

(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  
2006年11月9日 (09.11.2006)

PCT

(10) 国際公開番号  
WO 2006/117833 A1

(51) 国際特許分類:

H04L 12/26 (2006.01)

(21) 国際出願番号:

PCT/JP2005/007773

(22) 国際出願日:

2005年4月25日 (25.04.2005)

(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(米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 岡田 利司郎 (OKADA, Toshiro) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 山崎 利哉 (YAMAZAKI, Toshiya) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 上

原 隆男 (UEHARA, Takao) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 渡部 章彦 (WATANABE, Akihiko); 〒1160013 東京都荒川区西日暮里5丁目11番8号 三共セントラルプラザビル5階 開明国際特許事務所 Tokyo (JP).

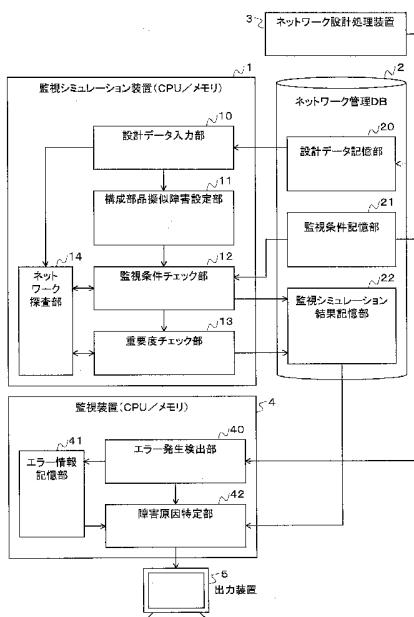
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ヨーラシア (AM, AZ,

/続葉有/

(54) Title: MONITORING SIMULATING DEVICE, METHOD, AND PROGRAM

(54) 発明の名称: 監視シミュレーション装置、方法およびそのプログラム



- 3...NETWORK DESIGNING DEVICE
- 1...MONITORING SIMULATION DEVICE (CPU/MEMORY)
- 10...DESIGN DATA INPUT SECTION
- 11...CONSTITUENT COMPONENT FALSE FAILURE SETTING SECTION
- 14...NETWORK EXAMINING SECTION
- 12...MONITORING CONDITION CHECK SECTION
- 13...IMPORTANCE DEGREE CHECK SECTION
- 2...NETWORK MANAGEMENT DB
- 20...DESIGN DATA STORAGE SECTION
- 21...MONITORING CONDITION STORAGE SECTION
- 22...MONITORING SIMULATION RESULT STORAGE SECTION
- 4...MONITORING DEVICE (CPU/MEMORY)
- 41...ERROR INFORMATION STORAGE SECTION
- 40...ERROR DETECTING SECTION
- 42...FAILURE CAUSE IDENTIFYING SECTION
- 5...OUTPUT DEVICE

(57) Abstract: A design data storage section (20) stores design data on constituent elements constituting a computer system to be monitored. A monitoring condition storage section (21) stores a monitoring condition of abnormal detection of the object to be monitored and error information to be outputted when the object meets the monitoring condition. A constituent component false failure setting section (11) makes a setting to cause the constituent elements in the design data to falsely fail one by one. A monitoring condition check section (12) checks if each monitoring condition is met when one constituent element is set in a failed state by instructing a network examining section (14) to examine the design data and extracts all the error information relevant to the met monitoring conditions. According to the results, information on the correspondence between the falsely failed constituent elements and all the extracted error information is stored in a monitoring simulation result storage section (22).

(57) 要約: 設計データ記憶部20は、監視対象のコンピュータシステムを構成する構成要素に関する設計データを記憶する。また、監視条件記憶部21は、監視対象に対する異常検出の監視条件と、監視対象が監視条件に該当する場合に出力すべきエラー情報とを記憶する。構成部品擬似障害設定部11は、設計データ中の各構成要素を、順に一つずつ擬似的に故障させる設定を行う。監視条件チェック部12は、各監視条件について、ネットワーク探査部14により設計データを探査することにより、一つの構成要素が故障状態に設定されている状態で監視条件が成立するか否かを調べ、成立する監視条件に該当するエラー情報をすべて抽出する。その結果に基づき、擬似的に故障させた構成要素と抽出したすべてのエラー情報との対応情報を、監視シミュレーション結果記憶部22に格納する。



BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書

## 明細書

### 監視シミュレーション装置、方法およびそのプログラム

#### 技術分野

[0001] 本発明は、コンピュータシステムの構成情報を用いて故障箇所と監視のエラーメッセージの関係を得るシミュレーションを行い、網羅的な故障箇所とエラーメッセージとの一覧を作成する監視シミュレーション装置、方法およびそのプログラムに関する。

#### 背景技術

[0002] コンピュータシステムを運用する場合、故障が発生したときにはできるだけ早く故障箇所を発見して復旧させることが求められる。このために、ネットワークシステム中に監視装置を組み込んで、監視ツールを使いシステムの動作状況を監視することが行われている。

[0003] 監視の方法には、監視地点から対象機器への通信が可能かどうかをPINGコマンドやHTTPなどのプロトコルを使って確認し、故障を発見する方法や、監視装置が対象機器から一定周期で生存通知のメッセージを受信し、一定期間を超えて生存通知メッセージが到着しない場合に故障と判定する方法や、各機器が自己チェックを行い、異常があった場合に通信を使って監視装置に通知する方法など、さまざまな方法がある。これらのエラーメッセージの通知や監視は、ネットワークシステムでは一般にIP通信によって行われるために、故障箇所とエラーメッセージとが必ずしも1対1には対応しない。

[0004] すなわち、複数の機器から構成されるコンピュータシステムにおいては、いずれかの機器で障害が発生すると、その障害が発生した機器からばかりではなく、その機器と通信を行っている他の機器などからもエラーメッセージが連鎖的に出力されることがある。そのため、コンピュータシステムの運用管理者がエラーメッセージを見ただけで障害が発生した機器を特定することは、大変難しいものとなっている。

[0005] これに対して、発生する複数のエラーの組み合わせと障害が発生した可能性がある機器との対応テーブルを作成し、そのテーブルを用いて発生したエラーの組み合わせから障害が発生した可能性がある機器を推定して出力する技術がある。このよう

な技術としては、例えば、特許文献1に記載されている画像処理システムなどの例がある。

- [0006] 特許文献1に記載されている画像処理システムでは、関連する複数のエラーが発生したときに真のエラーの原因特定を迅速に行うことができるようにするため、あらかじめ複数のエラー状態の組み合わせを示すエラーパターンごとにそれぞれ真のエラーに基づくエラーメッセージが格納された情報テーブルを作成しておき、発生したエラーパターンに対して情報テーブルを検索することにより、該当するエラーメッセージを出力している。

特許文献1:特開2002-139807号公報

### 発明の開示

#### 発明が解決しようとする課題

- [0007] しかし、従来の技術では、関連する複数のエラーが発生したときに真のエラー原因を特定する情報を出力するためには、コンピュータシステムの設計者が、特許文献1に示されるような情報テーブルをあらかじめ作成して用意する必要がある。
- [0008] 故障する機器の数やエラーメッセージの種類が比較的少ないシステムでは、人間が上記の情報テーブルをあらかじめ作成することはそれほど困難な作業ではない。しかし、特に、ネットワーク化されたコンピュータシステムでは、システムの監視装置が監視する機器の数が非常に多いのが普通であり、エラーメッセージの数も多く、どの機器が故障するとどのようなエラーメッセージの組み合わせが出力されるかを、設計者がネットワーク図を見て対応づけるのは大変な煩雑さを伴う作業であった。また、人手で作成することにより、エラーメッセージの組み合わせに漏れが生じたり、故障箇所の特定情報の設定誤りが生じる可能性が高くなるという問題があった。
- [0009] また、上記特許文献1の技術では、新たなエラーパターンに対しては、オペレータが、適切なエラーメッセージを情報テーブルにその都度登録する必要がある。したがって、従来の技術は、既知のエラーパターンに対しては真のエラーの原因を迅速に特定することができるが、情報テーブルに登録されていないエラーパターンに対しては真のエラー原因の特定は困難であった。
- [0010] 本発明は、従来上記の情報テーブルの作成を、コンピュータシステムの設計者がコ

コンピュータシステムのネットワーク図を見ながら人手で行っており、情報テーブルの作成作業が大変煩雑であるという問題、人為的なエラーメッセージの設定誤りが生じることがあるという問題を解決し、設計されたコンピュータシステムの構成情報から、網羅的な故障箇所とエラーメッセージとの一覧を自動的に作成する技術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

