

(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11月17日(17.11.2022)



(10) 国際公開番号

WO 2022/239235 A1

(51) 国際特許分類:
H04L 12/26 (2006.01)

(21) 国際出願番号: PCT/JP2021/018420

(22) 国際出願日: 2021年5月14日(14.05.2021)

(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: 胡 博(**HU, Bo**); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ

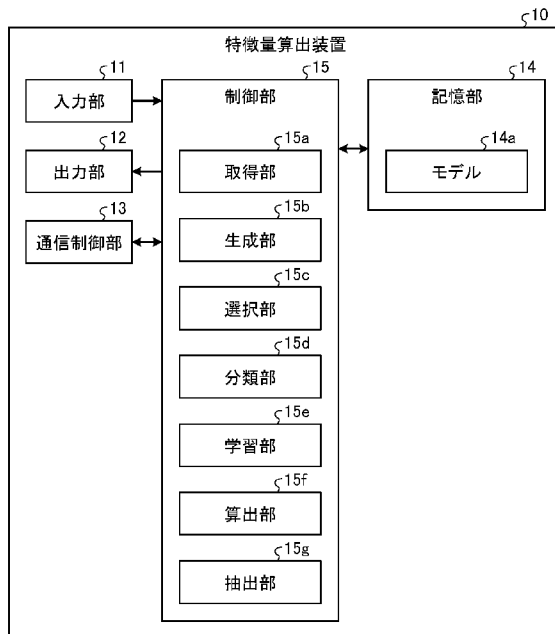
内 Tokyo (JP). 神谷 和憲(**KAMIYA, Kazunori**); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP).

(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,

(54) **Title:** FEATURE QUANTITY CALCULATION DEVICE, FEATURE QUANTITY CALCULATION METHOD, AND FEATURE QUANTITY CALCULATION PROGRAM

(54) 発明の名称: 特徴量算出装置、特徴量算出方法および特徴量算出プログラム



- 10 Feature quantity calculation device
- 11 Input unit
- 12 Output unit
- 13 Communication control unit
- 14 Storage unit
- 14a Model
- 15 Control unit
- 15a Acquisition unit
- 15b Generation unit
- 15c Selection unit
- 15d Classification unit
- 15e Learning unit
- 15f Calculation unit
- 15g Extraction unit

(57) **Abstract:** In the present invention, a generation unit (15b) generates, using communication information between network nodes, a graph that represents communication between the nodes. A selection unit (15c) selects associated nodes, among the nodes of the generated graph, that are connected by a path having a prescribed length. A classification unit (15d) classifies the selected nodes that are within a prescribed distance on the path into a group that corresponds to the node-to-node distance. A learning unit (15e) learns, for each of the classified groups, a model (14a) that represents a

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, 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))

feature quantity in the graph of the nodes within the group. A calculation unit (15f) synthesizes, for each of the selected nodes, feature quantities estimated using the model (14a) that has been learned for each group, thereby calculating a feature quantity.

(57) 要約：生成部（15b）が、ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する。選択部（15c）が、生成されたグラフのノードのうち、所定長のパスで接続された関連するノードを選択する。分類部（15d）が、選択されたノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する。学習部（15e）が、分類されたグループごとに、グループ内の各ノードのグラフでの特徴量を表すモデル（14a）を学習する。算出部（15f）が、選択されたノードのそれぞれについて、各グループで学習されたモデル（14a）を用いて推定された特徴量を合成することにより、特徴量を算出する。

明 細 書

発明の名称：

特徴量算出装置、特徴量算出方法および特徴量算出プログラム

技術分野

[0001] 本発明は、特徴量算出装置、特徴量算出方法および特徴量算出プログラムに関する。

背景技術

[0002] 悪意のあるプログラムによって乗っ取られた悪性サーバで構成されるボットネットと呼ばれるネットワークの構造は多様であり、悪性サーバ間の最短距離も、構造に応じて多様である。近年、このようなボットネットの構造を検知する技術が期待されている。IPホストをノードとし、IPホスト間のエンドツーエンド通信をエッジとするグラフの特徴量は、ボットネットの構造を検知するために有用な情報となる。

[0003] そこで、ネットワークフロー情報からなる通信グラフからノードの特徴量を学習するgraph embeddingと呼ばれる技術が知られている。例えば、グラフからノードのパスを生成し、パス上の所定ホップ数以内のノード間の類似性を学習することができる（非特許文献1参照）。

先行技術文献

非特許文献

[0004] 非特許文献1：Bryan Perozzi et al., “DeepWalk: Online Learning of Social Representations”, KDD '14, Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery, 2014年

