

(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 2022/149265 A1

- (51) 国際特許分類:
G06F 11/07 (2006.01) *G06F 11/34* (2006.01)
- (21) 国際出願番号: PCT/JP2021/000509
- (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: 鐘本 楊(KANEMOTO, Yo); 〒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). 芝原 俊樹(SHIBAHARA, Toshiki); 〒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). 秋山 満昭(AKIYAMA, Mitsuaki); 〒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).

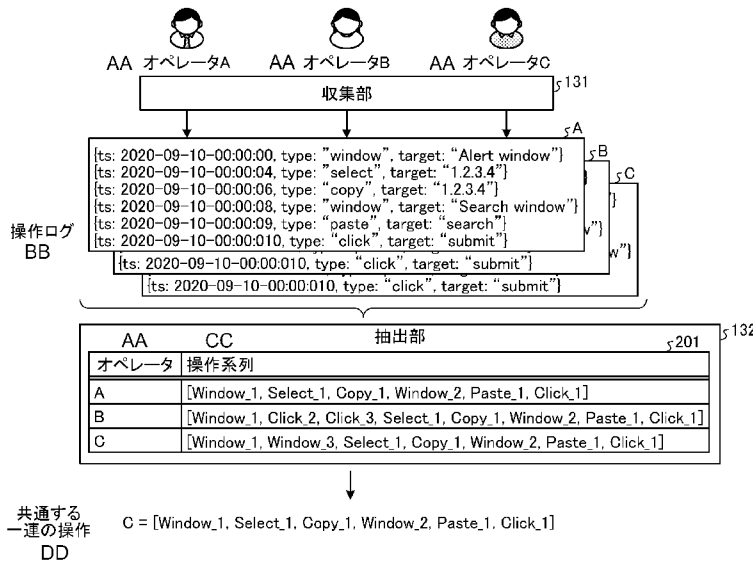
(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング Tokyo (JP).

(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,

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

(54) 発明の名称: 抽出装置、抽出方法、および、抽出プログラム

【図2】



131... COLLECTION UNIT
132... EXTRACTION UNIT
AA... OPERATOR
BB... OPERATION LOG
CC... OPERATION SEQUENCE
DD... COMMON SERIES OF OPERATIONS

(57) Abstract: This extraction device comprises a collection unit (131) and an extraction unit (132). The collection unit (131) collects, from the operating system (OS) of the computer operated by each operator, an operation log indicating the operations of the computer performed by each operator when each operator is operating the computer to perform a study. The extraction unit (132) extracts a series of operations common to each operator from the collected operation logs of the operators, and outputs the extracted series of operations. For example, the extraction unit (132) applies a maximum-length common portion string to an operation sequence indicating the series of operations of each operator, thereby extracting series of operations common to the operators.

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, 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))

(57) 要約：抽出装置は、収集部（１３１）および抽出部（１３２）を備える。収集部（１３１）は、各オペレータが操作するコンピュータのOS（Operating System）から、各オペレータがコンピュータを操作して調査を行う際における、各オペレータのコンピュータの操作を示す操作ログを収集する。抽出部（１３２）は、収集された各オペレータの操作ログから、各オペレータに共通する一連の操作を抽出し、抽出した一連の操作を出力する。例えば、抽出部（１３２）は、オペレータそれぞれの一連の操作を示す操作系列に対し、最長共通部分列を適用することにより、各オペレータに共通する一連の操作を抽出する。

明 細 書

発明の名称：抽出装置、抽出方法、および、抽出プログラム

技術分野

[0001] 本発明は、複数のオペレータに共通する一連の操作を抽出する、抽出装置、抽出方法、および、抽出プログラムに関する。

背景技術

[0002] セキュリティやネットワークのオペレーションでは、セキュリティ侵害やネットワーク障害があるか否かの判断を行うため、オペレータである人間が様々な機器から取得したログを調査することが行われている。

[0003] これらの調査には、明確な手順が示されているものもあれば、明確な手順が示されていないものもある。つまり、オペレータが行う調査手順の中には、暗黙知として存在するものもある。チームや複数名のオペレータが調査を行う際の全体的な効率性を考えると、調査手順は明示化されることが望ましい。そのため、暗黙知として存在する調査手順についても明示化されることが望ましい。

[0004] ここで、調査手順を明示化する技術として、オペレータがコンピュータを用いて調査を行う際にコンピュータの操作のログ（操作ログ）を記録し、記録された操作ログに基づき、オペレータが調査を行う際の行動モデルを作成する技術（非特許文献1参照）がある。また、オペレータによるコンピュータの操作をそのまま記録するRPA（Robotic Process Automation）技術（非特許文献2参照）がある。

先行技術文献

非特許文献

[0005] 非特許文献1：Zhong, Chen, et al., “Learning from Experts’ Experience: Towards Automated Cyber Security Data Triage”, IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity) 2016.

非特許文献2：RPA（ロボティック・プロセス・オートメーション）とは？基本から導入の進め方までまとめて解説、[online]、[2020年12月9日検索]、インターネット <URL：https://winactor.com/column/about_rpa>

発明の概要

発明が解決しようとする課題

[0006] しかし、非特許文献1に記載の技術は、独自のGUI（Graphical User Interface）操作ツールを用いる必要があるため、汎用的ではない。また、非特許文献2に記載の技術は、オペレータ個人によるコンピュータの操作をそのまま記録するものに過ぎず、複数のオペレータ間に暗黙知として共有される調査手順を明示化するものではない。

[0007] そこで、本発明は、前記した問題を解決し、独自のGUI操作ツールを用いることなく、複数のオペレータ間に暗黙知として共有される調査手順を明示化することを課題とする。

課題を解決するための手段

[0008] 前記した課題を解決するため、本発明は、各オペレータが操作するコンピュータのOS（Operating System）から、前記各オペレータがコンピュータを操作して調査を行う際における、前記各オペレータのコンピュータの操作を示す操作ログを収集する収集部と、収集された前記各オペレータの操作ログから、前記各オペレータに共通する一連の操作を抽出し、前記抽出した一連の操作を出力する抽出部と、を備えることを特徴とする。

発明の効果

[0009] 本発明によれば、独自のGUI操作ツールを用いることなく、複数のオペレータ間に暗黙知として共有される手順を明示化することができる。

図面の簡単な説明

[0010] [図1]図1は、第1の実施形態の抽出装置を含むシステムの構成例を示す図である。

[図2]図2は、第1の実施形態の抽出装置の動作概要を説明する図である。

[図3]図3は、各実施形態の抽出装置の構成例を示す図である。

[図4]図4は、図3の収集部が取得する操作および当該操作の取得対象の例を示す図である。

[図5]図5は、操作ログの例を説明する図である。

[図6]図6は、図3の抽出装置の処理手順の例を示すフローチャートである。

[図7]図7は、図6のS2の処理の例を示すフローチャートである。

[図8]図8は、操作ログの抽象化処理を説明する図である。

[図9]図9は、オペレータA、B、Cそれぞれの操作系列に対して、最長部分文字列(LCS)を複数回適用して、共通操作列Cを求める処理を説明する図である。

[図10]図10は、第2の実施形態の抽出装置の処理手順の例を示すフローチャートである。

[図11]図11は、第2の実施形態の抽出装置の処理の例を説明する図である。

[図12]図12は、第3の実施形態の抽出装置の処理手順の例を示すフローチャートである。

[図13]図13は、第3の実施形態の抽出装置の処理の例を説明する図である。

[図14]図14は、抽出プログラムを実行するコンピュータの構成例を示す図である。

発明を実施するための形態

[0011] 以下、図面を参照しながら、本発明を実施するための形態（実施形態）を第1の実施形態から第3の実施形態に分けて説明する。本発明は、各実施形態に限定されない。

