(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7631007号
(P7631007)

(45)発行日　令和7年2月18日(2025.2.18)

(24)登録日　令和7年2月7日(2025.2.7)

(51)国際特許分類		FI	
Ｇ０６Ｆ　21/55　(2013.01)		Ｇ０６Ｆ	21/55
Ｂ６０Ｗ　50/023(2012.01)		Ｂ６０Ｗ	50/023
Ｂ６０Ｗ　50/04　(2006.01)		Ｂ６０Ｗ	50/04

請求項の数　8　（全24頁）

(21)出願番号　特願2021-9152(P2021-9152)
(22)出願日　令和3年1月22日(2021.1.22)
(65)公開番号　特開2022-113050(P2022-113050A)
(43)公開日　令和4年8月3日(2022.8.3)
審査請求日　令和5年6月6日(2023.6.6)

(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　110002365
弁理士法人サンネクスト国際特許事務所
(72)発明者　粕谷 桃伽
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▲崎▼ 裕紀
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　片岡 幹雄
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
最終頁に続く

(54)【発明の名称】　電子制御装置、車載制御システム、及び冗長機能制御方法

(57)【特許請求の範囲】

【請求項１】

自動車の走行制御を行う車載制御システムに搭載され、第１の制御装置及び第２の制御装置を含む複数の制御装置と通信可能に接続される電子制御装置であって、

前記複数の制御装置の各制御装置におけるセキュリティ攻撃の有無を判定する攻撃判定部と、

前記攻撃判定部による判定結果に基づいて、前記第１の制御装置が担っていた機能と同様またはその一部の機能による冗長機能を、前記第２の制御装置に代替して実行させるか否かを判定する冗長系実行判定部と、

前記各制御装置の動作を監視し、前記各制御装置による前記機能の代替が必要な状況になっていないかを判断する機能監視部と、を備え、

前記機能監視部が前記第１の制御装置による前記機能の代替が必要な状況になっていると判断したとき、

前記冗長系実行判定部は、

前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が無いと判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させ、

前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が有ると判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させずに、前記第１の制御装置に対する所定のセキュリティ処理を実施させる

ことを特徴とする電子制御装置。

【請求項２】
前記各制御装置においてセキュリティ攻撃が生じた可能性を示す侵害推定度を算出する侵害推定度算出部をさらに備え、
前記攻撃判定部は、前記侵害推定度算出部によって算出された侵害推定度に基づいて、前記各制御装置におけるセキュリティ攻撃の有無を判定する
ことを特徴とする請求項１に記載の電子制御装置。
【請求項３】
前記第１の制御装置で検知されたセキュリティ異常を示す異常検知情報を受信するデータ通信部をさらに備え、
前記侵害推定度算出部は、前記データ通信部が受信した前記異常検知情報に基づいて、前記第１の制御装置における前記侵害推定度を算出する
ことを特徴とする請求項２に記載の電子制御装置。
【請求項４】
前記車載制御システム内で想定されるセキュリティ攻撃の攻撃経路を示す攻撃経路情報をさらに有し、
前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が有ると判定されたとき、
前記冗長系実行判定部は、
前記攻撃経路情報に基づいて、前記セキュリティ攻撃による影響を受ける可能性がある前記攻撃経路を特定し、前記特定した攻撃経路上に前記第２の制御装置が存在するか否かを判定し、
前記攻撃経路上に前記第２の制御装置が存在しない場合には、当該第２の制御装置に前記冗長機能を代替して実行させる一方、前記攻撃経路上に前記第２の制御装置が存在する場合には、当該第２の制御装置に前記冗長機能を代替して実行させない
ことを特徴とする請求項１に記載の電子制御装置。
【請求項５】
前記第１の制御装置による前記機能ごとに、対応する前記冗長機能を代替して実行し得る前記第２の制御装置の候補が予め定義され、
前記冗長系実行判定部が、前記第１の制御装置による前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させると判定した場合に、前記定義された候補の何れに前記冗長機能を代替して実行させるか、を管理する再配置管理部をさらに備える
ことを特徴とする請求項１に記載の電子制御装置。
【請求項６】
前記冗長機能を代替して実行する前記第２の制御装置には、自電子制御装置を含めることができる
ことを特徴とする請求項１に記載の電子制御装置。
【請求項７】
自動車の走行制御を行う車載制御システムであって、
所定の機能を有する第１の制御装置と、前記機能と同様またはその一部の機能による冗長機能を有する第２の制御装置と、を含む複数の制御装置と、
前記複数の制御装置と通信可能に接続される電子制御装置と、
を備え、
前記電子制御装置が、
前記複数の制御装置の各制御装置におけるセキュリティ攻撃の有無を判定する攻撃判定部と、
前記攻撃判定部による判定結果に基づいて、前記第１の制御装置が担っていた前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させるか否かを判定する冗長系実行判定部と、
前記各制御装置の動作を監視し、前記各制御装置による前記機能の代替が必要な状況になっていないかを判断する機能監視部と、を有し、

前記機能監視部が前記第１の制御装置による前記機能の代替が必要な状況になっていると判断したとき、
前記冗長系実行判定部は、
前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が無いと判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させ、
前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が有ると判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させずに、前記第１の制御装置に対する所定のセキュリティ処理を実施させる
ことを特徴とする車載制御システム。

【請求項８】

自動車の走行制御を行う車載制御システムに搭載され、第１の制御装置及び第２の制御装置を含む複数の制御装置と通信可能に接続される電子制御装置による冗長機能制御方法であって、
前記複数の制御装置の各制御装置におけるセキュリティ攻撃の有無を判定する攻撃判定ステップと、
前記攻撃判定ステップの判定結果に基づいて、前記第１の制御装置が担っていた機能と同様またはその一部の機能による冗長機能を、前記第２の制御装置に代替して実行させるか否かを判定する冗長系実行判定ステップと、
前記各制御装置の動作を監視し、前記各制御装置による前記機能の代替が必要な状況になっていないかを判断する機能監視ステップと、を備え、
前記機能監視ステップにおいて前記第１の制御装置による前記機能の代替が必要な状況になっていると判断したとき、
前記冗長系実行判定ステップでは、
前記攻撃判定ステップによって前記第１の制御装置においてセキュリティ攻撃が無いと判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させ、
前記攻撃判定ステップによって前記第１の制御装置においてセキュリティ攻撃が有ると判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させずに、前記第１の制御装置に対する所定のセキュリティ処理を実施させる
ことを特徴とする冗長機能制御方法。

【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、電子制御装置、車載制御システム、及び冗長機能制御方法に関し、自動車の車載制御システムに搭載される電子制御装置、車載制御システム、及び冗長機能制御方法に適用して好適なものである。

【背景技術】
【０００２】

従来、車載システムでは、システムの失陥時でも運転手の安全性を保障するために、何らかの失陥が発生した場合に備えて、運転を継続できるような冗長機能をシステム内に配置している。

【０００３】

上記のような車載システムの失陥に対応する技術として、例えば特許文献１には、故障によって電子制御装置の機能が正常に動作しなくなった場合でも自動車の走行を継続するために、正常時の機能（正常系）に加えて、正常時と同様の機能を冗長機能（冗長系）として備え、故障時には冗長機能を稼働させる方法が開示されている。

【先行技術文献】
【特許文献】
【０００４】

【文献】特開２００５－３３２０６４号公報

【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、近年では、車載ネットワークが外部ネットワーク（例えば、インターネットやＷｉＦｉ（登録商標））に接続され、ユーザの利便性が向上した反面、従来の車載システムでは考えられていなかった車外からのサイバー攻撃（セキュリティ攻撃）によって電子制御装置（ＥＣＵ：Electronic Control Unit）が失陥する危険性が指摘されるようになった。
【０００６】
しかし、特許文献１に開示された技術では、セキュリティ攻撃によって機能が停止する場合を考慮しておらず、自動車の走行を継続するために冗長系を稼働させることで、運転手を危険に晒す可能性があった。すなわち、セキュリティ攻撃によって正常系の機能が停止する場合には、正常系と同様の機能を有する冗長系もセキュリティ攻撃を受ける可能性があるが、特許文献１ではこのような危険性が考慮されていなかった。
【０００７】
本発明は以上の点を考慮してなされたもので、正常な動作ができない場合の原因がセキュリティ攻撃に起因するか否かを区別して適切な対処方法を決定することにより、安全性を確保しながら、車載制御システムによる自動車の走行制御（例えば自動運転）を継続できるようにするものであり、自動車の走行制御を維持しつつ、冗長系起動時のセキュリティ上の安全性を向上させることができる電子制御装置、車載制御システム、及び冗長機能制御方法を提案しようとするものである。
【課題を解決するための手段】
【０００８】
かかる課題を解決するため本発明においては、自動車の走行制御を行う車載制御システムに搭載され、第１の制御装置及び第２の制御装置を含む複数の制御装置と通信可能に接続される電子制御装置であって、前記複数の制御装置の各制御装置におけるセキュリティ攻撃の有無を判定する攻撃判定部と、前記攻撃判定部による判定結果に基づいて、前記第１の制御装置が担っていた機能と同様またはその一部の機能による冗長機能を、前記第２の制御装置に代替して実行させるか否かを判定する冗長系実行判定部と、前記各制御装置の動作を監視し、前記各制御装置による前記機能の代替が必要な状況になっていないかを判断する機能監視部と、を備え、前記機能監視部が前記第１の制御装置による前記機能の代替が必要な状況になっていると判断したとき、前記冗長系実行判定部は、前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が無いと判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させ、前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が有ると判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させずに、前記第１の制御装置に対する所定のセキュリティ処理を実施させる電子制御装置が提供される。
【０００９】
また、かかる課題を解決するため本発明においては、自動車の走行制御を行う車載制御システムであって、所定の機能を有する第１の制御装置と、前記機能と同様またはその一部の機能による冗長機能を有する第２の制御装置と、を含む複数の制御装置と、前記複数の制御装置と通信可能に接続される電子制御装置と、を備え、前記電子制御装置が、前記複数の制御装置の各制御装置におけるセキュリティ攻撃の有無を判定する攻撃判定部と、前記攻撃判定部による判定結果に基づいて、前記第１の制御装置が担っていた前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させるか否かを判定する冗長系実行判定部と、前記各制御装置の動作を監視し、前記各制御装置による前記機能の代替が必要な状況になっていないかを判断する機能監視部と、を有し、前記機能監視部が前記第１の制御装置による前記機能の代替が必要な状況になっていると判断したとき、前記冗長系実行判定部は、前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が無いと判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置

