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

特許第4140617号
(P4140617)

(45)発行日　平成20年8月27日(2008.8.27)　(24)登録日　平成20年6月20日(2008.6.20)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	673A
G06F 21/20	(2006.01)	H04L	9/00	673C
G06K 17/00	(2006.01)	H04L	9/00	673E
G06K 19/10	(2006.01)	G06F	15/00	330G
G09C 1/00	(2006.01)	G06K	17/00	T

請求項の数 3　(全 11 頁)　最終頁に続く

(21)出願番号　特願2005-118704 (P2005-118704)
(22)出願日　平成17年4月15日 (2005.4.15)
(62)分割の表示　特願2000-100337 (P2000-100337)の分割
原出願日　平成12年4月3日 (2000.4.3)
(65)公開番号　特開2005-237037 (P2005-237037A)
(43)公開日　平成17年9月2日 (2005.9.2)
審査請求日　平成17年4月15日 (2005.4.15)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100113077
弁理士　高橋　省吾
(74)代理人　100112210
弁理士　稲葉　忠彦
(74)代理人　100108431
弁理士　村上　加奈子
(74)代理人　100128060
弁理士　中鶴　一隆
(72)発明者　荒木　紀之
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】認証用記録媒体を用いた認証システムおよび認証用記録媒体の作成方法

(57)【特許請求の範囲】

【請求項１】

公開鍵を用いて暗号化された利用者のＩＤ及びパスワードが記録された認証用記録媒体から前記公開鍵に対応する秘密鍵を用いて利用者のＩＤ及びパスワードを復元し、その復元した利用者のＩＤ及びパスワードをブロック暗号により暗号化したものと前記利用者が入力部に入力したＩＤ及びパスワードとを前記利用者が指定した暗号アルゴリズムにより暗号化して認証データを作成し、その作成した認証データと当該認証データを復号化する復号鍵及び前記暗号アルゴリズムの情報を含む暗号パラメータとを送信する端末装置と、前記暗号パラメータに含まれる前記復号鍵及び前記暗号アルゴリズムの情報を用いて前記認証データから前記ブロック暗号により暗号化した利用者のＩＤ及びパスワードと前記利用者により入力されたＩＤ及びパスワードとを復号化し、その復号化した前記ブロック暗号により暗号化した前記利用者のＩＤ及びパスワードから前記利用者のＩＤ及びパスワードを復元し、その復元した前記利用者のＩＤ及びパスワードと前記利用者により入力されたＩＤ及びパスワードとを比較してユーザ認証を行う認証装置を備えた認証用記録媒体を用いた認証システム。

【請求項２】

前記認証装置は、ネットワークに接続されたサーバ装置である請求項１記載の認証用記録媒体を用いた認証システム。

【請求項３】

利用者のアクセスが管理された装置のユーザ認証に用いられる認証用記録媒体の作成方法

において、前記装置に対するアクセスを許可する利用者から通知されたＩＤ及びパスワードと前記装置の管理者が前記利用者に割り当てた鍵番号とを入力部に入力する工程と、前記管理者によって管理された利用者毎の鍵番号及びこれら鍵番号に対応する公開鍵が記録された情報と前記入力部に入力された利用者の鍵番号とから当該鍵番号に対応する公開鍵を選択し、その公開鍵を用いて前記入力部に入力された前記利用者のＩＤ及びパスワードを暗号化する工程と、その暗号化された前記利用者のＩＤ及びパスワードの暗文と前記利用者に割り当てられた鍵番号とを前記利用者の認証用記録媒体に書き込む工程とを備えた認証用記録媒体の作成方法。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、オープンネットワークシステムにおけるセキュリティに関するものであり、特にサーバまたは受信端末装置により実行される認証方法、認証用記録媒体を用いた認証システムおよび認証用記録媒体の作成方法に関する。

【背景技術】

【０００２】

従来の認証方法は、サーバに予め登録され、管理されているユーザのＩＤ、パスワードと、ユーザから送信されてきたＩＤとパスワードを比較し、両者が一致する場合に、ユーザ本人であることを確認する認証を行っていた。例えば、図８に、特開平１１－１４９４５２号公報に開示された認証方法の処理フローチャートを示す。特開平１１－１４９４５２号公報に開示された認証方法によると、端末装置はログイン名を暗号鍵として暗号化した（Ｓ８０５、Ｓ８０６）パスワードをホスト装置に送信する。ホスト装置は、予め登録されているログイン名を暗号鍵としてパスワードを暗号化する（Ｓ８０８）。そして、端末装置にて暗号化されて送信されたパスワードと、ホスト装置にて暗号化されたパスワードを比較して（Ｓ８０９）認証を行うものである。

【０００３】

また、特開平７－３２５７８５号公報に開示された認証方法によると、クライアントは、ユーザから入力されたＩＤとパスワード、およびサーバから発行された乱数を、サーバの公開鍵（Ｋｐ）で暗号化してサーバへ送信する。サーバは自分の秘密鍵（Ｋｓ）で、クライアントから送信されたＩＤ、パスワード、乱数を復号化して、この復号化された乱数とサーバが発行した乱数が一致するか確認して認証を行うものである。

