(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7147601号
(P7147601)

(45)発行日　令和4年10月5日(2022.10.5)

(24)登録日　令和4年9月27日(2022.9.27)

(51)国際特許分類

Ｈ０４Ｌ	*12/66*	*(2006.01)*	Ｈ０４Ｌ	12/66
Ｈ０４Ｌ	*12/22*	*(2006.01)*	Ｈ０４Ｌ	12/22
Ｈ０４Ｌ	*43/02*	*(2022.01)*	Ｈ０４Ｌ	43/02

ＦＩ

請求項の数　6　（全24頁）

(21)出願番号　特願2019-15085(P2019-15085)
(22)出願日　平成31年1月31日(2019.1.31)
(65)公開番号　特開2020-123871(P2020-123871A)
(43)公開日　令和2年8月13日(2020.8.13)
審査請求日　令和3年10月7日(2021.10.7)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅 義之
(74)代理人　100133570
弁理士　▲徳▼永 民雄
(72)発明者　野呂 正明
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
審査官　鈴木 香苗

最終頁に続く

(54)【発明の名称】　検査方法および検査システム

(57)【特許請求の範囲】

【請求項１】

サーバにより実行される検査方法であって、前記サーバが、

検査対象の装置宛ての肯定確認応答を破棄するようにパケットフィルタに設定し、

前記パケットフィルタで前記検査対象の装置宛ての肯定確認応答を破棄したタイミングに基づき、前記検査対象の装置が発信したパケットの数を表す第１のパケット数と、前記検査対象の装置が前記サーバに宛てて送信したパケットの数を表す第２のパケット数とを収集し、

前記第１のパケット数および前記第２のパケット数が所定の誤差範囲内で合致しているか否かにより、前記検査対象の装置の不正な通信を検査する、

ことを含む、検査方法。

【請求項２】

前記パケットフィルタが前記検査対象の装置宛ての肯定確認応答を破棄したタイミングは、前記パケットフィルタが前記検査対象の装置宛ての肯定確認応答を２つ連続で破棄したタイミングである、請求項１に記載の検査方法。

【請求項３】

前記パケットフィルタが前記検査対象の装置宛ての肯定確認応答を破棄したタイミングは、前記パケットフィルタが前記検査対象の装置宛ての肯定確認応答を３回以上の所定回数連続で破棄したタイミングである、請求項１に記載の検査方法。

【請求項４】

前記サーバは、受信バッファが一杯であることを示すフラグを立てるように改ざんした肯定確認応答を前記検査対象の装置に返した後で、前記検査対象の装置宛ての肯定確認応答を破棄するように前記パケットフィルタに設定する、請求項１に記載の検査方法。
【請求項５】
前記検査対象の装置は、スイッチのポートに接続しており、
前記サーバは、前記検査対象の装置が接続されている前記スイッチのポートに入力されたパケットの数を前記第１のパケット数として前記スイッチから取得する、
ことを更に含む、請求項１から４のいずれか１項に記載の検査方法。
【請求項６】
サーバと、パケット計数装置とを含む検査システムであって、
前記パケット計数装置は、入力されたパケットの数をポートごとに計数し、前記パケットを宛先のポートに出力し、
前記サーバは、
検査対象の装置宛ての肯定確認応答を破棄するようにパケットフィルタに設定する設定部と、
前記パケットフィルタで前記検査対象の装置宛ての肯定確認応答を破棄したタイミングに基づき、前記検査対象の装置が接続されているポートに入力されたパケットの数を表す第１のパケット数を前記パケット計数装置から取得し、および、前記検査対象の装置がサーバに宛てて送信したパケットの数を表す第２のパケット数を取得する取得部と、
前記第１のパケット数および前記第２のパケット数が所定の誤差範囲内で合致しているか否かにより、前記検査対象の装置の不正な通信を検査する検査部と、を含む、
検査システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、検査方法および検査システムに関する。
【背景技術】
【０００２】
近年、「モノのインターネット（IoT:Internet of Things）」という用語とともに、様々なものに通信機能を搭載してネットワークと接続することが行われている。そして、こうしたＩｏＴ機器からデータを収集し、収集したデータを活用して、これまでに無かったサービス、および、より価値を高めたサービスを提供する試みが成されている。
【０００３】
また、ネットワークのセキュリティに関連する技術が知られている（例えば、特許文献１および特許文献２）。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２０１０－１１２０６号公報
特開２００５－１９３５９０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ＩｏＴ機器がウイルスなどに感染し、他の機器を攻撃してしまうことがある。こうした脅威に対し、例えば、ＩｏＴ機器が十分な機能を有していれば、ＩｏＴ機器にセキュリティ対策ソフトをインストールしたりすることで、対策を講じることができる。しかしながら、ＩｏＴ機器のなかには、セキュリティ対策ソフトをインストールするといった対策を講じることのできない機器も含まれている。そのため、ＩｏＴ機器が不正な通信をしていないか検査することのできる更なる技術の提供が望まれている。
【０００６】

１つの側面では、本発明は、機器が不正な通信を実行していないかを検査することを目的とする。

【課題を解決するための手段】

【０００７】

本発明の一つの態様の検査方法は、サーバが、検査対象の装置宛ての肯定確認応答を破棄するようにパケットフィルタに設定し、パケットフィルタで検査対象の装置宛ての肯定確認応答を破棄したタイミングに基づき、検査対象の装置が発信したパケットの数を表す第１のパケット数と、検査対象の装置がサーバに宛てて送信したパケットの数を表す第２のパケット数とを収集し、第１のパケット数および第２のパケット数が所定の誤差範囲内で合致しているか否かにより、検査対象の装置の不正な通信を検査する、ことを含む。

【発明の効果】

【０００８】

機器が不正な通信を実行していないかを検査することができる。

【図面の簡単な説明】

【０００９】

【図１】例示的なＩｏＴシステムを示す図である。

【図２】実施形態に係るＩｏＴシステムを例示する図である。

【図３】実施形態に係るサーバのブロック構成を例示する図である。

【図４】実施形態に係る検査対象のＩｏＴ機器の不正通信の検査処理の動作フローを例示する図である。

【図５】実施形態に係るトラフィック情報取得処理を例示する図である。

【図６】パケット計数装置により収集される計数情報を例示する図である。

【図７】ＳＮＭＰプロトコルでの問い合わせを例示する図である。

【図８】例示的なＳＮＭＰプロトコルで提供されるパケット数に関する情報を含むオブジェクトを例示する図である。

【図９】パケット分析部により収集される分析情報を例示する図である。

【図１０】パケット分析部が実行するパケット分析処理を例示する図である。

【図１１】経路およびバッファ上のパケットを例示する図である。

【図１２】送信側の装置と受信側の装置との間のＴＣＰによる通信制御を説明する図である。

【図１３】実施形態に係る通信時のトラフィック情報取得処理の動作フローを例示する図である。

【図１４】実施形態に係る接続要求の破棄を説明する図である。

【図１５】別の実施形態に係るパケット分析部の配置を例示する図である。

【図１６】ＴＣＰのバージョンに応じたパケットの送信手順の違いを例示する図である。

【図１７】変形例１に係るＴＣＰの第２のバージョンにおけるトラフィック情報の収集の実行タイミングを例示する図である。

【図１８】変形例１に係る通信時のトラフィック情報取得処理の動作フローを例示する図である。

【図１９】変形例２に係るトラフィック情報の収集の実行タイミングを例示する図である。

【図２０】変形例２に係るトラフィック情報の収集の実行タイミングを更に例示する図である。

【図２１】変形例２に係る通信時のトラフィック情報取得処理の動作フローを例示する図である。

【図２２】変形例３に係るトラフィック情報の収集の実行タイミングを例示する図である。

【図２３】変形例３に係る通信時のトラフィック情報取得処理の動作フローを例示する図である。

【図２４】実施形態に係るサーバまたはパケット分析部を実現するためのコンピュータのハードウェア構成を例示する図である。

【発明を実施するための形態】

【００１０】
以下、図面を参照しながら、本発明のいくつかの実施形態について詳細に説明する。なお、複数の図面において対応する要素には同一の符号を付す。
【００１１】
図１は、例示的なＩｏＴシステム１００を示す図である。図１では、組織内のＩＴ網１５０の下にサーバ１０２と複数のＩｏＴ機器１０１とで形成される別なネットワーク１０５が示されている。サーバ１０２と複数のＩｏＴ機器１０１は、ＩｏＴシステム１００を形成している。ＩｏＴ機器１０１は、例えば、情報を収集する様々な機器であってよく、収集した情報をサーバ１０２に送信する。例えば、ＩｏＴ機器１０１が、温度計や湿度計などのセンサである場合、ＩｏＴ機器１０１は、計測した温度や湿度などの情報を定期的にサーバ１０２に提供してよい。また、例えば、ＩｏＴ機器１０１が、エアコンディショナーのコントローラなどの電化製品に搭載されたマイコンである場合は、電化製品に入力された操作などに関する情報がサーバ１０２に提供されてよい。そして、サーバ１０２は、例えば、ＩｏＴ機器１０１から収集した情報を用いて、組織内のＩＴ網１５０に接続した端末に、様々なサービスを提供してもよい。
【００１２】
ここで、ＩｏＴ機器１０１がウイルスなどに感染し、他の機器を攻撃してしまうことがある。こうした脅威は、例えば、ＩｏＴ機器１０１が十分な機能を有していれば、セキュリティ対策ソフトをインストールしたりすることで、対策を講じることができる。
【００１３】
しかしながら、ＩｏＴ機器１０１のなかには、セキュリティ対策ソフトをインストールするといった対策を講じることのできない機器も含まれている。例えば、ＩｏＴ機器１０１のなかには、独自のオペレーティングシステム（ＯＳ：Operating System）で動作していたり、旧式のＯＳで動作していたり、或いは、そもそもＯＳが無いものもあり、セキュリティ対策ソフトを導入できないことがある。そのため、ＩｏＴ機器の不正な通信を検出することのできる更なる技術の提供が望まれている。
【００１４】
ここで、ＩｏＴ機器１０１は、例えば、図１のサーバ１０２などの特定のホストにデータを上げ続けるといった利用をされることが多く、ＩｏＴ機器１０１は、しばしば特定のホストとのみ通信するように設定される。このような場合に、特定のホストとのみ通信するように設定されているＩｏＴ機器１０１が、ホスト以外の装置と通信していたとすると、そのＩｏＴ機器１０１は不正な通信を行っている可能性が高いと判定することが可能である。
【００１５】
そこで、以下で述べる実施形態では、例えば、ＩｏＴ機器１０１が送信したパケット数と、ＩｏＴ機器１０１からホストに届くパケット数とが所定の誤差範囲内で合致しているかを検査して、ＩｏＴ機器１０１がホスト以外の装置と通信しているか否かを検査する。所定の誤差範囲は、例えば、１％～２％など、ＩｏＴシステムで発生するパケットロスの頻度などを事前に調査することで、許容可能な誤差範囲に設定することができる。そして、例えば、ＩｏＴ機器１０１が送信したパケット数と、ＩｏＴ機器１０１からホストに届くパケット数とが所定の誤差範囲を超えて大きく異なれば、ＩｏＴ機器１０１はホスト以外の他の装置と不正な通信をしている可能性が高いと推定することができる。換言すると、例えば、ＩｏＴ機器１０１が不正な通信をしている場合、ＩｏＴ機器１０１が送信するパケットの数は不正な通信の数だけ増えることになる。一方で、それらの不正な通信のパケットはホストには届かないため、ＩｏＴ機器１０１からホストに届くパケット数に変化はなく、ＩｏＴ機器１０１が送信したパケット数の方が、ＩｏＴ機器１０１からホストに届くパケット数とよりも増えることになる。また、例えば、ＩｏＴ機器１０１が送信したパケット数と、ＩｏＴ機器１０１からホストに届くパケット数とが所定の誤差範囲内で合致していれば、ＩｏＴ機器１０１はホスト以外の他の装置とは通信していないことが推定できる。以下、実施形態を更に詳細に説明する。

