(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2021年3月4日(04.03.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/039523 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号： PCT/JP2020/031228

(22) 国際出願日： 2020年8月19日(19.08.2020)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
PCT/JP2019/034263 2019年8月30日(30.08.2019) JP

(71) 出願人: 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**) [US/US]; 90503 カリフォルニア州トーランス, スイート ２００, マリナー アベニュー ２００００ California (US).

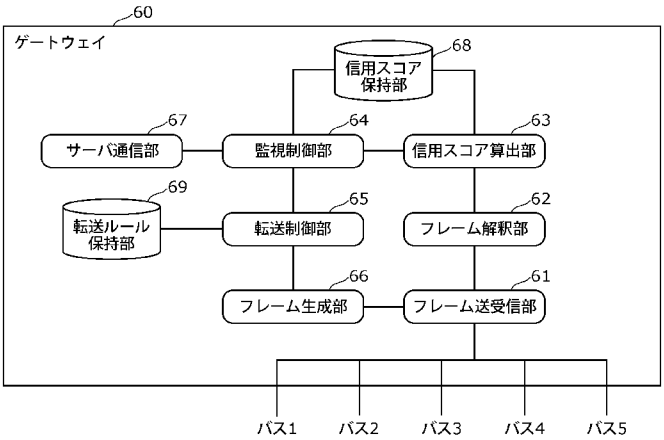
(72) 発明者: 岸 川 剛 (**KISHIKAWA, Takeshi**); 〒5718501 大阪府門真市大字門真１００６番地 パナソニック株式会社内 Osaka (JP). 平 野 亮 (**HIRANO, Ryo**). 氏 家 良 浩 (**UJIIE, Yoshihiro**). 芳賀 智之(**HAGA, Tomoyuki**).

(74) 代理人: 新 居 広 守, 外 (**NII, Hiromori** et al.); 〒5320011 大阪府大阪市淀川区西中島５丁目３番１０号タナカ・イトーピア新大阪ビル６階新居国際特許事務所内 Osaka (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) **Title:** VEHICLE MONITORING DEVICE AND VEHICLE MONITORING METHOD

(54) 発明の名称： 車両監視装置および車両監視方法



1, 2, 3, 4, 5 Bus
60 Gateway
61 Frame transmission/reception unit
62 Frame interpretation unit
63 Trust score calculation unit
64 Monitoring control unit
65 Forwarding control unit
66 Frame generation unit
67 Server communication unit
68 Trust score retention unit
69 Forwarding rule retention unit

(57) **Abstract:** A vehicle monitoring device in a vehicle onboard network system provided with one or more electronic control units, said vehicle monitoring device comprising: a frame transmission/reception unit (61) that receives frames passing through the vehicle onboard network system; and a trust score calculation unit (63) that, on the basis of a frame received by the frame transmission/reception unit (61) and vehicle data including information regarding one or more frames received by the frame transmission/reception unit (61) prior to receiving said frame, detects suspicious behavior differing from normal driving behavior, and on the basis of the detection result, calculates a trust score indicating the possibility that reverse engineering is being performed on a vehicle (200) that has the vehicle onboard network system installed therein.

WO 2021/039523 A1

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一　国際調査報告（条約第21条(3)）

(57) 要約：車両監視装置は、１以上の電子制御ユニットを備える車載ネットワークシステムにおける車両監視装置であって、前記車載ネットワークシステムに流れるフレームを受信するフレーム送受信部（６１）と、フレーム送受信部（６１）で受信したフレームと当該フレームの受信より前にフレーム送受信部（６１）で受信した１以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、検知結果に基づいて車載ネットワークシステムを搭載する車両（２００）に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出部（６３）とを備える。

明　細　書

発明の名称 ： 車両監視装置および車両監視方法

技術分野

[0001]　本開示は、１以上の電子制御ユニット（以下、ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ））によって構成される車載ネットワークシステムを監視する車両監視装置および車両監視方法に関する。

背景技術

[0002]　近年、自動車の中のシステムには、ＥＣＵ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が、その中でも最も主流な車載ネットワークの一つに、Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（以降、ＣＡＮ（登録商標、以下同様））という規格が存在する。また、さらに、自動運転またはコネクテッドカーの普及に伴い、車載ネットワークのトラフィックの増大に対応するため車載Ｅｔｈｅｒｎｅｔ（登録商標、以下同様）の普及が進んでいる。

[0003]　一方で、車載ネットワークに侵入し、車両を不正制御する脅威も報告されている。このような脅威に対して、非特許文献１には、従来のＩｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ（ＩＰ）通信で用いられてきた暗号通信を用いて不正なノードの通信による不正制御を防ぐ方法が開示されている。また、特許文献１には、車載ネットワークの異常な通信を検知し、不正なフレームを遮断する方法が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特許第５６６４７９９号公報

非特許文献

[0005] 非特許文献1：ＲＦＣ５４０６：Ｇｕｉｄｅｌｉｎｅｓ　ｆｏｒ　Ｓｐｅｃｉｆｙｉｎｇ　ｔｈｅ　Ｕｓｅ　ｏｆ　ＩＰｓｅｃ　Ｖｅｒｓｉｏｎ２、２０

０９年２月

発明の概要

発明が解決しようとする課題

[0006] しかしながら、非特許文献１の方法では、暗号通信を用いるため、送受信ノードによる暗号化・復号処理が必要となりオーバーヘッドが発生する。また、暗号通信に用いる鍵管理が重要となり、ＥＣＵの制御を奪われ、正規の鍵を利用された場合に、不正なフレーム送信による不正制御が可能となってしまう。

[0007] また、特許文献１の方法は、攻撃者によって不正なフレームが送信されたときの対処方法であり、攻撃の発生を未然に防ぐわけではない。このように、車載ネットワークの安全性には、改善の余地がある。

[0008] そこで、本開示は、車載ネットワークの安全性をより高めることができる車両監視装置および車両監視方法を提供する。

課題を解決するための手段

[0009] 本開示の一態様に係る車両監視装置は、１以上の電子制御ユニットを備える車載ネットワークシステムを監視する車両監視装置であって、前記車載ネットワークシステムに流れるフレームを受信するフレーム受信部と、前記フレーム受信部で受信した前記フレームと当該フレームの受信より前に前記フレーム受信部で受信した１以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、検知結果に基づいて前記車載ネットワークシステムを搭載する車両に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出部と、を備える。

[0010] 本開示の一態様に係る車両監視方法は、１以上の電子制御ユニットを備える車載ネットワークシステムを監視する車両監視方法であって、前記車載ネットワークシステムに流れるフレームを受信する受信ステップと、前記受信ステップで受信した前記フレームと当該フレームの受信より前に受信した１以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動

とは異なる不審挙動を検知し、検知結果に基づいて前記車載ネットワークシステムを搭載する車両に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出ステップとを含む。

発明の効果

[0011] 本開示の一態様に係る車両監視装置等によれば、車載ネットワークの安全性をより高めることができる。

図面の簡単な説明

[0012] [図1]図１は、実施の形態１における車載ネットワークシステムの全体構成を示す図である。

[図2]図２は、実施の形態１におけるＥＣＵの構成を示す図である。

[図3]図３は、実施の形態１におけるゲートウェイの構成を示す図である。

[図4A]図４Ａは、実施の形態１における信用スコアの一例を示す図である。

[図4B]図４Ｂは、実施の形態１における車両データの一例を示す図である。

[図5]図５は、実施の形態１における転送ルールの一例を示す図である。

[図6]図６は、実施の形態１におけるゲートウェイの処理を示すフローチャートである。

[図7]図７は、実施の形態１におけるゲートウェイの信用スコア算出のフローチャートである。

[図8]図８は、実施の形態１におけるゲートウェイの監視レベル変更のフローチャートである。

[図9]図９は、実施の形態１におけるゲートウェイの動作シーケンスを示す図である。

[図10]図１０は、実施の形態１におけるゲートウェイの動作シーケンスを示す図である。

[図11A]図１１Ａは、実施の形態１における運転者へ通知する表示内容の一例を示す図である。

[図11B]図１１Ｂは、実施の形態１における運転者へ通知する表示内容の別の一例を示す図である。

[図12]図１２は、実施の形態２におけるゲートウェイの処理を示すフローチャートである。

[図13]図１３は、実施の形態２におけるゲートウェイの不審スコア算出のフローチャートである。

[図14]図１４は、実施の形態２におけるゲートウェイの監視レベル変更のフローチャートである。

発明を実施するための形態

[0013] （本開示に至った経緯）

本開示の実施の形態等の説明に先立ち、本開示の基礎に至った経緯について説明する。

[0014] 上記のように、特許文献１および非特許文献１に開示されている技術では、車載ネットワークの安全性を高める観点から改善の余地がある。

[0015] 一般に、車両の不正制御を試みる攻撃者は、車両の不正制御を引き起こすためのフレームの調査等のリバースエンジニアを車載ネットワークに対して事前に行うことで攻撃方法を確立させていくことが想定される。

[0016] 車両の不正制御を実施する前の車載ネットワークの調査段階における攻撃者の活動を把握することができれば、攻撃発生の予兆として、攻撃者によるリバースエンジニアリングを妨害する、または、対象車両を重点的に監視し攻撃内容を未然に把握する等のアクションにつなげることができる。

[0017] そこで、本願発明者らは、車載ネットワークの調査段階における攻撃者の活動を把握することができる車両監視装置等について鋭意検討を行い、以下に説明する車両監視装置等を創案した。例えば、本願発明者らは、車載ネットワークにおけるフレームを監視し、攻撃者のリバースエンジニアによって発生する通常とは異なる車両の挙動を捉え、車両がリバースエンジニアをされている可能性を算出することで、車載ネットワークの調査段階における攻撃者の活動を把握することができることを見出した。

[0018] 本開示の一実施態様の車両監視装置は、１以上の電子制御ユニットを備える車載ネットワークシステムを監視する車両監視装置であって、前記車載ネ

ットワークシステムに流れるフレームを受信するフレーム受信部と、前記フレーム受信部で受信した前記フレームと当該フレームの受信より前に前記フレーム受信部で受信した１以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、検知結果に基づいて前記車載ネットワークシステムを搭載する車両に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出部と、を備える。

[0019] これにより、車載ネットワークシステムをリバースエンジニアリングしている疑わしさ（信用スコア）を算出することが可能となり、より疑わしい車両を把握することができ効果的である。つまり、車両監視装置は、信用スコアに基づいて、車両の不正制御を実施する前の車載ネットワークに対する調査段階における攻撃者の活動を把握することができるので、車両の車載ネットワークの安全性をより高めることができる。

[0020] また、前記不審挙動は、監視装置の接続、エラーフレーム、ネットワークの瞬断、バッテリー取り外しのいずれかが検知された場合に、パッシブモニタリング活動として検知され、前記信用スコア算出部は、前記パッシブモニタリング活動が検知された場合に、前記信用スコアを減少させるとしてもよい。

[0021] これにより、攻撃者が、車載ネットワークシステムのログを取得しようとする試行を捉えることが可能となり、効果的である。つまり、車両監視装置は、信用スコアに基づいて、パッシブモニタリング活動を把握することができるので、車両の車載ネットワークの安全性をより高めることができる。

[0022] また、前記不審挙動は、所定の第１時間内における、車内のボタンの操作回数、異常な運転挙動の検知回数のいずれかが所定数以上である、または、運転支援機能の発動間隔が所定値未満である場合に、アクティブモニタリング活動として検知され、前記運転支援機能は、自動駐車支援、オートクルーズコントロール、緊急ブレーキ、レーンキープアシストのいずれかであり、前記異常な運転挙動は、アクセル開度、ブレーキ圧、所定時間内における操

舵角の変化量が所定値以上であることであり、前記信用スコア算出部は、前記アクティブモニタリング活動が検知された場合に、前記信用スコアを減少させるとしてもよい。

[0023] これにより、攻撃者が、不正制御を行うためのヒントを得るための車載ネットワークログを積極的に取得しようとする活動を捉えることが可能となり効果的である。つまり、車両監視装置は、信用スコアに基づいて、アクティブモニタリング活動を把握することができるので、車両の車載ネットワークの安全性をより高めることができる。

[0024] また、前記不審挙動は、所定の第１時間内における、前記フレームの受信量、診断コマンドの受信量のいずれかが所定数以上である場合に、インジェクション活動として検知され、前記信用スコア算出部は、前記インジェクション活動が検知された場合に、前記信用スコアを減少させるとしてもよい。

[0025] これにより、攻撃者が、車載ネットワークに対して、何らかのフレーム注入を試行する活動を捉えることが可能となり効果的である。つまり、車両監視装置は、信用スコアに基づいて、インジェクション活動を把握することができるので、車両の車載ネットワークの安全性をより高めることができる。

[0026] また、前記不審挙動は、所定の第１時間内における、アップデートコマンドの受信量、同一属性のフレームの受信量のいずれかが所定数以上である場合に、リファインメント活動として検知され、前記同一属性のフレームとは、前記フレームに含まれる識別子、ＩＰアドレス、ＭＡＣアドレス、ポート番号のいずれか、または、いずれか２つ以上の組み合わせが同一であるフレームであり、前記信用スコア算出部は、前記リファインメント活動が検知された場合に、前記信用スコアを減少させるとしてもよい。

[0027] これにより、攻撃者が車両の不正制御を実現するために、より洗練された攻撃を試行していることを捉えることが可能となり効果的である。つまり、車両監視装置は、信用スコアに基づいて、リファインメント活動を把握することができるので、車両の車載ネットワークの安全性をより高めることができる。

[0028] また、前記車両監視装置は、さらに、監視レベル変更部を備え、前記監視レベル変更部は、前記信用スコアが所定の値未満となった場合に、前記信用スコアの値に基づいて、前記車両の機能の制限、前記車両の運転者への注意喚起、近隣車両またはサーバへの信用スコアの通知、および、前記車載ネットワークシステムの監視強化のいずれか１つ以上を実行するとしてもよい。

[0029] これにより、攻撃者によるリバースエンジニアリング活動の疑わしさが高い車両を重点的に監視することが可能となり効率的である。また、監視レベル変更部によれば、信用スコアの値に基づいて各種対応を行うので、リバースエンジニアリングが行われている場合に、攻撃者がリバースエンジニアリングを継続して行うことを抑制する効果が期待できる。

[0030] また、前記不審挙動は、前記リバースエンジニアリングの各段階を示す複数の種類を有し、前記信用スコア算出部は、前記不審挙動の前記複数の種類のそれぞれにおいて信用スコアを算出するとしてもよい。

[0031] これにより、攻撃者のリバースエンジニアリング活動のフェーズごとに不審挙動の疑わしさを把握することが可能となり、効果的である。つまり、車両監視装置は、複数の種類の信用スコアに基づいて、車両の不正制御を実施する前の車載ネットワークに対する調査段階における攻撃者の活動の段階（フェーズ）を把握することができるので、車両の車載ネットワークの安全性をさらに高めることができる。

[0032] また、前記不審挙動の前記複数の種類は、パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動、リファインメント活動の少なくとも２つを含み、前記パッシブモニタリング活動は、前記車両データを取得するための行動であり、前記アクティブモニタリング活動は、前記車両の特定機能動作中または特定状況における前記車両データを取得しようとするための動作であり、前記インジェクション活動は、前記車載ネットワークシステムへのフレームの注入を試行するための行動であり、前記リファインメント活動は、前記車載ネットワークシステムに注入されるフレームの精度を向上させるためのフレームの注入を試行するための行動であってもよ

い。

[0033] これにより、攻撃者のリバースエンジニアリング活動の段階が、パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動およびリファインメント活動の少なくとも２つのうちのいずれの活動であるかを把握することができる。つまり、車両監視装置は、現在行われているリバースエンジニアリング活動の段階をより詳細に取得することができるので、車両の車載ネットワークの安全性をさらに高めることができる。

[0034] また、前記不審挙動は、監視装置の接続、エラーフレーム、ネットワークの瞬断、バッテリー取り外しのいずれかが検知された場合に、前記パッシブモニタリング活動として検知され、所定の第１時間内における、運転支援機能の発動回数、車内のボタンの操作回数、異常な運転挙動の検知回数、のいずれかが所定数以上である場合に前記アクティブモニタリング活動として検知され、所定の第１時間内における、前記フレームの受信回数、診断コマンドの受信回数のいずれかが所定数以上である場合に前記インジェクション活動として検知され、所定の第１時間内における、アップデートコマンドの受信回数、同一属性のフレームの受信回数のいずれかが所定数以上である場合に前記リファインメントとして検知される。

[0035] これにより、信用スコアを算出するための専用の情報を用いることなく、攻撃者のリバースエンジニアリング活動の段階を取得することができる。つまり、車両監視装置は、より簡単に攻撃者のリバースエンジニアリング活動の段階を取得することができる。

[0036] また、前記車両監視装置は、さらに、監視レベル変更部を備え、前記監視レベル変更部は、前記不審挙動の前記複数の種類と、前記不審挙動の前記複数の種類のそれぞれに対応する信用スコアの値とに基づいて、前記車両の一部機能の制限、前記車両の運転者への注意喚起、および、近隣車両またはサーバへの信用スコアの通知のいずれか１つ以上を実行するとしてもよい。

[0037] これにより、攻撃者のリバースエンジニアリング活動のフェーズに応じた対応が可能となり、車載ネットワークの安全性向上に効果的である。

[0038] また、前記信用スコア算出部は、所定の第２時間が経過するまたは前記車両に対して所定の第１操作が実行されると、前記信用スコアを上昇させてもよい。また、前記信用スコア算出部は、所定の第３時間が経過するまたは前記車両に対して所定の第２操作が実行されると、前記信用スコアをリセットさせてもよい。

[0039] これにより、信用スコア算出部は、信用スコアを回復させることが可能となる。車両の運転者（攻撃者ではない通常の運転者）により信用スコアが低下する運転が行われた場合に、信用スコアを自動で補正することができる。よって、車両監視装置は、車載ネットワークに対する調査段階における攻撃者の活動を、より確実に把握することができる。

[0040] また本開示の一実施態様の車両監視方法は、１以上の電子制御ユニットを備える車載ネットワークシステムを監視する車両監視方法であって、前記車載ネットワークシステムに流れるフレームを受信する受信ステップと、前記受信ステップで受信した前記フレームと該フレームの受信より前に受信した１以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、検知結果に基づいて前記車載ネットワークシステムを搭載する車両に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出ステップとを含む。

[0041] これにより、上記の車両監視装置と同様の効果を奏する。例えば、車両監視方法によれば、車載ネットワークシステムをリバースエンジニアリングしている疑わしさを算出することが可能となり、より疑わしい車両を把握することができ効果的である。

[0042] 以下、図面を参照しながら、本開示の実施の形態に関わる車載ネットワーク異常検知システムについて説明する。なお、以下で説明する実施の形態は、いずれも本開示の好ましい一具体例を示す。つまり、以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置および接続形態、ステップ、ステップの順序などは、本開示の一例であり、本開示を限定する主旨ではない。本開示は、請求の範囲の記載に基づいて特定される。したがっ

