

(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
2021年9月23日(23.09.2021)



(10) 国際公開番号

WO 2021/186683 A1

(51) 国際特許分類:
G06F 21/57 (2013.01)

(21) 国際出願番号: PCT/JP2020/012365

(22) 国際出願日: 2020年3月19日(19.03.2020)

(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: 三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

(72) 発明者: 跡部 悠太(ATOBE, Yuta); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井 国際特許業務法人(MIZOI INTERNATIONAL PATENT FIRM); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

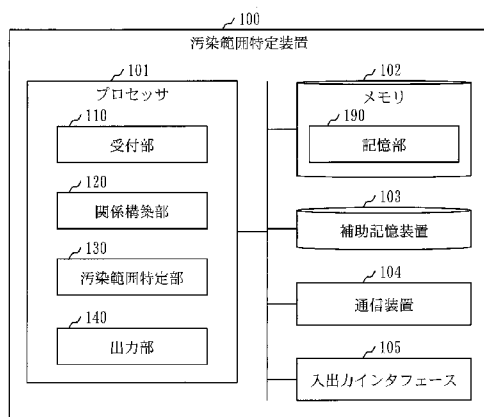
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, 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,

(54) **Title:** CONTAMINATION RANGE SPECIFYING DEVICE AND CONTAMINATION RANGE SPECIFYING PROGRAM

(54) 発明の名称: 汚染範囲特定装置および汚染範囲特定プログラム

図1



- 100 Contamination range specifying device
- 101 Processor
- 102 Memory
- 103 Auxiliary storage device
- 104 Communication device
- 105 Input/output interface
- 110 Acceptance unit
- 120 Relationship construction unit
- 130 Contamination range specifying unit
- 140 Output unit
- 190 Storage unit

(57) **Abstract:** A relationship construction unit (120) generates, on the basis of a plurality of software operation data, each of which includes the operation type of a software operation and operation object information that indicates a plurality of software objects used in the software operation, object relationship data that indicates the relationship between the plurality of software objects. A contamination range specifying unit (130) generates, on the basis of the object relationship data and alert data for issuing notification of the occurrence of a cyber attack, contamination range data that indicates a contamination range affected by the cyber attack.

(57) 要約: 関係構築部(120)は、ソフトウェア動作の動作タイプと前記ソフトウェア動作で使用された複数のソフトウェアオブジェクトを示す動作オブジェクト情報とをそれぞれが含む複数のソフトウェア動作データに基づいて、前記複数のソフトウェアオブジェクトの関係を示すオブジェクト関係データを生成する。汚染範囲特定部(130)は、前記オブジェクト関係データと、サイバー攻撃の発生を知らせるアラートデータと、に基づいて、サイバー攻撃の影響を受ける汚染範囲を示す汚染範囲データを生成する。

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：

一 国際調査報告（条約第21条(3)）

明 細 書

発明の名称： 汚染範囲特定装置および汚染範囲特定プログラム
技術分野

[0001] 本開示は、サイバー攻撃による汚染の再発防止に関するものである。

背景技術

[0002] サイバー攻撃に対して次のような対処がされる。

まず、監視対象に対するサイバー攻撃が検知される。

次に、サイバー攻撃の影響が判断される。

そして、サイバー攻撃の影響に応じて監視対象の縮退動作が決定される。

例えば、縮退動作において、機能の切替えまたは機能の再配置が行われる。

[0003] また、サイバー攻撃の影響に対して、汚染部分の除去および再発防止の対応を実施する必要がある。

汚染部分の除去は、汚染部分の削除、復元または初期化などを意味する。

汚染部分は、サイバー攻撃によって改変された部分である。例えば、汚染部分は、改変されたコードおよび改変されたデータである。汚染部分の除去のためには、汚染部分を特定する必要がある。

再発防止の対応は、汚染部分を除去しただけではサイバー攻撃を再び受ける恐れがあるため、実施する必要がある。再発防止の具体的な対応は、サイバー攻撃の侵入経路を遮断することである。サイバー攻撃の侵入経路を遮断するためにはサイバー攻撃の侵入経路を特定する必要がある。

[0004] 特許文献1は、車載システムにおいてセキュリティ攻撃に起因する異常が発生した場合であっても自動車の走行制御を安全な状態に保つための技術を開示している。

先行技術文献

特許文献

[0005] 特許文献1：特開2018-194909号公報

発明の概要

発明が解決しようとする課題

[0006] 特許文献 1 には、異常内容および異常個所に基づいて縮退動作を一意に決定することが開示されている。しかし、汚染部分の除去および再発防止の対応を実施するための方法は開示されていない。特に、侵入経路を特定する方法および汚染部分を特定する方法は開示されていない。

[0007] 本開示は、侵入経路および汚染部分を特定できるようにすることを目的とする。

課題を解決するための手段

[0008] 本開示の汚染範囲特定装置は、

ソフトウェア動作の動作タイプと前記ソフトウェア動作で使用された複数のソフトウェアオブジェクトを示す動作オブジェクト情報とをそれぞれが含む複数のソフトウェア動作データに基づいて、前記複数のソフトウェアオブジェクトの関係を示すオブジェクト関係データを生成する関係構築部と、

前記オブジェクト関係データと、サイバー攻撃の発生を知らせるアラートデータと、に基づいて、サイバー攻撃の影響を受ける汚染範囲を示す汚染範囲データを生成する汚染範囲特定部と、を備える。

発明の効果

[0009] 本開示によれば、侵入経路および汚染部分といった汚染範囲を特定することが可能となる。

図面の簡単な説明

[0010] [図1]実施の形態 1 における汚染範囲特定装置 100 の構成図。

[図2]実施の形態 1 における汚染範囲特定方法のフローチャート。

[図3]実施の形態 1 におけるオブジェクト関係データ 191 を示す図。

[図4]実施の形態 1 における侵入経路データ 192 を示す図。

[図5]実施の形態 1 における汚染オブジェクトデータ 193 を示す図。

[図6]実施の形態 1 における関係構築 (S110) のフローチャート。

[図7]実施の形態 1 における汚染範囲特定 (S120) のフローチャート。

[図8]実施の形態2におけるオブジェクト関係データ194を示す図。

[図9]実施の形態3におけるオブジェクト関係データ195Aを示す図。

[図10]実施の形態3におけるオブジェクト関係データ195Dを示す図。

[図11]実施の形態3におけるオブジェクト関係データ195Gを示す図。

[図12]実施の形態における汚染範囲特定装置100のハードウェア構成図。

発明を実施するための形態

[0011] 実施の形態および図面において、同じ要素または対応する要素には同じ符号を付している。説明した要素と同じ符号が付された要素の説明は適宜に省略または簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。

[0012] 実施の形態1.

汚染範囲特定装置100について、図1から図7に基づいて説明する。

[0013] ***構成の説明***

図1に基づいて、汚染範囲特定装置100の構成を説明する。

汚染範囲特定装置100は、プロセッサ101とメモリ102と補助記憶装置103と通信装置104と入出力インタフェース105といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0014] プロセッサ101は、演算処理を行うICであり、他のハードウェアを制御する。例えば、プロセッサ101は、CPU、DSPまたはGPUである。

ICは、Integrated Circuitの略称である。

CPUは、Central Processing Unitの略称である。

DSPは、Digital Signal Processorの略称である。

GPUは、Graphics Processing Unitの略称である。

[0015] メモリ 102 は揮発性または不揮発性の記憶装置である。メモリ 102 は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ 102 は RAM である。メモリ 102 に記憶されたデータは必要に応じて補助記憶装置 103 に保存される。

RAM は、Random Access Memory の略称である。

[0016] 補助記憶装置 103 は不揮発性の記憶装置である。例えば、補助記憶装置 103 は、ROM、HDD またはフラッシュメモリである。補助記憶装置 103 に記憶されたデータは必要に応じてメモリ 102 にロードされる。

ROM は、Read Only Memory の略称である。

HDD は、Hard Disk Drive の略称である。

[0017] 通信装置 104 はレシーバ及びトランスミッタである。例えば、通信装置 104 は通信チップまたは NIC である。

NIC は、Network Interface Card の略称である。

[0018] 入出力インタフェース 105 は、入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース 105 は USB 端子であり、入力装置はキーボードおよびマウスであり、出力装置はディスプレイである。

USB は、Universal Serial Bus の略称である。

[0019] 汚染範囲特定装置 100 は、受付部 110 と関係構築部 120 と汚染範囲特定部 130 と出力部 140 といった要素を備える。これらの要素はソフトウェアで実現される。

[0020] 補助記憶装置 103 には、受付部 110 と関係構築部 120 と汚染範囲特定部 130 と出力部 140 としてコンピュータを機能させるための汚染範囲特定プログラムが記憶されている。汚染範囲特定プログラムは、メモリ 102 にロードされて、プロセッサ 101 によって実行される。

補助記憶装置 103 には、さらに、OS が記憶されている。OS の少なくとも一部は、メモリ 102 にロードされて、プロセッサ 101 によって実行される。

プロセッサ１０１は、ＯＳを実行しながら、汚染範囲特定プログラムを実行する。

ＯＳは、Operating Systemの略称である。

[0021] 汚染範囲特定プログラムの入出力データは記憶部１９０に記憶される。

メモリ１０２は記憶部１９０として機能する。但し、補助記憶装置１０３、プロセッサ１０１内のレジスタおよびプロセッサ１０１内のキャッシュメモリなどの記憶装置が、メモリ１０２の代わりに、又は、メモリ１０２と共に、記憶部１９０として機能してもよい。

[0022] 汚染範囲特定装置１００は、プロセッサ１０１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ１０１の機能を分担する。

[0023] 汚染範囲特定プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0024] ***動作の説明***

汚染範囲特定装置１００の動作の手順は汚染範囲特定方法に相当する。また、汚染範囲特定装置１００の動作の手順は汚染範囲特定プログラムによる処理の手順に相当する。

[0025] 図２に基づいて、汚染範囲特定方法を説明する。

ステップＳ１１０において、関係構築部１２０は、複数のソフトウェア動作データに基づいて、オブジェクト関係データを生成する。

[0026] ソフトウェア動作データは、ソフトウェア動作を示すデータである。

[0027] ソフトウェア動作は、ソフトウェアの実行によって発生した動作である。
以下に、ソフトウェア動作の例を示す。

- (１) プロセス起動。
- (２) プロセス終了。
- (３) 通信。
- (４) ファイル書き込み。

- (5) ファイル読み込み。
- (6) ファイル権限変更。
- (7) システムコール。
- (8) アプリケーション動作。
- (9) 認証（成功）。
- (10) 認証（失敗）。
- (11) ポリシー違反