発明の概要

発明が解決しようとする課題

[0005] しかしながら、従来の技術では、質の高い特徴量を学習することが困難である。例えば、あるノードに着目した場合に、一定距離内の隣接ノードが持

つコンテキストが距離によって異なるため、コンテキストが異なるノードを同時に学習することにより、得られた特徴量の質が低下するという問題がある。

[0006] 本発明は、上記に鑑みてなされたものであって、通信ネットワークを表すグラフから質の高い特徴量を学習することを目的とする。

課題を解決するための手段

[0007] 上述した課題を解決し、目的を達成するために、本発明に係る特徴量学習装置は、ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する生成部と、生成された前記グラフのノードのうち、所定長のパスで接続された関連するノードを選択する選択部と、選択された前記ノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する分類部と、分類された前記グループごとに、グループ内の各ノードの前記グラフでの特徴量を表すモデルを学習する学習部と、選択された前記ノードのそれぞれについて、各グループで学習されたモデルを用いて推定された特徴量を合成することにより、特徴量を算出する算出部と、を有することを特徴とする。

発明の効果

[0008] 本発明によれば、通信ネットワークを表すグラフから質の高い特徴量を学習することが可能となる。

図面の簡単な説明

[0009] [図1]図1は、特徴量算出装置の概略構成を例示する模式図である。
[図2]図2は、特徴量算出装置の処理を説明するための図である。
[図3]図3は、特徴量算出装置の処理を説明するための図である。
[図4]図4は、特徴量算出装置の処理を説明するための図である。
[図5]図5は、特徴量算出処理手順を示すフローチャートである。
[図6]図6は、特徴量算出プログラムを実行するコンピュータを例示する図である。

発明を実施するための形態

[0010] 以下、図面を参照して、本発明の一実施形態を詳細に説明する。なお、この実施形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。

[0011] [特徴量算出装置の構成]

図1は、特徴量算出装置の概略構成を例示する模式図である。また、図2～図4は、特徴量算出装置の処理を説明するための図である。まず、図1に例示するように、特徴量算出装置10は、パソコン等の汎用コンピュータで実現され、入力部11、出力部12、通信制御部13、記憶部14、および制御部15を備える。

[0012] 入力部11は、キーボードやマウス等の入力デバイスを用いて実現され、操作者による入力操作に対応して、制御部15に対して処理開始などの各種指示情報を入力する。出力部12は、液晶ディスプレイなどの表示装置、プリンター等の印刷装置等によって実現される。

[0013] 通信制御部13は、NIC (Network Interface Card) 等で実現され、ネットワークを介したサーバ等の外部の装置と制御部15との通信を制御する。例えば、通信制御部13は、ネットワークの通信情報を収集し管理する管理装置等と制御部15との通信を制御する。

[0014] 記憶部14は、RAM (Random Access Memory)、フラッシュメモリ (Flash Memory) 等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。記憶部14には、特徴量算出装置10を動作させる処理プログラムや、処理プログラムの実行中に使用されるデータなどが予め記憶され、あるいは処理の都度一時的に記憶される。例えば、記憶部14は、後述する学習部の処理結果のモデル14a等を記憶する。なお、記憶部14は、通信制御部13を介して制御部15と通信する構成でもよい。

[0015] 制御部15は、CPU (Central Processing Unit) 等を用いて実現され、メモリに記憶された処理プログラムを実行する。これにより、制御部15

は、図 1 に例示するように、取得部 15 a、生成部 15 b、選択部 15 c、分類部 15 d、学習部 15 e、算出部 15 f および抽出部 15 g として機能する。なお、これらの機能部は、それぞれあるいは一部が異なるハードウェアに実装されてもよい。例えば、学習部 15 e と算出部 15 f とは異なるハードウェアに実装されてもよい。また、制御部 15 は、その他の機能部を備えてもよい。

[0016] 取得部 15 a は、収集されたネットワークのノードの通信情報を取得する。例えば、取得部 15 a は、後述する特徴量算出処理の処理対象の IP ホストのフロー情報等を、入力部 11 あるいは通信制御部 13 を介して、ネットワークの通信情報を収集し管理する管理装置等から取得する。なお、取得部 15 a は、取得したデータを記憶部 14 に記憶させてもよい。あるいは、取得部 15 a は、これらの情報を記憶部 14 に記憶させずに、以下に説明する生成部 15 b に転送してもよい。

[0017] 生成部 15 b は、ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する。例えば、生成部 15 b は、図 2 に示すように、取得した IP ホストのフロー情報を用いて、IP ホストをノードとし、IP ホスト間の通信をエッジとするグラフを作成する。図 2 には、悪性 (Bot) サーバと C & C (Command and Control) サーバとの通信グラフが例示されている。

[0018] 選択部 15 c は、生成されたグラフのノードのうち、所定長のパスで接続された関連するノードを選択する。例えば、選択部 15 c は、各ノードを起点として Random Walk を所定回数実行し、起点としたノードごとに、ノードを含む所定長のパスを生成する。

