(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4436294号
(P4436294)
(45)発行日　平成22年3月24日(2010.3.24)　(24)登録日　平成22年1月8日(2010.1.8)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A
G06F 21/20 (2006.01)　G06F 15/00 330B

請求項の数 18　(全 25 頁)

(21)出願番号　特願2005-246506(P2005-246506)
(22)出願日　平成17年8月26日(2005.8.26)
(65)公開番号　特開2007-60568(P2007-60568A)
(43)公開日　平成19年3月8日(2007.3.8)
審査請求日　平成20年6月13日(2008.6.13)

早期審査対象出願

(73)特許権者　300023383
株式会社トリニティーセキュリティーシステムズ
東京都目黒区青葉台三丁目１７番１３号
(74)代理人　100104190
弁理士　酒井　昭徳
(72)発明者　清水　明宏
高知県高知市知寄町２丁目３番１６－１１０２号　アルファステイツ知寄町
(72)発明者　辻　貴介
高知県香美郡土佐山田町旭町１－１－１０　スバルＫ５０１

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】認証処理方法、認証処理プログラム、記録媒体および認証処理装置

(57)【特許請求の範囲】
【請求項１】
被認証装置を認証する認証装置における認証処理方法において、
前記被認証装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて生成された今回の認証処理に用いる今回認証情報を取得する取得工程と、
次回の認証処理に用いる次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記所定の値を前記次回認証情報を用いて隠蔽した第２の送信情報とを、前記被認証装置から受信する受信工程と、
前記受信工程によって受信された前記第１の送信情報と前記取得工程によって取得された前記今回認証情報とを用いて前記次回認証情報を算出し、当該次回認証情報と前記第２の送信情報とを用いて前記所定の値を算出する算出工程と、
前記算出工程によって算出された前記所定の値と、前記取得工程によって取得された前記今回認証情報とに基づいて、前記被認証装置を認証するか否かを判断する判断工程と、を含み、
前記取得工程は、初回の認証時には前記被認証装置から前記今回認証情報を取得し、２回目以降の認証時には前回の認証時における前記次回認証情報を前記今回認証情報とすることを特徴とする認証処理方法。
【請求項２】
前記取得工程は、

前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算をおこなって生成された今回認証情報を取得し、
前記判断工程は、
前記所定の値に対して、前記一方向変換関数による演算をおこなった値が前記今回認証情報と一致するか否かを判断することを特徴とする請求項１に記載の認証処理方法。
【請求項３】
前記取得工程は、
前記今回認証情報とともに、前記被認証装置に固有の認証鍵を取得し、
前記受信工程は、
第１の送信情報として、前記次回認証情報と前記今回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を受信し、第２の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値によって前記所定の値を隠蔽した値を受信し、
前記算出工程は、
前記第１の送信情報と前記今回認証情報とに対して前記マスク関数による演算をおこなって前記次回認証情報を算出し、前記認証鍵と前記次回認証情報と前記第２の送信情報とを用いて前記所定の値を算出することを特徴とする請求項１または２のいずれか一つに記載の認証処理方法。
【請求項４】
前記取得工程は、
前記今回認証情報とともに、前記被認証装置に固有の認証鍵を取得し、
前記受信工程は、
第１の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値を、前記今回認証情報を用いて隠蔽した値を受信し、第２の送信情報として、前記所定の値と前記次回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を受信し、
前記算出工程は、
前記認証鍵と前記第１の送信情報と前記今回認証情報とを用いて前記次回認証情報を算出することを特徴とする請求項１または２のいずれか一つに記載の認証処理方法。
【請求項５】
前記取得工程は、
前記今回認証情報とともに、前記次回認証情報を暗号鍵として前記所定の値を暗号化した暗号情報を取得し、
前記判断工程は、
前記次回認証情報を暗号鍵として前記暗号情報を復号した値が、前記算出手段によって算出された前記所定の値と等しいか否かに基づいて、前記被認証装置を認証するか否かを判断することを特徴とする請求項１～４のいずれか一つに記載の認証処理方法。
【請求項６】
前記取得工程は、
前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算を２回おこなって生成された今回認証情報を取得し、
前記判断工程は、
前記所定の値に対して、前記一方向変換関数による演算を２回おこなった値が前記今回認証情報と一致するか否かを判断することを特徴とする請求項５に記載の認証処理方法。
【請求項７】
認証装置に認証を要求する被認証装置における認証処理方法において、
前記被認証装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて今回の認証処理に用いる今回認証情報および次回の認証に用いる次回認証情報を生成する生成工程と、
前記次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記所定の

値を前記次回認証情報を用いて隠蔽した第２の送信情報とを算出する算出工程と、
前記算出工程によって算出された前記第１の送信情報と前記第２の送信情報とを、前記認証装置に送信する送信工程と、
を含むことを特徴とする認証処理方法。
【請求項８】
初回の認証に用いる初回認証情報を生成する初回認証情報生成工程と、
前記初回の認証に先立って、前記初回認証情報生成工程によって生成された前記初回認証情報を前記認証装置に送付する送付工程と、
をさらに含むことを特徴とする請求項７に記載の認証処理方法。
【請求項９】
前記生成工程は、
前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算をおこなうことによって前記今回認証情報を生成することを特徴とする請求項７または８に記載の認証処理方法。
【請求項１０】
前記生成工程は、
前記今回認証情報とともに、前記被認証装置に固有の認証鍵を生成し、
前記送付工程は、
前記今回認証情報とともに、前記認証鍵を前記認証装置に送付し、
前記算出工程は、
第１の送信情報として、前記次回認証情報と前記今回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出し、第２の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値によって前記所定の値を隠蔽した値を算出することを特徴とする請求項７～９のいずれか一つに記載の認証処理方法。
【請求項１１】
前記生成工程は、
前記今回認証情報とともに、前記被認証装置に固有の認証鍵を生成し、
前記送付工程は、
前記今回認証情報とともに、前記認証鍵を前記認証装置に送付し、
前記算出工程は、
第１の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値を、前記今回認証情報を用いて隠蔽した値を算出し、第２の送信情報として、前記所定の値と前記次回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出することを特徴とする請求項７～９のいずれか一つに記載の認証処理方法。
【請求項１２】
前記生成工程は、
前記今回認証情報とともに、前記次回認証情報を暗号鍵として前記所定の値を暗号化した暗号情報を生成し、
前記送付工程は、
前記今回認証情報とともに、前記暗号情報を前記認証装置に送付することを特徴とする請求項７～１１のいずれか一つに記載の認証処理方法。
【請求項１３】
前記生成工程は、
前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算を２回おこなって前記今回認証情報を生成することを特徴とする請求項１２に記載の認証処理方法。
【請求項１４】
請求項１～１３のいずれか一つに記載の認証処理方法をコンピュータに実行させること

を特徴とする認証処理プログラム。
【請求項１５】
請求項１４に記載の認証処理プログラムを記録したコンピュータに読み取り可能な記録媒体。
【請求項１６】
被認証装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて生成された今回の認証処理に用いる今回認証情報を取得する取得手段と、
次回の認証処理に用いる次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記次回認証情報を用いて前記所定の値を隠蔽した第２の送信情報とを、前記被認証装置から受信する受信手段と、
前記受信手段によって受信された前記第１の送信情報と前記取得手段によって取得された前記今回認証情報とを用いて前記次回認証情報を算出し、当該次回認証情報と前記第２の送信情報とを用いて前記所定の値を算出する算出手段と、
前記算出手段によって算出された前記所定の値と、前記取得手段によって取得された前記今回認証情報とに基づいて、前記被認証装置を認証するか否かを判断する判断手段と、
を備え、
前記取得手段は、初回の認証時には前記被認証装置から前記今回認証情報を取得し、２回目以降の認証時には前回の認証時における前記次回認証情報を前記今回認証情報とすることを特徴とする認証処理装置。
【請求項１７】
自装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて今回の認証処理に用いる今回認証情報および次回の認証に用いる次回認証情報を生成する生成手段と、
前記次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記所定の値を前記次回認証情報を用いて隠蔽した第２の送信情報とを算出する算出手段と、
前記算出手段によって算出された前記第１の送信情報と前記第２の送信情報とを、前記他装置に送信する送信手段と、
を備えることを特徴とする認証処理装置。
【請求項１８】
前記生成手段は、初回の認証に用いる初回認証情報を生成し、
前記初回の認証に先立って、前記生成手段によって生成された前記初回認証情報を前記認証装置に送付する送付手段と、
をさらに備えることを特徴とする請求項１７に記載の認証処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報通信システムなどにおいて、通信相手やユーザの利用資格を認証する認証処理方法、認証処理プログラム、記録媒体および認証処理装置に関する。
【背景技術】
【０００２】
従来、認証者（サーバ）が被認証者（ユーザ）を認証する際に、ユーザにパスワードの入力を要求し、入力されたパスワードの正当性をもってユーザを認証するパスワード認証方式が広く用いられている。また、パスワード認証方式においてパスワードによる認証の安全性を担保するため、認証ごとに使い捨てのパスワードを用いるワンタイムパスワード方式や、パスワードそのものではなくパスワードから生成した認証情報を用いて認証をおこなう方式が知られている。
【０００３】
例えば、ＳＡＳ－２（Ｓｉｍｐｌｅ　Ａｎｄ　Ｓｅｃｕｒｅ　ｐａｓｓｗｏｒｄ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｐｒｏｔｏｃｏｌ　Ｖｅｒ．２）認証方式は、パスワード認

証方式の一例であり、サーバは以下のような手順によってユーザを認証する（例えば、下記非特許文献１参照。）。図１０および図１１は、ＳＡＳ－２認証方式におけるユーザ認証の処理工程を示すフローチャートである。

【０００４】

なお、以下の説明において用いる記号および演算は、「←」は右辺の左辺への代入、「Ｓ」はユーザが秘密に保持しているパスワード、「ＩＤ」はユーザ識別子、「ＸＯＲ」は排他的論理和演算、「ｎ」は認証回数、「N_n」は乱数（ｎは１以上の整数で、乱数を識別するために用いる）、をそれぞれ示している。また、「Ｆ」「Ｈ」はパスワードＳを用いない一方向変換関数、「Ｘ」はパスワードＳと乱数N_nを用いる一方向変換関数で、X_n＝Ｘ（ＩＤ，Ｓ　ＸＯＲ　N_n）、をそれぞれ示している。

【０００５】

まず、ユーザは、認証を受けたいサーバにあらかじめ登録をおこなっておく（以下、この登録作業を「初期登録」という）。ユーザの初期登録処理の手順を図１０を参照して説明する。図１０は、従来技術によるユーザの初期登録処理の手順を示すフローチャートである。ユーザは、あらかじめユーザ識別子ＩＤおよびパスワードＳを保持している。