て、以下の実施の形態における構成要素のうち、本開示の最上位概念を示す独立請求項に記載されていない構成要素は、本開示の課題を達成するために必ずしも必要ではないが、より好ましい形態を構成する構成要素として説明される。

[0043] 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。また、各図において、実質的に同一の構成に対しては同一の符号を付し、重複する説明は省略または簡略化される場合がある。

[0044] （実施の形態１）

以下、複数の電子制御ユニット（ＥＣＵ）が通信する車載ネットワーク（車載ネットワークシステム）を搭載した車両における、車両監視装置および車両監視方法について説明する。より具体的には、車載ネットワークシステムに流れるフレームに基づいて、攻撃者がリバースエンジニアリングを実施することによる車両挙動の不正度を表す信用スコアを算出し、算出した信用スコアに応じて車両の監視機能を変更する車載ネットワークセキュリティ技術について説明する。

[0045] ［１．１　車載ネットワークシステムの全体構成］

図１は、本実施の形態における車載ネットワークシステムの全体構成を示す図である。図１に示すように、車載ネットワークシステムは、ＥＣＵ１０、１１、２０、２１、３０、３１、４０、４１と、診断ポート５０と、ゲートウェイ６０とを備える。

[0046] ＥＣＵ１０とＥＣＵ１１とはバス１に接続し、ＥＣＵ２０とＥＣＵ２１とはバス２に接続し、ＥＣＵ３０とＥＣＵ３１とはバス３に接続し、ＥＣＵ４０とＥＣＵ４１とはバス４に接続している。また、診断ポート５０は、バス５に接続している。ゲートウェイ６０は、全てのバスに接続している。

[0047] 各ＥＣＵは、互いにＣｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＣＡＮ）で接続されており、フレームの通信を行う。各バスは、例えば車両２００の機能ごとにドメイン分離されていてもよい。例えばバス１は、パワートレイン系のＥＣＵが配置されており、エンジンの制御等に関わる通信が

行われる。また、例えば、バス２、はシャシー系のＥＣＵが配置されており、ステアリングの制御またはブレーキ制御を実現するための通信が行われる。また、バス３は、情報系のＥＣＵが配置されており、カーナビやインフォテインメント系の通信が行われる。また、バス４は、ボディ系のＥＣＵが配置され、搭乗者のボタン押下によるエアコン制御またはパワーウインドウ等の制御を行うための通信が行われる。

[0048] ゲートウェイ６０は、全てのバスの情報を受信し、必要であれば受信したフレームを、他のバスへ転送する処理を行う。例えばバス５に、診断用のフレームが流れていた場合には、当該フレームをバス１～４に転送する処理等を行う。ゲートウェイ６０は、車両監視装置の一例である。ゲートウェイ６０は、１以上のＥＣＵによって構成される車載ネットワークシステムにおける処理等を行う。

[0049] なお、本実施の形態では、各バスはＣＡＮで実現されているとしたが、通信プロトコルはこれに限らない。例えば、ＣＡＮ－ＦＤ（ＣＡＮ ｗｉｔｈ Ｆｌｅｘｉｂｌｅ Ｄａｔａ Ｒａｔｅ））、ＦｌｅｘＲａｙ（登録商標、以下同様）、Ｅｔｈｅｒｎｅｔであってもよいし、バスごとに通信プロトコルが異なっていても構わない。

[0050] ［１．２ ＥＣＵ１０の構成］

図２は、本実施の形態におけるＥＣＵ１０の構成を示す図である。なお、ＥＣＵ１１、ＥＣＵ２０、ＥＣＵ２１、ＥＣＵ３０、ＥＣＵ３１、ＥＣＵ４０、ＥＣＵ４１は、ＥＣＵ１０と同様の構成であるが、それぞれ接続されるセンサまたはアクチュエータが異なるので、実現する機能が異なる。

[0051] ＥＣＵ１０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る。図２に示すように、ＥＣＵ１０は、通信部１００とホスト部１０１とを有する。

[0052] 通信部１００は、バス１に接続し、バス１に流れるフレームの送受信を行う。通信部１００は、車載ネットワークシステムに流れるフレームを送受信するとも言える。通信部１００は通信コントローラまたはトランシーバ等に

よって実現される。

[0053] ホスト部１０１は、ＥＣＵ１０のメイン処理を行う部分であり、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）とメモリとによって実現される。ホスト部１０１は、通信部１００から受信したフレームを解釈し、通信内容（解釈結果）に応じた処理を実施する。例えばＥＣＵ１０は、エンジン制御を行うＥＣＵであるとする。クルーズコントロールの機能で車両速度の増加要求フレームを他のＥＣＵから受信した場合に、所望の車両速度となるように、当該ＥＣＵ１０のホスト部１０１は、エンジン回転数を上昇させる制御等を行う。また、ＥＣＵ１０がエンジン回転数の情報を受信した場合に、当該ＥＣＵ１０のホスト部１０１は、他のＥＣＵへ通知するためにフレームを送信する等の処理を行う。

[0054] ［１．３ ゲートウェイ６０の構成］

図３は、本実施の形態におけるゲートウェイ６０の構成を示す図である。ゲートウェイ６０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る。

[0055] 図３に示すように、ゲートウェイ６０は、フレーム送受信部６１と、フレーム解釈部６２と、信用スコア算出部６３と、監視制御部６４と、転送制御部６５と、フレーム生成部６６と、サーバ通信部６７と、信用スコア保持部６８と、転送ルール保持部６９とを有する。

[0056] フレーム送受信部６１は、バス１～５と接続される通信インタフェースであり、通信コントローラまたはトランシーバ等によって実現される。フレーム送受信部６１は、各バスで受信したフレームをフレーム解釈部６２へ転送する。また、フレーム送受信部６１は、フレーム生成部６６からの送信要求に従って、フレームの送信を行う。フレーム送受信部６１は、フレーム受信部の一例である。

[0057] フレーム解釈部６２は、フレーム送受信部６１から転送されたフレームの解釈を行い、フレームに応じた処理を行う。また、フレーム送受信部６１は、受信したフレームを、信用スコア算出部６３へ通知する。

[0058] 信用スコア算出部６３は、フレーム解釈部６２から通知されたフレームと、信用スコア保持部６８に保持されている車両情報（車両データ）とに基づいて、車両２００の信用スコアを算出し、信用スコア保持部６８に格納されている車両２００の信用スコアおよび車両情報を更新する。

[0059] 信用スコア算出部６３は、車両２００が通常とは異なる利用をされている度合いを信用スコアとして算出する。信用スコア算出部６３は、特に攻撃者が車両２００をリバースエンジニアリングする目的で活動している兆候を捉えるために信用スコアを算出する。

[0060] 信用スコアは、例えば、リバースエンジニアリングが行われている可能性（例えば、攻撃者がリバースエンジニアリングしている疑わしさ）を示す指標である。また、信用スコアは、例えば、リバースエンジニアリングが行われている可能性を判定可能な指標である。また、信用スコアは、例えば、通常の運転者であれば行わない、または、行う可能性が低い車両２００における利用が行われていることを示す指標であるとも言える。なお、本明細書におけるリバースエンジニアリングは、車載ネットワークシステムを解析することである。よって、信用スコアは、例えば、車両２００の車載ネットワークシステムの解析が行われている可能性、または、解析の度合いを示す指標であるとも言える。

[0061] 本実施の形態では、信用スコア算出部６３は、フレーム送受信部６１で受信したフレームと当該フレームの受信より前にフレーム送受信部６１で受信した１以上のフレームに関する車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、不審挙動の検知結果に基づいて車載ネットワークシステムを搭載する車両２００に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する。信用スコア算出部６３は、フレーム送受信部６１で受信したフレームと車両データとに基づいて、当該フレームを受信する前の信用スコアを更新するとも言える。

[0062] このように、信用スコア算出部６３は、フレーム送受信部６１で受信したフレームを含むフレームの時系列データに基づいて信用スコアを算出する。

信用スコア算出部６３は、例えば、現在受信したフレームと、現在より過去に受信したフレーム（車両データに含まれるフレーム）とに基づいて現在の信用スコアを算出する。

[0063] なお、通常の運転挙動とは、リバースエンジニアリングを行わない運転者が車両２００を運転するときに行い得ると想定される運転挙動である。また、ここでの運転挙動には、車両２００の走行時における運転状態の挙動（例えば、後述する図４Ｂに示す緊急ブレーキ発動間隔など）、および、車両２００の内部処理における挙動（例えば、後述する図４Ｂに示すエラーフレーム発生間隔など）の両方が含まれる。また、以下において、どのような不審挙動のときに信用スコアを減少させるかを例示するが、不審挙動は以下に限定されない。

[0064] 例えば、イグニッションがかかっている時間に対して、停車している時間の割合が高いことは、停車中の車両２００に対して、何らかの調査が行われている兆候とも考えられるため、信用スコア算出部６３は、信用スコアを減少させる。

[0065] また、数秒から数分といった短時間で、車両２００の運転支援機能（例えば、緊急ブレーキ、クルーズコントロール、自動駐車支援などのいずれか１つ以上）が繰り返し利用される場合も、攻撃者により、不正制御を引き起こすフレームを解析するために、車載ネットワークのログ取得が行われている可能性があるので、信用スコア算出部６３は、信用スコアを減少させる。また、運転支援機能には、レーンキープアシスト機能（車線逸脱防止支援機能）が含まれていてもよい。

[0066] また、車両２００の極端な運転状態（例えば、急アクセル、急ブレーキ、急ハンドルなど）の検知間隔が短い場合、または、エアコン、ライト等のボディ系を制御するために車内に配置されたボタンが繰り返し押下されている場合も、攻撃者により、車載ネットワーク解析のためのログ取得が行われている可能性があるので、信用スコア算出部６３は、信用スコアを減少させる。

[0067] また、車載ネットワークにおいてエラーフレームが発生する間隔が短い場合も、攻撃者によって不正なデバイスが接続されている影響が表れている可能性があるので、信用スコア算出部６３は、信用スコアを減少させる。

[0068] また、車載ネットワークのフレームが瞬断される時間が所定期間（例えば数秒程度）発生する場合も、攻撃者によって、車載ネットワークをロギングするためのデバイス、または、不正なフレームを注入するためのデバイスを接続する作業が行われている可能性があるので、信用スコア算出部６３は、信用スコアを減少させる。

[0069] また、車載ネットワークに流れる診断コマンドが所定量以上である場合は、攻撃者によって、診断コマンド注入時の車両２００への影響調査、または、攻撃試行の影響で生じた故障コードの消去作業が繰り返し行われている可能性があるので、信用スコア算出部６３は、信用スコアを減少させる。

[0070] 他にも、アップデートを行うためのフレーム数、バッテリーの電圧低下またはバッテリーの取り外しが行われる頻度、通常観測されないＩＰアドレスまたはポート番号を含むパケット数などに応じて、信用スコア算出部６３は、信用スコアを減少させうる。

[0071] 上記の信用スコアを減少させる状況は、必ずしも攻撃者による活動とは限らない。そのため、信用スコア算出部６３は、算出した信用スコアを不揮発メモリに保持しておき、所定の時間（所定の第２時間の一例）が経過すると（例えば１日おきに）信用スコアを所定値（例えば１）ずつ上昇させてもよい。信用スコア算出部６３は、信用スコアを回復させる処理も行うことで、信用スコアを減少させる活動が繰り返し観測される車両２００を適切に検出するようにしてもよい。なお、信用スコア算出部６３は、車両２００に対して所定の操作（所定の第１操作の一例）が実行されると信用スコアを所定値ずつ上昇させてもよい。所定の第１操作は、例えば、イグニッションＯＮする操作であってもよいし、その他の操作であってもよい。

[0072] 信用スコア算出部６３は、受信したフレームを監視制御部６４に通知する。

[0073] 監視制御部６４は、信用スコア保持部６８に保持されている信用スコアに基づいて、通知されたフレームに対する処理を決定する。監視制御部６４は、例えば、リバースエンジニアリングに対する監視のレベルを示す監視レベルを、信用スコアに基づいて変更する。監視制御部６４は、監視レベル変更部の一例である。

[0074] 信用スコアが、所定の閾値よりも高い場合、通知されたフレームに対して特に何も行わず、信用スコア算出部６３は、通知されたフレームを転送制御部６５へ通知する。

[0075] 信用スコアが、所定の閾値以下の場合、縮退モードに入るために、監視制御部６４は、通知されたフレームの破棄、または、転送制御部６５への縮退モード通知フレームの通知などを行う。縮退モード通知フレームは、他のＥＣＵへ縮退モードに入ることを示す通知を行うためのフレームを送信することを示す通知である。また、信用スコアが減少してきたことを通知するために、監視制御部６４は、車両ログ（車両データ）と信用スコアとをサーバ通信部６７へ通知する。ここで、車両ログは、車載ネットワークで観測されたフレームの情報を含みうる。

[0076] 転送制御部６５は、通知されたフレームを転送ルール保持部６９に保持されている転送ルールに基づいて、転送を行うように、フレーム生成部６６へ通知する。

[0077] フレーム生成部６６は、転送制御部６５から通知されたフレームについての送信要求をフレーム送受信部６１に対して行う。

[0078] サーバ通信部６７は、監視制御部６４から通知された内容をサーバへ通知し、サーバからの通知を受け、監視制御部６４へ内容を通知する。

[0079] 信用スコア保持部６８は、車両２００の信用スコアと、信用スコアを算出するためのデータとが格納されている。信用スコア保持部６８に格納される情報の詳細は、図４Ａおよび図４Ｂを用いて後述する。

[0080] 転送ルール保持部６９は、フレームの転送に用いるルールが格納されている。転送ルールの詳細は、図５を用いて後述する。

[0081] なお、ゲートウェイ６０が有する各構成要素の一部または全部は、車両２００の外部の装置（例えば、サーバ装置）が有していてもよい。この場合、車両２００は、受信したフレームおよび車両データを外部の装置に送信する。外部の装置は、車両２００からのフレームおよび車両データに基づいて信用スコアを算出し、車両２００に送信する。

[0082] ［１．４　信用スコア保持部６８に格納される信用スコアおよび車両データの一例］

図４Ａは、本実施の形態における信用スコアの一例を示す図である。図４Ｂは、本実施の形態における車両データの一例を示す図である。信用スコアおよび車両データは、信用スコア保持部６８に格納されている。また、車両データは、信用スコアの算出に用いられてもよい。また、図４Ｂに示す項目は、不審挙動と判定されうる項目である。

[0083] 図４Ａにおいて、信用スコアは８０であることを示している。信用スコアは、０～１００の値をとり、初期値は１００である。つまり、図４Ａでは、初期値が１００である信用スコアが、挙動不審が検知されたことにより、８０まで減少している例を示している。なお、図４Ａに示す８０は、例えば、現在の信用スコアを示す。

[0084] また、図４Ｂの車両データにおいて、イグニッションがＯＮされてからのデータとして、今回値と前回値が格納されている。前回値は、前回にイグニッションがＯＮされてからＯＦＦとなるまでの期間のデータが格納されている。車両データとして、車両２００の速度が時速０キロである割合を示す停車時間割合、緊急ブレーキがＯＮになってから、次に緊急ブレーキがＯＮとなる間隔を示す緊急ブレーキ発動間隔、クルーズコントロール発動間隔、自動駐車支援発動間隔、アクセル開度が１００％を示すフレームを受信した間隔を示す急アクセル検知間隔、急ブレーキ検知間隔、急ハンドル検知間隔、エラーフレームを受信した間隔を示すエラーフレーム発生間隔、メッセージ瞬断時間、バッテリー電圧低下有無またはバッテリーの取り外しの有無、診断コマンド受信回数、アップデートコマンド受信回数、車内に存在するエア

コンまたはライト等を制御するボタンが単位時間内（例えば１分間）に押された回数を示すボタン連続押下回数、サードパーティ装置の接続の有無に関する情報が格納されている。なお、発動間隔は、発動する時間間隔を意味し、検知間隔は、検知する時間間隔を意味する。サードパーティ装置は、監視装置の一例である。また、上記の受信回数は、受信量の一例であり、ボタン連続押下回数は、操作回数の一例である。なお、受信量は受信回数に限定されず、データ量であってもよい。例えば、図４Ｂは、診断コマンド受信回数に代えて診断コマンドのデータ量（所定の第１時間におけるデータの合計量）であってもよい。

[0085] 図４Ｂでは、格納されている車両データとして、停車時間割合が今回は７０％であるのに対して、前回は５０％であったことを示している。また、緊急ブレーキ発動間隔は、今回が６０秒であるのに対して、前回は、「－」であり、今回は緊急ブレーキが２回以上発動していないことを示している。また、クルーズコントロールの発動間隔は、今回は、「－」であり、今回は２回以上発動していないことを示しているのに対して、前回は１０００秒間隔で発動していることを示している。また、自動駐車支援発動間隔は、今回が３０秒間隔で発動しているのに対して、前回は、「－」であり、２回以上自動駐車支援が発動していないことを示している。

[0086] 急アクセル検知間隔は、今回、前回ともに、「－」であり、２回以上の急アクセルを検知していないことを示している。同様に、急ブレーキ検知間隔、急ハンドル検知間隔についても、前回、今回ともに「－」であり、２回以上の該当フレームを受信していないことを示している。なお、急アクセル、急ブレーキおよび急ハンドルは、異常な運転挙動の一例である。

[0087] エラーフレーム発生間隔は、今回は１秒間隔であり、前回は「－」である。今回は、１秒間隔で該当フレームを受信しているのに対し、前回は、２回以上の該当フレームを受信していないことを示している。また、メッセージ瞬断時間は、今回は３秒であり、前回は、０秒（つまり１秒未満）であることを示している。

[0088] バッテリー電圧低下有無については、今回はバッテリー電圧低下を検知しており、前回はバッテリー電圧低下を検知していないことを示している。診断コマンド受信回数と、アップデートコマンド受信回数は前回、今回ともに０回であることを示している。

[0089] ボタン連続押下回数については、今回は３０回押されたのに対して、前回は３回であることを示している。

[0090] サードパーティ装置の接続の有無については、今回は接続されたのに対して、前回は接続されなかったことを示している。

[0091] なお、図４Ｂに示す時間間隔に関する項目（例えば、緊急ブレーキ発動間隔、急アクセル検知間隔など）は、所定の第１時間内の発動回数または検知回数であってもよい。また、図４Ｂに示す回数に関する項目（例えば、診断コマンドまたはアップデートコマンド受信回数、ボタン連続押下回数など）は、前回の受信時刻または押下時刻、および、今回の受信時刻または押下時刻に基づく時間間隔であってもよい。信用スコア算出部６３は、図４Ｂに示す項目における時間間隔または回数のいずれかを用いて信用スコアを算出すればよい。車両データには、例えば、車載ネットワークで観測された各項目におけるフレームの情報が含まれる。車両データには、例えば、フレームの受信時刻を示す時刻情報またはフレームの受信量を示す情報などが含まれる。車両データには、例えば、現在より前に（過去に）フレーム送受信部６１で受信した１以上のフレームに関する情報が含まれるとも言える。また、図４Ｂに示す車両データは、ログ情報の一例である。また、車両データを車両ログまたは車両情報とも記載する。

