

(51) Int.Cl. ⁷	識別記号	F I	テ-マコード [*] (参考)
H04L 9/32		E05B 49/00	K 2E250
E05B 49/00		G06F 15/00	F 5B085
G06F 15/00	330	H04L 9/00	C 5J104

審査請求 未請求 請求項の数10 O L (全15頁)

(21)出願番号 特願2002 - 70326(P 2002 - 70326)

(22)出願日 平成14年 3月14日(2002.3.14)

(71)出願人 598125855

清水 明宏

高知県高知市知寄町二丁目 3 番地16号

(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

(74)代理人 100115749

弁理士 谷川 英和

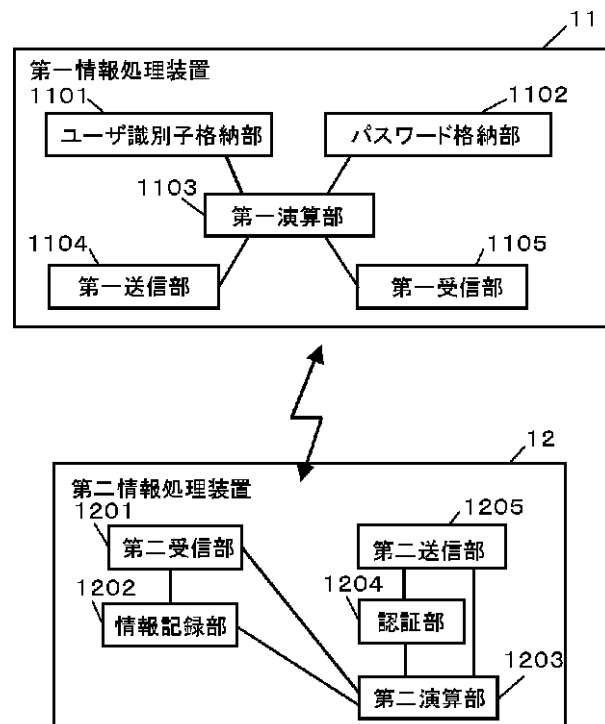
最終頁に続く

(54)【発明の名称】資格認証方法

(57)【要約】

【課題】 資格認証方法において、ユーザ側の装置での処理負担の大きい一方向性変換関数の適用回数は5回で高速な処理が困難であった。

【解決手段】 被認証装置がパスワード情報「S」と乱数N[n]に一方向性変換関数Xを施して今回マスク情報「A」を算出し、発生させた乱数N[n+1]と「S」に一方向性変換関数Xを施して次回マスク情報「C」を生成し、「C」に「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、今回マスク情報のいずれか等に定数を融合させたデータをそれぞれの今回マスク情報又は次回マスク情報とし、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二つのデータ「」送付し、認証装置が受信した「」「」から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。



【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、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、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」に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」を登録するステップを具備し、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」に対応に保存している乱数 $N[n]$ 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、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 」を算出し、当該算出した「 α 」と「 β 」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、第二情報処理装置において、前記「 α 」、前記「 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資格認証方法。

【請求項 2】 前記認証ステップにおいて、前記第二情報処理装置において、前記識別情報「ID」に対応に受信した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、前記「 γ 」を前記第一情報処理装置に送信するステップをさらに具備し、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、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、前記第二情報処理装置から受信したデータ「 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判断ステップ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」を保持している状態において、前記鍵において、前記鍵識別情報「K」を開閉装置に送信するステップをさらに具備し、前記開閉装置において、前記鍵から鍵識別情報「K」を受信するステップをさらに具備し、前記データ「 α 」、「 β 」の算出のために前記鍵識別情報「K」を利用し、前記開閉装置において、前記判断ステップにおける判断が、一致するとの判断である場合に、前記開閉装置の施錠を開閉するステップをさらに具備する請求項 2 記載の資格認証方法。