【０００６】

はじめに、ユーザは、乱数N_1を生成し、保存する（ステップＳ１００１）。そして、乱数N_1、秘密に保持しているパスワードＳ、ユーザ識別子ＩＤを用いて、下記式（１）に示す初回認証情報A_1を算出し（ステップＳ１００２）、ユーザ識別子ＩＤとともに安全な手段でサーバに送付する（ステップＳ１００３）。安全な手段とは、当該情報の専用線による送信や、当該情報を記憶した記憶媒体の郵送による送付などである。初回認証情報A_1は、初回（ｎ＝１）の認証に用いる認証情報である。

A_1　←　X_1（ＩＤ，Ｓ　ＸＯＲ　N_1）・・・（１）

【０００７】

サーバは、ステップＳ１００３でユーザから送付されたユーザ識別子ＩＤと、初回認証情報A_1とを対応づけて保存しておく（ステップＳ１００４）。以上がユーザの初期登録作業の手順である。

【０００８】

つぎに、初回（ｎ＝１）以降、ｎ回目の認証時の認証処理について、図１１を参照して説明する。図１１は、初回（ｎ＝１）以降、ｎ回目の認証時の認証処理の手順を示すフローチャートである。このとき、ユーザは、ＩＤ，Ｓ，N_nを保存している。また、サーバはＩＤ，A_n（初回認証時はｎ＝１）を保存している。まず、ユーザは保存している乱数N_nから、下記式（２）に示すA_nを算出する（ステップＳ１１０１）。

A_n　←　X_n（ＩＤ，Ｓ　ＸＯＲ　N_n）・・・（２）

【０００９】

つぎに、さらに新しい乱数N_{n+1}を生成、保存するか、あるいはA_nをN_{n+1}として、N_{n+1}を保存する（ステップＳ１１０２）。そして、N_{n+1}を用いて、下記式（３），（４）に示すＣ，Ｄを算出し、算出したＣ，Ｄ、およびA_nを用いて、下記式（５），（６）に示すαおよびβを算出する（ステップＳ１１０３）。

Ｃ　←　X_n（ＩＤ，Ｓ　ＸＯＲ　N_{n+1}）・・・（３）

Ｄ　←　Ｆ（ＩＤ，Ｃ），・・・（４）

α　←　Ｃ　ＸＯＲ（Ｄ＋A_n）・・・（５）

β　←　Ｄ　ＸＯＲ　A_n・・・（６）

【００１０】

そして、算出したα，βをＩＤとともにサーバに送付する（ステップＳ１１０４）。このとき、A_nは今回の認証処理に用いる今回認証情報、Ｃは次回の認証処理に用いる次回認証情報、Ｄは次回認証情報Ｃを一方向性変換したもうひとつの次回認証情報である。

【００１１】

サーバは、ユーザからαおよびβの送付を受けると、送付されたαとβに対して、ＩＤに対応して登録されている今回認証情報A_nを用いて、下記式（７）に示すＤを算出する

。さらに、算出したＤと今回認証情報A_nの和を用いて下記式（８）に示すＣを算出する（ステップＳ１１０５）。

Ｄ ← β ＸＯＲ A_n・・・（７）

Ｃ ← α ＸＯＲ（Ｄ＋A_n）・・・（８）

【００１２】

つぎに、サーバは上記式（８）によって算出したＣを、ＩＤとともに一方向性変換した結果と、Ｄとが一致するかどうか（Ｆ（ＩＤ，Ｃ）＝Ｄ？）を検証する（ステップＳ１１０６）。両者が一致する場合（ステップＳ１１０６：Ｙｅｓ）、ユーザに被認証者としての資格を認証し（認証成立）、次回（ｎ＋１回目）の認証に用いる認証情報（A_{n+1}）として、次回認証情報Ｃを保存する（ステップＳ１１０７）。

【００１３】

一方、両者が一致しない場合（ステップＳ１１０６：Ｎｏ）、認証不成立として（ステップＳ１１０８）、本フローチャートによる処理を終了する。以上のような処理によって、サーバは、認証を求めてきたユーザに対して認証をおこなうか否かを判断する。

【００１４】

【非特許文献１】辻貴介（Ｔａｋａｓｕｋｅ ＴＳＵＪＩ）、他２名、「シンプル アンド セキュア パスワード オーセンティケイション プロトコル バージョン２（Ｓｉｍｐｌｅ Ａｎｄ Ｓｅｃｕｒｅ ｐａｓｓｗｏｒｄ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｐｒｏｔｏｃｏｌ，Ｖｅｒ．２（ＳＡＳ－２））」、電子情報通信学会技術研究報告書、２００２年、ＯＩＳ２００２－３０、Ｖｏｌ．１０２、Ｎｏ．３１４、ｐ．７－１１

【発明の開示】

【発明が解決しようとする課題】

【００１５】

しかしながら、上述した従来技術によれば、サーバ側に記録されている今回認証情報Ａを用いてマスク処理された送付情報を用いて認証処理をおこなう。このため、サーバ側に保存されている今回認証情報を盗むことによって、容易に送付情報を生成することが可能であり、悪意を持った第三者によって不正認証がおこなわれる可能性があるという問題点がある。

【００１６】

特に、公共の場に設置されるサーバや、十分なセキュリティ知識を有していない者が設置したサーバなどは、悪意を有する者の標的にされやすく、今回認証情報が窃取されてしまう可能性が高い。また、サーバ側に悪意を有する者がいる場合、サーバに登録・保存されている今回認証情報を用いることによって、正当な被認証者に容易になりすますことができるという問題点がある。

【００１７】

さらに、このように、なりすましなどによって不正な認証が成功すると、機密情報が漏洩したり、正当な被認証者情報が書き換えられてしまうおそれがある。一度公になってしまった情報を機密の状態に戻すことはできず、被認証者および認証者の双方に重大な損失が生じることとなるという問題点がある。

【００１８】

本発明は、上述した従来技術による問題点を解消するため、認証処理の安全性をより向上させることができる認証処理方法、認証処理プログラム、記録媒体および認証処理装置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】

【００１９】

上述した課題を解決し、目的を達成するため、この発明にかかる認証処理方法は、被認証装置を認証する認証装置における認証処理方法において、前記被認証装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて生成された今回の認証処理に用いる今回認証情報を取得する取得工程と、次回の認証処理に用いる次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前

記所定の値を前記次回認証情報を用いて隠蔽した第２の送信情報とを、前記被認証装置から受信する受信工程と、前記受信工程によって受信された前記第１の送信情報と前記取得工程によって取得された前記今回認証情報とを用いて前記次回認証情報を算出し、当該次回認証情報と前記第２の送信情報とを用いて前記所定の値を算出する算出工程と、前記算出工程によって算出された前記所定の値と、前記取得工程によって取得された前記今回認証情報とに基づいて、前記被認証装置を認証するか否かを判断する判断工程と、を含み、前記取得工程は、初回の認証時には前記被認証装置から前記今回認証情報を取得し、２回目以降の認証時には前回の認証時における前記次回認証情報を前記今回認証情報とすることを特徴とする。

【００２０】

この発明によれば、悪意を有する第三者が、認証装置による認証を不正に得ようとしても、今回認証情報の元となる所定の値を知ることができず、第２の送信情報を生成することができない。このため、認証装置が被認証装置から取得した今回認証情報が第三者によって窃取されたとしても、不正な認証がおこなわれることがない。

【００２１】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記取得工程は、前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算をおこなって生成された今回認証情報を取得し、前記判断工程は、

前記所定の値に対して、前記一方向変換関数による演算をおこなった値が前記今回認証情報と一致するか否かを判断することを特徴とする。

【００２２】

この発明によれば、演算前の値を算出することが困難な一方向変換関数による演算を、所定の値に対しておこなうことによって今回認証情報を生成する。このため、被認証装置からの取得過程や取得後の保存過程で、第三者によって今回認証情報が窃取されたとしても、今回認証情報を元にして所定の値を算出することはできず、第２の認証情報を生成することができない。

【００２３】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記取得工程は、前記今回認証情報とともに、前記被認証装置に固有の認証鍵を取得し、前記受信工程は、第１の送信情報として、前記次回認証情報と前記今回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を受信し、第２の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値によって前記所定の値を隠蔽した値を受信し、前記算出工程は、前記第１の送信情報と前記今回認証情報とに対して前記マスク関数による演算をおこなって前記次回認証情報を算出し、前記認証鍵と前記次回認証情報と前記第２の送信情報とを用いて前記所定の値を算出することを特徴とする。

【００２４】

この発明によれば、演算前の値を算出することが容易なマスク関数による演算をおこなった値を受信する。このため、認証処理に用いられる今回認証情報や次回認証情報を、マスクした状態でやりとりすることができ、悪意を有する第三者によって送信情報を窃取されたとしても、不正な認証を防ぐことができる。また、この発明によれば、被認証装置に固有の認証鍵を用いて算出した値を第２の送信情報として受信する。このため、万一固有の認証鍵を持たない第三者によって送信情報が取得されてしまったとしても、不正な認証を防止することができる。

【００２５】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記取得工程は、前記今回認証情報とともに、前記被認証装置に固有の認証鍵を取得し、前記受信工程は、第１の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値を、前記今回認証情報を用いて隠蔽した値を受信し、第２の送信情報として、前記所定の値と前記次回認証情報とに対して、演算前の値を算出することが容易なマ

スク関数による演算をおこなった値を受信し、前記算出工程は、前記認証鍵と前記第１の送信情報と前記今回認証情報とを用いて前記次回認証情報を算出することを特徴とする。

【００２６】

この発明によれば、演算前の値を算出することが容易なマスク関数による演算をおこなった値を受信する。このため、認証処理に用いられる今回認証情報や次回認証情報を、マスクした状態でやりとりすることができ、悪意を有する第三者によって送信情報を窃取されたとしても、不正な認証を防ぐことができる。また、この発明によれば、被認証装置に固有の認証鍵を用いて算出した値を第１の送信情報として受信する。このため、万一固有の認証鍵を持たない第三者によって送信情報が取得されてしまったとしても、不正な認証を防止することができる。

【００２７】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記取得工程は、前記今回認証情報とともに、前記次回認証情報を暗号鍵として前記所定の値を暗号化した暗号情報を取得し、前記判断工程は、前記次回認証情報を暗号鍵として前記暗号情報を復号した値が、前記算出手段によって算出された前記所定の値と等しいか否かに基づいて、前記被認証装置を認証するか否かを判断することを特徴とする。

