

(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
2022年7月14日(14.07.2022)



(10) 国際公開番号

WO 2022/149261 A1

(51) 国際特許分類:
G06F 11/34 (2006.01)

(21) 国際出願番号: PCT/JP2021/000481

(22) 国際出願日: 2021年1月8日(08.01.2021)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

(72) 発明者: 酒井 優(SAKAI Masaru); 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT 知的財産センタ内 Tokyo (JP). 高橋 謙

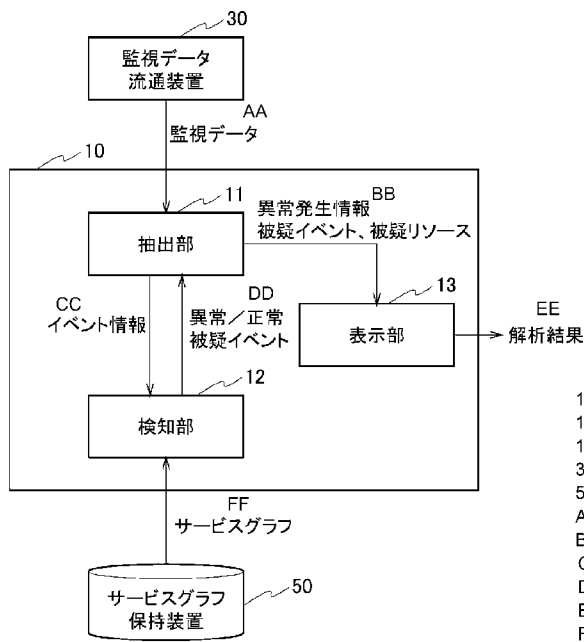
輔 (TAKAHASHI Kensuke); 〒1808585 東京都武蔵野市緑町3丁目9-11 NTT 知的財産センタ内 Tokyo (JP).

(74) 代理人: 三好 秀和, 外 (MIYOSHI Hidekazu et al.); 〒1050001 東京都港区虎ノ門1丁目2番8号 虎ノ門琴平タワー 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) Title: ANALYSIS DEVICE, ANALYSIS METHOD, AND PROGRAM

(54) 発明の名称: 解析装置、解析方法、およびプログラム



11 Extraction unit
12 Detecting unit
13 Display unit
30 Monitoring data distribution device
50 Service graph retention device
AA Monitoring data
BB Abnormal occurrence information, suspected event, suspected resource
CC Event information
DD Abnormal/normal, suspected event
EE Analysis result
FF Service graph

(57) Abstract: This invention is a service graph analysis device 10 for detecting abnormality of a service to be monitored 100 that implements a specific function through chained operation of a plurality of components. The service graph analysis device 10 is provided with: an extraction unit 11 for generating an ignition train obtained by extracting, and lining up in chronological order, processing start events and processing completion events from monitoring data including information pertaining to a series of processing at the service to be monitored 100; and a detecting unit 12 for determining whether events lined up in the ignition train can ignite in a service graph representative of dependency relationships be-

QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, 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))

tween components constituting the service to be monitored 100, and detecting an abnormality if there exists any event not allowing for ignition.

(57) 要約: 複数のコンポーネントが連鎖的に動作することで特定の機能を実現する監視対象サービス 100 の異常を検知するサービスグラフ解析装置 10 である。サービスグラフ解析装置 10 は、監視対象サービス 100 での一連の処理に関する情報を含む監視データから処理開始イベントと処理終了イベントを抽出して時刻順に並べた発火列を生成する抽出部 11 と、監視対象サービス 100 を構成するコンポーネント間の依存関係を表すサービスグラフにおいて発火列に並ぶイベントが発火可能であるか否かを判定し、発火不可能なイベントが存在する場合に異常を検知する検知部 12 を備える。

明 細 書

発明の名称： 解析装置、解析方法、およびプログラム

技術分野

[0001] 本発明は、解析装置、解析方法、およびプログラムに関する。

背景技術

[0002] 近年、Web、ICTなどのサービスを提供するアプリケーションをコンポーネントとして機能ごとに分割し、コンポーネント同士が通信を行い連鎖的に動作するマイクロサービスアーキテクチャが普及している。マイクロサービスの管理においては、リソースレベルでのメトリクス監視やログ監視だけでなく、アプリケーションレベルでの監視が併用される。例えば、アプリケーションの実行中に発生するイベントのログ、アプリケーションにおけるメトリクス（HTTP要求の数、トランザクション数、要求ごとの待機時間など）を集計し監視することで、複雑なマイクロサービスにおける異常検知や根本原因の解析に役立てることができる。

[0003] また、アプリケーションレベルでの監視技術の例として、アプリケーションへの1つのリクエストに対するコンポーネントの動きを可視化する技術が提案されている。このような技術はトレーシングと称される。非特許文献1、2は、アプリケーション自体には手を加えずに動作履歴データを取得するブラックボックススペースのトレーシングソフトウェアである。非特許文献3、4は、アプリケーションに対して手を加えて動作履歴データを取得するアノテーションベースのトレーシングソフトウェアである。マイクロサービスの様々な動きを一連の流れ可視化して保守者もしくは開発者に示すことで、普段と異なる動きの発見および異常の根本原因の発見に役立てることができる。

先行技術文献

非特許文献

[0004] 非特許文献1：B. Sang, J. Zhan, G. Lu et al., “Precise , Scalable , a

nd Online Request Tracing for Multitier Services of Black Boxes” , IE EE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp.1159-1167, 2012.

非特許文献2 : X. Zhao, Y. Zhang, D. Lion et al., “lprof : A Non-intrusive Request Flow Profiler for Distributed Systems” , 11th USENIX Symposium on Operating Systems Design and Implementation (OSDI ’ 14) , p p.629-644, 2014.

非特許文献3 : B. H. Sigelman, L. A. Barroso, M. Burrows, P. Stephenson, M. Plakal, D. Beaver, S. Jaspan, and C. Shanbhag. “Dapper, a large-scale distributed systems tracing infrastructure” , Technical report, Google, Inc., 2010.

非特許文献4 : “Jaeger: open source, end-to-end distributed tracing” , [online], インターネット < URL : <https://www.jaegertracing.io/> >

発明の概要

発明が解決しようとする課題

- [0005] アプリケーションレベルでの監視データはアプリケーションが使用されるごとに無数に蓄積されていくため、リアルタイムに1つ1つのデータを人が確認していくことは現実的ではない。
- [0006] そこで、発明者らは、「複数連携サービスのトレースデータに基づくサービスグラフ構築手法の提案」（信学技報, vol. 119, no. 438）において、コンポーネント間の依存関係を推定し、ペトリネットによってサービス全体のコンポーネント間の依存関係を表すサービスグラフを構築する手法を提案した。これにより、監視データを利用して、コンポーネント間の依存関係を表すサービスグラフを構築することができる。
- [0007] 構築したサービスグラフに従わない監視データを検知することで異常挙動を検知できるが、人手により無数の監視データを一つ一つ確認して異常を検知することは不可能である。
- [0008] 本発明は、上記に鑑みてなされたものであり、異常な監視データを抽出す

ることを目的とする。

課題を解決するための手段

[0009] 本発明の一態様の解析装置は、複数のコンポーネントが連鎖的に動作することで特定の機能を実現するサービスの異常を検知する解析装置であって、前記サービスでの一連の処理に関する情報を含む監視データから処理開始イベントと処理終了イベントを抽出して時刻順に並べた発火列を生成する抽出部と、前記サービスを構成するコンポーネント間の依存関係を表すサービスグラフにおいて前記発火列に並ぶイベントが発火可能であるか否かを判定し、発火不可能なイベントが存在する場合に異常を検知する検知部を備える。

