

(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
2014年5月8日(08.05.2014)



(10) 国際公開番号
WO 2014/068705 A1

- (51) 国際特許分類:
G06F 11/30 (2006.01) G06F 11/34 (2006.01)
- (21) 国際出願番号: PCT/JP2012/078185
- (22) 国際出願日: 2012年10月31日(31.10.2012)
- (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: 株式会社日立製作所(HITACHI, LTD.)
[JP/JP]; 〒1008280 東京都千代田区丸の内一丁目
6番6号 Tokyo (JP).
- (72) 発明者: 町田 多嘉之(MACHIDA, Takayuki); 〒
2440817 神奈川県横浜市戸塚区吉田町292番
地 株式会社日立製作所 ITプラットフォーム
事業本部内 Kanagawa (JP). 黒田 沢希(KUR-
ODA, Takaki); 〒2440817 神奈川県横浜市戸塚区吉
田町292番地 株式会社日立製作所 ITプ
ラットフォーム事業本部内 Kanagawa (JP).
- (74) 代理人: 特許業務法人ウィルフォート国際特許
事務所(WILLFORT INTERNATIONAL); 〒1010052
東京都千代田区神田小川町三丁目3番地 神田
小川町トーセイビル117階 Tokyo (JP).

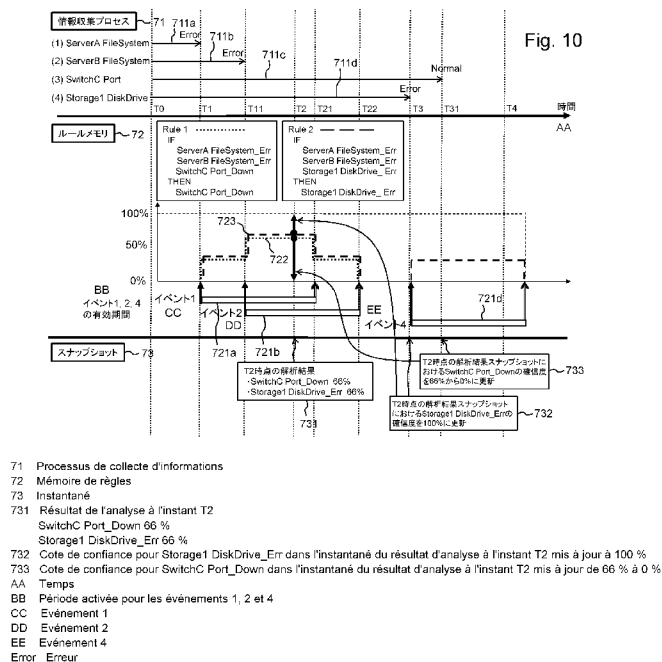
- (81) 指定国(表示のない限り、全ての種類の国内保
護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA,
BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN,
CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN,
IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR,
LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH,
PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, 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, LR, LS, MW,
MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシ
ア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ
(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,
GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT,
NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,
NE, SN, TD, TG).

添付公開書類:

— 国際調査報告(条約第21条(3))

(54) Title: MONITORING SYSTEM AND MONITORING PROGRAM

(54) 発明の名称: 監視システム及び監視プログラム



(57) Abstract: A monitoring system that transmits to multiple node devices a request wherein event occurrence information is requested and detects the occurrence of events on the basis of the event occurrence information included in the responses, and that calculates an index value for each conclusion in multiple rules indicating a correspondence relationship between one or more condition events and a conclusion, and that generates a snapshot indicating the index values for a prescribed time point at that time point. When a first response to a first request is received, on the basis of that first response the monitoring system updates the index values indicated by the snapshot generated during a period that includes the interval from the date and time of the transmission of the first request to the date and time of the receipt of the first response.

(57) 要約: 監視システムは、複数のノード装置に対してイベント発生情報を要求するリクエストを送信し、レスポンスに含まれるイベント発生情報に基づいてイベントの発生を検知し、1以上の条件イベントと結論との対応関係を示す複数のルールの各結論についての指標値を計算し、所定の時点でその時点における指標値を示すスナップショットを生成する。監視システムは、第1のリクエストに対する第1のレスポンスを受信した場合、第1のリクエストの送信日時から第1のレスポンスの受信日時までを含む期間に生成されたスナップショットが示す指標値を、第1のレスポンスに基づいて更新する。

明 細 書

発明の名称：監視システム及び監視プログラム

技術分野

[0001] 本発明は、監視対象のノード装置において発生したイベントの根本原因を解析するための技術に関する。

背景技術

[0002] サーバ、ストレージ、ネットワーク装置等のノード装置を監視し、監視対象のノード装置において発生した障害やステータス変更等の事象（以下「イベント」という）を検知し、検知したイベントの根本原因を解析する監視システムが知られている（例えば、特許文献1 参照）。

[0003] 監視システムは、例えば、複数のノード装置のいずれかに関する1 以上のイベントに対応する1 以上の条件イベントと当該1 以上の条件イベントが発生した場合に原因となる結論との対応関係を示す複数のルールを記憶し、ルール及び条件イベントの検知の有無に基づいて、各結論が原因であることの確からしさを示す確信度を計算する。例えば、或る結論についての確信度は、当該結論に対応付けられている条件イベントの総数に対する、当該結論に対応付けられている条件イベントのうちの監視システムが検知した条件イベントの数の割合とされる。監視システムは、計算した確信度を含む原因解析の結果を表示する。管理者は、監視システムに表示された原因解析の結果を参照して、根本原因を推定することができる。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第2009／144969号パンフレット

発明の概要

発明が解決しようとする課題

[0005] 例えば、監視システムは、次のようにしてノード装置におけるイベントの発生を検知する。すなわち、監視システムは、定期的又は不定期的に、ノー

ド装置においてイベントが発生しているか否かを示すイベント発生情報を要求するリクエストを各ノード装置に送信し、そのリクエストに対するレスポンスを受信するポーリング処理を行い、受信したレスポンスに含まれるイベント発生情報に基づいて、ノード装置に関するイベントの発生を検知する。

[0006] このように、監視システムがポーリング処理を行ってイベントの発生を検知する場合、例えば通信ネットワークにおけるデータ転送の遅延等の影響により、一部のノード装置からのレスポンスの受信が遅くなり、その一部のノード装置に関するイベントの検知が遅くなる場合がある。例えば、監視システムが、最初のイベントの検知から一定時間経過後の時点（第1時点）に原因解析を行うようにしている場合において、一部のノード装置に関するイベントの検知が第1時点よりも遅くなる場合がある。この場合、第1時点における原因解析では、その遅くなったイベントの検知が考慮されていないため、第1時点における原因解析の結果は、正確であるとは言えない。

[0007] また、監視システムは、例えば、遅れて検知されたイベントのその検知の時点或いはそれ以降の時点（第2時点）に原因解析を行ってもよい。しかし、監視システムが第2時点に原因解析を行う場合において、最初のイベントの検知から第2時点までの期間が長くなると、以下のような問題が生じる。

[0008] すなわち、通常、ルールに含まれる条件イベントに対応する各イベントには、有効期間が設定されている。すなわち、監視システムは、検知したイベントについて、当該イベントを検知してから当該イベントに設定されている有効期間が経過するまでは、当該イベントの検知を有効として原因解析を行い、検知してから有効期間が経過したイベントについては、当該イベントの検知を無効として原因解析を行う。

[0009] 従って、監視システムが第2の時点に原因解析を行う場合において、最初のイベントの検知から第2時点までの期間が長くなると、第2の時点において、既に最初に検知されたイベント等の有効期間が経過しており当該イベント等の検知が無効となっている場合が生じる。この場合、第2時点における原因解析では、その無効となった最初に検知されたイベント等の検知が考慮

されていないため、第2時点における原因解析の結果は、正確であるとは言えない。

[0010] ちなみに、イベントの有効期間を長くすれば、複数のイベントがそれぞれ間において検知された場合であっても、複数のイベントの検知が有効となる期間が重複する可能性が高まり、その結果、正確な確信度が得られるようになるとも考えられる。

[0011] しかしながら、イベントの有効期間が長いと、関係のないイベント（例えば、前回起きた原因によって発生したイベント等）の検知が有効のまま残り続けることになり、すなわちノイズが増えることとなって、かえって正確な原因解析ができなくなってしまう。

課題を解決するための手段

[0012] 監視システムは、複数のノード装置に対してイベント発生情報を要求するリクエストを送信し、レスポンスに含まれるイベント発生情報に基づいてイベントの発生を検知し、1以上の条件イベントと結論との対応関係を示す複数のルール各結論についての指標値を計算し、所定の時点でその時点における指標値を示すスナップショットを生成する。監視システムは、第1のリクエストに対する第1のレスポンスを受信した場合、第1のリクエストの送信日時から第1のレスポンスの受信日時までを含む期間に生成されたスナップショットが示す指標値を、第1のレスポンスに基づいて更新する。監視システムは、記憶デバイスを有していて、記憶デバイスユニットが、前述の複数のルールを記憶して良い。記憶デバイスユニットは、1又は複数の記憶デバイスを含んでおり、複数の記憶デバイスは、同種であっても異種であっても良い。

発明の効果

[0013] 監視対象のノード装置において発生したイベントの原因解析をより正確に行うことができる。

図面の簡単な説明

[0014] [図1] 図1は、実施形態に係る計算機システムの一例の構成図である。

[図2]図 2 は、実施形態に係る構成情報の一例の構成図である。

[図3]図 3 は、実施形態に係る汎用ルールの一列の構成図である。

[図4]図 4 は、実施形態に係る展開ルールの一列の構成図である。

[図5]図 5 は、実施形態に係るポーリング管理テーブルの一列の構成図である。
。

[図6]図 6 は、実施形態に係るステータス管理テーブルの一列の構成図である。
。

[図7]図 7 は、実施形態に係るルールメモリデータの一列の構成図である。

[図8]図 8 は、実施形態に係るイベント有効期間設定テーブルの一列の構成図である。

[図9]図 9 は、実施形態に係るイベント失効タスクテーブルの一列の構成図である。

[図10]図 10 は、実施形態に係る解析結果及び解析結果スナップショットの時間変化の一列を示す図である。

[図11]図 11 は、実施形態に係る解析結果スナップショットの更新対象範囲の一列を示す図である。

[図12A]図 12 A は、実施形態に係る条件テーブルの第 1 の例を示す図である。
。

[図12B]図 12 B は、実施形態に係る条件テーブルの第 2 の例を示す図である。
。

[図13A]図 13 A は、実施形態に係る展開ルールテーブルの第 1 の例を示す図である。

[図13B]図 13 B は、実施形態に係る展開ルールテーブルの第 2 の例を示す図である。

[図14A]図 14 A は、実施形態に係るスナップショットテーブルの第 1 の例を示す図である。

[図14B]図 14 B は、実施形態に係るスナップショットテーブルの第 2 の例を示す図である。

[図15]図 1 5 は、実施形態に係るスナップショット表示管理テーブルの一例の構成図である。

[図16]図 1 6 は、実施形態に係るルール展開処理のフローチャートである。

[図17]図 1 7 は、実施形態に係るリクエスト送信処理のフローチャートである。

[図18]図 1 8 は、実施形態に係る確信度計算処理のフローチャートである。

[図19]図 1 9 は、実施形態に係るスナップショット再計算処理のフローチャートである。

[図20]図 2 0 は、実施形態に係るイベント失効タスク生成処理のフローチャートである。

[図21]図 2 1 は、実施形態に係るイベント消去処理のフローチャートである。

[図22]図 2 2 は、実施形態に係るスナップショット表示処理のフローチャートである。

[図23]図 2 3 は、実施形態に係るスナップショット表示画面の一例の構成図である。

発明を実施するための形態

[0015] 実施形態について、図面を参照して説明する。なお、以下に説明する実施形態は特許請求の範囲にかかる発明を限定するものではなく、また実施形態の中で説明されている諸要素及びその組み合わせの全てが発明の解決手段に必須であるとは限らない。これらの図面において、複数の図を通じて同一の符号は同一の構成要素を示している。

[0016] なお、以後の説明では、「a a aテーブル」等の表現にて情報を説明することがあるが、これら情報はテーブル等のデータ構造以外で表現されていてもよい。そのため、データ構造に依存しないことを示すために「a a aテーブル」等について「a a a情報」と呼ぶことがある。

[0017] また、各情報の内容を説明する際に、「識別情報」、「識別子」、「名称」、「ID」という表現を用いるが、これらについては互いに置換が可能で

ある。

[0018] 以後の説明では「プログラム」を主語として説明を行う場合があるが、プログラムは、プロセッサによって実行されることで定められた処理をメモリ及び通信ポート（ネットワーク I/F）を用いながら行うため、プロセッサを主語とした説明としてもよい。また、プログラムを主語として開示された処理は、監視システム等の計算機が行う処理としてもよい。また、プログラムの一部または全ては、専用ハードウェアによって実現されてもよい。また、各種プログラムは、プログラム配布サーバや、計算機が読み取り可能な記憶メディアによって各計算機にインストールされてもよい。

[0019] 以後、計算機システムを監視し、表示用情報を表示する一つ以上の計算機の集合を監視システムと呼ぶことがある。監視コンピュータが表示用情報を表示する場合は監視コンピュータが監視システムである。また、監視コンピュータと表示用装置の組み合わせも監視システムである。また、処理の高速化や高信頼化のために複数の計算機で監視コンピュータと同等の処理を実現してもよく、この場合は当該複数の計算機（表示を表示用装置が行う場合は表示用装置も含め）が監視システムである。なお、計算機（或いは、計算機が有する制御デバイス（例えばプロセッサ））の「表示する」という行為は、計算機が、その計算機の表示デバイスに情報を表示する行為と、表示デバイスを有する別の計算機に、その表示デバイスに表示される情報（表示用情報）を送信する行為のいずれであっても良い。

[0020] 図 1 は、実施形態に係る計算機システムの一例の構成図である。

[0021] 計算機システムは、監視コンピュータ 1 と、1 以上のサーバ 2 と、1 以上のストレージ 3 と、1 以上のネットワーク装置 4 と、LAN（Local Area Network）等の通信ネットワーク 5 とを有する。本実施形態における計算機システムは、2 つのサーバ 2、すなわち、「Server A」という名称のサーバ 2（以下、サーバ「Server A」と表記する）と、「Server B」という名称のサーバ 2（以下、サーバ「Server B」と表記する）とを含む。また、本実施形態における計算機システムは、2 つのストレージ 3

、すなわち、「Storage 1」という名称のストレージ3（以下、ストレージ「Storage 1」と表記する）と、「Storage 2」という名称のストレージ3（以下、ストレージ「Storage 2」と表記する）とを含む。ネットワーク装置4は、IP（Internet Protocol）スイッチ（以下、単に「スイッチ」と呼ぶことがある）やルータ等である。監視コンピュータ1、サーバ2、及びストレージ3は、通信ネットワーク5及びネットワーク装置4を介して相互に接続される。

[0022] 以下、計算機システムを構成する装置（サーバ2、ストレージ3、ネットワーク装置4等）を「ノード装置」と呼ぶことがある。計算機システムは、例えば、ホストコンピュータ、NAS（Network Attached Storage）、ファイルサーバ、プリンタ等をノード装置として有していてもよい。また、ノード装置が有するデバイス等の論理的又は物理的な構成物を「コンポーネント」と呼ぶことがある。コンポーネントの例としては、CPU（Central Processing Unit）、メモリ、ネットワークI/F（インターフェース）、ディスク、プログラム、ストレージ3で定義されるボリューム、RAID（Redundant Arrays of Inexpensive Disks）グループ等がある。以下、監視コンピュータ1が監視の対象とするノード装置を「監視対象装置」と呼ぶことがある。

[0023] サーバ2は、サーバプログラム等を実行し、ユーザに対して所定のサービスを提供する計算機である。サーバ2は、CPU 21と、メモリ 22と、ネットワークI/F 23と、iSCSI（Internet Small Computer System Interface）イニシエータ（図示しない）とを有する。サーバ2には、ストレージ3の記憶領域が割り当てられた仮想的なボリュームであるiSCSIディスク（以下、単に「ディスク」と呼ぶ場合がある）24が形成される。サーバ2は、iSCSIイニシエータを介すことで、iSCSIディスク24をローカルハードディスクのように利用できる。ネットワークI/F 23は、通信ネットワーク5に接続するためのインターフェースデバイスである。なお、サーバ2は、物理サーバであってもよいし、1以上のVMを稼働させる

仮想サーバであってもよい。

[0024] ストレージ 3 は、サーバ 2 等に記憶領域を提供する装置である。ストレージ 3 は、ストレージコントローラ 3 1 と、ディスクドライブ 3 2 と、ネットワーク I/F 3 3 とを有する。ストレージ 3 は、ディスクドライブ 3 2 に代えて又はディスクドライブ 3 2 に加えて、固体記憶媒体、光記憶媒体等の他の種類の記憶媒体を有していてもよい。ネットワーク I/F 3 3 は、通信ネットワーク 5 に接続するためのインターフェースデバイスである。ストレージ 3 は、例えば、サーバ 2 に対して、iSCSI ディスク 2 4 を形成するための記憶領域を提供する。

[0025] 監視コンピュータ 1 は、監視対象装置を管理する計算機である。監視コンピュータ 1 は、例えば、汎用的な計算機であり、CPU 1 1 と、記憶資源 1 2 と、入出力 I/F 1 4 と、ネットワーク I/F 1 5 と、バス 1 6 とを有する。CPU 1 1、記憶資源 1 2、入出力 I/F 1 4、及びネットワーク I/F 1 5 は、バス 1 6 を介して相互に接続される。記憶資源 1 2 は、メモリであってもよいし、ハードディスクドライブ (HDD) 等の二次記憶装置であってもよいし、メモリ及び二次記憶装置の組み合わせであってもよい。

[0026] 記憶資源 1 2 は、ルール展開プログラム 1 2 1 と、リクエスト送信プログラム 1 2 2 と、イベント検知プログラム 1 2 3 と、確信度計算プログラム 1 2 4 と、スナップショット再計算プログラム 1 2 5 と、イベント失効タスク生成プログラム 1 2 6 と、イベント消去プログラム 1 2 7 とを記憶する。記憶資源 1 2 に記憶された各種プログラム 1 2 1 ~ 1 2 7 は、CPU 1 1 によって実行される。記憶資源 1 2 は、さらに、ルールメモリ 1 2 8 と、構成情報 1 3 1 と、汎用ルールリポジトリ 1 3 2 と、ポーリング管理テーブル (TBL) 1 3 3 と、ステータス管理テーブル 1 3 4 と、イベント有効期間設定テーブル 1 3 5 と、イベント失効タスクテーブル 1 3 6 と、条件テーブル 1 3 7 と、展開ルールテーブル 1 3 8 と、スナップショットテーブル 1 3 9 と、スナップショット表示管理テーブル 1 3 0 とを記憶する。ルールメモリ 1 2 8 には、確信度の計算を行う確信度計算処理に利用されるルールメモリデ

ータが格納される。汎用ルールリポジトリ 132 には、1 以上の汎用ルールが格納される。

[0027] ネットワーク I/F 15 は、通信ネットワーク 5 に接続するためのインターフェースデバイスである。入出力 I/F 14 は、ディスプレイ 17 に接続するためのインターフェースデバイスである。監視コンピュータ 1 は、原因解析の結果や他の情報をディスプレイ 17 に表示させることで、原因解析の結果等を管理者に提示する。なお、監視コンピュータ 1 が、内部にディスプレイ 17 を有していてもよい。

[0028] 監視コンピュータ 1 は、定期的又は不定期的に、監視対象装置に対して、監視対象装置それ自体又はそのコンポーネントがどのようなステータスになっているか、すなわち正常に動作しているか又は異常となっているかを問い合わせるためのデータ（以下「ステータスリクエスト」又は単に「リクエスト」という）を送信する。ステータスリクエストを受信した監視対象装置は、監視対象装置それ自体又はそのコンポーネントのステータスを示す情報（イベント発生情報、以下「ステータス情報」という）を含む応答データ（以下「ステータスレスポンス」又は単に「レスポンス」という）を監視コンピュータ 1 に送信する。監視コンピュータ 1 は、監視対象装置から受信したステータスレスポンスに基づいて、監視対象装置においてイベントが発生しているか否かを判定する。監視コンピュータ 1 は、例えば、監視対象装置又はそのコンポーネントのステータスに変更があった場合に、イベントの原因を解析する処理（確信度計算処理）等の種々の処理を行い、その処理結果を出力する。本実施形態において、定期的又は不定期的に、監視対象装置に対してステータスリクエストを送信し、監視対象装置又はそのコンポーネントに関するステータス情報を監視対象装置から取得する処理を「リクエスト送信処理」と呼ぶ。

