(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12月15日(15.12.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/259317 A1

(51) 国際特許分類:
H04L 12/70 (2013.01)

(21) 国際出願番号： PCT/JP2021/021581

(22) 国際出願日： 2021年6月7日(07.06.2021)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

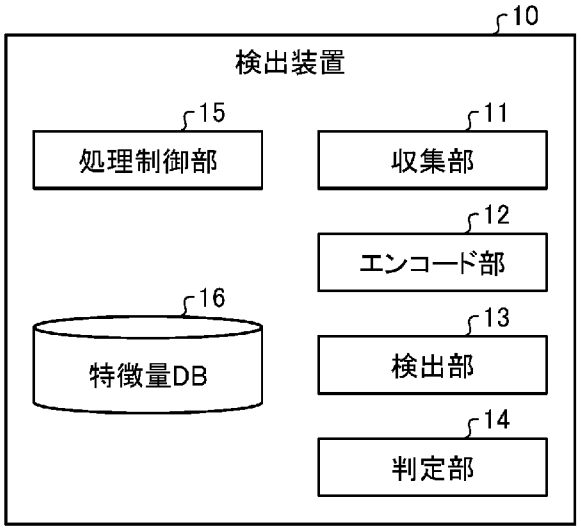
(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 寺本 泰大 (**TERAMOTO, Yasuhiro**); 〒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). 山田 真徳(**YAMADA, Masanori**); 〒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). 山中 友貴(**YAMANAKA, Yuki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 高橋 知克(**TAKAHASHI, Tomokatsu**); 〒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). 永井 智大 (**NAGAI, Tomohiro**); 〒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). 小山 高明(**KOYAMA, Takaaki**); 〒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).

(54) **Title:** DETECTION DEVICE, DETECTION METHOD, AND DETECTION PROGRAM

(54) 発明の名称： 検出装置、検出方法及び検出プログラム



10 Detection device
11 Collection unit
12 Encoding unit
13 Detection unit
14 Determination unit
15 Process control unit
16 Feature value DB

(57) **Abstract:** A detection device (10) includes: a feature value DB (16) that stores, in advance, feature values of packets, labels assigned to the feature values of the packets, and a threshold used for determination; an encoding unit (12) that converts a target packet into a feature value by using a first natural language processing model that has been trained beforehand using normal communication packets as training data; and a determination unit (14) that assigns a label to the feature value, which is obtained by the conversion using the first natural language processing model, on the basis of the feature value obtained by the conversion using the first natural language processing model and data stored in the feature value DB (16) and determines whether the target packet is anomalous on the basis of the assigned label.

WO 2022/259317 A1

［続葉有］

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, 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：検出装置（１０）は、パケットの特徴量、各パケットの特徴量に付与されたラベル、及び、判定に使用する閾値を予め記憶する特徴量ＤＢ（１６）と、正常通信のパケットを学習データとして事前に学習済みである第１の自然言語処理モデルを用いて、処理対象のパケットを特徴量に変換するエンコード部（１２）と、第１の自然言語処理モデルを用いて変換された特徴量と、特徴量ＤＢ（１６）において記憶されたデータとを基に、第１の自然言語処理モデルを用いて変換された特徴量にラベルを付与し、付与したラベルを基に処理対象のパケットの異常の有無を判定する判定部（１４）と、を有する。

明　細　書

発明の名称 ： 検出装置、検出方法及び検出プログラム

技術分野

[0001] 本発明は、検出装置、検出方法及び検出プログラムに関する。

背景技術

[0002] ネットワーク内のトラフィックから不正なパケットを検出する技術として、シグネチャ型検出技術や、アノマリ型検出技術がある。

[0003] シグネチャ型検出技術は、事前に攻撃データから攻撃に含まれる特有のシグネチャを生成して、通信とシグネチャのマッチングにより攻撃を検出する。シグネチャ型検出技術は、既知の攻撃を良く検出出来る一方、攻撃の亜種・難読化や未知の攻撃への対応が難しい。また、シグネチャ型検出技術は、シグネチャ生成のために膨大な実攻撃データを収集する必要がある。

[0004] アノマリ型検出技術は、システム内のトラフィックから正常状態を学習して、正常状態の乖離を異常と検出する。アノマリ型検出技術は、シグネチャ型検出技術と比較すると正常な通信データの学習が必要なものの、未知の攻撃も含めて検出可能であり、攻撃データを事前に収集する必要もない。

先行技術文献

特許文献

[0005] 特許文献1：特開２０２０－１０２６７１号公報

非特許文献

[0006] 非特許文献1：Diederik P. Kingma, Max Welling, “Auto-Encoding Variational Bayes”, ICLR 2014., [online], [令和３年５月１４日検索]、インターネット＜ＵＲＬ：https://arxiv.org/pdf/1312.6114.pdf＞

発明の概要

発明が解決しようとする課題

[0007] しかしながら、機械学習を用いたアノマリ型検出技術は、学習に時間を要するため、学習が完了するまでの間、無防備状態のまま、運用と学習を並行

する必要がある。このため、機械学習を用いたアノマリ型検出技術は、学習期間中に攻撃を受けるおそれや、攻撃パケットが混入していた場合には、この攻撃パケットを正常パケットとして誤認して学習するおそれがある。

[0008] シグネチャ型検出技術を併用する方法もあるが、シグネチャ生成のためには事前に様々な攻撃情報を収集する必要がある。したがって、アノマリ型検出技術において、システムの可用性を落とさずに、監視の空白期間を削減する、即時に攻撃を検出可能な学習モデルがあることが望ましい。

[0009] 本発明は、上記に鑑みてなされたものであって、システムの可用性を保持しながら、監視の空白期間を削減することができる検出装置、検出方法及び検出プログラムを提供することを目的とする。

課題を解決するための手段

[0010] 上述した課題を解決し、目的を達成するために、本発明の検出装置は、パケットの特徴量、各パケットの特徴量に付与されたラベル、及び、判定に使用する閾値を予め記憶する記憶部と、正常通信のパケットを学習データとして事前に学習済みである第１の自然言語処理モデルを用いて、処理対象のパケットを特徴量に変換する変換部と、第１の自然言語処理モデルを用いて変換された特徴量と、記憶部において記憶されたデータとを基に、第１の自然言語処理モデルを用いて変換された特徴量にラベルを付与し、付与したラベルを基に処理対象のパケットの異常の有無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

[0011] 本発明によれば、システムの可用性を落とさずに、監視の空白期間を削減することができる。

図面の簡単な説明

[0012] [図1]図１は、実施の形態に係る検出装置の構成の一例を示す図である。

[図2]図２は、ＶＡＥによる検出処理を説明する図である。

[図3]図３は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[図4]図４は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[図5]図５は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[図6]図６は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[図7]図７は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[図8]図８は、ＢＥＲＴモデルを用いた異常判定処理の処理手順を示すフローチャートである。

[図9]図９は、複数のＢＥＲＴモデルを用いた判定処理の処理手順を示すフローチャートである。

[図10]図１０は、プログラムが実行されることにより、検出装置が実現され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

[0013] 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。

[0014] ［実施の形態］

本発明の実施の形態について説明する。本実施の形態では、事前学習した自然言語処理モデルを用いてパケットから変換した特徴量と、過去のパケットの特徴量とを比較することで、パケットの異常の有無を判定する新たな判定方法を、アノマリ型検出モデルの学習期間中に使用する。この判定方法は、学習が不要であり、検出の処理時間が比較対象の過去のパケットの特徴量のデータ量に依存するのみであるため、即時に攻撃を検出可能である。このため、実施の形態では、この判定方法を、アノマリ型検出モデルの学習期間に用いることによって、システムの可用性を保持しながら、監視の空白期間を削減することができる。

[0015] ［検出装置の構成］

続いて、図１を用いて、実施の形態に係る検出装置の構成及び処理について説明する。図１は、実施の形態に係る検出装置の構成の一例を示す図である。

[0016] 実施の形態に係る検出装置１０は、例えば、ＲＯＭ（Read Only Memory

）、ＲＡＭ（Random Access Memory）、ＣＰＵ（Central Processing Unit）等を含むコンピュータ等に所定のプログラムが読み込まれて、ＣＰＵが所定のプログラムを実行することで実現される。図２に示すように、検出装置１０は、収集部１１、エンコード部１２（変換部）、検出部１３、判定部１４、処理制御部１５及び特徴量データベース（ＤＢ）１６を有する。

[0017] 収集部１５１は、処理対象のパケットを収集する。

[0018] エンコード部１５２は、自然言語処理モデル（例えば、ＢＥＲＴ（Bidirectional Encoder Representations from Transformers）モデル）を用いて、処理対象パケットを、特徴量である、１つの固定長ベクトルに変換する。ＢＥＲＴモデルは、正常通信のパケットを学習データとして事前に学習済みである。

[0019] ＢＥＲＴモデルは、１つのパケットを１つの文章とみなし、１つの固定長ベクトルへ変換する規則を学習したモデル、言い換えると、正常通信のパケットにおける内部のバイト列の順序等の頻出パターンを学習したモデルである。

[0020] 例えば、ＢＥＲＴモデルは、文書内のある単語を周辺の単語から予測する、という補助タスクを解くことで、パケットの特徴を反映した良い中間表現、すなわち、固定長ベクトルを習得する。また、ＢＥＲＴモデルは、パケット内のある位置のバイトを、周辺のバイトから予測することで、パケットの特徴を反映したベクトル表現を獲得する。エンコード部１５２は、ＢＥＲＴモデルを用いて、各パケットを、各パケットの特徴を反映した固定長ベクトルに変換する。

[0021] エンコード部１５２は、一つのＢＥＲＴモデル（第１の自然言語処理モデル）を保持するほか、後述するように、このＢＥＲＴモデルが未対応であるプロトコルのパケットを処理する場合には、新たなＢＥＲＴモデル（第２の自然言語処理モデル）を用いてもよい。

