(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
2019年5月16日(16.05.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/093201 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 12/58* (2006.01)
H04L 9/16 (2006.01) *H04L 12/66* (2006.01)

(21) 国際出願番号： PCT/JP2018/040472

(22) 国際出願日： 2018年10月31日(31.10.2018)

(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 2017-214927 2017年11月7日(07.11.2017) JP

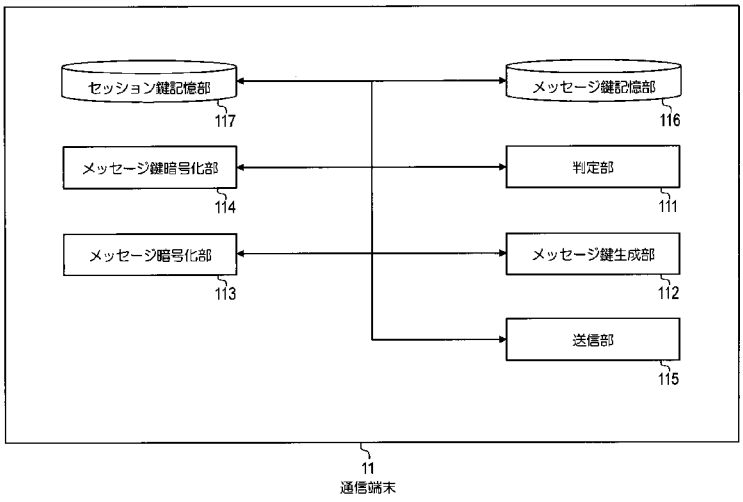
(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 岡野 裕樹 (**OKANO, Yuki**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 吉田 麗生 (**YOSHIDA, Reo**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 西巻 陵 (**NISHIMAKI, Ryo**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 小林 鉄太郎 (**KOBAYASHI, Tetsutaro**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(54) **Title:** COMMUNICATION TERMINAL, SERVER DEVICE, AND PROGRAM

(54) 発明の名称： 通信端末、サーバ装置、プログラム

[図3]



11 Communication terminal
111 Determining unit
112 Message-key generating unit
113 Message encrypting unit
114 Message-key encrypting unit
115 Transmission unit
116 Message-key storing unit
117 Session-key storing unit

(57) **Abstract:** Provided is a communication terminal capable of reducing a load on a server device by reusing a message key used for encryption of a message. The communication terminal comprises: a session-key storing unit for storing a session key that is shared with other communication terminals and is not shared with a server device; a message-key generating unit for generating a message key; a message-key storing unit for storing the message key to be reused in association with a message-key identifier; a message encrypting unit for generating a message cryptogram by using the

WO 2019/093201 A1

[続葉有]

(74) 代理人：中尾 直樹，外 (NAKAO, Naoki et al.)；〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル６階 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, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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：

— 国際調査報告（条約第21条(3)）

message and the message key on the basis of a common key cryptosystem; a message-key encrypting unit for generating a message-key cryptogram by using the session key and the message key on the basis of a re-encryptable common key cryptosystem; and a cryptogram transmission unit for transmitting, to the server device, a group identifier as an identifier of a group to which this communication terminal belongs, a message-key cryptogram or a message-key identifier, and a message cryptogram.

(57) 要約：メッセージの暗号化に用いるメッセージ鍵を再利用することにより、サーバ装置の負荷を軽減することができる通信端末を提供する。他の通信端末と共有され、サーバ装置と共有されないセッション鍵を記憶するセッション鍵記憶部と、メッセージ鍵を生成するメッセージ鍵生成部と、再利用されるメッセージ鍵をメッセージ鍵識別子と関連付けて記憶するメッセージ鍵記憶部と、メッセージとメッセージ鍵を用い、共通鍵暗号方式に基づいて、メッセージ暗号文を生成するメッセージ暗号化部と、セッション鍵とメッセージ鍵を用い、再暗号化可能な共通鍵暗号方式に基づいて、メッセージ鍵暗号文を生成するメッセージ鍵暗号化部と、自機が属するグループの識別子であるグループ識別子と、メッセージ鍵暗号文またはメッセージ鍵識別子と、メッセージ暗号文をサーバ装置に送信する暗号文送信部を含む。

明　細　書

発明の名称 ： 通信端末、サーバ装置、プログラム

技術分野

[0001] 本発明は、通信端末、サーバ装置、プログラムに関する。

背景技術

[0002] ビジネスでの使用を前提とするメッセージ送信システムとしてパソコンやスマートフォン等のマルチデバイスに対応可能なシステムが存在する。マルチデバイスに対応可能なシステムのうち、企業の機密情報漏えいを考慮し、通信端末にデータを残さないクラウドベース型のメッセージ送信システムが存在する。クラウドベース型のメッセージ送信システムの例として、非特許文献１が挙げられる。

[0003] このようなメッセージ送信システムにおいては、通信路を暗号化することで通信経路上の盗聴防止がなされていたり、既に述べたように、通信端末にデータを残さないことによって通信端末の紛失や不正な持ち出しに起因する情報漏えい防止がなされていたりする。このように、従来のメッセージ送信システムは「通信経路」と「通信端末」に対する脅威に対処している一方、サーバ装置に対する脅威への対処は不十分である。

[0004] ここでいうサーバ装置に対する脅威として「サーバ装置に対する外部からの攻撃」や「サーバ管理者等による内部不正」等が挙げられる。これらの脅威に対し、メッセージを暗号化して保存する、という対策が考えられる。しかしながら、サーバ装置側でメッセージを復号可能である以上、前述の脅威に対してサーバ装置からのメッセージ漏えいの可能性が依然として存在する。送受信・保存を行うサーバ装置に送られてくるメッセージがサーバ装置に対して秘匿化されている（サーバ装置側で盗聴されない）ことが重要である。

[0005] １つの方法として、サーバ装置に対してメッセージを秘匿し、通信端末でのみ復号可能なエンドツーエンドの暗号化通信を実現することが考えられる

。この場合、通信端末間で用いる共通鍵をどのように共有するかが問題となる。この問題の解決策として例えば非特許文献２が開示されている。非特許文献２では中央に認証サーバをもつスター型のネットワークにおいて、認証サーバに対していかなる情報ももらさずに利用者間で鍵（以下、セッション鍵）を共有するプロトコルが提案されている。

[0006] これによって、サーバ装置に対しメッセージを秘匿したまま通信端末間でやりとりすることができる。また、現在参加している通信端末でのみメッセージが読めるようセッション鍵の共有を行うため、ユーザの追加・削除等のイベントによりセッション鍵が更新される。

先行技術文献

非特許文献

[0007] 非特許文献1：ＮＴＴソフトウェア、“ビジネス向けグループチャットＴｏｐｉｃＲｏｏｍ”、[online]、ＮＴＴソフトウェア、[平成29年10月18日検索]、インターネット〈URL:https://www.ntt-tx.co.jp/products/topicroom/〉

非特許文献2：小林鉄太郎、米山一樹、吉田麗生、川原祐人、冨士仁、山本具英「スケーラブルな動的多者鍵配布プロトコル」、SCIS2016-暗号と情報セキュリティシンポジウム-講演論文集、一般社団法人電子情報通信学会、平成28年1月、4E2-3

発明の概要

発明が解決しようとする課題

[0008] 上記非特許文献２の技術によれば、サーバ装置に知られないよう、通信端末間でセッション鍵を共有することで、サーバ装置に対しメッセージを秘匿したままやりとりすることができる。しかし、上記のような通信システムにおいては、セッション鍵の更新に連動して、サーバ装置上で他の処理が発生する場合があり、サーバ装置の負荷が増大するおそれがある。特にグループチャットシステムのような、リアルタイム性が求められるシステムにおいて、サーバ装置上の処理に時間がかかるのは望ましくない。

[0009] そこで本発明は、メッセージの暗号化に用いるメッセージ鍵を再利用することにより、サーバ装置の負荷を軽減することができる通信端末を提供することを目的とする。

課題を解決するための手段

[0010] 本発明の通信端末は、サーバ装置を介して他の通信端末に暗号文を送信する通信端末であって、セッション鍵記憶部と、判定部と、メッセージ鍵生成部と、メッセージ鍵記憶部と、メッセージ暗号化部と、メッセージ鍵暗号化部と、暗号文送信部を含む。

[0011] セッション鍵記憶部は、他の通信端末と共有され、サーバ装置と共有されないセッション鍵を記憶する。判定部は、暗号文の送信がセッション鍵の生成後または更新後の最初の送信である場合にメッセージの暗号化に用いるメッセージ鍵を新規生成するものと判定し、それ以外の場合にメッセージ鍵を再利用するものと判定する。メッセージ鍵生成部は、判定の結果が新規生成である場合にメッセージ鍵を生成する。メッセージ鍵記憶部は、判定の結果が再利用である場合に再利用されるメッセージ鍵をメッセージ鍵識別子と関連付けて記憶する。メッセージ暗号化部は、メッセージと生成または記憶されたメッセージ鍵を用い、共通鍵暗号方式に基づいて、メッセージ暗号文を生成する。メッセージ鍵暗号化部は、判定の結果が新規生成である場合に、セッション鍵と生成されたメッセージ鍵を用い、再暗号化可能な共通鍵暗号方式に基づいて、メッセージ鍵暗号文を生成する。暗号文送信部は、判定の結果が新規生成である場合に、自機が属するグループの識別子であるグループ識別子と、メッセージ鍵暗号文と、メッセージ暗号文を、サーバ装置に送信し、判定の結果が再利用である場合に、グループ識別子と、メッセージ鍵識別子と、メッセージ暗号文をサーバ装置に送信する。

発明の効果

[0012] 本発明の通信端末によれば、メッセージの暗号化に用いるメッセージ鍵を再利用することにより、サーバ装置の負荷を軽減することができる。

図面の簡単な説明

[0013] [図1]実施例１の通信システムの構成を示すブロック図。

[図2]実施例１のサーバ装置の構成を示すブロック図。

[図3]実施例１のメッセージ送信動作を行う通信端末の構成を示すブロック図。

[図4]実施例１のメッセージ受信動作を行う通信端末の構成を示すブロック図。

[図5]実施例１の再暗号化鍵送信動作を行う通信端末の構成を示すブロック図。

[図6]実施例１のメッセージ配信動作（判定＝真）を示すシーケンス図。

[図7]実施例１のメッセージ配信動作（判定＝偽）を示すシーケンス図。

[図8]実施例１の再暗号化動作を示すシーケンス図。

発明を実施するための形態

[0014] 以下、本発明の実施の形態について、詳細に説明する。なお、同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

