(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 2015/140843 A1

(51) 国際特許分類:
G06F 11/30 (2006.01)

(21) 国際出願番号: PCT/JP2014/003227

(22) 国際出願日: 2014 年 6 月 17 日(17.06.2014)

(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 2014-058558 2014 年 3 月 20 日(20.03.2014) 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). 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). 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).

(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, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, INFLUENCE-PROCESS EXTRACTION METHOD, AND RECORDING MEDIUM

(54) 発明の名称 : 情報処理装置、影響過程抽出方法および記録媒体

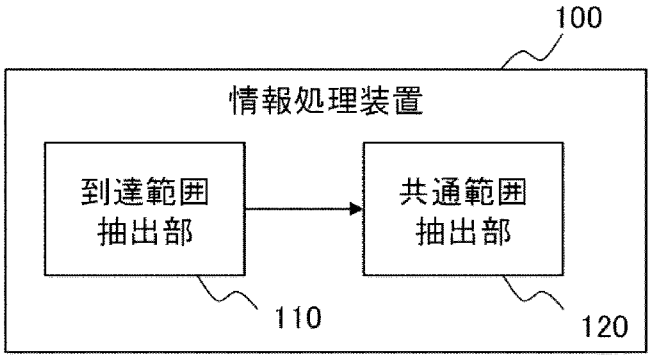


FIG. 1
100 Information processing device
110 Reach-extent extraction unit
120 Shared-extent extraction unit

(57) **Abstract**: This invention provides an information processing device that can more appropriately extract anomaly influence processes even if anomalies are found at multiple points. Said information processing device comprises a reach-extent extraction means and a shared-extent extraction means. Using both a relationship graph representing the relationships between a plurality of elements in a system and location information that indicates, on said relationship graph, a plurality of locations in the system where anomalies have been detected, the reach-extent extraction means starts at each of said locations and extracts a reach extent consisting of a path in the relationship graph comprising the set of elements that are directly or indirectly related to the location in question. The shared-extent extraction means extracts an anomaly influence process by extracting an extent that is shared among at least a prescribed number of the plurality of paths in the relationship graph that were extracted as reach extents.

(57) 要約:

[続葉有]

WO 2015/140843 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, 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)）

複数箇所で異常が発見された場合であっても、より好適に異常の影響過程を抽出する情報処理装置を提供する。情報処理装置は、システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検知された前記システム上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報を用いて、前記複数の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、到達範囲として抽出する到達範囲抽出手段と、前記到達範囲として抽出された前記関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出する共通範囲抽出手段と、を備える。

明　細　書

発明の名称 ： 情報処理装置、影響過程抽出方法および記録媒体

技術分野

[0001] 本発明は、情報処理装置、影響過程抽出方法および記録媒体に関する。

背景技術

[0002] 大規模なネットワークシステムにおいて、ある箇所で異常が検知された場合、当該異常の原因箇所がどこか、および、当該異常の影響範囲はどこかを、特定することは難しい。

[0003] したがって、上記異常が検知された場合、上記原因箇所および影響範囲の特定には、人手による上記ネットワークシステムに含まれるホスト等のログの解析が必要であった。したがって、上記原因箇所および影響範囲の特定は、多大な工数がかかるという問題があった。また、上記原因箇所および影響範囲の特定には、上記解析を行う作業者の能力に依存してしまうという問題があった。

[0004] 特許文献１には、監視対象ネットワーク内の機器で生成されたログに基づいて、複数種の評価パラメータを用いて、監視対象ネットワークに対する攻撃の攻撃元と攻撃経路を推定する攻撃判定装置が記載されている。

[0005] また、特許文献２には、ネットワークに潜在するサービス間の依存関係を形式的に表現した依存関係グラフを利用して、障害箇所を検出する方法が記載されている。その方法は、依存関係グラフ上における、依存関係を辿り、障害の原因となる、あるいは、障害が影響を与えるネットワーク機器上のサービスの集合を抽出・限定することにより障害箇所を検出する方法である。

先行技術文献

特許文献

[0006] 特許文献1：特開２０１０－１５２７７３号公報

特許文献2：特開平１１－２５９３３１号公報

発明の概要

発明が解決しようとする課題

[0007] しかしながら、上述の技術では、異常が検知された箇所（障害の発見箇所）が一か所の場合を想定しており、複数の箇所で異常が発見される場合については、開示されていない。したがって、複数箇所での異常が発見された場合、異常の影響過程を検出できない可能性がある。

[0008] 本発明は、上記課題に鑑みてなされたものであり、その目的は、複数箇所で異常が発見された場合であっても、より好適に異常の影響過程を抽出する情報処理装置を提供することにある。

課題を解決するための手段

[0009] 本発明の一態様に係る情報処理装置は、システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検知された前記システム上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報を用いて、前記複数の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、到達範囲として抽出する到達範囲抽出手段と、前記到達範囲として抽出された前記関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出する共通範囲抽出手段と、を備える。

[0010] 本発明の一態様に係る情報処理装置は、システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検出された前記システム上の位置を示す情報であって、当該関係グラフ上の位置を示す位置情報を取得する取得手段と、当該取得手段が取得した前記関係グラフおよび前記位置情報を用いて、前記位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、異常の影響過程として抽出する到達範囲抽出手段と、を備える。

[0011] 本発明の一態様に係る影響過程抽出方法は、システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検知された前記システム上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報を用いて、前記複数の位置の夫々を起点に、当該位置から直接的または間接的

に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、到達範囲として抽出し、前記到達範囲として抽出された前記関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出する。

[0012] 本発明の一態様に係る影響過程抽出方法は、情報処理装置の影響過程抽出方法であって、システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検出された前記システム上の位置を示す情報であって、当該関係グラフ上の位置を示す位置情報を取得し、前記取得した前記関係グラフおよび前記位置情報を用いて、前記位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、異常の影響過程として抽出する。

[0013] なお、上記情報処理装置または上記影響過程抽出方法を、コンピュータによって実現するコンピュータプログラム、およびそのコンピュータプログラムが格納されている、コンピュータ読み取り可能な記憶媒体も、本発明の範疇に含まれる。

発明の効果

[0014] 本発明によれば、複数箇所で異常が発見された場合であっても、より好適に異常の影響過程を抽出することができる。

図面の簡単な説明

[0015] [図1]本発明の第１の実施の形態に係る情報処理装置の機能構成の一例を示す機能ブロック図である。

[図2]本発明の第１の実施の形態に係る情報処理システムの構成の一例を示すブロック図である。

[図3]本発明の第１の実施の形態に係る情報処理装置で使用する関係グラフの一例を示す図である。

[図4]本発明の第１の実施の形態に係る情報処理装置で使用する関係グラフで表される要素間の関係を示す概念図である。

[図5]本発明の第１の実施の形態に係る情報処理装置の動作を説明するための

図である。

[図6]本発明の第２の実施の形態に係る情報処理装置の機能構成の一例を示す機能ブロック図である。

[図7]本発明の第２の実施の形態に係る情報処理装置の動作を説明するための図である。

[図8]本発明の第３の実施の形態に係る監視対象システムに含まれる要素の間の時間軸に対する関係を説明するための図である。

[図9]本発明の第３の実施の形態に係る情報処理装置で使用する関係グラフの一例を示す図である。

[図10]本発明の第３の実施の形態に係る情報処理装置の機能構成の一例を示す機能ブロック図である。

[図11]本発明の第３の実施の形態の変形例に係る情報処理装置で使用する関係グラフの一例を示す図である。

[図12]本発明の第３の実施の形態の変形例に係る情報処理装置の機能構成の一例を示す機能ブロック図である。

[図13]本発明の第４の実施の形態に係る情報処理装置の機能構成の一例を示す機能ブロック図である。

[図14]本発明の各実施形態に係る情報処理システムを実現可能な情報処理装置のハードウェア構成の一例を示す図である。

発明を実施するための形態

[0016] ＜第１の実施の形態＞

本発明の第１の実施の形態について、図面を参照して詳細に説明する。図１は、本発明の第１の実施の形態に係る情報処理装置１００の構成の一例を示す図である。図１に示す通り、情報処理装置１００は、到達範囲抽出部１１０と、共通範囲抽出部１２０とを備えている。

[0017] ここで、図２を参照して、情報処理装置１００を含む情報処理システム１について説明を行う。図２は、本実施の形態に係る情報処理システム１の構成の一例を示す図である。図２に示す通り、情報処理システム１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とを備えている。情報処理装置１００と監視対象システム９００とは、図示しないネットワークで接続されている。なお、図２の例に係わらず、複数の監視対象システム９００が、情報処理装置１００に接続されてよい。

[0018] 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。

[0019] 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。

[0020] 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。

[0021] 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。

[0022] 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。

[0023] 次に、情報処理装置１００の各部について説明する。

[0024] （到達範囲抽出部１１０）

到達範囲抽出部１１０は、監視対象システム９００に含まれる複数のノード（要素とも呼ばれる）間の関係を表す関係グラフと、当該関係グラフ上の複数の位置を示す情報（位置情報）とを、図示しない外部装置から受信する。この位置情報は、異常が検知された監視対象システム９００上の位置を示す情報である。なお、到達範囲抽出部１１０は、上記関係グラフと、上記位置情報とを、情報処理装置１００内の図示しない他の手段から取得する構成であってもよい。上記関係グラフおよび上記位置情報を取得する方法は、特に限定されない。

[0025] ここで、関係グラフについて、図３および４を参照して説明する。図３は、監視対象システム９００に含まれる複数の要素間の関係を表す関係グラフの一例を示す図である。

[0026] 関係グラフは、要素９２０のそれぞれを頂点（要素あるいは節点とも呼ばれる）とし、および、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。関係グラフは、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。図３に示すように、関係グラフは、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。

[0027] 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」との関係を表す辺を有し、その辺の属性は、「Ｌ０」である。第２に、要素９２０「Ｅ１」は、要素９２０「Ｅ３」との関係を表す２つの辺を有し、それら辺の属性は、いずれも「Ｌ１」である。

[0028] 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（関係しない）ことを示す。

[0029] 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、辺や辺の種別は、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。なお、関係グラフは、上述の例に係わらず任意の形式の関係グラフであってよい。

[0030] 図４は、関係グラフで表される要素９２０間の、関係を示す概念図である。図４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。

[0031] なお、関係グラフは、上述の例に係わらず任意の形式で示されてよい。例えば、関係グラフは、隣接リストや隣接行列などのデータ構造をとってもよい。

[0032] 次に、到達範囲抽出部１１０が取得する、位置情報について説明を行う。到達範囲抽出部１１０は、位置情報として、要素を示す情報および／または辺を示す情報を取得する。要素を示す情報とは、例えば、頂点識別子である。また、辺を示す情報としては、例えば、辺の両端に接続する頂点識別子で表される情報である。なお、位置情報はこれらに限定されるものではなく、関係グラフ上の位置を示す情報であればよい。

[0033] なお、本実施の形態において、異常が検知された監視対象システム９００上の位置とは、例えば、マルウェア等に感染したことが検知された監視対象システム９００上の位置であるが、本発明はこれに限定されるものではない。

[0034] 図１に戻り、到達範囲抽出部１１０について説明する。到達範囲抽出部１１０は、位置情報で示される、関係グラフ上の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を抽出する。到達範囲抽出部１１０は、例えば、バックトレースなどを用いて、各起点から到達する関係グラフ上の経路（当該起点と直接的または間接的に関係を有する範囲）を走査し、抽出する。ここで、バックトレースとは、関係グラフが有向グラフである場合に、有向辺を逆方向に辿ることである。なお、本実施の形態では、バックトレースを後方検索とも呼ぶ。

[0035] なお、上記経路の抽出方法は、上記に限定されるものではなく、例えば、ダイクストラ法などであってもよい。そして、到達範囲抽出部１１０は、上記異常が検知された関係グラフ上の位置ごとに抽出した関係グラフ上の経路（到達範囲）を、夫々、共通範囲抽出部１２０に供給する。

[0036] （共通範囲抽出部１２０）

共通範囲抽出部１２０は、到達範囲抽出部１１０から、異常が検知された関係グラフ上の位置ごとに抽出した関係グラフ上の経路を受け取る。そして、共通範囲抽出部１２０は、抽出された関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出する。なお、抽出される共通範囲は、要素であってもよいし、辺であってもよいし、これらの集合であってもよい。そして、共通範囲抽出部１２０は、抽出される共通範囲から、異常の影響過程を抽出する。また、所定数以上の経路とは、全ての経路であってもよいし、予め定められた数または割合以上の経路であってもよい。

[0037] 図５を参照して、情報処理装置１００の動作について、より具体的に説明する。図５は、情報処理装置１００の動作を説明するための図である。図５に示す図は、関係グラフの一例である。図５に示す関係グラフは、Ｅ１～Ｅ２２、Ｃ１およびＣ２の頂点識別子で示される要素と要素間を接続する有向の線分（辺）とで構成されている。なお、説明の便宜上、Ｅ１～Ｅ２２の頂点識別子で示される要素は円で示され、Ｃ１およびＣ２の頂点識別子で示される要素は、四角で示される。

[0038] ここで、異常が検知された関係グラフ上の位置を示す情報（位置情報）が、Ｃ１およびＣ２である場合、到達範囲抽出部１１０は、Ｃ１を起点として、Ｃ１から到達する関係グラフ上の経路を抽出する。そして、到達範囲抽出部１１０は、図５の一点鎖線で囲んだ範囲（経路）をＣ１から到達する到達範囲であると抽出する。

[0039] また、到達範囲抽出部１１０は、Ｃ２を起点として、Ｃ２から到達する関係グラフ上の経路（到達範囲）を抽出する。そして、到達範囲抽出部１１０は、図５の破線で囲んだ範囲をＣ２からの到達範囲であると抽出する。