【００１６】
図２は、実施形態に係るＩｏＴシステム２００を例示する図である。ＩｏＴシステム２００は、例えば、ＩｏＴ機器１０１と、サーバ２０２と、パケット計数装置２１１と、ハブ（ＨＵＢ）２１２と、パケット分析部２１３とを含む。なお、一実施形態において、ＩｏＴ機器１０１の不正な通信を検査する検査システム２５０は、サーバ２０２と、パケット計数装置２１１と、ハブ（ＨＵＢ）２１２と、パケット分析部２１３を含んでよい。ここで、ＩｏＴ機器１０１は、正常に動作しているときには、サーバ２０２のみと通信するように設定されているものとする。サーバ２０２は、例えば、ＩｏＴ機器１０１から各種の計測データを収集し、ＩＴ網１５０に接続する他の装置などに計測データを用いて様々なサービスを提供してよい。なお、サーバ２０２は、例えば、パケットをルーティングする機能は有していなくてよく、ＩｏＴ機器１０１が送信したパケットは、サーバ２０２を超えてＩＴ網１５０には流れなくてよい。
【００１７】
パケット計数装置２１１は、例えば、ＳＮＭＰ（Simple Network Management Protocol）対応のスイッチであってよく、一例では、インテリジェントスイッチであってよい。パケット計数装置２１１を、一実施形態においては、パケット計数スイッチと呼ぶことがある。パケット計数装置２１１は、例えば、入力されるパケットを、ポートごとにカウントし、パケットを宛先のポートに出力する。ＩｏＴ機器１０１は、例えば、パケット計数装置２１１の特定のポートと接続されていてよい。そのため、ＩｏＴ機器１０１が接続されるポートに対してパケット計数装置２１１がカウントしたパケット数は、そのポートに接続するＩｏＴ機器１０１が送信したパケット数として用いることができる。
【００１８】
パケット分析部２１３は、例えば、プロトコルアナライザであってよい。プロトコルアナライザは、例えば、ネットワークやデータ機器間を流れるデータを解析する装置やプログラムである。パケット分析部２１３は、例えば、入力されたパケットを、パケットの送信元を示すソースアドレスごとにカウントしてよい。なお、ソースアドレスとしては、例えば、ＭＡＣアドレス、またはＩＰアドレスなどを用いることができる。
【００１９】
ハブ２１２は、例えば、リピータハブであってよい。リピータハブは、例えば、受信したパケットを、接続する全ての端末に送信する。従って、図２において、パケット計数装置２１１から入力されたサーバ２０２宛てのパケットは全て、リピータハブによりパケット分析部２１３にも送信される。パケット分析部２１３は、パケットのソースアドレスを分析することで、検査対象のＩｏＴ機器１０１からサーバ２０２に宛てて送信されたパケットの個数を計数することが可能である。
【００２０】
そのため、サーバ２０２は、例えば、パケット計数装置２１１から、検査対象のＩｏＴ機器１０１が送信したパケット数を表す第１のパケット数を取得することができる。また、サーバ２０２は、パケット分析部２１３から、検査対象のＩｏＴ機器１０１がサーバ２０２に送信したパケット数を表す第２のパケット数を取得することができる。その後、サーバ２０２は、例えば、第１のパケット数と第２のパケット数とを比較することにより、検査対象のＩｏＴ機器１０１が不正な通信を行っているか否かを判定することができる。なお、以下で述べる実施形態では、検査対象のＩｏＴ機器１０１が送信したパケット数を表す第１のパケット数、および検査対象のＩｏＴ機器１０１がサーバ２０２に送信したパケット数を表す第２のパケット数をトラフィック情報と呼ぶことがある。
【００２１】
図３は、実施形態に係るサーバ２０２のブロック構成を例示する図である。サーバ２０２は、例えば、制御部３０１、記憶部３０２、および通信部３０３を含む。制御部３０１は、例えばＯＳ３５０、設定部３１１、取得部３１２、および検査部３１３などとして動作する。サーバ２０２の記憶部３０２は、例えば、プログラムおよびデータなどの情報を記憶していてよい。一実施形態においては、サーバ２０２の記憶部３０２は、例えば、後

述する分析情報９００を記憶している。これらの各部の詳細および記憶部３０２に格納されている情報の詳細については後述する。

【００２２】

図４は、実施形態に係る検査対象のＩｏＴ機器１０１による不正な通信の検査処理の動作フローを例示する図である。サーバ２０２の制御部３０１は、例えば、不正通信の検査処理の実行指示が入力されると、図４の検査処理を開始してよい。

【００２３】

ステップ４０１（以降、ステップを“Ｓ”と記載し、例えば、Ｓ４０１と表記する）において制御部３０１は、不正通信を検査するＩｏＴ機器１０１を選択する。例えば、制御部３０１は、ユーザからのＩｏＴ機器１０１の選択を受け付け、ユーザによって選択されたＩｏＴ機器１０１を検査対象として選択してよい。

【００２４】

Ｓ４０２において制御部３０１は、検査対象のＩｏＴ機器１０１と通信中か否かを判定する。検査対象のＩｏＴ機器１０１と通信中でない場合（Ｓ４０２がＮＯ）、フローはＳ４０３に進む。Ｓ４０３において制御部３０１は、図５を参照して後述するトラフィック情報収集処理を実行してトラフィック情報を収集し、フローはＳ４０５に進む。なお、トラフィック情報は、上述のように、例えば、ＩｏＴ機器１０１が不正な通信を実行しているか否かを検査するために用いる情報である。一例では、トラフィック情報は、ＩｏＴ機器１０１が送信したパケット数を表す第１のパケット数と、ＩｏＴ機器１０１からホストに送信されたパケット数を表す第２のパケット数とを含んでよい。

【００２５】

また、Ｓ４０２において検査対象のＩｏＴ機器１０１と接続を確立しており、通信中である場合（Ｓ４０２がＹＥＳ）、フローはＳ４０４に進む。Ｓ４０４において制御部３０１は、図１３を参照して後述する通信時のトラフィック情報収集処理を実行してトラフィック情報を収集し、フローはＳ４０５に進む。

【００２６】

Ｓ４０５において制御部３０１は、例えば、収集したトラフィック情報に基づいて、検査対象のＩｏＴ機器１０１が不正な通信をしているか否かを検査し、本動作フローは終了する。例えば、ＩｏＴ機器１０１が送信したパケット数を表す第１のパケット数と、ＩｏＴ機器１０１からホストに送信されたパケット数を表す第２のパケット数とが所定の誤差範囲内で合致していたとする。この場合、制御部３０１は、ＩｏＴ機器１０１が不正な通信をしていないと判定してよい。一方、例えば、第１のパケット数と、第２のパケット数とが所定の誤差範囲を超えて異なっていたとする（例えば、ＩｏＴ機器１０１が送信したパケット数を表す第１のパケット数の方が所定値以上多い）。この場合、制御部３０１は、ＩｏＴ機器１０１が不正な通信をしていると判定してよい。

【００２７】

（トラフィック情報収集処理）

続いて、図４のＳ４０３で実行されるトラフィック情報の収集処理について説明する。図５は、実施形態に係るトラフィック情報取得処理を例示する図である。制御部３０１は、例えば、図４のＳ４０３に進むと、図５の動作フローを開始してよい。

【００２８】

Ｓ５０１において制御部３０１は、例えば、パケット計数装置２１１から、検査対象のＩｏＴ機器１０１が接続しているポートのパケット数を、第１のパケット数として取得する。なお、制御部３０１は、一実施形態においては、以下の図６～図８で述べるようにして、検査対象のＩｏＴ機器１０１が接続しているポートのパケット数を取得してよい。

【００２９】

図６は、パケット計数装置２１１により収集される計数情報６００を例示する図である。パケット計数装置２１１は、例えば、パケットが入力されると、パケットが入力されたポートの情報と対応付けて、そのパケットのパケット番号を計数情報６００に登録する。なお、一例では、パケット計数装置２１１は、起動時からの累積で入力されたパケットの

情報を計数情報６００に記録してよい。また、パケット計数装置２１１は、例えば、インテリジェントスイッチであってよく、ＳＮＭＰプロトコルで外部と通信する。

【００３０】

図７は、ＳＮＭＰプロトコルでの問い合わせを例示する図である。パケット計数装置２１１は、例えば、メモリなどの記憶装置７０１備えていてよく、記憶装置７０１に計数情報６００を記憶している。そして、サーバ２０２は、例えば、ＧＥＴコマンドとともに、オブジェクト識別子（ＯＩＤ：Object Identifier）と、ポート番号（図７では「ｘ」）を指定して問い合わせをパケット計数装置２１１に送信する。それにより、サーバ２０２は、例えば、パケット計数装置２１１からオブジェクト識別子と対応する値の返信を受けることができる。