【００２８】

この発明によれば、次回認証情報を暗号鍵として暗号化した暗号情報を取得する。これにより、取得工程によって取得した情報と受信工程によって取得した情報の出所が同一かを判断することができ、第三者による情報の偽造の有無を検出することができる。

【００２９】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記取得工程は、前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算を２回おこなって生成された今回認証情報を取得し、前記判断工程は、前記所定の値に対して、前記一方向変換関数による演算を２回おこなった値が前記今回認証情報と一致するか否かを判断することを特徴とする。

【００３０】

この発明によれば、所定の値に対して一方向変換関数による演算を２回おこなった値によって正当な認証権限の有無を、同演算を１回おこなった値によって第三者による情報の偽造の有無を検出する。このように、それぞれの処理に用いる情報を異ならせることによって、不正な認証がおこなわれる可能性をより低くすることができる。

【００３１】

また、この発明にかかる認証処理方法は、認証装置に認証を要求する被認証装置における認証処理方法において、前記被認証装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて今回の認証処理に用いる今回認証情報および次回の認証に用いる次回認証情報を生成する生成工程と、前記次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記所定の値を前記次回認証情報を用いて隠蔽した第２の送信情報とを算出する算出工程と、前記算出工程によって算出された前記第１の送信情報と前記第２の送信情報とを、前記認証装置に送信する送信工程と、を含むことを特徴とする。

【００３２】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、初回の認証に用いる初回認証情報を生成する初回認証情報生成工程と、前記初回の認証に先立って、前記初回認証情報生成工程によって生成された前記初回認証情報を前記認証装置に送付する送付工程と、をさらに含むことを特徴とする。

【００３３】

この発明によれば、悪意を有する第三者が、認証装置による認証を不正に得ようとしても、今回認証情報の元となる所定の値を知ることができず、第２の送信情報を生成することができない。このため、被認証装置から認証装置に送付した今回認証情報が第三者によって窃取されたとしても、不正な認証がおこなわれることがない。

【００３４】
また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記生成工程は、前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算をおこなうことによって前記今回認証情報を生成することを特徴とする。
【００３５】
この発明によれば、演算前の値を算出することが困難な一方向変換関数による演算を、所定の値に対しておこなうことによって今回認証情報を生成する。このため、被認証装置からの送付過程や認証装置での保存過程で、第三者によって今回認証情報が窃取されたとしても、今回認証情報を元にして所定の値を算出することはできず、第２の認証情報を生成することができない。
【００３６】
また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記生成工程は、前記今回認証情報とともに、前記被認証装置に固有の認証鍵を生成し、前記送付工程は、前記今回認証情報とともに、前記認証鍵を前記認証装置に送付し、前記算出工程は、第１の送信情報として、前記次回認証情報と前記今回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出し、第２の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値によって前記所定の値を隠蔽した値を算出することを特徴とする。
【００３７】
この発明によれば、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出する。このため、認証処理に用いられる今回認証情報や次回認証情報を、マスクした状態でやりとりすることができ、悪意を有する第三者によって送信情報を窃取されたとしても、不正な認証を防ぐことができる。また、この発明によれば、被認証装置に固有の認証鍵を用いて算出した値を第２の送信情報として算出する。このため、万一固有の認証鍵を持たない第三者によって送信情報が取得されてしまったとしても、不正な認証を防止することができる。
【００３８】
また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記生成工程は、前記今回認証情報とともに、前記被認証装置に固有の認証鍵を生成し、前記送付工程は、前記今回認証情報とともに、前記認証鍵を前記認証装置に送付し、前記算出工程は、第１の送信情報として、前記次回認証情報に前記認証鍵を用いた所定の演算をおこなって得られた値を、前記今回認証情報を用いて隠蔽した値を算出し、第２の送信情報として、前記所定の値と前記次回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出することを特徴とする。
【００３９】
この発明によれば、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出する。このため、認証処理に用いられる今回認証情報や次回認証情報を、マスクした状態でやりとりすることができ、悪意を有する第三者によって送信情報を窃取されたとしても、不正な認証を防ぐことができる。また、この発明によれば、被認証装置に固有の認証鍵を用いて算出した値を第１の送信情報として算出する。このため、万一固有の認証鍵を持たない第三者によって送信情報が取得されてしまったとしても、不正な認証を防止することができる。
【００４０】
また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記生成工程は、前記今回認証情報とともに、前記次回認証情報を暗号鍵として前記所定の値を暗号化した暗号情報を生成し、前記送付工程は、前記今回認証情報とともに、前記暗号情報を前記認証装置に送付することを特徴とする。
【００４１】
この発明によれば、次回認証情報を暗号鍵として暗号化した暗号情報を今回認証情報とともに送付する。これにより、送付工程によって送付した情報と送信工程によって送信し

た情報の出所が同一であることを示すことができ、第三者による情報の偽造を防止することができる。

【００４２】

また、この発明にかかる認証処理方法は、上記の認証処理方法において、前記生成工程は、前記所定の値に対して、演算前の値を算出することが困難な一方向変換関数による演算を２回おこなって前記今回認証情報を生成することを特徴とする。

【００４３】

この発明によれば、所定の値に対して一方向変換関数による演算を２回おこなった値によって正当な認証権限を、同演算を１回おこなった値によって第三者による情報の偽造の有無を示すことができる。このように、それぞれの処理に用いる情報を異ならせることによって、不正な認証がおこなわれる可能性をより低くすることができる。

【００４４】

また、この発明にかかる認証処理プログラムは、上記の認証処理方法のいずれかをコンピュータに実行させることを特徴とする。

【００４５】

この発明によれば、上記の認証処理方法のいずれかをコンピュータに実行させることができる。

【００４６】

また、この発明にかかる記録媒体は、上記の認証処理プログラムをコンピュータに読み取り可能な状態で記録したことを特徴とする。

【００４７】

この発明によれば、上記の認証処理プログラムをコンピュータに読み取らせることができる。

【００４８】

また、この発明にかかる認証処理装置は、被認証装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて生成された今回の認証処理に用いる今回認証情報を取得する取得手段と、次回の認証処理に用いる次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記次回認証情報を用いて前記所定の値を隠蔽した第２の送信情報とを、前記被認証装置から受信する受信手段と、前記受信手段によって受信された前記第１の送信情報と前記取得手段によって取得された前記今回認証情報とを用いて前記次回認証情報を算出し、当該次回認証情報と前記第２の送信情報とを用いて前記所定の値を算出する算出手段と、前記算出手段によって算出された前記所定の値と、前記取得手段によって取得された前記今回認証情報とに基づいて、前記被認証装置を認証するか否かを判断する判断手段と、を備え、前記取得手段は、初回の認証時には前記被認証装置から前記今回認証情報を取得し、２回目以降の認証時には前回の認証時における前記次回認証情報を前記今回認証情報とすることを特徴とする。

【００４９】

この発明によれば、悪意を有する第三者が、認証装置による認証を不正に得ようとしても、今回認証情報の元となる所定の値を知ることができず、第２の送信情報を生成することができない。このため、認証装置が被認証装置から取得した今回認証情報が第三者によって窃取されたとしても、不正な認証がおこなわれることがない。

【００５０】

また、この発明にかかる認証処理装置は、自装置のみが保存する任意の固定値および認証処理ごとに異なる任意の変動値を用いて生成された所定の値を用いて今回の認証処理に用いる今回認証情報および次回の認証に用いる次回認証情報を生成する生成手段と、前記次回認証情報を前記今回認証情報を用いて隠蔽した第１の送信情報と、前記所定の値を前記次回認証情報を用いて隠蔽した第２の送信情報とを算出する算出手段と、前記算出手段によって算出された前記第１の送信情報と前記第２の送信情報とを、前記他装置に送信する送信手段と、を備えることを特徴とする。

【００５１】

また、この発明にかかる認証処理装置は、上記の認証処理装置において、前記生成手段は、初回の認証に用いる初回認証情報を生成し、前記初回の認証に先立って、前記生成手段によって生成された前記初回認証情報を前記認証装置に送付する送付手段と、をさらに備えることを特徴とする。

【００５２】

この発明によれば、悪意を有する第三者が、認証装置による認証を不正に得ようとしても、今回認証情報の元となる所定の値を知ることができず、第２の送信情報を生成することができない。このため、認証装置が被認証装置から取得した今回認証情報が第三者によって窃取されたとしても、不正な認証がおこなわれることがない。

【発明の効果】

【００５５】

本発明にかかる認証処理方法、認証処理プログラム、記録媒体および認証処理装置によれば、認証処理の安全性をより向上させることができるという効果を奏する。

【発明を実施するための最良の形態】

【００５６】

以下に添付図面を参照して、本発明にかかる認証処理方法、認証処理プログラム、記録媒体および認証処理装置の好適な実施の形態を詳細に説明する。

【００５７】

（実施の形態１）

まず、実施の形態にかかる認証処理システムのシステム構成について、図１を参照して説明する。なお、以下に説明する実施の形態１～３において、認証処理システムのシステム構成、ハードウェア構成、機能的構成（図１～３に相当）は共通である。

【００５８】

図１は、実施の形態にかかる認証処理システムのシステム構成を示す説明図である。認証処理システム１は、ユーザ２（２ａ～２ｆ）、サーバ３によって構成される。認証処理システム１において、ユーザ２は認証者に認証を要求する被認証者、サーバ３は被認証者を認証する認証者である。また、ユーザ２ａ～２ｆおよびサーバ３は、ネットワーク４によって接続されている。

【００５９】

ユーザ２は、サーバ３に認証を要求し、サーバ３が提供する所定のサービス（たとえばデータ通信接続サービス、ゲート通過許可、コンテンツ提供など）を受ける。サーバ３は、ユーザ２との間で認証処理をおこない、認証が成立した場合は、所定のサービスをおこなう。以下、サーバ３がユーザ２を認証した場合（認証が成立した場合）は、ユーザ２との間で相互接続を開始するものとする。なお、詳細な処理の説明は省略するが、更なる安全性の向上のため、ユーザ２においても、認証要求先のサーバ３が正当な者であるかを認証する相互認証をおこなってもよい。

【００６０】

つぎに、認証処理システム１を構成するユーザ２、サーバ３のハードウェア構成について図２を参照して説明する。図２は、認証処理システムを構成するユーザ、サーバのハードウェア構成の一例を示すブロック図である。なお、以下では説明の便宜上、ユーザ２およびサーバ３は同一のハードウェア構成を有するものとする。また、ユーザ２、サーバ３の機能を実現するものを以下「装置」と呼ぶ。

【００６１】

図２において、１１は装置全体を制御するＣＰＵを、１２は基本入出力プログラムを記憶したＲＯＭを、１３はＣＰＵ１１のワークエリアとして使用されるＲＡＭを、それぞれ示している。