【請求項 4】 今回マスク情報のいずれかに融合させる前記定数は次回マスク情報であり、また、次回マスク情報のいずれかに融合させる前記定数は今回マスク情報であることを特徴とする請求項 1 から請求項 3 いずれか記載の資格認証方法。

【請求項 5】 前記認証ステップにおいて、前記乱数 $N[n+1]$ を発生するステップを行わずに、前記乱数 $N[n+1]$ として今回マスク情報「A」を用いて今回の認証を行い、および前記乱数 $N[n+1]$ として今回マスク情報「A」を用いて次回マスク情報「C」を生成することを特徴とする請求項 1 から請求項 4 いずれか記載の資格認証方法。

【請求項 6】 請求項 1 または請求項 2 または請求項 4 または請求項 5 いずれか記載の資格認証方法を実現する被認証側の装置である情報処理装置。

【請求項 7】 請求項 1 または請求項 2 または請求項 4 または請求項 5 いずれか記載の資格認証方法を実現する認証側の装置である情報処理装置。

【請求項 8】 請求項 1 または請求項 2 または請求項 4 または請求項 5 いずれか記載の資格認証方法の前記認証ステップを実現する被認証側の装置である情報処理装置。

【請求項 9】 請求項 3 から請求項 5 いずれか記載の資

格認証方法を実現する被認証側の装置である開閉装置。

【請求項10】 請求項3から請求項5いずれか記載の資格認証方法を実現する認証側の装置である鍵。

【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】「 E 」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、「 $a XOR d$ 」、「 $c XOR b$ 」の演算を行い、「 a 」と「 c 」を算出する。そして、ユーザ側の装置は、「 a 」および「 c 」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、「 a 」と「 c 」と「 ID 」を受け取る。そして、センタ側の装置は、受け取った「 a 」と「 c 」に対して、以下の3つの演算を行う。①「 $c XOR b$ 」②「 $d = E(ID, c)$ 」 ③「 $a XOR d$ 」

【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

10

20

30

40

50

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」の一方方向性変換の元のデータ「a」には次回認証情報「c」に一方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、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」に対応に規定するパスワード情報「S」と乱数N[1]に一方方向性変換関数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「」と「」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、「」、前記「」、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「」と「」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」を乱数として用いた次回マスク情報「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】「 \square 」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、「 $X[n] = X(ID, S \text{ XOR } N[n])$ 」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「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、一的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は一部または、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、「 $A = X(ID, S \oplus N[1])$ 」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、「 $A = X(ID, S \oplus N[n])$ 」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。「 $C = X(ID, S \oplus N[n+1])$ 」、「 $D = F(ID, C)$ 」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。「 $D \oplus (A + D)$ 」、「 $C \oplus A$ 」の演算により、「 E 」と「 F 」を算出する。

【0055】そして、第一送信部1104は、「 E 」と「 F 」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、「 E 」と「 F 」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「 E 」と「 F 」と、今回マスク情報「A」を用いて、「 $C = (D \oplus (A + D)) \oplus A$ 」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「 $D = F(ID, C)$ 」で「D」を算出する。認

証部 1204 は、 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 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 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「 」と「 」から今回マスク情報を用いて 10 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

- (1) 「 D XOR (A + C)」、「 C XOR A」
- (2) 「 D XOR A」、「 C XOR (A + D)」
- (3) 「 D XOR A」、「 C XOR (A + C)」
- (4) 「 (A + D) XOR A」、「 C XOR A」
- (5) 「 D XOR A」、「 (A + C) XOR A」
- (6) 「 (B + C) XOR B」、「 C XOR A」
- (7) 「 (A + C) XOR B」、「 C XOR A」
- (8) 「 C XOR B」、「 (B + C) XOR A」
- (9) 「 C XOR B」、「 (A + C) XOR A」
- (10) 「 C XOR (B + C)」、「 C XOR A」
- (11) 「 C XOR B」、「 C XOR (A + C)」

