(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
2013 年 6 月 13 日 (13.06.2013)

W 画P O | P C T

(10) 国際公開番号
WO 2013/084304 A1

(51) 国際特許分類：
H04W 12/12 (2009.01) H04W 84/18 (2009.01)

(21) 国際出願番号： PCT/JP201 1/078216

(22) 国際出願日： 201 1 年 12 月 6 日 (06. 12.201 1)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士迪株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4 丁目1番1号 Kanagawa (JP).

(72) 発明者 ;および

(75) 発明者/出願人 (米国についてのみ):伊豆 哲也 (IZU, Tetsuya) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4 丁目1番1号 富士通株式会社内 Kanagawa (JP). 武仲 正彦 (TAKENAKA, Masahiko) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4 丁目1番1号 富士通株式会社内 Kanagawa (JP). 兒島 尚 (KOJIMA, Hisash り [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4 丁目1番1号 富士通株式会社内 Kanagawa (JP). 古川 和快 (FURUKAWA, Kazuyoshi) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4 丁目1番1号 富士通株式会社内 Kanagawa (JP).

(74) 代理人 酒井 昭徳 (SAKAI, Akinor り; 〒1006020 東京都千代田区霞が関3 丁目2番5号 霞が関ビルディング20 階 酒井総合特許事務所 Tokyo (JP)-

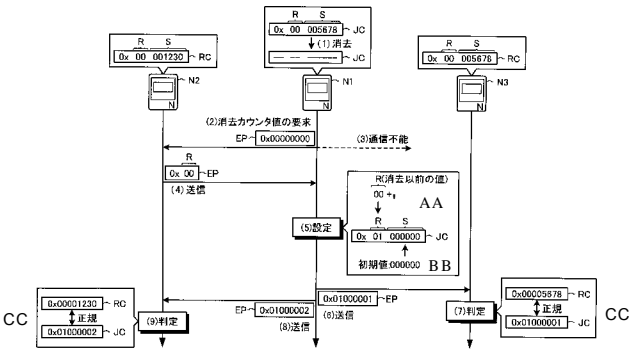
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, YL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT,

[続葉有]

(54) Title: NODES, COMMUNICATION METHOD, AND COMMUNICATION SYSTEM

(54) 発明の名称 :ノード、通信方法、および通信システム

[図1]



(1) Elimination
(2) Request for elimination counter value
(3) Communication impossible
(4), (6), (8) Transmissions
(5) Setting
(7), (9) Determinations
AA R (the value before elimination)
BB Initial value
CC Normal

(57) Abstract: A transmitting side node (NI) increments, by one per transmission, a joined counter value (JC), which is obtained by joining an elimination counter value (R) and a transmission counter value (S) in such a manner that the elimination counter value (R) forms upper-order digits of the joined counter value (JC) and the transmission counter value (S) forms the lower-order digits thereof, and the transmitting side node (NI) then transmits the thus incremented joined counter value (JC) to receiving side nodes (N2, N3). On the other hand, each of the receiving side nodes (N2, N3) determines that a packet, which has been received together with the joined counter value (JC) at this time, is a normal packet if the joined counter value (JC) received at this time is greater than the joined counter value (JC) received last time. At this moment, the transmitting side node (NI), if the joined counter value has been eliminated, generates a new joined counter value (JC) by incrementing, by one, the elimination counter value (R) present before the elimination and then joining the incremented elimination counter value (R) and the transmission counter value (S) in such a manner that the incremented elimination counter value (R) forms upper-order digits of the new joined counter value (JC) and the transmission counter value (S) forms the lower-order digits thereof. In this way, the transmitting side node (NI) can generate a new joined counter value (JC) that is greater than the joined counter values (JC) transmitted by the transmitting side node (NI) in the past.

(57) 要約:

[続葉有]

2013 084304 A1

QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

添付公開書類:

– 国際調査報告 (条約第21条(3))

送信側ノード (N1) は、消去カウンタ値 (R) を上位桁として送信カウンタ値 (S) を下位桁として連結した連結カウンタ値 (JC) を送信ごとに1加算して、受信側ノード (N2, N3) に送信する。一方、受信側ノード (N2, N3) は、前回受信した連結カウンタ値 (JC) より、今回受信した連結カウンタ値 (JC) が大きければ、今回連結カウンタ値 (JC) とともに受信したパケットを正規パケットと判断する。ここで、送信側ノード (N1) は、連結カウンタ値が消去された場合、消去以前の消去カウンタ値 (R) に1を加算した加算後の消去カウンタ値 (R) を上位桁とし、送信カウンタ値 (S) を下位桁として連結した新たな連結カウンタ値 (JC) を生成する。これにより、送信側ノード (N1) は、過去に送信側ノード (N1) が送信した連結カウンタ値 (JC) より大きい新たな連結カウンタ値 (JC) を生成できる。

明 細 書

発明の名称 ：ノー ド、通信方法、および通信システム

技術分野

[0001] 本発明は、ノー ド、通信方法、および通信システムに関する。

背景技術

[0002] ア ドホックネッ トワークは、無線通信でリンクする自己構成型のネッ トワ - クの一種である。ア ドホックネッ トワークは複数のノー ドにより構成される。また、ア ドホックネッ トワーク内の各ノー ドは、マルチホップ通信によりパケッ トの送受信を行う。マルチホップ通信は、互いの通信圏内に存在しないノー ド同士が、各ノー ドの通信圏内に存在する別のノー ドを介して通信を行う技都である。

[0003] ア ドホックネッ トワークを利用した技術として、各家庭の電力メータに無線通信可能なノー ドを組み込んで、作業員が現地に出向くことなく、ア ドホックネッ トワーク経由でメータ検針などの業務を行うシステムがある。各家庭の電力の使用量などの個人情報を扱うア ドホックネッ トワークでは、秘匿性、改ざん防止などの観点からセキュアな通信を行うことが要求される。

[0004] そこで、従来のシステムでは、ア ドホックネッ トワーク内のノー ド間で送受信されるバケツ トを暗号化することで、セキュアな通信の確保が行われている。関連する技術として、パケッ トの暗号化に用いる暗号鍵を、セキュアに配布する技術がある (例えば、下記特許文献 1 ~ 3 参照。) 。また、ノー ドがア ドホックネッ トワーク内から接続するゲー トウェイを発見する技術がある (例えば、下記特許文献 4 参照。) 。また、バスマネージャになった他ノー ドからバスジ工ネレーション番号を取得しておき、自ノー ドがバスマネ—ジャになったときに、取得したバスジェネレーション番号に 1 を加算して使用する技術がある (例えば、下記特許文献 5 参照。) 。

[0005] パケッ トが暗号化されている場合であっても、ア ドホックネッ トワークでは、過去にア ドホックネッ トワーク内に送信された正規パケッ トが、攻撃者

によりキヤプチャされうる。そして、攻撃者は、キヤプチヤした正規バケツトをアドホックネットワーク内に再送することで、ネットワークを輻輳させる攻撃 (再送攻撃) をすることができる。そこで、アドホックネットワークは、ネットワークとしての通信品質を確保するために、再送攻撃に備える必要がある。従来のシステムでは、パケットを送信するノードは、パケットの送信時刻をパケット内に格納するようにしている。そして、パケットを受信したノードは、自ノードの時刻と、受信したパケット内の送信時刻とを比較し、両者が大きくかけ離れている場合には、再送攻撃が行われたと見なし、そのバケツトを廃棄するという技術がある。

先行技術文献

特許文献

[0006] 特許文献1 :特開２００３_３４８０７２号公報

特許文献2 :特開２０１０_９８５９７号公報

特許文献3 :特開２００７_８８７９９号公報

特許文献4 :特開２００９_８１８５４号公報

特許文献5 :特開２００６_１２８８７６号公報

発明の概要

発明が解決しようとする課題

[0007] しかしながら、上述した従来技術では、アドホックネットワーク内の全ノードの時刻が同期されている必要がある。例えば、他のネットワークとの中継機器であるゲートウェイまたはアドホックネットワーク内の特定のノードが、定期的に時刻同期用のパケットをプロードキャストすることで、アドホックネットワーク内の全ノードの時刻同期を実現する。

[0008] そのため、メータ検針を行うアドホックネットワークでは、各メータの検針データバケツト以外に、時刻同期用のプロードキャストバケツトが送受信されることとなり、アドホックネットワークの通信負荷が増大するという問題がある。

[0009] 本発明は、上述した従来技術による問題点を解消するため、通信負荷の低減化を図ることができるノード、通信方法、および通信システム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

[001 0] 上述した課題を解決し、目的を達成するため、本発明の一側面によれば、自ノードでの消去回数を示す消去カウンタ値を上位桁とし自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段を備え、アドホックネットワーク内の他ノードにデータを送信する場合、記憶手段に記憶されている連結カウンタ値のうち送信カウンタ値を1加算し、データおよび加算後の連結カウンタ値を他ノードに送信し、記憶手段での連結カウンタ値の消去を検出し、消去が検出された場合、消去カウンタ値の取得要求をアドホックネットワークに配信し、取得要求が配信された結果、アドホックネットワークから消去カウンタ値を受信し、受信された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、生成された連結カウンタ値を記憶手段に保存するノードおよび通信方法が提案される。

[001 1] また、本発明の一側面によれば、自ノードでの消去回数を示す消去カウンタ値を上位桁とし自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段を備え、アドホックネットワーク内の他ノードにデータを送信する場合、記憶手段に記憶されている連結カウンタ値のうち送信カウンタ値を1加算し、データおよび加算後の連結カウンタ値を他ノードに送信し、記憶手段での連結カウンタ値の消去を検出し、消去が検出された場合、消去カウンタ値の更新要求をアドホックネットワークに配信し、更新要求が配信された結果、アドホックネットワークから消去カウンタ値に1加算された加算後の消去カウンタ値を受信し、受信された加算後の消去カウンタ値を上位桁とし消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、生成され

た連結カウンタ値を記憶手段に保存するノードおよび通信方法が提案される。

[001 2] また、本発明の一側面によれば、自ノードでの消去回数を示す消去カウンタ値を上位桁とし自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する揮発性の第1の記憶手段と、消去カウンタ値を記憶する不揮発性の第2の記憶手段と、を備え、アドホックネットワーク内の他ノードにデータを送信する場合、第1の記憶手段に記憶されている連結カウンタ値のうち送信カウンタ値を1加算し、データおよび加算後の連結カウンタ値を他ノードに送信し、第1の記憶手段での連結カウンタ値の消去を検出し、消去が検出された場合、第2の記憶手段から消去カウンタ値を抽出し、抽出された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、生成された連結カウンタ値を第1の記憶手段に保存するとともに、第2の記憶手段に記憶されている消去カウンタ値に対し加算後の消去カウンタ値を上書き保存するノードおよび通信方法が提案される。

[001 3] また、本発明の一側面によれば、他ノードでの消去回数を示す消去カウンタ値を上位桁とし他ノードからの送信回数を示す送信カウンタ値を下位桁とする第1の連結カウンタ値を、他ノードから受信し、受信された連結カウンタ値を記憶装置に保存し、第2の連結カウンタ値を他ノードから受信し、第2の連結カウンタ値が第1の連結カウンタ値よりも大きいか否かを判断し、大きいと判断された場合、第1の連結カウンタ値に第2の連結カウンタ値を上書保存するノードおよび通信方法が提案される。

[0014] また、本発明の一側面によれば、アドホックネットワーク内の第1のノードと第2のノードとが通信するシステムであって、第1のノードは、第1のノードでの消去回数を示す消去カウンタ値を上位桁とし第1のノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段を備え、アドホックネットワーク内の他ノードにデータを送信する場

合、記憶手段に記憶されている連結カウンタ値のうち送信カウンタ値を1加算し、第2のノードを宛先にする第1のデータおよび加算後の第1の連結カウンタ値を第2のノードに送信し、記憶手段での連結カウンタ値の消去を検出し、消去が検出された場合、消去カウンタ値の取得要求をアドホックネットワークに配信し、取得要求が配信された結果、アドホックネットワークから消去カウンタ値を受信し、受信された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、生成された連結カウンタ値を記憶手段に保存し、保存された後に、第2のノードを宛先にする第2のデータおよび記憶手段に記憶されている最新の連結カウンタ値のうち送信カウンタ値を1加算した第2の連結カウンタ値を、第2のノードに送信し、第2のノードは、第1の連結カウンタ値を、第1のノードから受信し、受信された第1の連結カウンタ値を記憶装置に保存し、第2の連結カウンタ値を、第1のノードから受信し、受信された第2の連結カウンタ値が第1の連結カウンタ値よりも大きいか否かを判断し、大きいと判断された場合、第1の連結カウンタ値を第2の連結カウンタ値に上書保存する通信システムが提案される。

[0015] また、本発明の一側面によれば、アドホックネットワーク内の第1のノードと第2のノードとが通信するシステムであって、第1のノードは、第1のノードでの消去回数を示す消去カウンタ値を上位桁とし第1のノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段を備え、アドホックネットワーク内の他ノードにデータを送信する場合、記憶手段に記憶されている連結カウンタ値のうち送信カウンタ値を1加算し、第2のノードを宛先にする第1のデータおよび加算後の第1の連結カウンタ値を第2のノードに送信し、記憶手段での連結カウンタ値の消去を検出し、消去が検出された場合、消去カウンタ値の更新要求をアドホックネットワークに配信し、更新要求が配信された結果、アドホックネットワークから消去カウンタ値に1加算された加算後の消去カウンタ値を受信し、受信さ

れた加算後の消去カウンタ値を上位桁とし消去により送信回数が0になつたことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、生成された連結カウンタ値を記憶手段に保存し、保存された後に、第2のノードを宛先にする第2のデータおよび記憶手段に記憶されている最新の連結カウンタ値のうち送信カウンタ値を1加算した第2の連結カウンタ値を第2のノードに送信し、第2のノードは、第1の連結カウンタ値を、第1のノードから受信し、受信された第1の連結カウンタ値を記憶装置に保存し、第2の連結カウンタ値を、第1のノードから受信し、受信された第2の連結カウンタ値が第1の連結カウンタ値よりも大きいか否かを判断し、大きいと判断された場合、第1の連結カウンタ値を第2の連結カウンタ値に上書保存する通信システムが提案される。

[0016] また、本発明の一側面によれば、アドホックネットワーク内の第1のノードと第2のノードとが通信するシステムであって、第1のノードは、第1のノードでの消去回数を示す消去カウンタ値を上位桁とし第1のノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する揮発性の第1の記憶手段と、消去カウンタ値を記憶する不揮発性の第2の記憶手段と、を備え、アドホックネットワーク内の他ノードにデータを送信する場合、第1の記憶手段に記憶されている連結カウンタ値のうち送信カウンタ値を1加算し、第2のノードを宛先にする第1のデータおよび加算後の第1の連結カウンタ値を第2のノードに送信し、第1の記憶手段での連結カウンタ値の消去を検出し、消去が検出された場合、第2の記憶手段から消去カウンタ値を抽出し、抽出された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、生成された連結カウンタ値を第1の記憶手段に保存するとともに、第2の記憶手段に記憶されている消去カウンタ値に対し加算後の消去カウンタ値を上書き保存し、保存された後に、第2のノードを宛先にする第2のデータおよび記憶手段に記憶されている最新の連結カウンタ値のうち送信カウンタ値を1加算した第2の連

結カウンタ値を第２のノードに送信し、第２のノードは、第１の連結カウンタ値を、第１のノードから受信し、受信された第１の連結カウンタ値を記憶装置に保存し、第２の連結カウンタ値を、第１のノードから受信し、受信された第２の連結カウンタ値が第１の連結カウンタ値よりも大きいか否かを判断し、大きいと判断された場合、第１の連結カウンタ値を第２の連結カウンタ値に上書保存する通信システムが提案される。

発明の効果

[001 7] 本発明の一側面によれば通信負荷の低減化を図ることができるという効果を奏する。

図面の簡単な説明

[001 8] [図1]図１は、ノードによるアドホックネットワークへの復帰処理例を示す説明図である。

[図2]図２は、実施の形態にかかるノードNのハードウエア構成例を示すブロック図である。

[図3]図３は、ノードＤＢ（ＤａｔａＢａｓｅ）の記憶内容の一例を示す説明図である。

[図4]図４は、ノードNの送信側としての機能的構成例を示す機能ブロック図である。

[図5]図５は、ノードNの受信側としての機能的構成例を示す機能ブロック図である。

[図6]図６は、アクセス鍵ＡＫを用いた暗号化通信の一例を示す説明図である。

[図7]図７は、アクセス鍵ＡＫを用いた暗号化通信の詳細を示す説明図である。

[図8]図８は、暗号化通信におけるバケット送信処理の詳細な処理手順を示すフローチャートである。

[図9]図９は、暗号化通信におけるバケット受信処理の詳細な処理手順を示すフローチャートである。

[図10] 図１０は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例１を示す説明図（その１）である。

[図11] 図１１は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例１を示す説明図（その２）である。

[図12] 図１２は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例１を示す説明図（その３）である。

[図13] 図１３は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例１を示す説明図（その４）である。

[図14] 図１４は、動作例１における連結カウンタ値生成処理の詳細な処理手順を示すフローチャートである。

[図15] 図１５は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例２を示す説明図（その１）である。

[図16] 図１６は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例２を示す説明図（その２）である。

[図17] 図１７は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例２を示す説明図（その３）である。

[図18] 図１８は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例２を示す説明図（その４）である。

[図19] 図１９は、動作例２における連結カウンタ値生成処理の詳細な処理手順を示すフローチャート（その１）である。

[図20] 図２０は、動作例２における連結カゥンタ値生成処理の詳細な処理手順を示すフローチャート（その２）である。

[図21] 図２１は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例３を示す説明図（その１）である。

[図22] 図２２は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例３を示す説明図（その２）である。

[図23] 図２３は、動作例３における連結カゥンタ値生成処理の詳細な処理手順を示すフローチャートである。

発明を実施するための形態

[001 9] 以下に添付図面を参照して、この発明にかかるノード、通信方法、および通信システムの実施の形態を詳細に説明する。

[0020] (ノードによるアドホックネットワークへの復帰処理例)

図1は、ノードによるアドホックネットワークへの復帰処理例を示す説明図である。図1において、ノードN1、ノードN2およびノードN3は、互いの通信圏内に存在する近隣ノードNである。ノードN1、ノードN2およびノードN3は、アドホックネットワーク内の各ノードNで共有される共通鍵(以下、「固定鍵」という)や、アドホックネットワーク内のノードN間で一定時間ごとに更新される共通鍵(以下、「アクセス鍵」という)を保持している。ノードN1、ノードN2およびノードN3は、固定鍵やアクセス鍵を用いてバケットを暗号化して得られた暗号化バケットEPの送受信を行っている。

[0021] ここでは、簡単のため、ノードN1は、暗号化パケットEPを近隣ノードNに送信する送信側のノードNであるとする。また、ノードN2およびノードN3は、暗号化パケットEPを近隣ノードNから受信する受信側のノードNであるとする。

[0022] ノードN1は、連結カウンタ値JCを保持している。連結カウンタ値JCは、上位桁のカウンタ値と下位桁のカウンタ値とが連結されたカウンタ値である。ここで、下位桁のカウンタ値は、今までにノードN1が暗号化バケットEPを送信した回数を示す送信カウンタ値Sである。上位桁のカウンタ値は、ノードN1において連結カウンタ値JCが消去された回数を示す消去カウンタ値Rである。図1の例では、ノードN1は、消去カウンタ値R「0x00」と、送信カウンタ値S「0x005678」と、を連結した連結カウンタ値JC「0x00005678」を保持している。なお、「0x」は16進数表記を示す。

[0023] ノードN1は、他ノードNを宛先にするデータの送信イベントがあると、連結カウンタ値JCに1を加算する。そして、ノードN1は、他ノードN(

例えば、ノードN２，Ｎ３）を宛先にするデータと、加算後の連結カウンタ値ＪＣと、を含むパケットを生成し、生成したパケットを暗号化して得られた暗号化パケットＥＰを、他ノードNに送信する。

[0024] また、ノードＮ１は、連結カウンタ値ＪＣが消去されたことを検知すると、消去カウンタ値Ｒの取得要求を他ノードNに送信する。ノードＮ１は、取得要求を送信した結果、消去以前の連結カウンタ値」Ｃの消去カウンタ値Ｒを他ノードNから受信する。そして、ノードＮ１は、受信した消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒと、送信カウンタ値Ｓの初期値と、を連結した連結カウンタ値ＪＣを生成する。このとき、消去カウンタ値Ｒは上位桁であるから、消去以前の消去カウンタ値Ｒに１加算した加算後の消去カウンタ値Ｒから生成された新たな連結カゥンタ値ＪＣは、送信カウンタ値Ｓの大小に関わらず、消去以前の連結カゥンタ値ＪＣより大きい値になる。

[0025] ノードＮ２およびノードＮ３は、他ノードN（例えば、ノードＮ１）から暗号化パケットＥＰを受信する。ノードＮ２およびノードＮ３は、受信した暗号化バケツトＥＰを復号して得られたバケツトから他ノードNでの連結カゥンタ値ＪＣを抽出する。そして、ノードＮ２およびノードＮ３は、抽出した連結カウンタ値」Ｃを、受信カウンタ値ＲＣとして保持する。

[0026] 図１の例では、ノードＮ２は、過去にノードＮ１から受信した暗号化パケットＥＰを復号して抽出した連結カウンタ値ＪＣ 『０ｘ００００１２３０」を、受信カウンタ値ＲＣとして保持している。また、ノードＮ３は、過去にノードＮ１から受信した暗号化バケツトＥＰを復号して抽出した連結カウンタ値ＪＣ 『０ｘ００００５６７８」を、受信カウンタ値ＲＣとして保持している。

[0027] ここで、ノードＮ１では、送信ごとに連結カウンタ値ＪＣに１を加算し、連結カゥンタ値ＪＣの消去後には消去前の連結カゥンタ値より大きい値になる新たな連結カウンタ値を生成している。そのため、ノードＮ２およびノードＮ３が、ノードＮ１からの正規パケットを受信し続けている限り、今回受

信した暗号化バケツトＥＰに含まれる連結カウンタ値ＪＣは、前回受信した暗号化バケツトＥＰに含まれる連結カウンタ値ＪＣより大きくなる。なお、上述したように、前回受信した暗号化バケツトＥＰに含まれていた連結カウンタ値ＪＣは、受信カウンタ値ＲＣとして保持されている。一方で、ノードＮが再送攻撃による不正バケツトを受信した場合、再送攻撃では過去に送信されたバケツトをそのまま送信しているため、ノードＮが今回受信したパケットに含まれる連結カウンタ値ＪＣは、受信カウンタ値ＲＣ以下となる。

[0028] そのため、ノードＮ２およびノードＮ３は、今回受信した暗号化パケットＥＰに含まれていた連結カウンタ値ＪＣが受信カウンタ値ＲＣより大きければ、暗号化パケットＥＰを正規パケットと判断する。一方、ノードＮ２およびノードＮ３は、今回受信した暗号化バケツトＥＰに含まれていた連結カウンタ値ＪＣが受信カウンタ値ＲＣ以下であれば、暗号化バケツトＥＰを不正バケツトと判断する。

[0029] ここで、図１において、停電によりノードＮ１に電力が供給されず、ノードＮ１が保持していた連結カゥンタ値ＪＣ 「０ｘ００００５６７８」が消去されてしまったとする。そのため、他ノードＮ（例えば、ノードＮ２，Ｎ３）に送信するパケットに含むべき連結カウンタ値ＪＣが不明になり、ノードＮ１は、他ノードＮにバケツトを送信することができない。

[0030] （１）まず、ノードＮ１は、停電が回復し電力が供給されると、連結カウンタ値ＪＣが消去されたことを検出する。

[0031] （２）次に、ノードＮ１は、連結カウンタ値ＪＣが消去されたことを検出すると、消去カウンタ値Ｒの取得要求を含むパケットを生成し、生成したパケットを固定鍵を用いて暗号化する。そして、ノードＮ１は、暗号化により得られた取得要求を含む暗号化バケツトＥＰを他ノードＮに送信する。図１の例では、ノードＮ１は、取得要求を含む暗号化バケツトＥＰを、ノードＮ２に送信できている。

[0032] （３）しかし、ノードＮ１は、ノードＮ３と通信不能の状態になっており、取得要求を含む暗号化パケットＥＰをノードＮ３に送信できていない。例

えば、ノードN３と通信不能の状態になる原因としては、ノードN１とノードN３との間に障害物が存在することが挙げられる。

[0033] （４）ノードN２は、ノードN１から暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰを固定鍵を用いて復号する。次に、ノードN２は、復号により得られたバケットに取得要求が含まれることを検出すると、受信カウンタ値ＲＣ「０ｘ００００１２３０」から消去カウンタ値Ｒ「０ｘ００」を抽出する。そして、ノードN２は、抽出した消去カウンタ値Ｒ「０χＯＯ」を含むパケットを生成し、生成したパケットを固定鍵を用いて暗号化する。次に、ノードN２は、暗号化により得られた暗号化パケットＥＰをノードN１に送信する。

[0034] （５）ノードN１は、ノードN２から暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰを固定鍵を用いて復号する。次に、ノードN１は、復号により得られたパケットから、消去カウンタ値Ｒ「０ｘ００」を取得する。そして、ノードN１は、連結カウンタ値ＪＣの消去以前での消去カウンタ値Ｒを示す取得した消去カウンタ値Ｒ「０ｘ００」に、１を加算する。次に、ノードN１は、加算後の消去カウンタ値Ｒ「０ｘ０１」と、送信カウンタ値Ｓの初期値「０ｘ０００００００」と、を連結して連結カウンタ値ＪＣ「０ｘ０１０００００００」を生成する。

[0035] ここで、ノードN１は、ノードN３と通信可能の状態になったとする。例えば、ノードN３と通信可能の状態になる原因としては、ノードN１とノードN３との間に存在した障害物が移動して、ノードN１とノードN３との間に障害物が存在しなくなつたことが挙げられる。

[0036] （６）ノードN１は、ノードN３を宛先にするデータの送信イベントがあると、連結カウンタ値ＪＣ「０ｘ０１０００００００」に１を加算する。次に、ノードN１は、ノードN３を宛先にするデータと、加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」と、を含むバケットを生成し、生成したパケットを固定鍵を用いて暗号化する。そして、ノードN１は、暗号化により得られた暗号化バケットＥＰを、データの宛先になるノードN３に送信する

。

[0037] （７）ノードＮ３は、ノードＮ１から暗号化パケットＥＰを受信すると、受信した暗号化バケツトＥＰの正当性の判断を行う。具体的には、ノードＮ３は、受信した暗号化パケットＥＰを、固定鍵を用いて復号する。次に、ノードＮ３は、復号により得られたパケットから連結カウンタ値ＪＣ「０ｘ０１０００００１」を取得する。そして、ノードＮ３は、前回受信した暗号化バケツトＥＰに含まれていた連結カウンタ値ＪＣを示す受信カウンタ値ＲＣ「０ｘ００００５６７８」と、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」と、の大小比較を行う。

[0038] ここで、ノードＮ３は、取得した連結カウンタ値ＪＣが受信カウンタ値ＲＣよりも大きいため、受信した暗号化バケツトＥＰは正規バケツトであると判断する。そして、ノードＮ３は、受信カウンタ値ＲＣ「０ｘ００００５６７８」を取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」で更新する。

[0039] （８）また、ノードＮ１は、ノードＮ２を宛先にするデータの送信イベントがあると、連結カウンタ値ＪＣ「０ｘ０１０００００１」に１を加算する。次に、ノードＮ１は、ノードＮ２を宛先にするデータと、加算後の連結カウンタ値ＪＣ「０ｘ０１０００００２」と、を含むバケツトを生成し、生成したパケットを固定鍵を用いて暗号化する。そして、ノードＮ１は、暗号化により得られた暗号化バケツトＥＰを、データの宛先になるノードＮ２に送信する。

[0040] （９）ノードＮ２は、ノードＮ１から暗号化パケットＥＰを受信すると、受信した暗号化バケツトＥＰの正当性の判断を行う。具体的には、ノードＮ２は、受信した暗号化パケットＥＰを、固定鍵を用いて復号する。次に、ノードＮ２は、復号により得られたパケットから連結カウンタ値ＪＣ「０ｘ０１０００００２」を取得する。そして、ノードＮ２は、前回受信した暗号化バケツトＥＰに含まれていた連結カウンタ値ＪＣを示す受信カウンタ値ＲＣ「０ｘ００００１２３０」と、取得した連結カウンタ値ＪＣ「０ｘ０１００

０００２」と、の大小比較を行う。

[0041] ここで、ノードN２は、取得した連結カウンタ値ＪＣが受信カウンタ値ＲＣよりも大きいため、受信した暗号化バケットＥＰは正規バケットであると判断する。そして、ノードN２は、受信カウンタ値ＲＣ「０ｘ０００１２３０」を取得した連結カウンタ値ＪＣ「０ｘ０１０００００２」で更新する。

[0042] このように、ノードN１は、連結カウンタ値ＪＣを保持し、連結カウンタ値ＪＣが消去されると、他ノードNに取得要求を送信することにより、消去以前の消去カウンタ値Ｒを他ノードNから取得する。そして、ノードN１は、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とする新たな連結カウンタ値ＪＣを生成する。これにより、過去にノードN１により送信された暗号化バケットＥＰに含まれていた連結カウンタ値ＪＣより、ノードN１により生成された新たな連結カウンタ値ＪＣが大きい値になる。そのため、ノードN１は、他ノードNが保持している受信カウンタ値ＲＣより大きい値になっている連結カウンタ値ＪＣを、他ノードNに送信する暗号化バケットＥＰに含むことができる。

[0043] 結果として、ノードN２およびノードN３は、保持している受信カウンタ値ＲＣより、ノードN１から受信した暗号化バケットＥＰに含まれる連結カウンタ値ＪＣが大きいため、ノードN１から受信した暗号化バケットＥＰを正規パケットと判断することができるようになる。そして、ノードN１は、他ノードNに送信する暗号化バケットＥＰが、他ノードNで不正バケットと判断されないようになるため、アドホックネットワークに復帰することができる。

[0044] また、従来のように、時刻情報を用いて不正パケットか否かを判断する場合、各ノードNが基準時刻との同期を、定期的または不定期に、アドホックネットワークを介して行う必要がある。この場合、時刻同期用のパケット量がアドホックネットワークに通信負荷をかける。一方、連結カウンタ値ＪＣは自ノードN内の処理のみで更新が可能な相対的な値であるから、各ノード

Nは、アドホックネットワークへの通信負荷を削減することができる。そのため、ノードN2およびノードN3は、時刻同期を必要とせずに、暗号化パケットEP内の連結カウンタ値JCが受信ごとに増加することを監視して、ノードN1から受信した暗号化バケットEPが不正バケットか否かを判断することができる。よって、アドホックネットワークには、時刻同期用のパケットによる通信負荷が生じない。さらに、不正パケットか否かの判断に時刻同期を必要としないため、時刻同期用のバケットを送信するゲートウェイが、アドホックネットワーク内に存在しなくてもよい。

[0045] なお、ノードN1は、送信カウンタ値Sが最大値「0xFFFFFF」になったとき、送信カウンタ値Sを初期値「0x000000」に戻してもよい。このとき、ノードN1は、ノードN2およびノードN3に、送信カウンタ値Sを初期値に戻したことを示すパケットを送信する。そして、ノードN2およびノードN3は、受信カウンタ値RC内の送信カウンタ値Sを、初期値に戻す。また、ノードN1は、消去カウンタ値Rが最大値「0xFF」になったとき、消去カウンタ値Rを初期値「0x00」に戻してもよい。このとき、ノードN1は、ノードN2およびノードN3に、消去カウンタ値Rを初期値に戻したことを示すパケットを送信する。そして、ノードN2およびノードN3は、受信カウンタ値RC内の消去カウンタ値Rを、初期値に戻す。

[0046] また、ノードN1は、送信カウンタ値Sが最大値「0xFFFFFF」になり、かつ、消去カウンタ値Rが最大値「0xFF」未満であり増加可能であるとき、送信カウンタ値Sを初期値「0x000000」に戻すとともに、消去カウンタ値Rに1を加算してもよい。これにより、過去にノードN1により送信された暗号化バケットEPに含まれていた連結カウンタ値JCより大きい値で、連結カウンタ値JCを更新することができる。結果として、ノードN1は、他ノードNに送信する暗号化パケットEPが、他ノードNで不正バケットと判断されないようになるため、アドホックネットワークに復帰することができる。このとき、ノードN1は、ノードN2およびノードN

