(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2月27日(27.02.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/040002 A1

(51) 国際特許分類:
H04L 12/70 (2013.01) *H04L 12/26* (2006.01)
H04L 12/24 (2006.01)

(21) 国際出願番号： PCT/JP2019/031847

(22) 国際出願日： 2019年8月13日(13.08.2019)

(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 2018-157845 2018年8月24日(24.08.2018) JP

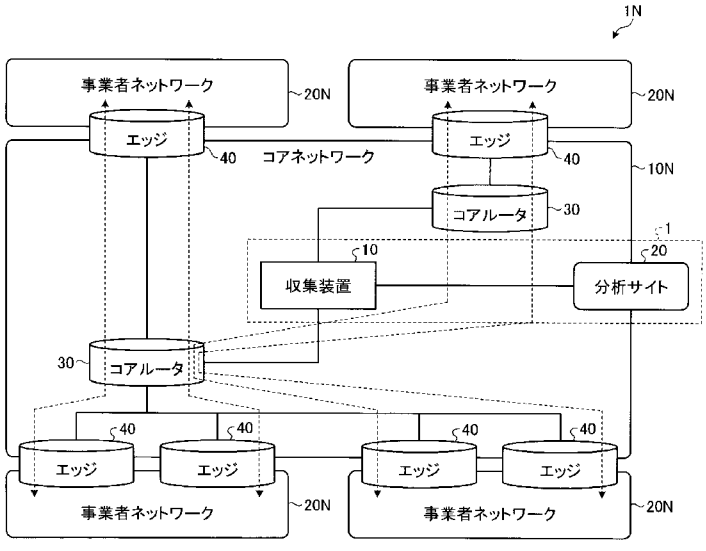
(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 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). 大西 浩行(**ONISHI, Hiroyuki**); 〒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). 鈴木 裕志(**SUZUKI, 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). 三好 勇樹(**MIYOSHI, 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). 林 裕平(**HAYASHI, Yuhei**);

(54) **Title:** ANALYSIS SYSTEM AND ANALYSIS METHOD

(54) 発明の名称： 分析システム及び分析方法

[図1]



10 Collection device
20 Analysis site
30 Core router
40 Edge
20N Provider network

(57) **Abstract:** A collection device (10) collects traffic from a core network (10N) connected to a plurality of provider networks (20N). Also, an analysis device has a plurality of functions for analyzing the traffic. Also, a setting device sets a scenario for indicating any of the plurality of functions. Also, a preprocessing device converts traffic collected by the collection device (10) into traffic in a format matching the function indicated by the scenario. Also, an allocation device allocates the traffic converted by the preprocessing device to the indicated functions.

WO 2020/040002 A1

［続葉有］

〒1808585 東京都武蔵野市緑町３丁目９－１１ＮＴＴ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, 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)）

(57) 要約：収集装置（１０）は、複数の事業者ネットワーク（２０Ｎ）と接続されたコアネットワーク（１０Ｎ）から、トラヒックを収集する。また、分析装置は、トラヒックを分析する複数の機能を有する。また、設定装置は、複数の機能のうちの少なくともいずれかを指定するシナリオを設定する。また、前処理装置は、収集装置（１０）によって収集されたトラヒックを、シナリオによって指定された機能に適合する形式のトラヒックに変換する。また、振分装置は、前処理装置によって変換されたトラヒックを、指定された機能に振り分ける。

明　細　書

発明の名称 ： 分析システム及び分析方法

技術分野

[0001]　本発明は、分析システム及び分析方法に関する。

背景技術

[0002]　キャリアネットワークは、複数の事業者ネットワーク及び当該事業者ネットワーク間を接続するコアネットワークを有する。従来、キャリアネットワークの故障分析及びセキュリティ分析を行う方法として、事業者ネットワークとコアネットワークのエッジに備えられたルータ等の機器（以降、単にエッジと呼ぶ場合がある）の所在地に派遣された技術者が、当該機器に分析装置を接続することで分析を行う方法が知られている。

先行技術文献

非特許文献

[0003] 非特許文献1：日本ネットワークセキュリティ協会（ＪＮＳＡ）、「セキュリティ対応組織の教科書　v1.0」、[online]、[２０１８年８月１３日検索]、インターネット（https://www.jnsa.org/result/2016/isog-j/data/textbook_soc-csirt_v1.0.pdf）

非特許文献2：情報処理推進機構（ＩＰＡ）、「OSSモデルカリキュラムの学習ガイダンス　3-2-応.ネットワーク管理に関する知識」、[online]、[２０１８年８月１３日検索]、インターネット（https://www.ipa.go.jp/files/000056034.pdf）

非特許文献3：さくらインターネット、「Non　Sampledトラフィック解析の応用例　－　iDC編」、[online]、[２０１８年８月１３日検索]、インターネット（https://www.janog.gr.jp/meeting/janog19/files/Flow_Ohkubo.pdf）

発明の概要

発明が解決しようとする課題

[0004]　しかしながら、従来の方法には、キャリアネットワークにおける故障分析

及びセキュリティ分析を効率良く行うことが困難な場合があるという問題がある。例えば、キャリアネットワークのエッジは、地理的に互いに離れた場所に設置される場合がある。そのような場合、各エッジへの技術者の派遣には、多大な経済的又は時間的なコストが生じる。

課題を解決するための手段

[0005] 上述した課題を解決し、目的を達成するために、分析システムは、複数のネットワークと接続されたコアネットワークから、トラヒックを収集する収集部と、トラヒックを分析する複数の機能を有する分析部と、前記複数の機能のうちの少なくともいずれかを指定するシナリオを設定する設定部と、前記収集部によって収集されたトラヒックを、前記シナリオによって指定された機能に適合する形式のトラヒックに変換する変換部と、前記変換部によって変換されたトラヒックを、前記指定された機能に振り分ける振分部と、を有することを特徴とする。

発明の効果

[0006] 本発明によれば、キャリアネットワークにおける故障分析及びセキュリティ分析を効率良く行うことができる。

図面の簡単な説明

[0007] [図1]図１は、第１の実施形態に係るキャリアネットワークの構成の一例を示す図である。

[図2]図２は、第１の実施形態に係る分析システムの構成の一例を示す図である。

[図3]図３は、第１の実施形態に係る分析システムの処理の一例を示すシーケンス図である。

[図4]図４は、第１の実施形態に係る分析システムの処理の流れを示すフローチャートである。

[図5]図５は、分析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

[0008] 以下に、本願に係る分析システム及び分析方法の実施形態を図面に基づいて詳細に説明する。なお、本発明は、以下に説明する実施形態により限定されるものではない。