- [0011] 本発明の監視シミュレーション装置は、上記の課題を解決するため、監視対象を含む複数の構成要素から構成されるコンピュータシステムの監視をシミュレーションするにあたって、コンピュータシステムを構成する各構成要素の接続関係情報を含む設計データを記憶する設計データ記憶部と、監視対象に対する異常検出の監視条件と、監視対象が監視条件に該当するという異常が検出された場合に出力すべきエラー情報を記憶する監視条件記憶部とを用い、まず、設計データ記憶部に記憶されている各構成要素を、順に一つずつ擬似的に故障させる設定を行う。次に、コンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、前記監視条件記憶部に記憶された各監視条件が成立するか否かを、設計データに基づいて探査し、監視条件が成立する場合に、その成立する監視条件に該当するエラー情報をすべて抽出する。この結果から、監視シミュレーション結果記憶部に、擬似的に故障させた構成要素と抽出したすべてのエラー情報との対応情報を格納する。
- [0012] このようにして、監視シミュレーション結果記憶部に、監視対象の網羅的な故障位置とエラー情報との一覧が作成されるので、監視装置は監視時にこれを参照することにより、複数のエラー情報をもとに障害原因の候補を特定することができる。また、故障位置とエラー情報との関係により、監視系を改善することができる。
- [0013] さらに、上記発明において、設計データ記憶部に記憶された構成要素とコンピュータシステムが行う業務との関係情報と、業務の重要度情報を用い、コンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、当該コンピュータシステムが業務を遂行できるか否かを、設計データに基づいて探査し、業務が遂行できないことを検出した場合に、その業務に該当する重要度の情報を抽出する。この重要度の情報を、擬似的に故障させた構成要素と抽出したすべてのエラー情報との対

応情報に加えて、監視シミュレーション結果記憶部に格納する。

- [0014] これにより、監視装置は、監視時にエラーが検出された場合に、その障害の重要度から緊急性を判断し、適切な対応をとるよう運用管理者に通知することが可能になる。また、システム設計者は、重要度の情報からコンピュータシステムの信頼性を高めるための設計改善情報を得ることができる。

## 発明の効果

- [0015] 本発明は、ネットワークシステムの構成情報とシステム監視ツールの監視条件の一覧を組み合わせて、監視シミュレーションを行い、故障位置と監視のエラーメッセージの関係の情報を収集し、網羅的な故障箇所とエラーメッセージとの一覧の作成を自動的に行うので、設計者の作業負担が軽減されるだけでなく、人為的なエラーメッセージの設定誤りや設定漏れをなくし、エラーメッセージから故障箇所を精度よく特定することができる。また、シミュレーションの結果得られた一覧表を逆引きして、監視不能箇所を発見したり、故障箇所の特定ができないエラーメッセージなどの監視の問題点を発見したりすることができるようになる。

## 図面の簡単な説明

- [0016] [図1]本発明の実施の形態による監視シミュレーション装置の構成例を示す図である。

◦

[図2]設計されたネットワーク図の例を示す図である。

[図3]各部品に付与された管理対象IDの例を示す図である。

[図4]機器テーブルの例を示す図である。

[図5]関係一覧テーブルの例を示す図である。

[図6]業務サーバマトリクスの例を示す図である。

[図7]通信マトリクスの例を示す図である。

[図8]業務ソフトウェアマトリクスの例を示す図である。

[図9]監視条件テーブルの例を示す図である。

[図10]設計データから作成されるトポロジデータの例を示す図である。

[図11]本実施の形態による監視シミュレーション処理フローチャートである。

[図12]監視シミュレーション結果テーブルの例を示す図である。

## 符号の説明

- [0017] 1 監視シミュレーション装置
- 2 ネットワーク管理DB
- 3 ネットワーク設計処理装置
- 4 監視装置
- 5 出力装置
- 10 設計データ入力部
- 11 構成部品擬似障害設定部
- 12 監視条件チェック部
- 13 重要度チェック部
- 14 ネットワーク探査部
- 20 設計データ記憶部
- 21 監視条件記憶部
- 22 監視シミュレーション結果記憶部
- 40 エラー発生検出部
- 41 エラー情報記憶部
- 42 障害原因特定部

## 発明を実施するための最良の形態

- [0018] 以下、本発明の実施の形態について、図を用いて説明する。
- [0019] 図1は、本発明の実施の形態による監視シミュレーション装置の構成例を示す図である。監視シミュレーション装置1は、設計データ入力部10、構成部品擬似障害設定部11、監視条件チェック部12、重要度チェック部13、ネットワーク探査部14を備える。これらは、CPUおよびメモリ等からなるハードウェアと、ソフトウェアプログラムとからなるコンピュータによって実現される。監視シミュレーション装置1には、ネットワーク管理DB(データベース)2が接続されている。
- [0020] ネットワーク管理DB2は、設計データ記憶部20、監視条件記憶部21、監視シミュレーション結果記憶部22を備える。
- [0021] ネットワーク設計処理装置3は、CADによりネットワークシステムを設計し、その設計

データを設計データ記憶部20に格納するコンピュータである。

- [0022] 設計データ入力部10は、ネットワーク管理DB2の設計データ記憶部20から設計データを入力し、入力された設計データからそのネットワークシステムを構成する各機器とそれらの接続および内蔵関係を示すトポロジデータを作成する。
- [0023] 構成部品擬似障害設定部11は、設計データ入力部10で作成されたトポロジデータにおいて、設計されたネットワークシステムを構成する各機器を、1つずつ順に擬似的に故障状態に設定する。実際に運用中の機器を故障状態にすることは容易ではないが、設計されたデータ上の機器のステータスを故障状態に設定することは容易である。
- [0024] 監視条件チェック部12は、ネットワーク管理DB2の監視条件記憶部21から監視条件を入力し、構成部品擬似障害設定部11によってある機器が擬似的に故障状態とされたトポロジデータの探査をネットワーク探査部14に依頼し、入力された監視条件の成立をチェックする。チェック結果は、ネットワーク管理DB2の監視シミュレーション結果記憶部22に記憶される。
- [0025] 重要度チェック部13は、構成部品擬似障害設定部11によってある機器が擬似的に故障状態とされたトポロジデータの探査をネットワーク探査部14に依頼し、設計されたネットワークシステムで行われる業務への影響をチェックする。チェック結果は、ネットワーク管理DB2の監視シミュレーション結果記憶部22に記憶される。
- [0026] ネットワーク探査部14は、監視条件チェック部12、重要度チェック部13からの依頼を受けてネットワークシステムの監視条件に基づく経路探査を行い、発生するエラー事象を検出してその結果を返す。
- [0027] 監視シミュレーション装置1によって得られる監視シミュレーション結果は、ネットワークシステムで発生し得るエラーの識別情報とそのエラーの原因となる機器との対応情報である。エラーの識別情報とは、エラーごとに一意に付与されたエラーコードまたはエラーメッセージである。その監視シミュレーション結果は、ネットワーク管理DB2で管理され、実際に運用されるネットワークシステムの監視に用いられる。
- [0028] 監視装置4は、実際に運用されるネットワークシステムの監視を行う。監視装置4は、エラー発生検出部40、エラー情報記憶部41、障害原因特定部42を備える。これら

は、CPUおよびメモリ等からなるハードウェアと、ソフトウェアプログラムとからなるコンピュータ・システムによって実現される。監視装置4には、出力装置5が接続されている。

- [0029] エラー発生検出部40は、運用中のネットワークシステムで発生する障害を検出し、そのエラー情報をエラー情報記憶部41に記憶する。
- [0030] 障害原因特定部42は、エラー情報記憶部41のエラー情報とネットワーク管理DB2の監視シミュレーション結果記憶部22の監視シミュレーション結果とから、障害の原因となっている機器を特定し、その特定された機器を出力装置5に出力する。
- [0031] 以下、図2～図12を用いて、本実施の形態をより具体的に説明する。
- [0032] 図2は、設計されたネットワーク図の例を示す図である。ここでは、ネットワーク設計処理装置3によって、図2のネットワーク図のウインドウ61内に表示されているようなネットワーク図が作成されたものとする。図2に示すネットワーク図において、設計されたネットワークシステムは、FireWall102から外部の端末であるterm128に接続されている。
- [0033] WWWサーバ111、DBサーバ120は、外部の顧客に対してサービスを行うためのサービス系サーバである。term128は、WWWサーバ111にアクセスすることにより、設計されたネットワークシステムが提供するサービスを受けることができる。
- [0034] ADMINサーバ123は、ネットワークシステムを構成する各機器の状態のチェックなどの保守管理を行うためのメンテナンス系サーバである。このADMINサーバ123は、例えば図1に示す監視装置4に相当する機能を持つ。
- [0035] FireWall102、WWWサーバ111、DBサーバ120、ADMINサーバ123には、ネットワークインターフェースカード(101, 103, 110, 112, 119, 122, 124)が装着されている。なお、以下、ネットワークインターフェースカードをNICと記す。
- [0036] NIC103、NIC110、NIC122は、それぞれLANケーブル104、LANケーブル109、LANケーブル121で、HUB(1)106のポート105、ポート108、ポート107に接続されている。また、NIC112、NIC119、NIC124は、それぞれLANケーブル113、LANケーブル118、LANケーブル125で、HUB(2)115のポート114、ポート117、ポート116に接続されている。