3に、消去カウンタ値Ｒを初期値に戻したことを示すバケツトを送信しなくて済む。

[0047] なお、ノード2およびノード3は、ノードN１から受信した暗号化バケツトＥＰに含まれる連結カウンタ値ＪＣと保持している受信カウンタ値ＲＣとの差がしきい値以上である場合に、受信した暗号化バケツトＥＰを不正パケットと判断してもよい。これにより、ノードN１により過去に送信された暗号化バケツトＥＰ内の連結カウンタ値」Ｃを書き換えて攻撃者が再送攻撃に使用した場合に、書き換えにより消去カウンタ値Ｒが大きく変化していれば、不正パケットと判断することができる。

[0048] （ノードNのハードウエア構成例）

図２は、実施の形態にかかるノードNのハードウエア構成例を示すプロック図である。図２において、ノードNは、ＣＰＵ２０１と、ＲＡＭ２０２と、フラッシュメモリ２０３と、Ｉ/ Ｆ２０４と、暗号化回路２０５と、を備えている。ＣＰＵ２０１～暗号化回路２０５は、バス２００によってそれぞれ接続されている。

[0049] ここで、ＣＰＵ２０１は、ノードNの全体の制御を司る。ＲＡＭ２０２は、ＣＰＵ２０１のワークエリアとして使用される。ＲＡＭ２０２は、揮発性の記憶装置である。ＲＡＭ２０２には、書き換えが頻繁に行われる連結カウンタ値ＪＣや暗号鍵（例えばアクセス鍵）の鍵情報が記憶される。フラッシュメモリ２０３は、不揮発性の記憶装置である。フラッシュメモリ２０３には、プログラムや暗号鍵（例えば固定鍵）の鍵情報が記憶される。Ｉ/ Ｆ２０４は、ユニホップ通信またはマルチホップ通信によりパケットを送受信する。

[0050] 暗号化回路２０５は、暗号鍵を用いてデータを暗号化する回路である。また、暗号化回路２０５は、暗号化されたデータを復号鍵を用いて復号する回路でもある。暗号化および復号をソフトウエア的に実行する場合は、暗号化回路２０５に相当するプログラムをフラッシュメモリ２０３に記憶させておくことで、暗号化回路２０５は不要となる。

[0051] （ノードＤＢの記憶内容）

図３は、ノードＤＢ（ＤａｔａＢａｓｅ）の記憶内容の一例を示す説明図である。図３に示すように、ノードＤＢ３００は、ノード項目のそれぞれに対応付けて、アクセス鍵項目と、受信カウンタ値項目と、を有する。ノードＤＢ３００は、ノードＮが暗号化バケットＥＰを受信するごとにレコードを構成する。

[0052] ノード項目には、アドホックネットワーク内のノードＮを示す識別子が記憶される。例えば、識別子としては、ノード番号が採用できる。また、識別子としては、ノードＮ固有のネットワークアドレスであるＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスやＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスを採用してもよい。図３の例では、ノードＮ１が有するノードＤＢを示している。ここで、ノード項目には、他ノードＮのノード番号 (Ｎ２～）が記憶されている。

[0053] アクセス鍵項目には、ノード項目の識別子が示すノードＮから受信したアクセス鍵ＡＫが記憶される。アクセス鍵ＡＫは、ノード項目の識別子が示すノードＮへ送信するパケットの暗号化に使用される。アクセス鍵ＡＫは、例えば、１２８～２５６ビット程度のバイナリデータである。受信カウンタ値項目には、ノード項目の識別子が示すノードＮから受信した暗号化バケットＥＰに含まれる連結カウンタ値ＪＣが記憶される。

[0054] （ノードＮの機能的構成例）

次に、図４および図５を用いて、ノードＮの機能的構成例について説明する。ここで、図４は、ノードＮの送信側としての機能的構成例を示している。また、図５は、ノードＮの受信側としての機能的構成例を示している。ここでは、便宜的に受信側としての機能と送信側としての機能を分けて説明しているが、ノードＮは受信側としての機能および送信側としての機能の両方を有する。

[0055] 図４は、ノードＮの送信側としての機能的構成例を示す機能ブロック図である。図４に示すように、ノードＮは、第１の記憶部４０１と、更新部４０

２と、送信部４０３と、暗号化部４０４と、乱数生成部４０５と、検出部４０６と、受信部４０７と、復号部４０８と、生成部４０９と、保存部４１０と、第２の記憶部４１１と、抽出部４１２と、を備える。更新部４０２ー保存部４１０および抽出部４１２は、具体的には、例えば、図２に示したフラッシュメモリ２０３などの記憶装置に記憶されたプログラムをＣＰＵ２０１に実行させることにより、または、Ｉ/ Ｆ２０４により、その機能を実現する。

[0056] 第１の記憶部４０１は、自ノー ドNでの消去回数を示す消去カウンタ値Ｒを上位桁とし自ノー ドNからの送信回数を示す送信カウンタ値Ｓを下位桁とする連結カウンタ値ＪＣを記憶する。具体的には、例えば、頻繁に書き換えが行われる連結カウンタ値ＪＣを記憶するため、データの読み書きを高速に行うことができる揮発性の記憶装置が採用される。第１の記憶部４０１は、例えば、上述したＲＡＭ２０２である。例えば、図１では、ノー ドN１の第１の記憶部４０１（ＲＡＭ２０２）は、連結カゥンタ値ＪＣ 「０ｘ００００５６７８」を保持している。

[0057] 更新部４０２は、アドホックネットワーク内の他ノー ドNにデータを送信する場合、第１の記憶部４０１に記憶されている連結カウンタ値ＪＣのうち送信カウンタ値Ｓを１加算する。ここで、データとは、例えば、ノー ドNが家庭に備え付けられた消費電力計である場合は、当該家庭の消費電力量である。データの送信は、送信イベントの発生をトリガに実行される。送信ィベントは、例えば、ノー ドNのユーザからの他ノー ドNを宛先にするデータの入力を受けることにより発生する。また、送信イベントは、ノー ドNが、一定時間ごとに自動的に発生させてもよい。

[0058] 更新部４０２は、具体的には、例えば、アドホックネットワーク内の他ノ- ドNを宛先にするデータの送信ィベントが検出された場合、ＲＡＭ２０２に保持されている連結カウンタ値ＪＣに１を加算する。これにより、更新部４０２は、ＲＡＭ２０２に保持されている連結カウンタ値ＪＣのうち送信カゥンタ値Ｓを、最新の送信カウンタ値Ｓに更新することができる。例えば、

図１の（6）では、ノードN１の更新部４０２は、送信に先立って、連結カウンタ値ＪＣ「0ｘ０１０００００００」に１を加算し、連結カウンタ値ＪＣ「0ｘ０１０００００１」に更新している。

[0059] 送信部４０３は、データおよび更新部４０２による更新後の連結カウンタ値ＪＣを他ノードNに送信する。送信部４０３は、具体的には、例えば、他ノードNを宛先とするデータと更新部４０２による更新後の連結カウンタ値ＪＣとを含むパケットを生成する。そして、送信部４０３は、生成したパケットを、データの宛先である他ノードNに送信する。ここで、パケットには、送信元である自ノードNを示す識別子が含まれてもよい。なお、ここでは、送信部４０３は、生成したパケットを、他ノードNにユニキャスト送信している。例えば、図１の（6）では、ノードN１の送信部４０３は、暗号化バケットＥＰを送信しているが、連結カウンタ値ＪＣ「0ｘ０１０００００１」を含む暗号化されないバケットをノードN３に送信してもよい。

[0060] なお、パケットの他ノードNへのユニキャスト送信は、送信部４０３がパケットを近隣ノードNに配信し、宛先の他ノードN以外の近隣ノードNが受信したバケットを廃棄し、宛先になる他ノードNが受信したバケットの内容に従って処理を実行することで実現される。ここで、処理としては、例えば、バケットのＲＡＭ２０２やフラッシュメモリ２０３への保存が挙げられる。これにより、送信部４０３は、正当性の判断に使用する連結カウンタ値ＪＣを含むパケットを、他ノードNに送信することができる。例えば、図１の（６）で、ノードN１の送信部４０３は、近隣ノードとなるノードN２およびノードN３に、ノードN３を宛先にする暗号化バケットＥＰを送信する。そして、ノードN２は、自ノードNが宛先でないため、受信した暗号化パケットＥＰを廃棄する。また、ノードN３は、受信した暗号化パケットＥＰの内容に従って処理を行う。

[0061] また、送信部４０３は、暗号化部４０４と乱数生成部４０５とを有する。暗号化部４０４は、自ノードNおよび他ノードNが有する共通鍵を用いて、データおよび更新部４０２による更新後の連結カウンタ値ＪＣを暗号化する

。ここで、自ノードNおよび他ノードNが有する共通鍵とは、例えば、アドホックネットワーク内のノードNで共有される共通鍵（固定鍵）であってもよいし、ノードN間で一定時間ごとに更新される共通鍵（アクセス鍵ＡＫ）であってもよい。

[0062] ここで、一定時間ごとに更新されるアクセス鍵ＡＫのほうが固定鍵よりセキュアであるため、アクセス鍵ＡＫを有しているときは、アクセス鍵Ａべが暗号化部４０４による暗号化に用いられる。一方、アクセス鍵ＡＫを有していないときは、固定鍵が暗号化部４０４による暗号化に用いられる。例えば、図１で、停電によりノードN１に電力供給されなくなったため、ＲＡＭ２０２に保持されていたアクセス鍵ＡＫが消去され、フラッシュメモリ２０３に保持されていた固定鍵が残っている状態であれば、固定鍵が暗号化部４０４による暗号化に用いられる。

[0063] 暗号化部４０４は、具体的には、例えば、送信部４０３によって生成されたバケツト内の他ノードNを宛先とするデータと更新部４０２による更新後の連結カウンタ値」Ｃとを、固定鍵またはアクセス鍵ＡＫを用いて暗号化する。例えば、図１の（6）または（8）では、ノードN１の暗号化部４０４は、連結カウンタ値ＪＣを含むバケツトを固定鍵を用いて暗号化している。ここで、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に、送信元である自ノードNを示す識別子が含まれてもよい。

[0064] この場合、送信部４０３は、暗号化部４０４による暗号化により得られた暗号化パケットＥＰを、データの宛先である他ノードNに送信する。これにより、送信部４０３は、正当性の判断に使用する連結カウンタ値ＪＣを含むパケットを、他ノードNに送信することができる。また、送信部４０３は、暗号化により得られた暗号化バケツトＥＰを送信するため、通信の安全性を担保することができる。例えば、図１の（6）では、ノードN１の送信部４０３は、連結カウンタ値ＪＣ「0ｘ０１０００００１」を含む暗号化バケツトＥＰを、ノードN３に送信している。また、図１の（8）では、送信部４０３は、連結カウンタ値ＪＣ「0ｘ０１０００００２」を含む暗号化バケツ

トＥＰを、ノードＮ２に送信している。

[0065] 乱数生成部４０５は、第１の識別情報となる乱数を生成する。ここで、第１の識別情報とは、通信ごとに生成される一時的な乱数である。乱数生成部４０５は、具体的には、例えば、ハードウェア乱数生成器を用いて乱数を生成する。なお、生成された乱数は、例えば、ＲＡＭ２０２などの記憶領域に記憶される。例えば、図１の (2) では、乱数が生成されていないが、ノードＮ１の乱数生成部４０５は乱数を生成してもよい。

[0066] 検出部４０６は、第１の記憶部４０１での連結カウンタ値ＪＣの消去を検出する。検出部４０６は、具体的には、例えば、停電によりノードＮに電力が供給されずに第１の記憶部４０１に保持されている連結カウンタ値ＪＣが消去された場合、停電が回復しノードＮに電力供給された後に連結カゥンタ値ＪＣが消去されていることを検出する。検出部４０６は、より具体的には、例えば、連結カウンタ値ＪＣの保持先に設定されている記憶領域の記憶内容が、電力供給されたときの初期化処理により「０ｘ００００００００」になっていることを検出する。

[0067] また、検出部４０６は、ノードＮのユーザによる操作により、第１の記憶部４０１に保持されている連結カウンタ値ＪＣが初期化されたことを検出してもよい。これにより、検出部４０６は、以後送信するパケットに含むべき連結カウンタ値ＪＣが不明になったことを検出し、アドホックネットワークへの復帰処理を開始するトリガを発生させることができる。ノードＮ１の検出部４０６は、例えば、図１の (1) においては、連結カウンタ値ＪＣが消去されたことを検出している。

[0068] 検出部４０６によって連結カウンタ値ＪＣの消去が検出された場合、暗号化バケツトＥＰを他ノードＮに正規バケツトと判断させるための連結カウンタ値ＪＣが不明であるため、連結カウンタ値ＪＣを復旧する必要がある。復旧する方法としては、例えば、下記の３通りの方法がある。

[0069] 第１の復旧方法は、他ノードＮに消去カウンタ値Ｒの取得要求を送信することにより、連結カウンタ値ＪＣを復旧する方法である。第２の復旧方法は

、取得要求ではなく、消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒの取得を要求する更新要求を送信することにより、連結カウンタ値」Ｃを復旧する方法である。第３の復旧方法は、消去カウンタ値Ｒを揮発性メモリではなく不揮発性の第２の記憶部４１１に保存しておくことにより、消去カウンタ値Ｒを読み出して連結カウンタ値ＪＣを復旧する方法である。ここでは、第１の復旧方法について説明し、第２，第３の復旧方法については後述する。

[0070] 第１の復旧方法では、送信部４０３は、検出部４０６によって消去が検出された場合、消去カウンタ値Ｒの取得要求をアドホックネットワークに配信する。ここで、取得要求とは、他ノードNに、自ノードNが過去に送信した送信カゥンタ値Ｓを示す他ノードNが保持している受信カゥンタ値ＲＣから消去カウンタ値Ｒを抽出させて、抽出させた消去カウンタ値Ｒを自ノードNへ送信させるためのリクエストである。

[0071] そして、送信部４０３は、具体的には、例えば、取得要求を含むパケットを生成し、生成したパケットを、他ノードNに送信する。ここで、パケットには、送信元である自ノードNを示す識別子が含まれてもよい。例えば、図１の（２）では、ノードＮ１の送信部４０３は、取得要求を含む暗号化パケットＥＰをノードＮ２に送信しているが、取得要求を含む暗号化されないパケットを送信してもよい。これにより、送信部４０３は、消去カウンタ値Ｒを取得要求元のノードNへ送信するトリガを他ノードNに与えることができる。

[0072] ここで、通信の安全性を担保するために、送信部４０３によって送信されるパケットは、暗号化されていてもよい。また、通信の安全性を担保するために、送信部４０３によって送信されるパケットは、さらに一時的な識別情報が含まれた上で、暗号化されていてもよい。一時的な識別情報とは、例えば、上述した乱数生成部４０５によって生成された乱数である。まず、送信部４０３によって送信されるバケツトが暗号化されている場合について説明する。

[0073] この場合、暗号化部４０４は、具体的には、例えば、送信部４０３によつて生成されたバケツト内の取得要求を、固定鍵またはアクセス鍵ＡＫを用いて暗号化する。例えば、図１の (2) では、ノードN１の暗号化部４０４は、取得要求を含むパケットを固定鍵を用いて暗号化している。ここで、パケット内の暗号化されない部分 (例えば、パケットのヘッダ部分) に、送信元である自ノードNを示す識別子が含まれてもよい。

[0074] そして、送信部４０３は、暗号化部４０４によって暗号化された取得要求をアドホックネットワークに配信する。具体的には、例えば、送信部４０３は、暗号化部４０４による暗号化により得られた取得要求を含む暗号化パケットEＰを、他ノードNに送信する。例えば、図１の (2) では、ノードN１の送信部４０３は、取得要求を含む暗号化バケツトEＰをノードN２に送信している。なお、送信部４０３は、暗号化パケットEＰを、近隣ノードNにマルチキャストで送信してもよいし、他ノードNにユニキャストで送信してもよい。

[0075] これにより、送信部４０３は、消去カウンタ値Ｒを取得要求元のノードNへ送信するトリガを他ノードNに与えることができる。また、送信部４０３は、暗号化により得られた暗号化パケットEＰを送信するため、通信の安全性を担保することができる。

[0076] 次に、通信の安全性を担保するために、送信部４０３によって送信されるバケツトが一時的な識別情報を含んだ上で、暗号化されている場合について説明する。この場合、送信部４０３は、取得要求と乱数生成部４０５によつて生成された乱数とを含むパケットを生成する。例えば、図１の (2) では、取得要求を含むバケツトが生成されているが、ノードN１の送信部４０３は、乱数と取得要求とを含むバケツトを生成してもよい。

[0077] また、この場合、暗号化部４０４は、自ノードNおよび他ノードNが有する共通鍵を用いて、自ノードN固有の第１の識別情報を含む取得要求を暗号化する。暗号化部４０４は、具体的には、例えば、送信部４０３によって生成された取得要求と乱数とを含むバケツトを、固定鍵またはアクセス鍵ＡＫ

を用いて暗号化する。例えば、図１の (2) では、取得要求を含むパケットが暗号化されているが、ノードN１の暗号化部４０４は、取得要求と乱数とを含むバケットを固定鍵を用いて暗号化してもよい。

[0078] この場合、送信部４０３は、暗号化部４０４による暗号化により得られた暗号化パケットＥＰを他ノードに送信する。例えば、図１の (2) では、取得要求を含む暗号化バケットＥＰが送信されているが、ノードN１の送信部４０３は、乱数と取得要求を含む暗号化バケットＥＰを送信してもよい。

[0079] なお、取得要求により消去カウンタ値Ｒが取得されてから、連結カウンタ値ＪＣが復旧するまでの処理については後述する。

[0080] 受信部４０７は、他ノードNから送信されたデータを受信する。受信部４０７は、具体的には、例えば、送信部４０３によって送信された要求 (例えば、取得要求) に対する他ノードNからの応答を受信する。受信部４０７は、より具体的には、例えば、送信部４０３によって取得要求が配信された結果、アドホックネットワークから消去カウンタ値Ｒを受信する。これにより、受信部４０７は、新たな連結カウンタ値ＪＣの生成に使用される消去以前の消去カウンタ値Ｒを取得することができる。

[0081] また、受信部４０７は、復号部４０８を有する。復号部４０８は、共通鍵を用いて暗号化されたデータを、共通鍵を用いて復号する。また、復号部４０８は、アクセス鍵ＡＫを用いて暗号化されたデータを、アクセス鍵ＡＫを用いて復号する。

[0082] ここで、通信の安全性を担保するために、受信部４０７によって受信される消去カウンタ値Ｒを含むパケットは、暗号化されていてもよい。この場合、復号部４０８は、受信部４０７によって受信された消去カウンタ値Ｒを含む暗号化パケットＥＰを、共通鍵を用いて復号する。

[0083] この場合、受信部４０７は、復号部４０８による復号により得られたパケットから、消去カウンタ値Ｒを取得する。これにより、受信部４０７は、新たな連結カウンタ値ＪＣの生成に使用される消去以前の消去カウンタ値Ｒを取得することができる。例えば、図１の (5) では、ノードN１の受信部４

０７は、ノードＮ２から消去カウンタ値Ｒ「０ｘ００」を含む暗号化バケットＥＰを受信している。なお、復号により得られたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0084] また、受信部４０７は、送信部４０３によって第１の識別情報を含む暗号化バケットＥＰが送信された結果、共通鍵を用いて暗号化された消去カウンタ値Ｒと共通鍵を用いて暗号化された第２の識別情報とを、アドホックネットワークから受信する。ここで、第２の識別情報とは、送信部４０３によつて送信された第１の識別情報を含む暗号化バケットＥＰを受信したノードＮで生成されるデータであり、第１の識別情報がそのまま第２の識別情報として使用される。第２の識別情報とは、例えば、乱数である。

[0085] 受信部４０７は、具体的には、例えば、送信部４０３によって取得要求が配信された結果、固定鍵を用いて暗号化された消去カウンタ値Ｒと乱数とを含む暗号化パケットＥＰを受信する。ここで、暗号化パケットＥＰ内の暗号化されない部分 (例えば、暗号化パケットＥＰのヘッダ部分)に、送信元である他ノードＮを示す識別子が含まれてもよい。

[0086] 例えば、図１の (5) では、消去カウンタ値Ｒ「０ｘ００」を含む暗号化パケットＥＰが受信されているが、ノードＮ１の受信部４０７は、消去カウンタ値Ｒ「０ｘ００」と乱数を含む暗号化パケットＥＰを受信してもよい。なお、受信された暗号化パケットＥＰは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0087] また、この場合、復号部４０８は、具体的には、例えば、受信部４０７によつて受信された消去カゥンタ値Ｒと第２の識別情報を含む暗号化パケットＥＰを、共通鍵を用いて復号する。そして、受信部４０７は、復号部４０８による復号により得られたバケットから、消去カウンタ値Ｒと第２の識別情報とを取得する。例えば、図１の (5) では、消去カウンタ値Ｒを含む暗号化パケットＥＰを復号したが、ノードＮ１の復号部４０８は、消去カウンタ値Ｒと乱数とを含む暗号化パケットＥＰを復号してもよい。そして、復号部４０８は、復号により得られたパケットから、消去カウンタ値Ｒと乱数とを

取得してもよい。

[0088] これにより、受信部４０７は、新たな連結カウンタ値ＪＣの生成に使用される消去以前の消去カウンタ値Ｒを取得することができる。また、受信部４０７は、第１の識別情報との一致判断により受信したバケツトの正当性判断に使用される第２の識別情報を取得することができる。なお、復号により得られたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0089] 生成部４０９は、受信部４０７によって受信された消去カウンタ値Ｒに１加算した加算後の消去カウンタ値Ｒを上位桁とし、消去により送信回数が０になったことを示す消去後の送信カウンタ値Ｓを下位桁とする連結カウンタ値ＪＣを生成する。生成部４０９は、具体的には、例えば、受信部４０７によって受信された消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とし、送信カウンタ値Ｓの初期値を下位桁とする連結カウンタ値ＪＣを生成する。

[0090] 例えば、図１の (5) では、ノードN１の生成部４０９は、受信した消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒ 「０ｘ０１」と送信カウンタ値Ｓの初期値 「０ｘ００００００」を連結した連結カウンタ値ＪＣ 「０ｘ０１０００００」を生成している。これにより、生成部４０９は、消去以前の連結カゥンタ値ＪＣより大きい値であつて、以後送信するパケットに含むべき連結カウンタ値ＪＣを生成することができる。

[0091] また、この場合、生成部４０９は、第１の識別情報と復号部４０８によつて復号された第２の識別情報との一致判断を行う。生成部４０９は、一致した場合に、復号部４０８によって復号された消去カウンタ値Ｒに１加算した加算後の消去カゥンタ値Ｒを上位桁とし消去により送信回数が０になったことを示す消去後の送信カウンタ値Ｓを下位桁とする連結カウンタ値ＪＣを生成する。

[0092] 生成部４０９は、具体的には、例えば、ＲＡＭ２０２に保持されている乱数と受信部４０７によって取得された乱数との一致判断を行う。そして、生成部４０９は、一致すると判断された場合、受信部４０７によって取得され

た消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とし、送信カウンタ値Ｓの初期値を下位桁とする連結カウンタ値ＪＣを生成する。例えば、図１の (5) では、乱数を用いた暗号化パケットＥＰの正当性の判断は行わなかったが、ノードＮ１の生成部４０９は、送信した暗号化パケットＥＰに含めた乱数と受信した乱数との一致判断から、暗号化パケットＥＰが不正パケットか否かを判断してもよい。これにより、生成部４０９は、消去以前の連結カウンタ値ＪＣより大きい値であつて、以後送信するパケットに含むべき連結カウンタ値ＪＣを生成することができる。

[0093] 保存部４１０は、生成部４０９によって生成された連結カウンタ値ＪＣを第１の記憶部４０１に保存する。保存部４１０は、具体的には、生成部４０９によって生成された連結カウンタ値ＪＣを、消去された連結カウンタ値ＪＣの代わりにＲＡＭ２０２に保存する。例えば、図１の (5) では、ノードＮ１の保存部４１０は、消去された連結カウンタ値の代わりに、生成した連結カウンタ値ＪＣ 「０ｘ０１０００００００」を保存している。

[0094] 第２の記憶部４１１は、消去カウンタ値Ｒを記憶する。第２の記憶部４１１としては、具体的には、例えば、不揮発性の記憶装置が採用される。第２の記憶部４１１とは、例えば、上述したフラッシュメモリ２０３である。例えば、図１では、連結カウンタ値ＪＣのみが保持されているが、ノードＮ１の第２の記憶部４１１は、消去カウンタ値Ｒを連結カウンタ値ＪＣとは別に保持していてもよい。これにより、第２の記憶部４１１は、自ノードＮに電力が供給されない状態であっても、消去カウンタ値Ｒを記憶しておくことができる。

[0095] 抽出部４１２は、検出部４０６によって消去が検出された場合、第２の記憶部４１１から消去カウンタ値Ｒを抽出する。抽出部４１２は、具体的には、例えば、検出部４０６によって消去が検出された場合、フラッシュメモリ２０３から消去カウンタ値Ｒを読み出す。例えば、図１では、他ノードＮから消去カウンタ値Ｒを取得したが、ノードＮ１の抽出部４１２は、自ノードＮ内のフラッシュメモリ２０３から、消去カウンタ値Ｒを抽出してもよい。

これにより、抽出部４１２は、消去以前の消去カウンタ値Ｒを抽出することができる。なお、抽出された消去カウンタ値Ｒは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0096] 次に、第２の復旧方法について説明する。第２の復旧方法は、取得要求ではなく、消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒの取得を要求する更新要求を送信することにより、連結カウンタ値ＪＣを復旧する方法である。第２の復旧方法は、送信部４０３と、暗号化部４０４と、乱数生成部４０５と、受信部４０７と、復号部４０８と、生成部４０９と、保存部４１０と、によって実行される。

[0097] 具体的には、送信部４０３は、検出部４０６によって消去が検出された場合、消去カウンタ値Ｒの更新要求をアドホックネットワークに配信する。ここで、更新要求とは、他ノードNに、自ノードNが過去に送信した送信カウンタ値Ｓを示す受信カウンタ値ＲＣから、消去カウンタ値Ｒを抽出させる要求である。また、更新要求とは、他ノードNに、抽出させた消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを自ノードNへ送信させる要求である。

[0098] そして、送信部４０３は、具体的には、例えば、更新要求を含むパケットを生成する。そして、送信部４０３は、生成したパケットを、他ノードNに送信する。ここで、パケットには、送信元である自ノードNを示す識別子が含まれてもよい。例えば、図１の (2) では、取得要求を含むパケットが生成されたが、ノードN１の送信部４０３は、取得要求ではなく更新要求を含むパケットを生成してもよい。そして、図１の (2) では、暗号化パケットＥＰがノードN２に送信されたが、ノードN１の送信部４０３は、更新要求を含む暗号化されないバケツトをノードN２に送信してもよい。これにより、送信部４０３は、消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを更新要求元のノードNへ送信するトリガを他ノードNに与えることができる。

[0099] ここで、通信の安全性を担保するために、送信部４０３によって送信され

るパケットは、暗号化されていてもよい。また、送信部４０３によって送信されるパケットは、さらに一時的な識別情報が含まれた上で、暗号化されていてもよい。まず、送信部４０３によって送信されるパケットが暗号化されている場合について説明する。

[01 00] この場合、暗号化部４０４は、自ノードNおよび他ノードNが有する共通鍵を用いて、更新要求を暗号化する。暗号化部４０４は、具体的には、例えば、送信部４０３によって生成された更新要求を含むパケットを、固定鍵またはアクセス鍵ＡＫを用いて暗号化する。例えば、図１の (2) では、取得要求を含むバケツトが暗号化されたが、ノードN１の暗号化部４０４は、更新要求と乱数を含むバケツトを暗号化してもよい。

[01 01] そして、送信部４０３は、暗号化部４０４によって暗号化された更新要求をアドホックネットワークに配信する。送信部４０３は、具体的には、例えば、暗号化部４０４による暗号化により得られた更新要求を含む暗号化パケットＥＰを、他ノードNに送信する。なお、送信部４０３は、暗号化バケツトＥＰを、近隣ノードNにマルチキャスト送信してもよいし、他ノードNにユニキャスト送信してもよい。例えば、図１の (2) では、取得要求を含む暗号化パケットＥＰが送信されたが、ノードN１の送信部４０３は、更新要求を含む暗号化バケツトＥＰをノードN２に送信してもよい。

[01 02] これにより、送信部４０３は、消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを更新要求元のノードNへ送信するトリガを他ノードNに与えることができる。また、送信部４０３は、暗号化により得られた暗号化バケツトＥＰを送信するため、通信の安全性を担保することができる。

[01 03] また、この場合、受信部４０７は、送信部４０３によって更新要求が配信された結果、アドホックネットワークから消去カウンタ値Ｒに１加算された加算後の消去カウンタ値Ｒを受信する。受信部４０７は、具体的には、例えば、送信部４０３によって更新要求が配信された結果、加算後の消去カウンタ値Ｒを含む暗号化パケットＥＰを受信する。ここで、暗号化パケットＥＰ内の暗号化されない部分 (例えば、暗号化パケットＥＰのヘッダ部分) に、

送信元である他ノードNを示す識別子が含まれてもよい。なお、受信された暗号化パケットＥＰは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。例えば、図１の (4) では、消去カウンタ値Ｒ「0ｘ００」を含む暗号化パケットＥＰが受信されたが、ノードＮ１の受信部４０７は、加算後の消去カウンタ値Ｒ「0ｘ０１」を含む暗号化パケットＥＰを受信してもよい。

[01 04] また、この場合、復号部４０８は、具体的には、例えば、受信部４０７によつて受信された加算後の消去カゥンタ値Ｒを含む暗号化パケットＥＰを、共通鍵を用いて復号する。そして、受信部４０７は、復号部４０８による復号により得られたパケットから、消去カウンタ値Ｒを取得する。これにより、受信部４０７は、新たな連結カウンタ値ＪＣの生成に使用される消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを取得することができる。

[01 05] なお、復号により得られたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。例えば、図１の (4) では、消去カウンタ値Ｒ「0ｘ００」を含む暗号化パケットＥＰを復号したが、ノードＮ１の復号部４０８は、加算後の消去カウンタ値Ｒ「0ｘ０１」を含む暗号化パケットＥＰを復号してもよい。そして、ノードＮ１の受信部４０７は、復号したパケット内の加算後の消去カウンタ値Ｒを取得する。

[01 06] また、この場合、生成部４０９は、受信部４０７によって受信された加算後の消去カウンタ値Ｒを上位桁とし、消去により送信回数が０になったことを示す消去後の送信カウンタ値Ｓを下位桁とする連結カウンタ値ＪＣを生成する。

[01 07] 具体的には、例えば、生成部４０９は、受信部４０７によって取得された加算後の消去カゥンタ値Ｒを上位桁とし、送信カゥンタ値Ｓの初期値を下位桁とする連結カウンタ値ＪＣを生成する。例えば、図１の (5) では、受信した消去カウンタ値Ｒ「0ｘ００」に１を加算して得た加算後の消去カウンタ値Ｒ「0ｘ０１」を用いて連結カウンタ値を生成したが、ノードＮ１の生成部４０９は、受信した加算後の消去カウンタ値Ｒ「0ｘ０１」を用いて連

結カウンタ値を生成してもよい。これにより、生成部４０９は、消去以前の連結カウンタ値ＪＣより大きい値であって、以後送信するバケツトに含むべき連結カウンタ値ＪＣを生成することができる。なお、生成された連結カウンタ値ＪＣは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 08] この場合、保存部４１０は、生成部４０９によって生成された連結カウンタ値ＪＣを第１の記憶部４０１に保存する。保存部４１０は、具体的には、生成部４０９によって生成された連結カウンタ値ＪＣを、消去された連結カゥンタ値ＪＣの代わりにＲＡＭ２０２に保存する。

[01 09] 上述のように、送信部４０３によって送信されるパケットは、暗号化されていてもよいが、さらに一時的な識別情報を含んでもよい。次に、送信部４０３によって送信されるバケツトが一時的な識別情報を含んだ上で、暗号化されている場合について説明する。

[01 10] この場合、送信部４０３は、乱数生成部４０５によって生成された一時的な識別情報になる乱数と更新要求とを含むパケットを生成する。例えば、図１の (2) では、取得要求を含むパケットが生成されたが、ノードＮ１の送信部４０３は、乱数と更新要求とを含むバケツトを生成してもよい。

[01 11] そして、暗号化部４０４は、自ノードＮおよび他ノードＮが有する共通鍵を用いて、自ノードＮ固有の第１の識別情報を含む更新要求を暗号化する。暗号化部４０４は、具体的には、例えば、送信部４０３によって生成された更新要求と乱数とを含むバケツトを、固定鍵またはアクセス鍵ＡＫを用いて暗号化する。例えば、図１の (2) では、取得要求を含むパケットが暗号化されたが、ノードＮ１の暗号化部４０４は、乱数と更新要求を含むバケツトを暗号化してもよい。

