(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4412031号
(P4412031)
(45)発行日　平成22年2月10日(2010.2.10)　(24)登録日　平成21年11月27日(2009.11.27)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00　３５１Ｍ

請求項の数 17　(全 26 頁)

(21)出願番号　特願2004-101827(P2004-101827)
(22)出願日　平成16年3月31日(2004.3.31)
(65)公開番号　特開2005-285040(P2005-285040A)
(43)公開日　平成17年10月13日(2005.10.13)
審査請求日　平成19年1月15日(2007.1.15)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１５年度通信・放送機構　委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088812
弁理士　▲柳▼川　信
(72)発明者　西岡　到
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　加美　伸治
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　高瀬　勤

最終頁に続く

(54)【発明の名称】ネットワーク監視システム及びその方法、プログラム

(57)【特許請求の範囲】
【請求項１】
複数のネットワーク機器の情報を収集して監視する監視システムであって、
前記ネットワーク機器の各々から収集されるべき初期監視情報およびそれに関連する監視情報を監視ルールとして予め格納した監視ルール格納手段と、
前記ネットワーク機器から収集される初期監視情報を処理することによって障害の予兆を発見する予兆発見手段と、
前記予兆発見手段による予兆発見に応答して前記初期監視情報に関連し前記障害の原因を特定する監視情報を前記監視ルール格納手段から検索して、この検索した前記監視情報を収集する収集監視情報決定手段と、
前記収集監視情報決定手段により収集された監視情報により障害詳細の判定処理をなす事後発見手段と、
を含むことを特徴とするネットワーク監視システム。
【請求項２】
前記初期監視情報は時系列に変化する時系列監視情報であり、
前記予兆発見手段は、現在までに収集されている時系列監視情報を統計処理する手段と、この統計処理された結果と最新の収集情報とを比較判定することにより、障害の予兆を検出する手段とを有すること特徴とする請求項１記載のネットワーク監視システム。
【請求項３】
前記初期監視情報は時系列に変化する時系列監視情報であり、

前記予兆発見手段は、現在までに収集されている複数の時系列監視情報の相関関係を統計処理する手段と、この統計処理された結果と最新の収集情報とを比較判定することにより、障害の予兆を検出する手段とを有すること特徴とする請求項１記載のネットワーク監視システム。

【請求項４】

前記関連する監視情報は前記ネットワーク機器が保持する経路情報であり、前記事後発見手段は前記経路情報を検査することにより、経路の正常性を確認するようにしたこと特徴とする請求項１～３いずれか記載のネットワーク監視システム。

【請求項５】

前記関連する監視情報は整数型の情報（整数型監視情報）であり、事後発見手段は整数値の判定を行うようにしたことを特徴とする請求項１～３いずれか記載のネットワーク監視システム。

【請求項６】

前記格納手段に格納されている前記初期監視情報に関連する監視情報は、順次詳細な関連する監視情報として、ツリー構造とされており、前記収集監視情報決定手段は、前記ツリー構造からより詳細な関連する監視情報を順次検索して当該監視情報の収集を決定し、前記事後発見手段は、収集された監視情報により障害詳細の判定処理をなすようにしたことを特徴とする請求項１～５いずれか記載のネットワーク監視システム。

【請求項７】

前記監視情報の収集はＳＮＭＰ（Simple Network Management Protocol）を用いて行われ、前記事後発見手段は、前記判定処理時にＭＩＢ（Management Information Base ）に定義されるデータ形式に基づいて判定処理機能を決定するようにしたことを特徴とする請求項１～６いずれか記載のネットワーク監視システム。

【請求項８】

前記収集監視情報決定手段により収集を指示された監視情報の判定の結果が正常であった場合には、前記監視情報の収集を終了すると共に、前記監視情報を監視するトリガとなった監視情報の異常状態を解放する手段を、更に含むことを特徴とする請求項１～７いずれか記載のネットワーク監視システム。

【請求項９】

複数のネットワーク機器の情報を収集して監視する監視方法であって、

前記ネットワーク機器の各々から収集されるべき初期監視情報およびそれに関連する監視情報を監視ルールとして予め格納した監視ルール格納手段を準備しておき、

前記ネットワーク機器から収集される前記初期監視情報を処理することによって障害の予兆を発見する予兆発見ステップと、

前記予兆発見ステップにおける予兆発見に応答して前記初期監視情報に関連し前記障害の原因を特定する監視情報を前記監視ルール格納手段から検索して、この検索した前記監視情報を収集する収集監視情報決定ステップと、

前記収集監視情報決定ステップにより収集された監視情報により障害詳細の判定処理をなす事後発見ステップと、

を含むことを特徴とするネットワーク監視方法。

【請求項１０】

前記初期監視情報は時系列に変化する時系列監視情報であり、

前記予兆発見ステップは、現在までに収集されている時系列監視情報を統計処理するステップと、この統計処理された結果と最新の収集情報とを比較判定することにより、障害の予兆を検出するステップとを有すること特徴とする請求項９記載のネットワーク監視方法。

【請求項１１】

前記初期監視情報は時系列に変化する時系列監視情報であり、

前記予兆発見ステップは、現在までに収集されている複数の時系列監視情報の相関関係を統計処理するステップと、この統計処理された結果と最新の収集情報とを比較判定する

ことにより、障害の予兆を検出するステップとを有すること特徴とする請求項９記載のネットワーク監視方法。
【請求項１２】
前記関連する監視情報は前記ネットワーク機器が保持する経路情報であり、前記事後発見ステップは前記経路情報を検査することにより、経路の正常性を確認するようにしたこと特徴とする請求項９～１１いずれか記載のネットワーク監視方法。
【請求項１３】
前記関連する監視情報は整数型の情報（整数型監視情報）であり、事後発見ステップは整数値の判定を行うようにしたことを特徴とする請求項９～１１いずれか記載のネットワーク監視方法。
【請求項１４】
前記格納手段に格納されている前記初期監視情報に関連する監視情報は、順次詳細な関連する監視情報として、ツリー構造とされており、前記収集監視情報決定ステップは、前記ツリー構造からより詳細な関連する監視情報を順次検索して当該監視情報の収集を決定し、前記事後発見ステップは、収集された監視情報により障害詳細の判定処理をなすようにしたことを特徴とする請求項９～１３いずれか記載のネットワーク監視方法。
【請求項１５】
前記監視情報の収集はＳＮＭＰ（Simple Network Management Protocol）を用いて行われ、前記事後発見ステップは、前記判定処理時にＭＩＢ（Management Information Base）に定義されるデータ形式に基づいて判定処理機能を決定するようにしたことを特徴とする請求項９～１４いずれか記載のネットワーク監視方法。
【請求項１６】
前記収集監視情報決定ステップにより収集を指示された監視情報の判定の結果が正常であった場合には、前記監視情報の収集を終了すると共に、前記監視情報を監視するトリガとなった監視情報の異常状態を解放するステップを、更に含むことを特徴とする請求項９～１５いずれか記載のネットワーク監視方法。
【請求項１７】
複数のネットワーク機器の情報を収集して監視する監視方法をコンピュータにより実行させるためのプログラムであって、
前記ネットワーク機器から収集される初期監視情報を処理することによって、障害の予兆を発見する処理と、
前記予兆発見に応答して前記初期監視情報に関連し前記障害の原因を特定する監視情報を監視ルール格納手段から検索して、この検索した前記監視情報を収集する処理と、
前記関連する監視情報により障害詳細の判定処理をなす事後発見処理と、
を含むことを特徴とするコンピュータ読取り可能なプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はネットワーク監視システム及びその方法、プログラムに関し、特に通信ネットワークにおける障害監視方式および障害情報分析方式に関するものである。
【背景技術】
【０００２】
近年の高度情報社会化により、データセンターなどでは様々なサービスを提供するサーバが絶えず稼動しており、これらを接続するために様々な種類にわたる膨大な数のネットワーク装置が導入されている。これらのネットワーク装置に障害があるとサービス利用者に迷惑をかけるだけではなく、サービス提供者が莫大な損失を被る。そのために、管理者が監視装置を使ってネットワーク装置を絶えず監視する必要がある。管理者は、監視しているネットワーク装置に障害があった場合、この障害の原因を特定して迅速に復旧する必要がある。
【０００３】

ネットワーク装置を監視する形態には、一般的に、ＳＮＭＰ（Simple Network Management Protocol）を使って監視する方法がある。この形態での監視情報の収集方法としては、定期的に装置の稼動状態をポーリングにより収集する方法、装置側に予め閾値を設定しておき閾値を超えるとアラームを上げるトラップによる方法がある。障害が発生した場合、上記２種類の収集方法を使って監視装置が集めた情報を元に管理者は障害原因の特定や影響範囲の分析を行う必要があるが、この作業を全て人手で行っており、分析に莫大な時間がかかるという問題がある。

【０００４】

この問題を解決するために、自動で障害情報の分析する技術が特許文献１に開示されている。この技術では、ネットワーク装置から収集した複数の情報をファジールールに基づいて、障害が発生しているかどうか、障害が発生していると判断した場合には、どの部分が障害となっているかを詳しく診断するというものである。

【０００５】

しかしながら、昨今の装置自体の複雑化およびネットワークの大規模化により、ネットワーク装置をきめ細やかに監視しようとすると、収集する監視情報の数が膨大になり、監視情報の収集のためにネットワーク自体に負荷をかけてしまうという問題が発生する。一方、ネットワークへの負荷を低減しようとすると、監視情報の量を減らさなければならず、詳細にネットワークの状態を管理者が把握することが難しくなるという問題が発生する。

【０００６】

この問題を解決するために、特許文献２では、予め限定された監視情報だけを収集し、この監視情報の判定に異常があった場合、予め関連づけされた監視情報を収集し、さらに判定するという動作を繰り返す方式が開示されている。また、その他の問題解決方法として、特許文献３では、過去の障害発生頻度の高い装置に対して優先的にポーリングにより監視情報を収集するという方式が開示されている。

【０００７】

特許文献２及び３の技術では、障害となったネットワーク装置や障害の項目のみを集中的に管理するので、ネットワークの負荷を軽減することが可能であるが、障害が発生してから動作を起こすため、障害に関連する情報が取得できない場合があり、障害の原因の分析ができない可能性がある。また、管理者が人手で分析をしなければならないという問題は改善されていない。

【０００８】

【特許文献１】特開平７－３０５４０号公報
【特許文献２】特開平８－０６５３０２号公報
【特許文献３】特開平４－２３９２４２号公報
【発明の開示】
【発明が解決しようとする課題】

【０００９】

上記した３つの従来技術の課題は、障害が発生してから動作を起こすため、すでに障害が発生しているネットワーク装置からは、監視情報が収集できない場合があるということである。例えば、データトラヒックによりネットワーク装置の負荷が非常に大きくなるといった問題が発生した場合、この装置から監視情報を収集しようとしても、ネットワーク装置は、負荷が大きいため、監視情報取得の要求にこたえられない。また、その他の例として、ネットワーク装置が何かの理由により再起動したとき、再起動前の情報が欠落しているため、管理者が再起動した理由を分析するための十分な情報を得ることができないという問題点がある。

【００１０】

本発明の目的は、ネットワーク装置に負荷をかけることなく、ネットワーク装置が障害となる前に関連情報を取得するネットワーク監視システム及びその方法、プログラムを提供することである。

