(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
2020年12月17日(17.12.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/250312 A1

(51) 国際特許分類:
G06N 20/00 (2019.01)

(21) 国際出願番号： PCT/JP2019/023151

(22) 国際出願日： 2019年6月11日(11.06.2019)

(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: 大川 真耶(**OKAWA, Maya**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 戸田 浩之(**TODA, Hiroyuki**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

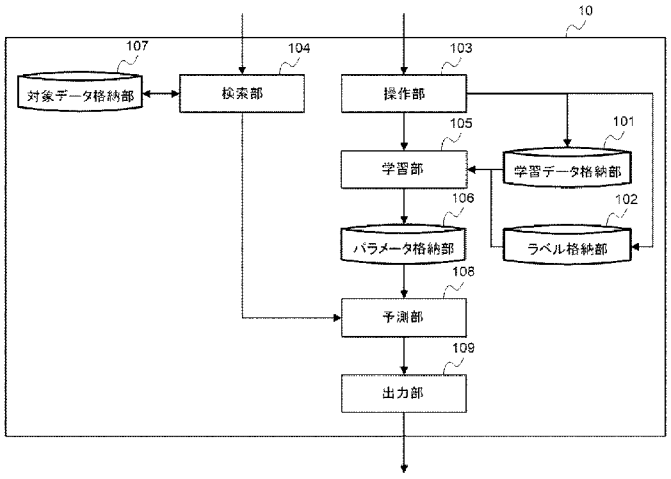
(74) 代理人: 特許業務法人太陽国際特許事務所 (**TAIYO, NAKAJIMA & KATO**); 〒1600022 東京都新宿区新宿４丁目３番１７号 Tokyo (JP).

(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, 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,

WO 2020/250312 A1

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

(54) 発明の名称： 異常検知装置、異常検知方法、及び異常検知プログラム



101 Learning data storage unit
102 Label storage unit
103 Operation unit
104 Search unit
105 Learning unit
106 Parameter storage unit
107 Object data storage unit
108 Prediction unit
109 Output unit

(57) **Abstract:** The present invention enables an anomaly of event data to be detected with good accuracy. A learning unit (105) learns a parameter of a model that outputs the level of anomaly of an object event series that is the object for which the level of anomaly is predicted when the object event series is inputted so as to optimize, on the basis of a plurality of event series that are event data in time series and a label that indicates anomaly or normal with respect to each event data in each of the plurality of event series, an objective function that represents a relationship between the occurrence probability

[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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))

of an event at each time of day in the time series and the level of anomaly of each of the plurality of event series.

(57) 要約:精度よくイベントデータの異常検知をすることができるようにする。学習部(１０５)は、時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する。

明　細　書

発明の名称 ：

異常検知装置、異常検知方法、及び異常検知プログラム

技術分野

[0001] 本開示は、異常検知装置、異常検知方法、及び異常検知プログラムに関する。

背景技術

[0002] 従来から、イベントデータの異常度を判定する異常検知は、多くのドメインで必要不可欠な技術である。例えば、金融取引の系列データの異常が検知できれば、不正取引を自動で特定することができる。タクシーの乗降履歴の系列の異常が検知できれば、混雑が起きている場所を特定し迅速に事前措置を取ることができる。イベントデータは、ある事象の発生時刻・発生場所の系列からなるデータで、一般的に点過程を用いてモデル化される（非特許文献１）。

[0003] イベントデータの異常を検知するモデルは過去にいくつか提案されているが、異常であることを示す正解データが与えられていない場合を想定しているものが多い。一方、異常又は正常を示す正解ラベルが事前に与えられている場合については、例えば、離散化された特徴量に基づいて教師ありで交通需要の異常予測を行う技術が提案されている（非特許文献２）。

先行技術文献

非特許文献

[0004] 非特許文献1：Ihler, Alexander, Jon Hutchins, and Padhraic Smyth. "Adaptive event detection with time-varying poisson processes". Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2006.

非特許文献2：A. Vahedian, X. Zhou, L. Tong, W. N. Street, and Y. Li., "Predicting urban dispersal events: A two-stage framework through de

ep survival analysis on mobility data", AAAI Conference on Artificial Intelligence, IEEE, 2018.

