(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
2023年1月26日(26.01.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/002575 A1

(51) 国際特許分類:
G06N 20/00 (2019.01)

(21) 国際出願番号： PCT/JP2021/027177

(22) 国際出願日： 2021年7月20日(20.07.2021)

(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).

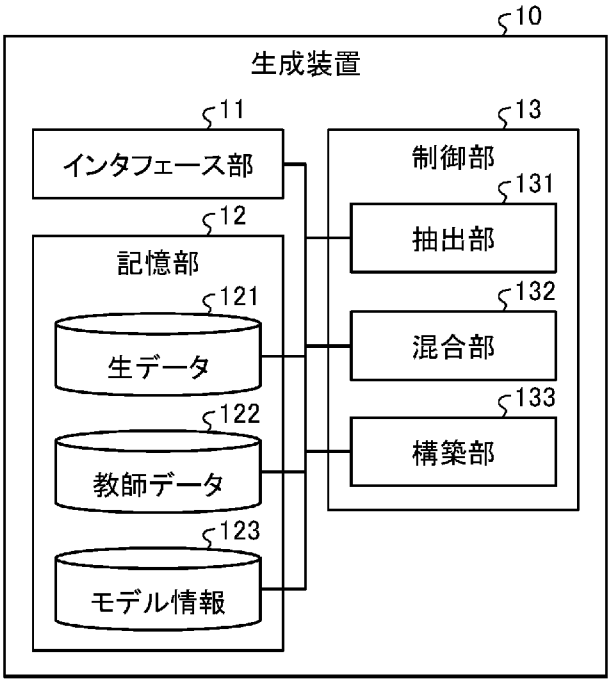
(72) 発明者: 芝原 俊樹 (**SHIBAHARA, Toshiki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 千葉 大紀 (**CHIBA, Daiki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 秋山 満昭 (**AKIYAMA, Mitsuaki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

(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,

(54) **Title:** GENERATION DEVICE, GENERATION METHOD, GENERATION PROGRAM, ASSESSMENT DEVICE, ASSESSMENT METHOD, AND ASSESSMENT PROGRAM

(54) 発明の名称： 生成装置、生成方法、生成プログラム、判定装置、判定方法及び判定プログラム



10 Generation device
11 Interface unit
12 Storage unit
13 Control unit
121 Raw data
122 Training data
123 Model information
131 Extraction unit
132 Mixing unit
133 Construction unit

(57) **Abstract:** An extraction unit (131) of a generation device (10) extracts a feature vector from data pertaining to software and labeled as malignant or not, on the basis of the occurrence of specific character strings in the data. A mixing unit (132) mixes a plurality of combinations of feature vectors extracted by the extraction unit (131) and labels assigned to the feature vectors to generate feature vectors and labels. A construction unit (133) uses the combination of the feature

WO 2023/002575 A1

［続葉有］

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, 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)）

vector and label extracted by the extraction unit (131) and the combination of the feature vector and label generated by the mixing unit (132) as training data to construct a model to predict labels on the basis of feature vectors.

(57) 要約：生成装置（１０）の抽出部（１３１）は、ソフトウェアに関するデータであって、悪性であるか否かを表すラベルが付与されたデータにおける特定の文字列の出現状況を基に、データから特徴ベクトルを抽出する。混合部（１３２）は、抽出部（１３１）によって抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して、特徴ベクトル及びラベルを生成する。構築部（１３３）は、抽出部（１３１）によって抽出された特徴ベクトルとラベルの組み合わせ、及び混合部（１３２）によって生成された特徴ベクトルとラベルの組み合わせを教師データとして用いて、特徴ベクトルを基にラベルを予測するモデルを構築する。

明　細　書

発明の名称 ：

生成装置、生成方法、生成プログラム、判定装置、判定方法及び判定プログラム

技術分野

[0001] 本発明は、生成装置、生成方法、生成プログラム、判定装置、判定方法及び判定プログラムに関する。

背景技術

[0002] 機械学習（ＭＬ：Machine Learning）アルゴリズム及びディープニューラルネットワーク（ＤＮＮ：Deep Neural Network）等を用いて、マルウェア検知及びネットワーク侵入検知といったサイバー攻撃を検知する技術が提案されている（例えば非特許文献１を参照）。

[0003] ここで、教師データありのＭＬ及びＤＮＮでは、モデルが教師データにはフィットするが、試験データ（評価データ）にはフィットしない、いわゆる過学習（オーバーフィッテイング）が発生する場合がある。

[0004] 一方で、このような過学習を抑制する方法として、Ｌ２正則化、drop out、batch normalizationが知られている。また、画像処理の分野では、過学習を抑制する方法として、Mixupが知られている（例えば非特許文献２を参照）。

先行技術文献

非特許文献

[0005] 非特許文献1：Daniel Arp et al. Drebin: Effective and explainable detection of android malware in your pocket. In Proceedings of the 2014 Network and Distributed System Security Symposium, 2014.

非特許文献2：Vikas Verma et al. Manifold mixup: Better representations by interpolating hidden states. arXiv preprint arXiv:

1806.05236, 2018.

発明の概要

発明が解決しようとする課題

[0006] しかしながら、従来の技術には、セキュリティタスクの解決に用いられるニューラルネットワークのユニット数が少ない場合、過学習を抑制することが難しい場合があるという問題がある。

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、生成装置は、ソフトウェアに関するデータであって、悪性であるか否かを表すラベルが付与されたデータにおける特定の文字列の出現状況を基に、前記データから特徴ベクトルを抽出する抽出部と、前記抽出部によって抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して、特徴ベクトル及びラベルを生成する混合部と、前記抽出部によって抽出された特徴ベクトルとラベルの組み合わせ、及び前記混合部によって生成された特徴ベクトルとラベルの組み合わせを教師データとして用いて、特徴ベクトルを基にラベルを予測するモデルを構築する構築部と、を有することを特徴とする。

[0008] 上述した課題を解決し、目的を達成するために、判定装置は、ソフトウェアに関する判定用データにおける特定の文字列の出現状況を基に、前記判定用データから特徴ベクトルを抽出する抽出部と、ソフトウェアに関する学習用データであって、悪性であるか否かを表すラベルが付与された学習用データにおける特定の文字列の出現状況を基に、前記学習用データから抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して得られた特徴ベクトル及びラベルを含む教師データによって学習が行われたモデルに、前記抽出部によって抽出された特徴ベクトルを入力して得られた出力を基に、前記判定用データが悪性であるか否かを判定する判定部と、を有することを特徴とする。

発明の効果

[0009] 本発明によれば、セキュリティタスクの解決に用いられるニューラルネットワークのユニット数が少ない場合であっても、過学習を抑制することができる。

図面の簡単な説明

[0010] [図1]図１は、第１の実施形態に係る生成装置の構成例を示す図である。

[図2]図２は、特徴ベクトルの抽出方法を説明する図である。

[図3]図３は、特徴ベクトルの混合方法を説明する図である。

[図4]図４は、モデルの構成例を示す図である。

[図5]図５は、第１の実施形態に係る生成装置の処理の流れを示すフローチャートである。

[図6]図６は、第１の実施形態に係る判定装置の構成例を示す図である。

[図7]図７は、第１の実施形態に係る判定装置の処理の流れを示すフローチャートである。

[図8]図８は、実験結果を示す図である。

[図9]図９は、実験結果を示す図である。

[図10]図１０は、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。

発明を実施するための形態

[0011] 以下に、本願に係る生成装置、生成方法、生成プログラム、判定装置、判定方法及び判定プログラムの実施形態を図面に基づいて詳細に説明する。なお、本発明は、以下に説明する実施形態により限定されるものではない。

