

(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
2019年9月26日(26.09.2019)



(10) 国際公開番号

WO 2019/181550 A1

- (51) 国際特許分類:
H04W 12/12 (2009.01) H04W 4/00 (2018.01)
H04L 12/70 (2013.01) H04W 24/04 (2009.01)
H04L 29/04 (2006.01) H04W 88/18 (2009.01)
H04L 29/14 (2006.01)
- (21) 国際出願番号: PCT/JP2019/009248
- (22) 国際出願日: 2019年3月8日(08.03.2019)
- (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 2018-057081 2018年3月23日(23.03.2018) 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: 原田 貴史 (HARADA, Takafumi); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP). 諸橋 玄武(MOROHASHI, Gembu); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP). 伊藤 宏樹(ITO, Hiroki); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP).
- (74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050014 東京都港区芝三丁目2番1号 セレスティン芝三井ビルディング11階 鈴榮特許総合事務所内 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,

(54) Title: ABNORMAL TRAFFIC ANALYSIS APPARATUS, ABNORMAL TRAFFIC ANALYSIS METHOD, AND ABNORMAL TRAFFIC ANALYSIS PROGRAM

(54) 発明の名称: 異常トラヒック分析装置、異常トラヒック分析方法及び異常トラヒック分析プログラム

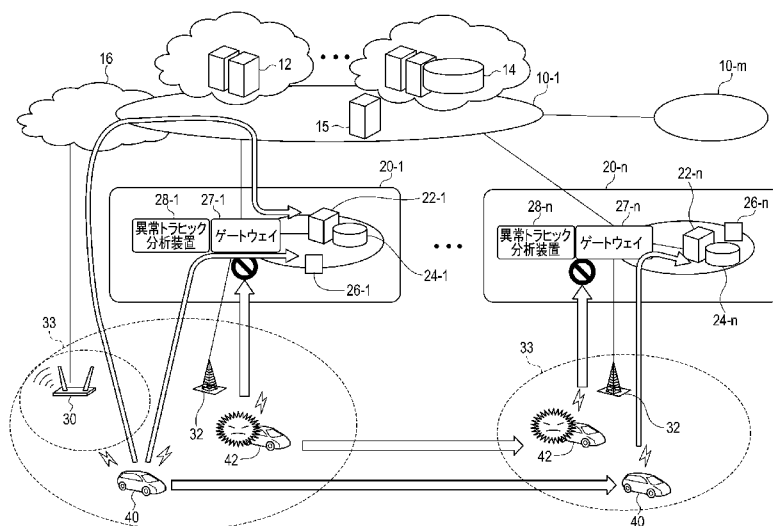


FIG. 1:
27-1, 27-n Gateway
28-1, 28-n Abnormal traffic analysis apparatus

(57) Abstract: This abnormal traffic analysis apparatus has: a reception means that receives traffic from one device via a plurality of communication paths using different communication systems; a plural communication management means that specifies a communication path by which the traffic was transmitted; an analysis method determination means that, in accordance with the communication path specified by the plural communication management means, determines an analysis algorithm for detecting an abnormality in the traffic; an analysis means that uses the analysis algorithm determined by the analysis method determination means to analyze whether the traffic is abnormal traffic; and an analysis result recording means that records the result of the analysis by the analysis means.

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：異常トラヒック分析装置は、1つの機器から異なる通信方式を用いた複数の通信経路を介してトラヒックを受信する受信手段と、前記トラヒックが送信された通信経路を特定する複数通信管理手段と、前記複数通信管理により特定された通信経路に応じて、前記トラヒックの異常を検出するための分析アルゴリズムを決定する分析方法決定手段と、前記分析方法決定手段により決定された分析アルゴリズムを用いて、前記トラヒックが異常トラヒックであるかを分析する分析手段と、前記分析手段による分析結果を記録させる分析結果記録手段とを有する。

明 細 書

発明の名称：

異常トラヒック分析装置、異常トラヒック分析方法及び異常トラヒック分析プログラム

技術分野

[0001] 本発明は、S I E M (Security Information and Event Management)、セキュリティエンジン、ヘテロロジーニクスネットワーク等に適用可能な異常トラヒック分析装置、異常トラヒック分析方法及び異常トラヒック分析プログラムに関する。

背景技術

[0002] 近年、I o T (Internet of Things) 機器の普及により、多数のI o T機器がネットワークに接続され、大量のトラヒックが発生するようになっている。また、I o T機器は、制御などの用途から、I T機器と比べ低遅延が要求される場合がある。このような傾向から、ネットワークや情報処理にかかわるアーキテクチャの変更が必要であり、その選択肢として、複数の通信方法（通信経路）を使い分けることにより、より効率的にネットワークトラヒックを捌くことが提案されている。

[0003] 一方、ネットワークを介して提供される各種サービスや、インフラなどに対して攻撃する不正な通信（サイバー攻撃）は、多種多様な手法を用いたものへと変化し、ますます脅威が増大している。従来では、このような不正な通信に対する対策として、不正な通信（異常トラヒック）を検出する装置がネットワークに設けられている。

先行技術文献

特許文献

[0004] 特許文献1：日本国特許第5 8 4 4 9 3 8号公報

特許文献2：日本国特開2 0 1 8－1 2 1 2 6 2号公報

発明の概要

発明が解決しようとする課題

[0005] 従来では、1つの対象とするIoT機器からのトラヒックは、例えばLTE (Long Term Evolution) など特定の1つの通信方式を用いて送信することを想定している。このため、不正な通信（異常トラヒック）を検出する装置は、トラヒックの送信に用いられる特定の通信方式に最適化された分析アルゴリズムを用いてトラヒックを分析している。

[0006] 従って、ネットワークに大量のトラヒックが発生することに対して、1つのIoT機器からトラヒックを送信する際に、アプリケーション側で通信方式を選択し、発生するトラヒック内容が変更されてしまうと、トラヒックに対して適切な分析ができない状況が発生する可能性がある。

[0007] 本発明は上記課題を解決するためになされたものであり、本発明の目的は、機器からトラヒックが送信される通信経路に関係なく適切な分析をすることが可能な異常トラヒック分析装置、異常トラヒック分析方法及び異常トラヒック分析プログラムを提供することにある。

課題を解決するための手段

[0008] 本発明は、課題を解決するために、以下のような手段を講じている。

[0009] 本発明の第1の態様は、異常トラヒック分析装置は、1つの機器から異なる通信方式を用いた複数の通信経路を介してトラヒックを受信する受信手段と、前記トラヒックが送信された通信経路を特定する複数通信管理手段と、前記複数通信管理により特定された通信経路に応じて、前記トラヒックの異常を検出するための分析アルゴリズムを決定する分析方法決定手段と、前記分析方法決定手段により決定された分析アルゴリズムを用いて、前記トラヒックが異常トラヒックであるかを分析する分析手段と、前記分析手段による分析結果を記録させる分析結果記録手段とを有する。

発明の効果

[0010] 本発明によれば、特定された通信経路に応じた適切な分析アルゴリズムを用いてトラヒックに対して分析を実施するので、異常トラヒックの検知率の向上が可能となる。