[01 12] そして、送信部４０３は、暗号化部４０４による暗号化により得られた暗号化パケットＥＰを他ノードＮに送信する。例えば、図１の (2) では、取得要求を含む暗号化バケツトＥＰが送信されたが、ノードＮ１の送信部４０３は、乱数と更新要求を含む暗号化バケツトＥＰを送信してもよい。

[01 13] これにより、送信部４０３は、消去カウンタ値Ｒに１を加算した加算後の

消去カウンタ値Ｒを更新要求元のノードNへ送信するトリガを他ノードNに与えることができる。また、送信部４０３は、暗号化により得られた暗号化パケットＥＰを送信するため、通信の安全性を担保することができる。また、送信部４０３は、送信するパケットに一時的な識別情報を含むことにより、通信の安全性を担保することができる。

[01 14] また、この場合、受信部４０７は、共通鍵を用いて暗号化された加算後の消去カウンタ値Ｒと共通鍵を用いて暗号化された第２の識別情報とを、アドホックネットワークから受信する。具体的には、例えば、受信部４０７は、送信部４０３によって更新要求が配信された結果、固定鍵を用いて暗号化された加算後の消去カウンタ値Ｒと乱数とを含む暗号化バケツトＥＰを受信する。ここで、暗号化パケットＥＰ内の暗号化されない部分 (例えば、暗号化パケットＥＰのヘッダ部分）に、送信元である他ノードNを示す識別子が含まれてもよい。例えば、図１の (5）では、消去カウンタ値Ｒ 「0ｘ００」を含む暗号化パケットＥＰが受信されたが、ノードＮ１の受信部４０７は、加算後の消去カウンタ値Ｒ 「0ｘ０１」と乱数を含む暗号化パケットＥＰを受信してもよい。なお、受信された暗号化パケットＥＰは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 15] また、この場合、復号部４０８は、具体的には、例えば、受信部４０７によって受信された加算後の消去カウンタ値Ｒと第２の識別情報を含む暗号化パケットＥＰを、共通鍵を用いて復号する。そして、受信部４０７は、復号部４０８による復号により得られたバケツトから、加算後の消去カウンタ値Ｒと第２の識別情報とを取得する。例えば、図１の (5）では、消去カウンタ値Ｒを含む暗号化バケツトＥＰが復号されたが、ノードＮ１の復号部４０８は、加算後の消去カウンタ値Ｒと乱数とを含む暗号化バケツトＥＰを復号してもよい。そして、復号部４０８は、復号により得られたパケットから、加算後の消去カウンタ値Ｒ 「0ｘ０１」と乱数とを取得してもよい。

[01 16] これにより、受信部４０７は、新たな連結カウンタ値ＪＣの生成に使用される消去以前の消去カゥンタ値Ｒに１を加算した加算後の消去カゥンタ値Ｒ

を取得することができる。また、受信部４０７は、第１の識別情報との一致判断により受信したバケツトの正当性判断に使用される第２の識別情報を取得することができる。なお、復号により得られたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 17] また、この場合、生成部４０９は、第１の識別情報と復号部４０８によつて復号された第２の識別情報との一致判断を行う。そして、生成部４０９は、一致した場合に、復号部４０８によって復号された加算後の消去カウンタ値Ｒを上位桁とし、消去により送信回数が０になったことを示す消去後の送信カウンタ値Ｓを下位桁とする連結カウンタ値ＪＣを生成する。

[01 18] また、この場合、生成部４０９は、具体的には、例えば、ＲＡＭ２０２に保持されている乱数と受信部４０７によって取得された乱数との一致判断を行う。そして、生成部４０９は、一致すると判断された場合、受信部４０７によって受信された加算後の消去カゥンタ値Ｒを上位桁とし、送信カゥンタ値Ｓの初期値を下位桁とする連結カウンタ値ＪＣを生成する。

[01 19] 例えば、図１の (5) では、乱数を用いた暗号化パケットＥＰの正当性の判断を行わなかったが、ノードＮ１の生成部４０９は、受信した暗号化パケットＥＰに含まれている乱数と保持しておいた乱数との一致判断を行ってもよい。そして、生成部４０９は、一致した場合、暗号化パケットＥＰが正規パケットと判断して、受信した消去カウンタ値Ｒ「０ｘ０１」と送信カウンタ値Ｓの初期値「０ｘ０００００００」を連結した連結カウンタ値ＪＣ「０ｘ０１０００００００」を生成する。

[01 20] これにより、生成部４０９は、消去以前の連結カウンタ値ＪＣより大きい値であって、以後送信するバケツトに含むべき連結カウンタ値ＪＣを生成することができる。なお、生成された連結カウンタ値ＪＣは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 21] この場合、保存部４１０は、生成部４０９によって生成された連結カウンタ値ＪＣを第１の記憶部４０１に保存する。保存部４１０は、具体的には、生成部４０９によって生成された連結カウンタ値ＪＣを、消去された連結カ

ゥンタ値ＪＣの代わりにＲＡＭ２０２に保存する。

[01 22] 次に、第３の復旧方法について説明する。第３の復旧方法は、消去カウンタ値Ｒを揮発性メモリではなく不揮発性の第２の記憶部４１１に保存しておくことにより、消去カウンタ値Ｒを読み出して連結カウンタ値ＪＣを復旧する方法である。第３の復旧方法は、生成部４０９と、保存部４１０と、第２の記憶部４１１と、抽出部４１２と、により実行される。

[01 23] 抽出部４１２は、具体的には、例えば、検出部４０６によって消去が検出された場合、第２の記憶部４１１から消去カウンタ値Ｒを抽出する。抽出部４１２は、具体的には、例えば、検出部４０６によって消去が検出された場合、フラッシュメモリ２０３から消去カウンタ値Ｒを読み出す。例えば、図１では、他ノードNから消去カウンタ値Ｒを取得したが、ノードＮ１の抽出部４１２は、自ノードN内のフラッシュメモリ２０３から、消去カウンタ値Ｒを抽出してもよい。これにより、抽出部４１２は、消去以前の消去カウンタ値Ｒを抽出することができる。なお、抽出された消去カウンタ値Ｒは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 24] この場合、生成部４０９は、抽出部４１２によって抽出された消去カウンタ値Ｒに１加算した加算後の消去カウンタ値Ｒを上位桁とし消去により送信回数が０になったことを示す消去後の送信カウンタ値Ｓを下位桁とする連結カウンタ値ＪＣを生成する。

[01 25] 具体的には、例えば、生成部４０９は、抽出部４１２によって抽出された消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とし、送信カウンタ値Ｓの初期値を下位桁とする連結カウンタ値ＪＣを生成する。例えば、ノードＮ１の生成部４０９は、図１の (5) で、他ノードNから受信した消去カウンタ値Ｒではなく、抽出した消去カウンタ値Ｒ 「０ｘ００」に１を加算する。そして、生成部４０９は、加算後の消去カウンタ値Ｒ 「０ｘ０１」と送信カウンタ値Ｓの初期値 「０ｘ０００００００」を連結した連結カウンタ値ＪＣ 「０ｘ０１０００００００」を生成する。

[01 26] これにより、生成部４０９は、消去以前の連結カウンタ値ＪＣより大きい

値であって、以後送信するバケツトに含むべき連結カウンタ値ＪＣを生成することができる。なお、生成された連結カウンタ値ＪＣは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 27] また、この場合、保存部４１０は、生成部４０９によって生成された連結カウンタ値ＪＣを第１の記憶部４０１に保存するとともに、第２の記憶部４１１に記憶されている消去カウンタ値Ｒに対し加算後の消去カウンタ値Ｒを上書き保存する。例えば、図１の (5) で、ノードN１の保存部４１０は、消去された連結カウンタ値の代わりに、生成した連結カウンタ値ＪＣ「Ｏｘ０１０００００」を保存してもよい。これにより、保存部４１０は、以後送信するバケツトに含むべき連結カウンタ値ＪＣを保存することができる。また、保存部４１０は、フラッシュメモリ２０３に保持されている消去カウンタ値Ｒを、最新の消去カゥンタ値Ｒに更新することができる。

[01 28] また、受信部４０７は、上述した暗号化部４０４による暗号化または復号部４０８による復号に使用されるアクセス鍵ＡＫを、他ノードNから受信する。このとき、アクセス鍵ＡＫは、他ノードNにより一定時間ごとに更新されてノードNに送信される。そして、更新後には、更新前のアクセス鍵ＡＫを用いて暗号化された暗号化バケツトＥＰは、不正バケツトと判断されるようになる。そのため、攻撃者がアクセス鍵ＡＫを解析しても、一定時間経過後には当該アクセス鍵ＡＫを使用した通信が不可能になり、通信の安全性を担保することができる。

[01 29] この場合、受信部４０７は、アドホックネットワーク内の近隣ノードNが有する第１の共通鍵を用いて暗号化された近隣ノードNが有する第２の共通鍵を、近隣ノードNから受信する。ここで、第１の共通鍵とは、上述した固定鍵である。第２の共通鍵とは、上述したアクセス鍵ＡＫである。

[01 30] 具体的には、例えば、受信部４０７は、固定鍵を用いて暗号化されたァクセス鍵ＡＫを含む暗号化バケツトＥＰを受信する。例えば、図１で、ノードＮ１の受信部４０７は、ノードN２からアクセス鍵ＡＫ２を含む暗号化パケットＥＰを受信してもよい。これにより、受信部４０７は、近隣ノードNへ

バケツトを送信する際に、バケツトの暗号化に使用するアクセス鍵ＡＫを含む暗号化パケットＥＰを受信することができる。なお、受信された暗号化パケットＥＰは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 31] また、この場合、復号部４０８は、受信部４０７によって受信された暗号化された第２の共通鍵を、第１の共通鍵を用いて復号する。復号部４０８は、具体的には、例えば、アクセス鍵ＡＫを含む暗号化パケットＥＰを固定鍵を用いて復号する。そして、復号部４０８は、復号により得られたパケットからアクセス鍵ＡＫを取得する。例えば、図１で、ノードＮ１の復号部４０８は、アクセス鍵ＡＫ２を含む暗号化パケットＥＰを復号してもよい。そして、ノードＮ１の復号部４０８は、アクセス鍵ＡＫ２を取得してもよい。

[01 32] これにより、復号部４０８は、近隣ノードＮへパケットを送信する際に、バケツトの暗号化に使用するアクセス鍵ＡＫを取得することができる。なお、復号により得られたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。なお、取得されたアクセス鍵ＡＫは、送信元を示す識別子と関連付けてノードＤＢ３００に記憶される。

[01 33] このとき、送信元を示す識別子と関連付けてノードＤＢ３００にアクセス鍵ＡＫが保持されている場合、保持されているアクセス鍵ＡＫが取得されたアクセス鍵ＡＫで更新される。また、送信元を示す識別子と関連付けてノードＤＢ３００にアクセス鍵ＡＫが保持されていない場合、送信元を示す識別子と取得されたアクセス鍵ＡＫとを関連付けたレコードがノードＤＢ３００に追加される。

[01 34] 図５は、ノードＮの受信側としての機能的構成例を示す機能ブロック図である。図５に示すように、ノードＮは、第１の受信部５０１と、第１の保存部５０２と、第２の受信部５０３と、判断部５０４と、第２の保存部５０５と、データ処理部５０６と、第３の受信部５０７と、抽出部５０８と、送信部５０９と、を備える。第１の受信部５０１～データ処理部５０６は、具体的には、例えば、図２に示したフラッシュメモリ２０３などの記憶装置に記憶されたプログラムをＣＰＵ２０１に実行させることにより、または、ＩＺ

Ｆ２０４により、その機能を実現する。

[01 35] 第１の受信部５０１は、他ノードNでの消去回数を示す消去カウンタ値Ｒを上位桁とし他ノードNからの送信回数を示す送信カウンタ値Ｓを下位桁とする第１の連結カウンタ値ＪＣを、他ノードNから受信する。具体的には、例えば、第１の受信部５０１は、連結カウンタ値ＪＣを含むバケットを受信する。そして、第１の受信部５０１は、受信したパケットから連結カウンタ値ＪＣを取得する。これにより、第１の受信部５０１は、以後に受信するパケットの正当性の判断に使用する受信カウンタ値ＲＣになる連結カウンタ値ＪＣを取得することができる。

[01 36] また、第１の受信部５０１によって受信されるパケットは、暗号化により得られた暗号化パケットＥＰであってもよい。このとき、第１の受信部５０１は、暗号化バケットＥＰを固定鍵ＦＫまたはアクセス鍵ＡＫを用いて復号する。例えば、ノードN２の第１の受信部５０１は、図１でノードN２に保持されている受信カウンタ値ＲＣになる連結カウンタ値ＪＣを含む暗号化パケットＥＰを、過去に受信している。

[01 37] 第１の保存部５０２は、第１の受信部５０１によって受信された連結カウンタ値ＪＣを記憶装置に保存する。ここで、記憶装置とは、例えば、上述したＲＡＭ２０２である。具体的には、例えば、第１の保存部５０２は、第１の受信部５０１によって取得された連結カウンタ値ＪＣを、受信カウンタ値ＲＣとしてＲＡＭ２０２に保存する。例えば、図１では、ノードN２の第１の保存部５０２は、過去にノードN１から受信した暗号化バケットＥＰを復号して抽出した連結カウンタ値ＪＣ「０ｘ００００１２３０」を、受信カウンタ値ＲＣとして保持している。これにより、第１の保存部５０２は、以後に受信するバケットの正当性の判断に使用する連結カウンタ値ＪＣを、以後にバケットが受信されるまで受信カウンタ値ＲＣとしてＲＡＭ２０２に保持しておくことができる。

[01 38] 第２の受信部５０３は、第２の連結カウンタ値ＪＣを他ノードNから受信する。具体的には、例えば、第２の受信部５０３は、第１の受信部５０１に

よってバケツトが受信された後に、連結カウンタ値ＪＣを含むバケツトを受信する。そして、第２の受信部５０３は、受信したパケットから連結カウンタ値ＪＣを取得する。なお、受信されたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。例えば、図１の (9) では、暗号化パケットＥＰを受信しているが、ノードＮ２の第２の受信部５０３は、連結カウンタ値ＪＣ「0ｘ０１０００００２」を含む暗号化されないパケットを受信してもよい。これにより、第２の受信部５０３は、受信したパケットの正当性の判断に使用される連結カウンタ値ＪＣを取得することができる。

[01 39] また、第２の受信部５０３によって受信されるパケットは、暗号化により得られた暗号化パケットＥＰであってもよい。このとき、第２の受信部５０３は、暗号化バケツトＥＰを固定鍵ＦＫまたはアクセス鍵ＡＫを用いて復号する。例えば、図１の (9) では、ノードＮ２の第２の受信部５０３は、連結カウンタ値ＪＣ「0ｘ０１０００００２」を含む暗号化バケツトＥＰを受信している。そして、第２の受信部５０３は、暗号化パケットＥＰを固定鍵を用いて復号している。

[0140] 判断部５０４は、第２の受信部５０３によって受信された第２の連結カウンタ値ＪＣが第１の連結カウンタ値ＪＣよりも大きいか否かを判断する。ここで、第１の連結カウンタ値ＪＣとは、上述した受信カウンタ値ＲＣである。具体的には、例えば、判断部５０４は、第２の受信部５０３によって取得された連結カウンタ値」Ｃが、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣよりも大きいか否かを判断する。そして、判断部５０４は、判断結果から、第２の受信部５０３によって受信されたバケツトが不正バケツトであるか否かを判断する。なお、判断結果は、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0141] ここで、送信元のノードＮでは、送信ごとに連結カウンタ値ＪＣに１を加算し、連結カウンタ値ＪＣの消去後には消去前の連結カゥンタ値より大きい値になる新たな連結カウンタ値を生成している。そのため、ノードＮが、ある送信元のノードＮからの正規バケツトを受信し続けている限り、今回受信

したバケツトに含まれる連結カウンタ値ＪＣは、前回受信したバケツトに含まれる連結カウンタ値ＪＣ（すなわち、受信カウンタ値ＲＣ）より大きくなる。一方で、ノードNが再送攻撃による不正パケットを受信した場合、再送攻撃では過去に送信されたバケツトをそのまま送信しているため、ノードNが今回受信したバケツトに含まれる連結カウンタ値ＪＣは、受信カウンタ値ＲＣ以下となる。

[0142] そのため、判断部５０４は、第２の受信部５０３によって取得された連結カウンタ値ＪＣが、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣよりも大きい場合、第２の受信部５０３によって受信されたバケツトを正規パケットと判断する。一方、判断部５０４は、第２の受信部５０３によって取得された連結カウンタ値」Ｃが、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣ以下の場合、第２の受信部５０３によって受信されたバケツトを不正パケットと判断する。例えば、図１の (9) では、ノードＮ２の判断部５０４は、受信カウンタ値ＲＣ 「０ｘ００００５６７８」と、取得した連結カウンタ値ＪＣ 「０ｘ０１０００００２」と、の大小比較を行っている。そして、ノードＮ２の判断部５０４は、連結カウンタ値ＪＣが受信カウンタ値ＲＣよりも大きいため、受信した暗号化バケツトＥＰは正規バケツトであると判断している。これにより、判断部５０４は、第２の受信部５０３によって受信されたバケツトが、不正バケツトであるか否かを判断することができる。

[0143] 第２の保存部５０５は、判断部５０４によって大きいと判断された場合、第１の連結カウンタ値ＪＣに第２の連結カウンタ値ＪＣを上書保存する。具体的には、第２の保存部５０５は、判断部５０４によって大きいと判断された場合、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣに、第２の受信部５０３によって取得された連結カウンタ値ＪＣを上書き保存する。例えば、図１の (9) では、ノードＮ２の第２の保存部５０５は、受信カウンタ値ＲＣ 「０ｘ００００５６７８」を、取得した連結カウンタ値ＪＣ 「０ｘ０１０００００２」で更新している。これにより、第２の保存部５０５は、受信カウンタ値ＲＣを、最新の受信カウンタ値ＲＣに更新することができる。

[0144] データ処理部５０６は、判断部５０４によって大きくないと判断された場合、第２の連結カウンタ値ＪＣとともに受信されたデータを廃棄する。具体的には、例えば、データ処理部５０６は、判断部５０４によって大きくないと判断され、第２の受信部５０３によって受信されたバケツトが不正バケツトであると判断された場合、不正バケツトの内容が処理要求であっても処理を実行しない。また、データ処理部５０６は、不正パケットの内容が転送要求であってもマルチホップ通信せずに廃棄する。

[0145] 例えば、図１の (9) で、ノードN２のデータ処理部５０６は、不正パケットと判断された場合、受信した暗号化パケットＥＰを廃棄する。これにより、データ処理部５０６は、不正パケットが他ノードNへ転送されることを防止でき、また、不正パケットの内容を実行することによるノードNの処理負担を軽減できる。

[0146] また、データ処理部５０６は、判断部５０４によって大きいと判断された場合、第２の連結カウンタ値ＪＣとともに受信されたデータを処理する。具体的には、例えば、データ処理部５０６は、判断部５０４によって大きいと判断され、第２の受信部５０３によって受信されたバケツトが正規バケツトであると判断された場合、正規パケットの内容が処理要求であれば、処理要求に従って処理を行う。また、データ処理部５０６は、正規パケットの内容が転送要求であれば、マルチホップ通信により他ノードNへ正規バケツトを転送する。これにより、データ処理部５０６は、正規パケットにはパケットの内容に応じた処理を行うことができる。

[0147] 第３の受信部５０７は、消去カウンタ値Ｒについての取得要求や更新要求を受信する。まず、第３の受信部５０７が取得要求を受信する場合について説明する。ここで、取得要求とは、他ノードNに、自ノードNが過去に送信した送信カウンタ値Ｓを示す他ノードNが保持している受信カウンタ値ＲＣから消去カウンタ値Ｒを抽出させて、抽出させた消去カウンタ値Ｒを自ノードNへ送信させる要求である。

[0148] この場合、第３の受信部５０７は、他ノードNから消去カウンタ値Ｒの取

得要求を受信する。具体的には、例えば、第３の受信部５０７は、他ノードＮから、取得要求を含むパケットを受信する。例えば、図１の (2) では、暗号化バケツトＥＰを受信しているが、ノードＮ２の第３の受信部５０７は、取得要求を含む暗号化されないパケットを受信してもよい。これにより、第３の受信部５０７は、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣの中から、消去カウンタ値Ｒを抽出するトリガを発生させることができる。なお、受信されたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0149] また、第３の受信部５０７によって受信されるパケットは、暗号化により得られた暗号化パケットＥＰであってもよい。このとき、第３の受信部５０７は、暗号化バケツトＥＰを固定鍵ＦＫまたはアクセス鍵ＡＫを用いて復号する。例えば、図１の (9) では、ノードＮ２の第３の受信部５０７は、取得要求を含む暗号化パケットＥＰを受信している。そして、第３の受信部５０７は、暗号化バケツトＥＰを固定鍵を用いて復号している。

[0150] また、この場合、抽出部５０８は、第３の受信部５０７によって取得要求が受信された場合、記憶装置に記憶されている連結カウンタ値ＪＣの中の消去カウンタ値Ｒを抽出する。具体的には、例えば、抽出部５０８は、第３の受信部５０７によって取得要求が取得された場合、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣの中から、消去カウンタ値Ｒを抽出する。例えば、図１の (4) では、ノードＮ２の抽出部５０８は、保持している受信カウンタ値ＲＣ 「０ｘ００００１２３０」の中から、消去カウンタ値Ｒ 「０ｘ００」を抽出している。これにより、抽出部５０８は、他ノードＮに送信する消去カウンタ値Ｒを抽出することができる。なお、抽出された消去カウンタ値Ｒは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[0151] また、この場合、送信部５０９は、抽出部５０８によって抽出された消去カウンタ値Ｒを他ノードＮに送信する。具体的には、送信部５０９は、抽出部５０８によって抽出された消去カウンタ値Ｒを含むバケツトを生成する。そして、送信部５０９は、生成したパケットを他ノードＮに送信する。

[01 52] なお、ここでは、送信部５０９は、生成したパケットを、他ノードNにユニキャスト送信している。なお、パケットの他ノードNへのユニキャスト送信は、送信部５０９がパケットを近隣ノードに配信し、宛先の他ノードN以外の近隣ノードNが受信したバケツトを廃棄し、宛先になる他ノードNが受信したパケットを処理することで実現される。例えば、図１の (4) では、ノードN２の送信部５０９は、消去カウンタ値Ｒ「0ｘ００」を含む暗号化パケットＥＰを送信している。これにより、送信部５０９は、他ノードNでの連結カウンタ値」Ｃの生成に使用される消去カウンタ値Ｒを送信することができる。

[01 53] 次に、第３の受信部５０７が更新要求を受信する場合について説明する。ここで、更新要求とは、他ノードNに、自ノードNが過去に送信した送信カウンタ値Ｓを示す受信カウンタ値ＲＣから、消去カウンタ値Ｒを抽出させる要求である。また、更新要求とは、他ノードNに、抽出させた消去カウンタ値尺に１を加算した加算後の消去カウンタ値Ｒを自ノードNへ送信させる要求である。

[01 54] この場合、第３の受信部５０７は、他ノードNから消去カウンタ値Ｒの更新要求を受信する。具体的には、例えば、第３の受信部５０７は、他ノードNから、更新要求を含むパケットを受信する。なお、受信されたパケットは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。例えば、図１の (2) では、取得要求を含む暗号化バケツトＥＰを受信しているが、ノードN２の第３の受信部５０７は、取得要求を含む暗号化されないバケツトを受信してもよい。これにより、第３の受信部５０７は、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣの中から、消去カウンタ値Ｒを抽出するトリガを発生させることができる。

[01 55] また、第３の受信部５０７によって受信されるパケットは、暗号化により得られた暗号化パケットＥＰであってもよい。このとき、第３の受信部５０７は、暗号化バケツトＥＰを固定鍵ＦＫまたはアクセス鍵ＡＫを用いて復号する。例えば、図１の (2) では、ノードN２の第３の受信部５０７は、取

得要求を含む暗号化パケットＥＰを受信している。そして、第３の受信部５０７は、暗号化バケツトＥＰを固定鍵を用いて復号している。

[01 56] また、この場合、抽出部５０８は、第３の受信部５０７によって更新要求が受信された場合、記憶装置に記憶されている連結カウンタ値ＪＣの中の消去カウンタ値Ｒを抽出する。ここで、記憶装置とは、ＲＡＭ２０２である。具体的には、例えば、抽出部５０８は、第３の受信部５０７によって更新要求が取得された場合、ＲＡＭ２０２に保持されている受信カウンタ値ＲＣの中から、消去カウンタ値Ｒを抽出する。例えば、図１の (4) では、ノードＮ２の抽出部５０８は、保持している受信カウンタ値ＲＣ 「0ｘ００００１２３０」の中から、消去カウンタ値Ｒ 「0ｘ００」を抽出している。これにより、抽出部５０８は、他ノードNに送信する消去カウンタ値Ｒを抽出することができる。なお、抽出された消去カウンタ値Ｒは、例えば、ＲＡＭ２０２などの記憶領域に記憶される。

[01 57] また、この場合、送信部５０９は、抽出部５０８によって抽出された消去カウンタ値Ｒに１加算した加算後の消去カウンタ値Ｒを他ノードNに送信する。具体的には、送信部５０９は、抽出部５０８によって抽出された消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを含むバケツトを生成する。そして、送信部５０９は、生成したパケットを他ノードNに送信する。なお、ここでは、送信部５０９は、生成したパケットを、他ノードNにユニキャストで送信している。

[01 58] 例えば、図１の (4) では、ノードＮ２の送信部５０９は、生成したパケットをノードＮ１に送信している。これにより、送信部５０９は、他ノードＮでの連結カウンタ値ＪＣの生成に使用される加算後の消去カウンタ値Ｒを送信することができる。また、送信部４０３によって送信されるパケットは、暗号化されてもよい。このとき、送信部４０３は、パケットを固定鍵ＦＫまたはアクセス鍵ＡＫを用いて暗号化する。

[01 59] （アクセス鍵ＡＫを用いた暗号化通信）

次に、図６および図７を用いて、アクセス鍵ＡＫを用いた暗号化通信の一

例について説明する。

[01 60] 図６は、アクセス鍵ＡＫを用いた暗号化通信の一例を示す説明図である。なお、図１で説明した箇所と同様の箇所についての説明は省略する。図６の例では、ノードＮ１は、ノードＮ２へ送信するバケットの暗号化に使用されるアクセス鍵ＡＫ２と、ノードＮ３へ送信するバケットの暗号化に使用されるアクセス鍵ＡＫ３と、を保持している。

[01 61] また、ノードＮ１は、連結カウンタ値ＪＣ「０ｘ００００１２３０」を保持している。ノードＮ２は、過去にノードＮ１から受信した暗号化パケットＥＰを復号して得られたバケットから抽出した連結カウンタ値ＪＣ「０ｘ００００１２３０」を、受信カウンタ値ＲＣとして保持している。ノードＮ３は、過去にノードＮ１から受信した暗号化バケットＥＰを復号して得られたバケットから抽出した連結カウンタ値ＪＣ「０ｘ００００１２２９」を、受信カウンタ値ＲＣとして保持している。

[01 62] ここでは、ノードＮ１からノードＮ２およびノードＮ３に、アクセス鍵ＡＫを用いて暗号化された暗号化バケットＥＰが送信される場合を例に挙げて、アクセス鍵ＡＫを用いた暗号化通信について説明する。

[01 63] （１１）ノードＮ１は、ノードＮ２を宛先にするデータの送信イベントがあると、連結カウンタ値ＪＣ「０ｘ００００１２３０」に１を加算する。

[01 64] （１２）次に、ノードＮ１は、ノードＮ２を宛先にするデータと、加算後の連結カウンタ値」Ｃ「０ｘ００００１２３１」と、を含むバケットを生成し、生成したパケットをアクセス鍵ＡＫ２を用いて暗号化する。そして、ノードＮ１は、暗号化により得られた暗号化パケットＥＰを、データの宛先になるノードＮ２に送信する。

[01 65] （１３）ノードＮ２は、ノードＮ１から暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰを、アクセス鍵ＡＫ２を用いて復号する。そして、ノードＮ２は、復号により得られたパケットに含まれる連結カウンタ値ＪＣ「０ｘ００００１２３１」と、前回受信した連結カウンタ値ＪＣを示す受信カウンタ値ＲＣ「０ｘ００００１２３０」と、の大小比較を行う。

[01 66] ここで、ノードN２は、復号により得られたパケットに含まれる連結カウンタ値ＪＣが受信カゥンタ値ＲＣよりも大きいため、受信した暗号化パケットＥＰが正規パケットであると判断する。そして、ノードN２は、受信カウンタ値ＲＣ「０ｘ００００１２３０」を、復号により得られたバケツトに含まれる連結カウンタ値」Ｃ「０ｘ００００１２３１」で更新する。

[01 67] （１４）また、ノードN１は、ノードN３を宛先にするデータの送信ィベントがあると、連結カウンタ値ＪＣ「０ｘ００００１２３１」に１を加算する。

[01 68] （１５）次に、ノードN１は、ノードN３を宛先にするデータと、加算後の連結カウンタ値」Ｃ「０ｘ００００１２３２」と、を含むバケツトを生成し、生成したパケットをアクセス鍵ＡＫ３を用いて暗号化する。そして、ノ―ドN１は、暗号化により得られた暗号化パケットＥＰを、データの宛先になるノードN３に送信する。

[01 69] （１６）ノードN３は、ノードN１から暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰを、アクセス鍵ＡＫ３を用いて復号する。そして、ノードN３は、復号により得られたパケットに含まれる連結カウンタ値ＪＣ「０ｘ００００１２３２」と、前回受信した連結カウンタ値ＪＣを示す受信カウンタ値ＲＣ「０ｘ００００１２２９」と、の大小比較を行う。ここで、ノードN３は、復号により得られたパケットに含まれる連結カウンタ値ＪＣが受信カウンタ値ＲＣよりも大きいため、受信した暗号化バケツトＥＰが正規パケットであると判断する。そして、ノードN３は、受信カウンタ値ＲＣ「０ｘ００００１２９９」を、復号により得られたバケツトに含まれる連結カウンタ値」Ｃ「０ｘ００００１２３２」で更新する。

[01 70] （アクセス鍵ＡＫを用いた暗号化通信の詳細）

次に、図７を用いて、図６に示したアクセス鍵ＡＫを用いた暗号化通信の詳細について説明する。

[01 7 1] 図７は、アクセス鍵ＡＫを用いた暗号化通信の詳細を示す説明図である。図７では、図６に示したノードN１とノードN２との間の暗号化通信の詳細

について説明する。

[01 72] （２１）ノードＮ１は、ノードＮ１のユーザからのノードＮ２を宛先にするデータの入力を受けると、ノードＮ２との暗号化通信を開始する。ここでは、ノードＮ１は、ユーザからのデータの入力をトリガにして暗号化通信を開始したが、ノードＮ１が自動的に発生させたデータ送信イベントをトリガにして暗号化通信を開始してもよい。（２２）次に、ノードＮ１は、ノードＮ２を宛先にするデータの入力を受けると、連結カウンタ値ＪＣ「０ｘ０００１２３０」に１を加算する。

[01 73] （２３）そして、ノードＮ１は、送信元を示す識別子「Ｎ１」と、ノードＮ２を宛先にするデータと、加算後の連結カウンタ値ＪＣ「０ｘ０００１２３１」と、を含むパケットを生成する。このとき、送信元を示す識別子は、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。以下の説明においても、同様に、送信元を示す識別子はバケット内の暗号化されない部分に含まれる。また、バケット内の暗号化される部分に、さらに送信元を示す識別子を含んでもよい。

[01 74] （２４）次に、ノードＮ１は、生成したパケット内のノードＮ２を宛先にするデータと加算後の連結カウンタ値ＪＣ「０ｘ０００１２３１」とをアクセス鍵ＡＫ２を用いて暗号化する。

[01 75] （２５）そして、ノードＮ１は、暗号化により得られた暗号化パケットＥＰを、データの宛先になるノードＮ２に送信する。

[01 76] （２６）ノードＮ２は、ノードＮ１から暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰから送信元を示す識別子「Ｎ１」を取得し、受信した暗号化バケットＥＰをアクセス鍵ＡＫ２を用いて復号する。そして、ノードＮ２は、復号により得られたパケットから、ノードＮ２を宛先にするデータと連結カウンタ値ＪＣ「０ｘ０００１２３１」とを取得する。

