

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7496404号
(P7496404)

(45)発行日 令和6年6月6日(2024.6.6)

(24)登録日 令和6年5月29日(2024.5.29)

(51)国際特許分類

F I

G 0 6 F 21/55 (2013.01)

G 0 6 F 21/55

請求項の数 8 (全47頁)

(21)出願番号	特願2022-199929(P2022-199929)	(73)特許権者	514136668
(22)出願日	令和4年12月15日(2022.12.15)		パナソニック インテレクチュアル プロ
(62)分割の表示	特願2021-109868(P2021-109868))の分割		パティ コーポレーション オブ アメリカ
原出願日	平成28年10月13日(2016.10.13)		Panasonic Intellec
(65)公開番号	特開2023-21333(P2023-21333A)		tual Property Corpo
(43)公開日	令和5年2月10日(2023.2.10)		ration of America
審査請求日	令和5年1月13日(2023.1.13)		アメリカ合衆国 9 0 5 0 4 カリフォル
(31)優先権主張番号	62/268,116		ニア州, トーランス, スイート 4 5 0
(32)優先日	平成27年12月16日(2015.12.16)	(74)代理人	100109210
(33)優先権主張国・地域又は機関	米国(US)		弁理士 新居 広守
		(74)代理人	100137235
			弁理士 寺谷 英作
		(74)代理人	100131417
			弁理士 道坂 伸一

最終頁に続く

(54)【発明の名称】 セキュリティ処理方法及びサーバ

(57)【特許請求の範囲】

【請求項1】

一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバで用いられるセキュリティ処理方法であって、

前記サーバは記憶媒体を含み、

前記記憶媒体には、

1つ又は複数の車両それぞれの当該車両の車載ネットワークにおいて受信された複数の第1フレームについての情報と、

前記一の車両の当該車両の車載ネットワークにおいて受信された第2フレームについての情報と、が格納され、

前記複数の第1フレームについての情報に基づいて、前記第2フレームについての情報に係る当該第2フレームの異常度を算定する算定ステップと、

前記算定ステップで算定された異常度に応じて前記一の車両のカーメーカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定する決定ステップと、

前記決定ステップで前記第1の送信用情報を送信すると決定した場合、前記第1の送信用情報を前記一の車両のカーメーカの装置又はセキュリティプロバイダに送信する送信ステップとを含み、

前記サーバは、異常の発生状況からセキュリティの重要度を示すアラートレベルを決定するためのテーブルを保持し、

前記決定ステップでは、前記算定ステップで算定された、前記第2フレームの異常度が

異常であることを示す場合において、前記テーブルを用いて前記アラートレベルを決定し、前記アラートレベルに応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定し、

前記複数の第1フレームについての情報は、前記複数の第1フレームに基づいて統計処理又は多変量解析を行った、異常状態との比較用に用いる所定モデルである、

セキュリティ処理方法。

【請求項2】

一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバで用いられるセキュリティ処理方法であって、

前記サーバは記憶媒体を含み、

前記記憶媒体には、

1つ又は複数の車両それぞれの当該車両の車載ネットワークにおいて受信された複数の第1フレームについての情報と、

前記一の車両の当該車両の車載ネットワークにおいて受信された第2フレームについての情報と、が格納され、

前記複数の第1フレームについての情報に基づいて、前記第2フレームについての情報に係る当該第2フレームの異常度を算定する算定ステップと、

前記算定ステップで算定された異常度に応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定する決定ステップと、

前記決定ステップで前記第1の送信用情報を送信すると決定した場合、前記第1の送信用情報を前記一の車両のカーメカの装置又はセキュリティプロバイダに送信する送信ステップとを含み、

前記サーバは、異常の発生状況からセキュリティの重要度を示すアラートレベルを決定するためのテーブルを保持し、

前記決定ステップでは、前記算定ステップで算定された、前記第2フレームの異常度が異常であることを示す場合において、前記テーブルを用いて前記アラートレベルを決定し、前記アラートレベルに応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定し、

前記テーブルは、前記第2フレームの異常度が、前記一の車両の位置と異常ありを示す同一車両の位置との距離に応じて前記アラートレベルが対応づけられ、

前記決定ステップでは、前記算定ステップで算定された、前記第2フレームの異常度が異常であることを示す場合において、前記テーブルを用いて前記アラートレベルを決定する、

セキュリティ処理方法。

【請求項3】

前記複数の第1フレームについての情報は、前記複数の第1フレームに基づいて統計処理又は多変量解析を行った、異常状態との比較用に用いる所定モデルである、

請求項2記載のセキュリティ処理方法。

【請求項4】

前記所定モデルは機械学習により更新される、

請求項1又は3に記載のセキュリティ処理方法。

【請求項5】

前記テーブルでは、攻撃の段階を示す攻撃フェーズと前記攻撃フェーズの各段階の攻撃が検知された数との組合せに対して前記アラートレベルが対応づけられ、

前記決定ステップでは、前記算定ステップで算定された、前記第2フレームの異常度が異常であることを示す場合において、当該第2フレームの攻撃フェーズを判定し、判定した攻撃フェーズと前記テーブルを用いて前記アラートレベルを決定する、

請求項1に記載のセキュリティ処理方法。

【請求項6】

前記テーブルは、車載ネットワークの構成が同一の車種ごとに、フレームの異常度が異

10

20

30

40

50

常であることを示す車両の累積台数または単位時間当たりの検知台数に対して前記アラートレベルが対応づけられ、

前記決定ステップでは、前記算定ステップで算定された、前記第2フレームの異常度が異常であることを示す場合において、当該第2フレームに係る異常と同一の異常が前記一の車両と車載ネットワークの構成が同一である1つ又は複数の車両で既に発生しているときには、当該発生している車両の数に応じて、前記アラートレベルを決定する、

請求項1に記載のセキュリティ処理方法。

【請求項7】

一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、

1つ又は複数の車両それぞれの当該車両の車載ネットワークにおいて受信された複数の第1フレームについての情報と、前記一の車両の当該車両の車載ネットワークにおいて受信された第2フレームについての情報を格納する格納部と、

前記複数の第1フレームについての情報と、前記第2フレームについての情報とに基づいて、前記第2フレームの異常度を算定する算定部と、

前記算定部によって算定された異常度に応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定するセキュリティ情報生成部と、

前記セキュリティ情報生成部で前記第1の送信用情報を送信すると決定した場合、前記第1の送信用情報を前記一の車両のカーメカの装置又はセキュリティプロバイダに送信する通信部とを備え、

前記サーバは、異常の発生状況からセキュリティの重要度を示すアラートレベルを決定するためのテーブルを保持し、

前記セキュリティ情報生成部は、前記算定部で算定された、前記第2フレームの異常度が異常であることを示す場合において、前記テーブルを用いて前記アラートレベルを決定し、前記アラートレベルに応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定し、

前記複数の第1フレームについての情報は、前記複数の第1フレームに基づいて統計処理又は多変量解析を行った、異常状態との比較用に用いる所定モデルである、

サーバ。

【請求項8】

一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、

1つ又は複数の車両それぞれの当該車両の車載ネットワークにおいて受信された複数の第1フレームについての情報と、前記一の車両の当該車両の車載ネットワークにおいて受信された第2フレームについての情報を格納する格納部と、

前記複数の第1フレームについての情報と、前記第2フレームについての情報とに基づいて、前記第2フレームの異常度を算定する算定部と、

前記算定部によって算定された異常度に応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定するセキュリティ情報生成部と、

前記セキュリティ情報生成部で前記第1の送信用情報を送信すると決定した場合、前記第1の送信用情報を前記一の車両のカーメカの装置又はセキュリティプロバイダに送信する通信部とを備え、

前記サーバは、異常の発生状況からセキュリティの重要度を示すアラートレベルを決定するためのテーブルを保持し、

前記セキュリティ情報生成部は、前記算定部で算定された、前記第2フレームの異常度が異常であることを示す場合において、前記テーブルを用いて前記アラートレベルを決定し、前記アラートレベルに応じて前記一の車両のカーメカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定し、

10

20

30

40

50

前記テーブルは、前記第２フレームの異常度が、前記一の車両の位置と異常ありを示す同一車両の位置との距離に応じて前記アラートレベルが対応づけられ、

前記セキュリティ情報生成部は、前記算定部で算定された、前記第２フレームの異常度が異常であることを示す場合において、前記テーブルを用いて前記アラートレベルを決定する、

サーバ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、車両に搭載される電子制御ユニットが通信を行う車載ネットワークにおいて送信され得る攻撃フレームの検知、対処等のためのセキュリティ技術に関する。

10

【背景技術】

【０００２】

近年、自動車の中のシステムには、電子制御ユニット（ＥＣＵ：Electronic Control Unit）と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐネットワークは車載ネットワークと呼ばれる。車載ネットワークには、多数の規格が存在する。その中でも最も主流な車載ネットワークの一つに、ＩＳＯ１１８９８－１で規定されているＣＡＮ（Controller Area Network）という規格が存在する。

【０００３】

ＣＡＮでは、通信路は２本のワイヤで構成されたバス（ＣＡＮバス）であり、バスに接続されているＥＣＵはノードと呼ばれる。ＣＡＮバスに接続されている各ノードは、フレーム（メッセージ）を送受信する。またＣＡＮでは、送信先や送信元を指す識別子は存在せず、送信ノードはフレーム毎に、メッセージＩＤと呼ばれるＩＤを付けて送信し、各受信ノードは予め定められたメッセージＩＤのみを受信する。自動車の中のシステムにおいては、多数のＥＣＵそれぞれは、様々なフレームの授受を行う。

20

【０００４】

ＣＡＮバスに不正なノードを接続すること、或いは、携帯情報端末、車外の通信装置等と通信する機能を有するＥＣＵ等を攻撃して不正なノードに変化させること等により、攻撃者が、攻撃フレームをＣＡＮバスに送信して、自動車を不正にコントロールする可能性がある。攻撃フレームは、不正な攻撃者によってＣＡＮバスに送信されたフレームであり、車載ネットワークの正常状態において本来は送信されないフレームである。

30

【０００５】

このような攻撃フレームを検知して防御する技術として、車載ネットワークにおいて周期的に送信されるべきメッセージＩＤのフレームについて、想定される周期を予め登録しておき、想定周期に基づいて不正か否かの判別を行う技術が知られている（特許文献１参照）。

【先行技術文献】

【特許文献】

【０００６】

【文献】特開２０１４－１４６８６８号公報

40

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかしながら、特許文献１の技術では、検知できる攻撃フレームが、登録された想定周期を用いて判別できる攻撃フレームに限定されるので、多様な攻撃フレームの検知、防御等に必ずしも有効とは限らない。

【０００８】

そこで、本発明は、車載ネットワークで送信され得る多様な攻撃フレームに適切に対処するために有用なセキュリティ処理方法を提供する。また、本発明は、多様な攻撃フレームに適切に対処するために有用なサーバ（サーバ装置）を提供する。

50

【課題を解決するための手段】

【0009】

上記課題を解決するために本発明の一態様に係るセキュリティ処理方法は、一の車両の車載ネットワークで送信される異常なフレームに対処するため、前記一の車両及び1つ又は複数の車両と通信可能なサーバで用いられるセキュリティ処理方法であって、前記1つ又は複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信する第1受信ステップと、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する第2受信ステップと、前記第1受信ステップで受信された、複数のフレームについての情報に基づいて、前記第2受信ステップで受信された、フレームについての情報に係る当該フレームの異常度を算定する算定ステップと、前記算定ステップで算定された異常度に応じて前記一の車両のカーメーカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定する決定ステップと、前記決定ステップで前記第1の送信用情報を送信すると決定した場合、前記第1の送信用情報を前記一の車両のカーメーカの装置又はセキュリティプロバイダに送信する送信ステップとを含むセキュリティ処理方法である。

10

【0010】

また、上記課題を解決するために本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、1つ又は複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する取得部と、前記取得部により受信された、複数のフレームについての情報と、当該複数のフレームについての情報の前記受信より後に、前記取得部により受信された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度を算定する算定部と、前記算定部によって算定された異常度に応じて前記一の車両のカーメーカの装置又はセキュリティプロバイダに第1の送信用情報の送信を行うか否かを決定するセキュリティ情報生成部と、前記セキュリティ情報生成部で前記第1の送信用情報を送信すると決定した場合、前記第1の送信用情報を前記一の車両のカーメーカの装置又はセキュリティプロバイダに送信する通信部とを備える。

20

【0011】

上記課題を解決するために本発明の一態様に係るセキュリティ処理方法は、一の車両の車載ネットワークで送信される異常なフレームに対処するためのセキュリティ処理方法であって、1つ又は複数の車両の車載ネットワークにおいて受信された複数のフレームについての情報を取得し、前記取得された複数のフレームについての情報に基づいて、当該複数のフレームについての前記受信より後に、前記一の車両の車載ネットワークにおいて受信されたフレームの異常度を算定するセキュリティ処理方法である。

30

【0012】

また、上記課題を解決するために本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、前記一の車両を含む1つ又は複数の車両の車載ネットワークにおいて受信されたフレームについての情報を受信することで取得する取得部と、前記取得部により取得された複数のフレームについての情報と、当該複数のフレームについての前記取得より後に、前記取得部により取得された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度を算定する算定部とを備えるサーバである。

40

【0013】

また、上記課題を解決するために本発明の一態様に係るセキュリティ処理方法は、一の車両の車載ネットワークで送信される異常なフレームに対処するためのセキュリティ処理方法であって、前記一の車両の車載ネットワークにおいて受信されたフレームの異常度を算定し、算定した前記異常度に応じて、前記一の車両と所定関係を有する車両に対して送

50

信用情報を送信するか否かを決定し、前記決定に従って当該送信用情報の送信の制御を行うセキュリティ処理方法である。

【発明の効果】

【0014】

本発明によれば、ある車載ネットワークで受信されたフレームの異常度（つまり異常の度合い）が算定されるので、結果的に、車載ネットワークの正常状態で本来送信されるものではない様々な攻撃フレームへの適切な対処が可能となり得る。

【図面の簡単な説明】

【0015】

【図1A】実施の形態に係る車載ネットワーク管理システムが提供するサービスの態様の一例を示す概念図である。

10

【図1B】実施の形態に係るデータセンタ運営会社の一例を示す概念図である。

【図2】実施の形態1に係る車載ネットワーク管理システムの全体構成を示す図である。

【図3】実施の形態1に係る車載ネットワークシステムの構成の一例を示す図である。

【図4】実施の形態1に係る異常検知サーバの構成図である。

【図5】実施の形態1に係る異常検知サーバの車両ログ格納データベース（DB：database）の内容例を示す図である。

【図6】実施の形態1に係る異常検知サーバの車両情報DBが保持する車両情報の一例を示す図である。

【図7】実施の形態1に係る異常検知サーバのセキュリティ情報DBが保持する攻撃フェーズ情報の一例を示す図である。

20

【図8】実施の形態1に係る異常検知サーバのセキュリティ情報DBが保持するアラートレベル情報の一例を示す図である。

【図9】実施の形態1に係る車載ネットワークにおけるゲートウェイの構成図である。

【図10】実施の形態1に係る異常検知サーバと車両との連携動作の一例を示すシーケンス図である。

【図11】実施の形態1に係る異常検知サーバにおける異常検知処理の一例を示すフローチャートである。

【図12A】実施の形態1におけるアラートレベル決定用情報の例1を示す図である。

【図12B】実施の形態1におけるアラートレベル決定用情報の例2を示す図である。

30

【図12C】実施の形態1におけるアラートレベル決定用情報の例3を示す図である。

【図12D】実施の形態1におけるアラートレベル決定用情報の例4を示す図である。

【図12E】実施の形態1におけるアラートレベル決定用情報の例5を示す図である。

【図13】実施の形態2に係る異常検知サーバによる不正検知用情報（ルール等）の配信の動作例を示すシーケンス図である。

【図14】実施の形態3に係る異常検知サーバが用いるMAC／暗号化保護対象メッセージIDリストの一例を示す図である。

【図15】実施の形態3に係る異常検知サーバによる鍵更新要求の動作例を示すシーケンス図である。

【図16】車載ネットワーク管理システムが提供するサービス（類型1）を示す概念図である。

40

【図17】車載ネットワーク管理システムが提供するサービス（類型2）を示す概念図である。

【図18】車載ネットワーク管理システムが提供するサービス（類型3）を示す概念図である。

【図19】車載ネットワーク管理システムが提供するサービス（類型4）を示す概念図である。

【発明を実施するための形態】

【0016】

本発明の一態様に係るセキュリティ処理方法は、一の車両の車載ネットワークで送信さ

50

れる異常なフレームに対処するためのセキュリティ処理方法であって、1つ又は複数の車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記受信された複数のフレームについての情報に基づいて、当該複数のフレームについての前記受信より後に、前記一の車両の車載ネットワークにおいて受信されたフレームの異常度を算定するセキュリティ処理方法である。セキュリティ処理方法において、車載ネットワークで既に受信された複数のフレームについての情報を取得（収集）することで、例えば統計処理、多変量解析、機械学習等の適用により、適切な異常度の算定が可能となり得る。これにより、算定された異常度は、ブラックリスト等の既存ルールに基づく不正検知手法では検知できない異常（例えば攻撃予兆、未知の攻撃等に係る攻撃フレーム）を表し得る。この異常度に基づいて、攻撃フレームに適切に対処することが可能となり得る。

10

【0017】

また、例えば、前記セキュリティ処理方法は、前記複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を、前記複数の車両及び前記一の車両と通信可能なサーバが受信する第1受信ステップと、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を、前記サーバが受信する第2受信ステップと、前記第1受信ステップで受信された、複数のフレームについての情報に基づいて、前記第2受信ステップで受信された、フレームについての情報に係る当該フレームの異常度の前記算定を行う算定ステップと、前記算定ステップで算定された異常度に応じて前記一の車両に送信すべき送信用情報の内容を決定する決定ステップと、前記決定ステップで決定された内容の送信用情報を前記一の車両に前記サーバが送信する送信ステップとを含むこととしても良い。これにより、一の車両の車載ネットワークで受信されたフレームについて算定された異常度に応じてサーバ（例えばクラウドサーバ等といった車両外部のコンピュータ）により送信用情報の送信が行われるので、フレームが異常である場合において、送信用情報を受信する車両では、送信用情報を活用した対処（アラート通知、車両の制御等）が可能となる。

20

【0018】

また、例えば、前記第2受信ステップで受信する、フレームについての情報は、当該フレームの識別情報を含み、前記決定ステップでは、前記算定ステップで算定された、フレームの異常度が異常であることを示す場合において当該フレームの識別情報に応じて、送信用情報の内容の前記決定を行うこととしても良い。これにより、例えば異常なフレームの識別情報で区別され得る攻撃フェーズ（攻撃予兆、攻撃等の各フェーズ）に対する適切なセキュリティ対策が可能となり得る。

30

【0019】

また、例えば、前記決定ステップでは、前記算定ステップで異常であることを示す異常度が算定されたフレームの識別情報が所定識別情報である場合に、前記一の車両の走行の停止又は走行速度の減速を指示する制御情報を前記送信用情報が含むように前記決定を行うこととしても良い。これにより、所定識別情報を、車両の走行上重要なフレームについて予め定められた識別情報（メッセージID）として定めておくことで、適切に車両をより安全状態な状態へと移行させるセキュリティ対策が実現可能となる。

