(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
2024年12月12日(12.12.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/252479 A1

(51) 国際特許分類:
H04L 41/16 (2022.01)

(21) 国際出願番号： PCT/JP2023/020845

(22) 国際出願日： 2023年6月5日(05.06.2023)

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

(72) 発明者: 松尾 洋一(**MATSUO, Yoichi**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

(74) 代理人: 伊東 忠重, 外(**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内ＭＹ ＰＬＡＺＡ （明治安田生命ビル） １６階 Tokyo (JP).

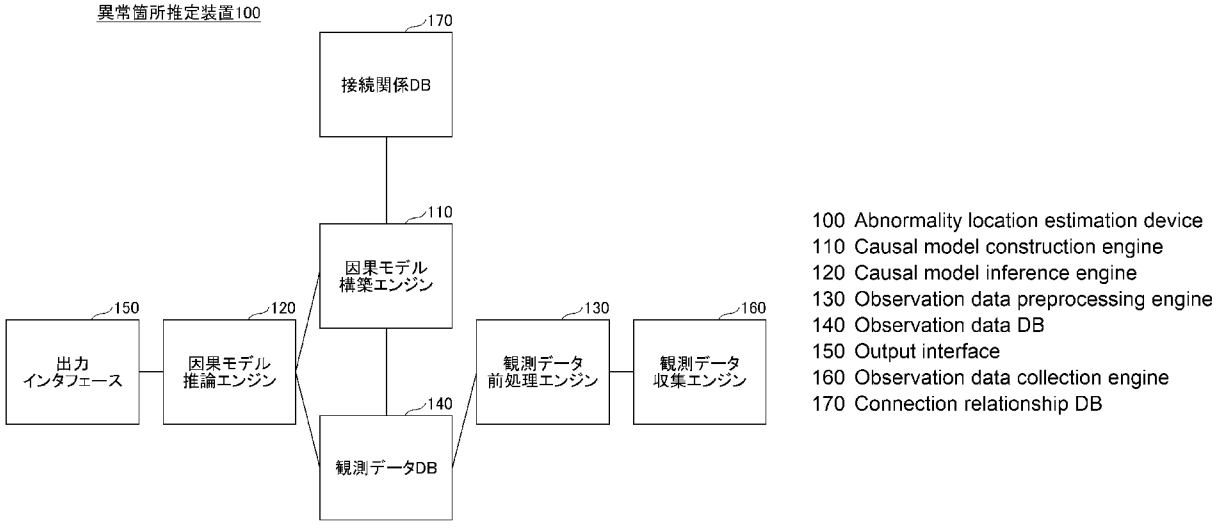
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, SC, SD, SL, ST, SZ, TZ, UG,

(54) **Title:** LOG PROCESSING DEVICE, LOG PROCESSING METHOD, AND PROGRAM

(54) 発明の名称： ログ処理装置、ログ処理方法、及びプログラム

[図1]



(57) **Abstract:** This log processing device comprises a log collection unit that collects logs from a communication network, and a log selection unit that determines a layer to which each log collected by the log collection unit belongs, and selects, on the basis of the layers, a log to be used for failure location estimation using a causal model.

(57) 要約：ログ処理装置において、通信ネットワークからログを収集するログ収集部と、前記ログ収集部により収集された各ログが属するレイヤを判定し、前記レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択するログ選択部とを備える。

［続葉有］

WO 2024/252479 A1

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)）

明　細　書

発明の名称 ： ログ処理装置、ログ処理方法、及びプログラム

技術分野

[0001] 本発明は、通信ネットワークから収集したログに基づいて、通信ネットワークの異常箇所を推定する技術に関連するものである。

背景技術

[0002] 通信事業者にとって、通信ネットワーク内に発生する異常に対して、異常の状態の把握や迅速な対応は重要である。こうした中で、通信ネットワーク内の異常を早期に検知するための研究や、異常箇所の推定を行う研究が行われている（非特許文献１、２）。

[0003] 異常箇所を推定する手法として、ベイジアンネットワークを用いて、異常箇所とそれによって引き起こされる通信ネットワーク内のデータ（観測データと呼ぶ）の変化の関係性をモデル化（因果モデルと呼ぶ）し、異常時の観測データから異常箇所を推定する手法が提案されている（非特許文献３）。

[0004] 例えば、ルータ間で通信ができなくなると対向ルータと通信できなくなったことを表すログが生成されるため、非特許文献３では、ルータの異常は、異常状態になったルータと物理的に隣接しているルータの観測データのみに影響があるという仮定をもとに、通信ネットワーク内の機器に対して、各機器の状態を表す機器ノードと、その機器からリンクダウンに関するログが発生したかどうかを表す観測ノードからなる因果モデルを構築し、異常箇所の判定を行っている。

[0005] また、非特許文献４では、通信ネットワーク内の様々な異常に対して、異常箇所推定を行えるように、物理的な対向装置のリンクダウン以外にも様々なログを用いている。例えば、ルータなどの機器からは、ＣＰＵやメモリ、インタフェースモジュールなどの機器の状態（機器レイヤと呼ぶ）を表すログ、物理的に接続している対向装置とのインタフェースの接続などの状態（物理レイヤと呼ぶ）を表すログ、及び、論理的に接続している機器の状態（

論理レイヤと呼ぶ）を表すログなど、異常になったレイヤごとに異なったログが出力される。これらを用いて、異常パターン、あるいは生成されるログの原因となりえる事象ごとにオペレーターの知識を用いて因果モデルを作成し、異常箇所の推定を行う。

先行技術文献

非特許文献

[0006] 非特許文献1：K. Tajiri, T. Iwata, Y. Matsuo and K. Watanabe, "Fault Detection of ICT systems with Deep Learning Model for Missing Data," 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021, pp. 445-451.

非特許文献2：Y. Matsuo, Y. Nakano, A. Watanabe, K. Watanabe, K. Ishibashi, and K. Kawahara, "Root-cause diagnosis for rare failures using Bayesian network with dynamic modification," Proc. IEEE, ICC, 2018.

非特許文献3：Srikanth Kandula, Dina Katabi, and Jean-philippe Vasseur. Shrink: A tool for failure diagnosis in IP networks. Proceedings of the 2005 ACM SIGCOMM workshop on Mining network data, pages 173-178, 2005.