【００３１】

図８は、例示的なＳＮＭＰプロトコルで提供されるパケット数に関する情報を含むオブジェクトを示す図である。サーバ２０２の制御部３０１は、例えば、パケット計数装置２１１に５回問い合わせを行い、図８に示す５つのオブジェクトの値を取得することで、ＩｏＴ機器１０１がパケット計数装置２１１のポートを介して送信したパケットの数を取得することができる。例えば、制御部３０１は、“ifInUcastPkts”および“ifInNUcastPkts”の２つを合算し、指定したポートの受信パケットの合算値を得る。また、制御部３０１は、“ifInDiscards”、“ifInErrors”、および“ifInUnknownProtos”の３つを合算することで、ポートに入力されたエラーパケットの合算値を得る。そして、制御部３０１は、受信パケットの合算値から、エラーパケットの合算値を差し引くことで、ＩｏＴ機器１０１がパケット計数装置２１１のポートを介して送信したパケットの数を取得してよい。

【００３２】

続いて、Ｓ５０２において制御部３０１は、検査対象のＩｏＴ機器１０１からサーバ２０２に宛てて送信されたパケットの数を第２のパケット数としてパケット分析部２１３から取得し、本動作フローは終了し、フローはＳ４０５に進む。なお、制御部３０１は、一実施形態においては、以下の図９～図１０に述べるようにして、検査対象のＩｏＴ機器１０１からサーバ２０２に宛てて送信されたパケットの数を取得してよい。

【００３３】

図９は、パケット分析部２１３により収集される分析情報９００を例示する図である。パケット分析部２１３は、例えば、パケットが入力されると、パケットの送信元を示すソースアドレスを分析し、ソースアドレス単位で入力されたパケットの数をカウントし、分析情報９００に登録する。なお、一例では、パケット分析部２１３は、起動時からの累積で入力されたパケットの数をカウントしてよい。パケット分析部２１３は、例えば、プロトコルアナライザであってよい。パケット分析部２１３は、例えば、サーバ２０２の問い合わせに応じて、問い合わせで指定されるソースアドレスを用いて、検査対象のＩｏＴ機器１０１がサーバ２０２に宛てて送信したパケット数を分析情報９００から読み出し、返信してよい。

【００３４】

図１０は、パケット分析部２１３が実行するパケット分析処理を例示する図である。パケット分析部２１３は、例えば、起動すると図１０の動作フローを開始してよい。

【００３５】

Ｓ１００１において制御部３０１は、パケットを受信したか否かを判定する。パケットを受信していない場合（Ｓ１００１がＮＯ）、フローはＳ１００１の処理を繰り返す。一方、Ｓ１００１においてパケットを受信した場合（Ｓ１００１がＹＥＳ）、フローはＳ１００２に進む。

【００３６】

Ｓ１００２において制御部３０１は、受信したパケットが、サーバ２０２からのパケット数の問い合わせか否かを判定する。サーバ２０２からのパケット数の問い合わせで無い場合（Ｓ１００２がＮＯ）、フローはＳ１００４に進む。一方、サーバ２０２からのパケット数の問い合わせである場合（Ｓ１００２がＹＥＳ）、フローはＳ１００３に進む。

【００３７】
Ｓ１００３において制御部３０１は、問い合わせにおいて、例えば、ＭＡＣアドレスまたはＩＰアドレスなどで指定される検査対象のＩｏＴ機器１０１を、ソースアドレスとする分析情報９００のエントリからパケット数を読み出し、サーバ２０２に返す。
【００３８】
Ｓ１００４において制御部３０１は、受信したパケットのソースアドレスを分析し、ソースアドレスと対応する分析情報９００のエントリのパケット数を１加算して、ソースアドレスごとにパケット数をカウントし、フローはＳ１００１に戻る。
【００３９】
図１０の動作フローにより、分析情報９００には、サーバに宛てて送信されたパケットの数が、ソースアドレスごとに登録される。また、図１０の動作フローにより、サーバ２０２の制御部３０１は、Ｓ５０２で送信されるサーバ２０２からの問い合わせに対して、検査対象のＩｏＴ機器１０１からサーバ２０２に宛てて送信されたパケットの数を表す第２のパケット数を取得することができる。
【００４０】
（通信時のトラフィック情報収集処理）
続いて、Ｓ４０４で制御部３０１が実行する通信時のトラフィック情報取得処理を説明する。
【００４１】
例えば、検査対象のＩｏＴ機器１０１の検査を実行する際に、検査対象のＩｏＴ機器１０１が、サーバ２０２と通信接続を確立していることがある。ここで、例えば、検査対象のＩｏＴ機器１０１が、サーバ２０２と通信接続を確立していなければ、検査対象のＩｏＴ機器１０１が過去に発信したサーバ２０２宛てのパケットは既に配送先への配送が完了している状態にある。そのため、サーバ２０２は、パケット計数装置２１１と、パケット分析部２１３とのそれぞれから取得した検査対象のＩｏＴ機器１０１のトラフィック情報を用いて、検査対象のＩｏＴ機器１０１が不正な通信を行っているか否かを判定することができる。
【００４２】
しかしながら、例えば、サーバ２０２が、検査対象のＩｏＴ機器１０１を検査する際に、検査対象のＩｏＴ機器１０１がサーバ２０２と通信接続を確立している場合、検査対象のＩｏＴ機器１０１はサーバ２０２にパケットを送信している。この場合、例えば、図１１に示すように、通信経路上、或いはパケット計数装置２１１およびパケット分析部２１３が備えるバッファなどに配送の完了していないパケットが存在し得る。そして、この様なタイミングで、パケット計数装置２１１およびパケット分析部２１３からパケット数を取得しても、未配送のパケットにより数に差がでてしまうことがある。また、そもそもパケット計数装置２１１と、パケット分析部２１３とでパケット数を取得するタイミングが合致していないと、検査対象のＩｏＴ機器１０１が正常に動作していても、パケット数に差がでてしまう。例えば、パケット数を取得する際にパケット計数装置２１１と、パケット分析部２１３とのそれぞれが最後にカウントしたパケットが同じであれば、パケット数を比較して検査対象のＩｏＴ機器１０１を検査することができる。しかしながら、例えば、パケット計数装置２１１とパケット分析部２１３とが最後にカウントしたパケットが、検査対象のＩｏＴ機器１０１において大きく異なるタイミングで発信されたパケットであれば、パケット数を比較しても、意味のある判定を実行できない。そして、こうしたＩｏＴ機器１０１の不正な通信以外に起因してパケット数にズレが生じてしまうと、パケット数を収集しても検査対象のＩｏＴ機器１０１を検査することができない。
【００４３】
この様な、ＩｏＴ機器１０１の不正な通信以外に起因するパケット数のズレを低減する一つの手法として、パケット数の取得時に検査対象のＩｏＴ機器１０１によるパケットの送信を一時的に停止させることが考えられる。検査対象のＩｏＴ機器１０１によるパケットの送信を停止させることで、例えば、経路上やバッファ上に存在する未配送のパケット

の配送の完了を待ってからトラフィック情報の収集を行うことが可能になる。また、ＩｏＴ機器１０１が発信した全てのパケットの配送が完了した状態であれば、パケット計数装置２１１およびパケット分析部２１３から収集タイミングの合致したパケット数を取得することができる。

【００４４】

しかしながら、ＩｏＴ機器１０１のなかには、外部からの制御インタフェースがほとんど用意されておらず、例えば、パケットの送信停止などの制御ができないＩｏＴ機器１０１もある。そこで、実施形態では、ＴＣＰ（Transmission Control Protocol）による通信制御の仕組みを利用して、ＩｏＴ機器１０１からのパケットの送信を停止させる。例えば、実施形態ではサーバ１０２の制御部３０１は、検査対象のＩｏＴ機器１０１からパケットを受信した場合に、そのパケットに対するＡＣＫ（肯定確認応答）を破棄する。ＡＣＫを破棄することで、検査対象のＩｏＴ機器１０１はＡＣＫ待ちの状態に入り、検査対象のＩｏＴ機器１０１からのパケットの送信が一時的に停止される。それにより、検査対象のＩｏＴ機器１０１がサーバ２０２と通信中であっても、トラフィック情報を収集して検査対象のＩｏＴ機器１０１を検査することができる。以下、検査対象のＩｏＴ機器１０１がサーバ２０２と通信接続を確立している状態におけるトラフィック情報の収集について更に詳細に説明する。

【００４５】

図１２は、送信側の装置と受信側の装置との間のＴＣＰによる通信制御を説明する図である。なお、送信側の装置は、例えば、ＩｏＴ機器１０１であってよい。また、受信側の装置は、例えば、サーバ２０２であってよい。

【００４６】

図１２（ａ）は、ＴＣＰによるパケットの送信の流れを例示している。図１２（ａ）に示す様に、送信側の装置が受信側の装置にパケットを送信したとする（図１２（ａ）の（１））。なお、ＴＣＰでは、パケットの送信にウィンドウ制御という方式が採用されておいる。ウィンドウ制御では、ウィンドウサイズ分の複数のパケットがＡＣＫによる確認なしで連続して送信され、ＡＣＫはそれらの複数のパケットに対して、１つだけ返送される。以下では、連続して送信されるウィンドウサイズ分の複数のパケットのかたまりを１箱とし、例えば、１箱のパケットを送信するといった表現を用いることがある。

【００４７】

送信側の装置が送信した１箱分のパケットを受信側の装置が受信すると、受信側の装置は、受信したパケットと対応するＡＣＫを返信する（図１２（ａ）の（２））。ＡＣＫを受信すると、送信側の装置は、ウィンドウサイズを増やすなどの調整を行い（図１２（ａ）の（３））、調整後のウィンドウサイズで次の箱のパケットを送信する（図１２（ａ）の（４））。ここで、受信側の装置からのＡＣＫが返らないと、送信側の装置はＡＣＫの受信待ちの状態に入る。