【０００４】

また、特開平５－２８２３４９号公報には、例えば銀行オンラインシステムに採用されるコンピュータシステムの安全保証方式に関し、盗難や偽造によるカードの不正使用を防止するために磁気カード（キャッシュカード）に暗号化した暗証番号を記録しておき、この磁気カードに記録された暗号化されている暗証番号を現金自動支払い機（ＣＤ）や自動窓口装置（ＡＴＭ）等の端末装置に読取らせ、その読取った暗号化されている暗証番号から復元した通常の暗証番号と端末装置のキーボードから入力した暗証番号とを比較し、それらが一致したときに業務を実行できるようにすることが記載されている。

【０００５】

【特許文献１】特開平１１－１４９４５２号公報（第４－５頁、図２）

【特許文献２】特開平７－３２５７８５号公報（第４－５頁、図３）

【特許文献３】特開平５－２８２３４９号公報（第２頁、図１－２）

【発明の開示】

【発明が解決しようとする課題】

【０００６】

ところで、従来の認証方法によると、サーバにはユーザのＩＤ、パスワードが登録されており、ユーザから送信されたＩＤ、パスワードとサーバに登録されたＩＤ、パスワードを比較して一致を確認するという点で、サーバ主導で認証が行われている。しかしながら

、多数のユーザのＩＤ、パスワードがサーバの管理下にあるため、サーバに対するハッキングやサーバ管理者の不正行為により多数のユーザのＩＤ、パスワードが漏洩する可能性があり、セキュリティやプライバシー保護の観点から改善が必要である。特にユーザのパスワードが漏洩すると、ネットワークを利用した電子商取引や電子メールなど通信の秘密が保証されないという点でユーザのリスクが大きくなる。

【０００７】

この発明は、上記のような課題を解決するためになされたもので、第三者による認証装置に対する不正行為や認証用記録媒体に書き込まれた利用者のＩＤとパスワードの読み出し等によって利用者のパスワードが外部に漏洩する危険性を抑制することができる新規な認証用記録媒体を用いた認証システムおよび認証用記録媒体の作成方法を提供することを目的とする。

【課題を解決するための手段】

【０００８】

この発明に係る認証用記録媒体を用いた認証システムは、公開鍵を用いて暗号化された利用者のＩＤ及びパスワードが記録された認証用記録媒体から前記公開鍵に対応する秘密鍵を用いて利用者のＩＤ及びパスワードを復元し、その復元した利用者のＩＤ及びパスワードをブロック暗号により暗号化したものと前記利用者が入力部に入力したＩＤ及びパスワードとを前記利用者が指定した暗号アルゴリズムにより暗号化して認証データを作成し、その作成した認証データと当該認証データを復号化する復号鍵及び前記暗号アルゴリズムの情報を含む暗号パラメータとを送信する端末装置と、前記暗号パラメータに含まれる前記復号鍵及び前記暗号アルゴリズムの情報を用いて前記認証データから前記ブロック暗号により暗号化した利用者のＩＤ及びパスワードと前記利用者により入力されたＩＤ及びパスワードとを復号化し、その復号化した前記ブロック暗号により暗号化した前記利用者のＩＤ及びパスワードから前記利用者のＩＤ及びパスワードを復元し、その復元した前記利用者のＩＤ及びパスワードと前記利用者により入力されたＩＤ及びパスワードとを比較してユーザ認証を行う認証装置を備えたものである。

【０００９】

この発明に係る認証用記録媒体の作成方法は、利用者のアクセスが管理された装置のユーザ認証に用いられる認証用記録媒体の作成方法において、前記装置に対するアクセスを許可する利用者から通知されたＩＤ及びパスワードと前記装置の管理者が前記利用者に割り当てた鍵番号とを入力部に入力する工程と、前記管理者によって管理された利用者毎の鍵番号及びこれら鍵番号に対応する公開鍵が記録された情報と前記入力部に入力された利用者の鍵番号とから当該鍵番号に対応する公開鍵を選択し、その公開鍵を用いて前記入力部に入力された前記利用者のＩＤ及びパスワードを暗号化する工程と、その暗号化された前記利用者のＩＤ及びパスワードの暗文と前記利用者に割り当てられた鍵番号とを前記利用者の認証用記録媒体に書き込む工程とを備えたものである。

【発明の効果】

【００１０】

この発明によれば、端末装置から送信された認証データを認証装置が受信してユーザ認証を行うので、各利用者の端末装置毎に認証機能を設ける必要がなく、複数の利用者が認証要求する場合においても容易にユーザ認証を行うことができる。また、認証装置において各利用者のパスワードを知らなくてもユーザ認証を行うことができるので、当該認証装置に対する不正行為によって利用者のパスワードが外部に漏洩する危険性を抑制することができる。