発明の効果

[0010] 本発明によれば、異常な監視データを抽出することができる。

図面の簡単な説明

[0011] [図1]図1は、本実施形態のサービスグラフ解析装置を含む保守管理システムの全体構成の一例を示す図である。

[図2]図2は、サービスグラフ解析装置の構成の一例を示す機能ブロック図である。

[図3]図3は、トレースデータの一例を示す図である。

[図4]図4は、コンポーネントをペトリネットで表現した図である。

[図5]図5は、コンポーネント間の親子関係をペトリネットで表現した図である。

[図6]図6は、コンポーネント間の順序関係をペトリネットで表現した図である。

[図7]図7は、コンポーネント間の排他関係をペトリネットで表現した図である。

[図8]図8は、サービスグラフの一例を示す図である。

[図9]図9は、保守管理システムの処理の流れの一例を示すシーケンス図である。

[図10]図10は、サービスグラフ解析装置の処理の流れの一例を示すフロー

チャートである。

[図11]図 1 1 は、サービスグラフ解析装置の処理の流れの一例を示すフローチャートである。

[図12]図 1 2 は、サービスグラフ上で被疑イベントを示した図である。

[図13]図 1 3 は、サービスグラフ解析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

[0012] 以下、本発明の実施の形態について図面を用いて説明する。

[0013] 図 1 を参照して、本実施形態のサービスグラフ解析装置 1 0 を含む保守管理システムの全体構成について説明する。図 1 の保守管理システムは、サービスグラフ解析装置 1 0、サービス監視装置 2 0、監視データ流通装置 3 0、サービスグラフ生成装置 4 0、サービスグラフ保持装置 5 0、および制御装置 6 0 を備える。

[0014] 監視対象サービス 1 0 0 は、複数のコンポーネントを含み、複数のコンポーネントが連鎖的に動作することで特定の機能を実現する。コンポーネントは、他のコンポーネントとの間でリクエストとレスポンスの送受信を行うことができるインタフェースを持ち、各種のプログラム言語で実装されるプログラムである。

[0015] サービス監視装置 2 0 は、アプリケーションレベルで監視対象サービス 1 0 0 を監視する装置であり、1 つのリクエストに対するコンポーネントの動きを可視化する。サービス監視装置 2 0 には、非特許文献 1 ないし 4 の技術を用いることができる。例えば、サービス監視装置 2 0 は、監視対象サービス 1 0 0 の各コンポーネントにおける処理をスパンという形式で記録し、1 つのリクエストに対する監視対象サービス 1 0 0 の動作の一連の流れをトレースデータ（以下、監視データともいう）として可視化する。監視対象サービス 1 0 0 の各コンポーネントには、ラベル運搬用のコードを埋め込んでおき、スパンを取得できるようにしておく。サービス監視装置 2 0 は、可視化したトレースデータを保守者に対して表示する。保守者は、監視対象サービ

ス１００のアプリケーションレベルでの挙動を可視化されたトレースデータで確認できる。

[0016] 監視データ流通装置３０は、サービス監視装置２０から監視データを受信し、保守管理システムの動作フェーズに応じて、監視データをサービスグラフ生成装置４０へ流通したり、サービスグラフ解析装置１０へ流通したりする。具体的には、監視データ流通装置３０は、学習フェーズのときは、監視データをサービスグラフ生成装置４０へ流通し、検知フェーズのときは、監視データをサービスグラフ解析装置１０へ流通する。学習フェーズでは、サービスグラフ生成装置４０による監視データに基づくサービスグラフの更新が行われる。検知フェーズでは、サービスグラフ解析装置１０によるサービスグラフにおける監視データのチェックが行われる。サービスグラフとは、監視対象サービス１００を構成するコンポーネント間の依存関係を表したグラフ構造である。サービスグラフを利用して監視対象サービス１００の動作の一連の流れの状態遷移を表現できる。監視データ流通装置３０は、制御装置６０からの指示に基づいて監視データの流通先を切り替える。

[0017] サービスグラフ生成装置４０は、学習フェーズのときに監視データを受信し、監視データからコンポーネント間の依存関係を推定し、推定した依存関係を元にサービスグラフを更新し、サービスグラフ保持装置５０にサービスグラフを格納する。

[0018] サービスグラフ保持装置５０は、サービスグラフを保持する。サービスグラフ保持装置５０の保持するサービスグラフは、保守者に対して表示されたり、サービスグラフ解析装置１０が監視データの解析のために用いられったりする。検知フェーズのときは、サービスグラフ保持装置５０の保持するサービスグラフには正常ラベルが付与され、学習フェーズのときは、サービスグラフから正常ラベルが削除される。正常ラベルの付与されたサービスグラフは、グラフの更新が収束し、確定した正常モデルである。

[0019] 開発者は、開発環境１１０で開発作業を行い、監視対象サービス１００をアップデートする。開発環境１１０は、監視対象サービス１００をアップデ

ートした際、アップデートタイミング通知を制御装置 60 へ通知する。

[0020] 制御装置 60 は、開発環境 110 からのアップデート情報の受信とサービスグラフの収束判断に基づいて学習フェーズと検知フェーズの切り替えを行う。具体的には、制御装置 60 は、検知フェーズ中に開発環境 110 から監視対象サービス 100 のアップデートがあった旨の通知を受け取ると学習フェーズに移行し、監視データの流通先をサービスグラフ生成装置 40 に切り替える指示を出す。制御装置 60 は、学習フェーズ中にサービスグラフ保持装置 50 の保持するサービスグラフの更新の収束を判断し、サービスグラフの更新が収束したと判断すると検知フェーズに移行し、監視データの流通先をサービスグラフ解析装置 10 に切り替える指示を出す。

[0021] サービスグラフ解析装置 10 は、検知フェーズのときに監視データを受信し、サービスグラフにおいて監視データの状態遷移の実行可能性をチェックすることで異常挙動であるか否かを判断する。異常挙動を検知した場合、サービスグラフ解析装置 10 は解析結果を保守者に提示する。

[0022] 図 2 を参照し、サービスグラフ解析装置 10 の構成について説明する。同図に示すサービスグラフ解析装置 10 は、抽出部 11、検知部 12、および表示部 13 を備える。

[0023] 抽出部 11 は、監視データから処理開始と処理終了のイベントを全て抽出し、抽出したイベントを時刻順にソートしてチェック対象となる発火列を作成する。

[0024] 抽出部 11 は、検知部 12 から異常を検知した被疑イベントを受信した場合に、監視データから被疑イベントが使用しているリソースを被疑リソースとして列挙する。

[0025] 検知部 12 は、サービスグラフ保持装置 50 の保持するサービスグラフにおいて監視データから作成した発火列の各イベントが発火可能であるか否かをチェックし、発火列に発火不可能なイベントが存在する場合は異常挙動と判断し、失敗原因状態を作り出した被疑イベントを抽出する。

[0026] 表示部 13 は、検知部 12 が異常挙動を検知した際、被疑イベントと被疑

リソースを可視化した解析結果を保守者へ提示する。

[0027] 次に、トレースデータ（監視データ）から生成するサービスグラフについて説明する。サービスグラフ解析装置 10 は、このサービスグラフを用いて監視データから生成した発火列をチェックする。

[0028] トレースデータは、監視対象サービス 100 に対するリクエストからレスポンスまでの一連の処理を構成するスパンの集合である。例えば、監視対象サービス 100 に対するエンドユーザの 1 回のリクエストからレスポンスまでの 1 つのトレースデータが得られる。スパンとは、各コンポーネントの処理の時刻データと親子関係を記録したデータである。図 3 に可視化したトレースデータの一例を示す。図 3 では、横軸に時間を取り、コンポーネントの処理期間を矩形の幅で表現している。A から E の文字を付与した 5 つの矩形のそれぞれが各コンポーネントのスパンを示す。矢印は、コンポーネント間のリクエストとレスポンスの送受信を示している。スパンは、例えば、コンポーネントの名前（Name）、トレース ID（Trace ID）、処理開始時間（Start Time）、処理時間（Duration）、および関係（Reference）の情報を含む。

[0029] 図 4 ないし図 7 を参照し、コンポーネントの依存関係に基づいてサービスグラフを表現する方法について説明する。

[0030] サービスグラフ生成装置 40 は、トレースデータの各スパンの時間情報からコンポーネント間の依存関係を推定し、推定した依存関係を元に、監視対象サービス 100 全体のコンポーネントレベルでのサービスグラフをペトリネットで表現する。ペトリネットは、プレースとトランジションという 2 種類のノードを持ち、プレースとトランジションがアークで接続される 2 部有向グラフである。プレースにトークンという変数が与えられる。各プレースが持つトークン数でペトリネット全体の状態を表したものをマーキングと呼ぶ。特にペトリネットの初期状態におけるマーキングを初期マーキングと呼ぶ。トランジションは、発火によって、自身の前に存在する全てのプレースのトークンを、自身の後に存在する全てのプレースに移す。トランジション