[0028] ソフトウェア動作データの具体例は、通信ログ、OSログ、ファイル操作ログ、アプリケーションログまたはメモリ操作ログなどのログデータである。ログデータは、例えば、OSまたはアプリケーションから出力される。

[0029] ソフトウェア動作データは、動作タイプと動作オブジェクト情報と動作時刻とを含む。

[0030] 動作タイプは、ソフトウェア動作の種類である。

[0031] 動作オブジェクト情報は、ソフトウェア動作で使用された複数のソフトウェアオブジェクトを示す。

ソフトウェアオブジェクトは、ソフトウェアの実行時に使用される要素である。以下に、ソフトウェアオブジェクトの例を示す。

- (1) データファイルまたはプログラムファイルなどのファイル。
- (2) データファイルの中の各データ。各データはプロセスで使用される。
- (3) プロセス。プロセスは、プログラムファイルが実行された後の各インスタンスである。

[0032] 具体的には、動作オブジェクト情報は、動作オブジェクトと対象オブジェクトとを示す。

動作オブジェクトは、ソフトウェア動作を行うソフトウェアオブジェクトである。つまり、動作オブジェクトは、ソフトウェア動作の主体となるソフトウェアオブジェクトである。動作オブジェクトの具体例はプロセスである。

対象オブジェクトは、ソフトウェア動作の対象となるソフトウェアオブジ

ェクトである。つまり、対象オブジェクトはソフトウェア動作の客体となるソフトウェアオブジェクトである。対象オブジェクトの具体例はファイルである。

[0033] 動作時刻は、ソフトウェア動作が発生した時刻である。

[0034] オブジェクト関係データは、複数のソフトウェアオブジェクトの関係を示すデータである。具体的には、オブジェクト関係データは、オブジェクト関係グラフを表す。

オブジェクト関係グラフは、ソフトウェアオブジェクト毎にノードを有し、ノードの組毎にエッジを有する。

ノードは、ソフトウェアオブジェクトを表す。

エッジは、ソフトウェアオブジェクト間の関係を表す。

[0035] 図3に、オブジェクト関係データ191を示す。オブジェクト関係データ191は、オブジェクト関係データの一例である。

オブジェクト関係データ191は、オブジェクト関係グラフ191Gを表す。

オブジェクト関係グラフ191Gにおいて、プロセス名、ファイル名またはログ名が記されている要素がノードである。ノードを結ぶ線がエッジである。矢印線で表されたエッジは、動作タイプに応じた有向関係性を表す有向エッジである。エッジに付された用語は動作タイプに応じた関係性を示す。

[0036] 図2に戻り、説明を続ける。

関係構築(S110)の手順について後述する。

[0037] ステップS120において、汚染範囲特定部130は、オブジェクト関係データとアラートデータとに基づいて、汚染範囲データを生成する。

[0038] アラートデータは、サイバー攻撃の発生を知らせるデータであり、異常オブジェクト情報を含む。

異常オブジェクト情報は、異常オブジェクトを示す。

異常オブジェクトは、サイバー攻撃が検知されたソフトウェアオブジェクトである。

[0039] 汚染範囲データは、汚染範囲を示すデータであり、侵入経路データと汚染オブジェクトデータとを含む。汚染範囲は、サイバー攻撃の影響を受ける範囲である。

侵入経路データは、サイバー攻撃の侵入経路を示す。サイバー攻撃の侵入経路は、汚染範囲に含まれる。

汚染オブジェクトデータは、汚染オブジェクトを示す。

汚染オブジェクトは、サイバー攻撃の影響を受けるソフトウェアオブジェクトである。

[0040] 図4に、侵入経路データ192を示す。侵入経路データ192は、侵入経路データの一例である。

侵入経路データ192は、外部プロセスからプロセス2までの侵入経路を示す。プロセス2が異常オブジェクトである。

[0041] 図5に、汚染オブジェクトデータ193を示す。汚染オブジェクトデータ193は、汚染オブジェクトデータの一例である。

汚染オブジェクトデータ193は、侵入経路上の各ソフトウェアオブジェクトの他に、プロセス2から影響を受ける各ソフトウェアオブジェクトを示す。

[0042] 図2に戻り、説明を続ける。

汚染範囲特定（S130）の手順について後述する。

[0043] ステップS130において、出力部140は、汚染範囲データを出力する。

つまり、出力部140は、侵入経路データと汚染オブジェクトデータとを出力する。

[0044] 図6に基づいて、関係構築（S110）の手順を説明する。

空のオブジェクト関係データが予め用意される。

ステップS111からステップS113は、ソフトウェア動作データごとに実行される。

[0045] ステップS111において、受付部110は、ソフトウェア動作データを

受け付ける。

具体的には、ソフトウェア動作データが汚染範囲特定装置 100 に入力される。そして、受付部 110 は、入力されたソフトウェア動作データを受け付けて記憶部 190 に記憶する。

ソフトウェア動作データは、利用者によって入力されてもよいし、監視対象との通信で入力されてもよいし、その他の方法で入力されてもよい。

[0046] ステップ S 112 において、関係構築部 120 は、ソフトウェア動作データから、動作タイプと動作オブジェクト情報とを抽出する。

[0047] ステップ S 113 において、関係構築部 120 は、動作タイプと動作オブジェクト情報とに基づいて、オブジェクト関係データを更新する。

[0048] オブジェクト関係データは以下のように更新される。オブジェクト関係データはオブジェクト関係グラフを表す。動作オブジェクト情報は、動作オブジェクトと対象オブジェクトとの 2 つのソフトウェアオブジェクトを示す。

関係構築部 120 は、オブジェクト関係グラフの中から、動作オブジェクト情報に示される各ソフトウェアオブジェクトを表すノードを探す。

関係構築部 120 は、見つからなかったノードを新規に生成し、生成したノードをオブジェクト関係グラフに追加する。

関係構築部 120 は、オブジェクト関係グラフから、動作オブジェクトノードと対象オブジェクトノードを選択する。動作オブジェクトノードは動作オブジェクトを表すノードであり、対象オブジェクトノードは対象オブジェクトを表すノードである。

関係構築部 120 は、選択した 2 つのノードを結ぶエッジを生成し、生成したエッジをオブジェクト関係グラフに追加する。具体的には、関係構築部 120 は、動作オブジェクトと対象オブジェクトの有向関係性を動作タイプに応じて特定し、動作オブジェクトノードから対象オブジェクトノードへの有向エッジを追加する。有向エッジは、特定された有向関係性を表す向きを有する。

[0049] 複数のソフトウェア動作データのそれぞれに対して関係構築 (S 110)

が実行されることにより、例えば、オブジェクト関係データ 191（図3参照）が生成される。

[0050] 図7に基づいて、汚染範囲特定（S120）の手順を説明する。

ステップS121において、受付部110は、アラートデータを受け付ける。

具体的には、アラートデータが汚染範囲特定装置100に入力される。そして、受付部110は、入力されたアラートデータを受け付けて記憶部190に記憶する。

アラートデータは、利用者によって入力されてもよいし、攻撃検知装置との通信で入力されてもよいし、その他の方法で入力されてもよい。攻撃検知装置は、監視対象を監視し、発生したサイバー攻撃を検知し、アラートデータを出力する装置である。

[0051] ステップS122において、汚染範囲特定部130は、アラートデータから、異常オブジェクト情報を抽出する。

[0052] ステップS123において、汚染範囲特定部130は、オブジェクト関係グラフを用いて、異常オブジェクトノードから外部プロセスノードまでの侵入経路を特定する。

[0053] 侵入経路は以下のように特定される。オブジェクト関係グラフの中の各エッジは有向エッジである。

まず、汚染範囲特定部130は、オブジェクト関係グラフの中から異常オブジェクトノードを選択する。異常オブジェクトノードは、異常オブジェクトを表すノードである。

そして、汚染範囲特定部130は、異常オブジェクトノードから外部プロセスノードまで各有向エッジを逆方向に辿る。外部プロセスノードは、外部プロセスを表すノードである。外部プロセスは、監視対象の外部で生成されたプロセスである。

異常オブジェクトノードから外部プロセスノードまでの経路が侵入経路である。

[0054] ステップS 1 2 4において、汚染範囲特定部 1 3 0は、オブジェクト関係グラフを用いて、汚染オブジェクトを特定する。

[0055] 汚染オブジェクトは以下のように特定される。

汚染範囲特定部 1 3 0は、オブジェクト関係グラフから、侵入経路に位置する各ノードを選択する。選択される各ノードによって表されるソフトウェアオブジェクトは汚染オブジェクトである。

さらに、汚染範囲特定部 1 3 0は、侵入経路に位置する各ノードから各有向エッジを順方向に辿る。辿った先の各ノードで表されるソフトウェアオブジェクトは汚染オブジェクトである。

[0056] ステップS 1 2 5において、汚染範囲特定部 1 3 0は、汚染範囲データを生成する。

つまり、汚染範囲特定部 1 3 0は、侵入経路データと汚染オブジェクトデータとを生成する。

[0057] 侵入経路データは以下のように生成される。

汚染範囲特定部 1 3 0は、ステップS 1 2 3で特定された侵入経路を示すデータを生成する。生成されるデータが侵入経路データである。

[0058] 汚染オブジェクトデータは以下のように生成される。

汚染範囲特定部 1 3 0は、ステップS 1 2 4で特定された汚染オブジェクトを示すデータを生成する。生成されるデータが汚染オブジェクトデータである。

[0059] オブジェクト関係データ 1 9 1（図 3 参照）を用いて汚染範囲特定（S 1 2 0）が実行されることにより、侵入経路データ 1 9 2（図 4 参照）および汚染オブジェクトデータ 1 9 3（図 5 参照）が生成される。異常オブジェクトはプロセス 2 である。

[0060] ***実施例の説明***

関係構築（S 1 1 0）（図 6 を参照）の実施例を以下に示す。

[0061] <実施例 1>

ステップS 1 1 1において、受付部 1 1 0は、プロセス終了を示すログデ

ータを受け取る。

ステップS 1 1 2において、関係構築部 1 2 0は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはプロセス終了である。動作オブジェクトは指示プロセスであり、対象オブジェクトは終了プロセスである。

