

(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2010-141655
(P2010-141655A)

(43) 公開日 平成22年6月24日(2010.6.24)

(51) Int.Cl.	F I	テーマコード (参考)
HO4L 12/56 (2006.01)	HO4L 12/56 400Z	5B089
GO6F 13/00 (2006.01)	GO6F 13/00 351N	5K030

審査請求 未請求 請求項の数 5 O L (全 14 頁)

(21) 出願番号 特願2008-316681 (P2008-316681)
(22) 出願日 平成20年12月12日 (2008.12.12)

(71) 出願人 000006507
横河電機株式会社
東京都武蔵野市中町2丁目9番32号
(72) 発明者 川俣 創
東京都武蔵野市中町2丁目9番32号 横河電機株式会社内
Fターム(参考) 5B089 GB02 JA35 JA36 JA37 KA12
KC48 MC06
5K030 GA14 HD03 JA10 MA04 MA06
MA07 MB03 MB06 MB09 MC08

(54) 【発明の名称】 ネットワーク監視装置

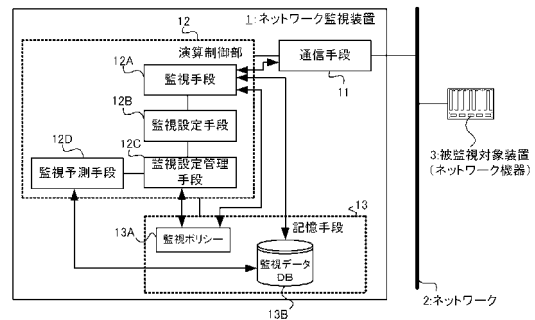
(57) 【要約】

【課題】 障害解析に必要な監視データを適切に把握できるネットワーク監視装置を実現すること。

【解決手段】 ネットワークを介し被監視対象装置と接続され、監視ポリシーを設定する監視設定手段と、前記監視ポリシーに基づき前記ネットワークまたは前記被監視対象装置の状態を示す監視データを取得する監視手段とを有するネットワーク監視装置において、前記監視手段により得られた過去および/または現在の監視データに基づき、前記ネットワークまたは前記被監視対象装置の将来の状態を示す予測監視データを予測・算出する監視予測手段と、前記監視予測手段により算出された前記予測監視データに基づき前記監視ポリシーを変更する監視設定管理手段と、を具備することを特徴とする。

【選択図】

図 1



【特許請求の範囲】**【請求項 1】**

ネットワークを介し被監視対象装置と接続され、監視ポリシーを設定する監視設定手段と、前記監視ポリシーに基づき前記ネットワークまたは前記被監視対象装置の状態を示す監視データを取得する監視手段とを有するネットワーク監視装置において、

前記監視手段により得られた過去および/または現在の監視データに基づき、前記ネットワークまたは前記被監視対象装置の将来の状態を示す予測監視データを予測・算出する監視予測手段と、

前記監視予測手段により算出された前記予測監視データに基づき前記監視ポリシーを変更する監視設定管理手段と、

を具備することを特徴とするネットワーク監視装置。

10

【請求項 2】

前記監視予測手段は、

任意の予測モデルに基づき前記予測監視データを算出し、前記監視ポリシーを変更して監視の頻度の増大および監視対象と監視項目とを拡大することを特徴とする

請求項 1 記載のネットワーク監視装置。

【請求項 3】

前記監視設定管理手段は、

前記監視予測手段により算出された前記予測監視データに基づいて、前記ネットワークまたは前記被監視対象装置に将来障害が検出されるものと予測される場合は、前記監視ポリシーを変更して監視の頻度の増大および監視対象と監視項目とを拡大することを特徴とする

請求項 1 または請求項 2 記載のネットワーク監視装置。

20

【請求項 4】

前記監視設定管理手段は、

前記監視予測手段により算出された前記予測監視データに基づいて、前記ネットワークまたは前記被監視対象装置のサービスレベルが将来低下するものと予測される場合は、前記監視ポリシーを変更して監視の頻度の増大および監視対象と監視項目とを拡大することを特徴とする

請求項 1 ~ 請求項 3 いずれかに記載のネットワーク監視装置。

30

【請求項 5】

前記監視予測手段は、

前記監視データに基づいてあらかじめ記憶されている複数の予測モデルを用いて同時に計算し、予測精度が最も高い予測モデルを選択して予測監視データを予測・算出することを特徴とする

請求項 1 ~ 請求項 4 いずれかに記載のネットワーク監視装置。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、各種機器が接続されるネットワークシステムの性能を把握するネットワーク監視装置に関し、特にネットワークの性能の変動をより精度高く予測することに関する。

40

【背景技術】**【0002】**

ネットワークを介して複数のサーバ、ルータやスイッチなどの中継機器（以下、ネットワーク機器という）やサーバマシン、クライアントマシンなどの各種端末が接続されるネットワークシステムでは、サーバへの過大な要求や攻撃、故障の発生などによりその性能が劣化してしまうことがある。そこで、従来から、このようなネットワークシステムを理想的に稼働させるために、ネットワークシステムの性能を測定・監視・モニタリングするネットワーク監視装置が提案されている。