【0020】

40

また、例えば、前記送信ステップでは、前記算定ステップで算定された異常度に応じて前記一の車両に送信すべき送信用情報の送信時期を決定し、決定した送信時期に当該送信用情報を前記一の車両に送信することとしても良い。これにより、セキュリティのための情報（例えばアラート通知等）は、例えば異常度が高いほど迅速に送信される等のように、適切な時期に送信されるようになり得る。

【0021】

また、例えば、前記決定ステップでは、前記算定ステップで算定された、フレームの異常度が異常であることを示す場合において、当該フレームに係る異常と同一の異常が前記一の車両と車載ネットワークの構成が同一である1つ又は複数の車両で既に発生しているときには、当該発生している車両の数又は前記一の車両と当該発生している車両との距離

50

に基づいて、前記一の車両に送信すべき送信用情報の内容の前記決定を行うこととしても良い。同一の異常は、例えば、同種のECUが送信するフレームの異常、同一の識別情報を有するフレームの異常等である。一の車両以外の車両についても例えば一の車両と同様に異常度を算定することで、異常か否かは区別できる。同一の異常が発生している車両の数は、総数であっても単位時間当たりの数であっても良い。これにより、攻撃者による攻撃の規模等が推定されその規模等に応じて、必要な情報の送信により適切なセキュリティ対策を行うことが可能となり得る。

【0022】

また、例えば、前記決定ステップでは、前記算定ステップで算定された、フレームの異常度が異常であることを示す場合において当該異常と同一の異常を車載ネットワークにおいて検知するためのルール又はアルゴリズムを示す不正検知用情報を前記送信用情報が含むように前記決定を行うこととしても良い。これにより、サーバから、車両のローカル環境で不正検知を行うための不正検知用情報を配信可能となり、このため車両のセキュリティを高めることが可能となる。

【0023】

また、例えば、前記第2受信ステップで受信する、フレームについての情報は、当該フレームの識別情報を含み、前記決定ステップでは、前記算定ステップで算定された、フレームの異常度が異常であることを示す場合において、当該フレームの識別情報が、暗号処理技術を適用してデータを伝送するためのフレーム用の予め規定された識別情報であるときには、当該暗号処理技術の適用に際して利用される鍵の更新を指示する制御情報を前記送信用情報が含むように前記決定を行うこととしても良い。これにより、例えば、暗号処理技術で保護されたフレームに係る攻撃の検知に関連して、鍵の更新というセキュリティ対策を行うので、鍵の漏洩等による被害を低減させることが可能となり得る。

【0024】

また、例えば、前記受信されるフレームについての前記情報は、少なくとも当該フレームの内容の一部を含み、前記複数のフレームについての情報の前記受信は、前記複数のフレームそれぞれについての情報の逐次受信であり、前記セキュリティ処理方法では、前記逐次受信されたフレームについての情報に基づいて所定モデルを逐次更新し、前記一の車両の車載ネットワークにおいて受信されたフレームの異常度の前記算定は、当該受信されたフレームについての情報と、前記所定モデルとを用いた演算処理により行われることとしても良い。これにより、例えば、各車両の車載ネットワークで受信されたフレームについての情報を反映した所定モデルと、異常度の算定対象のフレームとの比較、算術演算、論理演算、条件判断等といった各種処理の1つ以上の組み合わせである演算処理により、異常度が算定され得る。所定モデルは、例えば、異常度を複数段階に区別するために有用である。例えば、所定モデルは、統計処理、機械学習等により更新され得る。所定モデルが逐次更新されるので、各車両の最近の状況に対応して、適切に異常度の算定が行える可能性がある。

【0025】

また、例えば、前記セキュリティ処理方法は、前記逐次受信されたフレームについての情報に基づいて機械学習により前記所定モデルを逐次更新することとしても良い。これにより、機械学習により、適切に異常度の算定が行われ得る。そして、算定された異常度に基づいて、未知な攻撃に対応可能となり得る。

【0026】

また、例えば、前記送信ステップでは、前記算定ステップで算定された異常度に応じて前記一の車両と所定関係を有する車両に対して所定の送信用情報の送信を行うか否かを決定し、当該決定に従って当該所定の送信用情報の送信の制御を行うこととしても良い。これにより、攻撃者に攻撃された車両（攻撃フレームが車載ネットワークにおいて流された車両）のみならず、その車両と所定関係を有する車両（例えば同一車種の車両、同種ECUを有する車両等）に対してもセキュリティのための情報が送信されるので、所定関係を有する車両に対する攻撃を未然に防止するためのセキュリティ対策等が可能となり得る。

【0027】

また、例えば、前記第2受信ステップで受信する、フレームについての情報は、当該フレームの識別情報を含み、前記送信ステップでは、前記算定ステップで算定された、フレームの異常度が異常であることを示す場合において当該フレームの識別情報に応じて、前記一の車両と、車載ネットワークの構成が同一である車両に対して前記所定の送信用情報の送信を行うか否かを決定し、当該決定に従って当該所定の送信用情報の送信の制御を行うこととしても良い。これにより、例えば、異常なフレームの識別情報で区別され得る攻撃フェーズに応じて、異常なフレームが検知された車両と車載ネットワークの構成が同一の車両（例えば同一車種の車両）に対して、セキュリティの確保のための情報等が送信され得る。このため、例えば同一車種の複数の車両に対する攻撃の被害を抑制するためのセキュリティ対策等が可能となり得る。

10

【0028】

また、例えば、前記第2受信ステップで受信する、フレームについての情報は、当該フレームの識別情報を含み、前記送信ステップでは、前記算定ステップで算定された、フレームの異常度が異常であることを示す場合において当該フレームの識別情報に応じて、前記一の車両の車載ネットワークにおいて当該識別情報で識別されるフレームを送信する電子制御ユニットと同種の電子制御ユニットを搭載する車両に対して前記所定の送信用情報の送信を行うか否かを決定し、当該決定に従って当該所定の送信用情報の送信の制御を行うこととしても良い。これにより、例えば、異常なフレームの識別情報で区別され得る攻撃フェーズに応じて、異常なフレームが検知された車両でそのフレームを送信するECUと同種のECUを搭載する車両（例えば異常が検知された車両と同一車種の車両、同一型式のECUを搭載する別車種の車両等）に対して、セキュリティの確保のための情報等が送信され得る。このため、攻撃者が攻撃フレームを送信するために制御下に置いたECUと同種のECUを搭載する各車両に対する攻撃の被害を抑制するためのセキュリティ対策等が可能となり得る。

20

【0029】

また、本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、1つ又は複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する取得部と、前記取得部により受信された複数のフレームについての情報と、当該複数のフレームについての前記受信より後に、前記取得部により受信された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度の算定を行う算定部と、前記算定部により算定された異常度に応じて前記一の車両に送信すべき送信用情報の内容を決定するセキュリティ情報生成部と、前記セキュリティ情報生成部により決定された内容の送信用情報を前記一の車両に送信する通信部とを備え、前記取得部が受信する、フレームについての情報は、当該フレームの識別情報を含み、前記セキュリティ情報生成部は、前記算定部により算定された、フレームの異常度が異常であることを示す場合において当該フレームの識別情報に応じて、送信用情報の内容の前記決定を行い、異常であることを示す異常度が算定された前記フレームの識別情報が所定識別情報である場合に、前記一の車両の走行の停止又は走行速度の減速を指示する制御情報を前記送信用情報が含むように前記決定を行うサーバである。このサーバ（例えばクラウドサーバ等といった車両外部のコンピュータ）により算定された異常度に基づいて、多様な攻撃フレームへの適切な対処が可能となり得る。また、このサーバからは一の車両の車載ネットワークで受信されたフレームについて算定された異常度に応じて送信用情報の送信が行われるので、フレームが異常である場合において、送信用情報を受信する車両では、送信用情報を活用した対処（アラート通知、車両の制御等）が可能となる。また、例えば異常なフレームの識別情報で区別され得る攻撃フェーズ（攻撃予兆、攻撃等の各フェーズ）に対する適切なセキュリティ対策が可能となり得る。またこのサーバは、所定識別情報を、車両の走行上重

30

40

50

要なフレームについて予め定められた識別情報（メッセージID）を用いることで、適切に車両をより安全状態な状態へと移行させるセキュリティ対策を実現可能とする。

【0030】

また、本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、1つ又は複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する複数のフレームについての情報と、当該複数のフレームについての前記受信より後に、前記取得部により受信された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度の算定を行う算定部と、前記算定部により算定された異常度に応じて前記一の車両に送信すべき送信用情報の内容を決定するセキュリティ情報生成部と、前記セキュリティ情報生成部により決定された内容の送信用情報を前記一の車両に送信する通信部とを備え、前記通信部は、前記算定部により算定された異常度に応じて前記一の車両に送信すべき送信用情報の送信時期を決定し、決定した送信時期に当該送信用情報を前記一の車両に送信するサーバである。このサーバ（例えばクラウドサーバ等といった車両外部のコンピュータ）により算定された異常度に基づいて、多様な攻撃フレームへの適切な対処が可能となり得る。また、このサーバからは一の車両の車載ネットワークで受信されたフレームについて算定された異常度に応じて送信用情報の送信が行われるので、フレームが異常である場合において、送信用情報を受信する車両では、送信用情報を活用した対処（アラート通知、車両の制御等）が可能となる。また、セキュリティのための情報（例えばアラート通知等）は、例えば異常度が高いほど迅速に送信される等のように、適切な時期に送信されるようになり得る。

【0031】

また、本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、1つ又は複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する取得部と、前記取得部により受信された複数のフレームについての情報と、当該複数のフレームについての前記受信より後に、前記取得部により受信された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度の算定を行う算定部と、前記算定部により算定された異常度に応じて前記一の車両に送信すべき送信用情報の内容を決定するセキュリティ情報生成部と、前記セキュリティ情報生成部により決定された内容の送信用情報を前記一の車両に送信する通信部とを備え、前記セキュリティ情報生成部は、前記算定部により算定された、フレームの異常度が異常であることを示す場合において、当該フレームに係る異常と同一の異常が前記一の車両と車載ネットワークの構成が同一である1つ又は複数の車両で既に発生しているときには、当該発生している車両の数又は前記一の車両と当該発生している車両との距離に基づいて、前記一の車両に送信すべき送信用情報の内容の前記決定を行うサーバである。このサーバ（例えばクラウドサーバ等といった車両外部のコンピュータ）により算定された異常度に基づいて、多様な攻撃フレームへの適切な対処が可能となり得る。また、このサーバからは一の車両の車載ネットワークで受信されたフレームについて算定された異常度に応じて送信用情報の送信が行われるので、フレームが異常である場合において、送信用情報を受信する車両では、送信用情報を活用した対処（アラート通知、車両の制御等）が可能となる。また、攻撃者による攻撃の規模等が推定され、その規模等に応じて、必要な情報の送信により適切なセキュリティ対策を行うことが可能となり得る。

【0032】

また、本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、1つ又は複数の車両それぞれから、当該車

両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する取得部と、前記取得部により受信された複数のフレームについての情報と、当該複数のフレームについての前記受信より後に、前記取得部により受信された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度の算定を行う算定部と、前記算定部により算定された異常度に応じて前記一の車両に送信すべき送信用情報の内容を決定するセキュリティ情報生成部と、前記セキュリティ情報生成部により決定された内容の送信用情報を前記一の車両に送信する通信部とを備え、前記セキュリティ情報生成部は、前記算定部により算定された、フレームの異常度が異常であることを示す場合において当該異常と同一の異常を車載ネットワークにおいて検知するためのルール又はアルゴリズムを示す不正検知用情報を前記送信用情報が含むように前記決定を行うサーバである。このサーバ（例えばクラウドサーバ等といった車両外部のコンピュータ）により算定された異常度に基づいて、多様な攻撃フレームへの適切な対処が可能となり得る。また、このサーバからは一の車両の車載ネットワークで受信されたフレームについて算定された異常度に応じて送信用情報の送信が行われるので、フレームが異常である場合において、送信用情報を受信する車両では、送信用情報を活用した対処（アラート通知、車両の制御等）が可能となる。また、サーバから、車両のローカル環境で不正検知を行うための不正検知用情報を配信可能となり、このため車両のセキュリティを高めることが可能となる。

【0033】

また、本発明の一態様に係るサーバは、一の車両の車載ネットワークで送信される異常なフレームに対処するためのサーバであって、1つ又は複数の車両それぞれから、当該車両の車載ネットワークにおいて受信された複数のフレームについての情報を受信し、前記一の車両から、当該車両の車載ネットワークにおいて受信されたフレームについての情報を受信する取得部と、前記取得部により受信された複数のフレームについての情報と、当該複数のフレームについての前記受信より後に、前記取得部によりされた、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、前記一の車両の車載ネットワークにおいて受信された当該フレームの異常度の算定を行う算定部と、前記算定部により算定された異常度に応じて前記一の車両に送信すべき送信用情報の内容を決定するセキュリティ情報生成部と、前記セキュリティ情報生成部により決定された内容の送信用情報を前記一の車両に送信する通信部とを備え、前記取得部により受信された、前記一の車両の車載ネットワークにおいて受信されたフレームについての情報は、当該フレームの識別情報を含み、前記セキュリティ情報生成部は、前記算定部により算定された、フレームの異常度が異常であることを示す場合において、当該フレームの識別情報が、暗号処理技術を適用してデータを伝送するためのフレーム用の予め規定された識別情報であるときには、当該暗号処理技術の適用に際して利用される鍵の更新を指示する制御情報を前記送信用情報が含むように前記決定を行うサーバである。このサーバ（例えばクラウドサーバ等といった車両外部のコンピュータ）により算定された異常度に基づいて、多様な攻撃フレームへの適切な対処が可能となり得る。また、このサーバからは一の車両の車載ネットワークで受信されたフレームについて算定された異常度に応じて送信用情報の送信が行われるので、フレームが異常である場合において、送信用情報を受信する車両では、送信用情報を活用した対処（アラート通知、車両の制御等）が可能となる。また例えば、暗号処理技術で保護されたフレームに係る攻撃の検知に関連して、鍵の更新というセキュリティ対策を行うので、鍵の漏洩等による被害を低減させることが可能となり得る。

【0034】

また、本発明の一態様に係るセキュリティ処理方法は、一の車両の車載ネットワークで送信される異常なフレームに対処するためのセキュリティ処理方法であって、前記一の車両の車載ネットワークにおいて受信されたフレームの異常度を算定し、算定した前記異常度に応じて、前記一の車両と所定関係を有する車両に対して送信用情報を送信するか否かを決定し、前記決定に従って当該送信用情報の送信の制御を行うセキュリティ処理方法で

ある。これにより、一の車両でのフレームの異常度に応じて、セキュリティ対策としての情報を他の車両に送信するか否かを切り替えることができるため、適切なセキュリティ対策が可能となり得る。

【0035】

なお、これらの全般的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なＣＤ－ＲＯＭ等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されても良い。

【0036】

以下、実施の形態に係るサーバを含みセキュリティ処理方法を用いる車載ネットワーク管理システムについて、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本発明の一具体例を示すものである。従って、以下の実施の形態で示される数値、構成要素、構成要素の配置及び接続形態、並びに、ステップ（工程）及びステップの順序等は、一例であって本発明を限定するものではない。以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は、模式図であり、必ずしも厳密に図示されたものではない。

【0037】

（提供するサービスの全体像）

まず、本実施の形態における車載ネットワーク管理システムが提供するサービスの態様について説明する。

【0038】

図１Ａは、本実施の形態における車載ネットワーク管理システムが提供するサービスの態様の一例を示す図である。車載ネットワーク管理システムは、グループ１０００、データセンタ運営会社１１００及びサービスプロバイダ１２００を備える。

【0039】

グループ１０００は、例えば企業、団体又は家庭等であり、その規模を問わない。グループ１０００は、複数の車両１０１０（第一の車両、第二の車両等）を含み、各車両はゲートウェイ１０２０を備える。複数の車両１０１０は、インターネットと接続可能な装置（ゲートウェイ１０２０、ヘッドユニット、テレマティクスモジュール等）、及び、それ自身ではインターネットと接続不可能な装置（例えば、エンジンＥＣＵ等）を含む。複数の車両１０１０の各々は、車内のネットワーク（車載ネットワーク）等により、ゲートウェイ１０２０、或いは、ヘッドユニット、テレマティクスモジュール等を介してインターネットと接続可能となる各種ＥＣＵ等の装置を含み得る。なお、各車両は、必ずしもゲートウェイ１０２０を含まなくても良い。ユーザ１００１は、複数の車両１０１０における車両を使用し得る。

【0040】

データセンタ運営会社１１００は、クラウドサーバ１１１０を備える。クラウドサーバ１１１０は、インターネットを介して様々な機器と連携するコンピュータであり、例えば仮想化サーバである。クラウドサーバ１１１０は、例えば、通常のデータベース管理ツール等で扱うことが困難な巨大なデータ（ビッグデータ）等を管理する。データセンタ運営会社１１００は、データの管理、クラウドサーバ１１１０の管理、それらを行うデータセンタの運営等を行っている。なお、データセンタ運営会社１１００は、データの管理又はクラウドサーバ１１１０の管理のみを行っている管理会社に限られず、他の事業を併せて行っている会社であっても良く、例えば、複数の車両１０１０の全部又は一部を、開発又は製造している自動車製造業者（カーメーカ）であっても良い。また、データセンタ運営会社１１００は一つの会社に限られず、例えば、図１Ｂに示すように、カーメーカ及び管理会社が共同又は分担してデータの管理又はクラウドサーバ１１１０の管理を行っている場合は、カーメーカ及び管理会社の両者がデータセンタ運営会社１１００に該当し得る。また、カーメーカ及び管理会社的一方のみがデータセンタ運営会社１１００として機能していても良い。なお、上述したクラウドサーバ１１１０は、データの管理等に必要な機能

を実現するための特定のプログラムにより実現され得る。

【0041】

サービスプロバイダ1200は、サーバ1210を備える。サーバ1210は、例えば1台又は複数台のコンピュータで実現され、その規模は問わず、記憶媒体として大容量のハードディスク等のストレージを備えても良いし、例えば、PC内のメモリ等しか備えていなくても良い。なお、サーバ1210自体が記憶媒体を備えずに外部の記憶媒体を利用するものであっても良い。また、サービスプロバイダ1200は、サーバ1210を備えない場合もあり得る。

【0042】

次に、上述の態様の車載ネットワーク管理システムにおける情報の流れを説明する。

10

【0043】

まず、グループ1000の複数の車両1010（第一の車両、第二の車両等）はそれぞれ、各車両において逐次取得された情報であるログ情報をデータセンタ運営会社1100のクラウドサーバ1110に送信する。クラウドサーバ1110は、各車両のログ情報を受信して集積する。ここで、各車両がクラウドサーバ1110に送信するログ情報は、例えば、車載ネットワークを構成するCANバスに流れたフレーム（メッセージ）の内容、受信タイミング（間隔、頻度等）に関する情報を含む。ログ情報は、CANバスに流れたフレームの内容として、或いは別個の情報として、アクセル、ブレーキ等の変位置量、シフト（変速ギア）の状態、エンジンの回転数、ステアリングの操舵角、車速等の車両状態情報や車両の位置の情報等を含み得る。各車両が送信するログ情報は、更に、車両の識別情報（車両ID）を含み、また、路車間通信、車車間通信等により、その車両と無線接続される機器から取得された種々の情報を含んでも良い。なお、ログ情報は、インターネットを介して複数の車両1010の各々自体から直接、或いは路側機等の他装置を介して、クラウドサーバ1110へと送信され得る。