【００１１】

また、この発明によれば、管理者によって管理された利用者毎の鍵番号及びこれら鍵番号に対応する公開鍵の情報と入力部に入力された利用者の鍵番号とから当該鍵番号に対応する公開鍵を選択し、その公開鍵を用いて前記入力部に入力された前記利用者のＩＤ及びパスワードを暗号化して前記利用者の認証用記録媒体に書き込むので、第三者は認証用記録媒体に書き込まれた利用者のＩＤとパスワードを認証用記録媒体から読み出すことも改

窺することもできず、利用者のパスワードが外部に漏洩する危険性を抑制でき、第三者による認証用記録媒体の不正利用をも防止することができる。

【発明を実施するための最良の形態】

【００１２】

実施の形態１．

図１は本発明に係る認証方法の処理を説明するフローチャートである。図２は本発明に係る認証方法の処理を説明するフローチャートである。図３は本発明に係るコンピュータ通信システムの一例を示す概念図である。図４は端末装置の構成を示すブロック図である。図５はサーバの構成を示すブロック図である。図６は本発明に係る認証用記録媒体作成装置の構成を示すブロック図である。図７は暗号パラメータの一例を示す説明図である。

【００１３】

本発明に係るコンピュータ通信システムの一例について、図３を参照して説明する。図３において、１は送信側ユーザ端末装置、２はサーバである認証装置（以下、サーバと記載する）、３は通信ネットワーク、４はサーバである認証装置（以下、サーバと記載する）、５は受信側ユーザ端末装置である。サーバ２、サーバ４は端末装置１、端末装置５のユーザが、自ら名乗ったとおりの者、すなわち、通信システム３の使用を認められた本人であるか確認する「認証」を行うことにより、端末装置１、５の通信ネットワーク３へのアクセスを制御する。端末装置１、５間における電子メールを用いた通信は、サーバ２、４による認証を受けて通信ネットワーク３へのアクセスを許可された後に通信ネットワーク３を介して行われる。一方、端末装置１からの電子メールを受信した端末装置５は、電子メールの発信者が本人からのものであるか確認する認証を行うことにより、第３者が本人であると詐称する「なりすまし」を防止する。

【００１４】

次に、図３に示す端末装置１、５の構成について、図４を参照して説明する。図４において、６は認証用記録媒体、７は端末装置（図３に示す１、５）、８は認証データ作成部、９は認証部、１０は媒体入力部、１１は復号化処理部、１２は暗号化処理部、１３は入力部、１４は鍵入力部、１５は暗号パラメータ処理部、１６は認証データ保管部、１７は通信処理部、１８は鍵読取部、１９は第一の復号化処理部、２０は第二の復号化処理部、２１は比較判定部である。端末装置１、端末装置５は、ユーザ本人のＩＤとパスワードを暗号化して記録した認証用記録媒体から読み出したＩＤ、パスワードと、および、ユーザ本人が端末装置に入力したＩＤとパスワードとを暗号化した認証データを作成する認証データ作成部８と、受信した認証データに含まれる、認証用記録媒体から読み出されたＩＤとパスワードと、ユーザ本人が入力したＩＤとパスワードを復号化して読み出し、２種類のパスワードを比較して認証を行う認証部９より構成されている。

【００１５】

認証データ作成部８は、認証用記録媒体６から暗号化されたＩＤとパスワードを読み出す媒体入力部１０、媒体入力部１０が読み出したＩＤ、パスワードを復号化する復号化処理部１１、復号化処理部１１が復号化したＩＤとパスワードを、認証用記録媒体６からＩＤとパスワードを読み出した時間情報（年・月・日・時間）より作成された暗号鍵を用いて、ブロック暗号により暗号化する暗号化処理部１２、ユーザにより端末装置７に直接入力されたＩＤとパスワードの入力を受け付ける入力部１３、共通鍵暗号方式の暗号アルゴリズムのうち、ユーザが選択した暗号アルゴリズムの種類、暗号鍵、暗号化に用いる変換表の入力を受け付ける鍵入力部１４、暗号化処理部１２によりブロック暗号を用いて暗号化された暗文、および入力部１３から入力されたＩＤとパスワードの平文を、ユーザにより選択された、暗号アルゴリズム、暗号鍵、変換表を用いて暗号化して認証データを作成するとともに、鍵入力部１４を介して入力された暗号アルゴリズムの種類、暗号鍵、変換表を含み、受信側で認証データを復号化するための情報となる暗号パラメータを作成する暗号パラメータ処理部１５より構成される。