に代替して実行させ、前記攻撃判定部によって前記第１の制御装置においてセキュリティ攻撃が有ると判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させずに、前記第１の制御装置に対する所定のセキュリティ処理を実施させる車載制御システムが提供される。

【００１０】

また、かかる課題を解決するため本発明においては、自動車の走行制御を行う車載制御システムに搭載され、第１の制御装置及び第２の制御装置を含む複数の制御装置と通信可能に接続される電子制御装置による冗長機能制御方法であって、前記複数の制御装置の各制御装置におけるセキュリティ攻撃の有無を判定する攻撃判定ステップと、前記攻撃判定ステップの判定結果に基づいて、前記第１の制御装置が担っていた機能と同様またはその一部の機能による冗長機能を、前記第２の制御装置に代替して実行させるか否かを判定する冗長系実行判定ステップと、前記各制御装置の動作を監視し、前記各制御装置による前記機能の代替が必要な状況になっていないかを判断する機能監視ステップと、を備え、前記機能監視ステップにおいて前記第１の制御装置による前記機能の代替が必要な状況になっていると判断したとき、前記冗長系実行判定ステップでは、前記攻撃判定ステップによって前記第１の制御装置においてセキュリティ攻撃が無いと判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させ、前記攻撃判定ステップによって前記第１の制御装置においてセキュリティ攻撃が有ると判定された場合には、前記機能に対応する前記冗長機能を前記第２の制御装置に代替して実行させずに、前記第１の制御装置に対する所定のセキュリティ処理を実施させる冗長機能制御方法が提供される。

【発明の効果】

【００１１】

本発明によれば、車載制御システムによる自動車の走行制御（例えば自動運転）を維持しつつ、冗長系起動時のセキュリティ上の安全性を向上させることができる。

【図面の簡単な説明】

【００１２】

【図１】本発明の第１の実施形態に係る車載制御システム１０の構成例を示すブロック図である。

【図２】データの受信時に電子制御装置１４０が実行する受信時処理の処理手順例を示すフローチャートである。

【図３】故障処理の詳細な処理手順例を示すフローチャートである。

【図４】侵害推定度ＤＢ１５０の一例を示す図である。

【図５】攻撃判定ＤＢ１５１の一例を示す図である。

【図６】冗長系稼働先ＤＢ１５２の一例を示す図である。

【図７】本発明の第２の実施形態に係る車載制御システム２０の構成例を示すブロック図である。

【図８】冗長系実行判定部２４６による処理の処理手順例を示すフローチャートである。

【図９】攻撃経路ＤＢ２５０の一例を示す図である。

【図１０】車載制御システム２０における電子制御装置の接続構成の別例を示すブロック図である。

【図１１】図１０の接続構成時の攻撃経路ＤＢ２５０Ａの一例を示す図である。

【図１２】本発明の第３の実施形態に係る車載制御システム３０の構成例を示すブロック図である。

【図１３】第３の実施形態における故障処理の詳細な処理手順例を示すフローチャートである。

【図１４】再配置先ＤＢ３５０の一例を示す図である。

【発明を実施するための形態】

【００１３】

以下、図面を参照して、本発明の実施形態を詳述する。

【００１４】
（１）第１の実施形態
図１は、本発明の第１の実施形態に係る車載制御システム１０の構成例を示すブロック図である。車載制御システム１０は、自動車の走行を制御するためのシステムであって、例えば自動運転を制御するシステムである。車載制御システム１０は、図１に示すように、電子制御装置１１０，１２０，１３０，１４０とスイッチ１６０とセンサ１７０とを備える。
【００１５】
電子制御装置１１０，１２０，１３０，１４０は、自動車の内部に搭載される電子制御装置の１つであり、具体的にはＥＣＵやゲートウェイである。各電子制御装置１１０～１４０において、プログラムやデータベースは、ＲＡＭ（Random Access Memory）やフラッシュＲＯＭ（Read Only Memory）等の一般的な記録媒体に保存されるとし、その一部が外部メモリに保存されていてもよい。
【００１６】
車載制御システム１０内の構成要素は、通信バス１１～１４またはスイッチ１６０を介して通信可能に接続される。通信バス１１～１４は、車載制御システム１０内部の電子制御装置１１０～１４０に接続され、適宜スイッチ１６０を用いて、バス型やスター型のネットワークを構築してもよい。通信バス１１～１４の規格は、ＣＡＮ（Controller Area Network）やＥｔｈｅｒｎｅｔ（登録商標）、ＬＩＮ（Local Interconnect Network）などを用いるのが一般的である。以下では、一例として通信バス１１，１２，１３にＥｔｈｅｒｎｅｔが利用されているものとして説明する。
【００１７】
具体的には図１の場合、電子制御装置１１０は、通信バス１１及びスイッチ１６０を介して、電子制御装置１２０，１３０に接続され、通信バス１４を介して複数のセンサ１７０に接続される。また、電子制御装置１４０は、通信バス１２を介して電子制御装置１３０に接続され、通信バス１３を介して電子制御装置１２０に接続される。なお、本例では、電子制御装置１１０はセンサ１７０と接続されることを想定しているが、電子制御装置１１０はその他の外部装置と接続されてもよい。
【００１８】
なお、図１の場合、車載制御システム１０は、４つの電子制御装置１１０，１２０，１３０，１４０を備える構成とされているが、本実施形態あるいは後述する他の実施形態に係る車載制御システムは、４つの電子制御装置を備えることを必須とするものではなく、適宜、構成が変更されてもよい。例えば、電子制御装置１１０は、センサ１７０が電子制御装置１２０に接続されている場合には、電子制御装置１１０を構成から省くことができる。また、電子制御装置の機能が１乃至いくつかの電子制御装置に統合されていてもよい。例えば、電子制御装置１３０の機能が他の電子制御装置１１０，１２０，１４０で代替できる場合には、電子制御装置１３０を構成から省くことができる。
【００１９】
以下、車載制御システム１０の各構成要素を詳しく説明する。
【００２０】
電子制御装置１１０は、センサ１７０で収集された収集データを受信し、収集データ及び電子制御装置１１０内部における異常を確認（検知）し、その検知結果を電子制御装置１２０，１３０に送信する機能を有する。電子制御装置１１０は、データ通信部１１１及び異常検知部１１２を備える。
【００２１】
データ通信部１１１は、センサ１７０から収集データを受信したり、所定のデータを通信バス１１及びスイッチ１６０を介して電子制御装置１２０，１３０に送信したりする。データ通信部１１１が送信するデータには、異常検知部１１２による検知結果を示すデータ以外に、センサ１７０から受信した収集データが含まれてもよい。
【００２２】

異常検知部１１２は、故障検知機能１１２０及びセキュリティ異常検知機能１１２１からなり、収集データ及び電子制御装置１１０内部における異常を検知する。

【００２３】

故障検知機能１１２０は、電子制御装置１１０内部における故障を検知する機能である。故障検知機能１１２０は、上記故障の検知結果を示すデータとして故障検知情報を出力し、故障検知情報は、データ通信部１１１によって電子制御装置１２０，１３０に送信される。

【００２４】

セキュリティ異常検知機能１１２１は、センサ１７０からの収集データ及び電子制御装置１１０内部のセキュリティ上の異常を検知する機能である。セキュリティ異常検知機能１１２１は、上記異常の検知結果を示すデータとして異常検知情報を出力し、異常検知情報は、データ通信部１１１によって電子制御装置１２０，１３０に送信される。

【００２５】

電子制御装置１２０は、電子制御装置１１０からデータを受信し、受信データ及び電子制御装置１２０内部における異常を確認（検知）し、その検知結果を電子制御装置１４０に送信する機能と、電子制御装置１１０から受信したデータを電子制御装置１４０に転送する機能とを有する。電子制御装置１２０は、データ通信部１２１、主系の情報処理部１２２及び異常検知部１２３を備える。

