(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7530367号
(P7530367)

(45)発行日　令和6年8月7日(2024.8.7)

(24)登録日　令和6年7月30日(2024.7.30)

(51)国際特許分類

Ｇ０６Ｆ　21/55　(2013.01)	Ｇ０６Ｆ	21/55	３２０
Ｂ６０Ｒ　16/02　(2006.01)	Ｂ６０Ｒ	16/02	６５０Ｊ

ＦＩ

請求項の数　29　（全45頁）

(21)出願番号　特願2021-542969(P2021-542969)
(86)(22)出願日　令和2年8月26日(2020.8.26)
(86)国際出願番号　PCT/JP2020/032208
(87)国際公開番号　WO2021/039851
(87)国際公開日　令和3年3月4日(2021.3.4)
審査請求日　令和5年6月8日(2023.6.8)
(31)優先権主張番号　PCT/JP2019/034264
(32)優先日　令和1年8月30日(2019.8.30)
(33)優先権主張国・地域又は機関
日本国(JP)

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

(74)代理人　100109210
弁理士　新居 広守

(74)代理人　100137235
弁理士　寺谷 英作

(74)代理人　100131417
弁理士　道坂 伸一

最終頁に続く

(54)【発明の名称】　異常車両検出サーバおよび異常車両検出方法

(57)【特許請求の範囲】

【請求項１】

車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、

前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、

前記２以上の車両は、前記一の車両と同一の車種の車両を含み、

前記異常車両判定部は、前記一の車両の前記異常スコアと、前記一の車両と同一の車種の前記異常スコアに基づく前記統計値とを比較し、比較結果に基づいて前記一の車両が前記異常車両であるか否かを判定する、

異常車両検出サーバ。

【請求項２】

車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、

前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の

車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記２以上の車両は、前記一の車両と同一のエリアに位置する車両を含み、
前記異常車両判定部は、前記一の車両の前記異常スコアと、前記一の車両と同一のエリアに位置する車両の前記異常スコアに基づく前記統計値とを比較し、比較結果に基づいて前記一の車両が前記異常車両であるか否かを判定する、
異常車両検出サーバ。
【請求項３】
前記異常車両判定部は、さらに、前記異常車両と同一の車種である異常車種または、前記異常車両が検出されたエリアである異常エリアにおいて、所定の台数以下の前記異常車両が存在する場合、前記リバースエンジニアリングにおける攻撃の進行度が第一の攻撃段階であると判定し、前記所定の台数より多い前記異常車両が存在する場合、前記第一の攻撃段階より前記リバースエンジニアリングにおける攻撃の進行度が進行した第二の攻撃段階であると判定する、
請求項１または２に記載の異常車両検出サーバ。
【請求項４】
車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記異常車両判定部は、さらに、前記異常車両と同一の車種である異常車種または、前記異常車両が検出されたエリアである異常エリアにおいて、所定の台数以下の前記異常車両が存在する場合、前記リバースエンジニアリングにおける攻撃の進行度が第一の攻撃段階であると判定し、前記所定の台数より多い前記異常車両が存在する場合、前記第一の攻撃段階より前記リバースエンジニアリングにおける攻撃の進行度が進行した第二の攻撃段階であると判定する、
異常車両検出サーバ。
【請求項５】
前記異常スコア取得部は、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定されるネットワーク機器の接続頻発、インターネット接続異常、診断コマンドの頻発、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前記不審挙動であると検出し、前記不審挙動を検出した場合、前記不審挙動をネットワーク解析活動であると判定し、前記一の車両の前記異常スコアを増加させる、
請求項１から４のいずれか１項に記載の異常車両検出サーバ。
【請求項６】
車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記異常スコア取得部は、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定されるネットワーク機器の接続頻発、インターネット接続異常、診断コマンドの頻発、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前記不審挙動であると検出し、前記不審挙動を検出した場

合、前記不審挙動をネットワーク解析活動であると判定し、前記一の車両の前記異常スコアを増加させる、
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、
前記異常スコア取得部が前記不審挙動を前記ネットワーク解析活動であると判定した場合、前記異常対策通知部は、前記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、アクセス先およびアクセス元のアドレスの制限、前記ネットワーク機器の接続数の制限、および、ドライバへの警告のいずれか１つ以上を実施させる、
請求項５または６に記載の異常車両検出サーバ。
【請求項８】
前記異常スコア取得部は、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定される車両制御機能の頻発、システムエラーの頻発、システムエラーの削除、故障コードの頻発、システムログイン、および、ファイル数またはプロセス数の変化のいずれかを前記不審挙動であると検出し、前記不審挙動を検出した場合に、前記不審挙動をシステム解析活動であると判定し、前記一の車両の前記異常スコアを増加させる、
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】
車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記異常スコア取得部は、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定される車両制御機能の頻発、システムエラーの頻発、システムエラーの削除、故障コードの頻発、システムログイン、および、ファイル数またはプロセス数の変化のいずれかを前記不審挙動であると検出し、前記不審挙動を検出した場合に、前記不審挙動をシステム解析活動であると判定し、前記一の車両の前記異常スコアを増加させる、
異常車両検出サーバ。
【請求項１０】
さらに、異常対策通知部を備え、
前記異常スコア取得部が前記不審挙動を前記システム解析活動であると判定した場合、前記異常対策通知部は、前記異常スコアの値に応じて、車両制御機能の起動停止、前記車両ログの送信頻度の増加、前記車両ログの種類数の増加、および、ドライバへの警告のいずれか１つ以上を実施させる、
請求項８または９に記載の異常車両検出サーバ。
【請求項１１】
前記異常スコア取得部は、前記不審挙動を検出した場合であっても、前記不審挙動を検出した時刻に基づく所定の期間内に再度前記不審挙動を検出した場合または所定のエリアにて前記不審挙動を検出した場合、前記異常スコアを増加させない、
請求項１から１０のいずれか１項に記載の異常車両検出サーバ。
【請求項１２】
車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、

前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記異常スコア取得部は、前記不審挙動を検出した場合であっても、前記不審挙動を検出した時刻に基づく所定の期間内に再度前記不審挙動を検出した場合または所定のエリアにて前記不審挙動を検出した場合、前記異常スコアを増加させない、
異常車両検出サーバ。
【請求項１３】
前記異常スコア取得部は、前記不審挙動が検出された時刻に基づく所定の期間中に、前記不審挙動が検出された車両において再度前記不審挙動が検出されなかった場合、前記異常スコアを減少させる、
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】
車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記異常スコア取得部は、前記不審挙動が検出された時刻に基づく所定の期間中に、前記不審挙動が検出された車両において再度前記不審挙動が検出されなかった場合、前記異常スコアを減少させる、
異常車両検出サーバ。
【請求項１５】
前記異常車両判定部が前記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対策通知部をさらに備える、
請求項１から１４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を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備え、
前記異常車両判定部が前記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対策通知部をさらに備える、
異常車両検出サーバ。
【請求項１７】
前記異常車両判定部によって前記異常車種が前記第二の攻撃段階であると判定された場合、前記異常車両と判定した車両と同一の車種の車両に対して、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つ以上を要求する異常対策通知部をさらに備える、

請求項３または４に記載の異常車両検出サーバ。

【請求項１８】

前記異常車両判定部によって前記異常エリアにおいて前記異常車両が前記第二の攻撃段階であると判定された場合、当該異常エリアに位置する前記異常車両以外の車両に対して、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つ以上を要求する異常対策通知部をさらに備える、

請求項３または４に記載の異常車両検出サーバ。

【請求項１９】

前記異常スコアが高い順に前記異常車両をリスト表示する異常表示部をさらに備える、

請求項１から１８のいずれか１項に記載の異常車両検出サーバ。

【請求項２０】

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表示部をさらに備える、

請求項１から１８のいずれか１項に記載の異常車両検出サーバ。

【請求項２１】

前記異常車両判定部によって前記異常車種において前記第一の攻撃段階と判定された場合、前記異常車両と判定された車両、車種、および、位置情報の少なくとも１つの情報を表示し、前記第二の攻撃段階と判定された場合、前記攻撃の進行度が前記第一の攻撃段階より高い階層であると表示する異常表示部をさらに備える、

請求項３または４に記載の異常車両検出サーバ。

【請求項２２】

車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、

前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、

前記２以上の車両は、前記一の車両と同一の車種の車両を含み、

前記異常車両判定ステップは、前記一の車両の前記異常スコアと、前記一の車両と同一の車種の前記異常スコアに基づく前記統計値とを比較し、比較結果に基づいて前記一の車両が前記異常車両であるか否かを判定する、

異常車両検出方法。

【請求項２３】

車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、

前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判

定する異常車両判定ステップと、を含み、
前記２以上の車両は、前記一の車両と同一のエリアに位置する車両を含み、
前記異常車両判定ステップは、前記一の車両の前記異常スコアと、前記一の車両と同一のエリアに位置する車両の前記異常スコアに基づく前記統計値とを比較し、比較結果に基づいて前記一の車両が前記異常車両であるか否かを判定する、
異常車両検出方法。
【請求項２４】
車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、
前記異常車両判定ステップは、さらに、前記異常車両と同一の車種である異常車種または、前記異常車両が検出されたエリアである異常エリアにおいて、所定の台数以下の前記異常車両が存在する場合、前記リバースエンジニアリングにおける攻撃の進行度が第一の攻撃段階であると判定し、前記所定の台数より多い前記異常車両が存在する場合、前記第一の攻撃段階より前記リバースエンジニアリングにおける攻撃の進行度が進行した第二の攻撃段階であると判定する、
異常車両検出方法。
【請求項２５】
車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、
前記異常スコア取得ステップは、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定されるネットワーク機器の接続頻発、インターネット接続異常、診断コマンドの頻発、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前記不審挙動であると検出し、前記不審挙動を検出した場合、前記不審挙動をネットワーク解析活動であると判定し、前記一の車両の前記異常スコアを増加させる、
異常車両検出方法。
【請求項２６】
車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、
前記異常スコア取得ステップは、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定される車両制御機能の頻発、システムエラーの頻発、システムエラーの削除、故障コードの頻発、システムログイン、

および、ファイル数またはプロセス数の変化のいずれかを前記不審挙動であると検出し、前記不審挙動を検出した場合に、前記不審挙動をシステム解析活動であると判定し、前記一の車両の前記異常スコアを増加させる、
異常車両検出方法。
【請求項２７】
車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、
前記異常スコア取得ステップは、前記不審挙動を検出した場合であっても、前記不審挙動を検出した時刻に基づく所定の期間内に再度前記不審挙動を検出した場合または所定のエリアにて前記不審挙動を検出した場合、前記異常スコアを増加させない、
異常車両検出方法。
【請求項２８】
車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、
前記異常スコア取得ステップは、前記不審挙動が検出された時刻に基づく所定の期間中に、前記不審挙動が検出された車両において再度前記不審挙動が検出されなかった場合、前記異常スコアを減少させる、
異常車両検出方法。
【請求項２９】
車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、
前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含み、
前記異常車両判定ステップが前記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対策通知ステップをさらに含む、
異常車両検出方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、異常車両検出サーバおよび異常車両検出方法に関する。

【背景技術】
【０００２】
近年、自動車の中のシステムには、電子制御ユニット（以下、ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ））と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐネットワーク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（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、車載ネットワークトラフィックの増大が予想され、車載Ｅｔｈｅｒｎｅｔ（登録商標、以下同様（以下イーサネットとも記載する））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、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】
【文献】特許第５６６４７９９号公報
【非特許文献】
【０００５】
【文献】ＲＦＣ５４０６：Ｇｕｉｄｅｌｉｎｅｓ ｆｏｒ Ｓｐｅｃｉｆｙｉｎｇ ｔｈｅ Ｕｓｅ ｏｆ ＩＰｓｅｃ Ｖｅｒｓｉｏｎ２、２００９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、または、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る。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。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。
【０００７】
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異常検出サーバおよび車両異常検出方法を提供する。
【課題を解決するための手段】
【０００８】
本開示の一態様に係る車両異常検出サーバは、車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備える。
【０００９】
本開示の一態様に係る車両異常検出方法は、車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含む。

【発明の効果】

【００１０】

本開示の一態様に係る車両異常検出サーバ等によれば、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】

【００１１】

【図１】図１は、実施の形態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、実施の形態における異常スコア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、実施の形態における異常車両検出サーバが除外ルール共有サーバ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す図である。

