(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-294973
(P2005-294973A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/56	H04L 12/56	400Z	5K030
H04L 29/14	H04L 13/00	313	5K035

審査請求 有　請求項の数 4　OL　（全 10 頁）

(21)出願番号　特願2004-103670 (P2004-103670)
(22)出願日　平成16年3月31日 (2004.3.31)

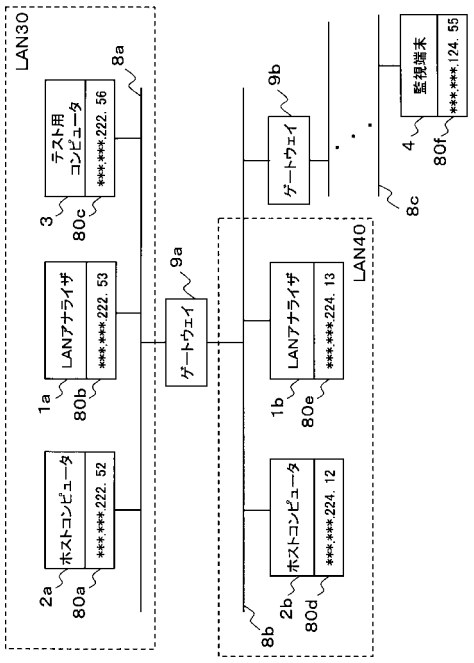
(71)出願人　000233491
日立電子サービス株式会社
神奈川県横浜市戸塚区品濃町５０４番地２
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　岡田　尚志
神奈川県横浜市戸塚区品濃町５０４番地２
日立電子サービス株式会社内
(72)発明者　廣田　陽一
神奈川県横浜市戸塚区品濃町５０４番地２
日立電子サービス株式会社内
(72)発明者　山岸　令和
神奈川県横浜市戸塚区品濃町５０４番地２
日立電子サービス株式会社内

最終頁に続く

(54)【発明の名称】ネットワーク監視システムおよびネットワーク監視方法

(57)【要約】
【課題】　ネットワーク監視装置がデータの取得を停止したときに、他のネットワーク監視装置にもデータの取得を停止させる。
【解決手段】
ホストコンピュータ２（２ａ，２ｂ）とＬＡＮアナライザ１（１ａ，１ｂ）とがネットワーク８（８ａ，８ｂ）を介して接続されている。ホストコンピュータ２は、所定の事象の発生を検知するとＬＡＮアナライザ１へそれを通知するためのパケットを送信する。ＬＡＮアナライザ１は、ネットワーク８から取り込んだパケットを記憶する記憶部と、ネットワーク８からパケットを取り込み、当該取り込んだパケットに含まれている情報を記憶部へ格納する取り込み手段と、ネットワーク８から取り込んだパケットが所定の事象の発生を通知するためのパケットであるときは、それ以降、取り込み手段に記憶部へのパケットの格納を停止させる制御手段と、前記制御手段により前記記憶部へのパケットの格納が停止すると、その旨を通知するためのパケットを予め定められた送信先へ送信する手段と、を備える。