[0012] ［第１の実施形態］

まず、図１を用いて、第１の実施形態に係る生成装置の構成について説明する。図１は、第１の実施形態に係る生成装置の構成例を示す図である。

[0013] 生成装置１０は、生データの入力を受け付け、学習済みのモデルのパラメータ等の情報を出力する。

[0014] ここで、モデルは、ニューラルネットワーク（ＮＮ）を使って、ソフトウェアが悪性であるか否かを判定するための情報を出力する。

[0015] 生成装置１０は、与えられた生データだけでなく、生データから生成したデータを教師データとして用いることで、モデルの過学習を抑制する。

[0016] また、生成装置１０において学習が行われる際には、生データにはラベルが付与されているものとする。また、生成装置１０は、生データから抽出した特徴ベクトルをモデルに入力する。生データ、ラベル及び特徴ベクトルの詳細については後述する。

[0017] 図１に示すように、生成装置１０は、インタフェース部１１、記憶部１２及び制御部１３を有する。

[0018] インタフェース部１１は、データの入力及び出力のためのインタフェースである。例えば、インタフェース部１１はＮＩＣ（Network Interface Card）である。インタフェース部１１は他の装置との間でデータの送受信を行うことができる。

[0019] また、インタフェース部１１は、マウスやキーボード等の入力装置と接続されていてもよい。また、インタフェース部１１は、ディスプレイ及びスピーカ等の出力装置と接続されていてもよい。

[0020] 記憶部１２は、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、光ディスク等の記憶装置である。なお、記憶部１２は、ＲＡＭ（Random Access Memory）、フラッシュメモリ、ＮＶＳＲＡＭ（Non Volatile Static Random Access Memory）等のデータを書き換え可能な半導体メモリであってもよい。

[0021] 記憶部１２は、生成装置１０で実行されるＯＳ（Operating System）や各種プログラムを記憶する。例えば、記憶部１２は生データ１２１、教師データ１２２及びモデル情報１２３モデル情報１２３を記憶する。

[0022] 生データ１２１は悪性であるか否かを判定する対象のソフトウェアに関するデータでる。例えば、生データ１２１は、ソフトウェア自体のファイル（例：ＡＰＫ（Android Application Package）ファイル、Windows（登録商標）の実行ファイル）、及びソフトウェアが発生させたログ（例：通信ログ）等である。

[0023] また、生データ１２１には、ラベルが付与されている。ラベルは、良性又は悪性であることを示す二値であってもよい。また、ラベルは、マルウェアのファミリ名（トロイの木馬、バックドア、ランサムウェア等）であってもよい。その場合、モデルのタスクは多クラス分類となる。

[0024] 本実施形態では、ラベルはone-hot encodingで表現されるものとする。すなわち、ラベルは、各要素がクラスに対応し、ある要素のみが１、他の要素が０のベクトルである。ここでは、クラスは良性及び悪性の２つであるものとする。

[0025] 教師データ１２２は、ラベルと特徴ベクトルの組み合わせである。例えば、教師データ１２２は、生データ１２１から抽出されるデータである。また、教師データ１２２は、生データ１２１から抽出されたデータをさらに混合することによって生成される。

[0026] モデル情報１２３は、モデルに関する情報である。モデル情報１２３には、ニューラルネットワークの重み等のパラメータが含まれる。モデル情報１２３は、教師データ１２２を用いた学習によって構築される。

[0027] 制御部１３は、生成装置１０全体を制御する。制御部１３は、例えば、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）、ＧＰＵ（Graphics Processing Unit）等の電子回路や、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）等の集積回路である。

[0028] また、制御部１３は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、内部メモリを用いて各処理を実行する。

[0029] 制御部１３は、各種のプログラムが動作することにより各種の処理部として機能する。例えば、制御部１３は、抽出部１３１、混合部１３２及び構築部１３３を有する。

[0030] 抽出部１３１は、ソフトウェアに関するデータであって、悪性であるか否かを表すラベルが付与されたデータにおける特定の文字列の出現状況を基に

、データから特徴ベクトルを抽出する。抽出部１３１は、生データ１２１から抽出した特徴ベクトルをラベルと組み合せて教師データ１２２に追加する。

[0031] 抽出部１３１は、特定の文字列のそれぞれに対応する要素を持つベクトルであって、特定の文字列のうちデータに出現する文字列に対応する要素の値と、特定の文字列のうちデータに出現しない文字列に対応する要素の値とが異なるベクトルを抽出する。

[0032] 図２を用いて特徴ベクトルの抽出方法を説明する。図２は、特徴ベクトルの抽出方法を説明する図である。

[0033] 図２に示すように、生データ１２１には、ＡＰＫファイル１２１ａ、ＡＰＫファイル１２１ｂ、ＡＰＫファイル１２１ｃが含まれる。

[0034] まず、抽出部１３１は、各ＡＰＫファイルから文字列を抽出する。抽出部１３１は、各ＡＰＫファイルを逆アセンブリしたファイルから文字列を抽出してもよい。

[0035] 抽出部１３１は、ＡＰＫファイルの全ての部分から文字列を抽出してもよいし、特定のカテゴリの文字列のみを抽出してもよい。例えば、特定のカテゴリは、例えばＡＰＩ名、パーミッション、ドメイン名、ＩＰアドレスを含む。

[0036] また、抽出部１３１は、抽出した文字列に関連する情報をさらに収集し、当該収集した文字列を抽出した文字列とみなしてもよい。例えば、抽出部１３１は、ＩＰアドレスの所在地の情報、ドメインの所有者等を収集する。

[0037] また、抽出部１３１は、生データ１２１の全体（例えば、ＡＰＫファイル１２１ａ、ＡＰＫファイル１２１ｂ、ＡＰＫファイル１２１ｃ）において一定回数（例：１０回）以上出現した文字列のみを抽出するようにしてもよい。

[0038] 図２の例では、抽出部１３１は、特定の文字列として「API 1」、「API 2」、「API 3」、「Permission 1」、「Permission 2」を抽出する。特定の文字列は、生データ１２１の全体の文字列の出現回数を集計して得られた

出現回数が一定回数であった文字列である。

[0039] 抽出部１３１は、ＡＰＫファイル１２１ａから文字列「API 1」、「API 2」、「Permission 1」を抽出する。また、抽出部１３１は、ＡＰＫファイル１２１ｂから文字列「API 1」、「API 3」、「Permission 2」を抽出する。また、抽出部１３１は、ＡＰＫファイル１２１ｃから文字列「API 2」、「API 3」、「Permission 2」を抽出する。

[0040] 抽出部１３１は、抽出した文字列を特徴ベクトルの各要素に割り当てる。例えば、抽出部１３１は、特徴ベクトルの要素のうち、抽出した文字列に対応する要素の値を１とし、抽出しなかった文字列に対応する要素の値を０とする。

[0041] このように、ＡＰＫファイルに出現する文字列に対応する要素の値と、ＡＰＫファイルに出現しない文字列に対応する要素の値とが異なる。

[0042] また、特定の文字列の種類の数がＮであれば、抽出部１３１によって抽出される特徴ベクトルは１×Ｎのベクトルとなる。さらに、抽出部１３１は、生データ１２１のサイズ、エントロピー等の連続値を、特徴ベクトルの要素に追加してもよい。

[0043] 図２の例では、特徴ベクトルの１番目の要素は文字列「API 1」に対応し、２番目の要素は文字列「API 2」に対応し、３番目の要素は文字列「API 3」に対応し、４番目の要素は文字列「Permission 1」に対応し、５番目の要素は文字列「Permission 2」に対応している。

[0044] 抽出部１３１は、ＡＰＫファイル１２１ａから特徴ベクトル１２２１ａを抽出し、ＡＰＫファイル１２１ｂから特徴ベクトル１２２１ｂを抽出し、ＡＰＫファイル１２１ｃから特徴ベクトル１２２１ｃを抽出する。

[0045] 混合部１３２は、抽出部１３１によって抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して、特徴ベクトル及びラベルを生成する。混合部１３２は、混合によって生成した特徴ベクトル及びラベルを組み合せて教師データ１２２に追加する。