【００６２】

また、１４はＣＰＵ１１の制御にしたがってＨＤ（ハードディスク）１５に対するデータのリード／ライトを制御するＨＤＤ（ハードディスクドライブ）を、１５はＨＤＤ１４の制御にしたがって書き込まれたデータを記憶するＨＤを、それぞれ示している。また、

１６はＣＰＵ１１の制御にしたがってＦＤ（フレキシブルディスク）１７に対するデータのリード／ライトを制御するＦＤＤ（フレキシブルディスクドライブ）を、１７はＦＤＤ１６の制御にしたがって書き込まれたデータを記憶する着脱自在のＦＤを、それぞれ示している。

【００６３】

また、１８はカーソル、メニュー、ウィンドウ、あるいは文字や画像などの各種データを表示するディスプレイを、１９はネットワーク４への／からのデータの送受信をおこなうネットワークＩ／Ｆ（インターフェース）を、それぞれ示している。また、２０は文字、数値、各種指示などの入力のための複数のキーを備えたキーボードを、２１は各種指示の選択や実行、処理対象の選択、カーソルの移動などをおこなうマウスを、それぞれ示している。

【００６４】

また、２２は文字や画像を光学的に読み取るスキャナを、２３は文字や画像を用紙上に印刷するプリンタを、２４は着脱可能な記録媒体であるＣＤ－ＲＯＭを、２５はＣＤ－ＲＯＭ２４に対するデータのリードを制御するＣＤ－ＲＯＭドライブを、２６は上記各部を接続するためのバスまたはケーブルを、それぞれ示している。

【００６５】

つぎに、実施の形態にかかる認証処理システム１の機能的構成について、図３を参照して説明する。図３は、認証処理システムを構成するユーザ、サーバの機能的構成を示すブロック図である。

【００６６】

ユーザ２は、生成部３１、送付部３２、算出部３３、送信部３４によって構成される。生成部３１は、任意の値（後述するａ）を用いて今回の認証処理に用いる今回認証情報（後述するＡ）を生成する。生成部３１は、具体的には、任意の値に対して、演算前の値を算出することが困難な一方向変換関数による演算をおこなうことによって今回認証情報を生成する。また、生成部３１は、今回認証情報とともに、ユーザ２に固有の認証鍵（後述するＫ）を生成する。

【００６７】

ここで、一方向変換関数とは、ある２つの値（ｘ，ｙとする）をその関数によって演算した場合、その演算結果の値（ｚとする）と、ある２つの値のうち１つ（例えば、ｘ）がわかっていても、それらからもう１つの値（ｙ）を算出することが困難な関数である。すなわち、一方向変換関数をｈとしたとき、ｘ，ｙをｈによって演算した値をｚとすると、ｚは、ｚ＝ｈ（ｘ，ｙ）と表せる。このとき、ｘ，ｚからｙを算出することが困難な関数である。

【００６８】

送付部３２は、生成部３１によって算出された今回認証情報をサーバ３に送付する。また、送付部３２は、今回認証情報とともに、認証鍵をサーバ３に送付する。ここで、送付とは、当該情報の専用線による送信や、当該情報を記憶した記憶媒体の郵送による送付など、当該情報がサーバ３以外の者に知得されないような方法でサーバ３に送る、との意味である。

【００６９】

算出部３３は、次回の認証処理に用いる次回認証情報（後述するＢ）を算出し、今回認証情報を用いて次回認証情報を隠蔽した第１の送信情報と、次回認証情報を用いて任意の値を隠蔽した第２の送信情報とを算出する。算出部３３は、具体的には、たとえば、第１の送信情報として、次回認証情報と今回認証情報とに対して、演算前の値を算出することが容易なマスク関数による演算をおこなった値を算出し、第２の送信情報として、次回認証情報（または次回認証情報および認証鍵の和）と任意の値とに対して、マスク関数による演算をおこなった値を算出する。

【００７０】

ここで、マスク関数とは、２度同じ演算をすると、元の値が演算結果となる関数であり

、例えば、排他的論理和演算（ＸＯＲ）が該当する。以下、マスク関数は排他的論理和演算として説明する。

【００７１】

送信部３４は、算出部３３によって算出された第１の送信情報と第２の送信情報とを、サーバ３に送信する。送信部３４は、たとえば、ネットワーク４を介して上述した送信情報をサーバ３に送信する。以上がユーザ２の機能的構成である。

【００７２】

つづいて、サーバ３の機能的構成を説明する。サーバ３は、取得部４１、受信部４２、算出部４３、判断部４４によって構成される。取得部４１は、ユーザ２の送付部３２によって送付された今回認証情報およびユーザ２に固有の認証鍵を取得する。受信部４２は、ユーザ２の送信部３４によって送信された第１の送信情報と第２の送信情報とを受信する。

【００７３】

算出部４３は、受信部４２によって受信された第１の送信情報と、取得部４１によって取得された今回認証情報とを用いて次回認証情報を算出し、当該次回認証情報と第２の送信情報とを用いて任意の値を算出する。算出部４３は、具体的には、たとえば、第１の送信情報と今回認証情報とに対して排他的論理和演算をおこなって次回認証情報（または次回認証情報および認証鍵の和）を算出し、当該次回認証情報（または次回認証情報および認証鍵の和）と第２の送信情報とに対して排他的論理和演算をおこなって任意の値を算出する。

【００７４】

判断部４４は、算出部４３によって算出された任意の値と、取得部４１によって取得された今回認証情報とに基づいて、ユーザ２を認証するか否かを判断する。判断部４４は、具体的には、たとえば、任意の値に対して、一方向変換関数による演算をおこなった値が今回認証情報と一致するか否かを判断する。そして、一致する場合はユーザ２を認証し、一致しない場合はユーザ２の認証を拒否する。以上がサーバ３の機能的構成である。

【００７５】

なお、上記各部は各装置のＨＤ１５やＦＤ１７、あるいはＣＤ－ＲＯＭ２４などの各種記録媒体からＲＡＭ１３に読み出されたプログラムの命令にしたがって、ＣＰＵ１１などが命令処理を実行することにより、それぞれの機能を実現する。

【００７６】

（認証者－被認証者間の認証処理）

つぎに、サーバ３（認証者）が、ユーザ２（被認証者）を認証する際の処理について説明する。認証処理に先立って、サーバ３に対してユーザ２の初期登録処理がおこなわれる。そして、初期登録処理時にサーバ３に登録された情報を用いて、サーバ３がユーザ２を認証する認証処理がおこなわれる。

【００７７】

なお、以下の説明において用いる記号および演算は、「←」は右辺の左辺への代入、「Ｓ」はユーザ（被認証者）が秘密に保持しているパスワード、「ＩＤ」はユーザ（被認証者）識別子、「ＸＯＲ」は排他的論理和、「ｎ」は認証回数、「N_n」は乱数（ｎは１以上の整数で、乱数を識別するために用いる）、「Ｆ」はパスワードＳを用いない一方向変換関数であり、ｚ＝Ｆ（ｘ，ｙ）とするとき、ｚとｘからｙを算出することが計算量的に困難な関数である。また、「Ｘ」はパスワードＳと乱数N_nを用いる一方向変換関数で、X_n＝Ｘ（ＩＤ、Ｓ、N_n）とする。

【００７８】

まず、ユーザ２の初期登録処理について図４を参照して説明する。図４は、ユーザの初期登録処理の手順を示すフローチャートである。図４において、ユーザ２は、複数存在するユーザ２から自身を識別するためのユーザ識別子ＩＤを保持している。また、ユーザ２は、自身のみが知る秘密のパスワードＳを保持している。ユーザ識別子ＩＤおよびパスワードＳは、ユーザ２に記録されていてもよいし、処理の都度入力を要求することとしても

よい。

【００７９】

はじめに、ユーザ２は、秘密鍵Ｋおよび乱数N_1を生成し、保存する（ステップＳ１０１）。そして、ユーザ識別子ＩＤ、パスワードＳ、乱数N_1を用いて、下記式（９），（１０）の手順によってA_1を算出する（ステップＳ１０２）。ここで、式（１０）に示すA_1は、初回（ｎ＝１）の認証に用いる認証情報A_nである。以下、A_1を初回認証情報という。

$a \leftarrow X(ID, S, N_1)$・・・（９）

$A_1 \leftarrow F(ID, a)$・・・（１０）

【００８０】

つぎに、ユーザ２はサーバ３に対して、ユーザ識別子ＩＤ、秘密鍵Ｋ、初回認証情報A_1を、安全な手段によって送信する（ステップＳ１０３）。ここで、安全な手段とは、当該情報の専用線による送信や、当該情報を記憶した記憶媒体の郵送による送付などである。また、ユーザ２は、算出した初回認証情報A_1を保存し（ステップＳ１０４）、本フローチャートによる処理を終了する。

【００８１】

サーバ３は、ユーザ２から送信された秘密鍵Ｋ、初回認証情報A_1を、それぞれユーザ識別子ＩＤに関連づけて保存して（ステップＳ１０５）、本フローチャートによる処理を終了する。以上のような処理によって、ユーザ２がサーバ３に初期登録される。

【００８２】

つぎに、初回（ｎ＝１）以降、ｎ回目の認証時の認証処理について、図５を参照して説明する。図５は、初回（ｎ＝１）以降、ｎ回目の認証処理の手順を示すフローチャートである。このとき、ユーザ２が保存している保存情報は、秘密鍵Ｋ、乱数Ｎｎ（初回認証の場合はｎ＝１）、認証情報A_n（初回認証の場合はｎ＝１）である。また、サーバ３が保存している保存情報は、ユーザ２のＩＤ、図４の初期登録時にユーザ２から送信された秘密鍵Ｋおよび認証情報A_n（初回認証の場合はｎ＝１）である。

【００８３】

まず、ユーザ２は、保存しているＮｎから、下記式（１１）に示すａを算出する（ステップＳ１５１）。また、さらに新しい乱数N_{n+1}を生成、保存し（ステップＳ１５２）、下記式（１２），（１３）の手順によってＢを算出する（ステップＳ１５３）。

$a \leftarrow X(ID, S, N_n)$・・・（１１）

$b \leftarrow X(ID, S, N_{n+1})$・・・（１２）

$B \leftarrow F(ID, b)$・・・（１３）

【００８４】

つぎに、ユーザ２は、算出したａ、Ｂおよび保存しているＫ、A_nを用いて、下記式（１４），（１５）に示すα，βを算出し（ステップＳ１５４）、ＩＤ，α，βをサーバ３に送信する（ステップＳ１５５）。また、次回認証情報A_{n+1}として、ステップＳ１５３で算出したＢを保存して（ステップＳ１５６）、ユーザ２は本フローチャートによる処理を終了する。また、ａは認証情報A_nの元となるデータである。