[0092] なお、本実施の形態では、信用スコアおよび車両データは平文で保持されているが、暗号化されて保持されていてもよい。

[0093] ［１．５　転送ルール保持部に格納される転送ルールの一例］

図５は、本実施の形態における転送ルールの一例である。転送ルール保持部６９は、同図に示すようにフレームのＩＤごとに、転送元および転送先が格納されたテーブル（転送ルール）を格納している。

[0094] 図５では、ＩＤが０ｘ１００のフレームの転送元はバス１であり、当該フレームは、バス２、３、４に転送されることを示している。同様にＩＤが０ｘ２００のフレームの転送元はバス２であり、バス３に転送されることを示しており、ＩＤが０ｘ２５０のフレームの転送元はバス２であり、バス４に転送されることを示しており、ＩＤが０ｘ３００のフレームの転送元はバス３であり、バス１に転送されることを示している。

[0095] ［１．６　ゲートウェイ６０の処理を示すフローチャート］

図６は、本実施の形態におけるゲートウェイ６０の処理を示すフローチャートである。

[0096] 図６に示すように、ゲートウェイ６０は、フレームを受信しているか否かを判定する（Ｓ１０）。

[0097] フレームを受信している場合（Ｓ１０でＹｅｓ）、ゲートウェイ６０は、信用スコアを算出する（Ｓ１１）。フレームを受信していない場合（Ｓ１０でＮｏ）、ゲートウェイ６０は、フレームを受信するまで待機する。

[0098] ゲートウェイ６０は、信用スコアを算出後、算出した信用スコアが所定値以下であるか否かを確認する（Ｓ１２）。監視制御部６４は、信用スコア算出部６３により算出された信用スコアが所定値以下であるか否かを判定する。

[0099] 信用スコアが所定値以下である場合（Ｓ１２でＹｅｓ）、ゲートウェイ６０は、監視レベルを変更し（Ｓ１３）、転送処理を実行する（Ｓ１４）。

[0100] 信用スコアが所定値よりも大きい場合（Ｓ１２でＮｏ）、ゲートウェイ６０は、監視レベルを変更せずに転送処理を実行する（Ｓ１４）。

[0101] 次に、ゲートウェイ６０の信用スコア算出部６３は、所定の時間が経過したか否かを判定する（Ｓ１５）。所定の時間は、例えば、前回ステップＳ１５でＹｅｓと判定してからの経過時間であるが、これに限定されず、信用スコアがリセットされてからの経過時間であってもよいし、信用スコアがリセットされてからの運転時間であってもよい。

[0102] 信用スコア算出部６３は、所定の時間経過した場合（Ｓ１５でＹｅｓ）、

信用スコアを１インクリメントする、または、信用スコアをリセットし（Ｓ１６）、処理を終了する。信用スコア算出部６３は、信用スコアを１インクリメントする場合、現在の信用スコアに１インクリメントした信用スコアを信用スコア保持部６８に格納する。また、信用スコア算出部６３は、信用スコアをリセットする場合、現在の信用スコアに関わらず、信用スコアの初期値（例えば、１００）を信用スコア保持部６８に格納する。

[0103] また、信用スコア算出部６３は、所定の時間経過していない場合（Ｓ１５でＮｏ）、信用スコアを変更せずに処理を終了する。

[0104] なお、ステップＳ１５の判定は、所定の時間に基づいて判定されることに限定されず、車両２００に対して所定の操作が実行されることにより行われてもよい。所定の操作は、例えば、ステップＳ１６の処理を実行することを示す操作（例えば、ボタンに対する操作）であってもよいし、イグニッションＯＮまたはＯＦＦする操作であってもよい。信用スコアをインクリメントするための操作は、所定の第１操作の一例であり、信用スコアをリセットするための操作は、所定の第２操作の一例である。

[0105] なお、信用スコアは、複数回インクリメントが行われた後に、リセットされてもよい。つまり、信用スコアがリセットされるときの時間（所定の第３時間の一例）は、信用スコアがインクリメントされるときの時間（所定の第２時間の一例）より長い時間であってもよい。

[0106] ［１．７　ゲートウェイ６０の信用スコア算出のフローチャート］

図７は、本実施の形態におけるゲートウェイ６０の信用スコア算出のフローチャートである。具体的には、図７は、図６のステップＳ１１の信用スコアを算出する処理の詳細を示すフローチャートである。なお、図７では、不審挙動として判定される項目が、診断コマンドまたはアップデートコマンドの受信回数、運転支援機能をＯＮするコマンドの受信間隔（例えば、緊急ブレーキの発動間隔）、および、急ブレーキ、急ハンドル、急アクセルの検知間隔である例について説明する。

[0107] 図７に示すように、ゲートウェイ６０は、受信したフレームが診断コマン

ドまたはアップデートコマンドであるか否かを確認する（Ｓ１１０１）。信用スコア算出部６３は、受信したフレームが診断コマンドまたはアップデートコマンドであるか否かを判定する。

[0108] 信用スコア算出部６３は、受信したフレームが診断コマンドまたはアップデートコマンドである場合（Ｓ１１０１でＹｅｓ）、該当コマンドの受信回数を更新する（Ｓ１１０２）。信用スコア算出部６３は、例えば、信用スコア保持部６８に格納されている該当コマンドの受信回数を１インクリメントする。

[0109] 次にゲートウェイ６０は、該当コマンドの受信回数が所定値以上（例えば１００回以上）であるか否かを判定する（Ｓ１１０３）。信用スコア算出部６３は、例えば、更新した当該コマンドの受信回数が、所定値以上であるか否かを判定する。ステップＳ１１０３の判定で用いる所定値は、信用スコア保持部６８に予め格納されている。

[0110] 所定の第１時間内における該当コマンドの受信回数が所定値以上である場合（Ｓ１１０３でＹｅｓ）、ゲートウェイ６０は、信用スコアを１デクリメントして（Ｓ１１０４）、処理を終了する。また、所定の第１時間内における該当コマンドの受信回数が所定値よりも小さい場合（Ｓ１１０３でＮｏ）、ゲートウェイ６０は、処理を終了する。つまり、信用スコア算出部６３は、該当コマンドの受信回数が所定値以上である場合、信用スコアを更新し、該当コマンドの受信回数が所定値よりも小さい場合、信用スコアの更新を行わない。なお、所定の第１時間は、例えば、ステップＳ１５の判定に用いた時間であってもよいし、図７に示す判定処理に用いられる専用の時間であってもよい。所定の第１時間は、例えば、信用スコア保持部６８に予め格納されている。また、図７の説明において使用する他の所定の第１時間においても同様である。

[0111] このように、信用スコア算出部６３は、不審挙動が、所定の第１時間内における診断コマンドまたはアップデートコマンドの受信回数のいずれかが所定数以上である場合に、信用スコアを減少させる。

[0112] また、信用スコア算出部６３は、所定の第１時間内における、診断コマンドの受信回数が所定数以上である場合に、当該不審挙動をインジェクション活動として検知し、インジェクション活動が検知された場合に、信用スコアを減少するとも言える。なお、インジェクション活動として検知される不審挙動は、診断コマンドの受信回数に限定されず、例えば、所定の第１時間内におけるフレームの受信回数であってもよい。

[0113] また、信用スコア算出部６３は、所定の第１時間内における、アップデートコマンドの受信回数が所定数以上である場合に、当該不審挙動をリファインメント活動として検知し、リファインメント活動が検知された場合に、信用スコアを減少してもよい。リファインメント活動として検知される不審挙動は、アップデートコマンドの受信回数が所定回数以上であることに限定されず、例えば、所定の第１時間内における同一属性のフレームの受信回数が所定回数以上であることであってもよい。

[0114] 同一属性のフレームとは、フレームに含まれる識別子、ＩＰアドレス、ＭＡＣアドレス、ポート番号のいずれか、または、いずれか２つ以上の組み合わせが同一であるフレームである。また、属性は、フレームを特定する情報であり、フレームに含まれる識別子、ＩＰアドレス、ＭＡＣアドレス、ポート番号などである。

[0115] ステップＳ１１０１において、受信したフレームが診断コマンドまたはアップデートコマンドでない場合（Ｓ１１０１でＮｏ）、ゲートウェイ６０は、受信したフレームが、運転支援機能がＯＮとなるコマンドであるか否かを確認する（Ｓ１１０５）。信用スコア算出部６３は、不審挙動がインジェクション活動またはリファインメント活動として検知されなかった場合、ステップＳ１１０５に進むとも言える。

[0116] 次に、受信したフレームが運転支援機能ＯＮコマンドである場合（Ｓ１１０５でＹｅｓ）、ゲートウェイ６０は、該当機能について前回に当該機能がＯＮとなった時刻（例えば、当該ＯＮコマンドを受信した時刻）からの経過時間を更新する（Ｓ１１０６）。信用スコア算出部６３は、運転支援機能Ｏ

Ｎコマンドのフレームを前回受信した時刻を信用スコア保持部６８から取得し、取得した時刻とステップＳ１１０５でＹｅｓと判定したフレームを受信した時刻とに基づいて経過時間を更新する。信用スコア算出部６３は、例えば、経過時間を当該２つの時刻の時間差とする。

[0117] 次に、ゲートウェイ６０は、更新した経過時間が所定値未満（例えば５分未満）であるか否かを確認する（Ｓ１１０７）。信用スコア算出部６３は、更新した経過時間が所定値未満であるか否かを判定する。ステップＳ１１０７の判定で用いる所定値は、信用スコア保持部６８に予め格納されている。

[0118] 所定の第１時間内における経過時間が所定値未満である場合（Ｓ１１０７でＹｅｓ）、ゲートウェイ６０は、信用スコアを１デクリメントし（Ｓ１１０４）、終了する。

[0119] 所定の第１時間内における経過時間が所定値以上である場合（Ｓ１１０７でＮｏ）、ゲートウェイ６０は、特に何もせずに処理を終了する。つまり、信用スコア算出部６３は、経過時間が所定値未満である場合、信用スコアを更新し、経過時間が所定値以上である場合、信用スコアの更新を行わない。

[0120] このように、信用スコア算出部６３は、不審挙動が、所定の第１時間内における運転支援機能の発動間隔が所定値未満である場合に、信用スコアを減少させる。なお、信用スコア算出部６３は、所定の第１時間内における、運転支援機能の発動回数が所定数以上である場合に、ステップＳ１１０７でＹｅｓと判定してもよい。運転支援機能の発動回数は、運転支援機能が発動した回数であってもよいし、運転支援機能ＯＮコマンドを受信した回数であってもよい。

[0121] また、信用スコア算出部６３は、所定の第１時間内における経過時間が所定値未満である場合、または、所定の第１時間内における運転支援機能の発動回数が所定数以上である場合に、当該不審挙動をアクティブモニタリング活動として検知し、アクティブモニタリング活動が検知された場合に、信用スコアを減少させてもよい。アクティブモニタリング活動として検知される不審挙動は、運転支援機能に関するものに限定されず、例えば、所定の第１

時間内における車内のボタンの操作回数（例えば、図４Ｂに示すボタン連続押下回数）が所定回数以上であることであってもよい。

[0122] ステップＳ１１０５において、受信したフレームが運転支援機能ＯＮコマンドでない場合（Ｓ１１０５でＮｏ）、ゲートウェイ６０は、受信したフレームから、急ブレーキ、急ハンドル、急アクセルのいずれかが検知されるか否かを確認する（Ｓ１１０８）。信用スコア算出部６３は、受信したフレームが急ブレーキ、急ハンドル、急アクセルのいずれかであるか否かを判定する。

[0123] 急ブレーキ、急ハンドル、急アクセルのいずれかが検知される場合（Ｓ１１０８でＹｅｓ）、ゲートウェイ６０は、前回の検知時刻からの経過時間を更新する（Ｓ１１０９）。信用スコア算出部６３は、急ブレーキ、急ハンドル、急アクセルのいずれかのフレームを前回受信した時刻を信用スコア保持部６８から取得し、取得した時刻とステップＳ１１０８でＹｅｓと判定したフレームを受信した時刻とに基づいて経過時間を更新する。信用スコア算出部６３は、例えば、経過時間を当該２つの時刻の時間差とする。経過時間は、検知間隔の一例である。

[0124] ゲートウェイ６０は、経過時間が、所定値未満（例えば５分未満）であるかを確認する（Ｓ１１１０）。信用スコア算出部６３は、更新した経過時間が所定値未満であるか否かを判定する。ステップＳ１１１０の判定で用いる所定値は、信用スコア保持部６８に予め格納されている。

[0125] 所定の第１時間内における経過時間が所定値未満である場合（Ｓ１１１０でＹｅｓ）、ゲートウェイ６０は、信用スコアを１デクリメントし（Ｓ１１０４）、終了する。

[0126] 所定の第１時間内における経過時間が所定値以上である場合（Ｓ１１１０でＮｏ）、ゲートウェイ６０は、特に何もせずに終了する。つまり、信用スコア算出部６３は、経過時間が所定値未満である場合、信用スコアを更新し、経過時間が所定値以上である場合、信用スコアの更新を行わない。

[0127] このように、信用スコア算出部６３は、不審挙動が、所定の第１時間内に

おける、急ブレーキ、急ハンドル、急アクセルのいずれか（異常な運転挙動の一例）の経過時間が所定値未満である場合に、信用スコアを減少するとも言える。

[0128] また、信用スコア算出部６３は、所定の第１時間内における、ブレーキ、急ハンドル、急アクセルのいずれかの経過時間が所定値未満である場合に、当該不審挙動をアクティブモニタリング活動として検知し、アクティブモニタリング活動が検知された場合に、信用スコアを減少するとも言える。

[0129] なお、不審挙動は、所定の第１時間内における異常な運転挙動の検知回数が所定値以上であることであってもよい。異常な運転挙動は、アクセル開度、ブレーキ圧、所定時間内における操舵角の変化量が所定値以上であることであってもよい。

[0130] ステップＳ１１０８において、受信したフレームが急ブレーキ、急ハンドルおよび急アクセルのいずれも検知されない場合（Ｓ１１０８でＮｏ）、ゲートウェイ６０は、受信したフレームがエラーフレームであるか否かを確認する（Ｓ１１１１）。信用スコア算出部６３は、受信したフレームがエラーフレームであるか否かを判定する。

[0131] エラーフレームでない場合（Ｓ１１１１でＮｏ）、ゲートウェイ６０は、何もせずに処理を終了する。

[0132] エラーフレームである場合（Ｓ１１１１でＹｅｓ）、ゲートウェイ６０は、前回の検知時刻からの経過時間を更新する（Ｓ１１１２）。信用スコア算出部６３は、エラーフレームを前回受信した時刻を信用スコア保持部６８から取得し、取得した時刻とステップＳ１１１１でＹｅｓと判定したフレームを受信した時刻とに基づいて経過時間を更新する。信用スコア算出部６３は、例えば、経過時間を当該２つの時刻の時間差とする。経過時間は、発生間隔の一例である。

[0133] ゲートウェイ６０は、経過時間が、所定値未満（例えば５分未満）であるかを確認する（Ｓ１１１３）。信用スコア算出部６３は、更新した経過時間が所定値未満であるか否かを判定する。ステップＳ１１１３の判定で用いる

所定値は、信用スコア保持部６８に予め格納されている。

[0134] 所定の第１時間内における経過時間が所定値未満である場合（Ｓ１１１３でＹｅｓ）、ゲートウェイ６０は、信用スコアを１デクリメントし（Ｓ１１０４）、終了する。

[0135] 所定の第１時間内における経過時間が所定値以上である場合（Ｓ１１１３でＮｏ）、ゲートウェイ６０は、何もせずに終了する。つまり、信用スコア算出部６３は、経過時間が所定値未満である場合、信用スコアを更新し、経過時間が所定値以上である場合、信用スコアの更新を行わない。

[0136] このように、信用スコア算出部６３は、不審挙動が、所定の第１時間内におけるエラーフレームの経過時間が所定値未満である場合に、信用スコアを減少させる。

[0137] また、信用スコア算出部６３は、所定の第１時間内における、エラーフレームの経過時間が所定値以上である場合に、当該不審挙動をパッシブモニタリング活動として検知し、パッシブモニタリング活動が検知された場合に、信用スコアを減少するとも言える。なお、パッシブモニタリング活動として検知される不審挙動は、エラーフレームが検知されたことであってもよい。また、パッシブモニタリング活動として検知される不審挙動は、サードパーティ装置（監視装置の一例）の接続、ネットワークの瞬断（例えば、メッセージの瞬断）、バッテリー電圧の低下またはバッテリーの取り外しのいずれかが検知されたことであってもよいし、当該いずれかの経過時間が所定値未満であることであってもよい。また、パッシブモニタリング活動として検知される不審挙動は、停車時間割合（例えば、所定の第１時間に対する停車している時間の割合）が所定割合以上であることであってもよい。

[0138] なお、信用スコア算出部６３は、図７に示すステップＳ１１０１、Ｓ１１０５、Ｓ１１０８およびＳ１１１１のうち、少なくとも１つの判定を行えばよい。信用スコア算出部６３は、例えば、パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動およびリファインメント活動の少なくとも１つを不審挙動として検知可能であればよい。

[0139] ［１．８　ゲートウェイ６０の監視レベル変更のフローチャート］

図８は、本実施の形態におけるゲートウェイ６０の監視レベル変更のフローチャートである。具体的には、図８は、図６のステップＳ１３の監視レベルを変更する処理の詳細を示すフローチャートである。なお、図８に示す動作は、例えば、監視制御部６４により実行される。

[0140] 図８に示すように、ゲートウェイ６０は、ステップＳ１２において、信用スコアが所定値以下である場合（Ｓ１２でＹｅｓ）、信用スコアが３０以下であるか否かを判定する（Ｓ１３０１）。監視制御部６４は、例えば、ステップＳ１１において算出された信用スコアが所定値以下であるか否かを判定する。ステップＳ１３０１の判定で用いる所定値は、信用スコア保持部６８に予め格納されている。また、信用スコア３０は、第１の閾値の一例である。

[0141] 信用スコアが３０以下の場合（Ｓ１３０１でＹｅｓ）、ゲートウェイ６０は、縮退モードへ移行する（Ｓ１３０２）。縮退モードとは、運転支援機能の一部またはすべてを無効化するモードである。縮退モードに移行する処理を行うために、ゲートウェイ６０は、他のＥＣＵへ通知を行ったり、機能を無効化したことを運転者に通知する（注意喚起する）表示を行ったり、ゲートウェイ６０で、一部のフレームの転送を止めたりする。その後、ゲートウェイ６０は、処理を終了する。なお、縮退モードへ移行することは、車両２００の機能を制限することの一例である。また、ゲートウェイ６０は、近隣車両またはサーバへ現在の信用スコアを通知してもよい。

[0142] また、車載ネットワークシステムに侵入検知システムが含まれる場合、縮退モードへ移行することは、侵入検知システムを有効化することであってもよい。侵入検知システムを有効化することは、車載ネットワークの監視を強化することの一例である。