- [0037] また, WWWサーバ111にはアプリケーションプログラム(以下, 単にアプリケーションという)のapl126が, DBサーバ120にはdb-soft127がインストールされている。
- [0038] さらに, 図2のネットワーク図には, サービス用とメンテナンス用の2種類の通信設定が記述されている。図中, 破線の矢印はサービス用の通信設定を表しており, 2点鎖線の矢印はメンテナンス用の通信設定を表している。
- [0039] 図2のネットワーク図には, サービス用の通信設定として, term128からWWWサーバ111のNIC110への通信設定129, WWWサーバ111のNIC112からDBサーバ120のNIC119への通信設定130が記述されている。
- [0040] また, 図2のネットワーク図には, メンテナンス用の通信設定として, ADMINサーバ123のNIC122から, FireWall102のNIC103, HUB106, WWWサーバ111のNIC110に, それぞれ通信設定131, 通信設定132, 通信設定133が, ADMINサーバ123のNIC124から, WWWサーバ111のNIC112, HUB115, DBサーバ120のNIC119に, それぞれ通信設定134, 通信設定135, 通信設定136が, apl126からWWWサーバ111のNIC112を経由してADMINサーバ123のNIC124に通信設定137が記述されている。
- [0041] ネットワークシステムの設計者は, プロパティ設定を行いたいネットワーク図上の機器または通信の矢印をマウスの右ボタンでクリックし(これを右クリックとい), プロパティ設定のウインドウ62を開く。設計者は, プロパティ設定のウインドウ62上で, その機器の各属性を設定することができる。属性とは, 例えば機器の名称, 型格, IPアドレス, バージョン番号, また他の機器との接続関係や内蔵関係を示す情報などである。通信の属性情報の場合には, 通信の種類, 通信の始点, 終点のIPアドレスやプロトコル情報を含む。
- [0042] 各機器および通信の属性情報は, あらかじめネットワーク図に使用する機器および通信の部品ごとに定義しておくことができ, これを部品属性情報として, ネットワーク設計処理装置3が管理する属性ファイル(図示省略)に保持しておくことができる。プロパティ設定のウインドウ62では, その属性ファイルに事前に定義されていた属性の項目については, 属性ファイルから読み出した属性情報がデフォルト値として埋め込まれる。したがって, 設計者は, プロパティ設定のウインドウ62から個々の機器または

通信に特有の属性情報だけを入力すればよく、例えばサーバのホスト名やアドレス情報など、必要最小限の属性情報を入力するだけでよい。

- [0043] 図3は、各部品に付与された管理対象IDの例を示す図である。ネットワーク図を構成する各部品には、それぞれを一意に認識することが可能な管理対象IDが付与されている。図3において、楕円の中の数字がその部品に付与された管理対象IDである。これらの管理対象IDは、ネットワーク図に図形要素の部品(オブジェクトという)が張り付けられるときに、ネットワーク設計処理装置3によって自動的に付与される識別子である。
- [0044] 図4は、機器テーブルの例を示す図である。図4の例に示す機器テーブル23は、ネットワーク設計処理装置3によって図2に示すネットワーク図をもとに作成されたネットワークの構成情報を持つテーブルであり、ネットワーク管理DB2中の設計データ記憶部20に格納される。機器テーブル23のレコードは、その機器を一意に識別する「管理対象ID」、その機器の「名称」、「型格」、その機器に割り当てられた「IPアドレス」の項目などからなる。
- [0045] 図5は、関係一覧テーブルの例を示す図である。図5の例に示す関係一覧テーブル24は、図2に示すネットワーク図をもとに作成された機器同士の関係を示す情報のテーブルであり、ネットワーク管理DB2中の設計データ記憶部20に格納される。関係一覧テーブル24は、親となる機器の管理対象IDを示す親ID、子となる機器の管理対象IDを示す子ID、親IDで示された機器と子IDで示された機器との関係の情報などからなる。関係としては、親IDと子IDの機器が接続されていることを示す「接続」、親IDの機器に子IDの機器が内蔵されていることを示す「内蔵」、親IDの機器に子IDのソフトウェアがインストールされていることを示す「インストール」などがあるが、これらをまとめて接続または内蔵関係という。
- [0046] 図6は、業務サーバマトリクスの例を示す図である。図6の例に示す業務サーバマトリクス25は、各業務処理と各サーバとの関連を示す情報であり、ネットワーク管理DB2中の設計データ記憶部20に格納される。図6の業務サーバマトリクス25において、監視業務はメンテナンス系の業務処理であり、業務Aはサービス系の業務処理である。この業務サーバマトリクス25は、ネットワーク図の作成時に入力されたサーバの属

性情報をもとに作成される。

- [0047] 各業務処理には、重要度が設定されている。重要度が高い業務処理は、障害発生時などに早急な復旧を必要とする業務処理である。これに対して重要度が低い業務処理は、障害発生時などに緊急の対処を要しない業務処理である。図6の業務サーバマトリクス25の例では、業務Aは重要度が高く設定されており、監視業務は重要度が低く設定されている。
- [0048] 図6の業務サーバマトリクス25から、監視業務に関連するのは、ADMINサーバ123であり、業務Aに関連するのは、WWWサーバ111、DBサーバ120であることがわかる。それぞれ関連するサーバに問題が発生すると、その業務処理に影響を及ぼす。例えば、ADMINサーバ123に問題が発生すると、監視業務に影響を及ぼす。
- [0049] 図7は、通信マトリクスの例を示す図である。図7の例に示す通信マトリクス26は、ネットワーク図上で設定された通信の情報であり、ネットワーク管理DB2中の設計データ記憶部20に格納される。この通信マトリクス26は、ネットワーク図の作成時に入力された通信設定の属性情報をもとに作成される。
- [0050] 図7の例の通信マトリクス26は、特にサービス系のアプリケーションを中心とした通信マトリクス26である。term128とWWWサーバ111+apl126との間の通信は、プロトコルとしてhttpを使用し、図2に示すネットワーク図の通信設定129にあたる。WWWサーバ111+apl126とDBサーバ120+db-soft127との間の通信は、プロトコルとしてsqlを使用し、図2に示すネットワーク図の通信設定130にあたる。なお、ここで“sql”はデータベース検索用のコマンドの総称である。
- [0051] 図7にはサービス系の通信マトリクス26の例のみが記載されているが、ネットワークシステムの保守管理を行うためのメンテナンス系の通信マトリクス26も、別に存在する。ここでは、説明の簡潔化のため図示を省略する。
- [0052] 図8は、業務ソフトウェアマトリクスの例を示す図である。図8の例に示す業務ソフトウェアマトリクス27は、各業務処理と各ソフトウェアとの関連を示す情報であり、ネットワーク管理DB2中の設計データ記憶部20に格納される。この業務ソフトウェアマトリクス27は、ネットワーク図の作成時に入力されたソフトウェアの属性情報をもとに作成される。

- [0053] 図8の業務ソフトウェアマトリクス27から、業務Aにはapl126とdb-soft127との使用が設定されていることがわかる。監視業務に関するソフトウェアについては、まだ設定されていない。
- [0054] 図9は、監視条件テーブルの例を示す図である。図9の例に示す監視条件テーブル28は、あらかじめ作成された図2のネットワーク図に示すネットワークシステムの監視条件のテーブルであり、ネットワーク管理DB2中の監視条件記憶部21に格納される。監視条件テーブル28のレコードは、監視の対象となる機器の「管理対象ID」、監視を行う「監視サーバ」、監視の対象となる機器の名称である「監視対象」、エラーが発生する「条件」、エラーが発生したときの「エラーコード」、「エラーメッセージ」の項目などからなる。なお、図9の監視条件テーブル28の1番下のレコードの条件にある“AP”は、アプリケーションを示す。
- [0055] 例えば、図9の監視条件テーブル28の1番上のレコードは、ADMINサーバ123から管理対象IDが“3”であるNIC103への通信ができない場合に、“E3”のエラーコード、“NIC103 PINGエラー”的エラーメッセージが出力されることを示している。
- [0056] 図9の監視条件テーブル28の各レコードは、上から順に、図2のネットワーク図における通信設定131、通信設定132、通信設定133、通信設定134、通信設定135、通信設定136、通信設定137に対応する。通信設定131、通信設定132、通信設定133、通信設定134、通信設定135、通信設定136については、ADMINサーバ123から各機器へのPINGによる監視を示す。通信設定137は、apl126がDBサーバ120との通信に異常を発見した場合に、apl126がDBサーバ120との間の通信異常をADMINサーバ123に通知することを示す。ADMINサーバ123は、この通信によってDB通信モジュールの異常を知ることができる。
- [0057] ここで、ネットワーク図の作成時に入力されたメンテナンス通信設定の属性情報から、監視条件テーブル28を作成することも可能である。例えば、図2のネットワーク図において、記述されたメンテナンス通信設定に属性情報として「条件」、「エラーコード」、「エラーメッセージ」などをプロパティで設定しておけば、それらの属性情報から自動的に監視条件テーブル28を作成することが可能である。
- [0058] 監視シミュレーション装置1は、設計データ記憶部20から入力した設計データから