[0019] 分類部 15 d は、選択されたノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する。例えば、分類部 15 d は、図 2 に示したグラフについて、図 3 に示すように、ノードペア A-C を距離 1 のグループに、ノードペア A-B を距離 2 のグループに、ノードペア A-E を距離 3 のグループに分類する。

- [0020] 学習部15eは、図4(a)に示すように、分類されたグループごとに、グループ内の各ノードのグラフでの特徴量を表すモデル14aを学習する。本実施形態では、学習部15eは、分類されたグループごとに異なるモデル14aを学習する。
- [0021] 学習部15eは、さらに、分類されたグループのうち、所定の距離の範囲の複数のグループについて、共通のモデル14aを学習してもよい。例えば、図4(a)に例示したグループのうち、距離2以下の複数のグループ、すなわち、距離1のグループと距離2のグループとにおいて、共通のモデル14aを学習するようにしてもよい。この場合に、学習部15eは、原則として各グループが異なるモデル14aを学習することとし、共通のモデル14aを学習する複数のグループを選択できるようにしてもよい。
- [0022] 算出部15fは、選択されたノードのそれぞれについて、各グループで学習されたモデル14aを用いて推定された特徴量を合成することにより、特徴量を算出する。例えば、算出部15fは、図4(b)に示すように、ノードごとに、各グループで学習された各モデル14aが出力する特徴量のすべてを結合して、当該ノードの特徴量とする。
- [0023] 抽出部15gは、算出された特徴量のうち、所定のしきい値以上の重要度の次元の値を抽出する。具体的には、抽出部15gは、教師データと学習されたモデル14aとを用いて、各ノードの特徴量を表す特徴ベクトルの次元ごとの重要度を算出する。例えば、抽出部15gは、Random Forestにより、各次元の重要度を算出する。そして、抽出部15gは、図4(c)に示すように、重要度が所定のしきい値以上の重要な次元のみを選択して、当該ノードの特徴量とする。
- [0024] また、抽出部15gは、出力部12を介して、算出された各ノードの特徴量を出力する。なお、抽出部15gに変えて、あるいは抽出部15gに加えて、算出部15fが算出した各ノードの特徴量を出力してもよい。
- [0025] [特徴量算出処理]

次に、図5を参照して、本実施形態に係る特徴量算出装置10による特徴

量算出処理について説明する。図5は、特徴量算出処理手順を示すフローチャートである。図5のフローチャートは、例えば、特徴量算出処理の開始を指示する操作入力があったタイミングで開始される。

[0026] まず、取得部15aが取得したネットワークのノードの通信情報を用いて、生成部15bがノード間の通信を表すグラフを生成する（ステップS1）。

[0027] また、選択部15cが、生成されたグラフのノードのうち、所定長のパスで接続された関連するノードを選択する（ステップS2）。また、分類部15dが、選択されたノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する（ステップS3）。

[0028] 次に、学習部15eが、分類されたグループごとに、グループ内の各ノードのグラフでの特徴量を表すモデル14aを学習する（ステップS4）。

[0029] その際に、学習部15eは、分類されたグループごとに異なるモデル14aを学習する。あるいは、学習部15eは、分類されたグループのうち、所定の距離の範囲の複数のグループについて、共通のモデル14aを学習してもよい。

[0030] そして、算出部15fが、選択されたノードのそれぞれについて、各グループで学習されたモデル14aを用いて推定された特徴量を合成することにより、特徴量を算出する（ステップS5）。

[0031] また、抽出部15gは、教師データと学習されたモデル14aとを用いて、各ノードの特徴量を表す特徴ベクトルの次元ごとの重要度を算出する。そして、抽出部15gは、重要度が所定のしきい値以上の重要な次元のみを抽出して、当該ノードの特徴量とする（ステップS6）。

[0032] また、抽出部15gが、出力部12を介して、各ノードの特徴量を出力する（ステップS7）。これにより、一連の特徴量算出処理が終了する。

[0033] 以上、説明したように、特徴量算出装置10において、生成部15bが、ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する。また、選択部15cが、生成されたグラフのノードのうち、所

定長のパスで接続された関連するノードを選択する。また、分類部 15 d が、選択されたノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する。また、学習部 15 e が、分類されたグループごとに、グループ内の各ノードのグラフでの特徴量を表すモデル 14 a を学習する。そして、算出部 15 f が、選択されたノードのそれぞれについて、各グループで学習されたモデル 14 a を用いて推定された特徴量を合成することにより、特徴量を算出する。

[0034] このように特徴量算出装置 10 は、ノード間の距離に応じて教師データを分割し、それぞれの距離のノード間の類似性を学習し、異なる距離のそれぞれで学習した各ノードの特徴量を合成することにより、各ノードの特徴量を算出する。これにより、隣接ノードの持つコンテキストの距離による違いを考慮して、ノードの特徴量を算出することができる。したがって、特徴量算出装置 10 は、通信ネットワークを表すグラフから質の高い特徴量を学習することが可能となる。