[0143] ゲートウェイ６０は、信用スコアが３０以下の場合、車両２００の機能の制限、車両２００の運転者への注意喚起、近隣車両またはサーバへの信用スコアの通知、車載ネットワークの監視強化のいずれか１つ以上を実行すれば

よい。

[0144] 信用スコアが３０より大きい場合（Ｓ１３０１でＮｏ）、ゲートウェイ６０は、信用スコアが５０以下であるか否かを判定する（Ｓ１３０３）。監視制御部６４は、ステップＳ１３０３において、信用スコアが３０より大きくかつ５０以下であるか否かを判定するとも言える。また、信用スコア５０は、第２の閾値の一例である。

[0145] 信用スコアが５０以下である場合（Ｓ１３０３でＹｅｓ）、ゲートウェイ６０は、運転者に注意喚起を行うためのフレームを、例えばインストルメントクラスタ等のディスプレイの制御を行うＥＣＵへ送信することで、運転者への注意喚起を行うとともに、サーバへ信用スコアまたは車両ログを通知し（Ｓ１３０４）、処理を終了する。なお、ステップＳ１３０４では、運転者への注意喚起およびサーバへの通知のいずれかが行われればよい。また、ゲートウェイ６０は、ステップＳ１３０４において、近隣車両へ信用スコアを通知してもよい。

[0146] 信用スコアが５０より大きい場合（Ｓ１３０３でＮｏ）、ゲートウェイ６０は、信用スコアが８０以下であるか否かを確認する（Ｓ１３０５）。監視制御部６４は、ステップＳ１３０５において、信用スコアが５０より大きくかつ８０以下であるか否かを判定するとも言える。また、信用スコア８０は、第３の閾値の一例である。

[0147] 信用スコアが８０以下である場合（Ｓ１３０５でＹｅｓ）、ゲートウェイ６０は、サーバへ信用スコアを通知する（Ｓ１３０６）。

[0148] 信用スコアが８０より大きい場合（Ｓ１３０５でＮｏ）、ゲートウェイ６０は、何もせずに処理を終了する。なお、ステップＳ１３０５でＮｏである場合も、サーバへの通知が行われてもよい。

[0149] このように、監視制御部６４は、信用スコアが所定の値以下となった場合に、信用スコアの値に基づいて、車両２００の機能の制限、車両２００の運転者への注意喚起、近隣車両またはサーバへの信用スコアの通知、車載ネットワークの監視強化のいずれか１つ以上を実行する。監視制御部６４は、例

えば、信用スコアが低くなると、監視レベルを強くするように、上記のいずれか１つ以上を実行する。監視制御部６４は、信用スコアが第１の閾値以下である場合、第１の監視レベルに対応する動作を実行し、信用スコアが第１の閾値より大きくかつ当該第１の閾値より大きい第２の閾値以下である場合、第１の監視レベルより監視レベルが低い第２の監視レベルに対応する動作を実行し、信用スコアが第２の閾値より大きくかつ当該第２の閾値より大きい第３の閾値以下である場合、第２の監視レベルより監視レベルが低い第３の監視レベルに対応する動作を実行する。第１の閾値は、例えば、信用スコアの最小値（例えば、０）より大きな値であり、第３の閾値は、例えば、信用スコアの初期値（例えば、１００）より低い値である。なお、第１の閾値～第３の閾値、および、第１の監視レベル～第３の監視レベルに対応する動作は、信用スコア保持部６８に予め格納されている。

[0150] ［１．９　ゲートウェイ動作シーケンス（信用スコアが５０以下となった場合）］

図９は、本実施の形態におけるゲートウェイ６０の動作シーケンスを示す図である。具体的には、図９は、ゲートウェイ６０における信用スコアが５１であった時に、不審な運転挙動によって信用スコアが５０以下となった場合の動作シーケンスを示す図である。ＥＣＵ２０は、緊急ブレーキを指示するフレームを送信するＥＣＵであり、ＥＣＵ３０はディスプレイの制御を行うＥＣＵであるとする。

[0151] 図９に示すように、ＥＣＵ２０は、緊急ブレーキＯＮを要求するフレームを送信し（Ｓ１００）、ゲートウェイ６０は、送信された緊急ブレーキＯＮを要求するフレームを受信する。なお、ブレーキを制御するＥＣＵも送信された緊急ブレーキＯＮを要求するフレームを受信し、緊急ブレーキを発動させるが、図示を省略する。

[0152] 次に、ＥＣＵ２０は、緊急ブレーキＯＮのフレームの送信完了後に、緊急ブレーキＯＦＦを要求するフレームを送信し（Ｓ１０１）、ゲートウェイ６０は、送信された緊急ブレーキＯＦＦを要求するフレームを受信する。

[0153] その後、ＥＣＵ２０は、再度、緊急ブレーキＯＮを要求するフレームを送信し（Ｓ１０２）、ゲートウェイ６０は送信された緊急ブレーキＯＮを要求するフレームを受信する。

[0154] ゲートウェイ６０は、ステップＳ１００における緊急ブレーキＯＮを要求するフレームの受信から、ステップＳ１０２における緊急ブレーキＯＮを要求するフレームの受信までの時間（検知間隔の一例）が所定値（例えば５分）より短い場合、信用スコアを１減少させる（Ｓ１０３）。ステップＳ１０３の処理は、図７に示すステップＳ１１０７でＹｅｓと判定された後に実行されるステップＳ１１０４の処理に相当する。

[0155] ゲートウェイ６０は、信用スコアを１減少させた結果、現在の信用スコアが５０になったため、運転者に注意喚起表示を行うためのフレームを送信する（Ｓ１０４）。ステップＳ１０４の処理は、図８に示すステップＳ１３０４の処理に相当する。

[0156] ＥＣＵ３０は、運転者へ注意喚起表示を行うためのフレームを受信し、ディスプレイに注意喚起を表示する（Ｓ１０５）。ディスプレイへの表示内容は、例えば、図１１Ａのような表示である。図１１Ａは、本実施の形態における運転者へ通知する表示内容の一例を示す図である。図１１Ａに示すように、ステップＳ１０５では、異常な挙動を検知したことを示す情報、および、それに対する対応方法（例えば、センターへ通知）が表示される。

[0157] ゲートウェイ６０は、サーバに対して信用スコアを含む車両ログを通知する（Ｓ１０６）。

[0158] ［１．１０　ゲートウェイ動作シーケンス（信用スコアが３０以下となった場合）］

図１０は、本実施の形態におけるゲートウェイ６０の動作シーケンスを示す図である。具体的には、図１０は、ゲートウェイ６０における信用スコアが３１であった時に、不審な運転挙動によって信用スコアが３０以下となった場合の動作シーケンスである。ＥＣＵ２０と、ＥＣＵ３０は、図９で説明した役割と同様であるとする。

[0159] 図１０に示すように、ＥＣＵ２０は、緊急ブレーキＯＮを要求するフレームを送信し（Ｓ１１０）、ゲートウェイ６０は、送信された緊急ブレーキＯＮを要求するフレームを受信する。

[0160] 次に、ＥＣＵ２０は、緊急ブレーキＯＮのフレームの送信完了後に、緊急ブレーキＯＦＦを要求するフレームを送信し（Ｓ１１１）、ゲートウェイ６０は、送信された緊急ブレーキＯＦＦを要求するフレームを受信する。

[0161] その後、ＥＣＵ２０は、再度、緊急ブレーキＯＮを要求するフレームを送信し（Ｓ１１２）、ゲートウェイ６０は、送信された緊急ブレーキＯＮを要求するフレームを受信する。

[0162] ゲートウェイ６０は、ステップＳ１１０における緊急ブレーキＯＮを要求するフレームの受信から、ステップＳ１１２における緊急ブレーキＯＮを要求するフレームの受信までの時間（検知間隔の一例）が所定値（例えば５分）より短い場合、信用スコアを１減少させる（Ｓ１１３）。ステップＳ１１３の処理は、図７に示すステップＳ１１０７でＹｅｓと判定された後に実行されるステップＳ１１０４の処理に相当する。

[0163] ゲートウェイ６０は、信用スコアを１減少させた結果、現在の信用スコアが３０以下となったため、縮退モードへ移行するためのフレーム（縮退モード要求フレーム）を送信する（Ｓ１１４）。ゲートウェイ６０は、縮退モードに緊急ブレーキを無効にすることが含まれる場合、ＥＵＣ２０に対して縮退モードへ移行するためのフレームを送信する。ステップＳ１４４の処理は、図８に示すステップＳ１３０２の処理に相当する。

[0164] ＥＣＵ２０は、送信された縮退モード要求フレームを受信し、以降の緊急ブレーキＯＮを要求するフレームの送信を無効にする（Ｓ１１５）。

[0165] ＥＣＵ３０は、送信された縮退モード要求フレームを受信し、ディスプレイに機能制限していることを通知するための表示を行う（Ｓ１１６）。ディスプレイの表示内容は、例えば図１１Ｂのような表示である。図１１Ｂは、本実施の形態における運転者へ通知する表示内容の別の一例を示す図である。図１１Ｂに示すように、ステップＳ１１６では、異常な挙動が継続したこ

とを示す情報、一部の機能を制限したことを示す情報、および、問い合わせ先が表示される。

[0166] ［１．１１　実施の形態１の効果］

実施の形態１に係るゲートウェイ６０（車両監視装置の一例）では、攻撃者による車載ネットワークシステムのリバースエンジニアリング活動が疑われる活動に対して、信用スコアを算出する。ゲートウェイ６０は、さらに信用スコアに基づいて、対応を決定する。ゲートウェイ６０は、サーバへ通知を行うことによって、サーバ側において疑わしい車両が把握され、当該車両を重点的な監視対象と特定することが可能となる。また、ゲートウェイ６０は、より疑わしい車両に対しては車両の機能を一部制限することでリバースエンジニアリング活動を妨害することが可能となる。これにより、ゲートウェイ６０は、車載ネットワークシステムの安全性を高めることができる。

[0167] （実施の形態２）

以下、複数の電子制御ユニット（ＥＣＵ）が通信する車載ネットワーク（車載ネットワークシステム）を搭載した車両２００における、車両監視方法について説明する。なお、本実施の形態は、実施の形態１と同様の車載ネットワークシステム構成のため、車載ネットワークシステムの全体構成を示す図を省略し、実施の形態１と異なるゲートウェイの処理フローチャートのみを説明する。

[0168] なお、本実施の形態では、不審挙動を検知が検知された場合、信用スコアを増加する例について説明する。この場合、信用スコアの初期値は、例えば、０である。また、以下において、不審挙動が検知された場合にスコアが増加する信用スコアを、実施の形態１と区別して不審スコアと記載する。

[0169] ［２．１　ゲートウェイの処理を示すフローチャート］

図１２は、本実施の形態におけるゲートウェイ６０の処理を示すフローチャートである。なお、図１２に示すステップＳ２０、２４、２５および２６のそれぞれは、図６に示すステップＳ１０、１４、１５および１６のそれぞれに対応し、以下では説明を省略または簡略化する。

[0170] 図１２に示すように、ゲートウェイ６０は、フレームを受信しているか否かを判定する（Ｓ２０）。

[0171] フレームを受信している場合（Ｓ２０でＹｅｓ）、ゲートウェイ６０は、各種不審スコアを算出する（Ｓ２１）。フレームを受信していない場合（Ｓ２０でＮｏ）、ゲートウェイ６０は、フレームを受信するまで待機する。

[0172] ゲートウェイ６０は、不審スコア算出後に、算出した不審スコアのうち、いずれかの不審スコアが所定値以上であるか否かを判定する（Ｓ２２）。

[0173] いずれかの不審スコアが所定値以上である場合（Ｓ２２でＹｅｓ）、ゲートウェイ６０は、監視レベルを変更する（Ｓ２３）。

[0174] 全ての不審スコアが所定値未満である場合（Ｓ２２でＮｏ）、ゲートウェイ６０は、転送処理を行って（Ｓ２４）、ステップＳ２５に進む。

[0175] ［２．２　ゲートウェイにおける不審スコア算出のフローチャート］

図１３は、本実施の形態におけるゲートウェイ６０の不審スコア算出のフローチャートである。具体的には、図１３は、図１２のステップＳ２１の不審スコア算出処理の詳細を示すフローチャートである。

[0176] 図１３に示すように、ゲートウェイ６０は、フレームを受信した時点で、診断ポート５０へのサードパーティ装置（監視装置の一例）の接続検知、エラーフレームの検知、ネットワークの瞬断検知、および、バッテリー外しの検知のいずれかが発生しているか否かを判定する（Ｓ２１０１）。また、ゲートウェイ６０は、ステップＳ２１０１において、停車時間割合が所定割合以上であるか否かの判定を行ってもよい。

[0177] ステップＳ２１０１でいずれかが検知された場合（Ｓ２１０１でＹｅｓ）、ゲートウェイ６０は、当該不審挙動をパッシングモニタリング活動として検知し、パッシブモニタリングスコアを１増加させ（Ｓ２１０２）、処理を終了する。パッシングモニタリング活動は、例えば、車載ネットワークシステムにおける車両データを取得するための行動である。パッシブモニタリングスコアは、車載ネットワークシステムに対するリバースエンジニアリング活動のうち、パッシブモニタリング活動に対する不審スコアを示す。つまり

、パッシブモニタリングスコアは、パッシブモニタリング活動が行われている可能性を示しており、パッシブモニタリングスコアが高いことは、車両２００に対してパッシブモニタリング活動が行われている可能性が高いことを示す。信用スコア算出部６３は、ステップＳ２１０２において、フレーム送受信部６１で受信したフレームと車両データとに基づいて、当該フレームを受信する前のパッシブモニタリングスコアを更新するとも言える。

[0178] ステップＳ２１０１でいずれも検知されなかった場合（Ｓ２１０１でＮｏ）、ゲートウェイ６０は、さらに緊急ブレーキ等の運転支援機能のＯＮ、または、急ブレーキ等の異常動作が繰り返し検知されたか否かを判定する（Ｓ２１０３）。ゲートウェイ６０は、例えば、ステップＳ２１０３において、所定の第１時間内における、運転支援機能の発動回数、または、異常な運転挙動の検知回数のいずれかが所定数以上であるか否かを判定する。また、ゲートウェイ６０は、運転支援機能の発動回数、車内のボタンの操作回数、または、異常な運転挙動の検知回数のいずれかが所定数以上であるか否かを判定してもよい。

[0179] ステップＳ２１０３でいずれかが検知された場合（Ｓ２１０３でＹｅｓ）、ゲートウェイ６０は、当該不審挙動をアクティブモニタリング活動として検知し、アクティブモニタリングスコアを１増加させ（Ｓ２１０４）、処理を終了する。アクティブモニタリング活動は、例えば、車両２００の特定機能動作中または特定状況における車載ネットワークの車両データを取得しようとするための動作である。アクティブモニタリングスコアは、車載ネットワークシステムに対するリバースエンジニアリング活動のうち、アクティブモニタリング活動に対する不審スコアを示す。つまり、アクティブモニタリングスコアは、アクティブモニタリング活動が行われている可能性を示しており、アクティブモニタリングスコアが高いことは、車両２００に対してアクティブモニタリング活動が行われている可能性が高いことを示す。信用スコア算出部６３は、ステップＳ２１０４において、フレーム送受信部６１で受信したフレームと車両データとに基づいて、当該フレームを受信する前の

アクティブモニタリングスコアを更新するとも言える。

[0180] ステップＳ２１０３でいずれも検知されなかった場合（Ｓ２１０３でＮｏ）、ゲートウェイ６０は、さらにフレームの受信回数、または、診断コマンドの受信回数が所定の閾値より大きいか否かを判定する（Ｓ２１０５）。受信回数は、受信量の一例である。

[0181] ステップＳ２１０５でいずれかの受信回数が所定の閾値より大きい場合（Ｓ２１０５でＹｅｓ）、ゲートウェイ６０は、当該不審挙動をインジェクション活動として検知し、インジェクションスコアを１増加させ（Ｓ２１０６）、処理を終了する。インジェクション活動は、例えば、車載ネットワークシステムへのフレームの注入を試行するための行動である。つまり、インジェクション活動は、攻撃者による不正なフレームの注入の試行が行われている段階であることを示す。

[0182] また、インジェクションスコアは、車載ネットワークシステムに対するリバースエンジニアリング活動のうち、インジェクション活動に対する不審スコアを示す。つまり、インジェクションスコアは、インジェクション活動が行われている可能性を示しており、インジェクションスコアが高いことは、車両２００に対してインジェクション活動が行われている可能性が高いことを示す。信用スコア算出部６３は、ステップＳ２１０６において、フレーム送受信部６１で受信したフレームと車両データとに基づいて、当該フレームを受信する前のインジェクションスコアを更新するとも言える。

[0183] ステップＳ２１０５でどちらの受信回数も閾値以下である場合（Ｓ２１０５でＮｏ）、ゲートウェイ６０は、さらにアップデートコマンドあるいは同一ＩＤフレームの受信回数が、所定の閾値を超えるか否かを判定する（Ｓ２１０７）。なお、同一ＩＤフレームは、同一属性のフレームであることの一例である。ステップＳ２１０７では、同一属性のフレームの受信回数に基づいて判定が行われてもよい。また、受信回数は、受信量の一例である。

[0184] ステップＳ２１０７でアップデートコマンドあるいは同一ＩＤフレームの受信回数が所定の閾値を超える場合（Ｓ２１０７でＹｅｓ）、ゲートウェイ

６０は、当該不審挙動をリファインメント活動として検知し、リファインメントスコアを１増加させ（Ｓ２１０８）、処理を終了する。リファインメント活動は、例えば、車載ネットワークシステムに注入されるフレームの精度を向上させるためのフレームの注入を試行するための行動である。つまり、リファインメント活動は、インジェクション活動に比べて攻撃者の攻撃内容が洗練されている段階であることを示す。

[0185] また、リファインメントスコアは、車載ネットワークシステムに対するリバースエンジニアリング活動のうち、リファインメント活動に対する不審スコアを示す。つまり、リファインメントスコアは、リファインメント活動が行われている可能性を示しており、リファインメントスコアが高いことは、車両２００に対してリファインメント活動が行われている可能性が高いことを示す。信用スコア算出部６３は、ステップＳ２１０８において、フレーム送受信部６１で受信したフレームと車両データとに基づいて、当該フレームを受信する前のリファインメントスコアを更新するとも言える。

[0186] ステップＳ２１０７でアップデートコマンドあるいは同一ＩＤフレームの受信回数が所定の閾値以下である場合（Ｓ２１０７でＮｏ）、信用スコア算出部６３は、何もせずに終了する。

[0187] ここで、サードパーティ装置の接続検知は、診断ポート５０から特定の診断コマンドが流れることから検知されうる。エラーフレームの検知は、ゲートウェイ６０のエラーカウンタまたはエラー割込み処理によって検知されうる。ネットワークの瞬断検知は、フレームの受信時刻を常に保持しておき、フレーム受信時に、前回フレームを受信した時刻と現在の時刻との差分が所定の閾値を超えた場合に検知されうる。バッテリー外しの検知は、ゲートウェイ６０への電源供給が遮断され、再度電源が供給されたときに、前回電源供給が遮断されたことを検知することで検知されうる。

