

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4941918号
(P4941918)

(45) 発行日 平成24年5月30日 (2012.5.30)

(24) 登録日 平成24年3月9日 (2012.3.9)

(51) Int.Cl.	F I
H04L 9/08 (2006.01)	H04L 9/00 601B
H04L 9/32 (2006.01)	H04L 9/00 601E
	H04L 9/00 675Z

請求項の数 7 (全 12 頁)

(21) 出願番号	特願平11-324712	(73) 特許権者	595032185
(22) 出願日	平成11年11月15日 (1999.11.15)		女屋 達廣
(65) 公開番号	特開2001-144745 (P2001-144745A)		東京都町田市高ヶ坂1646-25
(43) 公開日	平成13年5月25日 (2001.5.25)	(74) 代理人	100075306
審査請求日	平成18年9月1日 (2006.9.1)		弁理士 菅野 中
審判番号	不服2010-407 (P2010-407/J1)	(72) 発明者	女屋 達廣
審判請求日	平成22年1月8日 (2010.1.8)		東京都町田市原町田3-7-10 ハイコ ート矢口301
		合議体	
		審判長	赤川 誠一
		審判官	石井 茂和
		審判官	清木 泰

(54) 【発明の名称】 電子認証システム

(57) 【特許請求の範囲】

【請求項1】

第1の利用者の端末と、第2の利用者の端末と、第1の利用者の端末と第2の利用者の端末との間で使用する通信用鍵を、第1の利用者の端末と第2の利用者の端末の間での D i f f i e - H e l l m a n 型公開鍵配送法で共有された共有鍵を用いて、第1の利用者の端末にて暗号化された通信用鍵を一時格納し、該一時格納された暗号化された通信用鍵を、第2の利用者の端末に送信する鍵センターとからなる電子認証システムにおいて、

通信用鍵を鍵センターに送信する前に、第1の利用者の端末、第2の利用者の端末間で、D i f f i e - H e l l m a n 型公開鍵配送法を用いて鍵共有が行われ、

第1の利用者の端末の使用者及び第2の利用者の端末の使用者の個人用認証情報の鍵センターへの登録は通信用鍵を鍵センターに送信する前に行われ、

第1の利用者の端末から、鍵センターを介して第2の利用者の端末へ通信用鍵を送信する際に、第1の利用者の端末は、通信用鍵を、前記共有鍵を用いて暗号化して前記鍵センターに送信し、

鍵センターにおいて、登録された個人用認証情報を用いて前記第1の利用者の端末である送信側の認証が行われ、当該認証がとった場合に、暗号化された通信用鍵を前記鍵センターに一時格納し、

前記鍵センターは、登録された個人用認証情報を用いて、前記第2の利用者の端末である受信側の認証を行い、当該認証がとった場合に、前記暗号化された通信用鍵を、前記第2の利用者の端末へ送信して格納し、

10

20

前記第2の利用者の端末は、前記共有鍵を用いて前記暗号化された通信用鍵を復号し、
前記第1の利用者の端末は、通信文を前記通信用鍵を用いて暗号化して、直接、前記第
2の利用者の端末に送信し、
前記第2の利用者の端末は、受信した通信文を前記復号した通信用鍵を用いて復号する
電子認証システム。

【請求項2】

前記個人用認証情報は、各利用者が各自生成したそれぞれの利用者に固有の情報として
、乱数および、指紋、目の光彩をデジタル情報に変換したものであり、 前記鍵センター
は、提示された登録済みの前記個人用認証情報をもって、暗号化された通信用鍵を送信し
てきた利用者およびその暗号化された通信用鍵を送信すべき利用者本人を特定するもので
あることを特徴とする請求項1に記載の電子認証システム。

10

【請求項3】

前記各利用者の端末と前記鍵センター間の通信で送信される少なくとも前記個人用認証
情報は、各利用者の端末と鍵センター間のD i f f i e - H e l l m a n型公開鍵配送法
により共有した共有鍵を用いて暗号化されて送信されるものであることを特徴とする請求
項1に記載の電子認証システム。

【請求項4】

各利用者は、前記各利用者の端末で個人用認証情報を鍵センターにオンラインで登録し
た後、通信用鍵の送受信時および個人用認証情報の更新時以外に鍵センターへのアクセス
は不要であることを特徴とする請求項1に記載の電子認証システム。

20

【請求項5】

前記第2の利用者の端末は、前記第1の利用者の端末から前記鍵センターを介して送信
された暗号化された通信用鍵を受信した後、その暗号化された通信用鍵を前記第1の利用
者の端末、第2の利用者の端末間で、D i f f i e - H e l l m a n型公開鍵配送法によ
り共有した共有鍵を用いて復号して格納し、その復号された通信用鍵が変更されるまでは
、その復号された通信用鍵を用いて第1の利用者から送信されてきた暗号化された通信文
を復号化することを特徴とする請求項1に記載の電子認証システム。