【0003】

50

従来のネットワーク監視装置は、事前に定義されたモニタリング条件などの監視内容である監視ポリシーに従ってモニタリングを実行する。この監視ポリシーは監視対象、その監視対象に関する監視項目、監視する所定のインターバルなどがあらかじめ定められたものであり、ネットワーク・ネットワークシステムの状態が変化した場合でも不変のままモニタリングが実行されていた。

【0004】

ところで、従来のネットワーク監視装置は、監視ポリシーの変更が必要となる場合は、ネットワーク管理者が手動で監視ポリシーの設定・変更を行っていた。しかしながら刻一刻と変化するネットワークに対する監視では、ネットワーク管理者が手動で設定・変更を行っていると、その時々状況に応じて柔軟に適切な監視ポリシーを設定することが難しいという問題があった。

10

【0005】

一方、可能な限りの監視対象および監視項目をあらかじめ設定しておき、常にネットワークの情報を漏れなくモニタリングする方法がある。しかしながら、監視対象であるネットワーク機器やネットワーク、ネットワークシステム全体に多大な負荷をかけてしまうといった新たな問題がある。

【0006】

他方、従来のネットワーク監視装置では、ネットワークの状態に応じて動的に監視項目を変更する方法がある。この場合、監視対象機器などに与える負荷を最小限に抑えつつ、ネットワーク管理者による監視設定が行われるまでのタイムラグが無くなり、監視を常に効率良く行うことができるといったメリットがある。

20

【0007】

このようなネットワーク監視装置に関連する先行技術文献として、下記の特許文献1がある。

【0008】

【特許文献1】特開2005-275815号公報

【0009】

図6は従来のネットワーク監視装置の構成例を示す構成図であり、図6において、ネットワーク監視装置1は、イーサネット（登録商標）などの有線ネットワークであるネットワーク2を介してたとえばWebサーバなどを提供するサーバまたはネットワーク機器等である被監視対象装置3と接続されている。また特に図示していないが、ネットワーク2と、被監視対象装置3と、図示しないその他のネットワーク機器・各種端末装置とは、ネットワークシステムを構成する。

30

【0010】

ネットワーク監視装置1は、ネットワーク2を介して被監視対象装置3とデータ通信を行う通信手段11、各部・各手段の動作を制御する演算制御部12、記憶手段13などから構成され、ネットワーク2およびネットワークシステム全体の動作を監視する。演算制御部12は、監視手段12Aと、監視設定手段12Bと、監視設定管理手段12Cとを有する。

【0011】

監視手段12Aは、あらかじめ設定されている監視ポリシーに基づいて通信手段11を介して得られる監視対象である被監視対象装置3からのデータを収集し、被監視対象装置3、ネットワーク2およびネットワークシステムの挙動を監視・モニタリングする。

40

【0012】

これらのデータに基づいてネットワーク2およびネットワークシステム全体の性能を示す性能評価値の基となる性能基礎データを算出し記憶手段13に記憶する。いいかえれば監視手段12Aはネットワーク2およびネットワークシステムの挙動を監視・モニタリングする。

【0013】

監視設定手段12Bは、記憶手段13に記憶されている監視ポリシーを設定する。監視

50

設定管理手段 1 2 C は、監視手段 1 2 A により得られた監視結果に基づいて最適な監視内容を導き出し、記憶手段 1 3 に記憶されている監視ポリシーの再設定・変更を実行する。

【 0 0 1 4 】

記憶手段 1 3 は、監視対象・その監視対象に関する監視項目・監視する所定のインターバルなどが関連づけて格納されている監視ポリシー 1 3 A と、監視手段 1 2 A により収集・算出された、たとえばレスポンスタイム、トラフィック量、エラーパケット数などの監視データと測定時の年月日などが関連づけて格納されている監視データ D B 1 3 B と、を有する。

【 0 0 1 5 】

図 7 は従来のネットワーク監視装置の動作を説明するフロー図である。ステップ S P 1 0 1 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視手段 1 2 A は、監視設定手段 1 2 A により設定された監視ポリシーに基づき被監視対象装置 3 の挙動を監視し、監視データを収集し得られたデータを記憶手段 1 3 に記憶する。

10

【 0 0 1 6 】

具体的には、監視手段 1 2 A は監視ポリシーに基づき、図示しない W E B クライアント（またはネットワーク監視装置 1 ）からのリクエストに応じて W E B サーバ（被監視対象装置 3 ）が対応する処理を実行し、 W E B クライアントが処理結果を受信するまでの時間（以下、レスポンスタイムという）を、当該 W E B サーバにインストールされたソフトウェアなどを利用して 1 0 分間隔で測定し、得られたレスポンスタイムを記憶手段 1 3 に記憶する。

20

【 0 0 1 7 】

ステップ S P 1 0 2 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視手段 1 2 A は、収集した監視データに基づいて、ネットワーク 2、被監視対象装置 3、ネットワークシステムで障害が検知されたか否か判定する。障害が検知されればステップ S P 1 0 3 に移行し、それ以外の場合はステップ S P 1 0 1 に移行する。