非特許文献4：He Yan, Lee Breslau, Zihui Ge, Dan Massey, Dan Pei, and Jennifer Yates, " G-RCA: A Generic Root Cause Analysis Platform for Service Quality Management in Large IP Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 6, DECEMBER 2012

発明の概要

発明が解決しようとする課題

[0007] 非特許文献４に開示された技術では、使用するログの種類が増えるため、非特許文献３に開示された技術で発見できる異常箇所よりも多くの異常に対して異常箇所の推定が行える。しかし、事前に異常パターン、あるいは生成されるログの原因となりえる事象ごとにオペレーターの知識を用いて因果モ

デルを作成する必要があるという課題がある。

[0008] また、非特許文献３に開示された技術では、ルータの異常は、異常状態になったルータと物理的に隣接しているルータの観測データのみに影響があるという仮定をもとに因果モデルを作成しているため、接続関係の情報があれば因果モデルを構築できる。

[0009] しかし、非特許文献３において、使用するログが物理レイヤのリンクダウンに関するログである。そのため、物理レイヤの故障において、故障により疎通ができなくなるため、故障が発生したルータとその隣接しているルータの両方のルータからリンクダウンのログが生成される、あるいは、論理レイヤの故障において、物理的には対向ではないが論理的に接続している機器からリンクダウンのログが出る。従って、異常箇所が推定できない場合があるという課題がある。

[0010] 例えば、ルータ内のパケットを処理するチップが故障した場合、他のルータと疎通不可になるので、故障が発生した機器、故障した機器と物理的に接続している機器、故障した機器と論理的に接続している機器など、様々な機器からリンクダウンのログが出る。そのため、結果として異常箇所の推定精度が下がるという課題がある。

[0011] 本発明は上記の点に鑑みてなされたものであり、通信ネットワーク内の異常箇所の推定精度を向上させるための技術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

[0012] 開示の技術によれば、通信ネットワークからログを収集するログ収集部と、

前記ログ収集部により収集された各ログが属するレイヤを判定し、前記レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択するログ選択部と

を備えるログ処理装置が提供される。

発明の効果

[0013] 開示の技術によれば、通信ネットワーク内の異常箇所の推定精度を向上さ

せるための技術が提供される。

図面の簡単な説明

[0014] [図1]異常箇所推定装置１００の構成例を示す図である。

[図2]ログ処理装置２００の構成例を示す図である。

[図3]装置のハードウェア構成例を示す図である。

[図4]通信ネットワークの例を示す図である。

[図5]図４に基づく因果モデルの例を示す図である。

[図6]論理レイヤにおける接続関係の例を示す図である。

[図7]図６に基づく因果モデルの例を示す図である。

発明を実施するための形態

[0015] 以下、図面を参照して本発明の実施の形態（本実施の形態）を説明する。以下で説明する実施の形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施の形態に限られるわけではない。

[0016] 本実施の形態では、後述する異常箇所推定装置１００が、収集するログのレイヤを考慮して、因果モデルの構築と観測ノードを定義することで、機器の接続関係のみから因果モデルを構築し、かつ、様々な異常に対して異常箇所の推定を行うことができる。以下、課題を解決するための装置構成、及び装置動作を詳細に説明する。

[0017] （装置構成例）

図１に、本実施の形態における異常箇所推定装置１００の構成例を示す。図１に示すように、異常箇所推定装置１００は、観測データ収集エンジン１６０、観測データＤＢ１４０、観測データ前処理エンジン１３０、接続関係ＤＢ１７０、因果モデル構築エンジン１１０、因果モデル推論エンジン１２０、利用者への出力インタフェース１５０を有する。

[0018] なお、観測データ収集エンジン１６０、観測データ前処理エンジン１３０、因果モデル構築エンジン１１０、因果モデル推論エンジン１２０をそれぞれ、観測データ収集部１６０、観測データ前処理部１３０、因果モデル構築部１１０、因果モデル推論部１２０と呼んでもよい。また、観測データ収集

エンジン１６０、観測データ前処理エンジン１３０、因果モデル構築エンジン１１０、因果モデル推論エンジン１２０をそれぞれ、観測データ収集回路１６０、観測データ前処理回路１３０、因果モデル構築回路１１０、因果モデル推論回路１２０と呼んでもよい。

[0019] また、異常箇所推定装置１００をログ処理装置と呼んでもよい。また、観測データ収集エンジン１６０、観測データ前処理エンジン１３０をそれぞれ、ログ収集部、ログ選択部と呼んでもよい。異常箇所推定装置１００の動作概要は下記のとおりである。

[0020] 観測データ収集エンジン１６０は、通信ネットワークから観測データ（機器から発生するログ等）を収集する。観測データ前処理エンジン１３０は、観測データ収集エンジン１６０により収集されたログが属するレイヤを判定し、最も低レイヤのログのみを抽出し、抽出したログを観測データＤＢ１４０に格納する。

[0021] 因果モデル構築エンジン１１０は、観測データＤＢ１４０に格納されたログが属するレイヤに応じて、接続関係ＤＢ１７０に保存されている物理的あるいは論理的なノードの接続関係を入力とし、因果モデルを構築する。因果モデル推論エンジン１２０は観測データＤＢ１４０へ格納されたログの発生状況をもとに、観測ノードの値を決定し、異常箇所の推定を実施し、出力インタフェース１５０に推定結果である異常箇所を出力する。

[0022] 出力インタフェース１５０は、利用者に対して通信ネットワークの中の異常発生箇所とその際の最大事後確率等を表示する。また、出力インタフェース１５０は、運用システムに新たにマシンが追加された際などは、因果グラフへのノードの追加を行い、また、それに伴う因果関係の変化を利用者に修正させることもできる。

[0023] なお、異常箇所推定装置１００は、１つの装置（コンピュータ）であってもよいし、複数の装置からなるものであってもよい。

[0024] また、観測データ収集エンジン１６０と観測データ前処理エンジン１３０により１つの装置を構成し、それをログ処理装置と呼んでよい。

[0025] 図２にログ処理装置２００の構成例を示す。図２に示すように、ログ収集装置２００は、ログ収集部２１０、及びログ選択部２２０を含む。ログ収集部２１０とログ選択部２２０はそれぞれ観測データ収集エンジン１６０と観測データ前処理エンジン１３０に対応する。ログ収集装置２００は、因果モデル構築エンジン１１０等を更に含んでもよい。

[0026] ログ収集部２１０は、通信ネットワークからログを収集する。ログ選択部２２０は、ログ収集部２１０により収集された各ログが属するレイヤを判定し、当該レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択する。例えば、ログ選択部２２０は、判定された１つ以上のレイヤのうち、最も低いレイヤのログのみを、因果モデルを用いた障害箇所推定のために使用するログとして選択する。

[0027] （ハードウェア構成例）

本明細書に記載したいずれの装置（異常箇所推定装置１００、ログ処理装置２００）も、例えば、コンピュータにプログラムを実行させることにより実現できる。このコンピュータは、物理的なコンピュータであってもよいし、クラウド上の仮想マシンであってもよい。

[0028] すなわち、当該装置は、コンピュータに内蔵されるＣＰＵやメモリ等のハードウェア資源を用いて、当該装置で実施される処理に対応するプログラムを実行することによって実現することが可能である。上記プログラムは、コンピュータが読み取り可能な記録媒体（可搬メモリ等）に記録して、保存したり、配布したりすることが可能である。また、上記プログラムをインターネットや電子メール等、ネットワークを通して提供することも可能である。