【図１５】図１５は、実施の形態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、実施の形態における異常対策処理のフローチャートである。

【図２３】図２３は、実施の形態における異常カテゴリ別の異常対策処理のフローチャートの一例である。

【図２４】図２４は、実施の形態における異常カテゴリ別の異常対策処理のフローチャートの他の一例である。

【図２５】図２５は、実施の形態におけるエリア別攻撃段階判定処理のフローチャートである。

【図２６】図２６は、実施の形態における車種別攻撃段階判定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】

【００１２】

（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。

【００１３】
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。
【００１４】
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車載ネットワークのリバースエンジニアリングを事前に行う。このとき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または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る。
【００１５】
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異常検出サーバ等について鋭意検討を行い、以下に説明する車両異常検出サーバ等を創案した。例えば、本願発明者らは、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リングによって発生する所定（例えば通常）とは異なる車両挙動を不審挙動と捉え、車両がリバースエンジニアリングされている可能性の高さを示す異常スコアを算出し、同一車種等の異常スコアの統計値（例えば、平均値）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とに基づいて異常に対して対策を実施することで、車載ネットワークの安全性を効果的に高めることができることを見出した。
【００１６】
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を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得部と、前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定部と、を備える。
【００１７】
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、車載ネットワークシステムの安全性を効果的に高めることができる。
【００１８】
また、例えば、前記２以上の車両は、前記一の車両と同一の車種の車両を含み、前記異常車両判定部は、前記一の車両の前記異常スコアと、前記一の車両と同一の車種の前記異常スコアに基づく前記統計値とを比較し、比較結果に基づいて前記一の車両が前記異常車両であるか否かを判定してもよい。
【００１９】
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、車載ネットワークシステムの安全性をより効果的に高めることができる。
【００２０】
また、例えば、前記２以上の車両は、前記一の車両と同一のエリアに位置する車両を含み、前記異常車両判定部は、前記一の車両の前記異常スコアと、前記一の車両と同一のエリアに位置する車両の前記異常スコアに基づく前記統計値とを比較し、比較結果に基づいて前記一の車両が前記異常車両であるか否かを判定してもよい。
【００２１】
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、車載ネットワークシステムの安全性をより効果的に高めることができる。
【００２２】

また、例えば、前記異常車両判定部は、さらに、前記異常車両と同一の車種である異常車種または、前記異常車両が検出されたエリアである異常エリアにおいて、所定の台数以下の前記異常車両が存在する場合、前記リバースエンジニアリングにおける攻撃の進行度が第一の攻撃段階であると判定し、前記所定の台数より多い前記異常車両が存在する場合、前記第一の攻撃段階より前記リバースエンジニアリングにおける攻撃の進行度が進行した第二の攻撃段階であると判定してもよい。

【００２３】

これにより、所定の台数以下の少数の車両にのみ異常が発生している場合は、攻撃者が異常車両を解析途中である第一の攻撃段階（例えば偵察フェーズ）であると判定でき、所定の台数より多い車両に異常が発生している場合は、第二の攻撃段階（例えば、攻撃者が車両のネットワーク解析およびシステム解析に成功して他の車両への攻撃適用を試行しているデリバリーフェーズ）であると判定できる。攻撃段階が判定できれば、対策の手段の切り替えおよび解析の優先度の変更が可能となる。

【００２４】

また、例えば、前記異常スコア取得部は、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定されるネットワーク機器の接続頻発、インターネット接続異常、診断コマンドの頻発、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前記不審挙動であると検出し、前記不審挙動を検出した場合、前記不審挙動をネットワーク解析活動であると判定し、前記一の車両の前記異常スコアを増加させてもよい。

【００２５】

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車載ネットワークシステムの安全性をより一層効果的に高めることができる。

【００２６】

また、例えば、さらに、異常対策通知部を備え、前記異常スコア取得部が前記不審挙動を前記ネットワーク解析活動であると判定した場合、前記異常対策通知部は、前記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、アクセス先およびアクセス元のアドレスの制限、前記ネットワーク機器の接続数の制限、および、ドライバへの警告のいずれか１つ以上を実施させてもよい。

【００２７】

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、車載ネットワークシステムの安全性をより一層効果的に高めることができる。

【００２８】

また、例えば、前記異常スコア取得部は、前記車両ログに含まれる前記イベント内容に基づいて前記異常スコアを算出し、前記イベント内容に基づいて特定される車両制御機能の頻発、システムエラーの頻発、システムエラーの削除、故障コードの頻発、システムログイン、および、ファイル数またはプロセス数の変化のいずれかを前記不審挙動であると検出し、前記不審挙動を検出した場合に、前記不審挙動をシステム解析活動であると判定し、前記一の車両の前記異常スコアを増加させてもよい。

【００２９】

これにより、攻撃者が車両システムの車両制御機能または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、車載ネットワークシステムの安全性をより一層効果的に高めることができる。

【００３０】

また、例えば、さらに、異常対策通知部を備え、前記異常スコア取得部が前記不審挙動を前記システム解析活動であると判定した場合、前記異常対策通知部は、前記異常スコアの値に応じて、車両制御機能の起動停止、前記車両ログの送信頻度の増加、前記車両ログの種類数の増加、および、ドライバへの警告のいずれか１つ以上を実施させてもよい。

【００３１】

これにより、攻撃者が車両システムの車両制御機能または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、車載ネットワークシステムの安全性をより一層効果的に高めることができる。

【００３２】

また、例えば、前記異常スコア取得部は、前記不審挙動を検出した場合であっても、前記不審挙動を検出した時刻に基づく所定の期間内に再度前記不審挙動を検出した場合または所定のエリアにて前記不審挙動を検出した場合、前記異常スコアを増加させなくてもよい。

【００３３】

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、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を不審挙動であると検出することによる誤検知を防ぐことができるため、不審挙動の検出精度を効果的に向上させることができる。

【００３４】

また、例えば、前記異常スコア取得部は、前記不審挙動が検出された時刻に基づく所定の期間中に、前記不審挙動が検出された車両において再度前記不審挙動が検出されなかった場合、前記異常スコアを減少させなくてもよい。

【００３５】

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、攻撃対象車両であるか否かの判定精度を効果的に向上させることができる。

【００３６】

また、例えば、前記異常車両判定部が前記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対策通知部をさらに備えてもよい。

【００３７】

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、および、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、攻撃者の解析の妨害および攻撃者の攻撃内容の把握を効率的に行うことができる。

【００３８】

また、例えば、前記異常車両判定部によって前記異常車種が前記第二の攻撃段階であると判定された場合、前記異常車両と判定した車両と同一の車種の車両に対して、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つ以上を要求する異常対策通知部をさらに備えてもよい。

【００３９】

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、および、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、攻撃者の解析の妨害および攻撃者の攻撃内容の把握を効率的に行うことができる。

【００４０】

また、例えば、前記異常車両判定部によって前記異常エリアにおいて前記異常車両が前記第二の攻撃段階であると判定された場合、当該異常エリアに位置する前記異常車両以外

の車両に対して、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つ以上を要求する異常対策通知部をさらに備えてもよい。

【００４１】

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、および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、攻撃者の解析の妨害および攻撃者の攻撃内容の把握を効率的に行うことができる。

【００４２】

また、例えば、前記異常スコアが高い順に前記異常車両をリスト表示する異常表示部をさらに備えてもよい。

【００４３】

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、解析作業を効果的に行うことができる。

【００４４】

また、例えば、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表示部をさらに備えてもよい。

【００４５】

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定でき、解析の手がかりとすることができるため、解析作業を効果的に行うことができる。

【００４６】

また、例えば、前記異常車両判定部によって前記異常車種において前記第一の攻撃段階と判定された場合、前記異常車両と判定された車両、車種、および、位置情報の少なくとも１つの情報を表示し、前記第二の攻撃段階と判定された場合、前記攻撃の進行度が前記第一の攻撃段階より高い階層であると表示する異常表示部をさらに備えてもよい。

【００４７】

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を把握することができ、解析の優先度をつけることができるため、解析作業をより効果的に行うことができる。

【００４８】

また、本開示の一実施態様の異常車両検出方法は、車両に搭載された車両システムにおいて発生したイベント内容を含む車両ログに基づく車両情報であって複数の車両のそれぞれから受信した複数の前記車両情報に基づいて、所定の運転挙動とは異なる不審挙動を検出し、前記複数の車両のそれぞれについて、当該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取得する異常スコア取得ステップと、前記複数の車両のうちの一の車両の前記異常スコアと前記複数の車両のうちの２以上の車両の前記異常スコアの統計値とに基づいて、前記一の車両が異常車両であるか否かを判定する異常車両判定ステップと、を含む。

【００４９】

これにより、上記異常車両検出サーバと同様の効果を奏する。

【００５０】

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。

【００５１】

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。

【００５２】

（実施の形態）

［１　異常車両検出システムの全体構成図］

図１は、本実施の形態における異常車両検出システムの全体構成を示す図である。図１に示すように、異常車両検出システムは、異常車両検出サーバ１０と、車両システム２０と、除外ルール共有サーバ３０とを備える。また、異常車両検出システムでは、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と、車両システム２０とが通信可能に接続される。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）、または、３Ｇ／ＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）であっても良いが、これに限定されない。

【００５３】

車両システム２０は、車両に搭載され、車両ログ送信装置２００を備える。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へ送信する通信装置である。車両ログの詳細は後述する。なお、図１では、異常車両検出システムが備える車両システム２０は１台のみである場合を示しているが、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へ送信してもよい。異常車両検出システムは、例えば、複数の車両システム２０を備えていてもよい。

【００５４】

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２０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。除外ルールは、車両システム２０のソフトウェアアップデートのリスト、または、ディーラー、開発拠点、検証拠点、修理業者などのリストを含む。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と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、その期間、および、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。

【００５５】

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する。そして、異常車両検出サーバ１０は、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と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。

【００５６】

なお、異常スコアの算出は、以下では、異常車両検出サーバ１０で行われる例について説明するが、車両システム２０により行われてもよい。異常車両検出サーバ１０は、外部ネットワークを介して車両システム２０から当該車両システム２０の異常スコアを取得してもよい。異常車両検出サーバ１０が外部ネットワークを介して車両システム２０から取得する車両ログまたは異常スコアは、車両ログに基づく車両情報の一例である。

【００５７】

［２　車両システムの構成図］

図２は、本実施の形態における車両システム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とを備える。車両ログ送信装置２００と、セントラルＥＣＵ３００と、ＺｏｎｅＥＣＵ４００ａと、ＺｏｎｅＥＣＵ４００ｂと、ＺｏｎｅＥＣＵ４００ｃと、ＺｏｎｅＥＣＵ４００ｄとは、車載ネットワークであるイーサネット１３を介して接続される。ボディＥＣＵ５００ａと、ＺｏｎｅＥＣＵ４００ａとは、イーサネット１１を介して接続される。また、カーナビＥＣＵ５００ｂと、ＺｏｎｅＥＣＵ４００ｂとは、イーサネット１２を介して接続される。また、ステアリングＥＣＵ５００ｃと、ＺｏｎｅＥＣＵ４００ｃとは、ＣＡＮ１４を介して接続される。また、ブレーキＥＣＵ５００ｄと、ＺｏｎｅＥＣＵ４００ｄとは、ＣＡＮ－ＦＤ（ＣＡＮ ｗｉｔｈ Ｆｌｅｘｉｂｌｅ Ｄａｔａ Ｒａｔｅ）１５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とは、外部ネットワークにも接続される。

【００５８】

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。

【００５９】

セントラルＥＣＵ３００は、イーサネット１３を介して、ＺｏｎｅＥＣＵ４００ａ、ＺｏｎｅＥＣＵ４００ｂ、ＺｏｎｅＥＣＵ４００ｃ、および、ＺｏｎｅＥＣＵ４００ｄを制御し、車両システム２０全体を制御する。例えば、セントラルＥＣＵ３００は、自動駐車、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２０内で発生したネットワーク機器の接続またはインターネット接続異常などのイベント情報を、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。

【００６０】

ＺｏｎｅＥＣＵ４００ａ、ＺｏｎｅＥＣＵ４００ｂ、ＺｏｎｅＥＣＵ４００ｃ、および、ＺｏｎｅＥＣＵ４００ｄは、イーサネット１３を介して、セントラルＥＣＵ３００と他のＺｏｎｅＥＣＵとを通信する。例えば、ＺｏｎｅＥＣＵ４００ａは、イーサネット１１を介して、ボディＥＣＵ５００ａと通信し、車両のロック、ワイパーなどの車体に関わる機能を制御する。また、ＺｏｎｅＥＣＵ４００ｂは、イーサネット１２を介して、カーナビＥＣＵ５００ｂと通信し、カーナビの表示を制御する。例えば、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する。また、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。