[0029] 図 2 は、実施形態に係る構成情報の一例の構成図である。

[0030] 構成情報 131 は、計算機システムの構成を示す情報であり、具体的には、計算機システムがどんなノード装置によって構成されているか、各ノード

装置の構成がどのようなになっているか（例えば、ノード装置がどんなコンポーネントを有しているか）、ノード装置間或いはコンポーネント間の接続関係がどのようなになっているか、ノード装置とコンポーネントとの間の包含関係がどのようなになっているか等を示す情報である。構成情報 131 は、例えば、ルータ管理テーブル 1311 と、iSCSI ターゲット管理テーブル 1316 とを含む。

[0031] ルータ管理テーブル 1311 は、計算機システムに含まれるネットワーク装置 4 の一例である各ルータが接続するサブネットを管理するためのデータである。ルータ管理テーブル 1311 は、ノード ID 1312、ノードタイプ 1313、サブネット ID 1 1314、及びサブネット ID 2 1315 のフィールドを含む。ノード ID 1312 には、ルータの識別子が格納される。ノードタイプ 1313 には、ノード装置の種別がルータであることを示すデータ、例えば「Router」が格納される。サブネット ID 1 1314 及びサブネット ID 2 1315 のそれぞれには、ルータによって接続される 2 つのサブネットのそれぞれの識別子が格納される。例えば、図 2 のルータ管理テーブル 1311 の上から 1 番目のエントリから、識別子が「9」のルータは、識別子が「0」のサブネットと識別子が「1」のサブネットとを接続していることがわかる。

[0032] iSCSI ターゲット管理テーブル 1316 は、iSCSI ターゲットと当該 iSCSI ターゲットが接続を許可する iSCSI イニシエータとの対応関係を管理するためのデータである。iSCSI ターゲット管理テーブル 1316 は、ターゲット ID 1317、iSCSI ターゲット名 1318、及び接続許可 iSCSI イニシエータ名 1319 のフィールドを含む。ターゲット ID 1317 には、iSCSI ターゲットと当該 iSCSI ターゲットが接続を許可する iSCSI イニシエータとの組み合わせごとに付与される識別子が格納される。iSCSI ターゲット名 1318 には、iSCSI ターゲットを特定するデータが格納される。接続許可 iSCSI イニシエータ名 1319 には、接続が許可されている iSCSI イニシエータを特定す

るデータが格納される。例えば、図2のiSCSIターゲット管理テーブル1316の上から1番目のエントリから、iSCSIターゲットであるストレージ「Storage1」（「com.hi.sto1」によって特定されるストレージ3）は、iSCSIイニシエータであるサーバ「ServerA」（「com.hi.svA」によって特定されるサーバ2）に対して接続を許可していることがわかる。

[0033] 図3は、実施形態に係る汎用ルールの一例の構成図である。

[0034] 汎用ルールリポジトリ132には、1以上の汎用ルール61が格納される。汎用ルール61は、ノード装置のいずれかに関する1以上の条件イベントと、当該1以上の条件イベントが発生した場合に原因となる結論と、の対応関係を、計算機システムの実構成に依存しない形式で記述した情報である。汎用ルール61は、複数の結論を含んでもよい。本実施形態において、結論はイベントであり、結論を結論イベントと呼ぶことがある。

[0035] 汎用ルール61は、IF部611とTHEN部612とを有する。IF部611は、1以上の条件イベントデータ要素613を含む。条件イベントデータ要素613は、種別によって抽象化されたノード装置に関する条件イベントを示し、例えば、条件イベントに関係するノード装置の種別を示すデータと、条件イベントの種別を示すデータとを含む。また、THEN部612は、結論イベントデータ要素614を含む。結論イベントデータ要素614は、種別によって抽象化されたノード装置に関する結論イベントを示し、例えば、結論イベントに関係するノード装置の種別を示すデータと、結論イベントの種別を示すデータとを含む。なお、条件イベントデータ要素613及び結論イベントデータ要素614は、条件イベント又は結論イベントに関係するコンポーネントの種別を示すデータを含んでもよい。本実施形態において、条件イベント又は結論イベントに関係するコンポーネントの種別を示すデータは、条件イベント又は結論イベントの種別を示すデータに含まれている。例えば、「ファイルシステムエラー（FileSystem__Error）」のイベントは、ファイルシステムというコンポーネントに関するイベ

ントであり、「ポートダウン (Port_Down)」のイベントは、ポートというコンポーネントに関するイベントであり、「ディスクドライブエラー (DiskDrive_Err)」のイベントは、ディスクドライブ32というコンポーネントに関するイベントである。

[0036] 例えば、同図の汎用ルール「GenRule1」は、3つの条件イベントデータ要素613と1つの結論イベントデータ要素614とを含む。すなわち、汎用ルール「GenRule1」は、3つの条件イベントデータ要素613がそれぞれ示す3つの条件イベントが検知された場合に、結論イベントデータ要素614が示す結論イベントが原因であると特定されることを表している。具体的には、汎用ルール「GenRule1」に含まれる3つの条件イベントデータ要素613は、それぞれ、サーバ2に関する「ファイルシステムエラー」のイベントと、サーバ2に関する「ファイルシステムエラー」のイベントと、スイッチに関する「ポートダウン」のイベントとを示している。また、汎用ルール「GenRule1」に含まれる結論イベントデータ要素614は、スイッチに関する「ポートダウン」のイベントを示している。従って、汎用ルール「GenRule1」は、2つのサーバ2のそれぞれに関する2つの「ファイルシステムエラー」のイベントと、スイッチに関する「ポートダウン」のイベントとが検知された場合に、スイッチに関する「ポートダウン」のイベントが原因であると特定されることを表している。同様に、汎用ルール「GenRule2」は、2つのサーバ2のそれぞれに関する2つの「ファイルシステムエラー」のイベントと、ストレージ3に関する「ディスクドライブエラー」のイベントとが検知された場合に、ストレージ3に関する「ディスクドライブエラー」のイベントが原因であると特定されることを表している。

[0037] 図4は、実施形態に係る展開ルールの一例の構成図である。

[0038] 展開ルール62は、汎用ルール61を計算機システムの実構成に依存する形式に展開した情報である。展開ルール62は、複数の結論を含んでもよい。汎用ルール61と同様に、展開ルール62は、IF部621とTHE

N部622とを有する。IF部621は、1以上の条件イベントデータ要素623を含む。条件イベントデータ要素623は、具体的なノード装置に関する条件イベントを示し、例えば、条件イベントに関係するノード装置の名称と、条件イベントの種別を示すデータとを含む。また、THEN部622は、結論イベントデータ要素624を含む。結論イベントデータ要素624は、具体的なノード装置に関する結論イベントを示し、例えば、結論イベントに関係するノード装置の名称と、結論イベントの種別を示すデータとを含む。なお、条件イベントデータ要素623及び結論イベントデータ要素624は、条件イベント又は結論イベントに関係するコンポーネントの名称を示すデータを含んでいてもよい。

[0039] 例えば、同図の展開ルール「E x p R u l e 1」（以下「ルール1」という）は、3つの条件イベントデータ要素623と1つの結論イベントデータ要素624とを含む。すなわち、ルール1は、3つの条件イベントデータ要素623がそれぞれ示す3つの条件イベントが検知された場合に、結論イベントデータ要素624が示す結論イベントが原因であると特定されることを表している。具体的には、ルール1に含まれる3つの条件イベントデータ要素623は、それぞれ、サーバ「S e r v e r A」に関する「ファイルシステムエラー」のイベントと、サーバ「S e r v e r B」に関する「ファイルシステムエラー」のイベントと、スイッチ「S w i t c h C」に関する「ポートダウン」のイベントとを示している。また、ルール1に含まれる結論イベントデータ要素624は、スイッチ「S w i t c h C」に関する「ポートダウン」のイベントを示している。従って、ルール1は、サーバ「S e r v e r A」に関する「ファイルシステムエラー」のイベントと、サーバ「S e r v e r B」に関する「ファイルシステムエラー」のイベントと、スイッチ「S w i t c h C」に関する「ポートダウン」のイベントとが検知された場合に、スイッチ「S w i t c h C」に関する「ポートダウン」のイベントが原因であると特定されることを表している。同様に、展開ルール「E x p R u l e 2」（以下「ルール2」という）は、サーバ「S e r v e r A」に関

する「ファイルシステムエラー」のイベントと、サーバ「S e r v e r B」に関する「ファイルシステムエラー」のイベントと、ストレージ「S t o r a g e 1」に関する「ディスクドライブエラー」のイベントとが検知された場合に、ストレージ「S t o r a g e 1」に関する「ディスクドライブエラー」のイベントが原因であると特定されることを表している。

[0040] 図5は、実施形態に係るポーリング管理テーブルの一例の構成図である。

[0041] ポーリング管理テーブル133は、監視対象装置ごとに、当該監視対象装置に送信されたステータスリクエストの送信日時を管理するためのデータである。ポーリング管理テーブル133は、ノードID1331、及びリクエスト送信日時1332のフィールドを含む。ノードID1331には、ノード装置の識別子（以下「ノードID」という）が格納される。リクエスト送信日時1332には、ノードID1331によって示されるノード装置に送信されたステータスリクエストの送信日時を示すデータが格納される。また、リクエスト送信日時1332には、監視コンピュータ1が、ステータスリクエストに対するステータスレスポンスを対象のノード装置から受信した場合には、そのことを示すデータ、例えば「-」が格納される。例えば、同図の上から1番目のエントリから、ノードIDが「70」のノード装置に対して2008年4月13日の9時15分11秒にステータスリクエストが送信され、そのステータスリクエストに対するステータスレスポンスが、監視コンピュータ1によって未だ受信されていないことがわかる。また、同図の上から3番目のエントリから、ノードIDが「100」のノード装置に対して送信されたステータスリクエストに対するステータスレスポンスが、監視コンピュータ1によって既に受信されていることがわかる。

[0042] 図6は、実施形態に係るステータス管理テーブルの一例の構成図である。

[0043] ステータス管理テーブル134は、監視対象装置又はそのコンポーネントに関するステータス情報を管理するためのデータである。ステータス管理テーブル134は、ステータス管理ID1341、ノードID1342、ノード種別1343、ノード名1344、コンポーネントID1345、コンポ

ーネント名 1 3 4 6、イベント種別 1 3 4 7、最新のステータス (S t a t u s) 1 3 4 8、最新の情報収集プロセスのイベント受信日時 1 3 4 9、最新の情報収集プロセス開始日時 1 3 4 0、前回のステータス 1 3 4 a、及び前回の情報収集プロセス開始日時 1 3 4 b のフィールドを含む。

[0044] ステータス管理 I D 1 3 4 1 には、ステータス管理テーブル 1 3 4 に登録されるエントリの識別子（以下「ステータス管理 I D」という）が格納される。ノード I D 1 3 4 2 には、ステータス情報に関するノード装置のノード I D が格納される。ノード種別 1 3 4 3 には、ステータス情報に関するノード装置の種別を示すデータが格納される。ノード名 1 3 4 4 には、ステータス情報に関するノード装置の名称が格納される。コンポーネント I D 1 3 4 5 には、ステータス情報に関するコンポーネントの識別子が格納される。コンポーネント名 1 3 4 6 には、ステータス情報に関するコンポーネントの名称が格納される。イベント種別 1 3 4 7 には、ステータスが異常となることに対応するイベント、すなわち、ステータスが異常となった場合に発生したものとみなされるイベントの種別を示すデータが格納される。

[0045] 最新のステータス 1 3 4 8 には、直近のリクエスト送信処理によって取得された、最新のステータスを示すステータス情報が格納される。本実施形態において、ステータス情報の値は、対象の監視対象装置のコンポーネントが正常に動作している場合は「 N o r m a l 」とされ、対象の監視対象装置のコンポーネントが異常となっている場合は「 E r r o r 」とされる。最新の情報収集プロセスのイベント受信日時 1 3 4 9 には、最新のステータスを示すステータス情報の取得日時、すなわち、直近のリクエスト送信処理において、監視コンピュータ 1 がステータスレスポンスを受信した日時を示すデータが格納される。最新の情報収集プロセス開始日時 1 3 4 0 には、直近のリクエスト送信処理において、監視コンピュータ 1 がステータスリクエストを送信した日時を示すデータが格納される。前回のステータス 1 3 4 a には、前回のリクエスト送信処理によって取得された、前回のステータスを示すステータス情報が格納される。前回の情報収集プロセス開始日時 1 3 4 b には

、前回のリクエスト送信処理において、監視コンピュータ 1 がステータスリクエストを送信した日時を示すデータが格納される。

[0046] 例えば、同図のステータス管理 ID が「1」のエントリから、サーバ「Server A」のファイルシステム「File System A」の最新のステータスが異常となっていること、すなわち、サーバ「Server A」に関する「ファイルシステムエラー」のイベントが発生していることがわかる。また、同エントリから、サーバ「Server A」に対する直近のリクエスト送信処理において、監視コンピュータ 1 は、2008 年 4 月 13 日の 9 時 15 分 11 秒にステータスリクエストを送信し、2008 年 4 月 13 日の 9 時 20 分 11 秒にステータスレスポンスを受信、すなわち最新のステータスを示すステータス情報を取得していることがわかる。さらに、同エントリから、サーバ「Server A」のファイルシステム「File System A」の前回のステータスも異常となっていたこと、及び、サーバ「Server A」に対する前回のリクエスト送信処理において、監視コンピュータ 1 は、2008 年 4 月 13 日の 9 時 10 分 11 秒にステータスリクエストを送信していることがわかる。

[0047] 図 7 は、実施形態に係るルールメモリデータの一例の構成図である。

[0048] ルールメモリデータ 8 は、少なくとも、イベントの原因解析に用いられる複数の展開ルール 62 と、その展開ルール 62 の条件イベントに関する検知の有無を示すデータと、その展開ルール 62 の結論イベントが原因であることの確からしさを示す確信度とを、複数のオブジェクト及びそれらの関連付けにより表現したデータである。ルールメモリデータ 8 は、展開ルール 62 に基づいて生成されてもよいし、汎用ルール 61 及び構成情報 131 に基づいて生成されてもよい。

[0049] ルールメモリデータ 8 は、複数の条件オブジェクト 81 と、複数の結論オブジェクト 82 と、複数の演算子オブジェクト 83 と、それぞれの接続情報とを含む。条件オブジェクト 81 は、展開ルール 62 の条件イベントに対応し、結論オブジェクト 82 は、展開ルール 62 の結論イベントに対応する。

条件オブジェクト 8 1 と結論オブジェクト 8 2 とは、演算子オブジェクト 8 3 を介して接続される。条件オブジェクト 8 1 と結論オブジェクト 8 2 との接続関係は、展開ルール 6 2 における条件イベントと結論イベントとの対応関係を示している。なお、各オブジェクトは、コンピュータ言語では例えば構造体やクラスとして実装され、プログラム動作中はメモリに格納されるデータ（オブジェクトデータ）である。

[0050] 条件オブジェクト 8 1 は、条件イベントに関するデータを管理するオブジェクトである。条件オブジェクト 8 1 は、Node 8 1 1、NodeName 8 1 2、Component 8 1 3、ComponentName 8 1 4、Event 8 1 5、及びReceived 8 1 6 のフィールドを含む。Node 8 1 1 には、この条件オブジェクト 8 1 に対応する条件イベントに関するノード装置の種別を示すデータが格納される。NodeName 8 1 2 には、この条件オブジェクト 8 1 に対応する条件イベントに関するノード装置の名称が格納される。Component 8 1 3 には、この条件オブジェクト 8 1 に対応する条件イベントに関するコンポーネントの種別を示すデータが格納される。ComponentName 8 1 4 には、この条件オブジェクト 8 1 に対応する条件イベントに関するコンポーネントの名称が格納される。Event 8 1 5 には、この条件オブジェクト 8 1 に対応する条件イベントの種別を示すデータが格納される。Received 8 1 6 には、この条件オブジェクト 8 1 に対応する条件イベントが監視コンピュータ 1 によって検知された日時（検知日時）を示すデータが格納される。

[0051] 例えば、同図の上から 1 番目の条件オブジェクト 8 1 は、サーバ「Server A」に関する「ファイルシステムエラー」の条件イベントに関するデータを管理する。この条件オブジェクトのReceived 8 1 6 には、「4 / 13 / 2008 9 : 20 : 11」が格納されている。従って、この条件オブジェクトは、サーバ「Server A」に関する「ファイルシステムエラー」の条件イベントが、2008 年 4 月 13 日の 9 時 20 分 11 秒に、監視コンピュータ 1 によって検知されたことを示している。

[0052] 結論オブジェクト82は、結論イベントに関するデータを管理するオブジェクトである。結論オブジェクト82は、Rule 821、Node 822、Cause 823、及びMR 824のフィールドを含む。Rule 821には、この結論オブジェクト82に対応する結論イベントを含む展開ルール62の名称が格納される。Node 822には、この結論オブジェクト82に対応する結論イベントに関係するノード装置の名称が格納される。Cause 823には、この結論オブジェクト82に対応する結論イベントの種別を示すデータが格納される。MR 824には、この結論オブジェクト82に対応する結論イベントについての確信度が格納される。確信度は、後述する確信度計算処理において計算される。

[0053] なお、ルールメモリデータ8は、図7で説明した構造に限られるものではなく、条件イベント及び結論イベントの対応関係、条件イベントの検知の有無、及び結論イベントについての確信度を表現し得る他のデータ構造であってもよい。

[0054] 図8は、実施形態に係るイベント有効期間設定テーブルの一例の構成図である。

[0055] イベント有効期間設定テーブル135は、イベントごとに設定された有効期間を管理するためのデータである。ここで、イベントの有効期間とは、監視コンピュータ1によって検知されたイベントが、原因解析において検知されたものとして取り扱われる期間のこと、すなわちイベントの検知が有効とされる期間のことをいう。例えば、イベントAの有効期間がBに設定されている場合において、監視コンピュータ1が或る日時CにイベントAを検知した場合、日時Cから有効期間Bが経過するまでの間は、イベントAの検知は有効とされ、イベントAは検知されているものと取り扱われて原因解析が行われる。そして、日時Cから有効期間Bが経過した後、監視コンピュータ1が再度イベントAを検知するまでは、イベントAの検知は無効とされ、イベントAは検知されていないものと取り扱われて原因解析が行われる。

[0056] イベント有効期間設定テーブル135は、ノード種別1351、イベント

種別 1 3 5 2、及び有効期間 1 3 5 3 のフィールドを含む。ノード種別 1 3 5 1 には、イベントに係するノード装置の種別を示すデータが格納される。イベント種別 1 3 5 2 には、イベントの種別を示すデータが格納される。有効期間 1 3 5 3 には、イベントに設定されている有効期間を示すデータが格納される。例えば、同図の上から 3 番目のエントリから、サーバ 2 に関する「ファイルシステムエラー」のイベントには、有効期間「10」（分）が設定されていることがわかる。

[0057] 図 9 は、実施形態に係るイベント失効タスクテーブルの一例の構成図である。

[0058] イベント失効タスクテーブル 1 3 6 は、監視コンピュータ 1 によって検知されたイベントについてのイベント失効タスクに関する情報を管理するためのデータである。ここで、イベント失効タスクとは、有効期間が経過したイベントの検知を無効にするタスクのことをいう。イベント失効タスクテーブル 1 3 6 は、開始日時 1 3 6 1、ノード名 1 3 6 2、及びイベント種別 1 3 6 3 のフィールドを含む。開始日時 1 3 6 1 には、イベント失効タスクの実行が開始される日時（以下「タスク開始日時」という）を示すデータが格納される。タスク開始日時は、例えば、イベント失効タスクの対象となるイベントが検知された日時に当該イベントに設定されている有効期間を加えた日時とされる。ノード名 1 3 6 2 には、イベント失効タスクの対象となるイベントに係するノード装置の名称が格納される。イベント種別 1 3 6 3 には、イベント失効タスクの対象となるイベントの種別を示すデータが格納される。例えば、同図の上から 1 番目のエントリから、サーバ「Server A」に関する「ファイルシステムエラー」のイベントについてのイベント失効タスクが 2008 年 4 月 13 日の 9 時 20 分 11 秒に開始されることがわかる。