20

【0044】

次に、データセンタ運営会社1100のクラウドサーバ1110は、集積したログ情報に基づく情報をサービスプロバイダ1200に提供する。例えば、クラウドサーバ1110は、集積したログ情報に基づく情報を、リアルタイム又は任意のタイミングで、サービスプロバイダ1200のサーバ1210に送信する。このログ情報に基づく情報は、ログ情報の少なくとも一部と同一の情報を含むものであっても、その同一の情報を含まずログ情報に対して演算等の処理を施した結果としての情報であっても良い。また、このログ情報に基づく情報の送信の単位は、いかなる単位であっても良い。サーバ1210は、クラウドサーバ1110からの情報を取得する。

30

【0045】

そして、サービスプロバイダ1200（例えばサーバ1210）は、クラウドサーバ1110からの情報に対応して、ユーザ1001或いは複数の車両1010へ提供するための提供用情報を特定して、その提供用情報を、ユーザ1001或いは複数の車両1010へ提供可能にすべくクラウドサーバ1110に送信する。提供用情報は、例えばユーザ1001への警告のための情報、車両の走行制御等のための情報等であり得る。クラウドサーバ1110は、サーバ1210からの提供用情報を複数の車両1010のうち1台以上の車両に転送する又はその提供用情報に対して演算等の処理（ユーザに提供するサービスに適合するように情報を整理する処理等）を施した結果としての情報をその車両に送信する。この情報を受信した車両は、その情報に基づいて動作し、例えば、ディスプレイ等のユーザインタフェースを通じてユーザ1001に情報を提供する。情報が提供されるユーザは、複数の車両1010のいずれかを使用するユーザ1001でも良いし、外部のユーザ1002でも良い。ユーザ1002は、例えばカーメカ、ECUベンダ（ECUサプライヤ）等であっても良い。なお、サービスプロバイダ1200に代えて、データセンタ運営会社1100のクラウドサーバ1110が、ログ情報に基づく情報をユーザ1001に提供するサービスに適合するように整理しても良い。また、クラウドサーバ1110が、そのように整理した情報をサービスプロバイダ1200に送信することとしても良い。

40

50

また、サーバ1210が、クラウドサーバ1110を介さずに複数の車両1010のうち1台以上の車両と通信を行うことで、ログ情報の取得、及び、提供用情報の提供を行うこととしても良い。また、サービスプロバイダ1200を省略して、クラウドサーバ1110は、集積したログ情報に基づいて、提供用情報を特定してその提供用情報を、ユーザ1001或いは複数の車両1010へ提供しても良い。

【0046】

また、車載ネットワーク管理システムは、上述した例と異なる態様であっても良い。例えば、車載ネットワーク管理システムにおいて、データセンタ運営会社1100及びサービスプロバイダ1200を省いても良い。例えば、複数の車両1010のいずれかの車両は、自車両及び1台以上の他車両からログ情報を集積するクラウドサーバ1110と同様の機能を備え、集積したログ情報に基づいて提供用情報を特定して、その提供用情報を、自車両で活用し或いは他車両に提供することとしても良い。

【0047】

(実施の形態1)

以下、複数の電子制御ユニット(ECU)がCANバスを介して通信する車載ネットワーク(車載ネットワークシステム)を搭載した複数台の車両と、サーバ(異常検知サーバ)を含む車載ネットワーク管理システム、並びに、その車載ネットワーク管理システムで用いられるセキュリティ技術としてのセキュリティ処理方法について説明する。セキュリティ処理方法は、ある車両の車載ネットワークにおいてその車両に搭載された各ECU間での通信に用いられるCANバスで送信されたフレームが攻撃フレームの疑いがある場合等に適切に対処可能にするために、そのフレームについて異常度の算定等を行う方法である。異常度の算定は、異常なフレームに対して柔軟にセキュリティ対策(アラート通知、防御等)を行うために有用である。攻撃フレームは、不正な攻撃者によってCANバスに送信されたフレームであり、例えば、車両の走行機能(走る、曲がる、止まる等の機能)に対する攻撃を実施するフレーム、或いは、そのような攻撃の実施の前段階(攻撃予兆)のためのフレーム等である。

【0048】

ここでは、複数の車両(自動車)からログ情報(車載ネットワークで送信されるフレームの情報、車両ID等)を収集し分析し得る異常検知サーバであって、ある車両内のCANバスに送信されたフレームについて異常度の算定を行い、異常度に応じて、その車両或いは他の車両へ情報(警告、走行制御その他のための情報)を送信する異常検知サーバを中心として、車載ネットワーク管理システムについて説明する。なお、異常検知サーバは、1台の車両に搭載された装置であっても良いし、上述のクラウドサーバ1110或いはサーバ1210であっても良いが、ここでは上述のクラウドサーバ1110である例を想定して説明する。

【0049】

[1.1 車載ネットワーク管理システムの全体構成]

図2は、本実施の形態に係る車載ネットワーク管理システムの全体構成を示す図である。車載ネットワークシステムは、異常検知サーバ80と、車両1010a、1010b、1010c、1010d、1010e、1010fとが、通信路となるネットワーク81で接続されて構成される。ネットワーク81は、インターネット等を含み得る。異常検知サーバ80は、図1Aに示すクラウドサーバ1110に相当し、車両1010a、1010b、1010c、1010d、1010e、1010fは、図1Aに示す複数の車両1010に相当する。車両1010a、1010b、1010c、1010d、1010e、1010fは、車内の制御装置、センサ、アクチュエータ、ユーザインタフェース装置等の各種機器に接続されて、車内のバス(CANバス)を介してフレームに係る通信を行う複数のECUを含んで構成される車載ネットワークを備える。各車両の車載ネットワークでは各ECUはCANプロトコルに従って通信を行う。CANプロトコルにおけるフレームには、データフレーム、リモートフレーム、オーバーロードフレーム及びエラーフレームがある。ここでは主としてデータフレームに注目して説明する。なお、CANにおい

てデータフレームは、ID（メッセージID）を格納するIDフィールド、データ長を示すDLC（Data Length Code）、データを格納するデータフィールド等を含むように規定されている。

【0050】

車両1010a、1010bは、車種A、車両1010c、1010dは車種B、車両1010e、1010fは車種Cである。ここで、車種が同一の車両同士は、車載ネットワークの構成が同一である。即ち、ここでの車種が同一の車両は、例えば、型式（車両型式）が同一の車両であり、車両の識別情報としての車両IDの一部が同一の車両である。一例としては、車種が同一の車両は、車台番号における型式の値、或いは、車両識別番号（VIN：Vehicle Identification Number）における先頭からシリアル番号の前までの桁の値が、同一の車両である。同一車種の複数の車両において、車載ネットワークのCANバスに流れるデータフレーム（メッセージ）の利用に関する仕様（メッセージID毎のデータフィールドの内容の規定等）は同じである。また、車種が相違する車両同士において、同種のECUを備えることもある。同種のECUとは、構成が同一のECUであり、例えば、同じ製造事業者（ECUベンダ）による同型式のECUであり、また、主たる機能を実現するための構成が同一のECUを含むこととしても良い。車種が相違する車両同士において同種のECUを搭載している場合には、その各車両の同種ECUが送信するフレームのID（メッセージID）は互いに異なり得る。

10

【0051】

〔1.2 車載ネットワークシステムの構成〕

図3は、車種Aの車両1010a（車両1010bも同様）における車載ネットワークシステムの構成の一例を示す図である。他の車種の車両においては、図3に示す構成と同様の構成或いは一部異なる構成等を備える。

20

【0052】

車両1010a等における車載ネットワークシステムは、バス（CANバス）10～70により接続された、複数のECU（ECU100、101、200、201、300、301、302、400、401、500、600、700）とゲートウェイ90といった各ノードを含んで構成される。なお、図3では省略しているものの、車載ネットワークシステムには、更に多くのECUが含まれ得る。ECUは、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM、RAM等であり、プロセッサにより実行される制御プログラム（コンピュータプログラム）を記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作することにより、ECUは各種機能を実現することになる。なお、コンピュータプログラムは、所定の機能を達成するために、プロセッサに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

30

【0053】

バス10には、それぞれエンジン110、トランスミッション111に接続されたECU（エンジンECU）100及びECU（トランスミッションECU）101を含む、モータ、燃料、電池の制御といった車両の「走る」（走行）に関連する駆動系のECUが、接続されている。

40

【0054】

バス20には、それぞれブレーキ210、ステアリング211に接続されたECU（ブレーキECU）200及びECU（ステアリングECU）201を含む、「曲がる」、「止まる」等といった車両の挙動等の制御に関連するシャーシ系のECUが、接続されている。

【0055】

バス30には、それぞれ自動ブレーキ310、車線維持装置311、車車間通信装置312に接続されたECU300、ECU301及びECU302を含む、車間距離維持機能、衝突防止機能、エアバッグ等に関連する安全快適機能系のECUと車車間通信用のECUとが、接続されている。

50

【0056】

バス40には、それぞれドア410、ライト411に接続されたECU400及びECU401を含む、エアコン、ウィンカー等といった車両の装備の制御に関連するボディ系のECUが、接続されている。

【0057】

バス50には、インストルメントパネル510に接続されたECU500（ヘッドユニット）を含む、カーナビゲーション、オーディオ等に関連したインフォテインメント系のECUが、接続されている。なお、インストルメントパネル510とヘッドユニット（ECU500）との機能分担はいかなるものであっても良い。

【0058】

バス60には、ITS（Intelligent Transport Systems）装置610に接続されたECU600を含む、ETC（Electronic Toll Collection System）等の高度道路交通システムに対応するITS系のECUが、接続されている。

【0059】

バス70には、例えばOBD2（On-Board Diagnostics 2）等といった、外部の診断ツール（故障診断ツール）等と通信するためのインタフェースである診断ポート710に接続されたECU700が、接続されている。なお、ECU700を除き診断ポート710をバス70に接続していても良い。ここで示した各バスに接続されたECUに接続されている機器は、一例に過ぎず、例えば、他の1台又は複数台の機器に置き換えても良いし、省いても良い。

【0060】

ECU（ECU100、200等）のそれぞれは、接続されている機器（エンジン110、ブレーキ210等）の状態を取得し、定期的に状態を表すフレーム等を車載ネットワークつまりCANバスに送信している。

【0061】

バス10に接続されたECU100、101と、バス20に接続されたECU200、201と、バス30に接続されたECU300、301、302とは、MAC対応ECUであり、メッセージ認証コード（MAC）を処理する機能（MACの生成機能、MACの検証機能）を有する。また、バス40に接続されたECU400、401と、バス50に接続されたECU500と、バス60に接続されたECU600と、バス70に接続されたECU700とは、MAC非対応ECUであり、MACを処理する機能（MACの生成機能、MACの検証機能）を有さない。

【0062】

ゲートウェイ90は、異なる複数の通信路を接続して通信路間でデータを転送するゲートウェイ装置である。ゲートウェイ90は、バス10、バス20、バス30、バス40、バス50、バス60及びバス70と接続している。つまり、ゲートウェイ90は、一方のバスから受信したフレーム（データフレーム）を、一定条件下で他のバス（つまり条件に応じて選択した転送先バス）に転送する機能を有する一種のECUである。ゲートウェイ90は、車両の外部の異常検知サーバ80と通信するための通信装置（通信回路等）を備え、例えば、各バスから受信したフレームについての情報を異常検知サーバ80に送信（アップロード）する機能を有する。ゲートウェイ90の構成については、後に詳細に説明する。

【0063】

[1.3 異常検知サーバの構成]

図4は、サーバ（異常検知サーバ）80の構成図である。車両1010a等の車載ネットワークで送信される異常なフレームに対処するための異常検知サーバ80は、例えばプロセッサ、メモリ、通信インタフェース等を備えるコンピュータにより実現され、通信部810と、認証処理部820と、ログ収集処理部830と、ログ分析処理部840と、セキュリティ情報生成部850と、車両情報DB860と、車両ログ格納DB870と、分析結果格納DB880と、セキュリティ情報DB890とを含んで構成される。車両情報

10

20

30

40

50

DB860、車両ログ格納DB870、分析結果格納DB880及びセキュリティ情報DB890は、例えば、メモリ、ハードディスクといった記憶媒体等により実現され得る。また、認証処理部820、ログ収集処理部830、ログ分析処理部840、及び、セキュリティ情報生成部850それぞれの機能は、例えば、メモリに格納された制御プログラムがプロセッサにより実行されることにより、実現され得る。

【0064】

通信部810は、通信インタフェース、メモリに格納された制御プログラムを実行するプロセッサ等により実現される。通信部810は、車両1010a、1010b、1010c、1010d、1010e、1010fと、ネットワーク81を介して通信することで、各車載ネットワークのCANバス上に流れたフレーム（メッセージ）に関する情報等のログ情報を逐次受信する。ログ情報は、例えば、車載ネットワークでCANバスから受信されたフレーム（メッセージ）の内容、受信タイミング（間隔、頻度等）に関する情報を含む。通信部810は、各車両の車載ネットワークにおいて受信されたフレームについての情報を受信することで取得する取得部として機能する。また、通信部810は、セキュリティ情報生成部850が生成したセキュリティに関する送信用情報を送信する。送信用情報は、例えば、車両の乗員等を対象としたアラート（警告）通知のための提示用情報、車両の走行等の制御指示を示す制御情報、車両において暗号処理の適用に際して用いられる鍵の更新を指示するための制御情報、車両側でフレームに係る不正を検知するための不正検知用情報等である。

【0065】

認証処理部820は、暗号処理機能を備え、車両（車両1010a、1010b、1010c、1010d、1010e、1010f）と通信する際に、車両と異常検知サーバ80との間で行う相互認証を担い、暗号処理により安全な通信路を確立する。例えば、認証処理部820は、暗号処理機能により、相互認証に基づいて、通信部810が受信した、車両からの暗号化されたログ情報を復号し、車両に送信するための送信用情報を暗号化し得る。また、異常検知サーバ80は、各種DBに情報を暗号化して保存する際に、認証処理部820の暗号処理機能を利用する。

【0066】

ログ収集処理部830は、各車両から収集したログ情報の内容である各種データ（車載ネットワークで受信されたフレームについての情報等）を、車両ログ格納DB870に格納する。ログ収集処理部830は、各種データを車両ログ格納DB870へ格納する際に、各種データに所定の正規化等の処理を施しても良い。車両ログ格納DB870に格納されるデータ（車両ログ情報）については図5を用いて後に説明する。

【0067】

ログ分析処理部840は、車両ログ格納DB870に格納（蓄積）された各車両から収集されたログ情報を用いて分析することにより、ある車両の車載ネットワークで受信されたフレームが異常であるか否か（攻撃者によりその車載ネットワークに攻撃フレームが流されたか否か）に関連する指標である異常度を算定する機能を有する。ログ分析処理部840は、集積されたログ情報が表す、各車両から収集された複数のフレームについての情報（複数のフレームそれぞれの内容、受信タイミング等の情報）について、例えば、統計処理等を行い得る。ログ分析処理部840は、通信部810（取得部）により取得された複数のフレームについての情報と、その複数のフレームについての取得より後に、取得部により取得された、一の車両（例えば車両1010a）の車載ネットワークにおいて受信されたフレームについての情報とに基づいて、その一の車両の車載ネットワークにおいて受信されたそのフレームの異常度を算定する算定部として機能する。

【0068】

ログ分析処理部840は、例えば、正常状態において車載ネットワークで流れる各フレームについての所定モデルであって異常状態との比較用に用いることのできる所定モデルを構築し、逐次取得されるログ情報に基づいて機械学習を用いて所定モデルをより適切なものへと調整（更新）することとしても良い。この場合に、ログ分析処理部840は、集

10

20

30

40

50

積したログ情報が表す複数のフレームについての情報に適宜、加工処理（例えば多変量解析等）を施して、所定モデルの学習のために供給し得る。所定モデルの学習には、教師あり学習、教師なし学習のいずれの方式を用いても良い。例えば、各車両の車載ネットワークシステムにおいて、所定ルールに基づいてそのルールに適合しないフレーム（不正フレーム）がCANバスに流れたことを検知する不正検知機能がある場合には、不正フレームか不正でないフレームかの区別を示す情報をログ情報に含ませても良く、ログ分析処理部840では、その区別を示す情報に基づいて、所定モデルについて教師あり学習を行っても良い。また、ログ分析処理部840では、各車両から不正フレームでないフレームについてのログ情報を収集して、或いは不正フレームか否かについて区別せずにログ情報を収集して、これらのログ情報に基づいて、所定モデルについて教師なし学習を行っても良い。この所定モデルは、ある車両の車載ネットワークで受信されたフレームについての異常度（異常の度合い）の算定に利用される。所定モデルの内容は、そのフレームの異常度の算定に用いることのできるものであれば良い。異常度は、例えば、そのフレームについての情報と所定モデルとの比較（つまりフレームについての情報と所定モデルとを用いた演算処理）により算定される。ログ分析処理部840は、異常度の算定のための所定モデルとして、例えば、同一車種の各車両におけるログ情報に基づいて、正常状態において車載ネットワークで受信されるフレームについての特徴量（フレームの内容、受信間隔、受信頻度等の各成分を含む特徴ベクトル等）の分布を表わすように所定モデルを構築し得る。なお、所定モデルは、例えば、異常度を目的変数としてログ情報を説明変数とする場合の目的変数と説明変数との間の関係を表すモデルであってもよい。異常度は、例えば、異常なし（正常）を0（ゼロ）とし、異常ありの場合に異常の度合いに応じた正の数値をとるように定め得る。異常度は、0（例えば異常なし）と1（例えば異常あり）との2値をとるものであっても良いし、異常ありを複数段階に区別して3値以上をとるものであっても良い。異常度が所定閾値を超える場合に異常ありと判別するような活用も可能である。一例としては、ある車両の車載ネットワークで受信されたフレームの異常度は、そのフレームの特徴量が、既に集積されたログ情報に基づいて定められた所定モデルが示す特徴量の分布（例えば平均値と分散で特定される正規分布）に対する標準偏差に所定係数（例えば3）を乗じて定まる閾値を境界とする範囲の内に位置するか否かで算定でき、また、所定係数を複数用いることで異常度を複数段階に算定できる。異常度を算定するための所定モデルの構築に用いられる手法としては、外れ値検出、時系列上の急激な変化を検出する変化点検出等がある。

10

20

30

【0069】

このようにログ分析処理部840は、集積されたログ情報（車両ログ情報）が表す各車両の車載ネットワークで受信された複数のフレームについての情報に基づいて、その複数のフレームについての受信より後に、ある車両の車載ネットワークにおいて受信されたフレームの異常度を算定する。ある車両の車載ネットワークにおいて受信されたフレームの情報もその車両のログ情報から得ることができる。そしてログ分析処理部840で算定された異常度は、セキュリティ情報生成部850で生成する送信用情報の内容の決定、送信用情報の送信先の車両の範囲の決定、送信用情報の送信タイミング（時期）の決定等のために用いられる。ある車両の車載ネットワークで受信されたフレームについて算定した異常度により異常ありと判別した場合（つまり攻撃フレームを検知した場合）に、ログ分析処理部840は、セキュリティ情報生成部850に、その車両及び一定条件下で他の車両へと送信用情報の送信（警告の通知等）を行わせる。ログ分析処理部840は、集積したログ情報に基づく統計処理、所定モデルの更新（学習）、ある車両の車載ネットワークで受信されたフレームの異常度の算定等の各種分析処理を逐次行う。そしてログ分析処理部840は、その分析処理の結果（例えば更新後の所定モデルを表わす情報、算定した異常度に関する情報等）を、分析結果格納DB880に格納して保存し、次の分析処理（フレームの異常度の算定等）に利用する。

