

(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
2021年8月12日(12.08.2021)



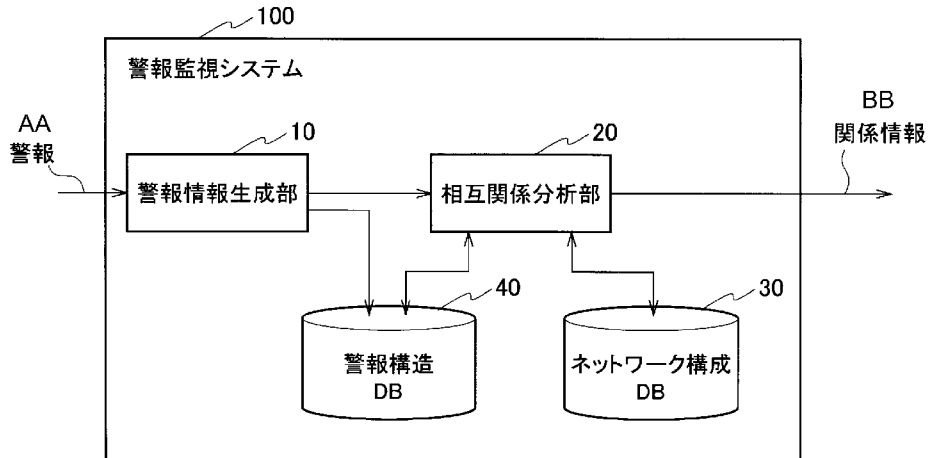
(10) 国際公開番号

WO 2021/156971 A1

- (51) 国際特許分類:
H04L 12/26 (2006.01) *G06F 11/07* (2006.01)
- (21) 国際出願番号: PCT/JP2020/004356
- (22) 国際出願日: 2020年2月5日(05.02.2020)
- (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: 佐藤 亮介 (SATO Ryosuke); 〒1808585 東京都武蔵野市緑町3丁目9-11 N T 知的財産センタ内 Tokyo (JP).
- (74) 代理人: 三好 秀和, 外 (MIYOSHI Hidekazu et al.); 〒1050001 東京都港区虎ノ門1丁目2番8号 虎ノ門琴平タワー Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) Title: ALARM MONITORING SYSTEM, ALARM MONITORING METHOD, AND PROGRAM

(54) 発明の名称: 警報監視システム、警報監視方法、及びプログラム



- 10 Alarm information generating unit
20 Correlation analyzing unit
30 Network configuration database
40 Alarm structure database
100 Alarm monitoring system
AA Alarm
BB Relationship information

(57) Abstract: The present invention comprises: an alarm information generating unit 10 which receives an alarm containing a device name and generated by a device constituting a network, and a knock-on alarm caused by said alarm, distinguishes the respective classifications of the alarm and the knock-on alarm from messages included therein, and generates alarm information in which the alarm and the knock-on alarm are associated with the classifications; a network configuration database 30 which stores network configuration information; and a correlation analyzing unit 20 which comprises

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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告 (条約第21条(3))

pre-established rules representing knock-on alarm generation states that differ by classification, and which searches the network configuration database 30 using the device name and target information determined by the pre-established rules as keys, acquires specific connection point information, and assigns a relationship between the alarm and the knock-on alarm.

(57) 要約：ネットワークを構成する装置が発する装置名を含む警報と該警報を因として生じる波及警報を受信し、警報及び波及警報に含まれるメッセージからそれぞれの種別を判別し、警報及び波及警報と種別を対応付けた警報情報を生成する警報情報生成部 10 と、ネットワークの構成情報を蓄積したネットワーク構成データベース 30 と、種別によって異なる波及警報の発生態様を表す事前ルールを備え、事前ルールで定められた対象情報と装置名をキーにネットワーク構成データベース 30 を検索して具体的な接続先情報を取得し、警報と波及警報を関係付ける相互関係分析部 20 とを備える。

明 細 書

発明の名称： 警報監視システム、警報監視方法、及びプログラム
技術分野

[0001] 本発明は、ネットワーク装置群の運用を監視する警報監視システム、警報監視方法、及びプログラムに関する。

背景技術

[0002] ネットワーク装置群の運用監視において、装置が故障した場合に、故障した装置から警報（主要因アラーム）が発せられる。その警報に加えて、ネットワークの周辺装置から関連した警報が波及的に多数発せられる（波及アラーム）。一般的に警報は、アラームと称される場合があるがここでは警報の文言に統一する。

[0003] 故障対応の際には多くの場合、故障した装置から発せられる警報について対処する必要がある。つまり、波及警報を、対応する警報と関連させて消し込む必要があるが、多数の警報の中から対象の警報を区別するには、オペレータに経験的な高いスキルが求められる。

[0004] この警報を区別する作業を支援する目的で、警報間の関係付けの判断ルールを事前に定義するルールベースの手法、過去の警報の発生パターンを学習する統計ベースの手法、及び学習結果をもとに判断ルールを自動生成する手法（例えば特許文献1）などが検討されて来ている。

先行技術文献

特許文献

[0005] 特許文献1：特開2018-28778号公報

発明の概要

発明が解決しようとする課題

[0006] しかしながら、統計及び生成された判断ルールは、ブラックボックス化し易いという問題がある。また、ルールベースによる手法は、故障時の警報間の共起関係を事前にルールに定義し、警報受信時にルールに従って関係する

警報を検索するが、柔軟なルールを定義することができず、波及警報を正確に区別することができないという問題もある。その結果、警報の区別に正確性を欠くとともに、区別した根拠の説明が求められても説明ができない場合があるという課題がある。

[0007] 本発明は、この課題に鑑みてなされたものであり、オペレータに経験的な高いスキルが無い場合でも対処すべき対象の警報を正しく区別でき、区別した根拠の説明ができる警報監視システム、警報監視方法、及びプログラ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

[0008] 本発明の一態様に係る警報監視システムは、ネットワークを構成する装置が発する装置名を含む警報と該警報を因として生じる波及警報を受信し、前記警報及び前記波及警報に含まれるメッセージからそれぞれの種別を判別し、前記警報及び前記波及警報と前記種別を対応付けた警報情報を生成する警報情報生成部と、前記ネットワークの構成情報を蓄積したネットワーク構成データベースと、前記種別によって異なる前記波及警報の発生態様を表す事前ルールを備え、前記事前ルールで定められた対象情報と前記装置名をキーに前記ネットワーク構成データベースを検索して具体的な接続先情報を取得し、前記警報と前記波及警報を関係付ける相互関係分析部とを備えることを要旨とする。