の発火によってペトリネットは初期マーキングから次のマーキングへと遷移していく。

[0031] 本実施形態では、1つのコンポーネントのペトリネットを図4に示すように定義する。具体的には、コンポーネントがとりうる状態を「未処理」、「処理中」、および「処理済」の3種類とし、この3種類の状態をプレースに対応付ける。プレース間に設けたトランジションの発火（処理開始または処理終了）によってトークンを移動させることで、コンポーネントの状態遷移を表現する。図4の未処理のプレースに配置された黒丸がトークンである。図4に示すコンポーネントが処理を開始すると、トークンは処理中のプレースに移される。

[0032] コンポーネント間の依存関係は、図4に示したコンポーネントのペトリネットに対してアークおよびプレースを追加することで表現できる。具体的には、図5ないし図7に示すように、コンポーネント間の親子関係、順序関係、および排他関係を表現する。親子関係とは、一方のコンポーネントが他方のコンポーネントを呼び出す関係である。順序関係とは、一方のコンポーネントが必ず他方のコンポーネントの処理後に実行される関係である。排他関係とは、並行して処理を実行することがないコンポーネント間の関係である。

[0033] コンポーネントA、B間の親子関係は図5のように表現できる。親のコンポーネントAの処理開始のトランジションから子のコンポーネントBの未処理のプレースにアークを配置し、子のコンポーネントBの処理済のプレースから親のコンポーネントAの処理終了のトランジションにアークを配置する。これにより、コンポーネントAの処理開始後、コンポーネントBの処理が開始し、コンポーネントBの処理終了後、コンポーネントBは処理済の状態となり、その後コンポーネントAの処理が終了することを表現できる。

[0034] コンポーネントA、B間の順序関係は図6のように表現できる。コンポーネントAの処理終了のトランジションから新たにアークとプレースを配置し、新たなプレースからコンポーネントBの処理開始のトランジションにアークを配置する。

クを配置する。これにより、コンポーネント A の処理終了後にコンポーネント B の処理が開始することを表現できる。

[0035] コンポーネント A, B 間の排他関係は図 7 のように表現できる。コンポーネント A およびコンポーネント B が両方とも処理中ではない状態を示す新たなプレースを配置し、新たなプレースにはトークンを配置しておく。コンポーネント A, B の処理終了のトランジションのそれぞれから新たなプレースにアークを配置し、新たなプレースからコンポーネント A, B の処理開始のトランジションのそれぞれにアークを配置する。これにより、コンポーネント B またはコンポーネント C の処理終了後にコンポーネント C またはコンポーネント B の処理が開始することを表現できる。

[0036] 図 8 に、監視対象サービス 100 のサービスグラフの一例を示す。図 8 のサービスグラフでは、監視対象サービス 100 を構成する全てのコンポーネントとコンポーネント間の依存関係が表現されている。監視データがサービスグラフ生成装置 40 に流通しているとき、サービスグラフ生成装置 40 は、監視データに含まれるトレースデータのそれぞれについて、兄弟コンポーネントのスパン間の時刻データを比較してコンポーネント間の順序関係または排他関係を推定してサービスグラフを更新する。サービスグラフ生成装置 40 は、新たに発見されたコンポーネント間の依存関係については、上記の方法で依存関係を表すグラフを追加し、消失した依存関係については、依存関係を表す部分のグラフを削除する。

[0037] サービスグラフ解析装置 10 は、トレースデータから処理開始と処理終了のイベントを抽出して発火列を作成し、サービスグラフの初期マーキングを設定し、発火列のイベントを順に発火可能であるか否かチェックする。発火不可能なイベントが存在する場合は異常挙動である。

[0038] 次に、図 9 のシーケンス図を参照し、保守管理システムの処理の流れについて説明する。

[0039] ステップ S 1 にて、抽出部 11 は、監視データ流通装置 30 から監視データを受信すると、ステップ S 2 にて、監視データから処理開始と処理終了の

イベントを抽出して時刻順にソートした発火列を作成し、検知部 12 へ送信する。

[0040] ステップ S 3 にて、検知部 12 は、サービスグラフ保持装置 50 からサービスグラフを取得し、ステップ S 4 にて、発火列に従ってサービスグラフを初期マーキングから順に遷移させて異常を検知する。

[0041] ステップ S 5 にて、検知部 12 は、発火列のチェック結果を抽出部 11 へ送信する。検知部 12 は、異常を検知した場合は被疑イベントを抽出部 11 へ通知する。

[0042] 検知部 12 が異常を検知した場合、ステップ S 6 にて、抽出部 11 は、監視データから被疑イベントに対応する被疑リソースを抽出し、被疑イベントと被疑リソースを含む異常発生情報を表示部 13 へ送信する。

[0043] ステップ S 7 にて、表示部 13 は、被疑イベントと被疑リソースを含む解析結果を保守者に提示する。

[0044] なお、検知部 12 が異常を検知していない場合は、ステップ S 6, S 7 の処理は実施されない。

[0045] 次に、図 10, 11 のフローチャートを参照し、サービスグラフ解析装置 10 の処理の流れについて説明する。

[0046] 図 10 のフローチャートのステップ S 11 にて、抽出部 11 が監視データを受信すると、ステップ S 12 にて、監視データから処理開始と処理終了のイベントを全て抽出し、時系列順にソートしてチェック対象の発火列を作成する。発火列を作成する際、抽出部 11 は、発火列に含まれるイベント名がサービスグラフのトランジションの名前と一致するように、命名規則を確認してイベント名を適切に加工する。例えば、イベントの「処理名」に処理開始を示す「__start」または処理終了を示す「__end」を追加する。

[0047] ステップ S 13 にて、検知部 12 は、根のスパンの種別を確認してサービスグラフの初期マーキングを設定する。根のスパンとは、一番初めに処理開始されるスパンである。初期マーキングは、例えば、根のスパンに対応するサブグラフにおける未処理のプレースにトークンが 1 つ置かれた状態である

。

- [0048] 発火列の全てのイベントを時刻順に順番に処理し、ステップS 1 4 にて、検知部 1 2 は、処理対象イベントに対応するトランジションをサービスグラフから検索し、該当トランジションの発火可能性をチェックする。トランジションの全ての入力プレースがトークンを持つ場合に処理対象イベントは発火可能である。
- [0049] 処理対象イベントが発火可能の場合、ステップS 1 5 にて、検知部 1 2 は、サービスグラフのマーキングを更新する。
- [0050] 発火列の全てのイベントが発火可能であれば、ステップS 1 6 にて、検知部 1 2 は、監視データの動作は正常と判断し、抽出部 1 1 へ監視データの動作は正常であることを通知する。
- [0051] 発火列に発火不可能のイベントが存在する場合、検知部 1 2 は、監視データの動作を異常と判断し、図 1 1 のフローチャートに処理を進める。
- [0052] 図 1 1 のフローチャートのステップS 2 1 にて、検知部 1 2 は、発火できず遷移に失敗するマーキングを失敗原因状態として抽出し、ステップS 2 2 にて、失敗原因状態に関連するイベントを被疑イベントとして抽出する。失敗原因状態のマーキングにおいてトークンを持つプレースが含まれるスパンは直前まで処理を行っていたスパンであり被疑箇所として挙げられる。例えば、図 1 2 のサービスグラフでは、符号 2 0 0 で示すサブグラフ（スパン）が被疑箇所である。検知部 1 2 は、失敗原因状態においてトークンを保持するプレースの前のトランジションの和集合を求め、和集合に含まれるトランジションと対応するイベントを被疑イベントとして全て列挙する。図 1 2 のサービスグラフでは、トークンを持つプレースの前のトランジションが被疑イベントとして挙げられる。複数のプレースがトークンを持つ場合は複数のイベントが被疑イベントとして列挙されることもあるし、プレースの前に複数のトランジションがある場合は複数のイベントが被疑イベントとして列挙されることもある。
- [0053] ステップS 2 3 にて、抽出部 1 1 は、被疑イベントに対応する監視データ

を参照し、被疑リソースを抽出する。監視データには、処理を実行している仮想マシンのIPアドレスなどのリソース情報が含まれる場合がある。抽出部11は、被疑イベントが使用しているリソースの和集合を被疑リソースとして列挙する。単純なケースであれば、原因イベントの特定および原因リソースの特定に至るが、複数の処理の待ち受けがあり、原因となりうる被疑イベントが多数存在する場合は原因リソースの特定まで至らない場合もある。

[0054] ステップS24にて、表示部13は、被疑イベントおよび被疑リソースを可視化して保守者に提示する。表示部13は、異常と判定した監視データを可視化して保守者に提示してもよい。

