(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
2010 年 4 月 8 日(08.04.2010)

PCT

(10) 国際公開番号
WO 2010/038327 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/JP2009/000285

(22) 国際出願日: 2009 年 1 月 26 日(26.01.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-252093 2008 年 9 月 30 日(30.09.2008) JP

(71) 出願人 (米国を除く全ての指定国について): 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; および

(75) 発明者/出願人 (米国についてのみ): 森村 知弘(MORIMURA, Tomohiro) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 永井 崇之(NAGAI, Takayuki) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 菅内 公徳(SUGAUCHI, Kiminori) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 黒田 沢希(KURODA, Takaki) [JP/JP]; 〒2448555 神奈川県横浜市戸塚区戸塚町５０３０番地 株式会社日立製作所 ソフトウェア事業部内 Kanagawa (JP). 荒砥 偉浩(ARATO, Yoshihiro) [JP/JP]; 〒2448555 神奈川県横浜市戸塚区戸塚町５０３０番地 株式会社日立製作所 ソフトウェア事業部内 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); 〒1010044 東京都千代田区鍛冶町２丁目３番２号 神田センタービルディング５階 Tokyo (JP).

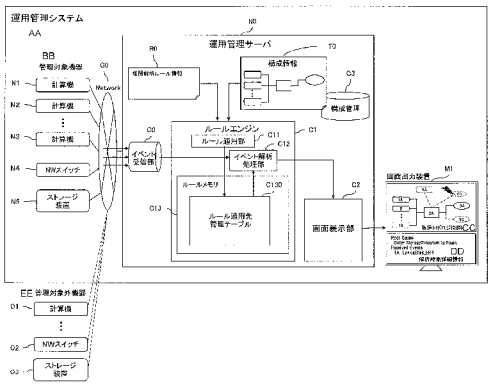
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY,

[続葉有]

(54) **Title**: ROOT CAUSE ANALYSIS METHOD TARGETING INFORMATION TECHNOLOGY (IT) DEVICE NOT TO ACQUIRE EVENT INFORMATION, DEVICE AND PROGRAM

(54) 発明の名称 : イベント情報取得外のＩＴ装置を対象とする根本原因解析方法、装置、プログラム。

図1



AA OPERATION MANAGEMENT SYSTEM
BB MANAGEMENT SUBJECT APPARATUS
N1-N3 COMPUTER
N4 NW SWITCH
N5 STORAGE DEVICE
N0 OPERATION MANAGEMENT SERVER
R0 CORRELATION ANALYSIS RULE INFORMATION
T0 STRUCTURE INFORMATION
C3 STRUCTURE MANAGEMENT
C0 EVENT RECEIVING UNIT
C1 RULE ENGINE
C11 RULE APPLICATION UNIT
C12 EVENT ANALYSIS PROCESSING UNIT
C13 RULE MEMORY
C130 RULE APPLIED PARTY MANAGEMENT TABLE
C2 SCREEN DISPLAY UNIT
M1 SCREEN OUTPUT DEVICE
CC ENVISAGED TOPOLOGY SCREEN
DD ANALYSIS RESULT DETAIL INFORMATION
EE OTHER THAN MANAGEMENT SUBJECT APPARATUS
O1 COMPUTER
O2 NW SWITCH
O3 STORAGE DEVICE
G0 Network

(57) **Abstract**: A root cause analysis method registers an information processing device of an event information acquisition target as an event acquisition target device in structure information at an operation management server, specifies event information to meet a rule stored in advance from a plurality of event information components stored at the operation management server, specifies a server device of a network service related to the event information components, and displays that a factor of the event occurring at a client information processing device that generates event information is the event in respect of a network service occurring at a server device.

(57) 要約: 運用管理サーバにて、イベント情報取得対象の情報処理装置をイベント取得対象装置として構成情報に登録し、運用管理サーバに格納した複数のイベント情報から、予め格納したルールに適合するイベント情報を特定し、当該イベント情報が関連するネットワークサービスのサーバ装置を特定し、イベント情報を生成したクライアント情報処理装置で発生した当該イベントの要因がサーバ装置で発生したネットワークサービスに関するイベントであることを表示する。

WO 2010/038327 A1

MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, 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)）

明　細　書

イベント情報取得外のＩＴ装置を対象とする根本原因解析方法、装置、プログラム。

技術分野

[0001] 本願明細書に開示される技術は、サーバコンピュータ、ネットワーク装置、ストレージ装置を含む情報処理システムの運用を管理する運用管理方法、装置、システム、プログラム、プログラムを含む媒体及びプログラムの配布装置に関する。

背景技術

[0002] 近年、ＩＴシステム（ＩＴはＩｎｆｏｒｍａｔｉｏｎ　Ｔｅｃｈｎｏｌｏｇｙの略。なお、以後はＩＴシステムを情報処理システムと呼ぶことがある）はネットワークを介して様々なＩＴ装置（以後、情報処理装置と呼ぶことがある）が接続することで複雑化・大規模化し、障害はネットワークを介して様々なＩＴ装置に影響を与えている。これらの障害の箇所と原因を特定する根本原因解析技術として、特許文献１にはＩＴ装置から障害内容を通知されるイベント情報を用いて障害箇所と原因を解析するイベント相関技術が開示されている。また、イベント相関技術は、障害時に計算機から送信されるイベントの相関を利用して、根本原因を推測する技術とも言える。

[0003] また、非特許文献２では、当該技術と障害時のイベントの組み合わせと推測される根本原因を対にしてルール化することで、エキスパートシステムをベースとした推論エンジンを用いて根本原因を迅速に突き止める技術が開示されている。

[0004] 特許文献1：米国特許第６，２４９，７５５号明細書

非特許文献1：“Ｒｅｔｅ：　Ａ　Ｆａｓｔ　Ａｌｇｏｒｉｔｈｍ　ｆｏｒ　ｔｈｅ　Ｍａｎｙ　Ｐａｔｔｅｒｎ／Ｍａｎｙ　Ｏｂｊｅｃｔ　Ｐａｔｔｅｒｎ　Ｍａｔｃｈ　Ｐｒｏｂｌｅｍ”，　ＡＲＴＩＦＩＣＩＡＬ　ＩＮＴＥＬＬＩＧＥＮＣＥ，　Ｖｏｌ．　１９，　ｎｏ．　１，　１９８２，　ｐｐ

. １７－３７

発明の開示

発明が解決しようとする課題

[0005] 運用管理に必要な処理を行う運用管理サーバはネットワークに接続された全てのＩＴ装置のイベントを採取することはできないため、運用管理サーバはイベント情報を受信（または取得）するＩＴ装置を限定し、根本原因解析技術を用いて解析結果を表示する。

[0006] しかし、当該解析技術はネットワークに接続された全てのＩＴ装置からイベント情報の取得ができることを前提としている。その結果、運用管理サーバがイベント情報を取得しないＩＴ装置でイベント（例えば障害）が発生し、イベント情報を取得しているＩＴ装置がこの障害の影響を受けた場合に、障害発生ＩＴ装置が解析対象外であるためにルールが適用されず、障害の根本原因を突き止められない。

課題を解決するための手段

[0007] 本発明は、複数の情報処理装置と画面出力装置とプロセッサとメモリを有する運用管理サーバとから構成される情報処理システムの、前記複数の情報処理装置で発生するイベントの解析に関する装置、システム、方法、プログラム、記憶メディアを提供する。

本発明の一実施例によると、前記運用管理サーバについて、前記複数の情報処理装置の各々が、クライアントとしてネットワークサービスを用いるためにアクセス対象とする前記複数の情報処理装置の一部であるサーバ装置の識別情報を、前記メモリが有する構成情報に格納し、前記複数の情報処理装置の一部であって、前記運用管理サーバがイベント情報を取得する対象である複数のイベント取得対象装置を前記メモリが有する構成情報に登録し、前記複数の情報処理装置で発生する前記ネットワークサービスに関連した第一のイベント種別を含むイベントと、前記ネットワークサービスに関連した前記第一のイベント種別とは異なる第二のイベント種別を含むイベントと、を検知した場合に、前記第二のイベント種別に対応するイベントの発生が原因で

前記第一のイベント種別に対応するイベントが発生し得ることを示す相関解析ルール情報を前記メモリに格納し、前記複数のイベント取得対象装置から収集した複数の前記イベント情報を前記メモリに格納し、前記相関解析ルール情報を元に、前記メモリに格納した複数の前記イベント情報から、前記第一のイベント種別を含む第一のイベント情報を特定し、前記構成情報を元に、前記第一のイベント情報を送信したイベント取得対象装置の一つである第一イベント取得対象装置と、前記第一のイベント種別に対応する前記ネットワークサービスにおける前記第一イベント取得対象装置のサーバ装置である障害要因装置とを特定し、前記相関解析ルール情報と前記構成情報とを元に、前記障害要因装置が前記複数のイベント取得対象装置でない場合に、前記第一イベント取得対象装置と前記第一のイベント種別と前記障害要因装置と前記第二のイベント種別とを特定する情報を前記画面出力装置へ送信することで、前記第一イベント取得対象装置で発生した前記第一のイベント情報に対応したイベントが、前記障害要因装置で前記第二のイベント種別のイベントが発生したことが要因と推定されることを前記画面出力装置へ表示させる。

[0008] なお、前記相関解析ルール情報は、前記第一のイベント種別が発生した前記複数の情報処理装置の一つである第一情報処理装置と、前記第二のイベント種別が発生した前記複数の情報処理装置の一つである第二情報処理装置と、の間のトポロジ条件を示すトポロジ条件情報を含み、前記要因特定ステップは、前記トポロジ条件情報に基づいて前記障害要因装置を特定してもよい。

[0009] また、前記相関解析ルール情報と前記構成情報に基づいて、前記複数のイベント取得対象装置のサーバ装置であって、前記複数のイベント取得対象装置に含まれない、前記複数の情報処理装置の一部であるイベント関連情報処理装置を特定し、前記イベント関連情報処理装置からイベント情報の取得が可能か調査し、前記調査の結果を元に、前記イベント関連情報処理装置からイベント情報の取得が可能な場合は前記イベント関連情報処理装置を特定す

る情報を前記画面出力装置へ送信することで、前記イベント関連情報処理装置からイベント情報の取得が可能であることを前記画面出力装置へ表示させてもよい。

[0010] また、前記イベント情報取得可否調査は、前記複数の情報処理装置であって予め調査範囲として設定されたＩＰアドレスの範囲に含まれるＩＰアドレスを有する情報処理装置に対して、前記運用管理サーバが所定の手順に基づくアクセスを行った結果に基づいてもよい。

[0011] また、前記障害要因装置はコントローラを有し、論理ボリュームを提供するストレージ装置であって、前記ネットワークサービスは前記論理ボリュームをブロックアクセス形式のプロトコルによって提供するサービスであって、前記第一のイベント種別が前記コントローラの障害発生であり、前記第一のイベント種別が前記論理ボリュームへのアクセス失敗であってもよい。

また、前記相関解析ルール情報と前記構成情報とを元に、前記障害要因装置が前記複数のイベント取得対象装置の一つの場合に、複数の前記イベント情報から前記第二のイベント種別を含み、前記障害要因装置が取得元である第二のイベント情報を特定し、前記第一イベント取得対象装置と前記第一のイベント情報と前記障害要因装置と前記第二のイベント情報とを特定する情報を前記画面出力装置へ送信することで、前記第一イベント取得対象装置で発生した前記第一のイベント情報に対応したイベントが、前記障害要因装置で発生した前記第二のイベント情報に対応したイベントが発生したことが要因であることを前記画面出力装置へ表示させてもよい。

また、本発明の別な一実施例によると、運用管理サーバにて、イベント情報取得対象の情報処理装置をイベント取得対象装置として構成情報に登録し、運用管理サーバに格納した複数のイベント情報から、予め格納したルールに適合するイベント情報を特定し、当該イベント情報が関連するネットワークサービスのサーバ装置を特定し、イベント情報を生成したクライアント情報処理装置で発生した当該イベントの要因がサーバ装置で発生したネットワークサービスに関するイベントと推定されることを表示する。

発明の効果

[0012] 本発明によれば、イベント情報を取得しないＩＴ装置にてイベントが発生した場合も解析結果を表示することができる。

図面の簡単な説明

[0013] [図1]本発明の運用管理システムの全体構成図を示したものである。

[図2]本発明における実施形態の１つである障害解析の全体処理フローを模式的に示したものである。

[図3]本発明が対象とするＩＴシステムの代表的な構成例の一つを模式的に示したものである。

[図4]本発明の運用管理システムで用いられる相関解析ルール情報を模式的に示したものである。

[図5]図４に示した相関解析ルール情報で適用対象として指定されるトポロジを模式的に示したものである。

[図6]ルールの適用先となるＩＴ装置のリストを管理するテーブル状のデータ構造の一例であるルール適用先管理テーブルを模式的に示したものである。

[図7]本発明の実施形態の１つである相関解析ルール情報の適用情報の生成処理フローである。

[図8]本発明の第一実施形態におけるＩＰ－ＳＡＮのクライアントとなる計算機で取得したＩＰ－ＳＡＮストレージ装置の接続情報を模式的に示したものである。

[図9]本発明の第一実施形態における、構成管理で保持する管理対象ＩＴ装置のＩＰ－ＳＡＮストレージに関する構成情報を模式的に示したものである。

[図10]本発明の第一実施形態における、管理外ＩＴ装置を管理対象に含めることをユーザに提案する画面表示例である。

[図11]本発明の第一実施形態における、管理外ＩＴ装置を管理するためのテーブル状のデータ構造の一例である管理外ＩＴ装置管理テーブルを模式的に示したものである。

[図12]本発明の第一実施形態における、ルールの適用先ＩＴ装置のリストを

保有するルール適用先管理テーブルを模式的に示したものである。

[図13]本発明の第一実施形態におけるＦＣ－ＳＡＮのクライアントとなる計算機で取得したＦＣ－ＳＡＮストレージ装置の接続情報を模式的に示したものである。

[図14]本発明の第一実施形態における、構成管理で保持する管理対象ＩＴ装置のＦＣ－ＳＡＮストレージに関する情報を模式的に示したものである。

[図15]本発明の第一実施形態における、ファイルサーバとなる計算機において取得できるファイルサーバに関する識別情報と公開名を模式的に示したものである。

[図16]本発明の第一実施形態における、障害解析結果の画面表示処理フローを模式的に示したものである。

[図17]本発明の第一実施形態における、管理外ＩＴ装置が障害の原因である場合の障害解析結果データの一例を模式的に示したものである。

[図18]本発明の第一実施形態における、管理外ＩＴ装置が障害の原因である場合の障害解析結果の画面表示の構成例を模式的に示したものである。

[図19]本発明の第一実施形態における、管理外ＩＴ装置が障害の原因である場合の障害解析結果の画面表示を模式的に示したものである。

[図20]本発明の第二実施形態における、障害解析の全体処理フローを模式的に示したものである。

[図21]本発明の実施形態の１つである相関解析ルール情報の適用情報の生成処理フローである。

符号の説明

[0014] ＮＯ．．．運用管理サーバ

ＮＮ１乃至Ｎ３．．．計算機

Ｎ４．．．ネットワーク（ＮＷ）スイッチ

Ｎ５．．．ストレージ装置

Ｏ１．．．計算機

Ｏ２．．．ＮＷスイッチ

Ｏ３．．．ストレージ装置

Ｍ１．．．画面出力装置

発明を実施するための最良の形態

[0015] 以下に、本発明の実施の形態を説明する。

実施例 1

[0016] 図１は、本発明を実施するため情報処理システムの１つの構成を示した概観図である。

情報処理システムは運用管理システムと、運用管理サーバから構成される。運用管理システムは、ＩＴシステムを構成する計算機、ネットワークスイッチ（ＮＷスイッチ）、及びストレージ装置を管理対象として、運用管理サーバＮＯでこれらを監視・管理している。

本発明の運用管理サーバＮＯは、管理対象のＩＴ装置における状態変化、障害情報、通知情報などのイベント情報を受信するイベント受信部ＣＯと、受信したイベント情報にもとづき、予め定義されたルールＲＯにもとづいて障害解析を行うルールエンジンＣ１と、管理対象のＩＴ装置の構成情報を管理する構成管理Ｃ３と、これらの運用管理するために必要となる情報を画面に出力するための画面表示部Ｃ２が備わっている。

[0017] また、運用管理システムには、画面表示部の制御と出力データに基づいて、運用管理のための情報を画面に表示するための装置である画面出力装置Ｍ１があり、運用管理サーバＮＯと接続している。なお、画面出力装置Ｍ１としては第一に運用管理サーバに接続されたディスプレイ装置であることが考えられるが、運用管理システムの管理者に解析結果情報を表示することができれば他の装置で代替してもよい。画面出力装置Ｍ１のそのほかの例としては、画面出力装置として運用管理サーバＮＯが送信する電子メールを受信し、表示可能な携帯端末であったり、運用管理サーバＮＯが送信する解析結果情報を元に管理者に情報提供し、また管理者からの入力を受け付けて運用管理サーバＮＯに送信するディスプレイ付計算機がある。