発明の概要

発明が解決しようとする課題

[0005] イベントデータの異常検知は、様々なドメインで大きな価値を持つ。しかし、既存の教師あり異常検知手法では、イベントデータを考慮することができない。例えば、非特許文献２の手法は、集計された特徴量を扱うものであるため、イベントデータに対して適用することができない。このため、精度よくイベントデータの異常検知をすることができない、という問題があった。

[0006] 開示の技術は、上記の点に鑑みてなされたものであり、精度よくイベントデータの異常検知をすることができる異常検知装置、異常検知方法、及び異常検知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

[0007] 本開示の第１態様は、異常検知装置であって、時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する学習部を含む。

[0008] 本開示の第２態様は、異常検知方法であって、学習部が、時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する。

[0009] 本開示の第３態様は、異常検知プログラムであって、学習部が、時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習することをコンピュータに実行させるための異常検知プログラムである。

発明の効果

[0010] 開示の技術によれば、精度よくイベントデータの異常検知をすることができる。

図面の簡単な説明

[0011] [図1]実施形態に係る異常検知装置として機能するコンピュータの概略構成を示すブロック図である。

[図2]実施形態に係る異常検知装置の機能構成の例を示すブロック図である。

[図3]検索履歴の一例を示す図である。

[図4]異常ラベルの一例を示す図である。

[図5]実施形態に係る異常検知装置の異常検知処理ルーチンを示すフローチャートである。

発明を実施するための形態

[0012] 以下、開示の技術の実施形態の例を、図面を参照しつつ説明する。なお、各図面において同一又は等価な構成要素及び部分には同一の参照符号を付与している。また、図面の寸法比率は、説明の都合上誇張されており、実際の比率とは異なる場合がある。

[0013] ＜本開示の技術の実施形態に係る異常検知装置の構成＞

図１は、本実施形態に係る異常検知装置１０のハードウェア構成を示すブロック図である。図１に示すように、異常検知装置１０は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１、ＲＯＭ（Ｒｅａｄ　Ｏ

ｎｌｙ　Ｍｅｍｏｒｙ）１２、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１３、ストレージ１４、入力部１５、表示部１６及び通信インタフェース（Ｉ／Ｆ）１７を有する。各構成は、バス１９を介して相互に通信可能に接続されている。

[0014] ＣＰＵ１１は、中央演算処理ユニットであり、各種プログラムを実行したり、各部を制御したりする。すなわち、ＣＰＵ１１は、ＲＯＭ１２又はストレージ１４からプログラムを読み出し、ＲＡＭ１３を作業領域としてプログラムを実行する。ＣＰＵ１１は、ＲＯＭ１２又はストレージ１４に記憶されているプログラムに従って、上記各構成の制御及び各種の演算処理を行う。本実施形態では、ＲＯＭ１２又はストレージ１４には、異常検知処理を実行するための異常検知プログラムが記憶されている。

[0015] ＲＯＭ１２は、各種プログラム及び各種データを記憶する。ＲＡＭ１３は、作業領域として一時的にプログラム又はデータを記憶する。ストレージ１４は、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）又はＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）により構成され、オペレーティングシステムを含む各種プログラム、及び各種データを記憶する。

[0016] 入力部１５は、マウス等のポインティングデバイス、及びキーボードを含み、各種の入力を行うために使用される。

[0017] 表示部１６は、例えば、液晶ディスプレイであり、各種の情報を表示する。表示部１６は、タッチパネル方式を採用して、入力部１５として機能しても良い。

[0018] 通信インタフェース１７は、他の機器と通信するためのインタフェースであり、例えば、イーサネット（登録商標）、ＦＤＤＩ、Ｗｉ－Ｆｉ（登録商標）等の規格が用いられる。

[0019] 次に、異常検知装置１０の機能構成について説明する。図２は、異常検知装置１０の機能構成の例を示すブロック図である。

[0020] 図２に示すように、異常検知装置１０は、機能構成として、学習データ格納部１０１と、ラベル格納部１０２と、操作部１０３と、検索部１０４と、

学習部１０５と、パラメータ格納部１０６と、対象データ格納部１０７と、予測部１０８と、出力部１０９と、を有する。各機能構成は、ＣＰＵ１１がＲＯＭ１２又はストレージ１４に記憶された異常検知プログラムを読み出し、ＲＡＭ１３に展開して実行することにより実現される。

