

(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8月27日(27.08.2020)



(10) 国際公開番号

WO 2020/170802 A1

(51) 国際特許分類:
H04L 12/70 (2013.01)

(21) 国際出願番号: PCT/JP2020/004102

(22) 国際出願日: 2020年2月4日(04.02.2020)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2019-027505 2019年2月19日(19.02.2019) JP

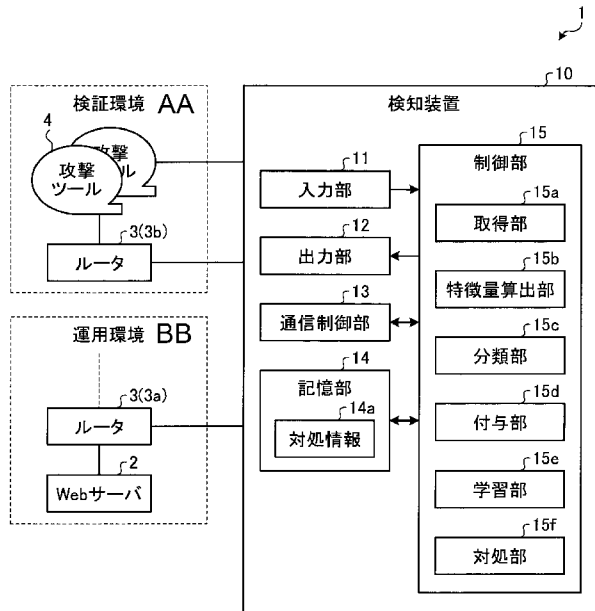
(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

(72) 発明者: 林 裕平 (HAYASHI, Yuhei); 〒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). 工藤 伊知郎 (KUDO, Ichiro); 〒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). 大澤 浩 (OSAWA, Hiroshi); 〒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). 西岡 孟朗 (NISHIOKA, Takeaki); 〒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

(54) Title: DETECTION DEVICE AND DETECTION METHOD

(54) 発明の名称: 検知装置および検知方法



2 Web server
3 Router
4 Attack tool
10 Detection device
11 Input unit
12 Output unit
13 Communication control unit
14 Storage unit
14a Handling information
15 Control unit
15a Acquisition unit
15b Feature quantity calculation unit
15c Classifying unit
15d Allocating unit
15e Learning unit
15f Handling unit
AA Verification environment
BB Operation environment

(57) Abstract: A feature quantity calculation unit (15b) calculates a feature quantity of header information of a packet. A classifying unit (15c) classifies the packet as being normal or abnormal, using the calculated feature quantity. An allocating unit (15d) allocates, to the header information of a packet that has been attacked using a known attack tool, a label indicating the tool name of the attack tool. A learning unit (15e) learns label allocation by using the label and the feature quantity calculated with respect to the labeled packet as teacher data.

関 3 丁 目 8 番 1 号 虎 の 門 三 井 ビ ル
ディング 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, 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：特徴量算出部（15 b）が、パケットのヘッダ情報の特徴量を算出する。分類部（15 c）が、算出された特徴量を用いてパケットを正常または異常のいずれかに分類する。付与部（15 d）が、既知の攻撃ツールを用いて攻撃されたパケットのヘッダ情報に、該攻撃ツールのツール名を示すラベルを付与する。学習部（15 e）が、ラベルと、ラベルが付与されたパケットについて算出された特徴量とを教師データとして用いて、ラベルの付与を学習する。

明 細 書

発明の名称： 検知装置および検知方法

技術分野

[0001] 本発明は、検知装置および検知方法に関する。

背景技術

[0002] 近年、HTTP Flood、Slow DoS (Denial Of Service) 等と呼ばれる、単位時間あたりのパケット数が少ない低レート攻撃の存在が知られている。また、このような低レート攻撃に対する対策技術が知られている。例えば、xFlowを用いて検知した攻撃通信をセキュリティ装置に引き込んで対策を行う技術が知られている（非特許文献1参照）。また、WAF (Web Application Firewall) 等のセキュリティ装置をインライン接続して攻撃通信を検知して対策する技術が知られている（非特許文献2参照）。また、Webサーバ上で攻撃を検知して対策を行う技術が知られている（非特許文献3，4参照）。また、特定の種別の攻撃を検知する技術が知られている（特許文献1，2参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開2017-147558号公報

特許文献2：特開2018-26747号公報

非特許文献

[0004] 非特許文献1：西塚要、“ISPにおけるDoS/DDoS攻撃の検知・対策技術”、[online]、2013年、NTTコミュニケーションズ株式会社、[2019年1月15日検索]、インターネット<URL:<https://www.nic.ad.jp/ja/materials/iw/2013/proceedings/s2/s2-nishizuka.pdf>>

非特許文献2：“Barracuda Web Application Firewall”、[online]、ITmedia Inc.、[2019年1月15日検索]、インターネット<URL:<http://www.keyman.or.jp/nwsec/waf/product/30973>>

非特許文献3：“Are you ready for slow reading?”、[online]、Qualys Inc.、[2019年1月15日検索]、インターネット<URL:<https://blog.qualys.com/securitylabs/2012/01/05/slow-read>>

非特許文献4：“ModSecurity 3.0”、[online]、Trustwave、[2019年1月15日検索]、インターネット<URL:<https://www.modsecurity.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、従来の技術では、低レート攻撃の検知が困難な場合がある。例えば、非特許文献1に記載の技術は、通信のサンプリングを前提とする技術であるため、低レート攻撃に関する情報を取得できず、セキュリティ装置への引き込みのトリガがないという問題がある。また、非特許文献2に記載の技術は、セキュリティ装置のGbps単価が高く、通常通信を検知の対象とするとコストが高くなるという問題がある。また、非特許文献3、4に記載の技術では、通常通信のQoSに影響があったりWebサーバへの負荷がかかったりするという問題がある。また、特許文献1、2に記載の技術では、検知できる攻撃の種別が限定され、攻撃に使われた攻撃ツールを判別できないという問題がある。

[0006] 本発明は、上記に鑑みてなされたものであって、低レート攻撃を容易に検知して対処可能とすることとする。

課題を解決するための手段

[0007] 上述した課題を解決し、目的を達成するために、本発明に係る検知装置は、パケットのヘッダ情報の特徴量を算出する特徴量算出部と、算出された前記特徴量を用いて前記パケットを正常または異常のいずれかに分類する分類部と、を備えることを特徴とする。

発明の効果

[0008] 本発明によれば、低レート攻撃を容易に検知して対処することが可能となる。

図面の簡単な説明

[0009] [図1]図 1 は、本実施形態に係る検知装置を含む検知システムの概要構成を例示する模式図である。

[図2]図 2 は、検知装置の処理概要を説明するための図である。

[図3]図 3 は、検知装置の処理を説明するための図である。

[図4]図 4 は、検知装置の処理を説明するための図である。

[図5]図 5 は、検知装置の処理を説明するための図である。

[図6]図 6 は、検知装置の処理を説明するための図である。

[図7]図 7 は、検知装置による検知処理手順を示すフローチャートである。

[図8]図 8 は、検知装置による検知処理手順を示すフローチャートである。

[図9]図 9 は、検知装置による検知処理手順を示すフローチャートである。

[図10]図 10 は、検知プログラムを実行す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

[0010] 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。

[0011] [検知システムの構成]

図 1 は、本実施形態に係る検知装置を含む検知システムの概略構成を例示する模式図である。図 1 に例示するように、検知システム 1 は、ルータ 3 と検知装置 10 とを含んで構成される。ルータ 3 は、例えば、NP (Network Processor) や FPG A (Field Programmable Gate Array) 等で実現され、運用環境のルータ 3 a と検証環境のルータ 3 b とを含む。運用環境のルータ 3 a は、運用中の Web サーバ 2 に接続し、Web サーバ 2 とユーザとの間でパケットを転送する転送装置である。検証環境のルータ 3 b は、既知の攻撃ツール 4 を用いて攻撃されたパケットを検知装置 10 に転送する転送装置である。

[0012] 検知装置 10 は、後述する検知処理により、運用環境のルータ 3 a および

検証環境のルータ 3 b から取得したパケットの L (Layer) 3 ~ L 4 情報を用いた学習により、運用環境での攻撃と、その攻撃に使用された攻撃ツール 4 とを検知する。