実施例 1

[0015] ＜概要＞

実施例１の通信システムでは、メッセージの暗号化に共通鍵暗号方式を利用する。メッセージの暗号化に利用する鍵（以下、メッセージ鍵）は、共通鍵ベースの再暗号化可能な暗号方式を利用してセッション鍵で暗号化される。このとき、メッセージ鍵を各メッセージの暗号化ごとに生成するのではなく、セッション鍵更新後、次にセッション鍵が更新されるまでの間、同じメッセージ鍵を使いまわす。サーバ装置ではメッセージの暗号文（以下、メッセージ暗号文）とメッセージ鍵の暗号文（以下、メッセージ鍵暗号文）をそれぞれ別のテーブル（記憶部）に記憶するが、その際、サーバ装置側でどのメッセージに対してどのメッセージ鍵が使いまわされているかを知ることができるようにするために鍵の識別子（鍵ＩＤ）を付加し、これをキーにして別のテーブル（記憶部）に記憶する。再暗号化処理が行われる際、サーバ装置はメッセージ鍵暗号文を記憶しているテーブル（記憶部）のみを更新する

。メッセージ鍵暗号文１つに対して、メッセージ暗号文は鍵ＩＤによって複数関連付けられているため、再暗号化対象は少なくなり、再暗号化処理時のサーバ装置の負荷が削減される。なお、再暗号化処理中はメッセージの復号を一度も行わないため、サーバ装置はメッセージの内容を知らないまま再暗号化処理を行うことになる。また、ログインやグループ参加時等で複数メッセージを同時に取得する際、メッセージ鍵を先に復号して一時的に保存し、メッセージ暗号文に付随する鍵ＩＤに対応するメッセージ鍵でメッセージを復号することによって、復号処理を削減することができる。

[0016] ＜準備＞

集合Nを正の整数全体の集合とする。$Kspace_1$,$Kspace_2$を鍵空間とする。共通鍵ベースの再暗号化可能な暗号方式は次の4つのアルゴリズム(KEM.Enc,KEM.Dec,KEM.ReKeyGen,KEM.ReEnc)からなり、それぞれ、以下の入出力をもつアルゴリズムである。

・$KEM.Enc(SK_{i1},K)\rightarrow C_1^{(i1)}$

$Kspace_1$の元SK_{i1}と$Kspace_2$の元Kを入力とし、暗号文$C_1^{(i1)}$を出力するアルゴリズム。

・$KEM.Dec(SK_j,C_1^{(i)})\rightarrow K'$

$Kspace_1$の元SK_jと暗号文$C_1^{(i)}$を入力とし、$Kspace_2$の元K'を出力するアルゴリズム。

・$KEM.ReKeyGen(SK_{i1},SK_{i2})\rightarrow RK_{i1,i2}$

$Kspace_1$の2つの元SK_{i1},SK_{i2}を入力とし、再暗号化鍵$RK_{i1,i2}$を出力するアルゴリズム。

・$KEM.ReEnc(RK_{i1,i2},C_1^{(i1)})\rightarrow C_1^{(i2)}$

再暗号化鍵$RK_{i1,i2}$と暗号文$C_1^{(i1)}$を入力とし、再暗号化暗号文$C_1^{(i2)}$を出力するアルゴリズム。

[0017] さらに、上記のアルゴリズムは以下の２条件も満たすものとする。

１）$Kspace_1$の任意の元SKと$Kspace_2$の任意の元Kに対し、KEM.Dec(SK,KEM.Enc(SK,K))=K

２）任意の整数n>1と$Kspace_1$の任意の鍵の列$SK_1,...,SK_n$と任意のi∈{1,...,n-1}に対してKEM.ReKeyGen(SK_i,SK_{i+1})によって出力される再暗号化鍵の列$RK_{1,2},...,RK_{n-1,n}$と$Kspace_1$の任意の元K，$1 \leqq i_1 < i_2 \leqq n$を満たす任意の$i_1$,$i_2$に対して、

KEM.Dec(SK_{i2},KEM.ReEnc($RK_{i2-1,i2}$,...KEM.ReEnc($RK_{i1,i1+1}$,KEM.Enc(SK_{i1},K))))=K

[0018] 上記を満たす再暗号化方式の例として参考特許文献１の方式が挙げられる。

（参考非特許文献１：D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan. 2015.Key Homo-morphic PRFs and Their Applications. CryptologyePrint Archive, Report 2015/220. (2015).）

[0019] これは以下のようにして構成される。まず、qを素数とし、Z_qを整数環Zに対する、qを法とする剰余環とする。Gを位数qの巡回群とし、$Kspace_2$=Gとする。ここでは、巡回群Gを乗法群で考えるが、加法群と考えてもよい。また、$Kspace_1$=Z_qとする。さらに、Randを乱数空間とし、H:Rand→GをRandを定義域とし、Gを値域とするハッシュ関数とする。$Kspace_1$=Z_qとRandとの直積を定義域とし、Gを値域とする関数F:Kspace×Rand→GをF(SK,r)=$H(r)^{SK}$で定義する。

・KEM.Enc(SK_{i1},K)→$C_1^{(i1)}$

r∈Randを一様ランダムに抽出し、$C_1^{(i1)}$=(r,K+F(SK,r))を出力する。

・KEM.Dec(SK_j,$C_1^{(i)}$)→K'

$C_1^{(i)}$=(r,C)と分解し、K'=C-F(SK,r)を出力する。

・KEM.ReKeyGen(SK_{i1},SK_{i2})→$RK_{i1,i2}$

$RK_{i1,i2}$=SK_{i2}-SK_{i1}を出力する。

・KEM.ReEnc($RK_{i1,i2}$,$C_1^{(i1)}$)→$C_1^{(i2)}$

$C_1^{(i1)}$=(r,C)と分解し、$C_1^{(i2)}$=(r,C+F($RK_{i1,i2}$,r))を出力する。

[0020] なお、再暗号化可能な暗号方式(KEM.Enc,KEM.Dec,KEM.ReKeyGen,KEM.ReEnc)の例として参考非特許文献１を挙げたが、上記以外の方法によって再暗号化可能な暗号方式を実現してもよく、特に限定しない。

[0021] 共通鍵暗号方式は次の２つのアルゴリズム(Enc,Dec)からなり、それぞれ、以下の入出力をもつアルゴリズムである。

・$Enc(K,m)\rightarrow C_2$

$Kspace_2$の元Kとメッセージmを入力とし、暗号文C_2を出力するアルゴリズムである。

・$Dec(K,C_2)\rightarrow m$

$Kspace_2$の元Kと暗号文C_2を入力とし、メッセージmを出力するアルゴリズムである。

[0022] さらに、上記のアルゴリズムは以下の条件を満たすものとする。

$Kspace_2$の任意の元Kと任意のメッセージmに対して、$Dec(K,Enc(K,m))=m$

[0023] 上記を満たす暗号方式の例として、AESやCamellia等が挙げられるが、ここでは限定しない。

[0024] 図１に示すように本実施例の通信システム１は、サーバ装置１０、通信端末１１、通信端末１２、通信端末１３を含み、各装置はネットワーク９により通信可能に接続されている。通信端末１１、通信端末１２、通信端末１３はパソコンやスマートフォン等で実現できるが特に限定しない。

[0025] 以下の説明では、通信端末１１はメッセージの暗号化および暗号化されたメッセージなどの送信を担当する端末であるものとし、通信端末１２は暗号化されたメッセージなどの受信および暗号化されたメッセージなどの復号を担当する端末であるものとし、通信端末１３は、後述する再暗号化鍵の生成および送信を担当する端末であるものとする。ただし、上記は説明の便宜上の割り振りであるため、例えば通信端末１１、通信端末１２、通信端末１３の機能をすべて併せ持つ通信端末を実現してもよい。

[0026] なお、本実施例の通信システム１では、チャットメッセージをやり取りするユーザのグループを形成することができる。各グループには識別子が与えられている。通信端末１１、通信端末１２、通信端末１３の利用者をそれぞれユーザＡ、ユーザＢ、ユーザＣとする。ユーザＡ、ユーザＢ、ユーザＣはグループ識別子groupIDを持つグループに属しているものとし、各通信端末はgroupIDを記憶しているものとする。

[0027] また、セッション鍵について説明する。セッション鍵は、グループ毎に、

そのグループに属するユーザが利用する通信端末間で共有される鍵のことをいう。その通信端末以外の、例えばサーバ装置１０に対してセッション鍵に関していかなる情報ももらさずに鍵を共有するプロトコルとして、参考非特許文献２が挙げられるが、セッション鍵共有方法については特に限定しない。

（参考非特許文献２：K. Yoneyama, R. Yoshida, Y. Kawahara, T. Kobayashi, H. Fuji,and T. Yamamoto. 2016.Multi-Cast Key Distribution. Scalable, Dynamic and Provably Secure Construction. Cryptology ePrint Archive, Report 2016/833. (2016).）

[0028] なお、セッション鍵を安全に共有するために、グループにユーザが追加される、グループからユーザが離脱する、一定時間が経過する、ユーザがログイン/ログアウトする度にセッション鍵が生成／更新されるものとする。

[0029] ＜通信システム１を構成する各装置の詳細＞

図２に示すように、サーバ装置１０は、受信部１０１と、メッセージ暗号文記憶部１０２と、メッセージ鍵暗号文記憶部１０３と、グループユーザ記憶部１０４と、配信部１０５と、再暗号化処理部１０６を含む。また、図３に示すように、通信端末１１は、判定部１１１と、メッセージ鍵生成部１１２と、メッセージ暗号化部１１３と、メッセージ鍵暗号化部１１４と、送信部１１５と、メッセージ鍵記憶部１１６と、セッション鍵記憶部１１７を含む。また、図４に示すように、通信端末１２は、受信部１２１と、メッセージ鍵復号部１２２と、メッセージ復号部１２３と、セッション鍵記憶部１２４と、メッセージ鍵記憶部１２５を含む。また、図５に示すように、通信端末１３は、再暗号化鍵生成部１３１と、送信部１３２と、セッション鍵記憶部１３３を含む。