作成されたトポジデータにおいて、ある機器を故障状態に設定してネットワーク探査を行う。このとき、監視条件テーブル28の条件が成立して発行される1または複数のエラーコードを抽出する。抽出された1または複数のエラーコードが、実際に運用されるネットワークシステム上でその機器が故障した場合に発生するエラーコードである。

- [0059] 図10は、設計データから作成されるトポジデータの例を示す図である。図10のトポジデータは、図4の機器テーブル23、図5の関係一覧テーブル24などから作成されるものである。図10のトポジデータにおいて、各機器を示す四角、三角、丸の中の数字は、図4の機器テーブル23の管理対象IDに対応する。なお、図10では、このトポジデータをわかりやすくするためにグラフ化して表示しているが、監視シミュレーション装置1のメモリ内では、各機器のノードとそれらをリンクするポインタの情報からなるデータとしてトポジデータが保持されることになる。
- [0060] 図10に示すようなトポジデータにおいて、構成部品擬似障害設定部11が各機器を順に故障状態に設定し、ネットワーク探査部14がネットワークシステムの探査を行い、監視条件チェック部12が監視条件テーブル28の条件成立のチェックを行う。ネットワークシステムの探査を行うとは、例えば監視条件として与えられた監視のための通信が正常に行われるかどうかをトポジデータをトレースして調べることであり、監視条件が成立するとは、ネットワークの探査により異常が検出されてエラーコードが確定することをいう。
- [0061] 例えば、図10に示すトポジデータにおいて、管理対象IDが“6”的HUB(1)106を故障状態に設定してネットワークシステムの探査を行うと、監視を行っている装置すなわち管理対象IDが“23”であるADMINサーバ123から、管理対象IDが“6”的HUB(1)106を経由した通信が行えないため、図9の監視条件テーブル28から、“E3”, “E6”, “E10”的エラーコードが抽出される。
- [0062] また、図10に示すようなトポジデータにおいて、構成部品擬似障害設定部11が各機器を順に故障状態に設定し、ネットワーク探査部14がネットワークシステムの探査を行い、重要度チェック部13が業務処理への影響のチェックを行う。
- [0063] 例えば、図10に示すトポジデータにおいて、管理対象IDが“6”的HUB(1)106

を故障状態に設定してネットワークシステムの探査を行うと、通信マトリクス26により、term128(管理対象ID=28)とWWWサーバ111のアプリケーションapl126との通信すなわちサービス用の通信設定129が通信不可となることが分かり、業務サーバマトリクス25により、WWWサーバ111は業務Aに関係することが分かるので、業務Aへの影響が検出される。また、図6の業務サーバマトリクス25から、重要度“高い”が抽出される。

- [0064] 図11は、本実施の形態による監視シミュレーション処理フローチャートである。監視シミュレーション装置1において、設計データ入力部10は、設計データ記憶部20から入力された設計データから、ネットワーク構成のトポロジデータを作成する(ステップS10)。
- [0065] 構成部品擬似障害設定部11は、トポロジデータの構成部品を1つ選択し(ステップS11)，その選択された構成部品を“故障中”に設定する(ステップS12)。
- [0066] ネットワーク探査部14は、選択された構成部品が“故障中”に設定されたネットワークを探査し、監視条件チェック部12は、監視条件記憶部21から入力された各監視条件の成立をチェックする(ステップS13)。成立する監視条件があれば(ステップS14)，選択された構成部品の監視シミュレーション結果に、監視条件成立によって発生するエラーコードを記録する(ステップS15)。
- [0067] また、重要度チェック部13は、ネットワーク探査部14による探査結果から、業務処理への影響を検査する(ステップS16)。業務サーバマトリクス25を参照し、業務処理への影響があれば(ステップS17)，選択された構成部品の監視シミュレーション結果に、重要度を設定する(ステップS18)。
- [0068] 次に、選択された部品の“故障中”的設定を解除する(ステップS19)。すべての構成部品についてシミュレーションが終了したかを判定し(ステップS20)，まだ終了していないなければ、すべての構成部品についてシミュレーションが終了するまで、ステップS11～S20の処理を繰り返す。
- [0069] 図12は、監視シミュレーション結果テーブルの例を示す図である。図12の例の監視シミュレーション結果テーブル29は、図2のネットワーク図に示すネットワークシステムにおいて、監視シミュレーション装置1による監視シミュレーション処理により得られ

る情報である。監視シミュレーション装置1は、図12に示すような監視シミュレーション結果テーブル29を、ネットワーク管理DB2の監視シミュレーション結果記憶部22に格納する。

- [0070] 図12の例の監視シミュレーション結果テーブル29のレコードは、故障状態が仮定された機器の「管理対象ID」、故障状態が仮定された機器の名称である「異常対象」、その機器の故障状態が仮定されたときに監視シミュレーション処理によって抽出される「エラーコード」、その機器の故障状態が仮定されたときに監視シミュレーション処理によって設定される「重要度」の項目などからなる。
- [0071] 重要度は、異常対象となる機器が業務処理に与える影響の程度が示されている。そのため、異常対象となる機器が業務処理に与える影響がない場合には、重要度は設定されなくてもよい。図12の監視シミュレーション結果テーブル29の例では、すべての機器について重要度が設定されているが、監視シミュレーションの対象となるネットワークシステムに冗長構成があれば、故障しても業務処理に影響を与えない機器が存在することとなる。
- [0072] 以上の監視シミュレーション処理の動作の例を説明する。例えば図11のステップS11において、管理対象ID=7のポート107を選択したとする。構成部品擬似障害設定部11は、図10のトポロジデータ上でポート107を故障中の状態に設定する(ステップS12)。監視条件チェック部12は、監視条件テーブル28中に設定されている各監視条件の通信が可能かどうかの経路の探査をネットワーク探査部14に依頼し、各監視条件の成立をチェックする(ステップS13)。
- [0073] 監視条件テーブル28における管理対象ID=3の監視対象(NIC103-FW)は、ポート107が故障中であるためADMINサーバ123からの通信経路がなく、通信できないという監視条件が成立することになる。したがって、監視条件チェック部12は、監視シミュレーション結果テーブル29におけるポート107(管理対象ID=7)のエラーコードの欄にエラーコードE3を記録する(ステップS15)。ここで、通信経路があるかどうかは、図10に示すトポロジデータにおいて、通信の始点と終点のノードを結ぶ線があるかどうかによって判断される。なお、途中に故障中の機器があると断線として扱われる。また、ADMINサーバ123とWWWサーバ111とDBサーバ120は、IPパケットを

中継する機能を持たないので、これらは通信の始点と終点にはなり得るが、通信がこれらを通過して行われることはない。

- [0074] 同様に、監視条件テーブル28における管理対象ID=6の監視対象(HUB(1))は、これもポート107が故障中であるためADMINサーバ123からの通信経路がなく、通信できないという監視条件が成立する。したがって、監視条件チェック部12は、監視シミュレーション結果テーブル29におけるポート107(管理対象ID=7)のエラーコードの欄にエラーコードE6を追記する。管理対象ID=10の監視対象(NIC110-WWW)に対しても通信経路がないため、エラーコードE10のエラーが生じることがわかり、監視シミュレーション結果テーブル29にこのエラーコードE10を追記する。
- [0075] この結果、監視シミュレーション結果テーブル29におけるポート107(管理対象ID=7)のエラーコードの欄には、E3, E6, E10のエラーコードが格納され、もし、運用中に、実際にポート107が故障すると、エラーコードE3, E6, E10のメッセージが出力されることがわかる。
- [0076] また、重要度チェック部13は、ポート107(管理対象ID=7)を擬似的に故障中に設定した状態で、業務処理への影響を検査する(ステップS16)。この業務処理への影響の検査は、図7に示す通信マトリクス(アプリケーション)26の通信が可能かどうかをネットワーク探査部14によって探査することによって行う。図10に示すトポロジデータから明らかなように、ポート107が故障してもterm(管理対象ID=28)とWWWサーバのアプリケーションaplとの通信が可能である。また、WWWサーバのアプリケーションaplとDBサーバのソフトウェアdb-softとの通信も支障がない。したがって、業務Aには影響がないことがわかる。一方、ADMINサーバの監視業務は、ポート107の故障によって影響を受けるので、図6に示す業務サーバマトリクス25から、ポート107の故障の重要度は「低い」ということがわかる。この結果から、重要度チェック部13は、監視シミュレーション結果テーブル29におけるポート107(管理対象ID=7)の重要度の欄に「低い」を記録する。
- [0077] 監視シミュレーション装置1は、以上のような故障状態の設定と、ネットワーク探査による監視条件のチェックおよび重要度のチェックを、トポロジデータの各ノード、すなわち図4に示す機器テーブル23の各機器に対して順次行うことにより、図12に示す