[0188] 上記のように、本実施の形態では、ゲートウェイ６０（具体的には、信用スコア算出部６３）は、リバースエンジニアリングの各段階を示すパッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動お

よびリファインメント活動のそれぞれにおいて、不審スコアを算出する。パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動およびリファインメント活動は、リバースエンジニアリングの各段階を示す複数の種類の一例である。つまり、不審挙動は、複数の種類を有する。そして、信用スコア算出部６３は、不審挙動の複数の種類のそれぞれに対する不審スコアを算出する。

[0189] なお、複数の種類は、２つ以上の種類を含んでいればよい。不審挙動の複数の種類は、例えば、パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動およびリファインメント活動の少なくとも２つを含んでいればよい。言い換えると、信用スコア算出部６３は、図１３に示すステップＳ２１０１、Ｓ２１０３、Ｓ２１０５およびＳ２１０７のうち、少なくとも２つの判定を行えばよい。信用スコア算出部６３は、例えば、パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動およびリファインメント活動の少なくとも２つを不審挙動として検知可能であればよい。

[0190] なお、リファインメント活動、インジェクション活動、アクティブモニタリング活動およびパッシブモニタリング活動の順に、リバースエンジニアリング活動が進んでいる、つまりこの順に車載ネットワークの解析が進んでいることを示す。

[0191] ［２．３　ゲートウェイにおける監視レベル変更のフローチャート］

図１４は、本実施の形態におけるゲートウェイ６０の監視レベル変更のフローチャートである。具体的には、図１４は、図１２のステップＳ２３の監視レベル変更処理の詳細を示すフローチャートである。なお、図１４に示す動作は、例えば、監視制御部６４により実行される。

[0192] 図１４に示すように、ゲートウェイ６０は、リファインメントスコアが３より大きいか否かを判定する（Ｓ２３０１）。３は、リファインメント活動が行われている可能性があるか否かを判定するための第４の閾値であり、例えば、信用スコア保持部６８に予め格納されている。なお、第４の閾値は、

３であることに限定されない。

[0193] リファインメントスコアが３より大きい場合（Ｓ２３０１でＹｅｓ）、ゲートウェイ６０は、縮退モードへ移行する要求フレームを各ＥＣＵに送信し、かつ、各不審スコアを含む車両データをサーバへ通知して（Ｓ２３０２）、処理を終了する。

[0194] リファインメントスコアが３以下である場合（Ｓ２３０１でＮｏ）、ゲートウェイ６０は、さらにインジェクションスコアが３より大きいか否かを判定する（Ｓ２３０３）。３は、インジェクション活動が行われている可能性があるか否かを判定するための第５の閾値であり、例えば、信用スコア保持部６８に予め格納されている。なお、第５の閾値は、３であることに限定されない。

[0195] インジェクションスコアが３より大きい場合（Ｓ２３０３でＹｅｓ）、ゲートウェイ６０は、車両２００の一部機能を制限し、かつ、各不審スコアを含む車両データをサーバへ通知して（Ｓ２３０４）、処理を終了する。

[0196] インジェクションスコアが３以下である場合（Ｓ２３０３でＮｏ）、ゲートウェイ６０は、さらにアクティブモニタリングスコアが３より大きいか否かを判定する（Ｓ２３０５）。３は、アクティブモニタリング活動が行われている可能性があるか否かを判定するための第６の閾値であり、例えば、信用スコア保持部６８に予め格納されている。なお、第６の閾値は、３であることに限定されない。

[0197] アクティブモニタリングスコアが３より大きい場合（Ｓ２３０５でＹｅｓ）、ゲートウェイ６０は、運転者への注意喚起を行うフレームを送信し、かつ、各不審スコアを含む車両データをサーバへ通知して（Ｓ２３０６）、処理を終了する。

[0198] アクティブモニタリングスコアが３以下である場合（Ｓ２３０５でＮｏ）、ゲートウェイ６０は、さらにパッシブモニタリングスコアが３より大きいか否かを判定する（Ｓ２３０７）。３は、パッシブモニタリング活動が行われている可能性があるか否かを判定するための第７の閾値であり、例えば、

信用スコア保持部６８に予め格納されている。なお、第７の閾値は、３であることに限定されない。

[0199] パッシブモニタリングスコアが３より大きい場合（Ｓ２３０７でＹｅｓ）、ゲートウェイ６０は、各不審スコアを含む車両データをサーバへ通知して（Ｓ２３０８）、処理を終了する。

[0200] パッシブモニタリングスコアが３以下である場合（Ｓ２３０７でＮｏ）、ゲートウェイ６０は、何もせずに終了する。

[0201] このように、監視制御部６４は、不審挙動の複数の種類と、不審挙動の複数の種類のそれぞれに対応する不審スコア（信用スコアの一例）の値とに基づいて、車両２００の機能の一部の制限、車両２００の運転者への注意喚起、近隣車両またはサーバへの信用スコアの通知のいずれか１つ以上を実行する。また、監視制御部６４は、車載ネットワークの監視強化を実行してもよい。監視制御部６４は、例えば、リバースエンジニアリング活動の段階が進むと、監視レベルを強くするように、車両２００の機能の一部の制限、車両２００の運転者への注意喚起、近隣車両またはサーバへの信用スコアの通知および車載ネットワークの監視強化のいずれか１つ以上を実行する。

[0202] 監視制御部６４は、リファインメントスコアが第４の閾値より大きい場合、第４の監視レベルに対応する動作を実行する。また、監視制御部６４は、インジェクションスコアが第５の閾値より大きく、かつ、リファインメントスコアが第４の閾値以下である場合、第４の監視レベルより監視レベルが低い第５の監視レベルに対応する動作を実行する。また、監視制御部６４は、アクティブモニタリングスコアが第６の閾値より大きく、かつ、リファインメントスコアが第４の閾値以下、および、インジェクションスコアが第５の閾値以下である場合、第５の監視レベルより監視レベルが低い第６の監視レベルに対応する動作を実行する。また、監視制御部６４は、パッシブモニタリングスコアが第７の閾値より大きく、かつ、リファインメントスコアが第４の閾値以下、インジェクションスコアが第５の閾値以下、および、アクティブモニタリングスコアが第６の閾値以下である場合、第６の監視レベルよ

り監視レベルが低い第７の監視レベルに対応する動作を実行する。

[0203] なお、第４の閾値は、例えば、リファインメントスコアの最小値（例えば、０であり、初期値）より大きく、かつ、リファインメントスコアの最大値（例えば、１００）以下の値である。第５の閾値は、例えば、インジェクションスコアの最小値（例えば、０であり、初期値）より大きく、かつ、インジェクションスコアの最大値（例えば、１００）以下の値である。第６の閾値は、例えば、アクティブモニタリングスコアの最小値（例えば、０であり、初期値）より大きく、かつ、アクティブモニタリングスコアの最大値（例えば、１００）以下の値である。第７の閾値は、例えば、パッシブモニタリングスコアの最小値（例えば、０であり、初期値）より大きく、かつ、パッシブモニタリングスコアの最大値（例えば、１００）以下の値である。

[0204] なお、第４の監視レベル～第７の監視レベルに対応する動作は、信用スコア保持部６８に予め格納されている。

[0205] ［２．４　実施の形態２の効果］

実施の形態２に係るゲートウェイ６０（車両監視装置の一例）では、攻撃者による車載ネットワークシステムのリバースエンジニアリング活動が疑われる活動に対して、活動のフェーズに応じて不審スコアを算出する。ゲートウェイ６０は、さらに各種不審スコアの値に基づいて対応方法を決定することで、より攻撃フェーズの進んだことが疑われる車両２００に対して、より重点的な監視を行うことが可能となり、これにより車載ネットワークシステムの安全性をさらに高めることができる。

[0206] ［その他変形例］

なお、本開示を上記各実施の形態に基づいて説明してきたが、本開示は、上記各実施の形態に限定されないのはもちろんである。以下のような場合も本開示に含まれる。

[0207] （１）上記の実施の形態では、バスはＣＡＮであったが、通信プロトコルはＣＡＮに限らない、例えばＣＡＮ－ＦＤ（ＣＡＮ　ｗｉｔｈ　Ｆｌｅｘｉｂｌｅ　Ｄａｔａ　Ｒａｔｅ）、ＦｌｅｘＲａｙ、Ｅｔｈｅｒｎｅｔであっ

てもよい。

[0208] （２）上記の実施の形態では、サーバ通信部がゲートウェイの構成要素として存在したが、サーバ通信部は、ゲートウェイの必須の構成要素でなくてもよい。例えば、サーバと通信を行う装置が他に存在してもよく、ゲートウェイは当該装置を介して通知を行ってもよい。

[0209] （３）上記の実施の形態では、信用スコア算出部は、ゲートウェイの構成要素であるが、必ずしもゲートウェイの構成要素となる必要はない。例えば、別のＥＣＵの構成要素としてもよいし、仮想マシン上のアプリケーションとして信用スコア算出部が機能してもよい。

[0210] （４）上記の実施の形態では、信用スコアが０～１００の値をとりうるとしたが、信用スコアのとりうる値はこれに限らない、例えば０～１０の１０段階としてもよいし、リバースエンジニアリングの疑わしさのレベルが段階的に示されるものであれば、何でもよい。

[0211] （５）上記の実施の形態では、信用スコアの初期値が１００として、疑わしい挙動を観測した場合に、信用スコアが減少していく例を示したが、信用スコアである必要はなく、不審スコアとして、疑わしい挙動の観測時にスコアが上昇してもよい。信用スコアは、リバースエンジニアリングの疑わしさのレベルが段階的に示されるものであれば、何でもよい。

[0212] （６）上記の実施の形態では、信用スコアが減少する条件を示したが、信用スコアが上昇する条件も存在してよい。例えば、１日（所定の第２時間の一例）経過ごとに信用スコアが上昇してもよいし、イグニッションのＯＮ時に、信用スコアが上昇してもよい。また、例えば、１日（所定の第３時間の一例）経過ごとに信用スコアがリセットされてもよい。また、診断コマンドによって、信用スコアがリセットされてもよいし、サーバからの通知に基づいて信用スコアがリセットされてもよい。これにより、正規の運転者が、疑わしいとされる挙動を偶然に繰り返した結果、信用スコアが低下してしまった場合でも、正常な信用スコアに回復することが可能となる。

[0213] （７）上記の実施の形態では、信用スコアが減少する条件に合致した場合

に、信用スコアが１減少したが、信用スコアの減少量は１に限らない。例えば、観測された不審な挙動に応じて減少量を変化させてもよいし、不審な挙動が繰り返し観測されることによって減少量を大きくしていってもよい。これにより、通常の利用において観測される可能性が低い不審な挙動に対しては、信用スコアをより大きく減少させることができ、不審な車両を特定しやすくなり効果的である。

[0214] （８）上記の実施の形態では、信用スコアを減少させる条件は同様に扱ったが、フェーズを分類し、フェーズごとに信用スコアを算出してもよい。例えば、攻撃者が単に車載ネットワークのログを取得しようとするパッシブモニタリングと、攻撃者が車両の特定機能動作中や特定状況における車載ネットワークのログを取得しようとするアクティブモニタリングと、攻撃者が車載ネットワークログに対してフレーム注入を試行するインジェクションと、攻撃者がより洗練された攻撃を試行するリファインメントと、に段階分けをしてもよい。これにより、攻撃者のリバースエンジニアリングのフェーズを把握することが可能となり、フェーズの進んだ攻撃者に対して重点的な監視ができ効率的である。パッシブモニタリングは、例えば、診断ポートへサードパーティデバイスの接続の検知、モニタリング装置（監視装置の一例）接続するためのネットワークの瞬断、バッテリーの取り外し、エラーフレームの検知回数または検知間隔などに基づいて判定されうる。アクティブモニタリングは、例えば、運転支援機能の利用間隔や利用量、車内に配置されるボタンの単位時間当たりの押下回数、極端なアクセル、ブレーキ、ハンドル操作が観測される頻度などに基づいて判定されうる。インジェクションは、フレームの受信量または受信間隔、診断コマンドの受信量または受信間隔などによって判定されうる。リファインメントは、同一のＩＤのフレームに対する受信量の増加または受信間隔の変化、アップデートコマンドの受信量または受信間隔などによって判定されうる。

[0215] （９）上記の実施の形態では、信用スコア保持部に、信用スコア算出に用いる車両データの今回値と前回値とが保持されているが、前回値でなく、過

去に信用スコアを減少させた実績を保存してもよい。例えば、過去１週間において、スコアが減点された量を保持していてもよい。そして、信用スコア算出部は、過去にスコアが減点された実績が信用スコア保持部に格納されている場合、過去にスコアが減点された実績のある不審な挙動を観測したときの信用スコアの減少量を、過去にスコアが減点された実績がないまたは減点された量が小さい不審な挙動を観測したときの信用スコアの減少量、または、予め設定されている減少量より大きくしてもよい。これにより、不審な挙動が繰り返し観測されている時に、よりリバースエンジニアリングが実施されている可能性が高いと判断することができ効果的である。

[0216] （１０）上記の実施の形態では、信用スコアをサーバへ通知していたが、通知先はサーバだけに限らず、近隣車両または路側機に対してＶ２Ｘ通信により信用スコアを通知してもよい。これにより、インターネット接続が遮断され信用スコアをサーバへ通知できない車両についても不審な車両を発見することが可能となり、セキュリティの向上に効果的である。

[0217] （１１）上記の実施の形態では、信用スコアを、車載ネットワークフレームのログに基づいて算出していたが、近隣車両の信用スコアを自車両の信用スコアの算出に用いてもよい。信用スコア算出部は、例えば、信用スコアが所定値以下の複数の車両が所定領域内に所定期間存在する場合に、攻撃者が自車両も解析ターゲット用の車両としている可能性が高いとして、信用スコアを補正（例えば、減少）してもよい。信用スコア算出部は、例えば、不審挙動の複数の種類のそれぞれに対する信用スコアのいずれかが所定値以下の複数の車両（他車両とも記載する）が所定領域内に所定期間存在する場合、信用スコアが所定値以下である不審挙動の種類に応じて、自車両の信用スコアを補正（例えば、減少）してもよい。信用スコア算出部は、例えば、他車両において所定値以下である不審挙動の種類と同じ不審挙動の種類の自車両における信用スコアを減少させてもよい。

[0218] （１２）上記の実施の形態２では、不審スコアの算出時に、パッシブモニタリングスコア、アクティブモニタリングスコア、インジェクションスコア

、リファインメントスコアの順で、スコア算出を行っていたが、処理の順番を限定するものではない。同様に監視レベル変更時における各不審スコアの判定処理の順番を限定するものではない。例えば、処理の順番を逆にしてもよいし、すべての判定処理を実行してから、スコア算出、監視レベルの変更などを行ってもよい。

[0219] （１３）上記の実施の形態１、２では、信用スコア（不審スコア）が所定の閾値を下回った（上回った）場合に、サーバ通知を行っているが、サーバ通知を行うタイミングはこれに限らない。例えば定期的にサーバへ車両ログを通知していてもよく、信用スコア（不審スコア）の値に応じて、サーバへの通知頻度または通知量を変更するという対応であってもよい。これにより、疑わしい車両からより詳細な車両ログを通知することで、重点的な監視を実現でき効果的である。また、車両ログは、車両の信用スコア（不審スコア）だけでなく、車載ネットワークシステムに流れるフレームから取得される情報を含んでもよい。例えば、車両の速度またはステアリング角度といった車両のセンサ情報であってもよいし、信用スコアを変化させた根拠となる、信用スコア保持部に格納されている車両データを含んでもよい。

[0220] （１４）上記の実施の形態では、フレーム受信時に、スコア算出を行っていたが、フレーム受信時に行わなくてもよい。例えば、内蔵タイマによって定期的にスコア算出を行ってもよい。

[0221] （１５）上記の実施の形態では、監視レベル変更時にスコアの閾値を設定しているが、閾値は本実施の形態で示した値に限らない。疑わしい車両の検知・対応の感度を高めるために閾値を高く（または低く）設定してもよいし、感度を下げるように設定してもよい。また、リバースエンジニアリングにおける状況（例えば、信用スコアの変化スピード、リバースエンジニアリングの段階など）に応じて閾値が動的に変更されてもよい。

[0222] （１６）上記の実施の形態２では、同一ＩＤフレームの受信量に基づいてリファインメントスコアを上昇させていたが、Ｅｔｈｅｒｎｅｔにおいては、同一ポート番号、同一ＩＰアドレス、ＭＡＣアドレスのフレームの受信量

としてもよい。あるいは、これらのヘッダ情報の組み合わせで定義される同一フローの受信量としてもよい。また、受信量は受信パケット数および受信データサイズのいずれでもよい。

[0223] （１７）上記の実施の形態１および２では、信用スコア（不審スコア）の算出条件、または、スコアに応じた処理内容を別途ルールとして保持していてもよい。

[0224] （１８）上記の実施の形態１および２では、信用スコア（不審スコア）は不揮発メモリに保存され、イグニッションＯＦＦとなった後でも保持されるとしたが、不揮発メモリに保持されず、イグニッションごとにリセットされてもよい。これにより、不揮発メモリが不要となり、低コストで車両監視装置を実現することができる。

[0225] （１９）上記の実施の形態では、信用スコア（不審スコア）の値に応じて、サーバ通知、車両の機能制限、運転者への通知などの対応を行っていたが、対応方法はこれらに限らない。例えば、車載ネットワークに侵入検知システムが存在し、侵入検知システムを有効化するとしてもよい。これにより、通常時は侵入検知システムを動作させる必要なく、省電力となり効果的である。あるいは、車載ネットワークログ保存を開始するとしてもよい。これにより、疑わしい挙動発生時の車載ネットワークログを保持しておくことが可能となり、メモリ使用量削減に効果的である。あるいは、サーバへの車載ネットワークログの通知量、通知頻度を変更してもよい。これにより、疑わしい車両からより多くの情報を取得し、通常の車両（信用スコアが所定値以上であり、リバースエンジニアリングが行われていないと想定される車両）からは少ない情報の取得で済むため、通信量の削減に効果的である。あるいは、コールセンターへ通話するとしてもよい。これにより、攻撃者の活動を牽制し、リバースエンジニアリングを抑止することに効果的である。

[0226] （２０）上記の実施の形態では、特に信用スコアを算出する時にモードを設定しなかったが、信用スコアを算出するモードが存在してもよい。例えば、衝突実験を繰り返すテスト車両において、信用スコアが低く算出されるの

を抑えるために、テストモードを設けてもよい。テストモードでは、異常な挙動に対して信用スコアが減少しにくく設定される。テストモードは、サーバとの認証によってアクティベートされ、テストモードの車両は、サーバで信用スコアが把握されるとしてもよい。