[0030] ＜判定＞

以下、図６、図７、図８を参照して、本実施例の通信システム１の各装置の動作について説明する。まず、ユーザＡは通信端末１１を用いて、グループ識別子groupIDによって特定されるグループに、メッセージmを暗号文の形

式で送るものとする。なお、各通信端末（通信端末１１、通信端末１２、通信端末１３）は最新のセッション鍵SK_1を共有しているものとし、これをそれぞれセッション鍵記憶部１１７、セッション鍵記憶部１２４、セッション鍵記憶部１３３に保持しているものとする。このセッション鍵SK_1はサーバ装置１０とは共有されていないため、サーバ装置１０はセッション鍵SK_1を知らない。

[0031] 通信端末１１の判定部１１１は、メッセージm（の暗号文）を送信する際、メッセージm（の暗号文）の送信が、セッション鍵SK_1生成後または更新後の最初の送信であるか否かを判定する（Ｓ１１１）。判定部１１１は、メッセージm（の暗号文）の送信が、セッション鍵SK_1生成後または更新後の最初の送信である場合には、メッセージ鍵を新規生成するものと判定し（判定＝真）、それ以外の場合には、メッセージ鍵を再利用するものと判定する（判定＝偽）。

[0032] ＜判定が真である場合の通信端末１１の動作＞

図６に示すように、通信端末１１のメッセージ鍵生成部１１２は、$Kspace_2$の元K_1（メッセージ鍵）を生成する（Ｓ１１２－１）。

[0033] 通信端末１１のメッセージ暗号化部１１３は、メッセージmと生成されたメッセージ鍵K_1を用い、共通鍵暗号方式に基づいて、メッセージ暗号文$C_{2,m}\leftarrow Enc(K_1,m)$を生成する（Ｓ１１３）。

[0034] また、通信端末１１のメッセージ鍵暗号化部１１４は、セッション鍵SK_1と生成されたメッセージ鍵K_1を用い、再暗号化可能な共通鍵暗号方式に基づいて、メッセージ鍵暗号文$C^{(1)}_{1,K1}\leftarrow KEM.Enc(SK_1,K_1)$を生成する（Ｓ１１４）。

[0035] 通信端末１１の送信部１１５は、自機が属するグループの識別子であるグループ識別子groupIDと、メッセージ鍵暗号文$C^{(1)}_{1,K1}$と、メッセージ暗号文$C_{2,m}$、すなわち、$(groupID,C^{(1)}_{1,K1},C_{2,m})$をサーバ装置１０に送信する（Ｓ１１５－１）。

[0036] なお、$(C^{(1)}_{1,K1},C_{2,m})$は、他のメッセージや他のメッセージ鍵の暗号文との区別をつけるため、便宜上K_1,mを記しているだけであり、暗号文からメッセージ

鍵K_1、メッセージmは推測されない。

[0037] 通信端末１１は、サーバ装置１０にメッセージを送信後、メッセージ鍵K_1をメッセージ鍵記憶部１１６に記憶するが、この時点でメッセージ鍵K_1にはメッセージ鍵識別子$KeyID_1$が割り当てられているものとする。メッセージ鍵識別子$KeyID_1$からメッセージ鍵K_1そのものが識別されないことが望ましい。識別子の生成方法として、SHA256ハッシュ関数等を用いて、メッセージ鍵K_1をSHA256ハッシュ関数に入力した際の出力値を識別子とする方法があるが、特に限定しない。

[0038] また、メッセージ鍵識別子$KeyID_1$は、通信端末１１が生成してもよいし、またはサーバ装置１０がメッセージの受信時に、メッセージ鍵暗号文に対して生成し、メッセージを受信したことを通信端末１１に知らせる際に$KeyID_1$も添付して送信してもよいが、ここでは限定しない。

[0039] 通信端末１１のメッセージ鍵記憶部１１６は、メッセージ鍵K_1とそのメッセージ鍵識別子$KeyID_1$を記憶する（Ｓ１１６）。記憶されたメッセージ鍵K_1は、上記の判定が再利用（判定＝偽）である場合に再利用される。

[0040] ＜判定が偽である場合の通信端末１１の動作＞

この場合、図７に示すように、通信端末１１のメッセージ鍵生成部１１２は、メッセージ鍵記憶部１１６から、メッセージ鍵K_1とそのメッセージ鍵識別子$KeyID_1$を取得する（Ｓ１１２－２）。このメッセージ鍵K_1は少なくとも1つ前のメッセージ送信の際にメッセージmの暗号化に使われたメッセージ鍵である。

[0041] 通信端末１１のメッセージ暗号化部１１３は、メッセージmとメッセージ鍵記憶部１１６に記憶されたメッセージ鍵K_1を用い、共通鍵暗号方式に基づいて、メッセージ暗号文$C_{2,m} \leftarrow Enc(K_1, m)$を生成する（Ｓ１１３）。

[0042] 通信端末１１の送信部１１５は、グループ識別子groupIDと、メッセージ鍵識別子$KeyID_1$と、メッセージ暗号文$C_{2,m}$、すなわち、$(groupID, KeyID_1, C_{2,m})$をサーバ装置１０に送信する（Ｓ１１５－２）。

[0043] 以下、サーバ装置１０が通信端末１１からメッセージ暗号文$C_{2,m}$を受信した

ときの動作について説明する。なお、メッセージ受信をトリガーにして他の通信端末への配信動作を記述しているが、ユーザの追加やログイン、その他通信端末からの要求に応じて、サーバ装置１０は記憶された暗号化メッセージを当該通信端末に配信することもある。

[0044] ＜判定が真である場合のサーバ装置１０の動作＞

すなわち、通信端末１１から送信されたメッセージの形式が(groupID,$C^{(1)}_{1,K_1}$,$C_{2,m}$)である場合に該当する。図６に示すように、サーバ装置１０の受信部１０１は、通信端末１１から、(groupID,$C^{(1)}_{1,K1}$,$C_{2,m}$)を受信する（Ｓ１０１－１）。

[0045] サーバ装置１０のメッセージ暗号文記憶部１０２は、メッセージ鍵識別子KeyID$_1$と、メッセージ暗号文$C_{2,m}$、すなわち(KeyID$_1$,$C_{2,m}$)を記憶する（Ｓ１０２）。

[0046] また、サーバ装置１０のメッセージ鍵暗号文記憶部１０３は、メッセージ鍵識別子KeyID$_1$と、メッセージ鍵暗号文$C^{(1)}_{1,K1}$、すなわち(KeyID$_1$,$C^{(1)}_{1,K1}$)を記憶する（Ｓ１０３－１）。なお、サーバ装置１０は(groupID,$C^{(1)}_{1,K1}$,$C_{2,m}$)の形式でデータを受信するたびに上記動作（Ｓ１０１－１、Ｓ１０２、Ｓ１０３－１）を実行するものとする。

[0047] サーバ装置１０は、グループユーザ記憶部１０４に記憶されている、groupIDに対応するグループに所属するユーザ（ユーザＢ，Ｃを含む）情報を参照する（Ｓ１０４）。サーバ装置１０の配信部１０５は、groupIDに対応するグループに所属する各ユーザに向けてメッセージ鍵暗号文$C^{(1)}_{1,K1}$と、メッセージ暗号文$C_{2,m}$、すなわち、（$C^{(1)}_{1,K1}$,$C_{2,m}$）を送信（配信）する（Ｓ１０５）。なお、本実施例では、サーバ装置１０は、通信端末１２に（$C^{(1)}_{1,K1}$,$C_{2,m}$）を送信（配信）する。

[0048] ＜判定が偽である場合のサーバ装置１０の動作＞

すなわち、通信端末１１から送信されたメッセージの形式が(groupID,KeyID$_1$,$C_{2,m}$)である場合に該当する。図７に示すように、サーバ装置１０の受信部１０１は、通信端末１１から、(groupID,KeyID$_1$,$C_{2,m}$)を受信する（Ｓ１０１－

２）。

[0049] サーバ装置１０のメッセージ暗号文記憶部１０２は、メッセージ鍵識別子KeyID$_1$と、メッセージ暗号文$C_{2,m}$、すなわち(KeyID$_1$,$C_{2,m}$)を記憶する（Ｓ１０２）。なお、サーバ装置１０は(groupID,KeyID$_1$,$C_{2,m}$)の形式でデータを受信するたびに上記動作（Ｓ１０１－２、Ｓ１０２）を実行するものとする。

[0050] サーバ装置１０のメッセージ鍵暗号文記憶部１０３は、KeyID$_1$に紐付くメッセージ鍵暗号文$C^{(1)}_{1,K1}$を取得する（Ｓ１０３－２）。

[0051] サーバ装置１０は、グループユーザ記憶部１０４に記憶されている、groupIDに対応するグループに所属するユーザ（ユーザＢ，Ｃを含む）情報を参照する（Ｓ１０４）。サーバ装置１０の配信部１０５は、groupIDに対応するグループに所属する各ユーザに向けてメッセージ鍵暗号文$C^{(1)}_{1,K1}$と、メッセージ暗号文$C_{2,m}$、すなわち、（$C^{(1)}_{1,K1}$,$C_{2,m}$）を送信（配信）する（Ｓ１０５）。なお、本実施例では、サーバ装置１０は、通信端末１２に（$C^{(1)}_{1,K1}$,$C_{2,m}$）を送信（配信）する。

[0052] ＜通信端末１２の動作＞

以下、図６（図７）を参照して通信端末１２の動作を説明する。前述したように、セッション鍵記憶部１２４は、他の通信端末と共有され、サーバ装置と共有されない最新のセッション鍵SK_1を記憶している。

[0053] 通信端末１２の受信部１２１は、メッセージ鍵暗号文$C^{(1)}_{1,K1}$と、メッセージ暗号文$C_{2,m}$、すなわち、（$C^{(1)}_{1,K1}$,$C_{2,m}$）をサーバ装置１０から受信する（Ｓ１２１）。