[0022] 検出部１３は、検出モデルを用いて、エンコード部１５２によって変換された固定長ベクトルを基に、パケットの異常の有無を検出することで攻撃を

検出する。検出装置１０では、判定部１４（後述）によって正常通信であると判定されたパケットの固定長ベクトルのパターンを学習させる。

[0023] 検出部１５３では、例えば、ＶＡＥ（Variational Auto Encoder）、ＡＥ（Auto Encoder）、ＬｏＦ（Local Outlier Factor）等の教師なし学習による検出モデルを検出モデルとして用いる。以降、検出モデルとして、ＶＡＥを用いる場合を例に説明する。

[0024] 例えば、ＶＡＥでは、正常通信パケットの確率密度を学習後、確率密度の低い通信を異常として検出するため、正常通信パケットのみが分かればよく、全ての悪性データを学習せずとも異常検出が可能である。ＶＡＥは、正常通信のパケットに対応する固定長ベクトルを学習データとして、異常度の学習を行う。

[0025] 検出部１３は、一つのＶＡＥ（第１の検出モデル）を保持する。このほか、エンコード部１２が、未対応プロトコルのパケットの処理のために新たなＢＥＲＴモデルを用いる場合、検出部１３は、この新たなＢＥＲＴモデルが変換した固定長ベクトルを処理するために、新たなＶＡＥ（第２の検出モデル）を用いてもよい。

[0026] 特徴量ＤＢ１６は、パケットの特徴量、各パケットの特徴量に付与されたラベル、及び、判定に使用する閾値を予め記憶する。特徴量は、ＢＥＲＴモデルによって変換されたパケットの固定長ベクトルである。

[0027] ラベルは、正常ラベル、異常ラベル、事前学習ラベルがある。正常ラベルは、正常通信のパケットを変換した固定長ベクトルであることを示すラベルである。異常ラベルは、異常通信のパケットを変換した固定長ベクトルであることを示すラベルである。事前学習ラベルは、事前学習に用いた正常通信のパケットを変換した固定長ベクトルであることを示すラベルである。特徴量ＤＢ１６は、事前学習に用いた固定長ベクトルの全てまたは代表的な固定長ベクトルに、事前学習ラベルを対応付けて記憶する。閾値は、判定部１４における、処理対象のパケットの固定長ベクトルと、特徴量ＤＢ１６に記憶される固定長ベクトルとに対する類似判定に使用される。

[0028] 判定部１４は、エンコード部１２のＢＥＲＴモデルを用いて変換された固定長ベクトルと、特徴量ＤＢ１６において記憶されたデータとを基に、ＢＥＲＴモデルを用いて変換された特徴量にラベルを付与し、付与したラベルを基に処理対象のパケットの異常の有無を判定する。

[0029] 判定部１４は、ＢＥＲＴモデルを用いて変換された固定長ベクトルに対し、閾値以上の類似度を有する固定長ベクトルを特徴量ＤＢ１６から検索する。そして、判定部１４は、検索した固定長ベクトルに付与されたラベルを、ＢＥＲＴモデルによって変換された固定長ベクトルに付与する。判定部１４は、ＢＥＲＴモデルを用いて変換された固定長ベクトルのうち、正常ラベルを付与した固定長ベクトルを、検出部１３のＶＡＥの学習データとして出力する。

[0030] 判定部１４は、事前学習ラベルが付与された固定長ベクトルと、エンコード部１２のＢＥＲＴモデルを用いて変換された処理対象のパケットの固定長ベクトルとの類似度を基に、このＢＥＲＴモデルにおける適正な固定長ベクトルの変換の可否を判定する。

[0031] 処理制御部１５は、判定部１４が、ＢＥＲＴモデルにおいて適正に特徴量が変換されていないと判定した場合、エンコード部１２に、新たなＢＥＲＴモデルを設け、この新たなＢＥＲＴモデルに、処理対象のパケットの固定長ベクトルへの変換を学習させる。

[0032] ［ＶＡＥの処理］

まず、検出部１３のＶＡＥの学習処理及び検出処理について説明する。図２は、ＶＡＥによる検出処理を説明する図である。

[0033] 図２に示すように、収集部１１は、学習対象或いは評価対象のパケットとして、可変長のパケットを複数取得する（図２の（１））。

[0034] エンコード部１２は、各パケットのバイト列の順序等の頻出パターンを学習したＢＥＲＴモデルを用いて、各パケットを、各パケットの特徴を反映した固定長ベクトルにそれぞれ変換する（図２の（２），（３））。

[0035] 検出部１３は、ＶＡＥを用いて、エンコード部１２によって変換された固

定長ベクトルに対する異常度（異常パケットの発生頻度）を取得する。学習段階では、ＶＡＥは、正常通信のパケットに対応する固定長ベクトルに基に、異常度（例えば、アノマリスコア）の学習を行う（図２の（４））。この場合、ＶＡＥが取得する異常度が最小化されるように、ＶＡＥの検出モデルのパラメータが調整される。

[0036] 評価段階では、検出部１３は、ＶＡＥを用いて、エンコード部１２によって変換された固定長ベクトルに対する異常度（例えば、アノマリスコア）を取得する（図２の（５））。そして、検出部１３は、アノマリスコアが所定の閾値を超えている場合に、評価対象のパケットの異常を検出し、アラートを発生する。閾値は、例えば、要求されている検出精度や、検出装置１０のリソース等に応じて、設定される。

[0037] ［ＢＥＲＴモデルを用いた異常判定処理］

次に、ＢＥＲＴモデルを用いた異常判定処理を説明する。図３～図５は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[0038] 検出部１３のＶＡＥでは、通信内容の分析のために、本番環境での異常度を算出するための学習が必要である（図３の（１）及び図４の（Ｂ））。しかしながら、ＶＡＥでは、学習に時間を要するため、学習期間中に攻撃を受けるおそれや、攻撃パケットを正常状態として誤認して学習するおそれがある。

[0039] ここで、適切にチューニングされた検出装置では、エンコード部１２のＢＥＲＴモデルがパケットのプロトコル構造を分析し（図３の（２））、検出部１３のＶＡＥがその環境における通信のパラメータを分析する。このＢＥＲＴモデルは、正常通信のパケットの内部のバイト列の順序等の頻出パターンを学習させることで、事前に作成可能である。

[0040] ここで、ＢＥＲＴモデルのエンコードによって出力された固定長ベクトルを用いることで、パケット同士の近さを比較することが可能である。これを基に、ＢＥＲＴモデルが変換した処理対象のパケットの固定長ベクトルと、予め求めておいた正常通信または異常通信のパケットの固定長ベクトルとの

いずれに類似するかを求めることで、処理対象のパケットが正常または異常であるかを判別できる。そこで、本実施の形態では、ＶＡＥの学習が完了するまで、ＢＥＲＴモデルを用いた異常パケット判定処理を攻撃検出に利用する（図３の（３））。

[0041] 具体的には、異常パケット判定処理として、判定部１４が、ＢＥＲＴモデルが変換した処理対象のパケットの固定長ベクトルと、予め求めておいた正常通信または異常通信のパケットの固定長ベクトルとの類似度を用いて、処理対象のパケットの異常の有無を判定する（図４の（Ａ））。例えば、判定部１４は、類似度として、ｃｏｓ類似度やＬ２ノルムを用いる。

[0042] ＶＡＥを用いた検出処理では、検出の処理時間は一定であるものの、ある程度データを収集した上で学習しないと、誤検出に繋がる場合があり、また、過検出補正はモデル全体の再学習が必要である。

[0043] これに対し、ＢＥＲＴモデルを用いた異常判定処理では、検出の処理時間はデータ量に依存するものの、過去のパケットとの比較のみでパケットの異常の有無を判定することが可能であるため、学習が不要である。また、ＢＥＲＴモデルを用いた異常判定処理では、過検出補正は過去のパケットのラベル付けを行うのみで足り、ラベル付けや利用データの工夫によって検出以外の様々な用途に利用可能である。

[0044] 続いて、図５を参照して、ＢＥＲＴモデルを用いた異常判定処理の適用について説明する。図５に示すように、特徴量ＤＢ１６には、ＢＥＲＴモデルの事前学習で用いた正常通信のパケットの特徴量（固定長ベクトル）、及び、本番学習で用いた正常通信のパケットの特徴量、異常通信のパケットの特徴量と、各パケットに対応付けられたラベルと、判定に使用するための閾値とが記憶される（矢印Ｙ１）。

[0045] 検出部１３のＶＡＥの学習中、判定部１４は、事前学習したエンコード部１２のＢＥＲＴモデルがパケットから変換した固定長ベクトルと（矢印Ｙ２）、特徴量ＤＢ１６が記憶するデータ（矢印Ｙ３）とを用いて、入力されたパケットのラベル付けを行う。

[0046] 具体的には、判定部１４は、ＢＥＲＴモデルを用いて変換された固定長ベクトルと、特徴量ＤＢ１６の固定長ベクトルとの間の類似度を算出する（図５の（１））。判定部１４は、閾値以上の類似度を有する固定長ベクトルを特徴量ＤＢ１６から抽出する。そして、判定部１４は、抽出した固定長ベクトルに付与されたラベルを、処理対象のパケットの固定長ベクトルに付与する。判定部１４は、付与したラベルを基に処理対象のパケットの異常の有無を判定する。

[0047] 判定部１４は、付与したラベルが異常である場合は、処理対象のパケットが異常通信のパケットと類似すると判定し（矢印Ｙ４）、異常アラートを発生させる（図５の（２））。そして、判定部１４は、付与したラベルが正常である場合は、処理対象のパケットが正常通信のパケットと類似すると判定し（矢印Ｙ５）、ＶＡＥの学習データに利用する（図５の（３））。