図面の簡単な説明

[0011] [図1]図 1 は、本実施形態の通信システムの一例を示す図である。

[図2]図 2 は、本実施形態の通信システムの一例を示す図である。

[図3]図 3 は、本実施形態における異常トラヒック分析装置の構成を示すブロック図である。

[図4]図 4 は、本実施形態における異常トラヒック検知エンジンの機能構成を示すブロック図である。

[図5]図 5 は、本実施形態における監視対象情報管理サーバの動作を示すフローチャートである。

[図6]図 6 は、監視対象情報管理サーバにおいて管理される管理テーブルの一例を示す図である。

[図7]図 7 は、異常トラヒック分析装置の処理の流れを示す図である。

発明を実施するための形態

[0012] 以下、本実施形態について、図面を参照しながら説明する。

図 1 及び図 2 は、本実施形態の通信システムの一例を示す図である。図 1 及び図 2 に示す通信システムは、例えば自動車等を自動走行させるための自律型モビリティシステムを実現するシステムである。自律型モビリティシステムは、例えば自動車等に設けられた各種のセンサや機器等により検出された各種のデータ（プローブデータ）を、例えば、自動車に搭載された I O T 機器 4 0 からサーバに送信する。自律型モビリティシステムは、多数の自動車等の I O T 機器から受信されたプローブデータをリアルタイムでダイナミックマップに反映させ、このダイナミックマップのデータを自動車の I O T 機器に送信する。自動車は、ダイナミックマップのデータをもとに自動走行の制御を実行する。

[0013] 本実施形態における通信システムでは、ネットワークに大量に発生するトラヒックを効率的に送受信するため、自動車等に搭載された I O T 機器とサーバとのデータ（トラヒック）の送受信を、異なる通信方式を用いた複数の通信経路の何れかを用いて行う。本実施形態では、複数の通信方法として、

例えばモバイルネットワーク（移動網 33）を使用するLTE（Long Term Evolution）通信と、インターネット 16を用いたWi-Fi通信の何れかを選択して用いることができるものとする。

[0014] なお、LTE通信とWi-Fi通信に限るものではなく、他の通信方法を用いることもできる。さらに、2つの通信方法に限らず、3つ以上の通信方法を選択して用いることができるようにしても良い。

[0015] 図1に示す通信システムでは、インターネット 16上にコアネットワーク 10（10-1, ..., 10-m）が設けられる。コアネットワーク 10には、例えばクラウドサーバ 12、ダイナミックマップサーバ 14、監視対象情報管理サーバ 15が設けられる。クラウドサーバ 12は、各種サービスに対応するサーバである。クラウドサーバ 12には、Wi-Fi通信方式による通信経路を介してインターネット 16に接続されたIoT機器を識別する認証サーバを含む。

[0016] 監視対象情報管理サーバ 15は、自動車等に搭載された端末（UE：User Equipment）など、監視対象とするIoT機器 40に関する情報を管理するサーバである。監視対象情報管理サーバ 15は、例えば端末が利用するサービス、端末がデータを送受信するエッジ（ローカルネットワーク 20）、端末の現在位置に対応するセル（基地局 32）の対応関係等を管理する。監視対象情報管理サーバ 15は、自動車の走行に伴って端末（IoT機器）が、異なるローカルネットワーク 20に対応するセル（基地局 32）の範囲に移動したことが検出された場合、複数のローカルネットワーク 20（20-1, ..., 20-n）のそれぞれに含まれる異常トラヒック分析装置 28（28-1, ..., 28-n）に対して、対象とするIoT機器が移動したことを通知するメッセージを同報配信する。

[0017] また、監視対象情報管理サーバ 15は、監視対象とするIoT機器について、認証サーバ及び移動網 33内に設けられた移動網の管理サーバ（図示せず）からのメッセージを受信して、IoT機器を特定する一意の識別子（IoT識別子）と対応づけて、監視対象とするIoT機器のWi-Fi通信方

式による通信とLTE通信方式による通信の状況を統合的に管理する。

[0018] ダイナミックマップサーバ14は、複数のIoT機器から受信されるデータ（プローブデータ）をもとにダイナミックマップを作成して、ダイナミックマップデータを端末（IoT機器）に配信する。ダイナミックマップサーバ14は、例えば、ローカルネットワーク20（20-1, ..., 20-n）のダイナミックマップサーバ24（24-1, ..., 24-n）が管理するダイナミックマップより上位のダイナミックマップを対象とする。

[0019] ローカルネットワーク20（20-1, ..., 20-n）は、通信システム（自律型モビリティシステム）をエッジコンピューティング方式により実現するためのネットワークである。すなわち、コアネットワーク10よりもIoT機器（端末）に近い位置に、自律型モビリティシステムのサービスを提供するネットワークスライスを構成している。これにより、IoT機器とサーバとの間の低遅延通信を実現している。エッジコンピューティング方式による通信システムでは、サービスを提供するエッジサーバ22（22-1, ..., 22-n）が、複数のローカルネットワーク20-1, ..., 20-nに分散して配置される。

[0020] 図2には、1つのローカルネットワーク20と、例えば自動車に搭載されたIoT機器40との関係を示している。

[0021] ローカルネットワーク20には、自律型モビリティシステムのサービスを提供するために、ダイナミックマップサーバ24、プローブ収集サーバ26、ゲートウェイ27、異常トラヒック分析装置28が配置される。なお、ローカルネットワーク20-1, ..., 20-nは、それぞれ同様に構成されるものとして、個々について詳細な説明を省略する。

[0022] ダイナミックマップサーバ24は、プローブ収集サーバ26により収集される複数のIoT機器40からのデータ（プローブデータPD）をもとにダイナミックマップを作成して、ゲートウェイ27を通じて、ダイナミックマップデータDMDをIoT機器40に配信する。ダイナミックマップサーバ24は、コアネットワーク10に設けられたダイナミックマップサーバ14

よりもローカルな範囲のダイナミックマップを管理する。

[0023] プローブ収集サーバ26は、複数のIoT機器40から送信されるデータ（プローブデータPD）を、ゲートウェイ27を通じて受信して記録する。プローブ収集サーバ26は、IoT機器40から収集したプローブデータをダイナミックマップサーバ24に提供する。プローブデータには、自動車の走行位置、車速、ブレーキング、燃費など、様々なデータを含む。

[0024] ゲートウェイ27は、ローカルネットワーク20（ネットワークスライス）と他のネットワークとを接続する。ゲートウェイ27は、例えば、Wi-Fiアクセスポイント30と接続されたIoT機器40からのデータを、インターネット16を通じて受信する。また、ゲートウェイ27は、基地局32と接続されたIoT機器40からのデータを、移動網33を通じて受信する。ゲートウェイ27は、異常トラヒック分析装置28と連携し、異常トラヒック分析装置28による分析によって異常と判断された、例えば悪意のあるIoT機器42から送信される異常トラヒックを遮断する機能を有する。

[0025] 異常トラヒック分析装置28は、ゲートウェイ27と連携して動作し、異常トラヒックを検出するための異常トラヒック検知エンジンとして動作する。異常トラヒック分析装置28は、ゲートウェイ27を通じて送受信されるトラヒック（ミラーリングトラヒック）を入力して分析し、例えば悪意のあるIoT機器42から送信される異常トラヒックの検知・判断を実行する。

[0026] 図3は、本実施形態における異常トラヒック分析装置28の構成を示すブロック図である。

異常トラヒック分析装置28は、プログラムを実行するコンピュータを備えており、プロセッサ28A、メモリ28B、通信インタフェース28C、記憶装置28Dを有する。

[0027] プロセッサ28Aは、例えばCPU（Central Processing Unit）であり、メモリ28Bに記憶されたプログラムを実行することで、異常トラヒック分析装置28の各部を制御する。プロセッサ28Aは、異常トラヒック分析プログラムPを実行することで、ゲートウェイ27を通じて送受信される異常

トラヒックを検出するための異常トラヒック検知エンジン（図４に示す）を実現する。異常トラヒック検知エンジンには、機能モジュール及びデータベースを含む。

[0028] メモリ２８Ｂは、プロセッサ２８Ａによる処理の作業エリアとして使用され、プログラムやデータが記憶される。

[0029] 通信インタフェース２８Ｃは、プロセッサ２８Ａのもとで通信を制御する。

[0030] 記憶装置２８Ｄは、例えばＨＤＤ（Hard Disk Drive）またはＳＳＤ（Solid State Drive）であり、プロセッサ２８Ａにより実行されるプログラム、各種データが記憶される。記憶装置２８Ｄに記憶されるプログラムには、異常トラヒック分析プログラムＰを含む。また、異常トラヒック分析プログラムＰの実行に伴い、トラヒックデータデータベースＤＢ１、ＵＥ別脅威レベルデータベースＤＢ２、分析結果ログＤＢ３等が記憶される。