[0040] そして、到達範囲抽出部１１０は、Ｃ１からの到達範囲を示す情報と、Ｃ２からの到達範囲を示す情報とを共通範囲抽出部１２０に供給する。

[0041] 共通範囲抽出部１２０は、供給された２つの範囲で共通する範囲を抽出する。図５に示す通り、一点鎖線で囲んだ範囲と、破線で囲んだ範囲とで共通する範囲は、斜線で記載された要素（Ｅ１１～Ｅ１４）を含む部分である。

[0042] 共通範囲抽出部１２０は、抽出した共通範囲から、異常の影響過程を抽出する。例えば、図５において、Ｃ１からの到達範囲に含まれるＥ６は、Ｅ５とＥ１４との経路が想定される。ここで、共通範囲は、Ｅ１４であるため、共通範囲抽出部１２０は、Ｅ５とＥ１４との内、Ｅ６から異常の影響が及んでいる経路がＥ１４の経路であると抽出する。このように、共通範囲抽出部１２０は、抽出した共通範囲を用いて、異常の影響過程を抽出することができる。

[0043] なお、共通範囲抽出部１２０が共通範囲として抽出する範囲は、複数の要素であってもよいし、１つの要素であってもよい。また、共通範囲が複数の要素の場合、共通範囲抽出部１２０は、各要素間を接続する辺も共通範囲として抽出してもよい。

[0044] なお、本実施の形態では、異常が検知された関係グラフ上の位置が２つであることを例に説明を行ったが、本発明はこれに限定されるものではない。異常が検知された関係グラフ上の位置は複数であってもよい。また、本実施の形態においては、異常が検知された関係グラフ上の位置が、要素であることを例に説明を行ったが、本発明はこれに限定されるものではない。異常が検知された位置は、辺であってもよい。

[0045] （効果）

本実施の形態に係る情報処理装置１００によれば、複数箇所で異常が発見された場合であっても、より好適に異常の影響過程を抽出することができる。

[0046] なぜならば、到達範囲抽出部１１０が関係グラフと、異常が検知された監視対象システム９００上の位置を示す情報であって、当該関係グラフ上の複

数の位置を示す位置情報を用いて、複数の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる関係グラフ上の経路を、到達範囲として抽出するからである。そして、共通範囲抽出部１２０が、抽出された複数の経路であって、関係グラフ上の経路のうち、所定数以上の経路で共通する範囲を、抽出することにより、異常の影響過程を抽出するからである。

[0047] 到達範囲抽出部１１０が、異常が検知された監視対象システム９００上の位置から関係グラフを用いて、当該位置から到達する範囲を抽出することにより、上記異常がシステムの、どの範囲に影響を与えた可能性があるのかを抽出することができる。

[0048] また、共通範囲抽出部１２０が、異常が検知された関係グラフ上の複数の位置の夫々からの経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出することにより、容易に異常の影響過程を抽出することができる。

[0049] （変形例）

本実施の形態に係る情報処理装置１００は、異常が検知された関係グラフ上の複数の位置（図５ではＣ１、Ｃ２）から、バックトレースを行うことにより、異常が検知された位置から到達する到達範囲を抽出することを例に説明を行ったが、本発明はこれに限定されるものではない。情報処理装置１００の到達範囲抽出部１１０は、異常が検知された位置から、フォワードトレースを行うことにより、到達範囲を抽出してもよい。ここで、フォワードトレースとは、関係グラフが有向グラフである場合に、有向辺を正方向に辿ることである。以降、フォワードトレースを前方検索とも呼ぶ。

[0050] これにより、異常が検出された関係グラフ上の位置から、当該異常が影響を与える可能性がある範囲も、異常の影響過程として抽出することができる。したがって、本変形例に係る情報処理装置１００は、より好適に異常の影響過程を抽出することができる。

[0051] ＜第２の実施の形態＞

本発明の第２の実施の形態について、図面を参照して詳細に説明する。なお、上述した第１の実施の形態で説明した図面に含まれる部材と同じ機能を有する部材については、同じ符号を付し、その詳細な説明を省略する。

[0052] 図６は、本実施の形態に係る情報処理装置１０１の機能構成の一例を示す機能ブロック図である。図６に示す通り、情報処理装置１０１は、共通範囲抽出部１２０と、到達範囲抽出部１３０とを備えている。このように、本実施の形態に係る情報処理装置１０１は、図６に示す通り、第１の実施の形態に係る情報処理装置１００における到達範囲抽出部１１０に代えて、到達範囲抽出部１３０を備えている。

[0053] （到達範囲抽出部１３０）

到達範囲抽出部１３０は、監視対象システム９００に含まれる複数の要素間の関係を表す関係グラフと、異常が検出された監視対象システム９００上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報とを、図示しない外部装置から受信する。

[0054] ここで、前述した第１の実施の形態における異常が検知された、関係グラフ上の位置を示す位置情報は、異常の発生が検知された監視対象システム９００上の複数の位置であって、関係グラフ上の複数の位置を示す位置情報であることを例に説明を行ったが、本発明はこれに限定されるものではない。本実施の形態で使用する位置情報は、第１の実施の形態で情報処理装置１００に入力された位置情報と異なる。その位置情報は、異常の発生が検知された、関係グラフ上の１または複数の位置を示す情報（第１の位置情報）と、異常の原因の可能性があるとして検知された、関係グラフ上の１または複数の位置を示す情報（第２の位置情報）とを含む。なお、第１の位置情報および第２の位置情報はこれに限定されるものではなく、異常として検出された情報であり、夫々、異常の内容が異なるものであればよい。

[0055] ここで、異常の発生を検知した関係グラフ上の位置とは、例えば、マルウェア等に感染したことを検知した関係グラフ上の位置である。また、異常の原因の可能性がある関係グラフ上の位置とは、例えば、脆弱性を有する可能

性があると検知された要素を示す関係グラフ上の位置であってもよいし、攻撃によって通常とは違うふるまいを行っていると検知された要素等を示す関係グラフ上の位置であってもよい。なお、到達範囲抽出部１３０は、上記関係グラフと、上記位置情報とを、情報処理装置１０１内の図示しない他の手段から取得する構成であってもよい。上記関係グラフおよび上記位置情報を取得する方法は、特に限定されない。

[0056] 到達範囲抽出部１３０は、図６に示す通り、第１の抽出部１３１と、第２の抽出部１３２とを含んでいる。第１の抽出部１３１は、一方の位置情報（例えば、第１の位置情報）から、到達する関係グラフ上の範囲を到達範囲として抽出する。また、第２の抽出部１３２は、他方の位置情報（例えば、第２の位置情報）から、上記第１の位置情報とは異なる方法を用いて、到達する関係グラフ上の範囲を到達範囲として抽出する。

[0057] 図７を参照して、情報処理装置１０１における到達範囲抽出部１３０の動作について、より具体的に説明する。図７は、情報処理装置１０１における到達範囲抽出部１３０の動作を説明するための図である。図７に示す図は、関係グラフの一例である。図７に示す関係グラフは、Ｅ１～Ｅ１１、Ｅ１３～２３、Ｃ１およびＣ３の頂点識別子で示される要素と要素間を接続する有向の線分（辺）とで構成されている。なお、説明の便宜上、Ｅ１～Ｅ１１、Ｅ１３～Ｅ２３の頂点識別子で示される要素は円で示され、Ｃ１およびＣ３の頂点識別子で示される要素は、ファイルを示す図形で示される。

[0058] １または複数の第１の位置情報のうちの１つがＣ１であり、１または複数の第２の位置情報のうちの１つがＣ３であるとする。到達範囲抽出部１３０の第１の抽出部１３１は、Ｃ１を起点として、Ｃ１から到達する関係グラフ上の範囲を走査する。なお、第１の抽出部１３１が、Ｃ１から到達する関係グラフ上の範囲を走査する方法は、例えば、バックトレースであるとするが、本発明はこれに限定されるものではない。そして、第１の抽出部１３１は、図７の一点鎖線で囲んだ範囲をＣ１から到達する範囲（第１の到達範囲）であると抽出する。

[0059] また、到達範囲抽出部１３０の第２の抽出部１３２は、Ｃ３を起点として、Ｃ３から到達する関係グラフ上の範囲を走査する。このとき、なお、第２の抽出部１３２が、Ｃ３から到達する関係グラフ上の範囲を走査する方法は、例えば、フォワードトレースであるとするが、本発明はこれに限定されるものではない。第２の抽出部１３２は、第１の抽出部１３１と異なる方法を用いて、上記範囲を走査するものであればよい。そして、第２の抽出部１３２は、図７の破線で囲んだ範囲をＣ３から到達する範囲（第２の到達範囲）であると抽出する。

[0060] そして、共通範囲抽出部１２０は、到達範囲抽出部１３０が抽出した第１の到達範囲および第２の到達範囲の間で共通する範囲を、共通範囲として抽出する。図７に示す通り、一点鎖線で囲んだ範囲と、破線で囲んだ範囲とで共通する範囲は、斜線で記載された要素（Ｅ６～８、Ｅ１３、Ｅ１４、Ｃ３、Ｃ１）を含む部分である。したがって、共通範囲抽出部１２０は、上記斜線で記載された共通範囲を異常の影響過程として抽出する。

[0061] なお、本実施の形態において、第１の位置情報によって示される、関係グラフ上の位置と、第２の位置情報によって示される、関係グラフ上の位置との間の経路（異常の影響過程）を、フォワードトレースとバックトレースとを用いて抽出したが、本発明はこれに限定されるものではない。上記経路は、例えば、第１の位置情報によって示される、関係グラフ上の位置と、第２の位置情報によって示される、関係グラフ上の位置とを用いた双方向ダイクストラ法によって、抽出されるものであってもよい。上記経路の抽出方法は、特に限定されない。

[0062] （効果）

本実施の形態に係る情報処理装置１０１によれば、複数箇所で異常が発見された場合であっても、より好適に異常の影響過程を抽出することができる。

[0063] なぜならば、到達範囲抽出部１３０が、以下の（１）および（２）の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する要素の集

合からなる関係グラフ上の経路を、到達範囲として抽出するからである。

（１）異常の発生が検知されたシステム上の位置を示す情報であって、関係グラフ上の位置を示す１または複数の第１の位置情報で示される位置。

（２）異常の原因の可能性があるとして検知された関係グラフ上の１または複数の位置を示す第２の位置情報で示される位置。

[0064] このように、本実施の形態に係る到達範囲抽出部１３０は、複数箇所で発見された異常の内容が異なる場合であっても、当該異常が検出された、関係グラフ上の夫々の位置を起点に、当該位置から到達する範囲を抽出することができる。

[0065] そして、共通範囲抽出部１２０が、第１および第２の位置情報で示される、関係グラフ上の位置の間の経路を、異常の影響過程として抽出するからである。

[0066] これにより、より少ない工数で異常の影響過程を抽出することができる。

[0067] ＜第３の実施の形態＞

本発明の第３の実施の形態について、図面を参照して詳細に説明する。なお、上述した第１および第２の実施の形態で説明した図面に含まれる部材と同じ機能を有する部材については、同じ符号を付し、その詳細な説明を省略する。

[0068] 本実施の形態では、時間情報を含む関係グラフを用いて、異常の影響過程を求める方法について説明する。

[0069] ここで、図８を参照して、監視対象システム９００の要素間の関係であって、時間軸に対する要素間の関係について説明する。図８は、監視対象システム９００に含まれる要素の間の時間軸に対する関係を説明するための図である。

[0070] 図８において、横軸は時間軸を示している。また、図８において、Ａ～Ｅは頂点識別子であり、円は各頂点識別子で表される要素を示している。また、「ＯＰ」は、各要素から他の要素に対し、ある処理がオープンしたことを示し、「ＣＬ」は、上記ある処理がクローズしたことを示している。つまり

、ある要素と他の要素とは、オープンからクローズまでの間で関係を有している。

[0071] 図８に示す通り、頂点識別子が「Ｃ」の要素（以降、要素（Ｃ）と呼ぶ）は、要素（Ｄ）に対し、「ｔ１」から「ｔ２」まで、および、「ｔ６」から「ｔ１５」まで、の間で関係を有している。同様に、要素（Ｄ）は、要素（Ｅ）に対し、「ｔ３」から「ｔ４」までの間で関係を有している。また、要素（Ｅ）は、要素（Ａ）に対し、「ｔ１２」から「ｔ１４」までの間で関係を有している。また、要素（Ａ）は、要素（Ｂ）に対し、「ｔ８」から「ｔ１３」までの間で関係を有している。また、要素（Ｂ）は、要素（Ｃ）に対し、「ｔ５」から「ｔ７」まで、および、「ｔ１０」から「ｔ１１」まで、の間で関係を有している。

[0072] したがって、本実施の形態に係る情報処理装置１０２で使用する関係グラフは、図９に示す通り、辺の属性として時間情報（第１の時間情報）を有している。各辺の属性として示される時間情報は、ある要素から他の要素に対し、最初の処理がオープンした時間と、最後の処理がクローズした時間とが含まれる。例えば、要素（Ｃ）から要素（Ｄ）に対する辺には、最初の処理がオープンした時間「ｔ１」と、最後の処理がクローズした時間「ｔ１５」が含まれている。なお、図９においては、最初の処理がオープンした時間「ｔ１」と、最後の処理がクローズした時間「ｔ１５」とを、（ｔ１，ｔ１５）と記載している。このように、ある要素間の最初の処理がオープンした時間をt_{first}とも呼び、最後の処理がクローズした時間を、t_{last}とも呼ぶ。そして、本実施の形態では、各辺の属性情報を（t_{first}，t_{last}）と表す。