[0009] ［第１の実施形態の構成］

まず、図１を用いて、第１の実施形態に係る分析システムを含むキャリアネットワークの構成について説明する。図１は、第１の実施形態に係るキャリアネットワークの構成の一例を示す図である。図１に示すように、キャリアネットワーク１Ｎは、コアネットワーク１０Ｎ及び事業者ネットワーク２０Ｎを有する。また、キャリアネットワーク１Ｎは、分析システム１を有する。

[0010] コアネットワーク１０Ｎは、コアルータ３０を有する。コアルータ３０は、コアネットワーク１０Ｎでのトラヒックのルーティング及び転送を行う。コアネットワーク１０Ｎと事業者ネットワーク２０Ｎとの間のエッジ４０は、それぞれ地理的に離れた場所にあるものとする。例えば、各エッジは、国内の異なる地域、さらには国外に設けられている場合がある。このため、キャリアネットワーク１Ｎの故障分析やセキュリティ分析のためにエッジ４０に技術者を派遣すると、多大なコストが生じる。

[0011] 分析システム１は、収集装置１０及び分析サイト２０を有する。分析システム１は、キャリアネットワーク１Ｎの故障分析やセキュリティ分析を行うためのシステムである。分析システム１によれば、技術者をエッジ４０に派遣することなく故障分析やセキュリティ分析を行うことが可能になる。

[0012] 収集装置１０は、複数の事業者ネットワーク２０Ｎと接続されたコアネットワーク１０Ｎから、トラヒックを収集する。また、収集装置１０は、収集したトラヒックを分析サイト２０に転送する。また、コアルータ３０に収集装置１０の機能を持たせてもよい。その場合、コアルータ３０は、コアネットワーク１０Ｎからトラヒックを収集し、収集したトラヒックを分析サイト２０に転送する。なお、収集装置１０及びコアルータ３０は、収集部の例で

ある。

[0013] ここで、分析サイト２０は、本実施形態における故障分析やセキュリティ分析を行うための装置等の集合である。分析サイト２０は、１つの装置であってもよいし、互いにデータの通信ができるように接続された複数の装置を含むシステムであってもよい。また、１つのコアネットワーク１０Ｎに対し、複数の分析サイト２０が存在していてもよい。なお、以降の説明では、トラヒックを、送受信されるパケットの集合と読み替えてもよい。

[0014] 例えば、収集装置１０は、コアルータ３０と接続され、コアルータ３０が転送するトラヒックを収集する。また、分析サイト２０は、コアネットワーク１０Ｎの内部又は外部に設けられ、少なくとも収集装置１０との間でデータの送受信を行うことができる。

[0015] 図２を用いて、分析システム１の構成について説明する。図２は、第１の実施形態に係る分析システムの構成の一例を示す図である。図２に示すように分析システム１は、設定装置２１、振分装置２２、前処理装置２３、分析機能群２４及び後処理装置２５を有する。また、分析機能群２４は、第１の分析装置２４１及び第２の分析装置２４２を含む。なお、分析システム１に含まれる分析装置は１つであってもよいし、複数であってもよい。

[0016] 収集装置１０は、複数の事業者ネットワーク２０Ｎと接続されたコアネットワーク１０Ｎから、トラヒックを収集する。収集装置１０は、サンプリングコピー又はノンサンプリングコピーによってコアネットワーク１０Ｎのトラヒックを収集する。

[0017] また、収集装置１０は、ポリシング機能を有する。例えば、ノンサンプリングコピーによって収集したトラヒックのコアネットワーク１０Ｎ内における帯域が１０Ｇｂｐｓであり、収集装置１０と分析サイト２０との間の帯域が５Ｇｂｐｓに制限されている場合、収集装置１０は、収集したトラヒックをポリシング機能により５Ｇｂｐｓに制限した上で分析サイト２０に転送する。また、収集装置１０は、収集したトラヒックをカプセル化して分析サイト２０に転送することができる。

[0018] また、収集装置１０は、トラヒックの収集を、分析が必要な事象が発生した場合に随時実施してもよいし、定常監視を行うために常時実施してもよいし、決まった日時で定期的に実施してもよい。また、収集装置１０は、ＡＣＬ（Access Control List）機能によりトラヒックをフィルタリングした上で収集することができる。

[0019] 設定装置２１は、設定装置２１は、複数の機能のうちの少なくともいずれかを指定するシナリオを設定する。シナリオは、分析機能群２４に含まれる分析機能のうちのいずれかを指定し、さらに、トラヒックの収集方法、前処理及び後処理等を指定する。設定装置２１は、ユーザから設定するシナリオの指定を受け付けてもよい。

[0020] 振分装置２２は、シナリオに従い、トラヒック及びトラヒックに基づいて得られたデータ（以降、両者をまとめて振り分けデータと呼ぶ）を分析サイト２０の各装置及び処理部に振り分ける。振分装置２２は、振り分けデータをフロー単位で振り分けることができる。

[0021] また、振分装置２２は、振り分けデータの振り分け先からさらにデータを受け取り、当該データをさらに次の振り分け先に振り分けることができる。また、振分装置２２は、複数の振り分け先を数珠つなぎにして、連続して振り分けデータを通過させることができる。また、振分装置２２は、ミラー機能により、複数の振り分け先に同一の振り分けデータを振り分けることができる。また、振分装置２２は、ＯＡＭ（Operations, Administration, Maintenance）機能により、振り分けが正しく行われたか否かを確認する。

[0022] 前処理装置２３は、トラヒックの分析のための前処理を行う。前処理装置２３は、変換部２３１、生成部２３２及び抽出部２３３を有する。

[0023] 変換部２３１は、収集装置１０によって収集されたトラヒックを、シナリオによって指定された機能に適合する形式のトラヒックに変換する。例えば、変換部２３１は、収集装置１０によって収集されたトラヒックに付与されたトンネルを除去する。

[0024] ここで、コアネットワーク１０Ｎでは、パケットを高速転送することや、

ユーザ単位に論理的にトラヒックを分割することを目的として、トンネル機能が用いられる。分析機能の中には、トンネルヘッダが付与されたパケットを分析することができないものがある。そこで、変換部２３１は、パケットからトンネルヘッダを除去することで、分析機能が分析可能なフォーマットにトラヒックを変換する。