[0013] ここで、図 2 は、検知装置 1 0 の処理概要を説明するための図である。詳細は後述するが、検知装置 1 0 は、運用環境のパケットの 5 t u p l e と所定のフィールド値等の L 3 ~ L 4 情報を用いて特徴量を算出し、教師無 M L (Machine Learning、以下、学習と記す) を行って、パケットを正常または異常に分類する。

[0014] また、検知装置 1 0 は、検証環境の既知の攻撃ツール 4 で攻撃されたパケットの L 3 ~ L 4 情報を取得して、攻撃ツール 4 の攻撃種別とツール名とを示すラベルを付与し、これを教師データとして教師有学習を行って、ラベルの付与を学習する。

[0015] これにより、検知装置 1 0 は、運用環境のパケットのうち、異常として分類したパケットに攻撃種別とツール名とを示すラベルを付与する。また、検知装置 1 0 は、検知した攻撃の攻撃種別に応じた対処法を選択し、運用環境のルータ 3 a に通知する。例えば、検知装置 1 0 は、ルータ 3 a に対し、フィルタ設定や R S T (Reset) パケットの送付を指示したりする。

[0016] [検知装置の構成]

図 1 の説明に戻る。検知装置 1 0 は、パソコン等の汎用コンピュータで実現され、入力部 1 1、出力部 1 2、通信制御部 1 3、記憶部 1 4、および制御部 1 5 を備える。

[0017] 入力部 1 1 は、キーボードやマウス等の入力デバイスによって実現され、操作者による入力操作に対応して、制御部 1 5 に対して処理開始などの各種指示情報を入力する。出力部 1 2 は、液晶ディスプレイなどの表示装置、プリンター等の印刷装置等によって実現される。

[0018] 通信制御部 1 3 は、N I C (Network Interface Card) 等で実現され、L A N (Local Area Network) やインターネット等の電気通信回線を介した I o T ゲートウェイ 2 等の外部の装置と制御部 1 5 との通信を制御する。

[0019] 記憶部 14 は、R A M (Random Access Memory)、フラッシュメモリ (Flash Memory) 等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。記憶部 14 には、検知装置 10 を動作させる処理プログラムや、処理プログラムの実行中に使用されるデータなどが予め記憶され、あるいは処理の都度一時的に記憶される。例えば、記憶部 14 には、後述する検知処理においてルータ 3 から取得したパケットの L 3 ~ L 4 情報や、分類の閾値、学習結果のモデルのパラメータ、および対処情報 14 a 等が記憶される。なお、記憶部 14 は、通信制御部 13 を介して制御部 15 と通信する構成でもよい。

[0020] 制御部 15 は、C P U (Central Processing Unit) 等によって実現され、メモリに記憶された処理プログラムを実行する。これにより、制御部 15 は、図 1 に例示するように、取得部 15 a、特徴量算出部 15 b、分類部 15 c、付与部 15 d、学習部 15 e および対処部 15 f として機能する。なお、これらの機能部は、それぞれ、あるいは一部が異なるハードウェアに実装されてもよい。例えば、対処部 15 f は、他の機能部とは異なる装置に実装されてもよい。また、制御部 15 は、その他の機能部が含まれて構成されてもよい。

[0021] 取得部 15 a は、ルータ 3 からパケットのヘッダ情報を取得する。例えば、取得部 15 a は、ルータ 3 を経由するパケットの L 3 ~ L 4 情報を抽出する。

[0022] ここで、図 3 ~ 図 6 は、検知装置 10 の処理を説明するための図である。まず、図 3 には、取得部 15 a の処理が例示されている。図 3 に例示するように、取得部 15 a は、ルータ 3 を経由するパケットのプロトコルスタック (E t h e r、I P v 4、T C P およびペイロード) を検知装置 10 に内蔵するパーサにロードする。そして、取得部 15 a は、全パケットの 5 t u p l e の値と所定のヘッダフィールドの値とを抽出し、記憶部 14 の所定のテーブルにロードする。

[0023] なお、図 3 に例示するように、取得部 15 a は、ルータ 3 を経由するパケ

ットの 5 t u p l e の値と所定のヘッダフィールドの値とを、ルータ 3 からのパケット入力 (ingress) 時に抽出してもよいし、ルータ 3 へのパケット出力 (egress) 時に抽出してもよい。

[0024] ここで、5 t u p l e とは、送信元 I P アドレス (src_ip)、送信先 I P アドレス (dst_ip)、送信元ポート番号 (src_port)、送信先ポート番号 (dst_port)、プロトコル (protocol) である。また、所定のヘッダフィールドとは、ヘッダの着目するフィールドのことである。図 3 に示すヘッダフィールド k e y とは、ヘッダの着目するフィールドを特定するフィールド名等を意味する。図 3 に例示するように、着目するヘッダフィールドは 1 つに限定されず、複数であってもよい。

[0025] 特徴量算出部 1 5 b は、パケットのヘッダ情報の特徴量を算出する。具体的には、特徴量算出部 1 5 b は、5 t u p l e ごとのパケット数と所定のヘッダフィールドの値の分布とを用いて、5 t u p l e ごとの特徴量を算出する。また、分類部 1 5 c は、算出された特徴量を用いてパケットを正常または異常のいずれかに分類する。

[0026] ここで、図 4 には、特徴量算出部 1 5 b および分類部 1 5 c の処理が例示されている。図 4 に例示するように、まず、特徴量算出部 1 5 b は、運用環境のルータ 3 a から取得部 1 5 a が取得したパケットのヘッダ情報を用いて特徴量を算出する。

[0027] 具体的には、特徴量算出部 1 5 b は、5 t u p l e ごとに、パケット数をカウントし、ヘッダフィールドごとに値の分布を作成する。また、特徴量算出部 1 5 b は、所定時間ごとに、分布の平均値、分散、最大値あるいは最頻値等の代表値とパケット毎秒 (p p s) とを算出する。そして、特徴量算出部 1 5 b は、各 5 t u p l e の各ヘッダフィールドの代表値とパケット毎秒とを用いて、5 t u p l e ごとの特徴量を算出する。この特徴量は、例えばベクトル形式で表される。

[0028] なお、特徴量算出部 1 5 b は、特徴量を算出した後に、パケット数のカウンタと作成した分布とをクリアする。

- [0029] 分類部 15 c は、特徴量算出部 15 b が算出した 5 t u p l e ごとの特徴量を用いて教師無学習を行って、5 t u p l e ごとの特徴量から算出されるスコアを正常または異常のいずれかに分類する。例えば、分類部 15 c は、学習の結果、決定された分類の閾値を記憶部 14 に記憶させ、以後の処理における分類の閾値として用いる。
- [0030] 図 4 には、異常と分類された場合が「攻撃 5 t u p l e」として例示されている。分類部 15 c は、異常と分類したパケットのヘッダ情報を、出力部 12 あるいは通信制御部 13 を介して外部の管理装置等に出力して、異常を通知してもよい。
- [0031] 図 1 の説明に戻る。付与部 15 d は、既知の攻撃ツール 4 を用いて攻撃されたパケットのヘッダ情報に、該攻撃ツールのツール名を示すラベルを付与する。また、学習部 15 e は、ラベルと、このラベルが付与されたパケットについて算出された特徴量とを教師データとして用いて、ラベルの付与を学習する。
- [0032] ここで、図 5 には、付与部 15 d、特徴量算出部 15 b および学習部 15 e の処理が例示されている。図 5 に例示するように、まず、付与部 15 d は、検証環境のルータ 3 b から取得部 15 a が取得した、既知の攻撃ツール 4 を用いて攻撃されたパケットのヘッダ情報に、攻撃ツール 4 の攻撃種別とツール名とを示すラベルを付与する。
- [0033] なお、付与部 15 d が付与するラベルは、必ずしも攻撃種別、ツール名の双方でなくてもよく、いずれか一方でもよい。例えば、攻撃ツール 4 のツール名から攻撃種別を一意に特定できる場合には、付与部 15 d は、ツール名を示すラベルのみを付与してもよい。
- [0034] また、特徴量算出部 15 b は、学習時の処理として、このラベルが付与されたパケットのヘッダ情報を用いて特徴量を算出する。具体的には、特徴量算出部 15 b は、パケット数をカウントし、ヘッダフィールドごとに値の分布を作成し、所定時間ごとに、代表値とパケット毎秒 (p p s) とを算出する。そして、特徴量算出部 15 b は、各ヘッダフィールドの代表値とパケッ

