(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7600166号
(P7600166)

(45)発行日　令和6年12月16日(2024.12.16)

(24)登録日　令和6年12月6日(2024.12.6)

(51)国際特許分類		FI		
Ｇ０６Ｆ　21/55　(2013.01)		Ｇ０６Ｆ	21/55	
Ｂ６０Ｒ　16/02　(2006.01)		Ｂ６０Ｒ	16/02	６５０Ｊ
Ｂ６０Ｒ　16/023 (2006.01)		Ｂ６０Ｒ	16/023	Ｐ
Ｇ０１Ｍ　17/007 (2006.01)		Ｇ０１Ｍ	17/007	Ｊ

請求項の数　4　（全13頁）

(21)出願番号　特願2022-37078(P2022-37078)
(22)出願日　令和4年3月10日(2022.3.10)
(65)公開番号　特開2023-132005(P2023-132005A)
(43)公開日　令和5年9月22日(2023.9.22)
審査請求日　令和6年2月29日(2024.2.29)

(73)特許権者　509186579
日立Ａｓｔｅｍｏ株式会社
茨城県ひたちなか市高場２５２０番地
(74)代理人　110002572
弁理士法人平木国際特許事務所
(72)発明者　井手口 恒太
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
(72)発明者　笹 晋也
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
(72)発明者　山口 隆
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
(72)発明者　藤井 康広
最終頁に続く

(54)【発明の名称】　車両診断システム

(57)【特許請求の範囲】
【請求項１】
車両内の機器に対して所定の処理の実施を要求する要求信号に対して該機器が該所定の処理を実施したか否かを示す第１ログの履歴を取得するログ取得部と、
前記履歴に、前記所定の処理が実施されなかったことを示す不実施ログが含まれていた場合に、該不実施ログに対応する前記要求信号の送信に利用された通信の正当性を判定する通信判定部と、を有する、
ことを特徴とする車両診断システム。
【請求項２】
請求項１に記載の車両診断システムであって、
前記履歴を時系列に沿って抽出してログ時系列データを生成するログ処理部と、
前記車両に実施された車両診断履歴を記憶する車両診断履歴記憶部と、をさらに有し、
前記通信判定部は、前記ログ時系列データと前記車両診断履歴とを照合し、前記不実施ログに対応する記録が前記車両診断履歴内に存在する場合に、該不実施ログに対応する通信を正当であると判定する、
ことを特徴とする車両診断システム。
【請求項３】
請求項２に記載の車両診断システムであって、
前記ログ処理部は、前記ログ時系列データから、前記通信判定部によって正当であると判定された前記通信に対応する前記第１ログを削除して修正ログ時系列データを生成し、

前記通信判定部は、前記修正ログ時系列データに前記不実施ログがさらに含まれていた場合に、該不実施ログに対応する前記通信を不正であると判定する、
ことを特徴とする車両診断システム。
【請求項４】
請求項３に記載の車両診断システムであって、
前記ログ取得部は、前記機器に異常が生じた際に生成される、該異常の種類を示す第２ログの履歴をさらに取得し、
前記通信判定部は、前記修正ログ時系列データに前記不実施ログがさらに含まれていた場合に、前記第２ログに基づいて、該不実施ログに対応する前記通信の正当性を再判定する、
ことを特徴とする車両診断システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両診断システムに関し、特に、車両の機器に異常またはその兆候が生じた場合に、該異常の原因を特定するための診断システムに関する。
【背景技術】
【０００２】
あらゆるモノがインターネットに繋がるＩｏＴ化が進む中、自動車業界においてもコネクテッドカーや自動運転車等ＩｏＴ化が進められている。しかし、こういった自動車のＩｏＴ化は、利便性をもたらす反面、インターネットを介したサイバー攻撃の危険性をも高めることになる。
【０００３】
車両に対するサイバー攻撃を検知する技術に関して、特許文献１～３が挙げられる。特許文献１には、車両等のハッキング被害を抑制する車両診断装置に関する技術が記載されている。特許文献２には、車両ログから攻撃者による不審な挙動を検知し異常車両を検出する技術が記載されている。特許文献３には、車両から外部サーバへ送信する車両ログの解析に関する技術が記載されている。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開第２０２１－０７９８５５号公報
【文献】国際公開第２０２１／０３８８７０号
【文献】再公表特許第２０２０／１１０４１４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
車両がサイバー攻撃を受けると、当然に車両の一部の機器に何等かの異常が生じる。しかし、近年のサイバー攻撃はその手口が巧妙になっていることもあり、異常が生じた車両の所有者は、当該異常が単に故障によるものだと判断する可能性が高い。このように判断した所有者は、整備工場に車両を持ち込んだり、カスタマーセンターに故障クレームとして報告したりすると考えられ、車両の提供者側はその対応をする必要がある。
【０００６】
しかしながら、車両に生じた異常がサイバー攻撃によるものだったにも関わらず単に故障によるものとして取り扱われた場合には、所有者はサイバー攻撃を受けたことを認識できず、攻撃者によるさらなる攻撃にさらされる危険性が高まる。また、後の検査段階等で異常がサイバー攻撃によるものであると判明した場合であっても、異常が生じた時点からすでに長時間経過していることも多いと考えられ、判明するまでの間に攻撃者によるさらなる攻撃をすでに受けていることもあり得る。したがって、車両に生じた異常がサイバー攻撃によるものかどうかを、迅速に判断することが要求される。

