(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
2023年7月6日(06.07.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/127460 A1

(51) 国際特許分類:
H04L 12/28 (2006.01) *H04L 43/106* (2022.01)
H04L 43/08 (2022.01)

(21) 国際出願番号： PCT/JP2022/045396

(22) 国際出願日： 2022年12月9日(09.12.2022)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2021-214171 2021年12月28日(28.12.2021) JP

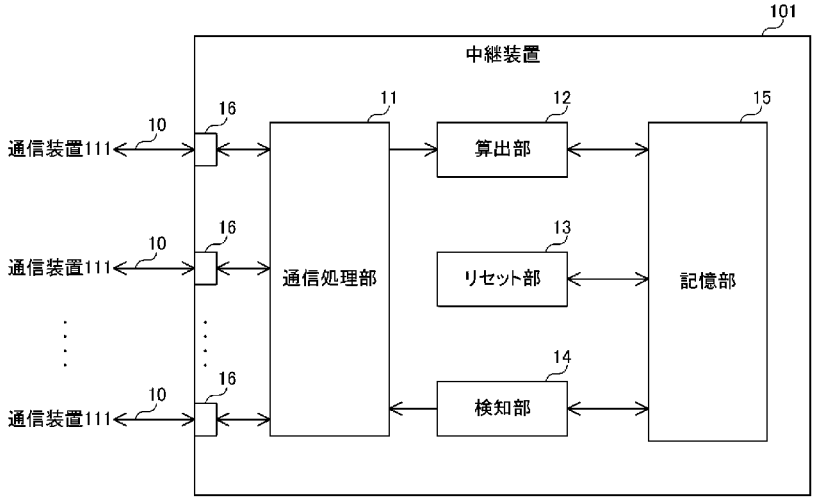
(71) 出願人: 住友電気工業株式会社 (**SUMITOMO ELECTRIC INDUSTRIES, LTD.**) [JP/JP]; 〒5410041 大阪府大阪市中央区北浜四丁目５番３３号 Osaka (JP). 住友電装株式会社 (**SUMITOMO WIRING SYSTEMS, LTD.**) [JP/JP]; 〒5108503 三重県四日市市西末広町１番１４号 Mie (JP). 株式会社オートネットワーク技術研究所 (**AUTONETWORKS TECHNOLOGIES, LTD.**) [JP/JP]; 〒5108503 三重県四日市市西末広町１番１４号 Mie (JP).

(72) 発明者: 増川京佑 (**MASUKAWA Kyosuke**); 〒5410041 大阪府大阪市中央区北浜四丁目５番３３号住友電気工業株式会社内 Osaka (JP). 上田浩史 (**UEDA Hiroshi**); 〒5108503 三重県四日市市西末広町１番１４号株式会社オートネットワーク技術研究所内 Mie (JP).

(74) 代理人: 弁理士法人ワンディーＩＰパートナーズ (**ONEDEE IP PARTNERS**); 〒5320003 大

(54) **Title:** DETECTION DEVICE AND DETECTION METHOD

(54) 発明の名称： 検知装置および検知方法



10 Communication device
11 Communication processing unit
12 Calculation unit
13 Reset unit
14 Detection unit
15 Storage unit
101 Relay device

(57) **Abstract:** This detection device detects an abnormality in a network through which a plurality of messages, including periodic messages, are transmitted and received. The detection device comprises: a calculation unit that calculates a detection index which increases/decreases according to the relationship between measurement results for the plurality of messages and reference information related to the measurement results; a detection unit that, on the basis of the detection index calculated by the calculation unit, performs detection processing for detecting an abnormality in the network; and a

WO 2023/127460 A1

[続葉有]

阪府大阪市淀川区宮原五丁目１番２８号新大阪八千代ビル別館 Osaka (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

reset unit that monitors the detection index, and resets the detection index used in the detection processing if an extreme value of the detection index is detected.

(57) 要約：検知装置は、周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置であって、前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出する算出部と、前記算出部により算出された前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行う検知部と、前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするリセット部とを備える。

明　細　書

発明の名称 ： 検知装置および検知方法

技術分野

[0001] 本開示は、検知装置および検知方法に関する。

この出願は、２０２１年１２月２８日に出願された日本出願特願２０２１－２１４１７１号を基礎とする優先権を主張し、その開示のすべてをここに取り込む。

背景技術

[0002] 特許文献１（国際公開第２０２１／１１１６８５号）には、以下のような検知装置が開示されている。すなわち、検知装置は、車載ネットワークにおける不正メッセージを検知する検知装置であって、前記車載ネットワークにおいて送信される周期メッセージの受信間隔の分布である対象分布を取得する取得部と、前記取得部によって取得された前記対象分布の一部を所定の基準に従って抽出する抽出部と、前記抽出部によって抽出された前記対象分布の一部に基づいて、前記不正メッセージを検知する検知処理を行う検知部とを備える。

先行技術文献

特許文献

[0003] 特許文献1：国際公開第２０２１／１１１６８５号

発明の概要

[0004] 本開示の検知装置は、周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置であって、前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出する算出部と、前記算出部により算出された前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行う検知部と、前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするリセット部とを備え

る。

[0005] 本開示の検知方法は、周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置、における検知方法であって、前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出するステップと、算出した前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行うステップと、前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするステップとを含む。

[0006] 本開示の一態様は、このような特徴的な処理部を備える検知装置として実現され得るだけでなく、かかる特徴的な処理のステップをコンピュータに実行させるためのプログラムとして実現され得たり、検知装置の一部または全部を実現する半導体集積回路として実現され得たり、検知装置を含むシステムとして実現され得る。

図面の簡単な説明

[0007] [図1]図１は、本開示の実施の形態に係る通信システムの構成を示す図である。

[図2]図２は、本開示の実施の形態に係る中継装置の構成を示す図である。

[図3]図３は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の一例を示す図である。

[図4]図４は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。

[図5]図５は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の一例を示す図である。

[図6]図６は、本開示の実施の形態の比較例に係る中継装置において検知処理に用いられる統計値の一例を示す図である。

[図7]図７は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。

[図8]図８は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の他の例を示す図である。

[図9]図９は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。

[図10]図１０は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の他の例を示す図である。

[図11]図１１は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。

[図12]図１２は、本開示の実施の形態に係る中継装置が検知処理を行う際の動作手順の一例を定めたフローチャートである。

[図13]図１３は、本開示の実施の形態に係るネットワークの接続トポロジの一例を示す図である。

[図14]図１４は、本開示の実施の形態に係る中継装置における算出部により算出される異常度の一例を示す図である。

発明を実施するための形態

[0008] 従来、ネットワークにおけるセキュリティを向上させるための技術が提案されている。

[0009] ［本開示が解決しようとする課題］

特許文献１に記載の技術を超えて、ネットワークにおける異常をより正しく検知することが可能な技術が望まれる。

[0010] 本開示は、上述の課題を解決するためになされたもので、その目的は、ネットワークにおける異常をより正しく検知することが可能な検知装置および検知方法を提供することである。

[0011] ［本開示の効果］

本開示によれば、ネットワークにおける異常をより正しく検知することができる。

[0012] ［本開示の実施形態の説明］

最初に、本開示の実施形態の内容を列記して説明する。

[0013] （１）本開示の実施の形態に係る検知装置は、周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置であって、前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出する算出部と、前記算出部により算出された前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行う検知部と、前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするリセット部とを備える。

[0014] このように、メッセージの観測結果と当該観測結果に関する参照情報との関係に応じて増減する検知指標に基づいて検知処理を行い、検知指標の極値を検出した場合において検知指標をリセットする構成により、たとえばネットワークにおける異常な状態が解消されることにより検知指標の増減傾向が変化した場合において、リセットされた検知指標に基づいて検知処理を行うことができる。これにより、ネットワークにおいて異常な状態が解消されたことをより早期に検知し、異常な状態が解消された正常状態における異常の誤検知を抑制することができる。したがって、ネットワークにおける異常をより正しく検知することができる。

[0015] （２）上記（１）において、前記参照情報は、前記観測結果に基づいて算出される過去の前記メッセージの受信間隔であってもよく、前記算出部は、前記観測結果に基づいて算出される前記メッセージの受信間隔と、前記過去のメッセージの受信間隔とを用いて、前記メッセージの受信間隔の移動平均値であって、前記メッセージの受信間隔と前記過去のメッセージの受信間隔との大小関係に応じて増減する前記移動平均値を、前記検知指標として前記メッセージごとに算出してもよい。

[0016] このような構成により、簡易な処理で検知指標を算出することができる。また、ネットワークにおける異常の発生に応じて変化し易い移動平均値を用いて検知処理を行うことができるので、異常の発生を早期に検知することができる。

[0017] （３）上記（２）において、前記検知部は、前記検知指標が所定のしきい値未満である場合、前記ネットワークにおける異常が発生していると判定してもよく、前記リセット部は、前記極値として前記検知指標の極小値を検出した場合、前記検知処理において用いる前記検知指標をリセットしてもよい。

[0018] このような構成により、ネットワークにおける異常な状態が解消されることにより移動平均値が減少傾向から増加傾向に転じた場合において、リセットされた移動平均値に基づいて、ネットワークにおける異常をより正しく検知することができる。

[0019] （４）上記（１）において、前記参照情報は、前記メッセージの受信間隔の平均値であってもよく、前記算出部は、前記観測結果に基づいて算出される前記メッセージの受信間隔と、前記平均値と、前記メッセージの受信間隔の標準偏差とを用いて、前記メッセージの受信間隔の統計値であって、前記メッセージの受信間隔と前記平均値との差分の大きさに応じて増減する前記統計値を、前記検知指標として前記メッセージごとに算出してもよい。

[0020] このような構成により、メッセージの受信間隔の、平均値すなわち正常値からの逸脱度合いを示す統計値に基づいて、ネットワークにおける異常をより正確に検知することができる。

[0021] （５）上記（４）において、前記検知部は、前記検知指標が所定のしきい値よりも大きい場合、前記ネットワークにおける異常が発生していると判定してもよく、前記リセット部は、前記極値として前記検知指標の極大値を検出した場合、前記検知処理において用いる前記検知指標をリセットしてもよい。

[0022] このような構成により、ネットワークにおける異常な状態が解消されることにより統計値が増加傾向から減少傾向に転じた場合において、リセットされた統計値に基づいて、ネットワークにおける異常をより正しく検知することができる。

[0023] （６）本開示の実施の形態に係る検知方法は、周期メッセージを含む複数

のメッセージが送受信されるネットワークにおける異常を検知する検知装置、における検知方法であって、前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出するステップと、算出した前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行うステップと、前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするステップとを含む。

