(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
2015 年 9 月 24 日(24.09.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/141221 A1

(51) 国際特許分類:
G06F 11/34 (2006.01)

(21) 国際出願番号: PCT/JP2015/001500

(22) 国際出願日: 2015 年 3 月 18 日(18.03.2015)

(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 2014-058497 2014 年 3 月 20 日(20.03.2014) JP
PCT/JP2014/003007 2014 年 6 月 5 日(05.06.2014) JP

(71) 出願人: 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 野村　崇志(NOMURA, Takashi); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 喜田　弘司(KIDA, Koji); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 上村　純平(KAMIMURA, Junpei); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 榮　純明(SAKAE, Yoshiaki); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 勝田　悦子(KATSUDA, Etsuko); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 山崎　健太郎(YAMASAKI, Kentaro); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 小林　佑嗣(KOBAYASHI, Yuji); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP). 磯山　和彦(ISOYAMA, Kazuhiko); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

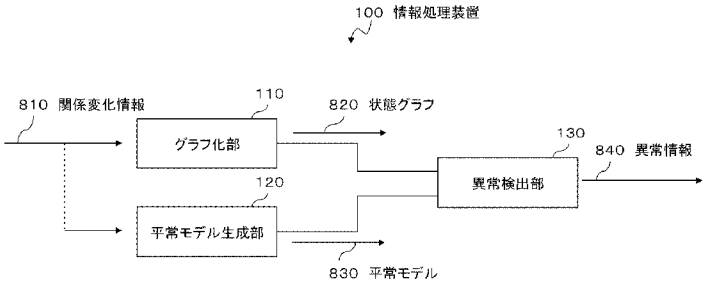
(74) 代理人: 下坂　直樹(SHIMOSAKA, Naoki); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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.

[続葉有]

(54) **Title**: INFORMATION PROCESSING DEVICE AND ERROR DETECTION METHOD

(54) 発明の名称 : 情報処理装置及び異常検知方法



100 Information processing device
110 Graphing unit
120 Normal model generation unit
130 Error detection unit
810 Relationship change information
820 State graph
830 Normal model
840 Error information

(57) **Abstract**: The present invention provides an information processing device that improves the detectability of system errors. This information processing device comprises: a means that generates a state graph on the basis of relationship change information indicating change in the relationship between a plurality of elements included in a system, said state graph having the elements as the vertices thereof and the relationship between the elements as the sides thereof; a means that generates a normal model having the state graph as a set of conditions to be fulfilled during normal system operation, on the basis of the relationship change information; and a means that detects system errors and outputs error information indicating detected errors, on the basis of the state graph and the normal model.

(57) 要約:

[続葉有]

WO 2015/141221 A1

(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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

本発明は、システムの異常についての検出性を向上する情報処理装置を提供する。その情報処理装置は、システムに含まれる複数の要素の関係の変化を示す関係変化情報に基づいて、その要素を頂点とし、その要素間の関係を辺とする、状態グラフを生成する手段と、その関係変化情報に基づいて、その状態グラフが、システムの平常時に満たすべき条件の集合である平常モデルを生成する手段と、状態グラフと平常モデルとに基づいて、システムに係る異常を検出し、検出した異常を示す異常情報を出力する手段と、を備える。

明　細　書

発明の名称 ： 情報処理装置及び異常検知方法

技術分野

[0001] 本発明は、システムの異常を検知する技術に関する。

背景技術

[0002] システムの異常を検知するためのさまざまな関連技術が知られている。

[0003] 例えば、特許文献１は、プロセス監視装置を開示する。特許文献１のプロセス監視装置は、以下のように動作する。

[0004] 第１に、そのプロセス監視装置は、プロセスの静的属性に基づいて要注意プロセスを抽出する。その静的属性は、例えば、プロセス名、そのプロセスに係るプログラムのメーカ名、プログラム（ソフトウェア）名、バージョン、このプロセスを起動した親プロセス名、及びプロセスサイズを含む。そのプロセス監視装置は、現在の静的属性が過去の静的属性から変化している場合に、該当するプロセスを要注意プロセスとして抽出する。そのプロセス監視装置は、過去の静的属性が存在しない場合に、該当するプロセスを要注意プロセスとして抽出する。そのプロセス監視装置は、親プロセスが発見できない場合に、該当するプロセスを要注意プロセスとして抽出する。更に、そのプロセス監視装置は、外部プロセスが親プロセスとなっている場合に、該当するプロセスを要注意プロセスとして抽出する。

[0005] 第２に、そのプロセス監視装置は、動的属性に基づいて、要注意プロセスについて警報を発する。動的属性は、例えば、動的専用メモリバイト数、動的共有メモリバイト数、リダイレクタの送信、受信トラフィック率、及びハードディスクアクセス率である。そのプロセス監視装置は、過去の動的属性と現在の動的属性とが統計的手法を用いて弁別可能である場合に、該当する要注意プロセスについて、警報の発生や監視対象プロセスとしての登録などを実行する。

[0006] 第３に、そのプロセス監視装置は、要注意プロセスと所定の関連性を有す

る関連プロセスを抽出し、その関連プロセスを監視対象プロセスとする。所定の関連性を持つプロセスとは、例えば、明確な親子リレーションがあるプロセス、明確な親子リレーションはないが、監視対象プロセスが動作するときに常に起動されるプロセスなどである。

[0007] 特許文献２は、セキュリティアプリケーションにおけるクラウドコンピューティングの使用に関連する技術を開示する。特許文献２のシステムは、以下のように動作する。

[0008] 第１に、そのシステムは、クライアントのトラフィックを監視する。

[0009] 第２に、そのシステムは、その監視したトラフィックと、そのクライアントの動作モードに対応する予測トラフィックパターンとを比較する。

[0010] 第３に、そのシステムは、その比較した結果に基づいて、セキュリティ脅威が示されているか否かを決定する。

先行技術文献

特許文献

[0011] 特許文献1：特開２００８－０２１２７４号公報

特許文献2：特表２０１２－５２３１５９号公報

発明の概要

発明が解決しようとする課題

[0012] しかしながら、上述の先行技術文献に記載された技術においては、個々の要素単位での異常、或いは予め定義される攻撃パターンによる異常を検出するにすぎないという問題点がある。換言すると、例えば、コンピュータシステムに対する未知の標的型攻撃による異常についての、検出が困難である、という問題点がある。

[0013] その理由は、特許文献１に記載された技術は、個々のプロセスについて、予め定義された静的属性及び動的属性に基づいて、異常を検出するにすぎないからである。そして、特許文献１に記載された技術は、関連プロセスの抽出において、親子関係と起動の同期性とについて考慮しているにすぎないか

らである。

[0014] また、特許文献２に記載された技術は、予測トラフィックパターンに基づいて、クライアントのトラフィックの異常を検出するにすぎないからである。

[0015] 本発明の目的は、上述した問題点を解決する情報処理装置、監視方法、及び、そのためのプログラム或いはそのプログラムを記録したコンピュータ読み取り可能な非一時的記録媒体を提供することにある。

課題を解決するための手段

[0016] 本発明の一様態における情報処理装置は、システムに含まれる複数の要素の、関係の変化を示す関係変化情報を時系列的に取得し、前記関係変化情報に基づいて、前記要素を頂点とし前記要素間の関係を辺とする状態グラフを生成するグラフ化手段と、前記関係変化情報に基づいて、前記状態グラフが、前記システムの平常時に満たすべき条件の集合である平常モデルを生成する平常モデル生成手段と、前記状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出し、検出した前記異常を示す異常情報を出力する異常検出手段と、を含む。

[0017] 本発明の一様態における異常検知方法は、システムに含まれる複数の要素の、関係の変化を示す関係変化情報を時系列的に取得し、前記関係変化情報に基づいて、前記要素を頂点とし前記要素間の関係を辺とする状態グラフを生成し、前記関係変化情報に基づいて、前記状態グラフが、前記システムの平常時に満たすべき条件の集合である平常モデルを生成し、前記状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出し、検出した前記異常を示す異常情報を出力する。

[0018] 本発明の一様態におけるコンピュータ読み取り可能な非一時的記録媒体は、システムに含まれる複数の要素の、関係の変化を示す関係変化情報を時系列的に取得し、前記関係変化情報に基づいて、前記要素を頂点とし前記要素間の関係を辺とする状態グラフを生成し、前記関係変化情報に基づいて、前記状態グラフが、前記システムの平常時に満たすべき条件の集合である平常

モデルを生成し、前記状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出し、検出した前記異常を示す異常情報を出力する、処理をコンピュータに実行させるプログラムを記録する。

発明の効果

[0019] 本発明は、システムの異常についての検出性を向上することが可能になるという効果がある。

図面の簡単な説明

[0020] [図1]図１は、本発明の第１の実施形態に係る情報処理装置の構成を示すブロック図である。

[図2]図２は、第１の実施形態に係る情報処理装置と監視対象システムとを備える情報処理システムの構成を示すブロック図である。

[図3]図３は、第１の実施形態における関係変化情報の一例を示す図である。

[図4]図４は、第１の実施形態における状態グラフの一例を示す図である。

[図5]図５は、第１の実施形態における状態グラフで表される要素間の関係を示す概念図である。

[図6]図６は、第１の実施形態における平常モデルの一例を示す図である。

[図7]図７は、第１の実施形態における異常情報の一例を示す図である。

[図8]図８は、第１の実施形態に係る情報処理装置を実現するコンピュータのハードウェア構成を示すブロック図である。

[図9]図９は、第１の実施形態における情報処理装置の動作を示すフローチャートである。

[図10]図１０は、第１の実施形態における情報処理装置の動作を示すフローチャートである。

[図11]図１１は、第１の実施形態における関係変化情報の一例を示す図である。

[図12]図１２は、第１の実施形態における状態グラフの一例を示す図である。

[図13]図１３は、本発明の第２の実施形態に係る情報処理装置の構成を示す

ブロック図である。

[図14]図１４は、第２の実施形態における異常情報の一例を示す図である。

[図15]図１５は、本発明の第３の実施形態に係る情報処理装置の構成を示すブロック図である。

[図16]図１６は、第３の実施形態における異常情報の一例を示す図である。

[図17]図１７は、本発明の第４の実施形態に係る情報処理装置の構成を示すブロック図である。

[図18]図１８は、第４の実施形態における異常情報の一例を示す図である。

[図19]図１９は、第４の実施形態における異常情報の他の一例を示す図である。

[図20]図２０は、本発明の第５の実施形態に係る情報処理装置の構成を示すブロック図である。

発明を実施するための形態

[0021] 本発明を実施するための形態について図面を参照して詳細に説明する。尚、各図面及び明細書記載の各実施形態において、同様の構成要素には同様の符号を付与し、適宜説明を省略する。

[0022] ＜＜＜第１の実施形態＞＞＞

図１は、本発明の第１の実施形態に係る情報処理装置１００の構成を示すブロック図である。

[0023] 図１に示すように、本実施形態に係る情報処理装置１００は、グラフ化部１１０、平常モデル生成部１２０及び異常検出部１３０を含む。尚、図１に示す構成要素は、ハードウェア単位の回路でも、コンピュータ装置の機能単位に分割された構成要素でもよい。ここでは、図１に示す構成要素は、コンピュータ装置の機能単位に分割された構成要素として説明する。

[0024] 図２は、情報処理装置１００と監視対象システム（単に「システム」とも呼ばれる）９００と関係変化監視手段９３０とを含む、情報処理システムの構成を示すブロック図である。

[0025] ＝＝＝監視対象システム９００＝＝＝

監視対象システム９００は、複数の要素９２０を含む。そして、その要素９２０のそれぞれは、他のその要素９２０のそれぞれと何らかの関係を有する。

[0026] 例えば、監視対象システム９００は、ネットワークで接続された複数のホスト（不図示）を含み、そのホスト上でプロセス（不図示）が動作する、情報処理システムである。

[0027] また、監視対象システム９００は、ソーシャルネットワークであってよい。

[0028] また、監視対象システム９００は、何らかの構造を有するデータアイテム（要素９２０）の集合であってもよい。何らかの構造を有するデータアイテムの集合は、例えば、ハイパーリンクと被ハイパーリンクとの関係を有するファイルの集合である。

[0029] 以上の例に関わらず、監視対象システム９００は、任意のシステムであってよい。

[0030] ＝＝＝関係変化監視手段９３０＝＝＝

関係変化監視手段９３０は、監視対象システム９００に含まれる要素９２０間の、関係の変化を監視する。そして、関係変化監視手段９３０は、検出したその関係の変化を関係変化情報８１０として、情報処理装置１００に送信する。尚、関係変化監視手段９３０は、監視対象システム９００に含まれてもよい。

[0031] 監視対象システム９００が情報処理システムである場合、関係変化監視手段９３０は、例えば、ホスト上で動作するエージェントであってよい。例えば、そのエージェントは、そのホスト上で動作するプロセスの挙動を監視し、プロセスイベントログを情報処理装置１００に送信する。

[0032] 監視対象システム９００がソーシャルネットワークである場合、関係変化監視手段９３０は、例えば、メールサーバ上で動作するメール監視エージェントであってよい。ここで、ソーシャルネットワークは、ソーシャル・ネットワーキング・サービス（ＳＮＳ（Ｓｏｃｉａｌ　Ｎｅｔｗｏｒｋｉｎｇ