【００４８】

図１２（ｂ）は、送信側の装置のＡＣＫの受信待ちの状態を例示する図である。図１２（ｂ）に示す様に、送信側の装置が１箱分のパケットを送信したとする（図１２（ｂ）の（１））。１箱分のパケットを受信側の装置が受信すると、受信側の装置は、受信したパケットと対応するＡＣＫを返信するが、このＡＣＫを破棄したとする（図１２（ｂ）の（２））。この場合、送信側の装置は、ＡＣＫの受信待ちの状態になる。ＡＣＫの受信待ちの状態は、（１）でパケットを送信してから、再送タイマに設定された所定の待ち時間が経過し、タイムアウトするまで続く。再送タイマがタイムアウトすると（図１２（ｂ）の（３））、送信側の装置は、例えば、ウィンドウサイズを減らすなどの調整を行う（図１２（ｂ）の（４））。そして、送信側の装置は、調整後のウィンドウサイズで１箱分のパケットを再送し（図１２（ｂ）の（５））、受信側の装置に再送パケットが届く（図１２（ｂ）の（６））。

【００４９】

この場合、送信側の装置は、（１）でパケットを送信した後は、（５）でパケットの再

送を実行するまでパケットの送信を停止する。そのため、このパケットの送信が停止する期間において、サーバ２０２は、測定誤差を抑えたトラフィック情報を収集することができる。

【００５０】

以上で述べた様に、受信側の装置は、ＡＣＫを破棄して送信側の装置からのパケットの送信を停止させることで、送信側の装置が受信側の装置に宛てて送信した全てのパケットの配送が完了した状態を作り出して、トラフィック情報の取得を実行することができる。

【００５１】

なお、図１２の例では、ＴＣＰの通信制御に従って、送信側の装置のパケットの送信を停止させている。そのため、例えば、ＴＣＰで通信していれば、ＩｏＴ機器１０１がパケットの送信停止などを受け付ける外部からの制御インタフェースを備えていなくても、ＩｏＴ機器１０１のパケットの送信を停止させることができる。

【００５２】

また、ＡＣＫの破棄は、一例では、受信側の装置のファイアウォールなどのパケットフィルタに、自装置から検査対象のＩｏＴ機器１０１宛てのＡＣＫまたはＴＣＰのパケットを破棄するように設定することで実行することができる。パケットフィルタを利用することで、例えば、ＯＳ３５０などに改変を加えなくても、ＡＣＫまたはＴＣＰのパケットを破棄することができる。

【００５３】

続いて、以上で述べたＡＣＫの破棄を用いる通信時のトラフィック情報取得処理の動作フローを説明する。図１３は、Ｓ４０４で制御部３０１が実行する通信時のトラフィック情報取得処理の動作フローを例示する図である。制御部３０１は、例えば、図４のＳ４０４に進むと、図１３の動作フローを開始してよい。

【００５４】

Ｓ１３０１において制御部３０１は、自装置から検査対象のＩｏＴ機器１０１宛てのＡＣＫまたはＴＣＰのパケットを破棄するようにパケットフィルタに設定する。

【００５５】

Ｓ１３０２において制御部３０１は、ＴＣＰのＡＣＫの破棄が実施されるまで待機する。ＡＣＫの破棄が実施されると、フローはＳ１３０３に進む。

【００５６】

続く、Ｓ１３０３およびＳ１３０４の処理は、図５のＳ５０１およびＳ５０２の処理と対応していてよく、制御部３０１は、Ｓ５０１およびＳ５０２の処理と同様の処理を実行してトラフィック情報を取得してよい。

【００５７】

Ｓ１３０５において制御部は、Ｓ１３０１で設定したパケットフィルタを解除し、本動作フローは終了し、フローはＳ４０５に進む。

【００５８】

以上で述べた様に、実施形態によれば、検査対象のＩｏＴ機器１０１のトラフィック情報を収集することで、ＩｏＴ機器１０１による不正な通信を検出することができる。そのため、例えば、セキュリティ対策ソフトをインストールすることのできない簡素な機能のみを有するＩｏＴ機器１０１であっても、不正な通信を実行しているか否かを検査することが可能である。

【００５９】

また、上述の実施形態によれば、ＩｏＴ機器１０１がサーバ２０２と通信中である場合には、ＴＣＰのＡＣＫを破棄することにより、ＩｏＴ機器１０１からのパケットの送信を一時的に停止させる。それにより、ＩｏＴ機器１０１が送信したパケット数と、それに対応するＩｏＴ機器１０１からサーバ２０２に送信されたパケット数とを測定誤差を抑えて取得することができる。そのため、ＩｏＴ機器１０１がサーバ２０２と通信中である場合にも、高い精度で検査対象のＩｏＴ機器１０１が不正な通信を行っているか否かを判定することができる。

【００６０】
なお、上述の図４の動作フローでは、サーバ２０２が検査対象のＩｏＴ機器１０１と通信中ではない場合（Ｓ４０２がＮＯ）、図５の動作フローを実行し、トラフィック情報の収集を行う例を述べている。しかしながら、図５の動作フローでトラフィック情報を収集している期間中に、検査対象のＩｏＴ機器１０１から接続要求を受信することがある。この場合、接続要求に対するＡＣＫを破棄することで、測定誤差を抑えてトラフィック情報を収集することができる。
【００６１】
図１４は、実施形態に係る接続要求の破棄を説明する図である。図１４（ａ）は、ＴＣＰの接続の確立を例示する図である。ＴＣＰでは、例えば、図１４（ａ）に示す様に、３ウェイハンドシェイクにより接続が確立する。この際に、図１４（ｂ）に示す様に、接続要求に対するＡＣＫを破棄し、その後でトラフィック情報の収集を再度開始することで、ＩｏＴ機器１０１との接続に起因する測定誤差を低減してトラフィック情報を収集することができる。
【００６２】
なお、制御部３０１は、例えば、図５の動作フローの実行中に検査対象のＩｏＴ機器１０１から接続要求を受信した場合、図５の動作フローを中止し、代わりに図１３の動作フローを実行して、接続要求に対するＡＣＫを破棄し、トラフィック情報を収集してよい。
【００６３】
また、サーバ２０２に流れ込むパケットの数を計数するために、上述の実施形態では図２に示す様にハブ２１２と、パケット分析部２１３とをハードウェアとして実装する例を述べている。しかしながら、実施形態は、これに限定されるものではない。例えば、図１５に示す様に、パケット分析部２１３は、サーバ２０２上で動作するアプリケーションとして実装することもできる。この場合、例えば、ネットワークインタフェースがプロミスキャスモードで動作するように、サーバ２０２のＯＳ３５０のカーネルに設定することで、パケット分析部２１３でパケットの情報を取得することが可能である。
【００６４】
（トラフィック情報の収集の変形例）
続いて、ＩｏＴ機器１０１がサーバ２０２と通信中である場合におけるトラフィック情報の取得について更なる変形例を説明する。
【００６５】
ＴＣＰは、バージョンに応じてパケットの送信手順が異なる。図１６は、ＴＣＰのバージョンに応じたパケットの送信手順の違いを例示する図である。図１６には、例えば、Tahoe，Renoなどに代表される第１のバージョンと、NewReno、BIC、CUBICなどに代表される第２のバージョンのパケットの送信手順が例示されている。
【００６６】
図１６（ａ）に示されるように、第１のバージョンでは、送信側の装置は、ウィンドウサイズ分の１箱のパケットを送信した後、受信側の装置から送信したパケットに対応するＡＣＫを受信するまで次の箱のパケットを送信しない。この場合、受信側の装置が、受信した１箱のパケットに対するＡＣＫを１つ破棄すると、その後、送信側の装置は再送を開始するまでは次の箱のパケットを送信してこない。そのため、第１のバージョンでは、受信側の装置は、ＡＣＫを１つ破棄した時点で、トラフィック情報の取得を開始してもよい。
【００６７】
一方、図１６（ｂ）に示されるように、第２のバージョンでは、送信側の装置は、１箱のパケットを送信した後、受信側の装置から送信した１箱のパケットに対するＡＣＫを受信する前に、次の箱のパケットを送信する。その後、送信側の装置は、先に送信した１箱のパケットのＡＣＫを受信するまでは待ちに入り、次の箱のパケットは送信しない。この場合、受信側の装置は、１つ目に受信したパケットの箱に対するＡＣＫを１つ破棄した後にも次の箱のパケットが届くことになる。そのため、第２のバージョンでは、受信側の装置は、ＡＣＫを１つ廃棄した後、送信側の装置が送ってくる次の箱のパケットを受信して

から、トラフィック情報の取得を開始すればよい。以下、第２のバージョンのＴＣＰにおけるトラフィック情報の取得について変形例１を説明する。

【００６８】

（変形例１）

図１７は、変形例１に係るＴＣＰの第２のバージョンにおけるトラフィック情報の収集の実行タイミングを例示する図である。まず、送信側の装置は、ウィンドウサイズ分のパケットを１箱、受信側の装置に送信する（図１７の（１））。受信側の装置は、トラフィック情報の収集を実行する場合、パケットフィルタをＯＮにしている。そのため、受信側の装置は、送信側の装置からパケットを受信するとＡＣＫを発信するが、そのＡＣＫはパケットフィルタで破棄される（図１７の（２））。また、第２のバージョンのＴＣＰでは、送信側の装置は、（１）で送信したパケットに対するＡＣＫを待たずに、次のパケットの箱を送信する（図１７の（３））。送信側の装置は次のパケットの箱を送信した時点で、ＡＣＫの待ち状態に入りパケットの送信を停止する。そのため、受信側の装置は、（３）で送信されたパケットを受信した時点で（図１７の（４））、トラフィック情報の取得を開始することができる。一例では、受信側の装置は、（３）で送信されたパケットに対するＡＣＫを発信し、そのＡＣＫをパケットフィルタで破棄したタイミングで（図１７の（５））、トラフィック情報の収集を開始してよい。その後、受信側の装置は、トラフィック情報の収集が完了すると、パケットフィルタをＯＦＦにして、ＡＣＫの破棄を停止する（図１７の（６））。

【００６９】

また、送信側の装置は、（１）で送信したパケットに対するＡＣＫの受信を待機するが、パケットを送信してから再送タイマが、所定の待ち時間を経過し、タイムアウトすると（図１７の（７））、パケットを再送する（図１７の（８））。