【００６１】

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。

【００６２】

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。

【００６３】

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。

【００６４】

ブレーキＥＣＵ５００ｄは、車両に搭載されるブレーキを制御する。

【００６５】

［３ 異常車両検出サーバ１０の構成図］

図３は、本実施の形態における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とを有する。

【００６６】

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、受信した除外ルールを除外ルール受信部１０４へ送信する。

【００６７】

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、受信した車両ログを車両ログ記憶部１０３へ記憶する。

【００６８】

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、受信した除外ルールをルール記憶部１０５へ記憶する。

【００６９】

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とが記載された対策ルールを記憶する。また、ルール記憶部１０５は、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。

【００７０】

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とを取得し、車両ログに記載されたイベント内容と、異常ルールと、除外ルールとに基づき、車両１台ごとに異常スコアを算出することで車両１台ごとの異常スコアを取得する。異常スコア算出部１０６は、例えば、車両システム２０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に基づく車両情報であって複数の車両のそれぞれから受信した複数の車両情報のイベント内容に基づいて、所定の運転挙動とは異なる不審挙動を検出し、複数の車両のそれぞれについて、当該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取得する異常スコアを算出する。異常スコア算出部１０６は、例えば、車両ログに含まれるイベント内容に基づいて、異常スコアを算出する。そして、異常スコア算出部１０６は、取得した（例えば、算出した）異常スコアを異常スコア記憶部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。異常スコア算出部１０６は、異常スコア取得部の一例である。

【００７１】

異常スコアは、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、異常スコアは、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、異常スコアは、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、車載ネットワークを解析することである。よって、異常スコアは、例えば、車両の車載ネットワーク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。

【００７２】

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。異常車両判定部１０８は、例えば、複数の車両のうちの一の車両の異常スコアと複数の車両のうち２以上の車両の異常スコアの統計値とに基づいて、一の車両が異常車両であるか否かを判定することで異常車両を検出する。また、異常車両判定部１０８は、異常車両の情報（例えば、車両情報）に基づいて、攻撃段階を判定する。異常車両の検出方法の詳細および攻撃段階の判定方法の詳細については後述する。また、２以上の車両は、異常車両であると判定された一の車両と同一の車種の車両を含んでいてもよいし、当該一の車両と同一のエリアに位置する車両を含んでいてもよい。また、２以上の車両は、当該一の車両と同一のＥＣＵを搭載する車両を含んでいてもよいし、当該一の車両と同一サプライヤ（同一メーカ）の車両を含んでいてもよいし、当該一の車両と同一の基地局を使用して無線通信している車両を含んでいてもよい。なお、２以上の車両に当該一の車両が含まれていてもよいし、含まれていなくてもよい。

【００７３】
異常対策通知部１０９は、異常車両判定部１０８が異常車両であると判定した車両と、異常車両と同一の車種の車両、および、異常車両と同一のエリアに位置する車両の少なくとも１つの車両とに対して、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、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、および、ドライバへの通知のうち、いずれか１つ以上の対策を含む通知である。異常対策通知部１０９は、不審挙動がネットワーク解析活動またはシステム解析活動であると判定された場合、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へ通知することで上記のいずれか１つ以上の対策を車両システム２０に実行させる。
【００７４】
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と、当該車両（異常車両）と同一の車種の車両、および、当該車両（異常車両）と同一のエリアに位置する車両の少なくとも１つの車両とに関する情報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、異常表示部１１０は、グラフィカルユーザーインターフェースを用いて当該情報を表示する。当該情報は、ユーザが重点的に監視する異常車両を特定可能な情報を含む。
【００７５】
［４　車両ログ送信装置の構成図］
図４は、本実施の形態における車両ログ送信装置２００の構成図である。車両ログ送信装置２００は、車両側通信部２１０と、車両ログ送信部２２０と、異常対策部２３０とを有する。
【００７６】
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、各種情報を交換する。
【００７７】
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へ受信した車両ログを送信する。
【００７８】
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、受信した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。異常対策部２３０は、例えば、対策通知内容が車両制御機能制限である場合、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る場合、車両ログ送信部２２０へ送信頻度の増加を指示する。
【００７９】
［５　車両ログの一例］
図５は、本実施の形態における車両ログ記憶部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２０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、イベント名を含んで構成される。図５では、車両ログ番号が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情報を用いて取得される、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、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、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。
【００８０】
また、車両制御機能作動は、緊急ブレーキ作動または自動駐車モードの起動など、車両システム２０を制御する機能が作動したイベントである。
【００８１】
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上で発生したネットワークエラーが発生したイベントである。また、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するイベントである。
【００８２】
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。
【００８３】
また、アドレスＢからアクセスは、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されたイベントである。
【００８４】
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。
【００８５】
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。
【００８６】
つまり、図５の例では、車両識別子が同一であり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とを参照することで、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。
【００８７】
また、車両識別子が同一であり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とを参照することで、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（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）切断およびＶＰＮ接続についても同様である。
【００８８】
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、Ｙ３」というエリアで発動し、時刻ＴＡ２４に、「Ｘ１、Ｙ４」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。エリアは、予め地図上において設定される領域（静的な領域）であってもよいし、異常車両の位置に応じて設定される領域（動的な領域）であってもよい。
【００８９】
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とを参照すれば、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。
【００９０】
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。イベント名は、イベント内容の一例である。
【００９１】
また、車両ログに含まれる時刻情報を参照することで、あるイベントが所定の期間内に所定の回数発生した場合に異常スコアを加算するという異常ルールに対して一致するか否

かを判定することが可能である。
【００９２】
［６　異常ルールの一例］
図６は、本実施の形態におけるルール記憶部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、異常カテゴリを含む。異常ルール内容が示す不審挙動の発生は、車両ログ（例えば、イベント名など）に基づいて特定可能である。
【００９３】
図６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」であり、異常カテゴリが「ネットワーク解析」であることが分かる。図６には、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ている。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ている。
【００９４】
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２０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回の接続を異常として判定する。
【００９５】
インターネットまたはＶＰＮ遮断は、攻撃者が車両システム２０および車両システム２０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分間に１回の発生を異常として判定する。
【００９６】
アクセス先アドレスの変化は、攻撃者が車両システム２０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、一例として１回で異常として判定する。
【００９７】
アクセス元アドレスの変化は、攻撃者が車両システム２０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。
【００９８】
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場合に発生するため、１時間に１０回の発生を異常として判定する。
【００９９】
システムエラー発生は、攻撃者が車両システム２０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時間に２回の発生で異常として判定する。
【０１００】
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回で異常として判定する。
【０１０１】
システムログインは、攻撃者が車両システム２０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。
【０１０２】
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２０にインストールした際に、ファイル数またはプロセス数が増加するため、１回で異常として判定する。
【０１０３】
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る。ネットワーク解析は、攻撃者が車両システム２０の通信機能を解析している可能性が高いこと

を示す。ネットワーク解析は、攻撃者が車両システム２０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。

【０１０４】

異常スコア算出部１０６は、例えば、ネットワーク機器の接続頻発、インターネット接続異常、診断コマンドの頻発、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であると検出し、当該不審挙動が発生した場合に、ネットワーク解析活動であると判定し、当該車両の異常スコアを増加させてもよい。また、異常スコア算出部１０６は、例えば、車両制御機能の頻発、システムエラーの頻発、システムエラーの削除、故障コードの頻発、システムログイン、および、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であると検出し、当該不審挙動が発生した場合に、システム解析活動であると判定し、当該車両の異常スコアを増加させてもよい。

【０１０５】

なお、図６に示す、異常ルールは一例であり、これに限定されない。また。図６に示す期間、回数、異常スコアの数値は一例であり、これに限定されない。

【０１０６】

［７　除外ルールの一例］

図７は、本実施の形態におけるルール記憶部１０５に格納される除外ルールの一例である。図７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。

【０１０７】

図７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示す「―」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では、修理業者Ａが存在し、修理業者Ａが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示す。

【０１０８】

また、図７の除外ルール番号が４である行では、位置情報が「日本」、有効期間が「Ｔ３～Ｔ４」、内容が「ソフト更新Ａ」、除外対象ルールが「ファイル数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２０のソフトウェア更新が行われるので、それに伴い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示す。

【０１０９】

また、図７の除外ルール番号Ｍの行では、位置情報Ｘ４、Ｙ４が示すエリアに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切断が発生する可能性があることから、インターネットまたはＶＰＮ切断が発生しても異常と判定せずに異常スコアをカウントしないことを示す。

【０１１０】

［８　異常スコアの一例］

図８は、本実施の形態における異常スコア記憶部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、除外ルールと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とを含む。なお、異常スコアは、少なくとも車両ログと、異常ルールとを用いて算出されればよい。

【０１１１】

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、車両別異常スコアでは、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車両別に記憶される。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るので、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。

【０１１２】

車種別平均異常スコアには、異常ルール番号および車種ごとに異常スコアが算出され、車種ごとの平均値が含まれる。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。

【０１１３】

エリア別平均異常スコアには、異常ルール番号および車種ごとに異常スコアが算出され、エリアごとの平均値が含まれる。例えば、異常ルール番号が６である行では、位置情報Ｘ２、Ｙ２が示すエリアの平均異常スコアが０．５であることを示している。

【０１１４】

［９　対策ルールの一例］

図９は、本実施の形態におけるルール記憶部１０５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、対策ルール内容とを含む。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、当該異常カテゴリの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と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。

【０１１５】

異常対策通知部１０９は、例えば、異常カテゴリがネットワーク解析であり、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ス元アドレスを制限」を選択する。

【０１１６】

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。図９の対策ルールに基づいて対策が選択されることで、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、異常スコアが小さいほど、攻撃者の攻撃試行の可能性が低いため、車両システム２０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。

【０１１７】

「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。

【０１１８】

「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。

【０１１９】

「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。

【０１２０】

「車両制御機能を停止」は、例えば、自動駐車モードまたは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。

【０１２１】

「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、つまり車両ログの送信頻度を増加することで、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。

【０１２２】

「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、つまり車両ログの種類数を増加することで、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。

【０１２３】

「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。

【０１２４】

図９に示すように、異常対策通知部１０９は、例えば、不審挙動がネットワーク解析活動であると判定された場合、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を遮断、アクセス先とアクセス元アドレスを制限、ネットワーク接続機器数を制限、および、ドライバへの警告のいずれか１つ以上を実施させる。また、異常対策通知部１０９は、例えば、不審挙動がシステム解析活動であると判定された場合、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、および、ドライバへの警告のいずれか１つ以上を実施させる。

【０１２５】

［１０　異常スコアリスト表示画面の一例］

図１０は、本実施の形態における異常表示部１１０が表示する異常スコアリスト表示画面の一例である。異常表示部１１０は、異常スコアリスト表示画面において、例えば、異常スコアの大きい順に車両識別子を並べて表示する。異常表示部１１０は、例えば、異常スコアが高い順に異常車両をリスト表示してもよい。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。なお、異常スコアリスト表示画面では、異常スコアの大きい順に車両識別子を表示することに限定されない。

【０１２６】

［１１　異常スコア地図表示画面の一例］

図１１は、本実施の形態における異常表示部１１０が表示する異常スコア地図表示画面の一例である。当該画面には、地図が表示されており、地図上に緯度Ｘ２、Ｘ３、Ｘ４と、経度Ｙ２、Ｙ３、Ｙ４が表示されている。また、異常車両と判定された車両の最新の位置である位置情報Ｘ４、Ｙ４に、異常車両が存在することを示す表示を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。例えば、異常エリアは、異常車両が異常と判定された地点を含む静的または動的なエリアであってもよい。図１１は、例えば、位置情報Ｘ３、Ｙ３が示す位置において車両が異常と判定され、異常と判定された異常車両が位置情報Ｘ４、Ｙ４が示す位置まで移動したことを示している。異常エリアと最新の異常車両の位置とは、地図上において互いに異なる位置であってもよい。このように、異常表示部１１０は、例えば、異常車両と判定された車両の位置情報を地図上に表示してもよい。