[01 77] （２７）次に、ノードＮ２は、取得した「Ｎ１」が示す送信元のノードＮ１に関連付けられた受信カウンタ値ＲＣを、ノードＤＢ３００から抽出する。（２８）そして、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ００

００１２３１」と、抽出した受信カウンタ値ＲＣ「０ｘ００００１２３０」との大小比較を行う。ここで、ノードＮ２は、取得した連結カウンタ値ＪＣが、抽出した受信カウンタ値ＲＣよりも大きいため、受信した暗号化バケットＥＰが正規バケットであると判断する。

[0178] （２９）次に、ノードＮ２は、暗号化パケットＥＰが正規パケットであると判断されると、ノードＤＢ３００の受信カウンタ値ＲＣ「０ｘ００００１２３０」を連結カウンタ値ＪＣ「０ｘ００００１２３１」で更新する。そして、ノードＮ２は、暗号化パケットＥＰが正規パケットであると判断されると、正規バケットの内容が処理要求であれば、処理要求に従って処理を行う。また、データ処理部は、正規バケットの内容が転送要求であれば、マルチホップ通信により他ノードＮへ正規パケットを転送する。これにより、ノードＮ２は、正規パケットには、パケットの内容に応じた処理を行うことができる。

[0179] 一方、ノードＮ２は、取得した連結カウンタ値ＪＣが、抽出した受信カウンタ値ＲＣ以下である場合は、受信した暗号化バケットＥＰが不正バケットであると判断する。そして、ノードＮ２は、不正パケットであると判断されると、復号により得られたパケットを廃棄する。

[0180] 具体的には、ノードＮ２は、不正パケットの内容が処理要求であっても処理を実行せずに、復号により得られたパケットを廃棄する。また、ノードＮ２は、不正バケットの内容が転送要求であってもマルチホップ通信せずに、復号により得られたパケットを廃棄する。これにより、ノードＮ２は、不正パケットが他ノードＮへ転送されることを防止でき、また、不正パケットの内容を実行することによるノードＮの処理負担を軽減できる。そして、ノードＮ２は、通信の安全性を担保することができる。

[0181] （バケット送信処理の処理内容）

次に、図８を用いて、図６および図７に示した暗号化通信におけるバケット送信処理について説明する。パケット送信処理は、図６および図７に示したノードＮ１が実行する処理である。ここでは、例としてノードＮ１を実行

主体として説明する。

[01 82] 図８は、暗号化通信におけるパケット送信処理の詳細な処理手順を示すフローチャートである。まず、ノードＮ１は、他ノードＮを宛先にするデータの送信イベントが発生したか否かを判定する (ステップＳ８０１)。ここで、送信イベントが発生していない場合 (ステップＳ８０１ :Ｎｏ)、ＣＰＵ２０１は、ステップＳ８０１に戻り、送信イベントの発生を待つ。

[01 83] 一方、送信イベントが発生した場合 (ステップＳ８０１ :Ｙｅｓ)、ノードＮ１は、連結カウンタ値ＪＣに１を加算する (ステップＳ８０２)。次に、ノードＮ１は、送信元になる自ノードＮを示す識別子と、他ノードＮを宛先にするデータと、加算後の連結カウンタ値ＪＣと、を含むパケットを生成する (ステツプＳ８０３)。

[01 84] そして、ノードＮ１は、データの宛先になるノードＮの識別子に関連付けてノードＤＢ３００に保持されているアクセス鍵ＡＫがあるか否かを判定する (ステップＳ８０４)。ここで、アクセス鍵ＡＫがある場合 (ステップＳ８０４ :Ｙｅｓ)、ノードＮ１は、生成したバケツトを、アクセス鍵ＡＫを用いて暗号化する (ステップＳ８０５)。

[01 85] 一方、アクセス鍵ＡＫがない場合 (ステップＳ８０４ :Ｎｏ)、ノードＮ１は、生成したパケットを、固定鍵を用いて暗号化する (ステップＳ８０６)。そして、ノードＮ１は、暗号化により得られた暗号化パケットＥＰを、データの宛先になるノードＮに送信し (ステップＳ８０７)、パケット送信処理を終了する。これにより、ノードＮは、送信するパケットを暗号化して、通信の安全性を担保することができる。

[01 86] (バケツト受信処理の処理内容)

次に、図９を用いて、図６および図７に示した暗号化通信におけるバケツト受信処理について説明する。パケット受信処理は、図６および図７に示したノードＮ２またはノードＮ３が実行する処理である。ここでは、例としてノードＮ２を実行主体として説明する。

[01 87] 図９は、暗号化通信におけるパケット受信処理の詳細な処理手順を示すフ

ローチヤー トである。まず、ノー ドN２は、暗号化パケットＥＰを受信したか否かを判定する (ステップＳ９０１)。ここで、暗号化パケットＥＰを受信していない場合 (ステップＳ９０１ :Ｎｏ)、ノー ドN２は、ステップＳ９０１に戻り、暗号化バケツ トＥＰの受信を待つ。

[01 88] 一方、暗号化パケットＥＰを受信した場合 (ステップＳ９０１ :Ｙｅｓ)、ノー ドN２は、暗号化パケットＥＰ内の暗号化されない部分 (例えば、パケッ トのヘッダ部分) から、送信元を示す識別子を取得する (ステップＳ９０２)。

[01 89] 次に、ノー ドN２は、自ノー ドNのアクセス鍵ＡＫまたは固定鍵を用いて、受信した暗号化パケットＥＰを復号する (ステップＳ９０３)。次に、ノー ドN２は、正常に復号できたか否かを判定する (ステップＳ９０４)。ここで、正常に復号できない場合 (ステップＳ９０４ :Ｎｏ)、ノー ドN２は、受信した暗号化パケットＥＰが不正パケッ トであると判断して、暗号化パケッ トＥＰを廃棄し (ステップＳ９０７)、パケッ ト受信処理を終了する。

[01 90] 一方、正常に復号できた場合 (ステップＳ９０４ :Ｙｅｓ)、ノー ドN２は、復号により得られたパケッ ト内の連結カウンタ値ＪＣが、送信元を示す識別子に関連付けてノー ドＤＢ３００に保持されている受信カウンタ値ＲＣより大きいか否かを判定する (ステップＳ９０５)。

[01 91] ここで、受信カウンタ値ＲＣ以下の場合 (ステップＳ９０５ :Ｎｏ)、ノー ドN２は、受信した暗号化パケットＥＰが不正パケッ トであるとして、暗号化パケットＥＰを廃棄し (ステップＳ９０７)、パケッ ト受信処理を終了する。

[01 92] 一方、受信カウンタ値ＲＣより大きい場合 (ステップＳ９０５ :Ｙｅｓ)、ノー ドN２は、受信した暗号化パケットＥＰが正規パケッ トであると判断する。そして、ノー ドN２は、送信元を示す識別子に関連付けてノー ドＤＢ３００に保持されている受信カウンタ値ＲＣを、復号により得られたバケツ ト内の連結カウンタ値ＪＣに更新して (ステップＳ９０６)、パケッ ト受信処理を終了する。これにより、ノー ドNは、受信した暗号化パケットＥ ロが

不正バケツトであるか否かを判断して、暗号化バケツトＥＰが不正バケツトと判断された場合、暗号化パケットＥＰを廃棄し、通信の安全性を担保する。

[01 93] （連結カウンタ値ＪＣが消去された場合の処理）

次に、連結カウンタ値ＪＣが消去された場合について説明する。例えば、連結カウンタ値ＪＣが消去された場合とは、停電によりノードＮに電力が供給されず、ＲＡＭ２０２に保持されている連結カウンタ値ＪＣが消去された場合である。また、連結カウンタ値ＪＣが消去された場合とは、ノードＮのユーザからの操作によってＲＡＭ２０２の記憶内容が初期化された場合であってもよい。

[01 94] この場合、ノードＮは、以後送信する暗号化パケットＥＰに含むべき連結カウンタ値ＪＣが不明であるため、以後送信する暗号化バケツトＥＰを他ノードＮで正規バケツトと判断させることができず、アドホックネットワークへ復帰することができない。以下では、新たな連結カウンタ値ＪＣを生成してアドホックネットワークに復帰する際のノードＮの動作例について説明する。

[01 95] （ノードＮの連結カウンタ値ＪＣが消去された場合の動作例１）

まず、図１０～図１３を用いて、ノードＮの連結カウンタ値ＪＣが消去された場合の動作例１について説明する。

[01 96] 図１０～図１３は、ノードＮの連結カウンタ値ＪＣが消去された場合の動作例１を示す説明図である。なお、図１で説明した箇所と同様の箇所についての説明は省略する。図１０の例では、ノードＮ１は、ノードＮ２から受信され、ノードＮ２へ送信するバケツトの暗号化に使用されるアクセス鍵ＡＫ２「０ｘ２２２２」を保持している。

[01 97] また、ノードＮ１は、連結カウンタ値ＪＣ「０ｘ００００１２３０」を保持している。ノードＮ２は、過去にノードＮ１から受信した暗号化パケットＥＰを復号して得られたバケツトから連結カウンタ値ＪＣを抽出し、抽出した連結カウンタ値」Ｃ「０ｘ００００１２３０」を、受信カウンタ値ＲＣと

して保持している。

[01 98] 図１０において、停電によりノードN１に電力が供給されず、ノードN１が保持していた連結カウンタ値ＪＣ「0ｘ００００１２３０」およびアクセス鍵ＡＫ２が消去されてしまったとする。そのため、他ノードNに送信するバケットに含むべき連結カウンタ値ＪＣが不明になり、ノードN１は、他ノードNにバケットを送信することができない。

[01 99] （３１）ここで、ノードN１は、停電が回復し電力が供給されると、保持していた連結カウンタ値ＪＣが消去されたことを検出する。

[0200] （３２）ノードN１は、連結カウンタ値ＪＣが消去されたことを検出すると、一時的な識別情報になる乱数を生成する。図１０の例では、ノードN１は、乱数として「0ｘ５８１９」を生成する。このとき、ノードN１は、生成した乱数「0ｘ５８１９」をＲＡＭ２０２に保持しておく。

[0201] （３３）ノードN１は、乱数を生成すると、送信元を示す識別子「N１」と、消去カウンタ値Ｒの取得要求を示す連結カウンタ値ＪＣとして設定されている「0ｘ００００００００」と、生成した乱数「0ｘ５８１９」と、を含むパケットを生成する。このとき、送信元を示す識別子は、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0202] （３４）ノードN１は、パケットを生成すると、生成したパケット内の連結カウンタ値ＪＣ「0ｘ００００００００」と乱数「0ｘ５８１９」とを、固定鍵ＦＫを用いて暗号化する。（３５）そして、ノードN１は、暗号化により得られた暗号化バケットＥＰを、ノードN２を含む近隣ノードNに送信する。次に、図１１に移る。

[0203] （３６）ノードN２は、（３５）でノードN１から送信された暗号化パケットＥＰを受信すると、受信した暗号化バケットＥＰから送信元を示す識別子「N１」を取得し、受信した暗号化パケットＥＰを固定鍵ＦＫを用いて復号する。そして、ノードN２は、復号により得られたパケットから、連結カウンタ値ＪＣ「0ｘ００００００００」と乱数「0ｘ５８１９」とを取得する。

[0204] （３７）ノードＮ２は、取得した連結カウンタ値ＪＣが、消去カウンタ値Ｒの取得要求を示す連結カウンタ値」Ｃとして設定されている「０ｘ０００００００」であることを検出する。そして、ノードＮ２は、取得した送信元を示す識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣをノードＤＢ３００から抽出し、抽出した受信カウンタ値ＲＣから消去カウンタ値Ｒ「０ｘ００」を抽出する。

[0205] （３８）ノードＮ２は、消去カウンタ値Ｒを抽出すると、送信元を示す識別子「Ｎ２」と、抽出した消去カウンタ値Ｒ「０ｘ００」と、取得した乱数「０ｘ５８１９」と、を含むパケットを生成する。このとき、送信元を示す識別子は、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0206] （３９）ノードＮ２は、生成したパケット内の消去カウンタ値Ｒ「０ｘ００」と乱数「０ｘ５８１９」とを固定鍵ＦＫを用いて暗号化する。

[0207] （４０）ノードＮ２は、暗号化により得られた暗号化パケットＥＰを、取得した識別子「Ｎ１」が示すノードＮ１に送信する。次に、図１２に移る。

[0208] （４１）ノードＮ１は、（４０）でノードＮ２から送信された暗号化パケットＥＰを受信すると、受信した暗号化バケツトＥＰから送信元を示す識別子「Ｎ２」を取得し、受信した暗号化パケットＥＰを、固定鍵ＦＫを用いて復号する。そして、ノードＮ１は、復号により得られたパケットから、消去カウンタ値Ｒ「０ｘ００」と乱数「０ｘ５８１９」とを取得する。

[0209] （４２）ノードＮ１は、乱数を取得すると、取得した乱数と（３２）でＲＡＭ２０２に保持しておいた乱数との一致判断を行う。ここで、ノードＮ１は、取得した乱数「０ｘ５８１９」とＲＡＭ２０２に保持しておいた乱数「０ｘ５８１９」とが一致するため、（４１）で受信した暗号化パケットＥＰは正規バケツトであると判断する。

[0210] （４３）ノードＮ１は、正規パケットであると判断されると、連結カウンタ値ＪＣが消去される以前の消去カウンタ値Ｒを示す取得した消去カウンタ値Ｒ「０ｘ００」に、１を加算する。そして、ノードＮ１は、加算後の消去

カウンタ値Ｒ「０ｘ０１」と送信カウンタ値Ｓの初期値「０ｘ０００００００」とを連結して、連結カウンタ値ＪＣ「０ｘ０１０００００００」を生成する。これにより、ノードＮ１は、消去された連結カウンタ値ＪＣの代わりに、新たな連結カウンタ値ＪＣを生成する。

[021 1] 一方、ノードＮ１は、取得した乱数と(３２)でＲＡＭ２０２に保持しておいた乱数とが一致しない場合は、(４１)で受信した暗号化パケットＥＰは不正パケットであると判断する。そして、ノードＮ１は、不正パケットであると判断されると、復号により得られたパケットを廃棄することで、通信の安全性を担保する。次に、図１３に移る。

[021 2] (４４)ノードＮ１は、ノードＮ１のユーザからのノードＮ２を宛先にするデータの入力を受けると、ノードＮ２との暗号化通信を開始する。ここでは、ノードＮ１は、ユーザからのデータの入力をトリガにして暗号化通信を開始したが、ノードＮ１が自動的に発生させたデータ送信イベントをトリガにして暗号化通信を開始してもよい。

[021 3] (４５)ノードＮ１は、ノードＮ２を宛先にするデータの入力を受けると、(４３)で生成された新たな連結カウンタ値ＪＣ「０ｘ０１０００００００」に１を加算する。

[0214] (４６)ノードＮ１は、送信元を示す識別子「Ｎ１」と、ノードＮ２を宛先にするデータと、加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」と、を含むパケットを生成する。このとき、送信元を示す識別子は、バケット内の暗号化されない部分(例えば、パケットのヘッダ部分)に含まれる。

[021 5] (４７)ノードＮ１は、パケットを生成すると、生成したパケット内のノードＮ２を宛先にするデータと加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」とを固定鍵ＦＫを用いて暗号化する。

[021 6] (４８)ノードＮ１は、暗号化により得られた暗号化パケットＥＰを、データの宛先であるノードＮ２に送信する。

[021 7] (４９)ノードＮ２は、ノードＮ１から送信された暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰから送信元を示す識別子「Ｎ１」

を取得し、受信した暗号化パケットＥＰを、固定鍵ＦＫを用いて復号する。そして、ノードＮ２は、復号により得られたパケットから、ノードＮ２を宛先にするデータと連結カウンタ値ＪＣ「０ｘ０１０００００１」とを取得する。

[021 8] （５０）ノードＮ２は、連結カウンタ値ＪＣ「０ｘ０１０００００１」を取得すると、取得した送信元を示す識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣをノードＤＢ３００から抽出する。

[021 9] （５１）そして、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」と、抽出した受信カウンタ値ＲＣ「０ｘ００００１２３０」と、の大小比較を行う。ここで、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」が、抽出した受信カウンタ値ＲＣ「０ｘ００００１２３０」よりも大きいため、受信した暗号化パケットＥＰが正規バケットであると判断する。

[0220] （５２）ノードＮ２は、正規パケットであると判断されると、ノードＤＢ３００において識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣ「０ｘ００００１２３０」を、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」で更新する。

[0221] 一方、ノードＮ２は、取得した連結カウンタ値ＪＣが、抽出した受信カウンタ値ＲＣ以下である場合は、受信した暗号化バケットＥＰが不正バケットであると判断する。そして、ノードＮ２は、不正パケットであると判断されると、復号により得られたパケットを廃棄することで、通信の安全性を担保する。

[0222] このように、ノードＮ１は、消去カウンタ値Ｒを上位桁とし、送信カウンタ値Ｓを下位桁として連結した連結カウンタ値」Ｃを保持し、連結カウンタ値ＪＣが消去されると、消去以前の消去カウンタ値Ｒを他ノードＮから取得する。そして、ノードＮ１は、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とする新たな連結カウンタ値ＪＣを生成する。

[0223] これにより、過去にノードN1により送信された暗号化パケットEPに含まれていた連結力ウンタ値JCより、ノードN1により生成された新たな連結力ウンタ値JCが大きい値になる。そのため、ノードN1は、他ノードNが保持している受信力ウンタ値RCより大きい値になっている連結力ウンタ値JCを、他ノードNに送信する暗号化バケットEPに含むことができる。

[0224] これにより、ノードN2は、保持している受信力ウンタ値RCより、ノードN1から受信した暗号化バケットEPに含まれる連結力ウンタ値JCが大きいため、ノードN1から受信した暗号化バケットEPを正規バケットと判断することができる。そして、ノードN1は、他ノードNに送信する暗号化バケットEPが、他ノードNで不正バケットと判断されないようになるため、アドホックネットワークに復帰することができる。

[0225] また、ノードN1は、取得要求を含むパケットを、固定鍵FKを用いて暗号化するため、固定鍵FKを有さない攻撃者による要求バケットの解析を防止することができる。また、ノードN1は、取得要求を含むパケットに、近隣ノードNとの通信ごとに生成した一時的な識別情報になる乱数を含める。これにより、ノードN1は、自ノードNが送信した暗号化パケットEPに含めた乱数と受信した暗号化バケットEPに含まれる乱数との一致判断により、正規バケットか否かを通信ごとに判断することができる。

[0226] ここで、通信ごとに異なる乱数が生成されるため、前回の取得要求に対する応答として近隣ノードNが送信した暗号化バケットEPを今回の取得要求に対する応答と偽って攻撃者が再送攻撃に使用しても、それぞれの暗号化パケットEPに含まれる乱数は不一致になる。そのため、ノードN1は、乱数の不一致から、今回の取得要求に対する応答として受信された暗号化バケットEPが再送攻撃による不正バケットと判断でき、通信の安全性を担保することができる。

[0227] また、ノードN1は、一度使用した乱数に有効期間を設定しておくことで、今回の通信で近隣ノードNが応答した暗号化バケットEPを攻撃者が再送攻撃に利用した場合に、有効期間を過ぎていれば不正バケットと判断でき、

通信の安全性を担保することができる。

[0228] (動作例１における連結カウンタ値生成処理の処理内容)

次に、図１４を用いて、図１０～図１３に示した動作例１における連結カウンタ値生成処理の詳細な処理手順について説明する。連結カウンタ値生成処理は、図１０～図１３に示したノードＮ１が実行する処理である。ここでは、例としてノードＮ１を実行主体として説明する。

[0229] 図１４は、動作例１における連結カウンタ値生成処理の詳細な処理手順を示すフローチャートである。まず、ノードＮ１は、連結カウンタ値ＪＣの消去が検出されたか否かを判定する (ステップＳ１４０１)。ここで、連結カウンタ値ＪＣの消去が検出されていない場合 (ステップＳ１４０１ :Ｎｏ)、ノードＮ１は、ステップＳ１４０１に戻り、連結カウンタ値ＪＣの消去が検出されるのを待つ。

[0230] 一方、連結カウンタ値ＪＣの消去が検出された場合 (ステップＳ１４０１ :Ｙｅｓ)、ノードＮ１は、一時的な識別情報になる乱数を生成する (ステップＳ１４０２)。次に、ノードＮ１は、送信元になる自ノードＮを示す識別子と、生成した乱数と、送信カウンタ値Ｓの取得要求と、を含むパケットを生成する (ステップＳ１４０３)。

[0231] そして、ノードＮ１は、生成したパケットを固定鍵ＦＫを用いて暗号化する (ステップＳ１４０４)。次に、ＣＰＵ２０１は、暗号化により得られた暗号化パケットＥＰを近隣ノードＮに送信する (ステップＳ１４０５)。

[0232] そして、ノードＮ１は、取得要求に対する応答になる暗号化パケットＥＰを近隣ノードＮから受信したか否かを判定する (ステップＳ１４０６)。ここで、暗号化パケットＥＰを受信していない場合 (ステップＳ１４０６ :Ｎｏ)、ノードＮ１は、ステップＳ１４０６に戻り、暗号化パケットＥＰの受信を待つ。

[0233] 一方、暗号化パケットＥＰを受信した場合 (ステップＳ１４０６ :Ｙｅｓ)、ノードＮ１は、受信した暗号化パケットＥＰを固定鍵ＦＫを用いて復号する (ステップＳ１４０７)。そして、ノードＮ１は、復号により得られた

パケットから乱数を抽出し、抽出した乱数が、ステップＳ１４０２で生成した乱数と一致するか否かを判定する（ステップＳ１４０８）。

[0234] ここで、一致する場合（ステップＳ１４０８：Ｙｅｓ）、ノードＮ１は、復号により得られたバケットから消去カウンタ値Ｒを抽出し、抽出した消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒと送信カウンタ値Ｓの初期値とを連結して連結カウンタ値ＪＣを生成する（ステップＳ１４０９）。そして、ノードＮ１は、生成した連結カウンタ値ＪＣをＲＡＭ２０２に保存して（ステップＳ１４１０）、連結カウンタ値生成処理を終了する。

[0235] 一方、一致しない場合（ステップＳ１４０８：Ｎｏ）、ノードＮ１は、受信した暗号化バケットＥＰが不正バケットであると判断して、復号により得られたバケットを廃棄し（ステップＳ１４１１）、連結カウンタ値生成処理を終了する。

[0236] これにより、ノードＮは、連結カウンタ値ＪＣが消去された場合であっても、消去された連結カウンタ値ＪＣより大きい値の新たな連結カウンタ値ＪＣを生成することができる。そして、ノードＮは、送信するパケットが他ノードＮに廃棄されないようになり、アドホックネットワークに復帰できる。

[0237] また、ノードＮは、取得要求を含むパケットを固定鍵ＦＫを用いて暗号化するため、固定鍵ＦＫを有さない攻撃者による要求バケットの解析を防止できる。また、ノードＮは、取得要求を含むパケットに、近隣ノードＮとの通信ごとに生成した一時的な識別情報になる乱数を含める。これにより、ノードＮは、自ノードＮが送信した暗号化バケットＥＰに含めた乱数と受信した暗号化バケットＥＰに含まれる乱数との一致判断により、正規バケットか否かを通信ごとに判断することができる。

[0238] ここで、通信ごとに異なる乱数が生成されるため、前回の取得要求に対する応答として近隣ノードＮが送信した暗号化バケットＥＰを今回の取得要求に対する応答と偽って攻撃者が再送攻撃に使用しても、それぞれの暗号化パケットＥＰに含まれる乱数は不一致になる。そのため、ノードＮは、乱数の不一致から、今回の取得要求に対する応答として受信された暗号化バケット

ＥＰが再送攻撃による不正バケツトと判断でき、通信の安全性を担保することができる。

[0239] また、ノードNは、一度使用した乱数に有効期間を設定しておくことで、今回の通信で近隣ノードNが応答した暗号化パケットＥＰを攻撃者が再送攻撃に利用した場合に、有効期間を過ぎていれば不正パケットと判断でき、通信の安全性を担保することができる。

[0240] （ノードNの連結カウンタ値ＪＣが消去された場合の動作例２）

次に、図１５～図１８を用いて、ノードNの連結カウンタ値ＪＣが消去された場合の動作例２について説明する。図１０～図１３に示した動作例１では、消去カウンタ値Ｒの取得要求を含むパケットを、固定鍵ＦＫを用いて暗号化したが、動作例２では、消去カウンタ値Ｒの取得要求を含むパケットをアクセス鍵ＡＫを用いて暗号化する。これにより、暗号化により得られた消去カウンタ値Ｒの取得要求を含む暗号化バケツトＥＰが、固定鍵を用いて暗号化する場合よりセキュアになり、通信の安全性を担保することができる。

[0241] 図１５～図１８は、ノードNの連結カウンタ値ＪＣが消去された場合の動作例２を示す説明図である。なお、図１で説明した箇所と同様の箇所についての説明は省略する。図１５の例では、また、ノードＮ１は、ノードＮ２から受信され、ノードＮ２へ送信するバケツトの暗号化に使用されるアクセス鍵ＡＫ２「０ｘ２２２２」を保持している。

[0242] また、ノードＮ１は、連結カウンタ値ＪＣ「０ｘ００００１２３０」を保持している。ノードＮ２は、過去にノードＮ１から受信した暗号化パケットＥＰを復号して得られたバケツトから連結カウンタ値ＪＣを抽出し、抽出した連結カウンタ値」Ｃ「０ｘ００００１２３０」を受信カウンタ値ＲＣとして保持している。

[0243] 図１５において、停電によりノードＮ１に電力が供給されず、ノードＮ１が保持していた連結カウンタ値ＪＣ「０ｘ００００１２３０」およびァクセス鍵ＡＫ２が消去されてしまったとする。そのため、他ノードNに送信するバケツトに含むべき連結カウンタ値ＪＣが不明になり、ノードＮ１は、他ノ

— ドNにバケツトを送信することができない。

[0244] （６１）ここで、ノードＮ１は、停電が回復し電力が供給されると、保持していた連結カウンタ値ＪＣが消去されたことを検出する。このとき、ノードＮ１は、近隣ノードＮからアクセス鍵ＡＫが送信されてくるまで待機する。

[0245] （６２）—方、ノードＮ２は、一定時間ごとにノードＮ２自体が自動的に発生させるアクセス鍵ＡＫ生成イベントをトリガにして、新たなアクセス鍵ＡＫ２「０ｘ６６６６」を生成する。

[0246] （６３）ノードＮ２は、アクセス鍵ＡＫ２を生成すると、送信元を示す識別子「Ｎ２」と、ノードＮ２の連結カウンタ値ＪＣ「０ｘ０００２２２２」と、生成したアクセス鍵ＡＫ２「０ｘ６６６６」と、を含むパケットを生成する。このとき、送信元を示す識別子は、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0247] （６４）ノードＮ２は、パケットを生成すると、生成したパケット内の連結カウンタ値ＪＣ「０ｘ０００２２２２」とアクセス鍵ＡＫ２「０ｘ６６６６」とを、固定鍵ＦＫを用いて暗号化する。

[0248] （６５）そして、ノードＮ２は、暗号化により得られた暗号化パケットＥＰを、ノードＮ１を含む近隣ノードＮに送信する。

[0249] （６６）ノードＮ１は、ノードＮ２から送信された暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰから送信元を示す識別子「Ｎ２」を取得し、受信した暗号化パケットＥＰを固定鍵ＦＫを用いて復号する。そして、ノードＮ１は、復号により得られたパケットから、連結カウンタ値ＪＣ「０ｘ０００２２２２」とアクセス鍵ＡＫ２「０ｘ６６６６」とを取得する。

[0250] このとき、停電によりノードＤＢ３００の記憶内容が消去されており、ノードＤＢ３００にノードＮ２についてのレコードが存在しない。

[0251] （６７）そのため、ノードＮ１は、取得した連結カウンタ値ＪＣ「０ｘ０００２２２２」とアクセス鍵ＡＫ２「０ｘ６６６６」とを、取得した識別

子「Ｎ２」に関連付けたレコードを、ノードＤＢ３００に追加しておく。

[0252] （６８）ノードＮ１は、ノードＤＢ３００にレコードを追加すると、一時的な識別情報になる乱数を生成する。図１５の例では、ノードＮ１は、乱数として「０ｘ５８１９」を生成する。このとき、ノードＮ１は、生成した乱数「０ｘ５８１９」をＲＡＭ２０２に保持しておく。

[0253] （６９）ノードＮ１は、乱数を生成すると、送信元を示す識別子「Ｎ１」と、消去カウンタ値Ｒの取得要求を示す連結カウンタ値ＪＣとして設定されている「０ｘ００００００００」と、生成した乱数「０ｘ５８１９」と、を含むパケットを生成する。このとき、送信元を示す識別子は、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0254] （７０）ノードＮ１は、パケットを生成すると、生成したパケット内の連結カウンタ値ＪＣ「０ｘ００００００００」と乱数「０ｘ５８１９」とを、アクセス鍵ＡＫ２を用いて暗号化する。

[0255] （７１）そして、ノードＮ１は、暗号化により得られた暗号化バケツトＥＰをノードＮ２に送信する。次に、図１６に移る。

[0256] （７２）ノードＮ２は、（７１）でノードＮ１から送信された暗号化パケットＥＰを受信すると、受信した暗号化バケツトＥＰから送信元を示す識別子「Ｎ１」を取得し、受信した暗号化パケットＥＰをアクセス鍵ＡＫ２を用いて復号する。そして、ノードＮ２は、復号により得られたパケットから、連結カウンタ値ＪＣ「０ｘ００００００００」と乱数「０ｘ５８１９」とを取得する。

[0257] （７３）ノードＮ２は、取得した連結カウンタ値ＪＣが、消去カウンタ値Ｒの取得要求を示す連結カウンタ値」Ｃとして設定されている「０ｘ００００００００」であることを検出する。そして、ノードＮ２は、取得した送信元を示す識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣをノードＤＢ３００から抽出し、抽出した受信カウンタ値ＲＣから消去カウンタ値Ｒ「０ｘ００」を抽出する。

[0258] （７４）ノードＮ２は、消去カウンタ値Ｒを抽出すると、送信元を示す識

別子「Ｎ２」と、抽出した消去カウンタ値Ｒ「０ｘ００」と、取得した乱数「０ｘ５８１９」と、を含むパケットを生成する。このとき、送信元を示す識別子は、パケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0259] （７５）ノードＮ２は、生成したパケット内の消去カウンタ値Ｒ「０ｘ００」と乱数「０ｘ５８１９」とを固定鍵ＦＫを用いて暗号化する。

[0260] （７６）ノードＮ２は、暗号化により得られた暗号化パケットＥＰを、取得した識別子「Ｎ１」が示すノードＮ１に送信する。次に、図１７に移る。

[0261] （７７）ノードＮ１は、（７６）でノードＮ２から送信された暗号化パケットＥＰを受信すると、受信した暗号化バケツトＥＰから送信元を示す識別子「Ｎ２」を取得し、受信した暗号化パケットＥＰを固定鍵ＦＫを用いて復号する。そして、ノードＮ１は、復号により得られたパケットから、消去カウンタ値Ｒ「０ｘ００」と乱数「０ｘ５８１９」とを取得する。

[0262] （７８）ノードＮ１は、乱数を取得すると、取得した乱数と（６８）でＲＡＭ２０２に保持しておいた乱数との一致判断を行う。ここで、ノードＮ１は、取得した乱数「０ｘ５８１９」とＲＡＭ２０２に保持しておいた乱数「０ｘ５８１９」とが一致するため、（７７）で受信した暗号化パケットＥＰは正規バケツトであると判断する。

[0263] （７９）ノードＮ１は、正規パケットであると判断されると、連結カウンタ値ＪＣが消去される以前の消去カウンタ値Ｒを示す取得した消去カウンタ値Ｒ「０ｘ００」に、１を加算する。そして、ノードＮ１は、加算後の消去カウンタ値Ｒ「０ｘ０１」と送信カウンタ値Ｓの初期値「０ｘ０００００」とを連結して、連結カウンタ値ＪＣ「０ｘ０１０００００」を生成する。これにより、ノードＮ１は、消去された連結カウンタ値ＪＣの代わりに、新たな連結カウンタ値ＪＣを生成する。

[0264] 一方、ノードＮ１は、取得した乱数と（６８）でＲＡＭ２０２に保持しておいた乱数とが一致しない場合は、（７７）で受信した暗号化バケツトＥＰは不正パケットであると判断する。そして、ノードＮ１は、不正パケットで

あると判断されると、復号により得られたパケットを廃棄することで、通信の安全性を担保する。次に、図１８に移る。

[0265] （８０）ノードＮ１は、ノードＮ１のユーザからのノードＮ２を宛先にするデータの入力を受けると、ノードＮ２との暗号化通信を開始する。ここでは、ノードＮ１は、ユーザからのデータの入力をトリガにして暗号化通信を開始したが、ノードＮ１が自動的に発生させたデータ送信イベントをトリガにして暗号化通信を開始してもよい。

