(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7501620号
(P7501620)

(45)発行日　令和6年6月18日(2024.6.18)

(24)登録日　令和6年6月10日(2024.6.10)

(51)国際特許分類
G06F 21/55 (2013.01)

FI
G06F 21/55 320

請求項の数　7　（全17頁）

(21)出願番号　特願2022-522147(P2022-522147)
(86)(22)出願日　令和2年5月12日(2020.5.12)
(86)国際出願番号　PCT/JP2020/019011
(87)国際公開番号　WO2021/229694
(87)国際公開日　令和3年11月18日(2021.11.18)
審査請求日　令和4年9月30日(2022.9.30)
前置審査

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100124844
弁理士　石原 隆治
(72)発明者　松林 勝
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内
(72)発明者　小山 卓麻
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】　攻撃検知装置、攻撃検知方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
周期的なメッセージとは非同期なメッセージの直後の前記周期的なメッセージの送信間隔が前記周期的なメッセージの周期となる第１の型と、前記非同期なメッセージが前記周期的なメッセージの周期に影響しない第２の型との通信が行われる機器内のネットワークに対する攻撃を検知する攻撃検知装置であって、
　前記ネットワークにおいて周期的に送信されるメッセージ又は前記メッセージとは非同期に送信されるメッセージのうち、或る期間において送信された共通の値を含む複数のメッセージの前記値が前記第１の型に対応する場合に、当該複数のメッセージの中から、ペイロードが同一である２つのメッセージの組を抽出する抽出部と、
前記値が前記第１の型に対応する場合に、前記組に係る２つのメッセージの送信の間における他のメッセージの送信の有無と、当該２つのメッセージの送信の間隔とに基づいて、前記攻撃の有無を判定する判定部と、
を有することを特徴とする攻撃検知装置。
【請求項２】
　前記判定部は、前記値が前記第１の型に対応する場合に、前記２つのメッセージの送信の間に他のメッセージが送信されておらず、かつ、前記２つのメッセージの送信の間隔と、前記周期的に送信されるメッセージの送信周期との差分が閾値を超える場合には、前記攻撃が有ると判定する、
ことを特徴とする請求項１記載の攻撃検知装置。

【請求項３】
前記判定部は、前記値が前記第１の型に対応する場合に、前記２つのメッセージの送信の間に他のメッセージが送信されおり、かつ、前記２つのメッセージの送信の間隔と、前記周期的に送信されるメッセージの送信周期との差分が閾値以下である場合には、前記攻撃が有ると判定する、
ことを特徴とする請求項１又は２記載の攻撃検知装置。
【請求項４】
周期的なメッセージとは非同期なメッセージの直後の前記周期的なメッセージの送信間隔が前記周期的なメッセージの周期となる第１の型と、前記非同期なメッセージが前記周期的なメッセージの周期に影響しない第２の型との通信が行われる機器内のネットワークに対する攻撃を検知する攻撃検知装置であって、
前記ネットワークにおいて周期的に送信されるメッセージ又は前記メッセージとは非同期に送信されるメッセージのうち、或る期間において送信された共通の値を含む複数のメッセージの前記値が前記第２の型に対応する場合に、当該複数のメッセージの中から、直前のメッセージとペイロードが同一であるメッセージを抽出する抽出部と、
前記値が前記第２の型に対応する場合に、前記抽出部が抽出したメッセージの送信の間隔と、前記周期的に送信されるメッセージの送信周期との差分が閾値を超える場合には、前記攻撃が有ると判定する判定部と、
を有することを特徴とする攻撃検知装置。
【請求項５】
周期的なメッセージとは非同期なメッセージの直後の前記周期的なメッセージの送信間隔が前記周期的なメッセージの周期となる第１の型と、前記非同期なメッセージが前記周期的なメッセージの周期に影響しない第２の型との通信が行われる機器内のネットワークに対する攻撃を検知する攻撃検知方法であって、
前記ネットワークにおいて周期的に送信されるメッセージ又は前記メッセージとは非同期に送信されるメッセージのうち、或る期間において送信された共通の値を含む複数のメッセージの前記値が前記第１の型に対応する場合に、当該複数のメッセージの中から、ペイロードが同一である２つのメッセージの組を抽出する抽出手順と、
前記値が前記第１の型に対応する場合に、前記組に係る２つのメッセージの送信の間における他のメッセージの送信の有無と、当該２つのメッセージの送信の間隔とに基づいて、前記攻撃の有無を判定する判定手順と、
をコンピュータが実行ことを特徴とする攻撃検知方法。
【請求項６】
周期的なメッセージとは非同期なメッセージの直後の前記周期的なメッセージの送信間隔が前記周期的なメッセージの周期となる第１の型と、前記非同期なメッセージが前記周期的なメッセージの周期に影響しない第２の型との通信が行われる機器内のネットワークに対する攻撃を検知する攻撃検知方法であって、
前記ネットワークにおいて周期的に送信されるメッセージ又は前記メッセージとは非同期に送信されるメッセージのうち、或る期間において送信された共通の値を含む複数のメッセージの前記値が前記第２の型に対応する場合に、当該複数のメッセージの中から、直前のメッセージとペイロードが同一であるメッセージを抽出する抽出手順と、
前記値が前記第２の型に対応する場合に、前記抽出手順が抽出したメッセージの送信の間隔と、前記周期的に送信されるメッセージの送信周期との差分が閾値を超える場合には、前記攻撃が有ると判定する判定手順と、
をコンピュータが実行ことを特徴とする攻撃検知方法。
【請求項７】
請求項１乃至４いずれか一項記載の攻撃検知装置としてコンピュータを機能させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、攻撃検知装置、攻撃検知方法及びプログラムに関する。
【背景技術】
【０００２】
ＩｏＴ機器の中には、複数の電子制御装置が搭載されているものがある。例えば、自動車には、電子制御装置としてＥＣＵ（Electronic Control Unit）が搭載されている。以下、ＩｏＴ機器の種別によらず、便宜上、その電子制御装置を「ＥＣＵ」という。
【０００３】
複数のＥＣＵは、バス型のネットワーク（以下、「ＣＡＮバス」という。）に接続され、ＣＡＮ（Controller Area Network）プロトコルに従ったメッセージをＣＡＮバスにブロードキャストすることで相互に通信を行って機能している。
【０００４】
ＣＡＮ通信において送受信されるメッセージ（以下、「通信メッセージ」という。）には、送信対象のデータ本体であるペイロードと、ペイロードの内容の識別に用いられるＩＤ（以下、「ＣＡＮ－ＩＤ」という。）が格納されている。
【０００５】
通信メッセージには送信元に関する情報が含まれていないため、なりすましによって不正なメッセージをＣＡＮバスに送信（挿入）することが容易である。例えば、不正なメッセージを挿入することによって自動車の制御が乗っ取られることが知られている。そのため、ＣＡＮバスに挿入された不正な通信メッセージを検知する技術が重要となっている。
【０００６】
自動車の制御等の機能に関わるほとんどの通信メッセージは、図１に示す通りＣＡＮ－ＩＤごとの送信周期で周期的に送信されるように設計されている。不正な通信メッセージの挿入攻撃が発生した場合、図２に示す通り、送信周期よりも短い間隔でのメッセージ送信が発生する。従来、この特徴を利用したルールベースな攻撃検知技術が存在する（例えば、非特許文献１）。
【先行技術文献】
【非特許文献】
【０００７】
【文献】大塚敏史，石郷岡祐，"既存ECUを変更不要な車載LAN向け侵入検知手法"，情報処理学会研究報告，Vol.2013-SLDM-160，No.6，pp.1-5 (2013).
【発明の概要】
【発明が解決しようとする課題】
【０００８】
自動車の制御等に関わるほとんどのＣＡＮ－ＩＤのメッセージはＣＡＮ－ＩＤごとに周期的に送信されている一方で、周期的なメッセージ送信に加えて運転手の操作等のイベントに連動したメッセージ送信が混在する通信（以下、「周期＋イベント型通信」という。）が存在する。従来技術では、「周期＋イベント型通信」については考慮されていないため、正常な通信について攻撃であると誤検知してしまう可能性が有る。
【０００９】
本発明は、上記の点に鑑みてなされたものであって、機器内のネットワークに対する攻撃の検知精度を向上させることを目的とする。
【課題を解決するための手段】
【００１０】
そこで上記課題を解決するため、周期的なメッセージとは非同期なメッセージの直後の前記周期的なメッセージの送信間隔が前記周期的なメッセージの周期となる第１の型と、前記非同期なメッセージが前記周期的なメッセージの周期に影響しない第２の型との通信が行われる機器内のネットワークに対する攻撃を検知する攻撃検知装置は、前記ネットワークにおいて周期的に送信されるメッセージ又は前記メッセージとは非同期に送信されるメッセージのうち、或る期間において送信された共通の値を含む複数のメッセージの前記