[0046] 混合部１３２は、第１の特徴ベクトルにあらかじめ定められた混合率を掛

けた値と、第２の特徴ベクトルに混合率を１から引いた値を掛けた値を足した第３の特徴ベクトルと、第１の特徴ベクトルに対応するラベルを表す第１のラベルベクトルに混合率を掛けた値と、第２の特徴ベクトルに対応するラベルを表す第２のラベルベクトルに混合率を１から引いた値を掛けた値を足した第３のラベルベクトルと、の組み合わせを生成する。

[0047] 図３を用いて、特徴ベクトルの混合方法を説明する。図３は、特徴ベクトルの混合方法を説明する図である。

[0048] 混合部１３２は、抽出部１３１によって抽出された特徴ベクトルだけでなく、ニューラルネットワークの中間層から取得した特徴ベクトルを混合してもよい。

[0049] まず、混合部１３２は、教師データ１２２の中から、ラベルと特徴ベクトルの複数の組み合わせを取得する。

[0050] 混合部１３２は、混合率を、事前に決められたベータ分布等の確率分布から決定してもよいし、取得した組み合わせに含まれるデータ間の類似度、ラベルの内容等の特性に基づき決定してもよい。

[0051] 混合部１３２は、混合率をλ、第１の特徴ベクトルをａ、第２の特徴ベクトルをｂとすると、（１）式のように第３の特徴ベクトルを計算する。この場合、（１）式の左辺が第３の特徴ベクトルに相当する。

[0052] [数1]

$$\mathrm{Mix}_{\lambda}(a,b)=\lambda a+(1-\lambda)b \qquad \cdots(1)$$

[0053] また、混合部１３２は、混合率をλ、第１のラベルベクトルをａ、第２のラベル徴ベクトルをｂとした場合も、同様に（１）式により第３のラベルベクトルを計算することができる。この場合、（１）式の左辺が第３のラベルベクトルに相当する。

[0054] 図３の例では、混合部１３２は、特徴ベクトル１２２１ａと特徴ベクトル１２２１ｂとを混合して、特徴ベクトル１２２１ａｂを得る。

[0055] また、図３の例では、混合部１３２は、ラベル１２２２ａとラベル１２２２ｂとを混合して、ラベル１２２２ａｂを得る。

[0056] なお、ラベルはベクトル（ラベルベクトル）で表され、１番目の要素が１であることは良性であることを意味し、２番目の要素が１であることは悪性であることを意味する。

[0057] また、図３のように、要素の値が二値であったベクトルを混合して得られたベクトルの各要素の値は連続値となる場合がある。

[0058] 構築部１３３は、抽出部１３１によって抽出された特徴ベクトルとラベルの組み合わせ、及び混合部１３２によって生成された特徴ベクトルとラベルの組み合わせを教師データとして用いて、特徴ベクトルを基にラベルを予測するモデルを構築する。

[0059] 図４は、モデルの構成例を示す図である。構築部１３３は、図４に示すモデルの学習を行う。

[0060] 図４のモデルは、１×Ｎの特徴ベクトルが入力される全結合ＮＮである。本実施形態によれば、特徴ベクトルによりデータの特性を表現するために最低限必要な個数にまでＮＮのユニット数を小さくした場合であっても、過学習を抑制することができる。

[0061] 図５は、第１の実施形態に係る生成装置の処理の流れを示すフローチャートである。図５に示すように、まず、生成装置１０は、ラベルが付与された生データにおける特定の文字列の出現状況を基に特徴ベクトルを抽出する（ステップＳ１０１）。

[0062] 続いて、生成装置１０は、ラベル及び抽出した特徴ベクトルを混合し、ラベル及び特徴ベクトルの組み合わせを生成する（ステップＳ１０２）。

[0063] 生成装置１０は、付与済みのラベル及び抽出した特徴ベクトルの組み合わせと、混合によって得られたラベル及び特徴ベクトルの組み合わせと、を教師データとして用いて、特徴ベクトルからラベルを予測するモデルを構築する（ステップＳ１０３）。

[0064] ここで、生成装置１０によって構築されたモデルを使って実際にソフトウェアが悪性であるか否かを判定する判定装置２０について説明する。

[0065] 図６は、第１の実施形態に係る判定装置の構成例を示す図である。図６に

示すように、判定装置２０は、インタフェース部２１、記憶部２２及び制御部２３を有する。

[0066] インタフェース部２１は、データの入力及び出力のためのインタフェースである。例えば、インタフェース部２１はＮＩＣである。インタフェース部２１は他の装置との間でデータの送受信を行うことができる。

[0067] また、インタフェース部２１は、マウスやキーボード等の入力装置と接続されていてもよい。また、インタフェース部２１は、ディスプレイ及びスピーカ等の出力装置と接続されていてもよい。

[0068] 記憶部２２は、ＨＤＤ、ＳＳＤ、光ディスク等の記憶装置である。なお、記憶部２２は、ＲＡＭ、フラッシュメモリ、ＮＶＳＲＡＭ等のデータを書き換え可能な半導体メモリであってもよい。

[0069] 記憶部２２は、判定装置２０で実行されるＯＳや各種プログラムを記憶する。例えば、記憶部２２はモデル情報２２１を記憶する。

[0070] モデル情報２２１は、モデルに関する情報である。モデル情報２２１には、ニューラルネットワークの重み等のパラメータが含まれる。

[0071] モデル情報２２１は、生成装置１０によって構築済みであるものとする。

[0072] 制御部２３は、判定装置２０全体を制御する。制御部２３は、例えば、ＣＰＵ、ＭＰＵ、ＧＰＵ等の電子回路や、ＡＳＩＣ、ＦＰＧＡ等の集積回路である。

[0073] また、制御部２３は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、内部メモリを用いて各処理を実行する。

[0074] 制御部２３は、各種のプログラムが動作することにより各種の処理部として機能する。例えば、制御部２３は、抽出部２３１及び判定部２３２を有する。

[0075] 抽出部２３１は、ソフトウェアに関する判定用データにおける特定の文字列の出現状況を基に、判定用データから特徴ベクトルを抽出する。

[0076] 判定部２３２は、ソフトウェアに関する学習用データであって、悪性であ

るか否かを表すラベルが付与された学習用データにおける特定の文字列の出現状況を基に、学習用データから抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して得られた特徴ベクトル及びラベルを含む教師データによって学習が行われたモデルに、抽出部２３１によって抽出された特徴ベクトルを入力して得られた出力を基に、判定用データが悪性であるか否かを判定する。

[0077] つまり、判定部２３２は、生成装置１０によって学習が行われたモデルに、抽出部２３１によって抽出された特徴ベクトルを入力することによって判定を行う。

[0078] 図７は、第１の実施形態に係る判定装置の処理の流れを示すフローチャートである。図７に示すように、まず、判定装置２０は、ラベルが未知の生データにおける特定の文字列の出現状況を基に特徴ベクトルを抽出する（ステップＳ２０１）。

[0079] そして、判定装置２０は、抽出した特徴ベクトルを学習済みのモデルに入力して得られたラベル、すなわちモデルによって予測されたラベルを基に、生データが悪性のものであるか否かを判定する（ステップＳ２０２）。学習済みのモデルは、生成装置１０によって学習が行われたモデルである。

[0080] これまで説明してきたように、生成装置１０の抽出部１３１は、ソフトウェアに関するデータであって、悪性であるか否かを表すラベルが付与されたデータにおける特定の文字列の出現状況を基に、データから特徴ベクトルを抽出する。混合部１３２は、抽出部１３１によって抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して、特徴ベクトル及びラベルを生成する。構築部１３３は、抽出部１３１によって抽出された特徴ベクトルとラベルの組み合わせ、及び混合部１３２によって生成された特徴ベクトルとラベルの組み合わせを教師データとして用いて、特徴ベクトルを基にラベルを予測するモデルを構築する。