[0266] （８１）ノードＮ１は、ノードＮ２を宛先にするデータの入力を受けると、（７９）で生成された新たな連結カウンタ値ＪＣ「０ｘ０１０００００」に１を加算する。

[0267] （８２）ノードＮ１は、送信元を示す識別子「Ｎ１」と、ノードＮ２を宛先にするデータと、加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」と、を含むパケットを生成する。このとき、送信元を示す識別子は、バケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0268] （８３）ノードＮ１は、パケットを生成すると、データの宛先であるノードＮ２を示す識別子「Ｎ２」に関連付けられたアクセス鍵ＡＫ２「０ｘ６６６６」を、ノードＤＢ３００から取得する。そして、ノードＮ１は、生成したバケット内のノードＮ２を宛先にするデータと加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」とを、アクセス鍵ＡＫ２を用いて暗号化する。

[0269] （８４）ノードＮ１は、暗号化により得られた暗号化パケットＥＰを、データの宛先であるノードＮ２に送信する。

[0270] （８５）ノードＮ２は、ノードＮ１から送信された暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰから送信元を示す識別子「Ｎ１」を取得し、受信した暗号化バケットＥＰをアクセス鍵ＡＫ２を用いて復号する。そして、ノードＮ２は、復号により得られたパケットから、ノードＮ２を宛先にするデータと連結カウンタ値」Ｃ「０ｘ０１０００００１」とを取得する。

[0271] （８６）ノードＮ２は、連結カウンタ値ＪＣ「０ｘ０１０００００１」を

取得すると、取得した送信元を示す識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣをノードＤＢ３００から抽出する。

[0272] （８７）そして、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」と、抽出した受信カウンタ値ＲＣ「０ｘ００００１２３０」と、の大小比較を行う。ここで、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」が、抽出した受信カウンタ値ＲＣ「０ｘ００００１２３０」よりも大きいため、受信した暗号化パケットＥＰが正規パケットであると判断する。

[0273] （８８）ノードＮ２は、正規パケットであると判断されると、ノードＤＢ３００において識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣ「０ｘ００００１２３０」を、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」で更新する。

[0274] 一方、ノードＮ２は、取得した連結カウンタ値ＪＣが、抽出した受信カウンタ値ＲＣ以下である場合は、受信した暗号化パケットＥＰが不正パケットであると判断する。そして、ノードＮ２は、不正パケットであると判断されると、復号により得られたパケットを廃棄することで、通信の安全性を担保する。

[0275] このように、ノードＮ１は、消去カウンタ値Ｒを上位桁とし、送信カウンタ値Ｓを下位桁として連結した連結カウンタ値」Ｃを保持し、連結カウンタ値ＪＣが消去されると、消去以前の消去カウンタ値Ｒを他ノードＮから取得する。そして、ノードＮ１は、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とする新たな連結カウンタ値ＪＣを生成する。

[0276] これにより、過去にノードＮ１により送信された暗号化パケットＥＰに含まれていた連結カウンタ値ＪＣより、ノードＮ１により生成された新たな連結カウンタ値ＪＣが大きい値になる。そのため、ノードＮ１は、他ノードＮが保持している受信カウンタ値ＲＣより大きい値になっている連結カウンタ値ＪＣを、他ノードＮに送信する暗号化パケットＥＰに含むことができる。

[0277] そして、ノードN２は、前回受信した暗号化パケットＥＰに含まれていた連結カウンタ値ＪＣを示す受信カウンタ値ＲＣより、今回受信した暗号化パケットＥＰに含まれる連結カウンタ値ＪＣが大きいため、正規バケットと判断することができる。なお、前回受信した暗号化パケットＥＰに含まれていた連結カウンタ値ＪＣは、受信カウンタ値ＲＣとして保持されている。そして、ノードN１は、他ノードNに送信する暗号化パケットＥＰが、他ノードNで不正バケットと判断されないようになるため、アドホックネットワークに復帰することができる。

[0278] また、ノードN１は、取得要求を含むパケットをアクセス鍵ＡＫを用いて暗号化するため、アクセス鍵ＡＫを有さない攻撃者による要求バケットの解析を防止することができる。また、ノードN１は、取得要求を含むパケットに、近隣ノードNとの通信ごとに生成した一時的な識別情報になる乱数を含める。これにより、ノードN１は、自ノードNが送信した暗号化パケットＥＰに含めた乱数と受信した暗号化バケットＥＰに含まれる乱数との一致判断により、正規バケットか否かを通信ごとに判断することができる。

[0279] ここで、通信ごとに異なる乱数が生成されるため、前回の取得要求に対する応答として近隣ノードNが送信した暗号化バケットＥＰを今回の取得要求に対する応答と偽って攻撃者が再送攻撃に使用しても、それぞれの暗号化パケットＥＰに含まれる乱数は不一致になる。そのため、ノードN１は、乱数の不一致から、今回の取得要求に対する応答として受信された暗号化バケットＥＰが再送攻撃による不正バケットと判断でき、通信の安全性を担保することができる。

[0280] また、ノードN１は、一度使用した乱数に有効期間を設定しておくことで、今回の通信で近隣ノードNが応答した暗号化バケットＥＰを攻撃者が再送攻撃に利用した場合に、有効期間を過ぎていれば不正バケットと判断でき、通信の安全性を担保することができる。

[0281] (動作例２における連結カウンタ値生成処理の処理内容)

次に、図１９および図２０を用いて、図１５～図１８に示した動作例２に

おける連結カウンタ値生成処理の詳細な処理手順について説明する。連結カウンタ値生成処理は、図１５～図１８に示したノードＮ１が実行する処理である。ここでは、例としてノードＮ１を実行主体として説明する。

[0282] 図１９および図２０は、動作例２における連結カウンタ値生成処理の詳細な処理手順を示すフローチャートである。まず、ノードＮ１は、連結カウンタ値ＪＣの消去が検出されたか否かを判定する（ステップＳ１９０１）。ここで、連結カウンタ値ＪＣの消去が検出されていない場合（ステップＳ１９０１：Ｎｏ）、ノードＮ１は、ステップＳ１９０１に戻り、連結カウンタ値ＪＣの消去が検出されるのを待つ。

[0283] 一方、連結カウンタ値ＪＣの消去が検出された場合（ステップＳ１９０１：Ｙｅｓ）、ノードＮ１は、アクセス鍵ＡＫを含む暗号化パケットＥＰを近隣ノードＮから受信したか否かを判定する（ステップＳ１９０２）。ここで、アクセス鍵ＡＫを含む暗号化パケットＥＰを受信していない場合（ステップＳ１９０２：Ｎｏ）、ノードＮ１は、ステップＳ１９０２に戻り、アクセス鍵ＡＫを含む暗号化バケットＥＰの受信を待つ。

[0284] 一方、アクセス鍵ＡＫを含む暗号化パケットＥＰを受信した場合（ステップＳ１９０２：Ｙｅｓ）、ノードＮ１は、暗号化バケットＥＰ内の暗号化されない部分（例えば、パケットのヘッダ部分）から、送信元を示す識別子を取得する（ステップＳ１９０３）。

[0285] そして、ノードＮ１は、受信した暗号化パケットＥＰを固定鍵ＦＫを用いて復号する（ステップＳ１９０４）。次に、ノードＮ１は、復号により得られたバケットからアクセス鍵ＡＫを抽出し、抽出したアクセス鍵ＡＫと取得した送信元を示す識別子と関連付けたレコードを、ノードＤＢ３００に追加する（ステップＳ１９０５）。

[0286] そして、ノードＮ１は、一時的な識別情報になる乱数を生成する（ステップＳ１９０６）。次に、ノードＮ１は、送信元になる自ノードＮを示す識別子と、生成した乱数と、送信カウンタ値Ｓの取得要求と、を含むパケットを生成する（ステップＳ１９０７）。

[0287] そして、ノードN１は、生成したパケットを、ステップＳ１９０５で抽出されたアクセス鍵ＡＫを用いて暗号化する（ステップＳ１９０８）。次に、ＣＰＵ２０１は、暗号化により得られた暗号化パケットＥＰを、ステップＳ１９０３で取得された識別子が示すノードNに送信する（ステップＳ１９０９）。そして、ノードＮ１は、図２０のステップＳ２００１に移行する。

[0288] 図２０において、ノードＮ１は、取得要求に対する応答になる暗号化パケットＥＰを、ステップＳ１９０３で取得された識別子が示すノードNから受信したか否かを判定する（ステップＳ２００１）。ここで、暗号化パケットＥＰを受信していない場合（ステップＳ２００１：Ｎｏ）、ノードＮ１は、ステップＳ２００１に戻り、暗号化バケツトＥＰの受信を待つ。

[0289] 一方、暗号化パケットＥＰを受信した場合（ステップＳ２００１：Ｙｅｓ）、ノードＮ１は、暗号化バケツトＥＰ内の暗号化されない部分（例えば、パケットのヘッダ部分）から、送信元を示す識別子を取得する（ステップＳ２００２）。

[0290] 次に、ノードＮ１は、受信した暗号化パケットＥＰを固定鍵ＦＫを用いて復号する（ステップＳ２００３）。そしてノードＮ１は、復号により得られたパケットから乱数を抽出し、抽出した乱数が、ステップＳ１９０６で生成した乱数と一致するか否かを判定する（ステップＳ２００４）。

[0291] ここで、一致する場合（ステップＳ２００４：Ｙｅｓ）、ノードＮ１は、復号により得られたバケツトから消去カウンタ値Ｒを抽出し、抽出した消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒと送信カウンタ値Ｓの初期値とを連結して連結カウンタ値ＪＣを生成する（ステップＳ２００５）。そして、ノードＮ１は、生成した連結カウンタ値ＪＣをＲＡＭ２０２に保存して（ステップＳ２００６）、連結カウンタ値生成処理を終了する。

[0292] 一方、一致しない場合（ステップＳ２００４：Ｎｏ）、ノードＮ１は、受信した暗号化バケツトＥＰが不正バケツトであると判断して、復号により得られたパケットを廃棄し（ステップＳ２００７）、連結カウンタ値生成処理を終了する。

[0293] これにより、ノードNは、連結カウンタ値ＪＣが消去された場合であっても、消去された連結カウンタ値ＪＣより大きい値の新たな連結カウンタ値ＪＣを生成することができる。そして、ノードNは、送信するパケットが他ノードNに廃棄されないようになり、アドホックネットワークに復帰できる。

[0294] また、ノードNは、取得要求を含むパケットをアクセス鍵ＡＫを用いて暗号化するため、アクセス鍵ＡＫを有さない攻撃者による要求バケットの解析を防止することができる。また、ノードNは、取得要求を含むパケットに、近隣ノードNとの通信ごとに生成した一時的な識別情報になる乱数を含める。これにより、ノードNは、自ノードNが送信した暗号化パケットＥＰに含めた乱数と受信した暗号化バケットＥＰに含まれる乱数との一致判断により、正規バケットか否かを通信ごとに判断することができる。

[0295] ここで、通信ごとに異なる乱数が生成されるため、前回の取得要求に対する応答として近隣ノードNが送信した暗号化バケットＥＰを今回の取得要求に対する応答と偽って攻撃者が再送攻撃に使用しても、それぞれの暗号化パケットＥＰに含まれる乱数は不一致になる。そのため、ノードNは、乱数の不一致から、今回の取得要求に対する応答として受信された暗号化バケットＥＰが再送攻撃による不正バケットと判断でき、通信の安全性を担保することができる。

[0296] また、ノードNは、一度使用した乱数に有効期間を設定しておくことで、今回の通信で近隣ノードNが応答した暗号化パケットＥＰを攻撃者が再送攻撃に利用した場合に、有効期間を過ぎていれば不正パケットと判断でき、通信の安全性を担保することができる。

[0297] （ノードNの連結カウンタ値ＪＣが消去された場合の動作例３）

次に、図２１および図２２を用いて、ノードNの連結カウンタ値ＪＣが消去された場合の動作例３について説明する。動作例１および動作例２は自ノードNに電力供給されなくなると連結カウンタ値ＪＣとともに消去カウンタ値Ｒも消去されたが、動作例３は自ノードNに電力供給されない状態でも消去されないように不揮発性メモリに消去カウンタ値Ｒを保持しておく。これ

により、他ノードNから消去カウンタ値Ｒを取得しないため、再送攻撃の危険性を低減し、通信の安全性を担保することができる。

[0298] 図２１および図２２は、ノードNの連結カゥンタ値ＪＣが消去された場合の動作例３を示す説明図である。なお、図１で説明した箇所と同様の箇所についての説明は省略する。図２１において、ノードＮ１は、ノードＮ２から受信され、ノードＮ２へ送信するバケツトの暗号化に使用されるアクセス鍵ＡＫ２「０ｘ２２２２」を保持している。

[0299] また、ノードＮ１は、連結カウンタ値ＪＣ「０ｘ００００１２３０」を保持している。ここで、連結カウンタ値ＪＣは、頻繁に書き換えが行われるため、揮発性であるＲＡＭ２０２に保持されている。ノードＮ１は、連結カウンタ値ＪＣとは別に、消去カウンタ値Ｒ「０ｘ００」を保持している。ここで、消去カウンタ値Ｒは、不揮発性であるフラッシュメモリ２０３に保持されている。

[0300] ノードＮ２は、過去にノードＮ１から受信した暗号化パケットＥＰを復号して得られたバケツトから連結カウンタ値ＪＣを抽出し、抽出した連結カウンタ値ＪＣ「０ｘ００００１２３０」を受信カウンタ値ＲＣとして保持している。

[0301] 図２１において、停電によりノードＮ１に電力が供給されず、ノードＮ１が保持していた連結カウンタ値ＪＣ「０ｘ００００１２３０」およびァクセス鍵ＡＫ２が消去されてしまったとする。そのため、他ノードNに送信するバケツトに含むべき連結カウンタ値ＪＣが不明になり、ノードＮ１は、他ノードNにバケツトを送信することができない。

[0302] （９１）ここで、ノードＮ１は、停電が回復し電力が供給されると、保持していた連結カウンタ値ＪＣが消去されたことを検出する。

[0303] （９２）ノードＮ１は、連結カウンタ値ＪＣが消去されたことを検出すると、フラッシュメモリ２０３に保持されている消去カウンタ値Ｒ「０ｘ００」に１を加算する。

[0304] （９３）そして、ノードＮ１は、フラッシュメモリ２０３に保持されてい

る加算後の消去カウンタ値Ｒ「０ｘ０１」と送信カウンタ値Ｓの初期値「０ｘ０００００」とを連結して、連結カウンタ値ＪＣ「０ｘ０１０００００」を生成する。これにより、ノードＮ１は、消去された連結カウンタ値ＪＣの代わりに、新たな連結カウンタ値ＪＣを生成する。次に、図２２に移る。

[0305] （９４）ノードＮ１は、ノードＮ１のユーザからのノードＮ２を宛先にするデータの入力を受けると、ノードＮ２との暗号化通信を開始する。ここでは、ノードＮ１は、ユーザからのデータの入力をトリガにして暗号化通信を開始したが、ノードＮ１が自動的に発生させたデータ送信イベントをトリガにして暗号化通信を開始してもよい。

[0306] （９５）ノードＮ１は、ノードＮ２を宛先にするデータの入力を受けると、（９３）で生成された新たな連結カウンタ値ＪＣ「０ｘ０１０００００」に１を加算する。

[0307] （９６）ノードＮ１は、送信元を示す識別子「Ｎ１」と、ノードＮ２を宛先にするデータと、加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」と、を含むパケットを生成する。このとき、送信元を示す識別子は、バケット内の暗号化されない部分（例えば、パケットのヘッダ部分）に含まれる。

[0308] （９７）ノードＮ１は、パケットを生成すると、生成したパケット内のノードＮ２を宛先にするデータと加算後の連結カウンタ値ＪＣ「０ｘ０１０００００１」とを固定鍵ＦＫを用いて暗号化する。

[0309] （９８）ノードＮ１は、暗号化により得られた暗号化パケットＥＰを、データの宛先であるノードＮ２に送信する。

[0310] （９９）ノードＮ２は、ノードＮ１から送信された暗号化パケットＥＰを受信すると、受信した暗号化パケットＥＰから送信元を示す識別子「Ｎ１」を取得し、受信した暗号化パケットＥＰを、固定鍵ＦＫを用いて復号する。そして、ノードＮ２は、復号により得られたパケットから、ノードＮ２を宛先にするデータと連結カウンタ値ＪＣ「０ｘ０１０００００１」とを取得する。

[031 1] （１００）ノードＮ２は、連結カウンタ値ＪＣ「０ｘ０１０００００１」を取得すると、取得した送信元を示す識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣをノードＤＢ３００から抽出する。

[031 2] （１０１）そして、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」と、抽出した受信カウンタ値ＲＣ「０ｘ０００１２３０」と、の大小比較を行う。ここで、ノードＮ２は、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」が、抽出した受信カウンタ値ＲＣ「０ｘ０００１２３０」よりも大きいため、受信した暗号化パケットＥＰが正規パケットであると判断する。

[031 3] （１０２）ノードＮ２は、正規パケットであると判断されると、ノードＤＢ３００において識別子「Ｎ１」に関連付けられた受信カウンタ値ＲＣ「０ｘ０００１２３０」を、取得した連結カウンタ値ＪＣ「０ｘ０１０００００１」で更新する。

[0314] 一方、ノードＮ２は、取得した連結カウンタ値ＪＣが、抽出した受信カウンタ値ＲＣ以下である場合は、受信した暗号化パケットＥＰが不正パケットであると判断する。そして、ノードＮ２は、不正パケットであると判断されると、復号により得られたパケットを廃棄することで、通信の安全性を担保する。

[031 5] このように、ノードＮ１は、揮発性メモリ（例えばＲＡＭ２０２）に連結カウンタ値ＪＣを保持しておくことで、送信時の連結カウンタ値ＪＣの読み出し処理や、受信時の連結カウンタ値ＪＣの更新処理を高速に実行できる。

[031 6] また、ノードＮ１は、不揮発性メモリ（例えばフラッシュメモリ２０３）に、書き換え頻度の低い消去カウンタ値Ｒのみを、連結カウンタ値ＪＣとは別に保持しておく。ノードＮ１は、連結カウンタ値ＪＣが消去されると、消去以前の消去カウンタ値Ｒを不揮発性メモリから取得する。そして、ノードＮ１は、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とする新たな連結カウンタ値ＪＣを生成する。これにより、過去にノードＮ１により送信された暗号化パケットＥＰに含まれていた連結カ

ゥンタ値ＪＣより、ノードＮ１により生成された新たな連結カウンタ値ＪＣが大きい値になる。そのため、ノードＮ１は、他ノードＮが保持している受信カウンタ値ＲＣより大きい値になっている連結カウンタ値ＪＣを、他ノードＮに送信する暗号化バケツトＥＰに含むことができる。

[031 7] これにより、ノードＮ２は、保持している受信カウンタ値ＲＣより、ノードＮ１から受信した暗号化バケツトＥＰに含まれる連結カウンタ値ＪＣが大きいため、ノードＮ１から受信した暗号化バケツトＥＰを正規バケツトと判断することができる。そして、ノードＮ１は、他ノードＮに送信する暗号化バケツトＥＰが、他ノードＮで不正バケツトと判断されないようになるため、アドホックネットワークに復帰することができる。また、他ノードＮから消去カウンタ値Ｒを取得しないため、再送攻撃の危険性を低減し、通信の安全性を担保することができる。

[031 8] (動作例３における連結カウンタ値生成処理の処理内容)

次に、図２３を用いて、図２１および図２２に示した動作例３における連結カウンタ値生成処理の詳細な処理手順を示すフローチャートである。連結カウンタ値生成処理は、図２１および図２２に示したノードＮ１が実行する処理である。ここでは、例としてノードＮ１を実行主体として説明する。

[031 9] 図２３は、動作例３における連結カゥンタ値生成処理の詳細な処理手順を示すフローチャートである。まず、ノードＮ１は、連結カウンタ値ＪＣの消去が検出されたか否かを判定する (ステップＳ２３０１)。連結カウンタ値ＪＣの消去が検出されていない場合 (ステップＳ２３０１ :Ｎｏ)、ノードＮ１は、ステップＳ２３０１に戻り、連結カウンタ値ＪＣの消去が検出されるのを待つ。

[0320] 一方、連結カウンタ値ＪＣの消去が検出された場合 (ステップＳ２３０１ :Ｙｅｓ)、ノードＮ１は、不揮発性メモリから消去カウンタ値Ｒを読み出す (ステップＳ２３０２)。そして、ノードＮ１は、読み出した消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒと送信カウンタ値Ｓの初期値とを連結した連結カウンタ値ＪＣを生成する (ステップＳ２３０３)。

[0321] そして、ノードN１は、生成した連結カウンタ値ＪＣをＲＡＭ２０２に保存して (ステップＳ２３０４)、連結カウンタ値生成処理を終了する。これにより、ノードNは、連結カウンタ値ＪＣが消去された場合であつても、消去された連結カゥンタ値ＪＣより大きい値の新たな連結カゥンタ値ＪＣを生成することができる。そして、ノードNは、送信するパケットが他ノードNに廃棄されないようになり、アドホックネットワークに復帰できる。

[0322] 以上説明したように、ノードNは、連結カウンタ値ＪＣを保持し、連結カゥンタ値ＪＣが消去されると、消去以前の消去カウンタ値Ｒを他ノードNから取得する。そして、ノードNは、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カゥンタ値Ｒを上位桁とする新たな連結カゥンタ値ＪＣを生成する。これにより、過去にノードNにより送信された暗号化パケットＥＰに含まれていた連結カウンタ値ＪＣより、新たな連結カウンタ値ＪＣが大きい値になる。そのため、ノードNは、他ノードNが保持している受信カウンタ値ＲＣより大きい値になっている連結カウンタ値ＪＣを、他ノードNに送信する暗号化バケツトＥＰに含むことができる。

[0323] これにより、他ノードNは、保持している受信カウンタ値ＲＣより、ノードNから受信した暗号化バケツトＥＰに含まれる連結カウンタ値ＪＣが大きいため、ノードNから受信した暗号化バケツトＥＰを正規バケツトと判断することができる。そして、ノードNは、他ノードNに送信する暗号化バケツトＥＰが、他ノードNで不正パケットと判断されないようになるため、アドホックネットワークに復帰することができる。このように、連結カウンタ値ＪＣが復旧されるため、時刻同期パケットによる同期が不要になり、アドホックネットワーク内の通信負荷の低減を図ることができる。

[0324] また、ノードNは、取得要求を含むパケットを固定鍵ＦＫを用いて暗号化するため、固定鍵ＦＫを有さない攻撃者による要求バケツトの解析を防止することができる。また、ノードNは、取得要求を含むパケットに、近隣ノードNとの通信ごとに生成した一時的な識別情報になる乱数を含める。これにより、ノードNは、自ノードNが送信した暗号化パケットＥＰに含めた乱数

と受信した暗号化バケツトＥＰに含まれる乱数との一致判断により、正規パケットか否かを通信ごとに判断することができる。

[0325] ここで、通信ごとに異なる乱数が生成されるため、前回の取得要求に対する応答として近隣ノードNが送信した暗号化バケツトＥＰを今回の取得要求に対する応答と偽って攻撃者が再送攻撃に使用しても、それぞれの暗号化パケットＥＰに含まれる乱数は不一致になる。そのため、ノードNは、乱数の不一致から、今回の取得要求に対する応答として受信された暗号化バケツトＥＰが再送攻撃による不正バケツトと判断でき、通信の安全性を担保することができる。

[0326] また、ノードNは、連結カウンタ値ＪＣを保持し、連結カウンタ値ＪＣが消去されると、消去以前の消去カウンタ値Ｒを他ノードNから取得する。そして、ノードNは、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とする新たな連結カウンタ値ＪＣを生成する。これにより、過去にノードNにより送信された暗号化バケツトＥＰに含まれていた連結カウンタ値」Ｃより、ノードNにより生成された新たな連結カウンタ値ＪＣが大きい値になる。そのため、ノードNは、他ノードNが保持している受信カウンタ値ＲＣより大きい値になっている連結カウンタ値ＪＣを、他ノードNに送信する暗号化バケツトＥＰに含むことができる。

[0327] これにより、他ノードNは、保持している受信カウンタ値ＲＣより、ノードNから受信した暗号化バケツトＥＰに含まれる連結カウンタ値ＪＣが大きいため、ノードNから受信した暗号化バケツトＥＰを正規バケツトと判断することができる。そして、ノードNは、他ノードNに送信する暗号化バケツトＥＰが、他ノードNで不正パケットと判断されないようになるため、アドホックネットワークに復帰することができる。

[0328] また、ノードNは、取得要求を含むパケットをアクセス鍵ＡＫを用いて暗号化するため、アクセス鍵ＡＫを有さない攻撃者による要求バケツトの解析を防止できる。また、ノードNは、取得要求を含むパケットに、近隣ノードNとの通信ごとに生成した一時的な識別情報になる乱数を含める。これによ

り、ノードNは、自ノードNが送信した暗号化パケットＥＰに含めた乱数と受信した暗号化バケットＥＰに含まれる乱数との一致判断により、正規パケットか否かを通信ごとに判断することができる。

[0329] ここで、通信ごとに異なる乱数が生成されるため、前回の取得要求に対する応答として近隣ノードNが送信した暗号化バケットＥＰを今回の取得要求に対する応答と偽って攻撃者が再送攻撃に使用しても、それぞれの暗号化パケットＥＰに含まれる乱数は不一致になる。そのため、ノードNは、乱数の不一致から、今回の取得要求に対する応答として受信された暗号化バケットＥＰが再送攻撃による不正バケットと判断でき、通信の安全性を担保することができる。

[0330] また、ノードNは、揮発性メモリ(例えばＲＡＭ２０２）に連結カウンタ値ＪＣを保持しておくことで、送信時の連結カウンタ値ＪＣの読み出し処理や、受信時の連結カウンタ値ＪＣの更新処理を高速に実行できる。また、ノードNは、不揮発性メモリ(例えばフラッシュメモリ２０３）に、書き換え頻度の低い消去カウンタ値Ｒのみを、連結カウンタ値ＪＣとは別に保持しておく。

[0331] ノードNは、連結カウンタ値ＪＣが消去されると、消去以前の消去カウンタ値Ｒを不揮発性メモリから取得する。そして、ノードNは、消去以前の消去カウンタ値Ｒに１を加算した加算後の消去カウンタ値Ｒを上位桁とする新たな連結カウンタ値ＪＣを生成する。これにより、過去にノードNにより送信された暗号化バケットＥＰに含まれていた連結カウンタ値ＪＣより、ノードNにより生成された新たな連結カウンタ値ＪＣが大きい値になる。そのため、ノードNは、他ノードNが保持している受信カウンタ値ＲＣより大きい値になっている連結カウンタ値ＪＣを、他ノードNに送信する暗号化バケットＥＰに含むことができる。

[0332] これにより、他ノードNは、保持している受信カウンタ値ＲＣより、ノードNから受信した暗号化バケットＥＰに含まれる連結カウンタ値ＪＣが大きいため、ノードNから受信した暗号化バケットＥＰを正規バケットと判断す

ることができる。そして、ノードNは、他ノードNに送信する暗号化パケットＥＰが、他ノードNで不正パケットと判断されないようになるため、アドホックネットワークに復帰することができる。また、他ノードNから消去カウンタ値Ｒを取得しないため、再送攻撃の危険性を低減し、通信の安全性を担保することができる。

[0333] なお、本実施の形態で説明した通信方法は、予め用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。本通信プログラムは、ハードディスク、フレキシブルディスク、ＣＤ_ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによつて記録媒体から読み出されることによって実行される。また本通信プログラムは、インターネット等のネットワークを介して配布してもよい。

符号の説明

[0334] Ｎ，Ｎ１～３　ノード

ＪＣ　連結カウンタ値

Ｒ　消去カウンタ値

Ｓ　送信カウンタ値

ＲＣ　受信カウンタ値

４０１　第１の記憶部

４０２　更新部

４０３　送信部

４０４　暗号化部

４０５　乱数生成部

４０６　検出部

４０７　受信部

４０８　復号部

４０９　生成部

４１０　保存部

４１１　第２の記憶部

４１２　抽出部

５０１　第１の受信部

５０２　第１の保存部

５０３　第２の受信部

５０４　判断部

５０５　第２の保存部

５０６　データ処理部

５０７　第３の受信部

５０８　抽出部

５０９　送信部

請求の範囲

[請求項1] アドホックネットワーク内のノードであって、

自ノードでの消去回数を示す消去カウンタ値を上位桁とし前記自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段と、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記記憶手段に記憶されている連結カウンタ値のうち前記送信カウンタ値を1加算する更新手段と、

前記データおよび前記更新手段による更新後の連結カウンタ値を前記他ノードに送信する送信手段と、

前記記憶手段での前記連結カウンタ値の消去を検出する検出手段と、

前記検出手段によって消去が検出された場合、前記消去カウンタ値の取得要求を前記アドホックネットワークに配信する配信手段と、

前記配信手段によつて前記取得要求が配信された結果、前記アドホックネットワークから前記消去カウンタ値を受信する受信手段と、

前記受信手段によって受信された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になつたことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成する生成手段と、

前記生成手段によって生成された連結カウンタ値を前記記憶手段に保存する保存手段と、

を備えることを特徴とするノード。

[請求項2] アドホックネットワーク内のノードであつて、

自ノードでの消去回数を示す消去カウンタ値を上位桁とし前記自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段と、

前記アドホックネットワーク内の他ノードにデータを送信する場合

、前記記憶手段に記憶されている連結カウンタ値のうち前記送信カウンタ値を1加算する更新手段と、

前記データおよび前記更新手段による更新後の連結カウンタ値を前記他ノードに送信する送信手段と、

前記記憶手段での前記連結カウンタ値の消去を検出する検出手段と、

前記検出手段によって消去が検出された場合、前記消去カウンタ値の更新要求を前記アドホックネットワークに配信する配信手段と、

前記配信手段によつて前記更新要求が配信された結果、前記アドホックネットワークから前記消去カウンタ値に1加算された加算後の消去カウンタ値を受信する受信手段と、

前記受信手段によって受信された加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成する生成手段と、

前記生成手段によって生成された連結カウンタ値を前記記憶手段に保存する保存手段と、

を備えることを特徴とするノード。

[請求項3] アドホックネットワーク内のノードであつて、

自ノードでの消去回数を示す消去カウンタ値を上位桁とし前記自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する揮発性の第1の記憶手段と、

前記消去カウンタ値を記憶する不揮発性の第2の記憶手段と、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記第1の記憶手段に記憶されている連結カウンタ値のうち前記送信カウンタ値を1加算する更新手段と、

前記データおよび前記更新手段による更新後の連結カウンタ値を前記他ノードに送信する送信手段と、

前記第1の記憶手段での前記連結カウンタ値の消去を検出する検出

手段と、

前記検出手段によつて消去が検出された場合、前記第２の記憶手段から前記消去カウンタ値を抽出する抽出手段と、

前記抽出手段によって抽出された消去カウンタ値に１加算した加算後の消去カウンタ値を上位桁とし前記消去により送信回数が０になつたことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成する生成手段と、

前記生成手段によって生成された連結カウンタ値を前記第１の記憶手段に保存するとともに、前記第２の記憶手段に記憶されている前記消去カウンタ値に対し前記加算後の消去カウンタ値を上書き保存する保存手段と、

を備えることを特徴とするノード。

[請求項4] 自ノードおよび前記他ノードが有する共通鍵を用いて、自ノード固有の第１の識別情報を含む前記取得要求を暗号化する暗号化手段と、

前記共通鍵を用いて暗号化されたデータを、前記共通鍵を用いて復号する復号手段と、を備え、

前記配信手段は、

前記暗号化手段によって暗号化された前記取得要求を前記アドホックネットワークに配信し、

前記受信手段は、

前記共通鍵を用いて暗号化された前記消去カウンタ値と前記共通鍵を用いて暗号化された第２の識別情報とを、前記アドホックネットワークから受信し、

前記復号手段は、

前記受信手段によって受信された暗号化された前記消去カウンタ値と暗号化された前記第２の識別情報を、前記共通鍵を用いて復号し、

前記生成手段は、

前記第１の識別情報と前記復号手段によって復号された前記第２の

識別情報とが一致した場合に、前記復号手段によって復号された前記消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成することを特徴とする請求項1に記載のノード。

