

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7498128号
(P7498128)

(45)発行日 令和6年6月11日(2024.6.11)

(24)登録日 令和6年6月3日(2024.6.3)

(51)国際特許分類 F I
H 0 4 L 43/00 (2022.01) H 0 4 L 43/00

請求項の数 11 (全14頁)

(21)出願番号	特願2021-28735(P2021-28735)	(73)特許権者	598057291 エフサステクノロジーズ株式会社 神奈川県川崎市中原区中丸子13番地2
(22)出願日	令和3年2月25日(2021.2.25)	(74)代理人	110002147 弁理士法人酒井国際特許事務所
(65)公開番号	特開2022-129879(P2022-129879 A)	(72)発明者	野崎 淳 神奈川県川崎市中原区中丸子13番地2 株式会社富士通エフサス内
(43)公開日	令和4年9月6日(2022.9.6)	(72)発明者	山中 基裕 神奈川県川崎市中原区中丸子13番地2 株式会社富士通エフサス内
審査請求日	令和5年3月15日(2023.3.15)	(72)発明者	石黒 信二 神奈川県川崎市中原区中丸子13番地2 株式会社富士通エフサス内
		(72)発明者	鈴木 大和

最終頁に続く

(54)【発明の名称】 監視装置、障害検知方法および障害検知プログラム

(57)【特許請求の範囲】

【請求項1】

ネットワークに含まれる複数のスイッチのうち、監視対象とする第1スイッチと、第2スイッチと、第1監視スイッチとをそれぞれ仮想ネットワークで接続した第2監視スイッチから、前記第1スイッチとの第1通信状況、前記第2スイッチとの第2通信状況、前記第1監視スイッチおよび前記第2監視スイッチとの第3通信状況とを取得する取得部と、前記第1通信状況と、前記第2通信状況と、前記第3通信状況とを基にして、前記第1スイッチおよび前記第2スイッチから、障害の発生したスイッチを検知する検知部と、を有することを特徴とする監視装置。

【請求項2】

前記検知部によって検出された障害の発生したスイッチに対してメッセージを送信することで、通信を停止させる制御を行う送信部を更に有することを特徴とする請求項1に記載の監視装置。

【請求項3】

前記検知部は、前記第1通信状況および前記第3通信状況にアラートが発生しておらず、第2通信状況のみにアラートが発生している場合には、前記第1スイッチまたは前記第2スイッチの障害を検知することを特徴とする請求項1または2に記載の監視装置。

【請求項4】

前記検知部は、前記第2通信状況および前記第3通信状況にアラートが発生しておらず、前記第1通信状況のみにアラートが発生している場合には、前記第1スイッチの障害を

検知することを特徴とする請求項 1、2 または 3 に記載の監視装置。

【請求項 5】

前記検知部は、前記第 1 通信状況および前記第 2 通信状況にアラートが発生しておらず、前記第 3 通信状況のみにアラートが発生している場合には、前記第 1 スwitch の障害を検知することを特徴とする請求項 1 ~ 4 のいずれか一つに記載の監視装置。

【請求項 6】

前記検知部は、前記第 2 通信状況にアラートが発生しておらず、前記第 1 通信状況および前記第 3 通信状況のみにアラートが発生している場合には、前記第 1 スwitch の障害を検知することを特徴とする請求項 1 ~ 5 のいずれか一つに記載の監視装置。

【請求項 7】

前記検知部は、前記第 3 通信状況にアラートが発生しておらず、前記第 1 通信状況および前記第 2 通信状況のみにアラートが発生している場合には、前記第 1 スwitch の障害を検知することを特徴とする請求項 1 ~ 6 のいずれか一つに記載の監視装置。

【請求項 8】

前記検知部は、前記第 1 通信状況にアラートが発生しておらず、前記第 2 通信状況および前記第 3 通信状況のみにアラートが発生している場合には、前記第 1 スwitch の異常を検知することを特徴とする請求項 1 ~ 7 のいずれか一つに記載の監視装置。

【請求項 9】

前記検知部は、前記第 1 通信状況と、前記第 2 通信状況と、前記第 3 通信状況とにアラートが発生している場合には、前記第 1 スwitch の障害を検知することを特徴とする請求項 1 ~ 8 のいずれか一つに記載の監視装置。

【請求項 10】

コンピュータが実行する障害検知方法であって、

ネットワークに含まれる複数のスitchのうち、監視対象とする第 1 スitchと、第 2 スitchと、第 1 監視スitchとをそれぞれ仮想ネットワークで接続した第 2 監視スitchから、前記第 1 スitchとの第 1 通信状況、前記第 2 スitchとの第 2 通信状況、前記第 1 監視スitchおよび前記第 2 監視スitchとの第 3 通信状況とを取得し、

前記第 1 通信状況と、前記第 2 通信状況と、前記第 3 通信状況とを基にして、前記第 1 スitchおよび前記第 2 スitchから、障害の発生したスitchを検知する