ステップS 1 1 3において、関係構築部 1 2 0は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 1 2 0は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードをオブジェクト関係グラフに追加する。そして、関係構築部 1 2 0は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0062] <実施例 2>

ステップS 1 1 1において、受付部 1 1 0は、通信を示すログデータを受け取る。

ステップS 1 1 2において、関係構築部 1 2 0は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプは通信である。動作オブジェクトは通信元プロセスであり、対象オブジェクトは通信先プロセスである。通信元プロセスと通信先プロセスとの各プロセスが外部プロセスである場合、各プロセスは外部アドレスで識別される。外部アドレスは、監視対象の外部の装置を識別するアドレスである。

ステップS 1 1 3において、関係構築部 1 2 0は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 1 2 0は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードをオブジェクト関係グラフに追加する。つまり、動作オブジェクト情報が動作オブジェクトまたは対象オブジェクトの識別子として外部アドレスを示す場合、外部プロセスを表すノードが生成される。そして、関係構築部 1 2 0は

、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0063] <実施例 3>

ステップ S 1 1 1 において、受付部 1 1 0 は、ファイル操作 (w r i t e) を示すログデータを受け取る。

ステップ S 1 1 2 において、関係構築部 1 2 0 は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはファイル書込みである。動作オブジェクトはプロセスであり、対象オブジェクトはファイルである。

ステップ S 1 1 3 において、関係構築部 1 2 0 は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 1 2 0 は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードをオブジェクト関係グラフに追加する。そして、関係構築部 1 2 0 は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0064] <実施例 4>

ステップ S 1 1 1 において、受付部 1 1 0 は、ファイル操作 (r e a d) を示すログデータを受け取る。

ステップ S 1 1 2 において、関係構築部 1 2 0 は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはファイル読込みである。動作オブジェクトはプロセスであり、対象オブジェクトはファイルである。

ステップ S 1 1 3 において、関係構築部 1 2 0 は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 1 2 0 は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードを

オブジェクト関係グラフに追加する。そして、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0065] <実施例 5>

ステップ S 111 において、受付部 110 は、ファイル操作（権限変更）を示すログデータを受け取る。

ステップ S 112 において、関係構築部 120 は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはファイル権限変更である。動作オブジェクトはプロセスであり、対象オブジェクトはファイルである。

ステップ S 113 において、関係構築部 120 は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 120 は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードをオブジェクト関係グラフに追加する。そして、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0066] <実施例 6>

ステップ S 111 において、受付部 110 は、OS システムコールを示すログデータを受け取る。

ステップ S 112 において、関係構築部 120 は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはシステムコールである。システムコールの種類は例えば名称で識別される。動作オブジェクトはプロセスであり、対象オブジェクトはプロセスまたはファイルである。

ステップ S 113 において、関係構築部 120 は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 120 は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードを

オブジェクト関係グラフに追加する。そして、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0067] <実施例 7>

ステップ S 111 において、受付部 110 は、アプリケーション動作を示すログデータを受け取る。

ステップ S 112 において、関係構築部 120 は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはアプリケーション動作である。アプリケーション動作の種類は例えば名称で識別される。動作オブジェクトはプロセスであり、対象オブジェクトはプロセスまたはファイルである。

ステップ S 113 において、関係構築部 120 は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 120 は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードをオブジェクト関係グラフに追加する。そして、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0068] <実施例 8>

ステップ S 111 において、受付部 110 は、セキュリティを示すログデータを受け取る。セキュリティの具体例は認証である。

ステップ S 112 において、関係構築部 120 は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプは認証成功、認証失敗またはポリシー違反である。動作オブジェクトはプロセスであり、対象オブジェクトはプロセスである。

ステップ S 113 において、関係構築部 120 は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部 120 は、オブジェクト関

係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードをオブジェクト関係グラフに追加する。そして、関係構築部120は、動作オブジェクトノードから対象オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。

[0069] ***実施の形態1の効果***

汚染範囲特定装置100は、侵入経路および汚染部分（汚染オブジェクト）を特定することができる。

汚染範囲特定装置100は、複数のソフトウェアオブジェクトの関係をオブジェクト関係グラフによって一元的に管理することができる。これにより、侵入経路および汚染部分が迅速に特定される。

侵入経路および汚染部分が特定されることにより、汚染部分の除去および再発防止の対応が可能となる。

[0070] 実施の形態2.

3つのソフトウェアオブジェクト間の関係を含むオブジェクト関係データを生成する形態について、主に実施の形態1と異なる点を図8に基づいて説明する。

[0071] ***構成の説明***

汚染範囲特定装置100の構成は、実施の形態1における構成（図1参照）と同じである。

[0072] ***動作の説明***

汚染範囲特定方法は、実施の形態1における方法（図2参照）と同じである。

但し、関係構築（S110）によって、3つのソフトウェアオブジェクト間の関係を含むオブジェクト関係データが生成される。

[0073] 図6に基づいて、関係構築（S110）の手順を説明する。

ステップS111において、受付部110は、ソフトウェア動作データを受け付ける。

ソフトウェア動作データは、動作タイプと動作オブジェクト情報を含む。

動作オブジェクト情報は、動作タイプで識別されるソフトウェア動作で使用する3つのソフトウェアオブジェクトを示す。

[0074] ステップS 1 1 2において、関係構築部 1 2 0は、ソフトウェア動作データから、動作タイプと動作オブジェクト情報を抽出する。

[0075] ステップS 1 1 3において、関係構築部 1 2 0は、動作タイプとオブジェクト情報とに基づいて、オブジェクト関係データを更新する。

[0076] オブジェクト関係データは以下のように更新される。オブジェクト関係データはオブジェクト関係グラフを表す。動作オブジェクト情報は、第1オブジェクトと第2オブジェクトと第3オブジェクトとの3つのソフトウェアオブジェクトを示す。

関係構築部 1 2 0は、オブジェクト関係グラフの中から、動作オブジェクト情報に示される各ソフトウェアオブジェクトを表すノードを探す。

関係構築部 1 2 0は、見つからなかったノードをオブジェクト関係グラフに追加する。

関係構築部 1 2 0は、オブジェクト関係グラフから、第1オブジェクトノードと第3オブジェクトノードを選択する。第1オブジェクトノードは第1オブジェクトを表すノードであり、第3オブジェクトノードは第3オブジェクトを表すノードである。関係構築部 1 2 0は、選択した2つのノードを結ぶエッジをオブジェクト関係グラフに追加する。具体的には、関係構築部 1 2 0は、第1オブジェクトノードから第3オブジェクトノードへの有向エッジを追加する。

関係構築部 1 2 0は、オブジェクト関係グラフから、第2オブジェクトノードと第3オブジェクトノードを選択する。第2オブジェクトノードは第2オブジェクトを表すノードである。関係構築部 1 2 0は、選択した2つのノードを結ぶエッジをオブジェクト関係グラフに追加する。具体的には、関係構築部 1 2 0は、第3オブジェクトノードから第2オブジェクトノードへの有向エッジを追加する。

[0077] ***実施例の説明***

図8に基づいて、関係構築（S110）（図6参照）の実施例を説明する。

図8は、オブジェクト関係データ194を示す。オブジェクト関係データ194はオブジェクト関係グラフ194Gを表す。

ステップS111において、受付部110は、プロセス起動を示すログデータを受け取る。

ステップS112において、関係構築部120は、ログデータから、動作タイプと動作オブジェクト情報を抽出する。動作タイプはプロセス起動である。第1オブジェクトは親プロセスであり、第2オブジェクトは子プロセスであり、第3オブジェクトはプログラムファイルである。

ステップS113において、関係構築部120は、オブジェクト関係グラフに第1オブジェクトノードがなければ、第1オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部120は、オブジェクト関係グラフに第2オブジェクトノードがなければ、第2オブジェクトノードをオブジェクト関係グラフに追加する。また、関係構築部120は、オブジェクト関係グラフに第3オブジェクトノードがなければ、第3オブジェクトノードをオブジェクト関係グラフに追加する。そして、関係構築部120は、第1オブジェクトノードから第3オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。さらに、関係構築部120は、第3オブジェクトノードから第2オブジェクトノードへのエッジをオブジェクト関係グラフに追加する。各エッジには動作タイプに応じた関係性が付記される。

[0078] ***実施の形態2の効果***

汚染範囲特定装置100は、2つのソフトウェアオブジェクト間の関係だけでなく3つのソフトウェアオブジェクト間の関係も管理することができる。

[0079] 実施の形態3.

オブジェクト関係グラフの中の各ノードと各エッジにプロファイルを付加する形態について、主に実施の形態1と異なる点を図9から図11に基づい

て説明する。

[0080] ***構成の説明***

汚染範囲特定装置 100 の構成は、実施の形態 1 における構成（図 1 参照）と同じである。

[0081] ***動作の説明***

汚染範囲特定方法は、実施の形態 1 における方法（図 2 参照）と同じである。

但し、関係構築（S 110）によって、オブジェクト関係グラフの中の各ノードと各エッジにプロファイルが付加される。

[0082] 図 6 に基づいて、関係構築（S 110）の手順を説明する。

ステップ S 111 において、受付部 110 は、ソフトウェア動作データを受け付ける。

[0083] ステップ S 112 において、関係構築部 120 は、ソフトウェア動作データから、動作タイプと動作オブジェクト情報と動作時刻とを抽出する。

[0084] ステップ S 113 において、関係構築部 120 は、動作タイプとオブジェクト情報と動作時刻とに基づいて、オブジェクト関係データを更新する。

[0085] オブジェクト関係データは以下のように更新される。オブジェクト関係データはオブジェクト関係グラフを表す。動作オブジェクト情報は、動作オブジェクトと対象オブジェクトとの 2 つのソフトウェアオブジェクトを示す。

関係構築部 120 は、オブジェクト関係グラフの中から、動作オブジェクト情報に示される各ソフトウェアオブジェクトを表すノードを探す。

関係構築部 120 は、見つかったノードに付加されているプロファイルを更新する。具体的には、プロファイルの中の更新時刻を今回の動作時刻すなわち最新の動作時刻に更新する。

関係構築部 120 は、見つからなかったノードをオブジェクト関係グラフに追加する。さらに、関係構築部 120 は、追加されたノードに対するプロファイルを生成し、生成されたプロファイルを追加されたノードに付加する。ノード用のプロファイルは、ノード識別子とノードタイプと更新時刻とを

