

(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
2015年7月16日(16.07.2015)



(10) 国際公開番号

WO 2015/104629 A1

- (51) 国際特許分類:
H04L 9/16 (2006.01) H04L 9/08 (2006.01)
- (21) 国際出願番号: PCT/IB2015/000006
- (22) 国際出願日: 2015年1月5日(05.01.2015)
- (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 2014-003550 2014年1月10日(10.01.2014) JP
- (71) 出願人: パナソニックIPマネジメント株式会社 (PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.) [JP/JP]; 〒5406207 大阪府大阪市中央区城見2丁目1番61号 Osaka (JP).
- (72) 発明者: 安健司(YASU, Kenji); 〒5718501 大阪府門真市大字門真1006番地 パナソニック株式会社内 Osaka (JP). 福田尚弘(FUKUDA, Naohiro); 〒5718501 大阪府門真市大字門真1006番地 パナソニック株式会社内 Osaka (JP). 蔵前健治(KURAMAE, Kenji); 〒5718501 大阪府門真市大字門真1006番地 パナソニック株式会社内 Osaka (JP). 増田洋一(MASUDA, Yoichi); 〒5718501 大阪府門真市大字門真1006番地 パナソニック株式会社内 Osaka (JP). 高添

智樹(TAKAZOE, Tomoki); 〒5718501 大阪府門真市大字門真1006番地 パナソニック株式会社内 Osaka (JP).

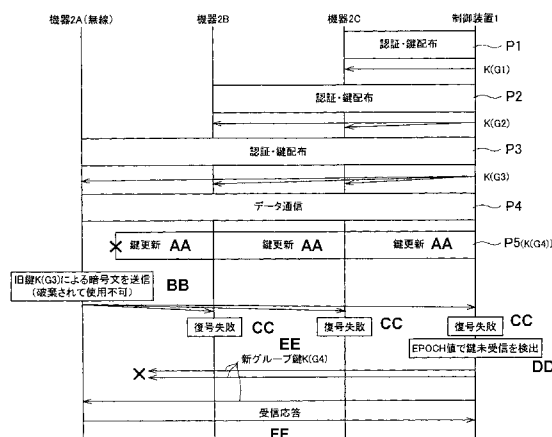
- (74) 代理人: 第一特許法人(FIRSTLAW P.C.); 〒137739 ソウル特別市瑞草区マバン路60 Seoul (KR).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, 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).

[続葉有]

(54) Title: KEY INFORMATION CONTROL DEVICE, KEY INFORMATION UPDATING DEVICE, PROGRAM AND RECORDING MEDIUM, KEY INFORMATION UPDATING METHOD, AND KEY INFORMATION UPDATING SYSTEM

(54) 発明の名称: 鍵情報制御装置、鍵情報更新装置、プログラム及び記録媒体、鍵情報更新方法、鍵情報更新システム

図7



1... Control device
2A...Device (wireless)
2B, 2C...Device
P1, P2, P3... Authentication/key distribution
P4...Data communication
AA...Key update

BB...Transmission of text encrypted using old key (K(G3)) (expired and unusable)
CC...Decryption failure
DD...Detect non-receipt of key using EPOCH value
EE...New group key (K(G4))
FF...Reception acknowledgement

(57) Abstract: Provided are a key information control device, etc., with which communication is possible even if a group key update has failed. Group keys (K(Gn)) that are used in a network including a key information control device (1) and a plurality of communication devices (2A, 2B, 2C) are updated. New group keys (K(G1), K(G2), K(G3)) are transmitted from the key information control device (1) by multicast communication, and the group keys of the communication devices (2A, 2B, 2C) are updated to the group keys (K(Gn)) transmitted from the key information control device (1). The EPOCH value, which is a value in the information transmitted from the communication devices (2A, 2B, 2C) that is updated each time the group key is updated, is checked, and if a communication device (2A) that has not received the updated group key (K(G3)) is detected, a key update message is transmitted to the communication device (2A) by unicast communication that has a retransmission function.

(57) 要約:

[続葉有]



添付公開書類:

— 国際調査報告 (条約第 21 条(3))

グループ鍵の更新に失敗した場合であっても通信を行うことができる鍵情報制御装置等を提供する。鍵情報制御装置 1 と複数の通信機器 2A,2B,2C とを含むネットワークにおいて使用されるグループ鍵 $K(Gn)$ を更新する。鍵情報制御装置 1 からマルチキャスト通信によって新たなグループ鍵 $K(G1)$ 、 $K(G2)$ 、 $K(G3)$ を送信し、鍵情報制御装置 1 から送信されたグループ鍵 $K(Gn)$ に、通信機器 2A,2B,2C のグループ鍵を更新し、通信機器 2A,2B,2C から送信された情報のうちグループ鍵が更新される度に変更される EPOCH 値を参照して、更新されたグループ鍵 $K(G3)$ を受信していない通信機器 2A を検出した場合に、再送機能付きユニキャスト通信を行って鍵更新メッセージを通信機器 2A に送信する。

明細書

鍵情報制御装置、鍵情報更新装置、プログラム及び記録媒体、
鍵情報更新方法、鍵情報更新システム

技術分野

本発明は、複数の機器で使用されるグループ鍵を更新する鍵情報制御装置、鍵情報更新装置、プログラム、記録媒体、鍵情報更新方法、鍵情報更新システムに関する。

背景技術

従来より、マルチキャスト通信用のグループ鍵を交換する技術が知られている（例えば、Multicast Extensions to the Security Architecture for the Internet Protocol (RFC5374) および The Multicast Group Security Architecture (RFC3740) 参照）。

この鍵交換技術は、まず、通信機器の固有鍵を用いて鍵暗号化鍵を制御装置と通信機器とで共有する。その後、制御装置は、マルチキャスト通信を用いてグループ鍵の更新をする。このとき、制御装置は、鍵暗号化鍵を用いてグループ鍵を暗号化する。

このグループ鍵は、暗号メッセージにおけるノンス空間に含まれるEPOCH値という鍵識別子によって管理される。このグループ鍵は、所定の条件（暗号通信回数、時間）となると鍵更新が行われる。

しかしながら、制御装置から複数の通信機器に通信メッセージをマルチキャスト通信しても、全ての通信機器に通信メッセージが送信されない場合がある。

例えば、通信機器が無線機器である場合にはノイズによって無線通信状態が悪化して通信メッセージが送信されない。また、複数の通信機器のうち何れかの通信機器がスリープ状態である場合には通信メッセージが通信路上で消失してしまう。この場合、さらに他の通信機器にも通信メッセージが送信できない恐れがある。

発明の概要

そこで、本発明は、上述した実情に鑑みて提案されたものである。本発明の目的は、グループ鍵の更新に失敗した場合であっても通信を行うことができる鍵情報制御装置、鍵情報更新装置、プログラム及び記録媒体、鍵情報更新方法、鍵情報更新システムを提供するものである。

課題を解決するための手段

本発明の第1の態様に係る鍵情報制御装置は、複数の通信機器を含むネットワークにおいて使用されるグループ鍵を制御する鍵情報制御装置であって、前記グループ鍵が更新される度に鍵識別子を変更し、前記鍵識別子及び新たなグループ鍵を生成する鍵管理手段と、前記鍵管理手段により生成された前記鍵識別子及び前記グループ鍵をマルチキャスト通信によって送信するマルチキャスト通信手段と、前記通信機器から送信された情報のうち前記鍵識別子を参照して、前記グループ鍵を受信していない前記通信機器を検出する通信品質検出手段と、前記通信品質検出手段により前記グループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器に、再送機能付きユニキャスト通信によって前記グループ鍵を送信するユニキャスト通信手段とを備える。

本発明の第2の態様に係る鍵情報制御装置は、第1の態様の鍵情報制御装置であって、前記鍵管理手段は、新たなグループ鍵に変更する度に前記鍵識別子の値を大きく変更し、前記通信品質検出手段は、前記通信機器から送信された情報に含まれる鍵識別子が、前記鍵管理手段により変更された鍵識別子よりも小さい場合に、前記マルチキャスト通信によって送信したグループ鍵を受信していないことを検出することを特徴とする。

本発明の第3の態様に係る鍵情報制御装置は、第1又は第2の態様の鍵情報制御装置であって、前記マルチキャスト通信手段によって使用するポート番号と、前記ユニキャスト通信手段によって使用するポート番号とで異なる値を割り当てることを特徴とする。

本発明の第4の態様に係る鍵情報制御装置は、第1乃至第3の何れかの態様の鍵情報制御装置であって、前記ユニキャスト通信手段は、前記グループ鍵に加えて、前記鍵管理手段が生成した最新の鍵識別子を送信することを特徴とする。

本発明の第5の態様に係る鍵情報制御装置は、第1乃至第4の何れかの態様の鍵情報制御装置であって、前記通信品質検出手段は、前記通信機器ごとに、所定期間における前記通信機器から送信されたメッセージの未受信回数又は所定期間における前

記通信機器による前記グループ鍵の未受信回数をカウントし、前記ユニキャスト通信手段は、前記通信品質検出手段によりカウントした未受信回数が所定の閾値を超えた場合に、当該未受信回数の通信機器に対し、前記マルチキャスト通信によって前記グループ鍵を送信する度にユニキャスト通信によって前記グループ鍵を送信することを特徴とする。

本発明の第6の態様に係る鍵情報制御装置は、第1乃至第5の何れかの態様の鍵情報制御装置であって、前記通信品質検出手段によりグループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器又は他の通信機器に通知を行う通知手段を有することを特徴とする。

本発明の第7の態様に係る鍵情報制御プログラムは、複数の通信機器を含むネットワークにおいて使用されるグループ鍵を制御する鍵情報制御プログラムであって、コンピュータを、前記グループ鍵が更新される度に鍵識別子を変更し、前記鍵識別子及び新たなグループ鍵を生成する鍵管理手段、前記鍵管理手段により生成された前記鍵識別子及び前記グループ鍵をマルチキャスト通信によって送信するマルチキャスト通信手段、前記通信機器から送信された情報のうち前記鍵識別子を参照して、前記グループ鍵を受信していない前記通信機器を検出する通信品質検出手段、前記通信品質検出手段により前記グループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器に、再送機能付きユニキャスト通信によって前記グループ鍵を送信するユニキャスト通信手段、として機能させる。

本発明の第8の態様に係る鍵情報制御プログラムを記録したコンピュータ読み取り可能な記録媒体は、複数の通信機器を含むネットワークにおいて使用されるグループ鍵を制御する鍵情報制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記コンピュータを、前記グループ鍵が更新される度に鍵識別子を変更し、前記鍵識別子及び新たなグループ鍵を生成する鍵管理手段、前記鍵管理手段により生成された前記鍵識別子及び前記グループ鍵をマルチキャスト通信によって送信するマルチキャスト通信手段、前記通信機器から送信された情報のうち前記鍵識別子を参照して、前記グループ鍵を受信していない前記通信機器を検出する通信品質検出手段、前記通信品質検出手段により前記グループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器に、再送機能付きユニキャスト通信によって前記グループ鍵を送信するユニキャスト通信手段、として機能させる。

本発明の第9の態様に係る鍵情報更新装置は、鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新装置であって、前記グループ鍵を、前記鍵情報制御装置からマルチキャスト通信によって受信されたグループ鍵に更新する鍵管理手段と、前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段と、他の通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているかいないかを

検出する通信品質検出手段と、前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵を要求するユニキャスト通信手段とを備える。

本発明の第10の態様に係る鍵情報更新装置は、第9の態様に係る鍵情報更新装置であって、前記通信品質検出手段は、前記鍵情報制御装置又は前記他の通信機器から送信された情報に含まれる鍵識別子が、自己に記憶された鍵識別子よりも大きい場合に、前記マルチキャスト通信によって送信したグループ鍵を受信していないことを検出することを特徴とする。

本発明の第11の態様に係る鍵情報更新プログラムは、鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新プログラムであって、コンピュータを、前記グループ鍵を、前記情報制御装置からマルチキャスト通信によって受信されたグループ鍵に更新する鍵管理手段、前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段、他の通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているか否かを検出する通信品質検出手段、前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵を要求するユニキャスト通信手段として機能させる。

本発明の第12の態様に係る鍵情報更新プログラムを記録したコンピュータ読み取り可能な記録媒体は、鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記コンピュータを、前記グループ鍵を、前記鍵情報制御装置からマルチキャスト通信によって受信されたグループ鍵に更新する鍵管理手段、前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段、他の通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているか否かを検出する通信品質検出手段、前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵を要求するユニキャスト通信手段として機能させる。

本発明の第13の態様に係る鍵情報更新方法は、鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新方法であって、前記鍵情報制御装置からマルチキャスト通信によって新たなグループ鍵を送信するステップと、前記鍵情報制御装置から送信されたグループ鍵に、前記通信機器のグループ鍵を更新するステップと、前記通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているか否かを検出するステップと、前記グ

グループ鍵が更新されていない前記通信機器が検出された場合に、再送機能付きユニキャスト通信を行ってグループ鍵を前記通信機器によって取得するステップとを含む。

本発明の第14の態様に係る鍵情報更新システムは、鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新システムであって、前記通信機器のグループ鍵を、前記鍵情報制御装置から送信されたグループ鍵に更新する鍵管理手段と、前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段と、前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、前記通信機器が前記グループ鍵が更新されているか否かを検出する通信品質検出手段と、前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、前記鍵情報制御装置によってグループ鍵を送信する通信方式をマルチキャスト通信から再送機能付きユニキャスト通信に切り替え、再送機能付きユニキャスト通信によって前記通信機器にグループ鍵を送信する通信手段とを備える。

本発明の第15の態様に係る鍵情報更新システムは、第14の態様に係る鍵情報更新システムであって、前記鍵情報制御装置は、前記グループ鍵をマルチキャスト通信によって送信する間隔を所定期間とし、前記通信機器は、前記所定期間を超えて前記グループ鍵を受信していない場合に、前記マルチキャスト通信によってグループ鍵を受信できていないことを検出することを特徴とする。

本発明の第16の態様に係る鍵情報更新方法は、鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を更新する鍵情報更新方法であって、前記鍵情報制御装置により前記グループ鍵とは異なり、前記鍵情報制御装置と前記複数の通信機器とを含むネットワークにおいて使用されるリカバリー鍵を生成するステップと、前記鍵情報制御装置により前記鍵情報制御装置と前記通信機器との間で認証処理を行った後に、前記リカバリー鍵を配布するステップと、前記鍵情報制御装置からマルチキャスト通信によって新たなグループ鍵を送信するステップと、前記鍵情報制御装置から送信されたグループ鍵に、前記通信機器のグループ鍵を更新するステップとを含む。

本発明の第17の態様に係る鍵情報更新方法は、第16の態様に係る鍵情報更新方法であって、前記鍵情報制御装置により、前記鍵情報制御装置が、前記通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を参照して、グループ鍵を更新していない通信機器ことを検出するステップと、前記鍵情報制御装置が、前記グループ鍵を更新していない通信機器が検出された場合に、前記リカバリー鍵を用いて暗号化したグループ鍵を送信するステップとを含むことを特徴とする。

本発明の第18の態様に係る鍵情報更新方法は、第16の態様に係る鍵情報更新方法であって、前記鍵情報制御装置により、前記通信機器が、前記グループ鍵によってメッセージが送信できない場合に、前記リカバリー鍵を用いて暗号化したメッセージ

を送信するステップを含むことを特徴とする。

発明の効果

本発明によれば、グループ鍵の更新に失敗した場合であっても通信を行うことができる。

図面の簡単な説明

【図 1】本発明の実施形態として示す鍵情報更新システムの構成を示すシステム図である。

【図 2】本発明の実施形態として示す鍵情報制御装置の構成を示すブロック図である。

【図 3】本発明の実施形態として示す通信機器の構成を示すブロック図である。

【図 4】本発明の実施形態として示す鍵情報更新システムにおいて授受されるノンス値を示し、(a) は第 1 構成例、(b) は第 2 構成例である。

【図 5】本発明の実施形態として示す鍵情報更新システムにおいて、通信不良が生じていないときの通信手順の一例を示すシーケンス図である。

【図 6】本発明の実施形態として示す鍵情報更新システムにおいて、グループ鍵を更新するときのノンス値の一例を示すシーケンス図である。

【図 7】本発明の実施形態として示す鍵情報更新システムにおいて、通信不良を鍵情報制御装置により検出するときの通信手順の一例を示すシーケンス図である。

【図 8】本発明の実施形態として示す鍵情報更新システムにおいて、通信不良を通信機器により検出するときの通信手順の一例を示すシーケンス図である。

【図 9】本発明の実施形態として示す鍵情報更新システムにおいて、通信不良を通信機器のタイマーにより検出するときの通信手順の一例を示すシーケンス図である。

【図 10】本発明の実施形態として示す鍵情報更新システムにおける鍵情報制御装置の処理手順の一例を示すフローチャートである。

【図 11】本発明の実施形態として示す鍵情報更新システムにおける通信機器の処理手順の一例を示すフローチャートである。

【図 12】本発明の実施形態として示す鍵情報更新システムにおいて、通信不良をカウンタ値、EPOCH 値により判定するときの通信手順の一例を示すシーケンス図である。

【図 13】本発明の実施形態として示す鍵情報更新システムにおいて、通信不良

となった通信機器にマルチキャスト通信とユニキャスト通信とを併用するときの通信手順の一例を示すシーケンス図である。

【図 1 4】本発明の実施形態として示す鍵情報更新システムにおいて、通信機器を通常モード又は保証モードに設定する処理手順の一例を示すフローチャートである。

【図 1 5】本発明の実施形態として示す鍵情報更新システムにおいて、不安定な通信路を通知するときの通信手順の一例を示すシーケンス図である。

【図 1 6】本発明の実施形態として示す鍵情報更新システムにおいて、鍵情報制御装置によって所定期間ごとに鍵更新メッセージを送信する処理手順の一例を示すフローチャートである。

【図 1 7】本発明の実施形態として示す鍵情報更新システムにおいて、鍵情報制御装置から複数の通信機器にリカバリー鍵を用いてグループ鍵を送信する通信手順の一例を示すシーケンス図である。

【図 1 8】本発明の実施形態として示す鍵情報更新システムにおいて、通信機器から鍵情報制御装置 1 及び通信機器にリカバリー鍵を用いてメッセージを送信する通信手順の一例を示すシーケンス図である。

発明を実施するための形態

以下、本発明の実施の形態について図面を参照して説明する。

本発明を適用した鍵情報更新システムは、例えば図 1 に示すように構成されている。

鍵情報更新システムは、鍵情報制御装置 1 と、複数の通信機器 2 A, 2 B, 2 C（以下、総称する場合には単に通信機器 2 と呼ぶ。）とを含む。鍵情報制御装置 1 及び通信機器 2 は、通信中継装置 100 に接続されている。鍵情報制御装置 1 及び通信機器 2 は、通信中継装置 100 によって情報が中継されて、相互に通信可能となっている。