【０１２７】

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、地図上の施設名等から、攻撃者による攻撃の状況を推測することができる。

【０１２８】

［１２　異常スコア段階表示画面の一例］

図１２は、本実施の形態における異常表示部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（Ｃｏｍｍａｎｄ　ａｎｄ　Ｃｏｎｔｒｏｌ）、目的実行を段階に分けて表示される。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と判定された場合、チェックマークが偵察の列に表示され、現在デリバリーフェーズであると判定された場合、チェックマークがデリバリーの列に表示される。図１２では、車両識別子Ａ１の車両が現在偵察フェーズおよびデリバリーフェーズであると判定された例を示している。偵察フェーズであることの判定方法およびデリバリーフェーズであることの判定方法の詳細は後述する。

【０１２９】
異常表示部１１０は、例えば、異常車両判定部１０８によって異常車種が偵察フェーズ（第一の攻撃段階の一例）であると判定された場合、異常車両と判定された車両、当該車両の車種、および、当該車両の位置情報の少なくとも１つの情報を表示し、偵察フェーズより攻撃の進行度が高いデリバリフェーズ（第二の攻撃段階の一例）であると判定された場合、現在がデリバリーフェーズの階層であることを示す情報を表示してもよい。なお、位置情報は、異常車両の現在位置を示す情報であるが、異常車両であると判定された位置を示す情報であってもよい。
【０１３０】
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。
【０１３１】
なお、攻撃の進行度は、サイバーキルチェーンに基づく進行度を示しているが、サイバーキルチェーンに基づく進行度に限定されない。
【０１３２】
［１３　車両ログ受信処理のシーケンス］
図１３は、本実施の形態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。
【０１３３】
（Ｓ１３０１）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。
【０１３４】
（Ｓ１３０２）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。
【０１３５】
（Ｓ１３０３）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。
【０１３６】
（Ｓ１３０４）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、受信した車両ログを車両ログ受信部１０２へ転送する。サーバ側通信部１０１は、複数の車両のそれぞれから車両ログを受信し、受信した複数の車両ログのそれぞれを車両ログ受信部１０２へ転送する。
【０１３７】
（Ｓ１３０５）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、受信した車両ログを車両ログ記憶部１０３に記憶する。
【０１３８】
図１３に示す動作は、定期的に実行されてもよいし、異常車両検出サーバ１０が複数の車両に車両ログを送信することを示す指示を送信することで実行されてもよい。
【０１３９】
［１４　除外ルール受信処理のシーケンス］
図１４は、本実施の形態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。
【０１４０】
（Ｓ１４０１）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の車両側通信部２１０に送信する。
【０１４１】
（Ｓ１４０２）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、受信した除外ルールを除外ルール受信部１０４へ転送する。
【０１４２】

（Ｓ１４０３）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、受信した除外ルールをルール記憶部１０５に記憶する。

【０１４３】

図１４に示す動作は、定期的に実行されてもよいし、異常車両検出サーバ１０が複数の車両から車両ログを受信すること、異常車両検出サーバ１０が複数の車両に車両ログを送信することを示す指示を送信すること、または、後述する図１５に示す動作を実行することをトリガとして実行されてもよい。

【０１４４】

［１５　異常スコア算出処理のシーケンス］

図１５は、本実施の形態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。

【０１４５】

（Ｓ１５０１）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とを取得する。

【０１４６】

（Ｓ１５０２）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、異常ルールとに基づき、異常スコアを算出して、異常スコア記憶部１０７に記憶する。異常スコア算出部１０６は、複数の車両のそれぞれにおいて異常スコアを算出し、算出した複数の車両それぞれの異常スコアを異常スコア記憶部１０７に記憶する。異常スコア算出部１０６は、例えば、複数の車両のそれぞれにおいて、異常カテゴリごとに異常スコアを算出してもよい。

【０１４７】

（Ｓ１５０３）異常スコア算出部１０６は、異常スコアを算出後、異常スコアを更新したことを異常車両判定部１０８へ通知する。異常スコア算出部１０６は、例えば、複数の車両のそれぞれにおいて、異常スコアを算出した後、異常車両判定部１０８へ通知する。また、異常スコア算出部１０６は、異常スコアを更新した車両を特定するための情報（例えば、車両識別子など）を当該通知とともに異常車両判定部１０８に送信してもよい。

【０１４８】

（Ｓ１５０４）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。

【０１４９】

［１６　異常対策処理のシーケンス］

図１６は、本実施の形態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。

【０１５０】

（Ｓ１６０１）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（例えば、異常エリア）と、異常スコアとを異常対策通知部１０９へ送信する。

【０１５１】

（Ｓ１６０２）異常車両検出サーバ１０の異常対策通知部１０９は、ステップＳ１６０１で送信された情報に基づいて、該当する車両へ異常が検出されたことを示す通知（異常車両通知）をするよう、当該通知をサーバ側通信部１０１へ送信する。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、受信した異常車両の車種と同一の車種の車両、および、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の少なくとも一方の車両へ異常が検出されたことを示す通知（異常車両通知）をするよう、当該通知をサーバ側通信部１０１へ送信する。異常対策通知部１０９は、例えば、ステップＳ１６０２において、異常車両と、当該異常車両と同一車種の車両および異常車両と同一エリアに位置する車両の少なくとも一方の車両とへ異常が検出されたことを示す通知をするよう、当該通知をサーバ側通信部１０１へ送信してもよい。当該通知は、異常カテゴリごと

の異常スコアを含んでいてもよい。
【０１５２】
（Ｓ１６０３）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、ステップＳ１６０２の通知（異常車両通知）を車両ログ送信装置２００の車両側通信部２１０へ送信する。
【０１５３】
（Ｓ１６０４）車両ログ送信装置２００の車両側通信部２１０は、ステップＳ１６０２の通知（異常車両通知）を異常対策部２３０へ送信する。
【０１５４】
（Ｓ１６０５）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。異常対策部２３０は、ステップＳ１６０２の通知（異常車両通知）と図９に示す対策ルールとに基づいた異常対策を車両ログ送信部２２０へ要求する。異常対策部２３０は、例えば、異常カテゴリがシステム解析であり、システム解析の異常カテゴリにおける異常スコアが１０以上２０未満である場合、車両ログの種類数の増加を車両ログ送信部２２０へ要求する。また、異常対策部２３０は、例えば、異常カテゴリがシステム解析であり、システム解析の異常カテゴリにおける異常スコアが２０以上３０未満である場合、車両ログの送信頻度増加を車両ログ送信部２２０へ要求する。
【０１５５】
（Ｓ１６０６）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。異常対策部２３０は、例えば、セントラルＥＣＵ３００に車両制御機能の制限（機能制限）を要求する。
【０１５６】
［１７　異常表示処理のシーケンス］
図１７は、本実施の形態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。
【０１５７】
（Ｓ１７０１）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、エリアとを異常表示部１１０へ送信する。異常車両判定部１０８は、さらに、異常スコアを異常表示部１１０へ送信してもよい。
【０１５８】
（Ｓ１７０２）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、エリアとを、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。異常表示部１１０は、異常車両判定部１０８から異常スコアを取得した場合、取得した異常スコアもグラフィカルユーザーインターフェースを用いて表示してもよい。
【０１５９】
（Ｓ１７０３）異常車両検出サーバ１０の異常車両判定部１０８は、エリア別の攻撃段階および車種別の攻撃段階を判定し、判定結果を異常表示部１１０へ送信する。攻撃段階の判定方法については後述する。
【０１６０】
（Ｓ１７０４）異常車両検出サーバ１０の異常表示部１１０は、受信した攻撃段階を、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。
【０１６１】
なお、ステップＳ１７０３およびＳ１７０４の処理は、行われなくてもよい。また、ステップＳ１７０３は、異常車両が存在する場合に実行される。
【０１６２】
［１８　車両別異常スコア算出処理のフローチャート］
図１８は、本実施の形態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。具体的には、図１８は、図１５に示すステップＳ１５０２の処理の一部を詳細に示しており、車両ごとに異常スコアを算出する処理を示すフローチャートである。

【０１６３】
（Ｓ１８０１）異常スコア算出部１０６は、変数ｉを用意し、ｉ＝１とする。そして、ステップＳ１８０２を実施する。ここで変数ｉは、１～Ｎの値で、Ｎは異常ルール数を示す。
【０１６４】
（Ｓ１８０２）異常スコア算出部１０６は、異常ルールｉを選択し、ステップＳ１８０３を実施する。
【０１６５】
（Ｓ１８０３）異常スコア算出部１０６は、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、異常ルールとを参照し、車両ログのイベントが異常ルールｉと合致し、異常であるか否かを判定する。異常スコア算出部１０６は、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（Ｓ１８０３でＹｅｓ）、ステップＳ１８０４を実施する。また、異常スコア算出部１０６は、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（Ｓ１８０３でＮｏ）、ステップＳ１８０５を実行する。
【０１６６】
（Ｓ１８０４）異常スコア算出部１０６は、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、除外ルールとを参照し、異常ルールｉが除外対象の異常ルールであるか否かを判定する。異常スコア算出部１０６は、異常ルールｉが除外対象の異常ルールでない場合（Ｓ１８０４でＮｏ）、ステップＳ１８０６を実行し、異常ルールｉが除外対象の異常ルールである場合（Ｓ１８０４でＹｅｓ）、ステップＳ１８０５を実行する。これにより、異常スコア算出部１０６は、システムエラーが解除されやすいディーラーもしくは修理業者による作業中、および、システム内のファイル数が増減する可能性のあるソフト更新期間中において、異常車両の誤検知を防ぐことが可能となる。
【０１６７】
（Ｓ１８０５）異常スコア算出部１０６は、異常スコアに記載される最終異常日時（図８を参照）を参照し、現在の日時から２４時間経過しているか否かを判定する。異常スコア算出部１０６は、現在の日時が読み出した最終異常日時から２４時間経過している場合（Ｓ１８０５でＹｅｓ）、ステップＳ１８０７を実施する。また、異常スコア算出部１０６は、現在の日時が読み出した最終異常日時から２４時間経過していない場合（Ｓ１８０５でＮｏ）、ステップＳ１８０８を実施する。つまり、異常スコア算出部１０６は、車両ログに記載される車両識別子と対応する車両の異常スコアを、異常ルールｉの異常スコアを含めずに算出する。
【０１６８】
異常スコア算出部１０６は、不審挙動を検出した場合（Ｓ１８０３でＹｅｓ）であっても、不審挙動を検出した時刻に基づく所定の期間内に再度不審挙動が検出された場合（Ｓ１８０５でＮｏ）、車両の異常スコアを増加させなくてもよい。なお、ステップＳ１８０５の判定は、所定のエリアにて不審挙動が検出されたか否かにより行われてもよい。この場合、異常スコア算出部１０６は、不審挙動を検出した場合（Ｓ１８０３でＹｅｓ）であっても、不審挙動を検出したエリアに基づく所定のエリアに再度不審挙動が検出された場合（Ｓ１８０５でＮｏ）、車両の異常スコアを増加させなくてもよい。所定の期間は、例えば、不審挙動を検出した時刻を当該期間の最初の時刻として含む期間であってもよい。
【０１６９】
（Ｓ１８０６）異常スコア算出部１０６は、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に、異常ルールｉに記載された異常スコアを加算し、ステップＳ１８０８を実施する。つまり、異常スコア算出部１０６は、車両ログに記載される車両識別子と対応する車両の異常スコアを、異常ルールｉの異常スコアを含めて算出する。
【０１７０】
（Ｓ１８０７）異常スコア算出部１０６は、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、ステップＳ１８０８を実施する。異常スコア算出部１０６は

、異常ルールｉが除外対象であり、かつ、現在の日時が最終異常日時から所定時間経過すると、異常スコアをリセットするとも言える。

【０１７１】

なお、異常スコア算出部１０６は、ステップＳ１８０７において、異常スコアを０にすることに限定されず、異常スコアを減らしてもよい。このように、異常スコア算出部１０６は、不審挙動が検出された時刻を含む所定の期間中に、不審挙動が検出された車両において再度不審挙動が検出されなかった場合、異常スコアを減少させてもよい。

【０１７２】

（Ｓ１８０８）異常スコア算出部１０６は、異常ルールｉがＮであるか否かを判定する。つまり、異常スコア算出部１０６は、全ての異常ルールｉに対して、ステップＳ１８０３以降の処理が行われたか否かを判定する。異常スコア算出部１０６は、異常ルールｉがＮである場合（Ｓ１８０８でＹｅｓ）、処理を終了し、そうでない場合（Ｓ１８０８でＮｏ）、ステップＳ１８０９を実施する。

