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

特許第4440513号
(P4440513)

(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15日(2010.1.15)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330F
E05B 49/00	(2006.01)	E05B	49/00	K
H04L 9/32	(2006.01)	H04L	9/00	673C

請求項の数 4　(全 22 頁)

(21)出願番号　特願2002-70326(P2002-70326)
(22)出願日　平成14年3月14日(2002.3.14)
(65)公開番号　特開2003-273864(P2003-273864A)
(43)公開日　平成15年9月26日(2003.9.26)
審査請求日　平成16年12月13日(2004.12.13)
審判番号　不服2008-1923(P2008-1923/J1)
審判請求日　平成20年1月24日(2008.1.24)

早期審理対象出願

(73)特許権者　598125855
清水　明宏
高知県高知市知寄町二丁目３番地１６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

合議体
審判長　山崎　達也
審判官　石田　信行
審判官　冨吉　伸弥

最終頁に続く

(54)【発明の名称】資格認証方法

(57)【特許請求の範囲】
【請求項１】
被認証側の装置である第一情報処理装置と認証側の装置である第二情報処理装置で行う資格認証方法であって、
ｎを認証回数とするとき、初期登録（ｎ＝０）を行う初期登録ステップと、
初回（ｎ＝１）以降でｎ回目の認証時の処理である認証ステップと、を具備し、
前記初期登録ステップは、
前記第一情報処理装置において、
乱数Ｎ［１］を生成するステップと、
前記乱数Ｎ［１］を保存するステップと、
第一情報処理装置を識別する識別情報「ＩＤ」対応に規定するパスワード情報「Ｓ」と前記乱数Ｎ［１］に一方向性変換関数Ｘを施して初回マスク情報「Ａ」を算出するステップと、
保持している前記識別情報「ＩＤ」と前記算出した初回マスク情報「Ａ」を前記第二情報処理装置に送信するステップと、を具備し、
前記第二情報処理装置において、
前記初回マスク情報「Ａ」と前記識別情報「ＩＤ」を受信するステップと、
前記受信した初回マスク情報「Ａ」と識別情報「ＩＤ」とを対応付けて登録するステップと、を具備し、
前記認証ステップは、

前記第一情報処理装置において、
秘密に保持しているか、または前記識別情報「ＩＤ」対応に入力されるパスワード情報「Ｓ」と、前記識別情報「ＩＤ」対応に保存している乱数Ｎ［ｎ］と、に一方向性変換関数Ｘを施して今回マスク情報「Ａ」を算出するステップと、
乱数Ｎ［ｎ＋１］を生成するステップと、
前記乱数Ｎ［ｎ＋１］を保存するステップと、
前記パスワード情報「Ｓ」と、前記乱数Ｎ［ｎ＋１］に一方向性変換関数Ｘを施して、今回の認証および次回送信時のマスクに用いる次回マスク情報「Ｃ」を算出するステップと、
前記識別情報「ＩＤ」と、前記次回マスク情報「Ｃ」とにパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して、もうひとつの次回マスク情報「Ｄ」を算出するステップと、
前記算出した次回マスク情報「Ｄ」の値と、当該次回マスク情報「Ｄ」に今回マスク情報「Ａ」の値を加算した値との排他的論理和をとったデータ「α」を算出するステップと、
前記次回マスク情報「Ｃ」の値と、前記今回マスク情報「Ａ」の値との排他的論理和をとったデータ「β」を算出するステップと、
前記算出したデータ「α」と「β」とを、前記識別情報「ＩＤ」とともに前記第二情報処理装置に送信するステップと、を具備し、
第二情報処理装置において、
前記「α」、「β」および前記識別情報「ＩＤ」を受信するステップと、
前記受信した識別情報「ＩＤ」に対応付けて登録された今回マスク情報「Ａ」を読み出すステップと、
前記読み出した今回マスク情報「Ａ」の値と、前記受信した「β」との排他的論理和演算によって次回マスク情報「Ｃ」を算出するステップと、
前記算出した次回マスク情報「Ｃ」と、前記第二情報処理装置に保存されている識別情報「ＩＤ」とに一方向性変換関数Ｆを施して次回マスク情報「Ｄ」を算出するステップと、
前記算出した次回マスク情報「Ｄ」の値と、前記受信したデータ「α」の値との排他的論理和が、前記今回マスク情報「Ａ」に前記次回マスク情報「Ｄ」を加算した値と等しいか否かを判定するステップと、
前記判定するステップにおける判定結果に応じて前記第一情報処理装置の資格を認証するステップと、
前記算出した次回マスク情報「Ｃ」を、あらたに今回マスク情報「Ａ」として識別情報「ＩＤ」に対応付けて登録するステップと、を具備する資格認証方法。
【請求項２】
前記認証ステップは、
前記第二情報処理装置において、
前記受信した識別情報「ＩＤ」と、前記算出した次回マスク情報「Ｄ」とに前記一方向性変換関数Ｈを施してデータ「γ」を算出するステップと、
前記算出した「γ」を前記第一情報処理装置に送信するステップと、をさらに具備し、
前記第一情報処理装置において、
前記「γ」を第二情報処理装置から受信するステップと、
前記第二情報処理装置から受信したデータ「γ」を、前記自装置の識別情報「ＩＤ」と、次回マスク情報「Ｄ」とに前記一方向性変換関数Ｈを施して得られるデータと比較するステップと、をさらに具備する請求項１記載の資格認証方法。
【請求項３】
前記第一情報処理装置が開閉装置であり、前記第二情報処理装置が鍵識別子「Ｋ」に対応する鍵である情報処理システムにおける資格認証方法であって、
前記初期登録ステップにより前記鍵が初回マスク情報「Ａ」を保持している場合、

前記鍵は、前記鍵識別子「Ｋ」を開閉装置に送信するステップをさらに含み、
前記開閉装置は、前記鍵から鍵識別子「Ｋ」を受信するステップをさらに含み、
さらに、前記開閉装置にて前記鍵識別子「Ｋ」を利用して算出した前記データ「α」、「β」が、前記鍵にて前記判定するステップにおける判定結果に応じて前記開閉装置の資格が認証された場合に、前記開閉装置の施錠を開閉するステップを含むことを特徴とする請求項１または２に記載の資格認証方法。

【請求項４】

被認証側の装置である第一情報処理装置と認証側の装置である第二情報処理装置とを備える資格認証システムであって、
前記第一情報処理装置は、
乱数を生成する生成手段と、
前記生成手段によって生成された乱数を保存する保存手段と、
前記生成手段によって生成された乱数を用いて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値を前記第二情報処理装置に送信する送信手段と、を備え、
前記第二情報処理装置は、
前記第一情報処理装置によって送信された値を受信する受信手段と、
前記受信手段によって受信した値を登録する登録手段と、
前記受信手段によって受信した値および前記登録手段によって登録された値を用いて所定の演算をおこない第一情報処理装置の資格を認証する認証手段と、
を備え、
ｎを認証回数とし、初期登録（ｎ＝０）を行う初期登録時において、
前記第一情報処理装置の、
前記生成手段は、乱数Ｎ［１］を生成し、
前記保存手段は、前記乱数Ｎ［１］を保存し、
前記算出手段は、前記第一情報処理装置を識別する識別情報「ＩＤ」対応に規定するパスワード情報「Ｓ」と前記乱数Ｎ［１］に一方向性変換関数Ｘを施して初回マスク情報「Ａ」を算出し、
前記送信手段は、前記保存手段が保持している前記識別情報「ＩＤ」と前記算出手段が算出した初回マスク情報「Ａ」とを前記第二情報処理装置に送信し、
前記第二情報処理装置の、
前記受信手段は、前記初回マスク情報「Ａ」と前記識別情報「ＩＤ」を受信し、
前記登録手段は、前記受信手段によって受信された初回マスク情報「Ａ」と識別情報「ＩＤ」とを対応付けて登録し、
初回（ｎ＝１）以降のｎ回目の認証時において、
前記第一情報処理装置の、
前記算出手段は、秘密に保持しているか、または前記識別情報「ＩＤ」対応に入力されるパスワード情報「Ｓ」と、前記識別情報「ＩＤ」対応に保存している乱数Ｎ［ｎ］と、に一方向性変換関数Ｘを施して今回マスク情報「Ａ」を算出し、
前記生成手段は、乱数Ｎ［ｎ＋１］を生成し、
前記保存手段は、前記生成手段によって生成された乱数Ｎ［ｎ＋１］を保存し、
前記算出手段は、
前記パスワード情報「Ｓ」と、前記乱数Ｎ［ｎ＋１］に一方向性変換関数Ｘを施して、今回の認証および次回送信時のマスクに用いる次回マスク情報「Ｃ」を算出し、
前記識別情報「ＩＤ」と、前記次回マスク情報「Ｃ」とにパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して、もうひとつの次回マスク情報「Ｄ」を算出し、
前記算出した次回マスク情報「Ｄ」の値と、当該次回マスク情報「Ｄ」に今回マスク情報「Ａ」の値を加算した値との排他的論理和をとったデータ「α」を算出し、
前記次回マスク情報「Ｃ」の値と、前記今回マスク情報「Ａ」の値との排他的論理和をとったデータ「β」を算出し、

前記送信手段は、前記算出手段によって算出されたデータ「α」と「β」とを、前記識別情報「ＩＤ」とともに前記第二情報処理装置に送信し、
第二情報処理装置の、
受信手段は、前記「α」、「β」および前記識別情報「ＩＤ」を受信し、
前記登録手段は、前記受信した識別情報「ＩＤ」に対応付けて登録された今回マスク情報「Ａ」を読み出し、
前記認証手段は、
前記読み出した今回マスク情報「Ａ」の値と、前記受信した「β」との排他的論理和演算によって次回マスク情報「Ｃ」を算出し、
前記算出した次回マスク情報「Ｃ」と、前記第二情報処理装置に保存されている識別情報「ＩＤ」と、に一方向性変換関数Ｆを施して次回マスク情報「Ｄ」を算出し、
前記算出した次回マスク情報「Ｄ」の値と、前記受信したデータ「α」の値との排他的論理和が、前記今回マスク情報「Ａ」に前記次回マスク情報「Ｄ」を加算した値と等しいか否かを判定し、
前記判定における判定結果に応じて前記第一情報処理装置の資格を認証し、
前記登録手段は、前記認証手段によって算出した次回マスク情報「Ｃ」を、あらたに今回マスク情報「Ａ」として識別情報「ＩＤ」に対応付けて登録することを特徴とする資格認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、情報通信システム、あるいは鍵の開閉システム等において、通信相手やユーザの利用資格を認証する方法に関するものである。