40

【0070】

セキュリティ情報生成部850は、車両情報DB860が保持する車両情報（図6参照

50

）と、セキュリティ情報DB890に格納された攻撃フェーズ情報（図7参照）及びアラートレベル情報（図8参照）とを参照して、ログ分析処理部840で算定された、ある車両の車載ネットワークで受信されたフレームについての異常度に応じて、セキュリティに関する送信用情報の内容を決定し、送信用情報の送信先の車両の範囲（同一車種の車両に所定の送信用情報を送信するか否か等）を決定し、送信用情報の送信時期を決定する。これらの決定については図6～図8を用いて後述する。これらの決定に従ってセキュリティ情報生成部850は、送信用情報の送信の制御を行い、つまり通信部810に送信先の車両へと送信用情報を送信させる。

【0071】

〔1.4 車両ログ情報〕

図5は、異常検知サーバ80の車両ログ格納DBの内容である車両ログ情報の一例を示す図である。同図に示すように車両ログ情報は、カーメーカが製造する各種車両について、車種と、車種毎に車両を識別するための車両IDと、車両に搭載される各ECUについてのIDと、その各ECUが送信するフレームについての情報であるCANログとを関連付けて表わす情報である。この車両ログ情報は、異常検知サーバ80が各車両から取得したログ情報を集積することで生成されている。ここでCANログは、例えばCANのフレームの識別情報（ID（メッセージID））、フレームの送信周期（受信周期）、フレームのDLCが示すデータ長、フレームのデータフィールドの内容であるデータ等を示し、各車両から受信したログ情報に基づく情報である。なお、CANログの各情報は、ログ情報が示すCANのフレームについての特徴量（例えば特徴ベクトル等）を正規化したものであっても良い。なお、車両ログ情報における車種は、例えば車両IDに基づいて特定され得る。

【0072】

この車両ログ情報に基づく分析処理により、ログ分析処理部840では、ある車両の車載ネットワークで受信されたフレームについての異常度の算定等が行われる。

【0073】

〔1.5 車両情報DB〕

図6は、異常検知サーバ80の車両情報DBが保持する車両情報の一例を示す図である。同図に示すように車両情報は、車種毎に、その車種の車両が搭載しているECUのID（ECUの種別を識別するための型式等）と、そのECUが送信するフレームのID（CANのメッセージID）とを対応付けた情報である。車両情報は、車種毎にその車種の車両に搭載される全てのECUのIDと、その各ECUが送信するフレームに係るCANのメッセージIDとを含むが、説明の便宜上、図6では一部のECUのID及びそのECUが送信する一部のフレームのIDしか示していない。

【0074】

図6の例は、車種Aの各車両が、CANのメッセージID「100」のフレームとメッセージID「101」のフレームとを送信する、ECUのID「001」のECUと、CANのメッセージID「200」のフレームを送信する、ECUのID「002」のECUとを搭載していることを示す。また、車種Bの各車両が、CANのメッセージID「110」のフレームとメッセージID「111」のフレームとを送信する、ECUのID「001」のECUと、CANのメッセージID「301」のフレームを送信する、ECUのID「003」のECUとを備えることを示す。この例では、車種Aの車両と車種Bの車両とは、同種（同一種別）のECU（ID「001」のECU）を搭載しているが、それぞれのECUが送信するフレームについてのCANのメッセージIDが互いに異なることを示している。このように同種のECUは、複数の車種の車両に搭載され得る。相違する車種の各車両に搭載された、同種のECUそれぞれが送信するフレームについては、フレームのメッセージIDが相違し得るだけで、その他のフレームの内容（DLCが示すデータ長、データフィールドのデータ等）、フレームの送信周期等は同一である。

【0075】

この車両情報を参照することで、セキュリティ情報生成部850は、異常度に応じた一

10

20

30

40

50

定条件下で、ある車両で異常なフレームを送信したECUと同種のECUを搭載する車種の車両を、セキュリティに関する送信用情報の送信先に含ませることができる。図6の例によれば、車種Aのある車両の車載ネットワークで受信されたCANのメッセージIDが「100」のフレームの異常度が異常ありに該当する場合においては、ECUのID「001」のECUが攻撃者に制御されている可能性がある。この場合に一定条件下で、セキュリティ情報生成部850は、同種のID「001」のECUを搭載する車種A及び車種Bの各車両に対して、セキュリティに関する所定の送信用情報を送信するように制御する。

【0076】

〔1.6 攻撃フェーズ情報〕

図7は、セキュリティ情報DB890が保持する攻撃フェーズ情報の一例を示す。攻撃フェーズ情報は、攻撃フレームを送信することによる攻撃者の攻撃について複数段階（ここでは4つの攻撃フェーズ）に区別し、各攻撃フェーズについてアラートレベルを対応付けた情報である。図7の例では、攻撃フェーズ情報は、攻撃フェーズ及びその攻撃フェーズの攻撃が検知された数（検知数）の組み合わせと、5段階の各アラートレベルとを対応付けている。この検知数は、累積的な検知数であっても一定の単位期間における検知数であっても良い。アラートレベルは、セキュリティ上の重要度を示し、異常検知サーバ80が車両に送信する、セキュリティに関する送信用情報に係る送信態様を区別するために用いられる指標である。アラートレベルに応じた送信用情報の各送信態様については、図8を用いて後述する。

【0077】

図7に示すように攻撃フェーズは、攻撃予兆と攻撃とに大別される。3段階に区別されたフェーズ1～3が攻撃予兆の攻撃フェーズである。また、フェーズ4が攻撃の攻撃フェーズである。攻撃フェーズは、攻撃者によって概ねフェーズ1、2、3、4の順に実行されることが想定されるが、必ずしもフェーズ1、2、3、4の順に実行されるとは限らない。

【0078】

以下、攻撃フェーズ毎に、想定される攻撃者による攻撃予兆或いは攻撃と、攻撃フェーズの判別手法の例と、アラートレベルとについて説明する。

【0079】

〔1.6.1 フェーズ1〕

一般に車載ネットワークで用いられるCANのフレーム（メッセージ）に係る仕様（例えばメッセージID毎のフレームの内容、用途等）は、非公開である。このため、攻撃者は、まず攻撃の準備として、1台の車両に対して、診断ポート（例えば図3の診断ポート710）を介して、様々なCANのフレーム（メッセージ）を車載ネットワークに不正に注入し、車両の挙動を確認しながらCANのフレームに係る仕様を解析する。この解析行為は、所望の攻撃メッセージのCANのフレームに係る仕様が解明するまで、トライアンドエラーを繰り返すことで行われる。また、CANのフレームに係る仕様の解析とは別にCANバスに攻撃フレームを送り込むために、車載ネットワークにおける欠陥（脆弱性）を探す。攻撃フェーズ情報では、この攻撃の準備の段階を、攻撃予兆のフェーズ1と定めている。

【0080】

セキュリティ情報生成部850は、例えば、異常ありを示す異常度が算定されたフレームのメッセージIDが、車載ネットワークの正常状態において車載ネットワークに接続された各ECUが送信すると規定されているメッセージID以外のメッセージIDであった場合、或いは、そのフレームの受信間隔（送信間隔）が正規のフレームのものと異なる場合等において、攻撃予兆のフェーズ1であると判別し得る。また、セキュリティ情報生成部850は、例えば、異常ありを示す異常度が算定されたフレームのメッセージIDが、診断コマンドのメッセージIDであって、フレーム1より上（重要度が高い）のフェーズに該当しないIDである場合に、攻撃予兆のフェーズ1であると判別し得る。なお、診断コマンドは、例えば、予め診断ポートに接続される正規の診断ツールが利用するものとし

10

20

30

40

50

て規定された特定のメッセージID（診断用メッセージID）を含むフレームである。なお、攻撃予兆のフェーズ1の判別手法として、他のいかなる方法を用いても良い。

【0081】

攻撃フェーズ情報は、フェーズ1を、検知数と関係なくアラートレベルの「1」と対応付けている。このため、セキュリティ情報生成部850は、フェーズ1と判別した場合に、アラートレベルの「1」に対応した送信態様で、送信用情報の車両への送信の制御を行う。

【0082】

[1.6.2 フェーズ2]

ある特定車種の車両の車載ネットワークに係る機器或いはECUに脆弱性が見つければ、攻撃者は、その脆弱性を突いて例えばその機器或いはECUを制御下に置くことを試みる。例えば、ヘッドユニット（ECU500）に脆弱性があり、ヘッドユニットがアプリケーションプログラム等のソフトウェアを外部ネットワークからダウンロード可能な仕様であるとする。この場合には、攻撃者は、ヘッドユニット向けのマルウェア（不正動作を行う悪意のあるソフトウェア等）を公開し、ユーザにマルウェアをダウンロードさせて脆弱性を突こうとする。また、攻撃者は、ヘッドユニットに接続する外部機器を介して、その脆弱性を突くかもしれない。例えば、ヘッドユニットがスマートフォンと接続できるのであれば、攻撃者は、インターネット上のサイト等にスマートフォン用のマルウェアを公開し、ユーザにダウンロードさせ、ユーザがスマートフォンとヘッドユニットを接続した際に、スマートフォン上のマルウェアからヘッドユニットの脆弱性を突くかもしれない。そして攻撃者は、ヘッドユニットの脆弱性を突いて、CANバスに不正アクセスするための攻撃基盤を構築するために、マルウェアにより、ヘッドユニットにおけるソフトウェア（ファームウェア等）を不正に書き換えてヘッドユニットを制御下に置くと考えられる。攻撃フェーズ情報では、この攻撃の準備の段階を、攻撃予兆のフェーズ2と定めている。また、V2X（車車間通信（V2V：Vehicle to Vehicle）及び路車間通信（V2I：Vehicle to Infrastructure））用のECU（例えばECU302）のような外部ネットワークと直接接続するECUに脆弱性があれば、攻撃者は、ヘッドユニット等を介さずに、そのECUに乗っ取って不正にそのECUのソフトウェアを書き換えるかもしれない。これらのCANバスに不正にアクセスできる状態にする行為の段階も、攻撃予兆のフェーズ2に該当する。即ち、ECUのソフトウェア（ファームウェア等）を不正に書き換える処理を行う段階を、攻撃予兆のフェーズ2としている。

【0083】

セキュリティ情報生成部850は、例えば、異常ありを示す異常度が算定されたフレームのメッセージIDが、ECUのファームウェア更新用のフレームのIDとして規定されているメッセージIDであった場合等において、攻撃予兆のフェーズ2であると判別し得る。なお、攻撃予兆のフェーズ2の判別手法として、他のいかなる方法を用いても良い。例えば、ファームウェア更新用のフレームが適切な更新時期でないのにCANバスに流れたことを確認する方法を用いても良い。

【0084】

攻撃フェーズ情報は、フェーズ2を、検知数が1の場合にアラートレベルの「2」と対応付け、検知数が1を超える場合にアラートレベルの「3」と対応付けている。このため、セキュリティ情報生成部850は、フェーズ2と判別した場合においてそのフェーズ2が検知された数が1であればアラートレベルの「2」に対応した送信態様で、フェーズ2が検知された数が複数であればアラートレベルの「3」に対応した送信態様で、送信用情報の車両への送信の制御を行う。

【0085】

[1.6.3 フェーズ3]

攻撃予兆のフェーズ2でマルウェアがECUのソフトウェアを不正に書き換える等により、ある特定車種の車両の車載ネットワークに攻撃基盤が構築された後において、マルウェアは、マルウェア自身が現在アクセスしている車両の車種等の情報を確認するために、

診断コマンド等をCANバスに送信することで、車両ID、ECU情報（ECU ID、ECUの名称等）等を取得しようとする。攻撃フェーズ情報では、この段階を、攻撃予兆のフェーズ3と定めている。

【0086】

セキュリティ情報生成部850は、例えば、異常ありを示す異常度が算定されたフレームのメッセージIDが、車両ID、ECU情報等の取得のための診断コマンドのメッセージIDである場合に、攻撃予兆のフェーズ3であると判別し得る。なお、攻撃予兆のフェーズ3の判別手法として、他のいかなる方法を用いても良い。

【0087】

攻撃フェーズ情報は、フェーズ3を、検知数が1の場合にアラートレベルの「3」と対応付け、検知数が1を超える場合にアラートレベルの「4」と対応付けている。このため、セキュリティ情報生成部850は、フェーズ3と判別した場合においてそのフェーズ3が検知された数が1であればアラートレベルの「3」に対応した送信態様で、フェーズ3が検知された数が複数であればアラートレベルの「4」に対応した送信態様で、送信用情報の車両への送信の制御を行う。

【0088】

[1.6.4 フェーズ4]

攻撃予兆のフェーズ3でマルウェアが車種等の情報を取得した後において、マルウェアが攻撃者の不正サーバにアクセスし、不正サーバから、該当車種に対応するCANの攻撃用のフレームの送信手順等を示すCAN攻撃セットを受信する。CAN攻撃セットは、例えば、車種毎の車両の車載ネットワークに対して車両の走行等を不正に制御するためのフレーム群の内容及び送信順序等を示すように攻撃者が準備したものである。マルウェアは、CAN攻撃セットに基づいて、CANバスに攻撃フレームを送信することで、攻撃を遂行し、車両を不正制御する。攻撃フェーズ情報では、この段階を、攻撃のフェーズ4と定めている。

【0089】

セキュリティ情報生成部850は、例えば、異常ありを示す異常度が算定されたフレームのメッセージIDが、そのフレームが受信された車両において重要な制御用のフレームのIDとして規定されている複数のメッセージIDのいずれかに該当する場合に、攻撃のフェーズ4であると判別し得る。重要な制御用のフレームは、重要性に鑑みて任意に規定可能であるが、例えば走行に関連するフレームである。走行に関連するフレームは、例えば、「走る」、「曲がる」、「止まる」等の車両の走行及び挙動の制御に関連する駆動系及びシャシ系のECU（例えばエンジンECU、トランスミッションECU、ブレーキECU、ステアリングECU等）により送信されることが規定されているフレームである。なお、攻撃のフェーズ4の判別手法として、他のいかなる方法を用いても良い。例えば、車両内のアクチュエータの制御指示を示すフレームの内容及び、アクチュエータの作用を反映した車両の状態を示すフレームの内容及びを比較することで、攻撃がなされているか否かを判別する方法を用いても良い。

【0090】

攻撃フェーズ情報は、フェーズ4を、検知数が1の場合にアラートレベルの「4」と対応付け、検知数が1を超える場合にアラートレベルの「5」と対応付けている。このため、セキュリティ情報生成部850は、フェーズ4と判別した場合においてそのフェーズ4が検知された数が1であればアラートレベルの「4」に対応した送信態様で、フェーズ4が検知された数が複数であればアラートレベルの「5」に対応した送信態様で、送信用情報の車両への送信の制御を行う。

【0091】

[1.7 アラートレベル情報]

図8は、セキュリティ情報DB890が保持するアラートレベル情報の一例を示す。アラートレベル情報は、アラートレベル毎の送信用情報の送信態様を示す情報である。図8の例では、アラートレベルを5段階に区別している。概ねアラートレベルが高い程、重要

10

20

30

40

50

度が高い。送信態様の要素には、送信先の車両の範囲、送信用情報の内容、送信用情報の送信時期等がある。図8の例では、送信先の車両の範囲を、3つのクラス（クラスA、B、C）に分類している。クラスAは、攻撃予兆或いは攻撃を観測した車両（つまり攻撃フレームが車載ネットワークにおいて受信された車両）を送信先とすることを示す。クラスB及びクラスCは、攻撃フレームが車載ネットワークにおいて受信された車両と所定関係を有する車両（同一車種或いは同種ECUを有する車両）について規定している。クラスBは、攻撃予兆或いは攻撃を観測した車両と同一車種の車両を送信先とすることを示す。クラスCは、攻撃予兆或いは攻撃を観測したECU（つまり攻撃フレームが車載ネットワークにおいて受信された車両において攻撃フレームと同じIDのフレームを送信するECU）と同種のECUを有し別の車種の車両を送信先とすることを示す。また、図8の例では、送信用情報の内容として、アラート（車両の乗員等に対する警告のための情報つまり警告の提示を指示する情報）と、制御情報（予め定められた安全な走行への移行を指示する情報、パワーステアリング機能の抑止、自動運転の抑制等といった、機能の縮退を指示する情報等）とを示している。予め定められた安全な走行への移行を指示する情報は、例えば、低速運転（走行速度の減速）を指示する情報、車両の走行の停止（路肩に停車等）を指示する情報等である。また、図8の例では、送信情報の送信時期について、即時通知（即時送信）と、通知（車両のエンジン始動時の通知、1日1回等の通知等に送信）とを区別している。

10

【0092】

セキュリティ情報生成部850は、アラートレベル情報が示すアラートレベルに対応する送信態様に従って、送信用情報の内容を決定して送信用情報の送信の制御を行う。図8の例では、アラートレベルの「5」は、クラスAの車両にはアラートと車両を安全な状態に移行させる制御情報とを即時通知（送信）し、クラスB、Cの車両にはアラートを即時通知するといった送信態様に対応する。アラートレベルの「4」は、クラスAの車両にはアラートと車両を安全な状態に移行させる制御情報とを即時通知（送信）し、クラスB、Cの車両には通知しないといった送信態様に対応する。アラートレベルの「3」は、クラスA、Bの車両にはアラートを即時通知し、クラスCの車両にはアラートを即時でなく通知するといった送信態様に対応する。アラートレベルの「2」は、クラスAの車両にのみアラートを即時通知し、クラスB、Cの車両には通知しないといった送信態様に対応する。アラートレベルの「1」は、クラスAの車両にのみアラートを即時でなく通知するが、クラスB、Cの車両には通知しないといった送信態様に対応する。なお、セキュリティ情報生成部850は、車両に送信用情報を送信する制御のみならず、カーメカ、ECUベンダのコンピュータ等といった装置に対してアラート通知を示す情報等を送信する制御を行っても良い。

20

30

【0093】

異常検知サーバ80から、上述のアラートを内容とする送信用情報を受信した車両においては、車両の運転者等の乗員に認知させる方法で警告の提示を行う。この警告の提示は、例えば、インストルメントパネル510に警告マーク或いは自動車ディーラーに行くことを勧める警告メッセージを表示すること、警報を鳴動すること、警告灯等を点灯すること、ハンドル（ステアリングホイール）、ブレーキペダル等に振動を加えること等により実現される。また、異常検知サーバ80から、上述の制御情報を内容とする送信用情報を受信した車両においては、車両内のECU等の各種機器が制御情報による指示に従った動作を行う。制御情報による指示は、低速運転、路肩に停車等の予め定められた安全な走行への移行の指示、機能の縮退の指示等の他に、車両を安全な状態にするためのいかなる指示であっても良い。

40

【0094】

[1.8 ゲートウェイの構成]

図9は、ある車両（例えば車両1010a）の車載ネットワークにおけるゲートウェイ90の構成を示す。同図に示すように、ゲートウェイ90は、フレーム送受信部901と、フレーム解釈部902と、不正フレーム検知部903と、ルール保持部904と、フレ