ト毎秒とを用いて、このラベルが付与されたパケットの特徴量を算出する。

[0035] そして、学習部 15 e は、ラベルと、このラベルが付与されたパケットのヘッダ情報から算出された特徴量とを教師データとして教師有学習を行って、パケットのヘッダ情報へのラベルの付与を学習する。例えば、学習部 15 e は、パケットのヘッダ情報を用いて算出される特徴量とラベルとの関係を示すモデルのパラメータを決定し、記憶部 14 に記憶させる。

[0036] なお、図 5 には、特徴量算出部 15 b の推測時の処理として、分類部 15 c によって異常と分類されたパケットのヘッダ情報を用いて特徴量を算出する処理が例示されている。この場合に、特徴量算出部 15 b は、図 4 に示した例と同様に、5 t u p l e ごとに、パケット数をカウントし、ヘッダフィールドごとに値の分布を作成し、所定時間ごとに、分布の代表値とパケット毎秒 (p p s) とを算出する。そして、特徴量算出部 15 b は、各攻撃 5 t u p l e の各ヘッダフィールドの代表値とパケット毎秒とを用いて、攻撃 5 t u p l e ごとの特徴量を算出する。なお、図 5 に示す例は、図 4 に示した例とは、処理対象のパケットの 5 t u p l e が攻撃 5 t u p l e であることのみが異なっている。

[0037] 図 1 の説明に戻る。対処部 15 f は、分類部 15 c によって異常と分類され、学習された学習部 15 e によってラベルが付与されたパケットに対し、記憶部 14 の対処情報 14 a を参照し、該ラベルに対応する攻撃種別の対処法を選択する。対処情報 14 a は、攻撃ツールの攻撃種別と対処法とを対応付けした情報である。

[0038] ここで、図 6 には、運用環境のパケットに対する処理が例示されている。運用環境において、まず、特徴量算出部 15 b は、取得部 15 a が運用環境のルータ 3 a から取得したパケットのヘッダ情報を用いて特徴量を算出する。なお、図 6 には、図 4 に示した処理と図 5 に示した推測時の処理とが区別されずに同一の処理として例示されている。

[0039] 次に、分類部 15 c が、特徴量算出部 15 b が算出した 5 t u p l e ごとの特徴量を用いて、5 t u p l e ごとの特徴量から算出されるスコアを正常

または異常のいずれかに分類する。また、異常と分類されたパケットのヘッダ情報に対し、図5に例示したようにして学習された学習部15eが、攻撃ツール4の攻撃種別とツール名とを示すラベルを付与する。この場合に、学習部15eは、例えば、記憶部14に記憶されているパラメータを適用したモデルを用いて、異常と分類されたパケットのヘッダ情報にラベルを付与する。

[0040] そして、攻撃ツール4の攻撃種別とツール名とを示すラベルが付与されたパケットについて、対処部15fが、対処情報14aを参照し、ラベルに対応する攻撃種別の対処法を選択する。図6に例示するように、対処情報14aは、「http_get_flooding」、「slow_dos」等の攻撃種別と、「フィルタ設定」、「RSTパケット送付」等の対処法とが対応付けされた情報である。

[0041] 対処部15fは、例えば、ラベルが示す攻撃ツール4の攻撃種別が「http_get_flooding」である場合に、対処法として「フィルタ設定」を選択する。そして、対処部15fは、選択した対処法をルータ3aに通知する。これにより、運用環境のルータ3aは、検知された攻撃に対する適切な対処を実施することが可能となる。

[0042] [検知処理]

図7～図9は、検知装置10による検知処理手順を示すフローチャートである。まず、図7には、運用環境における分類処理手順が例示されている。図7のフローチャートは、例えば、ユーザが開始を指示する操作入力を行ったタイミングで開始される。

[0043] まず、取得部15aが、運用環境のルータ3aからパケットのヘッダ情報を取得する（ステップS1）。例えば、取得部15aは、ルータ3aを経由するパケットのL3～L4情報を抽出する。

[0044] 次に、特徴量算出部15bが、パケットのヘッダ情報の特徴量を算出する（ステップS2）。具体的には、特徴量算出部15bは、5tupleごとのパケット数と所定のヘッダフィールドの値の分布とを用いて、5tupleごとの特徴量を算出する。

- [0045] 次に、分類部 15 c が、算出された特徴量を用いてパケットを正常または異常のいずれかに分類する（ステップ S 3）。具体的には、分類部 15 c は、特徴量算出部 15 b が算出した 5 t u p l e ごとの特徴量から算出されるスコアを正常または異常のいずれかに分類する。分類部 15 c は、例えば、学習の際に分類の閾値を決定し、以後の処理における分類の閾値として用いる。
- [0046] 分類部 15 c は、異常と分類したパケットのヘッダ情報を、出力部 12 あるいは通信制御部 13 を介して外部の管理装置等に出力して異常を通知してもよい。これにより一連の処理が終了する。
- [0047] 次に、図 8 には、ラベル付与の学習処理手順が例示されている。図 8 のフローチャートは、例えば、ユーザが開始を指示する操作入力を行ったタイミングで開始される。
- [0048] まず、取得部 15 a が、検証環境のルータ 3 b から既知の攻撃ツール 4 を用いて攻撃されたパケットのヘッダ情報を取得する（ステップ S 11）。例えば、取得部 15 a は、ルータ 3 b から転送されたパケットの L 3 ~ L 4 情報を抽出する。
- [0049] 次に、付与部 15 d が、攻撃されたパケットのヘッダ情報に、攻撃ツール 4 のツール名を示すラベルを付与する（ステップ S 12）。
- [0050] また、特徴量算出部 15 b が、ラベルが付与されたパケットのヘッダ情報を用いて特徴量を算出する。そして、学習部 15 e が、ラベルとラベルが付与されたパケットについて算出された特徴量とを教師データとして用いて、ラベルの付与を学習する（ステップ S 13）。学習部 15 e は、例えば、パケットのヘッダ情報を用いて算出される特徴量とラベルとの関係を示すモデルのパラメータを決定し、記憶部 14 に記憶させる。これにより、一連の処理が終了する。
- [0051] 次に、図 9 には、運用環境のパケットに対する処理手順が例示されている。図 9 のフローチャートは、例えば、ユーザが開始を指示する操作入力を行ったタイミングで開始される。

- [0052] まず、取得部15aが、運用環境のルータ3aからパケットのヘッダ情報を取得する（ステップS21）。例えば、取得部15aは、ルータ3aを経由するパケットのL3～L4情報を抽出する。
- [0053] 次に、特徴量算出部15bが、パケットのヘッダ情報の特徴量を算出する（ステップS22）。具体的には、特徴量算出部15bは、5tupleごとのパケット数と所定のヘッダフィールドの値の分布とを用いて、5tupleごとの特徴量を算出する。
- [0054] 次に、分類部15cが、算出された特徴量を用いてパケットを正常または異常のいずれかに分類する（ステップS23）。具体的には、分類部15cは、特徴量算出部15bが算出した5tupleごとの特徴量から算出されるスコアを正常または異常のいずれかに分類する。
- [0055] 次に、学習された学習部15eが、異常と分類されたパケットのヘッダ情報に対し、攻撃ツール4の攻撃種別とツール名とを示すラベルを付与する（ステップS24）。この場合に、学習部15eは、例えば、記憶部14に記憶したパラメータを適用したモデルを用いて、異常と分類されたパケットのヘッダ情報にラベルを付与する。
- [0056] そして、対処部15fが、対処情報14aを参照し、ラベルに対応する攻撃種別の対処法を選択する（ステップS25）。また、対処部15fは、選択した対処法をルータ3aに出力する。これにより、一連の処理が終了し、運用環境のルータ3aは、検知された攻撃に対する適切な対処を実施することが可能となる。
- [0057] 以上、説明したように、本実施形態の検知装置10において、特徴量算出部15bが、パケットのヘッダ情報の特徴量を算出する。具体的には、特徴量算出部15bは、5tupleごとのパケット数と所定のヘッダフィールドの値の分布とを用いて特徴量を算出する。また、分類部15cが、算出された特徴量を用いてパケットを正常または異常のいずれかに分類する。
- [0058] これにより、パケットのサンプリングもWebサーバ2側で処理も要することなく、容易かつ安価に低レート攻撃を検知することが可能となる。この