【０００２】

【従来の技術】

従来、被認証者（ユーザ）の装置が認証者（センタ）の装置に認証を受ける手順であって、ユーザが入力するパスワードの正当性をセンタ側で認証する機能を有する方法として、ＳＡＳ認証方式がある。このＳＡＳ認証方式は、「ワンタイムパスワード認証方式　ＳＡＳ　の安全性に関する検討」（電子情報通信学会技術研究報告書，ＯＦＳ２００１－４８，Ｎｏ．　４３５，ｐｐ．　５３－５８，２００１　）に記載されている。以下、このＳＡＳ認証方式について説明する。

【０００３】

なお、従来技術の説明に用いる記法を以下に示す。

【０００４】

「←」は、右辺の左辺への代入を示す。「Ｓ」は、被認証者が秘密に保持しているパスワードを示す。「ＩＤ」は、被認証者側の装置（以下、適宜、「被認証者」と言う。）を識別する情報である被認証者識別子を示す。「ＸＯＲ」は、排他的論理和の演算を示す。「ｎ」は、認証回数を示す。Ｎ［ｎ］のＮは、乱数を示す。ｎは１以上の整数で、乱数を識別するために用いる。「Ｅ」は、パスワードＳを用いない一方向性変換関数を示す。なお、一方向性変換関数とは「ｚ＝Ｅ（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を言う。「Ｅ［１］［ｎ］」は、パスワードＳと乱数Ｎ［ｎ］を用いる一方向性変換関数で、「Ｅ［１］［ｎ］＝Ｅ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［ｎ］）」により導き出せる。Ｅ［ｍ］［ｎ］（「ｍ」は２以上の整数）は、乱数Ｎ［ｎ］に対応した一方向性変換関数で、「Ｅ［ｍ］［ｎ］＝Ｅ（ＩＤ，Ｅ［ｍ－１］［ｎ］）」により導き出せる。

【０００５】

ＳＡＳ方式による認証の手順のうちの初期登録時の手順について、図８のフロー図を用いて説明する。

【０００６】

図８によれば、初期登録時、ユーザ（被認証者）側の装置において、以下の処理を行う。

まず、ユーザが秘密に保持しているパスワードＳ，乱数Ｎ［１］、ユーザ識別子ＩＤを用いて、「ａ←Ｅ［１］［１］＝Ｅ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［１］）」を演算して、「ａ」を導き出す。次に、「ｂ←Ｅ［２］［１］＝Ｅ（ＩＤ，ａ）」により、「ｂ」を導き出す。「ｂ」は、次回の認証に用いる認証情報である。

【０００７】

次に、ユーザ（被認証者）側の装置は、ユーザ識別子「ＩＤ」とともに、安全な手段でセンタに初回の認証に用いる認証情報「ｂ」を、センタ（認証者）側の装置に送付する。そして、ユーザ（被認証者）側の装置において、乱数Ｎ［１］は保存しておく。

【０００８】

次に、センタ側の装置では、受け取った初回の認証に用いる認証情報「ｂ」をユーザ識別子「ＩＤ」と共に登録（記録）しておく。

【０００９】

次に、図９を用いて、ＳＡＳ方式による認証の手順のうちの認証時の手順について説明する。ここで説明する認証時手順は、初回（ｎ＝１）以降で、ｎ回目の認証時の手順である。まず、ユーザ側の装置において、保存している乱数Ｎ［ｎ］から、「ａ←Ｅ［１］［ｎ］＝Ｅ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［ｎ］）」の演算を行い、次に、「ｂ←Ｅ［２］［ｎ］＝Ｅ（ＩＤ，ａ）」の演算を行う。そして、さらに新しい乱数Ｎ［ｎ＋１］を発生させ、当該乱数Ｎ［ｎ＋１］を保存する。そして、乱数Ｎ［ｎ＋１］を用いて、以下の３つの演算を行う。▲１▼「ｚ←Ｅ［１］［ｎ＋１］＝Ｅ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［ｎ＋１］）」▲２▼「ｃ←Ｅ［２］［ｎ＋１］＝Ｅ（ＩＤ，ｚ）」　▲３▼「ｄ←Ｅ［３］［ｎ＋１］＝Ｅ（ＩＤ，ｃ）」

【００１０】

以上の演算により、算出した「ａ」、「ｂ」、「ｃ」、「ｄ」を用いて、「α←ａ　ＸＯＲ　ｄ」「β←ｃ　ＸＯＲ　ｂ」の演算を行い、「α」と「β」を算出する。そして、ユーザ側の装置は、「α」および「β」を「ＩＤ」と共にセンタ側の装置に送付する。

【００１１】

この時、「ｂ」は今回認証情報、「ａ」は今回認証情報「ｂ」の一方向性変換の元の情報、「ｃ」は次回認証情報、「ｄ」は次回認証情報「ｃ」を一方向性変換したデータである。

【００１２】

次に、センタ側の装置において、「α」と「β」と「ＩＤ」を受け取る。そして、センタ側の装置は、受け取った「α」と「β」に対して、以下の３つの演算を行う。▲１▼「ｃ←β　ＸＯＲ　ｂ」▲２▼「ｄ←Ｅ（ＩＤ，ｃ）」　▲３▼「ａ←α　ＸＯＲ　ｄ」

【００１３】

以上の演算により、センタ側の装置は、「ａ」を算出し、「Ｅ（ＩＤ，ａ）」と，「ＩＤ」に対応して登録されている今回認証情報「ｂ」を比較し，一致すれば被認証者の資格を認証し、次回の認証に用いる認証情報として次回認証情報「ｃ」を新しく「ｂ」として登録する。

【００１４】

以上をまとめると、以下のようなことが言える。「ＳＡＳ認証方式」では、今回認証情報「ｂ」を事前に送付しておき、今回認証情報「ｂ」の一方向性変換の元のデータ「ａ」を認証時に送付し、このデータ「ａ」に同じ一方向性変換を適用した結果が今回認証情報「ｂ」に等しいかどうかを判断することにより、被認証者の資格を認証することを原理としている。

【００１５】

また、これら今回認証情報「ｂ」の一方向性変換の元のデータ「ａ」と次回認証情報「ｃ」を安全に送付するために、次回認証情報「ｃ」には今回認証情報「ｂ」を、また、「ｂ」の一方向性変換の元のデータ「ａ」には次回認証情報「ｃ」に一方向性変換を適用した情報「ｄ」をそれぞれ排他的論理和でマスクして送付することにより、送付途中のデータから今回認証情報「ｂ」、「ｂ」の一方向性変換の元のデータ「ａ」、次回認証情報「ｃ

」が第三者に取得されることを防いでいる。
【００１６】
【発明が解決しようとする課題】
しかし、従来の「ＳＡＳ認証方式」においては，ユーザ側の装置での一方向性変換関数の適用回数は５回で、かつ保存しておくデータは乱数１個分であるが、処理負担の大きい一方向性変換関数の適用回数は１回でも少ない方がよい。特に、ＰＤＡや携帯電話、ＩＣカード，通信プロトコル等への適用を考えた場合、高速な処理が要求されるのでなおさらである。
【００１７】
さらに，「ＳＡＳ認証方式」においては、被認証者側の装置において，認証者による認証が成功したことを確認するかあるいは被認証者が認証者を相互に認証する手段がないため，通信途中で通信がとぎれたり、何らかの原因で同期がずれたりした場合に，認証を失敗することが考えられる。
【００１８】
【課題を解決するための手段】
そこで、本発明の資格認証方法は、被認証側の装置である第一情報処理装置と認証側の装置である第二情報処理装置で行う資格の認証を受ける資格認証方法であって、ｎを認証回数とするとき、初期登録（ｎ＝０）を行う初期登録ステップと、初回（ｎ＝１）以降でｎ回目の認証時の処理である認証ステップを具備し、初期登録ステップは、以下のステップを具備する。つまり、初期登録ステップは、第一情報処理装置において、乱数Ｎ［１］を生成するステップと、乱数Ｎ［１］を保存するステップと、識別情報「ＩＤ」対応に規定するパスワード情報「Ｓ」と乱数Ｎ［１］に一方向性変換関数Ｘを施して初回マスク情報「Ａ」を算出するステップと、保持している第一情報処理装置を識別する識別情報「ＩＤ」と前記算出した初回マスク情報「Ａ」をと第二情報処理装置に送信するステップを具備し、第二情報処理装置において、初回マスク情報「Ａ」と識別情報「ＩＤ」を受信するステップと、受信した初回マスク情報「Ａ」と識別情報「ＩＤ」を登録するステップを具備する。認証ステップは、以下のステップを具備する。つまり、認証ステップは、第一情報処理装置において、保持しているパスワード情報「Ｓ」と保存している乱数Ｎ［ｎ］に一方向性変換関数Ｘを施して今回マスク情報「Ａ」を算出するステップと、乱数Ｎ［Ｎ＋１］を発生するステップと、乱数Ｎ［Ｎ＋１］を保存するステップと、パスワード情報「Ｓ」と乱数Ｎ［Ｎ＋１］に一方向性変換関数Ｘを施して，今回の認証および次回送信時のマスクに用いる次回マスク情報「Ｃ」を生成するステップと、今回マスク情報「Ａ」にパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して得られるもうひとつの今回マスク情報「Ｂ」を算出する第一演算、または、次回マスク情報「Ｃ」にパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して得られるもうひとつの次回マスク情報「Ｄ」を算出する第二演算のどちらかの演算を行うステップと、今回マスク情報のいずれか、または次回マスク情報のいずれかに、ある定数を融合させたデータを新しくそれぞれの今回マスク情報あるいは次回マスク情報にし、次回マスク情報と今回マスク情報の排他的論理和をとったふたつのデータ「α」と「β」を前記識別情報「ＩＤ」とともに第二情報処理装置に送付するステップと、第二情報処理装置において、「α」、前記「β」、および前記識別情報「ＩＤ」を受信するステップと、受信したデータ「α」と「β」から今回マスク情報を用いて次回マスク情報を取り出し、次回マスク情報同士あるいは次回マスク情報と今回マスク情報の関係を検証することにより第一情報処理装置の資格を認証するステップと、新しく次回マスク情報「Ｃ」を今回マスク情報「Ａ」として識別情報「ＩＤ」に対応付けて登録するステップを具備する。かかる、資格認証方法により、被認証者側および認証者側の処理を大幅に軽減できる。
【００１９】
上記資格認証方法によれば、原理的に次回マスク情報「Ｃ」を今回マスク情報「Ａ」でマスクするデータと、同じく今回マスク情報「Ａ」で次回マスク情報「Ｃ」の一方向性変換であるデータ「Ｄ」をマスクするデータの二つを送付するか、あるいは、次回マスク情報