【００２６】

データ通信部１２１は、データ通信部１１１と同様に、データの送受信を行う機能を有する。さらに、データ通信部１２１は、電子制御装置１１０から受信した故障検知情報及び異常検知情報を、通信バス１３を介して電子制御装置１４０に転送する機能も有する。

【００２７】

主系の情報処理部１２２は、電子制御装置１１０から受信したデータを処理する機能を有する。

【００２８】

異常検知部１２３は、故障検知機能１２３０及びセキュリティ異常検知機能１２３１からなり、異常検知部１１２と同様の機能を有する。すなわち、故障検知機能１２３０は、電子制御装置１２０内部における故障を検知する機能であり、上記故障の検知結果を示すデータとして故障検知情報を出力する。また、セキュリティ異常検知機能１２３１は、センサ１７０からの収集データ及び電子制御装置１２０内部のセキュリティ上の異常を検知する機能であり、上記異常の検知結果を示すデータとして異常検知情報を出力する。異常検知部１２３の各機能によって出力された故障検知情報及び異常検知情報は、データ通信部１２１によって、通信バス１３を介して電子制御装置１４０に送信される。

【００２９】

電子制御装置１３０は、電子制御装置１１０からデータを受信し、所定のデータ処理を行い、その処理結果を電子制御装置１４０に送信する機能と、電子制御装置１１０から受信したデータを電子制御装置１４０に転送する機能とを有する。電子制御装置１３０は、データ通信部１３１及び冗長系の情報処理部１３２を備える。電子制御装置１３０は、電子制御装置１２０において主系の情報処理部１２２の機能が停止した際に、冗長系（情報処理部１３２）を稼働させる装置である。但し、電子制御装置１３０の情報処理部１３２で行われるデータ処理は、電子制御装置１２０の情報処理部１２２で行われるデータ処理とは異なるものであってもよい。

【００３０】

データ通信部１３１は、データ通信部１１１，１２１と同様にデータの送受信を行う機能を有する。さらに、データ通信部１３１は、電子制御装置１１０から受信した故障検知情報及び異常検知情報を、通信バス１２を介して電子制御装置１４０に転送する機能を有してもよい。

【００３１】

冗長系の情報処理部１３２は、主系の情報処理部１２２におけるデータ処理において故

障やセキュリティ攻撃によって正規の処理が困難な状況と判断された際に、情報処理部１２２の機能の冗長機能として、当該機能と同様またはその一部の機能を代替する機能を有する。

【００３２】

電子制御装置１４０は、電子制御装置１２０または電子制御装置１３０から受信した故障検知情報や異常検知情報を集約し、集約した情報を用いて電子制御装置１１０，１２０が攻撃されているか否か、及び正規の動作をしているか否かを判断し、それらの判断結果を用いて、冗長系の情報処理部１３２の稼働の可否を決定する機能を有する。

【００３３】

電子制御装置１４０は、機能監視部１４１、データ通信部１４２、データ解析部１４３、侵害推定度算出部１４４、攻撃判定部１４５、冗長系実行判定部１４６、冗長系管理部１４７、侵害推定度データベース（ＤＢ）１５０、攻撃判定データベース（ＤＢ）１５１、及び冗長系稼働先データベース（ＤＢ）１５２を備える。

【００３４】

機能監視部１４１は、車載制御システム１０内の電子制御装置１１０，１２０，１３０の動作を監視し、機能代替が必要な状況になっていないかを判断する機能を有する。監視方法の一例としては、予め設定された所定時間における対象の電子制御装置からのデータの受信状況に基づいて監視する方法や、電子制御装置１４０から各電子制御装置に対して動作を確認するデータを送信することによって監視する方法等がある。

【００３５】

データ通信部１４２は、データ通信部１１１，１２１，１３１と同様に、データの送受信を行う機能を有する。

【００３６】

データ解析部１４３は、データ通信部１４２が受信したデータの種別を判定する機能を有する。受信データの種別は、少なくとも、故障検知情報、異常検知情報、及び制御情報に分類することができる。また、受信したデータが異常検知情報である場合、データ解析部１４３は、異常を検知した電子制御装置の特定も行う。

【００３７】

侵害推定度算出部１４４は、電子制御装置１４０が受信した異常検知情報を用いて、各電子制御装置が攻撃されているか否かを判断する際に使用する侵害推定度を計算し、その計算結果に基づいて、電子制御装置１４０が保持する侵害推定度を更新する機能を有する。侵害推定度の計算には、侵害推定度ＤＢ１５０（詳細は図４を参照）が用いられ、各電子制御装置における侵害推定度は、攻撃判定ＤＢ１５１（詳細は図５を参照）に格納される。侵害推定度の計算方法の一例として、異常検知情報や攻撃種別ごとに侵害推定度を加算する方法が挙げられる。

【００３８】

攻撃判定部１４５は、侵害推定度算出部１４４で計算された侵害推定度を用いて、各電子制御装置が攻撃されているか否かを判定する攻撃判定の機能を有する。攻撃判定の具体的な判定基準例としては、侵害推定度が事前に定めた閾値を超えたことや、事前に定義した特定の異常検知情報を受信したこと等が挙げられる。各電子制御装置に対する攻撃判定の結果を表す情報、攻撃判定情報として攻撃判定ＤＢ１５１に登録される。

【００３９】

冗長系実行判定部１４６は、対象とする電子制御装置への攻撃判定の結果に基づいて、該当電子制御装置に対する冗長系を起動させるか否かを判定する機能を有する。冗長系起動の判定には、攻撃判定ＤＢ１５１に格納されている攻撃判定情報を用いる。なお、冗長系起動時のルールを詳細に定義したい場合には、冗長系機能のルールを別途データベースに定義するようにしてもよい。ルールの具体例としては、複数機能において冗長系の稼働が必要となった場合には、冗長系を起動させないといったルールが挙げられる。

【００４０】

冗長系管理部１４７は、冗長系実行判定部１４６によって冗長系を稼働させると判定さ

れた際に、冗長系の稼働先を決定し、稼働先の電子制御装置に対して、稼働の指示を出す機能を有する。冗長系稼働先の決定には、冗長系稼働先ＤＢ１５２（詳細は図６を参照）が用いられる。

【００４１】

侵害推定度ＤＢ１５０は、電子制御装置１４０が各電子制御装置１１０～１３０から受信する異常検知情報に対する侵害推定度を格納する。侵害推定度ＤＢ１５０は、データ通信部１４２が異常検知情報を受信し、侵害推定度算出部１４４が侵害推定度を計算し更新する場合に利用される。侵害推定度ＤＢ１５０のデータ構造は、後述する図４において説明される。

【００４２】

攻撃判定ＤＢ１５１は、各電子制御装置１１０～１３０に対する攻撃判定情報及び侵害推定度を格納する。攻撃判定ＤＢ１５１のデータ構造は、後述する図５において説明される。

【００４３】

冗長系稼働先ＤＢ１５２は、各電子制御装置１１０～１３０である機能が故障した場合に起動させる、冗長系の稼働先に関する情報を格納する。冗長系稼働先ＤＢ１５２は、冗長系管理部１４７が冗長系の稼働先に稼働指示を出す際に利用される。冗長系稼働先ＤＢ１５２のデータ構造は、後述する図６において説明される。

【００４４】

スイッチ１６０は、受信した情報を適切な電子制御装置に向けて転送する機能を有する装置である。具体的には例えば、スイッチ１６０は、電子制御装置１１０から通信バス１１を介して送信された情報を通信バス１１を介して電子制御装置１２０及び電子制御装置１３０に転送することができるが、通常時（主系の稼働時）には電子制御装置１２０を転送先とし、冗長系の稼働時には電子制御装置１３０を転送先に変更する等を可能とする。なお、スイッチ１６０は、電子制御装置（例えば電子制御装置１１０）に含まれるとしてもよい。

【００４５】

センサ１７０は、車載制御システム１０による自動運転の制御に必要な情報を収集する機能を有する各種センサであって、具体的には例えば、カメラ、レーダー、またはＬｉＤＡＲ（Light Detection And Ranging）等である。なお、センサ１７０は、攻撃のエントリーポイントとなり得る、インターネットやＢｌｕｅｔｏｏｔｈ（登録商標）との接続機能等でもよい。

【００４６】

図２は、データの受信時に電子制御装置１４０が実行する受信時処理の処理手順例を示すフローチャートである。図２では、電子制御装置１４０が電子制御装置１２０からデータを受信した場合の処理手順を示しているが、同様に、車載制御システム１０の他の電子制御装置（例えば電子制御装置１３０）からデータを受信した場合の処理にも適用することができる。

【００４７】

図２によればまず、ステップＳ２００において、電子制御装置１４０に電源が入力され、電子制御装置１４０の稼働後、各電子制御装置１１０～１４０（及びセンサ１７０）の間でデータのやり取りが開始される。なお、ステップＳ２０１以下の処理は、電子制御装置１４０の稼働時に、定期的あるいは所定の契機で繰り返し実行されると考えてよい。所定の契機とは例えば、他の電子制御装置からのデータを受信したとき、想定されたタイミングでデータを受信しなかったとき、同期のためのデータを電子制御装置１４０から他の電子制御装置に送信したとき、等が挙げられる。