[請求項5] 自ノードおよび前記他ノードが有する共通鍵を用いて、自ノード固有の第1の識別情報を含む前記更新要求を暗号化する暗号化手段と、

前記共通鍵を用いて暗号化されたデータを、前記共通鍵を用いて復号する復号手段と、を備え、

前記配信手段は、

前記暗号化手段によって暗号化された前記更新要求を前記アドホックネットワークに配信し、

前記受信手段は、

前記共通鍵を用いて暗号化された前記加算後の消去カウンタ値と前記共通鍵を用いて暗号化された前記第2の識別情報とを、前記アドホックネットワークから受信し、

前記復号手段は、

前記受信手段によって受信された暗号化された前記加算後の消去カウンタ値と暗号化された前記第2の識別情報を、前記共通鍵を用いて復号し、

前記生成手段は、

前記第1の識別情報と前記復号手段によって復号された前記第2の識別情報とが一致した場合に、前記復号手段によって復号された前記加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成することを特徴とする請求項2に記載のノード。

[請求項6] 前記第1の識別情報は乱数であることを特徴とする請求項4または5に記載のノード。

[請求項7] アドホックネットワーク内のノードであって、

他ノードでの消去回数を示す消去カウンタ値を上位桁とし前記他ノードからの送信回数を示す送信カウンタ値を下位桁とする第1の連結カウンタ値を、前記他ノードから受信する第1の受信手段と、

前記第1の受信手段によって受信された連結カウンタ値を記憶装置に保存する第1の保存手段と、

第2の連結カウンタ値を前記他ノードから受信する第2の受信手段と、

前記第2の受信手段によつて受信された第2の連結カウンタ値が前記第1の連結カウンタ値よりも大きいか否かを判断する判断手段と、

前記判断手段によって大きいと判断された場合、前記第1の連結カウンタ値に前記第2の連結カウンタ値を上書保存する第2の保存手段と、

を備えることを特徴とするノード。

[請求項8] 前記他ノードから前記消去カウンタ値の取得要求を受信する第3の受信手段と、

前記第3の受信手段によって前記取得要求が受信された場合、前記記憶装置に記憶されている前記連結カウンタ値の中の消去カウンタ値を抽出する抽出手段と、

前記抽出手段によって抽出された消去カウンタ値を前記他ノードに送信する送信手段と、

を備えることを特徴とする請求項7に記載のノード。

[請求項9] 前記他ノードから前記消去カウンタ値の更新要求を受信する第3の受信手段と、

前記第3の受信手段によって前記更新要求が受信された場合、前記記憶装置に記憶されている前記連結カウンタ値の中の消去カウンタ値を抽出する抽出手段と、

前記抽出手段によって抽出された消去カウンタ値に1加算した加算

後の消去カウンタ値を前記他ノードに送信する送信手段と、

を備えることを特徴とする請求項7に記載のノード。

[請求項10] 前記判断手段によって大きくないと判断された場合、前記第2の連結カウンタ値とともに受信されたデータを廃棄する廃棄手段を備えることを特徴とする請求項7～9のいずれか一つに記載のノード。

[請求項11] アドホックネットワークを構成するノードにおける通信方法であつて、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記ノードでの消去回数を示す消去カウンタ値を上位桁とし前記自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段に記憶されている連結カウンタ値のうち、前記送信カウンタ値を1加算し、

前記データおよび加算後の連結カゥンタ値を前記他ノードに送信し、

前記記憶手段での前記連結カゥンタ値の消去を検出し、

消去が検出された場合、前記消去カウンタ値の取得要求を前記アドホックネットワークに配信し、

前記取得要求が配信された結果、前記アドホックネットワークから前記消去カウンタ値を受信し、

受信された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、

生成された連結カウンタ値を前記記憶手段に保存する、

ことを特徴とする通信方法。

[請求項12] アドホックネットワークを構成するノードにおける通信方法であつて、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記ノードでの消去回数を示す消去カウンタ値を上位桁とし前記自

ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段に記憶されている連結カウンタ値のうち、前記送信カウンタ値を1加算し、

前記データおよび加算後の連結カウンタ値を前記他ノードに送信し、

前記記憶手段での前記連結カウンタ値の消去を検出し、

消去が検出された場合、前記消去カウンタ値の更新要求を前記アドホックネットワークに配信し、

前記更新要求が配信された結果、前記アドホックネットワークから前記消去カウンタ値に1加算された加算後の消去カウンタ値を受信し、

受信された加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、

生成された連結カウンタ値を前記記憶手段に保存する、

ことを特徴とする通信方法。

[請求項13] アドホックネットワークを構成するノードにおける通信方法であつて、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記ノードでの消去回数を示す消去カウンタ値を上位桁とし前記自ノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する揮発性の第1の記憶手段に記憶されている連結カウンタ値のうち、前記送信カウンタ値を1加算し、

前記データおよび加算後の連結カウンタ値を前記他ノードに送信し、

前記第1の記憶手段での前記連結カウンタ値の消去を検出し、

消去が検出された場合、前記消去カウンタ値を記憶する不揮発性の第2の記憶手段から前記消去カウンタ値を抽出し、

抽出された消去カウンタ値に1加算した加算後の消去カウンタ値を上位桁とし前記消去により送信回数が0になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成し、

生成された連結カウンタ値を前記第1の記憶手段に保存するとともに、前記第2の記憶手段に記憶されている前記消去カウンタ値に対し前記加算後の消去カウンタ値を上書き保存する、

ことを特徴とする通信方法。

[請求項14] アドホックネットワークを構成するノードにおける通信方法であつて、

他ノードでの消去回数を示す消去カウンタ値を上位桁とし前記他ノードからの送信回数を示す送信カウンタ値を下位桁とする第1の連結カウンタ値を、前記他ノードから受信し、

受信された連結カウンタ値を記憶装置に保存し、

第2の連結カウンタ値を前記他ノードから受信し、

前記第2の連結カウンタ値が前記第1の連結カウンタ値よりも大きいか否かを判断し、

大きいと判断された場合、前記第1の連結カウンタ値に前記第2の連結カウンタ値を上書保存する、

ことを特徴とする通信方法。

[請求項15] アドホックネットワーク内の第1のノードと第2のノードとが通信するシステムであって、

前記第1のノードは、

前記第1のノードでの消去回数を示す消去カウンタ値を上位桁とし前記第1のノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段と、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記記憶手段に記憶されている連結カウンタ値のうち前記送信カウンタ値を1加算する更新手段と、

前記第２のノードを宛先にする第１のデータおよび前記更新手段による更新後の第１の連結カウンタ値を前記第２のノードに送信する第１の送信手段と、

前記記憶手段での前記連結カゥンタ値の消去を検出する検出手段と、

前記検出手段によって消去が検出された場合、前記消去カゥンタ値の取得要求を前記アドホックネットワークに配信する配信手段と、

前記配信手段によつて前記取得要求が配信された結果、前記アドホックネットワークから前記消去カゥンタ値を受信する応答受信手段と、

前記応答受信手段によって受信された消去カウンタ値に１加算した加算後の消去カゥンタ値を上位桁とし前記消去により送信回数が０になったことを示す消去後の送信カゥンタ値を下位桁とする連結カゥンタ値を生成する生成手段と、

前記生成手段によって生成された連結カゥンタ値を前記記憶手段に保存する生成値保存手段と、

前記生成値保存手段によって保存された後に、前記第２のノードを宛先にする第２のデータおよび前記記憶手段に記憶されている最新の連結カウンタ値について前記更新手段によって更新された第２の連結カウンタ値を、前記第２のノードに送信する第２の送信手段と、を備え、

前記第２のノードは、

前記第１の連結カウンタ値を、前記第１のノードから受信する第１の受信手段と、

前記第１の受信手段によって受信された第１の連結カウンタ値を記憶装置に保存する第１の保存手段と、

前記第２の連結カウンタ値を、前記第１のノードから受信する第２の受信手段と、

前記第２の受信手段によつて受信された第２の連結カウンタ値が前記第１の連結カウンタ値よりも大きいか否かを判断する判断手段と、

前記判断手段によって大きいと判断された場合、前記第１の連結カウンタ値を前記第２の連結カウンタ値に上書保存する第２の保存手段と、

を備えることを特徴とする通信システム。

[請求項16] アドホックネットワーク内の第１のノードと第２のノードとが通信するシステムであって、

前記第１のノードは、

前記第１のノードでの消去回数を示す消去カウンタ値を上位桁とし前記第１のノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する記憶手段と、

前記アドホックネットワーク内の他ノードにデータを送信する場合、前記記憶手段に記憶されている連結カウンタ値のうち前記送信カウンタ値を１加算する更新手段と、

前記第２のノードを宛先にする第１のデータおよび前記更新手段による更新後の第１の連結カウンタ値を前記第２のノードに送信する第１の送信手段と、

前記記憶手段での前記連結カウンタ値の消去を検出する検出手段と、

前記検出手段によって消去が検出された場合、前記消去カウンタ値の更新要求を前記アドホックネットワークに配信する配信手段と、

前記配信手段によつて前記更新要求が配信された結果、前記アドホックネットワークから前記消去カウンタ値に１加算された加算後の消去カウンタ値を受信する応答受信手段と、

前記応答受信手段によって受信された加算後の消去カウンタ値を上位桁とし前記消去により送信回数が０になったことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成する生成手段と、

前記生成手段によって生成された連結カウンタ値を前記記憶手段に保存する生成値保存手段と、

前記生成値保存手段によって保存された後に、前記第２のノードを宛先にする第２のデータおよび前記記憶手段に記憶されている最新の連結カウンタ値について前記更新手段によって更新された第２の連結カウンタ値を前記第２のノードに送信する第２の送信手段と、を備え、

前記第２のノードは、

前記第１の連結カウンタ値を、前記第１のノードから受信する第１の受信手段と、

前記第１の受信手段によって受信された第１の連結カウンタ値を記憶装置に保存する第１の保存手段と、

前記第２の連結カウンタ値を、前記第１のノードから受信する第２の受信手段と、

前記第２の受信手段によつて受信された第２の連結カウンタ値が前記第１の連結カウンタ値よりも大きいか否かを判断する判断手段と、

前記判断手段によって大きいと判断された場合、前記第１の連結カウンタ値を前記第２の連結カウンタ値に上書保存する第２の保存手段と、

を備えることを特徴とする通信システム。

[請求項17] アドホックネットワーク内の第１のノードと第２のノードとが通信するシステムであって、

前記第１のノードは、

前記第１のノードでの消去回数を示す消去カウンタ値を上位桁とし前記第１のノードからの送信回数を示す送信カウンタ値を下位桁とする連結カウンタ値を記憶する揮発性の第１の記憶手段と、

前記消去カウンタ値を記憶する不揮発性の第２の記憶手段と、

前記アドホックネットワーク内の他ノードにデータを送信する場合

、前記第１の記憶手段に記憶されている連結カウンタ値のうち前記送信カウンタ値を１加算する更新手段と、

前記第２のノー ドを宛先にする第１のデータおよび前記更新手段による更新後の第１の連結カウンタ値を前記第２のノー ドに送信する第１の送信手段と、

前記第１の記憶手段での前記連結カウンタ値の消去を検出する検出手段と、

前記検出手段によつて消去が検出された場合、前記第２の記憶手段から前記消去カウンタ値を抽出する抽出手段と、

前記抽出手段によって抽出された消去カウンタ値に１加算した加算後の消去カウンタ値を上位桁とし前記消去により送信回数が０になつたことを示す消去後の送信カウンタ値を下位桁とする連結カウンタ値を生成する生成手段と、

前記生成手段によって生成された連結カウンタ値を前記第１の記憶手段に保存するとともに、前記第２の記憶手段に記憶されている前記消去カウンタ値に対し前記加算後の消去カウンタ値を上書き保存する生成値保存手段と、

前記生成値保存手段によって保存された後に、前記第２のノー ドを宛先にする第２のデータおよび前記記憶手段に記憶されている最新の連結カウンタ値について前記更新手段によって更新された第２の連結カウンタ値を前記第２のノー ドに送信する第２の送信手段と、を備え、

前記第２のノー ドは、

前記第１の連結カウンタ値を、前記第１のノー ドから受信する第１の受信手段と、

前記第１の受信手段によって受信された第１の連結カウンタ値を記憶装置に保存する第１の保存手段と、

前記第２の連結カウンタ値を、前記第１のノー ドから受信する第２

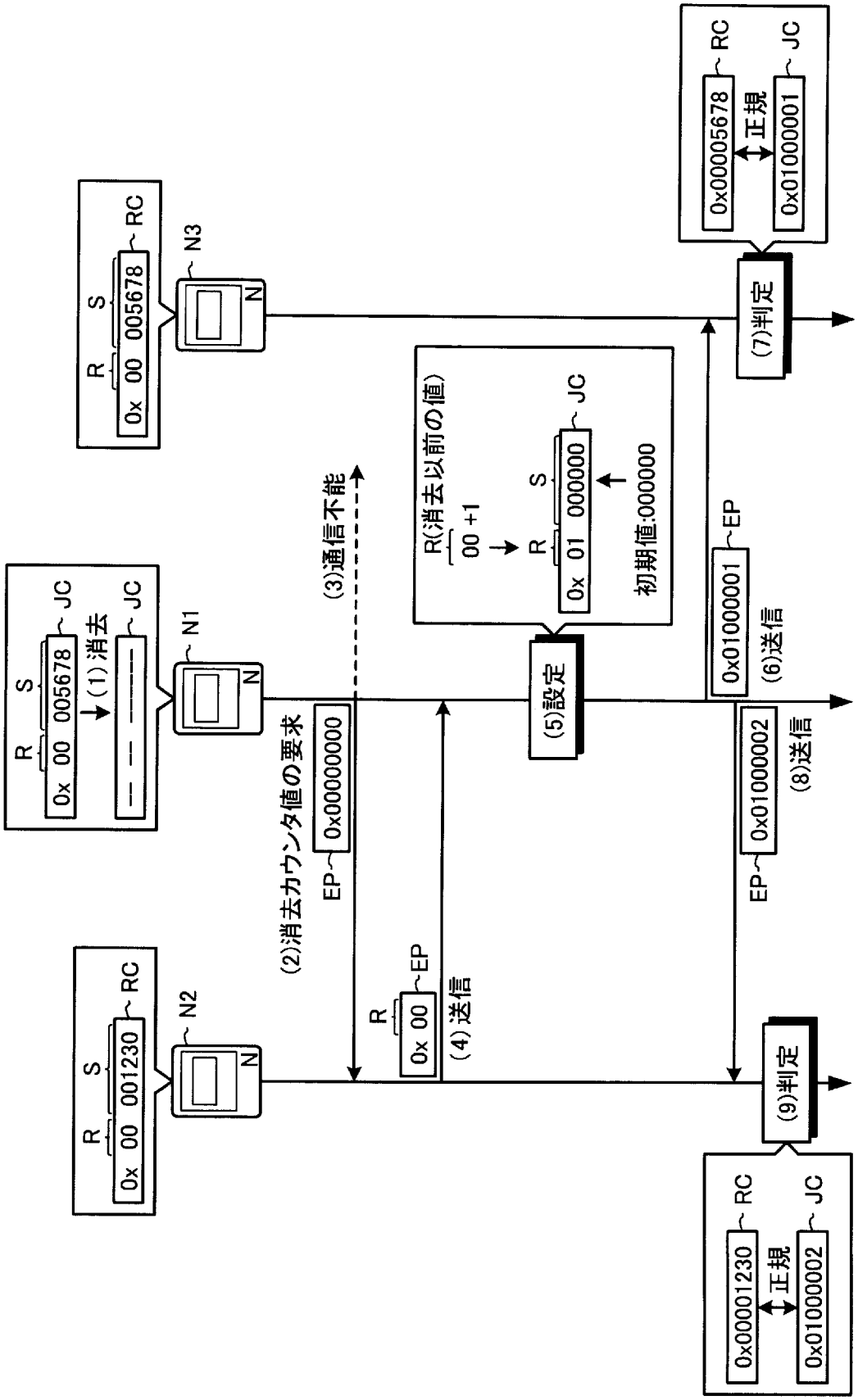
の受信手段と、

前記第２の受信手段によつて受信された第２の連結カウンタ値が前記第１の連結カウンタ値よりも大きいか否かを判断する判断手段と、

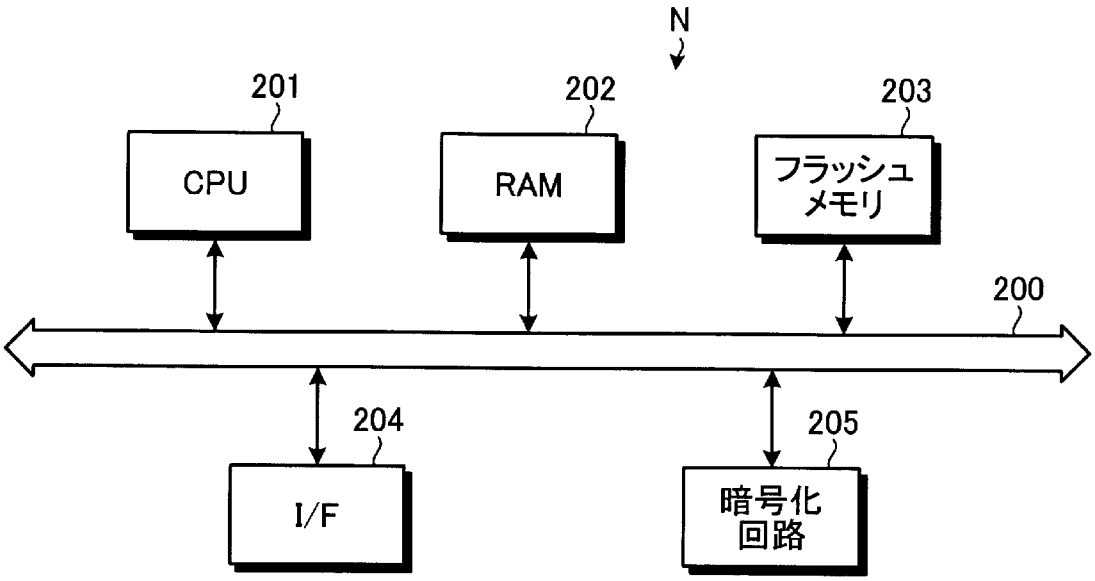
前記判断手段によって大きいと判断された場合、前記第１の連結カウンタ値を前記第２の連結カウンタ値に上書保存する第２の保存手段と、

を備えることを特徴とする通信システム。

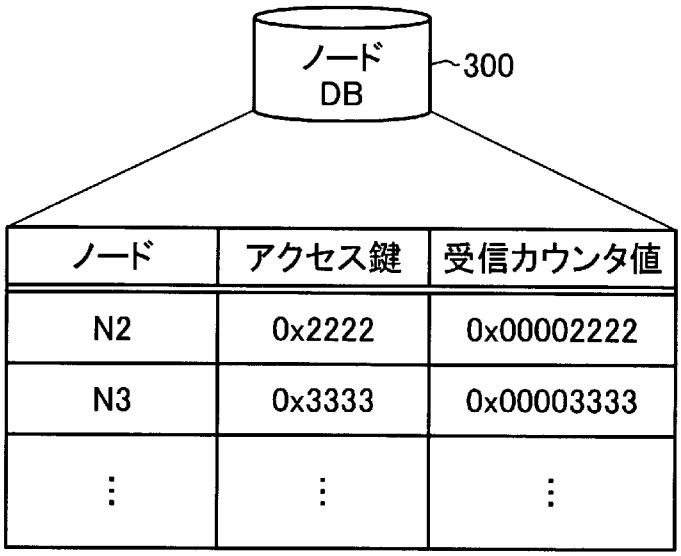
[図1]


N1
N2
N3
R S
0x 00 005678
JC
(1)消去
(2)消去カウンタ値の要求
EP
0x00000000
(3)通信不能
R
0x 00
(4)送信
R(消去以前の値)
00 +1
0x 01 000000
初期値:000000
(5)設定
0x01000001
(6)送信
0x01000002
(8)送信
(7)判定
(9)判定
RC
0x00005678
正規
0x01000001
0x00001230
0x01000002

[図2]

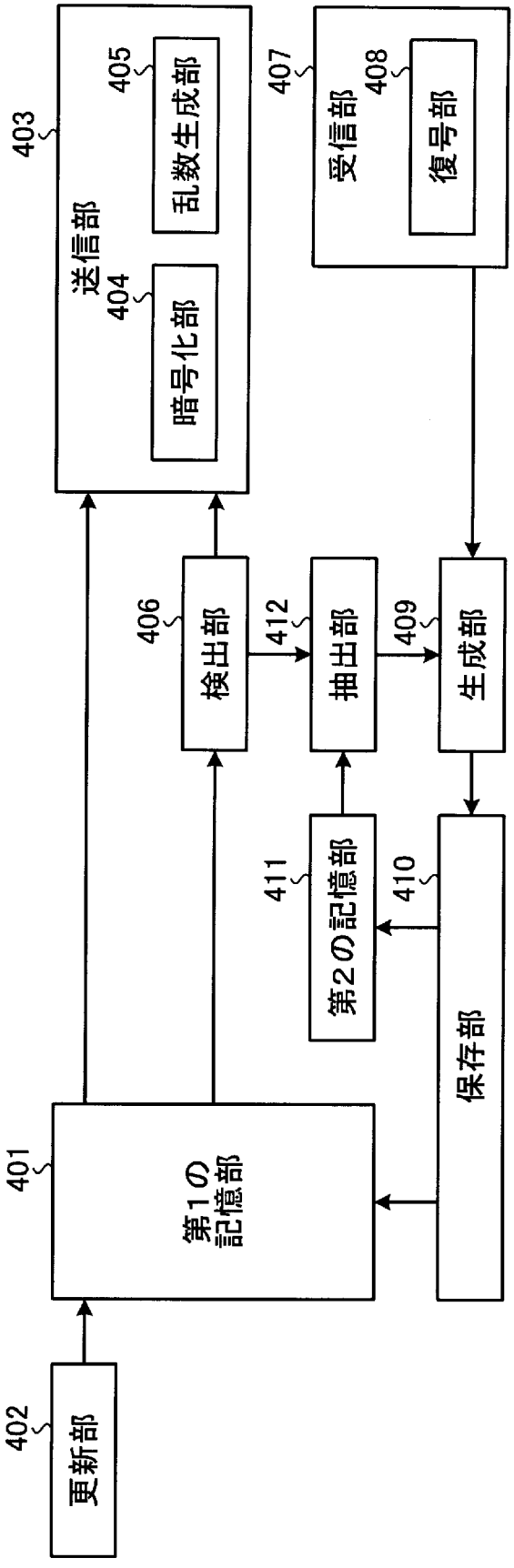


[図3]

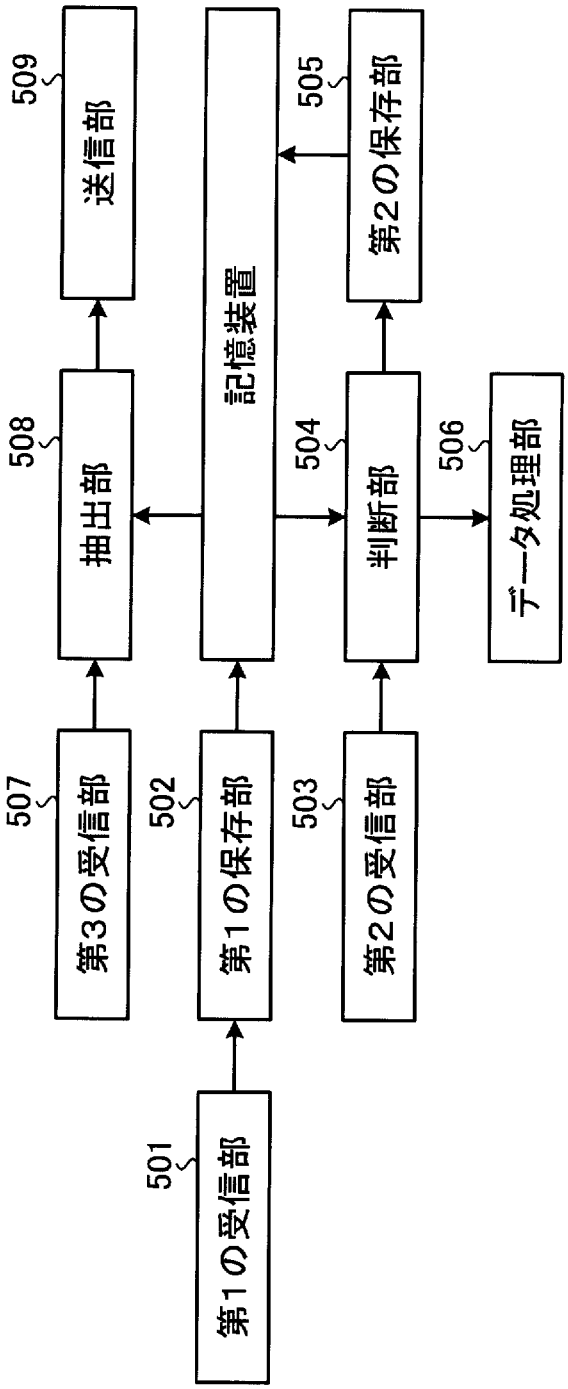


ノード	アクセス鍵	受信カウンタ値
N2	0x2222	0x00002222
N3	0x3333	0x00003333
⋮	⋮	⋮

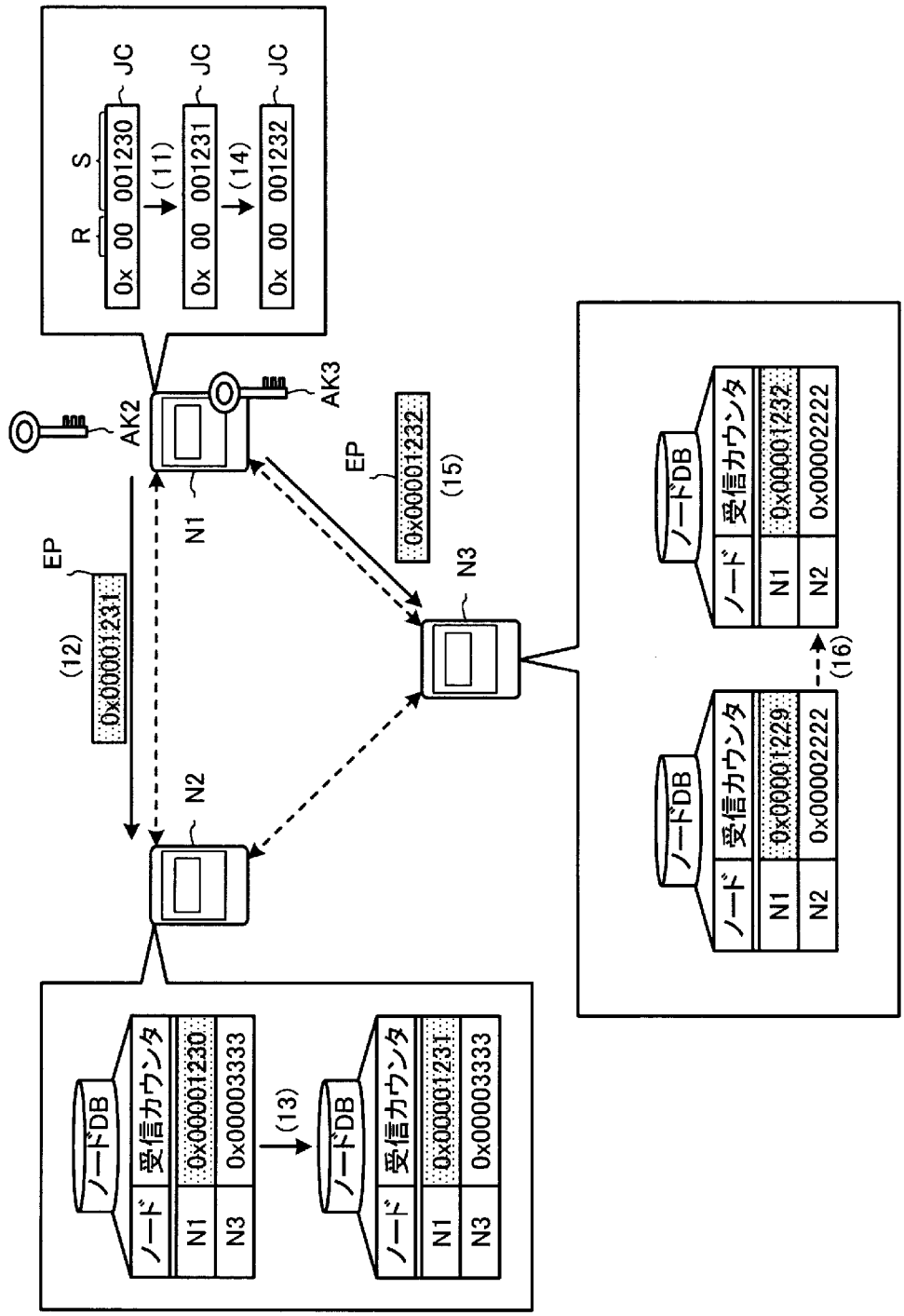
[図4]


403
送信部
405
乱数生成部
404
暗号化部
407
受信部
408
復号部
406
検出部
412
抽出部
409
生成部
411
第2の記憶部
410
保存部
401
第1の
記憶部
402
更新部

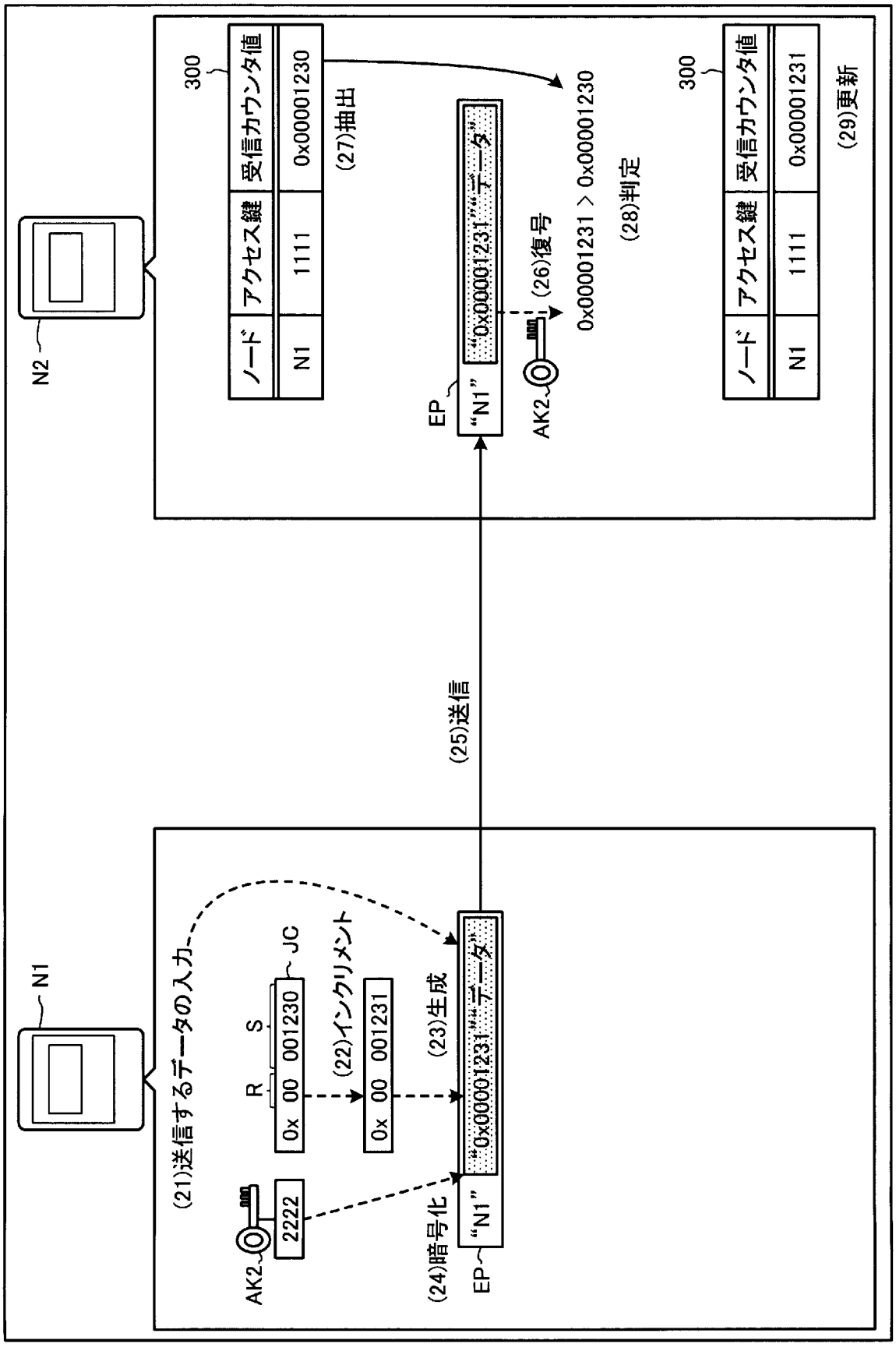
[図5]


