

(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10月20日(20.10.2022)



(10) 国際公開番号

WO 2022/219787 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

都武蔵野市緑町3丁目9-11 NTT
知的財産センタ内 Tokyo (JP).

(21) 国際出願番号: PCT/JP2021/015632

(22) 国際出願日: 2021年4月15日(15.04.2021)

(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: 真田 勝(**SANADA, Masaru**); 〒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). 川口 英俊(**KAWAGUCHI, Hidetoshi**); 〒1808585 東京

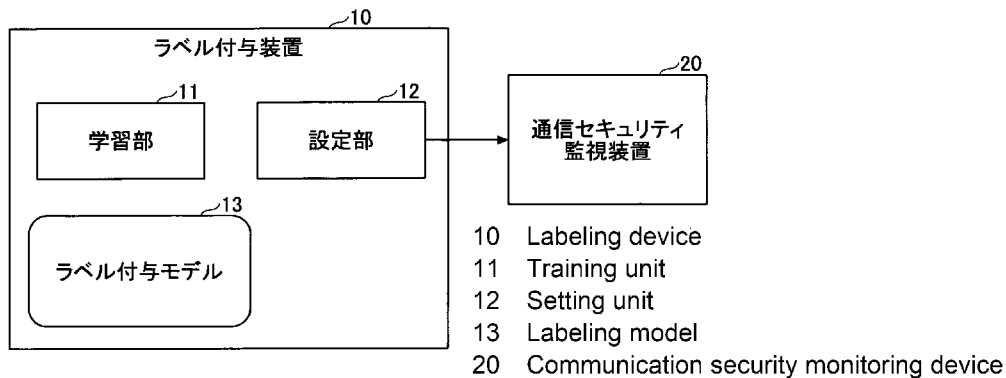
(74) 代理人: 伊東 忠重, 外(**ITO, Tadashige et al.**); 〒1000005 東京都千代田区丸の内二丁目1番1号 丸の内 M Y P L A Z A (明治安田生命ビル) 16階 Tokyo (JP).

(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, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,

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

(54) 発明の名称: ラベル付与装置、ラベル付与方法及びプログラム

[図3]



(57) **Abstract:** This labeling device comprises: a training unit which trains, on the basis of a first monitoring data group in which each of a plurality of pieces of monitoring data each showing characteristics of specific communication data is given a label indicating whether or not the monitoring data is necessary and indicating a method for coping with the specific communication data, a model that receives the monitoring data as an input and outputs the label corresponding to the monitoring data; and a setting unit which sets monitoring data with a label indicating that it is necessary among the first monitoring data group, to a monitoring device that monitors communication data on the basis of the monitoring data, whereby the load of setting work for a method for coping with the monitoring data is reduced.

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:

- 国際調査報告 (条約第21条(3))
-

(57) 要約: ラベル付与装置は、それぞれが特定の通信データの特徴を示す複数の監視データのそれぞれに対して当該監視データの要否及び前記特定の通信データに対する対処方法を示すラベルが付与された第1の監視データ群に基づいて、前記監視データを入力とし、当該監視データに対応する前記ラベルを出力するモデルを学習する学習部と、前記第1の監視データ群のうち必要であることを示すラベルが付与された監視データを、前記監視データに基づいて通信データを監視する監視装置へ設定する設定部と、を有することで、監視データに対する対処方法の設定作業の負荷を軽減する。

明 細 書

発明の名称： ラベル付与装置、ラベル付与方法及びプログラム
技術分野

[0001] 本発明は、ラベル付与装置、ラベル付与方法及びプログラムに関する。

背景技術

[0002] IDS (Intrusion Detection System) 又は IPS (Intrusion Prevention System) 等の通信セキュリティ監視装置は、通信路中に設けられ、通信データを監視し、悪意のある通信データ（脅威データ）を発見し対処（保存/通知/遮断等）する装置である（図1）。

[0003] IDS / IPS には、発見すべき脅威データ（監視データ）のリストが設定され、通信データと監視データとを比較することにより、脅威データを発見する。監視データには発見時の対処方法（保存する / 通知する / 遮断する、など）が設定されており、IDS / IPS はその設定に従って対処する。

[0004] IDS / IPS の監視データは、IDS / IPS を提供するセキュリティベンダから提供される。セキュリティベンダの監視データ（以下、「汎用監視データ」という。）は、汎用性を求めるため、網羅的であり膨大な数になる。

[0005] IDS / IPS を適用し運用する通信事業者がセキュリティベンダの汎用監視データをそのまま利用すると、通信データを膨大な数の汎用監視データと比較することになるため、通信の遅延などの通信性能劣化を引き起こすことになる。

[0006] そのため、通信事業者は、自通信システムの条件に応じて、必要な監視データ（以下、「個別監視データ」という。）のみを選別し、対処方法も自通信システム用に設定する。

先行技術文献

特許文献

[0007] 特許文献1：特開2019-174988

特許文献2：特開 2020-024513

特許文献3：特開 2020-160642

発明の概要

発明が解決しようとする課題

[0008] IDS／IPSを適用し運用する通信事業者にとって、セキュリティベンダの膨大な汎用監視データから個別監視データを選別し、個別の対処方法を設定するには大きな稼働を要する。

[0009] 本発明は、上記の点に鑑みてなされたものであって、監視データに対する対処方法の設定作業の負荷を軽減することを目的とする。

課題を解決するための手段

[0010] そこで上記課題を解決するため、ラベル付与装置は、それぞれが特定の通信データの特徴を示す複数の監視データのそれぞれに対して当該監視データの要否及び前記特定の通信データに対する対処方法を示すラベルが付与された第1の監視データ群に基づいて、前記監視データを入力とし、当該監視データに対応する前記ラベルを出力するモデルを学習する学習部と、前記第1の監視データ群のうち必要であることを示すラベルが付与された監視データを、前記監視データに基づいて通信データを監視する監視装置へ設定する設定部と、を有する。