含む。ノード識別子はノードを識別する。ノードタイプはノードによって表されるソフトウェアオブジェクトの種類を識別する。ノードタイプの具体例は、プロセス、データファイル、プログラムファイルおよびログファイルである。更新時刻は今回の動作時刻すなわち最新の動作時刻である。

関係構築部120は、オブジェクト関係グラフから、動作オブジェクトノードと対象オブジェクトノードを選択する。関係構築部120は、選択した2つのノードを結ぶエッジをオブジェクト関係グラフに追加する。具体的には、関係構築部120は、動作オブジェクトノードから対象オブジェクトノードへの有向エッジを追加する。さらに、関係構築部120は、追加されたエッジに対するプロファイルを生成し、生成されたプロファイルを追加されたエッジに付加する。エッジ用のプロファイルは、エッジ識別子とエッジタイプと更新時刻とを含む。エッジタイプは、動作タイプに応じた関係性を識別する。つまり、エッジタイプは、エッジによって結ばれる2つのソフトウェアオブジェクトの関係性を識別する。更新時刻は今回の動作時刻すなわち最新の動作時刻である。

[0086] ***実施例の説明***

関係構築（S110）（図6参照）の実施例を以下に示す。

ステップS111において、受付部110は、通信を示すログデータを受け取る。ログデータは通信データ情報を含んでもよい。通信データ情報は、通信データおよび通信データ量などを示す。

ステップS112において、関係構築部120は、ログデータから、動作タイプと動作オブジェクト情報と動作時刻とを抽出する。動作タイプは通信である。動作オブジェクトは通信元プロセスであり、対象オブジェクトは通信先プロセスである。通信先プロセスまたは通信先プロセスが外部アドレスで識別される場合、そのプロセスは外部プロセスである。関係構築部120は、ログデータから通信データ情報を抽出してもよい。

ステップS113において、関係構築部120は、オブジェクト関係グラフに動作オブジェクトノードがなければ、動作オブジェクトノードと動作オ

プロジェクトノード用のプロファイルをオブジェクト関係グラフに追加する。また、関係構築部 120 は、オブジェクト関係グラフに対象オブジェクトノードがなければ、対象オブジェクトノードと対象オブジェクトノード用のプロファイルをオブジェクト関係グラフに追加する。追加される各プロファイルは、ノード識別子とノードタイプと生成時刻と更新時刻とを含む。ノードタイプはプロセスである。生成時刻と更新時刻とのそれぞれは、ログデータから抽出された動作時刻と同じである。また、関係構築部 120 は、動作オブジェクトノードまたは対象オブジェクトノードがオブジェクト関係グラフにあれば、そのノード用のプロファイルの中の更新時刻を、ログデータから抽出された動作時刻に更新する。

さらに、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへのエッジとそのエッジプロファイルをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。エッジプロファイルは、エッジ用のプロファイルであり、エッジ識別子とエッジタイプと生成時刻と更新時刻とを含む。生成時刻と更新時刻とのそれぞれは、ログデータから抽出された動作時刻と同じである。

関係構築部 120 は、各プロファイルに通信データ情報を含めてもよい。

[0087] 図 9、図 10 および図 11 に、エッジプロファイルを含むオブジェクト関係グラフの例を示す。「Edge ID」はエッジ識別子を意味する。「Type」はエッジタイプを意味する。「Origin」は生成時刻を意味する。「Update」は更新時刻を意味する。

図 9 は、オブジェクト関係データ 195 A を示す。オブジェクト関係データ 195 A はオブジェクト関係グラフ 195 B を表す。オブジェクト関係グラフ 195 B はエッジプロファイル 195 C を含む。エッジプロファイル 195 C は、通信元プロセスから通信ログへのエッジ用のプロファイルである。

図 10 は、オブジェクト関係データ 195 D を示す。オブジェクト関係データ 195 D はオブジェクト関係グラフ 195 E を表す。オブジェクト関係

グラフ 195 E はエッジプロファイル 195 F を含む。エッジプロファイル 195 F は、通信先プロセスから通信ログへのエッジ用のプロファイルである。

図 11 は、オブジェクト関係データ 195 G を示す。オブジェクト関係データ 195 G はオブジェクト関係グラフ 195 H を表す。オブジェクト関係グラフ 195 H はエッジプロファイル 195 I を含む。エッジプロファイル 195 I は、通信元プロセスから通信先プロセスへのエッジ用のプロファイルである。

[0088] ***実施の形態 3 の効果***

汚染範囲特定装置 100 は、各ノードおよび各エッジにプロファイルを追加することができる。つまり、各ソフトウェアオブジェクトおよびソフトウェアオブジェクト間の関係をより詳細に管理することができる。

各プロファイルは時刻情報を有する。これにより、時系列の矛盾をなくして侵入経路および汚染部分を高精度に特定することが可能となる。

[0089] ***実施の形態 3 の補足***

実施の形態 3 に実施の形態 2 が適用されてもよい。つまり、実施の形態 3 におけるオブジェクト関係データは、実施の形態 2 におけるオブジェクト関係グラフと同様に、3 つのソフトウェアオブジェクト間の関係を含んでもよい。

[0090] 実施の形態 4.

各ノードプロファイルに有効フラグが追加される形態について、主に実施の形態 3 と異なる点を説明する。

[0091] ***構成の説明***

汚染範囲特定装置 100 の構成は、実施の形態 1 における構成（図 1 参照）と同じである。

[0092] ***動作の説明***

汚染範囲特定方法は、実施の形態 1 における方法（図 2 参照）と同じである。

但し、関係構築（S 1 1 0）によって、オブジェクト関係グラフの中の各ノードと各エッジにプロファイルが付加される。そして、各ノード用のプロファイルは有効フラグを含む。有効フラグは、ソフトウェアオブジェクトが有効であるか否かを示す。

[0093] 図6に基づいて、関係構築（S 1 1 0）の手順を説明する。

ステップS 1 1 1において、受付部1 1 0は、ソフトウェア動作データを受け付ける。

[0094] ステップS 1 1 2において、関係構築部1 2 0は、ソフトウェア動作データから、動作タイプと動作オブジェクト情報と動作時刻とを抽出する。

[0095] ステップS 1 1 3において、関係構築部1 2 0は、動作タイプとオブジェクト情報と動作時刻とに基づいて、オブジェクト関係データを更新する。

[0096] オブジェクト関係データは以下のように更新される。

オブジェクト関係データはオブジェクト関係グラフを表す。動作オブジェクト情報は、動作オブジェクトと対象オブジェクトとの2つのソフトウェアオブジェクトを示す。

関係構築部1 2 0は、オブジェクト関係グラフの中から、動作オブジェクト情報に示される各ソフトウェアオブジェクトを表すノードを探す。

関係構築部1 2 0は、見つかったノードに付加されているプロファイルを更新する。具体的には、プロファイルの中の更新時刻を今回の動作時刻に更新する。さらに、関係構築部1 2 0は、動作タイプがオブジェクト無効動作を識別するか判定する。オブジェクト無効動作は、ソフトウェアオブジェクトが無効になるソフトウェア動作である。例えば、オブジェクト無効動作は、プロセス終了またはファイル削除などである。動作タイプがオブジェクト無効動作を識別する場合、関係構築部1 2 0は、プロファイルの中の有効フラグの値を無効値に更新する。無効値は無効を意味する値である。

関係構築部1 2 0は、見つからなかったノードをオブジェクト関係グラフに追加する。さらに、関係構築部1 2 0は、追加されたノード用のプロファイルを生成し、生成されたプロファイルを追加されたノードに付加する。ノ

ード用のプロファイルは、ノード識別子とノードタイプと更新時刻と有効フラグとを含む。有効フラグの初期値は有効値である。有効値は有効を意味する値である。

関係構築部 120 は、オブジェクト関係グラフから、動作オブジェクトノードと対象オブジェクトノードを選択する。関係構築部 120 は、選択した 2 つのノードを結ぶエッジをオブジェクト関係グラフに追加する。具体的には、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへの有向エッジを追加する。さらに、関係構築部 120 は、追加されたエッジ用のプロファイルを生成し、生成されたプロファイルを追加されたエッジに付加する。エッジ用のプロファイルは、エッジ識別子とエッジタイプと更新時刻とを含む。

[0097] ***実施例の説明***

関係構築 (S 110) (図 6 参照) の実施例を以下に示す。

ステップ S 111 において、受付部 110 は、プロセス終了を示すログデータを受け取る。

ステップ S 112 において、関係構築部 120 は、ログデータから、動作タイプと動作オブジェクト情報と動作時刻とを抽出する。動作タイプはプロセス終了である。動作オブジェクトは指示プロセスであり、対象オブジェクトは終了プロセスである。

ステップ S 113 において、動作オブジェクトノードがオブジェクト関係グラフになく、対象オブジェクトノードがオブジェクト関係グラフにある。関係構築部 120 は、動作オブジェクトノードと動作オブジェクトノード用のプロファイルをオブジェクト関係グラフに追加する。追加されるプロファイルは、ノード識別子とノードタイプと生成時刻と更新時刻と有効フラグとを含む。ノードタイプはプロセスである。生成時刻と更新時刻とのそれぞれは、ログデータから抽出された動作時刻と同じである。有効フラグは有効値を示す。また、関係構築部 120 は、対象オブジェクトノード用のプロファイルの中の更新時刻を、ログデータから抽出された動作時刻に更新する。さ

らに、関係構築部 120 は、対象オブジェクトノード用のプロファイルの中の有効フラグの値を無効値に更新する。

さらに、関係構築部 120 は、動作オブジェクトノードから対象オブジェクトノードへのエッジとそのエッジプロファイルをオブジェクト関係グラフに追加する。エッジには動作タイプに応じた関係性が付記される。エッジプロファイルは、エッジ用のプロファイルであり、エッジ識別子とエッジタイプと生成時刻と更新時刻とを含む。生成時刻と更新時刻とのそれぞれは、ログデータから抽出された動作時刻と同じである。

[0098] ***実施の形態 4 の効果***

汚染範囲特定装置 100 は、各ノード用のプロファイルに有効フラグを含めることができる。これにより、侵入経路および汚染部分をより高精度に特定することが可能となる。

[0099] ***実施の形態の補足***

図 12 に基づいて、汚染範囲特定装置 100 のハードウェア構成を説明する。

汚染範囲特定装置 100 は処理回路 109 を備える。

処理回路 109 は、受付部 110 と関係構築部 120 と汚染範囲特定部 130 と出力部 140 とを実現するハードウェアである。

処理回路 109 は、専用のハードウェアであってもよいし、メモリ 102 に格納されるプログラムを実行するプロセッサ 101 であってもよい。

[0100] 処理回路 109 が専用のハードウェアである場合、処理回路 109 は、例えば、単回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ASIC、FPGA またはこれらの組み合わせである。