[0024] このように、メッセージの観測結果と当該観測結果に関する参照情報との関係に応じて増減する検知指標に基づいて検知処理を行い、検知指標の極値を検出した場合において検知指標をリセットする方法により、たとえばネットワークにおける異常な状態が解消されることにより検知指標の増減傾向が変化した場合において、リセットされた検知指標に基づいて検知処理を行うことができる。これにより、ネットワークにおいて異常な状態が解消されたことをより早期に検知し、異常な状態が解消された正常状態における異常の誤検知を抑制することができる。したがって、ネットワークにおける異常をより正しく検知することができる。

[0025] 以下、本開示の実施の形態について図面を用いて説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰り返さない。また、以下に記載する実施の形態の少なくとも一部を任意に組み合わせてもよい。

[0026] ［構成および基本動作］

図１は、本開示の実施の形態に係る通信システムの構成を示す図である。図１を参照して、通信システム３０１は、中継装置１０１と、複数の通信装置１１１とを備える。通信システム３０１は、たとえば車両に搭載される。この場合、通信装置１１１は、たとえば車載ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）である。

[0027] 中継装置１０１および通信装置１１１は、ネットワーク２０１を構成する。より詳細には、中継装置１０１および通信装置１１１は、伝送線１０を介して互いに接続される。伝送線１０は、たとえば、ＣＡＮ（Ｃｏｎｔｒｏｌ

ｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）（登録商標）、ＦｌｅｘＲａｙ（登録商標）、ＭＯＳＴ（Ｍｅｄｉａ　Ｏｒｉｅｎｔｅｄ　Ｓｙｓｔｅｍｓ　Ｔｒａｎｓｐｏｒｔ）（登録商標）、イーサネット（登録商標）、およびＬＩＮ（Ｌｏｃａｌ　Ｉｎｔｅｒｃｏｎｎｅｃｔ　Ｎｅｔｗｏｒｋ）等の規格に従うケーブルである。

[0028] 中継装置１０１は、通信装置１１１と通信を行うことが可能である。中継装置１０１は、たとえば、異なる伝送線１０に接続された複数の通信装置１１１間でやり取りされる情報を中継する中継処理を行う。

[0029] ネットワーク２０１では、周期的に送信されるメッセージを含む複数のメッセージが送受信される。

[0030] より詳細には、ネットワーク２０１では、たとえば、所定の取り決めに従って、通信装置１１１から他の通信装置１１１へ中継装置１０１経由で周期的にメッセージが送信される。以下、ネットワーク２０１において周期的に送信されるメッセージを、周期メッセージとも称する。なお、「周期メッセージ」とは、厳密に周期的に送信されたメッセージに限らず、周期的に送信されるべき種類のメッセージを意味するものとする。

[0031] また、ネットワーク２０１では、周期メッセージの他に、通信装置１１１から他の通信装置１１１へ中継装置１０１経由で不定期に送信されるメッセージが存在する。以下、ネットワーク２０１において不定期に送信されるメッセージを、イベントメッセージとも称する。

[0032] 通信装置１１１によるメッセージの送信は、ブロードキャストによって行われてもよいし、ユニキャストによって行われてもよいし、マルチキャストによって行われてもよい。

[0033] 中継装置１０１は、検知装置として機能し、ネットワーク２０１における異常を検知する。たとえば、中継装置１０１は、ネットワーク２０１における異常として、ネットワーク２０１における不正メッセージの存在を検知する。

[0034] 〔中継装置〕

図２は、本開示の実施の形態に係る中継装置の構成を示す図である。図２を参照して、中継装置１０１は、通信処理部１１と、算出部１２と、リセット部１３と、検知部１４と、記憶部１５と、複数の通信ポート１６とを備える。通信処理部１１、算出部１２、リセット部１３および検知部１４の一部または全部は、たとえば、１または複数のプロセッサを含む処理回路（Ｃｉｒｃｕｉｔｒｙ）により実現される。記憶部１５は、たとえば上記処理回路に含まれるフラッシュメモリである。通信ポート１６は、たとえばコネクタまたは端子である。各通信ポート１６には、伝送線１０が接続される。

[0035] 通信処理部１１は、通信装置１１１間で伝送されるメッセージを中継する中継処理を行う。たとえば、通信処理部１１は、通信装置１１１から対応の伝送線１０および対応の通信ポート１６経由でメッセージを受信すると、受信したメッセージの複製であるメッセージＣＰを生成し、生成したメッセージＣＰに、受信したメッセージの受信時刻を示すタイムスタンプを付与する。そして、通信処理部１１は、受信したメッセージを他の通信装置１１１へ対応の通信ポート１６および対応の伝送線１０経由で送信し、タイムスタンプが付与されたメッセージＣＰを算出部１２へ出力する。

[0036] （検知指標の算出）

算出部１２は、メッセージの受信時刻と、当該受信時刻に関する参照情報との関係に応じて増減する検知指標を算出する。メッセージの受信時刻は、メッセージの観測結果の一例である。

[0037] より詳細には、算出部１２は、通信処理部１１によって中継されるメッセージのうちの、中継装置１０１における検知処理の対象となるメッセージの受信時刻ｔを取得する。以下、中継装置１０１における検知処理の対象となるメッセージを、対象メッセージとも称する。対象メッセージは、１つの通信装置１１１から送信される１種類のメッセージであってもよいし、複数の通信装置１１１の各々から送信される複数種類のメッセージあってもよい。以下では、中継装置１０１が、ある通信装置１１１から送信されるメッセージを「対象メッセージＭ」として検知処理を行う例について説明する。

[0038] たとえば、記憶部１５は、対象メッセージの種類ごとのＩＤを記憶している。以下、対象メッセージＭのＩＤを対象ＩＤとも称する。

[0039] 算出部１２は、通信処理部１１からメッセージＣＰを受けて、受けたメッセージＣＰに含まれるＩＤ、および記憶部１５における対象ＩＤを確認する。

[0040] そして、算出部１２は、通信処理部１１から受けたメッセージＣＰに含まれるＩＤが対象ＩＤと一致する場合、当該メッセージＣＰの複製元のメッセージが対象メッセージＭであると認識し、当該メッセージＣＰに付与されたタイムスタンプを参照することにより、対象メッセージＭの受信時刻ｔを取得する。

[0041] 算出部１２は、対象メッセージＭの受信時刻ｔを取得すると、当該受信時刻ｔと、直前の対象メッセージＭの受信時刻ｔとの差分を対象メッセージＭの受信間隔ｘとして算出する。より詳細には、算出部１２は、通信処理部１１によって受信されたｍ番目の対象メッセージＭｍの受信時刻ｔｍから、通信処理部１１によって受信された（ｍ－１）番目の対象メッセージＭ（ｍ－１）の受信時刻ｔ（ｍ－１）を差し引くことにより、対象メッセージＭｍの受信間隔ｘｍを算出する。ここで、ｍは正の整数である。算出部１２は、算出した受信間隔ｘｍを記憶部１５に保存する。

[0042] 算出部１２は、算出した受信間隔ｘを用いて検知指標を算出する。たとえば、算出部１２は、受信間隔ｘの標準偏差σを用いて、受信間隔ｘの統計値Ｔを対象メッセージＭごとに算出する。統計値Ｔは、受信間隔ｘの、正常状態からの逸脱度合いを示す。統計値Ｔは、検知指標の一例である。

[0043] より詳細には、算出部１２は、対象メッセージＭｍの受信間隔ｘｍを算出すると、以下の式（１）に従って、対象メッセージＭｍの異常度Ｄｍを算出する。

[数1]

$$Dm = \left(\frac{xm-\mu}{\sigma}\right)^2 \quad \cdots (1)$$

[0044] ここで、μは、受信間隔ｘの平均値であり、対象メッセージＭに関する参照情報の一例である。標準偏差σおよび平均値μは、記憶部１５に保存されている。たとえば、標準偏差σは、予め通信システム３０１の製造者により受信間隔ｘに基づいて算出され、記憶部１５に保存される。また、たとえば、平均値μは、予め通信システム３０１の製造者により、ネットワーク２０１における対象メッセージＭの送信周期の設計値に基づいて算出される値であり、予め記憶部１５に保存される。なお、算出部１２は、定期的または不定期に、複数の対象メッセージＭに対応する複数の受信間隔ｘに基づいて標準偏差σおよび平均値μを算出し、記憶部１５における標準偏差σおよび平均値μを、算出した標準偏差σおよび平均値μに更新してもよい。

[0045] 算出部１２は、対象メッセージＭｍの異常度Ｄｍを算出すると、以下の式（２）に従って、対象メッセージＭｍの統計値Ｔｍを算出する。

[数2]

$$Tm = max\{0, (T(m-1) + Dm - k)\} \cdots (2)$$

[0046] ここで、ｋは、制限パラメータである。制限パラメータｋは、予め設定された定数である。式（２）に示すように、対象メッセージＭｍの統計値Ｔｍは、対象メッセージＭ（ｍ－１）の統計値Ｔ（ｍ－１）と異常度Ｄｍとの和から制限パラメータｋを差し引いた値、およびゼロのうちの大きい方の値となる。

[0047] 式（１）および式（２）に示されるように、統計値Ｔｍは、対象メッセージＭｍの受信間隔ｘｍと、平均値μとの差分の大きさに応じて増減する。具体的には、受信間隔ｘｍが平均値μから大きく乖離した値となることにより、異常度Ｄｍが制限パラメータｋよりも大きな値となった場合、対象メッセージＭｍの統計値Ｔｍは、直前の対象メッセージＭ（ｍ－１）の統計値Ｔ（ｍ－１）よりも大きな値となる。一方、受信間隔ｘｍが平均値μに近い値となることにより、異常度Ｄｍが制限パラメータｋよりも小さな値となった場合、対象メッセージＭｍの統計値Ｔｍは、ゼロとなるか、または直前の対象メッセージＭ（ｍ－１）の統計値Ｔ（ｍ－１）よりも小さな値となる。

[0048] 算出部１２は、統計値Ｔｍを算出すると、算出した統計値Ｔｍを記憶部１５に保存する。

[0049] （検知処理）

検知部１４は、算出部１２により算出された統計値Ｔに基づいて、ネットワーク２０１における異常を検知する検知処理を行う。たとえば、検知部１４は、算出部１２により算出された統計値Ｔと、所定のしきい値Ｔｈｘとに基づいて、ネットワーク２０１における異常として、ネットワーク２０１における不正メッセージの存在を検知する。

[0050] より詳細には、検知部１４は、算出部１２により算出された統計値Ｔを記憶部１５から取得し、取得した統計値Ｔとしきい値Ｔｈｘとを比較する。検知部１４は、統計値Ｔがしきい値Ｔｈｘ以下である場合、ネットワーク２０１における異常は発生していないと判定する。一方、検知部１４は、統計値Ｔがしきい値Ｔｈｘよりも大きい場合、ネットワーク２０１における異常が発生していると判定する。

[0051] 図３は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の一例を示す図である。図３において、横軸は時刻を示している。