発明の効果

[0011] 監視データに対する対処方法の設定作業の負荷を軽減することができる。

図面の簡単な説明

[0012] [図1] IDS／IPSを説明するための図である。

[図2] 本発明の実施の形態におけるラベル付与装置10のハードウェア構成例を示す図である。

[図3] 本発明の実施の形態におけるラベル付与装置10の機能構成例を示す図である。

[図4] ラベル付与モデル13の機能構成例を示す図である。

[図5]ラベル付与モデル13の初期学習を説明するための図である。

[図6]ラベル付き汎用監視データの構成例を示す図である。

[図7]学習済みラベル付与モデル13aを用いた運用及び学習済みラベル付与モデル13aの再学習を説明するための図である。

[図8]ラベル付与モデル13の学習手順を説明するための図である。

発明を実施するための形態

[0013] 以下、図面に基づいて本発明の実施の形態を説明する。図2は、本発明の実施の形態におけるラベル付与装置10のハードウェア構成例を示す図である。図2のラベル付与装置10は、それぞれバスBで相互に接続されているドライブ装置100、補助記憶装置102、メモリ装置103、プロセッサ104、及びインタフェース装置105等を有する。

[0014] ラベル付与装置10での処理を実現するプログラムは、CD-ROM等の記録媒体101によって提供される。プログラムを記憶した記録媒体101がドライブ装置100にセットされると、プログラムが記録媒体101からドライブ装置100を介して補助記憶装置102にインストールされる。但し、プログラムのインストールは必ずしも記録媒体101より行う必要はなく、ネットワークを介して他のコンピュータよりダウンロードするようにしてもよい。補助記憶装置102は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

[0015] メモリ装置103は、プログラムの起動指示があった場合に、補助記憶装置102からプログラムを読み出して格納する。プロセッサ104は、CPU若しくはGPU (Graphics Processing Unit)、又はCPU及びGPUであり、メモリ装置103に格納されたプログラムに従ってラベル付与装置10に係る機能を実行する。インタフェース装置105は、ネットワークに接続するためのインタフェースとして用いられる。

[0016] 図3は、本発明の実施の形態におけるラベル付与装置10の機能構成例を示す図である。図3において、ラベル付与装置10は、学習部11、設定部12及びラベル付与モデル13を含む。これら各部は、ラベル付与装置10

にインストールされた１以上のプログラムが、プロセッサ１０４に実行させる処理により実現される。

[0017] ラベル付与モデル１３は、セキュリティベンダから提供される監視データ（以下、「汎用監視データ」という。）の集合（以下、「汎用監視データ群」という。）を入力とし、当該監視データの分類結果と、当該分類結果に対する正誤の判定結果とを出力するモデルである。当該分類結果は、ラベルの形式で出力される。ラベルとは、当該ラベルが付与された汎用監視データの要否及び対処方法を示す情報である。ラベル付与モデル１３は、入力された汎用監視データに対して、分類結果としてのラベルを付与する。

[0018] 学習部１１は、汎用監視データ群に含まれる各汎用監視データと、当該汎用監視データに対するラベルとの対応関係をラベル付与モデル１３に学習させる。本実施の形態において、ラベル付与モデル１３の学習として、初期学習と再学習とが行われる。初期学習において、学習訓練データとして利用される汎用監視データに対するラベルは、ユーザによる手作業により付与される。

[0019] 設定部１２は、監視データに対する分類結果が示すラベルに基づいて、当該監視データの要否を判定し、必要な監視データを通信セキュリティ監視装置２０に設定する。なお、通信セキュリティ監視装置２０は、例えば、ＩＤＳ（Intrusion Detection System）又はＩＰＳ（Intrusion Prevention System）等である。すなわち、通信セキュリティ監視装置２０は、設定された監視データに基づき通信データを監視し、当該監視データに該当する特定の通信データを検知（発見）するとともに、当該特定の通信データに対して、当該監視データに付与されたラベルが示す対処方法に応じた処理を実行する。

[0020] 図４は、ラベル付与モデル１３の機能構成例を示す図である。図４が示すように、ラベル付与モデル１３は、分類推定部１３１、分類推定過程観測部１３２及び誤り判定部１３３の３つのモデルを含む。これら各部は、特許文献２に記載された同名の機能部と同様でよい。

[0021] 具体的には、分類推定部１３１は、入力された汎用監視データのラベルを

推定し、当該ラベルを分類結果として出力する。分類推定部 131 は、例えば、SVM、ニューラルネットワーク、ベイジアンネットワーク、決定木などの人工知能関連の技術を用いて実現できる。

[0022] 分類推定過程観測部 132 は、分類推定部 131 が汎用監視データのラベルを推定する際の計算過程（推定過程）を観測して、当該推定過程のデータを取得し、当該データを特徴ベクトルへ変換し、当該特徴ベクトルを誤り判定部 133 へ出力する。

[0023] 例えば、分類推定部 131 がニューラルネットワークを用いてラベルを推定する場合、分類推定過程観測部 132 は、ニューラルネットワークの各中間層と出力層の各ノード（活性化関数）から出力される値を特徴ベクトルとして出力してもよい。例えば、中間層の各ノードの値が 0.5, 0.4, 0.7 であり、出力層の各ノードの値が 0.2, 0.7, 0.1 である場合、特徴ベクトルは [0.5 0.4 0.7 0.2 0.7 0.1] と構成することができる。

[0024] 又は、分類推定部 131 が決定木を用いてラベルを推定する場合、分類推定過程観測部 132 は、分類が決定に至るルートを観測して特徴ベクトルを構成する。例えば、ノード 1 → ノード 3 → ノード 6 というルートで或るラベルが推定された場合、分類推定過程観測部 132 は、当該ルートを示す [1 0 1 0 0 1 0 0 0] を特徴ベクトルとして出力してもよい。この例では、ベクトルの要素の添え字と、決定木のノード番号とが対応しており、そのノードを通過したならそのノードに対応する要素に 1 が入り、通過していないなら 0 が入るようにして特徴ベクトルを構成している。

[0025] その他の特徴ベクトルの例については特許文献 2 に開示されている通りである。

[0026] 誤り判定部 133 は、分類推定過程観測部 132 から特徴ベクトルを受け取り、当該特徴ベクトルに基づいて、分類推定部 131 が推定したラベルが「正しい」か「誤り」であるかを判定する。

[0027] 誤り判定部 133 の構成方法は特定の方法に限定されない。例えば、誤り

判定部 133 は、特徴ベクトルの特定の値（特にニューラルネットワークの出力層の値やランダムフォレストの得票数）が閾値を越えているかどうかを判定することで、分類推定部 131 が推定したラベルが「正しい」ものか「誤り」であるかを判定することができる。

[0028] また、誤り判定部 133 は機械学習分野でよく用いられているモデルで構成することとしてもよい。例えば SVM、あるいはニューラルネットワークなどで誤り判定部 133 を構成することができる。これらのモデルを用いる場合、教師あり学習でモデルのパラメータチューニングを行なうことで誤り判定部 133 を実装することができる。