[0029] 図３は、上記コンピュータのハードウェア構成例を示す図である。図３のコンピュータは、それぞれバスＢＳで相互に接続されているドライブ装置１０００、補助記憶装置１００２、メモリ装置１００３、ＣＰＵ１００４、インタフェース装置１００５、表示装置１００６、入力装置１００７、出力装置１００８等を有する。

[0030] 当該コンピュータでの処理を実現するプログラムは、例えば、ＣＤ－ＲＯ

Ｍ又はメモリカード等の記録媒体１００１によって提供される。プログラムを記憶した記録媒体１００１がドライブ装置１０００にセットされると、プログラムが記録媒体１００１からドライブ装置１０００を介して補助記憶装置１００２にインストールされる。但し、プログラムのインストールは必ずしも記録媒体１００１より行う必要はなく、ネットワークを介して他のコンピュータよりダウンロードするようにしてもよい。補助記憶装置１００２は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

[0031] メモリ装置１００３は、プログラムの起動指示があった場合に、補助記憶装置１００２からプログラムを読み出して格納する。ＣＰＵ１００４は、メモリ装置１００３に格納されたプログラムに従って、当該装置に係る機能を実現する。インタフェース装置１００５は、ネットワークに接続するためのインタフェースとして用いられる。表示装置１００６はプログラムによるＧＵＩ（Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）等を表示する。入力装置１００７はキーボード及びマウス、ボタン、又はタッチパネル等で構成され、様々な操作指示を入力させるために用いられる。出力装置１００８は演算結果を出力する。

[0032] （動作例）

以下では、異常箇所推定装置１００の動作を、より詳細に説明する。なお、本実施の形態では、ルータにより構成される通信ネットワークを対象とすることを想定しているが、これは一例である。本発明に係る技術は、通信ネットワークを構成するノードの種類に依らずに適用可能である。

[0033] ＜因果モデルについて＞

本発明に係る技術に係る前処理について説明する前に、まず、非特許文献３に基づく、因果モデルの構築について説明する。

[0034] 図４に、観測データ収集エンジン１６０が観測データを収集する対象となる通信ネットワークの例を示す。これは、物理レイヤの接続関係に相当する。図４に示すように、この通信ネットワークは、ルータ１～６が図示すると

おりに接続されたネットワークである。例えば、ルータ１とルータ２は直接に接続されたおり、これらは互いに隣接関係にある。ルータ１とルータ４は直接には接続されておらず、これらは隣接関係にない。

[0035] 因果モデル構築エンジン１１０は、エキスパートオペレーターの知識等に基づいて、図４に示す通信ネットワーク（物理レイヤのネットワーク）に対して、図５に示す因果モデルを構築する。因果モデルは、通信ネットワーク内の機器（ルータ）に対して、各機器の状態を表す機器ノードと、その機器からログ（例：リンクダウンに関するｓｙｓｌｏｇ）が発生したかどうかを表す観測ノードからなる。つまり、観測ノードは、各機器の観測結果を表す。なお、因果モデルをベイジアンネットワークと呼んでもよい。

[0036] 例えば、図５の因果モデルにおいて、機器ノードのルータ１は、観測ノードのルータ１、２と接続されている。これは、ルータ１に異常が発生した場合に、ルータ１の観測データとルータ２の観測データに影響する可能性があるということを示している。

[0037] また、例えば、図５の因果モデルにおいて、機器ノードのルータ２は、観測ノードのルータ１、２、３、６と接続されている。これは、ルータ２に異常が発生した場合に、ルータ１、２、３、６のそれぞれの観測データに影響する可能性があるということを示している。

[0038] ＜観測データ前処理エンジン１３０についての詳細説明＞

本実施の形態において、観測データ前処理エンジン１３０は、観測データ収集エンジン１６０により収集されたログのレイヤを考慮して、収集されたログの中から、因果モデルを用いた異常箇所推定に使用するログを選択し、選択したログを観測データＤＢ１４０に格納する。前述のとおり、最も低いレイヤのログのみを抽出し、抽出したログを観測データＤＢ１４０に格納する。

[0039] なお、観測データ前処理エンジン１３０が選択するログは、最も低いレイヤのログに限定されるわけではない。例えば、観測データ前処理エンジン１３０は、複数レイヤ（例：最も低いレイヤと２番目に低いレイヤ）のログを

選択する場合があってもよい。

[0040] また、本実施の形態では、一般的なレイヤの概念と同様に、「物理」から「論理」へ、レイヤが高くなることを想定している。また、本実施の形態では、「機器」のほうが「物理」よりもレイヤが低いこととしている。ただし、レイヤの高／低の定義は任意に定めてよい。観測データ前処理エンジン１３０の具体的処理内容は下記のとおりである。

[0041] 通信ネットワーク内の異常において、機器レイヤの異常に関するログが発生した場合、他の機器と疎通ができなくなるため、物理レイヤ、論理レイヤのログも発生するが、機器レイヤのログが大元のログであるため、異常箇所推定装置１００は、物理レイヤのログ、論理レイヤのログを使用せず機器レイヤのログだけを使用して、異常箇所を判定する。つまり、観測データ前処理エンジン１３０は、機器レイヤのログ、物理レイヤのログ、論理レイヤのログのうち、最もレイヤの低い機器レイヤのログのみを抽出し、観測データＤＢ１４０に格納する。

[0042] また、機器レイヤの異常に関するログが発生せずに、物理レイヤの異常に関するログが発生した場合も、他の機器と疎通ができなくなるため論理レイヤのログも出るが、物理レイヤのログが大元のログであるため、異常箇所推定装置１００は、論理レイヤのログを使用せず、物理レイヤのログだけを使用し、異常箇所を判定する。つまり、観測データ前処理エンジン１３０は、物理レイヤのログ、及び論理レイヤのログのうち、最もレイヤの低い物理レイヤのログのみを抽出し、観測データＤＢ１４０に格納する。

[0043] また、機器レイヤの異常に関するログ及び物理レイヤの異常に関するログのいずれも発生せずに、論理レイヤの異常に関するログが発生した場合は、異常箇所推定装置１００は、論理レイヤのログを用いて異常箇所を判定する。つまり、観測データ前処理エンジン１３０は、論理レイヤのログのみを観測データＤＢ１４０に格納する。

[0044] ここで、各ログがどのレイヤに属するかは、オペレーターの知識をもとに一つ一つ決めることとしてもよいし、ログとそのログがどのレイヤに属する

かのデータのペアを用意し機械学習モデルなどを用いて学習し、各ログを該当レイヤに分類しても良い。

[0045] 各ログがどのレイヤに属するかを、オペレーターの知識をもとに一つ一つ決めておく場合においては、例えば、観測データ前処理エンジン１３０は、ログの種類とレイヤとを対応付けたテーブルを保持し、当該テーブルを参照することで、新たなログのレイヤを判断する。

