(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9月15日(15.09.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/190198 A1

(51) 国際特許分類:
H04L 12/70 (2013.01)

(21) 国際出願番号： PCT/JP2021/009228

(22) 国際出願日： 2021年3月9日(09.03.2021)

(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).

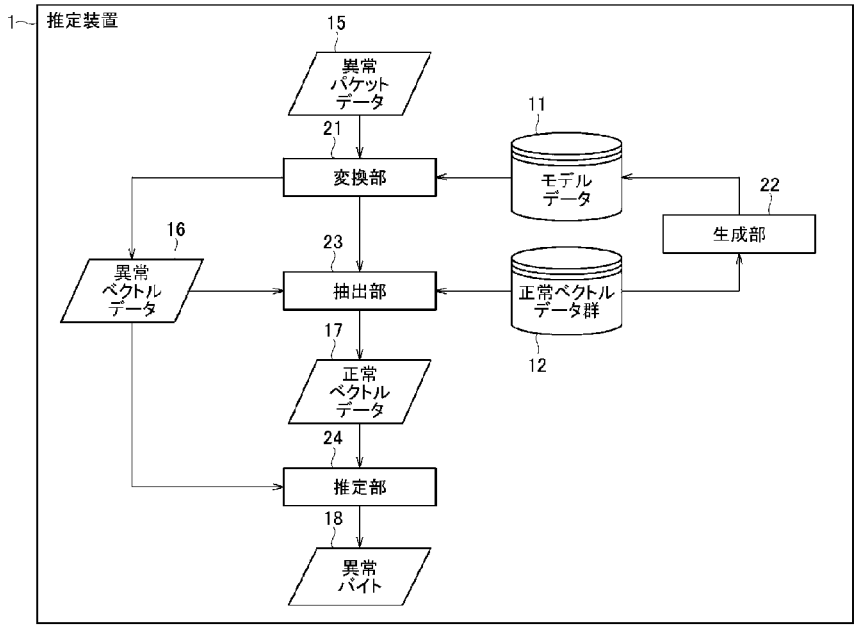
(72) 発明者: 山中 友貴 (**YAMANAKA Yuki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

(74) 代理人: 三好 秀和，外 (**MIYOSHI Hidekazu** et al.); 〒1050001 東京都港区虎ノ門１丁目２番８号 虎ノ門琴平タワー 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, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

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

(54) 発明の名称： 推定装置、推定方法およびプログラム



1 Estimation device
11 Model data
12 Normal vector data group
15 Abnormal packet data
16 Abnormal vector data
17 Normal vector data
18 Abnormal byte
21 Conversion unit
22 Generation unit
23 Extraction unit
24 Estimation unit

(57) **Abstract:** An estimation device 1 comprises: a conversion unit 21 that converts abnormal packet data 15 into abnormal vector data 16 by using a model for converting packet data into vector data in which a vector representing a feature of the value of each byte of the packet data is associated with the byte; an extraction unit 23 that extracts, from a plurality of pieces of normal vector data into which a plurality of pieces of normal packet data have been converted by using the model, normal vector data 17 having a relatively high similarity to the abnormal vector data 16; and an estimation unit

WO 2022/190198 A1

［続葉有］

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))

24 that estimates an abnormal byte in the abnormal packet data 15 from the similarity between a vector corresponding to each byte of the abnormal vector data 16 and a vector corresponding to each byte of the extracted normal vector data 17.

(57) 要約:推定装置１は、パケットデータを、前記パケットデータの各バイトに、各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換するモデルを用いて、異常パケットデータ１５を異常ベクトルデータ１６変換する変換部２１と、複数の正常パケットデータが前記モデルを用いて変換された複数の正常ベクトルデータから、異常ベクトルデータ１６の類似度が相対的に高い正常ベクトルデータ１７抽出する抽出部２３、異常ベクトルデータ１６の各バイトに対応するベクトルと、抽出された正常ベクトルデータ１７の各バイトに対応するベクトルとの類似度から、異常パケットデータ１５における異常バイトを推定する推定部２４を備える。

明　細　書

発明の名称 ： 推定装置、推定方法およびプログラム

技術分野

[0001] 本発明は、推定装置、推定方法およびプログラムに関する。

背景技術

[0002] 産業系・ビル系等におけるオペレーショナルテクノロジ（OT：Operational Technology）の通信ネットワークにおいて、異常検知システムまたは侵入検知システム（OT-IDS：Operational Technology Intrusion Detection System）が注目されている。このような通信ネットワークで送受信されるパケットは、１バイトなどの少量の不正な書き換えも見逃さずに検知される必要がある。例えば不正な書き換えにより温度の設定値が一桁変わってしまうなど、想定外のオペレーションが重大な事故を引き起こす場合がある。

[0003] ネットワークを監視するツールがある（非特許文献１および非特許文献２参照）。これらのツールでは、ネットワークで送受信されるデータを監視し、分析することができる。

先行技術文献

非特許文献

[0004] 非特許文献1：WIRESHARK、［online］、［2021年2月25日検索］、インターネット〈URL：https://www.wireshark.org/〉

非特許文献2：zeek、［online］、［2021年2月25日検索］、インターネット〈URL：https://zeek.org/〉

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、いずれの非特許文献も、異常パケットにおける異常バイトを特定することができない。

[0006] 本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、異常パケットにおける異常バイトを推定可能な技術を提供することである。

課題を解決するための手段

[0007] 本発明の一態様の推定装置は、パケットデータを、前記パケットデータの各バイトに、前記各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換するモデルを用いて、異常パケットデータを異常ベクトルデータに変換する変換部と、複数の正常パケットデータが前記モデルを用いて変換された複数の正常ベクトルデータから、前記異常ベクトルデータとの類似度が相対的に高い正常ベクトルデータを抽出する抽出部と、前記異常ベクトルデータの各バイトに対応するベクトルと、抽出された前記正常ベクトルデータの各バイトに対応するベクトルとの類似度から、前記異常パケットデータにおける異常バイトを推定する推定部を備える。

[0008] 本発明の一態様の推定方法は、コンピュータが、パケットデータを、前記パケットデータの各バイトに、前記各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換するモデルを用いて、異常パケットデータを異常ベクトルデータに変換し、前記コンピュータが、複数の正常パケットデータが前記モデルを用いて変換された複数の正常ベクトルデータから、前記異常ベクトルデータとの類似度が相対的に高い正常ベクトルデータを抽出し、前記コンピュータが、前記異常ベクトルデータの各バイトに対応するベクトルと、抽出された前記正常ベクトルデータの各バイトに対応するベクトルとの類似度から、前記異常パケットデータにおける異常バイトを推定する。