値が前記第１の型に対応する場合に、当該複数のメッセージの中から、ペイロードが同一である２つのメッセージの組を抽出する抽出部と、前記値が前記第１の型に対応する場合に、前記組に係る２つのメッセージの送信の間における他のメッセージの送信の有無と、当該２つのメッセージの送信の間隔とに基づいて、前記攻撃の有無を判定する判定部と、を有する。

【発明の効果】

【００１１】

機器内のネットワークに対する攻撃の検知精度を向上させることができる。

【図面の簡単な説明】

【００１２】

【図１】通信メッセージの周期性を説明するための図である。

【図２】従来技術における不正な通信メッセージの挿入攻撃の検知方法を説明するための図である。

【図３】第１の実施の形態における通信システム１の構成例を示す図である。

【図４】第１の実施の形態における通信情報処理装置１０のハードウェア構成例を示す図である。

【図５】Ｔｙｐｅ－Ａを説明するための図である。

【図６】Ｔｙｐｅ－Ｂを説明するための図である。

【図７】Ｔｙｐｅ－Ａにおける攻撃の誤検知を説明するための図である。

【図８】ルールＡ１によってＴｙｐｅ－Ａに対する攻撃を検知できる理由を説明するための図である。

【図９】ルールＡ２によってＴｙｐｅ－Ａに対する攻撃を検知できる理由を説明するための図である。

【図１０】Ｔｙｐｅ－Ｂに対する攻撃を検知できる理由を説明するための図である。

【図１１】第１の実施の形態における通信システム１の機能構成例を示す図である。

【図１２】通信情報処理装置１０が実行する処理手順の一例を説明するためのフローチャートである。

【図１３】Ｔｙｐｅ－Ａに関する処理手順の説明を補足するための図である。

【図１４】Ｔｙｐｅ－Ｂに関する処理手順の説明を補足するための図である。

【図１５】第２の実施の形態における通信システム１の機能構成例を示す図である。

【図１６】第３の実施の形態における通信システム１の機能構成例を示す図である。

【発明を実施するための形態】

【００１３】

以下、図面に基づいて本発明の実施の形態を説明する。図３は、第１の実施の形態における通信システム１の構成例を示す図である。図３において、機器ｄ１と外部装置３０とは、インターネット等の外部ネットワークＮ１を介して接続される。外部ネットワークＮ１は、移動体通信網等の無線通信網を含んでもよい。

【００１４】

機器ｄ１は、自動車や電車、飛行機、船、ドローン等の移動体や農業用センサネットワーク等に代表されるＩｏＴ（Internet of Things）機器である。本実施の形態では、機器ｄ１が自動車である例を想定するが、他の種類のＩｏＴ機器について本実施の形態が適用されてもよい。

【００１５】

図３において、機器ｄ１は、複数のＥＣＵ２０、ＣＡＮバスＮ２及び通信情報処理装置１０等のハードウェアを含む。

【００１６】

ＥＣＵ２０は、機器ｄ１の各種機能・機構を電子的に制御する電子制御装置の一例である。各ＥＣＵ２０は、バス型の機器内ネットワーク（以下、「ＣＡＮバスＮ２」という。）を介したＣＡＮ（Controller Area Network）通信によって相互にメッセージ（以下、「通信メッセージ」という。）の送受信を行う。本実施の形態では、ＣＡＮ通信を仮定

して説明するが、本実施の形態は、通信群をヘッダー情報等（ＣＡＮ通信の場合はＣＡＮ－ＩＤ）で分類すると、それぞれが通信間隔に周期性を有する、又はペイロードの特定の値の変化に従い周期性が変化する、といった通信特性を有する他の通信プロトコルや機器内ネットワークに対して適用可能である。なお、本実施の形態では、周期的な通信メッセージに加えて、機器ｄ１の操作者（機器ｄ１が自動車であれば運転手等）による操作等のイベントに連動したメッセージ送信が混在する通信（以下、「周期＋イベント型通信」という。）について考慮する。以下、通信メッセージのうち、周期的に送信されるメッセージを「周期的メッセージ」といい、周期的メッセージの周期とは非同期に発生するイベントに応じて送信されるメッセージを「イベントメッセージ」という。

【００１７】

通信情報処理装置１０は、ＣＡＮバスＮ２における通信メッセージを監視することで、ＣＡＮバスＮ２に対する攻撃の有無を判定し、判定結果を外部装置３０へ送信する装置（コンピュータ）である。

【００１８】

外部装置３０は、通信情報処理装置１０による判定結果を記憶する１以上のコンピュータである。

【００１９】

図４は、第１の実施の形態における通信情報処理装置１０のハードウェア構成例を示す図である。図４の通信情報処理装置１０は、それぞれバスＢで相互に接続されている補助記憶装置１０１、メモリ装置１０２、ＣＰＵ１０３、及びインタフェース装置１０４等を有する。