[0046] また、機械学習モデルを使用する場合には、例えば、観測データ前処理エンジン１３０は、ログとそのログが属するレイヤとの関係を学習した学習済みのモデルを保持し、当該モデルにログを入力することで、当該モデルからの出力として当該ログのレイヤを得ることができる。

[0047] ＜因果モデル構築エンジン１１０についての詳細説明＞

観測データ前処理エンジン１３０によるログ選択の次に、因果モデル構築エンジン１１０が、使用するログに基づいて因果モデルを構築する。使用するログが機器レイヤのログ、又は、物理レイヤのログである場合は非特許文献３と同様に、物理的な接続関係をもとに因果モデルを構築する。

[0048] この場合の因果モデル構築方法は、図４、図５を参照して説明したとおりであり、使用するログが機器レイヤのログである場合、及び、物理レイヤのログである場合のいずれの場合にも、例えば図５に示すような因果モデルが構築される。なお、ここでは、使用するログが機器レイヤのログである場合の因果モデルと、使用するログが物理レイヤのログである場合の因果モデルとが同じである例を想定しているが、これらが異なる場合もある。

[0049] 使用するログが論理レイヤのログである場合には、因果モデル構築エンジン１１０は、接続関係ＤＢ１７０から読み出した、論理レイヤにおける接続関係をもとに、因果モデルを構築する。

[0050] 上記の方法により、接続関係のみから因果モデルを構築することができ、かつ機器レイヤの異常から論理レイヤの異常まで、様々な異常箇所を推定できるので、異常箇所推定の精度向上が可能となる。

[0051] 非特許文献３に開示された技術では、機器の接続関係から因果モデルを構

築するため、図５に示すような因果モデルが作成される。

[0052] 一方、本実施の形態においては、物理レイヤの接続関係を用いて因果モデルを構築する場合には、前述のとおり、非特許文献３での因果モデルと同様となるが、論理レイヤの接続関係（論理的な接続関係）を用いて因果モデルを構築する場合には、当該因果モデルは、非特許文献３に開示されたものと異なったものとなる。

[0053] 図６は、本実施の形態に係る通信ネットワークの論理レイヤにおける接続関係の例を示す図である。図６に示すとおり、図４に示した物理レイヤ（あるいは機器レイヤ）の接続関係とは異なり、例えば、ルータ１とルータ３は直接に接続されている。この直接接続は、論理的な直接接続である。

[0054] 図７は、図６に示す論理レイヤにおける接続関係に基づいて構築された因果モデルの例を示す。例えば、図７の因果モデルにおいて、機器ノードのルータ１は、観測ノードのルータ１、３と接続されている。これは、ルータ１に異常が発生した場合に、ルータ１、３のそれぞれの観測データに影響する可能性があるということを示している。なお、この場合の異常は、論理レイヤのログに関連する異常である。

[0055] ＜因果モデル推論エンジン１２０についての詳細説明＞

本実施の形態では、構築した因果モデルに対して、以下のように観測ノードの値を定義する。

[0056] 異常箇所推定の対象となるシステム（通信ネットワーク）の因果モデルにおける機器ノードをx_i、観測ノードをy_i，$i \in$（１，…Ｎ）とする。Ｎは機器数である。

[0057] 各x_iは０（正常状態）か１（異常状態）の値を取るとする。なお、０か１の２値ではなく、３値以上の多値を取ることも可能であり、その場合は最小値が正常状態、最大値が異常状態、その間の値ｃは、「ｃ／（最大値－最小値）」の割合で異常となっていることを意味する値、などのように定義する。

[0058] 各y_iは０か１の値を取るとし、ｉ番目のルータでログが発生したことを表

す。既に説明したとおり、ここで使用するログは、大元になったレイヤのログ（最も低いレイヤのログ）だけとする。なお、０か１の２値ではなく、３値以上の多値を取ることも可能であり、その場合はｉ番目のルータで発生したログの発生件数を値とするなどのように定義する。

[0059] 上記の因果モデルへの入力値については、因果モデル推論エンジン１２０が、観測データＤＢ１４０から読み出したログから決定（計算）することができる。

[0060] 因果モデルを用いた推論自体は非特許文献３での手法と同じであり、事前確率Ｐ（x_i）と条件付き確率Ｐ（$y_j \mid x_i$）を規定し、推論を行う。

[0061] （実施の形態に係る技術の効果について）

上述したとおり、観測データ前処理エンジン１３０が、収集されたログが属するレイヤを判定し、最も低いレイヤのログのみを抽出することとしたので、通信ネットワーク内の異常箇所の推定精度を向上させることができる。

[0062] 以上の実施形態に関し、更に以下の付記を開示する。

[0063] ＜付記＞

（付記項１）

メモリと、

前記メモリに接続された少なくとも１つのプロセッサと、

を含み、

前記プロセッサは、

通信ネットワークからログを収集し、

前記収集された各ログが属するレイヤを判定し、前記レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択する

ログ処理装置。

（付記項２）

前記プロセッサは、判定された１つ以上のレイヤのうち、最も低いレイヤのログのみを、因果モデルを用いた障害箇所推定のために使用するログとして選択する

付記項１に記載のログ処理装置。

（付記項３）

前記プロセッサは、選択されたログが属するレイヤにおけるノード間の接続関係に基づいて、因果モデルを構築する

付記項１又は２に記載のログ処理装置。

（付記項４）

前記プロセッサは、ログとレイヤとの関係を学習済みのモデルを用いて各ログが属するレイヤを判定する

付記項１ないし３のうちいずれか１項に記載のログ処理装置。

（付記項５）

ログ処理装置が実行するログ処理方法であって、

通信ネットワークからログを収集するログ収集ステップと、

前記ログ収集ステップにより収集された各ログが属するレイヤを判定し、前記レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択するログ選択ステップと

を備えるログ処理方法。

（付記項６）

コンピュータを、付記項１ないし４のうちいずれか１項に記載のログ処理装置における各部として機能させるためのプログラムを記憶した非一時的記憶媒体。

[0064] 以上、本実施の形態について説明したが、本発明はかかる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

符号の説明

[0065] １００　異常箇所推定装置

１１０　因果モデル構築エンジン

１２０　因果モデル推論エンジン

１３０　観測データ前処理エンジン

１４０　観測データＤＢ

１５０　出力インタフェース

１６０　観測データ収集エンジン

１７０　接続関係ＤＢ

２００　ログ収集装置

２１０　ログ収集部

２２０　ログ選択部２２０

１０００　ドライブ装置

１００１　記録媒体

１００２　補助記憶装置

１００３　メモリ装置

１００４　ＣＰＵ

１００５　インタフェース装置

１００６　表示装置

１００７　入力装置

１００８　出力装置

請求の範囲

[請求項1] 通信ネットワークからログを収集するログ収集部と、

前記ログ収集部により収集された各ログが属するレイヤを判定し、前記レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択するログ選択部と