【００１６】

認証部９は、暗号パラメータより暗号アルゴリズムの種類、暗号鍵、変換表の種類を読

み取る鍵読取部１８、鍵読取部１８が読み出した暗号鍵を復号鍵として（共通鍵暗号方式の暗号の場合、暗号鍵と復号鍵は同一である）、認証データを復号化して、認証用記録媒体のＩＤとパスワードの暗文とユーザから入力されたＩＤとパスワードの平文を得る第一の復号化処理部１９、認証用記録媒体のＩＤとパスワードの暗文を復号化して平文を得る第二の復号化処理部２０、第一の復号化処理部１９からのＩＤとパスワードの平文と、第二の復号化処理部２０からのＩＤとパスワードの平文とを比較する比較判定部２１より構成される。図３に示す端末装置１は図４に示す認証データ作成部８において作成された認証データと暗号パラメータを送信する処理を行い、端末装置５は端末装置１から送信された認証データを認証部９において認証する処理を行う。

【００１７】

次に、図３に示すサーバである認証装置２、４の構成について、図５を参照して説明する。図５において、２２はサーバ、２３は通信処理部、２４は認証データ保管部、２５は鍵読取部、２６は第一の復号化処理部、２７は第二の復号化処理部、２８は比較判定部である。図５に示すサーバ２２は、図４に示す端末装置７の認証部９と同様の構成を採用し、同様の処理を行うことにより認証を行うので説明は省略する。

【００１８】

次に、図４に示す認証用記録媒体６を作成する認証用記録媒体作成装置について、図６を参照して説明する。図６において、２９は認証用記録媒体作成装置、３０は認証用記録媒体、３１は入力部、３２は暗号化処理部、３３は出力部、３４は格納部である。認証用記録媒体３０は、認証用記録媒体作成装置２９を用いて認証用記録媒体を作成する媒体作成者と、暗号鍵を管理する管理者により作成される。認証用記録媒体作成装置２９は公開鍵暗号方式の暗号アルゴリズムを用いてユーザのＩＤとパスワードを暗号化して認証用記録媒体３０の格納部３４に書き込むことによりユーザが本人であることを証明する認証用記録媒体を作成する。

【００１９】

ユーザは、認証用記録媒体を発行してもらうためにＩＤとパスワードを媒体作成者に通知する。媒体作成者はユーザ用に割り当てた鍵番号と、ユーザから通知されたＩＤとパスワードを入力部３１に入力する。入力された鍵番号と、ユーザのＩＤ、パスワードは入力部３１を介して暗号化処理部３２に伝達される。暗号化処理部３２には、鍵番号に対応する公開鍵が記録されており、入力された公開鍵番号に対応する公開鍵を選択して、ＩＤとパスワードを暗号化する。暗号化されたＩＤとパスワードは鍵番号とともに出力部３３を介して認証用記録媒体３０の格納部３４に書き込まれる。

【００２０】

なお、媒体作成者はユーザ毎に割り当てた鍵番号を知ることはできるが、ＩＤとパスワードを暗号化する公開鍵を知ることはできない。鍵番号と公開鍵の対応は、暗号鍵を管理するシステムの管理者のみが知ることができる。認証用記録媒体内に記録されている暗号化されたＩＤとパスワードは、媒体作成者及びユーザ本人も自由に変更できない。また、第３者は暗号化した公開鍵に対応する秘密鍵を知ることができないため、ＩＤとパスワードを認証用記録媒体から読み出すことも改竄することも不可能である。したがって、認証時にユーザ本人により入力されるＩＤ、パスワードと認証用記録媒体内のＩＤ、パスワードが一致すれば、認証用記録媒体を所持するユーザが本人であることを確認することができる。

【００２１】

以上を踏まえて本発明に係る認証方法について、図１および図２を参照して説明する。図１には、図３に示すサーバ２、４により実行される通信ネットワーク３へのアクセス制御を目的とした認証方法が示されている。ステップＳ１０５～ステップＳ１１２までは送信側の端末装置１による認証データ作成工程であり、ステップＳ１１３～ステップＳ１１９まではサーバ２による認証工程である。以下、認証データ作成工程から説明する。ステップＳ１０１において、図３に示す送信ユーザ端末装置１はサーバ２に対して認証開始パケットを送信する処理を行う。ステップＳ１０２において、サーバ２は、端末装置１から

の認証開始要求を受け付け、ステップＳ１０３において、端末装置１に認証開始のプロンプトを送信する。ステップＳ１０４において、端末装置１はサーバ２からの認証開始プロンプトを受信する。ステップＳ１０５において、認証開始プロンプトを確認した送信ユーザは、図４に示す認証用記録媒体６を端末装置に挿入する。

【００２２】

ステップＳ１０６において、端末装置１は媒体入力部１０を介して認証用記録媒体６から読み出したＩＤ、パスワードの暗文を、復号化処理部１１で鍵番号ｉの公開鍵（認証用記録媒体内のＩＤ、パスワードの暗号化に用いられた暗号鍵）に対応する秘密鍵で復号化してＩＤ、パスワードの平文を得る。ステップＳ１０７において、暗号化処理部１２は復号化処理部１１で復号化したＩＤ・ＰＷをブロック暗号により暗号化する。ブロック暗号とは、複数バイトを一度に暗号化する暗号方式である。ステップＳ１０７の暗号化に用いる暗号鍵は、送信ユーザが端末装置に媒体を挿入した時点の、年・月・日・時間等の時間情報により自動設定される。ステップＳ１０７において暗号化されたＩＤ、パスワードの暗文と、暗号鍵の平文は暗号パラメータ処理部１５に伝送される。