[0059] 図 10 は、実施形態に係る解析結果及び解析結果スナップショットの時間変化の一例を示す図である。

[0060] 同図は、図 4 で説明した 2 つの展開ルール 6 2（ルール 1 及びルール 2）

に基づいて原因解析が行われる場合の例である。ルール1又はルール2に係る監視対象装置は、サーバ「Server A」、サーバ「Server B」、スイッチ「Switch C」、及びストレージ「Storage 1」の4つである。

- [0061] 同図の情報収集プロセス項目71における4つの矢印711（711a、711b、711c、及び711d）は、4つの監視対象装置のそれぞれに関する、ステータスリクエストの送信からステータスレスポンスの受信までの期間を示している。この例では、監視コンピュータ1は、T0の時点で一斉に、4つの監視対象装置にステータスリクエストを送信している。そして、監視コンピュータ1は、T1の時点で、ファイルシステムに異常が発生していることを示すステータスレスポンスをサーバ「Server A」から受信している（矢印711a参照）。すなわち、監視コンピュータ1は、T1の時点で、サーバ「Server A」に関する「ファイルシステムエラー」のイベント（以下「イベント1」と表記する）の発生を検知している。また、監視コンピュータ1は、T11の時点で、ファイルシステムに異常が発生していることを示すステータスレスポンスをサーバ「Server B」から受信している（矢印711b参照）。すなわち、監視コンピュータ1は、T11の時点で、サーバ「Server B」に関する「ファイルシステムエラー」のイベント（以下「イベント2」と表記する）の発生を検知している。また、監視コンピュータ1は、T3の時点で、ディスクドライブ32に異常が発生していることを示すステータスレスポンスをストレージ「Storage 1」から受信している（矢印711d参照）。すなわち、監視コンピュータ1は、T3の時点で、ストレージ「Storage 1」に関する「ディスクドライブエラー」のイベント（以下「イベント4」と表記する）の発生を検知している。また、監視コンピュータ1は、T31の時点で、ポートが正常であることを示すステータスレスポンスをスイッチ「Switch C」から受信している（矢印711c参照）。すなわち、監視コンピュータ1は、T31の時点で、スイッチ「Switch C」に関する「ポートダウン」

のイベント（以下「イベント3」と表記する）は発生していないことを認識している。

[0062] 同図のルールメモリ項目72における3つの矩形721（721a、721b、及び721d）は、検知された3つのイベントの有効期間を示している。具体的には、矩形721aは、イベント1の有効期間を示している。イベント1の検知は、T1の時点から所定期間、すなわちイベント1に設定されている有効期間が経過するまで有効となっている。また、矩形721bは、イベント2の有効期間を示している。イベント2の検知は、T11の時点から所定期間、すなわちイベント2に設定されている有効期間が経過するまで有効となっている。また、矩形721dは、イベント4の有効期間を示している。イベント4の検知は、T3の時点から所定期間、すなわちイベント4に設定されている有効期間が経過するまで有効となっている。

[0063] 同図のルールメモリ項目72における点線722は、確信度計算処理で得られたルール1に関する解析結果、すなわち、ルール1の結論イベントであるイベント3が原因となることについての確信度（以下「ルール1の確信度」という）の時間変化を示している。T1の時点において、ルール1の条件イベントのうちの1つ、すなわちイベント1が検知されたため、T1の時点におけるルール1の確信度は、33%（ $1/3 \times 100\%$ ）（小数点以下を省略）となる。その後、T11の時点において、イベント2が検知される。T11の時点では、ルール1の条件イベントのうちの2つ、すなわちイベント1及びイベント2の検知が有効となるため、ルール1の確信度は、33%から66%（ $2/3 \times 100\%$ ）（小数点以下を省略）に増加する。その後、T21の時点においてイベント1の検知が無効にされると、ルール1の確信度は33%に減少し、T22の時点においてイベント2の検知が無効にされると、ルール1の確信度は0%となる。

[0064] また、同図のルールメモリ項目72における破線723は、確信度計算処理で得られたルール2に関する解析結果、すなわち、ルール2の結論イベントであるイベント4が原因となることについての確信度（以下「ルール2の

確信度」という)の時間変化を示している。ルール2は、ルール1と同様に、条件イベントにイベント1及びイベント2を含む。また、ルール2は、条件イベントとして、イベント4を含む。したがって、ルール2は、ルール1と同様に、条件イベントの総数が3である。すなわち、ルール1とルール2とは、確信度を計算する際の母数が同じである。また、イベント1及びイベント2以外のルール2の条件イベントであるイベント4は、イベント1及びイベント2以外のルール1の条件イベントであるイベント3と同様に、 $T1 \sim T22$ の期間は検知されない。従って、 $T1 \sim T22$ の期間におけるルール2の確信度の値の変化は、ルール1と同じである。

[0065] 同図の例では、 $T3$ の時点において、ルール2の条件イベントであるイベント4が検知される。しかし、 $T3$ の時点では、イベント4以外のルール2の条件イベント、すなわちイベント1及びイベント2は、既に有効期間を経過しておりその検知が無効となっている。従って、 $T3$ の時点におけるルール2の確信度は、 $33\% (1 / 3 \times 100\%)$ となる。すなわち、 $T3$ の時点において、ルール2の3つの条件イベントが全て監視コンピュータ1によって検知されたことになるが、イベントの検知日時のずれ及びイベントの有効期間の影響を受けて、ルール2の確信度(確信度計算処理で得られる確信度)は 100% とはならない。つまり、確信度計算処理で得られるルール2の確信度のピーク値は、ルール1と同じ 66% となる。このため、管理者は、確信度計算処理によって得られる確信度、すなわち点線722及び破線723が示す確信度を参照しただけでは、ルール1の結論イベントが原因であるのかルール2の結論イベントが原因であるのかを判断することができない。

[0066] ちなみに、イベントの有効期間を長くすれば、複数の条件イベントがそれぞれ間をおいて検知された場合であっても、複数の条件イベントの検知が有効となる期間が重複する可能性が高まり、結果として高い確信度が得られるようになる。しかしながら、イベントの有効期間が長いと、関係のないイベント(例えば、前回起きた原因によって発生したイベント等)の検知が有効

のまま残り続けることになり、すなわちノイズが増えることとなって、正確な原因解析ができなくなってしまう。従って、必要以上にイベントの有効期間を長くすることはできない。

[0067] 本実施形態に係る監視コンピュータ 1 は、所定のタイミングでその時点の解析結果を示すデータを生成して記憶資源 12 に保存する。以下、記憶資源 12 に保存された或る時点の解析結果を示すデータを「解析結果スナップショット」と呼ぶ。監視コンピュータ 1 は、例えば、イベントを受信してから一定時間経過後に解析結果スナップショットを生成してもよいし、確信度計算処理において確信度が計算された後に解析結果スナップショットを生成してもよい。イベントを受信してから一定時間経過後に解析結果スナップショットを生成する場合における上記一定時間は、例えば、受信したイベントの種別によらず一定であってもよいし、イベントの種別に応じて異なる値、例えば、重要度の大きいイベントであれば長く重要度の小さいイベントであれば短い値としてもよい。また、リクエスト送信処理におけるステータスリクエストの送信周期に基づいて、解析結果スナップショットを生成するタイミングが決定されてもよい。例えば、ステータスリクエストの送信周期が A であれば、監視コンピュータ 1 は、A の数倍（例えば、1.5 倍、2 倍等）或いは A の数分の一の周期で、解析結果スナップショットを生成してもよい。

[0068] 同図の例では、監視コンピュータ 1 は、最初のイベントの検知、つまりイベント 1 の検知から一定時間経過後の T2 の時点において、解析結果スナップショットを生成している。この解析結果スナップショットが示すルール 1 及びルール 2 の確信度は、この解析結果スナップショットが生成された時点、すなわち T2 の時点において、いずれも 66% である。

[0069] また、本実施形態に係る監視コンピュータ 1 は、ステータスレスポンスを受信した際に、受信したステータスレスポンスに含まれるステータス情報に基づいて、過去に生成された解析結果スナップショットが示す解析結果を更新する。更新の対象となる解析結果スナップショットは、例えば、受信したステータスレスポンスに対応するステータスリクエスト、すなわち受信した

ステータスレスポンスを要求したステータスリクエストの送信日時からその受信したステータスレスポンスの受信日時まで（受信したステータスレスポンスに対応するステータスリクエストの送信日時及び受信したステータスレスポンスの受信日時を除く）に生成された解析結果スナップショットである。なお、図 11 を参照して後述するように、例えば、前回受信したステータスレスポンスに対応するステータスリクエストの送信日時から直近に受信したステータスレスポンスの受信日時まで（前回のステータスリクエストの送信日時及び直近のステータスレスポンスの受信日時を除く）に生成された解析結果スナップショットを更新の対象としてもよい。

[0070] 例えば、監視コンピュータ 1 は、受信したステータスレスポンスに含まれるステータス情報が「E r r o r」であり、イベントの発生を検知した場合は、対象の解析結果スナップショットが示す確信度のうちの、その検知したイベントを条件イベントに含む展開ルール 62 の確信度を、そのイベントの検知が考慮された値に更新する。また、例えば、監視コンピュータ 1 は、受信したステータスレスポンスに含まれるステータス情報が「N o r m a l」であり、イベントが発生していないことを認識した場合は、対象の解析結果スナップショットが示す確信度のうちの、その未発生を認識したイベントを結論イベントとする展開ルール 62 の確信度を、0%に更新する。

[0071] 図 10 の例では、監視コンピュータ 1 は、T3 の時点において、ディスクドライブ 32 に異常が発生していることを示すステータスレスポンス（図 10 の説明において「レスポンス（4）」という）をストレージ「S t o r a g e 1」から受信し、イベント 4 の発生を検知している。ここで、レスポンス（4）に対応するステータスリクエストは、T0 の時点で送信されているため、T0～T3 の期間に生成された解析結果スナップショット、すなわち、同図の例では T2 の時点で生成された解析結果スナップショット（図 10 の説明において「スナップショット T2」という）が、更新の対象となる。従って、監視コンピュータ 1 は、スナップショット T2 が示す確信度のうちのイベント 4 を条件イベントに含むルール、すなわちルール 2 の確信度を、

イベント4の検知が考慮された値に更新する。つまり、スナップショットT2におけるルール2の確信度が、66%から100% ($3/3 \times 100\%$) に更新される。

[0072] また、監視コンピュータ1は、T31の時点において、ポートが正常であることを示すステータスレスポンス（図10の説明において「レスポンス（3）」という）をスイッチ「Switch C」から受信し、イベント3が発生していないことを認識している。ここで、レスポンス（3）に対応するステータスリクエストは、T0の時点で送信されているため、T0～T31の期間に生成された解析結果スナップショット、すなわち、同図の例ではスナップショットT2が、更新の対象となる。従って、監視コンピュータ1は、スナップショットT2が示す確信度のうちのイベント3を結論イベントとするルール、すなわちルール1の確信度を、0%に更新する。

[0073] 管理者は、更新されたスナップショットT2が示す確信度を参照することで、ルール2の結論イベント、すなわちイベント4が原因であると判断することができる。このように、管理者は、確信度計算処理によって得られる確信度に加えて、解析結果スナップショットが示す確信度を参照することで、より正確に原因を特定できるようになる。

[0074] 図11は、実施形態に係る解析結果スナップショットの更新対象範囲の一例を示す図である。

[0075] 同図において、矢印p1は、直近に行われたリクエスト送信処理におけるステータスリクエストの送信からステータスレスポンスの受信までの期間を示している。すなわち、直近に行われたリクエスト送信処理では、監視コンピュータ1は、t7の時点でステータスリクエストを送信し、t8の時点でステータスレスポンスを受信している。t8の時点で受信したステータスレスポンス、すなわち直近のステータスレスポンス（図11の説明において「レスポンスp1」という）は、異常のステータスを示している。また、矢印p2は、前回行われたリクエスト送信処理におけるステータスリクエストの送信からステータスレスポンスの受信までの期間を示している。すなわち、

前回行われたリクエスト送信処理では、監視コンピュータ 1 は、 t_5 の時点でステータスリクエストを送信し、 t_6 の時点でステータスレスポンスを受信している。 t_6 の時点で受信したステータスレスポンス、すなわち前回のステータスレスポンス（図 11 の説明において「レスポンス p 2」という）は、正常のステータスを示している。

[0076] このように、レスポンス p 1 が示すステータスが、レスポンス p 2 が示すステータスから変更されている場合、前回のステータスリクエスト（ t_5 の時点で送信されたステータスリクエストのことであり、図 11 の説明において「リクエスト p 2」という）が送信されてからレスポンス p 1 を受信するまでの期間、すなわち $t_5 \sim t_8$ の期間（ t_5 及び t_8 を除く）内のいずれかの時点で、ステータスが変更されたことになる。すなわち、ステータスの変更時点は、監視コンピュータ 1 がレスポンス p 2 を受信してからその後レスポンス p 1 を受信するまでの期間、すなわち $t_6 \sim t_8$ の期間内の時点には限られず、 $t_5 \sim t_6$ の期間内の時点（ t_5 を除く）である可能性もある。これは、ステータスレスポンスがノード装置によって送信される時点とそのステータスレスポンスが監視コンピュータ 1 によって受信される時点とに時間的なずれがあるからであり、具体的には、レスポンス p 2 が、 $t_5 \sim t_6$ のどの時点で送信されたか、すなわち $t_5 \sim t_6$ のどの時点のステータスを示しているかが不明だからである。例えば、 t_5 を経過した後すぐにレスポンス p 2 が送信され、その後すぐにステータスが異常に変更されていた可能性もある。この場合、 $t_5 \sim t_6$ の期間の大部分においてステータスが異常となっていたことになる。このような場合を考慮すると、 $t_5 \sim t_6$ の期間に生成され、レスポンス p 2 に基づいて更新された解析結果スナップショットが示す解析結果が正確でなかった可能性がある。そこで、本実施形態に係る監視コンピュータ 1 は、リクエスト p 2（前回のステータスリクエスト）の送信日時からレスポンス p 1（直近のステータスレスポンス）の受信日時までの期間、すなわち $t_5 \sim t_8$ の期間（ t_5 及び t_8 を除く）に生成された解析結果スナップショットを、レスポンス p 1 に基づく更新の対象とす

る。

[0077] また、監視コンピュータ 1 は、解析結果スナップショットを更新する際に、条件イベントに設定された重み値を参照する。本実施形態において、重み値は、0%～100%の範囲内の値をとる。重み値 0%は、その重み値が設定されている条件イベントが発生していないこと、すなわち、その条件イベントに関係するノード装置のステータスが正常であることを示している。また、重み値 100%は、その重み値が設定されている条件イベントが発生していること、すなわち、その条件イベントに関係するノード装置のステータスが異常となっていることを示している。監視コンピュータ 1 は、例えば、ステータスレスポンスを受信した場合に、受信したステータスレスポンスに含まれるステータス情報に基づいて、更新対象の解析結果スナップショットに関係する条件イベントのうちの、そのステータスレスポンスを送信したノード装置に関する条件イベントに、重み値を設定する。ここで、解析結果スナップショットに関係する条件イベントとは、解析結果スナップショットが示す確信度に対応する展開ルール 62（解析結果スナップショットに関する展開ルール 62）に含まれる条件イベントのことである。

[0078] 図 11 に示すように、レスポンス p 1 が示すステータスが、レスポンス p 2 が示すステータスから変更されている場合、t 5～t 8の期間（t 5及びt 8を除く）のどの時点でステータスが変更されたかが不明となる。すなわち、監視コンピュータ 1 は、レスポンス p 1 及びレスポンス p 2 を送信したノード装置のステータスが、t 5～t 8の期間において正常となっていたか異常となっていたかを特定することができない。そこで、監視コンピュータ 1 は、レスポンス p 1 が示すステータスが、レスポンス p 2 が示すステータスから変更されている場合、更新対象の解析結果スナップショットに関係する条件イベントのうちの、レスポンス p 1 及びレスポンス p 2 を送信したノード装置に関する条件イベントに、ステータスが正常であることを示す重み値（0%）とステータスが異常であることを示す重み値（100%）との中間値である 50%の重み値を設定する。なお、更新対象の解析結果スナップ

ショットは、リクエスト p 2 の送信日時からレスポンス p 1 の受信日時までの期間、すなわち t 5 ～ t 8 の期間（t 5 及び t 8 を除く）に生成された解析結果スナップショットである。

[0079] 図 1 2 A は、実施形態に係る条件テーブルの第 1 の例を示す図である。図 1 2 B は、実施形態に係る条件テーブルの第 2 の例を示す図である。

[0080] 条件テーブル 1 3 7 は、解析結果スナップショットごとに、当該解析結果スナップショットに関係する条件イベントと、その条件イベントに設定された重み値とを管理するためのデータである。条件テーブル 1 3 7 は、スナップショット I D 1 3 7 1、根本原因 1 3 7 2、展開ルール 1 3 7 3、ステータス管理 I D 1 3 7 4、N o t 条件 1 3 7 5、及び重み付け 1 3 7 6 のフィールドを含む。

[0081] スナップショット I D 1 3 7 1 には、解析結果スナップショットの識別子（以下「スナップショット I D」という）が格納される。根本原因 1 3 7 2 には、スナップショット I D 1 3 7 1 のスナップショット I D によって示される解析結果スナップショット（図 1 2 の説明において「対象スナップショット」という）に関係する展開ルール 6 2 に含まれる結論イベントを示すデータが格納される。展開ルール 1 3 7 3 には、対象スナップショットに関係する展開ルール 6 2 の名称が格納される。ステータス管理 I D 1 3 7 4 には、対象スナップショットに関係する条件イベントを示すデータが格納される。本実施形態では、条件イベントを示すデータとして、図 6 のステータス管理テーブル 1 3 4 のエントリの識別子（ステータス管理 I D）が採用される。すなわち、ステータス管理 I D 1 3 7 4 には、対象スナップショットに関係する条件イベントに対応するステータスを管理しているステータス管理テーブル 1 3 4 のエントリのステータス管理 I D が格納される。N o t 条件 1 3 7 5 には、解析結果スナップショットの確信度を再計算する際に参照されるデータ、例えば「T r u e」又は「F a l s e」が格納される。N o t 条件 1 3 7 5 の値「T r u e」は、ステータス管理 I D 1 3 7 4 のステータス管理 I D によって示される条件イベント（図 1 2 の説明において「対象条件

イベント」という) が検知された場合に確信度が下がることを示している。Not 条件 1375 の値「False」は、対象条件イベントが検知された場合に確信度が上がることを示している。なお、本実施形態において、Not 条件 1375 の値は、全て「False」である。重み付け 1376 には、対象スナップショットにおいて対象条件イベントに設定されている重み値が格納される。

[0082] 図 12A は、図 10 の T2 の時点における条件テーブル 137 を示している。例えば、同図の上から 1～6 番目のエントリから、スナップショット ID が「0001」の解析結果スナップショット（以下「スナップショット 1」という）は、ルール 1 及びルール 2 に関する解析結果を示しており、スナップショット 1 に関係する条件イベントとして、「1」～「4」のステータス ID によって示される 4 つの条件イベント、すなわち、イベント 1、イベント 2、イベント 3、及びイベント 4 があることがわかる。また、同図の上から 1 番目のエントリから、T2 の時点において、スナップショット 1 におけるイベント 1 には、イベント 1 が発生していることを示す 100% の重み値が設定されていることがわかる。また、同図の上から 3 番目及び 5 番目のエントリから、T2 の時点において、スナップショット 1 におけるイベント 4 及びイベント 3 には未だ重み値が設定されていないこと、すなわち、監視コンピュータ 1 が未だイベント 4 に関係するステータスレスポンス及びイベント 3 に関係するステータスレスポンスを受信していないことがわかる。