【００２０】

通信情報処理装置１０での処理を実現するプログラムは、補助記憶装置１０１にインストールされる。補助記憶装置１０１は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

【００２１】

メモリ装置１０２は、プログラムの起動指示があった場合に、補助記憶装置１０１からプログラムを読み出して格納する。ＣＰＵ１０３は、メモリ装置１０２に格納されたプログラムに従って通信情報処理装置１０に係る機能を実行する。インタフェース装置１０４は、ＣＡＮバスＮ２や外部ネットワークＮ１に接続するためのインタフェースとして用いられる。

【００２２】

なお、外部装置３０も同様のハードウェア構成を有してもよい。

【００２３】

本実施の形態における、周期＋イベント型通信について説明する。本実施の形態では、周期＋イベント型通信の型（Ｔｙｐｅ）をＴｙｐｅ－ＡとＴｙｐｅ－Ｂとに分類する。

【００２４】

図５は、Ｔｙｐｅ－Ａを説明するための図である。図５に示されるように、Ｔｙｐｅ－Ａは、イベントメッセージとその直後の周期的メッセージとの送信間隔が、当該周期的メッセージのＣＡＮ－ＩＤに対応した送信周期になる型である。

【００２５】

図６は、Ｔｙｐｅ－Ｂを説明するための図である。図６に示されるように、Ｔｙｐｅ－Ｂは、イベントメッセージの有無に関わらず、周期的メッセージの送信間隔が送信周期となる型（すなわち、イベントメッセージが、周期的メッセージの送信周期に影響しない型）である。

【００２６】

なお、非特許文献１の技術を用いてＴｙｐｅ－Ａのメッセージを監視した場合、$\beta < z$であれば誤検知の可能性は低い。しかし、$\beta \geqq z$の場合や、図７のように、イベントメッセージが２連続で送信された場合には、攻撃の発生を誤検知してしまう。

【００２７】

一方、非特許文献１の技術を用いてＴｙｐｅ－Ｂのメッセージを監視した場合、図６の通信メッセージｍ１と通信メッセージｍ２の間隔が送信周期＋β以内であれば、その間で発生する全てのイベントメッセージを攻撃として誤検知してしまう。

【００２８】

そこで、本実施の形態では、Ｔｙｐｅ（型）ごとに、当該Ｔｙｐｅに適した方法（以下、「検知方法」という。）で攻撃を検知する。

【００２９】

Ｔｙｐｅ－Ａに対する攻撃の検知方法について説明する。Ｔｙｐｅ－Ａに対する検知方法の手順の概要は、以下の通りである。

（１）或る期間における通信メッセージのうち、同一ペイロードを持つ２つのメッセージの全ての組を対象メッセージとして抽出

（２）抽出した各組の２つのメッセージから以下の２つの特徴量ａ１及びａ２を抽出

（ａ１）２つのメッセージが非隣接関係を有するか隣接関係を有するかを示す特徴量（「非隣接関係」／「隣接関係」）（以下、「特徴量ａ１」という。）

（ａ２）２つのメッセージの送信時刻の間隔（送信間隔）と送信周期との類否を示す特徴量（「類似」／「非類似」）（以下、「特徴量ａ２」という。）

なお、特徴量ａ１について、隣接関係とは、送信時刻（送信タイミング）が２つのメッセージの送信時刻（送信タイミング）の間に含まれる他のメッセージが存在しない関係をいう。一方、非隣接関係とは、送信時刻が２つのメッセージの送信時刻の間に含まれる他のメッセージが存在する関係をいう。

（３）抽出した２つの特徴量が以下のルールＡ１及びルールＡ２のいずれか一方、又は双方に該当する場合は攻撃が発生したと判定（攻撃の発生を検知）

ルールＡ１：特徴量ａ１＝「隣接関係」、かつ、特徴量ａ２＝「非類似」

ルールＡ２：特徴量ａ１＝「非隣接関係」、かつ、特徴量ａ２＝「類似」

上記のルールＡ１及びＡ２によって、Ｔｙｐｅ－Ａに対する攻撃を検知できる理由について説明する。

【００３０】

図８は、ルールＡ１によってＴｙｐｅ－Ａに対する攻撃を検知できる理由を説明するための図である。なお、図８において、通信メッセージｍ１～ｍ５のそれぞれに対して付与されている吹き出し内の文字「Ｐ」は、ペイロードの値を示す。すなわち、当該文字が同じ通信メッセージのペイロードは同一であることを示す。したがって、図８における通信メッセージｍ１～ｍ５のペイロードは同一である。

【００３１】

ＥＣＵ２０は、正常な状態（攻撃が無い状態）において、ＣＡＮ－ＩＤが同じ通信メッセージについて、周期的メッセージとペイロードが同一であるイベントメッセージ（以下、「ペイロード変化の無いイベントメッセージ」という。）の送信は行わない。すなわち、正常な状態（攻撃が無い状態）において、図８に示されるような状態（ルールＡ１に該当する状態）は発生しない。ルールＡ１によれば、ペイロード変化の無いイベントメッセージを検知することができる。したがって、ルールＡ１によって検知されるのは、正常なイベントメッセージではなく、リプレイ攻撃等の挿入攻撃であると検知可能である。

【００３２】

図９は、ルールＡ２によってＴｙｐｅ－Ａに対する攻撃を検知できる理由を説明するための図である。図９の吹き出しの意味は、図８と同じである。したがって、図９において、通信メッセージｍ３のペイロード「Ｒ」は、他の通信メッセージのペイロード「Ｐ」と異なる。

【００３３】

ＥＣＵ２０が送信する通信メッセージの送信周期やペイロードは、挿入攻撃（攻撃目的の通信メッセージの挿入）の影響を受けて変化することはない。つまり、挿入攻撃の前後の通信メッセージのペイロードが必ず等しく、かつ、送信間隔が周期間隔と等しくなる。ルールＡ２によれば、このような状態を検知することができるため攻撃を検知することが