[0009] 本発明の一態様は、上記推定装置として、コンピュータを機能させるプログラムである。

発明の効果

[0010] 本発明によれば、異常パケットにおける異常バイトを推定可能な技術を提供することができる。

図面の簡単な説明

[0011] [図1]図１は、本発明の実施の形態に係る推定装置の機能ブロックを説明する図である。

[図2]図２は、モデルが変換するデータの一例を説明する図である。

[図3]図３は、推定方法の処理の一例を示すフローチャートである。

[図4]図４は、推定装置の評価システムの各装置を説明する図である。

[図5]図５は、評価システムで得られたパケットの一例を説明する図である。

[図6]図６は、評価システムで得られた類似度行列の一例を説明する図である。

[図7]図７は、推定装置に用いられるコンピュータのハードウエア構成を説明する図である。

発明を実施するための形態

[0012] 以下、図面を参照して、本発明の実施形態を説明する。図面の記載において同一部分には同一符号を付し説明を省略する。

[0013] （推定装置）

図１を参照して本発明の実施の形態に係る推定装置１を説明する。推定装置１は、異常パケットが入力されると、その異常パケット中の異常バイトを推定して出力する。推定装置１は、他システムで異常と判定された異常パケットと、その他システムで正常と判定された正常パケットと比較して、入力された異常パケットにおける異常バイトを推定する。例えば正常パケットおよび異常パケットは、それぞれ一つのオペレーションテクノロジの通信ネットワークで収集される。他システムは、任意の方法で、パケットの正常または異常を判定すればよく、本発明の実施の形態において、判定方法は問わない。

[0014] 推定装置１は、モデルデータ１１、正常ベクトルデータ群１２、異常パケットデータ１５、異常ベクトルデータ１６、正常ベクトルデータ１７および異常バイト１８の各データと、変換部２１、生成部２２、抽出部２３および推定部２４の各機能を備える。各データは、メモリ９０２またはストレージ９０３に記憶される。各機能は、CPU９０１に実装される。

[0015] モデルデータ１１は、パケットデータを、ベクトルデータに変換するモデルを特定する。ベクトルデータは、パケットデータの各バイトに、各バイト

の値の特徴を表す各ベクトルを対応づける。モデルデータ１１は、後述の生成部２２によって、正常ベクトルデータ群１２の複数の正常パケットデータの各バイトの値を学習して生成される。各バイトの値の特徴は、複数の正常パケットデータの各バイトの値と比較して算出される。

[0016] モデルデータ１１は、入力されたパケットデータの各バイトを、それぞれのバイトの位置関係等を考慮して、適切な固定長のベクトルに変換するモデルを特定する。ここで適切な固定長のベクトルは、後述の推定部２４において、異常ベクトルデータ１６と正常ベクトルデータ１７とを比較することによって異常バイト１８を推定可能なベクトルを意味する。例えば図２に示すように、第１のバイトの値“２ｅ”、第２のバイトの値“３ｆ”、第３のバイトの値“００”・・・と、固定長のパケットデータがあるとする。このパケットデータの各バイトは、モデルによって、７８４次元ベクトルに変換される。図２に示す例においてモデルは、パケットデータの各バイトを、各バイトの値の特徴を表す７８４次元ベクトルに変換する。

[0017] モデルデータ１１は、例えばＢＥＲＴ(Bidirectional Encoder Representations from Transformers)によって生成される。ＢＥＲＴは、自然言語処理モデルである。本発明の実施の形態において、パケットデータの各バイトが一つの単語とみなされる。ＢＥＲＴを用いて生成されたモデルによって、パケットデータは、ベクトルデータに変換される。

[0018] 正常ベクトルデータ群１２は、複数の正常ベクトルデータを含む。正常ベクトルデータは、モデルデータ１１によって特定されるモデルを用いて、他システムにおいて正常と判定された正常パケットデータが変換されたデータである。正常ベクトルデータ群１２は、生成部２２がモデルデータ１１を生成する際、または抽出部２３が異常ベクトルデータ１６に類似する正常ベクトルデータ１７を抽出する際に参照される。正常ベクトルデータ群１２に含まれる複数の正常ベクトルデータを、生成部２２および抽出部２３がともに参照しても良い。あるいは正常ベクトルデータ群１２に含まれる複数の正常ベクトルデータを複数のグループにわけて、１つのグループを生成部２２が

参照し、別のグループを抽出部２３が参照しても良い。

[0019] 異常パケットデータ１５は、他システムにおいて異常パケットと特定されたパケットのデータである。推定装置１は、１つの異常パケットデータ１５について異常バイト１８を推定する。

[0020] 異常ベクトルデータ１６は、異常パケットデータ１５をモデルデータ１１が特定するモデルで変換されたデータである。異常ベクトルデータ１６は、異常パケットデータ１５の各バイトの位置の識別子に、各バイトの値の特徴を表す各ベクトルを対応づける。

[0021] 正常ベクトルデータ１７は、正常ベクトルデータ群１２に含まれる複数の正常ベクトルデータのうち、異常ベクトルデータ１６と相対的に類似度が高いデータである。正常ベクトルデータ１７は、正常ベクトルデータ群１２に含まれる複数の正常ベクトルデータのうち、異常ベクトルデータ１６と最も類似度が高い正常ベクトルデータである。あるいは正常ベクトルデータ１７は、類似度が高い所定数の正常ベクトルデータのうちの一つである。

[0022] 異常バイト１８は、異常パケットデータ１５の各バイトのうち、異常が推定されるバイトを特定するデータである。異常バイト１８は、例えば、異常パケットデータ１５の各バイトの位置を先頭から数えた順番で特定される。

[0023] 変換部２１は、モデルデータ１１で特定されるモデルを用いて、異常パケットデータ１５を異常ベクトルデータ１６に変換する。例えば図２に示すように、変換部２１は、異常パケットデータ１５の各バイトの値を、７８４次元ベクトルに変換する。変換部２１は、異常パケットデータ１５の各バイトの位置と、そのバイトから変換された７８４次元ベクトルを対応づけて、異常ベクトルデータ１６を出力する。

[0024] 生成部２２は、正常ベクトルデータ群１２の複数の正常パケットデータの各バイトの値を学習して、モデルデータ１１が特定するモデルを生成する。モデルは、パケットデータを、パケットデータの各バイトに、各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換する。生成部２２は、例えば、ＢＥＲＴに従ってモデルを生成する。生成部２２は、正常パ

ケットデータにおける各バイトの値の特徴を、ＭＬＭ(Masked Language Model)またはＮＳＰ(Next Sentence Prediction)などの補助タスクを解いて予備学習しても良い。ＭＬＭは、複数のバイトが欠落しているパケットにおいて、これらの欠落しているバイトの値を予測する。ＮＳＰは、２つのパケットデータが連続したパケットであるか否かを判定する。生成部２２は、これらの補助タスクにより、パケット内のデータの妥当性および連続するパケットの妥当性を特定して、生成部２２は、正常ベクトルデータを特定するモデルを生成する。ここに挙げる補助タスクは一例であって、生成部２２は、その他の補助タスクを解いて学習しても良い。

[0025] 抽出部２３は、正常ベクトルデータ群１２の複数の正常ベクトルデータから、異常ベクトルデータ１６との類似度が相対的に高い正常ベクトルデータを抽出する。抽出部２３は、抽出した正常ベクトルデータを、正常ベクトルデータ１７とする。