[0012] [第1の実施形態]

まず、図1を用いて第1の実施形態の抽出装置を含むシステムの構成例を説明する。システムは、例えば、セキュリティ機器やネットワーク機器（機器A、B）のログを蓄積するログDBと、ログDBに蓄積されたログを用い

て調査を行うオペレータの端末装置と、抽出装置 10 とを備える。

[0013] 抽出装置 10 は、ログの調査時における各オペレータの端末装置の操作を示す操作ログを収集する。そして、抽出装置 10 は、収集した各オペレータの操作ログから、各オペレータに共通する一連の操作を抽出し、出力する。

[0014] 例えば、図 2 に示すように、抽出装置 10 の収集部 131 は、調査時におけるオペレータ A, B, C の端末装置の操作ログ（操作ログ A, B, C）を収集する。その後、抽出装置 10 の抽出部 132 は、収集されたオペレータ A, B, C それぞれの操作ログの示す操作を抽象化し、オペレータ A, B, C それぞれ操作系列を作成する。そして、抽出部 132 は、オペレータ A, B, C それぞれの操作系列に共通する一連の操作を抽出する。例えば、抽出部 132 は、オペレータ A, B, C それぞれの操作系列に最長共通部分列を適用することにより、オペレータ A, B, C に共通する一連の操作を抽出する。

[0015] これにより抽出装置 10 は、独自の GUI 操作ツールを用いることなく、複数のオペレータ間に暗黙知として共有される操作手順を明示化することできる。

[0016] 次に、図 3 を用いて、抽出装置 10 の構成例を説明する。なお、抽出装置 10 a、抽出部 132 a については、第 2 の実施形態で説明する。また、抽出装置 10 b、抽出部 132 b については、第 3 の実施形態で説明する。

[0017] 抽出装置 10 は、入出力部 11 と、記憶部 12 と、制御部 13 とを備える。入出力部 11 は、各種データの入出力を司る。例えば、入出力部 11 は、各オペレータの操作ログの入力を受け付けたり、各オペレータに共通する一連の操作の抽出結果を出力したりする。記憶部 12 は、制御部 13 が各種処理を実行する際に参照する情報を記憶する。

[0018] 制御部 13 は、抽出装置 10 全体の制御を司る。制御部 13 は、収集部 131 と、抽出部 132 とを備える。収集部 131 は、ログの調査時における各オペレータの端末装置の操作を示す操作ログを収集する。

[0019] 例えば、収集部 131 は、オペレータの端末装置の OS (Operating Syst

em) のウインドウ機能を利用して、オペレータのクリック操作やキー入力等、人間が認識することができる最小の粒度の操作を取得する。

[0020] 収集部 131 が取得する操作、操作の補足情報、当該操作による取得対象の例を図 4 に示す。なお、操作が Web ブラウザ (browser) に対する操作である場合、収集部 131 は、クリック操作やキー入力以外に、Web ページの閲覧や注目タブ切り替えの操作も取得する。

[0021] 例えば、オペレータの端末装置において、図 5 に示す符号 501 に示す Alert window と符号 502 に示す Search window とが起動している場合を考える。この場合、収集部 131 は、当該端末装置から操作ログとして符号 503 に示す情報を取得する。

[0022] この符号 503 に示す操作ログには、オペレータが、端末装置において、Alert window をアクティブウインドウとし、表示されているテキスト 1, 2, 3, 4 を選択し、コピーで文字列をクリップボードに保存し、Search window をアクティブウインドウに切り替え、クリップボードに保存されたテキストをペーストし、submit ボタンをクリックした、という一連の操作が時系列に記録されている。

[0023] 図 2 の説明に戻る。抽出部 132 は、収集部 131 により収集された各オペレータの操作ログから、各オペレータに共通する一連の操作を抽出し、出力する。

[0024] 例えば、抽出部 132 は、各オペレータの操作ログから、各オペレータの一連の操作を示す操作系列を作成する。そして、抽出部 132 は、各オペレータの操作系列に対し、最長共通部分列を適用することにより、各オペレータに共通する一連の操作を抽出する。

[0025] 例えば、抽出部 132 は、図 2 に示す操作ログ A, B, C から、オペレータ A, B, C の一連の操作を示す操作系列 201 を作成する。そして、抽出部 132 は、オペレータ A, B, C の操作系列 201 に対し、最長共通部分列を適用することにより、オペレータ A, B, C に共通する一連の操作 C を抽出する。

[0026] 例えば、抽出部 132 は、まず、オペレータ A の操作系列とオペレータ B の操作系列に対し、最長共通部分列を適用することにより、オペレータ A、B の操作系列に共通する一連の操作を抽出する。次に、抽出部 132 は、オペレータ A、B の操作系列に共通する一連の操作と、オペレータ C の操作系列とに最長共通部分列を適用することにより、オペレータ A、B、C に共通する一連の操作 C を抽出する。

[0027] [処理手順の例]

次に、図 6 を用いて、抽出装置 10 の処理手順の例を説明する。例えば、抽出装置 10 の収集部 131 は、各オペレータの端末装置から、各機器のログの調査時における各オペレータの操作ログを収集する（S1）。次に、抽出部 132 は、S1 で収集された操作ログに基づき、各オペレータに共通する一連の操作を抽出する（S2）。そして、抽出部 132 は S2 で抽出した一連の操作を出力する（S3）。

[0028] 次に、図 7 を用いて、図 6 の S2 の処理を詳細に説明する。まず、抽出部 132 は、収集部 131 により収取された操作ログに対して、抽象化処理を行う（S201）。

[0029] 例えば、抽出部 132 は、図 8 の符号 801 に示すように、操作ログにおける時刻を消去したり、数字を、数字を表す符号に置換したり、選択文字列を、文字列の型を表す符号に変換したりする。これにより、例えば、符号 802 の左側に示す操作ログは右側に示す操作ログに変換される。

[0030] 図 7 の S201 の後、抽出部 132 は、S201 で抽象化された操作ログを、その操作ログの内容を表す識別子に変換する（図 7 の S202）。

[0031] 例えば、抽出部 132 は、図 8 の符号 803 の左側に示す操作ログを、右側に示す識別子に変換する。

[0032] 以上の処理により、抽出部 132 は、各オペレータの操作ログから、各オペレータの行った操作を抽象化した操作系列を得ることができる。

[0033] 図 7 の S202 の後、抽出部 132 は、各オペレータの操作系列に対し、最長部分文字列を適用することにより、各オペレータに共通する一連の操作

を抽出する（S203）。

[0034] 例えば、抽出部132は、図9に示す、オペレータA、B、Cそれぞれの操作系列に対して、最長部分文字列（LCS）を複数回適用して、共通操作列Cを求める。そして、抽出部132は、共通操作列CをオペレータA、B、Cに共通する一連の操作とする。