Ｓｅｒｖｉｃｅ））により構築されるネットワークである。例えば、そのメール監視エージェントは、ユーザ間でやり取りされるメールを監視し、メール送受信ログを情報処理装置１００に送信する。或いは、関係変化監視手段９３０は、ＳＮＳ用のサーバ上で動作する、エージェントであってもよい。そのエージェントは、ＳＮＳにおける友人申請情報（メッセージ情報）や、友人同士の繋がり（ユーザ接続情報／リンクの増加）、及びそれらの変化などを監視する。

[0033] 監視対象システム９００がウェブページの集合である場合、関係変化監視手段９３０は、例えば、ウェブサーバ上で動作するエージェントであってよい。例えば、そのエージェントは、例えば、ウェブページの生成や、消去、ウェブページ間のハイパーリンク関係などの変化を任意に監視し、その変化の内容を示すイベントログを情報処理装置１００に送信する。

[0034] 尚、関係変化監視手段９３０は、上述の例に係わらず、任意のシステムの任意の要素９２０間の関係の変化を監視し、任意の関係変化情報８１０を情報処理装置１００に送信してよい。

[0035] 情報処理装置１００と関係変化監視手段９３０とは、図示しないネットワークで接続されている。尚、図２の例に係わらず、同一の或いは異なる監視対象システム９００を監視する、複数の関係変化監視手段９３０が、情報処理装置１００に接続されてよい。

[0036] ＝＝＝情報処理装置１００のグラフ化部１１０＝＝＝

グラフ化部１１０は、例えば関係変化監視手段９３０から、監視対象システム９００の関係変化情報８１０を時系列的に取得する。次に、グラフ化部１１０は、取得した関係変化情報８１０に基づいて、状態グラフ８２０を生成し、その状態グラフ８２０を異常検出部１３０へ出力する。

[0037] ＝＝＝関係変化情報８１０＝＝＝

関係変化情報８１０は、監視対象システム９００に含まれる要素９２０間の、関係の変化を示す情報である。具体的には、関係変化情報８１０は、上述したように、さまざまな関係変化監視手段９３０から送信される情報であ

る。

[0038] 図３は、関係変化情報８１０の具体的な例である、関係変化情報８１１の一例を示す図である。図３に示す関係変化情報８１１は、「要素９２０「Ｅ２」と要素９２０「Ｅ３」との間に、種別「Ｌ２」の関係が発生した」というイベントを示す。尚、「Ｅ２」及び「Ｅ３」は要素９２０の識別子である。例えば、要素９２０「Ｅ２」は、識別子が「Ｅ２」である要素９２０を示す。また、「Ｌ２」は、要素９２０間の関係の種別の識別子である。例えば、種別「Ｌ２」は、識別子が「Ｌ２」である、要素９２０間の関係の種別を示す。

[0039] ＝＝＝状態グラフ８２０＝＝＝

状態グラフ８２０は、要素９２０のそれぞれを頂点（ノードあるいは節点とも呼ばれる）とし、及びそれらの要素９２０間の関係を辺（リンク、エッジ或いは枝とも呼ばれる）とする、グラフである。状態グラフ８２０は、監視対象システム９００内の要素９２０間の関係を表す。ここで、その関係は、例えば、「ある期間に、要素間でデータが伝達された」というデータ伝達関係や、「ある瞬間（または期間）に、要素間でデータ伝達が行われうる状態である」というデータ伝達関係などである。

[0040] 図４は、状態グラフ８２０の具体的な例である、状態グラフ８２１の一例を示す図である。図４に示すように、状態グラフ８２１は、頂点識別子と辺とを含むレコードからなる。頂点識別子は、頂点となる要素９２０の識別子である。辺は、頂点識別子のそれぞれで特定される頂点（要素９２０）と、他の頂点（要素９２０）との関係を示す情報である。

[0041] 例えば、頂点識別子の「Ｅ１」は、識別子が「Ｅ１」である要素９２０を特定する。そして、頂点識別子「Ｅ１」に対応する辺の「Ｅ２；Ｌ０、 Ｅ３；Ｌ１；Ｌ１」は、以下のことを示す。第１に、要素９２０「Ｅ１」は、要素９２０「Ｅ２」との辺を有し、その辺の属性は、「Ｌ０」である。第２に、要素９２０「Ｅ１」は、要素９２０「Ｅ３」との辺を２つ有し、その辺の属性は、いずれも「Ｌ１」である。

[0042] 例えば、頂点識別子が「Ｅ４」のレコードにおいて、辺が空欄であることは、要素９２０「Ｅ４」は、他のいずれの要素９２０に対しても、辺を持たないことを示す。

[0043] 辺は、例えば、その辺を有する要素９２０間において、通信を実行するための準備が完了している状態にあることを示す。辺の属性は、例えば、その辺において実行される通信の、プロトコルの種別を示す。尚、辺や辺の属性（例えば、種別）などは、上述の例に限らず、要素９２０間の関係を示す、任意の定義であってよい。

[0044] 例えば、頂点識別子が「Ｅ２」のレコードにおける辺の「Ｅ３；Ｌ２」、及び頂点識別子が「Ｅ３」のレコードにおける辺の「Ｅ２；Ｌ２」は、図３に示す関係変化情報８１１に基づくものである。

[0045] 尚、状態グラフ８２０は、上述の例に係わらず任意の形式の状態グラフ８２０であってよい。

[0046] ＝＝＝状態グラフ８２０で表される要素９２０間の関係＝＝＝

図５は、状態グラフ８２１で表される要素９２０間の、関係を示す概念図である。

[0047] 図５において、頂点は円形で示され、円形の中に頂点識別子が示されている。また、辺は円形を結ぶ線分で示されている。例えば、実線で示す線分は、種別が「Ｌ０」の辺を示す。一点鎖線で示す線分は、種別が「Ｌ１」の辺を示す。２点鎖線で示す線分は、種別が「Ｌ２」の辺を示す。また、矢印は、関係を生成する側から外へ向かう方向を示す。

[0048] ＝＝＝情報処理装置１００の平常モデル生成部１２０＝＝＝

平常モデル生成部１２０は、関係変化情報８１０に基づいて平常モデル８３０を生成し、その平常モデル８３０を異常検出部１３０へ出力する。その平常モデル８３０は、状態グラフ８２０が、監視対象システム９００の平常時に満たすべき条件の集合である。

[0049] ＝＝＝平常モデル８３０＝＝＝

図６は、平常モデル８３０の具体的な例である、平常モデル８３１の一例

を示す図である。図６に示すように、平常モデル８３１は、条件種別と条件値と有効フラグとを含むレコードからなる。

[0050] 例えば、条件種別が「関係頂点数」のレコードの、条件値の「上限値２」は、「１つの頂点（要素９２０）との辺を持つ他の要素９２０の数が２以下であること」という条件を示す。また、条件種別が「次数」のレコードの、条件値の「上限値６」は、「１つの頂点から出る辺の数が６以下であること」という条件を示す。また、条件種別が「辺属性」のレコードは、辺の属性（例えば、関係の種類や、頻度、関係の主従を示す方向、関係発生の時刻、など）の条件を示す。有効フラグは、そのレコードに含まれる条件値が有効か否かを示す。有効フラグの初期値は「無効」である。

[0051] 平常モデル生成部１２０は、例えば、所定期間における、全頂点のそれぞれの「関係頂点数」の平均値に、所定の値を加算した値を、条件種別が「関係頂点数」のレコードの条件値としてよい。その所定期間は、例えば、過去の特定の時刻から現在時刻までの期間（期間Ｐａと呼ぶ）である。また、その所定期間は、現在時刻から特定の時間遡った過去の時刻までの期間（期間Ｐｂと呼ぶ）であってよい。また、その所定期間は、過去の特定の第１の時刻から過去の特定の第２の時刻までの期間（期間Ｐｃと呼ぶ）であってよい。また、その所定期間は、所定の数の関係変化情報８１０を取得するのに要する期間であってよい。即ち、その所定期間は、現在時刻或いは過去の特定の時刻に対する最近の、所定数の関係変化情報８１０を取得した期間（期間Ｐｄ（対現在時刻）或いは期間Ｐｅ（対過去の時刻）と呼ぶ）であってもよい。更にその所定の期間は、期間Ｐａ、期間Ｐｂ、期間Ｐｃ或いは期間Ｐｄの期間中の、所定の断続的な期間であってよい。以上説明したように、平常モデル生成部１２０は、過去の固定期間（期間Ｐｃ及び期間Ｐｅ）或いは逐次的に変化する期間（期間Ｐａ、期間Ｐｂ及び期間Ｐｄ）などの任意の期間の関係変化情報８１０に基づいて平常モデル８３０を生成してよい。平常モデル生成部１２０が逐次的に変化する期間の関係変化情報８１０に基づいて平常モデル８３０を生成する場合、平常モデル８３０は、逐次的な関係変化

情報８１０の入力に従って、逐次的に更新される。

[0052] 上述の例に係わらず、平常モデル生成部１２０は、関係変化情報８１０に基づいて、任意の手法を用いて、任意の条件種別に対する条件値を算出してよい。

[0053] 平常モデル生成部１２０は、例えば、所定数の関係変化情報８１０に基づいて、条件値を生成或いは更新した場合に、有効フラグを「有効」に設定する。また、平常モデル生成部１２０は、所定期間の関係変化情報８１０に基づいて、条件値を生成或いは更新した場合に、有効フラグを「有効」に設定してもよい。

[0054] 平常モデル８３０は、上述の例に係わらず、以下に示すような種別の条件を示すレコードを含んでよい。

[0055] 平常モデル８３０は、頂点の属性（例えば、要素９２０の種類や、その頂点の発生した時刻、など）に対する条件のレコードを含んでよい。

[0056] 平常モデル８３０は、隣接頂点の属性に対する条件のレコードを含んでよい。

[0057] 平常モデル８３０は、頂点間のパスの有無や、本数、距離、経路中の頂点及び辺の属性などに対する任意の条件の、レコードを含んでよい。

[0058] 更に、平常モデル８３０は、グラフの特性（例えば、直径や、中心性、部分構造、など）に対する条件のレコードを含んでよい。

[0059] ＝＝＝情報処理装置１００の異常検出部１３０＝＝＝

異常検出部１３０は、状態グラフ８２０と平常モデル８３０とに基づいて、監視対象システム９００に係る異常を検出し、検出した異常を示す異常情報８４０を出力する。

[0060] 異常情報８４０は、例えば、監視対象システム９００の何らかの異常を検出したという情報である。また、異常情報８４０は、その異常に関する任意の情報を含んでよい。

[0061] 異常検出部１３０は、任意のタイミングで異常情報８４０を出力してよい。例えば、異常検出部１３０は、ある異常を検出した時点で、その検出した

異常を示す異常情報８４０を出力する。また、異常検出部１３０は、検出した異常を保持し、要求（所定の時刻や、管理者による指示）に応じて、保持している異常を示す異常情報８４０を出力してよい。更に、異常検出部１３０は、その要求に含まれる時刻（時間範囲）に対応する、状態グラフ８２０に対して異常を検出してもよい。

図７は、異常情報８４０の具体的な例である、異常情報８４１の一例を示す図である。図７に示すように、異常情報８４１は、関係頂点数の上限値の超過が発生したことを示す。

[0062] 以上が、情報処理装置１００の機能単位の構成要素についての説明である。

[0063] 次に、情報処理装置１００のハードウェア単位の構成要素について説明する。

[0064] 図８は、本実施形態における情報処理装置１００を実現するコンピュータ７００のハードウェア構成を示す図である。

[0065] 図８に示すように、コンピュータ７００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）７０１、記憶部７０２、記憶装置７０３、入力部７０４、出力部７０５及び通信部７０６を含む。更に、コンピュータ７００は、外部から供給される記録媒体（または記憶媒体）７０７を含む。例えば、記録媒体７０７は、情報を非一時的に記憶する不揮発性記録媒体（非一時的記録媒体）である。また、記録媒体７０７は、情報を信号として保持する、一時的記録媒体であってもよい。

[0066] ＣＰＵ７０１は、オペレーティングシステム（不図示）を動作させて、コンピュータ７００の全体の動作を制御する。例えば、ＣＰＵ７０１は、記憶装置７０３に装着された記録媒体７０７から、そのプログラムやデータを読み込み、読み込んだそのプログラムやそのデータを記憶部７０２に書き込む。ここで、そのプログラムは、例えば、後述の図９及び図１０に示すフローチャートの動作をコンピュータ７００に実行させるためのプログラムである。

[0067] そして、ＣＰＵ７０１は、その読み込んだプログラムに従って、またその読み込んだデータに基づいて、図１に示すグラフ化部１１０、平常モデル生成部１２０及び異常検出部１３０として各種の処理を実行する。

[0068] 尚、ＣＰＵ７０１は、通信網（不図示）に接続される外部コンピュータ（不図示）から、記憶部７０２にそのプログラムやそのデータをダウンロードしてもよい。

[0069] 記憶部７０２は、そのプログラムやそのデータを記憶する。記憶部７０２は、関係変化情報８１０や状態グラフ８２０、平常モデル８３０、異常情報８４０などを記憶してよい。

[0070] 記憶装置７０３は、例えば、任意の、光ディスク、フレキシブルディスク、磁気光ディスク、外付けハードディスク及び半導体メモリであって、記録媒体７０７を含む。記憶装置７０３（記録媒体７０７）は、そのプログラムをコンピュータ読み取り可能に記憶する。また、記憶装置７０３は、そのデータを記憶してもよい。記憶装置７０３は、関係変化情報８１０や状態グラフ８２０、平常モデル８３０、異常情報８４０などを記憶してよい。