[0029] 図 5 は、ラベル付与モデル 13 の初期学習を説明するための図である。

[0030] 初期学習の時点では、ラベル付与モデル 13 を学習させる学習訓練データが存在しない。そこで、学習部 11 は、初期学習の時点までの所定の期間にセキュリティベンダから提供された複数の汎用監視データの集合（以下、「汎用監視データ群 X」という。）の全て、又は一部の汎用監視データについて、ラベルの入力をユーザから受け付け、入力されたラベルが付与されたラベル付き汎用監視データ群 X を学習訓練データとして生成する（S101）。ラベルの付与対象を一部の汎用監視データに限定する場合、当該一部は、例えば、ランダムに選択されてもよい。

[0031] 図 6 は、ラベル付き汎用監視データの構成例を示す図である。図 6 における 1 行は、ラベル付き汎用監視データを示す。1 つのラベル付き汎用監視データは、汎用監視データとラベルとを含む。汎用監視データは、特定の（例えば、悪意のある）通信データ（脅威データ）の特徴を示すデータであり、例えば、プロトコル、ソースアドレス、ソースポート、宛先アドレス、宛先ポート及び通信内容データを含む。

[0032] 本実施の形態において、ラベルの値は、「不要」、「保存」、「通知」又は「遮断」である。

[0033] 「不要」は、当該ラベルを付与された汎用監視データが通信事業者にとって不要であることを示す。

- [0034] 「保存」、「通知」及び「遮断」は、通信事業者にとって必要な汎用監視データに対して付与されるラベルである。換言すれば、「保存」、「通知」及び「遮断」は、当該ラベルを付与された汎用監視データが通信事業者にとって必要であることとともに、当該汎用監視データに該当する通信データの発見時の対処方法を示す。
- [0035] 「保存」は、当該通信データを保存することを示す。「通知」は、当該通信データの検知を通信事業者へ通知させることを示す。「遮断」は、当該通信データを遮断することを示す。
- [0036] 例えば、通信事業者は、汎用監視データに関する別の情報（サイバー攻撃の報道や、業者内部の不具合の情報等）に基づき、汎用監視データ群Xに含まれる各汎用監視データについて要否を選別し、不要な汎用監視データには「不要」を付与し、必要な汎用監視データには当該汎用監視データに該当する通信データの発見時の対処を決定する。
- [0037] 設定部12は、ラベル付き汎用監視データ群Xから、「不要」以外のラベルが付与された汎用監視データ（以下、「ラベル付き個別監視データ」という。）を抽出し、各ラベル付き個別監視データを通信セキュリティ監視装置20へ設定する（S102）。この際、設定部12は、各ラベル付き個別監視データに該当する通信データを発見した場合の対処方法を各ラベル付き個別監視データに付与されているラベルに基づいて特定し、当該対処方法を通信セキュリティ監視装置20へ設定する。
- [0038] 一方、学習部11は、ラベル付き汎用監視データ群Xを学習訓練データとしてラベル付与モデル13を学習する（S103）。その結果、学習済みラベル付与モデル13aが生成される。
- [0039] 次に、学習済みラベル付与モデル13aを用いた運用及び学習済みラベル付与モデル13aの再学習について説明する。
- [0040] 図7は、学習済みラベル付与モデル13aを用いた運用及び学習済みラベル付与モデル13aの再学習を説明するための図である。再学習は、学習済みラベル付与モデル13aを用いた運用と並行して行われる。

[0041] 図7は、学習済みラベル付与モデル13aの生成後に、新たな複数の汎用監視データの集合（以下、「汎用監視データ群Y」という。）がセキュリティベンダから提供された場合の運用及び学習済みラベル付与モデル13aの再学習の例を示す。なお、汎用監視データ群Yは、汎用監視データ群Xを内包する場合と、新規データのみである場合が考えられる。

[0042] まず、学習済みラベル付与モデル13aに対して汎用監視データ群Yに含まれる各汎用監視データが入力される（S201）。学習済みラベル付与モデル13aは、当該汎用監視データごとに、当該汎用監視データに対するラベルと、当該ラベルについての正誤の判定結果とを出力する。正誤の判定結果は、「正しい」又は「誤り」である。以下、正誤の判定結果が「正しい」であるラベルに係る汎用監視データ群を、「確実なラベル付き汎用監視データ群Y（自動）」といい、当該判定結果が「誤り」であるラベルに係る汎用監視データ群を、「不確実なラベル付き汎用監視データ群Y」という。なお、「確実なラベル付き汎用監視データ群Y（自動）」における「（自動）」は、後述において、ユーザの手作業によって生成される、後述の確実なラベル付き汎用監視データ群Y（手動）と区別するための、便宜的な識別情報である。

[0043] 学習部11は、不確実なラベル付き汎用監視データ群Yに含まれる各ラベル付き汎用監視データについて、ユーザから正しいラベルの入力を受け付け、ユーザによって入力されたラベルによって、付与されているラベルを訂正（置換）する（S202）。これによって、不確実なラベル付き汎用監視データ群Yは、確実なラベル付き汎用監視データ群Y（手動）となる。すなわち、ユーザの手作業によってラベルの訂正が行われるため、正しいラベルが付与されたラベル付き汎用監視データが生成される。

[0044] 設定部12は、確実なラベル付き汎用監視データ群Y（自動）及び確実なラベル付き汎用監視データ群Y（手動）から、「不要」以外のラベルが付与された汎用監視データ（以下、「ラベル付き個別監視データ」という。）を抽出し、各ラベル付き個別監視データを通信セキュリティ監視装置20へ設

定する（S 2 0 3）。

[0045] 学習部 1 1 は、また、確実なラベル付き汎用監視データ群 Y（自動）及び確実なラベル付き汎用監視データ群 Y（手動）を学習訓練データとしてラベル付与モデル 1 3 を再学習する（S 2 0 4）。その結果、再学習済みラベル付与モデル 1 3 b が生成される。

[0046] なお、汎用監視データ群 Y が汎用監視データ群 X を内包する場合は、これらに基づく確実なラベル付き汎用監視データ群 Y を学習訓練データとして学習済みラベル付与モデル 1 3 a を再学習することができる。学習訓練データの数が多いほど学習効果は高くなり、正しい結果を得る可能性が高くなる。汎用監視データ群 Y が新規データのみである場合でも、新規の学習訓練データが得られる。新規の学習訓練データによる再学習によってラベル付与モデル 1 3 の性能の向上を期待することができる。