【００４８】

ステップＳ２０１では、電子制御装置１４０の機能監視部１４１が、冗長系を起動させる可能性がある電子制御装置（本例では、電子制御装置１２０）を対象として、機能代替が必要な状況になっていないかを確認する。ここで確認する状況は、具体的には例えば、

一定期間の間、対象の電子制御装置（該当電子制御装置）からデータを受信できていない状況や、電子制御装置１４０から機能代替が必要か否かの問い合わせを行った結果、該当電子制御装置から機能代替が必要であるとのレスポンスを受信した状況が挙げられる。電子制御装置１４０が該当電子制御装置の機能代替が必要であると判断した場合は（ステップＳ２０１のＹＥＳ）、ステップＳ２０９に進み、該当電子制御装置の機能代替が必要ないと判断した場合は（ステップＳ２０１のＮＯ）、ステップＳ２０２に進む。

【００４９】

ステップＳ２０２では、電子制御装置１４０は、電子制御装置１２０からデータを受信する。

【００５０】

次のステップＳ２０３では、データ解析部１４３が、ステップＳ２０２で受信したデータが故障検知情報であるか否かを確認する。受信データが故障検知情報である場合は（ステップＳ２０３のＹＥＳ）、ステップＳ２０１に移行し、機能代替が必要な状況であるか否かを確認する。受信データが故障検知情報ではない場合は（ステップＳ２０３のＮＯ）、ステップＳ２０４に移行する。

【００５１】

ステップＳ２０４では、データ解析部１４３が、ステップＳ２０２で受信したデータが異常検知情報であるか否かを確認する。受信データが異常検知情報である場合は（ステップＳ２０４のＹＥＳ）、ステップＳ２０５に移行する。受信データが異常検知情報ではない場合は（ステップＳ２０４のＮＯ）、ステップＳ２０３の確認結果と合わせると受信データが制御情報であることを意味するため、ステップＳ２０８に移行し、受信データで指示されている処理を実施し、今回の受信時処理を終了する。

【００５２】

ステップＳ２０５では、侵害推定度算出部１４４が、ステップＳ２０２で受信したデータに対して侵害推定度を計算し、侵害推定度ＤＢ１５０に格納された侵害推定度を更新する。侵害推定度算出部１４４は、異常を検知した電子制御装置の制御情報、及び異常検知情報に基づいて、侵害推定度ＤＢ１５０を用いて侵害推定度を計算し更新する。例えば、電子制御装置１２０から受信したデータであっても、電子制御装置１１０で異常を検知した場合には、電子制御装置１１０に関する侵害推定度が更新される。なお、侵害推定度の計算方法の一例として、異常検知情報を受信するごとに、侵害推定度を加算する方法等が挙げられる。

【００５３】

次のステップＳ２０６では、攻撃判定部１４５が、ステップＳ２０５で侵害推定度が導出された電子制御装置（該当電子制御装置）が攻撃されているか否かを判定するために、当該侵害推定度が所定の閾値以上であるか否かを判定する。上記所定の閾値を決定する方法としては例えば、電子制御装置１４０が受信した異常検知情報の回数や重要度に基づいて事前に決定する方法が挙げられる。侵害推定度が閾値以上である場合は（ステップＳ２０６のＹＥＳ）、ステップＳ２０７に移行し、侵害推定度が閾値未満である場合は（ステップＳ２０６のＮＯ）、ステップＳ２０１に移行する。

【００５４】

ステップＳ２０７では、攻撃判定部１４５は、ステップＳ２０６で侵害推定度が閾値以上であった該当電子制御装置が攻撃されているとする攻撃判定をし、攻撃判定の結果を攻撃判定ＤＢ１５１に登録する。なお、攻撃判定した際には、データの破棄や該当電子制御装置におけるリプログラムミングを禁止する等の処理を実施するようにしてもよい。ステップＳ２０７の処理後はステップＳ２０１に移行する。

【００５５】

一方、前述したように、ステップＳ２０１において電子制御装置１４０が該当電子制御装置の機能代替が必要であると判断した場合は（ステップＳ２０１のＹＥＳ）、ステップＳ２０９の処理が行われる。ステップＳ２０９では、冗長系実行判定部１４６が、攻撃判定ＤＢ１５１を参照して、機能代替を必要とする該当電子制御装置が攻撃判定されている

か否かを確認する。事前にステップＳ２０７の処理が実行されて該当電子制御装置が攻撃判定されていた場合は、攻撃判定ＤＢ１５１に攻撃判定が登録されているので、この場合（ステップＳ２０９のＹＥＳ）、冗長系実行判定部１４６は、該当電子制御装置の冗長系を起動させないと判定し、ステップＳ２１０に移行する。一方、該当電子制御装置が攻撃判定されていない場合（ステップＳ２０９のＮＯ）、冗長系実行判定部１４６は、該当電子制御装置の冗長系を起動させると判定し、ステップＳ２１１に移行する。

【００５６】

ステップＳ２１０では、電子制御装置１４０（例えば冗長系管理部１４７）は、該当電子制御装置に対するセキュリティ処理を実施する。前述したように、セキュリティ処理が実施される場合は、冗長系の電子制御装置１３０（情報処理部１３２）は稼働されない。具体的なセキュリティ処理としては、例えば、所定のデータを受け付けないように設定を変更したり、機能を制限した縮退運転に移行したり、管理センタへ異常を通知したりする等が挙げられ、これら複数の処理を実施するようにしてもよい。なお、セキュリティ処理は、例えば冗長系管理部１４７によって実施されるとしたが、電子制御装置１４０が備える任意の処理部によって実施されるとしてもよい。

【００５７】

ステップＳ２１１では、電子制御装置１４０（例えば冗長系管理部１４７）は、該当電子制御装置に対する故障処理を実施する。故障処理においては、例えば、電子制御装置１２０の主系の情報処理部１２２に対して故障処理を行う場合、情報処理部１２２の機能の冗長機能として、当該機能と同様またはその一部の機能を他の電子制御装置で稼働させる。図１の例では、主系の情報処理部１２２と同様の機能を持つ電子制御装置１３０の情報処理部１３２に機能を代替する。故障処理の具体的な処理手順例については、図３を参照して後述する。なお、故障処理は、例えば冗長系管理部１４７によって実施されるとしたが、電子制御装置１４０が備える任意の処理部によって実施されるとしてもよい。

【００５８】

以上のように、電子制御装置１４０では、他の電子制御装置からデータを受信した場合に、図２に示す処理が行われることにより、受信データの種別やその内容から故障やセキュリティ攻撃の状況に応じて、電子制御装置の機能を代替させる等の適切な処理を実施することができる。

【００５９】

図３は、故障処理の詳細な処理手順例を示すフローチャートである。故障処理は、図２のステップＳ２１１において電子制御装置１４０（例えば冗長系管理部１４７）によって実施される処理である。

【００６０】

故障処理の実施が決定すると、まず、冗長系管理部１４７が、冗長系稼働先ＤＢ１５２を用いて、冗長系の稼働先（起動先）を決定する（ステップＳ３００）。

【００６１】

次に、冗長系管理部１４７は、冗長系稼働のための準備を行い、ステップＳ３００で決定した冗長系の稼働先に対して、稼働の指示を出す（ステップＳ３０１）。ステップＳ３００で決定した冗長系の稼働先が電子制御装置１４０以外の構成である場合には、冗長系管理部１４７は、当該稼働先を備える電子制御装置に対して、稼働指示を送信する。

【００６２】

図４は、侵害推定度ＤＢ１５０の一例を示す図である。侵害推定度ＤＢ１５０は、侵害推定度の計算に用いられる情報を格納するものであり、具体的には図４の場合、電子制御装置名１５００、異常検知情報１５０１、及び侵害推定度１５０２のデータ項目を含んで構成される。

【００６３】

電子制御装置名１５００には、異常検知情報を検知する可能性がある電子制御装置名が記載され、電子制御装置における故障や異常を検知する機能を有する異常検知部（例えば異常検知部１１２，１２３）を備える全ての電子制御装置の名称が登録される。