を備えるログ処理装置。

[請求項2] 前記ログ選択部は、判定された１つ以上のレイヤのうち、最も低いレイヤのログのみを、因果モデルを用いた障害箇所推定のために使用するログとして選択する

請求項１に記載のログ処理装置。

[請求項3] 前記ログ選択部により選択されたログが属するレイヤにおけるノード間の接続関係に基づいて、因果モデルを構築する因果モデル構築部を更に備える請求項１に記載のログ処理装置。

[請求項4] 前記ログ選択部は、ログとレイヤとの関係を学習済みのモデルを用いて各ログが属するレイヤを判定する

請求項１に記載のログ処理装置。

[請求項5] ログ処理装置が実行するログ処理方法であって、

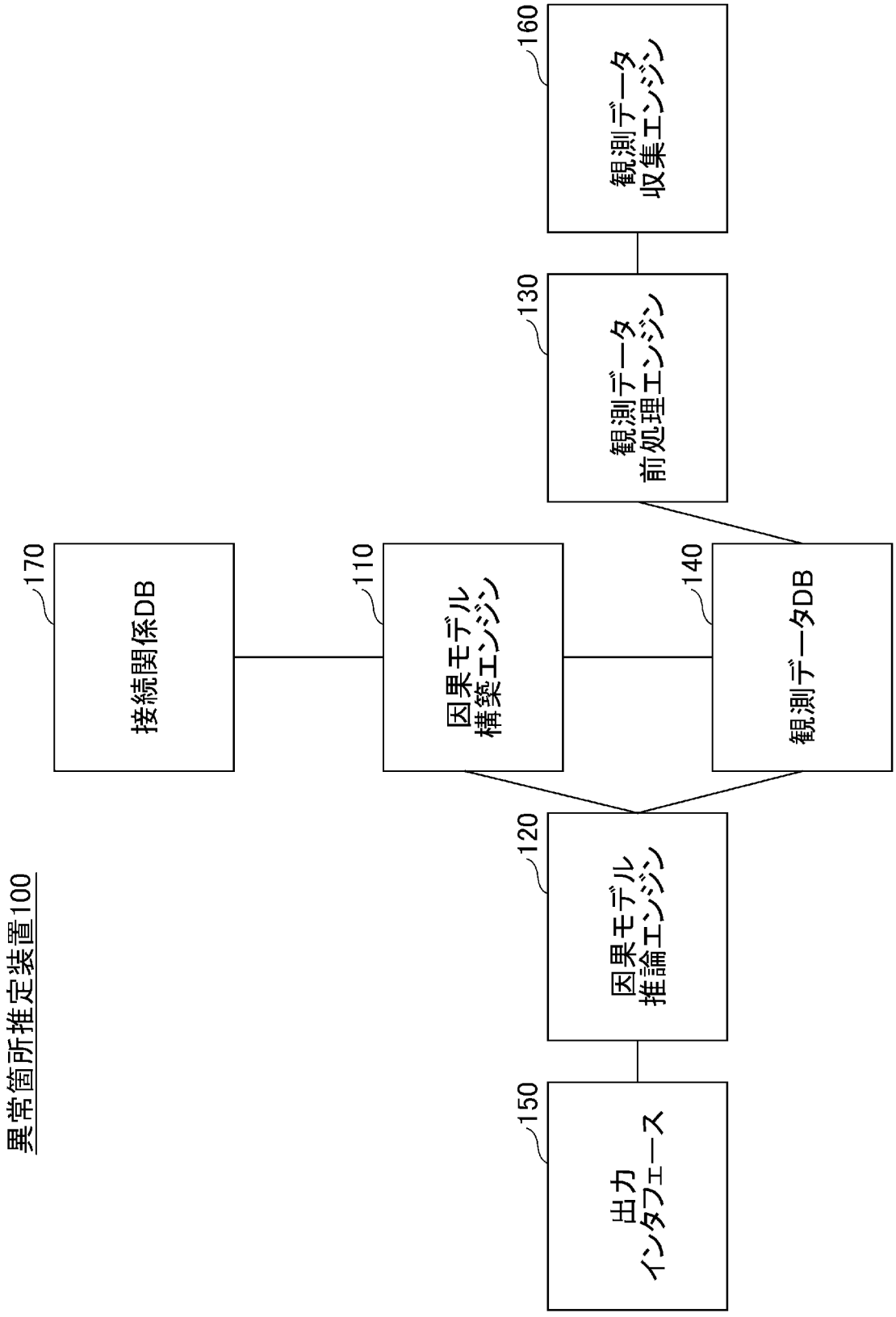
通信ネットワークからログを収集するログ収集ステップと、

前記ログ収集ステップにより収集された各ログが属するレイヤを判定し、前記レイヤに基づいて、因果モデルを用いた障害箇所推定のために使用するログを選択するログ選択ステップと