[0055] 以上説明したように、本実施形態のサービスグラフ解析装置10は、監視対象サービス100での一連の処理に関する情報を含む監視データから処理開始イベントと処理終了イベントを抽出して時刻順に並べた発火列を生成する抽出部11と、監視対象サービス100を構成するコンポーネント間の依存関係を表すサービスグラフにおいて発火列に並ぶイベントが発火可能であるか否かを判定し、発火不可能なイベントが存在する場合に異常を検知する検知部12を備える。サービスグラフは、コンポーネントの処理前、処理中、および処理後の状態をペトリネットのプレースとして表現し、コンポーネントの処理開始および処理終了をペトリネットのトランジションとして表現し、コンポーネント間の依存関係をコンポーネントのペトリネット間に新たなノードとアークを配置して表現したものである。検知部12は、発火列で発火不可能なイベントが存在するサービスグラフにおいてトークンが配置されたプレースを含むサブグラフに対応するコンポーネントを異常の発生したコンポーネントとして検知する。これにより、サービスグラフを利用して異常な監視データを抽出できる。

[0056] 上記説明したサービスグラフ解析装置10には、例えば、図13に示すような、中央演算処理装置（CPU）901と、メモリ902と、ストレージ903と、通信装置904と、入力装置905と、出力装置906とを備える汎用的なコンピュータシステムを用いることができる。このコンピュータ

システムにおいて、CPU 901がメモリ902上にロードされた所定のプログラムを実行することにより、サービスグラフ解析装置10が実現される。このプログラムは磁気ディスク、光ディスク、半導体メモリ等のコンピュータ読み取り可能な記録媒体に記録することも、ネットワークを介して配信することもできる。

符号の説明

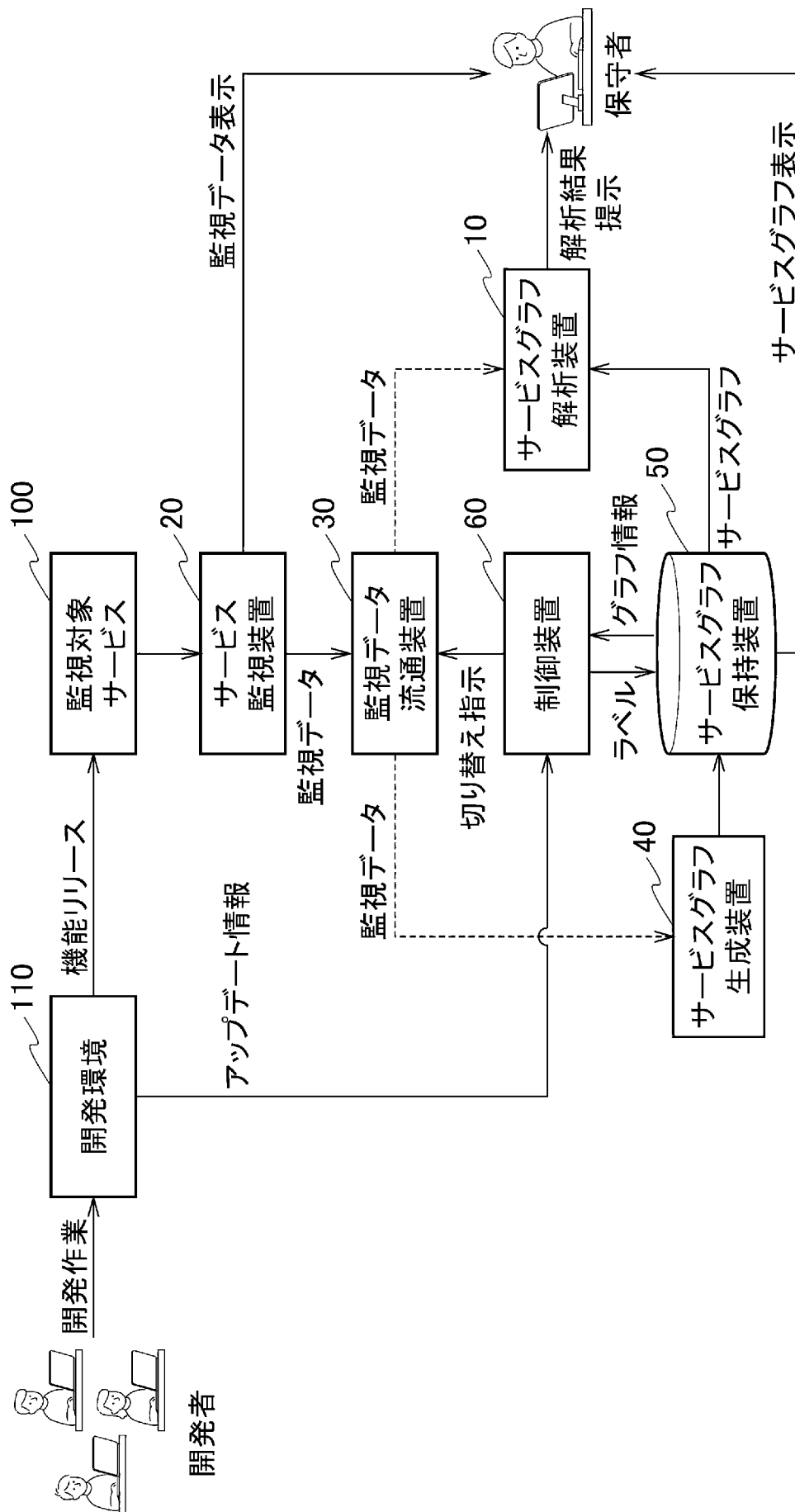
- [0057] 10…サービスグラフ解析装置
 11…抽出部
 12…検知部
 13…表示部
 20…サービス監視装置
 30…監視データ流通装置
 40…サービスグラフ生成装置
 50…サービスグラフ保持装置
 60…制御装置
 100…監視対象サービス
 110…開発環境