通信中継装置 100 は、例えばインターネット等の通信ネットワーク NT と有線接続されている。通信中継装置 100 は、例えばブロードバンドルータが該当する。

通信機器 2 は、例えば家庭内に設置された各種の機器である。本実施形態において、通信機器 2 A は、通信中継装置 100 との間で無線信号を授受する無線通信機器である。通信機器 2 B、2 C は、通信中継装置 100 と通信線で有線接続されている。

本実施形態において、通信機器 2 は、有線通信又は無線通信を行うものであってもよい。無線通信は、一般的に、有線通信よりも通信品質が低い。また、通信機器 2 は、任意のタイミングでスリープ状態となり、一定期間又は何らかの外部トリガーにより起動するものであってもよい。このスリープ状態は、最低限の電力のみで動作し、通信が行えないような状態を含む。なお、通信機器 2 は、3 つ以上であってもよい。

鍵情報制御装置 1 は、複数の通信機器 2 との間で通信を行い、複数の通信機器 2 を

制御する。鍵情報制御装置 1 は、通信機器 2 との間で暗号化通信を行う。このために、鍵情報制御装置 1 は、各通信機器 2 との間で認証処理、鍵配布処理を行う。さらに、鍵情報制御装置 1 は、複数の通信機器 2 を含むネットワークにおいて使用されるグループ鍵を更新する。

鍵情報制御装置 1 は、例えば図 2 に示すような機能的な各部を有している。鍵情報制御装置 1 は、プログラムを読み込んで実行可能なコンピュータである。鍵情報制御装置 1 は、コンピュータによってプログラムを実行することにより、図 2 に示すような各部として機能する。このプログラムは、本実施形態において、複数の通信機器 2 を含むネットワークにおいて使用されるグループ鍵を更新する鍵情報制御プログラムである。

鍵情報制御装置 1 は、制御部 11、通信部 12、認証処理部 13、認証情報記憶部 14、鍵管理部 15、及び、暗号処理部 16 を有する。さらに、鍵情報制御装置 1 は、通信品質計測部 17 及び通信品質記憶部 18 を有する。さらに、鍵情報制御装置 1 は、タイマー部 19 を有する。

通信部 12 は、通信機器 2 との間で通信を行う。通信部 12 は、マルチキャスト通信方式及びユニキャスト通信方式の何れかで通信機器 2 と通信を行う。この通信方式の切り替えは、制御部 11 によって制御される。

制御部 11 は、鍵情報制御装置 1 の各部を制御する。制御部 11 は、プログラムを記録したコンピュータ読み取り可能な記録媒体としての記憶部 11a に記憶された鍵情報制御プログラム 11b を実行する。

認証処理部 13 は、鍵情報制御装置 1 に接続される通信機器 2 との間で認証処理を行う。この認証処理部 13 は、既存の各種の認証処理が実行可能で有ればよい。

認証処理部 13 は、認証処理時に、認証情報記憶部 14 に記憶された認証情報を読み出す。認証情報は、例えば通信機器 2 のノード ID と機器固有鍵 KD (Key of Device) (又はパスワード) である。認証処理部 13 は、通信機器 2 から送信された認証情報と認証情報記憶部 14 に記憶された認証情報とを対比して、通信機器 2 が正当な権限を有しているか否かを判定する。なお、機器固有鍵 KD の代わりに公開鍵と秘密鍵を用いて、通信機器 2 が正当な権限を有しているかを判断してもよい。機器固有鍵 KD を秘密鍵としても同じように実施することができる。

鍵管理部 15 は、鍵情報制御装置 1 が通信機器 2 との間で暗号化通信を行う際に使用する鍵情報を管理する。鍵管理部 15 は、通信機器 2 の機器固有鍵 KD (ユニキャストでの通信機器の認証及び鍵暗号化鍵の配信用の鍵 (Key of Device))、鍵暗号化鍵 KEK (Key Encryption Key)、グループ鍵 K (Gn) を管理する。管理されている鍵情報は、鍵管理テーブル 15a に記憶される。

通信機器 2 ごとの機器固有鍵 KD は、鍵情報制御装置 1 が通信機器 2 へ送る鍵暗号化鍵 KEK の暗号化や通信機器 2 を認証するための鍵情報である。この機器固有鍵 KD は、予め鍵情報制御装置 1 と各通信機器 2 に設定され、共有される。

鍵暗号化鍵KEKは、鍵の暗号化用の鍵である。鍵暗号化鍵KEKは、鍵情報制御装置1が導出する。鍵暗号化鍵KEKは、認証、鍵配布時に全通信機器2と鍵情報制御装置1とで共有される。

なお、通信機器2の機器固有鍵KDは、鍵情報制御装置1と通信機器2との間で鍵暗号化鍵(KEK)を暗号化して通信機器2に配信するための鍵情報(暗号化鍵)である。鍵情報制御装置1はセキュリティ性を高めるために通信機器2の機器毎に異なる値の機器固有鍵KDを持つことができる。

グループ鍵K(Gn)は、鍵情報制御装置1及び全ての通信機器2間で暗号化したマルチキャスト通信を行うための鍵情報である。グループ鍵K(Gn)は、鍵情報制御装置1が導出する。グループ鍵K(Gn)は、鍵暗号化鍵KEKで暗号化され、マルチキャスト通信によって全ての通信機器2に配布される。なお、グループ鍵K(Gn)におけるnは鍵のバージョンである。鍵管理部15によって新たに生成することにより、n=1, 2, 3, ...と増加される。

鍵管理部15は、鍵暗号化鍵KEK、グループ鍵K(Gn)を導出し、予め全通信機器2の機器固有鍵KDを保持している。鍵管理部15は、導出した鍵暗号化鍵KEKを、通信部12から各通信機器2に送信させる。また、鍵管理部15は、マルチキャスト通信によってグループ鍵K(Gn)を更新させる。

鍵管理部15は、鍵識別子を管理する。鍵識別子は、グループ鍵K(Gn)が更新される度に変更される値(EPOCH値)である。鍵管理部15は、グループ鍵を更新する度に、古いEPOCH値を新たなEPOCH値に更新する。

暗号処理部16は、鍵管理テーブル15aに記憶されている鍵情報を用いて、メッセージの暗号化処理を行う。また、暗号処理部16は、通信部12によって受信した暗号化情報を鍵管理テーブル15aに記憶されている鍵情報を用いて、暗号化データを復号化する。このとき、暗号処理部16は、鍵管理テーブル15aに記憶された適切な鍵情報を選択して使用する。

通信品質計測部17は、各通信機器2との間における通信品質を計測する。通信品質計測部17は、通信機器2から送信された情報のうちEPOCH値を参照する。通信品質計測部17は、古いEPOCH値の場合に、マルチキャスト通信によって送信したグループ鍵K(Gn)を受信していない通信機器2を検出する(通信品質検出手段)。また、通信品質計測部17は、後述するように、ノンス値のカウンタ値を使用して通信品質を検出してもよい。

通信品質記憶部18は、通信品質計測部17によって参照したEPOCH値を通信機器2ごとに記憶する。EPOCH値は、通信品質計測部17によって参照される。これにより、通信品質計測部17は、EPOCH値の抜けがある通信機器2について、通信品質が低いと判定できる。

このような鍵情報制御装置1は、制御部11によって通信部12の通信方式を変更する。通信部12は、通常のグループ鍵K(Gn)の更新処理において、鍵管理部1

5により生成されたEPOCH値及びグループ鍵K(G_n)をマルチキャスト通信によって複数の通信機器2に送信する(マルチキャスト通信手段)。

通信部12は、通信品質検出手段としての通信品質計測部17によりグループ鍵K(G_n)を受信していない通信機器2が検出された場合に、当該通信機器2に、再送機能付きユニキャスト通信によってグループ鍵K(G_n)を送信する(ユニキャスト通信手段)。

タイマー部19は、グループ鍵K(G_n)をマルチキャスト通信によって送信する間隔を計測する。このグループ鍵K(G_n)の送信間隔は、制御部11によって所定期間が設定される。タイマー部19は、制御部11によってタイマー値のクリア、タイマー値の計時が制御される。

通信機器2は、例えば図3に示すような機能的な各部を有している。通信機器2は、プログラムを読み込んで実行可能なコンピュータである。通信機器2は、コンピュータによってプログラムを実行することにより、図3に示すような各部として機能する。このプログラムは、本実施形態において、自己が保持するグループ鍵を更新する鍵情報更新プログラムである。これにより、通信機器2は、鍵情報更新装置として機能する。

通信機器2は、制御部21、通信部22、認証処理部23、鍵管理部24、及び、暗号処理部25を有する。さらに、通信機器2は、通信品質計測部26及び通信品質記憶部27を有する。さらに、通信機器2は、タイマー部28を有する。

通信部22は、鍵情報制御装置1及び他の通信機器2との間で通信を行う。通信部22は、マルチキャスト通信方式及びユニキャスト通信方式の何れかで鍵情報制御装置1と通信を行う。この通信方式の切り替えは、制御部21によって制御される。

制御部21は、通信機器2の各部を制御する。制御部21は、プログラムを記録したコンピュータ読み取り可能な記録媒体としての記憶部21aに記憶された鍵情報更新プログラム21bを実行する。

認証処理部23は、鍵情報制御装置1との間で認証処理を行う。この認証処理部23は、既存の各種の認証処理が実行可能で有ればよい。

認証処理部23は、認証処理時に、予め設定された認証情報を読み出す。認証情報は、例えば通信機器2のノードIDと機器固有鍵KD(Key of Device)(又はパスワード)である。認証処理部23は、鍵情報制御装置1の要求に応じて、認証情報を通信部22から鍵情報制御装置1に送信させる。

鍵管理部24は、鍵情報制御装置1及び他の通信機器2との間で暗号化通信を行う際に使用する鍵情報を管理する。鍵管理部24は、通信機器2の機器固有鍵KD、鍵暗号化鍵KEK、グループ鍵K(G_n)を管理する。管理されている鍵情報は、鍵管理テーブル24aに記憶される。また、鍵管理部24は、鍵識別子を鍵管理テーブル24aに記憶させる。

暗号処理部25は、鍵管理テーブル24aに記憶されている鍵情報を用いて、メッ

セージの暗号化処理を行う。また、暗号処理部 25 は、通信部 22 によって受信した暗号化情報を鍵管理テーブル 24 a に記憶されている鍵情報を用いて、暗号化データを復号化する。このとき、暗号処理部 25 は、鍵管理テーブル 24 a に記憶された適切な鍵情報を選択して使用する。

通信品質計測部 26 は、鍵情報制御装置 1 との間における通信品質を計測する。通信品質計測部 26 は、鍵情報制御装置 1 又は他の通信機器 2 から送信された情報のうち EPOCH 値を参照する。通信品質計測部 26 は、受信した情報のうちの EPOCH 値と鍵管理テーブル 24 a に保持していると EPOCH 値を対比する。この対比の結果、通信品質計測部 26 は、双方の EPOCH 値が異なることや、EPOCH 値の差分を検出する。この場合、通信品質計測部 26 は、更新されたグループ鍵 K (Gn) を受信していないことを検出する（通信品質検出手段）。また、通信品質計測部 26 は、タイマー値を参照して、通信品質として、グループ鍵 K (Gn) を受信していないことを検出してもよい。

通信品質記憶部 27 は、通信品質計測部 26 によって参照した EPOCH 値を記憶する。EPOCH 値は、通信品質計測部 26 によって参照される。これにより、通信品質計測部 26 は、EPOCH 値の抜けがある場合に、通信品質が低いと判定できる。

このような通信機器 2 は、通信品質計測部 26 により更新されたグループ鍵 K (Gn) を受信していないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵 K (Gn) を要求する。このとき、通信機器 2 は、鍵要求メッセージを鍵情報制御装置 1 に送信する。これにより、通信機器 2 は、ユニキャスト通信によって、通信部 22 が現在のグループ鍵 K (Gn) を取得する（通信手段）。

タイマー部 28 は、グループ鍵 K (Gn) をマルチキャスト通信によって受信する間隔を計測する。このグループ鍵 K (Gn) の受信間隔は、予め鍵情報制御装置 1 との間で、所定期間が設定される。タイマー部 28 は、制御部 21 によってタイマー値のクリア、タイマー値の計時が制御される。これにより、タイマー部 28 は、所定期間を超えてグループ鍵 K (Gn) を受信していない場合に、マルチキャスト通信によってグループ鍵 K (Gn) を受信できていないことを検出する。

この鍵情報更新システムにおいて、鍵情報制御装置 1 は、通信機器 2 との間で暗号化通信を行う。このために、鍵情報制御装置 1 は、通信機器 2 をそれぞれ認証する。その後、鍵情報制御装置 1 は、各通信機器 2 との間のみで暗号化通信できる鍵暗号化鍵 KEK を配布する。さらに、鍵情報制御装置 1 は、全ての通信機器 2 と暗号化通信できるグループ鍵 K (Gn) を配布する。

これにより、グループ鍵 K (Gn) は、鍵情報制御装置 1 及び全ての通信機器 2 によって共有される。なお、グループ鍵 K (Gn) において、Gn は当該グループ鍵の時代 (EPOCH 値) に対応している。

このような鍵情報更新システムは、図 1 に示すように、鍵情報制御装置 1 から通信機器 2 にグループ鍵 S 1 をマルチキャスト通信により送信する。このグループ鍵 S 1

は、通信中継装置 100 を介して、通信機器 2 に送信される。通信機器 2 A は無線通信機器であるので、通信中継装置 100 から通信機器 2 A に無線信号 S 2 a が送信される。通信機器 2 B、2 C は有線通信機器であるので、通信中継装置 100 から通信機器 2 B、2 C に有線信号 S 2 b、S 2 c が送信される。

例えば、無線信号 S 2 a がノイズ等を起因とする通信不良によって消失したとする。この場合、通信機器 2 A は、鍵情報制御装置 1 及び他の通信機器 2 B、2 C が使用するグループ鍵 S 1 が受信できない。したがって、通信機器 2 A は、その後にグループ鍵 S 1 で暗号化されたマルチキャスト通信によって送信された情報を復号できない。また、通信機器 2 A は、古いグループ鍵で暗号化した情報を送信する。したがって、通信機器 2 A から送信された情報は、鍵情報制御装置 1 及び他の通信機器 2 B、2 C によって復号できない。

そこで、本実施形態の鍵情報更新システムは、グループ鍵の更新に失敗した場合であっても通信を行うことができるようにする。このため、鍵情報更新システムは、通信不良を検出する。通信不良が検出された場合、鍵情報更新システムは、マルチキャスト通信とユニキャスト通信とを併用して、通信不良が発生した通信機器 2 のグループ鍵を更新する。以下、この動作を詳細に説明する。

まず、鍵情報更新システムにおいて通信するパケットに含まれる EPOCH 値を含むノンス (Nonce) について、図 4 を参照して説明する。

鍵情報更新システムにおいて通信するパケットには、IP アドレスや UDP に加え、図 4 (a) 又は図 4 (b) に示すノンスが含まれている。ノンスは、データ暗号化時のパラメータの一つとして使用し、送信データメッセージのヘッダー部に付加される。図 4 (a) に示すノンスには、EPOCH 値及びカウンタ値が含まれている。図 4 (b) に示すノンスには、EPOCH 値、ノード ID、及び、カウンタ値が含まれている。

EPOCH 値は、グループ鍵 K (G_n) の識別子である。EPOCH 値は、鍵情報制御装置 1 によって、グループ鍵 K (G_n) が更新される度に変更される。鍵情報制御装置 1 は、グループ鍵 K (G_n) を新たなものとする度に、EPOCH 値をインクリメントする。

ノード ID は、鍵情報制御装置 1 及び通信機器 2 を識別する識別子である。鍵情報制御装置 1 及び通信機器 2 は、データを送信する際に自己のノード ID をメッセージに格納する。

カウンタ値は、EPOCH 値で識別されるグループ鍵 K (G_n) を用いて暗号化マルチキャスト通信を行った回数を表す。このカウンタ値は、鍵情報制御装置 1 及び通信機器 2 のそれぞれによって管理される。カウンタ値は、鍵情報制御装置 1 及び通信機器 2 がデータを送信するごとにカウントアップされる。グループ鍵 K (G_n) の更新は、鍵情報制御装置 1 によって、カウンタ値が最大値に達する前に実施される。

つぎに、この鍵情報更新システムにおいて、通信不良が発生していない場合の動作について、図 5 を参照して説明する。

先ず、鍵情報制御装置 1 と通信機器 2 C との間で、認証処理及び鍵配布処理 P 1 を行う。鍵情報制御装置 1 は、通信機器 2 C が正当な機器であると判定した後、ユニキャスト通信によって、鍵暗号化鍵 K_{EK} を配布する。

次に、鍵情報制御装置 1 は、マルチキャスト通信によってグループ鍵 $K(G1)$ を配布する。このとき、鍵情報制御装置 1 は、関数 $E(K_{EK}, K(G1))$ で得た暗号化情報をマルチキャスト通信で送信する。この関数 E は、鍵暗号化鍵 K_{EK} を用いてグループ鍵 $K(G1)$ を暗号化する関数である。この鍵暗号化鍵 K_{EK} は、処理 P 1 にて配布された鍵暗号化鍵 K_{EK} である。

通信機器 2 C は、鍵情報制御装置 1 からマルチキャスト通信された関数 E を受信すると、復号する。このとき、通信機器 2 C は、関数 $D(K_{EK}, E(K_{EK}, K(Gn)))$ なる演算を行う。この関数 D は、鍵暗号化鍵 K_{EK} を用いて、 $E(K_{EK}, K(Gn))$ で得た暗号化情報を復号する関数である。これにより、通信機器 2 C は、グループ鍵 $K(G1)$ を復号することができる。

鍵情報制御装置 1 は、通信機器 2 B、通信機器 2 A についても、同様に認証処理及び鍵配布処理 P 2、P 3 を行う。さらに、鍵情報制御装置 1 は、認証処理及び鍵配布処理 P 2、P 3 が完了する度に、グループ鍵 $K(G2)$ 、 $K(G3)$ を配布する。

これにより、鍵情報制御装置 1 及び全ての通信機器 2 は、グループ鍵 $K(G3)$ を用いて、暗号化マルチキャスト通信によってデータ通信処理 P 4 を行うことができる。

グループ鍵 $K(Gn)$ の更新タイミングとなると、鍵情報制御装置 1 及び通信機器 2 は、鍵更新処理 P 5 を行う。この鍵更新処理 P 5 は、鍵情報制御装置 1 によって生成した新たなグループ鍵 $K(G4)$ をマルチキャスト通信によって全ての通信機器 2 に配布する。そして、それぞれの通信機器 2 は、マルチキャスト通信によってグループ鍵 $K(G4)$ を受信し、鍵管理テーブル 2 4 a に記憶しているグループ鍵 $K(G3)$ を、新たなグループ鍵 $K(G4)$ に更新する。