[0018] ルールエンジンＣ１は、さらにイベントの相関解析のための解析ルール情

報ＲＯ（以後、相関解析ルール情報と呼ぶことがある）を読みこみ、構成管理Ｃ３から構成情報ＴＯを取得して、ルールをＩＴシステムのＩＴ装置に適用するための処理を行うルール適用部Ｃ１１と、ルール適用部においてルールをＩＴ装置に適用するための情報である適用情報を管理するルール適用先管理テーブルＣ１３０を管理し、ルールの解析処理を行うためのワーキングメモリであるルールメモリＣ１３と、イベント受信部ＣＯで受信したイベント情報を受け取り、イベントの相関解析を行う、イベント解析処理部Ｃ１２から成る。なお、ルール適用先管理テーブルＣ１３０はルールメモリＣ１３内に存在しなくても、運用管理サーバＮＯのメモリに格納されればよい。

[0019] なお、相関解析ルール情報は運用管理サーバＮＯの管理者によって作成・格納されてもよく、後述する本発明のプログラムに相関解析ルール情報を含めることでメモリに格納してもよく、または本発明のプログラムの初期化処理によって相関解析ルール情報をメモリに格納してもよい。

[0020] なお、運用管理サーバＮＯを構成するハードウェアとしては、プロセッサ、メモリ（半導体メモリ及びＨＤＤに代表される二次記憶装置を含む）、ネットワークポートがある。それぞれのハードウェアはバス等の内部ネットワークによって接続される。なお、イベント受信部ＣＯ、ルートエンジンＣ１、画面表示部Ｃ２、構成管理Ｃ３は運用管理サーバＮＯのメモリに格納され、プロセッサによって実行されるプログラムとして実現されることが第一に考えられるが、これら機能の一部または全てをハードウェアで実現してもよい。なお、以後の説明ではイベント受信部ＣＯ、ルートエンジンＣ１、画面表示部Ｃ２、構成管理Ｃ３を含むプログラムをイベント解析プログラムと呼ぶ。

[0021] また、また、相関解析ルール情報ＲＯ、構成情報ＴＯ、ルール適用先管理テーブルＣ１３０は、運用管理サーバＮＯのメモリに格納されている。さらに、構成情報ＴＯは後ほど説明する、ＩＰ－ＳＡＮストレージ装置の接続情報（図８）、ＩＰ－ＳＡＮストレージに関する情報（図９）、ＦＣ－ＳＡＮストレージ装置の接続情報（図１３）、ＦＣ－ＳＡＮストレージに関する情

報（図１４）、ファイルサーバに関する識別情報と公開名（図１５）の少なくとも一つが含まれる。また、後ほど説明する管理外ＩＴ装置管理テーブル（図１１）についても構成情報に含まれるものとして説明するが、運用管理サーバＮＯのメモリに格納されていれば構成情報ＴＯ以外の情報として格納されていてもよい。

[0022] さらに、相関解析ルール情報ＲＯ、構成情報ＴＯ、ルール適用先管理テーブルＣ１３０、ＩＰ－ＳＡＮストレージ装置の接続情報、ＩＰ－ＳＡＮストレージに関する情報、ＦＣ－ＳＡＮストレージ装置の接続情報、ＦＣ－ＳＡＮストレージに関する情報、ファイルサーバに関する識別情報と公開名、管理外ＩＴ装置管理テーブルについてはテキストファイルやテーブル、キュー構造など特定のフォーマット、データ構造である必要はなく、後ほど説明する情報が含まれていればよい。以後の説明及び請求項にてより一般的な情報であることを明記するため、相関解析ルール情報ＲＯ、構成情報ＴＯ、ルール適用先管理テーブルＣ１３０、ＩＰ－ＳＡＮストレージ装置の接続情報、ＦＣ－ＳＡＮストレージ装置の接続情報、ＩＰ－ＳＡＮストレージに関する情報、ＦＣ－ＳＡＮストレージに関する情報、ファイルサーバに関する識別情報と公開名、管理外ＩＴ装置管理テーブルを、それぞれ相関解析ルール情報情報、構成情報、ルール適用先管理情報、ＩＰ－ＳＡＮストレージ装置の接続情報、ＦＣ－ＳＡＮストレージ装置の接続情報、ＩＰ－ＳＡＮストレージに関する情報、ＦＣ－ＳＡＮストレージに関する情報、ファイルサーバに関する識別及び公開名情報、管理外ＩＴ装置管理情報と呼ぶことがある。

[0023] なお、図示はしていないが、運用管理サーバは管理対象の様々なＩＴ装置から受信するイベント情報をイベントエントリとしてメモリ内に定義したイベントデータベースに格納する。なお、イベントデータベースは一つ以上のイベントエントリが含まれていればどのようなデータ構造であっても良い。

[0024] なお、イベント情報はイベント内容が含まれるが、イベント発生時間を含んでもよい。さらにイベントデータベースは過去のイベント情報を定められた条件に従って履歴として残しても良い。また、イベントデータベースに含

め、メモリに格納する場合は、運用管理サーバのプログラム（特に構成管理Ｃ３）はイベント情報取得対象のＩＴ装置の識別情報と、運用管理サーバによるイベント情報受信時間と関連付け、共に含めるようにしてもよい。なお、イベント内容は少なくともイベントの種別が含まれ、場合によっては当該イベントが発生ＩＴ装置内のハードウェア及びソフトウェアを特体する情報が含まれてもよい。

[0025] またイベントの種別としては例えば以下が考えれれるが、これ以外の種別が存在してもよい。

（Ａ）当該ＩＴ装置のの稼動状態が予め定められた状態となったこと（例えばハードウェア障害や、ソフトウェア障害の発生がこれに含まれる）

（Ｂ）ヘルスチェック結果が予め定められた結果となったこと。（例えば一定時間ヘルスチェック応答が無かった場合がこれに含まれる）

（Ｃ）処理速度やＩＴ装置を構成するコンポーネントであるプロセッサやメモリ、ＨＤＤなどの消費リソース量が予め定められた条件に適合したこと（例えばＨＤＤの残り容量が１０％を下回った場合がこれに含まれる）

（Ｄ）ＩＴ装置が予め定められた条件を満たすネットワークアクセスを受信したこと（例えば、ＩＴ装置が受信したリクエストが所定の回数を超えた場合や、リクエストされたＤｏＳ攻撃と識別されるネットワークパケットを所定回数受信した場合や、定められたＩＴ装置以外のＩＴ装置からリクエストを受信した場合がこれに含まれる）

なお、イベント解析プログラムのメモリへの格納は当該プログラムを記憶したＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等の媒体からのインストールやコピーによる方法や、運用管理サーバＮＯと通信可能なプログラム配布サーバからの当該プログラム（または当該プログラムをメモリ上で生成可能な情報）を受信する方法が考えられるが、これ以外の方法であってもよい。また、運用管理サーバＮＯへのプログラム格納を予め格納した後で運用管理サーバＮＯを流通させる形態であってもよい。

[0026] 以上説明した運用管理サーバＮＯによって情報処理システムの障害の根本

原因を解析する。

[0027] なお、運用管理システムでは、予め管理する対象のＩＴ装置を指定し、イベント情報を相関解析による解析対象として当該ＩＴ装置から必要な情報を受信する。このように運用管理システムにおいて、受信するＩＴ装置を定めるのは、ネットワークに接続されたＩＴ装置を全て管理することは、管理するために必要となる管理サーバのプロセッサ、メモリ、ハードディスクなどの記憶装置などの消費量が膨大となり、実用的な監視が困難であるため、管理する対象を絞ることでこれを回避するためである。また、管理ツールが商用のものである場合には、管理するＩＴ装置の種類や台数などによりライセンス数に制限がある場合がほとんどである。このためＩＴシステムにおいては、イベント情報解析のために、運用管理サーバＮＯがイベント情報を取得するまたは取得を許可されているＩＴ装置（以後、監視されるＩＴ装置、又は管理されるＩＴ装置又は管理ＩＴ装置又は管理内ＩＴ装置又はイベント取得対象装置と表現することがある。なお同様の表現はＩＴ装置の実態である計算機、スイッチ、ルータ、ストレージ装置に対しても適用する）と、運用管理サーバＮＯがイベント情報取得を取得しない又は取得を抑止されているＩＴ装置（以後、監視されないＩＴ装置、又は管理されないＩＴ装置又は管理外のＩＴ装置又は管理外ＩＴ装置又はイベント関連情報処理装置と表現することがある。なお同様の表現はＩＴ装置の実態である計算機、スイッチ、ルータ、ストレージ装置に対しても適用する）が存在する。

[0028] 運用管理サーバＮＯにおいて監視・管理されないＩＴ装置については、さらに、一度でも運用管理サーバＮＯにおいて存在を発見、又は確認、又は管理されたことがあるＩＴ装置と、一度も運用管理サーバＮＯにおいて、その存在を発見、又は確認、又は管理されたことがないものに分類される。運用管理サーバＮＯによっては、一度でも管理したことがあるＩＴ装置、又は発見、又は確認したことがあるＩＴ装置については、監視・管理されているＩＴ装置と同等とはいわないまでも、当該発見または確認によって取得した構成情報、例えばＩＴ装置のＩＰアドレス、又はホスト名、又はＦＱＤＮ（Ｆ

ｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）などを内部に保持して管理するものもある。本発明では、対応する構成情報を運用管理サーバＮＯが持たない管理対象外のＩＴ装置と、対応する構成情報の一部又は全てを運用管理サーバＮＯに格納済みの管理対象外のＩＴ装置とを含めて、管理対象外のＩＴ装置として定義する。

[0029] 運用管理システムの管理対象外であるケースとしては、ＤＮＳサーバのようにグローバルに提供されたサービスを管理対象内のＩＴ装置が利用している場合や、ファイアーウォール、アクセス権の問題、ネットワーク構成、アクセス手段の不備などの事情により、運用管理システムが管理するための情報収集を十分に行えない場合などがある。

[0030] なお、本発明はネットワーク上に存在する複数のＩＴ装置同士の相関解析を対象としている。しかし、本来相関のある複数装置である要因によるイベントが同時発生したとしても個々の装置のクロックにはずれが生じ、さらにイベント情報転送のタイミングにもずれが生じるため、運用管理サーバＮＯが解析対象とするイベント情報はプログラム開発者が予め定めたられた時間幅（期間）または管理者が定めた期間内に発生または受信したイベント情報を解析する。また、ある要因が発生したとしても当該要因に関係するイベントの発生はずれが生じることがあるため（例えば、ＷｅｂサービスやＤＮＳサービス等、サーバ計算機からキャッシング処理を介在させて所定のネットワークサービスを受ける場合）、特定の時間ではなくて期間を対象とした解析が必要となる。

[0031] なお、イベントとして好適なものはある程度動的に発生する事項であることが好ましい。さらには、所定の要因が発生して要因となるＩＴ装置でのイベントが発生（または運用管理サーバが受信）する時間と、当該要因を受けて別なＩＴ装置でのイベントが発生（または運用管理サーバが受信）する時間の差が、前記期間内であるイベントの要因であることがより好適である。

[0032] 一方の構成情報として考えられる情報は、ＩＴ装置を構成するハードウェアの種類及び個数や、当該装置と通信するために必要な通信識別情報や名前

といったものが好適であり、一部ＩＴ装置の管理者によって変更は可能であるが準静的な情報が好適である。

[0033] 図２は、上記の構成にもとづく本発明における実施形態の１つの大まかな処理の流れを示したものである。

[0034] Ｓ１においてルールエンジンＣ１は、予め相関解析ルール情報Ｒ０を読み込み、構成管理Ｃ３から管理対象の構成情報Ｔ０を取得して、ルール群Ｒ０の適用先のＩＴ装置の識別情報をＴ０から検索して、ルール適用先管理テーブルＣ１３０に格納しておく。Ｓ１の処理は、この後に行うイベントによる障害解析処理のための準備であり、解析処理の前までに行えばよい。実施形態の１つである第一実施形態では、解析処理を運用開始前に行い、予めルール適用先管理テーブルＣ１３０をルールメモリＣ１３内に保持しているものとする。

[0035] Ｓ２においては、イベント受信部Ｃ０にて、運用管理システム内の管理対象のＩＴ装置から上げられるイベントの受信待ちうけを行う。

[0036] Ｓ３では、運用管理システムの運用操作に関するものであり、停止処理が指示されたかどうかを確認するためのステップであり、運用の停止を行うためのものである。

[0037] Ｓ４においては、イベント受信部Ｃ０でイベントを受信したかどうかの判断を行う。受信した場合には、Ｓ５においてイベント受信部Ｃ０より受信したイベントをイベント解析処理部Ｃ１２に入力して、ルール適用先管理テーブルＣ１３０にもとづいて該当するルールを求めて、該ルールに従い障害原因を特定する。

[0038] Ｓ５においては、特定した障害原因を画面表示部Ｃ１４に出力する。画面表示部Ｃ１４は、受け取った解析結果出力データを元に解析情報を送信することで、画面出力装置Ｍ１に運用管理に必要な画面を出力・表示する。

[0039] なお、Ｓ２及びＳ４の処理の代替として受信したイベント情報を一旦イベントデータベースに格納してもよい。

[0040] この大まかな処理の流れにおいて、ルール適用部の処理に手を加えること

で、構成やその後の処理の流れを大幅に変えることなく、管理対象でないＩＴ装置の障害の原因解析を行えることが本発明の効果の１つである。

[0041] 図３は、本発明の実施形態で想定するＩＴシステムの構成の１つを示した概観図である。図３のＩＴシステムは、管理サーバＮ０が運用管理する計算機Ｎ１０、計算機Ｎ１１、計算機Ｎ１２と、ネットワークスイッチであるＩＰスイッチＮ２１とＦＣスイッチＮ３１、ストレージ装置Ｎ４０とストレージ装置　Ｎ４１で構成される運用管理対象である運用管理システムと、管理サーバＮ０が管理しない管理対象外のＩＴ装置としてストレージ装置Ｕ２と計算機Ｕ５と、ルータＮ２０を介してネットワークＧ０に接続されるストレージ装置Ｕ１と、計算機Ｕ３と計算機Ｕ４と、から構成される。なお、個々で記した計算機、スイッチ、ルータ、ストレージ装置等のＩＴ装置の個数は一例であり、少なくともネットワークサービスを提供するサーバの役目を持ったＩＴ装置と、当該ネットワークサービスの提供を受けるクライアントの役目を持ったＩＴ装置が運用管理システムに含まれていればよい。

[0042] 管理対象外のＩＴ装置のストレージ装置Ｕ１はＩＰ－ＳＡＮのインタフェースを備えるストレージ装置であり、管理対象の計算機Ｎ１０に対して論理ボリュームを提供している。また、管理対象外のＩＴ装置のストレージ装置Ｕ２はＦＣ－ＳＡＮのインタフェースを備えるストレージ装置であり、管理対象のＦＣスイッチＮ３１を介して管理対象の計算機Ｎ１３に対して論理ボリュームを提供している。管理対象外のＩＴ装置の計算機Ｕ３又は計算機Ｕ５はファイルサーバであり、それぞれ管理対象の計算機Ｎ１０、Ｎ１１の両方にファイルシステムを公開しているが、計算機Ｕ３は運用管理システムとは違うネットワークセグメントに属しており、計算機Ｕ３に関する詳細な情報はネットワーク上から取得できないようになっている。

[0043] 一方で、計算機Ｕ５のファイルサーバは、運用管理システムと同一のネットワークセグメントに属しており、運用管理システムにより自動で存在を発見することができる計算機で、運用時に発見されたが、管理対象とはされなかったＩＴ装置である。また、管理対象外のＩＴ装置の計算機Ｕ４はＤＮＳ

サーバであり、図３のＩＴシステムの全てのＩＴ装置に対して名前解決機能を適用している。

[0044] ここでは理解のために第一実施形態について述べる前に、管理対象のＩＴ装置に対し、イベント相関技術のルールをどのように適用するかについて説明する。

[0045] 図４は、図１で示したＩＴシステムに対して、ストレージ装置のコントローラの障害が根本原因であることを示唆するルールの例である。こうした障害解析の根本原因を特定するルールは、イベント相関に基づき、発生すると予測されるイベントの組み合わせと、根本原因となる障害のペアをｉｆ－ｔｈｅｎ形式で示すことが多い。ｉｆ－ｔｈｅｎ形式のルール表現においては、“もしｉｆ に記述された条件が成立するならば、ｔｈｅｎ部分が真である”のような意味のルールを表記する。

[0046] 実施例では、エキスパートシステムなどの一般的なルールと同様にｉｆ－ｔｈｅｎの形式でルールが記述されているものとし、ルールの適用対象となるＩＴ装置に関する情報がｉｆの条件部分に予め定義されているものとする。なお、ルールの記述形式自体はｉｆ－ｔｈｅｎ形式でなくても良く、ルールを適用する対象となるＩＴ装置が特定できる何かしらの接続・関係情報としてトポロジが予め定義されていればよい。

