(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 2021/038870 A1

(51) 国際特許分類:
G06F 21/55 (2013.01) *H04L 12/28* (2006.01)

(21) 国際出願番号： PCT/JP2019/034264

(22) 国際出願日： 2019年8月30日(30.08.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(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).

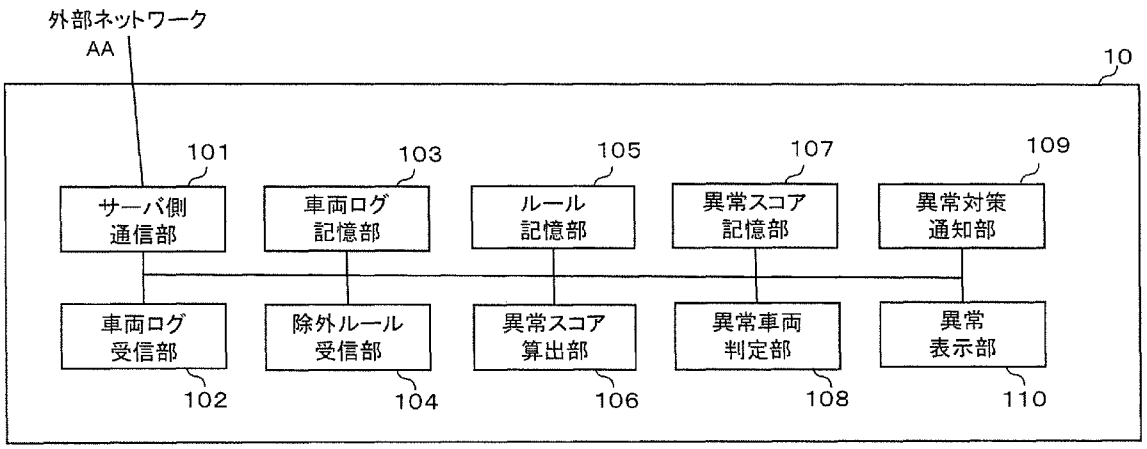
(72) 発明者: 平野 亮(HIRANO, Ryo); 〒5718501 大阪府門真市大字門真１００６番地 パナソニック株式会社内 Osaka (JP). 岸川 剛(KISHIKAWA, Takeshi). 氏家 良浩(UJIIE, Yoshihiro). 芳賀 智之(HAGA, Tomoyuki).

(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,

(54) **Title:** ANOMALOUS VEHICLE DETECTING SERVER AND ANOMALOUS VEHICLE DETECTING METHOD

(54) 発明の名称： 異常車両検出サーバおよび異常車両検出方法



101 Server-side communication unit
102 Vehicle log reception unit
103 Vehicle log storage unit
104 Exception rule reception unit
105 Rule storage unit
106 Anomaly score calculation unit
107 Anomaly score storage unit
108 Anomalous vehicle determination unit
109 Anomaly countermeasure notification unit
110 Anomaly display unit
AA External network

(57) **Abstract:** According to the present disclosure, a suspicious behavior indicative of a reverse engineering activity of an attacker is sensed from a vehicle log collected on a server, an anomaly score is calculated, and an anomalous vehicle is detected. Further, an appropriate countermeasure is selected on the basis of the anomaly score, thereby making it possible to monitor a suspicious vehicle in a focused manner and to analyze the vehicle with priority.

(57) 要約：本開示によれば、サーバ上で収集した車両ログから、攻撃者によるリバースエンジニアリング活動が疑われる不審な挙動を検知し、異常スコアを算出し、異常車両を検出する。さらに異常スコアに基づいて、適切な対策を選択することで不審な車両を重点的に監視、優先的に解析することを可能とする。

WO 2021/038870 A1

[続葉有]

HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(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)）

明　細　書

発明の名称 ： 異常車両検出サーバおよび異常車両検出方法

技術分野

[0001] 本開示は、車両ログのイベント内容に基づいて車両ごとに異常スコアを算出し、同一車種の平均異常スコアよりも高い異常スコアを有する車両を異常車両として検出する技術に関する。

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（以下、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を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）という規格が存在し、さらに、自動運転やコネクテッドカーの普及に伴い、車載ネットワークトラフィックの増大が予想され、車載Ｅｔｈｅｒｎｅｔ（登録商標）の普及が進んでいる。

[0003] 一方で、車載システムに侵入し、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、従来のＩｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ（ＩＰ）通信で用いられてきた、非特許文献１のように、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や、特許文献１にように、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の制御を奪わる、鍵が漏洩する等の場合には、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。また、特許文献１の方法は、不正なフレームを送信されたことによる異常への対処であり、攻撃の発生を未然に防ぐわけではない。一般に、車両の不正制御を試みる攻撃者は、事前に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車載ネットワークのリバースエンジニアを事前に行う。この時の車載ネットワークのフレーム調査段階における、攻撃者の活動を把握することができれば、フレームの調査段階を攻撃発生の予兆として捉え、攻撃者の調査の妨害や、対象車両の重点監視等のアクションにつなげることができ、より安全性を高めることができる。

[0007] そこで、本開示は、複数車両の車両ログをサーバ上で監視し、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不審挙動を捉え、車両がリバースエンジニアをされている可能性の高さを異常スコアとして算出し、同一車種の平均異常スコアよりも高い異常スコアを有する車両を異常車両として検出し、異常スコアの値と異常カテゴリに基づいて異常に対して対策する異常車両検出方法を提供する。

課題を解決するための手段

[0008] 上記目的を達成するために、車両システムにおいて発生したイベント内容のデータを含む車両ログを１以上の車両から受信する異常車両検出サーバであって、受信した車両ログのイベント内容に基づいて、通常の運転とは異なる不審挙動を検出し、前記車両ログと対応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異常スコアを算出する異常スコア算出部と、前記異常スコアが所定値以上の場合に、前記車両を異常車両として

判定する異常車両判定部とを備える、異常車両検出サーバを提供する。

発明の効果

[0009] 本開示によれば、車載システムにおいて、攻撃者が車両を不正制御するためのリバースエンジニアリング活動が疑われる不審な挙動を検知し、異常スコアを算出する。さらに異常スコアの値と異常カテゴリに基づいて、異常に対して対策を実施することで車載システムのセキュリティを維持することを可能とする。

図面の簡単な説明

[0010] [図1]図１は、実施の形態１における、異常車両検出システムの全体構成図である。

[図2]図２は、実施の形態１における、車両システムの構成図である。

[図3]図３は、実施の形態１における、異常車両検出サーバの構成図である。

[図4]図４は、実施の形態１における、車両ログ送信装置の構成図である。

[図5]図５は、実施の形態１における、車両ログ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、異常ルールの一例を示す図である。

[図7]図７は、実施の形態１における、除外ルールの一例を示す図である。

[図8]図８は、実施の形態１における、異常スコアの一例を示す図である。

[図9]図９は、実施の形態１における、対策ルールの一例を示す図である。

[図10]図１０は、実施の形態１における、異常リスト表示画面の一例を示す図である。

[図11]図１１は、実施の形態１における、異常エリア表示画面の一例を示す図である。

[図12]図１２は、実施の形態１における、異常階層表示画面の一例を示す図である。

[図13]図１３は、実施の形態１における、車両ログ受信処理のシーケンスを示す図である。

[図14]図１４は、実施の形態１における、外部ログ受信処理のシーケンスを示す図である。

[図15]図１５は、実施の形態１における、異常スコア算出処理のシーケンスを示す図である。

[図16]図１６は、実施の形態１における、異常対策処理のシーケンスを示す図である。

[図17]図１７は、実施の形態１における、異常表示処理のシーケンスを示す図である。

[図18]図１８は、実施の形態１における、車両別異常スコア算出処理のフローチャートである。

[図19]図１９は、実施の形態１における、車種別異常スコア算出処理のフローチャートである。

[図20]図２０は、実施の形態１における、エリア別異常スコア算出処理のフローチャートである。

[図21]図２１は、実施の形態１における、異常車両判定処理のフローチャートである。

[図22]図２２は、実施の形態１における、異常対策処理のフローチャートである。

発明を実施するための形態

[0011] 本開示の一実施態様の異常車両検出サーバは、車両システムにおいて発生したイベント内容のデータを含む車両ログを１以上の車両から受信する異常車両検出サーバであって、受信した車両ログのイベント内容に基づいて、通常の運転とは異なる不審挙動を検出し、前記車両ログと対応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異常スコアを算出する異常スコア算出部と、前記異常スコアが所定値以上の場合に、前記車両を異常車両として判定する異常車両判定部と、を備える、異常車両検出サーバである。

[0012] 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るため効果的である。

[0013] また、前記異常車両判定部は、さらに、一の車両に対して算出された異常スコアと、前記一の車両と同一の車種の異常スコアに基づく統計値を比較し、前記一の車両が異常車両であるか否かを判定するとしてもよい。

[0014] これにより、特定の車種において発生する可能性が高い異常を除外することができ、同一車種の他の車両では発生数が少なく、より疑わしい異常および車両を抽出できるため効果的である。

[0015] また、前記異常車両判定部は、一の車両に対して算出された異常スコアと、前記一の車両と同一のエリアに位置する車両の異常スコアに基づく統計値を比較し、前記一の車両が異常車両であるか否かを判定するとしてもよい。

[0016] これにより、特定のエリアにおいて発生する可能性が高い異常を除外することができ、同一エリアに位置する他の車両では発生数が少なく、より疑わしい異常および車両を抽出できるため効果的である。

[0017] また、前記異常スコア算出部は、ネットワーク機器接続頻発または、インターネット接続異常、アクセス先アドレスの変化、アクセス元アドレスの変化、ネットワークログイン試行のいずれかを不振挙動として検出し、前記不審挙動が発生した場合に、ネットワーク解析活動と判定し、車両に対して異常スコアを増加させるとしてもよい。

[0018] これにより、攻撃者が車両システムの通信機能を解析しようとする試行をとらえることができるため効果的である。

[0019] また、さらに、異常対策通知部を備え、前記異常スコア算出部が、前記不審挙動をネットワーク解析活動と判定した場合、前記異常対策通知部は、異常スコアの値に応じて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告のいずれか１つ以上の対策を実施してもよい。

[0020] これにより、攻撃者が車両システムの通信機能を解析しようとする試行を妨害することができるため効果的である。

[0021] また、前記異常スコア算出部は、車両制御機能頻発、システムエラー頻発、システムエラー削除、システムログイン、ファイル数またはプロセス数の

変化のいずれかを不審挙動として検出し、前記不審挙動が発生した場合に、システム解析活動と判定し、車両に対して異常スコアを増加させるとしてもよい。

[0022] これにより、攻撃者が車両システムの車両制御機能やホストマシン自体を解析しようとする試行をとらえることができるため効果的である。

[0023] また、さらに、異常対策通知部を備え、前記異常スコア算出部が、前記不審挙動をネットワーク解析活動と判定した場合、前記異常対策通知部は、異常スコアの値に応じて、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの警告のいずれか１つ以上の対策を実施してもよい。

[0024] これにより、攻撃者が車両システムの車両制御機能やホストマシン自体を解析しようとする試行を妨害することができるため効果的である。

[0025] また、前記異常スコア算出部は、前記不審挙動を検出した場合であっても、所定の期間内に前記不審挙動が発生した場合または所定のエリアにて前記不審挙動が発生した場合は、異常スコアを増加させないとしてもよい。

[0026] これにより、開発者が車両システムの検証のために不審挙動を発生させている場合や、修理業者がエラー解除している場合、車両システムのソフトウェア更新によってファイル数が変わる場合など、誤検知を防ぐことができるため効果的である。

[0027] また、前記異常スコア算出部は、所定の期間中に前記不審挙動が発生しなかった場合は、異常スコアを減少させるとしてもよい。

[0028] これにより、攻撃者が攻撃対象車両を通常走行に用いる可能性は低いと考えられるため、しばらく通常走行され、不審な挙動が発生しなかった場合は、攻撃対象車両である可能性が低いと考えられるため効果的である。

[0029] また、前記異常車両検出サーバは、さらに、前期異常車両判定装置が異常車両と判定した車両に対して、前記異常スコアの値または前記不審挙動の種別に基づいて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告

、ネットワーク接続制限と、車両制御機能制限、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策を要求する異常通知部を備えるとしてもよい。

[0030] 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に対して、車両制御機能を制限することで攻撃者の解析を妨げることや、車両ログの種類数を増やして、攻撃内容を解析することが可能となり効率的である。

[0031] また、前記異常車両検出サーバは、さらに、前期異常車両判定装置が異常車両と判定した車両と同一の車種に対して、前記異常スコアの値または前記不審挙動の種別に基づいて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告、ネットワーク接続制限と、車両制御機能制限、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策を要求する異常通知部を備えるとしてもよい。

[0032] 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種に対して、車両制御機能を制限することで攻撃者の解析を妨げることや、車両ログの種類数を増やして、攻撃内容を解析することが可能となり効率的である。

[0033] また、前記異常車両検出サーバは、さらに、前期異常車両判定装置が異常車両と判定した車両と同一のエリアに位置する車両に対して、前記異常スコアの値または前記不審挙動の種別に基づいて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告、ネットワーク接続制限と、車両制御機能制限、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策を要求する異常通知部を備えるとしてもよい。

[0034] 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エリアに対して、車両制御機能を制限することで攻撃者の解析を妨げることや、車両ログの種類数を増やして、攻撃内容を解析することが可能となり効率的である。

[0035] また、前記異常車両検出サーバは、前記異常スコアが高い順に異常車両をリスト表示する異常表示部を備えるとしてもよい。

[0036] これにより、異常表示部の表示内容を確認して異常車両を解析するオペレーターが、より疑わしい車両から優先的に解析することができるため効果的である。

[0037] また、前記異常車両検出サーバは、前記異常車両と判定された車両の位置情報を地図上に表示する異常車両表示部を備えるとしてもよい。

[0038] これにより、異常表示部の表示内容を確認して異常車両を解析するオペレーターが、異常車両がどのエリアに位置していて、どの施設で異常が発生しているかを判断でき、解析の手がかりとすることができるため効果的である。

[0039] また、前記異常車両検出サーバは、車両に対する攻撃を、攻撃の進行度に応じて階層別に表示し、前記異常車両と判定された車両または車種、位置情報のいずれか一つの情報を、攻撃の進行度が低い偵察フェーズの階層に表示する異常車両表示部を備えるとしてもよい。

[0040] これにより、異常表示部の表示内容を確認して異常車両を解析するオペレーターが、異常車両に対する攻撃の進行度が分かるため、解析の優先度をつけることができるため効果的である。

[0041] 以下、図面を参照しながら、本開示の実施の形態に関わる異常車両検出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。

[0042] （実施の形態１）

［１　異常車両検出システムの全体構成図］

図１は、本実施の形態に関わる異常車両検出システムの全体構成を示す図である。異常車両検出システムは、異常車両検出サーバ１０、車両システム２０、除外ルール共有サーバ３０、車両ログ送信装置２００から構成され、外部ネットワークを介して異常車両検出サーバ１０と、除外ルール共有サーバ３０、車両システム２０が接続される。外部ネットワークは、例えば、インターネットである。外部ネットワーク５０の通信方法は、有線であっても無線であっても良い。また、無線通信方式は既存技術であるＷｉ－Ｆｉ（登録商標）や、３Ｇ／ＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）であっても良い。