[0073] このような関係グラフを用いて、異常の影響過程を抽出する情報処理装置１０２について説明する。図１０は、本実施の形態に係る情報処理装置１０２の機能構成の一例を示す機能ブロック図である。図１０に示す通り、本実施の形態に係る情報処理装置１０２は、到達範囲抽出部１４０とデータ取得部１５０と、を備えている。このように、本実施の形態に係る情報処理装置

１０２は、図１０に示す通り、第１の実施の形態に係る情報処理装置１００における到達範囲抽出部１１０に代えて、到達範囲抽出部１４０およびデータ取得部１５０を備え、共通範囲抽出部１２０を備えない構成である。

[0074] データ取得部１５０は、監視対象システム９００に含まれる複数の要素間の関係を表す関係グラフと、異常が検知された監視対象システム９００上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報とを、図示しない外部装置から取得する。なお、データ取得部１５０は、上記関係グラフと、上記位置情報とを、情報処理装置１０２内の図示しない他の手段から取得する構成であってもよい。上記関係グラフおよび上記位置情報を取得する方法は、特に限定されない。関係グラフは、上述したとおり、辺の属性として時間情報を有している。また、位置情報には、異常が検知された時間を示す情報（第２の時間情報）が含まれている。

[0075] なお、データ取得部１５０は、上述した到達範囲抽出部１１０、または、到達範囲抽出部１３０に含まれる機能である。

[0076] データ取得部１５０は、取得した上記関係グラフと、上記位置情報とを、到達範囲抽出部１４０に供給する。

[0077] 到達範囲抽出部１４０は、データ取得部１５０から上記関係グラフと、上記位置情報とを受け取る。到達範囲抽出部１４０は、位置情報に含まれる異常が検知された時間に基づいて、当該時間を示す情報を含む位置情報によって示される関係グラフ上の位置を起点に、当該位置から到達する関係グラフ上の経路（到達範囲）を抽出する。

[0078] 図８および図９を参照して、情報処理装置１０２における到達範囲抽出部１４０の動作について、より具体的に説明する。ここでは、到達範囲抽出部１４０が、図９に示すような関係グラフと、時間「ｔ９」を含む、要素（Ｅ）を示す位置情報とを受け取った場合について説明する。

[0079] 時間「ｔ９」は、図８に星形七角形（符号９で示す位置）で示す通り、ｔ８より後の時間であり、ｔ１０より前の時間である。

[0080] まず、到達範囲抽出部１４０は、位置情報によって示される要素（Ｅ）の

時間ｔ９の関係グラフ上の位置を起点に、当該位置から後方探索と前方探索とを行う。なお、本実施の形態においては、要素間の辺を、例えば、辺（Ｄ，Ｅ）のように記載する。ここで、括弧内の最初の要素は、有向矢印の起点の要素の頂点識別子を示し、２つ目の要素は、有向矢印の終点の要素の頂点識別子を示している。

[0081] 後方探索では、到達範囲抽出部１４０は、まず、現時点で取得される最も古い時間（時間の最小値と呼ぶ）を求める。現時点で取得される最も古い時間とは、検知された異常に対して、影響を与えることができた最後の時間を示す。以降、現時点の最小値をt_{min}と呼ぶ。初期値は、位置情報で示される時間である。そのため最小値（t_{min}）の初期値は、ｔ９である。

[0082] 次に、到達範囲抽出部１４０は、探索対象の辺の属性情報の１つ目の要素（t_{first}）が、位置情報に含まれる時間（つまり、現時点の最小値（＝t_{min}））より前か否かを確認する。以降、不等号を用いて、「$t_{first} < t_{min}$」を満たすか否かを確認する、と記載する。辺（Ｄ，Ｅ）の属性情報は、図９に示す通り、（ｔ３，ｔ４）である。したがって、辺（Ｄ，Ｅ）のt_{first}は、ｔ３である。ｔ３＜ｔ９を満たすので、到達範囲抽出部１４０は、要素（Ｄ）が、要素（Ｅ）と関係を有していると判定し、要素（Ｄ）を後方探索の対象とする。

[0083] 次に、到達範囲抽出部１４０は、要素（Ｄ）が、検知された異常に対して、影響を与えることができた最後の時間を求める。つまり、到達範囲抽出部１４０は、ＭＩＮ（t_{min}，t_{last}）を用いて新しい最小値（t_{min}）を求める。ここで、ＭＩＮ（ｘ，ｙ）は、括弧内の要素のうち、小さい方を返す関数である。ＭＩＮ（ｔ９，ｔ４）＝ｔ４であるため、新しい最小値（t_{min}）は、t_{min}＝ｔ４となる。

[0084] 次に、到達範囲抽出部１４０は、辺（Ｃ，Ｄ）について、$t_{first} < t_{min}$を満たすか否かを確認する。ｔ１＜ｔ４を満たすため、到達範囲抽出部１４０は、要素（Ｃ）が、要素（Ｄ）と関係を有していると判定し、要素（Ｃ）を後方探索の対象とする。そして、到達範囲抽出部１４０は、新しい最小値

を、ＭＩＮ（t_{min}，t_{last}）を用いて求める。新しい最小値は、ＭＩＮ（ｔ４，ｔ１５）から、t_{min}＝ｔ４となる。

[0085] 同様に、到達範囲抽出部１４０は、辺（Ｂ，Ｃ）について、t_{first}＜t_{min}を満たすか否かを確認する。ｔ５＞ｔ４であり、上記条件を満たさないため、到達範囲抽出部１４０は、要素（Ｂ）を後方探索の対象としない。これにより、到達範囲抽出部１４０は、後方探索を終了する。

[0086] 次に、到達範囲抽出部１４０が行う前方探索について説明する。前方探索では、到達範囲抽出部１４０は、まず、現時点で取得される最も新しい時間（時間の最大値と呼ぶ）を求める。現時点で取得される最も新しい時間とは、検知された異常に対して、影響を与えることができた最初の時間を示す。以降、現時点の最大値をt_{max}と呼ぶ。初期値は、位置情報で示される時間である。そのため最大値（t_{max}）の初期値は、ｔ９である。

[0087] 次に、到達範囲抽出部１４０は、探索対象の辺の属性情報の２つ目の要素（t_{last}）が、位置情報に含まれる時間（現時点の最大値（＝t_{max}））より後か否かを確認する。以降、不等号を用いて、「t_{max}＜t_{last}」を満たすか否かを確認する、と記載する。辺（Ｅ，Ａ）の属性情報は、図１１に示す通り、（ｔ１２，ｔ１４）である。したがって、辺（Ｅ，Ａ）のt_{last}は、ｔ１４である。ｔ９＜ｔ１４を満たすため、到達範囲抽出部１４０は、要素（Ｅ）が、要素（Ａ）と関係を有していると判定し、要素（Ａ）を前方探索の対象とする。

[0088] 次に、到達範囲抽出部１４０は、要素（Ａ）が、検知された異常に対して、影響を与えることができた最初の時間を求める。つまり、到達範囲抽出部１４０は、ＭＡＸ（t_{max}，t_{first}）を用いて新しい最大値（t_{max}）を求める。ここで、ＭＡＸ（ｘ，ｙ）は、括弧内の要素のうち、大きい方を返す関数である。ＭＡＸ（ｔ９，ｔ１２）＝ｔ１２であるため、新しい最大値（t_{max}）は、t_{max}＝ｔ１２となる。

[0089] 次に、到達範囲抽出部１４０は、辺（Ａ，Ｂ）について、t_{max}＜t_{last}を満たすか否かを確認する。ｔ１２＜ｔ１３を満たすため、到達範囲抽出部

１４０は、要素（Ａ）が、要素（Ｂ）と関係を有していると判定し、要素（Ｂ）を前方探索の対象とする。そして、新しい最大値を、ＭＡＸ（t_{max}，t_{first}）を用いて求める。新しい最大値は、ＭＡＸ（ｔ１２，ｔ８）から、t_{max}＝ｔ１２となる。

[0090] 同様に、到達範囲抽出部１４０は、辺（Ｂ，Ｃ）について、t_{max}＜t_{last}を満たすか否かを確認する。ｔ１２＞ｔ１１であり、上記条件を満たさないため、到達範囲抽出部１４０は、要素（Ｃ）を前方探索の対象としない。これにより、到達範囲抽出部１４０は、前方探索を終了する。

[0091] 到達範囲抽出部１４０は、位置情報で示される関係グラフ上の位置ごとに、以上のように前方探索および後方探索して抽出した関係グラフ上の経路を、異常の影響過程として抽出する。

[0092] なお、本実施の形態では、到達範囲抽出部１４０が後方探索を行った後に前方探索を行うことについて説明を行ったが、本発明はこれに限定されるものではない。到達範囲抽出部１４０は、後方探索と前方探索とを同時に行ってもよいし、前方探索の後に後方探索を行ってもよい。

[0093] （効果）

本実施の形態に係る情報処理装置１０２によれば、より好適に異常の影響過程を抽出することができる。また、時間情報を用いて異常の影響過程の抽出を行うことにより、情報処理装置１０２は、異常の影響過程の探索時間を削減することができる。

[0094] したがって、より少ない工数で異常の影響過程を抽出することができる。

[0095] また、本発明の第２の目的として、特許文献１または２に記載の技術では、特定される異常の範囲が不十分、または、広すぎる可能性があるという、更なる課題がある。なぜならば、特許文献１または２に記載の技術では、異常が検知された時点におけるその異常が検知されたサービスや機器に対する依存関係について考慮されていないからである。つまり、特許文献１および２の技術では、システム全体では依存関係を有していても、異常が検知された時点において異常が検知されたサービスや機器に対する依存関係を有して

いないサービスや機器等も異常の影響過程として抽出される可能性がある。したがって、より好適に異常の影響過程を特定することが求められる。

[0096] 本実施の形態に係る情報処理装置１０２によれば、上記課題も解決することができる。

[0097] （変形例１）

本実施の形態に係る変形例１について、図１１を参照して説明を行う。図１１は、本変形例に係る情報処理装置１０２で使用する関係グラフの一例を示す図である。なお、本変形例に係る情報処理装置１０２は、図１０に示す情報処理装置１０２と同様の機能構成を有するため、その説明を省略する。

[0098] 上述した第３の実施の形態に係る情報処理装置１０２で用いる関係グラフには、時間情報が辺の属性として含まれる構成について説明を行ったが、本発明はこれに限定されるものではない。時間情報は、要素の属性として含まれる構成であってもよい。

[0099] 図１１に示す関係グラフは、図８を用いて説明した情報を含むものである。まず、図１１においては、時間ｔ０（初期状態）で複数の頂点（A_1，B_1，C_1，D_1，E_1）が生成されていることを示す。そして、各頂点は、他の要素から、ある処理がオープンした際に生成されたものである。言い換えると、ある要素Ｍが別の要素Ｎに、新たに影響を与えることができる状態になるたびに、Ｍのある時点の状態を表す頂点M_i、Ｎのある時点の状態を表す頂点N_jからの有向辺をもつ、要素Ｎの新たな状態を表す頂点N_{j+1}を生成している。なお、ｉおよびｊは、自然数である。例えば、図８において、要素（Ｃ）から要素（Ｄ）に対する処理が、時間「ｔ１」でオープンしている。そのため、図１１に示す通り、関係グラフには、時間「ｔ１」の位置に頂点D_2が含まれる。更に、関係グラフには、各頂点間の関係を示す辺（C_1からD_2に対する辺と、D_1からD_2に対する辺）が含まれる。

[0100] また、時間「ｔ１０」では、頂点（C_3）と、頂点（D_4）を新たに生成している。図８に示す通り、時間「ｔ１０」において、要素（Ｂ）から要素（Ｃ）に対し、処理が新たにオープンしている。そのため、図１１に示す関係

グラフには、時間「ｔ１０」の情報を有した頂点（C_3）が含まれる。ここで、要素（Ｃ）から要素（Ｄ）に対する処理は、時間「ｔ１０」の時点では、継続して行われている。したがって、要素（Ｃ）から要素（Ｄ）に対する処理は、要素（Ｂ）による要素（Ｃ）に対する処理の影響を受ける可能性がある。したがって、図１１に示す関係グラフには、頂点（C_3）が含まれる時間と同じ時間「ｔ１０」に、頂点（D_4）が含まれる。

[0101] 到達範囲抽出部１４０は、このような情報を含んだ関係グラフを用いて、位置情報および時間によって示される関係グラフ上の位置を起点に、当該位置から到達する関係グラフ上の経路を、異常の影響過程として抽出する。

[0102] 図１１を参照して、情報処理装置１０２における到達範囲抽出部１４０の動作について、より具体的に説明する。ここでは、到達範囲抽出部１４０が、図１１に示すような関係グラフと、時間「ｔ９」を含む、頂点（E_2）を示す位置情報とを受け取った場合について説明する。

[0103] まず、到達範囲抽出部１４０は、頂点（E_2）を起点に、当該頂点の位置から後方探索を行う。頂点（E_2）に関連付けられた経路は、図１１の破線の太い矢印で表される経路（C_1からD_2、D_1からD_2、D_2からE_2、E_1からE_2の経路）である。したがって、到達範囲抽出部１４０は、後方探索の結果として、当該経路を抽出する。

[0104] 次に、到達範囲抽出部１４０は、頂点（E_2）を起点に、当該頂点の位置から前方探索を行う。頂点（E_2）に関連付けられた経路は、図１１の破線の太い矢印で表される経路（E_2からA_2、A_2からB_3の経路）である。したがって、到達範囲抽出部１４０は、前方探索の結果として、当該経路を抽出する。

[0105] 到達範囲抽出部１４０は、位置情報で示される関係グラフ上の位置ごとに、以上のように前方探索および後方探索して抽出した関係グラフ上の経路を、異常の影響過程として抽出する。