[0009] また、本発明の一態様に係る警報監視方法は、上記の警報監視システムが行う警報監視方法であって、ネットワークを構成する装置が発する装置名を含む警報と該警報を因として生じる波及警報を受信し、前記警報及び前記波及警報に含まれるメッセージからそれぞれの種別を判別し、前記警報及び前記波及警報と前記種別を対応付けた警報情報を生成する警報情報生成ステップと、前記種別によって異なる前記波及警報の発生態様を表す事前ルールを備え、前記事前ルールで定められた対象情報と前記装置名をキーに前記ネットワークの構成情報を蓄積したネットワーク構成データベースを検索して具体的な接続先情報を取得し、前記警報と前記波及警報を関係付ける相互関係

分析ステップとを含むことを要旨とする。

[0010] また、本発明の一態様に係るプログラムは、上記の警報監視システムとしてコンピュータを機能させるためのプログラムであることを要旨とする。

発明の効果

[0011] 本発明によれば、オペレータに経験的な高いスキルが無い場合でも対処すべき対象の警報を正しく区別できる。また、対処すべき対象の警報と波及警報を関係付けるので区別した根拠の説明も容易にできる。

図面の簡単な説明

[0012] [図1]本発明の実施形態に係る警報監視システムの機能構成例を示すブロック図である。

[図2]図1に示す警報監視システムの動作例を説明する動作説明図である。

[図3]警報の構成例を示す図である。

[図4]図1に示す相互関係分析部が備える事前ルールの例を示す図である。

[図5]図1に示すネットワーク構成DBのレコードの例を模式的に示す図である。

[図6]図1に示す警報監視システムの他の動作例を説明する動作説明図である。

[図7]ネットワークの異なる階層で生じた故障の様子を模式的に示す図である。

[図8]事前ルールに記述されたラベル情報を模式的に示す図である。

[図9]図1に示す警報監視システムが行う警報監視方法の処理手順を示すフローチャートを示す図である。

[図10]図9に示す警報監視方法で関係情報を生成した例を示す図である。

[図11]汎用的なコンピュータシステムの構成例を示すブロック図である。

発明を実施するための形態

[0013] 以下、本発明の実施形態について図面を用いて説明する。複数の図面中同一のものには同じ参照符号を付し、説明は繰り返さない。

[0014] 図1は、本発明の実施形態に係る警報監視システムの機能構成例を示すブ

ロック図である。図 1 に示す警報監視システム 100 は、ネットワークを構成する各装置（図示せず）と制御線で接続され、各装置から発せられる警報を監視し、対処すべき対象の警報とそれ以外の波及警報とを関係付けるシステムである。

[0015] 警報監視システム 100 は、警報情報生成部 10、相互関係分析部 20、ネットワーク構成データベース 30、及び警報構造データベース 40 を備える。以降、データベースは DB と表記する。

[0016] 図 2 は、警報監視システム 100 の動作例を説明する動作説明図である。図 2 は、図 1 に示すブロック図に主要な情報の流れを記載した図である。図 2 と他の図を参照して警報監視システム 100 が、対処すべき警報と、その警報を原因（主）として波及的に生じる波及警報（従）とを関係付ける例の動作を説明する。

[0017] （関係付けの一例）

警報情報生成部 10 は、ネットワークを構成する各装置から警報を受信する。図 2 では、Host_A（装置）が故障したことを表す警報 EQP を生じさせた後に、その警報 EQP を原因として Host_B（装置）に波及警報 linkdown が生じた例を模式的に示す。

[0018] 警報情報生成部 10 は、警報を受信して警報情報を生成する。警報は、例えば警報 EQP と波及警報 linkdown を発したそれぞれの装置を識別する装置名と、警報 EQP 及び波及警報 linkdown の種別を表すメッセージとを含む。また、警報情報生成部 10 は、受信した警報を警報構造 DB 40 に記録する。図 2 の警報構造 DB 40 内に、記録した EQP と Port 1/2 Linkdown を示す。

[0019] 図 3 は、警報の構成例を示す図である。左から一列目は装置名、二列目はメッセージを示す。一行目は Host_A が発した警報 EQP である。三行目は Host_B が発した警報 linkdown である。なお、メッセージの文字列は、装置のベンダーによって異なる。

[0020] 警報情報生成部 10 は、警報に含まれるメッセージの文字列を認識してその警報の種別を判別する。警報の種別とは、装置本体故障、部位故障、物理

リンク故障、及び論理リンク故障等のことである。

[0021] 警報情報生成部 10 は、判別した種別と警報を対応付けた警報情報を相互関係分析部 20 に出力する。なお、その際、警報情報は警報構造 DB 40 に記録するようにしても良い。

[0022] 相互関係分析部 20 は、種別によって異なる波及警報の発生態様を表す事前ルールを備え、事前ルールで定められた対象情報と装置名をキーにネットワーク構成 DB 30 を検索して具体的な接続先情報を取得する。そして、警報と波及警報を関係付ける。事前ルールは予め人が設定する。なお、装置の特定のポートの接続先の装置を取得したい場合などは、装置名に加えてポート番号等を追加の検索パラメータとして用いても良い。

[0023] 図 4 は事前ルールの例を示す。図 4 の左から一列目は装置故障の種別を示し、二列目は種別に対応する事前ルールを示す。図 4 に示すように事前ルールは、警報の種別に対応させて、その警報によって異なる波及警報の発生態様を表したものである。

[0024] 警報情報生成部 10 において、警報 EQP は、そのメッセージから装置本体故障と判別される（図 3 の上から 2 行目）。装置本体故障の場合の事前ルールは「物理接続先の装置から波及警報 linkdown が生じる」である。また、物理リンク故障の場合の事前ルールは「物理接続先の装置から波及警報 linkdown が生じる」である。また、論理リンク故障の場合の事前ルールは「論理接続先の装置から波及警報 LOC が生じる」である。

[0025] 対象情報は、ネットワーク構成 DB 30 を検索するキーであり、検索する対象によって異なる情報である。例えば、物理接続先を検索する場合の対象情報は「物理接続先」である。また、論理接続先を検索する場合の対象情報は「論理接続先」である。

[0026] 相互関係分析部 20 は、事前ルールに定められた対象情報（この場合は物理接続先）と装置名（この場合 Host_A）をキーにネットワーク構成 DB 30 を検索して具体的な接続先情報を取得する。なお、検索キーには装置部位名を用いることもできる。以下同様である。