[0031] 図４は、本実施形態における異常トラヒック検知エンジン５０の機能構成を示すブロック図である。異常トラヒック検知エンジン５０は、プロセッサ２８Ａにより異常トラヒック分析プログラムＰを実行することにより実現される。

[0032] 異常トラヒック検知エンジン５０の機能モジュール５２には、トラヒック受信解析部Ｍ１、分析方法決定部Ｍ２、分析部Ｍ３、分析結果取得部Ｍ４、複数通信管理部Ｍ５が含まれる。また、機能モジュール５２により処理されるデータを記憶するデータベース５４として、トラヒックデータデータベースＤＢ１、ＵＥ別脅威レベルデータベースＤＢ２、分析結果ログＤＢ３が設けられる。

[0033] トラヒック受信解析部Ｍ１は、ゲートウェイ２７に送受信されるトラヒックと同じトラヒック（ミラーリングトラヒック）を受信する。トラヒック受信解析部Ｍ１により受信されるトラヒックは、１つのＩｏＴ機器４０から異なる通信方式（ＬＴＥ通信、Ｗｉ－Ｆｉ通信）を用いた複数の通信経路を介して受信されたトラヒックを含む。トラヒック受信解析部Ｍ１は、トラヒッ

クデータの記録、トラヒック（ヘッダ部及びペイロード部）についての解析、複数通信管理部M5に対するパケットの通信経路の問い合わせ、通信経路を示すデータを含むエントリデータの生成等を実行する。

[0034] 分析方法決定部M2は、複数通信管理部M5により特定された通信経路に応じて、トラヒックの異常を検出するための分析アルゴリズム、及び分析アルゴリズムに従う分析に使用されるパラメータを決定する。

[0035] 分析部M3は、トラヒックデータに対する分析を実行する。分析部M3は、トラヒックが送信される複数の通信経路（通信方法）のそれぞれに対応する複数の分析アルゴリズムを有し、分析方法決定部M2によって決定された分析アルゴリズム及びパラメータに応じてトラヒックに対する分析を実行する。

[0036] 分析結果取得部M4は、分析部M3による分析結果を取得して記録させる。

[0037] 複数通信管理部M5は、トラヒック受信解析部M1により受信されるトラヒックの通信経路を管理し、トラヒック受信解析部M1からの問い合わせに応じて通信経路を特定する。

[0038] 次に、本実施形態の通信システムにおける異常トラヒックの検出のための動作について説明する。

まず、監視対象情報管理サーバ15によるIoT機器40のWi-Fi通信方式による通信とLTE通信方式による通信の状況を統合的に管理する処理について説明する。

[0039] 図5は、本実施形態における監視対象情報管理サーバ15の動作を示すフローチャートである。ここでは、図5に示すUE情報管理処理（ステップS2）について説明する。図6は、監視対象情報管理サーバ15において管理される管理テーブルの一例を示す図である。

[0040] IoT機器40は、例えば自機器の動作状況や自動車の位置などに応じて通信経路（通信方法）を切り替えて、例えばプローブデータの送信を継続する。

- [0041] 監視対象情報管理サーバ15は、IoT機器40の動作状況を監視するため、IoT機器40がLTE通信を利用する場合には、移動網33の管理サーバからのメッセージを受信する。管理サーバからのメッセージでは、UE識別情報が通知される（ステップS21）。
- [0042] 監視対象情報管理サーバ15は、UE識別情報の通知に応じて、管理テーブルにIoT機器40に固有のIoT識別子（UE情報）と通信回線に対応する識別子や属性情報を対応させて保持する。通信回線に関する識別子は、例えばIMSI（International Mobile Subscriber Identity）と対応づけた端末識別子（UE識別子）とする。また、メッセージ中のIPアドレス／UE状態の値で、LTE IPアドレス／接続状態を示す属性情報となるデータを更新する（ステップS22）。Wi-Fiについては、認証サーバによって認証され、Wi-Fi識別子とIPアドレスの対応が特定されてメッセージにより通知される。IoT識別子に対応するIMSI及びWi-Fi識別子が示すIoT機器では、予め使用できる通信経路（ここでは、LTE通信、Wi-Fi通信）が特定されている。従って、管理テーブルでは、LTE通信とWi-Fi通信のそれぞれの使用状況を示すデータを、IoT識別子により紐付けて管理する。前述の図6に示す管理テーブルを保持しているため、IMSIやWi-Fi識別子が逐次、更新されることにより、IoT機器40が複数の通信経路の何れかに切り替えて用いた際に、トラヒックがどの通信方式による通信経路を通じて送信されたか特定することが可能になる。図6に示す管理テーブルの情報が更新されるたびに逐次的に異常トラヒック分析装置28（本実施形態におけるセキュリティエンジン）の複数通信管理部M5に対して送付することにより、トラヒックを分析する際にどのIPアドレスのトラヒックがどの通信方式かを検索することができる。
- [0043] 監視対象情報管理サーバ15は、IoT機器40の動作状況を監視するため、IoT機器40がWi-Fi通信を利用する場合には、クラウドの認証サーバからのメッセージを受信する。認証サーバ（Wi-Fi認証機能）からのメッセージでは、Wi-Fi識別子とWi-Fi IPアドレスが通知

される（ステップS21）。

[0044] 監視対象情報管理サーバ15は、メッセージにより通知されたWi-Fi識別子とWi-FiIPアドレスをもとに、IoT識別子（UE情報）に対応するWi-Fi識別子やWi-FiIPアドレスを更新する（ステップS23）。

[0045] こうして、管理テーブルでは、IoT識別子により特定されるIoT機器が使用する通信経路の状況が管理される。従って、異常トラフィック分析装置28において受信されるトラフィックに含まれるIoT機器に固有の識別子をもとに、管理テーブルを参照することにより、トラフィックが送信された通信経路（通信方法）を特定することができる。

[0046] 次に、本実施形態における異常トラフィック分析装置28の動作について、図4及び図7を参照しながら説明する。図7は、異常トラフィック分析装置28（異常トラフィック検知エンジン50）の処理の流れを示す図である。

[0047] （1）まず、トラフィック受信解析部M1は、トラフィックを受信すると、トラフィックデータD2を生成してトラフィックデータベースDB1へ書き出す。

[0048] （2）トラフィック受信解析部M1は、トラフィックに対して構文解析して、ヘッダ部に付加された送信元とするIoT機器に固有の識別子の抽出の他、分析対象のパケットの選別、IP（internet protocol）パケットヘッダにある5tuple情報（送信元アドレス、宛先アドレス、送信元ポート番号、宛先ポート番号、プロトコル情報）等の共通情報と、ペイロード情報等を取得する。IoT機器に固有の識別子は、例えばIPアドレスあるいはIoT機器の端末識別子（UE識別子）である。

[0049] トラフィック受信解析部M1は、IoT機器に固有の識別子をもとに、複数通信管理部M5にトラフィックの通信経路を問い合わせる。複数通信管理部M5は、トラフィック受信解析部M1からの問い合わせに応じて、監視対象情報管理サーバ15に通信経路を問い合わせる。

[0050] 監視対象情報管理サーバ15は、複数通信管理部M5からのIoT機器に固有の識別子をもとにした問い合わせを受信し（ステップS1）、IoT機

器に固有の識別子に応じた問い合わせ種別を判別する（ステップS 1 2）。

[0051] 複数通信管理部M 5 から受信した識別子が端末識別子（U E 識別子）の場合、監視対象情報管理サーバ1 5 は、管理テーブルを参照して、U E 識別子に対応するL T E I P アドレスとW i - F i I P アドレスをもとに通信経路を特定する（ステップS 1 3）。