【請求項6】

他人が別の個人用認証情報を鍵センターに登録して第1の利用者になりすました場合に
おいて、前記第1の利用者の端末は、前記認証登録手続きまたは前記通信用鍵の送受信手
続きに際し、鍵センターにアクセスしたときに、鍵センターは第1の利用者の個人用認証
情報として既に登録されている個人用認証情報とは異なるとして、第1の利用者の端末か
らのアクセスを拒否することによって、他人のなりすましが発覚するものであることを特
徴とする請求項1に記載の電子認証システム。

30

【請求項7】

前記鍵センターによって一度保証された通信用鍵の内容の変更は、鍵センターを介在せ
ずに第1の利用者によって任意に行うことができることを特徴とする請求項1に記載の電
子認証システム。

【発明の詳細な説明】

【0001】

40

【発明の属する技術分野】

本発明は、電子メールの送信者、受信者の認証の信頼性を高めて安全な電子メール通信を実現する電子認証方式に関する。

【0002】

【従来の技術】

電子認証方式には、公開鍵方式と、共通鍵方式とが従来より知られている。公開鍵方式は、不特定多数の人が通信文のやりとりするのに画期的な仕組みであるといわれてきた。とくに、別人をかたって他人になりすます、いわゆる「なりすまし」の危険性を度外視したならば、公開鍵方式は、通信回線上のデータの保全にはかなり有効な仕組みであり、一度相手の公開鍵が間違いないということが確定できれば、その後の通信上のデータの漏洩は

50

かなりの強度で防ぐ事が出来るものと考えられていた。

【0003】

つまり、公開鍵方式の特徴として、

(1) 鍵は、利用者本人が一对(公開鍵と秘密鍵)の鍵を持つだけで良いこと、

(2) 署名機能がある仕組みであること(注:利用者Aの秘密鍵で暗号化したものは、利用者Aが公開した公開鍵で復号化したならば、誰でもが復号化して内容の確認ができ、この暗号化したものは、利用者Aしか作成できないから、利用者Aの署名になる)、

(3) 利用者Aとは異なる利用者Bと通信したい人は、利用者Bの公開鍵で暗号化すれば、利用者Bしか復号化できない、

という特徴が強調され、公開鍵方式は、このような特徴を有する、という理由からかなりの程度に普及してきた。

10

【0004】

一方、共通鍵方式は、通信しようとする利用者Aと利用者Bとの双方で互いに鍵を持ち合う必要があり、鍵の管理が面倒で使いにくいという理由から不特定多数の通信には、採用されずに現在に至っている。

【0005】

【発明が解決しようとする課題】

しかしながら、公開鍵方式が有効な仕組みである、というのは、実は大いなる誤解であった。

【0006】

20

その第1の理由は、鍵の総数の問題である。たとえば、N人で利用する公開鍵方式では、各人が一個の公開鍵を持つだけでよく、したがって、鍵の総数はN個でよいが、N人で利用する共通鍵方式によるときには、利用者各人のそれぞれが通信の相手の総数である(N-1)人分の鍵を持つ必要があり、このため、共通鍵方式で使用される鍵の総数は、N×(N-1)個必要である、といわれてきた。

【0007】

ところが、利用者個人側からみると、公開鍵方式によるときも、共通鍵方式によるときも、いずれも必要な鍵の総数は、(N-1)種類必要である。

【0008】

実際、公開鍵方式でN人が相手と通信のやり取りをする場合に、通信をする側の各利用者個人を考えれば、通信の相手先別に(N-1)個の公開鍵がなければ通信することが出来ない。これに自分の公開鍵と秘密鍵とが必要であるから、公開鍵方式において、各利用者個人が持つ鍵の総数は、N+1個である。

30

【0009】

第2の理由は、公開鍵方式においては、公開鍵と秘密鍵とのペアをいくつでも作ることができる、という点である。公開鍵と秘密鍵とのペアをいくつでも作れる、ということは誰もが、別人に「なりすまし」ができてしまう、ということでもある。

【0010】

通信内容の秘密を確保するための認証方式が「なりすまし」に弱いというのは、認証方式として致命的な欠陥であると云わなければならない。このため、従来の公開鍵方式では、できるだけ信頼ができ、利用者の双方がともに知っているひとの公開鍵を証明に使うという苦肉の策でこの方式を運用していたのが実状であった。

40

【0011】

このような公開鍵方式の不備を解消する目的で登場したのが「公開鍵の認証方式」である。この方式は、概ね、以下の手続きを経て利用者間で通信を行なう方式である。その手順の要領を図5に示す。

