

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2018年2月8日(08.02.2018)



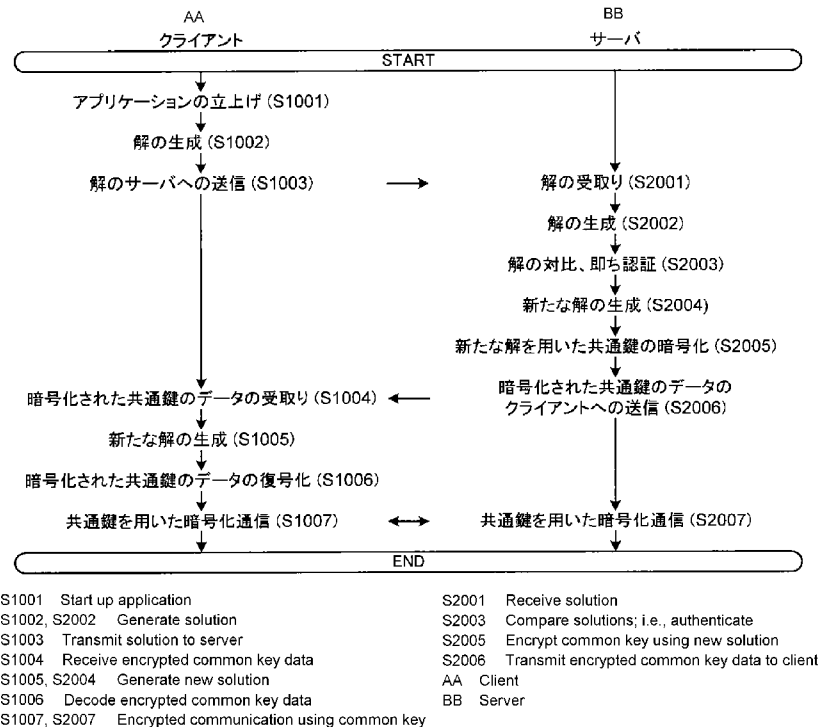
(10) 国際公開番号

WO 2018/025991 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) G09C 1/00 (2006.01)
G06F 21/44 (2013.01) H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2017/028391
- (22) 国際出願日: 2017年8月4日(04.08.2017)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2016-153699 2016年8月4日(04.08.2016) JP
- (71) 出願人: 株式会社エヌティーアイ (NTI, INC.)
[JP/JP]; 〒5108021 三重県四日市市松寺三丁目7番4号 Mie (JP).
- (72) 発明者: 中村 貴利 (NAKAMURA, Takatoshi);
〒5108021 三重県四日市市松寺三丁目7番4号 株式会社エヌティーアイ内 Mie (JP).
- (74) 代理人: 村松 義人 (MURAMATSU, Yoshihito);
〒1050003 東京都港区西新橋二丁目8番11号 第7東洋海事ビル2階 村松国際特許事務所 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION CLIENT, COMMUNICATION SERVER, COMMUNICATION METHOD, AND PROGRAM

(54) 発明の名称: 通信システム、通信用クライアント、通信用サーバ、通信方法、プログラム



(57) Abstract: The present invention proposes an encrypted communication technology which is less vulnerable to a third party attack, particularly an MITMA attack, than SSL. A client and a server both have the function of generating the same solution under the same condition. The client makes a first solution (S1002) and sends the first solution to the server (S1003). The server receives the solution, makes the server's own solution (S2002), and, if the server's solution matches the solution received from the client, authenticates the client as being valid (S2003). The server encrypts a common key that



MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告（条約第21条(3)）

the server has, using a second solution (S2005) as a key and sends the second solution to the client. The client generates the second solution and decodes the encrypted common key using the second solution (S1007) as a key. The server and the client perform an encrypted communication according to a common key scheme using the shared common key.

(57) 要約：SSLよりも第三者による攻撃、特にはMITMAによる攻撃に強い暗号化通信の技術を提案する。クライアントとサーバはともに、同じ条件下では同じ解を生成する機能を持つ。クライアントは、一つ目の解を作り（S1002）、それをサーバに送る（S1003）。サーバは解を受取ると自ら解を作り（S2002）、それがクライアントから受取った解と一致したらクライアントが正当だと認証する（S2003）。サーバは自らが持つ共通鍵を2番目の解を鍵として暗号化して（S2005）、クライアントに送る。クライアントは2番目の解を生成しそれを鍵として暗号化された共通鍵を復号化する（S1007）。サーバとクライアントは、共有した共通鍵で共通鍵方式の暗号化通信を行う。

明 細 書

発明の名称：

通信システム、通信用クライアント、通信用サーバ、通信方法、プログラム

技術分野

[0001] 本発明は、通信技術、より詳細には暗号化通信のための技術に関する。

背景技術

[0002] 例えば、インターネット上でインターネット上に存在する店舗への支払いを行う、インターネットバンキングで自らの口座の残高を見たり第三者への送金を行う等という場合には、それらを行うユーザは自らの端末（クライアント）と上記店舗等のサーバとの間でインターネットを介して通信を行う。かかる通信はもちろん秘匿性が高いものでなければならず、暗号化通信の技術が用いられている。

暗号化通信の技術の1つとしてSSL（secure sockets layer）と呼ばれる技術が実用化されている。なお、本願でSSLと言う場合には、SSLを標準化したものであるTLS（transport layer security）も当然にSSLに含まれる。

[0003] SSLには大きく分けて2つの側面がある。1つは本人確認（認証）であり、もう1つは暗号化通信である。これらがどのように実現されるかについて説明するため、SSL通信で実行される処理について説明する。

この例では、クライアントとサーバ間でSSL通信が実行されるものとする。

（1）前提処理

a. サーバは、一对の秘密鍵と公開鍵を生成する。秘密鍵と公開鍵とは、周知のように、そのいずれもが平文のデータを暗号化して暗号化データとすることが可能なものであるとともに、それらの他方で暗号化された暗号化データを復号化して平文のデータに戻すことができるものとされる。他方、サ

サーバには、自己の正当性を相手方が確認するためのデータであるサーバ証明書であって、自己の公開鍵を含み、且つそのサーバ証明書の正当性を示すための電子署名が付されているものがインストールされる。

b. クライアントは、共通鍵を準備する。共通鍵は、周知のように、平文のデータを暗号化して暗号化データとすることが可能なものであるとともに、同じ共通鍵で暗号化された暗号化データを復号化して平文のデータに戻すことができるものとされる。

c. クライアントには、ルート証明書がインストールされる。ルート証明書は、ルート認証局が作成したものである。ルート認証局は、上述のサーバ証明書を作成する者でもあり、サーバ証明書に電子署名を付す者でもある。クライアントは、ルート証明書とサーバ証明書に付された電子署名の組合せにより、サーバ証明書の正当性を確認することができる。

(2) サーバとクライアントでの共通鍵の共有

a. クライアントがサーバにSSL通信の要求を行う。

b. サーバがクライアントに対して上記サーバ証明書を送信する。上述のように、サーバ証明書には、サーバが用いる公開鍵が含まれ、電子署名が付されている。

c. クライアントは、自己が所有するルート証明書とサーバ証明書に付された電子署名とを用いてサーバ証明書の正当性を検証し、サーバ証明書が正当であれば自分が通信しているサーバが正当であると認証し、サーバ証明書が不当であればサーバが正当であるとの認証を行わない。

d. クライアントはサーバを認証した場合には、自己が所有する共通鍵を、サーバから受取ったサーバ証明書に含まれていた公開鍵で暗号化して、サーバに送る。

e. サーバは、クライアントから受取った暗号化された公開鍵を自己が所有する秘密鍵で復号化する。これにて、クライアントの共通鍵は、クライアントとサーバで共有されることになる。

(3) サーバとクライアント間での暗号化通信

サーバとクライアントとはともに、自分が持つ共通鍵で暗号化した暗号化データを相手方に送る。サーバとクライアントとはともに、相手から受取った暗号化データを自分が持つ共通鍵で復号化する。これにて、サーバとクライアントとの間では暗号化通信が可能となる。

[0004] 以上がSSL通信で実行される処理である。

乱暴であることを承知で言うと、SSL通信で実行したいのは、上記（３）のサーバとクライアント間での暗号化通信のみである。これを、共通鍵を用いて行いたいというのがSSL通信の要点である。なぜ共通鍵でかかる暗号化通信を行いたいかといえ、共通鍵での暗号化通信は、特に公開鍵と秘密鍵とを用いた暗号化通信に較べてその処理が格段に軽いからである。

もっとも、そのためには、共通鍵をサーバとクライアントとの間で共有しなければならない。それを実現するために、サーバが持つ公開鍵と秘密鍵とを用いてクライアントからサーバに共通鍵が送信されるというのが、SSL通信についての上記（２）の処理である。公開鍵と秘密鍵を使った暗号化通信では、暗号化と復号化に用いられる鍵が上述のように異なる。したがって、公開鍵で暗号化されたクライアントの共通鍵が仮に、クライアントからサーバに送られている途中で悪意のある第三者に盗まれたとしても、当該第三者は秘密鍵を持たないのでクライアントの共通鍵そのものが第三者に盗まれるということはない。この結果には、公開鍵が公開されていることはまったく影響しない。

クライアントから第三者に共通鍵を送る際には、上述したように、サーバからクライアントに送られてきた公開鍵が用いられる。しかしながら、ここでその公開鍵自体の正当性、ひいては公開鍵を送って来た者（サーバ）の正当性が問題となる。たとえば、悪意のある第三者が公開鍵をクライアントに送ってくることがあるからである。公開鍵乃至それを送ってきた者の正当性を担保するのが、SSL通信についての上記（１）、（２）の処理である。これら処理により、クライアントが、サーバの正当性を確認（認証）することで、SSL通信の正当性が保証されることになる。

発明の概要

発明が解決しようとする課題

[0005] 以上の説明によればSSL通信には、悪意の第三者が付け入る隙が無いようにも思われる。しかしながら、実際にはSSL通信でも悪意の第三者による盗聴が発生しており、例えばインターネットバンキングではユーザの口座の金銭がそのユーザの預かり知らない第三者の口座に勝手に送金される等の被害が頻繁に生じている。

そのようなことが生じる原因は複数あるが、例えば、クライアントにある上述したルート証明書が例えばハッキングや、コンピュータウィルスを用いる等の手法によって改竄されることがその一因となる。また、ルート証明書には通常有効期限があるにもかかわらず、多くのユーザは自らのクライアントにおいてルート証明書の更新をしていない。そうすると、クライアント内にあるルート証明書は改竄されたのと同様の状態となることがあり得る。

ルート証明書が改竄された場合には、悪意のある第三者は、改竄されたルート証明書によって自らの正当性がクライアントにおいて認証されるような偽のサーバ証明書を自ら作り、ユーザが正当なサーバへとSSL通信の要求を行ったときに、正当なサーバになりすまして、クライアントと正当なサーバとの間に入り込んでその要求を受取る。そしてその正当なサーバになりすました偽のサーバは、自らが作った、偽のサーバ証明書をクライアントへと送信する。そうするとクライアントは、改竄されたルート証明書を使ってその偽のサーバ証明書を正当なものと判断し、ひいては偽のサーバを正当なものと認証する。そうすると、クライアントは自らが持つ共通鍵を偽のサーバ証明書に含まれていた偽の公開鍵で暗号化して、偽のサーバへと送信する。それを受取った偽のサーバは自らが持つ上述の偽の公開鍵と対となった秘密鍵でその暗号化された共通鍵を復号化する。これをもって、クライアントが持っていた共通鍵は、悪意の第三者の手に渡るのである。以降においては、そのクライアントとサーバとの間の通信が仮に共通鍵による暗号化通信であったとしても、その暗号化通信のために必要な共通鍵を所有している悪意の

第三者は、その解読を自由に行えるようになる。

このような、クライアントとサーバの間に悪意の第三者が入り込んで行う攻撃を中間者攻撃（man-in-the-middle attack：MITMA）と称するが、他の暗号化通信の場合と同様、SSLの場合にもこれを防げていない。

[0006] そもそも暗号化通信の分野では、送信者と受信者が同じ鍵を持つ（つまり、共通鍵方式の通信を行う。）というのが基本であり、同じ鍵をどうやって共有するのかという点が古くから問題となっている。かかる問題は鍵の配送問題などと称されるが、SSL通信でもこの鍵の配送問題は解決されていないのである。

上述したようにSSL通信では最終的に共通鍵方式の通信を行うが、それに先立って、クライアントが持つ共通鍵をどうやって安全にサーバに配送するのかという点が問題となる。SSL通信では上述のように、秘密鍵方式の暗号化通信を初段に用い、且つサーバ証明書とルート証明書とを用いた認証技術を組合せることで、クライアントが持つ共通鍵を安全にサーバに配送せんとしているが、その試みは上述のように、完璧に成し遂げられているとは言えないのである。

[0007] 本願発明は、SSLよりも第三者による攻撃、特にMITMAによる攻撃に強い暗号化通信の技術を提案するものである。

課題を解決するための手段

[0008] かかる課題を解決するため、本願発明者は、以下に説明する発明を提案する。

本願発明は、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムで実行される通信方法である。かかる通信方法は、現在普及しているSSL通信の一態様であっても良いし、そうでなくても良い。言い換えれば、かかる通信方法は、SSL通信の進化版或いは改良版と捉えることもできるし、SSL通信とは無関係のものとして捉

えることもできる。本願発明をSSL通信の進化版或いは改良版と捉える（SSLの代替として応用するのであれば、第1通信装置は従来のサーバ、第2通信装置は従来のクライアントという位置づけとなる。なお、本願におけるネットワークは、典型的にはインターネットである。

そして、本願発明は、以下の過程を含む。

本願発明は、前記第2通信装置が、その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取る過程、前記第1通信装置が、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理か、又は前記第2通信装置を正当なものと認証したとの通知を前記第1通信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理の一方を行う過程、前記第1通信装置が前記共通鍵を暗号化した場合には、前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信するとともに、暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を、前記第1通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、前記第2通信装置が前記共通鍵を暗号化した場合には、前記第2通信装置から前記第1通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信するとともに、暗号化された前記共通鍵を受取った前記第1通信装置が、その解生成

手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置と、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、を含んでいる。

本願発明における上述の最後の過程、つまり、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置と、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程は、現在のSSL通信の場合でいうのであれば、上記(3)の処理に相当する。つまり、共通鍵方式の暗号化通信自体は極めて一般的であるから必ずしもそうする必要はないが、この部分はSSL通信で現在用いられている上記(3)の処理をそのまま踏襲することが可能である。

背景技術の欄で説明したように、SSL通信では、共通鍵の配送と、通信相手の認証を如何にして行うかというのが重要である。そして、この課題は他の暗号化通信でも同様に重要である。それらを本願発明では、上述の「以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置と、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程」の前に実現しているのである。以下、その仕組みについて説明する。

[0009] この発明では、第2通信装置と第1通信装置とで、解生成手段が用いられるというのが特徴的である。第2通信装置と第1通信装置とで用いられる解生成手段は同じものでも同じものでなくても構わないが、少なくとも、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできるものである。解生成手段には、例えば、ワンタイムパスワードの技術を流用することができる。ワンタイムパスワードには、2つの解生成手段で生成されたワンタイムパスワードの同じ順番で生成されたもの同士を比較した場合に両者が同じになるもの、2つの解生成手段で同じ時刻で

生成されたもの同士を比較した場合に両者が同じになるもの等の幾つかの方式があるが、ワンタイムパスワードの技術を流用するのであれば、この発明で用いられる解生成手段はそれらのどれでも構わない。

また、この発明における第2通信装置と第1通信装置とは、同じ解を用いた場合には同じ暗号化と復号化の処理を実行できるようになっている。この場合における、解は事実上、通常の暗号化と復号化の処理における共通鍵として機能する。典型的には、第2通信装置と第1通信装置とは、同じアルゴリズムを用いて、暗号化と復号化の処理を実行できるようになっている。なお、かかる暗号化と復号化の処理は、現在のSSL通信の場合における(2)の処理に相当するものであり、現在のSSL通信の場合における(3)の処理、即ち、「以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置と、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程」で実行される暗号化と復号化とは異なる。

第1通信装置と第2通信装置とが実行する具体的な処理内容について説明する。

まず、第2通信装置と第1通信装置との間で暗号化通信を行うにあたり、まず、第2通信装置が、その解生成手段で解を生成させ、その解をネットワークを介して第1通信装置に送信する過程が実行される。

次に、前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取る過程、が実行される。続けて、第1通信装置にて、認証の処理が行われる。認証の処理は、具体的には以下のようにして行われる。第1通信装置は、第1通信装置の解生成手段で解を生成させ、第1通信装置の解生成手段で生成した解と、第2通信装置から受取った解とを比較する。その結果、第1通信装置は、両者が一致した場合には、解を送ってきた第2通信装置を正当なものと認証し、両者が一致しなかった場合には、第2通信装置は正当なものでないと判断する。上述したように、第1通信装置が持つ解生成手段は、共通条件下で生成されたものを比較すれば第2通信装置で生

成された解と同じものとなる解を連続して生成することのできるものとなっている。したがって、正当な第2通信装置から送られてきた解と同じ解を第1通信装置の解生成手段は作ることができるのであるから、上述の如き認証は可能である。

第1通信装置で、第2通信装置が正当なものと認証された後の処理には2つの場合がある。簡単に言うと、共通鍵を最初に持っているのが第1通信装置の場合と第2通信装置の場合の2つの場合があるのである。前者の場合には、第1通信装置から第2通信装置へ暗号化された共通鍵が送られることにより、共通鍵が第1通信装置と第2通信装置で共有される。後者の場合には、第2通信装置から第1通信装置へと暗号化された共通鍵が送られることにより共通鍵が第1通信装置と第2通信装置で共有される。

具体的には、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理が実行される。この処理が実行された場合には、つまり、前記第1通信装置が前記共通鍵を暗号化した場合には、前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信するとともに、暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下（例えば、共通鍵を暗号化するために使われた第1通信装置における解の作られた順番と、その解の第2通信装置内で作られた順番とが同じこと）で生成された解を用いて暗号化された前記共通鍵を、前記第1通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程が実行される。上述したように、第1通信装置と第2通信装置はともに、互いに共通する同じ解を連続して発生するための解生成手段を備えている。そして、第1通信装置と第2通信装置とはその解を用いて、同じアルゴリズムで暗号化と復号化を行えるようになっている。したがって、第2通信装置は、第1通信装置である解を

用いて暗号化された共通鍵のデータを第1通信装置から受取った場合には、暗号化されたその共通鍵を自ら生成した解を用いて復号化することができる。ここで、重要なのは、第1通信装置が暗号化に用いる解、及び第2通信装置が復号化に用いる解はともに、第2通信装置の認証に使われた解ではなく、第1通信装置及び第2通信装置の解生成手段で生成された解であるということである。これらの解は、第1通信装置又は第2通信装置の内部にのみ存在するものであって、ネットワークを経由して送信されない。したがって、第三者はこの解を盗み取ることが事実上できない。それは即ち、暗号化してネットワーク上を送信される共通鍵のデータを悪意の第三者が盗んだとしても、その復号化を行えないということを意味する。本願発明では、第1通信装置と第2通信装置とが、第2通信装置から第1通信装置に送られた解の後に生成された幾つめの解を共通鍵の暗号化と復号化に用いるかは、第1通信装置と第2通信装置の間で最初から決定しておくことができる。例えば、第2通信装置から第1通信装置に送られた解の次に両者で発生された解を用いるとか、5番目に発生した解を用いるとか、そういう取極めを両者の間で予めしておくことができる。また、第2通信装置から第1通信装置に送られた解或いはそれと一緒に送られたデータ等に依存させるようにして、何番目に発生した解を第1通信装置での共通鍵の暗号化と第2通信装置での共通鍵の復号化に用いるかを变化させることも可能である。更にいえば、第1通信装置が暗号化に使う解と、第2通信装置が復号化に用いる解とは、それぞれ複数であっても良い。この場合には例えば、第1通信装置が共通鍵の暗号化に用いる鍵を、第2通信装置から第1通信装置に送られた解の後の1番目と4番目に発生したもの、第2通信装置が共通鍵の復号化に用いる解も、第2通信装置から第1通信装置に送られた解の後の1番目と4番目に発生したもの、といった取極めを予めしておくことができる。つまり、第1通信装置と第2通信装置で用いられる解は、その数とそれが生成された順番とが共通するものである必要があり、その数と順番についての取極めを第1通信装置と第2通信装置との間で予めしておく必要がある。第1通信装置が暗号化に使う

解と、第2通信装置が復号化に用いる解とを複数にすれば、第三者が暗号化された共通鍵を復号化することが益々難しくなる。

他方、前記第2通信装置を正当なものと認証したとの通知を前記第1通信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理を実行した場合、つまり、前記第2通信装置が前記共通鍵を暗号化した場合には、前記第2通信装置から前記第1通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信するとともに、暗号化された前記共通鍵を受取った前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程を実行するようにすることも可能である。この場合において、第2通信装置が暗号化に用いる解、及び第1通信装置が復号化に用いる解はともに、第2通信装置の認証に使われた解ではなく、その後第1通信装置及び第2通信装置の解生成手段で生成された解である。これらの解は、第1通信装置又は第2通信装置の内部にのみ存在するものであって、ネットワークを経由して送信されない。したがって、この場合においても、第三者はこの解を盗み取ることが事実上できない。

以上、2つの処理のいずれかが実行されることにより、前記第1通信装置と前記第2通信装置で共通鍵が共有されることになる。共有されることになった前記共通鍵を用いて、前記第1通信装置と、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程が最後に実行される。かかる過程は、既に述べた通り、SSL通信で現在用いられている上記(3)の処理をそのまま踏襲することが可能である。第三者に共通鍵が盗み取られていないのであれば、この暗号化通信は安全である。

[0010] なお、上述の通信方法では、基本的に悪意のある第三者が、MITMAで、第2通信装置と第1通信装置との間に入り込むことはできない。第三者が仮に第

2 通信装置と第 1 通信装置との間に入り込んだ場合でも、第 2 通信装置が持つ解生成手段と同じ解生成手段を持たない第三者は、正当な第 1 通信装置が行う上述の認証を行うことができないからである。もっとも、悪意の第三者は、送られて来た解が正当か否かに関わらず、とりあえず第 2 通信装置を正当なものと認証してしまうということも考えられる。そうすると、特に第 2 通信装置が持っていた共通鍵を第 2 通信装置から第 1 通信装置に暗号化して送る場合には、第 2 通信装置の共通鍵を第三者に盗まれる可能性がある。そのようなことを防ぐには、認証を行った第 1 通信装置が第 2 通信装置に対して第 2 通信装置を正当なものと認証したと通知する場合に、その通知と同時にそうでなくても良いが、第 1 通信装置の解生成手段で生成された解を第 2 通信装置に送信するようにすることができる。その場合、第 2 通信装置は第 1 通信装置から解を受取り、その解と、第 2 通信装置の解生成手段で生成した解とを比較し、両者が一致した場合にはその第 1 通信装置が適正なものと認証するようにすることができる。第 1 通信装置と第 2 通信装置が持つ解生成手段は上述のように共通の解を連続して生成することができるものであるから、正当な第 1 通信装置が正当な第 2 通信装置と共通の解を作れるのと同様に、正当な第 2 通信装置は正当な第 1 通信装置と共通の解を作ることができる。悪意の第三者は第 2 通信装置が作れるのと共通の解を作ることができないから、第 1 通信装置側での第 2 通信装置の認証だけでなく、第 2 通信装置側での第 1 通信装置の認証をも行うようにすることで、MITMAが成功する可能性は、殆ど 0 になる。