ような監視シミュレーション結果テーブル29の情報を得ることができる。

- [0078] 監視装置4は、監視シミュレーション結果記憶部22に格納された監視シミュレーション結果テーブル29を参照し、実際に運用されているネットワークシステムから発生したエラーコードの組み合わせから障害の原因となっている機器を特定する。図12に示すような監視シミュレーション結果テーブル29があれば、エラーコードの組み合わせから障害の原因となっている機器を絞り込むことができる。また、障害が業務処理に与える影響の程度を知ることができる。エラー情報記憶部41に記憶されたエラー情報は、障害の原因を特定した後に削除される。または、一定期間ごとにロギングデータとして出力された後、削除される。
- [0079] すなわち、実際の運用システムにおいて、図2に示すADMINサーバ123が、図9に示す監視条件テーブル28に従って、管理対象ID=3, 6, 10, 12, 15, 19に対してそれぞれPINGコマンドを発行し、その応答を監視したとする。このとき、例えば管理対象IDが12, 15, 19の機器からの応答がなく、これらがPINGエラーになったとすると、エラーコードE12, E15, E19がエラー情報として上がる。したがって、監視シミュレーション結果テーブル29のエラーコードの欄から、故障の可能性のある機器が、HUB(2)(管理対象ID=15), ポート116(管理対象ID=16), NIC124-ADMIN(管理対象ID=24)、またはLANケーブル(管理対象ID=25)のいずれかである可能性が大きいことが分かる。
- [0080] これにより、実際に運用されているネットワークシステムに障害が発生しても、その原因となっている機器の特定が容易となるため、ネットワークシステムの早期の復旧が期待できるようになる。また、故障箇所の業務処理に与える影響の程度が分かるため、早急な対応が必要か否かの判断が容易となる。
- [0081] また、実際にネットワークシステムの構築に入る前に監視シミュレーション結果テーブル29の内容を確認することにより、ネットワークシステム監視の盲点となる部分を洗い出し、ネットワークシステムの変更、メンテナンス通信設定の変更、追加などの対策を検討することも可能である。
- [0082] 例えば、図12の監視シミュレーション結果テーブル29を見ると、term128のエラーが検出できないことが分かる。したがって、ネットワークシステムの運用管理者は、AD

MINサーバ123からterm128に定期的にPINGコマンドを発行するなどの対策を検討する必要がある。

- [0083] また、例えば、NIC112に故障が発生するとapl126がDBサーバ120と通信することができなくなるため、E26が発生するはずである。ところが、図2のネットワーク図において、通信設定137はNIC112経由で設定されているため、NIC112の故障によりADMINサーバ123はE26を検出することができない。したがって、ネットワークシステムの運用管理者は、apl126からNIC110経由でADMINサーバ123に向かう通信設定を検討する必要があることが分かる。
- [0084] 以上の監視シミュレーション装置1が行う処理および監視装置4が行う処理は、コンピュータとソフトウェアプログラムとによって実現することができ、そのプログラムをコンピュータ読み取り可能な記録媒体に記録することも、ネットワークを通して提供することも可能である。

### 産業上の利用可能性

- [0085] 本発明は、ネットワークシステムの構成情報とシステム監視ツールの監視条件の一覧を組み合わせて、故障位置と監視のエラーメッセージの関係を得るシミュレーションを行い、網羅的な故障箇所とエラーメッセージとの一覧の作成を自動的に行い、監視系の改善やエラーメッセージから故障箇所を特定することを可能にする技術である。

## 請求の範囲

- [1] 監視対象を含む複数の構成要素から構成されるコンピュータシステムの監視をシミュレーションする監視シミュレーション装置であつて、  
前記コンピュータシステムを構成する各構成要素の接続関係情報を含む設計データを記憶する設計データ記憶部と、  
前記監視対象に対する異常検出の監視条件と、前記監視対象が監視条件に該当するという異常が検出された場合に出力すべきエラー情報を記憶する監視条件記憶部と、  
前記設計データ記憶部に記憶されている各構成要素を、順に一つずつ擬似的に故障させる設定を行う擬似障害設定部と、  
前記擬似障害設定部によりコンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、前記監視条件記憶部に記憶された各監視条件が成立するか否かを、前記設計データに基づいて探査し、監視条件が成立する場合に、その成立する監視条件に該当するエラー情報をすべて抽出する監視条件チェック部と、  
前記擬似的に故障させた構成要素と前記抽出したすべてのエラー情報との対応情報を記憶する監視シミュレーション結果記憶部とを備える  
ことを特徴とする監視シミュレーション装置。
- [2] 請求項1記載の監視シミュレーション装置において、  
前記設計データ記憶部は、さらに前記構成要素とコンピュータシステムが行う業務との関係情報を記憶し、  
前記擬似障害設定部によりコンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、当該コンピュータシステムが業務を遂行できるか否かを、前記設計データに基づいて探査し、業務が遂行できないことを検出した場合に、その業務に該当する重要度の情報を抽出する重要度チェック部を備え、  
前記監視シミュレーション結果記憶部は、前記擬似的に故障させた構成要素と前記抽出したすべてのエラー情報との対応情報を加えて、前記重要度チェック部が抽出した重要度の情報を記憶する  
ことを特徴とする監視シミュレーション装置。

- [3] 監視対象を含む複数の構成要素から構成されるコンピュータシステムの監視を、コンピュータがシミュレーションする監視シミュレーション方法であって、  
前記コンピュータが、  
前記コンピュータシステムを構成する各構成要素の接続関係情報を含む設計データを記憶する設計データ記憶部から設計データを入力する過程と、  
入力した設計データ中の各構成要素を、順に一つずつ擬似的に故障させる設定を行う過程と、  
前記監視対象に対する異常検出の監視条件と、前記監視対象が監視条件に該当するという異常が検出された場合に出力すべきエラー情報をあらかじめ記憶する監視条件記憶部から、監視条件を読み出す過程と、  
前記コンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、前記監視条件記憶部から読み出した監視条件が成立するか否かを、前記設計データに基づいて探査し、監視条件が成立する場合に、その成立する監視条件に該当するエラー情報をすべて抽出する過程と、  
前記擬似的に故障させた構成要素と前記抽出したすべてのエラー情報との対応情報を、監視シミュレーション結果記憶部に格納する過程とを有する  
ことを特徴とする監視シミュレーション方法。
- [4] 請求項3記載の監視シミュレーション方法において、  
前記設計データを入力する過程では、前記設計データ記憶部からさらに前記構成要素とコンピュータシステムが行う業務との関係情報を、業務の重要度情報を入力し、  
前記擬似的に故障させる設定を行う過程においてコンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、当該コンピュータシステムが業務を遂行できるか否かを、前記設計データに基づいて探査し、業務が遂行できないことを検出した場合に、その業務に該当する重要度の情報を抽出する過程と、  
前記監視シミュレーション結果記憶部に、前記擬似的に故障させた構成要素と前記抽出したすべてのエラー情報との対応情報を加えて、前記重要度チェック部が抽出した重要度の情報を格納する過程とを有する

ことを特徴とする監視シミュレーション方法。

[5] 監視対象を含む複数の構成要素から構成されるコンピュータシステムの監視をシミュレーションする監視シミュレーション方法をコンピュータに実行させるための監視シミュレーションプログラムであって、

前記コンピュータシステムを構成する各構成要素の接続関係情報を含む設計データを記憶する設計データ記憶部から設計データを入力する処理と、

入力した設計データ中の各構成要素を、順に一つずつ擬似的に故障させる設定を行う処理と、

前記監視対象に対する異常検出の監視条件と、前記監視対象が監視条件に該当するという異常が検出された場合に出力すべきエラー情報をあらかじめ記憶する監視条件記憶部から、監視条件を読み出す処理と、

前記コンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、前記監視条件記憶部から読み出した監視条件が成立するか否かを、前記設計データに基づいて探査し、監視条件が成立する場合に、その成立する監視条件に該当するエラー情報をすべて抽出する処理と、