[0025] 生成部２３２は、変換部２３１によって変換されたトラヒックを基に、トラヒックのフロー情報を生成する。分析機能の中には、トラヒックに含まれる個々のパケットではなく、netflow、sflow及びＩＰＦＩＸ（Internet Protocol Flow Information Export）といったフロー情報を分析対象とするものがある。

[0026] 抽出部２３３は、変換部２３１によって変換されたトラヒックに対してフィルタリングを行い、所定のトラヒックを抽出する。分析機能中には、収集装置１０が収集したトラヒックのうち、所定の条件に合致するトラヒックのみを分析対象とするものがある。このため、抽出部２３３は、５－ｔｕｐｌｅ及びプロトコル等によりトラヒックに含まれるパケットをフィルタリングし、分析機能が分析対象とするトラヒックを抽出することができる。

[0027] 変換部２３１、生成部２３２及び抽出部２３３は、それぞれの処理部で得られたデータをさらに処理対象とすることができる。例えば、抽出部２３３は、変換部２３１によってフォーマットが変換されたトラヒックに対してフィルタリングを行ってもよい。また、生成部２３２は、抽出部２３３によって抽出されたトラヒックからフロー情報を生成してもよい。また、変換部２３１、生成部２３２及び抽出部２３３への振り分けデータの振り分けは、振分装置２２によって行われる。

[0028] 分析機能群２４は、トラヒックを分析する複数の機能を有する。分析機能群２４は、複数の分析装置を有していてもよい。また、各分析装置は、複数の分析機能を有していてもよい。図２の例では、分析機能群２４は、第１の分析装置２４１及び第２の分析装置２４２を有する。また、第１の分析装置２４１は、分析機能２４１ａを有する。また、第２の分析装置２４２は、分

析機能２４２ａ及び分析機能２４２ｂを有する。

[0029] ここで、各分析機能は、市販されているトラヒック分析用のソフトウェアであってもよい。例えば、第１の分析装置２４１及び第２の分析装置２４２は、コンピュータにトラヒック分析用のソフトウェアをインストールしたものである。

[0030] また、例えば、分析機能の追加は、分析サイト２０内の接続スイッチに物理配線を行い、新たな分析装置を接続し、当該接続した分析装置に振り分けデータの振り分けが可能になるように、設定装置２１及び振分装置２２等の設定を変更することで実現できる。

[0031] また、分析装置を仮想化することで、複数の分析サイト２０が当該分析装置の分析機能を共有することができる。その際、複数の分析サイト２０による同時起動を不可にする占有制御を行うことで、分析結果に不整合が生じることを防止できる。

[0032] また、各分析機能へのトラヒック等の振り分けは、振分装置２２によって行われる。その際、振分装置２２は、前処理装置２３の各処理部によって前処理が行われたトラヒックを振り分けることができる。すなわち、振分装置２２は、変換部２３１によって変換されたトラヒックを、指定された機能に振り分ける。また、振分装置２２は、生成部２３２によって生成されたフロー情報を指定された機能に振り分ける。また、振分装置２２は、抽出部２３３によって抽出されたトラヒックを指定された機能に振り分ける。

[0033] 後処理装置２５は、格納部２５１及び再生部２５２を有する。また、後処理装置２５は、トラヒック情報２５３を記憶する。格納部２５１は、分析機能により分析が終了したトラヒックをトラヒック情報２５３として記憶領域に格納する。また、再生部２５２は、トラヒック情報２５３として記憶されているトラヒックを所定のネットワーク環境で再現する。なお、トラヒック情報２５３は、前処理装置２３による前処理が行われる前のトラヒックであってもよいし、前処理が行われた後のトラヒックであってもよい。また、後処理装置２５は、トラヒック情報２５３を、他の保存用ストレージに書き出

すことができる。

[0034] ここで、設定装置２１が設定するシナリオが指定する事項の例を以下に示す。

・収集装置１０がサンプリングコピーを行うかノンサンプリングコピーを行うか。

・収集装置１０のトラヒックを収集するタイミング（随時、常時又は定期的）。

・収集装置１０のポリシング機能、カプセル化機能、ＡＣＬ機能を有効化するか否か。

・振分装置２２の振り分け先及び振り分けの順序。

・振分装置２２のミラー機能及びＯＡＭ機能を有効化するか否か。

・変換部２３１によるフォーマット変換を行うか否か、及び変換するフォーマット。

・生成部２３２がフロー情報の生成を行うか否か、及びフロー情報の形式。

・抽出部２３３が抽出を行うか否か、及びフィルタリングの条件。

・分析機能群２４の分析機能のうち、使用する分析機能。

・格納部２５１によるトラヒック情報２５３の格納を行うか否か。

[0035] また、シナリオは、事象ごとに用意されているものとする。例えば、Ｗｅｂサーバへの攻撃分析と、機器の故障分析とでは、使用される分析機能及びトラヒックへの前処理等が異なるため、それぞれ別のシナリオが用意される。

[0036] ここで、図３を用いて、分析システム１の具体的な処理の一例を説明する。図３は、第１の実施形態に係る分析システムの処理の一例を示すシーケンス図である。また、図３の例では、フロー分析機能２４５ａ及びＵＴＭ（Unified Threat Management）詳細分析機能２４５ｂが使用されるものとする。また、フロー分析機能２４５ａ及びＵＴＭ詳細分析機能２４５ｂは、分析機能群２４に含まれる。

[0037] 図３に示すように、事象が発生すると（ステップＳ１０１）、ユーザは端

末２から設定装置２１に対し、フロー分析の開始を指示する（ステップＳ１０２）。ここで、端末２は、設定装置２１にアクセス可能な端末である。また、事象は、キャリアネットワーク１Ｎ上のサーバへの攻撃や機器の故障である。

[0038] 設定装置２１は、フロー分析機能２４５ａに対応するシナリオに従い、前処理装置２３に、トラヒックのフォーマット変換及びフロー情報の生成を指示する（ステップＳ１０３、Ｓ１０４）。また、設定装置２１は、フロー分析機能２４５ａにフロー分析の実行を指示する（ステップＳ１０５）。また、設定装置２１は、振分装置２２に、トラヒックの振り分けを指示する（ステップＳ１０６）。また、設定装置２１は、収集装置１０に、収集したトラヒックの転送を指示する（ステップＳ１０７）。