「Ｃ」を今回マスク情報「Ａ」に一方向性変換を適用したデータでマスクしたデータと、同じく次回マスク情報「Ｃ」を今回マスク情報「Ａ」でマスクしたデータの二つを送付することにより、従来技術の「ＳＡＳ認証方式」と同様、認証に用いる今回マスク情報「Ａ」と次回マスク情報「Ｃ」の第三者への漏洩を防いだ上で、今回マスク情報「Ａ」によりマスクされて送付される次回マスク情報「Ｃ」と、今回マスク情報「Ａ」に一方向性変換を適用したデータでマスクされる次回マスク情報「Ｃ」が等しいかどうかを検証することによって、被認証者の資格を認証するようにしている。

【００２０】

さらに、本発明の認証方法では、次回マスク情報あるいは今回マスク情報に、定数、あるいは次回マスク情報には今回マスク情報を、また今回マスク情報には次回マスク情報をそれぞれ融合することで、一度認証に用いた認証情報の再利用による不正行為を無効にするようにしている。ここで「融合する」とは、２以上のデータを加算したり、減算したり、ｂｉｔをずらしたりする各種演算を行う、ことを言う。

【００２１】

これらにより，今回マスク情報「Ａ」および次回マスク情報「Ｃ」の、それぞれの一方向性変換の元のデータを用意することが不要になり、処理負荷の大きい一方向性変換の適用回数を、「ＳＡＳ認証方式」の５回に対して、３回にすることができる。つまり、従来技術と比べて、２回も一方向性変換の適用回数を減らすことができる。これは、認証の処理速度を約４０％軽減できることを意味する。

【００２２】

また、毎回の認証時に個別に保管している乱数から今回マスク情報「Ａ」を、また、新しく発生させた乱数から次回マスク情報「Ｃ」を生成する方法に加え、本発明の認証方法では、各回の認証時に、今回マスク情報「Ａ」を乱数として用い次回マスク情報「Ｃ」の生成を行なうことにより、乱数発生機構を不要にすることができる。一般に乱数発生には一方向性変換と同様の処理負荷がかかることから、これを不要にすることで処理をさらに軽減することができる。

【００２３】

さらに、認証者側の装置において、被認証者側の装置から送付されてきた情報によって被認証者の認証が完了した後、認証者側の装置から被認証者側の装置へ、今回認証に用いた情報を加工して生成した確認情報を送付することによって、被認証者側において、認証者による認証が成功したことを確認するかあるいは被認証者が認証者を相互に認証することを可能にする。

【００２４】

【発明の実施の形態】

以下、被認証者側の第一情報処理装置と、認証者側の第二情報処理装置を有する情報処理システムおよびそのプログラム等の実施形態について図面を参照して説明する。なお、実施の形態において同じ符号を付した構成要素は同様の動作を行うので、再度の説明を省略する場合がある。

【００２５】

また、実施の形態において、以下の記法を用いる。

【００２６】

「←」は、右辺の左辺への代入を示す。「Ｓ」は、被認証者側の第一情報処理装置が秘密に保持しているパスワードを示す。「ＩＤ」は、被認証者側の第一情報処理装置を識別する情報である被認証者識別子を示す。「ＸＯＲ」は、排他的論理和の演算を示す。「ｎ」は、認証回数を示す。Ｎ［ｎ］のＮは、乱数を示す。Ｎ［ｎ］のｎは１以上の整数で、乱数を識別するために用いる。「Ｆ」、「Ｈ」は、パスワードＳを用いない一方向性変換関数を示す。なお、一方向性変換関数とは「ｚ＝Ｆ（ｘ，ｙ）」あるいは「ｚ＝Ｈ（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、もしくはｚとｘからｙを算出することができない関数を言う。「Ｘ」は、パスワードＳと乱数Ｎ［ｎ］を用いる一方向性変換関数であり、「Ｘ［ｎ］＝Ｘ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［ｎ］）」のよ

うに、「Ｘ［ｎ］」を算出するために用いる。

【００２７】

（実施の形態１）

【００２８】

本実施の形態における、被認証者（ユーザ）側の第一情報処理装置と認証者（センタ）の第二情報処理装置を有する情報処理システムの構成を示すブロック図を図１に示す。

【００２９】

情報処理システムは、第一情報処理装置１１と第二情報処理装置１２を有する。

【００３０】

第一情報処理装置１１は、ユーザ識別子格納部１１０１、パスワード格納部１１０２、第一演算部１１０３、第一送信部１１０４、第一受信部１１０５を有する。

【００３１】

ユーザ識別子格納部１１０１は、ユーザまたは第一情報処理装置を識別子するユーザ識別子（以下、ユーザ識別子を記号で、適宜「ＩＤ」と言う。）を格納している。このユーザ識別子は、認証処理の都度、ユーザに入力されるものであっても良いし、第一情報処理装置が予め格納しているＩＤを、認証処理の際に利用するものであっても良い。ユーザ識別子格納部１１０１は、不揮発性または揮発性の記録媒体で実現され得る。

【００３２】

パスワード格納部１１０２は、被認証者（ユーザ）を認証するためのパスワード（以下、パスワードを、適宜「Ｓ」と言う。）を格納している。パスワード「Ｓ」は、認証処理の都度、ユーザに入力されるものであっても良いし、第一情報処理装置が予め格納している「Ｓ」を、認証処理の際に利用するものであっても良い。パスワード格納部１１０２は、不揮発性または揮発性の記録媒体で実現され得る。

【００３３】

ユーザ識別子格納部１１０１、パスワード格納部１１０２は、通常、一の記録媒体で実現され得るが、異なる記録媒体で実現されても良い。

【００３４】

第一演算部１１０３は、一方向性変換（一方向性変換関数を用いた演算）や、乱数の発生や、排他的論理和の演算等の演算を行う。第一演算部１１０３は、通常、ＣＰＵやメモリ等から実現され得る。第一演算部１１０３が演算を行うための関数や処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００３５】

第一送信部１１０４は、第一演算部１１０３の演算結果等を第二情報処理装置１２に送信する。第一送信部１１０４は、無線または有線の通信手段または、放送手段で実現され得る。

【００３６】

第一受信部１１０５は、第二情報処理装置１２からデータを受信する。第一受信部１１０５は、無線または有線の通信手段または、放送を受信する手段（チューナーおよびソフトウェアドライバ等）で実現され得る。

【００３７】

なお、第一送信部１１０４と第一受信部１１０５は、通常、一の手段で実現されるが、異なる手段で実現されても良い。

【００３８】

第二情報処理装置１２は、第二受信部１２０１、情報記録部１２０２、第二演算部１２０３、認証部１２０４、第二送信部１２０５を有する。

【００３９】

第二受信部１２０１は、第一情報処理装置１１からデータを受信する。第二受信部１２０１は、通常、無線または有線の通信手段で実現され得るが、放送を受信する手段を排除するものではない。

【００４０】
情報記録部１２０２は、第二受信部１２０１が受信したデータの全部また一部または、第二演算部１２０３の演算結果等を記録する。情報記録部１２０２は、通常、ソフトウェアで実現され得るが、ハード（専用回路）で実現しても良い。情報記録部１２０２の情報の記録先は、第二情報処理装置１２に内蔵されている記録媒体でも、外付けの記録媒体でも良い。なお、記録媒体は、不揮発性の記録媒体でも、揮発性の記録媒体でも良い。
【００４１】
第二演算部１２０３は、一方向変換や、排他的論理和などの演算を行う。第二演算部１２０３は、通常、ＣＰＵ、メモリ、およびソフトウェア等から実現され得る。つまり、一方向性関数の演算式や、各種演算のアルゴリズムは、通常、ソフトウェアで実現され、当該ソフトウェアは、第二演算部１２０３のメモリ（ＲＯＭ等）に格納されている。
【００４２】
認証部１２０４は、第二演算部１２０３の演算結果等に基づいて、認証を行う。鍵側認証部５２０４は、通常、ソフトウェアで実現され得るが、ハードウェア（専用回路）で実現しても良い。
【００４３】
第二送信部１２０５は、第二情報処理装置１２から第一情報処理装置１１に、第二演算部１２０３の演算結果の情報を送信する。第二送信部１２０５は、無線または有線の通信手段、または放送手段で実現され得る。
【００４４】
以下、被認証者（ユーザ）側の第一情報処理装置１１が認証者（センタ）側の第二情報処理装置１２に認証を受ける手順を、図２、および図３を用いて説明する。まず、図２は、被認証者（ユーザ）の初期登録の手順を説明するフローである。
【００４５】
まず、ユーザ側の第一情報処理装置１１において、予めパスワード「Ｓ」とユーザ識別子「ＩＤ」が格納されている。そして、第一情報処理装置１１の第一演算部１１０３は、乱数Ｎ［１］を発生する。そして、第一演算部１１０３は、乱数Ｎ［１］を保存する。乱数を発生する技術は、既存技術であるので、説明は省略する。
【００４６】
次に、第一演算部１１０３は、乱数Ｎ［１］、ユーザ識別子「ＩＤ」、パスワード「Ｓ」を用いて、「Ａ←Ｘ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［１］）」の演算を行う。そして、初回の認証に用いるマスク情報「Ａ」を算出する。
【００４７】
次に、第一送信部１１０４は、ユーザ識別子「ＩＤ」とマスク情報「Ａ」をセンタ（認証者）側の第二情報処理装置１２に送信する。なお、マスク情報「Ａ」等の送信は、安全な手段で第二情報処理装置１２に送信されるのが好ましい。
【００４８】
次に、第二情報処理装置１２の第二受信部１２０１は、ユーザ識別子「ＩＤ」とマスク情報「Ａ」を受信する。次に、情報記録部１２０２は、第二受信部１２０１が受信したユーザ識別子「ＩＤ」とマスク情報「Ａ」を対応付けて登録する。
【００４９】
以上が、被認証者（ユーザ）の初期登録の手順である。
【００５０】
次に、初回（ｎ＝１）以降で、ｎ回目の認証時の処理について、図３のフローを用いて説明する。
【００５１】
まず、ユーザ側の第一情報処理装置１１は、保存している乱数Ｎ［ｎ］、「ＩＤ」、「Ｓ」を取り出す。なお、「ＩＤ」、「Ｓ」は、データ送信等が行われる毎（認証の必要がある場合毎）にユーザにより入力される場合もあれば、第一情報処理装置１１が格納している場合もある。第一情報処理装置１１が「ＩＤ」、「Ｓ」を格納している場合は、第一情