【０１７３】

（Ｓ１８０９）異常スコア算出部１０６は、異常ルールｉを１インクリメントし、ステップＳ１８０２以降の処理を実施する。異常スコア算出部１０６は、次の異常ルールｉに対して、ステップＳ１８０３以降の処理を実施する。

【０１７４】

なお、異常スコア算出部１０６は、ステップＳ１８０８でＹｅｓの場合、車両ごとに、異常ルールｉごとの異常スコアに所定の演算を行ってもよい。異常スコア算出部１０６は、ステップＳ１８０８でＹｅｓの場合、異常ルール全ての異常スコアを合計するが、例えば、異常カテゴリごと（例えば、ネットワーク解析、システム解析ごと）の異常スコアを合計してもよい。このように算出された異常スコアの合計値は、車両別異常スコアの一例である。

【０１７５】

［１９　車種別異常スコア算出処理のフローチャート］

図１９は、本実施の形態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。具体的には、図１９は、図１５に示すステップＳ１５０２の処理の一部を詳細に示しており、異常車両判定部１０８による異常車両であるか否かの判定に用いられる車種ごとの統計値（図１９の例では、異常スコアの平均値）を算出する処理を示すフローチャートである。

【０１７６】

（Ｓ１９０１）異常スコア算出部１０６は、車両別異常スコアを異常スコア記憶部１０７から取得する。異常スコア算出部１０６は、例えば、図１８の動作により算出された車両ごとの車両別異常スコア（例えば、車両ごとの異常スコアの合計値）を取得する。

【０１７７】

（Ｓ１９０２）異常スコア算出部１０６は、変数ｉを用意し、ｉ＝１とする。そして、異常スコア算出部１０６は、ステップＳ１９０３を実施する。ここで変数ｉは、１～Ｎの値で、Ｎは異常ルール数を示す。

【０１７８】

（Ｓ１９０３）異常スコア算出部１０６は、異常ルールｉを選択し、ステップＳ１９０４を実施する。異常スコア算出部１０６は、例えば、異常ルール番号(図６を参照)から変数ｉに対応する異常ルールｉ（異常ルール内容）を選択する。異常スコア算出部１０６は、例えば、変数ｉ＝１である場合、異常ルール番号が１であるネットワーク機器接続を選択する。

【０１７９】

（Ｓ１９０４）異常スコア算出部１０６は、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、抽出したすべての車両の異常スコアの平均値を算出する。異常スコア算出部１０６は、車種のすべての車両の異常ルールｉにおける異常スコアの平均値を、当該車種の異常ルールｉにおける異常スコアとして算

出する。
【０１８０】
なお、車種の異常ルールｉにおける異常スコアは、平均値に限定されず、統計値であればよい。車種の異常ルールｉにおける異常スコアは、最大値、最小値、中央値、最頻値などであってもよいし、それ以外の統計値であってもよい。
【０１８１】
（Ｓ１９０５）異常スコア算出部１０６は、変数ｉがＮであるか否かを判定する。異常スコア算出部１０６は、変数ｉがＮである場合（Ｓ１９０５でＹｅｓ）、処理を終了し、そうでない場合（Ｓ１９０４でＮｏ）、ステップＳ１９０６を実施する。
【０１８２】
（Ｓ１９０６）異常スコア算出部１０６は、変数ｉを１インクリメントし、ステップＳ１９０３を実施する。異常スコア算出部１０６は、次の異常ルールに対して、ステップＳ１９０３以降の処理を実施する。
【０１８３】
なお、異常スコア算出部１０６は、ステップＳ１９０５でＹｅｓの場合、車種ごとに、異常ルールｉごとの異常スコアの平均値に所定の演算を行ってもよい。異常スコア算出部１０６は、ステップＳ１９０５でＹｅｓの場合、車種ごとに、全ての異常スコアの平均値を算出するが、例えば、異常カテゴリごと（例えば、ネットワーク解析、システム解析ごと）の異常スコアの平均値を算出してもよい。このように算出された異常スコアの合計値は、車種別異常スコアの一例である。
【０１８４】
［２０　エリア別異常スコア算出処理のフローチャート］
図２０は、本実施の形態における異常スコア算出部１０６のエリア別異常スコア算出処理のフローチャートを示す。具体的には、図２０は、図１５に示すステップＳ１５０２の処理の一部を詳細に示しており、異常車両判定部１０８による異常車両であるか否かの判定に用いられるエリア（例えば、異常エリア）ごとの統計値（図２０の例では、異常スコアの平均値）を算出する処理を示すフローチャートである。なお、図２０に示すステップＳ２００１～Ｓ２００３、Ｓ２００５およびＳ２００６のそれぞれは、図１９に示すステップＳ１９０１～Ｓ１９０３、Ｓ１９０５およびＳ１９０６のそれぞれと同様であり、説明を簡略化する。
【０１８５】
（Ｓ２００１）異常スコア算出部１０６は、車両別異常スコアを異常スコア記憶部１０７から取得する。
【０１８６】
（Ｓ２００２）異常スコア算出部１０６は、変数ｉを用意し、ｉ＝１とする。そして、ステップＳ２００３を実施する。ここで変数ｉは１～Ｎの値で、Ｎは異常ルール数を示す。
【０１８７】
（Ｓ２００３）異常スコア算出部１０６は、異常ルールｉを選択し、ステップＳ２００４を実施する。
【０１８８】
（Ｓ２００４）異常スコア算出部１０６は、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、抽出したすべての車両の異常スコアの平均値を算出する。異常スコア算出部１０６は、エリア内のすべての車両の異常ルールｉにおける異常スコアの平均値を、当該エリアの異常ルールｉにおける異常スコアとして算出する。
【０１８９】
なお、エリアの異常ルールｉにおける異常スコアは、平均値に限定されず、統計値であればよい。エリアの異常ルールｉにおける異常スコアは、最大値、最小値、中央値、最頻値などであってもよいし、それ以外の統計値であってもよい。
【０１９０】

（Ｓ２００５）異常スコア算出部１０６は、変数ｉがＮである場合（Ｓ２００５でＹｅｓ）、処理を終了し、そうでない場合（Ｓ２００５でＮｏ）、ステップＳ２００６を実施する。

【０１９１】

（Ｓ２００６）異常スコア算出部１０６は、変数ｉを１インクリメントし、ステップＳ２００３を実施する。

【０１９２】

なお、異常スコア算出部１０６は、ステップＳ２００５でＹｅｓの場合、エリアごとに、異常ルールｉごとの異常スコアの平均値に所定の演算を行ってもよい。異常スコア算出部１０６は、ステップＳ２００５でＹｅｓの場合、エリアごとに、当該エリアに位置する車両全ての異常スコアの平均値を算出するが、例えば、異常カテゴリごと（例えば、ネットワーク解析、システム解析ごと）の異常スコアの平均値を算出してもよい。このように算出された異常スコアの合計値は、エリア別異常スコアの一例である。

【０１９３】

［２１　異常車両検出処理のフローチャート］

図２１は、本実施の形態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。具体的には、図２１は、図１５に示すステップＳ１５０４の処理の一部を詳細に示すフローチャートである。

【０１９４】

（Ｓ２１０１）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、ステップＳ２１０２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。特定車両の異常スコアは、各異常ルールに対する異常スコアの合計値であるが、ネットワーク解析における異常スコアの合計値またはシステム解析における異常スコアの合計値であってもよい。ステップＳ２１０１は、取得ステップの一例である。

【０１９５】

（Ｓ２１０２）異常車両判定部１０８は、異常スコアが１０よりも大きいか否かを判定する。異常車両判定部１０８は、異常スコアが１０よりも大きい場合（Ｓ２１０２でＹｅｓ）、ステップＳ２１０３を実施し、そうでない場合（Ｓ２１０２でＮｏ）、ステップＳ２１０４を実施する。なお、ステップＳ２１０２の判定に用いる基準は、１０に限定されず、適宜決定されればよい。ステップＳ２１０２は、異常車両判定ステップの一例である。

【０１９６】

（Ｓ２１０３）異常車両判定部１０８は、ステップＳ２１０２でＹｅｓの場合、選択中の車両（特定車両）を異常車両として検出し、ステップＳ２１０４を実施する。

【０１９７】

（Ｓ２１０４）異常車両判定部１０８は、ステップＳ２１０１で取得した異常スコアが選択中の車両（特定車両）と同一車種の車種別異常平均スコアよりも大きいか否かを判定する。異常車両判定部１０８は、例えば、ステップＳ２１０４において、車両の異常スコアと、当該車両と同一の車種の車両の異常スコアに基づく統計値とを比較し、比較結果に基づいて当該車両が異常車両であるか否かを判定する。異常車両判定部１０８は、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（Ｓ２１０４でＹｅｓ）、ステップＳ２１０５を実施し、そうでない場合（Ｓ２１０４でＮｏ）、ステップＳ２１０６を実施する。ステップＳ２１０４は、異常車両判定ステップの一例である。

【０１９８】

（Ｓ２１０５）異常車両判定部１０８は、選択中の車両（特定車両）を異常車両として検出し、ステップＳ２１０１で取得した異常スコアを２倍にして、異常スコア記憶部１０７に記憶し、ステップＳ２１０６を実施する。異常車両判定部１０８は、ネットワーク解析に関する異常スコアおよびシステム解析に関する異常スコアの両方を２倍する。異常車両判定部１０８は、２倍にした異常スコアを特定車両の異常スコアとして異常スコア記憶部１０７に記憶する。異常車両判定部１０８は、特定車両の異常スコアを車種別異常平均

スコアに基づいて更新するとも言える。これにより、同一車種の車両において、通常と異なる運転挙動を示す車両の異常スコアをより大きくすることができるので、優先的に解析することができる。

【０１９９】

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、車両の走行時における運転状態の挙動（例えば、図６に示す車両制御機能作動など）、および、車両の内部処理における挙動（例えば、図６にネットワーク機器接続、システムエラー発生など）の両方が含まれる。通常の運転挙動は、所定の運転挙動の一例である。所定の運転挙動は、例えば、図６に示す異常ルール、期間、階数に該当しない運転挙動であってもよい。

【０２００】

（Ｓ２１０６）異常車両判定部１０８は、ステップＳ２１０１で取得した異常スコアが選択中の車両（特定車両）が存在するエリアのエリア別異常平均スコアよりも大きいか否かを判定する。異常車両判定部１０８は、車両の異常スコアと、当該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とを比較し、比較結果に基づいて当該車両が異常車両であるか否かを判定するとも言える。異常車両判定部１０８は、異常スコアが選択中の車両の存在エリアのエリア別異常平均スコアよりも大きい場合（Ｓ２１０６でＹｅｓ）、ステップＳ２１０７を実施し、そうでない場合（Ｓ２１０６でＮｏ）、処理を終了する。ステップＳ２１０６は、異常車両判定ステップの一例である。

【０２０１】

（Ｓ２１０７）異常車両判定部１０８は、選択中の車両（特定車両）を異常車両として検出し、ステップＳ２１０１で取得した異常スコアまたはステップＳ２１０５で算出された異常スコアを２倍にして、異常スコア記憶部１０７に記憶し、処理を終了する。異常車両判定部１０８は、ネットワーク解析に関する異常スコアおよびシステム解析に関する異常スコアの両方を２倍する。異常車両判定部１０８は、２倍にした異常スコアを特定車両の異常スコアとして異常スコア記憶部１０７に記憶する。異常車両判定部１０８は、特定車両の異常スコアをエリア別異常平均スコアに基づいて更新するとも言える。これにより、同一エリアの車両において、通常（所定の一例）と異なる運転挙動を示す車両の異常スコアをより大きくすることができるので、オペレーターに異常スコアが大きな異常車両を優先的に解析させることができる。

【０２０２】

なお、異常車両判定部１０８は、図２１に示すステップＳ２１０２、Ｓ２１０４およびＳ２１０６の判定のうち、少なくとも１つの判定により異常車両を検出してもよい。

【０２０３】

［２２　異常対策処理のフローチャート］

図２２は、本実施の形態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。具体的には、図２２は、図１６に示すステップＳ１６０２で通知する異常車両通知の内容を決定する処理を示すフローチャートである。