$\alpha \leftarrow B \ XOR \ A_n$・・・（１４）

$\beta \leftarrow (B+K) \ XOR \ a$・・・（１５）

【００８５】

サーバ３は、ユーザ２から受信したαとβに対して、ユーザ２のＩＤに対応して登録されている認証情報A_nを用いて、下記式（１６）に示すＢ、およびＢとＫとの和を用いて下記式（１７）に示すａを算出する（ステップＳ１５７）。

$B \leftarrow \alpha \ XOR \ A_n$・・・（１６）

$a \leftarrow \beta \ XOR \ (B+K)$・・・（１７）

【００８６】

そして、算出したａと保存しているＩＤとを一方向性変換した結果Ｆ（ＩＤ，ａ）がA_nに等しいかどうかを判断し（ステップＳ１５８）、等しい場合は（ステップＳ１５８：

Ｙｅｓ）、ユーザ２に対して被認証者の資格を認証し、ユーザ２との接続を開始する（ステップＳ１５９）。また、次回の認証に用いる認証情報（A_{n+1}）としてＢを保存して（ステップＳ１６０）、サーバ３は本フローチャートによる処理を終了する。一方、Ｆ（ＩＤ，ａ）がA_nに等しくない場合は（ステップＳ１５８：Ｎｏ）、認証不成立として、ユーザ２にエラーメッセージを送信して（ステップＳ１６１）、サーバ３は本フローチャートによる処理を終了する。

【００８７】

なお、ステップＳ１５４におけるα，βの算出方法は、上記式（１４），（１５）に示した演算に限られるものではない。上記式（１４），（１５）に示した演算では、βを算出する際にＢにＫを加算しているが、この処理は、α，βがサーバ３への送信過程で第三者に取得されてしまった場合などに、取得された値を利用した攻撃を防ぐためのものである。すなわち、αの算出に用いるＢ、または、βの算出に用いるＢのいずれか一方に演算を施し、αとβのＢ部分（A_nあるいはａと排他的論理和演算する値）を一致させないようにして、α，βからＢが知られないようにしている。α，βの算出方法は、このような条件を満たすものであれば、上記式（１４），（１５）の演算には限られず、様々なバリエーションが存在する。

【００８８】

たとえば、ＩＤなどのユーザ２とサーバ３との間の共有情報、あるいはA_nなどの共有情報から生成した値をＫとして用いることが可能である。上述した例では、Ｋは図４のステップＳ１０１において秘密鍵として算出した値であるが、たとえば、ユーザ識別子ＩＤを用いて、下記式（１８），（１９）のように演算してもよい。

α ← Ｂ ＸＯＲ A_n・・・（１８）

β ← （Ｂ＋ＩＤ） ＸＯＲ ａ・・・（１９）

【００８９】

また、βの算出にあたって、Ｂに対してＫを加算するのではなく、下記式（２０），（２１）に示すようにＢからＫを減算することとしてもよい。この他、乗算や除算など、ＢとＫとの間でどのような演算をおこなってもよい。

α ← Ｂ ＸＯＲ A_n・・・（２０）

β ← （Ｂ－Ｋ） ＸＯＲ ａ・・・（２１）

【００９０】

また、αの算出においても、Ｋを用いた演算をおこなうこととしてもよい。たとえば、下記式（２２），（２３）に示すように、αの算出においてＢにＫを加算することとしてもよい。ただし、αの算出におけるＢへの演算は、Ｂ－Ｋのように、逆演算が可能なものでなくてはならない。

α ← （Ｂ＋Ｋ） ＸＯＲ A_n・・・（２２）

β ← Ｂ ＸＯＲ ａ・・・（２３）

【００９１】

以上のような算出方法のバリエーションに加え、下記式（２４），（２５）のように、これらのバリエーションを組み合わせた演算によって、α，βを算出することとしてもよい。

α ← （Ｂ－ＩＤ） ＸＯＲ A_n・・・（２４）

β ← Ｂ ＸＯＲ ａ・・・（２５）

【００９２】

このように、α，βの算出方法にはバリエーションがあるが、どのような演算によってα，βが算出されたかによって、ステップＳ１５７におけるａの算出方法が異なってくる。たとえば、上記式（１８），（１９）に示した演算によってα，βを算出した場合、下記式（２６），（２７）に示す演算によってａを算出することができる。

Ｂ ← α ＸＯＲ A_n・・・（２６）

ａ ← β ＸＯＲ （Ｂ＋ＩＤ）・・・（２７）

【００９３】

以上説明したように、実施の形態１にかかる認証処理システムによれば、認証処理に用いる認証情報は、被認証者（ユーザ２）のみが保存する認証情報の元となるデータ（パスワードＳ、乱数N_n）を用いなければ生成することができない。このため、認証者（サーバ３）に保存されている被認証者に関する情報（ＩＤ，Ｋ，A_n）を第三者が盗んだとしても、第三者は認証処理に用いる認証情報を生成することができず、認証者による認証を受けることができない。

【００９４】

（実施の形態２）

つづいて、実施の形態２にかかる認証処理システムについて説明する。実施の形態１にかかる認証処理システムでは、認証処理に用いる認証情報を、被認証者（ユーザ２）のみが保存するデータを元に生成することによって、認証者（サーバ３）からの被認証者情報の窃取に対応できるようにした。実施の形態２にかかる認証処理システムでは、さらに、次回（ｎ＋１回目）の認証に用いる次回認証情報（A_{n+1}：Ｂ）を用いて暗号化した情報から、今回（ｎ回目）の認証に用いる今回認証情報（A_n）の元となる情報が算出されるかを確認する。これにより、第三者による送付情報の偽造を検出することができる。

【００９５】

まず、ユーザ２の初期登録処理について図６を参照して説明する。図６は、ユーザの初期登録処理の手順を示すフローチャートである。図６において、ユーザ２は、複数存在するユーザ２から自身を識別するためのユーザ識別子ＩＤを保持している。また、ユーザ２は、自身のみが知る秘密のパスワードＳを保持している。

【００９６】

はじめに、ユーザ２は、秘密鍵Ｋを生成し、保存する（ステップＳ２０１）。また、乱数N_1，N_2を生成し、N_2を保存する（ステップＳ２０２）。そして、ユーザ識別子ＩＤ、パスワードＳ、乱数N_1，N_2を用いて、下記式（２８），（２９）の手順によってＡを、下記式（３０）～（３２）の手順によってγ_1を算出する（ステップＳ２０３）。ここで、A_1およびγ_1は、初回（ｎ＝１）の認証に用いる初回認証情報である。また、下記式（３２）に示すＥ＿{Ｂ}（ａ）は、Ｂを鍵としてａを暗号化した結果の値である。

ａ ← Ｘ（ＩＤ，Ｓ，N_1）・・・（２８）

A_1 ← Ｆ（ＩＤ，ａ）・・・（２９）

ｂ ← Ｘ（ＩＤ，Ｓ，N_2）・・・（３０）

Ｂ ← Ｆ（ＩＤ，ｂ）・・・（３１）

γ_1 ← Ｅ＿{Ｂ}（ａ）・・・（３２）

【００９７】

つぎに、ユーザ２はサーバ３に対して、ユーザ識別子ＩＤ、秘密鍵Ｋ、初回認証情報A_1、γ_1を、安全な手段によって送信する（ステップＳ２０４）。また、算出したａ，ｂ（以下、認証子ａ，ｂという）およびA_1，Ｂを保存して（ステップＳ２０５）、ユーザ２は本フローチャートによる処理を終了する。

【００９８】

サーバ３は、ユーザ２から送信された秘密鍵Ｋ、初回認証情報A_1，γ_1を、それぞれユーザ識別子ＩＤにそれぞれ関連づけて保存して（ステップＳ２０６）、本フローチャートによる処理を終了する。以上のような処理によって、ユーザ２がサーバ３に初期登録される。

【００９９】

つぎに、初回（ｎ＝１）以降、ｎ回目の認証時の認証処理について、図７を参照して説明する。図７は、初回（ｎ＝１）以降、ｎ回目の認証処理の手順を示すフローチャートである。このとき、ユーザ２が保存している情報は、秘密鍵Ｋ、乱数N_{n+1}（初回認証の場合はｎ＝１のためN_2）、認証情報A_n（初回認証の場合はｎ＝１）、Ｂ、認証子ａ、ｂである。サーバ３が保存している情報は、図６に示した初期登録時にユーザ２から送信された秘密鍵Ｋおよび認証情報A_n、γ_n（初回認証の場合はｎ＝１）である。

【０１００】

まず、ユーザ２は、保存しているN_{n+1}から、下記式（３３）に示すｂを算出し（ステップＳ２５１）、保存しているｂと等しいかを判断する（ステップＳ２５２）。このとき、ｂの算出に用いるＩＤ，Ｓは、認証処理の都度ユーザ２の利用者に入力を求めてもよいし、ユーザ２で保存しておいてもよい。保存しているｂと等しい場合は（ステップＳ２５２：Ｙｅｓ）、被認証者としての資格を認証し、ステップＳ２５３に移行する。一方、保存しているｂと等しくない場合は（ステップＳ２５２：Ｎｏ）、被認証者としての資格を認証せず、本フローチャートによる処理を終了する。

$$b \leftarrow X(ID, S, N_{n+1}) \cdots (33)$$

【０１０１】

また、ユーザ２は、新しい乱数N_{n+2}を生成、保存し（ステップＳ２５３）、下記式（３４），（３５）の手順によって認証子ｃおよび認証情報Ｃを算出する（ステップＳ２５４）。このとき、認証子ｃおよび認証情報Ｃは、次々回の認証に用いる次々回認証情報である。

$$c \leftarrow X(ID, S, N_{n+2}) \cdots (34)$$

$$C \leftarrow F(ID, c) \cdots (35)$$

【０１０２】

つぎに、ユーザ２は、算出したｂ，Ｃおよび保存しているＫ，A_n，Ｂを用いて、下記式（３６）～（３８）に示すα，β，γ_{n+1}を算出する（ステップＳ２５５）。そして、サーバ３にＩＤ，α，β，γ_{n+1}を送信する（ステップＳ２５６）。また、次回認証子ｂ、次回認証情報Ｂとして、算出した次々回認証子ｃ、次々回認証情報Ｃを保存して（ステップＳ２５７）、ユーザ２は本フローチャートによる処理を終了する。なお、α，βの算出方法は、実施の形態１で説明したように、さまざまなバリエーションが存在するが、以下では、その一例として下記式（３６），（３７）に示す演算をおこなうものとする。

$$\alpha \leftarrow B \ XOR \ A_n \cdots (36)$$

$$\beta \leftarrow (B+K) \ XOR \ a \cdots (37)$$

$$\gamma_{n+1} \leftarrow E\_\{C\}(b) \cdots (38)$$

【０１０３】

サーバ３は、ユーザ２から受信したα，βおよびＩＤに対応して保存されている認証情報A_n、秘密鍵Ｋを用いて、下記式（３９），（４０）の手順によってａを算出する（ステップＳ２５８）。

$$B \leftarrow \alpha \ XOR \ A_n \cdots (39)$$

$$a \leftarrow \beta \ XOR \ (B+K) \cdots (40)$$

【０１０４】

そして、サーバ３は、算出したａおよび保存しているＩＤを一方向性変換した結果Ｆ（ＩＤ，ａ）がA_nに等しいかどうかを判断し（ステップＳ２５９）、等しい場合は（ステップＳ２５９：Ｙｅｓ）、ユーザ２に対して被認証者の資格を認証する。つづいて、サーバ３は、受信したＢを用いて暗号化情報γ_nを復号し（D＿{B}（γ_n）と示す）、D＿{B}（γ_n）がａに等しいかを判断する（ステップＳ２６０）。