[0071] 入力部７０４は、オペレータによる操作の入力や外部からの情報の入力を受け付ける。入力操作に用いられるデバイスは、例えば、任意の、マウスやキーボード、内蔵のキーボタン及びタッチパネルなどである。

[0072] 出力部７０５は、例えばディスプレイで実現される。出力部７０５は、例えばＧＵＩ（ＧＲＡＰＨＩＣＡＬ Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅ）によるオペレータへの入力要求や、オペレータに対する出力提示などのために用いられる。

[0073] 通信部７０６は、関係変化監視手段９３０とのインタフェースを実現する。通信部７０６は、グラフ化部１１０、平常モデル生成部１２０及び異常検出部１３０の一部として含まれてよい。

[0074] 以上説明したように、図１に示す情報処理装置１００の機能単位のブロックは、図８に示すハードウェア構成のコンピュータ７００によって実現される。但し、コンピュータ７００が備える各部の実現手段は、上記に限定され

ない。すなわち、コンピュータ７００は、物理的に結合した１つの装置により実現されてもよいし、物理的に分離した２つ以上の装置を有線または無線で接続し、これら複数の装置により実現されてもよい。

[0075] 尚、上述のプログラムのコードを記録した記録媒体７０７が、コンピュータ７００に供給される場合、ＣＰＵ７０１は、記録媒体７０７に格納されたそのプログラムのコードを読み出して実行してもよい。或いは、ＣＰＵ７０１は、記録媒体７０７に格納されたそのプログラムのコードを、記憶部７０２、記憶装置７０３またはその両方に格納してもよい。すなわち、本実施形態は、コンピュータ７００（ＣＰＵ７０１）が実行するそのプログラム（ソフトウェア）を、一時的にまたは非一時的に、記憶する記録媒体７０７の実施形態を含む。尚、情報を非一時的に記憶する記憶媒体は、不揮発性記憶媒体とも呼ばれる。

[0076] 以上が、本実施形態における情報処理装置１００を実現するコンピュータ７００の、ハードウェア単位の各構成要素についての説明である。

[0077] 次に本実施形態の動作について、図面を参照して詳細に説明する。

[0078] 図９及び図１０は、本実施形態の動作を示すフローチャートである。尚、このフローチャートによる処理は、前述したＣＰＵ７０１によるプログラム制御に基づいて、実行されてよい。また、処理のステップ名については、Ｓ６１０のように、記号で記載する。

[0079] グラフ化部１１０は、関係変化情報８１０を受信したことを契機に、図９に示すフローチャートの動作を開始する。尚、グラフ化部１１０は、例えば、図８に示す通信部７０６を介して、監視対象システム９００から関係変化情報８１０を受信する。

[0080] グラフ化部１１０は、受信した関係変化情報８１０に基づいて、状態グラフ８２０を生成（新たに生成或いは更新により生成）する（ステップＳ６０１）。グラフ化部１１０は、例えば、図８に示す記憶部７０２或いは記憶装置７０３に、状態グラフ８２０を保持する。

[0081] 次に、平常モデル生成部１２０は、受信した関係変化情報８１０に基づい

て、平常モデル８３０の内容を生成（新たに生成或いは更新により生成）する（ステップＳ６０２）。即ち、第１に、平常モデル生成部１２０は、受信した関係変化情報８１０に関連する条件種別を含むレコードの条件値を生成或いは更新する。そのレコードは、平常モデル８３０のレコードである。第２に、平常モデル生成部１２０は、そのレコードについて所定の条件（例えば、条件値の更新回数）を満足した場合に、そのレコードの有効フラグの設定を「有効」に変更する。平常モデル生成部１２０は、例えば、図８に示す記憶部７０２或いは記憶装置７０３に、平常モデル８３０を保持する。

[0082] 次に、異常検出部１３０は、状態グラフ８２０及び平常モデル８３０に基づいて、監視対象システム９００に係る異常の検出処理を実行する（ステップＳ６０３）。その後、処理は、終了する。

[0083] 図９に示すフローチャートでは、グラフ化部１１０と平常モデル生成部１２０と異常検出部１３０とは、直列的に順番に動作する。しかし、グラフ化部１１０と平常モデル生成部１２０と異常検出部１３０とは、並列的に動作してもよい。

[0084] 図９に示すフローチャートに示す動作では、異常検出部１３０は、平常モデル生成部１２０が平常モデル８３０の内容を更新するたびに、異常の検出処理を実行する。しかし、異常検出部１３０は、任意のタイミング（例えば、特定の時刻や、管理者の指示を受けたとき）で異常の検出処理を実行してよい。

[0085] 図９に示すフローチャートに示す動作では、グラフ化部１１０及び平常モデル生成部１２０のそれぞれは、関係変化情報８１０を受信するたびに状態グラフ８２０及び平常モデル８３０のそれぞれを更新する。しかし、グラフ化部１１０及び平常モデル生成部１２０のそれぞれは、受信した関係変化情報８１０を蓄積し、特定のタイミングで、蓄積した関係変化情報８１０に基づいて状態グラフ８２０及び平常モデル８３０のそれぞれを生成或いは更新してもよい。その特定のタイミングは、例えば、異常検出部１３０が異常情報８４０を生成する直前であってよい。

[0086] 異常検出部１３０は、図９のステップＳ６０３において、以下の図１０に示すフローチャートの動作を実行する。

[0087] 異常検出部１３０は、ステップＳ６３０とステップＳ６３８との間の処理を、平常モデル８３０の全てのレコードに対して実行する。

[0088] 異常検出部１３０は、平常モデル８３０からレコードを取得する（ステップＳ６３１）。

[0089] 次に、異常検出部１３０は、有効フラグに基づいて、そのレコードが有効か否かを判定する（ステップＳ６３２）。その有効フラグが「無効」である場合（ステップＳ６３２でＮＯ）、処理はステップＳ６３８へ進む。

[0090] その有効フラグが「有効」である場合（ステップＳ６３２でＹＥＳ）、異常検出部１３０は、ステップＳ６３３とステップＳ６３７との間の処理を、状態グラフ８２０から抽出可能な全ての被確認値に対して実行する。

[0091] 異常検出部１３０は、そのレコードに含まれる条件種別に対応する被確認値を、状態グラフ８２０から抽出する（ステップＳ６３４）。

[0092] 次に、異常検出部１３０は、その被確認値が、そのレコードに含まれる条件値に合致しているか否かを判定する（ステップＳ６３５）。

[0093] その被確認値がその条件値に合致している場合（ステップＳ６３５でＹＥＳ）、処理はステップＳ６３７へ進む。

[0094] その被確認値がその条件値に合致していない場合（ステップＳ６３５でＮＯ）、異常検出部１３０は、異常が発生したと判定し、その異常の内容を示す情報を含めるように、異常情報８４０を生成或いは更新する（ステップＳ６３６）。

[0095] 次に、その抽出可能な全ての被確認値に対して処理が実行された場合、処理はステップＳ６３８へ進み、未処理の被確認値が残っている場合、処理はステップＳ６３４へ戻る（ステップＳ６３７）。

[0096] 次に、平常モデル８３０の全てのレコードに対して処理が実行された場合、処理はステップＳ６３９へ進み、未処理のレコードが残っている場合、処理はステップＳ６３１へ戻る（ステップＳ６３８）。

[0097] 異常検出部１３０は、異常情報８４０を出力する（ステップＳ６３９）。

[0098] 例えば、異常検出部１３０は、異常情報８４０を図８に示す出力部７０５を介して出力する。また、異常検出部１３０は、図８に示す通信部７０６を介して、図示しない機器に異常情報８４０を送信してもよい。また、異常検出部１３０は、図８に示す記憶装置７０３を介して、記録媒体７０７に異常情報８４０を記録してもよい。

[0099] 次に、具体的なデータを示して、関係変化情報８１０の受信から、異常情報８４０の出力までを説明する。

[0100] グラフ化部１１０は、例えば、図１１に示すような関係変化情報８１１を受信したことを契機に、図９に示すフローチャートの動作を開始する。図１１は、要素９２０の「Ｅ３」と要素９２０の「Ｅ４」との間に「Ｌ０」の関係が発生したことを示す、関係変化情報８１０の具体的な一例である。

[0101] 図９のステップＳ６０１において、グラフ化部１１０は、受信した図１１に示す関係変化情報８１１に基づいて、状態グラフ８２０を（例えば、図４に示す状態グラフ８２１を図１２に示す状態グラフ８２１に）更新する。

[0102] 次に、図９のステップＳ６０２において、平常モデル生成部１２０は、受信した関係変化情報８１１に基づいて、平常モデル８３０（例えば、図６に示す平常モデル８３１）の内容を更新する。但し、ここでは、平常モデル８３０（例えば、平常モデル８３１）の内容を更新する必要がなかったものとする。

[0103] 次に、図１０のステップＳ６３１において、異常検出部１３０は、平常モデル８３０（例えば、平常モデル８３１）から条件種別が「関係頂点数」であるレコードを抽出する。

[0104] 次に、図１０のステップＳ６３２において、異常検出部１３０は、そのレコードの有効フラグが「有効」であることを判定する。

[0105] 次に、図１０のステップＳ６３４において、異常検出部１３０は、状態グラフ８２０（例えば、図１２に示す状態グラフ８２１）から、被確認値を順次抽出する。

[0106] 次に、図１０のステップＳ６３５において、異常検出部１３０は、その被確認値が、そのレコードに含まれる条件値（上限値２）に合致しているか否かを順次判定する。ここで、異常検出部１３０は、頂点識別子が「Ｅ４」のレコードの辺の相手先となる要素９２０の数（即ち、頂点関係数）が「３」であり、その「３」が、「上限値２」と合致していないと判定する。

[0107] 次に、図１０のステップＳ６３６において、異常検出部１３０は、頂点関係数が上限値を超えていることを示す、異常情報８４０（例えば、図７に示す異常情報８４１）を生成する。

[0108] 異常検出部１３０は、条件種別が「辺数」及び「辺属性」であるレコードについても、処理を実行する。但し、ここでは、条件種別が「辺数」及び「辺属性」であるレコードについては、異常情報８４０（例えば、異常情報８４１）に追加する情報はない。

[0109] 次に、図１０のステップＳ６３９において、異常検出部１３０は、異常情報８４０（例えば、図７に示す異常情報８４１）を出力する。

[0110] 上述した本実施形態における効果は、システムの異常についての検出性を向上することが可能になる点である。例えば、未知の標的型攻撃によるシステムの異常を検出することが可能になる。

[0111] その理由は、以下の構造を含むからである。第１に、グラフ化部１１０が、関係変化情報８１０に基づいて、状態グラフ８２０を生成する。第２に、平常モデル生成部１２０が、関係変化情報８１０に基づいて、平常モデル８３０を生成する。第３に、異常検出部１３０が、状態グラフ８２０と平常モデル８３０とに基づいて、異常情報８４０を生成する。

[0112] ＜＜＜第２の実施形態＞＞＞

次に、本発明の第２の実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内容については説明を省略する。

[0113] 図１３は、本発明の第２の実施形態に係る情報処理装置２００の構成を示すブロック図である。

[0114] 図１３に示すように、本実施形態における情報処理装置２００は、第１の実施形態の情報処理装置１００と比べて、異常検出部１３０に替えて異常検出部２３０を含む点が異なる。

[0115] ＝＝＝異常検出部２３０＝＝＝

異常検出部２３０は、検出した異常に対応する、平常モデル８３０からの状態グラフ８２０のかい離の度合いを示す異常度を算出し、その異常度を含む異常情報８４０を出力する。

[0116] 異常検出部２３０は、上述の点を除き、図１に示す異常検出部１３０と同等である。

[0117] 例えば、図６に示す平常モデル８３１と図１２に示す状態グラフ８２１に基づいて、異常検出部２３０は、その被確認値の「３」が、そのレコードに含まれる条件値（上限値「２」）に対して、５０％かい離していることを示す、異常情報８４０を出力する。

[0118] 図１４は、異常検出部２３０が出力する、異常情報８４０の具体的な例である、異常情報８４２の一例を示す図である。

[0119] 上述した本実施形態における第１の効果は、第１の実施形態の効果に加え、システムの異常についての検出結果をより詳細に、ユーザに提示することを可能にする点である。

[0120] その理由は、異常検出部２３０が、異常度を含む異常情報８４０を出力するからである。

[0121] ＜＜＜第３の実施形態＞＞＞

次に、本発明の第３の実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内容については説明を省略する。

[0122] 図１５は、本発明の第３の実施形態に係る情報処理装置３００の構成を示すブロック図である。

[0123] 図１５に示すように、本実施形態における情報処理装置３００は、第１の実施形態の情報処理装置１００と比べて、異常検出部１３０に替えて異常検

出部３３０を含む点が異なる。

[0124] ＝＝＝異常検出部３３０＝＝＝

異常検出部３３０は、検出した異常に関連する、頂点（要素９２０）及び辺（要素９２０間の関係）を示す情報を含む異常情報８４０を出力する。

[0125] 異常検出部３３０は、上述の点を除き、図１に示す異常検出部１３０と同等である。

[0126] 例えば、図６に示す平常モデル８３１と図１２に示す状態グラフ８２１とに基づいて、異常検出部３３０は、関係頂点数が超過した頂点の識別子「Ｅ３」と、その関係頂点の識別子「Ｅ１」、「Ｅ２」及び「Ｅ３」とを含む異常情報８４０を出力する。