請求の範囲

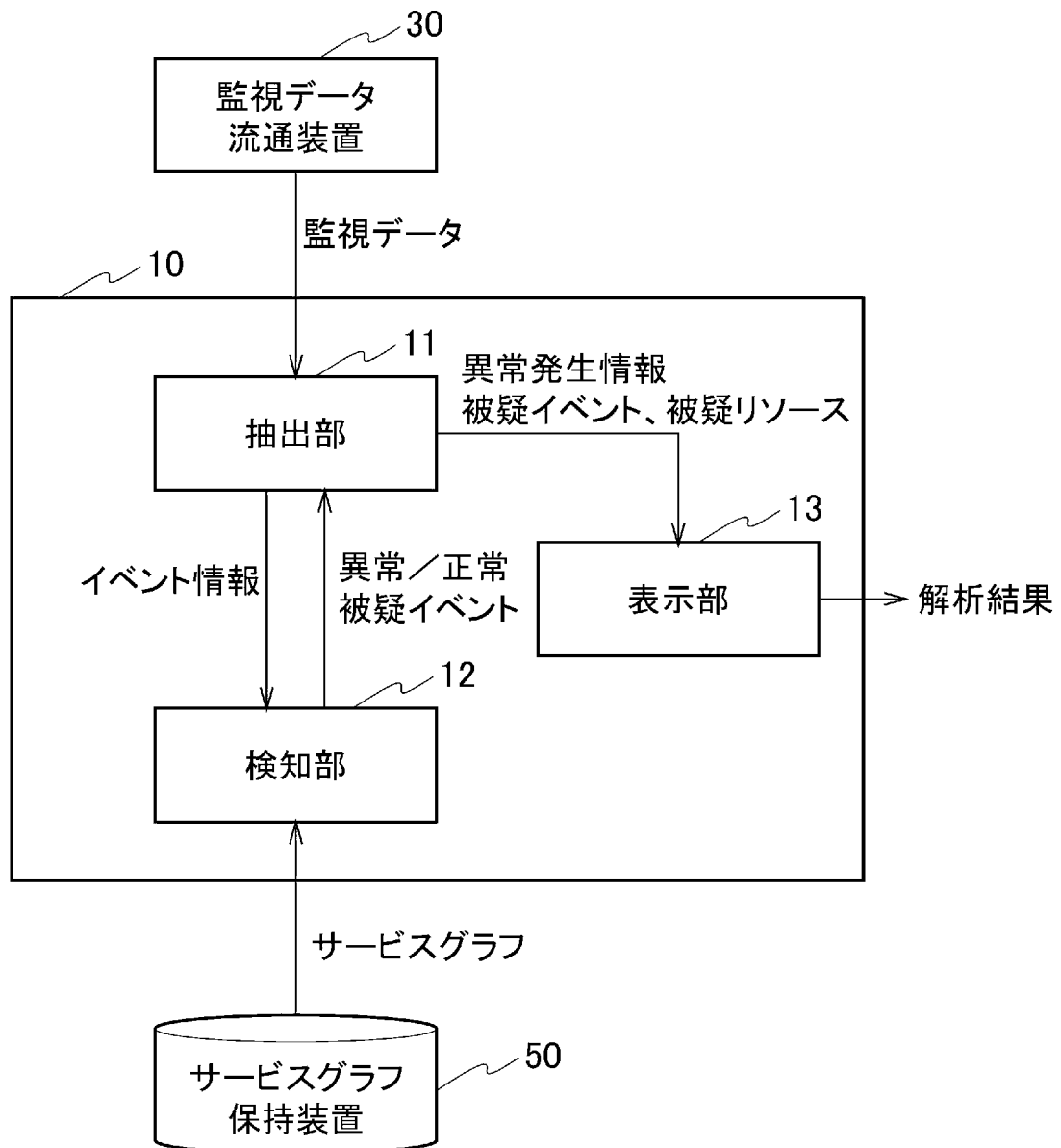
- [請求項1] 複数のコンポーネントが連鎖的に動作することで特定の機能を実現するサービスの異常を検知する解析装置であって、
- 前記サービスでの一連の処理に関する情報を含む監視データから処理開始イベントと処理終了イベントを抽出して時刻順に並べた発火列を生成する抽出部と、
- 前記サービスを構成するコンポーネント間の依存関係を表すサービスグラフにおいて前記発火列に並ぶイベントが発火可能であるか否かを判定し、発火不可能なイベントが存在する場合に異常を検知する検知部を備える
- 解析装置。
- [請求項2] 請求項1に記載の解析装置であって、
- 前記検知部は、発火不可能なイベントが存在するサービスグラフの状態から異常の発生した被疑イベントを抽出し、
- 前記抽出部は、前記異常の発生した被疑イベントに基づいて異常の発生したリソースを抽出する
- 解析装置。
- [請求項3] 請求項1または2に記載の解析装置であって、
- 前記サービスグラフは、前記コンポーネントの処理前、処理中、および処理後の状態をペトリネットのプレースとして表現し、前記コンポーネントの処理開始および処理終了をペトリネットのトランジションとして表現し、前記コンポーネント間の依存関係を前記コンポーネントのペトリネット間に新たなノードとアークを配置して表現したものであり、
- 前記検知部は、前記発火列で発火不可能なイベントが存在するサービスグラフにおいてトークンが配置されたプレースの前のトランジションを異常の発生した被疑イベントとして検知する
- 解析装置。

- [請求項4] 複数のコンポーネントが連鎖的に動作することで特定の機能を実現するサービスの異常を検知する解析装置による解析方法であって、
- 前記サービスでの一連の処理に関する情報を含む監視データから処理開始イベントと処理終了イベントを抽出して時刻順に並べた発火列を生成するステップと、
- 前記サービスを構成するコンポーネント間の依存関係を表すサービスグラフにおいて前記発火列に並ぶイベントが発火可能であるか否かを判定し、発火不可能なイベントが存在する場合に異常を検知するステップを有する
- 解析方法。
- [請求項5] 請求項1ないし3のいずれかに記載の解析装置の各部としてコンピュータを動作させるプログラム。

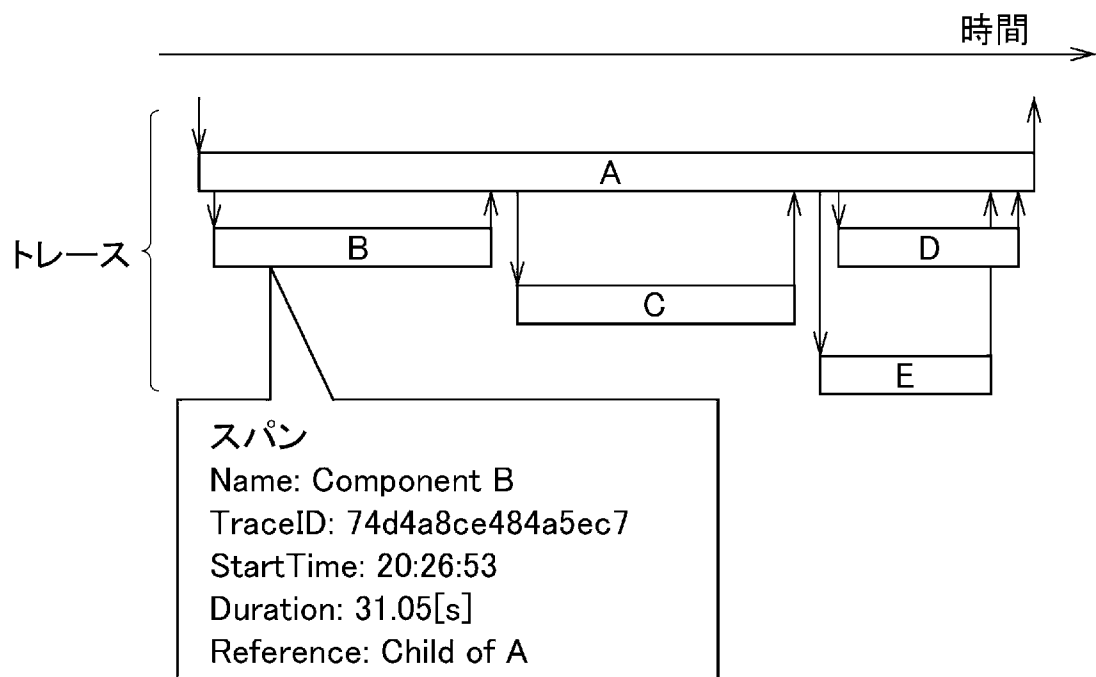
[図1]



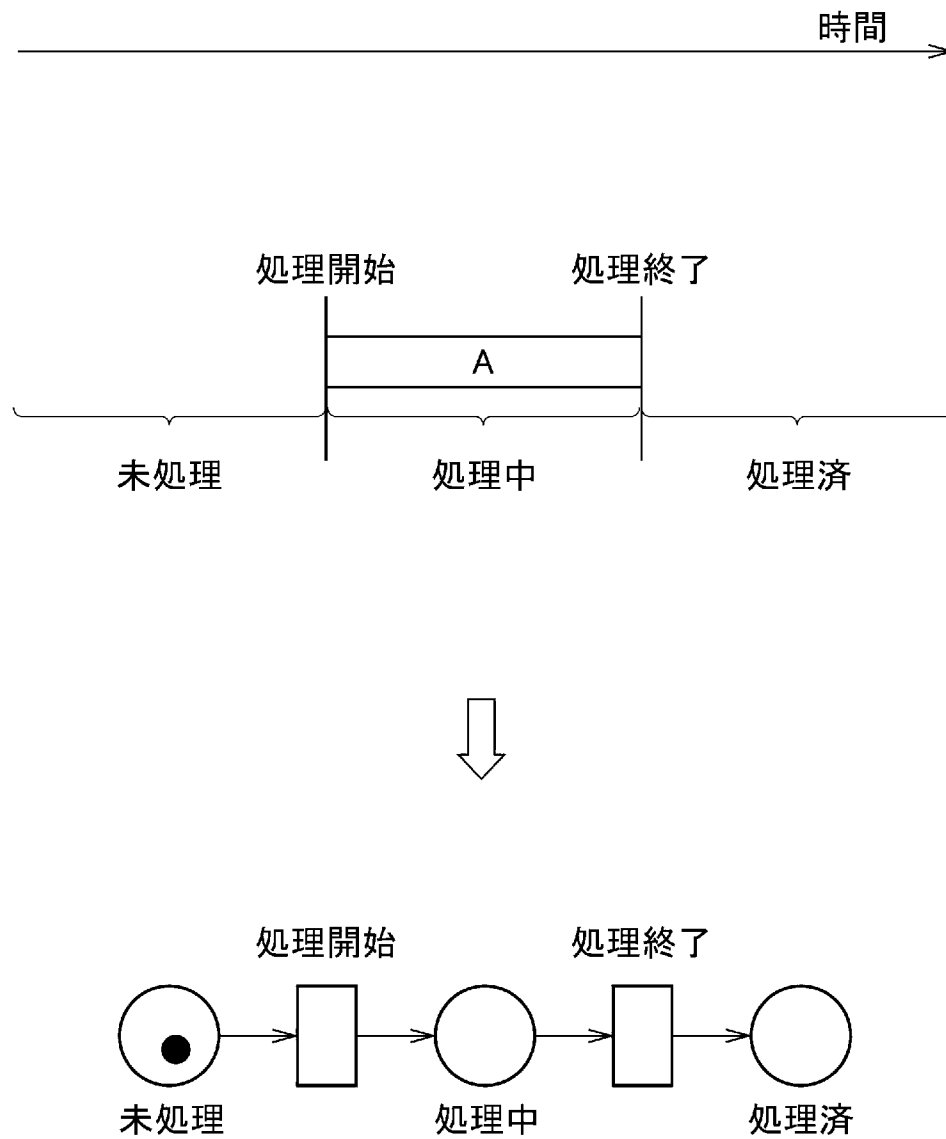
[図2]