【００６４】
異常検知情報１５０１には、電子制御装置１４０が受信した異常検知情報の種別が記載される。本実施形態では、図２のステップＳ２０７において攻撃判定がなされた後に実施する対処方法を、異常検知情報の種別に応じて異なるように設定してもよい。
【００６５】
侵害推定度１５０２には、異常が検知された電子制御装置（電子制御装置名１５００）と異常検視情報の種別（異常検知情報１５０１）との組み合わせに応じて決定される侵害推定度が記載される。侵害推定度１５０２は、異常検知情報の重要度に応じて事前に割り当てられており（重要度が高いほど侵害推定度も高い）、その重要度は、例えば異常の生じやすさや、異常による被害の甚大さに基づいて決定される。
【００６６】
図５は、攻撃判定ＤＢ１５１の一例を示す図である。攻撃判定ＤＢ１５１は、侵害推定度算出部１４４によって計算された侵害推定度、及び攻撃判定部１４５によって判定された攻撃判定の結果を表す情報を、各電子制御装置について格納するものであり、具体的には図５の場合、電子制御装置名１５１０、攻撃判定情報１５１１、及び侵害推定度１５１２のデータ項目を含んで構成される。
【００６７】
電子制御装置名１５１０には、電子制御装置名１５００と同様に、異常検知情報を検知する可能性がある電子制御装置名が記載される。
【００６８】
攻撃判定情報１５１１には、電子制御装置が攻撃されたか否かに関する攻撃判定の結果を表す情報が格納される。攻撃判定情報１５１１の一例として、攻撃判定がされていない場合（すなわち、通常時）には「０」が登録されており、図２のステップＳ２０７で攻撃判定された場合には「１」が登録されるとする。
【００６９】
侵害推定度１５１２には、侵害推定度算出部１４４によって計算された侵害推定度が格納される。格納された侵害推定度１５１２は、攻撃判定の際に利用される。なお、侵害推定度１５１２は、電子制御装置１４０が異常検知情報を受信するごとに、異常検知情報が検知された該当電子制御装置の侵害推定度が計算されて更新される。
【００７０】
具体的には、図５の攻撃判定ＤＢ１５１は、電子制御装置１１０において「周期検知エラー」の異常が検知され、電子制御装置１２０において「Ｄａｔａ　Ｆｏｒｍａｔエラー」の異常が検知された場合の一例を示している。また、侵害推定度１５１２の初期値を「０」とし、攻撃判定の基準とする閾値を「６．０」とする。このとき、図４の侵害推定度ＤＢ１５０を参照すると、電子制御装置１１０で検知された「周期検知エラー」に対応する侵害推定度１５０２は「５．２５」であるため、攻撃判定ＤＢ１５１において、電子制御装置１１０の侵害推定度１５１２には「５．２５」が登録される。そして「５．２５」の侵害推定度１５１２は閾値「６．０」未満であることから攻撃判定されず、電子制御装置１１０の攻撃判定情報１５１１は「０」となる。一方、図４の侵害推定度ＤＢ１５０を参照すると、電子制御装置１２０で検知された「Ｄａｔａ　Ｆｏｒｍａｔエラー」に対応する侵害推定度１５０２は「６．９８」であるため、攻撃判定ＤＢ１５１において電子制御装置１２０の侵害推定度１５１２には「６．９８」が登録される。そして「６．９８」の侵害推定度１５１２は閾値「６．０」以上であることから攻撃判定され、電子制御装置１２０の攻撃判定情報１５１１は「１」となる。
【００７１】
図６は、冗長系稼働先ＤＢ１５２の一例を示す図である。冗長系稼働先ＤＢ１５２は、冗長系の稼働先に関する情報を格納するものであり、具体的には図６の場合、各電子制御装置に実装されている処理名１５２０及び冗長系稼働先１５２１のデータ項目を含んで構成される。
【００７２】

処理名１５２０には、車載制御システム１０内の電子制御装置に実装されている処理名が格納される。但し、処理名１５２０に格納される処理名は、事前の設計段階において、異常が発生した場合に冗長系を稼働させる可能性がある処理として設計された処理に限られる。図６では、処理名１５２０に、電子制御装置１２０に実装されている主系の情報処理部１２２が登録されている例が示されている。

【００７３】

冗長系稼働先１５２１には、処理名１５２０に登録された処理で故障が生じて正規の動作が実施できなくなった場合に、冗長系を稼働させる電子制御装置の情報が登録される。図６の冗長系稼働先１５２１では、冗長系の情報処理部１３２が実装された電子制御装置１３０に「○」印が付けられることにより、電子制御装置１３０が情報処理部１２２の冗長系起動先として登録されている例が示されている。

【００７４】

具体的には、電子制御装置１２０で情報処理部１２２が提供する機能が故障した場合に、図３に示した故障処理の実施が決定された場合、冗長系管理部１４７は、図６の冗長系稼働先ＤＢ１５２を参照することにより、冗長系稼働先として電子制御装置１３０を決定することができる。そして、冗長系管理部１４７は、この電子制御装置１３０に対して、稼働指示を送信することにより、主系の情報処理部１２２に代替して、冗長系の情報処理部１３２を稼働させることができる。

【００７５】

以上に説明したように、本実施形態に係る車載制御システム１０によれば、異常検知部１１２，１２３を備える電子制御装置１１０，１２０（図示は省略したが、電子制御装置１３０も、異常検知部を備えることによって、含めることができる）において、センサ１７０で収集されたデータまたは電子制御装置内部における異常（セキュリティ異常、故障）を検知し、電子制御装置１４０が、それらの検知結果に基づいて、各電子制御装置におけるセキュリティ異常及び故障の発生の有無と、機能代替の必要性とを判定することができる。特に、電子制御装置１４０は、各電子制御装置においてセキュリティ異常が発生した場合には、セキュリティ異常による影響の度合いを示す侵害推定度を算出し、その算出結果に基づいて、該当電子制御装置がセキュリティ攻撃を受けているかの攻撃判定を行うことができる。そして、電子制御装置１４０は、電子制御装置において異常（セキュリティ異常または故障）が発生して、機能代替が必要と判断した場合には、その異常の種別に応じて、セキュリティ処理または故障処理を実施することができる。その結果、車載制御システム１０は、冗長系がダメージを受けない故障が主系の機能で発生した場合は、故障処理によって、故障した主系に代替して冗長系の機能を稼働させることができる一方、冗長系も同様の攻撃を受ける可能性があるセキュリティ異常が主系の機能で発生した場合は、セキュリティ処理によって、冗長系に代替稼働させずに、セキュリティ攻撃に特化した対応を実施することができる。すなわち、本実施形態に係る車載制御システム１０（電子制御装置１４０）は、各電子制御装置において正常な動作が行えない原因がセキュリティ攻撃に起因するか否かを区別して、適切な対処方法を決定できることにより、車載制御システム１０による制御の安全性を確保しながら、車載制御システム１０による走行制御（例えば、自動車の自動運転制御）を可能な限り継続して提供することができるため、車載制御システムによる自動車の走行制御（例えば自動運転）を維持しつつ、冗長系起動時のセキュリティ上の安全性を向上させることができる。

【００７６】

（２）第２の実施形態

図７は、本発明の第２の実施形態に係る車載制御システム２０の構成例を示すブロック図である。第１の実施形態に係る車載制御システム１０との相違点として、第２の実施形態に係る車載制御システム２０は、攻撃経路を考慮した冗長系稼働への切り替えを可能とする。図１に示した車載制御システム１０の構成と比較すると、図７に示した車載制御システム２０は、電子制御装置１４０に代えて電子制御装置２４０を備える点で異なる。電子制御装置２４０は、冗長系実行判定部１４６とは異なる処理を実行する冗長系実行判定

部２４６と、攻撃経路データベース（ＤＢ）２５０とを備える点で、電子制御装置１４０とは異なる。なお、第２の実施形態に係る車載制御システム２０において、第１の実施形態に係る車載制御システム１０と共通する構成には同一の番号を付し、説明を省略する。

【００７７】

冗長系実行判定部２４６は、冗長系機能を稼働したい電子制御装置とは別の電子制御装置に対する侵害推定度を考慮した上で、冗長系機能を稼働させるか否かを判定する機能を有する。冗長系実行判定部２４６による処理の具体的な処理手順は、後述する図８において説明される。

【００７８】

攻撃経路ＤＢ２５０は、車載制御システム２０における、エントリーポイントから保護資産までの攻撃経路を格納する。攻撃経路ＤＢ２５０は、冗長系実行判定部２４６が冗長系を稼働させるか否かを判定する際に利用される。なお、保護資産の一例として、自動車の制御に関する機能が挙げられる。攻撃経路ＤＢ２５０のデータ構造は、後述する図９において説明される。

【００７９】

図８は、冗長系実行判定部２４６による処理の処理手順例を示すフローチャートである。図８では、図２に示した処理と同様の処理については、同一のステップ番号を付して詳細な説明を省略する。なお、図８に示す処理のうち、ステップＳ２０１は、冗長系実行判定部２４６ではなく、機能監視部１４１によって実行される。

【００８０】

図８によればまず、ステップＳ２０１において、機能監視部１４１が、冗長系を起動させる可能性がある電子制御装置を対象として、機能代替が必要な状況になっていないかを確認する。そしてステップＳ２０１において機能代替が必要であると判断された場合は、図２のステップＳ２０９で説明したように、冗長系実行判定部１４６が、攻撃判定ＤＢ１５１を参照して、機能代替を必要とする該当電子制御装置が攻撃判定されているか否かを確認する。図８では、このステップＳ２０９において、機能代替を必要とする該当電子制御装置が攻撃判定されている状況であるとして、以降の処理が示されている。

【００８１】

次のステップＳ８００では、冗長系実行判定部２４６は、攻撃判定ＤＢ１５１を参照し、侵害推定度１５１２が「０」ではない電子制御装置が存在するか否かを確認する。攻撃判定ＤＢ１５１に登録された全ての電子制御装置（電子制御装置名１５１０）において侵害推定度１５１２が「０」である場合には（ステップＳ８００のＮＯ）、ステップＳ２１１に移行し、図２で説明した故障処理が実施される。一方、攻撃判定ＤＢ１５１において侵害推定度１５１２が「０」ではない電子制御装置（電子制御装置名１５１０）が少なくとも１つ登録されている場合には（ステップＳ８００のＹＥＳ）、ステップＳ８０１に移行する。