ASIC は、Application Specific Integrated Circuit の略称である。

FPGA は、Field Programmable Gate Array の略称である。

[0101] 汚染範囲特定装置 100 は、処理回路 109 を代替する複数の処理回路を

備えてもよい。複数の処理回路は、処理回路 109 の機能を分担する。

[0102] 処理回路 109 において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0103] このように、汚染範囲特定装置 100 の機能はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0104] 各実施の形態は、好ましい形態の例示であり、本開示の技術的範囲を制限することを意図するものではない。各実施の形態は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。

[0105] 汚染範囲特定装置 100 の要素である「部」は、「処理」または「工程」と読み替えてもよい。

符号の説明

[0106] 100 汚染範囲特定装置、101 プロセッサ、102 メモリ、103 補助記憶装置、104 通信装置、105 入出力インタフェース、109 処理回路、110 受付部、120 関係構築部、130 汚染範囲特定部、140 出力部、190 記憶部、191 オブジェクト関係データ、191G オブジェクト関係グラフ、192 侵入経路データ、193 汚染オブジェクトデータ、194 オブジェクト関係データ、194G オブジェクト関係グラフ、195A オブジェクト関係データ、195B オブジェクト関係グラフ、195C エッジプロファイル。

請求の範囲

- [請求項1] ソフトウェア動作の動作タイプと前記ソフトウェア動作で使用された複数のソフトウェアオブジェクトを示す動作オブジェクト情報とをそれぞれが含む複数のソフトウェア動作データに基づいて、前記複数のソフトウェアオブジェクトの関係を示すオブジェクト関係データを生成する関係構築部と、
- 前記オブジェクト関係データと、サイバー攻撃の発生を知らせるアラートデータと、に基づいて、サイバー攻撃の影響を受ける汚染範囲を示す汚染範囲データを生成する汚染範囲特定部と、
- を備える汚染範囲特定装置。
- [請求項2] 前記関係構築部は、各ソフトウェア動作データから動作タイプと動作オブジェクト情報とを抽出し、抽出された動作オブジェクト情報に示される複数のソフトウェアオブジェクトを表す複数のノードと、抽出された動作タイプに応じた向きを有して前記複数のノードを結ぶ有向エッジと、を含むオブジェクト関係グラフを表すデータを前記オブジェクト関係データとして生成する
- 請求項1に記載の汚染範囲特定装置。
- [請求項3] 各ソフトウェア動作データは、ソフトウェア動作が発生した動作時刻を含み、
- 前記関係構築部は、各ノードに対して、ノードを識別するノード識別子と、ノードによって表されるソフトウェアオブジェクトの種類を識別するノードタイプと、最新の動作時刻を示す更新時刻と、を含むプロファイルを付加する
- 請求項2に記載の汚染範囲特定装置。
- [請求項4] 前記関係構築部は、各エッジに対して、エッジを識別するエッジ識別子と、エッジによって結ばれる2つのソフトウェアオブジェクトの関係性を識別するエッジタイプと、最新の動作時刻を示す更新時刻と、を含むプロファイルを付加する

請求項3に記載の汚染範囲特定装置。

- [請求項5] 前記関係構築部は、各ノードに付加されるプロファイルに、ノードによって表されるソフトウェアオブジェクトが有効であるか否かを示す有効フラグを含める

請求項3または請求項4に記載の汚染範囲特定装置。

- [請求項6] 前記汚染範囲データは、侵入経路データを含み、
前記汚染範囲特定部は、前記アラートデータから前記サイバー攻撃が検知されたソフトウェアオブジェクトである異常オブジェクトを示す異常オブジェクト情報を抽出し、前記オブジェクト関係グラフを用いて前記異常オブジェクトのノードから外部プロセスのノードまで各有向エッジを逆方向に辿り、前記異常オブジェクトのノードから前記外部プロセスのノードまでの経路である侵入経路を示すデータを前記侵入経路データとして生成する

請求項2から請求項5のいずれか1項に記載の汚染範囲特定装置。

- [請求項7] 前記汚染範囲データは、汚染オブジェクトデータを含み、
前記汚染範囲特定部は、前記オブジェクト関係グラフから前記侵入経路に位置する各ノードを選択し、選択された各ノードから各有向エッジを順方向に辿り、選択された各ノードで表されるソフトウェアオブジェクトと辿った先の各ノードで表されるソフトウェアオブジェクトとを示すデータを前記汚染オブジェクトデータとして生成する

請求項6に記載の汚染範囲特定装置。

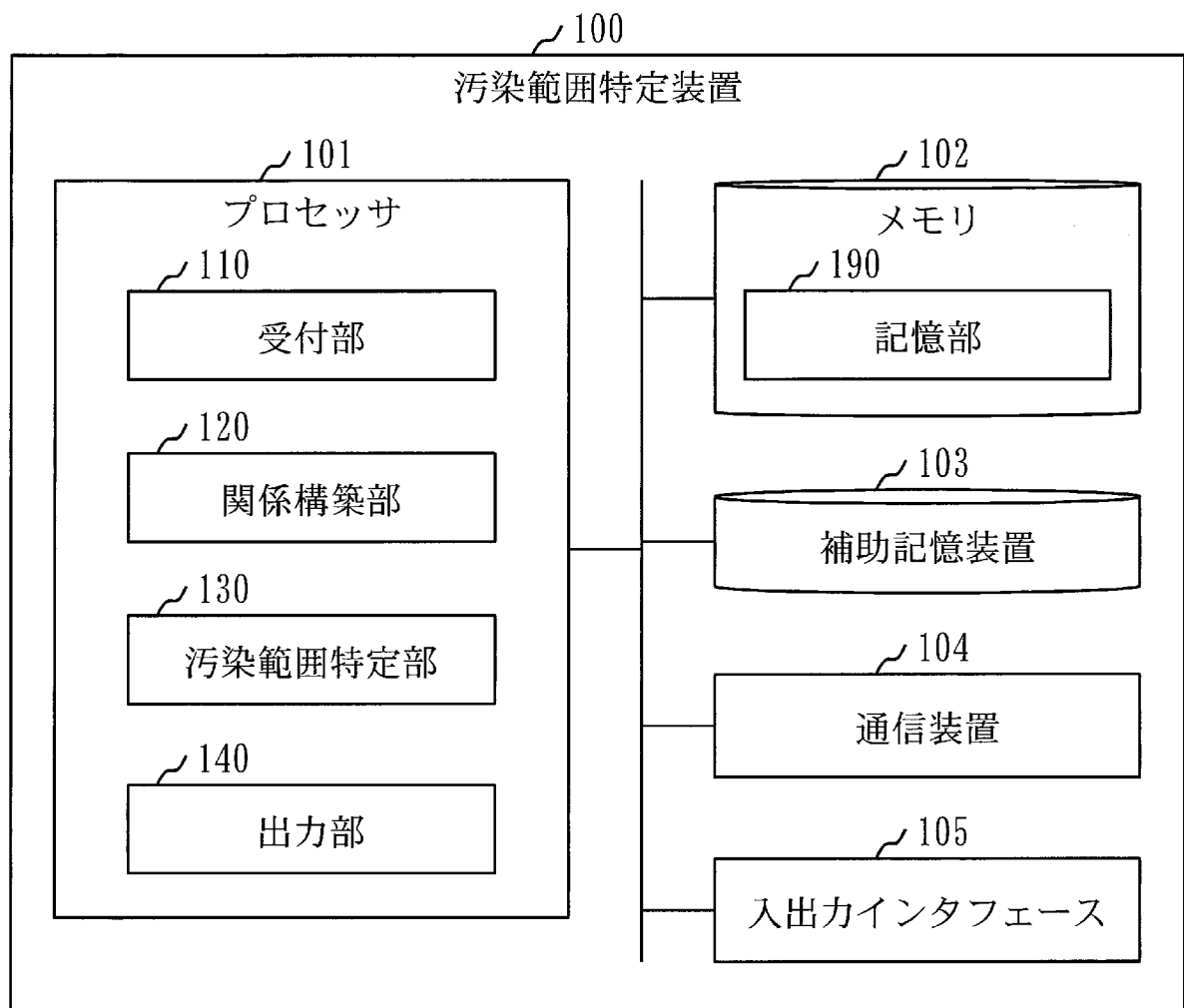
- [請求項8] ソフトウェア動作の動作タイプと前記ソフトウェア動作で使用された複数のソフトウェアオブジェクトを示す動作オブジェクト情報とをそれぞれが含む複数のソフトウェア動作データに基づいて、前記複数のソフトウェアオブジェクトの関係を示すオブジェクト関係データを生成する関係構築処理と、

前記オブジェクト関係データと、サイバー攻撃の発生を知らせるアラートデータと、に基づいて、サイバー攻撃の影響を受ける汚染範囲

を示す汚染範囲データを生成する汚染範囲特定処理と、
をコンピュータに実行させるための汚染範囲特定プログラム。

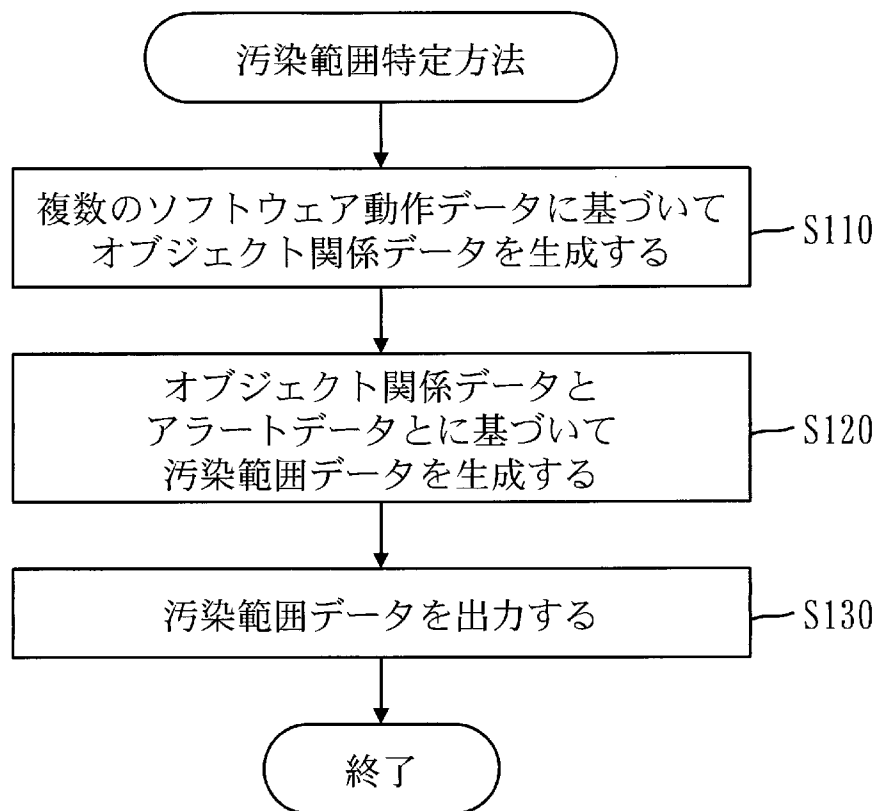
[図1]