50

ーム生成部 905 と、転送制御部 906 と、転送ルール保持部 907 と、鍵処理部 920 と、鍵保持部 921 と、フレームアップロード部 950 と、不正検知通知部 930 と、更新処理部 940 とを含んで構成される。これらの各構成要素の各機能は、例えばゲートウェイ 90 における通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。例えば、フレームアップロード部 950 及び更新処理部 940 は、異常検知サーバ 80 と通信するための通信回路等により実現される。

【0095】

フレーム送受信部 901 は、バス 10、バス 20、バス 30、バス 40、バス 50、バス 60、及び、バス 70 のそれぞれに対して、CAN プロトコルに従ったフレームを送受信する。フレーム送受信部 901 は、バスからフレームを 1 bit ずつ受信し、フレーム
10
解釈部 902 に通知する。また、フレーム生成部 905 より通知を受けた転送先のバスを示すバス情報及び送信用のフレームに基づいて、そのフレームの内容を、バス 10、バス 20、バス 30、バス 40、バス 50、バス 60、及び、バス 70 のうち転送先のバスに、1 bit ずつ送信する。

【0096】

フレーム解釈部 902 は、フレーム送受信部 901 よりフレームの値を受け取り、CAN プロトコルで規定されているフレームフォーマットにおける各フィールドにマッピング
20
するよう解釈を行う。フレーム解釈部 902 は、受信されたフレームの各フィールドの情報を不正フレーム検知部 903 へ通知する。なお、フレーム解釈部 902 は、受け取ったフレームが CAN プロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部 905 へ通知する。また、フレーム解釈部 902 は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

【0097】

不正フレーム検知部 903 は、ルール保持部 904 が保持する、不正フレームか否かの判定用（不正フレームの検知用）のルール又はアルゴリズム（例えば不正検知用プログラム等）を示す情報（不正検知用情報）を参照し、受信されたフレームが不正フレームか否かを判定する。不正フレームの検知用のルール又はアルゴリズムを示す情報の一例としては、受信が許可される CAN のフレーム（メッセージ）の条件（特定ののための情報）を列
30
挙したホワイトリスト、受信が許可されない条件を列挙したブラックリスト等が挙げられる。不正フレームは、不正フレームの検知用のルールに適合しないフレームである。不正フレームと判定した場合には、不正フレーム検知部 903 は、不正フレームが送信されている途中において、不正フレームが送信されているバスに、エラーフレームを送信することで不正フレームを無効化するよう制御する。つまり不正フレームが検知された場合に、不正フレーム検知部 903 は、フレーム送受信部 901 にエラーフレームを送信させることで、不正フレームを無効化する。また、不正フレーム検知部 903 は、不正フレームか否かの判定結果を、フレーム解釈部 902 へ通知する。不正フレーム検知部 903 で不正フレームと判定されなかった場合にフレーム解釈部 902 は、そのフレームの各フィールドの情報を転送制御部 906 に通知する。また、不正フレーム検知部 903 は、不正フレーム
40
と判定した場合（不正フレームを検知した場合）にその不正フレームについての情報（例えば、不正検知の旨を示す情報、或いは、不正検知の旨及び不正フレームの内容を示す情報）を不正検知通知部 930 に通知する。なお、不正フレーム検知部 903 は、不正フレームと判定した場合には不正フレームの内容を示す情報を十分に取得するために、不正フレームを無効化するエラーフレームの送信を、不正フレームの特定部分（例えばデータフィールド部分）が受信されるまで待ってから速やかに行うこととしても良い。

【0098】

転送制御部 906 は、転送ルール保持部 907 が保持する転送ルール情報に従って、受信したフレームの ID（メッセージ ID）、及び、転送元バス（つまりそのフレームを受信したバス）に応じて、転送先のバスを選択し、転送先のバスを示すバス情報と、転送さ
50

れるべきフレームの内容（例えばフレーム解釈部 902 より通知されたメッセージ ID、DLC（データ長）、データ（データフィールドの内容）等）をフレーム生成部 905 へ通知して、送信を要求する。

【0099】

転送ルール保持部 907 は、バス毎のフレームの転送についてのルールを示す転送ルール情報を保持する。転送ルール情報は、転送元となり得る各バスについて、そのバスで受信された転送すべきフレームのメッセージ ID と転送先のバスとを示す。また転送ルール情報は、各バスが、フレーム内容を暗号化すると規定されたバスか否か、及び、フレームに MAC が付与されると規定されたバス（MAC 対応 ECU が接続されたバス）か否かを示す情報を含む。この情報を参照することで転送制御部 906 は、フレームの転送に際して、暗号化及び MAC の付与のそれぞれに関する処理を行う。例えば、転送制御部 906 は、転送先が MAC に対応している場合は、鍵保持部 921 が保持している MAC 鍵を用いて鍵処理部 920 に MAC を生成させ、フレームに MAC を付与して転送するように制御する。また、転送制御部 906 は、転送元が暗号化に対応している場合は、鍵保持部 921 が保持している、転送元のバスに接続された各 ECU と共有している暗号鍵を用いて、鍵処理部 920 にフレームの内容を復号させる。そして、転送先が暗号化に対応している場合は、転送制御部 906 は、鍵保持部 921 が保持している、転送先のバスに接続された各 ECU と共有している暗号鍵を用いて、鍵処理部 920 にフレームの内容を暗号化させて転送するよう制御する。鍵処理部 920 では、フレームの内容の暗号化、及び、フレームの内容等に基づく MAC の生成のそれぞれについて、いかなる方式を用いても良い。MAC は、例えばフレームのデータフィールド内の一部の値に基づいて生成しても良いし、その値と、他のフィールドの値或いはその他の情報（例えばフレームの受信回数をカウントするカウンタ値等）を結合したものに基いて生成しても良い。MAC の計算方法としては、例えば HMAC（Hash-based Message Authentication Code）、CBC-MAC（Cipher Block Chaining Message Authentication Code）等を用いることができる。

【0100】

フレーム生成部 905 は、転送制御部 906 からの送信の要求に従い、転送制御部 906 より通知されたフレームの内容を用いて送信用のフレームを構成し、その送信用のフレーム及びバス情報（例えば転送先のバスの識別子等）をフレーム送受信部 901 へ通知する。

【0101】

不正検知通知部 930 は、不正フレーム検知部 903 が不正フレームを検知した場合に不正検知の旨を運転者等に通知するために、不正フレームについての情報（例えば、不正検知の旨を示す情報、或いは、不正検知の旨及び不正フレームの内容を示す情報）をヘッドユニットに通知する制御（フレーム送受信部 901 の制御等）を行う。また、不正検知通知部 930 は、不正フレーム検知部 903 が不正フレームを検知した場合に、例えば、不正検知の旨を示す情報と、その不正フレームについての情報とを含ませたログ情報等を、異常検知サーバ 80 に通知する制御を行っても良い。この不正検知の旨により不正フレームを不正でないフレームと区別するログ情報は、例えば、異常検知サーバ 80 において教師あり学習に用いられ得る。また、不正検知の旨を示す情報は、異常検知サーバ 80 によって例えば各種通知（例えばカーメーカ、ECU ベンダ等といった各種の送信先への送信等）のためにも利用され得る。

【0102】

更新処理部 940 は、ルール保持部 904 が保持している不正フレームの検知用のルール又はアルゴリズムを示す情報（ホワイトリスト、ブラックリスト等）を、異常検知サーバ 80 から取得される情報に基づいて、更新する。

【0103】

フレームアップロード部 950 は、フレーム送受信部 901 により、いずれかの CAN バスから受信されたフレームを逐次取得し、受信されたフレームについての情報（例えば

フレームの内容、受信間隔、受信頻度等)を含むログ情報を異常検知サーバ80に送信(アップロード)する。フレームアップロード部950は、ログ情報に、ゲートウェイ90を搭載している車両の識別情報(車両ID)を含める。また、フレームアップロード部950は、ログ情報に、その他の各種情報(例えば車両状態情報、車両の位置の情報等)を含めても良い。フレームアップロード部950は、受信されたフレームについての情報として、異常検知サーバ80で統計処理、機械学習等を行う場合に取り扱い易いように、フレームの内容、受信間隔、受信頻度等を加工する加工処理を施しても良い。ここで、フレームの受信間隔は、例えば、そのフレームの受信時刻と、そのフレームと同一IDのフレームが前回受信された時刻との差である。また、フレームの受信頻度は、例えば、一定の単位時間において、そのフレームと同一IDのフレームが受信された数である。この加工処理は、例えば、フレームに関するデータの整形、データの分析(主成分分析等を含む多変量解析等)に係る処理である。加工処理は、例えば、フレームの内容、受信間隔、受信頻度等の特徴から特徴量を抽出し、正規化等を行い、特徴量の情報量の縮約を行うこと等である。特徴量の情報量の縮約は、例えば特徴量を各成分としての特徴ベクトルで表し、異常検知サーバ80と連携して得た情報に基づいて、特徴ベクトルの次元数を主成分分析で削減すること等により実現される。また、フレームアップロード部950は、フレーム送受信部901がCANバスからフレームを受信する毎に、そのフレームについての情報を含むログ情報を異常検知サーバ80に送信することとしても良いし、複数のフレームが受信された段階でその各フレームについての情報を含むログ情報を異常検知サーバ80に送信することとしても良い。但し、CANバスから受信されたフレームについての情報を、迅速に異常検知サーバ80へと伝え、そのフレームが異常であるか否かを異常検知サーバ80に迅速に検知させて迅速な対処を可能にし得る。また、フレームアップロード部950は、例えば異常検知サーバ80とのトラフィック量を削減すべく、無条件で又は通信状況に応じて、ログ情報を圧縮して異常検知サーバ80に送信しても良いし、フレーム送受信部901がCANバスから受信したフレームのうち全てのフレームについての情報ではなく特定の1つ又は複数のIDのフレームだけについての情報をログ情報に含めて送信しても良い。

【0104】

なお、異常検知サーバ80から送信用情報の送信がなされた場合に対応して、ゲートウェイ90は、その送信用情報を受信し、送信用情報(アラート、制御情報等)に従って、CANバスを介して予め定められたECUに必要な情報を送信する等によって、警告の提示、車両の走行の制御、機能の縮退の制御等を実現させる。

【0105】

[1.9 異常検知サーバと車両との連携動作]

図10は、異常検知サーバ80と車両との連携動作の一例を示すシーケンス図である。同図は、主として、ある車両(車両1010a)が、車載ネットワークのCANバスで受信されたフレームについての情報(フレームの情報を加工処理して得られた特徴ベクトル)を含むログ情報を、異常検知サーバ80に送信し、異常検知サーバ80で、フレームの異常度の算定等の処理(異常検知処理)を行う動作例を示す。具体的には、ある車両のゲートウェイ90が1つのフレームを受信する際の動作例を表わしている。この例では車両1010aがログ情報を異常検知サーバ80に送信する例を示すが、異常検知サーバ80に対しては、その他の各車両(車両1010b、1010c、1010d、1010e、1010f等)が同様にログ情報を送信する。以下、図10に即して動作例を説明する。

【0106】

車両1010aの車載ネットワークにおけるバス10に接続された1つのECU(例えばエンジンECU100、トランスミッションECU101等)がバス10にCANのフレームを送信し始める(ステップS101)。

【0107】

車両1010aのゲートウェイ90は、ステップS101により送信されているフレームをバス10から受信する(ステップS102)。

【0108】

ゲートウェイ90は、ステップS101でフレームが送信されている間において、不正フレーム検知部903により、ステップS102で受信したフレームが不正か否かについて、不正フレームの検知用のルール又はアルゴリズムを示す情報を参照することで、判定する（ステップS103）。ゲートウェイ90は、ステップS103で、不正と判定した場合（不正検知の場合）には、ステップS101で送信され始めたフレームの送信が完了する前に、エラーフレームを送信して不正フレームを無効化する（ステップS104）。なお、このエラーフレームの送信により、バス10に接続された、不正フレームを送信中のECUでは、エラーフレームを受信することになり（ステップS105）、エラーフレームを受信するとフレームの送信を中断する（ステップS106）。また、バス10に接続された他のECUも、エラーフレームの受信により、ステップS101で送信され始めたフレームの受信を中止する。

10

【0109】

ゲートウェイ90は、ステップS103で、不正と判定しなかった場合に、或いは、ステップS104でのエラーフレームの送信後に、ステップS102で受信したフレームの内容、受信間隔、受信頻度等に基づいて特徴量を特定（算出）する（ステップS107）。

【0110】

続いてゲートウェイ90は、フレームアップロード部950により、ステップS107で算出された、フレームについての特徴量に基づいて加工処理を行う（ステップS108）。フレームアップロード部950は、加工処理の結果として、フレームについての特徴ベクトルを含むログ情報を、異常検知サーバ80に送信する（ステップS109）。

20

【0111】

また、ゲートウェイ90は、受信したフレームがステップS103で不正と判定された場合を除いて、転送制御部906により、フレーム転送処理（転送ルール情報に基づいてフレームの転送を行う処理）を行う（ステップS110）。図10の例では、フレーム転送処理により、ゲートウェイ90は、バス20にフレームを転送し、バス20に接続されたブレーキECU200或いはステアリングECU201は、転送されたフレームを受信する（ステップS111）。

【0112】

異常検知サーバ80は、ゲートウェイ90から、車両1010aの車載ネットワークで受信されたフレームについての特徴ベクトルを含むログ情報を受信する（ステップS112）。そして、異常検知サーバ80は、受信した特徴ベクトルを含むログ情報を利用して、異常検知処理を行う（ステップS113）。次に異常検知処理について図11を用いて説明する。

30

【0113】

[1.10 異常検知サーバにおける異常検知処理]

図11は、異常検知サーバ80における異常検知処理の一例を示すフローチャートである。以下、同図に即して、異常検知処理について説明する。

【0114】

異常検知サーバ80は、各車両から送信されたログ情報（各車両の車載ネットワークで受信されたフレームについての情報を含むログ情報）に基づいて、統計的異常検知処理を行う（ステップS201）。統計的異常検知処理は、各車両から取得したログ情報（つまり車両ログ情報として集積した各ログ情報）を参照して、車載ネットワークで受信されたフレームについての情報に基づいて統計処理、多変量解析等を行うことで、異常状態との比較用に用いることのできる所定モデルの構築或いは機械学習による所定モデルの更新を行う処理を含む。また、統計的異常検知処理は、過去に各車両の車載ネットワークで受信されたフレームに基づくその所定モデルと、ある車両（ここでは車両1010aとする。）から最後に取得したログ情報が含むその車両の車載ネットワークで受信されたフレームについての情報（特徴ベクトル等）とを用いた演算処理（比較等）により、その車両1010aで受信されたフレームの異常度について算定する処理を含む。この演算処理は、例

40

50

例えば、外れ値検出、時系列上の急激な変化を検出する変化点検出等のための処理を含み得る。異常検知サーバ80では、上述したログ分析処理部840により、フレームの異常度を算定する。なお、異常検知サーバ80が、異常度について算定するフレームは、車両1010aの車載ネットワークで受信されたフレームに限定されるものではなく、他の車両の車載ネットワークで受信されたフレームでも良い。

【0115】

異常検知サーバ80は、ステップS201の統計的異常検知処理によりフレームについて算定した異常度が、予め定められた閾値より高いか否かにより、フレームが異常であるか否かの判定（異常検知）を行う（ステップS202）。

【0116】

ステップS202でフレームが異常であると判定した場合には、異常検知サーバ80は、異常と判定したフレームの識別情報（メッセージID）等に応じて、例えば攻撃予兆、攻撃等のどの段階の攻撃フェーズであるかを判別することにより、攻撃フェーズ情報（図7参照）を用いてアラートレベルの決定（つまり送信用情報の内容、送信時期、送信先の車両の範囲等といった送信態様の決定）を行う（ステップS203）。

【0117】

次に、異常検知サーバ80は、ステップS203で決定したアラートレベルに従った送信態様で送信用情報（アラート、制御情報等）の送信を行う（ステップS204）。これにより、アラートレベル情報（図8参照）に従って、アラート通知、走行制御等のための送信用情報が、1台又は複数台の車両へと送信されることになる。

【0118】

ステップS204の後、或いは、ステップS202でフレームが異常でないと判定した場合には、異常検知サーバ80は、ステップS202での判定結果或いはステップS201での統計的異常検知処理での更新後の所定モデルを表す情報を分析結果格納DB880に格納して保存する（ステップS205）。また、異常検知サーバ80は、車両1010aから最後に受信したデータ（ログ情報）を車両ログ情報に含ませて保存する（ステップS206）。なお、異常検知サーバ80における機械学習による所定モデルの更新は、例えば、ステップS201の統計的異常検知処理内ではなくステップS206において実行することとしても良い。

【0119】

〔1.11 アラートレベル決定方法の変形例〕

車両1010a等の車載ネットワークで受信されたフレームについて、異常検知サーバ80は、算定した異常度が異常ありを示す場合に、アラートレベルを決定するために図7に示すような攻撃フェーズ情報を参照することとした。異常検知サーバ80は、この攻撃フェーズ情報を用いて、上述したフレームのメッセージID等に基づいて攻撃フェーズを判別することで、アラートレベルを決定する方法の代わりに、以下に示すようなアラートレベル決定用情報に従ったアラートレベルの決定方法を用いても良い。

【0120】

図12Aは、アラートレベル決定用情報の例1を示す。この例は、異常検知サーバ80が算定した、車両の車載ネットワークで受信されたフレームについての異常度が、異常ありを示すところの車両の累積数（累積台数）を基準とし、この累積台数に応じて、アラートレベルを変化させる例である。累積台数が多くなるほど、アラートレベルが高くなる。異常検知サーバ80は、累積台数を、例えば同一車種の車両毎に算定し得る。

【0121】

図12Bは、アラートレベル決定用情報の例2を示す。この例は、異常検知サーバ80が算定した、車両の車載ネットワークで受信されたフレームについての異常度が、異常ありを示すところの車両の、単位時間（例えば数十時間等）当たりの数（検知台数）を基準とし、この検知台数に応じて、アラートレベルを変化させる例である。単位時間当たりの検知台数が多くなるほど、アラートレベルが高くなる。このように、単位時間当たりの検知台数を区別することで、攻撃が急激に増えている場合にアラートレベルを上げて対処す

10

20

30

40

50

ることが可能となる。異常検知サーバ80は、検知台数を、例えば同一車種の車両毎に算定し得る。

【0122】

図12Cは、アラートレベル決定用情報の例3を示す。この例は、異常検知サーバ80が算定した、車両の車載ネットワークで受信されたフレームについての異常度が、異常ありを示すところの同一車種の車両の位置との距離（例えば最小距離、最大距離、平均距離等）を基準とし、この距離に応じて、アラートレベルを変化させる例である。なお、フレームに係る異常が発生している車両と、同一車種で同一の異常が発生している1つ又は複数の車両との距離を基準とする他に、これらの全部の車両間の相対距離の最小値、最大値或いは平均値等を基準としてアラートレベルを変化させても良い。距離が短くなるほど、アラートレベルが高くなる。このように、異常が発生した車両の距離を区別することで、局地的に攻撃が発生している場合にアラートレベルを上げて対処することが可能となる。なお、アラートレベルの決定のために、この例3のような異常ありの車両間の距離を用いる代わりに、異常ありの車両群の密度を用いることとしても良い。