【００８２】

ステップＳ８０１では、冗長系実行判定部２４６が、攻撃経路ＤＢ２５０を用いて、ステップＳ８００で確認した侵害推定度が「０」以外の電子制御装置に関連する攻撃経路を攻撃経路情報２５００から特定する（図９参照）。

【００８３】

次のステップＳ８０２では、冗長系実行判定部２４６がステップＳ８０１で特定した攻撃経路のなかに機能代替を実施したい該当電子制御装置が含まれるか否かを確認する。経路のなかに機能代替を実施したい該当電子制御装置が含まれていない場合は（ステップＳ８０２のＮＯ）、ステップＳ２１１に移行し、故障処理が実施される。一方、経路のなかに機能代替を実施したい該当電子制御装置が含まれる場合は（ステップＳ８０２のＹＥＳ）、ステップＳ２１０に移行し、セキュリティ処理が実施される。

【００８４】

以上のように、電子制御装置２４０では、他の電子制御装置からデータを受信したときに、ある電子制御装置において機能代替が必要で、かつ攻撃判定された場合に、ステップ

Ｓ８００～Ｓ８０２の処理が実行された結果、異常の状態に応じて、ステップＳ２１０のセキュリティ処理またはステップＳ２１１の故障処理を実施することができる。このとき特に、冗長系実行判定部２４６は、侵害推定度が「０」以外の電子制御装置に関する攻撃経路のなかに、機能代替が必要な電子制御装置が含まれている場合に、セキュリティ処理の実施を決定する。なお、図２でも説明したように、ステップＳ２１０で実施されるセキュリティ処理では、該当電子制御装置の冗長系は起動されず、ステップＳ２１１で実施される故障処理では、該当電子制御装置の冗長系が起動及び稼働される。この結果、車載制御システム２０（電子制御装置２４０）は、攻撃経路を考慮した冗長系稼働への切り替えを実現することができる。

【００８５】

また、本実施形態における故障処理の別の処理手順としては例えば、冗長系実行判定部１４６は、ステップＳ８０１において、攻撃判定ＤＢ１５１を参照して、機能代替を実施したい該当電子制御装置を含む攻撃経路を全て特定し、ステップＳ８０２において、特定した攻撃経路上に侵害推定度が「０」以外の電子制御装置が存在するか否かを判定するようにしてもよい。このようなステップＳ８０１～Ｓ８０２の処理手順でも、冗長系実行判定部１４６は、セキュリティ攻撃を受けている電子制御装置を含む攻撃経路上（セキュリティ攻撃を受ける可能性がある経路上）に、機能代替を実施したい該当電子制御装置が存在するか否かを確認することができる。

【００８６】

図９は、攻撃経路ＤＢ２５０の一例を示す図である。攻撃経路ＤＢ２５０は、車載制御システム２０におけるエントリーポイントから保護資産までの攻撃経路を格納するものであり、具体的には図９の場合、攻撃経路情報２５００のデータ項目を含んで構成される。なお、攻撃経路とは、セキュリティ攻撃が行われた場合に、当該攻撃が伝わる経路を示すものであり、一般的には、装置間の接続経路に概ね一致する。

【００８７】

攻撃経路情報２５００には、エントリーポイントから保護資産までの攻撃経路を示す情報が登録される。具体的には、図９の攻撃経路ＤＢ２５０には、センサ（例えばセンサ１７０の１つ）をエントリーポイントとし、走行制御に関する電子制御装置（電子制御装置１１０～１４０）を保護資産とするとき、センサから電子制御装置１４０までの２通りの攻撃経路が、攻撃経路情報２５００として登録されている。なお、図９の攻撃経路情報２５００における「通信１１」～「通信１４」は、通信バス１１～通信バス１４に対応する。

【００８８】

なお、第２の実施形態に係る車載制御システム２０が冗長系稼働への切り替えの際に考慮することができる攻撃経路は、図７の接続構成に限定されるものではなく、様々な接続構成に適用することができる。以下では、車載制御システム２０が、図７よりも複雑な電子制御装置の接続構成である場合を例に挙げて、冗長系稼働への切り替えを説明する。

【００８９】

図１０は、車載制御システム２０における電子制御装置の接続構成の別例を示すブロック図である。図１０に示した車載制御システム２０は、図７に示したよりも多くの電子制御装置が接続されて構成されている。なお、各電子制御装置の間を接続する通信２１～通信２５は、それぞれ、通信バスによって形成される通信経路である。

【００９０】

図１０において、例えば、電子制御装置２６０，２７０，２８０，２９０はそれぞれ、電子制御装置１１０，１２０，１３０と同様の機能を有する電子制御装置とする。図１０に示したように、電子制御装置２６０は、通信２１を介して電子制御装置１２０に接続される。電子制御装置１２０は、通信２１を介して電子制御装置２６０に接続され、通信２２を介して電子制御装置２４０に接続される。電子制御装置２４０は、通信２２を介して電子制御装置１２０に接続され、通信２３を介して電子制御装置２７０に接続され、通信２５を介して電子制御装置２９０に接続される。電子制御装置２７０は、通信２３を介して電子制御装置２４０に接続される。電子制御装置２８０は、通信２４を介して電子制御

装置２９０に接続される。電子制御装置２９０は、通信２４を介して電子制御装置２８０に接続され、通信２５を介して電子制御装置２４０に接続される。

【００９１】

図１１は、図１０の接続構成時の攻撃経路ＤＢ２５０Ａの一例を示す図である。図１１の攻撃経路ＤＢ２５０Ａでは、電子制御装置２７０に走行制御に関連する機能が含まれていると仮定しており、その攻撃経路情報２５００Ａには、エントリーポイント（電子制御装置２６０，２８０）から保護資産（電子制御装置２７０）までの攻撃経路が登録されている。

【００９２】

ここで、図１１の攻撃経路ＤＢ２５０Ａを用いて、図８のステップＳ８００～Ｓ８０２の処理手順を具体的に示すことにより、２通りの状況（第１の状況、第２の状況）において、電子制御装置１２０を代替する冗長系を稼働させるか否かの処理フローを説明する。

【００９３】

まず、第１の状況は、ステップＳ８００において、電子制御装置１２０は攻撃判定されていないが、電子制御装置２６０の侵害推定度が「０」ではない状況を想定する。このとき、ステップＳ８００は、上記想定により、侵害推定度が「０」ではない電子制御装置２６０が存在するため、ステップＳ８０１に移行し、電子制御装置２４０の冗長系実行判定部２４６が、図１１の攻撃経路ＤＢ２５０Ａを参照して、攻撃経路を特定する。具体的には、ステップＳ８０１では、電子制御装置２６０に関連する攻撃経路として、攻撃経路情報２５００Ａのデータ行の１行目のレコードが特定される。次のステップＳ８０２では、ステップＳ８０１で特定した攻撃経路のなかに、機能代替を実施したい電子制御装置１２０が含まれていることから、冗長系実行判定部２４６は「ＹＥＳ」と判定する。すなわち、機能代替を実施したい電子制御装置１２０が電子制御装置２６０の攻撃経路上に存在することから、ステップＳ２１０に移行し、冗長系を稼働させず、セキュリティ処理が実施される。ここで、同様の第１の状況について、図２の処理フローに従って第１の実施形態における処理を確認すると、電子制御装置１２０が攻撃判定されていないことから、ステップＳ２０９で冗長系実行判定部１４６がＮＯと判定し、冗長系の起動（故障処理の実施）が決定されてしまう。しかし、第２の実施形態では、上述したように図８の処理フローを実行することで、攻撃経路上に存在する電子制御装置で微かでもセキュリティ攻撃の兆候を検知した（「０」以外の侵害推定度が計算されている）場合には、冗長系を稼働させる措置を選択しないため、第１の実施形態よりも冗長系起動時のセキュリティ上の安全性を高めることができる。

【００９４】

次に、第２の状況は、ステップＳ８００において、電子制御装置１２０が攻撃判定されておらず、電子制御装置２８０の侵害推定度が「０」ではない状況を想定する。このとき、ステップＳ８００は、上記想定により、侵害推定度が「０」ではない電子制御装置２８０が存在するため、ステップＳ８０１に移行し、電子制御装置２４０の冗長系実行判定部２４６が、図１１の攻撃経路ＤＢ２５０Ａを参照して、攻撃経路を特定する。具体的には、ステップＳ８０１では、電子制御装置２８０に関連する攻撃経路として、攻撃経路情報２５００Ａのデータ行の２行目のレコードが特定される。次のステップＳ８０２では、ステップＳ８０１で特定した攻撃経路のなかに、機能代替を実施したい電子制御装置１２０が含まれていないことから、冗長系実行判定部２４６は「ＮＯ」と判定する。すなわち、第２の状況では、第１の状況とは異なり、機能代替を実施したい電子制御装置１２０が電子制御装置２８０の攻撃経路上に存在しないことから、ステップＳ２１１に移行し、冗長系を稼働させる故障処理が実施される。言い換えると、第２の状況では、電子制御装置２８０において侵害推定度が「０」ではなく、何らかのセキュリティ攻撃を受けていたとしても、電子制御装置１２０に代替する状況系の稼働には影響を及ぼすことがないため、セキュリティ上の安全性を維持しながら、冗長系への切り替えが可能となる。

