(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7197638号
(P7197638)

(45)発行日　令和4年12月27日(2022.12.27)

(24)登録日　令和4年12月19日(2022.12.19)

(51)国際特許分類
G06F 21/55 (2013.01)

FI
G06F 21/55

請求項の数　4　（全46頁）

(21)出願番号　特願2021-109868(P2021-109868)
(22)出願日　令和3年7月1日(2021.7.1)
(62)分割の表示　特願2018-150171(P2018-150171)の分割
原出願日　平成28年10月13日(2016.10.13)
(65)公開番号　特開2021-152977(P2021-152977A)
(43)公開日　令和3年9月30日(2021.9.30)
審査請求日　令和3年7月1日(2021.7.1)
(31)優先権主張番号　62/268,116
(32)優先日　平成27年12月16日(2015.12.16)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　514136668
パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ
Panasonic Intellectual Property Corporation of America
アメリカ合衆国 90504 カリフォルニア州，トーランス，スイート 450，ウエスト 190ストリート 2050
(74)代理人　100109210
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、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、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、

セキュリティ処理方法。

【請求項２】

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、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３】

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、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４】

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、

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、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、

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。

【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。

【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。

【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

【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。

【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。

【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。

【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。

【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。

【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。

【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。
【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。
【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。
【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。
【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。

【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。

【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】

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。

【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。

【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の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。

【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。

【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。

【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、例えばカーメーカ、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。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）と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。

【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。

【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。

【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。

【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。

【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 Diagnostics２）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。

【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、次回の分析処理（フレームの異常度の算定等）に利用する。

【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）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の内容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に脆弱性が見つかれば、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を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ーシ系の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と、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とを比較することで、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。

【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、カーメーカ、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。

【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。

【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１ｂｉｔずつ受信し、フレーム解釈部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

、１ｂｉｔ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（特定のための情報）を列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づ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－ＭＡ
Ｃ（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へと伝えると、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。

【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）。
【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。
【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。

【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。

【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て利用しても良い。

【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。

【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ベンダ等に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。

【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。
【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）。
【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。
【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）。
【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。

【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。

【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。

【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。

【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）。

【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）。

【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、カーメーカ、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（例えばカーメーカ、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】

（サービスの類型２：ＩａａＳ利用型クラウドサービス）

図１７は、サービスの類型２（ＩａａＳ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、ＩａａＳ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動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。

【０１５９】

本類型では、データセンタ運営会社１１００が、データセンタ（クラウドサーバ）２０３０を運営及び管理している。また、サービスプロバイダ１２００は、ＯＳ２０２０及びアプリケーション２０１０を管理する。サービスプロバイダ１２００は、サービスプロバイダ１２００が管理する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。

【０１６０】
（サービスの類型３：ＰａａＳ利用型クラウドサービス）
図１８は、サービスの類型３（ＰａａＳ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、ＰａａＳ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動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。
【０１６１】
本類型では、データセンタ運営会社１１００は、ＯＳ２０２０を管理し、データセンタ（クラウドサーバ）２０３０を運営及び管理している。また、サービスプロバイダ１２００は、アプリケーション２０１０を管理する。サービスプロバイダ１２００は、データセンタ運営会社１１００が管理するＯＳ２０２０及びサービスプロバイダ１２００が管理するアプリケーション２０１０を用いてサービスを提供する。
【０１６２】
（サービスの類型４：ＳａａＳ利用型クラウドサービス）
図１９は、サービスの類型４（ＳａａＳ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、ＳａａＳとは、ソフトウェア・アズ・ア・サービスの略である。ＳａａＳ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使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。
【０１６３】
本類型では、データセンタ運営会社１１００は、アプリケーション２０１０を管理し、ＯＳ２０２０を管理し、データセンタ（クラウドサーバ）２０３０を運営及び管理している。また、サービスプロバイダ１２００は、データセンタ運営会社１１００が管理する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。
【０１６４】
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１２００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。
【０１６５】
（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。
【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いても良い。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いても良い。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コンフィギュラブル・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等に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、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。