[0106] なお、本変形例では、到達範囲抽出部１４０が後方探索を行った後に前方探索を行うことについて説明を行ったが、本発明はこれに限定されるもので

はない。到達範囲抽出部１４０は、後方探索と前方探索とを同時に行ってもよいし、前方探索の後に後方探索を行ってもよい。

[0107] このように、図１１に示すような関係グラフであっても、本変形例１における情報処理装置１０２によれば、上述した第３の実施の形態と同様に、より好適に異常の影響過程を抽出することができる。したがって、上述した第２の実施の形態と同様に、より少ない工数で異常の影響過程を抽出することができる。

[0108] なお、上述した関係グラフの時間情報の持ち方、および、それを利用した探索方法は、一例であり、本発明はこれに限定されるものではない。

[0109] （変形例２）

本実施の形態に係る変形例２について、図１２を参照して説明を行う。図１２は、本変形例に係る情報処理装置１０３の機能構成を示す機能ブロック図である。なお、上述した第１から第３の実施の形態で説明した図面に含まれる部材と同じ機能を有する部材については、同じ符号を付し、その詳細な説明を省略する。

[0110] 本変形例に係る情報処理装置１０３は、図１２に示す通り、共通範囲抽出部１２０、到達範囲抽出部１４０、および、データ取得部１５０を備えている。図１２に示す通り、本変形例に係る情報処理装置１０３は、第３の実施の形態において説明した情報処理装置１０２に、共通範囲抽出部１２０を更に備える構成である。

[0111] 情報処理装置１０３における到達範囲抽出部１４０は、位置情報で示される関係グラフ上の位置ごとに、第３の実施の形態で説明した前方探索および後方探索して抽出した関係グラフ上の経路を、到達範囲として抽出する。そして、異常が検出された、関係グラフ上の複数の位置の夫々に対し、抽出した到達範囲を、共通範囲抽出部１２０に供給する。

[0112] 共通範囲抽出部１２０は、上述した第１および第２の実施の形態と同様に、到達範囲抽出部１４０が、関係グラフ上の複数の位置の夫々に対して抽出した上記到達範囲を用いて、所定数以上の到達範囲で共通する範囲を抽出す

る。共通範囲抽出部１２０は、この抽出した範囲を異常の影響過程として抽出することができる。

[0113] このように、本変形例に係る情報処理装置１０３の構成であっても、上述した第１から第３の実施の形態と同様の効果を得ることができる。

[0114] ＜第４の実施の形態＞

本発明の第４の実施の形態について、図面を参照して詳細に説明する。なお、上述した第１から第３の実施の形態で説明した図面に含まれる部材と同じ機能を有する部材については、同じ符号を付し、その詳細な説明を省略する。

[0115] 図１３は、本実施の形態に係る情報処理装置１０４の機能構成の一例を示す機能ブロック図である。図１３に示す通り、情報処理装置１０４は、到達範囲抽出部１１０と、共通範囲抽出部１２０と、経路異常度評価部１６０とを備えている。なお、図１３に示す情報処理装置１０４は、第１の実施の形態の情報処理装置１００に、更に経路異常度評価部１６０を備える構成であるが、その他の実施の形態の情報処理装置に経路異常度評価部１６０を備える構成であってもよい。

[0116] （経路異常度評価部１６０）

経路異常度評価部１６０は、監視対象システム９００に含まれる複数の要素間の関係を表す関係グラフを、図示しない外部装置から受信する。なお、経路異常度評価部１６０は、上記関係グラフを、情報処理装置１０４内の図示しない他の手段から取得する構成であってもよい。上記関係グラフを取得する方法は、特に限定されない。

[0117] 経路異常度評価部１６０が取得する関係グラフには、辺の属性として、辺の異常度（例えば、重み）が含まれる。例えば、通常の動作では関係を有しない要素同士が、取得した関係グラフ上では辺で接続されている場合、当該辺には、当該辺の属性として高い異常度が含まれる。また、通常の動作で関係を有する要素同士を接続する辺には、当該辺の属性として低い異常度が含まれる。経路異常度評価部１６０は、このような辺の属性を含む関係グラフ

を取得する。また、異常度は、辺に限定されず、ノードに対して付されたものであってもよい。

[0118] また、経路異常度評価部１６０には、異常が検出された監視対象システム９００上の位置を示す情報であって、関係グラフ上の位置を示す位置情報を取得する。

[0119] 経路異常度評価部１６０は、取得した関係グラフと、位置情報とから、当該位置情報によって示される関係グラフ上の位置を起点にした経路に対し、当該経路の異常度を評価する。経路異常度評価部１６０は、評価した結果（評価結果）である、経路の異常度を示す情報を生成し、当該情報を到達範囲抽出部１１０に供給する。

[0120] なお、辺の異常度は、辺の属性として、関係グラフに含まれることを例に説明を行ったが、本発明はこれに限定されるものではない。経路異常度評価部１６０は、辺の異常度を、関係グラフとは別に取得する構成であってもよい。

[0121] また、経路異常度評価部１６０は、各辺に対し、当該辺の異常度を算出する構成であってもよい。経路異常度評価部１６０は、例えば、各辺の距離の合計を求め、当該各辺の距離の合計を辺の総数で割った数を閾値とし、当該閾値より距離が長い辺を異常度が高いと評価し、距離が短い辺を異常度が低いと評価する。なお、上記閾値は予め定められた値であってもよい。

[0122] なお、経路異常度評価部１６０が経路の異常度を評価する方法はこれに限定されるものではない。経路異常度評価部１６０は、例えば、各辺で表される要素間の関係の発生回数が所定の閾値より小さいか否かを判定することにより、各辺の異常度を評価してもよい。また、上記閾値は、上記回数の合計を辺の総数で割った数としてもよい。

[0123] このように、経路異常度評価部１６０は、到達範囲抽出部１１０による探索をより効率化するための情報（評価結果）を到達範囲抽出部１１０に供給する。

[0124] 到達範囲抽出部１１０は、経路異常度評価部１６０から供給された評価結

果と、取得した関係グラフと、取得した位置情報とを用いて、到達経路を抽出する。このとき、到達範囲抽出部１１０は、評価結果に基づいて、異常度が高い経路を到達範囲として抽出する。到達範囲抽出部１１０の到達範囲の抽出方法は、例えば、位置情報によって示される関係グラフ上の位置から、上記関係グラフ上の経路中の各辺の異常度を累積し、累積値が所定の値より高い経路を抽出する方法であってもよいし、そのほかの方法であってもよい。例えば、到達範囲抽出部１１０は、異常度の平均値を求め、当該平均値より異常度が高い辺を有する経路を抽出してもよい。

[0125] そして、到達範囲抽出部１１０は、抽出した到達範囲を、共通範囲抽出部１２０に供給する。なお、このとき、到達範囲抽出部１１０は、経路異常度評価部１６０から取得した評価結果を共通範囲抽出部１２０に供給してもよい。

[0126] また、共通範囲抽出部１２０は、到達範囲抽出部１１０から供給された評価結果と、到達範囲とを用いて共通範囲を抽出してもよい。これにより、共通範囲抽出部１２０は、異常度を反映した影響過程を抽出することができる。また、共通範囲抽出部１２０は、供給された評価結果を抽出した影響過程と共に出力してもよい。

[0127] （効果）

本実施の形態に係る情報処理装置１０４によれば、より好適に異常の影響過程を抽出することができる。なぜならば、経路異常度評価部１６０が、関係グラフの経路の異常度を評価し、評価結果を生成するからである。

[0128] これにより、到達範囲抽出部１１０は、上記評価結果を用いて到達範囲を抽出するため、より好適な範囲の到達範囲を抽出することができる。

[0129] また、共通範囲抽出部１２０は、上記評価結果を用いて、異常の影響過程を抽出するため、より、異常の度合いを反映させた影響過程を抽出することができる。

[0130] （ハードウェア構成について）

なお、図１、６、１０、１２および１３に示した情報処理装置の各部は、

図１４に例示するハードウェア資源で実現してもよい。即ち、図１４に示す構成は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１１１、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１１２、通信インタフェース１１３、記憶媒体１１４およびＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１５を備える。ＣＰＵ１１５は、ＲＯＭ１１２または記憶媒体１１４に記憶された各種ソフトウェアプログラム（コンピュータプログラム）を、ＲＡＭ１１１に読み出して実行することにより、情報処理装置の全体的な動作を司る。すなわち、上記各実施形態において、ＣＰＵ１１５は、ＲＯＭ１１２または記憶媒体１１４を適宜参照しながら、情報処理装置が備える各機能（各部）を実行するソフトウェアプログラムを実行する。

[0131] また、各実施形態を例に説明した本発明は、情報処理装置に対して、上記説明した機能を実現可能なコンピュータプログラムを供給した後、そのコンピュータプログラムを、ＣＰＵ１１５がＲＡＭ１１１に読み出して実行することによって達成される。

[0132] また、係る供給されたコンピュータプログラムは、読み書き可能なメモリ（一時記憶媒体）またはハードディスク装置等のコンピュータ読み取り可能な記憶デバイスに格納すればよい。そして、このような場合において、本発明は、係るコンピュータプログラムを表すコード或いは係るコンピュータプログラムを格納した記憶媒体によって構成されると捉えることができる。

[0133] 上述した各実施形態では、図１、６、１０、１２および１３に示した情報処理装置における各ブロックに示す機能を、図１４に示すＣＰＵ１１５が実行する一例として、ソフトウェアプログラムによって実現する場合について説明した。しかしながら、図１、６、１０、１２および１３に示した各ブロックに示す機能は、一部または全部を、ハードウェアの回路として実現してもよい。

[0134] なお、上述した各実施の形態は、本発明の好適な実施の形態であり、上記各実施の形態にのみ本発明の範囲を限定するものではなく、本発明の要旨を逸脱しない範囲において当業者が上記各実施の形態の修正や代用を行い、種

々の変更を施した形態を構築することが可能である。

[0135] この出願は、２０１４年３月２０日に出願された日本出願特願２０１４－０５８５５８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

[0136] １ 情報処理システム

１００ 情報処理装置

１０１ 情報処理装置

１０２ 情報処理装置

１０３ 情報処理装置

１０４ 情報処理装置

１１０ 到達範囲抽出部

１２０ 共通範囲抽出部

１３０ 到達範囲抽出部

１３１ 第１の抽出部

１３２ 第２の抽出部

１４０ 到達範囲抽出部

１５０ データ取得部

１６０ 経路異常度評価部

９００ 監視対象システム

９２０ 要素

請求の範囲

[請求項1] システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検知された前記システム上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報を用いて、前記複数の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、到達範囲として抽出する到達範囲抽出手段と、

前記到達範囲として抽出された前記関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出する共通範囲抽出手段と、を備えることを特徴とする情報処理装置。

[請求項2] 前記位置情報には、異常の発生が検知された前記システム上の位置を示す情報であって、前記関係グラフ上の位置を示す複数の第１の位置情報が含まれ、

前記到達範囲抽出手段は、前記複数の第１の位置情報の夫々で示される関係グラフ上の位置から、到達範囲を抽出する、ことを特徴とする請求項１に記載の情報処理装置。

[請求項3] 前記位置情報には、異常の発生が検知された前記システム上の位置を示す情報であって、前記関係グラフ上の位置を示す１または複数の第１の位置情報と、異常の原因の可能性があるとして検知された関係グラフ上の１または複数の位置を示す第２の位置情報とが含まれ、

前記到達範囲抽出手段は、前記第１の位置情報によって示される、前記関係グラフ上の位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、第１の到達範囲として抽出する第１の抽出手段と、前記第２の位置情報によって示される、前記関係グラフ上の位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、第２の到達範囲として抽出する第２の抽出手段

とを含み、

前記共通範囲抽出手段は、前記第１の位置情報によって示される、前記関係グラフ上の位置と、前記第２の位置情報によって示される、前記関係グラフ上の位置との間の経路を、前記異常の影響過程として抽出することを特徴とする請求項１に記載の情報処理装置。

[請求項4] 前記関係グラフには、前記要素および／または前記辺の属性として、第１の時間情報が含まれ、

前記位置情報には、前記異常が検知された時間を示す第２の時間情報が含まれ、

前記到達範囲抽出手段は、前記第２の時間情報によって示される、前記異常が検知された時間に基づいて、当該第２の時間情報を含む前記位置情報によって示される、前記関係グラフ上の位置を起点に、当該位置から到達する前記関係グラフ上の経路を、前記到達範囲として抽出する、ことを特徴とする請求項１から３の何れか１項に記載の情報処理装置。

[請求項5] 前記第１の時間情報が前記要素の属性であるとき、前記到達範囲抽出手段は、前記異常が検知された時間より前の時間を検索する第１の検索、および／または、前記異常が検知された時間より後の時間を検索する第２の検索を行うことにより、前記位置情報によって示される前記関係グラフ上の位置から到達する前記関係グラフ上の経路を抽出する、ことを特徴とする請求項４に記載の情報処理装置。

[請求項6] 前記第１の時間情報には、各辺に対し、前記辺の一方の端部に接続された要素から他方の端部に接続された要素に対し、最初に影響を及ぼした開始時間と、最後に影響を及ぼした終了時間とが含まれ、

前記第１の検索は、現時点で取得可能な最も古い時間と前記終了時間とを比較し、古い方の時間を前記最も古い時間とし、前記開始時間が当該最も古い時間より前の時間の場合、当該開始時間を含む辺の前記一方の端部に接続された前記要素を前記到達範囲に含ませ、前記開

始時間が前記最も古い時間より後の時間の場合、前記開始時間を含む辺の前記一方の端部に接続された前記要素を前記到達範囲に含ませない、ことを特徴とする請求項５に記載の情報処理装置。