【００１１】
また、本発明の他の目的は、情報収集の課程で、同時に障害原因や障害影響範囲の分析結果を管理者に通知するようにしたネットワーク監視システム及びその方法、プログラムを提供することである。
【課題を解決するための手段】
【００１２】
本発明によるネットワーク監視システムは、
複数のネットワーク機器の情報を収集して監視する監視システムであって、
前記ネットワーク機器の各々から収集されるべき初期監視情報およびそれに関連する監視情報を監視ルールとして予め格納した監視ルール格納手段と、
前記ネットワーク機器から収集される初期監視情報を処理することによって障害の予兆を発見する予兆発見手段と、
前記予兆発見手段による予兆発見に応答して前記初期監視情報に関連し前記障害の原因を特定する監視情報を前記監視ルール格納手段から検索して、この検索した前記監視情報を収集する収集監視情報決定手段と、
前記収集監視情報決定手段により収集された監視情報により障害詳細の判定処理をなす事後発見手段と、
を含むことを特徴とする。
【００１３】
本発明によるネットワーク監視方法は、
複数のネットワーク機器の情報を収集して監視する監視方法であって、
前記ネットワーク機器の各々から収集されるべき初期監視情報およびそれに関連する監視情報を監視ルールとして予め格納した監視ルール格納手段を準備しておき、
前記ネットワーク機器から収集される前記初期監視情報を処理することによって障害の予兆を発見する予兆発見ステップと、
前記予兆発見ステップにおける予兆発見に応答して前記初期監視情報に関連し前記障害の原因を特定する監視情報を前記監視ルール格納手段から検索して、この検索した前記監視情報を収集する収集監視情報決定ステップと、
前記収集監視情報決定ステップにより収集された監視情報により障害詳細の判定処理をなす事後発見ステップと、
を含むことを特徴とする。
【００１４】
本発明によるプログラムは、
複数のネットワーク機器の情報を収集して監視する監視方法をコンピュータにより実行させるためのプログラムであって、
前記ネットワーク機器から収集される初期監視情報を処理することによって、障害の予兆を発見する処理と、
前記予兆発見に応答して前記初期監視情報に関連し前記障害の原因を特定する監視情報を監視ルール格納手段から検索して、この検索した前記監視情報を収集する処理と、
前記関連する監視情報により障害詳細の判定処理をなす事後発見処理と、
を含むことを特徴とする。
【００１５】
本発明の作用を述べる。複数のネットワーク装置からの監視情報を取得する通信機能を有するネットワーク監視システムにおいて、監視情報収集部で、初期監視情報として連続量情報を収集し、監視情報判定部で、この連続量情報の統計的な振舞いを監視し、通常と異なる振舞いを検出した場合には、異常が発生する予兆を発見したとみなして、収集監視情報決定部で、監視ルールデータベースを参照して、監視情報収集部に対して、関連する複数の監視情報を収集する様指示する。そして、監視情報判定部で、その値を判定することにより、障害の原因を特定する。
【発明の効果】

【００１６】
本発明の第一の効果は、ネットワーク監視システムがネットワーク装置を監視するときに、ネットワーク装置およびネットワークに与える負荷を最小限に抑えることである。その理由は、監視情報全てを同時にネットワーク装置から取るのではなく、発生した管理情報のアラームに対して関連する必要最低限の監視情報を決定し、その決定に基づいた監視情報のみを必要な期間だけ収集する手段を有するためである。
【００１７】
本発明の第二の効果は、ネットワーク監視システムがネットワークの障害を迅速に発見できることである。その理由は、ネットワーク監視システムが障害の予兆を検出し、その予兆に関する障害を動的かつ詳細に監視し始めるためである。予兆に基づいて関連する情報を動的に監視し始めることにより、同時に監視している情報を削減できるため、これまで全てのパラメータを監視するときには３０分程度の監視間隔であったのに対し、本発明では、これまでと同程度の負荷で監視間隔を１分程度にまで短縮が実現できるためである。
【００１８】
本発明の第三の効果は、ネットワーク管理者が、ネットワークの障害に対して迅速に対処することできることである。その理由は、本発明のネットワーク管理システムでは、予兆発見、障害発見の後に、障害の原因特定および影響範囲を検査し、その結果をネットワーク管理者に報告するためである。
【発明を実施するための最良の形態】
【００１９】
以下に、図面を参照しつつ本発明の実施の形態について詳細に説明する。本発明では、図１における情報収集部１０１が情報を収集する手段として、ＩＥＴＦ（Internet Engineering Task Force ）で標準化されているＳＮＭＰ（Simple Network Management Protocol）を用いることを前提とする。本発明の説明では、ネットワーク監視システムは装置で、管理者はネットワーク監視システムを使ってネットワークを管理する人を表すものとする。
【００２０】
図１は本発明の第一の実施例におけるネットワーク監視システムならびに本発明のネットワーク監視システムを用いて監視される監視対象ネットワークを示すブロック図である。図１において、ネットワーク監視システム１００は、複数のネットワーク装置１１１から監視情報を収集する監視情報収集部１０１と、判定機能部１０３で予め定義された判定機能のいずれかを使って収集した監視情報に異常があるかどうかを判断する監視情報判定部１０２と、監視ルールを規定する監視ルールＤＢ（データベース）１０５と、次に収集する監視情報を監視ルールＤＢ１０５を参照して決定する収集監視情報決定部１０４と、監視システムが収集した情報やアラームの有無を保管するログ蓄積部１０６とを含んで構成されている。
【００２１】
ログ蓄積部１０６の情報には、監視サイト１２０にある監視端末１２１を通してネットワークを監視する管理者がアクセスすることができると共に、ログ蓄積部に異常情報が入力された場合には、監視端末１２１に自動的に通知される。
【００２２】
監視ルールＤＢ１０５の情報は、図２に示すように、複数の監視オブジェクトからなり、この監視オブジェクトのそれぞれには、管理者が監視している情報を識別するための監視情報名、監視情報収集部１０１がＳＮＭＰを使って監視情報を収集するためのＭＩＢ（Management Information Base ）オブジェクト名、監視情報の関係を示す監視ツリー番号、監視するネットワーク装置を示す監視ノードアドレス、監視時間を示すタイムアウト時間、収集した情報を判定するために利用する判定値、および次に監視をする監視情報を示す子監視ツリー番号が記載されている。
【００２３】

また、各監視情報の監視ツリー番号は、”１．１”や”１．１．１．１”のように、”．（ドット）”で区切られており、これにより親監視情報に異常があった場合に監視する子監視情報を関連付けることができる。この監視ツリーはこれまで発生した障害の経験を元に、管理者により予め構築されて、監視ルールＤＢ１０５に格納されているものとする。

【００２４】

収集した監視情報を分析する判定機能部１０３は、時系列情報判定機能１０３ａ、複数時系列情報判定機能１０３ｂ、整数型情報判定機能１０３ｃ、配列型情報判定機能１０３ｄからなる。これら判定機能の選択方法について説明する。

【００２５】

ＳＮＭＰが収集した監視情報がＭＩＢの表記形式であるＳＭＩ（Structure of Management Information ）であることから、本発明で監視する監視情報のデータ型は、Ｃｏｕｎｔｅｒ（時間に伴い増加する負でない整数）、Ｇａｕｇｅ（最大値を維持する負でない整数）、Ｉｎｔｅｇｅｒ（整数値）、ＩＰ　Ａｄｄｒｅｓｓ（ＩＰアドレス）、Ｐｈｙｓｉｃａｌ　Ａｄｄｒｅｓｓ（物理的なアドレスで、例として、ＭＡＣアドレスがある）および、Ｌｉｓｔ（他のデータ型の値を複数並べたリスト）とＴａｂｌｅ（Ｌｉｓｔを複数並べたもの）がある。

【００２６】

これらの型に従って、データ型がＣｏｕｎｔｅｒ、Ｇａｕｇｅであるならば時系列情報判定機能１０３ａが、単一のＩｎｔｅｇｅｒ、ＩＰ　Ａｄｄｒｅｓｓ、Ｐｈｙｓｉｃａｌ　Ａｄｄｒｅｓｓであるならば整数型情報判定機能１０３ｄが、複数のネットワーク装置から収集したＣｏｕｎｔｅｒ、Ｇａｕｇｅであるならば複数時系列情報判定機能が１０３ｂが、Ｉｎｔｅｇｅｒ、ＩＰ　Ａｄｄｒｅｓｓ、Ｐｈｙｓｉｃａｌ　ＡｄｄｒｅｓｓのＬｉｓｔまたはＴａｂｌｅ、または複数のネットワーク装置から収集したデータであるならば配列型情報判定機能１０３ｄが、それぞれ選択される。

【００２７】

以下に、監視情報のデータ型のそれぞれについて判定方法を説明する。入力監視情報が、単一のＣｏｕｎｔｅｒ、またはＧａｕｇｅの場合、図３に示す時系列情報判定機能を用いて、図４に示す動作フローに従って、ネットワークの状態を診断する。すなわち、時系列情報判定機能では、過去のデータを統計処理し、統計処理したデータと新たなデータを比較してその外れ値の大きさを算出し、異常を判定する。情報収集装置１０１から収集した監視情報Ａt を保存期間Ｗの間、監視情報ＤＢ１０に保存し（Ｓ１０）、時系列情報Ａ［ｔ］を作成する。そして、統計処理装置１１では、この時系列情報Ａ［ｔ］を統計的に処理して発生分布関数θを導き出す（Ｓ１１）。

【００２８】

異常判定装置１２では、新たな監視情報Ａt+1 と分布関数θを比較して、Ａt+1 と分布関数θの差分を算出し（Ｓ１２）、この差分を監視ルールＤＢ１０５のエラー条件と比較し（Ｓ１３）、真（異常）であるならば、監視情報決定部１０４に対して異常を通知すると共に、ログ蓄積部１０６に異常を保管する（Ｓ１４）。また、偽（正常）であるならば、収集監視情報決定部１０４に正常を通知し、同時に、監視情報ＤＢ１０は、保存している最も古い情報Ａt-w を廃棄し、Ａt+1 を保存する（Ｓ１５）。

【００２９】

入力監視情報が、複数のＣｏｕｎｔｅｒ、またはＧａｕｇｅの場合、図５に示す複数時系列情報判定機能を用いて、図６に示す動作フローに従って、ネットワークの状態を診断する。複数時系列情報判定機能では、過去の複数のデータを相関処理し、相関処理したデータを統計処理したものと新たな複数のデータの相関処理したデータを比較してその外れ値の大きさを算出し、異常を判定する。情報収集装置１０１から収集した複数の監視情報Ａt 、Ｂt 、Ｃt を保存期間Ｗの間、監視情報ＤＢ１０に保存し（Ｓ２０）、時系列情報Ａ［ｔ］、Ｂ［ｔ］、Ｃ［ｔ］を作成する（Ｓ２１）。

【００３０】

相関処理装置１１では、この時系列情報Ａ［ｔ］、Ｂ［ｔ］、Ｃ［ｔ］をそれぞれの間で相関処理して、共分散Γ_{AB}、Γ_{BC}、Γ_{CA}を導き出す（Ｓ２２）。さらにこれらの共分散の発生分布関数θ_{AB}、θ_{BC}、θ_{CA}を導き出す（Ｓ２３）。異常判定装置１２では、新たな監視情報Ａt+1 、Ｂt+1 、Ｃt+1 の共分散を計算し（Ｓ２４）、その共分散とそれぞれの分布関数θを比較して、新たなデータと分布関数θとの差分を算出する（Ｓ２５）。

【００３１】

この差分を監視ルールＤＢ１０５のエラー条件と比較し（Ｓ２６）、真（異常）であるならば、収集監視情報決定部１０４に対して異常を通知すると共に、ログ蓄積部１０６に異常を保管する（Ｓ２７）。また、偽（正常）であるならば、収集監視情報決定部１０４に正常を通知する。同時に、監視情報ＤＢ１０は、保存している最も古い情報Ａt-w 、Ｂt-w 、Ｃt-w を廃棄し、Ａt+1 、Ｂt+1 、Ｃt+1 を保存する（Ｓ２８）。

【００３２】

入力監視情報が、単一のＩｎｔｅｇｅｒ、ＩＰ　Ａｄｄｒｅｓｓ、Ｐｈｙｓｉｃａｌ　Ａｄｄｒｅｓｓである場合、図７に示す整数型情報判定機能を用いて、図８に示す動作フローに従って、ネットワークの状態を診断する。整数型情報判定機能では、収集した監視情報の値が正常かどうか判定する。情報収集装置１０１から収集した監視情報Ａと監視ルールＤＢ１０５のエラー条件を比較する（Ｓ３０，Ｓ３１）。真（異常）であるならば、収集監視情報決定部１０４に対して異常を通知すると共に、ログ蓄積部１０６に異常を保管し（Ｓ３２）、偽（正常）であるならば、収集監視情報決定部１０４に正常を通知する（Ｓ３３）。

【００３３】

入力監視情報が、複数のＩＰ　Ａｄｄｒｅｓｓ、Ｐｈｙｓｉｃａｌ　Ａｄｄｒｅｓｓである場合、図９に示す配列型情報判定機能を用いて、図１０に示す動作フローに従って、ネットワークの状態を診断する。配列型情報判定機能では複数のネットワーク機器から収集した監視情報の論理的なつながり（例えば、ＩＰルーティングテーブルやＬ２　Ｆｏｒｗａｒｄｉｎｇ　Ｔａｂｌｅなど）が正常であるかどうかを判定する。情報収集装置１０１から収集した監視情報Ａ［ｘ］、Ｂ［ｘ］、Ｃ［ｘ］の各テーブルは、図１１にその例を示す様に、テーブル結合装置１４により、宛先毎に各ネットワーク装置での転送先をならべた一つのテーブル（結合テーブルΩ）に結合される（Ｓ４０）。異常判定装置１２は、構成情報ＤＢ１３を参照して、宛先毎に経路を検査する（Ｓ４１）。経路の検査により、ループの発見、経路なしの発見が可能である。

