(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
2024年12月12日(12.12.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/252481 A1

(51) 国際特許分類:
H04L 43/50 (2022.01) *G06F 11/263* (2006.01)
G06F 11/22 (2006.01)

(21) 国際出願番号： PCT/JP2023/020847

(22) 国際出願日： 2023年6月5日(05.06.2023)

(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: 高橋 洋介 (**TAKAHASHI, Yosuke**); 〒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). 池内光希(**IKEUCHI, Hiroki**); 〒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). 渡邉 暁(**WATANABE, Akio**); 〒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).

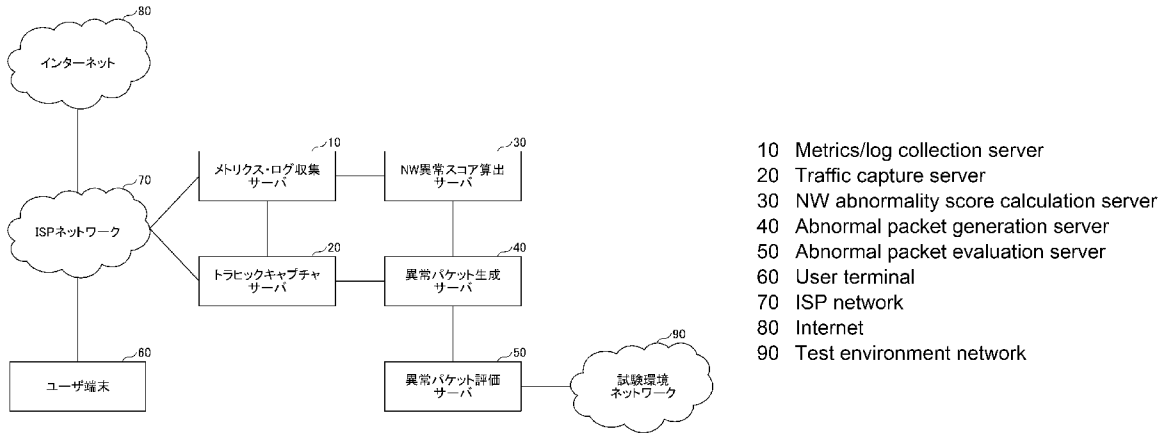
(74) 代理人: 伊東 忠重, 外(**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内 ＭＹ ＰＬＡＺＡ （明治安田生命ビル） １６階 Tokyo (JP).

(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,

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

(54) 発明の名称： 異常パケット生成装置、異常パケット生成方法、及びプログラム

[図1]



(57) **Abstract:** An abnormal packet generation device according to an aspect of the present disclosure comprises: an acquisition unit that acquires packets of the same time as log data and metrics for which a first abnormality score calculated by a trained abnormality detector exceeds a first predetermined threshold value; a generation unit that generates abnormal packet candidates by data augmentation from the packets; and a selection unit that selects, as abnormal packets from among the abnormal packet candidates, top N abnormal packet candidates based on a second abnormality score calculated by a trained classifier.

(57) 要約：本開示の一態様による異常パケット生成装置は、学習済み異常検知器によって算出された第１の異常スコアが所定の第１の閾値を超えているメトリクス及びログデータと同一時刻のパケットを取得する取得部と、前記パケットからデータ拡張により異常パケット候補を生成する生成部と、前記異常パケット候補から学習済み分類器によって算出された第２の異常スコアが上位Ｎ件の異常パケット候補を異常パケットとして選択する選択部と、を有する。

WO 2024/252481 A1

［続葉有］

BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

明　細　書

発明の名称 ：

異常パケット生成装置、異常パケット生成方法、及びプログラム

技術分野

[0001] 本開示は、異常パケット生成装置、異常パケット生成方法、及びプログラムに関する。

背景技術

[0002] インターネットサービスプロバイダ（ＩＳＰ）のネットワーク装置は、インターネットの安定性や速度を維持するために極めて重要な役割を担っている。一方で、これらのネットワーク装置は、例えば、ソフトウェアのバグ、設定ミス、ハードウェアの不具合等により、異常パケットをトリガーとして機能停止することがある。このため、異常パケットを事前に生成し、ネットワーク装置のテストに活用することが行われている。

[0003] 異常パケットを生成するための従来手法として、総当たりによるパケット生成、既知の脆弱性に基づくパケット生成、機械学習を利用したパケット生成（例えば、非特許文献１及び２）等が知られている。

先行技術文献

非特許文献

[0004] 非特許文献1：Cheng, Adriel. "PAC-GAN: Packet generation of network traffic using generative adversarial networks." 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2019.

非特許文献2：Nukavarapu, Santosh Kumar, Mohammed Ayyat, and Tamer Nadeem. "MirageNet-towards a GAN-based framework for synthetic network traffic generation." GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, 2022.

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、異常パケットを生成するための従来手法では、効果的な異常パケットを効率的に生成することができなかった。例えば、総当たりによるパケット生成では試行回数が膨大となり、効率性の点で問題がある。また、例えば、既知の脆弱性に基づくパケット生成では未知の脆弱性に対して効果的な異常パケットを生成することはできない。また、例えば、機械学習を利用したパケット生成では機械学習アルゴリズムにより実際のパケットに類似するパケットを生成するため、事前に大量の異常パケットを準備する必要があり、効率性の点で問題がある。

[0006] 本開示は、上記の点に鑑みてなされたもので、効果的な異常パケットを効率的に生成できる技術を提供する。

課題を解決するための手段

[0007] 本開示の一態様による異常パケット生成装置は、学習済み異常検知器によって算出された第１の異常スコアが所定の第１の閾値を超えているメトリクス及びログデータと同一時刻のパケットを取得する取得部と、前記パケットからデータ拡張により異常パケット候補を生成する生成部と、前記異常パケット候補から学習済み分類器によって算出された第２の異常スコアが上位Ｎ件の異常パケット候補を異常パケットとして選択する選択部と、を有する。

発明の効果

[0008] 効果的な異常パケットを効率的に生成できる技術が提供される。

図面の簡単な説明

[0009] [図1]本実施形態に係るシステムの全体構成の一例を示す図である。

[図2]本実施形態に係るＮＷ異常スコア算出サーバの機能構成の一例を示す図である。

[図3]本実施形態に係る異常パケット生成サーバの機能構成の一例を示す図である。

[図4]本実施形態に係る異常パケット評価サーバの機能構成の一例を示す図で

ある。

[図5]異常パケットの生成及び分類器の再学習処理の一例を示すフローチャートである。

[図6]コンピュータのハードウェア構成の一例を示す図である。

発明を実施するための形態

[0010] 以下、本発明の一実施形態について説明する。以下の実施形態では、未知の脆弱性に対しても効果的な異常パケットを効率的に生成し、更にその異常パケットを用いてパケットが正常又は異常のいずれであるかを分類する分類器を再学習する場合について説明する。

[0011] ＜全体構成例＞

本実施形態に係るシステムの全体構成例を図１に示す。図１に示すように、本実施形態に係るシステムには、メトリクス・ログ収集サーバ１０と、トラヒックキャプチャサーバ２０と、ＮＷ異常スコア算出サーバ３０と、異常パケット生成サーバ４０と、異常パケット評価サーバ５０と、ユーザ端末６０とが含まれる。