【０００７】
サイバー攻撃と単なる故障とを切り分けて判断するには、車両の提供者が例えばＰＳＩＲＴ（Ｐｒｏｄｕｃｔ Ｓｅｃｕｒｉｔｙ Ｉｎｃｉｄｅｎｔ Ｒｅｓｐｏｎｓｅ Ｔｅａｍ）を設置し、自社の製品およびサービスのセキュリティレベル向上を目的とした安全管理、セキュリティ面におけるユーザーサポート、そして製品／サービスに関連するインシデントが発生したときの対応に備える必要があるが、これは時間もコストも増加させてしまう。
【０００８】
特許文献１～３に記載の技術もハッキング等車両に生じた異常を診断する技術に関するが、これらによっても車両に生じた異常が攻撃によるものなのか単なる故障なのかを切り分けて判断することはできない。
【０００９】
本発明は、上記課題に鑑みてなされたものであり、多大な時間やコストをかけずとも、車両に生じた異常やその兆候が攻撃によるものなのか単なる故障なのかを容易に診断することを目的とする。
【課題を解決するための手段】
【００１０】
上記課題を解決するために、本発明に係る車両診断システムは、車両内の機器に対して所定の処理の実施を要求する要求信号に対して該機器が該所定の処理を実施したか否かを示す第１ログの履歴を取得するログ取得部と、履歴に、所定の処理が実施されなかったことを示す不実施ログが含まれていた場合に、該不実施ログに対応する要求信号の送信に利用された通信の正当性を判定する通信判定部と、を有する。
【発明の効果】
【００１１】
本発明によれば、従来のように多大な時間やコストをかけずとも、車両に生じた異常やその兆候が攻撃によるものなのか単なる故障なのかを容易に診断することが可能になる。
本発明に関連する更なる特徴は、本明細書の記述、添付図面から明らかになるものである。また、上記した以外の課題、構成及び効果は、以下の実施例の説明により明らかにされる。
【図面の簡単な説明】
【００１２】
【図１】自動車供給に係る各フェーズ中保守フェーズにおいて各部門／組織に求められる運用を示す全体概要図。
【図２】本発明に係る車両診断システムが適用される診断サーバ及び車両の構成を示すブロック図。
【図３】本発明において取り扱われる各データのデータ構造を説明するための図。
【図４】診断サーバ、車両及び攻撃者が実施する処理の関係性を示すシーケンス図。
【図５】車両内のＥＣＵに故障が発生した場合に想定される処理の一覧。
【図６】車両内のＥＣＵが攻撃された場合に想定される処理の一覧。
【図７】ログ取得部が行う処理を示すフローチャート。
【図８】実施例１において車両診断システムが行う処理を示すフローチャート。
【図９】実施例２において車両診断システムが行う処理を示すフローチャート。
【発明を実施するための形態】
【００１３】
以下、図面に沿って実施例を説明する。
図１は、自動車供給に係る各フェーズ中保守フェーズにおいて各部門／組織に求められる運用を示す全体概要図である。
【００１４】
自動車の供給者は、需要者に自動車を供給する際に通常図１に示すような設計～保守のフェーズの運用を行う。この中で、近年は特に保守フェーズにおける顧客対応の多様化が

求められている。
【００１５】
具体的には、顧客は、所有する車両に異常が生じた場合には上述したようにまずは故障が生じたと考え、カスタマーセンターに報告する。その後は、図示のようにカスタマーセンターから品質保証部門、開発部門、及びサプライヤに対して各種依頼／情報が伝達され、製品の改修及び調査結果の顧客への回答等が行われる。
【００１６】
また、上記処理と並行して、ディーラーや整備工場等の外部組織や、車両の出荷後における運用中のセキュリティを管理するＶＳＯＣ（Ｖｅｈｉｃｌｅ　Ｓｅｃｕｒｉｔｙ　Ｏｐｅｒａｔｉｏｎ　Ｃｅｎｔｅｒ）から脅威・脆弱性情報やインシデント情報（セキュリティイベントに関するログ等）が検出された場合には、上述したＰＳＩＲＴへと報告され、ＰＳＩＲＴからも品質保証部門、開発部門及びサプライヤへと情報が伝達される。
【００１７】
このように、前述のようにセキュリティ確保の観点からＰＳＩＲＴを設置した場合には、車両になんらかの異常もしくはその可能性が生じた場合に、最初に報告を受ける窓口が分散することにもなり、故障とサイバー攻撃との切り分け業務に関する工数が増加し、車両異常への対応の遅延につながっている。
【００１８】
本発明はこうした背景を基になされたものである。図２に、本発明に係る車両診断システムの適用対象に関する概要図を示す。
【００１９】
本発明に係る車両診断システムは、例えばクラウド上の診断サーバ１上に実装される。診断サーバ１は、ネットワーク２を介して車両３と接続されている。車両診断システムとしてはクラウド上に実装されるものに限られず、ＣＰＵ及びメモリを備えたハードウェアとして個々の車両内に搭載されるものを採用してもよい。
【００２０】
診断サーバ１は、通信部１１、リクエストメッセージ生成部１２、ログ取得部１３、ログ処理部１４、通信判定部１５、異常特定部１６、及び車両診断履歴記憶部１７を有する。車両３は、通信部３１と、複数のＥＣＵ３２を有する。ＥＣＵ３２は、自己診断が可能な各種制御系に関する機器である。
【００２１】
診断サーバ１の通信部１１は、車両３の各ＥＣＵ３２に対してリクエストメッセージを送信し、各ＥＣＵ３２からレスポンスメッセージを受信する。リクエストメッセージ生成部１２はこのリクエストメッセージを生成する。ログ取得部１３は、車両３から受信した情報をログとして記録する。
【００２２】
ここで、リクエストメッセージ及びレスポンスメッセージ、並びにログ取得部１３が取得するログの内容について図３を用いて説明する。まず、リクエストメッセージは、車両３の各ＥＣＵ３２に対して、自己診断等所定の処理の実施を要求するための指令信号であり、図３（ａ）に示すように、要求する処理の大枠を示す、１バイトの識別番号（ＳＩＤ）を含む。また、選択的に、要求する処理の詳細を示す、１バイトの識別番号（Ｓｕｂｆｕｎｃｔｉｏｎ）、要求する処理の対象を示す、１～２バイトのＩＤ番号（ＤａｔａＩＤ）、及び処理の実施に必要な、上記以外のデータ（Ｄａｔａ）を含む。
【００２３】
車両３内の各ＥＣＵ３２は、リクエストメッセージの受信に応じて処理の実施を試行し、その結果としてレスポンスメッセージを生成、診断サーバ１に送信する。レスポンスメッセージは、ＥＣＵ３２が要求された処理を実施できた場合には図３（ｂ）のポジティブレスポンスメッセージであり、ＥＣＵ３２が要求された処理を実施できなかった場合には図３（ｃ）のネガティブレスポンスメッセージである。
【００２４】