この場合、第 1 通信装置が第 2 通信装置に送信する解は、第 1 通信装置又は第 2 通信装置で共通鍵を暗号化し、また暗号化された共通鍵を復号化するのに用いられる解としては用いられない。第 1 通信装置が第 2 通信装置に送信する解は、第 1 通信装置又は第 2 通信装置で共通鍵を暗号化し、また暗号化された共通鍵を復号化するのに用いられる解より先に生成された解でも良いし、それらよりも後に生成された解でも良いが、いずれにせよ第 2 通信装置が第 1 通信装置に送った解よりも後に生成された解とすることができる。

[0011] 本願発明は、第2通信装置で実行される通信方法と捉えることもできる。
かかる通信方法の効果は上記のとおりである。

その方法は例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置で実行される通信方法である。

そしてこの通信方法は、前記第2通信装置が実行する、以下の過程を含む。

その過程は、その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証し、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理が実行された後に、前記第1通信装置から暗号化された前記共通鍵を前記ネットワークを介して受取る過程、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、暗号化された前記共通鍵を、前記第1通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

かかる通信方法では、上述の通り、前記第1通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、前記第2通信装置が、暗号化された前記共通鍵を復号化

する処理を実行するために、その解生成手段で生成された解を複数用いてもよい。

[0012] 本願発明を、第2通信装置で実行される通信方法と捉える場合、その通信方法は以下のように捉えることもできる。かかる通信方法の効果は上記のとおりである。

その方法は例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置で実行される通信方法である。

そしてこの通信方法は、前記第2通信装置が実行する、以下の過程を含む。

その過程は、その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証し、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置から前記第2通信装置が正当なものだと認証されたという通知を前記ネットワークを介して受取る過程、前記通知を受取った後に、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、暗号化した共通鍵を、前記第1通信装置へと前記ネットワークを介して送信する過程、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する処理を

実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

かかる通信方法では、上述の通り、前記第2通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、前記第1通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いてもよい。

[0013] 本願発明は、第1通信装置で実行される通信方法と捉えることもできる。かかる通信方法の効果は上記のとおりである。

その方法は例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置で実行される通信方法である。

そしてこの通信方法は、前記第1通信装置が実行する、以下の過程を含む。

その過程は、前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信する過程、暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2

つ目以降の予め定められた条件下で生成された解を用いて、暗号化された前記共通鍵を、前記第 1 通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化することによって、前記第 1 通信装置と前記第 2 通信装置で共有されることになった前記共通鍵を用いて、前記第 2 通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

かかる通信方法では、上述の通り、前記第 1 通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、前記第 2 通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いてもよい。

[0014] 本願発明を、第 1 通信装置で実行される通信方法と捉える場合、その通信方法は以下のように捉えることもできる。かかる通信方法の効果は上記のとおりである。

その方法は例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第 1 通信装置と第 2 通信装置とを含んで構成される暗号化通信システムの前記第 1 通信装置で実行される通信方法である。

そしてこの通信方法は、前記第 1 通信装置が実行する、以下の過程を含む。

その過程は、前記第 2 通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、前記第 1 通信装置の解生成手段で解を生成させ、前記第 1 通信装置の解生成手段で生成した解と、前記第 2 通信装置から受取った解とを比較して、両者が一致した場合には、前記第 2 通信装置を正当なものと認証する過程、前記第 2 通信装置が正当だとの認証が前記第 1 通信装置で行われた場合に、前記第 2 通信装置を正当なものと認証したとの通知を前記ネットワークを介して前記第 2 通信装置に送る過程、前記第 2 通信装置を正当なものと認証したとの通知を前記第 1 通

信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理を行った後に、前記第2通信装置から前記ネットワークを介して送信された暗号化された前記共通鍵を受取る過程、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、前記第2通信装置から受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

かかる通信方法では、上述の通り、前記第2通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、前記第1通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いてもよい。

[0015] 本願発明は、第1通信装置との組合せにより、暗号化通信システムを構成するための、ネットワークに接続可能とされた第2通信装置と捉えることもできる。かかる第2通信装置の効果は上記のとおりである。

第2通信装置は例えば、解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いた暗号化を行うことができる第1通信装置第1暗号化復号化手段と、認証手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、を備えており、所定のネットワークと接続可能とされている第1通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第2通信装置である。

そして、第2通信装置は、前記第1通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続し

て生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第1通信装置第1暗号化復号化手段で行われるのと同じ復号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えている。

また、第2通信装置は、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して前記第1通信装置に送るようになっており、前記第1通信装置は、前記第2通信装置から前記ネットワークを介して前記解を受取り、前記第1通信装置解生成手段で解を生成させ、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっており、前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第1通信装置解生成手段が2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて自らが持つ共通鍵を前記第1通信装置第1暗号化復号化手段で暗号化する処理を実行して、暗号化された前記共通鍵を前記ネットワークを介して前記第2通信装置に送るようになっており、前記第2通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第2通信装置解生成手段によって生成された解を用いて、前記第1通信装置から受取った暗号化された前記共通鍵を前記第2通信装置第1暗号化復号化手段で復号化するようになっており、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第1通信装置との間で共通鍵方式の暗号化通信を行うようになっている。

[0016] 本願発明を、第1通信装置との組合せにより、暗号化通信システムを構成するための、ネットワークに接続可能とされた第2通信装置と捉える場合、その第2通信装置は以下のように捉えることもできる。かかる第2通信装置の効果は上記のとおりである。

その第2通信装置は例えば、解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いた復号化を行うことができる第1通信装置第1暗号化復号化手段と、認証手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、を備えており、所定のネットワークと接続可能とされている第1通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第2通信装置である。

そして、第2通信装置は、前記第1通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第1通信装置第1暗号化復号化手段で行われるのと同じ暗号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えている。

また、第2通信装置は、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して前記第1通信装置に送るようになっており、前記第1通信装置は、前記第2通信装置から前記ネットワークを介して前記解を受取り、前記第1通信装置解生成手段で解を生成させ、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっており、前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第2通信装置を正当なものと認証

したとの通知を前記ネットワークを介して前記第2通信装置に送るようになっており、前記通知を前記第1通信装置から受けた前記第2通信装置の前記第2通信装置解生成手段が2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を前記第2通信装置第1暗号化復号化手段で暗号化するとともに暗号化された前記共通鍵を前記ネットワークを介して前記第1通信装置に送るようになっており、前記第1通信装置は、前記第1通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第1通信装置との間で共通鍵方式の暗号化通信を行うようになっている。

[0017] 本願発明は、第2通信装置との組合せにより、暗号化通信システムを構成するための、ネットワークに接続可能とされた第1通信装置と捉えることもできる。かかる第1通信装置の効果は上記のとおりである。

第1通信装置は例えば、解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いた復号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えており、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して前記第1通信装置に送るようになっている、所定のネットワークと接続可能とされている第2通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第1通信装置である。

そして、第1通信装置は、前記第2通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第2通信装置第1暗号化復号化手段で行われるのと同じ暗号化を行うことができる第1通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものとして認証するようになっている認証手段と、を備えている。

また、第1通信装置は、前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第1通信装置解生成手段が2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて自らが持つ共通鍵を前記第1通信装置第1暗号化復号化手段で暗号化する処理を実行して、暗号化された前記共通鍵を前記ネットワークを介して前記第2通信装置に送るようになっており、前記第2通信装置は、前記第2通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第2通信装置解生成手段によって生成された解を用いて、前記第1通信装置から受取った暗号化された前記共通鍵を前記第2通信装置第1暗号化復号化手段で復号化するようになっており、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第2通信装置との間で共通鍵方式の暗号化通信を行うようになっている。

[0018] 本願発明を、第2通信装置との組合せにより、暗号化通信システムを構成するための、ネットワークに接続可能とされた第1通信装置と捉える場合、

その第1通信装置は以下のように捉えることもできる。かかる第1通信装置の効果は上記のとおりである。

第1通信装置は例えば、解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いた暗号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えており、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して前記第1通信装置に送るようになっている、所定のネットワークと接続可能とされている第2通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第1通信装置である。

そして、第1通信装置は、前記第2通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第2通信装置第1暗号化復号化手段で行われるのと同じ復号化を行うことができる第1通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するようになっている認証手段と、を備えている。

また、第1通信装置は、前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第2通信装置を正当なものと認証したとの通知を前記ネットワークを介して前記第2通信装置に送るようになっており、前記第2通信装置は、前記通知を前記第1通信装置から受けたら、前記第2通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を前記第2通信装置第1暗号化復号化手段で暗号化するとともに暗号化された前記

共通鍵を前記ネットワークを介して前記第1通信装置に送るようになっており、前記第1通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第2通信装置との間で共通鍵方式の暗号化通信を行うようになっている。

[0019] 本願発明は、汎用のコンピュータを、本願発明の第2通信装置として機能させるためのコンピュータプログラムとして捉えることもできる。かかるコンピュータプログラムの効果は上記のとおりである。

そのコンピュータプログラムは例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置として、コンピュータを機能させるためのコンピュータプログラムである。

そしてこのコンピュータプログラムは、前記コンピュータに以下の過程を実行させるためのものである。

その過程は、その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証し、前記第2通信装置が正当だとの認証が前記第

1 通信装置で行われた場合に、前記第 1 通信装置が、その解生成手段で 2 つ目或いはそれ以降の解を生成するとともに、2 つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理が実行された後に、前記第 1 通信装置から暗号化された前記共通鍵を前記ネットワークを介して受取る過程、その解生成手段で 2 つ目或いはそれ以降の解を生成するとともに、2 つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を復号化する過程、以上により前記第 1 通信装置と前記第 2 通信装置で共有されることになった前記共通鍵を用いて、前記第 1 通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

[0020] 本願発明を、汎用のコンピュータを、本願発明の第 2 通信装置として機能させるためのコンピュータプログラムとして捉える場合、そのコンピュータプログラムは以下のように捉えることもできる。かかるコンピュータプログラムの効果は上記のとおりである。

そのコンピュータプログラムは例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第 1 通信装置と第 2 通信装置とを含んで構成される暗号化通信システムの前記第 2 通信装置として、コンピュータを機能させるためのコンピュータプログラムである。

そしてこのコンピュータプログラムは、前記コンピュータに以下の過程を実行させるためのものである。

その過程は、その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第 1 通信装置に送信する過程、前記第 1 通信装置が、前記第 2 通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第 1 通信装置の解生成手段で生成した解と、前記第 2 通信装置から受取った解とを比較して、両者が一致した場合には、前記第 2 通信装置を正当なものと認証し、前記第 2 通信装置が正当だとの認証が前記第 1 通信装置で行われた場合に、前記第 1 通信装置から前記第 2 通信装置が正

当なものだと認証されたという通知を前記ネットワークを介して受取る過程、前記通知を受取った後に、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、暗号化した共通鍵を、前記第1通信装置へと前記ネットワークを介して送信する過程、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を復号化する処理を実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

[0021] 本願発明は、汎用のコンピュータを、本願発明の第1通信装置として機能させるためのコンピュータプログラムとして捉えることもできる。かかるコンピュータプログラムの効果は上記のとおりである。

そのコンピュータプログラムは例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置として、コンピュータを機能させるためのコンピュータプログラムである。

そしてこのコンピュータプログラムは、前記コンピュータに以下の過程を実行させるためのものである。

その過程は、前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、その解生成手段で2つ目

或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信する過程、暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を復号化することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

[0022] 本願発明を、汎用のコンピュータを、本願発明の第1通信装置として機能させるためのコンピュータプログラムとして捉える場合、そのコンピュータプログラムは以下のように捉えることもできる。かかるコンピュータプログラムの効果は上記のとおりである。

そのコンピュータプログラムは例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置として、コンピュータを機能させるためのコンピュータプログラムである。

そしてこのコンピュータプログラムは、前記コンピュータに以下の過程を実行させるためのものである。

その過程は、前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第2通信装置を正当なものと認証したとの通知を前記ネットワークを介して前記第2通信装置に

送る過程、前記第2通信装置を正当なものと認証したとの通知を前記第1通信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理を行った後に、前記第2通信装置から前記ネットワークを介して送信された暗号化された前記共通鍵を受取る過程、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、第2通信装置から受取った暗号化された前記共通鍵を復号化する過程、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、である。

[0023] コンピュータを本願発明の第2通信装置として機能させるための上述のコンピュータプログラムは、前記共通鍵方式の暗号化通信を行う場合の暗号化と復号化を、第2通信装置を構成する前記コンピュータ上における、前記コンピュータ上で実行される暗号化の対象となる平文のデータを扱う所定のアプリケーションと、TCP/IPとの間で実行させるようになっているとともに、前記アプリケーションで生成された平文を暗号化してから前記第1通信装置に送信するために前記TCP/IPに渡し、前記TCP/IPから渡された前記第1通信装置から送られてきた暗号化されたデータを平文に復号化してから前記アプリケーションに渡すようになっていてもよい。

現在のSSL通信のコンピュータプログラムは、アプリケーションと、TCP/IPとの間で暗号化と復号化とを行うようになっている。上述の如きコンピュータプログラムであれば、現在のSSL通信用のコンピュータプログラムに置換するのが容易である。

[0024] コンピュータを本願発明の第1通信装置として機能させるための上述のコンピュータプログラムは、前記共通鍵方式の暗号化通信を行う場合の暗号化と復号化を、第1通信装置を構成する前記コンピュータ上における、前記コンピュータ上で実行される暗号化の対象となる平文のデータを扱う所定のア

アプリケーションと、TCP/IPとの間で実行させるようになっているとともに、前記アプリケーションで生成された平文を暗号化してから前記第2通信装置に送信するために前記TCP/IPに渡し、前記TCP/IPから渡された前記第2通信装置から送られてきた暗号化されたデータを平文に復号化してから前記アプリケーションに渡すようになっていてもよい。

これによっても、本願発明の上記コンピュータプログラムで、現在のSSL通信のコンピュータプログラムを置換するのが容易になる。

[0025] 次に、本願の更に異なる態様について説明する。ここまでの発明は、第2通信装置から第1通信装置に解を送り、第1通信装置でまず第2通信装置から第1通信装置に送られてきた解に基いて、第2通信装置についての認証を行い、かかる認証を行う、そしてその後に、第1通信装置又は第2通信装置の一方に存在した共通鍵を暗号化し、それらの他方に対してそれを送信した上でそれらの他方において暗号化された共通鍵を復号化することにより、第1通信装置と第2通信装置で共通鍵を共有する、というものであった。

これに代えて、第2通信装置から第1通信装置に対して、第1通信装置で上述の認証が行われる前に、解と暗号化された鍵を送ってしまうことも可能である。本願の第3の態様とでもいうべき以下に説明する発明はすべてそのような発明である。

[0026] 第3の態様とでもいうべき発明の1つとして、第2通信装置が実行する方法を提案する。

その方法は、例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置で実行される通信方法である。

そしてその方法は、前記第2通信装置が実行する、その解生成手段で複数の解を生成させ、その解のうちの1つと、その解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものと、を前記ネットワークを介して前記第

1 通信装置に送信する過程、前記第 1 通信装置が、前記第 2 通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で複数の解を生成させ、前記第 1 通信装置の解生成手段で生成した解であって前記第 2 通信装置から送られてきた解が前記第 2 通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第 2 通信装置から受取った解とを比較して、両者が一致した場合には、前記第 2 通信装置を正当なものと認証するとともに、前記第 1 通信装置の解生成手段で生成した解であって前記第 2 通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第 2 通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第 2 通信装置から前記第 1 通信装置が受取った暗号化された前記共通鍵を、前記第 2 通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する処理を実行することによって、前記第 1 通信装置と前記第 2 通信装置で共有されることになった前記共通鍵を用いて、前記第 1 通信装置との間で、共通鍵方式の暗号化通信を行う過程、を含んでなる。

[0027] 第 3 の態様とでもいうべき発明の 1 つとして、第 1 通信装置が実行する方法を提案する。

その方法は、例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段とともに備える第 1 通信装置と第 2 通信装置とを含んで構成される暗号化通信システムの前記第 1 通信装置で実行される通信方法である。

そしてその方法は、前記第 1 通信装置が実行する、前記第 2 通信装置が、その解生成手段で複数の解を生成させ、その解のうちの 1 つと、その解のうちの他の 1 つを用いて自らが持つ共通鍵を暗号化したものとの前記ネットワークを介して送ってきた場合に前記解と暗号化された共通鍵とを受取る過程、前記第 1 通信装置の解生成手段で複数の解を生成させ、前記第 1 通信装置の解生成手段で生成した解であって前記第 2 通信装置から送られてきた解が

前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、を含んでなる。

[0028] 第3の態様とでもいうべき発明の1つとして、第2通信装置を提案する。

第2通信装置は、例えば、解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いた暗号化と復号化を行うことができる第1通信装置第1暗号化復号化手段と、認証手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、を備えており、所定のネットワークと接続可能とされている第1通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第2通信装置であって、前記第1通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第1通信装置第1暗号化復号化手段で行われるのと同じ暗号化と復号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えている。

そして、第2通信装置は、前記第2通信装置解生成手段で生成した複数の

解のうちの1つと、前記第2通信装置解生成手段で生成した解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものとを前記ネットワークを介して前記第1通信装置に送るようになっており、前記第1通信装置は、前記第2通信装置から前記ネットワークを介して前記解と暗号化された前記共通鍵とを受取り、前記第1通信装置解生成手段で複数の解を生成させ、前記第1通信装置解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっており、前記第1通信装置解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化の際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第1通信装置との間で共通鍵方式の暗号化通信を行うようになっている。

[0029] 第3の態様とでもいうべき発明の1つとして、第1通信装置が実行する方法を提案する。

第1通信装置は、例えば、解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いた暗号化と復号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えており、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して第1通信装置に送るようになってい

る、所定のネットワークと接続可能とされている第2通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第1通信装置であって、前記第2通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第2通信装置第1暗号化復号化手段で行われるのと同じ暗号化と復号化を行うことのできる第1通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するようになっている認証手段と、を備えている。

そして、第1通信装置は、前記第2通信装置が、前記第2通信装置解生成手段で生成した複数の解のうちの1つと、前記第2通信装置解生成手段で生成した解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものとの前記ネットワークを介して前記第1通信装置に送ってきた場合に、それらを受取るようになっているとともに、前記第1通信装置解生成手段で複数の解を生成させ、前記第1通信装置解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっているとともに、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装

置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第2通信装置との間で共通鍵方式の暗号化通信を行うようになっている。

[0030] 第3の態様とでもいうべき発明の1つとして、汎用のコンピュータを第2通信装置として機能させるためのコンピュータプログラムを提案する。

そのコンピュータプログラムは、例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置として、コンピュータを機能させるためのコンピュータプログラムである。

そして、そのコンピュータプログラムは、前記コンピュータに、その解生成手段で複数の解を生成させ、その解のうちの1つと、その解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものと、を前記ネットワークを介して前記第1通信装置に送信する過程、前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で複数の解を生成させ、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するとともに、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する処理を実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記

共通鍵を用いて、前記第 1 通信装置との間で、共通鍵方式の暗号化通信を行う過程、を実行させるためのものとなっている。

[0031] 第 3 の態様とでもいうべき発明の 1 つとして、汎用のコンピュータを第 1 通信装置として機能させるためのコンピュータプログラムを提案する。

そのコンピュータプログラムは、例えば、所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第 1 通信装置と第 2 通信装置とを含んで構成される暗号化通信システムの前記第 1 通信装置として、コンピュータを機能させるためのコンピュータプログラムである。

そして、そのコンピュータプログラムは、前記コンピュータに、前記第 2 通信装置が、その解生成手段で複数の解を生成させ、その解のうちの 1 つと、その解のうちの他の 1 つを用いて自らが持つ共通鍵を暗号化したものとの前記ネットワークを介して送ってきた場合に前記解と暗号化された共通鍵とを受取る過程、前記第 1 通信装置の解生成手段で複数の解を生成させ、前記第 1 通信装置の解生成手段で生成した解であって前記第 2 通信装置から送られてきた解が前記第 2 通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第 2 通信装置から受取った解とを比較して、両者が一致した場合には、前記第 2 通信装置を正当なものと認証する過程、前記第 1 通信装置の解生成手段で生成した解であって前記第 2 通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第 2 通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第 2 通信装置から受取った暗号化された前記共通鍵を、前記第 2 通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、以上により前記第 1 通信装置と前記第 2 通信装置で共有されることになった前記共通鍵を用いて、前記第 2 通信装置との間で、共通鍵方式の暗号化通信を行う過程、を実行させるためのものとなっている。

図面の簡単な説明

[0032] [図1]第1実施形態による通信システムの全体構成を示す図。

[図2]図1に示した通信システムに含まれるクライアントの外観を示す図。

[図3]図1に示した通信システムに含まれるクライアントのハードウェア構成を示す図。

[図4]図1に示した通信システムに含まれるクライアントの内部に生成される機能ブロックを示すブロック図。

[図5]図4に示した暗号化復号化部の内部に生成される機能ブロックを示すブロック図。

[図6]図1に示した通信システムに含まれるサーバの内部に生成される機能ブロックを示すブロック図。

[図7]図6に示した暗号化復号化部の内部に生成される機能ブロックを示すブロック図。

[図8]図1に示した通信システムで通信が行われるときに実行される処理の流れを示す図。

[図9]変形例1のクライアントの暗号化復号化部の内部に生成される機能ブロックを示す図。

[図10]変形例1の通信システムで通信が行われるときに実行される処理の流れを示す図。

[図11]第2実施形態のクライアントの暗号化復号化部の内部に生成される機能ブロックを示す図。

[図12]第2実施形態のサーバの暗号化復号化部の内部に生成される機能ブロックを示す図。

[図13]第2実施形態の通信システムで通信が行われるときに実行される処理の流れを示す図。

[図14]第3実施形態の通信システムで通信が行われるときに実行される処理の流れを示す図。

発明を実施するための形態

[0033] 以下、本発明の第1～第3実施形態について説明する。各実施形態、変形

例の説明で同じ対象には同一の符号を付すものとし、重複する説明は場合により省略するものとする。

[0034] 《第1実施形態》

図1に、第1実施形態の通信システムの全体構成を概略で示す。

通信システムは、複数のクライアント100-1～100-N（以後、単に、「クライアント100」と記載する場合もある。）、及びサーバ200を含んで構成されている。これらはすべて、ネットワーク400に接続可能とされている。