[0047] その後、新たな汎用監視データ群がセキュリティベンダから提供された場合には、図 7 と同じ手順によって再学習済みラベル付与モデル 1 3 b を用いて運用が行われるとともに、再学習済みラベル付与モデル 1 3 b について再学習が行われる。

[0048] 続いて、図 5 のステップ S 1 0 3 及び図 7 のステップ S 2 0 4 の詳細について説明する。図 8 は、ラベル付与モデル 1 3 の学習手順を説明するための図である。図 8 における（ラベル付き）汎用監視データ群 Z は、図 5 の場合には、（ラベル付き）汎用監視データ群 X であり、図 7 の場合には、（確実なラベル付き）汎用監視データ群 Y（自動又は手動）である。

[0049] まず、学習部 1 1 は、ラベル付き汎用監視データ群 Z を用いて、汎用監視データとラベルとの対応関係を分類推定部 1 3 1 に学習させる（S 3 0 1）。

[0050] 続いて、学習部 1 1 は、学習済みの分類推定部 1 3 1 に対して汎用監視データ群 Z を入力する（S 3 0 2）。分類推定部 1 3 1 は、汎用監視データ群 Z に含まれるそれぞれの汎用監視データに対して推定したラベルのリスト（以下、「推定ラベルリスト」という。）を出力する（S 3 0 3）。この際、

分類推定過程観測部 1 3 2 は、当該汎用監視データごとに、ラベルの推定過程のデータを取得し（S 3 0 4）、当該データごとに特徴ベクトルを出力する（S 3 0 5）。

[0051] 続いて、学習部 1 1 は、ラベル付き汎用監視データ群 Z に含まれるそれぞれのラベル付き汎用監視データに付与されている正しいラベルのリスト（以下、「正解ラベルリスト」という。）と、推定ラベルリストとをリストの要素ごと（すなわち、同一の汎用監視データに対応するラベルごと）に比較し、推定ラベルリストに含まれる各ラベルの正誤を示すリスト（以下、「正誤リスト」という。）を生成する（S 3 0 6）。正誤リストは、例えば、「1 0 1 1 . . . 」のように、1 又は 0 のリストである。0 は正解のラベルを示し、1 は誤りのラベルを示す。

[0052] 続いて、学習部 1 1 は、特徴ベクトルのリストと正誤リストとの対応関係を誤り判定部 1 3 3 に学習させる（S 3 0 7）。その結果、誤り判定部 1 3 3 は、学習済みとなる。なお、誤り判定部 1 3 3 の学習については、特許文献 2 にも詳しい。

[0053] 上述したように、本実施の形態によれば、ラベル付与モデル 1 3 によって、汎用監視データに対して自動的なラベル付けを可能とすることができる。その結果、監視データに対する対処方法の設定作業の負荷を軽減することができる。また、ラベル付与モデル 1 3 を再学習することで、分類精度を向上させることができる。

[0054] なお、本実施の形態において、学習部 1 1 は、再学習部の一例でもある。

[0055] 以上、本発明の実施の形態について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

符号の説明

[0056] 1 0 ラベル付与装置
1 1 学習部
1 2 設定部

1 3	ラベル付与モデル
1 3 a	学習済みラベル付与モデル
1 3 b	再学習済みラベル付与モデル
2 0	通信セキュリティ監視装置
1 0 0	ドライブ装置
1 0 1	記録媒体
1 0 2	補助記憶装置
1 0 3	メモリ装置
1 0 4	プロセッサ
1 0 5	インタフェース装置
1 3 1	分類推定部
1 3 2	分類推定過程観測部
1 3 3	誤り判定部
B	バス

請求の範囲

- [請求項1] それぞれが特定の通信データの特徴を示す複数の監視データのそれぞれに対して当該監視データの要否及び前記特定の通信データに対する対処方法を示すラベルが付与された第1の監視データ群に基づいて、前記監視データを入力とし、当該監視データに対応する前記ラベルを出力するモデルを学習する学習部と、
- 前記第1の監視データ群のうち必要であることを示すラベルが付与された監視データを、前記監視データに基づいて通信データを監視する監視装置へ設定する設定部と、
- を有することを特徴とするラベル付与装置。
- [請求項2] 前記学習部は、前記監視データを入力とし、当該監視データに対応する前記ラベルと当該ラベルについての正誤の判定結果とを出力する前記モデルを学習し、
- 第2の監視データ群に含まれる前記監視データのうち、前記モデルが正しいと判定した第1のラベルが出力された前記監視データに対して当該第1のラベルが付与された第1のラベル付き監視データと、前記モデルが誤りであると判定した前記ラベルが出力された前記監視データに対してユーザによって入力された第2のラベルが付与された第2のラベル付き監視データとに基づいて前記モデルを再学習する再学習部、
- を有することを特徴とする請求項1記載のラベル付与装置。
- [請求項3] 前記設定部は、前記第1のラベル付き監視データと前記第2のラベル付き監視データとを前記監視装置へ設定する、
- ことを特徴とする請求項2記載のラベル付与装置。
- [請求項4] それぞれが特定の通信データの特徴を示す複数の監視データのそれぞれに対して当該監視データの要否及び前記特定の通信データに対する対処方法を示すラベルが付与された第1の監視データ群に基づいて、前記監視データを入力とし、当該監視データに対応する前記ラベル

を出力するモデルを学習する学習手順と、

前記第 1 の監視データ群のうち必要であることを示すラベルが付与された監視データを、前記監視データに基づいて通信データを監視する監視装置へ設定する設定手順と、

をコンピュータが実行することを特徴とするラベル付与方法。

[請求項5]

前記学習手順は、前記監視データを入力とし、当該監視データに対応する前記ラベルと当該ラベルについての正誤の判定結果とを出力する前記モデルを学習し、

第 2 の監視データ群に含まれる前記監視データのうち、前記モデルが正しいと判定した第 1 のラベルが出力された前記監視データに対して当該第 1 のラベルが付与された第 1 のラベル付き監視データと、前記モデルが誤りであると判定した前記ラベルが出力された前記監視データに対してユーザによって入力された第 2 のラベルが付与された第 2 のラベル付き監視データとに基づいて前記モデルを再学習する再学習手順、