[0048] また、判定部１４は、算出した類似度が閾値を下回る場合、この処理対象のパケットが未知のデータであるとし、管理者に確認要求を通知する。管理者は、この通知を参照すると、処理対象のパケットの正常性を判断し（図５の（４））、判断結果を検出装置１０に入力する。この判断結果は、判定部１４によって、特徴量ＤＢ１６にフィードバックされ、次回の判定に使用されることで、過検出を抑制する。言い換えると、判定部１４は、特徴量にラベルが付与されていない処理対象のパケットに関する通知を出力し、該処理対象のパケットに対するラベルが入力された場合、特徴量ＤＢ１６に、該処理対象のパケットの特徴量と、入力されたラベルとを対応付けて記憶させる。

[0049] また、判定部１４は、事前学習ラベルが付された特徴量との類似度を算出し、算出した類似度が閾値を下回る場合には、ＢＥＲＴモデルが未対応であるプロトコルのパケットとして管理者への通知を行い（矢印Ｙ６）、正常度判定を行わない。または、判定部は、7-tuple判定を利用して、判定を行ってもよい。

[0050] 判定部１４における判定例を説明する。例えば、パケット１については、

管理者によって正常と確認される。判定部１４は、パケットの１の特徴量に正常ラベルを対応付けて特徴量ＤＢ１６に保存する。パケット２については、判定部１４は、パケット１との類似度を算出し、類似度が閾値を下回るため、管理者に確認要求を通知する。パケット２については、管理者によって正常と確認されたため、判定部１４は、パケットの２の特徴量に正常ラベルを対応付けて特徴量ＤＢ１６に保存する。

[0051] 判定部１４は、パケット３については、パケット１，２との類似度を算出し、いずれのパケットについても類似度が閾値を下回るため、管理者に確認要求を通知する。パケット３については、管理者によって異常と確認されたため、判定部１４は、パケットの３の特徴量に異常ラベルを対応付けて特徴量ＤＢ１６に保存する。

[0052] 判定部１４は、パケット４については、パケット１～３との類似度を算出し、パケット２と最も類似するため、正常通信と判定する。なお、パケット４については、特徴量ＤＢ１６への特徴量等の保存は行わない。

[0053] 判定部１４は、パケット５については、パケット１～３との類似度を算出し、パケット３と最も類似するため、異常通信と判定し、アラートを出力する。なお、初期の過検出抑制のために、判定部１４は、最初の数分の間は、処理パケットを正常データとして処理し、各特徴量に正常ラベルを付与して特徴量ＤＢ１６に保管してもよい。また、新たな通信パターンが発生するたびに特徴量ＤＢ１６のレコードが増え、パフォーマンスが落ちることから、検出装置１０は、検出部１３のＶＡＥの学習が完了した場合には、検出方法を、ＶＡＥを介する方法（図３の（Ｂ））に切り替える。

[0054] ［複数のＢＥＲＴモデルを用いた判定処理］

また、検出装置１０では、複数のＢＥＲＴモデル及びＶＡＥを用いて判定を行ってもよい。図６及び図７は、ＢＥＲＴモデルを用いた異常判定処理を説明する図である。

[0055] 検出装置１０では、第１ＶＡＥ１３－１の学習期間中、事前学習済みの第１ＢＥＲＴモデル１２－１（第１の自然言語処理モデル）が正常通信である

と判定したパケットについては、第１ＢＥＲＴモデル１２－１において対応済みであるプロトコルのパケットとして（矢印Ｙ１１）、この第１ＢＥＲＴモデル１２－１に対応する第１ＶＡＥ１３－１に出力する。

[0056] そして、事前学習に用いたパケットに含まれていないプロトコル（独自プロトコルやマイナープロトコル）は、事前学習データの代表的な特徴量と比較することで検出が可能である。判定部１４は、事前学習ラベルが付された特徴量と処理対象のパケットの特徴量との類似度を算出し、算出した特徴量が、閾値を下回る場合には、処理対象のパケットが、第１ＢＥＲＴモデル１２－１において未対応であるプロトコルの通信であると判定する（図６の（１））。

[0057] ここで、未対応であるプロトコルの通信の学習のために、第１ＢＥＲＴモデル１２－１全体を再学習すると、ＢＥＲＴモデルが生成する特徴量そのものが変化してしまい、第１ＶＡＥ１３－１も全て再学習する必要がある。

[0058] このため、検出装置１０では、第１ＢＥＲＴモデル１２－１が対応していないプロトコルのみ、新規に、第２ＢＥＲＴモデル１２－２（第２の自然言語処理モデル）と、この第２ＢＥＲＴモデル１２－２に対応する第２ＶＡＥ１３－２（第２の検出モデル）とを設けて、検出に利用する（図６の（２））。検出装置１０は、第２ＢＥＲＴモデル１２－２に、処理対象のパケットの特徴量への変換を学習させる。そして、判定部１４は、第２ＢＥＲＴモデル１２－２が変換した特徴量を、第２ＶＡＥ１３－２の学習データとして出力する。このように、検出装置１０によれば、第１ＢＥＲＴモデル１２－１が未対応であるプロトコルの通信パケットが入力された場合、第１ＶＡＥ１３－１の再学習を行わずとも、適切に処理可能である。

[0059] そして、監視中においては、図７に示すように、判定部１４は、第１ＢＥＲＴモデル１２－１と第２ＢＥＲＴモデル１２－２とのうち、処理対象のパケットの変換後の特徴量が、学習データの特徴量と最も類似するＢＥＲＴモデルを選択し、選択したＢＥＲＴモデルに対応するＶＡＥモデルを用いて攻撃の検出を実行させる。

[0060] 例えば、判定部１４は、処理対象のパケットについて、第１ＢＥＲＴモデル１２－１が変換した特徴量と、特徴量ＤＢ１６が保持する事前学習に用いた正常通信のパケットの特徴量との類似度を算出する。そして、判定部１４は、処理対象のパケットについて、第２ＢＥＲＴモデル１２－２が変換した特徴量と、特徴量ＤＢ１６－２が保持する、第２ＢＥＲＴモデル１２－２が学習した本番環境において学習されたパケットの特徴量との類似度を算出する。

[0061] 続いて、判定部１４は、算出した類似度を比較し、類似度が高い方のＢＥＲＴモデルに対応するＶＡＥを選択して、検出を実行させる。このように、検出装置１０は、検出に適したＢＥＲＴモデル及びＶＡＥを選択して検出を行うことで、検出精度を上げることができる。なお、検出装置１０は、ＶＡＥの再学習のタイミングに合わせて、第１ＢＥＲＴモデル１２－１と第２ＢＥＲＴモデル１２－２も１つのモデルに圧縮してもよい。

[0062] ［ＢＥＲＴモデルを用いた異常判定処理の処理手順］

次に、ＶＡＥの学習中における、ＢＥＲＴモデルを用いた異常判定処理の処理手順について説明する。図８は、ＢＥＲＴモデルを用いた異常判定処理の処理手順を示すフローチャートである。

[0063] 図８に示すように、処理対象のパケットが入力されると（ステップＳ１１）、エンコード部１２は、ＢＥＲＴモデルを用いて、特徴量である固定長ベクトルに変換する（ステップＳ１２）。

[0064] 判定部１４は、ＢＥＲＴモデルによって変換された処理対象のパケットの特徴量と、閾値以上の類似度を有する特徴量及びそのラベルを特徴量ＤＢ１６から検索する（ステップＳ１３）。判定部１４は、検索した特徴量のラベルを、処理対象のパケットの特徴量に付与する。続いて、判定部１４は、処理対象のパケットの特徴量に付与したラベルが正常ラベルであるか否かを判定する（ステップＳ１４）。

[0065] ラベルが正常ラベルである場合（ステップＳ１４：Ｙｅｓ）、判定部１４は、この処理対象のパケットの特徴量を、検出部１３のＶＡＥの学習データ

として出力し（ステップＳ１５）、検出部１３のＶＡＥの学習を進めさせる。

[0066] これに対し、ラベルが正常ラベルではない場合（ステップＳ１４：Ｎｏ）、判定部１４は、処理対象のパケットの特徴量に付与したラベルが異常であるか否かを判定する（ステップＳ１６）。ラベルが異常ラベルである場合（ステップＳ１６：Ｙｅｓ）、判定部１４は、処理対象のパケットが異常である旨を示すアラートを発する（ステップＳ１７）。

[0067] また、ラベルが異常ラベルでない場合（ステップＳ１６：Ｎｏ）、判定部１４は、処理対象のパケットの特徴量に付与したラベルが事前学習ラベルであるか否かを判定する（ステップＳ１８）。

[0068] ラベルが事前学習ラベルである場合（ステップＳ１８：Ｙｅｓ）、処理対象のパケットが未知のデータである旨を示すアラートを発する（ステップＳ１９）。判定部１４は、ステップＳ１７，Ｓ１９のアラートに対して、管理者から、このパケットのラベルを含むフィードバックを取得すると（ステップＳ２０）、特徴量ＤＢ１６に、この処理対象のパケットの特徴量に対応させて、管理者の判断したラベルを保存し、類似判定の際に使用する閾値を更新する（ステップＳ２１）。

[0069] そして、判定部１４は、管理者によって判断されたラベルが正常ラベルである場合には（ステップＳ２２：Ｙｅｓ）、この処理対象のパケットの特徴量を、検出部１３のＶＡＥの学習データとして出力し（ステップＳ２３）、検出部１３のＶＡＥの学習を進めさせる。管理者によって判断されたラベルが正常ラベルでない場合には（ステップＳ２２：Ｎｏ）、この処理対象のパケットに対する異常判定処理を終了する。