[0039] ここで、フロー分析機能２４５ａは、フロー分析を実行する（ステップＳ１０８）。ただし、このとき、収集装置１０、振分装置２２及び前処理装置２３は、設定装置２１による指示に従ってそれぞれの処理を実行しているため、フロー分析機能２４５ａには、前処理が実施されたトラヒックが振り分けられてきている。

[0040] フロー分析機能２４５ａは、分析結果を設定装置２１に提供する（ステップＳ１０９）。さらに、設定装置２１は、分析結果を端末２に提供する（ステップＳ１１０）。ここで、端末２を用いて分析結果を確認したユーザは、設定装置２１に詳細分析の開始を指示する（ステップＳ１１１）。

[0041] 設定装置２１は、ＵＴＭ詳細分析機能２４５ｂに対応するシナリオに従い、前処理装置２３に、トラヒックの抽出を指示する（ステップＳ１１２）。また、設定装置２１は、ＵＴＭ詳細分析機能２４５ｂに詳細分析の実行を指示する（ステップＳ１１３）。また、設定装置２１は、後処理装置２５に、トラヒックの保存を指示する（ステップＳ１１４）。また、設定装置２１は、振分装置２２に、トラヒックの振り分け及びコピーを指示する（ステップＳ１１５）。

[0042] ここで、ＵＴＭ詳細分析機能２４５ｂは、詳細分析を実行する（ステップ

Ｓ１１６）。また、後処理装置２５は、振分装置２２によってコピーされたトラヒックをトラヒック情報２５３として保存する。

[0043] ＵＴＭ詳細分析機能２４５ｂは、分析結果を設定装置２１に提供する（ステップＳ１１７）。さらに、設定装置２１は、分析結果を端末２に提供する（ステップＳ１１８）。

[0044] ［第１の実施形態の処理］

図４を用いて、分析システム１の処理の流れについて説明する。図４は、第１の実施形態に係る分析システムの処理の流れを示すフローチャートである。図４に示すように、まず、収集装置１０は、トラヒックを収集し、分析サイト２０に転送する（ステップＳ１１）。

[0045] 振分装置２２は、トラヒックを変換部２３１、生成部２３２、抽出部２３３の順で振り分ける（ステップＳ１２）。なお、前処理装置２３のどの処理部を実行するかはシナリオによる。ここでは、変換部２３１、生成部２３２、抽出部２３３のすべてで処理が実行されるものとする。

[0046] 変換部２３１は、振り分けられたトラヒックのフォーマットを変換する（ステップＳ１３）。また、生成部２３２は、振り分けられたトラヒックからフロー情報を生成する（ステップＳ１４）。また、抽出部２３３は、振り分けられたトラヒックからフィルタリングによりトラヒックを抽出する（ステップＳ１５）。

[0047] 次に、振分装置２２は、トラヒックをシナリオで指定された分析機能に振り分ける（ステップＳ１６）。分析機能はトラヒックの分析を実行する（ステップＳ１７）。また、後処理装置２５は、分析に使用されたトラヒックを、トラヒック情報２５３として記憶領域に格納する。

[0048] ［第１の実施形態の効果］

収集装置１０は、複数の事業者ネットワーク２０Ｎと接続されたコアネットワーク１０Ｎから、トラヒックを収集する。また、分析装置は、トラヒックを分析する複数の機能を有する。また、設定装置２１は、複数の機能のうちの少なくともいずれかを指定するシナリオを設定する。また、前処理装置

２３は、収集装置１０によって収集されたトラヒックを、シナリオによって指定された機能に適合する形式のトラヒックに変換する。また、振分装置２２は、前処理装置２３によって変換されたトラヒックを、指定された機能に振り分ける。このように、本実施形態では、キャリアネットワークの分析に必要な機能を、分析サイトに集約している。また、分析サイトには、キャリアネットワークのトラヒックが転送される。このため、本実施形態によれば、エッジ等の設置場所に技術者を派遣する必要がなく、キャリアネットワークにおける故障分析及びセキュリティ分析を効率良く行うことができる。

[0049] 前処理装置２３は、収集装置１０によって収集されたトラヒックに付与されたトンネルを除去する。これにより、トンネルが付与されていないトラヒックのみを対象とする分析機能を使った分析が可能になる。

[0050] 生成部２３２は、変換部２３１によって変換されたトラヒックを基に、トラヒックのフロー情報を生成する。また、振分装置２２は、生成部２３２によって生成されたフロー情報を指定された機能に振り分ける。これにより、フロー情報を対象とする分析機能を使った分析が可能になる。

[0051] 抽出部２３３は、変換部２３１によって変換されたトラヒックに対してフィルタリングを行い、所定のトラヒックを抽出する。また、振分装置２２は、抽出部２３３によって抽出されたトラヒックを指定された機能に振り分けるこれにより、分析に必要なトラヒックのみを抽出することができ、分析機能の処理負荷を低減することができる。

[0052] ［その他の実施形態］

上記の実施形態は、シナリオの設定、トラヒックの振り分け、前処理、分析及び後処理が、それぞれ別の装置で実行されるものであった。一方で、シナリオの設定、トラヒックの振り分け、前処理、分析及び後処理は、１つの装置で実行されてもよい。

[0053] ［システム構成等］

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように構成されていることを要しない。すなわち、各装置の

分散及び統合の具体的形態は図示のものに限られず、その全部又は一部を、各種の負荷や使用状況等に応じて、任意の単位で機能的又は物理的に分散又は統合して構成することができる。さらに、各装置にて行われる各処理機能は、その全部又は任意の一部が、ＣＰＵ及び当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0054] また、本実施形態において説明した各処理のうち、自動的に行われるものとして説明した処理の全部又は一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部又は一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

[0055] ［プログラム］

一実施形態として、分析システム１の各装置は、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分析処理を実行する分析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、上記の分析プログラムを情報処理装置に実行させることにより、情報処理装置を分析装置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、デスクトップ型又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）等の移動体通信端末、さらには、ＰＤＡ（Personal Digital Assistant）等のスレート端末等がその範疇に含まれる。

[0056] また、分析システム１は、ユーザが使用する端末装置をクライアントとし、当該クライアントに上記の分析処理に関するサービスを提供する分析サーバ装置として実装することもできる。例えば、分析サーバ装置は、コアネットワークのトラヒックを入力とし、分析結果を出力とする分析サービスを提供するサーバ装置として実装される。この場合、分析サーバ装置は、Ｗｅｂ