[0052] 一方、複数通信管理部M 5 から受信した識別子がI P アドレスの場合、監視対象情報管理サーバ1 5 は、管理テーブルを参照して、受信したI P アドレスに対応するU E 識別子と通信経路を特定する（ステップS 1 4）。

[0053] 監視対象情報管理サーバ1 5 は、特定した通信経路を示すデータを複数通信管理部M 5 に返却する。

[0054] 異常トラヒック分析装置2 8 の複数通信管理部M 5 は、監視対象情報管理サーバ1 5 から通知された通信経路（通信方法）をトラヒック受信解析部M 1 に通知する。トラヒック受信解析部M 1 は、複数通信管理部M 5 から取得された通信方式（通信経路）を示すデータをエントリデータD 1 に加える。

[0055] なお、前述した説明では、複数通信管理部M 5 は、トラヒック受信解析部M 1 からの要求に応じて、監視対象情報管理サーバ1 5 に対して問い合わせるとしているが、監視対象情報管理サーバ1 5 から管理テーブルを取得しておき、この管理テーブルを参照して通信経路（通信方法）を特定するようにしても良い。管理テーブルのデータは、特定の範囲にあるI o T 機器について、状況の変化があった場合に監視対象情報管理サーバ1 5 から取得することができる。

[0056] （3）トラヒック受信解析部M 1 は、さらに、構文解析により得られた各情報、複数通信管理部M 5 により特定された通信経路を示すデータとを含むエントリデータD 1 を生成して、分析方法決定部M 2 へ引渡す。

[0057] （4）分析方法決定部M 2 は、受け取ったエントリデータD 1 をもとに、分析部M 3 における分析で用いる分析アルゴリズム及びパラメータを決定し、これらの分析方法を示すデータをエントリデータD 1 に付加して分析部M 3 へ引渡す。すなわち、トラヒックが送信された通信経路（通信方法）に応

じた、最適な分析アルゴリズムとパラメータが決定され、分析部M3に指示される。

[0058] (5) 分析部M3は、受け取ったエントリデータD1に対応するトラヒックデータD2を、トラヒックデータベースDB)から取得する。

[0059] (6) 分析部M3は、分析方法決定部M2において決定された分析方法(分析アルゴリズム、パラメータ)を用いて、エントリデータD1について分析し、その分析結果D3及びエントリデータD1を分析結果取得部M4へ引渡す。分析部M3は、例えば攻撃検知の詳細度(次数)の再設定を繰り返しながら分析して、対象エントリ別の脅威レベルを判定する分析を実行する。分析の具体例については後述する。

[0060] (7) 分析結果取得部M4は、受け取った分析結果D3から対象エントリ別脅威レベルD4(後述する)を取得して、監視対象のIoT機器の脅威レベルを決定するためのルールに適用してUE別脅威レベルを決定し、UE別脅威レベルデータベースDB2を更新する。

[0061] (8) 分析結果取得部M4は、更に、受け取った分析結果D3を分析結果ログDB3へ保存する。

[0062] (9) 分析結果取得部M4は、分析結果D3から対象エントリ別脅威レベルD4を取得し、次の分析が必要な該当エントリデータD1および対象エントリ別脅威レベルD4を分析方法決定部M2へ引渡す。

[0063] なお、(3) 分析方法決定部M1は、1つ前の分析次数および対象エントリ別脅威レベルと該当エントリデータD1を、分析次数決定ルールにより分析方法を決定して分析方法が付加されたエントリデータを分析部M3へ引渡す。

[0064] ここで、分析部M3による分析の具体例について説明する。

UE別脅威レベルデータベースDB2には、過去の通信を対象として、発信元を特定する情報(例えばIPアドレスや端末ID)に紐づけて、一次検知(分析A)の検知結果、二次検知(分析B)の検知結果、…といった具合に、攻撃検知の詳細度(以下、次数ともいう)ごとに、攻撃検知の結果が記

憶されている。これに加え、UE別脅威レベルデータベースDB2には、詳細度ごとの攻撃検知結果から導き出される脅威レベルが対応付けられて記憶されている。

[0065] 脅威レベルは、0または1の2値としてもよいし、3値以上の数値を設定してもよい。例えば脅威レベルに10種類の数字0, 1, ..., 9を設定し、数字が大きければ大きいほど悪性度が強いことを意味するものとし、脅威レベルカラムの数字が9であれば明らかな悪性としてもよい。

[0066] UE別脅威レベルデータベースDB2には、少なくとも、過去に受信した情報の発信元（例えばIPアドレスや端末ID）と過去に受信した情報の脅威レベルとが対応付けられてエントリデータとして予め記憶されているものとする。

[0067] 分析部M3は、UE別脅威レベルデータベースDB2の各エントリと特定された発信元とを照合し、受信した情報に対する攻撃検知の詳細度を決定する。より具体的には、分析部M3は、発信元が特定されたトラヒックに対し、これと同一の発信元に該当するエントリがUE別脅威レベルデータベースDB2に存在するか否かを確認する。分析部M3は、例えば以下のような分析次数決定ルール（1）（2）で、受信した情報に対する攻撃検知の詳細度を決定してもよい。

[0068] （1）具体例

UE別脅威レベルデータベースDB2に対応するエントリがなかった場合、詳細度（次数）を1次と設定する。一方、UE別脅威レベルデータベースDB2に対応するエントリがあった場合、詳細度（次数）をエントリが示す脅威レベルの一つ上の次数に設定する。

[0069] （2）具体例

UE別脅威レベルデータベースDB2に対応するエントリがなかった場合、詳細度（次数）を1次と設定する。一方、UE別脅威レベルデータベースDB2に対応するエントリがあった場合、詳細度（次数）をエントリが示す脅威レベルと等しい次数に設定する。

[0070] 本実施形態の異常トラヒック分析装置28では、トラヒックが送信された通信経路（通信方法）に応じて、攻撃検知アルゴリズムと詳細度（次数）が決定されるものとする。本実施例で用いることができる攻撃検知アルゴリズムとしては、例えばルールベース攻撃検知、ポートスキャンの検知、利用ポートの変化検知、トラヒック流量の変化検知、パケット受信タイミングの変化検知、DPI、時系列データとして取得されたデータを用いて予測されたデータと、実測されたデータとのはずれ具合で異常を検知する攻撃検知などが挙げられる。攻撃検知アルゴリズムが詳細かつ高コストであるほど、詳細度（次数）が高く設定される。

[0071] 次に、分析部M3は、受信したトラヒックに対して、決定された詳細度（次数）（分析パラメータ）に基づく攻撃検知を実行する。

[0072] 攻撃検知の結果が正常であった場合、分析部M3は、分析結果D3を分析結果取得部M4に渡す。分析結果取得部M4は、発信元を特定する情報と検知結果（対象エントリ別脅威レベルD4）を分析結果ログDB3およびUE別脅威レベルデータベースDB2に保存する。分析結果ログDB3には、アノマリ識別子、タイムスタンプ、発信元を特定する情報（IPアドレスや端末ID）、詳細度ごとの検知結果、詳細度ごとの検知回数、最終検知結果、対処済フラグなどが保存される。

[0073] 一方、攻撃検知の結果が正常でない場合（懸念有、または異常有であった場合）、分析部M3は、受信したトラヒックに対する高次の攻撃検知の必要性を判断する。高次の攻撃検知の必要性があると判断されなかった場合、分析結果取得部M4は、分析部M3による分析結果として、発信元を特定する情報と、検知結果を分析結果ログDB3およびUE別脅威レベルデータベースDB2に保存する。