[0052] 図３を参照して、通信処理部１１により受信される複数の対象メッセージＭは、受信時刻ｔ１から受信時刻ｔ１２までの期間において、所定の送信周期Ｃｍに基づくタイミングで受信される正当な周期メッセージである対象メッセージＭ１～Ｍ４，Ｍ６，Ｍ８，Ｍ１０，Ｍ１２と、受信時刻ｔ５から受信時刻ｔ１３までの期間において、たとえば送信周期Ｃｍに基づくタイミングで受信される不正メッセージＢＭである対象メッセージＭ５，Ｍ７，Ｍ９，Ｍ１１，Ｍ１３とを含む。すなわち、受信時刻ｔ５から受信時刻ｔ１３までの期間において、正当な周期メッセージと不正な周期メッセージとが、中継装置１０１へ交互に到来する。

[0053] 図４は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。図４において、横軸は時刻を示しており、

縦軸は統計値を示している。図４における統計値Ｔ１～Ｔ１３は、図３に示す対象メッセージＭ１～Ｍ１３の受信時刻ｔ１～ｔ１３に基づいて、上述した式（２）に従って算出部１２により算出された統計値Ｔである。

[0054] 図４を参照して、受信時刻ｔ１から受信時刻ｔ４までの期間では、一定の送信周期Ｃｍで送信される正当な対象メッセージＭ１～Ｍ４のみが通信処理部１１により受信され、受信間隔ｘ１～ｘ４が平均値μとほぼ等しい値となるので、算出部１２により算出される統計値Ｔ１～Ｔ４はゼロである。

[0055] 検知部１４は、算出部１２により算出された統計値Ｔ１～Ｔ４がしきい値Ｔｈｘ以下であるので、受信時刻ｔ１から受信時刻ｔ４までの期間においてネットワーク２０１における異常は発生していないと判定する。

[0056] 一方、受信時刻ｔ５から受信時刻ｔ１３までの期間では、送信周期Ｃｍで送信される対象メッセージＭ６，Ｍ８，Ｍ１０，Ｍ１２に加えて、不正メッセージＢＭが通信処理部１１により受信され、受信間隔ｘ５～ｘ１３が平均値μから乖離した値となるので、算出部１２により算出される統計値Ｔ５～Ｔ１３は徐々に増加する。

[0057] 検知部１４は、算出部１２により算出された統計値Ｔ９がしきい値Ｔｈｘを超えるので、受信時刻ｔ９においてネットワーク２０１における異常が発生したと判定する。検知部１４は、ネットワーク２０１における異常が発生したと判定した場合、ネットワーク２０１における異常が発生したことを示す警報情報を通信処理部１１経由で通信システム３０１外における上位装置へ送信する。上位装置は、たとえば、警報情報を受けて所定の処理を行うサーバ等の装置である。

[0058] ここで、しきい値Ｔｈｘは、ネットワーク２０１の製造者により任意に設定可能である。たとえば、しきい値Ｔｈｘをより小さい値に設定することにより、ネットワーク２０１における不正メッセージの送信が開始された後、より早期に、ネットワーク２０１における異常が発生していると判定することができる。

[0059] 図５は、本開示の実施の形態に係る中継装置により受信される対象メッセ

ージおよび受信時刻の分布の一例を示す図である。図５において、横軸は時刻を示している。図５は、図３に示す受信時刻ｔ１３以降の受信時刻ｔ１４～ｔ１６において、通信処理部１１により受信される対象メッセージＭ１４～Ｍ１６を示している。

[0060] 図５を参照して、通信処理部１１により受信される対象メッセージＭ１４～Ｍ１６は、受信時刻ｔ１４から受信時刻ｔ１６までの期間において送信周期Ｃｍで送信される正当な周期メッセージである。すなわち、受信時刻ｔ１３において、中継装置１０１への不正メッセージの到来は終了している。

[0061] ［課題］

図６は、本開示の実施の形態の比較例に係る中継装置において検知処理に用いられる統計値の一例を示す図である。図６において、横軸は時刻を示しており、縦軸は統計値を示している。図６における統計値Ｔ４～Ｔ１６は、図５に示す対象メッセージＭ４～Ｍ１６の受信時刻ｔ４～ｔ１６に基づいて、上述した式（２）に従って算出部１２により算出された統計値Ｔである。

[0062] 図６を参照して、受信時刻ｔ１４から受信時刻ｔ１６までの期間では、一定の送信周期Ｃｍで送信される正当な対象メッセージＭ１４～Ｍ１６のみが中継装置に到来するので、算出される統計値Ｔ１４～Ｔ１６は徐々に減少する。

[0063] しかしながら、比較例に係る中継装置では、統計値Ｔ１４～Ｔ１６がしきい値Ｔｈｘよりも大きいので、受信時刻ｔ９から受信時刻ｔ１３までの期間に加えて、受信時刻ｔ１４以降の期間においても、ネットワーク２０１における異常が発生していると判定する。すなわち、比較例に係る中継装置は、統計値Ｔ１４～Ｔ１６に基づいて検知処理を行う場合、受信時刻ｔ１３において不正メッセージの到来は終了しており、ネットワーク２０１への攻撃が発生していない状態であるにもかかわらず、不正メッセージの到来終了を検知することができず、ネットワーク２０１における異常が継続していると判定してしまう。

[0064] そこで、本開示の実施の形態に係る中継装置１０１は、以下のような構成

により、上記の課題を解決する。

[0065] （リセット処理）

リセット部１３は、統計値Ｔを監視し、統計値Ｔの極大値を検出した場合、検知処理において用いられる統計値Ｔをリセットする。たとえば、リセット部１３は、統計値Ｔが極大値であるか否かを判断する。リセット部１３は、あるタイミングの統計値Ｔが極大値であると判断し、かつ当該統計値Ｔがしきい値Ｔｈｘよりも大きい場合、当該タイミングにおける統計値Ｔをリセットすることにより更新する。

[0066] たとえば、検知部１４は、算出部１２により統計値Ｔが記憶部１５に保存されると、リセット部１３により当該統計値Ｔが極大値ではないと判断されるか、またはリセット部１３により当該統計値Ｔが更新されるまで、当該統計値Ｔに基づく検知処理を待機する。検知部１４は、リセット部１３により統計値Ｔが極大値ではなく、更新の必要がないと判断された場合、当該統計値Ｔに基づいて検知処理を行う。一方、検知部１４は、リセット部１３により統計値Ｔが更新された場合、更新後の統計値Ｔに基づいて検知処理を行う。

[0067] 検知部１４は、リセット部１３により統計値Ｔが極大値ではないと判断されるか、または統計値Ｔが更新される度に、当該統計値Ｔに基づいて順次検知処理を行ってもよいし、リセット部１３により極大値ではないと判断されるか、または更新された所定数の統計値Ｔを蓄積し、蓄積した統計値Ｔに基づいて事後的に検知処理を行ってもよい。

[0068] 図７は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。図７において、横軸は時刻を示しており、縦軸は統計値を示している。図７における統計値Ｔ４～Ｔ１３は、図５に示す対象メッセージＭ４～Ｍ１３の受信時刻ｔ４～ｔ１３に基づいて、上述した式（２）に従って算出部１２により算出された統計値Ｔである。図７における統計値Ｔ１４～Ｔ１６は、対象メッセージＭ１４～Ｍ１６の受信時刻ｔ１４～ｔ１６に基づいて、上述した式（２）に従って算出部１２により算出

され、かつリセット部１３により更新された統計値Ｔである。

[0069] 図７を参照して、リセット部１３は、算出部１２により記憶部１５に保存される統計値Ｔを監視し、統計値Ｔ（ｍ－１）および統計値Ｔｍの２つの統計値Ｔが連続して増加しており、かつ統計値Ｔ（ｍ＋１）および統計値Ｔ（ｍ＋２）の２つの統計値Ｔが連続して減少している場合、統計値Ｔｍは極大値であると判断する。

[0070] 具体的には、リセット部１３は、記憶部１５を参照し、統計値Ｔ１３が統計値Ｔ１２から増加しており、統計値Ｔ１４が統計値Ｔ１３から増加しており、統計値Ｔ１５が統計値Ｔ１４から減少しており、かつ統計値Ｔ１６が統計値Ｔ１５から減少していると判断する。そして、リセット部１３は、統計値Ｔ１３，Ｔ１４が連続して増加しており、かつ統計値Ｔ１５，Ｔ１６が連続して減少しているので、統計値Ｔ１４は極大値であると判断する。

[0071] そして、リセット部１３は、極大値であると判断した統計値Ｔ１４がしきい値Ｔｈｘよりも大きいので、記憶部１５における統計値Ｔ１４を、たとえばゼロであるリセット値に更新する。また、リセット部１３は、統計値Ｔ１４の算出タイミングよりも後に算出されて記憶部１５に保存されている他の統計値Ｔ１５，Ｔ１６を、更新後の統計値Ｔ１４に基づいて更新する。より詳細には、リセット部１３は、更新後の統計値Ｔ１４を用いて、上述した式（２）に従って統計値Ｔ１５を算出する。

[0072] リセット部１３は、統計値Ｔ１５を算出すると、記憶部１５における統計値Ｔ１５を、算出した統計値Ｔ１５に更新する。リセット部１３は、同様にして、統計値Ｔ１６を算出し、記憶部１５における統計値Ｔ１６を、算出した統計値Ｔ１６に更新する。

[0073] 検知部１４は、リセット部１３による更新後の統計値Ｔ１４～Ｔ１６がしきい値Ｔｈｘ以下であるので、受信時刻ｔ１４～ｔ１６までの期間においてネットワーク２０１における異常は発生していないと判定する。すなわち、検知部１４は、受信時刻ｔ９から始まった異常な状態が、受信時刻ｔ１３までに終了したと判定する。

[0074] このように、検知部１４が、リセットされた統計値Ｔ１４に基づいて検知処理を行う構成により、リセットされていない統計値Ｔ１４に基づいて検知処理を行う構成と比べて、中継装置１０１への不正メッセージの到来が終了した場合において、より早期に不正メッセージの到来終了を検知し、異常な状態が解消された正常状態における異常の誤検知を抑制することができる。

[0075] 図８は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の他の例を示す図である。図８において、横軸は時刻を示している。

[0076] 図８を参照して、通信処理部１１により受信される複数の対象メッセージＭは、受信時刻ｔ１から受信時刻ｔ１１までの期間において、送信周期Ｃｍに基づくタイミングで受信される正当な周期メッセージである対象メッセージＭ１，Ｍ３，Ｍ４，Ｍ６，Ｍ７，Ｍ９～Ｍ１１と、受信時刻ｔ２から受信時刻ｔ８までの期間において、たとえば送信周期Ｃｍの２倍の周期に基づくタイミングで受信される不正メッセージＢＭである対象メッセージＭ２，Ｍ５，Ｍ８とを含む。