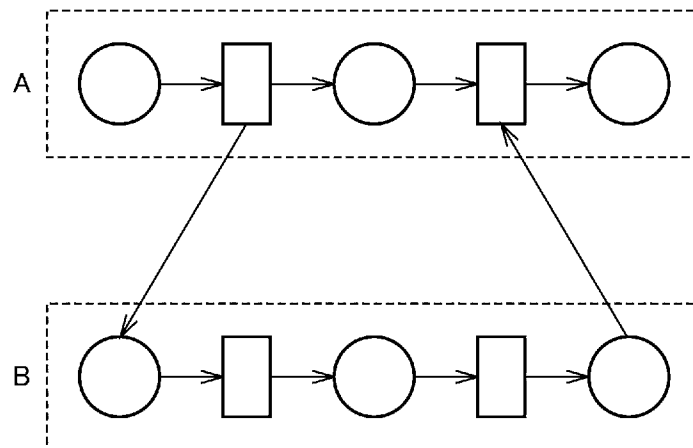
[図3]



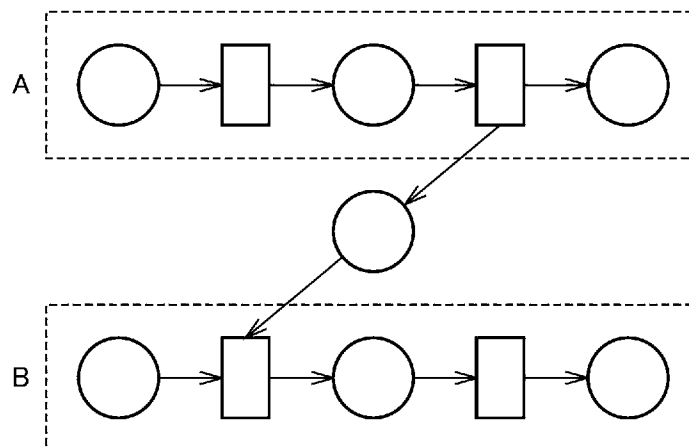
[図4]



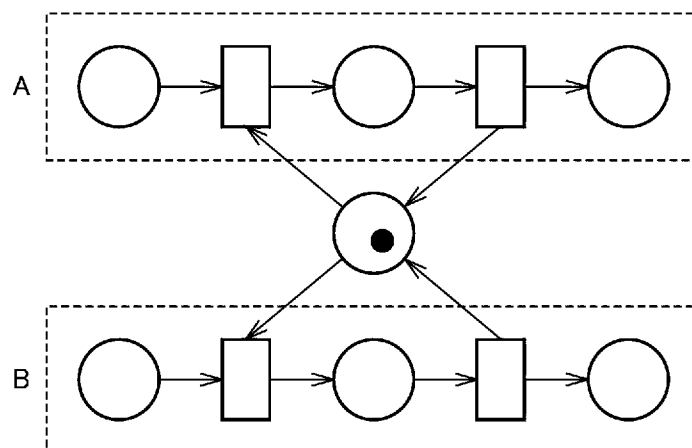
[図5]



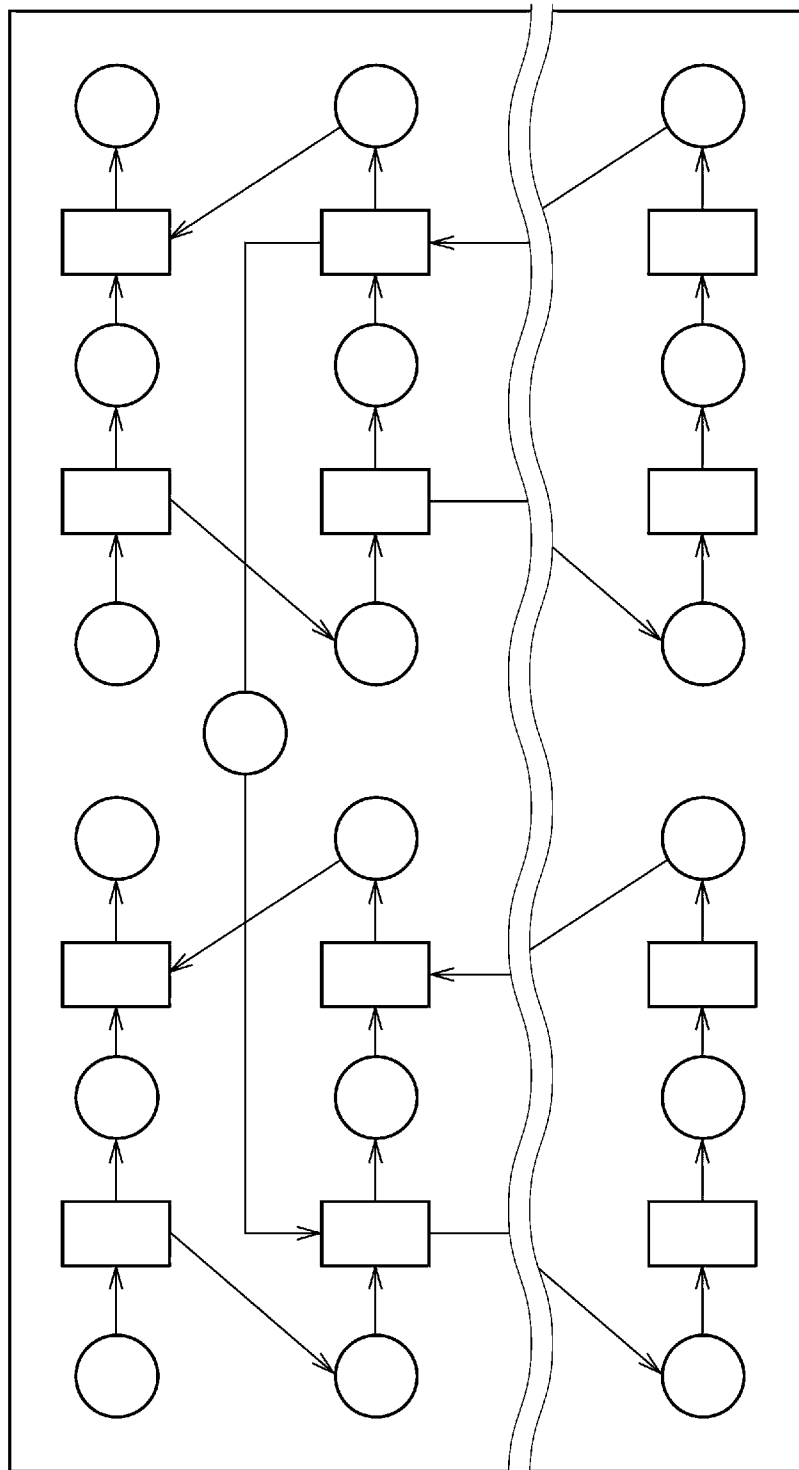
[図6]