[0026] 類似度が相対的に高いとは、異常ベクトルデータ１６とある正常ベクトルデータとの類似度が、異常ベクトルデータ１６と他の正常ベクトルデータとの類似度よりも高いことを言う。抽出部２３は、異常ベクトルデータ１６との類似度が最も高い正常ベクトルデータを抽出しても良い。あるいは抽出部２３は、異常ベクトルデータ１６との類似度が高い所定数または所定割合の複数の正常ベクトルデータから、一つの正常ベクトルデータを抽出しても良い。

[0027] 抽出部２３は、異常ベクトルデータ１６と、正常ベクトルデータ群１２の各正常ベクトルデータとの類似度を算出する。抽出部２３は、正常ベクトルデータ群１２のうちの一部の正常ベクトルデータとの類似度を算出しても良い。例えば一部の正常ベクトルデータは、複数の正常パケットデータから、MMD-Critic(MMD:Maximum Mean Discrepancy)で複数の代表パケットデータを抽出し、抽出した各代表パケットデータをモデルで変換して得られた複数の正常ベクトルデータである。あるいは一部の正常ベクトルデータは、複数の正常パケットデータから異常パケットデータ１５と同じパケット長の正常パケ

ットデータを抽出し、抽出した各正常パケットデータをモデルで変換して得られた複数の正常ベクトルデータである。

[0028] モデルがＢＥＲＴの場合、抽出部２３は、類似度として、ＢＥＲＴＳｃｏｒｅを用いても良い。あるいは、抽出部２３は、異常ベクトルデータ１６の各バイトについて、異常ベクトルデータ１６のベクトルと正常ベクトルデータのベクトルとの類似度を算出して、各バイトについて算出された類似度から、異常ベクトルデータ１６と正常ベクトルデータとの類似度を算出しても良い。各バイトのベクトル間の類似度は、Cosine類似度が用いられても良い。異常ベクトルデータ１６と正常ベクトルデータ１７の類似度は、例えば、各バイトについて算出された類似度の平均である。このとき、異常ベクトルデータ１６のベクトルの数と、正常ベクトルデータ１７のベクトルの数が異なる場合、少ないベクトルの数にあわせて、類似度が算出されても良い。なお各ベクトルデータのベクトルの数は、変換前のパケットデータのバイト数である。

[0029] 推定部２４は、異常ベクトルデータ１６の各バイトに対応するベクトルと、抽出された正常ベクトルデータ１７の各バイトに対応するベクトルとの類似度から、異常パケットデータ１５における異常バイト１８を推定する。

[0030] 抽出部２３は、異常ベクトルデータ１６に含まれる各ベクトルと正常ベクトルデータ１７に含まれる各ベクトルとの間で、図６に示すようなCosine類似度行列を計算する。Cosine類似度行列の(n,m)成分は、異常ベクトルデータ１６のnバイト目に対応するベクトルと、正常ベクトルデータ１７のmバイト目に対応するベクトル間のCosine類似度である。

[0031] 推定部２４は、例えば、異常パケットデータ１５の所定のバイトに対応するベクトルと、抽出された正常ベクトルデータ１７の各バイトに対応するベクトルとの類似度のうち、最も高い類似度が所定の閾値よりも低い場合、所定のバイトを異常バイト１８と推定する。異常パケットデータ１５のi番目のバイトが異常バイトであるかどうかを以下のように推定する。ｍを正常パケットデータのパケット長とする。推定部２４は、上記で算出したCosine類似

度行列の(i, 1)成分, (i, 2)成分, (i, 3)成分, … (i, m)成分の各成分に着目する。推定部２４は、各正文のうち最もCosine類似度が高い成分が、ある閾値以下であれば、i番目のバイトは異常バイト１８であると推定する。

[0032] 異常パケットデータ１５のバイト数と、正常ベクトルデータ１７の変換前のパケットデータのバイト数が同じ場合、異常パケットデータ１５と正常ベクトルデータ１７の同じバイトに対応する各ベクトルを比較しても良い。例えば異常パケットデータ１５のｉ番目バイトが異常バイトであるか否かを推定する際、異常パケットデータ１５のｉ番目のバイトに対応するベクトルデータと、正常パケットデータのｉ番目のバイトに対応するベクトルデータの類似度が、所定の閾値よりも低い場合、推定部２４は、異常パケットデータ１５のｉ番目のバイトを異常バイトと推定する。

[0033] 推定部２４が異常バイトであるか否かを判定するための閾値は、例えば、０．５等の固定値でも良い。あるいは閾値は、所定の計算により特定されても良い。例えば、互いに類似する２つの正常パケットのペアを複数抽出し、所定のバイトに対応する２つの正常パケットの各ベクトルの類似度のうち、最も低い類似度から、閾値が特定されても良い。

[0034] 図３を参照して、本発明の実施の形態に係る推定装置１による推定方法を説明する。

[0035] ステップＳ１において推定装置１は、異常パケットデータ１５を異常ベクトルデータ１６に変換する。ステップＳ２において推定装置１は、正常ベクトルデータ群１２から、ステップＳ１で変換した異常ベクトルデータ１６に類似する正常ベクトルデータ１７を抽出する。

[0036] 異常ベクトルデータ１６の各ベクトル、換言すると、異常パケットデータ１５の各バイトに対応する各ベクトルについて、ステップＳ３ないしステップＳ５の処理を繰り返す。

[0037] ステップＳ２で抽出した正常ベクトルデータ１７の各ベクトルについて、ステップＳ３の処理を繰り返す。ステップＳ３において推定装置１は、異常ベクトルデータ１６の処理対象のベクトルと、正常ベクトルデータ１７の処

理対象のベクトルとの類似度を算出する。類似度が算出されると、処理はステップＳ４に進む。

[0038] ステップＳ４において推定装置１は、異常ベクトルデータ１６の処理対象のベクトルと正常ベクトルデータ１７の各ベクトルについて算出された複数の類似度のうち、最も高い類似度が、所定の閾値より低いか否かを判定する。最も高い類似度が所定の閾値より高い場合、推定装置１は、異常ベクトルデータ１６の処理対象のベクトルは、異常バイトに対応しないと推定する。推定装置１は、次の処理対象のベクトルについてステップＳ３を処理する。

[0039] 最も高い類似度が所定の閾値より低い場合、推定装置１は、異常ベクトルデータ１６の処理対象のベクトルは、異常バイトに対応すると推定する。推定装置１は、ステップＳ６において、異常ベクトルデータ１６の処理対象のベクトルに対応するバイトを、異常バイト１８として出力する。