その後、例えば鍵情報制御装置 1 から全ての通信機器 2 に暗号化データを送信する。この暗号化データは、関数 $E(K(G4), \text{データ})$ で得た暗号化情報を含む。各通信機器 2 は、鍵情報制御装置 1 から送信された暗号化データがマルチキャスト通信によって受信する。各通信機器 2 は、暗号化データをグループ鍵 $K(G4)$ で復号する。これにより、各通信機器 2 は、関数 $D(K(G4), E(K(G4), \text{データ}))$ なる演算を行って、データを得ることができる。

つぎに、上述した鍵情報更新システムにおいて、グループ鍵 $K(Gn)$ を更新するときのノンス値について、図 6 を参照して説明する。ノンスに含まれる EPOCH 値、ノード ID、カウンタ値は、図 6 において、 $\text{Nonce} = \{\text{EPOCH}, \text{ノード ID}, \text{カウンタ値}\}$ として示している。

通信機器 2 C によってグループ鍵 $K(G1)$ を用いて暗号化した暗号化データを送信する。この暗号化データには、ノンス値が付加される。この暗号化データは、マル

チキャスト通信によって通信機器 2 A、通信機器 2 B、及び、鍵情報制御装置 1 に送信される。

まず、1 回目に送信される暗号化データには、Nonce = {0, 3, 0} が付加される。2 回目に送信される暗号化データには、カウンタ値が増加された Nonce = {0, 3, 1} が付加される。そして、カウンタ値の最大値から 1 だけ差し引いた回数に送信される暗号化データには Nonce = {0, 3, $2^{3^2}-1$ } が付加される。

鍵情報制御装置 1 は、最大値から 1 だけ引いたカウンタ値をノンス値 Nonce = {0, 3, $2^{3^2}-1$ } から検出する。すると、鍵情報制御装置 1 は、マルチキャスト通信によって新たなグループ鍵 K (G 2) を含む鍵更新メッセージを送信する。これにより、通信機器 2 C は、グループ鍵 K (G 1) を、新たなグループ鍵 K (G 2) に更新する。

その後、通信機器 2 C は、グループ鍵 K (G 2) で暗号化した暗号化データのそれぞれに、Nonce = {1, 3, 0}、Nonce = {1, 3, 1}、Nonce = {1, 3, $2^{3^2}-1$ } を付加できる。さらにその後、グループ鍵 K (G 2) によって暗号化した暗号化データを送信した回数が $2^{3^2}-1$ となると、グループ鍵 K (G 2) を、新たなグループ鍵 K (G 3) に更新することとなる。

つぎに、上述した鍵情報更新システムにおいて、鍵情報制御装置 1 がグループ鍵 K (G n) の未受信を検出した場合の動作について、図 7 を参照して説明する。

まず、鍵情報更新システムは、図 5 を参照して説明したように、鍵情報制御装置 1 と通信機器 2 A、2 B、2 C との間で、認証処理及び鍵配布処理 P 1、P 2、P 3 を行う。さらに、鍵情報制御装置 1 は、認証処理及び鍵配布処理後に、グループ鍵 K (G n) をマルチキャスト通信によって配布する。その結果、鍵情報制御装置 1 及び通信機器 2 A、2 B、2 C は、最新のグループ鍵 K (G 3) を用いてデータ通信処理 P 4 を行う。

その後、グループ鍵 K (G n) の更新タイミングとなると、鍵情報制御装置 1 は、通信機器 2 A、2 B、2 C に対して、マルチキャスト通信によってグループ鍵 K (G 4) を配布する鍵更新処理 P 5 を行う (マルチキャスト通信手段)。このグループ鍵 K (G 4) に対応した EPOCH 値は「3」である。このとき、鍵情報制御装置 1 から通信機器 2 A に送信された鍵更新メッセージは通信不良により通信機器 2 A に受信されなかったとする。

その後、通信機器 2 A は、旧グループ鍵 K (G n) としてのグループ鍵 K (G 3) によって暗号化した暗号化データを送信する。このグループ鍵 K (G 3) に対応した EPOCH 値は「2」である。すると、この暗号化データは、通信機器 2 B、2 C、及び、鍵情報制御装置 1 に受信される。しかし、通信機器 2 B、2 C、及び、鍵情報制御装置 1 は、最新のグループ鍵 K (G 4) を用いて復号しようとしても復号が失敗する。

復号が失敗すると、鍵情報制御装置 1 は、通信機器 2 A から送信された情報のうち EPOCH 値を参照する。すると、鍵情報制御装置 1 が保持している EPOCH 値は

「3」であるのに対し、通信機器2 Aから送信された情報のうちEPOCH値は「2」である。これにより、鍵情報制御装置1は、マルチキャスト通信によって送信したグループ鍵K (G 4)を受信していない通信機器として通信機器2 Aを検出する(通信品質検出手段)。

この場合、鍵情報制御装置1は、通信機器2 Aに、再送機能付きユニキャスト通信によってグループ鍵K (G 4)を送信する(ユニキャスト通信手段)。このとき、鍵情報制御装置1は、認証処理及び鍵配布処理P 3において配布した鍵暗号化鍵KEKによって、新たなグループ鍵K (G 4)を暗号化する。

鍵情報制御装置1は、ユニキャスト通信によってグループ鍵K (G 4)を送信する場合、再送機能付きユニキャスト通信を行う。この再送機能付きユニキャスト通信は、通信機器2から受信応答を受信するまで、ユニキャスト通信を繰り返す。鍵情報制御装置1は、例えば、2回に亘りユニキャスト通信を行ってグループ鍵K (G 4)が通信不良によって消失しても、3回目のユニキャスト通信によって通信機器2 Aにグループ鍵K (G 4)を送信できる。

このユニキャスト通信によって送信されたグループ鍵K (G 4)は、通信機器2 Aの鍵暗号化鍵KEKを用いて復号される。通信機器2 Aは、グループ鍵K (G 3)を、最新のグループ鍵K (G 4)に更新できる。通信機器2 Aは、最新のグループ鍵K (G 4)を受信すると、鍵情報制御装置1に対し、ユニキャスト通信によって受信応答を送信する。

また、鍵情報制御装置1は、再送機能付きユニキャスト通信によって、グループ鍵K (G n)に加えて、最新のEPOCH値を送信してもよい。この場合、通信機器2 Aは、グループ鍵K (G 3)をグループ鍵K (G 4)に更新すると共に、記憶しているEPOCH値「2」を、最新のEPOCH値「3」に更新できる。

以上のように、鍵情報更新システムによれば、マルチキャスト通信によって送信したグループ鍵K (G n)が通信不良によって消失しても、グループ鍵K (G n)を送信する通信方式を自動的にマルチキャスト通信から再送機能付きユニキャスト通信に切り替える。

これにより、鍵情報更新システムは、マルチキャスト通信方式から、受信応答を要する再送機能付きユニキャスト通信に切り替えてグループ鍵K (G n)を送信することにより、グループ鍵K (G n)の更新をより確実に実施することができる。

また、この鍵情報更新システムによれば、鍵管理部15によって、新たなグループ鍵に変更する度にEPOCH値の値を大きく変更する。鍵情報制御装置1は、通信品質計測部17によって、通信機器2から送信されたEPOCH値が、鍵管理部15により変更されたEPOCH値よりも小さい場合に、マルチキャスト通信によって送信したグループ鍵を受信していないことを検出できる。

このように、EPOCH値を参照して、マルチキャスト通信による鍵更新メッセージが消失したことを検出し、再送機能付きユニキャスト通信に切り替えて鍵更新を実

施できる。これにより、確実にグループ鍵を更新でき、かつ、再度認証処理及びシステム全体の鍵更新の処理を行うことなく、グループ鍵を用いたマルチキャスト通信を実施できる。

さらに、この鍵情報更新システムによれば、鍵情報制御装置 1 によって、最新のグループ鍵に加えて、鍵管理部 15 が生成した最新の EPOCH 値を送信することができる。これにより、鍵情報制御装置 1 から通信機器 2 に、再送機能付きユニキャスト通信によって、最新の EPOCH 値を送信できる。これにより、鍵情報更新システムは、鍵情報制御装置 1 から通信機器 2 に最新の EPOCH 値を送信して、直ちにグループ鍵を用いたマルチキャスト通信を容易に開始できる。

つぎに、上述した鍵情報更新システムにおいて、通信機器 2 がグループ鍵 K (G_n) の未受信を検出した場合の動作について、図 8 を参照して説明する。

鍵情報更新システムは、上述したように、鍵情報制御装置 1 と通信機器 2 A, 2 B, 2 C との間で、認証処理及び鍵配布処理 P 1、P 2、P 3 を行う。さらに、鍵情報制御装置 1 及び通信機器 2 A, 2 B, 2 C は、最新のグループ鍵 K (G₃) を用いてデータ通信処理 P 4 を行う。その後、グループ鍵 K (G_n) の更新タイミングとなり、鍵情報制御装置 1 から通信機器 2 A に送信された鍵更新メッセージは通信不良により通信機器 2 A に受信されなかったとする。

その後、鍵情報制御装置 1 は、新たなグループ鍵 K (G₄) によって暗号化した暗号化データをマルチキャスト通信によって送信する。このグループ鍵 K (G₄) に対応した EPOCH 値は「3」である。すると、この暗号化データは、通信機器 2 A, 2 B, 2 C に受信される。通信機器 2 B, 2 C は、鍵更新処理 P 5 によって得た新たなグループ鍵 K (G₄) によって暗号化データの復号に成功できる。

しかし、通信機器 2 A は、自身が鍵管理テーブル 24 a に記憶しているグループ鍵 K (G₃) によって復号しようとしても復号が失敗する。復号が失敗すると、通信機器 2 A は、鍵情報制御装置 1 から送信された情報のうち EPOCH 値を参照する。すると、通信機器 2 A が保持している EPOCH 値は「2」であるのに対し、鍵情報制御装置 1 から送信された情報のうち EPOCH 値は「3」である。これにより、通信機器 2 A は、最新のグループ鍵 K (G_n) を受信していないことを検出する（通信品質検出手段）。

この場合、通信機器 2 A は、鍵情報制御装置 1 に、再送機能付きユニキャスト通信によって最新のグループ鍵 K (G_n) の送信を要求する（ユニキャスト通信手段）。なお、通常は平文で、新たなグループ鍵の要求メッセージを送る。この平文のメッセージは、[MSG、EPOCH、D__2 A] の構成例になる。ここで、MSG は要求であることを示す識別子であり、EPOCH は通信機器 2 A が鍵情報制御装置 1 から受信した EPOCH 値であり、D__2 A は通信機器 2 A を識別できる識別子または ID である。

このとき、通信機器 2 A は、認証処理及び鍵配布処理 P 3 において配布した暗号化

鍵KEKによって、新たなグループ鍵K (G_n)を要求する鍵要求メッセージにメッセージ認証コード(MAC)の情報を付加してもよい。このメッセージ認証コードの情報は、通信機器2Aであることを証明するための情報である。

このメッセージ認証コード(MAC)を付加した要求は、例えば、{MSG, EPOCH, D_2A, MAC(KD_2A, MSG, D_2A, EPOCH)}の構成例になる。関数MACは、鍵情報としてKD_2A、メッセージとしてMSG, D_2A, EPOCHを入力値として計算し、MAC値を出力する。このMAC値は、通信機器2Aの機器固有鍵KDが含まれている。このため、機器固有鍵KDが異なると同じMSG, D_2A, EPOCHを入力してもMAC値は一致しない。したがって、MAC値は、通信機器2Aであることを証明する情報となる。MSGは要求であることを示す識別子(文字列も含む)である。EPOCHは、通信機器2Aが鍵情報制御装置1から受信したEPOCH値である。D_2Aは通信機器2Aを識別できる識別子またはノードIDである。

通信機器2Aは、ユニキャスト通信によってグループ鍵K (G_n)を要求する場合、再送機能付きユニキャスト通信を行う。この再送機能付きユニキャスト通信は、鍵情報制御装置1から受信応答を受信するまで、ユニキャスト通信を繰り返す。通信機器2Aは、例えば、2回に亘りユニキャスト通信を行ってグループ鍵K (G_n)の要求が通信不良によって消失しても、3回目のユニキャスト通信によって鍵情報制御装置1にグループ鍵K (G_n)の鍵要求メッセージを送信できる。

このユニキャスト通信によって送信されたグループ鍵K (G_n)の鍵要求メッセージは、メッセージ認証が付加されていた場合、鍵情報制御装置1の通信機器2Aの機器固有鍵KDを用いて検証される。メッセージ認証コードが付加されていない場合は、通信相手が正当な通信機器2Aではないと判定する。一方、メッセージ認証コードが付加されていた場合は通信機器2Aであることが確認でき、鍵情報制御装置1は、通信機器2Aに最新のグループ鍵K (G₄)を送信するようユニキャスト通信を行う。このとき、鍵情報制御装置1は、再送機能付きユニキャスト通信によって、グループ鍵K (G₄)を送信してもよい。

通信機器2Aは、グループ鍵K (G_n)の鍵要求メッセージに対して、鍵情報制御装置1から最新のグループ鍵K (G₄)を受信すると、鍵暗号化鍵KEKを用いて復号できる。これにより、通信機器2Aは、グループ鍵K (G₃)を、最新のグループ鍵K (G₄)に更新できる。通信機器2Aは、最新のグループ鍵K (G₄)を受信すると、鍵情報制御装置1に対し、ユニキャスト通信によって受信応答を送信する。

また、鍵情報制御装置1は、再送機能付きユニキャスト通信によって、グループ鍵K (G_n)に加えて、最新のEPOCH値を送信してもよい。この場合、通信機器2Aは、グループ鍵K (G₃)をグループ鍵K (G₄)に更新すると共に、記憶しているEPOCH値「2」を、最新のEPOCH値「3」に更新できる。

以上のように、鍵情報更新システムによれば、マルチキャスト通信によって送信し

たグループ鍵 $K(G_n)$ が通信不良によって消失しても、グループ鍵 $K(G_n)$ を送信する通信方式を自動的にマルチキャスト通信から再送機能付きユニキャスト通信に切り替える。

これにより、鍵情報更新システムは、通信機器2によって受信応答を要する再送機能付きユニキャスト通信によってグループ鍵 $K(G_n)$ の鍵要求メッセージを送信することにより、鍵情報制御装置1から最新のグループ鍵 $K(G_n)$ を得ることができる。したがって、この通信機器2によれば、マルチキャスト通信によって最新のグループ鍵 $K(G_n)$ が消失しても、グループ鍵 $K(G_n)$ の更新をより確実に実施することができる。

また、通信機器2は、鍵情報制御装置1又は他の通信機器2から送信された情報に含まれるEPOCH値が、通信機器2（自己）に記憶されたEPOCH値よりも大きい場合に、マルチキャスト通信によって送信したグループ鍵を受信していないことを検出できる。すなわち、通信機器2は、自身のEPOCH値が小さく、自身が保有しているグループ鍵 $K(G_n)$ が古い場合に、鍵更新メッセージを要求することができる。

このように、EPOCH値を参照して、マルチキャスト通信による鍵更新メッセージが消失したことを検出し、再送機能付きユニキャスト通信に切り替えて鍵更新を実施できる。これにより、通信相手に問い合わせることなく確実にグループ鍵を更新でき、かつ、再度認証処理及びシステム全体の鍵更新の処理を行うことなく、グループ鍵を用いたマルチキャスト通信を実施できる。

つぎに、上述した鍵情報更新システムにおいて、通信機器2がグループ鍵 $K(G_n)$ の未受信を検出する他の動作について、図9を参照して説明する。

通信機器2は、最新のグループ鍵 $K(G_3)$ を配布する鍵更新メッセージを受信すると、タイマー部28を起動させる。通信機器2は、所定時間 t を超えてグループ鍵 $K(G_n)$ を含む鍵更新メッセージを受信していない場合に、マルチキャスト通信によってグループ鍵を受信できていないことを検出する。

この場合、通信機器2Aは、鍵情報制御装置1に、再送機能付きユニキャスト通信によって最新のグループ鍵 $K(G_n)$ の送信を要求する（ユニキャスト通信手段）。なお、通常は平文で、新たなグループ鍵の要求メッセージを送る。この平文のメッセージは、{MSG、EPOCH、D_2A}の構成例になる。MSGは要求であることを示す識別子である。EPOCHは通信機器2Aが鍵情報制御装置1から受信したEPOCH値である。D_2Aは通信機器2Aを識別できる識別子またはIDである。

このとき、通信機器2Aは、認証処理及び鍵配布処理P3において配布した鍵暗号化鍵KEKによって、新たなグループ鍵 $K(G_n)$ を要求する鍵要求メッセージにメッセージ認証(MAC)の情報を暗号化して付加してもよい。このメッセージ認証コードの情報は、通信機器2Aであることを証明するための情報である。

このメッセージ認証コード(MAC)を付加した要求は、例えば、{MSG、EP

OCH, D__2A, MAC (KD__2A, MSG, D__2A, EPOCH)} の構成例になる。関数MACは、鍵情報としてKD__2A, メッセージとしてMSG, D__2A, EPOCHを入力値として計算し、MAC値を出力する。このMAC値は、通信機器2Aの機器固有鍵KDが含まれている。このため、機器固有鍵KDが異なると同じMSG, D__2A, EPOCHを入力してもMAC値は一致しない。したがって、MAC値は、通信機器2Aであることを証明する情報となる。MSGは要求であることを示す識別子（文字列も含む）である。EPOCHは、通信機器2Aが鍵情報制御装置1から受信したEPOCH値である。D__2Aは通信機器2Aを識別できる識別子またはノードIDである。

このユニキャスト通信によって送信されたグループ鍵K (Gn) の鍵要求メッセージは、メッセージ認証が付加されていた場合、鍵情報制御装置1の通信機器2Aの機器固有鍵KDを用いて検証される。メッセージ認証コードが付加されていない場合は、通信相手が正当な通信機器2Aではないと判定する。一方、メッセージ認証コードが付加されていた場合は通信機器2Aであることが確認でき、鍵情報制御装置1は、通信機器2Aに最新のグループ鍵K (G4) を送信するようユニキャスト通信を行う。

通信機器2Aは、グループ鍵K (Gn) の鍵要求メッセージに対して、鍵情報制御装置1から最新のグループ鍵K (G4) を受信すると、鍵暗号化鍵KEKを用いて復号できる。これにより、通信機器2Aは、グループ鍵K (G3) を、最新のグループ鍵K (G4) に更新できる。通信機器2Aは、最新のグループ鍵K (G4) を受信すると、鍵情報制御装置1に対し、ユニキャスト通信によって受信応答を送信する。

この鍵情報更新システムによれば、鍵情報制御装置1によってグループ鍵をマルチキャスト通信によって送信する間隔を所定期間とする。一方、通信機器2は、所定期間を超えてグループ鍵を受信していない場合に、マルチキャスト通信によってグループ鍵を受信できていないことを検出する。この鍵情報更新システムによれば、通信機器2によって容易に鍵更新メッセージの通信不良を検出できる。これにより、通信機器2が直ちにグループ鍵を要求でき、通信機器2がマルチキャスト通信の不能な期間を短縮できる。