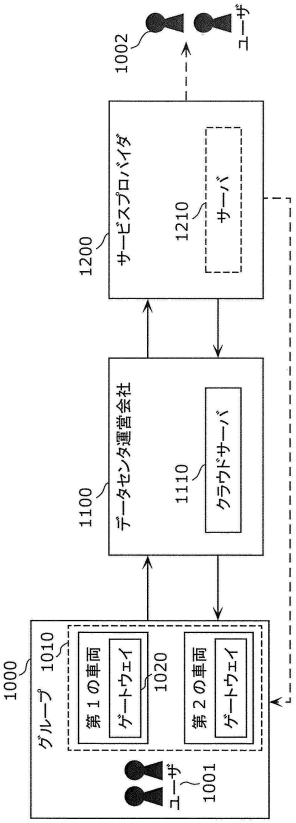
【産業上の利用可能性】

【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
９０７　転送ルール保持部
９２０　鍵処理部
９２１　鍵保持部
９３０　不正検知通知部
９４０　更新処理部
９５０　フレームアップロード部
１０００　グループ
１００１、１００２　ユーザ
１０１０、１０１０ａ、１０１０ｂ、１０１０ｃ、１０１０ｄ、１０１０ｅ、１０１０ｆ　車両
１１００　データセンタ運営会社
１１１０、２０３０　クラウドサーバ

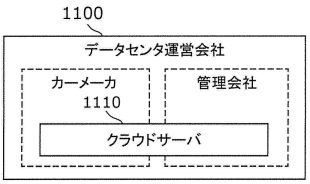
１２００　サービスプロバイダ
１２１０　サーバ
２０１０　アプリケーションプログラム（アプリケーション）
２０２０　オペレーティングシステム（ＯＳ）