をコンピュータが実行することを特徴とする請求項 4 記載のラベル付与方法。

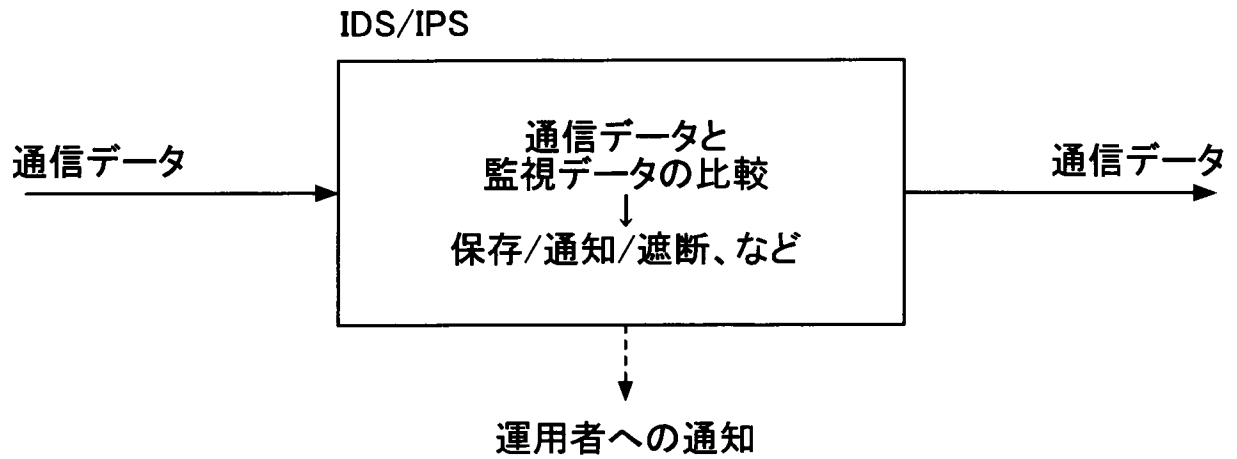
[請求項6]

前記設定手順は、前記第 1 のラベル付き監視データと前記第 2 のラベル付き監視データとを前記監視装置へ設定する、
ことを特徴とする請求項 5 記載のラベル付与方法。

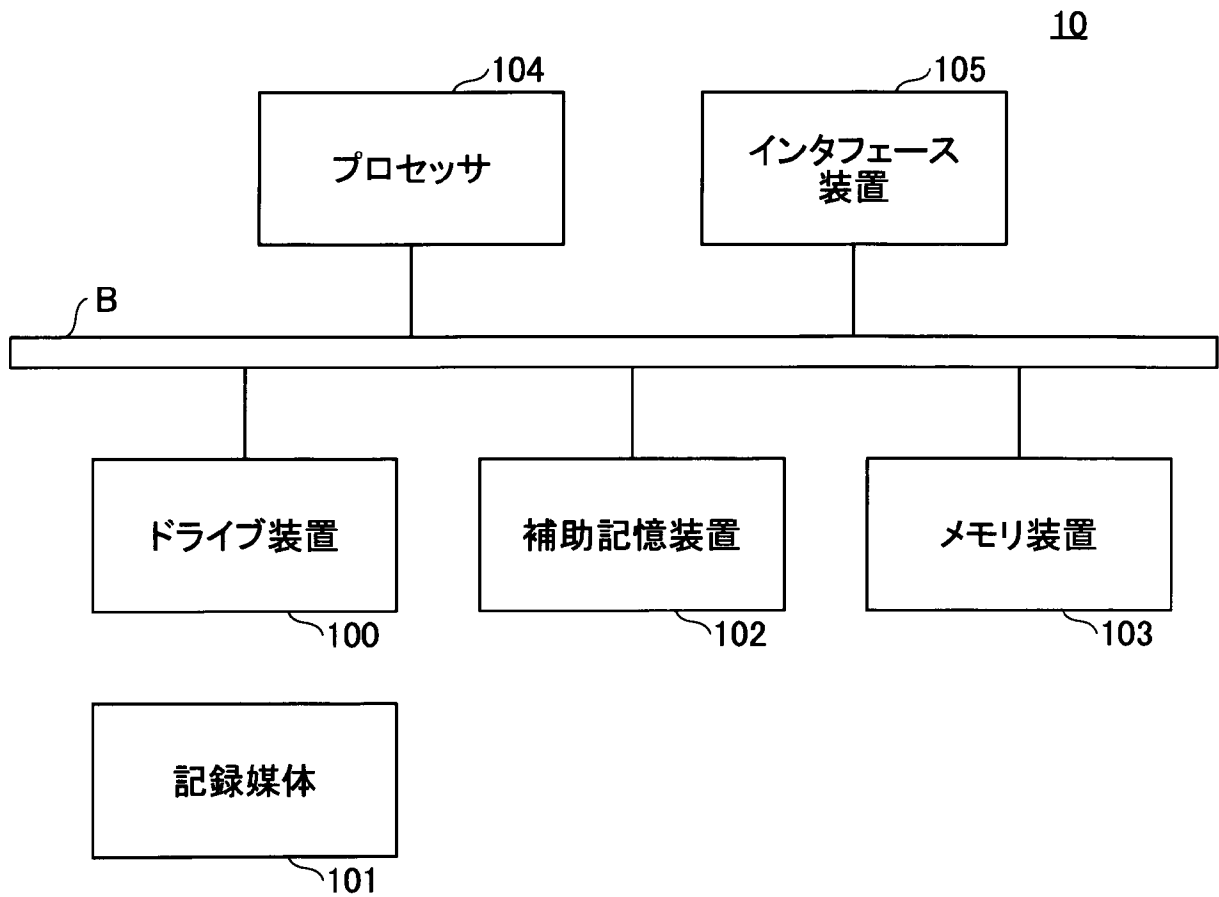
[請求項7]