【0012】

この方式において、利用者A、Bは、それぞれ公開鍵と秘密鍵(利用者Aの公開鍵を「XXXX」、秘密鍵を「aaaaa」、利用者Bの公開鍵を「YYYYY」、秘密鍵を「bbbbbb」とする)を保有している。

50

【0013】

さらに、利用者A、B以外の利用者を代表してこれをC（公開鍵「ZZZZZZ」）とすると、認証センターCAは、各利用者が登録した公開鍵（利用者Aの公開鍵「XXXXXX」、利用者Bの公開鍵「YYYYYY」および利用者Cの公開鍵「ZZZZZZ」）とともに、各利用者と通信するための秘密鍵「ssssss」と、公開鍵「PPPPPP」を保有している。

【0014】

通信に先立ち、あるいは必要時に各利用者は、通信相手の公開鍵及び認証センターの公開鍵を認証センターCAから受取り、通信の相手方に対する通信文の暗号化処理は、通信相手の公開鍵を用いて行ない、受取った暗号文の復号化処理は、自分の秘密鍵を用いて行われる。

10

【0015】

図5において、利用者は、以下の手続きを行なって利用者間で通信を行なう。

すなわち、利用者の各人が認証センターCAに自分の公開鍵を登録しておく▲1▼（利用者Aは、公開鍵「XXXXXX」、利用者Bは、公開鍵「YYYYYY」を認証センターCAに登録する）。

【0016】

利用者間で通信をしようとするとき（例えば第1の利用者Aが、第2の利用者Bに通信をするとき）には、利用者Aは、認証センターCAに、自分がAであることの証明書の交付を申請し（▲2▼-1）、認証センターCAは、この利用者Aの申請を受けて、証明書を利用者Aに交付する（▲2▼-2）。

20

【0017】

証明書を受取った利用者Aは、通信文に自己署名や証明書を添付し、鍵情報とともにその通信文を暗号化し、その暗号文を直接利用者Bに送付する（▲2▼-3）。

【0018】

利用者Aからの通信文を受取った利用者Bは、認証センターCAに対し、通信文に添付されている証明書の確認を申請する（▲2▼-4）。この申請に対し、認証センターCAは、証明書が利用者Aのものであれば、「証明書は利用者Aのものであることに相違ない」ことの確認を利用者Bに通知する（▲2▼-5）。この確認通知によって、利用者Bは、「発信者がAであるとして送信されてきた通信文は、間違いなく利用者Aからのものである」、という認証センターCAの認証を信頼し、暗号文を平分に復号化することができる。

30

【0019】

通信文の本文は、RSA、DESを用いて作られ、利用者Aから利用者B宛ての通信文は、利用者Bの公開鍵「YYYYYY」で暗号化された暗号文である。通信文を受取った利用者Bは、利用者Bの秘密鍵「bbbbbb」を用いて通信文を復号化し、利用者Aから受取った暗号文を平文化する。

【0020】

この認証方式を利用して利用者Aが利用者Bと通信する場合に、利用者A、Bは、それぞれ認証センターCAに公開鍵の登録をした後、各回の通信に際しても、利用者は、通信文に添付すべき証明書の申請、あるいは証明書の確認のために、その都度、認証センターCAにアクセスしなければならない、逆に、認証センターCAは、認証のため、利用者間の各回の通信の度毎に介入しなければならない。

40

【0021】

このような「公開鍵の認証方式」を運用するには、公開鍵の登録にかなり厳格な登録手続きが必要である。実際に、公開鍵の登録手続きに際し、この手続きが完璧でないかぎり、他人の「なりすまし」を許す事になり、すべてのセキュリティの土台が崩れる。

【0022】

公開鍵の登録手続きに際し、本人を照合するには、通常、申請者に運転免許証、印鑑証明書その他本人を証明する書類を提示することによってなされる。本人を証明する手段に運転免許証、印鑑証明書の類を利用する限り、オンラインによる登録手続きは到底望むべく

50

もない。本人を特定するためには、勿論、厳重な登録手続きが必要である。公開鍵の登録手続きを厳格にすればするほど、一見他人の「なりすまし」の危険が減少し、セキュリティの安全性が高まるように思われるが、逆に公開鍵の登録手続きが厳格であればあるほど別の弊害を生ずる可能性が大きくなるのである。

【0023】

つまり、公開鍵の登録手続きが厳格であればあるほど、公開鍵を変更する場合にも、その手続きが面倒であるという理由から、公開鍵が変更されないまま、長期間にわたり固定化される傾向が強くなる。公開鍵が長期間にわたり固定化されればされるほど、公開鍵とペアで用いられる秘密鍵が解読される危険性、つまり、鍵の秘密が漏洩する可能性は増大するのである。