[0077] 図９は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。図９において、横軸は時刻を示しており、縦軸は統計値を示している。図９における統計値Ｔ１～Ｔ８は、図８に示す対象メッセージＭ１～Ｍ８の受信時刻ｔ１～ｔ８に基づいて、上述した式（２）に従って算出部１２により算出された統計値Ｔである。図９における統計値Ｔ９～Ｔ１１は、対象メッセージＭ９～Ｍ１１の受信時刻ｔ９～ｔ１１に基づいて、上述した式（２）に従って算出部１２により算出され、かつリセット部１３により更新された統計値Ｔである。

[0078] 図９を参照して、正当な対象メッセージＭ１の受信時刻ｔ１から送信周期Ｃｍが経過する前の受信時刻ｔ２において不正な対象メッセージＭ２が通信処理部１１により受信され、かつ受信時刻ｔ１から送信周期Ｃｍ経過後の受信時刻ｔ３において正当な対象メッセージＭ３が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ２，Ｔ３は徐々に増加す

る。

[0079] 次に、受信時刻ｔ３から送信周期Ｃｍ経過後の受信時刻ｔ４において正当な対象メッセージＭ４が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ４は統計値Ｔ３から減少する。

[0080] 次に、受信時刻ｔ４から送信周期Ｃｍが経過する前の受信時刻ｔ５において不正な対象メッセージＭ５が通信処理部１１により受信され、かつ受信時刻ｔ４から送信周期Ｃｍ経過後の受信時刻ｔ６において正当な対象メッセージＭ６が通信処理部１１により受信される。したがって、算出部１２により算出される統計値Ｔ５，Ｔ６は徐々に増加し、統計値Ｔ５，Ｔ６がしきい値Ｔｈｘを超える。検知部１４は、算出部１２により算出された統計値Ｔ５がしきい値Ｔｈｘよりも大きいので、受信時刻ｔ５においてネットワーク２０１における異常が発生したと判定する。

[0081] 次に、受信時刻ｔ６から送信周期Ｃｍ経過後の受信時刻ｔ７において正当な対象メッセージＭ７が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ７は統計値Ｔ６から減少する。

[0082] 次に、受信時刻ｔ７から送信周期Ｃｍが経過する前の受信時刻ｔ８において不正な対象メッセージＭ８が通信処理部１１により受信され、かつ受信時刻ｔ７から送信周期Ｃｍ経過後の受信時刻ｔ９において正当な対象メッセージＭ９が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ８，Ｔ９は徐々に増加する。

[0083] 次に、受信時刻ｔ９から送信周期Ｃｍ経過後の受信時刻ｔ１０において正当な対象メッセージＭ１０が通信処理部１１により受信され、かつ受信時刻ｔ１０から送信周期Ｃｍ経過後の受信時刻ｔ１１において正当な対象メッセージＭ１１が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ１０，Ｔ１１は統計値Ｔ９から徐々に減少する。

[0084] リセット部１３は、統計値Ｔ８，Ｔ９が連続して増加しており、かつ統計値Ｔ１０，Ｔ１１が連続して減少しているので、統計値Ｔ９は極大値であると判断する。そして、リセット部１３は、極大値であると判断した統計値Ｔ

９がしきい値Ｔｈｘよりも大きいので、統計値Ｔ９をリセット値に更新する。さらに、リセット部１３は、算出部１２により算出された統計値Ｔ１０を、更新後の統計値Ｔ９を用いて算出した統計値Ｔ１０に更新し、算出部１２により算出された統計値Ｔ１１を、更新後の統計値Ｔ１０を用いて算出した統計値Ｔ１１に更新する。

[0085] 検知部１４は、リセット部１３による更新後の統計値Ｔ９～Ｔ１１がしきい値Ｔｈｘ以下であるので、受信時刻ｔ９～ｔ１１までの期間においてネットワーク２０１における異常は発生していないと判定する。すなわち、検知部１４は、受信時刻ｔ５から始まった異常な状態が、受信時刻ｔ８までに終了したと判定する。

[0086] 図１０は、本開示の実施の形態に係る中継装置により受信される対象メッセージおよび受信時刻の分布の他の例を示す図である。図１０において、横軸は時刻を示している。

[0087] 図１０を参照して、通信処理部１１により受信される複数の対象メッセージＭは、受信時刻ｔ１から受信時刻ｔ１２までの期間において、送信周期Ｃｍに基づくタイミングで受信される正当な周期メッセージである対象メッセージＭ１，Ｍ３，Ｍ４，Ｍ７，Ｍ８，Ｍ１０～Ｍ１２と、受信時刻ｔ２から受信時刻ｔ９までの期間においてたとえば送信周期Ｃｍの２倍の周期に基づくタイミングで受信される不正メッセージＢＭである対象メッセージＭ２，Ｍ６，Ｍ９と、受信時刻ｔ５において送信されるイベントメッセージＩＭである対象メッセージＭ５とを含む。

[0088] 図１１は、本開示の実施の形態に係る中継装置において検知処理に用いられる統計値の一例を示す図である。図１１において、横軸は時刻を示しており、縦軸は統計値を示している。図１１における統計値Ｔ１～Ｔ９は、図１０に示す対象メッセージＭ１～Ｍ９の受信時刻ｔ１～ｔ９に基づいて、上述した式（２）に従って算出部１２により算出された統計値Ｔである。図１１における統計値Ｔ１０～Ｔ１２は、対象メッセージＭ１０～Ｍ１２の受信時刻ｔ１０～ｔ１２に基づいて、上述した式（２）に従って算出部１２により

算出され、かつリセット部１３により更新された統計値Ｔである。

[0089] 図１１を参照して、正当な対象メッセージＭ１の受信時刻ｔ１から送信周期Ｃｍが経過する前の受信時刻ｔ２において不正な対象メッセージＭ２が通信処理部１１により受信され、かつ受信時刻ｔ１から送信周期Ｃｍ経過後の受信時刻ｔ３において正当な対象メッセージＭ３が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ２，Ｔ３は徐々に増加する。

[0090] 次に、受信時刻ｔ３から送信周期Ｃｍ経過後の受信時刻ｔ４において正当な対象メッセージＭ４が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ４は統計値Ｔ３から減少する。

[0091] 次に、受信時刻ｔ４から送信周期Ｃｍが経過する前の受信時刻ｔ５，ｔ６において、不定期に送信される正当な対象メッセージＭ５および不正な対象メッセージＭ６が通信処理部１１によりそれぞれ受信され、かつ受信時刻ｔ４から送信周期Ｃｍ経過後の受信時刻ｔ７において正当な対象メッセージＭ７が通信処理部１１により受信される。したがって、算出部１２により算出される統計値Ｔ５，Ｔ６，Ｔ７は徐々に増加し、統計値Ｔ６，Ｔ７がしきい値Ｔｈｘを超える。検知部１４は、算出部１２により算出された統計値Ｔ６がしきい値Ｔｈｘよりも大きいので、受信時刻ｔ６においてネットワーク２０１における異常が発生したと判定する。

[0092] 次に、受信時刻ｔ７から送信周期Ｃｍ経過後の受信時刻ｔ８において正当な対象メッセージＭ８が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ８は統計値Ｔ７から減少する。

[0093] 次に、受信時刻ｔ８から送信周期Ｃｍが経過する前の受信時刻ｔ９において不正な対象メッセージＭ９が通信処理部１１により受信され、かつ受信時刻ｔ８から送信周期Ｃｍ経過後の受信時刻ｔ１０において正当な対象メッセージＭ１０が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ９，Ｔ１０は徐々に増加する。

[0094] 次に、受信時刻ｔ１０から送信周期Ｃｍ経過後の受信時刻ｔ１１において

正当な対象メッセージＭ１１が通信処理部１１により受信され、かつ受信時刻ｔ１１から送信周期Ｃｍ経過後の受信時刻ｔ１２において正当な対象メッセージＭ１２が通信処理部１１により受信されるので、算出部１２により算出される統計値Ｔ１１，Ｔ１２は統計値Ｔ１０から徐々に減少する。

[0095] リセット部１３は、統計値Ｔ９，Ｔ１０が連続して増加しており、かつ統計値Ｔ１１，Ｔ１２が連続して減少しているので、統計値Ｔ１０は極大値であると判断する。そして、リセット部１３は、極大値であると判断した統計値Ｔ１０がしきい値Ｔｈｘよりも大きいので、統計値Ｔ１０をリセット値に更新する。さらに、リセット部１３は、算出部１２により算出された統計値Ｔ１１を、更新後の統計値Ｔ１０を用いて算出した統計値Ｔ１１に更新し、算出部１２により算出された統計値Ｔ１２を、更新後の統計値Ｔ１１を用いて算出した統計値Ｔ１２に更新する。

[0096] 検知部１４は、リセット部１３による更新後の統計値Ｔ１０～Ｔ１２がしきい値Ｔｈｘ以下であるので、受信時刻ｔ１０～ｔ１２までの期間においてネットワーク２０１における異常は発生していないと判定する。

[0097] ＜変形例＞

中継装置１０１は、統計値Ｔ以外の検知指標に基づいて検知処理を行う構成であってもよい。一例として、算出部１２は、対象メッセージＭの受信間隔ｘの移動平均を用いて検知指標を算出する。

[0098] たとえば、算出部１２は、通信処理部１１により受信された直近のｐ個の対象メッセージＭの受信間隔ｘの移動平均値Ａを対象メッセージＭごとに算出する。ｐは、２以上の整数である。移動平均値Ａは、検知指標の一例である。

[0099] より詳細には、算出部１２は、対象メッセージＭｍの受信間隔ｘｍを算出すると、受信間隔ｘｍと、過去の対象メッセージＭ（ｍ－１），Ｍ（ｍ－２）・・・Ｍ（ｍ－ｐ＋１）の受信間隔ｘ（ｍ－１），ｘ（ｍ－２）・・・，ｘ（ｍ－ｐ＋１）とを用いて、対象メッセージＭｍに対応する移動平均値Ａｍを算出する。ここで、受信間隔ｘ（ｍ－１），ｘ（ｍ－２）・・・，ｘ（

ｍ－ｐ＋１）は、対象メッセージＭに関する参照情報の一例である。以下、受信間隔ｘ（ｍ－１），ｘ（ｍ－２）・・・，ｘ（ｍ－ｐ＋１）を、参照間隔ｒｍとも称する。移動平均値Ａｍは、対象メッセージＭｍの受信間隔ｘｍと、参照間隔ｒｍとの大小関係に応じて増減する。

[0100] たとえば、算出部１２により算出される移動平均値Ａは、図３に示すように通信処理部１１により受信される複数の対象メッセージＭが不正メッセージＢＭを含む場合、受信時刻ｔ５から受信時刻ｔ１３までの期間において徐々に減少する。