ネットワーク400は、これには限られないが、この実施形態ではインターネットである。

この実施形態におけるクライアント100は、本願でいう第2通信装置に相当するものである。また、この実施形態におけるサーバ200は本願でいう第2通信装置に相当する。もっとも本願における第1通信装置と第2通信装置に相当するサーバ200とクライアント100とは、いわゆるサーバとクライアントの関係である必要はなく、2つの互いに対等な通信装置であっても構わない。

[0035] クライアント100は、本願でいうクライアントに相当するものであり、コンピュータを含んでいる。より詳細には、この実施形態におけるクライアント100は、汎用のコンピュータにより構成されている。

[0036] 次に、クライアント100の構成を説明する。各クライアント100-1～100-Nの構成は、本願発明との関連でいえば同じである。

クライアント100は、携帯電話、スマートフォン、タブレット、ノート型パソコン、デスクトップ型パソコン等である。それらはすべて、ネットワーク400を介しての通信が可能なものであり、また後述するコンピュータプログラムをインストールすることによって後述する機能ブロックをその内部に生成し、そして後述する処理を実行できるものであることが求められ、それが可能であるのであればそれ以外の仕様は特に問わない。

例えば、クライアント100がスマートフォンかタブレットなのであれば

、スマートフォンとしてのクライアント１００は例えば、Apple Japan 合同会社が製造、販売を行う iPhone で良いし、タブレットとしてのクライアント１００は例えば、Apple Japan 合同会社が製造、販売を行う iPad でよい。以下、これには限られないが、クライアント１００がスマートフォンであることとして話を進める。

[0037] クライアント１００の外観の一例を図２に示す。

クライアント１００は、ディスプレイ１０１を備えている。ディスプレイ１０１は、静止画又は動画を表示するためのものであり、公知、或いは周知のものをを用いることができる。ディスプレイ１０１は例えば、液晶ディスプレイである。クライアント１００は、また入力装置１０２を備えている。入力装置１０２は、ユーザが所望の入力をクライアント１００に対して行うためのものである。入力装置１０２は、公知或いは周知のものをを用いることができる。この実施形態におけるクライアント１００の入力装置１０２はボタン式のものとなっているが、これには限られず、テンキー、キーボード、トラックボール、マウスなどを用いることも可能である。特に、クライアント１００がノート型パソコン、デスクトップ型パソコンである場合には、入力装置１０２はキーボードや、マウス等になるであろう。また、ディスプレイ１０１がタッチパネルである場合、ディスプレイ１０１は入力装置１０２の機能を兼ねることになり、この実施形態ではそうされている。

[0038] クライアント１００のハードウェア構成を、図３に示す。

ハードウェアには、CPU (central processing unit) １１１、ROM (read only memory) １１２、RAM (random access memory) １１３、インターフェイス１１４が含まれており、これらはバス１１６によって相互に接続されている。

CPU １１１は、演算を行う演算装置である。CPU １１１は、例えば、ROM １１２、或いはRAM １１３に記録されたコンピュータプログラムを実行することにより、後述する処理を実行する。図示をしていないが、ハードウェアはHDD (hard disk drive) その他の大容量記録装置を備えていて

もよく、コンピュータプログラムは大容量記録装置に記録されていても構わない。

ここでいうコンピュータプログラムには、本願発明のクライアントとしてこのクライアント100を機能させるためのコンピュータプログラムが少なくとも含まれる。このコンピュータプログラムは、クライアント100にプリインストールされていたものであっても良いし、事後的にインストールされたものであっても良い。このコンピュータプログラムのクライアント100へのインストールは、メモリカード等の所定の記録媒体を介して行なわれても良いし、LAN或いはインターネットなどのネットワークを介して行なわれても構わない。

ROM112は、CPU111が後述する処理を実行するために必要なコンピュータプログラムやデータを記録している。ROM112に記録されたコンピュータプログラムとしては、これに限られず、クライアント100がスマートフォンであれば、クライアントをスマートフォンとして機能させるために必要な、例えば、通話や電子メールを実行するためのコンピュータプログラムやデータが記録されている。クライアント100は、また、ネットワーク400を介して受取ったデータに基づいて、ホームページを閲覧することも可能とされており、それを可能とするための公知のwebブラウザを実装している。

RAM113は、CPU111が処理を行うために必要なワーク領域を提供する。

インターフェイス114は、バス116で接続されたCPU111やRAM113等と外部との間でデータのやり取りを行うものである。インターフェイス114には、上述のディスプレイ101と、入力装置102とが接続されている。入力装置102から入力された操作内容は、インターフェイス114からバス116に入力されるようになっている。また、周知のようにディスプレイ101に画像を表示するための画像データは、インターフェイス114から、ディスプレイ101に出力されるようになっている。インタ

ーフェイス 114 は、また、インターネットであるネットワーク 400 を介して外部と通信を行うための公知の手段である送受信機構（図示を省略）に接続されており、それにより、クライアント 100 は、ネットワーク 400 を介してデータを送信することと、ネットワーク 400 を介してデータを受信することとが可能になっている。かかるネットワーク 400 を介してのデータの送受信は、有線で行われる場合もあるが無線で行われる場合もある。例えば、クライアント 100 がスマートフォンである場合には、かかる通信は無線で行われるのが通常であろう。それが可能な限り、送受信機構の構成は、公知或いは周知のものとすることができる。送受信機構がネットワーク 400 から受取ったデータは、インターフェイス 114 により受取られるようになっており、インターフェイス 114 から送受信機構にわたされたデータは、送受信機構によって、ネットワーク 400 を介して外部、例えば、サーバ 200 に送られるようになっている。

[0039] CPU 111 がコンピュータプログラムを実行することにより、クライアント 100 内部には、図 4 で示されたような機能ブロックが生成される。なお、以下の機能ブロックは、クライアント 100 を本願発明のクライアントとして機能させるための上述のコンピュータプログラム単体の機能により生成されていても良いが、上述のコンピュータプログラムと、クライアント 100 にインストールされた OS その他のコンピュータプログラムとの協働により生成されても良い。

クライアント 100 内には、本願発明の機能との関係で、アプリケーション 121 と、暗号化復号化部 122 と、送受信部 123 とが生成される。

もっとも、これらのうちアプリケーション 121 は、公知のブラウザのソフトウェア、電子メールのソフトウェア等であり、また、送受信部 123 はネットワーク 400 を介してのデータの送受信を行うソフトウェアであって、いずれもが本願発明でいうコンピュータプログラムの機能によって生成されるものではない。

アプリケーション 121 は、クライアント 100 からサーバ 200 に暗号

化して送られるデータの元となる暗号化されていないデータを生成するものであり、またサーバ200からクライアント100へ暗号化して送られたデータを復号化してから使用するものである。そのようなものである限り、アプリケーション121は上で例示したものに限られない。アプリケーション121はインターフェイス114と接続されており、インターフェイス114を介して受取る入力装置102からの操作内容に関するデータにしたがって動作する。アプリケーション121はその動作の結果、暗号化してネットワーク400を介してサーバ200に送るべき平文のデータを生成する。このデータは暗号化復号化部122に送られるようになっている。アプリケーション121は、また、動作の結果、例えば上述した画像データを生成する。画像データはインターフェイス114に送られ、そこからディスプレイ101に送られるようになっている。

また、送受信部123は、サーバ200等とネットワーク400を介して送受信を行う機能ブロックであって、例えば相手装置の宛先を決定したり、送信されるデータに所定の内容を書き込んだりという、公知、周知の機能を有している。送受信部123は、少なくともTCP/IPを用いてネットワーク400を介しての通信を行えるようになっている。送受信部123は、送受信機構がネットワーク400から受取ったデータをインターフェイス114を介して受取る。送受信部123は、インターフェイス114を介して送受信機構から受取ったデータを暗号化復号化部122へ送るようになっている。また、送受信部123は、暗号化復号化部122からデータを受取る場合がある。送受信部123はその暗号化復号化部122から受取ったデータをインターフェイス114に送り、送受信機構からネットワーク400を介してサーバ200へ送るようになっている。

[0040] 暗号化復号化部122は、簡単にいうと、送受信部123から受取ったデータのうち必要なものに復号化の処理を行い、また、アプリケーション121から受取ったデータのうちの必要なものに対して暗号化の処理を行う機能を有するとともに、サーバ200との間のクライアント100の認証に必要

な処理を行うものである。つまり、暗号化復号化部 122 は、本願発明におけるクライアント 100 とサーバ 200 の間の暗号化通信の中心的な役割を担うものであり、本願発明のコンピュータをクライアントとして機能させるためのコンピュータプログラムにより、クライアント 100 内に生成されるものであると言える。

また、暗号化復号化部 122 には、入力装置 102 から入力された操作内容についてのデータが、インターフェイス 114 を介して入力される場合がある。

[0041] 暗号化復号化部 122 の中には入力部 122 A、主制御部 122 B、クライアント解生成部 122 C、解データ記録部 122 D、クライアント第 1 暗号化復号化部 122 E、クライアント第 2 暗号化復号化部 122 F、及び出力部 122 G が生成される。

[0042] 入力部 122 A は、インターフェイス 114 又はアプリケーション 121 からデータを受取るものである。インターフェイス 114 を介して入力装置 102 から操作内容についてのデータが入力された場合には、入力部 122 A は、それを主制御部 122 B に送るようになっている。また、入力部 122 A には後述するように、サーバ 200 から送られてきた暗号化されたデータ、それも共通鍵で暗号化されたデータが、インターフェイス 114、送受信部 123 を介して送られてくることがある。そのデータを受取ったら入力部 122 A は、それをクライアント第 2 暗号化復号化部 122 F に送るようになっている。入力部 122 A には、また、後述するように、サーバ 200 から暗号化された状態で送られてきた共通鍵のデータが、インターフェイス 114、送受信部 123 を介して入力される場合がある。かかるデータを受取ったら入力部 122 A は、それをクライアント第 1 暗号化復号化部 122 E に送るようになっている。入力部 122 A はまた、インターフェイス 114、送受信部 123 を介してアプリケーション 121 から送られてきたデータを受取ることがある。このデータは後述するように、暗号化してからサーバ 200 に送られることを意図したものであるが、このデータを受取ったら

入力部 1 2 2 A は、そのデータをクライアント第 2 暗号化復号化部 1 2 2 F に送るようになっている。

[0043] 主制御部 1 2 2 B は、暗号化復号化部 1 2 2 全体の制御を行うものである。主制御部 1 2 2 B は上述のように、入力部 1 2 2 A から操作内容についてのデータを受取る場合があり、それを受取った場合には、それに基づいた指示を適宜暗号化復号化部 1 2 2 内の機能ブロックに送るようになっている。例えば、あるデータを受取った場合、主制御部 1 2 2 B は、クライアント解生成部 1 2 2 C に対して解を生成せよとの指示を送るようになっている。

[0044] クライアント解生成部 1 2 2 C は、解を連続して生成することのできるものとされている。解は、数字、文字、記号の少なくとも 1 つの羅列である。後述するように、サーバ 2 0 0 にはサーバ解生成部が存在し、サーバ解生成部も連続して解を生成するようになっているが、サーバ解生成部が生成する解と、クライアント解生成部 1 2 2 C が生成する解とを比較した場合、共通条件下で生成された解同士を比較すれば両者は常に一致するようになっている。簡単に言えば、クライアント解生成部 1 2 2 C と、サーバ解生成部とは同期されており、或いはクライアント解生成部 1 2 2 C で生成される解と、サーバ解生成部で生成される解とは同期されている。それが可能な限り、クライアント解生成部 1 2 2 C 及びサーバ解生成部で解を生成する方法はどのようなものでもよい。

クライアント解生成部 1 2 2 C とサーバ解生成部で解を生成する方法が、上述の条件が充足される限りどのようなものでもよいのは既に述べたとおりである。そのような技術は既に、ワンタイムパスワードの生成の技術として完成し、実用されている。クライアント解生成部 1 2 2 C 及びサーバ解生成部では、そのような技術を流用することができる。サーバ解生成部でも同じであるからクライアント解生成部 1 2 2 C についてのみに言及するが、より詳細には、クライアント解生成部 1 2 2 C は、例えば、ある初期値に対して決められた演算を行うことで解を得て、次いでその解に対して再び決められた演算を行うことで次の解を得て、次いでその解に対して再び決められた演

算を行うことで次の解を得て…、という処理を繰り返すことで、連続して解を生成するものとすることができる。このような技術は、擬似乱数を生成するための技術として周知である。

解を生成するより具体的な方法について説明する。

解を生成するには、ある初期値（以下の、（a）、（c）のように2つ以上の場合もある）を用い、過去の値を所定の関数に代入することにより、新しい値を順次作るという方法を、解が必要となる度に実行すれば良い。そうすることにより、上記解を連続して生成することができる。この場合の解は、初期値依存性のある擬似乱数となる。

上述の解を作るのに使われる関数の例として、以下の（a）～（c）を挙げる。以下の（a）～（c）はいずれも、N番目の解である X_N を作るための式である。また、P、Q、R、Sは自然数である。

$$(a) \quad (X_N) = (X_{N-1})^P + (X_{N-2})^Q$$

$$(b) \quad (X_N) = (X_{N-1})^P$$

$$(c) \quad (X_N) = (X_{N-1})^P (X_{N-2})^Q (X_{N-3})^R (X_{N-4})^S$$

（a）は、過去の解2つを用い、それらをそれぞれP乗とQ乗したものを足し合わせることで、新しい解を生成する。なお、正確には、過去の解2つを用い、それらをP乗とQ乗したものを足し合わせると通常、桁数が増えるため、実際には得られた値のうちの頭から適当な桁数を抜き出す、末尾から適当な桁数を抜き出す、或いはその値のうちの適当な部分から適当な桁数を抜き出すこと等により、新しい解を生成する。

（b）は、過去の解1つを用い、それをP乗したものの桁数を上述のように整理したものを新しい解とするものである。

（c）は、過去の解4つを用い、それらをそれぞれP乗、Q乗、R乗、S乗したものの積を取り、その後上述したように桁数を整理したものを新しい解とするものである。

上述の（a）～（c）は解を生成するためのアルゴリズムの一例であり、解を生成する際にアルゴリズムに変化を加える、例えば、上述の（a）～（

c) を順番に用いる等の変化を加えることも可能である。また、上述の解に、時間依存性を与えれば、つまりそのときの時刻に合わせた変化を加えるようにすることもできる。

いずれにせよ、サーバ200にあるサーバ解生成部と、クライアント解生成部122Cとは、上述の如く、解を同期させられるようにされている。

これには限られないが、この実施形態のクライアント解生成部122Cは上記(a)のアルゴリズムを用いて解を生成することとしている。その場合、新しい解を生成するには、初期値乃至過去の解が必要となる。解データ記録部122Dには当初初期値が記録されており、クライアント解生成部122Cが新しい解を生成するたびに、初期値が新しい解により上書きされ、その新しい解が更に新しい解により上書きされるようになっている。解データ記録部122Dには、このように初期値又は解が記録されており、クライアント解生成部122Cは新しい解を生成するたびに、解データ記録部122Dから新しい解を読みだすようになっている。

クライアント解生成部122Cは、また、解を生成した場合、それをクライアント第1暗号化復号化部122E又は出力部122Gに送るようになっている。

[0045] クライアント第1暗号化復号化部122Eは、暗号化、復号化の処理を行えるようになっている。もっとも、この実施形態では、後述するように少なくとも復号化の処理を行えれば足りる。クライアント第1暗号化復号化部122Eは、サーバ200の後述するサーバ第1暗号化復号化部で暗号化されたデータを少なくとも復号化できるようになっている。クライアント第1暗号化復号化部122Eでの暗号化、復号化には、解が使われる。上述のようにクライアント解生成部122Cで生成された解はクライアント解生成部122Cからクライアント第1暗号化復号化部122Eに送られるが、その解はクライアント第1暗号化復号化部122Eで上述の復号化が行われる際に使用される。他方、クライアント第1暗号化復号化部122Eには、入力部122Aから暗号化された共通鍵のデータが送られてくる。この共通鍵のデ

ータは、後述するようにサーバ200から送られてくるものであり、これも後述するようにサーバ200のサーバ第1暗号化復号化部で暗号化されたものである。つまり、クライアント第1暗号化復号化部122Eは、この暗号化された共通鍵のデータを、解を用いて復号化することができるようになっている。

クライアント第1暗号化復号化部122Eは、復号化した共通鍵のデータを、クライアント第2暗号化復号化部122Fに送るようになっている。

[0046] クライアント第2暗号化復号化部122Fは、暗号化、復号化の処理を行うものである。ここで行われる暗号化、復号化の処理は、クライアント第1暗号化復号化部122Eから送られてきた共通鍵を用いて行われる。暗号化の対象となるのは、アプリケーション121から入力部122Aを介して送られてきた平文のデータであり、また復号化の対象となるのは、サーバ200から、ネットワーク400、送受信機構、インターフェイス114、入力部122Aを介して送られてきた暗号化されたデータである。

クライアント第2暗号化復号化部122Fで行われる暗号化、復号化の処理は共通鍵を用いて行われる共通鍵方式の暗号化、復号化であればどのようなものでもよく、例えばSSLの本願の背景技術で述べた(3)の通信で用いられている公知或いは周知の手法をこれに応用することができる。例えば、クライアント第2暗号化復号化部122Fは、DES暗号法を実行するものとすることができる。

クライアント第2暗号化復号化部122Fは、アプリケーション121から送られてきたデータを暗号化したものを出力部122Gに送るようになっているとともに、サーバ200から送られてきた暗号化されたデータを復号化したものを出力部122Gに送るようになっている。

[0047] 出力部122Gは、暗号化復号化部122内で生成されたデータを外部に出力するためのものである。

出力部122Gには、クライアント解生成部122Cから解が送られてくる場合があり、またクライアント第2暗号化復号化部122Fから、アプリ

ケーション 1 2 1 から送られてきたデータをクライアント第 2 暗号化復号化部 1 2 2 F で暗号化したものと、サーバ 2 0 0 から送られてきた暗号化されたデータをクライアント第 2 暗号化復号化部 1 2 2 F で復号化したものとを送られてくる場合がある。

出力部 1 2 2 G は、これらのうち、解と、アプリケーション 1 2 1 から送られてきたデータをクライアント第 2 暗号化復号化部 1 2 2 F で暗号化したものとを送受信部 1 2 3 を介してインターフェイス 1 1 4 に送っている。インターフェイス 1 1 4 に送られたこれらデータは、送受信機構、ネットワーク 4 0 0 を介してサーバ 2 0 0 に送られるようになっている。出力部 1 2 2 G は、また、サーバ 2 0 0 から送られてきた暗号化されたデータをクライアント第 2 暗号化復号化部 1 2 2 F で復号化したものをアプリケーション 1 2 1 に送っている。それらデータは、アプリケーション 1 2 1 で使用される。

[0048] 次に、サーバ 2 0 0 の構成について説明する。

サーバ 2 0 0 は、ハードウェアとして見た場合には、既存の公知又は周知のサーバで構わない。また、そのハードウェア構成も一般的なものでよく、大雑把に言えば、CPU 1 1 1、ROM 1 1 2、RAM 1 1 3、インターフェイス 1 1 4 をバス 1 1 6 で接続するという、クライアント 1 0 0 のハードウェア構成を踏襲することができる。もっとも、サーバ 2 0 0 は通常、HDD その他の大容量記録装置を有するのが一般的であろう。

サーバ 2 0 0 が備える CPU、ROM、RAM、インターフェイス、バス、及び大容量記録装置の構成、機能は、クライアント 1 0 0 におけるそれらの構成、機能と変わらない。また、サーバ 2 0 0 が備えるインターフェイスには、クライアント 1 0 0 が備えていたのと同様の、サーバ 2 0 0 外の機器とネットワーク 4 0 0 を介しての通信を行うための送受信機構が接続されている。サーバ 2 0 0 が備えるインターフェイスには、クライアント 1 0 0 が備えていたのと同様のディスプレイ、入力装置が接続されていても構わないが、本願とはあまり関係がないのでその説明は省略する。

[0049] サーバ200の内部におけるROM、大容量記録装置等に記録されていたコンピュータプログラムを実行することによって、サーバ200の内部には以下に説明するような機能ブロックが生成される。なお、以下の機能ブロックは、サーバ200を本願発明のサーバとして機能させるためのコンピュータプログラム単体の機能により生成されていても良いが、かかるコンピュータプログラムと、サーバ200にインストールされたOSその他のコンピュータプログラムとの協働により生成されても良い。また、上記コンピュータプログラムのサーバ200へのインストールは、メモリカード等の所定の記録媒体を介して行なわれても良いし、LAN或いはインターネットなどのネットワークを介して行なわれても構わない。これらの事情は、クライアント100の場合と同様である。

サーバ200内には、本願発明の機能との関係で、アプリケーション221と、暗号化復号化部222と、送受信部223とが生成される。

もっとも、これらのうちアプリケーション221は、クライアント100のブラウザに所望の画像を表示させるための公知のソフトウェア、クライアント100を操作するユーザの意思決定に基いてインターネットバンキングでの決済を実行するソフトウェア等であり、また、送受信部223はネットワーク400を介してのデータの送受信を行うソフトウェアであって、いずれもが本願発明でいうコンピュータプログラムの機能によって生成されるものではない。この事情は、クライアント100の場合と同様である。

アプリケーション221は、サーバ200からクライアント100に暗号化して送られるデータの元となる暗号化されていないデータを生成するものであり、またクライアント100からサーバ200へ暗号化して送られたデータを復号化してから使用するものである。そのようなものである限り、アプリケーション221は上で例示したものに限られない。アプリケーション221はインターフェイスと接続されており、インターフェイスを介して受取る入力装置からの操作内容に関するデータにしたがって、或いは予め作成されたプログラムにしたがって自動的に動作する。アプリケーション221

はその動作の結果、暗号化してネットワーク４００を介してクライアント１００に送るべき平文のデータを生成する。このデータは暗号化復号化部２２２に送られるようになっている。アプリケーション２２１は、また、動作の結果、例えば画像データを生成する場合がある。画像データはインターフェイスに送られ、そこから、サーバ２００のディスプレイに送られて画像を表示する。

また、送受信部２２３は、クライアント１００等とネットワーク４００を介して送受信を行う機能ブロックであって、例えば相手装置の宛先を決定したり、送信されるデータに所定の内容を書き込んだりという、公知、周知の機能を有している。送受信部２２３は、少なくともＴＣＰ／ＩＰを用いてネットワーク４００を介しての通信を行えるようになっている。送受信部２２３は、送受信機構がネットワーク４００から受取ったデータをインターフェイスを介して受取る。送受信部２２３は、インターフェイスを介して送受信機構から受取ったデータを暗号化復号化部２２２へ送るようになっている。また、送受信部２２３は、暗号化復号化部２２２からデータを受取る場合がある。送受信部２２３はその暗号化復号化部２２２から受取ったデータをインターフェイスに送り、送受信機構からネットワーク４００を介してクライアント１００へ送るようになっている。