[0021] 学習データ格納部１０１には、時系列のイベントデータであるイベント系列が複数格納されている。具体的には、学習データ格納部１０１は、学習部１０５からの要求に従って、イベント系列を読み出し、読み出したイベント系列を学習部１０５に渡す。イベントデータはある事象（イベント）の発生時刻及び発生場所の系列からなるデータであり、例えば金融市場における取引の記録、タクシーの乗降履歴、Ｅ－ｃｏｍｍｅｒｃｅサイトにおける購買履歴、犯罪の履歴等である。より具体的には、イベントデータは、例えば、ルート検索アプリの検索ログであり、あるエリア（駅等）l_i、ある日にちd_i、ある時間h_i、を対象とする検索が行われた時刻χ_jにおけるイベント系列$x=\{\chi_1, \chi_2, ...\}$で定義される。なお、“イベント系列ｘ”の“ｘ”は、数式中は太字のｘで表す。本開示では、時刻Ｔまでに観測されたｎ個のイベント系列ｘからなるデータセット$X=\{x_i\}_{i=1}^{n}$が与えられた場合を考える。各イベント系列x_iの長さをn_iとおく。

[0022] 図３に、イベントデータの例として、検索ログ（履歴）をイベントデータとした場合を示す。図３に示すように、検索対象のエリア、検索対象の日にち、検索対象の時間に紐づいて、検索ログが、学習データ格納部１０１に格納されている。図３中の検索ログは、例えば、検索対象のエリアl_iを“Ａ駅”、検索対象の日にちd_iを“２０１８／１／２”、検索対象の時間h_iを“１０：００”を対象とする検索が行われた時刻χ_j（１，３，１２等）が時系列に格納されている。

[0023] ラベル格納部１０２には、複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルが格納されている。具体的には、ラベル格納部１０２は、学習部１０５からの要求に従って、異常又は正常を示すラベルを読み出し、読み出したラベルを学習部１０５に渡す。異常又は正常

を示すラベルは、例えば金融取引であれば「不正取引が行われていたかどうか」、「株価の乱高下が発生していたかどうか」、タクシーの乗降履歴なら「乗降時に混雑が起きていたかどうか」等、手動又は自動で取得されたものである。本開示では、ｎ個のイベント系列ｘからなるデータセットＸと共に、エリアｌ$_i$、日にちｄ$_i$、時間帯ｈ$_i$の各々に対応するラベルＹ＝｛ｙ$_i$｝$^{n}_{i=1}$が与えられているものとする。ここでｙ$_i$は、例えばエリアｌ$_i$、日にちｄ$_i$、時間帯ｈ$_i$において混雑が起きているか否かを表す二値データｙ$_i$∈［０，１］である。

[0024] 図４に、イベントデータが上記の検索ログである場合の、ラベルの例を示す。図４中の異常の項目が、ラベルである。図４の例において、ラベルは、異常である（混雑が発生した）場合、１（混雑あり）となり、正常である（混雑が発生していない）場合、０（混雑なし）となる。

[0025] なお、学習データ格納部１０１及びラベル格納部１０２は、Ｗｅｂサーバや、データベースを具備するデータベースサーバ等として構成することもできる。

[0026] 操作部１０３は、学習データ格納部１０１及びラベル格納部１０２に格納されているデータに対する各種操作を受け付ける。各種操作とは、データを登録、修正、削除する操作等である。

[0027] 検索部１０４は、対象イベント系列ｘ′$_i$の入力を受け付ける。具体的には、検索部１０４は、まず、異常度の予測の対象となるイベント系列についての、時刻及び場所の情報を受け付ける。次に、検索部１０４は、受け付けた時刻及び場所に紐づく各イベントデータを、対象データ格納部１０７から取得し、対象イベント系列ｘ′$_i$とする。そして、検索部１０４は、対象イベント系列ｘ′$_i$を、予測部１０８に渡す。

[0028] 学習部１０５は、複数のイベント系列ｘと、複数のイベント系列ｘの各々の各イベントデータについての異常又は正常を示すラベルｙとに基づいて、時系列の各時刻におけるイベントの発生確率と複数のイベント系列ｘの各々の異常度との関係を表す目的関数Ｌを最適化するように、異常度を予測する