ポジティブレスポンスメッセージは、ＳＩＤと、要求された処理を実施した結果等を含む。具体的には、要求された処理詳細の値をそのまま復唱する［Ｓｕｂ ｆｕｎｃｔｉｏｎ］、要求されたデータＩＤの値をそのまま復唱する［Ｄａｔａ ＩＤ］、及び処理を実施した結果得られたデータを示す［Ｄａｔａ］を含む。

【００２５】

ネガティブレスポンスメッセージは、ネガティブレスポンスであることを示す識別番号（ＳＩＤ：０ｘ７Ｆで固定）と、実施できなかった処理のＳＩＤＲＱと、実施できなかった理由を示すコード番号であるネガティブレスポンスコード（ＮＲＣ）を含む。ＮＲＣは、ＩＳＯ １４２２９－１にて定義される１バイトのコードであり、タイムアウト等単に処理を実施できなかった場合を示すコードの他、認証の多数回失敗や証明書検証失敗など、セキュリティ関連のエラーコードも含まれる。

【００２６】

また、上記のリクエストメッセージ及びレスポンスメッセージは、ＵＤＳ（Ｕｎｉｆｉｅｄ Ｄｉａｇｎｏｓｔｉｃ Ｓｅｒｖｉｃｅｓ）通信を利用して送受信される。ＵＤＳとは、ＩＳＯ１４２２９に準拠する、実務に利用した経験を踏まえてＫＷＰを大幅に改良した、新しいダイアグ通信仕様の枠組みであり、仕様が整理され、標準化の範囲が大きく広げられた通信プロトコルである。近年においては特に車両診断の分野に用いられており、低位層であるＣＡＮ上にセッション層として実装される。

【００２７】

上述したレスポンスメッセージに関する情報を、ログ取得部１３は、車両３の各ＥＣＵが要求された処理を実施できたか否かを示す第１ログとして取得する。リクエストメッセージは、１台のＥＣＵ３２に対して複数回生成されることもあれば、複数のＥＣＵ３２に対して生成されることもあり、したがってログ取得部１３は、上記の情報を第１ログの履歴としてタイムスタンプとともに取得し、保存する。この履歴には、各ＥＣＵ３２へアクセスする際に利用されたＵＤＳ通信の内容に関する情報も含まれる。ログ取得部１３が行う処理については図７のフローチャートに示されている。ステップ７０１でＥＣＵ３２に対しリクエストメッセージを送信し、ステップ７０２でＥＣＵ３２からレスポンスメッセージを受信し、ステップ７０３でログ情報としてログ取得部１３内に記録している。

【００２８】

ログ取得部１３はまた、ＥＣＵ３２になんらかの異常が生じた場合に生成される、該異常の種類を示す診断故障コード(ＤＴＣ：Ｄｉａｇｎｏｓｉｓ Ｔｒｏｕｂｌｅ Ｃｏｄｅ）を第２ログとして取得し、保存することも可能である。ＤＴＣとは、車両の異常状態を表す３バイトのコードであり、ＩＳＯ １５０３１－６にて定義されている。ＤＴＣは、図３（ｄ）に示すようなデータ構造を有する。

【００２９】

ＤＴＣコードには標準化されたパラメータ領域とＯＥＭ定義のパラメータ領域があり、後者はＯＥＭが独自に利用可能である。ＤＴＣにおいては、１バイトのステータスフラグ（ＦＴＢ：Ｆａｉｌｕｒｅ Ｔｙｐｅ Ｂｙｔｅ）で該当ＤＴＣコードの状態（確定故障か未確定故障かなど）を表す。

【００３０】

また、ＤＴＣは、異常の原因究明のために、ＤＴＣ発生時のＥＣＵ制御データを記録するＤＴＣスナップショットデータや、故障発生頻度や最初の発生時のオドメータ値などを記録するＤＴＣ拡張データを含むこともある。

【００３１】

ログ取得部１３は、第１ログと同様に１台のＥＣＵ及び／又は複数のＥＣＵにおいて生成されたＤＴＣに関する情報を第２ログの履歴としてタイムスタンプとともに取得し、ログ取得部１３内に記憶する。

【００３２】

ログ取得部１３によって取得、記憶されたログは、ログ処理部１４によって処理される。ログ処理部１４は、上記のログのタイムスタンプを参照し、時系列に沿って抽出して並

べ替え、ログ時系列データを生成する。

【００３３】

通信判定部１５は、第１ログに、任意のＥＣＵ３２が、所定の処理を実施できなかったことを示す不実施ログが含まれていた場合、すなわちＮＲＣが含まれていた場合に、このＮＲＣが含まれるネガティブレスポンスメッセージに対応する処理の実施を要求した要求信号の送信に利用されたＵＤＳ通信の正当性を判定する。この判定方法については後述する。

【００３４】

異常特定部１６は、通信判定部１５によって不正な利用であると判定されたＵＤＳ通信が存在する場合に、その原因を特定する。

【００３５】

車両診断履歴記憶部１７は、各車両３が、過去に実施した車両診断の履歴を保存する。この履歴は、通信判定部１５によって、ＵＤＳ通信の正当性の判定のために用いられる。また、この履歴については、ディーラー、整備工場、サプライヤからリアルタイムで取得できる。