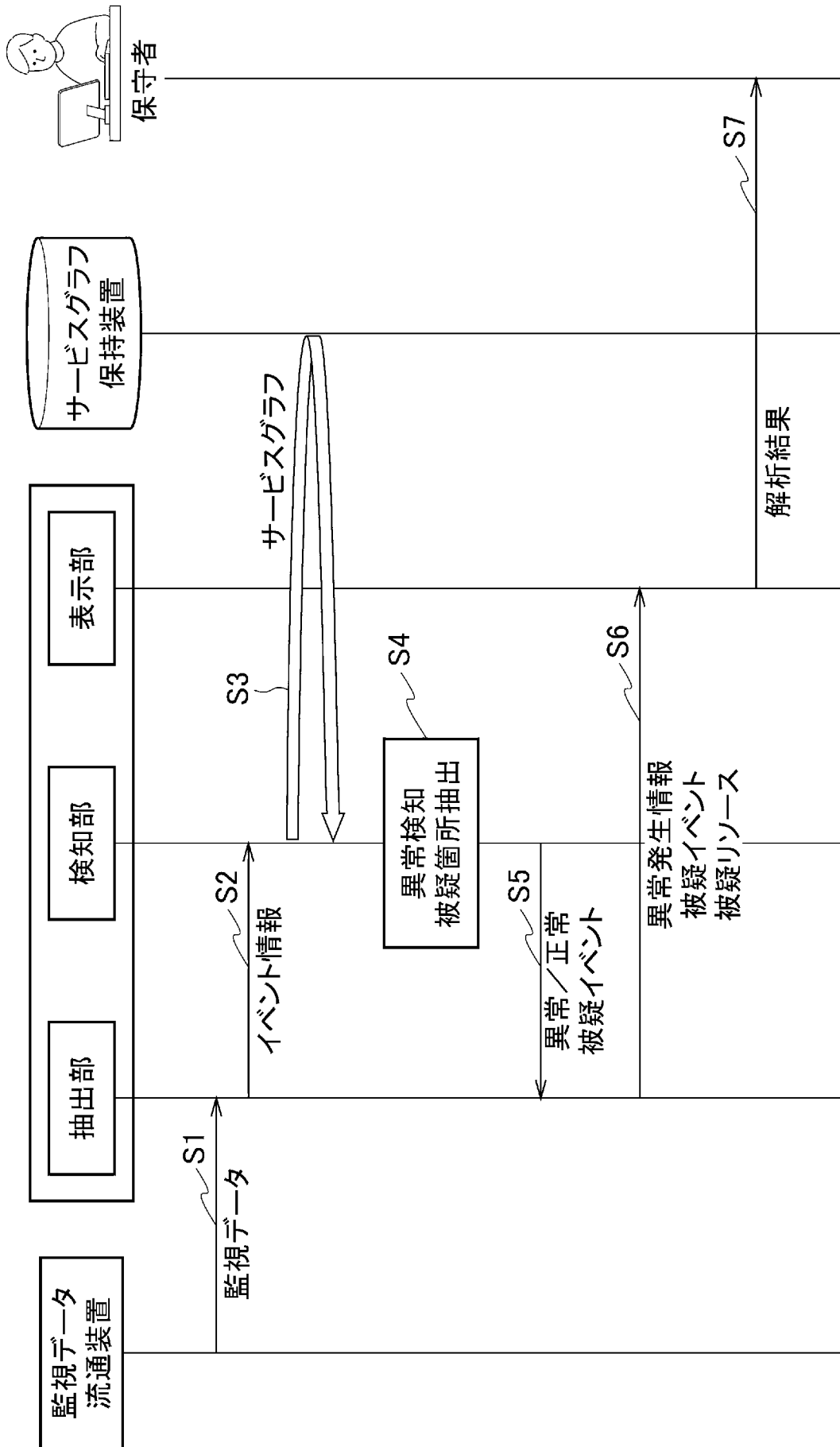
[図7]



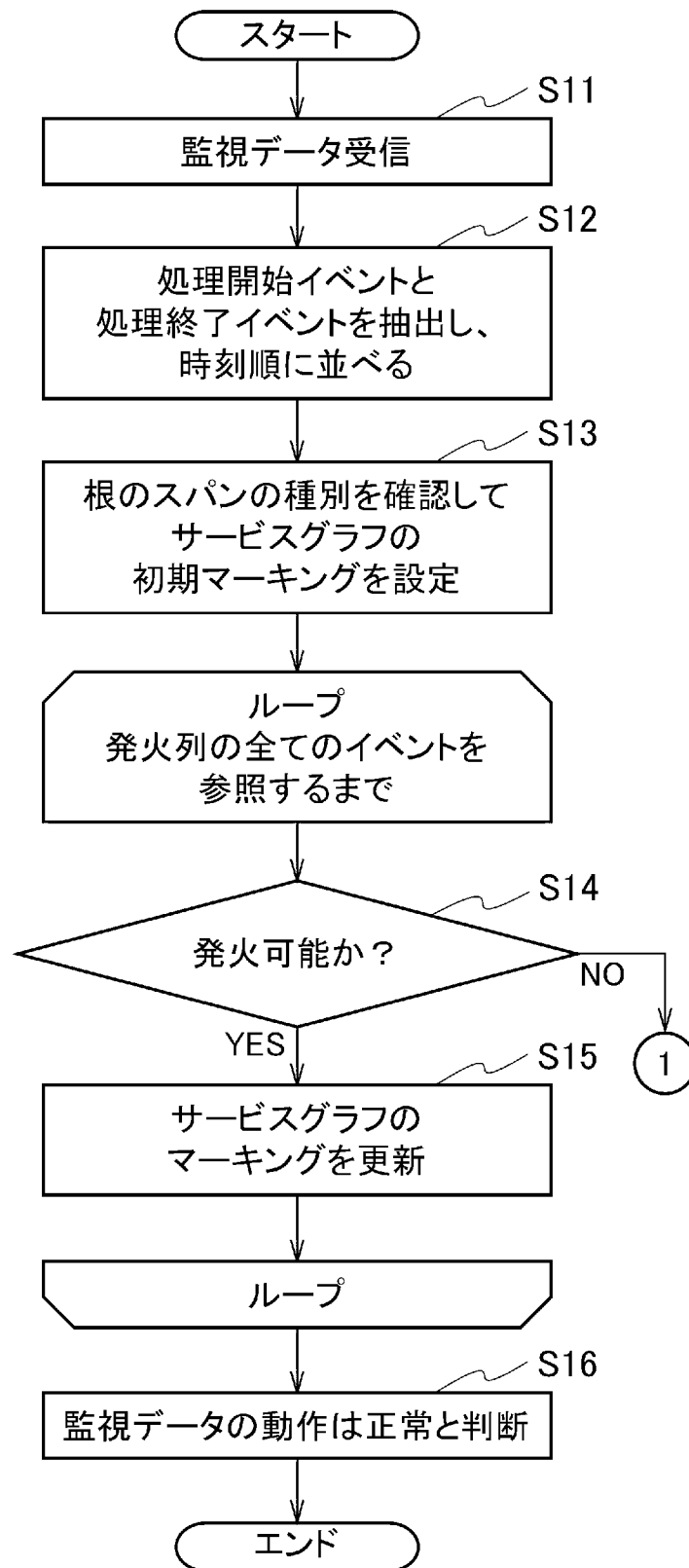
[図8]



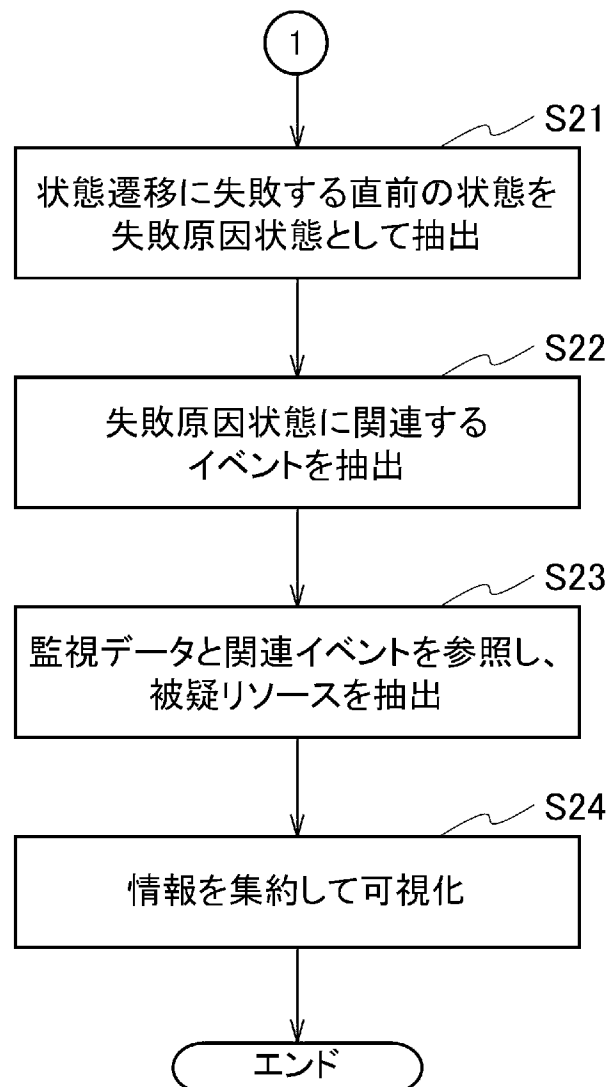
[図9]