対象となるイベント系列である対象イベント系列ｘ′を入力した場合に、対象イベント系列ｘ′の異常度ｓ′を出力するモデルのパラメータを学習する。

[0029] 具体的には、学習部１０５は、まず、学習データ格納部１０１からデータセットＸを、ラベル格納部１０２からラベルＹを取得する。次に、学習部１０５は、取得したデータセットＸ及びラベルＹに基づいて、イベント系列ｘと当該イベント系列ｘの異常度ｓとの関係を示すモデルのパラメータを学習する。

[0030] ここで、学習部１０５におけるパラメータの学習手順を説明する。学習部１０５では、過去のイベントをトリガーとして起こるイベントを、点過程を用いてモデル化する。一般的な点過程モデルの手続きに従い、まず強度関数の設計を行う。強度関数は、単位時間当たりにイベントが発生する確率である発生確率を表す関数である。以下にその一例を示す。

[0031] まず、イベント系列をモデル化するため、点過程の強度関数λ（ｘ｜θ）を導入する。ここで、強度関数λ（ｘ｜θ）は時刻χにおけるイベント（検索行動）の発生確率、θは強度関数のパラメータである。強度関数λ（ｘ｜θ）が与えられた下で、ｉ番目のイベント系列$x_i = \{\chi_1, \ldots, \chi_{n_i}\}$に対する点過程の尤度$Z_i$は、下記式（１）で表すことができる。

[0032] [数1]

$$Z_i \equiv \log p(\mathbf{x}_i|\lambda(x;\theta)) = \sum_{j=1}^{n_i} \lambda(x_j;\theta) - \int_0^T \lambda(x;\theta)dx \qquad \cdots (1)$$

[0033] 一般的な点過程の枠組みでは、各イベント系列に対する尤度Z_iの和$\Sigma^{n}_{i=1} Z_i$を最大化するθを求める。本開示では、当該尤度Z_iの和を最大化する目的関数を下記式（２）で表す。

[0034] [数2]

$$\mathcal{L} = \sum_{i=1}^{n} D(y_i|f(Z_i;\beta)) \qquad \cdots (2)$$

[0035] ここで、Ｄ（Ａ｜Ｂ）はＡとＢの乖離度を表す規準であり、例えば二乗誤差等を用いることができる。また、ｆ（・）は線形回帰モデル、βは線形回帰モデルのパラメータである。学習部１０５は、上記式（２）を最大化するように、パラメータθ及びβを学習する。当該最適化にはどのような方法を用いても良い。例えば、上記式（２）の目的関数を、勾配法を用いて最適化することができる。そして、学習部１０５は、学習したパラメータθ^（数式中は、θの上に“^”とする）及びβ^を、パラメータ格納部１０６に格納する。

[0036] パラメータ格納部１０６には、学習部１０５により学習されたパラメータθ^及びβ^の組を格納する。パラメータ格納部１０６は、推定したパラメータの組が保存され、復元可能なものであれば、なんでも良い。例えば、データベースや、予め備えられた汎用的な記憶装置（メモリやハードディスク装置）の特定領域に記憶される。

[0037] 対象データ格納部１０７には、異常度を予測する対象となるイベント系列ｘ′が格納されている。イベントデータは、学習データ格納部１０１に格納されているイベントデータと同様、時刻χ'_jのイベント系列ｘ′＝｛χ'_1，χ'_2，...｝で定義される。本開示では、時刻Ｔまでに観測されたｎ′個のイベント系列ｘ′からなるデータセットＸ′＝｛x'_i｝$^{n'}_{i=1}$が与えられているものとする。また、各イベント系列x'_iの長さをn'_iとおく。

[0038] 予測部１０８は、対象イベント系列x'_iと、モデルと、学習部１０５により学習されたパラメータθ^とに基づいて、対象イベント系列x'_iの異常度を算出する。

[0039] 具体的には、予測部１０８は、まず、パラメータ格納部１０６から学習済みパラメータθ^を取得する。次に、予測部１０８は、n'_i個のイベントからなる新しいイベント系列｛χ'_1，χ'_2，...｝とパラメータの推定値θ^とに基づいて、対象イベント系列ｘ′の異常度ｓ′を、下記式（３）及び（４）を用いて算出する。

[0040]