図1



【特許請求の範囲】
【請求項１】
ホストコンピュータとネットワーク監視装置とがネットワークを介して接続されていて、
前記ホストコンピュータは、
所定の事象の発生を検知すると前記ネットワーク監視装置へ前記所定の事象の発生を通知するためのパケットを送信する手段を備え、
前記ネットワーク監視装置は、
前記ネットワークから取り込んだパケットを記憶する記憶部と、
前記ネットワークからパケットを取り込み、当該取り込んだパケットに含まれている情報を前記記憶部へ格納する取り込み手段と、
前記ネットワークから取り込んだパケットが前記所定の事象の発生を通知するためのパケットであるときは、それ以降、前記取り込み手段に前記記憶部へのパケットの格納を停止させる制御手段と、
前記制御手段により前記記憶部へのパケットの格納が停止すると、その旨を通知するためのパケットを予め定められた送信先へ送信する手段と、を備えるネットワーク監視システム。
【請求項２】
前記予め定められた送信先は、前記ネットワークとゲートウェイを介して接続された他のネットワークに接続されている他のネットワーク監視装置である請求項１記載のネットワーク監視システム。
【請求項３】
前記記憶部に格納されている前記パケットに含まれている情報を、前記ネットワークを監視するための監視端末へ送信する手段をさらに備える請求項１記載のネットワーク監視システム。
【請求項４】
ホストコンピュータが、所定の事象の発生を検知すると前記所定の事象の発生を通知するためのパケットをネットワーク監視装置へ送信し、
前記ネットワーク監視装置は、
ネットワークからパケットを逐次取り込み、当該取り込んだパケットに含まれている情報を記憶部へ格納する処理を行っているときに、前記所定の事象の発生を通知するためのパケットを受信すると、それ以降、前記ネットワークから取り込んだパケットを前記記憶部へ格納することを停止し、
前記記憶部へのパケットの格納が停止すると、その旨を通知するためのパケットを予め定められた送信先へ送信するネットワーク監視方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク監視のための技術に関し、特にネットワークからのパケットの取り込みを制御する技術に関する。
【背景技術】
【０００２】
ネットワークトラブルの原因を解析するために、ネットワーク上のパケットを取り込んで、ログとして保持するＬＡＮアナライザなどのネットワーク監視装置が広く用いられている。ＬＡＮアナライザでは、このパケットを保持するための記憶領域は容量が限られているので、サイクリックに利用される。したがって、一定時間が経過すると取り込んだパケットであっても上書きされて、消失する。
【０００３】
そこで、従来のＬＡＮアナライザでは、例えば、プロトコルにＴＣＰ／ＩＰを採用しているネットワークであれば、物理層、データリンク層、ネットワーク層、トランスポート

層、セッション層でのプロトコルエラーを検出し、データの取得を停止して、その時点で記憶領域に保持されているデータが消失しないようにするストップトリガー機能がある。

【０００４】

また、ホストコンピュータが実行しているアプリケーションにおいてエラーが発生したときでもストップトリガーをかけるためのネットワーク監視システムが、例えば特許文献１に記載されている。

【０００５】

【特許文献１】特開２００２－６４５０７公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

ここで、特許文献１では、エラーの起きたホストコンピュータから送られたパケットを同一セグメント内のＬＡＮアナライザが受信すると、データの取得を停止する。

【０００７】

しかし、エラーの起きたホストコンピュータから送られたパケットが届かないところに設置されているＬＡＮアナライザは、ストップトリガーがかからず、データの取得を停止することがない。また、ＬＡＮアナライザがストップトリガーによりデータの取得を停止しても、ネットワーク上の他の装置はそれを知り得ない。

【０００８】

本発明の目的は、ネットワーク監視装置がデータの取得を停止したときに、他のネットワーク監視装置にもデータの取得を停止させるための技術を提供することである。

【０００９】

本発明の他の目的は、ネットワーク監視装置がデータの取得を停止したときに、ネットワーク上の他の装置へデータの取得が停止したことを通知するための技術を提供することである。

【課題を解決するための手段】

【００１０】

本発明の一つの実施態様に従うネットワーク監視システムは、ホストコンピュータとネットワーク監視装置とがネットワークを介して接続されている。前記ホストコンピュータは、所定の事象の発生を検知すると前記ネットワーク監視装置へ前記所定の事象の発生を通知するためのパケットを送信する手段を備える。前記ネットワーク監視装置は、前記ネットワークから取り込んだパケットを記憶する記憶部と、前記ネットワークからパケットを取り込み、当該取り込んだパケットに含まれている情報を前記記憶部へ格納する取り込み手段と、前記ネットワークから取り込んだパケットが前記所定の事象の発生を通知するためのパケットであるときは、それ以降、前記取り込み手段に前記記憶部へのパケットの格納を停止させる制御手段と、前記制御手段により前記記憶部へのパケットの格納が停止すると、その旨を通知するためのパケットを予め定められた送信先へ送信する手段と、を備える。

【００１１】

好適な実施形態では、前記予め定められた送信先は、前記ネットワークとゲートウェイを介して接続された他のネットワークに接続されている他のネットワーク監視装置であっても良い。

【００１２】

好適な実施形態では、前記記憶部に格納されている前記パケットに含まれている情報を、前記ネットワークを監視するための監視端末へ送信する手段をさらに備えることもできる。