処理を実行することを特徴とする障害検知方法。

【請求項 11】

コンピュータに、

ネットワークに含まれる複数のスitchのうち、監視対象とする第 1 スitchと、第 2 スitchと、第 1 監視スitchとをそれぞれ仮想ネットワークで接続した第 2 監視スitchから、前記第 1 スitchとの第 1 通信状況、前記第 2 スitchとの第 2 通信状況、前記第 1 監視スitchおよび前記第 2 監視スitchとの第 3 通信状況とを取得し、

前記第 1 通信状況と、前記第 2 通信状況と、前記第 3 通信状況とを基にして、前記第 1 スitchおよび前記第 2 スitchから、障害の発生したスitchを検知する

処理を実行させることを特徴とする障害検知プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、監視装置等に関する。

【背景技術】

【0002】

クラウドの普及に伴って、データセンター（DC：Data Center）の基盤となる DC ネットワークには、今まで以上に高い品質が求められている。DC ネットワークでは、スitch等のネットワーク機器が障害アラートを発しないにも関わらず、誤動作するサイレント障害が発生する場合がある。このサイレント障害は、その発見が認識されにくいいため、障害復旧が遅延し、多くのサービスに影響を及ぼす恐れがある。

10

20

30

40

50

【0003】

図9は、サイレント障害の一例を説明するための図である。図9に示す例では、スイッチ4, 5が、監視装置6に接続されている。スイッチ4は、コントロールプレーン4aと、データプレーン4bとを有する。コントロールプレーン4aは、スイッチ4全体を制御する制御部である。データプレーン4bは、実際にデータ通信を司るASIC (Application Specific Integrated Circuit: 特定用途向け集積回路) である。スイッチ5には、スイッチ4と同様にして、コントロールプレーン5aと、データプレーン5bとが含まれる。

【0004】

たとえば、スイッチ4のデータプレーン4bに異常が発生し、通信に支障をきたしているが、コントロールプレーン4aが正常である場合には、サイレント障害となる。ここで、コントロールプレーン4aが正常に動作している場合、監視装置6が、SNMPリクエストをスイッチ4に送信しても、異常を示すアラートが、監視装置6に通知されず、監視装置6は、SNMPリクエストによって、データプレーン4bの障害を検知できない。

10

【0005】

上記のサイレント障害を検知する従来技術として、従来技術1, 2がある。従来技術1では、監視装置から、監視対象装置に対してテストデータを定期的送信し、応答の有無で異常(サイレント障害等)を検知する。

【0006】

従来技術2では、監視装置が、各監視対象装置の情報を定期的に収集し、収集した情報を基にして、システムの管理者が、通常時のネットワークの振る舞いを定義しておき、通常時の振る舞いとの違いや兆候を基にして異常(サイレント障害等)を検知する。

20

【先行技術文献】

【特許文献】

【0007】

【文献】特開2020-88786号公報

【文献】特開2011-211350号公報

【発明の概要】

【発明が解決しようとする課題】

【0008】

上述した従来技術では、効率よくサイレント障害を検知することができないという問題がある。

30

【0009】

たとえば、従来技術1をそのまま、大規模なネットワークに適用すると、テストデータによってトラフィックの量が増加してしまうという問題がある。また、従来技術2では、通常時のネットワークの振る舞いを定義する管理者の負担が大きく、運用コストもかかる。

【0010】

1つの側面では、本発明は、効率よくサイレント障害を検知することができる監視装置、障害検知方法および障害検知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】

40

【0011】

第1の案では、監視装置は、取得部と、検知部とを有する。取得部は、ネットワークに含まれる複数のスイッチのうち、監視対象とする第1スイッチと、第2スイッチと、他の監視スイッチとをそれぞれ仮想ネットワークで接続した監視スイッチから、第1スイッチとの第1通信状況、第2スイッチとの第2通信状況、他の監視スイッチとの第3通信状況とを取得する。検知部は、第1通信状況と、第2通信状況と、第3通信状況とを基にして、第1スイッチおよび第2スイッチから、障害の発生したスイッチを検知する。

【発明の効果】

【0012】

効率よくサイレント障害を検知することができる。

50

【図面の簡単な説明】**【 0 0 1 3 】**

【図 1】図 1 は、本実施例に係る監視システムを示す図である。

【図 2】図 2 は、IP SLA 機能を説明するための図である。

【図 3】図 3 は、本実施例に係る監視装置の構成を示す機能ブロック図である。

【図 4】図 4 は、パターンテーブルのデータ構造の一例を示す図である。

【図 5】図 5 は、判定ポリシーテーブルのデータ構造の一例を示す図である。

【図 6】図 6 は、メッセージ送信による経路切り替えの一例を説明するための図である。

【図 7】図 7 は、本実施例に係る監視装置の処理手順を示すフローチャートである。

【図 8】図 8 は、実施例の監視装置と同様の機能を実現するコンピュータのハードウェア構成の一例を示す図である。

10

【図 9】図 9 は、サイレント障害の一例を説明するための図である。

【発明を実施するための形態】**【 0 0 1 4 】**

以下に、本願の開示する監視装置、障害検知方法および障害検知プログラムの実施例を図面に基づいて詳細に説明する。なお、この実施例によりこの発明が限定されるものではない。