[0081] このように、生成装置１０は、実際に収集したソフトウェアに関するデータから抽出した教師データを混合することで、さらなる教師データを生成す

ることができる。その結果、本実施形態によれば、セキュリティタスクの解決に用いられるニューラルネットワークのユニット数が少ない場合であっても、過学習を抑制することができる。

[0082] 抽出部１３１は、特定の文字列のそれぞれに対応する要素を持つベクトルであって、特定の文字列のうちデータに出現する文字列に対応する要素の値と、特定の文字列のうちデータに出現しない文字列に対応する要素の値とが異なるベクトルを抽出する。

[0083] これにより、ソフトウェアの特性を定量的に表現した特徴ベクトルを得ることができるようになる。

[0084] 混合部１３２は、第１の特徴ベクトルにあらかじめ定められた混合率を掛けた値と、第２の特徴ベクトルに混合率を１から引いた値を掛けた値を足した第３の特徴ベクトルと、第１の特徴ベクトルに対応するラベルを表す第１のラベルベクトルに混合率を掛けた値と、第２の特徴ベクトルに対応するラベルを表す第２のラベルベクトルに混合率を１から引いた値を掛けた値を足した第３のラベルベクトルと、の組み合わせを生成する。

[0085] これにより、教師データを増加させ、過学習を抑制しつつモデルの精度を向上させることができる。

[0086] 判定装置２０の抽出部２３１は、ソフトウェアに関する判定用データにおける特定の文字列の出現状況を基に、判定用データから特徴ベクトルを抽出する。判定部２３２は、ソフトウェアに関する学習用データであって、悪性であるか否かを表すラベルが付与された学習用データにおける特定の文字列の出現状況を基に、学習用データから抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して得られた特徴ベクトル及びラベルを含む教師データによって学習が行われたモデルに、抽出部２３１によって抽出された特徴ベクトルを入力して得られた出力を基に、判定用データが悪性であるか否かを判定する。

[0087] これにより、過学習を抑制して学習が行われたモデルを用いて、ソフトウェアの悪性判定（マルウェア検知）を精度良く行うことができる。

[0088] （実施例）

例えば、本実施形態は、Androidマルウェア（ＯＳとしてAndroidが搭載された端末で稼働するマルウェア）の検知に利用することができる。下記方法でAndroidマルウェアを検知するモデルを構築し、Androidマルウェア検知に用いる。

[0089] この場合、生成装置１０は、生データ１２１として、収集された既知の悪性及び良性のＡＰＫファイルを用いる。

[0090] 例えば、悪性ＡＰＫファイルは、VirusTotal等のサービスから収集したファイル、又はgoogle playから収集されたＡＰＫファイルのうちアンチウイルスソフトで悪性と検知されたものである。例えば、良性ＡＰＫファイルは、google playから収集されたＡＰＫファイルのうちアンチウイルスソフトで悪性と検知されなかったものである。

[0091] そして、判定装置２０は、Androidを搭載したスマートフォンのＡＰＫファイルから特徴ベクトルを抽出する。そして、判定装置２０は、学習済みのモデルを用いて、抽出した特徴ベクトルが悪性であるか否かを判定する。

[0092] 例えば、判定装置２０は、判定結果が悪性であった場合、その旨をユーザに通知し、ＡＰＫファイルの削除等の対策を実施する。

[0093] （実験）

図８及び図９に、本実施形態と従来技術とを比較するために行った実験の結果を示す。図８及び図９は、実験結果を示す図である。

[0094] 実験では、上記の実施例と同様に、AndroidのＡＰＫファイルの悪性判定及びそのためのモデルの構築を行った。

[0095] 図８及び図９の、Ｌ２、ＤＯ、ＢＮは、それぞれＬ２正則化、drop out、batch normalizationに相当する。また、Mixupは本実施形態に相当する。例えば、「Ｌ２＋Mixup＋ＢＮ」は、Ｌ２正則化、batch normalization及び本実施形態による教師データの生成を用いてモデルの構築を行った場合の結果を意味する。

[0096] 図８は、過学習の抑制度合いを示している。Training（学習時）とTest（

推論時）でｐＡＵＣの差（Difference）が小さいほど過学習が抑制されているということができる。図８に示すように、Ｌ２とＬ２＋Mixupを比較すると、本実施形態のは一定の過学習の抑制効果があるということができる。

[0097] 図９は、ＮＮのユニットサイズごとのｐＡＵＣを示している。図９に示すように、特にＬ２＋Mixupの場合に、小さいユニットサイズにおいてｐＡＵＣが大きくなる。

[0098] これより、本実施形態によれば、ＮＮのユニット数が少なくても、過学習を抑制し、正解率の高い学習モデルを作成することができるということができる。また、ユニット数が少ないＮＮはパラメータ数が少ないため、少ない計算資源しか利用できない環境（例：モバイル）で学習、識別を行うことができる。

[0099] また、ユニット数が少ないＮＮは必要な計算資源が少ないため、ハイパーパラメータの探索の効率化や電力消費の削減も可能である。

[0100] ［システム構成等］

また、図示した各装置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（Central Processing Unit）及び当該ＣＰＵにて解析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。

[0101] また、本実施形態において説明した各処理のうち、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。

[0102] ［プログラム］

一実施形態として、生成装置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生成処理を実行する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、情報処理装置を生成装置１０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）等のスレート端末等がその範疇に含まれる。

[0103] また、生成装置１０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生成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。例えば、サーバ装置は、生データを入力とし、教師データ又は学習済みのモデル情報を出力するサービスを提供するサーバ装置として実装される。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生成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。

[0104] 図１０は、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ブインタフェース１０３０、ディスクドライブインタフェース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。

[0105] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１及び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１０９０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。

[0106] 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、生成装置１０の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、生成装置１０の生成処理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。

[0107] また、上述した実施形態の処理で用いられる設定データは、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。

[0108] 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（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された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

[0109] １０　生成装置

１１、２１　インタフェース部

１２、２２　記憶部

１３、２３　制御部

２０　判定装置

１２１　生データ

１２２　教師データ

１２３　モデル情報

１３１、２３１　抽出部

１３２　混合部

１３３　構築部

２３２　判定部

請求の範囲

[請求項1] ソフトウェアに関するデータであって、悪性であるか否かを表すラベルが付与されたデータにおける特定の文字列の出現状況を基に、前記データから特徴ベクトルを抽出する抽出部と、

前記抽出部によって抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して、特徴ベクトル及びラベルを生成する混合部と、

前記抽出部によって抽出された特徴ベクトルとラベルの組み合わせ、及び前記混合部によって生成された特徴ベクトルとラベルの組み合わせを教師データとして用いて、特徴ベクトルを基にラベルを予測するモデルを構築する構築部と、

を有することを特徴とする生成装置。

[請求項2] 前記抽出部は、前記特定の文字列のそれぞれに対応する要素を持つベクトルであって、前記特定の文字列のうち前記データに出現する文字列に対応する要素の値と、前記特定の文字列のうち前記データに出現しない文字列に対応する要素の値とが異なるベクトルを抽出することを特徴とする請求項１に記載の生成装置。

[請求項3] 前記混合部は、

第１の特徴ベクトルにあらかじめ定められた混合率を掛けた値と、第２の特徴ベクトルに前記混合率を１から引いた値を掛けた値を足した第３の特徴ベクトルと、

前記第１の特徴ベクトルに対応するラベルを表す第１のラベルベクトルに前記混合率を掛けた値と、前記第２の特徴ベクトルに対応するラベルを表す第２のラベルベクトルに前記混合率を１から引いた値を掛けた値を足した第３のラベルベクトルと、

の組み合わせを生成することを特徴とする請求項１又は２に記載の生成装置。

[請求項4] 生成装置によって実行される生成方法であって、

ソフトウェアに関するデータであって、悪性であるか否かを表すラベルが付与されたデータにおける特定の文字列の出現状況を基に、前記データから特徴ベクトルを抽出する抽出工程と、