10

【0024】

秘密鍵の秘密漏洩の可能性を少なくするため、従来は、公開鍵ペアの鍵長を長くすることによって対応していたが、公開鍵ペアの鍵長が長くなればなるほど、処理速度が指数関数的に増大し、その結果、認証センター、各利用者には大きな負担を強いられることになっていた。しかも、このような負担を強いられるシステムであるにもかかわらず、他人の「なりすまし」を排除する事が出来ず、一旦「なりすまし」をされたときに、このシステムでは、「なりすまし」を発見できるシステムにはなっておらず、したがって、自分に「なりすまし」た他人を発見する事は、極めて困難である。

【0025】

本発明の目的は、簡単な手続きによって安全なセキュリティメールの送受信を可能とした電子認証方式を提供することにある。

20

【0026】

【課題を解決するための手段】

上記目的を達成するため、本発明による電子認証システムにおいては、第1の利用者の端末と、第2の利用者の端末と、通信用鍵を、第1の利用者の端末と第2の利用者の端末の間でD i f f i e－H e l l m a n型公開鍵配送法で共有された共有鍵を用いて、第1の利用者の端末にて暗号化された通信用鍵を一時格納し、該一時格納された暗号化された通信用鍵を、第2の利用者の端末に送信する鍵センターとからなる電子認証システムにおいて、

通信用鍵を鍵センターに送信する前に、第1の利用者の端末、第2の利用者の端末間で、D i f f i e－H e l l m a n型公開鍵配送法を用いて鍵共有が行われ、

30

第1の利用者の端末の使用者及び第2の利用者の端末の使用者の個人用認証情報の鍵センターへの登録は通信用鍵を鍵センターに送信する前に行われ、

第1の利用者の端末から、鍵センターを介して第2の利用者の端末へ通信用鍵を送信する際に、第1の利用者の端末は、通信用鍵を、前記共有鍵を用いて暗号化して前記鍵センターに送信し、

鍵センターにおいて、登録された個人用認証情報を用いて第1の利用者の端末である送信側の認証が行われ、当該認証がおった場合に、暗号化された通信用鍵を前記鍵センターに一時格納し、

前記鍵センターは、登録された個人用認証情報を用いて、第2の利用者の端末である受信側の認証を行い、当該認証がおった場合に、前記暗号化された通信用鍵を、前記第2の利用者の端末へ送信し、

40

前記第2の利用者の端末は、前記共有鍵を用いて前記暗号化された通信用鍵を復号し、前記第1の利用者の端末は、通信文を前記通信用鍵を用いて暗号化して、直接、前記第2の利用者の端末に送信し、

前記第2の利用者の端末は、受信した通信文を前記復号した通信用鍵を用いて復号するものである。

【0027】

また、前記個人用認証情報は、各利用者が各自生成したそれぞれの利用者に固有の情報として、乱数および、指紋、目の光彩をデジタル情報に変換したものであり、前記鍵セン

50

ターは、提示された登録済みの前記個人用認証情報をもって、暗号化された通信用鍵を送信してきた利用者およびその暗号化された通信用鍵を送信すべき利用者本人を特定するものである。

【0028】

また、前記各利用者の端末と前記鍵センター間の通信で送信される少なくとも前記個人用認証情報は、各利用者の端末と鍵センター間のD i f f i e - H e l l m a n型公開鍵配送法により共有した共有鍵を用いて暗号化されて送信されるものである。

【0029】

また、前記暗号化された通信用鍵は、鍵センターの端末を仲介して第1の利用者の端末から第2の利用者の端末へ送信される際には、第1の利用者と、第2の利用者間のDH方式を用いて暗号化されて送信されるものであり、鍵センターの端末は、第1の利用者の端末から預かって、第2の利用者の端末に送信する暗号化された通信用鍵の内容には関与できないものである。

10

【0030】

また、各利用者は、前記各利用者の端末で個人用認証情報を鍵センター端末にオンラインで登録した後、通信用鍵の送受信時および個人用認証情報の更新時以外に鍵センター端末へのアクセスは不要である。

【0031】

また、前記第2の利用者の端末は、前記第1の利用者の端末から前記鍵センターを介して送信された暗号化された通信用鍵を受信した後、その暗号化された通信用鍵を前記第1の利用者の端末、第2の利用者の端末間で、D i f f i e - H e l l m a n型公開鍵配送法により共有した共有鍵を用いて復号して格納し、その復号された通信用鍵が変更されるまでは、その復号された通信用鍵を用いて第1の利用者から送信されてきた暗号化された通信文を復号化するものである。

20

【0032】

また、他人が別の個人用認証情報を鍵センターに登録して第1の利用者になりすました場合において、前記第1の利用者の端末は、前記認証登録手続きまたは前記通信用鍵の送受信手続きに際し、鍵センターの端末にアクセスしたときに、鍵センターの端末は第1の利用者の個人用認証情報として既に登録されている個人別認証情報とは異なるとして、第1の利用者の端末からのアクセスを拒否することによって、他人のなりすましが発覚するものである。