[0035] このようにすることで抽出装置10は、オペレータ間での暗黙知であった、調査のための一連の操作を抽出することができる。

[0036] [第2の実施形態]

また、抽出装置は、各オペレータの操作系列から、n-gramずつ操作系列を抽出し、抽出したn-gramずつの操作系列間での共通度を求めることにより、各オペレータに共通する一連の操作を抽出してもよい。この場合の抽出装置を第2の実施形態の抽出装置10a（図3参照）として説明する。第1の実施形態と同じ構成は同じ符号を付して、説明を省略する。

[0037] 図10を用いて、図3に示す抽出装置10aにおける抽出部132aの処理手順の例を説明する。図10のS211、S212の処理は、図7のS201、S202の処理と同様なので説明を省略し、図10のS213から説明する。

[0038] S212の後、抽出部132aは、各オペレータの操作系列からn-gramずつ操作系列を抽出する（S213）。そして、抽出部132aは、各オペレータ間でのn-gramの操作系列の共通度を算出する（S214）。抽出部132は、上記のS213、S214の処理をn=[a, b]で繰り返す。

[0039] 例えば、n=[3, 3]の場合、抽出部132aは、図11の符号111に示すオペレータA、B、Cの操作系列から、符号112の左側に示すn-gram系列を抽出する。そして、抽出部132aは、抽出したn-gram系列のオペレータA、B、C間での共通度を算出する。

[0040] 図10のS214の後、抽出部132aは、S214で算出した共通度が閾値T以上のn-gramの操作系列を、各オペレータに共通する一連の操作として抽出する（S215）。

[0041] 例えば、閾値 $T = 1$ 、 0 とした場合、抽出部 132a は、図 11 の符号 112 に示す n -gram の操作系列から、符号 113 に示す操作系列をオペレータ A、B、C に共通する一連の操作として抽出する。

[0042] このようにすることでも抽出装置 10a は、オペレータ間での暗黙知であった、調査のための一連の操作を抽出することができる。

[0043] [第 3 の実施形態]

また、抽出装置は、各オペレータの操作系列から、操作の状態遷移を示す状態遷移モデルを作成し、作成した状態遷移モデルの正規表現を各オペレータに共通する一連の操作として抽出してもよい。この場合の抽出装置を第 3 の実施形態の抽出装置 10b (図 3 参照) として説明する。第 1 の実施形態、第 2 の実施形態と同じ構成は同じ符号を付して、説明を省略する。

[0044] 図 12 を用いて、図 3 に示す抽出装置 10b における抽出部 132b の処理手順の例を説明する。図 12 の S221、S222 の処理は、図 7 の S201、S202 の処理と同様なので説明を省略し、図 12 の S223 から説明する。

[0045] 図 12 の S222 の後、抽出部 132b は、各オペレータの操作系列から、操作の遷移状態を示す状態遷移モデルを作成する (S223)。

[0046] 例えば、抽出部 132b は、図 13 の符号 1301 に示すオペレータ A、B、C の操作系列から、符号 1302 に示す状態遷移モデルを作成する。

[0047] 図 12 の S223 の後、抽出部 132b は、S223 で作成した状態遷移モデルから正規表現を作成する (S224)。そして、抽出部 132b は、S224 で作成した正規表現を、各オペレータに共通する一連の操作とする (S225)。

[0048] 例えば、抽出部 132b は、図 13 の符号 1302 に示す状態遷移モデルから正規表現を作成する要領で、符号 1303 に示す共通操作を抽出する。なお、符号 1302 に示す正規表現における「*」は、何が入ってもよいことを表す。

[0049] このようにすることでも抽出装置 10b は、オペレータ間での暗黙知であ

った、調査のための一連の操作を抽出することができる。

[0050] [システム構成等]

また、図示した各部の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部又は一部を、各種の負荷や使用状況等に応じて、任意の単位で機能的又は物理的に分散・統合して構成することができる。さらに、各装置にて行われる各処理機能は、その全部又は任意の一部が、CPU及び当該CPUにて実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0051] また、前記した実施形態において説明した処理のうち、自動的に行われるものとして説明した処理の全部又は一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部又は一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

[0052] [プログラム]

前記した抽出装置10、10a、10bは、パッケージソフトウェアやオンラインソフトウェアとしてプログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記のプログラムを情報処理装置に実行させることにより、情報処理装置を各実施形態の抽出装置10、10a、10bとして機能させることができる。ここで言う情報処理装置には、デスクトップ型又はノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはスマートフォン、携帯電話機やPHS (Personal Handyphone System) 等の移動体通信端末、さらには、PDA (Personal Digital Assistant) 等の端末等がその範疇に含まれる。

[0053] また、抽出装置10、10a、10bは、ユーザが使用する端末装置をクライアントとし、当該クライアントに上記の処理に関するサービスを提供す

るサーバ装置として実装することもできる。この場合、サーバ装置は、Webサーバとして実装することとしてもよいし、アウトソーシングによって上記の処理に関するサービスを提供するクラウドとして実装することとしてもかまわない。

[0054] 図10は、抽出プログラムを実行するコンピュータの一例を示す図である。コンピュータ1000は、例えば、メモリ1010、CPU1020を有する。また、コンピュータ1000は、ハードディスクドライバインタフェース1030、ディスクドライバインタフェース1040、シリアルポートインタフェース1050、ビデオアダプタ1060、ネットワークインタフェース1070を有する。これらの各部は、バス1080によって接続される。

[0055] メモリ1010は、ROM (Read Only Memory) 1011及びRAM (Random Access Memory) 1012を含む。ROM1011は、例えば、BIOS (Basic Input Output System) 等のブートプログラムを記憶する。ハードディスクドライバインタフェース1030は、ハードディスクドライブ1090に接続される。ディスクドライバインタフェース1040は、ディスクドライブ1100に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ1100に挿入される。シリアルポートインタフェース1050は、例えばマウス1110、キーボード1120に接続される。ビデオアダプタ1060は、例えばディスプレイ1130に接続される。

[0056] ハードディスクドライブ1090は、例えば、OS1091、アプリケーションプログラム1092、プログラムモジュール1093、プログラムデータ1094を記憶する。すなわち、上記の抽出装置10, 10a, 10bが実行する各処理を規定するプログラムは、コンピュータにより実行可能なコードが記述されたプログラムモジュール1093として実装される。プログラムモジュール1093は、例えばハードディスクドライブ1090に記憶される。例えば、抽出装置10, 10a, 10bにおける機能構成と同様の

処理を実行するためのプログラムモジュール1093が、ハードディスクドライブ1090に記憶される。なお、ハードディスクドライブ1090は、SSDにより代替されてもよい。

[0057] また、上述した実施形態の処理で用いられる各データは、プログラムデータ1094として、例えばメモリ1010やハードディスクドライブ1090に記憶される。そして、CPU1020が、メモリ1010やハードディスクドライブ1090に記憶されたプログラムモジュール1093やプログラムデータ1094を必要に応じてRAM1012に読み出して実行する。