前記擬似的に故障させた構成要素と前記抽出したすべてのエラー情報との対応情報を、監視シミュレーション結果記憶部に格納する処理とを、

コンピュータに実行させるための監視シミュレーションプログラム。

[6] 請求項5記載の監視シミュレーションプログラムにおいて、

前記設計データを入力する処理では、前記設計データ記憶部からさらに前記構成要素とコンピュータシステムが行う業務との関係情報を、業務の重要度情報を入力し、

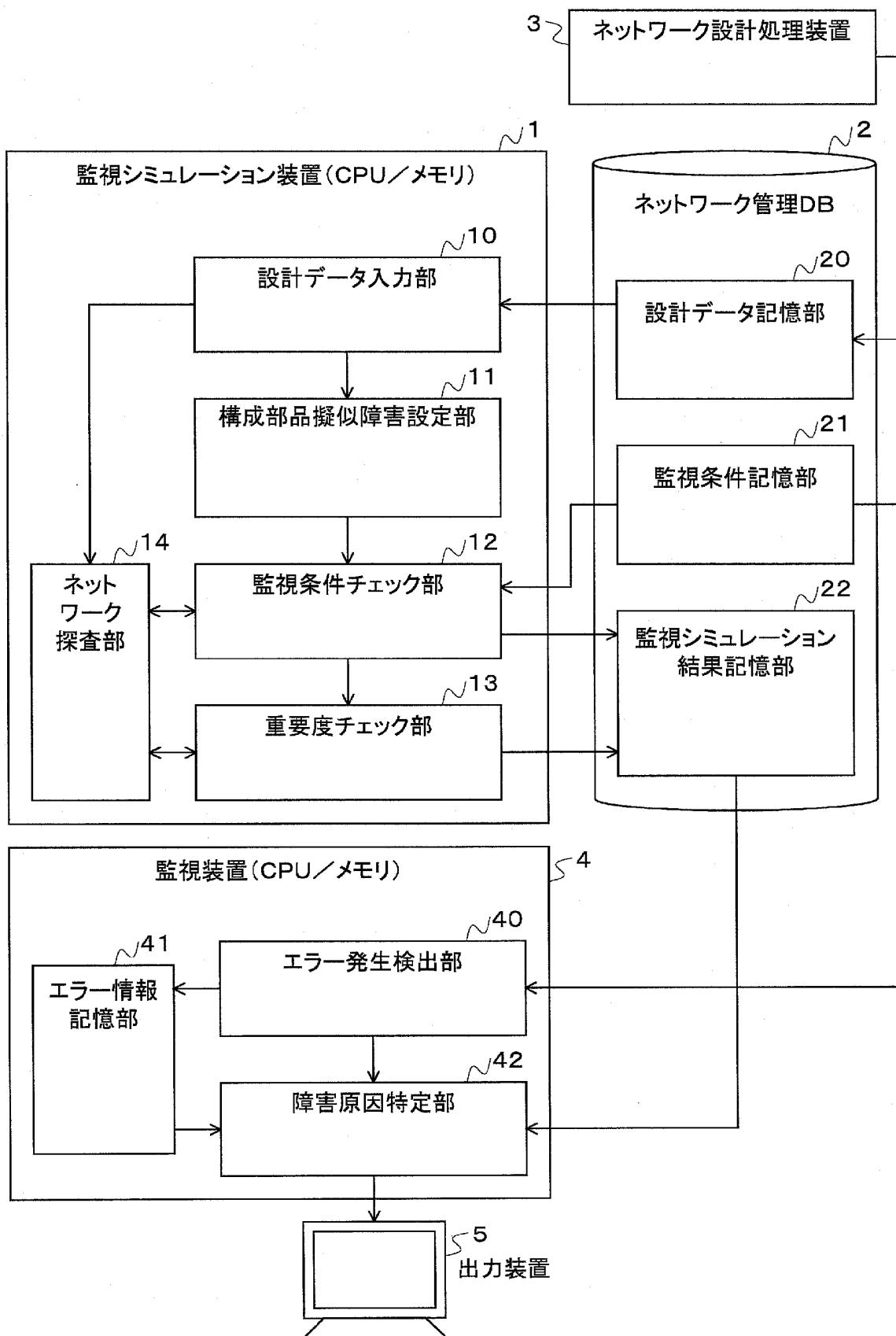
前記擬似的に故障させる設定を行う処理においてコンピュータシステムにおける一つの構成要素を擬似的に故障させた状態で、当該コンピュータシステムが業務を遂行できるか否かを、前記設計データに基づいて探査し、業務が遂行できないことを検出した場合に、その業務に該当する重要度の情報を抽出する処理と、