【０２０４】

（Ｓ２２０１）異常対策通知部１０９は、異常車両判定部１０８が検出した異常車両の情報を取得し、ステップＳ２２０２を実施する。当該情報には、異常スコアが含まれる。

【０２０５】

（Ｓ２２０２）異常対策通知部１０９は、異常車両と判定された車両の異常スコアを参照し、異常カテゴリごとの異常スコアの合計値を算出し、ステップＳ２２０３を実施する。

【０２０６】

（Ｓ２２０３）異常対策通知部１０９は、異常カテゴリが、ネットワーク解析である異常スコアの合計値（異常スコア合計値）に対する処理を実行する。

【０２０７】

（Ｓ２２０４）異常対策通知部１０９は、異常カテゴリが、システム解析である異常ス

コアの合計値（異常スコア合計値）に対する処理を実行する。

【０２０８】

ここで、図２２に示すステップＳ２２０３およびＳ２２０４の詳細について、図２３および図２４を参照しながら説明する。図２３は、本実施の形態における異常カテゴリ別の異常対策処理のフローチャートの一例である。図２３は、図２２に示すステップＳ２２０３の詳細を示すフローチャートの一例である。なお、図２３は、異常スコアのうち、ネットワーク解析における異常スコアを用いて行われる処理である。言い換えると、図２３に示す処理において、異常スコアのうち、システム解析における異常スコアは用いられない。なお、図２３に示す動作は、異常車両または異常エリアにおいて第二の攻撃段階であると判定された場合に実行されてもよい。

【０２０９】

（Ｓ２２３１）異常対策通知部１０９は、ネットワーク解析における異常カテゴリが３０（第１の閾値）以上であるか否かを判定する。異常対策通知部１０９は、異常カテゴリが３０以上である場合（Ｓ２２３１でＹｅｓ）、ステップＳ２２３２を実施する。

【０２１０】

（Ｓ２２３３）異常対策通知部１０９は、異常カテゴリが３０未満である場合（Ｓ２２３１でＮｏ）、異常カテゴリが２０以上（第１の閾値より小さい第２の閾値）であるか否かを判定する。異常対策通知部１０９は、３０未満２０以上である場合（Ｓ２２３３でＹｅｓ）、ステップＳ２２３４を実施する。

【０２１１】

（Ｓ２２３５）異常対策通知部１０９は、異常カテゴリが２０未満である場合（Ｓ２２３５でＮｏ）、異常カテゴリが１０以上（第２の閾値より小さい第３の閾値）であるか否かを判定する。異常対策通知部１０９は、２０未満１０以上の場合（Ｓ２２３５でＹｅｓ）、ステップＳ２２３６を実施する。

【０２１２】

（Ｓ２２３７）異常対策通知部１０９は、異常カテゴリが１０未満である場合（Ｓ２２３５でＮｏ）、異常カテゴリが１以上（第３の閾値より小さい第４の閾値）であるか否かを判定する。異常対策通知部１０９は、異常カテゴリが１以上の場合（Ｓ２２３７でＹｅｓ）、ステップＳ２２３８を実施し、異常カテゴリが０の場合（Ｓ２２３７でＮｏ）、対策を実施せずにステップＳ２２０４を実施する。

【０２１３】

（Ｓ２２３２）異常対策通知部１０９は、ネットワークインターフェースを遮断し、Ｓ２２０４を実施する。

【０２１４】

（Ｓ２２３４）異常対策通知部１０９は、アクセス先およびアクセス元アドレスを制限し、Ｓ２２０４を実施する。

【０２１５】

（Ｓ２２３６）異常対策通知部１０９は、ネットワーク接続機器数を制限し、Ｓ２２０４を実施する。

【０２１６】

（Ｓ２２３８）異常対策通知部１０９は、ドライバへ警告し、Ｓ２２０４を実施する。

【０２１７】

このように、異常対策通知部１０９は、ネットワーク解析における異常スコアが高いほど、ネットワークにおける制限が強くなるように、対策を決定する。なお、上記の第１～第４の閾値は、一例であり数値はこれに限定されない。

【０２１８】

なお、異常対策通知部１０９は、ネットワーク解析における異常スコア合計値に対応する処理に加え、当該異常スコア合計値以下に対応する処理を実行してもよい。異常対策通知部１０９は、例えば、ステップＳ２２３１でＹｅｓの場合、ステップＳ２２３２の処理に加え、ステップＳ２２３４、Ｓ２２３６およびＳ２２３８の少なくとも１つの処理を実

行してもよい。
【０２１９】
図２４は、本実施の形態における異常カテゴリ別の異常対策処理のフローチャートの他の一例である。図２４は、図２２に示すステップＳ２２０４の詳細を示すフローチャートの一例である。なお、図２４は、異常スコアのうち、システム解析における異常スコアを用いて行われる処理である。言い換えると、図２４に示す処理において、異常スコアのうち、ネットワーク解析における異常スコアは用いられない。なお、図２４に示す動作は、異常車両または異常エリアにおいて第二の攻撃段階であると判定された場合に実行されてもよい。
【０２２０】
（Ｓ２２４１）異常対策通知部１０９は、システム解析における異常カテゴリが３０（第５の閾値）以上であるか否かを判定する。異常対策通知部１０９は、異常カテゴリが３０以上である場合（Ｓ２２４１でＹｅｓ）、ステップＳ２２４２を実施する。
【０２２１】
（Ｓ２２４３）異常対策通知部１０９は、異常カテゴリが３０未満である場合（Ｓ２２４１でＮｏ）、異常カテゴリが２０以上（第５の閾値より小さい第６の閾値）であるか否かを判定する。異常対策通知部１０９は、３０未満２０以上である場合（Ｓ２２４３でＹｅｓ）、ステップＳ２２４４を実施する。
【０２２２】
（Ｓ２２４５）異常対策通知部１０９は、異常カテゴリが２０未満である場合（Ｓ２２４３でＮｏ）、異常カテゴリが１０以上（第６の閾値より小さい第７の閾値）であるか否かを判定する。異常対策通知部１０９は、２０未満１０以上の場合（Ｓ２２４５でＹｅｓ）、ステップＳ２２４６を実施する。
【０２２３】
（Ｓ２２４７）異常対策通知部１０９は、異常カテゴリが１０未満である場合（Ｓ２２４５でＮｏ）、異常カテゴリが１以上（第７の閾値より小さい第８の閾値）であるか否かを判定する。異常対策通知部１０９は、異常カテゴリが１以上の場合（Ｓ２２４７でＹｅｓ）、ステップＳ２２４８を実施し、異常カテゴリが０の場合（Ｓ２２４７でＮｏ）、対策を実施せずに処理を終了する。
【０２２４】
（Ｓ２２４２）異常対策通知部１０９は、車両制御機能を停止し、終了する。
【０２２５】
（Ｓ２２４４）異常対策通知部１０９は、異常車両検出サーバ１０へ送信する車両ログの送信頻度を増加させ、終了する。
【０２２６】
（Ｓ２２４６）異常対策通知部１０９は、異常車両検出サーバ１０へ送信する車両ログの種類数を増加させ、終了する。
【０２２７】
（Ｓ２２４８）異常対策通知部１０９は、ドライバへ警告し、終了する。
【０２２８】
このように、異常対策通知部１０９は、システム解析における異常スコアが高いほど、車両システム２０における制限が強くなるように、対策を決定する。なお、上記の第５～第８の閾値は、一例であり数値はこれに限定されない。
【０２２９】
なお、異常対策通知部１０９は、システム解析における異常スコア合計値に対応する処理に加え、当該異常スコア合計値以下に対応する処理を実行してもよい。異常対策通知部１０９は、例えば、ステップＳ２２４１でＹｅｓの場合、ステップＳ２２４２の処理に加え、ステップＳ２２４４、Ｓ２２４６およびＳ２２４８の少なくとも１つの処理を実行してもよい。
【０２３０】

図２３および図２４に示すように、異常対策通知部１０９は、異常車両と判定した車両と同一の車種の車両または異常車両と判定した車両が位置する異常エリアに位置する車両に対して、異常スコアの値（例えば、異常車両と判定された車両の異常スコアの値）または不審挙動の種別（例えば、ネットワーク解析またはシステム解析）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、および、ドライバへの通知のうち、いずれか１つ以上を要求してもよい。当該１つ以上の要求は、例えば、異常車両、異常車両と判定した車両と同一の車種の車両、および、異常エリアに位置する異常車両以外の車両に対して行われる。

【０２３１】

［２３　エリア別攻撃段階判定処理のフローチャート］

図２５は、本実施の形態における異常車両判定部１０８のエリア別攻撃段階判定処理のフローチャートを示す。具体的には、図２５は、攻撃者による攻撃の進行度を判定する処理の一例を示すフローチャートである。図２５に示す処理は、例えば、図２２に示す処理と並行して行われてもよい。

【０２３２】

（Ｓ２３０１）異常車両判定部１０８は、検出した異常車両の情報を取得し、異常車両が検出された位置情報を異常エリアとして取得し、ステップＳ２３０２を実施する。

【０２３３】

（Ｓ２３０２）異常車両判定部１０８は、ステップＳ２３０１にて取得した異常エリア内に、複数の異常車両が存在するか否かを判定する。異常車両判定部１０８は、異常エリア内にステップＳ２３０１で取得した異常車両以外の異常車両が複数存在する場合（Ｓ２３０２でＹｅｓ）、ステップＳ２３０３を実施し、ステップＳ２３０１で取得した異常車両以外の異常車両が存在しない場合（Ｓ２３０２でＮｏ）、ステップＳ２３０５を実施する。なお、異常車両判定部１０８は、異常エリア内にステップＳ２３０１で取得した異常車両以外の異常車両が所定数以上である場合、ステップＳ２３０２でＹｅｓと判定し、異常エリア内にステップＳ２３０１で取得した異常車両以外の異常車両が所定数未満である場合、ステップＳ２３０２でＮｏと判定してもよい。

【０２３４】

（Ｓ２３０３）異常車両判定部１０８は、ステップＳ２３０２でＹｅｓと判定した場合、異常車両が検出された異常エリアに対する攻撃がデリバリーフェーズ（第二の攻撃段階の一例）であると判定する。

【０２３５】

（Ｓ２３０４）異常車両判定部１０８は、デリバリーフェーズである場合、異常対策通知部１０９を介して異常エリアの車両に対して警告を行い、処理を終了する。異常車両判定部１０８は、異常エリアの車両に対して、デリバリーフェーズであることを示す情報をドライバ等に報知するための情報を送信する。異常車両判定部１０８は、例えば、異常エリアに位置する全ての車両に対して警告を行う。異常車両判定部１０８は、例えば、異常車両ではない１以上の車両のそれぞれに対しても警告を行うとも言える。報知するための情報は、さらに異常に対する対策を行うための情報を含んでいてもよい。報知するための情報は、例えば、図２３に示すステップＳ２２３２、Ｓ２２３４、Ｓ２２３６、Ｓ２２３８、および、図２４に示すステップＳ２２４２、Ｓ２２４４、Ｓ２２４６、Ｓ２２４８の少なくとも１つを実行するための情報を含んでいてもよい。

【０２３６】

（Ｓ２３０５）異常車両判定部１０８は、異常車両が検出された異常エリアに対する攻撃が偵察フェーズ（第一の攻撃段階の一例）であると判定して終了する。異常車両判定部１０８は、例えば、異常エリア内の異常車両以外の車両に対して、警告を行わない。なお、異常対策通知部１０９は、異常車両判定部１０８がステップＳ２３０５の判定を行うと、現在偵察フェーズであることを示す情報を車両に通知してもよい。