ように、検知装置 10 によれば、低レート攻撃を容易に検知して対処することが可能となる。

[0059] また、付与部 15 d が、既知の攻撃ツールを用いて攻撃されたパケットのヘッダ情報に、該攻撃ツールのツール名を示すラベルを付与する。また、学習部 15 e が、ラベルと、ラベルが付与されたパケットについて算出された特徴量とを教師データとして用いて、ラベルの付与を学習する。これにより、多様な攻撃を検知して、攻撃ツールを推測することが可能となる。したがって、運用環境のルータ 3 a が適切な対処を行って攻撃通信を遮断することが可能となる。

[0060] また、記憶部 14 が、攻撃ツールの攻撃種別と対処法とを対応付けした対処情報 14 a を記憶する。また、対処部 15 f が、分類部 15 c によって異常と分類され、学習された学習部 15 e によってラベルが付与されたパケットに対し、記憶部 14 を参照し、該ラベルに対応する攻撃種別の対処法を選択する。これにより、運用環境のルータ 3 a が容易に適切な対処を実行することが可能となる。

[0061] [プログラム]

上記実施形態に係る検知装置 10 が実行する処理をコンピュータが実行可能な言語で記述したプログラムを検知することもできる。一実施形態として、検知装置 10 は、パッケージソフトウェアやオンラインソフトウェアとして上記の検知処理を実行する検知プログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記の検知プログラムを情報処理装置に実行させることにより、情報処理装置を検知装置 10 として機能させることができる。ここで言う情報処理装置には、デスクトップ型またはノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはスマートフォン、携帯電話機や PHS (Personal Handyphone System) などの移動体通信端末、さらには、PDA (Personal Digital Assistant) などのスレート端末などがその範疇に含まれる。また、検知装置 10 の機能を、クラウドサーバに実装してもよい。

[0062] 図10は、検知プログラムを実行す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と、CPU1020と、ハードディスクドライブインタフェース1030と、ディスクドライブインタフェース1040と、シリアルポートインタフェース1050と、ビデオアダプタ1060と、ネットワークインタフェース1070とを有する。これらの各部は、バス1080によって接続される。

[0063] メモリ1010は、ROM (Read Only Memory) 1011およびRAM 1012を含む。ROM 1011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1031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1041に接続される。ディスクドライブ1041には、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挿入される。シリアルポートインタフェース1050には、例えば、マウス1051およびキーボード1052が接続される。ビデオアダプタ1060には、例えば、ディスプレイ1061が接続される。

[0064] ここで、ハードディスクドライブ1031は、例えば、OS 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およびプログラムデータ1094を記憶する。上記実施形態で説明した各情報は、例えばハードディスクドライブ1031やメモリ1010に記憶される。

[0065] また、検知プログラムは、例えば、コンピュータ1000によって実行される指令が記述されたプログラムモジュール1093として、ハードディスクドライブ1031に記憶される。具体的には、上記実施形態で説明した検知装置10が実行する各処理が記述されたプログラムモジュール1093が、ハードディスクドライブ1031に記憶される。

[0066] また、検知プログラムによる情報処理に用いられるデータは、プログラムデータ1094として、例えば、ハードディスクドライブ1031に記憶される。そして、CPU1020が、ハードディスクドライブ1031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、上述した各手順を実行する。

[0067] なお、検知プログラムに係る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1031に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ1041等を介してCPU1020によって読み出されてもよい。あるいは、検知プログラムに係るプログラムモジュール1093やプログラムデータ1094は、LANやWAN (Wide Area Network) 等のネットワークを介して接続された他のコンピュータに記憶され、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。

[0068] 以上、本発明者によってなされた発明を適用した実施形態について説明したが、本実施形態による本発明の開示の一部をなす記述および図面により本発明は限定されることはない。すなわち、本実施形態に基づいて当業者等によりなされる他の実施形態、実施例およ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

- [0069]
- 1 検知システム
 - 2 Webサーバ
 - 3、3a、3b ルータ
 - 10 検知装置
 - 11 入力部
 - 12 出力部
 - 13 通信制御部
 - 14 記憶部
 - 14a 対処情報
 - 15 制御部
 - 15a 取得部
 - 15b 特徴量算出部