【実施例】**【 0 0 1 5 】**

図 1 は、本実施例に係る監視システムの一例を示す図である。図 1 に示すように、この監視システム 1 は、コアスイッチ 10 A、10 B、フロアスイッチ 20、監視スイッチ 30 A、30 B、監視装置 100 を有する。

20

【 0 0 1 6 】

コアスイッチ 10 A、10 B、フロアスイッチ 20、監視スイッチ 30 A、30 B はそれぞれ無線 LAN (Local Area Network) 又は有線 LAN によって相互に接続される。また、図示を省略するが、コアスイッチ 10 A、10 B、フロアスイッチ 20、監視スイッチ 30 A、30 B は、無線 LAN 又は有線 LAN によって、ネットワーク内の他のスイッチ、端末装置に接続される。

【 0 0 1 7 】

コアスイッチ 10 A は、ネットワーク内でパケット転送、中継を行うネットワークスイッチである。たとえば、コアスイッチ 10 A は、ルーティングテーブルを保持しており、コアスイッチ 10 B、他のスイッチ、端末装置からパケットを受信した場合には、ルーティングテーブルを基にして、データの転送、中継を行う。コアスイッチ 10 A は、スイッチング機能も有する。

30

【 0 0 1 8 】

コアスイッチ 10 B は、ネットワーク内でパケット転送、中継を行うネットワークスイッチである。たとえば、コアスイッチ 10 B は、ルーティングテーブルを保持しており、コアスイッチ 10 A、他のスイッチ、端末装置からパケットを受信した場合には、ルーティングテーブルを基にして、データの転送、中継を行う。コアスイッチ 10 B は、スイッチング機能も有する。

40

【 0 0 1 9 】

フロアスイッチ 20 は、ネットワークの中枢部と末端部との橋渡しを行うネットワークスイッチである。

【 0 0 2 0 】

監視スイッチ 30 A は、IP SLA 機能を備え、コアスイッチ 10 A、10 B を経由してフロアスイッチ 20 に到達する VLAN (Virtual Local Area Network) を作成し、コアスイッチ 10 A、10 B、フロアスイッチ 20、監視スイッチ 30 B を監視する。

【 0 0 2 1 】

監視スイッチ 30 B は、IP SLA 機能を備え、コアスイッチ 10 A、10 B を経由してフロアスイッチ 20 に到達する VLAN を作成し、コアスイッチ 10 A、10 B、フ

50

コアスイッチ 20、監視スイッチ 30 A を監視する。

【0022】

図 2 は、IP SLA 機能を説明するための図である。一例として、監視スイッチ 30 A と、監視対象としてコアスイッチ 10 A とを用いて説明を行う。監視スイッチ 30 A は、監視パケットをコアスイッチ 10 A に送信し、コアスイッチ 10 A からの応答を基にして、コアスイッチ 10 A のアラートの発生の有無を判定する。以下では説明を省略するが、監視スイッチ 30 A とコアスイッチ 10 A とは、VLAN を介して、監視パケットに関する情報をやり取りする。

【0023】

監視スイッチ 30 A は、監視パケットを送信し、コアスイッチ 10 A から応答を受信した場合には、コアスイッチ 10 A にアラートが発生していないと判定する。

10

【0024】

一方、監視スイッチ 30 A は、監視パケットをコアスイッチ 10 A に送信し、コアスイッチ 10 A から応答を受信しない場合には、コアスイッチ 10 A にアラートが発生したと判定し、アラート情報を、監視装置 100 に送信する。アラート情報の通信には、SYSLLOG / SNMP trap 等のプロトコルが用いられる。

【0025】

監視スイッチ 30 A は、他の監視対象となるコアスイッチ 10 B、フロアスイッチ 20、監視スイッチ 30 B についても、VLAN を介して、監視パケットに関する情報をやり取りすることで、アラートの発生の有無を判定し、アラートが発生した場合には、アラート情報を、監視装置 100 に送信する。

20

【0026】

アラート情報には、送信元の監視スイッチ 30 A の情報と、アラートの発生した監視対象の情報が設定される。監視スイッチ 30 A は、アラートの発生した監視対象を検知するたびに、アラート情報を、監視装置 100 に送信する。

【0027】

監視スイッチ 30 B は、監視スイッチ 30 A と同様にして、監視パケットを監視対象（コアスイッチ 10 A、10 B、フロアスイッチ 20、監視スイッチ 30 A）に送信し、監視対象からの応答を基にして、監視対象のアラートの発生の有無を判定する。監視スイッチ 30 B は、監視対象にアラートが発生したと判定した場合には、アラート情報を、監視装置 100 に送信する。