前記監視シミュレーション結果記憶部に、前記擬似的に故障させた構成要素と前記抽出したすべてのエラー情報との対応情報を加えて、前記重要度チェック部が抽

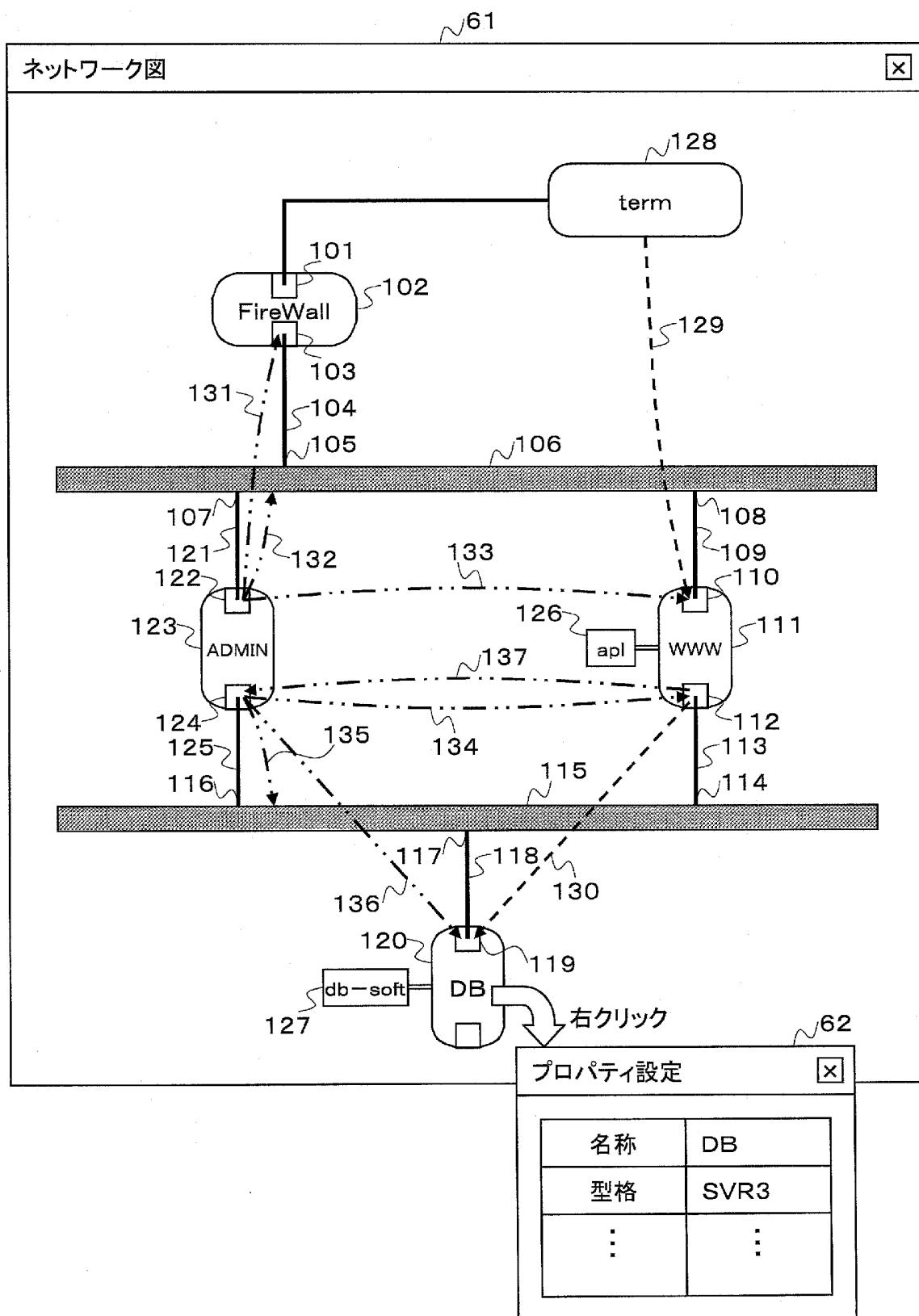
出した重要度の情報を格納する処理とを、

さらにコンピュータに実行させるための監視シミュレーションプログラム。

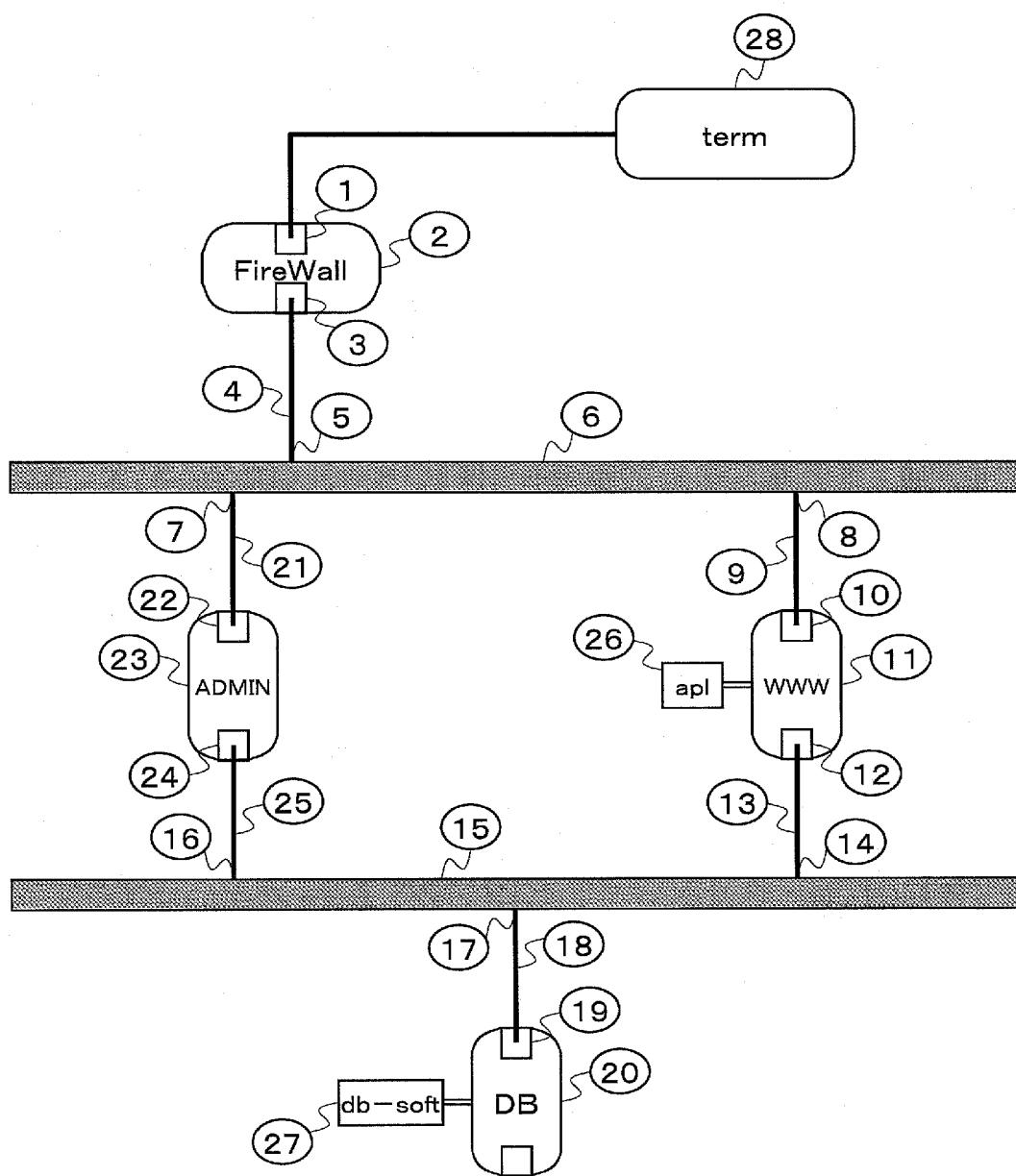
[図1]



[図2]



[図3]



[図4]

機器テーブル 23

管理対象ID	名称	型格	IPアドレス
1	NIC101-FW	NICFW	10.1.0.1/24
2	FireWall	FW1	
3	NIC103-FW	NICFW	192.168.2.1/24
4	LANケーブル	CBL1	
5	ポート105	PT1	
6	HUB(1)	HUB123	192.168.2.5/24
7	ポート107	PT1	
8	ポート108	PT1	
9	LANケーブル	CBL1	
10	NIC110-WWW	NICSV	192.168.2.2/24
11	WWWサーバ	SVR1	
12	NIC112-WWW	NICSV	192.168.1.2/24
13	LANケーブル	CBL1	
14	ポート114	PT1	
15	HUB(2)	HUB123	192.168.1.5/24
16	ポート116	PT1	
17	ポート117	PT1	
18	LANケーブル	CBL1	
19	NIC119-DB	NICSV	192.168.1.6/24
20	DBサーバ	SVR3	
21	LANケーブル	CBL1	
22	NIC122-ADMIN	NICSV	192.168.2.3/24
23	ADMINサーバ	SVR2	
24	NIC124-ADMIN	NICSV	192.168.1.3/24
25	LANケーブル	CBL1	
26	apl	apl1	
27	db-soft	db-soft	
28	term	term1	ANY

[図5]

関係一覧テーブル 24

No.	親ID	子ID	関係
1	28	1	接続
2	2	1	内蔵
3	2	3	内蔵
4	3	4	接続
5	5	4	接続
6	6	5	内蔵
7	6	7	内蔵
8	6	8	内蔵
9	8	9	接続
10	10	9	接続
11	11	10	内蔵
12	11	12	内蔵
13	11	26	インストール
14	20	27	インストール

[図6]

業務サーバマトリクス  $\sim^{25}$ 

	監視業務	業務A
重要度	低い	高い
ADMINサーバ	○	×
WWWサーバ	×	○
DBサーバ	×	○

○:関係あり

×:関係なし

[図7]

通信マトリクス(アプリケーション)  $\sim^{26}$ 

終点 始点 \	term	WWWサーバ + apl	DBサーバ + db-soft
term		http	
WWWサーバ + apl			sql
DBサーバ + db-soft			

[図8]

業務ソフトウェアマトリクス  $\sim^{27}$ 

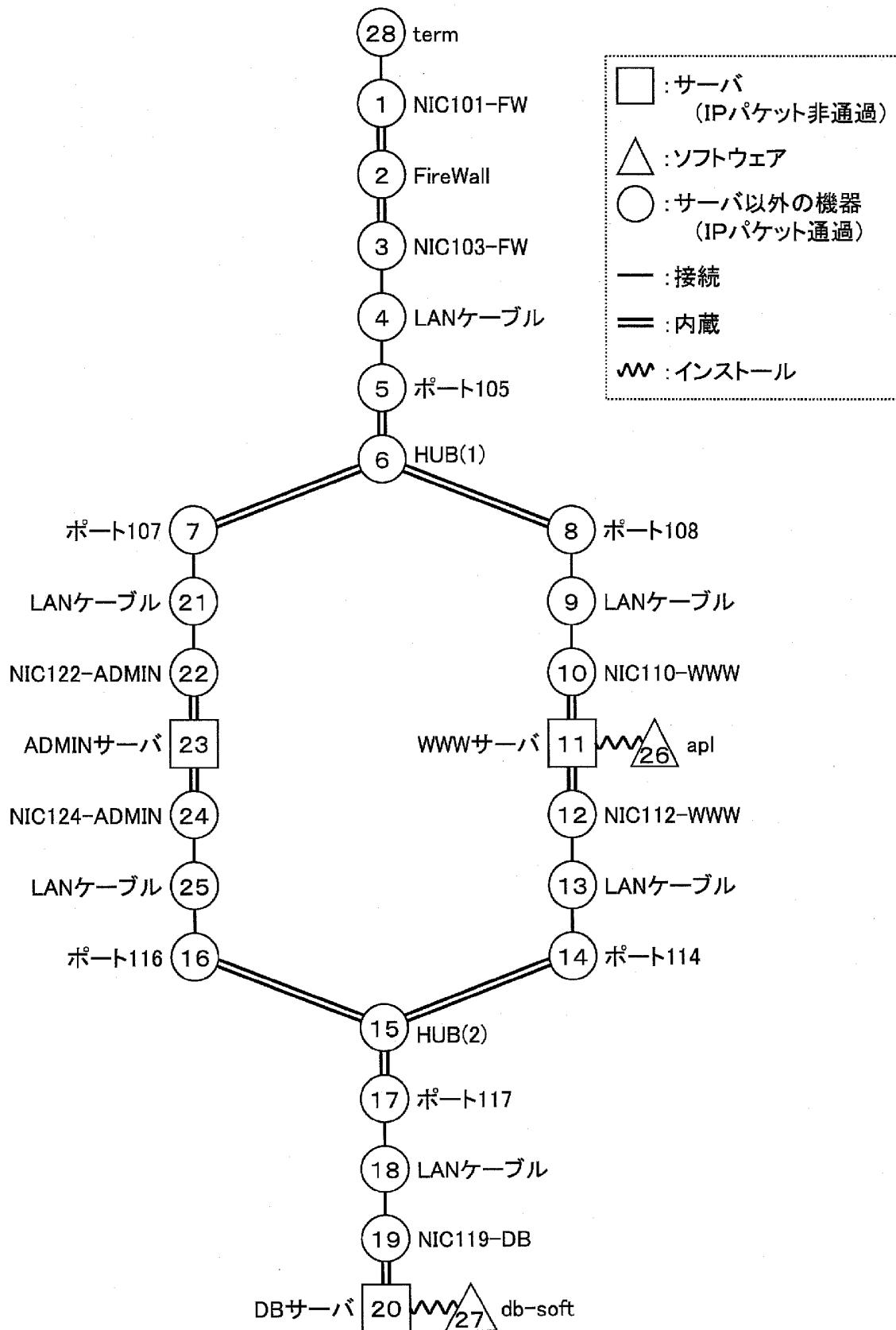
	監視業務	業務A
apl		○
db-soft		○

[図9]