1 5 c 分類部

1 5 d 付与部

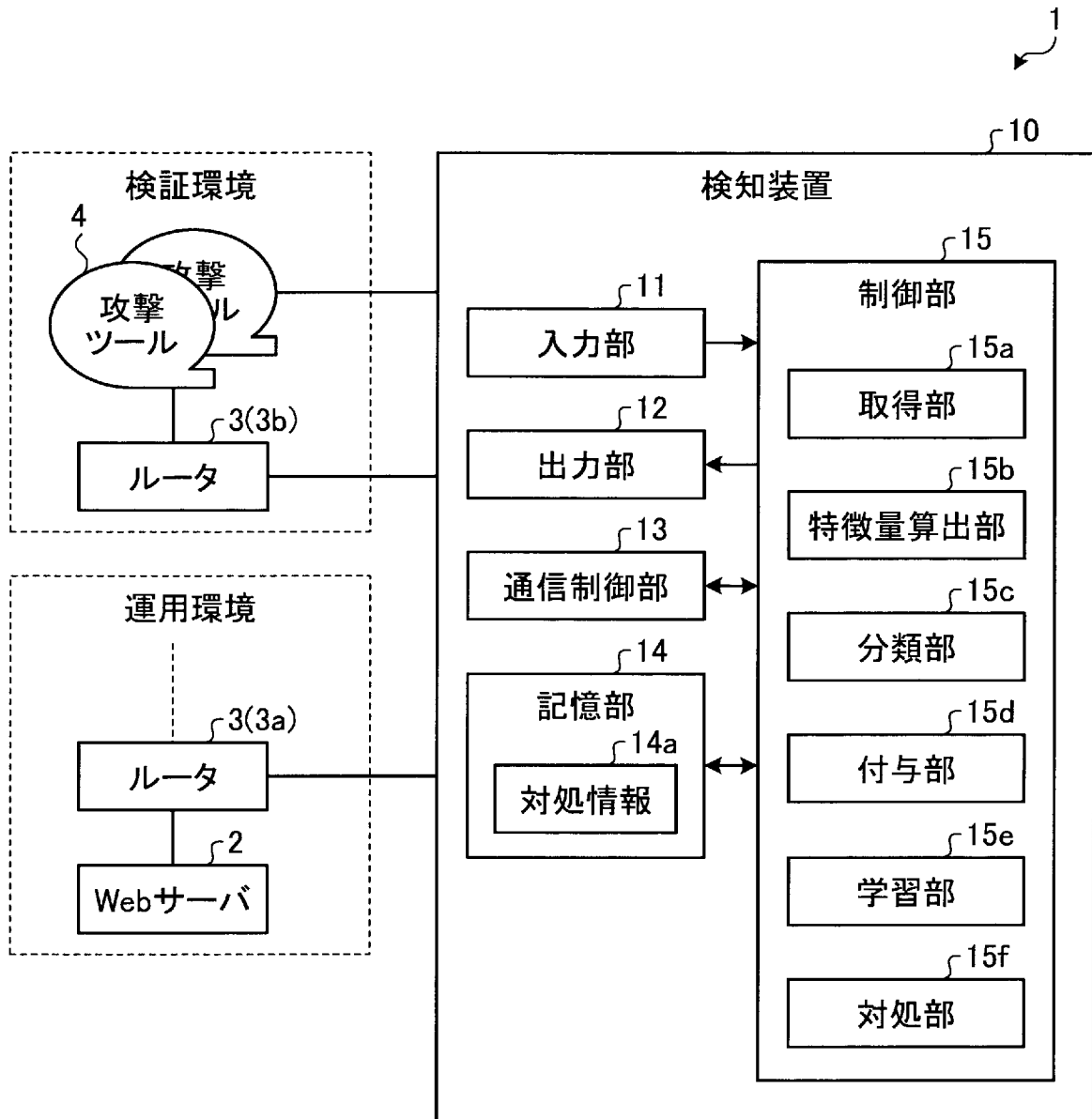
1 5 e 学習部

1 5 f 対処部

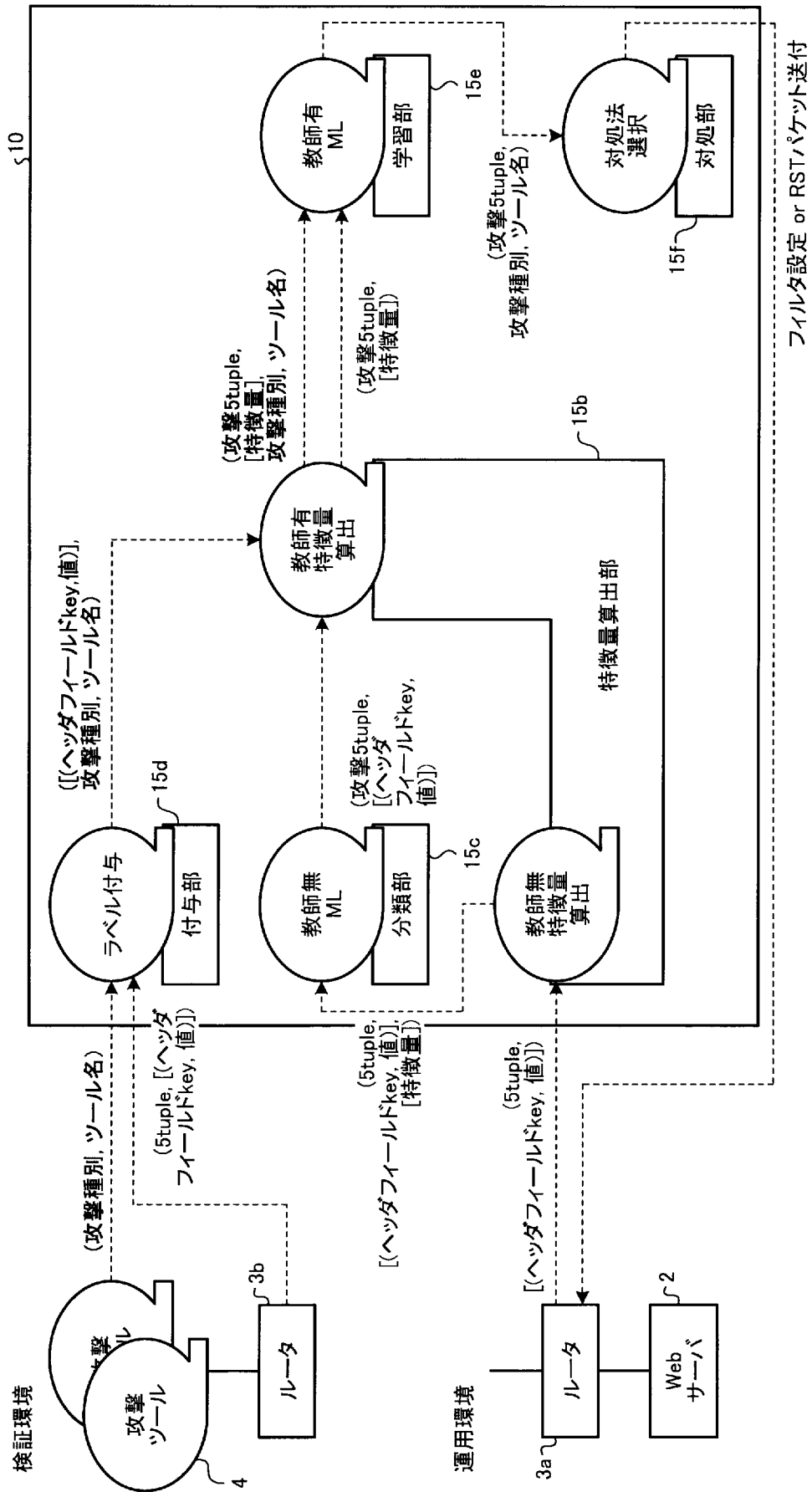
請求の範囲

- [請求項1] パケットのヘッダ情報の特徴量を算出する特徴量算出部と、
算出された前記特徴量を用いて前記パケットを正常または異常のいずれかに分類する分類部と、
を備えることを特徴とする検知装置。
- [請求項2] 前記特徴量算出部は、5 t u p l e ごとのパケット数と所定のヘッダフィールドの値の分布とを用いて特徴量を算出することを特徴とする請求項1に記載の検知装置。
- [請求項3] 既知の攻撃ツールを用いて攻撃されたパケットのヘッダ情報に、該攻撃ツールのツール名を示すラベルを付与する付与部と、
前記ラベルと、該ラベルが付与されたパケットについて算出された前記特徴量とを教師データとして用いて、前記ラベルの付与を学習する学習部と、
をさらに備えることを特徴とする請求項1に記載の検知装置。
- [請求項4] 前記攻撃ツールの攻撃種別と対処法とを対応付けした対処情報を記憶する記憶部と、
前記分類部によって異常と分類され、学習された前記学習部によって前記ラベルが付与されたパケットに対し、前記記憶部を参照し、該ラベルに対応する攻撃種別の対処法を選択する対処部と、
をさらに備えることを特徴とする請求項3に記載の検知装置。
- [請求項5] 検知装置で実行される検知方法であって、
パケットのヘッダ情報の特徴量を算出する特徴量算出工程と、
算出された前記特徴量を用いて前記パケットを正常または異常のいずれかに分類する分類工程と、
を含んだことを特徴とする検知方法。

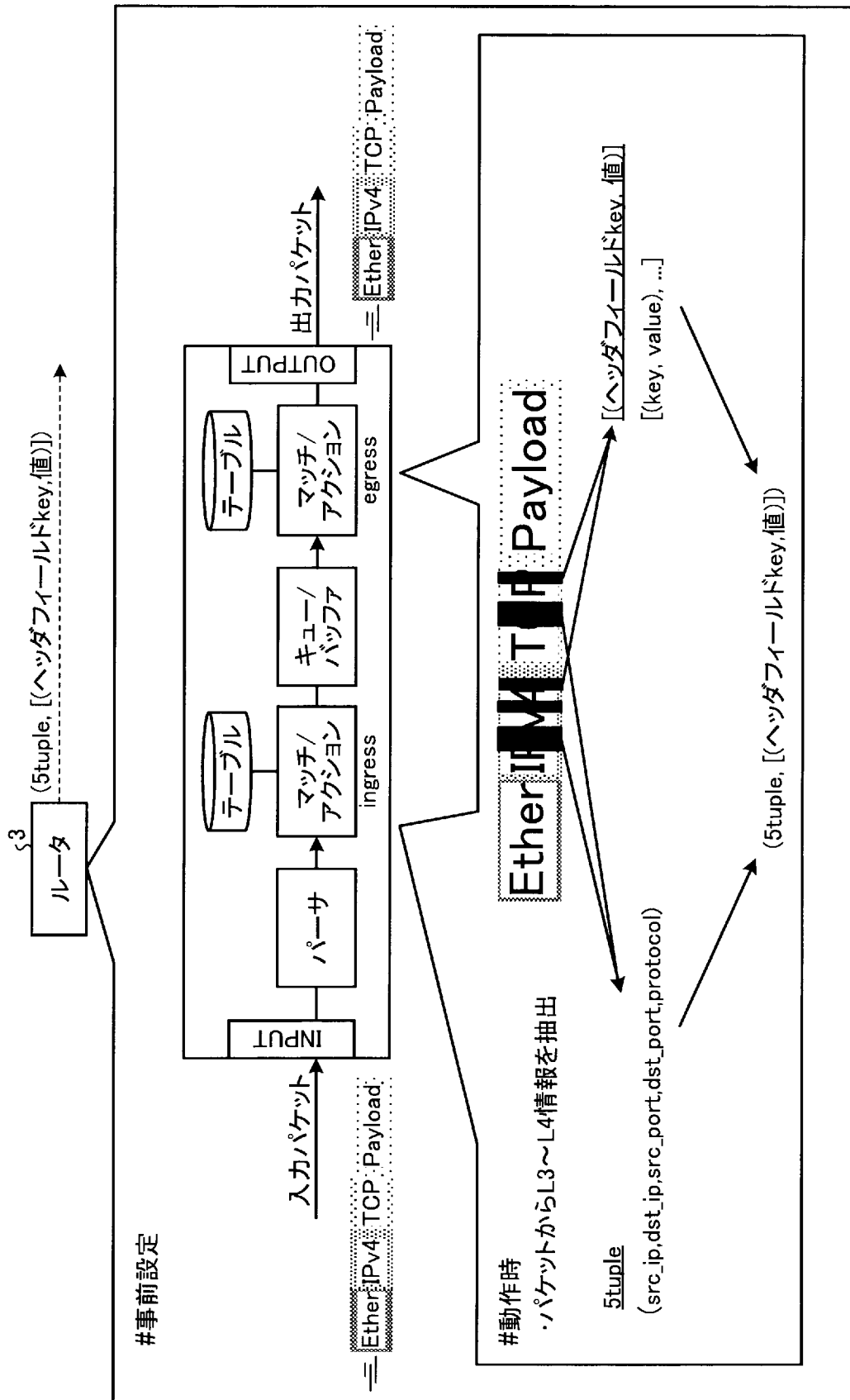
[図1]