【００２３】

ステップＳ１０８において、送信ユーザは送信ユーザ端末装置に本人のＩＤ・ＰＷを直接入力する。ユーザにより入力されたＩＤ、パスワードは入力部１３を介して暗号パラメータ処理部１５に出力される。また、ステップＳ１０９において、送信ユーザは、暗号化に用いる暗号アルゴリズムと変換表、暗号鍵を指定し、鍵入力部１４を介して端末装置に入力する。鍵入力部１４を介して送信ユーザにより指定された暗号アルゴリズムと変換表、暗号鍵は暗号パラメータ処理部１５に伝達される。ステップＳ１１０において、暗号パラメータ処理部１５は、暗号化処理部１２で暗号化されたＩＤ、パスワードの暗文と、この暗号化に用いられた暗号鍵の平文、および入力部１３を介して送信ユーザにより直接入力されたＩＤ、パスワードの平文を、送信ユーザにより指定された暗号アルゴリズムと変換表、暗号鍵を用いて暗号化して認証データを生成する。

【００２４】

また、ステップＳ１１０において、暗号パラメータ処理部１５は認証データを作成するとともに、この認証データを作成するにあたって使用した暗号アルゴリズム、変換表、暗号鍵を含み、認証データとともに送信される暗号パラメータを作成する。暗号パラメータは、認証データを復号化するために必要な情報を受信側の認証装置に提供するものであり、認証データの暗号化に用いた暗号アルゴリズム、変換表、暗号鍵を含むものである。図３に示すサーバ２あるいは受信側ユーザ端末装置５は、送信側ユーザ端末装置から送信されてきた認証データと暗号パラメータを受信して、暗号パラメータから暗号アルゴリズム、変換表、暗号鍵を読み出して認証データを復号化して認証を行う。暗号パラメータの一例を図７に示す。図７「暗号パラメータのフォーマット」に示すように、暗号パラメータ（Key.s）は、送信ユーザにより選択されて認証データの暗号化に用いられた暗号アルゴリズム、変換表、暗号鍵の３つの情報を含んでいる。

【００２５】

例えば、図７「使用可能な暗号アルゴリズム」に示すように、使用可能な暗号アルゴリズムとして「複合シフトレジスタ（１０）」、「ＤＥＳ（１１）」等があるとする。そして、「入力例」に示すように、暗号アルゴリズムとして「ＤＥＳ（１１）」、変換表として「第３２表」、暗号鍵として「0123456789abcde」を設定したとする。その場合、「暗号パラメータの設定例」に示すように、暗号パラメータKey.sは「11320123456789abcde」となる。この暗号パラメータは、単に暗号アルゴリズムおよび変換表の番号と暗号鍵をそのまま並べて作成したものである。しかしながら、暗号パラメータは認証データとともに送信されるものであり、しかも認証データを復号化する情報を含んでいるものであるから、実際にはより複雑な形式に加工してセキュリティ強度を上げて使用される。ステップＳ１１１において、暗号パラメータ処理部１５で生成された認証データと暗号パラメータは認証データ保管部１６に出力される。ステップＳ１１２において、通信処理部１７は認証データ保管部１６に保管された認証データと暗号パラメータを読み出して送信する。

【００２６】
以下のステップは、図３に示すサーバ２、あるいは図５に示すサーバ２２により実行される認証工程である。ステップＳ１１３において、サーバ２２の通信処理部２３は、図４に示す端末装置７から送信された認証データと暗号パラメータを受信する。受信した認証データは認証データ保管部２４に保管された後、鍵読取部２５において自動的に暗号パラメータより暗号アルゴリズム、変換表、暗号鍵を読み取り、認証データの復号化に必要な情報を認識する。ステップＳ１１４において、第一の復号化処理部２６は、鍵読取部２５が読み出した変換表と暗号鍵を用いて認証データを復号化し、送信側ユーザが端末装置に直接入力したＩＤ、パスワードの平文と、ブロック暗号で暗号化されているＩＤ、パスワードの暗文、およびその暗号鍵を読み出す。。

【００２７】
ステップＳ１１５において、第二の復号化処理部２７はＩＤ、パスワードの暗文を第一の復号鍵により復号化して、認証用記録媒体内に記録されていたＩＤ、パスワードの平文を得る。ステップＳ１１６において、比較判定部２８は、ユーザから入力されたＩＤ、パスワードと、認証用記録媒体内に記録されていたＩＤ、パスワードとを比較して両者が一致している確認する。ステップＳ１１７において、両者が一致していれば送信ユーザは本人であると判断し、ステップＳ１１８において認証確認のプロンプトを送信側ユーザ端末装置に送信する。一方、ステップＳ１１７において、両者が一致しなければ送信ユーザは本人ではない第３者と判断し、ステップＳ１１９において認証未確認のプロンプトを送信側ユーザ端末装置に送信する。