[請求項7] 前記第１の時間情報には、各辺に対し、前記辺の一方の端部に接続された要素から他方の端部に接続された要素に対し、最初に影響を及ぼした開始時間と、最後に影響を及ぼした終了時間とが含まれ、

前記第２の検索は、現時点で取得可能な最も新しい時間と前記開始時間とを比較し、新しい方の時間を前記最も新しい時間とし、前記終了時間が当該最も新しい時間より後の時間の場合、当該終了時間を含む辺の前記他方の端部に接続された前記要素を前記到達範囲に含ませ、前記終了時間が当該最も新しい時間より前の時間の場合、前記終了時間を含む辺の前記他方の端部に接続された前記要素を前記到達範囲に含ませない、ことを特徴とする請求項５または６に記載の情報処理装置。

[請求項8] 前記関係グラフには、ある要素が他の要素に影響を与えることができる状態になるたびに生成される、第１の時間情報を含む頂点が含まれ、

前記位置情報には、前記異常が検知された時間を示す第２の時間情報が含まれ、

前記到達範囲抽出手段は、前記第２の時間情報によって示される、前記異常が検知された時間に基づいて、前記第２の時間情報を含む前記位置情報によって示される、前記関係グラフ上の位置を起点に、当該位置から到達する前記関係グラフ上の経路を、前記到達範囲として抽出する、ことを特徴とする請求項１から３の何れか１項に記載の情報処理装置。

[請求項9] 前記関係グラフの経路の異常度を評価し、評価結果を生成する、経路異常度評価手段を更に備え、

前記到達範囲抽出手段は、前記評価結果を用いて、前記到達範囲を

抽出する、ことを特徴とする請求項１から８の何れか１項に記載の情報処理装置。

[請求項10] 前記共通範囲抽出手段は、前記評価結果を用いて、前記異常の影響過程を抽出する、ことを特徴とする請求項９に記載の情報処理装置。

[請求項11] システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検出された前記システム上の位置を示す情報であって、当該関係グラフ上の位置を示す位置情報を取得する取得手段と、

当該取得手段が取得した前記関係グラフおよび前記位置情報を用いて、前記位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、異常の影響過程として抽出する到達範囲抽出手段と、を備えることを特徴とする情報処理装置。

[請求項12] 前記関係グラフには、前記要素および／または前記辺の属性として、第１の時間情報が含まれ、

前記位置情報には、前記異常が検知された時間を示す第２の時間情報が含まれ、

前記到達範囲抽出手段は、前記第２の時間情報によって示される、異常が検知された時間に基づいて、当該第２の時間情報を含む前記位置情報によって示される前記関係グラフ上の位置を起点に、当該位置から到達する前記関係グラフ上の経路を、前記異常の影響過程として特定する、ことを特徴とする請求項１１に記載の情報処理装置。

[請求項13] 前記第１の時間情報が前記要素の属性であるとき、前記到達範囲抽出手段は、前記異常が検知された時間より前の時間を検索する第１の検索、および／または、前記異常が検知された時間より後の時間を検索する第２の検索を行うことにより、前記位置情報によって示される前記関係グラフ上の位置から到達する前記関係グラフ上の経路を抽出する、ことを特徴とする請求項１２に記載の情報処理装置。

[請求項14] 前記第１の時間情報には、各辺に対し、前記辺の一方の端部に接続

された要素から他方の端部に接続された要素に対し、最初に影響を及ぼした開始時間と、最後に影響を及ぼした終了時間とが含まれ、

前記第１の検索は、現時点で取得可能な最も古い時間と前記終了時間とを比較し、古い方の時間を前記最も古い時間とし、前記開始時間が当該最も古い時間より前の時間の場合、当該開始時間を含む辺の前記一方の端部に接続された前記要素を前記異常の影響過程に含ませ、前記開始時間が前記最も古い時間より後の時間の場合、前記開始時間を含む辺の前記一方の端部に接続された前記要素を前記異常の影響過程に含ませない、ことを特徴とする請求項１３に記載の情報処理装置。

[請求項15] 前記第１の時間情報には、各辺に対し、前記辺の一方の端部に接続された要素から他方の端部に接続された要素に対し、最初に影響を及ぼした開始時間と、最後に影響を及ぼした終了時間とが含まれ、

前記第２の検索は、現時点で取得可能な最も新しい時間と前記開始時間とを比較し、新しい方の時間を前記最も新しい時間とし、前記終了時間が当該最も新しい時間より後の時間の場合、当該終了時間を含む辺の前記他方の端部に接続された前記要素を前記異常の影響過程に含ませ、前記終了時間が当該最も新しい時間より前の時間の場合、前記終了時間を含む辺の前記他方の端部に接続された前記要素を前記異常の影響過程に含ませない、ことを特徴とする請求項１３または１４に記載の情報処理装置。

[請求項16] 前記関係グラフには、ある要素が他の要素に影響を与えることができる状態になるたびに生成される、第１の時間情報を含む頂点が含まれ、

前記位置情報には、前記異常が検知された時間を示す第２の時間情報が含まれ、

前記到達範囲抽出手段は、前記第２の時間情報によって示される、前記異常が検知された時間に基づいて、前記第２の時間情報を含む前

記位置情報によって示される、前記関係グラフ上の位置を起点に、当該位置から到達する前記関係グラフ上の経路を、前記異常の影響過程として抽出する、ことを特徴とする請求項１１に記載の情報処理装置。

[請求項17] 前記関係グラフの経路の異常度を評価し、評価結果を生成する、経路異常度評価手段を更に備え、

前記到達範囲抽出手段は、前記評価結果を用いて、前記異常の影響過程を抽出する、ことを特徴とする請求項１１から１６の何れか１項に記載の情報処理装置。

[請求項18] 情報処理装置の影響過程抽出方法であって、

システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検知された前記システム上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報を用いて、前記複数の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、到達範囲として抽出し、

前記到達範囲として抽出された前記関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出する、ことを特徴とする影響過程抽出方法。

[請求項19] 情報処理装置の影響過程抽出方法であって、

システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検出された前記システム上の位置を示す情報であって、当該関係グラフ上の位置を示す位置情報を取得し、

前記取得した前記関係グラフおよび前記位置情報を用いて、前記位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、異常の影響過程として抽出する、ことを特徴とする影響過程抽出方法。

[請求項20] 情報処理装置を含むコンピュータに、

システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検知された前記システム上の位置を示す情報であって、当該関係グラフ上の複数の位置を示す位置情報を用いて、前記複数の位置の夫々を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、到達範囲として抽出する処理と、

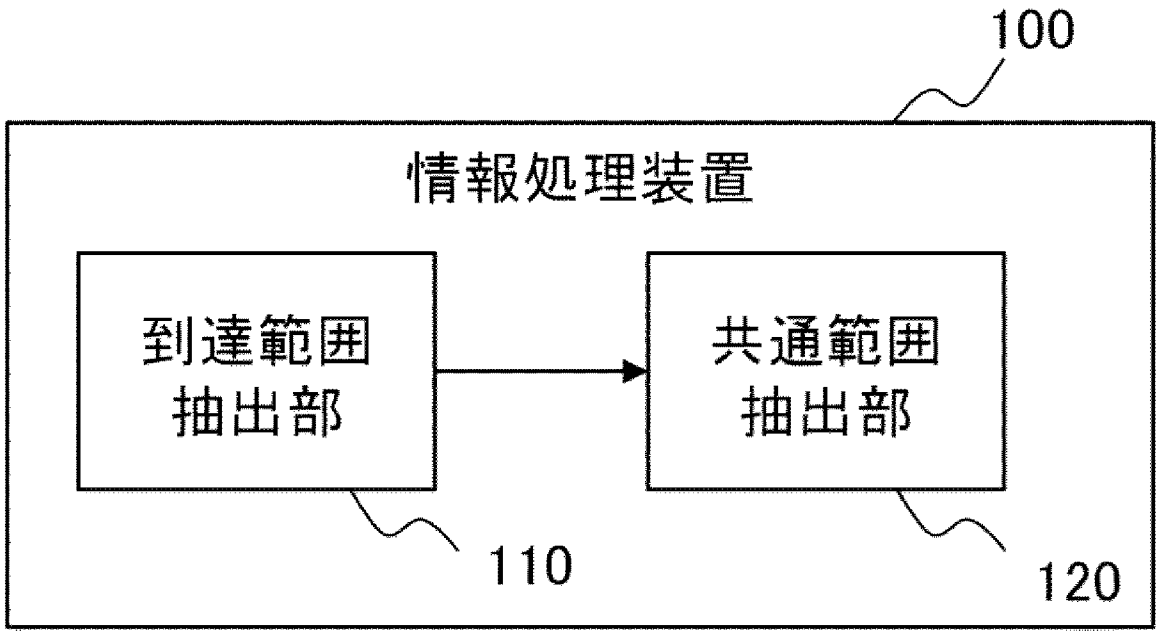
前記到達範囲として抽出された前記関係グラフ上の複数の経路のうち、所定数以上の経路で共通する範囲を抽出することにより、異常の影響過程を抽出する処理と、を実行させるプログラムを記録するコンピュータで読み取り可能な記録媒体。

[請求項21] 情報処理装置を含むコンピュータに、

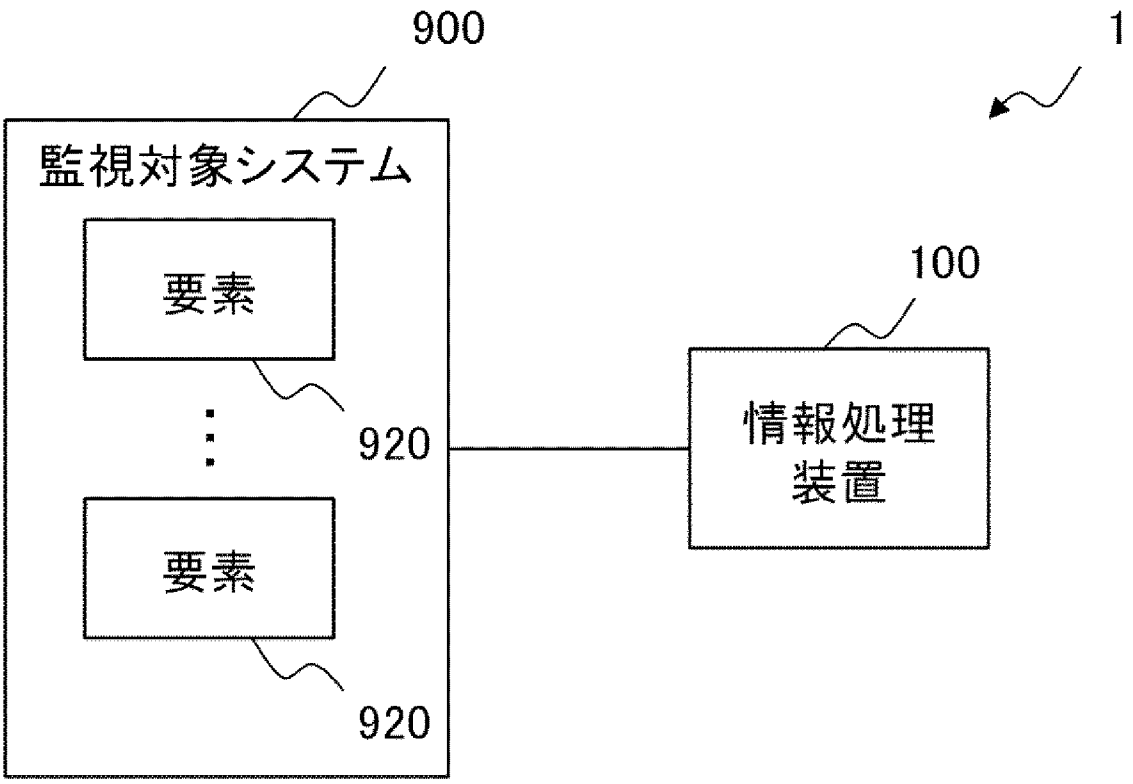
システムに含まれる複数の要素間の関係を表す関係グラフ、および、異常が検出された前記システム上の位置を示す情報であって、当該関係グラフ上の位置を示す位置情報を取得する処理と、

前記取得した前記関係グラフおよび前記位置情報を用いて、前記位置を起点に、当該位置から直接的または間接的に関係を有する前記要素の集合からなる前記関係グラフ上の経路を、異常の影響過程として抽出する処理と、を実行させるプログラムを記録するコンピュータで読み取り可能な記録媒体。

[図1]