【００３４】

ＩＰルーティングテーブルの経路の検査方法を例に挙げ、図１１を参照しながら説明する。結合テーブルΩのＤｅｓｔ１の経路に対して、ネットワーク装置Ａは、インターフェースＡ－１に転送することがわかる。構成情報ＤＢ１３を参照して、インターフェースＡ－１は、同じくネットワーク装置Ａに属するので、この経路は正常であると判断する。次に、Ｄｅｓｔ１の経路に対して、ネットワーク装置Ｂは、インターフェースＡ－２に転送する。構成情報ＤＢ１３を参照して、インターフェースＡ－２は、ネットワーク装置Ａのインターフェースなので、すでにＤｅｓｔ１に対するネットワーク装置Ａは検査済みであり、よってこの経路も正常と判断する。

【００３５】

次に、Ｄｅｓｔ１の経路に対するネットワーク装置Ｃでは、ネットワーク装置Ｂと同様、ネットワーク装置Ａに転送されるので、この経路も正常と判断し、Ｄｅｓｔ１に対する経路は、全て正常であると判断する。

【００３６】

結合テーブルΩのＤｅｓｔ２に対して、ネットワーク装置Ａは、インターフェースＢ－２宛てにパケットを転送することがわかる。次に、構成情報ＤＢ１３を参照して、インターフェースＢ－２を持つネットワーク装置を検索し、ネットワーク装置Ｂであることがわかる。次に、結合テーブルΩにおいて、Ｄｅｓｔ２に対してネットワーク装置Ｂが、インターフェースＢ－１に転送し、インターフェースＢ－１は同じネットワーク装置Ｂに属す

るインターフェースであるので、正常なルートと判断し、結合テーブルΩのなかでＤｅｓｔ２に対する次のネットワーク装置Ｃに対しての検査に移る。

【００３７】

ネットワーク装置Ｃでは、Ｄｅｓｔ２に対して経路を持たないので、経路なしのエラーと判断する。このエラー情報は、全ての経路の検査が終了するまで、保持される。結合テーブルΩのＤｅｓｔ３に対して、ネットワーク装置Ａは、インターフェースＣ－３宛てにパケットを転送することがわかる。

【００３８】

次に、構成情報ＤＢ１３を参照して、インターフェースＣ－３を持つネットワーク装置を検索し、ネットワーク装置Ｃであることがわかる。次に、結合テーブルΩにおいて、Ｄｅｓｔ３に対してネットワーク装置Ｃが、インターフェースＡ－３に転送し、インターフェースＡ－３はネットワーク装置Ａに属するインターフェースであることが判明する。ネットワーク装置Ａは、Ｄｅｓｔ３での経路においてすでにチェック済みであるので、この経路でループ発生のエラーが検出される。このエラー情報は、全ての経路の検査が終了するまで保持される（Ｓ４２）。

【００３９】

次に、未検査のネットワーク装置Ｂの検査に移る。ネットワーク装置Ｂは、インターフェースＣ－２宛てにパケットを転送することがわかる。構成情報ＤＢ１３を参照して、インターフェースＣ－２は、ネットワーク装置Ｃに属することがわかり、ネットワーク装置Ｃでは、Ｄｅｓｔ３に対して、既にループ検出エラーが発生しているので、経路検査は終了する。経路検査が終了すると（Ｓ４３）、収集監視情報決定部１０４に対して異常を検査時に検出したエラーと含めて通知すると共に、ログ蓄積部１０６に異常情報を保管する（Ｓ４４）。

【００４０】

本説明では、ＩＰルーティングテーブルの経路検査を例に挙げて説明したが、この手法はＥｔｈｅｒｎｅｔ（登録商標）などのＭＡＣフォワーディングテーブルの経路検査でも同様に適用可能である。

【００４１】

次に、これら４つの判定機能の組み合わせ方について述べる。図１２は４つの判定機能１０３ａ～１０３ｄの性質を記載した表である。時系列情報判定機能および複数時系列情報判定機能は事前発見型手段として、整数型情報判定機能や配列型情報判定機能は事後発見型手段として分類される。事前発見型手段は、監視情報の統計処理や相関処理を行い、これまでになかったパターンを異常の兆候として検出する。異常の兆候を検出できるため、監視システムは異常の事前検出が可能であるが、その反面、その後に実際には異常は発生しない場合も検出する可能性があるため、異常検出の精度は低い。

【００４２】

一方、事後発見型手段では、ネットワーク装置からのリアルタイムな監視情報を使って判定を行い、異常を検出する。このため、実際にネットワーク装置に異常が発生した後に、監視システムは異常検出するという事後検出となるが、異常検出の精度は高い。これらの特性から、事前発見手段をルールＤＢのツリー構造の上流側、事後発見手段をルールＤＢのツリー構造の下流側に配置することにより、迅速に障害の予兆を発見し、その予兆が本当に障害となるかを迅速かつ様々な種類の障害に対して確認することができる。

【００４３】

以下、事前発見手段および事後発見手段を組み合わせて、ネットワークの状態を監視するネットワーク監視システムの動作について以下に説明する。図１３は、図１に示すネットワーク監視システム１００の動作の手順を示したフローチャートである。初めに、図１と図１３を用いて発生したイベントに基づきネットワーク装置が監視情報を順次、収集し判定する手順について説明する。

【００４４】

監視情報収集部１０１が、監視ルールＤＢ１０５から初期監視情報（監視ルールＤＢに

おいて最初に収集を始める監視情報）を読込み（Ｓ２００）、監視ルールＤＢに指定された間隔で監視情報ａ（図２参照）の収集をＳＮＭＰのポーリングを用いて開始する（Ｓ２０１）。

【００４５】

ネットワーク装置１１１から収集された監視情報は、監視情報判定部１０２に渡され、監視情報判定部１０２は監視情報のデータ型に基づいて判定機能部１０３から適切な判定機能を選択し、監視情報の判定を行う（Ｓ２０２）。この場合の適切な判定機能の選択は、図２に示したＭＩＢオブジェクト名の示されたデータ型に基づいて行われる。監視情報判定部の応答と監視ルールＤＢの判定値を比較して、判定値より小さければ正常、大きければ異常と判断する（Ｓ２０３）。

【００４６】

異常である場合、収集監視情報決定部１０４は、ルールＤＢを参照して異常である監視情報ａの子監視ツリー番号を検索し、子監視ツリー番号１．１の監視情報ｂ（図２参照）の収集を開始するように監視情報収集部に通知する（Ｓ２０５）。通知を受けた監視情報収集部１０１は、監視情報ｂを監視ルールＤＢに指定された間隔で収集し（Ｓ２０１）、以下、同様の手順でこれら監視情報の判定を順次繰り返す。このとき、それぞれの監視情報ではアラーム状態を保持しており、親の監視情報ａのアラーム状態はエラー状態のまま監視情報を収集し、判定を継続する。このとき、仮に監視情報の値が、監視ルールＤＢに示す判定値と比較して偽となった場合でも、アラーム状態はエラー状態のままであるものとする。

【００４７】

次に、図１と図１３とを用いて、発生しているアラーム解放の手順について説明する。アラームの解放は、ネットワーク監視者により問題が対処された場合やネットワークの自己修復機能が対処した場合などに、ネットワークの状態が変化し、監視している監視情報の判定値が変化することにより開始される。

【００４８】

Ｓ２０３において、監視情報判定部１０２の応答が正常である場合、収集監視情報決定部１０３は、監視している監視情報のうち最下層の当たる監視情報が初期監視情報であるかどうかを判断し（Ｓ２０４）、初期監視情報であるならば（つまり、図２の監視情報ａ）、アラームが発生していない状態なので、監視情報決定部１０３は何もしない。Ｓ２０４において、最下層の監視情報が初期監視情報でないならば（つまり、図２の監視情報ｂまたは監視情報ｃ）、現在監視している監視情報の収集を終了するよう監視情報収集部に通知する（Ｓ２０６）。

【００４９】

次に、監視していた監視情報の親の監視情報がアラーム状態であれば、直接の親監視情報の監視情報判定部１０２の判定結果を監視する（Ｓ２０７）。判定結果が真（異常）であるなら、判定結果が偽（正常）になるまで、判定結果の監視を続ける（Ｓ２０７）。判定結果が偽（正常）となると、その監視情報が初期監視情報かどうかを判断し（Ｓ２０４）、監視している監視情報の最下層が初期監視情報になるまで、つまり、全てのアラームが解放されるまで、Ｓ２０６以降の動作を続ける。

【００５０】

全てのアラームが解放されたあとは、初期監視情報のみの監視を実行しており、再び初期監視情報に異常が発生した場合、同様の動作を繰り返す。このアラーム解放動作により、事前発見手段において異常を誤検出した場合でも、初期状態に戻り、通常の監視動作を継続することが可能である。

【００５１】

以上の本発明の実施の形態において、監視ルールＤＢを使った動的な監視情報の収集により、監視情報収集のためにネットワークに与える負荷を最小限に抑制することが可能、事前発見手段を監視ルールＤＢのツリー構造の上流に配置することによりネットワーク管理者が障害の兆候の迅速な発見が可能、事後発見手段を監視ルールＤＢのツリー構造の下

流側に配置することにより、発生した障害の原因が何であるか、または、障害の影響範囲がどこまで及ぶかをネットワーク管理者が瞬時に判断することが可能となる。

【００５２】

また、本発明の実施の形態においては、監視ルールＤＢのツリー構造の上流に事前発見手段を、下流に事後発見手段を配置した場合の形態について説明したが、本発明は、これに限定されることなく、任意の形で監視ルールＤＢの構築が可能である。

【実施例】

【００５３】

次に、本発明の実施例を説明する。以下に述べる実施例では、ネットワーク管理者が障害を監視する際に構築する監視ルールＤＢ１０５の構築例とそれを用いた動作例を、詳細に説明するものとする。図１４は本発明の第一、第二、第三の実施例で用いるネットワーク構成を示した図である。図１４に示すように、ネットワーク構成は、ルータＲ１～Ｒ３およびそれぞれローカルネットワークＬ１～Ｌ３に所属するクライアントＨ１、Ｈ２、ストリーミングサーバＨ３、Ｈ４、ハブＨＵＢからなる。ここで、お互いを接続しているリンクは、１００Ｍｂｔ／ｓのＦａｓｔ　Ｅｔｈｅｒｎｅｔ（登録商標）であるものとする。

【００５４】

ネットワーク監視装置１００が監視する対象は、ルータＲ１～Ｒ３のネットワーク機器である。ネットワーク監視装置１００はルータＲ２に接続されており、その他の各ルータに対して、ルータＲ２を介して到達可能である。

【００５５】

以下、図１４と図１５とを参照して本発明の第一の実施例を説明する。図１５は、第一の実施例でのネットワーク監視装置１００内の監視ルールＤＢの各監視情報のつながりを記述するツリーを示す図である。図１５に示すように、第一の実施例では、トラヒックの急増を検出し（予兆発見）、それに関連するパケット落ち障害が無いかどうかを監視し（障害発見）、もし障害が発生していた場合は、どの方路（インターフェース）からのトラヒックが原因で障害が発生しているかを特定する（原因特定）という手順である。

【００５６】

初期監視情報として、ネットワーク監視装置１００は、各ルータのローカルネットワークへのインターフェースの出力トラヒック量であるＭＩＢ情報ｉｆＯｕｔＯｃｔｅｓ（Ｍ１、Ｍ２、Ｍ３）を取得し、この情報を時系列情報判定機能を使って監視する。ここで、ストリーミングサーバＨ３からクライアントＨ１に２０Ｍｂｉｔ／ｓでストリーミングを配信中に、ストリーミングサーバＨ４から６０Ｍｂｉｔ／ｓでストリーミングの配信を開始するとする。ストリーミングサーバＨ４から配信が始まった時、監視情報Ｍ１で突然のトラヒック増を検出する。

【００５７】

監視情報Ｍ１が異常となるので、ネットワーク監視装置１００は、次の監視情報であるパケット落ちを監視するために、図２における子監視ツリー番号１．１および１．２に相当する、インターフェースのＭＩＢ情報ｉｆＯｕｔＤｉｓｃａｒｄ（Ｍ１１）およびルータのＭＩＢ　ｉｐＯｕｔＤｉｓｃａｒｄ（Ｍ１２）を取得して、整数型情報判定機能を使って監視する。