[0012] メトリクス・ログ収集サーバ１０は、ＩＳＰネットワーク７０内のネットワーク装置やサーバ等のメトリクスデータ（例えば、ＣＰＵ（Central Processing Unit）使用率、メモリ使用率、ネットワークワークロード等）とログデータとを収集する。以下、メトリクスデータとログデータとをまとめて「メトリクス・ログデータ」と呼ぶことにする。なお、メトリクス・ログ収集サーバ１０では、各時刻のメトリクス・ログデータが収集される。

[0013] トラヒックキャプチャサーバ２０は、ＩＳＰネットワーク７０内のトラヒック（パケット）を収集する。なお、トラヒックキャプチャサーバ２０では、各時刻のパケットが収集される。

[0014] ＮＷ異常スコア算出サーバ３０は、メトリクス・ログ収集サーバ１０からメトリクス・ログデータを取得し、その特徴量を表すベクトル形式のデータ（以下、特徴量ベクトルともいう。）からネットワーク異常スコアを算出する。ネットワーク異常スコアとは、ＩＳＰネットワーク７０の異常度合いを

表す指標値のことである。

[0015] 異常パケット生成サーバ４０は、ＮＷ異常スコア算出サーバ３０から取得したネットワーク異常スコアを用いてトラヒックキャプチャサーバ２０からパケットを取得し、それらのパケットから異常パケットを生成すると共に分類器を再学習する。

[0016] 異常パケット評価サーバ５０は、異常パケット生成サーバ４０から異常パケットを取得し、それらの異常パケットを用いて試験環境ネットワーク９０内のネットワーク装置でテストして当該異常パケットを評価する。

[0017] ユーザ端末６０は、ＩＳＰネットワーク７０を介してインターネット８０にパケットを送信する。なお、ユーザ端末６０としては、例えば、ＰＣ（パーソナルコンピュータ）、スマートフォン、タブレット端末、ウェアラブルデバイス、ゲーム機器等が挙げられる。

[0018] なお、図１に示すシステムの全体構成は一例であって、これに限られるものではない。例えば、メトリクス・ログ収集サーバ１０、トラヒックキャプチャサーバ２０、ＮＷ異常スコア算出サーバ３０、異常パケット生成サーバ４０、及び異常パケット評価サーバ５０のうちの２つ以上のサーバが同一のサーバで実現されていてもよい。

[0019] ＜機能構成例＞

以下、ＮＷ異常スコア算出サーバ３０、異常パケット生成サーバ４０、及び異常パケット評価サーバ５０の機能構成例について説明する。

[0020] ≪ＮＷ異常スコア算出サーバ３０≫

本実施形態に係るＮＷ異常スコア算出サーバ３０の機能構成例を図２に示す。図２に示すように、本実施形態に係るＮＷ異常スコア算出サーバ３０は、メトリクス・ログ取得部３０１と、ＮＷ異常スコア算出部３０２とを有する。これら各部は、例えば、ＮＷ異常スコア算出サーバ３０にインストールされた１以上のプログラムが、ＣＰＵ等のプロセッサに実行させる処理により実現される。

[0021] メトリクス・ログ取得部３０１は、メトリクス・ログ収集サーバ１０から

メトリクス・ログデータを取得する。例えば、メトリクス・ログ取得部３０１は、或る時間幅に含まれる各時刻のメトリクス・ログデータを取得する。以下、各時刻ｔ∈Ｔのメトリクス・ログデータが取得されるものとする。ここで、Ｔはメトリクス・ログデータの取得対象となる時間帯（日時幅であってもよい。）であり、ＮＷ異常スコア算出サーバ３０に与えられる。

[0022] ＮＷ異常スコア算出部３０２は、メトリクス・ログ取得部３０１によって取得されたメトリクス・ログデータから特徴量ベクトルを算出し、その特徴量ベクトルから学習済みの異常検知器によりネットワーク異常スコアを算出する。以下、時刻ｔのメトリクス・ログデータの特徴量ベクトルから算出されたネットワーク異常スコアをｓ（ｔ）とし、ネットワーク異常スコア集合｛ｓ（ｔ）｜ｔ∈Ｔ｝が得られたものとする。このネットワーク異常スコア集合｛ｓ（ｔ）｜ｔ∈Ｔ｝は異常パケット生成サーバ４０に送信される。

[0023] ここで、異常検知器とは、特徴量ベクトルを入力としてネットワーク異常スコアを算出及び出力する機械学習モデルである。異常検知器としては、例えば、自己符号化器（オートエンコーダ）等を用いることができる（参考文献１）。異常検知器として自己符号化器が用いられる場合、異常検知器は、正常時のメトリクス・ログデータの特徴量ベクトルを用いて教師なし学習手法により予め学習される。これにより、学習済みの異常検知器では、ネットワークの正常状態からの乖離度をネットワーク異常スコアとして算出することが可能となる。例えば、異常検知器に入力した特徴量ベクトルと、異常検知器から出力されたベクトルとの差を表す値をネットワーク異常スコアとして算出することができる。なお、メトリクス・ログデータから特徴量ベクトルを算出する方法については、既存の任意の特徴量抽出手法を用いればよい。

[0024] ≪異常パケット生成サーバ４０≫

本実施形態に係る異常パケット生成サーバ４０の機能構成例を図３に示す。図３に示すように、本実施形態に係る異常パケット生成サーバ４０は、パケット取得部４０１と、異常パケット候補生成部４０２と、異常パケットス

コア算出部４０３と、異常パケット選択部４０４と、再学習部４０５と、終了判定部４０６とを有する。これら各部は、例えば、異常パケット生成サーバ４０にインストールされた１以上のプログラムが、ＣＰＵ等のプロセッサに実行させる処理により実現される。

[0025] パケット取得部４０１は、ネットワーク異常スコア集合｛ｓ（ｔ）｜ｔ∈Ｔ｝に含まれるネットワーク異常スコアのうち、予め決められた閾値th_1を超えているネットワーク異常スコアの時刻ｔのパケットをトラヒックキャプチャサーバ２０から取得する。すなわち、パケット取得部４０１は、ｓ（ｔ）＞th_1を満たす時刻ｔ∈Ｔのパケットをトラヒックキャプチャサーバ２０から取得する。以下、パケット取得部４０１によって取得されたパケットの集合を｛p_1，・・・，p_n｝とする。ここで、ｎはパケット取得部４０１によって取得されたパケットの数である。

[0026] 異常パケット候補生成部４０２は、パケット取得部４０１によって取得されたパケットに対してデータ拡張技術を利用し、異常パケット候補を生成する。データ拡張技術としては、ノイズ追加若しくはパケット合成又はその両方を用いればよい。

[0027] ノイズ追加では、パケットにノイズを追加することにより異常パケット候補を生成する。ノイズとしては、例えば、パケットのヘッダ情報にランダムな変更を加えること等とすればよい。ノイズの強度や種類を変えることにより様々な異常パケットを生成することができる。例えば、ＴＴＬ（Time to live）フィールドを対象とする場合、ＴＴＬ値を増減させることにより異常パケット候補を作成する。

[0028] パケット合成では、２つ以上のパケットを組み合わせることにより異常パケット候補を生成する。例えば、複数のパケットからヘッダ情報を抽出し、異なるパケットのヘッダ情報を組み合わせることにより異常パケット候補を生成する。