【００２８】
次に、図３に示す送信側ユーザ端末装置１、受信側ユーザ端末装置５間で実行される、送信ユーザが自ら名乗ったとおりの本人であるか確認することを目的とする認証方法について図２を参照して説明する。なお、図２に示すステップＳ２０１以降の処理を実行する前に、端末装置１と端末装置５（ともに図４に示す端末装置７）はそれぞれサーバ２、サーバ４の認証を受け、通信ネットワーク３へのログインを許可されているものとする。ステップＳ２０１において、端末装置１は送信する電子メール本文に図１に示すステップＳ１０５からステップＳ１１２で作成した認証データ、暗号パラメータを添付する。そして、ステップＳ２０２において端末装置５あてに認証データ、暗号パラメータが添付された電子メールを送信する。ステップＳ２０３において、端末装置５は、端末装置１から送信された電子メールを受信する。

【００２９】
ステップＳ２０４において、端末装置５の図４に示す鍵読取部１８は、暗号パラメータより暗号アルゴリズム、変換表、暗号鍵を読み出し、第一の復号化処理部１９は変換表、暗号鍵を用いて認証データを復号化し、ユーザにより入力されたＩＤ、パスワードの平文と、認証用記録媒体から読み出されたＩＤ、パスワードがブロック暗号により暗号化された暗文と、ブロック暗号鍵の平文を得る。ステップＳ２０５において、第二の復号化処理部２０は、ブロック暗号により暗号化された暗文をブロック暗号鍵を用いて復号化して、認証用記録媒体に記録されていたＩＤ、パスワードの平文を得る。そして、ステップＳ２０６において、比較判定部２１は、ユーザから入力されたＩＤ、パスワードと、認証用記録媒体に記録されていたＩＤ、パスワードとを比較して両者が一致するか確認する。ステップＳ２０７において、両者が一致した場合、ステップＳ２０８において認証確認メッセージが受信側ユーザ端末装置の表示画面に表示される。一方、両者が不一致であった場合、認証未確認メッセージが表示画面に表示される。

【００３０】
以上説明したように、上記説明による認証方法は、暗号化されたＩＤ、パスワードを記録した認証用記録媒体から読み出したＩＤ、パスワードと、ユーザが端末装置に入力したＩＤ、パスワードを暗号化した認証データを作成してサーバに送信し、サーバは認証データを復号化して、認証データに含まれる認証用記録媒体のＩＤ、パスワードと、ユーザが入力したＩＤ、パスワードの一致を確認することにより認証を行うので、サーバはユーザ

のＩＤさえ管理しておけば、ユーザのパスワードを知らなくても認証を行うことが可能である。したがって、サーバにユーザのパスワードを管理させる必要がなくなり、サーバに対する不正行為によってユーザのパスワードが外部に漏洩する危険性を抑制することができる。

【００３１】

また、上記認証方法は、サーバによるネットワークへのアクセス制御を目的とする認証のみならず、受信側ユーザにより、送信者が自ら名乗ったとおりの本人であることを確認する認証にも適用できるので、コンピュータ通信の信頼性が確保される。

【００３２】

また、上記認証方法は、認証データを復号化するための情報を暗号パラメータに含ませておくことにより、サーバなどの受信側でユーザによる操作を必要とせず、自動的に認証データを復号化することが可能となる。また、この暗号パラメータを使用することにより、ユーザは暗号化に用いる暗号アルゴリズムを自由に設定変更でき、受信側にもその内容を通知することができるので、通信を傍受する第３者が、使用されている暗号アルゴリズムを推測することは困難になる。

【００３３】

また、上記説明による認証用記録媒体は、ユーザのＩＤ、パスワードを暗号化して記録するので、認証用記録媒体を取得した者が認証用記録媒体内のＩＤ、パスワードを知ることはできない。また、認証用記録媒体内のデータを改ざんすることもできないので、認証用記録媒体内のＩＤ、パスワードを他のＩＤ、パスワードに改ざんして通信ネットワークにアクセスする事もできないので、認証用記録媒体の所有者になりすます不正行為を防止することができる。

【００３４】

また、上記端末装置は、認証データをユーザ自身が選択した暗号アルゴリズムを用いて作成し、この暗号化に用いた暗号アルゴリズム、復号鍵、変換表を含み、受信側で認証データを復号化するのに必要な情報となる暗号パラメータを認証データとともに送信するので、送受信者間で自由に暗号アルゴリズムを設定でき、通信を傍受した第３者に対する通信の守秘性が高められる。また、自動的に認証データを復号化して認証を行うことが可能になる。

【００３５】

また、認証用記録媒体作成装置は、鍵番号に対応する公開鍵が内部に記憶されており、ユーザのＩＤ、パスワードを鍵番号に対応する公開鍵で暗号化するので、認証用記録媒体作成装置を操作する媒体作成者は鍵番号に対応する公開鍵を知ることはできないため、認証用記録媒体内のデータを改ざんすることはできない。また、公開鍵暗号方式は共通鍵暗号方式と比較して管理すべき鍵の数が少ないので、鍵管理も容易である。