【００９５】

以上のように、第２の実施形態に係る車載制御システム２０では、セキュリティ攻撃と

故障とが同時期に発生した場合、攻撃由来である可能性がある故障に対しては（第１の状況）、冗長系を稼働させないようにする一方で、攻撃由来ではない故障に対しては（第２の状況）、冗長系を稼働させることが可能なため、例えば電子制御装置２７０による走行制御の機能を継続して提供することができる。

【００９６】

（３）第３の実施形態

図１２は、本発明の第３の実施形態に係る車載制御システム３０の構成例を示すブロック図である。第１または第２の実施形態に係る車載制御システム１０，２０と比べると、第３の実施形態に係る車載制御システム３０は、設計段階で冗長系の稼働先が決定（特定）されておらず、冗長系を稼働しようとするときに、電子制御装置３４０の再配置管理部３４１が再配置先データベース（ＤＢ）３５０を用いて冗長系の再配置先（稼働先）を決定する必要がある点を特徴とする。この冗長系の再配置先の候補は複数用意することができる。また、第３の実施形態では、第２の実施形態と同様に、攻撃経路を考慮した冗長系稼働への切り替えを可能にする。なお、第３の実施形態に係る車載制御システム３０において、第１または第２の実施形態に係る車載制御システム１０，２０と共通する構成には同一の番号を付し、説明を省略する。

【００９７】

図１２に示したように、車載制御システム３０は、車載制御システム１０の電子制御装置１４０や車載制御システム２０の電子制御装置２４０に代えて、電子制御装置３４０を備える。この電子制御装置３４０は、冗長系管理部１４７を持たず、新たに、再配置管理部３４１、冗長系候補の情報処理部３４２、及び再配置先データベース（ＤＢ）３５０を備えて構成される。また、車載制御システム１０等では電子制御装置１３０が冗長系の情報処理部１３２を備えていたが、車載制御システム３０では、電子制御装置３３０が冗長系候補の情報処理部３３１を備えて構成される。

【００９８】

再配置管理部３４１は、再配置先ＤＢ３５０、攻撃判定ＤＢ１５１、及び攻撃経路ＤＢ２５０を用いて、主系の情報処理部１２２を代替する冗長系の再配置先（稼働先）を決定する。冗長系の再配置先として複数の候補が存在する場合、再配置管理部３４１は、リソースに余裕がある電子制御装置や、データのルーティングが少ない（短い）電子制御装置を優先して、冗長系の再配置先（稼働先）を決定する。この他にも、攻撃経路上に存在しない電子制御装置等の条件を組み合わせて、より適切な冗長系の稼働先を決定するようにしてもよい。

【００９９】

電子制御装置３３０が備える冗長系候補の情報処理部３３１、及び電子制御装置３４０が備える冗長系候補の情報処理部３４２は、電子制御装置１２０における主系の情報処理部１２２が正規の動作ができなくなった場合の冗長系の稼働先の候補である。情報処理部３３１，３４２では、情報処理部１２２と同様またはその一部の機能（冗長機能）を代替する機能を有する。

【０１００】

再配置先ＤＢ３５０は、主系の情報処理部に対応する冗長系の再配置先（稼働先）の候補について、設計段階における定義を格納する。第３の実施形態では、冗長系の再配置先は１つに確定されておらず、複数の候補を用意することができるため、再配置先ＤＢ３５０に定義された複数の候補のうちから、再配置管理部３４１によって１つの再配置先が決定される。再配置先ＤＢ３５０のデータ構造は、後述する図１４において説明される。

【０１０１】

図１３は、第３の実施形態における故障処理の詳細な処理手順例を示すフローチャートである。図１３に示す故障処理は、第３の実施形態において、図２または図８で示したステップＳ２１１の故障処理の際に、再配置管理部３４１が実施する処理である。

【０１０２】

主系の情報処理部１２２に対する故障判定の後、故障処理の実施が決定すると、まず、

再配置管理部３４１が、情報処理部１２２の機能に代替する冗長機能を再配置する電子制御装置を決定する（ステップＳ１３００）。再配置先の決定には、再配置先ＤＢ３５０及び攻撃経路ＤＢ２５０が用いられる。そして攻撃経路ＤＢ２５０を参照して攻撃経路の候補が特定できる場合、特定した攻撃経路上にある電子制御装置には、冗長系を再配置しないとする。

【０１０３】

次いで、再配置管理部３４１は、冗長系稼働のための準備を行い、ステップＳ１３００で決定した冗長系の再配置先に対して、冗長系の稼働指示を送信する（ステップＳ１３０１）。

【０１０４】

図１４は、再配置先ＤＢ３５０の一例を示す図である。再配置先ＤＢ３５０は、設計段階で定義された冗長系の再配置先の候補を格納するものであり、具体的には図１４の場合、処理名３５００及び再配置先３５０１のデータ項目を含んで構成される。

【０１０５】

処理名３５００には、車載制御システム３０内の電子制御装置に実装されている処理名が格納される。但し、処理名３５００に格納される処理名は、事前の設計段階において、異常が発生した場合に冗長系を稼働させる可能性がある処理として設計された処理に限られる。図１４では、処理名３５００に、電子制御装置１２０に実装されている主系の情報処理部１２２が登録されている例が示されている。

【０１０６】

再配置先３５０１には、処理名３５００に登録された処理で故障が生じて正規の動作が実施できなくなった場合の、冗長系の再配置先の候補が登録される。図１４の再配置先３５０１では、情報処理部３３１が実装された電子制御装置３３０と、情報処理部３４２が実装された電子制御装置３４０とに「○」印が付けられることにより、電子制御装置３３０，３４０が情報処理部１２２の冗長系の再配置先の候補として登録されている例が示されている。

【０１０７】

以上のように、第３の実施形態に係る車載制御システム３０では、冗長系の再配置が前提とされたシステム構成において、ある電子制御装置で故障が発生した場合に、設計段階で定義された再配置先の候補のうちから、故障発生時の状況に応じて適切な再配置先を決定し、当該再配置先で冗長系を稼働させることができるため、セキュリティ上の安全性を維持しながら冗長系への切り替えが可能となる。

【０１０８】

なお、本発明は上記した各実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上記した各実施形態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、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施形態の構成の一部を他の実施形態の構成に置き換えることが可能であり、また、ある実施形態の構成に他の実施形態の構成を加えることも可能である。また、各実施形態の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【０１０９】

また、上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、ＳＳＤ（Solid State Drive）等の記録装置、または、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に置くことができる。

【０１１０】

また、図面において制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。実際にはほとんど全ての構成が相互に接続されていると考えてもよい。

【符号の説明】
【０１１１】
１０，２０，３０　車載制御システム
１１～１４，２１～２５　通信バス
１１０，１２０，１３０，１４０，２４０，２６０，２７０，２８０，２９０，３３０，３４０　電子制御装置
１１１，１２１，１３１，１４２　データ通信部
１１２，１２３　異常検知部
１２２，１３２，３３１，３４２　情報処理部
１４１　機能監視部
１４３　データ解析部
１４４　侵害推定度算出部
１４５　攻撃判定部
１４６，２４６　冗長系実行判定部
１４７　冗長系管理部
１５０　侵害推定度データベース（ＤＢ）
１５１　攻撃判定データベース（ＤＢ）
１５２　冗長系稼働先データベース（ＤＢ）
１６０　スイッチ
１７０　センサ
２５０，２５０Ａ　攻撃経路データベース（ＤＢ）
３４１　再配置管理部
３５０　再配置先データベース（ＤＢ）
１１２０，１２３０　故障検知機能
１１２１，１２３１　セキュリティ異常検知機能