前記抽出工程によって抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して、特徴ベクトル及びラベルを生成する混合工程と、

前記抽出工程によって抽出された特徴ベクトルとラベルの組み合わせ、及び前記混合工程によって生成された特徴ベクトルとラベルの組み合わせを教師データとして用いて、特徴ベクトルを基にラベルを予測するモデルを構築する構築工程と、

を含むことを特徴とする生成方法。

[請求項5] コンピュータを、請求項１から３のいずれか１項に記載の生成装置として機能させるための生成プログラム。

[請求項6] ソフトウェアに関する判定用データにおける特定の文字列の出現状況を基に、前記判定用データから特徴ベクトルを抽出する抽出部と、

ソフトウェアに関する学習用データであって、悪性であるか否かを表すラベルが付与された学習用データにおける特定の文字列の出現状況を基に、前記学習用データから抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して得られた特徴ベクトル及びラベルを含む教師データによって学習が行われたモデルに、前記抽出部によって抽出された特徴ベクトルを入力して得られた出力を基に、前記判定用データが悪性であるか否かを判定する判定部と、

を有することを特徴とする判定装置。

[請求項7] 判定装置によって実行される判定方法であって、

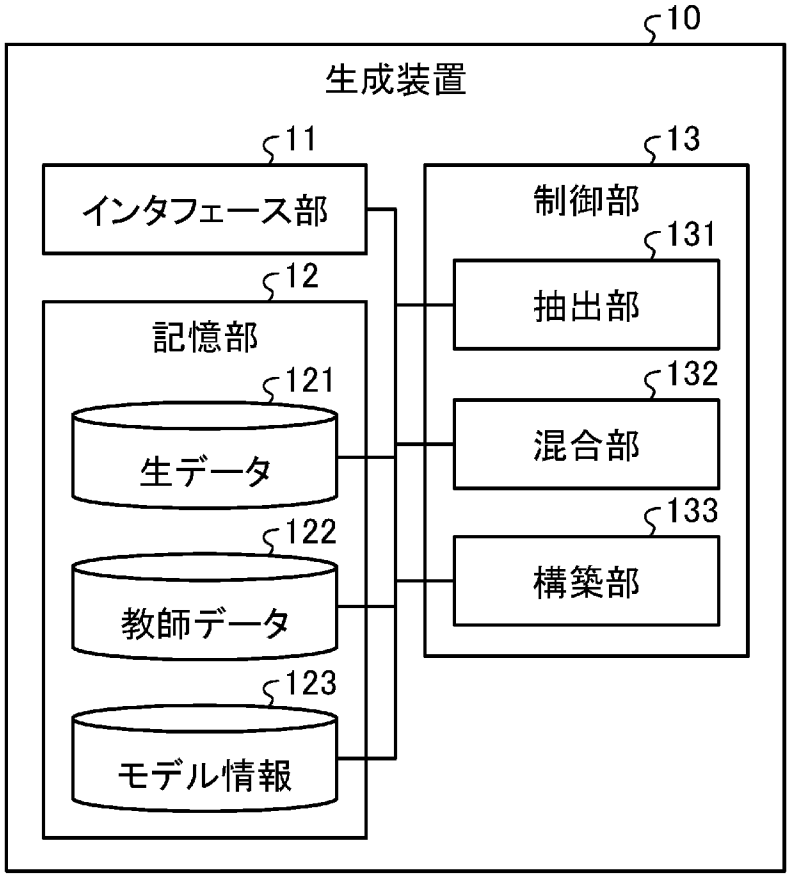
ソフトウェアに関する判定用データにおける特定の文字列の出現状況を基に、前記判定用データから特徴ベクトルを抽出する抽出工程と、

ソフトウェアに関する学習用データであって、悪性であるか否かを表すラベルが付与された学習用データにおける特定の文字列の出現状況を基に、前記学習用データから抽出された特徴ベクトルと当該特徴ベクトルに付与されたラベルの複数の組み合わせを混合して得られた特徴ベクトル及びラベルを含む教師データによって学習が行われたモデルに、前記抽出工程によって抽出された特徴ベクトルを入力して得られた出力を基に、前記判定用データが悪性であるか否かを判定する判定工程と、