[0050] 暗号化復号化部２２２は、簡単にいうと、送受信部２２３から受取ったデータのうち必要なものに復号化の処理を行い、また、アプリケーション２２１から受取ったデータのうちの必要なものに対して暗号化の処理を行う機能を有するとともに、サーバ２００との間のクライアント１００の認証に必要な処理を行うものである。つまり、暗号化復号化部２２２は、本願発明におけるクライアント１００とサーバ２００の間の暗号化通信の中心的な役割を担うものであり、本願発明のコンピュータをサーバとして機能させるためのコンピュータプログラムにより、サーバ２００内に生成されるものであると言える。

また、暗号化復号化部２２２には、入力装置から入力された操作内容につ

いてのデータが、インターフェイスを介して入力される場合がある。

[0051] 暗号化復号化部２２２の中には入力部２２２Ａ、主制御部２２２Ｂ、サーバ解生成部２２２Ｃ、解データ記録部２２２Ｄ、サーバ第１暗号化復号化部２２２Ｅ、サーバ第２暗号化復号化部２２２Ｆ、出力部２２２Ｇ、及び認証部２２２Ｈが生成される。

[0052] 入力部２２２Ａは、インターフェイス又はアプリケーション２２１からデータを受取るものである。入力部２２２Ａには後述するように、クライアント１００から送られてきた暗号化されたデータ、それも共通鍵で暗号化されたデータが、インターフェイス、送受信部２２３を介して送られてくることがある。そのデータを受取ったら入力部２２２Ａは、それをサーバ第２暗号化復号化部２２２Ｆに送るようになっている。入力部２２２Ａには、また、後述するように、クライアント１００から送られてきた解のデータが、インターフェイスを介して入力される場合がある。かかるデータを受取ったら入力部２２２Ａは、それを主制御部２２２Ｂに送るようになっている。入力部２２２Ａはまた、インターフェイスを介してアプリケーション２２１から送られてきたデータを受取ることがある。このデータは後述するように、暗号化してからクライアント１００に送られることを意図したものであるが、このデータを受取ったら入力部２２２Ａは、そのデータをサーバ第２暗号化復号化部２２２Ｆに送るようになっている。

[0053] 主制御部２２２Ｂは、暗号化復号化部２２２全体の制御を行うものである。主制御部２２２Ｂには上述のように、入力部２２２Ａから、クライアント１００から送られてきた解のデータを受取る場合があり、それを受取った場合には、それを認証部２２２Ｈへ送るようになっているとともに、サーバ解生成部２２２Ｃに対して解を生成せよとの指示を送るようになっている。主制御部２２２Ｂは、また、認証部２２２Ｈから後述する認証データを受取ることがあり、それを受取った場合には、サーバ解生成部２２２Ｃに対して解を生成せよとの指示を送るようになっている。

主制御部２２２Ｂは、共通鍵を保有しているか、新たに作り出す機能を有

している。この実施形態では主制御部 2 2 2 B は共通鍵を必要になる度に作ることができるようになっている。共通鍵を製造する方法は、周知又は公知技術によればよい。主制御部 2 2 2 B は、上述の認証データを受取った場合、生成した共通鍵のデータをサーバ第 1 暗号化復号化部 2 2 2 E に送るようになっている。

[0054] サーバ解生成部 2 2 2 C は、クライアント解生成部 1 2 2 C 同様に、解を連続して生成することのできるものとされている。サーバ解生成部 2 2 2 C で連続して生成される解のそれぞれは、共通条件下においてクライアント解生成部 1 2 2 C で連続して生成される解と一致するようになっている。この実施形態では、サーバ解生成部 2 2 2 C で解を連続して生成する方法と、クライアント解生成部 1 2 2 C で解を連続して生成する方法とは共通である。

解データ記録部 2 2 2 D には、新たな解を生成するためのデータ、つまり、クライアント 1 0 0 の解データ記録部 1 2 2 D に記録されていたのと同様の初期値、或いは過去の解のデータが記録されている。もっとも、サーバ 2 0 0 は、多数のクライアント 1 0 0 の認証を行う必要がある。したがって、サーバ 2 0 0 は、各クライアント 1 0 0 を識別するためのデータ（この実施形態では各クライアント 1 0 0 の IP アドレスを、各クライアント 1 0 0 を識別するためのデータとして利用することとしているが、他のデータ例えば各クライアント 1 0 0 が販売された段階から各クライアント 1 0 0 に割り振られている、クライアント 1 0 0 の販売業者や認証を行うための組織等により厳格に管理されている各クライアント 1 0 0 にユニークな識別子等を、かかるデータとして利用することもできる。）と各クライアント 1 0 0 毎の新たな解を生成するためのデータとを、互いに紐付けた状態で記録している。つまり、この実施形態では、各クライアント 1 0 0 のクライアント解生成部 1 2 2 C で連続して生成される解の列はそれぞれ異なるものとなっているが、サーバ 2 0 0 の側では、各クライアント 1 0 0 で生成されるそれぞれ異なる解の列と同じ解の列を、各クライアント 1 0 0 に対応して生成することができるようになっている。言い換えれば、サーバ 2 0 0 にあるサーバ解生成

部 2 2 2 C と、各クライアント 1 0 0 にあるクライアント解生成部 2 2 2 C のそれぞれとは、解を同期させられるようにされている。

サーバ解生成部 2 2 2 C は、解を生成した場合、それをサーバ第 1 暗号化復号化部 2 2 2 E か又は認証部 2 2 2 H に送るようになっている。解生成部 2 2 2 C が解を認証部 2 2 2 H に送るときには、解データ記録部 2 2 2 D に記録されていたものであり、その解を生成する際に参照された、クライアント 1 0 0 を特定するためのデータをも認証部 2 2 2 H に送るようになっている。

[0055] サーバ第 1 暗号化復号化部 2 2 2 E は、暗号化、復号化の処理を行えるようになっている。もっとも、この実施形態では、後述するように少なくとも暗号化の処理を行えば足りる。サーバ第 1 暗号化復号化部 2 2 2 E が暗号化したデータは、クライアント 1 0 0 の少なくともクライアント第 1 暗号化復号化部 1 2 2 E で復号化できるようになっている。サーバ第 1 暗号化復号化部 2 2 2 E での暗号化、復号化には、クライアント第 1 暗号化復号化部 1 2 2 E での暗号化、復号化の場合と同様に、解が使われる。上述のようにサーバ解生成部 2 2 2 C で生成された解はサーバ解生成部 2 2 2 C からサーバ第 1 暗号化復号化部 2 2 2 E に送られるが、その解はサーバ第 1 暗号化復号化部 2 2 2 E で上述の暗号化が行われる際に使用される。他方、サーバ第 1 暗号化復号化部 2 2 2 E には、主制御部 2 2 2 B から共通鍵のデータが送られてくる。この共通鍵のデータは、後述するようにクライアント 1 0 0 に送られるものであり、サーバ第 1 暗号化復号化部 2 2 2 E にて暗号化される。この暗号化された共通鍵のデータが、後述するように、クライアント第 1 暗号化復号化部 1 2 2 E で復号化され、共通鍵のデータに戻されるのである。

サーバ第 1 暗号化復号化部 2 2 2 E は、暗号化していない共通鍵のデータを、サーバ第 2 暗号化復号化部 2 2 2 F に送るようになっている。また、サーバ第 1 暗号化復号化部 2 2 2 E は、暗号化した共通鍵のデータを出力部 2 2 2 G に送るようになっている。

[0056] サーバ第 2 暗号化復号化部 2 2 2 F は、暗号化、復号化の処理を行うもの

である。ここで行われる暗号化、復号化の処理は、サーバ第1暗号化復号化部222Eから送られてきた共通鍵を用いて行われる。暗号化の対象となるのは、アプリケーション221から入力部222Aを介して送られてきた平文のデータであり、また復号化の対象となるのは、クライアント100から、ネットワーク400、送受信機構、インターフェイス、入力部222Aを介して送られてきた暗号化されたデータである。

サーバ第2暗号化復号化部222Fで行われる暗号化、復号化の処理は共通鍵を用いて行われる共通鍵方式の暗号化、復号化であればどのようなものでもよいが、同じ共通鍵を用いた場合には、ここで暗号化されたデータはクライアント第2暗号化復号化部122Fで復号化でき、クライアント第2暗号化復号化部122Fで暗号化されたデータは、ここで復号化できるものとされる。

サーバ第2暗号化復号化部222Fは、アプリケーション221から送られてきたデータを暗号化したものを出力部222Gに送るようになっているとともに、クライアント200から送られてきた暗号化されたデータを復号化したものを出力部222Gに送るようになっている。

[0057] 認証部222Hは、クライアント100が正当か否かの判断、つまりクライアント100の認証を行うためのものである。上述したように、認証部222Hには主制御部222Bから、クライアント100から送られてきた解のデータが送られてくる。また、解データ記録部222Dから解のデータと、その解を生成する際に参照されたクライアント100を特定するためのデータが認証部222Hに送られる。認証部222Hは、これら3つのデータを用いてクライアント100が正当か否かについての判断を行い、クライアント100が正当であると認証したときに認証データを生成する。なお、具体的な認証の方法については追って説明する。

かかる認証が行われた場合には、認証部222Hは認証データを生成し、その認証データを主制御部222Bに送るようになっている。

[0058] 出力部222Gは、暗号化復号化部222内で生成されたデータを外部に

出力するためのものである。

出力部２２２Ｇには、サーバ第２暗号化復号化部２２２Ｆから、アプリケーション２２１から送られてきたデータをサーバ第２暗号化復号化部２２２Ｆで暗号化したものと、クライアント１００から送られてきた暗号化されたデータをサーバ第２暗号化復号化部２２２Ｆで復号化したものとが送られてくる場合がある。

出力部２２２Ｇは、これらのうち、アプリケーション２２１から送られてきたデータをサーバ第２暗号化復号化部２２２Ｆで暗号化したものを、送受信部２２３を介してインターフェイスに送るようになっている。インターフェイスに送られたこれらデータは、送受信機構、ネットワーク４００を介してクライアント１００に送られるようになっている。出力部２２２Ｇは、また、クライアント１００から送られてきた暗号化されたデータをサーバ第２暗号化復号化部２２２Ｆで復号化したものをアプリケーション２２１に送るようになっている。それらデータは、アプリケーション２２１で使用される。

[0059] 次に、クライアント１００とサーバ２００を含んでなるこの通信システムの使用方法、及び動作について説明する。

かかる説明には、主に図８を用いる。

[0060] まず、ユーザは、自らのクライアント１００を操作し、クライアント１００とサーバ２００との間での通信を試みる。例えば、ユーザは、サーバ２００に接続して、サーバ２００が提供するウェブサイトを開覧しようとする。

そのために、ユーザはまず、クライアント１００上のアプリケーション１２１を立ち上げる（Ｓ１００１）。ウェブサイトを開覧するためのアプリケーション１２１であれば、通常は周知のブラウザを立ち上げることになる。ユーザは、入力装置１０２を適宜操作してブラウザを立ち上げる。ブラウザを立ち上げるための操作内容は、入力装置１０２からインターフェイス１１４を介してアプリケーション１２１に送られる。それによりアプリケーション１２１が動作し、画像データがインターフェイス１１４を介してディス

プレイ 101 に送られることにより、ブラウザがクライアント 100 のディスプレイ 101 上に表示される。

[0061] その状態でユーザは、サーバ 200 が提供するウェブサイトを閲覧しようとする。通常は、サーバ 200 のウェブアドレス (URL) をブラウザ上で指定することにより、クライアント 100 はサーバ 200 との通信を開始する。このとき、クライアント 100 は、まず、クライアント 100 の認証に必要な処理を始める。具体的には、サーバ 200 のウェブアドレスをユーザがブラウザ上で指定すると、その操作内容のデータが入力装置 102 からインターフェイス 114 を介して、入力部 122 A に送られてくる。この操作内容のデータは入力部 122 A から、主制御部 122 B に送られる。これを受取った主制御部 122 B は、クライアント解生成部 122 C に解を生成せよとの指示を送る。クライアント解生成部 122 C は、解を生成する (S1002)。

クライアント解生成部 122 C が解を生成する方法は上述した通りである。クライアント解生成部 122 C が解を生成するのが初めてなのであれば、クライアント解生成部 122 C は解データ記録部 122 D から初期値を読み出し、また、解を生成するのが初めてでないのであれば、クライアント解生成部 122 C は解データ記録部 122 D から過去に生成した解を読みだす。そのいずれかに基いて、クライアント解生成部 122 C は新たな解を生成する。生成された解は、クライアント解生成部 122 C から、出力部 122 G へ送られる。

[0062] 出力部 122 G は、受取った解を送受信部 123 に送る。送受信部 123 は、解のデータに TCP/IP の規則にのっとりヘッダを付すなどの所定の処理を行う。このときヘッダには、クライアント 100 を他のクライアント 100 から識別するための情報となるクライアント 100 の IP アドレスや、サーバ 200 のウェブアドレス等が含まれる。SSL の通信では、ウェブアドレスに続けて相手方のポート番号として決まった数字 (一般には 443) の記載を行うことによりそのヘッダを含むデータが SSL による通信を

求めるものであることを示すといった共通ルールがあるが、この暗号化通信でもそのようなルールに従ってもよい。いずれにせよ、そのようなヘッダが付された解のデータは、送受信部123から、インターフェイス114を介して、送受信機構に送られる。

解のデータは、送受信機構から、インターネットを介して、サーバ200に送られる(S1003)。なお、解のデータをクライアント100で暗号化してからサーバ200に送ることも可能であるが、この実施形態では暗号化しないままで解をサーバ200に送ることとしている。

[0063] 解は、サーバ200によって受取られる(S2001)。具体的には、解を含むデータは、サーバ200の送受信機構によって受取られ、インターフェイスから、送受信部223に送られる。送受信部223は、そこから解のデータと、ヘッダに含まれていたその解を送ってきたクライアント100のIPアドレスとを入力部222Aへと送る。それらは、入力部222Aから、主制御部222Bへと送られる。

主制御部222Bは、互いに紐付けた状態で解及びIPアドレスのデータを認証部222Hに送る。

他方、主制御部222Bは、そのIPアドレスのデータをサーバ解生成部222Cに送るとともに、サーバ解生成部222Cに解を生成せよとの指示を送る。これを受けたサーバ解生成部222Cは、解を生成する(S2002)。サーバ解生成部222Cは、解データ記録部222Dに記録されている各クライアント100についての新たな解を生成するためのデータ(初期値か過去の解のデータ)のうち、主制御部222Bから受取ったIPアドレスと紐付けられていたものを読みだす。そして、その初期値か過去の解のデータを用いて、既に述べた方法で新たな解を生成する。サーバ解生成部222Cは、生成した解と、その解を送ってきたクライアント100を特定するIPアドレスとをそれらを互いに紐付けた状態で認証部222Hへと送る。

[0064] 認証部222には、上述のように、主制御部222Bから送られてきた解及びIPアドレスが存在する。他方、認証部222Hには、サーバ解生成部

222Cから送られてきた解及びIPアドレスが存在する。ここで、IPアドレスが必要となるのは、短時間の間に複数のクライアント100から多数の解が送られて来た場合には、認証部222Hにおいて行われる、後述する、主制御部222Bから送られてきた解とサーバ解生成部222Cから送られてきた解との対比を行うにあたり、どの解とどの解を対比すべきかが不明となることがあり得るからである。これには限られないが、この実施形態では、同じIPアドレスに紐付けられている主制御部222Bから送られてきた解と、サーバ解生成部222Cから送られてきた解とを比較することにより、その解を送ってきたクライアント100が正当なものであるか否かの認証を行うこととしている。

上述したように、サーバ解生成部222Cで生成される解は、各クライアント100のクライアント解生成部122Cで生成される解と同期させられている。したがって、クライアント100が正当なものであれば、対比の対象となる上述の2つの解は一致するはずである。両者が一致した場合には、認証部222Hは、その解を送ってきたクライアント100が正当なものであると認証し、その旨を示す認証データを生成する（S2003）。

認証データは、それにより認証されたクライアント100のIPアドレスと紐付けた状態で、主制御部222Bへと送られる。2つの解が一致しなかったら、認証部222Hはクライアント100が正当でないという旨を主制御部222Bへ通知し、そこでクライアント100とサーバ200の間の通信を打ち切ることが可能であり、この実施形態ではそうしている。このときサーバ200はそのクライアント100に、クライアント100が認証されなかったということを通知するようになっていてももちろん良い。

[0065] 主制御部222Bは、認証データとIPアドレスとを受取った場合には、そのIPアドレスで特定されるクライアント100と暗号化通信を行うための共通鍵を生成する。共通鍵の生成は上述したように公知の方法で行えば良い。

主制御部222Bは、その共通鍵を、上記IPアドレスと紐付けた状態で

サーバ第1暗号化復号化部222Eに送るとともに、新たな解を生成せよとの指示をサーバ解生成部222Cに送る。サーバ解生成部222Cは、少なくとも1つの解を生成する(S2004)。生成された解は、その解を生成する指示のきっかけとなったIPアドレスとともにサーバ第1暗号化復号化部222Eに送られる。ここで、サーバ解生成部222Cでどのような条件で解を生成するのか、例えば幾つの解を生成するのか、またそのうちのどれを(例えば、2番目に生成されたものを、或いは100番目に生成されたものを)サーバ第1暗号化復号化部222Eに送るのかは、予め決定されており、その情報はクライアント100と共有されている。

上述したように、サーバ第1暗号化復号化部222Eは、受取った共通鍵のデータを暗号化する(S2005)。かかる暗号化には、サーバ解生成部222Cから送られてきた解が使われる。共通鍵を暗号化する際に用いる解は、それらに互いに紐付けられたIPアドレスが同じものを選択すればよい。ここで、サーバ第1暗号化復号化部222Eで行われる暗号化は、暗号化の結果得られるデータが解に依存したものとなる。解の使い方は暗号化の結果得られるデータが解に依存する限りどのようなものでも良いが、例えば解を暗号化の鍵として用いてもよい。なお、このときその共通鍵のデータと紐付けられていたIPアドレスのデータは暗号化しない。

暗号化された共通鍵のデータは、暗号化される前の共通鍵のデータと紐付けられていたIPアドレスのデータとともに出力部222Gへと送られる。

他方、サーバ第1暗号化復号化部222Eは、暗号化していない状態の共通鍵のデータをサーバ第2暗号化復号化部222Fに送る。これにより、サーバ第2暗号化復号化部222Fは、共通鍵方式の暗号化通信を行うために必要となる共通鍵を持った状態となる。

[0066] 出力部222Gは、それらデータを送受信部223へと送る。送受信部223は、暗号化された共通鍵のデータに対して、その送信先を示すヘッダを付す。その送信先は、上述のIPアドレスにより特定可能である。ヘッダを付された暗号化された共通鍵のデータは、送受信部223からインターフェ

イスに送られ、更には送受信機構から、ネットワーク４００を介してクライアント１００へと送られる（Ｓ２００６）。

[0067] クライアント１００は、暗号化された共通鍵のデータを受取る（Ｓ１００４）。暗号化された共通鍵のデータは、クライアント１００の送受信機構で受取られ、インターフェイス１１４を介して、送受信部１２３に送られる。送受信部１２３は、そのデータを、入力部１２２Ａに送る。

入力部１２２Ａは、暗号化された共通鍵のデータをクライアント第１暗号化復号化部１２２Ｅへと送る。他方、入力部１２２Ａは、暗号化された共通鍵のデータを受取った旨の通知を主制御部１２２Ｂへ送る。これを受取った主制御部１２２Ｂは、クライアント解生成部１２２Ｃに対して新たな解を生成せよとの指示を送る。

[0068] この指示を受取ったクライアント解生成部１２２Ｃは新たな解を少なくとも１つ生成する（Ｓ１００５）。そして、生成された解はクライアント解生成部１２２Ｃからクライアント第１暗号化復号化部１２２Ｅに送られる。

ここで、クライアント解生成部１２２Ｃでどのような条件下で解を生成するのか、例えば幾つの解を生成するのか、また、そしてそのうちのどれを（例えば、２番目に生成されたものを、或いは１００番目に生成されたものを）クライアント第１暗号化復号化部１２２Ｅに送るのかは、予め決定されており、その情報はサーバ２００と共有されている。クライアント解生成部１２２Ｃは、共通の条件下ではサーバ解生成部２２２Ｃと共通の解を連続して生成できるものとなっているのであるから、結果として、サーバ第１暗号化復号化部２２２Ｅが共通鍵のデータを暗号化するのに使用する解としてサーバ解生成部２２２Ｃが生成してサーバ第１暗号化復号化部２２２Ｅに送った解とまったく同じ解が、クライアント解生成部１２２Ｃからクライアント第１暗号化復号化部１２２Ｅへと送られることになる。

この解を用いて、クライアント第１暗号化復号化部１２２Ｅは、暗号化された共通鍵のデータを復号化して、暗号化されていない共通鍵のデータに戻す（Ｓ１００６）。クライアント第１暗号化復号化部１２２Ｅにおける復号

化の処理は、解に依存するものであり、且つ同じ解を用いた場合には、サーバ解生成部 222C で暗号化されたデータを復号化して元の平文のデータに戻すことが可能な処理である。したがって、暗号化された共通鍵のデータは、サーバ 200 の主制御部 222B が生成した通りの共通鍵のデータに戻る。

そして、共通鍵のデータは、クライアント第 1 暗号化復号化部 122E から、クライアント第 2 暗号化復号化部 122F に送られる。これにより、クライアント第 2 暗号化復号化部 122F は、共通鍵方式の暗号化通信を行うために必要な共通鍵を持った状態となる。

つまり、以上の処理により、サーバ 200 におけるサーバ第 2 暗号化復号化部 222F と、クライアント 100 におけるクライアント第 2 暗号化復号化部 122F とは、共通の共通鍵を持った状態となる。この実施形態では、元々サーバ 200 内に存在した共通鍵がサーバ 200 からクライアント 100 に提供されている。そして、サーバ 200 からクライアント 100 に提供される暗号共通鍵は、サーバ 200 で暗号化してからクライアント 100 に提供される。サーバ 200 で共通鍵を暗号化するために、また、クライアント 100 で暗号化された共通鍵を復号化するために、サーバ 200 とクライアント 100 とでそれぞれ生成された同じ解が用いられている。しかも、その解は、サーバ 200 とクライアント 100 の内部にのみ存在し、ネットワーク 400 を介してサーバ 200 とクライアント 100 との間を送信されることがない。つまり、以上の処理においては、悪意の第三者から見れば、共通鍵を暗号化し、復号化するために必要な解を盗む機会がない。

[0069] サーバ 200 におけるサーバ第 2 暗号化復号化部 222F と、クライアント 100 におけるクライアント第 2 暗号化復号化部 122F とが、共通の共通鍵を持った状態となったのであれば、サーバ 200 とクライアント 100 とは、従来の SSL 通信の上記 (3) の過程で実行していたと同様の暗号化通信を行えるようになる。