サーバとして実装することとしてもよいし、アウトソーシングによって上記の分析に関するサービスを提供するクラウドとして実装することとしてもかまわない。

[0057] 図５は、分析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、ＣＰＵ１０２０を有する。また、コンピュータ１０００は、ハードディスクドライブインタフェース１０３０、ディスクドライブインタフェース１０４０、シリアルポートインタフェース１０５０、ビデオアダプタ１０６０、ネットワークインタフェース１０７０を有する。これらの各部は、バス１０８０によって接続される。

[0058] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１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１０９０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１１００に接続される。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、ディスクドライブ１１００に挿入される。シリアルポートインタフェース１０５０は、例えばマウス１１１０、キーボード１１２０に接続される。ビデオアダプタ１０６０は、例えばディスプレイ１１３０に接続される。

[0059] ハードディスクドライブ１０９０は、例えば、ＯＳ１０９１、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、プログラムデータ１０９４を記憶する。すなわち、分析システム１の各処理を規定するプログラムは、コンピュータにより実行可能なコードが記述されたプログラムモジュール１０９３として実装される。プログラムモジュール１０９３は、例えばハードディスクドライブ１０９０に記憶される。例えば、分析システム１における機能構成と同様の処理を実行するためのプログラムモジュール１０９３が、ハードディスクドライブ１０９０に記憶される。なお、ハードディスクドライブ１０９０は、ＳＳＤにより代替されてもよい。

[0060] また、上述した実施形態の処理で用いられる設定データは、プログラムデータ１０９４として、例えばメモリ１０１０やハードディスクドライブ１０９０に記憶される。そして、ＣＰＵ１０２０は、メモリ１０１０やハードディスクドライブ１０９０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、上述した実施形態の処理を実行する。

[0061] なお、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１０９０に記憶される場合に限らず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ１１００等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、プログラムモジュール１０９３及びプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶されてもよい。そして、プログラムモジュール１０９３及びプログラムデータ１０９４は、他のコンピュータから、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。