つぎに、上述した鍵情報更新システムにおいて、鍵情報制御装置1及び通信機器2のそれぞれの内部動作について説明する。

図10は、鍵情報制御装置1の動作手順を示すフローチャートである。この動作は、コンピュータとしての鍵情報制御装置1が、記録媒体としての記憶部11aに記憶された鍵情報制御プログラム11bを実行することによって行われる処理である。

先ずステップS1において、通信部12によって、外部から送信されたメッセージを受信する。

次のステップS2において、制御部11によって、ステップS1にて受信したメッセージが、通信機器2から送信された鍵要求メッセージか否かを判定する。このとき、制御部11は、アドレス情報又はノードIDを参照して、メッセージの送信元の通信

機器2を特定する。また、制御部11は、ノンス値に付加された暗号化データを参照して、受信したメッセージが鍵要求メッセージか否かを判定する。鍵要求メッセージである場合にはステップS3に処理を進め、そうでない場合にはステップS5に処理を進める。

ステップS3において、通信部12は、再送機能付きユニキャスト通信によって、最新のグループ鍵K(G_n)を送信する。このとき、鍵管理部15は、制御部11の制御に従って、鍵管理テーブル15aから最新のグループ鍵K(G_n)を読み出す。また、鍵管理部15は、鍵要求メッセージの送信元の通信機器2に対応した鍵暗号化鍵KEKを読み出し、暗号処理部16によって暗号化させる。

次のステップS4において、通信部12は、ステップS3においてグループ鍵K(G_n)を送信したことに対し、ユニキャスト通信によって、通信機器2から受信応答を受信する。

ステップS5において、通信品質計測部17は、ステップS1にて受信したメッセージに含まれるEPOCH値(受信EPOCH値)が、現在のEPOCH値よりも古いか否かを判定する。このとき、通信品質計測部17は、現在鍵管理テーブル15aに記憶しているEPOCH値と受信EPOCH値との大小関係を比較する。受信EPOCH値が、鍵管理テーブル15aに記憶したEPOCH値よりも小さい場合には、受信EPOCH値が古いのでステップS6に処理を進める。双方のEPOCH値が同じ値である場合にはステップS9に処理を進める。

ステップS6において、制御部11は、ステップS1にて受信したメッセージに含まれるノードID、EPOCH値を含む機器情報を通信品質記憶部18に記録する。

次のステップS7において、通信部12は、ユニキャスト通信によって、グループ鍵K(G_n)を更新する鍵更新メッセージを送信する。このとき、制御部11の制御に従って、鍵管理部15は鍵管理テーブル15aから最新のグループ鍵K(G_n)を読み出す。暗号処理部16は、制御部11の制御に従って、グループ鍵K(G_n)を、鍵暗号化鍵KEKによって暗号化する。通信部12は、暗号化されたグループ鍵K(G_n)を含みメッセージ送信元機器のノードIDを含む鍵更新メッセージを送信する。

このユニキャスト通信のポート番号Bは、マルチキャスト通信によって使用するポート番号Aとは異なる値を使用することが望ましい。

次のステップS8において、通信部12は、ステップS7において送信した鍵更新メッセージに対する受信応答をユニキャスト通信によって受信する。

ステップS9において、暗号処理部16は、ステップS1にて受信したメッセージを、最新のグループ鍵K(G_n)によって復号する。

ステップS10において、制御部11は、ステップS9にて復号されたメッセージに従って各種の処理を行う。

ステップS11において、制御部11は、ノンス値に含まれるカウンタ値が閾値以上であるか否かを判定する。この閾値は、予め設定された値であり、例えばカウンタ

値の割当ビット量に応じた $2^3 - 1$ 等の値が設定されている。カウンタ値が閾値以上である場合にはステップS 1 2に処理を進め、そうでない場合には処理を終了する。

ステップS 1 2において、通信部 1 2は、全ての通信機器 2のグループ鍵 $K(G_n)$ を最新にするために、最新のグループ鍵 $K(G_n)$ を含む鍵更新メッセージを送信する。この鍵更新メッセージは、鍵管理部 1 5が導出した最新のグループ鍵 $K(G_n)$ を鍵暗号化鍵 K_{EK} によって暗号化した値を含む。このとき、通信部 1 2は、マルチキャスト通信方式によって、鍵更新メッセージを送信する。

通信部 1 2は、マルチキャスト通信（マルチキャスト通信手段）によって使用するポート番号Aを、ユニキャスト通信（ユニキャスト通信手段）によって使用するポート番号Bとは異なる値としてもよい。

次のステップS 1 3において、制御部 1 1は、通信機器 2のうち、保証モードとなっている通信機器 2があるか否かを判定する。保証モードとなっている通信機器 2がある場合にはステップS 1 4に処理を進め、ない場合には処理を終了する。なお、この保証モードについては後述する。

ステップS 1 4において、通信部 1 2は、再送機能付きユニキャスト通信によって、通信機器 2に対して鍵更新メッセージを送信する。このとき、通信部 1 2は、マルチキャスト通信において使用するポート番号Aとは異なる値のポート番号Bを使用してもよい。

以上のように、鍵情報制御装置 1は、通信機器 2からの鍵要求メッセージに応じて、ユニキャスト通信によってグループ鍵 $K(G_n)$ を送信できる。また、鍵情報制御装置 1は、受信EPOCH値が篩場合には再送機能付きユニキャスト通信によって通信機器 2に最新のグループ鍵 $K(G_n)$ を送信できる。さらに、鍵情報制御装置 1は、カウンタ値が閾値以上となった場合にマルチキャスト通信によって全ての通信機器 2のグループ鍵 $K(G_n)$ を更新できる。

図 1 1は、通信機器 2の動作手順を示すフローチャートである。この動作は、コンピュータとしての通信機器 2が、制御部 2 1に記憶された鍵情報更新プログラム 2 1 bを実行することによって行われる処理である。

先ずステップS 2 1において、通信部 2 2によって、外部から送信されたメッセージを受信する。

次のステップS 2 2において、制御部 2 1によって、ステップS 2 1にて受信したメッセージが、鍵情報制御装置 1からマルチキャスト通信によって送信された鍵更新メッセージか否かを判定する。このとき、制御部 2 1は、アドレス情報又はノードIDを参照して、メッセージの送信元が鍵情報制御装置 1であるかを特定する。また、制御部 2 1は、ノンス値に付加された暗号化データを参照して、受信したメッセージが鍵更新メッセージか否かを判定する。鍵更新メッセージである場合にはステップS 2 3に処理を進め、そうでない場合にはステップS 2 4に処理を進める。

ステップS 2 3において、制御部 2 1は、ステップS 2 1にて受信した鍵更新メッ

セージを暗号処理部 25 によって復号する。このとき、暗号処理部 25 は、鍵管理テーブル 24 a に記憶された鍵暗号化鍵 K E K を用いて鍵更新メッセージを復号して、最新のグループ鍵 K (G n) を得る。鍵管理部 24 は、鍵管理テーブル 24 a に記憶している最新のグループ鍵 K (G n) を、鍵更新メッセージから取り出したグループ鍵 K (G n) に更新する。

ステップ S 24 において、通信品質計測部 26 は、ステップ S 21 にて受信したメッセージに含まれる EPOCH 値 (受信 EPOCH 値) が、現在の EPOCH 値よりも新しいか否かを判定する。このとき、通信品質計測部 26 は、現在鍵管理テーブル 24 a に記憶している EPOCH 値と受信 EPOCH 値との大小関係を比較する。受信 EPOCH 値が、鍵管理テーブル 24 a に記憶した EPOCH 値よりも大きい場合には、受信 EPOCH 値が新しいのでステップ S 25 に処理を進める。双方の EPOCH 値が同じ値である場合にはステップ S 29 に処理を進める。

ステップ S 25 において、制御部 21 は、ステップ S 21 にて受信したメッセージを一時的に保存する。

次のステップ S 26 において、通信部 22 は、最新のグループ鍵 K (G n) を要求する鍵要求メッセージを送信する。このとき、通信部 22 は、ユニキャスト通信によって、機器固有鍵 K D によるメッセージ認証を付加した鍵要求メッセージを送信する。

次のステップ S 27 において、通信部 22 は、ステップ S 26 にて送信した鍵要求メッセージに対し、ユニキャスト通信によって鍵情報制御装置 1 から送信された鍵更新メッセージを受信する。このとき、鍵更新メッセージのポート番号 B が、マルチキャスト通信によって使用されているポート番号 A と異なってもよい。この場合、通信部 22 は、ユニキャスト通信に対応するポート番号 B によって受信を行う。

ステップ S 28 において、制御部 21 は、ステップ S 27 にて受信した鍵更新メッセージを暗号処理部 25 によって復号する。このとき、暗号処理部 25 は、鍵管理テーブル 24 a に記憶された鍵暗号化鍵 K E K を用いて鍵更新メッセージを復号して、最新のグループ鍵 K (G n) を得る。鍵管理部 24 は、鍵管理テーブル 24 a に記憶している最新のグループ鍵 K (G n) を、鍵更新メッセージから取り出したグループ鍵 K (G n) に更新する。

次のステップ S 29 において、暗号処理部 16 は、ステップ S 28 にて更新された最新のグループ鍵 K (G n) を用いて、ステップ S 25 で一時的に保存したメッセージを復号する。

次のステップ S 30 において、通信部 22 は、ステップ S 21 にて受信したメッセージに応じ、各種のマルチキャスト通信処理を行う。

以上のように、通信機器 2 は、鍵情報制御装置 1 からマルチキャスト通信によって鍵更新メッセージが送信された場合にはグループ鍵 K (G n) を更新できる。また、通信機器 2 は、受信 EPOCH 値が新しい場合には、ユニキャスト通信によって鍵要求メッセージを送信し、ユニキャスト通信によって最新のグループ鍵 K (G n) を受

信してグループ鍵 $K(G_n)$ を更新できる。さらに、通信機器2は、例えば最新のグループ鍵 $K(G_n)$ を保持していなくても一時的にメッセージを保存しておき、最新のグループ鍵 $K(G_n)$ を取得して復号できる。

さらに、上述した鍵情報更新システムにおいて、鍵情報制御装置1及び通信機器2は、マルチキャスト通信に使用するポート番号とユニキャスト通信に使用するポート番号とを異なる値を割り当てる。これにより、鍵情報制御装置1及び通信機器2から送信するメッセージに、当該メッセージを暗号化した鍵を記述する必要がなくなる。また、グループ鍵 $K(G_n)$ のカウント値とは別に、鍵暗号化鍵 KEK のカウント値を管理でき、グループ鍵 $K(G_n)$ を更新する管理を容易にすることができる。

つぎに、上述した鍵情報更新システムにおいて、通信機器2の通信不良が所定の閾値を超えたことを判定する処理について説明する。

図12に、通信機器2Aによってグループ鍵 $K(G_1)$ を用いた暗号化データ通信のシーケンス図を示す。この例において、通信機器2Aが通信を開始する時には、鍵情報制御装置1及び全ての通信機器2との間で認証処理及び初期のグループ鍵 $K(G_1)$ は共有できているとする。

通信機器2Aは、カウント値が最大値となるまでマルチキャスト通信を繰り返す。この例では、ノンス値が $Nonce=\{0, 1, 1\}$ 、 $Nonce=\{0, 1, 2\}$ 、 $Nonce=\{0, 1, 5\}$ のメッセージは通信機器2B、2C、鍵情報制御装置1に到達する前に消失している。一方、ノンス値が $Nonce=\{0, 1, 0\}$ 、 $Nonce=\{0, 1, 3\}$ 、 $Nonce=\{0, 1, 4\}$ 、 $Nonce=\{0, 1, 6\}$ のメッセージは通信機器2B、2C及び鍵情報制御装置1に到達している。

このようなシーケンスが行われる鍵情報更新システムにおいて、鍵情報制御装置1は、通信機器2ごとに、カウント値を用いて通信不良を判定する。

鍵情報制御装置1は、グループ鍵 $K(G_n)$ の更新タイミングとなると、マルチキャスト通信によって、鍵更新メッセージを送信する。図12の例では、グループ鍵 $K(G_n)$ が $K(G_2)$ 、 $K(G_3)$ 、 $K(G_4)$ 、 $K(G_5)$ と更新するごとに、鍵更新メッセージを配信する。各鍵更新メッセージのEPOCH値は、 $K(G_2)$ 、 $K(G_3)$ 、 $K(G_4)$ 、 $K(G_5)$ と更新するごとに、1、2、3、4と増加する。

このような通信シーケンスにおいて、EPOCH値が0、1、4の鍵更新メッセージは通信機器2Aに受信されている。これにより、通信機器2Aは、EPOCH値が0、1、4に対応したグループ鍵 $K(G_1)$ 、 $K(G_2)$ 、グループ鍵 $K(G_5)$ を用いたマルチキャスト通信を行って鍵情報制御装置1と通信できる。一方、EPOCH値が2、3、の鍵更新メッセージは通信機器2Aに到達する前に消失している。したがって、通信機器2Aは、EPOCH値が2、3に対応したグループ鍵 $K(G_3)$ 、 $K(G_4)$ を用いたマルチキャスト通信は行えない。

このようなシーケンスが行われる鍵情報更新システムにおいて、鍵情報制御装置1は、通信機器2ごとに、EPOCH値を用いて通信不良を判定する。

鍵情報制御装置1は、カウント値又はEPOCH値を用いて通信機器2ごとの通信

不良を判定する。鍵情報制御装置 1 は、図 1 2 のような通信シーケンスにおいて、通信機器 2 A の通信不良を判定する。

この場合、鍵情報制御装置 1 は、図 1 3 に示すように、通信機器 2 A に対し、マルチキャスト通信によってグループ鍵 $K(G_n)$ を送信する度にユニキャスト通信によって通信機器 2 A にグループ鍵 $K(G_n)$ を送信する。

このような鍵情報更新システムにおける鍵情報制御装置 1 の動作を図 1 4 に示す。

まず、ステップ S 4 1 において、制御部 1 1 は、タイマー部 1 9 を制御して、通信不良判定のためのタイマー値としての所定時間 t を設定する。

次のステップ S 4 2 において、タイマー部 1 9 は、起動して計時を行うタイマー処理を行う。

次のステップ S 4 3 において、制御部 1 1 は、タイマー部 1 9 により計時しているタイマー値が所定時間 t に達して満了したか否かを判定する。タイマー値が満了した場合にはステップ S 4 4 に処理を進め、そうでない場合にはステップ S 4 2 のタイマー処理を継続する。

このタイマー処理を継続している所定時間 t において、鍵情報制御装置 1 は、通信品質記憶部 1 8 によって通信機器 2 から送信されたメッセージにおけるカウンタ値を蓄積する。又は、鍵情報制御装置 1 は、通信機器 2 から送信されたメッセージに含まれる EPOCH 値を蓄積する。

ステップ S 4 4 において、通信品質計測部 1 7 は、通信機器 2 ごとに、所定時間 t における未受信回数を集計する。

未受信検出手段としての通信品質計測部 1 7 は、通信品質記憶部 1 8 に蓄積された通信機器 2 ごとのメッセージにおけるカウンタ値を参照する。通信品質計測部 1 7 は、カウンタ値における抜けを検出する。これにより通信品質計測部 1 7 は、通信機器 2 ごとに所定時間 t における通信機器 2 から送信されたメッセージの未受信回数を計測する。

又は、通信品質検出手段としての通信品質計測部 1 7 は、通信品質記憶部 1 8 に蓄積された通信機器 2 ごとのメッセージにおける EPOCH 値を参照する。通信品質計測部 1 7 は、EPOCH 値における抜けを検出する。これにより通信品質計測部 1 7 は、通信機器 2 ごとに所定時間 t における通信機器 2 によるグループ鍵 $K(G_n)$ の未受信回数を計測する。

次のステップ S 4 5 において、制御部 1 1 は、ステップ S 4 4 において集計された未受信回数が所定の閾値より大きい通信機器 2 があるか否かを判定する。未受信回数が閾値よりも大きい通信機器 2 がある場合にはステップ S 4 6 に処理を進め、ない場合にはステップ S 4 7 に処理を進める。

ステップ S 4 6 において、制御部 1 1 は、未受信回数が閾値よりも大きいことに該当した通信機器 2 を保証モードに設定する。この保証モードは、図 1 3 に示したように、通信機器 2 が閾値以上の通信不良を発生させた場合、マルチキャスト通信と併用

し、当該マルチキャスト通信によって送信したメッセージを再送付きユニキャスト通信によって送信する動作モードである。

ステップS 47において、制御部11は、未受信回数が閾値よりも大きくことに該当しない通信機器2を通常モードに設定する。この通常モードは、上述したようにマルチキャスト通信のみを行う動作モードである。

このような鍵情報制御装置1は、通信品質記憶部18によって、通信機器2ごとに、所定時間 t [分]に受信したカウンタ値を蓄積する。図12に示した通信シーケンスの場合、通信品質記憶部18は、通信機器2Aに対応して、カウンタ値としての0、3、4、6を蓄積する。

通信品質計測部17は、所定時間 t が経過すると、通信品質記憶部18に蓄積したカウンタ値を参照して、鍵情報制御装置1に未達のメッセージを検出する。図12の場合、通信品質計測部17は、カウンタ値1、2、5のメッセージが通信機器2Aに送信されたが、鍵情報制御装置1には未達（未受信）であることを検出する。これにより、制御部11は、所定時間 t 中に、7回中、3回が未受信回数であったと判定する。

制御部11は、メッセージの未受信回数と予め設定した閾値（例えば2回）とを比較する。メッセージの未受信回数が閾値を超えているので、制御部11は、通信機器2Aの動作モードを保証モードに設定する。これにより、制御部11は、図13に示したように、通信機器2Aに対するマルチキャスト通信によってメッセージを送信し、さらに、再送付きユニキャスト通信によってメッセージを送信する。

同様に、鍵情報制御装置1は、通信品質記憶部18によって、通信機器2ごとに、所定時間 t [分]に受信したEPOCH値を蓄積する。図12に示した通信シーケンスの場合、通信品質記憶部18は、通信機器2Aに対応して、EPOCH値としての0、1、4を蓄積する。

通信品質計測部17は、所定時間 t が経過すると、通信品質記憶部18に蓄積したEPOCH値を参照して、通信機器2Aに未達の鍵更新メッセージを検出する。図12の場合、通信品質計測部17は、EPOCH値が2、3の鍵更新メッセージが通信機器2Aには未達（未受信）であることを検出する。これにより、制御部11は、所定時間 t 中に、4回中、2回が未受信回数であったと判定する。

制御部11は、メッセージの未受信回数と予め設定した閾値（例えば2回）とを比較する。メッセージの未受信回数が閾値を超えているので、制御部11は、通信機器2Aの動作モードを保証モードに設定する。これにより、制御部11は、図13に示したように、通信機器2Aに対するマルチキャスト通信によってメッセージを送信し、さらに、再送付きユニキャスト通信によってメッセージを送信する。

以上のように、この鍵情報更新システムによれば、通信不良であることが判定された通信機器2についての動作モードを保証モードに設定する。これにより、鍵情報制御装置1は、マルチキャスト通信に加えて、再送付きユニキャスト通信によってメッ