30

【0033】

また、前記鍵センターの端末によって一度保証された通信用鍵の内容の変更は、鍵センターの端末を介在せずに第1の利用者によって任意に行うことができるものである。

【0035】

また、請求項1に記載の電子認証システムであって、
前記鍵センターの端末は、前記認証登録手続きと、前記通信用鍵の送受信手続きを行い、第1の利用者と第2の利用者の端末間で送信される暗号化された通信用鍵の内容には関与できないものである。

【0036】

【発明の実施の形態】

以下に本発明の実施の形態を図によって説明する。図1において、本発明は、各利用者(A, B, C...)が鍵センターKCに個人用認証情報を登録し、これら利用者の内、暗号化された通信用鍵を送信する第1の利用者(この実施形態では、利用者Aとして説明する)と、その暗号化された通信用鍵を受信する特定の第2の利用者(この実施形態では利用者Bとして説明する)間で通信を行なう場合において、各利用者は、認証情報登録手続き(1)と、通信用鍵の送受信手続き(2)と、セキュリティメールの送受信手続き(3)(なおここでの(1)(2)(3)は○内に1, 2, 3が記入された記号に相当する)とを行ない、鍵センターKCは、送信者(利用者A)の本人を認証するものである。

40

【0037】

50

なお、本発明に云う鍵センターK Cは、利用者を認証する意味では、従来の公開鍵方式による「認証センター」C Aと同じであるが、認証の機能が異なるため、本発明においては、「鍵センター」の用語を用いて公開鍵方式による「認証センター」C Aとは区別している。

【0038】

以下に順をおって、手続きの手順を説明する。本発明において、鍵センターK Cは、たとえば云うならば、厳格な郵便局であり、あるいは結婚のなかだちをする仲人の役割とも云うべき役割を担い、互いに通信しようとする利用者間に一回介入するだけで、その後、利用者間の通信に介入する事はない。

【0039】

すなわち、本発明において、鍵センターK Cは、各利用者の個人用認証情報の登録を受付けてこれを管理する役割と、利用者Aから利用者Bへの通信用鍵の送付（送信）の依頼があったときに、利用者Aと、利用者Bとの個人用認証情報を確認のうえ、利用者Aから暗号化された通信用鍵をうけとり、これを利用者Bに配達（送信）する役割とを受け持ち、特別の場合を除いて原則的に、利用者Aと利用者B間で交信される暗号化された通信用鍵の内容に関わる事項について関与することはできない。

【0040】

また、鍵センターK Cは、利用者個人が任意に選んだ個人用認証情報（印鑑証明登録というべきもの）の登録を受付けるが、図5に示した従来の認証方式のように、個人別公開鍵情報は使わない。

【0041】

1. 認証登録手続き

図2において、認証登録手続き▲1▼は、初期処理であり、各利用者が自分の個人用認証情報を鍵センターK Cにオンラインで登録をする手続きである。個人用認証情報の登録は、各利用者A、Bと、鍵センターK C間で通信をして鍵センターK Cに自己の個人用認証情報（利用者Aの個人用認証情報「xxxxxx」、利用者Bの個人用認証情報「yyyyyy」）を登録する。利用者A、B以外の利用者を代表してこれをCとしたとき、利用者Cも同様に自分の個人用認証情報「zzzzzz」を鍵センターK Cに登録する。

【0042】

鍵センターK Cは、各個人の認証情報を登録管理する。各利用者は、それぞれ個人用認証情報と、通信相手別の通信用鍵（公開鍵方式に用いる公開鍵に相当する）を保有している。個人用認証情報および通信用鍵は、一定の規約をクリアしていれば利用者が任意に設定する事が出来る。

【0043】

各利用者は、自分で作製した個人用認証情報を鍵センターK Cにオンライン登録する。したがって、利用者Aは、個人用認証情報「xxxxxx」、利用者Bは、個人用認証情報「yyyyyy」、利用者Cは、個人用認証情報「zzzzzz」をそれぞれ鍵センターK Cにオンライン登録をすることになる。

【0044】

各利用者A、B、Cが鍵センターK Cにアクセスするのは各利用者の自由であるが、手続き上必要が生ずるのは、個人用認証情報の新規登録や、更新時、初期の通信用鍵の配送時のみである。鍵センターK Cへの個人用認証情報の登録変更もオンラインで行なえばよく、しかもいつでもその変更の登録が可能である。

【0045】

各利用者と鍵センターとの通信は、DH方式（Diffie、Hellmanの鍵配送方式：利用者A、とBが暗号鍵（共通鍵）を秘密裡に共有できる方式）をベースにしたもので、ワンタイムパスワードで暗号化された暗号文をもって行われ、通信傍受に対しても登録の個人用認証情報の漏洩は防止される。