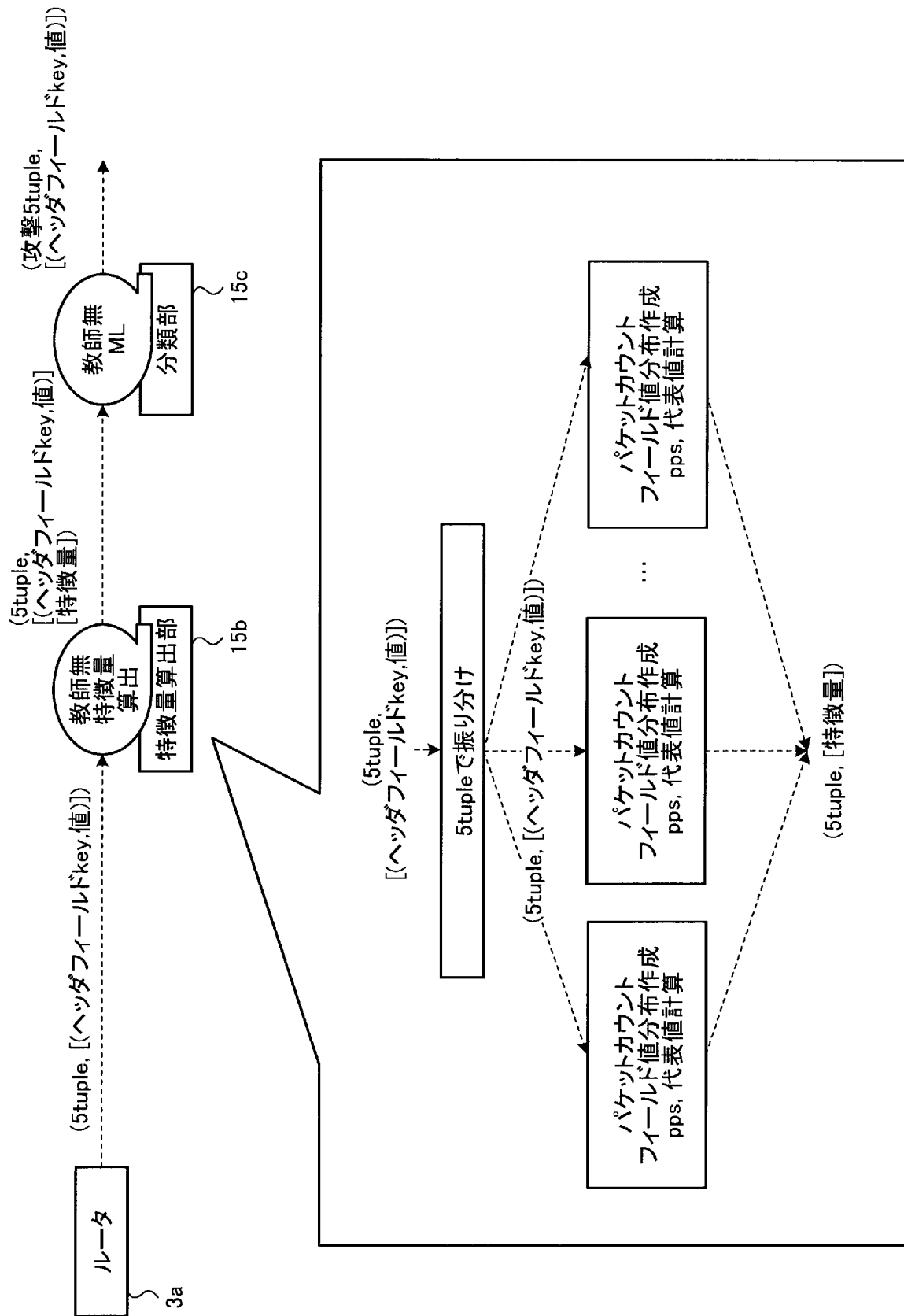
[図2]



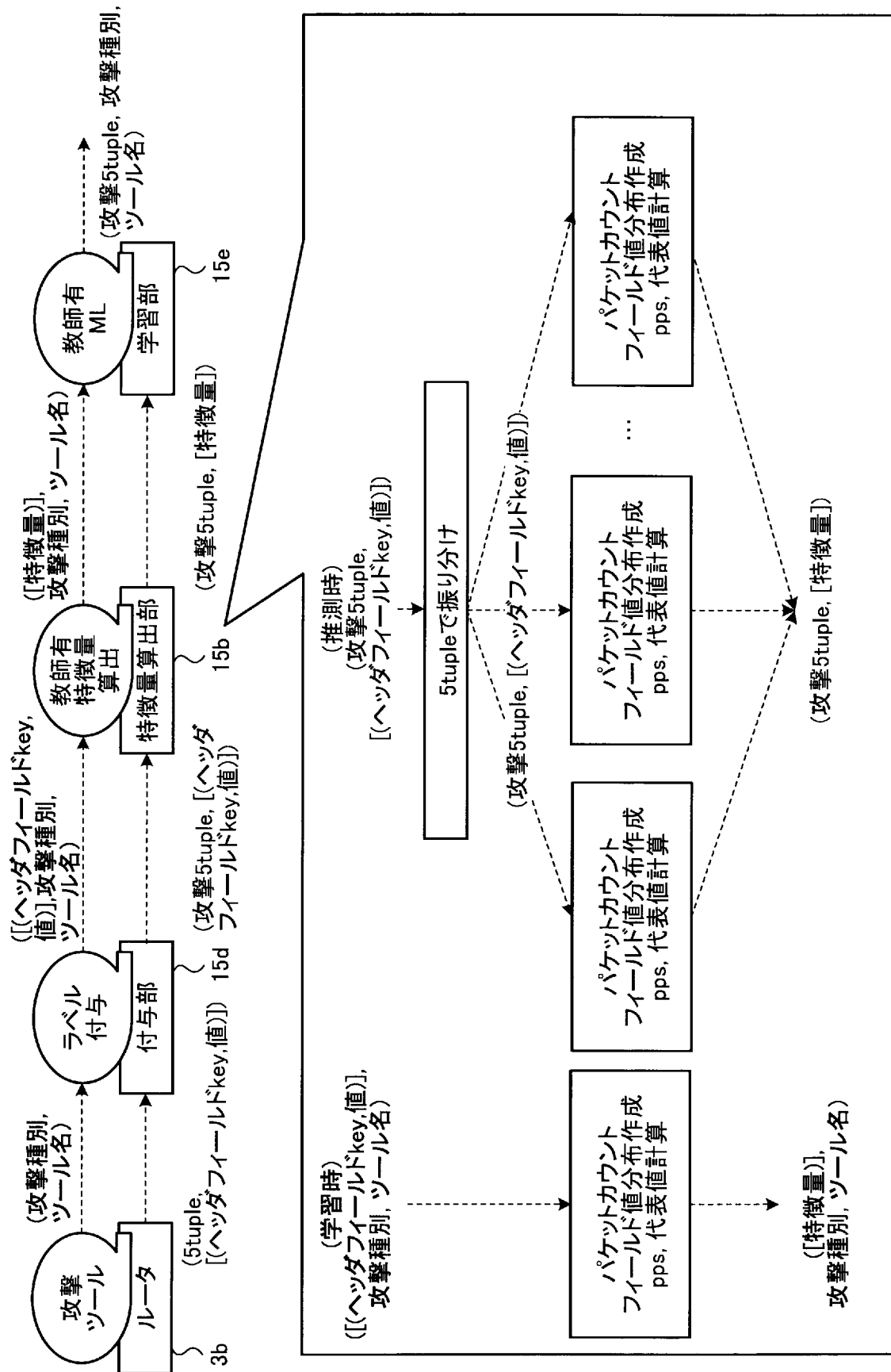
[図3]