509
送信部
505
第2の保存部
記憶装置
508
抽出部
504
判断部
506
データ処理部
507
第3の受信部
502
第1の保存部
503
第2の受信部
501
第1の受信部

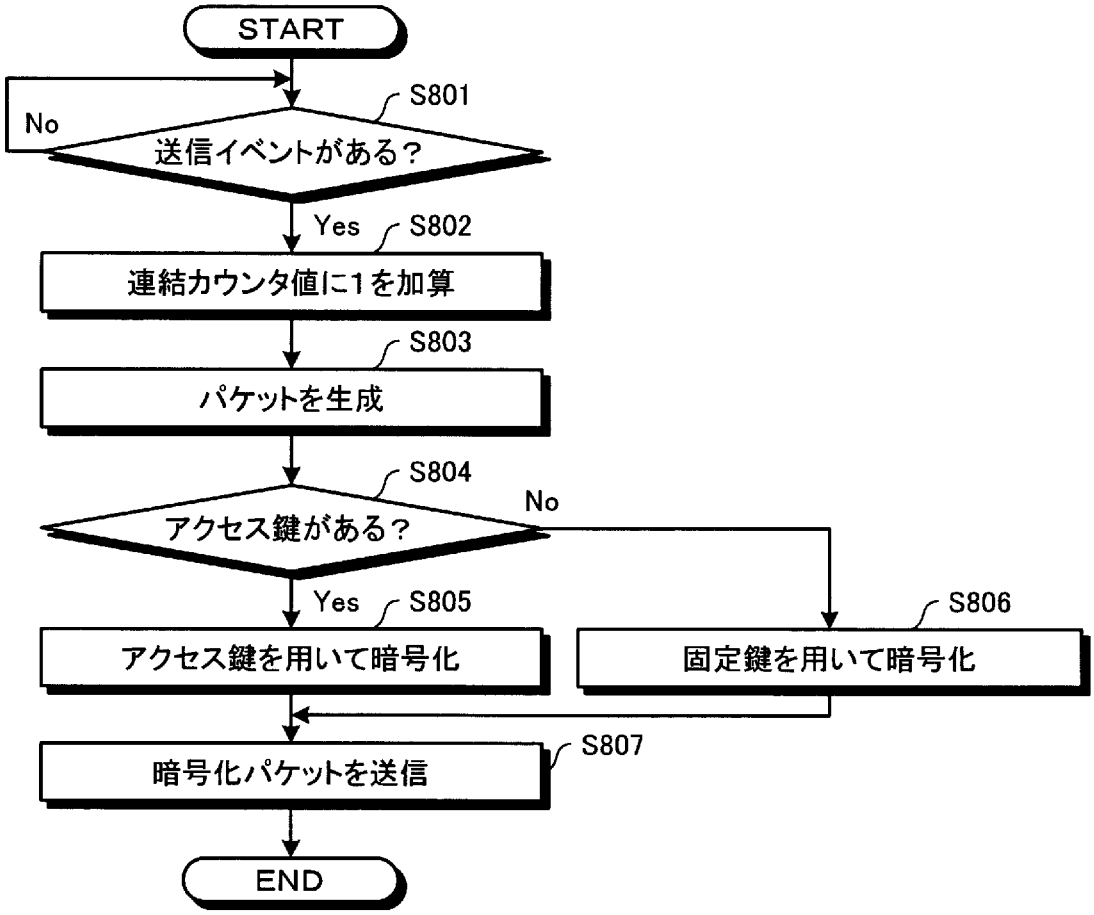
[図6]


JC
JC
JC
R
S
0x 00 001230
0x 00 001231
0x 00 001232
(11)
(14)
AK2
AK3
N1
N2
N3
EP
0x00001231
(12)
EP
0x00001232
(15)
ノードDB
ノード
受信カウンタ
N1
0x00001230
N3
0x00003333
(13)
ノードDB
ノード
受信カウンタ
N1
0x00001231
N3
0x00003333
ノードDB
ノード
受信カウンタ
N1
0x00001229
N2
0x00002222
(16)
ノードDB
ノード
受信カウンタ
N1
0x00001232
N2
0x00002222

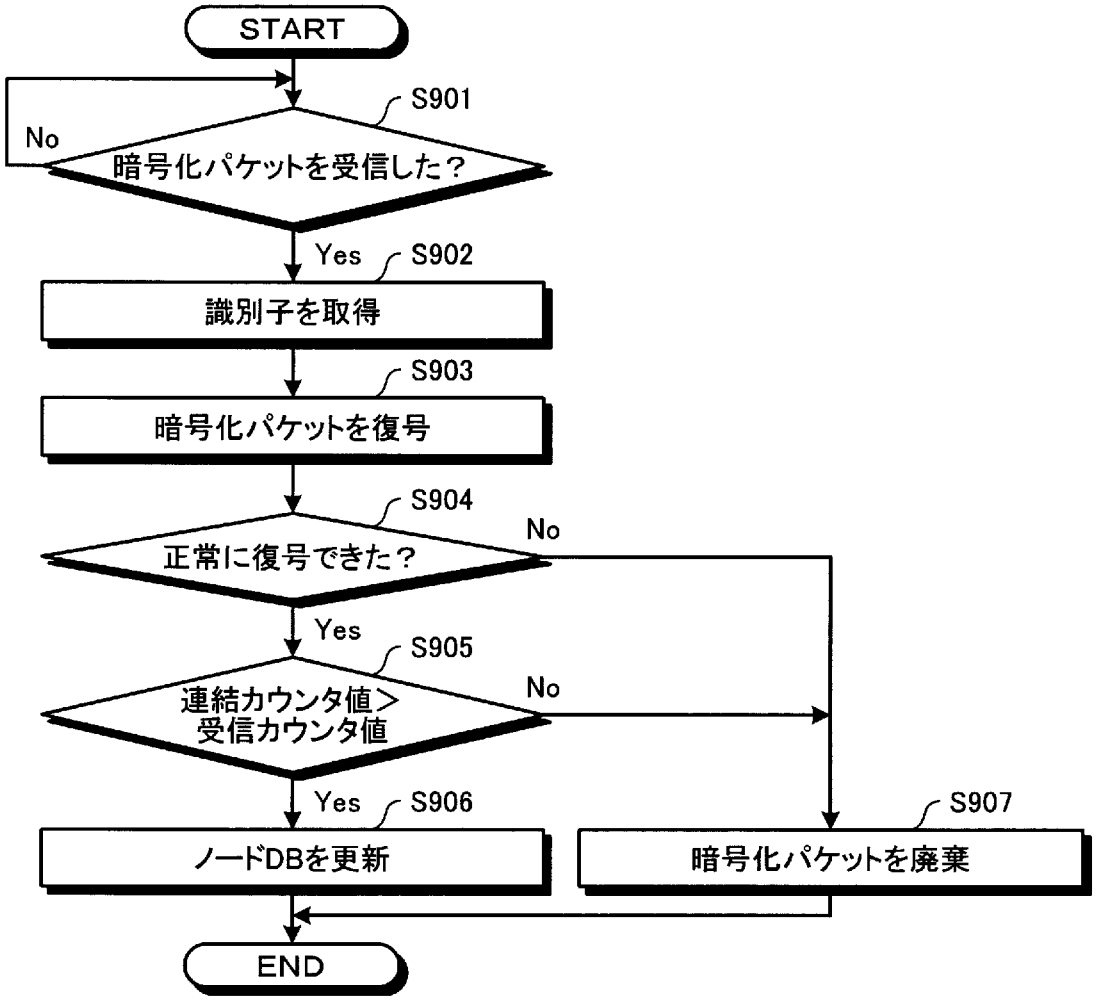
[図7]


N1
N2
(21)送信するデータの入力
R
S
JC
0x 00 001230
(22)インクリメント
0x 00 001231
(23)生成
"0x00001231""データ"
(24)暗号化
AK2
2222
EP
"N1"
(25)送信
300
ノード
アクセス鍵
受信カウンタ値
N1
1111
0x00001230
(27)抽出
(26)復号
0x00001231 > 0x00001230
(28)判定
0x00001231
(29)更新

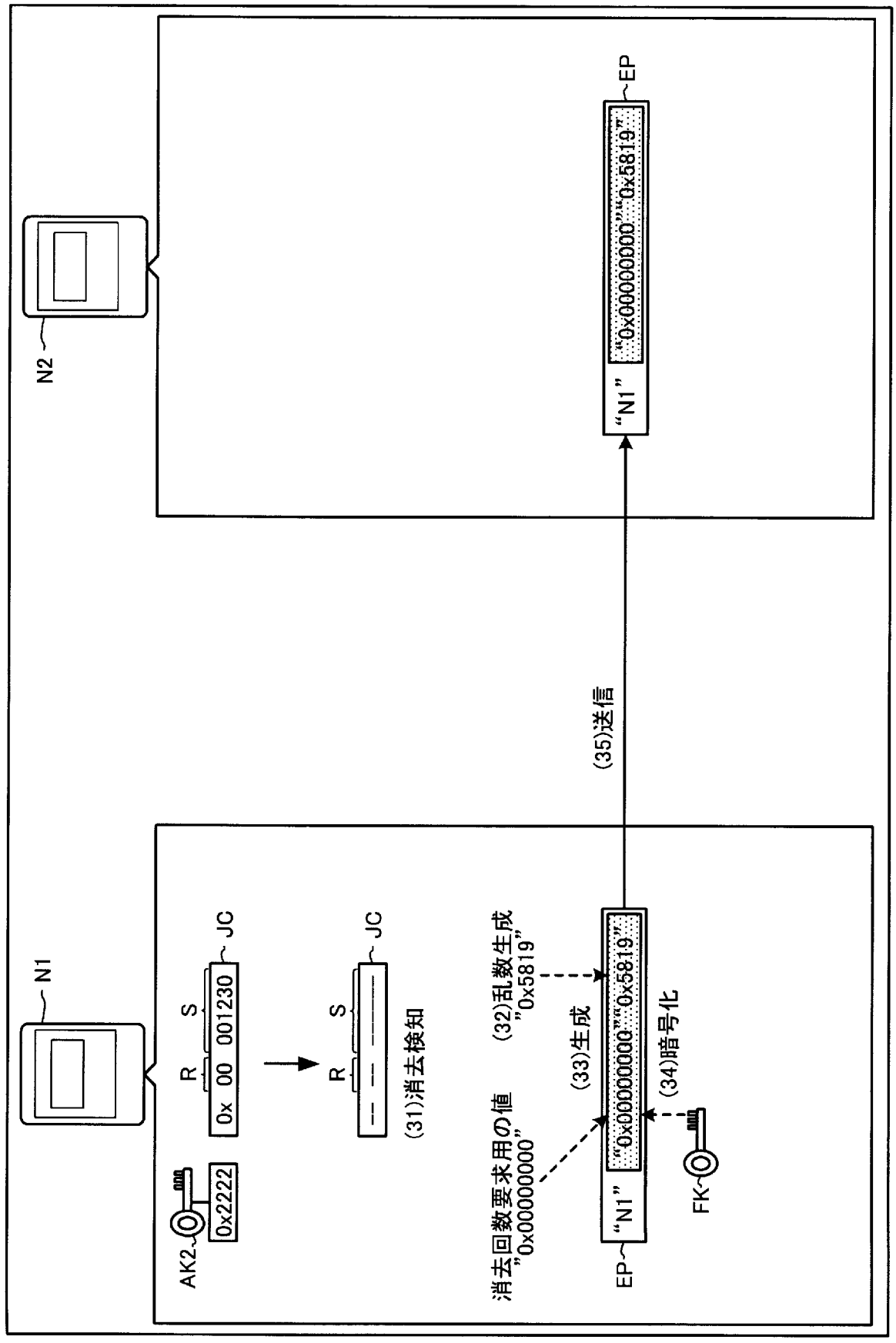
[図8]


START
S801
No
送信イベントがある？
Yes
S802
連結カウンタ値に1を加算
S803
パケットを生成
S804
アクセス鍵がある？
No
Yes
S805
アクセス鍵を用いて暗号化
S806
固定鍵を用いて暗号化
S807
暗号化パケットを送信
END

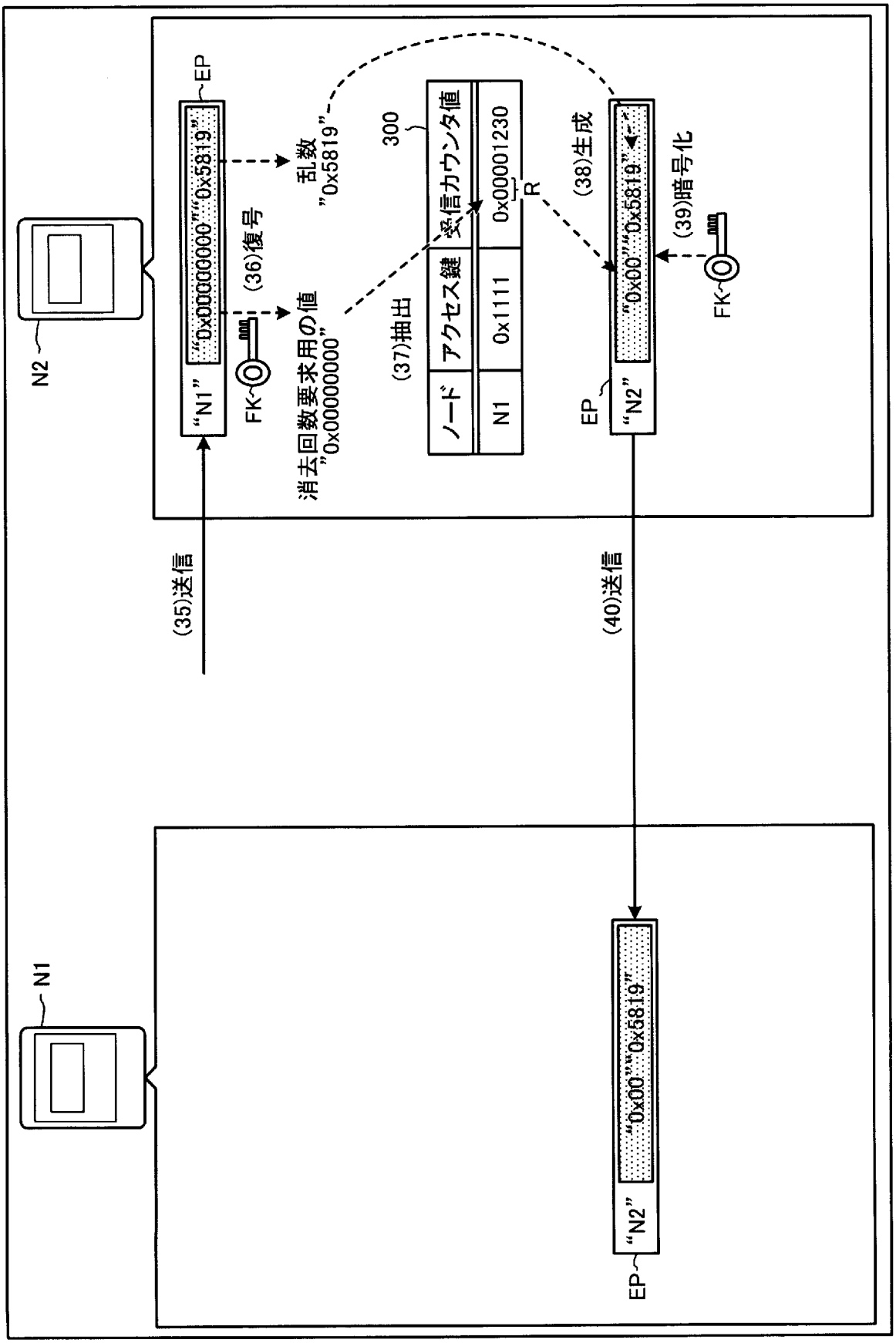
[図9]


START
S901
No
暗号化パケットを受信した？
Yes
S902
識別子を取得
S903
暗号化パケットを復号
S904
正常に復号できた？
No
Yes
S905
連結カウンタ値＞
受信カウンタ値
No
Yes
S906
ノードDBを更新
S907
暗号化パケットを廃棄
END

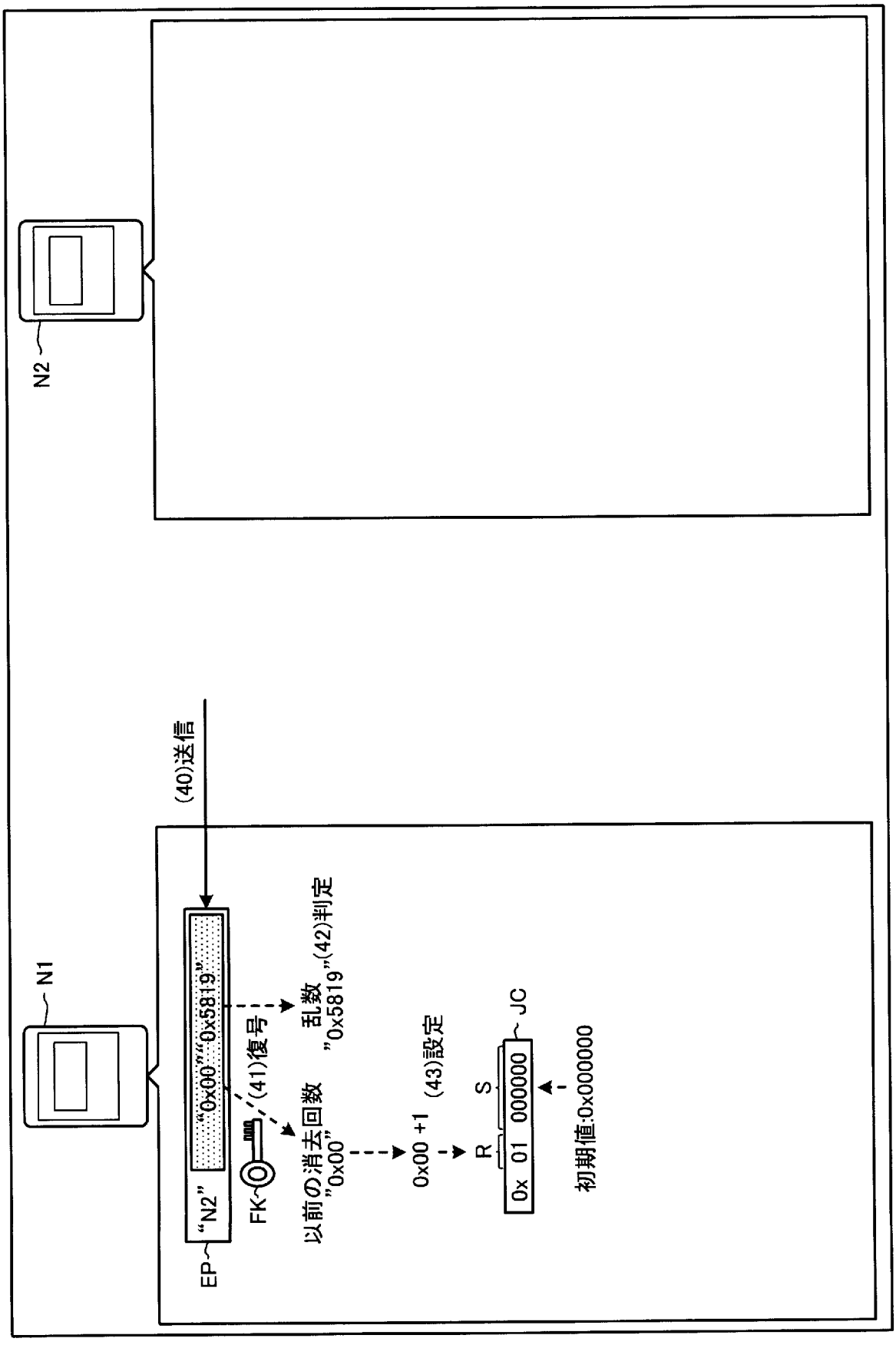
[図10]


N2
EP
"N1"
"0x00000000"
"0x5819"
(35)送信
N1
R
S
JC
0x
00
001230
AK2
0x2222
(31)消去検知
(32)乱数生成
"0x5819"
消去回数要求用の値
"0x00000000"
(33)生成
(34)暗号化
EP
"N1"
"0x00000000"
"0x5819"
FK

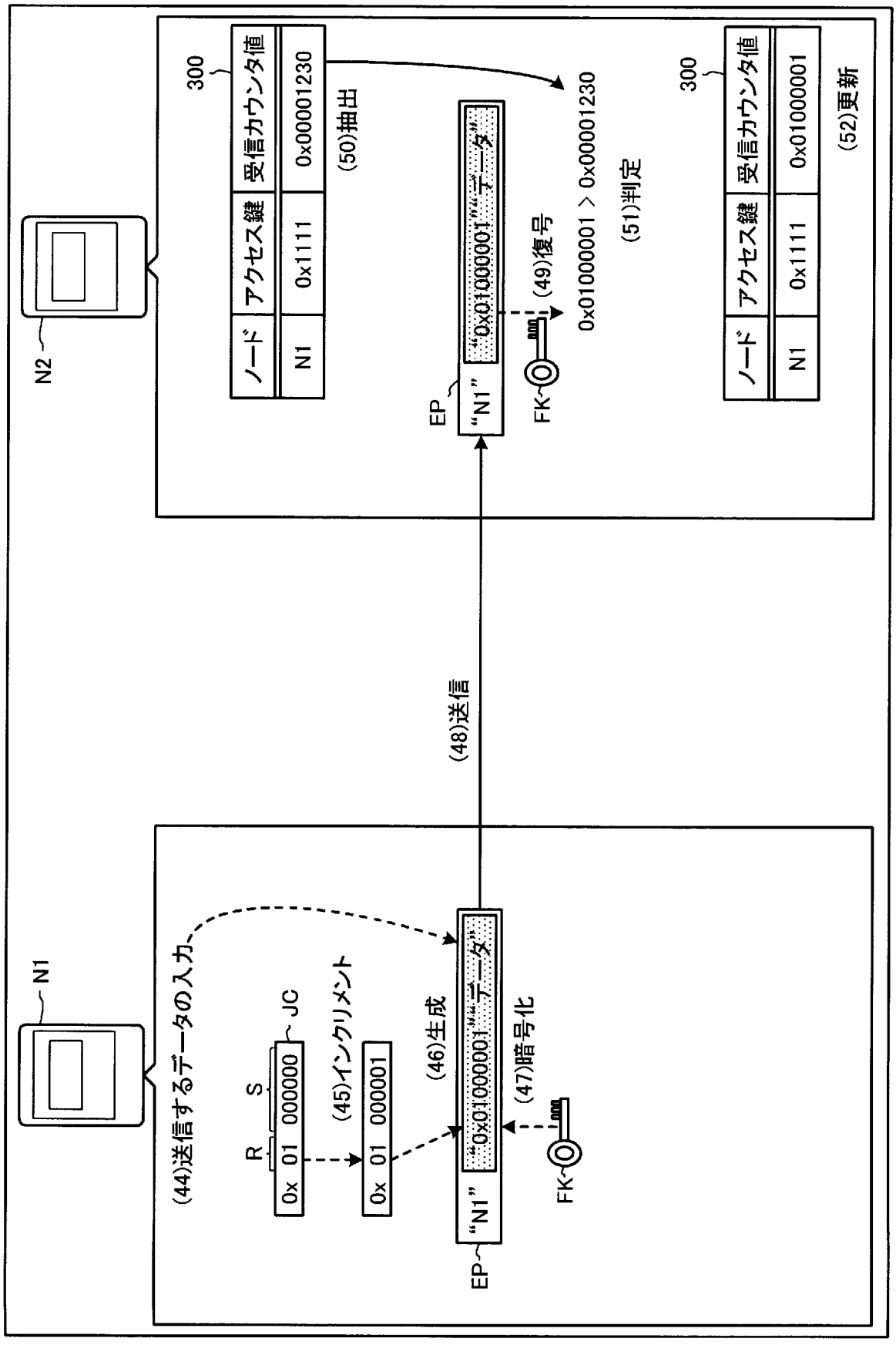
[図11]


N2
EP
"N1"
"0x00000000""0x5819"
FK
(36)復号
乱数
"0x5819"
消去回数要求用の値
"0x00000000"
300
(37)抽出
ノード
アクセス鍵
受信カウンタ値
N1
0x1111
0x00001230
R
(38)生成
EP
"N2"
"0x00""0x5819"
(39)暗号化
FK
(35)送信
(40)送信
N1
EP
"N2"
"0x00""0x5819"

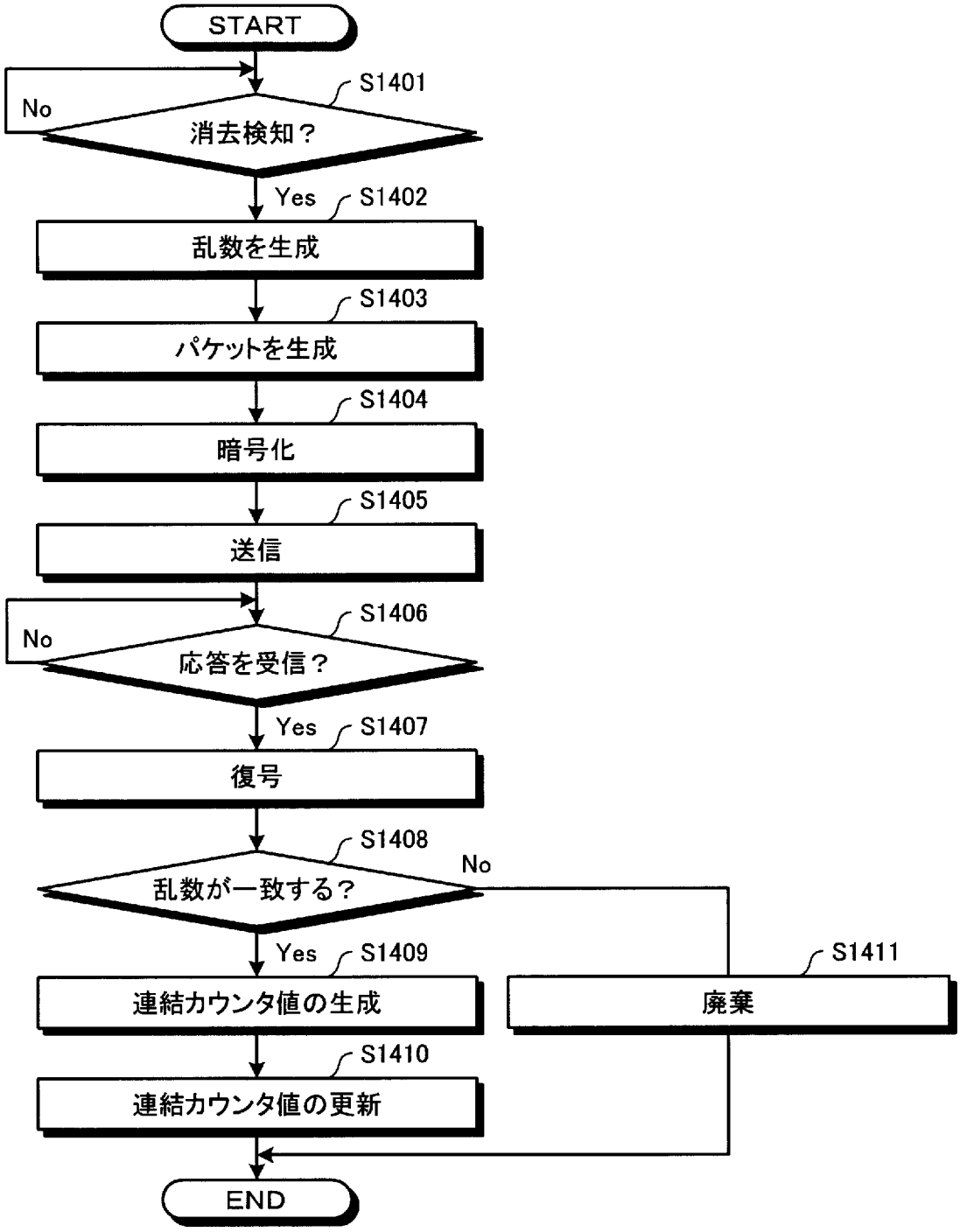
[図12]


N2
N1
(40)送信
EP
"N2"
"0x00""0x5819"
FK
(41)復号
以前の消去回数
"0x00"
乱数
"0x5819"(42)判定
0x00 +1
(43)設定
R
S
JC
0x 01 000000
初期値:0x000000

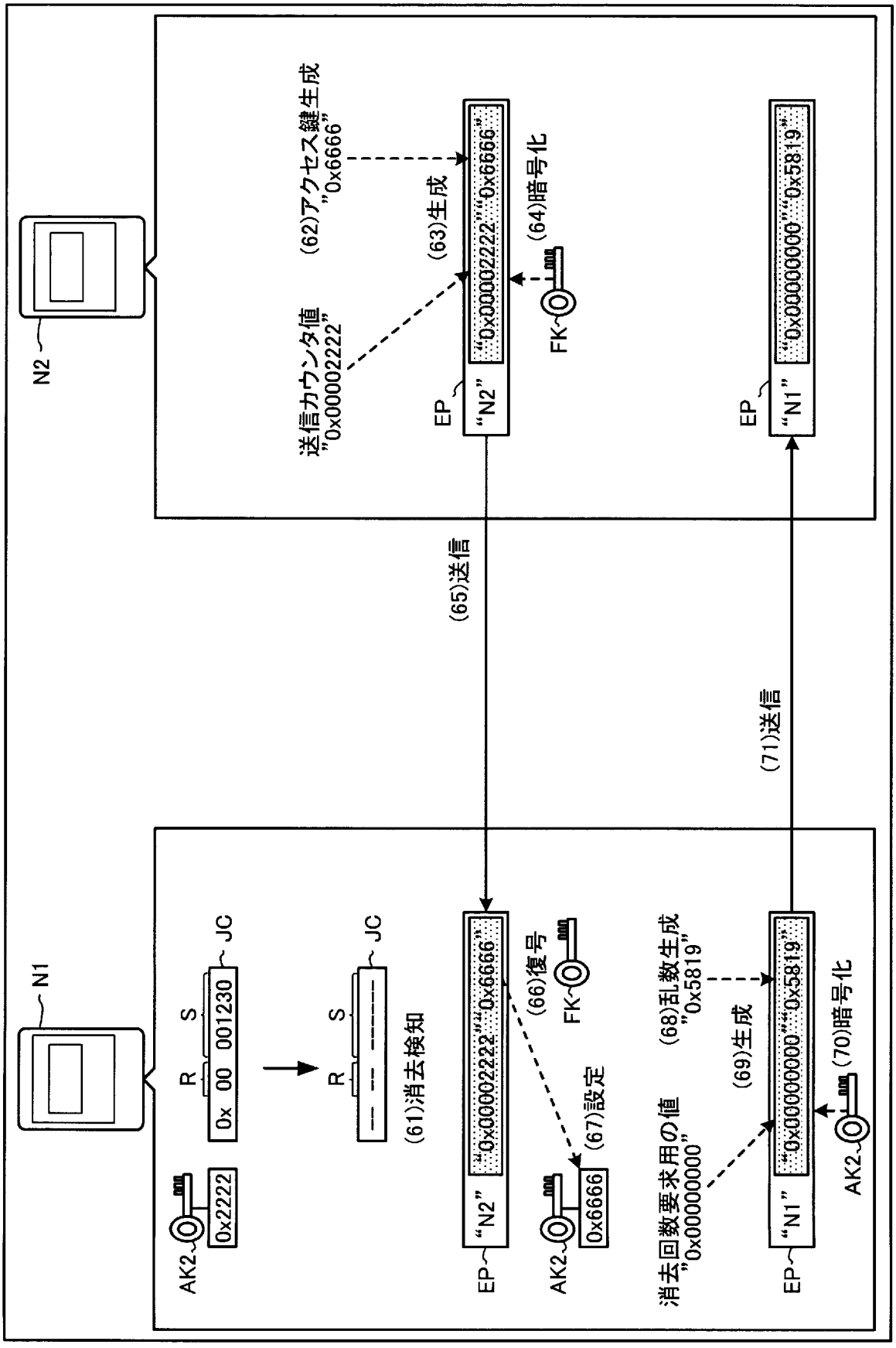
[図13]