【 0 0 1 8 】

ステップ S P 1 0 3 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視設定管理手段 1 2 C は、障害が検知された監視データに基づき、新たに監視すべき監視項目を抽出し記憶手段 1 3 に記憶されている監視ポリシーに追加する。

【 0 0 1 9 】

具体的には、監視設定管理手段 1 2 C は、図示しないクライアント（またはネットワーク監視装置 1 ）から被監視対象装置 3 までのネットワーク経路のトラフィック量と被監視対象装置 3 の C P U 使用率を監視項目として自動的に追加する。

30

【 0 0 2 0 】

ステップ S P 1 0 4 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視手段 1 2 A は、監視ポリシーに基づき、レスポンスタイムに加えてトラフィック量と被監視対象装置 3 の C P U 使用率のモニタリングを開始し、得られた監視データを記憶手段 1 3 に記憶する。

【 0 0 2 1 】

ここで、ネットワーク管理者が新たに追加された監視項目であるトラフィック量の監視値に基づき検討すれば、あるネットワーク経路上での輻輳を見つけ出し、それを解決することが可能となる。

40

【 0 0 2 2 】

ステップ S P 1 0 5 において、監視手段 1 2 A は、収集した通信データに基づいて、ネットワークシステムで障害が検知されたか否か判定する。障害が検知されればステップ S P 1 0 3 に移行し、それ以外の場合はステップ S P 1 0 6 に移行する。

【 0 0 2 3 】

ステップ S P 1 0 6 において、監視設定管理手段 1 2 C は、被監視対象装置 3 における障害がないものと判断されると、ステップ S P 1 0 4 にて新たに追加した監視項目を削除する。

50

【 0 0 2 4 】

具体的には、監視設定管理手段 1 2 C は、レスポンスタイム（たとえば 4 0 ミリ秒など）が閾値（たとえば 5 0 ミリ秒など）を下回れば、ステップ S P 1 0 4 にて新たに追加した監視項目である、トラフィック量と C P U 使用率を監視ポリシーから削除する。

【 0 0 2 5 】

このように、従来のネットワーク監視装置では、ネットワークの状態に応じて動的に監視項目を変更できる。

【 発明の開示 】

【 発明が解決しようとする課題 】

【 0 0 2 6 】

しかしながら、従来のネットワーク監視装置は、障害を検知してから監視項目の追加を行うので、被監視対象装置 3 の障害が起きた時点での状況（いいかえればリアルタイムの状況）およびそれ以前の状況が分からないという問題点があった。そうすると、障害解析に必要な情報が抜けてしまい、適切な解析および監視項目の設定が行えないという問題点があった。

【 0 0 2 7 】

図 8 は従来のネットワーク監視装置の問題点の説明図であり、図 8 において、たとえば、以下のように状態推移していた場合であると障害の原因（輻輳発生）が特定できないという問題点があった。

時刻 A) ネットワーク 2 上で輻輳が発生

時刻 B) ネットワーク監視装置 1 が W e b サーバである被監視対象装置 3 に H T T P リクエスト送信し、被監視対象装置 3 を監視

時刻 B) ネットワーク監視装置 1 が H T T P レスポンスを受信しレスポンスタイムを取得。また監視手段 1 2 A は H T T P レスポンスタイムが閾値を超えたものと判断し障害を検知。

時刻 D) ネットワーク 2 上に発生していた輻輳が一時的に解消

時刻 E) 監視設定管理手段 1 2 C は、監視ポリシーにトラフィック量と C P U 使用率を監視項目として追加

時刻 F) 監視手段 1 2 A は、追加された監視項目についてもモニタリングを開始

時刻 G) 監視手段 1 2 A によりモニタリングされたトラフィック量は、輻輳が一時的に解消されているので、自動的に新たに追加された監視項目は削除される。

【 0 0 2 8 】

このように、監視手段 1 2 A が障害を検知した後で一時的にネットワーク 2 上での輻輳が解消すると、問題無い監視データを取得することになるので、 H T T P レスポンスタイムが閾値を超えた原因が特定できないという問題点があった。

【 0 0 2 9 】

そうすると、従来のネットワーク監視装置では、図 8 (B) のように、ネットワーク 2 上で短時間に繰り返し生じる輻輳（パースト的に発生する輻輳）についても、監視手段 1 2 A が障害を検知した後で一時的にネットワーク 2 上での輻輳が解消するとあたかも問題無い監視データを取得することになり（これを繰り返すことになってしまい）障害の原因が特定できないという問題点があった。

【 0 0 3 0 】

本発明は上述の問題点を解決するものであり、その目的は、障害解析に必要な監視データを適切に把握できるネットワーク監視装置を実現することにある。

【 課題を解決するための手段 】

【 0 0 3 1 】

このような課題を達成するために、本発明のうち請求項 1 記載の発明は、

ネットワークを介し被監視対象装置と接続され、監視ポリシーを設定する監視設定手段と、前記監視ポリシーに基づき前記ネットワークまたは前記被監視対象装置の状態を示す監視データを取得する監視手段とを有するネットワーク監視装置において、