[0054] 通信端末１２のメッセージ鍵復号部１２２は、セッション鍵記憶部１２４から取り出した最新のセッション鍵SK_1とメッセージ鍵暗号文$C^{(1)}_{1,K1}$から、K_1←KEM.Dec(SK_1,$C^{(1)}_{1,K1}$)を計算して、メッセージ鍵K_1を復号する（Ｓ１２２）。

[0055] 通信端末１２のメッセージ復号部１２３は、共通鍵暗号方式に基づいて、復号したメッセージ鍵K_1と、メッセージ暗号文$C_{2,m}$からm←Dec(K_1,$C_{2,m}$)を計算して、メッセージmを復号する（Ｓ１２３）。これによって、通信端末１２は通信端末１１から送信されたメッセージmを正しく表示できる。

[0056] ＜通信端末１３の動作＞

以下、図８を参照して通信端末１３の動作を説明する。例えば、groupIDに対応するグループにおいてセッション鍵がSK_1からSK_2に更新されたものとする。このとき、通信端末１１、通信端末１２、通信端末１３は最新のセッション鍵SK_2を共有しており、最新のセッション鍵SK_2を、それぞれセッション鍵記憶部１１７、セッション鍵記憶部１２４、セッション鍵記憶部１３３に記憶している（図８、新しいセッション鍵の共有）。また、通信端末１３のセッション鍵記憶部１３３は、更新前のセッション鍵SK_1も保持しているものとする。

[0057] なお、セッション鍵SK_1, SK_2はサーバ装置１０とは共有されていないため、サーバ装置１０は、セッション鍵SK_1, SK_2を知らない。

[0058] また、サーバ装置１０は、メッセージ鍵暗号文記憶部１０３において、groupIDに付随する暗号文、すなわち、グループ識別子groupID向けに送信された暗号文、$C^{(1)}_{1,Ki1},\ldots,C^{(1)}_{1,Kin}$を保持しているものとする。なお、$i_1,\ldots,i_n$は本実施例を記述する上で用いた、メッセージ鍵を区別する添え字である。

[0059] 同図に示すように、通信端末１３の再暗号化鍵生成部１３１は、更新前のセッション鍵SK_1と更新後のセッション鍵SK_2から、$RK_{1,2} \leftarrow KEM.ReKeyGen(SK_1, SK_2)$を計算して、再暗号化鍵$RK_{1,2}$を生成する（Ｓ１３１）。

[0060] 通信端末１３の送信部１３２は、グループ識別子groupIDと、再暗号化鍵$RK_{1,2}$の組、すなわち$(groupID, RK_{1,2})$をサーバ装置１０に送信する（Ｓ１３２）。

[0061] ＜サーバ装置１０の再暗号化動作＞

引き続き、図８を参照してサーバ装置１０の再暗号化動作について説明する。サーバ装置１０の受信部１０１は、通信端末１３からグループ識別子groupIDと再暗号化鍵$RK_{1,2}$の組$(groupID, RK_{1,2})$を受信する（Ｓ１０１－３）。

[0062] サーバ装置１０の再暗号化処理部１０６と、メッセージ鍵暗号文記憶部１０３は、各$j \in \{i_1,\ldots,i_n\}$に対して、以下の処理を繰り返し実行する。

・メッセージ鍵暗号文記憶部１０３は、メッセージ鍵暗号文$C^{(1)}_{1,Kj}$を取り出す。再暗号化処理部１０６は、再暗号化可能な共通鍵暗号方式に基づいて、再

暗号化鍵$RK_{1,2}$と、グループ識別子groupIDに対応するメッセージ鍵暗号文$C^{(1)}_{1,Kj}$から、$C^{(2)}_{1,Kj} \leftarrow KEM.ReEnc(RK_{1,2}, C^{(1)}_{1,Kj})$を実行して、再暗号化後のメッセージ鍵暗号文$C^{(2)}_{1,Kj}$を生成する（Ｓ１０６）。

・メッセージ鍵暗号文記憶部１０３は、メッセージ鍵暗号文$C^{(1)}_{1,Kj}$に対して再暗号化後のメッセージ鍵暗号文$C^{(2)}_{1,Kj}$を上書き記憶する（Ｓ１０３－３）。

[0063] なお、この処理の後も、各メッセージ鍵識別子には変更はない。そのため、メッセージ暗号文記憶部１０２にあるメッセージ暗号文とメッセージ鍵暗号文記憶部１０３にあるメッセージ鍵暗号文の対応関係に変化はない。

[0064] 上記処理後、サーバ装置１０から配信されたgroupIDに付随する暗号文を受信した通信端末は、最新のセッション鍵SK_2を保持していれば、メッセージ受信時と同じ動作によって、各メッセージを正しく復号することができる。

[0065] ＜メッセージの複数受信＞

ログイン時やグループ追加時等で、１０メッセージや２０メッセージといった、複数のメッセージを１度に受信することがある。その時の動作について説明する。ここでは、通信端末１２がログイン時に所定のグループに入室し、最新の５メッセージをダウンロードするものとして説明する。サーバ装置１０は、メッセージ暗号文記憶部１０２から、当該グループで送信された最新の５メッセージを抽出する。

[0066] これらは、新しいものから順に、$(KeyID_1, C_{2,m1})$、$(KeyID_1, C_{2,m2})$、$(KeyID_2, C_{2,m3})$、$(KeyID_1, C_{2,m4})$、$(KeyID_3, C_{2,m5})$であるとする。抽出したメッセージに含まれる、メッセージ鍵識別子は$KeyID_1$、$KeyID_2$、$KeyID_3$の３種類であるから、サーバ装置１０は、メッセージ鍵暗号文記憶部１０３から、メッセージ鍵識別子とメッセージ鍵暗号文の組$(KeyID_1, C_{1,K1})$、$(KeyID_2, C_{1,K2})$、$(KeyID_3, C_{1,K3})$を抽出する。

[0067] サーバ装置１０は、通信端末１２に、メッセージ鍵識別子とメッセージ鍵暗号文の組$(KeyID_1, C_{1,K1})$、$(KeyID_2, C_{1,K2})$、$(KeyID_3, C_{1,K3})$とメッセージ鍵識別子とメッセージ暗号文の組$(KeyID_1, C_{2,m1})$、$(KeyID_1, C_{2,m2})$、$(KeyID_2, C_{2,m3})$、$(KeyID_1, C_{2,m4})$、$(KeyID_3, C_{2,m5})$を送信する。

[0068] メッセージ鍵識別子とメッセージ鍵暗号文の組$(KeyID_1, C_{1,K1})$、$(KeyID_2, C_{1,K2})$、$(KeyID_3, C_{1,K3})$とメッセージ鍵識別子とメッセージ暗号文の組$(KeyID_1, C_{2,m1})$、$(KeyID_1, C_{2,m2})$、$(KeyID_2, C_{2,m3})$、$(KeyID_1, C_{2,m4})$、$(KeyID_3, C_{2,m5})$を受信した通信端末１２は、セッション鍵記憶部１２４から、最新のセッション鍵SK_1を取り出す。

[0069] 通信端末１２のメッセージ鍵復号部１２２は、$K_1 \leftarrow KEM.Dec(SK_1, C_{1,K1})$、$K_2 \leftarrow KEM.Dec(SK_1, C_{1,K2})$、$K_3 \leftarrow KEM.Dec(SK_1, C_{1,K3})$をそれぞれ計算して、メッセージ鍵$K_1, K_2, K_3$を復号し、メッセージ鍵記憶部１２５に、メッセージ鍵識別子とメッセージ鍵の組$(KeyID_1, K_1)$、$(KeyID_2, K_2)$、$(KeyID_3, K_3)$をそれぞれ一時的に保存しておく。

[0070] 次にメッセージ復号を行う。メッセージ暗号文は、メッセージ鍵識別子との組み合わせで取得しているので、対応するメッセージ鍵を抽出して復号処理を行う。すなわち、メッセージ復号部１２３で$m_1 \leftarrow Dec(K_1, C_{2,m1})$、$m_2 \leftarrow Dec(K_1, C_{2,m2})$、$m_3 \leftarrow Dec(K_2, C_{2,m3})$、$m_4 \leftarrow Dec(K_1, C_{2,m4})$、$m_5 \leftarrow Dec(K_3, C_{2,m5})$を計算して、各メッセージを復号する。これによって、各メッセージ毎にメッセージ鍵暗号文を復号する処理を軽減することができ、また、各メッセージを正しく表示できる。なお、全メッセージ取得後、メッセージ鍵記憶部１２５に保存されたメッセージ鍵識別子とメッセージ鍵の組はすべて削除しておくのが安全性上望ましい。

[0071] ＜補記＞

本発明の装置は、例えば単一のハードウェアエンティティとして、キーボードなどが接続可能な入力部、液晶ディスプレイなどが接続可能な出力部、ハードウェアエンティティの外部に通信可能な通信装置（例えば通信ケーブル）が接続可能な通信部、ＣＰＵ（Central Processing Unit、キャッシュメモリやレジスタなどを備えていてもよい）、メモリであるＲＡＭやＲＯＭ、ハードディスクである外部記憶装置並びにこれらの入力部、出力部、通信部、ＣＰＵ、ＲＡＭ、ＲＯＭ、外部記憶装置の間のデータのやり取りが可能なように接続するバスを有している。また必要に応じて、ハードウェアエンテ

ィティに、ＣＤ－ＲＯＭなどの記録媒体を読み書きできる装置（ドライブ）などを設けることとしてもよい。このようなハードウェア資源を備えた物理的実体としては、汎用コンピュータなどがある。

[0072] ハードウェアエンティティの外部記憶装置には、上述の機能を実現するために必要となるプログラムおよびこのプログラムの処理において必要となるデータなどが記憶されている（外部記憶装置に限らず、例えばプログラムを読み出し専用記憶装置であるＲＯＭに記憶させておくこととしてもよい）。また、これらのプログラムの処理によって得られるデータなどは、ＲＡＭや外部記憶装置などに適宜に記憶される。