[0035] また、学習部 15 e が、分類されたグループごとに異なるモデル 14 a を学習する。これにより、特徴量算出装置 10 は、モデル 14 a 学習がより高精度に可能となる。

[0036] また、学習部 15 e は、分類されたグループのうち、所定の距離の範囲の複数のグループについて、共通のモデル 14 a を学習する。これにより、特徴量算出装置 10 は、モデル 14 a の学習が高効率に可能となる。

[0037] また、抽出部 15 g は、教師データと学習されたモデル 14 a とを用いて、各ノードの特徴量を表す特徴ベクトルの次元ごとの重要度を算出する。そして、抽出部 15 g が、算出された特徴量のうち、所定のしきい値以上の重要度の次元の値を抽出する。これにより、特徴量算出装置 10 は、各ノードの質の高い特徴量を効率よく算出することが可能となる。

[0038] [プログラム]

上記実施形態に係る特徴量算出装置 10 が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。一実施形態

として、特徴量算出装置１０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上記の特徴量算出処理を実行する特徴量算出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、上記の特徴量算出プログラムを情報処理装置に実行させることにより、情報処理装置を特徴量算出装置１０として機能させることができる。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）等のスレート端末等がその範疇に含まれる。また、特徴量算出装置１０の機能を、クラウドサーバに実装してもよい。

[0039] 図６は、特徴量算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と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有する。これらの各部は、バス１０８０によって接続される。

[0040] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１およびＲＡＭ１０１２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ブインタフェース１０３０は、ハードディスクドライブ１０３１に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１０４１に接続される。ディスクドライブ１０４１には、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挿入される。シリアルポートインタフェース１０５０には、例えば、マウス１０５１およびキーボード１０５２が接続される。ビデオアダプタ１０６０には、例えば、ディスプレイ１０６１が接続される。

[0041] ここで、ハードディスクドライブ１０３１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およびプログラムデータ１０９４を記憶する。上記実施形態で説明した各情報は、

例えばハードディスクドライブ１０３１やメモリ１０１０に記憶される。

[0042] また、特徴量算出プログラムは、例えば、コンピュータ１０００によって実行される指令が記述されたプログラムモジュール１０９３として、ハードディスクドライブ１０３１に記憶される。具体的には、上記実施形態で説明した特徴量算出装置１０が実行する各処理が記述されたプログラムモジュール１０９３が、ハードディスクドライブ１０３１に記憶される。

[0043] また、特徴量算出プログラムによる情報処理に用いられるデータは、プログラムデータ１０９４として、例えば、ハードディスクドライブ１０３１に記憶される。そして、ＣＰＵ１０２０が、ハードディスクドライブ１０３１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、上述した各手順を実行する。

[0044] なお、特徴量算出プログラムに係る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１０３１に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ１０４１等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、特徴量算出プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ＬＡＮ（Local Area Network）やＷＡＮ（Wide Area Network）等のネットワークを介して接続された他のコンピュータに記憶され、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。

[0045] 以上、本発明者によってなされた発明を適用した実施形態について説明したが、本実施形態による本発明の開示の一部をなす記述および図面により本発明は限定されることはない。すなわち、本実施形態に基づいて当業者等によりなされる他の実施形態、実施例および運用技術等は全て本発明の範疇に含まれる。

符号の説明

[0046] １０ 特徴量算出装置
 １１ 入力部

- 1 2 出力部
- 1 3 通信制御部
- 1 4 記憶部
- 1 4 a モデル
- 1 5 制御部
- 1 5 a 取得部
- 1 5 b 生成部
- 1 5 c 選択部
- 1 5 d 分類部
- 1 5 e 学習部
- 1 5 f 算出部
- 1 5 g 抽出部

請求の範囲

- [請求項1] ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する生成部と、
- 生成された前記グラフのノードのうち、所定長のパスで接続された関連するノードを選択する選択部と、
- 選択された前記ノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する分類部と、
- 分類された前記グループごとに、グループ内の各ノードの前記グラフでの特徴量を表すモデルを学習する学習部と、
- 選択された前記ノードのそれぞれについて、各グループで学習されたモデルを用いて推定された特徴量を合成することにより、特徴量を算出する算出部と、
- を有することを特徴とする特徴量算出装置。
- [請求項2] 前記学習部は、分類された前記グループごとに異なるモデルを学習することを特徴とする請求項1に記載の特徴量算出装置。
- [請求項3] 前記学習部は、分類された前記グループのうち、所定の距離の範囲の複数のグループについて、共通のモデルを学習することを特徴とする請求項2に記載の特徴量算出装置。
- [請求項4] 算出された前記特徴量のうち、所定のしきい値以上の重要度の次元の値を抽出する抽出部を、さらに有することを特徴とする請求項1に記載の特徴量算出装置。
- [請求項5] 前記抽出部は、教師データと学習された前記モデルとを用いて、各ノードの特徴量を表す特徴ベクトルの次元ごとの重要度を算出することを特徴とする請求項4に記載の特徴量算出装置。
- [請求項6] 特徴量算出装置が実行する特徴量算出方法であって、
- ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する生成工程と、
- 生成された前記グラフのノードのうち、所定長のパスで接続された