【0067】さらに、任意の定数「V」を用いて、 は、以下の演算により算出しても良い。

- (12) 「 D XOR (A + V)」、「 C XOR A」
- (13) 「 D XOR A」、「 C XOR (A + V)」
- (14) 「 (V + D) XOR A」、「 C XOR A」
- (15) 「 D XOR A」、「 (V + C) XOR A」
- (16) 「 (V + C) XOR B」、「 C XOR A」
- (17) 「 C XOR B」、「 (V + C) XOR A」
- (18) 「 C XOR (B + V)」、「 C XOR A」
- (19) 「 C XOR B」、「 C XOR (A + V)」

【0069】上記の 19 の演算により「 」や「 」を算出して、当該「 」や「 」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、「 」と「 」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 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

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」を乱数として使い、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、 の算出は、「 D XOR (A + D)」、「 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】

【0068】

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。

【 0 0 7 2 】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。

【 0 0 7 3 】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。

【 0 0 7 4 】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。

【 0 0 7 5 】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。

【 0 0 7 6 】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。

【 0 0 7 7 】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「 」と「 」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。

【 0 0 7 8 】さらに、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、「 」、「 」、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「 」と「 」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。

【 0 0 7 9 】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。

【 0 0 8 0 】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。

【 0 0 8 1 】 (実施の形態 2)

【 0 0 8 2 】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

10

20

30

40

50

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「 S 」および「 N 」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 」に一方方向性変換「 F 」を施して得られるデータ「 D 」に、さらに一方方向性変換「 H 」を施して得られるデータ「 $H(ID, D)$ 」を算出する。すなわち、第二情報処理装置は「 $H(ID, D)$ 」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「 $H(ID, D)$ 」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 」に一方方向性変換「 F 」を施して得られるデータ「 D 」に、一方方向性変換「 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「 $H(ID, D)$ 」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「 B 」と「 D 」を前記識別情報「 ID 」とともに送付するステップと、「 B 」を第二情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「 B 」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、「 S 」、「 N 」、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「 B 」と「 D 」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者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 」を用いない一方方向性変換関数 H を施しデータ「 B 」を算出するステップと、「 B 」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と言う。鍵52は、例えば、ICカードや、データ送受信が可能なる自動車の鍵や、その他データ送受信が可能なる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5

101、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、「AX(ID XOR K, S XOR N[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

10

20

30

40

50

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、「 $A \times (ID \text{ XOR } K, S \text{ XOR } N[n])$ 」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、「 $C \times (ID \text{ XOR } K, S \text{ XOR } N[n+1])$ 」、「 $D \times F(ID \text{ XOR } K, C)$ 」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、「 $D \text{ XOR } (A+D)$ 」、「 $C \text{ XOR } A$ 」の演算を行う。

【0125】次に、装置側情報送信部 5105 は、「」および「」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、「」「」「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「」「」「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、「 $C \text{ XOR } A$ 」の演算を行い、「C」を算出する。次に、鍵側演算部 5203 は、「 $F(ID \text{ XOR } K, C) + A$ 」の演算を行う。次に、鍵側演算部 5203 は、「 $\text{XOR} (F(ID \text{ XOR } K, C) + A)$ 」の演算を行う。

【0128】次に、鍵側認証部 5204 は、上記「 $\text{XOR} (F(ID \text{ XOR } K, C) + A)$ 」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、「 $F(ID \text{ XOR } K, D)$ 」により「」を算出する。そして、鍵側情報送信部 5205 は、「」を開閉装置 51 に送付する。この「」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「」を算出し、鍵 52 から受信した「」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 XOR R」、「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