できる。
【００３４】
なお、本実施の形態では、Ｔｙｐｅ－Ａに対して２つのルールが採用される例を説明するが、ルールＡ１及びルールＡ２のうちのいずれか一方のみが採用されてもよい。
【００３５】
次に、Ｔｙｐｅ－Ｂに対する攻撃の検知方法について説明する。Ｔｙｐｅ－Ｂに対する検知方法の手順の概要は、以下の通りである。
（１）対象メッセージとして、直前の通信メッセージと同一のペイロードを含む２以上の通信メッセージを抽出
（２）抽出された通信メッセージ群から以下の特徴量ｂを抽出
（ｂ）抽出された通信メッセージ間の送信時刻の間隔（送信間隔）と送信周期との類否を示す特徴量（「類似」／「非類似」）
（３）特徴量ｂが、以下のルールＢに該当する場合は攻撃であると判定
ルールＢ：特徴量ｂ＝「非類似」
ルールＢによってＴｙｐｅ－Ｂに対する攻撃を検知できる理由について説明する。図１０は、Ｔｙｐｅ－Ｂに対する攻撃を検知できる理由を説明するための図である。
【００３６】
Ｔｙｐｅ－Ｂの正常状態では、イベントメッセージの有無に関わらず、図１０（１）に示されるように、「直前の通信メッセージと同一のペイロードを含む通信メッセージ」が必ず周期間隔で送信される。なお、図１０（１）において、通信メッセージｍ１の直前の通信メッセージは図示されていないが、通信メッセージｍ１は、非図示の直前の通信メッセージと同一のペイロードを含む通信メッセージであるとする。そうすると、図１０（１）において、通信メッセージｍ１、ｍ２、ｍ４及びｍ５が、直前の通信メッセージと同一のペイロードを含む通信メッセージに該当し、これらの送信間隔は周期的である。
【００３７】
一方、挿入攻撃が行われた場合、図１０（２）に示す通り、「直前の通信メッセージと同一のペイロードを含む通信メッセージ」が必ず周期間隔で出現しなくなる。なお、図１０（２）において、通信メッセージｍ１は、（１）と同様に、非図示の直前の通信メッセージと同一のペイロードを含む通信メッセージである。そうすると、図１０（２）において、通信メッセージｍ１、ｍ５、ｍ６及びｍ７が直前の通信メッセージと同一のペイロードを含む通信メッセージに該当するところ、これらの通信メッセージの送信間隔は非周期である（本来の周期ではない）。Ｔｙｐｅ－Ｂに対するルールは、「直前の通信メッセージと同一のペイロードを含む通信メッセージ」が周期間隔で出現しなくなったことを検知するルールであるため、挿入攻撃を検知できる。
【００３８】
上記のような攻撃の検知を実現するために、通信システム１は、図１１に示されるような機能構成を有する。図１１は、第１の実施の形態における通信システム１の機能構成例を示す図である。以下では、一つのＣＡＮ－ＩＤ（に係る通信メッセージ）を監視対象(以下、「対象ＩＤ」という。)とした場合について説明する。監視対象のＣＡＮ－ＩＤが複数存在する場合には、ＣＡＮ－ＩＤごとに以下の説明の内容が実施されればよい。
【００３９】
図１１において、通信情報処理装置１０は、通信メッセージ取得部１１、Ｔｙｐｅ判定部１２、対象メッセージ抽出部１３、特徴量抽出部１４及びルール判定部１５等を含む。これら各部は、通信情報処理装置１０にインストールされた１以上のプログラムが、ＣＰＵ１０３に実行させる処理により実現される。通信情報処理装置１０は、また、ＩＤ情報ＤＢ１６及びルールＤＢ１７等のデータベース（記憶部）を利用する。これら各データベース（各記憶部）は、例えば、補助記憶装置１０１等を用いて実現可能である。
【００４０】
なお、Ｔｙｐｅ判定部１２、対象メッセージ抽出部１３、特徴量抽出部１４、ルール判定部１５、ＩＤ情報ＤＢ１６及びルールＤＢ１７は、攻撃検知部１１０を構成する。

【００４１】
一方、外部装置３０は、判定結果記憶部３１を有する。判定結果記憶部３１は、外部装置３０が有する補助記憶装置等を用いて実現可能である。
【００４２】
通信メッセージ取得部１１は、或る期間内（以下、「対象期間」という。）に発生した、対象ＩＤを含む各通信メッセージの「ペイロード」及び「送信時刻」を取得する。但し、通信メッセージ取得部１１は、ＣＡＮ－ＩＤやＤＬＣ（Data Length Code）等の他のフィールドの値を追加で取得してもよい。なお、「送信時刻」は、通信メッセージ取得部１１が通信メッセージを取得した時刻（タイミング）である。「送信時刻」の値は、絶対時刻でもよいし、何らかの基準時刻からの相対時刻（経過時間）でもよい。また、対象期間は、対象ＩＤに対してＩＤ情報ＤＢ１６に設定されている送信周期の２倍以上の期間であることが望ましいが、対象期間は、当該送信周期以下でもよい。また、通信メッセージ取得部１１は、全ての通信メッセージを取得してもよいし、何らかの条件が満たされた場合（例えば別の異常検知機構が異常を検知した場合）に、当該異常に関連する通信メッセージを取得してもよい。
【００４３】
ＩＤ情報ＤＢ１６には、ＣＡＮ－ＩＤごとに予め設定された、送信周期、マージンβ及びＴｙｐｅが、各ＣＡＮ－ＩＤに対応付けられて記憶されている。但し、ＩＤ情報ＤＢ１６に記憶される情報は、これらに限られなくてもよい。
【００４４】
Ｔｙｐｅ判定部１２は、ＩＤ情報ＤＢ１６に記憶されている情報を参照して、対象ＩＤに対応するＴｙｐｅを判定する。
【００４５】
対象メッセージ抽出部１３は、Ｔｙｐｅに応じた対象メッセージを抽出する。
【００４６】
特徴量抽出部１４は、対象ＩＤの送信周期、マージンβ及びＴｙｐｅをＩＤ情報ＤＢ１６から取得し、これらの情報に基づいて、対象メッセージ抽出部１３が抽出した対象メッセージから、当該Ｔｙｐｅに応じた特徴量（後述される特徴量ａ１及びａ２又は特徴量ｂ）を抽出する。但し、特徴量抽出部１４は、特徴量ａ１及びａ２又は特徴量ｂ以外の特徴量を追加で抽出してもよい。
【００４７】
ルールＤＢ１７には、予め定義されたルール（上記したルールＡ１及びＡ２、並びにルールＢ）がＴｙｐｅごとに記憶されている。ルールとは、攻撃を検知するためのルールをいう。但し、ルールＡ１及びＡ２、並びにルールＢ以外のルール（以下、「ルールＣ」という。）がルールＤＢ１７に記憶されてもよい。
【００４８】
ルール判定部１５は、対象ＩＤに対応するＴｙｐｅをＩＤ情報ＤＢ１６から取得し、当該Ｔｙｐｅに対応するルールをルールＤＢ１７から取得する。ルール判定部１５は、特徴量抽出部１４が抽出した特徴量がルールに該当（合致）するかどうか否かを判定し、攻撃の有無を判定（攻撃を検知）する。ルール判定部１５は、判定結果を判定結果記憶部３１に記録（送信）する。
【００４９】
なお、ＩＤ情報ＤＢ１６及びルールＤＢ１７からの情報又はルールの取得は、最初に１度だけ行われてもよいし、判定の都度行われてもよい。また、ルールＣがルールＤＢ１７に記憶されている場合、ルール判定部１５は、ルールＣも用いて攻撃の有無を判定してもよい。
【００５０】
以下、通信情報処理装置１０が実行する処理手順について説明する。図１２は、通信情報処理装置１０が実行する処理手順の一例を説明するためのフローチャートである。
【００５１】