[0074] 攻撃検知の結果が正常でない場合として、具体的には以下のようなケース（1）（2）が考えられる。（1）該当の通信が異常（不正）であることが明白であるため、さらに高次の攻撃検知を実行する必要性が乏しい。例えば、前述の脅威レベルカラムの数字が9である場合などには、該当の通信が悪

性であることが明白であるため、さらに高次の攻撃検知を省略することができ、計算リソースを効果的に用いることができる。(2)すでに最高次の攻撃検知が実行されており、これよりも高次の攻撃検知が実行できない。

[0075] 一方、高次の攻撃検知の必要性があると判断された場合、分析部M3は、攻撃検知の結果に基づいて、受信した情報に対する攻撃検知の詳細度を再度決定する。分析部M3は、再度決定された詳細度(次数)に基づく攻撃検知を再度実行する。攻撃検知の結果が正常でないと判断される場合、分析部M3は、さらに高次の攻撃検知の必要性を判断する。このように、攻撃検知の結果が正常でないと判断される限りにおいて、繰り返し実行される。分析部M3の詳細度(次数)の再決定方法として以下の具体的方法(1)~(4)が考えられる。

[0076] (1) 具体例

対象の攻撃検知の詳細度(次数)を常に1増やす。

[0077] (2) 具体例

攻撃検知アルゴリズムの出力が、正常/懸念有り/異常有りの3段階で表現される場合、

出力=懸念有り→判断結果=Y e s (次数を1増やす)

出力=異常有り→判断結果=Y e s (次数を2増やす)

(3) 具体例

攻撃検知アルゴリズムの出力が、正常/懸念有り/異常有りの3段階で表現される場合、

出力=懸念有り→判断結果=N o (次数を増やさない→S 1 5 a N→エンド)

出力=異常有り→判断結果=Y e s (次数を1増やす)

(4) 具体例

攻撃検知アルゴリズムの出力が、異常の有無を数値で表現する場合。例えば、攻撃検知アルゴリズムの出力が0.0~1.0であって、値が1.0に近づくほど異常性が高く、異常有無判断の閾値が0.5だった場合。

[0078] 出力＝0.5以上0.6未満→判断結果＝Ｙｅｓ（次数を1増やす）

出力＝0.6以上0.7未満→判断結果＝Ｙｅｓ（次数を2増やす）

出力＝0.7以上0.8未満→判断結果＝Ｙｅｓ（次数を3増やす）

出力＝0.8以上0.9未満→判断結果＝Ｙｅｓ（次数を4増やす）

出力＝0.9以上→判断結果＝Ｙｅｓ（次数を5増やす）

本実施例の異常トラヒック分析装置28によれば、危険性の低いＩｏＴ機器（機器）については、早々に攻撃検知を打ち切るため、計算リソースが無駄にならない。

[0079] また、明らかに不正なＩｏＴ機器についても同様に、早々に攻撃検知を打ち切るため、計算リソースが無駄にならない。

[0080] また、該当のＩｏＴ機器の危険性がグレーゾーンにある場合は、処理を繰り返し実行することにより、攻撃検知の信頼性が担保される。

[0081] また、ＵＥ別脅威レベルデータベースＤＢ２にエントリとして登録されているＩｏＴ機器については、登録済みの脅威レベルに応じた詳細度が最初に設定されるため、詳細度の低い攻撃検知が適宜スキップされ、計算リソースが無駄にならない。

[0082] このように、本実施例の異常トラヒック分析装置28によれば、計算リソースを効果的に用いることができる。

[0083] なお、前述したトラヒックに対する分析は一例であって、他の分析を対象とすることができる。その場合、前述と同様にして、トラヒックの通信経路を特定し、それにあわせて、分析アルゴリズムおよび分析パラメータを選択する。例えば、ＤＯＳ（Denial of Service attack）攻撃検知のための分析をする場合において、閾値を通信方式に応じて変更する。

[0084] このようにして、本実施形態における異常トラヒック分析装置28では、トラヒックが送信された通信経路（通信方法）を特定し、通信経路（通信方法）に応じた分析アルゴリズム及び分析パラメータを用いてトラヒックに対する分析を実行する。従って、ＩｏＴ機器40のアプリケーションにより通信経路が変更されたとしても、通信経路に関係なく適切な分析をすることが

可能となり、異常トラヒックの検知率の向上が可能となる。

[0085] また、各実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウェア手段）として、例えば磁気ディスク（フレキシブルディスク、ハードディスク等）、光ディスク（CD-ROM、DVD、MO等）、半導体メモリ（ROM、RAM、フラッシュメモリ等）等の記録媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウェア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含む。本装置を実現する計算機は、記録媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウェア手段を構築し、このソフトウェア手段によって動作が制御されることにより上述した処理を実行する。なお、本明細書でいう記録媒体は、頒布用に限らず、計算機内部あるいはネットワークを介して接続される機器に設けられた磁気ディスクや半導体メモリ等の記憶媒体を含むものである。

[0086] なお、本願発明は、上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合組み合わせた効果が得られる。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適当な組み合わせにより種々の発明が抽出され得る。

符号の説明

[0087] 10（10-1，…，10-m）…コアネットワーク
12…クラウドサーバ
14…ダイナミックマップサーバ
16…インターネット
20（20-1，…，20-n）…ローカルネットワーク
22（22-1，…，22-n）…エッジサーバ