【０１０５】

D＿{B}（γ_n）がａに等しい場合は（ステップＳ２６０：Ｙｅｓ）、認証情報Ｂが改ざんされていないことが証明され、ユーザ２との接続を開始する（ステップＳ２６１）。また、次回（ｎ＋１回目）の認証処理時に用いる認証情報（A_{n+1}）としてＢを保存して（ステップＳ２６２）、本フローチャートによる処理を終了する。

【０１０６】

一方、ステップＳ２５９において、Ｆ（ＩＤ，ａ）がA_nに等しくない場合は（ステップＳ２５９：Ｎｏ）、認証不成立として、ユーザ２にエラーメッセージを送信して（ステップＳ２６３）、本フローチャートによる処理を終了する。また、ステップＳ２６０において、D＿{B}（γ_n）がａに等しくない場合は（ステップＳ２６０：Ｎｏ）、認証情報Ｂが改ざんされているとして、ユーザ２にエラーメッセージを送信して（ステップＳ２６３）、本フローチャートによる処理を終了する。

【０１０７】
以上説明したように、実施の形態２にかかる認証処理システムによれば、認証処理に用いる認証情報は、被認証者（ユーザ２）のみが保存する認証情報の元となるデータ（パスワードＳ、乱数N_{n+1}）を用いなければ生成することができない。このため、認証者（サーバ３）に保存されている被認証者に関する情報（ＩＤ，Ｋ，A_n，γ_n）を第三者が盗んだとしても、第三者は認証処理に用いる認証情報を生成することができず、認証者による認証を受けることができない。
【０１０８】
さらに、次回認証情報（Ｂ）を用いて暗号化した情報（γ_n：Ｅ｛Ｂ｝（ａ））から、今回の認証に用いる今回認証情報の元となるデータ（ａ：Ｄ｛Ｂ｝（γ_n））が算出されるかを確認することによって、第三者による送信情報の偽造を検出することができる。
【０１０９】
（実施の形態３）
つづいて、実施の形態３にかかる認証処理システムについて説明する。実施の形態３にかかる認証処理システムでは、送付情報の偽造検出に用いるデータと、認証処理に用いるデータを異なるデータとする。これにより、認証処理時の安全性を向上させることができる。
【０１１０】
まず、ユーザ２の初期登録処理について説明する。図８は、ユーザの初期登録の処理手順を示すフローチャートである。図８において、ユーザ２は、複数存在するユーザ２から自身を識別するためのユーザ識別子ＩＤを保持している。また、ユーザ２は、自身のみが知る秘密のパスワードＳを保持している。
【０１１１】
はじめに、ユーザ２は、秘密鍵Ｋを生成し、保存する（ステップＳ３０１）。また、乱数N_1、N_2を生成し、N_2を保存する（ステップＳ３０２）。そして、ユーザ識別子ＩＤ、パスワードＳ、乱数N_1を用いて、下記式（４１）～（４３）に示す手順によってA'_1を、下記式（４４）～（４７）の手順によってγ_1を算出する（ステップＳ３０３）。ここで、A'_1およびγ_1は、初回（ｎ＝１）の認証に用いる初回認証情報である。また、下記式（４７）に示すＥ＿｛Ｂ’｝（ａ）は、Ｂ’を鍵としてａを暗号化した結果の値である。

$$a \leftarrow X(ID, S, N_1) \cdots (41)$$
$$A \leftarrow F(ID, a) \cdots (42)$$
$$A'_1 \leftarrow F(ID, A) \cdots (43)$$
$$b \leftarrow X(ID, S, N_2) \cdots (44)$$
$$B \leftarrow F(ID, b) \cdots (45)$$
$$B' \leftarrow F(ID, B) \cdots (46)$$
$$\gamma_1 \leftarrow E\_\{B'\}(a) \cdots (47)$$

【０１１２】
つぎに、ユーザ２はサーバ３に、ユーザ識別子ＩＤ、秘密鍵Ｋ、初回認証情報A'_1，γ_1を安全な手段によって送信する（ステップＳ３０４）。また、ユーザ２は、算出したａ，ｂ（以下、認証子ａ，ｂという）およびＡ，A'_1，Ｂ，Ｂ’を保存して（ステップＳ３０５）、本フローチャートによる処理を終了する。
【０１１３】
サーバ３は、ユーザ２から送信された秘密鍵Ｋ、初回認証情報A'_1，γ_1を、それぞれユーザ識別子ＩＤに関連づけて保存して（ステップＳ３０６）、本フローチャートによる処理を終了する。以上のような処理によって、ユーザ２がサーバ３に初期登録される。
【０１１４】
つぎに、初回（ｎ＝１）以降、ｎ回目の認証時の認証処理について、図９を参照して説明する。図９は、初回（ｎ＝１）以降、ｎ回目の認証処理の手順を示すフローチャートである。このとき、ユーザ２が保存している情報は、秘密鍵Ｋ、乱数N_{n+1}（初回認証の場

合はｎ＝１のためN_2）、認証情報A'_n（初回認証の場合はｎ＝１），Ａ，Ｂ’，Ｂ、認証子ａ，ｂである。また、サーバ３が保存している情報は、図８に示した初期登録時にユーザ２から送信された秘密鍵Ｋおよび認証情報A'_n，γ_n（初回認証の場合はｎ＝１）である。

【０１１５】

まず、ユーザ２は、保存しているN_{n+1}から、下記式（４８）に示すｂを算出し（ステップＳ３５１）、保存しているｂと等しいかを判断する（ステップＳ３５２）。このとき、ｂの算出に用いるＩＤ，Ｓは、認証処理の都度ユーザ２の利用者に入力を求めてもよいし、ユーザ２で保存しておいてもよい。保存しているｂと等しい場合は（ステップＳ３５２：Ｙｅｓ）、被認証者としての資格を認証し、ステップＳ３５３に移行する。一方、保存しているｂと等しくない場合は（ステップＳ３５２：Ｎｏ）、被認証者としての資格を認証せず、本フローチャートによる処理を終了する。

ｂ ← Ｘ（ＩＤ，Ｓ，N_{n+1}）・・・（４８）

【０１１６】

また、ユーザ２は、さらに新しい乱数N_{n+2}を生成、保存し（ステップＳ３５３）、下記式（４９）～（５１）の手順によってＣ’を算出する（ステップＳ３５４）。

ｃ ← Ｘ（ＩＤ，Ｓ，N_{n+2}）・・・（４９）

Ｃ ← Ｆ（ＩＤ，ｃ）・・・（５０）

Ｃ’ ← Ｆ（ＩＤ，Ｃ）・・・（５１）

【０１１７】

つぎに、ユーザ２は、算出したｂ，Ｃ’および保存しているＫ，A_n，A'_n，Ｂ’を用いて、下記式（５２）～（５４）に示すα，β，γ_{n+1}を算出する（ステップＳ３５５）。そして、サーバ３にＩＤ，α，β，γ_{n+1}を送信する（ステップＳ３５６）。また、次回認証子ｂ、次回認証情報Ｂとして、算出した次々回認証子ｃ、次々回認証情報Ｃを保存して（ステップＳ３５７）、本フローチャートによる処理を終了する。なお、α，βの算出方法は、実施の形態１で説明したように、さまざまなバリエーションが存在するが、以下では、その一例として下記式（５２），（５３）に示す演算をおこなうものとする。

α ← Ｂ’ ＸＯＲ A'_n・・・（５２）

β ← （Ｂ’＋Ｋ） ＸＯＲ Ａ・・・（５３）

γ_{n+1} ← Ｅ＿{Ｃ’}（ｂ）・・・（５４）

【０１１８】

サーバ３は、ユーザ２から受信したα、βおよびＩＤに対応して保存されている認証情報A'_n、秘密鍵Ｋを用いて、下記式（５５），（５６）の手順によってA_nを算出する（ステップＳ３５８）。

Ｂ’ ← α ＸＯＲ A'_n・・・（５５）

Ａ ← β ＸＯＲ （Ｂ’＋Ｋ）・・・（５６）

【０１１９】

そして、サーバ３は、算出したＡおよび保存しているＩＤを一方向性変換した結果Ｆ（ＩＤ、Ａ）がA'_nに等しいかどうかを判断し（ステップＳ３５９）、等しい場合は（ステップＳ３５９：Ｙｅｓ）、ユーザ２に対して被認証者の資格を認証する。つづいて、受信したＢ’を用いて暗号化情報γ_nを復号し（この処理をＤ＿{Ｂ’}（γ_n）と示す）、下記式（５７）に示すａを算出する（ステップＳ３６０）。

ａ ← Ｄ＿{B'_n}（γ_n）・・・（５７）

【０１２０】

そして、算出したａをＩＤとともに一方向性変換したＦ（ＩＤ，ａ）がＡに等しいかを判断する（ステップＳ３６１）。Ｆ（ＩＤ，ａ）がＡに等しい場合は（ステップＳ３６１：Ｙｅｓ）、認証情報Ｂ’が改ざんされていないことが証明され、ユーザ２との接続を開始する（ステップＳ３６２）。

【０１２１】

また、次回（ｎ＋１回目）の認証処理時に用いる認証情報（A'_{n+1}）としてＢ’を保

存する（ステップＳ３６３）。また、次回（ｎ＋１回目）の認証に用いる認証情報として、ステップＳ３５６でユーザ２から送信されたγ_{n+1}をγ_nの代わりに保存して（ステップＳ３６４）、本フローチャートによる処理を終了する。