[0043] 車両システム２０は、車両ログ送信装置２００を備え、車両ログ送信装置２００は、外部ネットワークを介して、車両ログを異常車両検出サーバ１０へ送信する装置である。車両ログの詳細は後述する。図では、車両システム２０は１台のみ記載しているが、１以上の車両システム２０それぞれが、車両ログを異常車両検出サーバ１０へ送信する。

[0044] 除外ルール共有サーバ３０は、異常車両検出サーバ１０が利用する除外ルールを異常車両検出サーバ１０へ送信するサーバである。除外ルールは、例えば、車両システムの開発者によって作成され、除外ルール共有サーバ３０へアップロードされる。車両システムのソフトウェアアップデートのリストや、ディーラーまたは開発拠点、検証拠点、ディーラー、修理業者のリストである。除外ルールには、異常車両検出サーバ１０が車両ログのイベント内容と異常ルールを参照して異常スコアを算出する際に、除外対象となる異常ルールと、その期間と位置情報の少なくとも１つ以上が記載される。除外ルールの詳細は後述する。

[0045] 異常車両検出サーバ１０は車両ログ送信装置２００から車両ログを受信し、除外ルール共有サーバ３０から除外ルールを受信し、車両ログと、除外ルールと、事前に記憶された車両ログを異常と判定する条件が記載された異常ルールに基づいて車両ごとに異常スコアを算出し、異常車両を検出するサーバである。異常スコアの算出方法および異常車両の判定方法の詳細は後述する。

[0046] ［２　車両システムの構成図］

図２は、車両システム２０の構成図である。車両システム２０は、車両ログ送信装置２００からと、セントラルＥＣＵ３００と、ＺｏｎｅＥＣＵ４００ａと、ＺｏｎｅＥＣＵ４００ｂと、ＺｏｎｅＥＣＵ４００ｃと、ＺｏｎｅＥＣＵ４００ｄと、ボディＥＣＵ５００ａと、カーナビＥＣＵ５００ｂと、ステアリングＥＣＵ５００ｃと、ブレーキＥＣＵ５００ｄを備え、車両ログ送信装置２００と、セントラルＥＣＵ３００と、ＺｏｎｅＥＣＵ４００ａと、ＺｏｎｅＥＣＵ４００ｂと、ＺｏｎｅＥＣＵ４００ｃと、ＺｏｎｅＥＣＵ４００ｄは、車載ネットワークであるイーサネット（登録商標）１３を介して接続される。ボディＥＣＵ５００ａとＺｏｎｅＥＣＵ４００ａはイーサネット１１を介して接続され、カーナビＥＣＵ５００ｂとＺｏｎｅＥＣＵ４００ｂはイーサネット１２を介して接続され、ステアリングＥＣＵ５００ｃとＺｏｎｅＥＣＵ４００ｃはＣＡＮ１４を介して接続され、ブレーキＥＣＵ５００ｄとＺｏｎｅＥＣＵ４００ｄはＣＡＮ－ＦＤ１５を介して接続される。車両ログ送信装置２００と、セントラルＥＣＵ３００は外部ネットワークにも接続される。

[0047] 車両ログ送信装置２００は、イーサネット１３を介して、セントラルＥＣＵ３００から車両ログを収集し、外部ネットワークを介して、収集した車両ログを異常車両検出サーバ１０へ送信する装置である。

[0048] セントラルＥＣＵ３００は、ＺｏｎｅＥＣＵ４００ａ、ＺｏｎｅＥＣＵ４００ｂ、ＺｏｎｅＥＣＵ４００ｃ、ＺｏｎｅＥＣＵ４００ｄと、イーサネット１３を介して、ＺｏｎｅＥＣＵ４００ａ、ＺｏｎｅＥＣＵ４００ｂ、Ｚｏ

ｎｅＥＣＵ４００ｃ、ＺｏｎｅＥＣＵ４００ｄを制御し、車両システム全体を制御する。例えば、自動駐車や自動運転などの車両制御機能を制御する。また、車両システム内で発生したネットワーク機器の接続やインターネット接続異常などイベント情報をＺｏｎｅＥＣＵ４００ａ～ｄから収集し、収集したイベント情報を車両ログとして記憶し、車両ログを車両ログ送信装置２００へ送信する。

[0049] ＺｏｎｅＥＣＵ４００ａ、ＺｏｎｅＥＣＵ４００ｂ、ＺｏｎｅＥＣＵ４００ｃ、ＺｏｎｅＥＣＵ４００ｄは、イーサネット１３を介して、セントラルＥＣＵ３００と他のＺｏｎｅＥＣＵと通信し、ＺｏｎｅＥＣＵ４００ａは、イーサネット１３を介して、ボディＥＣＵ５００ａと通信し、車両のロックやワイパーなど車体に関わる機能を制御し、ＺｏｎｅＥＣＵ４００ｂは、イーサネット１１を介して、カーナビＥＣＵ５００ｂと通信し、カーナビの表示を制御し、ＺｏｎｅＥＣＵ４００ｃは、ＣＡＮ１４を介して、ステアリングＥＣＵ５００ｃと通信し、ステアリングの操舵を制御し、ＺｏｎｅＥＣＵ４００ｄは、ＣＡＮ－ＦＤ１５を介して、ブレーキＥＣＵ５００ｄと通信し、ブレーキを制御する機能を有するＥＣＵである。

[0050] ボディＥＣＵ５００ａは車両に搭載される車体に関わる機能を制御するＥＣＵである。

[0051] カーナビＥＣＵ５００ｂは車両に搭載されるカーナビの表示を制御するＥＣＵである。

[0052] ステアリングＥＣＵ５００ｃは車両に搭載されるステアリングの操舵を制御するＥＣＵである。

[0053] ブレーキＥＣＵ５００ｄは車両に搭載されるブレーキを制御するＥＣＵである。

[0054] ［３　異常車両検出サーバの構成図］

図３は、異常車両検出サーバ１０の構成図である。異常車両検出サーバ１０は、サーバ側通信部１０１と、車両ログ受信部１０２と、車両ログ記憶部１０３と、除外ルール受信部１０４と、ルール記憶部１０５と、異常スコア

算出部１０６と、異常スコア記憶部１０７と、異常車両判定部１０８と、異常対策通知部１０９と、異常表示部１１０とで構成される。

[0055] サーバ側通信部１０１は、外部ネットワークを介して、車両ログ送信装置２００から車両ログを受信し、車両ログ受信部１０２へ送信する。また、除外ルール共有サーバ３０から除外ルールを受信し、除外ルールを除外ルール受信部１０４へ送信する。

[0056] 車両ログ受信部１０２は、サーバ側通信部１０１から車両ログを受信し、車両ログ記憶部１０３へ記憶する。

[0057] 除外ルール受信部１０４は、サーバ側通信部１０１から除外ルールを受信し、ルール記憶部１０５へ記憶する。

[0058] ルール記憶部１０５は、事前に、車両ログに含まれるイベントのうち異常と判定する条件が記載された異常ルールと、異常ルールに記載された異常カテゴリと異常スコアに応じた対策内容が記載された対策ルールを記憶する。また、除外ルール受信部１０４が除外ルール共有サーバ３０から受信した除外ルールを記憶する。

[0059] 異常スコア算出部１０６は、車両ログを受信すると、ルール記憶部１０５から異常ルールと除外ルールを取得し、車両ログに記載されたイベントと、異常ルールと、除外ルールに基づき、車両１台ごとに異常スコアを算出する。そして、異常スコア記憶部１０７に異常スコアを記録する。異常スコアの算出方法の詳細については後述する。

[0060] 異常車両判定部１０８は、異常スコア記憶部１０７が記憶する異常スコアを参照し、攻撃を試行されていると推測される異常車両を検出する。異常車両の検出方法の詳細については後述する。

[0061] 異常対策通知部１０９は、異常車両判定部１０８が異常車両と判定した車両または異常車両と同一の車種、異常車両と同一のエリアに位置する車両に対して、異常対策通知を送信する。異常対策通知は、例えば、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告、ネットワーク接続制限と、

車両制御機能制限、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策であり、車両システム２０の車両ログ送信装置２００またはセントラルＥＣＵ３００へ通知することとで実現する。

[0062] 異常表示部１１０は、異常車両判定部１０８が異常車両と判定した車両または異常車両と同一の車種、異常車両と同一のエリアに位置する車両をユーザに対して表示する。例えば、異常車両検出サーバ１０を利用して解析を行うオペレーターがユーザであり、グラフィカルユーザーインターフェースを用いて表示する。

[0063] ［４　車両ログ送信装置の構成図］

図４は、車両ログ送信装置の２００の構成図である。車両ログ送信装置は、車両側通信部２１０と、車両ログ送信部２２０と、異常対策部２３０と、で構成される。

[0064] 車両側通信部２１０は、外部ネットワークを介して、異常車両検出サーバ１０と接続され、情報を交換する。

[0065] 車両ログ送信部２２０は、イーサネット１３を介して、セントラルＥＣＵ３００と接続され、セントラルＥＣＵ３００から車両ログを受信し、車両側通信部２１０を経由して、異常車両検出サーバ１０へ車両ログを送信する。

[0066] 異常対策部２３０は、異常車両検出サーバ１０が異常車両を検出した場合、異常車両検出サーバ１０が送信した異常対策通知を受信し、異常対策通知の内容に応じて、セントラルＥＣＵ３００または車両ログ送信部２２０へ対策を指示する。例えば、対策通知内容が車両制御機能制限である場合はセントラルＥＣＵ３００へ機能制限を指示し、対策通知内容が車両ログの送信頻度の増加であれば、車両ログ送信部２２０へ送信頻度の増加を指示する。

[0067] ［５　車両ログの一例］

図５は、車両ログ記憶部１０３に格納される車両ログの一例である。車両ログは車両システム内で発生したイベント内容であり、異常スコア算出部１０６が異常スコアを算出する際に用いられる。車両ログは、イベントごとに

、車両ログ番号、車両識別子、車種、時刻、車両位置情報、イベント名で構成される。図では、車両ログは番号が１である行では、車両と１対１で対応する車両識別子が「Ａ１」であり、車両の車種を表す車種が「Ａ」であり、イベント発生時刻を表す時刻が「ＴＡ１１」であり、イベント発生時の車両の位置を表す車両位置情報が「Ｘ１、Ｙ１」であり、イベント名が「ネットワーク機器登録」であることを示している。例えば、車両位置情報はＧＰＳ情報を用いてイベントが発生した時刻における車両の位置情報である。ネットワーク機器登録およびネットワーク機器削除は、例えば、スマートフォンがＢｌｕｅｔｏｏｔｈ（登録商標）でカーナビＥＣＵ５００ｂと接続または削除されたイベントである。または、タブレット機器がカーナビＥＣＵ５００ｂとＷｉ－Ｆｉで接続または削除されたイベントである。

[0068] また、車両制御機能作動は、緊急ブレーキ作動や自動駐車モードの起動など、車両システムを制御する機能が作動したイベントである。

[0069] また、システムエラー発生は、セントラルＥＣＵ３００が、ＺｏｎｅＥＣＵ４００ａ～ｄ上で発生したエラーまたは、イーサネット１３、イーサネット１１、イーサネット１２、ＣＡＮ１４、ＣＡＮ－ＦＤ１５上にて発生したネットワークエラーが発生したイベントであり、システムエラー解除は、ディーラー等で利用される車両診断ツールを用いて、システムエラーを解除されたイベントである。

[0070] また、アドレスＡへアクセスは、カーナビＥＣＵ５００ｂがアドレスＡのＷｅｂサーバに対してアクセスしたイベントである。

[0071] また、アドレスＢからアクセスは、また、アドレスＢのサーバからカーナビＥＣＵ５００ｂに対してアクセスがあったイベントである。

[0072] また、システムログインは、カーナビＥＣＵ５００ｂに対してログインが試行されたイベントである。

[0073] ファイル数増加は、セントラルＥＣＵ３００上に格納されるファイルの種類数が増加したイベントである。

[0074] つまり、車両識別子が同一で、イベント名がネットワーク機器登録である

行と、イベント名がネットワーク機器削除である行を参照することで、時刻ＴＡ１１からＴＡ１２の間で、ネットワーク機器が１個接続され、その後１個減少したことが分かる。

[0075] また、車両識別子が同一で、イベント名がインターネット切断である行と、直近の時刻で発生したイベント名がインターネット接続の行を参照することで、時刻の差からインターネット切断時間を得ることができる。ＶＰＮ切断およびＶＰＮ接続についても同様である。

[0076] また、アドレスＡへのアクセスアクセス先アドレスの変化車両ログ番号が７である行と８である行の車両ログを参照することで、緊急ブレーキが、時刻ＴＡ２３に「Ｘ１、Ｙ１」というエリアで発動し、時刻ＴＡ２４に、「Ｘ１、Ｙ１」というエリアで発動したことがわかる。以降では車両位置情報をエリアとして表記することもある。

[0077] また、車両ログ番号が７である行と８である行の車両ログを参照することで、緊急ブレーキが、時刻ＴＡ２３に「Ｘ１、Ｙ１」というエリアで発動し、時刻ＴＡ２４に、「Ｘ１、Ｙ１」というエリアで発動したことがわかる。以降では車両位置情報をエリアとして表記することもある。

[0078] また、イベント名がアドレスＡへアクセスのイベントと、イベント名がアドレスＢへのアクセスのイベントを参照すれば、カーナビＥＣＵ５００ｂが２のアドレスへアクセスしたことが分かるため、アクセス先アドレスの変化を取得することができる。

[0079] また、イベント名がファイル数またはプロセス数が増加のイベントを複数参照すれば、ファイル数またはプロセス数の変化を取得することができる。

[0080] ［６　異常ルールの一例］

図６は、ルール記憶部１０５に格納される異常ルールの一例である。異常ルールは異常ルール番号、異常ルール内容、期間、回数、異常スコア、異常カテゴリからなる。図のルール番号「１」の行では、ルール内容が「ネットワーク機器接続」であり、期間が「１時間」であり、回数が「４」であり、異常スコアが「＋１」であることが分かる。例えば、車両ログから１時間以

内のネットワーク接続数を取得し、４回以上であれば、異常スコアを「＋１」するというルールが記載される。また、期間「―」は期間を考慮しないことを示し、例えば、異常ルール番号が８の行では、車両ログからシステムログイン回数を取得し、１回以上であれば異常スコアを「＋５」するというルールが記載される。

[0081] ネットワーク機器接続は、攻撃者がスマートフォンなどの端末を車両システムにつなげることで、侵入を図る際に増加するため、１時間に４回の接続は異常として判定する。

[0082] インターネットまたはＶＰＮ遮断は、攻撃者が車両システムと車両システムと接続されるサーバの通信を傍受する場合または、攻撃者が攻撃発覚を恐れて意図的に切断する場合に発生するため、１０分間で１回以上発生した場合に異常として判定する。