【発明を実施するための最良の形態】

【００１３】

以下、本発明の一実施形態に係るネットワークシステムについて、図面を用いて説明する。

【００１４】
図１は、本実施形態に係るネットワークシステムの全体構成図である。すなわち、本システムは、ネットワーク監視装置であるＬＡＮアナライザ１（１ａ，１ｂ）と、ホストコンピュータ２（２ａ，２ｂ）とがネットワーク８（８ａ，８ｂ）を介して接続されている。ここでは、ネットワーク８ａには、ＬＡＮアナライザ１ａと、ホストコンピュータ２ａと、テスト用コンピュータ３ａとが接続され、ＬＡＮ（Local Area Network）３０が形成されている。ネットワーク８ｂには、ＬＡＮアナライザ１ｂと、ホストコンピュータ２ｂとが接続され、ＬＡＮ４０が形成されている。ＬＡＮ３０，４０には、それぞれホストコンピュータ２ａ、２ｂが複数台あってもよい。各ホストコンピュータ２ａ、２ｂは、それぞれのＬＡＮ３０，４０内の他のホストコンピュータおよび他のＬＡＮ３０，４０のホストコンピュータと通信を行うことができる。

【００１５】
ネットワーク８ａとネットワーク８ｂとはゲートウェイ９ａを介して接続され、ＷＡＮ（Wide Area Network）が形成されている。従って、ＬＡＮ３０およびＬＡＮ４０は、互いに異なるセグメントである。また、ネットワーク８ｂには、さらにゲートウェイ９ｂが接続されていて、さらに別のネットワークと接続されている。そして、数段先のネットワーク８ｃには、このネットワークシステム全体を監視する監視端末４が接続されている。

【００１６】
図１に示すネットワークシステムは、通信プロトコルにＴＣＰ/ＩＰを用いることができる。ただし、通信プロトコルはＴＣＰ/ＩＰに限定されない。たとえば、他の通信プロトコルを用いてもよいし、ＩＰ（インターネットプロトコル）と、ＴＣＰ（トランスミッションコントロールプロトコル）以外の上位プロトコルとを組み合わせてもよい。

【００１７】
本実施の形態では、ホストコンピュータ２ａ、２ｂが、あらかじめ定められた事象の発生を検出して、それをＬＡＮアナライザ１ａ、１ｂが検知可能な事象に変換を行う。例えば、コンピュータ２ａ、２ｂが、アプリケーション層でのエラー等を検出すると、ネットワーク上にあるすべてのコンピュータにとって、論理的に存在しないＩＰアドレス（新規に割り当てられたＩＰアドレス）、またはＬＡＮアナライザ１のＩＰアドレスに対するｐｉｎｇコマンドの発行という事象に変換する。

【００１８】
ＬＡＮアナライザ１は、ネットワークのトラブル発生時等に設置され、ネットワーク８上のパケットを取り込んで、このパケットに含まれている情報を保持する。ネットワークの保守担当者は、ＬＡＮアナライザ１に保持されたパケットに含まれている情報を解析して、トラブルの原因の究明に役立てる。ＬＡＮアナライザ１の詳細な構成は図２（ａ）を用いて説明する。

【００１９】
ＬＡＮアナライザ１は、図２（ａ）に示すように、キーボード等の入力装置１０１およびＣＲＴ、液晶ディスプレイ等の表示装置１０２が接続されている。ＬＡＮアナライザ１は、ネットワーク上のパケットを取り込んで保持するキャプチャー部１２と、ＩＰアドレス記憶部１３と、データ判別部１４と、プロトコル検査部１５と、データ取得制御部１６と、データベース１７と、表示制御部１８とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【００２０】
キャプチャー部１２は、ネットワークからデータを取り込むデータ取込部１２１と、取り込んだデータを保持するデータ保持部１２２とを有する。データ取込部１２１は、ネットワーク上のパケットを取り込み、このパケットに含まれる一部または全部の情報をデータ保持部１２２へ格納する。データ保持部１２２は、データ取込部１２１が取り込んだパケットに含まれる情報をログとして保持する。データ保持部１２２は、例えば、一定の容量を持つサイクリックバッファで構成される。つまり、例えば１００メガバイト程度の容