【００５８】

ここで、いずれかの監視情報において閾値異常のパケット落ちを検出すると、次に、ネットワーク監視装置１００はルータＲ２、ルータＲ３からの入力トラヒック量を調べるために、それぞれのインターフェースのＭＩＢ情報ｉｐＩｎＯｃｔｅｓ（Ｍ１１１、Ｍ１１２）を整数型情報判定機能を使って監視を開始する。

【００５９】

ストリーミングサーバＨ４からのトラヒックは６０Ｍｂｉｔ／ｓであるので、予めルールＤＢの監視情報Ｍ１１２に設定してある閾値である５０Ｍｂｉｔ／ｓを越えているという異常を検出するため、ネットワーク管理者は、パケット落ち障害の主たる原因がインタ

ーフェースＩＦ：１９２．１６８．３１．２／２４に入ってくるトラヒックが原因であることがわかる。

【００６０】

なお、図１５において、ＩＦ　ＩＤがＮｏｄｅ　ＩＤと同一となっている部分があるが、この場合には、ＩＦをチェックするのではなく、ルータをチェックすることを意味するものとし、以下の図１６，１７においても同様である。

【００６１】

次に、図１４と図１６とを参照して本発明の第二の実施例を説明する。図１６は、第二の実施例でのネットワーク監視装置１００内の監視ルールＤＢの監視情報のつながりを記述するツリーを示す図である。図１６に示すように、第二の実施例では、エラーによるパケットの棄却の増加傾向を検出し（予兆発見）、検出後、各ルータが持つルーティングテーブルを検査し（障害発見）、もし経路障害が発生していれば、障害となっている経路の通知と経路障害の原因がルーティングプロトコルによる経路棄却であるかどうかを検査する（障害原因特定）という手順である。

【００６２】

初期監視情報として、ネットワーク監視装置１００は、各ルータでＴＴＬ（Time To Live）値が“０”となったために棄却されたパケット数を示すＭＩＢ情報ｉｃｍｐＯｕｔＴｉｍｅＥｘｃｄｓ（Ｍ４、Ｍ５、Ｍ６）と、経路が無いため棄却されたパケット数を示すＭＩＢ情報ｉｃｍｐＯｕｔＤｅｓｔＵｎｒｅａｃｈ（Ｍ７、Ｍ８、Ｍ９）とを取得し、この情報を時系列情報判定機能を使って監視する。

【００６３】

なお、上記ＴＴＬ値は、伝送されるＩＰパケットのヘッダに付加された情報であって、このパッケットがルータを一つ通過する毎に、ＴＴＬ値が“１”減算され、値が“０”になると、そのときのルータはこのパケットを棄却するようになっている。

【００６４】

ここで、各ルータにＯＳＰＦ（Open Shortest Path First）やＲＩＰ（Routing Information Protocol）などの複数のルーティングプロトコルが動作している環境で、ルーティングテーブルを決定する際に、異なるルータ間で違うルーティングプロトコルの経路を採用してしまったことが原因で、ルータＲ１とＲ２間で経路にループが発生したとする。このとき、ネットワーク監視装置１００は、監視情報Ｍ４および監視情報Ｍ５で、パケット棄却数が急激な増加を検出する。監視情報Ｍ４および監視情報Ｍ５が異常となったので、ネットワーク監視装置１００は、次の監視情報である経路検査を行うために、ルータの経路情報であるＭＩＢ情報ｉｐＲｏｕｔｅＥｎｔｒｙ（Ｍ４１）を全ルータから取得して、配列型情報判定機能を使って経路を検査する。

【００６５】

この検査においてループが発見され、ループの位置が特定されると、管理者は、このループの位置情報を見て適切な処置を施すことができる。次に、ループが発生した原因が経路の棄却であるかどうかを判定するために、ネットワーク監視装置１００は、ルータの経路棄却数を示すｉｐＲｏｕｔｅＤｉｓｃａｒｄ（Ｍ４１１、Ｍ４１２、Ｍ４１３）を整数型情報判定機能を使って検査する。ここでは、ループ発生の原因が異なるプロトコルの経路を採用したことが原因であるので、監視情報Ｍ４１１と監視情報Ｍ４１２は異常とならない。

【００６６】

また、ルーティングプロトコルの異常で、ルーティングテーブルから経路が削除されてしまったことを想定すると、監視情報Ｍ７、監視情報Ｍ８、監視情報Ｍ９のいずれかが異常となり、監視情報Ｍ４１にて経路検査により経路なしを検出したあと、監視情報Ｍ４１１、監視情報Ｍ４１２、監視情報Ｍ４１３のいずれかが異常となるため、管理者はルーティングプロトコルの異常がどのルータで発生しているのか迅速に発見することができる。

【００６７】

次に、図１４と図１７とを参照して本発明の第三の実施例を説明する。図１７は、第三

の実施例でのネットワーク監視装置１００内の監視ルールＤＢの監視情報のつながりを記述するツリーを示す図である。図１７に示すように、第三の実施例は、正常なパケット棄却数の増加傾向を検出し（予兆発見）、パケット棄却につながるＣＰＵオーバロード障害、または温度障害が発生していないか監視し（障害発見）、ＣＰＵオーバロードが発生しているとプロセスが暴走していないかどうか調べ、温度異常であるとファンの状態を調べる（障害原因特定）という手順である。

【００６８】

初期監視情報として、ネットワーク監視装置１００は、各インターフェースで正常なパケットが棄却された数を示すＭＩＢ情報ｉｆＯｕｔＤｉｓｃａｒｄ（ＭＭ１０、ＭＭ１２、ＭＭ１４）と、各ルータで正常なパケットが棄却された数を示すＭＩＢ情報ｉｐＯｕｔＤｉｓｃａｒｄ（ＭＭ１１、ＭＭ１３、ＭＭ１５）を取得し、時系列情報判定機能を使って監視する。

【００６９】

ここで、ルータＲ１内で動作しているプロトコルの暴走が原因となり、ＣＰＵがオーバフローしたとする。オーバフローが原因でルーティングプロトコルが正しく動作しなくなり、現在のルーティングテーブルにない経路はＲ１で棄却される。このとき、ネットワーク監視装置１００は、監視情報ＭＭ１０もしくは監視情報ＭＭ１１で、正常なパケットの棄却数が次第に増加するのを検出する。

【００７０】

監視情報ＭＭ１０または監視情報ＭＭ１１が異常となったので、ネットワーク監視装置１００は、次の監視情報であるＣＰＵオーバロードおよび温度異常を監視するために、ルータのＣＰＵ使用率を示すＭＩＢ情報ｃｐｍＣＰＵＴｏｔａｌ５ｓｅｃ（ＭＭ１０１）と温度状態を示すＭＩＢ情報ｃｉｓｃｏＥｎｖＭｏｎＴｅｍｐｅｒａｔｕｒｅＳｔａｔｕｓＶａｌｕｅ（ＭＭ１１１）をそれぞれ取得し、整数型情報判定機能にて検査を行う。

【００７１】

この検査において、ＣＰＵ使用率が監視情報ＭＭ１０１の閾値より大きいと、ネットワーク監視装置１００は障害が発生しているとみなし、次にどのプロセスが原因となっているかを検査するために、プロセスごとのＣＰＵ占有率を示すＭＩＢ情報ｃｐｍＰｒｏｃｅｓｓＡｖｅｒａｇｅＵＳｅｃｓ（ＭＭ１０１１）を取得し、整数型情報判定機能を使って検査する。ここで、監視情報ＭＭ１０１１の閾値より大きいと、ネットワーク監視装置１００は異常であるとみなし、そのプロセスＩＤを管理者に通知する。

【００７２】

これにより、管理者は、どのプロセスが異常であるかが迅速に発見することができる。また、温度障害が発生したことを想定しても、上記と同様の動作で、どのファンに原因があるかを迅速に管理者に知らせることが可能である。

【００７３】

なお、上述した実施の形態および各実施例に示した動作フローは、その動作手順を予めプログラムとしてＲＯＭなどの記録媒体に記録しておき、これをコンピュータ（ＣＰＵ）に読取らせて実行させる様に構成できることは勿論である。

【図面の簡単な説明】

【００７４】

【図１】本発明の実施の形態におけるネットワーク管理システムの構成および監視対象ネットワークの構成を示すブロック図である。

【図２】本発明の実施の形態におけるネットワーク管理システムが使用する、監視ルールＤＢ内の監視ルールの例を示す図である。

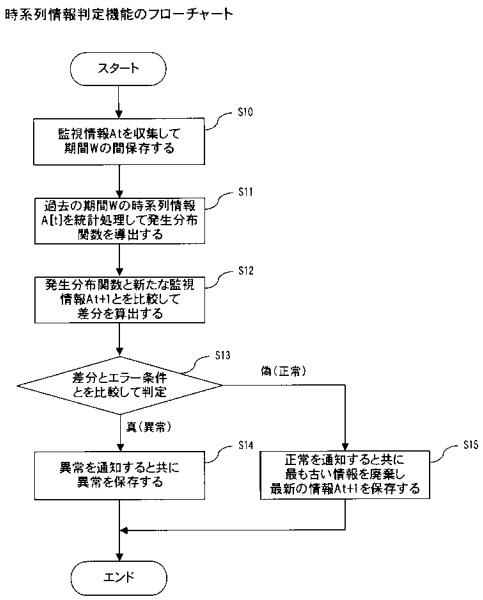
【図３】本発明の実施の形態における判定機能である時系列情報判定機能の構成を示すブロック図である。

【図４】図３の動作フローを示す図である。

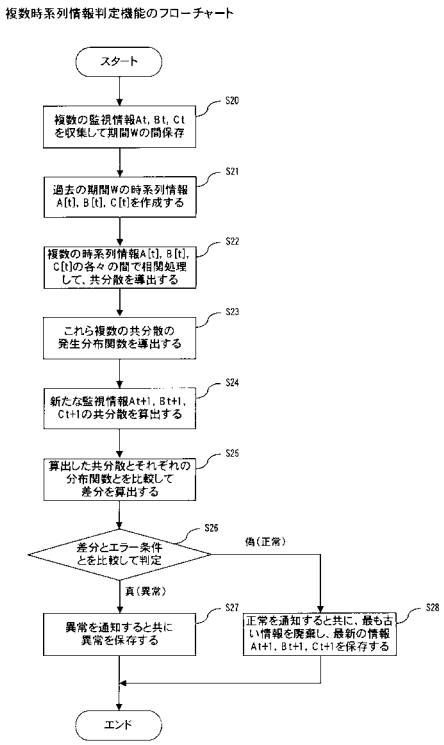
【図５】本発明の実施の形態における判定機能である複数時系列情報判定機能の構成を示

すブロック図である。
【図６】図５の動作フローを示す図である。
【図７】本発明の実施の形態における判定機能である整数型情報判定機能の構成を示すブロック図である。
【図８】図７の動作フローを示す図である。
【図９】本発明の実施の形態における判定機能である配列型情報判定機能の構成を示すブロック図である。
【図１０】図９の動作フローを示す図である。
【図１１】本発明の実施の形態における配列型判定機能の処理の流れを示す図である。
【図１２】本発明の実施の形態における判定機能のそれぞれの特徴を示す図である。
【図１３】本発明の実施の形態におけるネットワーク管理システムの動作の流れを示すフローチャートである。
【図１４】本発明の実施例の説明に用いるネットワーク構成例を示したブロック図である。
【図１５】本発明の第一の実施例における監視ルールを示す図である。
【図１６】本発明の第二の実施例における監視ルールを示す図である。
【図１７】本発明の第三の実施例における監視ルールを示す図である。
【符号の説明】
【００７５】
１００　ネットワーク監視システム
１０１　監視情報収集部
１０２　監視情報判定部
１０３　判定機能部
１０４　収集監視情報決定部
１０５　監視ルールＤＢ（データベース）
１０６　ログ蓄積部
１２０　監視サイト
１２１　監視端末

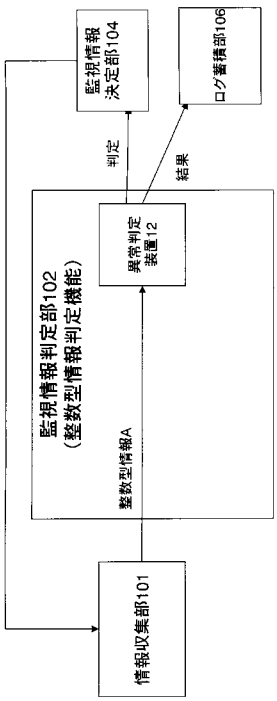
【図４】


時系列情報判定機能のフローチャート
スタート
監視情報Atを収集して期間Wの間保存する
S10
過去の期間Wの時系列情報A[t]を統計処理して発生分布関数を導出する
S11
発生分布関数と新たな監視情報At+1とを比較して差分を算出する
S12
差分とエラー条件とを比較して判定
S13
偽(正常)
真(異常)
異常を通知すると共に異常を保存する
S14
正常を通知すると共に最も古い情報を廃棄し最新の情報At+1を保存する
S15
エンド