[0073] ハードウェアエンティティでは、外部記憶装置（あるいはＲＯＭなど）に記憶された各プログラムとこの各プログラムの処理に必要なデータが必要に応じてメモリに読み込まれて、適宜にＣＰＵで解釈実行・処理される。その結果、ＣＰＵが所定の機能（上記、…部、…手段などと表した各構成要件）を実現する。

[0074] 本発明は上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。また、上記実施形態において説明した処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されるとしてもよい。

[0075] 既述のように、上記実施形態において説明したハードウェアエンティティ（本発明の装置）における処理機能をコンピュータによって実現する場合、ハードウェアエンティティが有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記ハードウェアエンティティにおける処理機能がコンピュータ上で実現される。

[0076] この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体

メモリ等どのようなものでもよい。具体的には、例えば、磁気記録装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等を、光磁気記録媒体として、ＭＯ（Magneto-Optical disc）等を、半導体メモリとしてＥＥＰ－ＲＯＭ（Electronically Erasable and Programmable-Read Only Memory）等を用いることができる。

[0077] また、このプログラムの流通は、例えば、そのプログラムを記録したＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

[0078] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるＡＳＰ（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるも

の（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

[0079] また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、ハードウェアエンティティを構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

請求の範囲

[請求項1] サーバ装置を介して他の通信端末に暗号文を送信する通信端末であって、

前記他の通信端末と共有され、前記サーバ装置と共有されないセッション鍵を記憶するセッション鍵記憶部と、

前記暗号文の送信が前記セッション鍵の生成後または更新後の最初の送信である場合にメッセージの暗号化に用いるメッセージ鍵を新規生成するものと判定し、それ以外の場合に前記メッセージ鍵を再利用するものと判定する判定部と、

前記判定の結果が新規生成である場合に前記メッセージ鍵を生成するメッセージ鍵生成部と、

前記判定の結果が再利用である場合に再利用されるメッセージ鍵をメッセージ鍵識別子と関連付けて記憶するメッセージ鍵記憶部と、

前記メッセージと生成または記憶された前記メッセージ鍵を用い、共通鍵暗号方式に基づいて、メッセージ暗号文を生成するメッセージ暗号化部と、

前記判定の結果が新規生成である場合に、前記セッション鍵と生成された前記メッセージ鍵を用い、再暗号化可能な共通鍵暗号方式に基づいて、メッセージ鍵暗号文を生成するメッセージ鍵暗号化部と、

前記判定の結果が新規生成である場合に、自機が属するグループの識別子であるグループ識別子と、前記メッセージ鍵暗号文と、前記メッセージ暗号文を、前記サーバ装置に送信し、前記判定の結果が再利用である場合に、前記グループ識別子と、前記メッセージ鍵識別子と、前記メッセージ暗号文を前記サーバ装置に送信する暗号文送信部と、

を含む通信端末。

[請求項2] サーバ装置を介して他の通信端末が送信した暗号文を受信する通信端末であって、

前記他の通信端末と共有され、前記サーバ装置と共有されないセッション鍵を記憶するセッション鍵記憶部と、

前記セッション鍵と前記他の通信端末が生成したメッセージ鍵を用い、再暗号化可能な共通鍵暗号方式に基づいて生成されたメッセージ鍵暗号文と、前記他の通信端末が生成したメッセージと前記他の通信端末が生成または記憶する前記メッセージ鍵を用い、共通鍵暗号方式に基づいて生成されたメッセージ暗号文を、前記サーバ装置から受信する受信部と、

再暗号化可能な共通鍵暗号方式に基づいて前記セッション鍵と前記メッセージ鍵暗号文から前記メッセージ鍵を復号するメッセージ鍵復号部と、

共通鍵暗号方式に基づいて前記メッセージ鍵と前記メッセージ暗号文から前記メッセージを復号するメッセージ復号部と、

を含む通信端末。

[請求項3] 他の通信端末と共有され、サーバ装置と共有されないセッション鍵が更新されるたびに再暗号化鍵を前記サーバ装置に送信する通信端末であって、

前記セッション鍵を記憶するセッション鍵記憶部と、

更新前の前記セッション鍵と更新後の前記セッション鍵から前記再暗号化鍵を生成する再暗号化鍵生成部と、

前記再暗号化鍵を前記サーバ装置に送信する送信部と、

を含む通信端末。

[請求項4] サーバ装置を介して他の通信端末に暗号文を送信し、前記サーバ装置を介して前記他の通信端末が送信した前記暗号文を受信し、前記他の通信端末と共有され、前記サーバ装置と共有されないセッション鍵が更新されるたびに再暗号化鍵を前記サーバ装置に送信する通信端末であって、

前記セッション鍵を記憶するセッション鍵記憶部と、

前記暗号文の送信が前記セッション鍵の生成後または更新後の最初の送信である場合にメッセージの暗号化に用いるメッセージ鍵を新規生成するものと判定し、それ以外の場合に前記メッセージ鍵を再利用するものと判定する判定部と、

前記判定の結果が新規生成である場合に前記メッセージ鍵を生成するメッセージ鍵生成部と、

前記判定の結果が再利用である場合に再利用されるメッセージ鍵をメッセージ鍵識別子と関連付けて記憶するメッセージ鍵記憶部と、

前記メッセージと生成または記憶された前記メッセージ鍵を用い、共通鍵暗号方式に基づいて、メッセージ暗号文を生成するメッセージ暗号化部と、

前記判定の結果が新規生成である場合に、前記セッション鍵と生成された前記メッセージ鍵を用い、再暗号化可能な共通鍵暗号方式に基づいて、メッセージ鍵暗号文を生成するメッセージ鍵暗号化部と、

前記判定の結果が新規生成である場合に、自機が属するグループの識別子であるグループ識別子と、前記メッセージ鍵暗号文と、前記メッセージ暗号文を、前記サーバ装置に送信し、前記判定の結果が再利用である場合に、前記グループ識別子と、前記メッセージ鍵識別子と、前記メッセージ暗号文を前記サーバ装置に送信する暗号文送信部と、

前記メッセージ鍵暗号文と前記メッセージ暗号文を前記サーバ装置から受信する受信部と、

再暗号化可能な共通鍵暗号方式に基づいて前記セッション鍵と前記メッセージ鍵暗号文から前記メッセージ鍵を復号するメッセージ鍵復号部と、

共通鍵暗号方式に基づいて前記メッセージ鍵と前記メッセージ暗号文から前記メッセージを復号するメッセージ復号部と、

更新前の前記セッション鍵と更新後の前記セッション鍵から前記再

暗号化鍵を生成する再暗号化鍵生成部と、

前記再暗号化鍵を前記サーバ装置に送信する送信部と、

を含む通信端末。

[請求項5] 複数の通信端末間で共有され、自機と共有されないセッション鍵が更新されるたびに、対応するメッセージ鍵暗号文を再暗号化するサーバ装置であって、

前記通信端末から、前記通信端末が属するグループの識別子であるグループ識別子と、更新前の前記セッション鍵と更新後の前記セッション鍵から生成された再暗号化鍵を受信する受信部と、

再暗号化可能な共通鍵暗号方式に基づいて、前記再暗号化鍵と、前記グループ識別子に対応する前記メッセージ鍵暗号文から再暗号化後の前記メッセージ鍵暗号文を生成する再暗号化処理部と、

を含むサーバ装置。

[請求項6] コンピュータを請求項１から４の何れかに記載の通信端末として機能させるプログラム。

[請求項7] コンピュータを請求項５に記載のサーバ装置として機能させるプログラム。

[図1]