量を持ち、パケットを順次記憶していき、全領域にデータが記憶された状態になると、時間的に最も古いデータに上書きして記憶していく。

【００２１】

データ保持部１２２に格納されているログデータは、データベース１７へコピーすることができる。これにより、データ保持部１２２にデータが上書きされてデータが消失することを防止できる。例えば、後述するように、キャプチャーが停止されたときのデータ保持部１２２の内容をデータベース１７へコピーして確保しておけば、保守担当者がこれをエラー解析などに利用することができ、かつ、直ちにキャプチャーを再開できる。

【００２２】

ＩＰアドレス記憶部１３には、自己のＩＰアドレス、同じＬＡＮに属するテスト用コンピュータ3に設定されたＩＰアドレス、別セグメントのＬＡＮに属するＬＡＮアナライザ１のＩＰアドレス、および監視端末４のＩＰアドレスが記憶されている。例えば、ＬＡＮアナライザ１ａのＩＰアドレス記憶部１３には、自己のＩＰアドレス８０ｂ、テスト用コンピュータ３ａのＩＰアドレス８０ｃ、ＬＡＮアナライザ１ｂのＩＰアドレス８０ｅおよび監視端末４のＩＰアドレス８０ｆが記憶されている。

【００２３】

データ判別部１４は、キャプチャー部１２が取り込んだパケットが特定のパケットであるかどうかを判別する。判別の結果、特定のパケットである場合は、その旨をデータ取得制御部１６へ通知する。この特定のパケットとは、例えば、後述するように、ホストコンピュータ２でエラー、あるいは警告に相当するような所定の事象が発生したことを通知するためのパケット（ＡＰエラー通知）であってもよいし、あるいは、別セグメントのＬＡＮアナライザ１がキャプチャーを停止したことを通知するためのパケット（キャプチャー停止通知）であってもよい。特定のパケットであるかは、例えば、取り込んだパケットの送信先のＩＰアドレスがＩＰアドレス記憶部１３に記憶されているＩＰアドレスと一致するかどうかで判別しても良い。例えば、ＬＡＮアナライザ１ａにおけるＡＰエラー通知の判定は、取り込んだパケットの送信先ＩＰアドレスが、ＩＰアドレス８０ｃまたは自己のＩＰアドレス８０ｂであるかにより行う。また、ＬＡＮアナライザ１ａにおけるキャプチャー停止通知の判定は、発信元ＩＰアドレスがＬＡＮアナライザ１ｂのＩＰアドレス８０ｅであるかにより行う。いずれの場合も、さらに、取り込んだパケットがＰｉｎｇコマンドであるかどうかを併せて判別してもよい。

【００２４】

プロトコル検査部１５は、ネットワーク８から取り込んだパケットにプロトコル異常があるかを判定する。例えば、プロトコル検査部１５は、プロトコルの下位階層の異常を検出する。プロトコルの異常があったときは、データ取得制御部１６へその旨を通知する。

【００２５】

データ取得制御部１６は、キャプチャー部１２が行うキャプチャーを停止させるなど、キャプチャーの制御を行う。例えば、データ判別部１４から、特定のパケットを受信したことの通知を受けたり、プロトコル検査部１５からプロトコル異常の通知を受けたりすると、キャプチャー部１２に対してキャプチャーを停止させるように指示する。キャプチャーの停止とは、例えば、その特定のパケットより後のパケットを保持しないようにすることである。つまり、特定のパケットより後にネットワーク上を伝送されてくるパケットは、データ取込部１２１が取り込まないように制限してもよいし、特定のパケットより後にネットワーク上を伝送されてきて、データ取込部１２１が取り込んだパケットについては、データ保持部１２２へ書き込まないようにしてもよい。

【００２６】

こうすることで、特定のパケットを受信した以降、データ保持部１２２の記憶内容が更新されて、書きかえられてしまうことを回避できる。その結果、特定のパケットを受信する直前にネットワーク上に存在したパケットに関する情報がデータ保持部１２２に残って保持され続け、上書きされてしまうことがない。