10

20

30

40

50

前記監視手段により得られた過去および／または現在の監視データに基づき、前記ネットワークまたは前記被監視対象装置の将来の状態を示す予測監視データを予測・算出する監視予測手段と、

前記監視予測手段により算出された前記予測監視データに基づき前記監視ポリシーを変更する監視設定管理手段と、
を具備することを特徴とするネットワーク監視装置である。

【0032】

請求項2記載の発明は、請求項1記載のネットワーク監視装置において

前記監視予測手段は、

任意の予測モデルに基づき前記予測監視データを算出し、前記監視ポリシーを変更して監視の頻度の増大および監視対象と監視項目とを拡大することを特徴とする。

10

【0033】

請求項3記載の発明は、請求項2記載のネットワーク監視装置において

前記監視設定管理手段は、

前記監視予測手段により算出された前記予測監視データに基づいて、前記ネットワークまたは前記被監視対象装置に将来障害が検出されるものと予測される場合は、前記監視ポリシーを変更して監視の頻度の増大および監視対象と監視項目とを拡大することを特徴とする。

【0034】

請求項4記載の発明は、請求項1～請求項3いずれかに記載のネットワーク監視装置において、

20

前記監視設定管理手段は、

前記監視予測手段により算出された前記予測監視データに基づいて、前記ネットワークまたは前記被監視対象装置のサービスレベルが将来低下するものと予測される場合は、前記監視ポリシーを変更して監視の頻度の増大および監視対象と監視項目とを拡大することを特徴とする。

【0035】

請求項5記載の発明は、請求項1～請求項4いずれかに記載のネットワーク監視装置において、

前記監視予測手段は、

30

前記監視データに基づいてあらかじめ記憶されている複数の予測モデルを用いて同時に計算し、予測精度が最も高い予測モデルを選択して予測監視データを予測・算出することを特徴とする。

【発明の効果】

【0036】

このように、本発明に係るネットワーク監視装置は、本発明に係るネットワーク監視装置は、監視手段が監視設定手段によって設定された監視ポリシーに基づき、ネットワークまたは被監視対象装置の状態を示す監視データを取得し、監視予測手段が得られた過去および現在の監視データから予測監視データを算出・予測し、監視設定管理手段がこの予測データに基づき監視ポリシーを変更することにより、ネットワークの状態を予測しこの予測された状態に応じて動的に監視項目を変更でき、障害解析に必要な監視データを適切に把握できる。

40

【発明を実施するための最良の形態】

【0037】

図1は本発明に係るネットワーク監視装置の一実施例を示す構成図であり、図6などと共通する部分には同一の符号を付けて適宜説明を省略する。図1と図6との相違点は、図1では監視手段12Aにより監視された過去の監視データおよび現在の監視データに基づき将来の監視データを予測する監視予測手段12Dを有する点、監視設定管理手段12Cが監視予測手段12Dで予測された将来の監視データに基づき将来検知されうる障害に応じた監視ポリシーの監視項目を設定する点などである。

50

【0038】

図1において、ネットワーク監視装置1は、イーサネット（登録商標）などの有線ネットワークであるネットワーク2を介してたとえばWebサーバなどを提供するサーバまたはネットワーク機器等である被監視対象装置3と接続されている。また特に図示していないが、ネットワーク2と、被監視対象装置3と、図示しないその他のネットワーク機器・各種端末装置とは、ネットワークシステムを構成する。

【0039】

ネットワーク監視装置1は、ネットワーク2を介して被監視対象装置3とデータ通信を行う通信手段11、各部・各手段の動作を制御する演算制御部12、記憶手段13などから構成され、ネットワーク2およびネットワークシステム全体の動作を監視する。演算制御部12は、監視手段12Aと、監視設定手段12Bと、監視設定管理手段12C、監視予測手段12Dとを有する。

10

【0040】

監視手段12Aは、あらかじめ設定されている監視ポリシーに基づいて通信手段11を制御してネットワーク2を介して被監視対象装置3から監視データを収集し、被監視対象装置3、ネットワーク2およびネットワークシステムの挙動を監視・モニタリングする。

【0041】

また監視手段12Aは、これらのデータに基づいてネットワーク2およびネットワークシステム全体の性能を示す性能評価値の基となる性能基礎データを算出し記憶手段13に記憶してネットワーク2およびネットワークシステムの挙動を監視・モニタリングするものでもよい。

20

【0042】

監視設定手段12Bは、記憶手段13に記憶されている監視ポリシーを設定する。監視設定管理手段12Cは、監視手段12Aにより得られた監視結果に基づき最適な監視内容を導き出して記憶手段13に記憶されている監視ポリシーの再設定・変更を実行し、また監視予測手段12Dで予測された将来の監視データに基づき将来検知されうる障害に応じた監視ポリシーの監視項目を設定する。