【０１２２】

一方、ステップＳ３５９において、Ｆ（ＩＤ，Ａ）がＡ’$_n$に等しくない場合は（ステップＳ３５９：Ｎｏ）、認証不成立として、ユーザ２にエラーメッセージを送信して（ステップＳ３６５）、本フローチャートによる処理を終了する。また、ステップＳ３６１において、Ｆ（ＩＤ，ａ）がＡに等しくない場合は（ステップＳ３６１：Ｎｏ）、認証情報Ｂ’が改ざんされているとして、ユーザ２にエラーメッセージを送信して（ステップＳ３６５）、本フローチャートによる処理を終了する。

【０１２３】

以上説明したように、実施の形態３にかかる認証処理システムによれば、認証処理に用いる認証情報は、被認証者（ユーザ２）のみが保存する認証情報の元となるデータ（パスワードＳ、乱数N_{n+1}）を用いなければ生成することができない。このため、認証者（サーバ３）に保存されている被認証者に関する情報（ＩＤ，Ｋ，Ａ’，γ_n）を第三者が盗んだとしても、第三者は認証処理に用いる認証情報を生成することができず、認証者による認証を受けることができない。

【０１２４】

また、次回認証情報（Ｂ’）を用いて暗号化した情報（γ_n：Ｅ＿｛Ｂ’｝（ａ））から、今回の認証に用いる今回認証情報の元となるデータ（ａ：Ｄ＿｛Ｂ’｝（γ_n））が算出されるかを確認することによって、第三者による送信情報の偽造を検出することができる。

【０１２５】

さらに、認証に用いるデータ（Ａ’）と、送付情報の偽造の検出に用いるデータ（Ａ）とを異なるデータにすることによって、認証処理の安全性を高めることができる。

【０１２６】

以上説明したように、本発明にかかる認証処理方法、認証処理プログラム、記録媒体および認証処理装置では、認証処理に用いるデータは、それぞれマスク処理されて送受信される。このため、認証処理に用いるデータの第三者への漏洩を防ぐことができる。また、今回認証情報の元となるデータａに一方向性変換を適用したデータと、今回認証情報Ａとが等しいか否かを検証することによって、被認証者の資格を認証することができる。

【０１２７】

また、本発明にかかる認証処理方法、認証処理プログラム、記録媒体および認証処理装置では、認証者に送付された情報の関係検証に加え、今回認証情報の元となるデータａに一方向性変換を適用したデータと今回認証情報Ａが等しいかを検証する。これにより、送付情報が正当な被認証者によって生成されたか否かを検知することができ、認証者側に登録されている今回認証情報Ａが盗まれたとしても、認証者本人以外による不正な認証を防止することができる。

【０１２８】

なお、本実施の形態で説明した認証処理方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、インターネット等のネットワークを介して配布することが可能な伝送媒体であってもよい。

【産業上の利用可能性】

【０１２９】

以上のように、本発明にかかる認証処理方法、認証処理プログラム、記録媒体および認証処理装置は、被認証者の利用資格、通信資格などの認証に有用であり、特に、情報通信

システムや鍵の開閉システムなどに適している。

【図面の簡単な説明】

【０１３０】

【図１】実施の形態にかかる認証処理システムのシステム構成を示す説明図である。

【図２】認証処理システムを構成するユーザ、サーバのハードウェア構成の一例を示すブロック図である。

【図３】認証処理システムを構成するユーザ、サーバの機能的構成を示すブロック図である。

【図４】ユーザの初期登録処理の手順を示すフローチャートである。

【図５】初回（ｎ＝１）以降、ｎ回目の認証処理の手順を示すフローチャートである。

【図６】ユーザの初期登録処理の手順を示すフローチャートである。

【図７】初回（ｎ＝１）以降、ｎ回目の認証処理の手順を示すフローチャートである。

【図８】ユーザの初期登録の処理手順を示すフローチャートである。

【図９】初回（ｎ＝１）以降、ｎ回目の認証処理の手順を示すフローチャートである。

【図１０】ＳＡＳ－２認証方式におけるユーザ認証の処理工程を示すフローチャートである。

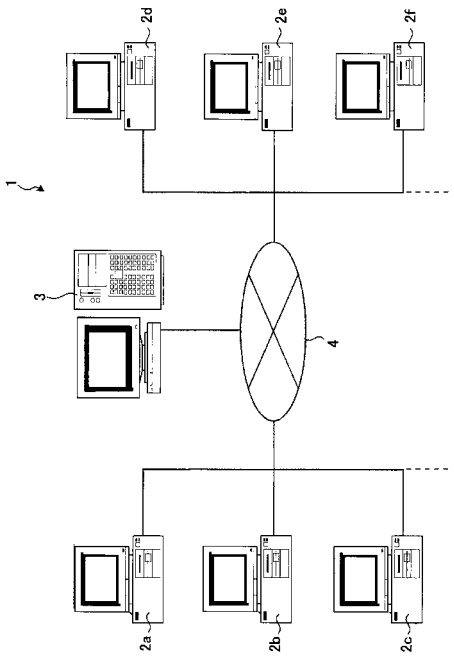
【図１１】ＳＡＳ－２認証方式におけるユーザ認証の処理工程を示すフローチャートである。

【符号の説明】

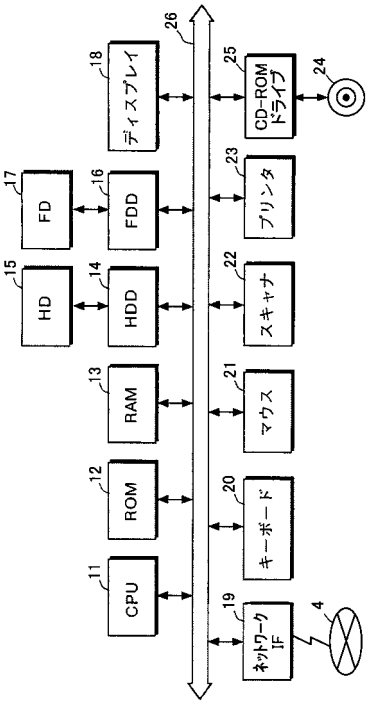
【０１３１】

１　認証処理システム
２ａ～２ｆ　ユーザ
３　サーバ
４　ネットワーク
３１　生成部
３２　送付部
３３　算出部
３４　送信部
４１　取得部
４２　受信部
４３　算出部
４４　判断部

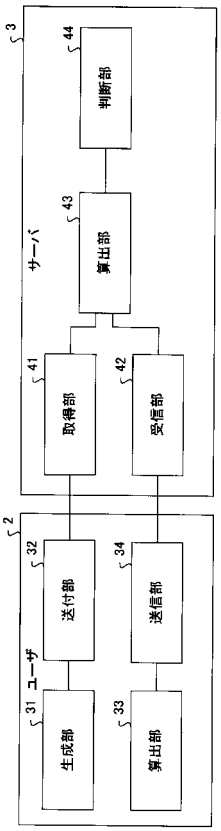
【図１】


1
2a
2b
2c
2d
2e
2f
3
4

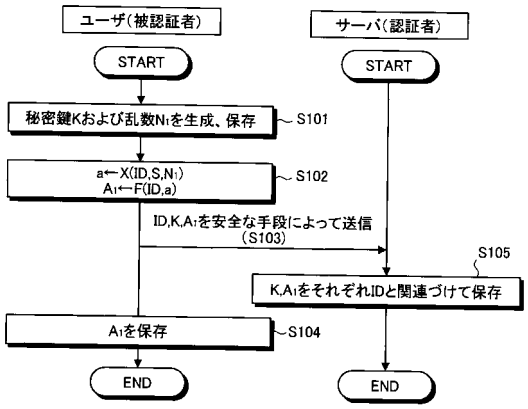
【図２】


CPU
ROM
RAM
HDD
HD
FDD
FD
ディスプレイ
CD-ROMドライブ
プリンタ
スキャナ
マウス
キーボード
ネットワークIF
4
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

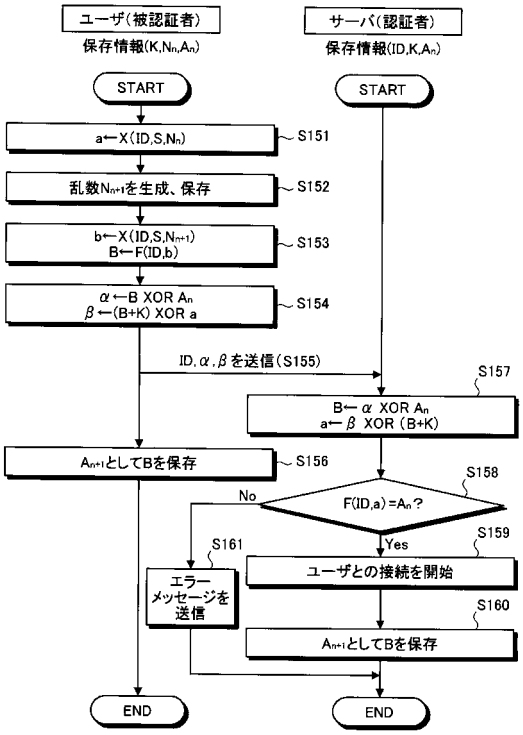
【図３】


サーバ
判断部
算出部
取得部
受信部
ユーザ
送付部
送信部
生成部
算出部
2
3
31
32
33
34
41
42
43
44

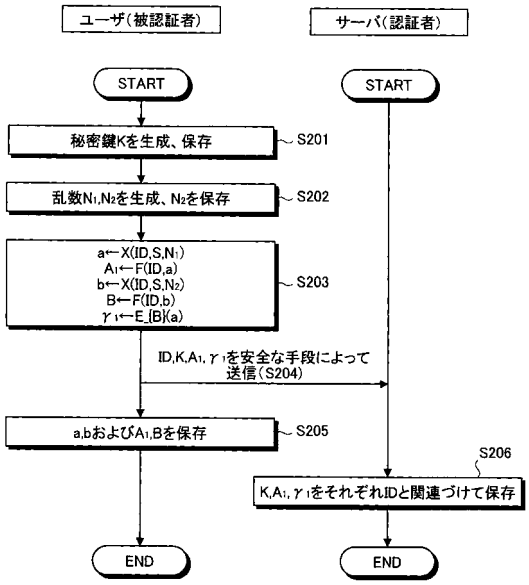
【図４】


ユーザ(被認証者)
サーバ(認証者)
START
START
秘密鍵Kおよび乱数N1を生成、保存
S101
a←X(ID,S,N1)
A1←F(ID,a)
S102
ID,K,A1を安全な手段によって送信
(S103)
S105
K,A1をそれぞれIDと関連づけて保存
A1を保存
S104
END
END