[0047] なお、それぞれのルールを実際に格納する情報はルールエントリである。相関解析ルール情報は一つ以上のルールエントリを含む。なお、より抽象化すると当該ルールエントリは以下の情報が含まれると言っても良い。

（Ａ）当該ルールが適合するイベントの種別を含んだ条件を示す条件エントリ。上記の通り、この条件エントリにはトポロジを条件として含めてもよい。

（Ｂ）当該条件が適合した場合に原因となるイベントと、当該イベントが関係するＩＴ装置又はＩＴ装置のハードウェア・ソフトウェアの箇所を表す原因エントリ。

[0048] 第１実施例として、ｉＳＣＳＩを利用したＩＰ－ＳＡＮのストレージ装置

のコントローラ障害を根本原因とするルールＲ１と、Ｆｉｂｒｅ　Ｃｈａｎｎｅｌを利用したＦＣ－ＳＡＮのストレージ装置のコントローラ障害を根本原因とするルールＲ２と、ファイルサーバの障害を根本原因とするルールＲ３と、ＤＮＳサーバへのネットワーク不到達を根本原因とするルールＲ４が図４に示すように予め定義されているものとする。また、図６には、ルールに対して、該ルールを適用するＩＴ装置を保持する情報である、ルール適用先管理テーブルを示した。ルール適用先管理テーブルは、ルールを指し示す識別情報のカラムＣ１０１とそのルールを適用させる対象のＩＴ装置の識別情報を格納する適用先ＩＴ装置のリストのカラムＣ１０２から成る情報であり、データベース上のテーブルである必要はない。なお、本テーブル状のデータ構造は、テーブルを正規化することにより、複数のテーブル状のデータ構造に分割して管理されていてもよい。

[0049] 図３で示したルールＲ１乃至Ｒ４に対して、それぞれのルールを適用させるトポロジのパターンを図５に示した。図５の（１）は、ルールＲ１のＩＦ部が示唆する接続・関係情報のトポロジを示しており、計算機を示すＣｏｍｐｕｔｅｒが、ｉＳｃｓｉＩｎｉｔｉａｔｏｒを持ち、ＩＰスイッチを示すＩｐＳｗｉｔｃｈを介して、ストレージ装置を示すＳｔｏｒａｇｅのｉＳｃｓｉＴａｒｇｅｔと接続されていることを示す。ｉＳｃｓｉＴａｒｇｅｔは、ｉＳｃｓｉＩｎｉｔｉａｔｏｒの接続先を識別するためのｉＳＣＳＩ名であり、計算機が持つ接続先のｉＳｃｓｉＴａｒｇｅｔと、ストレージ装置が持つｉＳｃｓｉのポートのｉＳＣＳＩ名が一致する計算機とストレージ装置の組み合わせに対してルールＲ１が適用される。図３で示されるＩＴシステムにおいては、ルールＲ１の適用先のＩＴ装置は図６のＬ１０１とＬ１０２の行のようになる。

[0050] また、図５の（２）についても同様に、ルールＲ２のＩＦ部が示唆するように、計算機がＦｃＨｂａを備え、ＦｃＨｂａがＦｃＳｗｉｔｃｈを介して、ストレージ装置のＦｃＰｏｒｔに繋がっていることを示す。このとき、ＦｃＨｂａが持つ接続先ポートWWN（WWN： Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎ

ａｍｅ）と、ストレージ装置のＦｉｂｒｅ　Ｃｈａｎｎｅｌのポートである
ＦｃＰｏｒｔのWWNであるＦｃＰｏｒｔWWNは一致しているものを接続
関係があるものとしてルールＲ２の適用対象とする。図３のＩＴシステムに
おいて、これらの計算機とストレージ装置の組み合わせとしてルールＲ２の
適用先のＩＴ装置は図６のＬ１０３の行になる。

[0051] 図５の（３）については、ルールＲ３のＩＦ部がファイルサーバークライ
アントのトポロジを示している。ファイルサーバのファイルシステムをマウ
ントしていることを示す情報ＩｍｐｏｒｔｅｄＦｉｌｅＳｈａｒｅを持つコ
ンピュータＴ３１と、外部にファイルシステムを公開していることを示す情
報ＥｘｐｏｒｔｅｄＦｉｌｅＳｈａｒｅを持つコンピュータＴ３３は、ＩＰ
スイッチＴ３２を介してそれぞれクライアントーファイルサーバの関係であ
る。このとき、ＩｍｐｏｒｔｅｄＦｉｌｅＳｈａｒｅ　Ｔ３１１にはマウン
ト元のファイルサーバに関する情報として、ファイルサーバの識別情報（Ｉ
ＰアドレスやＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ
Ｎａｍｅ）など）と、公開しているファイルシステムの公開名を持ち、Ｅｘ
ｐｏｒｔｅｄＦｉｌｅＳｈａｒｅ　Ｔ３３１には、公開しているファイルシ
ステムの場所と公開名（共有名とも呼ばれる）を持つ。

[0052] ＩｍｐｏｒｔｅｄＦｉｌｅＳｈａｒｅが指しているファイルサーバの識別
情報で示されるコンピュータで、なおかつそのコンピュータがＥｘｐｏｒｔ
ｅｄＦｉｌｅＳｈａｒｅの情報を持ち、ＥｘｐｏｒｔｅｄＦｉｌｅＳｈａｒ
ｅの公開名がコンピュータＴ３１のＩｍｐｏｒｔｅｄＦｉｌｅＳｈａｒｅが
指している公開名と一致するコンピュータのペアをファイルクライアントー
ファイルサーバのトポロジとしてルールＲ３を適用する。したがって、図３
のＩＴシステムにおいては、これを満たす組み合わせとしてルールＲ３の適
用先のＩＴ装置は図６のＬ１０４の行になる。

[0053] 図５の（４）については、ルールＲ４が示唆するＤＮＳサーバとクライア
ントのトポロジであり、名前解決サービスを提供しているＤＮＳサーバであ
るコンピュータＴ４２と、ＤＮＳサーバによりＩＰアドレスとＦＱＤＮの名

前を解決しているクライアントのコンピュータＴ４１がペアとなって、図６に示す適用先管理テーブルに格納される。

[0054] こうしたルールに記述された接続や関係に関するトポロジ情報に対する構成は、予めシステムで定義されているものとし、ルールの記述によって一意に定められる。

[0055] ルールに対する適用先のＩＴ装置に関しては図６の適用先管理テーブルを持つことにより、イベント発生時にこのテーブルを参照することで、イベントがどのルールに関連するものなのかを判断し、適用すべきルールを選択することができる。以上が、管理対象のＩＴ装置に対するルールの適用方法である。

[0056] 図７及び図２１は、図２のルール適用部Ｃ１１におけるステップＳ１について、本発明の実施形態の１つを詳細化したものである。この処理フローに従い、図３のＩＴシステムと、図４のルールＲ１乃至Ｒ４を想定して第一実施形態を説明する。なお、図７及び図２１の処理は、全てルール適用部において行われるものである。また、予め運用管理システムは、一度発見したことがあるＩＴ装置について記憶しており、発見済みのＩＴ装置であると判断できることを前提とする。あるいは、運用管理システムが、ＩＴシステム内のＩＴ装置を自動で発見する機能を持たない場合、又は自動で発見する機能を持っていても、発見したＩＴ装置について記憶する機能がない場合には、発見済みのＩＴ装置は存在しないものとして図７及び図２１の処理を行う。

[0057] （一般的なフローの説明及びルールＲ１を適用した場合について）

Ｓ１０１において、相関解析ルール情報情報Ｒ０に読み込むルール、すなわち読み込み済みでないルールが存在するかを判断する。判断の結果、読み込むルールが存在する（ＹＥＳの）場合には、Ｓ１０２に移る。そうでなければ（ＮＯの場合）終了する。読み込むルールはＲ１乃至Ｒ４と存在するので、ここではＹＥＳとなりＳ１０２に移る。

[0058] Ｓ１０２においては、ルールを１つ読み込み、読み込み済みとわかるように、例えばしるしをつけたり、読み込み済みのルールとして記憶したりする

。実施形態では、ルールのＲ１を読み込み、ルールＲ１を読み込み済みルールとして記憶してＳ１０３に移る。

[0059] Ｓ１０３においては、ルールに記述されたトポロジ情報に対応するＩＴ装置の検索条件を求めてＳ４に移る。実施形態では、ルールＲ１のトポロジ情報として、ｉＳｃｓｉＩｎｉｔｉａｔｏｒを持つ計算機と、ｉＳｃｓｉＴａｒｇｅｔで識別されるｉＳＣＳＩのポートを持つストレージ装置、およびこれらに接続されたＩＰスイッチがルールＲ１を適用するＩＴ装置の検索条件となる。検索条件は、予めルールの記述に対して定義されているものとする。

[0060] Ｓ１０４においては、トポロジ情報のうち、クライアント側のＩＴ装置を管理対象のＩＴ装置の構成情報から検索する。なお、構成情報の検索は、構成情報を管理しているものがデータベースであればデータベースに対して行い、ファイルであればファイルに対して行い、検索対象とする記憶メディアやデバイスなどは問わない。実施形態では、ルールＲ１のトポロジにおいてクライアントを示す、ｉＳｃｓｉＩｎｉｔｉａｔｏｒを持つ計算機を構成情報から検索する。本実施例では、計算機Ｎ１０又は計算機Ｎ１１がｉＳｃｓｉＩｎｉｔｉａｔｏｒを持つものとすると、計算機Ｎ１０と計算機Ｎ１１の識別情報が検索により見つかる。

[0061] Ｓ１０５においては、Ｓ１０６以降の処理を複数の計算機の場合について実行するため、検索で見つかったＩＴ装置で未選択なＩＴ装置があるかを判断する。本実施例では、計算機Ｎ１０と計算機Ｎ１１が未選択なＩＴ装置であるためＳ１０６に進む。

[0062] Ｓ１０６においては、未選択なＩＴ装置から１つを選択し、選択済みとする。本実施例では計算機Ｎ１０を選択し、計算機Ｎ１０を選択済みとしてＳ１０７に進む。

[0063] Ｓ１０７においては、Ｓ１０６に於いて選択したＩＴ装置とトポロジ上で対向となるサーバ側のＩＴ装置の情報を取得する。ここでサーバ側のＩＴ装置の情報としては、サーバ側のＩＴ装置を識別する情報（ＩＰアドレス、又

はホスト名、ＦＱＤＮなど）や、提供するサービスに関する情報（ファイルサーバにおける公開ファイルシステムの公開名（共有名とも呼ばれる）や、ストレージ装置のディスクボリュームを識別するＬＵＮ番号、あるいは接続先のｉＳＣＳＩ名、またはＦＣ　ＰｏｒｔのWWN）がある。本実施例では、計算機Ｎ１０に対向するサーバ側のストレージ装置の情報として、図８に示す接続先のｉＳＣＳＩ名であるＣｏｎｎｅｃｔｅｄＩｓｃｓｉＴａｒｇｅｔを取得する。

[0064] Ｓ１０８においては、Ｓ１０７で取得したサーバ側のＩＴ装置に関する情報のうち、その情報に対応するＩＴ装置を検索していないものが存在するかを判断し、存在する（ＹＥＳ）場合にはＳ１０９に、存在しない（ＮＯ）場合にはＳ１０５に移る。本実施例では、図８に示すように少なくとも３つの未検索の情報が存在する（ＹＥＳ）ため、Ｓ１０９に移る。

[0065] なお、ここで図８に含まれる情報を説明すると、当該情報にはＩＴ装置（より具体的には計算機）を示す識別情報と、当該ＩＴ装置が接続先とするストレージ装置のｉＳＣＳＩにおける識別情報を有する。

[0066] Ｓ１０９においては、Ｓ１０７で取得したサーバ側のＩＴ装置の情報のうち、未検索のものを１つ選択し、この情報を元にサーバ側のＩＴ装置を管理対象の構成情報から検索する。本実施例では、計算機Ｎ１０より取得した図８に示されるＣｏｎｎｅｃｔｅｄＩｓｃｓｉＴａｒｇｅｔのＬ２０１行で示されるｉＳＣＳＩ名をｉＳｃｓｉＴａｒｇｅｔに持つストレージ装置を管理対象の構成情報から検索する。

[0067] Ｓ１１０において、Ｓ１０９の検索の結果、管理対象のＩＴ装置に該当するものが存在しない（ＮＯ）場合には、Ｓ１１１に移る。一方で、管理対象のＩＴ装置に該当するものが存在する（ＹＥＳ）場合には、通常のルール適用処理と同様となり、Ｓ１２１に移る。本実施例では、管理対象のストレージ装置のｉＳｃｓｉＴａｒｇｅｔに関する構成情報は図９に示したものとする。このとき、図８のＬ２０１行のＣｏｎｎｅｃｔｅｄＩｓｃｓｉＴａｒｇｅｔと一致するｉＳｃｓｉＴａｒｇｅｔを持つストレージ装置は図９に示し

たように管理対象には存在しないため、Ｓ１１１に移る。

[0068] なお、ここで図９に含まれる情報を説明すると、当該情報にはストレージ装置を示す識別情報と、当該ストレージ装置が有するｉＳＣＳＩにおける識別情報を有する。

[0069] なお、発見済みの一つ以上のＩＴ装置毎に当該装置がイベント取得対象であるかどうか（すなわち当該装置が監視される装置であるかどうか、言い方を代えると当該装置に対するイベント取得を許可しているか抑止しているか）を示すイベント取得可否情報が構成情報Ｔ０に含まれており、当該データを参照することでＳ１１０の判断を行う。

[0070] Ｓ１１１においては、運用管理システムにおいて既に発見したことがあるＩＴ装置であるかどうかを判断する。すなわち、運用管理システムにおいて、一度でも存在を発見、又は確認、又は管理されたことがあるＩＴ装置であって、部分的に運用管理システムが静的構成情報を持つようなＩＴ装置であるかどうかをここでは判断する。本実施例では、図８のＬ２０１行のＣｏｎｎｅｃｔｅｄＩｓｃｓｉＴａｒｇｅｔと一致するｉＳｃｓｉＴａｒｇｅｔを持つストレージ装置に関する構成情報は一切なく、発見済みリソースでない（ＮＯ）であるものとしてＳ１１２に進む。

[0071] なお、Ｓ１１１の判断は構成情報に当該装置に関する情報（例えばイベント取得可否情報）が存在するかどうかで判別する方法がある。

[0072] Ｓ１１２において、図８のＬ２０１行のＣｏｎｎｅｃｔｅｄＩｓｃｓｉＴａｒｇｅｔと一致するｉＳｃｓｉＴａｒｇｅｔを持つストレージ装置を、管理外のＩＴ装置から発見を試みる。Ｓ１１２の管理外ＩＴ装置の有無の検索方法の一例としては、構成情報より取得、又はユーザにより入力された対象となるリソースに対応するＩＰアドレスやＦＱＤＮなどの通信識別子、又は構成情報から取得、又はユーザにより入力された対象となるリソースを含むネットワークセグメントに対応するＩＰアドレスであるネットワークアドレス内のＩＰアドレス、又はＦＱＤＮなどの通信識別子に対して、対象となるリソースに関するサービス提供を求めるリクエストを送信し、その応答の有

無を待って対象とするリソースの存在を確認する方法がある。本実施例では、図３に示すＩＴシステムから発見を試みる。

[0073] Ｓ１１３においては、Ｓ１１２で試みた発見が成功したかどうかを判断する。成功した（ＹＥＳ）場合にはＳ１４に移る。さもなければ（ＮＯ）Ｓ１１６に移る。本実施例では、図３に示すストレージ装置Ｕ３が該当するストレージ装置として発見されたものとしてＳ１１４に移る。

[0074] Ｓ１１４においては、Ｓ１１３に於いて発見したＩＴ装置を、運用管理システムの管理対象とすることができるかどうかを判断する。管理対象とすることができるかどうかの判断は、その運用管理システムが監視・管理するために必要となる情報が、対象のＩＴ装置から取得できるかどうかで判断する。監視・管理するために必要となる情報については、運用管理システムごとに様々であるが、共通的なものとしては、そのＩＴ装置を識別する情報、例えばＩＰアドレス、又はWWN（Ｗｏｒｌｄ Ｗｉｄｅ Ｎａｍｅ）、又は何かしらのユニークな識別情報（番号）、装置名（ホスト名）、ＦＱＤＮなど、少なくとも１つ以上の情報である。

[0075] また、そのＩＴ装置を構成するハードウェアの種類または個数に関する一つ以上の情報も、ある程度は取得できるほうが好ましい。本発明では、運用管理サーバＮ０が所定の判断基準を持ち、その判断基準によってこの判断を行うものとする。本実施例では、ストレージ装置Ｕ３に関する情報として、このストレージ装置がｉＳＣＳＩのポートを備え、そのｉＳＣＳＩポートのｉＳＣＳＩ名としてｉＳｃｓｉＴａｒｇｅｔの情報が取得できるものとし、管理対象にすることができると判定されたものとしてＳ１１５に進む。なお、続く処理にて当該装置を管理対象とする場合があるため、本ステップにて当該ＩＴ装置からイベント情報が受信可能であることを確認処理に加え、確認できた場合のみＳ１１５に進むようにしてもよい。