【図面】

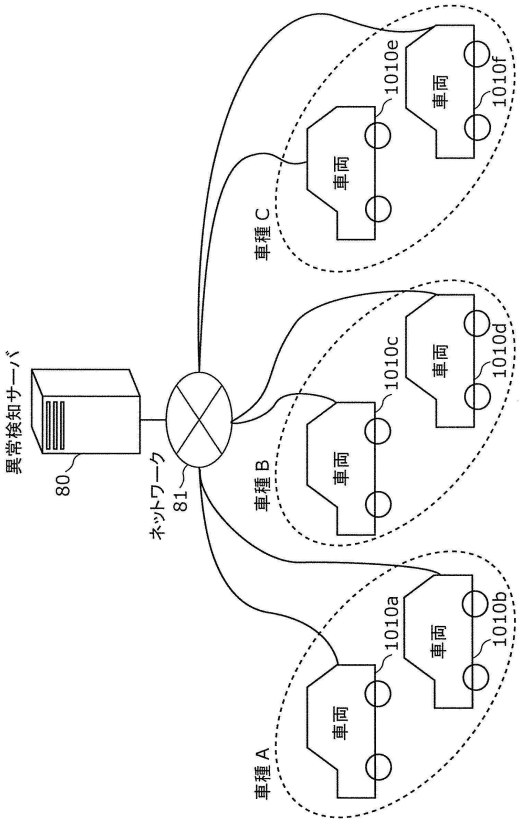
【図１Ａ】



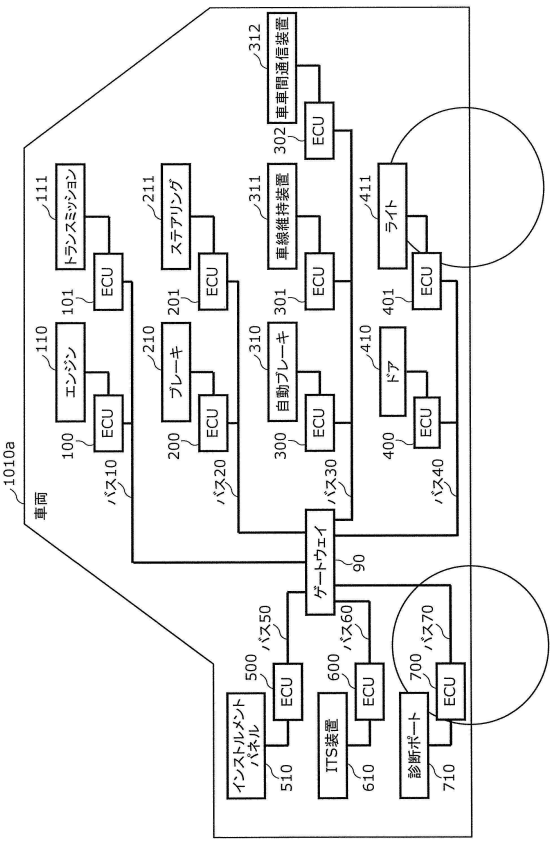
【図１Ｂ】



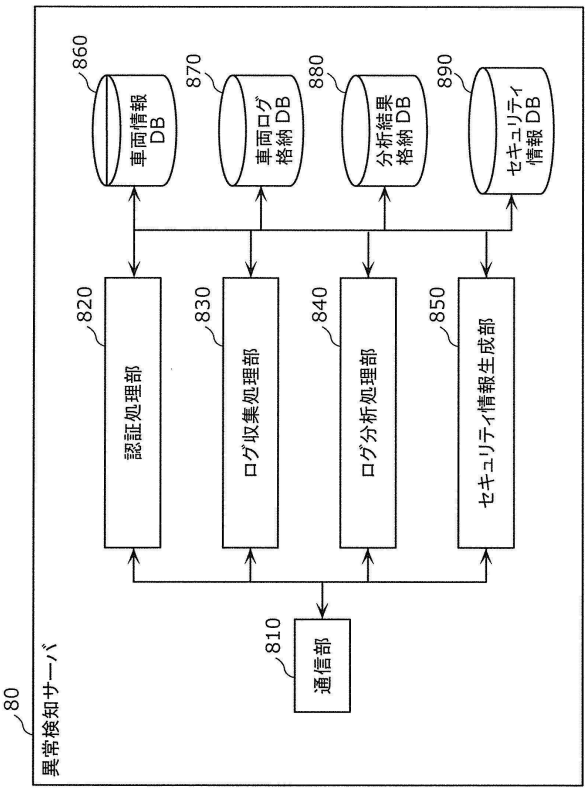
【図２】


異常検知サーバ
80
ネットワーク
81
車種 A
車種 B
車種 C
車両
1010a
1010b
1010c
1010d
1010e
1010f

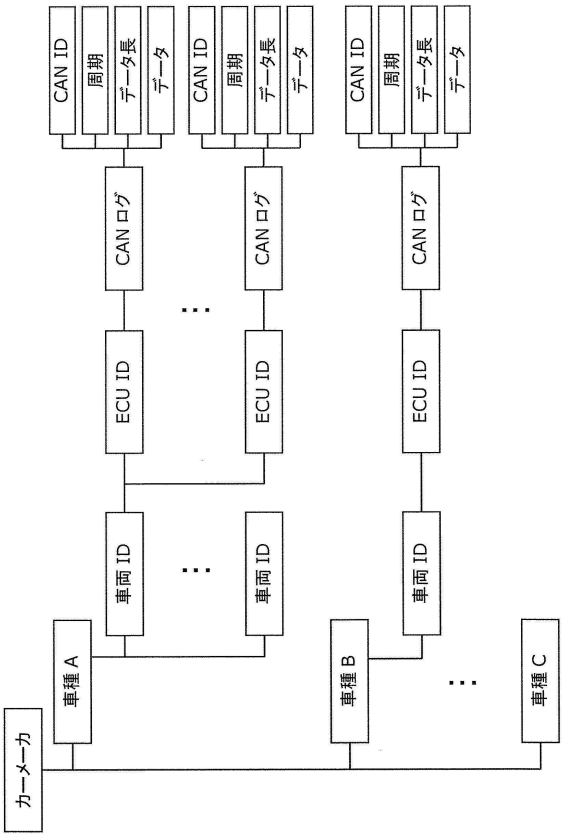
【図３】


1010a
車両
ゲートウェイ
90
バス10
バス20
バス30
バス40
バス50
バス60
バス70
ECU
エンジン
ブレーキ
自動ブレーキ
ドア
トランスミッション
ステアリング
車線維持装置
ライト
車車間通信装置
インストルメントパネル
ITS装置
診断ポート

【図４】


80
異常検知サーバ
通信部
認証処理部
ログ収集処理部
ログ分析処理部
セキュリティ情報生成部
車両情報 DB
車両ログ格納 DB
分析結果格納 DB
セキュリティ情報 DB