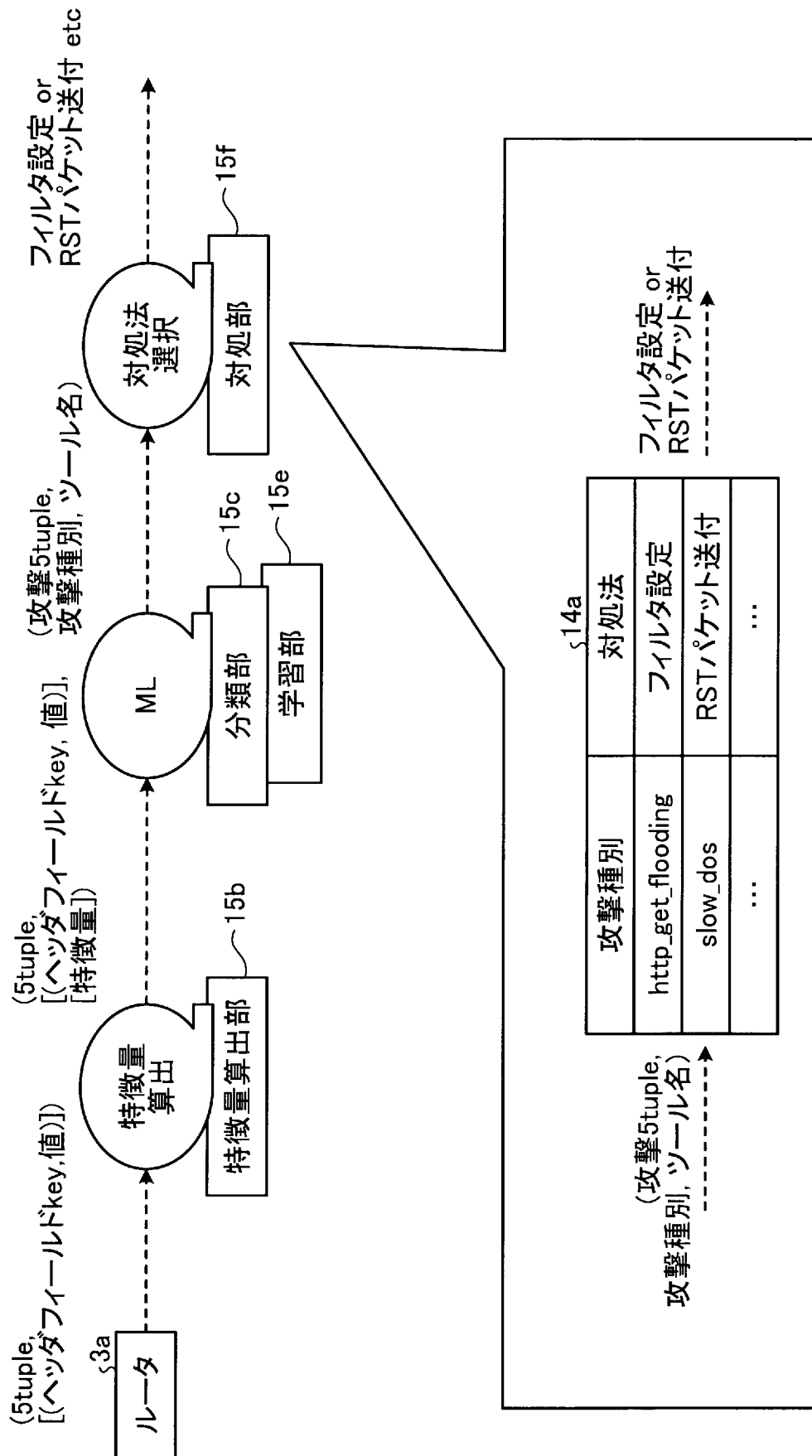
[図4]



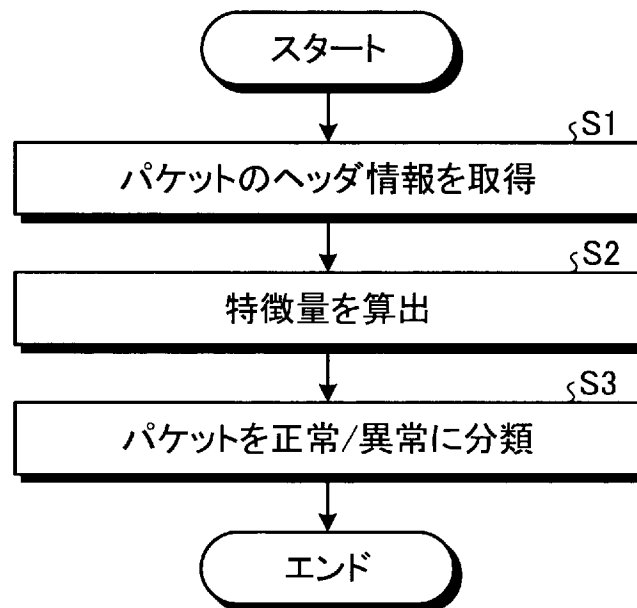
[図5]



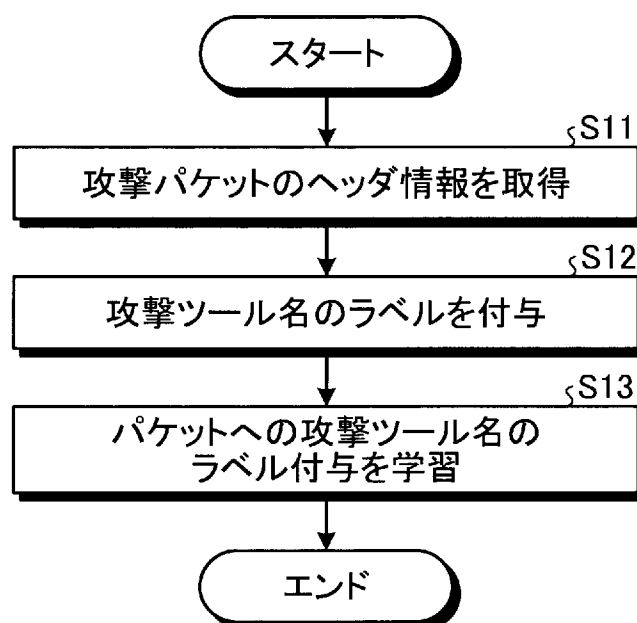
[図6]



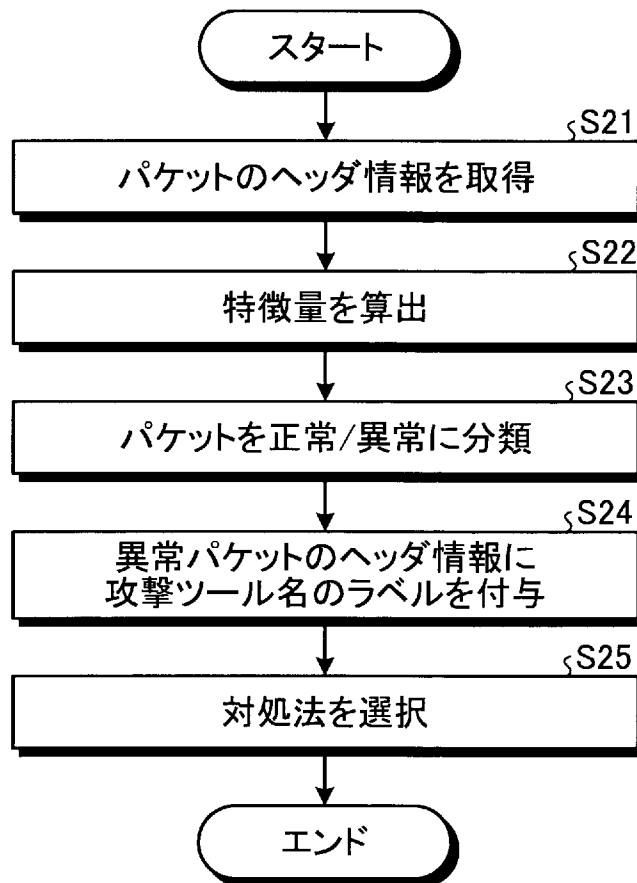
[図7]