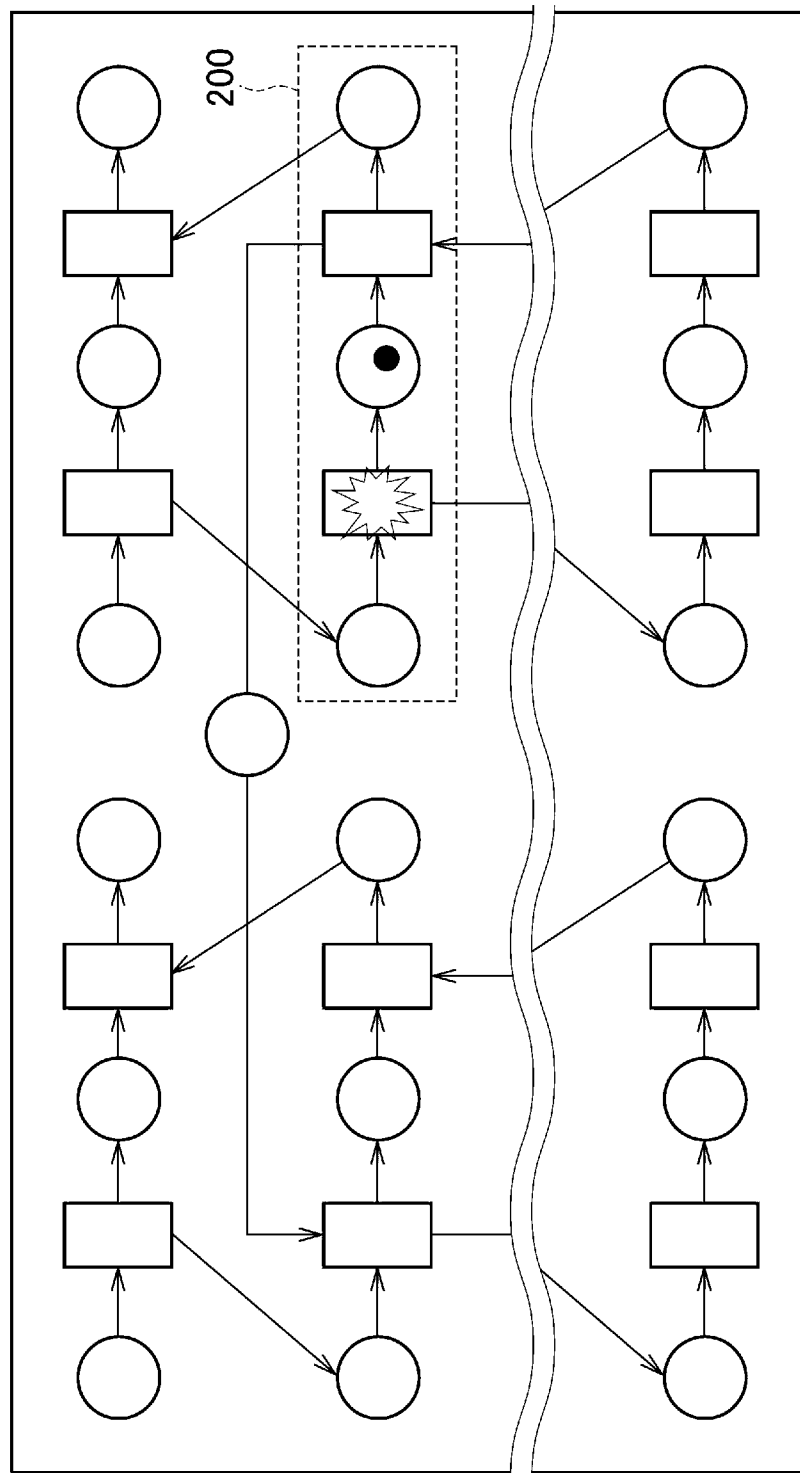
[図10]



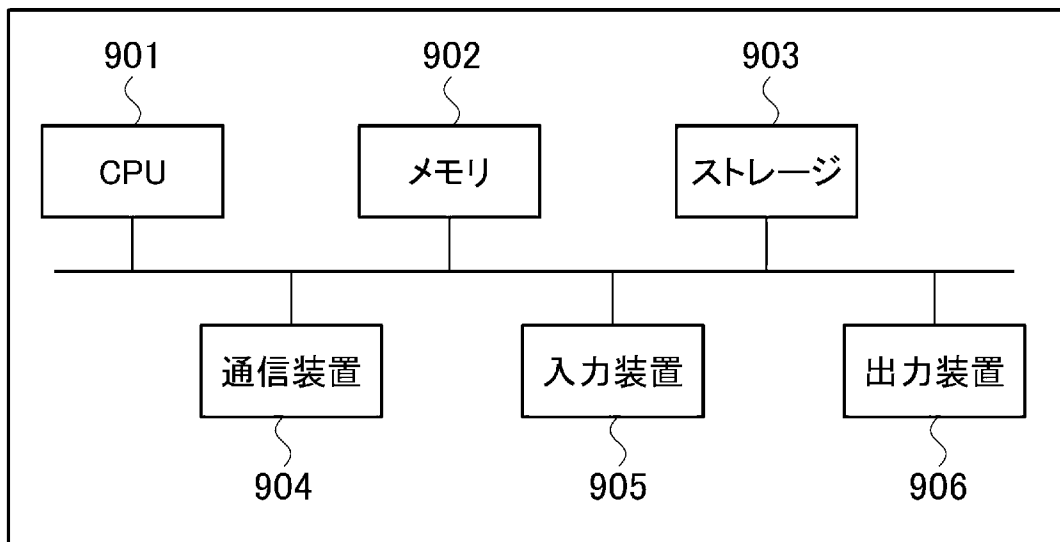
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/000481

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F11/34 (2006.01) i

FI: G06F11/34166

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. G06F11/34

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2021

Registered utility model specifications of Japan 1996-2021

Published registered utility model applications of Japan 1994-2021

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 A	酒井 優, 外 2 名, 複数連携サービスのトレースデータに基づくサービスグラフ構築手法の提案, 電子情報通信学会技術研究報告, 27 April 2020, vol. 119, no. 438, pp. 5-10, particularly, sections 3, 4, (SAKAI, Masaru and 2 others, A service graph construction method based on distributed tracing data of multiple cooperation services, IEICE Technical Report)	1, 4-5 2-3
Y A	平井健治, 外 2 名, 分散制御システムのデバッグ手法, 情報処理学会研究報告, 07 February 1991, vol. 91, no. 13, pp. 51-56, particularly, sections 2, 3, 5, (HIRAI, Kenji and 2 others, Debugging of distributed control system, IPSJ SIG technical reports)	1, 4-5 2-3

☐ Further documents are listed in the continuation of Box C.	☐ See patent family annex.
---	---

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 29 March 2021	Date of mailing of the international search report 06 April 2021
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 11/34(2006.01)i FI: G06F11/34 166		
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）） 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 1971-2021年 日本国実用新案登録公報 1996-2021年 日本国登録実用新案公報 1994-2021年		
国際調査でを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	酒井 優, 外2名, 複数連携サービスのトレースデータに基づくサービスグラフ構築手法の提案, 電子情報通信学会技術研究報告, 2020.04.27, Vol. 119, No. 438, pp. 5-10 特に, Section 3-4	1, 4-5
A		2-3
Y	平井健治, 外2名, 分散制御システムのデバッグ手法, 情報処理学会研究報告, 1991.02.07, Vol. 91, No. 13, pp. 51-56 特に, Section 2, 3, 5	1, 4-5
A		2-3
☐ 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抵触するものではなく、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 29.03.2021		国際調査報告の発送日 06.04.2021
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 大桃 由紀雄 5B 5583 電話番号 03-3581-1101 内線 3545