10

【0123】

図12Dは、アラートレベル決定用情報の例4を示す。この例は、異常検知サーバ80が算定した、車両の車載ネットワークで受信されたフレームについての異常度が、異常ありを示すところのそのフレームの識別情報（CANのメッセージID）を基準とし、このメッセージIDに応じて、アラートレベルを変化させる例である。アラートレベル決定用情報として、予めアラートレベル毎に、メッセージIDが規定されている。例えば、フレームのデータが車両の走行への影響が大きいものであるほど、そのフレームのメッセージIDに、高いアラートレベルを対応付けておくことが有用である。

20

【0124】

異常検知サーバ80から車両への送信用情報の送信の各種送信態様に対応するアラートレベルの決定方法は、上述したものに限られることはなく、いかなる基準を用いることとしても良い。例えば、アラートレベルの決定方法として、アラートレベル決定用情報の例1～例4で用いた基準を、いくつかを組み合わせる利用しても良い。

【0125】

異常検知サーバ80で算定した、フレームの異常度に応じて、異常度が異常ありを示す場合に何らかの基準を用いて、アラートレベルを決定する上述の各決定方法の他に、フレームの異常度に応じて直接的にアラートレベルを決定することとしても良い。図12Eは、フレームの異常度に応じて直接的にアラートレベルを決定するためのアラートレベル決定用情報の例5を示す。この例は、異常検知サーバ80が算定した、車両の車載ネットワークで受信されたフレームについての異常度を基準とし、この異常度に応じて、アラートレベルを変化させる例である。異常度が高くなるほど、アラートレベルが高くなる。なお、この例5では、異常度を整数値で表すこととしたが、異常度はいかなる表現態様で表されても良い。また、異常度を複数段階に区分してその各区分を上述した各攻撃フェーズに相当するものとして、攻撃フェーズ情報（図7参照）に基づいてアラートレベルを決定することとしても良い。なお、アラートレベルで特定される送信態様（送信用情報の内容、送信時期、送信先の範囲等）は、いかなる内容であっても良く、例えば、送信用情報の内容としては、異常なフレームが検知された車両について送信する送信用情報と、その車両と所定関係を有する車両に送信する送信用情報（所定の送信用情報）とを、同一にしても良いし、相違させても良い。

30

40

【0126】

[1.12 実施の形態1の効果]

実施の形態1に係る車載ネットワーク管理システムでは、異常検知サーバ80が各車両から車載ネットワークで受信されたフレームについての情報等を集積して機械学習等により所定モデルを調整し、ある車載ネットワークで受信されたフレームについての異常度をそのフレームについての情報と所定モデルとの比較に係る演算処理により算定するセキュリティ処理方法を実行する。所定モデルには、例えば、概ね正常状態における各車両の車

50

載ネットワークに流れたフレームがどのようなタイミングでどのような内容を含むか等の特徴の分布が反映され得る。このため、ブラックリスト等の既存ルールに基づく不正検知手法では検知できない異常（例えば攻撃予兆、未知の攻撃等に係る攻撃フレーム）が異常検知サーバ80により検知され得る。異常検知サーバ80では、統計的異常検知処理を行うことで、正常ではないつまり異常なフレームのうち、既存のルールに適合しないフレーム（不正フレーム）ではないものも、検知し得る。このように異常検知サーバ80により、各車両の車載ネットワークのセキュリティが高まり得る。

【0127】

また、異常検知サーバ80は、算定した異常度に応じて、直接的に又は他の基準を併用してアラートレベルを決定して、アラートレベルに対応する送信態様で、セキュリティに関する送信用情報（アラート通知等）を1台又は複数台の車両へと送信する。これにより、車両の運転者等に異常に対する注意を促すこと、或いは、車両を制御して、より安全な状態に移行すること等が、実現され得る。異常検知サーバ80により、例えば攻撃フェーズに応じてアラートレベルを変化させること等で、攻撃予兆、攻撃等の程度、規模等に応じて適切なセキュリティ対策を実現し得る。異常検知サーバ80は、一定条件下で、攻撃予兆或いは攻撃が検知された車両だけでなく、その車両と同じ車種の車両、或いは、攻撃対象とされたECUと同種のECUを備える別車種の車両にまでアラート通知等を送信する。このため、現在の攻撃又はその後の攻撃の影響を、最小限に抑えることが可能となり得る。

【0128】

また、異常検知サーバ80は、複数台の車両における異常を検知可能であるため、同時多発的に発生している攻撃を検知して対処するために有用である。異常検知サーバ80が、一定条件下で車両の運転者、カーメーカ、ECUベンダ等アラート通知を送信することで、攻撃への適切な対処（例えば、攻撃の未然防止等のための対処等）が可能となり得る。

【0129】

上述したように異常検知サーバ80は、フレームについての情報に基づいてそのフレームの異常度を算定する機能等を有する。そこで、車両は、車載ネットワークで受信されたフレームが、攻撃フレームか否かの判別が困難なグレーゾーンのフレームであると判定した場合に、そのフレームについての情報を異常検知サーバ80に伝えて、異常度の算定、或いは、その異常度に基づく異常か否かの判定等といった異常検知を要求することとしても良い。この場合には、車両は異常検知結果を受け取ることで、グレーゾーンのフレームに適切に対処することが可能となる。

【0130】

また、例えば、セキュリティ情報共有組織であるISAC（Information Sharing and Analysis Center）における自動車に対するサイバー攻撃の脅威、脆弱性についての情報共有、分析、対策検討等を行うAuto-ISAC、或いは、同種のセキュリティ組織等において、異常検知サーバ80に集積した車載ログ情報（各車両から収集した各ログ情報）を、インシデントが発生した後の分析（ドライブレコーダの分析）に活用することも可能となる。

【0131】

（実施の形態2）

実施の形態1では、異常検知サーバ80が、ある車両の車載ネットワークで受信されたフレームが異常であることを検知した場合に、車両に送信する送信用情報の内容として、主に、アラート通知、及び、車両の走行等の制御指示を示す制御情報について、説明した。本実施の形態では、送信用情報の内容が、車両側でフレームに係る不正を検知するための不正検知用情報である例について説明する。本実施の形態で示す車載ネットワーク管理システムの構成は実施の形態1で示したもの（図2参照）と同様である。

【0132】

【2.1 不正検知用情報を配信する異常検知サーバ】

異常検知サーバ８０は、ここで特に示さない点は、実施の形態１で示した構成を備える（図４参照）。

【０１３３】

異常検知サーバ８０は、ある車両の車載ネットワークで受信されたフレームについての情報に基づいてそのフレームの異常度を算定する。そのフレームの異常度が、異常であることを示す場合において、異常検知サーバ８０は、その異常と同一の異常を車載ネットワークにおいて検知するためのルール又はアルゴリズムを示す不正検知用情報を含む送信用情報を、その車両、及び、その車両と同一車種の車両に送信（配信）する。なお、異常検知サーバ８０は、各車種について車両のゲートウェイ９０のルール保持部９０４が保持する、不正フレームか否かの判定用（不正フレームの検知用）のルール又はアルゴリズムを示す不正検知用情報の内容を識別する管理情報（例えば不正検知用情報のバージョン番号等）を管理する。

10

【０１３４】

〔２．２ 不正検知用情報の配信の動作例〕

図１３は、異常検知サーバ８０による不正検知用情報（ルール等）の配信の動作例を示すシーケンス図である。

【０１３５】

異常検知サーバ８０は、各車両から送信されたログ情報に基づいて、統計的異常検知処理を行う（ステップＳ３０１）。このステップＳ３０１の統計的異常検知処理は、実施の形態１で示したステップＳ２０１の処理と同様である。ここでは、車種Ａの車両１０１０ａでの攻撃フレームの検知を例にして説明する。ステップＳ３０１で、過去に各車両の車載ネットワークで受信されたフレームに基づくその所定モデルと、車両１０１０ａから取得したログ情報が含むその車両の車載ネットワークで受信されたフレームについての情報（特徴ベクトル等）とを用いた演算処理（比較等）により、その車両１０１０ａで受信されたフレームの異常度が算定される。

20

【０１３６】

異常検知サーバ８０は、ステップＳ３０１の統計的異常検知処理により、車両１０１０ａの車載ネットワークで受信されたフレームについて算定した異常度が、予め定められた閾値より高いか否かにより、フレームが異常であるか否かの判定（異常検知）を行う（ステップＳ３０２）。

30

【０１３７】

ステップＳ３０２でフレームが異常である（つまり攻撃フレームである）と判定した場合には、異常検知サーバ８０は、車両１０１０ａのゲートウェイ９０のルール保持部９０４で保持している不正検知用情報が示すルール又はアルゴリズムでその異常な攻撃フレームが検知可能か否かを、不正検知用情報の管理情報等に基づいて、確認する（ステップＳ３０３）。

【０１３８】

ステップＳ３０３で、ゲートウェイ９０のルール保持部９０４で保持している不正検知用情報が示すルール又はアルゴリズムで該当の異常（攻撃フレーム）を検知可能でないと確認した場合に、異常検知サーバ８０は、その異常な攻撃フレームを検知するための新たなルール又はアルゴリズムを生成する（ステップＳ３０４）。なお、異常検知サーバ８０は、ステップＳ３０４で新たなルール等を生成するに際して、ユーザインタフェースを介して操作者等の指示を受けることにより、その生成を行っても良い。ステップＳ３０２で異常でないと判定された場合、或いは、ステップＳ３０３で、車両が保持しているルール等でその異常な攻撃フレームを検知可能であると確認された場合には、不正検知用情報の配信は行われない。

40

【０１３９】

異常検知サーバ８０は、生成した新たなルール又はアルゴリズムを、車両で攻撃フレームの検知のために用いて問題が生じないか否かについての検証テストを行い、その検証テストが成功した場合にのみ（ステップＳ３０５）、そのルール又はアルゴリズムを示す不

50

不正検知用情報を含む送信用情報を、車両 1010a を含む車種 A の車両へ配信する（ステップ S306）。なお、検証テストは、例えば車両をシミュレーションする環境において行われる。また、検証テストが成功しない場合においては、新たなルール又はアルゴリズムの調整等を行って、検証テストが成功するようにしてからその調整等したルール又はアルゴリズムを示す不正検知用情報の配信が行われ得る。

【0140】

不正検知用情報の配信を受けた車両（つまり不正検知用情報を含む送信用情報を受信した車両）のゲートウェイ 90 は、更新処理部 940 により、ルール保持部 904 が保持している、不正検知のためのルール又はアルゴリズムを示す不正検知用情報を、異常検知サーバ 80 から取得した不正検知用情報に基づいて、更新する（ステップ S307）。

10

【0141】

〔2.3 実施の形態 2 の効果〕

実施の形態 2 に係る車載ネットワーク管理システムでは、異常検知サーバ 80 がある車両の車載ネットワークで受信されたフレームについて算定した異常度により、そのフレームが異常（攻撃フレーム）であると判定した場合に、一定条件下で、その車両と同一車種の車両に対して、その異常（その攻撃フレーム）を車両側において検知するためのルール又はアルゴリズムを示す不正検知用情報を配信する。

【0142】

これにより、同様の攻撃フレームが送信された場合に、車両内の装置（例えばゲートウェイ 90）でその不正検知用情報を用いて、その攻撃フレームを、ルールに適合しない不正フレームとして、検知することが可能となる。従って、各車両の車載ネットワークのセキュリティが高まり得る。

20

【0143】

（実施の形態 3）

本実施の形態では、異常検知サーバ 80 が、暗号処理技術（暗号化或いは MAC 付与）を適用してデータを伝送することでデータを保護するように規定されているフレームの異常の検知に対応して、鍵更新要求（車両において暗号処理技術の適用に際して用いられる鍵の更新を指示するための制御情報を含む送信用情報）を車両に送信する例について説明する。本実施の形態で示す車載ネットワーク管理システムの構成は実施の形態 1 で示したもの（図 2 参照）と同様である。

30

【0144】

〔3.1 異常検知サーバ〕

異常検知サーバ 80 は、ここで特に示さない点は、実施の形態 1 で示した構成を備える（図 4 参照）。

【0145】

異常検知サーバ 80 は、ある車両の車載ネットワークで受信されたフレームについての情報に基づいてそのフレームの異常度を算定する。そのフレームの異常度が、異常であることを示す場合において、一定条件が満たされたときに、異常検知サーバ 80 は、その車両（異常なフレームが検知された車両）と、その車両と所定関係を有する車両とに、鍵更新要求を送信する。異常なフレームが検知された車両と所定関係を有する車両は、例えば、同一車種の車両、同種の ECU を搭載している車両等である。この所定関係を有する車両は、異常なフレームが検知された車両に関する情報に基づいて特定できる車両であれば、その他の一定の関係を有する車両であっても良い。また、上述の一定条件は、暗号鍵（例えば暗号化鍵）又は MAC 鍵が漏洩したと推定するための条件であり、例えば、異常なフレームが、鍵関連メッセージであるとき（つまりフレーム内容を暗号化すると規定されたフレーム、或いは、フレームに MAC が付与されると規定されたフレームであるとき）に満たされることとする。また、この一定条件には、更に、車両の走行状態等が異常となっている等の条件（暗号鍵又は MAC 鍵が漏洩したことをより精度良く推定するための条件）を加えても良い。異常検知サーバ 80 は、車両から取得したログ情報と、所定モデルとを用いた演算処理によって、暗号鍵又は MAC 鍵が漏洩したと推定できるか否かを判別

40

50

しても良い。

【0146】

異常検知サーバ80は、暗号化或いはMACにより保護されているフレームの異常を検知するために、予め定められたMAC／暗号化保護対象メッセージIDリストを用いる。図14は、MAC／暗号化保護対象メッセージIDリストの一例を示す図である。MAC／暗号化保護対象メッセージIDリストは、図14に示すように、車種毎に、その車種の車両が搭載するECUのID（ECUの種別を識別するための型式等）と、そのECUが送信するフレームのID（CANのメッセージID）と、そのメッセージIDのフレームがMAC対応（MACで保護されている）か否かと暗号化対応（暗号化により保護されている）か否かとを対応付けた情報である。MAC／暗号化保護対象メッセージIDリストは、車種毎にその車種の車両に搭載される全てのECUのIDと、その各ECUが送信するフレームに係るCANのメッセージIDとを含むが、説明の便宜上、図14では一部のECUのID及びそのECUが送信する一部のフレームのIDしか示していない。MAC／暗号化保護対象メッセージIDリストにより、暗号処理技術を適用してデータを伝送するためのフレーム用の予め規定された識別情報（メッセージID）を特定することができる。

10

【0147】

図14のMAC／暗号化保護対象メッセージIDリストの例は、車種Aの各車両が搭載する、ID「001」のECUにより送信されるCANのメッセージID「100」のフレームは、MACで保護され、暗号化で保護されていないことを示している。また、そのECUにより送信されるCANのメッセージID「101」のフレームは、MACで保護されず、暗号化で保護されていることを示している。また、車種Bの各車両が搭載する、ID「001」のECUにより送信されるCANのメッセージID「111」のフレームは、MACと暗号化との両方で保護されていることを示している。

20

【0148】

〔3.2 異常検知に応じた鍵更新要求の動作例〕

図15は、異常検知サーバ80が、暗号鍵又はMAC鍵が漏洩したと推定される異常の検知に対応して、鍵更新要求を行う動作例を示すシーケンス図である。

【0149】

異常検知サーバ80は、統計的異常検知処理（図11のS201）を行い、ある車両（例えば車両1010a）の車載ネットワークで受信されたフレームの異常度を算定し、そのフレームの異常度が所定閾値を超えるか否かにより異常ありか否かを判定する（ステップS401）。

30

【0150】

ステップS401で異常ありと判定したフレームのメッセージIDに基づいて、異常検知サーバ80は、そのフレームが鍵関連メッセージ（フレーム内容を暗号化すると規定されたフレーム、或いは、フレームにMACが付与されると規定されたフレーム）であるか否かを判定する（ステップS402）。

【0151】

ステップS402で、鍵関連メッセージで異常が検知されたと判定された場合（つまり異常ありのフレームが鍵関連メッセージであると判定された場合）には、異常検知サーバ80は、そのフレームが検知された車両1010a、及び、車両1010aと所定の関係を有する車両（本動作例では同一車種の車両1010b）に対して、鍵更新要求（つまり車両において暗号処理（暗号化或いはMAC付与）の適用に際して用いられる鍵の更新を指示するための制御情報を含む送信用情報）を送信する（ステップS403）。

40

【0152】

これに対して、車両1010aのゲートウェイ90は鍵更新要求を受信し（ステップS404）、その鍵更新要求に従って、鍵保持部921が保持する鍵を更新する（ステップS405）。異常検知サーバ80が送信し、ゲートウェイ90が受信する鍵更新要求は、新たな鍵を含む情報であっても良い。異常検知サーバ80は、異常なフレームに関連する

50

鍵は暗号鍵であるかMAC鍵であるかその両方であるかを指定する鍵指定情報を鍵更新要求に含ませても良い。車両1010aにおいてはその鍵指定情報に基づいて適切な鍵の更新を行うことが可能になる。

【0153】

また、同様に、車両1010bのゲートウェイ90は鍵更新要求を受信し（ステップS406）、その鍵更新要求に従って、鍵保持部921が保持する鍵を更新する（ステップS407）。ゲートウェイ90では、鍵更新要求に新たな鍵の情報が含まれていればその鍵へと更新し、新たな鍵の情報が含まれていなければ予め定められた手順で新たな鍵を生成してその鍵へと更新する。

【0154】

なお、異常検知サーバ80は、ステップS403で、車両に対して鍵更新要求を示す送信用情報を送信するのみならず、カーメカ、ECUベンダのコンピュータ等といった装置に対して、車載ネットワークで暗号処理に用いられる鍵（暗号鍵或いはMAC鍵）の漏洩に関する情報を送信することとしても良い。

【0155】

〔3.3 実施の形態3の効果〕

実施の形態3に係る車載ネットワーク管理システムでは、異常検知サーバ80がある車両の車載ネットワークで受信されたフレームについて算定した異常度等により、鍵関連メッセージであるフレームが異常であると判定した場合に、一定条件下で、その車両と所定の関係を有する車両に対して鍵更新要求を示す送信用情報を送信する。これにより、ECUが攻撃者に支配されて暗号処理に用いる鍵（暗号鍵或いはMAC鍵）を不正に利用されることに適切に対処可能となり、車載ネットワークのセキュリティの確保が実現され得る。

【0156】

（他の実施の形態）

上記実施の形態で示した車載ネットワーク管理システムに係る技術は、上述したサービスの態様（図1A参照）の他、例えば、以下のクラウドサービスの類型において実現され得る。但し、上記実施の形態で示した技術の適用が、ここで説明するクラウドサービスの類型に限られるものではない。