[0083] アクセス先アドレスの変化は、攻撃者が車両システムに対して、悪意のあるＵＲＬへアクセスさせようと試行した際に変化するため、１回で異常として判定する。

[0084] アクセス元アドレスの変化は、攻撃者が車両システムに対して、ポートスキャンなど攻撃を試行した際に変化するため、１回で異常として判定する。

[0085] 車両制御機能作動は、攻撃者が緊急ブレーキの発動コマンドを調査する際に、緊急ブレーキを複数回発動させる際に発生するため、１時間に１０回以上で異常として判定する。

[0086] システムエラー発生は、攻撃者が車両システムをブルートフォース攻撃した際に、エラーとなるような通信を発生させてしまう場合に発生するため、２４時間以内に２回以上で異常として判定する。

[0087] システムエラー解除は、攻撃者がシステムエラーを発生させてしまった場合に、車両診断ツールなどを用いて自らシステムエラーを消去する場合に発生するため、１回以上で異常として判定する。

[0088] システムログインは、攻撃者が車両システムに対してユーザログインを試行した場合に発生するため、１回で異常として判定する。

[0089] ファイル数またはプロセス数の変化は、攻撃者がマルウェアを車両システムにインストールした際に、ファイル数が増加または、プロセス数が増加するため、１回以上で異常として判定する。

[0090] 異常カテゴリは、ネットワーク解析またはシステム解析のいずれかが記載され、ネットワーク解析は攻撃者が車両システムの通信機能を解析している可能性が高いことを示し、ネットワーク解析は攻撃者が車両システムのホストマシンを解析している可能性が高いことを示す。異常カテゴリは異常対策時に、効果的な異常対策手段を選択するために利用される。

[0091] ［７　除外ルールの一例］

図７は、ルール記憶部１０５に格納される除外ルールの一例である。図では、１つの除外ルールごとに、除外ルール番号、位置情報、有効期間、内容、除外対象異常ルールが記載される。

[0092] 図の除外ルール番号が３である行では、位置情報がＸ６．Ｙ６であり、有効期限が設定なしを表す「―」であり、内容が修理業者Ａであり、除外対象ルールがシステムエラー解除である。つまり、位置情報Ｘ６．Ｙ６には、修理業者Ａが存在するため、システムエラーを専用ツールで解除する可能性があるため、異常ルールにおいてシステムエラー解除のイベントを異常と判定せずに、異常スコアをカウントしないことを表す。

[0093] また、図の除外ルール番号が４である行では、位置情報「日本」、有効期間「Ｔ３～Ｔ４」、内容「ソフト更新」、除外対象ルール「ファイル数の変化またはプロセス数の変化」である。つまり、有効期間Ｔ３～Ｔ４の間は、車両システムのソフトウェア更新のため、ファイル数が増えることがあるため、ファイル数またはプロセス数の変化を異常と判定せず、異常スコアをカウントしないことを表す。

[0094] また。図の番号Ｍの行では、位置情報Ｘ４、Ｙ４ではトンネルがあることがわかるため、攻撃者によらないインターネットまたはＶＰＮ切断であることから、異常と判定せずに異常スコアをカウントしないことを表す。

[0095] ［８　異常スコアの一例］

図８は、異常スコア記憶部１０７に格納される異常スコアの一例である。異常スコアは異常スコア算出部１０６によって車両ログと、異常ルールと、除外ルールを用いて算出される。異常スコアは、車両ごとの異常スコアである車両別異常スコアと、車種ごとの異常スコアの平均である車種別平均異常スコアと、エリア別の異常スコアの平均であるエリア別平均異常スコアから構成される。

[0096] 車両別異常スコアでは、異常ルール番号ごとに異常スコアが算出される。異常スコアの算出方法は後述する。例えば、異常ルール番号が２である行では、車両識別子がＡ１である車両の異常スコアが１であることを示している。また、最後に異常と判定されたイベントの発生時刻である最終異常日時が格納される。最終異常日時を確認することで、特定の車両に対して、異常が発生していない期間を取得することができ、攻撃者が攻撃をしていない、つまり、異常が一定期間発生していない車両に対しては異常スコアを低下させることができる。

[0097] 車種別平均異常スコアでは、異常ルール番号と車種ごとに異常スコアが算出し、車種ごとの平均値が格納される。例えば、異常ルール番号が１である行では、車種Ａの平均異常スコアが０であることを示している。

[0098] エリア別平均異常スコアでは、異常ルール番号と車種ごとに異常スコアが算出し、車種ごとの平均値が格納される。例えば、異常ルール番号が６である行では、車種Ａの平均異常スコアが０．５であることを示している。

[0099] ［９　対策ルールの一例］

図９は、ルール記憶部に格納される対策ルールの一例である。対策ルールは、対策ルール番号と、異常カテゴリと、異常スコア、対策ルール内容から構成される。異常対策通知部１０９は、異常と判定された車両の異常スコアを参照し、異常スコアが最も高い異常ルールの異常カテゴリと、異常スコアの値を取得し、異常カテゴリと異常スコアの値に応じて対策ルールを選択し、対策ルール内容を異常対策部２３０へ通知する。

[0100] 例えば、異常カテゴリがネットワーク解析で、異常スコアが２５であった

場合、対策ルール内容は、「アクセス先とアクセル元アドレスを制限」を選択する。

[0101] 異常スコアの値の大きさによって、攻撃者が攻撃を試行している可能性を把握することができるため、異常スコアが大きいほど、より攻撃者の攻撃試行を妨害する対策を講じることができる。異常スコアが小さい場合、攻撃者の攻撃試行の可能性は低いため、車両システムの通常利用に影響がない範囲での対策を講じることができる。

[0102] ネットワークインターフェースを遮断は、外部ネットワークとのインタフェースを利用不能にし、インターネット接続を完全に遮断する対策である。

[0103] アクセス先とアクセス元アドレスを制限は、インターネットのアクセス先のアドレスを一部に制限し、アクセス元アドレスおよびポートを一部に制限することで、攻撃者のネットワーク解析を妨害する対策である。

[0104] ネットワーク接続機器数を制限は、ネットワーク接続機器を少数に制限することで、ＷｉＦｉパスワードに対するブルートフォース攻撃などのネットワーク解析を妨害する対策である。

[0105] 車両制御機能を停止は、例えば、自動駐車モードや緊急ブレーキの発動自体を停止することで、攻撃者のシステム解析を妨害する対策である。

[0106] 車両ログの送信頻度を増加は、車両ログが定常時には１時間に１回送信である場合に、１０分に１回送信に変更することで、攻撃者のシステム解析の状況をより詳細に捉えるための対策である。

[0107] 車両ログの種類数を増加は、車両ログが定常時には２種類である場合に、５種類に変更することで、攻撃者のシステム解析の状況をより詳細に捉えるための対策である。

[0108] ドライバへの警告は、攻撃者であった場合に、車両システムを監視していることを通知することで、今後の解析を妨害する対策である。

[0109] ［１０　異常スコアリスト表示画面の一例］

図１０は、異常表示部１１０が表示する異常スコアリスト表示画面の一例である。異常スコアの大きい順に車両識別子を並べる。これにより、異常車

両検出サーバ１０を利用するオペレーターは、より攻撃が疑われる車両を容易に見つけ出すことができ、優先的に車両ログを解析することができる。

[0110] ［１１　異常スコア地図表示画面の一例］

図１１は、異常表示部１１０が表示する異常スコア地図表示画面の一例である。画面には、地図が表示されており、地図上に緯度がＸ２、Ｘ３、Ｘ４と表示され、経度がＹ２、Ｙ３、Ｙ４と表示されている。また、異常車両と判定された車両の最新の位置情報の地点、例えば、Ｘ４、Ｙ４を異常車両として地図上に表示している。また、異常車両と判定された車両が位置するエリア、例えばＸ３、Ｙ３を異常エリアとして地図上に表示している。

[0111] これにより、オペレーターは容易に攻撃者が攻撃試行している可能性が高い車が存在する位置を直観的に把握することができ、地図上の施設名から、状況を推測することができる。

[0112] ［１２　異常スコア段階表示画面の一例］

図１２は、異常表示部１１０が表示する異常スコア段階表示画面の一例である。画面には攻撃の進行度を表すフェーズである、偵察、武器化、デリバリー、エクスプロイト、インストール、Ｃ＆Ｃ、目的実行を段階に分けて表示されており、異常車両と判定された車両識別子Ａ１の車両が現在偵察フェーズであることを示している。

[0113] これにより、オペレーターは、車両Ａ１に対する攻撃がどの程度進行しているかを直観的に把握することができる。

[0114] ［１３　車両ログ受信処理のシーケンス］

図１３は、本開示の実施の形態１における異常車両検出サーバ１０が、車両システム２０から車両ログを受信して記憶するまでの処理シーケンスを示している。

[0115] 車両システム２０のセントラルＥＣＵ３００は、イーサネット１３を介して車両ログを収集し、収集した車両ログを車両ログ送信装置２００の車両ログ送信部２２０に送信する（Ｓ１３０１）。

[0116] 車両ログ送信装置２００の車両ログ送信部２２０は、車両側通信部２１０

へ車両ログを送信する（Ｓ１３０２）。

[0117] 車両ログ送信装置２００の車両側通信部２１０は、外部ネットワークを介して、異常車両検出サーバ１０のサーバ側通信部１０１へ車両ログを送信する（Ｓ１３０３）。

[0118] 異常車両検出サーバ１０のサーバ側通信部１０１は、車両ログを受信し、車両ログ受信部１０２へ転送する（Ｓ１３０４）。

[0119] 異常車両検出サーバ１０の車両ログ受信部１０２は、車両ログを受信し、車両ログ記憶部１０３に格納する（Ｓ１３０５）。

[0120] ［１４　除外ルール受信処理のシーケンス］

図１４は、本開示の実施の形態１における異常車両検出サーバ１０が、除外ルール共有サーバ３０から除外ルールを受信して記憶するまでの処理シーケンスを示している。

[0121] 除外ルール共有サーバ３０は、外部ネットワークを介して、除外ルールを異常車両検出サーバ１０のサーバ側通信部１０１に送信する（Ｓ１４０１）。

[0122] 異常車両検出サーバ１０のサーバ側通信部１０１は、除外ルールを受信し、除外ルール受信部１０４へ転送する（Ｓ１４０２）。

[0123] 異常車両検出サーバ１０の除外ルール受信部１０４は、除外ルールを受信し、ルール記憶部１０５に格納する（Ｓ１４０３）。

[0124] ［１５　異常スコア算出処理のシーケンス］

図１５は、本開示の実施の形態１における異常車両検出サーバ１０が、異常スコアを算出し、異常車両を検出するまでの処理シーケンスを示している。

[0125] 異常車両検出サーバ１０の異常スコア算出部１０６は、車両ログ記憶部１０３から車両ログを取得し、ルール記憶部１０５から除外ルールと異常ルールを取得する（Ｓ１５０１）。

[0126] 異常スコア算出部１０６は、取得した車両ログと、除外ルールと、異常ルールに基づき、異常スコアを算出して、異常スコア記憶部１０７に格納する

（Ｓ１５０２）。

[0127] 異常スコア算出部１０６は、異常スコア算出後、異常車両判定部１０８へ通知する（Ｓ１５０３）。

[0128] 異常車両判定部１０８は、異常スコア記憶部１０７から異常スコアを取得し、異常車両を検出する（Ｓ１５０４）。

[0129] ［１６　異常対策処理のシーケンス］

図１６は、本開示の実施の形態１における異常車両検出サーバ１０が、異常車両を検出後、異常に対して対策を講じるまでの処理シーケンスを示している。

[0130] 異常車両検出サーバ１０の異常車両判定部１０８は、検出した異常車両の車両識別子と、車種と、エリアと、異常スコアを異常対策通知部１０９へ送信する（Ｓ１６０１）。

[0131] 異常車両検出サーバ１０の異常対策通知部１０９は、受信した異常車両の車両識別子に対応する車両または、受信した異常車両の車種と同一の車種の車両、受信した異常車両のエリアと同一エリアに位置する車両へ通知するよう、サーバ側通信部１０１へ送信する（Ｓ１６０２）。

[0132] 異常車両検出サーバ１０のサーバ側通信部１０１は、外部ネットワークを介して、Ｓ１６０２の通知を車両ログ送信装置２００の車両側通信部２１０へ送信する（Ｓ１６０３）。

[0133] 車両ログ送信装置２００の車両側通信部２１０は、Ｓ１６０２の通知を異常対策部２３０へ送信する（Ｓ１６０４）。

[0134] 車両ログ送信装置２００の異常対策部２３０は、車両ログ送信部２２０へ異常対策を要求する（Ｓ１６０５）。例えば、車両ログの種類量や頻度の増加を要求する。

[0135] 車両ログ送信装置２００の異常対策部２３０は、イーサネット１３を介して、セントラルＥＣＵ３００へ異常対策を要求する（Ｓ１６０６）。例えば、車両制御機能の制限を要求する。

[0136] ［１７　異常表示処理のシーケンス］

図１７は、本開示の実施の形態１における異常車両検出サーバ１０が、異常車両を検出後、異常をオペレーターへ表示するまでの処理シーケンスを示している。

[0137] 異常車両検出サーバ１０の異常車両判定部１０８は、検出した異常車両の車両識別子と、車種と、エリアと、異常スコアを異常表示部１１０へ送信する（Ｓ１７０１）。

[0138] 異常車両検出サーバ１０の異常表示部１１０は、受信した異常車両の車両識別子と、車種と、エリアを、グラフィカルユーザーインターフェースを用いて表示する（Ｓ１７０２）。

[0139] ［１８　車両別異常スコア算出処理のフローチャート］

図１８に、本開示の実施の形態１における異常スコア算出部１０６の車両別異常スコア算出処理のフローチャートを示す。

[0140] 異常スコア算出部１０６は、変数ｉを用意し、ｉ＝１とする（Ｓ１８０１）。そして、Ｓ１８０２を実施する。ここでｉは１～Ｎの値で、Ｎは異常ルール数を表す。

[0141] 異常ルールｉを選択し（Ｓ１８０２）、Ｓ１８０３を実施する。

[0142] 車両ログに記載されるイベント内容と、位置情報と、時刻と、除外ルールを参照し、異常ルールｉが除外対象異常ルールでない場合、Ｓ１８０４を実行し、異常ルールｉが除外対象異常ルールである場合、Ｓ１８０５を実行する（Ｓ１８０３）。

[0143] 車両ログに記載されるイベント内容と位置情報と時刻と、除外ルールを参照し、車両ログのイベントが異常ルールｉと合致し、異常であると判定される場合、Ｓ１８０６を実施する（Ｓ１８０４）。また、車両ログのイベントが異常ルールｉと合致せず、異常でないと判定される場合、Ｓ１８０５を実行する。