【００２７】

また、データ取得制御部１６は、上述のようにしてキャプチャー部１２にキャプチャーを停止させると、これを別セグメントのＬＡＮアナライザ１、あるいは、監視端末４など、他の装置へ通知するためのパケットを生成して、送信する。例えば、ＬＡＮアナライザ１ａのデータ取得制御部１６は、ＩＰアドレス記憶部１３を参照して、ＬＡＮアナライザ１ｂおよび監視端末４へキャプチャー停止を通知するためのパケットを生成し、ネットワーク８ａへ出力する。

【００２８】

また、別セグメントのＬＡＮアナライザ１からのキャプチャー停止通知を受けてキャプチャーを停止させたときは、そのキャプチャー停止通知の送信元のＬＡＮアナライザ１に対してキャプチャー停止完了を通知するためのリプライを返しても良い。

【００２９】

さらに、データ取得制御部１６は、キャプチャーが停止しているときに、データ保持部１２２に保持されているログデータをデータベース１７へコピーする。データベース１７へのコピーが完了すると、データ取得制御部１６はキャプチャー部１２に対して、キャプチャーを再開するよう指示しても良い。

【００３０】

また、データ取得制御部１６は、データ保持部１２２に保持されているログデータを監視端末４へ送信する。ここで、監視端末４へ送信するデータは、データ保持部１２２に保持されている全データであっても良いし、一部のデータ（例えば、取り込んだ日時が新しいものから所定時間内のもの）であってもよい。このとき、データ保持部１２２からデータベース１７へコピーされたデータを用いて転送しても良い。

【００３１】

監視端末４がログデータを受信すると、これを報知するために図示しない表示装置にポップアップウィンドウでエラーメッセージを表示したり、警報音を発したりしても良い。また、ネットワークの保守担当者は、監視端末４で受信したログデータを図示しない表示装置、プリンタなどへ出力して、エラーの原因解析に利用できる。

【００３２】

入出力制御部１８は、入力装置１０１および表示装置１０２の制御を行う。例えば、入力装置１０１から入力を受け付け、表示装置１０２にデータ保持部１２２に保持しているログデータを表示させる。

【００３３】

次に、ホストコンピュータ２について説明する。ホストコンピュータ２ａおよびホストコンピュータ２ｂには、それぞれＩＰアドレス８０ａ，８０ｄが割り振られていて、相互に通信を行い、所定のアプリケーションを実行することができる。

【００３４】

ホストコンピュータ２の詳細な構成を図２（ｂ）に示す。同図に示すように、ホストコンピュータ２は、通信制御部２１と、１以上のデータ処理部２２と、データ処理部２２でのエラー発生を検出するエラー検出部２３と、ＩＰアドレス記憶部２４を、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【００３５】

通信制御部２１は、ネットワーク上の他の装置との通信を制御する。例えば、ＬＡＮ８上のパケットを取得し、自コンピュータ２宛てのパケットを受け付ける。また、ネットワーク上の他の装置へ送信するために、パケットを生成して、ＬＡＮ８へ出力する。

【００３６】

データ処理部２２は、通信制御部２１が受け付けたパケットが示す情報に基づいて、ユーザが定義した所定のアプリケーション処理を行う。

【００３７】

エラー検出部２３は、データ処理部２２であらかじめ定められた事象が発生したかどうかを監視し、当該事象が発生するとそれを検出する。エラー検出部２３が検出すべき事象

は、ユーザが任意に指定することができる。たとえば、データ処理部２２における処理の異常終了、他の装置との通信処理におけるタイムアウト等の通信不良、プロトコルの上位階層でのエラー等を検出するようにしてもよい。さらに、いわゆる警告のような軽微な不具合をエラーとして検出するようにしてもよい。

【００３８】

さらに、エラー検出部２３がエラーを検出すると、ＩＰアドレス記憶部２４に記憶されているＩＰアドレスの装置に対してＡＰエラーの検出を通知する。例えば、ＩＰアドレス記憶部２４に記憶されているＩＰアドレスへ宛てて、ＡＰエラー通知としてＰｉｎｇコマンドを発行するように通信制御部２１へ指示する。