[数3]

$$Z' = \sum_{i=1}^{n'_i} \lambda(x'_i;\hat{\theta}) - \int_0^T \lambda(x;\hat{\theta})dx \quad \cdots (3)$$

$$s' = f(Z') \quad \cdots (4)$$

[0041] そして、予測部１０８は、算出した異常度ｓ′を、出力部１０９に渡す。

[0042] 出力部１０９は、予測部１０８により算出された異常度ｓ′を、予測結果として出力する。

[0043] ＜本開示の技術の実施形態に係る異常検知装置の作用＞

次に、異常検知装置１０の作用について説明する。

図５は、異常検知装置１０による異常検知処理ルーチンの流れを示すフローチャートである。ＣＰＵ１１がＲＯＭ１２又はストレージ１４から異常検知プログラムを読み出して、ＲＡＭ１３に展開して実行することにより、異常検知処理ルーチンが行なわれる。

[0044] ステップＳ１０１において、ＣＰＵ１１は、学習部１０５として、学習データ格納部１０１からデータセットＸを、ラベル格納部１０２からラベルＹを取得する。

[0045] ステップＳ１０２において、ＣＰＵ１１は、学習部１０５として、上記ステップＳ１０１により取得したデータセットＸ及びラベルＹに基づいて、イベント系列ｘと当該イベント系列ｘの異常度ｓとの関係を示すモデルのパラメータを学習する。

[0046] ステップＳ１０３において、ＣＰＵ１１は、学習部１０５として、上記ステップＳ１０２により学習したパラメータθ^及びβ^を、パラメータ格納部１０６に格納する。

[0047] ステップＳ１０４において、ＣＰＵ１１は、検索部１０４として、対象イベント系列ｘ′$_i$の入力を受け付ける。

[0048] ステップＳ１０５において、ＣＰＵ１１は、予測部１０８として、パラメータ格納部１０６から学習済みのパラメータθ^を取得する。

[0049] ステップＳ１０６において、ＣＰＵ１１は、予測部１０８として、対象イベント系列ｘ′ｉと、モデルと、上記ステップＳ１０５により取得したパラメータθ^とに基づいて、対象イベント系列ｘ′ｉの異常度を算出する。

[0050] ステップＳ１０７において、ＣＰＵ１１は、出力部１０９として、上記ステップＳ１０６により算出された異常度ｓ′を、予測結果として出力する。

[0051] 以上説明したように、本開示の実施形態に係る異常検知装置によれば、時系列のイベントデータである複数のイベント系列と、複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、時系列の各時刻におけるイベントの発生確率と複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、対象イベント系列の異常度を出力するモデルのパラメータを学習するため、精度よくイベントデータの異常検知をすることができる。

[0052] なお、本開示は、上述した実施形態に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。

[0053] 上記実施形態では、学習部及び予測部を含む各機能構成が１つのコンピュータで実現される場合について説明したが、学習部と予測部とは、それぞれ別のコンピュータで実現してもよい。この場合、学習部を含むコンピュータで学習されたパラメータをパラメータ格納部に格納しておき、予測部を含むコンピュータからパラメータ格納部に格納されたパラメータを読み出して、異常検知処理を実行すればよい。

[0054] なお、上記実施形態でＣＰＵがソフトウェア（プログラム）を読み込んで実行した異常検知プログラムを、ＣＰＵ以外の各種のプロセッサが実行してもよい。この場合のプロセッサとしては、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）等の製造後に回路構成を変更可能なＰＬＤ（Ｐｒｏｇｒａｍｍａｂｌｅ　Ｌｏｇｉｃ　Ｄｅｖｉｃｅ）、及びＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）等の特定の処理を実行させるために専用に設計さ

れた回路構成を有するプロセッサである専用電気回路等が例示される。また、異常検知プログラムを、これらの各種のプロセッサのうちの１つで実行してもよいし、同種又は異種の２つ以上のプロセッサの組み合わせ（例えば、複数のＦＰＧＡ、及びＣＰＵとＦＰＧＡとの組み合わせ等）で実行してもよい。また、これらの各種のプロセッサのハードウェア的な構造は、より具体的には、半導体素子等の回路素子を組み合わせた電気回路である。

[0055] また、上記各実施形態では、異常検知プログラムがＲＯＭ１２又はストレージ１４に予め記憶（インストール）されている態様を説明したが、これに限定されない。プログラムは、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＤＶＤ－ＲＯＭ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、及びＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）メモリ等の非一時的（ｎｏｎ－ｔｒａｎｓｉｔｏｒｙ）記憶媒体に記憶された形態で提供されてもよい。また、プログラムは、ネットワークを介して外部装置からダウンロードされる形態としてもよい。