[0058] なお、プログラムモジュール1093やプログラムデータ1094は、ハードディスクドライブ1090に記憶される場合に限らず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ1100等を介してCPU1020によって読み出されてもよい。あるいは、プログラムモジュール1093及びプログラムデータ1094は、ネットワークされたーク（LAN（Local Area Network）、WAN（Wide Area Network）等）を介して接続他のコンピュータに記憶されてもよい。そして、プログラムモジュール1093及びプログラムデータ1094は、他のコンピュータから、ネットワークインタフェース1070を介してCPU1020によって読み出されてもよい。

符号の説明

[0059] 10, 10a, 10b 抽出装置

11 入出力部

12 記憶部

13 制御部

131 収集部

132 抽出部

請求の範囲

[請求項1] 各オペレータが操作するコンピュータのOS（Operating System）から、前記各オペレータがコンピュータを操作して調査を行う際における、前記各オペレータのコンピュータの操作を示す操作ログを収集する収集部と、

収集された前記各オペレータの操作ログから、前記各オペレータに共通する一連の操作を抽出し、前記抽出した一連の操作を出力する抽出部と、

を備えることを特徴とする抽出装置。

〔請求項2〕 前記抽出部は、

前記オペレータそれぞれの一連の操作を示す操作系列に対し、最長共通部分列を適用することにより、前記各オペレータに共通する一連の操作を抽出する

ことを特徴とする請求項 1 に記載の抽出装置。

〔請求項3〕 前記抽出部は、

前記オペレータそれぞれの一連の操作を示す操作系列から、n-gramずつ操作系列を抽出し、抽出したn-gramの操作系列について前記各オペレータ間での共通度が所定の閾値以上のn-gramの操作系列を、前記各オペレータに共通する一連の操作として抽出する。

ことを特徴とする請求項 1 に記載の抽出装置。

〔請求項4〕 前記抽出部は、

前記オペレータそれぞれの一連の操作を示す操作系列から、前記操作の状態遷移を示す状態遷移モデルを作成し、作成した状態遷移モデルから作成した正規表現を前記各オペレータに共通する一連の操作とする

ことを特徴とする請求項 1 に記載の抽出装置。

【請求項5】 抽出装置により実行される抽出方法であって、

各オペレータが操作するコンピュータのOS (Operating System

）から、前記各オペレータがコンピュータを操作して調査を行う際における、前記各オペレータのコンピュータの操作を示す操作ログを収集する工程と、

収集された前記各オペレータの操作ログから、前記各オペレータに共通する一連の操作を抽出し、前記抽出した一連の操作を出力する工程と、

を含むことを特徴とする抽出方法。

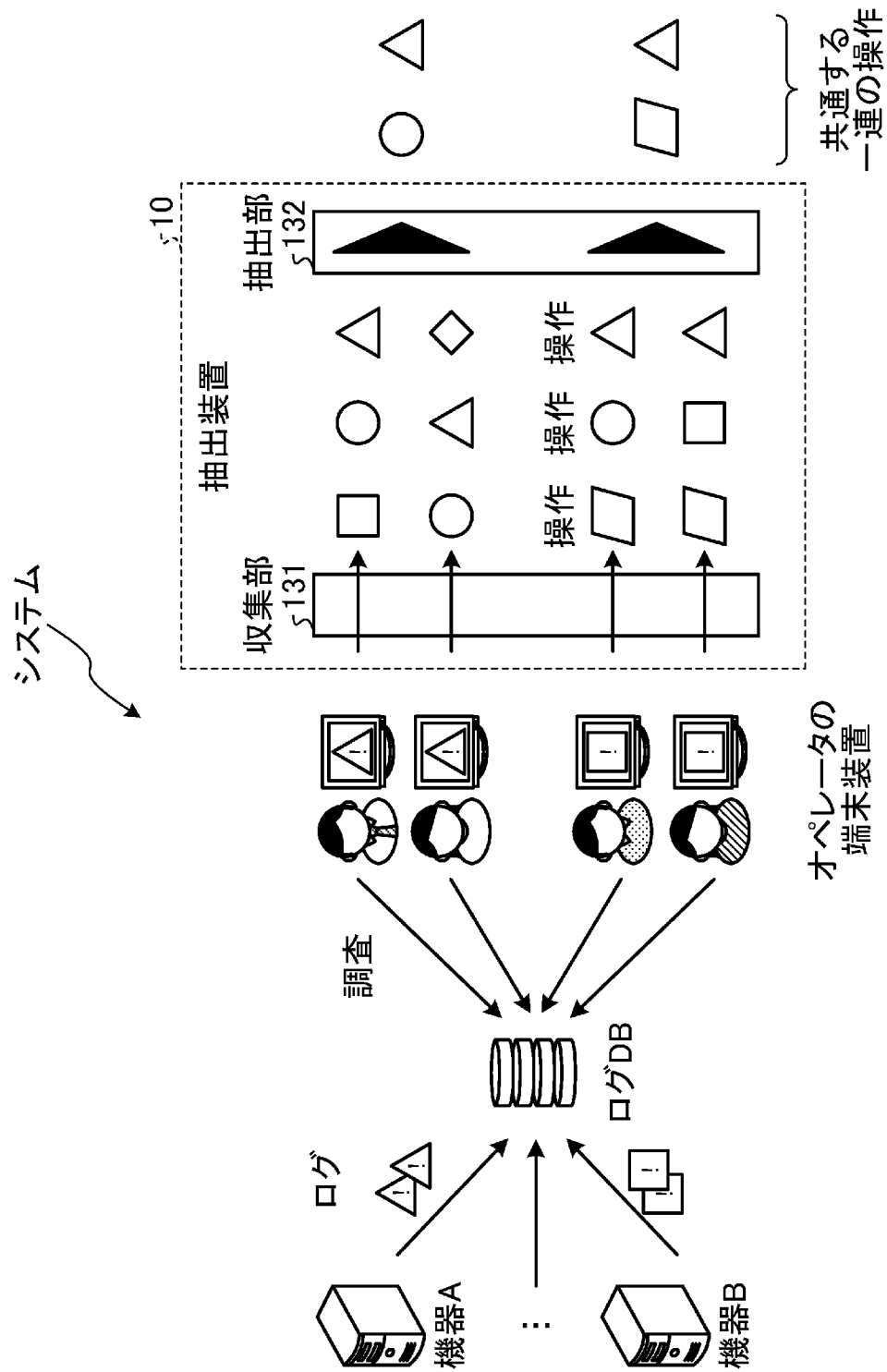
[請求項6]

各オペレータが操作するコンピュータのOS (Operating System) から、前記各オペレータがコンピュータを操作して調査を行う際における、前記各オペレータのコンピュータの操作を示す操作ログを収集する工程と、