[0029] 以下、異常パケット候補生成部４０２によって生成された異常パケット候補の集合を｛q_1，・・・，q_m｝とする。ここで、ｍは異常パケット候補の

数であり、$m \geqq n$（特に、$m > n$であることが好ましい。）である。

[0030] 異常パケットスコア算出部４０３は、異常パケット候補生成部４０２によって生成された異常パケット候補から学習済みの分類器により異常パケットスコアを算出する。以下、異常パケット候補q_i（$i = 1, \cdots, m$）から算出された異常パケットスコアをS_iとする。

[0031] ここで、分類器とは、パケットを入力としてそのパケットが異常であるかを表す確率を異常パケットスコアとして算出及び出力する機械学習モデルである。分類器としては、例えば、勾配ブースティング決定木（ＧＢＤＴ：Gradient Boosting Decision Trees）等を用いることができる。分類器は、正常又は異常のいずれかを表すラベルが付与されたパケットを用いて、そのラベルを教師データとして既知の教師あり学習手法により予め学習される。これにより、学習済みの分類器では、異常パケット候補q_iが異常である確率を異常パケットスコアS_iとして算出することが可能となる。以下、一例として、ラベルは、正常であるときは０、異常であるときは１を取るものとする。

[0032] 異常パケット選択部４０４は、異常パケットスコアS_iが予め決められた閾値th_2を超えている異常パケット候補q_iが異常パケット候補集合$\{q_1, \cdots, q_m\}$の中に存在するか否かを判定する。そして、異常パケット選択部４０４は、そのような異常パケット候補q_iが存在すると判定した場合、異常パケット候補集合$\{q_1, \cdots, q_m\}$の中から異常パケットスコアが高い上位Ｎ個の異常パケット候補を異常パケットとして選択する。Ｎは予め決められた１以上の整数である。以下、異常パケットの集合を$\{r_1, \cdots, r_N\}$とする。この異常パケット集合$\{r_1, \cdots, r_N\}$は異常パケット評価サーバ５０に送信される。

[0033] 再学習部４０５は、異常パケット評価サーバ５０から送信されたラベル付き異常パケットの集合$\{(r_1, L_1), \cdots, (r_N, L_N)\}$を用いて、分類器を再学習する。すなわち、再学習部４０５は、$i = 1, \cdots, N$に対して、異常パケットr_iを入力データ、ラベルL_iを教師データとして、既知の教師あり学習手法により分類器を再学習する。ここで、各ラベルL_iは、

異常パケットr_iが正常又は異常のいずれであるかを表し、正常であるときは０、異常であるときは１を取る。

[0034] 終了判定部４０６は、異常パケットの生成及び分類器の再学習を終了するか否かを判定する。

[0035] ≪異常パケット評価サーバ５０≫

本実施形態に係る異常パケット評価サーバ５０の機能構成例を図４に示す。図４に示すように、本実施形態に係る異常パケット評価サーバ５０は、評価部５０１と、ラベル付け部５０２とを有する。これら各部は、例えば、異常パケット評価サーバ５０にインストールされた１以上のプログラムが、ＣＰＵ等のプロセッサに実行させる処理により実現される。

[0036] 評価部５０１は、異常パケット生成サーバ４０から送信された異常パケット集合$\{r_1, \cdots, r_N\}$に含まれる各異常パケットr_iを試験環境ネットワーク９０内のネットワーク装置に送信し、そのネットワーク装置で異常が発生するか否かを評価する。

[0037] ラベル付け部５０２は、評価部５０１による評価結果（つまり、ネットワークで異常が発生したか否か）を用いて、各異常パケットr_iに対して、その異常パケットr_iをネットワーク装置に送信したときに当該ネットワーク装置で異常が発生したか否かを表すラベルL_iを付与する。これにより、ラベル付き異常パケット集合$\{(r_1, L_1), \cdots, (r_N, L_N)\}$が得られる。このラベル付き異常パケット集合$\{(r_1, L_1), \cdots, (r_N, L_N)\}$は異常パケット生成サーバ４０に送信される。なお、各ラベルL_iには、異常パケットr_iをネットワーク装置に送信したときに当該ネットワーク装置で異常が発生したときは１、そうでないときは０が与えられる。

[0038] ＜異常パケットの生成及び分類器の再学習処理＞

以下、異常パケットを生成し、分類器を再学習する処理について、図５を参照しながら説明する。なお、以下では、メトリクス・ログ収集サーバ１０によって少なくとも時間帯Ｔに含まれる各時刻ｔのメトリクス・ログデータが収集されていると共に、トラヒックキャプチャサーバ２０によって少なく

とも時間帯Ｔに含まれる各時刻ｔのパケットが収集されているものとする。

[0039] まず、ＮＷ異常スコア算出サーバ３０のメトリクス・ログ取得部３０１は、各時刻ｔ∈Ｔのメトリクス・ログデータをメトリクス・ログ収集サーバ１０から取得する（ステップＳ１０１）。

[0040] 次に、ＮＷ異常スコア算出サーバ３０のＮＷ異常スコア算出部３０２は、上記のステップＳ１０１で取得されたメトリクス・ログデータから特徴量ベクトルを算出し、その特徴量ベクトルから学習済みの異常検知器によりネットワーク異常スコアを算出する（ステップＳ１０２）。これにより、ネットワーク異常スコア集合｛ｓ（ｔ）｜ｔ∈Ｔ｝が得られる。

[0041] 次に、異常パケット生成サーバ４０のパケット取得部４０１は、ネットワーク異常スコア集合｛ｓ（ｔ）｜ｔ∈Ｔ｝に含まれるネットワーク異常スコアのうち、予め決められた閾値th_1を超えているネットワーク異常スコアの時刻ｔのパケットをトラヒックキャプチャサーバ２０から取得する（ステップＳ１０３）。これにより、$s(t) > th_1$を満たす時刻ｔ∈Ｔのパケットの集合$\{p_1, \cdots, p_n\}$が得られる。

[0042] 次に、異常パケット生成サーバ４０の異常パケット候補生成部４０２は、上記のステップＳ１０３で取得されたパケットの集合$\{p_1, \cdots, p_n\}$に対してデータ拡張技術を利用し、異常パケット候補を生成する（ステップＳ１０４）。これにより、異常パケット候補の集合$\{q_1, \cdots, q_m\}$が得られる。以下、異常パケット候補集合をＱで表し、$Q = \{q_1, \cdots, q_m\}$とする。

[0043] 次に、異常パケット生成サーバ４０の異常パケットスコア算出部４０３は、上記のステップＳ１０４で生成された異常パケット候補集合Ｑに含まれる各異常パケット候補q_iの異常パケットスコアS_iを学習済みの分類器により算出する（ステップＳ１０５）。

[0044] 次に、異常パケット生成サーバ４０の異常パケット選択部４０４は、異常パケットスコアS_iが予め決められた閾値th_2を超えている異常パケット候補q_iが異常パケット候補集合Ｑの中に存在するか否かを判定する（ステップ

Ｓ１０６）。すなわち、異常パケット選択部４０４は、$S_i > th_2$を満たす異常パケット候補q_iが異常パケット候補集合Ｑの中に存在するか否かを判定する。これは、異常パケットスコアS_iが高い異常パケット候補q_iが異常パケット候補集合Ｑの中に存在するか否かを判定していることを意味する。すべての異常パケット候補q_iの異常パケットスコアS_iが低い場合、すべての異常パケット候補q_iが正常なパケットであると考えられるためである。