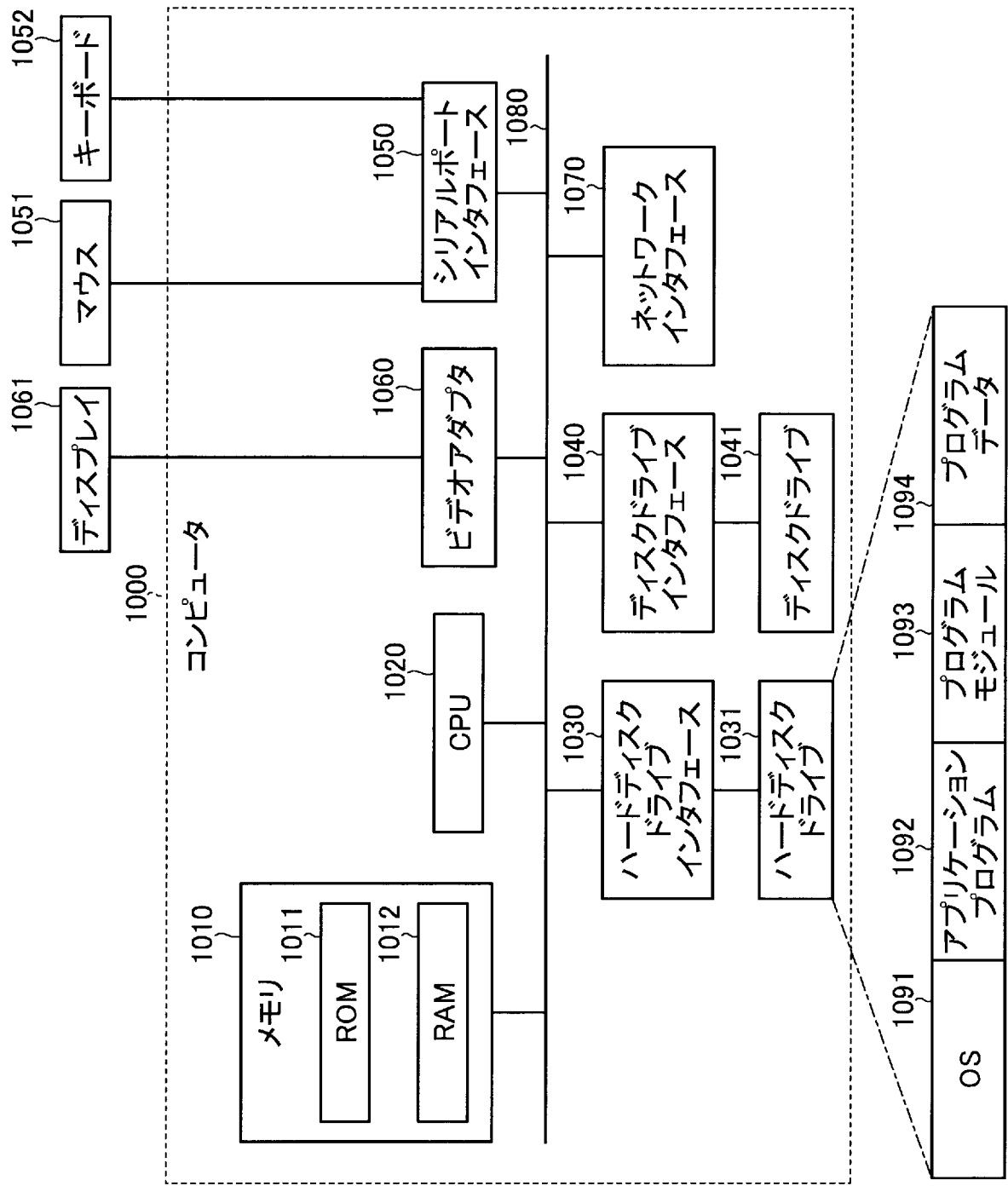
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/004102

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L12/70 (2013.01) i

FI: H04L12/70100Z

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 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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	WO 2016/002915 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 07.01.2016 (2016-01-07), paragraphs [0028]-[0069], fig. 1-5, etc.	1-2, 5
X A	風戸 雄太, パケットヘッダを用いた攻撃検知における Gini importance に着目した特徴量選定手法の提案と評価, 電子情報通信学会技術研究報告, vol. 117, no. 353, 07 December 2017, pp. 91-96, particularly, 「1. はじめに」-「2.2. 機械学習を用いた攻撃検知方法」, 「5. 提案手法」-「6.2. データセット」, 「6.4. 評価結果」の「(3) 攻撃種類ごとの検出率の結果」, (KAZATO, Yuta, A study of Gini importance-based header feature selection methods for cyber attack detection, IEICE Technical Report), non-official translation ("1. Introduction" - "2.2. Attack detection method using machine learning", "5. Proposed method" - "6.2. Data set", "6.4. Evaluation results", "(3) Detection rate results	1, 5 3



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

"I" 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
03.04.2020Date of mailing of the international search report
14.04.2020Name 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

International application No.

PCT/JP2020/004102

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2018/0152475 A1 (FOUNDATION OF SOONGSIL UNIVERSITY-INDUSTRY COOPERATION) 31.05.2018 (2018-05-31), paragraphs [0006], [0014], [0031]-[0045], [0058]-[0088], fig. 1-3	1, 5 4
X	JP 2017-147558 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 24.08.2017 (2017-08-24), paragraphs [0014], [0016]-[0018], [0023]-[0051], fig. 1-6	1, 5
A	JP 2008-306706 A (MITSUBISHI ELECTRIC INFORMATION TECHNOLOGY CENTRE EUROPA BV) 18.12.2008 (2008-12-18), paragraphs [0028], [0029], [0048]-[0050], [0052], [0053], fig. 3A, 3B	3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2020/004102

WO 2016/002915 A1	07.01.2016	(Family: none)
US 2018/0152475 A1	31.05.2018	KR 10-2018-0062318 A
JP 2017-147558 A	24.08.2017	(Family: none)
JP 2008-306706 A	18.12.2008	US 2008/0263661 A1 paragraphs [0043], [0044], [0061]-[0063], [0065], [0066], fig. 3A, 3B EP 1986391 A1

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 <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 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020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 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020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 - 2020年									
日本国実用新案登録公報	1996 - 2020年									
日本国登録実用新案公報	1994 - 2020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								
X	WO 2016/002915 A1（日本電信電話株式会社）07.01.2016（2016 - 01 - 07） [0028]-[0069], 図1-5等	1-2, 5								
X	風戸 雄太 Yuta Kazato, パケットヘッダを用いた攻撃検知における Gini importance に着目した特徴量選定手法の提案と評価 A study of Gini importance-based header feature selection methods for cyber attack detection, 電子情報通信学会技術研究報告 Vol. 117 No. 353 IEICE Technical Report, 2017.12.07, P.91-96 特に、「1. はじめに」 - 「2.2. 機械学習を用いた攻撃検知方法」、「5. 提案手法」 - 「6.2. データセット」、「6.4. 評価結果」の「(3) 攻撃種類ごとの検出率の結果」	1, 5								
A		3								
X	US 2018/0152475 A1 (FOUNDATION OF SOONGSIL UNIVERSITY-INDUSTRY COOPERATION) 31.05.2018 (2018 - 05 - 31) [0006], [0014], [0031]-[0045], [0058]-[0088], FIGs.1-3	1, 5								
A		4								
X	JP 2017-147558 A（日本電信電話株式会社）24.08.2017（2017 - 08 - 24） [0014], [0016]-[0018], [0023]-[0051], 図1-6	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 03.04.2020		国際調査報告の発送日 14.04.2020								
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								

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 2008-306706 A (ミツビシ・エレクトリック・インフォメーション・テクノロジー・センター・ヨーロッパ・ビーヴィ) 18.12.2008 (2008 - 12 - 18) [0028]-[0029], [0048]-[0050], [0052]-[0053], 図3A-3B	3

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/JP2020/004102

引用文献			公表日	パテントファミリー文献	公表日
WO	2016/002915	A1	07.01.2016	(ファミリーなし)	
US	2018/0152475	A1	31.05.2018	KR 10-2018-0062318	A
JP	2017-147558	A	24.08.2017	(ファミリーなし)	
JP	2008-306706	A	18.12.2008	US 2008/0263661	A1
				[0043]-[0044],	
				[0061]-[0063], [0065]-	
				[0066], FIGs. 3A-3B	
				EP 1986391	A1