[0027] 図5は、ネットワーク構成DB30のレコードの例を示す図である。図5の左から一列目（装置名）と二列目（対象情報）は検索キーである。三列目はその検索キーで検索されるデータである。

[0028] 装置名（Host_A）と物理接続先をキーにネットワーク構成DB30を検索すると、Host_B、スロット1、ポート2の接続先情報が得られる。よって、事前ルールによれば、その接続先から波及警報linkdownが生じることとなる。

[0029] 相互関係分析部20は、警報情報生成部10が波及警報linkdownを受信した場合、又は波及警報linkdownを既に受信済みの場合に、その波及警報linkdownの原因となった警報EQP（この場合、Host_A）と波及警報linkdownを関係付ける。関係付けは、例えばそれぞれをノード（節）で表してそれぞれのノードをエッジ（辺）で接続させたデータ構造で表すことで行う。

[0030] 警報と波及警報の関係を表す関係情報は、警報構造DB30に記録するようにしても良い。図2に示す警報構造DB40内に関係情報の例を示す。

[0031] 図2に例示する関係情報は、警報EQP（Host_A, EQP）をノード1、波及警報linkdown（Host_B Port1/2 linkdown）をノード2とし、ノード1とノード2をエッジ1で接続させたものである。エッジ1は方向性を持ち、例えば図2に示す”edge1で始まる文字列で表せる。Srcは波及警報を生じさせる主要因である警報であることを表し、dstはその警報（主要因）を原因として生じる波及警報であることを表す。

[0032] このように、警報と波及警報の関係情報は、警報と波及警報のそれぞれを表すノードと、該ノードのそれぞれを接続されるエッジとで表される。これにより、主要因である警報とその以外の波及警報の区別が容易になる。

[0033] （関係付けの他の一例）

警報と波及警報の関係付けは、装置間の物理接続に関するものに限られない。例えば論理的な接続に対しても行える。

[0034] 図6は、中継装置を介して2つの装置が論理的に接続され、中継装置又は通信線が故障したことによって、Host_Aに通信切断を意味する警報LOCが生じ、続けてその論理接続先のHost_Bに警報LOCが生じる場合を示す。

- [0035] 警報情報生成部 10 は、Host_A に生じた警報 LOC に含まれるメッセージの文字列 (LOC) を認識してその警報の種別を判別する。判別した種別はこの例では「論理リンク故障」である。判別した種別を含む警報情報は、警報構造 DB 40 に記録する。
- [0036] 相互関係分析部 20 は、警報情報生成部 10 で判別した種別を含む警報情報を入力とし、その種別に対応する事前ルールを参照する。論理リンク故障の場合の事前ルールは「論理接続先の装置から波及警報 LOC が生じる」である。
- [0037] この場合、相互関係分析部 20 は、「Host_A」と「論理接続先」をキーにネットワーク構成 DB 30 を検索する。ネットワーク構成 DB 30 は、Host_A の論理接続先として Host_B を記録している。
- [0038] 相互関係分析部 20 は、この場合の具体的な接続先情報として Host_B を取得する。その後、警報情報生成部 10 が波及警報 LOC を受信すると、その波及警報 LOC と、その原因となった警報 LOC (この場合、Host_A) を関係付ける。
- [0039] LOC 同士の関係付けは、2つのノードを双方向の矢印で接続させて行う。警報情報生成部 10 が Host_A から受信した警報 LOC は、中継装置の故障によって生じた波及警報である。また、その次に Host_B から受信した警報 LOC も波及警報である。
- [0040] このように警報の種別が物理リンク故障、論理リンク故障等の場合は、2つの警報間でそれぞれの他方を波及警報と区別した結果、2つの警報は双方向の矢印で関係付けられる。なお、警報情報生成部 10 が受信する警報の順番は、Host_A→Host_B の順番に限られない。ネットワークの通信状況によっては順番が逆転する場合もあり得る。
- [0041] 警報情報生成部 10 が受信する警報の順番が入れ替わるのは、主要因の警報と波及警報の組合せの場合も同じである。警報 linkdown を先に受信し、その後警報 EQP を受信する場合もある。
- [0042] 警報 linkdown を受信した場合、警報情報生成部 10 はその警報の種別を「物理リンク故障 (図 3 の 4 行目)」と判別する。種別が「物理リンク故障」の

場合の相互関係分析部 20 の事前ルールは「物理接続先の装置から波及警報 linkdownが生じる（図 4 の4行目）」である。

[0043] その後、警報情報生成部 10 は、Host_Aから警報EQPを受信する。警報EQPの事前ルールは「物理接続先の装置から波及警報 linkdownが生じる（図 4 の2行目）」である。よって、ネットワーク構成DB30を参照することで、既に受信済みの波及警報 linkdownとHost_Aから受信した警報EQPを関係付けることができる。

[0044] このように、ネットワークの通信状況によって、警報EQPと警報 linkdownの順番が入れ替わっても主要因の警報と波及的に生じる波及警報に区別して関係付けることができる。要するに、警報情報生成部 10 は、主要因の警報と波及警報のどちらを先に受信しても良い。また、波及警報だけを受信しても波及警報同士を関係付けることができる。

[0045] 以上説明したように本実施形態に係る警報監視システムは、ネットワークを構成する装置が発する装置名を含む警報と該警報を因として生じる波及警報を受信し、警報及び波及警報に含まれるメッセージからそれぞれの種別を判別し、警報及び波及警報と種別を対応付けた警報情報を生成する警報情報生成部 10 と、ネットワークの構成情報を蓄積したネットワーク構成DB30と、種別によって異なる波及警報の発生態様を表す事前ルールを備え、事前ルールで定められた対象情報と装置名をキーにネットワーク構成DB30を検索して具体的な接続先情報を取得し、警報と波及警報を関係付ける相互関係分析部 20 と、警報と波及警報の関係を表す関係情報を蓄積する警報構造DB40とを備える。これにより、オペレータに経験的な高いスキルが無い場合でも対処すべき対象の警報を区別できる。また、対処すべき対象の警報と波及警報を関係付けるので区別した根拠の説明も容易に行える。

[0046] 上記の実施形態では、「装置本体故障」、「論理リンク故障」、及び「物理リンク故障」の種別の警報について説明したが、これ以外の種別の警報についても事前ルールを適切に設定することで、対処すべき警報とそれ以外の警報を区別することができる。また、2個以上の複数の警報についても、それ