【図面の簡単な説明】

【００３６】

【図１】本発明に係る認証方法の処理を説明するフローチャートである。
【図２】本発明に係る認証方法の処理を説明するフローチャートである。
【図３】本発明に係るコンピュータ通信システムの一例を示す概念図である。
【図４】端末装置の構成を示すブロック図である。
【図５】サーバの構成を示すブロック図である。
【図６】本発明に係る認証用記録媒体作成装置の構成を示すブロック図である。
【図７】暗号パラメータの一例を示す説明図である。
【図８】従来の認証方法の処理を説明するフローチャートである。

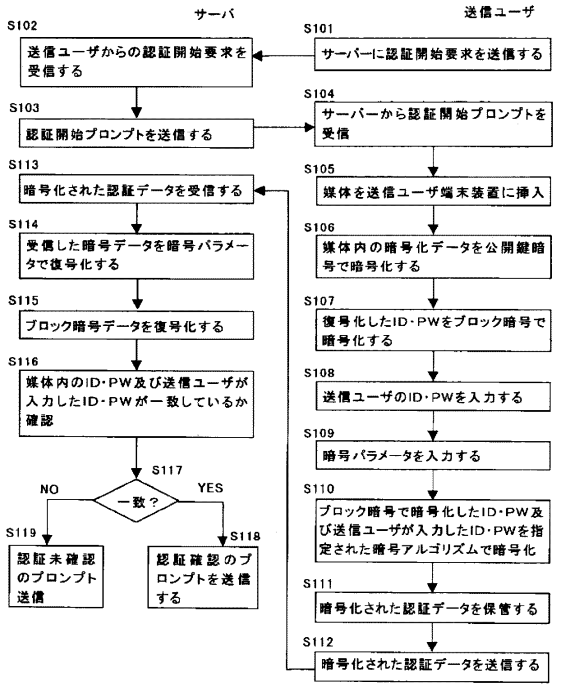
【符号の説明】

【００３７】

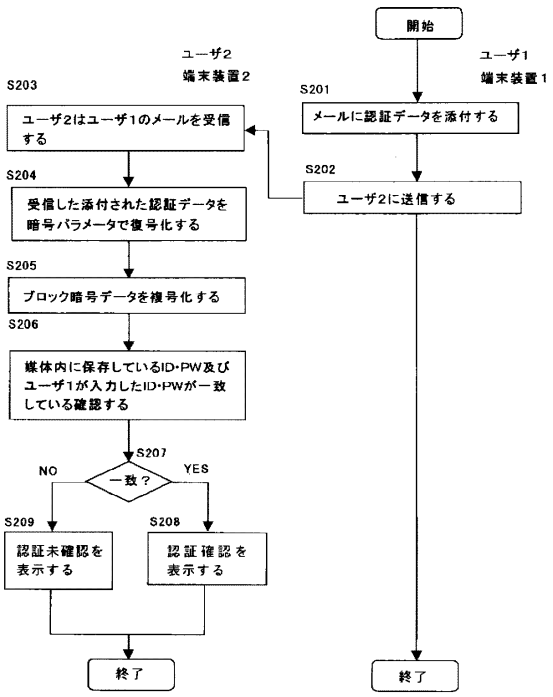
１　端末装置、２　認証装置（サーバ）、３　通信ネットワーク、
４　認証装置（サーバ）、５　端末装置、６　認証用記録媒体、７　端末装置、
８　認証データ作成部、９　認証部、１０　媒体入力部、１１　復号化処理部、

１２　暗号化処理部、１３　入力部、１４　鍵入力部、１５　暗号パラメータ処理部、
１６　認証データ保管部、１７　通信処理部、１８　鍵読取部、
１９　第一の復号化処理部、２０　第二の復号化処理部、２１　比較判定部、
２２　サーバ、２３　通信処理部、２４　認証データ保管部、２５　鍵読取部、
２６　第一の復号化処理部、２７　第二の復号化処理部、２８　比較判定部、
２９　認証用記録媒体作成装置、３０　認証用記録媒体、３１　入力部、
３２　暗号化処理部、３３　出力部、３４　格納部。