[0083] 図 12B は、図 10 の T4 の時点における条件テーブル 137 を示している。同図の上から 3 番目のエントリからわかるように、T4 の時点において、スナップショット 1 におけるイベント 4 には、イベント 4 が発生していることを示す 100% の重み値が設定されている。図 12A 及び図 12B を比較するとわかるように、スナップショット 1 におけるイベント 4 の重み値が、未設定から 100% に変更されている。これは、監視コンピュータ 1 が、図 10 の T3 の時点において、レスポンス (4) を受信してイベント 4 の発生を検知し、そのことに基づいて、スナップショット 1 におけるイベント 4

の重み値を100%に変更したことによる。また、同図の上から5番目のエントリは、T4の時点において、スナップショット1におけるイベント3には、イベント3が発生していないことを示す0%の重み値が設定されている。図12A及び図12Bを比較するとわかるように、スナップショット1におけるイベント3の重み値が、未設定から0%に変更されている。これは、監視コンピュータ1が、図10のT31の時点において、レスポンス(3)を受信してイベント3が発生していないことを認識し、そのことに基づいて、スナップショット1におけるイベント3の重み値を0%に変更したことによる。

[0084] 図13Aは、実施形態に係る展開ルールテーブルの第1の例を示す図である。図13Bは、実施形態に係る展開ルールテーブルの第2の例を示す図である。

[0085] 展開ルールテーブル138は、解析結果スナップショットごとに、当該解析結果スナップショットに関する展開ルール62と、その展開ルール62に関する確信度とを管理するためのデータである。展開ルールテーブル138は、スナップショットID1381、根本原因1382、展開ルール1383、条件イベント数1384、及び確信度1385のフィールドを含む。

[0086] スナップショットID1381には、スナップショットIDが格納される。根本原因1382には、スナップショットID1381のスナップショットIDによって示される解析結果スナップショット(図13の説明において「対象スナップショット」という)に関する展開ルール62に含まれる結論イベントを示すデータが格納される。展開ルール1383には、対象スナップショットに関する展開ルール62の名称が格納される。条件イベント数1384には、展開ルール1383によって示される展開ルール62に含まれる条件イベントの総数が格納される。確信度1385には、展開ルール1383によって示される展開ルール62の、対象スナップショットにおける確信度が格納される。

[0087] 図13Aは、図10のT2の時点における展開ルールテーブル138の具

体例を示している。例えば、同図の上から1番目のエントリから、スナップショット1に関する展開ルール62であるルール2は3つの条件イベントを含んでおり、T2の時点において、スナップショット1におけるルール2の確信度は66%であることがわかる。また、同図の上から2番目のエントリから、スナップショット1に関する展開ルール62であるルール1は3つの条件イベントを含んでおり、T2の時点において、スナップショット1におけるルール1の確信度は66%であることがわかる。

[0088] 図13Bは、図10のT4の時点における展開ルールテーブル138の具体例を示している。同図の上から1番目のエントリからわかるように、T4の時点において、スナップショット1におけるルール2の確信度は100%となっている。図13A及び図13Bを比較するとわかるように、スナップショット1におけるルール2の確信度が、66%から100%に変更されている。これは、監視コンピュータ1が、図10のT3の時点においてイベント4の発生を検知し、そのことに基づいて、スナップショット1におけるルール2の確信度を、イベント4の検知が考慮された値に変更したことによる。また、同図の上から2番目のエントリからわかるように、T4の時点において、スナップショット1におけるルール1の確信度は0%となっている。図13A及び図13Bを比較するとわかるように、スナップショット1におけるルール1の確信度が、66%から0%に変更されている。これは、監視コンピュータ1が、図10のT3の時点において、ルール1の結論イベントであるイベント3が発生していないことを認識し、そのことに基づいて、スナップショット1におけるルール1の確信度を0%に変更したことによる。

[0089] 図14Aは、実施形態に係るスナップショットテーブルの第1の例を示す図である。図14Bは、実施形態に係るスナップショットテーブルの第2の例を示す図である。

[0090] スナップショットテーブル139は、解析結果スナップショットに関する情報を管理するためのデータである。スナップショットテーブル139は、

スナップショットID 1391、根本原因1392、確信度1393、スナップショット化した日時1394、及び更新日時1395のフィールドを含む。

[0091] スナップショットID 1391には、スナップショットIDが格納される。根本原因1392には、スナップショットID 1391のスナップショットIDによって示される解析結果スナップショット（図14の説明において「対象スナップショット」という）に関係する展開ルール62に含まれる結論イベントを示すデータが格納される。確信度1393には、根本原因1392によって示される結論イベントを含む展開ルール62の、対象スナップショットにおける確信度が格納される。スナップショット化した日時1394には、対象スナップショットが生成された日時（生成日時）を示すデータが格納される。更新日時1395には、対象スナップショットが更新された日時（更新日時）を示すデータが格納される。例えば、対象スナップショットが複数回更新された場合は、更新日時1395には、最新の更新が行われた日時を示すデータが格納される。本実施形態において、対象スナップショットが一度も更新されていない場合、更新日時1395には、対象スナップショットの生成日時を示すデータが格納される。

[0092] 図14Aは、図10のT2の時点におけるスナップショットテーブル139の具体例を示している。例えば、同図の上から1番目のエントリから、T2の時点において、イベント4を結論イベントとする展開ルール62（ルール2）の、スナップショット1における確信度が66%であることがわかる。また、同エントリから、スナップショット1は、2008年4月20日の9時30分11秒に生成され、一度も更新されていないことがわかる。また、同図の上から2番目のエントリから、T2の時点において、イベント3を結論イベントとする展開ルール62（ルール1）の、スナップショット1における確信度が66%であることがわかる。また、同エントリからも、スナップショット1が、2008年4月20日の9時30分11秒に生成され、一度も更新されていないことがわかる。

[0093] 図14Bは、図10のT4の時点におけるスナップショットテーブル139の具体例を示している。例えば、同図の上から1番目のエントリからわかるように、T4の時点において、イベント4を結論イベントとする展開ルール62（ルール2）の、スナップショット1における確信度が100%となっている。これは、監視コンピュータ1が、図10のT3の時点においてイベント4の発生を検知し、そのことに基づいてスナップショット1におけるルール2の確信度を更新したことによる。同エントリから、2008年4月20日の9時41分11秒に、スナップショット1におけるルール2の確信度が更新されたことがわかる。また、同図の上から2番目のエントリからわかるように、T4の時点において、イベント3を結論イベントとする展開ルール62（ルール1）の、スナップショット1における確信度が0%となっている。これは、監視コンピュータ1が、図10のT3の時点においてイベント3が発生していないことを認識し、そのことに基づいてスナップショット1におけるルール1の確信度を更新したことによる。同エントリから、2008年4月20日の9時46分11秒に、スナップショット1におけるルール1の確信度が更新されたことがわかる。

[0094] 図15は、実施形態に係るスナップショット表示管理テーブルの一例の構成図である。

[0095] スナップショット表示管理テーブル130は、解析結果スナップショットごとに、当該解析結果スナップショットの前回表示日時を管理するためのデータである。ここで、解析結果スナップショットの前回表示日時とは、その解析結果スナップショットが示す解析結果が、後述するスナップショット表示画面（図23参照）において表示され、管理者によって参照された日時のうちの直近の日時のことをいう。なお、スナップショット表示画面は、解析結果スナップショットが示す解析結果を表示するための画面である。スナップショット表示管理テーブル130は、スナップショットID1301、及び前回表示日時1302のフィールドを含む。スナップショットID1301には、スナップショットIDが格納される。前回表示日時1302には、

スナップショット I D 1 3 0 1 によって示される解析結果スナップショットの前回表示日時を示すデータが格納される。例えば、同図の上から 1 番目のエントリから、スナップショット 1 の前回表示日時は 2 0 0 8 年 4 月 2 0 日の 9 時 3 5 分 1 1 秒であることがわかる。

[0096] 次に、監視コンピュータ 1 の動作について説明する。

[0097] 図 1 6 は、実施形態に係るルール展開処理のフローチャートである。

[0098] ルール展開処理は、汎用ルール 6 1 及び構成情報 1 3 1 に基づいてルールメモリデータ 8 を生成する処理である。

[0099] まず、ルール展開プログラム 1 2 1 は、計算機システムの複数のノード装置から構成情報 1 3 1 を構成する種々の情報を取得し、取得した情報に基づいて構成情報 1 3 1 を生成又は更新する（ステップ S 1 0 1）。

[0100] 次に、ルール展開プログラム 1 2 1 は、汎用ルール 6 1 及び構成情報 1 3 1 に基づいて展開ルール 6 2 を生成する（ステップ S 1 0 2）。

[0101] 次に、ルール展開プログラム 1 2 1 は、ステップ S 1 0 2 で生成した展開ルール 6 2 に基づいてルールメモリデータ 8 を生成する（ステップ S 1 0 3）。

[0102] その後、ルール展開プログラム 1 2 1 は、ステップ S 1 0 3 で生成したルールメモリデータ 8 をルールメモリ 1 2 8 に格納する（ステップ S 1 0 4）。その後、ルール展開プログラム 1 2 1 は、ルール展開処理を終了する。

[0103] 図 1 7 は、実施形態に係るリクエスト送信処理のフローチャートである。

[0104] リクエスト送信処理は、監視コンピュータ 1 が、定期的又は不定期的に、監視対象装置に対してステータスリクエストを送信し、監視対象装置又はそのコンポーネントに関するステータス情報を監視対象装置から取得する処理である。

[0105] まず、リクエスト送信プログラム 1 2 2 は、ポーリング管理テーブル 1 3 3 におけるリクエスト送信日時 1 3 3 2 に「-」が格納されている監視対象装置、すなわち前回送信したステータスリクエストに対するステータスレスポンスを既に受信している監視対象装置に対して、ステータスリクエストを

送信する（ステップS 2 0 1）。

[0106] 次に、リクエスト送信プログラム 1 2 2 は、ポーリング管理テーブル 1 3 3 において、ステップS 2 0 1 でステータスリクエストを送信した監視対象装置に関するエントリのリクエスト送信日時 1 3 3 2 に、ステップS 2 0 1 において送信したステータスリクエストの送信日時、例えば現在の日時を示すデータを格納する（ステップS 2 0 2）。

[0107] その後、リクエスト送信プログラム 1 2 2 は、監視対象装置からステータスレスポンスを受信するまで待機する（ステップS 2 0 3）。リクエスト送信プログラム 1 2 2 は、監視対象装置からステータスレスポンスを受信した場合、処理をステップS 2 0 4 へ進める。以下、ステップS 2 0 3 で受信したステータスレスポンスを「受信レスポンス」と呼び、受信レスポンスを送信した監視対象装置を「対象ノード装置」と呼ぶ。

[0108] ステップS 2 0 4 において、リクエスト送信プログラム 1 2 2 は、受信レスポンスに含まれるステータス情報に基づいて、ステータス管理テーブル 1 3 4 における対象のデータを更新する。

[0109] 具体的には、まず、リクエスト送信プログラム 1 2 2 は、対象ノード装置、受信レスポンスに含まれるステータス情報が示すステータスに関するコンポーネント、及び受信レスポンスに含まれるステータス情報が示すステータスが異常となることに対応するイベントの種別に関するエントリ（以下「対象ステータスエントリ」という）を特定する。そして、リクエスト送信プログラム 1 2 2 は、対象ステータスエントリの最新のステータス 1 3 4 8 及び最新の情報収集プロセス開始日時 1 3 4 0 に格納されているデータを、それぞれ前回のステータス 1 3 4 a 及び前回の情報収集プロセス開始日時 1 3 4 b に移動又はコピーする。その後、リクエスト送信プログラム 1 2 2 は、対象ステータスエントリの最新のステータス 1 3 4 8 に、受信レスポンスに含まれるステータス情報を格納し、対象ステータスエントリの最新の情報収集プロセスのイベント受信日時 1 3 4 9 に、受信レスポンスを受信した日時を示すデータを格納し、対象ステータスエントリの最新の情報収集プロセス

開始日時 1 3 4 0 に、受信レスポンスを要求したステータスリクエストの送信日時を示すデータを格納する。ここで、受信レスポンスを要求したステータスリクエストの送信日時は、ポーリング管理テーブル 1 3 3 における対象ノード装置に関するエントリのリクエスト送信日時 1 3 3 2 によって示される送信日時である。

[0110] その後、イベント検知プログラム 1 2 3 は、対象ステータスエントリの最新のステータス 1 3 4 8 が示すステータス（以下「対象最新ステータス」という）と、対象ステータスエントリの前回のステータス 1 3 4 a が示すステータス（以下「対象前回ステータス」という）とが異なるか否かを判定する（ステップ S 2 0 5）。対象最新ステータスと対象前回ステータスとが異なる場合（ステップ S 2 0 5 : Y E S）、イベント検知プログラム 1 2 3 は、処理をステップ S 2 0 6 へ進める。一方、対象最新ステータスと対象前回ステータスとが同じである場合（ステップ S 2 0 5 : N O）、イベント検知プログラム 1 2 3 は、処理をステップ S 2 1 2 へ進める。

[0111] ステップ S 2 0 6 において、イベント検知プログラム 1 2 3 は、ステータスが正常から異常に変化したか否か、すなわち、対象前回ステータスが正常であり且つ対象最新ステータスが異常であるか否かを判定する。

[0112] ステータスが正常から異常に変化している場合、すなわち、対象前回ステータスが正常であり且つ対象最新ステータスが異常である場合（ステップ S 2 0 6 : Y E S）は、対象ノード装置に関するイベントであって対象ステータスエントリのイベント種別 1 3 4 7 によって示されるイベント（以下「対象イベント」という）の発生が検知されたことを意味する。この場合、イベント検知プログラム 1 2 3 は、ルールメモリデータ 8 において、対象イベントに対応する条件オブジェクト 8 1 を特定し、特定した条件オブジェクト 8 1 の R e c e i v e d 8 1 6 に、対象イベントの検知日時、例えば受信レスポンスを受信した日時を示すデータを格納する（ステップ S 2 0 7）。

[0113] その後、イベント検知プログラム 1 2 3 は、確信度計算プログラム 1 2 4 に確信度計算処理（図 1 8 参照）を実行させる（ステップ S 2 0 8）。確信

度計算処理を実行させる際、イベント検知プログラム１２３は、ステップＳ２０７で特定した条件オブジェクト８１を指定するパラメータを、確信度計算プログラム１２４に入力する。この確信度計算処理により、対象イベントに対応付けられている各結論イベントについて、確信度が計算される。

[0114] その後、イベント検知プログラム１２３は、イベント失効タスク生成プログラム１２６にイベント失効タスク生成処理（図２０参照）を実行させる（ステップＳ２０９）。イベント失効タスク生成処理を実行させる際、イベント検知プログラム１２３は、ステップＳ２０７で特定した条件オブジェクト８１を指定するパラメータを、イベント失効タスク生成プログラム１２６に入力する。このイベント失効タスク生成処理により、対象イベントについてのイベント失効タスクが生成される。その後、イベント検知プログラム１２３は、処理をステップＳ２１２へ進める。

[0115] ステップＳ２０６の判定において、ステータスが異常から正常に変化している場合、すなわち、対象前回ステータスが異常であり且つ対象最新ステータスが正常である場合（ステップＳ２０６：ＮＯ）は、対象イベントが発生していないことが監視コンピュータ１によって認識されたことを意味する。この場合、イベント検知プログラム１２３は、ルールメモリデータ８において、対象イベントに対応する条件オブジェクト８１を特定し、特定した条件オブジェクト８１のReceived 816に格納されているデータをクリアする（ステップＳ２１０）。

[0116] その後、イベント検知プログラム１２３は、確信度計算プログラム１２４に確信度計算処理（図１８参照）を実行させる（ステップＳ２１１）。確信度計算処理を実行させる際、イベント検知プログラム１２３は、ステップＳ２１０で特定した条件オブジェクト８１を指定するパラメータを、確信度計算プログラム１２４に入力する。この確信度計算処理により、対象イベントに対応付けられている各結論イベントについて、確信度が計算される。その後、イベント検知プログラム１２３は、処理をステップＳ２１２へ進める。

[0117] ステップＳ２１２において、イベント検知プログラム１２３は、スナップ

ショット再計算プログラム 125 にスナップショット再計算処理（図 19 参照）を実行させる。スナップショット再計算処理を実行させる際、イベント検知プログラム 123 は、対象ステータスエントリを指定するパラメータを、スナップショット再計算プログラム 125 に入力する。このスナップショット再計算処理により、更新対象の解析結果スナップショットが示す確信度のうちの、対象イベントを条件イベント又は結論イベントとして含む展開ルール 62 の確信度が再計算される。

[0118] その後、リクエスト送信プログラム 122 は、ポーリング管理テーブル 133 における対象ノード装置に関するエントリのリクエスト送信日時 1332 に、対象ノード装置からステータスレスポンスを受信したことを示すデータ、すなわち「-」を格納する（ステップ S213）。

[0119] その後、リクエスト送信プログラム 122 は、一定時間待機し（ステップ S214）、一定時間が経過した後に再度リクエスト送信処理を行う。

[0120] 図 18 は、実施形態に係る確信度計算処理のフローチャートである。

[0121] 確信度計算処理は、ルールメモリデータ 8 に基づいて、入力された条件オブジェクト 81 に接続されている各結論オブジェクト 82 について、その結論イベントの確信度を計算する処理である。確信度計算処理は、図 17 におけるステップ S208 若しくはステップ S211 の処理又は図 21 におけるステップ S607 の処理に対応する。

[0122] まず、確信度計算プログラム 124 は、確信度計算処理を実行させたイベント検知プログラム 123 又はイベント消去プログラム 127 によって入力されたパラメータを受信する（ステップ S301）。

[0123] 次に、確信度計算プログラム 124 は、入力されたパラメータによって指定される条件オブジェクト 81 に接続されている演算子オブジェクト 83 を、ルールメモリデータ 8 から取得する（ステップ S302）。

[0124] 次に、確信度計算プログラム 124 は、ステップ S302 において取得した演算子オブジェクト 83 に接続されている結論オブジェクト 82 を、ルールメモリデータ 8 から取得する（ステップ S303）。

- [0125] その後、確信度計算プログラム124は、ステップS303において取得した結論オブジェクト82のそれぞれに対して、ステップS305の処理を行う（ステップS304～S306）。図18の説明において、ステップS303において取得された結論オブジェクト82のうちの処理対象の結論オブジェクト82を「対象結論オブジェクト」と呼び、対象結論オブジェクトに対応する結論イベントを「対象結論イベント」と呼ぶ。
- [0126] ステップS305において、確信度計算プログラム124は、対象結論イベントについての確信度を計算する。本実施形態において、結論イベントについての確信度は、当該結論イベントに対応付けられている条件イベントの総数に対する、当該結論イベントに対応付けられている条件イベントのうちの監視コンピュータ1が検知した条件イベントの数の割合である。例えば、確信度計算プログラム124は、対象結論オブジェクト82に接続されている条件オブジェクト81のうちのReceived816に検知日時が格納されている条件オブジェクト81の数を、対象結論オブジェクト82に接続されている条件オブジェクト81の総数で除算し、除算して得られた値に100を乗算することにより、対象結論イベントについての確信度を計算する。その後、確信度計算プログラム124は、計算した確信度を、対象結論オブジェクトのMR824に格納する。
- [0127] その後、一定時間経過後、確信度計算プログラム124は、その時点における解析結果スナップショットを生成し、生成した解析結果スナップショットを記憶資源12に保存する（ステップS307）。
- [0128] 具体的には、確信度計算プログラム124は、例えばステップS304～ステップS306で計算した複数の確信度のそれぞれに関する、スナップショットテーブル139のエントリを作成し、作成したエントリ（以下「作成スナップショットエントリ」という）をスナップショットテーブル139に追加する。例えば、作成スナップショットエントリのスナップショットID1391には、このステップS307で生成される解析結果スナップショット（以下「生成スナップショット」という）に割り当てられたスナップショ

ットIDが格納される。また、作成スナップショットエントリの根本原因1392には、当該エントリが示す確信度に関する結論イベントを示すデータが格納される。また、作成スナップショットエントリの確信度1393には、当該エントリが示す確信度が格納される。また、作成スナップショットエントリのスナップショット化した日時1394には、生成スナップショットの生成日時、例えば現在の日時を示すデータが格納される。