30

【0028】

監視装置 100 は、監視スイッチ 30 A、30 B からアラート情報を受信した場合に、アラート情報を基にして、サイレント障害の発生した監視対象のスイッチを検知する装置である。監視装置 100 は、サイレント障害の発生した監視対象のスイッチを検知すると、検知したスイッチに対して、メッセージを送信することで、監視対象のポートを閉塞させる。たとえば、ネットワークが冗長化されていれば、かかる処理を実行することで、自動的に、サイレント障害のスイッチを検知して、ネットワークを障害から復旧させることができる。

【0029】

次に、監視装置 100 の構成の一例について説明する。図 3 は、本実施例に係る監視装置の構成を示す機能ブロック図である。図 3 に示すように、この監視装置 100 は、通信部 110 と、入力部 120 と、表示部 130 と、記憶部 140、制御部 150 とを有する。

40

【0030】

通信部 110 は、ネットワークを介して、監視スイッチ 30 A、30 B との間で情報の送受信を行う。たとえば、通信部 110 は、NIC (Network Interface Card) 等によって実現される。

【0031】

入力部 120 は、各種の情報を、入力する入力装置である。入力部 120 は、キーボードやマウス、タッチパネル等に対応する。

50

【 0 0 3 2 】

表示部 1 3 0 は、制御部 1 5 0 から出力される情報を表示する表示装置である。表示部 1 3 0 は、液晶ディスプレイ、有機 E L (Electro Luminescence) ディスプレイ、タッチパネル等に対応する。

【 0 0 3 3 】

記憶部 1 4 0 は、登録テーブル 1 4 1、パターンテーブル 1 4 2、判定ポリシーテーブル 1 4 3 を有する。記憶部 1 4 0 は、たとえば、R A M (Random Access Memory)、フラッシュメモリ (Flash Memory) 等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。

【 0 0 3 4 】

登録テーブル 1 4 1 は、監視スイッチ 3 0 A , 3 0 B から送信されるアラート情報を保持するテーブルである。アラート情報には、このアラート情報の送信元となる監視スイッチの識別情報 (I P < Internet Protocol > アドレス、M A C < Media Access Control > アドレス等) と、アラートの発生した監視対象のスイッチの識別情報 (I P アドレス、M A C アドレス等) が含まれる。

【 0 0 3 5 】

パターンテーブル 1 4 2 は、アラートの発生した監視対象と、アラートの発生していない監視対象との組み合わせに対応するパターンを定義するテーブルである。図 4 は、パターンテーブルのデータ構造の一例を示す図である。図 4 に示すように、このパターンテーブル 1 4 2 は、アラート発生箇所と、パターンとを対応付ける。アラート発生箇所は、監視パケットによってアラートが検出されたスイッチを示す。ここではアラート発生箇所として、監視スイッチ (監視スイッチ 3 0 A , 3 0 B)、コアスイッチ 1 0 A、フロアスイッチ 2 0 を用いて説明する。

【 0 0 3 6 】

たとえば、監視スイッチ 3 0 A から送信されたアラート情報において監視スイッチ 3 0 B にアラートが発生しておらず、かつ、監視スイッチ 3 0 B から送信されたアラート情報において監視スイッチ 3 0 A にアラートが発生していない場合に、パターンテーブル 1 4 2 の監視スイッチの判定が「 」となる。

【 0 0 3 7 】

一方、監視スイッチ 3 0 A から送信されたアラート情報において監視スイッチ 3 0 B にアラートが発生している場合、または、監視スイッチ 3 0 B から送信されたアラート情報において監視スイッチ 3 0 A にアラートが発生している場合には、パターンテーブル 1 4 2 の監視スイッチの判定が「 x 」となる。

【 0 0 3 8 】

監視スイッチ 3 0 A から送信されたアラート情報においてコアスイッチ 1 0 A にアラートが発生しておらず、かつ、監視スイッチ 3 0 B から送信されたアラート情報においてコアスイッチ 1 0 A にアラートが発生していない場合に、パターンテーブル 1 4 2 のコアスイッチの判定が「 」となる。

【 0 0 3 9 】

監視スイッチ 3 0 A から送信されたアラート情報においてコアスイッチ 1 0 A にアラートが発生している場合、または、監視スイッチ 3 0 B から送信されたアラート情報においてコアスイッチ 1 0 A にアラートが発生している場合には、パターンテーブル 1 4 2 のコアスイッチの判定が「 x 」となる。

【 0 0 4 0 】

監視スイッチ 3 0 A から送信されたアラート情報においてフロアスイッチ 2 0 にアラートが発生しておらず、かつ、監視スイッチ 3 0 B から送信されたアラート情報においてフロアスイッチ 2 0 にアラートが発生していない場合に、パターンテーブル 1 4 2 のフロアスイッチの判定が「 」となる。

【 0 0 4 1 】

監視スイッチ 3 0 A から送信されたアラート情報においてフロアスイッチ 2 0 にアラート

10

20

30

40

50

トが発生している場合、または、監視スイッチ 3 0 B から送信されたアラート情報においてフロアスイッチ 2 0 にアラートが発生している場合には、パターンテーブル 1 4 2 のコアシッチの判定が「×」となる。