通信メッセージ取得部１１は、対象期間において、ＣＡＮバスＮ２に送信される通信メッセージ群のうち、対象ＩＤを含む複数の通信メッセージのそれぞれの「ペイロード」及び「送信時刻」を取得する（Ｓ１０１）。続いて、Ｔｙｐｅ判定部１２は、対象ＩＤに対応するＴｙｐｅをＩＤ情報ＤＢ１６から取得して、当該Ｔｙｐｅが「Ｔｙｐｅ－Ａ」であるか「Ｂ」であるかを判定する（Ｓ１０２）。

【００５２】

対象ＩＤに対応するＴｙｐｅが「Ｔｙｐｅ－Ａ」である場合（Ｓ１０３でＹｅｓ）、対象メッセージ抽出部１３は、通信メッセージ取得部１１が取得した複数の通信メッセージから、同一ペイロードを含む２つのメッセージの全ての組のそれぞれを対象メッセージとして抽出する（Ｓ１０４）。

【００５３】

図１３は、Ｔｙｐｅ－Ａに関する処理手順の説明を補足するための図である。図１３では、ステップＳ１０１において、｛ｍ１，ｍ２，ｍ３，ｍ４，ｍ５，ｍ６｝の通信メッセージが取得された例が示されている。図１３において、横軸は、時間に対応し、縦軸はペイロードに対応する。すなわち、ステップＳ１０４では、縦軸において同じ値を有する通信メッセージの組が抽出される。例えば、｛ｍ１，ｍ２｝、｛ｍ３，ｍ４｝、｛ｍ３，ｍ６｝、｛ｍ４，ｍ６｝の４つの組のそれぞれが対象メッセージとして抽出される。具体的には、｛ｍ１，ｍ２｝のペイロードはＰａである。｛ｍ３，ｍ４｝、｛ｍ３，ｍ６｝及び｛ｍ４，ｍ６｝のペイロードはＰｃである。なお、通信メッセージｍ５のペイロードは、Ｐｂであるところ、Ｐｂと同一のペイロードを有する通信メッセージは、対象期間において取得（観測）されなかったため、通信メッセージｍ５を含む組は抽出されない。

【００５４】

続いて、特徴量抽出部１４は、対象ＩＤに対応する送信周期、マージンβ及びＴｙｐｅをＩＤ情報ＤＢ１６から取得し、これらの情報に基づいて、各対象メッセージ（各組）から、当該Ｔｙｐｅ（＝Ｔｙｐｅ－Ａ）に対応する特徴量（以下の特徴量ａ１及びａ２）を抽出する（Ｓ１０５）。

（ａ１）２つのメッセージが非隣接関係を有するか隣接関係を有することを示す特徴量（「非隣接関係」／「隣接関係」）

（ａ２）２つのメッセージの送信時刻の間隔と対象ＩＤに対応する送信周期との類否を示す特徴量（「類似」／「非類似」）

ここで、特徴量ａ２における送信時刻の間隔と送信周期との類否は、例えば、以下のように定義される。

・２つのメッセージの送信時刻の間隔が送信周期±βの範囲内であれば（すなわち、当該送信時刻の間隔と当該送信周期との差分（差の絶対値）が閾値（＝β）以下であれば）、当該間隔と当該送信周期とは類似している。なお、βは、送信周期未満であるのが望ましい。

・２つのメッセージの送信時刻の間隔が送信周期±βの範囲外であれば（すなわち、当該送信時刻の間隔と当該送信周期との差分（差の絶対値）が閾値（＝β）を超えれば）、当該間隔と当該送信周期とは類似していない。

【００５５】

なお、図１３の例では、｛ｍ１，ｍ２｝及び｛ｍ３，ｍ４｝のそれぞれの組について抽出される特徴量ａ１は、「隣接関係」であり、｛ｍ３，ｍ６｝及び｛ｍ４，ｍ６｝のそれぞれの組について抽出される特徴量ａ１は、「非隣接関係」である。また、｛ｍ１，ｍ２｝、｛ｍ３，ｍ４｝及び｛ｍ４，ｍ６｝のそれぞれの組について抽出される特徴量ａ２は、「類似」であり、｛ｍ３，ｍ６｝の組について抽出される特徴量ａ２は、「非類似」である。

【００５６】

続いて、ルール判定部１５は、対象メッセージごとに抽出された特徴量に基づいて、攻撃の有無を判定する（Ｓ１０６）。すなわち、ルール判定部１５は、対象ＩＤに対応するＴｙｐｅをＩＤ情報ＤＢ１６から取得すると共に、当該Ｔｙｐｅ（＝Ｔｙｐｅ－Ａ）に対