[0101] 検知部１４は、算出部１２により算出された移動平均値Ａに基づいて検知処理を行う。たとえば、検知部１４は、算出部１２により算出された移動平均値Ａと、所定のしきい値Ｔｈｙとに基づいて、ネットワーク２０１における異常を検知する。

[0102] より詳細には、検知部１４は、算出部１２により算出された移動平均値Ａとしきい値Ｔｈｙとを比較する。検知部１４は、移動平均値Ａがしきい値Ｔｈｙ以上である場合、ネットワーク２０１における異常は発生していないと判定する。一方、検知部１４は、移動平均値Ａがしきい値Ｔｈｙ未満である場合、ネットワーク２０１における異常が発生していると判定する。

[0103] リセット部１３は、移動平均値Ａを監視し、移動平均値Ａの極小値を検出した場合、検知処理において用いられる移動平均値Ａをリセットする。たとえば、リセット部１３は、統計値Ｔが極大値であるか否かを判断する手順と同様にして、移動平均値Ａが極小値であるか否かを判断する。リセット部１３は、移動平均値Ａが極小値であると判断し、かつ当該移動平均値Ａがしきい値Ｔｈｙ未満である場合、当該移動平均値Ａをリセットすることにより更新する。

[0104] 検知部１４は、リセット部１３により移動平均値Ａが更新された場合、更新された移動平均値Ａに基づいて検知処理を行う。

[0105] ［動作の流れ］

図１２は、本開示の実施の形態に係る中継装置が検知処理を行う際の動作

手順の一例を定めたフローチャートである。

[0106] 図１２を参照して、まず、中継装置１０１は、メッセージの到来を待ち受け（ステップＳ１０２でＮＯ）、メッセージを受信すると（ステップＳ１０２でＹＥＳ）、受信したメッセージが対象メッセージＭであるか否かを判断する（ステップＳ１０４）。

[0107] 次に、中継装置１０１は、受信したメッセージが対象メッセージＭではないと判断した場合（ステップＳ１０６でＮＯ）、新たなメッセージの到来を待ち受ける（ステップＳ１０２でＮＯ）。

[0108] 一方、中継装置１０１は、受信したメッセージが対象メッセージＭであると判断した場合（ステップＳ１０６でＹＥＳ）、当該対象メッセージＭの受信時刻ｔを用いて統計値Ｔを算出する。中継装置１０１は、算出した統計値Ｔを記憶部１５に保存する（ステップＳ１０８）。

[0109] 次に、中継装置１０１は、所定回数前に算出した統計値Ｔが極大値であるか否かを判断する（ステップＳ１１０）。

[0110] 次に、中継装置１０１は、所定回数前に算出した統計値Ｔが極大値ではないと判断した場合（ステップＳ１１２でＮＯ）、当該統計値Ｔに基づいて検知処理を行う（ステップＳ１１６）。

[0111] 一方、中継装置１０１は、所定回数前に算出した統計値Ｔが極大値であると判断した場合（ステップＳ１１２でＹＥＳ）、当該統計値Ｔをリセットすることにより更新する。また、中継装置１０１は、当該統計値Ｔの算出タイミングよりも後に算出して記憶部１５に保存した他の統計値Ｔを、更新後の統計値Ｔに基づいて更新する（ステップＳ１１４）。

[0112] 次に、中継装置１０１は、更新した統計値Ｔに基づいて検知処理を行う（ステップＳ１１６）。

[0113] 次に、中継装置１０１は、ネットワーク２０１における異常は発生していないと判定した場合（ステップＳ１１８でＮＯ）、新たなメッセージの到来を待ち受ける（ステップＳ１０２でＮＯ）。

[0114] 一方、中継装置１０１は、ネットワーク２０１における異常が発生したと

判定した場合（ステップＳ１１８でＹＥＳ）、ネットワーク２０１における異常が発生したことを示す警報情報を通信システム３０１外における上位装置へ送信する（ステップＳ１２０）。

[0115] 次に、中継装置１０１は、新たなメッセージの到来を待ち受ける（ステップＳ１０２でＮＯ）。

[0116] なお、本開示の実施の形態に係る通信システム３０１では、中継装置１０１が、ネットワーク２０１における異常を検知する構成であるとしたが、これに限定するものではない。通信システム３０１では、中継装置１０１とは別の装置が、検知装置として機能し、ネットワーク２０１における異常を検知する構成であってもよい。たとえば、通信システム３０１は、伝送線１０を介して中継装置１０１に接続された検知装置を備える。中継装置１０１は、通信装置１１１からメッセージを受信すると、受信したメッセージの複製であるミラーメッセージを伝送線１０経由で当該検知装置へ送信する。当該検知装置は、中継装置１０１から受信したミラーメッセージの中継装置１０１における受信時刻に基づいて、検知指標の算出および検知処理を行う。

[0117] また、本開示の実施の形態に係る通信システム３０１では、検知装置として機能する中継装置１０１が伝送線１０に直接接続される構成であるとしたが、これに限定するものではない。

[0118] 図１３は、本開示の実施の形態に係るネットワークの接続トポロジの一例を示す図である。図１３を参照して、検知装置１５１が、通信装置１１１を介して伝送線１０に接続される構成であってもよい。この場合、検知装置１５１は、たとえば、当該通信装置１１１が送受信するメッセージを監視することにより、ネットワーク２０１における異常を検知する。より詳細には、検知装置１５１は、算出部１２、リセット部１３、検知部１４および記憶部１５を備える。検知装置１５１における算出部１２は、通信装置１１１が受信する対象メッセージＭの受信時刻ｔを取得し、取得した受信時刻ｔに基づいて統計値Ｔを算出する。

[0119] また、本開示の実施の形態に係る中継装置１０１では、算出部１２は、受

信間隔ｘの統計値Ｔを算出する構成であるとしたが、これに限定するものではない。算出部１２は、たとえば、定期的または不定期に、対象メッセージＭの通信負荷を算出し、受信間隔ｘの代わりに当該通信負荷に基づいて、統計値Ｔ等の検知指標を算出する構成であってもよい。通信負荷は、メッセージの観測結果の一例である。

[0120] また、本開示の実施の形態に係る中継装置１０１では、算出部１２は、式（１）に従って異常度Ｄｍを算出する構成であるとしたが、これに限定するものではない。たとえば、算出部１２は、受信間隔ｘｍが以下の式（３）を満たす場合、式（１）に従って異常度Ｄｍを算出する一方で、受信間隔ｘｍが以下の式（４）を満たす場合、以下の式（５）に従って異常度Ｄｍを決定する。

[数3]

$$(xm-\mu)^2 < (n\sigma)^2 \cdots (3)$$

[数4]

$$(xm-\mu)^2 \geq (n\sigma)^2 \cdots (4)$$

[数5]

$$Dm = n^2 \cdots (5)$$

[0121] ここで、ｎは、正当な周期メッセージの度数分布に基づいて予め設定される定数である。

[0122] 図１４は、本開示の実施の形態に係る中継装置における算出部により算出される異常度の一例を示す図である。図１４において、横軸は、受信間隔ｘｍと平均値μとの差分の２乗を示し、縦軸は異常度Ｄｍを示している。

[0123] 図１４を参照して、算出部１２が式（１）および式（３）～（５）に従って異常度Ｄｍを算出する構成により、通信処理部１１により受信された正当なイベントメッセージである対象メッセージＭｍの受信間隔ｘｍが平均値μから大きく乖離している場合であっても、対象メッセージＭｍの異常度Ｄｍ

はｎの二乗以下の値となるので、正当なイベントメッセージが到来することによる統計値Ｔの大幅な増加を抑制し、異常な状態が解消された正常状態における異常の誤検知の発生を抑制することができる。

[0124] また、本開示の実施の形態に係る中継装置１０１では、リセット部１３は、統計値Ｔ（ｍ－１）および統計値Ｔｍの２つの統計値Ｔが連続して増加しており、かつ統計値Ｔ（ｍ＋１）および統計値Ｔ（ｍ＋２）の２つの統計値Ｔが連続して減少している場合、統計値Ｔｍは極大値であると判断する構成であるとしたが、これに限定するものではない。リセット部１３は、統計値Ｔ（ｍ－ａ＋１）から統計値Ｔｍまでのａ個の統計値Ｔが連続して増加しており、かつ統計値Ｔ（ｍ＋１）から統計値Ｔ（ｍ＋ｂ）までのｂ個の統計値Ｔが連続して減少している場合、統計値Ｔｍは極大値であると判断する構成であってもよい。ａおよびｂは、２以上の整数である。

[0125] ところで、ネットワークにおける異常をより正しく検知することが可能な技術が望まれる。

[0126] これに対して、本開示の実施の形態に係る中継装置１０１では、算出部１２は、対象メッセージＭの観測結果と、当該観測結果に関する参照情報との関係に応じて増減する検知指標を算出する。検知部１４は、算出部１２により算出された検知指標に基づいて、ネットワーク２０１における異常を検知する検知処理を行う。リセット部１３は、検知指標を監視し、検知指標の極値を検出した場合、検知処理において用いる検知指標をリセットする。ここで、極値とは、極大値または極小値を意味する。

[0127] このように、メッセージの観測結果と当該観測結果に関する参照情報との関係に応じて増減する検知指標に基づいて検知処理を行い、検知指標の極値を検出した場合において検知指標をリセットする構成により、たとえばネットワーク２０１における異常な状態が解消されることにより検知指標の増減傾向が変化した場合において、リセットされた検知指標に基づいて検知処理を行うことができる。これにより、ネットワーク２０１において異常な状態が解消されたことをより早期に検知し、異常な状態が解消された正常状態に

おける異常の誤検知を抑制することができる。したがって、ネットワーク２０１における異常をより正しく検知することができる。

[0128] 上記実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記説明ではなく請求の範囲によって示され、請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

[0129] 上述の実施形態の各処理（各機能）は、１または複数のプロセッサを含む処理回路（Ｃｉｒｃｕｉｔｒｙ）により実現される。上記処理回路は、上記１または複数のプロセッサに加え、１または複数のメモリ、各種アナログ回路、各種デジタル回路が組み合わされた集積回路等で構成されてもよい。上記１または複数のメモリは、上記各処理を上記１または複数のプロセッサに実行させるプログラム（命令）を格納する。上記１または複数のプロセッサは、上記１または複数のメモリから読み出した上記プログラムに従い上記各処理を実行してもよいし、予め上記各処理を実行するように設計された論理回路に従って上記各処理を実行してもよい。上記プロセッサは、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＧＰＵ（Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ）、ＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）、およびＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）等、コンピュータの制御に適合する種々のプロセッサであってよい。なお、物理的に分離した上記複数のプロセッサが互いに協働して上記各処理を実行してもよい。たとえば、物理的に分離した複数のコンピュータのそれぞれに搭載された上記プロセッサがＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ （Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、およびインターネット等のネットワークを介して互いに協働して上記各処理を実行してもよい。上記プログラムは、外部のサーバ装置等から上記ネットワークを介して上記メモリにインストールされても構わないし、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ

Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＤＶＤ－ＲＯＭ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、および半導体メモリ等の記録媒体に格納された状態で流通し、上記記録媒体から上記メモリにインストールされても構わない。

[0130] 以上の説明は、以下に付記する特徴を含む。

［付記１］

周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置であって、

前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出する算出部と、

前記算出部により算出された前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行う検知部と、

前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするリセット部とを備え、

前記算出部は、前記メッセージの受信間隔と、前記受信間隔に関する参照情報との関係に応じて増減する前記検知指標を算出する、検知装置。

[0131] ［付記２］

周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置であって、

処理回路を備え、

前記処理回路は、

前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出し、

算出した前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行い、

前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットする、検知装置。

符号の説明

[0132] １０　伝送線

１１　通信処理部

１２　算出部

１３　リセット部

１４　検知部

１５　記憶部

１６　通信ポート

１０１　中継装置

１１１　通信装置

１５１　検知装置

２０１　ネットワーク

３０１　通信システム

請求の範囲

[請求項1] 周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置であって、

前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出する算出部と、

前記算出部により算出された前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行う検知部と、

前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするリセット部とを備える、検知装置。

[請求項2] 前記参照情報は、前記観測結果に基づいて算出される過去の前記メッセージの受信間隔であり、

前記算出部は、前記観測結果に基づいて算出される前記メッセージの受信間隔と、前記過去のメッセージの受信間隔とを用いて、前記メッセージの受信間隔の移動平均値であって、前記メッセージの受信間隔と前記過去のメッセージの受信間隔との大小関係に応じて増減する前記移動平均値を、前記検知指標として前記メッセージごとに算出する、請求項１に記載の検知装置。

[請求項3] 前記検知部は、前記検知指標が所定のしきい値未満である場合、前記ネットワークにおける異常が発生していると判定し、

前記リセット部は、前記極値として前記検知指標の極小値を検出した場合、前記検知処理において用いる前記検知指標をリセットする、請求項２に記載の検知装置。

[請求項4] 前記参照情報は、前記メッセージの受信間隔の平均値であり、

前記算出部は、前記観測結果に基づいて算出される前記メッセージの受信間隔と、前記平均値と、前記メッセージの受信間隔の標準偏差とを用いて、前記メッセージの受信間隔の統計値であって、前記メッセージの受信間隔と前記平均値との差分の大きさに応じて増減する前

記統計値を、前記検知指標として前記メッセージごとに算出する、請求項１に記載の検知装置。

[請求項5] 前記検知部は、前記検知指標が所定のしきい値よりも大きい場合、前記ネットワークにおける異常が発生していると判定し、

前記リセット部は、前記極値として前記検知指標の極大値を検出した場合、前記検知処理において用いる前記検知指標をリセットする、請求項４に記載の検知装置。

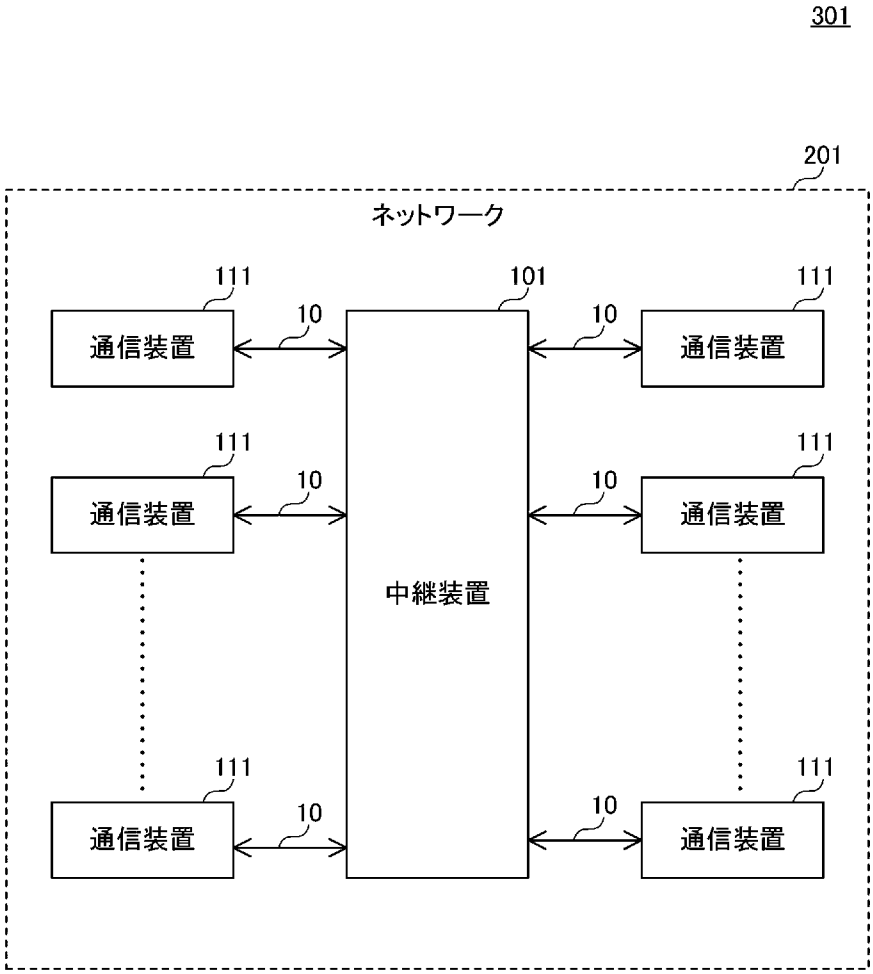
[請求項6] 周期メッセージを含む複数のメッセージが送受信されるネットワークにおける異常を検知する検知装置、における検知方法であって、

前記複数のメッセージの観測結果と、前記観測結果に関する参照情報との関係に応じて増減する検知指標を算出するステップと、

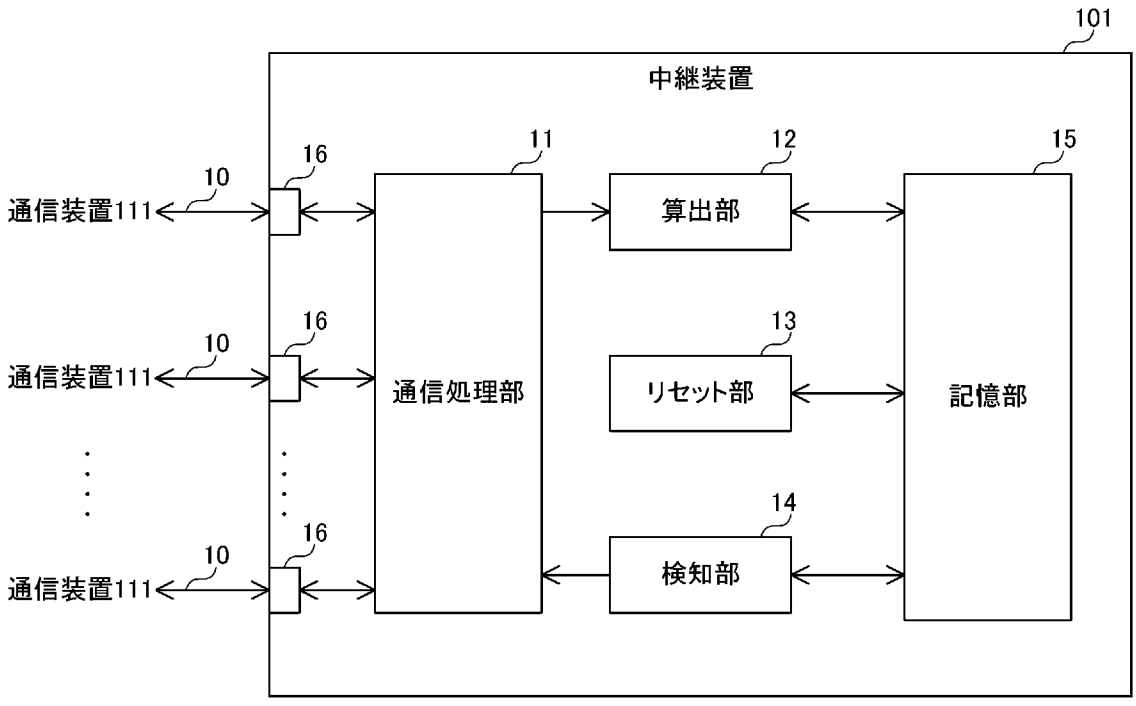
算出した前記検知指標に基づいて、前記ネットワークにおける異常を検知する検知処理を行うステップと、

前記検知指標を監視し、前記検知指標の極値を検出した場合、前記検知処理において用いる前記検知指標をリセットするステップとを含む、検知方法。

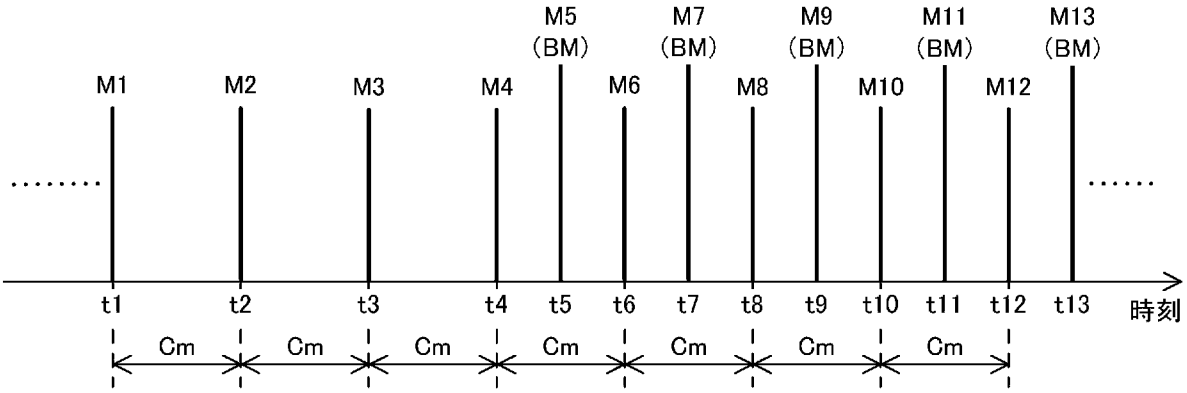
[図1]


301
201
ネットワーク
111
101
111
10
10
通信装置
通信装置
111
111
10
10
通信装置
通信装置
中継装置
111
111
10
10
通信装置
通信装置