[0040] 異常ベクトルデータ１６の各ベクトルについてステップＳ３ないしステップＳ５の処理が終了すると、推定装置１は処理を終了する。

[0041] 図４ないし図６を参照して、推定装置１の評価を説明する。推定装置１の評価において、仮想の評価システムを用いる。

[0042] 評価システムは、図４に示すように４つのベルトコンベアＣ１－Ｃ４を矩形に配置し、ＰＬＣ（Programmable Logic Controller）（図示せず）を用いて、荷物Ｂ１およびＢ２の移動を制御する。図４に示す各装置は、Modbus/TCPプロトコル等に従って、ＰＬＣに状態を通知するパケットを送信したり、ＰＬＣから駆動内容を指定するパケットを受信したりする。正常状態においてＰＬＣは、センサＳ１－Ｓ４の検出状況に従ってプッシャーＰ１－Ｐ４を駆動することにより、ベルトコンベアＣ１－Ｃ４は、一定速度で反時計回りに荷物Ｂ１およびＢ２を運ぶ。ベルトコンベアの速度は、ＰＬＣによって逐次監視される。ベルトコンベアの速度が一定速度を超過すると、ＰＬＣにより、図４に示す各装置に対して緊急停止命令が発せられ、各装置は停止する。

[0043] 例えば荷物Ｂ１は、ベルトコンベアＣ１上を移動する。このときベルトコンベアＣ１は、ベルトの移動速度を通知するパケットをＰＬＣに送信する。

荷物Ｂ１が、センサＳ１が出射するレーザー光に当接すると、センサＳ１は、荷物が到達したことを知らせるパケットをＰＬＣに送信する。なお図４に示す例において、レーザー光は一点鎖線で示す。ＰＬＣは、パケットを受信すると、プッシャーＰ１をＯＮにするパケットを送信する。プッシャーＰ１は、受信したパケットに従って、ボックスから延伸して、荷物Ｂ１をベルトコンベアＣ２まで運ぶ。センサＳ１が出射するレーザー光に荷物が当接しなくなると、センサＳ１は、荷物がないことを知らせるパケットをＰＬＣに送信する。ＰＬＣは、パケットを受信すると、プッシャーＰ１をＯＦＦにするパケットを送信する。プッシャーＰ１は、受信したパケットに従って、短縮してボックスに収容される。このような処理を各装置が繰り返すことにより、荷物Ｂ１は、図４に示すベルトコンベア上を反時計回りに移動する。荷物Ｂ２についても同様に、図４に示すベルトコンベア上を反時計回りに移動する。

[0044] ＰＬＣは、図４に示す各装置が正常に稼働している際に正常パケットデータを収集する。生成部２２は、ＰＬＣによって収集された複数の正常パケットデータを学習して、モデルデータ１１を生成する。評価システムにおいて、抽出部２３は、ＰＬＣが収集した各正常パケットデータから変換された複数の正常ベクトルデータを参照する。また類似度の尺度として、ＢＥＲＴＳｃｏｒｅＦ１を用いる。

[0045] 速度が異常値になるように手動でベルトコンベアを早く動かすことで、異常状態を発生させる。ＰＬＣに、異常パケットデータ１５として、この異常状態におけるベルトコンベアの速度を通知するパケットが入力される。

[0046] 抽出部２３は、異常パケットデータ１５から変換された異常ベクトルデータ１６に最も類似する正常ベクトルデータを抽出する。図５は、異常パケットデータ１５と、抽出部２３が抽出した正常ベクトルデータの変換前の正常パケットデータを比較して示す。

[0047] 図５において１バイト目および２バイト目は、交信ＩＤが設定される。交信ＩＤは、図４に示すシステムにおいて送受信されるパケットを特定する識

別子である。１１バイト目は、ベルトコンベアの速度が設定される。図５に示す例において、１バイト目、２バイト目および１１バイト目において、異常パケットと正常パケットの値は相違するが、それ以外のバイトの値は一致する。抽出部２３は、異常ベクトルデータ１６に最も類似する正常ベクトルデータを抽出したことがわかる。

[0048] 図６は、異常パケットと正常パケットの各バイトのベクトル間の類似度行列である。図６から高い類似度は、対角線上に配置されていることがわかる。但し対角線上のうち、１バイト目同士、２バイト目同士および１１バイト目同士を比較した類似度は、低い値を有する。異常パケットの１バイト目、２バイト目、または１１バイト目が異常バイトの可能性があると考えられる。

[0049] 一方、互いに類似する２つの正常パケットから変換された２つの正常ベクトルデータを比較した結果、同じバイトに対応するベクトルを比較した類似度のうち最も低い類似度が０．９１であった。この０．９１を、異常バイトを検出する際の閾値とする。

[0050] １バイト目および２バイト目の各類似度は、０．９１より大きいので、推定部２４は、１バイト目および２バイト目について異常バイトでないと推定する。１バイト目および２バイト目は、各パケットよって異なる交信ＩＤが設定されることから、正常パケットと異常パケットとで異なる値が設定されても、閾値よりも高い類似度が算出される。

[0051] 一方１１バイト目の類似度は０．８２７で、０．９１より小さいので、推定部２４は、１１バイト目を異常バイトと推定する。１１バイト目は、ベルトコンベアの速度が設定される。推定部２４によるこの推定は、手動でベルトコンベアを早く動かすことで異常状態を発生させた状況とも合致する。

[0052] このような本発明の実施の形態に係る推定装置１は、異常パケットデータ１５における異常バイト１８を推定することができる。これにより推定装置１は、ペイロードの内容の精緻な分析が可能になる。例えば産業系・ビル系等におけるオペレーショナルテクノロジの通信ネットワークなどに推定装置

１を導入することにより、１バイトなどの少量の不正な書き換えも見逃さずに検知することが可能になる。

[0053] 上記説明した本実施形態の推定装置１は、例えば、CPU（Central Processing Unit、プロセッサ）９０１と、メモリ９０２と、ストレージ９０３（HDD：Hard Disk Drive、SSD：Solid State Drive）と、通信装置９０４と、入力装置９０５と、出力装置９０６とを備える汎用的なコンピュータシステムが用いられる。このコンピュータシステムにおいて、CPU９０１がメモリ９０２上にロードされたプログラムを実行することにより、推定装置１の各機能が実現される。

[0054] なお、推定装置１は、１つのコンピュータで実装されてもよく、あるいは複数のコンピュータで実装されても良い。また推定装置１は、コンピュータに実装される仮想マシンであっても良い。

[0055] 推定装置１のプログラムは、HDD、SSD、USB（Universal Serial Bus）メモリ、CD（Compact Disc）、DVD（Digital Versatile Disc)などのコンピュータ読取り可能な記録媒体に記憶することも、ネットワークを介して配信することもできる。

[0056] なお、本発明は上記実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

符号の説明

[0057] １　推定装置

１１　モデルデータ

１２　正常ベクトルデータ群

１５　異常パケットデータ

１６　異常ベクトルデータ

１７　正常ベクトルデータ

１８　異常バイト

２１　変換部

２２　生成部

２３　抽出部

２４　推定部

９０１　CPU

９０２　メモリ

９０３　ストレージ

９０４　通信装置

９０５　入力装置

９０６　出力装置

請求の範囲

[請求項1] パケットデータを、前記パケットデータの各バイトに、前記各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換するモデルを用いて、異常パケットデータを異常ベクトルデータに変換する変換部と、