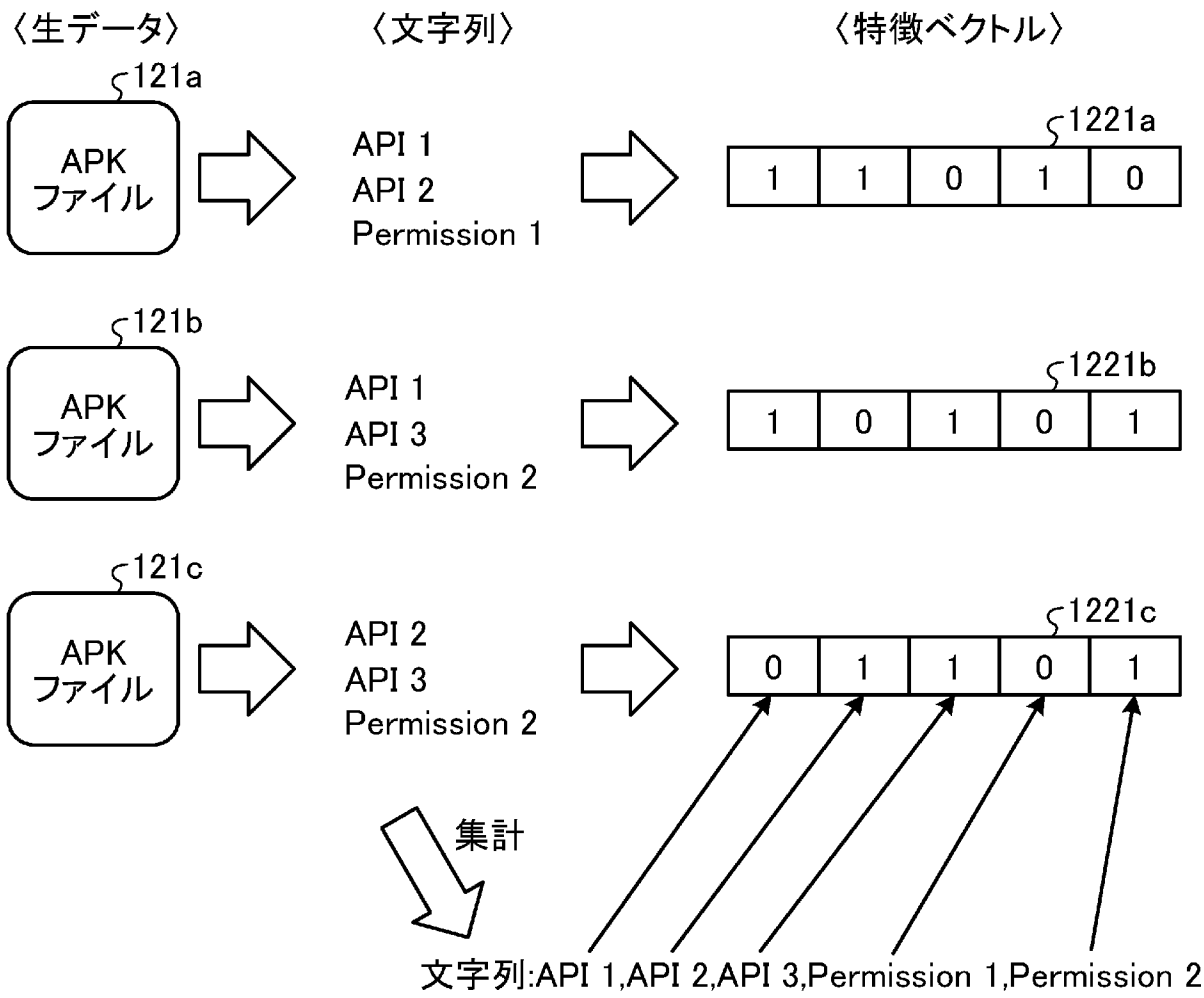
を含むことを特徴とする判定方法。

[請求項8] コンピュータを、請求項６に記載の判定装置として機能させるための判定プログラム。

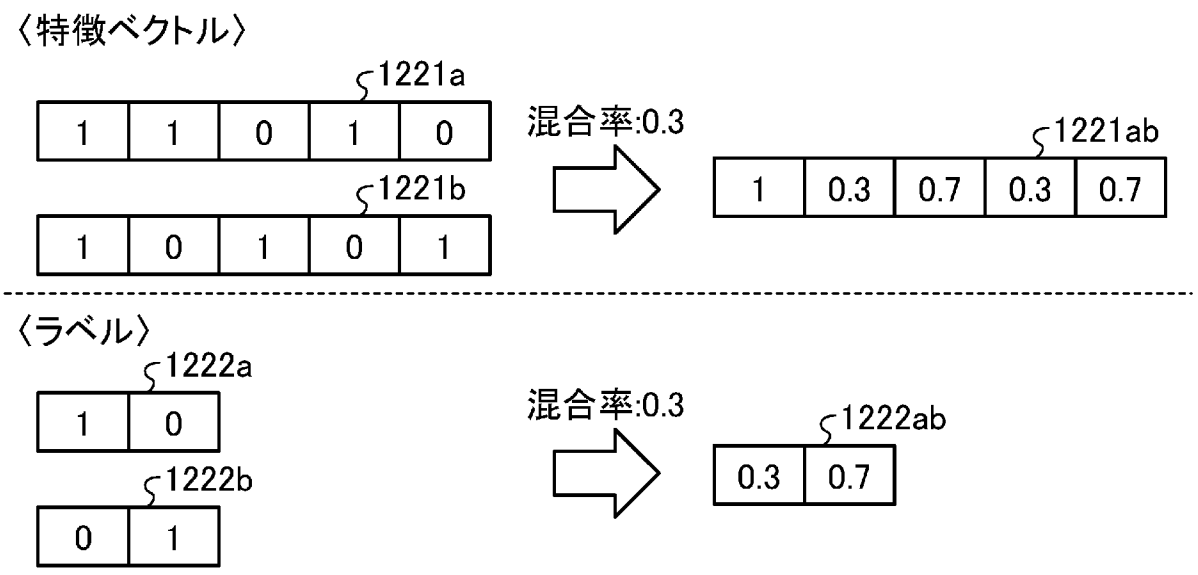
[図1]


10
生成装置
11
インタフェース部
12
記憶部
121
生データ
122
教師データ
123
モデル情報
13
制御部
131
抽出部
132
混合部
133
構築部

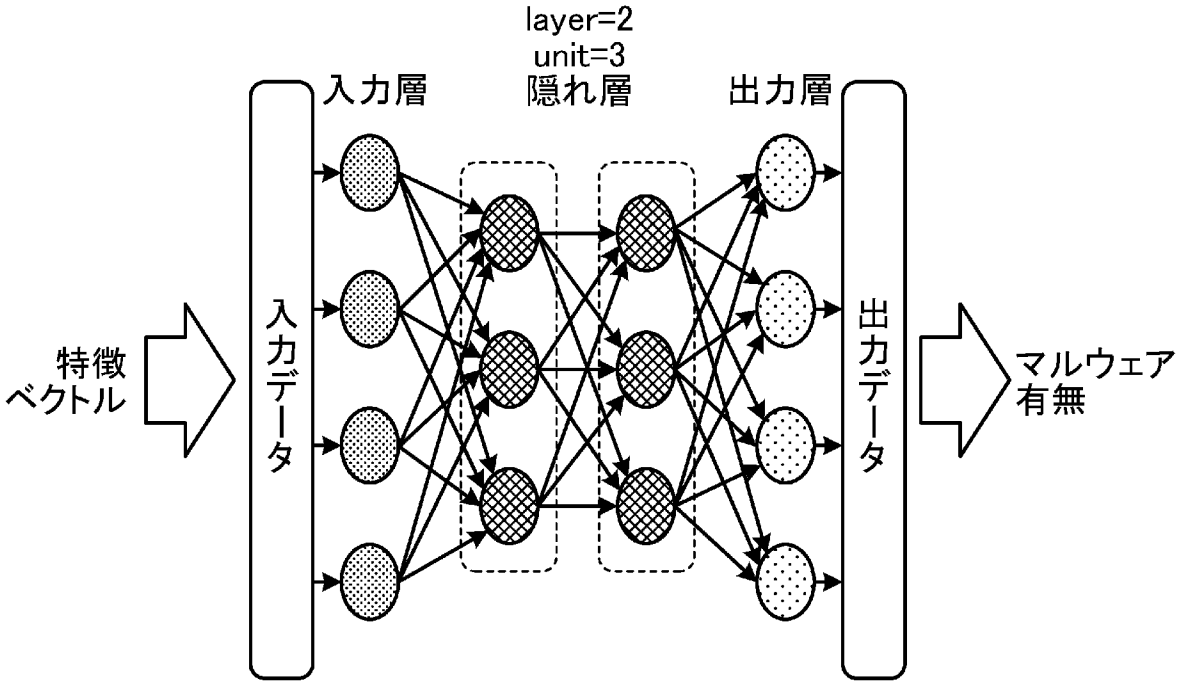
[図2]


〈生データ〉
〈文字列〉
〈特徴ベクトル〉
121a
APK
ファイル
API 1
API 2
Permission 1
1221a
1 1 0 1 0
121b
APK
ファイル
API 1
API 3
Permission 2
1221b
1 0 1 0 1
121c
APK
ファイル
API 2
API 3
Permission 2
1221c
0 1 1 0 1
集計
文字列:API 1,API 2,API 3,Permission 1,Permission 2

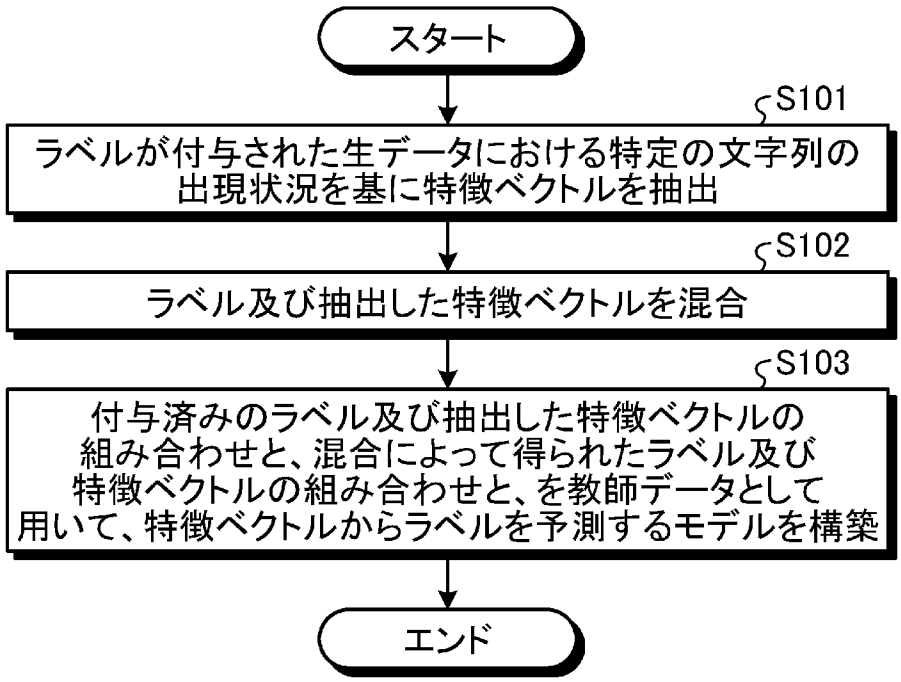
[図3]