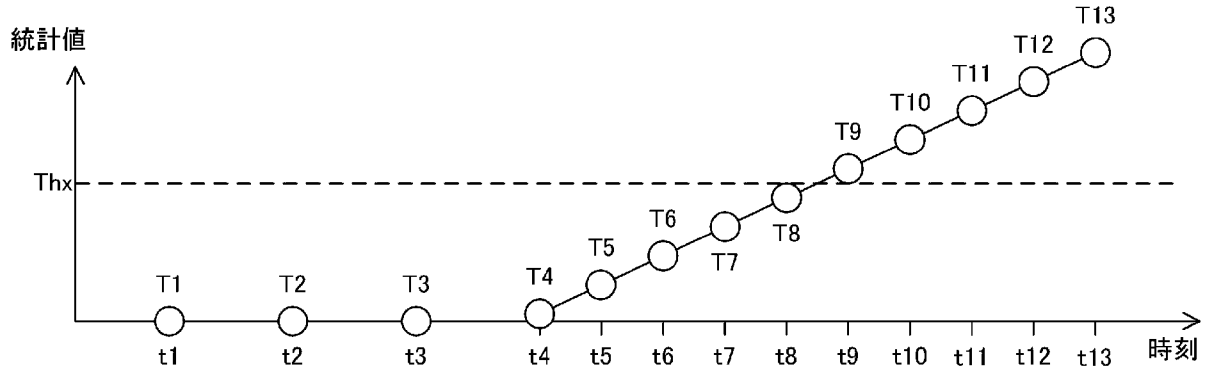
[図2]


101
中継装置
16
11
12
15
10
通信装置111
算出部
16
13
10
通信装置111
通信処理部
リセット部
記憶部
14
16
10
通信装置111
検知部

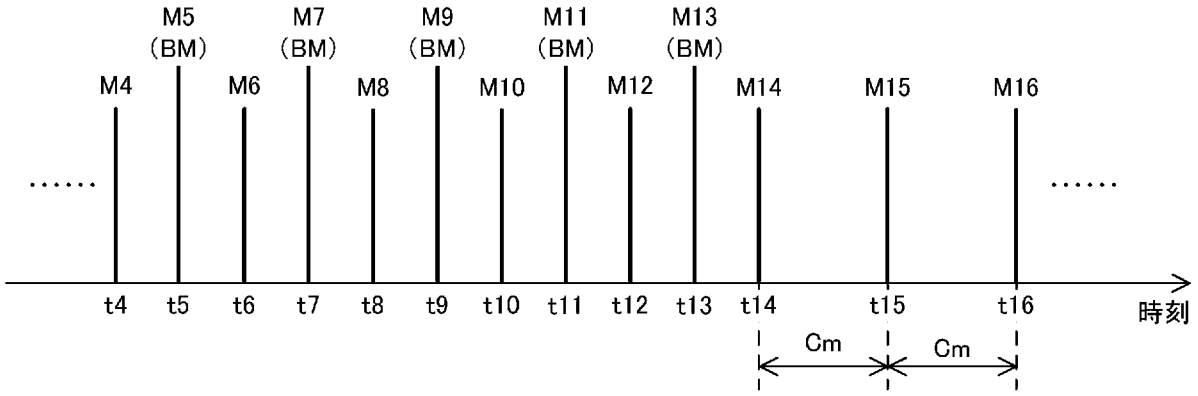
[図3]


M1
M2
M3
M4
M5
(BM)
M6
M7
(BM)
M8
M9
(BM)
M10
M11
(BM)
M12
M13
(BM)
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
t12
t13
時刻
Cm
Cm
Cm
Cm
Cm
Cm
Cm

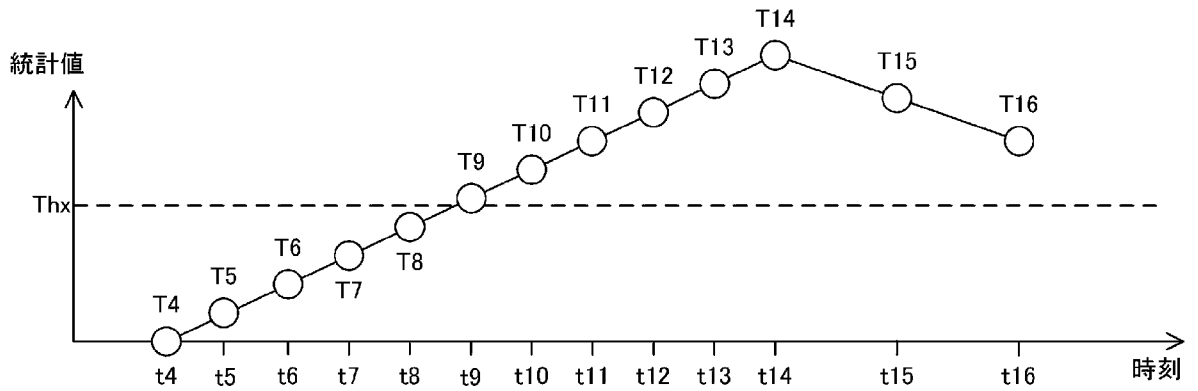
[図4]


統計値
Thx
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
t12
t13
時刻

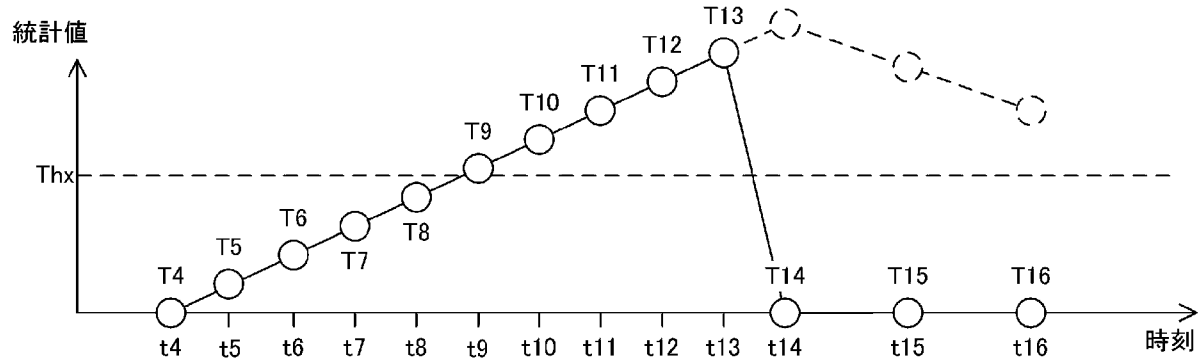
[図5]


M4
M5
(BM)
M6
M7
(BM)
M8
M9
(BM)
M10
M11
(BM)
M12
M13
(BM)
M14
M15
M16
t4
t5
t6
t7
t8
t9
t10
t11
t12
t13
t14
t15
t16
時刻
Cm
Cm

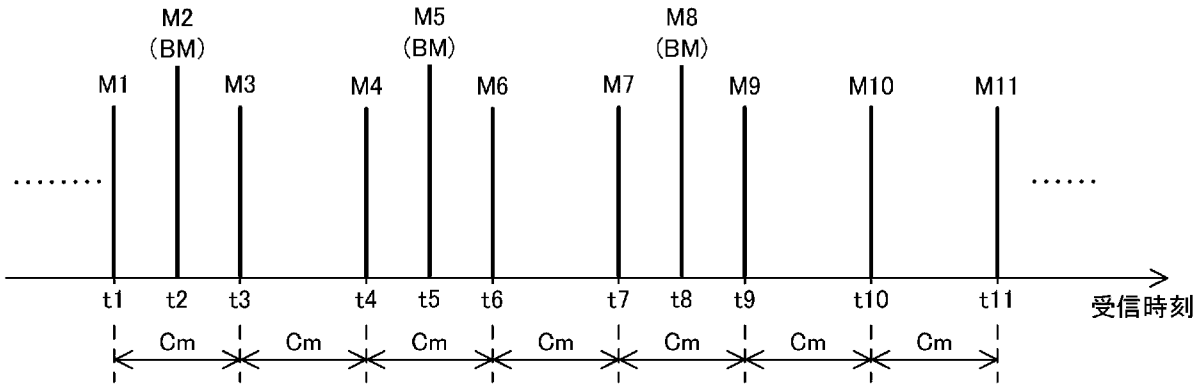
[図6]


統計値
Thx
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
T14
T15
T16
t4
t5
t6
t7
t8
t9
t10
t11
t12
t13
t14
t15
t16
時刻

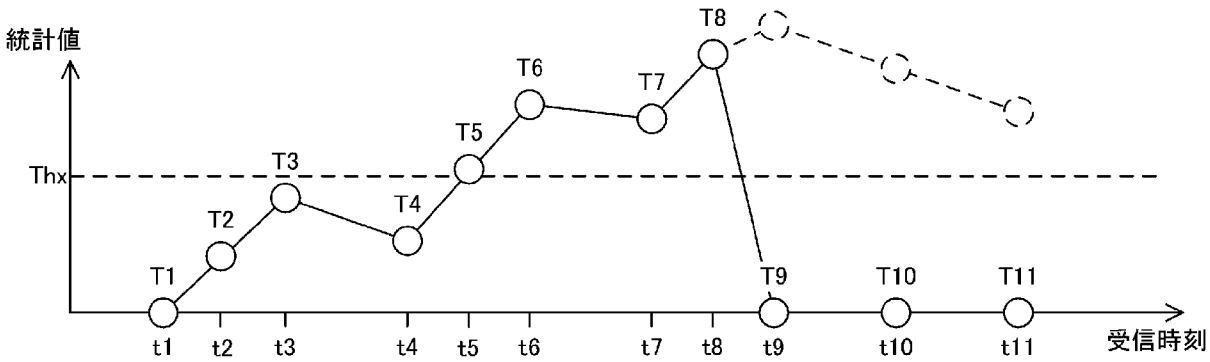
[図7]


統計値
Thx
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
T14
T15
T16
t4
t5
t6
t7
t8
t9
t10
t11
t12
t13
t14
t15
t16
時刻

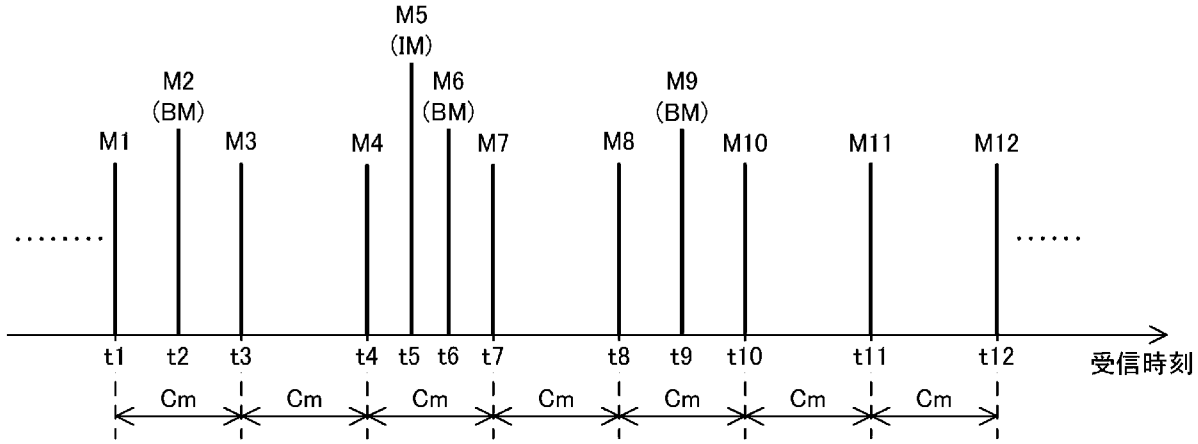
[図8]