【0046】

本発明において、個人用認証情報には、それぞれの利用者に固有の情報が用いられる。利

10

20

30

40

50

ユーザーに固有の情報とは、その個人用認証情報を使用する利用者以外には知り得ない情報、あるいは特定の利用者以外には使用出来ない情報を含むものである。たとえば、任意に配列された数字（乱数）は前者の例であり、指紋、目の光彩のような個人に固有の特性は後者の例である。

【0047】

指紋、目の光彩のような固定的な情報自体は、他人に真似ができない情報ではあるが、これらが個人用認証情報として使用されているかも知れないと予測される可能性が大きく、しかも個人用認証情報としてオンライン登録するに際しては、当然、指紋、目の光彩のデータがデジタル情報に変換されるため、コピーが可能であり、機密漏洩のおそれ大きい。

10

【0048】

個人用認証情報には、好ましくは、乱数のような、個人用認証情報としての使用の予測性がなく、しかも容易に変更が出来るデジタル情報を使用するのが望ましい。

【0049】

2. 通信用鍵の送受信手続き

図3において、利用者Aは、通信用鍵の送信手続き（▲2▼-1）として、通信の相手側として特定した利用者B用の通信用鍵「A B A B A B」を鍵センターKCにオンラインで送付（送信）し、鍵センターKCに、利用者Bへ通信用鍵「A B A B A B」の配送を依頼する。

【0050】

20

鍵センターKCは、利用者Aの個人認証情報「xxxxxx」を確認し、利用者Aから送付された利用者B宛での暗号化された通信用鍵「A B A B A B」を一時プールする。その後、利用者Bと通信して利用者Bの個人認証情報「yyyyyy」を確認した後、鍵センターKCは、利用者Bに利用者Aの通信用鍵「A B A B A B」をオンラインで送付（送信）し（▲2▼-2）、利用者Bは、自分宛での通信用鍵「A B A B A B」を入手する。

【0051】

なお、利用者Bは、鍵センターKCから送付されてきた通信用鍵の受取りを拒否するときには、その旨を鍵センターKCに伝え、鍵センターKCは、受け取りが拒否されたことを利用者Aに通知する。

【0052】

30

この手続きは、鍵センターKCの認証を受けた上で、利用者Aから利用者Bに渡す通信用鍵を封書（利用者A、B間のDH暗号処理、センターは見えない）に入れ、鍵センターKCを通して利用者Bに配送してもらう、という手続きにたどる事が出来る。第1の利用者Aから第2の利用者Bへ配送される通信用鍵「A B A B A B」は、第1の利用者Aと第2の利用者B間のDH方式によって共有した共有鍵を用いて暗号化される。

【0053】

利用者Bは、封書（DH暗号処理）から利用者Aから送付された鍵を取出す（正しくは、同じ鍵を作り出して復号する）ことができる。利用者AまたはBと鍵センターKCとの通信は、DH方式をベースにしたものでワンタイムパスワードにて処理され、通信傍受にも通信用鍵の漏洩は防がれる。鍵センターが利用者Bに送付する通信用鍵「A B A B A B」は、利用者Aにより利用者Aと利用者B用のDH方式によって共有した共有鍵を用いて暗号化されるものであるから、鍵センターKCにおいても通信用鍵の変造や、他人が利用者Aに「なりすまし」は出来ない。

40

【0054】

利用者Bが鍵センターから受取った通信用鍵「A B A B A B」は、鍵センターKCが保証した利用者Aからの通信用鍵なので信頼できる。

【0055】

3. セキュリティメールの送受信手続き

図4において、セキュリティメールの送受信手続き（3）として、利用者Aは、通信用鍵「A B A B A B」を用いて通信文を暗号化し、暗号化された通信文を直接利用者Bに送

50

付し、利用者Bはこれを受信する。利用者Aから送付されてきた暗号化された通信文は、鍵センターKCから受取った利用者Bに対する利用者Aの通信用鍵「A B A B A B」を用いて復号化して平文にする事が出来る。

【0056】

この手続きにおいて、利用者Aから直接利用者Bへ送付された通信文は、鍵センターKCから送付された通信用鍵「A B A B A B」を使用して暗号化された通信文であり、その暗号化された通信文は、通信用鍵の所有者である利用者Aにしか作成することができない。

【0057】

逆に利用者Bにとってみれば、暗号化された通信文の復号が可能な通信用鍵「A B A B A B」を送信した者がとりもなおさず利用者Aであることの確証となる。したがって、通信用鍵は、署名と同じ効果を持ち、しかもその通信用鍵は、利用者Aのものであることが鍵センターKCによって保証されているので安心して商用通信が可能となる。利用者Aの通信用鍵「A B A B A B」は、以後利用者Aから利用者Bへの通信に使用される。逆に利用者Bが通信文を送信する第1の利用者になって、利用者Aを通信文を受信する第2の利用者として通信する場合には、別の通信用鍵を設定する必要がなく、通信用鍵「A B A B A B」は利用者A B間の通信用鍵として使用できる。