【 0 0 4 2 】

ここで、図 4 に示すように、監視スイッチの判定が「」、コアシッチ 1 0 A の判定が「」、フロアスイッチ 2 0 の判定が「×」の場合には、パターン「A」となる。監視スイッチの判定が「」、コアシッチ 1 0 A の判定が「×」、フロアスイッチ 2 0 の判定が「」の場合には、パターン「B」となる。

【 0 0 4 3 】

監視スイッチの判定が「×」、コアシッチ 1 0 A の判定が「」、フロアスイッチ 2 0 の判定が「」の場合には、パターン「C」となる。監視スイッチの判定が「×」、コアシッチ 1 0 A の判定が「×」、フロアスイッチ 2 0 の判定が「」の場合には、パターン「D」となる。

【 0 0 4 4 】

監視スイッチの判定が「」、コアシッチ 1 0 A の判定が「×」、フロアスイッチ 2 0 の判定が「×」の場合には、パターン「E」となる。監視スイッチの判定が「×」、コアシッチ 1 0 A の判定が「」、フロアスイッチ 2 0 の判定が「×」の場合には、パターン「F」となる。監視スイッチの判定が「×」、コアシッチ 1 0 A の判定が「×」、フロアスイッチ 2 0 の判定が「×」の場合には、パターン「G」となる。

【 0 0 4 5 】

ここで、図 4 で説明したパターンテーブル 1 4 2 は、コアシッチ 1 0 A に対応するパターンテーブルであるが、コアシッチ 1 0 B に対応するパターンテーブルも同様となる。説明の便宜上、一部について説明すると、監視スイッチ 3 0 A から送信されたアラート情報においてコアシッチ 1 0 B にアラートが発生しておらず、かつ、監視スイッチ 3 0 B から送信されたアラート情報においてコアシッチ 1 0 B にアラートが発生していない場合に、パターンテーブル（コアシッチ 1 0 B に対応するパターンテーブル）のコアシッチの判定が「」となる。

【 0 0 4 6 】

監視スイッチ 3 0 A から送信されたアラート情報においてコアシッチ 1 0 B にアラートが発生している場合、または、監視スイッチ 3 0 B から送信されたアラート情報においてコアシッチ 1 0 B にアラートが発生している場合には、パターンテーブル（コアシッチ 1 0 B に対応するパターンテーブル）のコアシッチの判定が「×」となる。

【 0 0 4 7 】

そして、監視スイッチ、コアシッチ 1 0 A、フロアスイッチ 2 0 の「」、「×」の組み合わせによって、コアシッチ 1 0 B に関するパターンが特定される。

【 0 0 4 8 】

判定ポリシーテーブル 1 4 3 は、パターンに応じたサイレント障害の要因を判定するための情報を保持する。図 5 は、判定ポリシーテーブルのデータ構造の一例を示す図である。図 5 に示すように、この判定ポリシーテーブル 1 4 3 は、パターンと、要因とを対応付ける。パターンは、図 4 で説明したパターン A ~ G に対応する。要因は、サイレント障害の要因を示す。ここでは一例として、コアシッチ 1 0 A に関するパターンを用いて説明を行う。

【 0 0 4 9 】

たとえば、パターン A の要因は、「フロアスイッチ 2 0 またはコアシッチ 1 0 A（コアシッチ 1 0 A のルーティング機能）に障害発生」となる。パターン B の要因は、「コアシッチ 1 0 A に障害発生」となる。

【 0 0 5 0 】

パターン C の要因は、「コアシッチ 1 0 A（コアシッチ 1 0 A のスイッチング機能）に障害発生」となる。パターン D の要因は、「コアシッチ 1 0 A に障害発生」となる。

【 0 0 5 1 】

10

20

30

40

50

パターンEの要因は、「コアシッチ10A(コアシッチ10Aのルーティング機能)に障害発生」となる。パターンFの要因は、「コアシッチ10A(コアシッチ10Aのルーティング機能、スイッチング機能)に障害発生」となる。パターンGの要因は、「コアシッチ10Aに障害発生」となる。

【0052】

図5では、コアシッチ10Aに関するパターンを用いて説明を行った。図示を省略するが、コアシッチ10Bのパターンに対応する要因は、上記説明のコアシッチ10Aを、コアシッチ10Bに置き換えたものとなる。

【0053】

図3の説明に戻る。制御部150は、取得部151と、検知部152と、送信部153とを有する。制御部150は、たとえば、CPU(Central Processing Unit)やMPU(Micro Processing Unit)により実現される。また、制御部150は、例えばASIC(Application Specific Integrated Circuit)やFPGA(Field Programmable Gate Array)等の集積回路により実行されてもよい。

【0054】

取得部151は、監視スイッチ30A,30Bから、アラート情報を取得する。取得部151は、取得したアラート情報を、登録テーブル141に登録する。取得部151は、アラート情報を取得する度に、上記処理を繰り返し実行する。