それぞれの警報を例えば上記の有向グラフで関係付けることが可能である。したがって、2個以上の複数の警報の中から対処すべき対象の警報を区別することができる。なお、警報構造DB40は、関係情報を表示装置（図示せず）又は印刷装置（図示せず）に出力するようにすれば無くても構わない。

[0047] （ネットワークの階層を跨る警報の関係付け）

警報の関係付けは、複数の事前ルールを適用することで行われる。よって、ネットワークの異なる階層で発生した警報についても関係付けることが可能である。

[0048] 図7は、ネットワーク層（IPレイヤ）とデータリンク層（伝送レイヤ）を跨って警報が生じる場合の例を模式的に示す図である。図7（a）に示すブロックは装置を表す。各装置の近くに表記した文字列は警報を表す。IPレイヤのHost_CとHost_Dのそれぞれに警報linkdownが発生し、伝送レイヤのHost_Bに警報linkdownが発生し、同じ伝送レイヤのHost_Aに警報EQPが発生する例を示す。

[0049] 図7（a）に示すように警報が発生した場合、本実施形態に係る警報監視システム100によれば、上記の説明済みの動作を行って各警報を有向グラフで関係付けることができる。

[0050] 図7（b）は、図7（a）に示す警報を有向グラフで関係付けた図である。各ノード（警報）を結ぶ有向グラフによって主要因の警報を特定することができる。

[0051] 図7に示すように警報EQPは、自己の方向に矢印が向いているエッジが存在しないので主要因の警報であると特定する。逆に、方向が自己に向けられたエッジを含むノードは波及警報に区別される。

[0052] 警報を有向グラフで関係付ける方法は、各ノードに対するエッジの向きが判明しないと主要因の警報であるのか波及警報であるのかを区別することができない。よって、区別するまでに時間を要してしまう場合がある。

[0053] 区別する時間を短縮する方法としては、関係の属性から主要因を判定する方法が考えられる。例えば、事前ルールに、結果として生じる波及警報とそ

の原因となる警報情報の関係を表すラベル情報を含める。ラベル情報は、原因から結果を関係付けても、結果から原因を関係付けてもどちらでも構わない。

[0054] 例えば、図2で説明した警報linkdownが生じる場合、その警報linkdownが結果として生じる警報EQPは主要因であるとして、事前ルールに例えばSTORE_ROOTのラベル情報を含ませる。

[0055] この他に、因果関係はあるが主要因であるか否かの判定はしないSTORE、関係はあるが主従の関係が無いCONNET等のラベル情報を事前ルールに含める。これらのラベル情報を事前ルールに含めることで、事前ルールによって主要因の警報であることを特定することが可能である。つまり、警報と波及警報は、ラベル情報に基づいて区別しても良い。これにより、主要因の警報であるのか波及警報であるのかを区別するのに要する時間を短縮することができる。

[0056] (警報監視方法)

図9は、本実施形態に係る警報監視システム100が行う警報監視方法の処理手順を示すフローチャートである。

[0057] 警報情報生成部10は、ネットワークを構成する装置が発する警報と該警報を因として生じる波及警報のそれぞれを識別する装置名と警報及び波及警報の種別を表すメッセージとを含む警報を受信する(ステップS1)。

[0058] 次に、警報情報生成部10は、受信したメッセージの文字列を認識して警報の種別を判定する(ステップS2)。警報の種別は、装置本体故障、部位故障、物理リンク故障、論理リンク故障等に判別される。

[0059] 相互関係分析部20は、警報の種別によって異なる波及警報の発生態様を表す事前ルールを備え、事前ルールで定められた対象情報と装置名をキーにネットワーク構成DB30を検索して具体的な接続先情報を取得する(ステップS3)。警報情報の種別が例えば「装置本体故障」の場合は、事前ルールは「物理接続先の装置から波及警報linkdownが生じる」である。

[0060] この場合、Host_Aと「物理接続先」をキーにネットワーク構成DB30を

検索して具体的な接続先情報を含む応答情報 (Host_b Port 1/2 linkdown) を取得する (ステップ S 3)。

[0061] そして、相互関係分析部 20 は、対象情報と応答情報から、警報と波及警報を関係付ける関係情報を生成する (ステップ S 4)。

[0062] 関係情報は、警報情報 DB 40 に記録される (ステップ S 5)。関係情報は、例えば、図 2 に "edge1..." で示される文字列で表される。

[0063] なお、関係情報を記録するステップ S 5 は行わなくても構わない。生成した関係情報を外部 (表示装置又は印刷装置) に出力するだけでも良い。

[0064] 図 10 は、本実施形態の警報監視方法で関係情報を生成した例を示す図である。図 10 の左から一列目は受信順序、二列目と三列目は警報、四列目は関係情報を示す。この例は、ネットワーク構成の表記は省略するが、Host_A、Host_B、及び Host_C が通信線で接続され、Host_C と Host_D は制御線のみで接続された場合を示す。

[0065] 図 10 に示す受信順序で警報が発生したと仮定すると、通信線で接続された装置から発生する警報は、主要因の警報と波及警報に区別される。図 10 の上から二行目の 1/主要因の 1/ は、警報群のグループに割り振られる ID (識別子) である。

[0066] 図 10 の四行目と五行目の 1/波及は、1/主要因の警報によって生じた波及警報であることを示す。オペレータは、関係情報 (図 10) を見ることで主要因の警報と、その警報によって生じた波及警報を容易に区別することができる。

[0067] 以上説明したように本実施形態に係る警報監視方法は、警報監視システム 100 が行う警報監視方法であって、ネットワークを構成する装置が発する装置名を含む警報と該警報を因として生じる波及警報を受信し、警報及び波及警報に含まれるメッセージからそれぞれの種別を判別し、警報及び波及警報と種別を対応付けた警報情報を生成する警報情報生成ステップ (S 1, S 2) と、種別によって異なる波及警報の発生態様を表す事前ルールを備え、事前ルールで定められた対象情報と装置名をキーにネットワークの構成情報

を蓄積したネットワーク構成DBを検索して具体的な接続先情報を取得し、警報と波及警報を関係付ける相互関係分析ステップ（S3，S4）とを含む。これにより、ネットワークを監視するオペレータに高いスキルが無くても、対処すべき対象の警報と対処の不要な波及警報を正しく区別することができる。