報処理装置「ＩＤ」、「Ｓ」を取り出す。

【００５２】

次に、第一演算部１１０３は、乱数Ｎ［ｎ］、「ＩＤ」、「Ｓ」を用いて、「Ａ←Ｘ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［ｎ］）」の演算を行う。そして、「Ａ」を算出する。

【００５３】

そして、第一演算部１１０３は、さらに、新しい乱数Ｎ［ｎ＋１］を発生させるか、または、「Ａ」をＮ［ｎ＋１］として、以下の演算を行う。「Ｃ←Ｘ（ＩＤ，Ｓ　ＸＯＲ　Ｎ［Ｎ＋１］）」、「Ｄ←Ｆ（ＩＤ，Ｃ）」の演算により、「Ｃ」と「Ｄ」を算出する。

【００５４】

次に、第一演算部１１０３は、算出した「Ａ」、「Ｃ」、「Ｄ」を用いて、以下の演算を行う。「α←Ｄ　ＸＯＲ　（Ａ＋Ｄ）」、「β←Ｃ　ＸＯＲ　Ａ」の演算により、「α」と「β」を算出する。

【００５５】

そして、第一送信部１１０４は、「α」と「β」を「ＩＤ」と共にセンタ側の第二情報処理装置に送付する。

【００５６】

この時、第一情報処理装置は、乱数Ｎ［ｎ＋１］（「Ａ」の場合もあり得る。）を保存しておく。

【００５７】

なお、「Ａ」は今回マスク情報、「Ｃ」は次回マスク情報、「Ｄ」は次回マスク情報「Ｃ」を一方向性変換したもうひとつの次回マスク情報である。

【００５８】

次に、センタ側の第二情報処理装置における処理を説明する。第二情報処理装置の第二受信部１２０１は、「α」と「β」と「ＩＤ」を受信する。そして、第二演算部１２０３は、受け取った「ＩＤ」に対応する今回マスク情報「Ａ」を取り出す。そして、第二演算部１２０３は、受け取った「α」と「β」と、今回マスク情報「Ａ」を用いて、「Ｃ←β　ＸＯＲ　Ａ」の演算を行い、「Ｃ」を算出する。

【００５９】

そして、第二演算部１２０３は、算出した「Ｃ」から「Ｆ（ＩＤ，Ｃ）」で「Ｄ」を算出する。認証部１２０４は、αと排他的論理和をとったものが「Ａ＋Ｄ」に等しいかどうかを検証する。

【００６０】

または、第二演算部１２０３は、「Ｃ」から「Ｆ（ＩＤ，Ｃ）」で「Ｄ」を算出し，「Ａ」を加えたもの（「Ｆ（ＩＤ，Ｃ）＋Ａ」）とαの排他的論理和を算出する。認証部１２０４は、当該第二演算部１２０３の演算結果（（「Ｆ（ＩＤ，Ｃ）＋Ａ」）とαの排他的論理和）と「Ｄ」が等しいかどうかを検証する。

【００６１】

以上の検証は、第二受信部１２０１が受信したデータ「α」と「β」から今回マスク情報を用いて次回マスク情報を取り出し、次回マスク情報同士あるいは次回マスク情報と今回マスク情報の関係を検証するものである。

【００６２】

認証部１２０４は、両データが一致すれば、被認証者（第一情報処理装置）の資格を認証する。「資格を認証する」とは、第一情報処理装置からのアクセスが適正であると判断する、ことを言う。そして、情報記録部１２０２は、次回の認証に用いるマスク情報として次回マスク情報「Ｃ」を新しく「Ａ」として登録する。

【００６３】

以上、本実施の形態において、被認証者側の装置において、従来技術の「ＳＡＳ認証方式」の５回と比較して２回減らし、３回の適用回数で認証が可能になる。また、相互認証の手順を付加しない場合は、認証者側の装置において、「ＳＡＳ証方式」の２回に対して、半分の１回にすることができる。従って、高速な認証処理が可能である。

【００６４】
さらに，毎回の認証時に個別に保管している乱数から今回マスク情報「Ａ」を、また、新しく発生させた乱数から次回マスク情報「Ｃ」を生成する方法に加え、本実施の形態における資格認証方法では、各回の認証時に、今回マスク情報「Ａ」を乱数として用い、次回マスク情報「Ｃ」の生成を行なうことにより、乱数発生機構を不要にすることができる。一般に乱数発生には一方向性変換と同様の処理負荷が必要であることから、これを不要にすることで被認証者側の処理をさらに軽減することができる。
【００６５】
なお、本実施の形態において、α，βの算出は、「α←Ｄ　ＸＯＲ　（Ａ＋Ｄ）」、「β←Ｃ　ＸＯＲ　Ａ」とする場合を示したが、以下の演算により算出しても良い。
【００６６】
（１）「α←Ｄ　ＸＯＲ　（Ａ＋Ｃ）」、「β←Ｃ　ＸＯＲ　Ａ」
（２）「α←Ｄ　ＸＯＲ　Ａ」、「β←Ｃ　ＸＯＲ　（Ａ＋Ｄ）」
（３）「α←Ｄ　ＸＯＲ　Ａ」、「β←Ｃ　ＸＯＲ　（Ａ＋Ｃ）」
（４）「α←（Ａ＋Ｄ）　ＸＯＲ　Ａ」、「β←Ｃ　ＸＯＲ　Ａ」
（５）「α←Ｄ　ＸＯＲ　Ａ」、「β←（Ａ＋Ｃ）　ＸＯＲ　Ａ」
（６）「α←（Ｂ＋Ｃ）　ＸＯＲ　Ｂ」、「β←Ｃ　ＸＯＲ　Ａ」
（７）「α←（Ａ＋Ｃ）　ＸＯＲ　Ｂ」、「β←Ｃ　ＸＯＲ　Ａ」
（８）「α←Ｃ　ＸＯＲ　Ｂ」、「β←（Ｂ＋Ｃ）　ＸＯＲ　Ａ」
（９）「α←Ｃ　ＸＯＲ　Ｂ」、「β←（Ａ＋Ｃ）　ＸＯＲ　Ａ」
（１０）「α←Ｃ　ＸＯＲ　（Ｂ＋Ｃ）」、「β←Ｃ　ＸＯＲ　Ａ」
（１１）「α←Ｃ　ＸＯＲ　Ｂ」、「β←Ｃ　ＸＯＲ　（Ａ＋Ｃ）」
【００６７】
さらに、任意の定数「Ｖ」を用いて、α，βは、以下の演算により算出しても良い。
【００６８】
（１２）「α←Ｄ　ＸＯＲ　（Ａ＋Ｖ）」、「β←Ｃ　ＸＯＲ　Ａ」
（１３）「α←Ｄ　ＸＯＲ　Ａ」、「β←Ｃ　ＸＯＲ　（Ａ＋Ｖ）」
（１４）「α←（Ｖ＋Ｄ）　ＸＯＲ　Ａ」、「β←Ｃ　ＸＯＲ　Ａ」
（１５）「α←Ｄ　ＸＯＲ　Ａ」、「β←（Ｖ＋Ｃ）　ＸＯＲ　Ａ」
（１６）「α←（Ｖ＋Ｃ）　ＸＯＲ　Ｂ」、「β←Ｃ　ＸＯＲ　Ａ」
（１７）「α←Ｃ　ＸＯＲ　Ｂ」、「β←（Ｖ＋Ｃ）　ＸＯＲ　Ａ」
（１８）「α←Ｃ　ＸＯＲ　（Ｂ＋Ｖ）」、「β←Ｃ　ＸＯＲ　Ａ」
（１９）「α←Ｃ　ＸＯＲ　Ｂ」、「β←Ｃ　ＸＯＲ　（Ａ＋Ｖ）」
【００６９】
上記の１９の演算により「α」や「β」を算出して、当該「α」や「β」を認証に用いても、本実施の形態において説明した認証方法での認証が可能である。つまり、「α」と「β」を算出する演算式のバランスが取れていなければ良い。演算式のバランスが取れていないようにする、とは、すでにやり取りされたα、βのＸＯＲでの演算項が今回以降の演算において出現しないようにすることによって、再利用攻撃を防止することを意味する。
【００７０】
また、本実施の形態において、今回マスク情報と次回マスク情報の融合は１箇所で行ったが、今回マスク情報と次回マスク情報の融合を複数箇所で行っても良い。
【００７１】
また、本実施の形態において、加算による今回マスク情報と次回マスク情報の融合を示したが、今回マスク情報と次回マスク情報は、減算や乗算やビットシフトなどの、その他の演算により融合しても良い。
【００７２】
また、本実施の形態において、ユーザ側の装置は、初期登録の処理と、初回（ｎ＝１）以降、ｎ回目の認証処理は、同一の第一情報処理装置で行ったが、初期登録の処理を行う装置と、初回（ｎ＝１）以降、ｎ回目の認証処理を行う装置が異なっていても良い。例えば