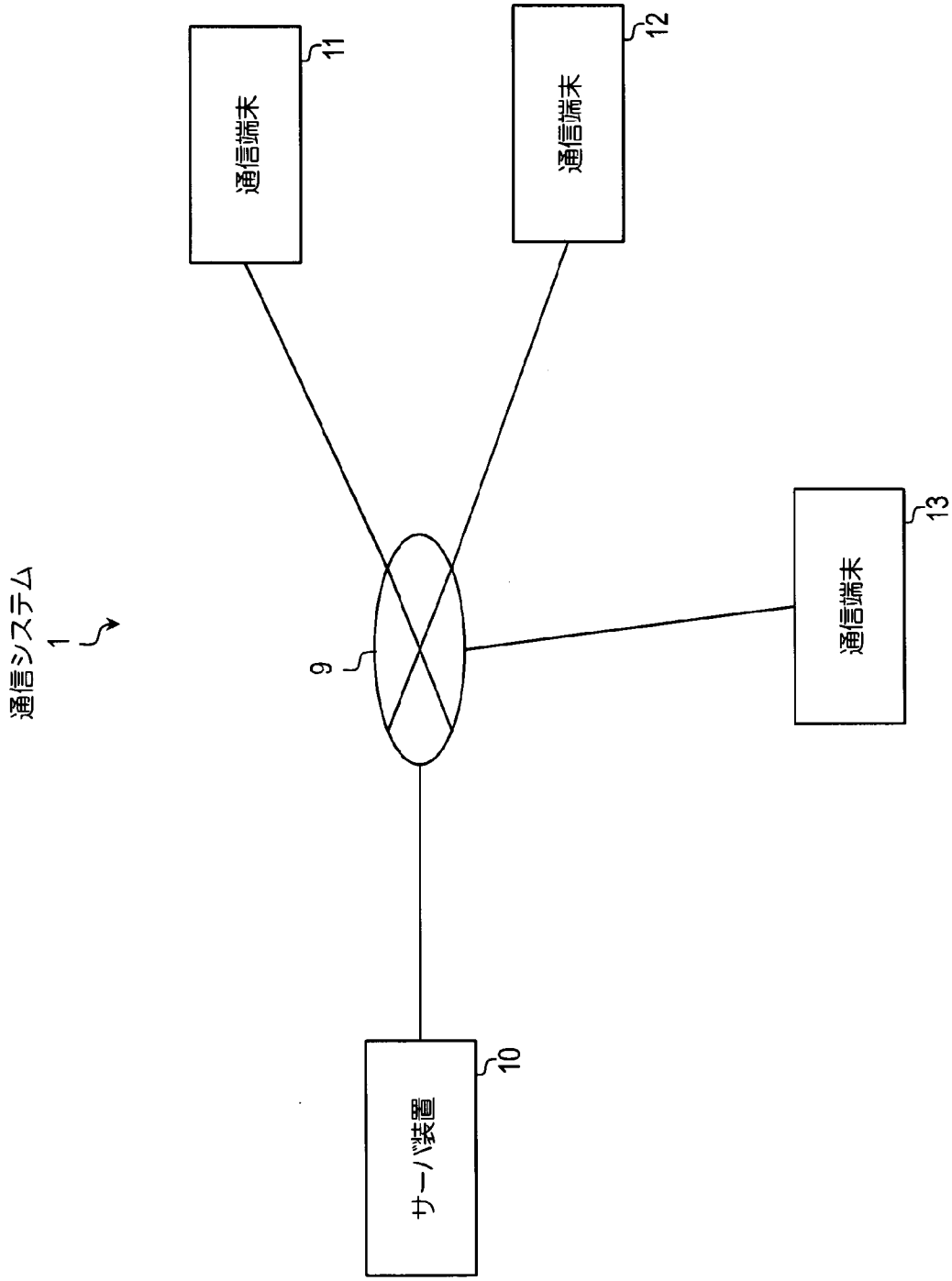
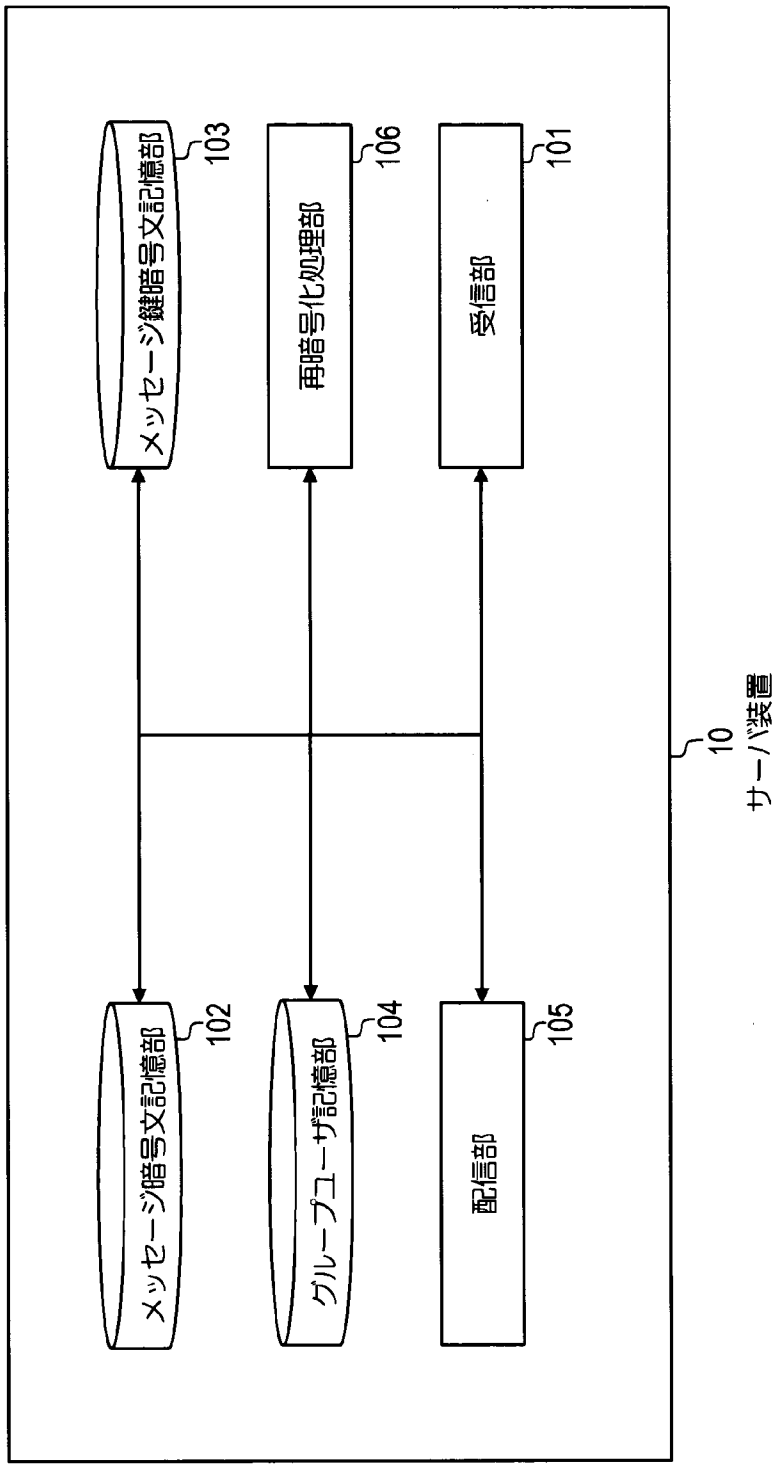


図1

[図2]

図2


メッセージ鍵暗号文記憶部
103
再暗号化処理部
106
受信部
101
メッセージ暗号文記憶部
102
グループユーザ記憶部
104
配信部
105
10
サーバ装置

[図3]

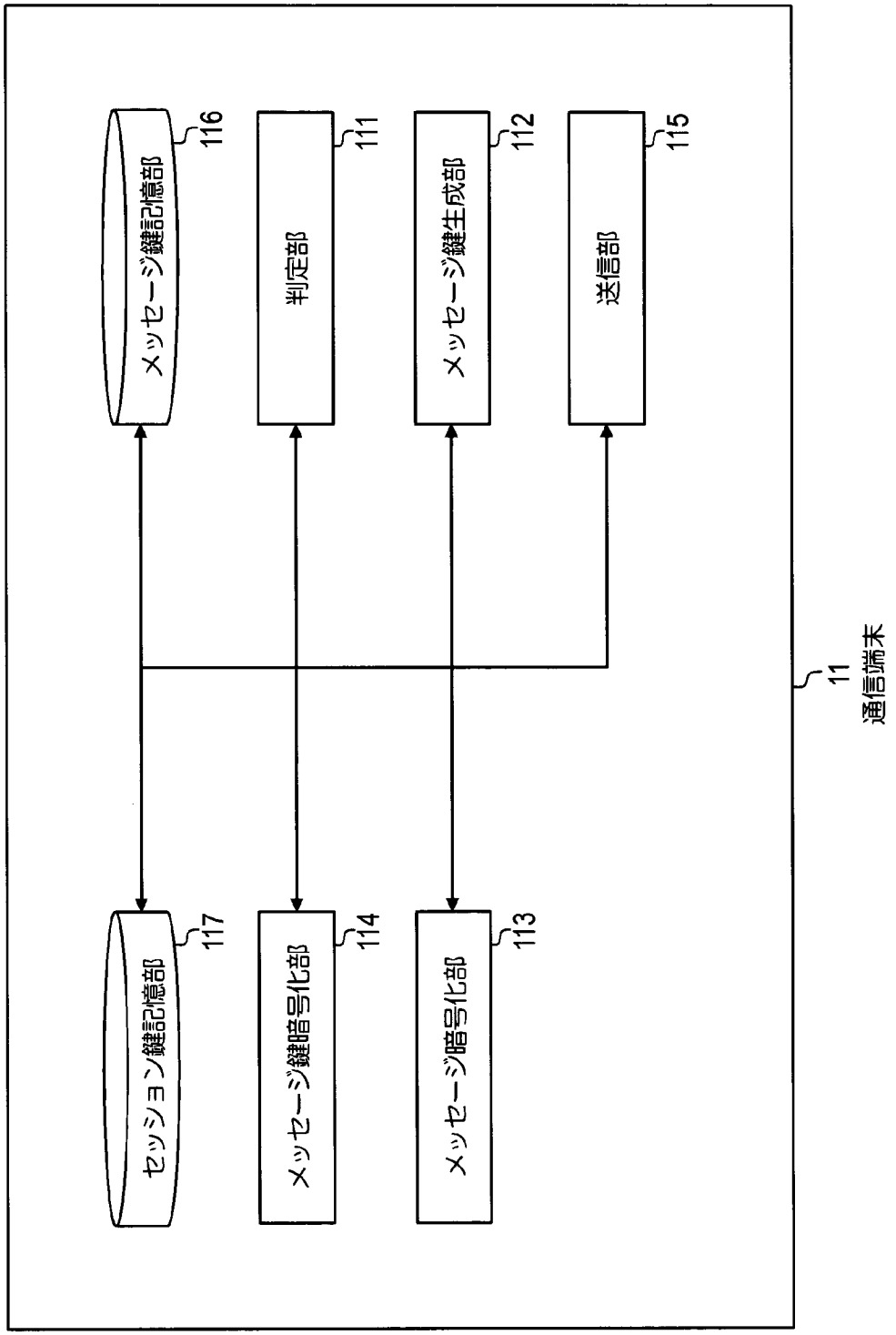
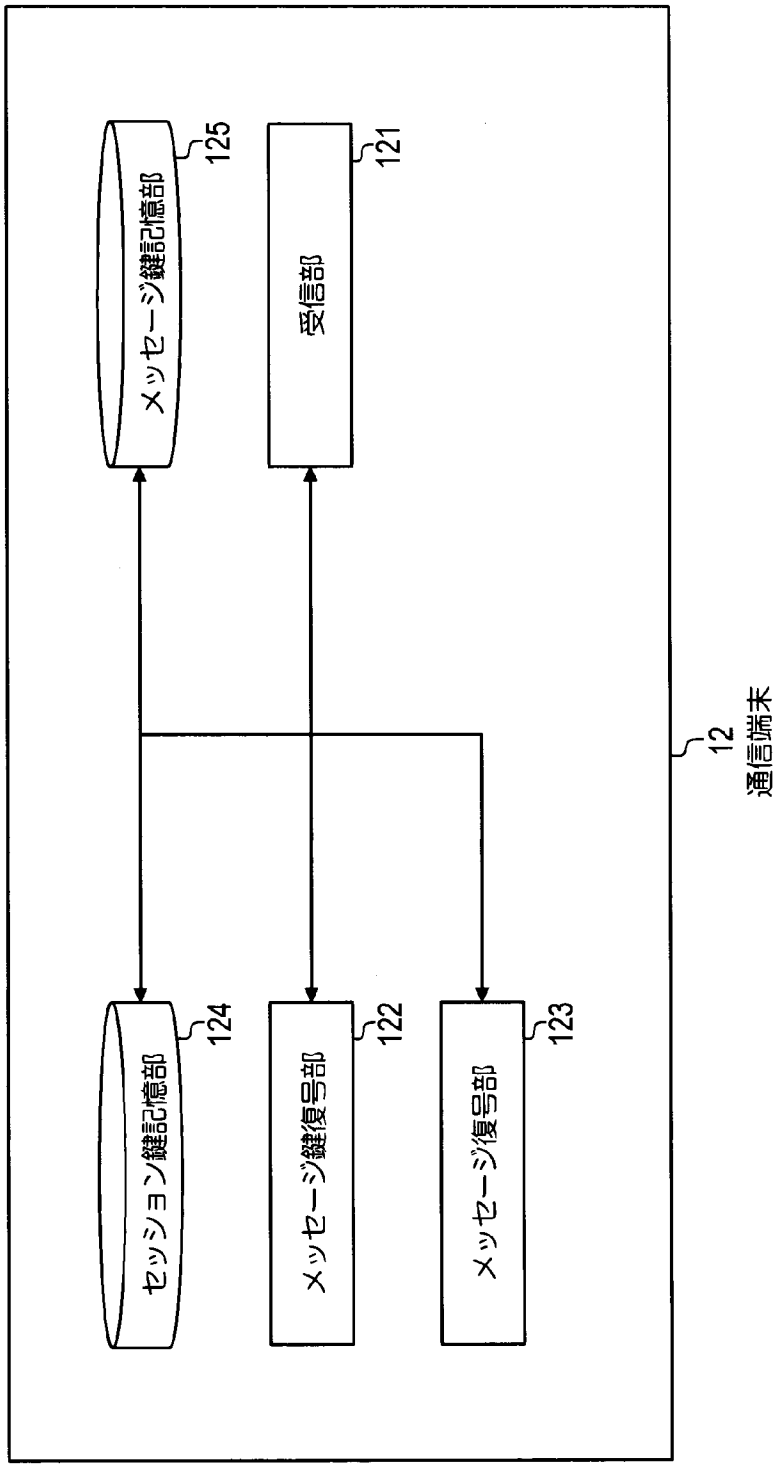