図1



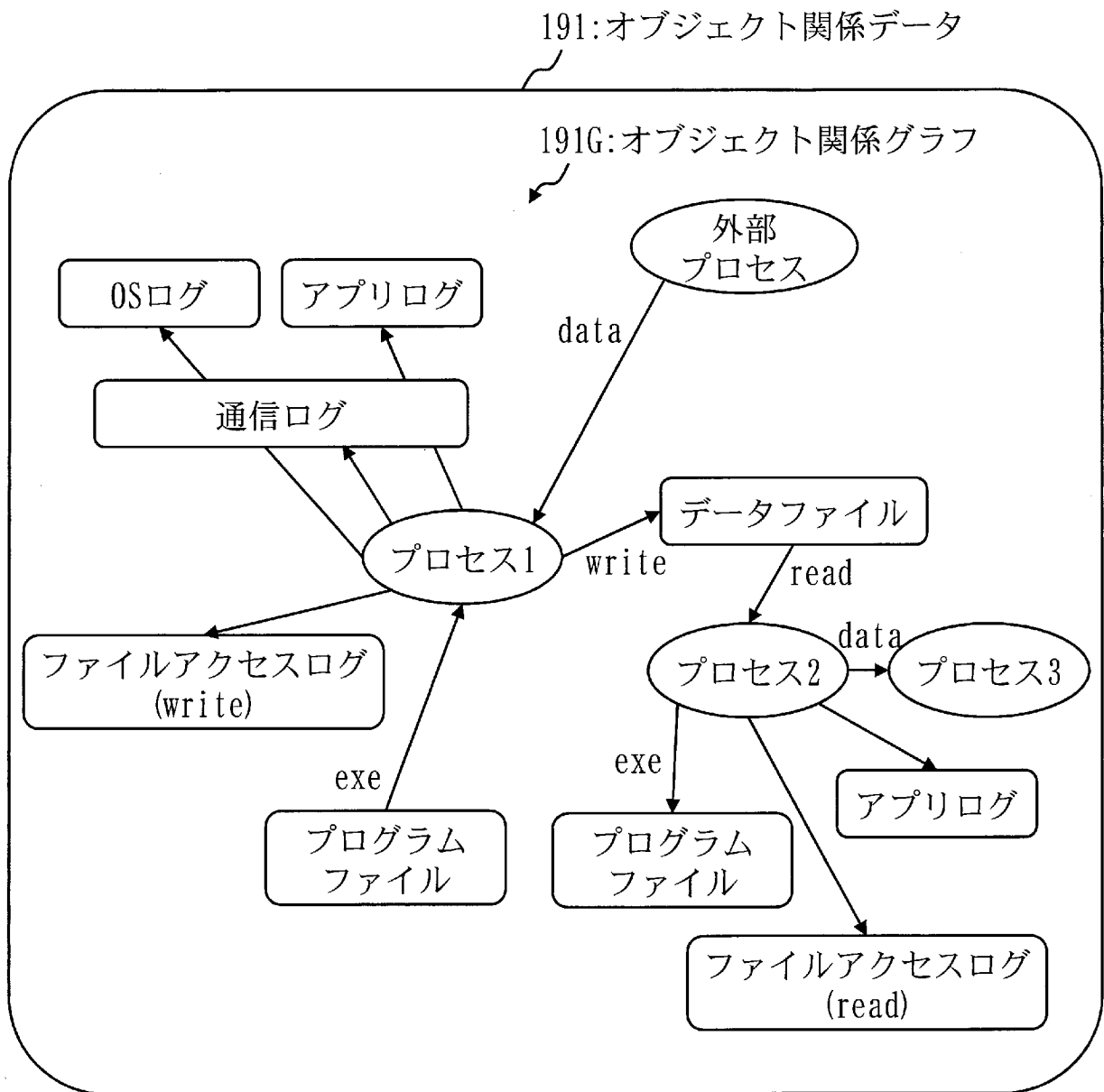
[図2]

図2



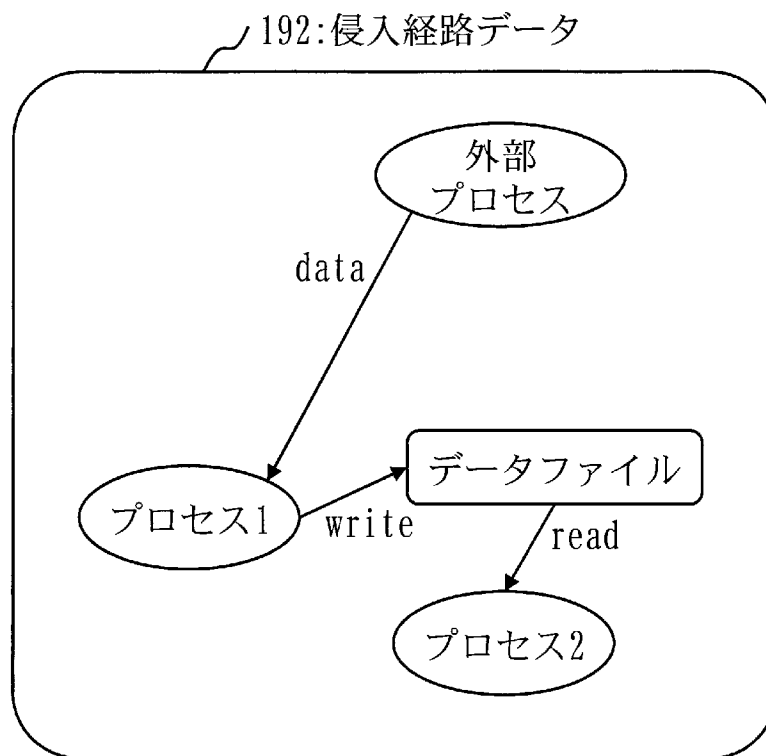
[図3]

図3



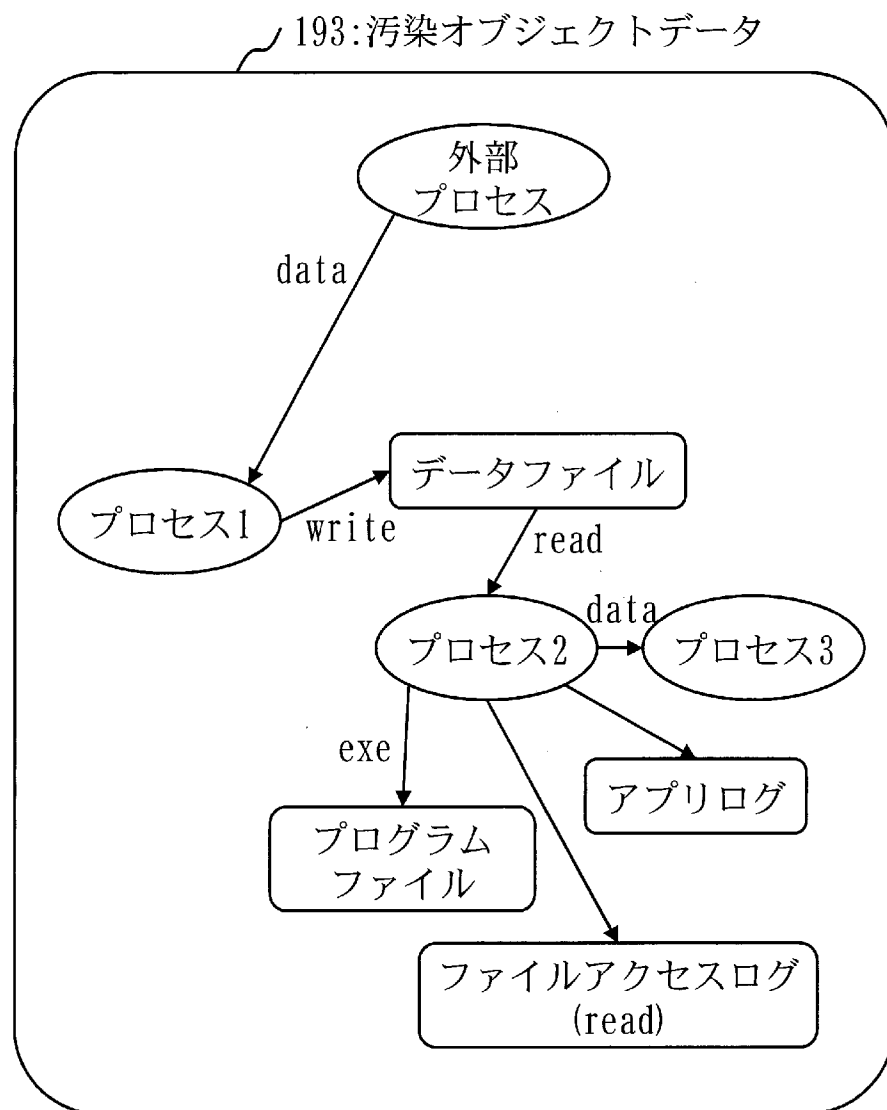
[図4]