24 (24-1, ..., 24-n) ...ダイナミックマップサーバ

26 (26-1, ..., 26-n) ...プローブ収集サーバ

27 (27-1, ..., 27-n) ...ゲートウェイ

28 (28-1, ..., 28-n) ...異常トラヒック分析装置

28A ...プロセッサ

28B ...メモリ

28C ...通信インタフェース

28D ...記憶装置

30 ...Wi-Fiアクセスポイント

32 ...基地局

M1 ...トラヒック受信解析部

M2 ...分析方法決定部

M3 ...分析部

M4 ...分析結果取得部

M5 ...複数通信管理部

DB1 ...トラヒックデータデータベース

DB2 ...UE別脅威レベルデータベース

DB3 ...分析結果ログ

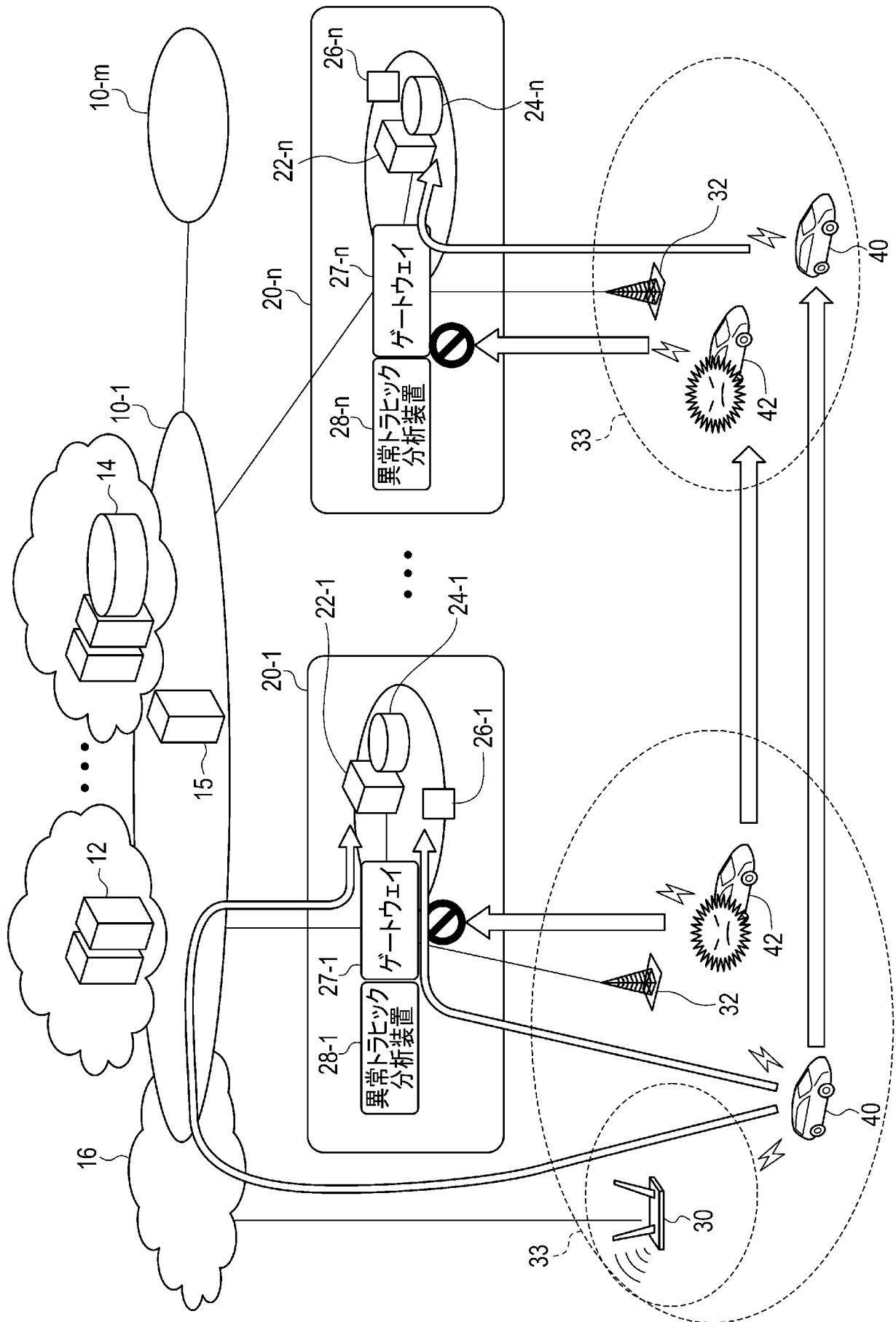
請求の範囲

- [請求項1] 1つの機器から異なる通信方式を用いた複数の通信経路を介してトラヒックを受信する受信手段と、
- 前記トラヒックが送信された通信経路を特定する複数通信管理手段と、
- 前記複数通信管理手段により特定された通信経路に応じて、前記トラヒックの異常を検出するための分析アルゴリズムを決定する分析方法決定手段と、
- 前記分析方法決定手段により決定された分析アルゴリズムを用いて、前記トラヒックが異常トラヒックであるかを分析する分析手段と、
- 前記分析手段による分析結果を記録させる分析結果記録手段と
- を有する異常トラヒック分析装置。
- [請求項2] 前記複数通信管理手段は、前記トラヒックに含まれる識別子をもとに、前記機器による通信の状況を管理する外部サーバに問い合わせ、前記トラヒックが送信された通信経路を示すデータを取得する請求項1記載の異常トラヒック分析装置。
- [請求項3] 前記分析方法決定手段は、前記複数通信管理手段により特定された通信経路に応じた分析アルゴリズムで使用する分析パラメータを、前記通信経路に応じて変更する請求項1記載の異常トラヒック分析装置。
- [請求項4] 1つの機器から異なる通信方式を用いた複数の通信経路を介してトラヒックを受信する受信工程と、
- 前記トラヒックが送信された通信経路を特定する複数通信管理工程と、
- 前記複数通信管理工程により特定された通信経路に応じて、前記トラヒックの異常を検出するための分析アルゴリズムを決定する分析方法決定工程と、
- 前記分析方法決定工程により決定された分析アルゴリズムを用いて

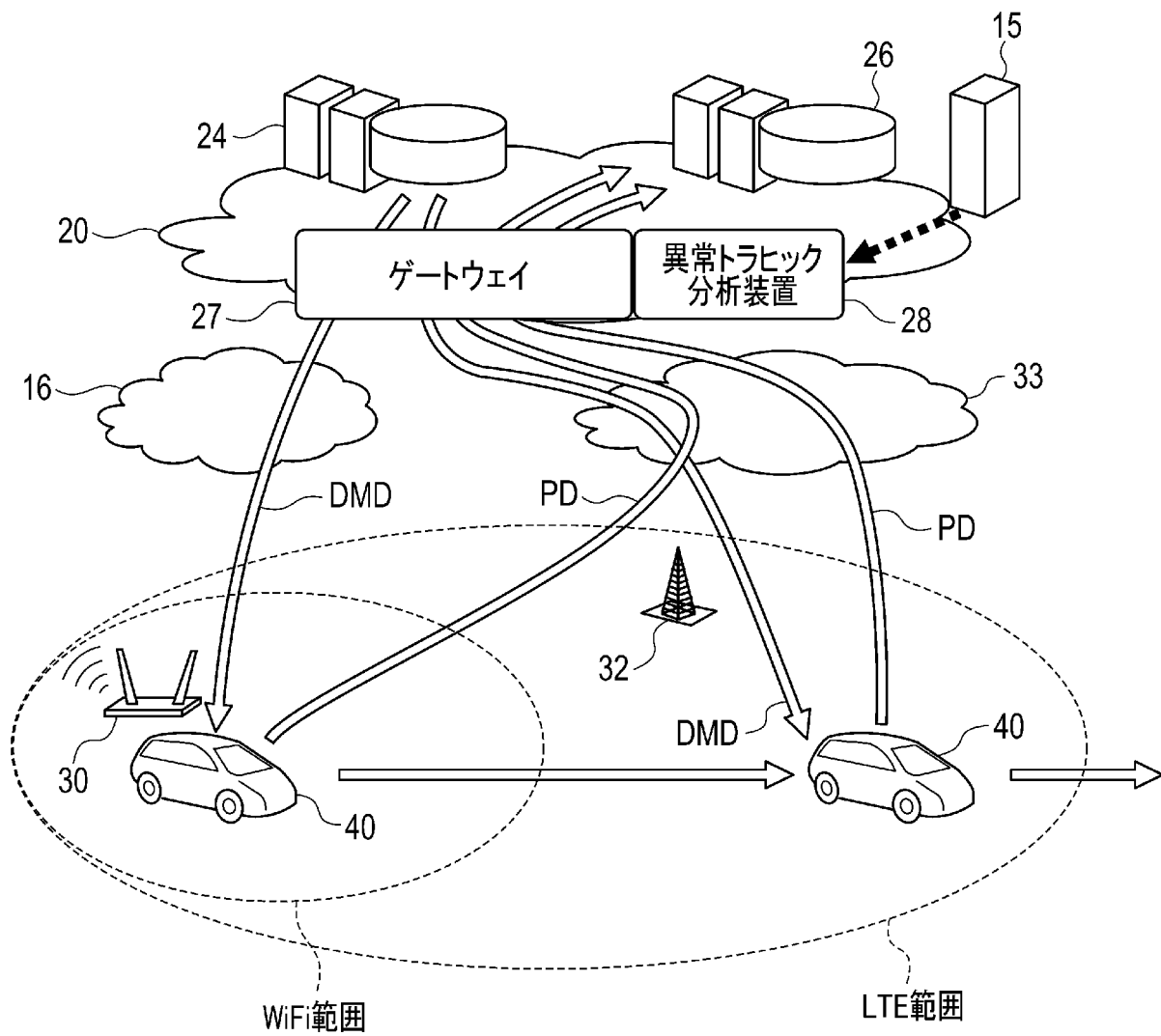
、前記トラヒックが異常トラヒックであるかを分析する分析工程と、
前記分析工程による分析結果を記録させる分析結果記録工程とを有する異常トラヒック分析方法。

[請求項5] 請求項1乃至3の何れかに記載の異常トラヒック分析装置が具備する各手段が行う処理を、当該異常トラヒック分析装置が備えるコンピュータに実行させる異常トラヒック分析プログラム。