【0157】

（サービスの類型1：自社データセンタ型クラウドサービス）

図16は、サービスの類型1（自社データセンタ型クラウドサービス）における車載ネットワーク管理システムが提供するサービスの全体像を示す図である。本類型では、サービスプロバイダ1200が、グループ1000から情報を取得し、ユーザ1002に対してサービスを提供する。本類型では、サービスプロバイダ1200が、データセンタ運営会社の機能を有している。即ち、サービスプロバイダ1200が、ビッグデータを管理するクラウドサーバ2030（クラウドサーバ1110に相当）を保有している。従って、データセンタ運営会社は存在しない。上述した異常検知サーバ80の一部又は全部は、例えばクラウドサーバ2030として実現され得る。本類型では、サービスプロバイダ1200は、データセンタとしてのクラウドサーバ2030を有し、運営及び管理する。また、サービスプロバイダ1200は、オペレーティングシステム（OS）2020及びアプリケーション（アプリケーションプログラム）2010を管理する。サービスプロバイダ1200は、OS2020及びアプリケーション2010を用いて、サービスを提供する。このサービスの類型1或いは以下の類型2～4におけるサービスの提供（例えば情報の提供）の対象は、ユーザ1002（例えばカーメカ、ECUベンダ等の事業者、特定の個人、団体等）に限られることはなく、車両を使用するユーザ1001、或いは、複数の車両1010における車両（例えば車両1010a等）自体であっても良い。例えば、サービスプロバイダ1200は、OS2020及びアプリケーション2010を用いて、クラウドサーバ2030により車両1010aの装置（ゲートウェイ90等）と通信することで、サービスを提供し得る。

【0158】

10

20

30

40

50

(サービスの類型 2 : I a a S 利用型クラウドサービス)

図 1 7 は、サービスの類型 2 (I a a S 利用型クラウドサービス) における車載ネットワーク管理システムが提供するサービスの全体像を示す図である。ここで、I a a S とは、インフラストラクチャー・アズ・ア・サービスの略であり、コンピュータシステムを構築及び稼働させるための基盤そのものを、インターネット経由のサービスとして提供するクラウドサービス提供モデルである。

【 0 1 5 9 】

本類型では、データセンタ運営会社 1 1 0 0 が、データセンタ (クラウドサーバ) 2 0 3 0 を運営及び管理している。また、サービスプロバイダ 1 2 0 0 は、OS 2 0 2 0 及びアプリケーション 2 0 1 0 を管理する。サービスプロバイダ 1 2 0 0 は、サービスプロバイダ 1 2 0 0 が管理する OS 2 0 2 0 及びアプリケーション 2 0 1 0 を用いてサービスを提供する。

10

【 0 1 6 0 】

(サービスの類型 3 : P a a S 利用型クラウドサービス)

図 1 8 は、サービスの類型 3 (P a a S 利用型クラウドサービス) における車載ネットワーク管理システムが提供するサービスの全体像を示す図である。ここで、P a a S とは、プラットフォーム・アズ・ア・サービスの略であり、ソフトウェアを構築及び稼働させるための土台となるプラットフォームを、インターネット経由のサービスとして提供するクラウドサービス提供モデルである。

【 0 1 6 1 】

20

本類型では、データセンタ運営会社 1 1 0 0 は、OS 2 0 2 0 を管理し、データセンタ (クラウドサーバ) 2 0 3 0 を運営及び管理している。また、サービスプロバイダ 1 2 0 0 は、アプリケーション 2 0 1 0 を管理する。サービスプロバイダ 1 2 0 0 は、データセンタ運営会社 1 1 0 0 が管理する OS 2 0 2 0 及びサービスプロバイダ 1 2 0 0 が管理するアプリケーション 2 0 1 0 を用いてサービスを提供する。

【 0 1 6 2 】

(サービスの類型 4 : S a a S 利用型クラウドサービス)

図 1 9 は、サービスの類型 4 (S a a S 利用型クラウドサービス) における車載ネットワーク管理システムが提供するサービスの全体像を示す図である。ここで、S a a S とは、ソフトウェア・アズ・ア・サービスの略である。S a a S 利用型クラウドサービスは、例えば、データセンタ (クラウドサーバ) を保有しているプラットフォーム提供者が提供するアプリケーションを、データセンタ (クラウドサーバ) を保有していない会社又は個人等の利用者がインターネット等のネットワーク経由で利用できる機能を有するクラウドサービス提供モデルである。

30

【 0 1 6 3 】

本類型では、データセンタ運営会社 1 1 0 0 は、アプリケーション 2 0 1 0 を管理し、OS 2 0 2 0 を管理し、データセンタ (クラウドサーバ) 2 0 3 0 を運営及び管理している。また、サービスプロバイダ 1 2 0 0 は、データセンタ運営会社 1 1 0 0 が管理する OS 2 0 2 0 及びアプリケーション 2 0 1 0 を用いてサービスを提供する。

【 0 1 6 4 】

40

以上、いずれのクラウドサービスの類型においても、サービスプロバイダ 1 2 0 0 がサービスを提供する。また、例えば、サービスプロバイダ又はデータセンタ運営会社は、OS、アプリケーション又はビッグデータのデータベース等を自ら開発しても良いし、また、第三者に開発させても良い。

【 0 1 6 5 】

(その他変形例)

以上のように、本発明に係る技術の例示として実施の形態 1 ~ 3 を説明した。しかしながら、本発明に係る技術は、これに限定されず、適宜、変更、置き換え、付加、省略等を行った実施の形態にも適用可能である。例えば、以下のような変形例も本発明の一実施態様に含まれる。

50

【0166】

(1) 上記実施の形態では、車両がCANのプロトコルに従った通信を行う車載ネットワーク（車載ネットワークシステム）を有する例を用いて説明したが、これに限定されることはなく、ネットワーク種別（通信プロトコル）は、いかなるものであっても良い。例えば、車載ネットワークは、CAN-FD、Ethernet（登録商標）、LIN（Local Interconnect Network）、Flexray（登録商標）等であっても良いし、これらを組み合わせた構成であっても良い。

【0167】

(2) 上記実施の形態では、異常検知サーバ80が、複数の車両の車載ネットワークにおいて受信された複数のフレームについての情報を取得し、その取得した複数のフレームについての情報に基づいて、所定モデルの機械学習による更新等を行って、その所定モデルとの比較に係る演算処理等により、その複数のフレームについての受信より後に、車両1010aの車載ネットワークにおいて受信されたフレームの異常度を算定する統計的異常検知処理の例を示した。しかし、異常検知サーバ80の代わりに、車両1010a内部の装置（例えばゲートウェイ90その他のECU）で、統計的異常検知処理の全部又は一部を行うこととしても良い。例えば、車両1010aのゲートウェイ90で、1つ又は複数の車両の車載ネットワーク（例えば車両1010aの車載ネットワークだけでも良いし、他の車両の車載ネットワークであっても良い。）において受信された複数のフレームについての情報を取得し、その取得した複数のフレームについての情報に基づいて、所定モデルの機械学習による更新等を行って、その所定モデルとの比較に係る演算処理等により、その複数のフレームについての受信より後に、車両1010aの車載ネットワークにおいて受信されたフレームの異常度を算定することとしても良い。そして、ゲートウェイ90は、算定した異常度に応じて、異常か否かの判定、異常ありの場合における運転者等への警告（アラート通知）、車両の走行の制御、車両における暗号処理の適用に際して用いられる鍵の更新、他の車両への送信用情報（アラート通知、制御情報等）の送信等を行うこととしても良い。なお、車両1010a内部の装置は、統計的異常検知処理の全部又は一部を行った結果を、クラウドサーバ（例えば異常検知サーバ80）に送信することとし、クラウドサーバでその結果を活用（ユーザへの情報提供等）することとしても良い。

【0168】

(3) 上記実施の形態では、クラウドサーバ等に相当する異常検知サーバ80で、統計的異常検知処理を実行する例を示したが、よりローカル環境（車両）に近いエッジサーバで統計的異常検知処理を実行するようにしても良く、これにより通信遅延が低減され得る。例えばエッジサーバが路側機であり、車両は路側機に車載ネットワークで受信されたフレームについての情報をアップロードし、路側機が、統計的異常検知処理を行って異常検知の結果をクラウドサーバにアップロードするようにしても良い。

【0169】

(4) 上記実施の形態では、特徴ベクトルの作成の処理等を含む加工処理を、車両のゲートウェイ90のフレームアップロード部950で行う例を示した。しかし、車両内の装置（フレームアップロード部950等）と異常検知サーバ80とのどちらが、その車両の車載ネットワークで受信されたフレームについての情報の加工処理を行うこととしても良いし、車両内のサーバ及び異常検知サーバ80の双方が、加工処理を任意の配分で分担することとしても良い。

【0170】

(5) 上記実施の形態では、車両のゲートウェイ90は、不正フレームか否かに拘わらず受信したフレームについての情報を含むログ情報を異常検知サーバ80に送信することとした。しかし、車両のゲートウェイ90は、不正フレームであることを検知してエラーフレームを送信する場合においては、その不正フレームについての情報（特徴ベクトル等）を、異常検知サーバ80に送信しないこととしても良い。

【0171】

(6) 上記実施の形態では、異常検知サーバ80が、カーメーカ、ECUベンダのコン

10

20

30

40

50

コンピュータ等といった装置に対してアラート通知を示す情報等を送信する制御を行い得ることを示した。このアラート通知は任意の送信先に送信して良い。例えば、異常検知サーバ80は、アラート通知等の送信用情報を、ユーザが所有する情報端末等に送信しても良いし、複数のカーメーカに共通して利用され得るセキュリティプロバイダに送信しても良い。
【0172】

(7) 上記実施の形態では、異常検知サーバ80が統計的異常検知処理を行うことで、あるフレームの異常度を算定し、異常度が例えば異常ありの場合において、アラートレベルを決定することとした。この他に、異常検知サーバ80は、統計的異常検知処理に依らずに、予め定められたアルゴリズム等によって、そのフレームの異常度を算定し、異常度に応じて（例えば異常ありか否かに応じて）アラートレベルを決定する機能を有しても良い。例えば、そのフレームが、ファームウェア更新用のフレームについて予め規定されたメッセージIDを有するフレームであって、そのフレームが適切な更新時期以外においてCANバスに流れたことを確認した場合に、異常ありを示す異常度を算定してアラートレベルを決定してアラート通知等を行っても良いし、この場合においては攻撃予兆のフェーズ2に該当すると見做して攻撃フェーズ情報（図7参照）を用いてアラートレベルを決定しても良い。また、異常検知サーバ80は、統計的異常検知処理と、不正フレームの検知用の予め定められたルール又はアルゴリズムを用いて不正フレームを検知する処理とを併用することで、異常度の算定を行っても良く、この場合には、不正フレームと検知されたフレームについては、異常ありを示すように異常度の算定を行う。

【0173】

(8) 上記実施の形態で示した各種処理の手順（例えば図10、図11、図13、図15に示した手順等）の実行順序は、必ずしも、上述した通りの順序に制限されるものではなく、発明の要旨を逸脱しない範囲で、実行順序を入れ替えたり、複数の手順を並列に行ったり、その手順の一部を省略したりすることができる。

【0174】

(9) 上記実施の形態におけるゲートウェイその他のECUは、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置であることとしたが、ハードディスク装置、ディスプレイ、キーボード、マウス等のハードウェア構成要素を含んでも良い。また、異常検知サーバ80は、例えばプロセッサ、メモリ、通信インタフェース等を備えるコンピュータであることとしたが、ハードディスク装置、ディスプレイ、キーボード、マウス等のハードウェア構成要素を含んでも良い。また、上記実施の形態で示した各装置（ECU、異常検知サーバ80等）は、メモリに記憶された制御プログラムがプロセッサにより実行されてソフトウェア的に機能を実現する代わりに、専用のハードウェア（デジタル回路等）によりその機能を実現することとしても良い。

【0175】

(10) 上記実施の形態における各装置を構成する構成要素の一部又は全部は、1個のシステムLSI（Large Scale Integration：大規模集積回路）から構成されているとしても良い。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAM等を含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。また、上記各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又は全部を含むように1チップ化されても良い。また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現しても良い。LSI製造後に、プログラムすることが可能なFPGA（Field Programmable Gate Array）や、LSI内部の回路セルの接続や設定を再構成可能なリプログラマブル・プロセッサを利用しても良い。更には、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化

を行っても良い。バイオ技術の適用等が可能性としてあり得る。

【0176】

(11) 上記各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なICカード又は単体のモジュールから構成されているとしても良い。前記ICカード又は前記モジュールは、マイクロプロセッサ、ROM、RAM等から構成されるコンピュータシステムである。前記ICカード又は前記モジュールは、上記の超多機能LSIを含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ICカード又は前記モジュールは、その機能を達成する。このICカード又はこのモジュールは、耐タンパ性を有するとしても良い。

【0177】

(12) 本発明の一態様としては、例えば図10、図11、図13、図15等を示す処理手順の全部又は一部を含むセキュリティ処理方法であるとしても良い。例えば、セキュリティ処理方法は、一の車両（例えば車両1010a）の車載ネットワークで送信される異常なフレームに対処するためのセキュリティ処理方法であって、1つ又は複数の車両（例えば車両1010b等）の車載ネットワークにおいて受信された複数のフレームについての情報を取得し、その取得された複数のフレームについての情報に基づいて、その複数のフレームについての各車載ネットワークでの受信より後に、一の車両（例えば車両1010a）の車載ネットワークにおいて受信されたフレームの異常度を算定するセキュリティ処理方法である。このセキュリティ処理方法は、例えば、複数の車両（例えば車種Aの複数の車両）それぞれから、その車両の車載ネットワークにおいて受信された複数のフレームについての情報を、その複数の車両及び一の車両（例えば車両1010a）と通信可能な異常検知サーバ80が受信することにより、上述の取得を行う第1受信ステップ（例えば車種Aの複数の車両それぞれからフレームに係る特徴ベクトル等を受信するステップS112）と、一の車両から、一の車両の車載ネットワークにおいて受信されたフレームについての情報を、異常検知サーバ80が受信する第2受信ステップ（例えば車両1010aのゲートウェイ90からフレームに係る特徴ベクトル等を受信するステップS112）と、第1受信ステップで受信された、複数のフレームについての情報に基づいて、第2受信ステップで受信されたフレームについての情報に係るそのフレームの異常度の算定を行う算定ステップ（例えば統計的異常検知処理のステップS201）と、算定ステップで算定された異常度に応じて一の車両に送信すべき送信用情報の内容を決定する決定ステップ（例えば送信態様に関わるアラートレベルの決定のステップS203）と、決定ステップで決定された内容の送信用情報を一の車両に異常検知サーバ80が送信する送信ステップ（例えば送信のステップS204）とを含むこととしても良い。なお、算定ステップ及び決定ステップにおける処理（例えば異常に対応する不正検知用情報を送信用情報に含ませる場合における不正検知用情報の内容の特定等）については、例えばカーメーカ、ECUベンダその他の事業者等、或いは、その事業者等のコンピュータ等により実行しても良い。また、例えば、セキュリティ処理方法は、一の車両（例えば車両1010a）の車載ネットワークで送信される異常なフレームに対処するためのセキュリティ処理方法であって、一の車両の車載ネットワークにおいて受信されたフレームの異常度を算定し、算定した異常度に応じて、一の車両と所定関係を有する車両（例えば同一車種の車両、同種のECUを搭載する車両等）に対して送信用情報を送信するか否かを決定し、決定に従って送信用情報の送信の制御を行うセキュリティ処理方法である。また、本発明の一態様としては、このセキュリティ処理方法に係る処理をコンピュータにより実現するコンピュータプログラムであるとしても良いし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD（Blu-ray（登録商標）Disc）、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線

10

20

30

40

50

、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしても良い。また、本発明の一態様としては、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するものとしても良い。また、前記プログラム若しくは前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム若しくは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するものとしても良い。

【0178】

(13) 上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることで実現される形態も本発明の範囲に含まれる。

【産業上の利用可能性】

【0179】

本発明は、車載ネットワークで送信され得る多様な攻撃フレームに適切に対処するために利用可能である。

【符号の説明】

【0180】

- 10、20、30、40、50、60、70 バス（CANバス）
- 80 サーバ（異常検知サーバ）
- 81 ネットワーク
- 90、1020 ゲートウェイ
- 100、101、200、201、300、301、302、400、401、500
- 、600、700 電子制御ユニット（ECU）
- 110 エンジン
- 111 トランスミッション
- 210 ブレーキ
- 211 ステアリング
- 310 自動ブレーキ
- 311 車線維持装置
- 312 車車間通信装置
- 410 ドア
- 411 ライト
- 510 インストルメントパネル
- 610 ITS装置
- 710 診断ポート
- 810 通信部（取得部）
- 820 認証処理部
- 830 ログ収集処理部
- 840 ログ分析処理部（算定部）
- 850 セキュリティ情報生成部
- 860 車両情報DB
- 870 車両ログ格納DB
- 880 分析結果格納DB
- 890 セキュリティ情報DB
- 901 フレーム送受信部
- 902 フレーム解釈部
- 903 不正フレーム検知部
- 904 ルール保持部
- 905 フレーム生成部
- 906 転送制御部

10

20

30

40

50

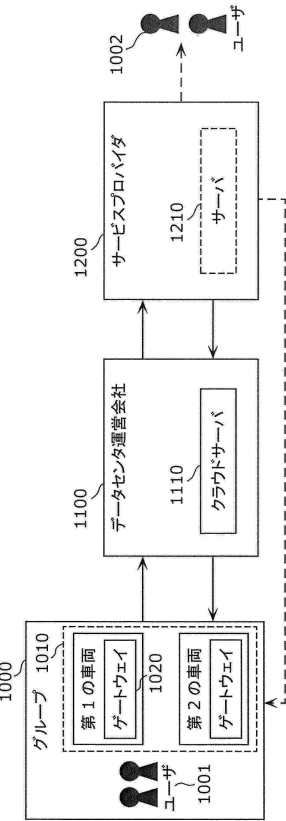
- 9 0 7 転送ルール保持部
- 9 2 0 鍵処理部
- 9 2 1 鍵保持部
- 9 3 0 不正検知通知部
- 9 4 0 更新処理部
- 9 5 0 フレームアップロード部
- 1 0 0 0 グループ
- 1 0 0 1、1 0 0 2 ユーザ
- 1 0 1 0、1 0 1 0 a、1 0 1 0 b、1 0 1 0 c、1 0 1 0 d、1 0 1 0 e、1 0 1 0

f 車両

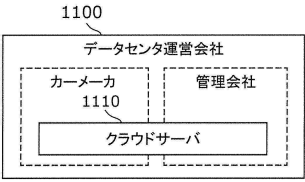
- 1 1 0 0 データセンタ運営会社
- 1 1 1 0、2 0 3 0 クラウドサーバ
- 1 2 0 0 サービスプロバイダ
- 1 2 1 0 サーバ
- 2 0 1 0 アプリケーションプログラム（アプリケーション）
- 2 0 2 0 オペレーティングシステム（OS）