【００３６】

次に、本実施例に係る診断サーバ、車両内ＥＣＵ、及び攻撃者との間に発生しうるイベント（故障、攻撃）の一例について図４を用いて説明する。

【００３７】

前述のように、近年においては車両に対するサイバー攻撃が問題となっているが、攻撃者は車両に対するサイバー攻撃を仕掛ける際に上述したＵＤＳ通信を用いることが多い。これは、ＵＤＳ通信は各ＥＣＵの機能を診断するという性質上管理者権限を有するといえるものであり、攻撃者からするとこの通信を利用することで各ＥＣＵに直接攻撃を仕掛けることが可能になるからである。

【００３８】

図４において、まず、ステップ４０１でＥＣＵ３２に故障が生じると、ＤＴＣコードが発行され、そのＥＣＵに記録される（ステップ４０２）。このＤＴＣは自動で消去されることはなく、従って後にログとして取得することができる。

【００３９】

次に、攻撃者が何等かの理由でＵＤＳ通信を不正に利用し、ＥＣＵ３２にサイバー攻撃を仕掛けたとする（ステップ４０３）。この攻撃は必ずしも成功するとは限らない。それは、ＥＣＵ３２側が、ＵＤＳ通信によるアクセスを検知すると、チャレンジ＆レスポンス認証を行い、その結果ハッシュ値が一致せずに攻撃者のその後のアクセスを拒否する場合もあるからである。この場合には、上述したＮＲＣを生成し、ネガティブレスポンスメッセージとして攻撃者に送信する（ステップ４０４、４０５）。また、この生成されたＮＲＣ及び攻撃者によって不正に利用されたＵＤＳ通信に関する情報もＥＣＵ３２内に記録される。

【００４０】

その後、診断サーバ１から、正常なＵＤＳ通信の利用によってＥＣＵ３２にリクエストメッセージが送信されたとする（ステップ４０６）。さらに、このリクエストメッセージに対して、なんらかの理由でＥＣＵによる処理が実施されず、ＮＲＣが生成されたと想定する（ステップ４０７）。すると、このＮＲＣを含むネガティブレスポンスメッセージが診断サーバ１へと送信される（ステップ４０８）。診断サーバ１は、上述した一連の情報について、ログ情報として記録する（ステップ４０９）。

【００４１】

図４においては、生じ得るイベントとして、ＥＣＵ３２に故障が生じ、攻撃者による攻撃を受けたがその攻撃は失敗してＮＲＣが生成され、診断サーバ１からのリクエストメッセージに対してＮＲＣが生成される、という一連のフローを説明した。

【００４２】

上述したような、生じ得るイベントを網羅したものを図５及び図６に示す。図５は、Ｅ

ＣＵ３２に故障が生じた場合を示し、図６は攻撃者から攻撃を受けた場合を示している。

【００４３】

図５（ａ）については、図４中ステップ４０１、４０２に対応しており、図示は省略しているがその後リクエストメッセージに対してポジティブレスポンスメッセージが返信される例である。図５（ｂ）については、図４中ステップ４０１、４０２が連続して生じる場合である。これはたとえば、セントラルＥＣＵに故障が生じた場合に、ゾーンＥＣＵにも故障が波及するような場合である。

【００４４】

図５（ｃ）は、図４中ステップ４０１、４０２、４０６、４０７及び４０８のフローを経過した場合を示している。このように、ＥＣＵ３２に故障が生じた場合かつＮＲＣ応答が生じる場合には、利用されるＵＤＳ通信は正常なものであると想定される。

【００４５】

次に、攻撃者から攻撃を受けた場合について図６を用いて説明する。まず図６（ａ）は、攻撃者がＵＤＳ通信を用いずに（例えば物理的に）攻撃を仕掛けた場合である。この場合にはＵＤＳの利用については何ら記録されず、ＥＣＵに異常が生じた場合にはＤＴＣが発行されて記録される。

【００４６】

図６（ｂ）は、図４中のステップ４０３、４０４、及び４０５に対応する場合である。図６（ｃ）は、その後にＥＣＵに異常が生じ、ＥＣＵにＤＴＣが記録された場合である。これは例えば、攻撃者による攻撃が長時間続き、当初はアクセスが拒否されてＮＲＣが生成される状態だったがなんらかの理由で攻撃が成功した場合が考えられる。

【００４７】

図６（ｄ）は、攻撃者による攻撃が成功し、ＥＣＵに異常が生じてＤＴＣが記録された後、その後不正なＵＤＳ利用と判定されてＮＲＣが発行された場合である。例えば、攻撃者がまず車両内のカーナビゲーションシステムに攻撃を与え、これが成功した場合にはカーナビゲーションシステムにおいてはＤＴＣが記録される。その後、攻撃者は今度はカーナビゲーションシステムを介してセントラルゲートウェイに攻撃を与えたが、これは失敗した、というような場合である。図６（ｅ）及び（ｆ）については、上述したパターンが組み合わされた場合を示す。

【００４８】

図６から理解される通り、攻撃者による攻撃が生じた場合にＮＲＣ応答が生じるのは、不正なＵＤＳ通信の利用がされた場合である。したがって、このことを利用することによって、ＥＣＵに異常が生じた場合に、異常の原因が故障によるものなのか、攻撃によるものなのか切り分けることが可能になる。なお、ＮＲＣ応答がない場合（図５（ａ）、（ｂ）及び図６（ａ）並びに図６（ｅ）及び（ｆ）の一部）については、従来通りの方法で故障及び攻撃の切り分けを行う。