100
情報処理装置
到達範囲
抽出部
共通範囲
抽出部
110
120

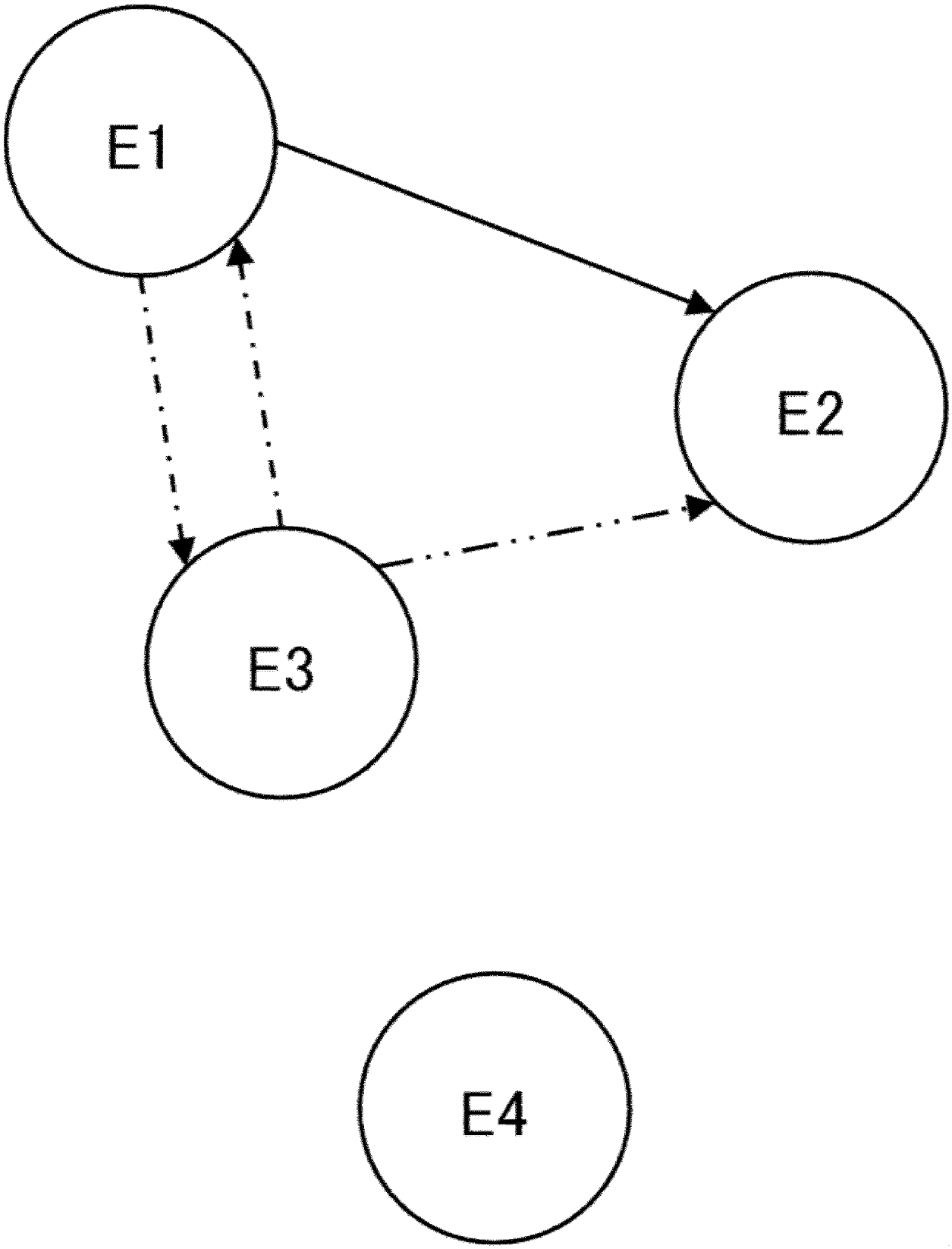
[図2]


900
1
監視対象システム
要素
100
920
情報処理
装置
要素
920

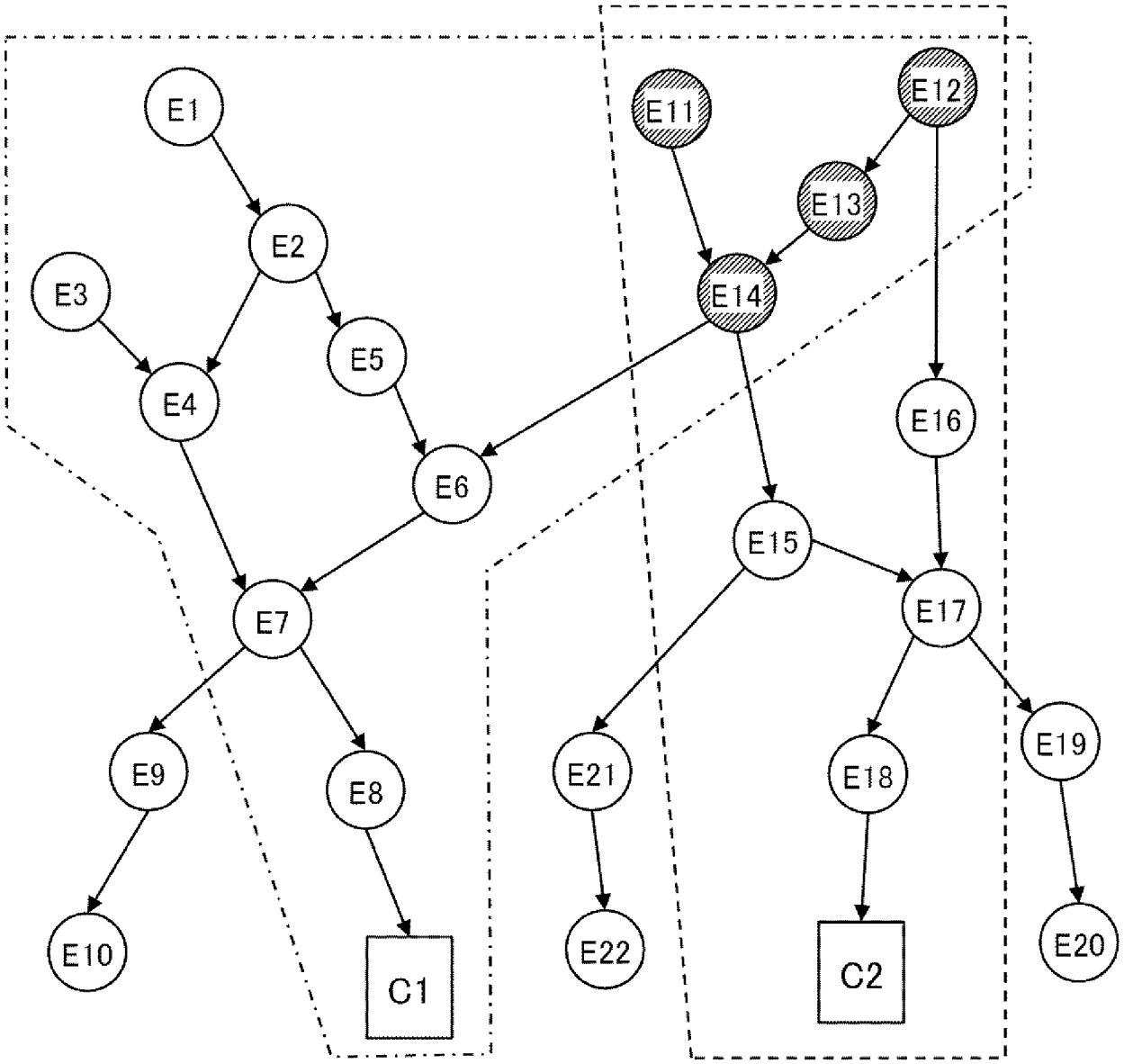
[図3]

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

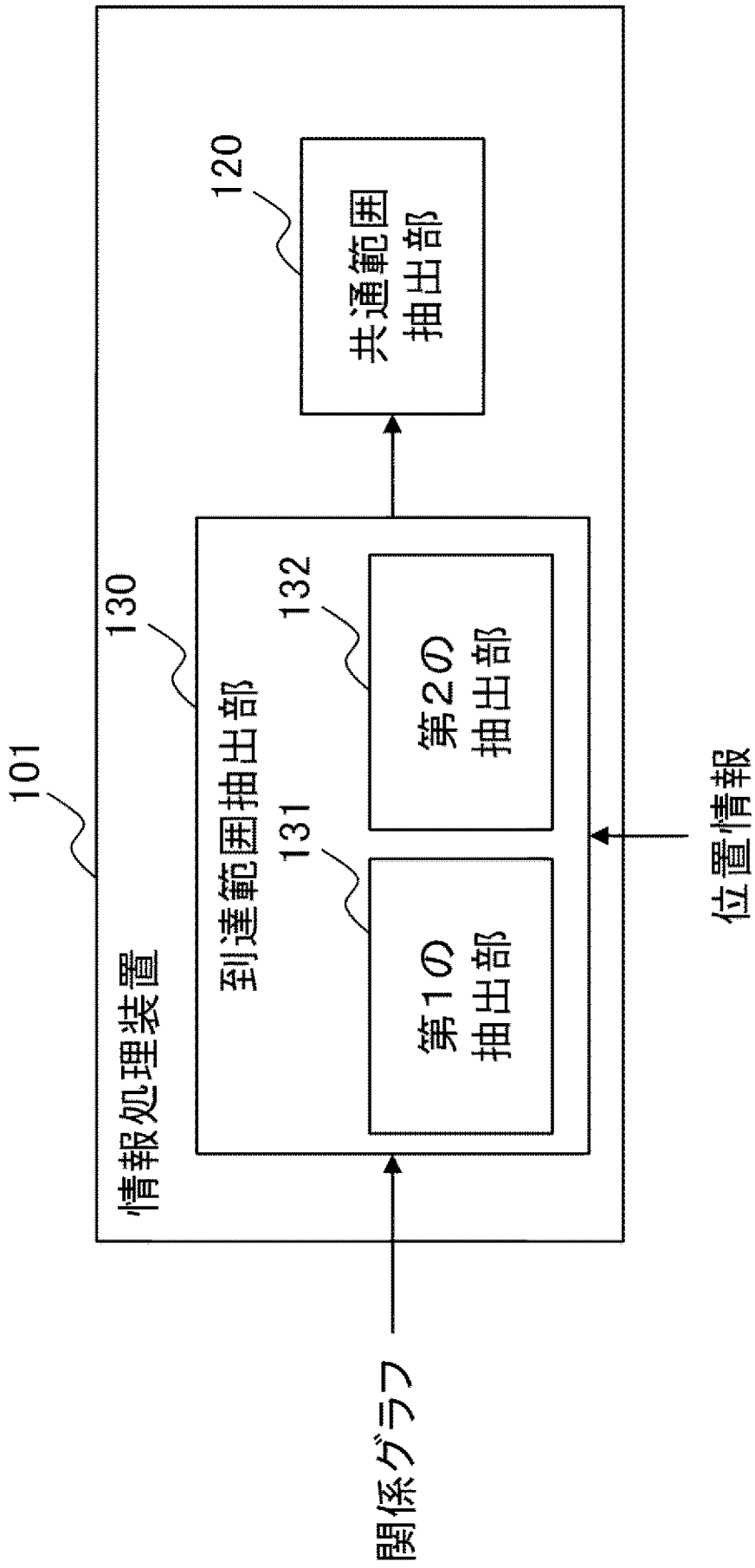
[図4]



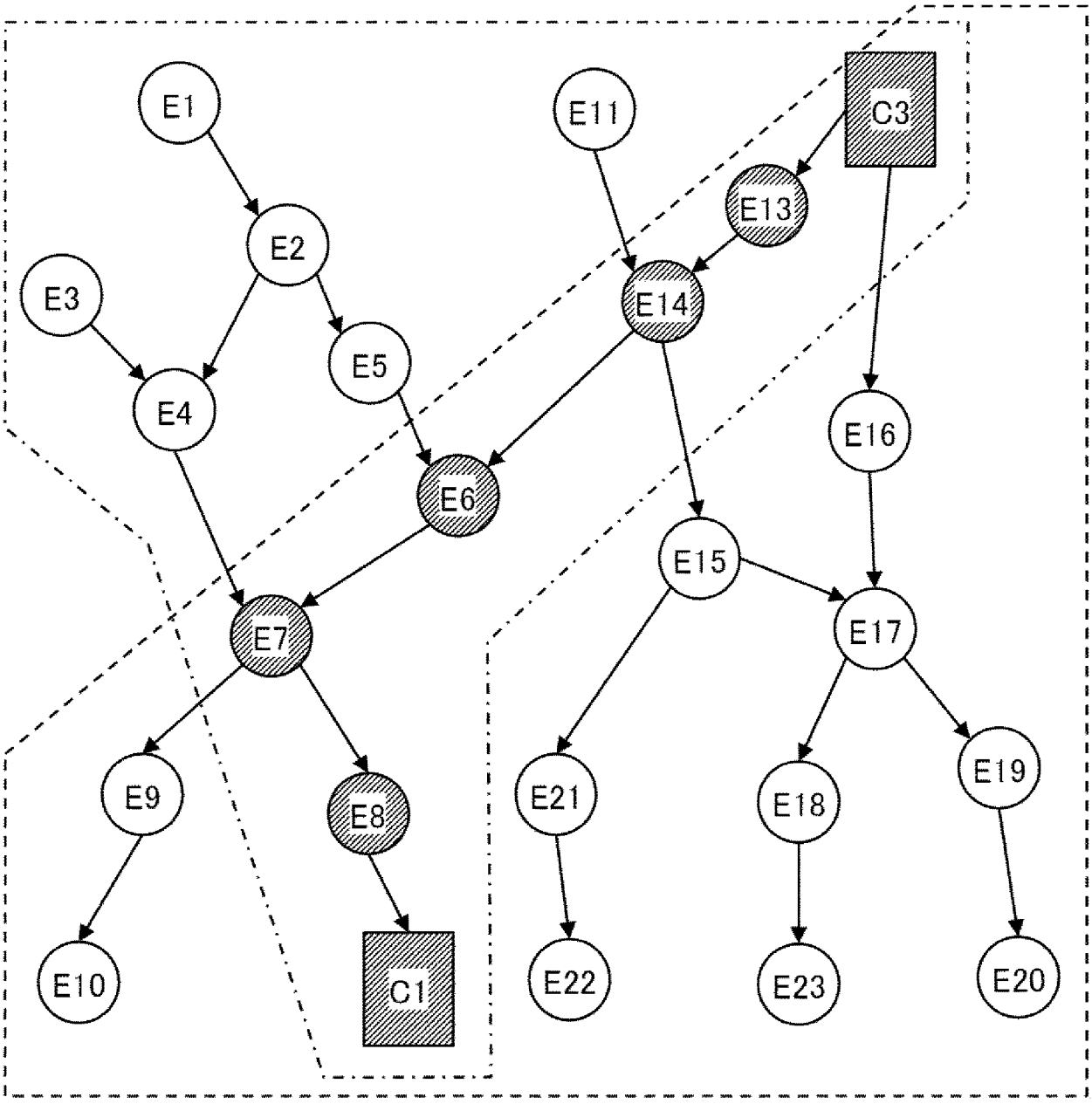
[図5]