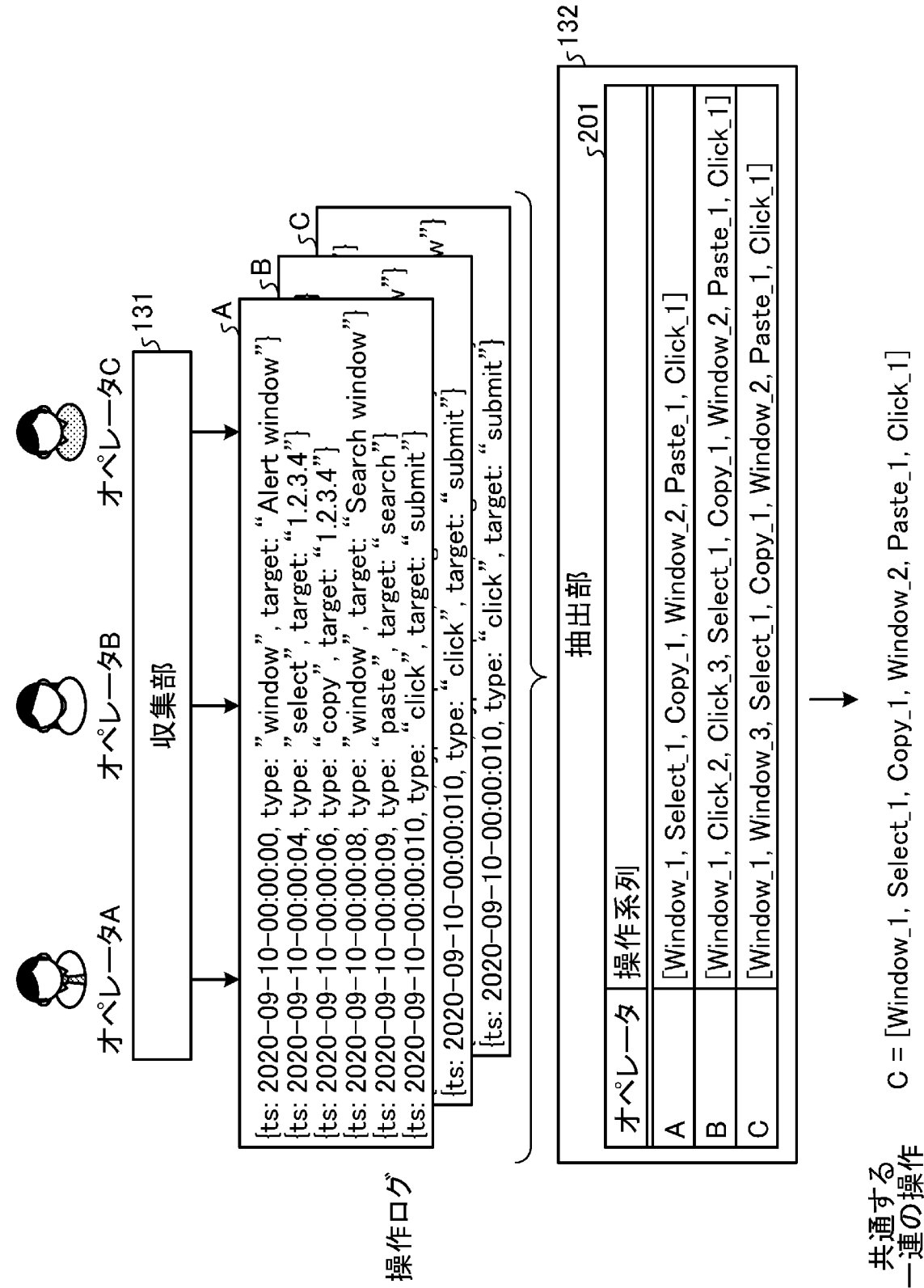
収集された前記各オペレータの操作ログから、前記各オペレータに共通する一連の操作を抽出し、前記抽出した一連の操作を出力する工程と、

をコンピュータに実行させることを特徴とする抽出プログラム。

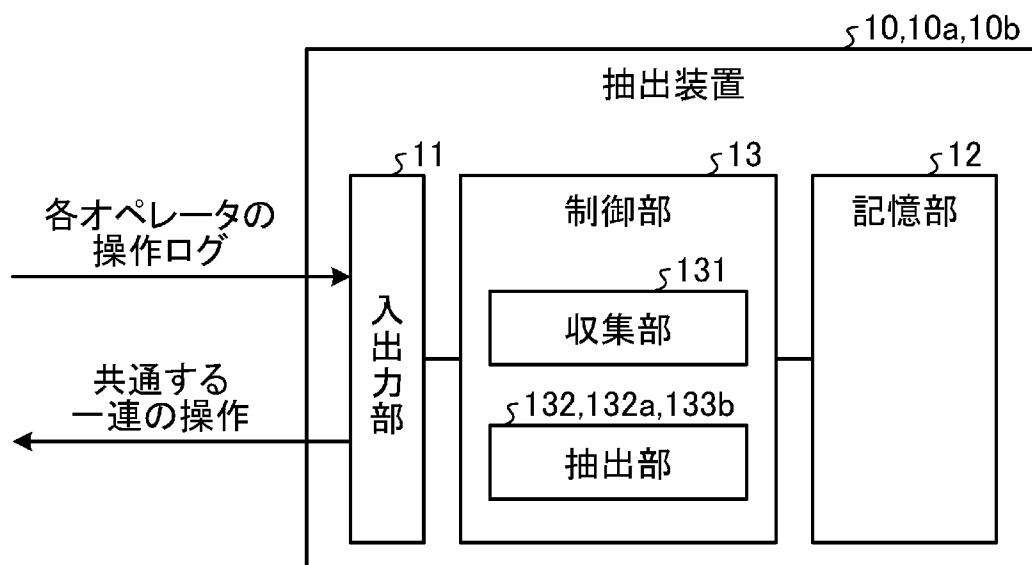
[図1]



[図2]



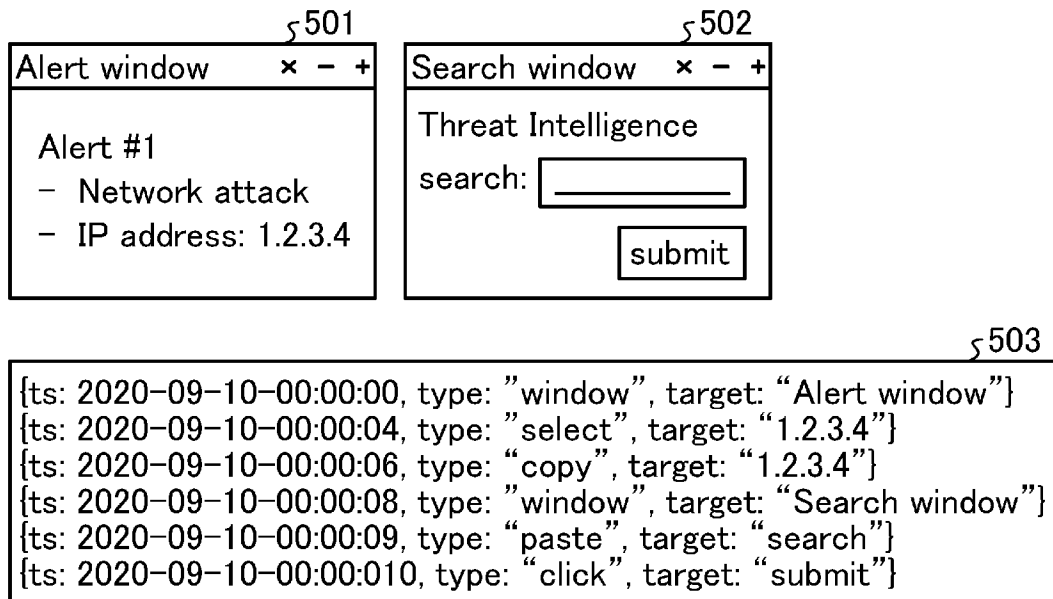
[図3]