【0043】

たとえば、監視設定管理手段12Cは、監視予測手段12Dによりネットワーク2または被監視対象装置3のサービスレベルが低下するものと予測される場合は、監視ポリシー13Aで設定されている監視内容を変更して監視の頻度の増大、および監視対象と監視項目とを拡大するものでもよい。

30

【0044】

監視予測手段12Dは、記憶手段13に記憶されている監視手段12Aが監視した過去の監視データおよび現在の監視データに基づき将来のネットワークまたは被監視対象装置3の状態を予測する、つまり将来得られる監視データ（以下予測監視データという）を予測する。

【0045】

記憶手段13は、監視対象・その監視対象に関する監視項目・監視する所定のインターバルなどが関連づけて格納されている監視ポリシー13Aと、監視手段12Aにより収集・算出された、たとえばレスポンスタイム、トラフィック量、エラーパケット数などの監視データと測定時の年月日などが関連づけて格納されている監視データDB13Bと、を有する。

40

【0046】

図2は本発明のネットワーク監視装置の動作を説明するフロー図である。ステップSP201において、ネットワーク監視装置1の演算制御部12の監視手段12Aは、監視設定手段12Aにより設定された監視ポリシーに基づき被監視対象装置3の挙動を監視し、監視データを収集し得られたデータを記憶手段13に記憶する。

【0047】

具体的には、監視手段12Aは監視ポリシーに基づき、図示しないWEBクライアント

50

(またはネットワーク監視装置1)からのリクエストに応じてWEBサーバ(被監視対象装置3)が対応する処理を実行し、WEBクライアントが処理結果を受信するまでの時間(以下、レスポンスタイムという)を、当該WEBサーバにインストールされたソフトウェアなどを利用して10分間隔で測定し、得られたレスポンスタイムを記憶手段13に記憶する。

【0048】

ステップSP202において、ネットワーク監視装置1の演算制御部12の監視予測手段12Dは、記憶手段13に格納されている監視手段12Aにより収集・監視した過去の監視データおよび現在の監視データに基づき将来の監視データ(以下、予測監視データという)を予測・算出する。(具体的な動作の一例については図3にて後述する。)

10

【0049】

ステップSP203において、ネットワーク監視装置1の演算制御部12の監視予測手段12Dは、予測監視データに基づいて、ネットワーク2、被監視対象装置3、ネットワークシステムで将来障害が検知されるか否か判定する。障害が検知されればステップSP204に移行し、それ以外の場合はステップSP201に移行する。

【0050】

たとえば監視予測手段12Dは、予測監視データに基づいて、予測監視データの一例である、レスポンスタイムが3時間後にあらかじめ記憶手段13に設定記憶されている閾値(例えば50ミリ秒など)を超えた場合には障害が検知されたものとして判定する。

【0051】

20

ステップSP204において、ネットワーク監視装置1の演算制御部12の監視設定管理手段12Cは、将来障害が検知されうる予測監視データに基づき、新たに監視すべき監視項目を抽出し記憶手段13に記憶されている監視ポリシーに追加する。または監視ポリシーを変更するものでもよい。

【0052】

具体的には、監視設定管理手段12Cは、図示しないクライアント(またはネットワーク監視装置1)から被監視対象装置3までのネットワーク経路のトラフィック量と被監視対象装置3のCPU使用率を監視項目として自動的に追加する。レスポンスタイムはデータ転送時間(リクエストにかかる時間+レスポンスにかかる時間)とWebサーバでの処理時間の和であるため、レスポンスタイムはトラフィック量とCPU使用率の影響を受けるためである。

30

【0053】

なお、監視設定管理手段12Cは、監視予測手段12Dが将来ネットワークまたは前記被監視対象装置のサービスレベルが低下するものと予測する場合は、監視ポリシーを変更して監視の頻度を増大させ、監視対象および監視項目を拡大する。

【0054】

また、監視設定管理手段12Cは、将来障害が検知されうる予測監視データおよび記憶手段13の監視ポリシー13Aに基づき、新たに監視すべき監視項目を抽出するものでもよい。

【0055】

40

たとえば、あらかじめ監視ポリシー13Aには、ポリシーのひとつとしてレスポンスタイムの詳細な監視にはトラフィック量・CPU使用率などの監視項目を監視すべき旨が記憶されており、監視設定管理手段12Cは、レスポンスタイムに基づき障害検知がなされた場合は、監視ポリシー13Aに基づいて新たに監視すべき監視項目トラフィック量・CPU使用率を抽出するものでもよい。

【0056】

ステップSP205において、ネットワーク監視装置1の演算制御部12の監視手段12Aは、監視ポリシーに基づき、レスポンスタイムに加え、トラフィック量と被監視対象装置3のCPU使用率のモニタリングを開始し、得られた監視データを記憶手段13に記憶する。

50

【 0 0 5 7 】

ステップ S P 2 0 6 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視手段 1 2 A は、収集した監視データに基づいて、ネットワーク 2、被監視対象装置 3、ネットワークシステムで障害が検知されたか否か判定する。障害が検知されればステップ S P 2 0 7 に移行し、それ以外の場合はステップ S P 2 0 9 に移行する。