E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
C1
E11
E12
E13
E14
E15
E16
E17
E18
E19
E20
E21
E22
C2

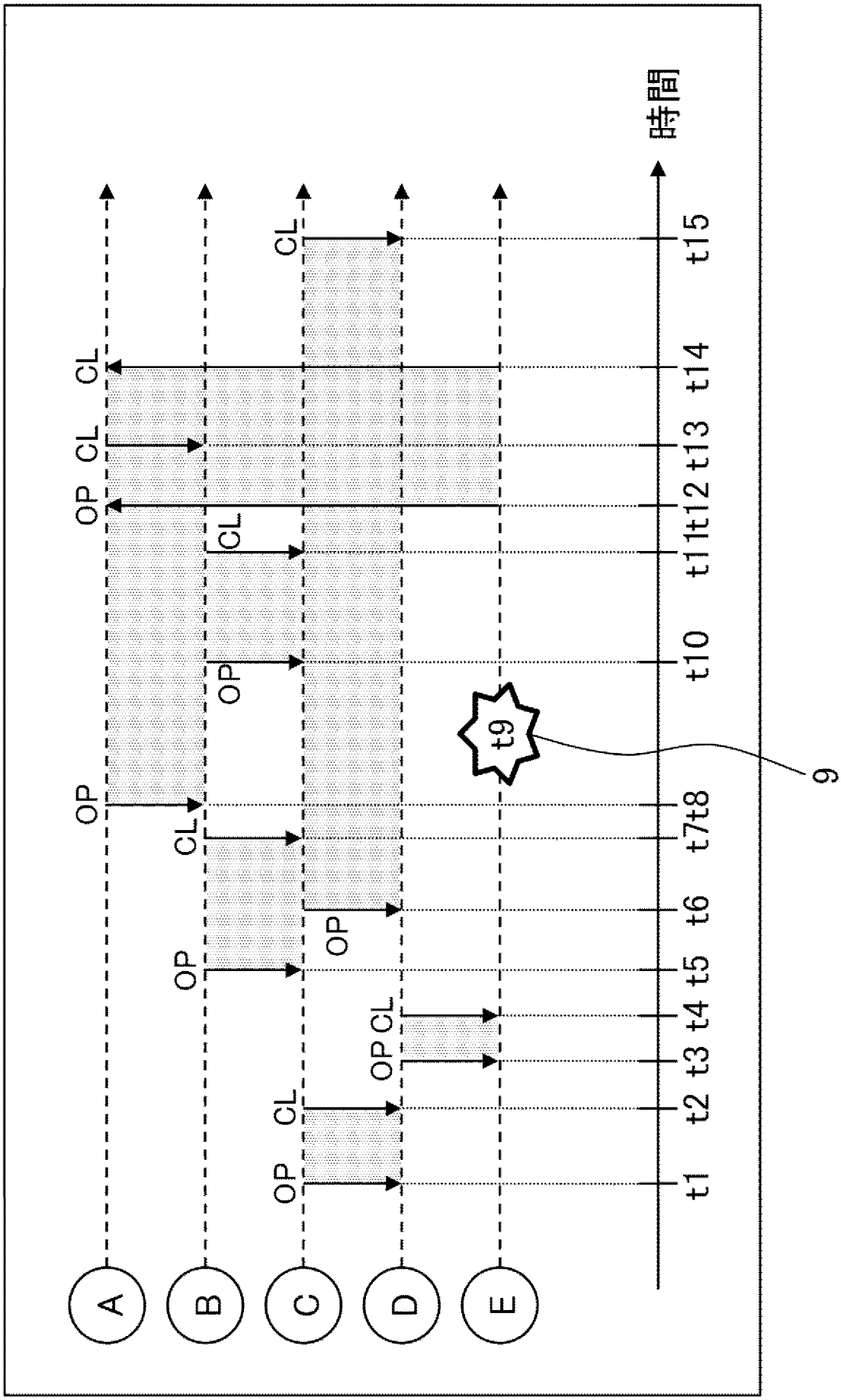
[図6]


101
情報処理装置
130
到達範囲抽出部
131
第1の
抽出部
132
第2の
抽出部
120
共通範囲
抽出部
関係グラフ
位置情報

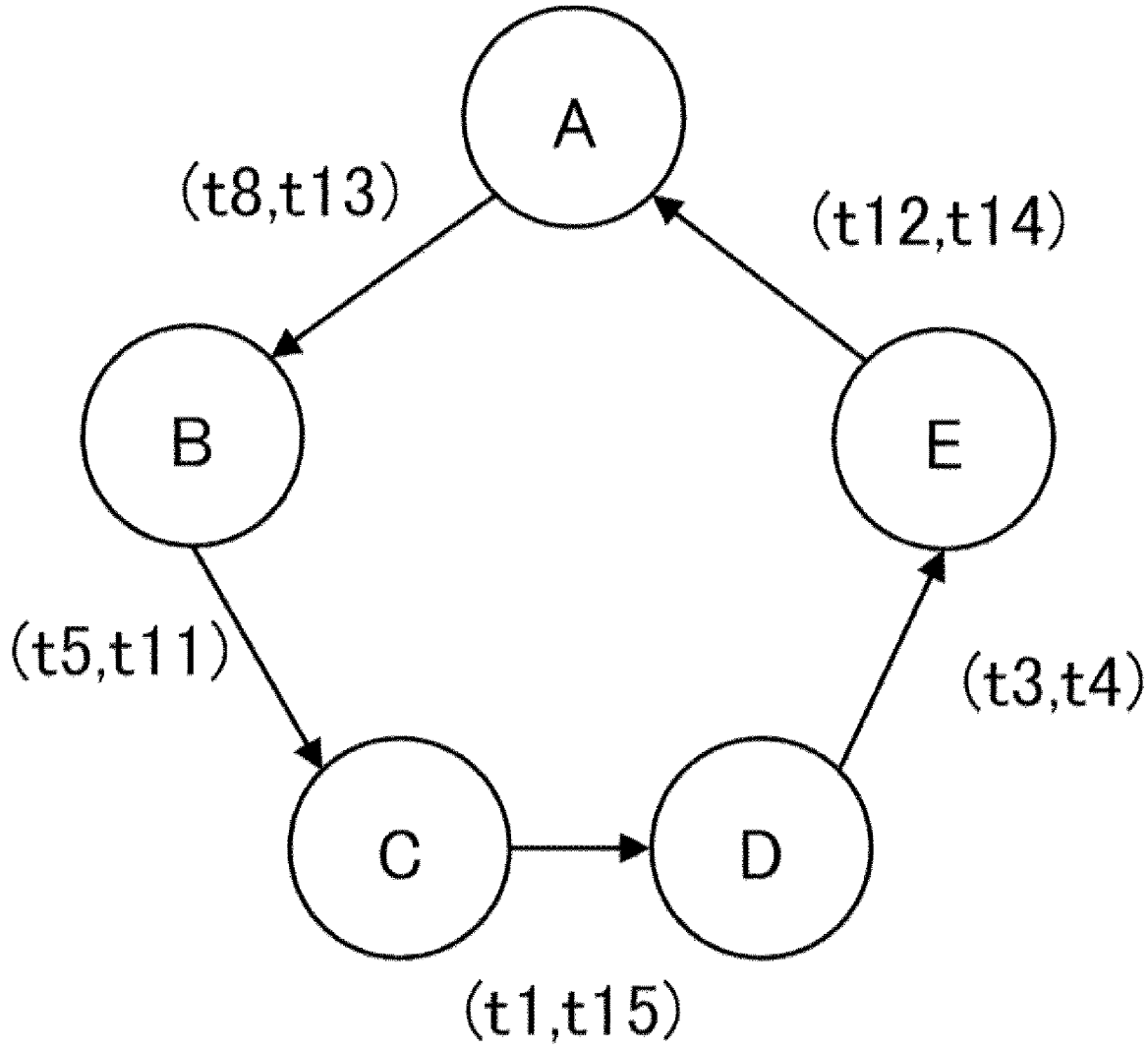
[図7]


E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
C1
E11
C3
E13
E14
E16
E15
E17
E21
E18
E19
E22
E23
E20

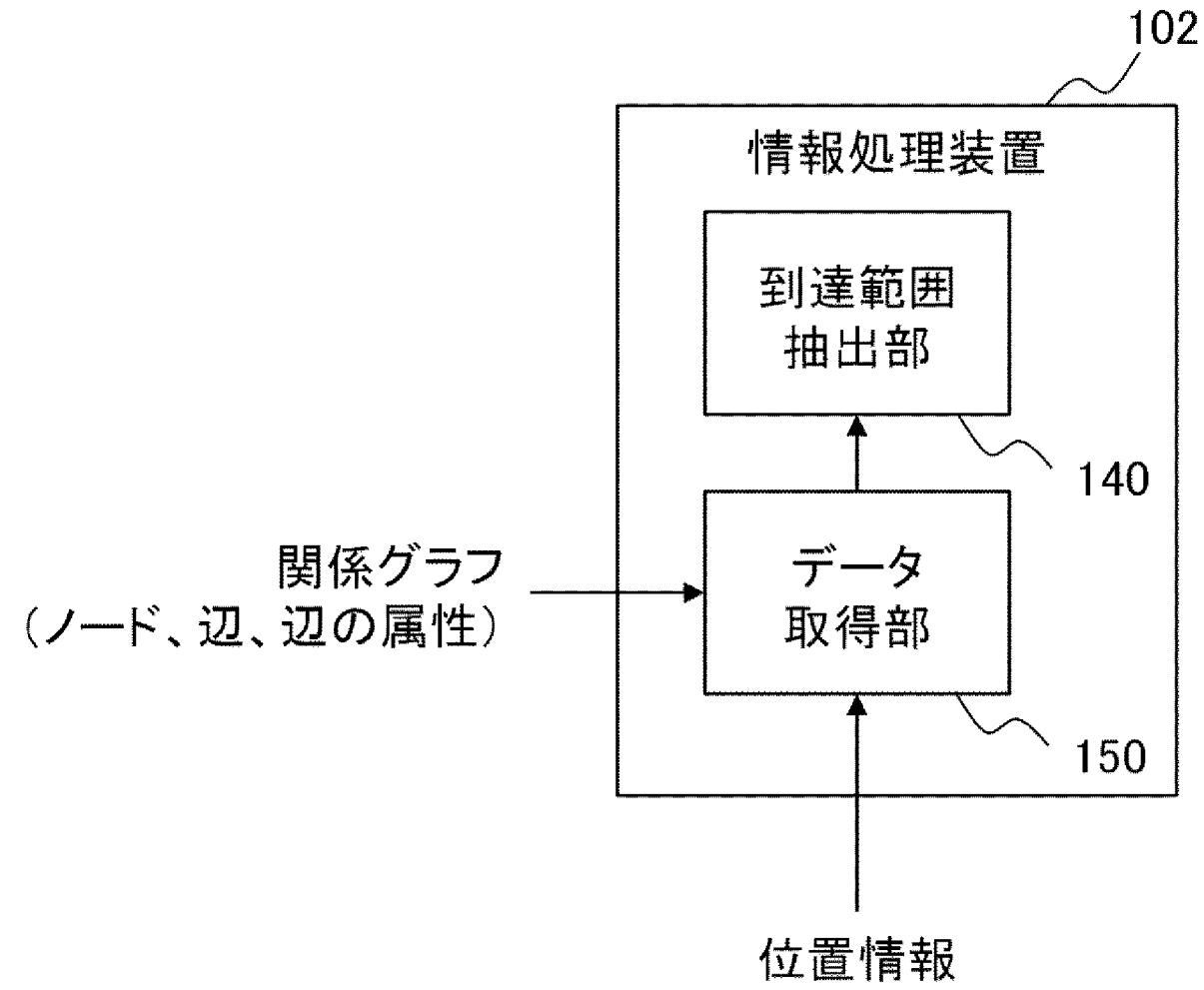
[図8]