図4



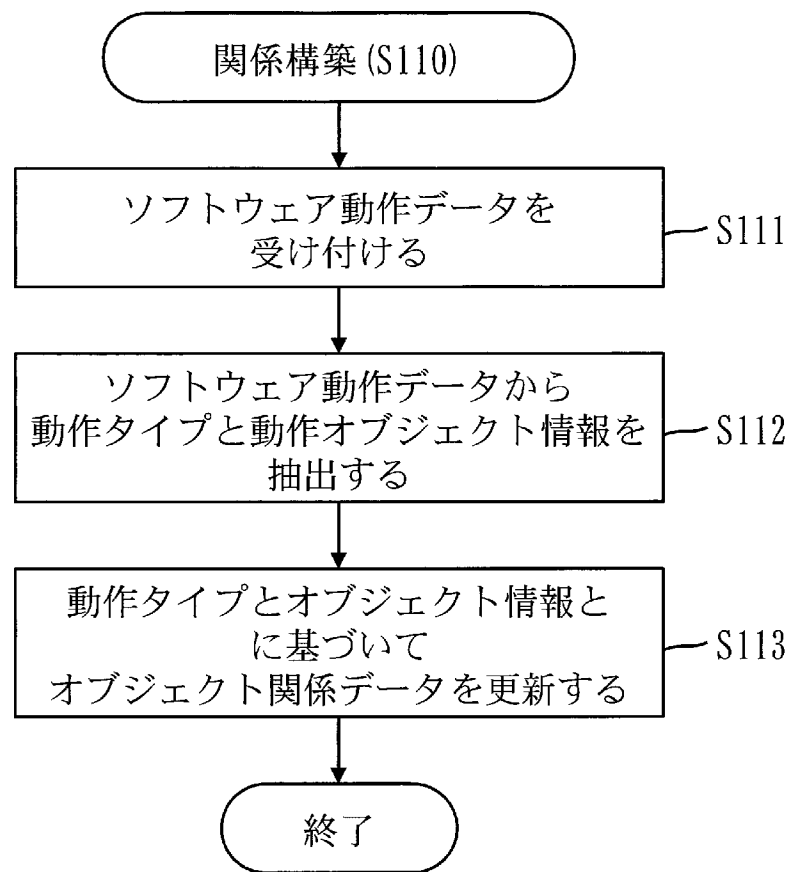
[図5]

図5



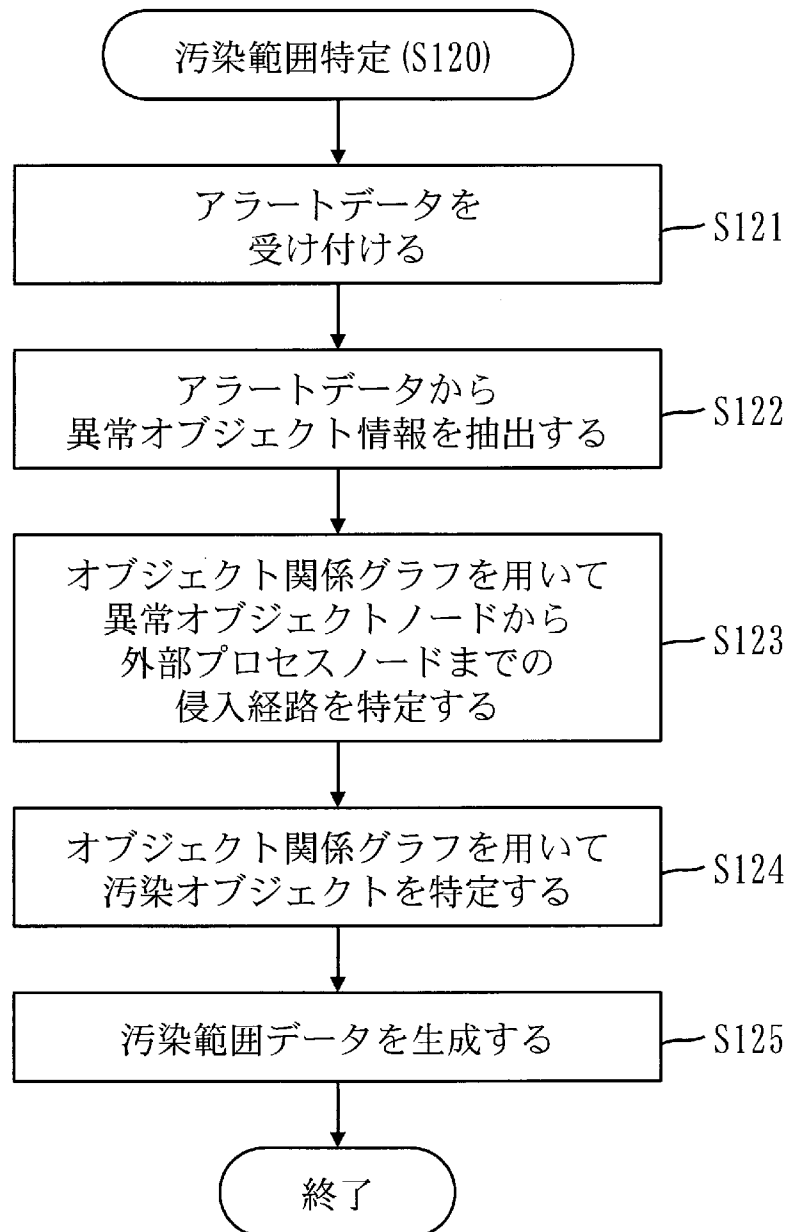
[図6]

図6



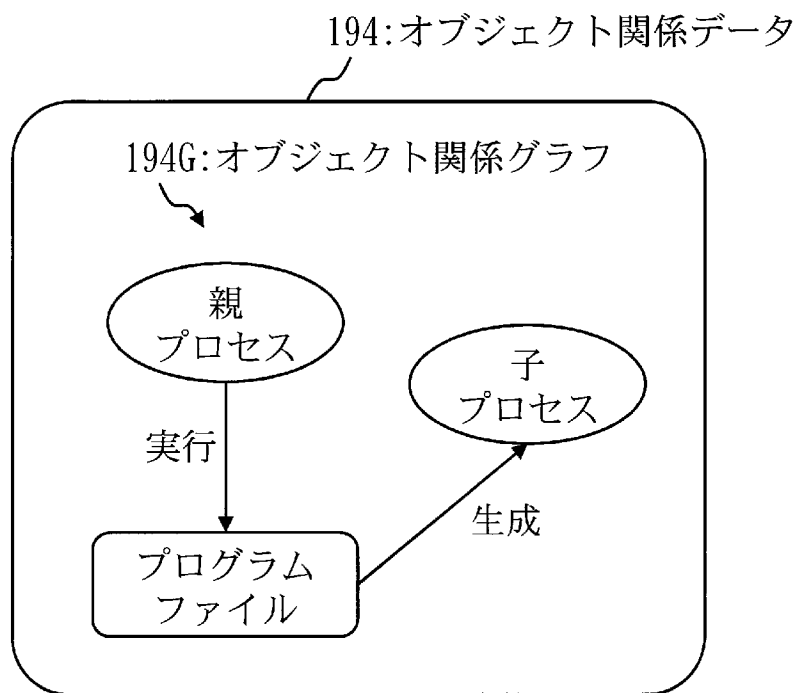
[図7]

図7



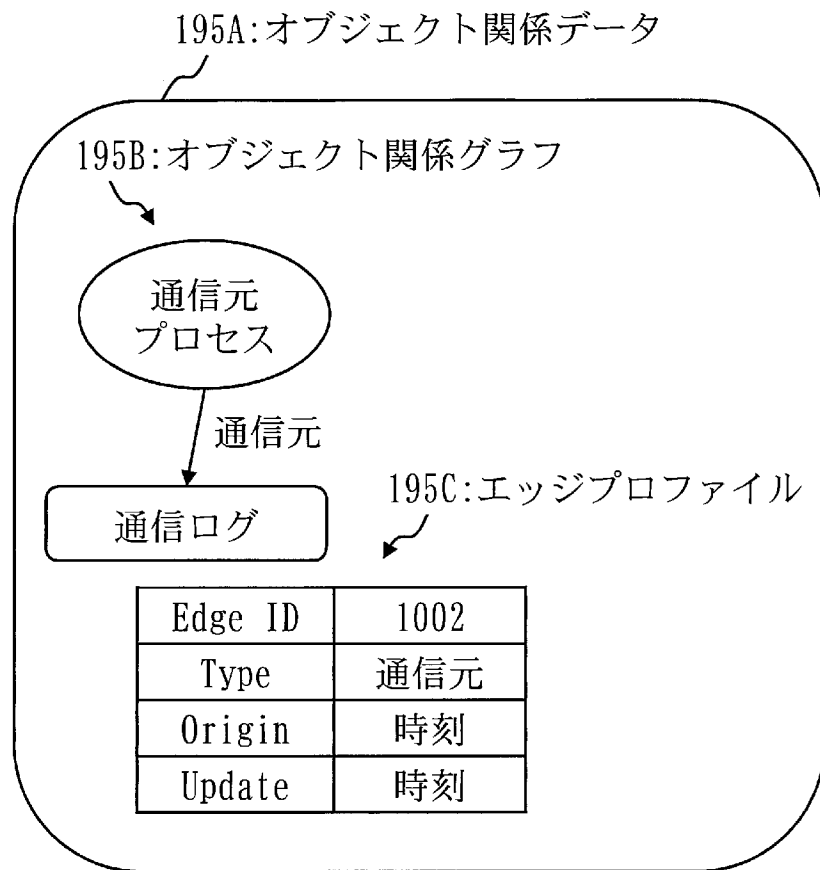
[図8]