複数の正常パケットデータが前記モデルを用いて変換された複数の正常ベクトルデータから、前記異常ベクトルデータとの類似度が相対的に高い正常ベクトルデータを抽出する抽出部と、

前記異常ベクトルデータの各バイトに対応するベクトルと、抽出された前記正常ベクトルデータの各バイトに対応するベクトルとの類似度から、前記異常パケットデータにおける異常バイトを推定する推定部

を備える推定装置。

[請求項2] 前記モデルは、複数の正常パケットデータの各バイトの値を学習して生成される

請求項１に記載の推定装置。

[請求項3] 前記抽出部は、前記異常ベクトルデータの各バイトについて、前記異常ベクトルデータのベクトルと前記正常ベクトルデータのベクトルとの類似度を算出して、前記各バイトについて算出された類似度から、前記異常ベクトルデータと前記正常ベクトルデータとの類似度を算出する

請求項１に記載の推定装置。

[請求項4] 前記推定部は、前記異常パケットデータの所定のバイトに対応するベクトルと、前記抽出された正常ベクトルデータの各バイトに対応するベクトルとの類似度のうち、最も高い類似度が所定の閾値よりも低い場合、前記所定のバイトを前記異常バイトと推定する

請求項１に記載の推定装置。

[請求項5] コンピュータが、パケットデータを、前記パケットデータの各バイ

トに、前記各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換するモデルを用いて、異常パケットデータを異常ベクトルデータに変換し、

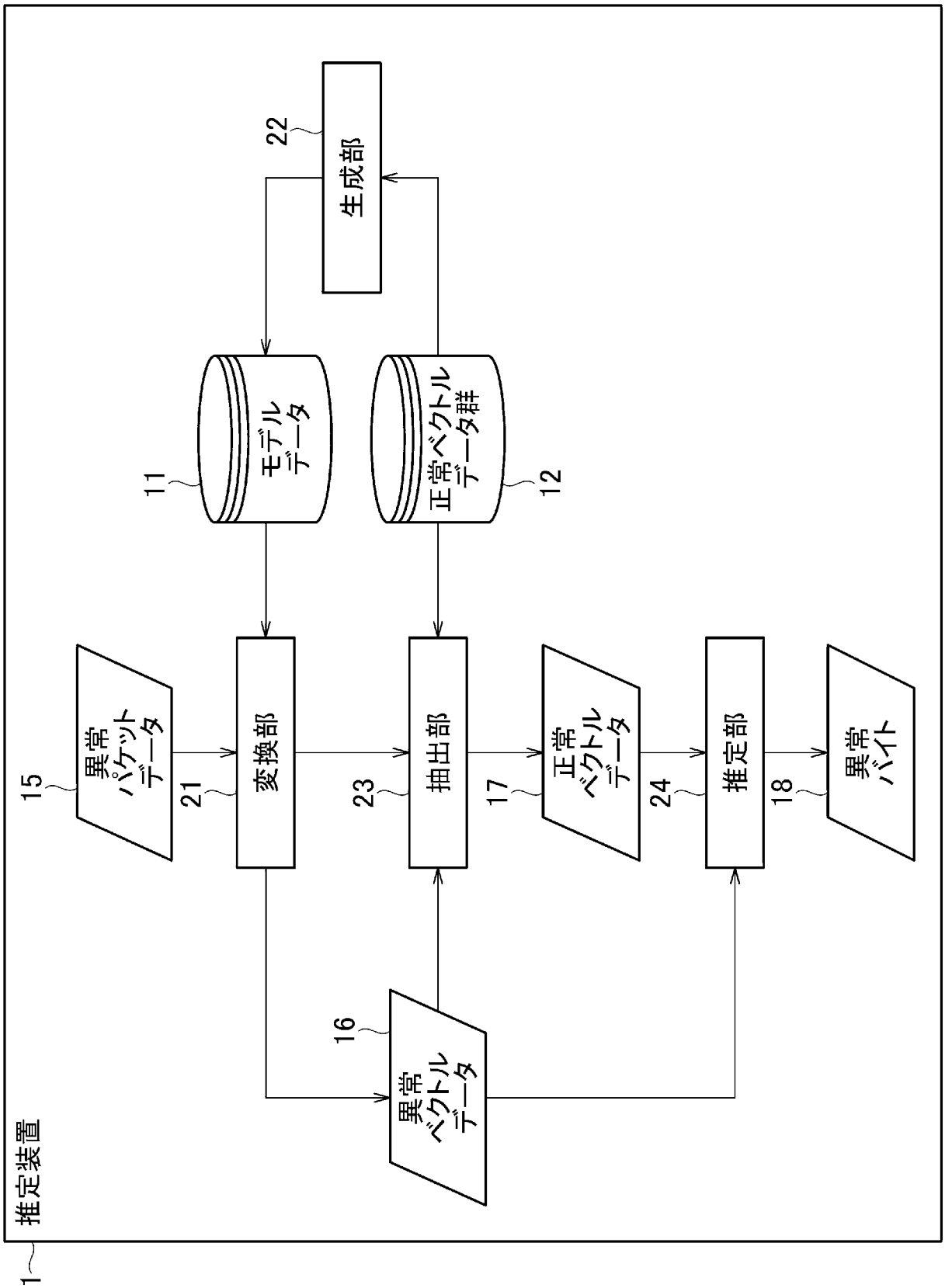
前記コンピュータが、複数の正常パケットデータが前記モデルを用いて変換された複数の正常ベクトルデータから、前記異常ベクトルデータとの類似度が相対的に高い正常ベクトルデータを抽出し、

前記コンピュータが、前記異常ベクトルデータの各バイトに対応するベクトルと、抽出された前記正常ベクトルデータの各バイトに対応するベクトルとの類似度から、前記異常パケットデータにおける異常バイトを推定する