応する、以下のルールＡ１及びルールＡ２をルールＤＢ１７から取得する。ルール判定部１５は、対象メッセージごと（組ごと）に抽出された特徴量ａ１及びａ２の組（以下、当該組を「特徴量ａ」という。）が、当該ルールＡ１及びルールＡ２のうちの少なくともいずれか一方に該当するか否かを判定することで、攻撃の有無を判定する。
ルールＡ１：特徴量ａ１＝「隣接関係」、かつ、特徴量ａ２＝「非類似」
ルールＡ２：特徴量ａ１＝「非隣接関係」、かつ、特徴量ａ２＝「類似」
　すなわち、ルール判定部１５は、少なくともいずれか一方のルールに該当する特徴量ａが有る場合は、対象期間（において通信メッセージ取得部１１によって取得された通信メッセージ群の中）中に攻撃が含まれると判定する。
【００５７】
　図１３の例では、｛ｍ３，ｍ６｝の特徴量ａがルールＡ２に該当する。したがって、この場合、対象期間（において通信メッセージ取得部１１によって取得された通信メッセージ群の中）に攻撃が含まれていると判定される。
【００５８】
　一方、対象ＩＤに対応するＴｙｐｅが「Ｔｙｐｅ－Ｂ」である場合（Ｓ１０３でＮｏ）、対象メッセージ抽出部１３は、通信メッセージ取得部１１が取得した複数の通信メッセージから、直前の通信メッセージと同一のペイロードを含む通信メッセージのそれぞれを対象メッセージとして抽出する（Ｓ１０７）。
【００５９】
　図１４は、Ｔｙｐｅ－Ｂに関する処理手順の説明を補足するための図である。図１４では、ステップＳ１０１において、｛ｍ１，ｍ２，ｍ３，ｍ４，ｍ５，ｍ６｝の通信メッセージが取得された例が示されている。図１４における横軸及び縦軸の意味は、図１３と同じである。したがって、図１４の例では、ステップＳ１０７においてｍ２及びｍ４のそれぞれが対象メッセージとして抽出される。すなわち、通信メッセージｍ２のペイロードはＰａであるところ、直前の通信メッセージｍ１のペイロードもＰａである。また、通信メッセージｍ４のペイロードはＰｃであるところ、直前の通信メッセージｍ３のペイロードもＰｃである。
【００６０】
　続いて、特徴量抽出部１４は、対象ＩＤに対応する送信周期、マージンβ及びＴｙｐｅをＩＤ情報ＤＢ１６から取得し、これらの情報に基づいて、対象メッセージ群から、当該Ｔｙｐｅ（＝Ｔｙｐｅ－Ｂ）に対応する特徴量（以下の特徴量ｂ）を抽出する（Ｓ１０８）。
（ｂ）対象メッセージの送信時刻の間隔と送信周期との類否を示す特徴量（「類似」／「非類似」）
　なお、特徴量ｂに関する類否の判定方法は、特徴量ａ２と同様でよい。
【００６１】
　続いて、ルール判定部１５は、対象ＩＤに対応するＴｙｐｅをＩＤ情報ＤＢ１６から取得すると共に、当該Ｔｙｐｅ（＝Ｔｙｐｅ－Ｂ）に対応する、以下のルールＢをルールＤＢ１７から取得して、対象メッセージごと（組ごと）に抽出された特徴量ｂが、ルールＢに該当するか否かを判定することで、攻撃の有無を判定する（Ｓ１０９）。
ルールＢ：特徴量ｂ＝「非類似」
　すなわち、ルール判定部１５は、いずれかの特徴量ｂがルールＢに該当する場合、対象期間（において通信メッセージ取得部１１によって取得された通信メッセージ群の中）に攻撃が含まれると判定する。なお、対象メッセージが１つしか抽出されない場合、ルール判定部１５は、攻撃が有ると判定してもよい。
【００６２】
　ステップＳ１０６又はステップＳ１０９に続いて、ルール判定部１５は、ステップＳ１０６又はステップＳ１０９の判定結果（攻撃の有無）を示す情報を判定結果記憶部３１に記録（送信）する（Ｓ１１０）。当該情報は、例えば、対象期間の開始時刻及び終了時刻と、攻撃の有無の判定結果とを含んでもよい。更に、攻撃が有ると判定された場合（攻撃

が検知された場合）、攻撃を検知したルールが当該情報に含まれてもよい。
【００６３】
上述したように、第１の実施の形態によれば、周期型のみならず、周期＋イベント型のＣＡＮ－ＩＤを持つメッセージで発生する正常なイベント送信と挿入攻撃を見分けることができるようになる。その結果、正常なイベントメッセージを攻撃として誤検知する可能性を低下させることができ、挿入攻撃を検知できる可能性を高めることができる。すなわち、機器内のネットワークに対する攻撃の検知精度を向上させることができる。
【００６４】
なお、本実施の形態では、自動車の制御通信（ＣＡＮ通信）を仮定して説明したが、本実施の形態は、次の通信特性を有する他の通信プロトコルやＩｏＴ機器内ネットワーク通信に対して適用可能な不正メッセージの挿入攻撃検知技術である。
【００６５】
次に、第２の実施の形態について説明する。第２の実施の形態では第１の実施の形態と異なる点について説明する。第２の実施の形態において特に言及されない点については、第１の実施の形態と同様でもよい。
【００６６】
図１５は、第２の実施の形態における通信システム１の機能構成例を示す図である。図１５中、図１１と同一部分には同一符号を付し、その説明は省略する。
【００６７】
図１５において、通信情報処理装置１０は、更に、対象期間選択部１８を有する。対象期間選択部１８は、対象期間（通信メッセージ取得部１１が通信メッセージを監視（取得）する期間）を選択する。例えば、対象期間選択部１８は、何らかの基準を満たす期間、又は他の異常検知器で異常が検知された期間を対象期間として選択してもよい。何らかの基準を満たす期間の一例として、対象ＩＤを含む通信メッセージについて、ペイロードが変化したタイミングを中心とした期間や、送信間隔が送信周期よりも短い通信メッセージが観測されたタイミングを中心とした期間等が挙げられる。
【００６８】
次に、第３の実施の形態について説明する。第３の実施の形態では第１又は第２の実施の形態と異なる点について説明する。第３の実施の形態において特に言及されない点については、第１又は第２の実施の形態と同様でもよい。
【００６９】
図１５は、第３の実施の形態における通信システム１の機能構成例を示す図である。図１５中、図１１と同一部分には同一符号を付し、その説明は省略する。
【００７０】
図１５では、外部装置３０が攻撃検知部１１０を有する構成が示されている。この場合、通信メッセージ取得部１１は、取得した各通信メッセージの「ペイロード」及び「送信時刻」を外部装置３０へ送信する。外部装置３０の攻撃検知部１１０は、これらの情報を受信すると、図１２のステップＳ１０２以降の処理手順を実行する。
【００７１】
このように、攻撃の有無の判定（攻撃の検知）は、機器ｄ１の外部のコンピュータを用いて行われてもよい。
【００７２】
なお、第３の実施の形態において、通信情報処理装置１０は、対象期間選択部１８を有さなくてもよい。
【００７３】
なお、上記各実施の形態は、周期型のＣＡＮ－ＩＤを対象とした既存の異常検知技術と組み合わせることで、周期型のＣＡＮ－ＩＤも監視対象として実施されてもよい。
【００７４】
なお、上記各実施の形態において、通信情報処理装置１０又は外部装置３０は、攻撃検知装置の一例である。対象メッセージ抽出部１３は、抽出部の一例である。ルール判定部

１５は、判定部の一例である。

【００７５】

以上、本発明の実施の形態について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

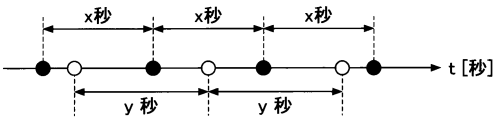
【符号の説明】

【００７６】

１	通信システム
１０	通信情報処理装置
１１	通信メッセージ取得部
１２	Ｔｙｐｅ判定部
１３	対象メッセージ抽出部
１４	特徴量抽出部
１５	ルール判定部
１６	ＩＤ情報ＤＢ
１７	ルールＤＢ
１８	対象期間選択部
２０	ＥＣＵ
３０	外部装置
３１	判定結果記憶部
１０１	補助記憶装置
１０２	メモリ装置
１０３	ＣＰＵ
１０４	インタフェース装置
１１０	攻撃検知部
Ｂ	バス
ｄ１	機器
Ｎ１	外部ネットワーク
Ｎ２	ＣＡＮバス