メッセージ鍵記憶部
116
判定部
111
メッセージ鍵生成部
112
送信部
115
セッション鍵記憶部
117
メッセージ鍵暗号化部
114
メッセージ暗号化部
113
11
通信端末

図3

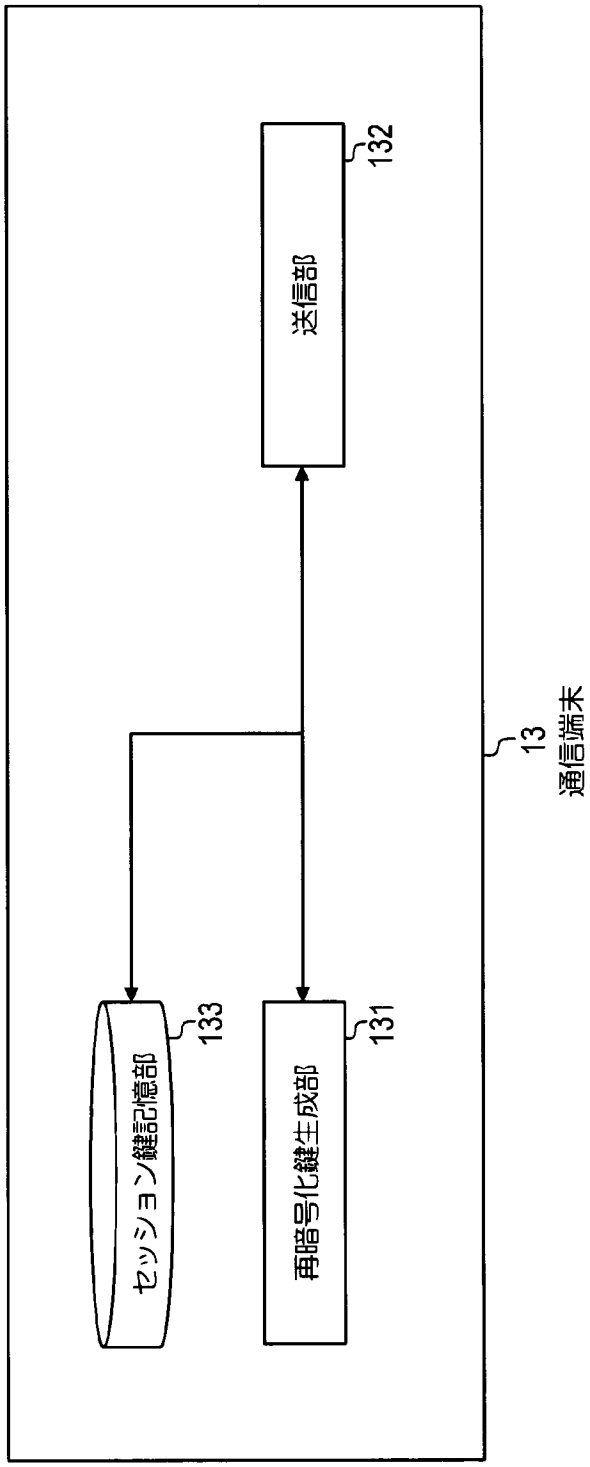
[図4]

図4


12
通信端末
125
メッセージ鍵記憶部
121
受信部
124
セッション鍵記憶部
122
メッセージ鍵復号部
123
メッセージ復号部

[図5]

図5



[図6]

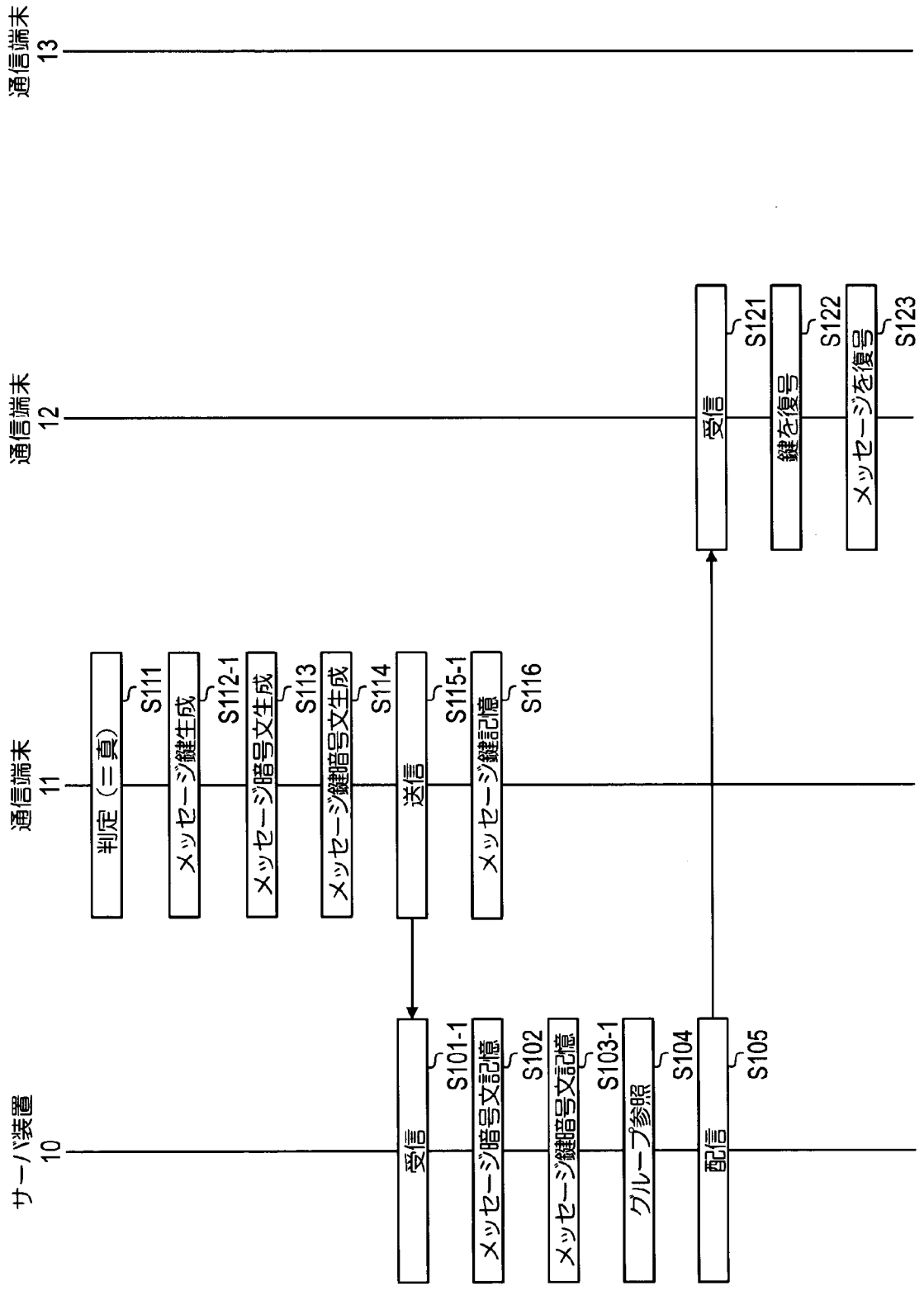

通信端末 13
通信端末 12
通信端末 11
サーバ装置 10
判定（＝真）
S111
メッセージ鍵生成
S112-1
メッセージ暗号文生成
S113
メッセージ鍵暗号文生成
S114
送信
S115-1
メッセージ鍵記憶
S116
受信
S101-1
メッセージ暗号文記憶
S102
メッセージ鍵暗号文記憶
S103-1
グループ参照
S104
配信
S105
受信
S121
鍵を復号
S122
メッセージを復号
S123

図6

[図7]