セージを通信機器 2 に送信できる。これにより、鍵情報更新システムは、不安定な通信路にある通信機器 2 にマルチキャスト通信によって送信する鍵更新メッセージを確実に受信させることができる。

さらに、上述した鍵情報更新システムにおいて、鍵情報制御装置 1 は、不安定な通信路を検出した場合に、当該不安定な通信路にある通信機器 2 又は他の通信機器 2 に通知を行ってもよい（通信手段）。

例えば、図 15 に示すように、全ての通信機器 2 にグループ鍵 K（G 3）を配布してデータ通信処理 P 4 を行った後、通信機器 2 A の通信不良が発生したとする。この場合、鍵情報制御装置 1 は、上述したように、マルチキャスト通信によって鍵要求メッセージを送信し、さらに、ユニキャスト通信によって鍵要求メッセージを送信する。

この場合、鍵情報制御装置 1 は、制御部 11 の制御によって、不安定な通信路を通知する。制御部 11 は、不安定な通信路にある通信機器 2 A、通信機器 2 A と通信を行う通信機器 2 B、2 C に通知を行う。このとき、制御部 11 は、認証処理及び鍵配布処理 P 1、P 2、P 3 によって認証が許可された通信機器 2 の情報に基づいて通知を行う。

このような鍵情報制御装置 1 によれば、不安定な通信路にある通信機器 2 を通知することにより、不安定な通信路にある通信機器 2 によって、マルチキャスト通信に加えて、再送機能付きユニキャスト通信によってメッセージを送信する設定に変更できる。また、鍵情報制御装置 1 によれば、任意の通信機器 2 が不安定な通信路にある通信機器 2 と通信を行う場合に、マルチキャスト通信に加えて、再送機能付きユニキャスト通信によってメッセージを送信する設定に変更できる。これにより、この鍵情報更新システムによれば、メッセージを確実に通信相手に受信させることができる。

さらに、上述した鍵情報更新システムにおいて、鍵情報制御装置 1 は、グループ鍵 K（G n）をマルチキャスト通信によって送信する間隔を所定期間とする。これに対し、通信機器 2 は、所定期間を超えてグループ鍵 K（G n）を受信していない場合に、マルチキャスト通信によってグループ鍵 K（G n）を受信できていないことを検出する。

このような鍵情報更新システムにおいて、鍵情報制御装置 1 は、図 16 に示すような処理手順によって動作する。

まず、ステップ S 5 1 において、鍵情報制御装置 1 は、タイマー部 19 によってグループ鍵 K（G n）を更新するためのタイマー設定を行う。このとき、制御部 11 は、鍵要求メッセージを送信する所定期間を設定する。

次のステップ S 5 2 において、タイマー部 19 は、ステップ S 5 1 にて設定された所定期間を計時する。

次のステップ S 5 3 において、制御部 11 は、タイマー部 19 により計時しているタイマー値が所定時間に達して満了したか否かを判定する。タイマー値が満了した場合にはステップ S 5 4 に処理を進め、そうでない場合にはステップ S 5 2 のタイマー

処理を継続する。

ステップS54において、通信部12は、制御部11の制御に従って、暗号処理部16によって導出した最新のグループ鍵 $K(G_n)$ のための鍵更新メッセージをマルチキャスト通信によって送信する。

鍵更新メッセージは、所定期間ごとに鍵情報制御装置1から送信される。これにより、通信機器2は、タイマー部28によって所定期間を計時し、所定期間を超えて鍵更新メッセージを受信していない場合に通信不良を検出できる。通信機器2は、通信不良を検出した場合に、鍵情報制御装置1に鍵要求メッセージを送信することができる。

なお、この実施形態では、タイマー部19及びタイマー部28によって所定期間を計時したが、これに限らず、鍵更新メッセージを周期的に送信する時刻を設定してもよい。

この鍵情報更新システムによれば、タイマー又は時刻を用いて周期的に鍵更新メッセージの送信を実施するので、通信機器2によって容易に通信不良を検出できる。そして、通信機器2によって通信不良を検出した直後に鍵要求メッセージを送信できる。したがって、この鍵情報更新システムによれば、通信不良の通信機器2が新たなグループ鍵 $K(G_n)$ を用いて通信を再開するための期間を短縮できる。

さらに、上述した鍵情報更新システムは、認証処理及び鍵配布処理において、鍵暗号化鍵 KEK に加えて、リカバリー鍵を鍵情報制御装置1及び全ての通信機器2に配布してもよい。このリカバリー鍵は、通信機器2が通信不良となった場合に一時的に通信を行うために使用される。

この鍵情報更新システムにおいて、認証処理及び鍵配布処理P1、P2、P3では、鍵情報制御装置1は、グループ鍵 $K(G_n)$ とは異なり、鍵情報制御装置1と複数の通信機器2とを含むネットワークにおいて使用されるリカバリー鍵を生成する。なお、このリカバリー鍵は、グループ鍵 $K(G_0)$ またはグループ鍵 $K(G(nの最大値))$ を生成してリカバリー鍵としてもよい。このとき、グループ鍵 $K(G_0)$ をリカバリー鍵とした場合は、グループ鍵はグループ鍵 $K(G_1)$ から使用する。グループ鍵 $K(G(nの最大値))$ とした場合は、グループ鍵はグループ鍵 $K(G_0)$ から使用することとしても良い。次に、鍵情報制御装置1は、鍵情報制御装置1と通信機器2との間で認証処理を行った後に、リカバリー鍵を配布する。

その後、鍵情報更新システムは、鍵情報制御装置1からマルチキャスト通信によって新たなグループ鍵 $K(G_n)$ を通信機器2に送信する。これにより、鍵情報更新システムは、鍵情報制御装置1から送信されたグループ鍵 $K(G_n)$ に、通信機器2のグループ鍵 $K(G_n)$ を更新する。これにより、鍵情報更新システムは、鍵情報制御装置1及び全ての通信機器2に対し、グループ鍵 $K(G_n)$ を設定する。なお、この時に、リカバリー鍵を設定してもよい。

鍵情報制御装置1は、リカバリー鍵を用いて、通信機器2と暗号化通信を行う。例

例えば図 17 に示すように、鍵更新処理 P5 において、最新のグループ鍵 K (Gn) をグループ鍵 K (G4) に更新する鍵更新メッセージを送信する。このとき、通信機器 2A、2B が通信不良によって鍵更新メッセージが受信できなかったとする。この場合、鍵情報制御装置 1 は、上述したように、通信機器 2A、2B から送信された EPOCH 値を参照して、更新されたグループ鍵 K (G4) を受信していないことを検出できる。

このとき、鍵情報制御装置 1 は、リカバリー鍵を用いて暗号化したグループ鍵 K (G4) を送信する。この場合、鍵情報制御装置 1 は、1 つのリカバリー鍵によって暗号化した鍵更新メッセージを、通信機器 2A、2B の双方に再送機能付きユニキャスト通信によって送信する。

したがって、この鍵情報更新システムによれば、通信不能となった通信機器 2 が複数存在する場合であっても、1 つのリカバリー鍵によって複数の通信機器 2 に再送機能付きユニキャスト通信によって鍵更新メッセージを送信できる。これにより、新しいグループ鍵 K (Gn) を容易に特定の通信機器 2 のみに再度配布できる。すなわち、全ての通信機器 2 のグループ鍵 K (Gn) を更新する必要が無く、最小限の通信で新たなグループ鍵 K (Gn) に更新できる。

通信機器 2 は、リカバリー鍵を用いて鍵情報制御装置 1 及び他の通信機器 2 と暗号化通信を行う。例えば図 18 に示すように、通信機器 2A が鍵情報制御装置 1 から送信されたマルチキャスト通信の鍵更新メッセージ (K (G4)) を受信できなかったとする。この状況において、緊急に、通信機器 2A が他の通信機器 2、鍵情報制御装置 1 にメッセージを送信する必要が発生したとする。

この場合、通信機器 2A は、マルチキャスト通信によって古いグループ鍵 K (G3) で暗号化したメッセージを送信しても、受信応答を得ることができない。そこで、通信機器 2A は、リカバリー鍵を用いてメッセージを暗号化して、他の通信機器 2 及び鍵情報制御装置 1 に再送機能付きユニキャスト通信を行う。

これにより、通信機器 2A は、緊急性が高いメッセージをマルチキャスト通信によって送信できない場合であっても、リカバリー鍵によって暗号化して他の通信機器 2 及び鍵情報制御装置 1 にメッセージを送信できる。

なお、上述の実施の形態は本発明の一例である。このため、本発明は、上述の実施形態に限定されることはなく、この実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。

特許請求の範囲

【請求項 1】

複数の通信機器を含むネットワークにおいて使用されるグループ鍵を制御する鍵情報制御装置であって、

前記グループ鍵が更新される度に鍵識別子を変更し、前記鍵識別子及び新たなグループ鍵を生成する鍵管理手段と、

前記鍵管理手段により生成された前記鍵識別子及び前記グループ鍵をマルチキャスト通信によって送信するマルチキャスト通信手段と、

前記通信機器から送信された情報のうち前記鍵識別子を参照して、前記グループ鍵を受信していない前記通信機器を検出する通信品質検出手段と、

前記通信品質検出手段により前記グループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器に、再送機能付きユニキャスト通信によって前記グループ鍵を送信するユニキャスト通信手段と

を備える鍵情報制御装置。

【請求項 2】

前記鍵管理手段は、新たなグループ鍵に変更する度に前記鍵識別子の値を大きく変更し、

前記通信品質検出手段は、前記通信機器から送信された情報に含まれる鍵識別子が、前記鍵管理手段により変更された鍵識別子よりも小さい場合に、前記マルチキャスト通信によって送信したグループ鍵を受信していないことを検出すること

を特徴とする請求項 1 に記載の鍵情報制御装置。

【請求項 3】

前記マルチキャスト通信手段によって使用するポート番号と、前記ユニキャスト通信手段によって使用するポート番号とで異なる値を割り当てることを特徴とする請求項 1 又は請求項 2 に記載の鍵情報制御装置。

【請求項 4】

前記ユニキャスト通信手段は、前記グループ鍵に加えて、前記鍵管理手段が生成した最新の鍵識別子を送信することを特徴とする請求項 1 乃至請求項 3 の何れか一項に記載の鍵情報制御装置。

【請求項 5】

前記通信品質検出手段は、前記通信機器ごとに、所定期間における前記通信機器から送信されたメッセージの未受信回数又は所定期間における前記通信機器による前記グループ鍵の未受信回数をカウントし、

前記ユニキャスト通信手段は、前記通信品質検出手段によりカウントした未受信回数が所定の閾値を超えた場合に、当該未受信回数の通信機器に対し、前記マルチキャスト通信手段によって送信するグループ鍵を受信していないことを検出すること

スト通信によって前記グループ鍵を送信する度にユニキャスト通信によって前記グループ鍵を送信すること

を特徴とする請求項 1 乃至請求項 4 の何れか一項に記載の鍵情報制御装置。

【請求項 6】

前記通信品質検出手段によりグループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器又は他の通信機器に通知を行う通知手段を有することを特徴とする請求項 1 乃至請求項 5 の何れか一項に記載の鍵情報制御装置。

【請求項 7】

複数の通信機器を含むネットワークにおいて使用されるグループ鍵を制御する鍵情報制御プログラムであって、

コンピュータを、

前記グループ鍵が更新される度に鍵識別子を変更し、前記鍵識別子及び新たなグループ鍵を生成する鍵管理手段、

前記鍵管理手段により生成された前記鍵識別子及び前記グループ鍵をマルチキャスト通信によって送信するマルチキャスト通信手段、

前記通信機器から送信された情報のうち前記鍵識別子を参照して、前記グループ鍵を受信していない前記通信機器を検出する通信品質検出手段、

前記通信品質検出手段により前記グループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器に、再送機能付きユニキャスト通信によって前記グループ鍵を送信するユニキャスト通信手段、

として機能させる鍵情報制御プログラム。

【請求項 8】

複数の通信機器を含むネットワークにおいて使用されるグループ鍵を制御する鍵情報制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記コンピュータを、

前記グループ鍵が更新される度に鍵識別子を変更し、前記鍵識別子及び新たなグループ鍵を生成する鍵管理手段、

前記鍵管理手段により生成された前記鍵識別子及び前記グループ鍵をマルチキャスト通信によって送信するマルチキャスト通信手段、

前記通信機器から送信された情報のうち前記鍵識別子を参照して、前記グループ鍵を受信していない前記通信機器を検出する通信品質検出手段、

前記通信品質検出手段により前記グループ鍵を受信していない前記通信機器が検出された場合に、当該通信機器に、再送機能付きユニキャスト通信によって前記グループ鍵を送信するユニキャスト通信手段、

として機能させる鍵情報制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 9】

鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新装置であって、

前記グループ鍵を、前記鍵情報制御装置からマルチキャスト通信によって受信されたグループ鍵に更新する鍵管理手段と、

前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段と、

他の通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているかいないかを検出する通信品質検出手段と、

前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵を要求するユニキャスト通信手段と

を備える鍵情報更新装置。

【請求項 10】

前記通信品質検出手段は、前記鍵情報制御装置又は前記他の通信機器から送信された情報に含まれる鍵識別子が、自己に記憶された鍵識別子よりも大きい場合に、前記マルチキャスト通信によって送信したグループ鍵を受信していないことを検出することを特徴とする請求項 9 に記載の鍵情報更新装置。

【請求項 11】

鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新プログラムであって、

コンピュータを、

前記グループ鍵を、前記情報制御装置からマルチキャスト通信によって受信されたグループ鍵に更新する鍵管理手段、

前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段、

他の通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているか否かを検出する通信品質検出手段、

前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵を要求するユニキャスト通信手段

として機能させる鍵情報更新プログラム。

【請求項 12】

鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

コンピュータを、

前記グループ鍵を、前記鍵情報制御装置からマルチキャスト通信によって受信されたグループ鍵に更新する鍵管理手段、

前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段、

他の通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているか否かを検出する通信品質検出手段、

前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、再送機能付きユニキャスト通信によってグループ鍵を要求するユニキャスト通信手段

として機能させる鍵情報更新プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 13】

鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新方法であって、

前記鍵情報制御装置からマルチキャスト通信によって新たなグループ鍵を送信するステップと、

前記鍵情報制御装置から送信されたグループ鍵に、前記通信機器のグループ鍵を更新するステップと、

前記通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、グループ鍵が更新されているか否かを検出するステップと、

前記グループ鍵が更新されていない前記通信機器が検出された場合に、再送機能付きユニキャスト通信を行ってグループ鍵を前記通信機器によって取得するステップと

を含む鍵情報更新方法。

【請求項 14】

鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を有し、これを更新する鍵情報更新システムであって、

前記通信機器のグループ鍵を、前記鍵情報制御装置から送信されたグループ鍵に更新する鍵管理手段と、

前記鍵管理手段により更新されたグループ鍵を用いてデータを暗号化又は復号化する暗号処理手段と、

前記グループ鍵が更新される度に変更される鍵識別子を自分が持っている鍵識別子と比較して、前記通信機器が前記グループ鍵が更新されているか否かを検出する通信品質検出手段と、

前記通信品質検出手段により前記グループ鍵が更新されていないことが検出された場合に、前記鍵情報制御装置によってグループ鍵を送信する通信方式をマルチキャスト通信から再送機能付きユニキャスト通信に切り替え、再送機能付きユニキャスト通信によって前記通信機器にグループ鍵を送信する通信手段とを備える鍵情報更新システム。

【請求項 15】

前記鍵情報制御装置は、前記グループ鍵をマルチキャスト通信によって送信する間隔を所定期間とし、

前記通信機器は、前記所定期間を超えて前記グループ鍵を受信していない場合に、前記マルチキャスト通信によってグループ鍵を受信できていないことを検出すること

を特徴とする請求項 14 に記載の鍵情報更新システム。

【請求項 16】

鍵情報制御装置と複数の通信機器とを含むネットワークにおいて使用されるグループ鍵を更新する鍵情報更新方法であって、

前記鍵情報制御装置により前記グループ鍵とは異なり、前記鍵情報制御装置と前記複数の通信機器とを含むネットワークにおいて使用されるリカバリー鍵を生成するステップと、

前記鍵情報制御装置により前記鍵情報制御装置と前記通信機器との間で認証処理を行った後に、前記リカバリー鍵を配布するステップと、

前記鍵情報制御装置からマルチキャスト通信によって新たなグループ鍵を送信するステップと、

前記鍵情報制御装置から送信されたグループ鍵に、前記通信機器のグループ鍵を更新するステップと

を含む鍵情報更新方法。

【請求項 17】

前記鍵情報制御装置により、前記鍵情報制御装置が、前記通信機器から送信された情報のうち前記グループ鍵が更新される度に変更される鍵識別子を参照して、グループ鍵を更新していない通信機器を検出するステップと、