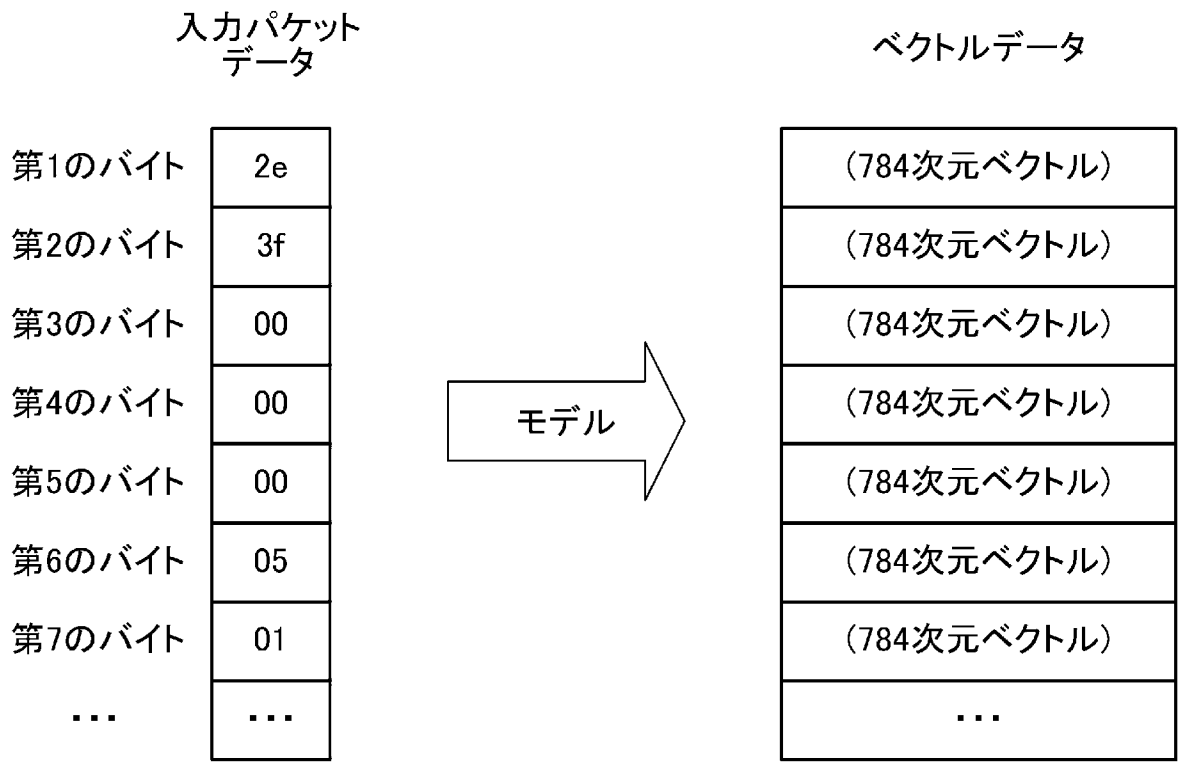
推定方法。

[請求項6] コンピュータを、請求項１ないし請求項４のいずれか１項に記載の推定装置として機能させるためのプログラム。

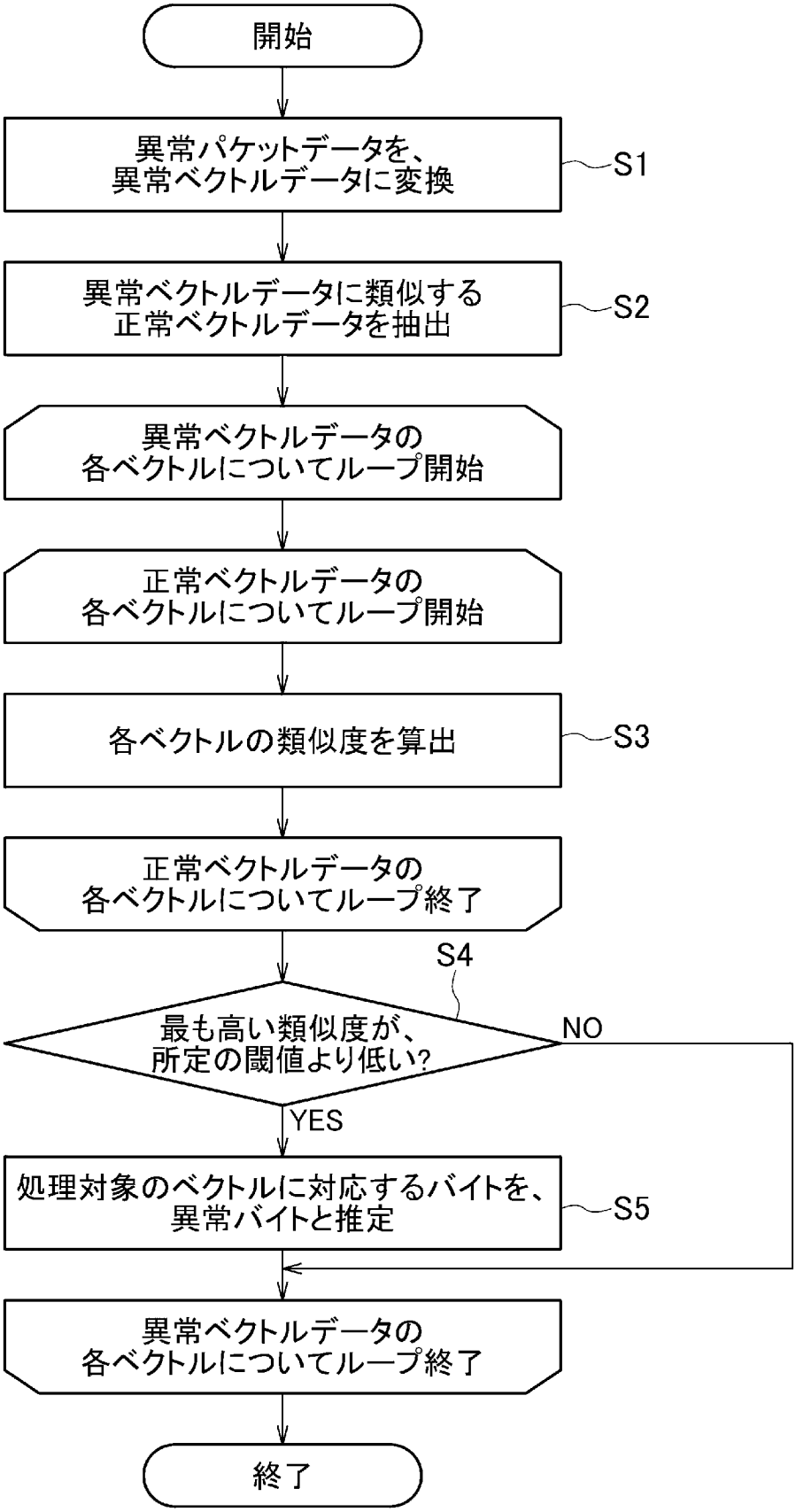
[図1]


推定装置
1
生成部
22
モデルデータ
11
正常ベクトルデータ群
12
異常パケットデータ
15
変換部
21
抽出部
23
正常ベクトルデータ
17
推定部
24
異常バイト
18
異常ベクトルデータ
16