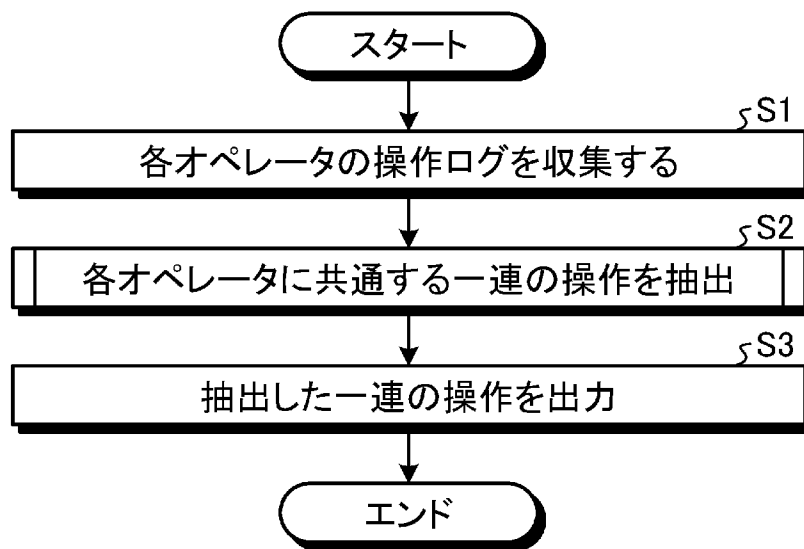
[図4]

操作		補足情報	取得対象
マウスクリック	click	・時刻 ・ボタン: (左 or 右) ・画面座標位置 ・クリック対象 ・クリック対象の画像	window browser
キー入力	key	・時刻 ・入力文字列	window browser
テキスト選択	select	・時刻 ・選択文字列	window browser
コピー・カット・ ペースト	copy, cut, paste	・時刻 ・対象文字列	window browser
スクロール	scroll	・時刻 ・スクロール割合	window browser
注目ウィンドウ変化	window	・時刻 ・ウィンドウのタイトル	window
ページ閲覧	page	・時刻 ・URL	browser
注目タブ変化	tab	・時刻 ・タブで閲覧しているWebページの URL	browser

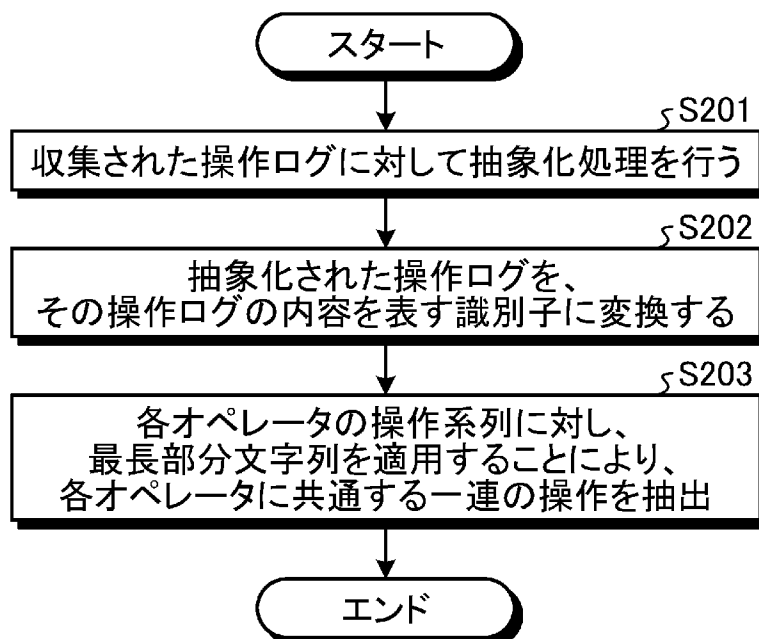
[図5]



[図6]



[図7]



[図8]

5801

操作の内容	抽象化内容
時刻	消去
数字	数字を表す符号に置換
選択文字列	文字列の型を表す符号に変換 (例: 1.2.3.4 → IPアドレス)

5802

変換前	変換後
{ts: 2020-09-10-00:00:00, type: "window", target: "Alert window"}	{type: "window", target: "Alert window"}
{ts: 2020-09-10-00:00:04, type: "select", target: "1.2.3.4"}	{type: "select", target: "1.2.3.4"}

5803

変換前	変換後
{type: "window", target: "Alert window"}	Window_1
{type: "select", target: "1.2.3.4"}	Select_1

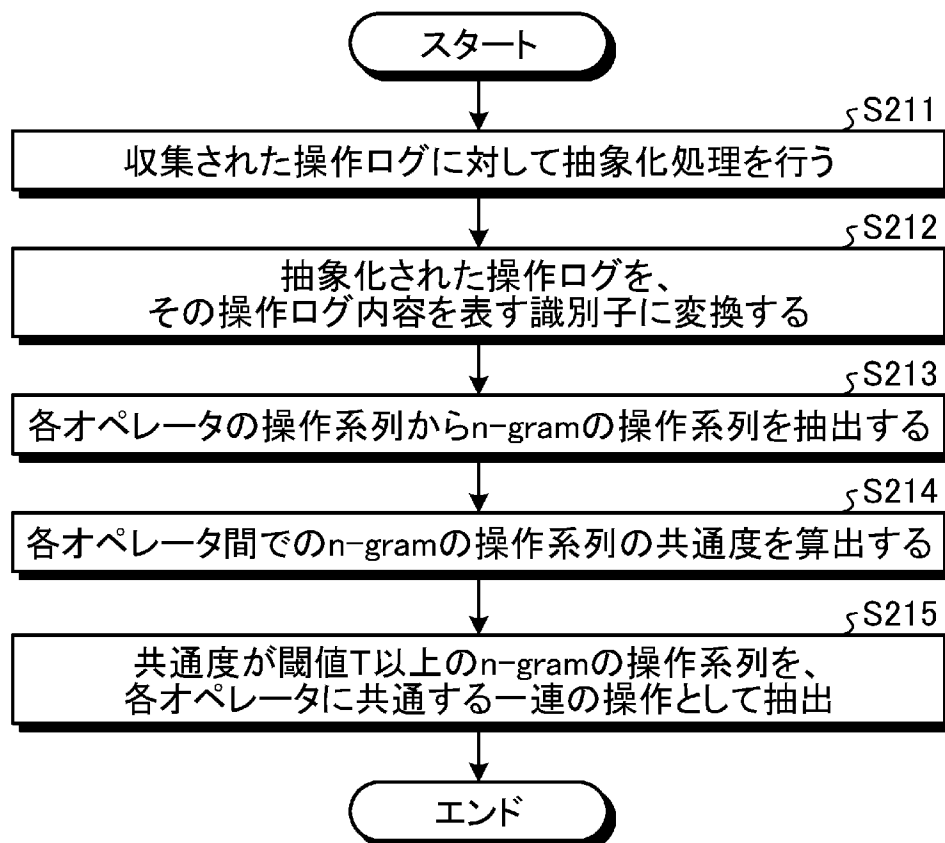
[図9]