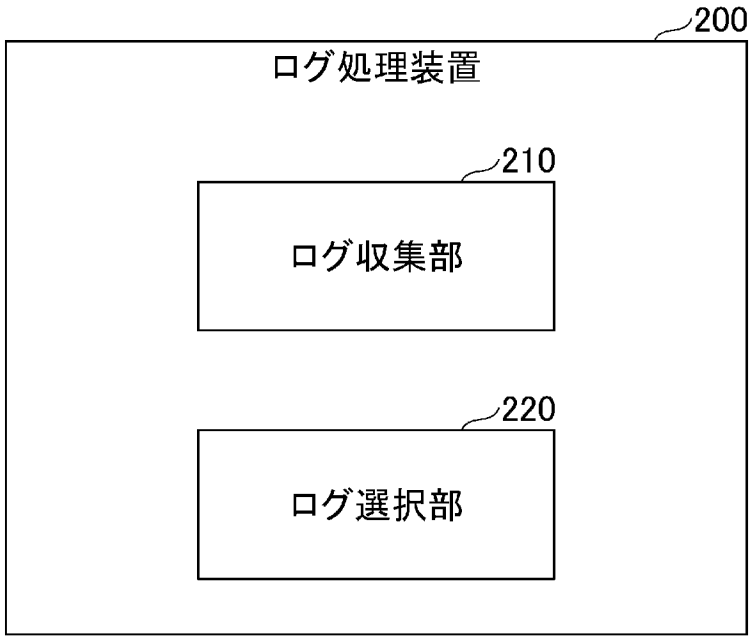
を備えるログ処理方法。

[請求項6] コンピュータを、請求項１ないし４のうちいずれか１項に記載のログ処理装置における各部として機能させるためのプログラム。

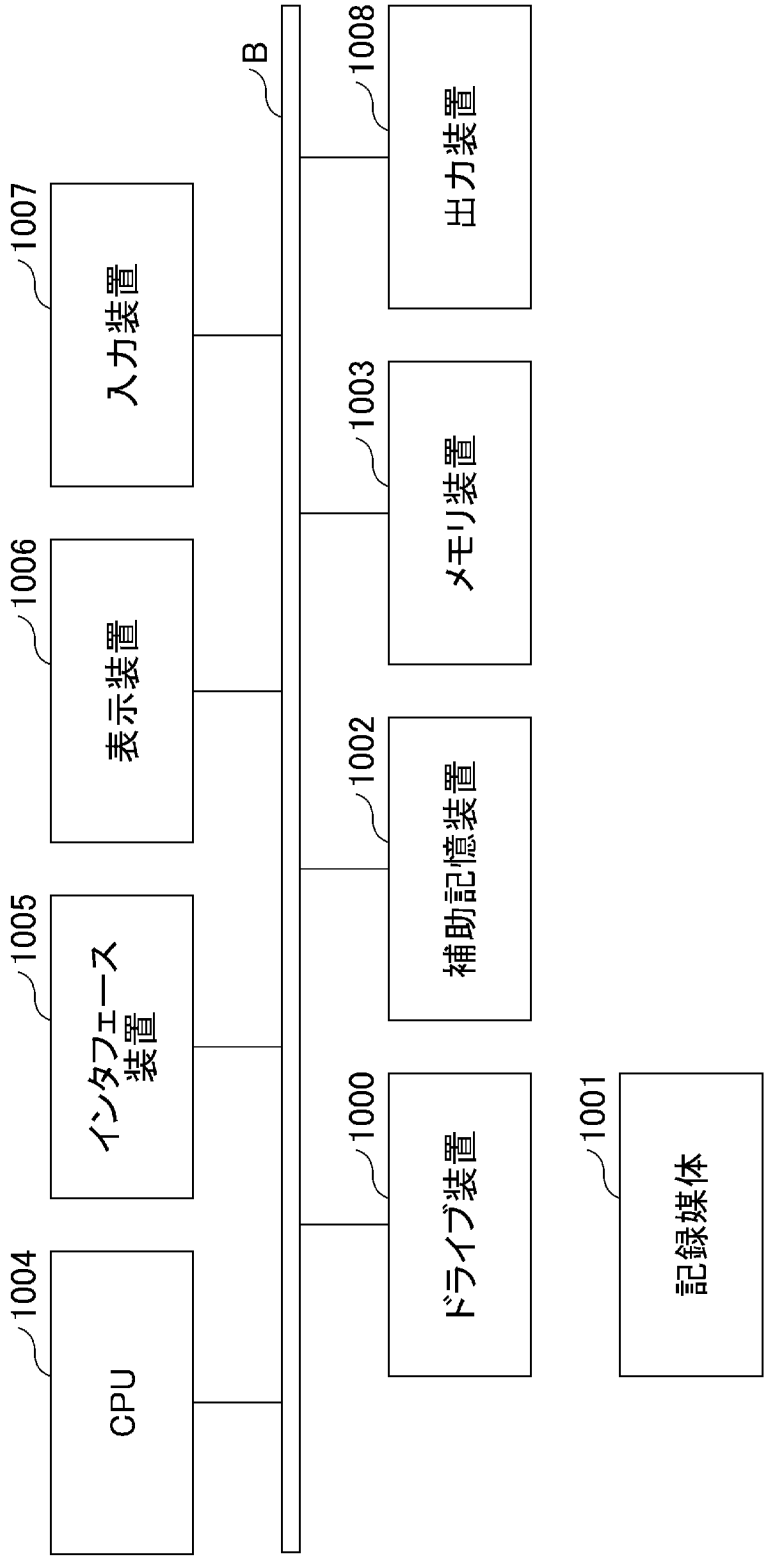
[図1]


異常箇所推定装置100
160
観測データ
収集エンジン
130
観測データ
前処理エンジン
170
接続関係DB
110
因果モデル
構築エンジン
140
観測データDB
120
因果モデル
推論エンジン
150
出力
インタフェース

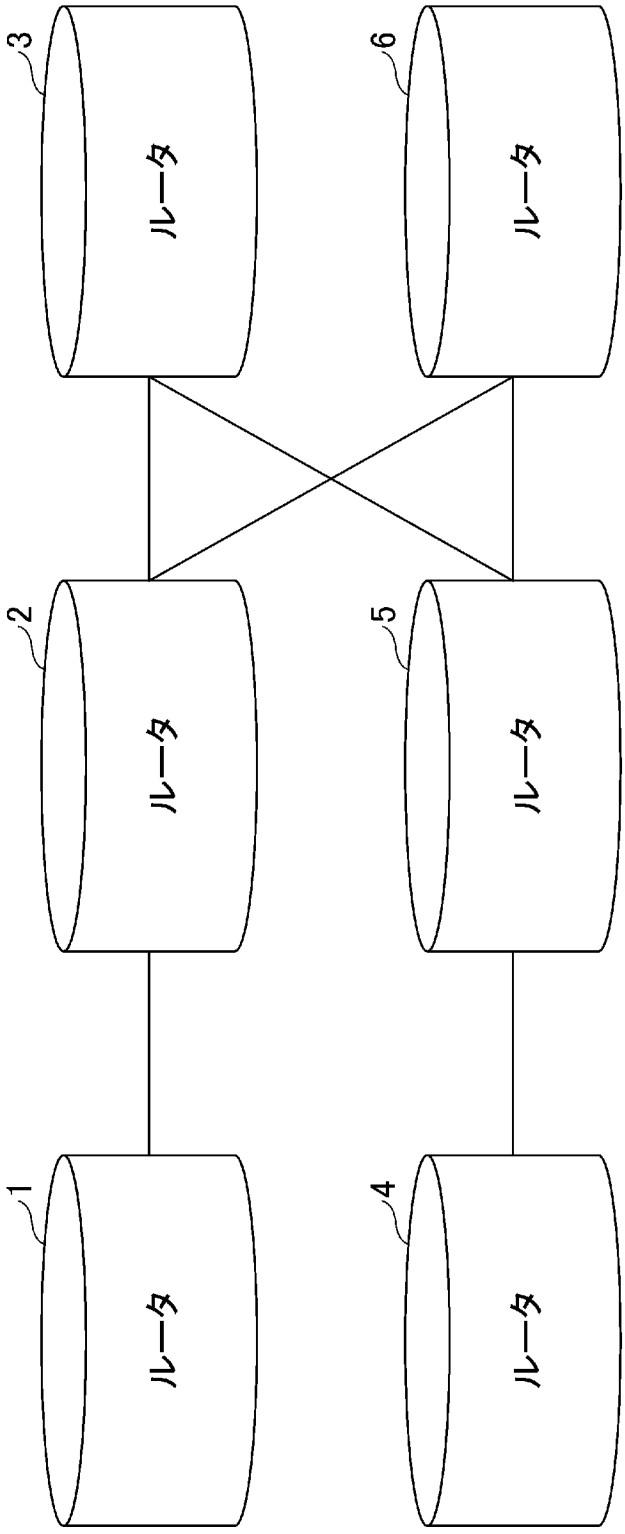
[図2]