【０２３７】
このように、異常車両判定部１０８は、異常車両が検出されたエリアである異常エリアにおいて、所定の台数以下の異常車両が存在する場合、第一の攻撃段階であると判定し、所定の台数より多い異常車両が存在する場合、第一の攻撃段階よりリバースエンジニアリングにおける攻撃の進行度が進行した第二の攻撃段階であると判定する。そして、攻撃が第二の攻撃段階である場合、異常エリアの車両に対して、警告が行われる。
【０２３８】
［２４　エリア別攻撃段階判定処理のフローチャート］
図２６は、本実施の形態における異常車両判定部１０８の車種別攻撃段階判定処理のフローチャートを示す。具体的には、図２６は、攻撃者による攻撃の進行度を判定する処理の他の一例を示すフローチャートである。
【０２３９】
（Ｓ２４０１）異常車両判定部１０８は、検出した異常車両の情報を取得し、取得した情報に基づいて異常車両の車種を異常車種として取得し、ステップＳ２４０２を実施する。
【０２４０】
（Ｓ２４０２）異常車両判定部１０８は、ステップＳ２４０１にて取得した異常車種において、複数の異常車両が存在するか否かを判定する。異常車両判定部１０８は、異常車種にステップＳ２４０１で取得した異常車両以外の異常車両が複数存在する場合（Ｓ２４０２でＹｅｓ）、ステップＳ２４０３を実施し、ステップＳ２４０１で取得した異常車両以外の異常車両が存在しない場合（Ｓ２４０２でＮｏ）に、ステップＳ２４０５を実施する。なお、異常車両判定部１０８は、異常車種にステップＳ２４０１で取得した異常車両以外の異常車両が所定数以上存在する場合、ステップＳ２４０２でＹｅｓと判定し、異常車種にステップＳ２４０１で取得した異常車両以外の異常車両が所定数未満存在する場合、ステップＳ２４０２でＮｏと判定してもよい。
【０２４１】
（Ｓ２４０３）異常車両判定部１０８は、ステップＳ２４０２でＹｅｓと判定した場合、異常車両の車種に対する攻撃がデリバリーフェーズ（第二の攻撃段階の一例）であると判定する。
【０２４２】
（Ｓ２４０４）異常車両判定部１０８は、デリバリーフェーズである場合、異常対策通知部１０９を介して異常車種の車両に対して警告を行い、処理を終了する。異常車両判定部１０８は、異常車種の車両に対して、デリバリーフェーズであることを示す情報をドライバ等に報知するための情報を送信する。異常車両判定部１０８は、例えば、異常車種の車両の全てに対して警告を行う。異常車両判定部１０８は、例えば、異常車種において異常車両ではない１以上の車両のそれぞれに対して警告を行うとも言える。報知するための情報は、さらに異常に対する対策を行うための情報を含んでいてもよい。報知するための情報は、図２３に示すステップＳ２２３２、Ｓ２２３４、Ｓ２２３６、Ｓ２２３８、および、図２４に示すステップＳ２２４２、Ｓ２２４４、Ｓ２２４６、Ｓ２２４８の少なくとも１つを実行するための情報を含んでいてもよい。
【０２４３】
（Ｓ２４０５）異常車両判定部１０８は、異常車両の車種に対する攻撃は偵察フェーズ（第一の攻撃段階の一例）であると判定して終了する。異常車両判定部１０８は、例えば、異常車種における異常車両以外の車両に対して、警告を行わない。なお、異常対策通知部１０９は、異常車両判定部１０８がステップＳ２４０５の判定を行うと、現在偵察フェーズであることを示す情報を車両に通知してもよい。
【０２４４】
このように、異常車両判定部１０８は、異常車両が検出された車種（異常車種）において、所定の台数以下の異常車両が存在する場合、第一の攻撃段階であると判定し、所定の台数より多い異常車両が存在する場合、第一の攻撃段階よりリバースエンジニアリングにおける攻撃の進行度が進行した第二の攻撃段階であると判定する。そして、攻撃が第二の

攻撃段階である場合、異常車種の車両に対して、警告が行われる。

【０２４５】

なお、第一の攻撃段階が偵察フェーズであり、第二の攻撃段階がデリバリーフェーズである例について説明したが、第一の攻撃段階および第二の攻撃段階はこれに限定されない。図１２に示すサイバーキルチェーンを例に説明すると、第二の攻撃段階は、第一の攻撃段階とは異なる段階であって、第一の攻撃段階より攻撃の進行度が高い段階（フェーズ）であれば特に限定されない。

【０２４６】

［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。

【０２４７】

（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。

【０２４８】

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。

【０２４９】

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、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に適用してもよい。

【０２５０】

（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、回数および異常スコアの値は、変更してもよい。各値は、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特に限定されない。

【０２５１】

（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。

【０２５２】

（４）上記の実施の形態において、異常スコア算出部１０６は、車種および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。

【０２５３】

（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。

【０２５４】

（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。

【０２５５】

（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。

【０２５６】

（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。

【０２５７】
（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とに、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。
【０２５８】
（１０）上記の実施の形態において、エリア別攻撃段階判定処理のフローチャートおよび車種別攻撃段階判定処理のフローチャートでは、異常車両が１台のみであれば偵察フェーズと判定し、複数台であればデリバリーフェーズと判定したが、判定基準の異常車両の台数は、１ではなく所定値で判定してもよい。
【０２５９】
（１１）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。
【０２６０】
（１２）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。
【０２６１】
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、一部またはすべてを含むように１チップ化されてもよい。
【０２６２】
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、専用回路また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。
【０２６３】
さらには、半導体技術の進歩また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。
【０２６４】
（１３）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。
【０２６５】
（１４）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。

【０２６６】

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。

【０２６７】

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。

【０２６８】

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。

【０２６９】

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。

【０２７０】

（１５）また、上記実施の形態において説明された複数の処理の順序は一例である。複数の処理の順序は、変更されてもよいし、複数の処理は、並行して実行されてもよい。また、複数の処理の一部は、実行されなくてもよい。

【０２７１】

（１６）また、上記実施の形態における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、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、異常スコアが所定値以上の場合に、車両を異常車両として判定する異常車両判定部と、を備える構成であってもよい。

【０２７２】

（１７）上記実施の形態およ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】

【０２７３】

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を管理する情報処理装置に有用である。

【符号の説明】

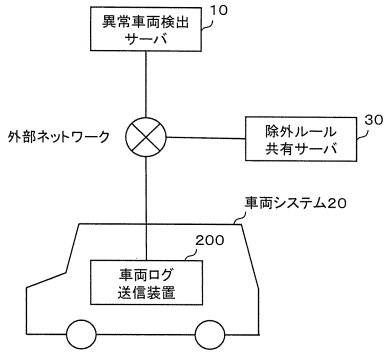
【０２７４】

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
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

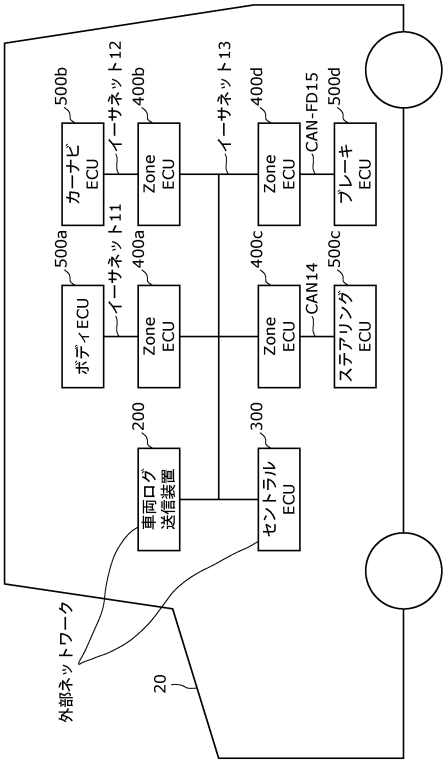
１０６　異常スコア算出部
１０７　異常スコア記憶部
１０８　異常車両判定部
１０９　異常対策通知部
１１０　異常表示部
２００　車両ログ送信装置
２１０　車両側通信部
２２０　車両ログ送信部
２３０　異常対策部
３００　セントラルＥＣＵ
４００ａ、４００ｂ、４００ｃ、４００ｄ　ＺｏｎｅＥＣＵ
５００ａ　ボディＥＣＵ
５００ｂ　カーナビＥＣＵ
５００ｃ　ステアリングＥＣＵ
５００ｄ　ブレーキＥＣＵ

【図面】

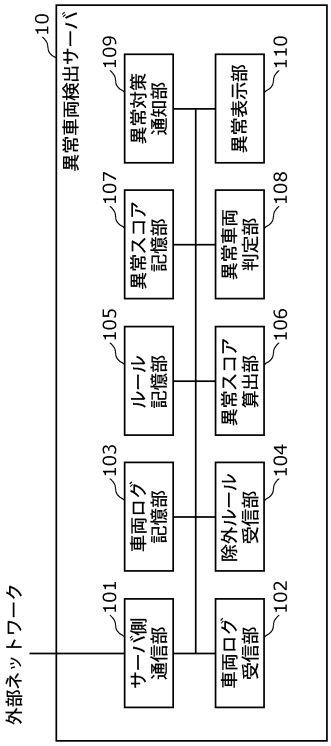
【図１】



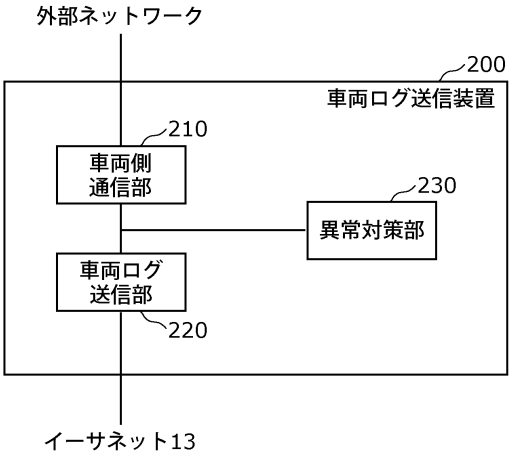
【図２】



【図３】



【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	0	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	0	…	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	—	—	—	—	—	—