【0055】

検知部152は、登録テーブル141に登録されたアラート情報の組み合わせと、パターンテーブル142とを基にして、パターンを特定する。検知部152は、特定したパターンと、判定ポリシータブル143とを基にして、サイレント障害の要因となる箇所を検知し、検知結果を送信部153に出力する。検知部152は、検知結果を表示部130に出力して、表示させてもよい。

【0056】

たとえば、検知部152は、登録テーブル141に登録された各アラート情報を参照し、監視スイッチ(30A,30B)、コアシッチ10A、コアシッチ10B、フロアスイッチについて、「」か「」かの判定を実行する。検知部152が「」か「」かを判定する処理は、図4で説明した方法に対応する。

【0057】

検知部152は、「」、「」の判定結果の組み合わせと、パターンテーブル142とを基にして、パターンを特定する。検知部152が、パターンを特定する処理は、図4で説明した方法に対応する。なお、検知部152は、全ての判定結果が「」となる場合には、サイレント障害が発生していないものとして、いずれかの判定結果が「」となるまで、上記処理を繰り返し実行する。

【0058】

検知部152は、パターン(図4で説明したパターンA~Gのいずれか)を特定すると、特定したパターンと、判定ポリシータブル143とを基にして、サイレント障害の要因となる箇所を検知し、検知した結果を、送信部153に出力する。検知部152は、サイレント障害の要因となる箇所に加えて、ルーティング機能、スイッチング機能に障害があるのかを合わせて出力してもよい。

【0059】

送信部153は、検知部152の検知結果を基にして、サイレント障害の要因となる箇所となるスイッチに対してメッセージを送信する。メッセージには、あて先となるスイッチの識別情報が設定されるものとする。

【0060】

送信部153のメッセージを受信したスイッチは、他のスイッチとの通信を停止する処理を行う。たとえば、送信部153は、監視スイッチ30A,30Bを介して、該当するスイッチにメッセージを送信する。係る処理が実行されることで、コアシッチ10A,10Bによる経路の切り替えが発生する。

10

20

30

40

50

【 0 0 6 1 】

図 6 は、メッセージ送信による経路切り替えの一例を説明するための図である。たとえば、監視装置 1 0 0 が、コアスイッチ 1 0 A にサイレント障害が発生したことを検知し、送信部 1 5 3 が、メッセージをコアスイッチ 1 0 A に送信した場合について説明する。

【 0 0 6 2 】

監視スイッチ 3 0 A は、監視装置 1 0 0 の送信部 1 5 3 からメッセージを受信すると、メッセージをコアスイッチ 1 0 A に転送する。コアスイッチ 1 0 A は、メッセージを受信すると、所定のスクリプトを実行し、コアスイッチ 1 0 A のポートをダウンさせる。コアスイッチ 1 0 A のポートがダウンすることで、それまでコアスイッチ 1 0 A を経由していたパケットが、コアスイッチ 1 0 B を経由して転送されるようになり、経路の切り替えが発生する。これによって、一部のコアスイッチにサイレント障害が発生しても、ネットワークを自動的に復旧させることができる。

10

【 0 0 6 3 】

次に、本実施例に係る監視装置 1 0 0 の処理手順の一例について説明する。図 7 は、本実施例に係る監視装置の処理手順を示すフローチャートである。図 7 に示すように、監視装置 1 0 0 の取得部 1 5 1 は、監視スイッチ 3 0 A , 3 0 B からアラート情報を受信した場合に、アラート情報を登録テーブル 1 4 1 に登録する (ステップ S 1 0 1) 。

【 0 0 6 4 】

監視装置 1 0 0 の検知部 1 5 2 は、登録テーブル 1 4 1 の各アラート情報と、パターンテーブル 1 4 2 とを比較して、パターンを特定する (ステップ S 1 0 2) 。検知部 1 5 2 は、パターンと判定ポリシーテーブル 1 4 3 とを基にして、サイレント障害の発生したスイッチを検知する (ステップ S 1 0 3) 。

20

【 0 0 6 5 】

監視装置 1 0 0 の送信部は、サイレント障害の発生したスイッチに対してメッセージを送信し、送信先のスイッチのポートを閉塞させる (ステップ S 1 0 4) 。

【 0 0 6 6 】

監視装置 1 0 0 は、処理を継続するか否かを判定する (ステップ S 1 0 5) 。監視装置 1 0 0 は、処理を継続する場合には (ステップ S 1 0 5 , Y e s) 、ステップ S 1 0 1 に移行する。監視装置 1 0 0 は、処理を継続しない場合には (ステップ S 1 0 5 , N o) 、処理を終了する。

30

【 0 0 6 7 】

次に、本実施例に係る監視装置 1 0 0 の効果について説明する。監視装置 1 0 0 は、監視対象となるスイッチを監視する監視スイッチ 3 0 A , 3 0 B から、アラート情報を取得し、アラートの発生したスイッチの組み合わせを基にして、サイレント障害の発生したスイッチを検知する。これによって、効率的に監視対象となるスイッチのサイレント障害を検知することができる。