【 0 0 5 8 】

ステップ S P 2 0 7 において、ネットワーク監視装置 1 の監視手段 1 2 A は、通信手段 1 1 を制御しネットワーク 2 を介して接続されている特に図示していないユーザのネットワーク管理用の端末に、ネットワークシステムなどで障害が検知された旨を知らせるメッセージ（メールなど）を送信する。または、ネットワーク監視装置 1 の演算制御手段 1 2 は、ネットワーク監視装置 1 に備えられている表示手段（図示せず）に障害が検知された旨を表示する。

10

【 0 0 5 9 】

ここで、この通知 / 表示により、ネットワーク管理者が新たに追加された監視項目であるトラフィック量の監視データに基づき検討して、あるネットワーク経路上での輻輳を見つけ出し、それを解決する。

【 0 0 6 0 】

ステップ S P 2 0 8 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視手段 1 2 A は、収集した監視データに基づいて、ネットワーク 2、被監視対象装置 3、ネットワークシステムで障害が検知されたか否か判定する。障害が検知されればステップ S P 2 0 7 に移行し、それ以外の場合はステップ S P 2 0 9 に移行する。

20

【 0 0 6 1 】

ステップ S P 2 0 9 において、ネットワーク監視装置 1 の演算制御部 1 2 の監視設定管理手段 1 2 C は、被監視対象装置 3 における障害がなくなったものと判断し、ステップ S P 2 0 4 にて新たに追加した監視項目を削除する。

【 0 0 6 2 】

具体的には、ネットワーク監視装置 1 の演算制御部 1 2 の監視設定管理手段 1 2 C は、レスポンスタイム（たとえば 4 秒など）が閾値（たとえば 5 0 ミリ秒など）を下回れば、ステップ S P 2 0 4 にて新たに追加した監視項目である、トラフィック量と C P U 使用率を監視ポリシーから削除する。

30

【 0 0 6 3 】

この結果、本発明に係るネットワーク監視装置は、監視手段が監視設定手段によって設定された監視ポリシーに基づき、ネットワークまたは被監視対象装置の状態を示す監視データを取得し、監視予測手段が得られた過去および現在の監視データから予測監視データを算出・予測し、監視設定管理手段がこの予測データに基づき監視ポリシーを変更することにより、ネットワークの状態を予測しこの予測された状態に応じて動的に監視項目を変更でき、障害解析に必要な監視データを適切に把握できる。

【 0 0 6 4 】

なお、本発明に係るネットワーク監視装置は、監視予測手段 1 2 D が予測した監視データにより問題発生が予測されうる場合は、その旨およびその監視データをネットワーク管理者に通知する予測監視データ通知手段を有するものであってもよい。この場合、予測監視データ通知手段は、通信手段 1 2 を制御してネットワーク 2 を介し接続されている特に図示していないユーザのネットワーク管理用の端末に、ネットワークシステムなどで障害が検知された旨を知らせるメッセージ（メールなど）を送信する。

40

【 0 0 6 5 】

このため、監視データにより問題発生が予測されうる場合に、監視データを障害発生前に事前にネットワーク管理者に通知することにより、障害の予知保全が可能となる。また、このような本発明による問題が生じうる予測監視データによる予知保全は、障害自体の予測に加えてさらにその障害解析に必要な情報を必要なタイミングで自動的に（効率良く）取得してできる点で、単なる未来予測による通常の予知保全よりも障害解析、障害の予

50

防に有効である。これにより、障害が予知されてから実際に対応するまでの時間を短縮できる。

【0066】

ここで、本発明に係るネットワーク監視装置は、監視予測手段12Dが過去の監視データおよび現在の監視データに基づき予測監視データを予測する一例について説明する。図3は本発明のネットワーク性能監視装置の動作を説明するフロー図である。

【0067】

図3において、ステップSP301において、ネットワーク性能監視装置1の演算制御部12の監視手段12Aは、ネットワーク機器3の監視データ（たとえばレスポンスタイム）を収集する。

【0068】

ステップSP302において、ネットワーク性能監視装置1の監視手段12Aは、監視データ（たとえばレスポンスタイム）とその測定を行った年月日などを関連づけて記憶手段13の蓄積情報DB13Bに蓄積・記憶する。

【0069】

ステップSP303において、ネットワーク性能監視装置の監視予測手段12Cは、蓄積情報DB13Aに蓄積・記憶された複数の監視データ（たとえばレスポンスタイム）に基づいて、記憶手段13に格納されている特に図示しない予測モデルDBに格納されている複数の予測モデルを用いて将来の応答時間を予測する。

【0070】

たとえば、監視予測手段12Cは、蓄積情報DB13Bに記憶されているレスポンスタイムに基づいて1ヶ月の平均レスポンスタイムを算出し、次月度の平均レスポンスタイムを算出（予測）する。図4は、過去の月間レスポンスタイムを示す説明図である。図5は各予測モデルによる予測監視データ（レスポンスタイム）を示す説明図であり、（A）は線形近似を用いたモデルによる予測結果、（B）は対数近似を用いたモデルによる予測結果、（C）は多項式近似を用いたモデルによる予測結果、（D）は累乗近似を用いたモデルによる予測結果、（E）は指数近似を用いたモデルによる予測結果である。