関連するノードを選択する選択工程と、

選択された前記ノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する分類工程と、

分類された前記グループごとに、グループ内の各ノードの前記グラフでの特徴量を表すモデルを学習する学習工程と、

選択された前記ノードのそれぞれについて、各グループで学習されたモデルを用いて推定された特徴量を合成することにより、特徴量を算出工程と、

を含んだことを特徴とする特徴量算出方法。

[請求項7]

コンピュータに

ネットワークのノード間の通信情報を用いて、ノード間の通信を表すグラフを生成する生成ステップと、

生成された前記グラフのノードのうち、所定長のパスで接続された関連するノードを選択する選択ステップと、

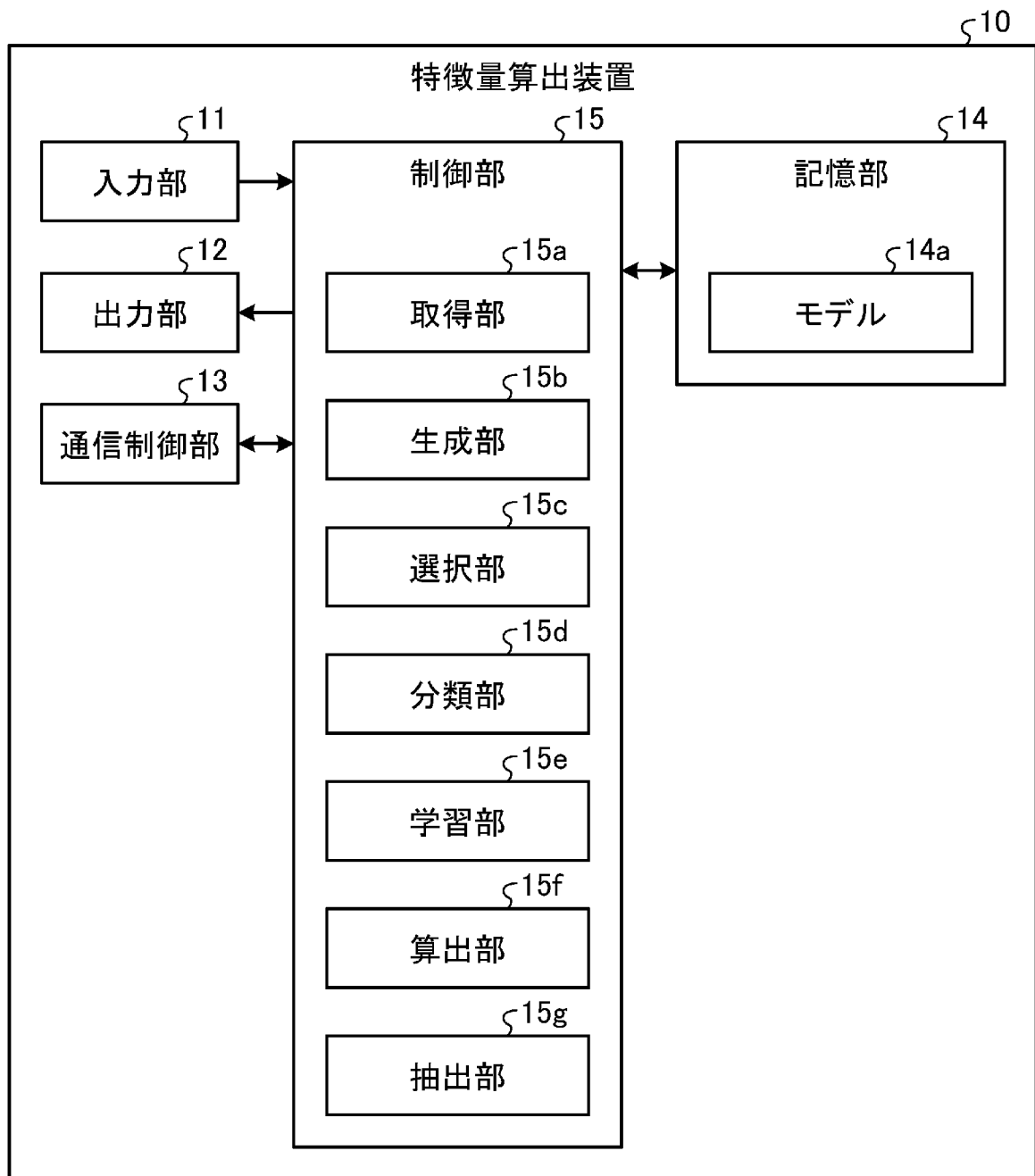
選択された前記ノードに対して、パス上の所定距離内のノード同士をノード間の距離に応じたグループに分類する分類ステップと、