[0056] 以上の実施形態に関し、更に以下の付記を開示する。

（付記項１）

メモリと、

前記メモリに接続された少なくとも１つのプロセッサと、

を含み、

前記プロセッサは、

時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する

ように構成されている異常検知装置。

[0057] （付記項２）

時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する

ことをコンピュータに実行させる異常検知プログラムを記憶した非一時的記憶媒体。

符号の説明

[0058] １０　異常検知装置

１１　ＣＰＵ

１２　ＲＯＭ

１３　ＲＡＭ

１４　ストレージ

１５　入力部

１６　表示部

１７　通信インタフェース

１９　バス

１０１　学習データ格納部

１０２　ラベル格納部

１０３　操作部

１０４　検索部

１０５　学習部

１０６　パラメータ格納部

１０７　対象データ格納部

１０８ 予測部

１０９ 出力部

請求の範囲

[請求項1] 時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する学習部

を含む異常検知装置。

[請求項2] 前記発生確率は、点過程の強度関数で表され、

前記目的関数は、前記複数のイベント系列の各々についての前記点過程の尤度を用いて表される線形回帰モデルで表され、

前記学習部は、前記目的関数の値が最大となるように、前記モデルのパラメータを学習する

請求項１記載の異常検知装置。

[請求項3] 前記対象イベント系列の入力を受け付ける検索部と、

前記対象イベント系列と、前記モデルと、前記学習部により学習されたパラメータとに基づいて、前記対象イベント系列の異常度を算出する予測部と、

を更に含む請求項１又は請求項２記載の異常検知装置。

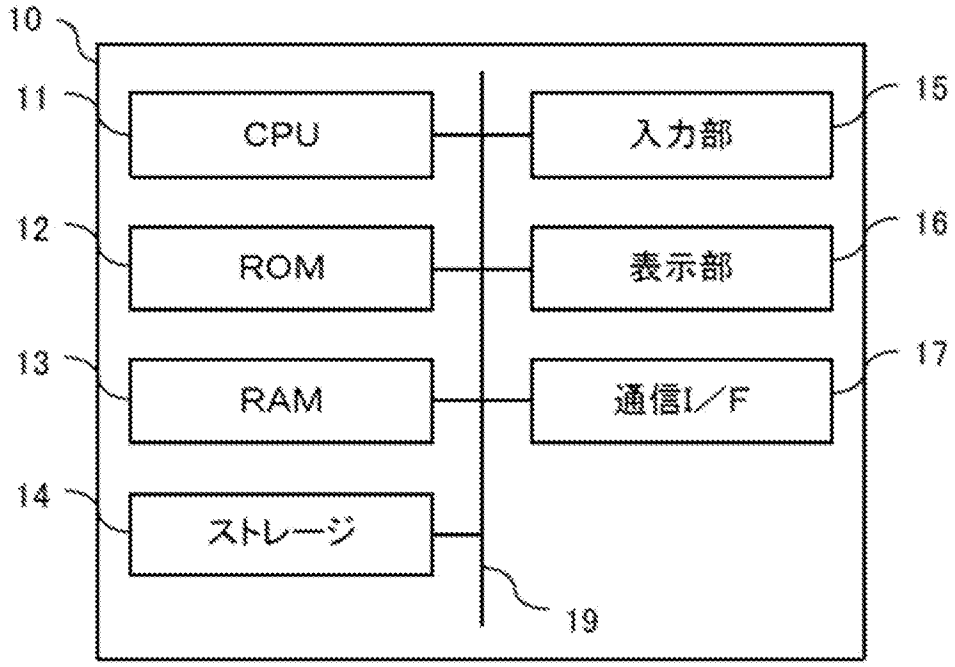
[請求項4] 学習部が、時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する