【図５】


カーメーカ
車種 A
車種 B
車種 C
車両 ID
ECU ID
CAN ログ
CAN ID
周期
データ長
データ

【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

【図７】

攻撃フェーズ情報

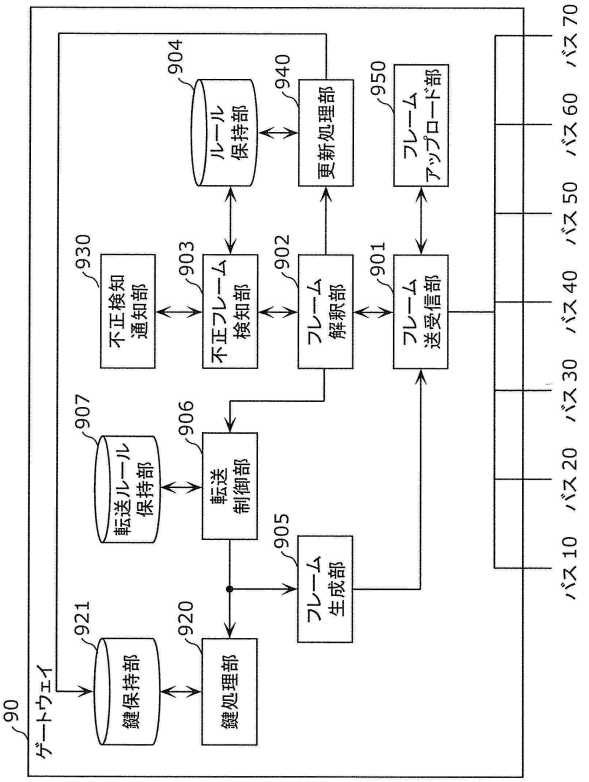
攻撃分類	攻撃フェーズ	観測される攻撃事象	検知数 N	アラートレベル
攻撃予兆	フェーズ 1	1 台の車でトライアンドエラー	-	1
	フェーズ 2	ECU 書き換え処理	1	2
			N>1	3
	フェーズ 3	車両識別情報の取得要求、ECU 識別情報取得要求	1	3
			N>1	4
攻撃	フェーズ 4	不正制御確認	1	4
			N>1	5

【図８】

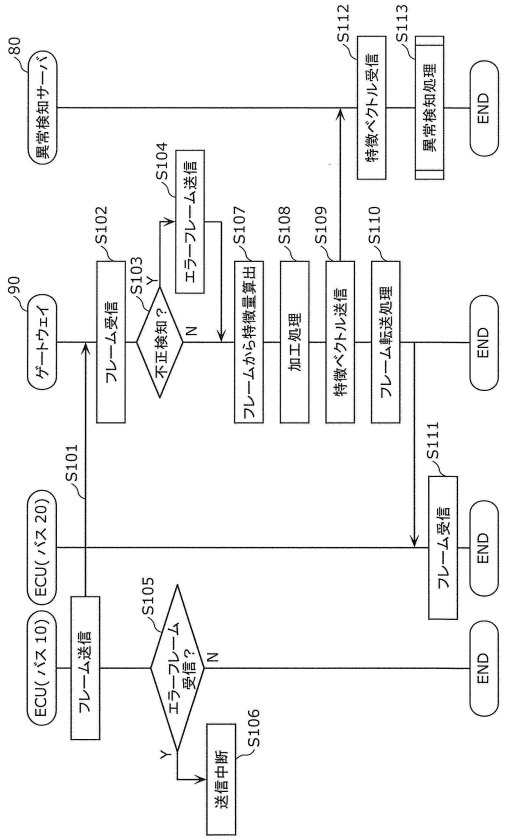
アラートレベル情報

アラートレベル	クラス A（攻撃予兆 / 攻撃を観測した車両）	クラス B（攻撃予兆 / 攻撃観測車両と同一車種の車両）	クラス C（攻撃予兆 / 攻撃観測 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）

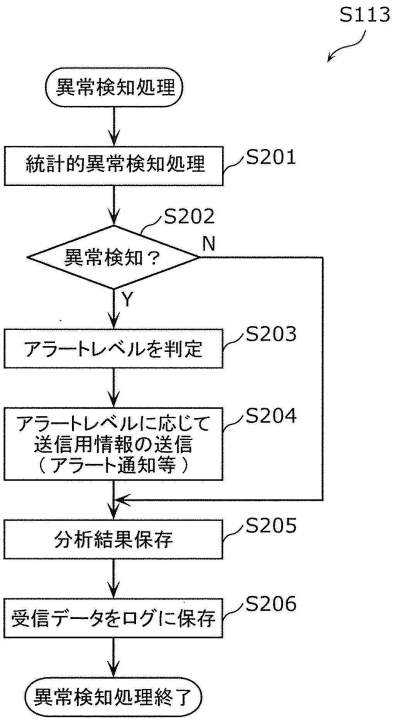
【図９】



【図１０】



【図１１】



【図１２Ａ】

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≦10	3
10<N≦100	4
100<N≦1000	5
1000<N≦10000	6