【００７０】

以上で例示したように、第２のバージョンのＴＣＰでも、ＡＣＫを破棄することで、送信側の装置がサーバ２０２に送信したパケットの配送が完了した状態でトラフィック情報の収集を実行することができる。

【００７１】

図１８は、図４のＳ４０４において変形例１で制御部３０１が実行する通信時のトラフィック情報取得処理の動作フローを例示する図である。Ｓ１８０１、およびＳ１８０３からＳ１８０５の処理は、図１３のＳ１３０１、およびＳ１３０３からＳ１３０５の処理とそれぞれ対応しており、制御部３０１は、Ｓ１３０１、およびＳ１３０３からＳ１３０５と同様の処理を実行してよい。ただし、図１８の処理では、制御部３０１は、Ｓ１８０２でＡＣＫを連続して２つ破棄するまで待機する。それにより、第２のバージョンのＴＣＰでも、測定誤差を抑えてトラフィック情報を収集することができる。

【００７２】

（変形例２）

上述の変形例１では、受信側の装置の制御部３０１は、図１７の（５）で２つ目のＡＣＫを破棄してからトラフィック情報の収集を開始している。ここで、トラフィック情報の収集は、送信側の装置でＡＣＫの受信待ちがタイムアウトしてパケットの再送が実行される前までに完了することが望ましい。しかしながら、実際には通信環境などによって、トラフィック情報の収集が間に合わないこともある。この場合に、パケットの再送時にウィンドウサイズを縮小させるＴＣＰの性質を利用することでトラフィック情報の収集に利用可能な時間を延ばすことができる。そこで、変形例２では、受信側の装置でＡＣＫを３個連続で廃棄してからトラフィック情報の収集を開始することで、トラフィック情報の収集に利用可能な時間を延ばす例を述べる。

【００７３】

図１９は、変形例２に係るトラフィック情報の収集の実行タイミングを例示する図である。図１９において（１）から（３）までは、図１７と同様に処理が実行されてよい。（４）において、受信側の装置は、送信側の装置からパケットを受信すると、ＡＣＫを発信

するが、そのＡＣＫはパケットフィルタで破棄される（図１９の（５））。送信側の装置は、ＡＣＫ待ちの状態にあるが、ＡＣＫ待ちのタイムアウトの時間が経過すると（図１９の（６））、パケットを再送する（図１９の（７））。そして、変形例２では受信側の装置は、再送されたパケットのＡＣＫを破棄したタイミングで（図１９の（８））、トラフィック情報の取得を開始する。

【００７４】

この場合、再送のタイマは（７）のパケットの再送信からカウントが開始しており、また、ＴＣＰではパケットの再送の際にＡＣＫを待つ再送タイマのタイムアウトまでの時間が延長されるため、再送タイマの待ち時間も延長されている。また、例えば、タイムアウト後はウィンドウサイズが縮小され、送信側の装置は、パケットを１つ送信しては、そのＡＣＫを待つように動作する。そのため、１箱分のパケットの送信にかかる時間も短くなる。その結果、変形例２では、変形例１よりも長い時間を、トラフィック情報の取得のために確保することができる。

【００７５】

また更に、ＴＣＰでは、ＡＣＫを待つ再送タイマのタイムアウトまでの時間は、パケットの再送を繰り返すたびに延長される。例えば、タイムアウトの時間は、初期値が３秒であってよく、また、再送のたびに、３秒ずつ延長されてよい。この場合、図２０に示す様に、再送タイマの待ち時間は、タイムアウトで再送されたパケットに対するＡＣＫを破棄するごとに、３秒ずつ延長されてゆく。

【００７６】

なお、再送タイマの待ち時間には、例えば、ＯＳ３５０ごとに上限が設定されている。例えば、Windows（登録商標）では、待ち時間の上限は、２１秒に設定されており、Linux（登録商標）では、待ち時間の上限は３８１秒に設定されている。待ち時間の上限を超えると、接続が切断されるため、実施形態では、待ち時間の上限以下で、トラフィック情報の取得に適した待ち時間となるように廃棄するＡＣＫの数を設定することができる。例えば、図１６（ａ）の第１のバージョンのＴＣＰでは、待ち時間は、「破棄したＡＣＫの数×３秒」で見積もることができる。また、図１６（ｂ）の第２のバージョンのＴＣＰでは、最初にＡＣＫを破棄した後、ＡＣＫを待たずに送信される次の箱のパケットのＡＣＫを破棄する分だけ１回増えるため、「（破棄したＡＣＫの数－１回）×３秒」で待ち時間を見積もることができる。

【００７７】

図２１は、図４のＳ４０４において変形例２で制御部３０１が実行する通信時のトラフィック情報取得処理の動作フローを例示する図である。Ｓ２１０１、およびＳ２１０３からＳ２１０５までの処理は、図１３のＳ１３０１、およびＳ１３０３からＳ１３０５までの処理とそれぞれ対応しており、制御部３０１は、Ｓ１３０１、およびＳ１３０３からＳ１３０５と同様の処理を実行してよい。ただし、図２１の処理では、制御部３０１は、Ｓ２１０２でＡＣＫを連続して所定の回数だけ破棄するまで待機する。所定の回数は、例えば、連続してＡＣＫを破棄する回数であり、３回以上の回数であってよく、ＩｏＴシステム２００の構成に応じて、トラフィック情報の取得が可能な待ち時間となるように、ＡＣＫを破棄する回数が設定されてよい。

【００７８】

以上の図１９から図２１で述べた様に、ＡＣＫの破棄を繰り返すことで、ＡＣＫ待ち時間を長くすることができるため、トラフィック情報の収集に時間がかかる場合にも、十分な時間を確保することができる。

【００７９】

（変形例３）

変形例２では、再送タイマのタイムアウト後にウィンドウサイズが縮小するＴＣＰの性質を利用して１箱分のパケットの数を減少させて、１箱分のパケットが受信側の装置に到達するまでの時間を短縮している。それにより、トラフィック情報の収集に利用できる時間を長く確保することができる。しかしながら、この場合、送信側の装置で再送タイマが

タイムアウトするまでの待ち時間が発生する。そこで、変形例３では、改変したＡＣＫを送信側の装置に送信することで、送信側の装置のウィンドウサイズを縮小させる例を述べる。それにより、再送タイマがタイムアウトするまで待たなくても、トラフィック情報の収集を開始することが可能になる。

【００８０】

ＴＣＰでは、ＡＣＫの種類によって、送信側の装置のウィンドウサイズを縮小させることが可能である。例えば、ＴＣＰでは、ＡＣＫに受信バッファが一杯であることを示すフラグがあり、このフラグがＯＮである場合、送信側の装置は、ウィンドウサイズを縮小する。そこで、変形例３では、受信側の装置は、受信バッファが一杯であることを示すフラグを立てるように改ざんしたＡＣＫを送信側の装置に送信し、それにより送信側の装置のウィンドウサイズを縮小させる。

【００８１】

図２２は、変形例３に係るトラフィック情報の収集の実行タイミングを例示する図である。トラフィック情報を収集する場合、送信側の装置がパケットを送信すると（図２２の（１））、受信側の装置は、そのパケットに対して、受信バッファが一杯であることを示すフラグを立てるように改ざんしたＡＣＫを返す（図２２の（２））。その後、受信側の装置は、パケットフィルタをＯＮに設定し（図２２の（３））、以降、送信側の装置がパケットを送信してくると（図２２の（４））、そのパケットを受信したことを示すＡＣＫを破棄する（図２２の（５））。

【００８２】

また、送信側の装置は、改ざんしたＡＣＫを受信すると、ウィンドウサイズを縮小し（図２２の（６））、以降、パケットを１つずつ送信してＡＣＫを待つ（図２２の（７））。そのため、受信側の装置は、（８）においてパケットに対するＡＣＫを破棄すると、トラフィック情報の収集を開始することができる。この場合、送信側の装置において、（７）で送信したパケットに対する再送タイマがタイムアウトするまでの間に、受信側の装置は、トラフィック情報の収集を完了すればよい。トラフィック情報の収集を完了すると、受信側の装置は、パケットフィルタをＯＦＦにする（図２２の（９））。そして、送信側の装置は、再送タイマがタイムアウトするとパケットの再送を行う（図２２の（１０））。

【００８３】

以上で述べた様に、変形例３では、送信側の装置のタイムアウトを待たずに、送信側の装置のウィンドウサイズを縮小させてトラフィック情報の収集を行うことができる。例えば、変形例３では、変形例２の図１９の（６）のタイムアウトを待たなくてよい。

【００８４】

なお、変形例３では受信側の装置は、改ざんしたＡＣＫを送信側の装置に返している。送信側の装置に改ざんしたＡＣＫを返すための手法の一例としては、受信側の装置においてＡＣＫを生成するＯＳ３５０を、アプリケーションからの依頼を受けて、改ざんしたＡＣＫを返すように改変することが考えられる。また、別の例では、特定のインタフェースで受けたパケットをまるごとアプリケーションに送るようにＯＳ３５０を設定しておき、ＯＳ３５０の処理をバイパスして、アプリケーション上でＴＣＰのパケットを処理することが考えられる。この場合、アプリケーションが改ざんしたＡＣＫを返すため、ＯＳ３５０を改変しなくても、変形例３の処理を実行することができる。

【００８５】

図２３は、図４のＳ４０４において変形例３で制御部３０１が実行する通信時のトラフィック情報取得処理の動作フローを例示する図である。図２３の処理では、制御部３０１は、Ｓ２３０１で改ざんしたＡＣＫをＩｏＴ機器に送信する。例えば、制御部３０１は、受信バッファが一杯であることを示すフラグを立てるようにＡＣＫを改ざんすることで、改ざんしたＡＣＫを生成することができる。改ざんしたＡＣＫを送信後、制御部３０１は、Ｓ２３０２で自装置から検査対象のＩｏＴ機器１０１宛てのＡＣＫまたはＴＣＰのパケットを破棄するようにパケットフィルタに設定する。そして、Ｓ２３０３で制御部３０１は、ＡＣＫを２つ連続で破棄するまで待機する。続く、Ｓ２３０４からＳ２３０６までの