請求項 4 乃至 6 いずれか一項記載のラベル付与方法をコンピュータに実行させることを特徴とするプログラム。

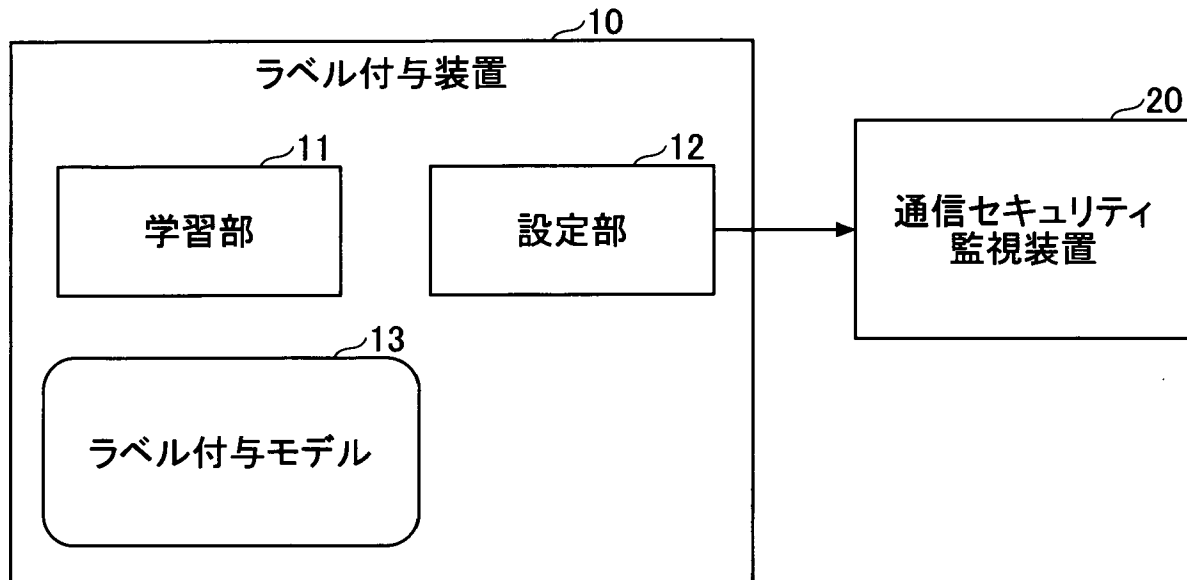
[図1]



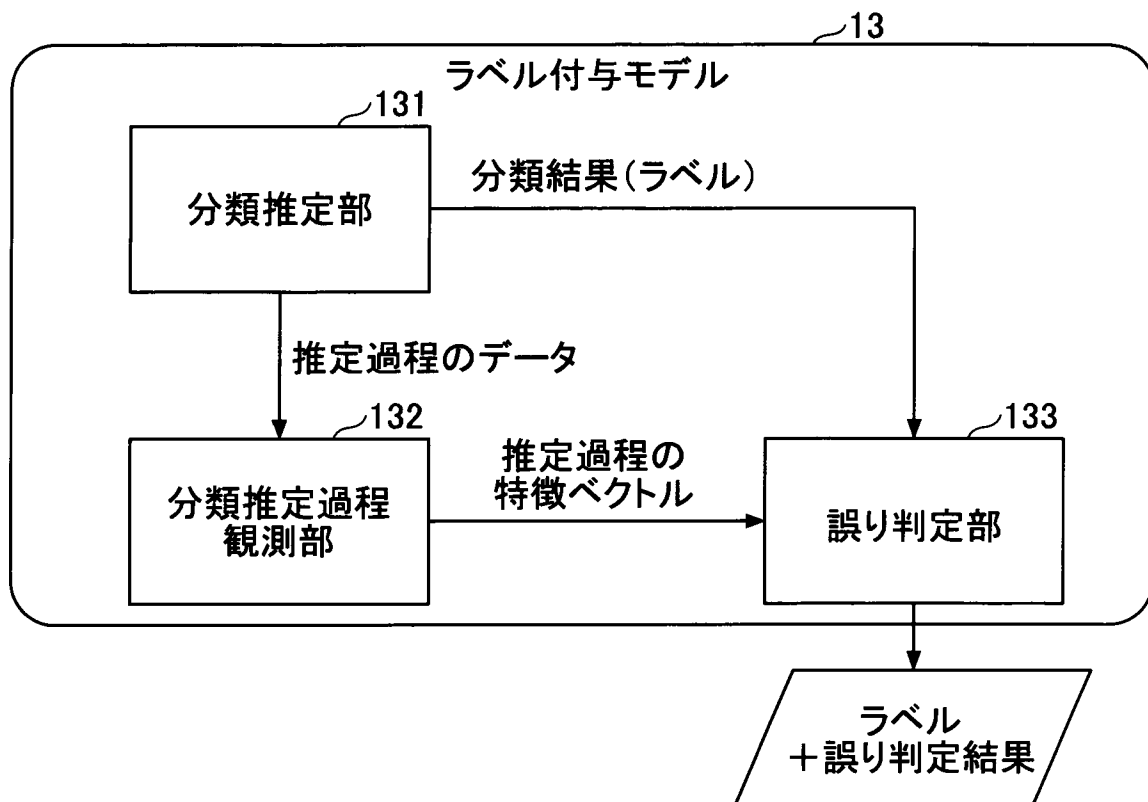
[図2]