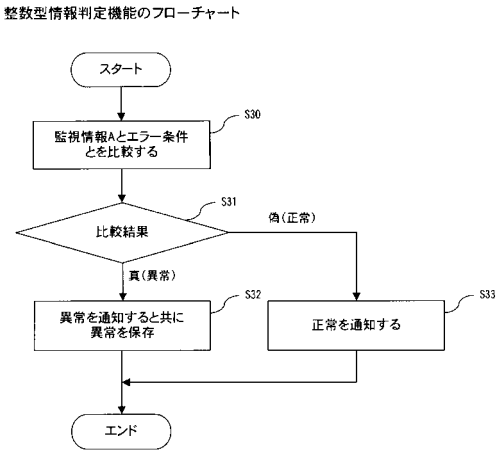
【図６】


複数時系列情報判定機能のフローチャート
スタート
複数の監視情報At, Bt, Ctを収集して期間Wの間保存
S20
過去の期間Wの時系列情報A[t], B[t], C[t]を作成する
S21
複数の時系列情報A[t], B[t], C[t]の各々の間で相関処理して、共分散を導出する
S22
これら複数の共分散の発生分布関数を導出する
S23
新たな監視情報At+1, Bt+1, Ct+1の共分散を算出する
S24
算出した共分散とそれぞれの分布関数とを比較して差分を算出する
S25
差分とエラー条件とを比較して判定
S26
偽(正常)
真(異常)
異常を通知すると共に異常を保存する
S27
正常を通知すると共に、最も古い情報を廃棄し、最新の情報At+1, Bt+1, Ct+1を保存する
S28
エンド

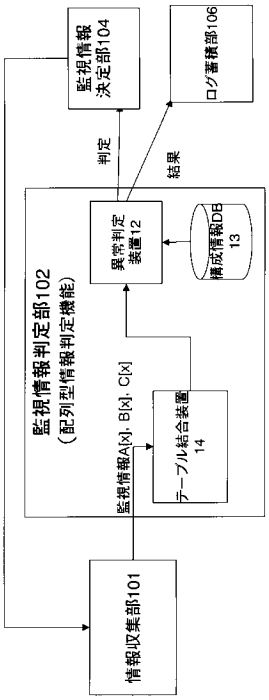
【図７】


監視情報決定部104
ログ蓄積部106
判定
結果
異常判定装置12
監視情報判定部102
(整数型情報判定機能)
整数型情報A
情報収集部101

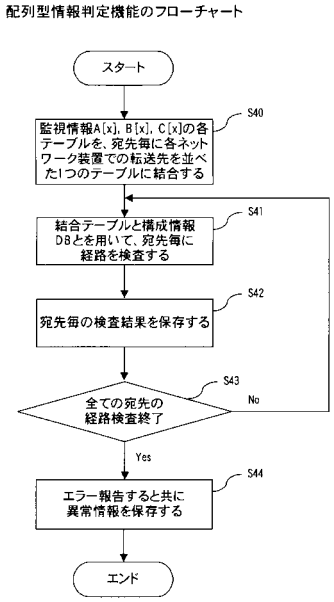
【図８】


整数型情報判定機能のフローチャート
スタート
監視情報Aとエラー条件とを比較する
S30
比較結果
S31
偽(正常)
真(異常)
異常を通知すると共に異常を保存
S32
正常を通知する
S33
エンド

【図９】



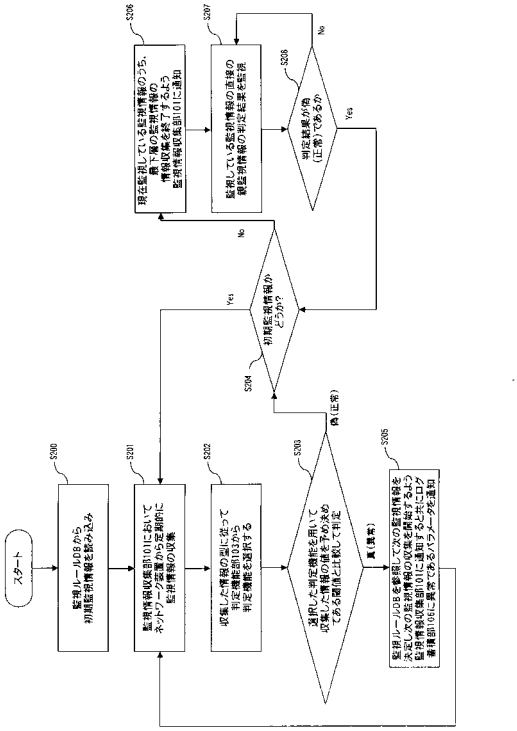
【図１０】



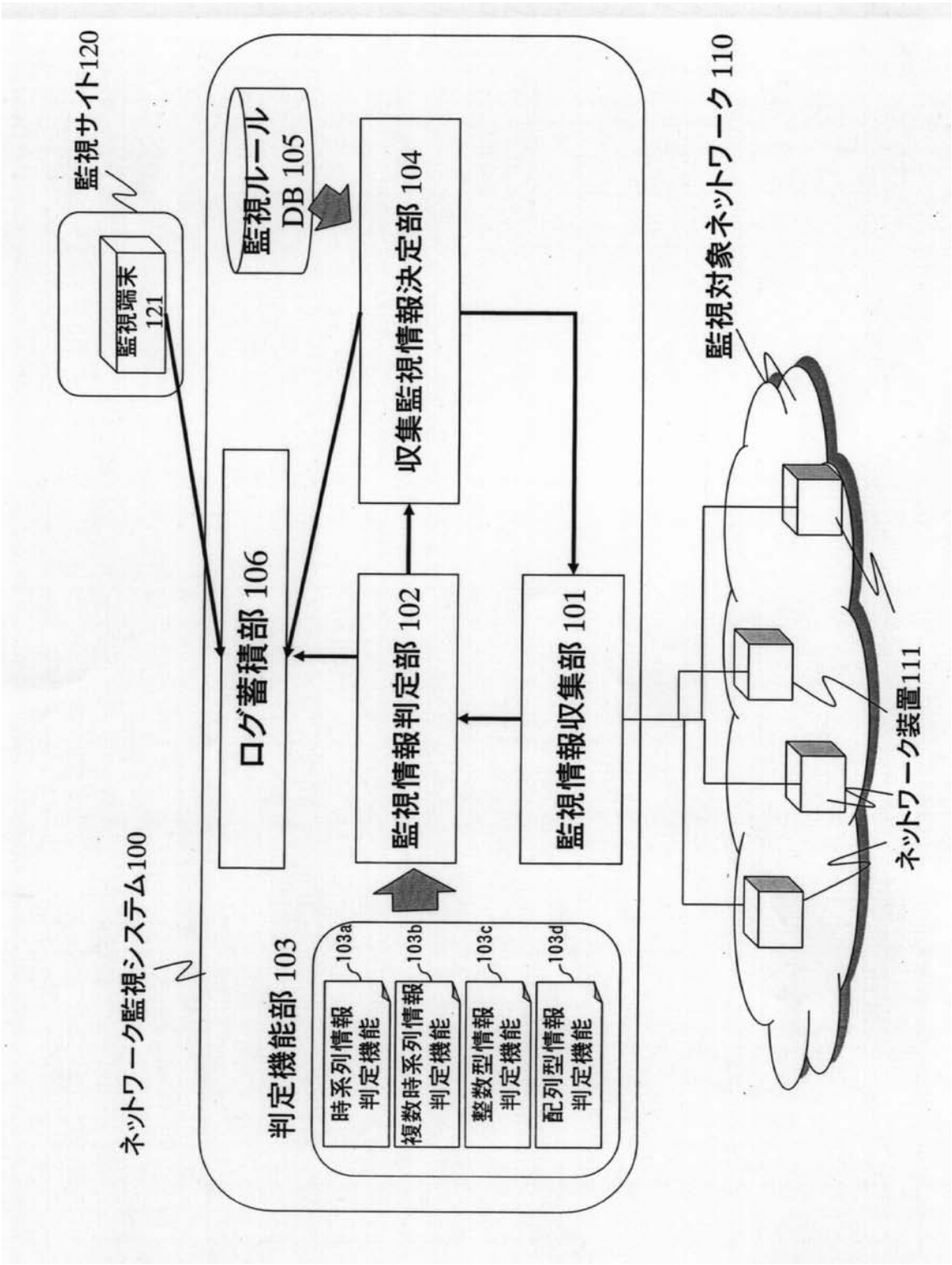
【図１２】

	検出の異常	異常検出の精度	
時系列情報判定機能	異常の兆候	異常が発生しない場合あり	事前発見型手段
複数時系列情報判定機能	異常の兆候	異常が発生しない場合あり	
整数型情報判定機能	異常が発生	高い	事後発見型手段
配列型情報判定機能	異常が発生	高い	