[0227] （２１）上記の実施の形態では、自動車に搭載される車載ネットワークにおけるセキュリティ対策として説明したが、上記実施の形態のゲートウェイの適用範囲はこれに限られない。ゲートウェイは、自動車に限らず、建機、農機、船舶、鉄道、飛行機などのモビリティに適用されてもよい。

[0228] すなわち、上記実施の形態のゲートウェイは、モビリティネットワークおよびモビリティネットワークシステムにおけるサイバーセキュリティ対策として適用可能である。

[0229] また、上記実施の形態のゲートウェイは、工場またはビルなどの産業制御システムで利用される通信ネットワーク、または、組込みデバイスを制御するための通信ネットワークなどに適用されてもよい。

[0230] （２２）上記の実施の形態における各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。ＲＡＭまたはハードディスクユニットには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここで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、コンピュータ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。

[0231] （２３）上記の実施の形態における各装置を構成する構成要素の一部または全部は、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よい。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などを含んで構成されるコンピュータシステムである。ＲＡＭには、コンピュータプログ

ラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたが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。

[0232] また、上記の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、一部又はすべてを含むように１チップ化されてもよい。

[0233] 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よい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）、または、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。

[0234] さらには、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よい。バイオ技術の適用等が可能性としてありえる。

[0235] （２４）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。ＩＣカードまたはモジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。ＩＣカードまたはモジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、ＩＣカードまたはモジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0236] （２５）本開示は、上記に示す方法であるとしてもよい。また、これらの方法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よいし、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よい。

[0237] また、本開示は、コンピュータプログラムまたはデジタル信号をコンピュータ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）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されているデジタル信号であるとしてもよい。

[0238]　また、本開示は、コンピュータプログラムまたはデジタル信号を、電気通信回線、無線または有線通信回線、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よい。

[0239]　また、本開示は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、メモリは、上記コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムにしたがって動作するとしてもよい。

[0240]　また、プログラムまたはデジタル信号を記録媒体に記録して移送することにより、またはプログラムまたはデジタル信号を、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よい。

[0241]　（２６）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0242]　本開示は、攻撃者によるリバースエンジニアリング活動が行われる可能性があるモビリティに有用である。

符号の説明

[0243]　１、２、３、４、５　バス

１０、１１、２０、２１、３０、３１、４０、４１　ＥＣＵ

５０　診断ポート

６０　ゲートウェイ

６１　フレーム送受信部

６２　フレーム解釈部

６３　信用スコア算出部

６４　監視制御部

６５　転送制御部

６６　フレーム生成部

６７　サーバ通信部

６８　信用スコア保持部

６９　転送ルール保持部

１００　通信部

１０１　ホスト部

２００　車両

請求の範囲

[請求項1] 1以上の電子制御ユニットを備える車載ネットワークシステムを監視する車両監視装置であって、

前記車載ネットワークシステムに流れるフレームを受信するフレーム受信部と、

前記フレーム受信部で受信した前記フレームと当該フレームの受信より前に前記フレーム受信部で受信した1以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、検知結果に基づいて前記車載ネットワークシステムを搭載する車両に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出部と、を備える、

車両監視装置。

[請求項2] 前記不審挙動は、監視装置の接続、エラーフレーム、ネットワークの瞬断、バッテリー取り外しのいずれかが検知された場合に、パッシブモニタリング活動として検知され、

前記信用スコア算出部は、前記パッシブモニタリング活動が検知された場合に、前記信用スコアを減少させる、

請求項1に記載の車両監視装置。

[請求項3] 前記不審挙動は、所定の第1時間内における、車内のボタンの操作回数、異常な運転挙動の検知回数のいずれかが所定数以上である、または、運転支援機能の発動間隔が所定値未満である場合に、アクティブモニタリング活動として検知され、

前記運転支援機能は、自動駐車支援、オートクルーズコントロール、緊急ブレーキ、レーンキープアシストのいずれかであり、

前記異常な運転挙動は、アクセル開度、ブレーキ圧、所定時間内における操舵角の変化量が所定値以上であることであり、

前記信用スコア算出部は、前記アクティブモニタリング活動が検知された場合に、前記信用スコアを減少させる、

請求項１または２に記載の車両監視装置。

[請求項4] 前記不審挙動は、所定の第１時間内における、前記フレームの受信量、診断コマンドの受信量のいずれかが所定数以上である場合に、インジェクション活動として検知され、

前記信用スコア算出部は、前記インジェクション活動が検知された場合に、前記信用スコアを減少させる、

請求項１～３のいずれか１項に記載の車両監視装置。

[請求項5] 前記不審挙動は、所定の第１時間内における、アップデートコマンドの受信量、同一属性のフレームの受信量のいずれかが所定数以上である場合に、リファインメント活動として検知され、

前記同一属性のフレームとは、前記フレームに含まれる識別子、ＩＰアドレス、ＭＡＣアドレス、ポート番号のいずれか、または、いずれか２つ以上の組み合わせが同一であるフレームであり、

前記信用スコア算出部は、前記リファインメント活動が検知された場合に、前記信用スコアを減少させる、

請求項１～４のいずれか１項に記載の車両監視装置。

[請求項6] 前記車両監視装置は、さらに、監視レベル変更部を備え、

前記監視レベル変更部は、前記信用スコアが所定の値未満となった場合に、前記信用スコアの値に基づいて、前記車両の機能の制限、前記車両の運転者への注意喚起、近隣車両またはサーバへの信用スコアの通知、および、前記車載ネットワークシステムの監視強化のいずれか１つ以上を実行する、

請求項１～５のいずれか１項に記載の車両監視装置。

[請求項7] 前記不審挙動は、前記リバースエンジニアリングの各段階を示す複数の種類を有し、

前記信用スコア算出部は、前記不審挙動の前記複数の種類のそれぞれにおいて信用スコアを算出する、

請求項１に記載の車両監視装置。

[請求項8] 前記不審挙動の前記複数の種類は、パッシブモニタリング活動、アクティブモニタリング活動、インジェクション活動、リファインメント活動の少なくとも２つを含み、

前記パッシブモニタリング活動は、前記車両データを取得するための行動であり、

前記アクティブモニタリング活動は、前記車両の特定機能動作中または特定状況における前記車両データを取得しようとするための動作であり、

前記インジェクション活動は、前記車載ネットワークシステムへのフレームの注入を試行するための行動であり、

前記リファインメント活動は、前記車載ネットワークシステムに注入されるフレームの精度を向上させるためのフレームの注入を試行するための行動である、

請求項７に記載の車両監視装置。

[請求項9] 前記不審挙動は、監視装置の接続、エラーフレーム、ネットワークの瞬断、バッテリー取り外しのいずれかが検知された場合に、前記パッシブモニタリング活動として検知され、所定の第１時間内における、運転支援機能の発動回数、車内のボタンの操作回数、異常な運転挙動の検知回数、のいずれかが所定数以上である場合に前記アクティブモニタリング活動として検知され、所定の第１時間内における、前記フレームの受信回数、診断コマンドの受信回数のいずれかが所定数以上である場合に前記インジェクション活動として検知され、所定の第１時間内における、アップデートコマンドの受信回数、同一属性のフレームの受信回数のいずれかが所定数以上である場合に前記リファインメントとして検知される、

請求項８に記載の車両監視装置。

[請求項10] 前記車両監視装置は、さらに、監視レベル変更部を備え、

前記監視レベル変更部は、前記不審挙動の前記複数の種類と、前記

不審挙動の前記複数の種類のそれぞれに対応する信用スコアの値とに基づいて、前記車両の一部機能の制限、前記車両の運転者への注意喚起、および、近隣車両またはサーバへの信用スコアの通知のいずれか１つ以上を実行する、

請求項７～９のいずれか１項に記載の車両監視装置。

[請求項11] 前記信用スコア算出部は、所定の第２時間が経過するまたは前記車両に対して所定の第１操作が実行されると、前記信用スコアを上昇させる、

請求項１～１０のいずれか１項に記載の車両監視装置。

[請求項12] 前記信用スコア算出部は、所定の第３時間が経過するまたは前記車両に対して所定の第２操作が実行されると、前記信用スコアをリセットする、

請求項１～１１のいずれか１項に記載の車両監視装置。

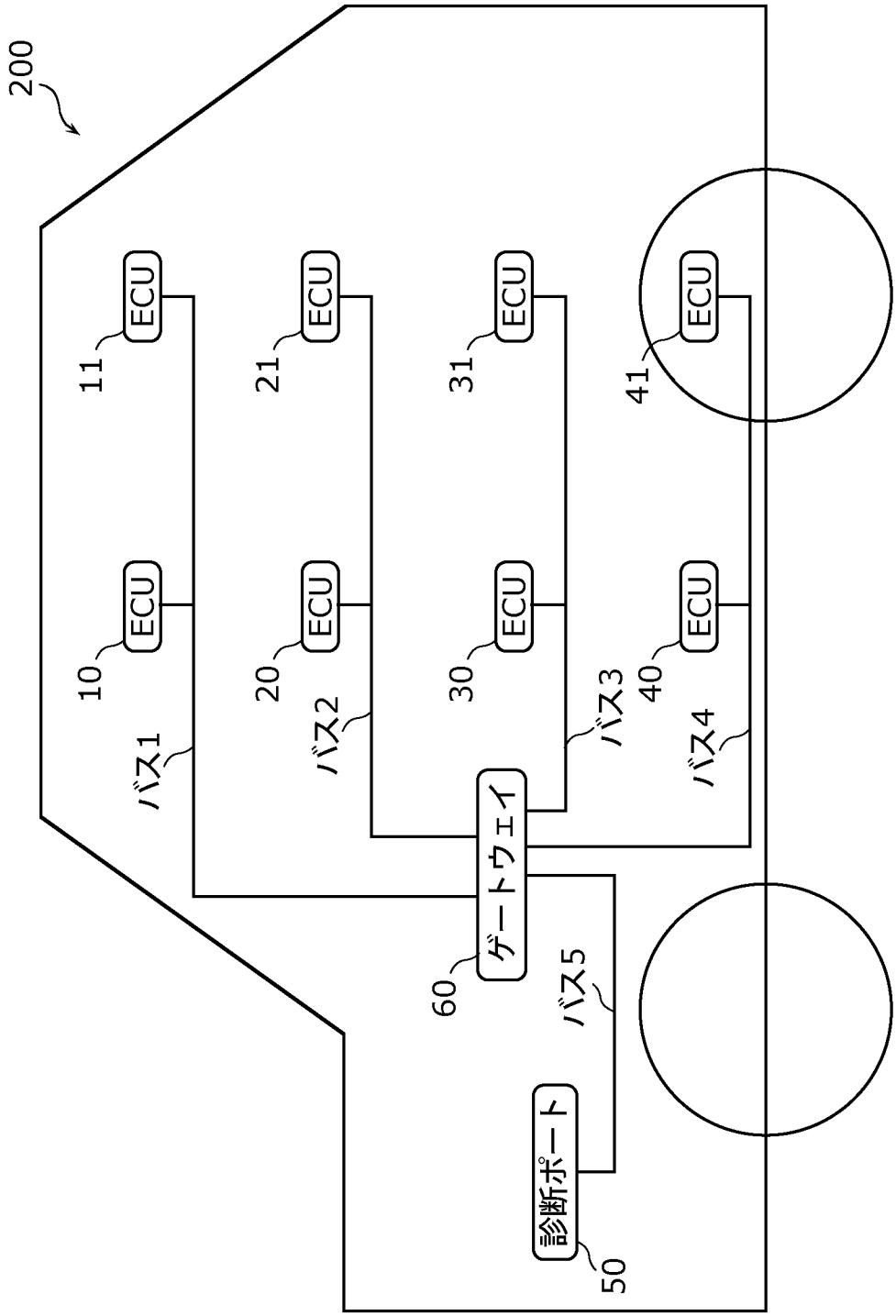
[請求項13] １以上の電子制御ユニットを備える車載ネットワークシステムを監視する車両監視方法であって、

前記車載ネットワークシステムに流れるフレームを受信する受信ステップと、

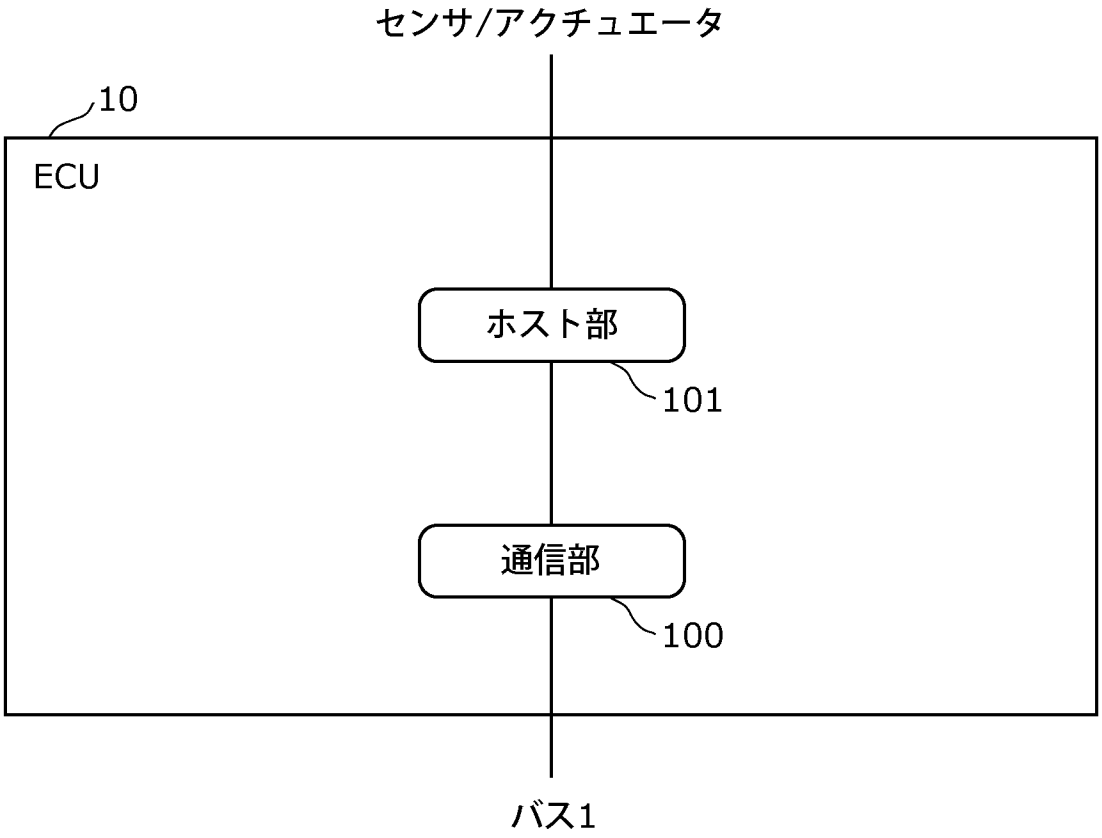
前記受信ステップで受信した前記フレームと当該フレームの受信より前に受信した１以上のフレームに関する情報を含む車両データとに基づいて通常の運転挙動とは異なる不審挙動を検知し、検知結果に基づいて前記車載ネットワークシステムを搭載する車両に対してリバースエンジニアリングが行われている可能性を示す信用スコアを算出する信用スコア算出ステップとを含む、

車両監視方法。

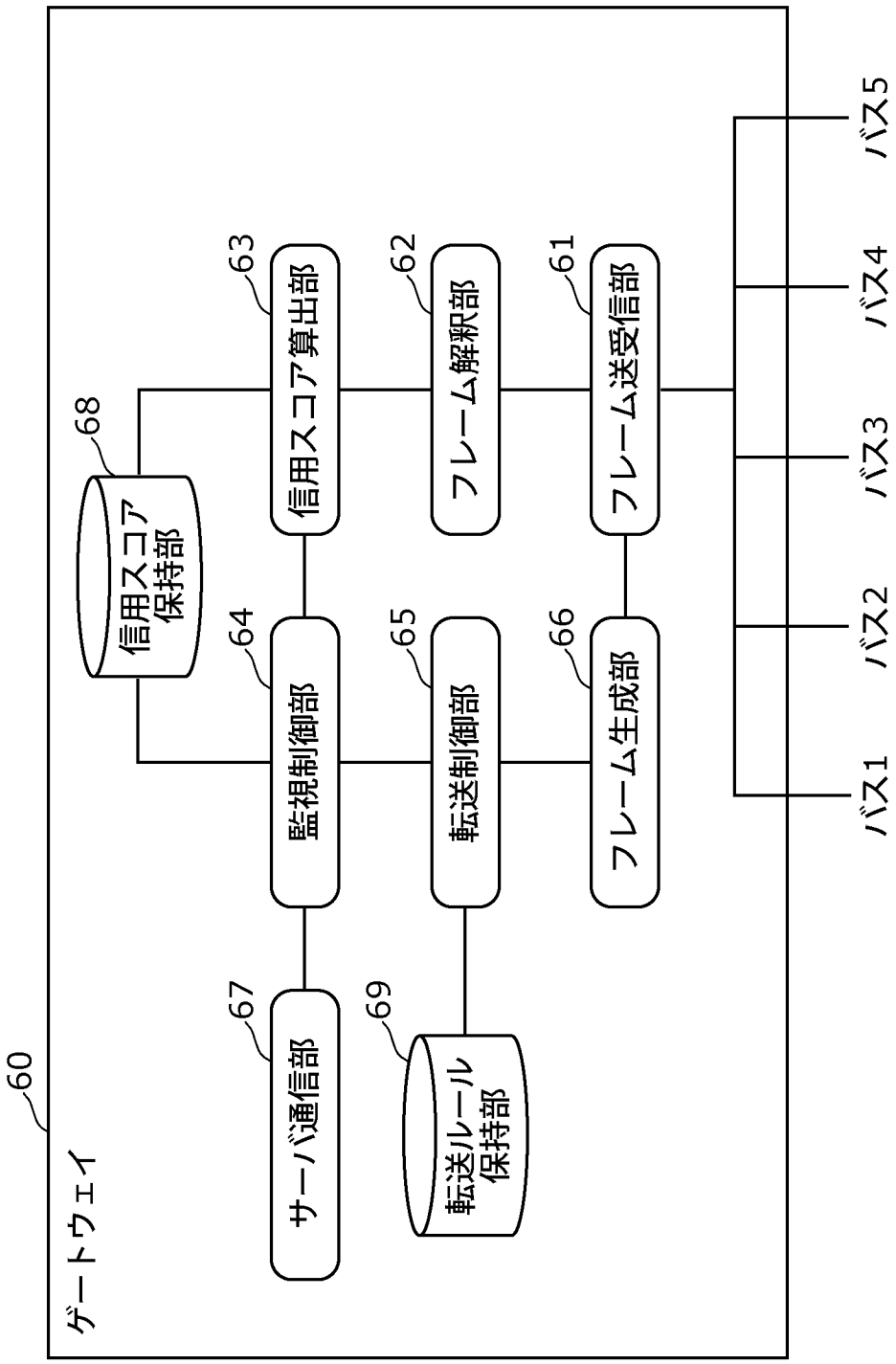
[図1]