[0129] また、確信度計算プログラム124は、例えばステップS304～ステップS306で計算した複数の確信度のそれぞれに関する展開ルール62についての、展開ルールテーブル138のエントリを作成し、作成したエントリ（以下「作成ルールエントリ」という）を展開ルールテーブル138に追加する。例えば、作成ルールエントリのスナップショットID1381には、生成スナップショットに割り当てられたスナップショットIDが格納される。また、作成ルールエントリの根本原因1382には、当該エントリが示す展開ルール62に含まれる結論イベントを示すデータが格納される。また、作成ルールエントリの展開ルール1383には、当該エントリが示す展開ルール62の名称が格納される。また、作成ルールエントリの条件イベント数1384には、当該エントリが示す展開ルール62に含まれる条件イベントの総数が格納される。また、作成ルールエントリの確信度1385には、当該エントリが示す展開ルール62に関する、ステップS305において計算された確信度が格納される。

[0130] また、例えば、確信度計算プログラム124は、作成ルールエントリが示す展開ルール62に含まれる各条件イベントについての、条件テーブル137のエントリを作成し、作成したエントリ（以下「作成条件エントリ」という）を条件テーブル137に追加する。例えば、作成条件エントリのスナップショットID1371には、生成スナップショットに割り当てられたスナップショットIDが格納される。また、作成条件エントリの根本原因1372には、作成ルールエントリが示す展開ルール62に含まれる結論イベントを示すデータが格納される。また、作成条件エントリの展開ルール1373

には、作成ルールエントリが示す展開ルール 62 の名称が格納される。また、作成条件エントリのステータス管理 ID 1374 には、作成条件エントリが示す条件イベントを示すデータが格納される。また、作成条件エントリの重み付け 1376 には、作成条件エントリが示す条件イベントに設定された重み値が格納される。例えば、監視コンピュータ 1 が、作成条件エントリが示す条件イベントに対応するステータスを示すステータスレスポンスを既に受信しており、そのステータスレスポンスが正常のステータスを示している場合は、作成条件エントリの重み付け 1376 には、0 [%] が格納される。また、監視コンピュータ 1 が、作成条件エントリが示す条件イベントに対応するステータスを示すステータスレスポンスを既に受信しており、そのステータスレスポンスが異常のステータスを示している場合は、作成条件エントリの重み付け 1376 には、100 [%] が格納される。一方、監視コンピュータ 1 が、作成条件エントリが示す条件イベントに対応するステータスを示すステータスレスポンスを未だ受信していない場合は、作成条件エントリの重み付け 1376 には、重み値が未だ設定されていないことを示すデータ、例えば「-」が格納される。

[0131] その後、確信度計算プログラム 124 は、確信度計算処理を終了する。

[0132] なお、本実施形態では、監視コンピュータ 1 は、確信度計算処理において確信度が計算された後に、解析結果スナップショットを生成している。すなわち、監視コンピュータ 1 は、リクエスト送信処理において受信レスポンスが示すステータスが前回から変更されていることを認識した都度、及びイベント消去処理においてイベントの検知を無効とした都度、解析結果スナップショットを生成している。しかし、解析結果スナップショットを生成するタイミングは、図 18 が示すタイミングに限定されない。上述したように、イベントを受信してから一定時間経過後に解析結果スナップショットが生成されてもよいし、リクエスト送信処理におけるステータスリクエストの送信周期に基づいて、解析結果スナップショットを生成するタイミングが決定されてもよい。また、確信度計算処理において確信度が計算された後に解析結果

スナップショットを生成する場合において、監視コンピュータ 1 は、例えば、複数回行われる確信度計算処理のうちのいずれかにおいてだけ、解析結果スナップショットを生成するようにしてもよい。

[0133] 図 19 は、実施形態に係るスナップショット再計算処理のフローチャートである。

[0134] スナップショット再計算処理は、受信したステータスレスポンスに基づいて更新対象の解析結果スナップショットが示す確信度を再計算する処理である。スナップショット再計算処理は、図 17 におけるステップ S 2 1 2 の処理に対応する。

[0135] まず、スナップショット再計算プログラム 125 は、スナップショット再計算処理を実行させたイベント検知プログラム 123 によって入力されたパラメータ、すなわち対象ステータスエントリを指定するパラメータを受信する（ステップ S 4 0 1）。

[0136] スナップショット再計算プログラム 125 は、更新対象の解析結果スナップショットのそれぞれに対して、ステップ S 4 0 2～ステップ S 4 1 4 の処理を行う。ここで、更新対象の解析結果スナップショットは、対象ステータスエントリの前回の情報収集プロセス開始日時 134 b によって示される日時、すなわち対象ノード装置に対する前回のステータスリクエストの送信日時よりも後、且つ、対象ステータスエントリの最新の情報収集プロセスのイベント受信日時 134 9 によって示される日時、すなわち対象ノード装置から受信レスポンス（直近のステータスレスポンス）を受信した日時よりも前に生成された解析結果スナップショットである。図 19 の説明において、更新対象の解析結果スナップショットのうちの処理対象の解析結果スナップショットを「対象スナップショット」と呼ぶ。

[0137] スナップショット再計算プログラム 125 は、条件テーブル 137 における対象スナップショット及び対象イベントに関するエントリのそれぞれに対して、ステップ S 4 0 3～ステップ S 4 1 3 の処理を行う。図 19 の説明において、条件テーブル 137 における対象スナップショット及び対象イベン

トに関するエントリのうちの処理対象のエントリを「対象条件エントリ」と呼ぶ。

- [0138] ステップS404において、スナップショット再計算プログラム125は、対象条件エントリの重み付け1376に格納されている重み値（以下「以前の重み値」という）を記憶資源12の所定の個所にコピーする。そして、スナップショット再計算プログラム125は、対象最新ステータス及び対象前回ステータスをチェックする。
- [0139] 対象最新ステータス及び対象前回ステータスがいずれも正常である場合（ステップS404：全てNormal）、スナップショット再計算プログラム125は、対象条件エントリの重み付け1376に0 [%] を格納する（ステップS405）。すなわち、スナップショット再計算プログラム125は、受信レスポンスが示すステータスが、前回のステータスレスポンスが示すステータスから正常のまま変更されていない場合は、更新対象の解析結果スナップショットにおける対象イベントに、対象イベントが発生していないことを示す0 %の重み値を設定する。
- [0140] 一方、対象最新ステータス及び対象前回ステータスがいずれも異常である場合（ステップS404：全てError）、スナップショット再計算プログラム125は、対象条件エントリの重み付け1376に100 [%] を格納する（ステップS407）。すなわち、スナップショット再計算プログラム125は、受信レスポンスが示すステータスが、前回のステータスレスポンスが示すステータスから異常のまま変更されていない場合は、更新対象の解析結果スナップショットにおける対象イベントに、対象イベントが発生していることを示す100 %の重み値を設定する。
- [0141] 一方、対象最新ステータス及び対象前回ステータスのうちのいずれか一方が正常であり他方が異常である場合（ステップS404：NormalとError）、スナップショット再計算プログラム125は、対象条件エントリの重み付け1376に50 [%] を格納する（ステップS406）。すなわち、スナップショット再計算プログラム125は、受信レスポンスが示す

ステータスが、前回のステータスレスポンスが示すステータスから変更されている場合は、更新対象の解析結果スナップショットにおける対象イベントに、50%の重み値を設定する。

[0142] その後、スナップショット再計算プログラム125は、対象条件エントリの展開ルール1373によって示される展開ルール62（以下「対象展開ルール」という）に対して、ステップS408～ステップS412の処理を行う。ここで、対象展開ルールは、対象スナップショットに関する展開ルール62のうちの、ステップS405、ステップS406又はステップS407において重み値が設定された条件イベントを含む展開ルール62を意味している。

[0143] ステップS409において、スナップショット再計算プログラム125は、対象展開ルールに関する確信度を再計算し、再計算によって得られた確信度（以下「更新後の確信度」という）を、展開ルールテーブル138における対象展開ルールに関するエントリの確信度1385に格納する。

[0144] 例えば、スナップショット再計算プログラム125は、次のように確信度を再計算する。すなわち、スナップショット再計算プログラム125は、まず、展開ルールテーブル138における対象展開ルールに関するエントリの確信度1385から、対象展開ルールに関する再計算前の確信度（以下「更新前の確信度」という）を取得する。また、スナップショット再計算プログラム125は、展開ルールテーブル138における対象展開ルールに関するエントリの条件イベント数1384から、対象展開ルールに含まれる条件イベントの総数を取得する。また、スナップショット再計算プログラム125は、対象条件エントリの重み付け1376から、ステップS405、ステップS406又はステップS407において対象イベントに設定された重み値（以下「新しい重み値」という）を取得する。そして、スナップショット再計算プログラム125は、新しい重み値から以前の重み値を減算し、その減算によって得られた値を対象展開ルールに含まれる条件イベントの総数で除算し、その除算によって得られた値を更新前の確信度に加算することにより

、更新後の確信度を得る。なお、スナップショット再計算プログラム 125 は、確信度計算処理（図 18）のステップ S305 で行われる計算を再度行うことにより、すなわち、条件イベントの総数に対する監視コンピュータ 1 が検知した条件イベントの数の割合を再計算することにより、更新後の確信度を得てもよい。

[0145] その後、スナップショット再計算プログラム 125 は、更新後の確信度が、スナップショットテーブル 139 における対象スナップショット及び対象展開ルールに関するエントリ（以下「対象スナップショットエントリ」という）の確信度 1393 に格納されている確信度よりも大きいか否かを判定する（ステップ S410）。

[0146] 更新後の確信度が、対象スナップショットエントリの確信度 1393 に格納されている確信度よりも大きい場合（ステップ S410：YES）、スナップショット再計算プログラム 125 は、対象スナップショットエントリの確信度 1393 に、更新後の確信度を格納し、対象スナップショットエントリの更新日時 1395 に、対象スナップショットの更新日時、すなわち現在の日時を示すデータを格納する（ステップ S411）。一方、更新後の確信度が、対象スナップショットエントリの確信度 1393 に格納されている確信度よりも大きくない場合（ステップ S410：NO）、スナップショット再計算プログラム 125 は、処理をステップ S412 に進める。

[0147] スナップショット再計算プログラム 125 は、条件テーブル 137 における対象スナップショット及び対象イベントに関するエントリのそれぞれに対してステップ S403～ステップ S413 の処理を終え、更新対象の解析結果スナップショットのそれぞれに対してステップ S402～ステップ S414 の処理を終えた後、スナップショット再計算処理を終了する。

[0148] 図 20 は、実施形態に係るイベント失効タスク生成処理のフローチャートである。

[0149] イベント失効タスク生成処理は、入力された条件オブジェクト 81 に対応する条件イベントについてのイベント失効タスクを生成する処理である。

[0150] まず、イベント失効タスク生成プログラム 126 は、イベント失効タスク生成処理を実行させたイベント検知プログラム 123 によって入力されたパラメータを受信する（ステップ S501）。

[0151] 次に、イベント失効タスク生成プログラム 126 は、ステップ S501 で受信したパラメータによって指定される条件オブジェクト 81 に対応する条件イベント（つまり、対象イベント）についてのイベント失効タスクを生成する（ステップ S502）。具体的には、イベント失効タスク生成プログラム 126 は、対象イベントに関する、イベント失効タスクテーブル 136 のエントリを作成し、作成したエントリをイベント失効タスクテーブル 136 に追加する。作成したエントリのノード名 1362 には、対象ノード装置の名称が格納される。また、作成したエントリのイベント種別 1363 には、対象イベントの種別を示すデータが格納される。

[0152] 次に、イベント失効タスク生成プログラム 126 は、ステップ S502 で生成したイベント失効タスクのタスク開始日時を決定する（ステップ S503）。具体的には、イベント失効タスク生成プログラム 126 は、イベント有効期間設定テーブル 135 から、対象イベントに設定されている有効期間を取得する。そして、イベント失効タスク生成プログラム 126 は、対象イベントの検知日時に対象イベントに設定されている有効期間を加えた日時を、生成したイベント失効タスクのタスク開始日時と決定する。

[0153] その後、イベント失効タスク生成プログラム 126 は、ステップ S502 で追加したエントリの開始日時 1361 に、ステップ S503 で決定したタスク開始日時を示すデータを格納する（ステップ S504）。その後、イベント失効タスク生成プログラム 126 は、イベント失効タスク生成処理を終了する。

[0154] 図 21 は、実施形態に係るイベント消去処理のフローチャートである。

[0155] イベント消去処理は、有効期間が経過したイベントの検知を無効にする処理である。

[0156] まず、イベント消去プログラム 127 は、イベント失効タスクテーブル 1

36から、開始日時1361に格納されている日時が最も早いエントリを取得する（ステップS601）。図21の説明において、取得したエントリを「対象エントリ」といい、対象エントリに対応するイベント失効タスク、すなわち対象エントリによって情報が管理されるイベント失効タスクを「対象イベント失効タスク」という。

[0157] 次に、イベント消去プログラム127は、対象エントリの開始日時1361が示す日時、すなわち対象イベント失効タスクのタスク開始日時が、現在日時と同一であるか、又は現在日時よりも前であるか否かを判定する（ステップS602）。対象イベント失効タスクのタスク開始日時が現在日時よりも後である場合（ステップS602：NO）、イベント消去プログラム127は、一定時間待機し、その後再度イベント消去処理を行う。

[0158] 一方、対象イベント失効タスクのタスク開始日時が現在日時と同一であるか、又は現在日時よりも前である場合（ステップS602：YES）、イベント消去プログラム127は、対象エントリのノード名1362、及びイベント種別1363から、対象イベント失効タスクの対象となるイベント（以下「失効イベント」という）に関係するノード装置の名称、及び失効イベントの種別を示すデータを取得する（ステップS603）。

[0159] 次に、イベント消去プログラム127は、ルールメモリデータ8から、失効イベントに対応する条件オブジェクト81（図21の説明において「対象条件オブジェクト」という）を取得する（ステップS604）。具体的には、イベント消去プログラム127は、失効イベントに関係するノード装置の名称及び失効イベントの種別をキーにルールメモリデータ8を検索し、NodeName812及びEvent815が示すノード装置の名称及びイベントの種別がキーと一致する条件オブジェクト81を、対象条件オブジェクトとして特定する。

[0160] その後、イベント消去プログラム127は、対象条件オブジェクトのReceived816に格納されているデータをクリアする（ステップS605）。

- [0161] その後、イベント消去プログラム 127 は、イベント失効タスクテーブル 136 から対象エントリを削除する（ステップ S606）。
- [0162] その後、イベント消去プログラム 127 は、確信度計算プログラム 124 に確信度計算処理（図 18 参照）を実行させる（ステップ S607）。確信度計算処理を実行させる際、イベント消去プログラム 127 は、対象条件オブジェクトを指定するパラメータを、確信度計算プログラム 124 に入力する。この確信度計算処理により、失効イベントに対応付けられている各結論イベントについて、確信度が計算される。その後、イベント消去プログラム 127 は、一定時間待機し、その後再度イベント消去処理を行う。
- [0163] 図 22 は、実施形態に係るスナップショット表示処理のフローチャートである。
- [0164] スナップショット表示処理は、管理者からの指示に基づいてスナップショット表示画面（図 23 参照）を表示する処理である。
- [0165] 監視コンピュータ 1 は、スナップショット表示画面を表示することの指示を管理者から受け付けると、スナップショットテーブル 139 に基づいて、当該テーブル 139 で管理されている解析結果スナップショットが示す解析結果を含むスナップショット表示画面を生成し、生成した画面をディスプレイ 17 に表示させる（ステップ S701）。
- [0166] その後、監視コンピュータ 1 は、スナップショットテーブル 139 で管理されている解析結果スナップショットのそれぞれに対して、ステップ S702～ステップ S703 の処理を行う。図 22 の説明において、処理対象の解析結果スナップショットを「対象スナップショット」と呼ぶ
- [0167] ステップ S702 において、監視コンピュータ 1 は、対象スナップショットの前回表示日時が対象スナップショットの更新日時よりも前であるか否かを判定する。ここで、対象スナップショットの前回表示日時は、スナップショット表示管理テーブル 130 における対象スナップショットに関するエントリの前回表示日時 1302 に格納されている日時である。また、対象スナップショットの更新日時は、スナップショットテーブル 139 における対象

スナップショットに関するエントリの更新日時 1 3 9 5 に格納されている日時である。なお、スナップショットテーブル 1 3 9 において対象スナップショットに関するエントリが複数ある場合、すなわち対象スナップショットに係る展開ルール 6 2 が複数ある場合は、例えば、それら複数のエントリの更新日時 1 3 9 5 に格納されている日時のうちの最新の日時が、対象スナップショットの更新日時とされる。

[0168] 対象スナップショットの前回表示日時が対象スナップショットの更新日時よりも前である場合（ステップ S 7 0 2 : Y E S）、監視コンピュータ 1 は、ステップ S 7 0 1 で表示させたスナップショット表示画面に、対象スナップショットが示す解析結果が、管理者が前回参照した後に更新されたことを示すマーク（以下「更新マーク」という）を表示させる（ステップ S 7 0 3）。なお、対象スナップショットの前回表示日時が対象スナップショットの更新日時よりも前でない場合（ステップ S 7 0 2 : N O）、監視コンピュータ 1 は、ステップ S 7 0 3 の処理を実行しない。

[0169] スナップショットテーブル 1 3 9 で管理されている解析結果スナップショットのそれぞれに対してステップ S 7 0 2 ～ステップ S 7 0 3 の処理を終えた後、監視コンピュータ 1 は、処理をステップ S 7 0 4 へ進める。

[0170] ステップ S 7 0 4 において、監視コンピュータ 1 は、スナップショット表示画面においてどの解析結果スナップショットが示す解析結果が管理者によって参照されたかを判定する。そして、監視コンピュータ 1 は、スナップショット表示管理テーブル 1 3 0 において、管理者によって参照された解析結果を示す解析結果スナップショットに関するエントリの前回表示日時 1 3 0 2 に、現在の日時を示すデータを格納する。スナップショット表示画面の表示を終了することの指示を管理者から受け付けた場合、監視コンピュータ 1 は、スナップショット表示処理を終了する。

[0171] 図 2 3 は、実施形態に係るスナップショット表示画面の一例の構成図である。

[0172] スナップショット表示画面 9 は、解析結果スナップショットが示す解析結

果を表示するための画面である。スナップショット表示画面 9 は、スナップショットテーブル 139 に基づいて生成される。スナップショット表示画面 9 は、スナップショットテーブル 139 で管理されている解析結果スナップショットのそれぞれを特定するデータ、例えば解析結果スナップショットの生成日時を表示するための領域 91 と、領域 91 に表示された解析結果スナップショットのうちの管理者によって選択された解析結果スナップショットについての詳細情報（解析結果等）を表示するための領域 92 とを含む。

[0173] 領域 91 において、管理者によって未だ参照されていない解析結果、すなわち前回参照された後に更新された解析結果を示す解析結果スナップショットには、更新マーク 93 が表示される。また、領域 92 は、例えば、選択された解析結果スナップショットが示す 1 以上の確信度と、各確信度に関する結論イベントを示すデータ、例えば結論イベントに関するノード装置の名称、結論イベントの種別を示すデータ等を含む。

[0174] 管理者は、スナップショット表示画面 9 の更新マーク 93 を参照することにより、前回参照してから現在に至るまでに更新された解析結果スナップショットを容易に知ることができる。また、管理者は、スナップショット表示画面 9 を参照することにより、確信度計算処理によって得られる確信度に加えて、生成後に受信したステータス情報に基づいてより正確な確信度に更新され得る解析結果スナップショットが示す確信度をも参照できるので、より正確に原因を特定できるようになる。

[0175] なお、本発明は、以上説明した実施形態に限定されるものでなく、その趣旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

符号の説明

[0176] 1：監視コンピュータ、2：サーバ、3：ストレージ、4：ネットワーク装置

請求の範囲

[請求項1]

複数のノード装置に接続された通信インターフェースデバイスと、
前記通信インターフェースデバイスに接続された制御デバイスと
を有し、

前記制御デバイスは、

(A) 複数のノード装置のそれぞれに対して、当該ノード装置においてイベントが発生しているか否かを示すイベント発生情報を要求するリクエストを送信し、前記リクエストに対するレスポンスに含まれるイベント発生情報に基づいて、当該ノード装置に関するイベントの発生を検知し、