[0068] 警報監視システム100は、図11に示す汎用的なコンピュータシステムで実現することができる、例えば、CPU90、メモリ91、ストレージ92、通信部93、入力部94、及び出力部95を備える汎用的なコンピュータシステムにおいて、CPU90がメモリ91上にロードされた所定のプログラムを実行することにより、警報監視システム100の各機能が実現される。所定のプログラムは、HDD、SSD、USBメモリ、CD-ROM、DVD-ROM、MOなどのコンピュータ読取り可能な記録媒体に記録することも、ネットワークを介して配信することもできる。なお、警報監視システム100の各機能部は、それぞれをコンピュータシステム（サーバ）で構成しても構わない。

[0069] 本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で変形が可能である。例えば、警報情報生成部10は、警報を受信して警報情報を生成する例で説明したが、この例に限定されない。受信と警報情報生成は、それぞれの作用を分けて構成しても構わない。また、ネットワーク構成DB30のデータ形式は上記の例に限定されない。例えばリレーショナルDB及びグラフDB等でも良い。また、警報情報生成部10は、相互関係分析部20に警報情報と種別を対応付けた構造化データで引き渡すことができれば、警報を受信するプロトコルは何でも構わない。

[0070] このように、本発明はここでは記載していない様々な実施形態等を含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

符号の説明

[0071] 10：警報情報生成部
20：相互関係分析部

30 : ネットワーク構成データベース

40 : 警報構造データベース

100 : 警報監視システム

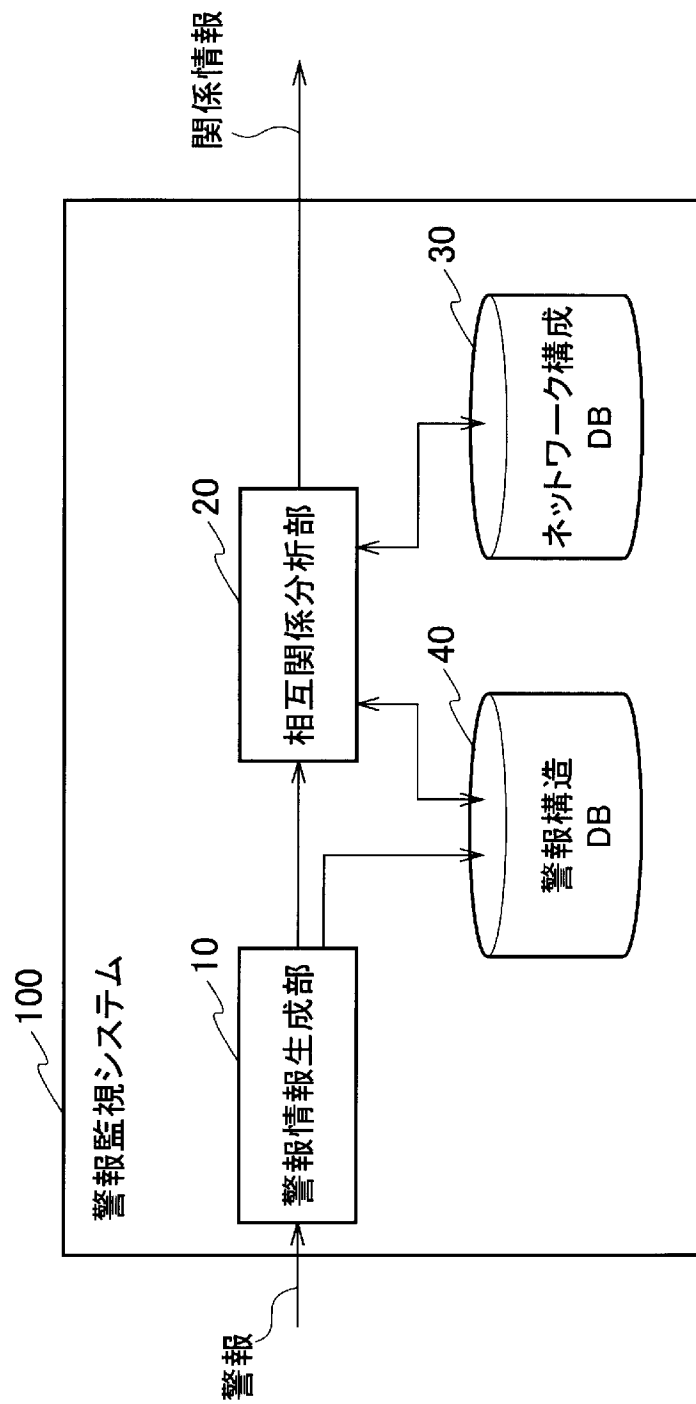
請求の範囲

- [請求項1] ネットワークを構成する装置が発する装置名を含む警報と該警報を
因として生じる波及警報を受信し、前記警報及び前記波及警報に含ま
れるメッセージからそれぞれの種別を判別し、前記警報及び前記波及
警報と前記種別を対応付けた警報情報を生成する警報情報生成部と、
前記ネットワークの構成情報を蓄積したネットワーク構成データベ
ースと、
前記種別によって異なる前記波及警報の発生態様を表す事前ルール
を備え、前記事前ルールで定められた対象情報と前記装置名をキーに
前記ネットワーク構成データベースを検索して具体的な接続先情報を
取得し、前記警報と前記波及警報を関係付ける相互関係分析部と
を備える警報監視システム。
- [請求項2] 前記関係情報は、前記警報と前記波及警報のそれぞれを表すノード
と、該ノードのそれぞれを接続させるエッジとで表される
請求項1に記載の警報監視システム。
- [請求項3] 前記事前ルールは、前記警報と前記波及警報の関係を表すラベル情
報を含み、前記関係は該ラベル情報に基づいて区別される
請求項1又は2に記載の警報監視システム。
- [請求項4] 方向が自己に向けられた前記エッジを含む前記ノードは前記波及警
報に区別される
請求項2に記載の警報監視システム。
- [請求項5] 警報監視システムが行う警報監視方法であって、
ネットワークを構成する装置が発する装置名を含む警報と該警報を
因として生じる波及警報を受信し、前記警報及び前記波及警報に含ま
れるメッセージからそれぞれの種別を判別し、前記警報及び前記波及
警報と前記種別を対応付けた警報情報を生成する警報情報生成ステッ
プと、
前記種別によって異なる前記波及警報の発生態様を表す事前ルール