[0076] Ｓ１１５においては、Ｓ１１３において発見されたＩＴ装置を管理対象とするかどうかをユーザに提示する。本実施例では、ストレージ装置Ｕ３が計算機Ｎ１のストレージサーバとして発見されたことと、ストレージ装置Ｕ３

を管理対象に入れるかどうかを提示する。提示画面は、図１０である。

[0077] Ｓ１１６においては、運用管理サーバＮＯ（特にルールエンジン）は管理画面出力装置からの入力を受信する。

[0078] Ｓ１１７において、ユーザが発見したＩＴ装置を管理対象としたかどうかを判断し、管理対象とした（ＹＥＳ）場合にはＳ１１８に進み、そうでなければ（ＮＯ）Ｓ１１９に進む。本実施例においては、ユーザはストレージ装置Ｕ３を管理対象としなかったものとしＳ１１９に進む。

[0079] Ｓ１１８においては、ユーザが管理対象に含める判断をしたＩＴ装置に対して情報を取得し、管理対象のＩＴ装置として構成管理に情報を格納する。本実施例では、この時点ではこちらの分岐には来ていない。

[0080] Ｓ１１９においては、クライアントと対向となるサーバを、管理外ＩＴ装置として管理外ＩＴ装置管理テーブルに取得可能な情報について格納して管理し、Ｓ１２０に進む。本実施例では、ストレージ装置Ｕ３について、装置を識別する情報としてＦＱＤＮと、ストレージ装置のＩＰポートのｉＳＣＳＩ名であるｉＳｃｓｉＴａｒｇｅｔが取得可能な情報であるものとし、これを図１１の管理外ＩＴ装置管理テーブルＴＬ３に格納する。

[0081] なお、ここで図１１の説明を行うと、管理害ＩＴ装置管理テーブルＴＬ３には発見した管理外ＩＴ装置の各々について以下の情報を含む。

（Ａ）管理外ＩＴ装置の識別情報

（Ｂ）管理外ＩＴ装置の種別であるＣ４０１

（Ｃ）管理外ＩＴ装置の通信識別情報であるＣ４０２

（Ｄ）管理外ＩＴ装置のサービスにアクセスするために必要な識別情報であるＣ４０３

Ｓ１２０においては、管理外ＩＴ装置の識別情報を、該ＩＴ装置が管理外であることがわかるような印をつけた上で、図１２に示すようにルール適用先管理テーブルＴＬ１に格納する。本実施例では、ストレージ装置Ｕ３に関する管理外ＩＴ装置管理テーブルの情報を元に識別情報を、ルール適用先管理テーブルＴＬ１に格納する。格納した後、選択したクライアント側のＩＴ

装置に対向するサーバ側のＩＴ装置に関する検索情報が存在するかについてＳ８に戻る。

[0082] 本実施例において、Ｓ１０８に戻ると、Ｓ１０７に於いて取得したサーバ側のストレージ装置に関する検索情報で未検索のものが存在するかを判断するが、計算機Ｎ１０に関するサーバ側のストレージに関する検索情報は図８のＬ２０２の行が存在するため、Ｓ１０９に移る。

[0083] Ｓ１０９に移ると、Ｌ２０２に対応するストレージ装置を構成管理にて検索する。実施例では図９のように、Ｌ２０２に対応するストレージ装置が存在するため、Ｌ２０２に対するＩＴ装置は管理対象であることがわかるので、Ｓ１１０において管理対象のＩＴ装置であると判断してＳ１２０に移る。Ｓ１２０では、管理対象のＩＴ装置としてストレージ装置Ｎ４０と計算機Ｎ１０のリストをルールＲ１の適用先ＩＴ装置として図１１のルール適用先管理テーブルのＬ１０１に格納する。

[0084] 以上のステップにより、計算機Ｎ１０に対して論理ボリュームを提供している管理対象外のストレージ装置Ｕ１を含めてルールＲ１を適用できるようになる。

[0085] 次に図１１のルール適用先管理テーブルを用いて、図２のＳ６の一例、つまり管理外のストレージ装置Ｕ１で障害が発生した場合に、前記ストレージ装置Ｕ１を障害の根本原因として画面表示する処理について説明する。

[0086] ストレージ装置Ｕ１からコントローラの障害イベントが発生し、図１のイベント解析処理部Ｃ１２において図１１のルール適用先管理テーブルを元にルールによるイベント相関によって障害の原因箇所を特定されると、解析結果の情報が、画面表示部Ｃ２に送信される。画面表示部Ｃ２では、図１６のフローにもとづき、根本原因のＩＴ装置が管理対象かどうかを判断して、適切な画面を画面表示装置Ｍ１に表示させる。

[0087] 図１６のステップ６０１から６０３において画面標示部Ｃ２において、図１７に示したルールエンジンにおける障害解析の結果を示す障害解析結果データＤ１をルールエンジンＣ１から取得する。なお、ルールエンジンＣ１（

特にイベント処理解析部Ｃ１２）は図２のＳ４及び図４及び図５にて説明した処理を行っている。

[0088] 障害解析結果データＤ１は、障害原因ＩＴ装置に関する情報である障害原因ＩＴ装置情報と、運用管理システムが受信した管理対象のＩＴ装置のイベントに関する情報である受信イベントリストと、を含むデータから成る。障害原因ＩＴ装置情報Ｄ１１は、障害原因ＩＴ装置を示す情報と、障害箇所の部位に関する情報を含む。障害箇所の部位に関する情報は、管理対象外のＩＴ装置である障害原因ＩＴ装置からどの程度の障害情報を取得できるかによる。全く障害情報を取得できない場合には、図１７のように不明となる。受信イベントリストは、この障害について定義されているルールにおいて、関連がある受信イベントに関する情報である、受信イベントの発信元に関する情報である受信イベント発信元と、イベントの内容に関する情報を示すイベント種別とを含む。

[0089] Ｓ６０４において、取得した障害解析結果データＤ１１の障害原因ＩＴ装置の情報から、管理対象か管理対象外かを判断する。本実施例では管理対象外のＩＴ装置であるため、Ｓ６０５に進む。

[0090] Ｓ６０５では、障害解析結果データＤ１１の障害原因ＩＴ装置の情報を元に図１１の管理外ＩＴ装置管理テーブルを検索して、該管理外ＩＴ装置に関する情報を取得してＳ６０６に進む。本実施例ではストレージ装置Ｕ１について図１１のＬ４０１から取得する。

[0091] Ｓ６０６では、Ｓ６０５にて取得した情報を含めて、発生した障害の根本原因が、管理外のＩＴ装置が原因であることを画面に表示する。その際の画面の構成例は、図１８のように、管理外ＩＴ装置が障害の根本原因であることを伝えるメッセージと、障害の原因について解析した結果である障害解析結果と、発生した障害に関して運用管理システムが検知している障害情報、例えば受信しているイベントなど、とを含んだウィンドウ、又はダイアログなど、画面表示を画面出力装置Ｍ１に出す。本実施例の管理外のＩＴ装置であるストレージＵ１の障害が根本原因であるケースにおける画面表示例は、

図１９のようになる。障害原因ＩＴ装置が、管理対象外であることがわかる情報と、そのＩＴ装置の種別が何であるか、例えばＩＰ－ＳＡＮストレージ装置であり、ＩＴ装置の識別情報として例えばＩＰアドレスが１９２．１６８．１００．１５であることを含むような画面表示である。

[0092] 以上のステップにより、管理対象外ＩＴ装置のストレージ装置Ｕ１に障害があった場合に、ルールＲ１のようなＩＰ－ＳＡＮストレージの障害が管理対象外で起こった場合について適用できるようになり、根本原因が管理対象外のＩＰ－ＳＡＮストレージであることを画面に表示することができる。

[0093] （ルールＲ２についての処理フロー）

ルールＲ２について、図３のＩＴシステムを対象とした実施例をもとにフローを説明する。

[0094] Ｓ１０１においてルールＲ２があるためＳ１０２に進み、Ｓ１０２では、ルールＲ２を読み込み、Ｒ２に読み込み済みの印をつける。Ｓ１０３において、ルールＲ２に記述されたトポロジ情報として図４の（２）のＦＣ－ＳＡＮトポロジとして、クライアント側にＦｉｂｒｅ　ＣｈａｎｎｅｌのＨｏｓｔ　Ｂｕｓ　Ａｄａｐｔｅｒ、すなわちＦｃＨｂａＴ２１１を持つ計算機Ｔ２１、ＦＣスイッチＴ２２を介して、サーバ側にＦｉｂｒｅ　ＣｈａｎｎｅｌのポートであるＦｃＰｏｒｔＴ２３１を持つストレージ装置Ｔ２３が接続されているトポロジを検索条件に定める。

[0095] Ｓ１０４において、クライアント側のＩＴ装置として、ＦｃＨｂａを持つ計算機である計算機Ｎ１３が見つかったものとする。

[0096] Ｓ１０５において、計算機Ｎ１３が未選択なＩＴ装置であるので、Ｓ１０６に進む。

[0097] Ｓ１０６において、計算機Ｎ１３を選択して、選択済みとする。

[0098] Ｓ１０７において、図１３に示したように計算機Ｎ１３より、接続先のサーバ側のストレージ装置のＦｉｂｒｅ　ＣｈａｎｎｅｌのポートであるＦＣ　ＰｏｒｔのWWNを示すＣｏｎｎｅｃｔｅｄＦｃＰｏｒｔWWN　Ｃ５０２を収集する。

[0099] なお、図１３のＦＣ－ＳＡＮストレージ装置の接続情報について説明すると、個々のＩＴ装置に対応する情報として、接続先のストレージ装置が有するＦｉｂｒｅＣｈａｎｎｅｌの通信識別情報を含む。

[0100] Ｓ１０８において、計算機Ｎ１３における接続先のストレージ装置に関する検索情報であるＣｏｎｎｅｃｔｅｄＦｃＰｏｒｔWWNについて、未検索であるためＳ１０９に進む。

[0101] Ｓ１０９において、計算機Ｎ１３で取得したＣｏｎｎｅｃｔｅｄＦｃＰｏｒｔWWNとして、Ｌ５０１行目のＣ５０２の値を用いて、構成管理において、このWWNをＦｃＰｏｒｔのWWNに持つストレージ装置を検索する。

[0102] Ｓ１１０において、Ｓ１０９で検索の結果、図１３のＬ５０１行目のＣ５０２の値をＦｃＰｏｒｔのWWNとして持つストレージが図１４に示すように管理対象の構成情報には存在しなかったため、Ｓ１１１に進む。

[0103] なお、ここで図１４に含まれる情報を説明すると、当該情報にはストレージ装置を示す識別情報と、当該ストレージ装置が有するＦｉｂｒｅＣｈａｎｎｅｌにおける通信識別情報を有する。

[0104] Ｓ１１１において、発見済みのストレージ装置の中で、図１３のＬ５０１行目のＣ５０２の値をＦｃＰｏｒｔのWWNとして持つストレージ装置Ｕ２を発見したため、Ｓ１１５に進む。

[0105] Ｓ１１５において、発見済みのストレージ装置Ｕ２を管理内に含めるように提案する画面を表示する。図１０は、ルールＲ１における画面表示例であるが、画面表示の構成は基本的に同様であり、メッセージの中身が実際のＩＴ装置のものに置き換わるのみである。

[0106] Ｓ１１６にて管理者よりストレージ装置Ｕ２の識別情報と当該装置を管理対象とする指示情報を受信する。

[0107] Ｓ１１７において、ユーザが管理対象に含めたかどうかを確認し、本実施例では管理対象に含めたためＳ１１８に進む。

[0108] Ｓ１１８において、管理対象として新たに追加したストレージ装置Ｕ２について、管理対象のＩＴ装置として取得が必要な情報を収集する。管理対象

として取得する情報は、イベント情報と構成管理情報である。

[0109] Ｓ１２１においては、ストレージ装置Ｕ２を管理対象のＩＴ装置として、計算機Ｎ１４とともにルールＲ２の適用先ＩＴ装置としてルール適用先管理テーブルに登録する。本ケースの例では図１２に示したルールのカラムＣ１０１と、そのルールの適用先となるＩＴ装置リストを格納するカラムＣ１０２から成る、テーブル状のデータ構造に登録する。

[0110] 以上により、ルールＲ２に対して、管理対象外のＩＴ装置であるＦＣ－ＳＡＮストレージ装置の障害解析が従来のルールベースのイベント相関で行えるようになる。

なお、障害解析の結果データを元に、管理対象外のＩＴ装置であるＦＣ－ＳＡＮストレージが障害の根本原因であると画面表示を出す処理については、ルールＲ１の管理対象外のＩＰ－ＳＡＮストレージを障害の根本原因であると画面表示した処理と同様にして図１６のステップで行う。

[0111] 上記の処理ステップにより、ルールＲ２に対しても、管理対象外ＩＴ装置のストレージ装置Ｕ２に障害があった場合に、ルールＲ２のようなＦＣ－ＳＡＮストレージの障害が管理対象外で起こった場合について適用できるようになり、根本原因が管理対象外のＦＣ－ＳＡＮストレージであることを画面に表示することができる。

（ルールＲ３についての処理フロー）

ルールＲ３について、図３のＩＴシステムを対象とした実施例をもとにフローを説明する。

[0112] Ｓ１０１においてルールＲ３があるためＳ１０２に進み、Ｓ１０２では、ルールＲ３を読み込み、Ｒ１０３に読み込み済みの印をつける。Ｓ１０３において、ルールＲ３に記述されたトポロジ情報として図４の（３）のファイルサーバ・クライアントのトポロジとして、クライアント側に公開されているファイルシステムをマウントしていることを示すＩｍｐｏｒｔｅｄＦｉｌｅＳｈａｒｅＴ３１１を持つ計算機Ｔ３１、ＩＰスイッチＴ３２を介して、サーバ側に他の計算機に公開しているファイルシステムを持つことを示すＥ

ｘｐｏｒｔｅｄＦｉｌｅＳｈａｒｅＴ３３１を持つ計算機Ｔ３３が接続されているトポロジを検索条件に定める。

[0113] Ｓ１０４において、図４の（３）のトポロジのクライアント側のＩＴ装置として、図３の計算機Ｎ１０が見つかったものとする。

[0114] Ｓ１０５において、検索されたクライアント側のＩＴ装置として計算機Ｎ１０があり、未選択であるため、Ｓ１０６に進む。

[0115] Ｓ１０６において、未選択のクライアント側のＩＴ装置として図３の計算機Ｎ１０を選択し、選択済みとする。

[0116] Ｓ１０７において、計算機Ｎ１０と、図４の（３）のトポロジのサーバ側のＩＴ装置として対向する計算機の検索情報として、どのファイルサーバの公開ファイルシステムをマウントしているかを示すＩｍｐｏｒｔｅｄＦｉｌｅＳｈａｒｅの情報を取得する。クライアント側から取得するファイルサーバに関する情報を管理するテーブルとして図１５のようなクライアント側のコンピュータのカラムＣ７０１と、それに対応するファイルサーバに関する識別情報のカラムＣ７０２と、ファイルサーバの公開名に関するカラムＣ７０３を含むデータ構造、例えばテーブルなどで管理する。なお、クライアント側から取得するファイルサーバに関する情報は、予め構成情報として図１５のテーブルで取得済みであっても構わないし、Ｓ７の処理においてクライアント側のＩＴ装置から取得してきても構わない。すなわち取得するタイミングは、Ｓ１０７の処理が完了するまでに行われていればよい。

[0117] なお、ここで図１５に含まれる情報を説明すると、当該情報には個々のファイルサーバ毎に以下の情報を含む。

（Ａ）ファイルサーバーのＩＴ装置としての識別情報

（Ｂ）一つ以上のファイルサーバとしての識別情報と公開名

Ｓ１０８において、Ｓ１０７で取得したクライアント側のファイルサーバに関する情報は、図１５のＬ７０１行であり、未検索であるためＳ９に進む。

[0118] Ｓ１０９において、図１５のＬ７０１行目のファイルサーバの識別情報の

カラムＣ７０２の値、すなわちｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍというＦＱＤＮを持つＩＴ装置を検索する。

[0119] Ｓ１１０において、管理対象の構成情報Ｔ０の中にｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍというＦＱＤＮを持つ計算機が存在しないことから、Ｓ１１１に進む。

[0120] Ｓ１１１において、発見済みリソースの中にｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍ というＦＱＤＮを持つ計算機が存在しないことから、Ｓ１１２に進む。