(B) 前記複数のノード装置のいずれかに関する1以上のイベントに対応する1以上の条件イベントと、前記1以上の条件イベントが発生した場合に原因となる結論との対応関係を示す複数のルール各結論について、当該結論に対応付けられている1以上の条件イベントの検知の有無に基づいて、当該結論が原因であることの確からしさを示す指標値を計算し、

(C) 所定の時点でその時点における前記指標値を示す解析結果スナップショットを生成し、前記解析結果スナップショットと前記解析結果スナップショットの生成日時とを関連付けて管理し、

(D) 前記複数のノード装置のいずれかの第1のノード装置に送信された第1のリクエストに対する第1のレスポンスを受信した場合、前記第1のリクエストの送信日時から前記第1のレスポンスの受信日時までを含む更新対象期間に生成された解析結果スナップショットが示す前記指標値を、前記第1のレスポンスに含まれるイベント発生情報に基づいて更新する

監視システム。

[請求項2]

前記制御デバイスは、前記解析結果スナップショットが示す前記指標値と、当該指標値に関係する結論とを表示する

請求項 1 に記載の監視システム。

[請求項3] 前記制御デバイスは、前記（D）において、前記更新対象期間を、前記第 1 のリクエストの前に前記第 1 のノード装置に送信した第 2 のリクエストの送信日時から前記第 1 のレスポンスの受信日時までとして、前記更新対象期間に生成された解析結果スナップショットが示す前記指標値を更新する

請求項 2 に記載の監視システム。

[請求項4] 前記制御デバイスは、前記第 1 のレスポンスに含まれるイベント発生情報と、前記第 2 のリクエストに対する第 2 のレスポンスに含まれるイベント発生情報とが異なる内容を示している場合、前記（D）において、前記更新対象期間に生成された解析結果スナップショットが示す前記指標値のうちの、前記第 1 のノード装置に関する条件イベントに対応付けられている結論についての指標値を、前記第 1 のノード装置に関する条件イベントが発生しているか否かが不確定であることが考慮された値に更新する

請求項 3 に記載の監視システム。

[請求項5] 前記制御デバイスは、
前記解析結果スナップショットが示す前記指標値を更新した場合、前記解析結果スナップショットと前記解析結果スナップショットの更新日時とを関連付けて管理し、

前記解析結果スナップショットが示す前記指標値を表示した場合、前記解析結果スナップショットと前記解析結果スナップショットの表示日時とを関連付けて管理し、

前記解析結果スナップショットが示す前記指標値を表示する場合において、当該解析結果スナップショットに関連付けられている前記更新日時が前記表示日時よりも後である場合、前記解析結果スナップショットが示す前記指標値が以前表示された後に更新されていることを示すデータをさらに表示する

請求項4に記載の監視システム。

[請求項6] 前記複数のノード装置のいずれかに関するイベントには、有効期間が設定されており、

前記制御デバイスは、前記複数のノード装置のいずれかに関する第1のイベントの発生を検知した場合、前記(B)において、前記第1のイベントを検知してから前記第1のイベントに設定されている有効期間が経過するまでは、前記第1のイベントの検知を有効として前記指標値を計算し、前記第1のイベントを検知してから前記第1のイベントに設定されている有効期間が経過した後は、前記第1のイベントの検知を無効として前記指標値を計算する

請求項5に記載の監視システム。

[請求項7] 前記制御デバイスは、前記(A)において、前記複数のノード装置のそれぞれに対して、定期的又は不定期的に繰り返して前記リクエストを送信し、前記リクエストを送信する時点において、前回送信したリクエストに対するレスポンスが前記監視システムによって受信されていないノード装置に対しては、前記リクエストを送信しないようにする

請求項6に記載の監視システム。

[請求項8] 複数のノード装置に接続されたコンピュータに実行させる監視プログラムであって、

前記コンピュータに、

(A) 複数のノード装置のそれぞれに対して、当該ノード装置においてイベントが発生しているか否かを示すイベント発生情報を要求するリクエストを送信させ、前記リクエストに対するレスポンスに含まれるイベント発生情報に基づいて、当該ノード装置に関するイベントの発生を検知させ、

(B) 前記複数のノード装置のいずれかに関する1以上のイベントに対応する1以上の条件イベントと、前記1以上の条件イベントが発生

した場合に原因となる結論との対応関係を示す複数のルールの各結論について、当該結論に対応付けられている 1 以上の条件イベントの検知の有無に基づいて、当該結論が原因であることの確からしさを示す指標値を計算させ、

(C) 所定の時点でその時点における前記指標値を示す解析結果スナップショットを生成させ、前記解析結果スナップショットと前記解析結果スナップショットの生成日時とを関連付けて管理させ、

(D) 前記複数のノード装置のいずれかの第 1 のノード装置に送信された第 1 のリクエストに対する第 1 のレスポンスを受信した場合、前記第 1 のリクエストの送信日時から前記第 1 のレスポンスの受信日時までを含む更新対象期間に生成された解析結果スナップショットが示す前記指標値を、前記第 1 のレスポンスに含まれるイベント発生情報に基づいて更新させる

監視プログラム。

[請求項9] 前記コンピュータに、前記解析結果スナップショットが示す前記指標値と、当該指標値に関係する結論とを表示させる
請求項 8 に記載の監視プログラム。

[請求項10] 前記コンピュータに、前記 (D) において、前記更新対象期間を、前記第 1 のリクエストの前に前記第 1 のノード装置に送信した第 2 のリクエストの送信日時から前記第 1 のレスポンスの受信日時までとして、前記更新対象期間に生成された解析結果スナップショットが示す前記指標値を更新させる
請求項 8 に記載の監視プログラム。

[請求項11] 前記コンピュータに、前記第 1 のレスポンスに含まれるイベント発生情報と、前記第 2 のリクエストに対する第 2 のレスポンスに含まれるイベント発生情報とが異なる内容を示している場合、前記 (D) において、前記更新対象期間に生成された解析結果スナップショットが示す前記指標値のうちの、前記第 1 のノード装置に関する条件イベン

トに対応付けられている結論についての指標値を、前記第1のノード装置に関する条件イベントが発生しているか否かが不確定であることが考慮された値に更新させる

請求項10に記載の監視プログラム。

[請求項12]

前記コンピュータに、

前記解析結果スナップショットが示す前記指標値を更新した場合、前記解析結果スナップショットと前記解析結果スナップショットの更新日時とを関連付けて管理させ、

前記解析結果スナップショットが示す前記指標値を表示した場合、前記解析結果スナップショットと前記解析結果スナップショットの表示日時とを関連付けて管理させ、

前記解析結果スナップショットが示す前記指標値を表示する場合において、当該解析結果スナップショットに関連付けられている前記更新日時が前記表示日時よりも後である場合、前記解析結果スナップショットが示す前記指標値が以前表示された以降に更新されていることを示すデータをさらに表示させる

請求項9に記載の監視プログラム。

[請求項13]

前記複数のノード装置のいずれかに関するイベントには、有効期間が設定されており、

前記コンピュータに、前記複数のノード装置のいずれかに関する第1のイベントの発生を検知した場合、前記(B)において、前記第1のイベントを検知してから前記第1のイベントに設定されている有効期間が経過するまでは、前記第1のイベントの検知を有効として前記指標値を計算させ、前記第1のイベントを検知してから前記第1のイベントに設定されている有効期間が経過した後は、前記第1のイベントの検知を無効として前記指標値を計算させる

請求項8に記載の監視プログラム。

[請求項14]

前記コンピュータに、前記(A)において、前記複数のノード装置

のそれぞれに対して、定期的又は不定期的に繰り返して前記リクエストを送信させ、前記リクエストを送信する時点において、前回送信したリクエストに対するレスポンスが前記監視システムによって受信されていないノード装置に対しては、前記リクエストを送信しないようにさせる

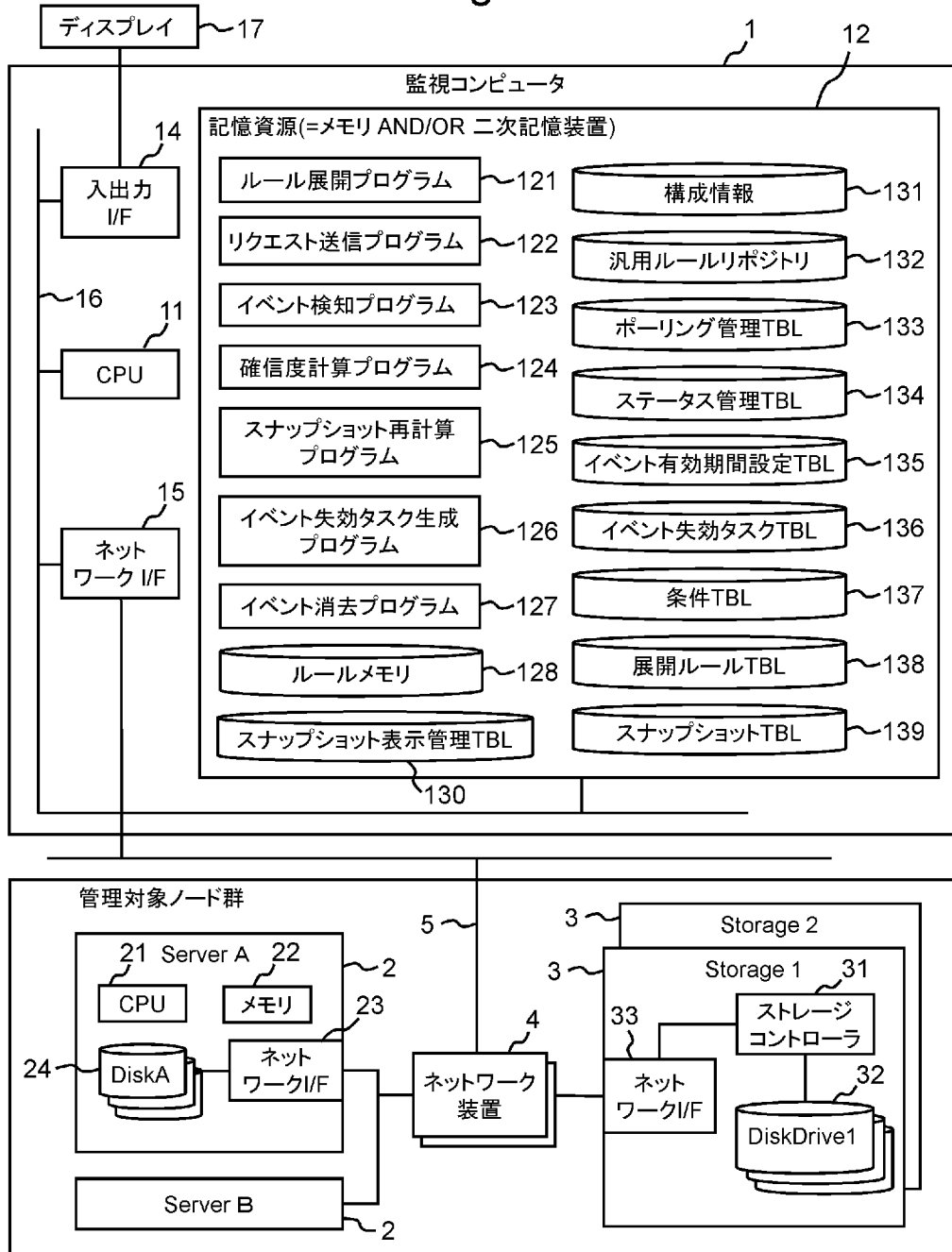
請求項 8 に記載の監視プログラム。

[請求項15]

前記コンピュータに、前記（D）において、前記第 1 のレスポンスに含まれるイベント発生情報が、前記第 1 のノード装置に関するイベントが発生していることを示している場合、前記更新対象期間に生成された解析結果スナップショットが示す前記指標値を、前記第 1 のノード装置に関する条件イベントの検知が考慮された値に更新させる
請求項 8 に記載の監視プログラム。

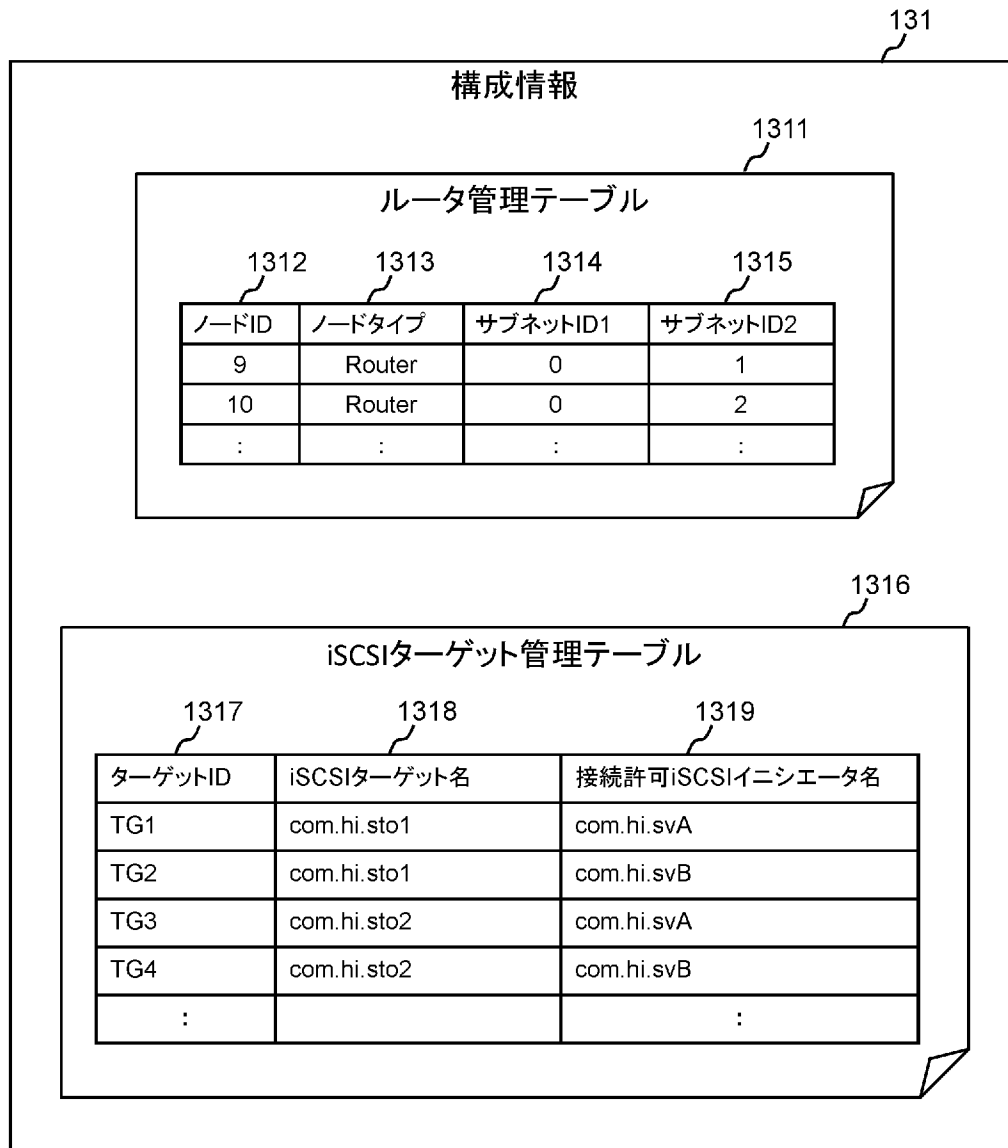
[図1]

Fig. 1



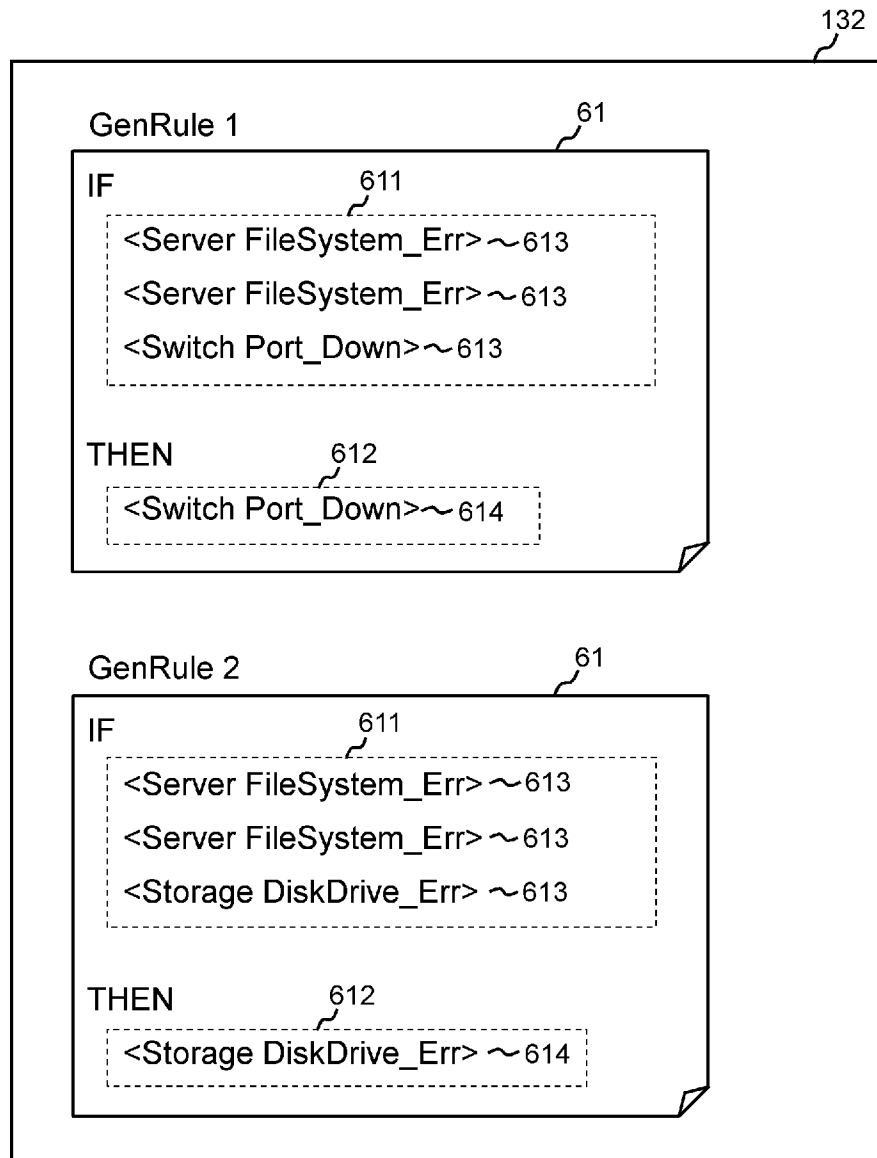
[図2]