[0127] 図１６は、異常検出部３３０が出力する、異常情報８４０の具体的な例である、異常情報８４３の一例を示す図である。

[0128] 尚、異常検出部３３０は、第２の実施形態の異常検出部２３０の機能を含んでもよい。この場合、異常検出部２３０の機能を含む異常検出部３３０は、検出した異常に関連する、任意の辺及び頂点毎に異常度を算出してよい。

[0129] 上述した本実施形態における第１の効果は、第１の実施形態の効果に加え、システムの異常についての検出結果をより詳細に、ユーザに提示することを可能にする点である。

[0130] その理由は、異常検出部３３０が、検出した異常に関連する、頂点及び辺を示す情報を含む異常情報８４０を出力するからである。例えば、あるコンピュータＡの異常を検出した場合、異常検出部３３０が、異常情報８４０として「コンピュータＡにおいてコンピュータＢとの通信が異常」と出力する。即ち、ユーザは、「コンピュータＡが異常」とだけ出力される場合に比べて、コンピュータＡ内のコンピュータＢとの通信に関わる部分が異常であることを、詳細に知ることができる。

[0131] ＜＜＜第４の実施形態＞＞＞

次に、本発明の第４実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内

容については説明を省略する。

[0132] 図１７は、本発明の第４の実施形態に係る情報処理装置４００の構成を示すブロック図である。

[0133] 図１７に示すように、本実施形態における情報処理装置４００は、第１の実施形態の情報処理装置１００と比べて、異常検出部１３０に替えて異常検出部４３０を含む点が異なる。

[0134] ＝＝＝異常検出部４３０＝＝＝

異常検出部４３０は、状態グラフ８２０と平常モデル８３０とに基づいて生成した、異常を表すための図表を含む異常情報８４０を出力する。異常を表すための図表は、ネットワーク図（詳細は後述）やマトリックス（詳細は後述）、その他の任意の図表である。

[0135] 異常検出部４３０は、以下のようにすることで、異常を表す異常情報８４０を出力する。異常検出部４３０は、例えば、状態グラフ８２０上における異常に対応する部分の、図形の線や文字などの線幅を太くする。また、異常検出部４３０は、状態グラフ８２０上における異常に対応する部分の、図形の線や文字などのサイズを大きくしてよい。また、異常検出部４３０は、状態グラフ８２０上における異常に対応する部分の、図形の線や文字などの表示色を変更してよい。また、異常検出部４３０は、状態グラフ８２０上における異常に対応する部分の、図形の線や文字などの背景色を変更してよい。

[0136] また、異常検出部４３０は、異常情報８４０における図形や文字、マトリクスのセルの配置の仕方により、状態グラフ８２０上における異常に対応する部分を強調するようにしてもよい。具体的には、異常検出部４３０は、状態グラフ８２０上における異常に対応する部分の図形を、ネットワーク図中の所定の領域（例えば、ネットワーク図の左寄り、中央付近など）に集中させてよい。また、異常検出部４３０は、状態グラフ８２０上における異常に対応するセルが、マトリックス中に所定の順序（例えば、最左端の列かつ最上段の行からの順番）で並ぶように、リストを並べ替えてマトリックスを生成してもよい。

[0137] 異常検出部４３０は、上述の例に係わらず、状態グラフ８２０上における異常に対応する部分を任意の手法で強調して、異常を表す異常情報８４０を出力してよい。

[0138] 異常検出部４３０は、更に、平常モデルに基づいた図表（以後、平常モデル図表と呼ぶ）を出力してよい。例えば、異常検出部４３０は、異常を表す図表と平常モデル図表とをユーザが比較して参照できるように、平常モデル図表を出力する。尚、異常検出部４３０は、平常モデル図表を異常情報８４０に含めて或いは単独で出力してよい。

[0139] 異常検出部４３０は、平常モデル図表を、例えば、平常モデル生成部１２０が生成した平常モデル８３０に基づいて生成してよい。

[0140] また、異常検出部４３０は、平常モデル生成部１２０が生成した平常モデル図表を取得してもよい。この場合、平常モデル生成部１２０は、例えば、異常検出部４３０からの要求に基づいて、平常モデル８３０から平常モデル図表を生成し、それを出力する。

[0141] また、平常モデル生成部１２０は、例えば、異常検出部４３０からの要求に基づいて、グラフ化部１１０に平常モデル８３０を渡し、平常モデル図表の生成を依頼してもよい。グラフ化部１１０或いは平常モデル生成部１２０で生成された平常モデル図表は、直接或いは異常検出部４３０を経由して出力されてよい。

[0142] 異常検出部４３０もしくは平常モデル生成部１２０において平常モデル図表を生成する手順は、例えば、以下の手順であってよい。その手順の第１の処理は、全ての頂点の組み合わせ（要素９２０間の関係）を平常モデル８３０と照らし合わせ、平常と判定される頂点の組み合わせを抽出する処理である。その手順の第２の処理は、抽出した頂点の組み合わせを、平常モデル図表に含める処理である。

[0143] 異常検出部４３０は、上述の点を除き、図１に示す異常検出部１３０と同等である。

[0144] 次に、図６に示す平常モデル８３１と図１２に示す状態グラフ８２１とに

基づいて、異常検出部４３０が出力する、異常情報８４０の例を示す。

[0145] 図１８は、異常検出部４３０が出力する、異常情報８４０の具体的な例である、ネットワーク図で表す異常情報８４４の一例を示す図である。

[0146] 図１８において、円形は頂点を示し、円形の中の文字列は頂点識別子を示す。また、円形を結ぶ線分は辺を示す。例えば、２重線の円形及び２重線の線分は、異常と判定した頂点（要素９２０）や辺（要素９２０間の関係）を強調して示す。

[0147] ネットワーク図は、図１８の例に係わらず、任意の形式のネットワーク図であってよいし、異常を示す表示も任意の形式であってよい。

[0148] 図１９は、異常検出部４３０が出力する、異常情報８４０の具体的な例である、マトリックスで表す異常情報８４５の一例を示す図である。

[0149] 異常情報８４５は、縦軸の頂点識別子（左端の頂点識別子）のリストで特定される頂点を辺のｆｒｏｍ（始端）側の頂点とし、横軸の頂点識別子（最上行の頂点識別子）のリストで特定される頂点を辺のｔｏ（終端）側の頂点とする、マトリックスである。このマトリックスのセル内の文字列（例えば、「Ｌ０」）は、ｆｒｏｍ側の頂点からｔｏ側の頂点への辺の有無（ＮＬ：辺なし、ＮＬ以外：辺あり）及び属性（Ｌ０、Ｌ１及びＬ２）を示す。図１９において、異常に関連する頂点及び辺は、斜体文字で示される。

[0150] マトリックスは、図１９の例に係わらず、任意の形式のマトリックスであってよいし、異常を示す表示も任意の形式であってよい。

[0151] 異常検出部４３０は、上述の例に係わらず、任意の種類の図表に任意の手法により異常を表す任意の異常図表、及び平常モデル８３０に基づいて生成される任意の種類の平常図表を、任意に組み合わせて異常情報８４０として或いは単独で出力してよい。例えば、異常検出部４３０は、その異常図表に、平常モデル図表を重畳して出力してよい。

[0152] 尚、異常検出部４３０は、第２の実施形態の異常検出部２３０及び第３の実施形態の異常検出部３３０の機能を含んでもよい。

[0153] ＜＜＜第４の実施形態の変形例＞＞＞

異常検出部４３０は、状態グラフ８２０、平常モデル８３０及び異常情報８４０のそれぞれの時間的変化を、単独で或いは任意に関連付けて表す表示情報を出力してよい。尚、時間的変化とは、即ち時間の経過に伴う変化である。

[0154] その表示情報は、例えば、状態グラフ８２０、平常モデル８３０及び異常情報８４０の任意のものの状態の変化を動画で示す情報であってよい。また、その表示情報は、状態グラフ８２０、平常モデル８３０及び異常情報８４０の任意のものの複数の時点の状態を、並べて示す情報であってもよい。

[0155] その表示情報は、現在時刻に対応してリアルタイムに更新される情報であってよい。

[0156] 上述した本実施形態における第１の効果は、第１の実施形態の効果に加え、システムの異常についての検出結果をより人が理解しやすい形式で、ユーザに提示することを可能にする点である。

[0157] その理由は、異常検出部４３０が、異常を表すための図表を含む異常情報８４０を出力するからである。加えて、異常検出部４３０が、平常モデル図表を出力するからである。更に、異常検出部４３０が、状態グラフ８２０、平常モデル８３０及び異常情報８４０のそれぞれの時間的変化を表す表示情報を出力するからである。

[0158] 上述した本実施形態における第２の効果は、システムに実際に異常が発生したとき以外においても、平常と見なされる通信が発生する頂点間と異常な通信が発生する頂点間とを識別することが可能になる点である。更に、この識別が可能になることにより、平常な通信が発生すると見なされる頂点間のみ通信を許可するなどすることで、異常な通信の発生を事前に防ぐことが可能となる。

[0159] その理由は、以下の構成を含むからである。第１に、異常検出部４３０もしくは平常モデル生成部１２０が、全ての頂点の組み合わせを平常モデル８３０と照らし合わせて平常と判定される頂点の組み合わせを抽出し、抽出した頂点のその組み合わせを平常モデル図表に含める。第２に、異常検出部４

３０が、異常を表すための図表に、その平常モデル図表を重畳して出力する。

[0160] ＜＜＜第５の実施形態＞＞＞

次に、本発明の第５実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内容については説明を省略する。

[0161] 図２０は、本発明の第５の実施形態に係る情報処理装置５００の構成を示すブロック図である。

[0162] 図２０に示すように、本実施形態における情報処理装置５００は、第１の実施形態の情報処理装置１００と比べて、グラフ化部１１０に替えてグラフ化部５１０を、異常検出部１３０に替えて異常検出部５３０を含み、履歴蓄積部５４０を更に含む点が異なる。

[0163] ＝＝＝グラフ化部５１０＝＝＝

グラフ化部５１０は、所定のタイミングで、その時点の状態グラフ８２０を復元可能な情報を、例えばその時点の時刻を関連付けて、履歴蓄積部５４０に記録する。その所定のタイミングは、例えば所定の時刻である。また、その所定のタイミングは、関係変化情報８１０の処理数が、所定の閾値に達するタイミングであってよい。その所定のタイミングは、上述の例に係わらず、任意のタイミングであってよい。その時点の状態グラフ８２０を復元可能な情報は、例えば、以前のいずれかの時点（例えば、１つ前の時点）の状態グラフ８２０からの差分である。また、その時点の状態グラフ８２０を復元可能な情報は、その時点の状態グラフ８２０そのものであってもよい。

[0164] 更に、グラフ化部５１０は、最新の状態グラフ８２０を暫定状態グラフとして履歴蓄積部５４０に記録し、関係変化情報８１０を取得するたびに、その暫定状態グラフと関連付けられた時刻とを更新してもよい。この場合、グラフ化部５１０は、その所定のタイミングで、その暫定状態グラフの更新を停止し、その暫定状態グラフを確定された状態グラフ８２０としてよい。

[0165] グラフ化部５１０は、上述の点を除き、図１に示すグラフ化部１１０と同

等である。

[0166] ＝＝＝履歴蓄積部５４０＝＝＝

履歴蓄積部５４０は、状態グラフ８２０を記憶する。履歴蓄積部５４０は、更に、上述の暫定状態グラフを記憶してよい。

[0167] ＝＝＝異常検出部５３０＝＝＝

異常検出部５３０は、履歴蓄積部５４０に記憶されている状態グラフ８２０と平常モデル８３０とに基づいて、監視対象システム９００に係る異常を検出する。異常検出部５３０は、履歴蓄積部５４０に記憶されている暫定状態グラフに更に基づいて、監視対象システム９００に係る異常を検出してよい。異常検出部５３０は、上述の点を除き、図１に示す異常検出部１３０と同等である。

[0168] 尚、異常検出部５３０は、第１の実施形態の異常検出部１３０、第２の実施形態の異常検出部２３０、第３の実施形態の異常検出部３３０及び第４の実施形態の異常検出部４３０の、任意の機能を含んでよい。

[0169] 例えば、異常検出部５３０が異常検出部４３０の機能を含む場合、第４の実施形態の変形例における表示情報は、要求された時間範囲に対応する情報であってもよい。

[0170] 上述した本実施形態における効果は、第１の実施形態の効果に加え、現在の平常モデル８３０に対する、過去の状態グラフ８２０における異常情報８４０を、ユーザに提供することを可能にする点である。

[0171] その理由は、以下の構成を備えるからである。第１に、グラフ化部５１０が所定のタイミングで状態グラフ８２０を履歴蓄積部５４０に記録し、履歴蓄積部５４０がその状態グラフ８２０を記憶する。第２に、異常検出部５３０が履歴蓄積部５４０に記憶されている状態グラフ８２０と平常モデル８３０とに基づいて、監視対象システム９００に係る異常を検出する。

[0172] 以上、各実施形態を参照して本発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本発明のスコープ内で当業者が理解し得るさまざまな変更をすることができる。

[0173] この出願は、２０１４年３月２０日に出願された日本出願特願２０１４－０５８４９７、及び２０１４年６月６日に出願されたＰＣＴ国際出願ＰＣＴ／ＪＰ２０１４／００３０１４を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0174]