かかる暗号化通信は、必要に応じてクライアント 100 からサーバ 200

に、或いはサーバ200からクライアント100に、暗号化したデータが送られることにより実現される（S1007、S2007）。

例えば、クライアント100のアプリケーション121で、暗号化してサーバ200に送るべきデータが生成され、そのデータがアプリケーション121から、暗号化復号化部122に送られる。暗号化復号化部122の入力部122Aがそのデータを受取ると、そのデータはクライアント第2暗号化復号化部122Fに送られ、そこで共通鍵を用いて暗号化される。暗号化されたそのデータは、出力部122Gから、送受信部123へ送られ、上述のようなヘッダを付す処理が必要に応じて行われた上で、インターフェイス114から送受信機構に送られ、そこからネットワーク400を介して、サーバ200に送られる。

サーバ200は、その送受信機構でそのデータを受取る。そのデータは、サーバ200の送受信機構からインターフェイスに送られ、そして送受信部223を経て、入力部222Aに送られる。その暗号化されたデータは、サーバ第2暗号化復号化部222Fで共通鍵を用いて復号化され、出力部222Gへと送られる。出力部222Gは復号化されたそのデータを、アプリケーション221に送り、アプリケーション221はそのデータを適宜用いる。

他方、サーバ200のアプリケーション221が、暗号化してクライアント100に送るべき平文のデータを生成する場合がある。アプリケーション221がそのようなデータを生成した場合、そのデータは、暗号化復号化部222中の入力部222Aに送られる。そのデータは、入力部222Aからサーバ第2暗号化復号化部222Fへと送られ、そこで共通鍵を用いて暗号化される。サーバ第2暗号化復号化部222Fで暗号化されたそのデータは、出力部222Gを介して送受信部223に送られる。送受信部223では、その暗号化されたデータにヘッダを付す上述の如き処理が必要に応じて行われる。かかる処理が行われたそのデータは、送受信部223からインターフェイスを介してサーバ200の送受信機構に送られ、そこからネットワー

ク４００を介してクライアント１００に送られる。

クライアント１００は、その送受信機構でそのデータを受取る。そのデータは、クライアント１００の送受信機構からインターフェイス１１４に送られ、そして送受信部１２３を経て、入力部１２２Ａに送られる。その暗号化されたデータは、クライアント第２暗号化復号化部１２２Ｆで共通鍵を用いて復号化され、出力部１２２Ｇへと送られる。出力部１２２Ｇは復号化されたそのデータを、アプリケーション１２１に送り、アプリケーション１２１はそのデータを適宜用いる。

以上のようにして、サーバ２００とクライアント１００との間で共通鍵を用いた共通鍵方式の暗号化通信が行われる。

上述の暗号化通信において暗号化、復号化が行われるのは、サーバ２００においては、アプリケーション２２１と、ＴＣＰ／ＩＰの通信を行う送受信部２２３との間にある暗号化復号化部２２２であり、クライアント１００においては、アプリケーション１２１と、ＴＣＰ／ＩＰの通信を行う送受信部１２３との間にある暗号化復号化部１２２である。アプリケーションと、ＴＣＰ／ＩＰとの間で暗号化と復号化の処理を実行するというのは、従来からのＳＳＬ通信のプロトコルに共通するものであるので、この実施形態の発明を既存のＳＳＬ通信に応用するのは比較的簡単である。もっとも、本願発明は、暗号化と復号化の処理を必ずしも、アプリケーションと、ＴＣＰ／ＩＰとの間で行うには及ばない。

通信を行う必要がなくなれば、サーバ２００とクライアント１００との間の暗号化通信が終了する。

[0070] <変形例１>

変形例１における通信システムについて説明する。

変形例１における通信システムは、概ね第１実施形態におけるそれと同様である。異なるのは、第１実施形態における通信システムにおけるクライアント１００とサーバ２００との間の通信では、通信する相手方が正当であるということについての認証を、サーバ２００がクライアント１００が正当で

あるということをサーバ２００における認証部２２２Ｈで行うのみであったが、変形例１では、クライアント１００も、サーバ２００が正当であるということを認証するようにしている、という点である。

[0071] 以上の相違点とともなって、変形例１におけるクライアント１００には、認証部１２２Ｈが設けられている（図９）。かかる認証部１２２Ｈは、サーバ２００の認証を行うためのものである。認証部１２２Ｈで行われるサーバ２００の認証の方法は、サーバ２００の認証部２２２Ｈで行われるクライアント１００の認証の方法と概ね同じであるが、その方法については追って説明する。

変形例１におけるサーバ２００は、機能ブロックでいえば第１実施形態の場合と変わらないが、一部の機能ブロックの機能が第１実施形態の場合と異なる。サーバ２００の各機能ブロックの機能のうちのどこが第１実施形態の場合と異なっているのかについては追って説明する。

[0072] 変形例１の通信システムの使用方法、動作について説明する。

かかる通信システムで実行される方法は、概ね第１実施形態の場合と同じであるので、その差分を中心として説明することにする（図１０）。

まず、クライアント１００で実行される、第１実施形態におけるＳ１００１～Ｓ１００３の処理、及びサーバ２００で実行される、第１実施形態におけるＳ２００１～Ｓ２００３までの処理は、変形例１でも同じである。

変形例１でも、サーバ２００の認証部２２２Ｈで、クライアント１００が正当であるとの認証が行われる（Ｓ２００３）。かかる認証が行われると、変形例１でも、第１実施形態の場合と同様に認証データが生成される。

第１実施形態の場合、認証部２２２Ｈが認証データを生成すると、それは主制御部２２２Ｂに送られ、続けて新たな解の生成（Ｓ２００４）の処理、新たな解を用いた共通鍵の暗号化（Ｓ２００５）の処理が行われた。しかしながら、変形例１の場合には、認証部２２２Ｈが認証データを生成した後に、クライアント１００でサーバ２００を認証する処理が実行されることになる。

認証部 222H が認証データを生成すると、認証データは、その認証データを生成するきっかけとなった解を送って来たクライアント 100 を特定するための IP アドレスとともに、主制御部 222B に送られる。認証データを受取ると、主制御部 222B は、その認証データと IP アドレスとをサーバ解生成部 222C に送るとともに、サーバ解生成部 222C に対して新たな解を生成せよとの指示を送る。以上のデータ及び指示を受けると、サーバ解生成部 222C はその IP アドレスについての解を少なくとも 1 つ生成し、生成した解の中の 1 つを出力部 222G に送る (S2003A)。この解は、追ってクライアント 100 でサーバ 200 の認証が行われるときに使用されるものである。サーバ 200 において、何番目の解がサーバ解生成部 222C から出力部 222G に送られるのかということ、つまり何番目の解がサーバ 200 の認証のためにクライアント 100 で使用されるのかということは、予め定められており、サーバ 200 とクライアント 100 との間で共有されている。新たに生成された解は、IP アドレスのデータとともに、サーバ解生成部 222C から出力部 222G へと送られる。

出力部 222G は、受取った解と IP アドレスのデータを、送受信部 223 に送る。送受信部 223 は、上述したようにヘッダを生成し、ヘッダの付された新たに生成された解のデータをインターフェイスを介してサーバ 200 の送受信機構に送る。新たに生成された解のデータは、サーバ 200 から、上記 IP アドレスで特定されるクライアント 100 へと送られることになる (S2003B)。

[0073] クライアント 100 は、新たに生成された解のデータをサーバ 200 から受取る (S1003A)。

具体的には、クライアント 100 は、その解のデータを、その送受信機構にて受取る。受取られた解のデータは、送受信機構から、インターフェイス 114 を介して送受信部 123 に送られ、入力部 122A に送られる。入力部 122A は、その解のデータを主制御部 122B に送る。

主制御部 122B は、サーバ 200 から送られてきた新たに生成された解

を受取ると、それを認証部 1 2 2 H に送るとともに、クライアント解生成部 1 2 2 C に対して新たな解を生成せよとの指示を送る。かかる指示を受取るとクライアント解生成部 1 2 2 C は、少なくとも 1 つの解を生成し、生成した解のいずれかを認証部 1 2 2 H に送る (S 1 0 0 3 B)。クライアント解生成部 1 2 2 C が幾つの解を生成し、どの解をクライアント解生成部 1 2 2 C に送るかという条件乃至それについての情報は、上述のようにサーバ 2 0 0 のサーバ解生成部 2 2 2 C と共有されている。

この状態では、クライアント 1 0 0 の認証部 1 2 2 H には、サーバ 2 0 0 から送られてきた解と、クライアント 1 0 0 のクライアント解生成部 1 2 2 C で生成された解との双方が存在している。認証部 1 2 2 H では、それら 2 つの解を対比する。その結果、2 つの解が一致した場合には認証部 1 2 2 H は、その解を送ってきたサーバ 2 0 0 が正当なものであると認証する (S 1 0 0 3 C)。繰り返しになるが、サーバ 2 0 0 のサーバ解生成部 2 2 2 C とクライアント 1 0 0 のクライアント解生成部 1 2 2 C とは、共通の条件下では共通の解を連続して生成することができるようになっている。したがって、連続して生成される解のうちどの解をサーバ 2 0 0 の認証に用いるのかという条件をサーバ 2 0 0 とクライアント 1 0 0 との間で共有しているのであれば、サーバ 2 0 0 が正当なものである限り、サーバ 2 0 0 から送られてきた解は、クライアント解生成部 1 2 2 C で生成された解と一致するはずである。他方、悪意の第三者がサーバ 2 0 0 になりすまそうとしても、当該悪意の第三者はサーバ解生成部 2 2 2 C でどのように解が生成されるかを知らないで、仮にクライアント 1 0 0 からサーバ 2 0 0 に先に送られたクライアント 1 0 0 で生成された解を不正に入手していたとしても、サーバ 2 0 0 からクライアント 1 0 0 へ送られた上述のサーバ解生成部 2 2 2 C で生成された解と同じ解を生成することができない。つまり、クライアント 1 0 0 でサーバ 2 0 0 が適正なものか否かの認証を行う場合には、悪意のある第三者はサーバ 2 0 0 になりすますることが事実上不可能となる。

サーバ 2 0 0 が適正なものであると認証した場合、認証部 1 2 2 H はその

旨を示す情報であるクライアント認証データを生成する。クライアント認証データは主制御部 1 2 2 B に送られ、そこから出力部 1 2 2 G に送られる。クライアント認証データには主制御部 1 2 2 B から出力部 1 2 2 G に送られる間に特に処理を行う必要はないので、主制御部 1 2 2 B から出力部 1 2 2 G にクライアント認証データが送られる際のその経路は自由である。

出力部 1 2 2 G はクライアント認証データを送受信部 1 2 3 に送る。送受信部 1 2 3 は、上述の如き処理により必要に応じてクライアント認証データに対してヘッダを付し、それをインターフェイス 1 1 4 からクライアント 1 0 0 の送受信機構に送る。クライアント認証データは、送受信機構からネットワーク 4 0 0 を介してサーバ 2 0 0 へと送られる (S 1 0 0 3 D)。

[0074] サーバ 2 0 0 は、クライアント 1 0 0 から認証データを受取る (S 2 0 0 3 C)。

かかるクライアント認証データは、クライアント認証データを送ってきたクライアント 1 0 0 の IP アドレスとともに、サーバ 2 0 0 の送受信機構から、インターフェイス、送受信部 2 2 3 を介して入力部 2 2 2 A へと送られる。入力部 2 2 2 A は、クライアント認証データを上記 IP アドレスとともに主制御部 2 2 2 B へ送る。

これを受取ると、主制御部 2 2 2 B は共通鍵を生成する。主制御部 2 2 2 B は、生成したその共通鍵を、受取った上記 IP アドレスと紐付けた状態でサーバ第 1 暗号化復号化部 2 2 2 E に送るとともに、新たな解を生成せよとの指示をサーバ解生成部 2 2 2 C に送る。サーバ解生成部 2 2 2 C は、少なくとも 1 つの解を生成する (S 2 0 0 4)。

変形例 1 におけるここから先の処理は、第 1 実施形態の場合と同様である。

[0075] ≪第 2 実施形態≫

第 2 実施形態における通信システムについて説明する。第 2 実施形態における通信システムの構成及び動作は概ね第 1 実施形態における通信システムにおけるそれらと同じである。第 2 実施形態の通信システムが第 1 実施形態

における通信システムと異なるのは、第1実施形態では、サーバ200内に元々存在した共通鍵を、暗号化した状態でサーバ200からクライアント100へと提供することにより共通鍵をサーバ200とクライアント100とで共有することにしていたが、第2実施形態ではこれとは逆に、クライアント100内に元々存在している共通鍵を、暗号化した状態でクライアント100からサーバ200へと提供することにより共通鍵をサーバ200とクライアント100とで共有するようにしている、という点である。

[0076] 第2実施形態におけるクライアント100の中に生成される機能ブロックを図11に示し、第2実施形態におけるサーバ200の中に生成される機能ブロックを図12に示す。

その内部に生成される機能ブロック自体は、第1実施形態のクライアント100においても第2実施形態のクライアント100においても変わらない。同様に、その内部に生成される機能ブロック自体は、第1実施形態のサーバ200においても第2実施形態のサーバ200においても変わらない。もっとも、第2実施形態におけるクライアント100内の、或いはサーバ200内の機能ブロックの機能は、第1実施形態の場合のそれらと若干異なる場合がある。その相違については後述する。

[0077] 第2実施形態の通信システムの使用方法、動作について説明する。

かかる通信システムで実行される方法は、概ね第1実施形態の場合と同じであるので、その差分を中心として説明することにする（図13）。

まず、クライアント100で実行される、第1実施形態におけるS1001～S1003の処理、及びサーバ200で実行される、第1実施形態におけるS2001～S2003までの処理は、第2実施形態でも同じである。

第2実施形態でも、サーバ200の認証部222Hで、クライアント100が正当であるとの認証が行われる（S2003）。かかる認証が行われると、第2実施形態でも、第1実施形態の場合と同様に認証データが生成される。

第1実施形態の場合、認証部222Hが認証データを生成すると、それは

主制御部 2 2 2 B に送られ、続けて新たな解の生成 (S 2 0 0 4) の処理、新たな解を用いた共通鍵の暗号化 (S 2 0 0 5) の処理が行われた。しかしながら、第 2 実施形態の場合には、認証部 2 2 2 H が認証データを生成すると、認証データはクライアント 1 0 0 に送られ、クライアント 1 0 0 で共通鍵が暗号化されることになる。以下、詳述する。

[0078] 認証部 2 2 2 H で認証データが生成されると、認証データは認証部 2 2 2 H から主制御部 2 2 2 B へと送られる。主制御部 2 2 2 B は認証データを、出力部 2 2 2 G に送る。主制御部 2 2 2 B から出力部 2 2 2 G に送るまでに認証データには特段の処理が行われないため、主制御部 2 2 2 B から出力部 2 2 2 G へ認証データを送る際の経路は不問である。

出力部 2 2 2 G に認証データが送られると、出力部 2 2 2 G は認証データを送受信部 2 2 3 に送る。送受信部 2 2 3 は、上述の如きヘッダを必要に応じて生成し、ヘッダを付した認証データをインターフェイスを介してサーバ 2 0 0 の送受信機構に送る。送受信機構は、ネットワーク 4 0 0 を介して認証データをクライアント 1 0 0 へ送信する (S 2 0 0 8)。

[0079] クライアント 1 0 0 は、認証データを受取る (S 1 0 0 8)。より詳細には、認証データはクライアント 1 0 0 の送受信機構によって受取られる。送受信機構によって受取られた認証データは、インターフェイス 1 1 4 を介して送受信部 1 2 3 に送られ、そこから、暗号化復号化部 1 2 2 の入力部 1 2 2 A に送られる。入力部 1 2 2 A は受取った認証データを、主制御部 1 2 2 B に送るようになっている。

認証データを受取ると、主制御部 1 2 2 B は、共通鍵を生成するようになっている。第 1 実施形態では、サーバ 2 0 0 の主制御部 2 2 2 B が共通鍵を生成する機能を有していたが、第 2 実施形態ではその機能をクライアント 1 0 0 の主制御部 1 2 2 B に移している。したがって、クライアント 1 0 0 の主制御部 1 2 2 B は、必要になる都度共通鍵を生成するようになっていても良いが、第 1 実施形態におけるサーバ 2 0 0 の主制御部 2 2 2 B のように、当初から固定の共通鍵を持っているようにしてもよい。とりあえずこの実施

形態における主制御部 1 2 2 B は、必要になる都度、言い換えれば認証データを受取る都度、共通鍵のデータを生成することとしている。

生成された共通鍵のデータは、クライアント第 1 暗号化復号化部 1 2 2 E へと送られる。他方、主制御部 1 2 2 B は、クライアント解生成部 1 2 2 C に対して、新たな解を生成せよとの指示を送る。かかる指示を受取ったクライアント解生成部 1 2 2 C は、少なくとも 1 つの新たな解を生成する (S 1 0 0 9)。生成された解のうち予め定められたものが、クライアント解生成部 1 2 2 C からクライアント第 1 暗号化復号化部 1 2 2 E に送られる。かかる解は、上述の共通鍵を暗号化する際に、クライアント第 1 暗号化復号化部 1 2 2 E で用いられるものである。そして、どの解が共通鍵を暗号化する際に用いられるかということは予め決定されており、且つその情報はサーバ 2 0 0 のサーバ第 1 暗号化復号化部 2 2 2 E と共有されている。

いずれにせよ、クライアント第 1 暗号化復号化部 1 2 2 E には、共通鍵のデータと、クライアント解生成部 1 2 2 C が生成した解のデータが存在する状態となる。

[0080] クライアント第 1 暗号化復号化部 1 2 2 E は、共通鍵のデータを暗号化する (S 1 0 1 0)。かかる暗号化には、クライアント解生成部 1 2 2 C から受取った解のデータが用いられる。クライアント第 1 暗号化復号化部 1 2 2 E で実行されるかかる暗号化の処理は、第 1 実施形態におけるサーバ第 1 暗号化復号化部 2 2 2 E で行われた共通鍵の暗号化の処理と同様のものである。

暗号化された共通鍵のデータは、クライアント第 1 暗号化復号化部 1 2 2 E から、出力部 1 2 2 G へと送られる。かかる暗号化された共通鍵のデータは、出力部 1 2 2 G から、送受信部 1 2 3 へと送られ、そこで上述した如きヘッダが必要に応じて付される。そして、ヘッダが必要に応じて付された暗号化された共通鍵のデータは、インターフェイス 1 1 4 からクライアント 1 0 0 の送受信機構に送られ、そこからネットワークを介してサーバ 2 0 0 へ送られる (S 1 0 1 1)。

他方、クライアント第1暗号化復号化部122Eは、暗号化していない共通鍵のデータを、クライアント第2暗号化復号化部122Fに送る。

[0081] サーバ200は、暗号化された共通鍵のデータをクライアント100から受取る(S2009)。暗号化された共通鍵のデータの受取は、サーバ200の送受信機構によって行われる。暗号化された共通鍵のデータは、送受信機構からインターフェイスを介して送受信部223へと送られ、送受信部223から、その共通鍵を送ってきたクライアント100のIPアドレスのデータとともに、入力部222Aを介して、主制御部222Bに送られる。

それらを受取った主制御部222Bは、暗号化された共通鍵のデータを、サーバ第1暗号化復号化部222Eに送る。また、主制御部222Bは、受取ったIPアドレスのデータをサーバ解生成部222Cへと送るとともに、新たな解を生成せよとの指示をもサーバ解生成部222Cに送る。

IPアドレスのデータと上述の指示を受取ったサーバ解生成部222Cは、そのIPアドレスと紐付けられていた新たな解を生成するために必要な情報を解データ記録部222Dから読出し、それを用いて少なくとも1つの新しい解を生成して、それをサーバ第1暗号化復号化部222Eへと送る(S2010)。サーバ解生成部222Cが、新しく生成された解のデータのうちのどの解をサーバ第1暗号化復号化部222Eへと送るかは、上述したように、クライアント解生成部122Cとの間で共有された条件によって決定される。結果、悪意のある第三者による介入がなければ、クライアント解生成部122Cがクライアント第1暗号化復号化部122Eに送った解と、サーバ解生成部222Cがサーバ第1暗号化復号化部222Eに送った解とは完全に一致したものとなる。

以上により、サーバ第1暗号化復号化部222Eは、クライアント100から送られてきた暗号化された共通鍵のデータと、サーバ解生成部222Cで生成された解とを持った状態となる。サーバ第1暗号化復号化部222Eは、クライアント100から送られてきた暗号化された共通鍵のデータを、解を用いて復号化する(S2011)。かかる復号化の処理は、第1実施形

態におけるクライアント第1暗号化復号化部122Eで行われた処理と、同様のものとなる。サーバ第1暗号化復号化部222Eは、同じ解を用いれば、クライアント100のクライアント第1暗号化復号化部122Eで暗号化されたデータを復号化できるものとなっており、且つクライアント第1暗号化復号化部122Eで共通鍵を暗号化するときに用いられた解と、サーバ第1暗号化復号化部222Eにサーバ解生成部222Cから送られてきた解とは、上述のように同一のものとなっている。したがって、サーバ第1暗号化復号化部222Eは、クライアント100から送られてきた暗号化された共通鍵のデータを、暗号化されていない元の共通鍵のデータに戻すことが可能である。

なお、以上の説明で明らかなように、第2実施形態のクライアント第1暗号化復号化部122Eとサーバ第1暗号化復号化部222Eでそれぞれ実行される処理は、第1実施形態の場合と逆転している。したがって、第1実施形態の場合とは逆に、第2実施形態におけるクライアント第1暗号化復号化部122Eは、暗号化の処理だけを行えば足り、第2実施形態におけるサーバ第1暗号化復号化部222Eは、復号化の処理だけを行えば足り、といえる。

サーバ第1暗号化復号化部222Eは、復号化された共通鍵のデータをサーバ第2暗号化復号化部222Fに送る。

[0082] 以上の処理により、サーバ200におけるサーバ第2暗号化復号化部222Fと、クライアント100におけるクライアント第2暗号化復号化部122Fとは、第2実施形態では元々クライアント100に存在した共通の共通鍵を持った状態となる。第1実施形態の場合と同様に、共通鍵を暗号化し、また復号化するための解はそれぞれ、クライアント100とサーバ200の内部で生成され、クライアント100とサーバ200の間で送信されることがないから、第三者はその解を盗む機会がない。

サーバ200におけるサーバ第2暗号化復号化部222Fと、クライアント100におけるクライアント第2暗号化復号化部122Fとが、共通の共

通鍵を持った状態となったのであれば、サーバ200とクライアント100とは、従来のSSL通信の上記(3)の過程で実行していたと同様の暗号化通信を行えるようになる。かかる処理は、第1実施形態のS1007、S2007の処理に同じである。

[0083] なお、第2実施形態の通信システムにおいても、第1実施形態の通信システムの変形例1のように、サーバ200でクライアント100の正当性の認証を行うだけでなく、クライアント100でサーバ200の正当性の認証を行うようにすることができる。