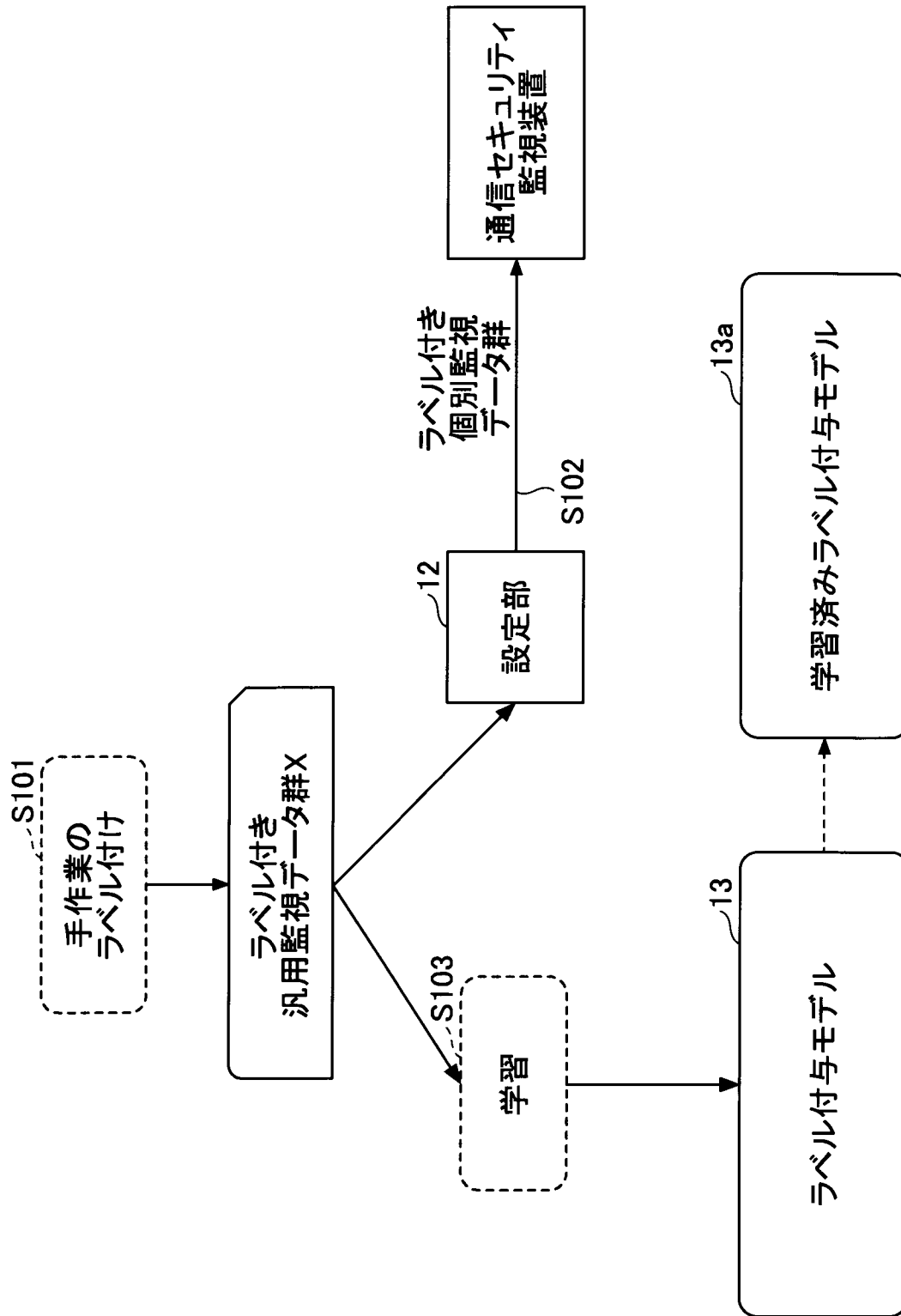
[図3]



[図4]



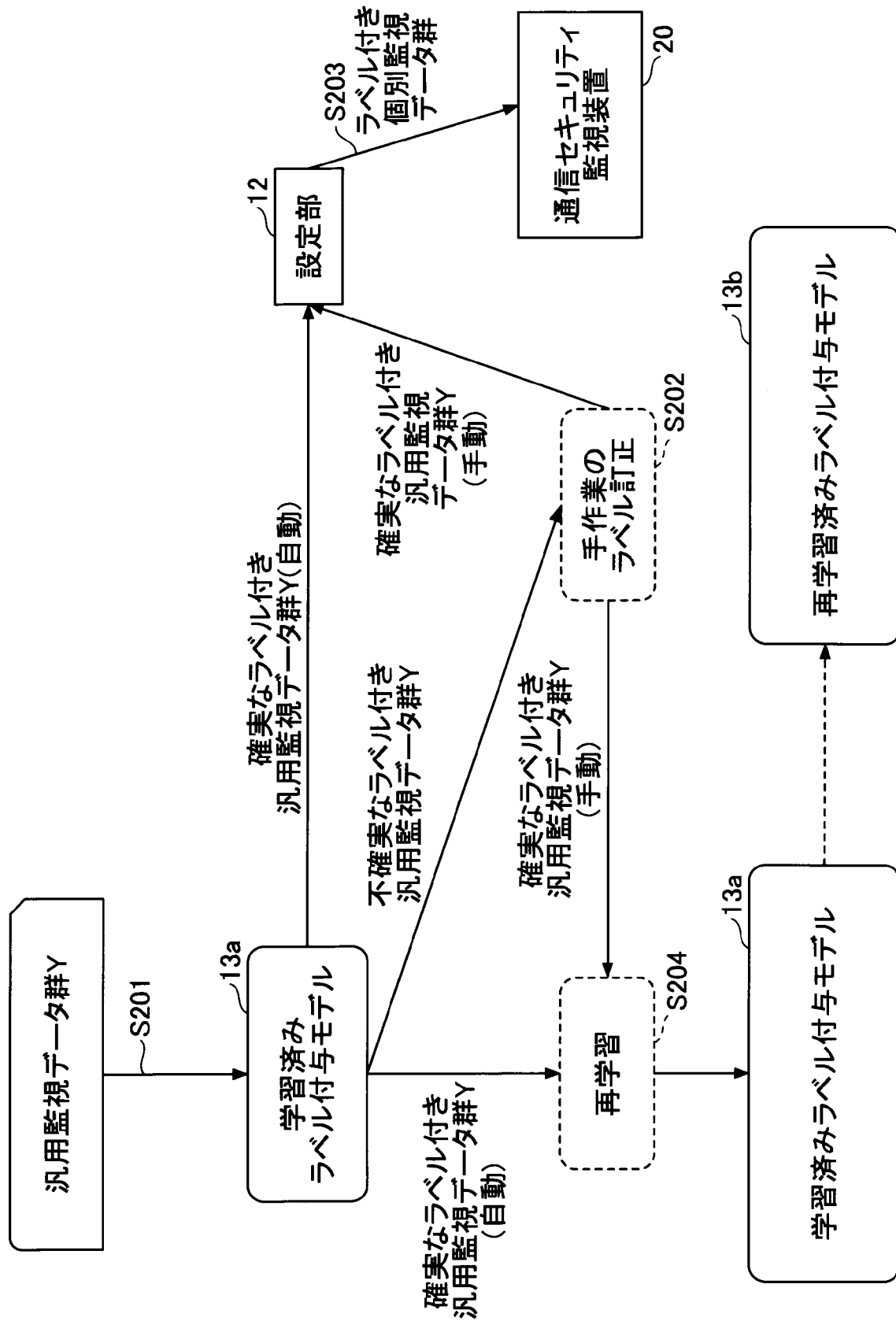
[図5]