、初期登録の処理は、パーソナルコンピュータで行い、初回（ｎ＝１）以降、ｎ回目の認証処理は持ち運び可能な携帯端末（携帯電話を含む）で行うこと等が考えられる。かかる場合、初期登録処理を行ったパーソナルコンピュータに記録されている乱数Ｎ［１］を何らかの手段で携帯端末（携帯電話を含む）に記録しなければならない。かかる処理は、乱数Ｎ［１］のパーソナルコンピュータから携帯端末への送信により、記録することが考えられる。但し、処理は、他の処理でも良い。

【００７３】

また、本実施の形態における認証処理は、各種アプリケーションで応用可能である。例えば、本認証処理は、メールの送受信で利用され得る。また、本認証処理は、ホームページへのアクセス時の認証処理として利用され得る。各種アプリケーションで応用可能であるのは、他の実施の形態において説明する認証処理においても同様である。

【００７４】

さらに、本実施の形態における処理は、ソフトウェアで実現しても良い。そして、このソフトウェアをソフトウェアダウンロード等により配布しても良い。また、このソフトウェアをＣＤ－ＲＯＭなどの記録媒体に記録して流布しても良い。なお、このことは、本明細書における他の実施の形態においても該当する。

【００７５】

本実施の形態における処理は、ソフトウェアで実現する場合も、初期登録を行うステップと、認証を行うステップは分離されていても良い。また、上記第一情報処理装置で行う処理と、第二情報処理装置で行う処理は、プログラムとして分離されている。つまり、第一情報処理装置において初期登録を行うプログラムは、コンピュータに、乱数Ｎ［１］を生成するステップと、乱数Ｎ［１］を保存するステップと、保持しているパスワード情報「Ｓ」と乱数Ｎ［１］に一方向性変換関数Ｘを施して初回マスク情報「Ａ」を算出するステップと、保持している第一情報処理装置を識別する識別情報「ＩＤ」と前記算出した初回マスク情報「Ａ」を送信するステップを実行させるためのプログラムである。

【００７６】

また、第二情報処理装置において初期登録を行うプログラムは、コンピュータに、初回マスク情報「Ａ」と識別情報「ＩＤ」を受信するステップと、受信した初回マスク情報「Ａ」と識別情報「ＩＤ」を登録するステップを実行させるためのプログラムである。

【００７７】

また、第一情報処理装置において認証を行うプログラムは、コンピュータに、保持しているパスワード情報「Ｓ」と保存している乱数Ｎ［ｎ］に一方向性変換関数Ｘを施して今回マスク情報「Ａ」を算出するステップと、乱数Ｎ［Ｎ＋１］を発生するステップと、乱数Ｎ［Ｎ＋１］を保存するステップと、パスワード情報「Ｓ」と乱数Ｎ［Ｎ＋１］に一方向性変換関数Ｘを施して，今回の認証および次回送信時のマスクに用いる次回マスク情報「Ｃ」を生成するステップと、今回マスク情報「Ａ」にパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して得られるもうひとつの今回マスク情報「Ｂ」を算出する第一演算、または、次回マスク情報「Ｃ」にパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して得られるもうひとつの次回マスク情報「Ｄ」を算出する第二演算のどちらかの演算を行うステップと、今回マスク情報のいずれか、または次回マスク情報のいずれかに、ある定数を融合させたデータを新しくそれぞれの今回マスク情報あるいは次回マスク情報にし、次回マスク情報と今回マスク情報の排他的論理和をとったふたつのデータ「α」と「β」を前記識別情報「ＩＤ」とともに送付するステップを実行させるためのプログラムである。

【００７８】

さらに、第二報処理装置において認証を行うプログラムは、コンピュータに、「α」、「β」、および識別情報「ＩＤ」を受信するステップと、受信したデータ「α」と「β」から今回マスク情報を用いて次回マスク情報を取り出し、次回マスク情報同士あるいは次回マスク情報と今回マスク情報の関係を検証することにより被認証側の資格を認証するステップと、新しく次回マスク情報「Ｃ」を今回マスク情報「Ａ」として識別情報「ＩＤ」に

対応付けて登録するステップを実行させるためのプログラムである。

【００７９】

なお、上記のプログラムは、今回マスク情報「Ａ」、次回マスク情報「Ｃ」、今回マスク情報「Ｂ」あるいは次回マスク情報「Ｄ」を算出した後、今回マスク情報のいずれかには次回マスク情報のいずれかを、また次回マスク情報のいずれかには今回マスク情報のいずれかを、それぞれ定数として融合させたデータを、新しくそれぞれの今回マスク情報あるいは次回マスク情報にして、上記ステップをコンピュータに実行させるプログラムであっても良い。

【００８０】

また、上記プログラムは、乱数Ｎ［ｎ＋１］を発生するステップを行わずに、乱数Ｎ［ｎ＋１］として今回マスク情報「Ａ」を用いて今回の認証を行い、および乱数Ｎ［ｎ＋１］として今回マスク情報「Ａ」を用いて次回マスク情報「Ｃ」を生成するものであっても良い。

【００８１】

（実施の形態２）

【００８２】

本実施の形態における情報処理システム、つまり第一情報処理装置と第二情報処理装置の構成については、実施の形態１で説明した構成と概ね同じである。実施の形態１の情報処理システムと実施の形態２の情報処理システムでは、第一演算部や第二演算部の演算アルゴリズムが異なる。従って、本実施の形態において、情報処理システムの構成については説明しない。

【００８３】

以下、被認証者（ユーザ）側の第一情報処理装置が認証者（センタ）の第二情報処理装置に認証を受ける手順を、図２、および図４を用いて説明する。被認証者（ユーザ）の初期登録の手順を説明するフローは図２であり、既に説明した。

【００８４】

次に、初回（ｎ＝１）以降で、ｎ回目の認証時の処理について、図４のフローを用いて説明する。

【００８５】

被認証者の第一情報処理装置から送付されてきた「α」および「β」により，認証者側の第二情報処理装置における被認証者側の第一情報処理装置の認証が成立した後に以下の処理を行う。

【００８６】

認証者側の第二情報処理装置で、次回マスク情報「Ｃ」に一方向性変換「Ｆ」を施して得られるデータ「Ｄ」に、さらに一方向性変換「Ｈ」を施して得られるデータ「γ」を算出する。すなわち、第二情報処理装置は「γ←Ｈ（ＩＤ，Ｄ）」の演算をする。そして、認証者側の第二情報処理装置から被認証者側の第一情報処理装置へ「γ」を送付する。

【００８７】

被認証者側の第一情報処理装置において、次回マスク情報「Ｃ」に一方向性変換「Ｆ」を施して得られるデータ「Ｄ」に、一方向性変換「Ｈ」を施したデータ「Ｈ（ＩＤ，Ｄ）」を算出し、第二情報処理装置から受け取ったデータ「γ」と比較する。両データが一致すれば、第一情報処理装置は、認証者による認証が成功したことを確認する、または／および被認証者側の第一情報処理装置が認証者側の第二情報処理装置を相互に認証する。

【００８８】

以上、本実施の形態において、ユーザ側の装置（第一情報処理装置）での一方向性変換関数の適用回数が減少するがために、高速な認証処理が可能である。また、認証者側の装置（第二情報処理装置）で被認証者の装置（第一情報処理装置）から送付されてきた情報によって被認証者の装置の認証が完了した後、認証者側の装置から被認証者側の装置へ、今回認証に用いた情報を加工して生成した確認情報を送付することによって、被認証者側の装置において、認証者側の装置による認証が成功したことを確認するかあるいは被認証者

側の装置が認証者側の装置を相互に認証することを可能にしている。
【００８９】
なお、本実施の形態における処理は、ソフトウェアで実現しても良い。そして、このソフトウェアをソフトウェアダウンロード等により配布しても良い。また、このソフトウェアをＣＤ－ＲＯＭなどの記録媒体に記録して流布しても良い。
【００９０】
本実施の形態における処理は、ソフトウェアで実現する場合も、初期登録を行うステップと、認証を行うステップは分離されていても良い。また、上記第一情報処理装置で行う処理と、第二情報処理装置で行う処理は、プログラムとして分離されている。
【００９１】
つまり、第一情報処理装置において認証を行うプログラムは、コンピュータに、保持しているパスワード情報「Ｓ」と保存している乱数Ｎ［ｎ］に一方向性変換関数Ｘを施して今回マスク情報「Ａ」を算出するステップと、乱数Ｎ［Ｎ＋１］を発生するステップと、乱数Ｎ［Ｎ＋１］を保存するステップと、パスワード情報「Ｓ」と乱数Ｎ［Ｎ＋１］に一方向性変換関数Ｘを施して，今回の認証および次回送信時のマスクに用いる次回マスク情報「Ｃ」を生成するステップと、今回マスク情報「Ａ」にパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して得られるもうひとつの今回マスク情報「Ｂ」を算出する第一演算、または、次回マスク情報「Ｃ」にパスワード情報「Ｓ」を用いない一方向性変換関数Ｆを施して得られるもうひとつの次回マスク情報「Ｄ」を算出する第二演算のどちらかの演算を行うステップと、今回マスク情報のいずれか、または次回マスク情報のいずれかに、ある定数を融合させたデータを新しくそれぞれの今回マスク情報あるいは次回マスク情報にし、次回マスク情報と今回マスク情報の排他的論理和をとったふたつのデータ「α」と「β」を前記識別情報「ＩＤ」とともに送付するステップと、「γ」を第二報処理装置から受信するステップと、同じく次回マスク情報あるいは今回マスク情報のいずれかに一方向性変換関数Ｈを施して得られるデータを算出するステップと、受信したデータ「γ」と、算出したデータを比較して、一致するか否かを判断するステップを実行させるためのプログラムである。
【００９２】
また、第二情報処理装置において認証を行うプログラムは、コンピュータに、「α」、「β」、および識別情報「ＩＤ」を受信するステップと、受信したデータ「α」と「β」から今回マスク情報を用いて次回マスク情報を取り出し、次回マスク情報同士あるいは次回マスク情報と今回マスク情報の関係を検証することにより被認証側の資格を認証するステップと、新しく次回マスク情報「Ｃ」を今回マスク情報「Ａ」として識別情報「ＩＤ」に対応付けて登録するステップと、次回マスク情報あるいは今回マスク情報のいずれかに、さらにパスワード「Ｓ」を用いないある一方向性変換関数Ｈを施しデータ「γ」を算出するステップと、「γ」を送付するステップを実行させるためのプログラムである。
【００９３】
（実施の形態３）
【００９４】
本実施の形態において、上述した認証方法を開閉システムへ適用する態様について述べる。
【００９５】
本開閉システムは、図５に示すように、開閉装置５１と鍵５２を有する。鍵５２とは、電子的な鍵を言い、情報を格納できる記録媒体を有し、情報の送受信が可能なものを言う。鍵５２は、例えば、ＩＣカードや、データ送受信が可能な自動車の鍵や、その他データ送受信が可能なドアや金庫等の各種鍵である。
【００９６】
開閉装置５１は、開閉装置識別子格納部５１０１、鍵対応開閉装置秘密情報格納部５１０２、装置側鍵識別子格納部５１０３、装置側演算部５１０４、装置側情報送信部５１０５、装置側情報受信部５１０６を有する。