[0144] 異常スコアに記載される最終異常日時を参照し、現在の日時から２４時間経過している場合、Ｓ１８０７を実施する（Ｓ１８０５）。

[0145] 車両ログに記載される車両識別子と対応する異常スコアを、異常ルールｉ

に記載された異常スコア分を加算し（Ｓ１８０６）、Ｓ１８０８を実施する。

[0146] 車両ログに記載される車両識別子と対応する異常スコアを、０に変更し（Ｓ１８０７）、Ｓ１８０８を実施する。

[0147] ｉがＮである場合、終了し、そうでない場合Ｓ１８０９を実施する（Ｓ１８０８）。

[0148] ｉを１インクリメントし（Ｓ１８０９）、Ｓ１８０２を実施する。

[0149] ［１９　車種別異常スコア算出処理のフローチャート］

図１９に、本開示の実施の形態１における異常スコア算出部１０６の車種別異常スコア算出処理のフローチャートを示す。

[0150] 異常スコア算出部１０６は、車両別異常スコアを取得する（Ｓ１９０１）。

[0151] 変数ｉを用意し、ｉ＝１とする（Ｓ１９０２）。そして、Ｓ１９０３を実施する。ここでｉは１～Ｎの値で、Ｎは異常ルール数を表す。

[0152] 異常ルールｉを選択し（Ｓ１９０３）、Ｓ１９０４を実施する。

[0153] 車種ごとに、すべての車両の車両別異常スコアから、異常ルールｉと対応する異常スコアを抽出し、平均値を算出する（Ｓ１９０４）。

[0154] ｉがＮである場合、終了し、そうでない場合Ｓ１９０６を実施する（Ｓ１９０５）。

[0155] ｉを１インクリメントし（Ｓ１９０６）、Ｓ１９０３を実施する。

[0156] ［２０　エリア別異常スコア算出処理のフローチャート］

図２０に、本開示の実施の形態１における異常スコア算出部１０６の車種別異常スコア算出処理のフローチャートを示す。

[0157] 異常スコア算出部１０６は、車両別異常スコアを取得する（Ｓ２００１）。

[0158] 変数ｉを用意し、ｉ＝１とする（Ｓ２００２）。そして、Ｓ２００３を実施する。ここでｉは１～Ｎの値で、Ｎは異常ルール数を表す。

[0159] 異常ルールｉを選択し（Ｓ２００３）、Ｓ２００４を実施する。

[0160] エリアごとに、すべての車両の車両別異常スコアから、異常ルールｉと対応する異常スコアを抽出し、平均値を算出する（Ｓ２００４）。

[0161] ｉがＮである場合、終了し、そうでない場合Ｓ２００９を実施する（Ｓ２００５）。

[0162] ｉを１インクリメントし（Ｓ２００６）、Ｓ２００２を実施する。

[0163] ［２１　異常車両検出処理のフローチャート］

図２１に、本開示の実施の形態１における異常車両判定部１０８の異常車両検出処理のフローチャートを示す。

[0164] 異常車両判定部１０８は、特定車両を選択し、選択した車両の異常スコアを取得し（Ｓ２１０１）、Ｓ２１０２と、Ｓ２１０４と、Ｓ２１０６を実施する。ここで異常スコアは車両別異常スコア、車種別異常スコア、エリア別異常スコアを含む。

[0165] 異常スコアが１０よりも大きい場合に、Ｓ２１０３を実施し、そうでない場合に、終了する（Ｓ２１０２）。

[0166] 選択中の車両を異常車両として検出し（Ｓ２１０３）、終了する。

[0167] 異常スコアが選択中の車両と同一車種の車種別異常平均スコアよりも大きい場合に、Ｓ２１０５を実施し、そうでない場合に、終了する（Ｓ２１０４）。

[0168] 選択中の車両を異常車両として検出し、異常スコアを２倍にして、異常スコア記憶部１０７に格納し（Ｓ２１０５）、終了する。これにより、通常とより異なる挙動を示す車両の異常スコアを大きくすることができ、優先的に解析することができる。

[0169] 異常スコアが選択中の車両と同一エリアに位置するエリア別異常平均スコアよりも大きい場合に、Ｓ２１０７を実施し、そうでない場合に、終了する（Ｓ２１０６）。

[0170] 選択中の車両を異常車両として検出し、異常スコアを２倍にして、異常スコア記憶部１０７に格納し（Ｓ２１０７）、終了する。これにより、通常とより異なる挙動を示す車両の異常スコアを大きくすることができ、優先的に

解析することができる。

[0171] ［２２　異常対策処理のフローチャート］

図２２に、本開示の実施の形態１における異常対策通知部１０９の異常対策処理のフローチャートを示す。

[0172] 異常車両判定部１０８が検出した異常車両の情報を取得し（Ｓ２２０１）、Ｓ２２０２を実施する。

[0173] 異常車両と判定された車両の異常スコアを参照し、異常スコアの値が最も大きい異常ルールと対応する異常カテゴリを抽出し（Ｓ２２０２）、Ｓ２２０３を実施する。

[0174] 異常カテゴリが、ネットワーク解析である場合、Ｓ２２０４を実施し、そうでない場合、Ｓ２２０５を実施する（Ｓ２２０３）。

[0175] ルール記憶部が記憶する対策ルールに基づいて、異常カテゴリと異常スコアの値を参照し、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告のいずれか１つ以上の対策を選択する（Ｓ２２０４）。そして、車両側通信部２１０へその対策を通知し、終了する。

[0176] 異常カテゴリが、システム解析である場合、Ｓ２２０６を実施し、そうでない場合、終了する（Ｓ２２０５）。

[0177] ルール記憶部が記憶する対策ルールに基づいて、異常カテゴリと異常スコアの値を参照し、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告のいずれか１つ以上の対策を選択する（Ｓ２２０６）。そして、車両側通信部２１０へその対策を通知し、終了する。

[0178] ［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。

[0179] （１）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、適用範囲はこれに限られない。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も適用してもよい。

[0180] すなわち、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。

[0181] また、工場や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や、組込みデバイスを制御するための通信ネットワークに適用してもよい。

[0182] （２）上記の実施の形態において、異常ルールに記載される、期間と、回数、異常スコアの値は、変更してもよい。攻撃が疑われる特定の条件を満たした場合に異常スコアが加算されればよい。

[0183] （３）上記の実施の形態において、異常スコア算出部１０６は、異常ルールごとに異常スコアを算出すると説明したが、異常ルールすべてを適応した異常スコアの合計値を算出してもよい。

[0184] （４）上記の実施の形態において、異常スコア算出部１０６は、車種とエリアごとに異常スコアの平均値を算出すると説明したが、合計値または中央値のような統計値を用いてもよい。

[0185] （５）上記の実施の形態において、異常スコアリスト表示画面は、異常スコアの高い順に表示させると説明したが、異常スコアの昇順または降順にソートできる機能を用意してもよい。

[0186] （６）上記の実施の形態において、異常スコア地図表示画面は、異常エリアと異常車両を地図上に表示すると説明したが、異常エリアと異常車両はそれぞれ複数表示してもよく、異常スコアを合わせて表示してもよい。

[0187] （７）上記の実施の形態において、異常スコア段階表示画面は、特定の異常車両の攻撃進行度を示す段階別に表示すると説明したが、すべての段階を表示する必要はなく、偵察フェーズのみを表示してもよい。

[0188] （８）上記の実施の形態において、異常スコア算出処理のフローチャートでは、最終異常日時から２４時間経過していた場合、異常スコアを０にすると説明したが、必ずしも２４時間である必要はなく所定の時間であればよい

。また、異常スコアを必ずしも０にする必要はなく、減少させてもよい。

[0189] （９）上記の実施の形態において、異常車両検出処理のフローチャートでは、異常スコアが車種別異常平均スコアよりも大きい場合とエリア別異常平均スコアよりも大きい場合に、異常スコアを２倍すると説明したが、必ずしも２倍である必要はなく、固定値を加えるなど異常スコアが大きくなればよい。

[0190] （１０）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。

[0191] （１１）上記の実施の形態における各装置は、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。

[0192] 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。

[0193] 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）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・プロセッサーを利用しても良い。

[0194] 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。

[0195] （１２）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。

[0196] （１３）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。

[0197] 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前記デジタル信号であるとしてもよい。

[0198] 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。

[0199] また、本開示は、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、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。

[0200] 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。

[0201] （１４）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

[0202] 本開示は、車載システムのログから、攻撃者によるリバースエンジニアリング活動が疑われる異常な挙動を検知し、異常スコアを算出する。さらに、同一車種や同一エリアの車載システムと異常スコアを比較することで、正常車両とは異なる攻撃対象となっている可能性の高い異常車両を検知する。そして、異常車両に対して、異常スコアと異常カテゴリに応じた対策を実施することで異常な車両を優先的に適切に解析することを可能とする。

符号の説明

[0203] １０　異常車両検出サーバ

１１、１２、１３　イーサネット

１４　ＣＡＮ

１５　ＣＡＮ－ＦＤ

２０　車両システム

３０　除外ルール共有サーバ

２００　車両ログ送信装置

３００　セントラルＥＣＵ

４００ａ、４００ｂ、４００ｃ、４００ｄ　ＺｏｎｅＥＣＵ

５００ａ　ボディＥＣＵ

５００ｂ　カーナビＥＣＵ

５００ｃ　ステアリングＥＣＵ

５００ｄ　ブレーキＥＣＵ

１０１　サーバ側通信部

１０２　車両ログ受信部

１０３　車両ログ記憶部

１０４　除外ルール受信部

１０５　ルール記憶部

１０６　異常スコア算出部

１０７　異常スコア記憶部

１０８　異常車両判定部

１０９　異常対策通知部

１１０　異常表示部

２１０　車両側通信部

２２０　車両ログ送信部

２３０　異常対策部

請求の範囲

[請求項1] 車両システムにおいて発生したイベント内容のデータを含む車両ログを１以上の車両から受信する異常車両検出サーバであって、

受信した車両ログのイベント内容に基づいて、通常の運転とは異なる不審挙動を検出し、前記車両ログと対応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異常スコアを算出する異常スコア算出部と、

前記異常スコアが所定値以上の場合に、前記車両を異常車両として判定する異常車両判定部と、

を備える、異常車両検出サーバ。

[請求項2] 前記異常車両判定部は、さらに、一の車両に対して算出された異常スコアと、前記一の車両と同一の車種の異常スコアに基づく統計値を比較し、前記一の車両が異常車両であるか否かを判定する、

請求項１記載の異常車両検出サーバ。

[請求項3] 前記異常車両判定部は、

一の車両に対して算出された異常スコアと、前記一の車両と同一のエリアに位置する車両の異常スコアに基づく統計値を比較し、前記一の車両が異常車両であるか否かを判定する、

請求項１記載の異常車両検出サーバ。

[請求項4] 前記異常スコア算出部は、ネットワーク機器接続頻発または、インターネット接続異常、診断コマンド頻発、アクセス先アドレスの変化、アクセス元アドレスの変化のいずれかを不審挙動として検出し、前記不審挙動が発生した場合に、ネットワーク解析活動と判定し、車両に対して異常スコアを増加させる、

請求項１から３のいずれか１項に記載の異常車両検出サーバ。

[請求項5] さらに、異常対策通知部を備え、

前記異常スコア算出部が、前記不審挙動をネットワーク解析活動と判定した場合、前記異常対策通知部は、異常スコアの値に応じて、ネ

ットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告のいずれか１つ以上の対策を実施する、

請求項４記載の異常車両検出サーバ。

[請求項6] 前記異常スコア算出部は、車両制御機能頻発、システムエラー頻発、システムエラー削除、故障コード頻発、システムログイン、ファイル数またはプロセス数の変化のいずれかを不審挙動として検出し、前記不審挙動が発生した場合に、システム解析活動と判定し、車両に対して異常スコアを増加させる、

請求項１から３のいずれか１項に記載の異常車両検出サーバ。

[請求項7] さらに、異常対策通知部を備え、

前記異常スコア算出部が、前記不審挙動をネットワーク解析活動と判定した場合、前記異常対策通知部は、異常スコアの値に応じて、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの警告のいずれか１つ以上の対策を実施する、

請求項６記載の異常車両検出サーバ。

[請求項8] 前記異常スコア算出部は、前記不審挙動を検出した場合であっても、所定の期間内に前記不審挙動が発生した場合または所定のエリアにて前記不審挙動が発生した場合は、異常スコアを増加させない、

請求項１から７のいずれか１項に記載の異常車両検出サーバ。

[請求項9] 前記異常スコア算出部は、所定の期間中に前記不審挙動が発生しなかった場合は、異常スコアを減少させる、

請求項１から８のいずれか１項に記載の異常車両検出サーバ。

[請求項10] 前記異常車両検出サーバは、さらに、前期異常車両判定装置が異常車両と判定した車両に対して、前記異常スコアの値または前記不審挙動の種別に基づいて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告、ネットワーク接続制限と、車両制御機能制限、

車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策を要求する異常通知部を備える、

請求項１から９のいずれか１項に記載の異常車両検出サーバ。

[請求項11] 前記異常車両検出サーバは、さらに、前記異常車両判定装置が異常車両と判定した車両と同一の車種に対して、前記異常スコアの値または前記不審挙動の種別に基づいて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告、ネットワーク接続制限と、車両制御機能制限、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策を要求する異常通知部を備える、

請求項１から９のいずれか１項に記載の異常車両検出サーバ。

[請求項12] 前記異常車両検出サーバは、さらに、前記異常車両判定装置が異常車両と判定した車両と同一のエリアに位置する車両に対して、前記異常スコアの値または前記不審挙動の種別に基づいて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバへの警告、ネットワーク接続制限と、車両制御機能制限、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバへの通知のうち、いずれか１つ以上の対策を要求する異常通知部を備える、

請求項１から９のいずれか１項に記載の異常車両検出サーバ。

[請求項13] 前記異常車両検出サーバは、前記異常スコアが高い順に異常車両をリスト表示する異常車両表示部を備える、

請求項１から１２のいずれか１項に記載の異常車両検出サーバ。

[請求項14] 前記異常車両検出サーバは、前記異常車両と判定された車両の位置情報を地図上に表示する異常車両表示部を備える、

請求項１から１２のいずれか１項に記載の異常車両検出サーバ。

[請求項15] 前記異常車両検出サーバは、車両に対する攻撃を、攻撃の進行度に応じて階層別に表示し、前記異常車両と判定された車両または車種、位置情報のいずれか一つの情報を、攻撃の進行度が低い偵察フェーズの階層に表示する異常車両表示部を備える、