オペレータ	操作系列
A	[Window_1, Select_1, Copy_1, Window_2, Paste_1, Click_1]
B	[Window_1, Click_2, Click_3, Select_1, Copy_1, Window_2, Paste_1, Click_1]
C	[Window_1, Window_3, Select_1, Copy_1, Window_2, Paste_1, Click_1]

↓ 共通操作列

C = [Window_1, Select_1, Copy_1, Window_2, Paste_1, Click_1]

[図10]



[図11]

5111

オペレータ	操作系列
A	[Window_1, Select_1, Copy_1, Window_2, Paste_1, Click_1]
B	[Window_1, Click_2, Click_3, Select_1, Copy_1, Window_2, Paste_1, Click_1]
C	[Window_1, Window_3, Select_1, Copy_1, Window_2, Paste_1, Click_1]

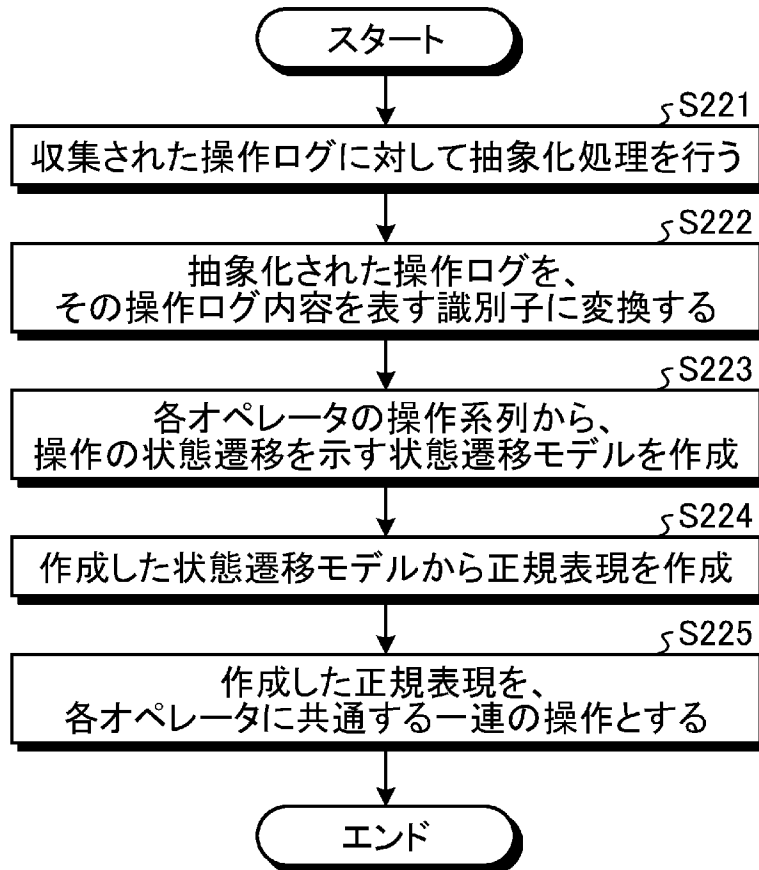
5112

n-gram操作系列	共通度
[Window_1, Select_1, Copy_1]	1/3
[Select_1, Copy_1, Window_2]	3/3
[Copy_1, Window_2, Paste_1]	3/3
[Window_2, Paste_1, Click_1]	3/3
[Window_1, Click_2, Click_3]	1/3
[Click_2, Click_3, Select_1]	1/3
[Click_3, Select_1, Copy_1]	1/3
[Window_1, Window_3, Select_1]	1/3
[Window_3, Select_1, Copy_1]	1/3

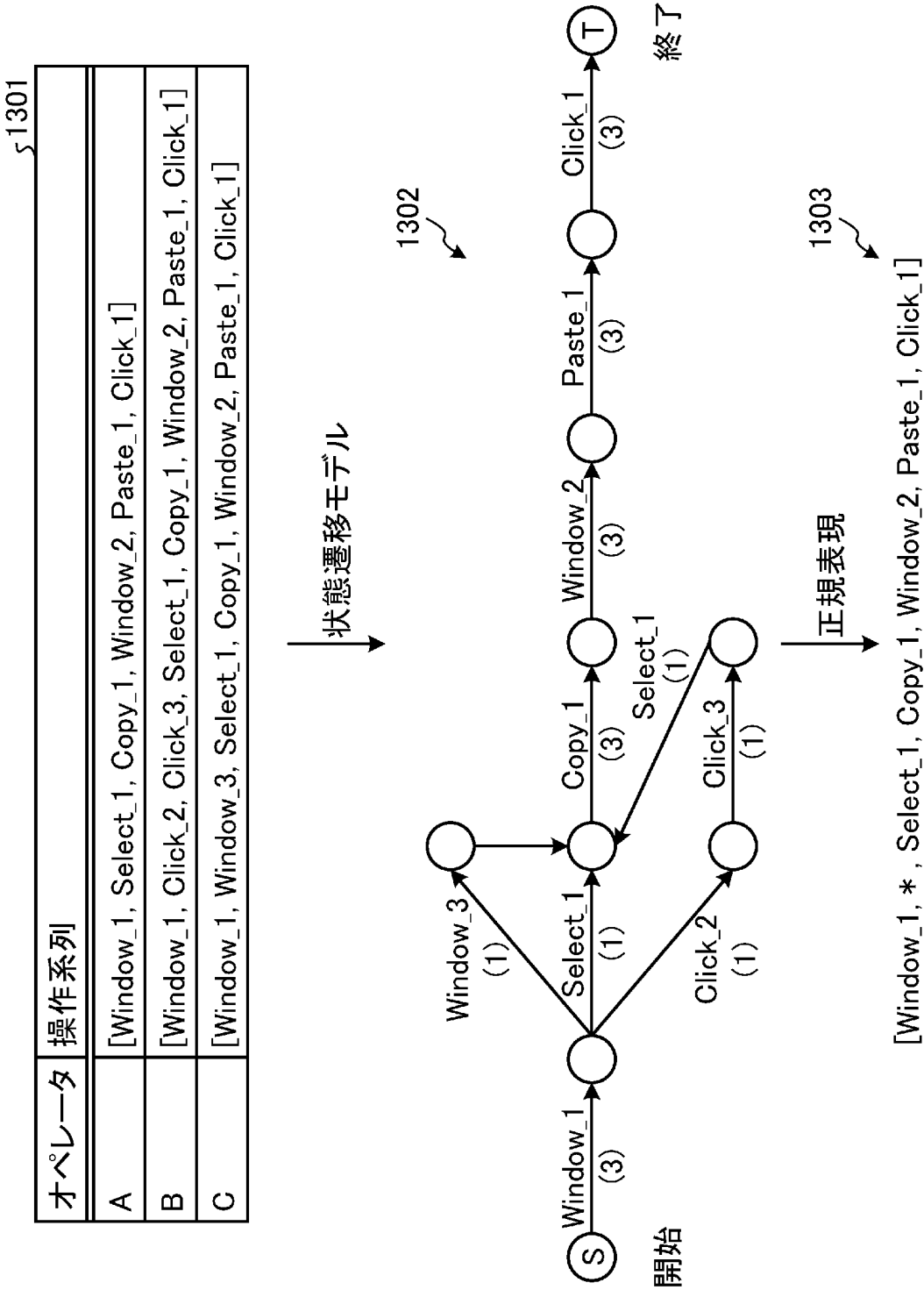
5113

[Select_1, Copy_1, Window_2]	3/3
[Copy_1, Window_2, Paste_1]	3/3
[Window_2, Paste_1, Click_1]	3/3