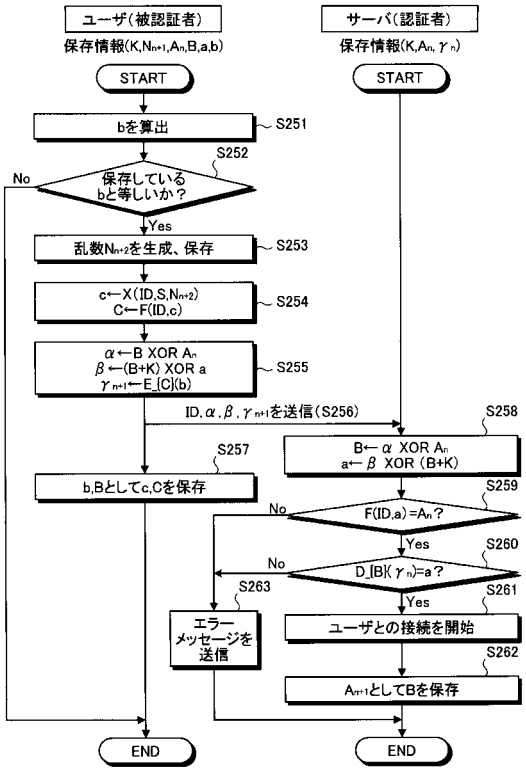
【図５】


ユーザ(被認証者)
保存情報(K,Nn,An)
サーバ(認証者)
保存情報(ID,K,An)
START
START
a←X(ID,S,Nn)
S151
乱数Nn+1を生成、保存
S152
b←X(ID,S,Nn+1)
B←F(ID,b)
S153
α←B XOR An
β←(B+K) XOR a
S154
ID,α,βを送信(S155)
S157
B←α XOR An
a←β XOR (B+K)
An+1としてBを保存
S156
S158
No
F(ID,a)=An?
Yes
S159
S161
ユーザとの接続を開始
エラーメッセージを送信
S160
An+1としてBを保存
END
END

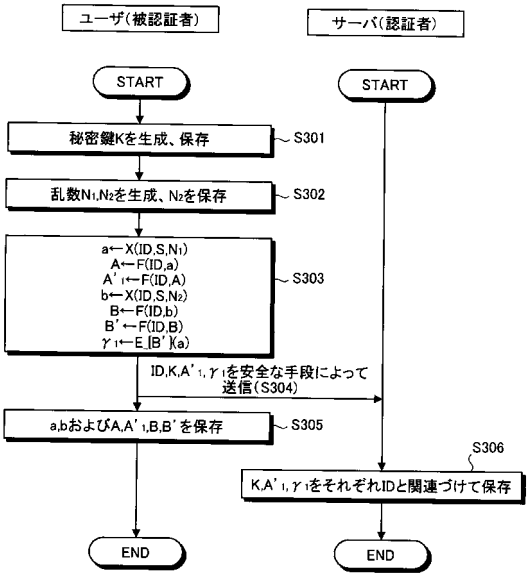
【図６】


ユーザ(被認証者)
サーバ(認証者)
START
START
秘密鍵Kを生成、保存
S201
乱数N1,N2を生成、N2を保存
S202
a←X(ID,S,N1)
A1←F(ID,a)
b←X(ID,S,N2)
B←F(ID,b)
γ1←E_[B](a)
S203
ID,K,A1,γ1を安全な手段によって送信(S204)
a,bおよびA1,Bを保存
S205
S206
K,A1,γ1をそれぞれIDと関連づけて保存
END
END

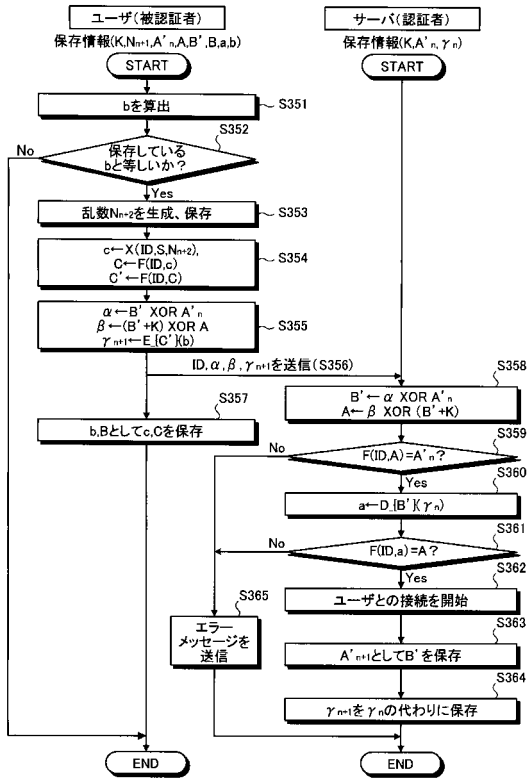
【図７】


ユーザ(被認証者)
保存情報(K,Nn+1,An,B,a,b)
サーバ(認証者)
保存情報(K,An,γn)
START
START
bを算出
S251
S252
No
保存しているbと等しいか?
Yes
乱数Nn+2を生成、保存
S253
c←X(ID,S,Nn+2)
C←F(ID,c)
S254
α←B XOR An
β←(B+K) XOR a
γn+1←E_[C](b)
S255
ID,α,β,γn+1を送信(S256)
S258
B←α XOR An
a←β XOR (B+K)
S257
b,Bとしてc,Cを保存
S259
No
F(ID,a)=An?
Yes
S260
No
D_[B](γn)=a?
Yes
S263
S261
エラーメッセージを送信
ユーザとの接続を開始
S262
An+1としてBを保存
END
END

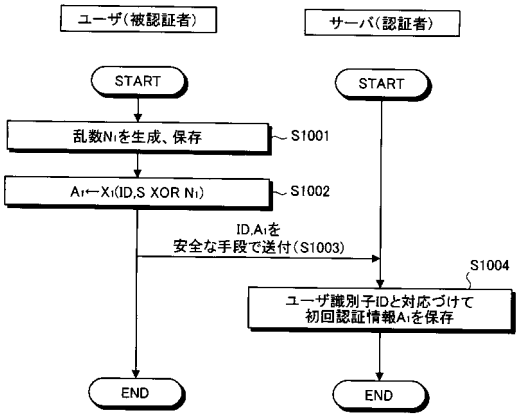
【図８】


ユーザ(被認証者)
サーバ(認証者)
START
START
秘密鍵Kを生成、保存
S301
乱数N1,N2を生成、N2を保存
S302
a←X(ID,S,N1)
A←F(ID,a)
A'1←F(ID,A)
b←X(ID,S,N2)
B←F(ID,b)
B'←F(ID,B)
γ1←E_[B'](a)
S303
ID,K,A'1,γ1を安全な手段によって送信(S304)
a,bおよびA,A'1,B,B'を保存
S305
S306
K,A'1,γ1をそれぞれIDと関連づけて保存
END
END

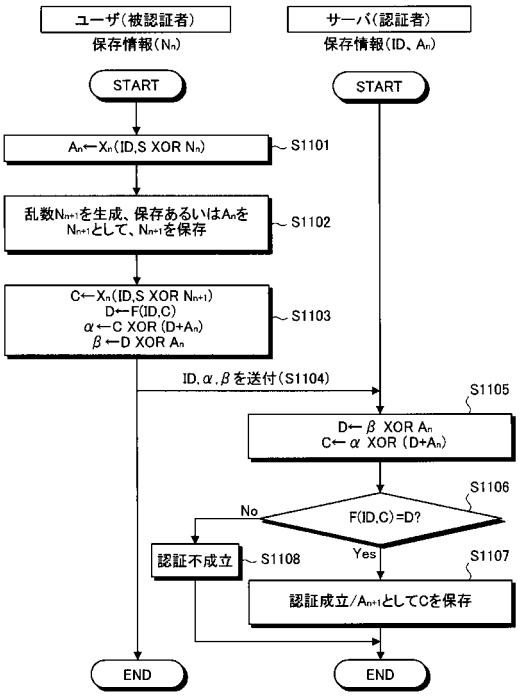
【図９】


ユーザ(被認証者)
保存情報(K,Nn+1,A'n,A,B',B,a,b)
サーバ(認証者)
保存情報(K,A'n,γn)
START
START
bを算出
S351
S352
保存している bと等しいか？
No
Yes
乱数Nn-2を生成、保存
S353
c←X(ID,S,Nn-2), C←F(ID,c) C'←F(ID,C)
S354
α←B' XOR A'n β←(B'+K) XOR A γn+1←E(C')(b)
S355
ID,α,β,γn+1を送信(S356)
S358
B'←α XOR A'n A←β XOR (B'+K)
S357
b,Bとしてc,Cを保存
S359
No
F(ID,A)=A'n?
Yes
S360
a←D(B')(γn)
S361
No
F(ID,a)=A？
Yes
S362
ユーザとの接続を開始
S365
エラー メッセージを 送信
S363
A'n+1としてB'を保存
S364
γn+1をγnの代わりに保存
END
END

【図１０】


ユーザ(被認証者)
サーバ(認証者)
START
START
乱数N1を生成、保存
S1001
A1←X1(ID,S XOR N1)
S1002
ID,A1を 安全な手段で送付(S1003)
S1004
ユーザ識別子IDと対応づけて 初回認証情報A1を保存
END
END

【図１１】


ユーザ(被認証者)
保存情報(Nn)
サーバ(認証者)
保存情報(ID、An)
START
START
An←Xn(ID,S XOR Nn)
S1101
乱数Nn+1を生成、保存あるいはAnを Nn+1として、Nn+1を保存
S1102
C←Xn(ID,S XOR Nn+1) D←F(ID,C) α←C XOR (D+An) β←D XOR An
S1103
ID,α,βを送付(S1104)
S1105
D←β XOR An C←α XOR (D+An)
S1106
No
F(ID,C)=D?
Yes
認証不成立
S1108
S1107
認証成立/An+1としてCを保存
END
END

フロントページの続き

(56)参考文献 特開２００５－０４５６９０（ＪＰ，Ａ）
特開２００３－１５２７１６（ＪＰ，Ａ）
特開２００２－２０８９２５（ＪＰ，Ａ）
特開２００１－０３６５２２（ＪＰ，Ａ）
特開平１０－１４５３５６（ＪＰ，Ａ）
特開平０２－０６５５４２（ＪＰ，Ａ）

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