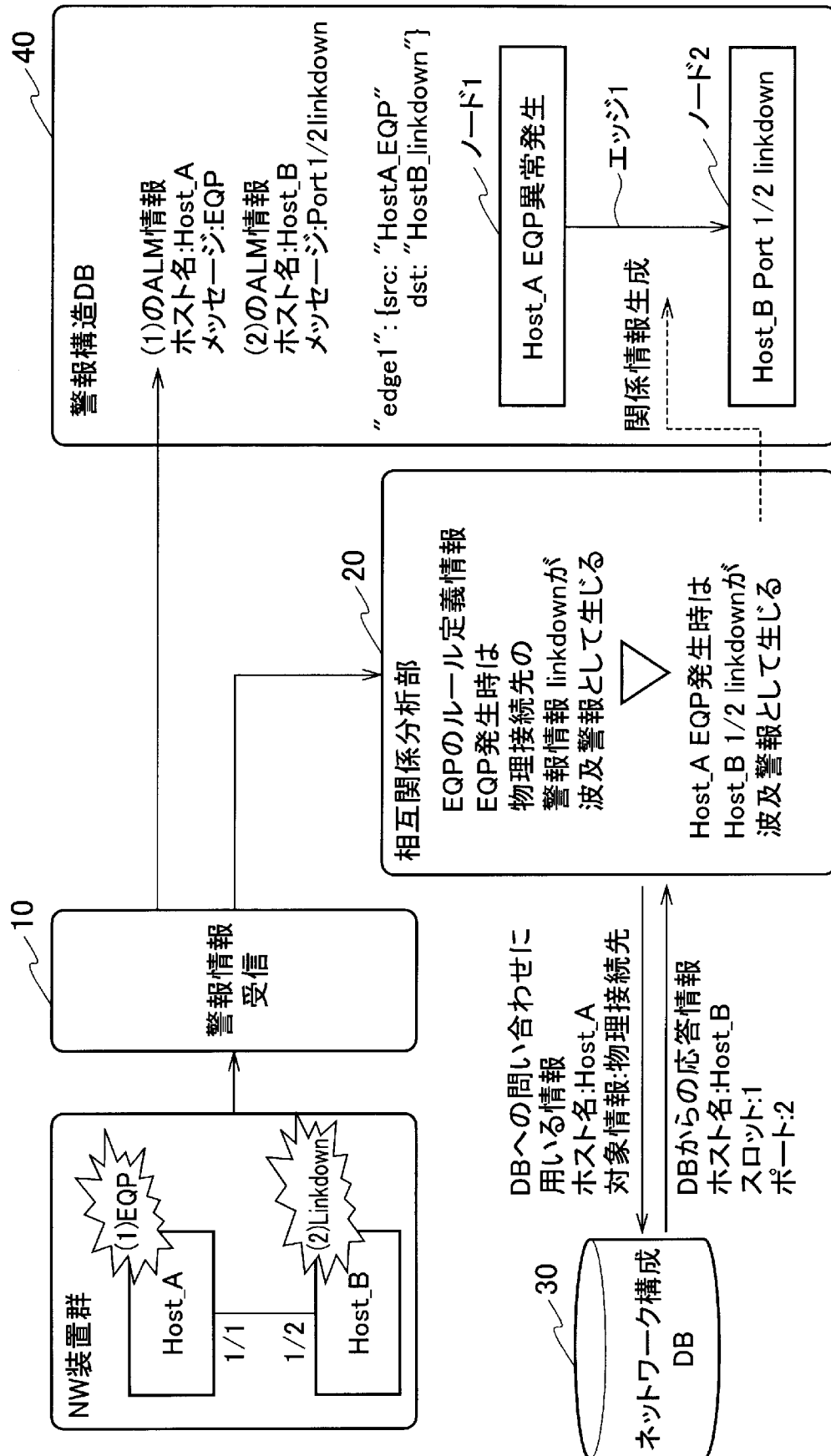
を備え、前記事前ルールで定められた対象情報と前記装置名をキーに前記ネットワークの構成情報を蓄積したネットワーク構成データベースを検索して具体的な接続先情報を取得し、前記警報と前記波及警報を関係付ける相互関係分析ステップとを含む警報監視方法。

[請求項6] 請求項1乃至4の何れかに記載の警報監視システムとしてコンピュータを機能させるためのプログラム。

[図1]



[図2]



[図3]

装置名	メッセージ
Host_A	EQP, device fault, ...
Host_A	LOC
Host_B	Port ½ linkdown
Host_B	LOC
⋮	⋮

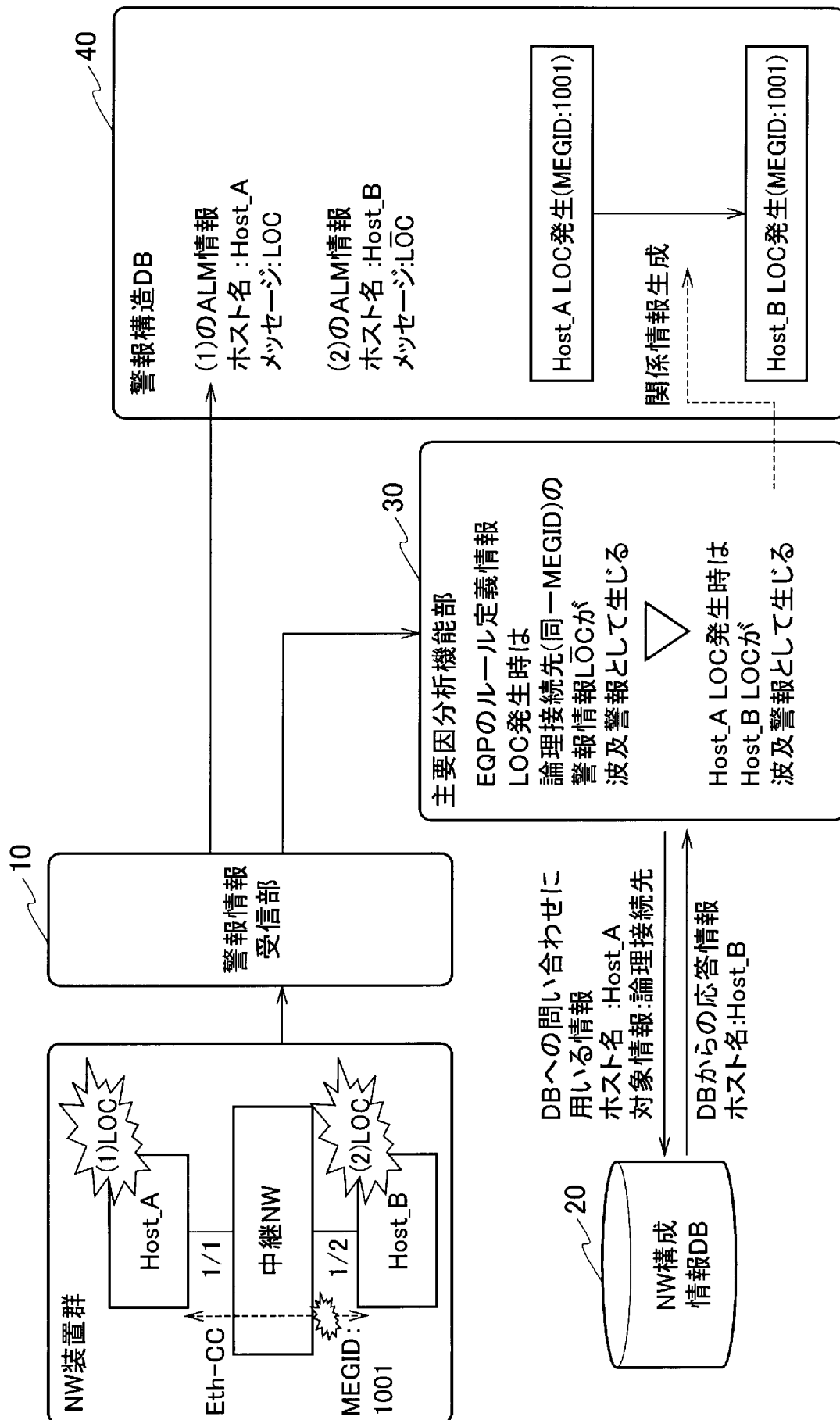
[図4]