請求項１から１２のいずれか１項に記載の異常車両検出サーバ。

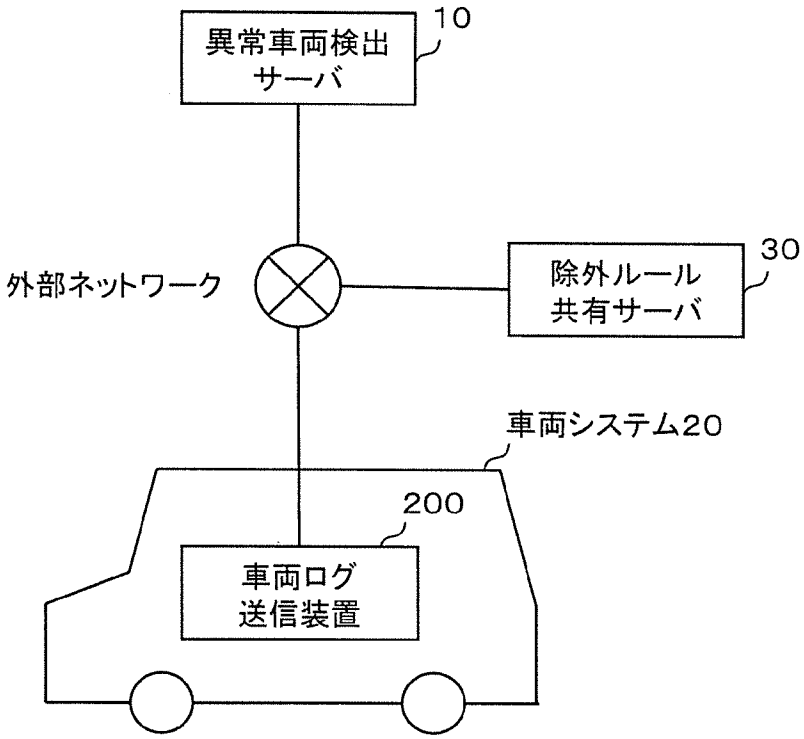
[請求項16] 車両システムにおいて発生したイベント内容のデータを含む車両ログを１以上の車両から受信する異常車両検出方法であって、

受信した車両ログのイベント内容に基づいて、通常の運転とは異なる不審挙動を検出し、前記車両ログと対応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異常スコアを算出する異常スコア算出ステップと、

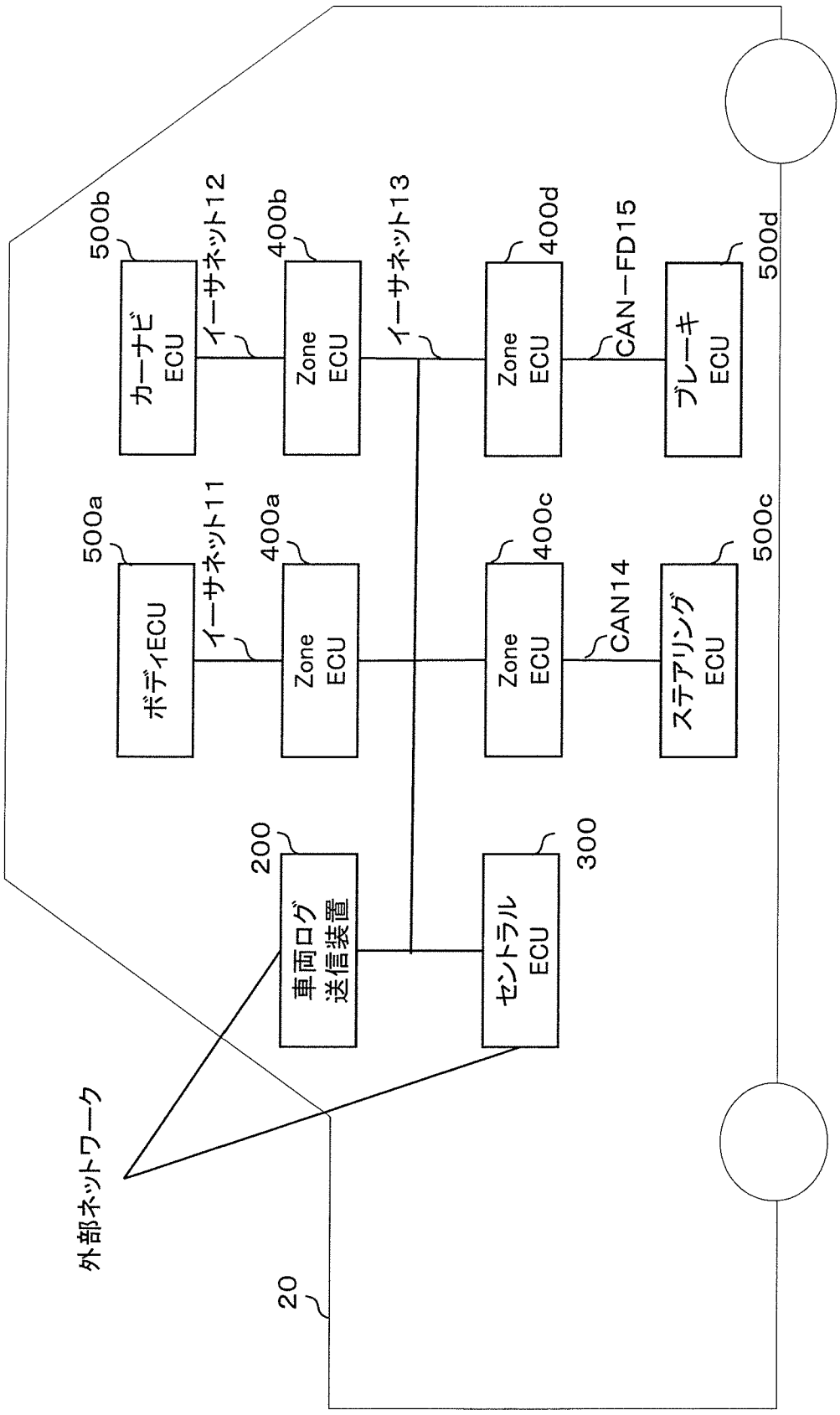
前記異常スコアが所定値以上の場合に、前記車両を異常車両として判定する異常車両判定ステップと、

を備える、異常車両検出方法。

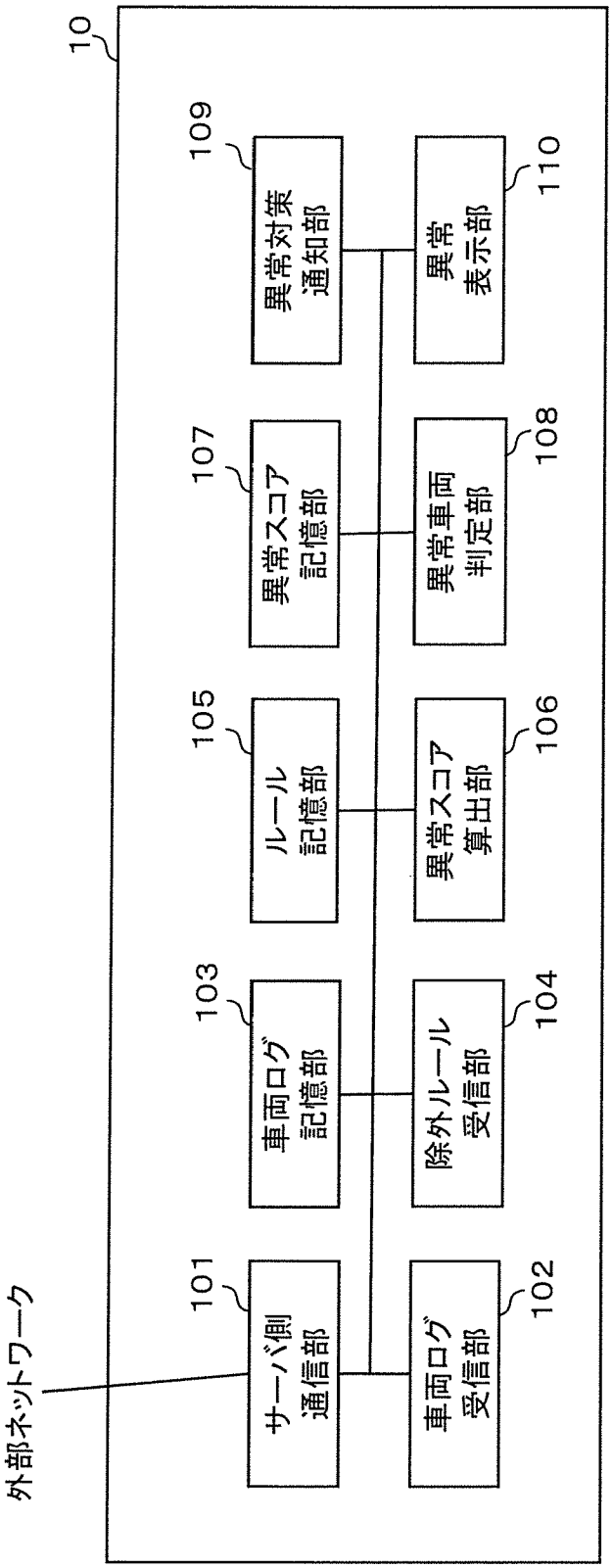
[図1]


異常車両検出
サーバ
10
外部ネットワーク
除外ルール
共有サーバ
30
車両システム20
200
車両ログ
送信装置

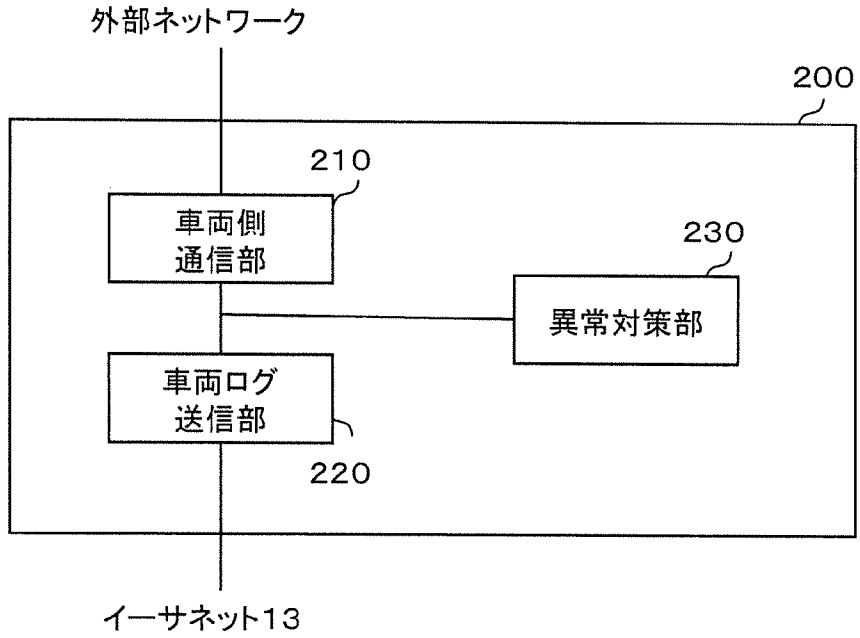
[図2]


500b
カーナビ ECU
イーサネット12
400b
Zone ECU
イーサネット13
400d
Zone ECU
CAN−FD15
ブレーキ ECU
500d
500a
ボディECU
イーサネット11
400a
Zone ECU
400c
Zone ECU
CAN14
ステアリング ECU
500c
200
車両ログ 送信装置
300
セントラル ECU
外部ネットワーク
20

[図3]


10
外部ネットワーク
101
サーバ側
通信部
102
車両ログ
受信部
103
車両ログ
記憶部
104
除外ルール
受信部
105
ルール
記憶部
106
異常スコア
算出部
107
異常スコア
記憶部
108
異常車両
判定部
109
異常対策
通知部
110
異常
表示部

[図4]



[図5]

車両ログ番号	車両識別子	車種	時刻	車両位置情報	イベント名
1	A1	A	TA11	X1, Y1	ネットワーク機器登録
2	A1	A	TA12	X1, Y1	ネットワーク機器削除
3	A1	A	TA13	X1, Y1	インターネット切断
4	A1	A	TA14	X1, Y1	インターネット接続
5	A2	A	TA21	X1, Y1	VPN切断
6	A2	A	TA22	X1, Y1	VPN接続
7	A2	A	TA23	X1, Y3	車両制御機能作動
8	A2	A	TA24	X1, Y4	車両制御機能作動
9	B1	B	TB11	X2, Y2	システムエラー発生
10	B1	B	TB12	X2, Y2	システムエラー解除
11	B1	B	TB13	X2, Y2	車両制御機能作動
12	B1	B	TB14	X2, Y2	車両制御機能作動
…	…	…	…	…	…
C1	C1	C	TC11	X3, Y3	アドレスAへアクセス
C2	C1	C	TC12	X3, Y3	アドレスBからアクセス
C3	C1	C	TC13	X3, Y3	システムログイン
C4	C1	C	TC14	X4, Y4	ファイル数またはプロセス数が増加

[図6]

異常ルール番号	異常ルール内容	期間	回数	異常スコア	異常カテゴリ
1	ネットワーク機器接続	1時間	4	+1	ネットワーク解析
2	インターネットまたはVPN遮断	10分	1	+1	ネットワーク解析
3	アクセス先アドレスの変化	—	1	+1	ネットワーク解析
4	アクセス元アドレスの変化	—	1	+1	ネットワーク解析
5	車両制御機能作動	1時間	10	+2	システム解析
6	システムエラー発生	24時間	2	+1	システム解析
7	システムエラー解除	—	1	+3	システム解析
8	システムログイン	—	1	+5	システム解析
...	...	...	...	...	...
N	ファイル数またはプロセス数の変化	—	1	+1	システム解析

[図7]

除外ルール番号	位置情報	有効期間	内容	除外対象異常ルール
1	X2，Y2	—	テストコースA	車両制御機能作動
2	X5，Y5	—	ディーラーA	システムエラー解除
3	X6，Y6	—	修理業者A	システムエラー解除
4	日本	T3～T4	ソフト更新A	ファイル数またはプロセス数の変化
5	北米	T5～T6	ソフト更新B	ファイル数またはプロセス数の変化
…	…	…	…	…
M	X4、X4	—	トンネルA	インターネットまたはVPN遮断

[図8]

異常ルール番号	車両別異常スコア						車種別平均異常スコア			エリア別平均異常スコア		
	A1	A2	B1	…	C1		A	B	C	X1、Y1	X2、Y2	X3、Y3
1	回数不足	0	0	…	0		0	0	0	0	0	0
2	1	1	0	…	0		1	0	0	1	0	0
3	0	0	0	…	1		0	0	1	0	0	0
4	0	0	0	…	1		0	0	1	0	0	0
5	0	2	0	…	0		1	0	0	0	1	0
6	0	0	除外	…	0		0	0	0	0	0.5	0
7	0	0	1	…	0		0	1	0	0	0	0
8	0	0	0	…	5		0	0	1	0	0	0
…	…	…	…	…	…		…	…	…	…	…	…
N	0	0	0	…	0		0	0	0	0	0	0
最終異常日時	TN1	TN2	TN3	…	TN4		—	—	—	—	—	—