前記鍵情報制御装置が、前記グループ鍵を更新していない通信機器が検出された場合に、前記リカバリー鍵を用いて暗号化したグループ鍵を送信するステップと

を含むことを特徴とする請求項 16 に記載の鍵情報更新方法。

【請求項 18】

前記鍵情報制御装置により、前記通信機器が、前記グループ鍵によってメッセージが送信できない場合に、前記リカバリー鍵を用いて暗号化したメッセージを送信するステップ

を含むことを特徴とする請求項 16 に記載の鍵情報更新方法。

図 1

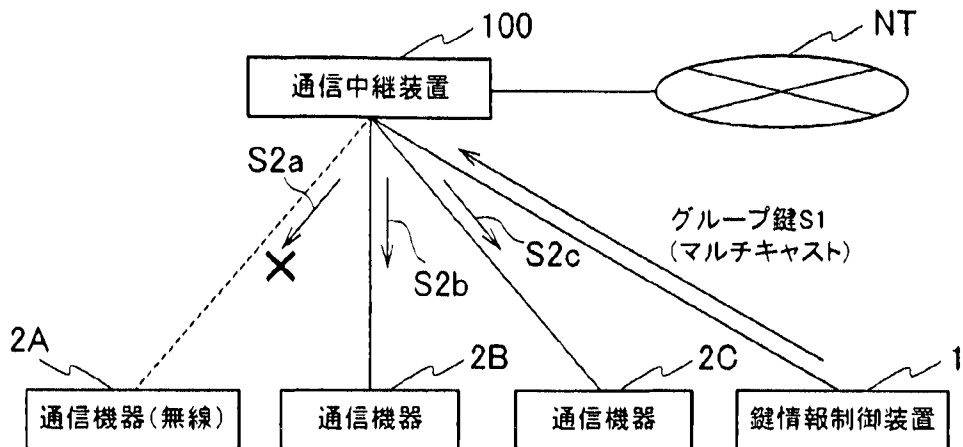


図 2

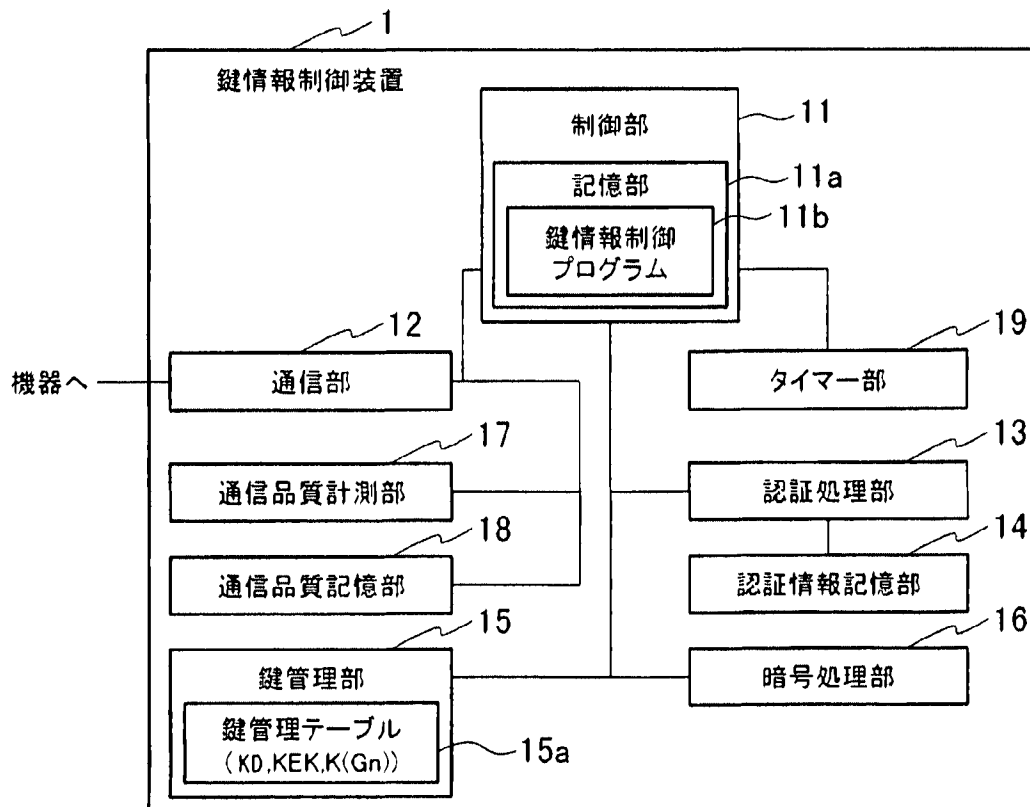


図 3

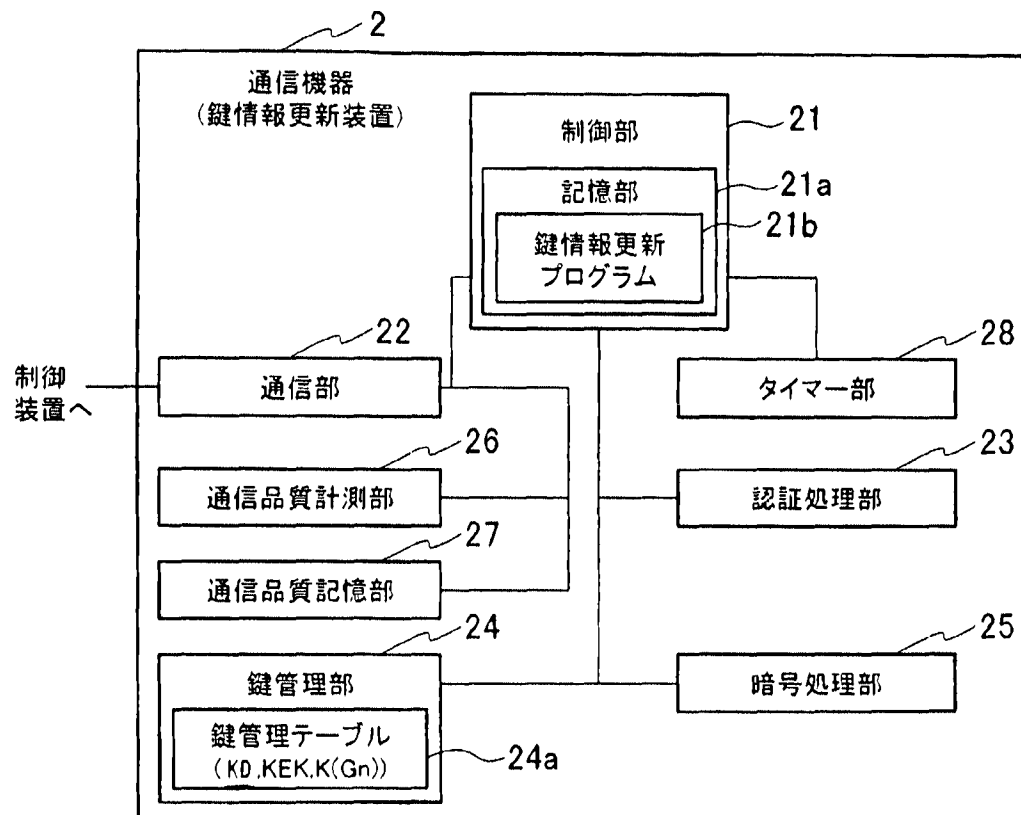
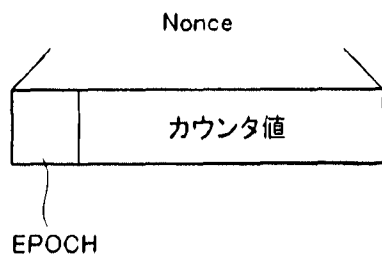


図 4

(a)



(b)