符号の説明

[0062] １　分析システム

１Ｎ　キャリアネットワーク

２　端末

１０　収集装置

１０Ｎ　コアネットワーク

２０　分析サイト

２０Ｎ　事業者ネットワーク

２１　設定装置

２２　振分装置

２３　前処理装置

２４　分析機能群

２５　後処理装置

３０　コアルータ

４０　エッジ

２３１　変換部

２３２　生成部

２３３　抽出部

２４１　第１の分析装置

２４１ａ、２４２ａ、２４２ｂ　分析機能

２４２　第２の分析装置

２４５ａ　フロー分析機能

２４５ｂ　ＵＴＭ詳細分析機能

２５１　格納部

２５２　再生部

２５３　トラヒック情報

請求の範囲

[請求項1] 複数のネットワークと接続されたコアネットワークから、トラヒックを収集する収集部と、

トラヒックを分析する複数の機能を有する分析部と、

前記複数の機能のうちの少なくともいずれかを指定するシナリオを設定する設定部と、

前記収集部によって収集されたトラヒックを、前記シナリオによって指定された機能に適合する形式のトラヒックに変換する変換部と、

前記変換部によって変換されたトラヒックを、前記指定された機能に振り分ける振分部と、

を有することを特徴とする分析システム。

[請求項2] 前記変換部は、前記収集部によって収集されたトラヒックに付与されたトンネルを除去することを特徴とする請求項１に記載の分析システム。

[請求項3] 前記変換部によって変換されたトラヒックを基に、前記トラヒックのフロー情報を生成する生成部をさらに有し、

前記振分部は、前記生成部によって生成されたフロー情報を前記指定された機能に振り分けることを特徴とする請求項１又は２に記載の分析システム。

[請求項4] 前記変換部によって変換されたトラヒックに対してフィルタリングを行い、所定のトラヒックを抽出する抽出部をさらに有し、

前記振分部は、前記抽出部によって抽出されたトラヒックを前記指定された機能に振り分けることを特徴とする請求項１から３のいずれか１項に記載の分析システム。

[請求項5] トラヒックを分析する複数の機能を有する分析部を有する分析システムによって実行される分析方法であって、

複数のネットワークと接続されたコアネットワークから、トラヒックを収集する収集工程と、

トラヒックを分析する複数の機能を有する分析工程と、

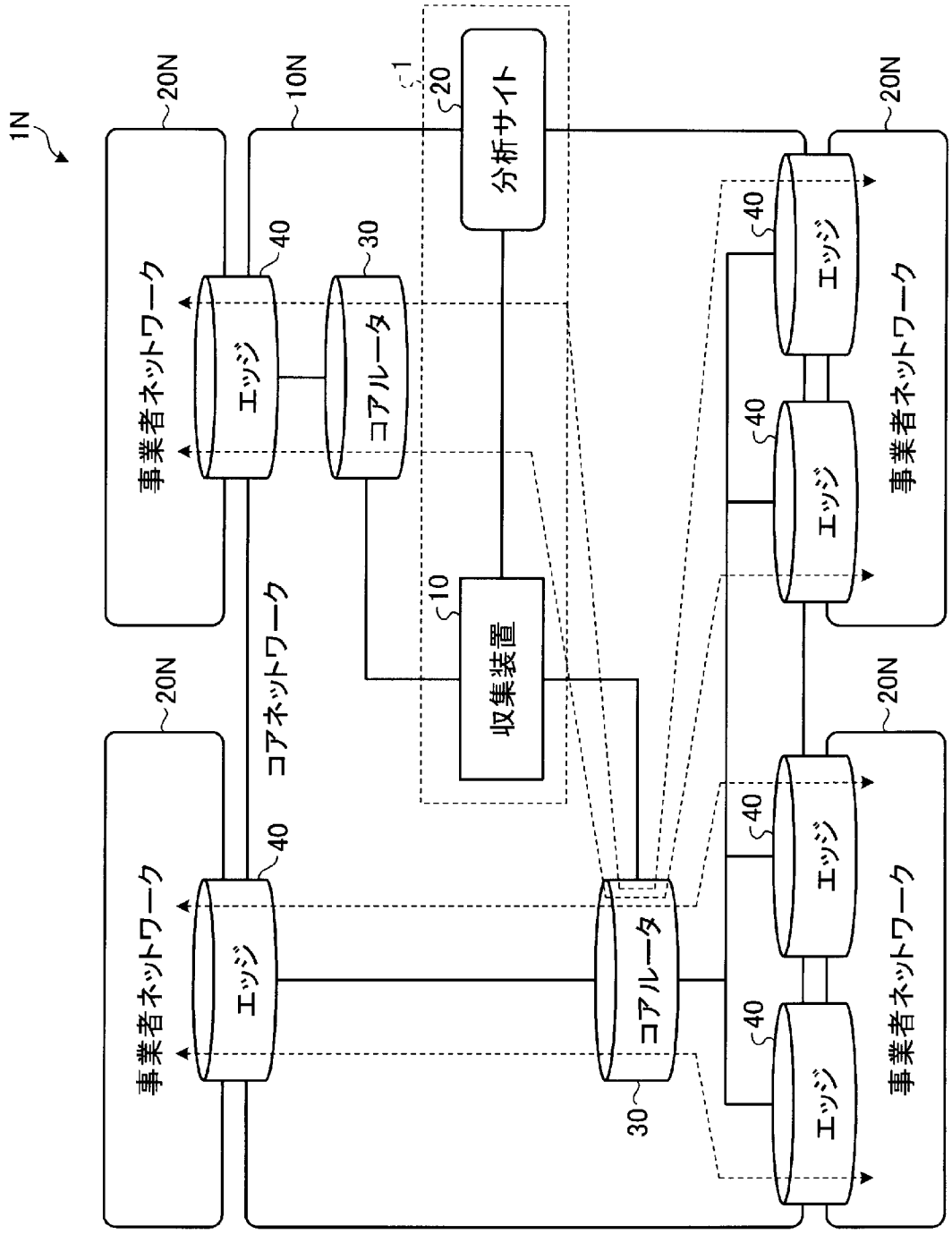
前記複数の機能のうちの少なくともいずれかを指定するシナリオを設定する設定工程と、

前記収集工程によって収集されたトラヒックを、前記シナリオによって指定された機能に適合する形式のトラヒックに変換する変換工程と、

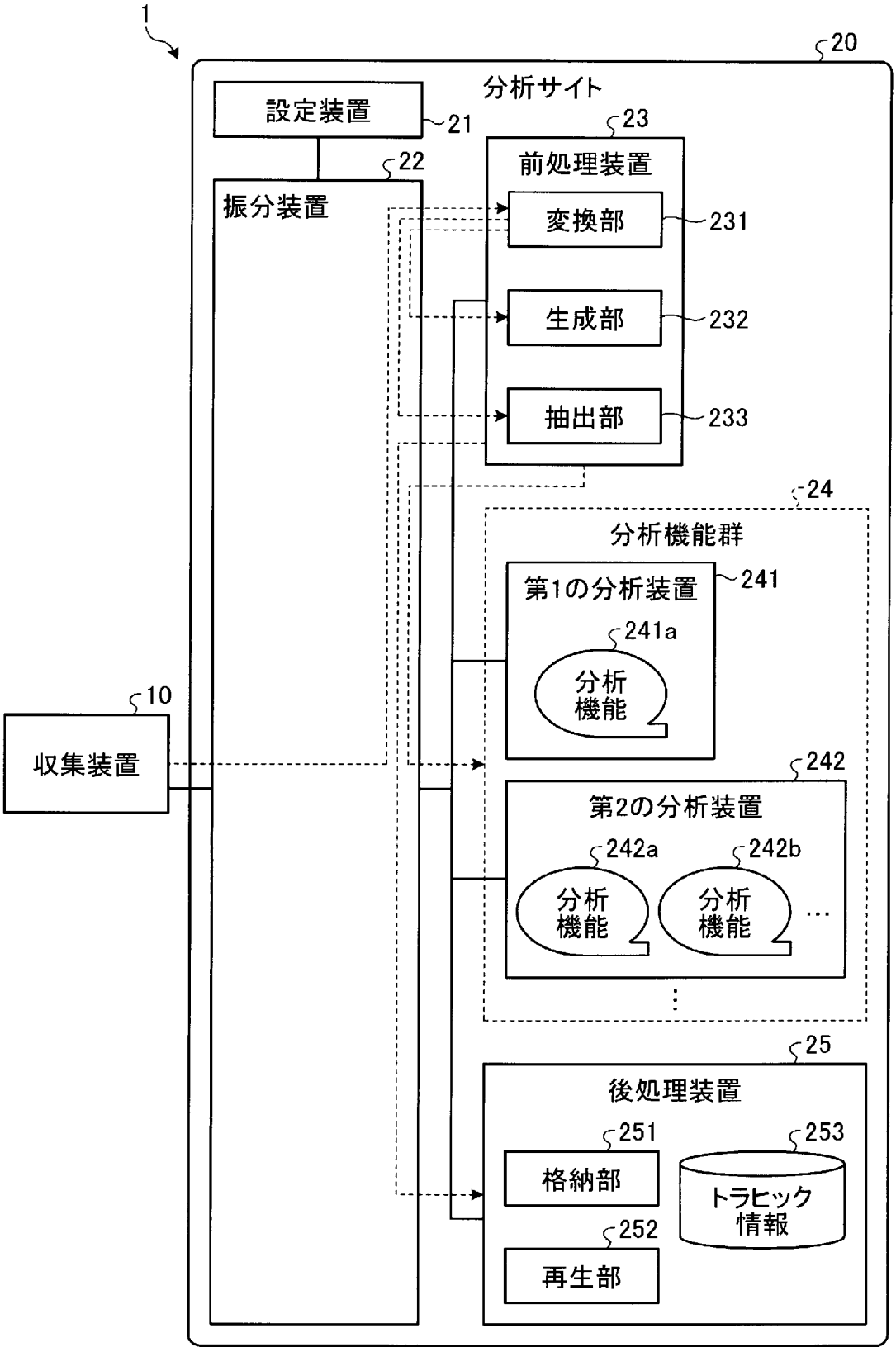
前記変換工程によって変換されたトラヒックを、前記指定された機能に振り分ける振分工程と、