【図面】

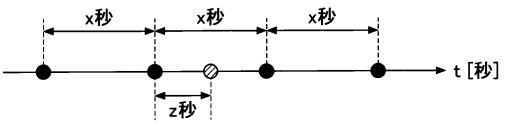
【図１】



● CAN-ID=Aのメッセージ(送信周期x秒)が送信された時刻

○ CAN-ID=Bのメッセージ(送信周期y秒)が送信された時刻

【図２】

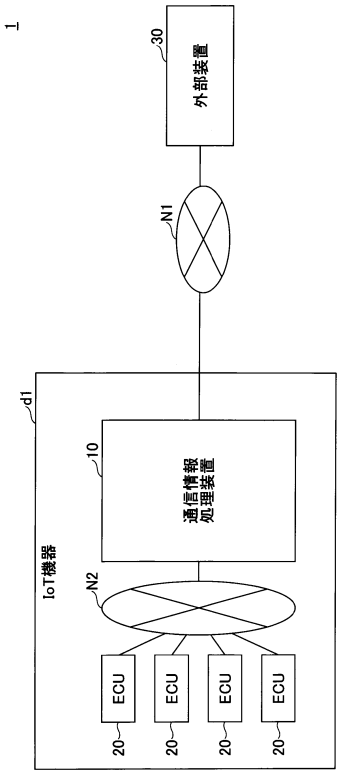


z秒 (z < x) でのメッセージ送信が発生

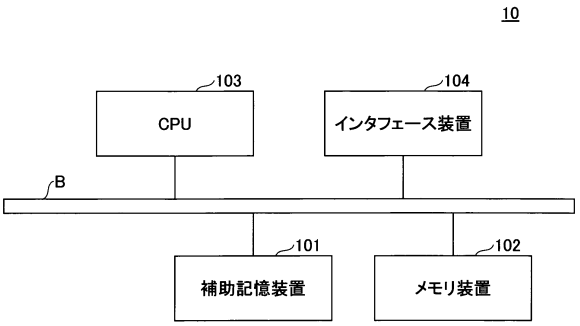
● CAN-ID=Aのメッセージ(送信周期x秒)が送信された時刻

⊘ CAN-ID=Aの不正メッセージが挿入された時刻

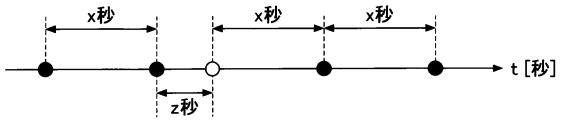
【図３】



【図４】



【図５】

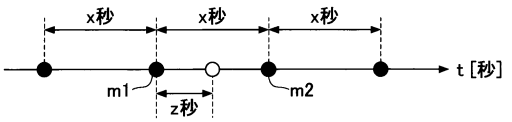


z秒 (z < x) でイベント送信

● CAN-ID=Aの周期的メッセージ(送信周期x秒)が送信された時刻

○ CAN-ID=Aのイベントメッセージが送信された時刻

【図６】

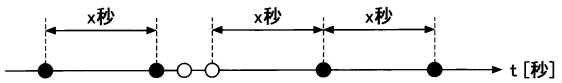


z秒 (z < x) でイベント送信

● CAN-ID=Aの周期的メッセージ(送信周期x秒)が送信された時刻

○ CAN-ID=Aのイベントメッセージが送信された時刻

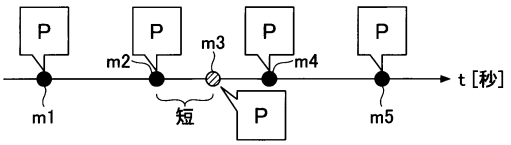
【図７】



● CAN-ID=Aの周期的メッセージ(送信周期x秒)が送信された時刻

○ CAN-ID=Aのイベントメッセージが送信された時刻

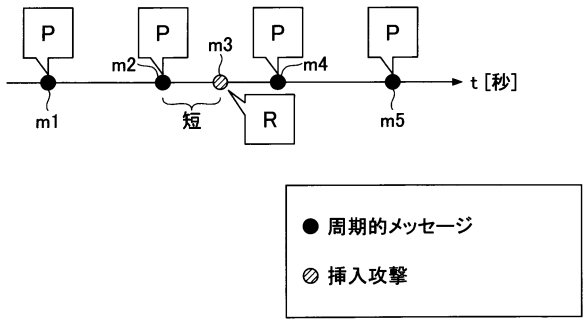
【図８】



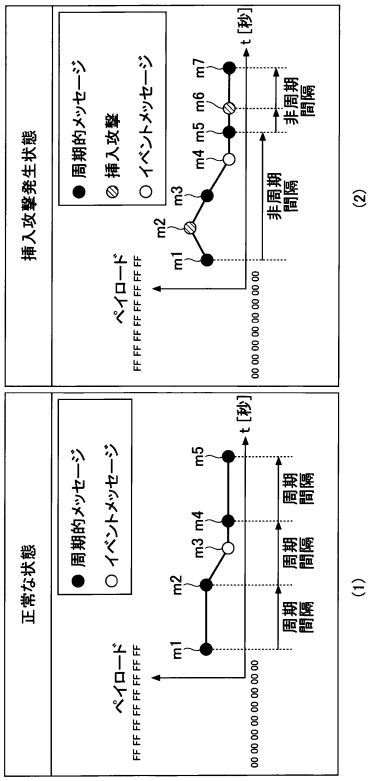
● 周期的メッセージ

⊘ 挿入攻撃