【図１２Ｂ】

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≦10	3
10<N≦100	4
100<N≦1000	5
1000<N≦10000	6

【図１２Ｃ】

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１２Ｄ】

アラートレベル情報

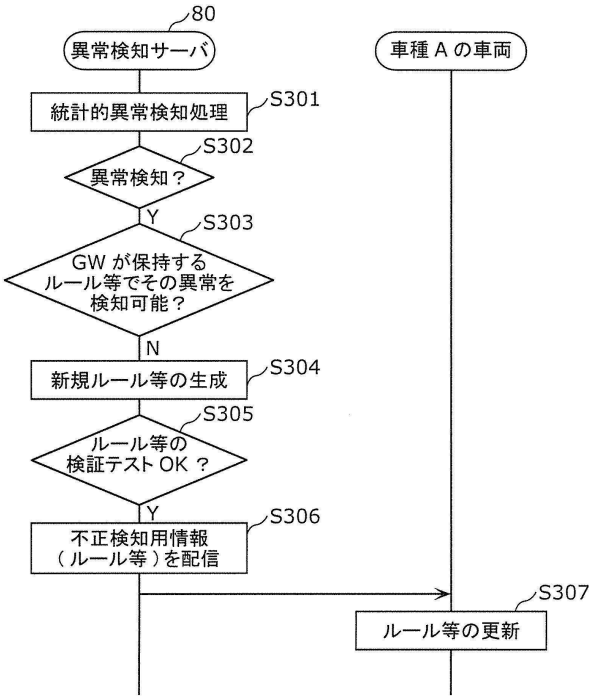
CAN ID	アラートレベル
301,302,303	1
101,102	2
201,202	3
401,402	4
501,502	5
601,602,701	6