を含むことを特徴とする分析方法。

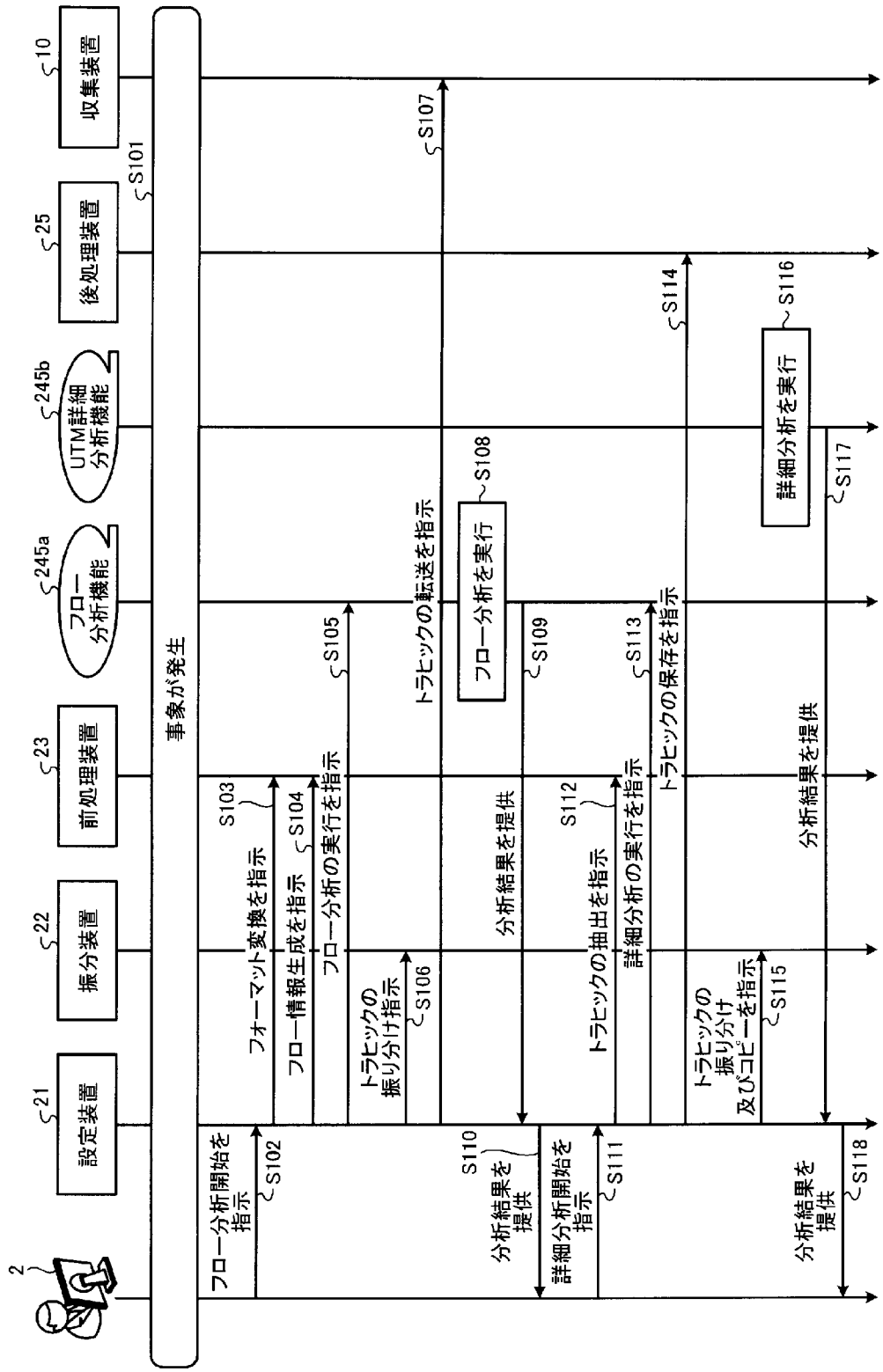
[図1]


1N
20N
10N
1
20
分析サイト
事業者ネットワーク
40
エッジ
30
コアルータ
10
収集装置
コアネットワーク
20N
40
エッジ
20N
事業者ネットワーク
40
エッジ
40
エッジ
20N
事業者ネットワーク
40
エッジ
40
エッジ
30
コアルータ

[図2]


1
20
分析サイト
設定装置
21
23
前処理装置
22
振分装置
変換部
231
生成部
232
抽出部
233
24
分析機能群
第1の分析装置
241
241a
分析機能
10
収集装置
242
第2の分析装置
242a
242b
分析機能
分析機能
…
25
後処理装置
251
格納部
253
トラヒック情報
252
再生部