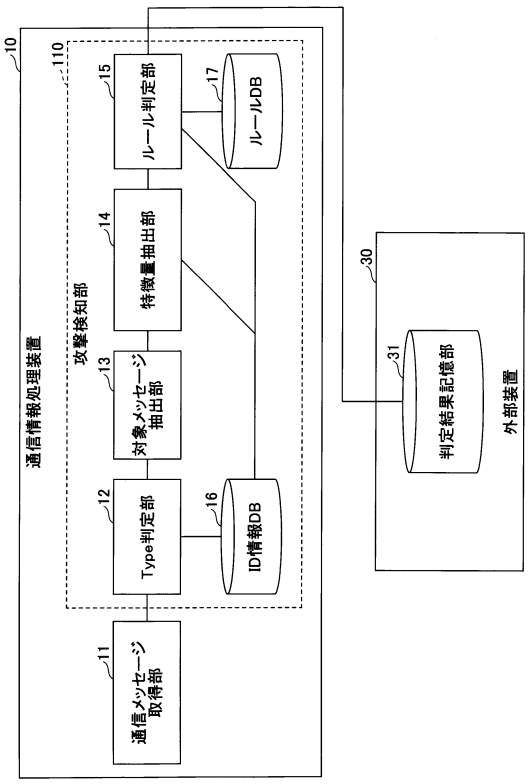
【図９】



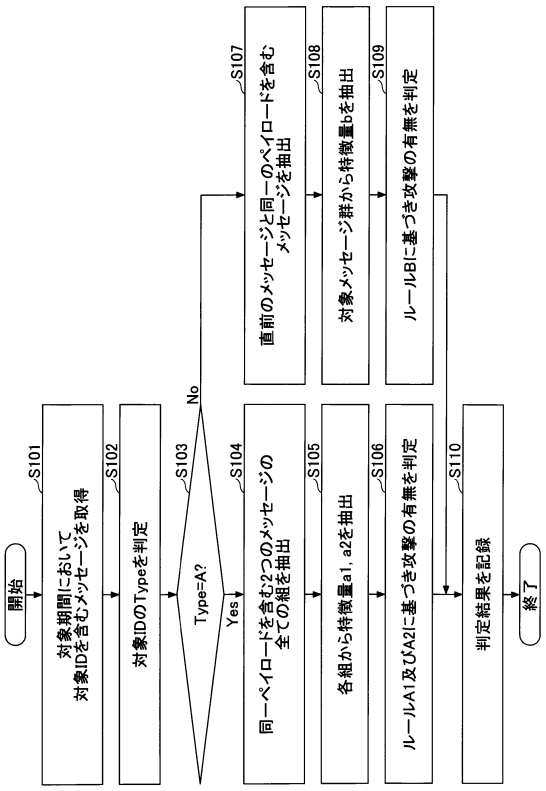
【図１０】



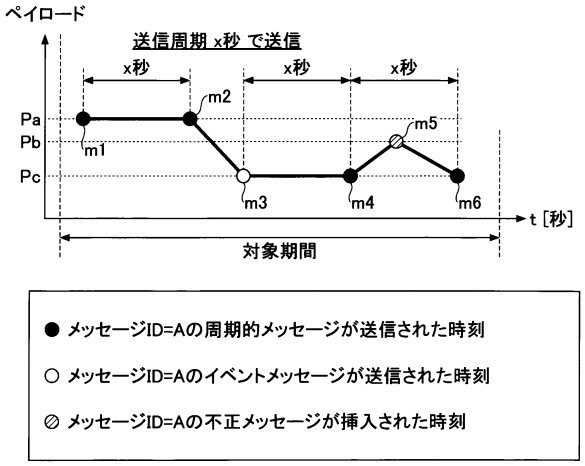
【図１１】



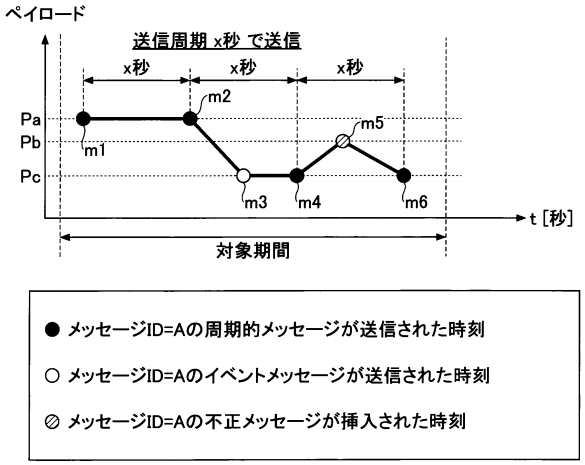
【図１２】



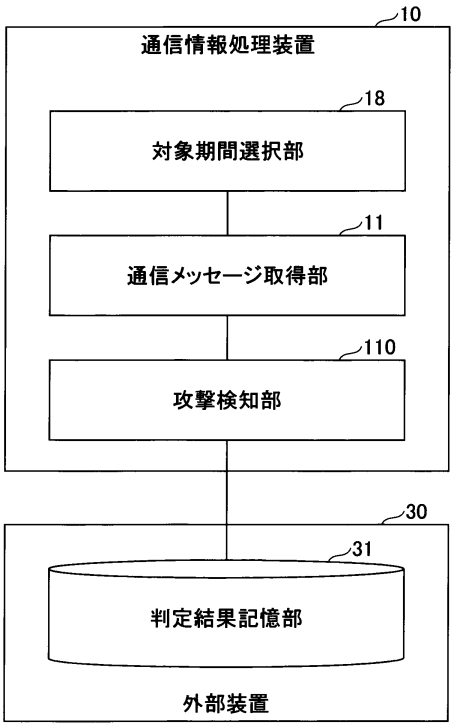
【図１３】



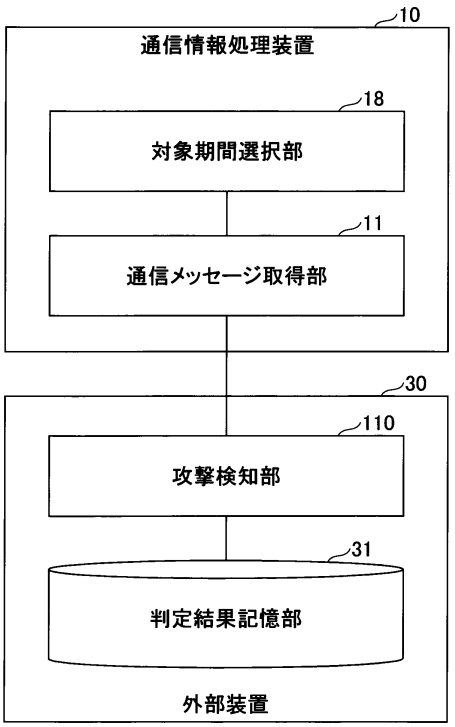
【図１４】



【図１５】



【図１６】



フロントページの続き

(72)発明者　岡野 靖
東京都千代田区大手町一丁目５番１号 日本電信電話株式会社内
(72)発明者　田中 政志
東京都千代田区大手町一丁目５番１号 日本電信電話株式会社内
審査官　松平 英
(56)参考文献　国際公開第２０１７／１８７５２０（WO，Ａ１）
藤倉 俊幸 他，ＡｕｔｏＥｎｃｏｄｅｒを利用した攻撃検知のためのＣＡＮパケット分析，２０１９年 暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１９）予稿集 ［ＵＳＢ］ ２０１９年 暗，日本，一般社団法人電子情報通信学会，2019年01月15日，2E1-5
小山 卓麻 他，機械学習により機能毎に最適な分析方式を適用する車載ネットワーク異常通信検知方法の提案，２０１８年 暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１８）予稿集，日本，一般社団法人電子情報通信学会，2018年01月23日，1E2-3
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ１２／１４
２１／００－２１／８８
Ｇ０９Ｃ １／００－５／００
Ｈ０４Ｋ １／００－３／００
Ｈ０４Ｌ ９／００－９／４０