Fig. 2



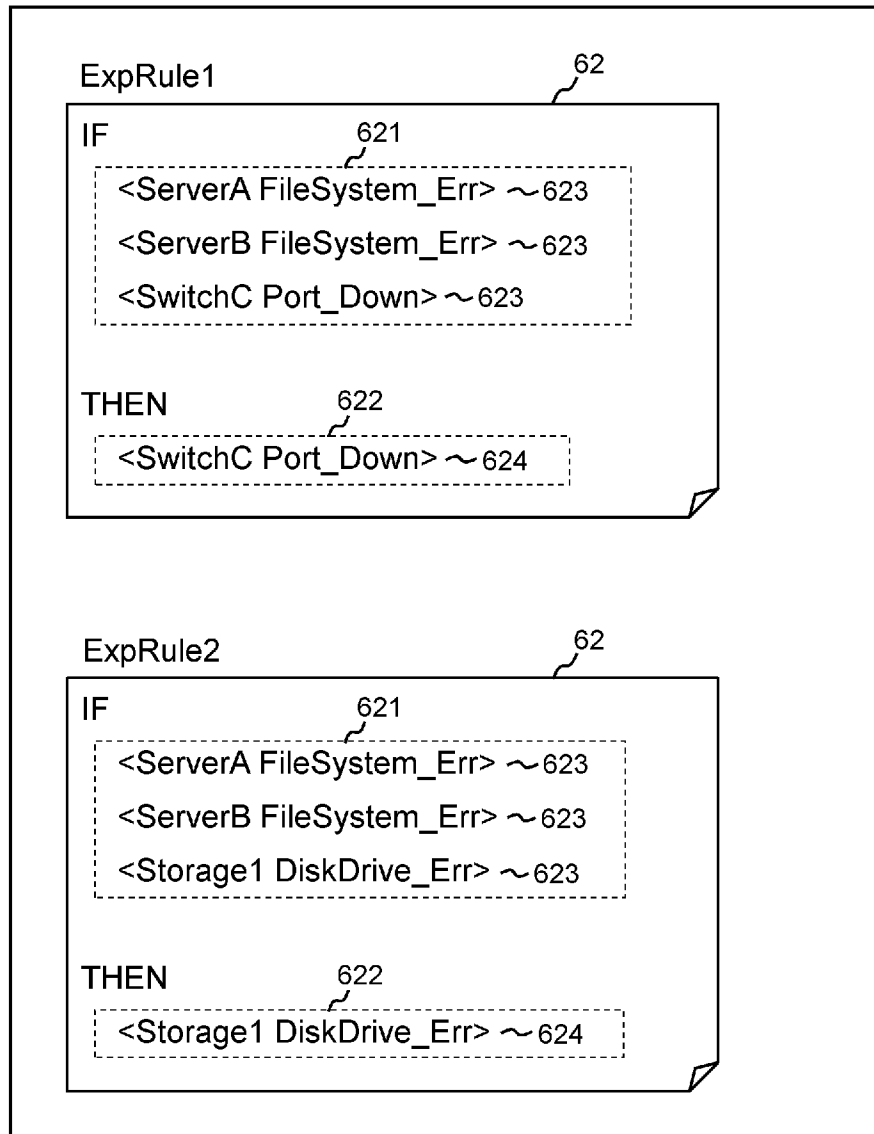
[図3]

Fig. 3



[図4]

Fig. 4



[図5]

Fig. 5

ノードID	リクエスト送信日時
70	4/13/2008 9:15:11
80	4/13/2008 9:15:20
100	-
115	-
120	-

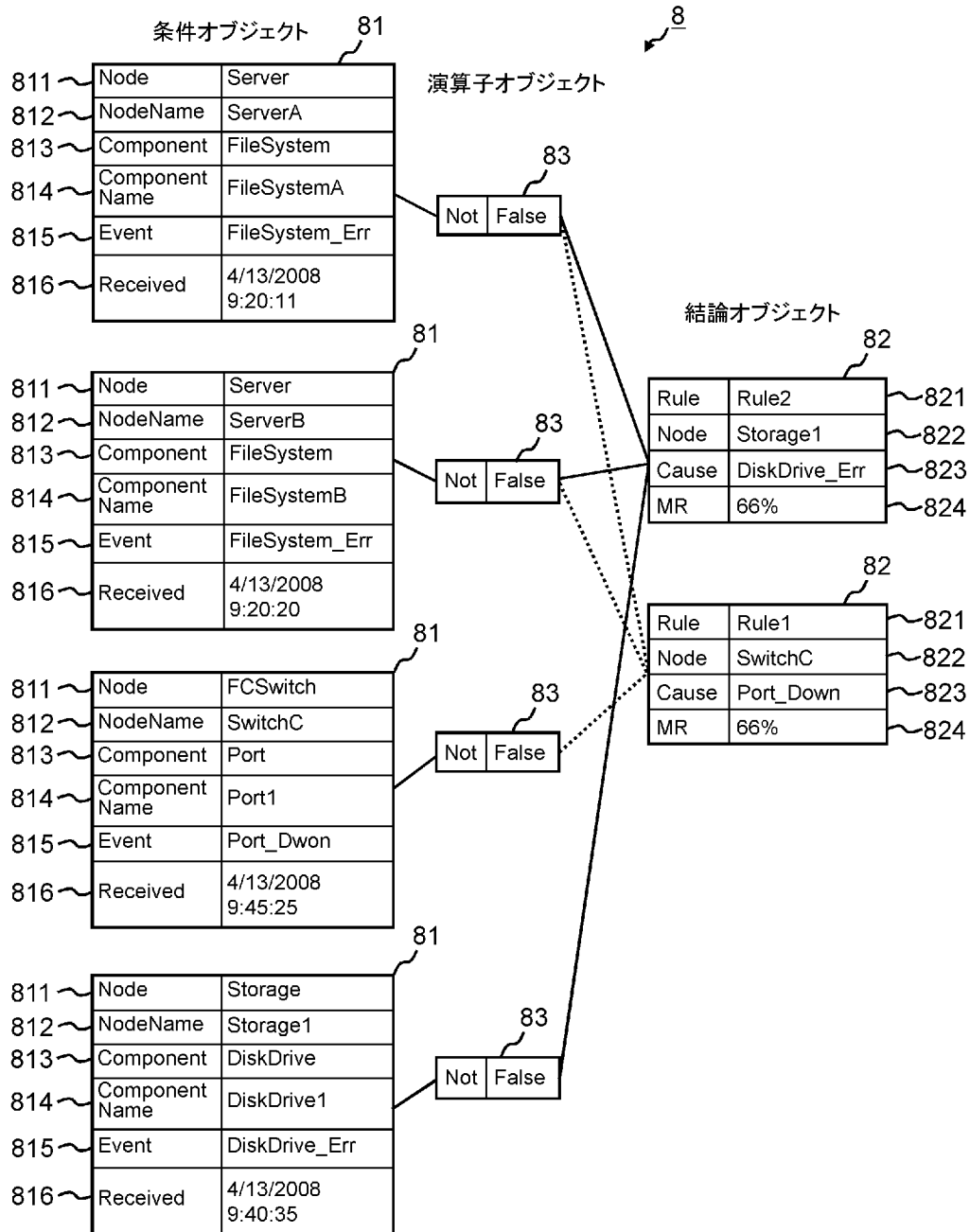
[図6]

Fig. 6

1341	ステータス管理 ID	1342	ノード種別	1343	ノード名	1344	コンポーネント ID	1345	コンポーネント名	1346	イベント種別	1347	最新の Status	1348	最新の情報収集プロセスのイベント受信日時	1349	最新の情報収集プロセス開始日時	1340	前回の Status	134a	前回の情報収集プロセス開始日時	134b	134
	1	70	Server	ServerA	111	FileSystemA	FileSystemm_Err	Error	4/13/2008 9:20:11	4/13/2008 9:15:11	Error	4/13/2008 9:10:11	4/13/2008 9:10:20	—	—	—	—	Normal	4/13/2008 9:10:35				
	2	71	Server	ServerB	222	FileSystemB	FileSystemm_Err	Error	4/13/2008 9:20:20	4/13/2008 9:15:20	Normal	4/13/2008 9:45:25	4/13/2008 9:15:25	—	—	—	—	Normal	4/13/2008 9:10:35				
	3	72	Switch	SwitchC	223	Port1	Port_Down	Error	4/13/2008 9:40:35	4/13/2008 9:15:35	Error	4/13/2008 9:28:35	4/13/2008 9:22:45	—	—	—	—	Normal	4/13/2008 9:10:35				
	4	80	Storage	Storage1	224	DiskDrive1	DiskDrive_Err	Error	4/13/2008 9:28:35	4/13/2008 9:22:45	Error	4/13/2008 9:28:35	4/13/2008 9:22:45	—	—	—	—	Normal	4/13/2008 9:10:35				
	5	90	Storage	Storage2	330	LU2	LU_Err	Error	4/13/2008 9:28:35	4/13/2008 9:22:45	Error	4/13/2008 9:28:35	4/13/2008 9:22:45	—	—	—	—	Normal	4/13/2008 9:10:35				

[図7]

Fig. 7



[図8]

Fig. 8

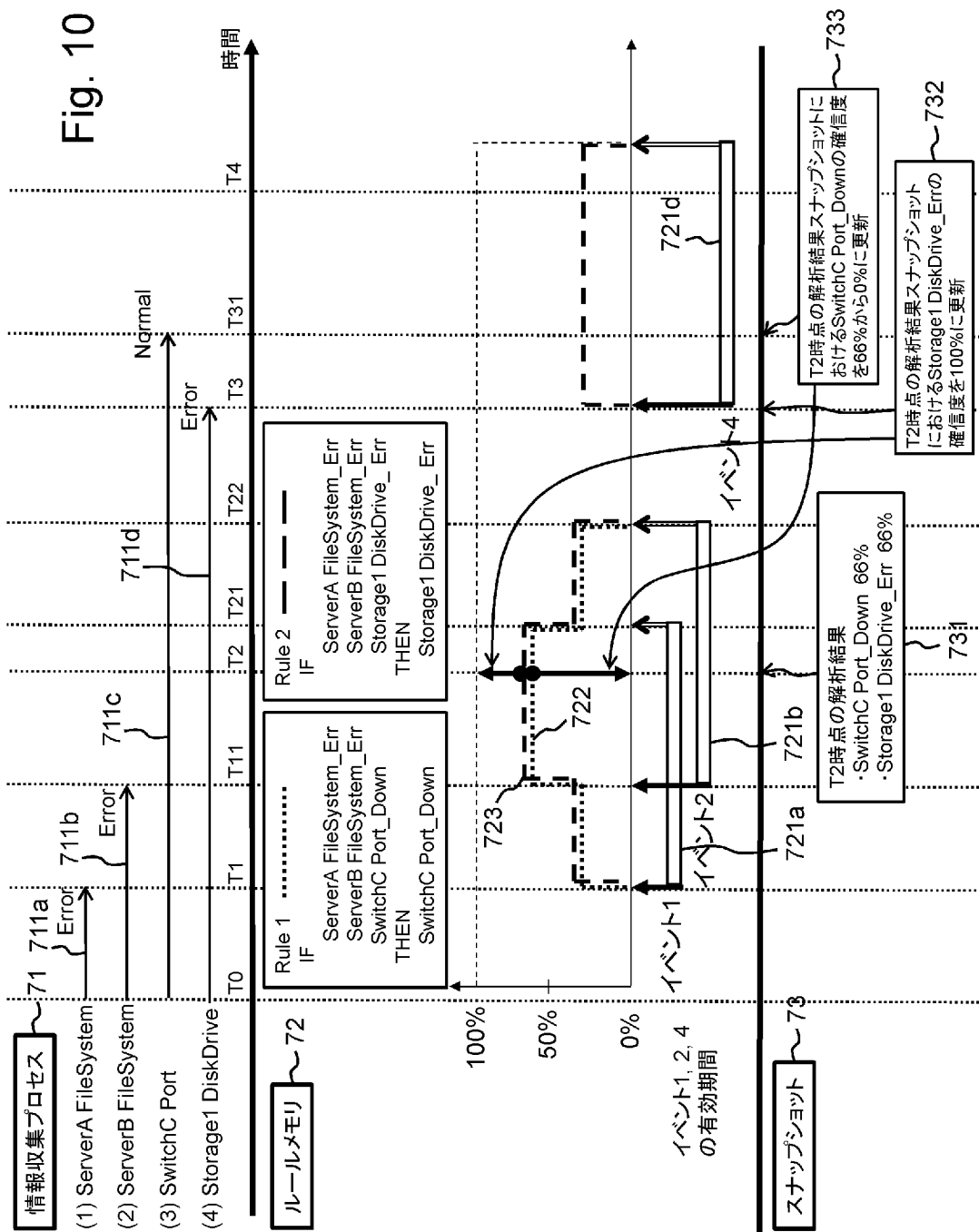
1351 ノード種別	1352 イベント種別	1353 有効期間(分)
Server	Cpu_Pfm_Err	5
Server	iSCSI_Comm_Err	10
Server	FileSystem_Err	10
Switch	Port_Down	10
...	...	...
Storage	Controller_Err	10
Storage	DiskDrive_Err	10
...	...	...

[図9]

Fig. 9

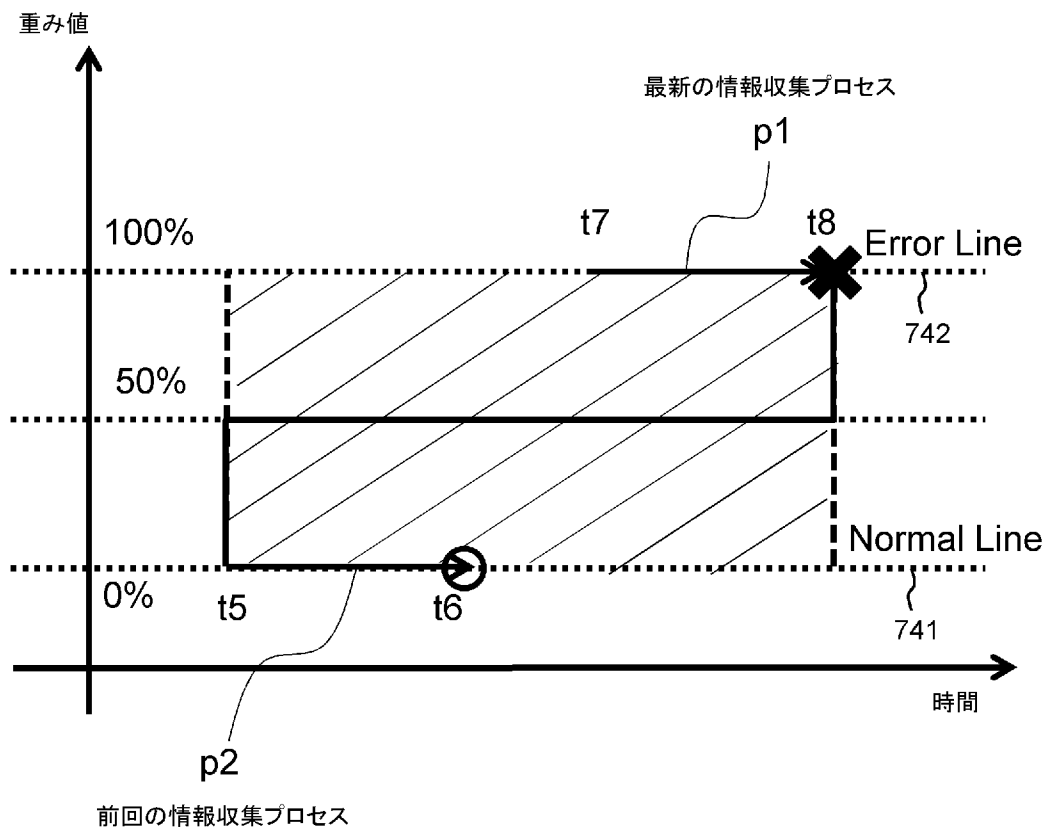
1361 開始日時	1362 ノード名	1363 イベント種別
4/13/2008 9:20:11	ServerA	FileSystem_Err
4/13/2008 9:20:20	ServerB	FileSystem_Err
4/13/2008 9:40:35	Storage1	DiskDrive_Err
...	...	...

[図10]



[図11]

Fig. 11



[図12A]

Fig. 12A

1371	1372	1373	1374	1375	1376	137
スナップ ショットID	根本原因	展開ルール	ステータス管理ID	Not条件	重み付け	
0001	"Storage1" Disk Drive_Err	Rule2	1	False	100%	
0001	"Storage1" Disk Drive_Err	Rule2	2	False	100%	
0001	"Storage1" Disk Drive_Err	Rule2	4	False	—	
0001	"SwitchC" Port_Down	Rule1	1	False	100%	
0001	"SwitchC" Port_Down	Rule1	3	False	—	
0001	"SwitchC" Port_Down	Rule1	2	False	100%	
0002	"Storage2" Controller_Err	Rule3	5	False	50%	
...	...	...	...	...	...	

[図12B]

Fig. 12B

1371	1372	1373	1374	1375	1376	137
スナップ ショットID	根本原因	展開ルール	スレータス管理ID	Not条件	重み付け	
0001	"Storage1" Disk Drive_Err	Rule2	1	False	100%	
0001	"Storage1" Disk Drive_Err	Rule2	2	False	100%	
0001	"Storage1" Disk Drive_Err	Rule2	4	False	<u>100%</u>	
0001	"SwitchC" Port_Down	Rule1	1	False	100%	
0001	"SwitchC" Port_Down	Rule1	3	False	<u>0%</u>	
0001	"SwitchC" Port_Down	Rule1	2	False	100%	
0002	"Storage2" Controller_Err	Rule3	5	False	50%	
...	...	...	...	...	...	

[図13A]

Fig. 13A

スナップショットID	根本原因	展開ルール	条件イベント数	確信度
0001	"Storage1" Disk Drive_Err	Rule2	3	66%
0001	"SwitchC" Port_Down	Rule1	3	66%
0002	"Server9" FCHBA_Err	Rule20	2	25%

[図13B]

Fig. 13B

1381	スナップショットID	1382	根本原因	1383	展開ルール	1384	条件イベント数	1385	確信度
	0001	"Storage1" Disk Drive_Err		Rule2		3		<u>100%</u>	
	0001	"SwitchC" Port_Down		Rule1		3		<u>0%</u>	
	0002	"Server9" FCHBA_Err		Rule20		2		25%	

[図14A]

Fig. 14A

1391		1392	1393	1394	1395	139
スナップショットID	根本原因	確信度	スナップショット化した日時	更新日時		
0001	"Storage1" Disk Drive_Err	66%	4/20/2008 9:30:11	4/20/2008 9:30:11		
0001	"SwitchC" Port_Down	66%	4/20/2008 9:30:11	4/20/2008 9:30:11		
0002	"Server9" FCHBA_Err	25%	4/20/2008 9:40:11	4/20/2008 9:40:11		
0003	"Storage2" Disk Drive_Err	75%	4/20/2008 9:50:11	4/20/2008 9:50:11		

[図14B]

Fig. 14B

スナップショットID	根本原因	確信度	スナップショット化した日時	更新日時
0001	"Storage1" Disk Drive_Err	100%	4/20/2008 9:30:11	4/20/2008 9:41:11
0001	"SwitchC" Port_Down	0%	4/20/2008 9:30:11	4/20/2008 9:46:11
0002	"Server9" FCHBA_Err	25%	4/20/2008 9:40:11	4/20/2008 9:40:11
0003	"Storage2" Disk Drive_Err	75%	4/20/2008 9:50:11	4/20/2008 9:50:11

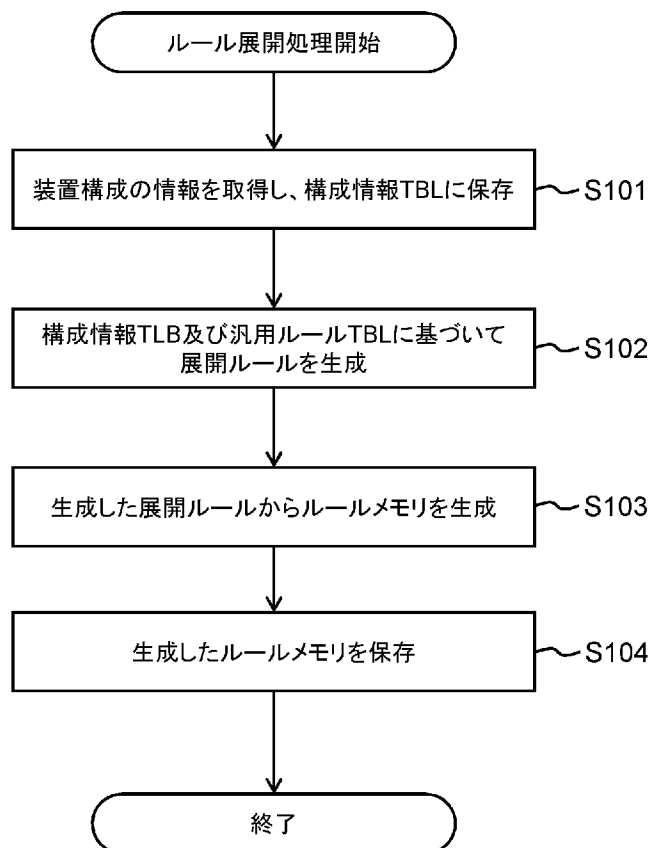
[図15]

Fig. 15

スナップショットID	前回表示日時
0001	4/20/2008 9:35:11
0002	4/20/2008 9:15:20
0003	4/13/2008 10:46:26
0004	4/15/2008 14:51:42
0005	4/13/2008 8:11:52