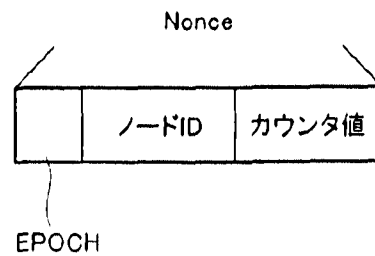


図 5

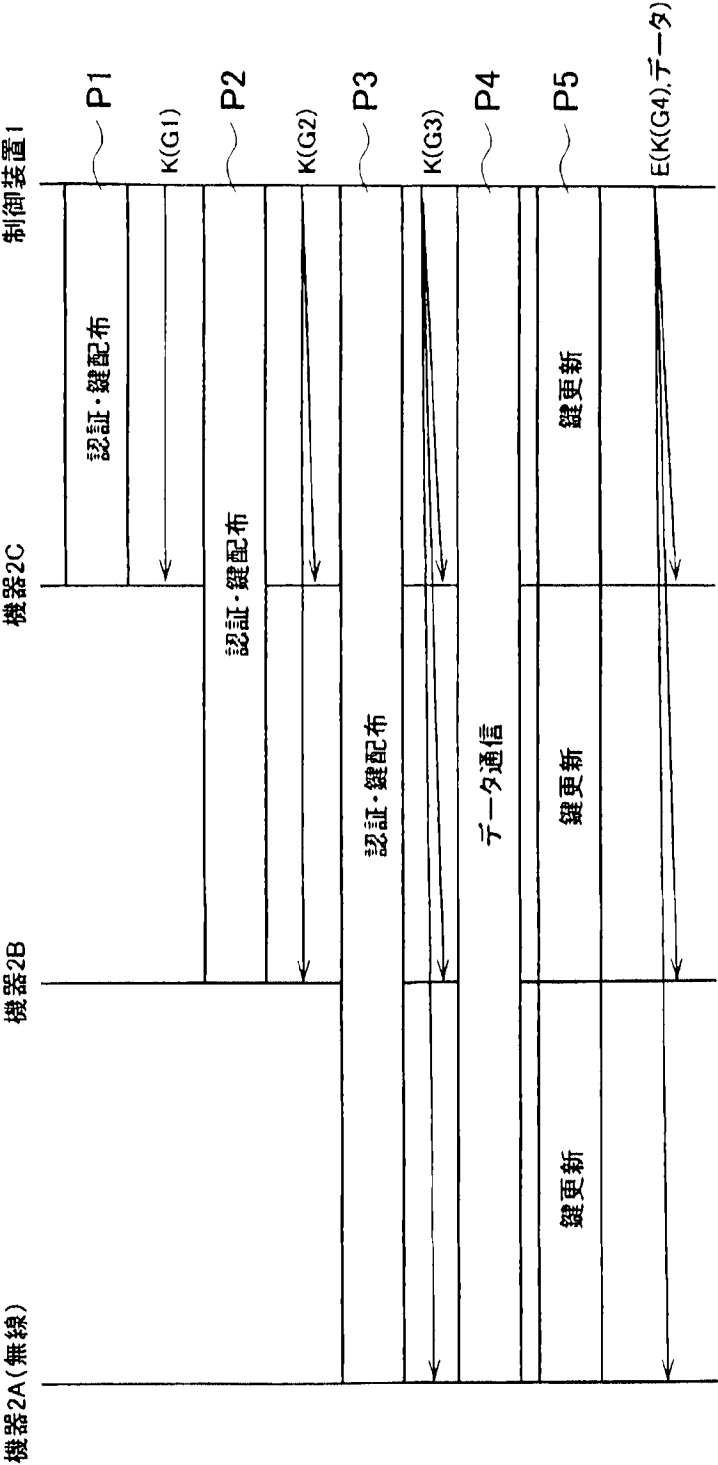


図 6

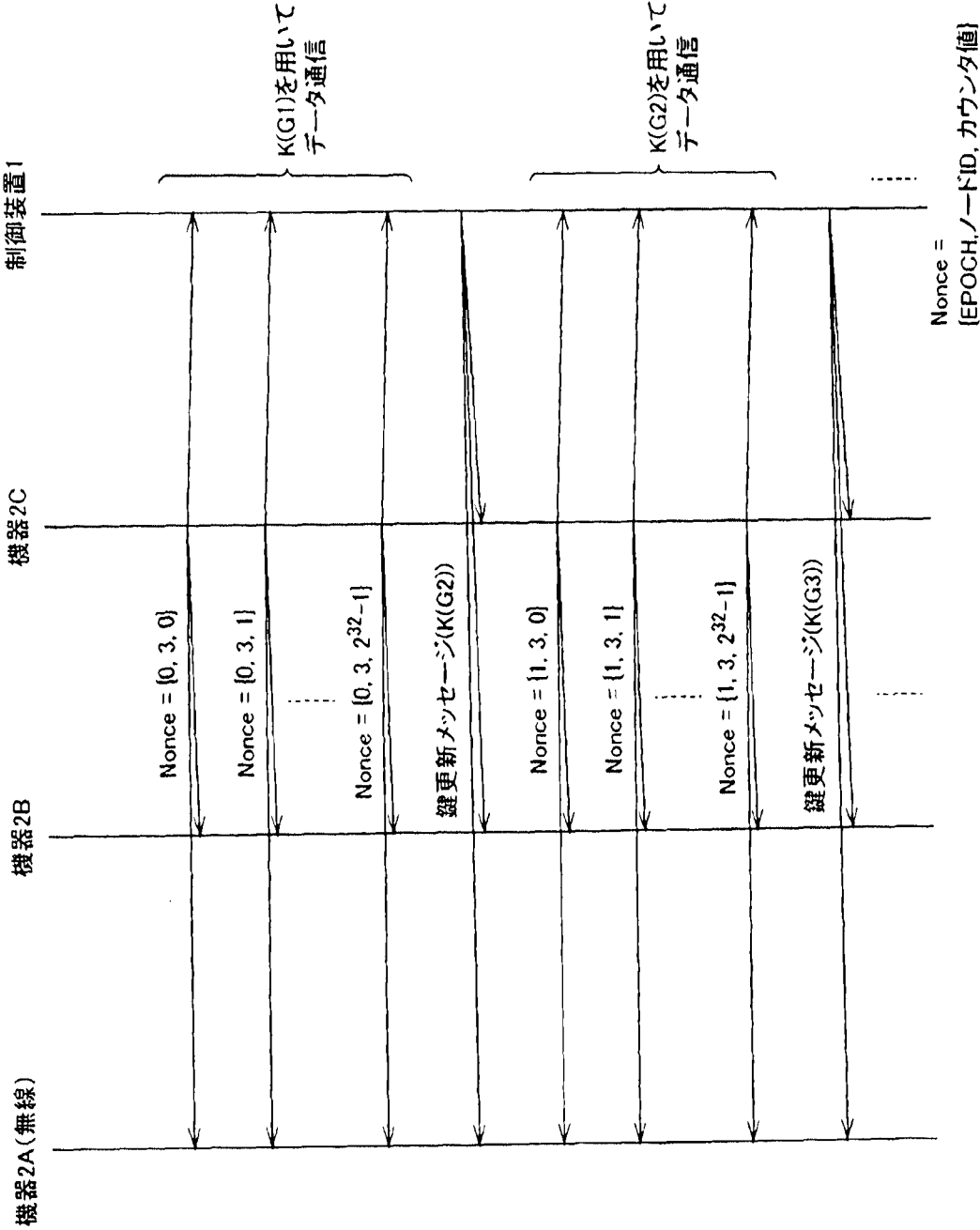


図 7

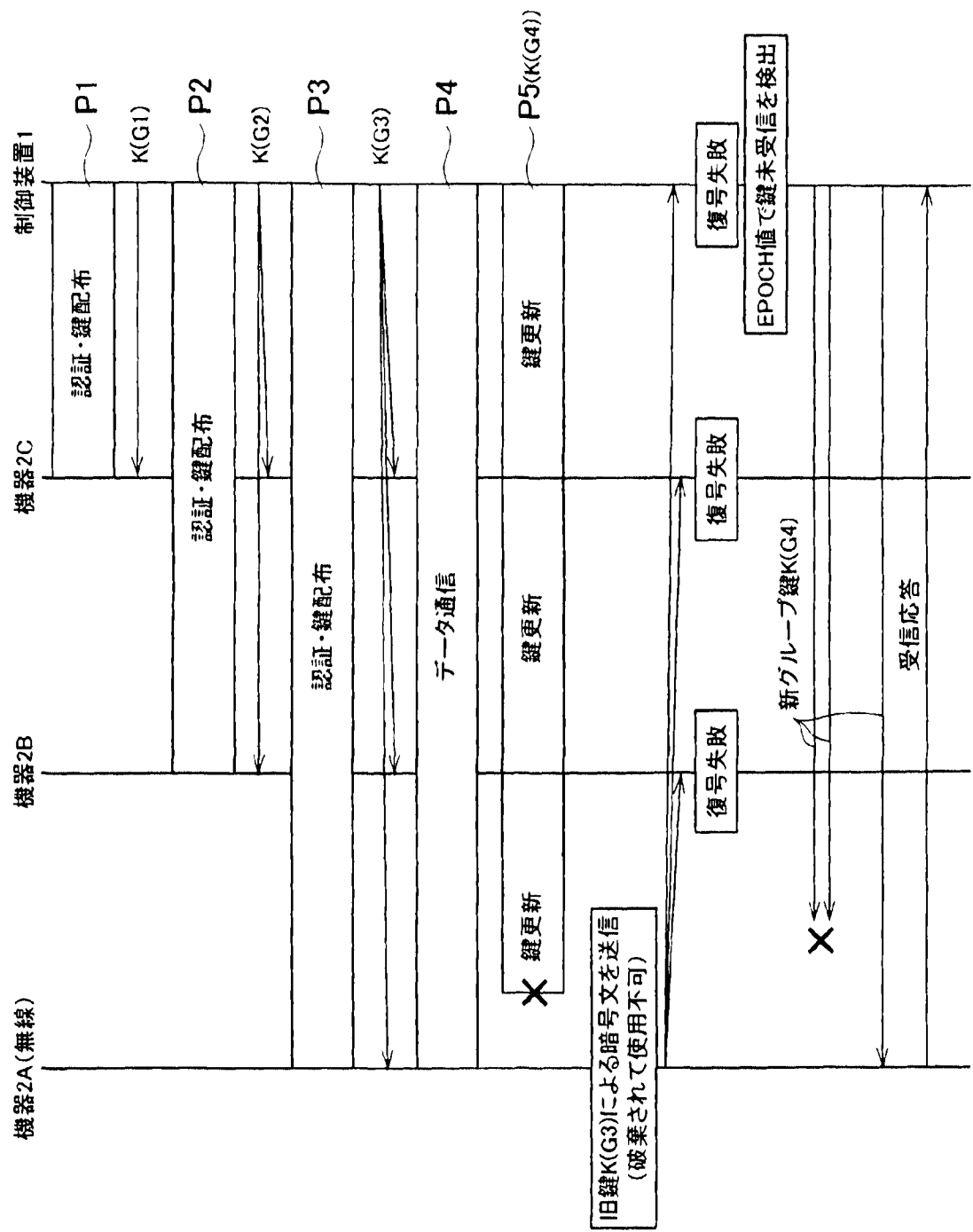


図 8

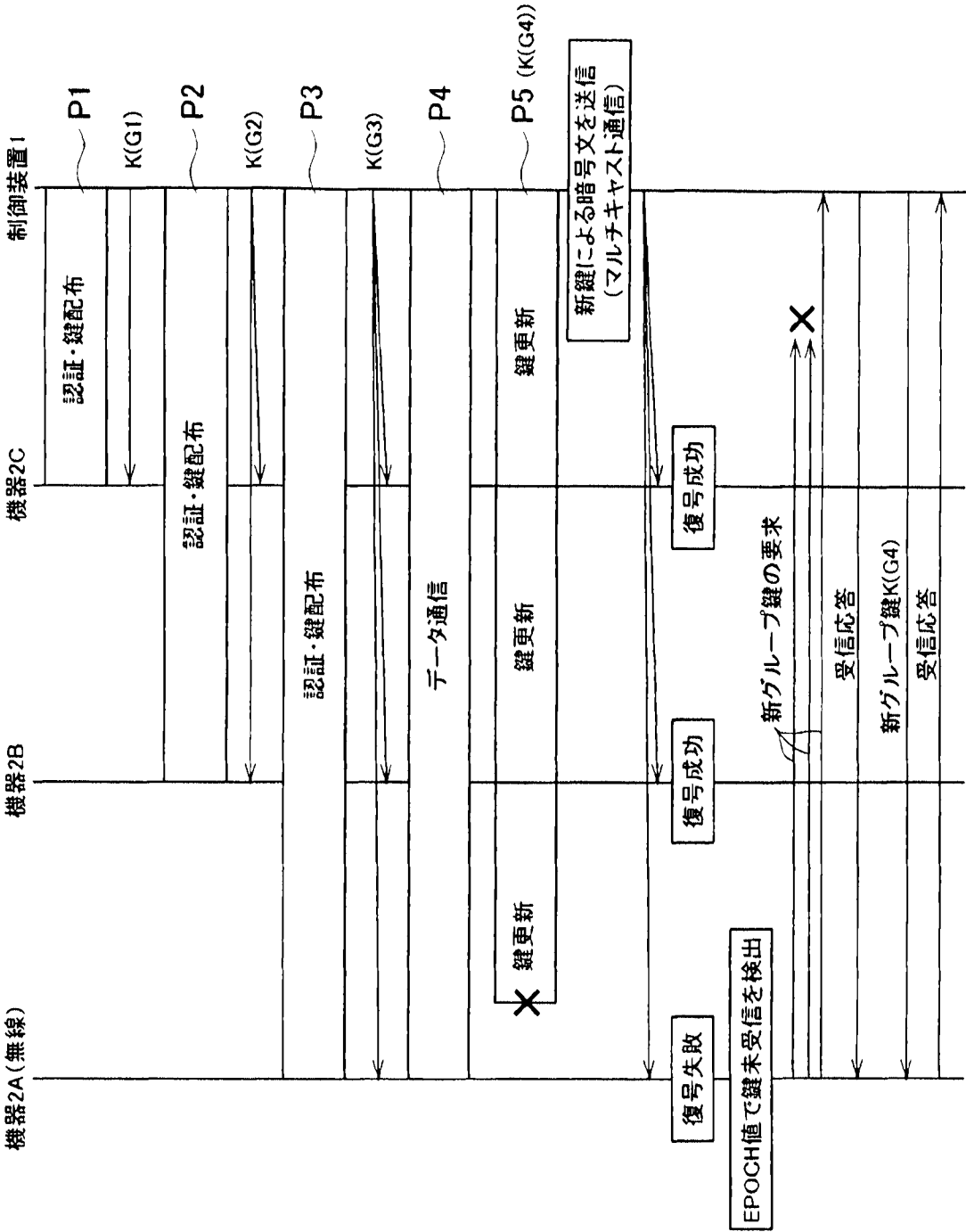


図 9

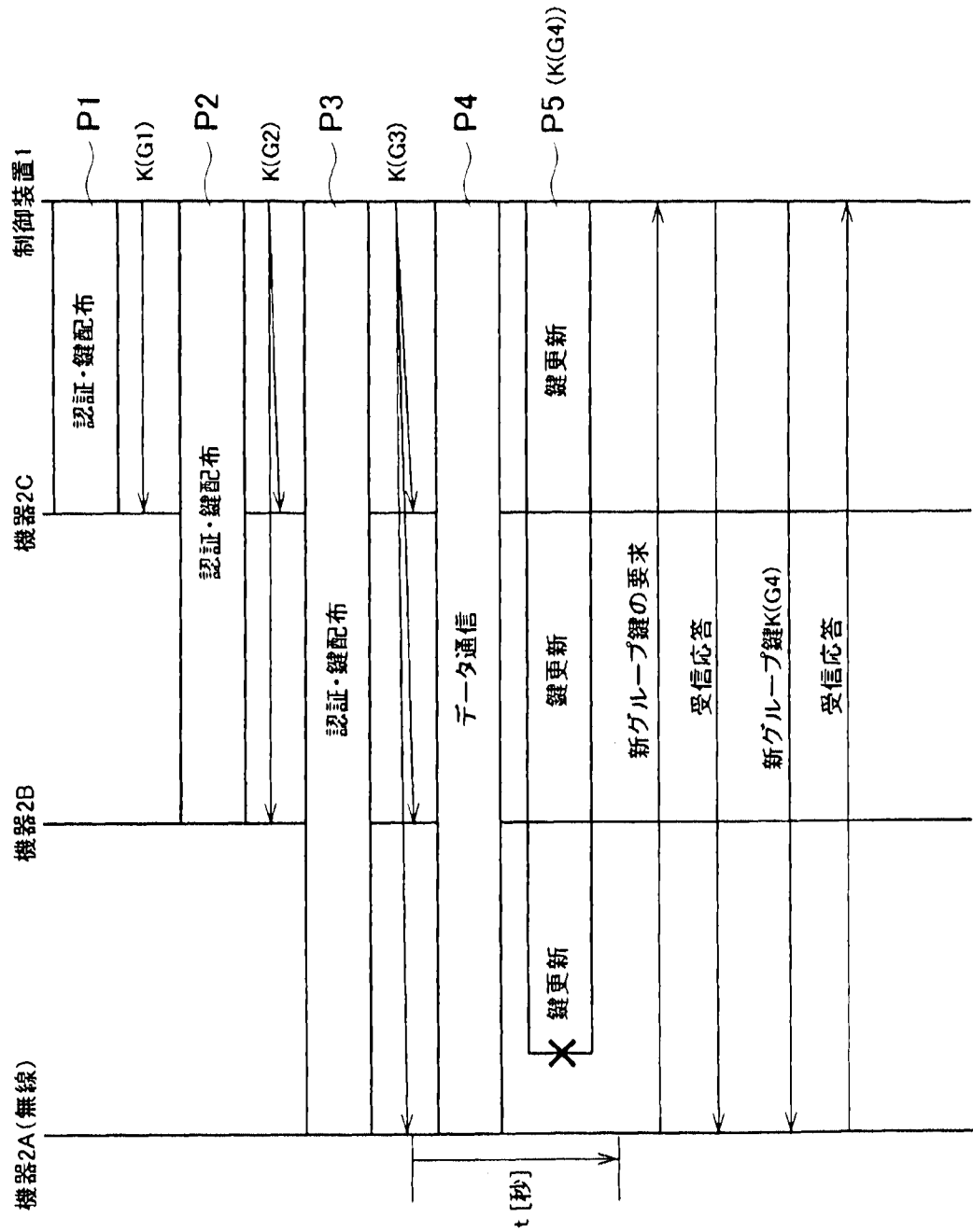


図 10

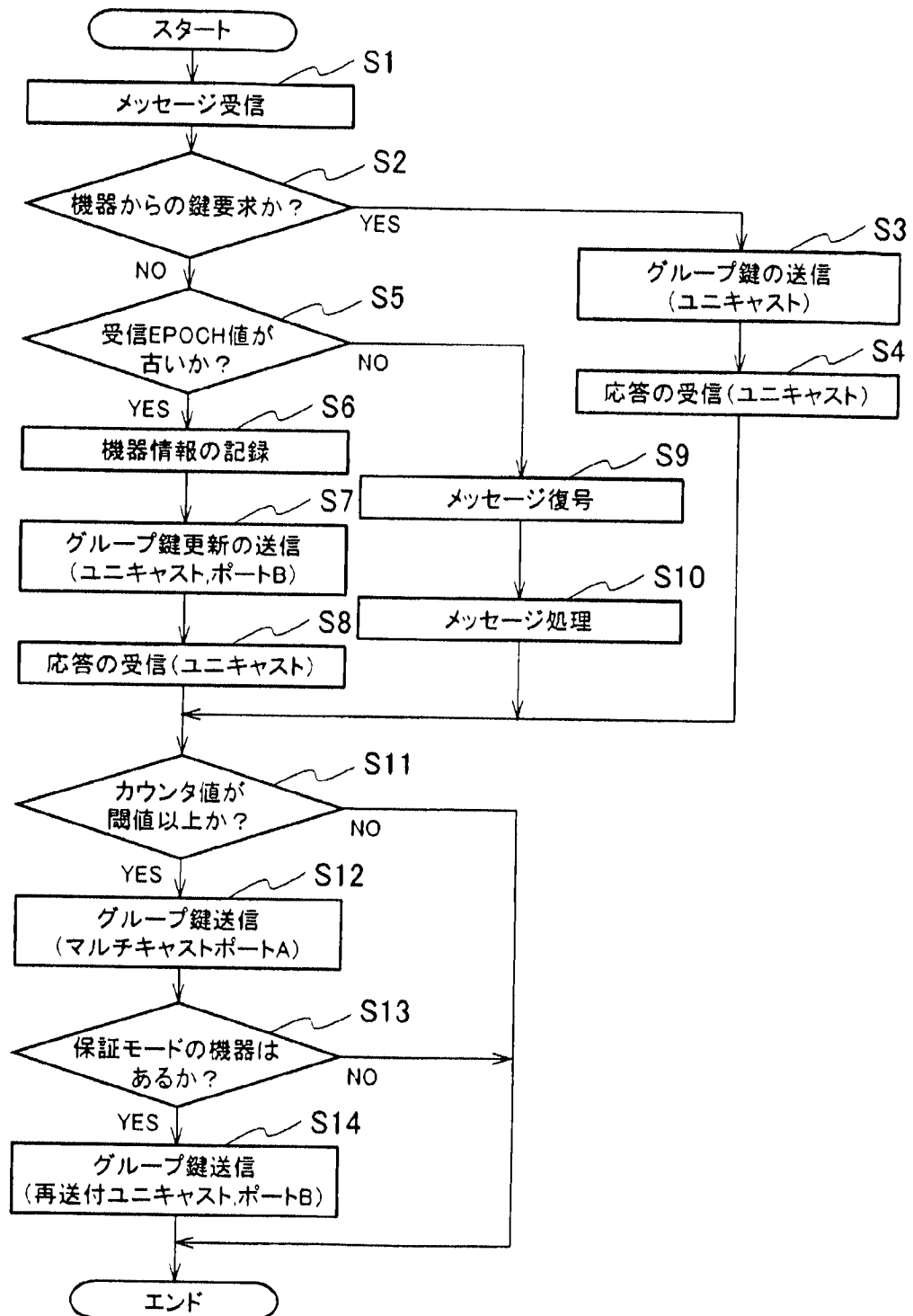


図 11

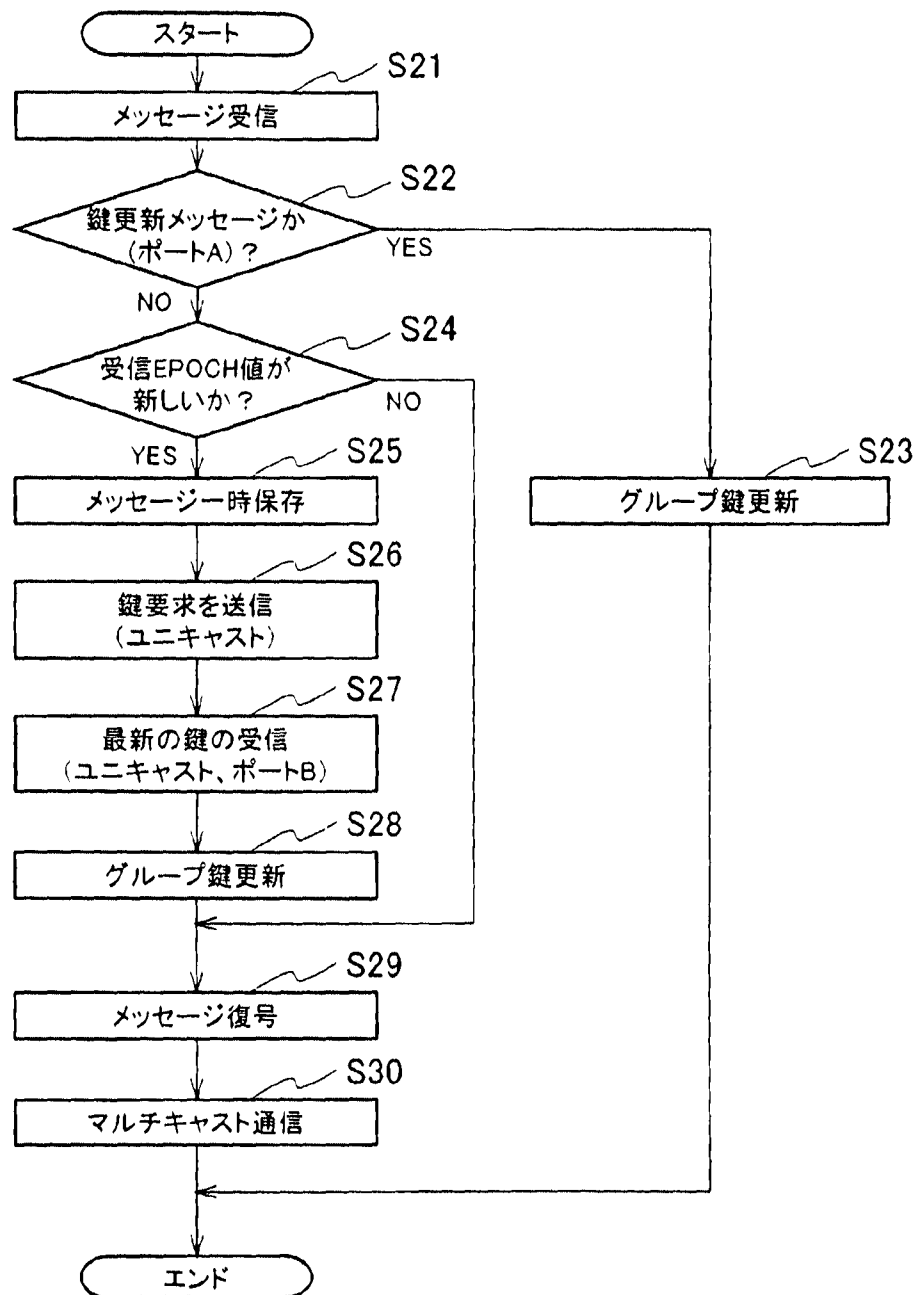


図 12

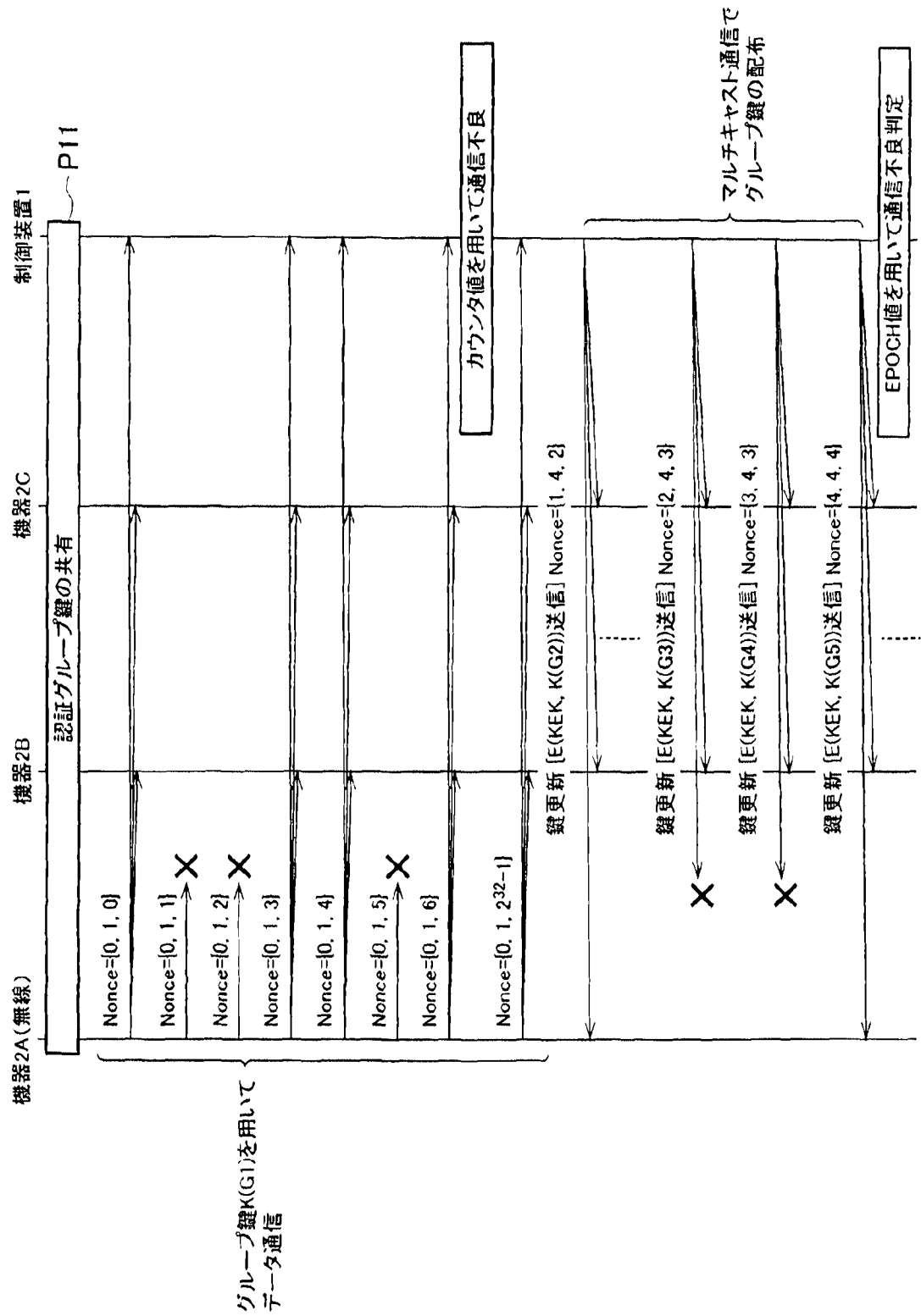


図 13

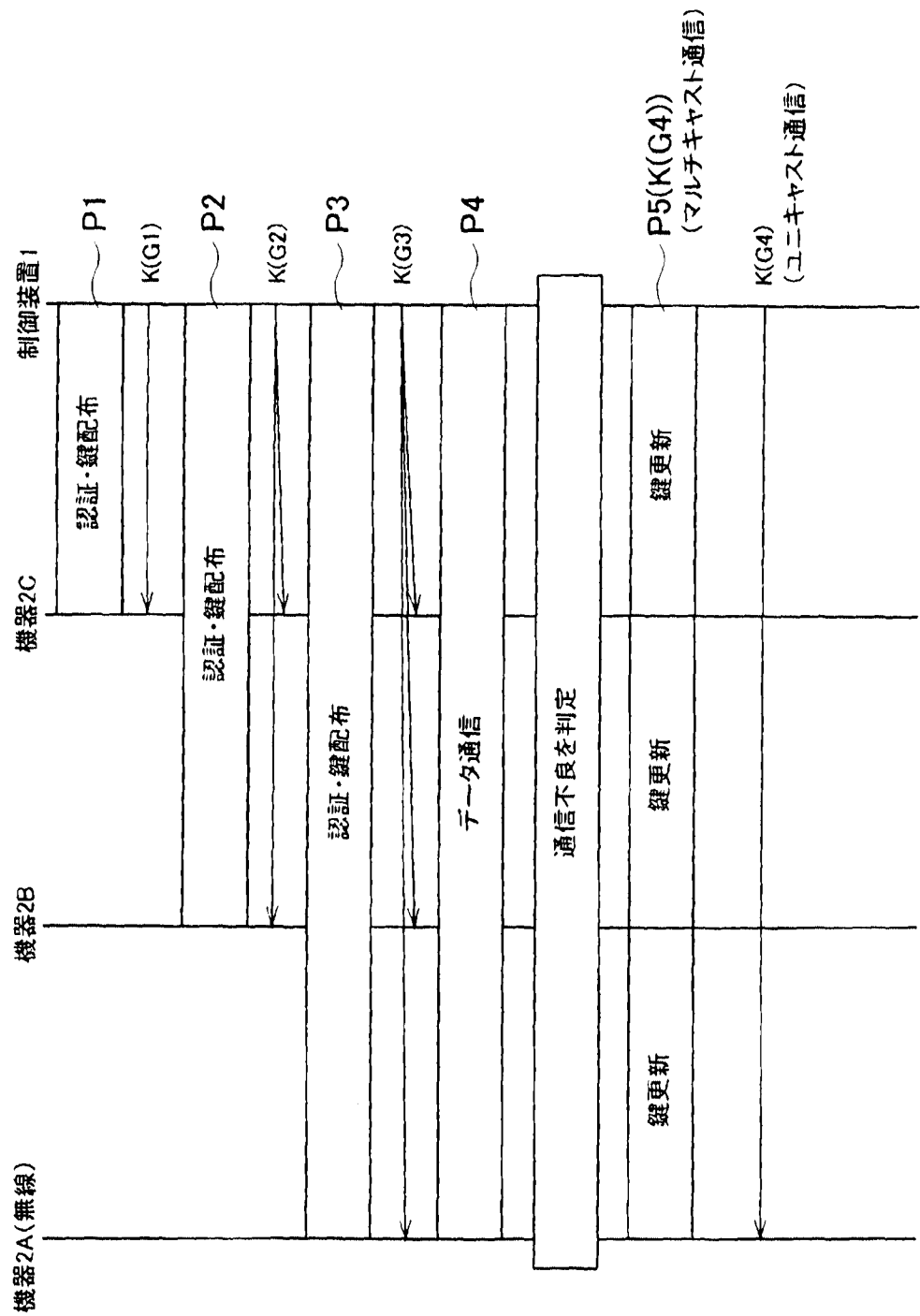
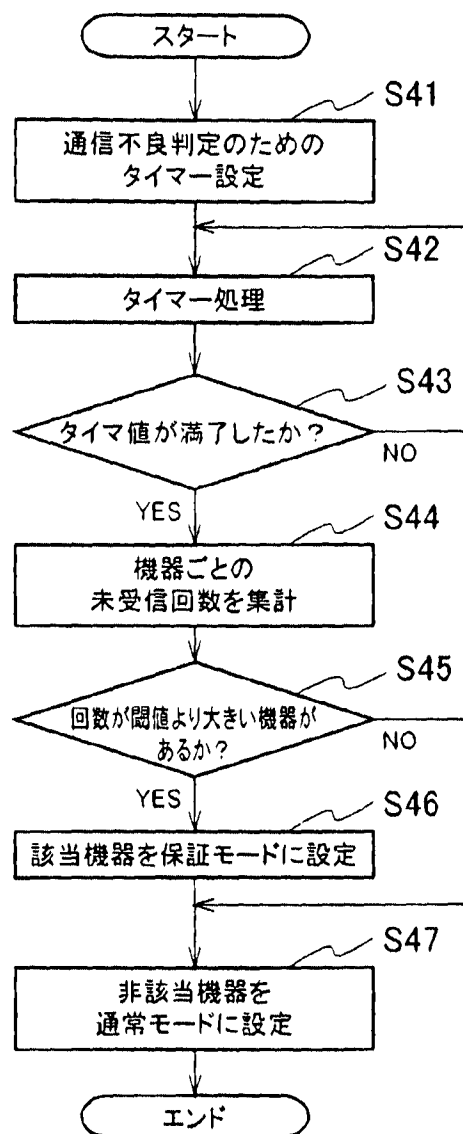


図 14



15

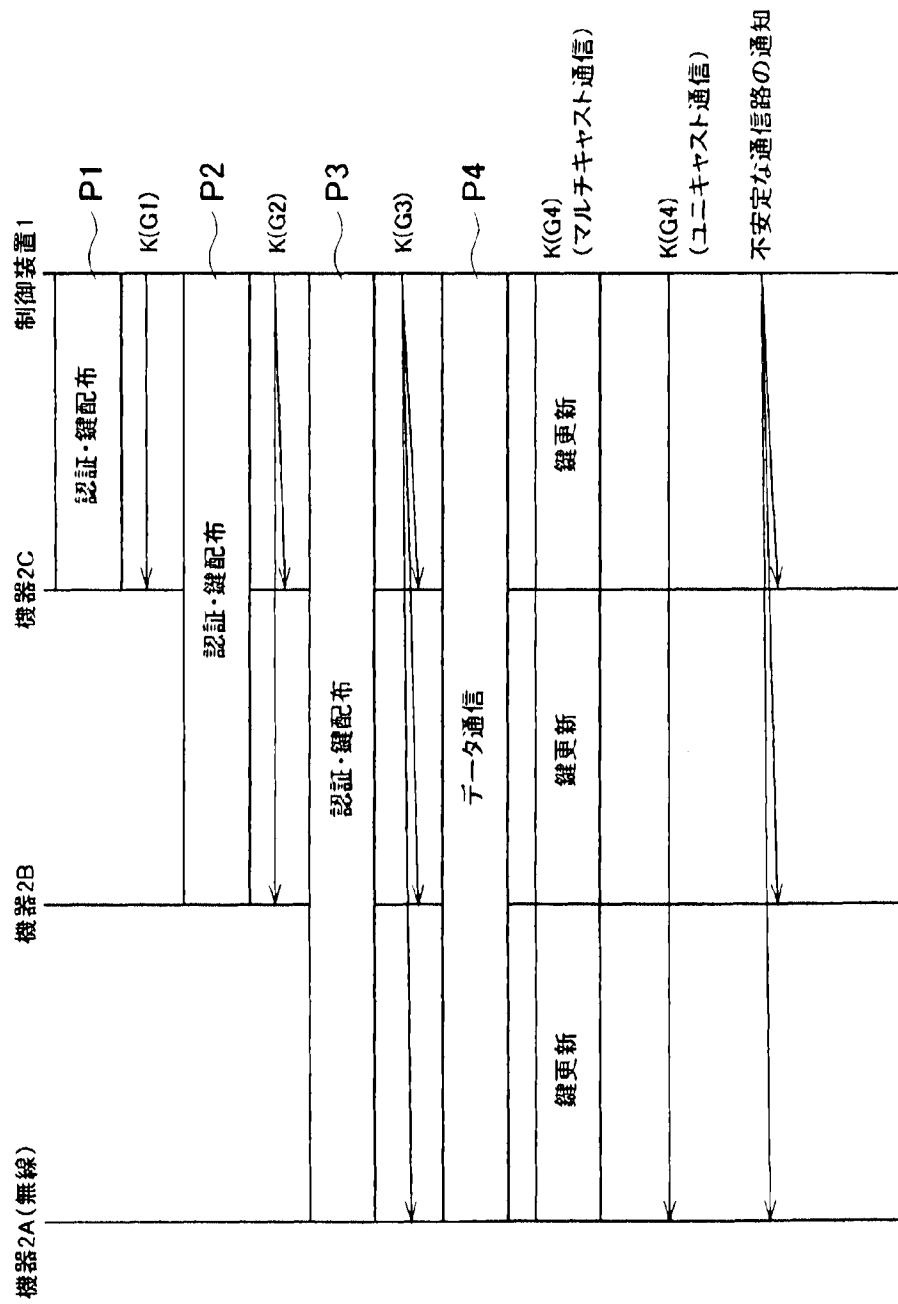


図 16

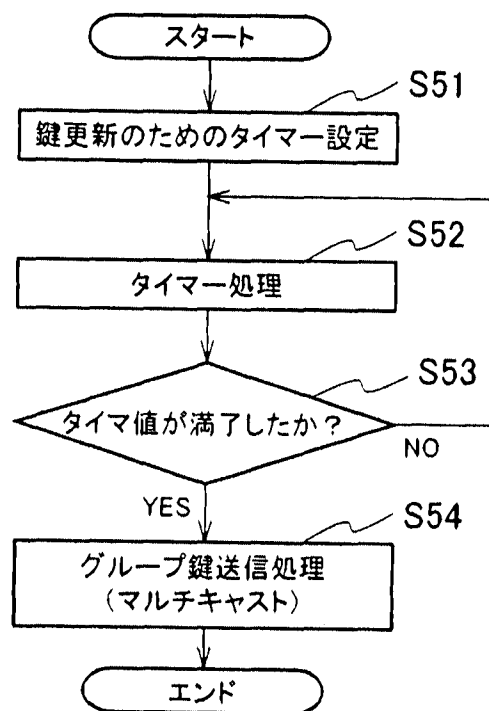


図 17

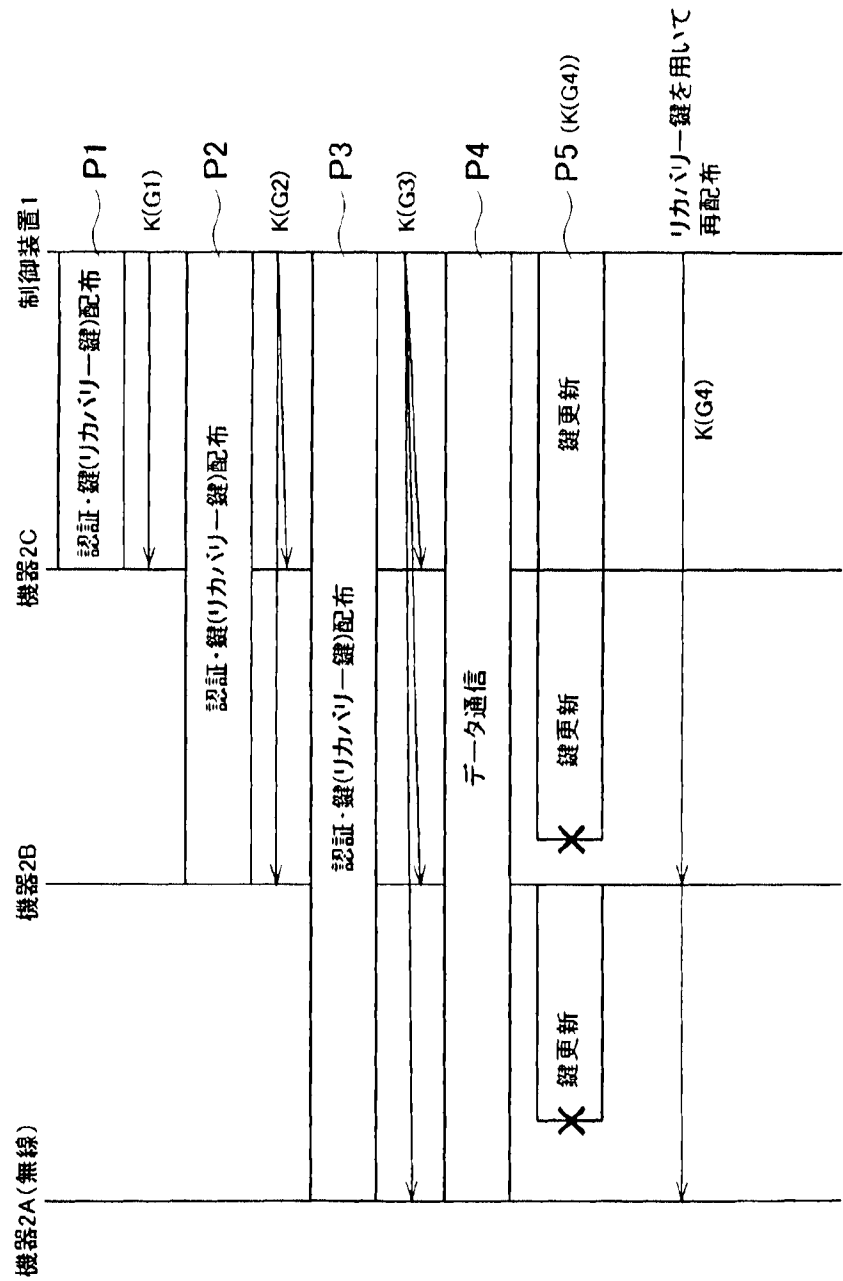
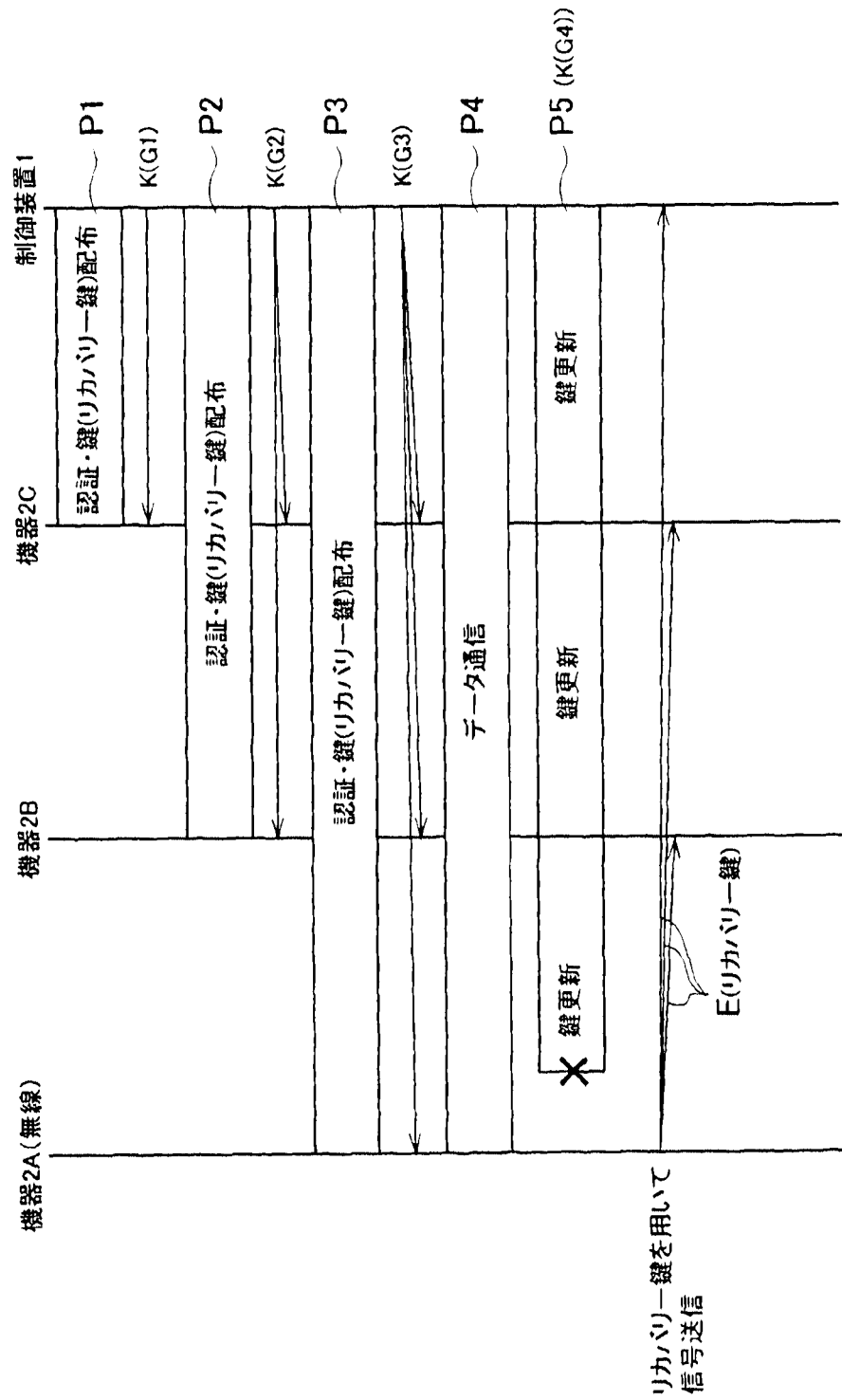


図 18



INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2015/000006

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/16(2006.01)i, H04L9/08(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)

H04L9/16, H04L9/08

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 1996-2015
Kokai Jitsuyo Shinan Koho 1971-2015 Toroku Jitsuyo Shinan Koho 1994-2015

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 A	JP 9-319673 A (Matsushita Electric Works, Ltd.), 12 December 1997 (12.12.1997), paragraphs [0012] to [0018] (Family: none)	16, 18 1-15, 17
Y A	JP 2002-247022 A (Nippon Telegraph and Telephone Corp.), 30 August 2002 (30.08.2002), paragraphs [0048] to [0068] (Family: none)	16, 18 1-15, 17
Y A	JP 11-274999 A (Hitachi, Ltd.), 08 October 1999 (08.10.1999), paragraphs [0032] to [0047] (Family: none)	16, 18 1-15, 17

☒ 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
16 March 2015 (16.03.15)

Date of mailing of the international search report
24 March 2015 (24.03.15)

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/IB2015/000006

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2010-517330 A (Panasonic Electric Works Co., Ltd.), 20 May 2010 (20.05.2010), paragraphs [0030], [0032] & JP 5033188 B & US 2008/0175387 A1 & EP 2104989 A1 & WO 2008/088084 A1 & KR 10-2009-0110334 A & CN 101641903 A & RU 2009131314 A & TW 200840297 A	16, 18 1-15, 17