[0070] そして、ラベルが事前学習ラベルではない場合（ステップＳ１８：Ｎｏ）、処理対象のパケットがＢＥＲＴモデルの未対応プロトコルのパケットである旨を示すアラートを発する（ステップＳ２４）。この場合、検出装置１０は、エンコード部１２に、新たなＢＥＲＴモデルを設け（ステップＳ２５）、この新たなＢＥＲＴモデルに、処理対象のパケットの固定長ベクトルへの

変換を学習させる。そして、検出装置１０は、検出部１３の新たなＶＡＥに、新たなＢＥＲＴモデルが変換した固定長ベクトルを学習データとして学習させる。

[0071] ［複数のＢＥＲＴモデルを用いた異常判定処理の処理手順］

図９は、複数のＢＥＲＴモデルを用いた判定処理の処理手順を示すフローチャートである。

[0072] 処理対象のパケットが入力されると（ステップＳ３１）、処理対象のパケットについて、第１ＢＥＲＴモデル１２－１及び第２ＢＥＲＴモデル１２－２は、特徴量の変換を行う（ステップＳ３２）。

[0073] 判定部１４は、第１ＢＥＲＴモデル１２－１が変換した特徴量と、特徴量ＤＢ１６が保持する事前学習に用いた正常通信のパケットの特徴量との類似度、及び、第２ＢＥＲＴモデル１２－２が変換した特徴量と、特徴量ＤＢ１６－２が保持する特徴量との類似度を算出する。そして、判定部１４は、算出した類似度を比較し、類似度が高いＢＥＲＴモデルを判定する（ステップＳ３３）。

[0074] 類似度が高いＢＥＲＴモデルが第１ＢＥＲＴモデル１２－１である場合には（ステップＳ３３：第１ＢＥＲＴモデル１２－１）、判定部１４は、第１ＢＥＲＴモデル１２－１が変換した特徴量を第１ＶＡＥ１３－１に入力し、第１ＶＡＥ１３－１を用いて検出を実行させる（ステップＳ３４）。類似度が高いＢＥＲＴモデルが第２ＢＥＲＴモデル１２－２である場合には（ステップＳ３３：第２ＢＥＲＴモデル１２－２）、第２ＢＥＲＴモデル１２－２が変換した特徴量を第２ＶＡＥ１３－２に入力し、第２ＶＡＥ１３－２を用いて検出を実行させる（ステップＳ３５）。

[0075] ［実施の形態の効果］

実施の形態に係る検出装置１０では、事前学習したＢＥＲＴモデルを用いてパケットから変換した特徴量と、過去のパケットの特徴量とを比較することで、パケットの異常の有無を判定する新たな判定方法を適用する。この判定方法は、監視時における学習が不要であり、検出の処理時間が比較対象の

過去のパケットの特徴量のデータ量に依存するのみであるため、即時に攻撃を検出可能である。このため、検出装置１０では、この判定方法を、アノマリ型検出モデルの学習期間に用いることによって、システムの可用性を保持しながら、監視の空白期間を削減することができる。

[0076] なお、ＢＥＲＴモデルは、事前学習後に別環境のデータを変換する際も正しく認識するか認証済みであり、ＢＥＲＴモデルを用いた異常の有無の判定も精度よく実行可能である。

[0077] ［実施の形態のシステム構成について］

検出装置１０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、検出装置１０の機能の分散及び統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散または統合して構成することができる。

[0078] また、検出装置１０においておこなわれる各処理は、全部または任意の一部が、ＣＰＵ、ＧＰＵ（Graphics Processing Unit）、及び、ＣＰＵ、ＧＰＵにより解析実行されるプログラムにて実現されてもよい。また、検出装置１０においておこなわれる各処理は、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てもよい。

[0079] また、実施の形態において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的に行うこともできる。もしくは、手動的におこなわれるものとして説明した処理の全部また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、上述及び図示の処理手順、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適宜変更することができる。

[0080] ［プログラム］

図１２は、プログラムが実行されることにより、検出装置１０が実現され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。

[0081] メモリ１０１０は、ＲＯＭ１０１１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。

[0082] ハードディスクドライブ１０９０は、例えば、ＯＳ（Operating System）１０９１、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、検出装置１０の各処理を規定するプログラムは、コンピュータ１０００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、検出装置１０及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（Solid State Drive）により代替されてもよい。

[0083] また、上述した実施の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。

[0084] 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。

[0085] 以上、本発明者によってなされた発明を適用した実施の形態について説明したが、本実施の形態による本発明の開示の一部をなす記述及び図面により本発明は限定されることはない。すなわち、本実施の形態に基づいて当業者等によりなされる他の実施の形態、実施例及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

[0086] １０ 検出装置

１１ 収集部

１２ エンコード部

１３ 検出部

１４ 判定部

１５ 処理制御部

１６ 特徴量ＤＢ

請求の範囲

[請求項1] パケットの特徴量、各パケットの特徴量に付与されたラベル、及び、判定に使用する閾値を予め記憶する記憶部と、

正常通信のパケットを学習データとして事前に学習済みである第１の自然言語処理モデルを用いて、処理対象のパケットを特徴量に変換する変換部と、

前記第１の自然言語処理モデルを用いて変換された特徴量と、前記記憶部において記憶されたデータとを基に、前記第１の自然言語処理モデルを用いて変換された特徴量にラベルを付与し、付与したラベルを基に前記処理対象のパケットの異常の有無を判定する判定部と、

を有することを特徴とする検出装置。

[請求項2] 前記判定部は、前記特徴量に前記ラベルが付与されていない前記処理対象のパケットに関する通知を出力し、該処理対象のパケットに対するラベルが入力された場合、前記記憶部に、該処理対象のパケットの特徴量と、入力された前記ラベルとを対応付けて記憶させることを特徴とする請求項１に記載の検出装置。

[請求項3] 前記判定部は、前記ラベルを付与した特徴量に対して、付与した前記ラベルが誤りであることが入力された場合には、前記記憶部が記憶する前記閾値を更新することを特徴とする請求項１または２に記載の検出装置。

[請求項4] 前記判定部は、前記第１の自然言語処理モデルを用いて変換された特徴量のうち、正常ラベルを付与した特徴量を、攻撃を検出する第１の検出モデルの学習データとして出力することを特徴とする請求項１～３のいずれか一つに記載の検出装置。

[請求項5] 前記記憶部は、事前学習に用いた特徴量の全てまたは代表的な特徴量に、事前学習に用いた特徴量であることを示す事前学習ラベルを対応付けて記憶し、

前記判定部は、前記事前学習ラベルが付与された特徴量と、前記第

１の自然言語処理モデルを用いて変換された前記処理対象のパケットの特徴量との類似度を基に、前記第１の自然言語処理モデルにおける適正な特徴量の変換の可否を判定することを特徴とする請求項１～４のいずれか一つに記載の検出装置。

[請求項6] 前記判定部が、前記第１の自然言語処理モデルにおいて適正に特徴量が変換されていないと判定した場合、前記変換部に、新たな第２の自然言語処理モデルを設け、前記第２の自然言語処理モデルに前記処理対象のパケットの特徴量への変換を学習させる処理制御部をさらに有し、

前記判定部は、前記第２の自然言語処理モデルが変換した特徴量を、攻撃を検出する第２の検出モデルの学習データとして出力する請求項５に記載の検出装置。

[請求項7] 前記判定部は、前記第１の自然言語処理モデルと前記第２の自然言語処理モデルとのうち、変換後の特徴量が、学習データであるパケットの特徴量と最も類似する自然言語処理モデルを選択し、選択した自然言語処理モデルに対応する検出モデルを用いて攻撃の検出を実行させることを特徴とする請求項６に記載の検出装置。

[請求項8] 検出装置が実行する検出方法であって、

正常通信のパケットを学習データとして事前に学習済みである第１の自然言語処理モデルを用いて、処理対象のパケットを特徴量に変換する工程と、

前記第１の自然言語処理モデルを用いて変換された特徴量と、予め求められたパケットの特徴量、各パケットの特徴量に付与されたラベル、及び、判定に使用する閾値とを基に、前記第１の自然言語処理モデルを用いて変換された特徴量にラベルを付与し、付与したラベルを基に前記処理対象のパケットの異常の有無を判定する工程と、