分類された前記グループごとに、グループ内の各ノードの前記グラフでの特徴量を表すモデルを学習する学習ステップと、

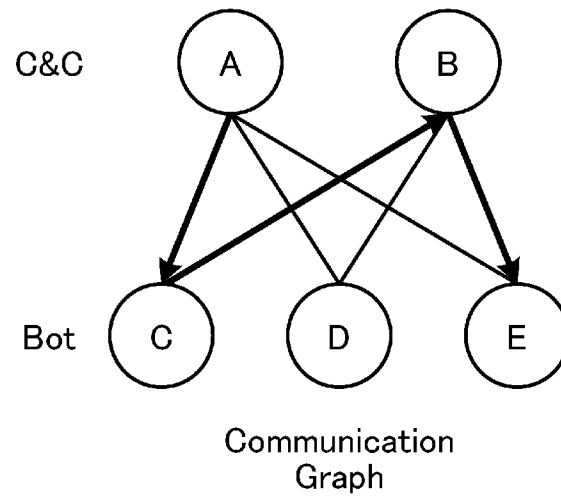
選択された前記ノードのそれぞれについて、各グループで学習されたモデルを用いて推定された特徴量を合成することにより、特徴量を算出ステップと、

を実行させることを特徴とする特徴量算出プログラム。

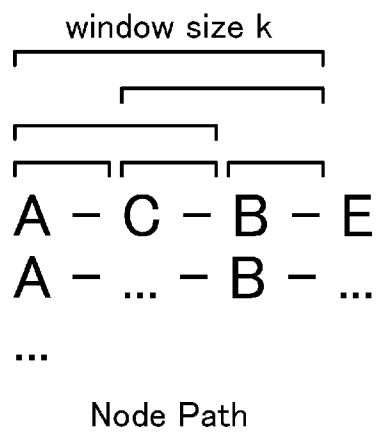
[図1]



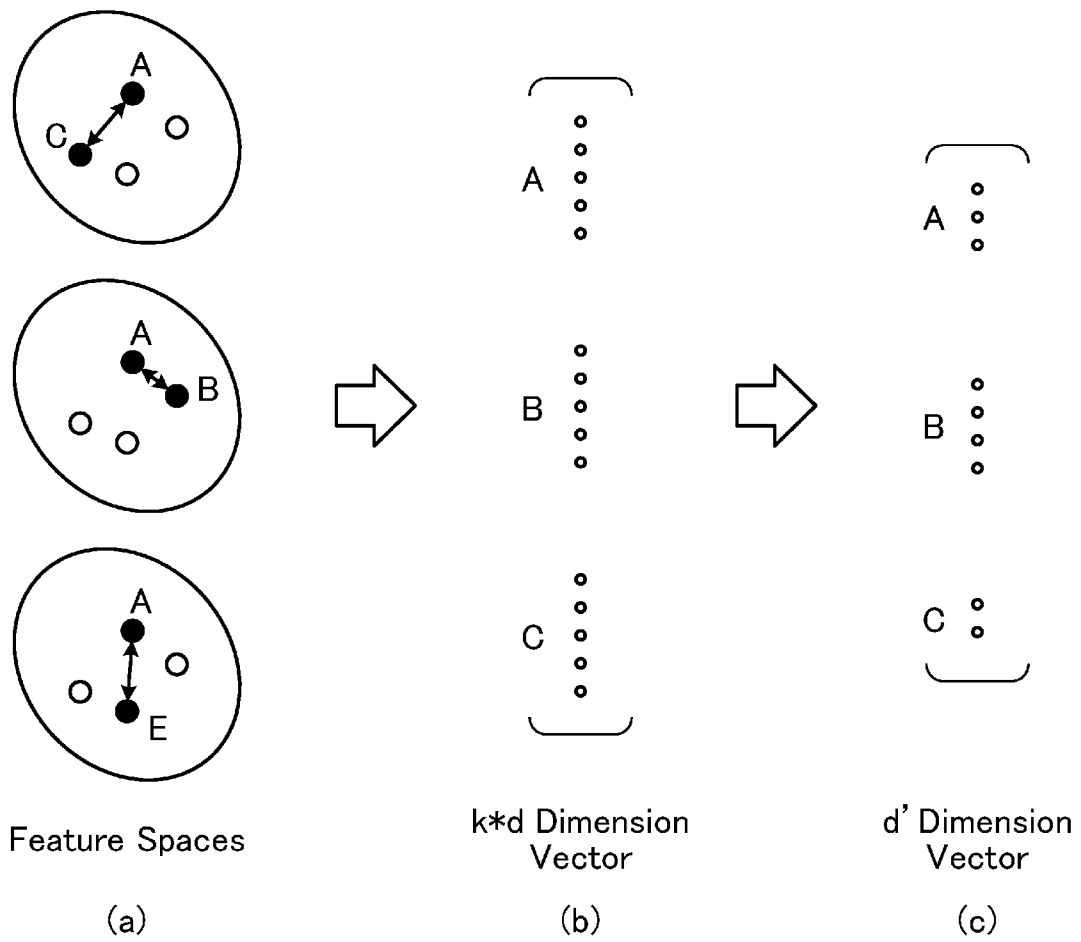
[図2]