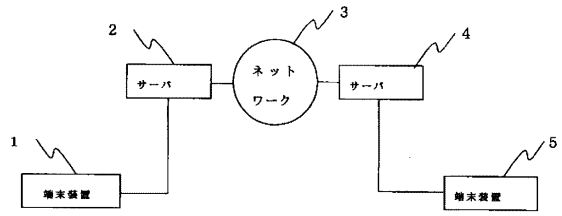
【図１】



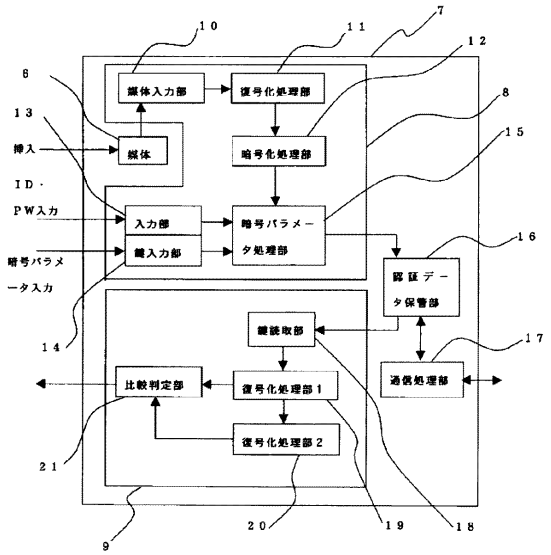
【図２】



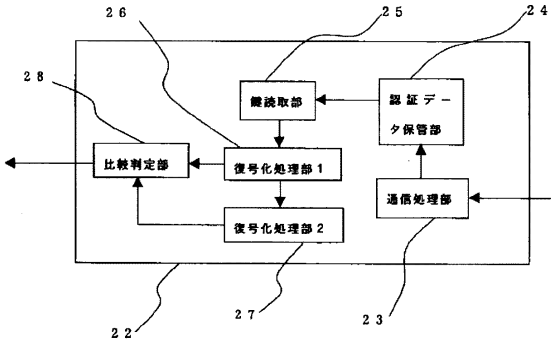
【図３】



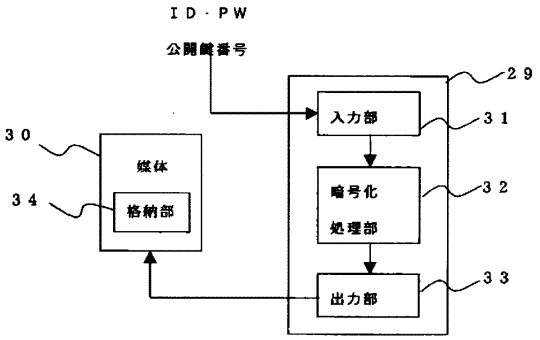
【図４】



【図５】



【図６】



【図７】

１　暗号パラメータのフォーマット

Ｋｅｙ．ｓ＝

「暗号アルゴリズム、変換表、暗号鍵」

２　使用可能な暗号アルゴリズム

１０：複合シフトレジスタ

１１：ＤＥＳ

１２：　・

１３：　・

１４：その他

３　入力例

・ブロック暗号：ＤＥＳ

・変換表　　：第３２表

・暗号鍵　　：０１２３４５６７８９ａｂｃｄｅｆ

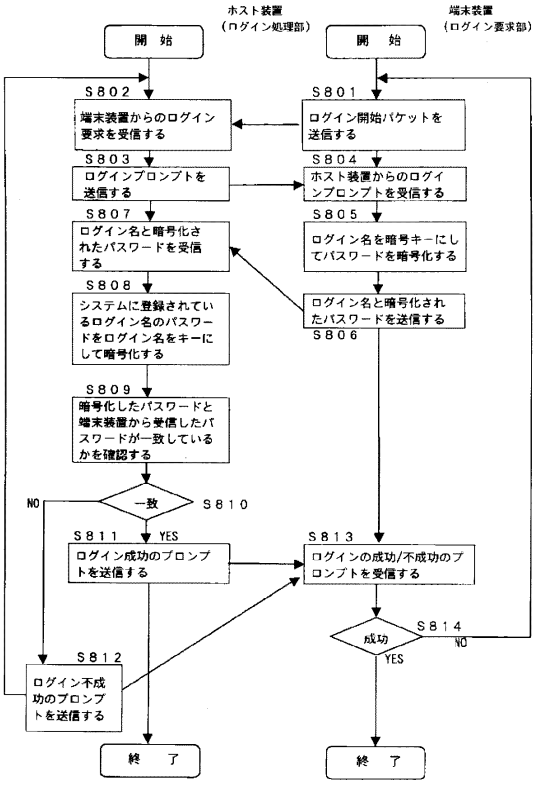
４　暗号パラメータの設定例

Ｋｅｙ．ｓ＝「１１３２０１２３４５６７８９ａｂｃｄｅｆ」

暗号パラメータ対応表

暗号 / 項目	アルゴリズム					
	１０	１１	１２	１３	・・	・・
変換表（６４表）	００～６３					
初期値（１６進法）	１６ａ１					

【図８】



フロントページの続き

(51)Int.Cl. FI
G06K 19/00 R
G09C 1/00 640E

審査官 速水 雄太

(56)参考文献 特開平1－267586（JP, A）
特開昭64－76270（JP, A）
特開平10－124642（JP, A）
特開平11－163853（JP, A）

(58)調査した分野(Int.Cl., DB名)
H04L 9／32
G06F 21／20
G06K 17／00
G06K 19／10
G09C 1／00