処理は、図１３のＳ１３０３からＳ１３０５までの処理とそれぞれ対応しており、制御部３０１は、Ｓ１３０３からＳ１３０５と同様の処理を実行してよい。なお、変形例３でも、変形例２と同様に、トラフィック情報の取得に適した待ち時間を確保するために３回以上ＡＣＫを廃棄してもよい。

【００８６】

以上の変形例１から変形例３によれば、ＴＣＰのバージョンが第２のバージョンであっても、或いは、トラフィック情報の収集に時間を要する場合にも、測定誤差を抑えてトラフィック情報を収集し、ＩｏＴ機器１０１を検査することができる。

【００８７】

なお、上述の実施形態において、例えば、Ｓ１３０１、Ｓ１８０１、Ｓ２１０１、Ｓ２３０２の処理では、サーバ２０２の制御部３０１は、設定部３１１として動作する。また、例えば、Ｓ５０１、Ｓ５０２、Ｓ１３０３、Ｓ１３０４、Ｓ１８０３、Ｓ１８０４、Ｓ２１０３、Ｓ２１０４、Ｓ２３０４、およびＳ２３０５の処理では、サーバ２０２の制御部３０１は、取得部３１２として動作する。例えば、Ｓ４０５の処理では、サーバ２０２の制御部３０１は、検査部３１３として動作する。

【００８８】

以上において、実施形態を例示したが、実施形態はこれに限定されるものではない。例えば、上述の動作フローは例示であり、実施形態はこれに限定されるものではない。可能な場合には、動作フローは、処理の順番を変更して実行されてもよく、別に更なる処理を含んでもよく、または、一部の処理が省略されてもよい。例えば、上述のＳ５０１とＳ５０２の処理、Ｓ１３０３とＳ１３０４の処理、Ｓ１８０３とＳ１８０４の処理、Ｓ２１０３とＳ２１０４の処理、Ｓ２３０４とＳ２３０５の処理はそれぞれ順序を入れ替えて実行されてもよい。

【００８９】

また、例えば、上述の変形例１～変形例３では、ＡＣＫを破棄したタイミングでトラフィック情報の収集を開始する例を述べている。しかしながら、実施形態はこれに限定されるものではない。例えば、別の実施形態では、制御部３０１は、ＡＣＫを破棄したタイミングに基づいてトラフィック情報の収集の開始タイミングを決定してもよい。例えば、上述の変形例１において、制御部３０１は、１つ目のＡＣＫを破棄してから、ウィンドウサイズ分のパケットを受信したタイミングでトラフィック情報の収集を開始してもよい。または、制御部３０１は、１つ目のＡＣＫを破棄してから、所定時間経過したタイミングでトラフィック情報の収集を開始してもよい。この場合、所定時間は、例えば、往復遅延時間（RTT：Round-Trip Time）などに応じて、送信側の装置が送信してくる次の箱のパケットの受信が完了する長さに設定されてよい。

【００９０】

図２４は、実施形態に係るサーバ２０２またはパケット分析部２１３を実現するためのコンピュータ２４００のハードウェア構成を例示する図である。図２４のサーバ２０２またはパケット分析部２１３を実現するためのハードウェア構成は、例えば、プロセッサ２４０１、メモリ２４０２、記憶装置２４０３、読取装置２４０４、および通信インタフェース２４０６を備える。なお、プロセッサ２４０１、メモリ２４０２、記憶装置２４０３、読取装置２４０４、通信インタフェース２４０６は、例えば、バス２４０８を介して互いに接続されている。

【００９１】

プロセッサ２４０１は、例えば、シングルプロセッサであっても、マルチプロセッサやマルチコアであってもよい。プロセッサ２４０１は、メモリ２４０２を利用して例えば上述の動作フローの手順を記述したプログラムを実行することにより、上述した制御部３０１またはパケット分析部２１３の一部または全部の機能を提供する。例えば、サーバ２０２のプロセッサ２４０１は、記憶装置２４０３に格納されているプログラムを読み出して実行することで、設定部３１１、取得部３１２、および検査部３１３として動作する。また、プロセッサ２４０１は、例えば、記憶装置２４０３に格納されているプログラムを読

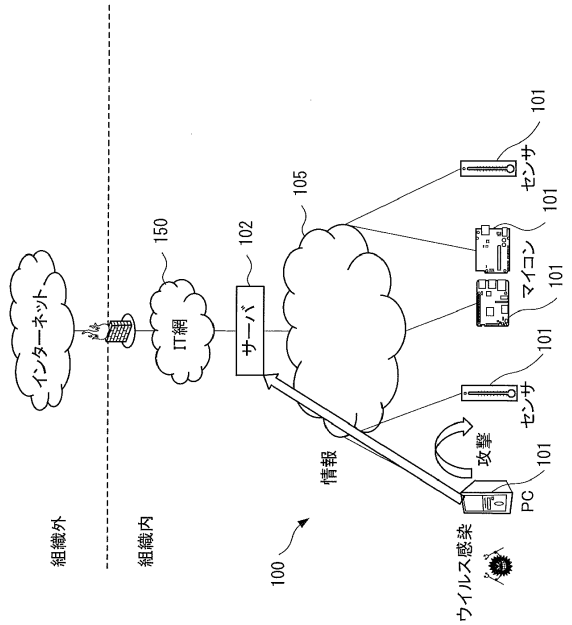
み出して実行することで、パケット分析部２１３として動作してよい。
【００９２】
メモリ２４０２は、例えば半導体メモリであり、ＲＡＭ領域およびＲＯＭ領域を含んでいてよい。記憶装置２４０３は、例えばハードディスク、フラッシュメモリ等の半導体メモリ、または外部記憶装置である。なお、ＲＡＭは、Random Access Memoryの略称である。また、ＲＯＭは、Read Only Memoryの略称である。
【００９３】
読取装置２４０４は、プロセッサ２４０１の指示に従って着脱可能記憶媒体２４０５にアクセスする。着脱可能記憶媒体２４０５は、例えば、半導体デバイス（ＵＳＢメモリ等）、磁気的作用により情報が入出力される媒体（磁気ディスク等）、光学的作用により情報が入出力される媒体（ＣＤ－ＲＯＭ、ＤＶＤ等）などにより実現される。なお、ＵＳＢは、Universal Serial Busの略称である。ＣＤは、Compact Discの略称である。ＤＶＤは、Digital Versatile Diskの略称である。
【００９４】
なお、上述の記憶部３０２は、例えば、メモリ２４０２、記憶装置２４０３、および着脱可能記憶媒体２４０５を含んでよい。サーバ２０２の記憶装置２４０３またはパケット分析部２１３の記憶装置２４０３には、例えば、分析情報９００が格納されていてよい。
【００９５】
通信インタフェース２４０６は、プロセッサ２４０１の指示に従ってネットワークを介してデータを送受信する。通信インタフェース２４０６は、例えば、上述の通信部３０３の一例である。
【００９６】
実施形態に係る各プログラムは、例えば、下記の形態でサーバ２０２およびパケット分析部２１３に提供される。
（１）記憶装置２４０３に予めインストールされている。
（２）着脱可能記憶媒体２４０５により提供される。
（３）プログラムサーバなどのサーバから提供される。
【００９７】
なお、図２４を参照して述べたサーバ２０２およびパケット分析部２１３を実現するためのコンピュータ２４００のハードウェア構成は、例示であり、実施形態はこれに限定されるものではない。例えば、上述の機能部の一部または全部の機能がＦＰＧＡおよびＳｏＣなどによるハードウェアとして実装されてもよい。なお、ＦＰＧＡは、Field Programmable Gate Arrayの略称である。ＳｏＣは、System-on-a-chipの略称である。
【００９８】
以上において、いくつかの実施形態が説明される。しかしながら、実施形態は上記の実施形態に限定されるものではなく、上述の実施形態の各種変形形態および代替形態を包含するものとして理解されるべきである。例えば、各種実施形態は、その趣旨および範囲を逸脱しない範囲で構成要素を変形して具体化できることが理解されよう。また、前述した実施形態に開示されている複数の構成要素を適宜組み合わせることにより、種々の実施形態が実施され得ることが理解されよう。更には、実施形態に示される全構成要素からいくつかの構成要素を削除してまたは置換して、或いは実施形態に示される構成要素にいくつかの構成要素を追加して種々の実施形態が実施され得ることが当業者には理解されよう。
【符号の説明】
【００９９】
１００　ＩｏＴシステム
１０１　ＩｏＴ機器
１０２　サーバ
１０５　ネットワーク
１５０　ＩＴ網
２００　ＩｏＴシステム

２０２　　サーバ
２１１　　パケット計数装置
２１２　　ハブ
２１３　　パケット分析部
２５０　　検査システム
３０１　　制御部
３０２　　記憶部
３０３　　通信部
３１１　　設定部
３１２　　取得部
３１３　　検査部
２４００　コンピュータ
２４０１　プロセッサ
２４０２　メモリ
２４０３　記憶装置
２４０４　読取装置
２４０５　着脱可能記憶媒体
２４０６　通信インタフェース
２４０８　バス