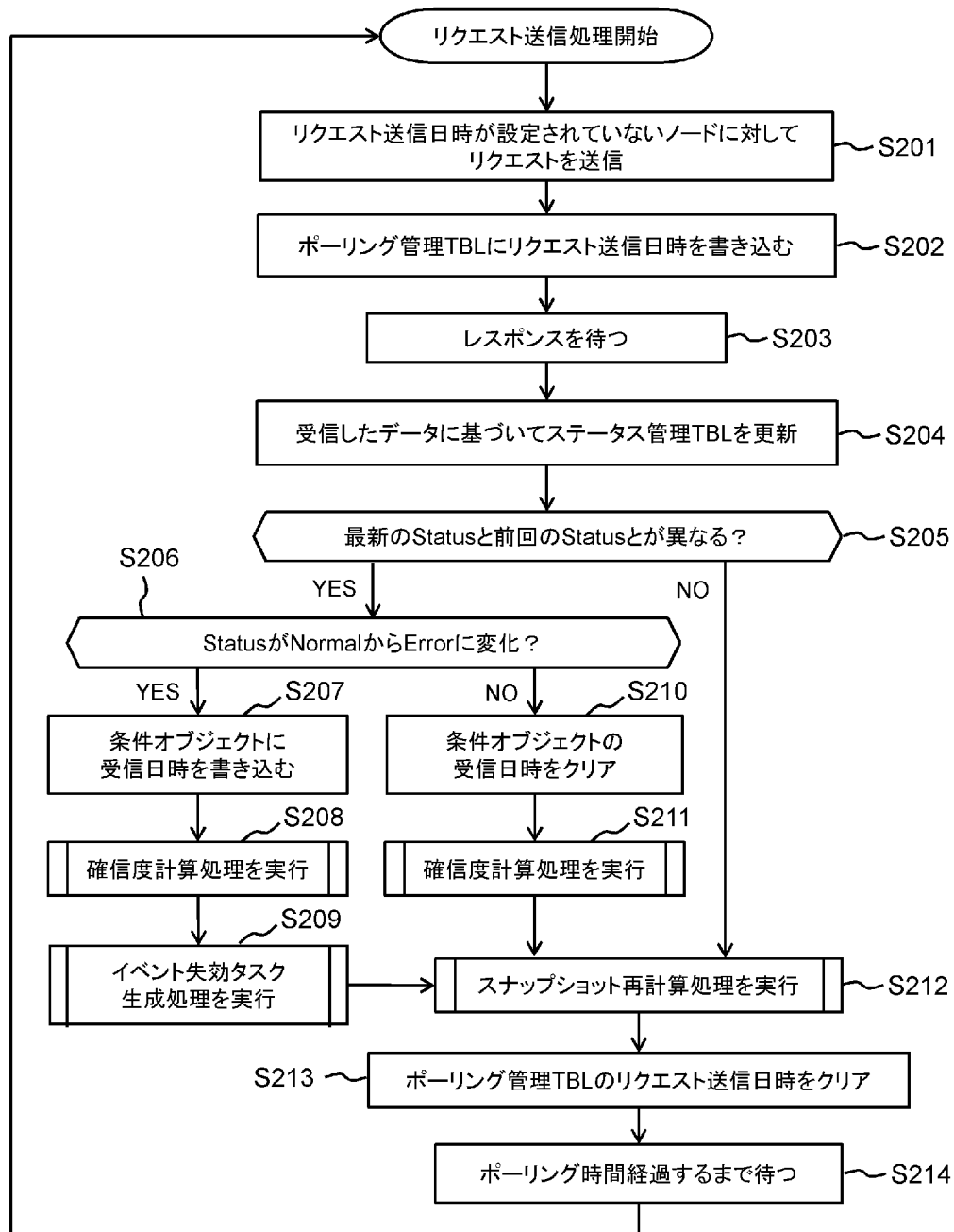
[図16]

Fig. 16



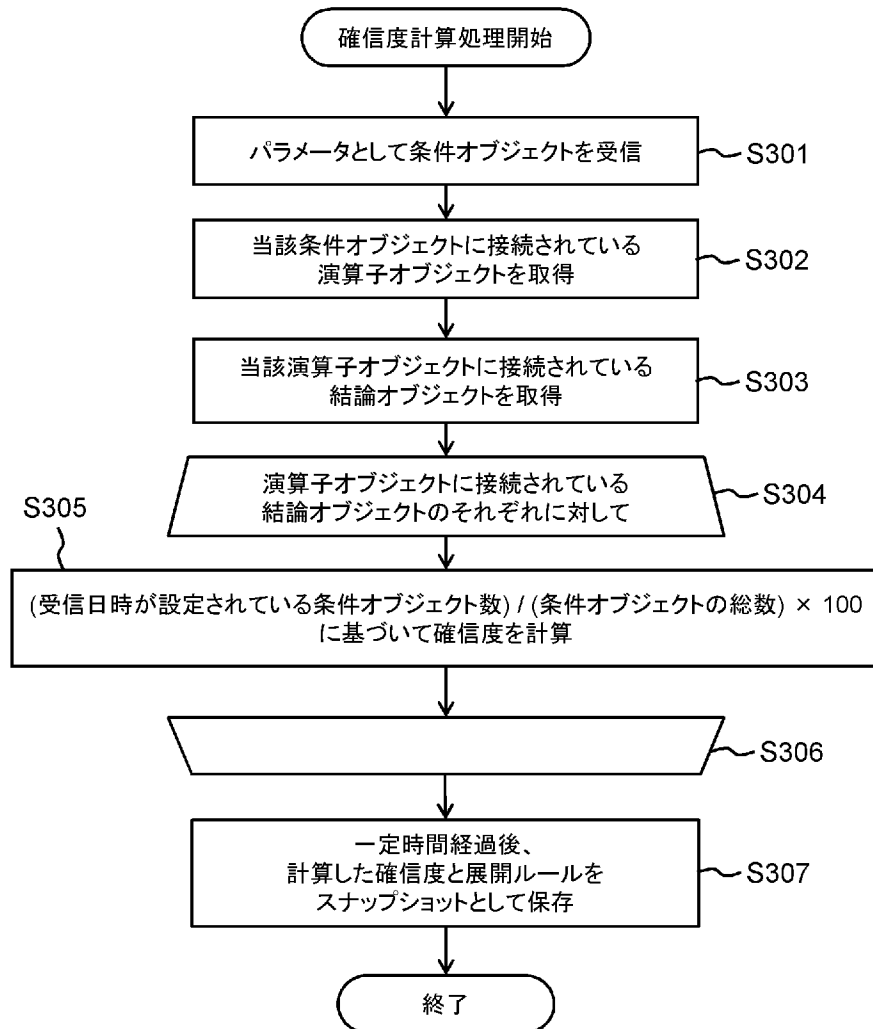
[図17]

Fig. 17



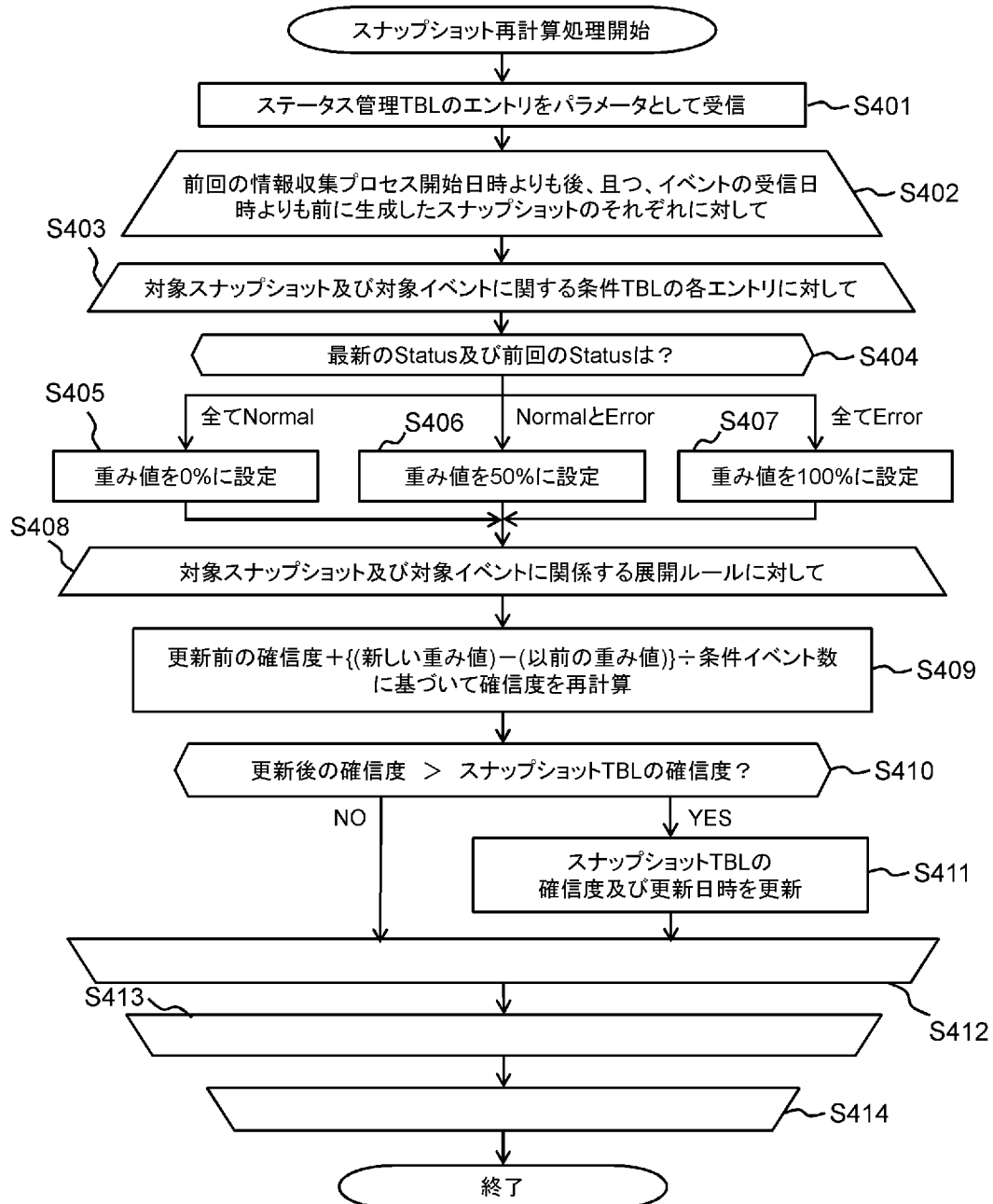
[図18]

Fig. 18



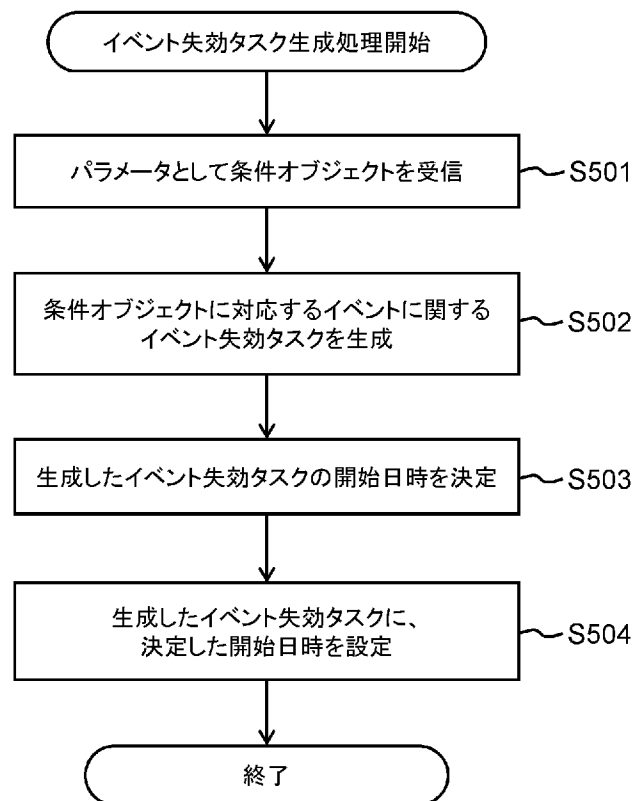
[図19]

Fig. 19



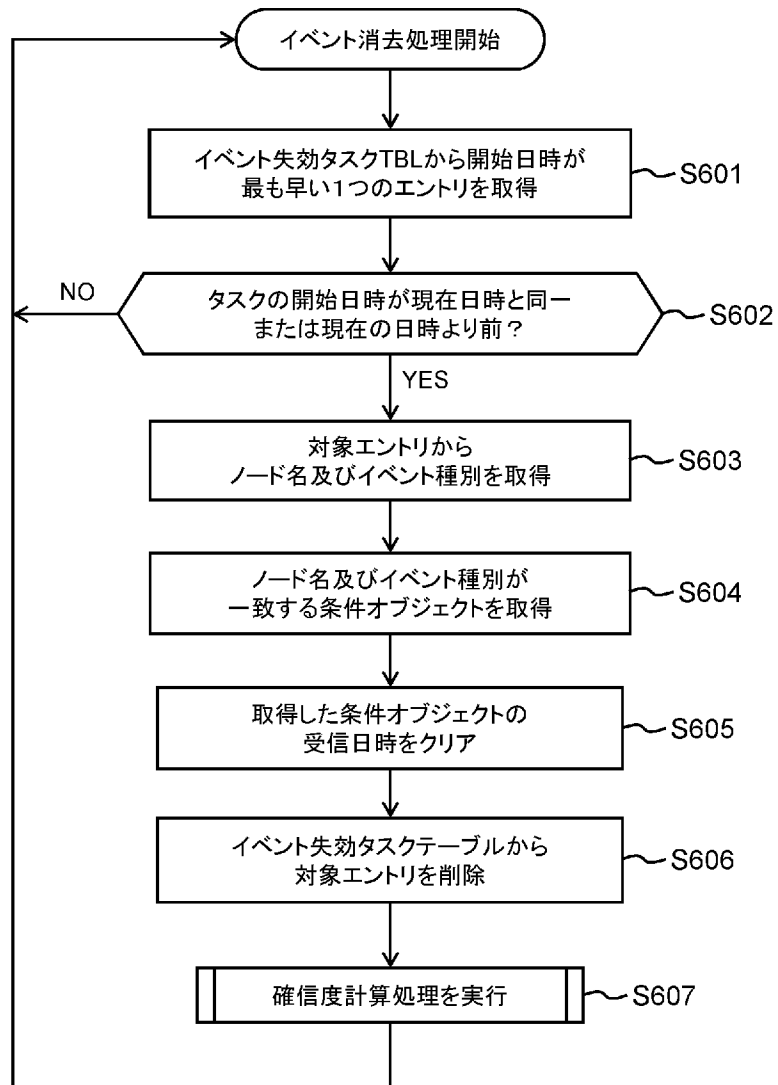
[図20]

Fig. 20



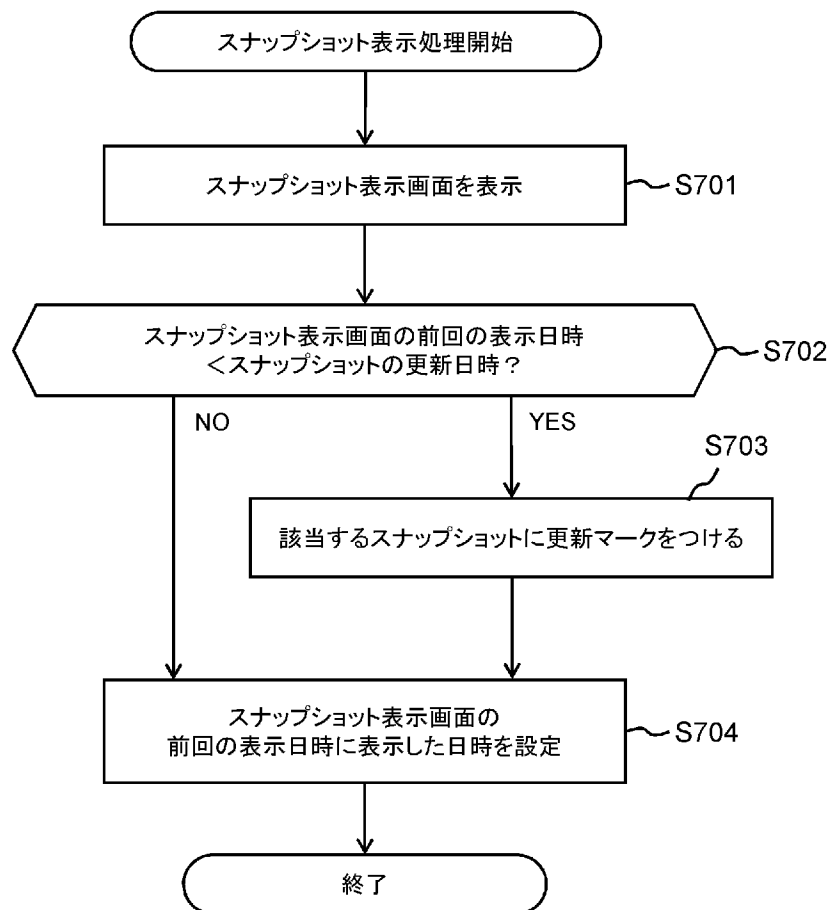
[図21]

Fig. 21



[図22]

Fig. 22



[図23]

Fig. 23

91	92	9			
SnapShot	Availability Snapshots 2008-4-13 9:30 +0900				
-2008-4-13 9:30 -#1 Storage1 Disk -#2 SwitchC ...	Name	Component	Certainly	Event Detected Nodes	
93	#1	Storage1	DiskDrive	100%	ServerA,ServerB
	#2	SwitchC	FCport	0%	ServerA,ServerB
	Description				
+2008-4-13 9:40					
+2008-4-13 9:50					
+2008-4-13 10:02					
+2008-4-13 10:20					

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/078185

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/30 (2006.01) i, G06F11/34 (2006.01) i

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)

G06F11/22, G06F11/30, G06F11/34, G06F13/00, G06N5/04

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	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

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 2011-518359 A (Hitachi, Ltd.), 23 June 2011 (23.06.2011), paragraphs [0030] to [0095]; fig. 7 to 16 & US 2009/0313198 A1 & EP 2291742 A1 & EP 2341434 A1 & WO 2009/153901 A1	1-15
A	JP 2012-22614 A (Hitachi, Ltd.), 02 February 2012 (02.02.2012), paragraphs [0057] to [0059], [0087] to [0099], [0142]; fig. 10, 15 & US 2012/0017127 A1 & WO 2012/008058 A1	1-15
A	JP 2011-76409 A (Hitachi Solutions, Ltd.), 14 April 2011 (14.04.2011), paragraphs [0019] to [0064]; fig. 1 to 11 (Family: none)	1-15



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
29 November, 2012 (29.11.12)

Date of mailing of the international search report
11 December, 2012 (11.12.12)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G06F11/30(2006.01)i, G06F11/34(2006.01)i

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 (I P C))

Int.Cl. G06F11/22, G06F11/30, G06F11/34, G06F13/00, G06N5/04

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 2 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 2 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 2 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 請求項の番号
A	JP 2011-518359 A (株式会社日立製作所) 2011.06.23, 【0030】 - 【0095】 , 図 7-16 & US 2009/0313198 A1 & EP 2291742 A1 & EP 2341434 A1 & WO 2009/153901 A1	1 - 1 5
A	JP 2012-22614 A (株式会社日立製作所) 2012.02.02, 【0057】 - 【0059】 , 【0087】 - 【0099】 , 【0142】 , 図 10, 15 & US 2012/0017127 A1 & WO 2012/008058 A1	1 - 1 5

☒ 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
「&」同一パテントファミリー文献

国際調査を完了した日

2 9 . 1 1 . 2 0 1 2

国際調査報告の発送日

1 1 . 1 2 . 2 0 1 2

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

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)

多賀 実

5 B

9 3 6 7

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 5

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 請求項の番号
A	JP 2011-76409 A (株式会社日立ソリューションズ) 2011. 04. 14, 【0019】 - 【0064】 , 図 1-11 (ファミリーなし)	1 - 1 5