【００９７】
開閉装置識別子格納部５１０１は、開閉装置５１を識別する開閉装置識別子（以下、開閉装置識別子を記号で、適宜「ＩＤ」と言う。）を格納している。開閉装置識別子格納部５１０１は、ハードディスクなどの不揮発性の記録媒体でも、揮発性の記録媒体でも良い。
【００９８】
鍵対応開閉装置秘密情報格納部５１０２は、ある鍵に対応する秘密情報（パスワード）である鍵対応開閉装置秘密情報（以下、鍵対応開閉装置秘密情報を記号で、記号で「Ｓ」と言う。）を格納している。鍵対応開閉装置秘密情報格納部５１０２は、ハードディスクなどの不揮発性の記録媒体でも、揮発性の記録媒体でも良い。
【００９９】
鍵識別子格納部５１０３は、鍵を識別する情報である鍵識別子（以下、鍵識別子を記号で、適宜「Ｋ」と言う。）を格納している。鍵識別子格納部５１０３は、ハードディスクなどの不揮発性の記録媒体でも、揮発性の記録媒体でも良い。
【０１００】
開閉装置識別子格納部５１０１、鍵対応開閉装置秘密情報格納部５１０２、および鍵識別子格納部５１０３は、通常、一の記録媒体であるが、それぞれ異なる記録媒体でも良い。
【０１０１】
装置側演算部５１０４は、一方向性関数「Ｘ」または「Ｆ」、または排他的論理和の演算を行う。装置側演算部５１０４は、通常、ＣＰＵ、メモリ、およびソフトウェア等から実現され得る。つまり、一方向性関数「Ｘ」または「Ｆ」の演算式や、各種演算のアルゴリズムは、通常、ソフトウェアで実現され、当該ソフトウェアは、装置側演算部５１０４のメモリ（ＲＯＭ等）に格納されている。
【０１０２】
装置側情報送信部５１０５は、装置側演算部５１０４の演算結果の情報を鍵５２に送信する。装置側情報送信部５１０５は、無線または有線の通信手段、または放送手段で実現され得る。
【０１０３】
装置側情報受信部５１０６は、鍵５２から送信される情報を受信する。装置側情報受信部５１０６は、無線または有線の通信手段、または放送手段で実現され得る。
【０１０４】
鍵５２は、鍵側情報受信部５２０１、情報記録部５２０２、鍵側演算部５２０３、鍵側認証部５２０４、鍵側情報送信部５２０５を有する。
【０１０５】
鍵側情報受信部５２０１は、開閉装置５１から情報を受信する。鍵側情報受信部５２０１は、無線または有線の通信手段、または放送手段で実現され得る。
【０１０６】
情報記録部５２０２は、情報を記録する。情報記録部５２０２は、鍵側情報受信部５２０１が受信した情報等を記録（登録）する。情報記録部５２０２が情報を記録する先は、通常は、鍵５２が内部に保持する、不揮発性または揮発性の記録媒体である。但し、情報記録部５２０２が情報を記録する先は、鍵５２に外付けの、不揮発性または揮発性の記録媒体でも良い。
【０１０７】
鍵側演算部５２０３は、一方向性関数「Ｆ」や排他的論理和の演算を行う。鍵側演算部５２０３は、通常、ＣＰＵ、メモリ、およびソフトウェア等から実現され得る。つまり、一方向性関数「Ｘ」または「Ｆ」の演算式や、各種演算のアルゴリズムは、通常、ソフトウェアで実現され、当該ソフトウェアは、鍵側演算部５２０３のメモリ（ＲＯＭ等）に格納されている。
【０１０８】
鍵側認証部５２０４は、鍵側演算部５２０３の演算結果等に基づいて、認証を行う。鍵側認証部５２０４は、通常、ソフトウェアで実現され得るが、ハードウェア（専用回路）で

実現しても良い。

【０１０９】

鍵側情報送信部５２０５は、鍵５２から開閉装置５１に、鍵側演算部５２０３の演算結果の情報または／および鍵側認証部５２０４における認証結果に関する情報を送信する。鍵側情報送信部５２０５は、無線または有線の通信手段、または放送手段で実現され得る。

【０１１０】

鍵側鍵識別子格納部５２０５は、鍵を識別する情報である鍵識別子（以下、鍵識別子を記号で、適宜「Ｋ」と言う。）を格納している。鍵側鍵識別子格納部５２０５は、ハードディスクなどの不揮発性の記録媒体でも、揮発性の記録媒体でも良い。

【０１１１】

以下、開閉システムの動作について、図６、図７のフローを用いて説明する。

【０１１２】

図６、図７において、認証者を鍵、被認証者をドア等、鍵によって施錠される開閉装置と考える。なお、パスワード情報「Ｓ」は、個々の鍵に対応した開閉装置側の秘密情報であって、毎回入力するのではなく登録されているものとする。

【０１１３】

以下、図６のフロー図を用いて、初期登録（初期登録時（ｎ＝０））の手順を説明する。

【０１１４】

まず、開閉装置５１の装置側演算部５１０４は、鍵識別子「Ｋ」に対応する乱数Ｎ［１］を生成し、保存する。次に、装置側演算部５１０４は、開閉装置識別子格納部５１０１から開閉装置識別子「ＩＤ」を取り出す。そして、装置側演算部５１０４は、鍵対応開閉装置秘密情報格納部５１０２から鍵対応の秘密情報「Ｓ」を取り出す。また、装置側演算部５１０４は、装置側鍵識別子格納部５１０３から鍵識別子「Ｋ」を取り出す。

【０１１５】

そして、装置側演算部５１０４は、「Ａ←Ｘ（ＩＤ　ＸＯＲ　Ｋ，Ｓ　ＸＯＲＮ［１］）」の演算を行い、初回マスク情報「Ａ」を算出する。なお、乱数発生関数、一方向性関数「Ｘ」、排他的論理和の演算式等は装置側演算部５１０４に格納されている、とする。

【０１１６】

そして、装置側情報送信部５１０５は、「ＩＤ」「Ｋ」「Ａ」を鍵５２に送信する。

【０１１７】

次に、鍵５２の鍵側情報受信部５２０１は、「ＩＤ」「Ｋ」「Ａ」を受信する。そして、情報記録部５２０２は、開閉装置識別子「ＩＤ」とともに、初回の認証に用いるマスク情報「Ａ」を登録する。

【０１１８】

次に、図７のフロー図を用いて、鍵の開閉時（ｎ回目の開閉，ｎ≧１）の認証手順を説明する。まず，鍵５２から鍵識別子「Ｋ」を識別子「ＩＤ」の開閉装置５１に送付する。

【０１１９】

次に、開閉装置５１の鍵側情報受信部５２０１は、鍵識別子「Ｋ」を識別子「ＩＤ」を受信する。そして、装置側演算部５１０４は、鍵側情報受信部５２０１が受信した鍵識別子「Ｋ」を識別子「ＩＤ」を取得する。また、装置側演算部５１０４は、鍵対応開閉装置秘密情報格納部５１０２に格納されているパスワード情報「Ｓ」を取得する。

【０１２０】

そして、装置側演算部５１０４は、鍵識別子「Ｋ」に対応付けて保存している乱数Ｎ［ｎ］を取り出す。

【０１２１】

そして、装置側演算部５１０４は、上記取得した「ＩＤ」「Ｋ」「Ｓ」「Ｎ［ｎ］」を用いて、「Ａ←Ｘ（ＩＤ　ＸＯＲ　Ｋ，　Ｓ　ＸＯＲ　Ｎ［ｎ］）」の演算を行う。装置側演算部５１０４は、以上の処理により、「Ａ」を算出する。

【０１２２】

そして、装置側演算部５１０４は、続いて、新しい乱数Ｎ［ｎ＋１］を発生させるか、「

Ａ」をＮ［ｎ＋１］つする。そして、装置側演算部５１０４は、乱数Ｎ［ｎ＋１］（「Ａ」の場合もあり得る。）は、鍵識別子「Ｋ」に対応付けて開閉装置５１に保存する。なお、「Ａ」をＮ［ｎ＋１］とする場合は、開閉装置５１には、乱数発生機構が不要である。

【０１２３】

そして、装置側演算部５１０４は、「Ｃ←Ｘ（ＩＤ　ＸＯＲ　Ｋ，　Ｓ　ＸＯＲ　Ｎ［ｎ＋１］）」、「Ｄ←Ｆ（ＩＤ　ＸＯＲ　Ｋ，Ｃ）」の演算を行い、「Ｃ」および「Ｄ」を算出する。