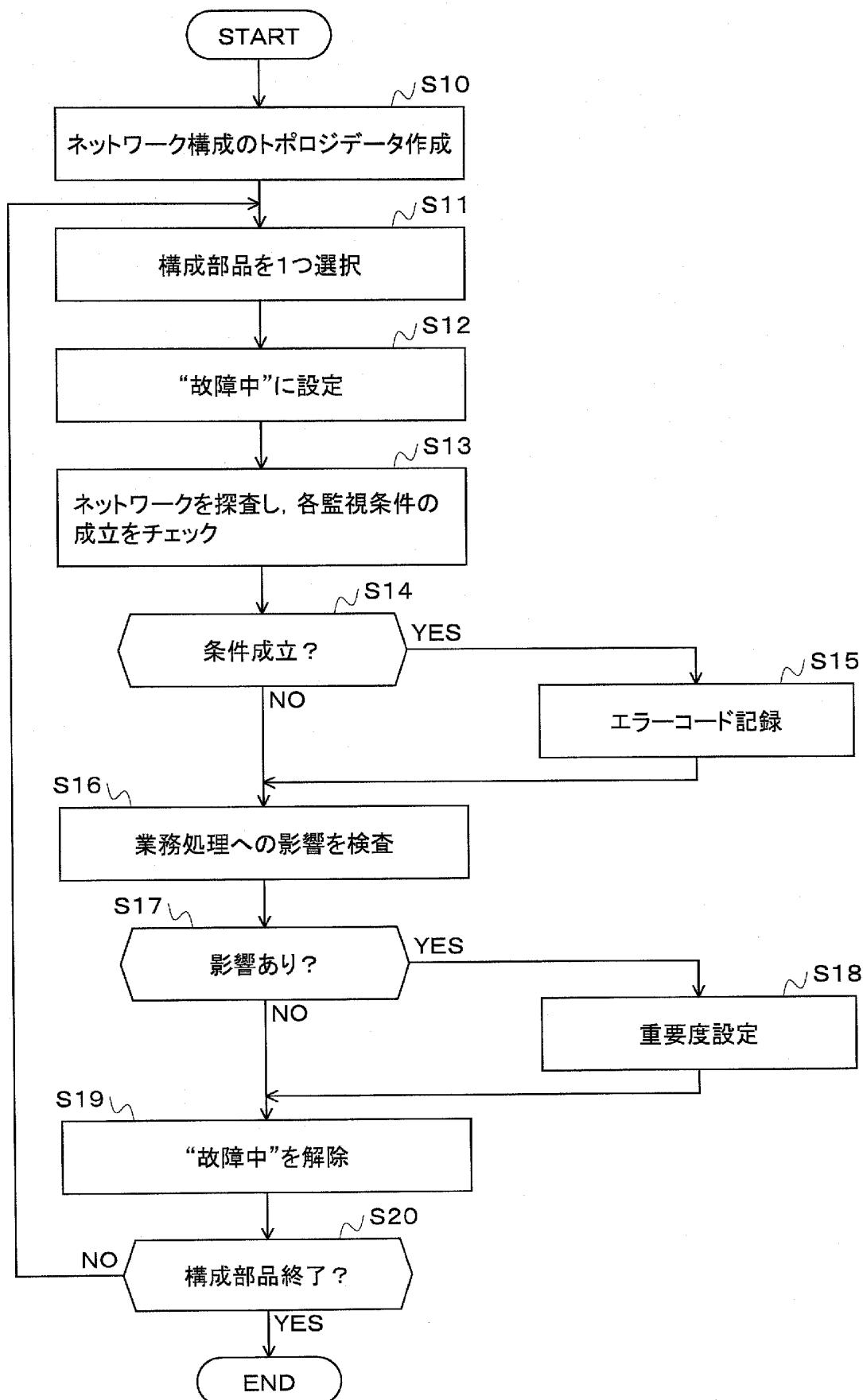
監視条件テーブル 28

管理対象ID	監視サーバ	監視対象	条件	エラーコード	エラーメッセージ
3	ADMINサーバ	NIC103-FW	通信できない	E3	NIC103 PINGエラー
6	ADMINサーバ	HUB(1)	通信できない	E6	HUB(1) PINGエラー
10	ADMINサーバ	NIC110-WWW	通信できない	E10	NIC110 PINGエラー
12	ADMINサーバ	NIC112-WWW	通信できない	E12	NIC112 PINGエラー
15	ADMINサーバ	HUB(2)	通信できない	E15	HUB(2) PINGエラー
19	ADMINサーバ	NIC119-DB	通信できない	E19	NIC119 PINGエラー
26	ADMINサーバ	apl	APがDBとの通信に異常発見	E26	DB通信モジュール異常

[図10]



[図11]



[図12]

監視シミュレーション結果テーブル ~29

管理対象ID	異常対象	エラーコード	重要度
1	NIC101-FW	なし	高い
2	FireWall	E3	高い
3	NIC103-FW	E3	高い
4	LANケーブル	E3	高い
5	ポート105	E3	高い
6	HUB(1)	E3,6,10	高い
7	ポート107	E3,6,10	低い
8	ポート108	E10	高い
9	LANケーブル	E10	高い
10	NIC110-WWW	E10	高い
11	WWWサーバ	E10,12	高い
12	NIC112-WWW	E12	高い
13	LANケーブル	E12	高い
14	ポート114	E12	高い
15	HUB(2)	E15,E12,E19	高い
16	ポート116	E15,E12,E19	低い
17	ポート117	E19,E26	高い
18	LANケーブル	E19,E26	高い
19	NIC119-DB	E19,E26	高い
20	DBサーバ	E19,E26	高い
21	LANケーブル	E3,E6,E10	低い
22	NIC122-ADMIN	E3,E6,E10	低い
23	ADMINサーバ	なし	低い
24	NIC124-ADMIN	E15,E12,E19	低い
25	LANケーブル	E15,E12,E19	低い
26	apl	E26	高い
27	db-soft	E26	高い
28	term	なし	高い

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/007773

**A. CLASSIFICATION OF SUBJECT MATTER**  
 Int.Cl<sup>7</sup> 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<sup>7</sup> H04L12/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

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	JP 2000-322284 A (NEC Ibaraki Ltd.), 24 November, 2000 (24.11.00), Full text; all drawings (Family: none)	1-6
A	JP 2002-223293 A (Hitachi, Ltd.), 09 August, 2002 (09.08.02), Abstract; Claims (Family: none)	1-6
A	JP 6-75807 A (Fujitsu Ltd.), 18 March, 1994 (18.03.94), Full text; all drawings (Family: none)	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  
22 July, 2005 (22.07.05)

Date of mailing of the international search report  
09 August, 2005 (09.08.05)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2005/007773

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 5-66958 A (NEC Corp.) , 19 March, 1993 (19.03.93) , Abstract (Family: none)	1-6

## A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.<sup>7</sup> 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））

Int.Cl.<sup>7</sup> H04L12/26

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

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

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）

## 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 請求の範囲の番号
A	JP 2000-322284 A (茨城日本電気株式会社) 2000. 11. 24 全文、全図 (ファミリーなし)	1-6
A	JP 2002-223293 A (株式会社日立製作所) 2002. 08. 09 要約、特許請求の範囲 (ファミリーなし)	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。

## \* 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矛盾するものではなく、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

「&amp;」同一パテントファミリー文献

国際調査を完了した日

22. 07. 2005

国際調査報告の発送日

09. 8. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

5 X 3047

玉木 宏治

電話番号 03-3581-1101 内線 3596

C (続き) 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 請求の範囲の番号
A	J P 6-75807 A (富士通株式会社) 1994. 03. 18 全文, 全図 (ファミリーなし)	1-6
A	J P 5-66958 A (日本電気株式会社) 1993. 03. 19 要約 (ファミリーなし)	1-6