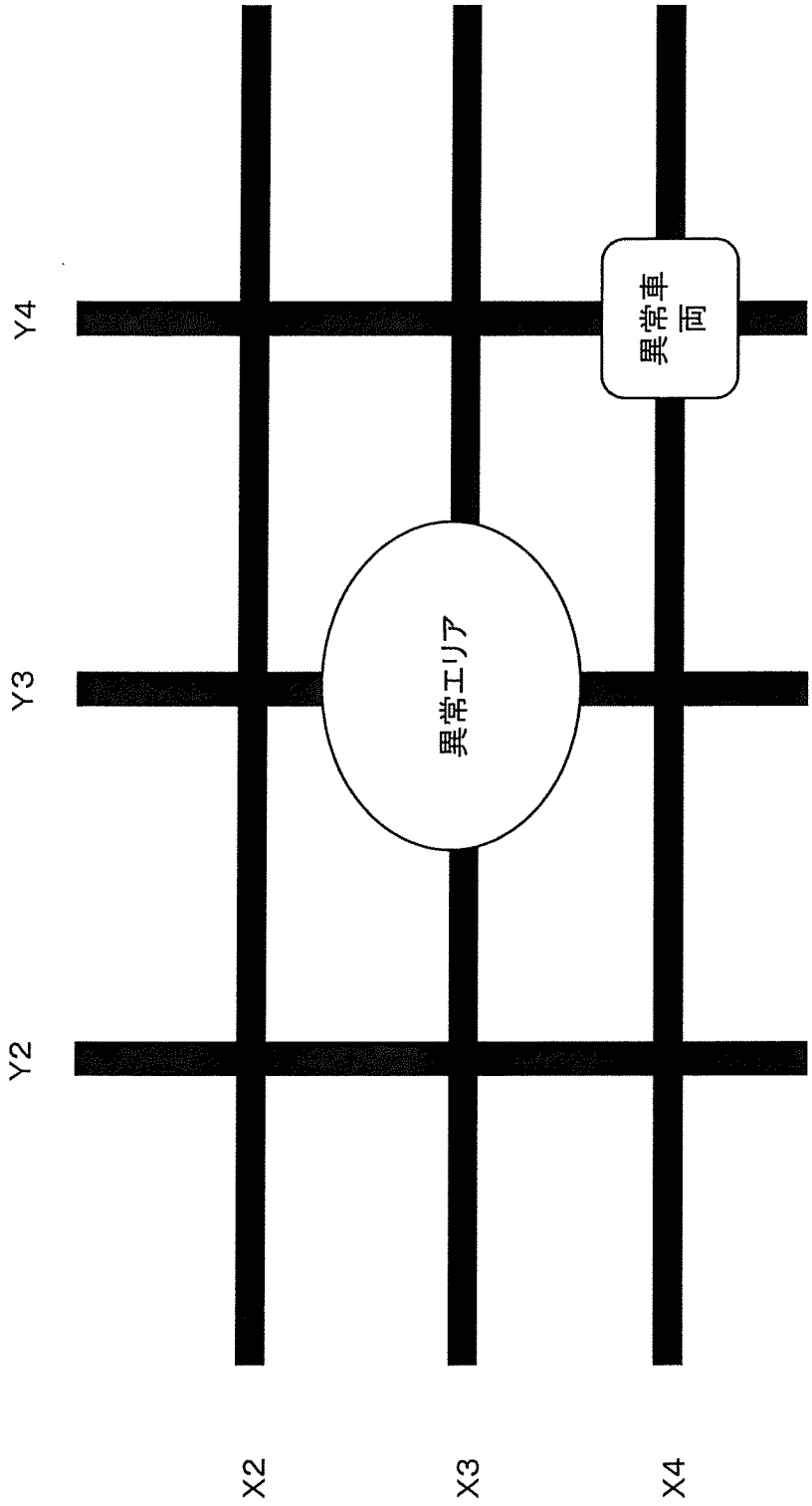
[図9]

対策ルール番号	異常カテゴリ	異常スコア	対策ルール内容
1	ネットワーク解析	30以上	ネットワークインタフェースを遮断
		30未満 20以上	アクセス先とアクセス元アドレスを制限
		20未満 10以上	ネットワーク接続機器数を制限
		1以上	ドライバへ警告
2	システム解析	30以上	車両制御機能を停止
		30未満 20以上	車両ログの送信頻度を増加
		20未満 10以上	車両ログの種類数を増加
		1以上	ドライバへ警告

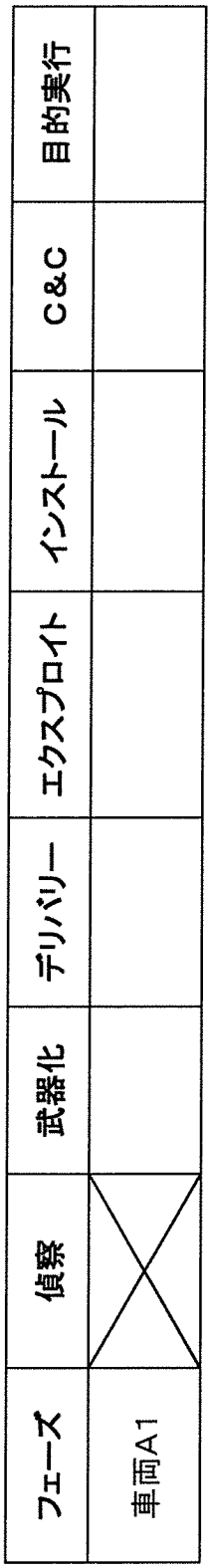
[図10]

異常スコア	車両識別子
100	H1
90	H2
80	H3
・・・	・・・
1	H4

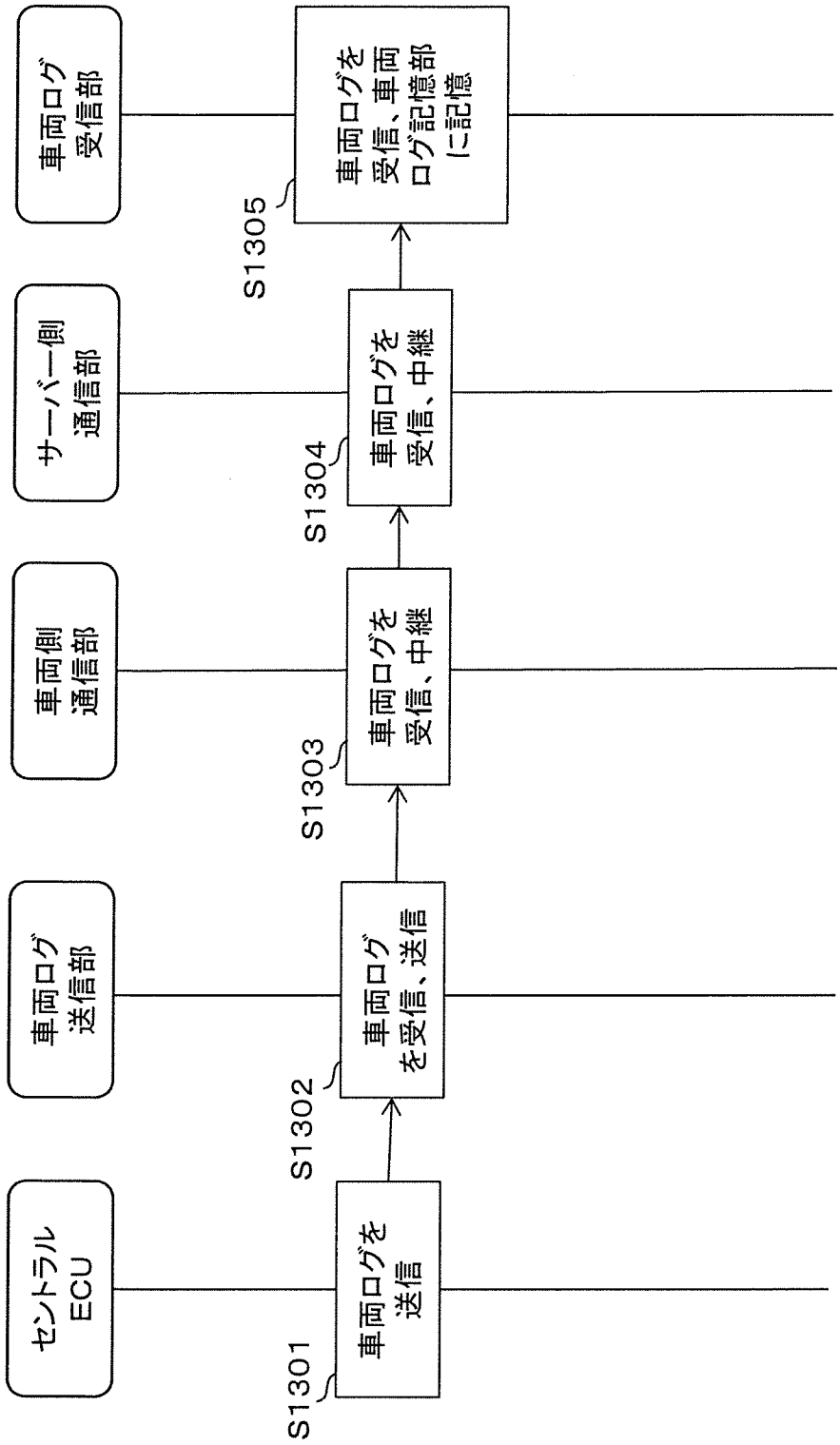
[図11]



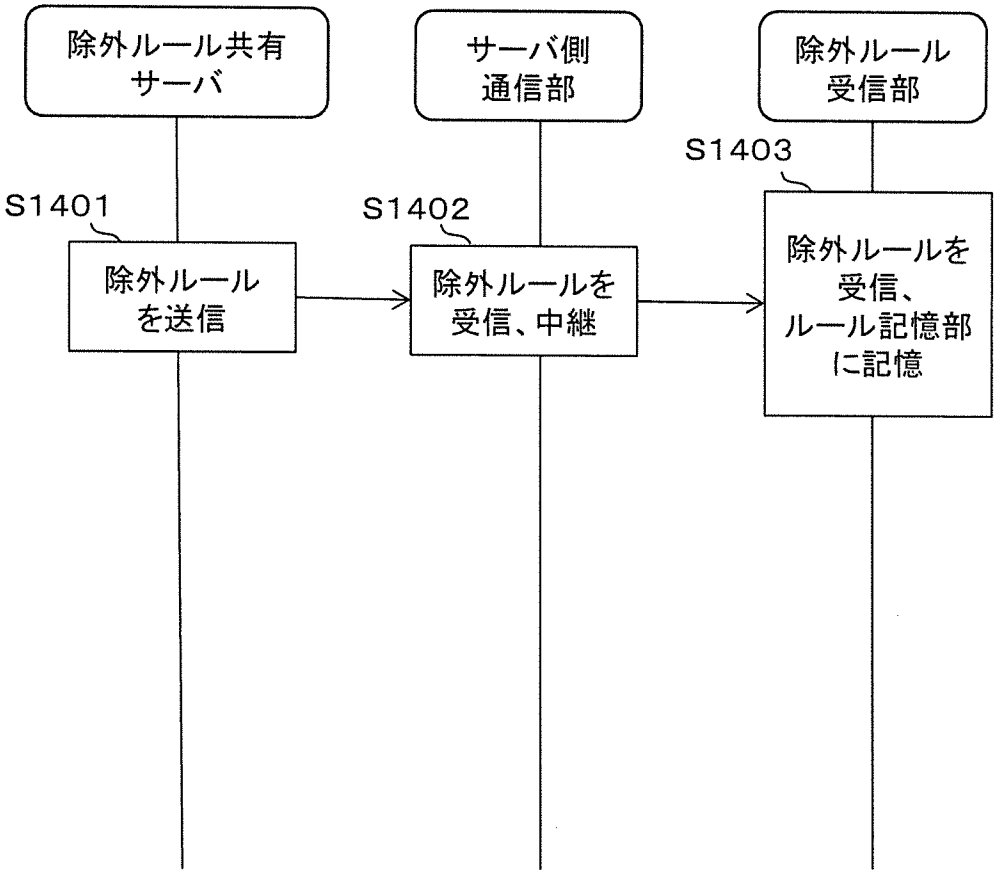
[図12]



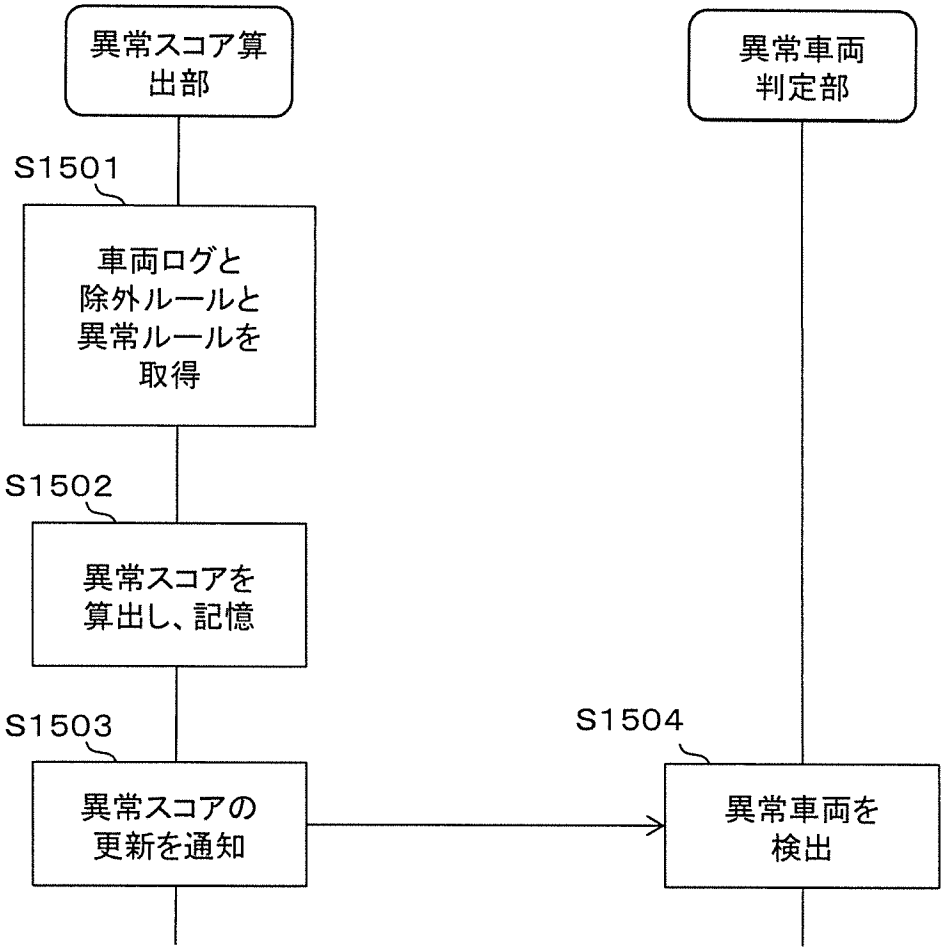
[図13]


セントラル ECU
車両ログ 送信部
車両側 通信部
サーバー側 通信部
車両ログ 受信部
車両ログを 送信
車両ログ を受信、送信
車両ログを 受信、中継
車両ログを 受信、中継
車両ログを 受信、車両 ログ記憶部 に記憶
S1301
S1302
S1303
S1304
S1305