[0045] 上記のステップＳ１０６で$S_i > th_2$を満たす異常パケット候補q_iが存在しないと判定された場合、異常パケット生成サーバ４０は、異常パケットの生成及び分類器の再学習処理を終了する。一方で、上記のステップＳ１０６で$S_i > th_2$を満たす異常パケット候補q_iが存在すると判定された場合、異常パケット生成サーバ４０の異常パケット選択部４０４は、異常パケット候補集合Ｑの中から異常パケットスコアが高い上位Ｎ個の異常パケット候補を異常パケットとして選択する（ステップＳ１０７）。これにより、異常パケット集合$\{r_1, \cdots, r_N\}$が得られる。

[0046] 次に、異常パケット評価サーバ５０の評価部５０１は、異常パケット集合$\{r_1, \cdots, r_N\}$に含まれる各異常パケットr_iを試験環境ネットワーク９０内のネットワーク装置に送信し、そのネットワーク装置で異常が発生するか否かを評価する（ステップＳ１０８）。なお、評価部５０１は、例えば、当該ネットワーク装置の状態を監視することにより、そのネットワーク装置で異常が発生したか否かを評価することが可能である。

[0047] 次に、異常パケット評価サーバ５０のラベル付け部５０２は、上記のステップＳ１０８における評価結果を用いて、各異常パケットr_iに対してラベルL_iを付与する（ステップＳ１０９）。これにより、ラベル付き異常パケット集合$\{(r_1, L_1), \cdots, (r_N, L_N)\}$が得られる。なお、ラベル付けは、上記のステップＳ１０８における評価結果を人に提示して人手で行われてもよいし、当該評価結果に基づいて自動的に行われてもよい。

[0048] なお、上記のステップＳ１０７～ステップＳ１０９では、異常パケットスコアが高い上位Ｎ件の異常パケット候補を異常パケットとして選択した上で

、実際に異常パケットをネットワーク装置に送信してその異常パケットを評価し、その評価から異常パケットのラベル付けを行っている。これは、能動学習（Ａｃｔｉｖｅ　Ｌｅａｒｎｉｎｇ）の枠組みを活用したものであり、分類器を再学習する際の学習効果が高い異常パケット候補のみを異常パケットとして選択してラベル付けを行っていることを意味する。これにより、高い学習効果を実現しつつラベル付けに要するコストを削減することが可能となる。

[0049] 次に、異常パケット生成サーバ４０の再学習部４０５は、ラベル付き異常パケット集合｛（r_1，L_1），・・・，（r_N，L_N）｝を用いて、既知の教師あり学習手法により分類器を再学習する（ステップＳ１１０）。これにより、より精度の良い分類器が得られることが期待できる。

[0050] 次に、異常パケット生成サーバ４０の終了判定部４０６は、異常パケットの生成及び分類器の再学習を終了するか否かを判定する（ステップＳ１１１）。ここで、終了判定部４０６は、例えば、現在の異常パケット候補集合Ｑの要素数がＮ個未満となった場合に終了すると判定してもよいし、ユーザ等から終了指示を受け付けた場合に終了すると判定してもよいし、その他の終了条件を満たした場合に終了すると判定してもよい。

[0051] 上記のステップＳ１１１で終了すると判定された場合、異常パケット生成サーバ４０は、異常パケットの生成及び分類器の再学習処理を終了する。一方で、上記のステップＳ１１１で終了すると判定されなかった場合、異常パケット生成サーバ４０の異常パケット選択部４０４は、現在の異常パケット候補集合Ｑの中から異常パケットr_1，・・・，r_Nを削除して（ステップＳ１１２）、ステップＳ１０６に戻る。これにより、新たな異常パケット候補集合Ｑ←Ｑ＼｛r_1，・・・，r_N｝を用いてステップＳ１０６～ステップＳ１１０が実行される。

[0052] ＜ハードウェア構成例＞

本実施形態に係るメトリクス・ログ収集サーバ１０、トラヒックキャプチャサーバ２０、ＮＷ異常スコア算出サーバ３０、異常パケット生成サーバ４

０、及び異常パケット評価サーバ５０、及びユーザ端末６０は、例えば、図６に示すコンピュータ９００のハードウェア構成により実現される。図６に示すコンピュータ９００は、入力装置９０１と、表示装置９０２と、外部Ｉ／Ｆ９０３と、通信Ｉ／Ｆ９０４と、ＲＡＭ（Random Access Memory）９０５と、ＲＯＭ（Read Only Memory）９０６と、補助記憶装置９０７と、プロセッサ９０８とを有する。これらの各ハードウェアは、それぞれがバス９０９を介して通信可能に接続される。

[0053] 入力装置９０１は、例えば、キーボード、マウス、タッチパネル、物理ボタン等である。表示装置９０２は、例えば、ディスプレイ、表示パネル等である。なお、コンピュータ９００は、例えば、入力装置９０１及び表示装置９０２のうちの少なくとも一方を有していなくてもよい。

[0054] 外部Ｉ／Ｆ９０３は、記録媒体９０３ａ等の外部装置とのインタフェースである。記録媒体９０３ａとしては、例えば、ＣＤ（Compact Disc）、ＤＶＤ（Digital Versatile Disk）、ＳＤメモリカード（Secure Digital memory card）、ＵＳＢ（Universal Serial Bus）メモリカード等が挙げられる。

[0055] 通信Ｉ／Ｆ９０４は、コンピュータ９００が他の装置等と通信を行うためのインタフェースである。ＲＡＭ９０５は、プログラムやデータを一時保持する揮発性の半導体メモリ（記憶装置）である。ＲＯＭ９０６は、電源を切ってもプログラムやデータを保持することができる不揮発性の半導体メモリ（記憶装置）である。補助記憶装置９０７は、例えば、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、フラッシュメモリ等の不揮発性の記憶装置である。プロセッサ９０８は、例えば、ＣＰＵやＧＰＧＰＵ（General Purpose computing with Graphic Processing Unit）等の各種演算装置である。

[0056] なお、図６に示すハードウェア構成は一例であって、コンピュータ９００のハードウェア構成はこれに限られるものではない。例えば、コンピュータ９００は、複数の補助記憶装置９０７や複数のプロセッサ９０８を有していてもよいし、図示したハードウェアの一部を有していなくてもよいし、図示

したハードウェア以外の種々のハードウェアを有していてもよい。

[0057] ＜まとめ＞

以上のように、本実施形態に係る異常パケット生成サーバ４０では、異常検知器によるネットワーク異常スコアを利用して対象のパケットを絞り込んだ上、データ拡張（ノイズ追加、パケット合成）によって異常パケット候補を生成する。また、本実施形態に係る異常パケット生成サーバ４０と異常パケット評価サーバ５０は、能動学習の枠組みを活用し、異常パケット候補のうち、分類器による異常パケットスコアが高いものを異常パケットとして選択した上で、それらの異常パケットを実際のネットワーク装置で評価してラベル付けする。

[0058] このように、対象となるパケットを絞り込んだ上でデータ拡張によって異常パケット候補を生成し、その中から異常パケットスコアにより異常パケットを選択するため、実際に異常を引き起こす可能性が高いパケットを従来手法によりも効率的に生成することができる。また、実際にユーザ端末６０の通信行動によって発生するパケットを利用してデータ拡張により異常パケットを生成するため、未知の脆弱性を引き起こすような異常パケットの生成が期待できる。更に、異常パケットを実際に評価する際には能動学習の枠組みを活用することにより、その評価回数を削減し、またラベル付けのコストも削減できるため、効果的かつ効率的に分類器を学習することもできるようになる。加えて、能動学習の枠組みを活用により、分類器が繰り返し再学習されるため、異常パケットの特徴が変化する状況に対しても適応的に分類器を再学習させることが可能となり、その結果、様々な状況下で異常パケット検出性能の向上が期待できる。

[0059] 本発明は、具体的に開示された上記の実施形態に限定されるものではなく、請求の範囲の記載から逸脱することなく、種々の変形や変更、既知の技術との組み合わせ等が可能である。

[0060] ［参考文献］

参考文献１：Tajiri, Kengo, et al. ”Dividing deep learning model for

continuous anomaly detection of inconsistent ict systems.” NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2020.