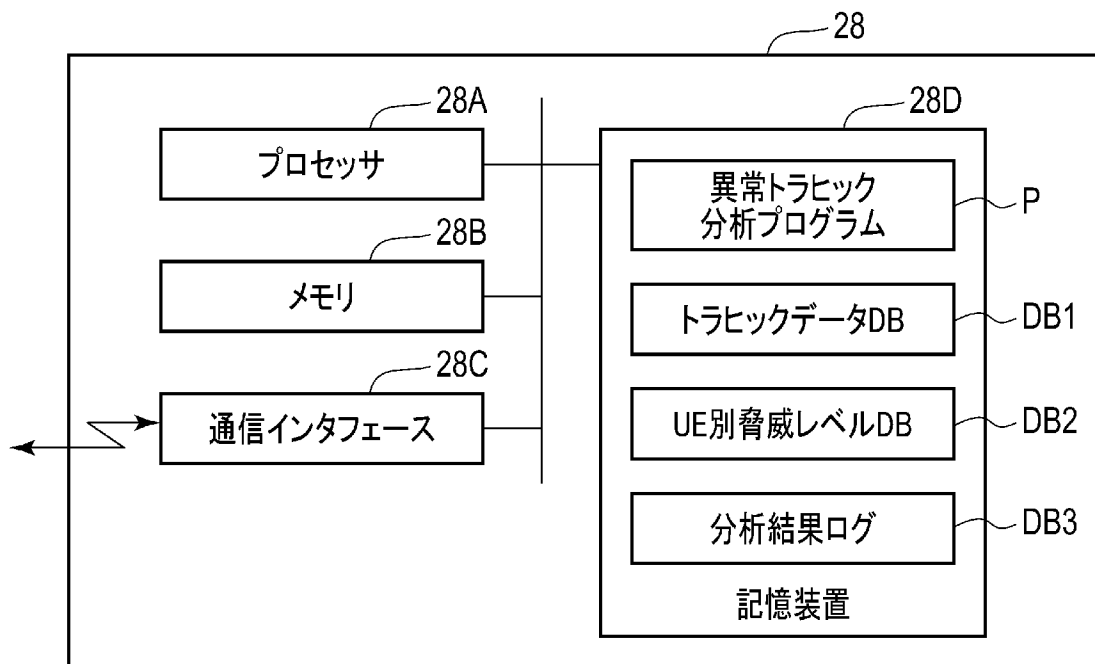
[図1]



[図2]

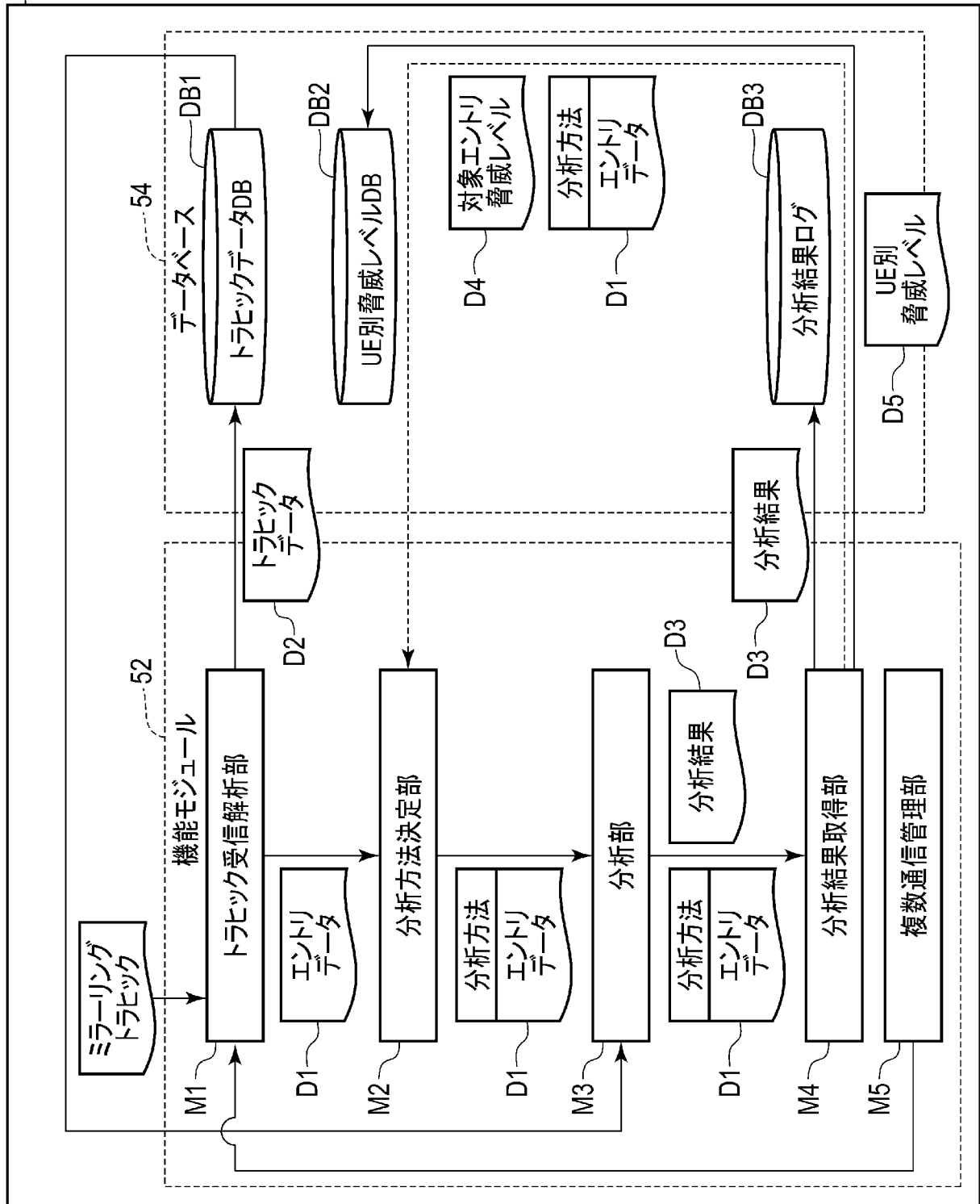


[図3]