【００３９】

ＩＰアドレス記憶部２４は、同一セグメントおよび別セグメントのテスト用コンピュータ３あるいはＬＡＮアナライザ１に設定されたＩＰアドレスを記憶する。例えば、ホストコンピュータ２ａのＩＰアドレス記憶部２４には、テスト用コンピュータ３ａのＩＰアドレス８０ｃと、ＬＡＮアナライザ１ａのＩＰアドレス８０ｂとが記憶される。ホストコンピュータ２ｂのＩＰアドレス記憶部２４には、ＬＡＮアナライザ１ｂのＩＰアドレス８０ｅが記憶される。

【００４０】

テスト用コンピュータ３ａは、ネットワークトラブルの解析用に設置されるコンピュータである。したがって、通常時には設置する必要はない。各テスト用コンピュータ３ａには、それぞれＩＰアドレス８０ｃが割り振られている。テスト用コンピュータ３は、ＩＰアドレスを割り振って、ネットワーク８に接続できる装置であればなんでもよい。

【００４１】

次に、ＬＡＮアナライザ１の処理手順について、図３のフローチャートを用いて説明する。

【００４２】

まず、ＬＡＮアナライザ１が動作を開始すると、キャプチャー部１２がネットワーク８上のパケットを取り込み、データ保持部１２２へ格納する（Ｓ１１）。

【００４３】

次に、プロトコル検査部１５は、取り込んだパケットを解析し、プロトコルに異常がないか検査する（Ｓ１２）。また、データ判別部１４は、取り込んだパケットがホストコンピュータ２からのＡＰエラー通知であったかの判定（Ｓ１３）、および、別セグメントのＬＡＮアナライザ１からのキャプチャー停止通知であったかを判定する（Ｓ１４）。なお、ステップＳ１２～Ｓ１４は、これ以外の順序で判定を行ってもよい。また、ステップＳ１２～Ｓ１４の処理は、ステップＳ１１のデータ保持部１２２へのデータ格納前に行ってもよい。

【００４４】

ステップＳ１２～Ｓ１４のいずれかにも該当しない場合は、ステップＳ１１へ戻る。一方、ステップＳ１２～Ｓ１４のいずれかに該当する場合は、データ取得制御部１６の指示に基づき、キャプチャー部１２はキャプチャーを停止する（Ｓ１５）。

【００４５】

キャプチャーが停止すると、データ取得制御部１６がキャプチャー停止通知パケットを生成し、他のＬＡＮに属するＬＡＮアナライザ１へ送信する（Ｓ１６）。

【００４６】

次に、データ保持部１２２に格納されているログデータがデータベース１７へ格納され（Ｓ１７）、監視端末４へ転送される（Ｓ１８）。

【００４７】

これにより、ＷＡＮにおいて、あるセグメントのＬＡＮアナライザ１がエラーなどを検知してキャプチャーを停止すると、別セグメントのＬＡＮアナライザのキャプチャーも停止させることができる。この結果、あるＬＡＮアナライザ１がエラーを検知してキャプチャーを停止させたときに、そのエラーの原因が別セグメントのホストコンピュータ２から

受信したデータにあるようなときでも、別セグメントのＬＡＮアナライザ１のログを確保できるので、その原因究明が容易になる。

【００４８】

上述した本発明の実施形態は、本発明の説明のための例示であり、本発明の範囲をそれらの実施形態にのみ限定する趣旨ではない。当業者は、本発明の要旨を逸脱することなしに、他の様々な態様で本発明を実施することができる。