１００	情報処理装置
１１０	グラフ化部
１２０	平常モデル生成部
１３０	異常検出部
２００	情報処理装置
２３０	異常検出部
３００	情報処理装置
３３０	異常検出部
４００	情報処理装置
４３０	異常検出部
５００	情報処理装置
５１０	グラフ化部
５３０	異常検出部
５４０	履歴蓄積部
７００	コンピュータ
７０１	ＣＰＵ
７０２	記憶部
７０３	記憶装置
７０４	入力部
７０５	出力部
７０６	通信部
７０７	記録媒体
８１０	関係変化情報

８１１　関係変化情報

８２０　状態グラフ

８２１　状態グラフ

８３０　平常モデル

８３１　平常モデル

８４０　異常情報

８４１　異常情報

８４２　異常情報

８４３　異常情報

８４４　異常情報

８４５　異常情報

９００　監視対象システム

９２０　要素

９３０　関係変化監視手段

請求の範囲

[請求項1] システムに含まれる複数の要素の、関係の変化を示す関係変化情報を時系列的に取得し、前記関係変化情報に基づいて、前記要素を頂点とし前記要素間の関係を辺とする状態グラフを生成するグラフ化手段と、

前記関係変化情報に基づいて、前記状態グラフが、前記システムの平常時に満たすべき条件の集合である平常モデルを生成する平常モデル生成手段と、

前記状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出し、検出した前記異常を示す第１の異常情報を出力する異常検出手段と、を含む

情報処理装置。

[請求項2] 前記システムは、ネットワークで接続された複数のホストを含み、

前記ホスト上で動作するプロセスは、前記頂点である

ことを特徴とする請求項１記載の情報処理装置。

[請求項3] 前記異常検出手段は、前記検出した異常に対応する、前記平常モデルからの前記状態グラフのかい離の度合いを示す異常度を算出し、算出した前記異常度を少なくとも含む前記第１の異常情報を出力する

請求項１または２記載の情報処理装置。

[請求項4] 前記異常検出手段は、前記検出した異常に対応する、前記要素の識別情報及び前記要素間の関係の情報を少なくとも含む前記第１の異常情報を出力する

請求項１乃至３のいずれか1項に記載の情報処理装置。

[請求項5] 前記異常検出手段は、前記状態グラフと前記第１の異常情報とに基づいて生成した異常を表すための図表を含む第２の異常情報を出力する

請求項１乃至４のいずれか1項に記載の情報処理装置。

[請求項6] 前記異常検出手段は、全ての前記要素間の関係のうち、前記平常モ

デルと照らし合わせて平常と見なされる前記要素間の関係を抽出し、前記異常を表すための図表に抽出した前記要素間の関係を重畳して出力する

請求項５記載の情報処理装置。

[請求項7] 前記異常検出手段は、前記状態グラフと前記平常モデルと前記第２の異常情報のそれぞれの時間的変化を、単独で或いは任意に関連付けて表す表示情報を出力する

請求項５または６記載の情報処理装置。

[請求項8] 状態グラフを記憶する履歴蓄積手段を更に含み、

前記グラフ化手段は、前記状態グラフを前記履歴蓄積手段に記録し、

前記異常検出手段は、更に、前記履歴蓄積手段に記録された前記履歴状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出する

請求項１乃至７のいずれか１項に記載の情報処理装置。

[請求項9] 前記関係変化情報は、前記要素間の関係の発生、消滅及び変化、並びに要素の発生及び消滅の内、少なくともいずれかひとつを示す情報である

請求項１乃至８のいずれか１項に記載の情報処理装置。

[請求項10] 前記平常モデルにおける前記条件は、前記頂点の属性、前記頂点に隣接する頂点の数、前記頂点に隣接する頂点の属性、前記辺の属性、前記頂点間の経路の有無、前記経路の本数、前記経路の距離、前記経路中の前記頂点の属性、前記経路中の前記辺の属性、及び状態グラフの特性の内、少なくともいずれかひとつの範囲を含む

請求項１乃至９のいずれか１項に記載の情報処理装置。

[請求項11] 請求項１乃至１０のいずれか１項に記載の情報処理装置と、

前記システムを監視し、関係変化情報を送信する関係変化監視手段と、を含む、

情報処理システム。

[請求項12] システムに含まれる複数の要素の、関係の変化を示す関係変化情報を時系列的に取得し、前記関係変化情報に基づいて、前記要素を頂点とし前記要素間の関係を辺とする状態グラフを生成し、

前記関係変化情報に基づいて、前記状態グラフが、前記システムの平常時に満たすべき条件の集合である平常モデルを生成し、

前記状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出し、

検出した前記異常を示す異常情報を出力する

異常検知方法。

[請求項13] システムに含まれる複数の要素の、関係の変化を示す関係変化情報を時系列的に取得し、前記関係変化情報に基づいて、前記要素を頂点とし前記要素間の関係を辺とする状態グラフを生成し、

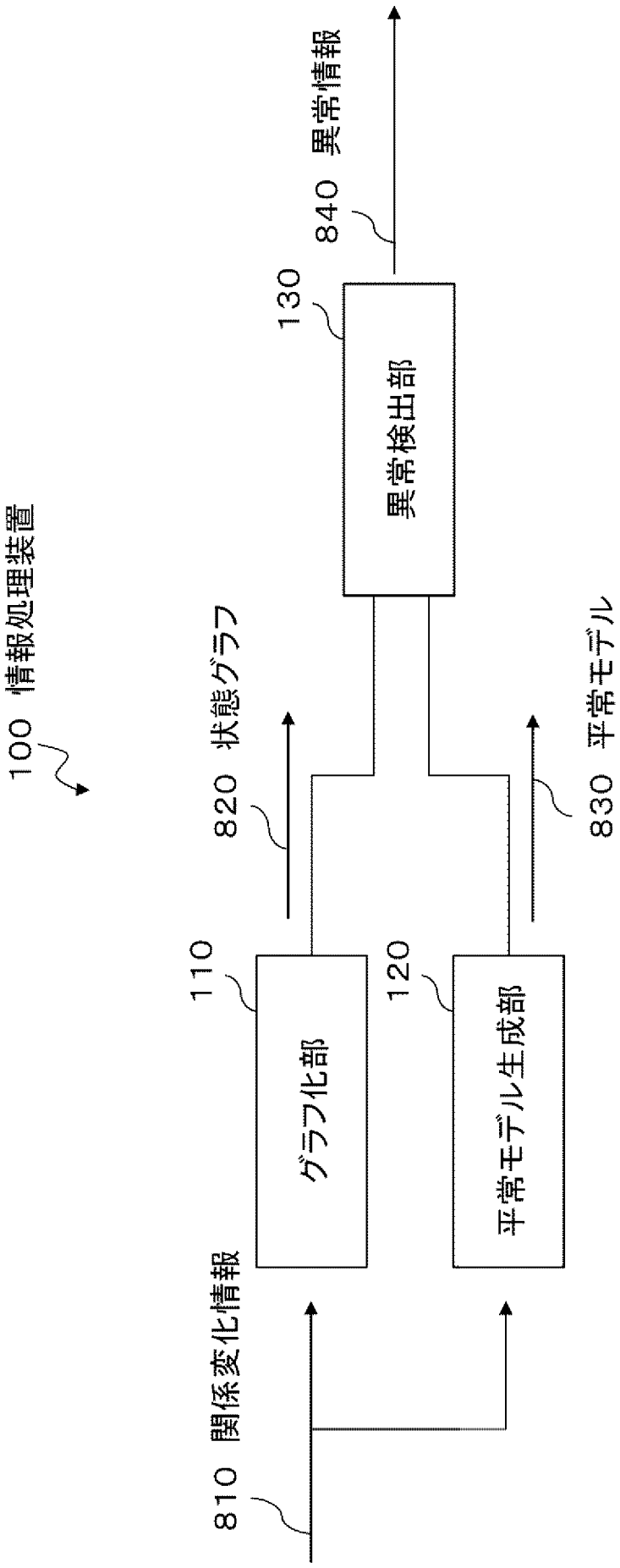
前記関係変化情報に基づいて、前記状態グラフが、前記システムの平常時に満たすべき条件の集合である平常モデルを生成し、

前記状態グラフと前記平常モデルとに基づいて、前記システムに係る異常を検出し、

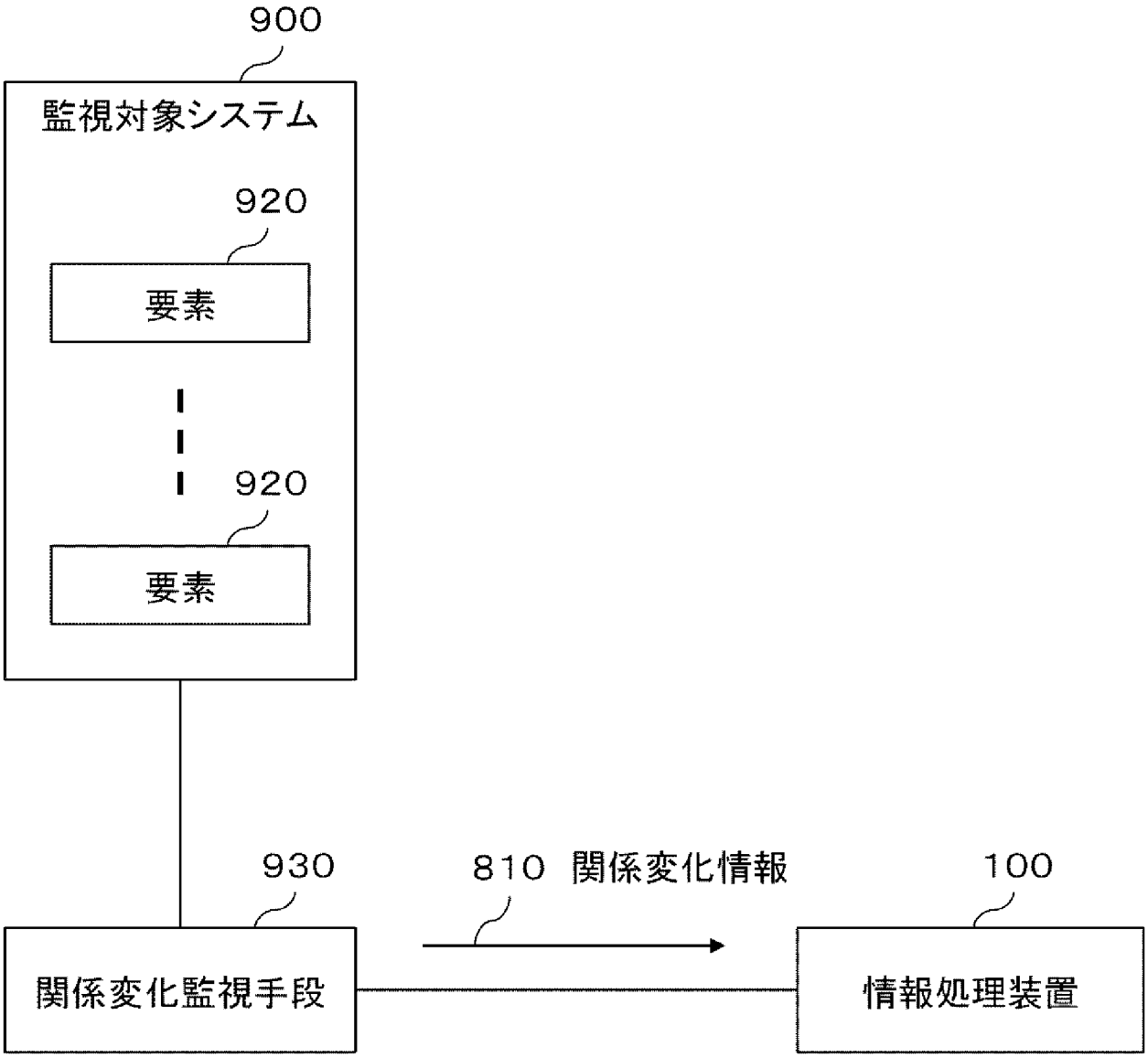
検出した前記異常を示す異常情報を出力する、処理をコンピュータに実行させるプログラムを記録した

コンピュータ読み取り可能な非一時的記録媒体。

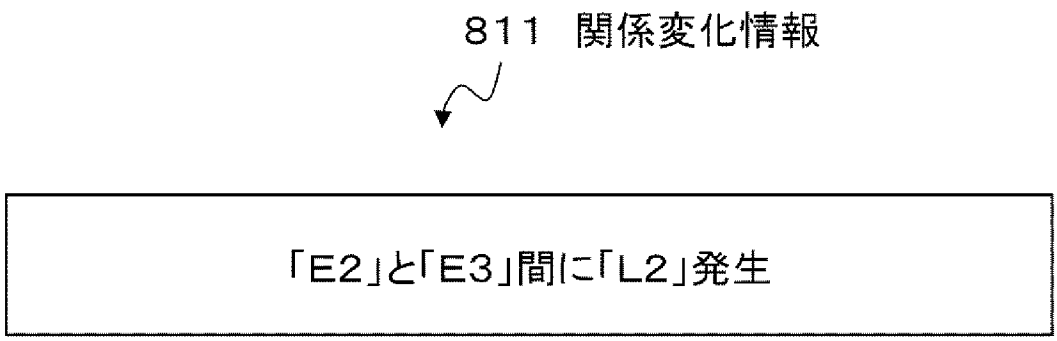
[図1]