[0084] ≪第3実施形態≫

次に、本願発明の第3実施形態について説明する。第3実施形態の通信システムは、本願における第3の態様とでもいうべき発明に相当するものである。

第3の発明は概ね第1実施形態の通信システムに同じであり、ネットワーク400に接続可能なクライアント100とサーバ200とから構成される。第3実施形態のクライアント100が備えるハードウェア構成、及びその内部に生成される機能ブロックは第1実施形態の場合と変わらず、サーバ200についても同様である。

[0085] 次に、クライアント100とサーバ200を含んでなるこの通信システムの使用方法、及び動作について説明する。

かかる説明には、主に図14を用いる。

[0086] ユーザはまず、第1実施形態の場合と同様に、クライアント100上のアプリケーション121を立ち上げる(S1001)。

ユーザは、サーバ200が提供するウェブサイトを閲覧しようとする。サーバ200のウェブアドレスをユーザがブラウザ上で指定すると、クライアント解生成部122Cは、複数の解を生成する(S1102)。

複数の解の生成方法は、第1実施形態の場合と同様である。そのうちの1つの解は、クライアント第1暗号化復号化部122Eに送られる。また、主制御部122Bからサーバ第1暗号化復号化部122Eには共通鍵が送られ

る。クライアント第1暗号化復号化部122Eは、共通鍵を暗号化する（S1102）。かかる暗号化には、クライアント解生成部122Cから送られた解が用いられる。どの解がクライアント第1暗号化復号化部122Eに送られるか、即ちどの解がかかる暗号化に用いられるかは第1実施形態の場合と同様、サーバ第1暗号化復号化部222Eと共有されている。

他方、クライアント第1暗号化復号化部122Eは、暗号化していない状態の共通鍵を、クライアント第2暗号化復号化部122Fに送る。

複数生成された解のうちの、共通鍵を暗号化するために用いられなかったもの1つが、クライアント解生成部122Cから、出力部122Gに送られる。この解は後述するようにサーバ200に送られるが、ここで、どの解が出力部122Gに送られるか、ひいてはサーバ200に送られるかは、予め決定されており、その情報はサーバ200と共有されている。また、暗号化された共通鍵もクライアント第1暗号化復号化部122Eから出力部122Gに送られる。

出力部122Gに送られた解と暗号化された共通鍵のデータは、サーバ200に送られる（S1103）。それらの送信の仕方は第1実施形態に倣う。

[0087] サーバ200は、クライアント100から、解と暗号化された共通鍵のデータとを受取る（S2101）。サーバ200におけるそれらの受信のされ方は、第1実施形態に倣う。

解と暗号化された共通鍵のデータは、入力部222Aから、主制御部222Bに送られる。主制御部222Bは、解を認証部222Hに送るとともに、暗号化された共通鍵をサーバ第1暗号化復号化部222Eに送る。他方、主制御部222Bは、サーバ解生成部222Cに解を生成するように指示する。それにより、サーバ解生成部222Cは複数の解を生成する（S2102）。なお、解は、以下の認証と、暗号化された共通鍵の復号化が行われる前に少なくとも2つ存在していれば足り、必要となる都度生成されるようになっていてもよい。

生成された複数の解のうち、クライアント１００からサーバ２００へ送られてきた解と共通条件下（この実施形態では、同じ順番）で生成された解は、サーバ解生成部２２２Ｃから認証部２２２Ｈへ送られる。認証部２２２Ｈは、クライアント１００から送られてきた解と、サーバ解生成部２２２Ｃから送られてきた解とを対比して、第１実施形態の場合と同様の方法で認証を行う。即ち、両者が一致した場合には、その解を送ってきたクライアント１００が正当なものであるとの認証を行う（Ｓ２１０３）。

かかる認証が行われると次に、サーバ解生成部２２２Ｃからサーバ第１暗号化復号化部２２２Ｅに対して解が送られる。サーバ第１暗号化復号化部２２２Ｅは、サーバ解生成部２２２Ｃから送られた解を用いて暗号化された共通鍵を復号化する（Ｓ２１０４）。サーバ解生成部２２２Ｃからサーバ第１暗号化復号化部２２２Ｅに送られる解は、クライアント第１暗号化復号化部１２２Ｅで共通鍵を暗号化するために使用された解と共通条件下（この実施形態では同じ順番）で生成されたものである。したがって、クライアント第１暗号化復号化部１２２Ｅで共通鍵を暗号化する際に使われた解と、サーバ第１暗号化復号化部２２２Ｅが暗号化された共通鍵を復号化する際に使用する鍵とは、クライアント１００が正当なものであるのであれば同じであるはずである。したがって、第三者による何らかの妨害がない限り、第１実施形態の場合と同様の理屈で、暗号化された共通鍵の鍵は復号化される。もっとも、暗号化された共通鍵の復号化がクライアント１００の認証の前に行われても構わない。この場合には、暗号化された共通鍵が復号化できても、上述のクライアント１００の認証ができなかった場合にはその復号化された共通鍵は使用されない。

サーバ第１暗号化復号化部２２２Ｅは復号化された共通鍵のデータをサーバ第２暗号化復号化部２２２Ｆに送る。

以上の処理により、サーバ２００におけるサーバ第２暗号化復号化部２２２Ｆと、クライアント１００におけるクライアント第２暗号化復号化部１２２Ｆとは、共通の共通鍵を持った状態となる。

[0088] サーバ200におけるサーバ第2暗号化復号化部222Fと、クライアント100におけるクライアント第2暗号化復号化部122Fとが、共通の共通鍵を持った状態となったのであれば、サーバ200とクライアント100とは、第1実施形態のS1007、S2007で述べた通りの、共通鍵方式の暗号化通信を安全に行うことができる。

請求の範囲

[請求項1]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムで実行される通信方法であって、

前記第2通信装置が、その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、

前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取る過程、

前記第1通信装置が、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理か、又は前記第2通信装置を正当なものと認証したとの通知を前記第1通信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理の一方を行う過程、

前記第1通信装置が前記共通鍵を暗号化した場合には、前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信するとともに、暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成され

た解を用いて暗号化された前記共通鍵を、前記第 1 通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、

前記第 2 通信装置が前記共通鍵を暗号化した場合には、前記第 2 通信装置から前記第 1 通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信するとともに、暗号化された前記共通鍵を受取った前記第 1 通信装置が、その解生成手段で 2 つ目或いはそれ以降の解を生成するとともに、2 つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を、前記第 2 通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、

以上により前記第 1 通信装置と前記第 2 通信装置で共有されることになった前記共通鍵を用いて、前記第 1 通信装置と、前記第 2 通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を含んでなる、通信方法。

[請求項2]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第 1 通信装置と第 2 通信装置とを含んで構成される暗号化通信システムの前記第 2 通信装置で実行される通信方法であって、

前記第 2 通信装置が実行する、

その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第 1 通信装置に送信する過程、

前記第 1 通信装置が、前記第 2 通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第 1 通信装置の解生成手段で生成した解と、前記第 2 通信装置から受取った解とを比較して、両者が一致した場合には、前記第 2 通信装置を正当なものと認証し、前記第 2 通信装置が正当だとの認証が前記第 1 通信装置で行われた場合に、前記第 1 通信装置が、その解生成手段で 2 つ目或いはそれ以降の解を生成するとともに、2 つ目以降の予め定められ

た条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理が実行された後に、前記第1通信装置から暗号化された前記共通鍵を前記ネットワークを介して受取る過程、

その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、暗号化された前記共通鍵を、前記第1通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を含んでなる、通信方法。

[請求項3]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置で実行される通信方法であって、

前記第2通信装置が実行する、

その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、

前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証し、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置から前記第2通信装置が正当なものと認証されたという通知を前記ネットワークを介して受取る過程、

前記通知を受取った後に、その解生成手段で2つ目或いはそれ以降

の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、

暗号化した共通鍵を、前記第1通信装置へと前記ネットワークを介して送信する過程、

前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する処理を実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を含んでなる、通信方法。

[請求項4]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置で実行される通信方法であって、

前記第1通信装置が実行する、

前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、

前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自

らが持つ共通鍵を暗号化する過程、

前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信する過程、

暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、暗号化された前記共通鍵を、前記第1通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を含んでなる、通信方法。

[請求項5]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置で実行される通信方法であって、

前記第1通信装置が実行する、

前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、

前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第2通信装置を正当なものと認証したとの通知を前記ネットワークを介して前記第2通信装置に送る過程、

前記第2通信装置を正当なものと認証したとの通知を前記第1通信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いは

それ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理を行った後に、前記第2通信装置から前記ネットワークを介して送信された暗号化された前記共通鍵を受取る過程、

その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、前記第2通信装置から受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を含んでなる、通信方法。

[請求項6]

解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いた暗号化を行うことができる第1通信装置第1暗号化復号化手段と、認証手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、を備えており、所定のネットワークと接続可能とされている第1通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第2通信装置であって、

前記第1通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第2通信装置解生成手段と、

前記第2通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第1通信装置第1暗号化復号化手段で行われるのと同じ復号化を行うことができる第2通信装置第1暗号化復号化手段と、

共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、

を備えており、

前記第2通信装置解生成手段で生成した解を前記ネットワークを介して前記第1通信装置に送るようになっており、

前記第1通信装置は、前記第2通信装置から前記ネットワークを介して前記解を受取り、前記第1通信装置解生成手段で解を生成させ、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっており、前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第1通信装置解生成手段が2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて自らが持つ共通鍵を前記第1通信装置第1暗号化復号化手段で暗号化する処理を実行して、暗号化された前記共通鍵を前記ネットワークを介して前記第2通信装置に送るようになっており、

前記第2通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第2通信装置解生成手段によって生成された解を用いて、前記第1通信装置から受取った暗号化された前記共通鍵を前記第2通信装置第1暗号化復号化手段で復号化するようになっており、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第1通信装置との間で共通鍵方式の暗号化通信を行うようになっている、

第2通信装置。

[請求項7]

解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いた復号化を行うことができる第1通信装置第1暗号化復号化手段と、認証手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、を備えており、所定のネットワークと接続可能とされている第1通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第2通信装置であって、

前記第1通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第2通信装置解生成手段と、

前記第2通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第1通信装置第1暗号化復号化手段で行われるのと同じ暗号化を行うことができる第2通信装置第1暗号化復号化手段と、

共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、

を備えており、

前記第2通信装置解生成手段で生成した解を前記ネットワークを介して前記第1通信装置に送るようになっているとともに、

前記第1通信装置は、前記第2通信装置から前記ネットワークを介して前記解を受取り、前記第1通信装置解生成手段で解を生成させ、前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっているとともに、前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第2通信装置を正当なものと認証したとの通知を前記ネット

ワークを介して前記第2通信装置に送るようになっており、

前記通知を前記第1通信装置から受けた前記第2通信装置の前記第2通信装置解生成手段が2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を前記第2通信装置第1暗号化復号化手段で暗号化するとともに暗号化された前記共通鍵を前記ネットワークを介して前記第1通信装置に送るようになっており、

前記第1通信装置は、前記第1通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第1通信装置との間で共通鍵方式の暗号化通信を行うようになっている、

第2通信装置。

[請求項8]

解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いた復号化を行うことのできる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えており、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して第1通信装置に送るようになっている、所定のネットワークと接続可能とされている第2通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第1通信装置であって、

前記第2通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第1通信装置解生成手段と、

前記第1通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第2通信装置第1暗号化復号化手段で行われるのと同じ暗号化を行うことができる第1通信装置第1暗号化復号化手段と、

共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、

前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するようになっている認証手段と、

を備えており、

前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第1通信装置解生成手段が2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて自らが持つ共通鍵を前記第1通信装置第1暗号化復号化手段で暗号化する処理を実行して、暗号化された前記共通鍵を前記ネットワークを介して前記第2通信装置に送るようになっており、

前記第2通信装置は、前記第2通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第2通信装置解生成手段によって生成された解を用いて、前記第1通信装置から受取った暗号化された前記共通鍵を前記第2通信装置第1暗号化復号化手段で復号化するようになっており、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに

に、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第2通信装置との間で共通鍵方式の暗号化通信を行うようになっている、

第1通信装置。

[請求項9]

解を連続して生成することのできる第2通信装置解生成手段と、前記第2通信装置解生成手段で生成された解を用いた暗号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えており、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して第1通信装置に送るようになっている、所定のネットワークと接続可能とされている第2通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第1通信装置であって、

前記第2通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第1通信装置解生成手段と、

前記第1通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第2通信装置第1暗号化復号化手段で行われるのと同じ復号化を行うことができる第1通信装置第1暗号化復号化手段と、

共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、

前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するようになっている認証手段と、

を備えており、

前記第2通信装置が正当だとの認証が前記認証手段で行われた場合に、前記第2通信装置を正当なものと認証したとの通知を前記ネット

ワークを介して前記第2通信装置に送るようになっており、

前記第2通信装置は、前記通知を前記第1通信装置から受けたら、前記第2通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を前記第2通信装置第1暗号化復号化手段で暗号化するとともに暗号化された前記共通鍵を前記ネットワークを介して前記第1通信装置に送るようになっており、

前記第1通信装置解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で前記第1通信装置解生成手段によって生成された解を用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第2通信装置との間で共通鍵方式の暗号化通信を行うようになっている、

第1通信装置。

[請求項10]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置として、コンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、

前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証し、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理が実行された後に、前記第1通信装置から暗号化された前記共通鍵を前記ネットワークを介して受取る過程、

その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を復号化する過程、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を実行させるためのコンピュータプログラム。

[請求項11]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置として、コンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

その解生成手段で解を生成させ、その解を前記ネットワークを介して前記第1通信装置に送信する過程、

前記第1通信装置が、前記第2通信装置から前記ネットワークを介して前記解を受取り、その解生成手段で解を生成させ、前記第1通信

装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証し、前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第1通信装置から前記第2通信装置が正当なものと認証されたという通知を前記ネットワークを介して受取る過程、

前記通知を受取った後に、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、

暗号化した共通鍵を、前記第1通信装置へと前記ネットワークを介して送信する過程、

前記第1通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を復号化する処理を実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を実行させるためのコンピュータプログラム。

[請求項12]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置として、コンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、

前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する過程、

前記第1通信装置から前記第2通信装置に暗号化された前記共通鍵を前記ネットワークを介して送信する過程、

暗号化された前記共通鍵を受取った前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて暗号化された前記共通鍵を復号化することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を実行させるためのコンピュータプログラム。

[請求項13]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置として、コンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

前記第2通信装置が、その解生成手段で解を生成させ、前記ネットワークを介して送ってきた前記解を受取る過程、

前記第1通信装置の解生成手段で解を生成させ、前記第1通信装置の解生成手段で生成した解と、前記第2通信装置から受取った解とを

比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第2通信装置が正当だとの認証が前記第1通信装置で行われた場合に、前記第2通信装置を正当なものと認証したとの通知を前記ネットワークを介して前記第2通信装置に送る過程、

前記第2通信装置を正当なものと認証したとの通知を前記第1通信装置から受けた前記第2通信装置が、その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて自らが持つ共通鍵を暗号化する処理を行った後に、前記第2通信装置から前記ネットワークを介して送信された暗号化された前記共通鍵を受取る過程、

その解生成手段で2つ目或いはそれ以降の解を生成するとともに、2つ目以降の予め定められた条件下で生成された解を用いて、第2通信装置から受取った暗号化された前記共通鍵を復号化する過程、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を実行させるためのコンピュータプログラム。

[請求項14]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置で実行される通信方法であって、

前記第2通信装置が実行する、

その解生成手段で複数の解を生成させ、その解のうちの1つと、その解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものと、を前記ネットワークを介して前記第1通信装置に送信する過程、

前記第1通信装置が、前記第2通信装置から前記ネットワークを介

して前記解を受取り、その解生成手段で複数の解を生成させ、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するとともに、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する処理を実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、
を含んでなる、通信方法。

[請求項15]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置で実行される通信方法であって、

前記第1通信装置が実行する、

前記第2通信装置が、その解生成手段で複数の解を生成させ、その解のうちの1つと、その解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものとを前記ネットワークを介して送ってきた場合に前記解と暗号化された共通鍵とを受取る過程、

前記第1通信装置の解生成手段で複数の解を生成させ、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置の解生成手段で生成されたときと共通

条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を含んでなる、通信方法。

[請求項16]

解を連続して生成することのできる第1通信装置解生成手段と、前記第1通信装置解生成手段で生成された解を用いた暗号化と復号化を行うことができる第1通信装置第1暗号化復号化手段と、認証手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、を備えており、所定のネットワークと接続可能とされている第1通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第2通信装置であって、

前記第1通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第2通信装置解生成手段と、

前記第2通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第1通信装置第1暗号化復号化手段で行われるのと同じ暗号化と復号化を行うことができる第2通信装置第1暗号化復号化手段と、

共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、

を備えており、

前記第2通信装置解生成手段で生成した複数の解のうちの1つと、前記第2通信装置解生成手段で生成した解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものとを前記ネットワークを介して前記第1通信装置に送るようになっており、

前記第1通信装置は、前記第2通信装置から前記ネットワークを介して前記解と暗号化された前記共通鍵とを受取り、前記第1通信装置解生成手段で複数の解を生成させ、前記第1通信装置解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっており、前記第1通信装置解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第1通信装置との間で共通鍵方式の暗号化通信を行うようになっている、

第2通信装置。

[請求項17]

解を連続して生成することのできる第2通信装置解生成手段と、前

記第2通信装置解生成手段で生成された解を用いた暗号化と復号化を行うことができる第2通信装置第1暗号化復号化手段と、共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第2通信装置第2暗号化復号化手段と、を備えており、前記第2通信装置解生成手段で生成した解を前記ネットワークを介して第1通信装置に送るようになっている、所定のネットワークと接続可能とされている第2通信装置との組合せにより、暗号化通信システムを構成するための、前記ネットワークに接続可能とされた第1通信装置であって、

前記第2通信装置解生成手段で生成されたものと共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる第1通信装置解生成手段と、

前記第1通信装置解生成手段で生成された解を用いて、同じ解が用いられる場合には前記第2通信装置第1暗号化復号化手段で行われるのと同じ暗号化と復号化を行うことができる第1通信装置第1暗号化復号化手段と、

共通鍵を用いた共通鍵方式での暗号化と復号化とを行うことのできる第1通信装置第2暗号化復号化手段と、

前記第1通信装置解生成手段で生成した解と、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するようになっている認証手段と、

を備えており、

前記第2通信装置が、前記第2通信装置解生成手段で生成した複数の解のうちの1つと、前記第2通信装置解生成手段で生成した解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものとを前記ネットワークを介して前記第1通信装置に送ってきた場合に、それらを受取るようになっているとともに、

前記第1通信装置解生成手段で複数の解を生成させ、前記第1通信装置解生成手段で生成した解であって前記第2通信装置から送られて

きた解が前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記認証手段で前記第2通信装置を正当なものと認証するようになっているとともに、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を前記第1通信装置第1暗号化復号化手段で復号化するようになっており、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うとともに、前記第2通信装置第2暗号化復号化手段が送受信の対象となるデータに対して暗号化と復号化を行うことで、前記第2通信装置との間で共通鍵方式の暗号化通信を行うようになっている、

第1通信装置。

[請求項18]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第2通信装置として、コンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

その解生成手段で複数の解を生成させ、その解のうちの1つと、その解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものと、を前記ネットワークを介して前記第1通信装置に送信する過程、

前記第1通信装置が、前記第2通信装置から前記ネットワークを介

して前記解を受取り、その解生成手段で複数の解を生成させ、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた解が前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証するとともに、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から前記第1通信装置が受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する処理を実行することによって、前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第1通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を実行させるためのコンピュータプログラム。

[請求項19]

所定のネットワークにそれぞれ接続可能とされると共に、共通条件下で生成されたもの同士を比較すれば同じものとなる解を連続して生成することのできる解生成手段をともに備える第1通信装置と第2通信装置とを含んで構成される暗号化通信システムの前記第1通信装置として、コンピュータを機能させるためのコンピュータプログラムであって、

前記コンピュータに、

前記第2通信装置が、その解生成手段で複数の解を生成させ、その解のうちの1つと、その解のうちの他の1つを用いて自らが持つ共通鍵を暗号化したものとを前記ネットワークを介して送ってきた場合に前記解と暗号化された共通鍵とを受取る過程、

前記第1通信装置の解生成手段で複数の解を生成させ、前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送ら

れてきた解が前記第2通信装置の解生成手段で生成されたときと共通条件下で生成されたものと、前記第2通信装置から受取った解とを比較して、両者が一致した場合には、前記第2通信装置を正当なものと認証する過程、

前記第1通信装置の解生成手段で生成した解であって前記第2通信装置から送られてきた暗号化された前記共通鍵を暗号化する際に使用された解が前記第2通信装置の解生成手段で生成されたときと共通条件下で作成されたものを用いて、前記第2通信装置から受取った暗号化された前記共通鍵を、前記第2通信装置が前記共通鍵を暗号化したのと同じアルゴリズムを用いて復号化する過程、

以上により前記第1通信装置と前記第2通信装置で共有されることになった前記共通鍵を用いて、前記第2通信装置との間で、共通鍵方式の暗号化通信を行う過程、

を実行させるためのコンピュータプログラム。

[請求項20] 前記第1通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、

前記第2通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いる、

請求項2記載の通信方法。

[請求項21] 前記第2通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、

前記第1通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いる、

請求項3記載の通信方法。

[請求項22] 前記第1通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、

前記第2通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いる、

請求項4記載の通信方法。

[請求項23] 前記第2通信装置が、自らが持つ共通鍵を暗号化する処理を実行するために、その解生成手段で生成された解を複数用いるとともに、

前記第1通信装置が、暗号化された前記共通鍵を復号化する処理を実行するために、その解生成手段で生成された解を複数用いる、

請求項5記載の通信方法。

[請求項24] 前記共通鍵方式の暗号化通信を行う場合の暗号化と復号化を、第2通信装置を構成する前記コンピュータ上における、前記コンピュータ上で実行される暗号化の対象となる平文のデータを扱う所定のアプリケーションと、TCP/IPとの間で実行させるようになっているとともに、

前記アプリケーションで生成された平文を暗号化してから前記第1通信装置に送信するために前記TCP/IPに渡し、前記TCP/IPから渡された前記第1通信装置から送られてきた暗号化されたデータを平文に復号化してから前記アプリケーションに渡すようになっている、