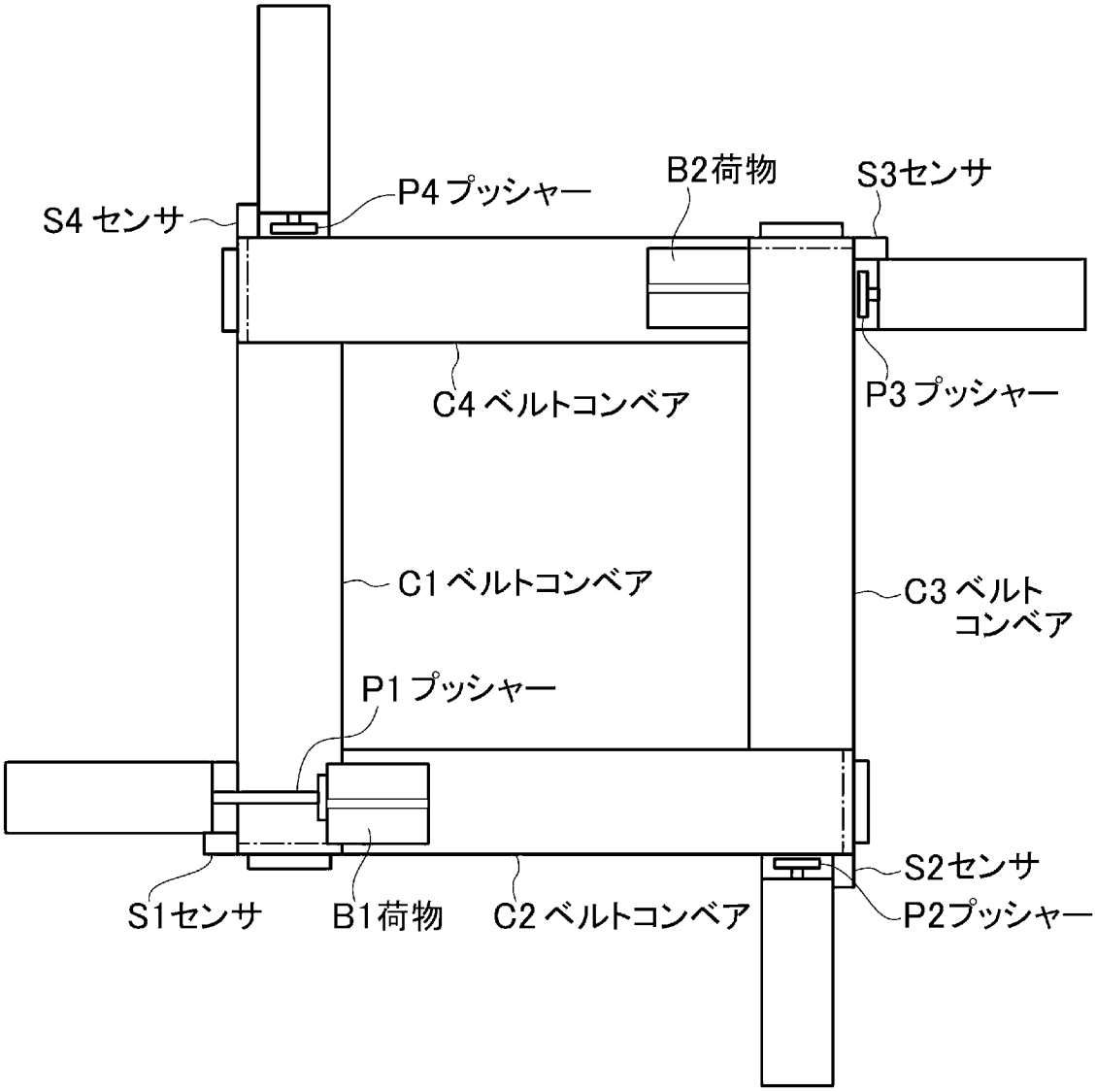
[図2]


入力パケット
データ
第1のバイト
2e
第2のバイト
3f
第3のバイト
00
第4のバイト
00
第5のバイト
00
第6のバイト
05
第7のバイト
01
・・・
・・・
モデル
ベクトルデータ
(784次元ベクトル)
(784次元ベクトル)
(784次元ベクトル)
(784次元ベクトル)
(784次元ベクトル)
(784次元ベクトル)
(784次元ベクトル)
・・・

[図3]


開始
異常パケットデータを、
異常ベクトルデータに変換
S1
異常ベクトルデータに類似する
正常ベクトルデータを抽出
S2
異常ベクトルデータの
各ベクトルについてループ開始
正常ベクトルデータの
各ベクトルについてループ開始
各ベクトルの類似度を算出
S3
正常ベクトルデータの
各ベクトルについてループ終了
S4
最も高い類似度が、
所定の閾値より低い?
NO
YES
処理対象のベクトルに対応するバイトを、
異常バイトと推定
S5
異常ベクトルデータの
各ベクトルについてループ終了
終了

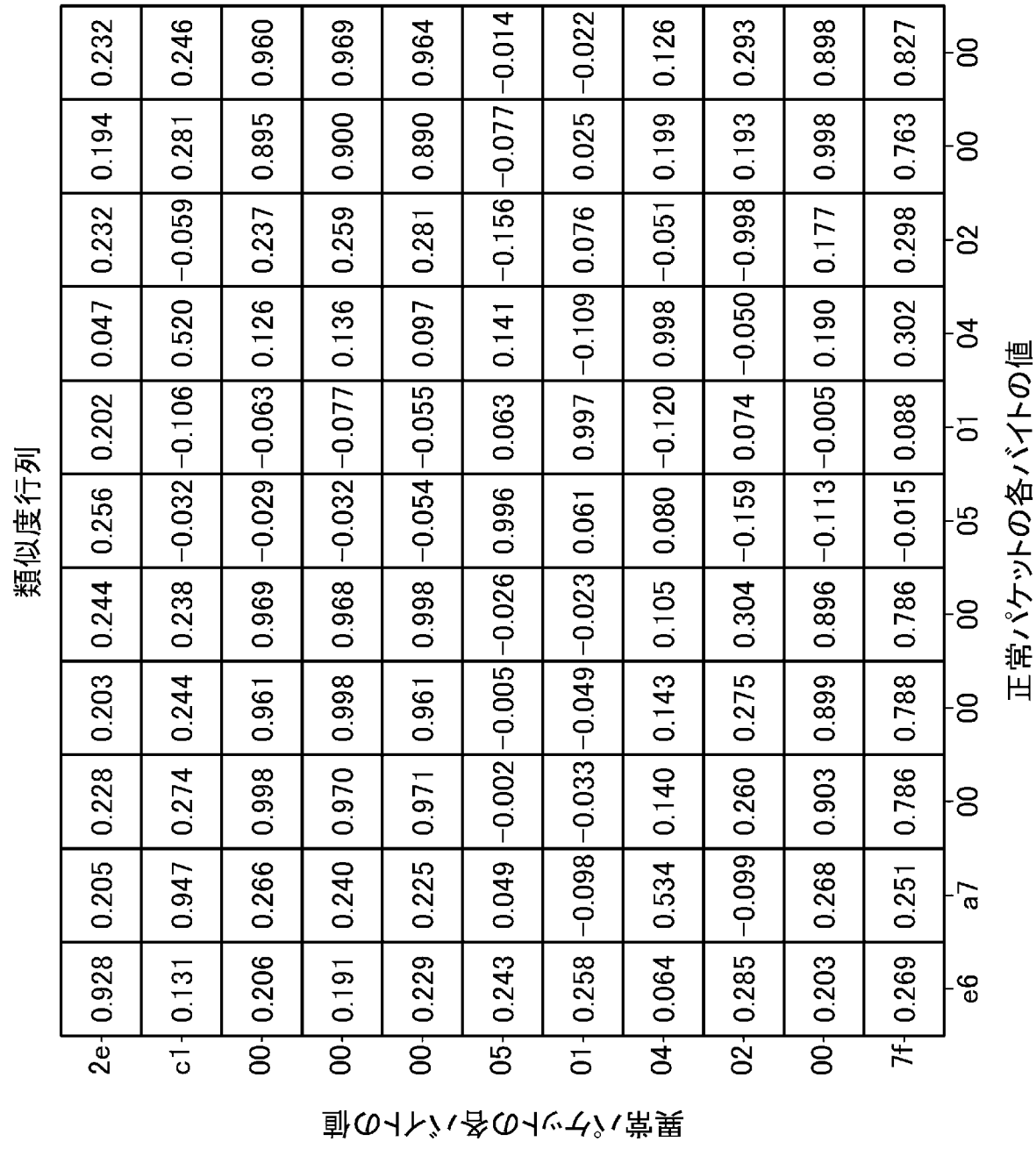
[図4]