[0121] Ｓ１１２において、ｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍという計算機の発見を試みる。発見は、ＤＮＳサーバに問い合わせてＩＰアドレスを解決し、そのＩＰアドレスに対してｐｉｎｇによりか存在を確認した上で、ｔｅｌｎｅｔ、又はｓｓｈ、又はＷｉｎｄｏｗｓ（登録商標）のリモート接続などによりアクセスを試みる。本実施例では、ｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍに対するＩＰアドレスに対するｐｉｎｇは成功を返し、存在が確認できるが、そのサーバの認証情報を持たないため、その他のアクセスは失敗してログインできないものとしてＳ１１４に進む。

[0122] Ｓ１１４において、発見したｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍの計算機は、ｐｉｎｇでの応答を返すものの、それ以外の情報が取得できず、管理対象とすることができないのでＳ１１９に進む。

[0123] Ｓ１１９において、ｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍの計算機を図１１の管理外ＩＴ装置管理テーブルに登録する。具体的には図１０のＬ４０３のように、ファイルサーバ識別情報と、サービス識別情報にクライアント側で取得した情報を格納する。

[0124] Ｓ１２０において、クライアント側の計算機Ｎ１０とｅｘｐｏｒｔｆｓ．ｄｏｍａｉｎ２．ｃｏｍの計算機Ｕとのペアに対するルール適用情報を生成する。具体的には、図１２１のＬ１０７のように、ルールＲ３に対して、適用先ＩＴ装置リストに、計算機Ｎ１０と管理外ＩＴ装置である計算機Ｕ３を登録する。

[0125] 以上により、計算機Ｎ１０のファイルサーバである管理外のＩＴ装置である計算機Ｕ３についても障害解析が行えるようになる。

[0126] 同様にして、Ｓ１０１からＳ１０４のステップにより、ルールＲ３についてクライアント側のＩＴ装置として計算機Ｎ１１が見つかった場合の実施形態の処理フローを説明する。

Ｓ１０５からＳ１０７のステップにより、計算機Ｎ１１に対するファイルサーバとして

図１５のＬ７０３の行に示したファイルサーバに関する情報を取得する。Ｓ１０９において管理対象のＩＴ装置に図１５のＬ７０３行で示されたファイルサーバは見つからないため、Ｓ１１１に進む。Ｓ１１１においては、発見済みのリソースの中に図１５のＬ７０３行で示されたＩＰアドレスを持つ計算機Ｕ５が存在するので、Ｓ１１５に進む。

[0127] Ｓ１１５において、計算機Ｕ５を管理対象に含めるように提案する画面を表示し、Ｓ１１６にてユーザ入力としてユーザが計算機Ｕ５を管理対象とする指示を受信する。

[0128] Ｓ１１７において、Ｓ１１６ユーザが計算機Ｕ５を管理対象とする指示を受信したため、Ｓ１１８に進む。

[0129] Ｓ１１８において、計算機Ｕ５を管理対象とするための情報として、発見済みリソースとして保持していたＩＴ装置の識別情報、アクセスのための情報の他に、計算機Ｕ５の接続デバイスの構成情報と、稼動状態と、性能情報とを含む監視情報を取得して、構成管理Ｃ３の管理対象の構成情報Ｔ０に格納する。

[0130] Ｓ１２１において、管理内ＩＴ装置として計算機Ｎ１１をクライアント、計算機Ｕ５をファイルサーバとするトポロジに対してルールＲ３を適用できるように、図１２のＬ１０８行目のようなデータ構造としてルールメモリに格納する。

[0131] 以上により、発見済みのＩＴ装置で、なおかつ管理対象外であったファイルサーバの計算機Ｕ５に対する障害解析が、図２のフローにしたがって行え

、画面表示部Ｃ２において図１６のフローに行うことで、画面表示装置Ｍ１に障害原因を出力することができるようになる。

[0132] （ルールＲ４についての処理フロー）

ルールＲ４について、図３のＩＴシステムを対象とした実施例をもとにフローを説明する。

[0133] ＳＴＡＲＴからＳ１０４のステップにより、ルールＲ４についてクライアント側のＩＴ装置として計算機Ｎ１０を見つける。Ｓ１０５からＳ１０７のステップにより、計算機Ｎ１０に対するＤＮＳサーバの検索情報として、計算機Ｎ１０よりＤＮＳサーバのＩＰアドレス１９２．１６８．１００．１を取得する。 Ｓ１０８からＳ１１０のステップにより、取得したＩＰアドレス１９２．１６８．１００．１を利用して構成管理Ｃ３の管理対象の構成情報Ｔ０にＤＮＳサーバが存在しないことを確認し、Ｓ１１１に進む。Ｓ１１１では、ＤＮＳサーバは発見済みＩＴ装置ではないことを判断して、Ｓ１１２に進み、Ｓ１１２において実ＩＴシステムからＩＰアドレス１９２．１６８．１００．１のノードに対するアクセスを試みる。アクセスの結果、ｐｉｎｇによるネットワーク到達が確認できたものの、認証情報を持たないためログインはできず、Ｓ１１４において管理対象とすることができないと判断してＳ１１９に進む。Ｓ１１９においては、ＩＰアドレス１９２．１６８．１００．１の計算機を管理対象外ＩＴ装置として図１１のＬ４０４に示したようにＤＮＳサーバとして識別情報Ｕ４で情報を格納・管理してＳ１２０に進む。Ｓ１２０において、クライアントの計算機Ｎ１０と、ＤＮＳサーバである管理外のＩＴ装置の計算機Ｕ４をルール４の適用先ＩＴ装置リストとして図１２のＬ１０９行のように格納する。

[0134] 以上のステップにより、管理外のＤＮＳサーバである計算機Ｕ４の障害解析が、従来のルールによるイベント相関により解析できるようになり、障害原因として管理外のＤＮＳサーバを特定することができるようになる。

[0135] 図３のそのほかのＩＴ装置に対するルール４の適用についても同様にして、管理外のＤＮＳサーバである計算機Ｕ４に対して適用情報が生成されるこ

とで行える。

[0136] また、他のルールの実施例と同様にして、図１６のフローを画面表示部Ｃ２にて行うことで、管理外のＩＴ装置であるＤＮＳサーバが障害の根本原因であることを画面に表示することができる。

実施例 2

[0137] 本発明の第２の実施形態は、第１の実施形態において図２に示した障害解析の全体処理フローの処理手順を、図２０に示したように、ルール適用部Ｃ１１における適用情報を作成するステップＳ４ｂをイベント受信するステップＳ３ｂよりもあとで、なおかつイベント解析部Ｃ１２におけるイベント解析処理のステップＳ５ｂよりも前のステップで行う。

この第２実施形態と、第１実施形態の違いは、ルールの適用情報を作成するタイミングのみである。

[0138] 上記のように、ルールの適用情報のタイミングを変えて本発明を実施しても効果は損なわれず、管理対象外のＩＴ装置を障害の根本原因装置であると画面に表示することは可能である。

[0139] 以上、本願明細書の実施例１と実施例２による複数の情報処理装置と画面出力装置とに接続され、プロセッサとメモリを有する運用管理サーバにおける前記複数の情報処理装置で発生するイベントの解析を実現するプログラムは以下の処理の一部または全てを有する。

（ａ）前記複数の情報処理装置の各々が、クライアントとしてネットワークサービスを用いるためにアクセス対象とする前記複数の情報処理装置の一部であるサーバ装置の識別情報を、前記メモリが有する構成情報に格納する構成情報格納処理。

（ｂ）前記複数の情報処理装置の一部であって、前記運用管理サーバがイベント情報を取得する対象である複数のイベント取得対象装置を前記メモリが有する構成情報に登録する登録処理。

（ｃ）前記複数の情報処理装置で発生する前記ネットワークサービスに関連した第一のイベント種別を含むイベントと、前記ネットワークサービスに関

連した前記第一のイベント種別とは異なる第二のイベント種別を含むイベントと、を検知した場合に、前記第二のイベント種別に対応するイベントの発生が原因で前記第一のイベント種別に対応するイベントが発生し得ることを示す相関解析ルール情報を前記メモリに格納するルール格納処理。

（ｄ）前記複数のイベント取得対象装置から収集した複数の前記イベント情報を前記メモリに格納するイベント格納処理。

（ｅ）前記相関解析ルール情報を元に、前記メモリに格納した複数の前記イベント情報から、前記第一のイベント種別を含む第一のイベント情報を特定するイベント情報特定処理。

（ｆ）前記構成情報を元に、前記第一のイベント情報を送信したイベント取得対象装置の一つである第一イベント取得対象装置と、前記第一のイベント種別に対応する前記ネットワークサービスにおける前記第一イベント取得対象装置のサーバ装置である障害要因装置とを特定する、要因特定処理。

（ｇ）前記相関解析ルール情報と前記構成情報とを元に、前記障害要因装置が前記複数のイベント取得対象装置でない場合に、前記第一イベント取得対象装置と前記第一のイベント種別と前記障害要因装置と前記第二のイベント種別とを特定する情報を前記画面出力装置へ送信することで、前記第一イベント取得対象装置で発生した前記第一のイベント情報に対応したイベントが、前記障害要因装置で前記第二のイベント種別のイベントが発生したことが要因と推定されることを前記画面出力装置へ表示させる解析結果送信処理。

[0140] さらには、前記相関解析ルール情報は、前記第一のイベント種別が発生した前記複数の情報処理装置の一つである第一情報処理装置と、前記第二のイベント種別が発生した前記複数の情報処理装置の一つである第二情報処理装置と、の間のトポロジ条件を示すトポロジ条件情報を含み、前記要因特定ステップは、前記トポロジ条件情報に基づいて前記障害要因装置を特定してもよい。このような処理によってイベントが発生した情報処理装置が実際に用いている情報処理装置に限定して推定を提示できるため、より運用管理サーバの利用者に利便性の高い。

[0141] また、運用管理サーバは以下の処理を有してもよい。

（ｈ）前記相関解析ルール情報と前記構成情報に基づいて、前記複数のイベント取得対象装置のサーバ装置であって、前記複数のイベント取得対象装置に含まれない、前記複数の情報処理装置の一部であるイベント関連情報処理装置を特定する、関連装置特定処理。

（ｉ）前記イベント関連情報処理装置からイベント情報の取得が可能か調査する、イベント情報取得可否調査処理。

（ｊ）前記調査の結果を元に、前記イベント関連情報処理装置からイベント情報の取得が可能な場合は前記イベント関連情報処理装置を特定する情報を前記画面出力装置へ送信することで、前記イベント関連情報処理装置からイベント情報の取得が可能であることを前記画面出力装置へ表示させる、イベント情報取得対象追加提案処理。

[0142] このような処理は、情報処理装置の管理者または管理方法の変更によって新たに運用管理サーバでイベント監視が必要または可能となった時点から迅速に、登録忘れをせずに運用管理サーバへの登録を促進することができる。

[0143] さらには、前記イベント情報取得可否調査処理は、前記複数の情報処理装置であって予め調査範囲として設定されたＩＰアドレスの範囲に含まれるＩＰアドレスを有する情報処理装置に対して、前記運用管理サーバが所定の手順に基づくアクセスを行った結果に基づいてもよい。情報処理装置（特にインターネットを介してアクセスするサーバ計算機）には不正アクセスや不正攻撃を防止するために当該装置外部からのアクセスを監視している場合があり、当該調査処理によるアクセスを行った場合もアクセス監視により不正アクセスや不正攻撃と見なされることがある。そのため、明らかにイベント監視の対象としない情報処理装置のＩＰアドレス、またはイベント監視対象になりうる情報処理装置のＩＰアドレスの範囲を特定することで、こうした不正アクセスや不正攻撃と誤認されるような通信を抑止することができる。

[0144] さらには、前記障害要因装置はコントローラを有し、論理ボリュームを提供するストレージ装置であって、前記ネットワークサービスは前記論理ボリ

ュームをブロックアクセス形式のプロトコル（例えばＦｉｂｒｅＣｈａｎｎｅｌやｉＳＣＳＩがある）によって提供するサービスであって、前記第一のイベント種別が前記ストレージ装置の障害発生であり、前記第一のイベント種別が前記論理ボリュームへのアクセス失敗であってもよい。

[0145] さらには、前記障害要因装置は前記ネットワークサービスとしてＤＮＳを提供する計算機であって、前記第一のイベント種別がＤＮＳ要求失敗であり、前記第一のイベント種別がＤＮＳサーバの通信断絶であってもよい。

[0146] さらには、前記障害要因装置は前記複数の情報処理装置の少なくとも一つからデータを受信するＮＩＣを有し、格納したファイルを前記複数の情報処理装置の少なくとも一つに提供するファイルサーバ計算機であって、前記ネットワークサービスは前記ファイルサーバ計算機が格納したファイルを共有するネットワークファイル共有サービスであって、前記第一のイベント種別が前記ファイルサーバの障害発生（例えばＮＩＣの障害発生、ファイルサーバが有するプロセッサが実行するソフトウェアの不具合の発生、その他ファイルサーバの通信機能が停止する障害の発生）であり、前記第一のイベント種別が前記ネットワークファイル共有サービスで提供されたファイルへのアクセス失敗であってもよい。

[0147] さらには、前記相関解析ルール情報と前記構成情報とを元に、前記障害要因装置が前記複数のイベント取得対象装置の一つの場合に、複数の前記イベント情報から前記第二のイベント種別を含み、前記障害要因装置が取得元である第二のイベント情報を特定し、前記第一イベント取得対象装置と前記第一のイベント情報と前記障害要因装置と前記第二のイベント情報とを特定する情報を前記画面出力装置へ送信することで、前記第一イベント取得対象装置で発生した前記第一のイベント情報に対応したイベントが、前記障害要因装置で発生した前記第二のイベント情報に対応したイベントが発生したことが要因であることを前記画面出力装置へ表示させてもよい。

[0148] さらには、前記第一情報処理装置が計算機であり、前記第二情報処理装置がストレージ装置であり、前記トポロジ条件情報は、前記計算機と前記スト

レージ装置とが接続するトポロジの接続関係を示す、前記計算機に対応する通信識別情報と前記ストレージ装置に対応する通信識別情報との組み合わせを含めても良い。なお、これら通信識別情報としてはｉＳＣＳＩ名と、ＩＰアドレスと、ＦｉｂｒｅＣｈａｎｎｅｌにおけるWWNとの少なくとも一つが考えられる。

[0149] さらには、前記第一情報処理装置が計算機であり、前記第二情報処理装置はファイル共有サービスによって格納したファイルを前記複数の情報処理装置へ提供するファイルサーバ計算機であり、前記トポロジ条件情報は、前記計算機と前記ファイルサーバ計算機とが接続するトポロジの接続関係を示す前記計算機に対応する通信識別情報と前記ファイルサーバ計算機に対応する通信識別情報又は前記ファイルを公開するエクスポート名との組み合わせを含めても良い。

[0150] さらには、前記第一情報処理装置は計算機であり、前記第二情報処理装置がネットワーク共有サービスとしてＤＮＳを前記複数の情報処理装置に提供するＤＮＳサーバ計算機であり、前記トポロジ条件情報は、前記計算機と前記ＤＮＳサーバ計算機とが接続するトポロジの接続関係を示す前記計算機に対応する通信識別情報と前記ＤＮＳサーバ計算機に対応する通信識別情報との組み合わせを含めても良い。なお、前記計算機に対応する通信識別情報と前記ＤＮＳサーバ計算機に対応する通信識別情報とは、ＩＰアドレス又はＦＱＤＮが考えられる。

[0151] さらには、前記運用管理サーバは一つ以上の計算機から構成されてもよい。

請求の範囲

[1] 複数の情報処理装置と画面出力装置とに接続され、プロセッサとメモリを有する運用管理サーバにおける前記複数の情報処理装置で発生するイベントの解析方法であって、

前記複数の情報処理装置の各々が、クライアントとしてネットワークサービスを用いるためにアクセス対象とする前記複数の情報処理装置の一部であるサーバ装置の識別情報を、前記メモリが有する構成情報に格納する構成情報格納ステップと、

前記複数の情報処理装置の一部であって、前記運用管理サーバがイベント情報を取得する対象である複数のイベント取得対象装置を前記メモリが有する構成情報に登録する登録ステップと、

前記複数の情報処理装置で発生する前記ネットワークサービスに関連した第一のイベント種別を含むイベントと、前記ネットワークサービスに関連した前記第一のイベント種別とは異なる第二のイベント種別を含むイベントと、を検知した場合に、前記第二のイベント種別に対応するイベントの発生が原因で前記第一のイベント種別に対応するイベントが発生し得ることを示す相関解析ルール情報を前記メモリに格納するルール格納ステップと、

前記複数のイベント取得対象装置から収集した複数の前記イベント情報を前記メモリに格納するイベント格納ステップと、

前記相関解析ルール情報を元に、前記メモリに格納した複数の前記イベント情報から、前記第一のイベント種別を含む第一のイベント情報を特定するイベント情報特定ステップと、