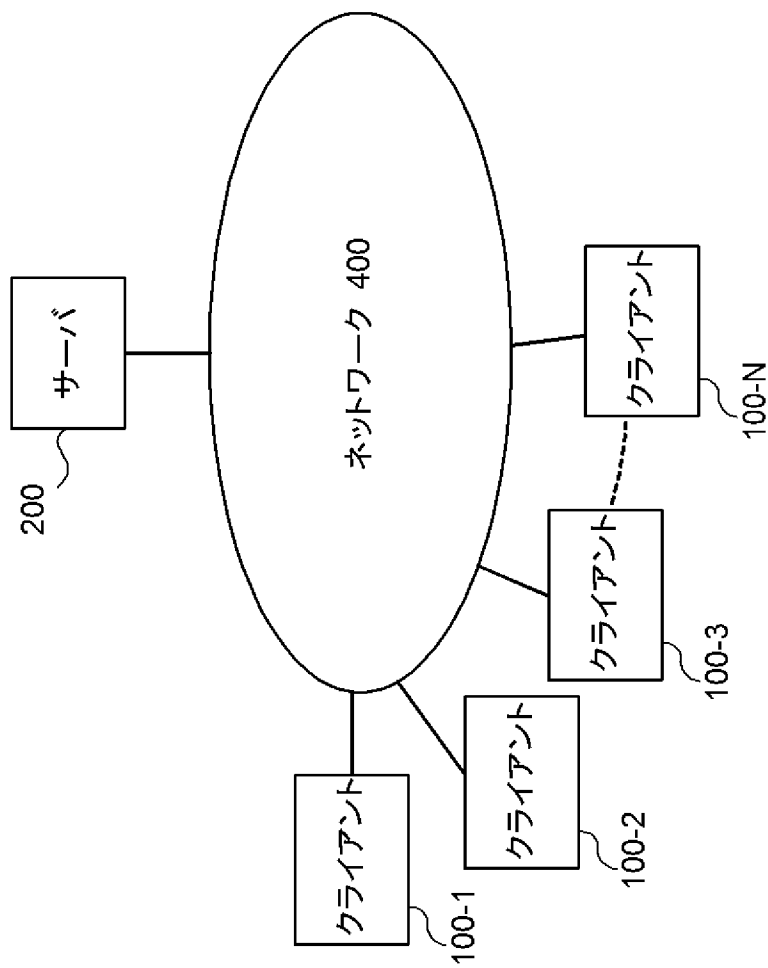
請求項10、11又は18記載のコンピュータプログラム。

[請求項25] 前記共通鍵方式の暗号化通信を行う場合の暗号化と復号化を、第1通信装置を構成する前記コンピュータ上における、前記コンピュータ上で実行される暗号化の対象となる平文のデータを扱う所定のアプリケーションと、TCP/IPとの間で実行させるようになっているとともに、

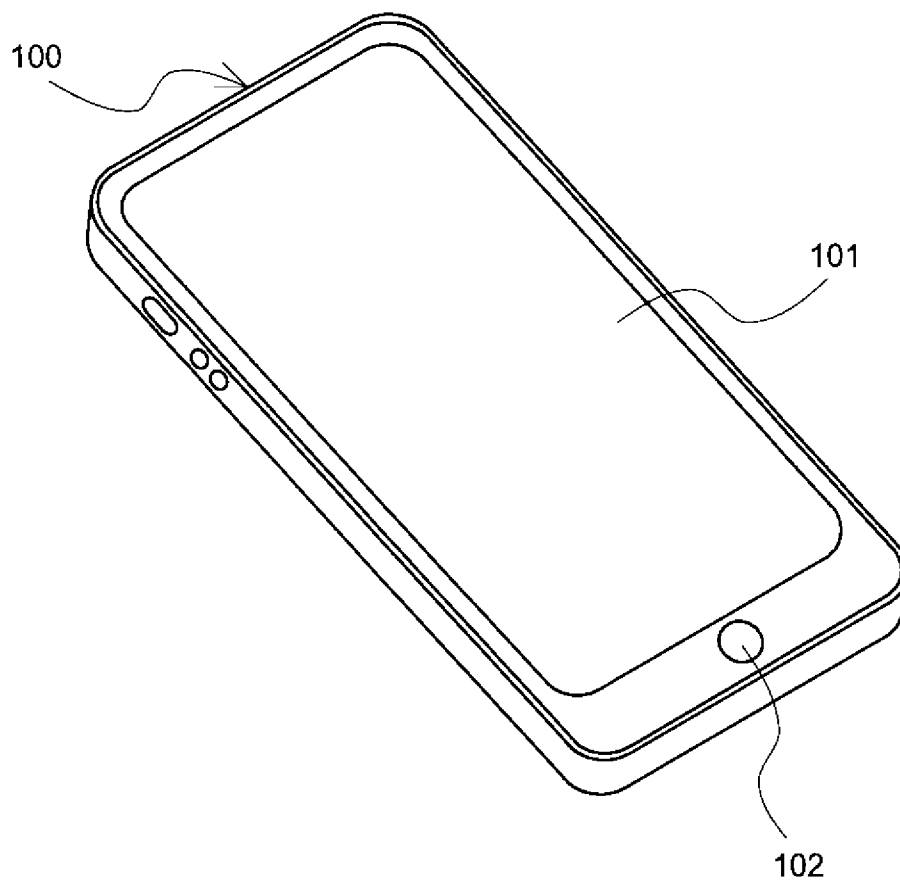
前記アプリケーションで生成された平文を暗号化してから前記第2通信装置に送信するために前記TCP/IPに渡し、前記TCP/IPから渡された前記第2通信装置から送られてきた暗号化されたデータを平文に復号化してから前記アプリケーションに渡すようになっている、

請求項12、13又は19記載のコンピュータプログラム。

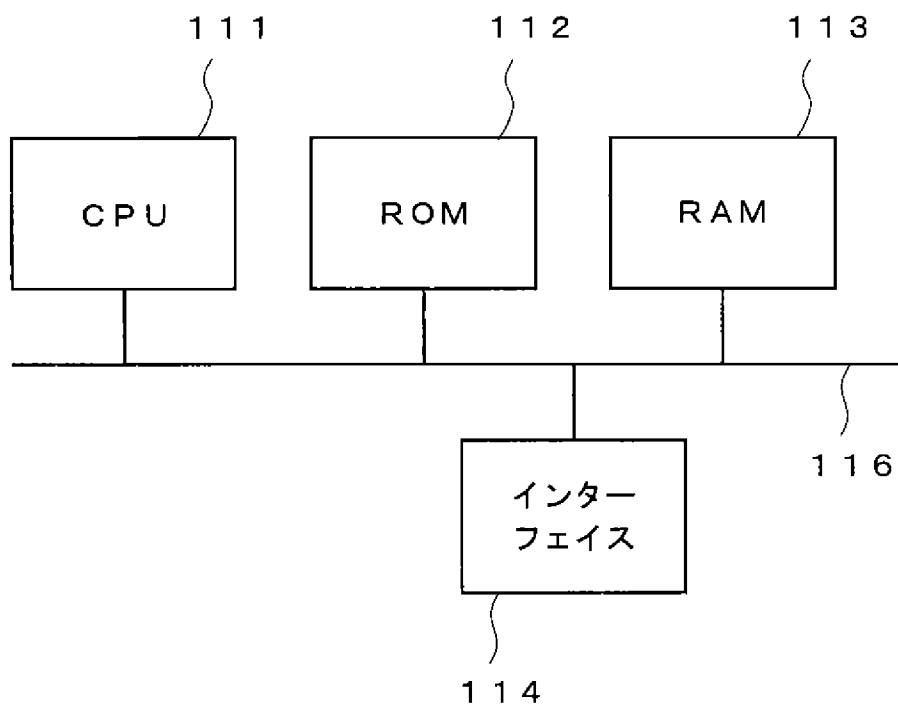
[図1]



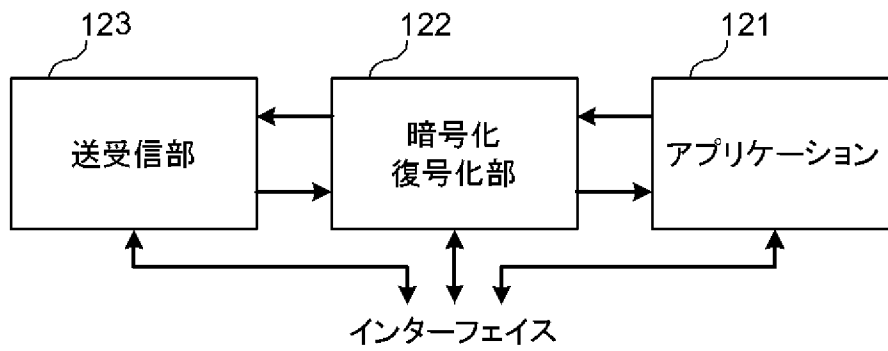
[図2]



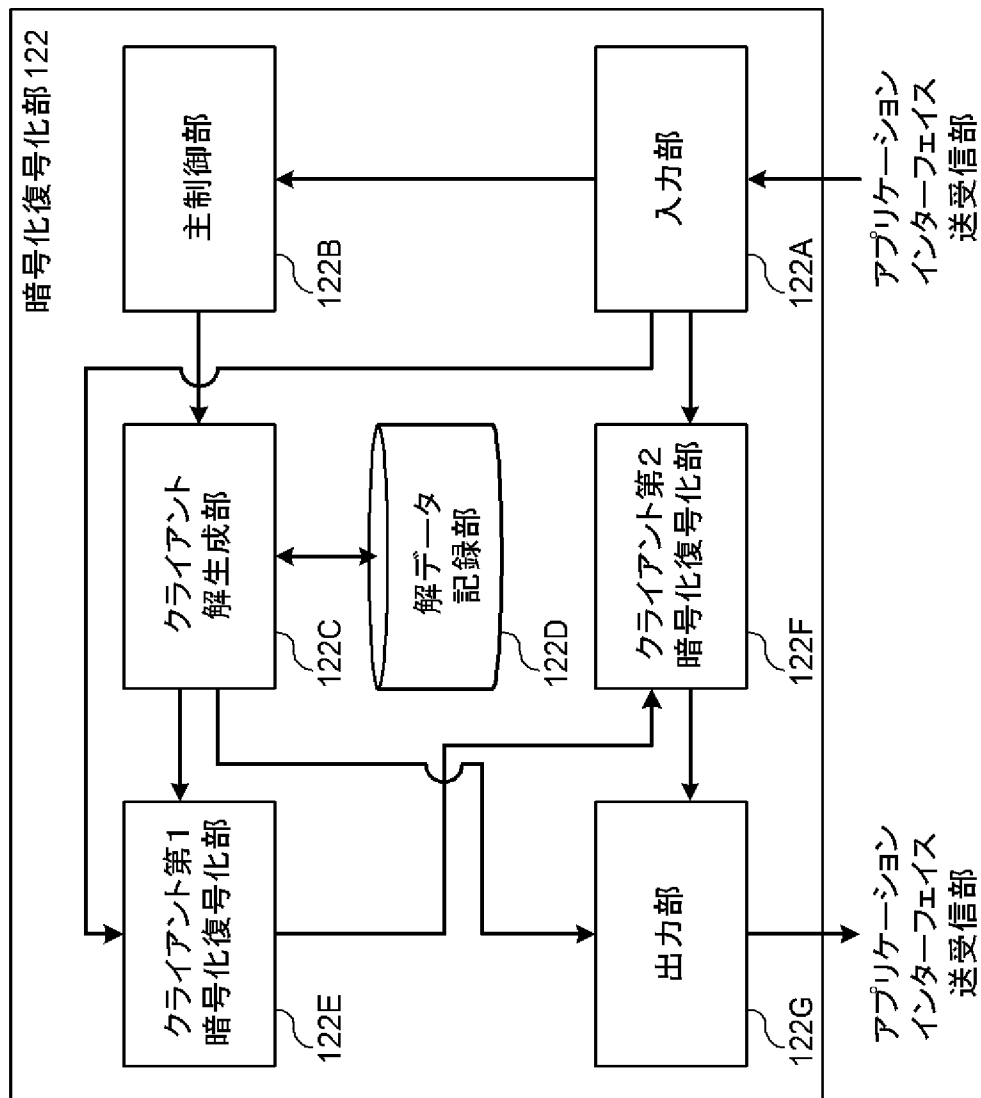
[図3]



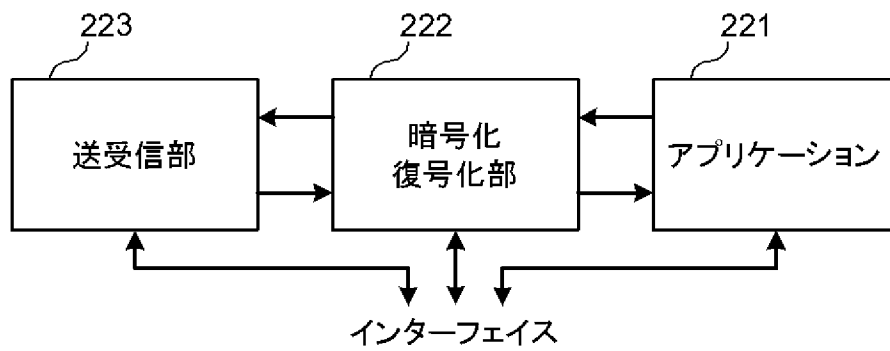
[図4]



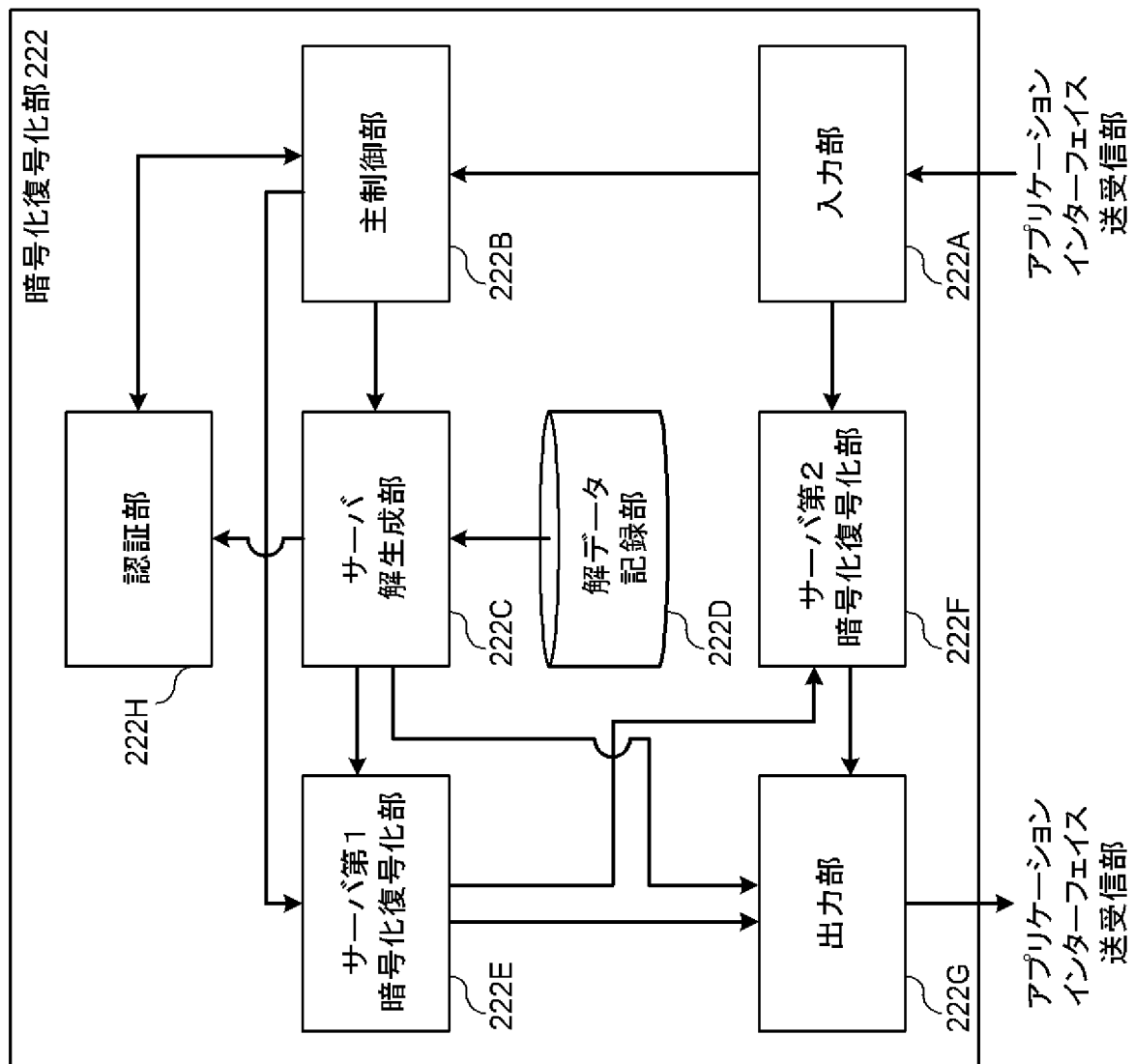
[図5]



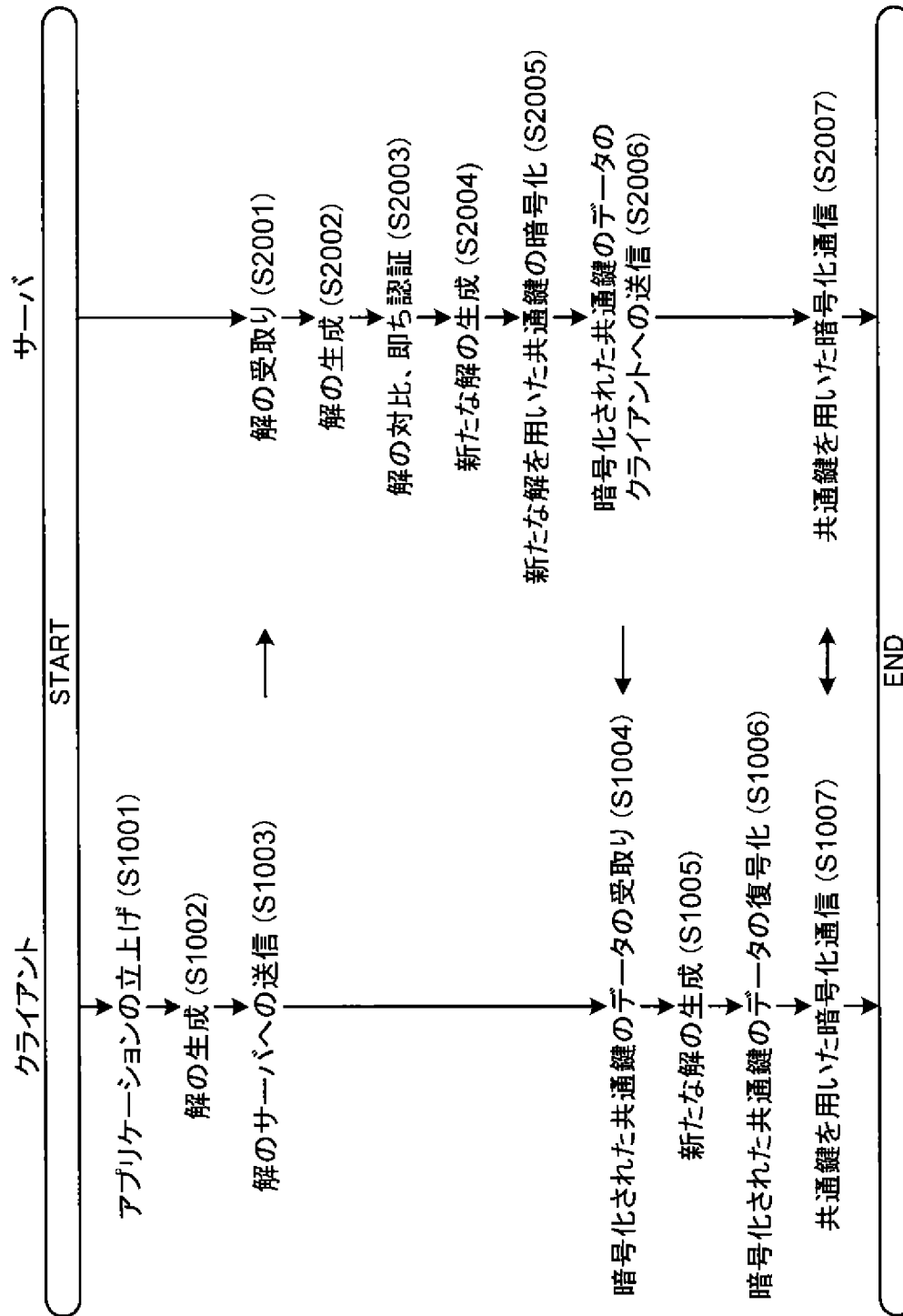
[図6]



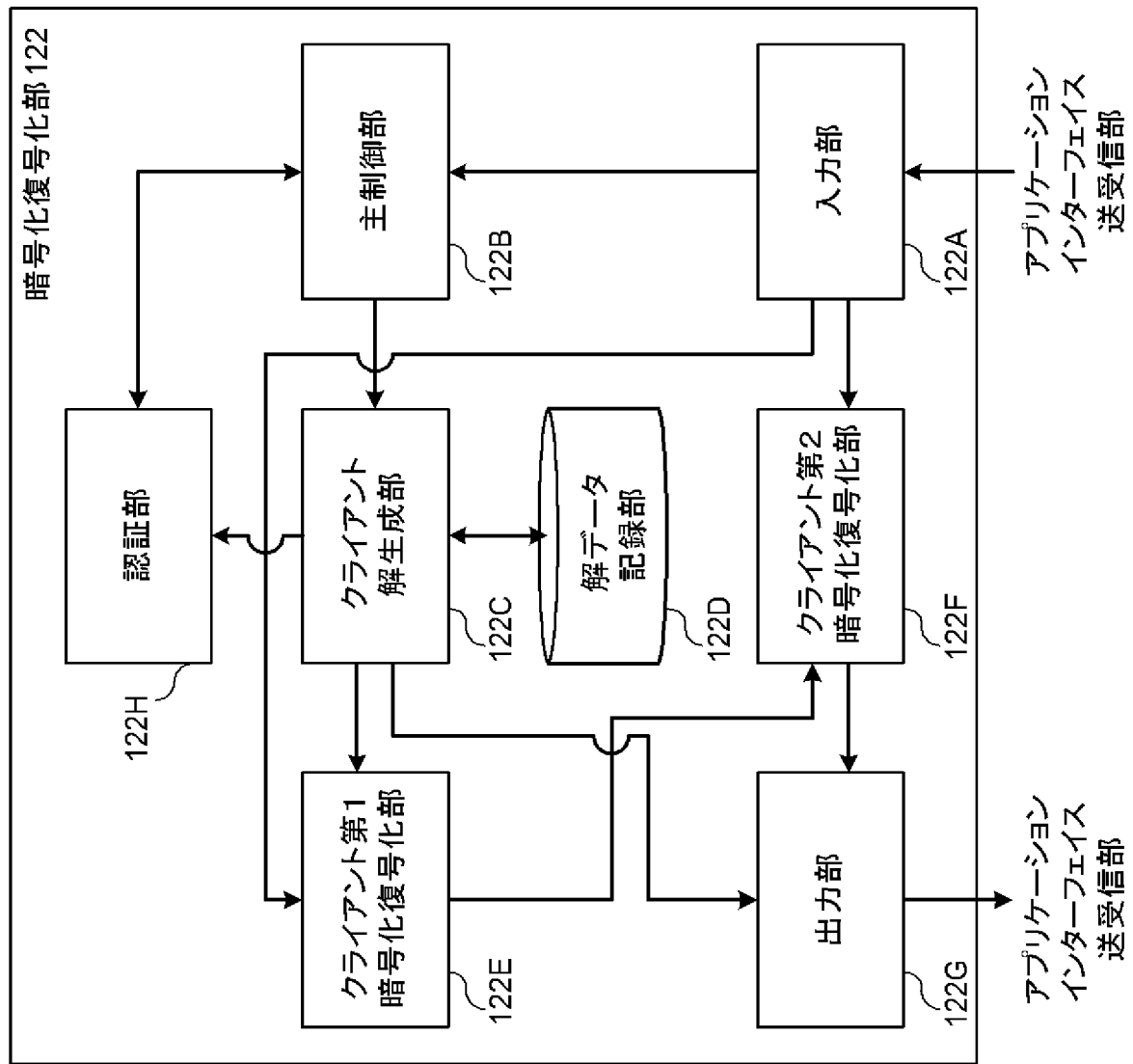
[図7]