を含んだことを特徴とする検出方法。

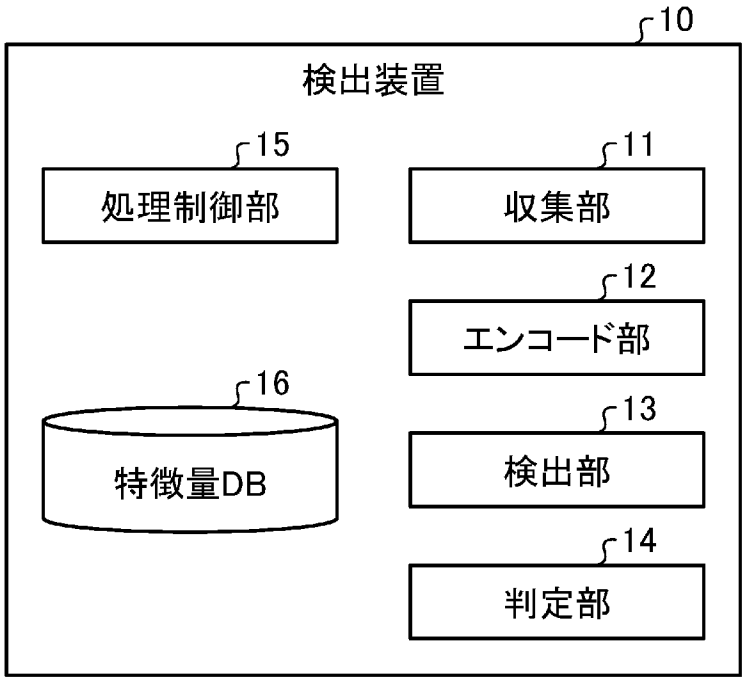
[請求項9] 正常通信のパケットを学習データとして事前に学習済みである第１

の自然言語処理モデルを用いて、処理対象のパケットを特徴量に変換するステップと、

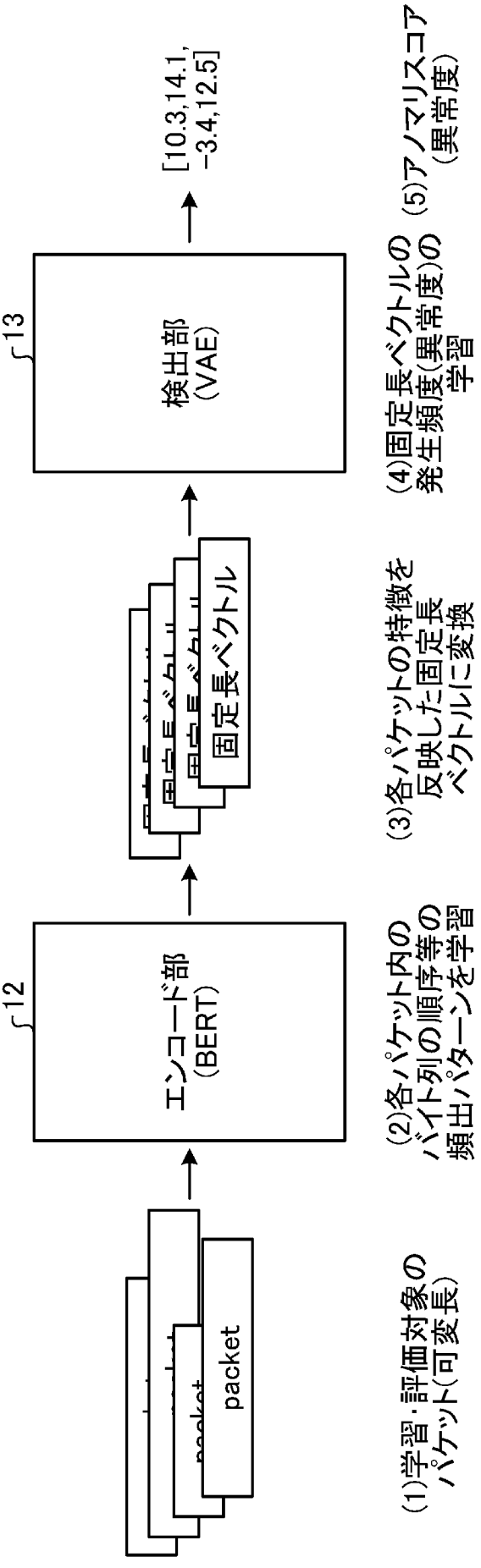
前記第１の自然言語処理モデルを用いて変換された特徴量と、予め求められたパケットの特徴量、各パケットの特徴量に付与されたラベル、及び、判定に使用する閾値とを基に、前記第１の自然言語処理モデルを用いて変換された特徴量にラベルを付与し、付与したラベルを基に前記処理対象のパケットの異常の有無を判定するステップと、

をコンピュータに実行させる検出プログラム。

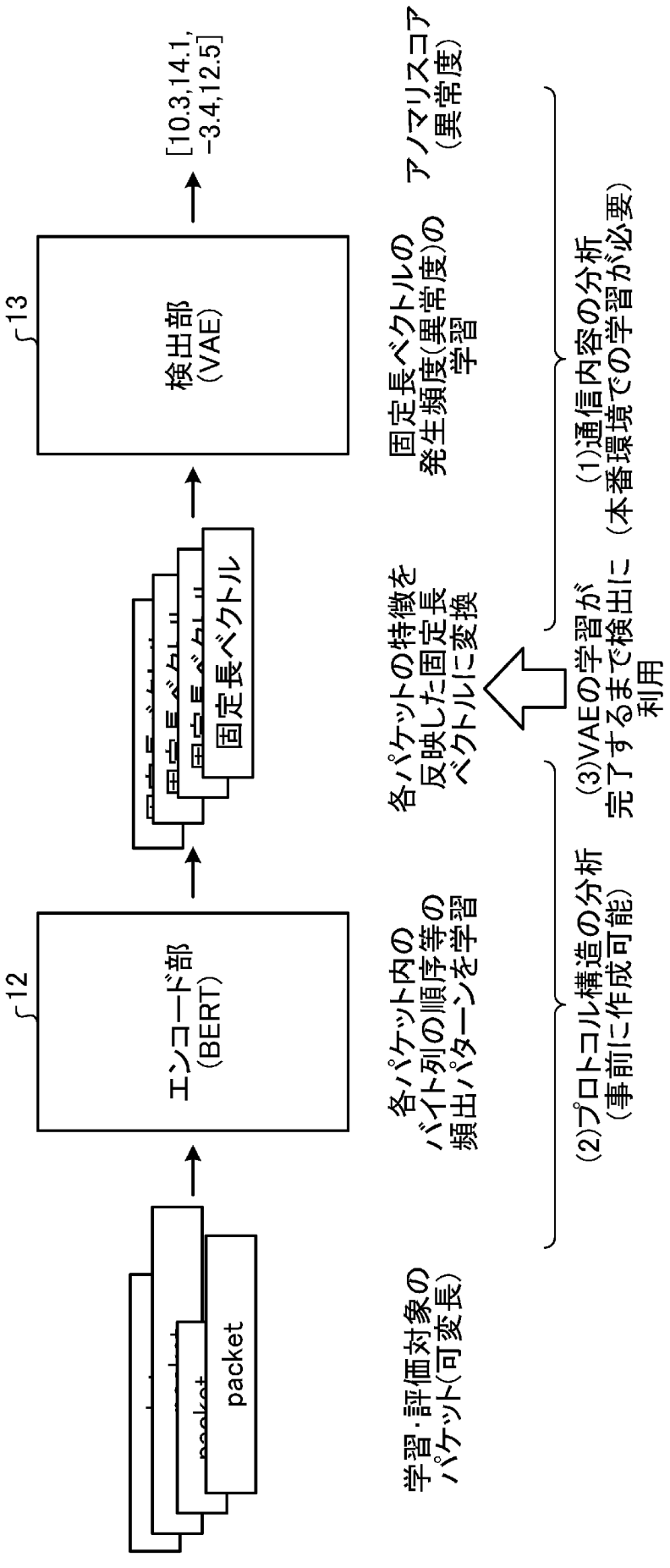
[図1]



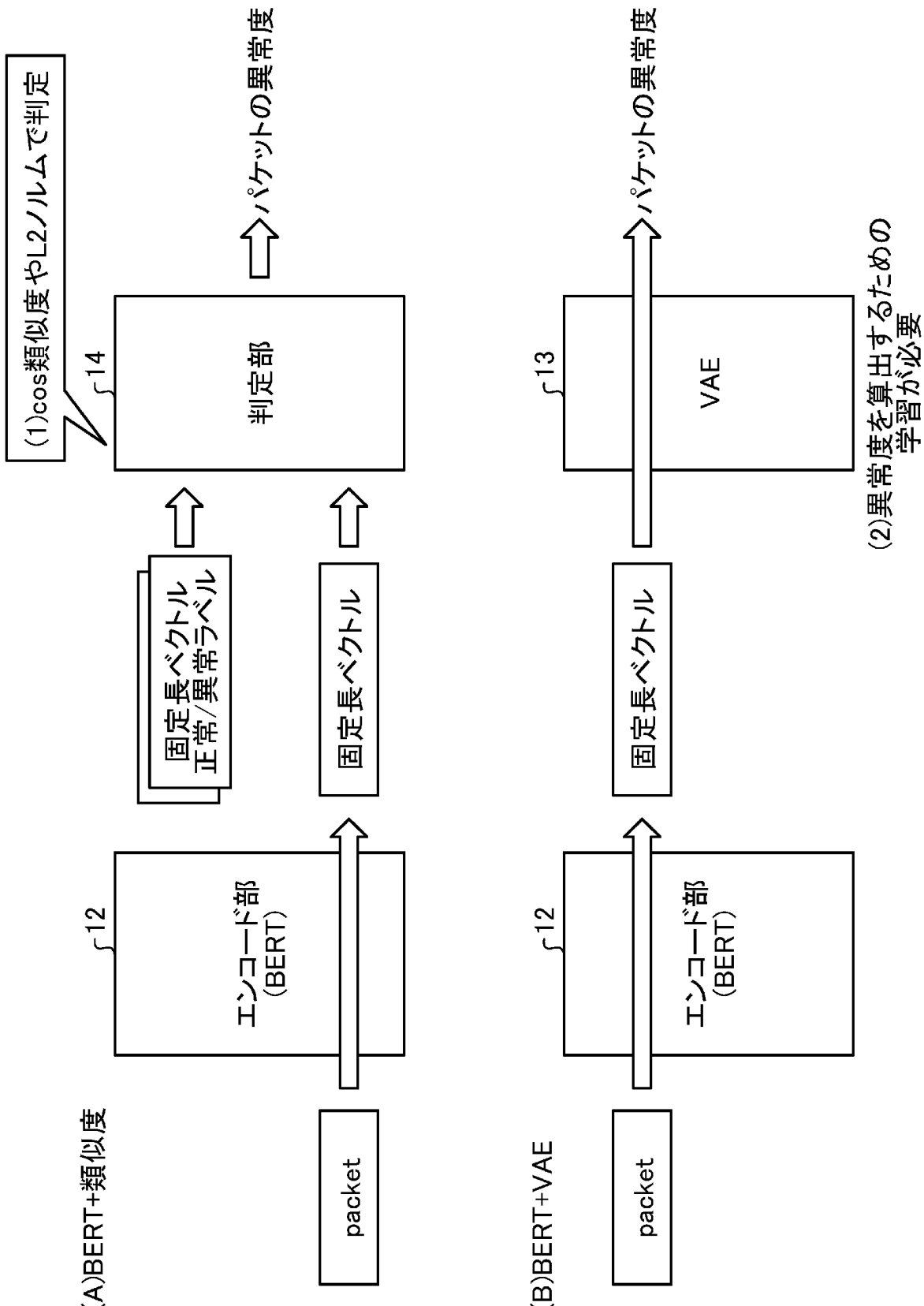
[図2]


packet
エンコード部
(BERT)
12
固定長ベクトル
検出部
(VAE)
13
[10.3,14.1,
−3.4,12.5]
(1)学習・評価対象の
パケット(可変長)
(2)各パケット内の
バイト列の順序等の
頻出パターンを学習
(3)各パケットの特徴を
反映した固定長
ベクトルに変換
(4)固定長ベクトルの
発生頻度(異常度)の
学習
(5)アノマリスコア
(異常度)