【図面の簡単な説明】

【００４９】

【図１】本発明の一実施形態に係るネットワークシステムの構成図である。

【図２】ＬＡＮアナライザおよびホストコンピュータの詳細な構成図である。

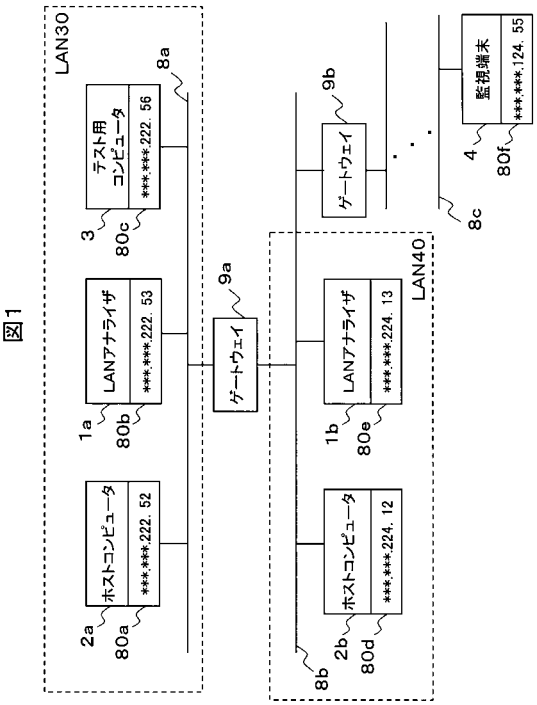
【図３】ＬＡＮアナライザの処理手順を示すフローチャートである。

【符号の説明】

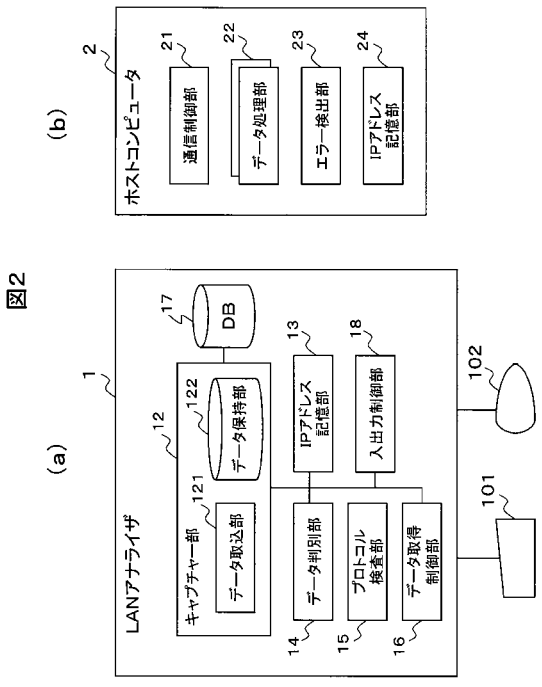
【００５０】

１…ＬＡＮアナライザ、２…ホストコンピュータ、４…監視端末、８…ネットワーク、９…ゲートウェイ、１２…キャプチャー部、１６…データ取得制御部

【図１】

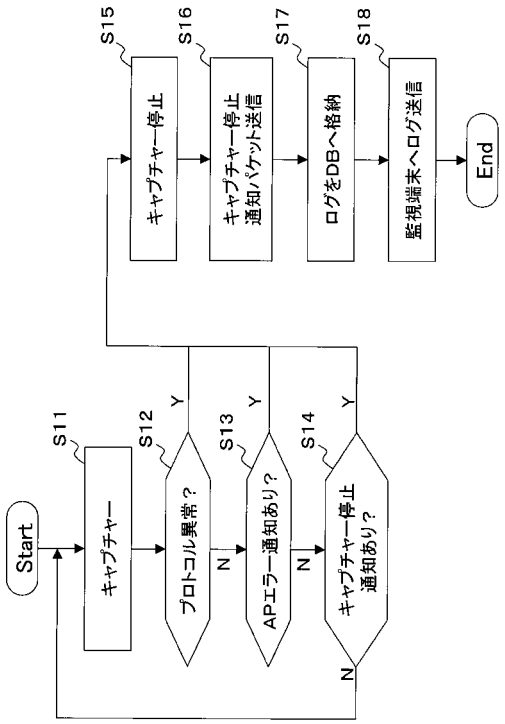


【図２】



【図３】

図3


Start
S11
キャプチャー
S12
プロトコル異常？
Y
N
S13
APエラー通知あり？
Y
N
S14
キャプチャー停止
通知あり？
Y
N
S15
キャプチャー停止
S16
キャプチャー停止
通知パケット送信
S17
ログをDBへ格納
S18
監視端末へログ送信
End

フロントページの続き

(72)発明者　武貞　睦治
神奈川県横浜市戸塚区品濃町５０４番地２　日立電子サービス株式会社内

Ｆターム(参考) 5K030 GA14 HA08 HD03 JA10 KA02 MA04 MC08
5K035 AA03 BB01 DD01 EE01 LL01

【要約の続き】
【選択図】　図１