200
ECU
10
ECU
11
ECU
20
ECU
21
ECU
30
ECU
31
ECU
40
ECU
41
バス1
バス2
バス3
バス4
バス5
ゲートウェイ
60
診断ポート
50

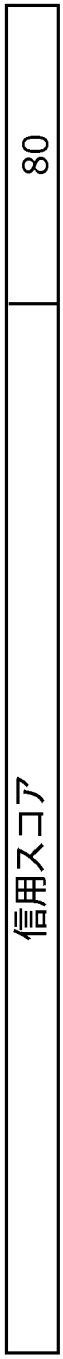
[図2]



[図3]


60
ゲートウェイ
68
信用スコア保持部
63
信用スコア算出部
64
監視制御部
67
サーバ通信部
62
フレーム解釈部
65
転送制御部
69
転送ルール保持部
61
フレーム送受信部
66
フレーム生成部
バス1
バス2
バス3
バス4
バス5

[図4A]



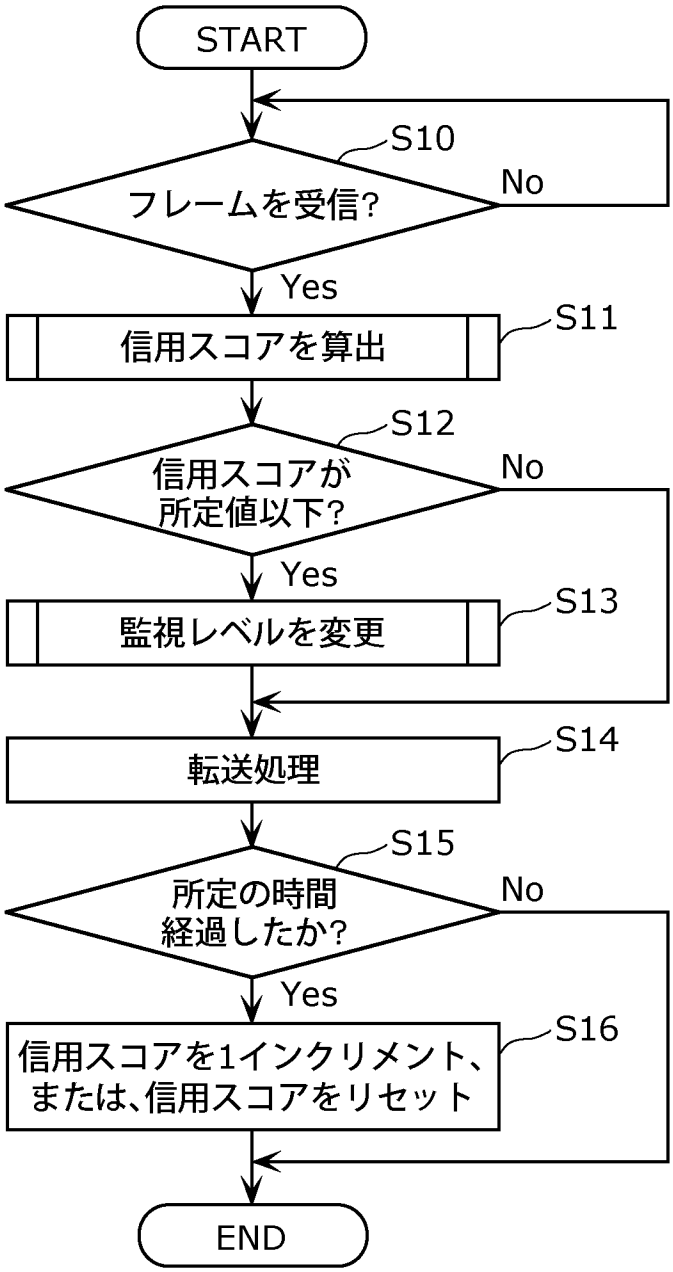
[図4B]

項目	今回値	前回値
停車時間割合	70%	50%
緊急ブレーキ発動間隔	60(秒)	−
クルーズコントロール発動間隔	−	1000(秒)
自動駐車支援発動間隔	30(秒)	−
急アクセル検知間隔	−	−
急ブレーキ検知間隔	−	−
急ハンドル検知間隔	−	−
エラーフレーム発生間隔	1(秒)	−
メッセージ瞬断時間	3(秒)	0(秒)
バッテリー電圧低下有無、または、バッテリーの取り外しの有無	有	無
診断コマンド受信回数	0	0
アップデートコマンド受信回数	0	0
ボタン連続押下回数	30(回)	3(回)
サードパーティ装置の接続の有無	有	無

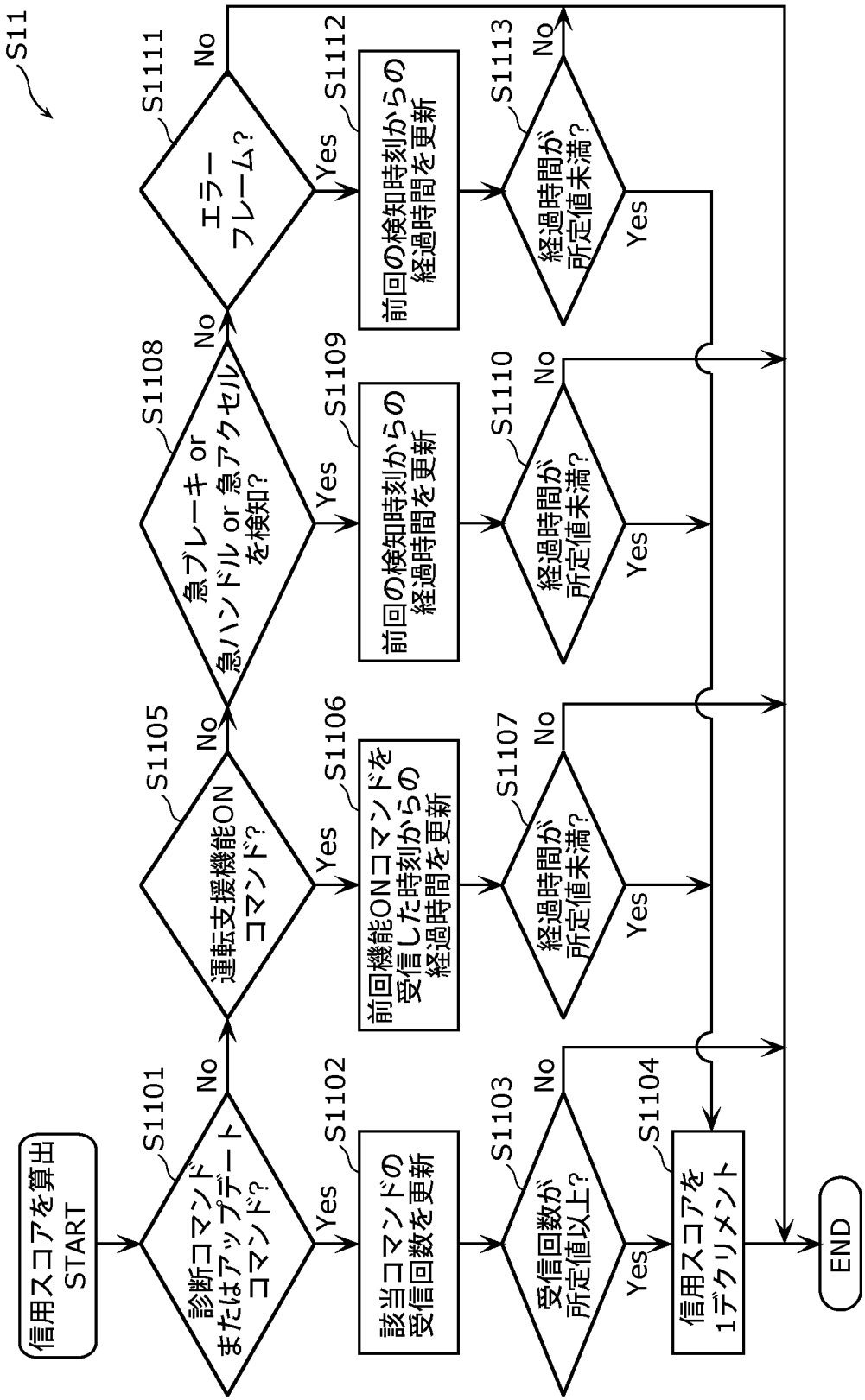
[図5]

ID	転送元	転送先
0x100	バス1	バス2、3, 4
0x200	バス2	バス3
0x250	バス2	バス4
0x300	バス3	バス1
・・・	・・・	・・・

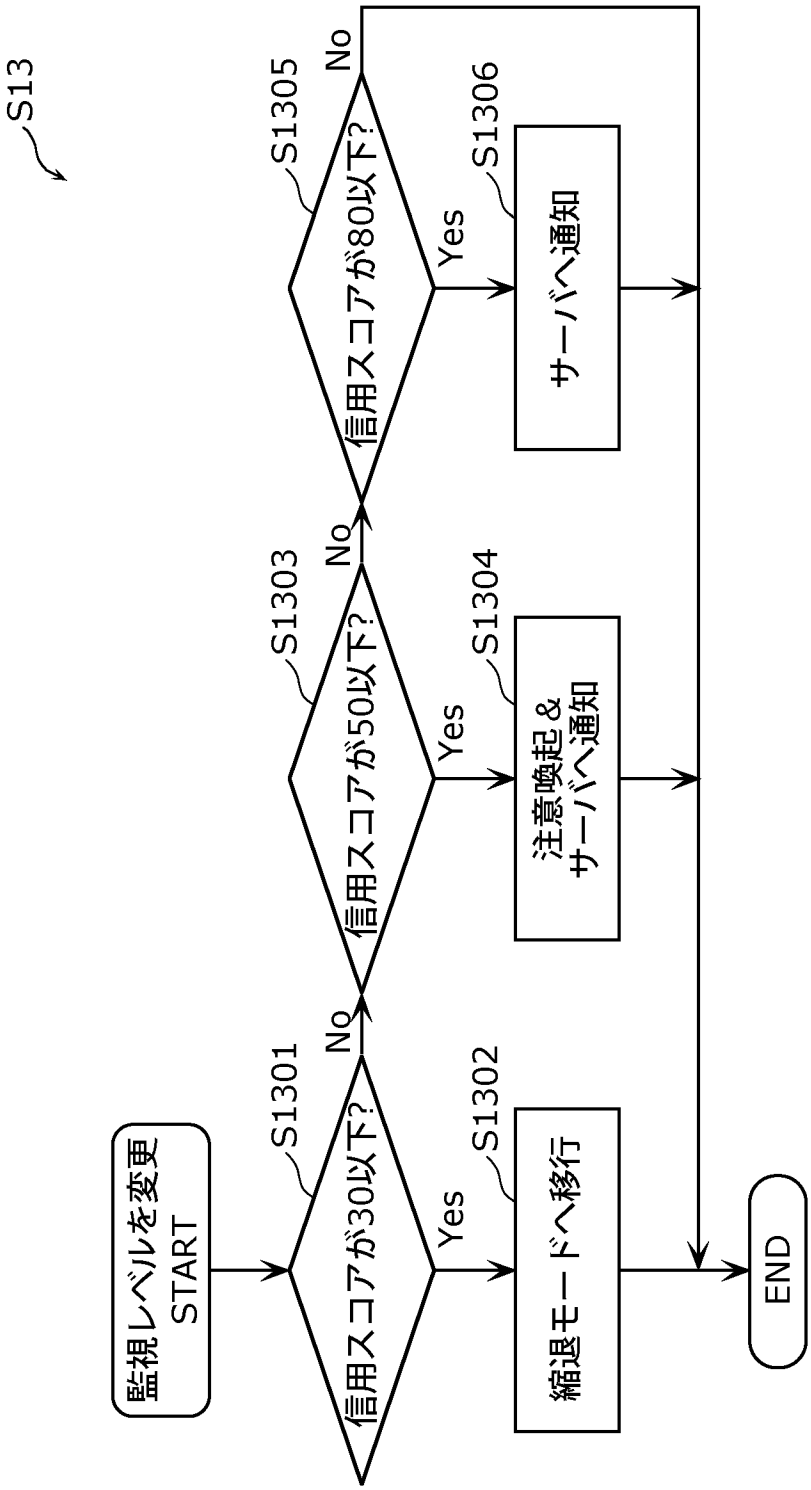
[図6]



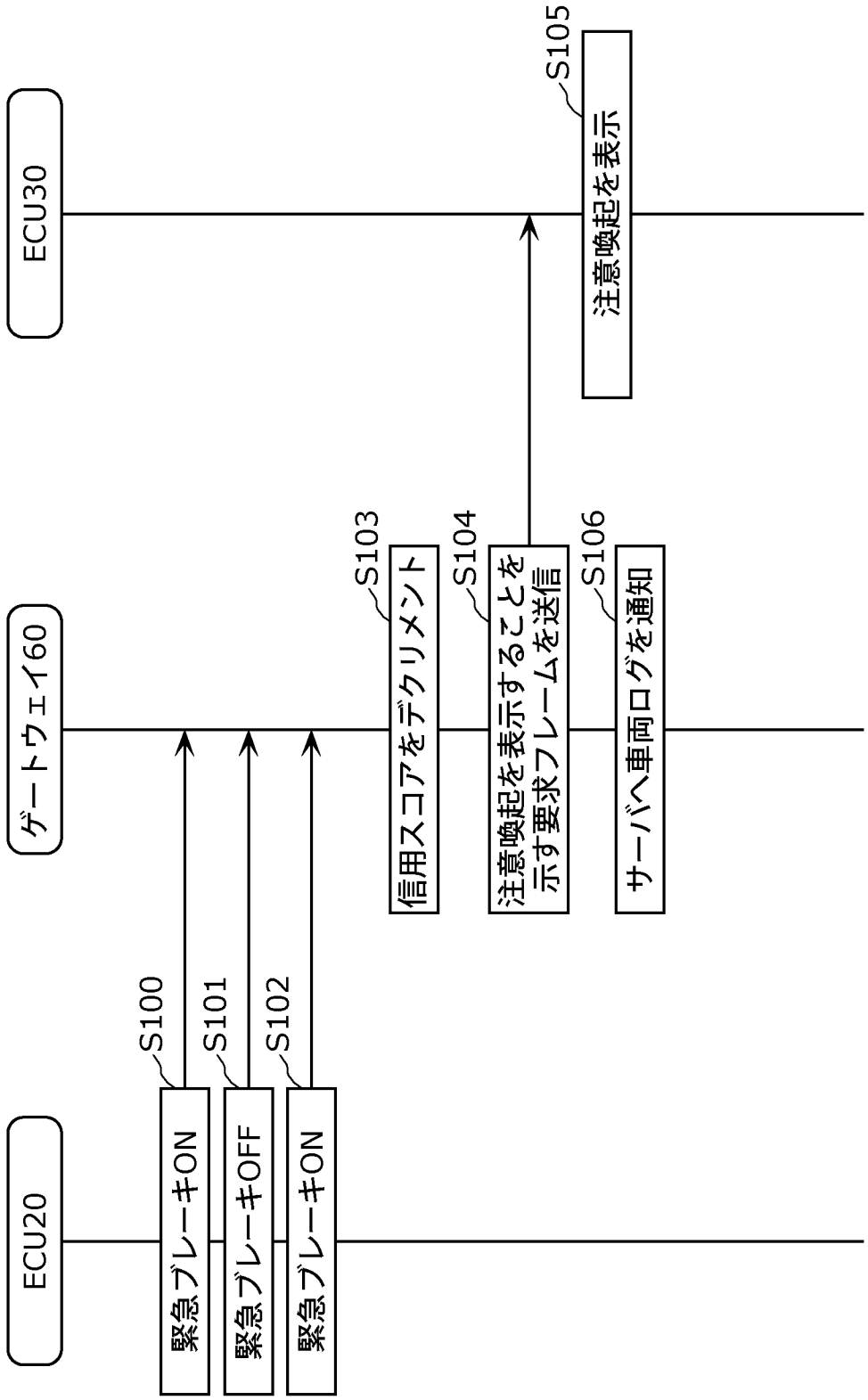
[図7]


S11
信用スコアを算出
START
S1101
診断コマンド
またはアップデート
コマンド?
Yes
No
S1102
該当コマンドの
受信回数を更新
S1103
受信回数が
所定値以上?
Yes
No
S1104
信用スコアを
1デクリメント
END
S1105
運転支援機能ON
コマンド?
Yes
No
S1106
前回機能ONコマンドを
受信した時刻からの
経過時間を更新
S1107
経過時間が
所定値未満?
Yes
No
S1108
急ブレーキ or
急ハンドル or 急アクセル
を検知?
Yes
No
S1109
前回の検知時刻からの
経過時間を更新
S1110
経過時間が
所定値未満?
Yes
No
S1111
エラー
フレーム?
Yes
No
S1112
前回の検知時刻からの
経過時間を更新
S1113
経過時間が
所定値未満?
Yes
No

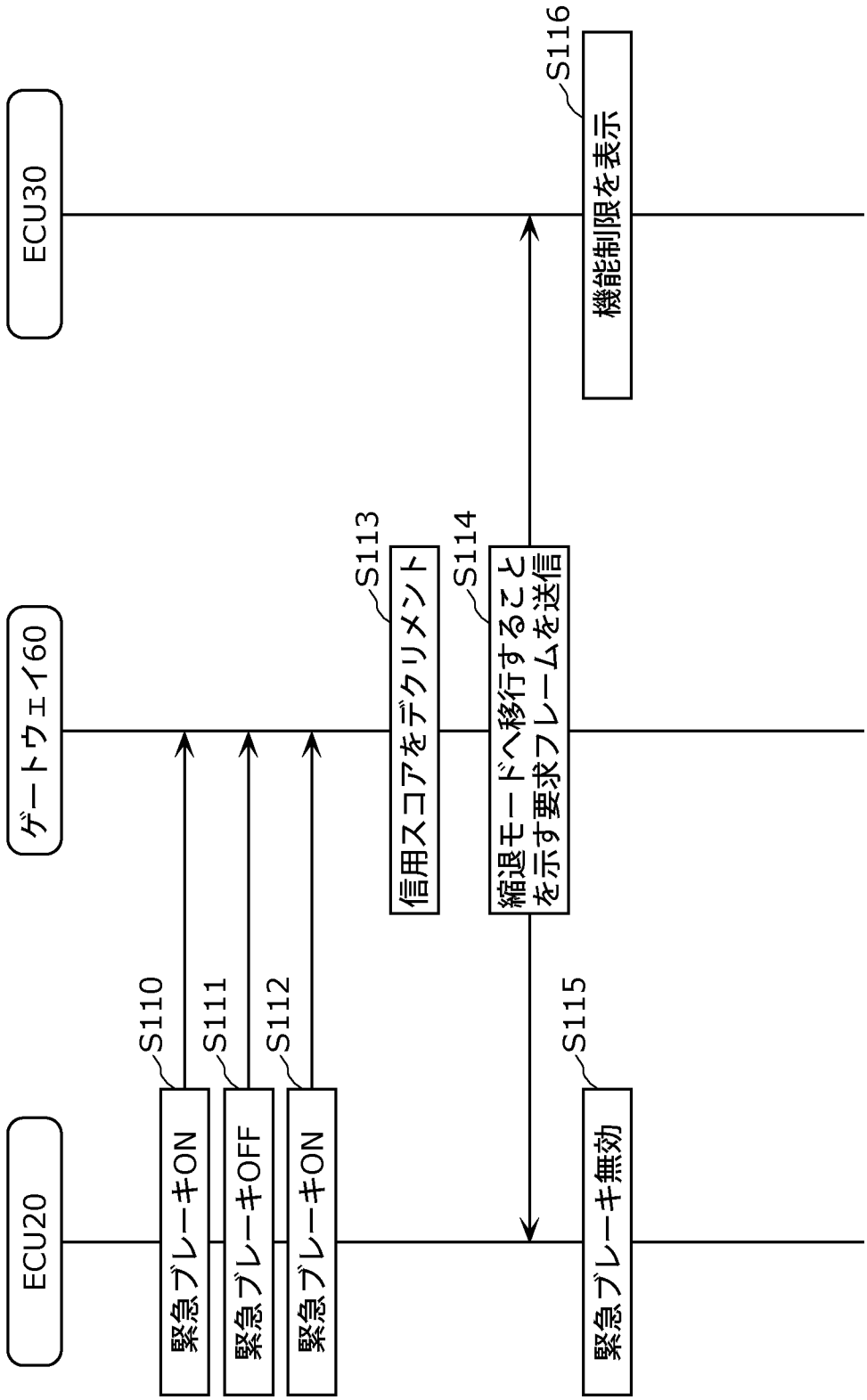
[図8]