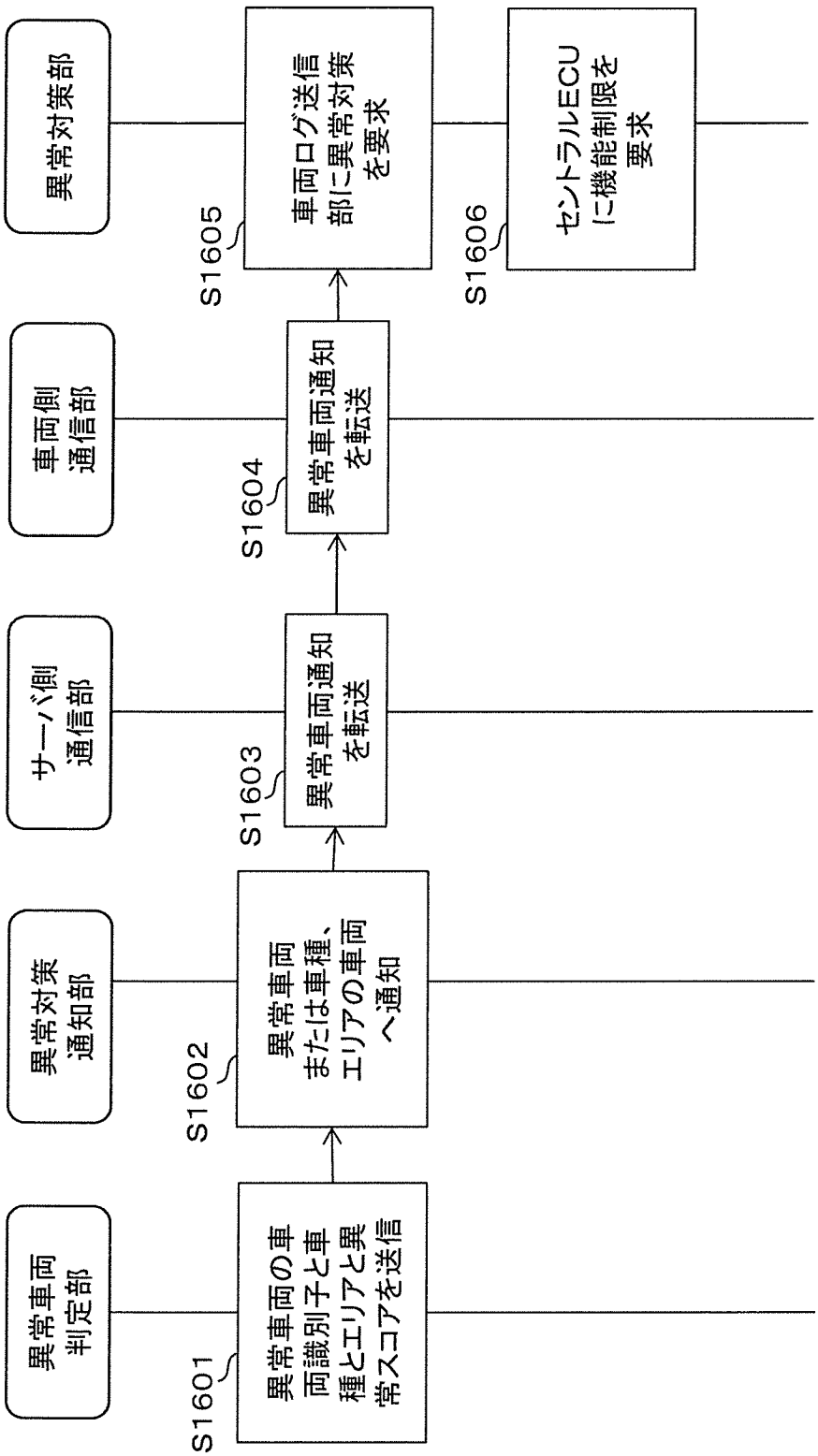
[図14]


除外ルール共有サーバ
サーバ側通信部
除外ルール受信部
S1401
除外ルールを送信
S1402
除外ルールを受信、中継
S1403
除外ルールを受信、ルール記憶部に記憶

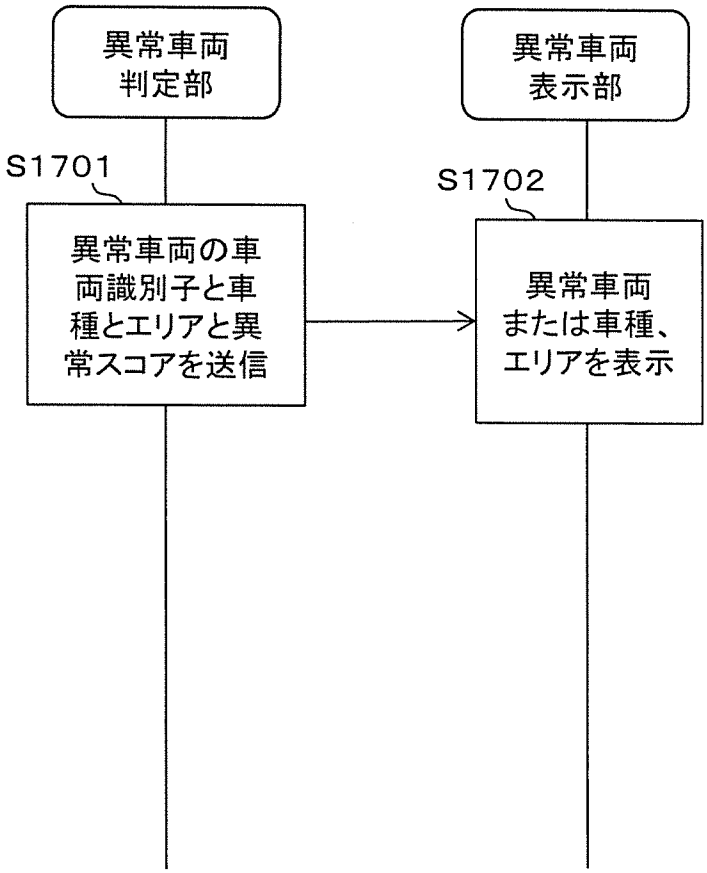
[図15]


異常スコア算出部
S1501
車両ログと除外ルールと異常ルールを取得
S1502
異常スコアを算出し、記憶
S1503
異常スコアの更新を通知
異常車両判定部
S1504
異常車両を検出

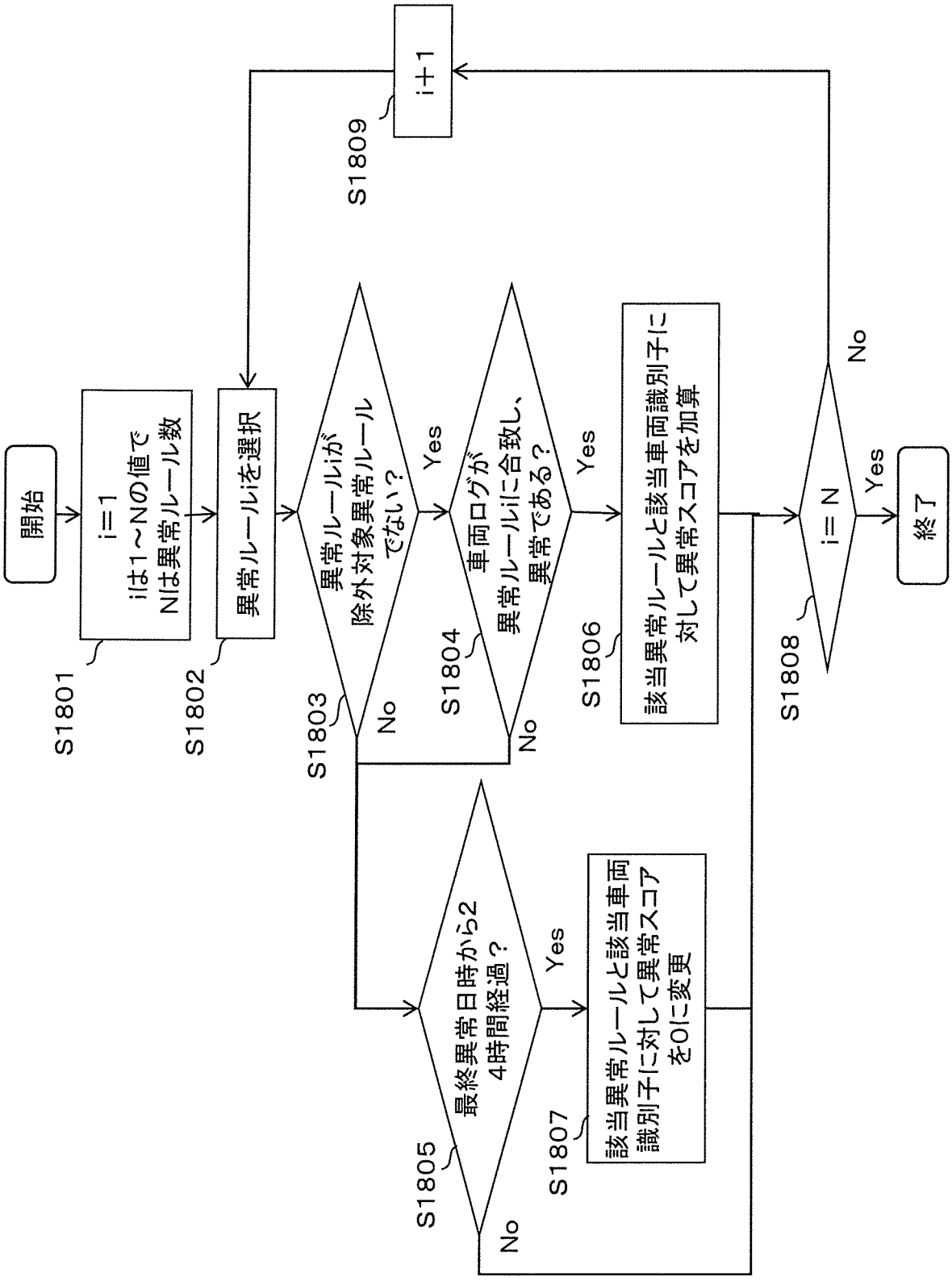
[図16]


異常車両
判定部
異常車両の車
両識別子と車
種とエリアと異
常スコアを送信
S1601
異常対策
通知部
異常車両
または車種、
エリアの車両
へ通知
S1602
サーバ側
通信部
異常車両通知
を転送
S1603
車両側
通信部
異常車両通知
を転送
S1604
異常対策部
車両ログ送信
部に異常対策
を要求
S1605
セントラルECU
に機能制限を
要求
S1606

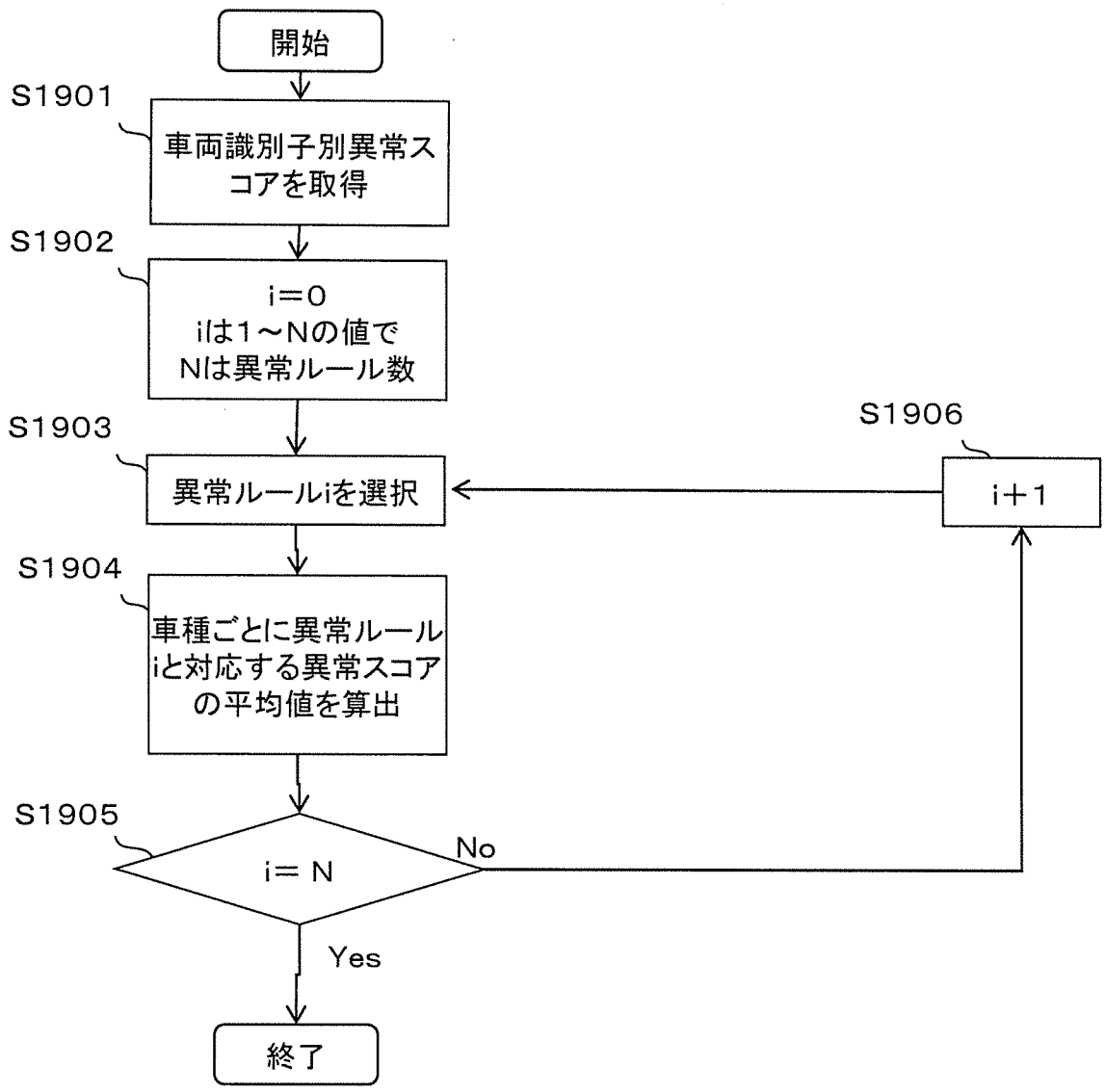
[図17]