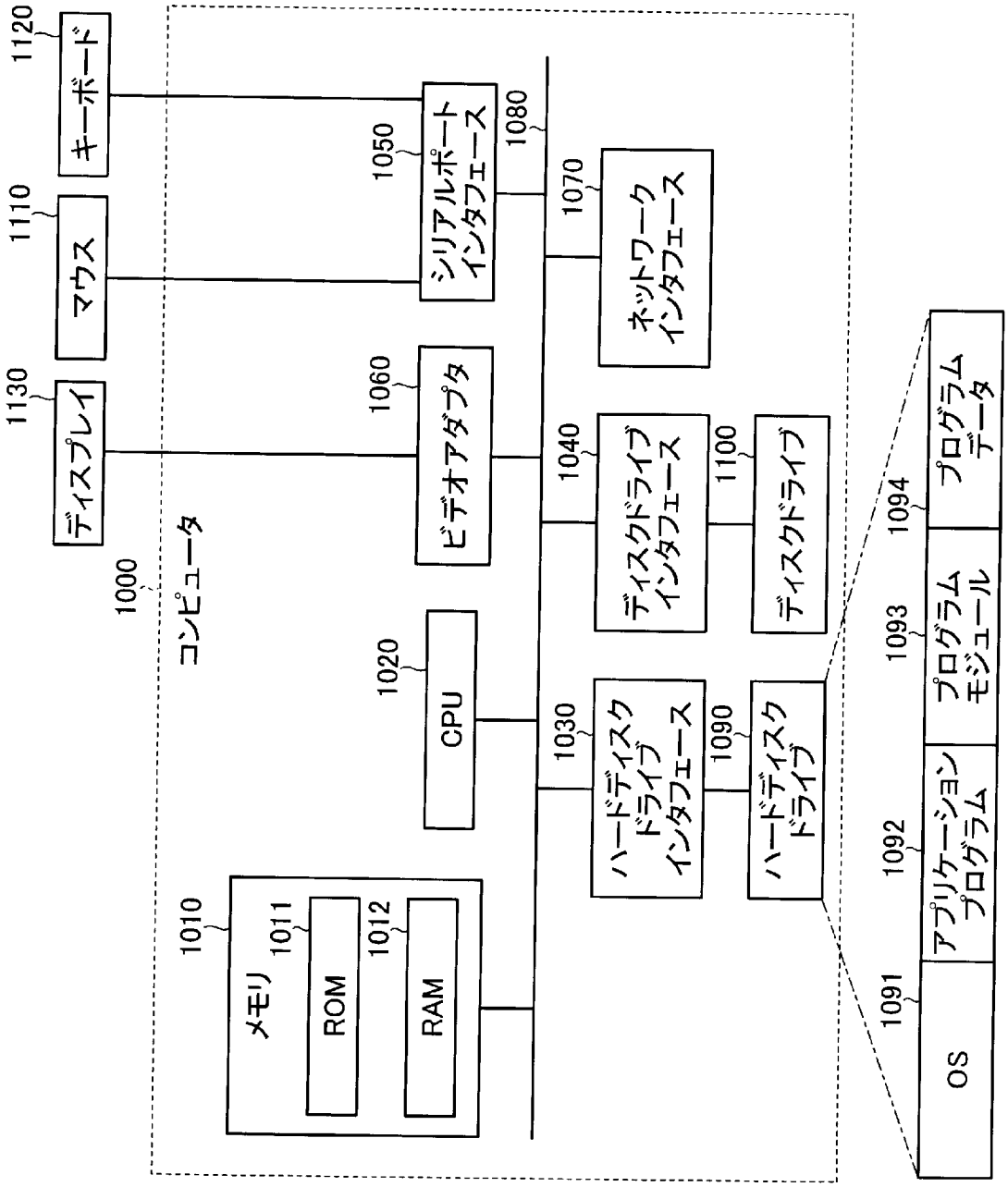
[図3]


2
21 設定装置
22 振分装置
23 前処理装置
245a フロー分析機能
245b UTM詳細分析機能
25 後処理装置
10 収集装置
事象が発生
S101
フロー分析開始を指示
S102
フォーマット変換を指示
S103
フロー情報生成を指示
S104
フロー分析の実行を指示
S105
トラヒックの振り分け指示
S106
トラヒックの転送を指示
S107
フロー分析を実行
S108
分析結果を提供
S109
分析結果を提供
S110
詳細分析開始を指示
S111
トラヒックの抽出を指示
S112
詳細分析の実行を指示
S113
トラヒックの保存を指示
S114
トラヒックの振り分け及びコピーを指示
S115
詳細分析を実行
S116
分析結果を提供
S117
分析結果を提供
S118

[図4]


スタート
S11
トラヒックを収集し、分析サイトに転送
S12
トラヒックを変換部、生成部、
抽出部の順で振り分け
S13
トラヒックのフォーマットを変換
S14
トラヒックから情報を生成
S15
フィルタリングによりトラヒックを抽出
S16
トラヒックを分析機能に振り分け
S17
トラヒックの分析を実行
S18
トラヒック情報を格納
終了

[図5]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1040
ディスクドライブインタフェース
1050
シリアルポートインタフェース
1060
ビデオアダプタ
1070
ネットワークインタフェース
1080
1090
ハードディスクドライブ
1100
ディスクドライブ
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ
1110
マウス
1120
キーボード
1130
ディスプレイ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/031847

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L12/70(2013.01)i, H04L12/24(2006.01)i, H04L12/26(2006.01)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. H04L12/70, H04L12/24, H04L12/26

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.
Y	小林淳史, フロー計測技術を用いた多目的トラヒック計測技術の検討, 電子情報通信学会技術研究報告(信学技報), 10 July 2009, vol. 109, no. 137, pp. 43-48(IA2009-29), 3. Mediation技術の提案, fig. 7-9, (KOBAYASHI, Atsushi, Multipurpose traffic monitoring with flow-based measurement, IEICE Technical Report), non-official translation (3. Proposal of mediation technical)	1-5
Y	JP 2013-98706 A (NEC CORPORATION) 20 May 2013, paragraphs [0013], [0014], fig. 1 (Family: none)	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 07.10.2019	Date of mailing of the international search report 15.10.2019
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

International application No.
PCT/JP2019/031847

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2008-219685 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 18 September 2008, paragraph [0036], fig. 4 (Family: none)	1-5
Y	八木 毅 他, オーバレイネットワークにおける分散型トラヒックモニタ方式, 電子情報通信学会技術研究報告(信学技報), 09 February 2006, vol. 105, no. 602, pp. 7-12(IN2005-144), 3. 従来の機能集中型トラヒックモニタ方式, 4. 提案の分散型トラヒックモニタ方式, fig. 4, 5, (YAGI, Takeshi et al., A distributed traffic-monitoring scheme for overlay networks, IEICE Technical Report), non-official translation (3. Traditional function-intensive type traffic-monitoring scheme, 4. Proposed distributed type traffic-monitoring scheme)	1-5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０３１８４７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/70(2013.01)i, H04L12/24(2006.01)i, H04L12/26(2006.01)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.　H04L12/70, H04L12/24, H04L12/26

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
Y	小林　淳史, フロー計測技術を用いた多目的トラヒック計測技術の検討, 電子情報通信学会技術研究報告（信学技報）, 2009.07.10, 第109巻, 第137号, pp.43-48(IA2009-29), 3.Mediation技術の提案, 図7-9	1-5
Y	JP 2013-98706 A（日本電気株式会社）2013.05.20, [0013]-[0014], 図１（ファミリーなし）	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
０７．１０．２０１９	１５．１０．２０１９

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）　５Ｘ　３０４７
玉木　宏治
電話番号　０３－３５８１－１１０１　内線　３５９６

Ｃ（続き）．　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
Y	JP 2008-219685 A（日本電信電話株式会社）2008.09.18, [0036],図4（ファミリーなし）	1-5
Y	八木　毅　他，オーバレイネットワークにおける分散型トラヒックモニタ方式，電子情報通信学会技術研究報告（信学技報），2006.02.09，第105巻，第602号，pp.7-12(IN2005-144)，3.従来の機能集中型トラヒックモニタ方式，4.提案の分散型トラヒックモニタ方式，図4,5	1-5