【０１２４】

次に、装置側演算部５１０４は、算出した「Ａ」、「Ｃ」、「Ｄ」を用いて、「α←Ｄ　ＸＯＲ　（Ａ＋Ｄ）」、「β←Ｃ　ＸＯＲ　Ａ」の演算を行う。

【０１２５】

次に、装置側情報送信部５１０５は、「α」および「β」を「ＩＤ」とともに鍵５２に送付する。

【０１２６】

次に、鍵５２における認証処理を行う。

【０１２７】

鍵側情報受信部５２０１は、「α」「β」「ＩＤ」を受信する。そして、鍵側演算部５２０３は、鍵側情報受信部５２０１が受信した「α」「β」「ＩＤ」を取得する。次に、鍵側演算部５２０３は、識別子「ＩＤ」を有する開閉装置対応に保存してある今回マスク情報「Ａ」を取り出す。そして、鍵側演算部５２０３は、「Ｃ←β　ＸＯＲ　Ａ」の演算を行い、「Ｃ」を算出する。次に、鍵側演算部５２０３は、「Ｆ（ＩＤ　ＸＯＲ　Ｋ，Ｃ）＋Ａ」の演算を行う。次に、鍵側演算部５２０３は、「α　ＸＯＲ　（Ｆ（ＩＤ　ＸＯＲ　Ｋ，Ｃ）＋Ａ）」の演算を行う。

【０１２８】

次に、鍵側認証部５２０４は、上記「α　ＸＯＲ　（Ｆ（ＩＤ　ＸＯＲ　Ｋ，Ｃ）＋Ａ）」の演算結果が、「Ｄ」と一致するか否かを判断する。鍵側認証部５２０４は、両データが一致すれば開閉装置５１の正当性を認証し、一致しなければ開閉装置５１の認証は不成立、とする。認証が成立すれば、情報記録部５２０２は、開閉装置識別子「ＩＤ」に対応するマスク情報として「Ｃ」を登録する。

【０１２９】

さらに、鍵５２は、例えば，一方向性変換「Ｈ」として、次回マスク情報「Ｃ」の一方向性変換に用いた「Ｆ」を用いる場合、「γ←Ｆ（ＩＤ　ＸＯＲ　Ｋ，Ｄ）」により「γ」を算出する。そして、鍵側情報送信部５２０５は、「γ」を開閉装置５１に送付する。この「γ」が開閉装置５１を開閉するための鍵になる。

【０１３０】

次に、開閉装置５１では、上記と同じ手順で、次回マスク情報「Ｃ」に一方向性変換「Ｆ」を施して得られるデータ「Ｄ」から「γ」を算出し、鍵５２から受信した「γ」と比較する。比較の結果、両者が一致すれば開閉装置５１の開閉を行う。

【０１３１】

なお、開閉装置を閉じるオペレーションの場合、鍵自身が開閉装置の外にあることを検出する機構は必要である。

【０１３２】

以下、本開閉システムの具体的な適用例について説明する。

【０１３３】

本発明における開閉システムの適用例としては、専用の鍵がある。また、本開閉システムは、開閉装置識別子「ＩＤ」と鍵識別子「Ｋ」を設けているため、鍵として専用の鍵のみならず、汎用の鍵として利用できる。つまり、ひとつの鍵が、複数の開閉装置に対応する鍵機能を持つことができる。そして、携帯電話やＰＤＡを上記の認証機能を有する鍵としても良い。また、メモリ機能に加えて上記説明した認証機能をもつ次世代のＩＣカードを上記の認証機能を有する鍵としても良い。携帯電話やＰＤＡやＩＣカードは普及しており

、かつ処理能力が比較的低いので、本実施の形態における資格認証方法は有効である。

【０１３４】

また、本実施の形態における資格認証方法を用いた開閉装置においては、複数の鍵識別子に対応する鍵、すなわちスペア鍵を持つことができる。

【０１３５】

また、通常の鍵形状の装置に本実施の形態において説明した認証機能を組み込む場合、一方向性変換処理を簡易に実現することによってコストを削減することができる。つまり、一方向性変換関数に変わって簡易な処理を行う演算である簡易演算を適用するのである。簡易演算の例は、排他的論理和（ＸＯＲ）がある。具体的には以下のような処理を行う。例えば、一方向性変換を適用するデータの左右半分のデータを「Ｌ」、「Ｒ」とし、一方向性変換Ｆを、「Ｌ←Ｌ　ＸＯＲＲ」、「Ｒ←Ｌ　ＸＯＲ　Ｒ」とする。

【０１３６】

さらに、「Ｌ」の左右半分のデータを「Ｌ１」「Ｌ２」、「Ｒ」の左右半分のデータを「Ｒ１」「Ｒ２」とし、一方向性変換Ｈを「Ｌ１←Ｌ１　ＸＯＲ　Ｌ２」、「Ｌ２←Ｌ１　ＸＯＲ　Ｌ２」、「Ｒ１←Ｒ１　ＸＯＲ　Ｒ２」、「Ｒ２←Ｒ１　ＸＯＲ　Ｒ２」とすれば、通常用いる共通鍵暗号方式による一方向性変換に代わって、排他的論理和のみで鍵の処理を構成できるため、鍵のコストを大幅に削減することができる。

【０１３７】

以上、本実施の形態によれば、相互認証方法を開閉装置と鍵を有する開閉システムに応用する（つまり、被認証者側の装置を開閉装置に、認証者の装置を鍵にする。）ことによって、電子的に安全に鍵の開閉を行うシステムを構築することができる。

【０１３８】

なお、本実施の形態において、第一情報処理装置を開閉装置、第二情報処理装置を鍵にした開閉システムを説明したが、逆でも良い。つまり、第一情報処理装置を鍵、第二情報処理装置を開閉装置にしても良い。

【発明の効果】

本発明の認証方法によれば、認証処理において、処理負荷の大きい一方向性変換の適用回数を少なくすることができ、認証者側および被認証者側の処理を大幅に高速化できる。

【図面の簡単な説明】

【図１】実施の形態１における情報処理システムの構成を示すブロック図

【図２】実施の形態１における初期登録手順を説明するフロー図

【図３】実施の形態１における認証手順を説明するフロー図

【図４】実施の形態２における認証手順を説明するフロー図

【図５】実施の形態３における開閉システムの構成を示すブロック図

【図６】実施の形態３における初期登録手順を説明するフロー図

【図７】実施の形態３における認証手順を説明するフロー図

【図８】従来技術における初期登録手順を説明するフロー図

【図９】従来技術における認証手順を説明するフロー図

【符号の説明】

１１　第一情報処理装置

１２　第二情報処理装置

５１　開閉装置

５２　鍵

１１０１　ユーザ識別子格納部

１１０２　パスワード格納部

１１０３　第一演算部

１１０４　第一送信部

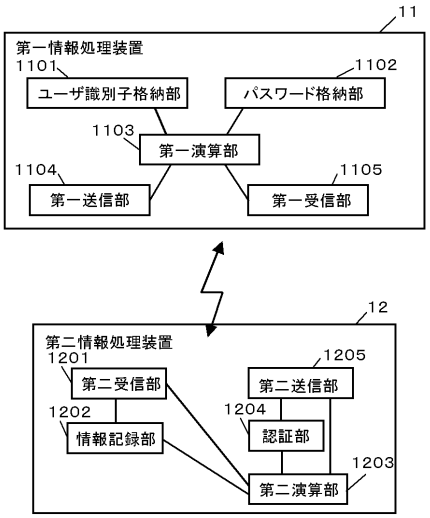
１１０５　第一受信部

１２０１　第二受信部

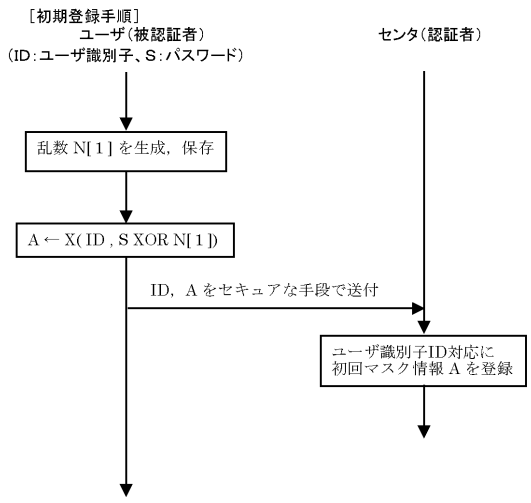
１２０２　情報記録部

１２０３　第二演算部
１２０４　認証部
１２０５　第二送信部
５１０１　開閉装置識別子格納部
５１０２　鍵対応開閉装置秘密情報格納部
５１０３　鍵識別子格納部
５１０３　装置側鍵識別子格納部
５１０４　装置側演算部
５１０５　装置側情報送信部
５１０６　装置側情報受信部
５２０１　鍵側情報受信部
５２０２　情報記録部
５２０３　鍵側演算部
５２０４　鍵側認証部
５２０５　鍵側鍵識別子格納部
５２０５　鍵側情報送信部