【図１２Ｅ】

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１３】

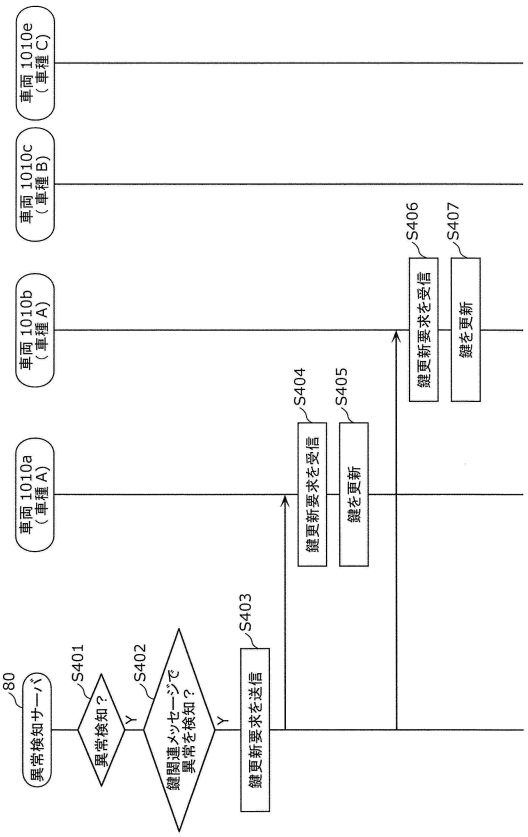


【図１４】

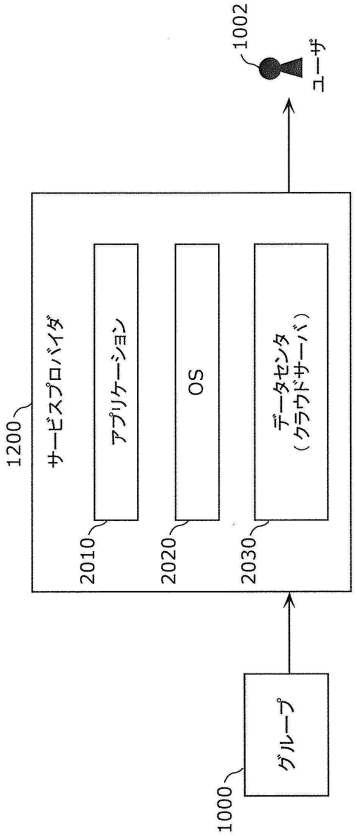
MAC/ 暗号化保護対象メッセージ ID リスト

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

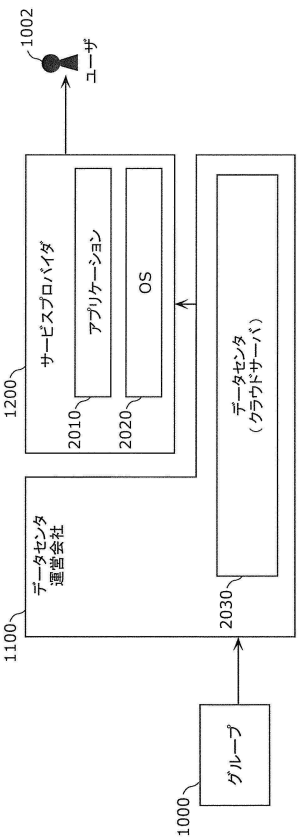
【図１５】



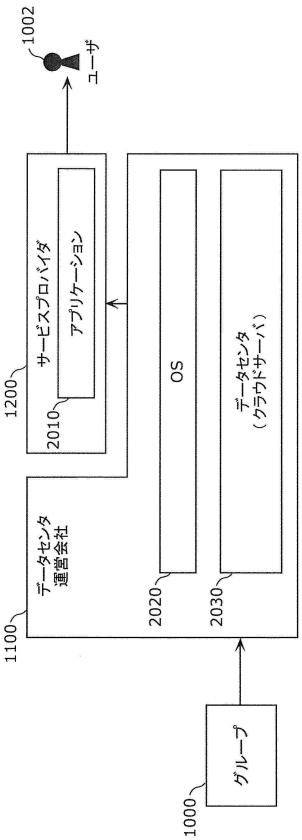
【図１６】



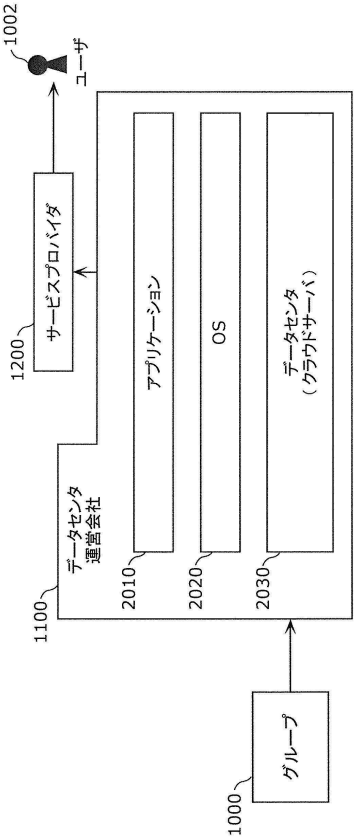
【図１７】



【図１８】


1002
ユーザ
1200
サービスプロバイダ
2010
アプリケーション
OS
2020
データセンタ
（クラウドサーバ）
2030
1100
データセンタ
運営会社
グループ
1000

【図１９】


1002
ユーザ
1200
サービスプロバイダ
アプリケーション
2010
OS
2020
データセンタ
（クラウドサーバ）
2030
1100
データセンタ
運営会社
グループ
1000

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 パナソニック株式会社内
(72)発明者　安齋 潤
大阪府門真市大字門真１００６番地 パナソニック株式会社内
審査官　打出 義尚
(56)参考文献　特開２０１７－１１１７９６（ＪＰ，Ａ）
特開２０１５－１３６１０７（ＪＰ，Ａ）
国際公開第２００９／０３８０２８（WO，Ａ１）
特開２０１５－２１４１６９（ＪＰ，Ａ）
特開２００９－２９４００４（ＪＰ，Ａ）
特開２０１３－１３１０５５（ＪＰ，Ａ）
国際公開第２０１５／１５９５２０（WO，Ａ１）
米国特許出願公開第２０１１／０２５８０４４（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５