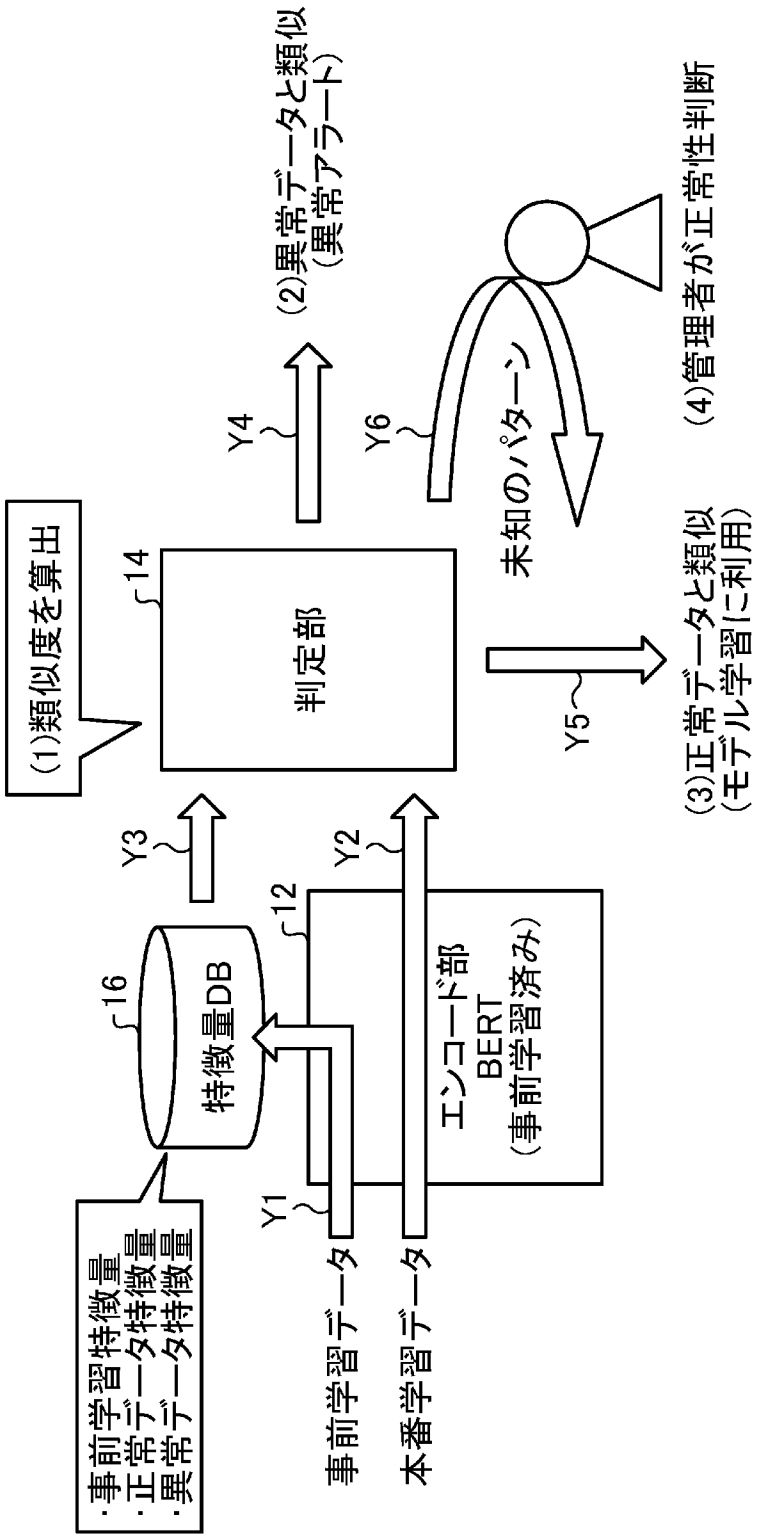
[図3]


学習・評価対象の
パケット(可変長)
packet
12
エンコード部
(BERT)
各パケット内の
バイト列の順序等の
頻出パターンを学習
固定長ベクトル
各パケットの特徴を
反映した固定長
ベクトルに変換
13
検出部
(VAE)
[10.3,14.1,
-3.4,12.5]
固定長ベクトルの
発生頻度(異常度)の
学習
アノマリスコア
(異常度)
(2)プロトコル構造の分析
(事前に作成可能)
(3)VAEの学習が
完了するまで検出に
利用
(1)通信内容の分析
(本番環境での学習が必要)

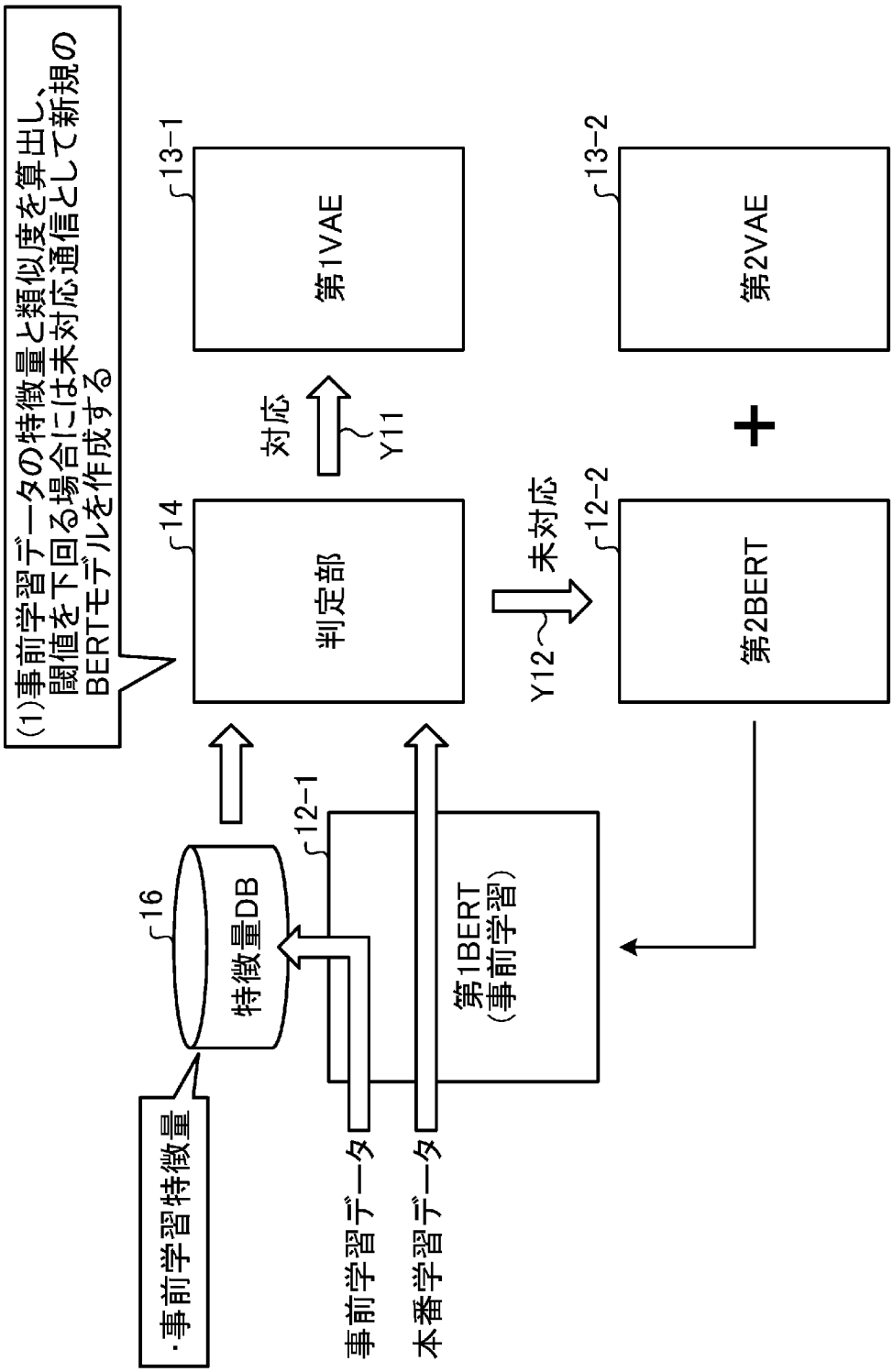
[図4]


(A)BERT+類似度
packet
エンコード部
(BERT)
12
固定長ベクトル
固定長ベクトル
正常/異常ラベル
判定部
14
(1)cos類似度やL2ノルムで判定
パケットの異常度
(B)BERT+VAE
packet
エンコード部
(BERT)
12
固定長ベクトル
VAE
13
パケットの異常度
(2)異常度を算出するための
学習が必要