【0058】

各利用者は、特定の利用者の通信用鍵を入手した後、その通信用鍵を保管し、その通信用鍵が変更されるまでは、その通信用鍵を用いて特定の利用者から送付されてきた暗号化された通信文を復号化することができる。

【0059】

なお、一度、鍵センターによって保証された通信用鍵を使用した相手側からの通信用鍵の変更は、問題なく応じることができるため、以後は双方の意志にて通信用鍵は、鍵センターを介在しなくても任意に変更できる。

【0060】

もっとも、内容証明や、通信履歴の証明が必要な時には、毎回センターを介して送信することもできる。その場合は、通信用鍵の配送とは異なり、鍵センターが通信文を解読できる情報あるいは、通信履歴が分るように通信文を鍵センターに送付すればよい。

【0061】

他人（第三者）が利用者Aの名をかたって個人用認証情報（例えば「ffffff」）で利用者Aになりすましたときには、利用者Aが自分の個人用認証情報「xxxxxx」で鍵センターKCにアクセスしても、送付されてきた個人用認証情報「xxxxxx」は、鍵センターKCに利用者Aの個人用認証情報として既に登録されている個人用認証情報「ffffff」とは異なるとして、鍵センターKCは、本物の利用者Aのアクセスを拒否する。

【0062】

つまり、利用者は、認証登録手続きまたは通信用鍵の送受信手続きに際し、鍵センターKCにアクセスして個人情報の認証確認をしたときに、自己の個人用認証情報が通用しないことによって、他人の「なりすまし」が発覚する。

【0063】

本発明において、厳密に云えば他人の「なりすまし」が可能な機会は、初期登録時のみである。つまり、利用者が鍵センターと無縁の間、具体的は、その利用者がセキュリティ通信を行わない間または、個人用認証情報が未登録の間だけ、その利用者に他人が「なりすます」ことが可能であるといえる。しかし、利用者としてユーザが一度でも鍵センターにアクセスしたときに、他人の「なりすまし」が発覚する仕組みになっているということである。

【0064】

なお、個人用認証情報、通信用鍵、通信文を含めて、鍵センターと、各利用者間、或いは各利用者間で通信して、それぞれの利用者の端末機器及び鍵センターの端末機器に格納される情報の暗号化に際しては、各利用者の端末機器、或いは鍵センターの端末機器に固有

10

20

30

40

50

の情報（ハードウェア情報）と、ユーザーが任意に設定できる情報（ソフトウェア情報）とを用いて二重に暗号化し、暗号化された結果情報だけをそれぞれの端末機器に格納しておく事により、他者による意図的な盗聴、改ざんから情報を防護でき、万一、端末機器に格納された情報が漏洩した場合でも、予め定めた端末機器以外の他の端末機器での情報の復号化が困難であるため、鍵センターの内部者といえども、容易には不正操作が出来ず、セキュリティの強度を著しく高める事が出来る。

【0065】

【発明の効果】

以上のように本発明は、利用者、鍵センターの何れにも、負担の大きい公開鍵方式を使用せず、共通鍵方式の一形態である通信用鍵の使用と、DH方式との組合せによって、利用者本人の認証と、安全なセキュリティメールの送受信を実現するものである。本発明によれば、あたかも住民登録をするように、利用者が自己の個人用認証情報を鍵センターに登録するだけでよく、しかも個人用認証情報の登録は、オンラインで自動登録ができるので手続きは簡便である。

10

【0066】

また、個人用認証情報の登録後は、特別の場合を除いて、個人用認証情報の登録更新や、初期の通信用鍵の配送の場合のみ、利用者は鍵センターにアクセスするだけでよく、利用者は勿論、鍵センター側の負担が少ない。

【0067】

また、本発明によれば、鍵センターへの個人用認証情報の登録は、オンラインで行なうことが可能であり、しかもいつでも任意に変更する事ができる。これは、従来の公開鍵方式では、全く考えられなかったことである。また、本発明のシステムによれば、他人の「なりすまし」を許す可能性は少ないが、たとえ、あったとしても、一度でもセキュリティ通信をすることによって、他人の「なりすまし」を発見できる。

20

【0068】

本発明は、すべてのセキュリティのベースとなる個人用認証情報は、利用者自らがコントロールできる仕組みであるから、ユーザとしての利用者は安心であり、セキュリティの安全度は高い。さらに、本発明によるときには、セキュリティメールの通信電文の暗号化は、従来の共通鍵方式に相当する方式によるため、通信文に余計な情報の添付は不要であり、その分高速処理が可能となる。