【００４９】

上記の、ＮＲＣ応答があった場合に故障及び攻撃を切り分ける方法について図８のフローチャートを用いて説明する。まず、ステップ８０１において、ログ処理部１４は、ログ取得部１３が取得したログ情報について、時系列に沿って並べ替え、ログ時系列データを生成する。ステップ８０２において、ログ処理部１４は、ログ時系列データから、正常なＵＤＳ通信に基づくＮＲＣログを削除する。正常なＵＤＳ通信は、診断サーバ１の車両診断履歴記憶部１７に保存されている車両診断の履歴を参照することで判定できる。つまり、車両診断の履歴には、その時点までに、ディーラー、整備工場、及びサプライヤ等、正当な権限を有する者によって実施された診断情報が記録されているため、例えばＮＲＣが生成された時のタイムスタンプと、診断情報に含まれるタイムスタンプとを照合することによって、そのＵＤＳ通信が正当な利用であるかどうかを判定することができる。これを図４にあてはめると、診断サーバ１からの正常ＵＤＳ通信の利用によって送信されたリクエストメッセージに対して、ステップ４０７で生成されたＮＲＣは削除されることになる。このようにしてログ処理部１４は修正ログ時系列データを生成する。

【００５０】
修正ログ時系列データは通信判定部１５へと送られる。ステップ８０３において通信判定部１５は、修正ログ時系列データに、なおＮＲＣログが存在しているか判定する（ステップ８０３）。ＮＲＣログが最早存在しない場合には処理を終了する。ＮＲＣログが存在する場合には、異常特定部１６は、ステップ８０４に移行してＮＲＣの生成源（攻撃源）を特定する。これは、図４に当てはめると、修正ログ時系列データには、ステップ４０３の、攻撃者によるＵＤＳ通信を不正に利用したサイバー攻撃に応答してステップ４０４で生成されたＮＲＣログが存在していることになり、従って通信判定部１５は、このステップ４０３におけるＵＤＳ通信を不正な利用であると判定することが可能になる。そして、異常特定部１６はステップ８０５において、このＵＤＳ通信の不正利用に関する異常情報を記録する。

【００５１】
このように、本実施例においては、車両内のＥＣＵがＮＲＣを生成した場合に、該ＮＲＣに対応するＵＤＳ通信の利用の正当性を判定することのみによって故障及び攻撃の切り分けを行っている。したがって、従来のように、各部門に実際に異常が生じた製品を送り込んで分析したりＰＳＩＲＴによる調査を行ったりせずとも、容易かつ迅速に異常の原因を特定することが可能になる。

【００５２】
上記の例は、ＮＲＣに関する第１ログのみ用いていたが、ＤＴＣに関する第２ログを用いると図９に示す処理フローとなる。図９に示す処理は、図８に示す処理に加えて、ステップ９０１から９０４に示す処理を実施する。

【００５３】
ステップ８０３にて修正ログ時系列データにＮＲＣログが存在すると判定された場合に、ログ取得部１３は、上述したＤＴＣに関する第２ログを取得する（ステップ９０１）。そして、当該ログを通信判定部１５へと送信し、ＵＤＳ通信の誤検知があったか否かを判定する（ステップ９０２）。例えば、ＤＴＣが発行される１つの原因として、ＥＣＵに実装されている診断プログラム（ＵＤＳ通信を利用するプログラム）が、ＥＣＵ故障の影響で起動してしまい、ＵＤＳ通信が実施される、というものがある。このＵＤＳ通信の利用は、攻撃者によるＵＤＳ通信の不正利用ではないものの、車両診断履歴に記録されておらず、ゆえに不正なＵＤＳ通信の利用とみなされてしまう可能性がある。

【００５４】
従って、ＤＴＣの示す内容を検証し、不正なＵＤＳ通信の利用であると判定されていたが、攻撃者による不正な利用ではないと判定されたＵＤＳ通信に対応するＮＲＣについては、これを削除する（ステップ９０３）。その後はステップ９０４において再びＮＲＣログが存在するか否かを判定し、存在する場合にはステップ８０４へと移行しＮＲＣの発信源（攻撃源）を特定する。ステップ９０２で通信の誤検知がないと判定された場合も同様である。

【００５５】
このように、ＮＲＣに関する第１ログに加えて、ＤＴＣに関する第２ログをも考慮することによって、より精度良く故障及び攻撃の切り分けを行うことが可能になる。

【００５６】
なお、本実施例においてはＮＲＣを第１ログとして取得する例を説明したが、ＥＣＵが処理を正常に実施したことを示すＰＲＣ（Ｐｏｓｉｔｉｖｅ　Ｒｅｓｐｏｎｓｅ　Ｃｏｄｅ）を第１ログとして取得することもできる。ただし、ＰＲＣはＮＲＣよりも発行される頻度が高く、それゆえに通常は揮発的に記憶されること、発行の頻度が高いゆえに誤検知の可能性が高まることに留意する必要がある。

【００５７】
以上で説明した本発明の実施例によれば、以下の作用効果を奏する。
（１）本発明に係る車両診断システムは、車両内の機器に対して所定の処理の実施を要求する要求信号に対して該機器が該所定の処理を実施したか否かを示す第１ログの履歴を取

得するログ取得部と、履歴に、所定の処理が実施されなかったことを示す不実施ログが含まれていた場合に、該不実施ログに対応する要求信号の送信に利用された通信の正当性を判定する通信判定部と、を有する。

【００５８】

上記構成により、多大な時間やコストをかけずとも、車両に生じた異常が攻撃によるものなのか単なる故障なのかを容易に診断することが可能になる。

【００５９】

（２）履歴を時系列に沿って抽出してログ時系列データを生成するログ処理部と、車両に実施された車両診断履歴を記憶する車両診断履歴記憶部と、をさらに有し、通信判定部は、ログ時系列データと車両診断履歴とを照合し、不実施ログに対応する記録が車両診断履歴内に存在する場合に、該不実施ログに対応する通信を正当であると判定する。車両の診断履歴は容易に収集することが可能であるため、複雑な処理を要さずにＵＤＳ通信の正当性を判定できる。