異常検知方法。

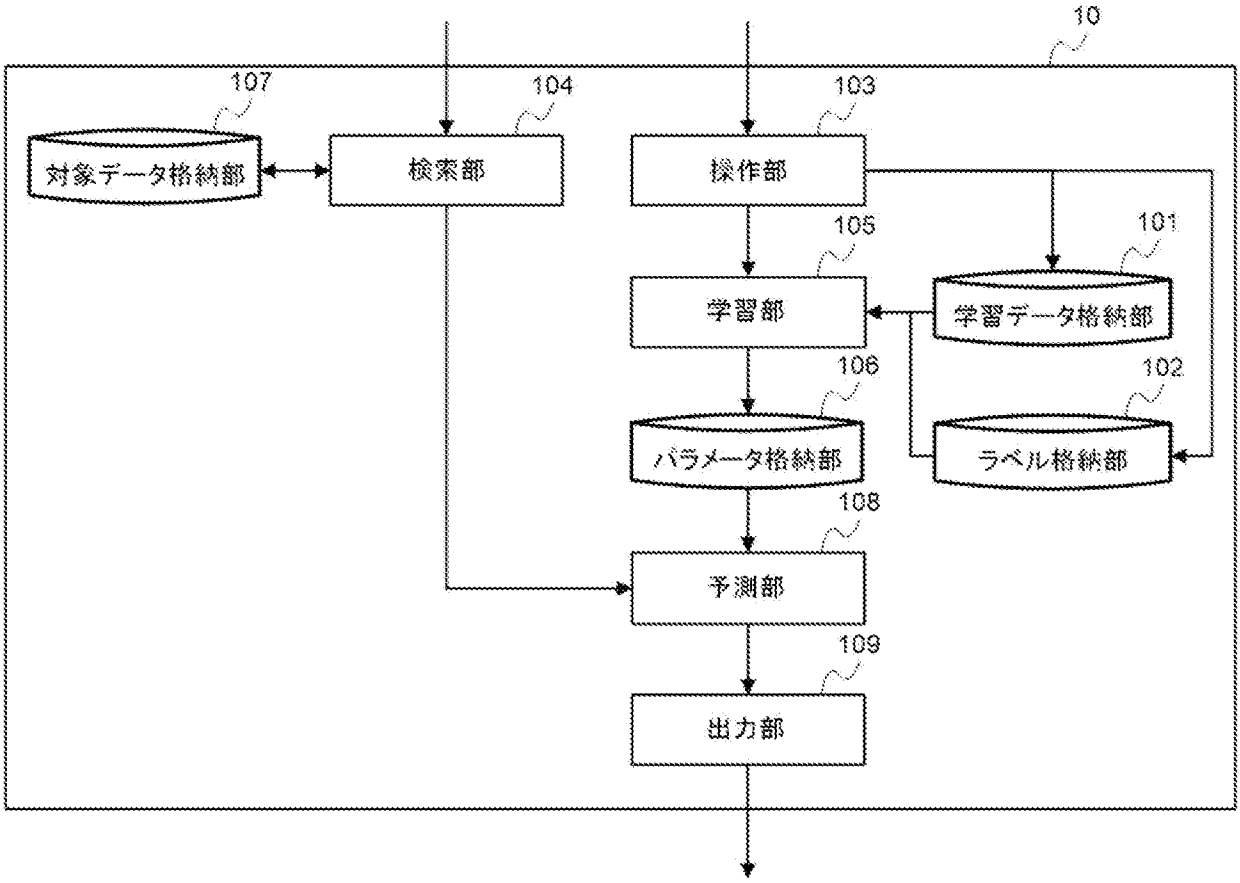
[請求項5] 学習部が、時系列のイベントデータである複数のイベント系列と、前記複数のイベント系列の各々の各イベントデータについての異常又は正常を示すラベルとに基づいて、前記時系列の各時刻におけるイベントの発生確率と前記複数のイベント系列の各々の異常度との関係を表す目的関数を最適化するように、異常度を予測する対象となるイベント系列である対象イベント系列を入力した場合に、前記対象イベント系列の異常度を出力するモデルのパラメータを学習する

ことを含む処理をコンピュータに実行させるための異常検知プログラム。

[図1]


10
11
CPU
12
ROM
13
RAM
14
ストレージ
19
15
入力部
16
表示部
17
通信I／F

[図2]


10
107
対象データ格納部
104
検索部
103
操作部
105
学習部
101
学習データ格納部
106
パラメータ格納部
102
ラベル格納部
108
予測部
109
出力部

