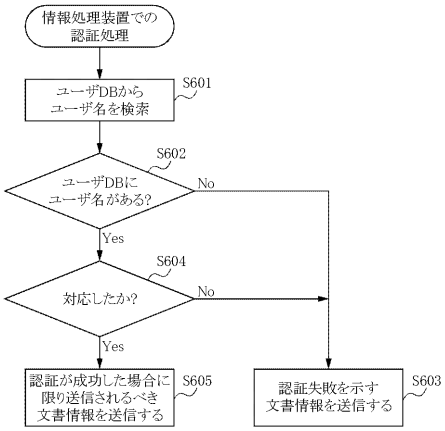
【図４】


管理画面
401
SSLの設定
● 有効 ○ 無効
402
SSLの設定が有効時の認証サーバによる認証
● 許可する ○ 禁止する
認証サーバの登録
403
Auth1.domain.net
Auth2.domain.net
設定を保存

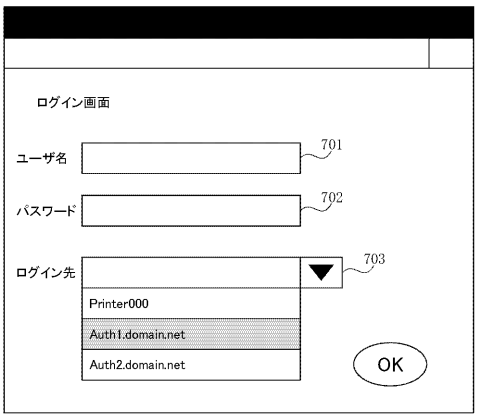
【図５】


ログイン画面
ユーザ名
501
パスワード
502
ログイン先
503
Printer000
OK

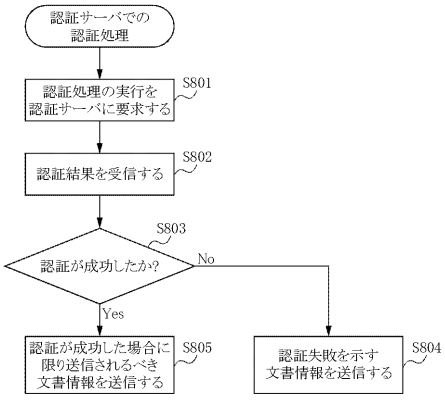
【図６】


情報処理装置での
認証処理
ユーザDBから
ユーザ名を検索
S601
S602
ユーザDBに
ユーザ名がある?
No
Yes
S604
対応したか?
No
Yes
認証が成功した場合に
限り送信されるべき
文書情報を送信する
S605
認証失敗を示す
文書情報を送信する
S603

【図７】


ログイン画面
ユーザ名
701
パスワード
702
ログイン先
703
Printer000
Auth1.domain.net
Auth2.domain.net
OK

【図８】


認証サーバでの
認証処理
認証処理の実行を
認証サーバに要求する
S801
認証結果を受信する
S802
S803
認証が成功したか?
No
Yes
認証が成功した場合に
限り送信されるべき
文書情報を送信する
S805
認証失敗を示す
文書情報を送信する
S804

フロントページの続き

(51)Int.Cl. FI
B41J 29/38 Z

(56)参考文献 特開２００３－３４５７８９（ＪＰ，Ａ）
特開２００６－０１８３９９（ＪＰ，Ａ）
特表２００７－５００９７６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０