【図面】

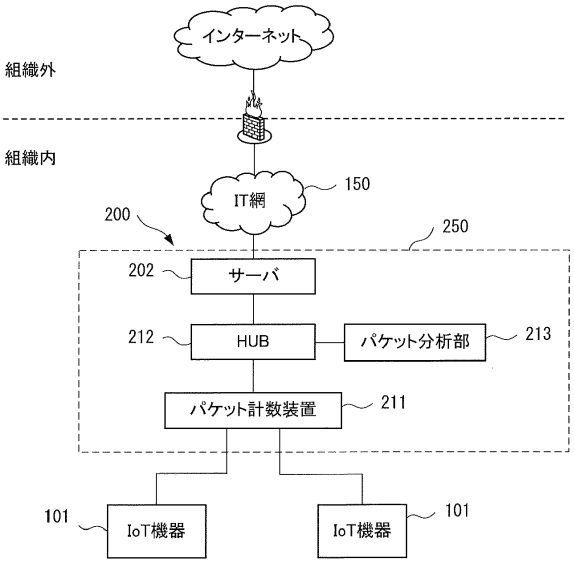
【図１】

例示的なIoTシステムを示す図



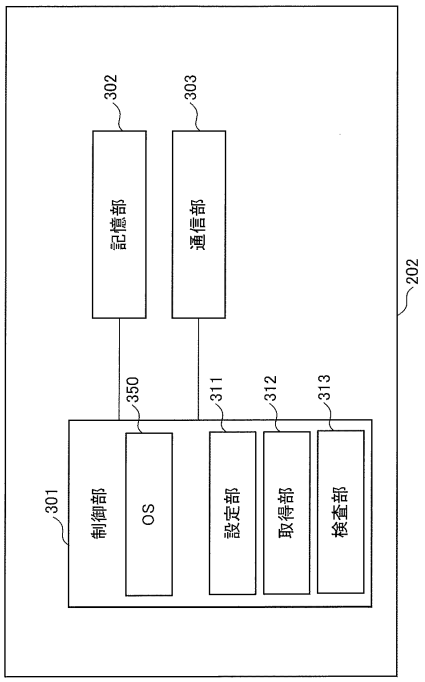
【図２】

実施形態に係るIoTシステムを例示する図



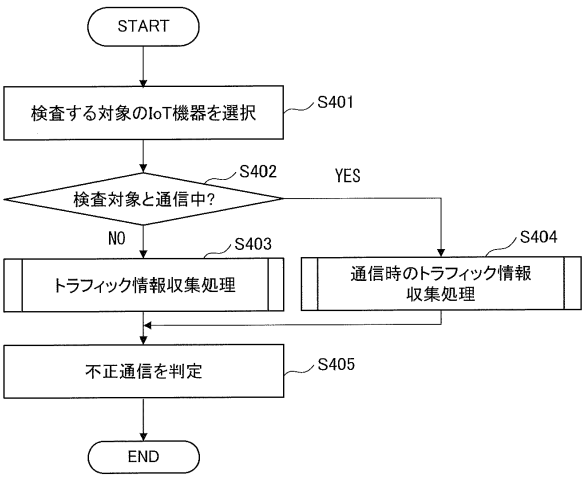
【図３】

実施形態に係るサーバのブロック構成を例示する図



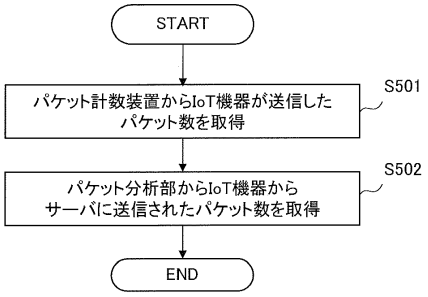
【図４】

実施形態に係る検査対象のIoT機器の
不正通信の検査処理の動作フローを例示する図



【図５】

実施形態に係るトラフィック
情報取得処理を例示する図



【図６】

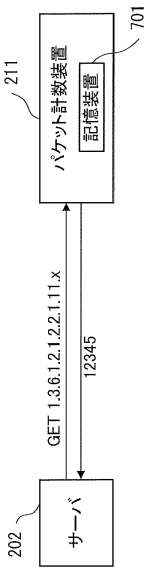
パケット計数装置により収集される
計数情報を例示する図

ポート番号	パケット番号
1	p1
⋮	⋮
8	p8

600

【図７】

SNMPプロトコルでの
問い合わせを例示する図



【図８】

例示的なSNMPプロトコルで提供される
パケット数に関する情報を含むオブジェクトを例示する図

OID等	名前	型	内容
1.3.6.1.2.1.2.2.1.11	ifInUcastPkts	32bit 非負 整数	受信したユニキャストパケット数
1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts		受信したマルチキャスト・ブロードキャストパケット数
1.3.6.1.2.1.2.2.1.13	ifInDiscards		資源の制限などのために廃棄される受信パケット数
1.3.6.1.2.1.2.2.1.14	ifInErrors		エラーのための上位プロトコルに配信できなかった受信パケット数
1.3.6.1.2.1.2.2.1.15	ifInUnknownProtos		不明または未定義のプロトコルのため廃棄された受信パケット数