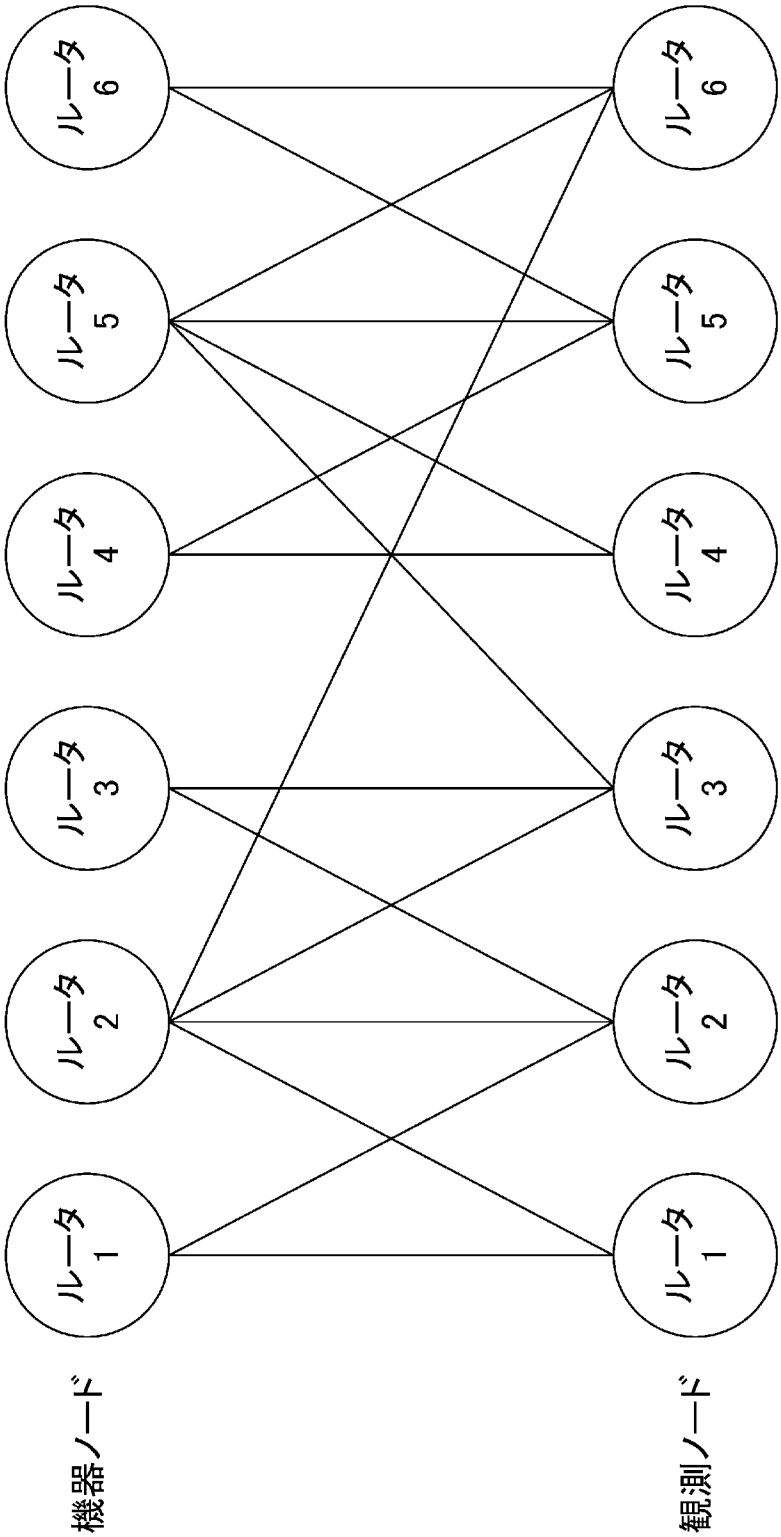
[図3]


B
1004
CPU
1005
インタフェース装置
1006
表示装置
1007
入力装置
1000
ドライブ装置
1002
補助記憶装置
1003
メモリ装置
1008
出力装置
1001
記録媒体

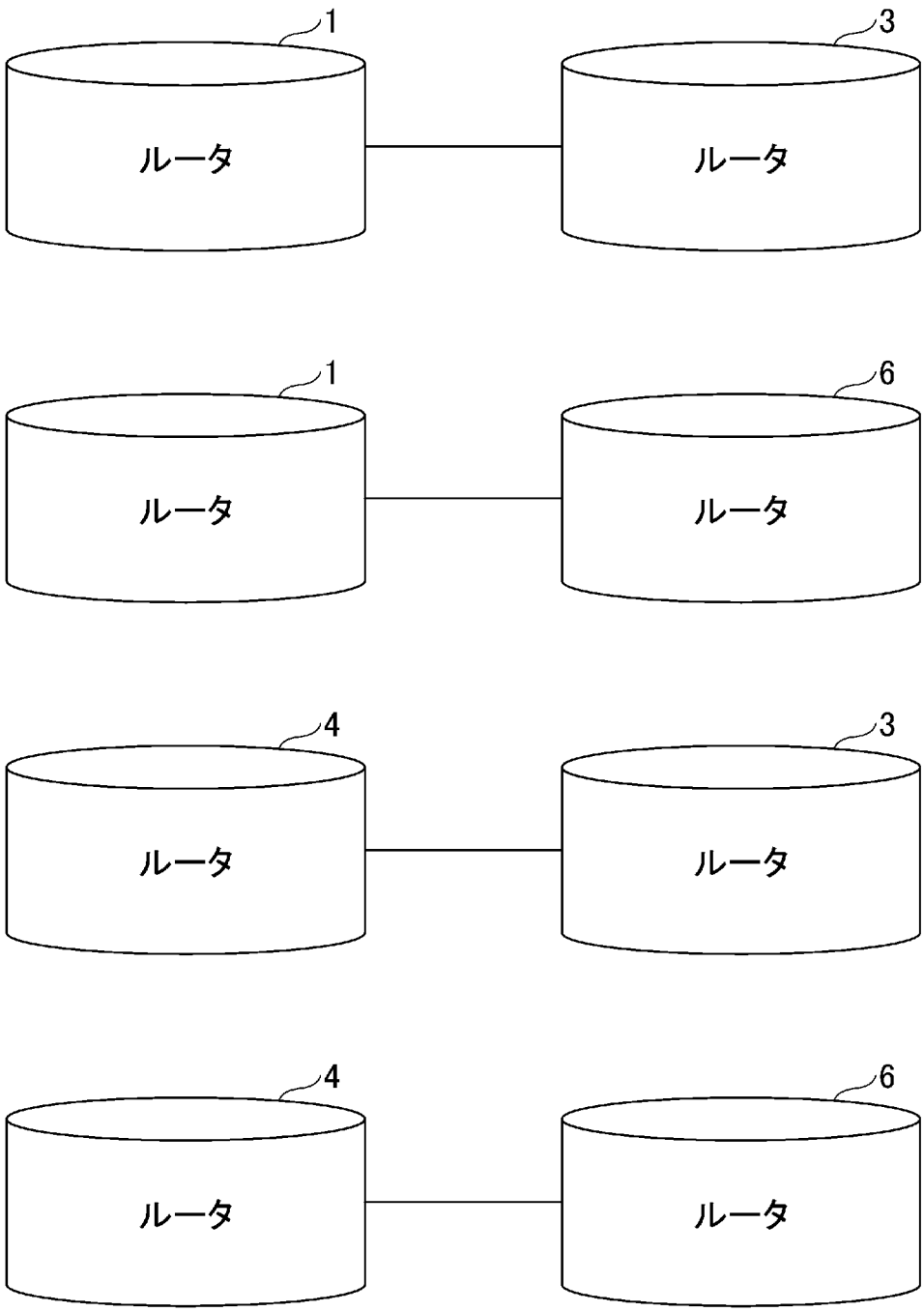
[図4]