【0071】

監視予測手段12Dは、図8のように過去7ヶ月分の月間平均レスポンスタイム（1月：14ミリ秒、2月：18ミリ秒、3月：24ミリ秒・・・）を算出して記憶手段13に記憶し、図5のように各予測モデルを用いて次月度（8月度）のレスポンスタイムを予測して（たとえば（A）線形近似：34ミリ秒、（B）対数近似：30.6ミリ秒、（C）多項式近似：31.7ミリ秒、（D）累乗近似：31.9ミリ秒、（E）指数近似：36.8ミリ秒）記憶手段13に記憶する。

【0072】

ステップSP304において、監視予測手段12Dは、各モデルを用いて算出された予測結果の各予測精度を比較する。

【0073】

具体的には、監視予測手段12Dは、各予測モデルにおけるR-2乗値を算出し、このR-2乗値を用いて予測精度を比較する。このR-2乗値は、値が1に近づくほど信頼性が高くなることを示す。

【0074】

ステップSP305において、監視予測手段12Dは、予測精度を比較した結果、最も予測精度の高かった予測モデルを選択し、これより以降、応答時間の予測データを算出するための予測モデルとして設定・記憶する。たとえば図8の例では、R-2乗値が最も高い累乗近似を用いた予測モデルを選択する。

【0075】

ステップSP306において、監視予測手段12Dは、ステップSP305で選択された予測モデルを用いてレスポンスタイムの予測データを算出し、記憶手段13に記憶する。また図示しない表示部などに表示する。

10

20

30

40

50

【0076】

具体的には、監視予測手段12Dは、累乗近似を用いた予測モデルを用いて月間レスポンスタイムの予測値(31.9ミリ秒)を算出し、記憶手段13に記憶する。

【0077】

このように本発明のネットワーク性能監視装置は、ネットワークシステムの将来の監視データを予測することができる。

【0078】

また、上述の実施例のネットワーク性能監視装置では、被監視対象装置3(Webサーバ)が提供するWebサイトのリソースの取得にかかるレスポンスタイムに基づきネットワークの性能を把握すると説明しているが、特にこれに限定するものではなく、ICMPパケットを用いて応答時間を測定しネットワークの性能を把握するものであってもよい。

10

【0079】

また、本発明のネットワーク監視装置の演算制御部12は、記憶部13に格納されているOSなどを起動して、このOS上で格納されたプログラムを読み出して実行することによりネットワーク監視装置1全体(たとえば、演算制御部12はプログラムを読み出し実行することにより監視手段12A、監視設定手段12B、監視設定管理手段12C、監視予測手段12Dなどの各手段)を制御し、ネットワーク監視装置固有の動作を行うものでもよい。

【0080】

このとき記憶手段13は、演算制御手段12によって実行されるプログラムやアプリケーションをプログラム格納エリアに展開し、入力されたデータや、プログラムやアプリケーションの実行時に生じる処理結果などのデータをワークエリアに一時的に記憶する。

20

【0081】

以上説明したように、本発明では、ネットワーク監視装置が、ネットワークの状態を予測しこの予測された状態に応じて動的に監視項目を変更でき、障害解析に必要な監視データを適切に把握できるので、ネットワークの障害をより精度高く解析でき、解析結果に基づいて最適に通信資源を制御してネットワークシステム全体の障害の除去および適切な運転に貢献することができる。

【図面の簡単な説明】

【0082】

30

【図1】本発明に係るネットワーク監視装置の一実施例を示す構成図である。

【図2】本発明のネットワーク監視装置1の動作を説明するフロー図である。

【図3】本発明のネットワーク性能監視装置1の動作を説明するフロー図である。

【図4】過去の月間レスポンスタイムを示す説明図である。

【図5】各予測モデルによる予測監視データ(レスポンスタイム)を示す説明図である。

【図6】従来のネットワーク監視装置の構成例を示す構成図である。

【図7】従来のネットワーク監視装置の動作を説明するフロー図である。

【図8】従来のネットワーク監視装置の問題点の説明である。

【符号の説明】

【0083】

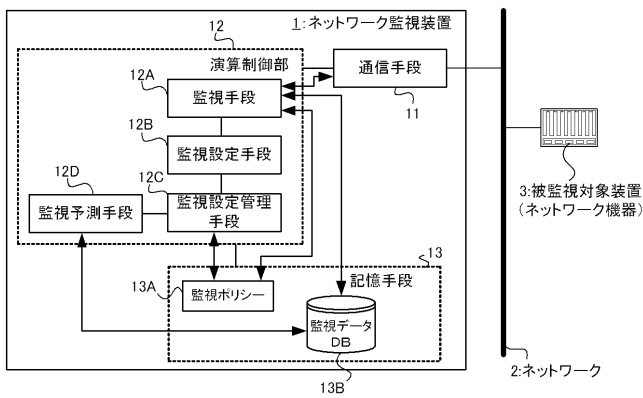
40

- 1 ネットワーク監視装置
 - 11 通信手段
 - 12 演算制御部
 - 12A 監視手段
 - 12B 監視設定手段
 - 12C 監視変更手段
 - 12D 監視予測手段
 - 13 記憶手段
 - 13A 監視ポリシー
 - 13B 監視データDB