前記構成情報を元に、前記第一のイベント情報を送信したイベント取得対象装置の一つである第一イベント取得対象装置と、前記第一のイベント種別に対応する前記ネットワークサービスにおける前記第一イベント取得対象装置のサーバ装置である障害要因装置とを特定する、要因特定ステップと、

前記相関解析ルール情報と前記構成情報とを元に、前記障害要因装置が前記複数のイベント取得対象装置でない場合に、前記第一イベント取得対象装置

と前記第一のイベント種別と前記障害要因装置と前記第二のイベント種別とを特定する情報を前記画面出力装置へ送信することで、前記第一イベント取得対象装置で発生した前記第一のイベント情報に対応したイベントが、前記障害要因装置で前記第二のイベント種別のイベントが発生したことが要因と推定されることを前記画面出力装置へ表示させる解析結果送信ステップと、

を有することを特徴としたイベントの解析方法。

[2] 請求項１記載のイベント解析方法であって、

前記相関解析ルール情報は、前記第一のイベント種別が発生した前記複数の情報処理装置の一つである第一情報処理装置と、前記第二のイベント種別が発生した前記複数の情報処理装置の一つである第二情報処理装置と、の間のトポロジ条件を示すトポロジ条件情報を含み、

前記要因特定ステップは、前記トポロジ条件情報に基づいて前記障害要因装置を特定する、

ことを特徴としたイベントの解析方法。

[3] 請求項２記載のイベントの解析方法であって、

前記相関解析ルール情報と前記構成情報に基づいて、前記複数のイベント取得対象装置のサーバ装置であって、前記複数のイベント取得対象装置に含まれない、前記複数の情報処理装置の一部であるイベント関連情報処理装置を特定する、関連装置特定ステップと、

前記イベント関連情報処理装置からイベント情報の取得が可能か調査する、イベント情報取得可否調査ステップと、

前記調査の結果を元に、前記イベント関連情報処理装置からイベント情報の取得が可能な場合は前記イベント関連情報処理装置を特定する情報を前記画面出力装置へ送信することで、前記イベント関連情報処理装置からイベント情報の取得が可能であることを前記画面出力装置へ表示させる、イベント情報取得対象追加提案ステップと、

を有することを特徴としたイベントの解析方法。

[4] 請求項３記載のイベントの解析方法であって、

前記イベント情報取得可否調査ステップは、前記複数の情報処理装置であって予め調査範囲として設定されたＩＰアドレスの範囲に含まれるＩＰアドレスを有する情報処理装置に対して、前記運用管理サーバが所定の手順に基づくアクセスを行った結果に基づくことを特徴としたイベントの解析方法。

[5] 請求項１記載のイベントの解析方法であって、
前記障害要因装置はコントローラを有し、論理ボリュームを提供するストレージ装置であって、
前記ネットワークサービスは前記論理ボリュームをブロックアクセス形式のプロトコルによって提供するサービスであって、
前記第一のイベント種別が前記ストレージ装置の障害発生であり、前記第一のイベント種別が前記論理ボリュームへのアクセス失敗である、
ことを特徴としたイベントの解析方法。

[6] 請求項５記載のイベントの解析方法であって、前記ブロックアクセス形式のプロトコルはＦｉｂｒｅＣｈａｎｎｅｌ又はｉＳＣＳＩであることを特徴としたイベントの解析方法。

[7] 請求項１記載のイベントの解析方法であって、
前記障害要因装置は前記ネットワークサービスとしてＤＮＳを提供する計算機であって、前記第一のイベント種別がＤＮＳ要求失敗であり、前記第一のイベント種別がＤＮＳサーバの通信断絶である、
ことを特徴としたイベントの解析方法。

[8] 請求項１記載のイベントの解析方法であって、
前記障害要因装置は格納したファイルを前記複数の情報処理装置の少なくとも一つに提供するファイルサーバ計算機であって、
前記ネットワークサービスは前記ファイルサーバ計算機が格納したファイルを共有するネットワークファイル共有サービスであって、
前記第一のイベント種別が前記ファイルサーバ計算機の障害発生であり、前記第一のイベント種別が前記ネットワークファイル共有サービスで提供されたファイルへのアクセス失敗である、

ことを特徴としたイベントの解析方法。

[9] 請求項１記載のイベントの解析方法であって、

前記相関解析ルール情報と前記構成情報とを元に、前記障害要因装置が前記複数のイベント取得対象装置の一つの場合に、複数の前記イベント情報から前記第二のイベント種別を含み、前記障害要因装置が取得元である第二のイベント情報を特定し、前記第一イベント取得対象装置と前記第一のイベント情報と前記障害要因装置と前記第二のイベント情報とを特定する情報を前記画面出力装置へ送信することで、前記第一イベント取得対象装置で発生した前記第一のイベント情報に対応したイベントが、前記障害要因装置で発生した前記第二のイベント情報に対応したイベントが発生したことが要因であることを前記画面出力装置へ表示させる第二解析結果送信ステップ、

とを有することを特徴としたイベントの解析方法。

[10] 請求項２記載のイベントの解析方法であって、

前記第一情報処理装置が計算機であり、前記第二情報処理装置がストレージ装置であり、

前記トポロジ条件情報は、前記計算機と前記ストレージ装置とが接続するトポロジの接続関係を示す、前記計算機に対応する通信識別情報と前記ストレージ装置に対応する通信識別情報との組み合わせを含む、

ことを特徴としたイベントの解析方法。

[11] 請求項１０記載のイベントの解析方法であって、

前記計算機に対応する計算機通信識別情報と前記ストレージ装置に対応する通信識別情報とは、ｉＳＣＳＩ名と、ＩＰアドレスと、ＦｉｂｒｅＣｈａｎｎｅｌにおけるWWNとの少なくとも一つであることを特徴とするイベントの解析方法。

[12] 請求項２記載のイベントの解析方法であって、

前記第一情報処理装置が計算機であり、前記第二情報処理装置はファイル共有サービスによって格納したファイルを前記複数の情報処理装置へ提供するファイルサーバ計算機であり、

前記トポロジ条件情報は、前記計算機と前記ファイルサーバ計算機とが接続するトポロジの接続関係を示す前記計算機に対応する通信識別情報と前記ファイルサーバ計算機に対応する通信識別情報又は前記ファイルを公開するエクスポート名との組み合わせを含む、

ことを特徴としたイベントの解析方法。

[13] 請求項２記載のイベントの解析方法であって、

前記第一情報処理装置は計算機であり、前記第二情報処理装置がネットワーク共有サービスとしてＤＮＳを前記複数の情報処理装置に提供するＤＮＳサーバ計算機であり、

前記トポロジ条件情報は、前記計算機と前記ＤＮＳサーバ計算機とが接続するトポロジの接続関係を示す前記計算機に対応する通信識別情報と前記ＤＮＳサーバ計算機に対応する通信識別情報との組み合わせを含む、

ことを特徴としたイベントの解析方法。

[14] 請求項１３記載のイベントの解析方法であって、

前記計算機に対応する通信識別情報と前記ＤＮＳサーバ計算機に対応する通信識別情報とは、ＩＰアドレス又はＦＱＤＮである、

ことを特徴としたイベントの解析方法。

[図1]

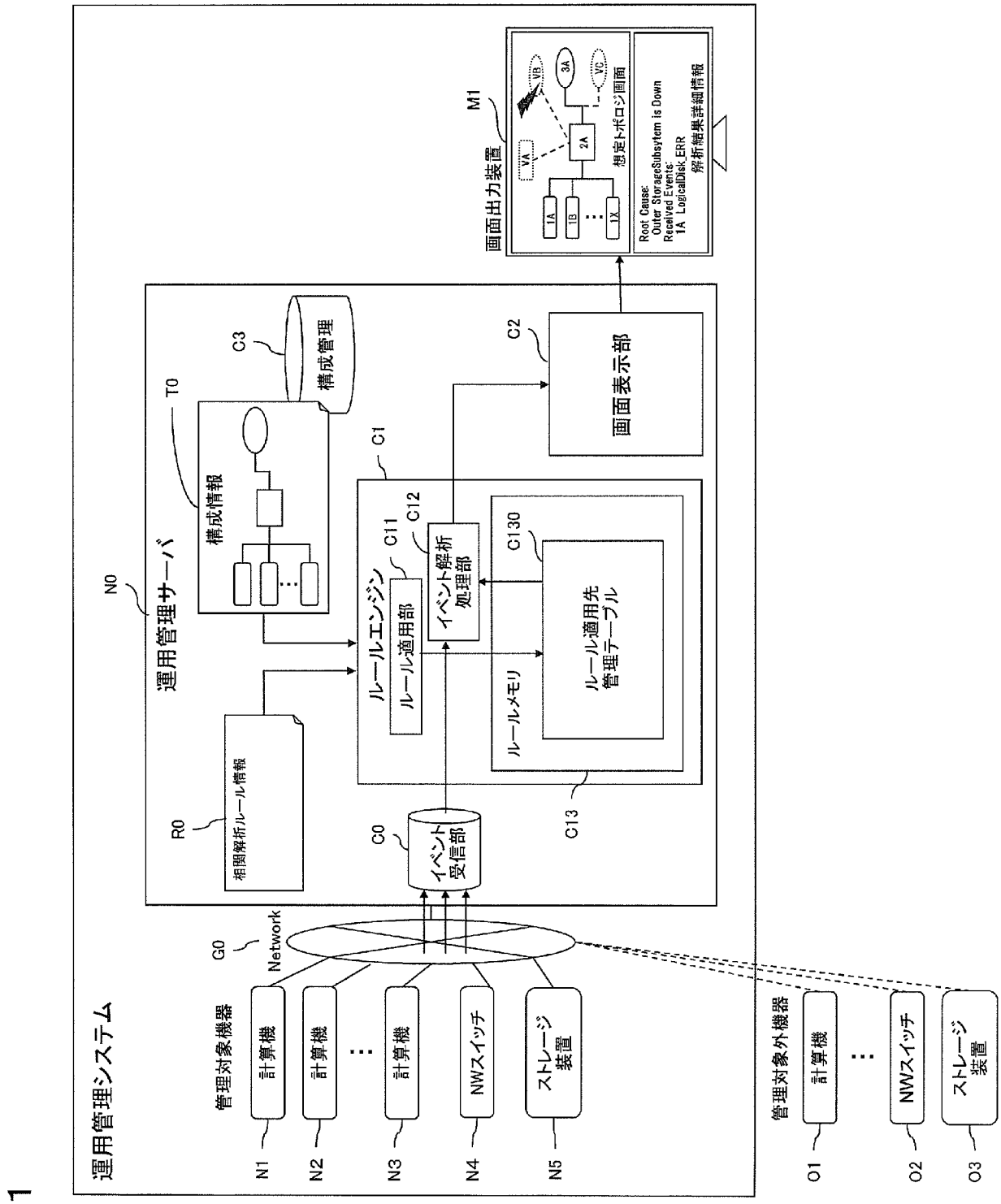
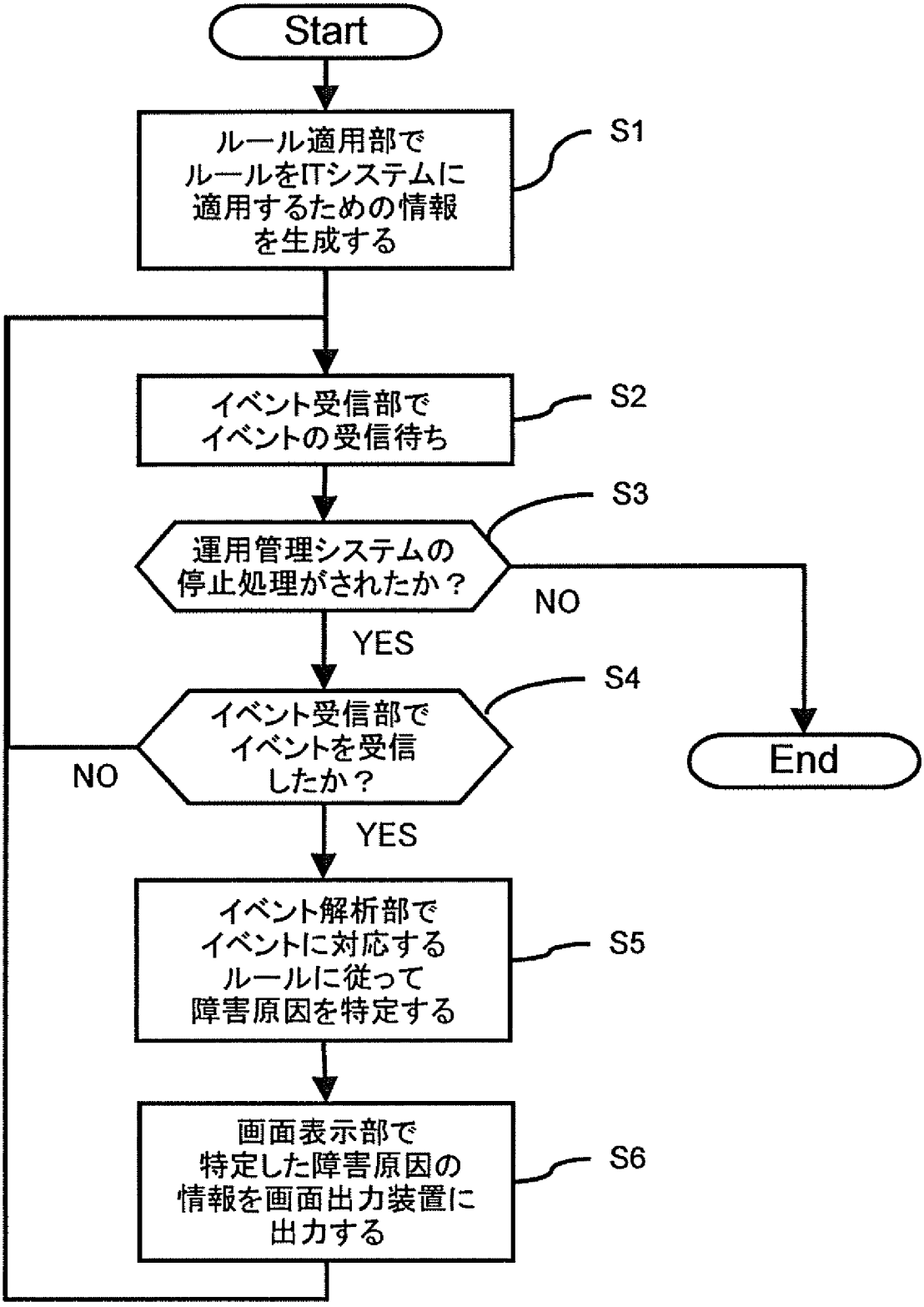

運用管理システム
N0
運用管理サーバ
T0
構成情報
C3
構成管理
C1
ルールエンジン
ルール適用部
C11
イベント解析処理部
C12
ルールメモリ
C130
ルール適用先管理テーブル
C13
C2
画面表示部
M1
画面出力装置
想定トポロジ画面
VA
VB
VC
1A
1B
1X
2A
3A
Root Cause:
Outer StorageSubsytem is Down
Received Events:
1A LogicalDisk ERR
解析結果詳細情報
R0
相関解析ルール情報
C0
イベント受信部
G0
Network
管理対象機器
計算機
計算機
計算機
NWスイッチ
ストレージ装置
N1
N2
N3
N4
N5
管理対象外機器
計算機
NWスイッチ
ストレージ装置
O1
O2
O3

図1

[図2]

図2


Start
ルール適用部で
ルールをITシステムに
適用するための情報
を生成する
S1
イベント受信部で
イベントの受信待ち
S2
運用管理システムの
停止処理がされたか？
S3
NO
YES
イベント受信部で
イベントを受信
したか？
S4
NO
End
YES
イベント解析部で
イベントに対応する
ルールに従って
障害原因を特定する
S5
画面表示部で
特定した障害原因の
情報を画面出力装置に
出力する
S6

[図3]