符号の説明

[0061]

１０	メトリクス・ログ収集サーバ
２０	トラヒックキャプチャサーバ
３０	ＮＷ異常スコア算出サーバ
４０	異常パケット生成サーバ
５０	異常パケット評価サーバ
６０	ユーザ端末
７０	ＩＳＰネットワーク
８０	インターネット
９０	試験環境ネットワーク
３０１	メトリクス・ログ取得部
３０２	ＮＷ異常スコア算出部
４０１	パケット取得部
４０２	異常パケット候補生成部
４０３	異常パケットスコア算出部
４０４	異常パケット選択部
４０５	再学習部
４０６	終了判定部
５０１	評価部
５０２	ラベル付け部
９００	コンピュータ
９０１	入力装置
９０２	表示装置
９０３	外部Ｉ／Ｆ
９０３ａ	記録媒体

９０４　　通信Ｉ／Ｆ

９０５　　ＲＡＭ

９０６　　ＲＯＭ

９０７　　補助記憶装置

９０８　　プロセッサ

９０９　　バス

請求の範囲

[請求項1] 学習済み異常検知器によって算出された第１の異常スコアが所定の第１の閾値を超えているメトリクス及びログデータと同一時刻のパケットを取得する取得部と、

前記パケットからデータ拡張により異常パケット候補を生成する生成部と、

前記異常パケット候補から学習済み分類器によって算出された第２の異常スコアが上位Ｎ件の異常パケット候補を異常パケットとして選択する選択部と、

を有する異常パケット生成装置。

[請求項2] 前記異常パケットと、前記異常パケットをネットワーク装置に送信したときに前記ネットワーク装置に異常が発生するか否かを評価することによって付与されたラベルとを用いて、教師あり学習の手法により前記分類器を再学習する再学習部を更に有する請求項１に記載の異常パケット生成装置。

[請求項3] 前記学習済み分類器は、正常又は異常のいずれかを表すラベルが付与されたパケットを用いて教師あり学習の手法により学習された勾配ブースティング決定木である、請求項２に記載の異常パケット生成装置。

[請求項4] 前記選択部は、

前記第２の異常スコアが所定の第２の閾値を超えている異常パケット候補が存在する場合、前記第２の異常スコアが上位Ｎ件の異常パケット候補を異常パケットとして選択する、請求項１乃至３の何れか一項に記載の異常パケット生成装置。

[請求項5] 前記生成部は、

前記データ拡張としてノイズ追加とパケット合成の少なくとも一方を用いて、前記パケットから前記異常パケット候補を生成する、請求項４に記載の異常パケット生成装置。

[請求項6] 学習済み異常検知器によって算出された第１の異常スコアが所定の第１の閾値を超えているメトリクス及びログデータと同一時刻のパケットを取得する取得手順と、

前記パケットからデータ拡張により異常パケット候補を生成する生成手順と、

前記異常パケット候補から学習済み分類器によって算出された第２の異常スコアが上位Ｎ件の異常パケット候補を異常パケットとして選択する選択手順と、

をコンピュータが実行する異常パケット生成方法。

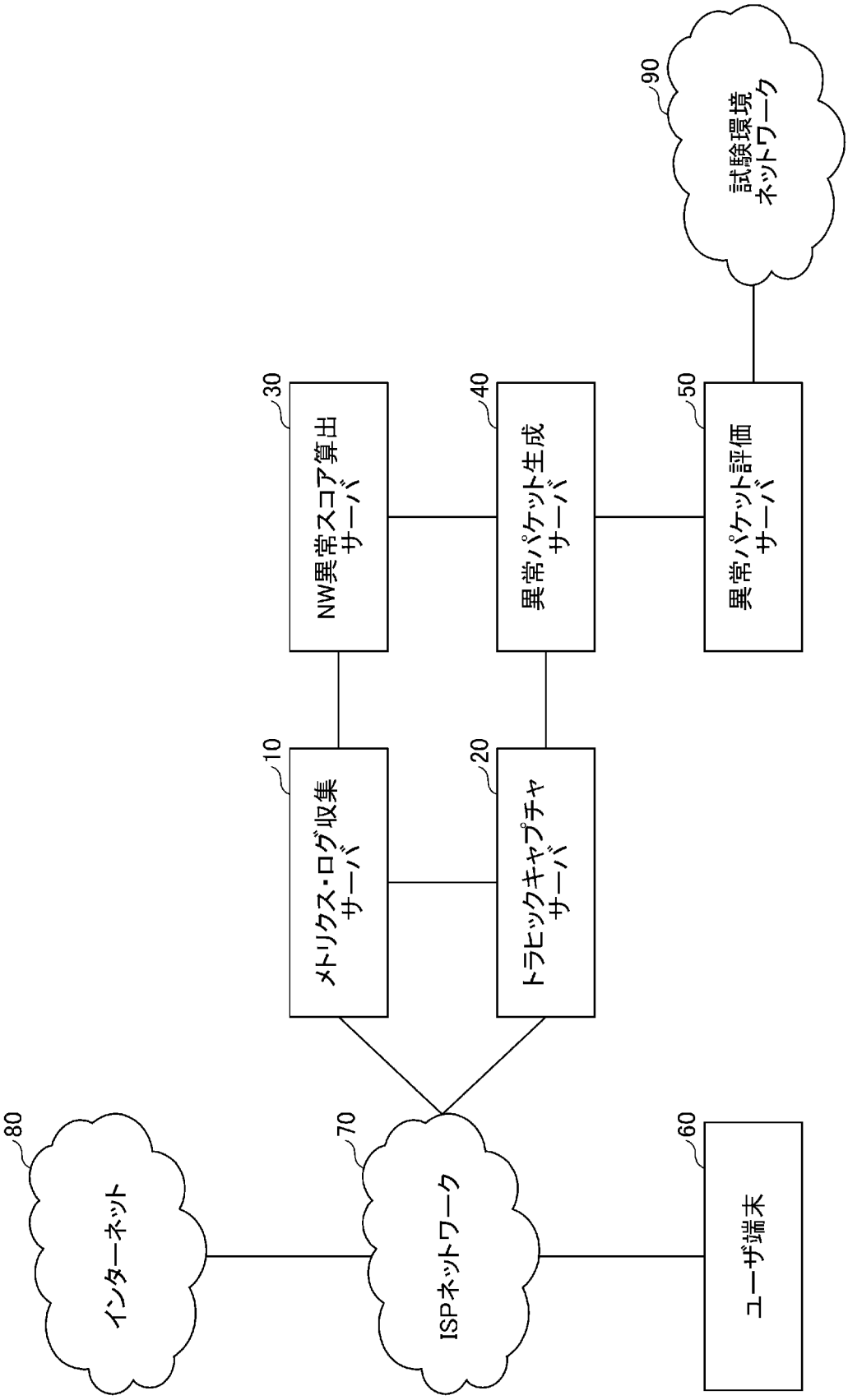
[請求項7] 学習済み異常検知器によって算出された第１の異常スコアが所定の第１の閾値を超えているメトリクス及びログデータと同一時刻のパケットを取得する取得手順と、