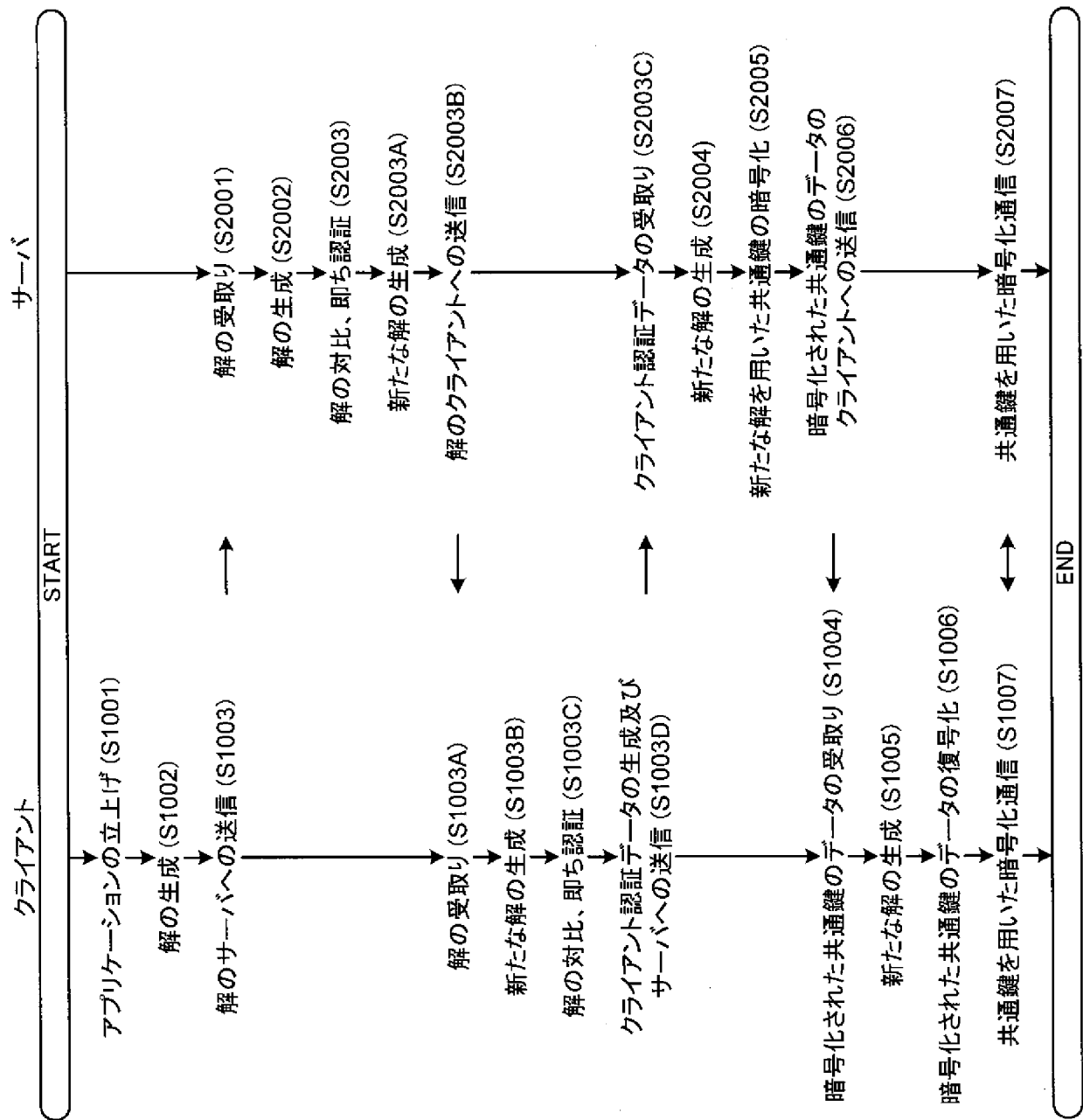
[図8]



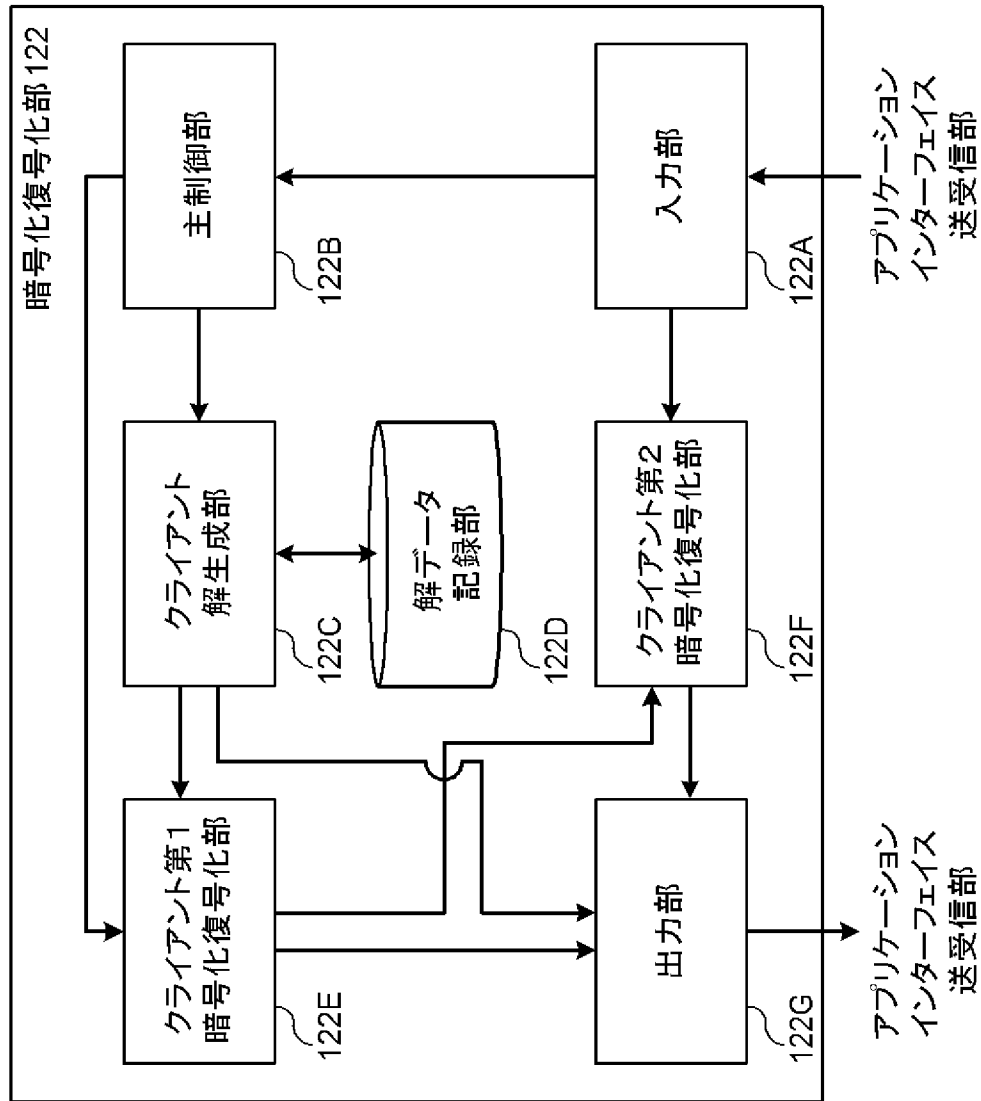
[図9]



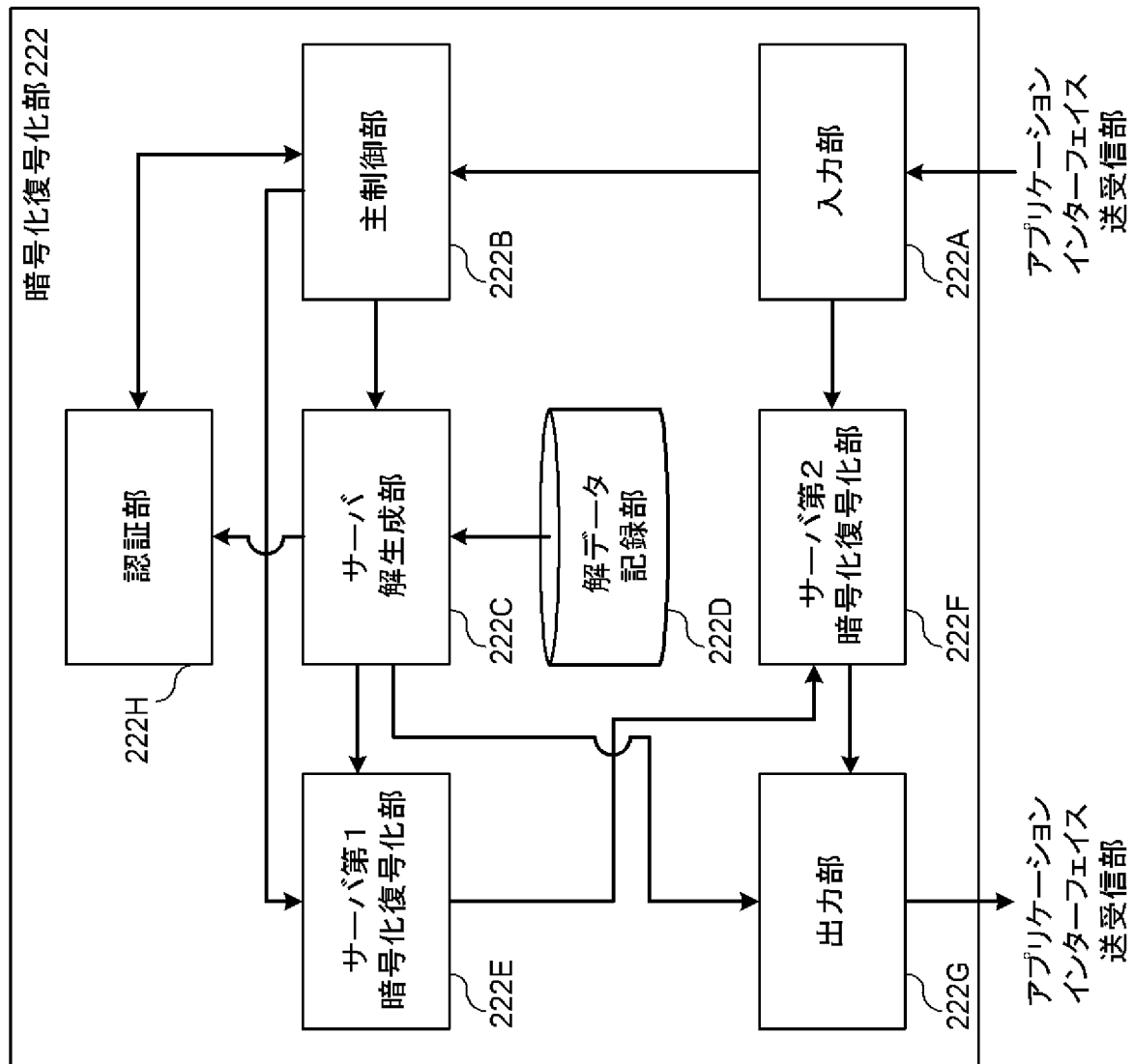
[図10]



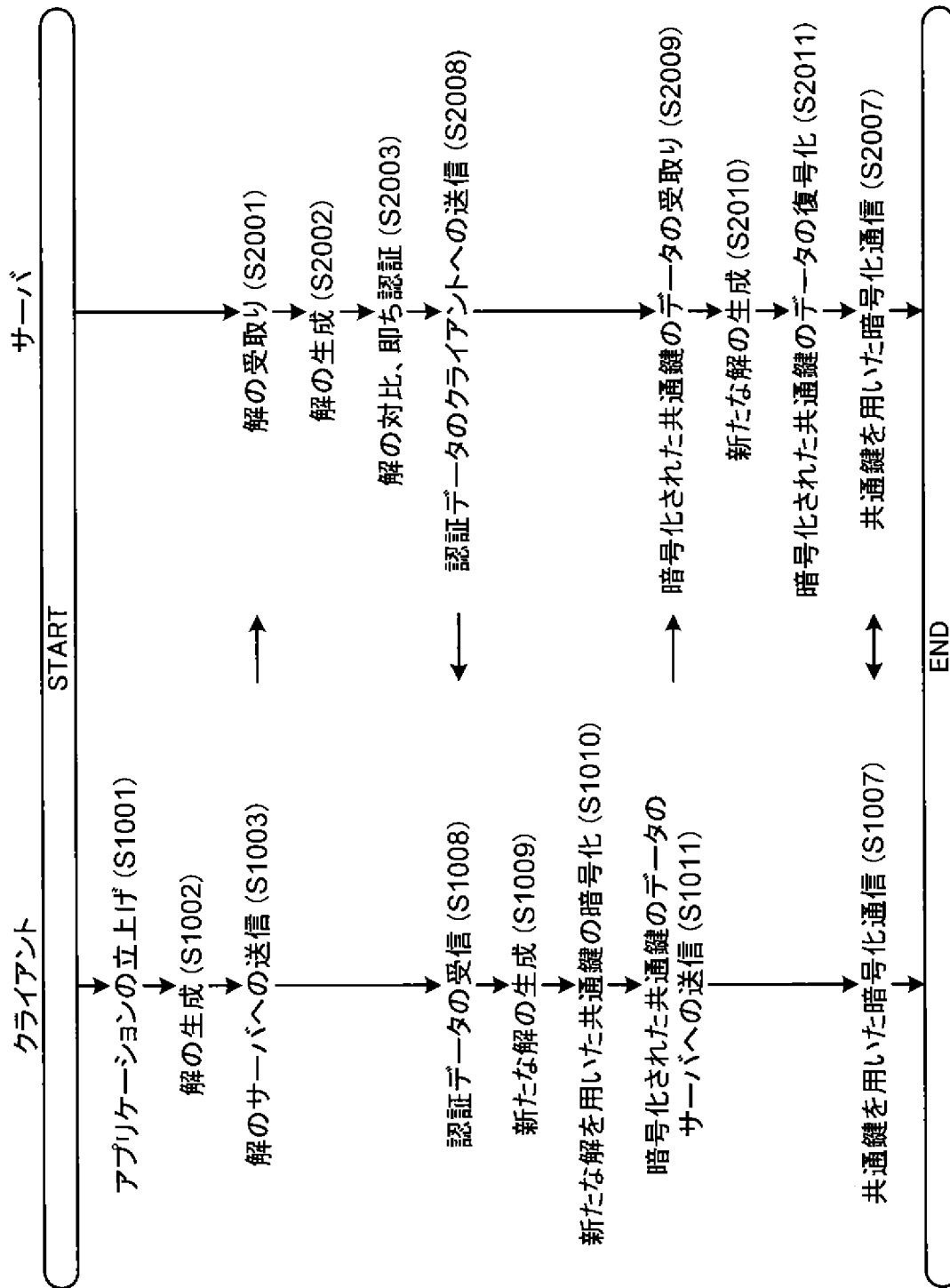
[図11]



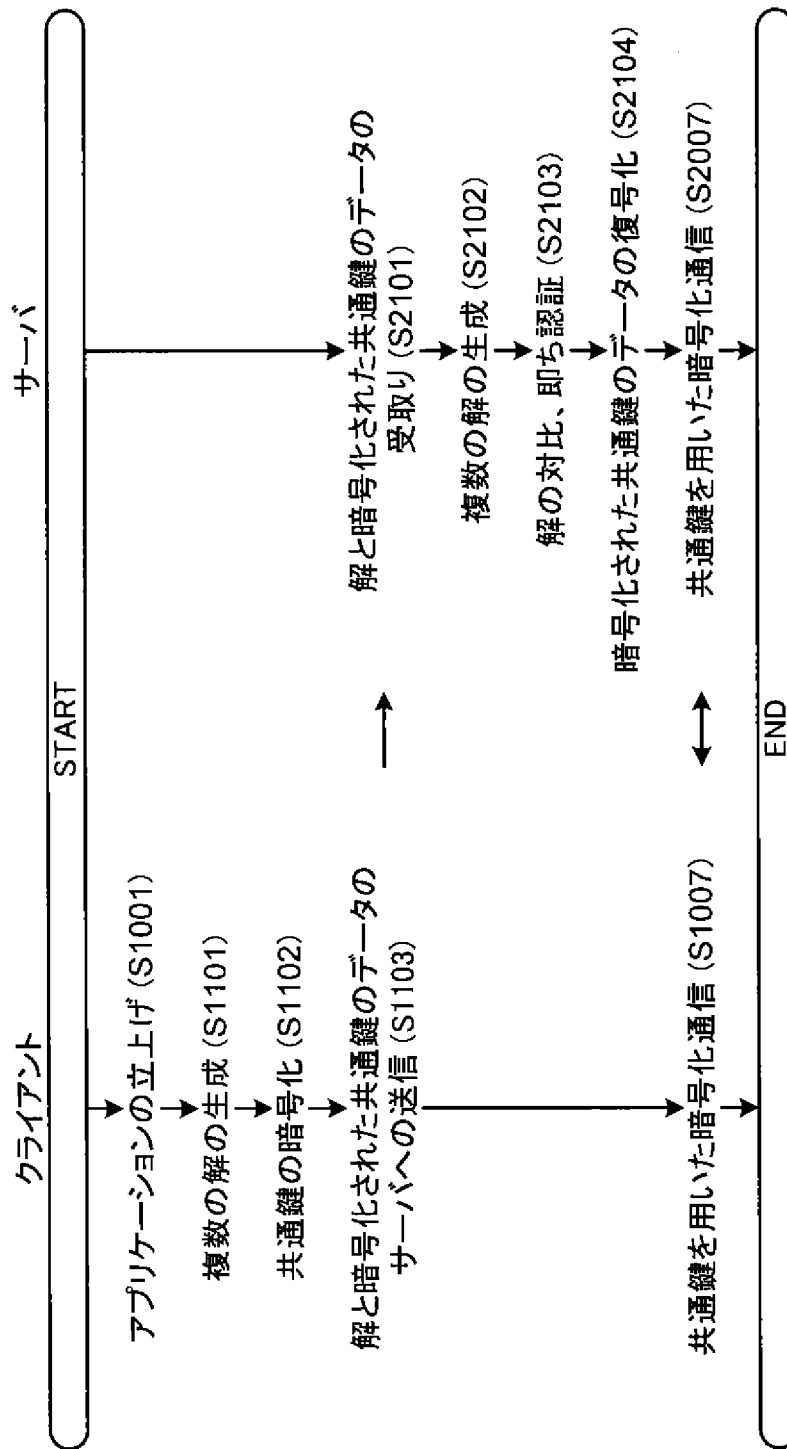
[図12]



[図13]



[図14]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/028391

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i, G06F21/44(2013.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/08, G06F21/44, G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2009-253650 A (N-Crypt Lab., Inc.), 29 October 2009 (29.10.2009), paragraphs [0022] to [0046], [0048]; fig. 1 to 5 & US 2011/0305334 A1 paragraphs [0089] to [0204], [0212]; fig. 1 to 5 & US 2015/0067324 A1 & WO 2009/123366 A1 & EP 2267937 A1 & TW 201014312 A	1-25
Y	JP 2008-234048 A (Quality Corp.), 02 October 2008 (02.10.2008), paragraphs [0041] to [0056], [0063] to [0081]; fig. 1 to 4 (Family: none)	1-25

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
04 October 2017 (04.10.17)

Date of mailing of the international search report
17 October 2017 (17.10.17)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/028391

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-218866 A (Communications Research Laboratory), 31 July 2003 (31.07.2003), paragraphs [0063] to [0073]; fig. 2 & US 2003/0145202 A1 paragraphs [0070] to [0080]; fig. 2 & DE 10303074 A	1-13, 24-25
Y	JP 2015-72511 A (Sakura Information Systems Co., Ltd.), 16 April 2015 (16.04.2015), paragraphs [0050] to [0054] & JP 5555799 B1	14-23
A	JP 2015-130633 A (Panasonic Intellectual Property Management Co., Ltd.), 16 July 2015 (16.07.2015), paragraphs [0036], [0044], [0054] to [0058]; fig. 1, 3 & US 2015/0195280 A1 paragraphs [0051], [0059], [0069] to [0073]; fig. 1, 3 & WO 2015/104765 A1 & EP 3092769 A1	1-25

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/08(2006.01)i, G06F21/44(2013.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. H04L9/08, G06F21/44, G09C1/00, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2009-253650 A（株式会社エヌクリプトラボ）2009.10.29, 段落 [0022] - [0046]、[0048]、[図1] - [図5] & US 2011/0305334 A1, 段落 [0089] - [0204]、[0212]、 FIG. 1-5 & US 2015/0067324 A1 & WO 2009/123366 A1 & EP 2267937 A1 & TW 201014312 A	1-25
Y	JP 2008-234048 A（クオリティ株式会社）2008.10.02, 段落 [0041] - [0056]、[0063] - [0081]、 [図1] - [図4]（ファミリーなし）	1-25

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

04.10.2017

国際調査報告の発送日

17.10.2017

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

青木 重徳

5 S

4229

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2003-218866 A (独立行政法人通信総合研究所) 2003.07.31, 段落 [0063] - [0073]、[図2] & US 2003/0145202 A1, 段落 [0070] - [0080]、FIG. 2 & DE 10303074 A	1-13, 24-25
Y	JP 2015-72511 A (さくら情報システム株式会社) 2015.04.16, 段落 [0050] - [0054] & JP 5555799 B1	14-23
A	JP 2015-130633 A (パナソニックIPマネジメント株式会社) 2015.07.16, 段落 [0036]、[0044]、[0054] - [0058]、[図1]、[図3] & US 2015/0195280 A1, 段落 [0051]、[0059]、[0069] - [0073]、FIG. 1、FIG. 3 & WO 2015/104765 A1 & EP 3092769 A1	1-25