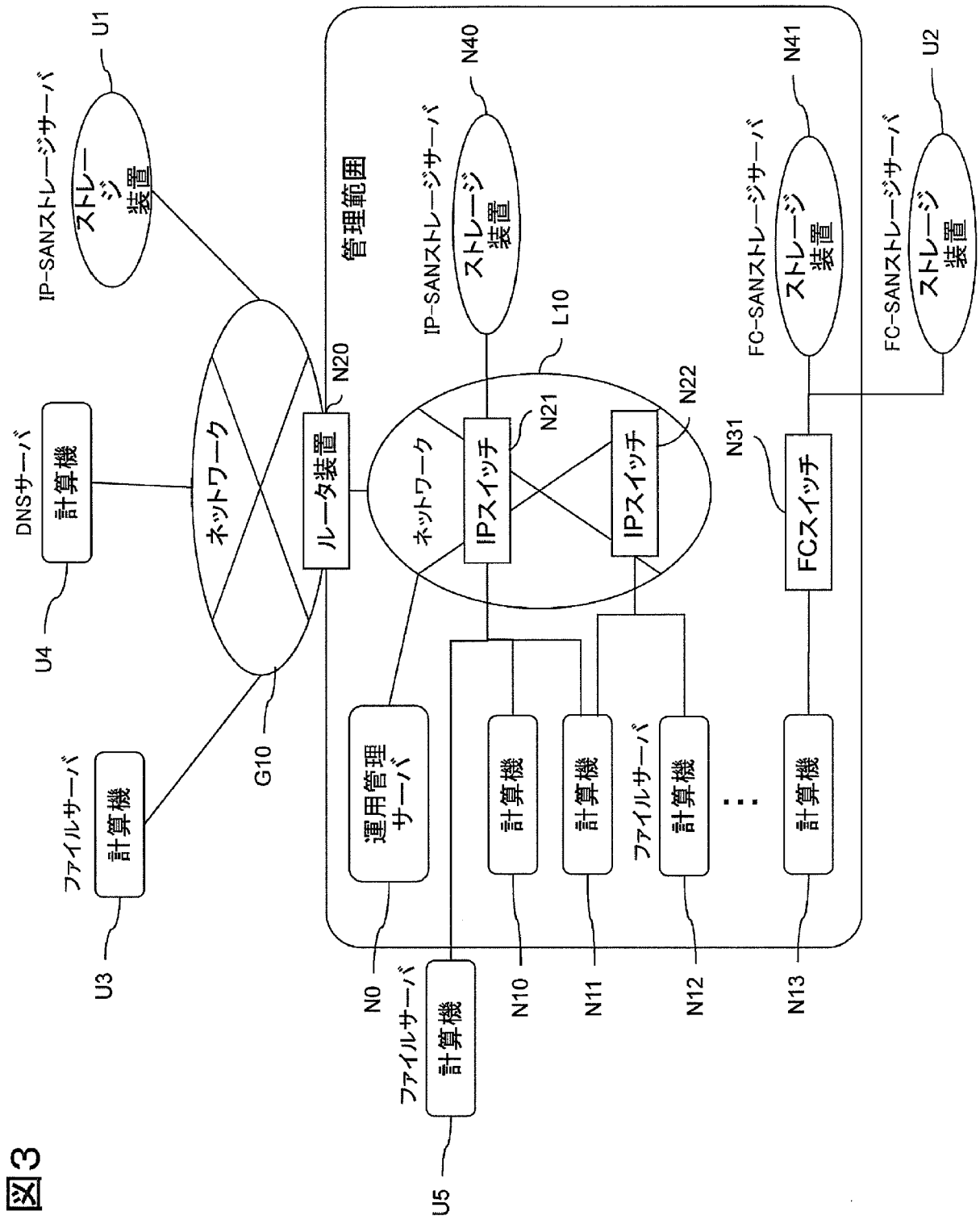

IP-SANストレージサーバ
ストレージ装置
U1
DNSサーバ
計算機
U4
ファイルサーバ
計算機
U3
ネットワーク
G10
ルータ装置
N20
管理範囲
IP-SANストレージサーバ
ストレージ装置
N40
L10
ネットワーク
IPスイッチ
N21
IPスイッチ
N22
FC-SANストレージサーバ
ストレージ装置
N41
FCスイッチ
N31
FC-SANストレージサーバ
ストレージ装置
U2
運用管理サーバ
N0
計算機
N10
計算機
N11
ファイルサーバ
計算機
N12
計算機
N13
ファイルサーバ
計算機
U5

図3

[図4]

図4

(1) ストレージコントローラ(IP-SAN)故障のRCAルール

```
Rule-ID: R1
IF
  <Computer.has(iScsiInitiator) LogicalDisk_ERR>
  <IpSwitch>
  <Storage.has(iScsiTarget) Controller_ERR>
THEN
  <Storage.has(iScsiTarget) RootCause(Controller_ERR) >
```

R1

(2) ストレージコントローラ(FC-SAN)故障のRCAルール

```
Rule-ID: R2
IF
  <Computer.has(FcHba) LogicalDisk_ERR>
  <IpSwitch>
  <Storage.has(FcPort) Controller_ERR>
THEN
  <Storage.has(FcPort) RootCause(Controller_ERR) >
```

R2

(3) ファイルサーバのNIC故障のRCAルール

```
Rule-ID: R3
IF
  <Computer.is(ImportedFileShare) LogicalDisk_ERR>
  <IpSwitch>
  <Computer.is(ExportedFileShare) NIC_ERR>
THEN
  <Computer(ExportedFileShare) RootCause(NIC_ERR) >
```

R3

(4) DNSサーバのネットワーク不到達障害のRCAルール

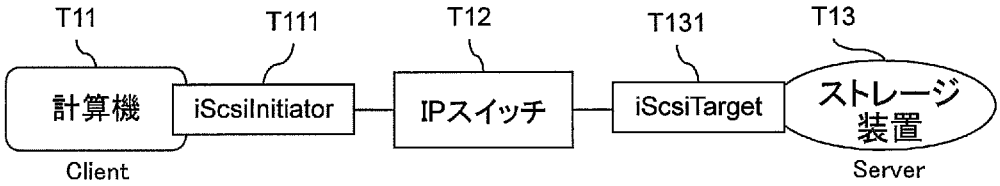
```
Rule-ID: R4
IF
  <Computer Network_ERR>
  <Computer(DNSService) Unreachable_ERR>
THEN
  <Computer(DNSService) RootCause(Unreachable_ERR) >
```

R4

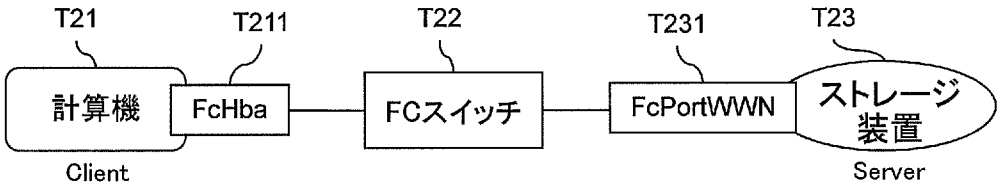
[図5]

図5

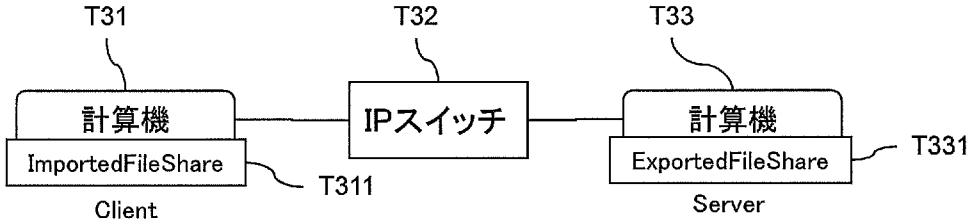
(1) ルールR1が示すIP-SANトポロジ



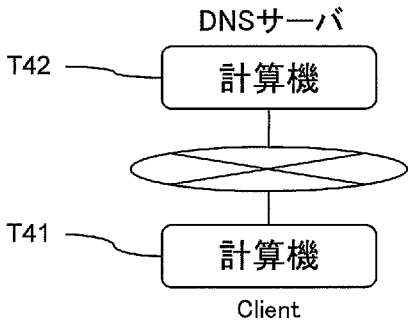
(2) ルールR2が示すFC-SANトポロジ



(3) ルールR3が示すファイルサーバ・クライアントのトポロジ



(4) ルールR4が示すNFSサーバのトポロジ



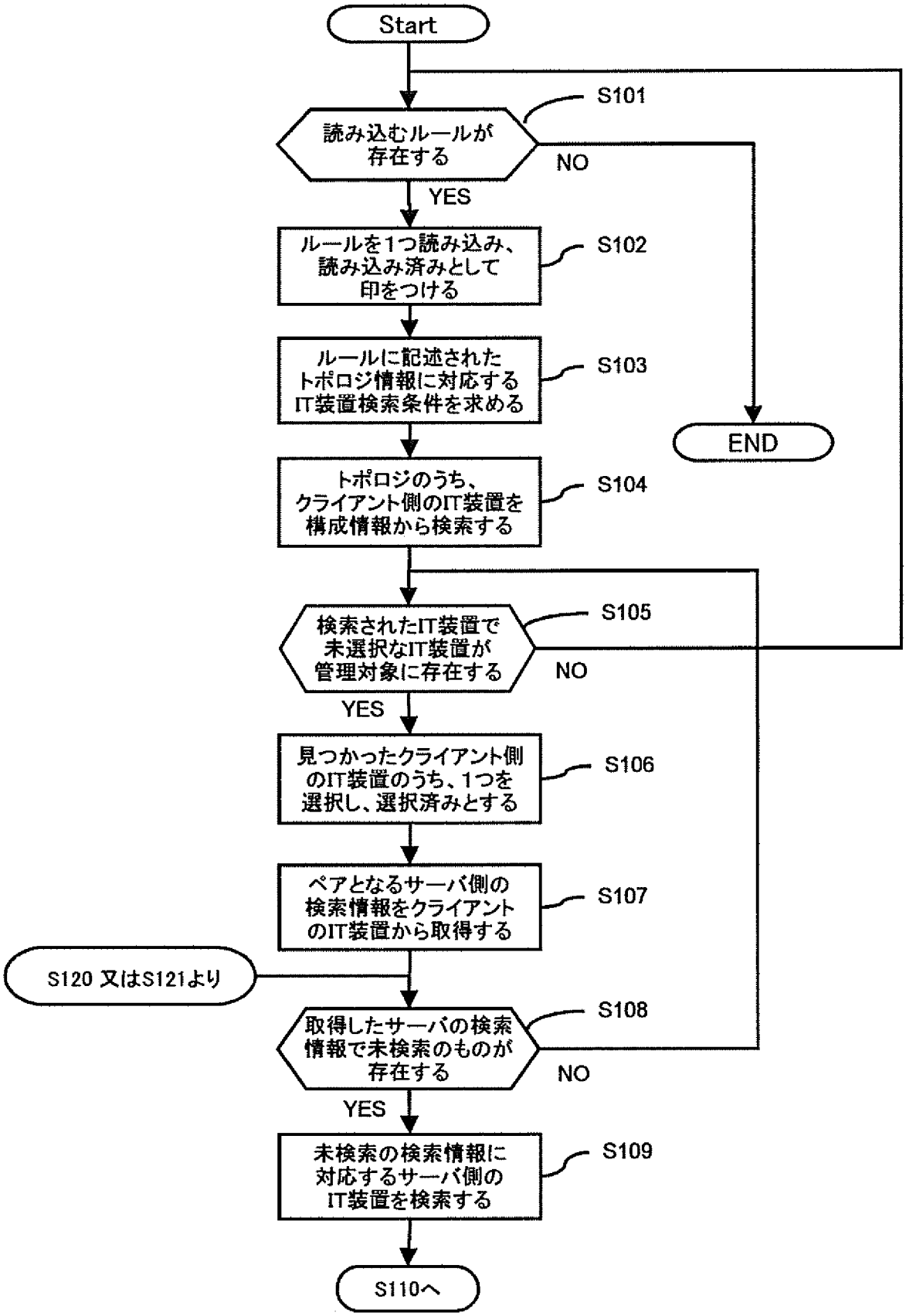
[図6]

図6

	TL1 / C101 ルール	C102 適用先IT装置リスト
L101	R1	N10, N40
L102	R1	N11, N40
L103	R2	N13, N41
L104	R3	N11, N12
	⋮	⋮

[図7]

図7


Start
S101
読み込むルールが存在する
NO
YES
ルールを1つ読み込み、読み込み済みとして印をつける
S102
ルールに記述されたトポロジ情報に対応するIT装置検索条件を求める
S103
END
トポロジのうち、クライアント側のIT装置を構成情報から検索する
S104
検索されたIT装置で未選択なIT装置が管理対象に存在する
S105
NO
YES
見つかったクライアント側のIT装置のうち、1つを選択し、選択済みとする
S106
ペアとなるサーバ側の検索情報をクライアントのIT装置から取得する
S107
S120 又はS121より
取得したサーバの検索情報で未検索のものが存在する
S108
NO
YES
未検索の検索情報に対応するサーバ側のIT装置を検索する
S109
S110へ

[図8]

図8

TL2

	C201 Computer	C202 ConnectedIscsiTarget
L201	N10	iqn.1994-04.com. domain2:sos.df700.t.com.domain2.10966.0b027
L202	N10	iqn.1994-04.com. domain:sos.df700.t.com.domain.10966.0b055
L202	N11	iqn.1994-04.com. domain:sos.df700.t.com.domain.10966.0b055
	⋮	⋮

[図9]

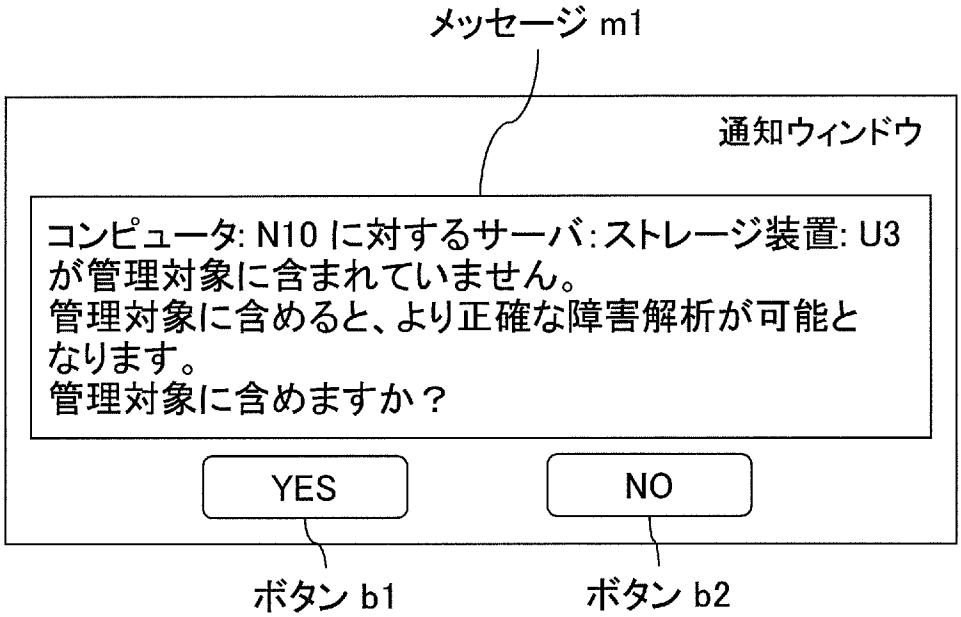
図9

TL3

	C301 Storage	C302 IscsiTarget
L301	N40	iqn.1994-04.com.domain:sos.df700.t.com.domain.10966.0b055

[図10]

図10



[図11]

図11

TL4

	ID	C401 種別	C402 ノード識別子	C403 サービス識別情報
L401	U1	IP-SAN Storage	192.168.100.15	iqn.1994-04.com.domain2:sos.df700.t.com.domain1.10966.0b027
L402	U2	FC-SAN Storage	192.168.10.16	50:06:0E:85:10:03:4D:01
L403	U3	File Server	exportfs.domain2.com	export_01
L404	U4	DNS Server	192.168.100.1	-
	⋮	⋮	⋮	⋮

[図12]

図12

TL1

	C101 ルール	C102 適用先IT装置リスト
L101	R1	N10, N40
L102	R1	N11, N40
L103	R2	N13, N41
L104	R3	N11, N12
L105	R1	N10, U1
L106	R2	N13, U2
L107	R3	N10, U3
L108	R3	N11, U5
L109	R4	N10, U4
L110	R4	N11, U4
	⋮	⋮

[図13]

図13

TL5

	C501 Computer	C502 ConnectedFcPortWWN
L501	N13	50:06:0E:85:10:03:4D:01
L502	N13	50:06:0E:85:10:03:4D:02
	⋮	⋮

[図14]

図14

TL6

	C601 Storage	C602 FcPortWWN
L601	N41	50:06:0E:85:10:03:4D:02

[図15]