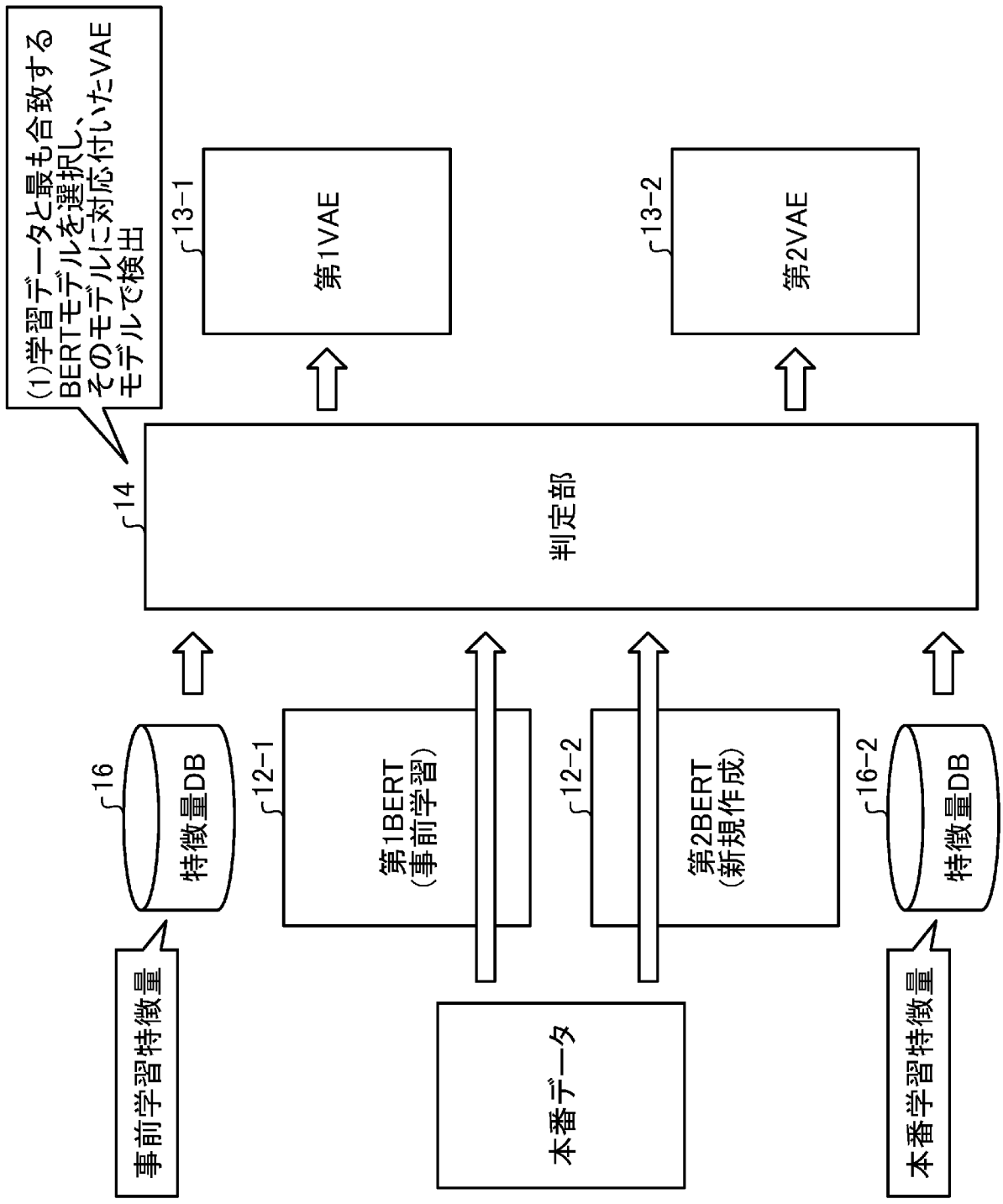
[図5]


・事前学習特徴量
・正常データ特徴量
・異常データ特徴量
16
特徴量DB
12
エンコード部
BERT
(事前学習済み)
Y1
事前学習データ
Y2
本番学習データ
Y3
(1)類似度を算出
14
判定部
Y4
(2)異常データと類似
(異常アラート)
Y5
(3)正常データと類似
(モデル学習に利用)
Y6
未知のパターン
(4)管理者が正常性判断

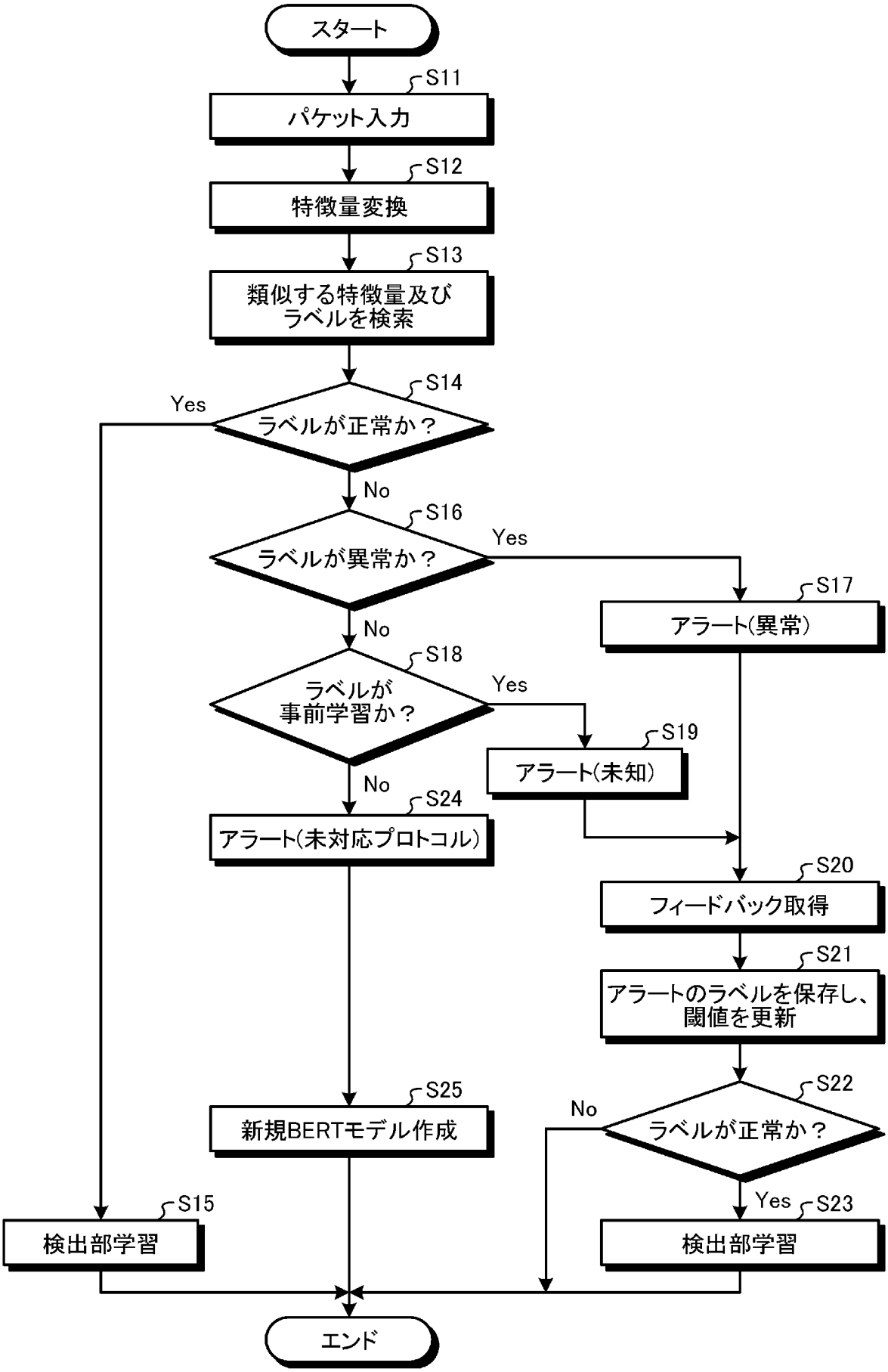
[図6]


(1)事前学習データの特徴量と類似度を算出し、
閾値を下回る場合には未対応通信として新規の
BERTモデルを作成する
13-1
第1VAE
13-2
第2VAE
対応
Y11
14
判定部
未対応
Y12
12-2
第2BERT
+
16
特徴量DB
12-1
第1BERT
(事前学習)
・事前学習特徴量
事前学習データ
本番学習データ