A	JP 2000-269951 A (Advanced Mobile Telecommunications Security Technology Research Laboratories Co., Ltd.), 29 September 2000 (29.09.2000), paragraphs [0030] to [0031] (Family: none)	1-15, 17
A	JP 61-82547 A (Hitachi, Ltd.), 26 April 1986 (26.04.1986), page 2, upper left column, line 12 to page 3, upper left column, line 9 (Family: none)	1-15, 17
A	JP 2003-101533 A (Toshiba Corp.), 04 April 2003 (04.04.2003), paragraphs [0046] to [0051], [0068] to [0075] & US 2003/0061518 A1	1-15, 17

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L9/16(2006.01)i, H04L9/08(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. H04L9/16, H04L9/08

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	1971-2015年
日本国実用新案登録公報	1996-2015年
日本国登録実用新案公報	1994-2015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 A	JP 9-319673 A (松下電工株式会社) 1997. 12. 12, 段落 0012-0018 (ファミリーなし)	16, 18 1-15, 17
Y A	JP 2002-247022 A (日本電信電話株式会社) 2002. 08. 30, 段落 0048-0068 (ファミリーなし)	16, 18 1-15, 17
Y A	JP 11-274999 A (株式会社日立製作所) 1999. 10. 08, 段落 0032-0047 (ファミリーなし)	16, 18 1-15, 17

☒ 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

16. 03. 2015

国際調査報告の発送日

24. 03. 2015

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)

金沢 史明

5 S

4 5 3 8

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 A	JP 2010-517330 A (パナソニック電気株式会社) 2010. 05. 20, 段落 0030, 0032 & JP 5033188 B & US 2008/0175387 A1 & EP 2104989 A1 & WO 2008/088084 A1 & KR 10-2009-0110334 A & CN 101641903 A & RU 2009131314 A & TW 200840297 A	16, 18 1-15, 17
A	JP 2000-269951 A (株式会社高度移動通信セキュリティ技術研究所) 2000. 09. 29, 段落 0030-0031 (ファミリーなし)	1-15, 17
A	JP 61-82547 A (株式会社日立製作所) 1986. 04. 26, 2 頁左上欄 12 行目-3 頁左上欄 9 行目 (ファミリーなし)	1-15, 17
A	JP 2003-101533 A (株式会社東芝) 2003. 04. 04, 段落 0046-0051, 0068-0075 & US 2003/0061518 A1	1-15, 17