100 情報処理装置
810 関係変化情報
110
グラフ化部
820 状態グラフ
120
平常モデル生成部
830 平常モデル
130
異常検出部
840 異常情報

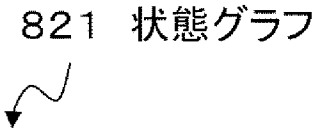
[図2]


900
監視対象システム
920
要素
920
要素
930
関係変化監視手段
810 関係変化情報
100
情報処理装置

[図3]

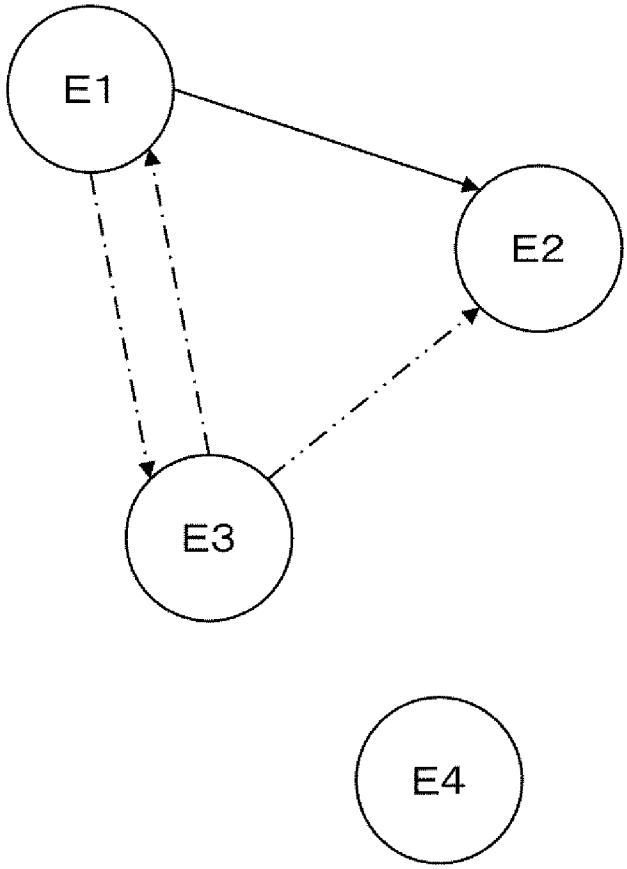

811 関係変化情報
「E2」と「E3」間に「L2」発生

[図4]



頂点識別子	辺
E1	E2;L0、 E3;L1;L1
E2	E1;L0、 E3;L2
E3	E1;L1;L1、 E2;L2
E4	

[図5]

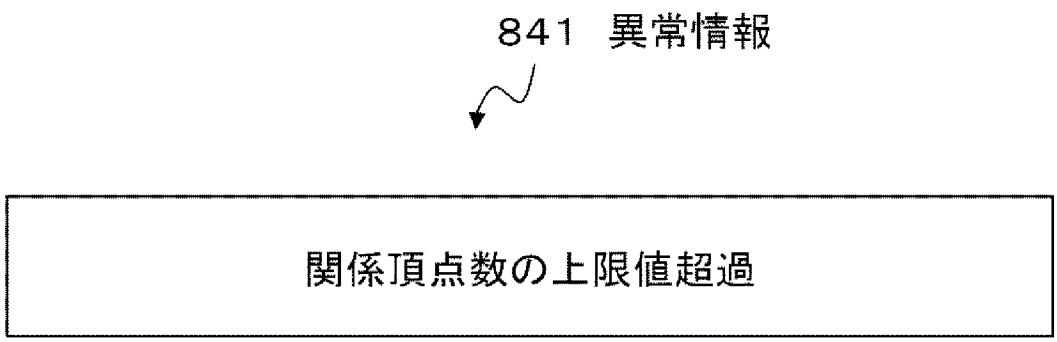


[図6]

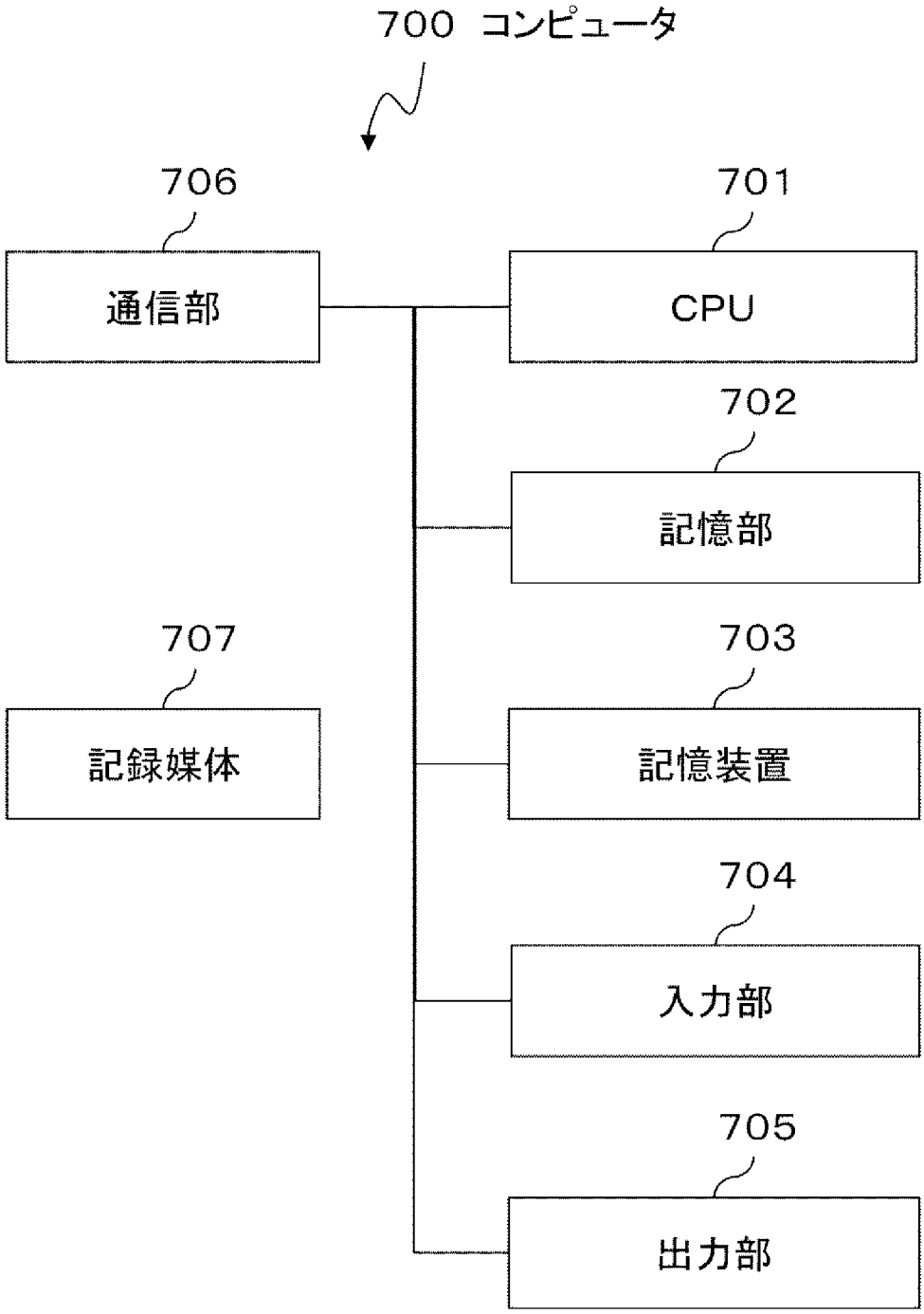
831 平常モデル

条件種別	条件値	有効フラグ
関係頂点数	上限値2	有効
次数	上限値6	有効
辺属性		無効

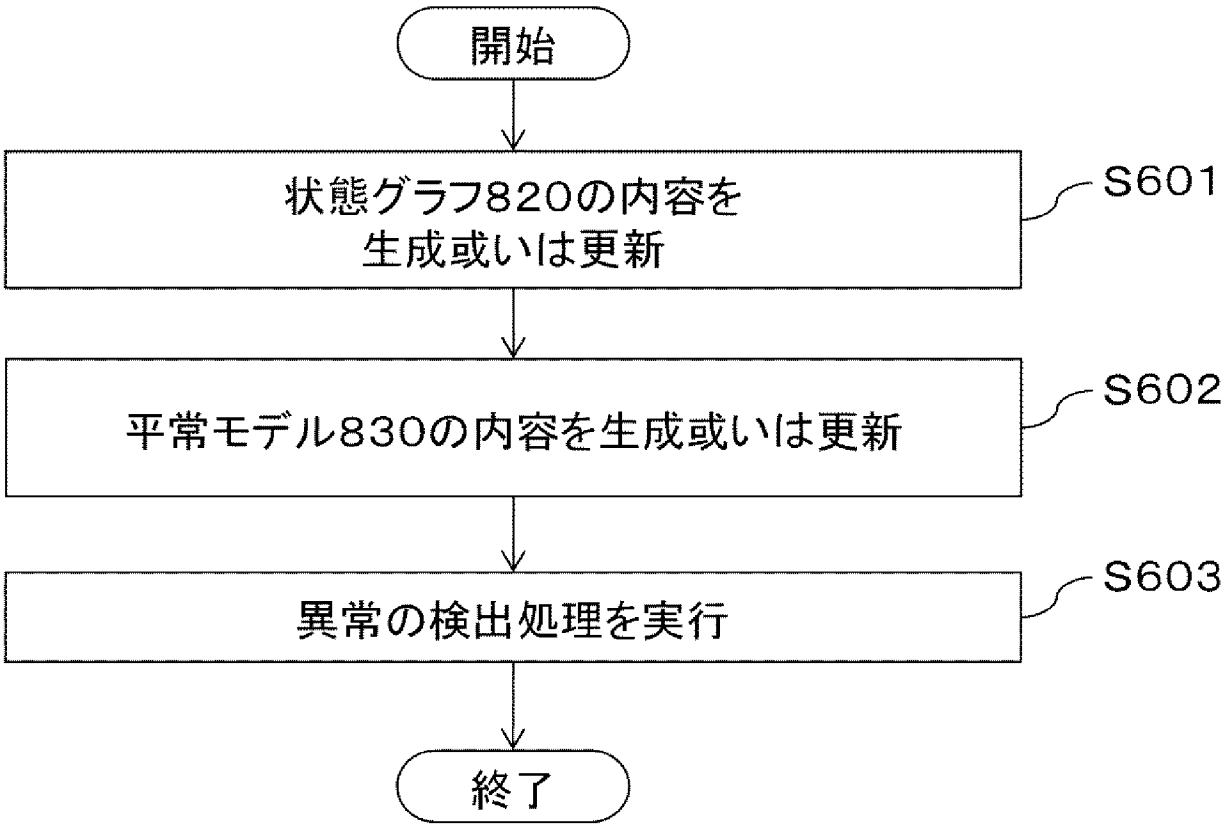
[図7]



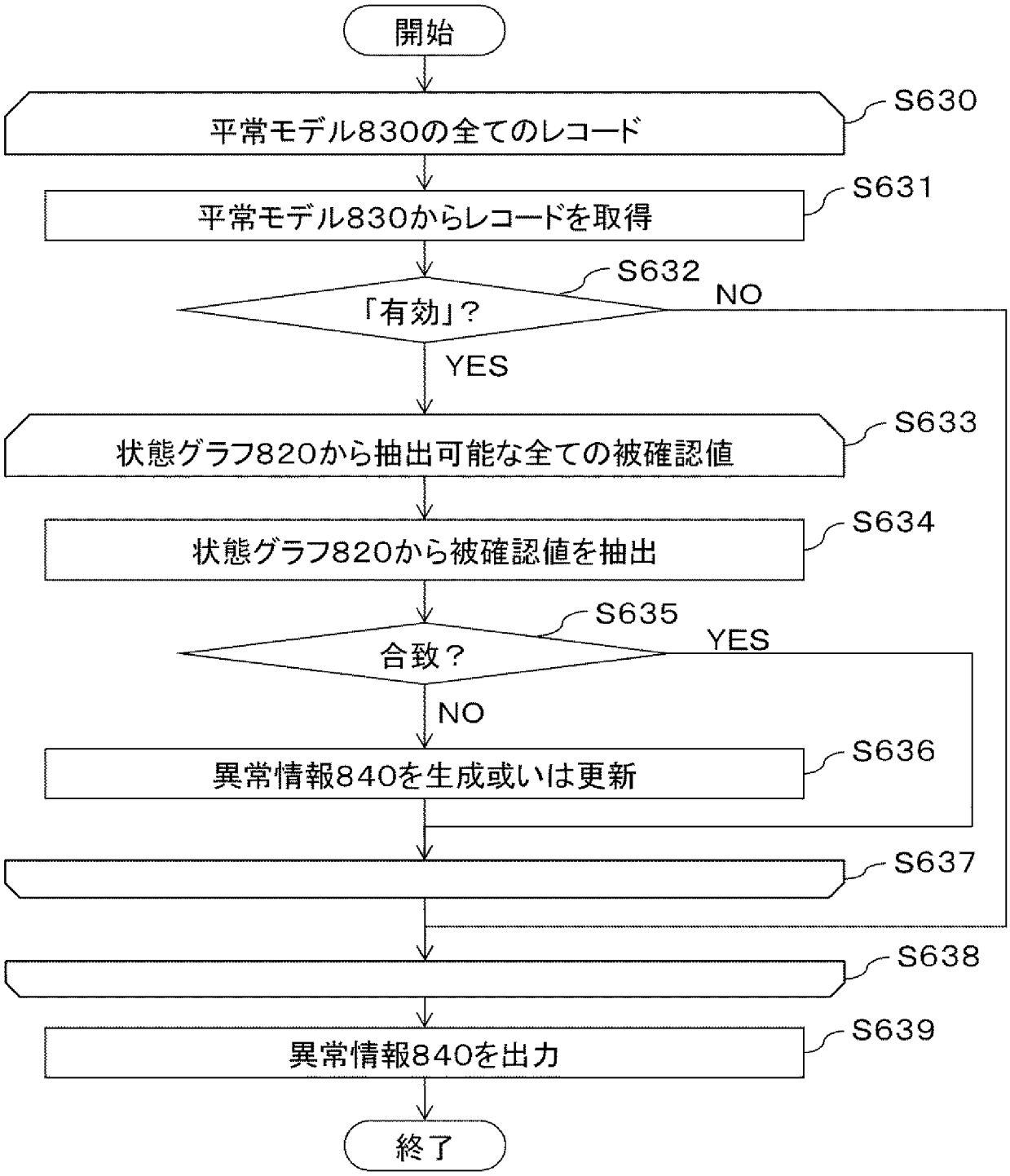
[図8]