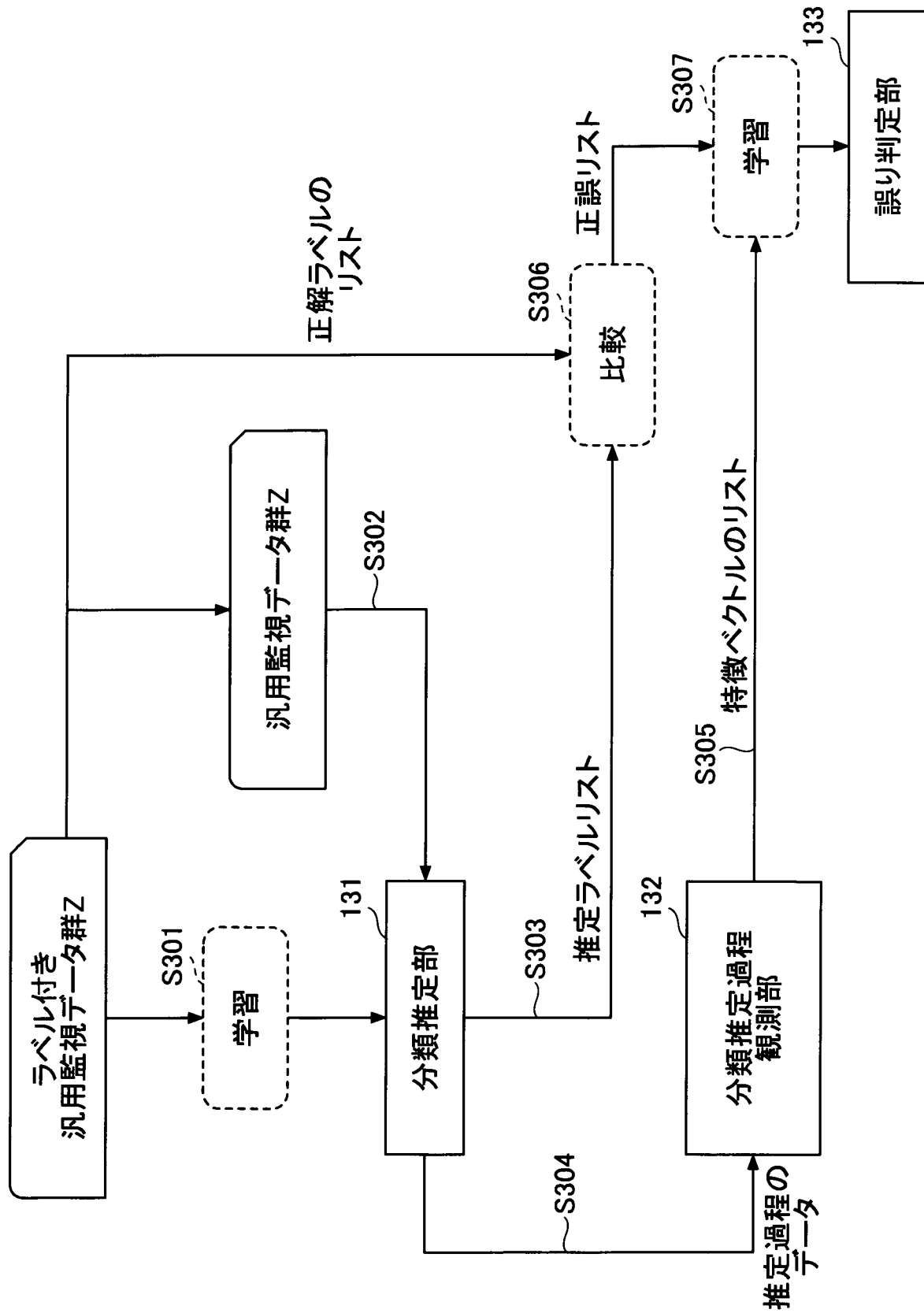
[図6]

プロトコル	ソースアドレス	ソースポート	宛先アドレス	宛先ポート	通信内容	ラベル
A	111	100	7070	100	Aaaabbbb	保存
A	222	100	7070	100	Aaaabbbb	通知
B	444	500	8800	500	Cccddd	不要
C	666	200	9000	300	Eeefff	遮断

[图7]



[図8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/015632

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55(2013.01)i

FI: G06F21/55

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)

G06F21/55

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2020/031960 A1 (NIPPON TELEGRAPH & TELEPHONE) 13 February 2020 (2020-02-13) claims 1-4, paragraph [0002]	1-7
A	JP 2018-77607 A (HITACHI SYSTEMS LTD) 17 May 2018 (2018-05-17) claim 1	1-7
A	JP 2020-149090 A (FUJITSU LTD) 17 September 2020 (2020-09-17) claim 1	1-7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
23 June 2021 (23.06.2021)

Date of mailing of the international search report
06 July 2021 (06.07.2021)

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/JP2021/015632

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2020/031960 A1	13 Feb. 2020	JP 2020-24513 A	
JP 2018-77607 A	17 May 2018	WO 2018/088383 A1	
JP 2020-149090 A	17 Sep. 2020	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/55(2013.01)i FI: G06F21/55														
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）） G06F21/55 最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2021年	日本国実用新案登録公報	1996 - 2021年	日本国登録実用新案公報	1994 - 2021年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2021年													
日本国実用新案登録公報	1996 - 2021年													
日本国登録実用新案公報	1994 - 2021年													
C. 関連すると認められる文献														
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号												
A	WO 2020/031960 A1（日本電信電話株式会社）13.02.2020（2020 - 02 - 13） 請求項1-4,段落[0002]	1-7												
A	JP 2018-77607 A（株式会社日立システムズ）17.05.2018（2018 - 05 - 17） 請求項1	1-7												
A	JP 2020-149090 A（富士通株式会社）17.09.2020（2020 - 09 - 17） 請求項1	1-7												
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</td> </tr> <tr> <td>“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</td> <td>“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</td> </tr> <tr> <td>“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献	“O” 口頭による開示、使用、展示等に言及する文献		“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献	
* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの													
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの													
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献													
“O” 口頭による開示、使用、展示等に言及する文献														
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献														
国際調査を完了した日 23.06.2021	国際調査報告の発送日 06.07.2021													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 宮司 卓佳 5S 9555 電話番号 03-3581-1101 内線 3546													

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/JP2021/015632

引用文献			公表日	パテントファミリー文献			公表日
WO	2020/031960	A1	13.02.2020	JP	2020-24513	A	
JP	2018-77607	A	17.05.2018	WO	2018/088383	A1	
JP	2020-149090	A	17.09.2020	(ファミリーなし)			