〈特徴ベクトル〉
1221a
1 1 0 1 0
1221b
1 0 1 0 1
混合率:0.3
1221ab
1 0.3 0.7 0.3 0.7
〈ラベル〉
1222a
1 0
1222b
0 1
混合率:0.3
1222ab
0.3 0.7

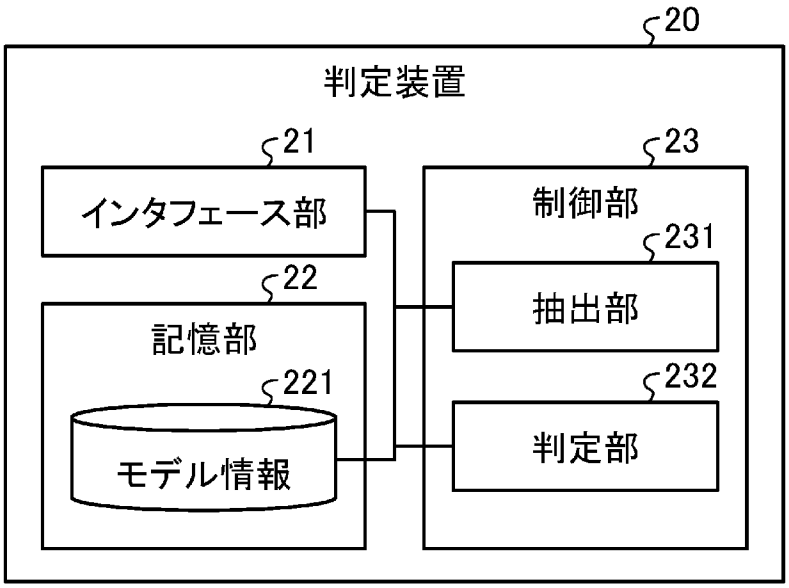
[図4]


layer=2
unit=3
入力層
隠れ層
出力層
特徴
ベクトル
入力データ
出力データ
マルウェア
有無

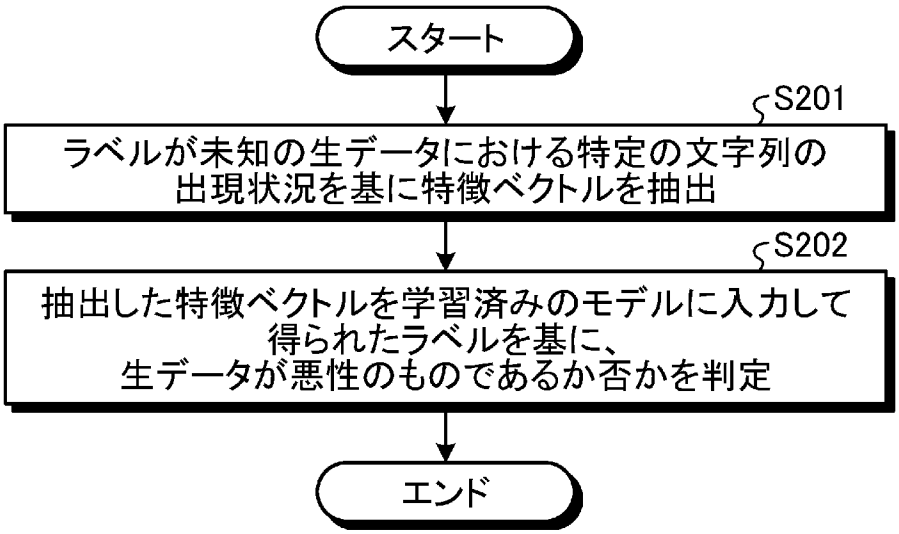
[図5]


スタート
S101
ラベルが付与された生データにおける特定の文字列の
出現状況を基に特徴ベクトルを抽出
S102
ラベル及び抽出した特徴ベクトルを混合
S103
付与済みのラベル及び抽出した特徴ベクトルの
組み合わせと、混合によって得られたラベル及び
特徴ベクトルの組み合わせと、を教師データとして
用いて、特徴ベクトルからラベルを予測するモデルを構築
エンド

[図6]


20
判定装置
21
インタフェース部
22
記憶部
221
モデル情報
23
制御部
231
抽出部
232
判定部

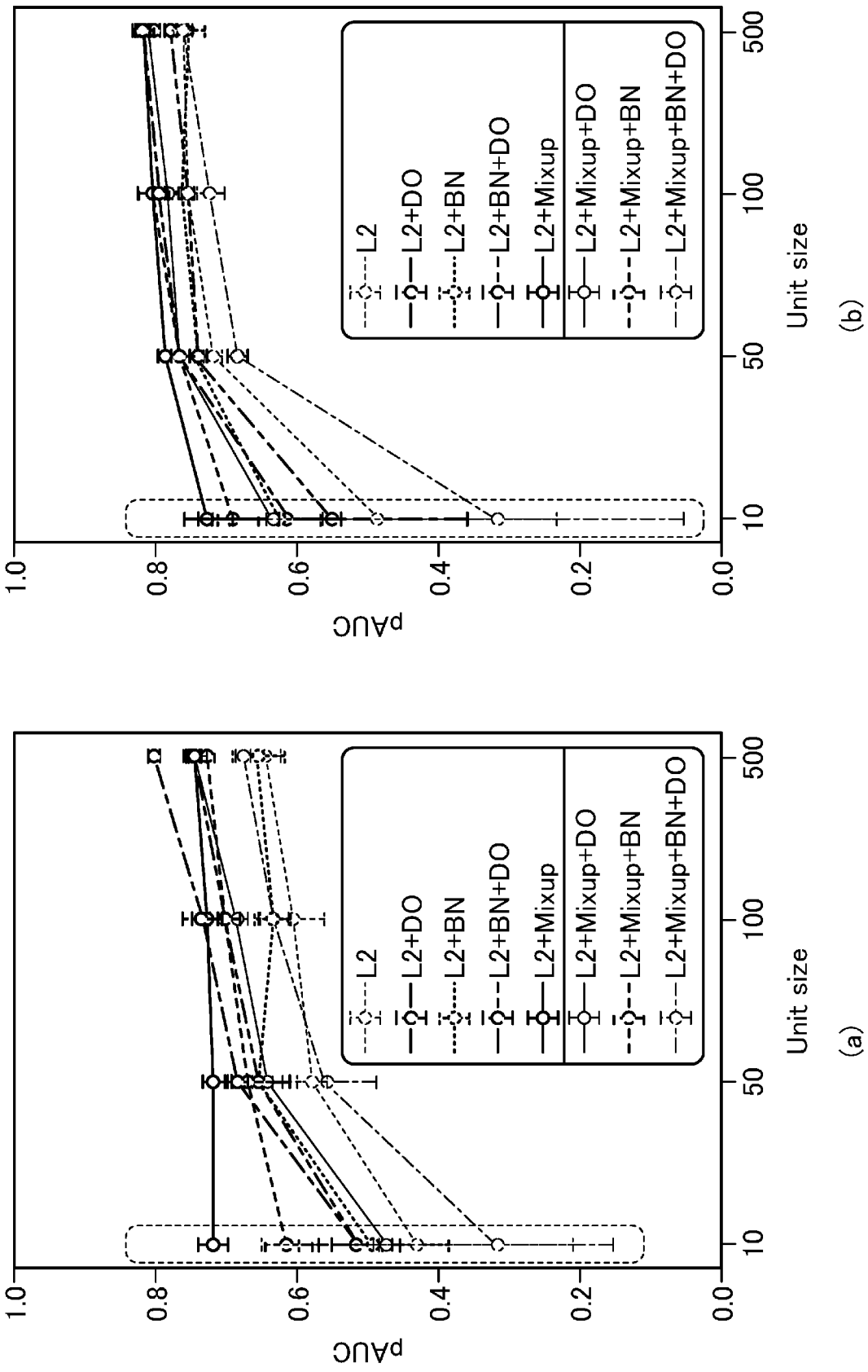
[図7]