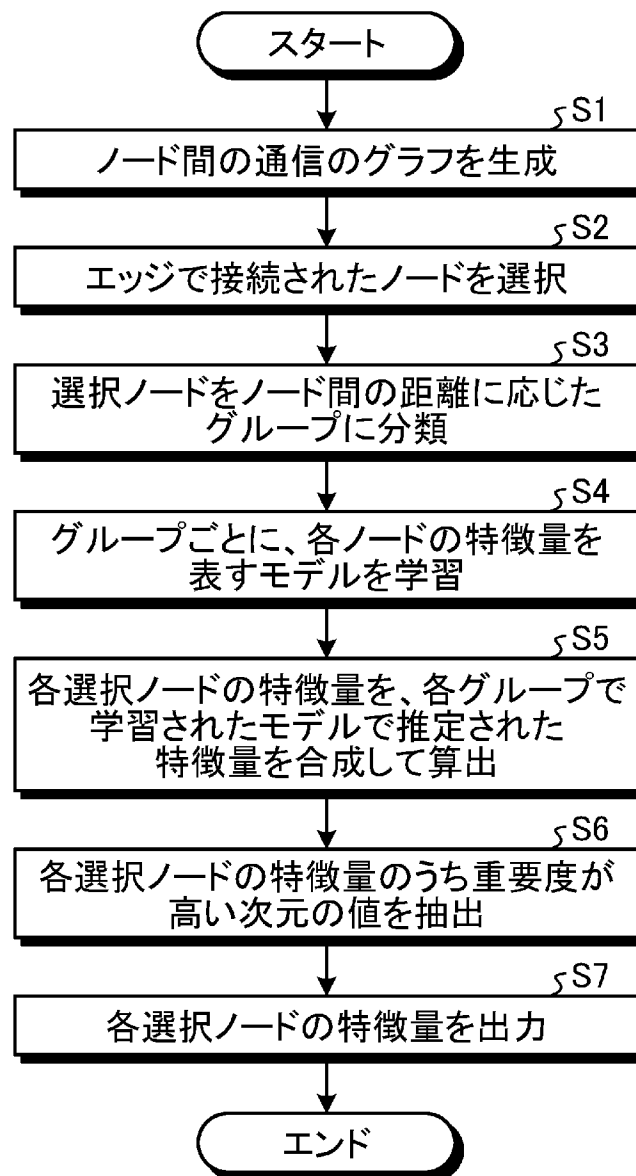
[図3]