【図面】

【図１】

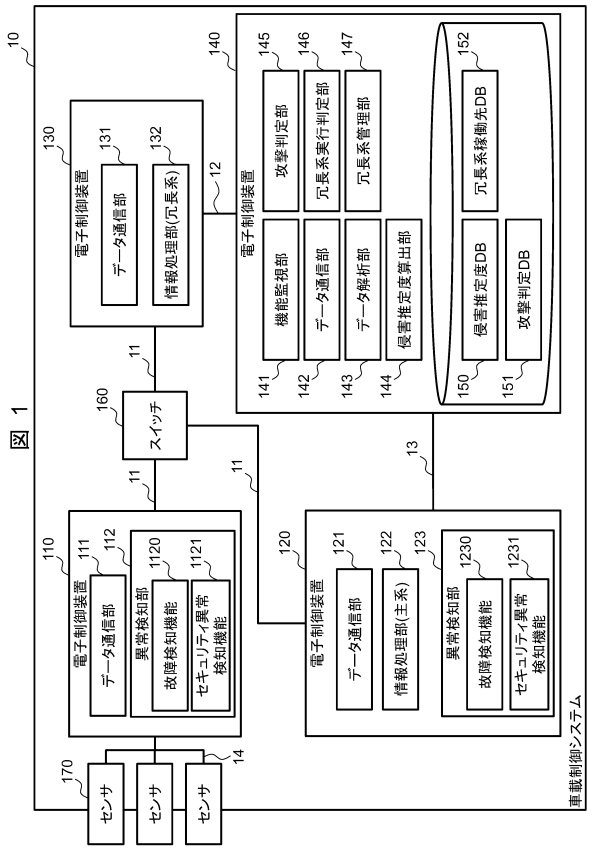
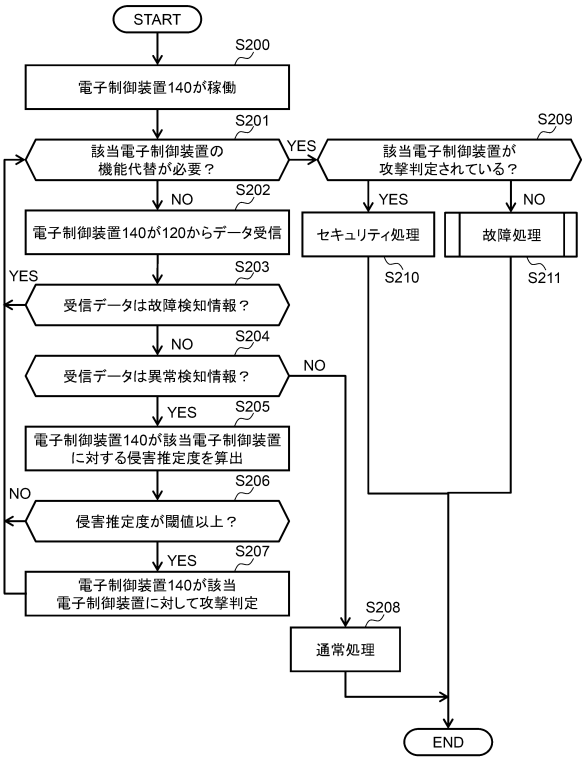


図 1

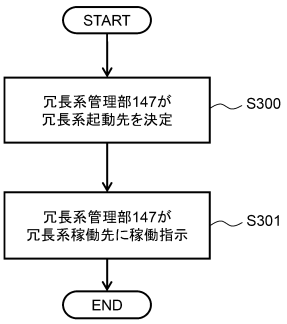
【図２】

図 2



【図３】

図 3



【図４】

図 4

150

1500	1501	1502
電子制御装置名	異常検知情報	侵害推定度
電子制御装置110	周期検知エラー	5.25
電子制御装置110	Packet Format エラー	5.25
電子制御装置110	Data Format エラー	6.98
電子制御装置120	Data Format エラー	6.98

【図５】

図 5

151

1510 電子制御装置名	1511 攻撃判定情報	1512 侵害推定度
電子制御装置110	0	5.25
電子制御装置120	1	6.98
電子制御装置130	0	0

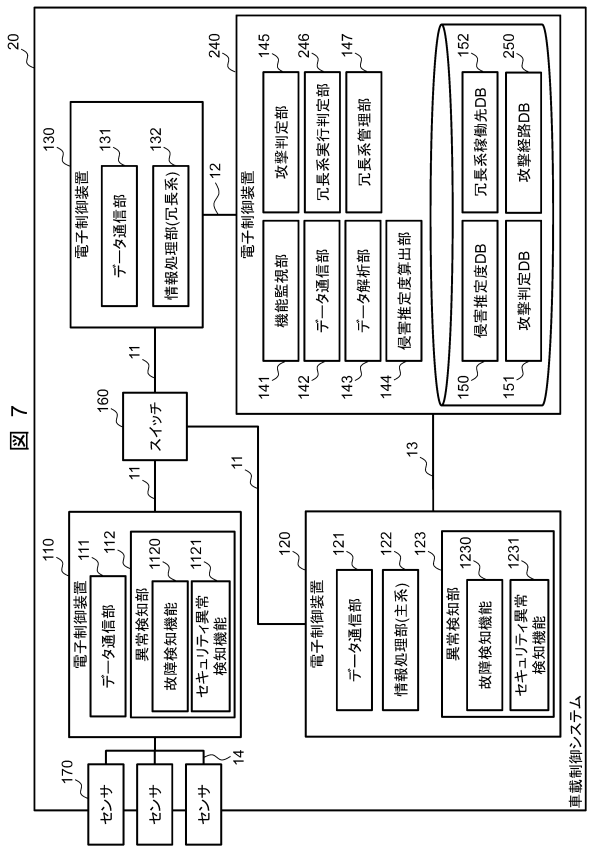
【図６】

図 6

152

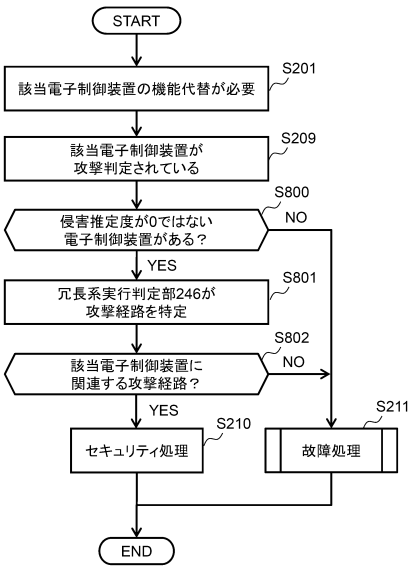
1520 処理名	1521 冗長系稼働先			
	電子制御装置110	電子制御装置120	電子制御装置130	電子制御装置140
情報処理部122	－	－	○	－

【図７】



【図８】

図 8



【図９】

図 9

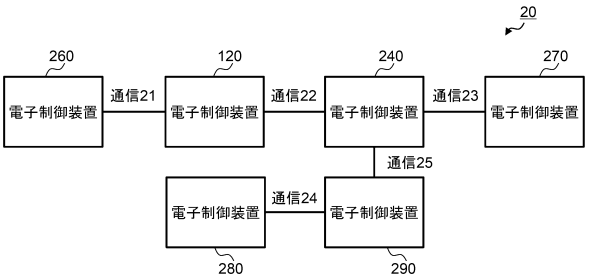
250

2500

攻撃経路情報						
センサ	通信14	電子制御装置 110	通信11	電子制御装置 120	通信13	電子制御装置 140
センサ	通信14	電子制御装置 110	通信11	電子制御装置 130	通信12	電子制御装置 140

【図１０】

図 10



【図１１】

図 11

250A

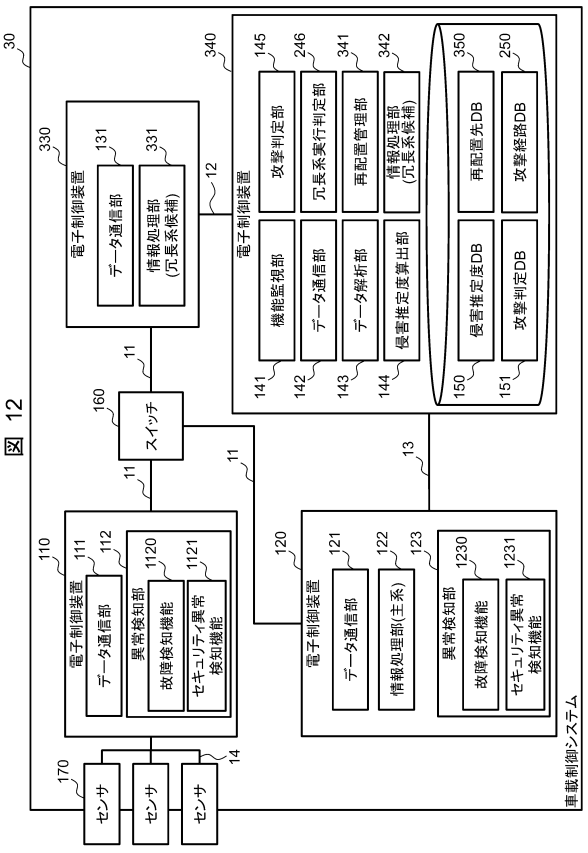
2500A

攻撃経路情報

電子制御装置 260	通信21	電子制御装置 120	通信22	電子制御装置 240	通信23	電子制御装置 270
電子制御装置 280	通信24	電子制御装置 290	通信25	電子制御装置 240	通信23	電子制御装置 270

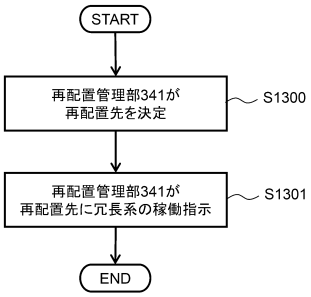
【図１２】

図 12



【図１３】

図 13



【図１４】

図 14

350

3500 処理名	3501 再配置先			
	電子制御装置 110	電子制御装置 120	電子制御装置 330	電子制御装置 340
情報処理部122	－	－	○	○

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 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 藤井 康広
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 稲本 遥

(56)参考文献 国際公開第２０２０／２４６０３１（WO，Ａ１）
特開２０１７－０８１２９０（ＪＰ，Ａ）
米国特許出願公開第２０１９／０３３７５２６（ＵＳ，Ａ１）
特開２０１９－１２５３４４（ＪＰ，Ａ）
米国特許出願公開第２０１９／０３１２８９２（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｂ６０Ｗ １０／００－１０／３０
３０／００－６０／００
Ｇ０８Ｇ １／００－９９／００
Ｇ０６Ｆ ２１／５５