S4 センサ
P4 プッシャー
B2荷物
S3センサ
C4 ベルトコンベア
P3 プッシャー
C1 ベルトコンベア
C3 ベルト
コンベア
P1 プッシャー
S2センサ
P2プッシャー
S1センサ
B1荷物
C2 ベルトコンベア

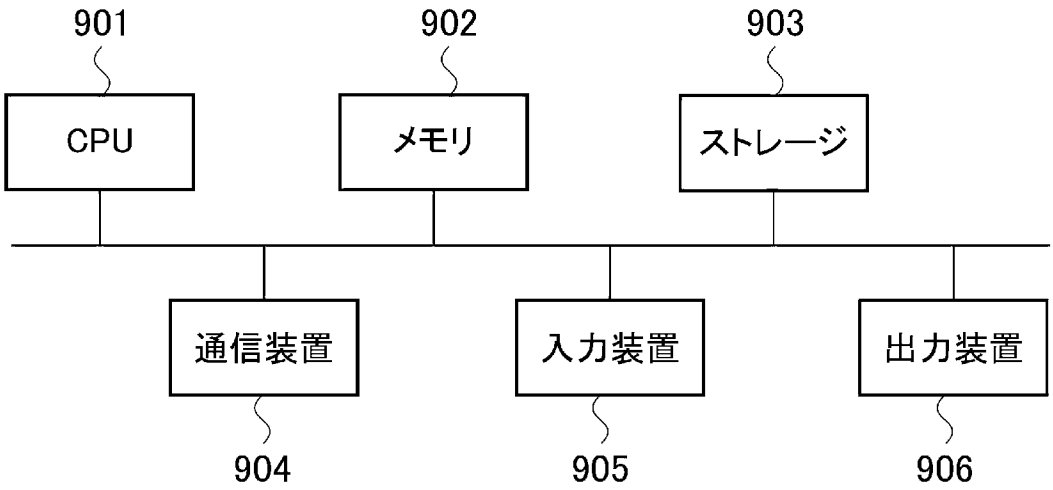
[図5]

バイト	1	2	3	4	5	6	7	8	9	10	11
異常パケット	2e	3f	00	00	00	06	01	04	02	00	7f
正常パケット	e6	a7	00	00	00	06	01	04	02	00	00

[図6]


類似度行列
異常パケットの各バイトの値
正常パケットの各バイトの値
2e
c1
00
00
00
05
01
04
02
00
7f
e6
a7
00
00
00
05
01
04
02
00
00
0.928 0.205 0.228 0.203 0.244 0.256 0.202 0.047 0.232 0.194 0.232
0.131 0.947 0.274 0.244 0.238 −0.032 −0.106 0.520 −0.059 0.281 0.246
0.206 0.266 0.998 0.961 0.969 −0.029 −0.063 0.126 0.237 0.895 0.960
0.191 0.240 0.970 0.998 0.968 −0.032 −0.077 0.136 0.259 0.900 0.969
0.229 0.225 0.971 0.961 0.998 −0.054 −0.055 0.097 0.281 0.890 0.964
0.243 0.049 −0.002 −0.005 −0.026 0.996 0.063 0.141 −0.156 −0.077 −0.014
0.258 −0.098 −0.033 −0.049 −0.023 0.061 0.997 −0.109 0.076 0.025 −0.022
0.064 0.534 0.140 0.143 0.105 0.080 −0.120 0.998 −0.051 0.199 0.126
0.285 −0.099 0.260 0.275 0.304 −0.159 0.074 −0.050 −0.998 0.193 0.293
0.203 0.268 0.903 0.899 0.896 −0.113 −0.005 0.190 0.177 0.998 0.898
0.269 0.251 0.786 0.788 0.786 −0.015 0.088 0.302 0.298 0.763 0.827

[図7]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/009228

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. H04L12/70(2013.01)i
FI: H04L12/70 Z

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. 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.
A	JP 2019-110513 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 04 July 2019 (2019-07-04), paragraphs [0032], [0089]-[0117]	1-6
A	JP 2019-4419 A (HITACHI, LTD.) 10 January 2019 (2019-01-10), claims 1-2, paragraphs [0019]-[0025], [0044]-[0047]	1-6
A	JP 2007-74339 A (TOHOKU UNIVERSITY) 22 March 2007 (2007-03-22), paragraphs [0028]-[0045]	1-6
A	JP 2019-33312 A (HITACHI, LTD.) 28 February 2019 (2019-02-28), claims 1-3, paragraphs [0003], [0030], [0051]-[0056]	1-6

☐ 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
27.05.2021	08.06.2021
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/JP2021/009228

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
JP 2019-110513 A	04.07.2019	US 2019/0190938 A1 paragraphs [0047], [0110]-[0140]	
JP 2019-4419 A	10.01.2019	(Family: none)	
JP 2007-74339 A	22.03.2007	(Family: none)	
JP 2019-33312 A	28.02.2019	US 2019/0044913 A1 claims 1-3, paragraphs [0004], [0048], [0069]-[0074]	

国際調査報告

国際出願番号
PCT/JP2021/009228

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 Z

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
A	JP 2019-110513 A (パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ) 04.07.2019 (2019-07-04) [0032],[0089]-[0117]	1-6
A	JP 2019-4419 A (株式会社日立製作所) 10.01.2019 (2019-01-10) 請求項1-2, [0019]-[0025],[0044]-[0047]	1-6
A	JP 2007-74339 A (国立大学法人東北大学) 22.03.2007 (2007-03-22) [0028]-[0045]	1-6
A	JP 2019-33312 A (株式会社日立製作所) 28.02.2019 (2019-02-28) 請求項1-3,[0003],[0030],[0051]-[0056]	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
27.05.2021	08.06.2021

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）
羽岡　さやか 5X 3149
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/JP2021/009228

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-110513 A	04.07.2019	US 2019/0190938 A1 [0047],[0110]-[0140]	
JP 2019-4419 A	10.01.2019	（ファミリーなし）	
JP 2007-74339 A	22.03.2007	（ファミリーなし）	
JP 2019-33312 A	28.02.2019	US 2019/0044913 A1 claims1-3, [0004],[0048], [0069]-[0074]	