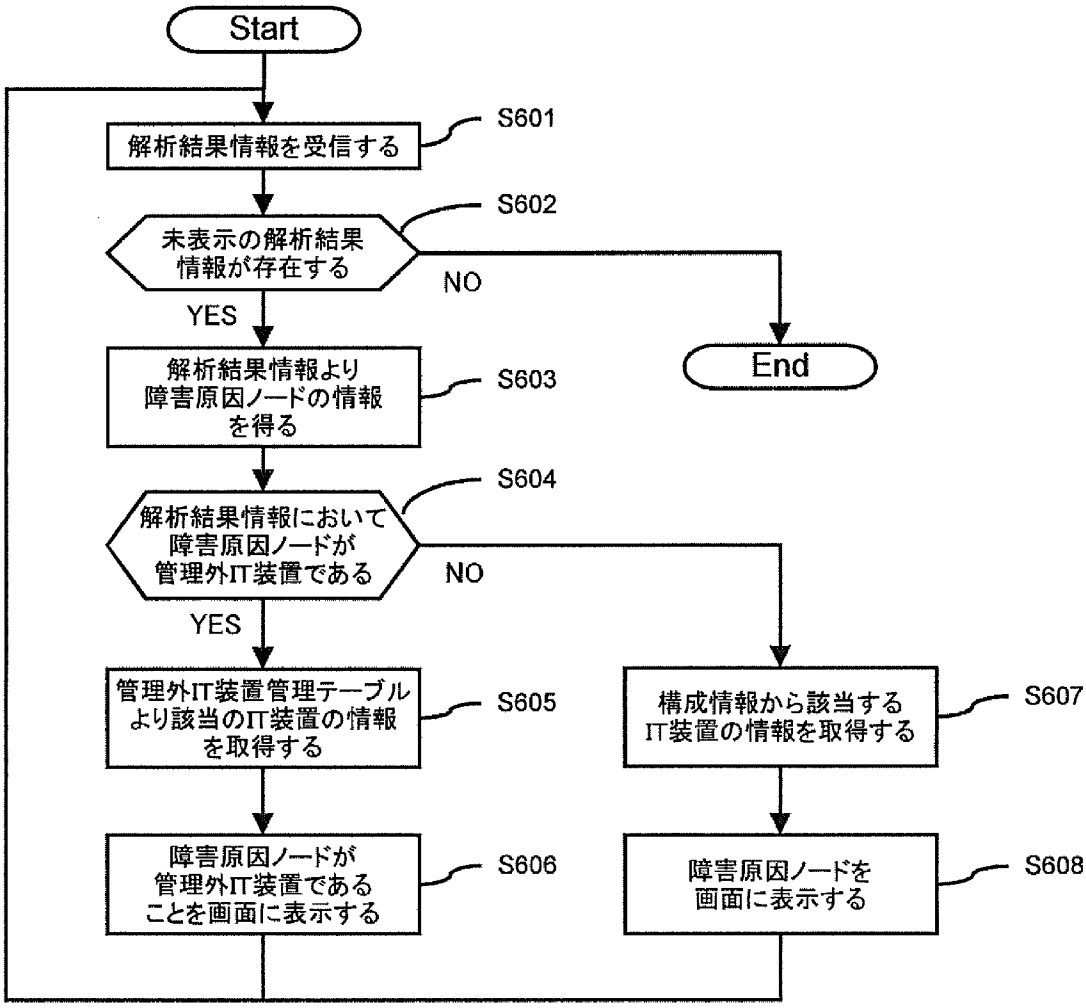
図15

TL7

	C10 コンピュータ	C11 ファイルサーバ識別情報	C12 公開名
L701	N10	exportfs.domain2.com	export_01
L702	N11	N12	share_docs
L703	N11	192.168.10.15	/export/home
	⋮	⋮	⋮

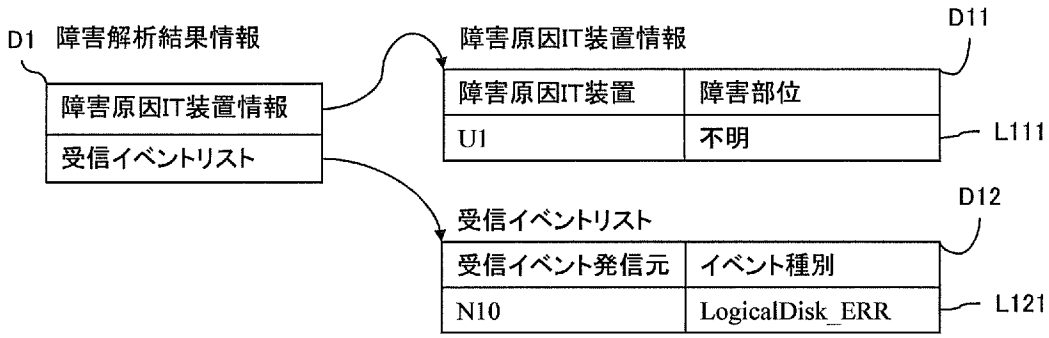
[図16]

図16



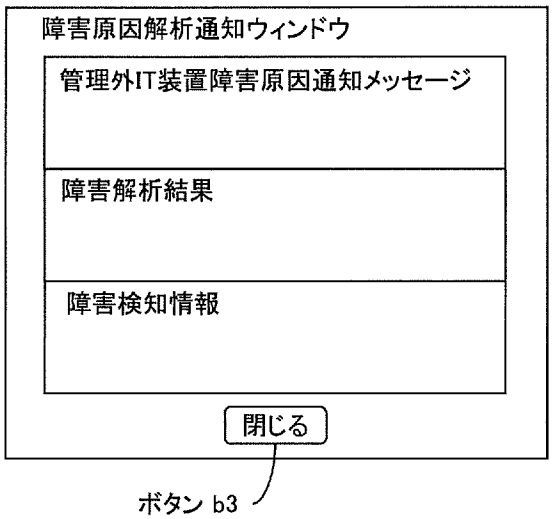
[図17]

図17



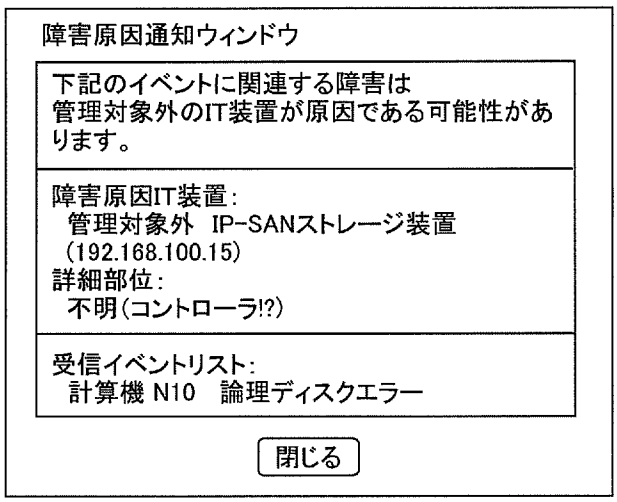
[図18]

図18



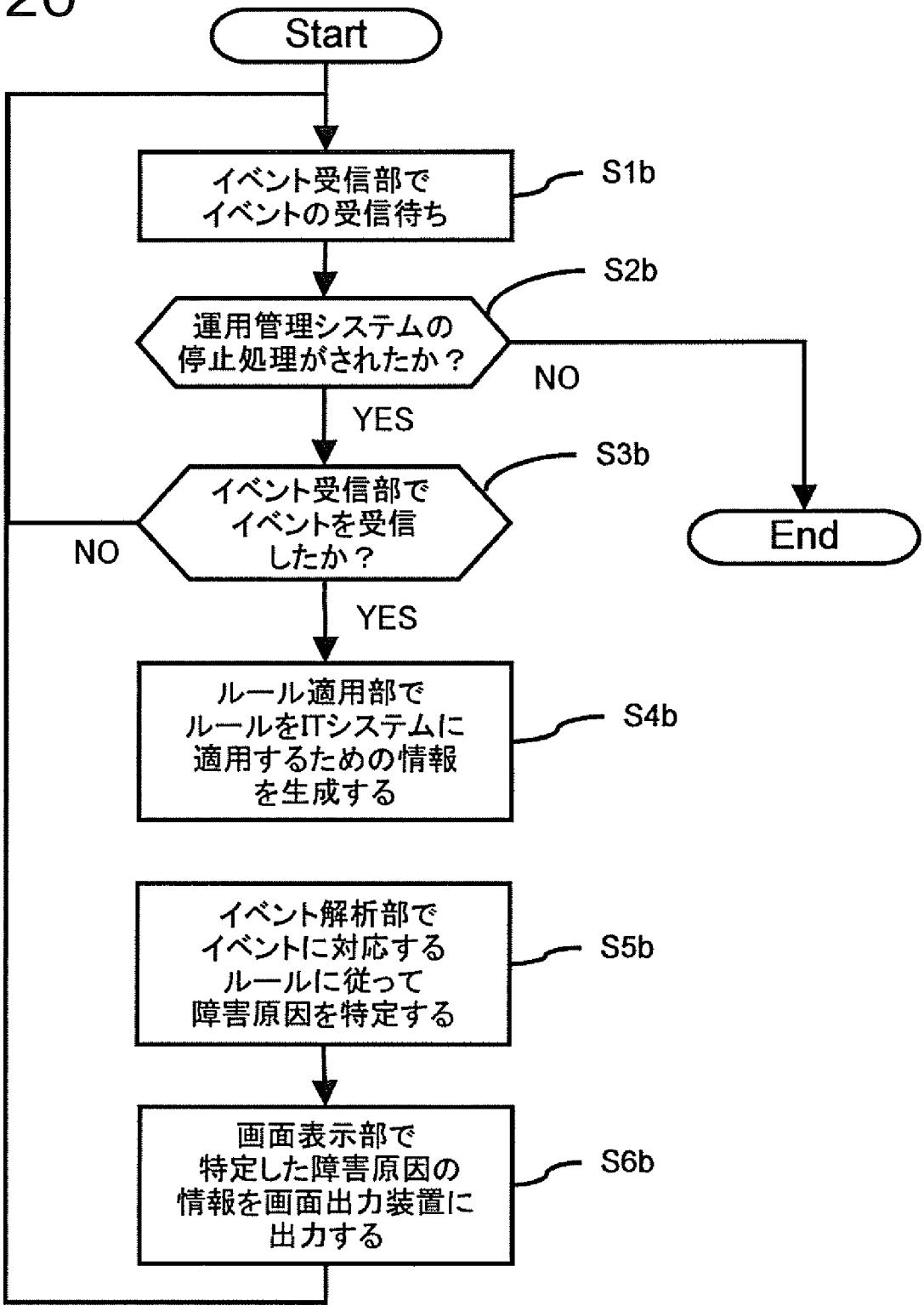
[図19]

図19



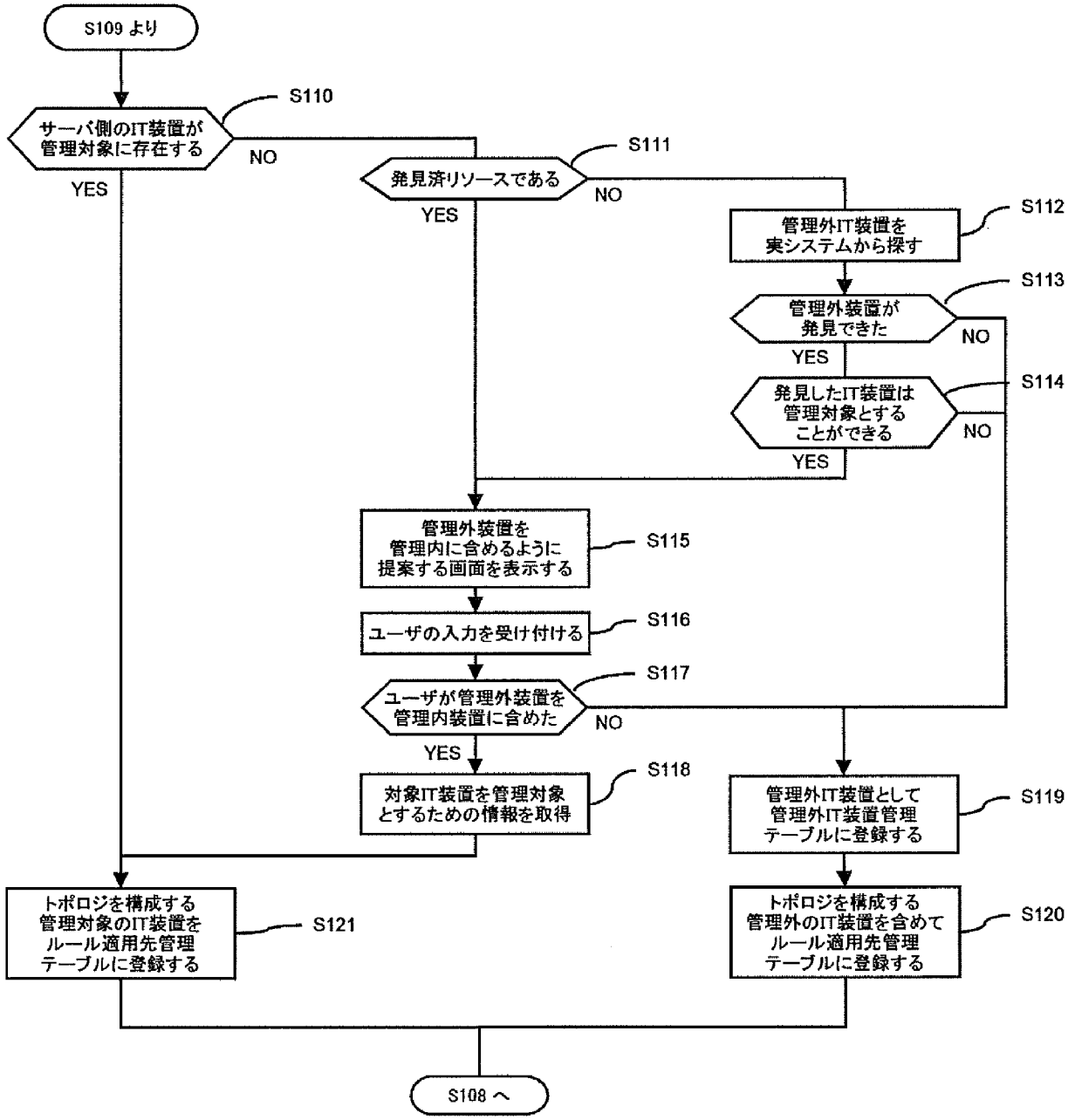
[図20]

図20


Start
イベント受信部で
イベントの受信待ち
S1b
運用管理システムの
停止処理がされたか？
S2b
NO
YES
イベント受信部で
イベントを受信
したか？
S3b
NO
End
YES
ルール適用部で
ルールをITシステムに
適用するための情報
を生成する
S4b
イベント解析部で
イベントに対応する
ルールに従って
障害原因を特定する
S5b
画面表示部で
特定した障害原因の
情報を画面出力装置に
出力する
S6b

[図21]

図21


S109 より
S110
サーバ側のIT装置が管理対象に存在する
NO
YES
S111
発見済リソースである
NO
YES
S112
管理外IT装置を実システムから探す
S113
管理外装置が発見できた
NO
YES
S114
発見したIT装置は管理対象とすることができる
NO
YES
S115
管理外装置を管理内に含めるように提案する画面を表示する
S116
ユーザの入力を受け付ける
S117
ユーザが管理外装置を管理内装置に含めた
NO
YES
S118
対象IT装置を管理対象とするための情報を取得
S119
管理外IT装置として管理外IT装置管理テーブルに登録する
S120
トポロジを構成する管理外のIT装置を含めてルール適用先管理テーブルに登録する
S121
トポロジを構成する管理対象のIT装置をルール適用先管理テーブルに登録する
S108 へ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/000285

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)
G06F11/30, G06F11/34

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 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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 2004-348640 A (Hitachi, Ltd.), 09 December, 2004 (09.12.04), Full text; all drawings (Family: none)	1-14
A	JP 2007-334716 A (NEC Corp.), 27 December, 2007 (27.12.07), Full text; all drawings (Family: none)	1-14
A	JP 2006-133983 A (Hitachi, Ltd.), 25 May, 2006 (25.05.06), Full text; all drawings & US 2006/0230122 A1	1-14

☒ 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	Date of mailing of the international search report
27 February, 2009 (27.02.09)	10 March, 2009 (10.03.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/000285

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 2006-338305 A (Toshiba Corp.), 14 December, 2006 (14.12.06), Full text; all drawings (Family: none)	1-14
A	JP 11-259331 A (Nippon Telegraph And Telephone Corp.), 24 September, 1999 (24.09.99), Full text; all drawings (Family: none)	1-14
A	JP 2005-316728 A (Mitsubishi Electric Corp.), 10 November, 2005 (10.11.05), Full text; all drawings (Family: none)	1-14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０００２８５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

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（ＩＰＣ））

Int.Cl.　G06F11/30, G06F11/34

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	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９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 2004-348640 A (株式会社日立製作所) 2004.12.09, 全文, 全図 (ファミリーなし)	１－１４
A	JP 2007-334716 A (日本電気株式会社) 2007.12.27, 全文, 全図 (ファミリーなし)	１－１４
A	JP 2006-133983 A (株式会社日立製作所) 2006.05.25, 全文, 全図 & US 2006/0230122 A1	１－１４

☑　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 ２７．０２．２００９	国際調査報告の発送日 １０．０３．２００９
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）　５Ｂ　３５６２ 多胡　滋 電話番号　０３－３５８１－１１０１　内線　３５４５

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	JP 2006-338305 A（株式会社東芝）2006.12.14，全文，全図（ファミリーなし）	１－１４
Ａ	JP 11-259331 A（日本電信電話株式会社）1999.09.24，全文，全図（ファミリーなし）	１－１４
Ａ	JP 2005-316728 A（三菱電機株式会社）2005.11.10，全文，全図（ファミリーなし）	１－１４