M1
M2
(BM)
M3
M4
M5
(BM)
M6
M7
M8
(BM)
M9
M10
M11
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
受信時刻
Cm
Cm
Cm
Cm
Cm
Cm
Cm

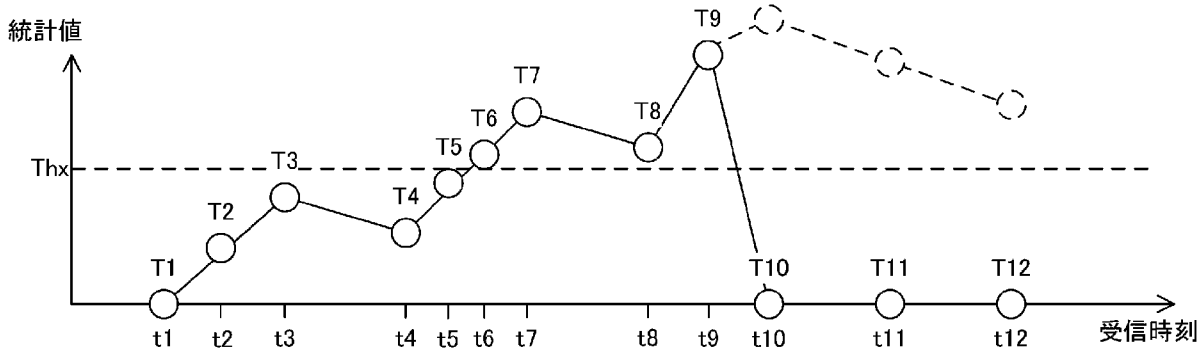
[図9]


統計値
Thx
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
受信時刻

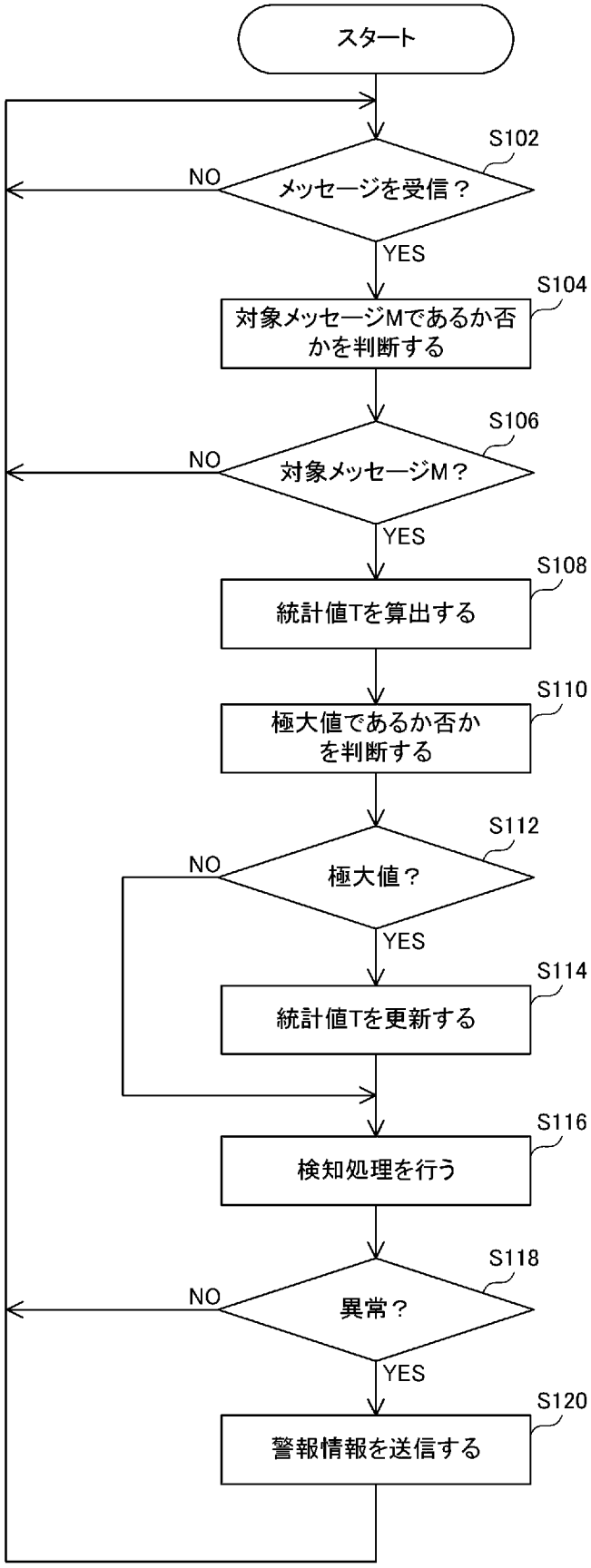
[図10]


M5
(IM)
M2
(BM)
M6
(BM)
M9
(BM)
M1
M3
M4
M7
M8
M10
M11
M12
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
t12
受信時刻
Cm
Cm
Cm
Cm
Cm
Cm
Cm

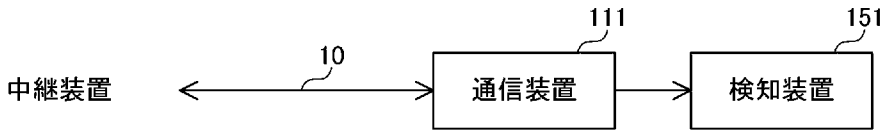
[図11]


統計値
Thx
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10
t11
t12
受信時刻

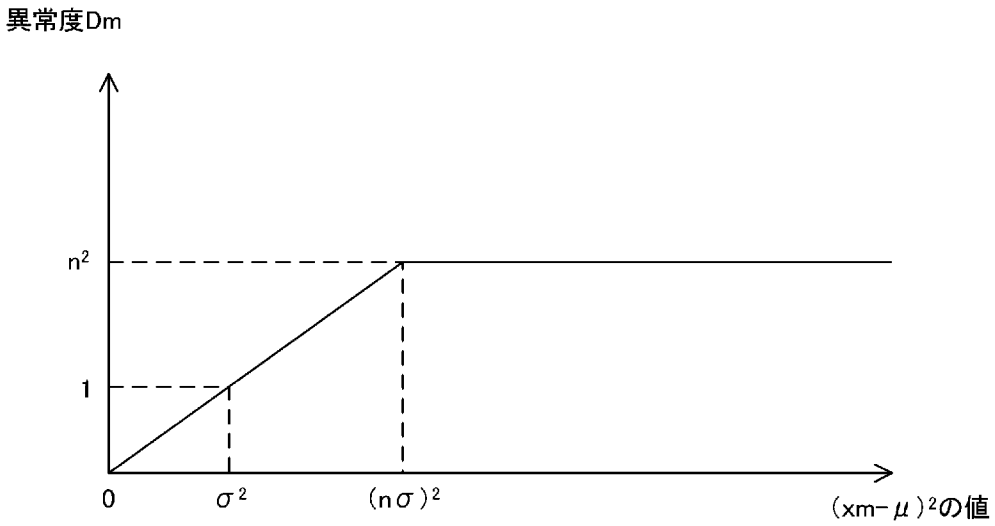
[図12]


スタート
S102
メッセージを受信？
NO
YES
S104
対象メッセージMであるか否かを判断する
S106
対象メッセージM？
NO
YES
S108
統計値Tを算出する
S110
極大値であるか否かを判断する
S112
極大値？
NO
YES
S114
統計値Tを更新する
S116
検知処理を行う
S118
異常？
NO
YES
S120
警報情報を送信する

[図13]



[図14]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/045396

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/28(2006.01)i; ***H04L 43/08***(2022.01)i; ***H04L 43/106***(2022.01)i
FI: H04L12/28 200Z; H04L43/08; H04L43/106

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)

H04L12/28; H04L43/08; H04L43/106

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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	WO 2021/111685 A1 (SUMITOMO ELECTRIC INDUSTRIES, LTD.) 10 June 2021 (2021-06-10) paragraphs [0142]-[0151]	1-6
A	JP 2019-029961 A (SUMITOMO ELECTRIC INDUSTRIES, LTD.) 21 February 2019 (2019-02-21) paragraphs [0319]-[0399]	1-6
A	JP 2014-146868 A (HITACHI AUTOMOTIVE SYSTEMS LTD) 14 August 2014 (2014-08-14) paragraph [0009]	1-6

☐ 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
24 January 2023	**31 January 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/045396

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2021/111685 A1	10 June 2021	(Family: none)	
JP 2019-029961 A	21 February 2019	US 2020/0213340 A1 paragraphs [0362]-[0445] CN 111033504 A	
JP 2014-146868 A	14 August 2014	US 2015/0358351 A1 paragraph [0010] CN 104956626 A	

国際調査報告

国際出願番号
PCT/JP2022/045396

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 12/28(2006.01)i; H04L 43/08(2022.01)i; H04L 43/106(2022.01)i
FI: H04L12/28 200Z; H04L43/08; H04L43/106

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））

H04L12/28; H04L43/08; H04L43/106

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３年

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

C.　関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 2021/111685 A1 (住友電気工業株式会社) 10.06.2021 (2021-06-10) [0142]-[0151]	1-6
A	JP 2019-029961 A (住友電気工業株式会社) 21.02.2019 (2019-02-21) [0319]-[0399]	1-6
A	JP 2014-146868 A (日立オートモティブシステムズ株式会社) 14.08.2014 (2014-08-14) [0009]	1-6

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

*　引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
“O” 口頭による開示、使用、展示等に言及する文献
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、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
24.01.2023	31.01.2023

名称及びあて先

日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）

木村　雅也 5X 3980

電話番号 03-3581-1101 内線 3596

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/045396

引用文献	公表日	パテントファミリー文献	公表日
WO 2021/111685 A1	10.06.2021	（ファミリーなし）	
JP 2019-029961 A	21.02.2019	US 2020/0213340 A1 [0362]-[0445] CN 111033504 A	
JP 2014-146868 A	14.08.2014	US 2015/0358351 A1 [0010] CN 104956626 A	