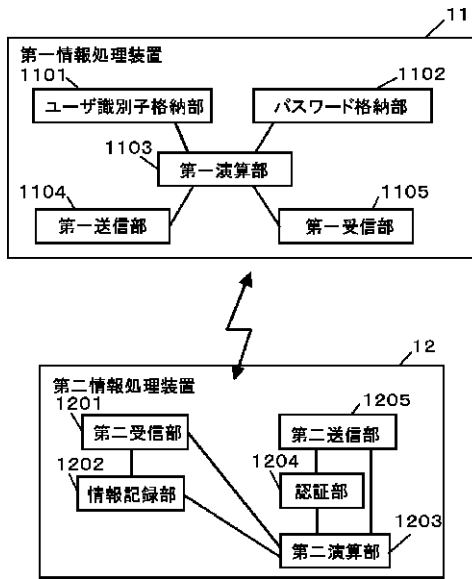
【図8】従来技術における初期登録手順を説明するフロー図

【図9】従来技術における認証手順を説明するフロー図

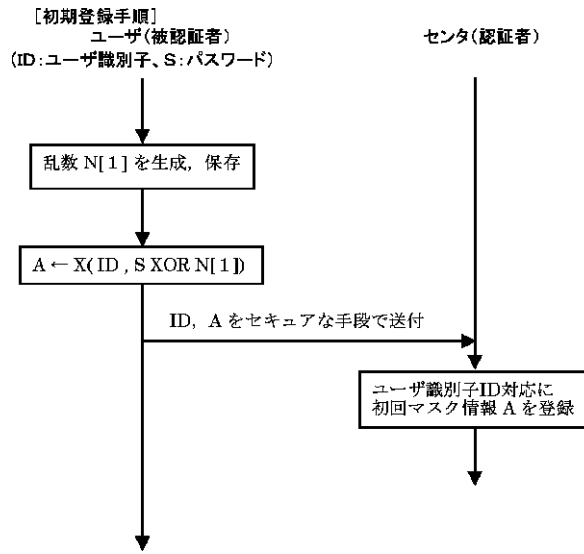
【符号の説明】

- 10 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
- 20 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