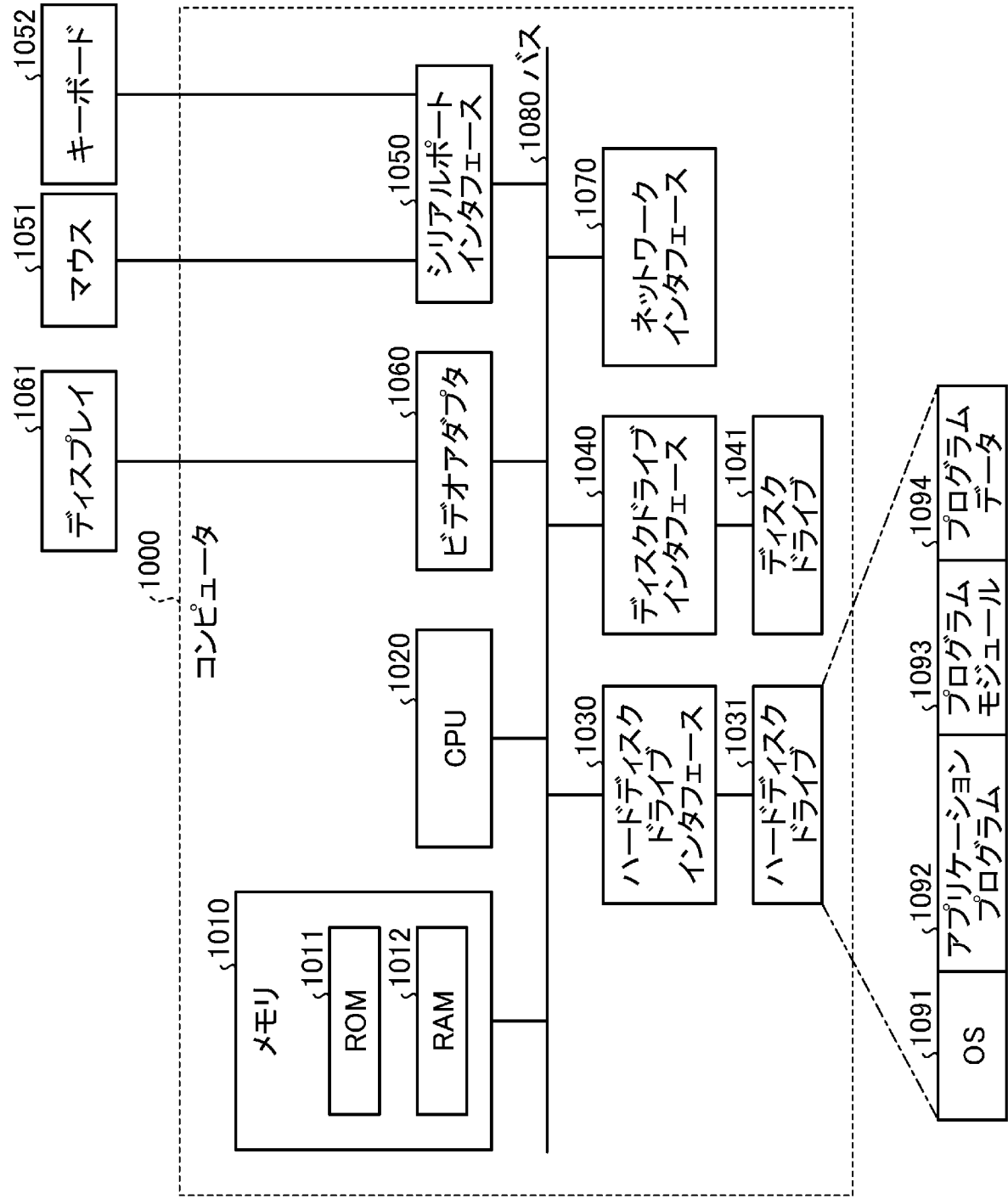
[図4]



[図5]



[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/018420

A. CLASSIFICATION OF SUBJECT MATTER**H04L 12/26**(2006.01)i

FI: H04L12/26

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)

H04L12/26

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	WO 2019/168072 A1 (NIPPON TELEGRAPH & TELEPHONE) 06 September 2019 (2019-09-06) paragraphs [0016]-[0033]	1-7
A	熊谷 将也, 松本 亮介, 侵入検知システムのためのグラフ構造に基づいた機械学習および可視化 Graph Based Machine Learning and Visualization for Intrusion Detection System, 電子情報通信学会技術研究報告 vol. 118 no. 480 IEICE Technical Report, 28 February 2019 p. 359, chapter 3 to p. 362, chapter 4, (KUMAGAI, Masaya. MATSUMOTO, Ryosuke.)	1-7
A	ABOU DAYA, Abbas et al. BotChase: Graph-Based Bot Detection Using Machine Learning. IEEE Transactions on Network and Service Management. vol. 17, no. 1, March 2020, pp. 15-29, <URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8986547 >, <DOI: 10.1109/TNSM.2020.2972405> pp. 17-20, chapter 3	1-7

☐ 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

29 June 2021

Date of mailing of the international search report

06 July 2021

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 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/JP2021/018420

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2019/168072	A1	06 September 2019	JP	2019-149681	A	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 12/26(2006.01)i FI: H04L12/26														
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）） H04L12/26 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 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）			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				
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													
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	WO 2019/168072 A1（日本電信電話株式会社）06.09.2019（2019 - 09 - 06） [0016]-[0033]	1-7												
A	熊谷 将也, 松本 亮介, 侵入検知システムのためのグラフ構造に基づいた機械学習および可視化 Graph Based Machine Learning and Visualization for Intrusion Detection System, 電子情報通信学会技術研究報告 Vol.118 No.480 IEICE Technical Report, 2019.02.28 p.359第3章-p.362第4章	1-7												
A	ABOU DAYA, Abbas et al., BotChase: Graph-Based Bot Detection Using Machine Learning, IEEE Transactions on Network and Service Management, Vol.17, No.1, 2020.03, pp.15-29, <URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8986547 >, <DOI: 10.1109/TNSM.2020.2972405> pp.17-20第3章	1-7												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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	“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	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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													
“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	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 29.06.2021		国際調査報告の発送日 06.07.2021												
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） 佐々木 洋 5X 4811 電話番号 03-3581-1101 内線 3556												

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/JP2021/018420

引用文献			公表日	パテントファミリー文献			公表日
WO	2019/168072	A1	06.09.2019	JP	2019-149681	A	