30

【図面の簡単な説明】

【図1】本発明による電子認証システムの構成を示す図である。

【図2】認証登録手続きの要領を示す図である。

【図3】通信用鍵の送受信手続きの手順を示す図である。

【図4】セキュリティメールの送受信手続きの手順を示す図である。

【図5】従来の公開鍵方式による認証方式の構成を示す図である。

【符号の説明】

K C 鍵センター

A, B, C 利用者

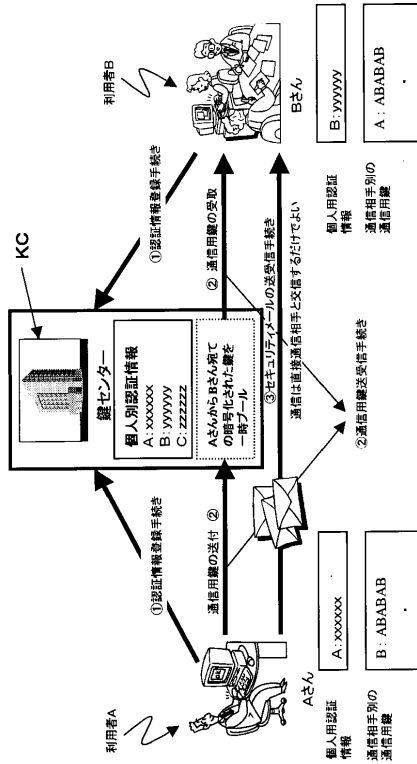
xxxxxx 利用者Aの個人用認証情報

yyyyyy 利用者Bの個人用認証情報

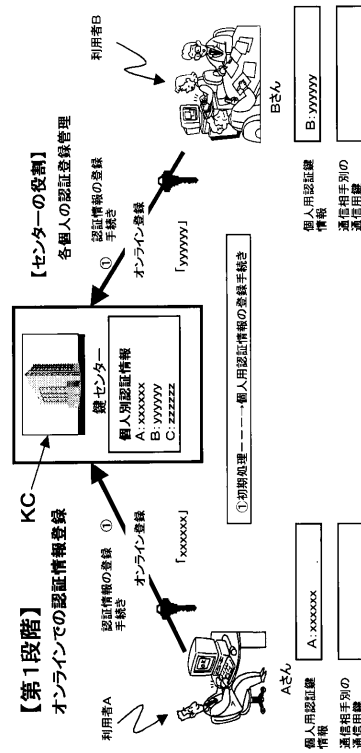
A B A B A B 利用者Aから利用者Bに送付する通信用鍵

40

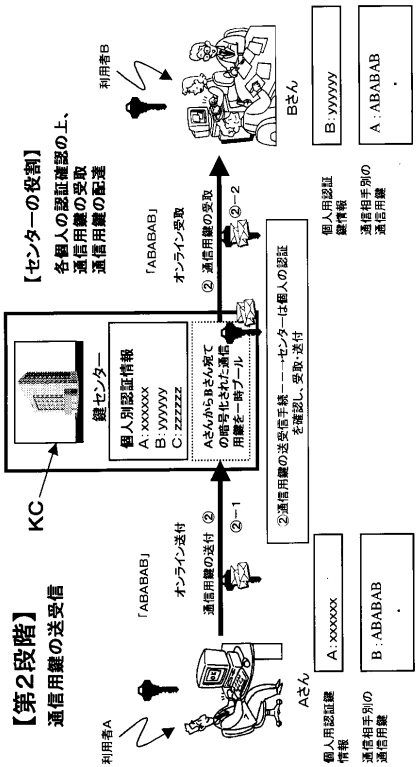
【図 1】



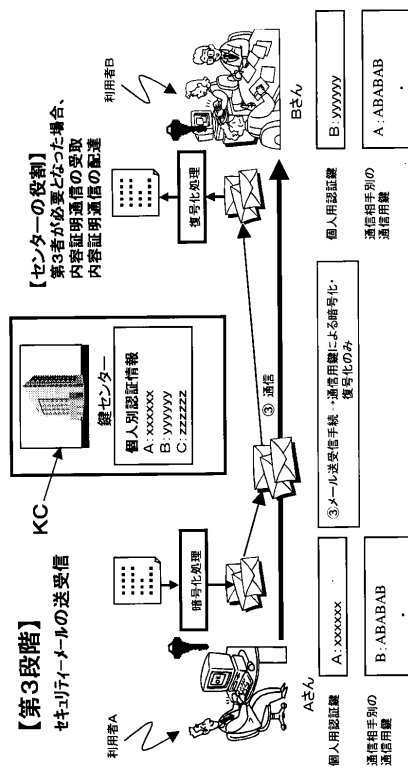
【図 2】



【図 3】



【図 4】



【図 5】