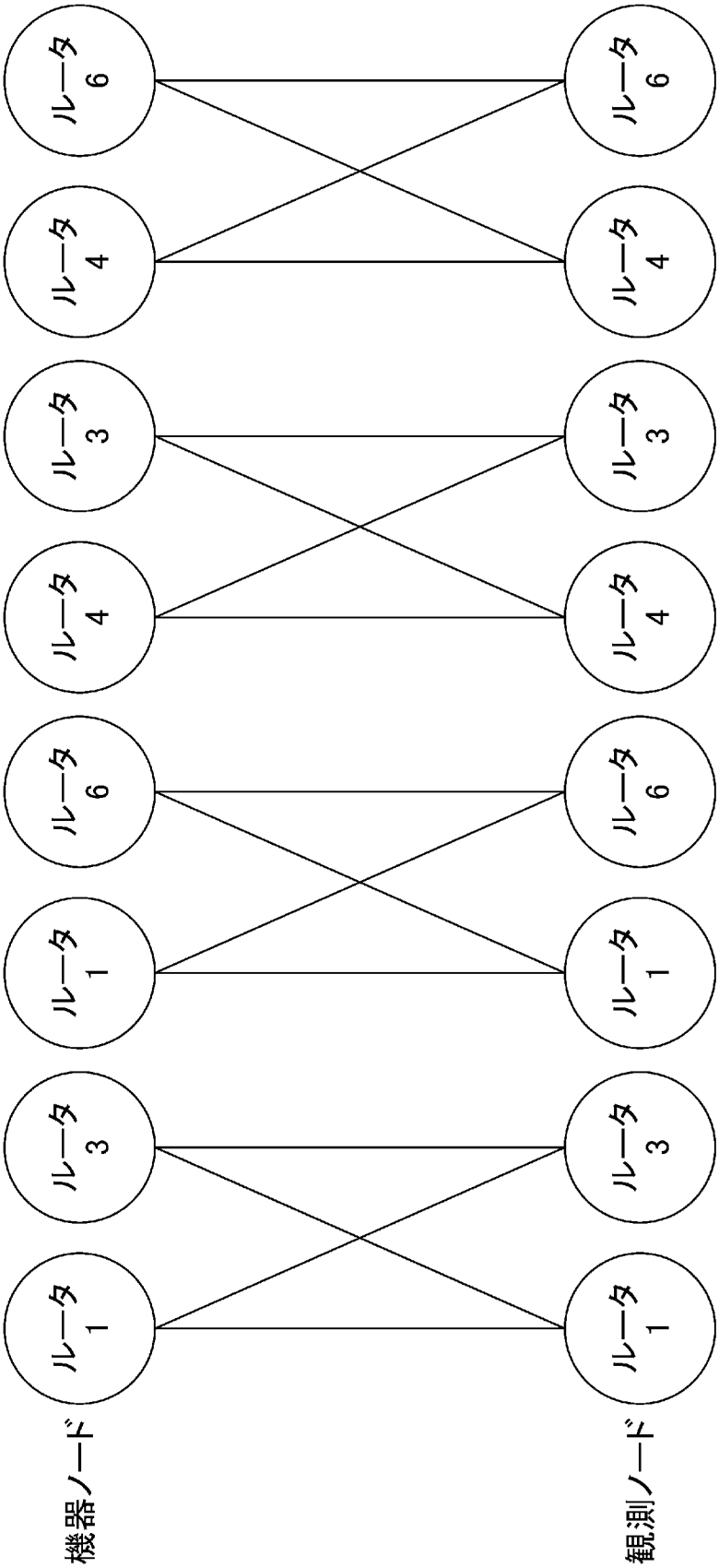
[図5]



[図6]



[図7]


機器ノード
ルータ 1
ルータ 3
ルータ 1
ルータ 6
ルータ 4
ルータ 3
観測ノード
ルータ 1
ルータ 3
ルータ 1
ルータ 6
ルータ 4
ルータ 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/020845

A. CLASSIFICATION OF SUBJECT MATTER

H04L 41/16(2022.01)i
FI: H04L41/16

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)

H04L41/16

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.
X	US 2019/0165988 A1 (GOOGLE LLC.) 30 May 2019 (2019-05-30) particularly, paragraphs [0016]-[0059], fig. 1-5, etc.	1-6
A	JP 2002-354038 A (FUJITSU LTD.) 06 December 2002 (2002-12-06) abstract, claim 1, paragraphs [0026]-[0082], fig. 1	1-6
A	WO 2021/079521 A1 (NIPPON TELEGRAPH & TELEPHONE) 29 April 2021 (2021-04-29) paragraphs [0002], [0026]-[0027], fig. 1	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
04 August 2023	**15 August 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/JP2023/020845

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019/0165988 A1	30 May 2019	WO 2019/104196 A1	
JP 2002-354038 A	06 December 2002	US 2002/0178397 A1 abstract, claim1, paragraphs [0056]-[0114], fig. 1	
WO 2021/079521 A1	29 April 2021	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2023/020845

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 41/16(2022.01)i
FI: H04L41/16

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））

H04L41/16

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
X	US 2019/0165988 A1 (GOOGLE LLC) 30.05.2019 (2019-05-30) 特に、[0016]-[0059],Figures 1-5等	1-6
A	JP 2002-354038 A (富士通株式会社) 06.12.2002 (2002-12-06) 要約,請求項１,[0026]-[0082], 図1	1-6
A	WO 2021/079521 A1 (日本電信電話株式会社) 29.04.2021 (2021-04-29) [0002],[0026]-[0027],図1	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
04.08.2023	15.08.2023

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）

羽岡　さやか 5X 3149

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/JP2023/020845

引用文献	公表日	パテントファミリー文献	公表日
US 2019/0165988 A1	30.05.2019	WO 2019/104196 A1	
JP 2002-354038 A	06.12.2002	US 2002/0178397 A1 ABSTRACT,claim1,[0056]-[0114], FIG.1	
WO 2021/079521 A1	29.04.2021	（ファミリーなし）	