【図面】

【図 1 A】



【図 1 B】



10

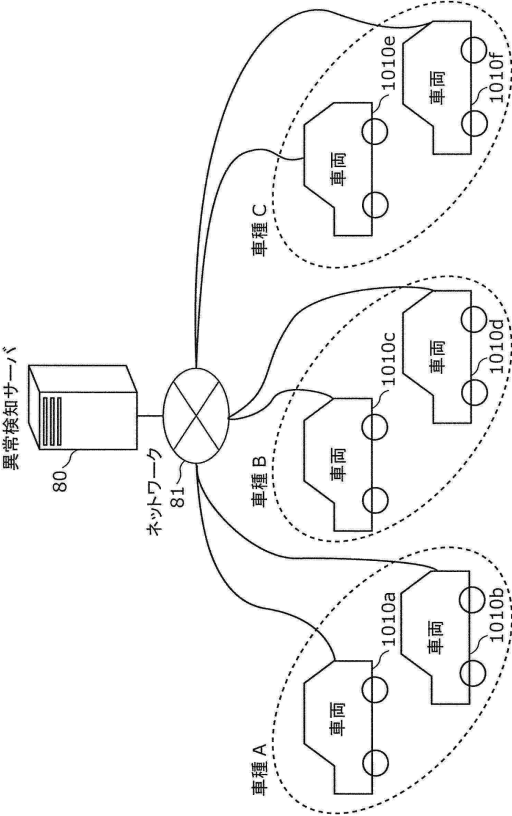
20

30

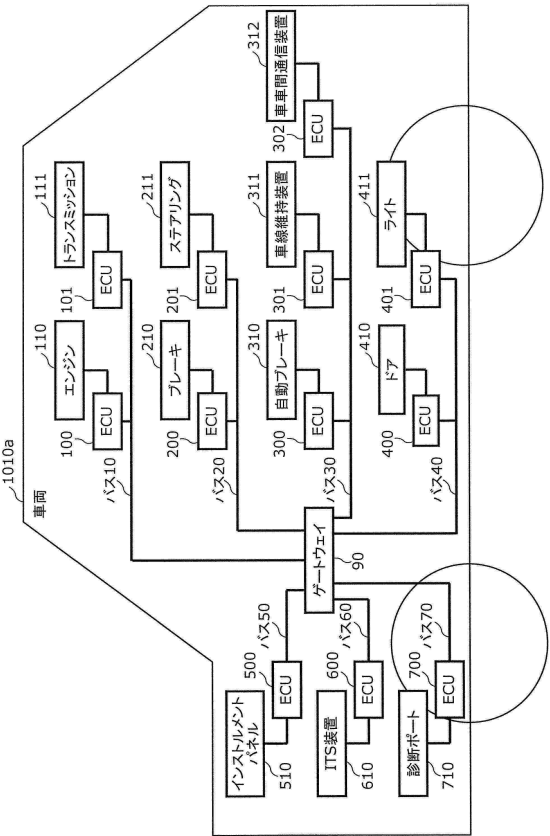
40

50

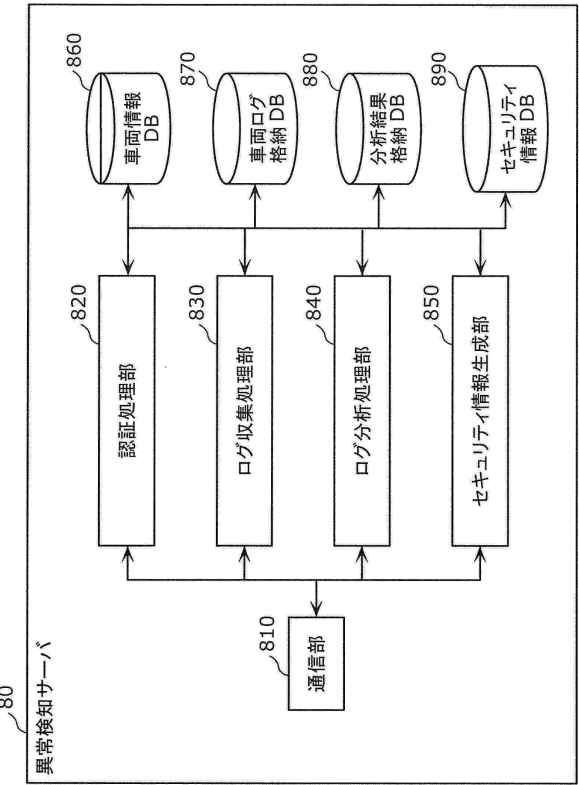
【図 2】



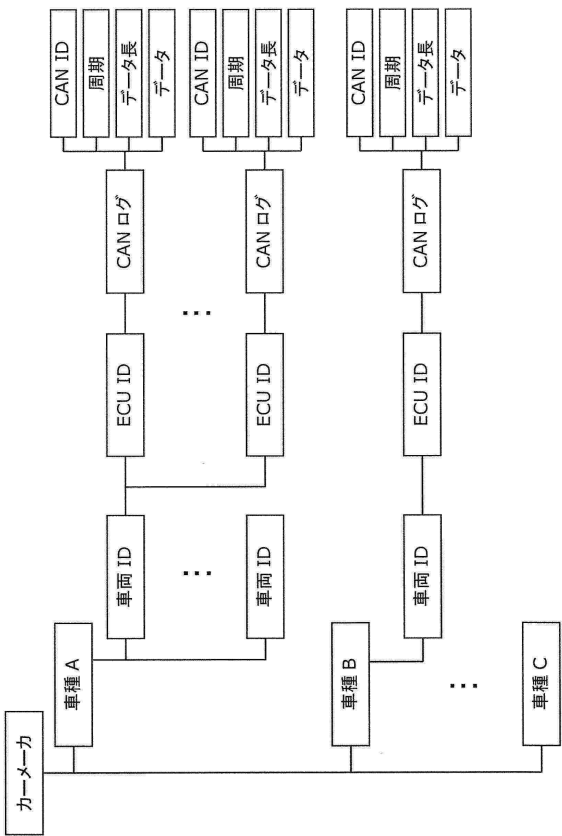
【図 3】



【図 4】



【図 5】



10

20

30

40

50

【図 6】

車両情報

車種	ECU ID	CAN ID
A	001	100
		101
	002	200
B	001	110
		111
	003	301
C	004	400
	005	500

【圖 7】

攻撃フェーズ情報

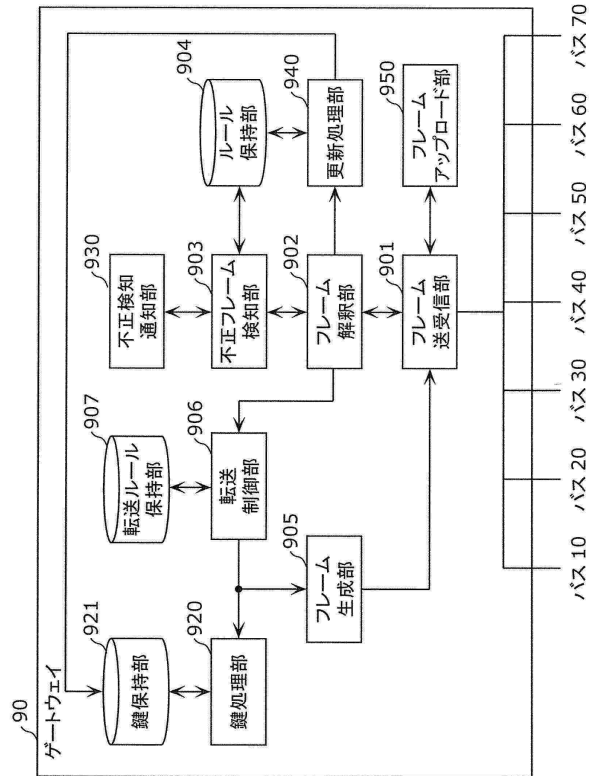
攻撃分類	攻撃フェーズ	観測される攻撃事象	検知数 N	アラートレベル
攻撃予兆	フェーズ 1	1 台の車でドライアンドブレー	-	1
	フェーズ 2	ECU 書き換え処理	1	2
			N>1	3
	フェーズ 3	車両識別情報の取得要求、 ECU 識別情報取得要求	1	3
			N>1	4
	攻撃	フェーズ 4	不正制御確認	1
		N>1		5

【図 8】

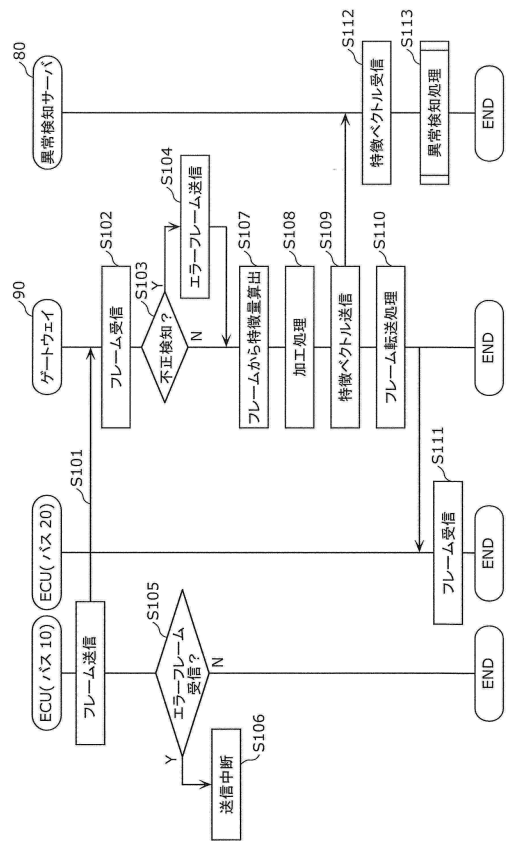
アラートレベル情報

アラートレベル	クラス A (攻撃予兆 / 攻撃を 報知した車両)	クラス B (攻撃予兆 / 攻撃報知車両と 同一車種の車両)	クラス C (攻撃予兆 / 攻撃報知 ECU を 持つ異なる車種の車両)
1	通知する (アラート)	通知しない	通知しない
2	即時通知する (アラート)	通知しない	通知しない
3	即時通知する (アラート)	即時通知する (アラート)	通知する (アラート)
4	即時通知する (アラート & 制御情報)	通知しない	通知しない
5	即時通知する (アラート & 制御情報)	即時通知する (アラート)	即時通知する (アラート)

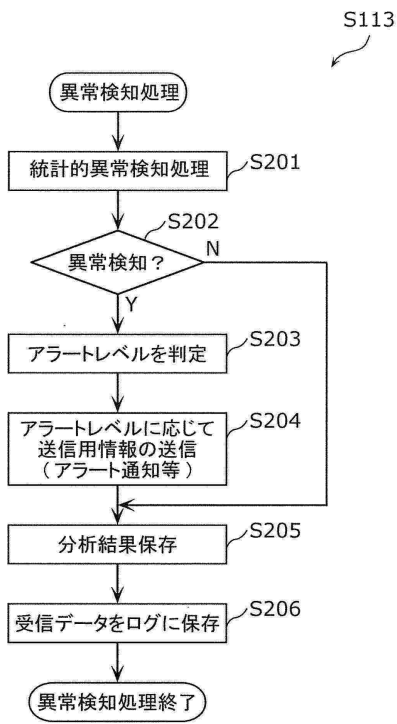
【図 9】



【図 10】



【図 11】



【図 12 A】

アラートレベル情報

累積検知台数 N	アラートレベル
1	1
2	2
$2 < N \leq 10$	3
$10 < N \leq 100$	4
$100 < N \leq 1000$	5
$1000 < N \leq 10000$	6

【図 12 B】

アラートレベル情報

単位時間当たりの検知台数 N	アラートレベル
1	1
2	2
$2 < N \leq 10$	3
$10 < N \leq 100$	4
$100 < N \leq 1000$	5
$1000 < N \leq 10000$	6

10

20

30

40

50

【図 1 2 C】

アラートレベル情報

2 つの攻撃検知間の距離 D (km)	アラートレベル
D>500	1
200<D≤500	2
200<D≤500	3
100<D≤200	4
10<D≤100	5
D≤10	6

【図 1 2 D】

アラートレベル情報

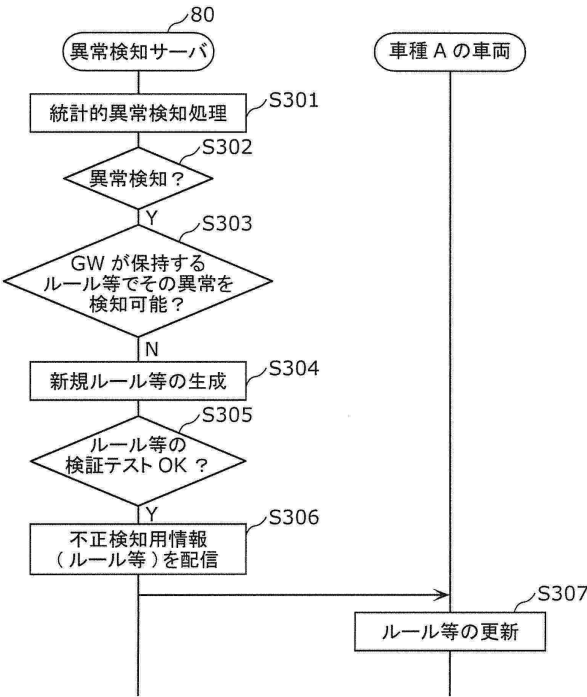
CAN ID	アラートレベル
301,302,303	1
101,102	2
201,202	3
401,402	4
501,502	5
601,602,701	6

【図 1 2 E】

アラートレベル情報

異常度	アラートレベル
1	1
2	2
3 ~ 4	3
5 ~ 10	4
11 ~ 20	5
21 ~	6

【図 1 3】



10

20

30

40

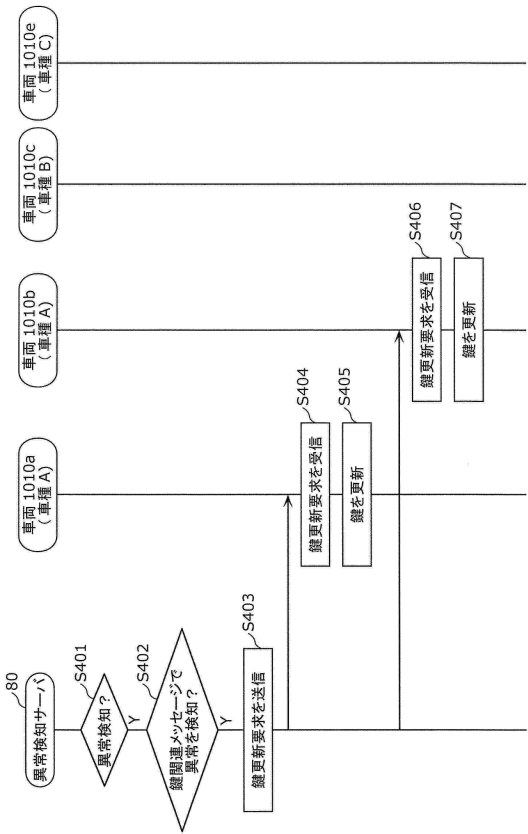
50

【図 1 4】

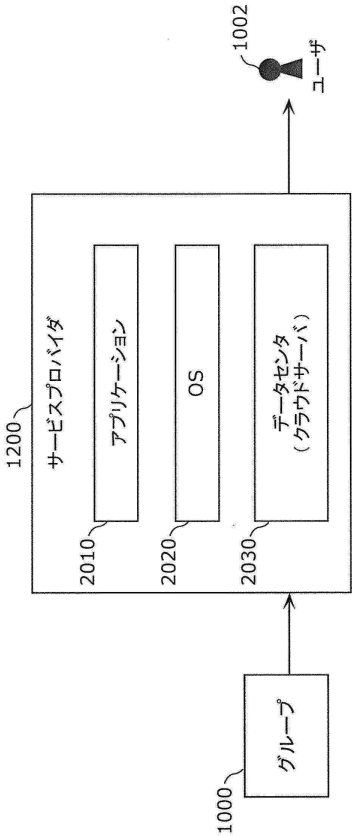
MAC/ 暗号化保護対象メッセージ ID リスト

車種	ECU ID	CAN ID	MAC 対応	暗号化
A	001	100	Y	N
		101	N	Y
	002	200	Y	N
B	001	110	N	Y
		111	Y	Y
	003	301	N	Y
C	004	400	N	Y
	005	500	N	Y

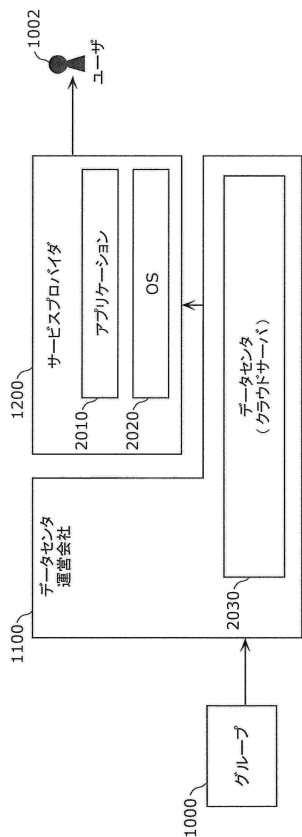
【図 1 5】



【図 1 6】



【図 1 7】



10

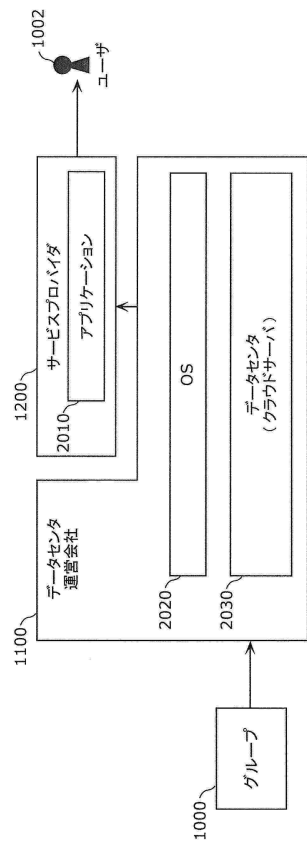
20

30

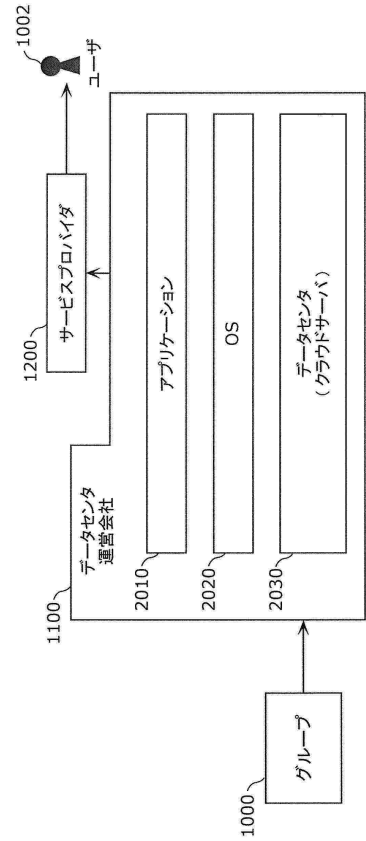
40

50

【図 18】



【図 19】



10

20

30

40

50

フロントページの続き

- (72)発明者 芳賀 智之
大阪府門真市大字門真１００６番地 パナソニックホールディングス株式会社内
- (72)発明者 松島 秀樹
大阪府門真市大字門真１００６番地 パナソニックホールディングス株式会社内
- (72)発明者 前田 学
大阪府門真市大字門真１００６番地 パナソニックホールディングス株式会社内
- (72)発明者 氏家 良浩
大阪府門真市大字門真１００６番地 パナソニックホールディングス株式会社内
- (72)発明者 岸川 剛
大阪府門真市大字門真１００６番地 パナソニックホールディングス株式会社内
- (72)発明者 鶴見 淳一
大阪府門真市大字門真１００６番地 パナソニックホールディングス株式会社内
- (72)発明者 安齋 潤
神奈川県横浜市都筑区池辺町４２６１番地 パナソニックオートモーティブシステムズ株式会社内
- 審査官 三森 雄介
- (56)参考文献 国際公開第２００９／０３８０２８（ＷＯ，Ａ１）
特開２０１５－１３６１０７（ＪＰ，Ａ）
国際公開第２０１５／１７０４５３（ＷＯ，Ａ１）
国際公開第２０１５／１５９５２０（ＷＯ，Ａ１）
- (58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５５