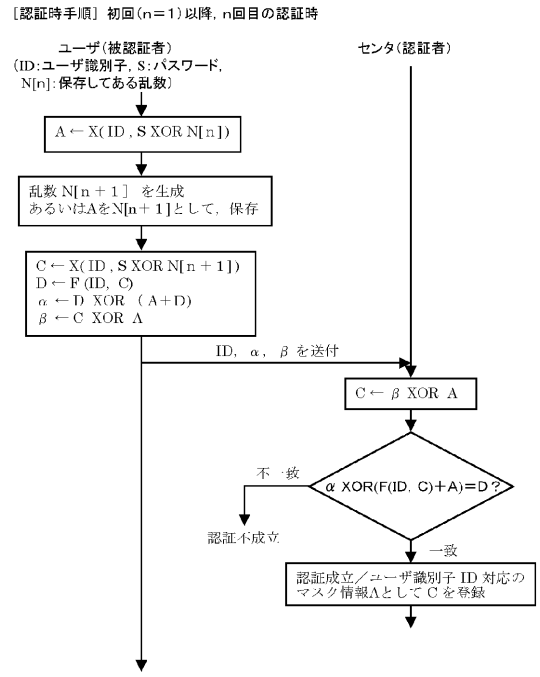
【図１】



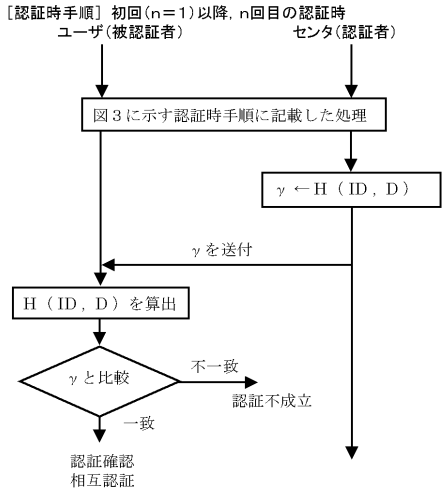
【図２】



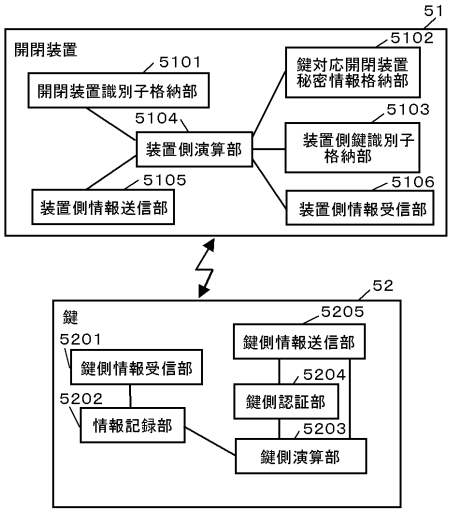
【図３】


［認証時手順］ 初回（n＝1）以降，n回目の認証時
ユーザ（被認証者）
（ID：ユーザ識別子，S：パスワード，
N[n]：保存してある乱数）
センタ（認証者）
A ← X(ID , S XOR N[n])
乱数 N[n ＋ 1] を生成
あるいはAをN[n＋1]として，保存
C ← X(ID , S XOR N[n ＋ 1])
D ← F (ID, C)
α ← D XOR （A＋D)
β ← C XOR A
ID, α, β を送付
C ← β XOR A
α XOR(F(ID, C)＋A)=D？
不一致
認証不成立
一致
認証成立／ユーザ識別子 ID 対応の
マスク情報Aとして C を登録

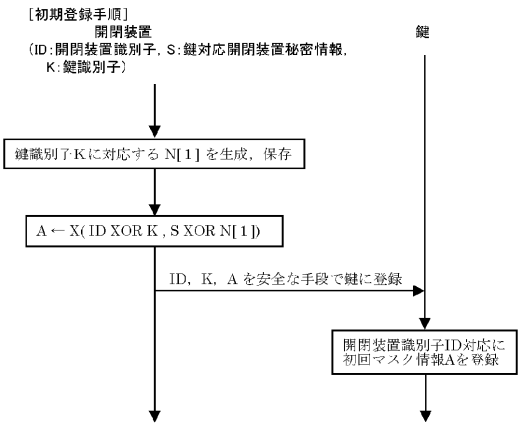
【図４】


［認証時手順］ 初回（n＝1）以降，n回目の認証時
ユーザ（被認証者）
センタ（認証者）
図３に示す認証時手順に記載した処理
γ ← H （ ID , D ）
γを送付
H （ ID , D ）を算出
γと比較
不一致
認証不成立
一致
認証確認
相互認証

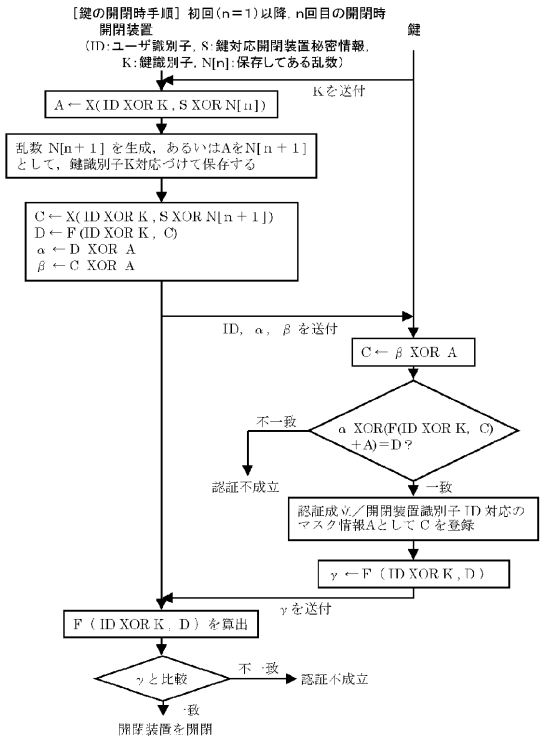
【図５】


51
開閉装置
5101
開閉装置識別子格納部
5102
鍵対応開閉装置
秘密情報格納部
5103
装置側鍵識別子
格納部
5104
装置側演算部
5105
装置側情報送信部
5106
装置側情報受信部
52
鍵
5201
鍵側情報受信部
5202
情報記録部
5205
鍵側情報送信部
5204
鍵側認証部
5203
鍵側演算部

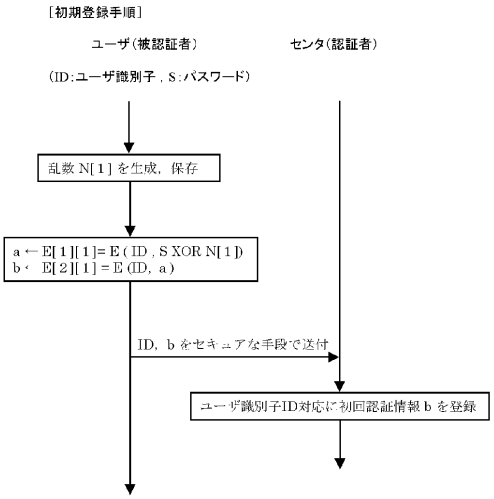
【図６】


［初期登録手順］
開閉装置
（ID：開閉装置識別子，S：鍵対応開閉装置秘密情報，
K：鍵識別子）
鍵
鍵識別子Kに対応する N[1] を生成，保存
A ← X(ID XOR K , S XOR N[1])
ID，K，A を安全な手段で鍵に登録
開閉装置識別子ID対応に
初回マスク情報Aを登録

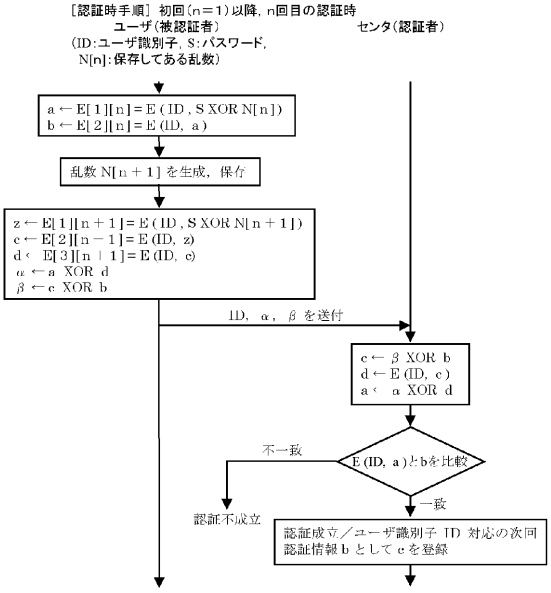
【図７】


［鍵の開閉時手順］初回（n＝1）以降，n回目の開閉時
開閉装置
（ID：ユーザ識別子，S：鍵対応開閉装置秘密情報，
K：鍵識別子，N[n]：保存してある乱数）
鍵
Kを送付
A ← X(ID XOR K , S XOR N[n])
乱数 N[n＋1] を生成，あるいはAをN[n ＋ 1]
として，鍵識別子K対応づけて保存する
C ← X(ID XOR K , S XOR N[n ＋ 1])
D ← F (ID XOR K , C)
α ← D XOR A
β ← C XOR A
ID， α， β を送付
C ← β XOR A
不一致
α XOR(F(ID XOR K, C)
＋A)＝D ?
認証不成立
一致
認証成立／開閉装置識別子 ID 対応の
マスク情報Aとして C を登録
γ ← F （ ID XOR K , D ）
γを送付
F （ ID XOR K , D ） を算出
γと比較
不一致
認証不成立
一致
開閉装置を開閉

【図８】


［初期登録手順］
ユーザ（被認証者）
センタ（認証者）
（ID：ユーザ識別子，S：パスワード）
乱数 N[1] を生成，保存
a ← E[1][1]= E (ID , S XOR N[1])
b ← E[2][1] = E (ID, a)
ID，b をセキュアな手段で送付
ユーザ識別子ID対応に初回認証情報 b を登録

【図９】


［認証時手順］初回（n＝1）以降，n回目の認証時
ユーザ（被認証者）
センタ（認証者）
（ID：ユーザ識別子，S：パスワード，
N[n]：保存してある乱数）
a ← E[1][n] = E (ID , S XOR N[n])
b ← E[2][n] = E (ID, a)
乱数 N[n ＋ 1] を生成，保存
z ← E[1][n ＋ 1] = E (ID , S XOR N[n ＋ 1])
c ← E[2][n － 1] = E (ID, z)
d ← E[3][n － 1] = E (ID, c)
α ← a XOR d
β ← c XOR b
ID， α， β を送付
c ← β XOR b
d ← E (ID, c)
a ← α XOR d
不一致
E (ID, a)とbを比較
一致
認証不成立
認証成立／ユーザ識別子 ID 対応の次回
認証情報 b として c を登録

フロントページの続き

(56)参考文献　特開２００１－０３６５２２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
G06F15/00