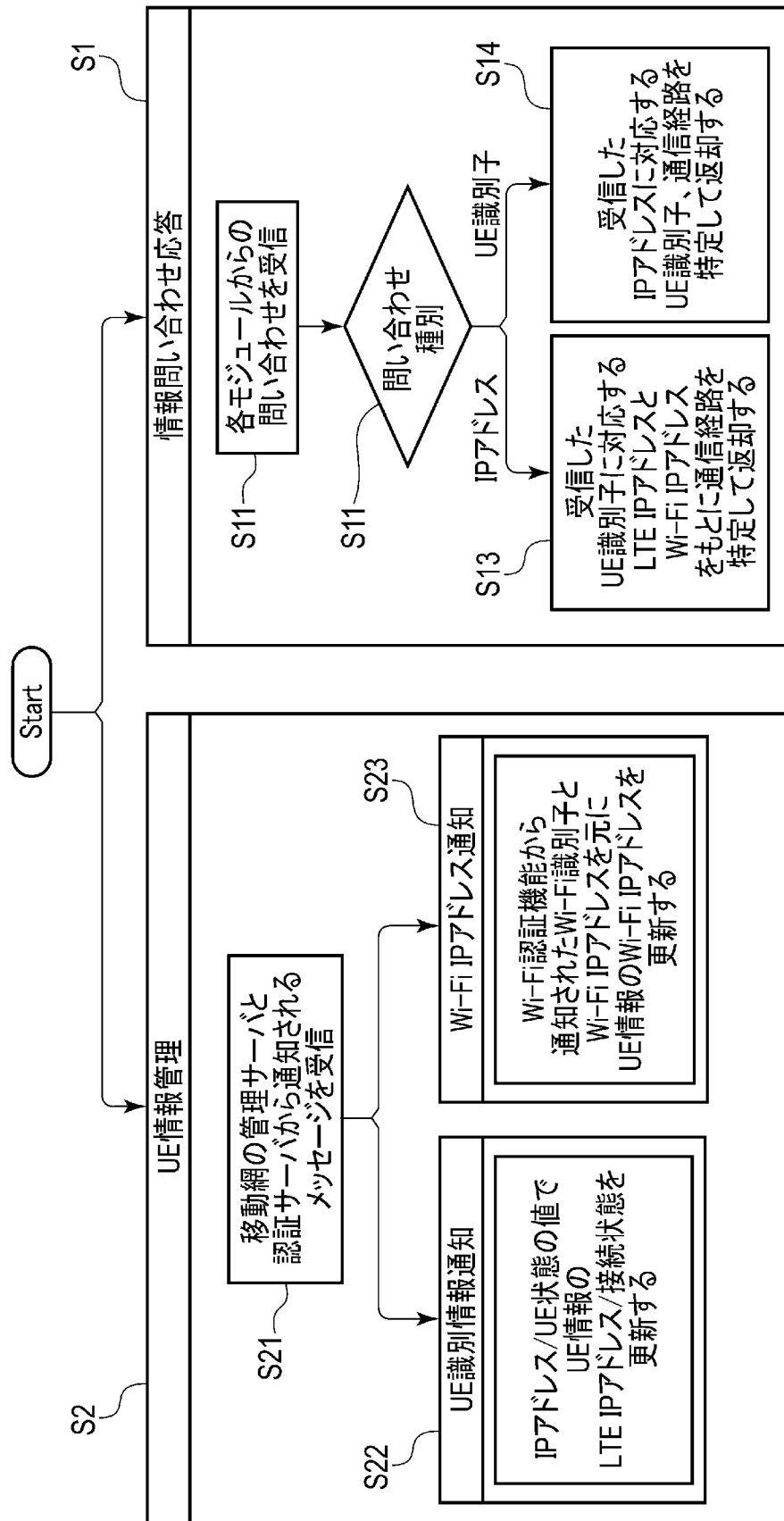


[図4]

50



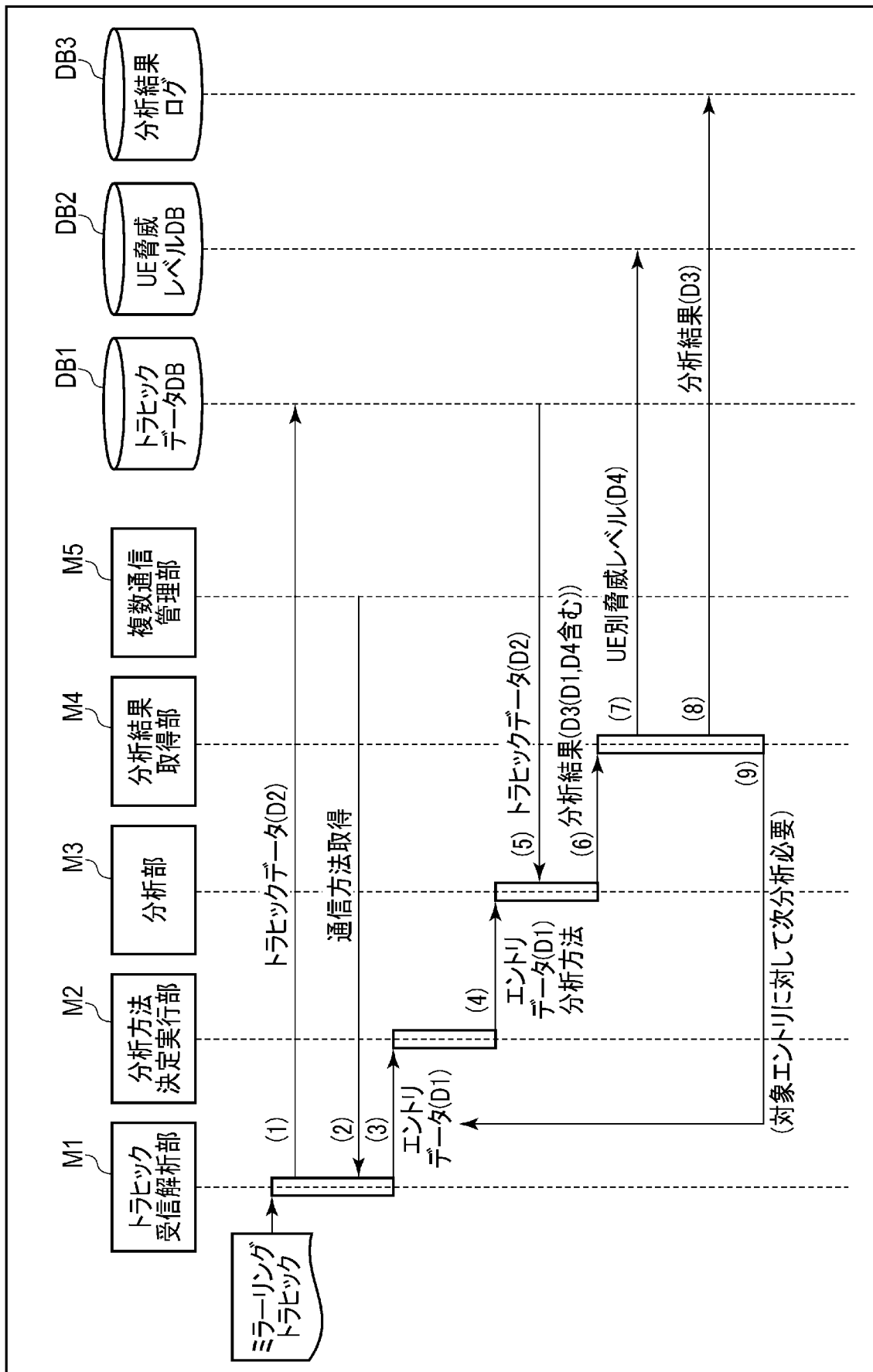
[図5]



[図6]

lot 識別子	IMSI	LTE IPアドレス	接続状態	Wi-Fi 識別子	Wi-Fi IPアドレス	...

[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/009248

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04W12/12 (2009.01) i, H04L12/70 (2013.01) i, H04L29/04 (2006.01) i, H04L29/14 (2006.01) i, H04W4/00 (2018.01) i, H04W24/04 (2009.01) i, H04W88/18 (2009.01) 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. H04W4/00-99/00, H04L12/70, H04L29/04, H04L29/14

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	JP 2011-259014 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 22 December 2011, paragraphs [0013]-[0015], [0030], [0040]-[0048], fig. 1 (Family: none)	1-5
Y	WO 2016/031384 A1 (NEC CORPORATION) 03 March 2016, paragraphs [0025]-[0031], 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
20.05.2019

Date of mailing of the international search report
28.05.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04W12/12(2009.01)i, H04L12/70(2013.01)i, H04L29/04(2006.01)i, H04L29/14(2006.01)i,
H04W4/00(2018.01)i, H04W24/04(2009.01)i, H04W88/18(2009.01)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. H04W4/00-99/00, H04L12/70, H04L29/04, H04L29/14

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	JP 2011-259014 A（日本電信電話株式会社）2011.12.22, [0013]-[0015], [0030], [0040]-[0048], 図1（ファミリーなし）	1-5
Y	W0 2016/031384 A1（日本電気株式会社）2016.03.03, [0025]-[0031], 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

20.05.2019

国際調査報告の発送日

28.05.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

齋藤 浩兵

電話番号 03-3581-1101 内線 3534

5 J

3794