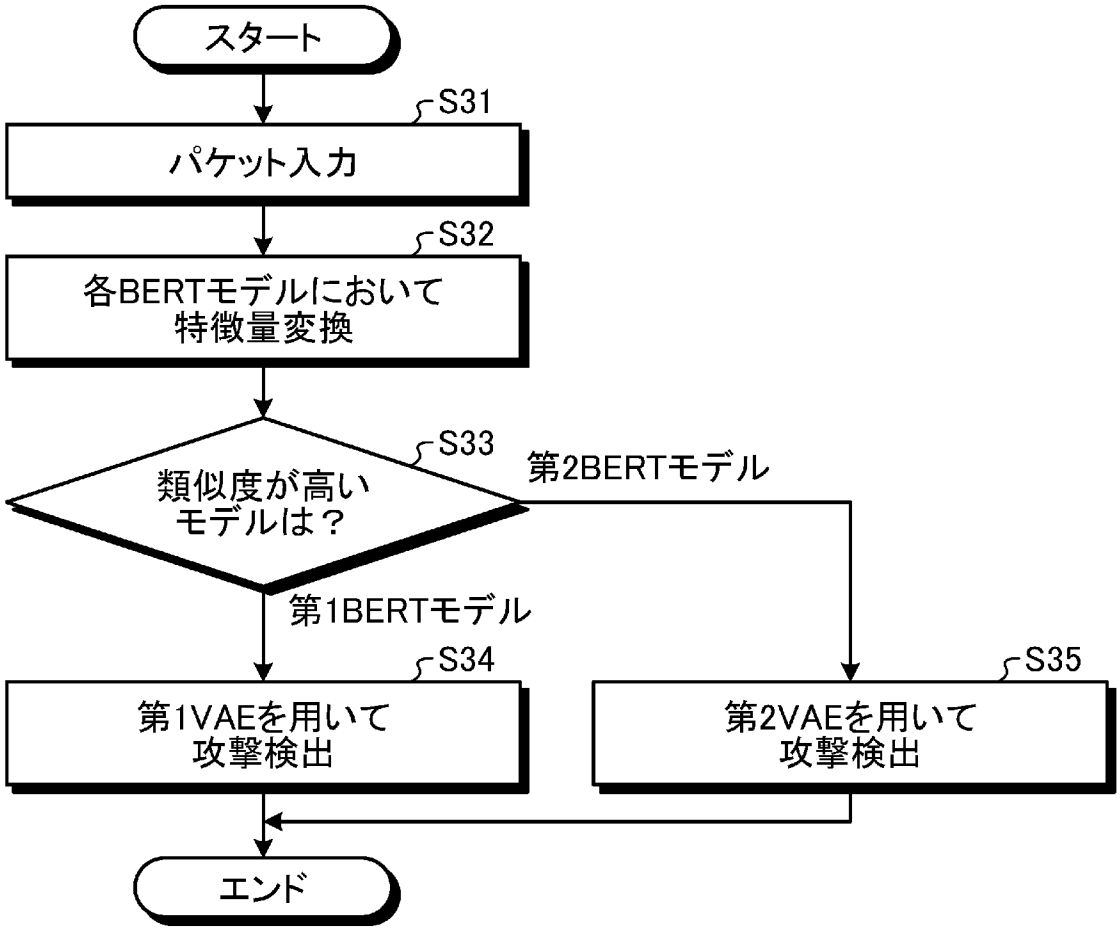
[図7]


(1)学習データと最も合致する
BERTモデルを選択し、
そのモデルに対応付いたVAE
モデルで検出
14
判定部
13-1
第1VAE
13-2
第2VAE
16
特徴量DB
12-1
第1BERT
(事前学習)
12-2
第2BERT
(新規作成)
16-2
特徴量DB
事前学習特徴量
本番データ
本番学習特徴量

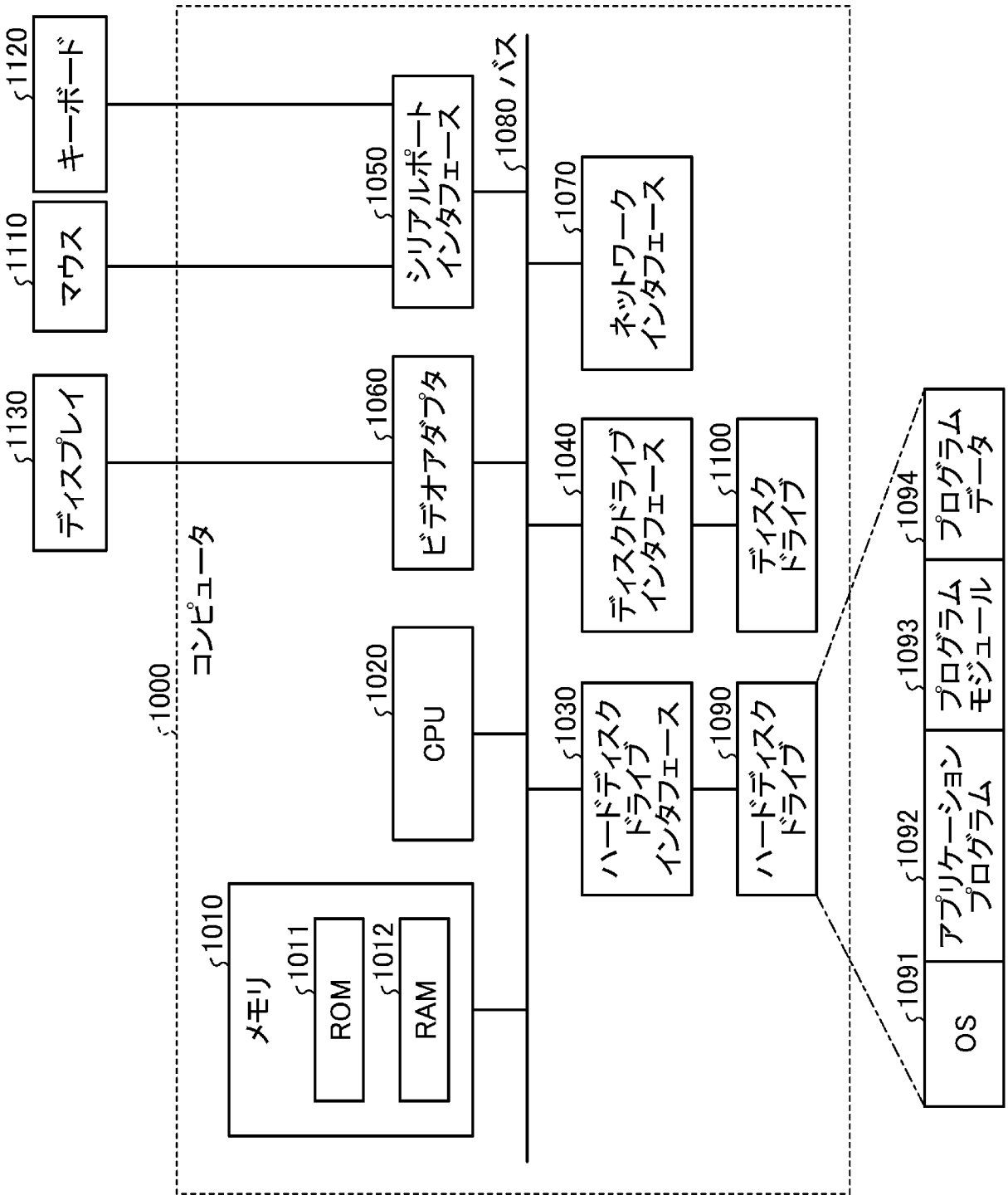
[図8]


スタート
S11
パケット入力
S12
特徴量変換
S13
類似する特徴量及び
ラベルを検索
S14
ラベルが正常か？
Yes
No
S16
ラベルが異常か？
Yes
S17
アラート(異常)
No
S18
ラベルが
事前学習か？
Yes
S19
アラート(未知)
No
S24
アラート(未対応プロトコル)
S20
フィードバック取得
S21
アラートのラベルを保存し、
閾値を更新
S22
ラベルが正常か？
No
Yes
S23
検出部学習
S25
新規BERTモデル作成
S15
検出部学習
エンド

[図9]


スタート
S31
パケット入力
S32
各BERTモデルにおいて
特徴量変換
S33
類似度が高い
モデルは？
第2BERTモデル
第1BERTモデル
S34
第1VAEを用いて
攻撃検出
S35
第2VAEを用いて
攻撃検出
エンド

[図10]


1000
コンピュータ
1120
キーボード
1110
マウス
1130
ディスプレイ
1050
シリアルポート
インタフェース
1060
ビデオアダプタ
1080 バス
1070
ネットワーク
インタフェース
1040
ディスクドライブ
インタフェース
1100
ディスク
ドライブ
1020
CPU
1030
ハードディスク
ドライブ
インタフェース
1090
ハードディスク
ドライブ
1010
メモリ
1011
ROM
1012
RAM
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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/021581

A. CLASSIFICATION OF SUBJECT MATTER
H04L 12/70(2013.01)i
FI: H04L12/70 100Z

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)
H04L12/70

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.
X A	江田 智尊 外５名，分散表現を用いたネットワーク通信ログのアノマリ検知，マルチメディア，分散，協調とモバイル(DICOM02020) シンポジウム論文集 情報処理学会シンポジウムシリーズ vol. 2020 no. 1 [DVD-ROM] IPSJ Symposium Series, 24 June 2020, pp. 698-705, pp. 698-705, (KODA, Satoru et al. Anomalous IP Address Detection on Traffic Logs Using Novel Word Embedding.), non-official translation (Proceedings of Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOM02020). IPSJ Symposium Series vol. 2020, no. 1 [DVD-ROM].)	1-5, 8-9 6-7
A	JP 2007-96735 A (FUJITSU LTD) 12 April 2007 (2007-04-12) entire text, all drawings	1-9

☐ 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
12 August 2021 (12.08.2021)	31 August 2021 (31.08.2021)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/021581

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2007-96735 A	12 Apr. 2007	US 2007/0074272 A1 entire text, all drawings	

国際調査報告

国際出願番号
PCT/JP2021/021581

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 12/70(2013.01)i
FI: H04L12/70 100Z

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））

H04L12/70

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
X	江田 智尊 外５名，分散表現を用いたネットワーク通信ログのアノマリ検知 ，マルチメディア，分散，協調とモバイル（ＤＩＣＯＭＯ２０２０）シンポジウム論文集 情報処理学会シンポジウムシリーズ Ｖｏｌ．２０２０ Ｎｏ．１ [ＤＶＤ－ＲＯＭ] IPSJ Symposium Series, 2020.06.24, pp.698～705 pp.698～705	1-5,8-9
A		6-7
A	JP 2007-96735 A (富士通株式会社) 12.04.2007 (2007-04-12) 全文、全図	1-9

☐ 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
12.08.2021	31.08.2021

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）
野元　久道 5X 9184

電話番号 03-3581-1101 内線 3596

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/JP2021/021581

引用文献	公表日	パテントファミリー文献	公表日
JP 2007-96735 A	12.04.2007	US 2007/0074272 A1 全文、全図	