図8



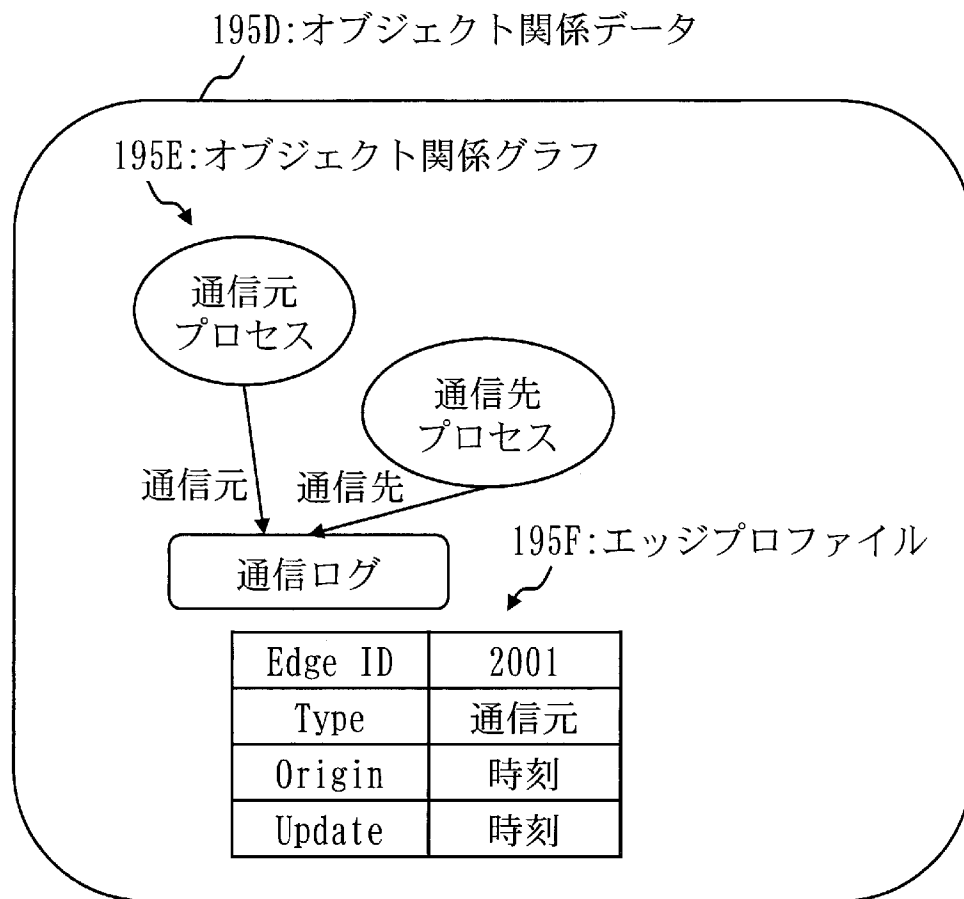
[図9]

図9



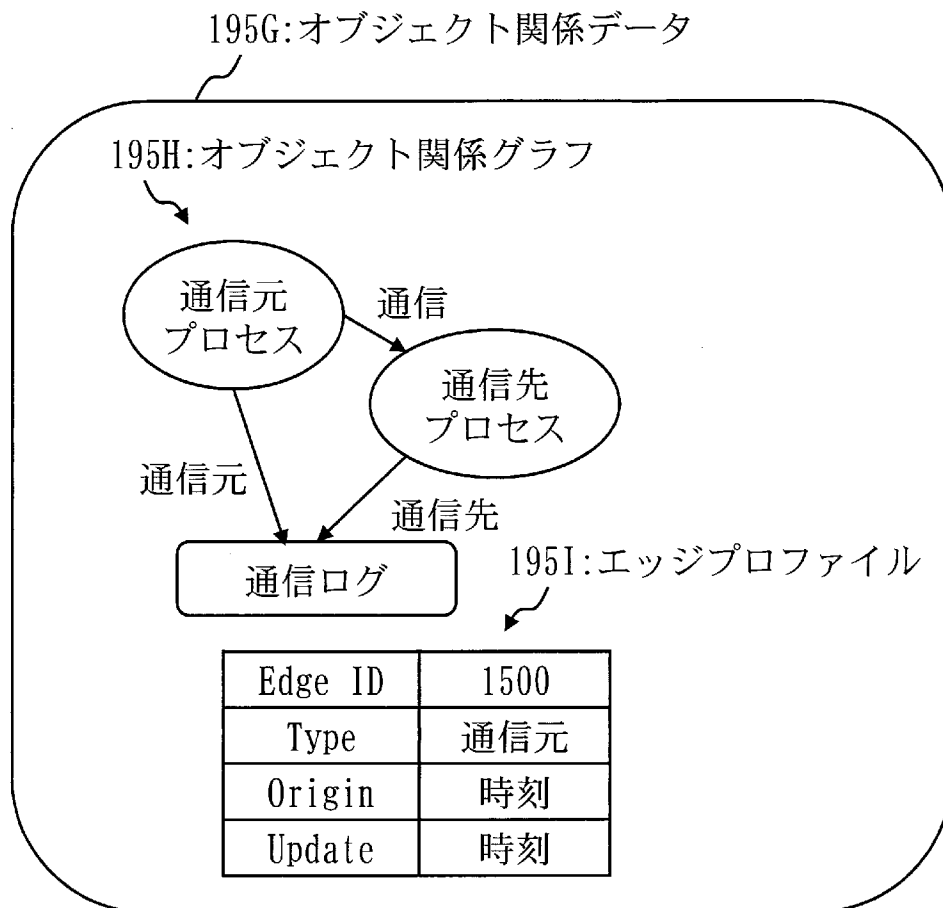
[図10]

図10



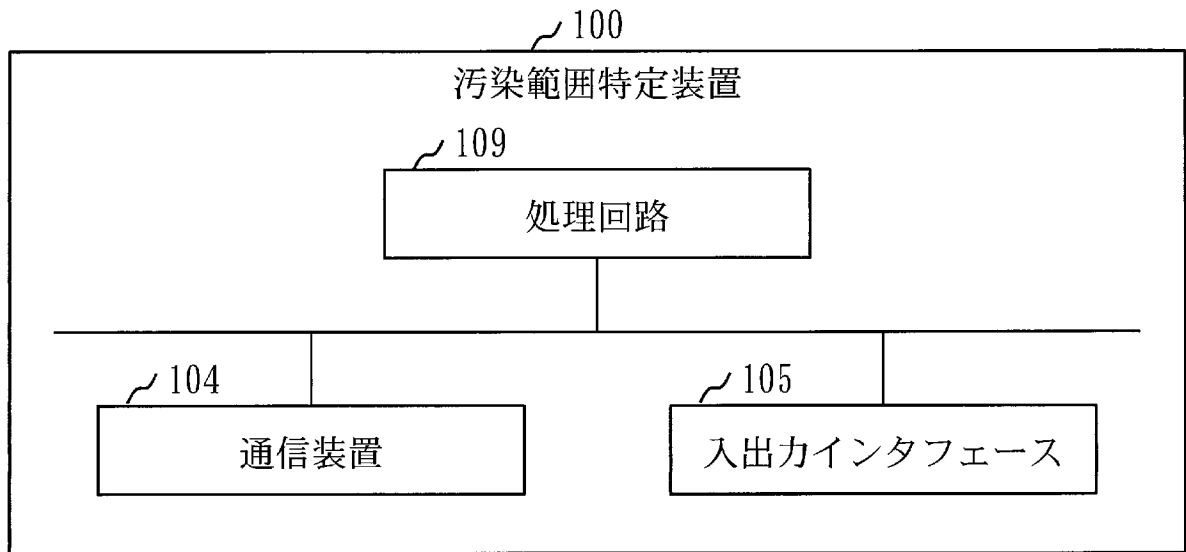
[図11]

図11



[図12]

図12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/012365

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06F21/57 (2013.01) i

FI: G06F21/57 370

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. G06F21/57, 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 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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	JP 11-259331 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 24 September 1999, paragraphs [0001]-[0048]	1, 2, 6-8 3-5
Y	WO 2019/186777 A1 (NEC CORP.) 03 October 2019, paragraphs [0015]-[0018], [0047]-[0059]	1, 2, 6-8
Y	WO 2015/140843 A1 (NEC CORP.) 24 September 2015, paragraphs [0016]-[0050], [0067]-[0108]	1, 2, 6-8
Y	WO 2016/072310 A1 (CANON ELECTRONICS INC.) 12 May 2016, paragraphs [0001]-[0160]	1, 2, 6-8
A	WO 2015/140842 A1 (NEC CORP.) 24 September 2015, paragraphs [0017]-[0051], [0085]-[0119]	1-8



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
11.08.2020

Date of mailing of the international search report
01.09.2020

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/012365

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2017/175283 A1 (MITSUBISHI ELECTRIC CORP.) 12 October 2017, paragraphs [0001]-[0110]	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2020/012365

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 11-259331 A	24.09.1999	(Family: none)	
WO 2019/186777 A1	03.10.2019	(Family: none)	
WO 2015/140843 A1	24.09.2015	US 2017/0093900 A1 paragraphs [0029]- [0067], [0086]-[0129] EP 3121723 A1	
WO 2016/072310 A1	12.05.2016	US 2017/0019415 A1 paragraphs [0001]- [0265]	
WO 2015/140842 A1	24.09.2015	US 2017/0075746 A1 paragraphs [0042]- [0088], [0124]-[0170] EP 3121725 A1 AU 2015233419 A CN 106104495 A	
WO 2017/175283 A1	12.10.2017	US 2019/0050568 A1 paragraphs [0001]- [0380] GB 2563530 A CN 109074457 A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/57(2013.01)i FI: G06F21/57 370		
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）） G06F21/57, 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 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020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 A	JP 11-259331 A（日本電信電話株式会社）24.09.1999（1999-09-24） 段落[0001]-[0048]	1,2,6-8 3-5
Y	WO 2019/186777 A1（日本電気株式会社）03.10.2019（2019-10-03） 段落[0015]-[0018], [0047]-[0059]	1,2,6-8
Y	WO 2015/140843 A1（日本電気株式会社）24.09.2015（2015-09-24） 段落[0016]-[0050], [0067]-[0108]	1,2,6-8
Y	WO 2016/072310 A1（キャノン電子株式会社）12.05.2016（2016-05-12） 段落[0001]-[0160]	1,2,6-8
A	WO 2015/140842 A1（日本電気株式会社）24.09.2015（2015-09-24） 段落[0017]-[0051], [0085]-[0119]	1-8
A	WO 2017/175283 A1（三菱電機株式会社）12.10.2017（2017-10-12） 段落[0001]-[0110]	1-8
☐ 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 11.08.2020		国際調査報告の発送日 01.09.2020
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） 中里 裕正 5S 9364 電話番号 03-3581-1101 内線 3546

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2020/012365

引用文献			公表日	パテントファミリー文献	公表日
JP	11-259331	A	24.09.1999	(ファミリーなし)	
WO	2019/186777	A1	03.10.2019	(ファミリーなし)	
WO	2015/140843	A1	24.09.2015	US 2017/0093900	A1
				段落[0029]-[0067], [0086]-[0129]	
				EP 3121723	A1
WO	2016/072310	A1	12.05.2016	US 2017/0019415	A1
				段落[0001]-[0265]	
WO	2015/140842	A1	24.09.2015	US 2017/0075746	A1
				段落[0042]-[0088], [0124]-[0170]	
				EP 3121725	A1
				AU 2015233419	A
				CN 106104495	A
WO	2017/175283	A1	12.10.2017	US 2019/0050568	A1
				段落[0001]-[0380]	
				GB 2563530	A
				CN 109074457	A