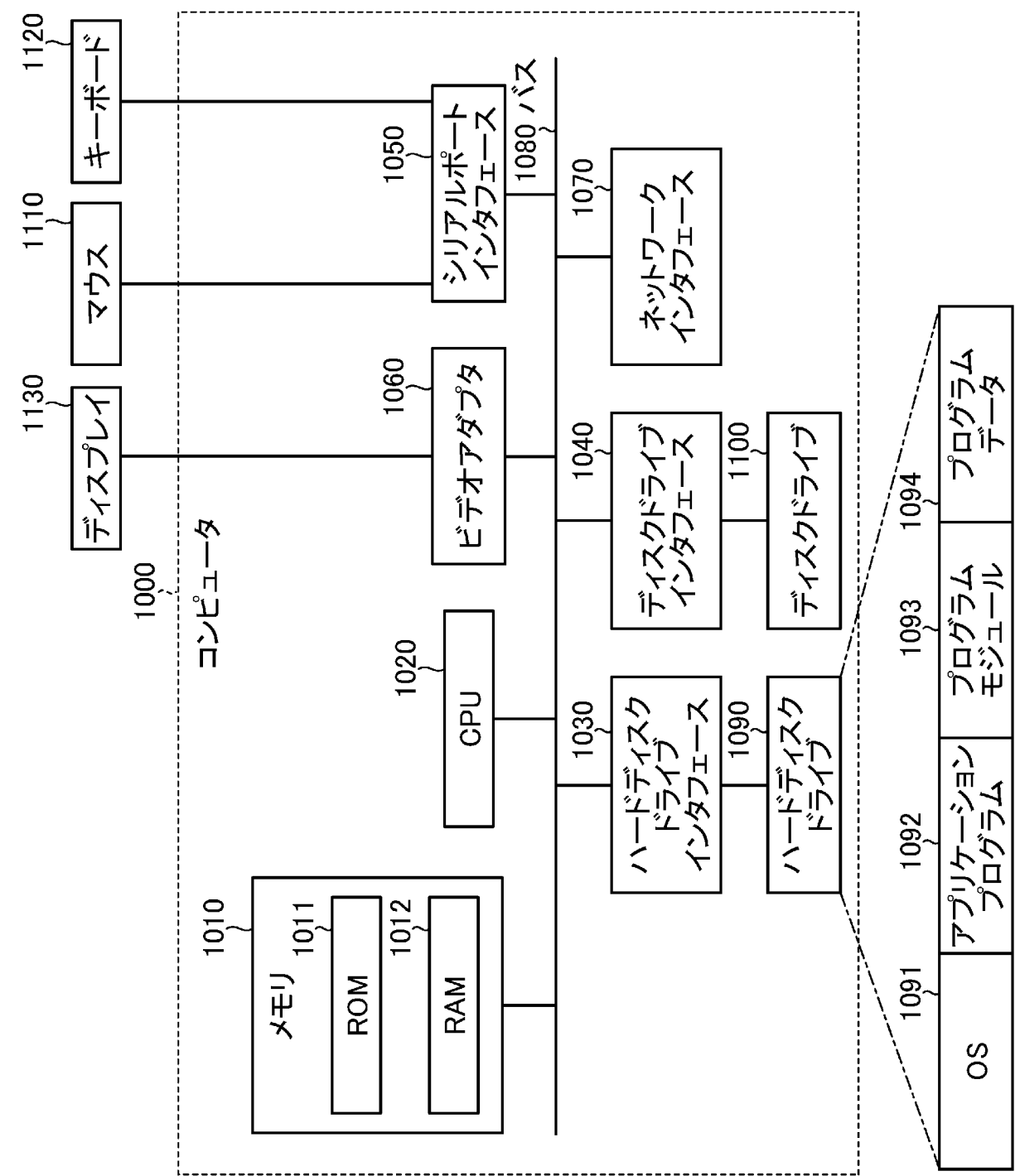
[図12]



[図13]



[図14]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/000509

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F11/07 (2006.01) i, G06F11/34 (2006.01) i
FI: G06F11/34176, G06F11/07193

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. G06F11/07, 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.
A	US 2019/0057148 A1 (BEIJING HANSIGHT TECH CO., LTD.) 21 February 2019 (2019-02-21), entire text, all drawings	1-6
A	JP 2006-259891 A (NEC CORPORATION) 28 September 2006 (2006-09-28), entire text, all drawings	1-6
A	JP 2013-54000 A (CLARION CO., LTD.) 21 March 2013 (2013-03-21), paragraphs [0068], [0069]	1-6
A	渡邊 暁 ほか, 故障対応の把握に向けた作業ログにおける大量対処分岐点の特定, 電子情報通信学会技術研究報告, 30 June 2016, vol. 116, no. 124, pp. 27-32, ISSN 0913-5685, entire text, all drawings, (WATANABE, Akio et al., Multiple isolating actions extraction from action logs for clarifying trouble-shooting process, IEICE Technical Report)	1-6

☐ 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
14 April 2021

Date of mailing of the international search report
27 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.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/000509

US 2019/0057148 A1	21 February 2019	WO 2017/067364 A1	
		entire text, all drawings	
		CN 106610965 A	
		entire text, all drawings	
JP 2006-259891 A	28 September 2006	(Family: none)	
JP 2013-54000 A	21 March 2013	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 11/07(2006.01)i; G06F 11/34(2006.01)i FI: G06F11/34 176; G06F11/07 193		
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）） G06F11/07; 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
A	US 2019/0057148 A1 (BEIJING HANSIGHT TECH CO., LTD.,) 21.02.2019 (2019-02-21) 全文, 全図	1-6
A	JP 2006-259891 A (日本電気株式会社) 28.09.2006 (2006-09-28) 全文, 全図	1-6
A	JP 2013-54000 A (クラリオン株式会社) 21.03.2013 (2013-03-21) [0068] - [0069]	1-6
A	渡邊 暁 ほか, 故障対応の把握に向けた作業ログにおける複数の対処分岐点の特定, 電子情報通信学会技術研究報告, 2016.06.30, Vol.116, No.124, p.27-32, ISSN 0913-5685 全文, 全図	1-6
☐ 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、一般的な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 14.04.2021		国際調査報告の発送日 27.04.2021
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） 石川 亮 5B 3351 電話番号 03-3581-1101 内線 3545

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/JP2021/000509

引用文献			公表日	パテントファミリー文献	公表日
US	2019/0057148	A1	21.02.2019	W0 2017/067364 A1 全文, 全図 CN 106610965 A 全文, 全図	
JP	2006-259891	A	28.09.2006	(ファミリーなし)	
JP	2013-54000	A	21.03.2013	(ファミリーなし)	