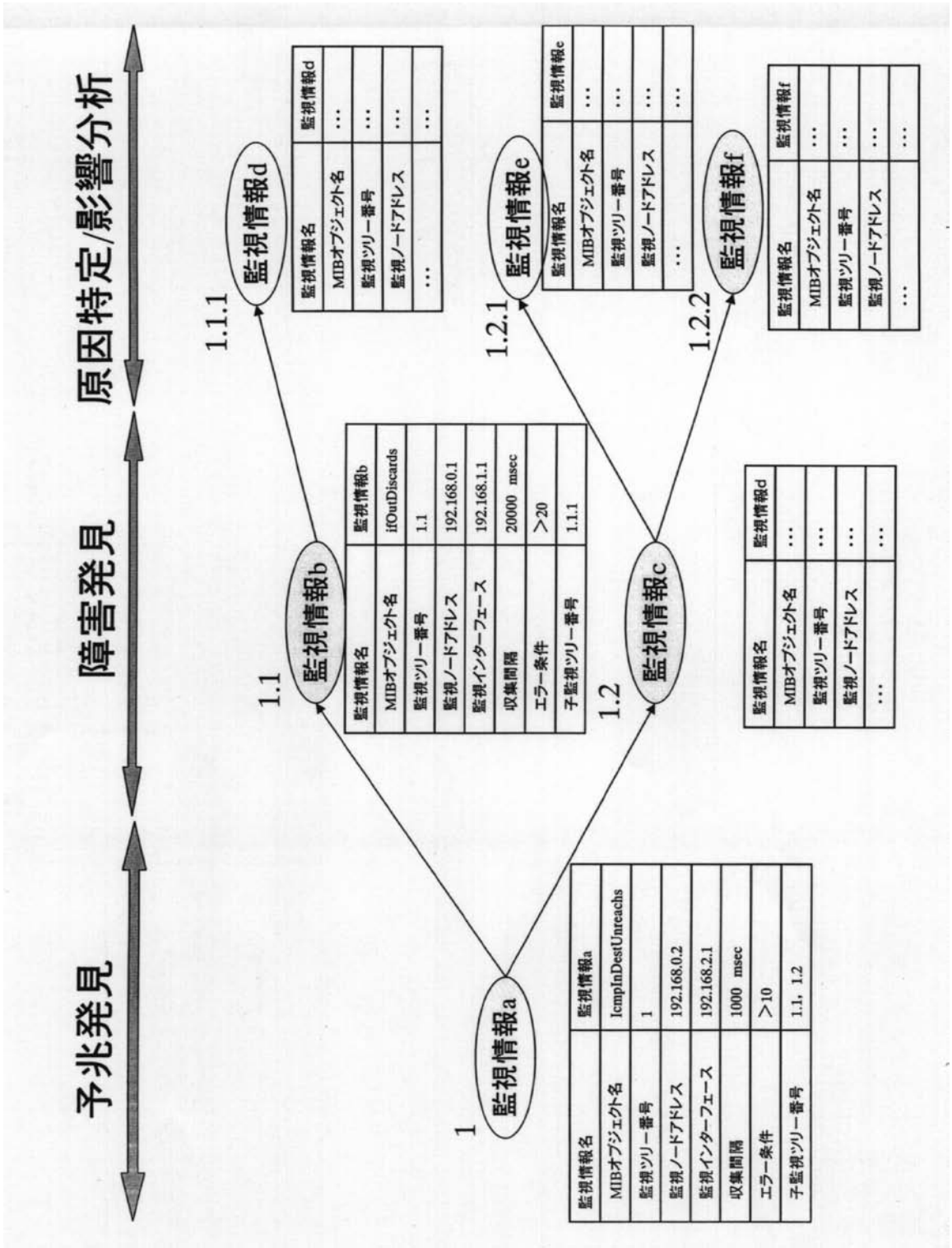
【図１３】



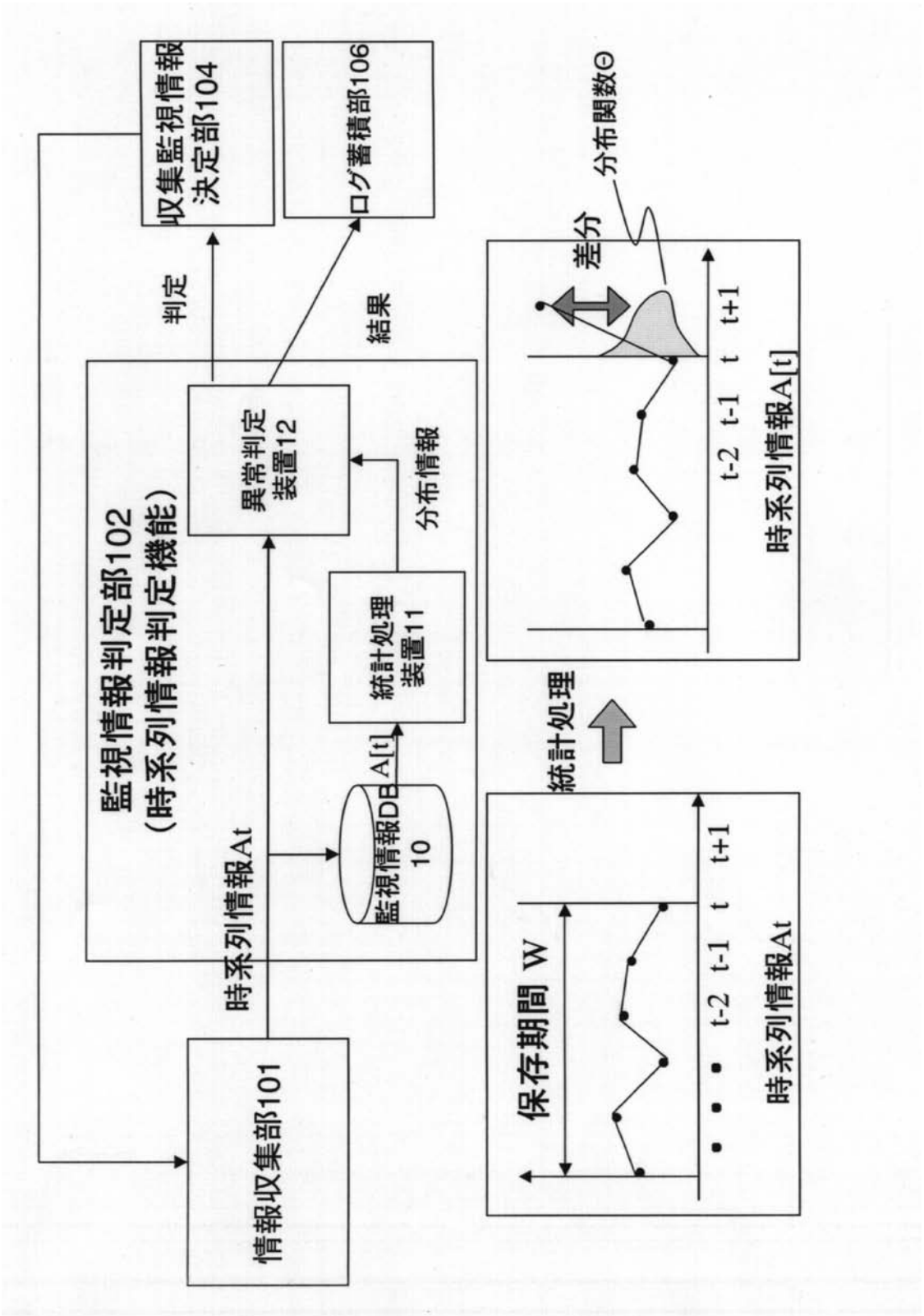
【図１】


監視サイト120
監視端末
121
監視ルール
DB 105
ネットワーク監視システム100
ログ蓄積部 106
収集監視情報決定部 104
監視情報判定部 102
監視情報収集部 101
判定機能部 103
103a
時系列情報
判定機能
103b
複数時系列情報
判定機能
103c
整数型情報
判定機能
103d
配列型情報
判定機能
監視対象ネットワーク 110
ネットワーク装置111

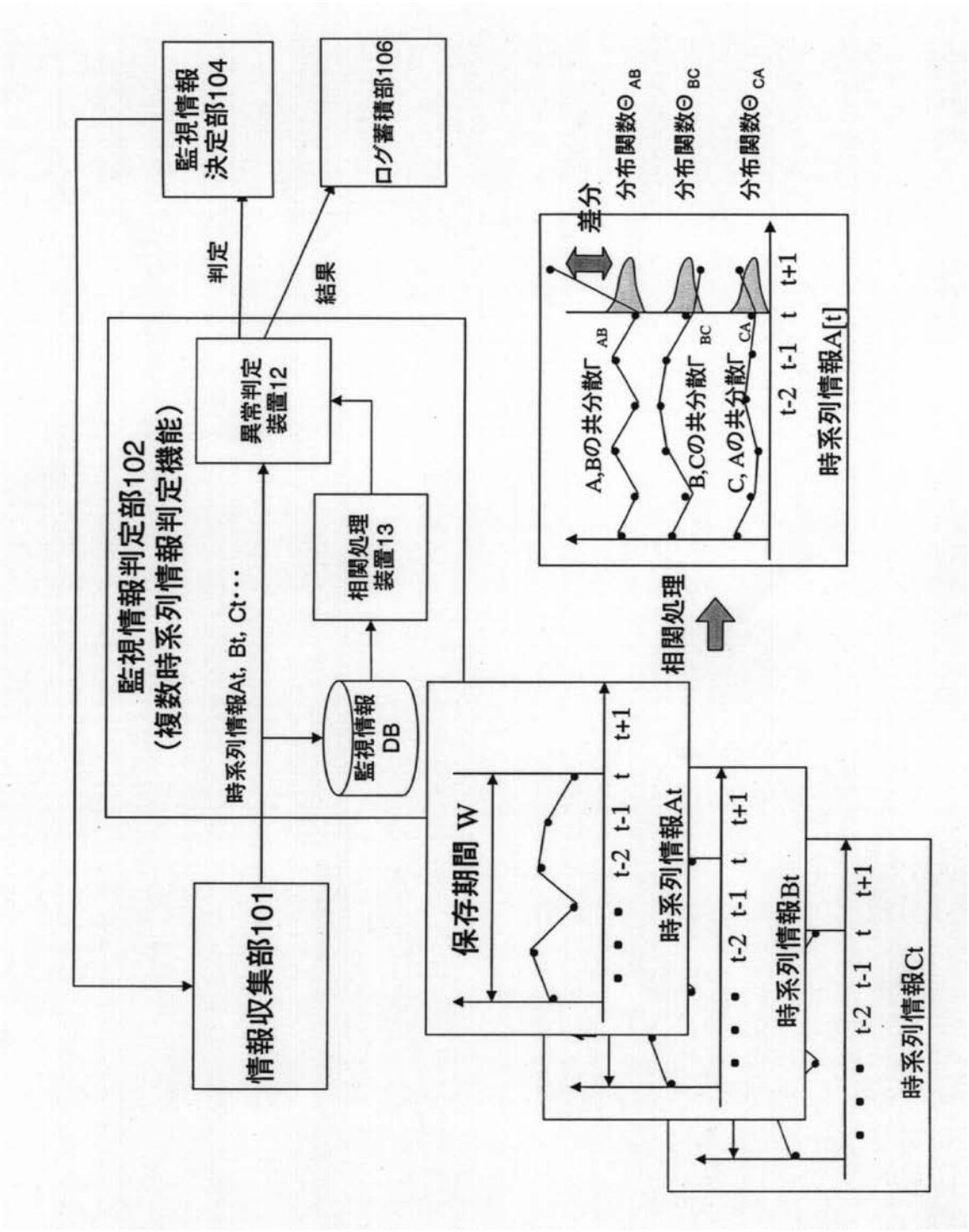
【図２】


予兆発見
障害発見
原因特定/影響分析
1
監視情報a
監視情報名 | 監視情報a
MIBオブジェクト名 | IcmpInDestUnreachs
監視ツリー番号 | 1
監視ノードアドレス | 192.168.0.2
監視インターフェース | 192.168.2.1
収集間隔 | 1000 msec
エラー条件 | >10
子監視ツリー番号 | 1.1, 1.2
1.1
監視情報b
監視情報名 | 監視情報b
MIBオブジェクト名 | ifOutDiscards
監視ツリー番号 | 1.1
監視ノードアドレス | 192.168.0.1
監視インターフェース | 192.168.1.1
収集間隔 | 20000 msec
エラー条件 | >20
子監視ツリー番号 | 1.1.1
1.1.1
監視情報d
監視情報名 | 監視情報d
MIBオブジェクト名 | …
監視ツリー番号 | …
監視ノードアドレス | …
… | …
1.2
監視情報c
監視情報名 | 監視情報d
MIBオブジェクト名 | …
監視ツリー番号 | …
監視ノードアドレス | …
… | …
1.2.1
監視情報e
監視情報名 | 監視情報e
MIBオブジェクト名 | …
監視ツリー番号 | …
監視ノードアドレス | …
… | …
1.2.2
監視情報f
監視情報名 | 監視情報f
MIBオブジェクト名 | …
監視ツリー番号 | …
監視ノードアドレス | …
… | …

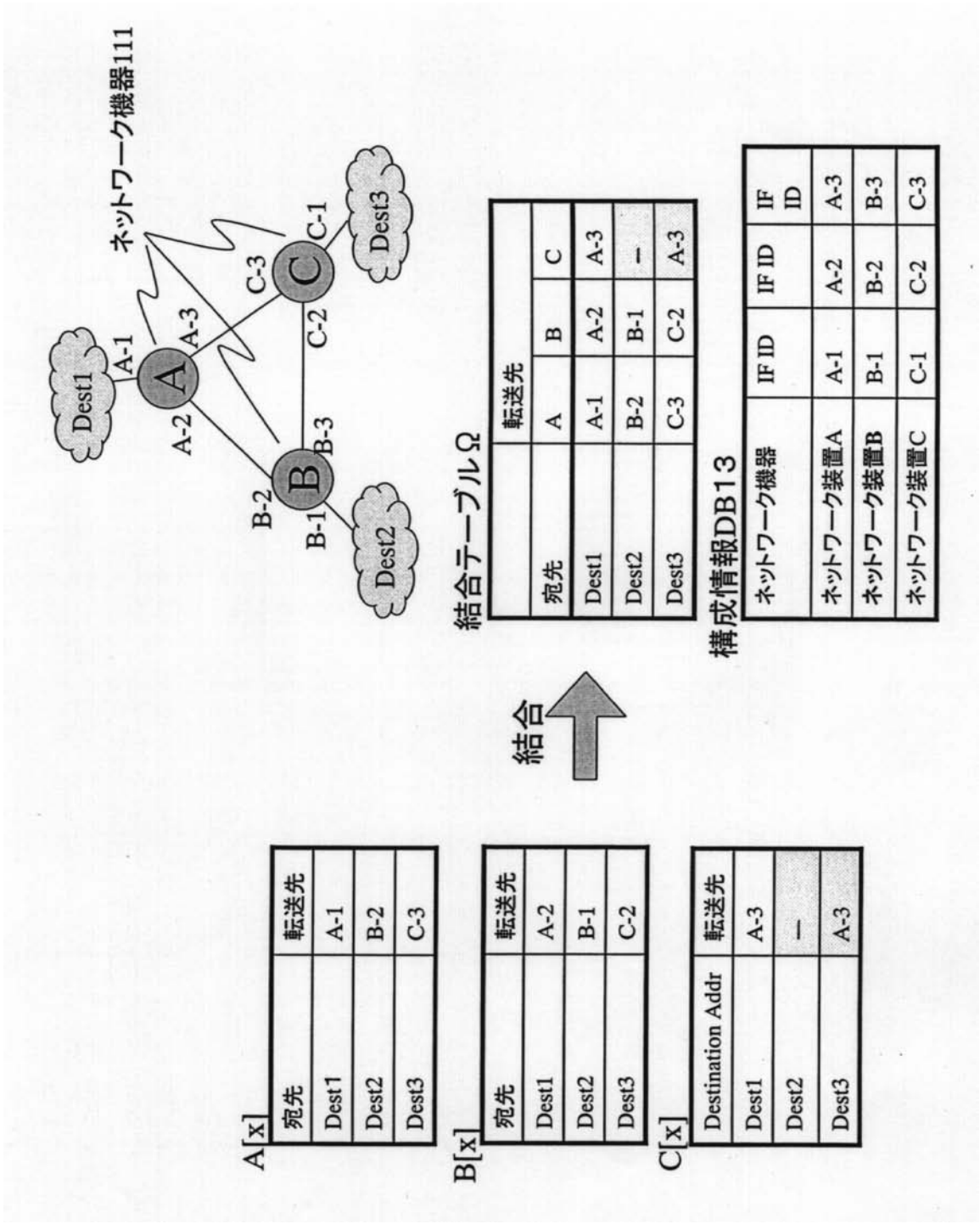
【図３】


収集監視情報決定部104
ログ蓄積部106
判定
結果
監視情報判定部102
(時系列情報判定機能)
異常判定装置12
分布情報
統計処理装置11
監視情報DB 10
A[t]
時系列情報At
情報収集部101
差分
分布関数Θ
t-2 t-1 t t+1
時系列情報A[t]
統計処理
保存期間 W
• • • t-2 t-1 t t+1
時系列情報At