警報情報の種別	事前ルール
装置本体故障	物理接続先の装置から波及警報linkdownが生じる
部位故障	
物理リンク故障	物理接続先の装置から波及警報linkdownが生じる
論理リンク故障	論理接続先の装置から波及警報LOCが生じる
⋮	⋮

[図5]

ホスト名	対象情報	データ
Host_A	物理接続先	Host_B, Slot:1, Port:2
Host_A	論理リンク故障	Host_B
⋮	⋮	⋮

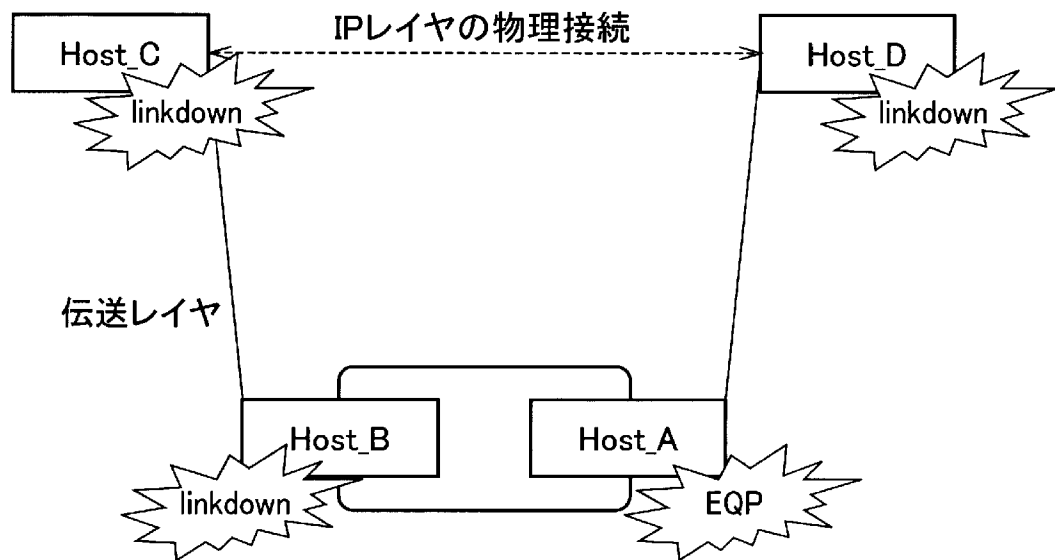
[図6]



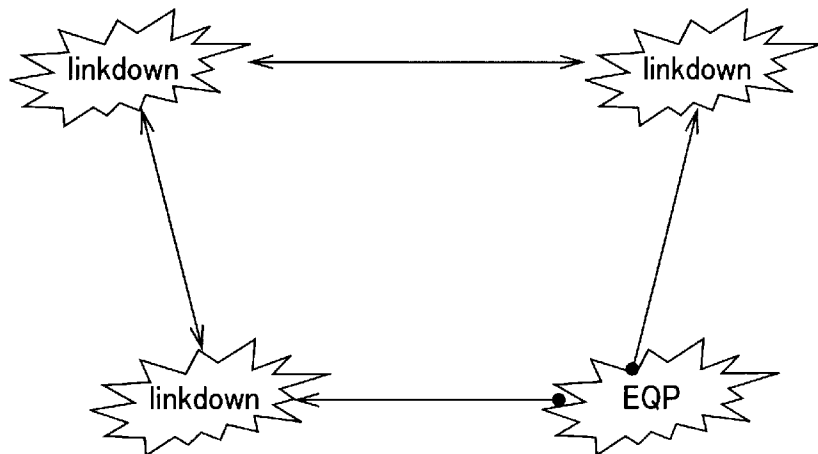
[図7]

(a)