前記パケットからデータ拡張により異常パケット候補を生成する生成手順と、

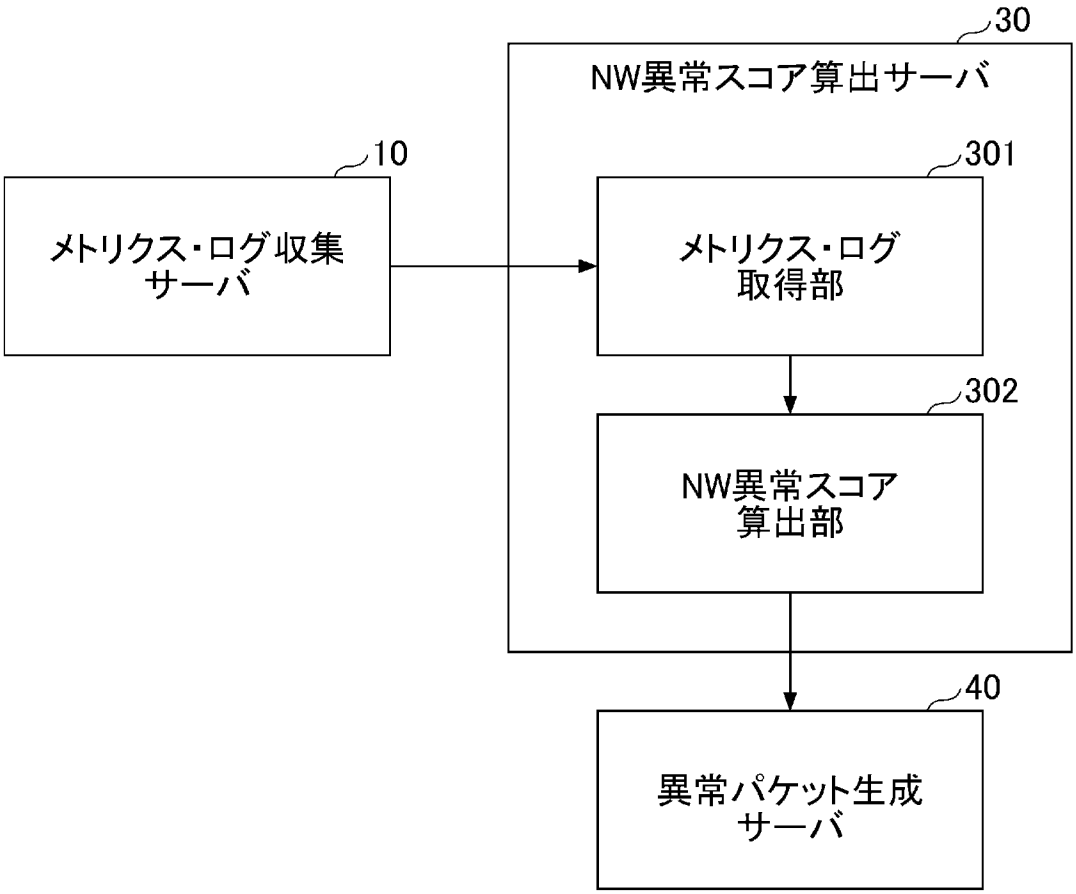
前記異常パケット候補から学習済み分類器によって算出された第２の異常スコアが上位Ｎ件の異常パケット候補を異常パケットとして選択する選択手順と、

をコンピュータに実行させるプログラム。

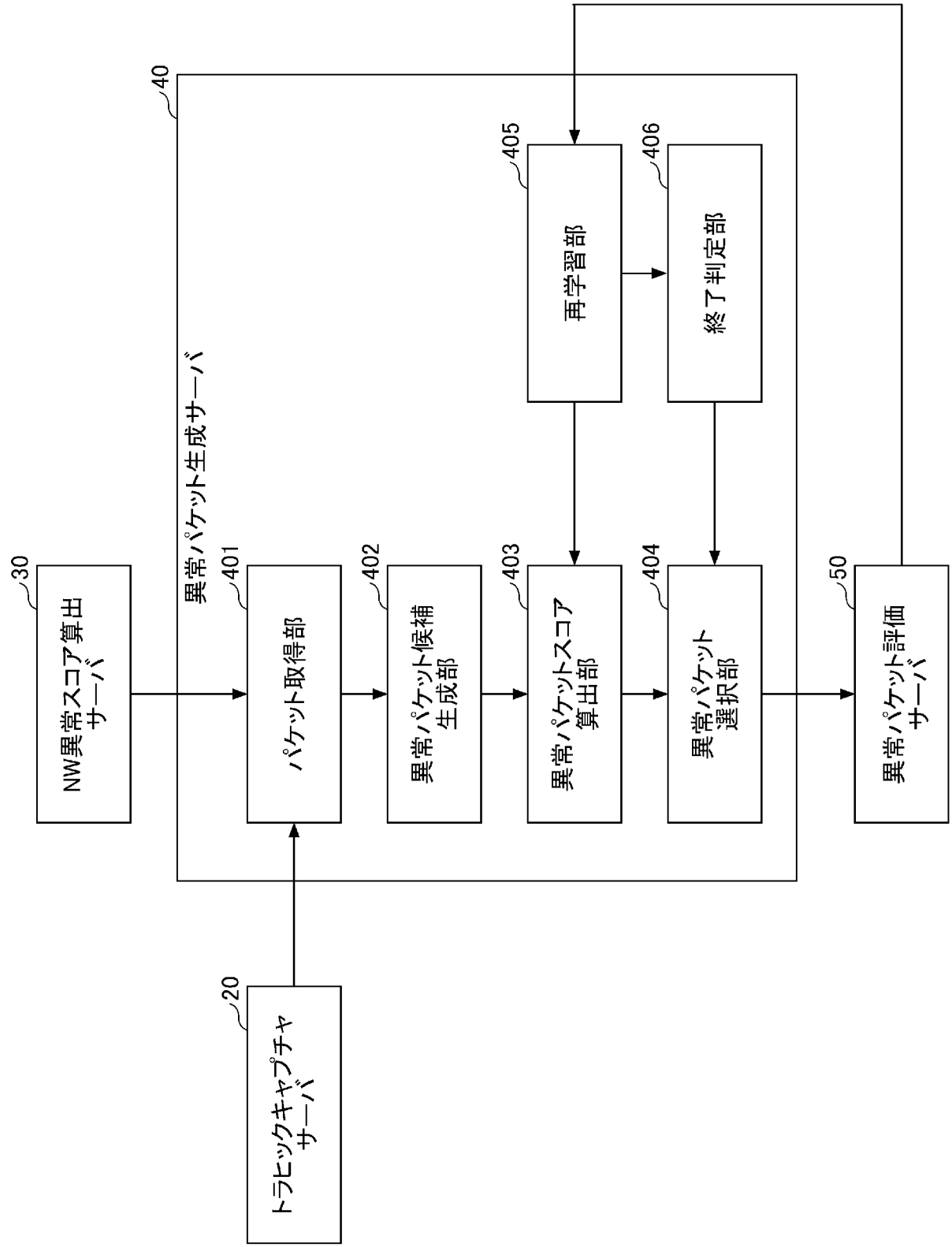
[図1]