S13
監視レベルを変更
START
S1301
信用スコアが30以下?
Yes
No
S1302
縮退モードへ移行
S1303
信用スコアが50以下?
Yes
No
S1304
注意喚起＆
サーバへ通知
S1305
信用スコアが80以下?
Yes
No
S1306
サーバへ通知
END

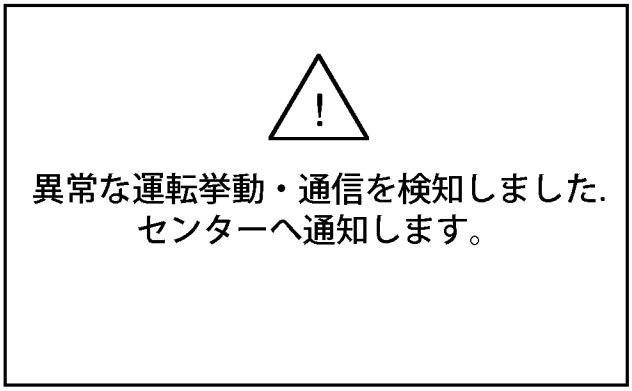
[図9]


ECU20
ゲートウェイ60
ECU30
緊急ブレーキON
緊急ブレーキOFF
緊急ブレーキON
S100
S101
S102
信用スコアをデクリメント
S103
注意喚起を表示することを示す要求フレームを送信
S104
サーバへ車両ログを通知
S106
注意喚起を表示
S105

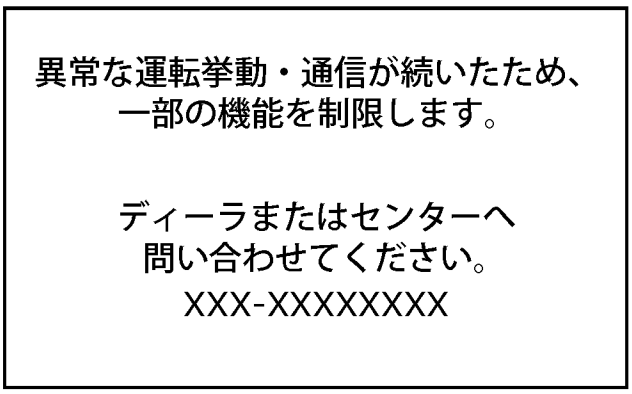
[図10]


ECU20
ゲートウェイ60
ECU30
緊急ブレーキON
緊急ブレーキOFF
緊急ブレーキON
信用スコアをデクリメント
縮退モードへ移行することを示す要求フレームを送信
緊急ブレーキ無効
機能制限を表示
S110
S111
S112
S113
S114
S115
S116

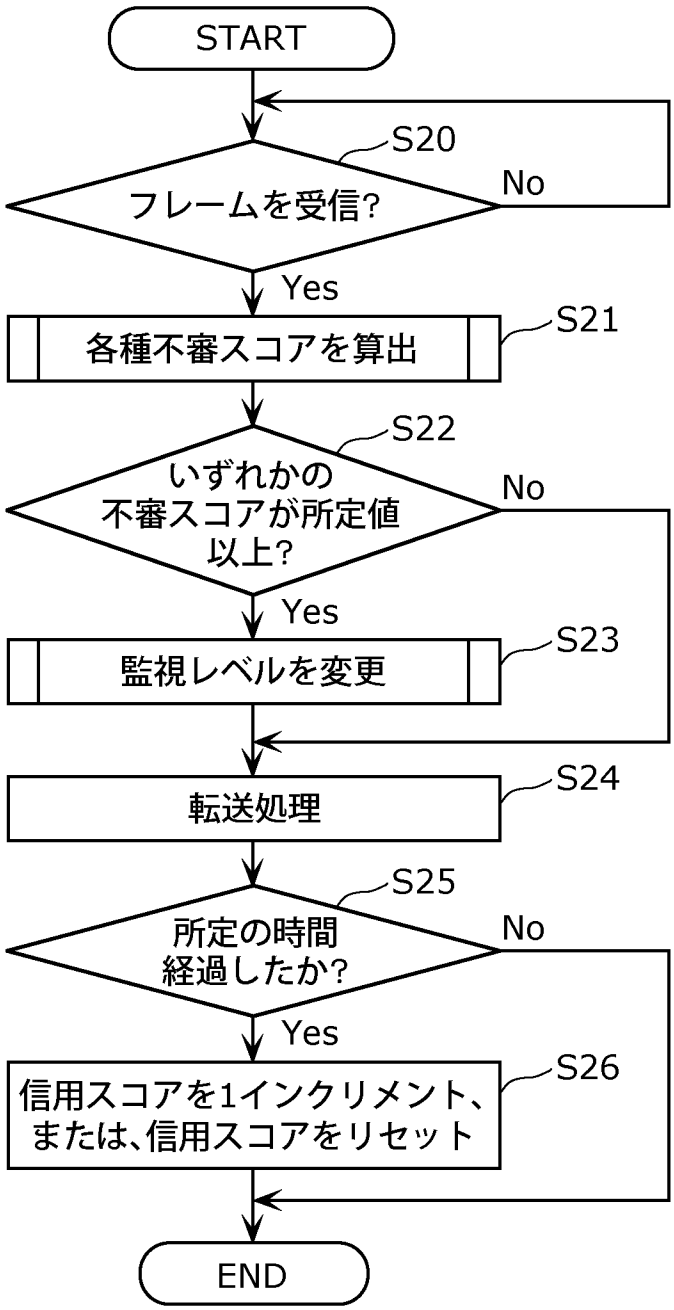
[図11A]


異常な運転挙動・通信を検知しました.
センターへ通知します。

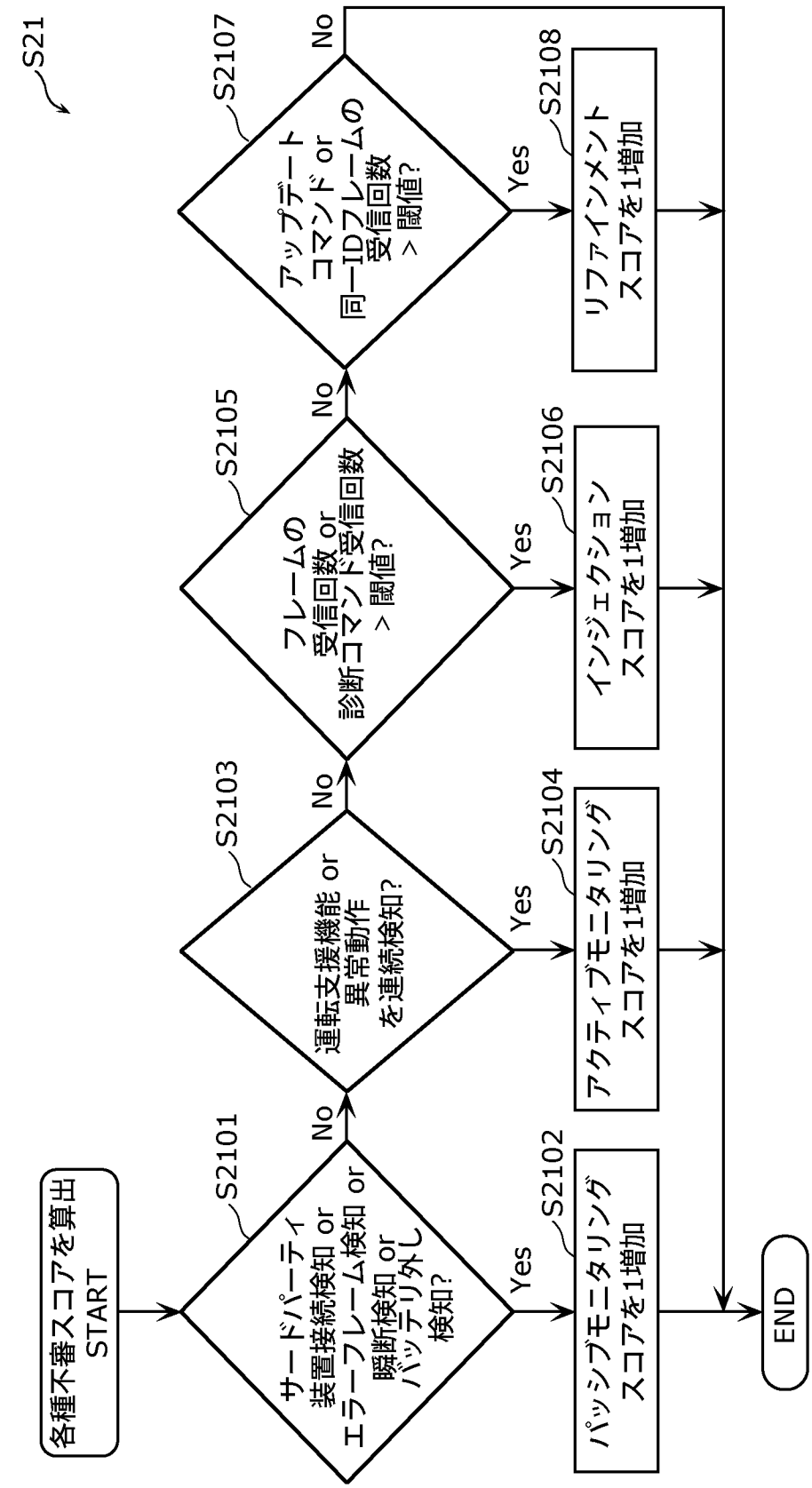
[図11B]


異常な運転挙動・通信が続いたため、
一部の機能を制限します。
ディーラまたはセンターへ
問い合わせてください。
XXX-XXXXXXXX

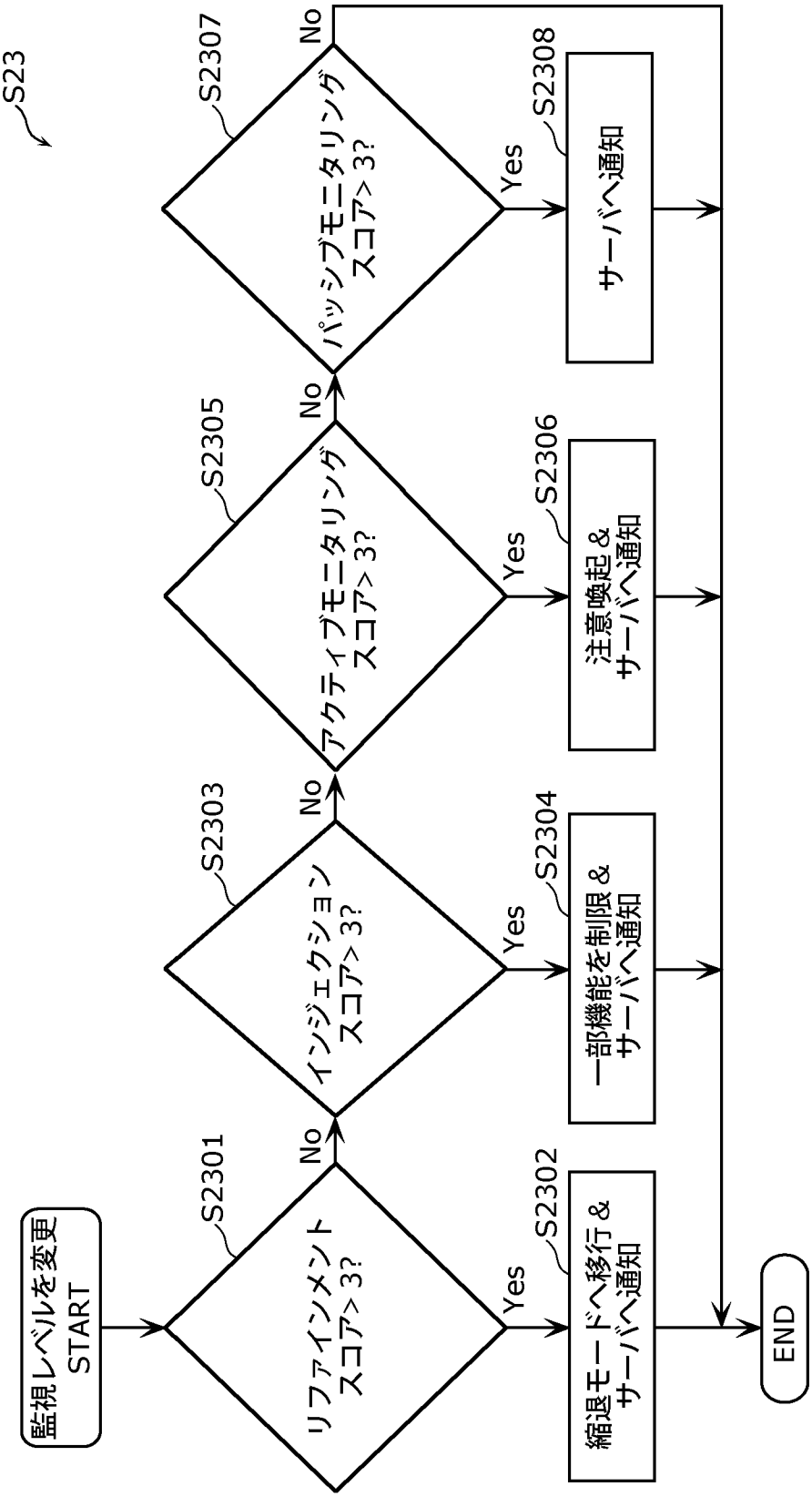
[図12]


START
S20
フレームを受信?
No
Yes
S21
各種不審スコアを算出
S22
いずれかの
不審スコアが所定値
以上?
No
Yes
S23
監視レベルを変更
S24
転送処理
S25
所定の時間
経過したか?
No
Yes
S26
信用スコアを1インクリメント、
または、信用スコアをリセット
END

[図13]


S21
各種不審スコアを算出
START
S2101
サードパーティ
装置接続検知 or
エラーフレーム検知 or
瞬断検知 or
バッテリ外し
検知?
Yes
No
S2102
パッシブモニタリング
スコアを1増加
S2103
運転支援機能 or
異常動作
を連続検知?
Yes
No
S2104
アクティブモニタリング
スコアを1増加
S2105
フレームの
受信回数 or
診断コマンド受信回数
> 閾値?
Yes
No
S2106
インジェクション
スコアを1増加
S2107
アップデート
コマンド or
同一IDフレームの
受信回数
> 閾値?
Yes
No
S2108
リファインメント
スコアを1増加
END

[図14]


S23
監視レベルを変更
START
S2301
リファインメント
スコア> 3?
Yes
No
S2302
縮退モードへ移行 &
サーバへ通知
S2303
インジェクション
スコア> 3?
Yes
No
S2304
一部機能を制限 &
サーバへ通知
S2305
アクティブモニタリング
スコア> 3?
Yes
No
S2306
注意喚起 &
サーバへ通知
S2307
パッシブモニタリング
スコア> 3?
Yes
No
S2308
サーバへ通知
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/031228

A. CLASSIFICATION OF SUBJECT MATTER
G06F 21/55(2013.01)i
FI: G06F21/55 340

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/55

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2017-111796 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 22 June 2017 (2017-06-22) entire text, all drawings	1-13
A	SMITH, Craig, 自動車ハッククラブ訳, カーハッカーズ・ハンドブック, 初版第１刷, 株式会社オライリー・ジャパン, 2017, ISEN 978-4-87311-823-9, pp. 73-98, pp. 73-98, (translated by Car hack club, "The Car Hacker's Handbook", 1st edition 1st printing, O'REILLY JAPAN INC.)	1-13
A	WO 2019/030763 A1 (ARGUS CYBER SECURITY LTD.) 14 February 2019 (2019-02-14) entire text, all drawings	1-13

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 12 November 2020 (12.11.2020)	Date of mailing of the international search report 24 November 2020 (24.11.2020)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/031228

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2017-111796 A	22 Jun. 2017	US 2018/0295147 A1	
		CN 107925600 A	
WO 2019/030763 A1	14 Feb. 2019	JP 2020-530624 A	

国際調査報告

国際出願番号
PCT/JP2020/031228

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/55(2013.01)i
FI: G06F21/55 340

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

G06F21/55

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2017-111796 A (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) 22.06.2017 (2017-06-22) 全文，全図	1-13
A	SMITH,Craig, 自動車ハッククラブ訳, カーハッカーズ・ハンドブック, 初版第１刷, 株式会社オライリー・ジャパン, 2017, ISBN 978-4-87311-823-9, pp.73-98 pp.73-98	1-13
A	WO 2019/030763 A1 (ARGUS CYBER SECURITY LTD.) 14.02.2019 (2019-02-14) 全文，全図	1-13

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

*　引用文献のカテゴリー
"A"　特に関連のある文献ではなく、一般的技術水準を示すもの
"E"　国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
"L"　優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
"O"　口頭による開示、使用、展示等に言及する文献
"P"　国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

"T"　国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
"X"　特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
"Y"　特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
"&"　同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
12.11.2020	24.11.2020

名称及びあて先

日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）

吉田　歩 5S 1206

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/031228

引用文献	公表日	パテントファミリー文献	公表日
JP 2017-111796 A	22.06.2017	US 2018/0295147 A1 CN 107925600 A	
WO 2019/030763 A1	14.02.2019	JP 2020-530624 A	