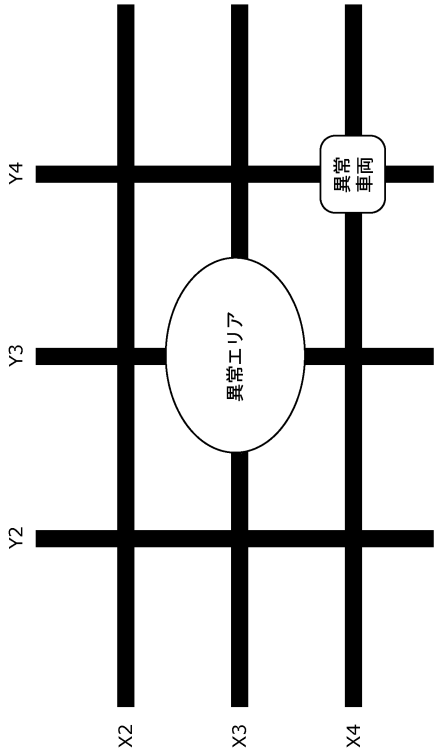
【図９】

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

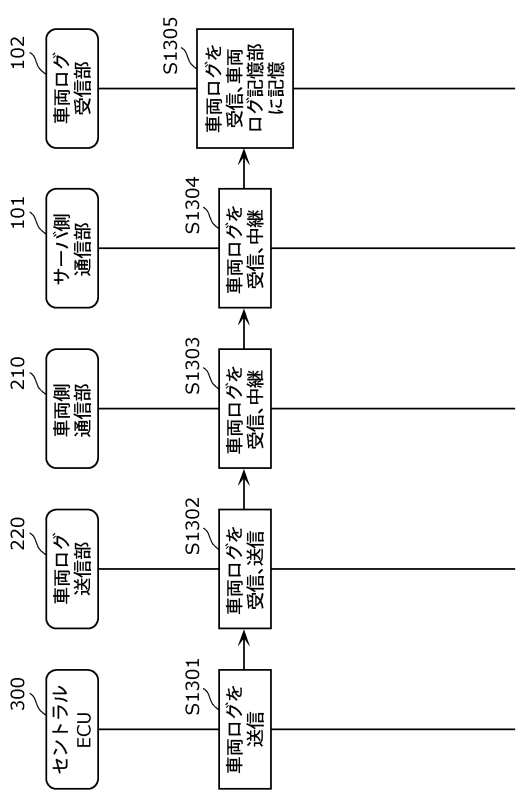
【図１１】



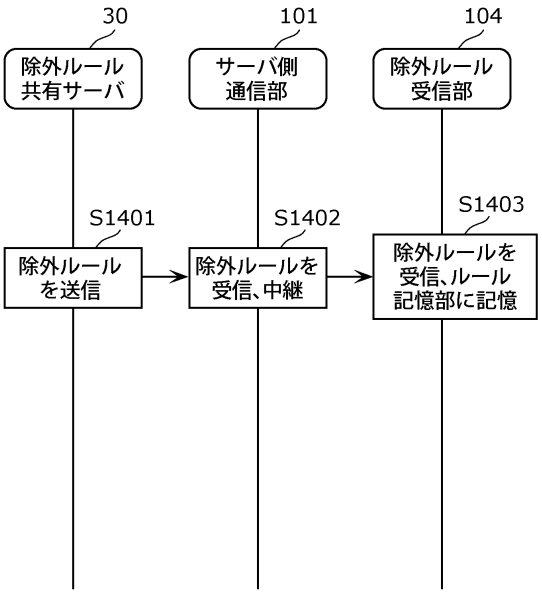
【図１２】

フェーズ	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
車両A1							

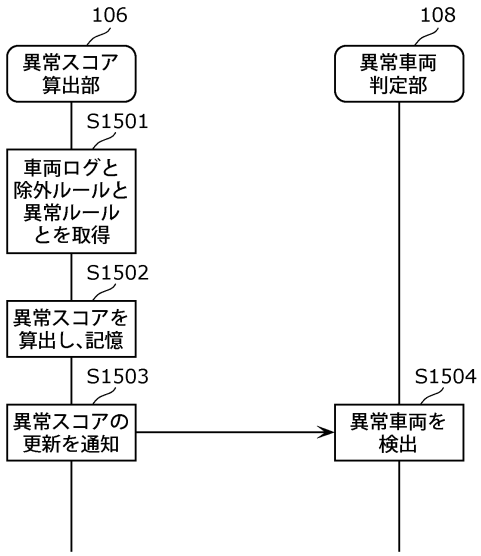
【図１３】



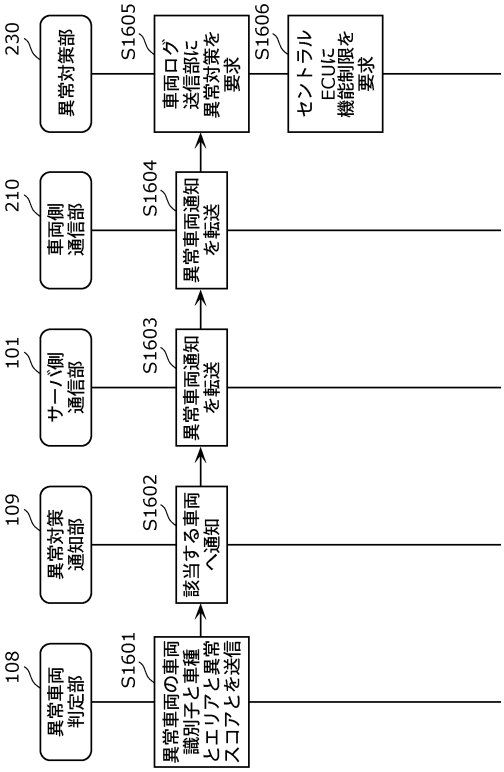
【図１４】



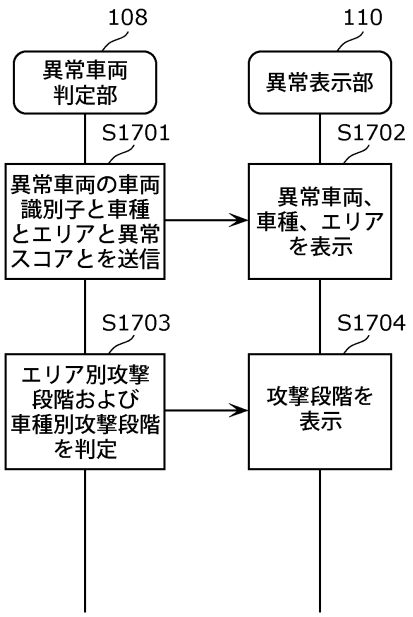
【図１５】



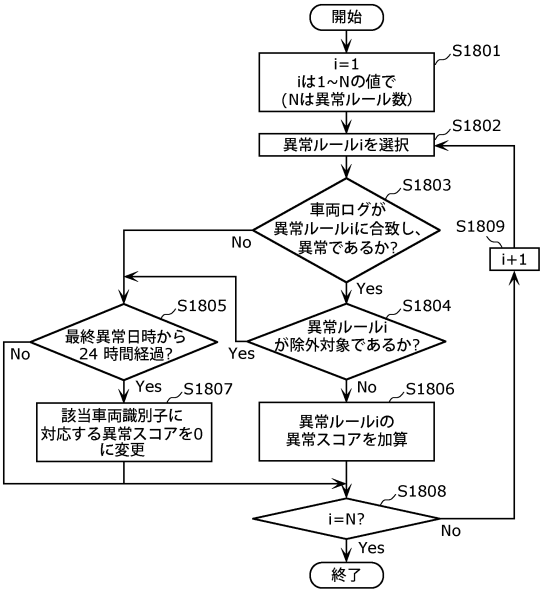
【図１６】



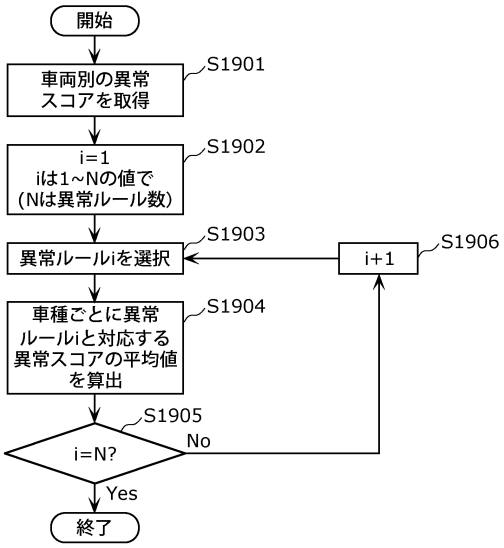
【図１７】



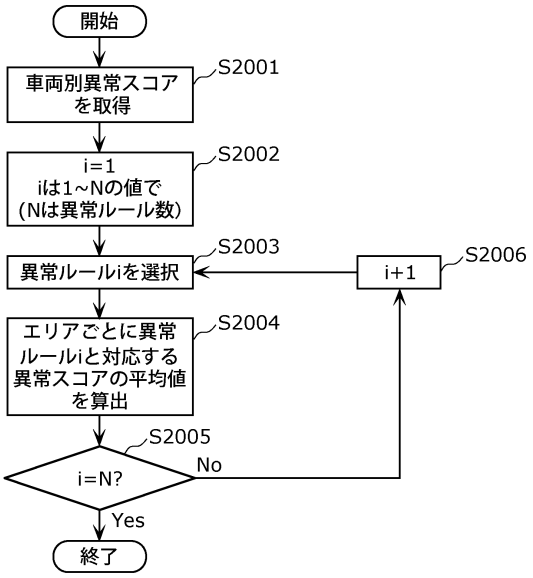
【図１８】



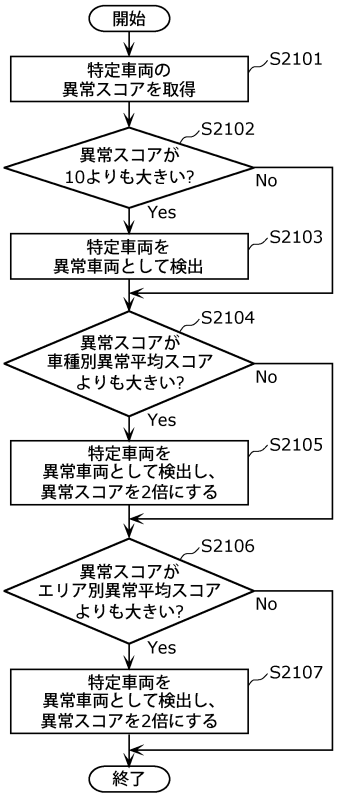
【図１９】



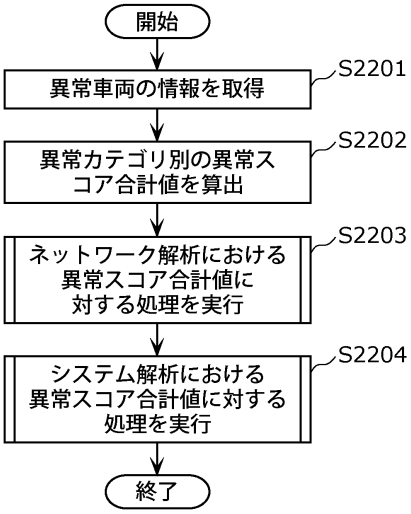
【図２０】



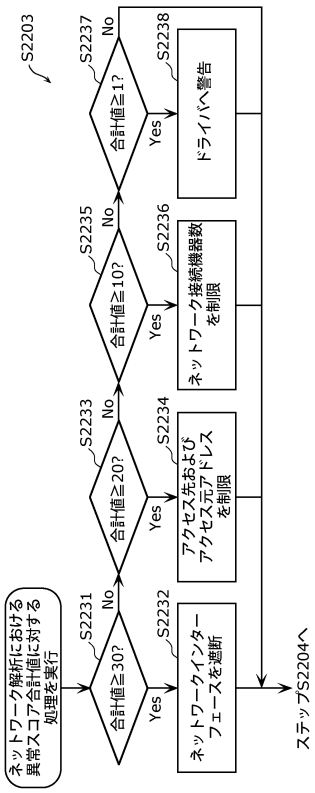
【図２１】



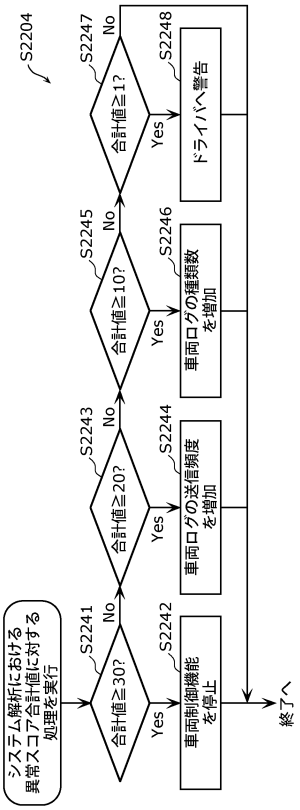
【図２２】



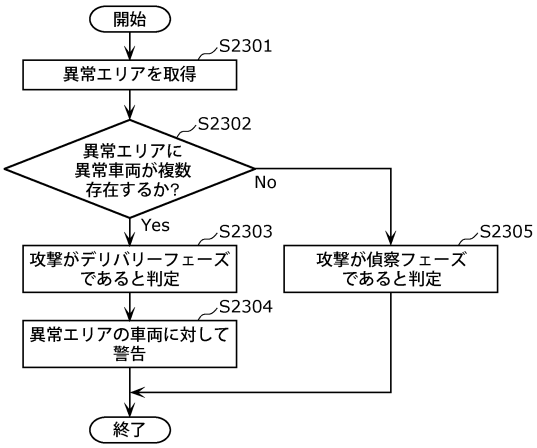
【図２３】



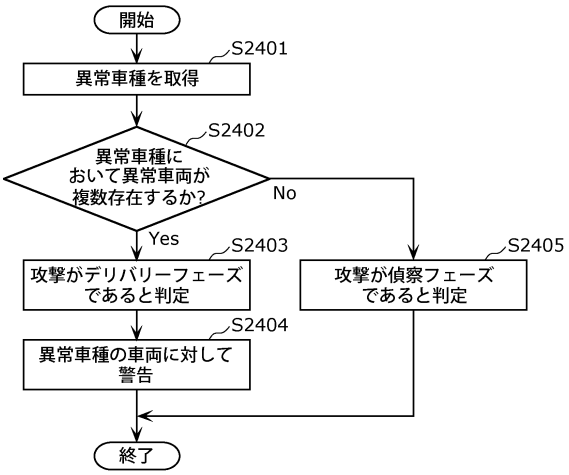
【図２４】



【図２５】



【図２６】



フロントページの続き

(72)発明者　平野 亮
日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　岸川 剛
日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　氏家 良浩
日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　芳賀 智之
日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内

審査官　辻 勇貴

(56)参考文献　特開２０１８－１９０４６５（ＪＰ，Ａ）
特開２０１９－１２９５２８（ＪＰ，Ａ）
特開２０１７－１１１７９６（ＪＰ，Ａ）
桑原 拓也 ほか7名，CANメッセージ頻度に注目した車載ネットワークの統計的異常検知，SCIS2016 暗号と情報セキュリティシンポジウム2016，電子情報通信学会，2016年，pp.1-7

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｂ６０Ｒ　１６／０２