700 コンピュータ
706
通信部
701
CPU
702
記憶部
707
記録媒体
703
記憶装置
704
入力部
705
出力部

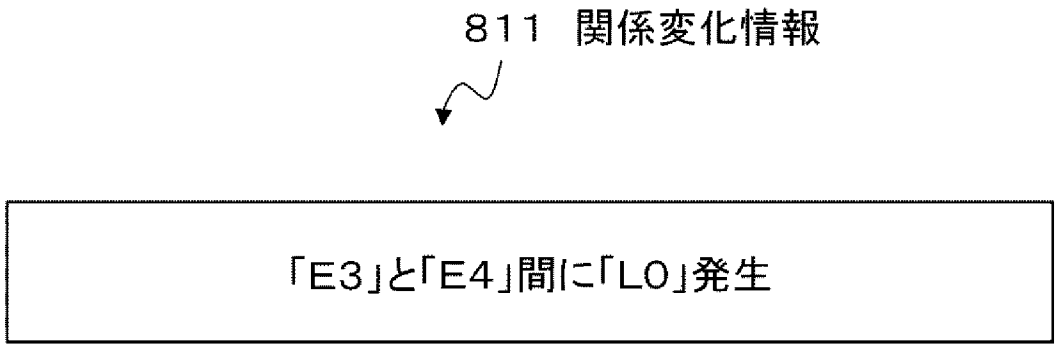
[図9]


開始
状態グラフ820の内容を
生成或いは更新
S601
平常モデル830の内容を生成或いは更新
S602
異常の検出処理を実行
S603
終了

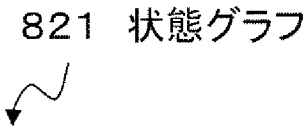
[図10]


開始
平常モデル830の全てのレコード
S630
平常モデル830からレコードを取得
S631
「有効」？
S632
NO
YES
状態グラフ820から抽出可能な全ての被確認値
S633
状態グラフ820から被確認値を抽出
S634
合致？
S635
YES
NO
異常情報840を生成或いは更新
S636
S637
S638
異常情報840を出力
S639
終了

[図11]

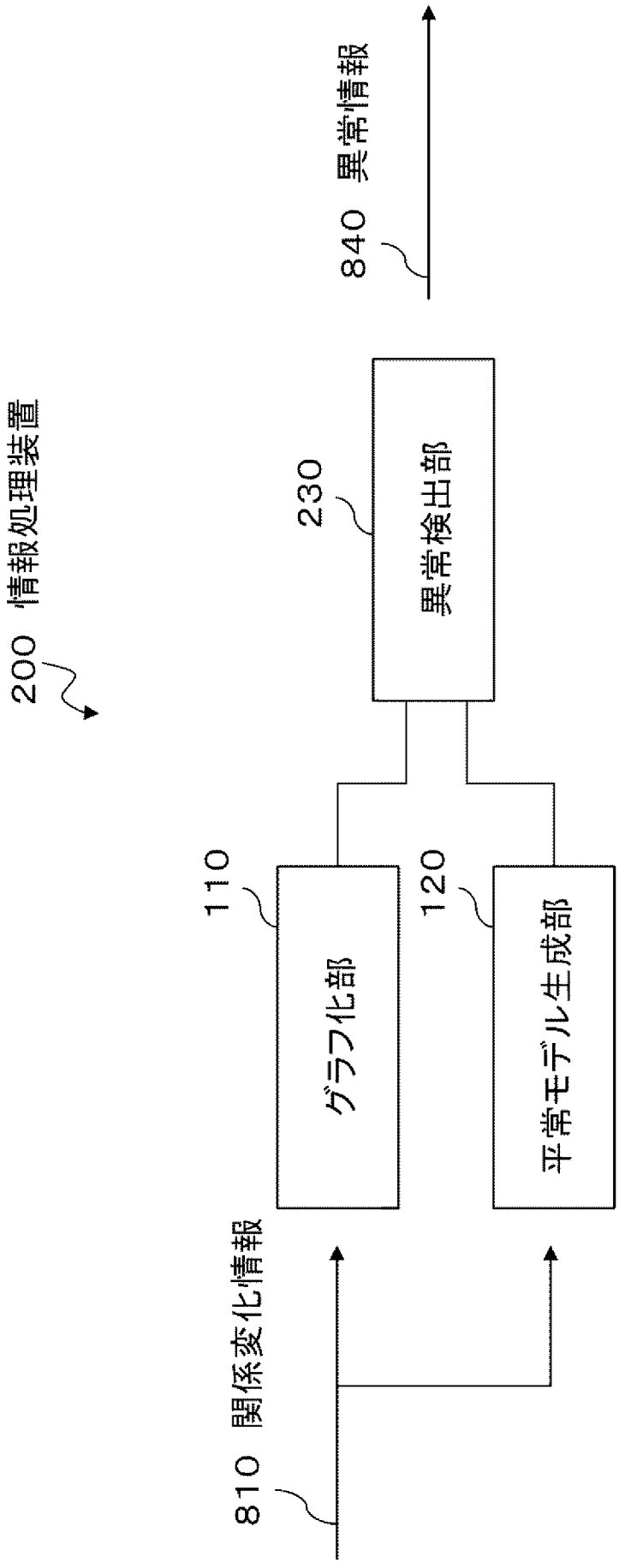

811 関係変化情報
「E3」と「E4」間に「LO」発生

[図12]

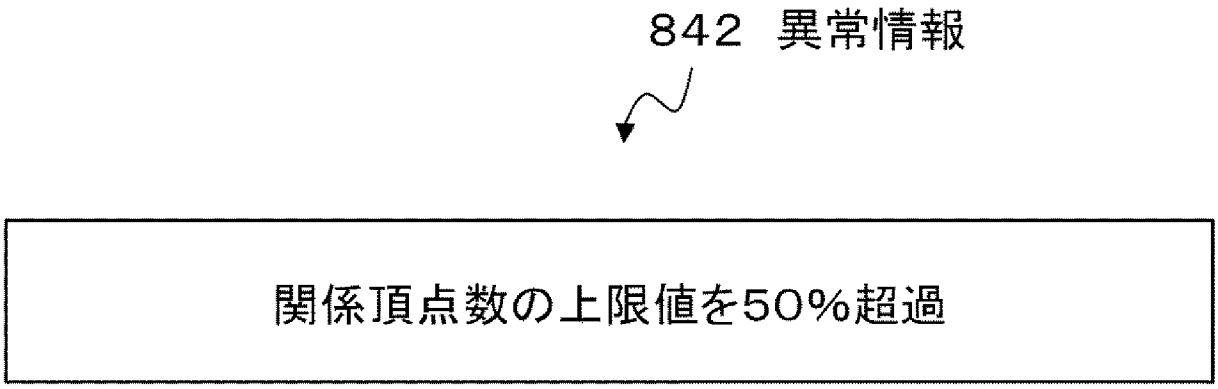


頂点識別子	辺
E1	E2;L0, E3;L1;L1
E2	E1;L0, E3;L2
E3	E1;L1;L1、 E2;L2、 E4;L0
E4	E3;L0

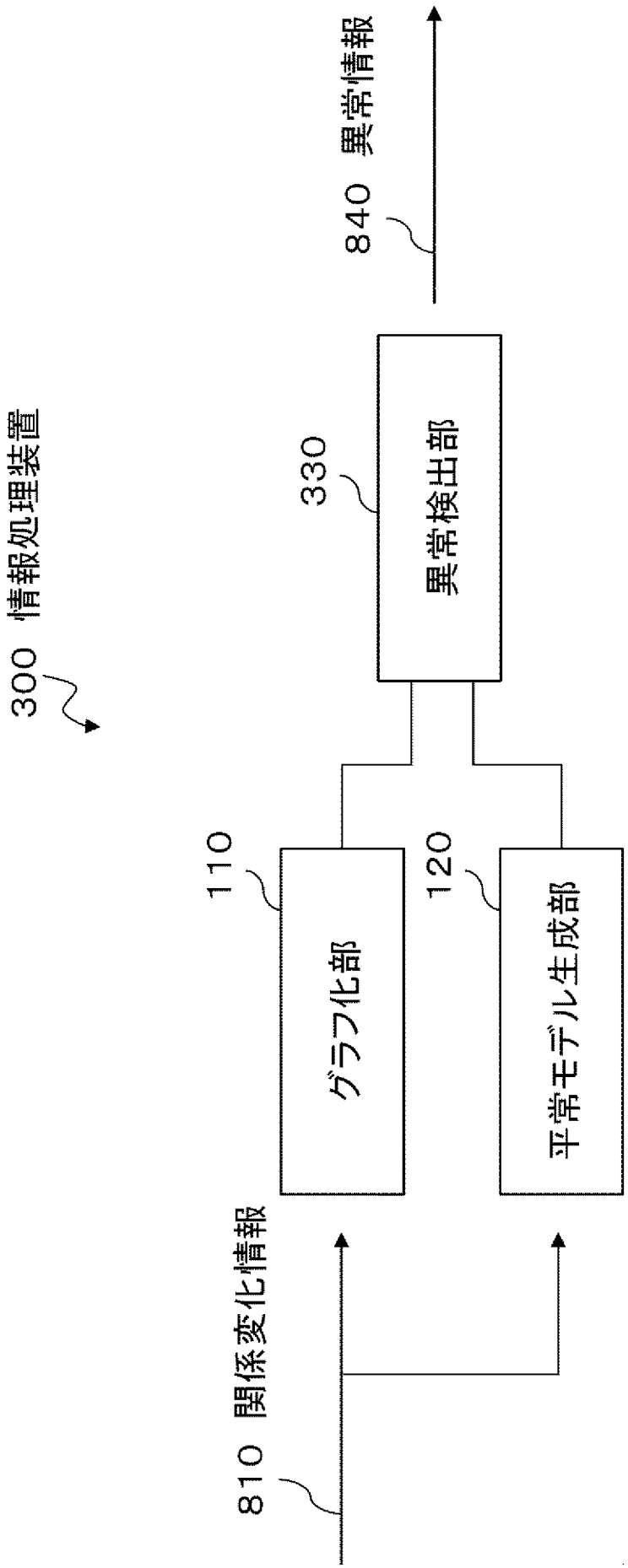
[図13]


200 情報処理装置
810 関係変化情報
110 グラフ化部
120 平常モデル生成部
230 異常検出部
840 異常情報

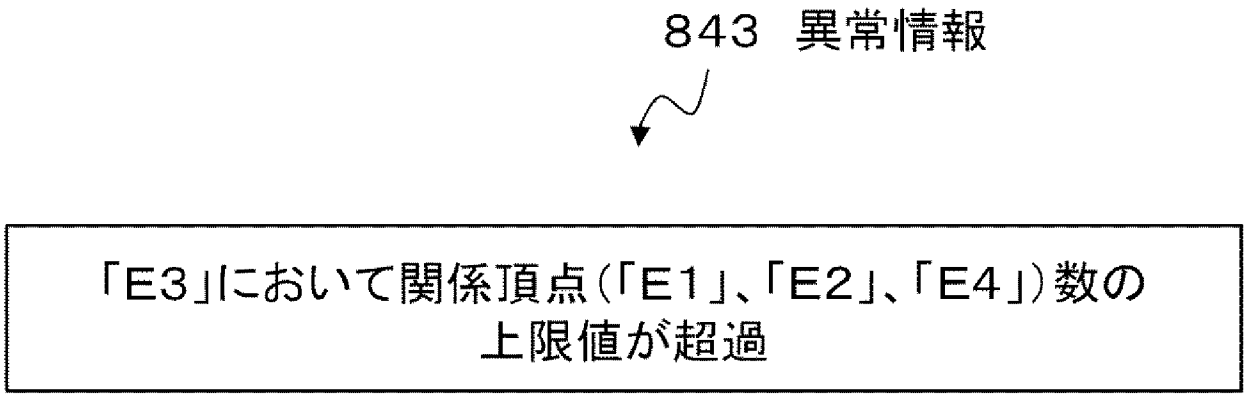
[図14]