【図９】

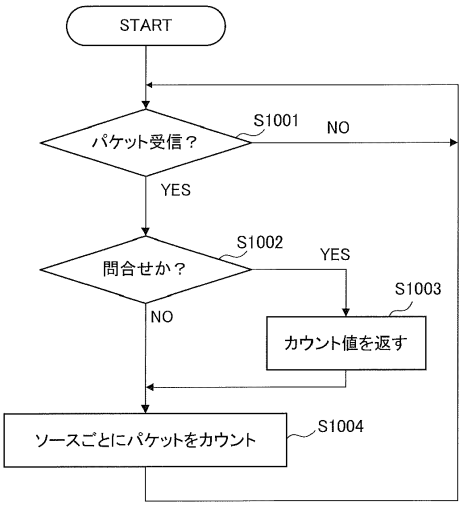
パケット分析部により収集される
分析情報を例示する図

ソースアドレス	パケット数
A	a
B	b
：	：
Z	z

900

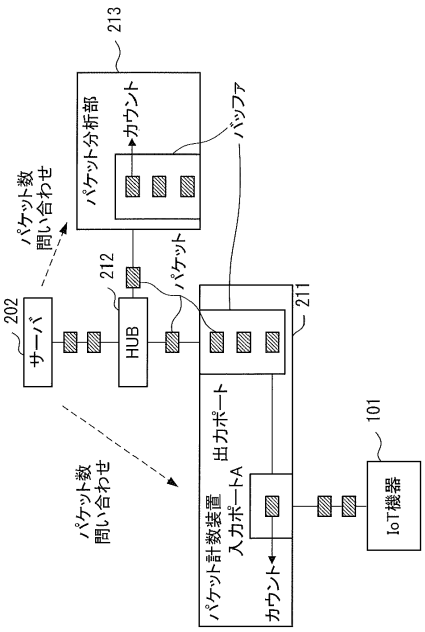
【図１０】

パケット分析部が実行するパケット分析処理を例示する図



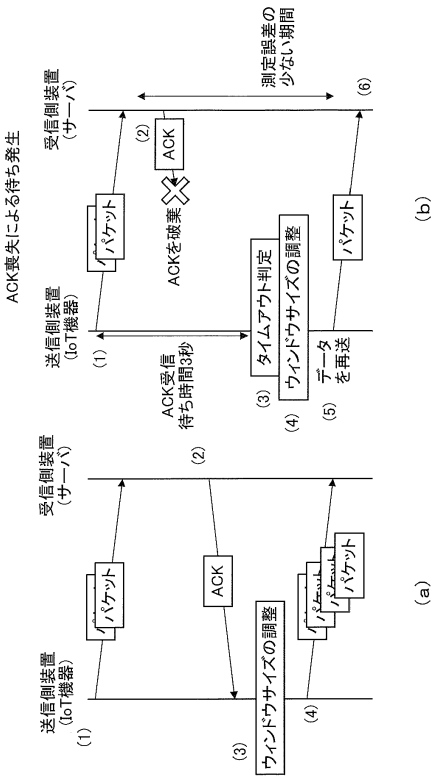
【図１１】

経路およびバッファ上のパケットを例示する図



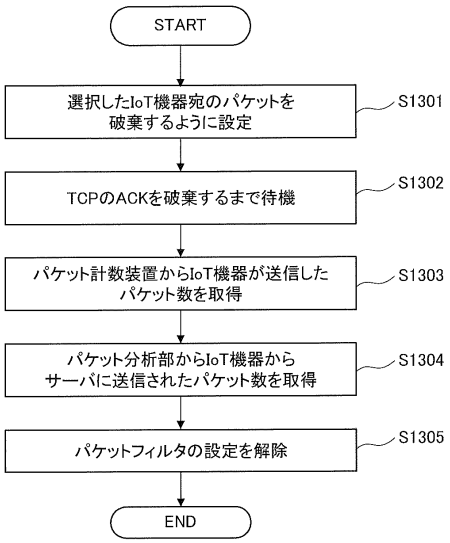
【図１２】

送信側の装置と受信側の装置との間の
TCPによる通信制御を説明する図



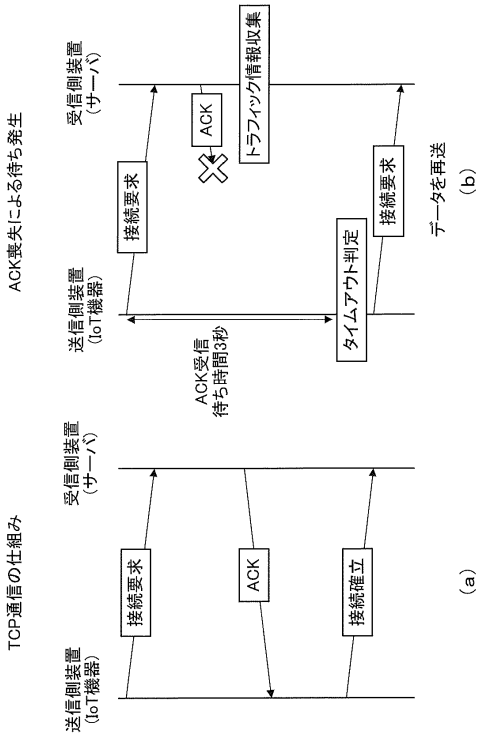
【図１３】

実施形態に係る通信時のトラフィック
情報取得処理の動作フローを例示する図



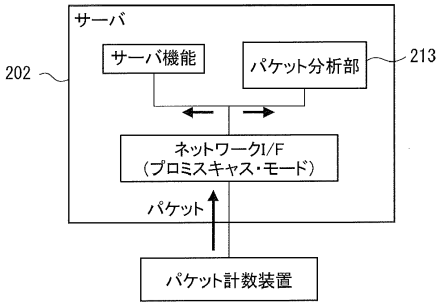
【図１４】

実施形態に係る接続要求の破棄を説明する図



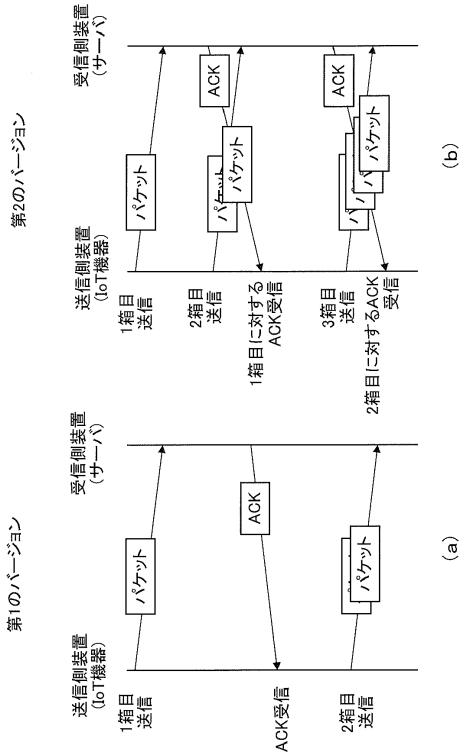
【図１５】

別の実施形態に係るパケット
分析部の配置を例示する図



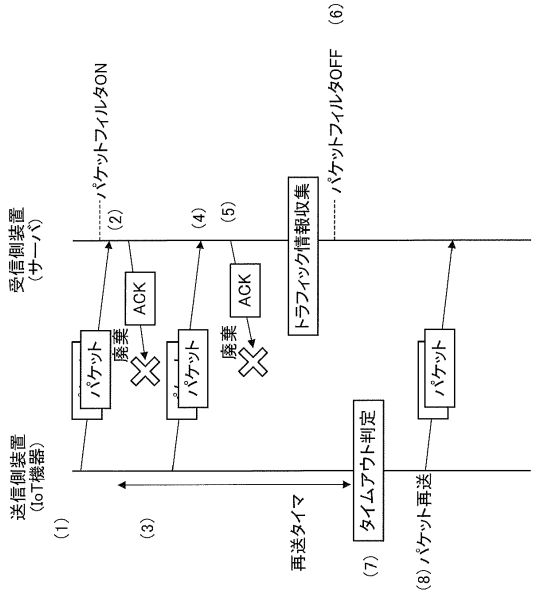
【図１６】

TCPのバージョンに応じたパケットの
送信手順の違いを例示する図



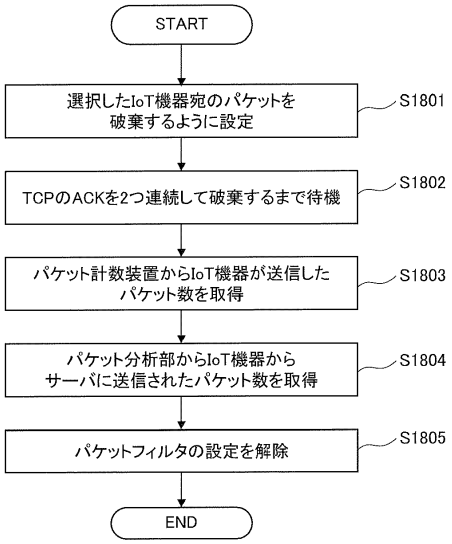
【図１７】

変形例1に係るTCPの第2のバージョンにおける
トラフィック情報の収集の実行タイミングを例示する図



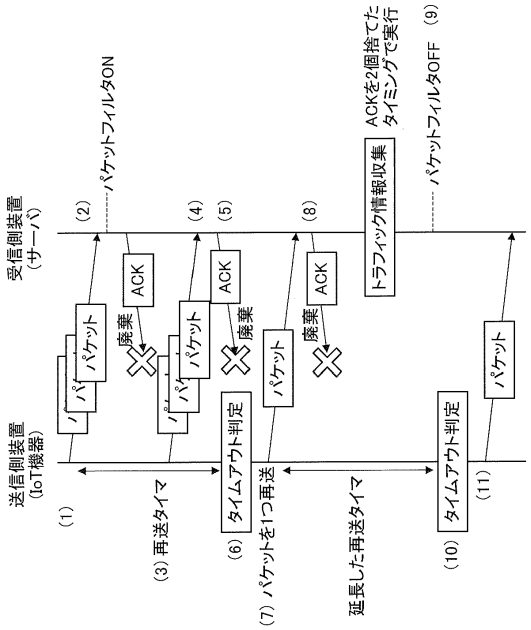
【図１８】

変形例1に係る通信時のトラフィック
情報取得処理の動作フローを例示する図



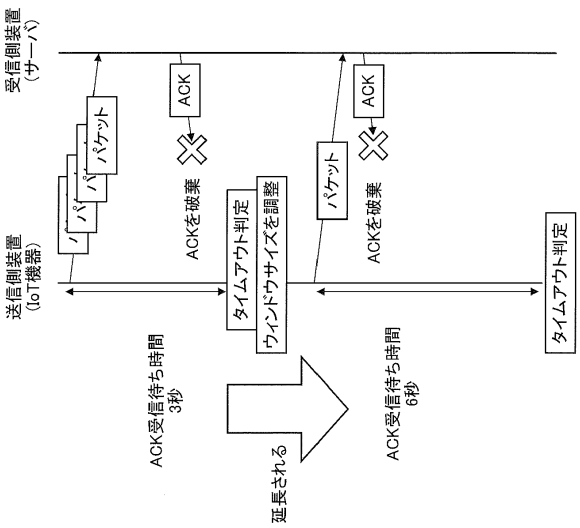
【図１９】

変形例2に係るトラフィック情報の
収集の実行タイミングを例示する図



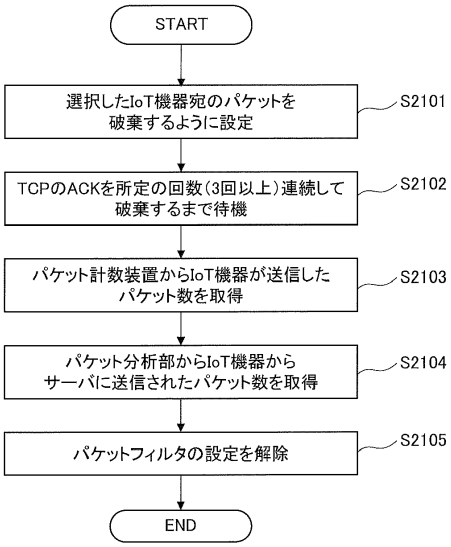
【図２０】

変形例2に係るトラフィック情報の
収集の実行タイミングを更に例示する図



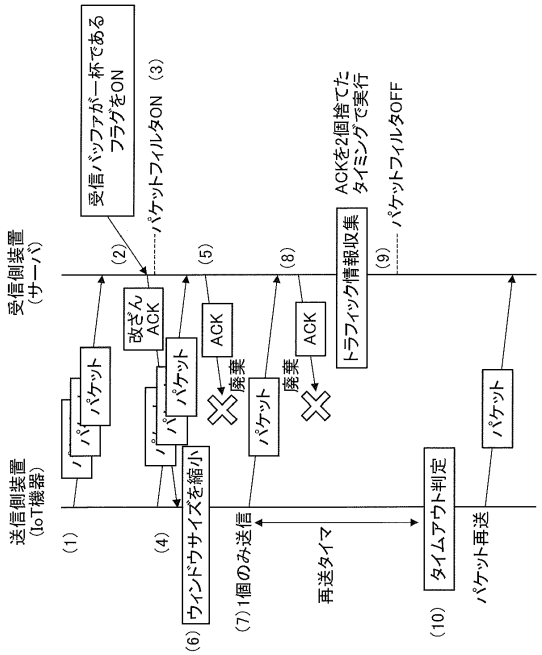
【図２１】

変形例2に係る通信時のトラフィック情報
取得処理の動作フローを例示する図



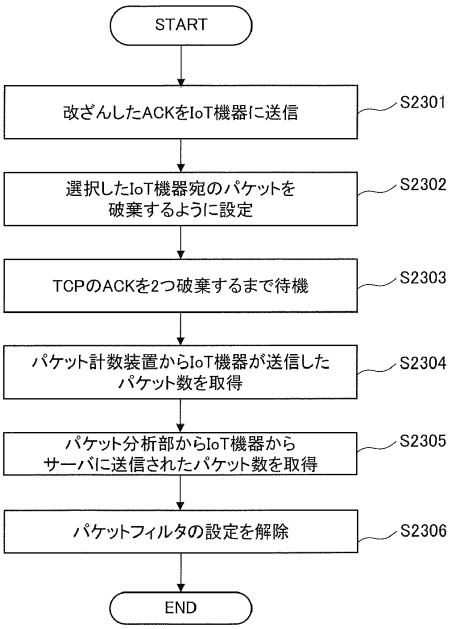
【図２２】

変形例3に係るトラフィック情報の
収集の実行タイミングを例示する図



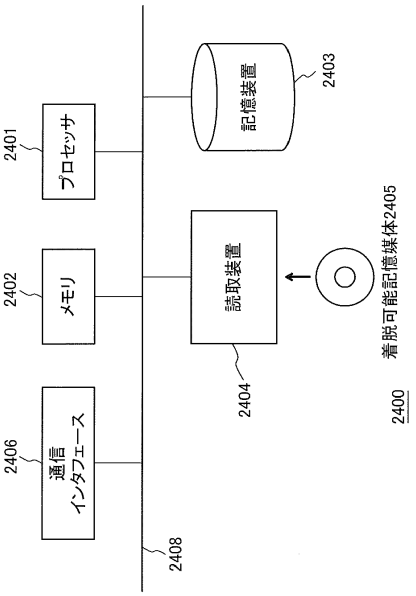
【図２３】

変形例3に係る通信時のトラフィック情報
取得処理の動作フローを例示する図



【図２４】

実施形態に係るサーバまたはパケット分析部を実現
するためのコンピュータのハードウェア構成を例示する図



フロントページの続き

(56)参考文献 特開２０１９－１５３８７５（ＪＰ，Ａ）
特開２０１４－０４１４４５（ＪＰ，Ａ）
特開２０１４－１５０４８５（ＪＰ，Ａ）
特開２０１３－１７５８３７（ＪＰ，Ａ）
特開２０１６－１３９９０３（ＪＰ，Ａ）
特開２０１６－１１９５５３（ＪＰ，Ａ）
国際公開第２０１６／１４３０７３（ＷＯ，Ａ１）
米国特許出願公開第２０１４／０３６２７１９（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／６６
Ｈ０４Ｌ １２／２２
Ｈ０４Ｌ ４３／０２