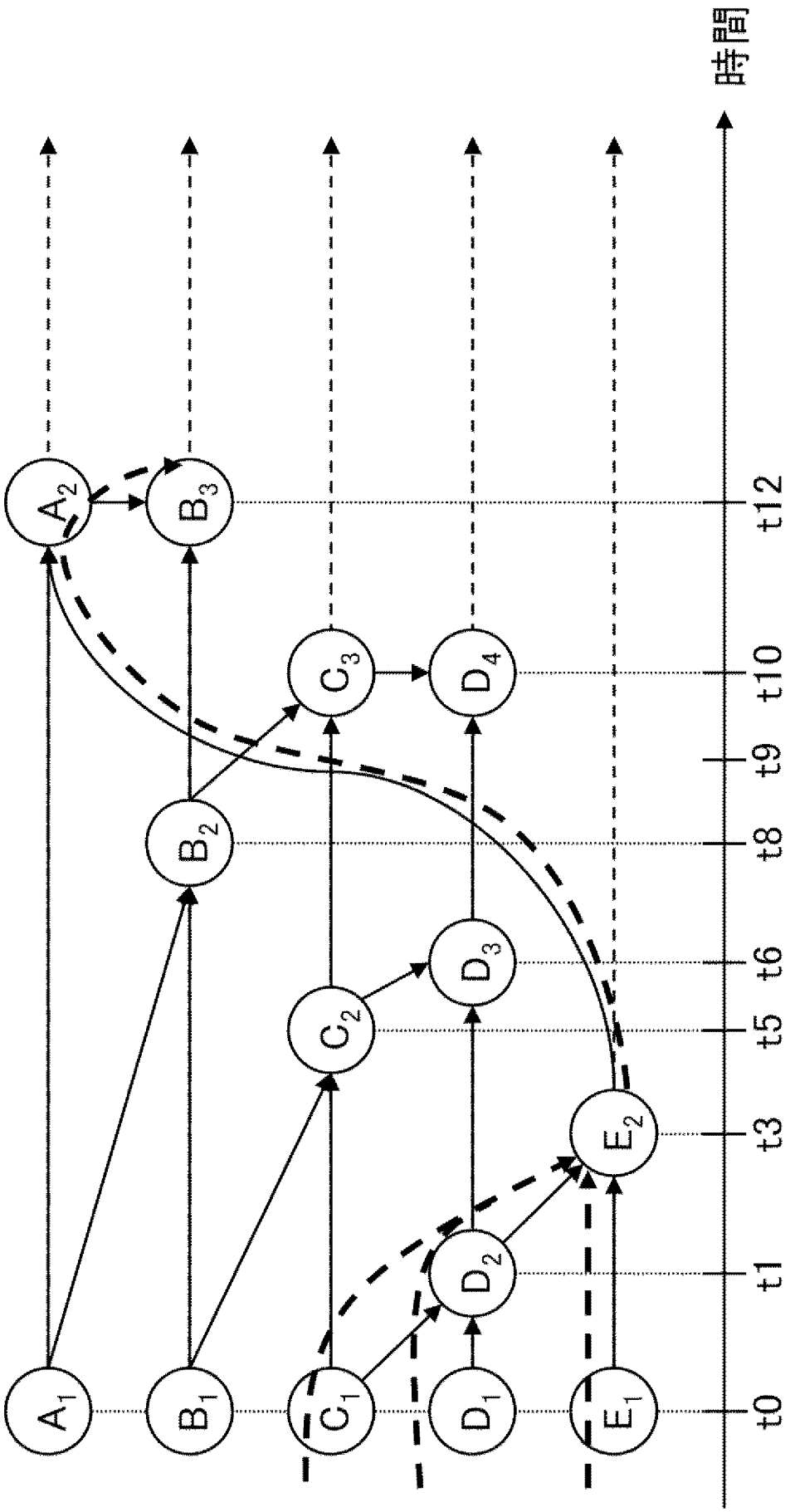
[図9]



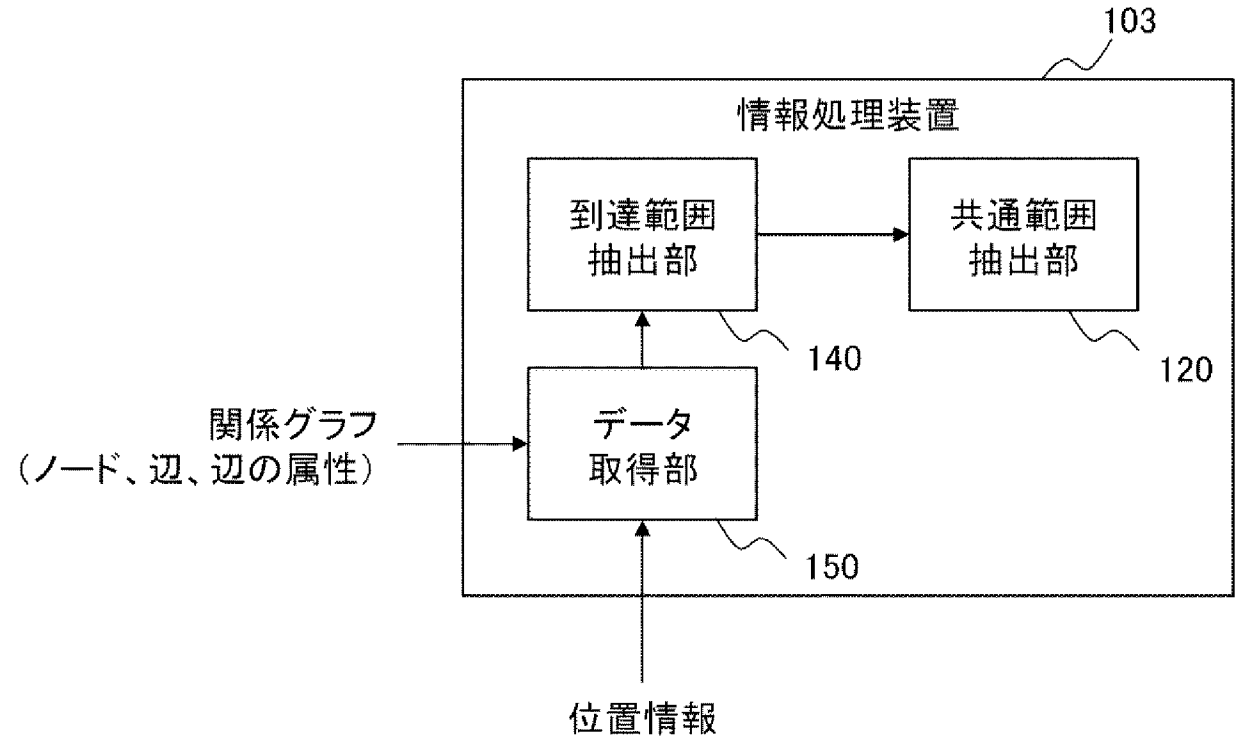
[図10]



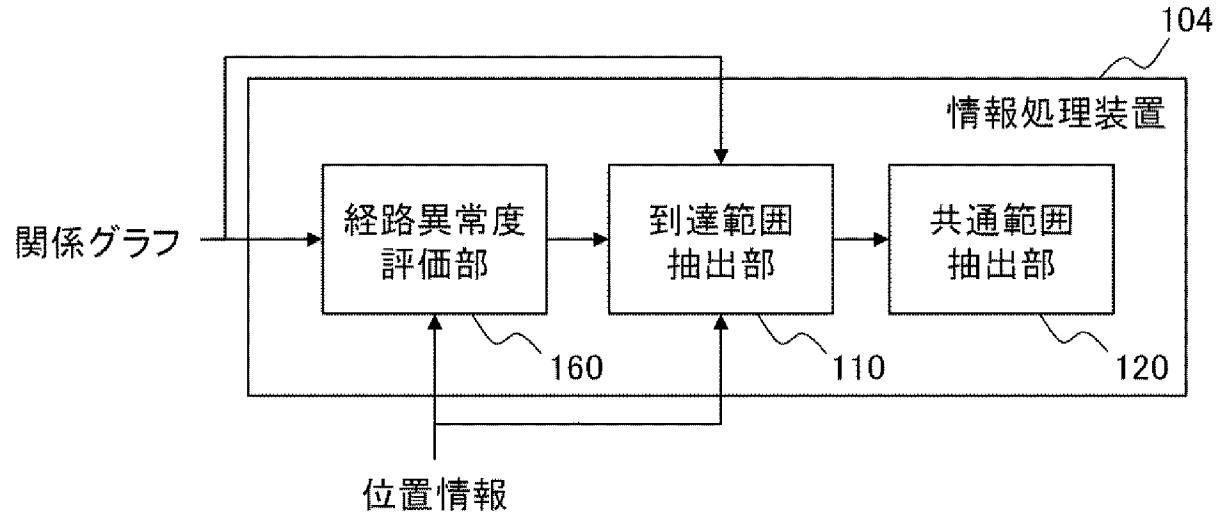
[図11]


時間
t0
t1
t3
t5
t6
t8
t9
t10
t12
A1
B1
C1
D1
E1
A2
B3
C3
D4
B2
D3
C2
E2
D2

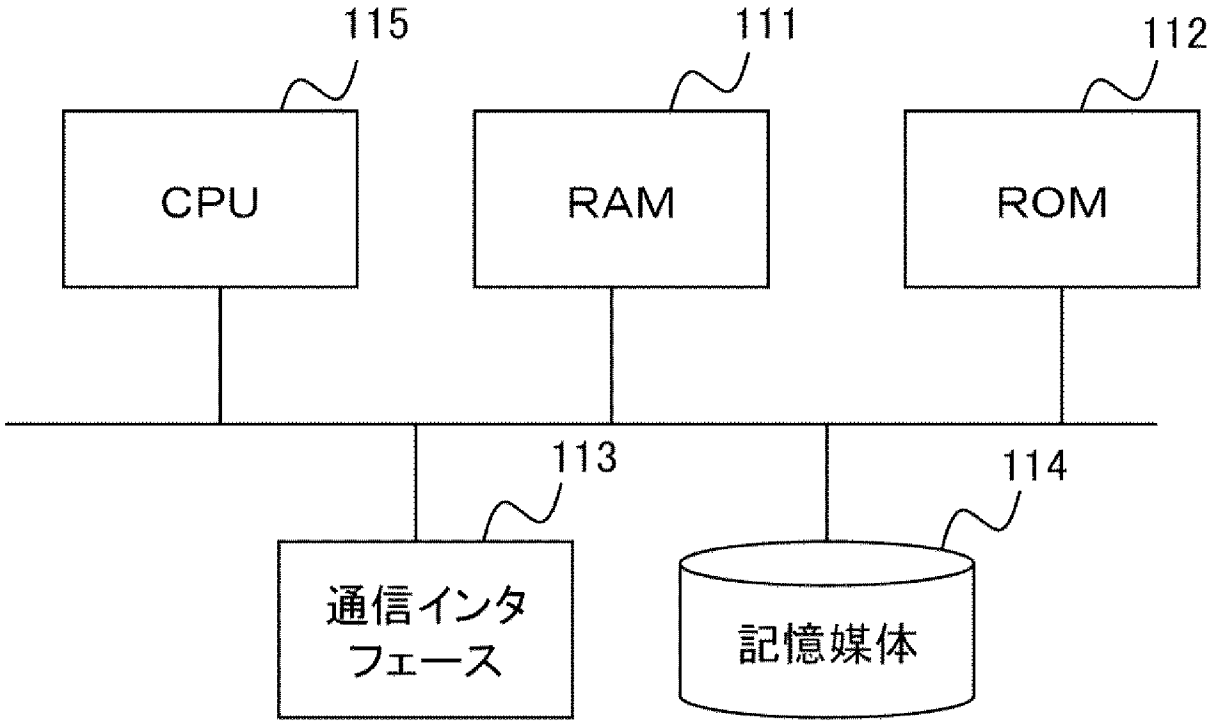
[図12]


103
情報処理装置
到達範囲
抽出部
共通範囲
抽出部
140
120
関係グラフ
（ノード、辺、辺の属性）
データ
取得部
150
位置情報

[図13]


104
情報処理装置
関係グラフ
経路異常度
評価部
到達範囲
抽出部
共通範囲
抽出部
160
110
120
位置情報

[図14]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/003227

A. CLASSIFICATION OF SUBJECT MATTER
G06F11/30(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

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	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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.
X Y A	JP 2011-113122 A (Mitsubishi Electric Corp.), 09 June 2011 (09.06.2011), paragraphs [0001], [0011], [0020] to [0030], [0070], [0081], [0092] to [0093]; fig. 1, 3, 8, 13 (Family: none)	11,17,19,21 1-3,9-10,18, 20 4-8,12-16
Y	JP 6-175884 A (Nippon Telegraph and Telephone Corp.), 24 June 1994 (24.06.1994), paragraphs [0012] to [0018], [0038] to [0040]; fig. 4 (Family: none)	1-3,9-10,18, 20

☒ 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
06 November, 2014 (06.11.14)	18 November, 2014 (18.11.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/003227

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 11-259331 A (Nippon Telegraph and Telephone Corp.), 24 September 1999 (24.09.1999), paragraphs [0006] to [0007]; fig. 1 (Family: none)	1-21
A	JP 2011-113571 A (Electronics and Telecommunications Research Institute), 09 June 2011 (09.06.2011), paragraphs [0009] to [0017], [0044] to [0050]; fig. 7 to 9 & US 2011/0131252 A1 & KR 10-2011-0059295 A	1-21
A	WO 2012/073686 A1 (Japan Science and Technology Agency), 07 June 2012 (07.06.2012), entire text; all drawings & US 2013/0297972 A1 & JP 5280587 B2 & EP 2648104 A1	1-21
A	US 2012/0215912 A1 (John R. HOULIHAN), 23 August 2012 (23.08.2012), entire text; all drawings (Family: none)	1-21

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／００３２２７

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

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

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	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４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
X Y	JP 2011-113122 A（三菱電機株式会社）2011.06.09, 段落【0001】, 【0011】, 【0020】-【0030】, 【0070】, 【0081】, 【0092】-【0093】, 第1,3,8,13図（ファミリーなし）	11,17,19,21 1-3,9-10,18,20
A		4-8,12-16
Y	JP 6-175884 A（日本電信電話株式会社）1994.06.24, 段落【0012】-【0018】, 【0038】-【0040】, 第４図（ファミリーなし）	1-3,9-10,18,20

☑　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	国際調査報告の発送日
０６．１１．２０１４	１８．１１．２０１４

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　４６８０
大塚　俊範
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
A	JP 11-259331 A (日本電信電話株式会社) 1999.09.24, 段落【0006】-【0007】, 第1図 (ファミリーなし)	1-21
A	JP 2011-113571 A (韓國電子通信研究院) 2011.06.09, 段落【0009】-【0017】, 【0044】-【0050】, 第7-9図 & US 2011/0131252 A1 & KR 10-2011-0059295 A	1-21
A	WO 2012/073686 A1 (独立行政法人科学技術振興機構) 2012.06.07, 全文, 全図 & US 2013/0297972 A1 & JP 5280587 B2 & EP 2648104 A1	1-21
A	US 2012/0215912 A1 (John R. HOULIHAN) 2012.08.23, 全文, 全図 (ファミリーなし)	1-21