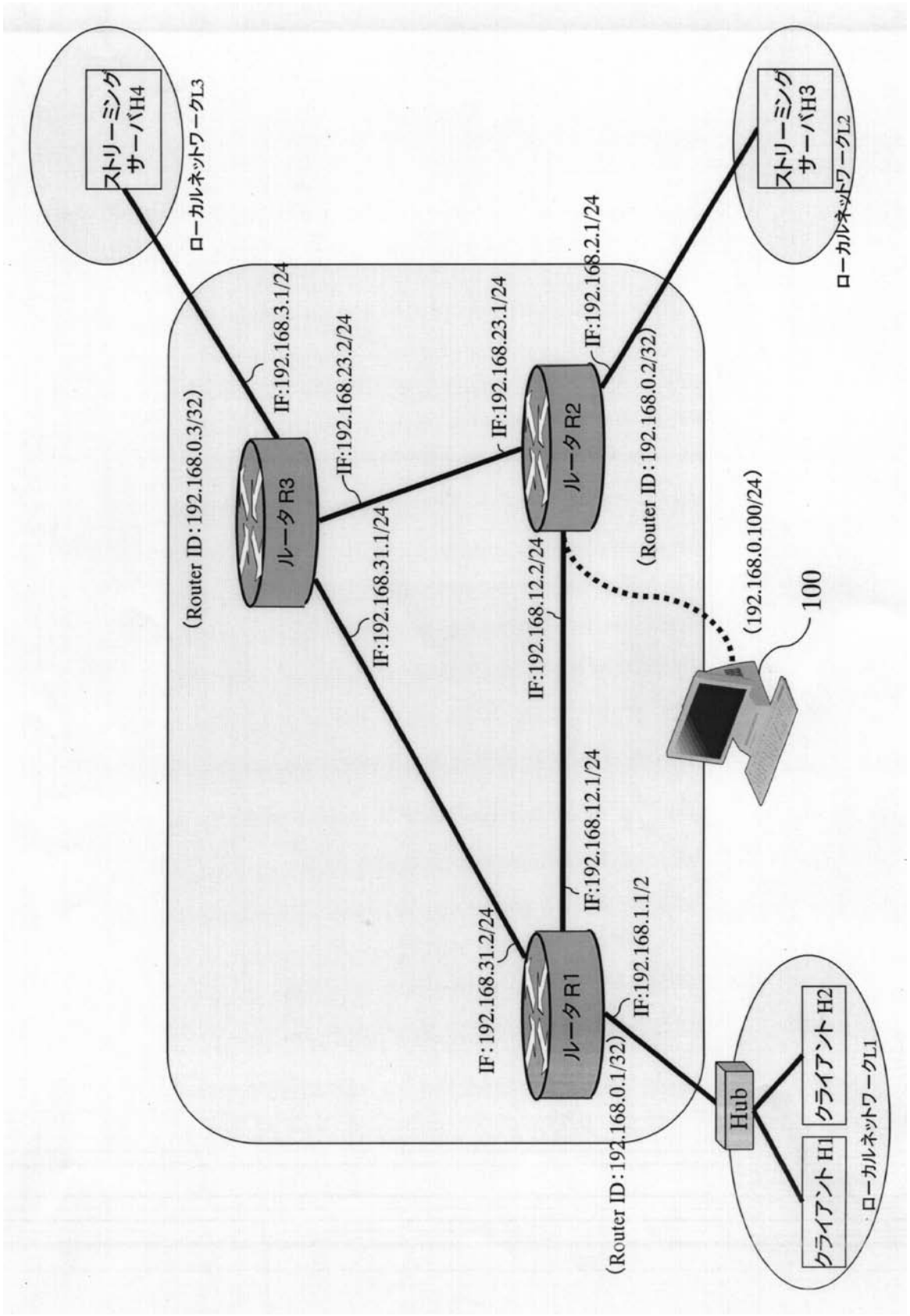
【図５】


監視情報判定部102
(複数数時系列情報判定機能)
情報収集部101
異常判定装置12
相関処理装置13
監視情報DB
監視情報決定部104
ログ蓄積部106
判定
結果
時系列情報At, Bt, Ct・・・
保存期間 W
時系列情報At
時系列情報Bt
時系列情報Ct
t-2 t-1 t t+1
相関処理
差分
分布関数Θ AB
分布関数Θ BC
分布関数Θ CA
A,Bの共分散Γ AB
B,Cの共分散Γ BC
C, Aの共分散Γ CA
時系列情報A[t]

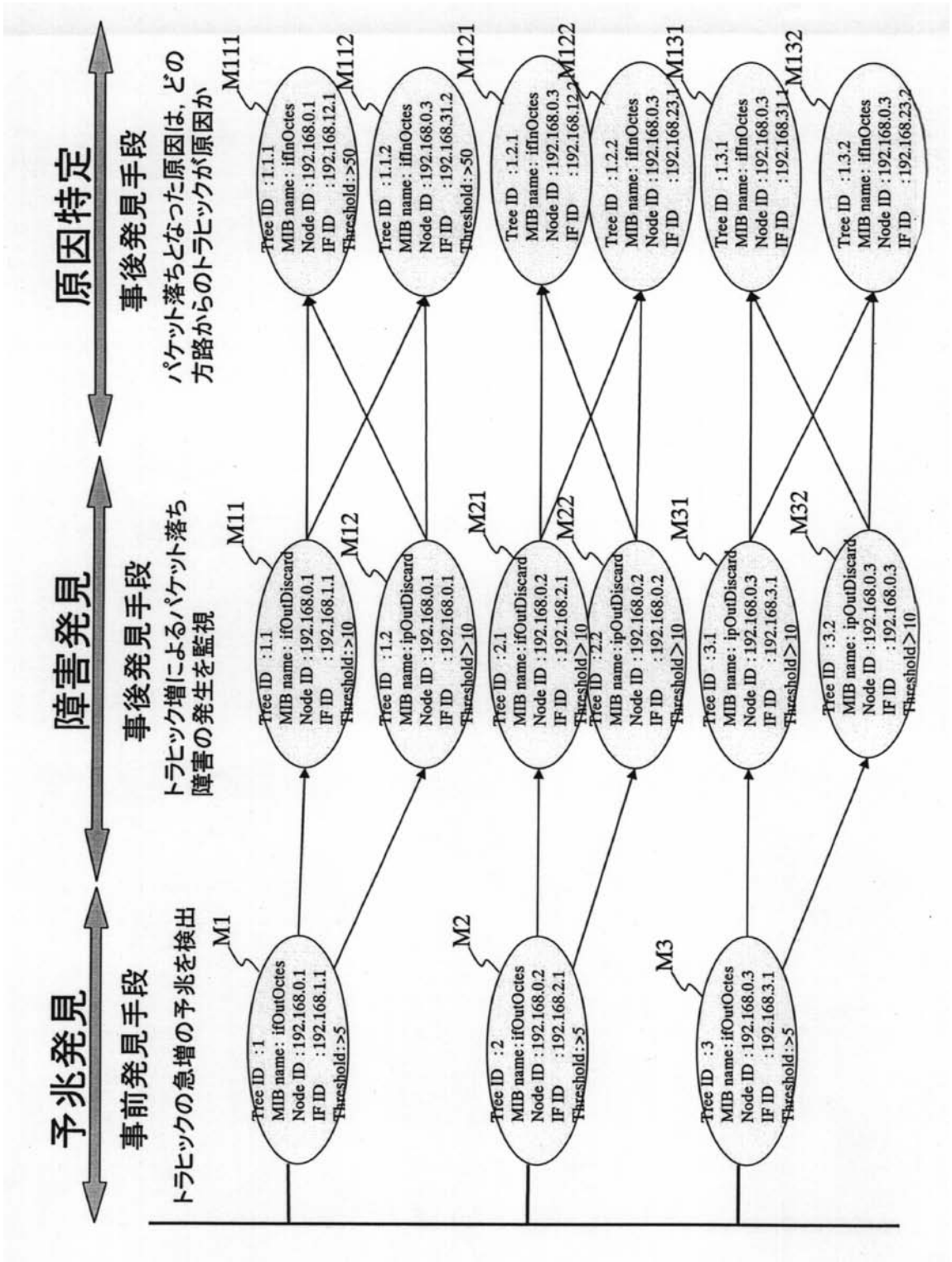
【図１１】


ネットワーク機器111
Dest1
Dest2
Dest3
A
B
C
A-1
A-2
A-3
B-1
B-2
B-3
C-1
C-2
C-3
A[x]
宛先
転送先
Dest1
A-1
Dest2
B-2
Dest3
C-3
B[x]
宛先
転送先
Dest1
A-2
Dest2
B-1
Dest3
C-2
C[x]
Destination Addr
転送先
Dest1
A-3
Dest2
—
Dest3
A-3
結合
結合テーブルΩ
宛先
転送先
A
B
C
Dest1
A-1
A-2
A-3
Dest2
B-2
B-1
—
Dest3
C-3
C-2
A-3
構成情報DB13
ネットワーク機器
IF ID
IF ID
IF ID
ネットワーク装置A
A-1
A-2
A-3
ネットワーク装置B
B-1
B-2
B-3
ネットワーク装置C
C-1
C-2
C-3