異常車両
判定部
異常車両
表示部
S1701
S1702
異常車両の車両識別子と車種とエリアと異常スコアを送信
異常車両または車種、エリアを表示

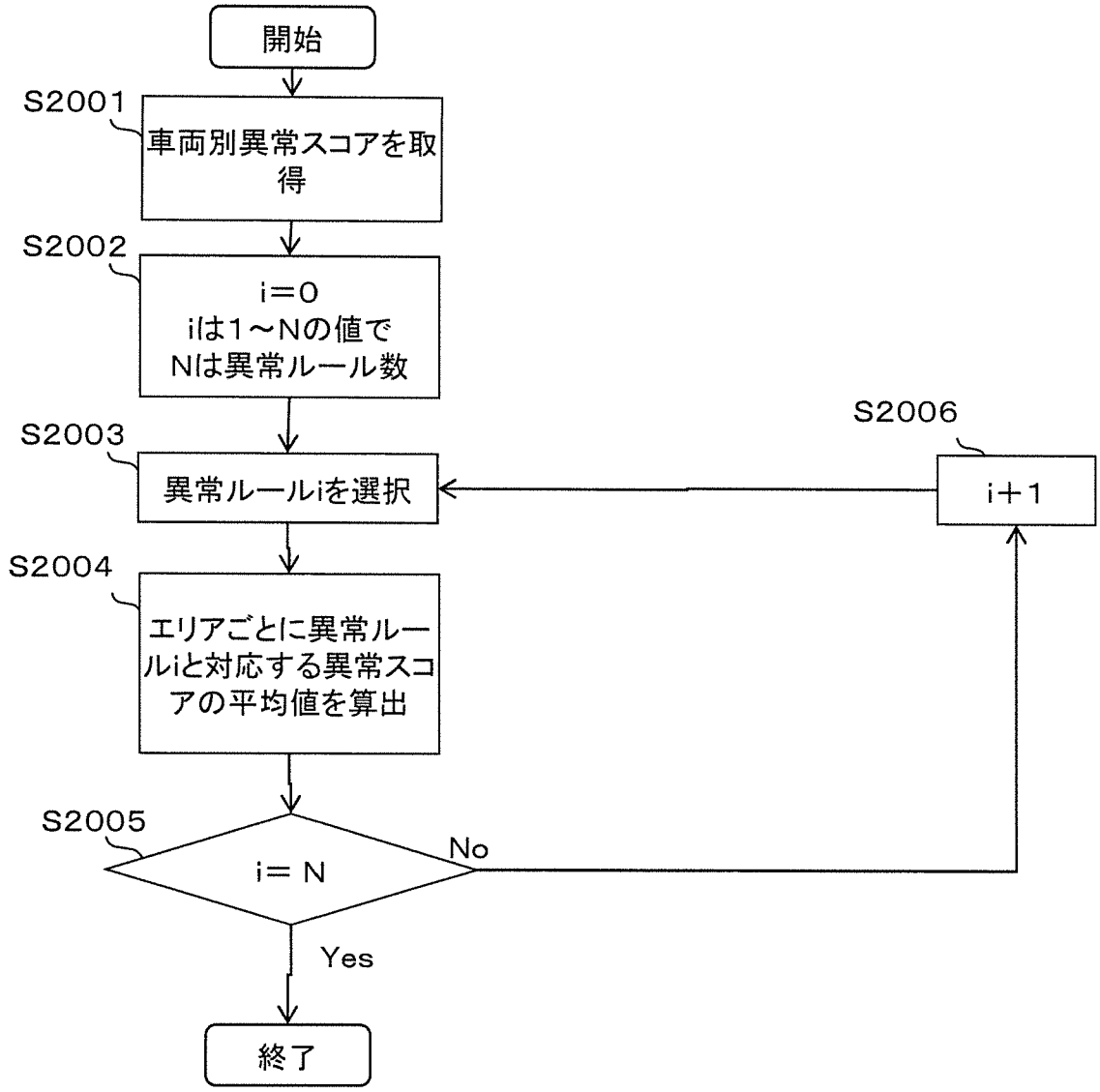
[図18]


開始
i=1
iは1～Nの値で
Nは異常ルール数
S1801
異常ルールiを選択
S1802
異常ルールiが
除外対象異常ルール
でない？
S1803
Yes
No
車両ログが
異常ルールiに合致し、
異常である？
S1804
Yes
No
該当異常ルールと該当車両識別子に
対して異常スコアを加算
S1806
最終異常日時から2
4時間経過？
S1805
Yes
No
該当異常ルールと該当車両
識別子に対して異常スコア
を0に変更
S1807
i＝N
S1808
Yes
No
終了
i+1
S1809

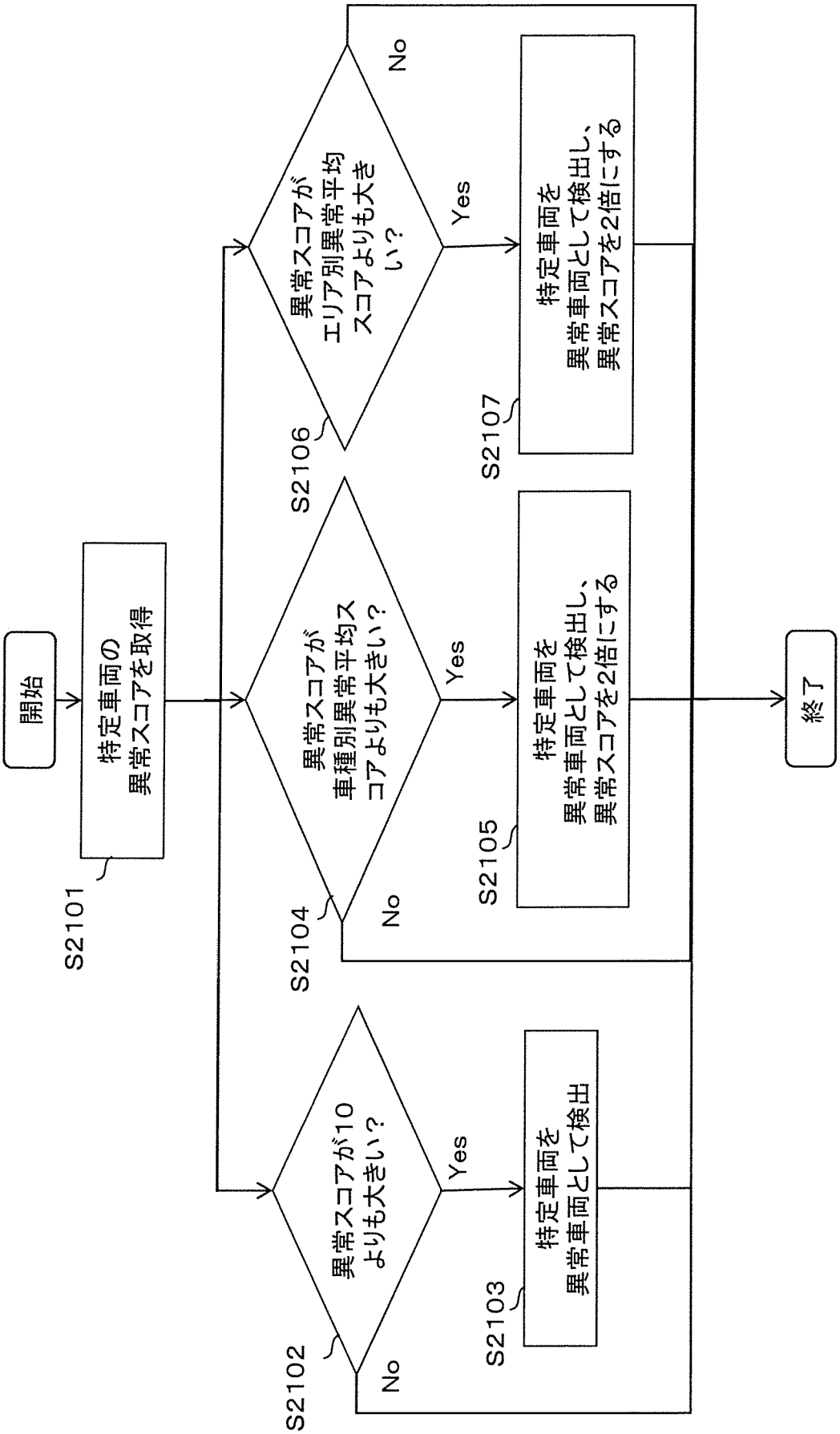
[図19]


開始
S1901
車両識別子別異常スコアを取得
S1902
i=0
iは1～Nの値で
Nは異常ルール数
S1903
異常ルールiを選択
S1904
車種ごとに異常ルールiと対応する異常スコアの平均値を算出
S1905
i= N
No
Yes
終了
S1906
i+1

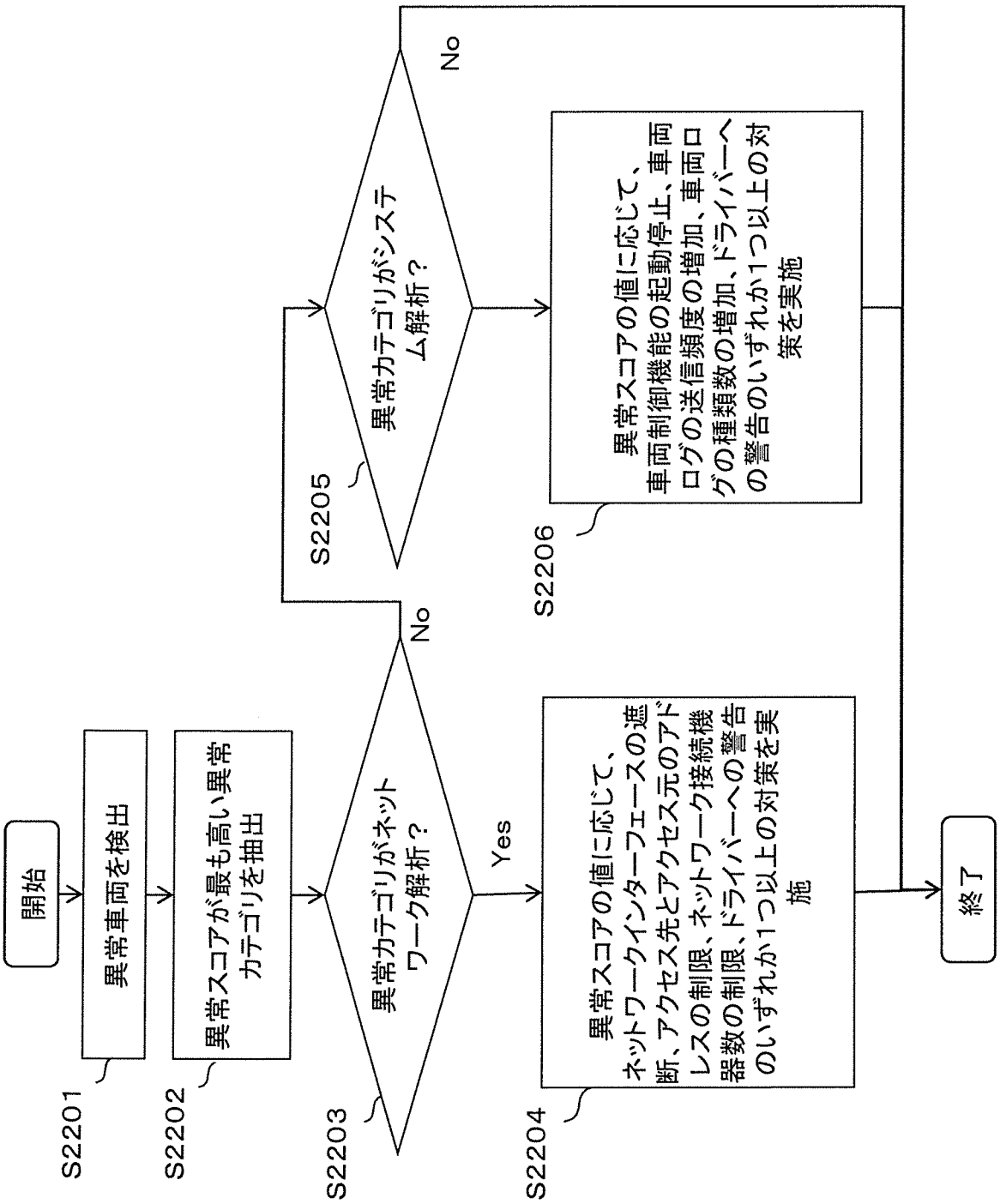
[図20]


開始
S2001
車両別異常スコアを取得
S2002
i＝0
iは1～Nの値で
Nは異常ルール数
S2003
異常ルールiを選択
S2004
エリアごとに異常ルールiと対応する異常スコアの平均値を算出
S2005
i＝N
No
Yes
S2006
i＋1
終了

[図21]


開始
特定車両の異常スコアを取得
S2101
異常スコアが10よりも大きい？
S2102
Yes
No
特定車両を異常車両として検出
S2103
異常スコアが車種別異常平均スコアよりも大きい？
S2104
Yes
No
特定車両を異常車両として検出し、異常スコアを2倍にする
S2105
異常スコアがエリア別異常平均スコアよりも大きい？
S2106
Yes
No
特定車両を異常車両として検出し、異常スコアを2倍にする
S2107
終了

[図22]


開始
異常車両を検出
S2201
異常スコアが最も高い異常カテゴリを抽出
S2202
異常カテゴリがネットワーク解析？
S2203
Yes
No
異常スコアの値に応じて、ネットワークインターフェースの遮断、アクセス先とアクセス元のアドレスの制限、ネットワーク接続機器数の制限、ドライバーへの警告のいずれか1つ以上の対策を実施
S2204
異常カテゴリがシステム解析？
S2205
No
異常スコアの値に応じて、車両制御機能の起動停止、車両ログの送信頻度の増加、車両ログの種類数の増加、ドライバーへの警告のいずれか1つ以上の対策を実施
S2206
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/034264

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G06F21/55(2013.01)i, H04L12/28(2006.01)i

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)
Int. Cl. G06F21/55, H04L12/28

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 1971-2019
Registered utility model specifications of Japan 1996-2019
Published registered utility model applications of Japan 1994-2019

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.
Y A	JP 2017-111796 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 22 June 2017, paragraphs [0037], [0057]-[0066], [0073], [0074], [0121] & US 2018/0295147 A1, paragraphs [0055], [0079]-[0088], [0095], [0096], [0143] & CN 107925600 A	1-2, 9-11, 13, 16 3-8, 12, 14-15
Y A	WO 2018/168291 A1 (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 20 September 2018, paragraphs [0101]-[0118] & US 2019/0140778 A1, paragraphs [0119]-[0136] & CN 108885664 A	1-2, 9-11, 13, 16 3-8, 12, 14-15
Y A	JP 2018-530066 A (SYMANTEC CORPORATION) 11 October 2018, paragraph [0050] & US 2017/0093902 A1, paragraph [0053] & CN 108040493 A	9-11, 13 12, 14-15

☒ 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	Date of mailing of the international search report
31.10.2019	19.11.2019
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

International application No.
PCT/JP2019/034264

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2017-5422 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 05 January 2017, paragraph [0070] (Family: none)	13 14-15
A	JP 2019-129529 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 01 August 2019 & WO 2019/142476 A1	1-16

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０３４２６４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55(2013.01)i, H04L12/28(2006.01)i

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））

Int.Cl.　G06F21/55, H04L12/28

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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
Y	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) 2017.06.22, 段落0037,0057-0066,0073-0074,0121 & US 2018/0295147 A1,段落0055,0079-0088,0095-0096,0143 & CN 107925600 A	1-2,9-11,13,16
A		3-8,12,14-15
Y	WO 2018/168291 A1 (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) 2018.09.20, 段落0101-0118 & US 2019/0140778 A1,段落0119-0136 & CN 108885664 A	1-2,9-11,13,16
A		3-8,12,14-15

☑　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矛盾するものではなく、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
３１．１０．２０１９	１９．１１．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　１２０６
吉田　歩
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　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
Y A	JP 2018-530066 A（シマンテック　コーポレーション）2018.10.11, 段落0050 & US 2017/0093902 A1,段落0053 & CN 108040493 A	9-11,13 12,14-15
Y A	JP 2017-5422 A（日本電信電話株式会社）2017.01.05, 段落0070（ファミリーなし）	13 14-15
A	JP 2019-129529 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）2019.08.01, & WO 2019/142476 A1	1-16