【 0 0 6 8 】

たとえば、監視装置 1 0 0 は、アラートの発生したスイッチの組み合わせを、パターン A ~ パターン G のいずれかに分類し、分類したパターンと、判定ポリシーテーブル 1 4 3 とを基にして、サイレント障害の発生したスイッチを検知する。これにより、精度よく、サイレント障害に対応する箇所を特定することができる。

40

【 0 0 6 9 】

監視装置 1 0 0 は、サイレント障害の発生したスイッチを検知した場合に、検知したスイッチに対して、メッセージを送信し、スイッチのポートを閉塞させる。冗長化されたネットワークにおいて、かかる処理を実行することで、サイレント障害が発生した場合でも、ネットワークを自動的に復旧させることができる。

【 0 0 7 0 】

次に、上記実施例に示した監視装置 1 0 0 と同様の機能を実現するコンピュータのハードウェア構成の一例について説明する。図 8 は、実施例の監視装置と同様の機能を実現するコンピュータのハードウェア構成の一例を示す図である。

50

【0071】

図8に示すように、コンピュータ200は、各種演算処理を実行するCPU201と、ユーザからのデータの入力を受け付ける入力装置202と、ディスプレイ203とを有する。また、コンピュータ200は、有線または無線ネットワークを介して、外部装置等との間でデータの授受を行う通信装置204と、インタフェース装置205とを有する。また、コンピュータ200は、各種情報を一時記憶するRAM206と、ハードディスク装置207とを有する。そして、各装置201~207は、バス208に接続される。

【0072】

ハードディスク装置207は、取得プログラム207a、検知プログラム207b、送信プログラム207cを有する。また、CPU201は、各プログラム207a~207cを読み出してRAM206に展開する。

10

【0073】

取得プログラム207aは、取得プロセス206aとして機能する。検知プログラム207bは、検知プロセス206bとして機能する。送信プログラム207cは、送信プロセス206cとして機能する。

【0074】

取得プロセス206aの処理は、取得部151の処理に対応する。検知プロセス206bの処理は、検知部152の処理に対応する。送信プロセス206cの処理は、送信部153の処理に対応する。

【0075】

なお、各プログラム207a~207dについては、必ずしも最初からハードディスク装置207に記憶させておかなくても良い。例えば、コンピュータ200に挿入されるフレキシブルディスク(FD)、CD-ROM、DVD、光磁気ディスク、ICカードなどの「可搬用の物理媒体」に各プログラムを記憶させておく。そして、コンピュータ200が各プログラム207a~207dを読み出して実行するようにしてもよい。

20

【符号の説明】

【0076】

- 100 監視装置
- 110 通信部
- 120 入力部
- 130 表示部
- 140 記憶部
- 141 登録テーブル
- 142 パターンテーブル
- 143 判定ポリシーテーブル
- 150 制御部
- 151 取得部
- 152 検知部
- 153 送信部

30

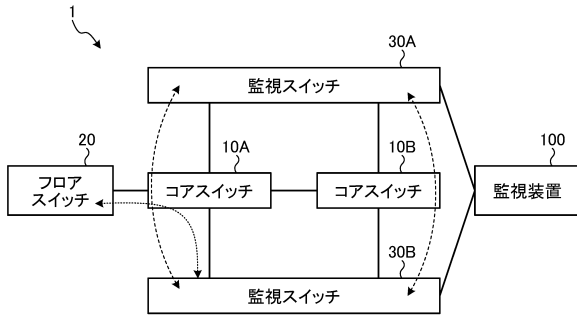
40

50

【図面】

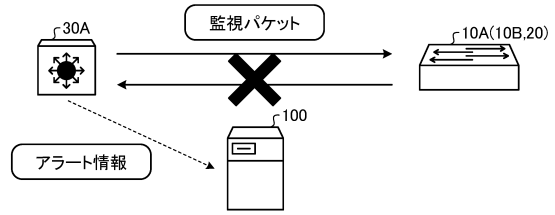
【図 1】

本実施例に係る監視システムを示す図



【図 2】

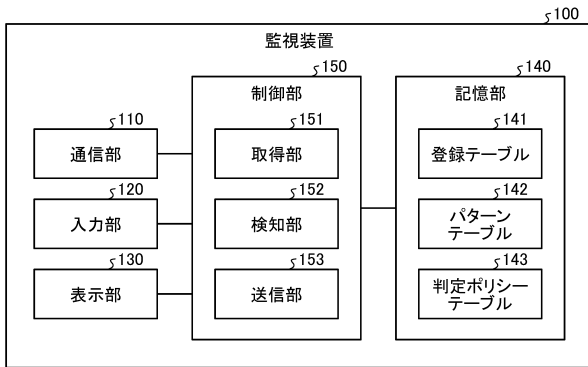
IP SLA機能を説明するための図



10

【図 3】

本実施例に係る監視装置の構成を示す機能ブロック図



【図 4】

パターンテーブルのデータ構造の一例を示す図

アラート発生箇所	パターン						
	A	B	C	D	E	F	G
監視スイッチ(30A,30B)	○	○	×	×	○	×	×
コアスイッチ10A	○	×	○	×	×	○	×
フロアスイッチ20	×	○	○	○	×	×	×