【００６０】

（３）ログ処理部は、ログ時系列データから、通信判定部によって正当であると判定された通信に対応する第１ログを削除して修正ログ時系列データを生成し、通信判定部は、修正ログ時系列データに不実施ログがさらに含まれていた場合に、該不実施ログに対応する通信を不正であると判定する。通信判定部によって正当であると判定された通信に対応する第１ログのみ削除するため、不正な通信に基づく第１ログを削除することなく、当初のログ時系列データよりもデータ容量を抑えつつ、扱いやすく、かつ信頼性の高い修正ログ時系列データを生成し、管理することが可能になる。

【００６１】

（４）ログ取得部は、機器に異常が生じた際に生成される、該異常の種類を示す第２ログの履歴をさらに取得し、通信判定部は、修正ログ時系列データに不実施ログがさらに含まれていた場合に、第２ログに基づいて、該不実施ログに対応する通信の正当性を再判定する。このように、ＮＲＣに関する第１ログに加えてＤＴＣに関する第２ログをも考慮することで、より精度良くＵＤＳ通信の正当性を判定できる。

【００６２】

なお、本発明は、上記の実施例に限定されるものではなく、様々な変形が可能である。例えば、上記の実施例は、本発明を分かりやすく説明するために詳細に説明したものであり、本発明は、必ずしも説明した全ての構成を備える態様に限定されるものではない。また、ある実施例の構成の一部を他の実施例の構成に置き換えることが可能である。また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、削除したり、他の構成を追加・置換したりすることが可能である。

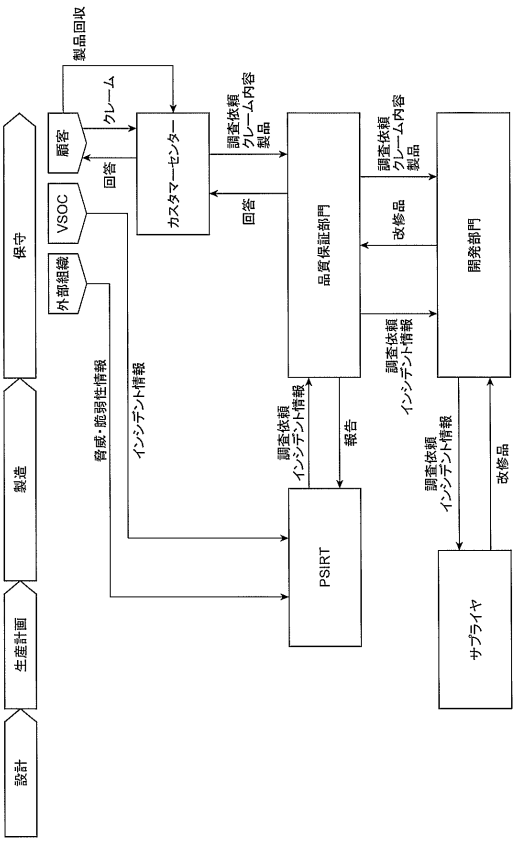
【符号の説明】

【００６３】

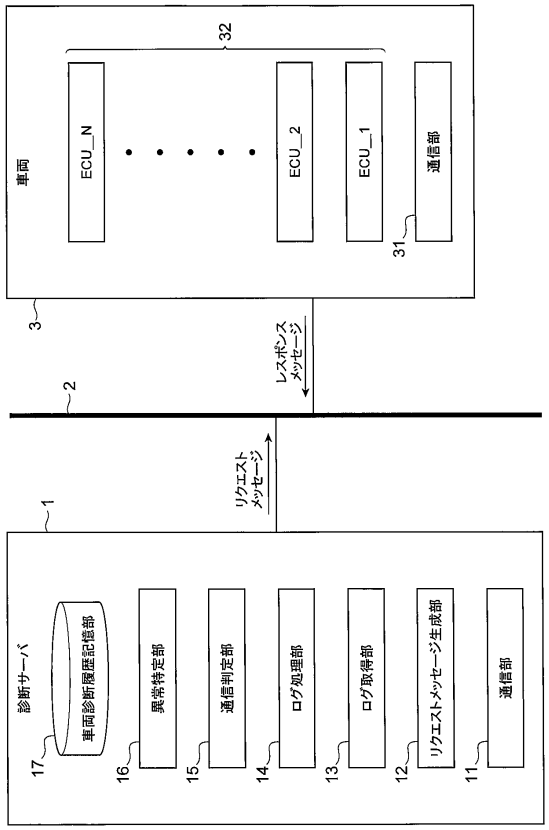
１　診断サーバ（車両診断システム）、３　車両、１３　ログ取得部、１４　ログ処理部、１５　通信判定部、１７　車両診断履歴記憶部

【図面】

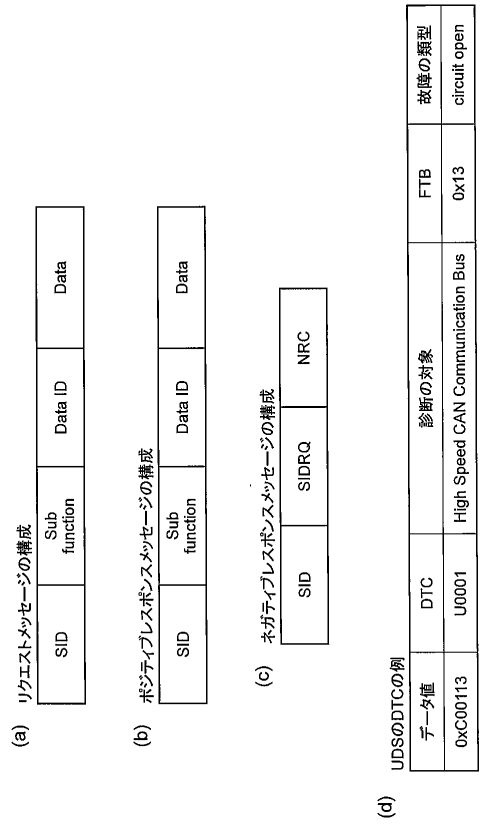
【図１】


製品回収
クレーム
顧客
回答
VSOC
外部組織
カスタマーセンター
調査依頼
クレーム内容
製品
回答
品質保証部門
改修品
調査依頼
クレーム内容
製品
開発部門
保守
製造
生産計画
設計
脅威・脆弱性情報
インシデント情報
調査依頼
インシデント情報
報告
調査依頼
インシデント情報
改修品
PSIRT
サプライヤ