スタート
S201
ラベルが未知の生データにおける特定の文字列の
出現状況を基に特徴ベクトルを抽出
S202
抽出した特徴ベクトルを学習済みのモデルに入力して
得られたラベルを基に、
生データが悪性のものであるか否かを判定
エンド

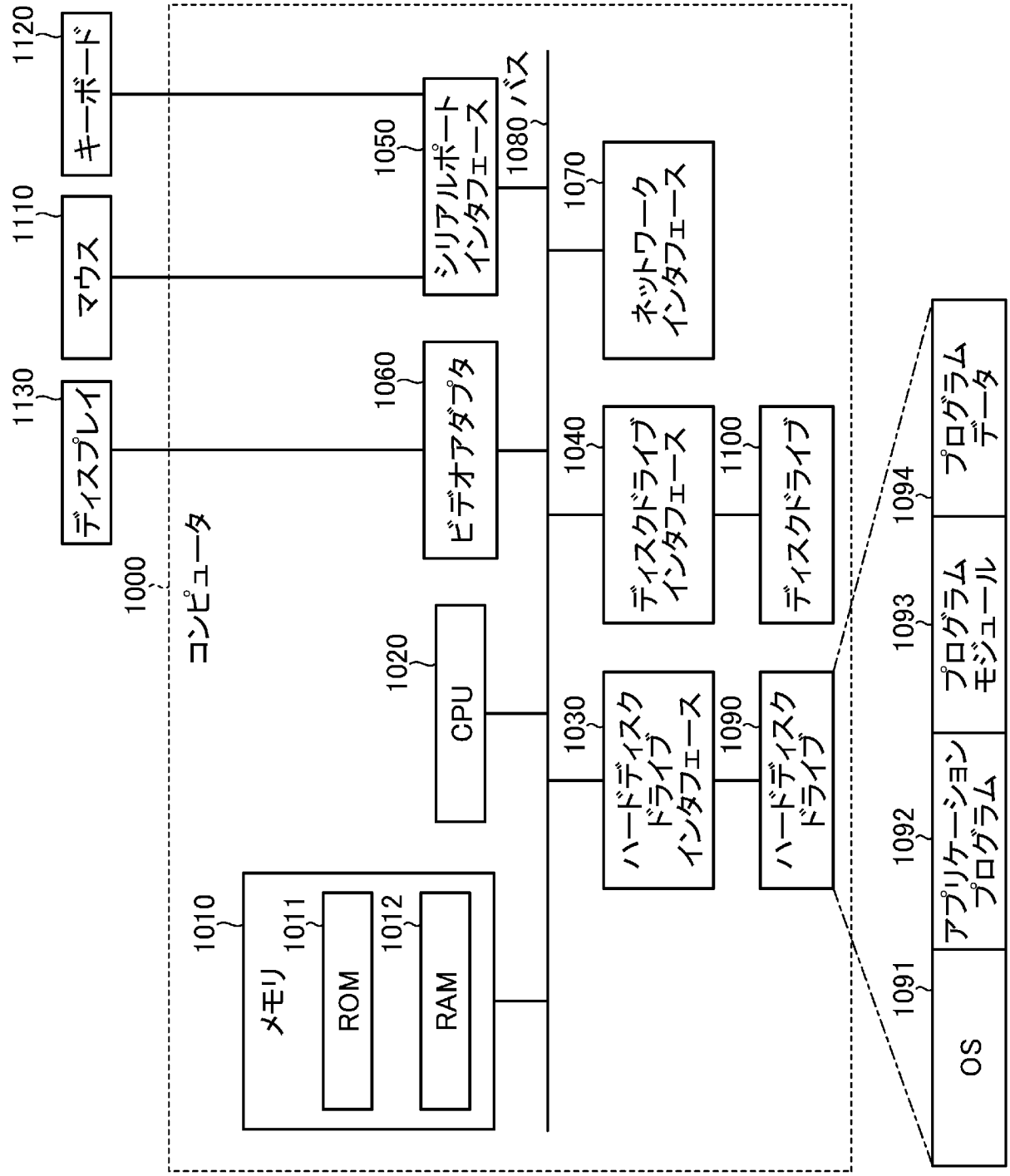
[図8]

Method	Training	Test	Difference
Dataset 1			
L2	0.9709±0.0000	0.6067±0.0438	0.3642±0.0437
L2+DO	0.9255±0.0013	0.7343±0.0261	0.1912±0.0271
L2+BN	0.9709±0.0000	0.6360±0.0232	0.3349±0.0232
L2+Mixup	0.9623±0.0005	0.7283±0.0218	0.2340±0.0218
Dataset 2			
L2	0.9405±0.0000	0.7503±0.0110	0.1902±0.0110
L2+DO	0.9073±0.0008	0.7928±0.0028	0.1144±0.0022
L2+BN	0.9409±0.0000	0.7617±0.0214	0.1792±0.0214
L2+Mixup	0.9316±0.0005	0.8068±0.0040	0.1249±0.0037

[図9]


pAUC
1.0
0.8
0.6
0.4
0.2
0.0
10
50
100
500
Unit size
L2
L2+DO
L2+BN
L2+BN+DO
L2+Mixup
L2+Mixup+DO
L2+Mixup+BN
L2+Mixup+BN+DO
(b)
pAUC
1.0
0.8
0.6
0.4
0.2
0.0
10
50
100
500
Unit size
L2
L2+DO
L2+BN
L2+BN+DO
L2+Mixup
L2+Mixup+DO
L2+Mixup+BN
L2+Mixup+BN+DO
(a)

[図10]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1040
ディスクドライブインタフェース
1050
シリアルポートインタフェース
1060
ビデオアダプタ
1070
ネットワークインタフェース
1080
バス
1090
ハードディスクドライブ
1100
ディスクドライブ
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ
1110
マウス
1120
キーボード
1130
ディスプレイ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/027177

A. CLASSIFICATION OF SUBJECT MATTER

G06N 20/00(2019.01)i
FI: G06N20/00 130

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)

G06N20/00

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	VINAYAKUMAR, R. et al. Deep android malware detection and classification. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) [online]. IEEE, 13 September 2014, pp. 1677-1683, Retrieved from the Internet: <URL:https://ieeexplore.ieee.org/document/8126084>, [Retrieved on 28 September 2021], DOI: 10.1109/ICACCI.2017.8126084 particularly, abstract, section IV, A, D, fig. 6	1-8
Y	JP 2020-154925 A (KDDI CORP.) 24 September 2020 (2020-09-24) particularly, paragraphs [0018], [0035], [0044]	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	Date of mailing of the international search report
28 September 2021	**05 October 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/JP2021/027177

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2020-154925 A	24 September 2020	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2021/027177

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06N 20/00(2019.01)i
FI: G06N20/00 130

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））

G06N20/00

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
Y	VINAYAKUMAR, R., et al., Deep Android Malware Detection and Classification, 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) [online], IEEE, 2014.09.13, pp. 1677-1683, Retrieved from the Internet: <URL: https://ieeexplore.ieee.org/document/8126084> [Retrieved on 2021-09-28], DOI: 10.1109/ICACCI.2017.8126084 特にAbstract, Sec. IV.A. and D., Fig. 6	1-8
Y	JP 2020-154925 A（ＫＤＤＩ株式会社）24.09.2020 (2020-09-24) 特に段落[0018], [0035], [0044]	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	国際調査報告の発送日
28.09.2021	05.10.2021

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）
金木　陽一　5B 4876
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/JP2021/027177

引用文献	公表日	パテントファミリー文献	公表日
JP 2020-154925 A	24.09.2020	（ファミリーなし）	