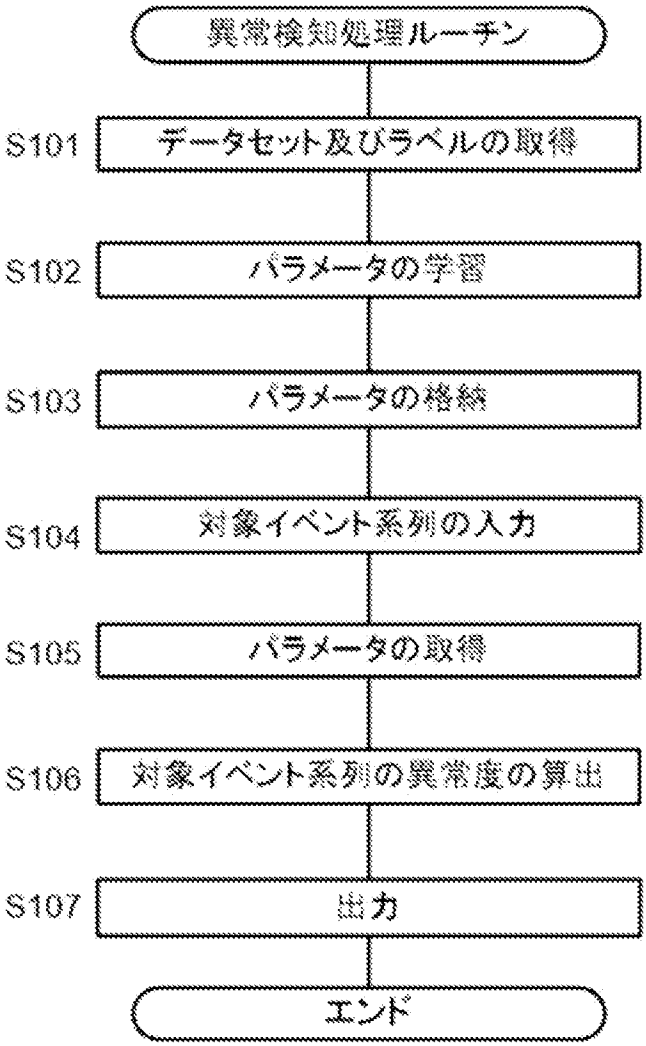
[図3]

検索対象のエリア	検索対象の日にち	検索対象の時間	検索ログ
A駅	2018/1/2	10:00	1,3,3,10,12,...
B駅	2018/1/4	12:00	5,10,10,12,,...
⋮		⋮	⋮
C駅	2018/12/30	21:00	1,1,2,3,5,...

[図4]

検索対象のエリア	検索対象の日にち	検索対象の時間	異常(混雑)
A駅	2018/1/2	10:00	1(混雑あり)
B駅	2018/1/4	12:00	0(混雑なし)
⋮		⋮	⋮
C駅	2018/12/30	21:00	0(混雑なし)

[図5]


異常検知処理ルーチン
S101
データセット及びラベルの取得
S102
パラメータの学習
S103
パラメータの格納
S104
対象イベント系列の入力
S105
パラメータの取得
S106
対象イベント系列の異常度の算出
S107
出力
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/023151

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06N20/00(2019.01)i

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. 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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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 2018-139085 A (NTT COMMUNICATIONS CORPORATION) 06 September 2018, paragraphs [0016], [0047]-[0053], fig. 4-5 (Family: none)	1-5
A	JP 2016-62544 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 25 April 2016, paragraphs [0014]-[0015], [0033]-[0035], fig. 2 & US 2016/0196505 A1, paragraphs [0023]-[0024], [0042]-[0044], fig. 2	1-5

☐ 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
07 August 2019 (07.08.2019)	20 August 2019 (20.08.2019)

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

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２３１５１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06N20/00(2019.01)i

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））

Int.Cl.　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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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 2018-139085 A (エヌ・ティ・ティ・コミュニケーションズ株式会社) 2018.09.06, 段落[0016], [0047]-[0053]及び[図4]-[図5] (ファミリーなし)	1-5
A	JP 2016-62544 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 2016.04.25, 段落[0014]-[0015], [0033]-[0035]及び[図2] & US 2016/0196505 A1, 段落[0023]-[0024], [0042]-[0044]及び[図2]	1-5

☐　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矛盾するものではなく、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
０７．０８．２０１９	２０．０８．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｂ　１５９９
多賀　実
電話番号　０３－３５８１－１１０１　内線　３５４５