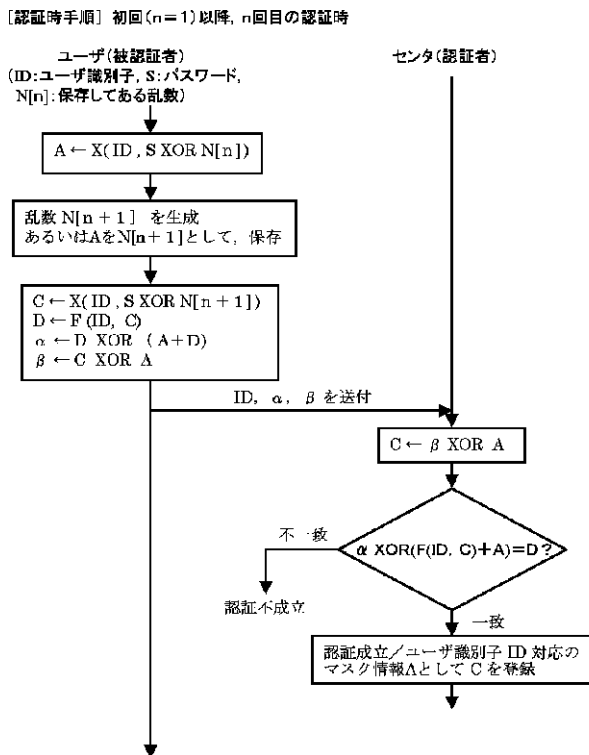
【 図 1 】



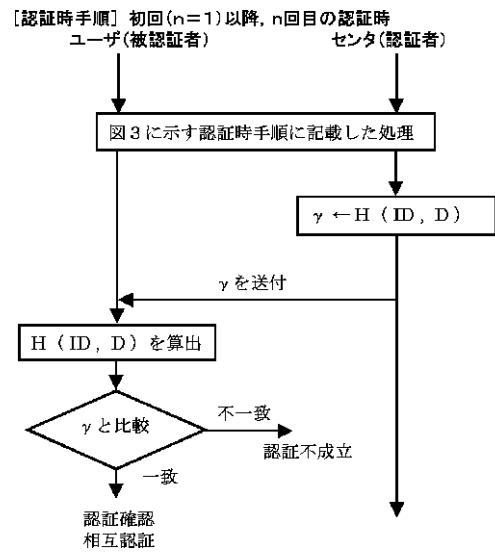
【 図 2 】



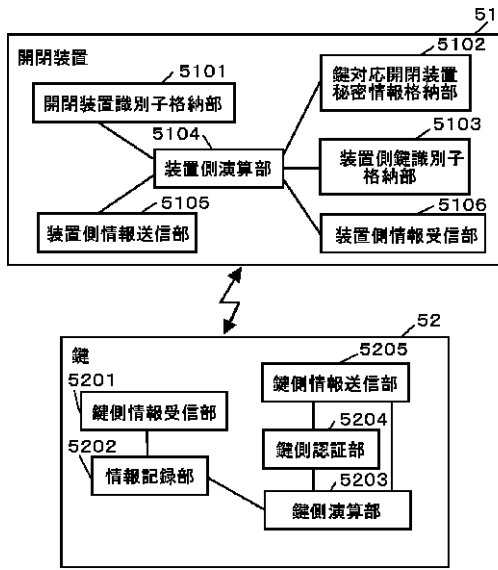
【 図 3 】



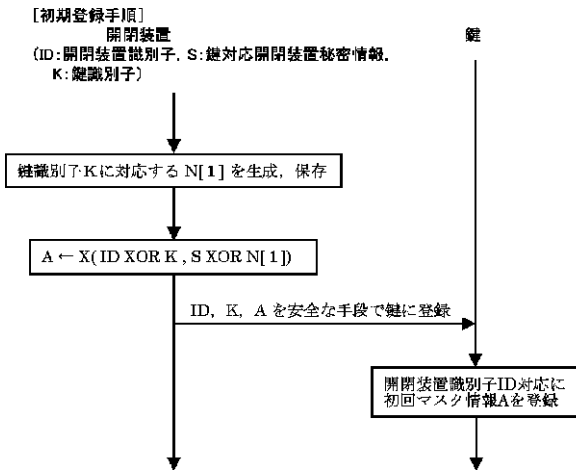
【 図 4 】



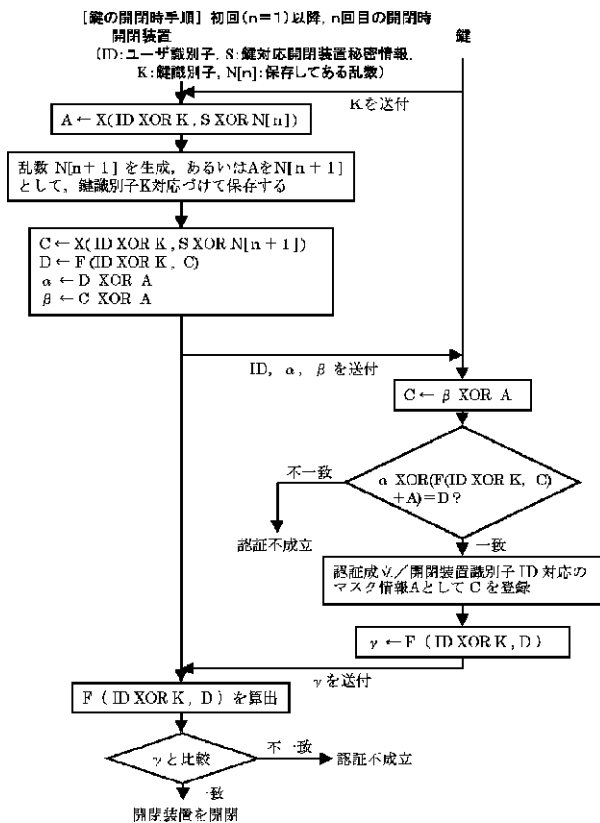
【図 5】



【図 6】



【図 7】



【図 8】