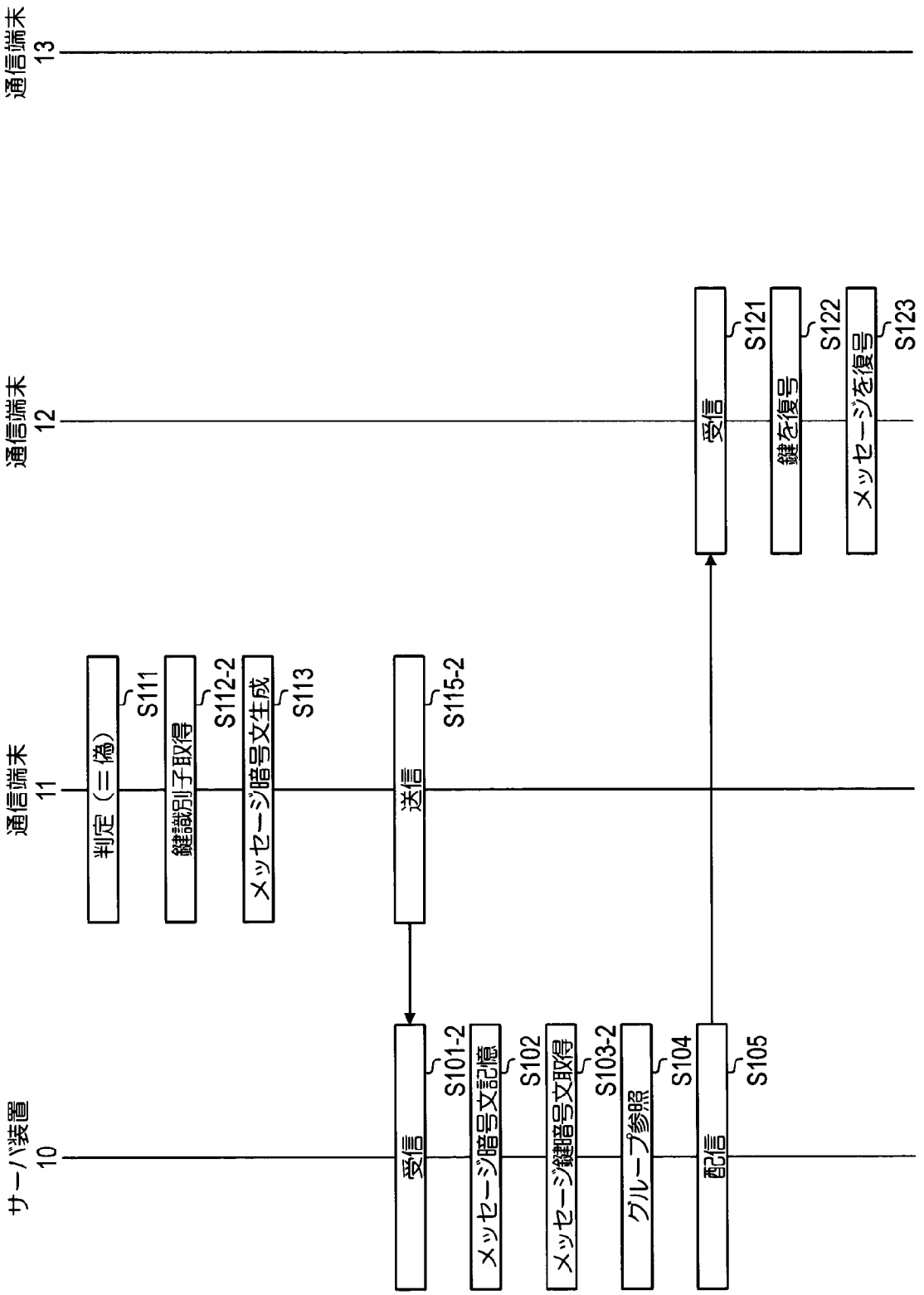

通信端末
13
通信端末
12
通信端末
11
サーバ装置
10
判定（二倍）
S111
鍵識別子取得
S112-2
メッセージ暗号文生成
S113
送信
S115-2
受信
S121
鍵を復号
S122
メッセージを復号
S123
受信
S101-2
メッセージ暗号文記憶
S102
メッセージ鍵暗号文取得
S103-2
グループ参照
S104
配信
S105

図7

[図8]

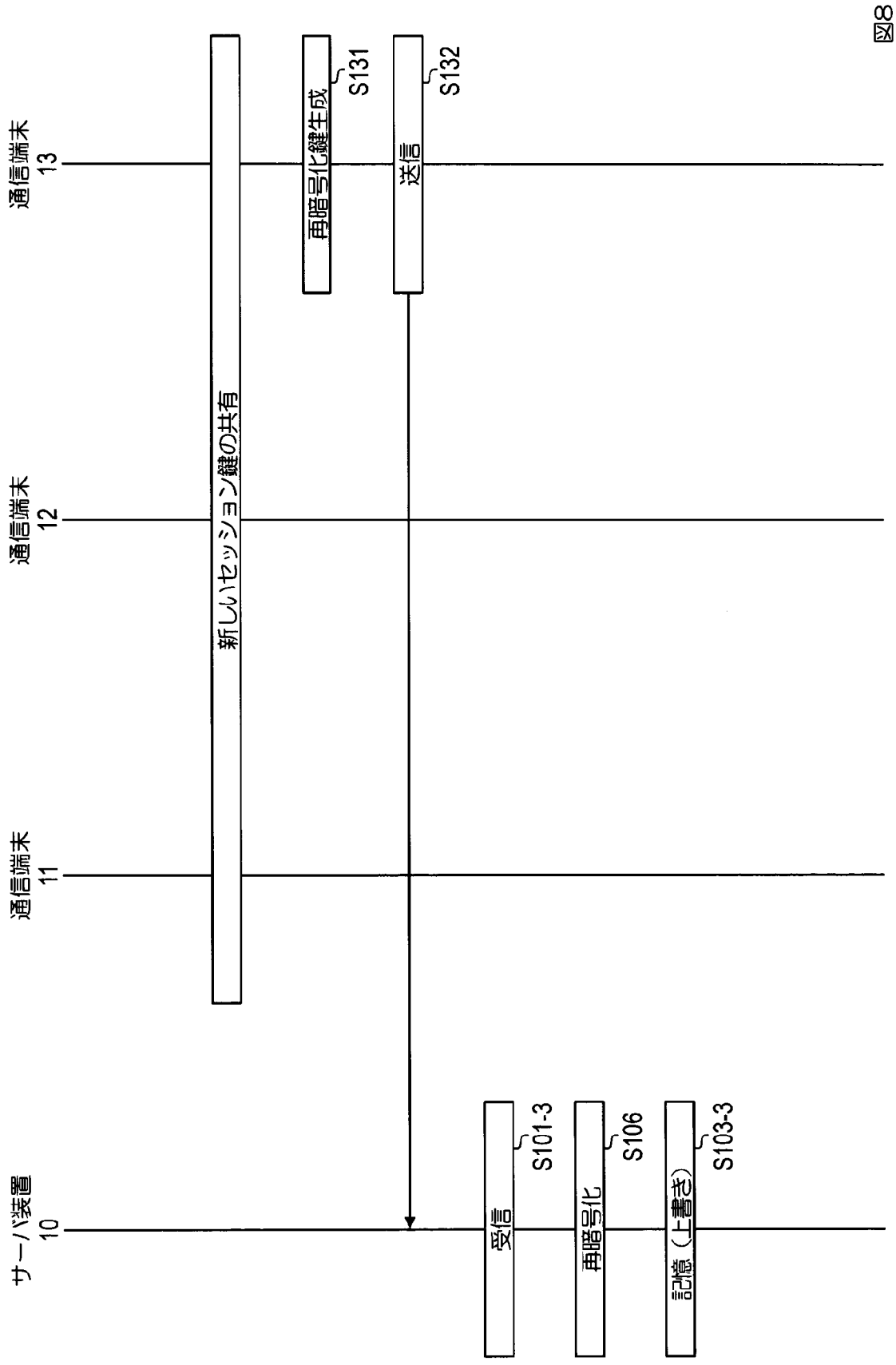


図8
通信端末 13
通信端末 12
通信端末 11
サーバ装置 10
新しいセッション鍵の共有
再暗号化鍵生成
S131
送信
S132
受信
S101-3
再暗号化
S106
記憶（上書き）
S103-3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/040472

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/08(2006.01)i, H04L9/16(2006.01)i, H04L12/58(2006.01)i, H04L12/66(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)
Int.Cl. H04L9/08, H04L9/16, H04L12/58, H04L12/66

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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.
X A	岡野裕樹，他，セキュアビジネスチャットにおける代理人再暗号化付き検索可能暗号，2017年暗号と情報セキュリティシンポジウム(SCIS2017)，24 January 2017, 3F3-4, pp. 1-8 in particular, "2. Overview of each encryption method used in business chat system", non-official translation (OKANO, Yuki et al., "Searchable code with proxy re-encryption in secure business chat", The 2017 Symposium on Cryptography and Information Security(SCIS2017))	2-3, 5-7 1, 4
A	JP 2017-5587 A (KONICA MINOLTA, INC.) 05 January 2017 & US 2016/0365976 A1	1-7

☐ 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 21 January 2019 (21.01.2019)	Date of mailing of the international search report 29 January 2019 (29.01.2019)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０４０４７２

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, H04L9/16(2006.01)i, H04L12/58(2006.01)i, H04L12/66(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, H04L9/16, H04L12/58, H04L12/66

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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
X	岡野 裕樹, 他, セキュアビジネスチャットにおける代理人再暗号化付き検索可能暗号, 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), 2017.01.24, 3F3-4, pp. 1-8 特に、2 ビジネスチャットシステムに用いた各暗号方式の概要	2-3, 5-7
A		1, 4
A	JP 2017-5587 A (コニカミノルタ株式会社) 2017.01.05, & US 2016/0365976 A1	1-7

☐　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	国際調査報告の発送日
２１．０１．２０１９	２９．０１．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｓ　４５３８
金沢　史明
電話番号　０３－３５８１－１１０１　内線　３５４６