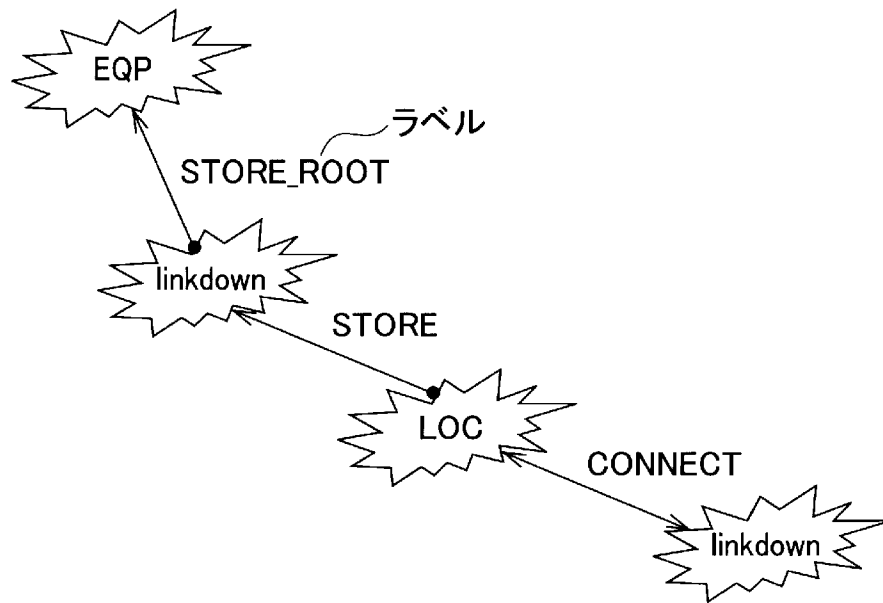
IPレイヤ



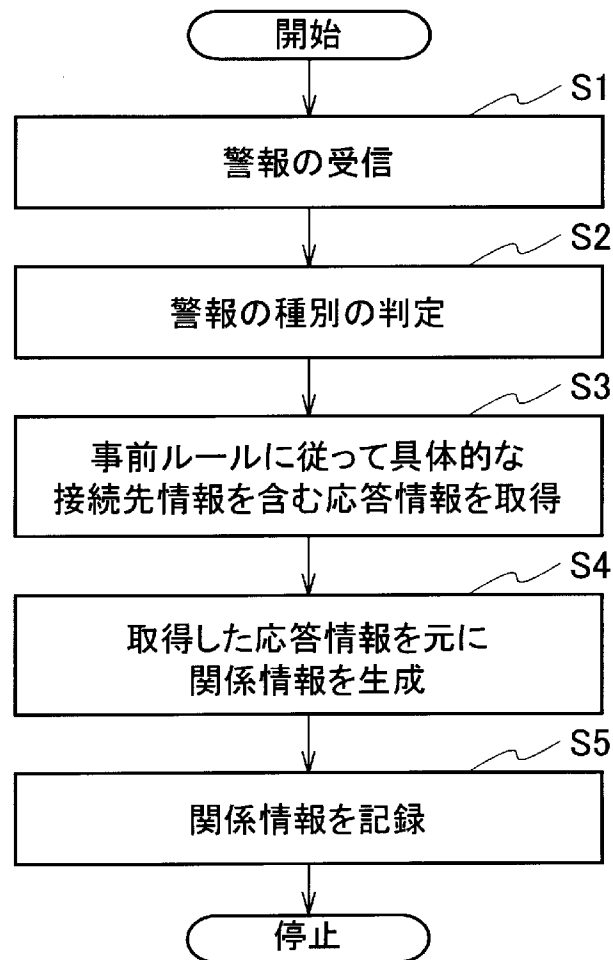
(b)



[図8]



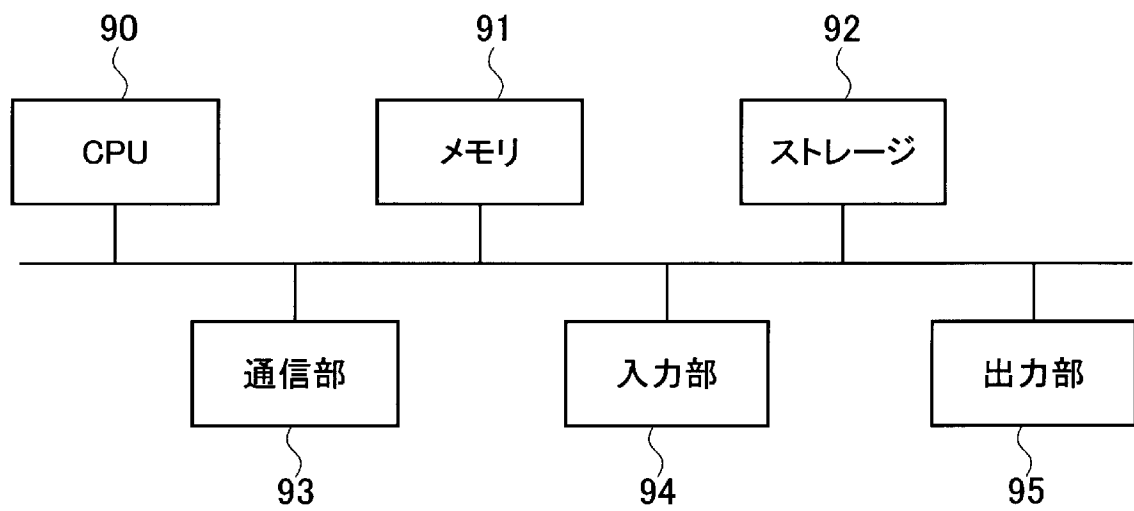
[図9]



[図10]

受信順序	装置名	メッセージ	故障事象id /主要因
1	Host_A	EQP(本体故障)	1/主要因
2	...	...	
3	Host_B	Port 1/1 linkdown	1/波及
4	...	...	
5	Host_E	Port 1/2 linkdown	2/未確定
6	Host_C	Port 1/2 linkdown	1/波及
7	...	...	
8	...	...	
9	Host_D	Port 1/1 linkdown	2/未確定
10	...	...	

[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/004356

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. H04L12/26(2006.01) i, G06F11/07(2006.01) i
FI: G06F11/07 190, G06F11/07 140A, H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. H04L12/26, G06F11/07

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 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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 2014/141460 A1 (HITACHI, LTD.) 18 September 2014	1-6
A	JP 2012-213112 A (NIPPON TELEGRAPH & TELEPHONE EAST CORP.) 01 November 2012	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
04.09.2020

Date of mailing of the international search report
15.09.2020

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2020/004356

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
WO 2014/141460 A1	18.09.2014	US 2015/0244599 A1	
JP 2012-213112 A	01.11.2012	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 12/26(2006.01)i; G06F 11/07(2006.01)i FI: G06F11/07 190; G06F11/07 140A; H04L12/26										
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）） H04L12/26; G06F11/07 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020年
日本国実用新案公報	1922 - 1996年									
日本国公開実用新案公報	1971 - 2020年									
日本国実用新案登録公報	1996 - 2020年									
日本国登録実用新案公報	1994 - 2020年									
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 2014/141460 A1（株式会社日立製作所）18.09.2014（2014 - 09 - 18）	1-6								
A	JP 2012-213112 A（東日本電信電話株式会社）01.11.2012（2012 - 11 - 01）	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。										
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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						
* 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 04.09.2020		国際調査報告の発送日 15.09.2020								
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） 塚田 肇 5B 3652 電話番号 03-3581-1101 内線 3545								

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/JP2020/004356

引用文献			公表日	パテントファミリー文献			公表日
WO	2014/141460	A1	18.09.2014	US	2015/0244599	A1	
JP	2012-213112	A	01.11.2012	(ファミリーなし)			