N1
N2
(44)送信するデータの入力
R
S
JC
0x 01 000000
(45)インクリメント
0x 01 000001
(46)生成
"N1"
"0x01000001""データ"
EP
FK
(47)暗号化
(48)送信
300
ノード
アクセス鍵
受信カウンタ値
N1
0x1111
0x00001230
(50)抽出
(49)復号
0x01000001 > 0x00001230
(51)判定
0x01000001
(52)更新

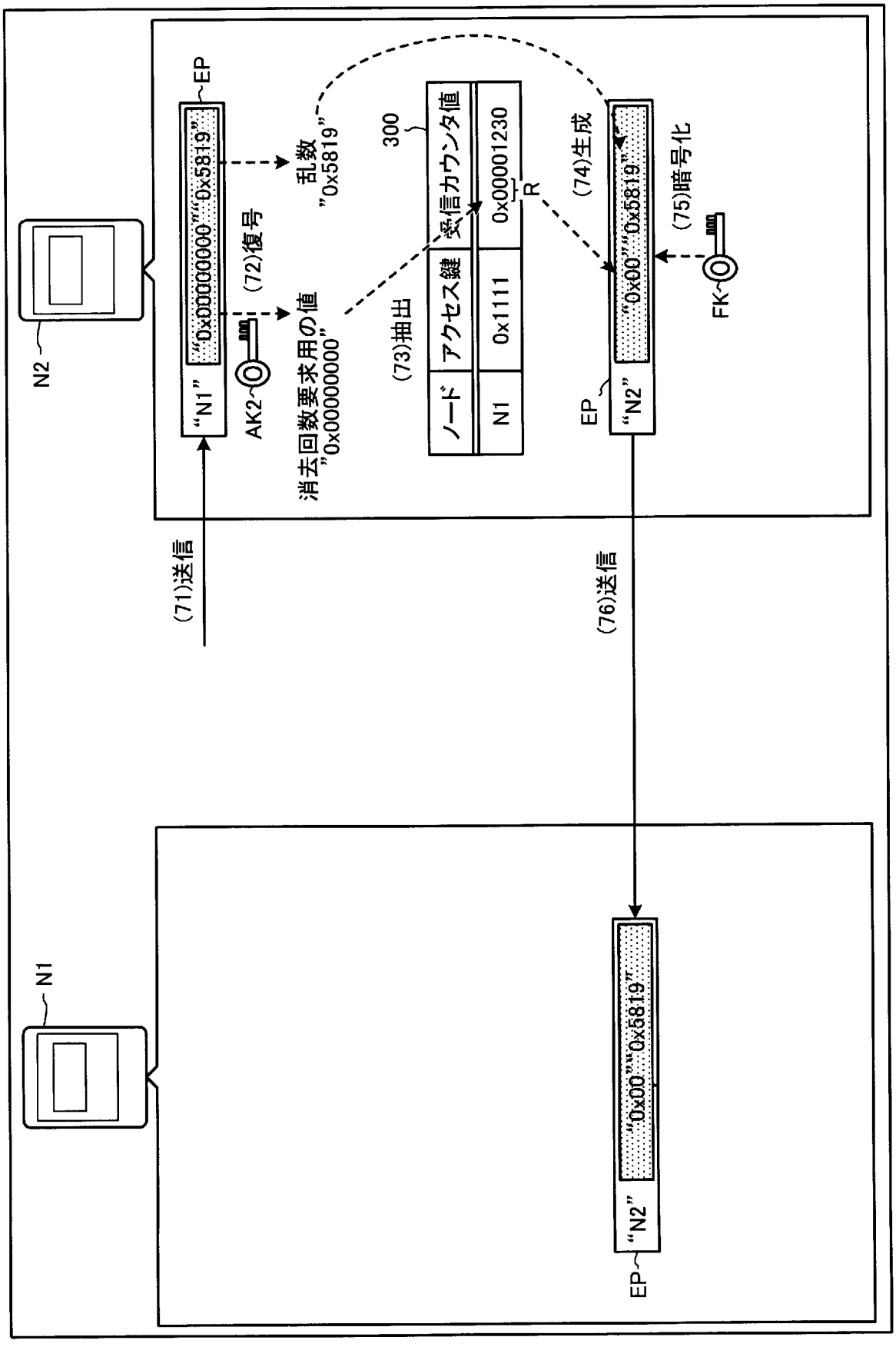
[図14]


START
S1401
No
消去検知？
Yes
S1402
乱数を生成
S1403
パケットを生成
S1404
暗号化
S1405
送信
S1406
No
応答を受信？
Yes
S1407
復号
S1408
乱数が一致する？
No
Yes
S1409
連結カウンタ値の生成
S1410
連結カウンタ値の更新
S1411
廃棄
END

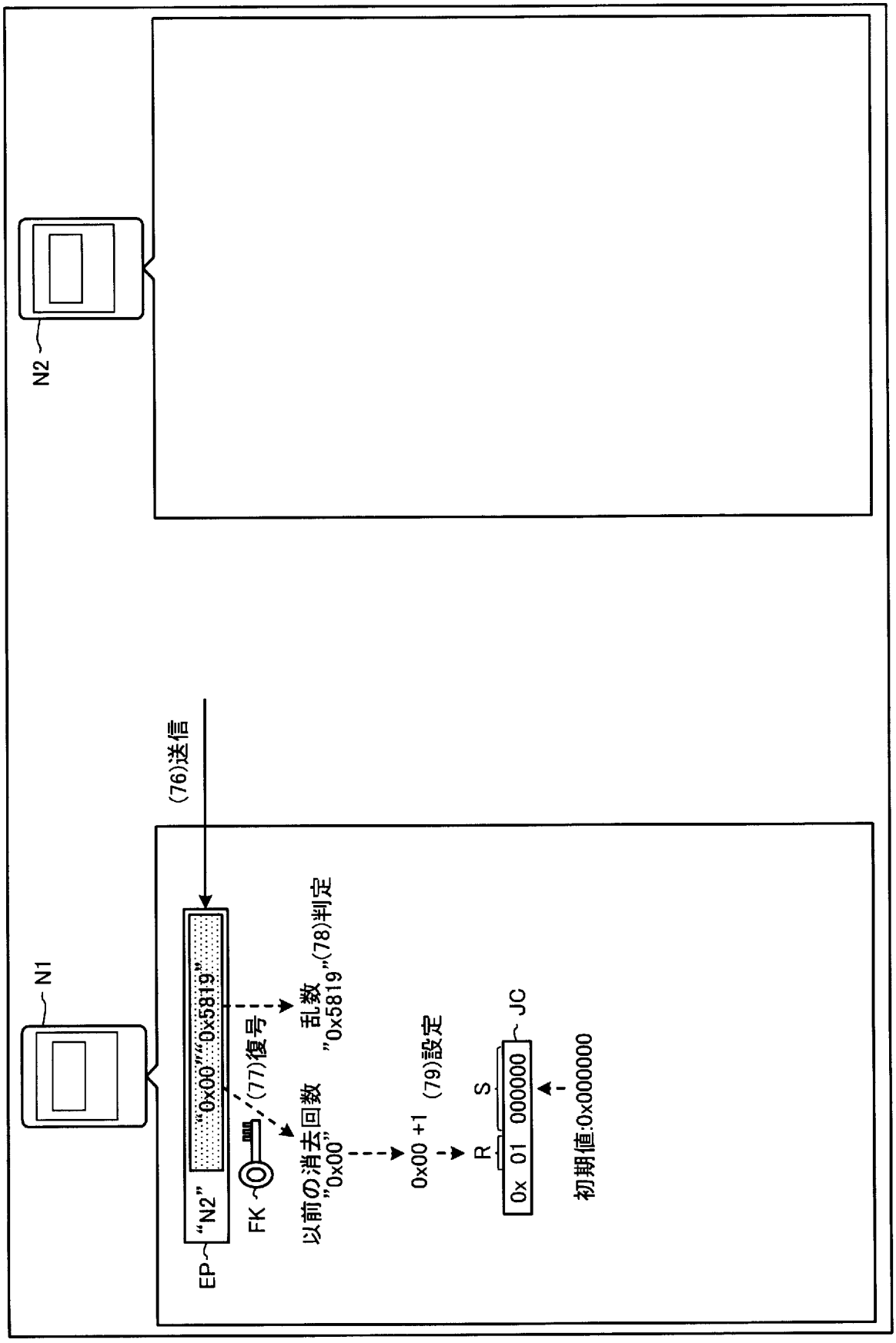
[図15]


N2
(62)アクセス鍵生成
"0x6666"
(63)生成
(64)暗号化
送信カウンタ値
"0x00002222"
FK
EP
"N2"
"0x00002222""0x6666"
EP
"N1"
"0x00000000""0x5819"
(65)送信
(71)送信
N1
R S JC
0x 00 001230
AK2
0x2222
(61)消去検知
R S JC
EP
"N2"
"0x00002222""0x6666"
(66)復号
FK
AK2
0x6666
(67)設定
消去回数要求用の値
"0x00000000"
(68)乱数生成
"0x5819"
(69)生成
EP
"N1"
"0x00000000""0x5819"
AK2
(70)暗号化

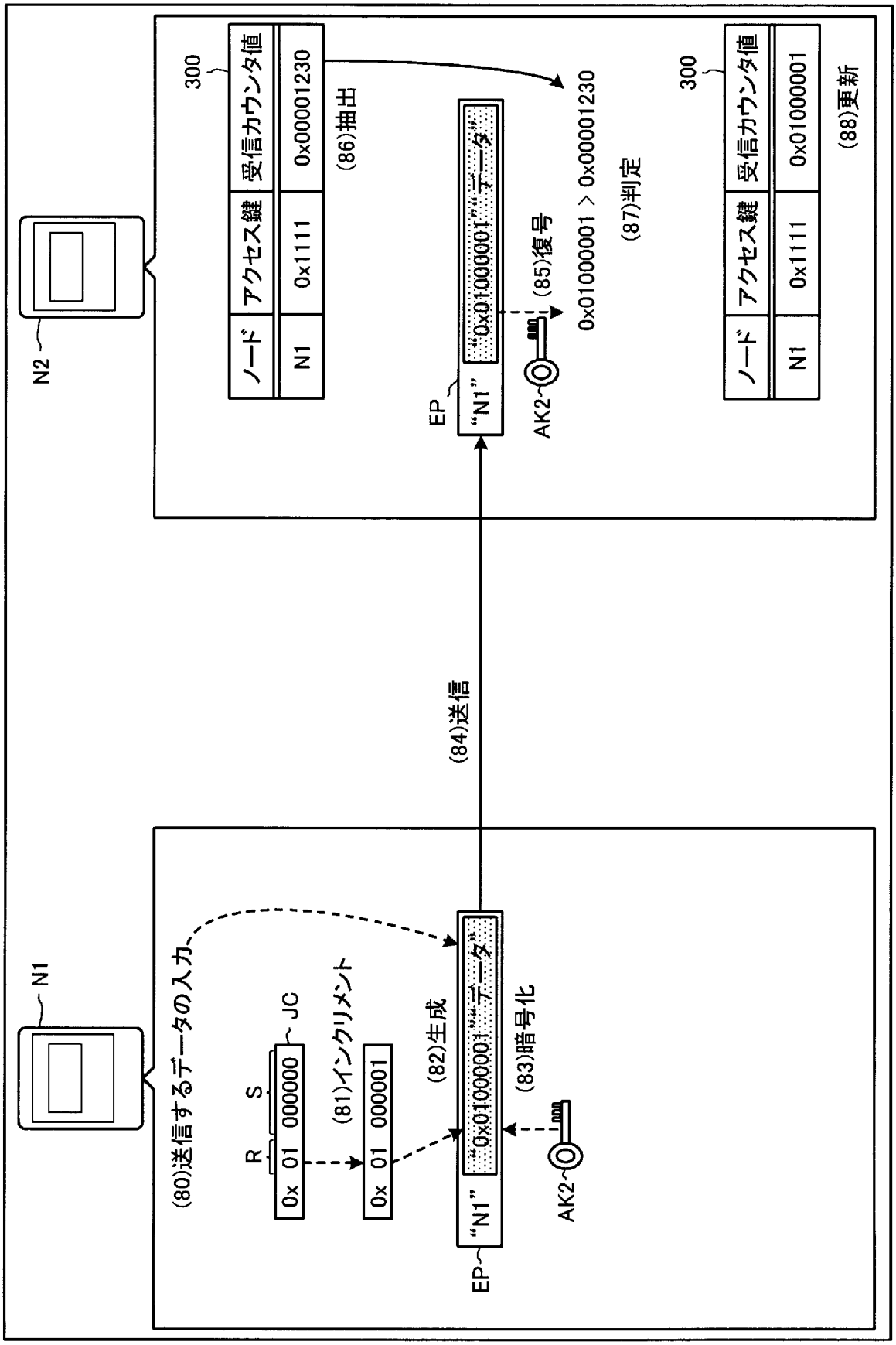
[図16]


N2
EP
"N1"
"0x00000000""0x5819"
AK2
(72)復号
乱数
"0x5819"
消去回数要求用の値
"0x00000000"
300
(73)抽出
ノード
アクセス鍵
受信カウンタ値
N1
0x1111
0x00001230
R
(74)生成
EP
"N2"
"0x00""0x5819"
(75)暗号化
FK
(71)送信
(76)送信
N1
"N2"
"0x00""0x5819"
EP

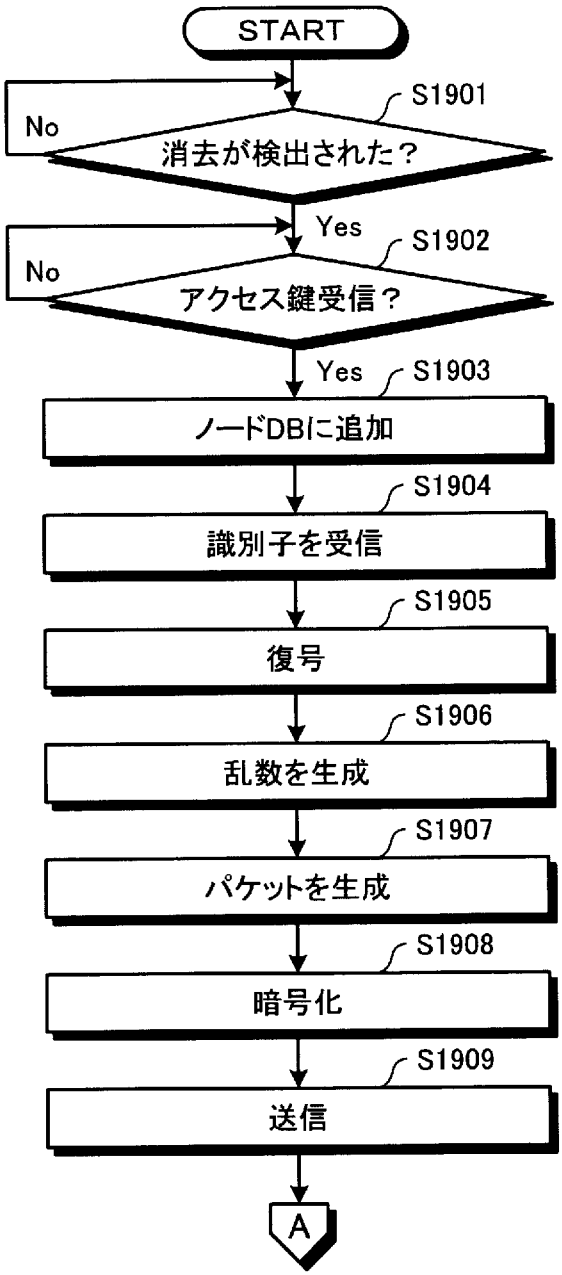
[図17]


N2
(76)送信
N1
"N2"
EP
"0x00""0x5819"
FK
(77)復号
以前の消去回数
"0x00"
乱数
"0x5819"(78)判定
0x00 +1
(79)設定
R
S
JC
0x 01 000000
初期値:0x000000

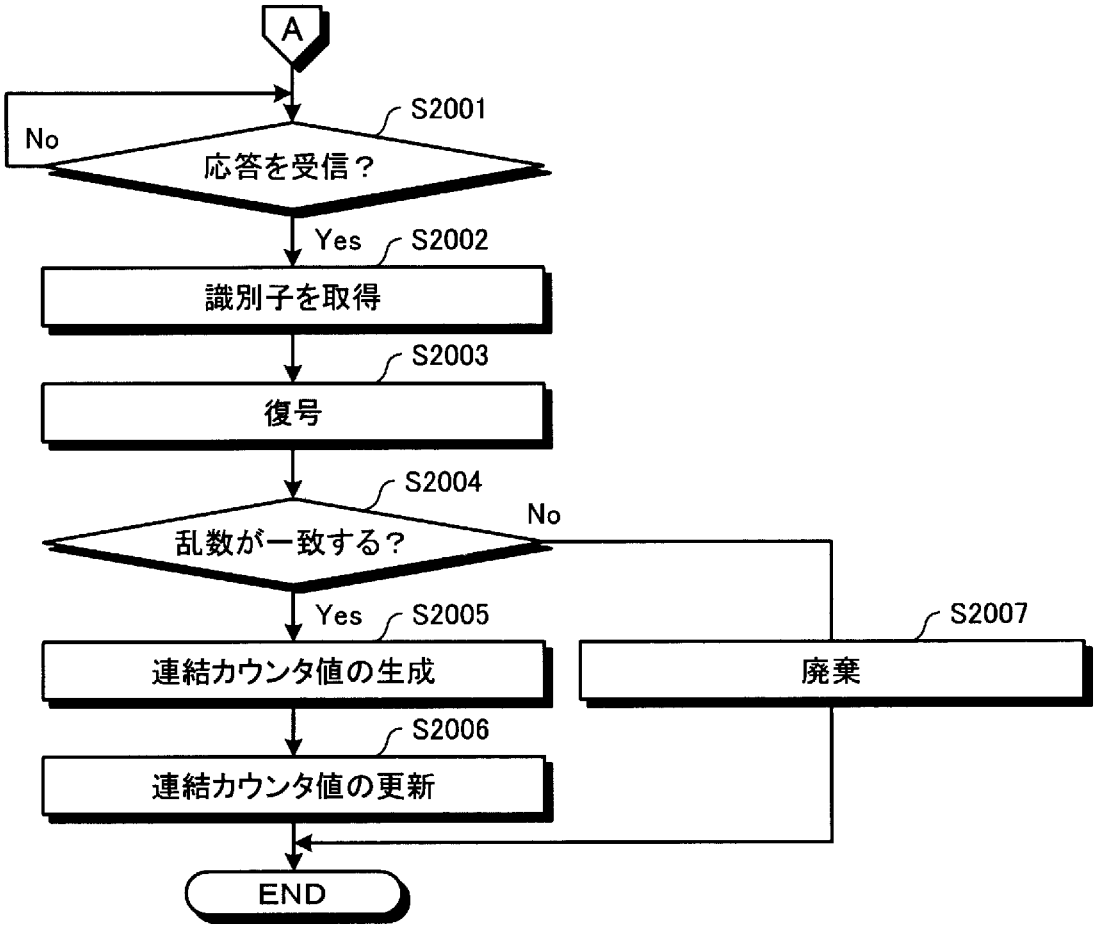
[図18]


N1
N2
(80)送信するデータの入力
R
S
JC
0x 01 000000
(81)インクリメント
0x 01 000001
(82)生成
"N1"
"0x01000001"データ
EP
(83)暗号化
AK2
(84)送信
300
ノード
アクセス鍵
受信カウンタ値
N1
0x1111
0x00001230
(86)抽出
EP
"N1"
"0x01000001"データ
AK2
(85)復号
0x01000001 > 0x00001230
(87)判定
300
ノード
アクセス鍵
受信カウンタ値
N1
0x1111
0x01000001
(88)更新

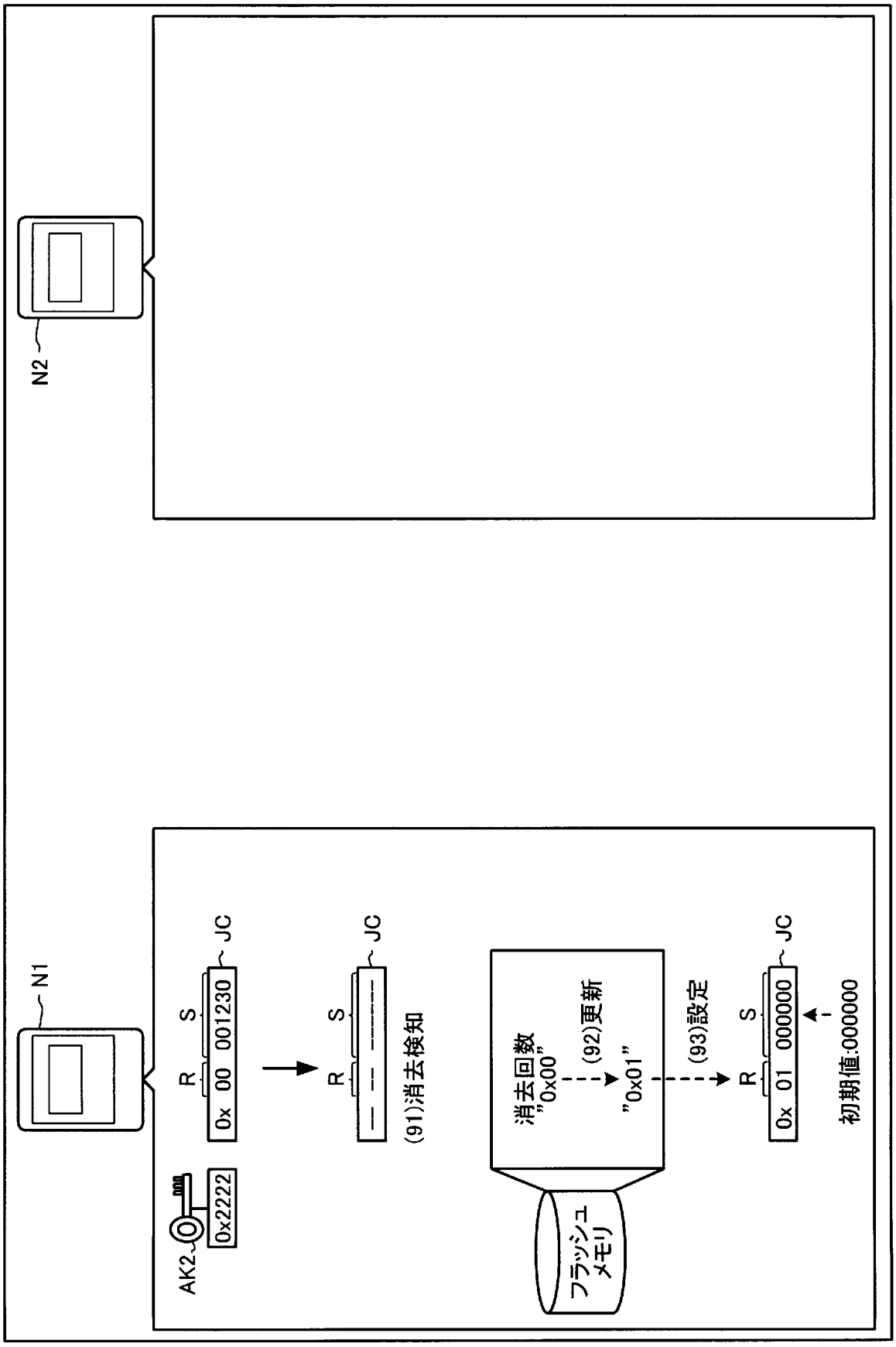
[図19]


START
S1901
No
消去が検出された？
Yes
S1902
No
アクセス鍵受信？
Yes
S1903
ノードDBに追加
S1904
識別子を受信
S1905
復号
S1906
乱数を生成
S1907
パケットを生成
S1908
暗号化
S1909
送信
A

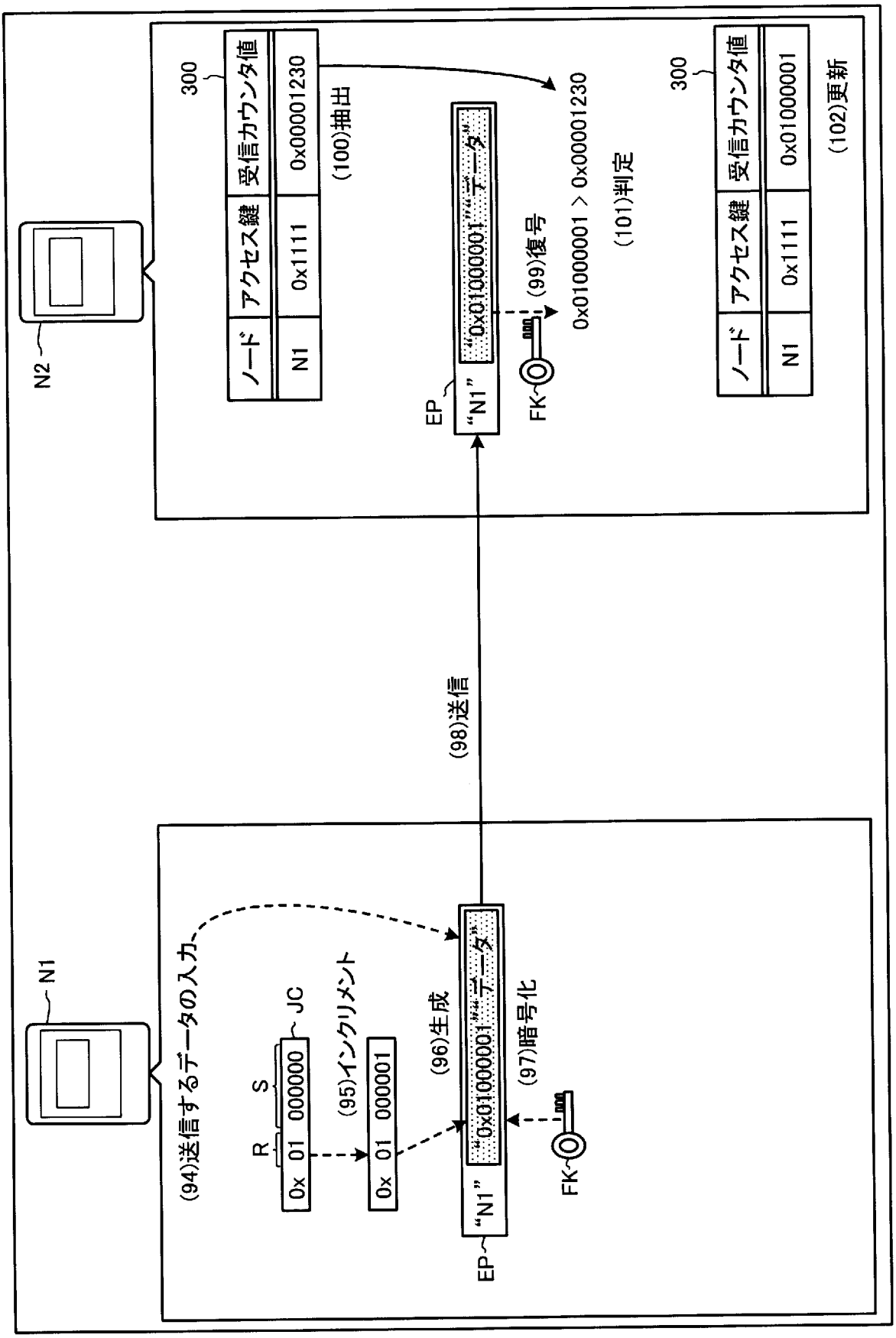
[図20]


A
S2001
No
応答を受信？
Yes
S2002
識別子を取得
S2003
復号
S2004
乱数が一致する？
No
Yes
S2005
連結カウンタ値の生成
S2007
廃棄
S2006
連結カウンタ値の更新
END

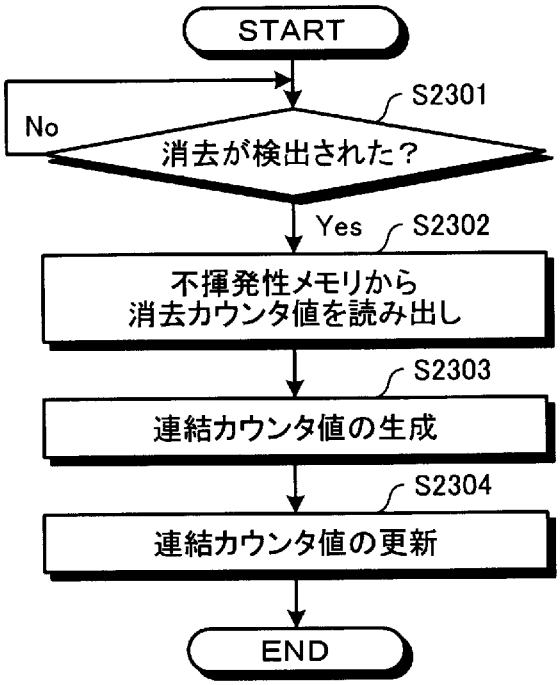
[図21]


N2
N1
JC
S
R
0x 00 001230
AK2
0x2222
(91):消去検知
消去回数
"0x00"
(92)更新
"0x01"
(93)設定
フラッシュ
メモリ
0x 01 000000
初期値:000000

[図22]


N1
N2
(94)送信するデータの入力
R
S
JC
0x 01 000000
0x 01 000001
(95)インクリメント
(96)生成
"0x01000001"データ"
"N1"
EP
(97)暗号化
FK
(98)送信
300
ノード
アクセス鍵
受信カウンタ値
N1
0x1111
0x00001230
(100)抽出
(99)復号
0x01000001 > 0x00001230
(101)判定
(102)更新
0x01000001

[図23]


START
S2301
No
消去が検出された？
Yes
S2302
不揮発性メモリから
消去カウンタ値を読み出し
S2303
連結カウンタ値の生成
S2304
連結カウンタ値の更新
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT / JP2 011 / 078216

A. CLASSIFICATION OF SUBJECT MATTER
H04 W12/1 2{2009.01)i, HO4W84 / 18{2009.01)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)
H04B7/24-7/26, H04W4/00-99/00, H04L12/00—12/26; 12/28; 12/44-12/46;
12/50-12/66; 29/00-29/10; 29/12, H04L13/02; 13/08-13/16; 13/18

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 1996-2012
Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

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.
A	JP 5-91108 A (Hitachi, Ltd.), 09 April 1993 (09.04.1993), entire text (Family: none)	1-17
A	JP 2003-244156 A (Daido Signal Co., Ltd.), 29 August 2003 (29.08.2003), entire text (Family: none)	1-17
A	JP 2011-515988 A (Silver Spring Networks, Inc.), 19 May 2011 (19.05.2011), abstract & US 2009/0245270 A1 & US 2009/0262642 A1 & EP 2272218 A & WO 2009/120345 A2 & WO 2010/110846 A1	1-17

[X] 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	Date of mailing of the international search report
27 February, 2012 (27.02.12)	13 March, 2012 (13.03.12)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT / JP2 011/ 078216

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/028936 A1 (SIEMENS AG.), 18 March 2010 (18.03.2010), Whole document & US 2011/0158410 A1 & EP 2324595 A & DE 102008046563 A & DE 102008046563 A1	1-17

国際調査報告

国際出願番号 PCT／JP2011/078216

A. 発明の属する分野の分類 (国際特許分類 (IPC))

IntCl. H04W12/12 (2009.01)i, H04W84/18 (2009.01)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))

IntCl. H04B 7/24-7/26, H04W 4/00-99/00 ,
H04L 12/00-12/26 ; 12/28 ;12/44-12/46 ; 12/50-12/66 ; 29/00-29/10 ; 29/12
H04L 13/02 ;13/08-13/16 ; 13/18

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

ヨ本国実用新案公報	1922—1996年
日本国公開実用新案公報	1971—2012年
日本国実用新案登録公報	1996—2012年
日本国登録実用新案公報	1994—2012年

国際調査で使用した電子デ､ータベ-ス (デ-タベ-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
A	JP 5-91108 A (株式会社日立製作所) 1993.04.09, 全文 (ファミリーなし)	1-17
A	JP 2003-244156 A (大同信号株式会社) 2003.08.29, 全文 (ファミリーなし)	1-17

☑ 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つ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
27.02.2012	13.03.2012

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) 5J 3984
桑原 聡一
電話番号 03—3581—1101 内線 3534

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
A	JP 2011-515988 A（シルバー スプリング ネットワークス インコーポレイテッド）2011. 05. 19，要約 & US 2009/0245270 A1 & US 2009/0262642 A1 & EP 2272218 A & WO 2009/120345 A2 & WO 2010/110846 A1	1-17
A	WO 2010/028936 A1 (SIEMENS AKTIENGESELLSCHAFT) 2010. 03. 18, Whole document & US 2011/0158410 A1 & EP 2324595 A & DE 102008046563 A & DE 102008046563 A1	1-17