90
試験環境
ネットワーク
30
NW異常スコア算出
サーバ
40
異常パケット生成
サーバ
50
異常パケット評価
サーバ
10
メトリクス・ログ収集
サーバ
20
トラヒックキャプチャ
サーバ
80
インターネット
70
ISPネットワーク
60
ユーザ端末

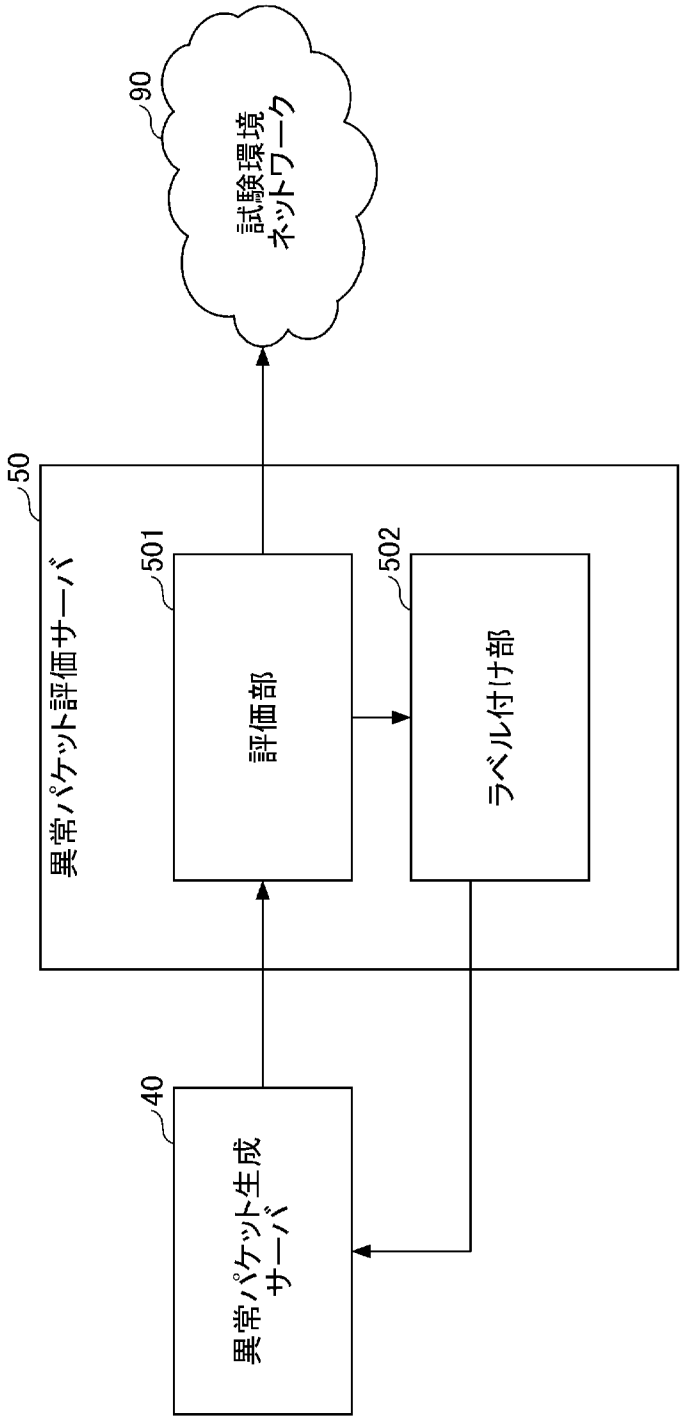
[図2]


30
NW異常スコア算出サーバ
10
メトリクス・ログ収集
サーバ
301
メトリクス・ログ
取得部
302
NW異常スコア
算出部
40
異常パケット生成
サーバ

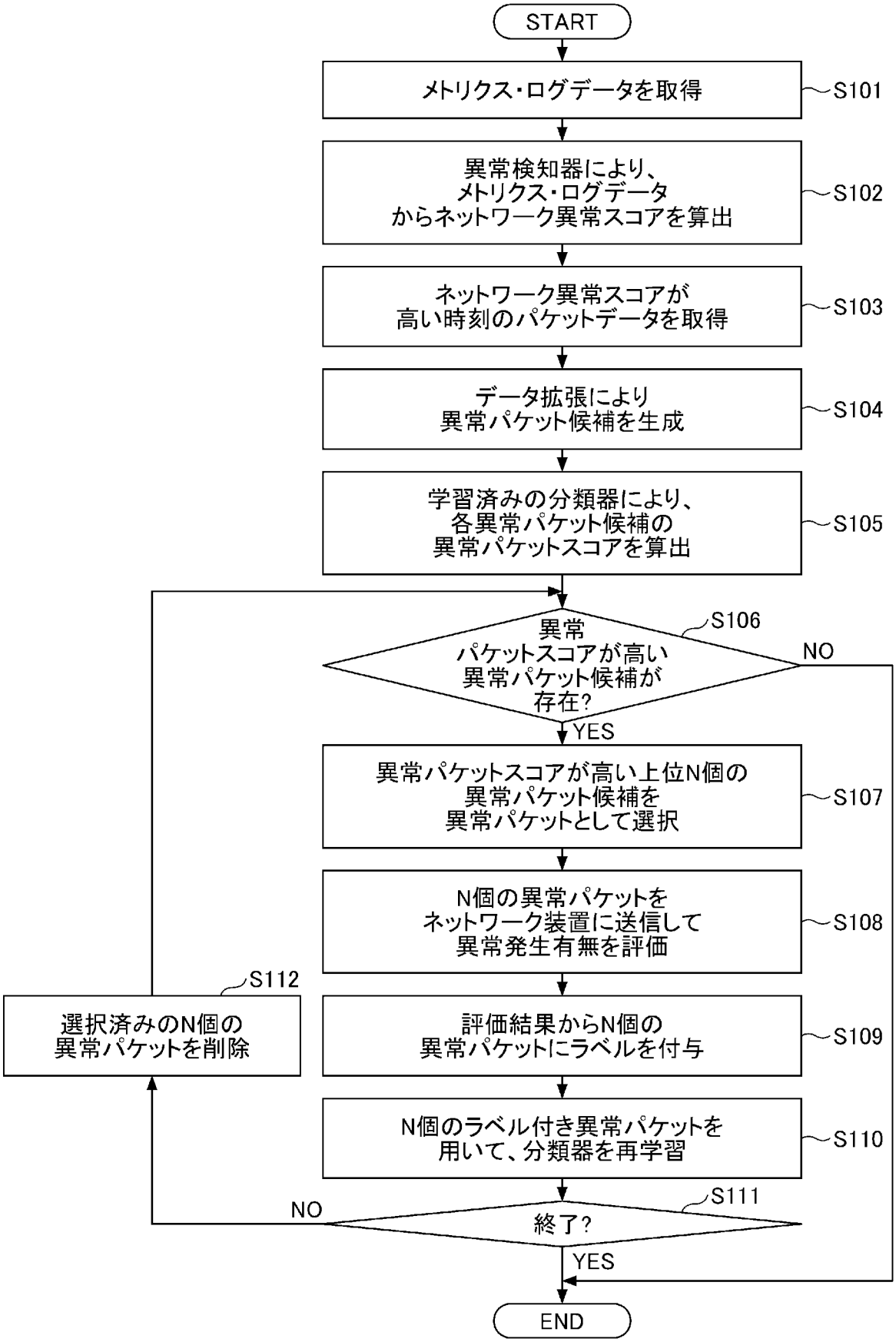
[図3]