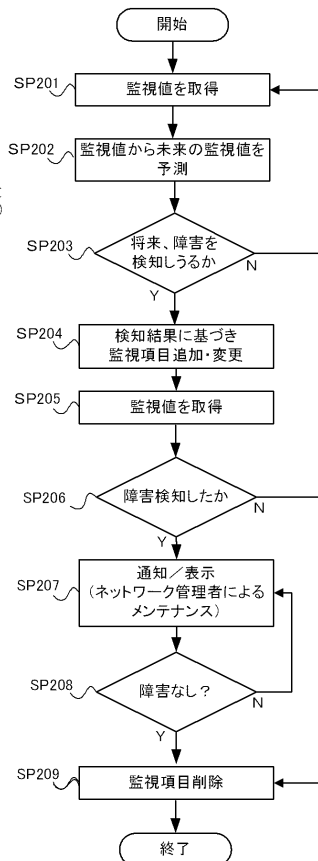
50

- 2 ネットワーク
- 3 ネットワーク機器

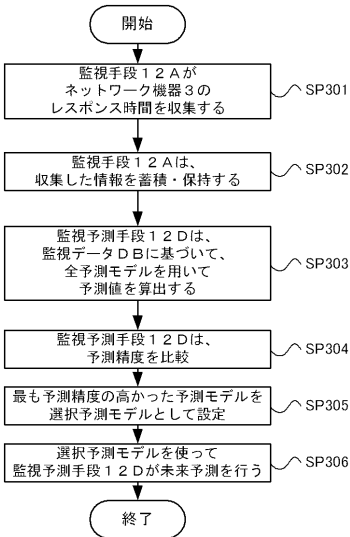
【図1】



【図2】



【 図 3 】



【 図 4 】

日付(○月度)	平均レスポンス時間(ミリ秒)
1	14
2	18
3	24
4	22
5	27
6	28
7	31

【 図 5 】

(A) 線形近似を用いた予測モデルと予測結果

予測レスポンス時間(8月度)	34.0
モデル式	$12.857 + 2.6429 * X$
R-2乗値	0.9238

(B) 対数近似を用いた予測モデルと予測結果

予測レスポンス時間(8月度)	30.6
モデル式	$13.233 + 8.3717 * \ln(X)$
R-2乗値	0.9315

(C) 多項式近似を用いた予測モデルと予測結果

予測レスポンス時間(8月度)	31.7
モデル式	$10.571 + -0.1905 * X^2 + 4.1667 * X$
R-2乗値	0.9381

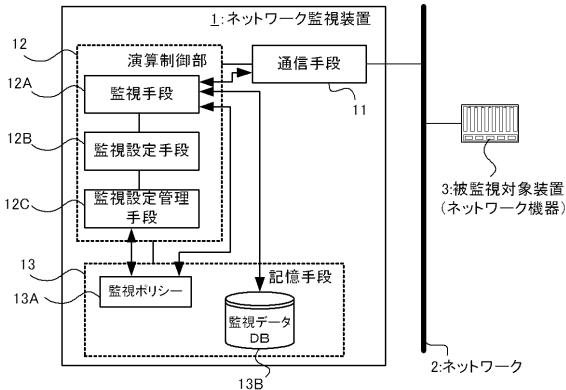
(D) 累乗近似を用いた予測モデルと予測結果

予測レスポンス時間(8月度)	31.9
モデル式	$14.026 * X^{0.3958}$
R-2乗値	0.9525

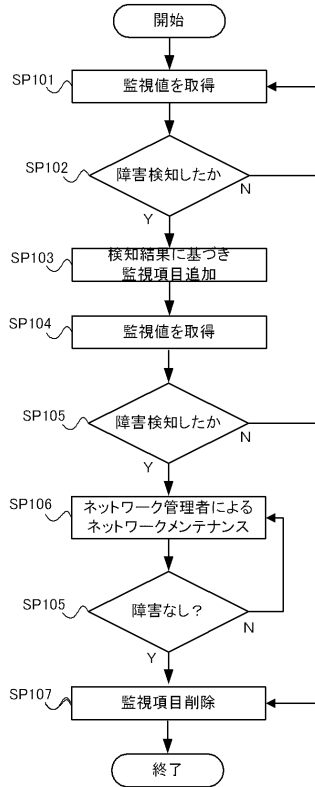
(E) 指数近似を用いた予測モデルと予測結果

予測レスポンス時間(8月度)	36.8
モデル式	$14.002 * e^{(0.1209 * X)}$
R-2乗値	0.885

【 図 6 】



【 図 7 】



【 図 8 】