20

30

40

50

【 図 5 】

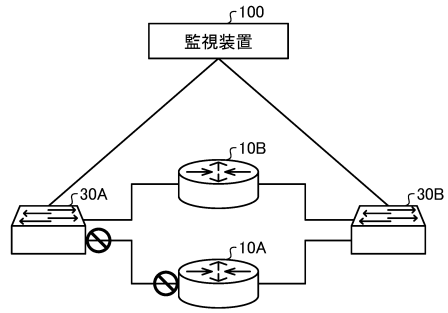
判定ポリシーテーブルのデータ構造の一例を示す図

パターン	要因
A	フロアスイッチまたはコアスイッチ（ルーティング機能）に障害発生
B	コアスイッチに障害発生
C	コアスイッチ（スイッチング機能）に障害発生
D	コアスイッチに障害発生
E	コアスイッチ（ルーティング機能）に障害発生
F	コアスイッチ（ルーティング機能、スイッチング機能）に障害発生
G	コアスイッチに障害発生

143

【 図 6 】

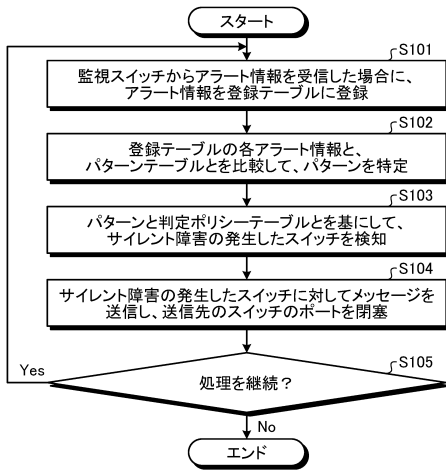
メッセージ送信による経路切り替えの一例を説明するための図



10

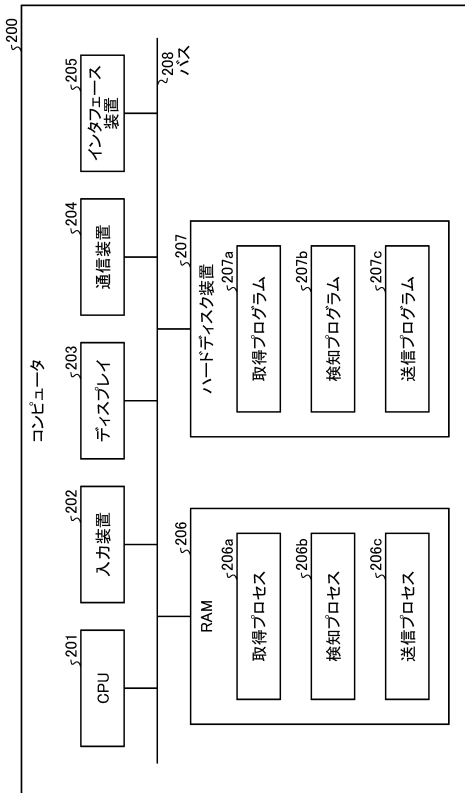
【 図 7 】

本実施例に係る監視装置の処理手順を示すフローチャート



【 図 8 】

実施例の監視装置と同様の機能を実現するコンピュータのハードウェア構成の一例を示す図



20

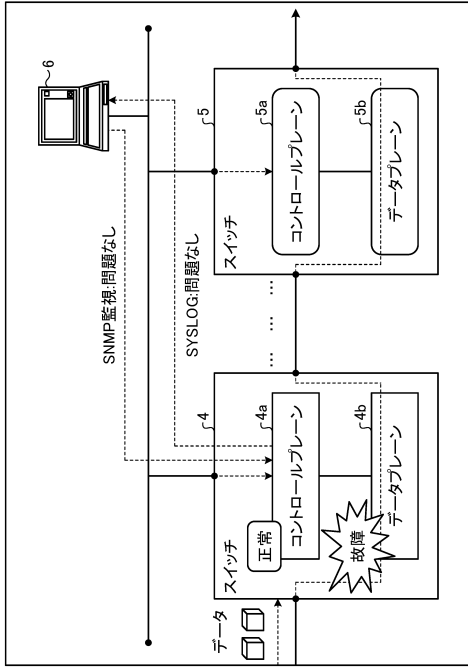
30

40

50

【 図 9 】

サイレント障害の一例を説明するための図



10

20

30

40

50

フロントページの続き

神奈川県川崎市中原区中丸子 1 3 番地 2 株式会社富士通エフサス内

審査官 和平 悠希

(58)調査した分野 (Int.Cl., D B名)

H 0 4 L 4 3 / 0 0