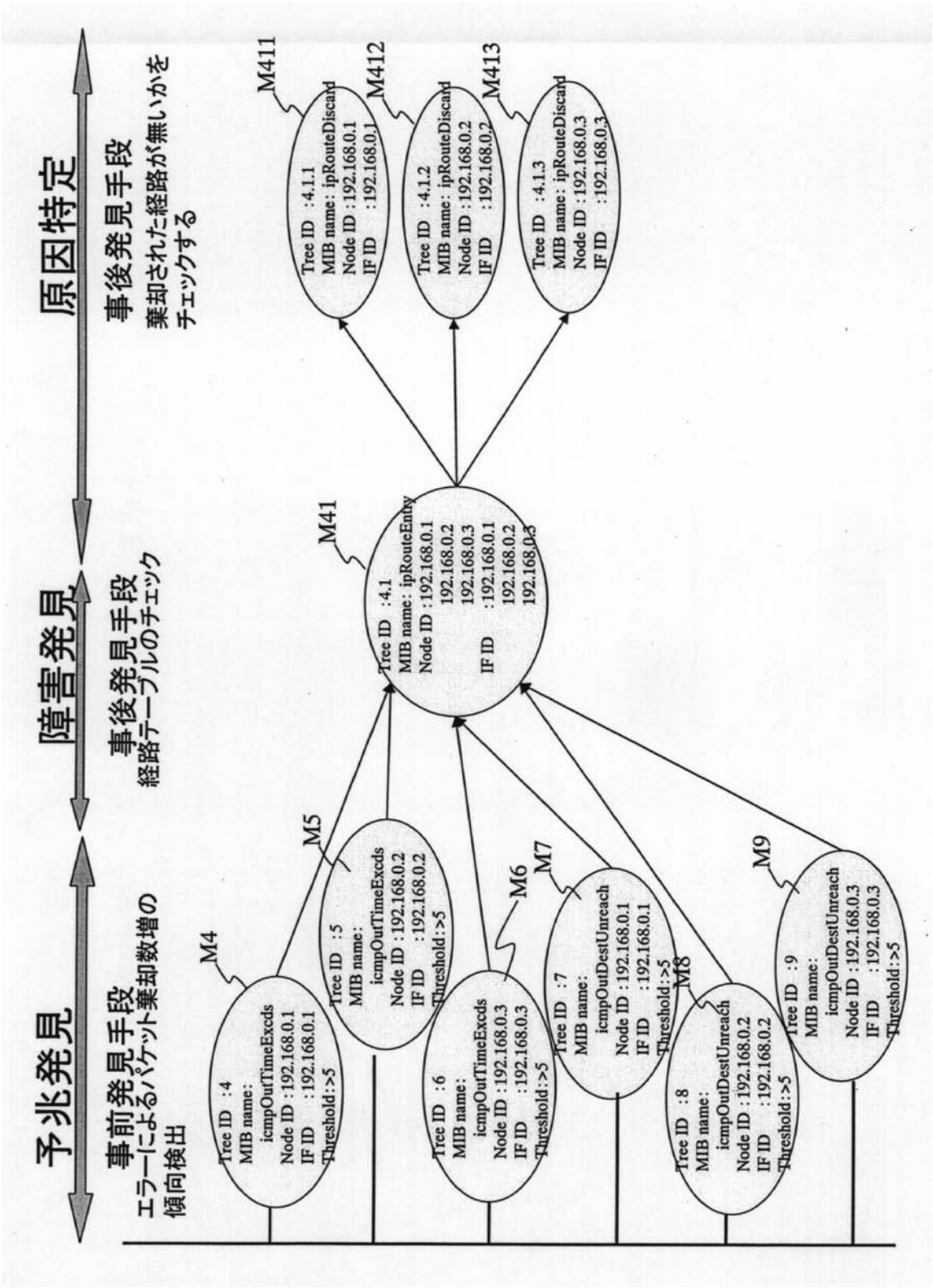
【図１４】


ストリーミング
サーバH4
ローカルネットワークL3
ストリーミング
サーバH3
ローカルネットワークL2
(Router ID:192.168.0.3/32)
IF:192.168.3.1/24
IF:192.168.23.2/24
IF:192.168.23.1/24
IF:192.168.2.1/24
ルータ R3
ルータ R2
(Router ID:192.168.0.2/32)
IF:192.168.31.1/24
IF:192.168.12.2/24
(192.168.0.100/24)
100
IF:192.168.12.1/24
IF:192.168.31.2/24
IF:192.168.1.1/2
ルータ R1
(Router ID:192.168.0.1/32)
Hub
クライアント H1
クライアント H2
ローカルネットワークL1

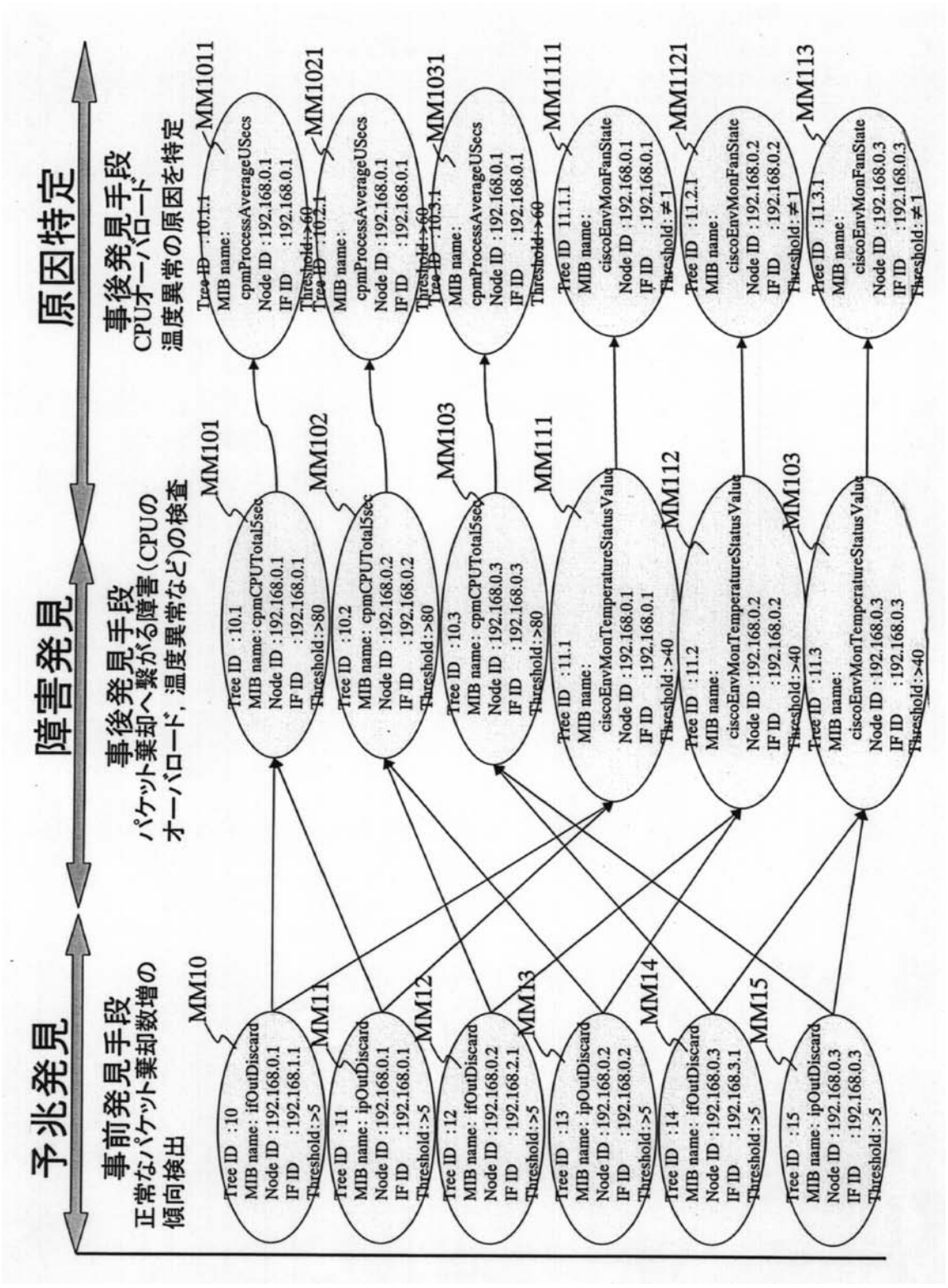
【図１５】


予兆発見
障害発見
原因特定
事前発見手段
トラヒックの急増の予兆を検出
事後発見手段
トラヒック増による/パケット落ち
障害の発生を監視
事後発見手段
パケット落ちとなった原因は，どの
方路からのトラヒックが原因か
M1
M2
M3
M11
M12
M21
M22
M31
M32
M111
M112
M121
M122
M131
M132
Tree ID :1
MIB name: ifOutOctes
Node ID :192.168.0.1
IF ID :192.168.1.1
Threshold:>5
Tree ID :2
MIB name: ifOutOctes
Node ID :192.168.0.2
IF ID :192.168.2.1
Threshold:>5
Tree ID :3
MIB name: ifOutOctes
Node ID :192.168.0.3
IF ID :192.168.3.1
Threshold:>5
Tree ID :1.1
MIB name: ifOutDiscard
Node ID :192.168.0.1
IF ID :192.168.1.1
Threshold:>10
Tree ID :1.2
MIB name: ipOutDiscard
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold>10
Tree ID :2.1
MIB name: ifOutDiscard
Node ID :192.168.0.2
IF ID :192.168.2.1
Threshold>10
Tree ID :2.2
MIB name: ipOutDiscard
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold>10
Tree ID :3.1
MIB name: ipOutDiscard
Node ID :192.168.0.3
IF ID :192.168.3.1
Threshold>10
Tree ID :3.2
MIB name: ipOutDiscard
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold>10
Tree ID :1.1.1
MIB name: ifInOctes
Node ID :192.168.0.1
IF ID :192.168.12.1
Threshold:>50
Tree ID :1.1.2
MIB name: ifInOctes
Node ID :192.168.0.3
IF ID :192.168.31.2
Threshold:>50
Tree ID :1.2.1
MIB name: ifInOctes
Node ID :192.168.0.3
IF ID :192.168.12.2
Tree ID :1.2.2
MIB name: ifInOctes
Node ID :192.168.0.3
IF ID :192.168.23.1
Tree ID :1.3.1
MIB name: ifInOctes
Node ID :192.168.0.3
IF ID :192.168.31.1
Tree ID :1.3.2
MIB name: ifInOctes
Node ID :192.168.0.3
IF ID :192.168.23.2

【図１６】


予兆発見
障害発見
原因特定
事前発見手段
エラーによるパケット棄却数増の
傾向検出
事後発見手段
経路テーブルのチェック
事後発見手段
棄却された経路が無いかを
チェックする
M4
Tree ID :4
MIB name:
icmpOutTimeExcds
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>5
M5
Tree ID :5
MIB name:
icmpOutTimeExcds
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold:>5
M6
Tree ID :6
MIB name:
icmpOutTimeExcds
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold:>5
M7
Tree ID :7
MIB name:
icmpOutDestUnreach
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>5
M8
Tree ID :8
MIB name:
icmpOutDestUnreach
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold:>5
M9
Tree ID :9
MIB name:
icmpOutDestUnreach
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold:>5
M41
Tree ID :4.1
MIB name: ipRouteEntry
Node ID :192.168.0.1
192.168.0.2
192.168.0.3
IF ID :192.168.0.1
192.168.0.2
192.168.0.3
M411
Tree ID :4.1.1
MIB name: ipRouteDiscard
Node ID :192.168.0.1
IF ID :192.168.0.1
M412
Tree ID :4.1.2
MIB name: ipRouteDiscard
Node ID :192.168.0.2
IF ID :192.168.0.2
M413
Tree ID :4.1.3
MIB name: ipRouteDiscard
Node ID :192.168.0.3
IF ID :192.168.0.3

【図１７】


予兆発見
障害発見
原因特定
事前発見手段
正常なパケット棄却数増の
傾向検出
事後発見手段
パケット棄却へ繋がる障害(CPUの
オーバロード，温度異常など)の検査
事後発見手段
CPUオーバロード
温度異常の原因を特定
MM10
MM11
MM12
MM13
MM14
MM15
MM101
MM102
MM103
MM111
MM112
MM103
MM1011
MM1021
MM1031
MM1111
MM1121
MM113
Tree ID :10
MIB name: ifOutDiscard
Node ID :192.168.0.1
IF ID :192.168.1.1
Threshold:>5
Tree ID :11
MIB name: ipOutDiscard
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>5
Tree ID :12
MIB name: ifOutDiscard
Node ID :192.168.0.2
IF ID :192.168.2.1
Threshold:>5
Tree ID :13
MIB name: ipOutDiscard
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold:>5
Tree ID :14
MIB name: ifOutDiscard
Node ID :192.168.0.3
IF ID :192.168.3.1
Threshold:>5
Tree ID :15
MIB name: ipOutDiscard
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold:>5
Tree ID :10.1
MIB name: cpmCPUTotal5sec
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>80
Tree ID :10.2
MIB name: cpmCPUTotal5sec
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold:>80
Tree ID :10.3
MIB name: cpmCPUTotal5sec
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold:>80
Tree ID :11.1
MIB name:
ciscoEnvMonTemperatureStatusValue
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>40
Tree ID :11.2
MIB name:
ciscoEnvMonTemperatureStatusValue
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold:>40
Tree ID :11.3
MIB name:
ciscoEnvMonTemperatureStatusValue
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold:>40
Tree ID :10.1.1
MIB name:
cpmProcessAverageUSecs
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>60
Tree ID :10.2.1
MIB name:
cpmProcessAverageUSecs
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>60
Tree ID :10.3.1
MIB name:
cpmProcessAverageUSecs
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:>60
Tree ID 11.1.1
MIB name:
ciscoEnvMonFanState
Node ID :192.168.0.1
IF ID :192.168.0.1
Threshold:≠1
Tree ID :11.2.1
MIB name:
ciscoEnvMonFanState
Node ID :192.168.0.2
IF ID :192.168.0.2
Threshold:≠1
Tree ID :11.3.1
MIB name:
ciscoEnvMonFanState
Node ID :192.168.0.3
IF ID :192.168.0.3
Threshold:≠1

フロントページの続き

(56)参考文献 特開２００２－１５２２０４（ＪＰ，Ａ）
特開平０８－０６５３０２（ＪＰ，Ａ）
特開平０７－０３０５４０（ＪＰ，Ａ）
特開２００４－０７０６９９（ＪＰ，Ａ）
特開２００３－３１８９８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００