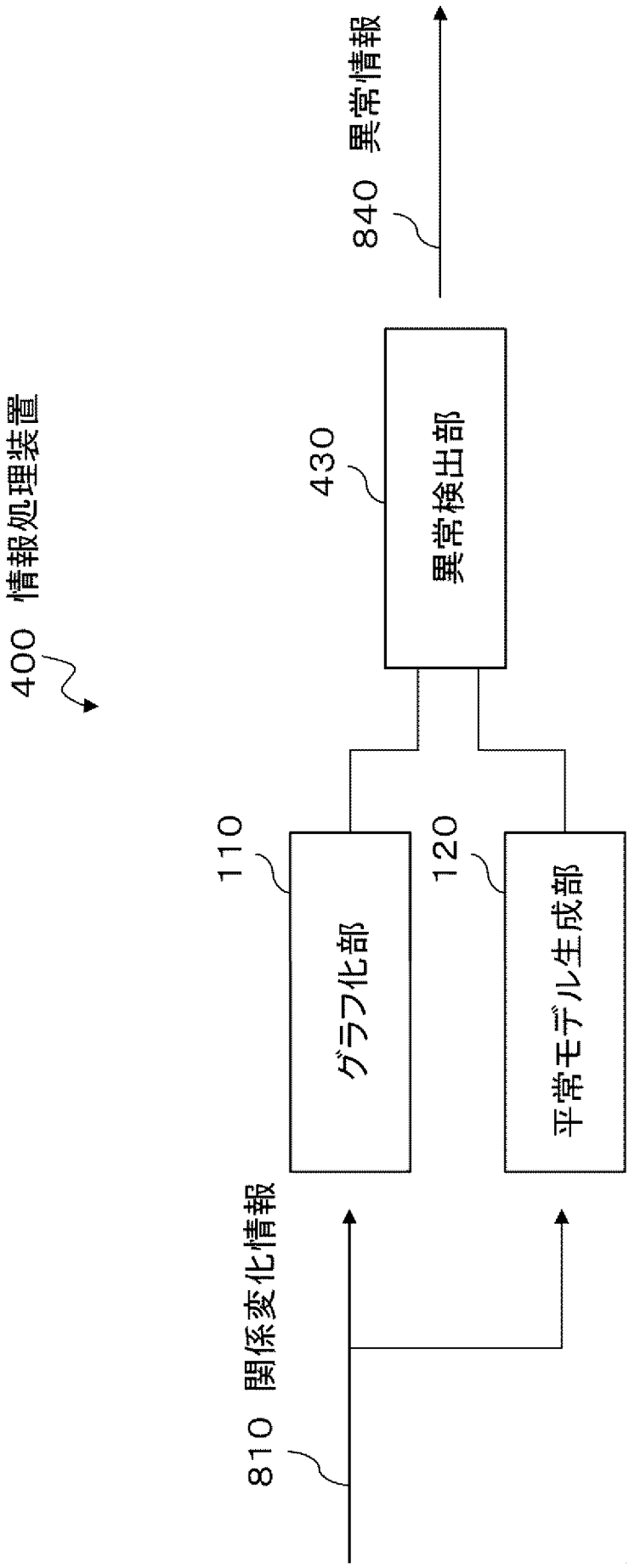
[図15]


300 情報処理装置
330 異常検出部
840 異常情報
110 グラフ化部
120 平常モデル生成部
810 関係変化情報

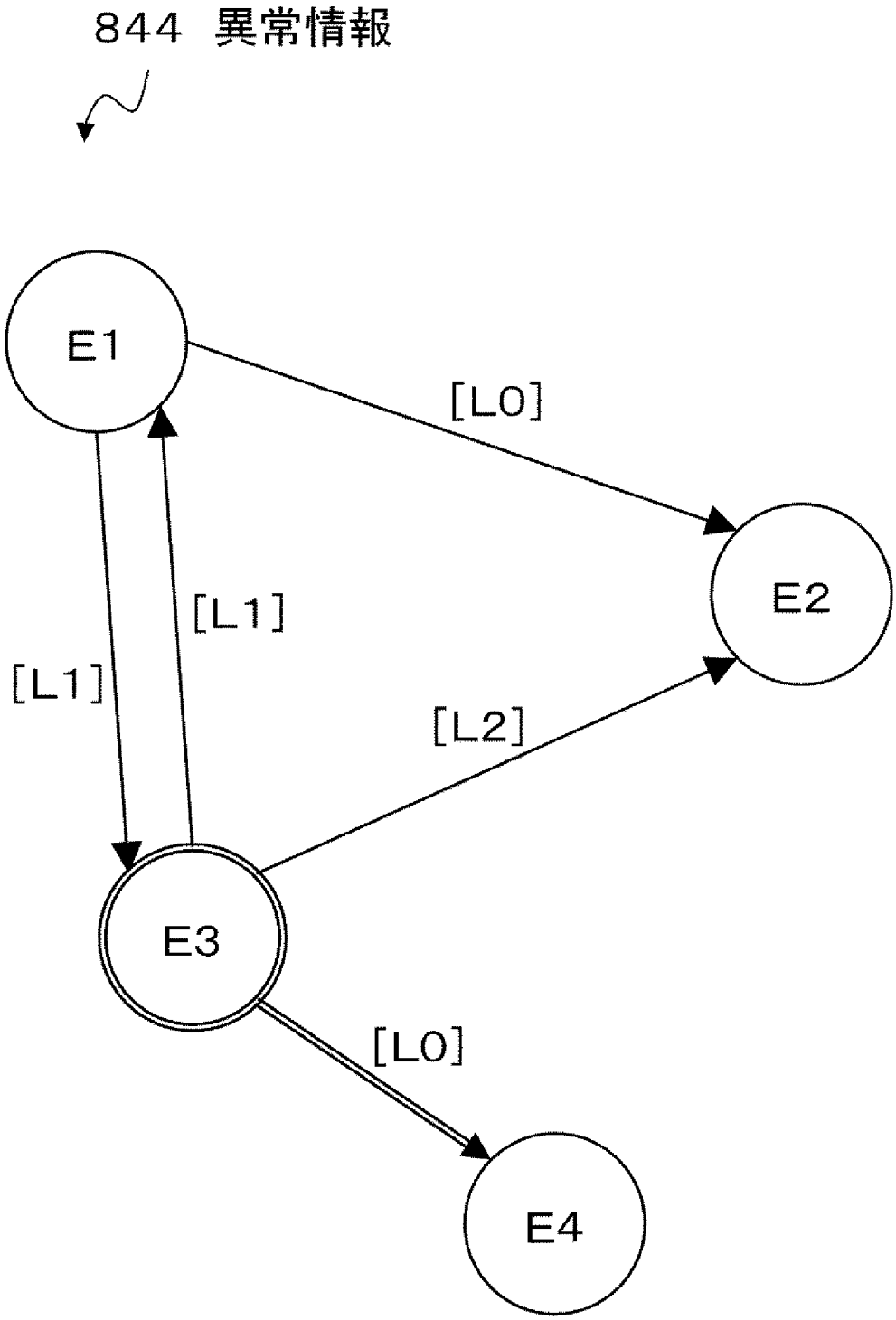
[図16]



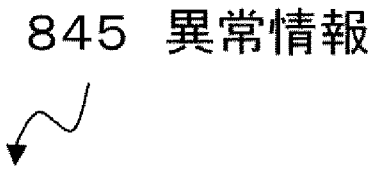
[図17]


400 情報処理装置
430 異常検出部
840 異常情報
110 グラフ化部
120 平常モデル生成部
810 関係変化情報

[図18]

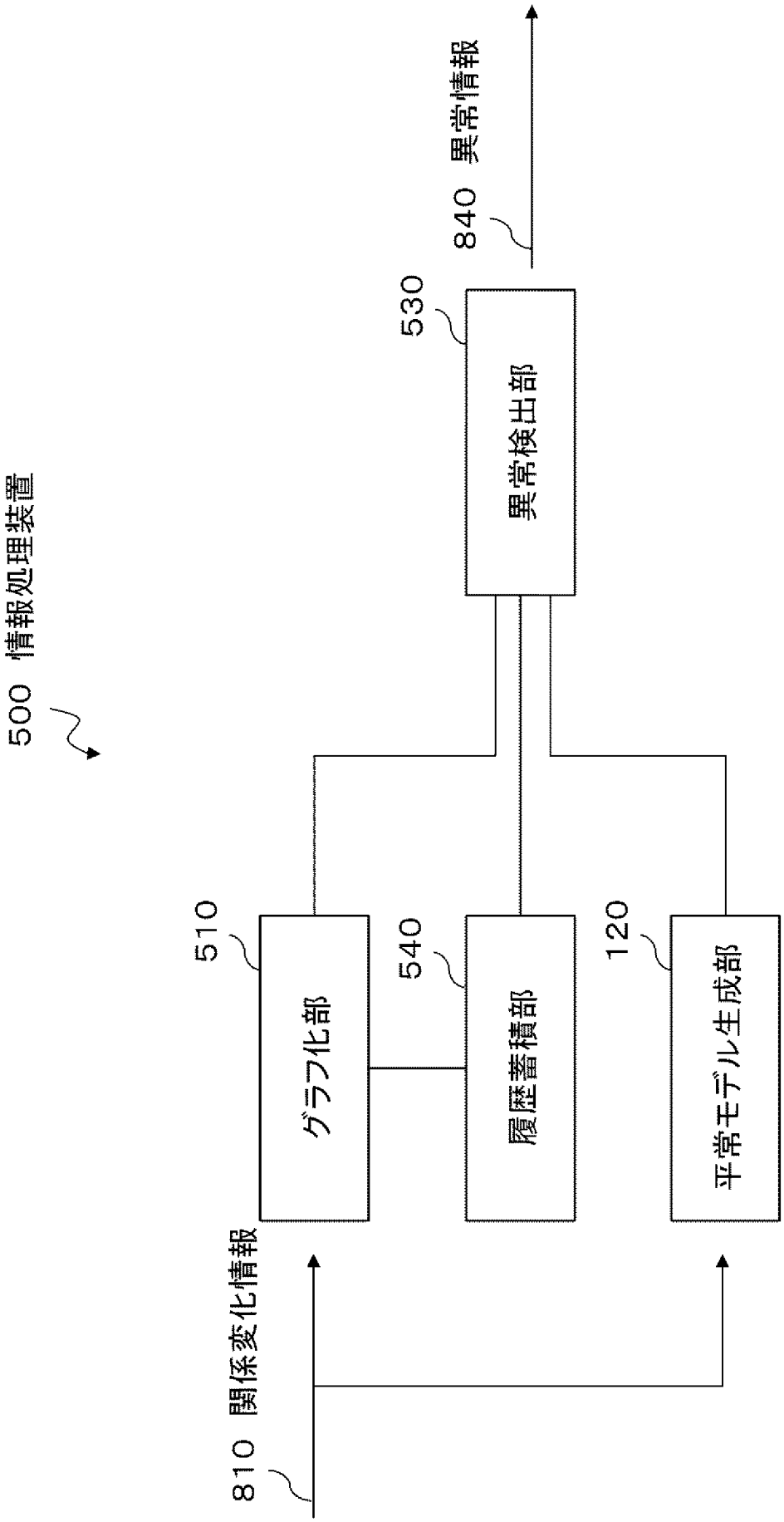


[図19]



	E1	E2	E3	E4
E1	NL	L0	L1	NL
E2	NL	NL	NL	NL
E3	L1	L2	NL	*L0*
E4	NL	NL	NL	NL

[図20]


500 情報処理装置
530
異常検出部
840 異常情報
510
グラフ化部
540
履歴蓄積部
120
平常モデル生成部
810 関係変化情報

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/001500

A. CLASSIFICATION OF SUBJECT MATTER
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)
G06F11/34

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	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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.
Y	JP 2010-128673 A (NEC Corp.), 10 June 2010 (10.06.2010), paragraphs [0020] to [0037], [0056] to [0062] (Family: none)	1-13
Y	JP 2012-221502 A (Computer Associates Think Inc.), 12 November 2012 (12.11.2012), paragraphs [0045] to [0050], [0064] to [0066], [0093] to [0102], [0121] to [0123], [0135] to [0137] & US 2012/0260236 A1 & EP 2508997 A1	1-13

☒ 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
01 June 2015 (01.06.15)	16 June 2015 (16.06.15)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/001500

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Osamu AKASHI et al., "IM-VIS: Inter-domain network-status visualization system based on information integration", IPSJ SIG Notes, vol.2009, no.6, Information Processing Society of Japan, 21 January 2009 (21.01.2009), pages 75 to 82, ISSN:0919-6072	6-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／００１５００

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　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.　G06F11/34

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	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５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
Y	JP 2010-128673 A（日本電気株式会社）2010.06.10, 段落[0020]-[0037],[0056]-[0062]（ファミリーなし）	1-13
Y	JP 2012-221502 A（コンピュータ　アソシエイツ　シンク　インク）2012.11.12, 段落[0045]-[0050],[0064]-[0066],[0093]-[0102],[0121]-[0123],[0135]-[0137] & US 2012/0260236 A1 & EP 2508997 A1	1-13

☑　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 ０１．０６．２０１５	国際調査報告の発送日 １６．０６．２０１５
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	関連する請求項の番号
Ｙ	明石修，他２名，ＩＭ－ＶＩＳ： 情報統合機能を用いたネットワーク状態可視化システムの提案, 情報処理学会研究報告, 第2009巻, 第6号, 社団法人情報処理学会, 2009.01.21, pp.75-82, ISSN:0919-6072	6-11