40
異常パケット生成サーバ
405
再学習部
406
終了判定部
30
NW異常スコア算出
サーバ
401
パケット取得部
402
異常パケット候補
生成部
403
異常パケットスコア
算出部
404
異常パケット
選択部
50
異常パケット評価
サーバ
20
トラヒックキャプチャ
サーバ

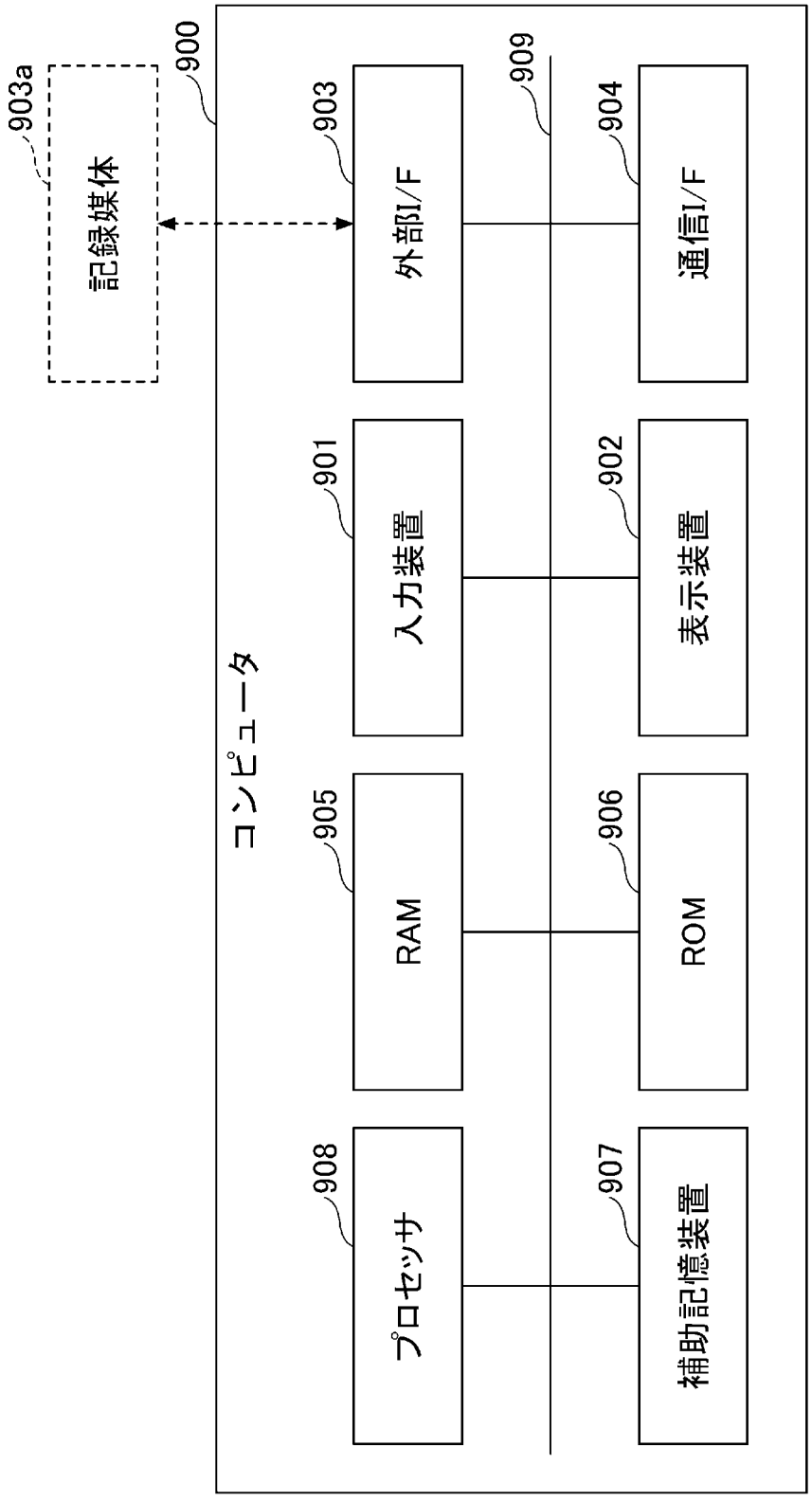
[図4]


90
試験環境
ネットワーク
50
異常パケット評価サーバ
501
評価部
502
ラベル付け部
40
異常パケット生成
サーバ

[図5]


START
メトリクス・ログデータを取得
S101
異常検知器により、
メトリクス・ログデータ
からネットワーク異常スコアを算出
S102
ネットワーク異常スコアが
高い時刻のパケットデータを取得
S103
データ拡張により
異常パケット候補を生成
S104
学習済みの分類器により、
各異常パケット候補の
異常パケットスコアを算出
S105
異常
パケットスコアが高い
異常パケット候補が
存在?
S106
NO
YES
異常パケットスコアが高い上位N個の
異常パケット候補を
異常パケットとして選択
S107
N個の異常パケットを
ネットワーク装置に送信して
異常発生有無を評価
S108
評価結果からN個の
異常パケットにラベルを付与
S109
N個のラベル付き異常パケットを
用いて、分類器を再学習
S110
終了?
S111
NO
YES
選択済みのN個の
異常パケットを削除
S112
END

[図6]


900
コンピュータ
903a
記録媒体
903
外部I/F
904
通信I/F
909
901
入力装置
902
表示装置
905
RAM
906
ROM
908
プロセッサ
907
補助記憶装置

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/020847

A. CLASSIFICATION OF SUBJECT MATTER

H04L 43/50(2022.01)i; ***G06F 11/22***(2006.01)i; ***G06F 11/263***(2006.01)i
FI: H04L43/50; G06F11/22 675H; G06F11/263

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)

H04L12/00-12/66;H04L41/00-101/695;G06F11/22-11/277

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 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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 2008-176706 A (YOKOGAWA ELECTRIC CORP.) 31 July 2008 (2008-07-31) paragraphs [0029]-[0030], [0033]	1-7
A	JP 2009-020673 A (SHARP KABUSHIKI KAISHA) 29 January 2009 (2009-01-29) paragraphs [0024]-[0025]	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	Date of mailing of the international search report
21 July 2023	**15 August 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/020847

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2008-176706 A	31 July 2008	US 2008/0174419 A1 paragraphs [0031]-[0032], [0035]	
JP 2009-020673 A	29 January 2009	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2023/020847

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 43/50(2022.01)i; G06F 11/22(2006.01)i; G06F 11/263(2006.01)i
FI: H04L43/50; G06F11/22 675H; G06F11/263

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））

H04L12/00-12/66;H04L41/00-101/695;G06F11/22-11/277

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	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３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 2008-176706 A (横河電機株式会社) 31.07.2008 (2008-07-31) [0029]-[0030],[0033]	1-7
A	JP 2009-020673 A (シャープ株式会社) 29.01.2009 (2009-01-29) [0024]-[0025]	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。

*　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
21.07.2023	15.08.2023

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）

小林　義晴 5X 2574

電話番号 03-3581-1101 内線 3556

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/JP2023/020847

引用文献	公表日	パテントファミリー文献	公表日
JP 2008-176706 A	31.07.2008	US 2008/0174419 A1 [0031]-[0032],[0035]	
JP 2009-020673 A	29.01.2009	（ファミリーなし）	