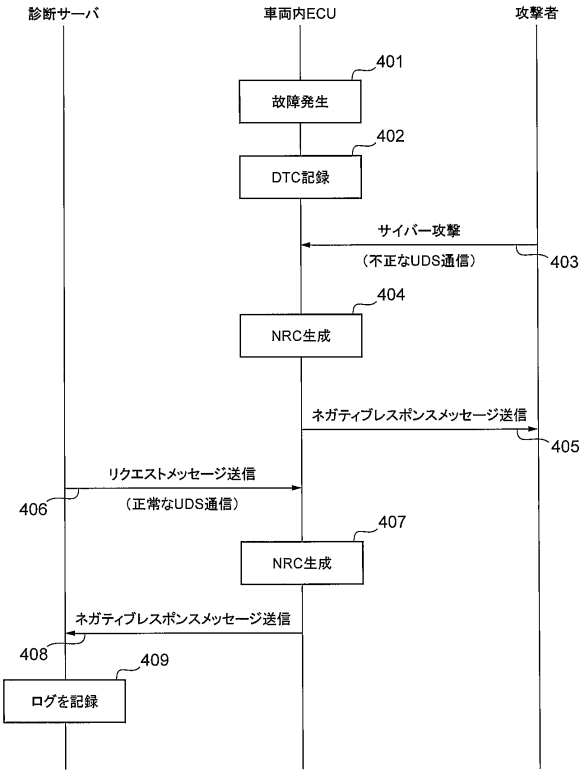
【図２】


車両
ECU_N
ECU_2
ECU_1
通信部
32
31
3
レスポンス
メッセージ
2
リクエスト
メッセージ
1
診断サーバ
車両診断履歴記憶部
異常特定部
通信判定部
ログ処理部
ログ取得部
リクエストメッセージ生成部
通信部
17
16
15
14
13
12
11

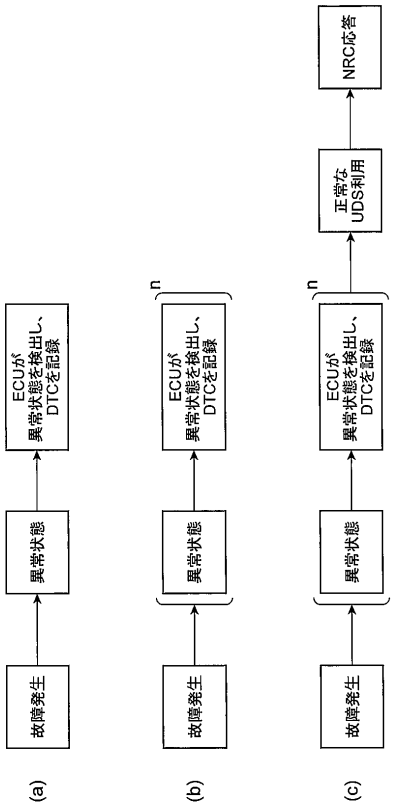
【図３】


(a) リクエストメッセージの構成
SID
Sub function
Data ID
Data
(b) ポジティブレスポンスメッセージの構成
SID
Sub function
Data ID
Data
(c) ネガティブレスポンスメッセージの構成
SID
SIDRQ
NRC
UDSのDTCの例
データ値
0xC00113
DTC
U0001
診断の対象
High Speed CAN Communication Bus
FTB
0x13
故障の類型
circuit open
(d)

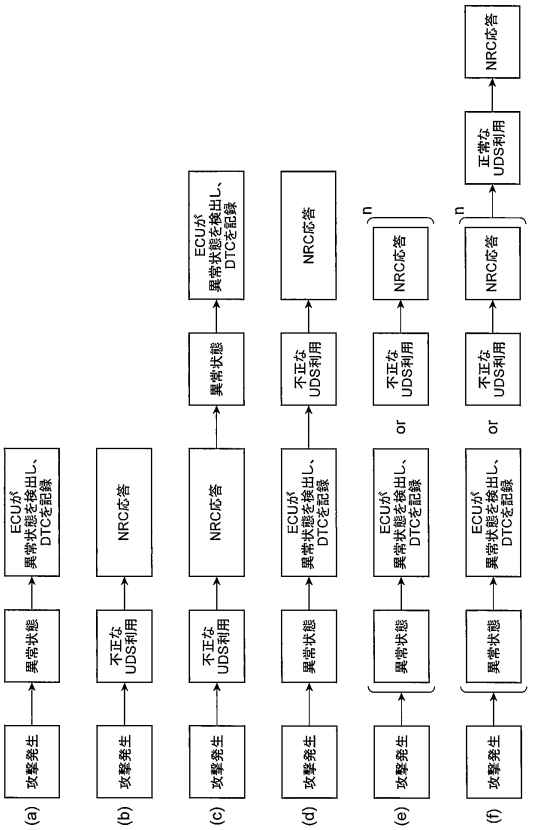
【図４】


診断サーバ
車両内ECU
攻撃者
401
故障発生
402
DTC記録
サイバー攻撃
（不正なUDS通信）
403
404
NRC生成
ネガティブレスポンスメッセージ送信
405
リクエストメッセージ送信
（正常なUDS通信）
406
407
NRC生成
ネガティブレスポンスメッセージ送信
408
409
ログを記録

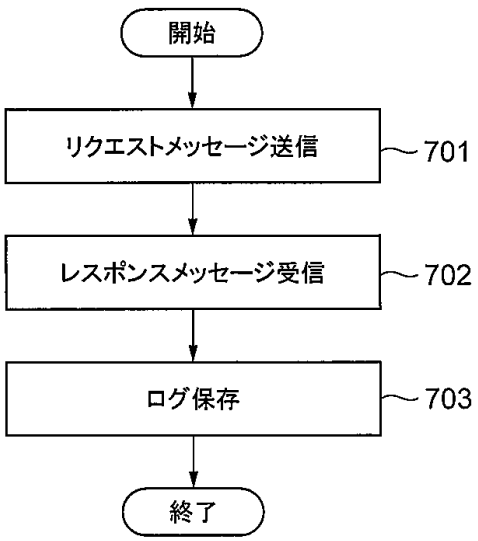
【図５】


故障発生
異常状態
ECUが異常状態を検出し、DTCを記録
n
正常なUDS利用
NRC応答
(a)
(b)
(c)

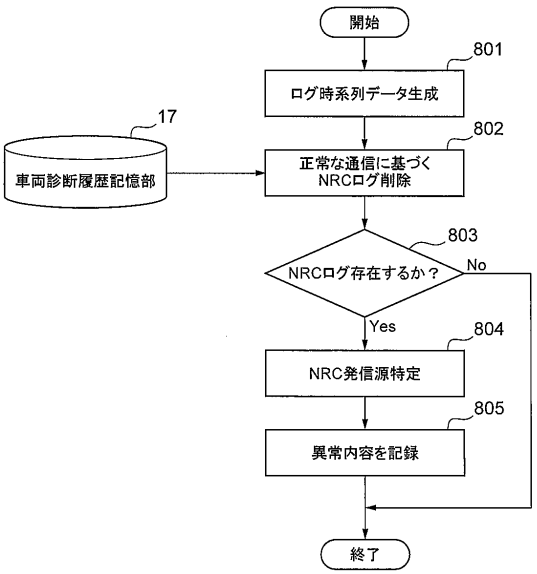
【図６】


攻撃発生
異常状態
不正なUDS利用
NRC応答
ECUが異常状態を検出し、DTCを記録
n
or
(a)
(b)
(c)
(d)
(e)
(f)

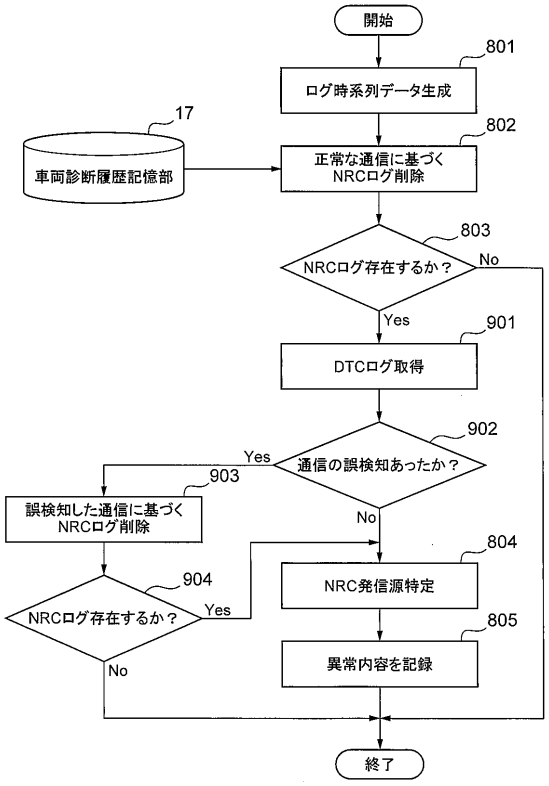
【図７】


開始
リクエストメッセージ送信
701
レスポンスメッセージ受信
702
ログ保存
703
終了

【図８】


開始
801
ログ時系列データ生成
17
車両診断履歴記憶部
802
正常な通信に基づくNRCログ削除
803
NRCログ存在するか？
No
Yes
804
NRC発信源特定
805
異常内容を記録
終了

【図９】


開始
801
ログ時系列データ生成
17
車両診断履歴記憶部
802
正常な通信に基づく
NRCログ削除
803
NRCログ存在するか？
No
Yes
901
DTCログ取得
902
通信の誤検知あったか？
Yes
903
誤検知した通信に基づく
NRCログ削除
No
804
NRC発信源特定
904
NRCログ存在するか？
Yes
805
異常内容を記録
No
終了

フロントページの続き

東京都千代田区丸の内一丁目６番６号 株式会社日立製作所内
(72)発明者 森田 伸義
東京都千代田区丸の内一丁目６番６号 株式会社日立製作所内
審査官 中里 裕正
(56)参考文献 特開２０２０－１７０６５（ＪＰ，Ａ）
特開２０２０－６１７１７（ＪＰ，Ａ）
特開２０２１－１１７５６８（ＪＰ，Ａ）
特開２０２２－１７８７３（ＪＰ，Ａ）
米国特許出願公開第２０１８／０３００４７７（ＵＳ，Ａ１）
国際公開第２０２０／０７５８０１（WO，Ａ１）
国際公開第２０２１／１３１１９３（WO，Ａ１）
MANSOR, H. et al.，Log your car: The non-invasive vehicle forensics，IEEE TrustCom/BigDataSE/ISPA 2016，2016年08月，pp.974-982
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５５
Ｂ６０Ｒ １６／０２
Ｂ６０Ｒ １６／０２３
Ｇ０１Ｍ １７／００７
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