(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-174111
(P2017-174111A)
(43)公開日　平成29年9月28日(2017.9.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/62		5K033
B60R 16/02	(2006.01)	B60R	16/02	660U	
B60R 16/023	(2006.01)	B60R	16/023	P	
H04L 12/46	(2006.01)	H04L	12/46	Z	
		H04L	12/46	100C	

審査請求 未請求　請求項の数 22　ＯＬ　（全 35 頁）

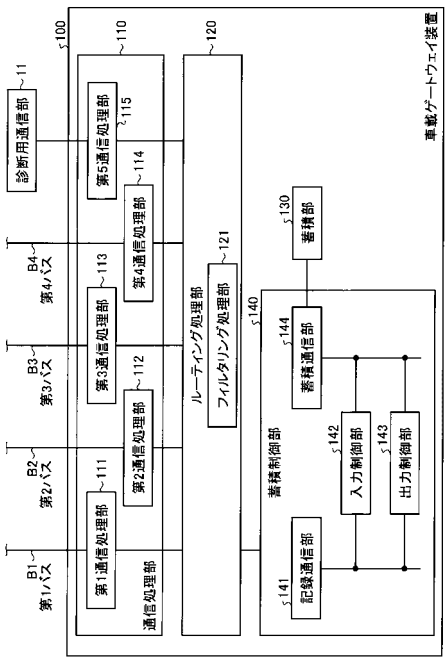
(21)出願番号　特願2016-58798(P2016-58798)
(22)出願日　平成28年3月23日(2016.3.23)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　磯崎　宏
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　加藤　拓
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　金井　遵
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】車載ゲートウェイ装置、蓄積制御方法およびプログラム

(57)【要約】
【課題】蓄積するデータを保護しながら、データの用途に応じてその出力を制限できる車載ゲートウェイ装置、蓄積制御方法およびプログラムを提供する。
【解決手段】実施形態の車載ゲートウェイ装置１００は、車載システムに搭載される車載ゲートウェイ装置であって、車載システムに含まれるＥＣＵ（電子制御ユニット）が出力するデータを蓄積する蓄積部１３０と、少なくとも一つのＥＣＵが接続される内部通信処理部を含む複数の内部通信処理部１１１－１１５と、複数の内部通信処理部１１１－１１５の間でデータを転送するとともに、転送したデータの少なくとも一部を蓄積部１３０に蓄積可能に出力するルーティング処理部１２０と、蓄積部１３０に蓄積するデータと蓄積部１３０から出力するデータとの少なくともいずれかを所定のルールに従って加工または選別する蓄積制御部１４０と、を備える。
【選択図】図２



【特許請求の範囲】
【請求項１】
車載システムに搭載される車載ゲートウェイ装置であって、
前記車載システムに含まれる電子制御ユニットが出力するデータを蓄積する蓄積部と、
少なくとも一つの電子制御ユニットが接続される内部通信処理部を含む複数の内部通信処理部と、
前記複数の内部通信処理部の間でデータを転送するとともに、転送したデータの少なくとも一部を前記蓄積部に蓄積可能に出力するルーティング処理部と、
前記蓄積部に蓄積するデータと前記蓄積部から出力するデータとの少なくともいずれかを所定のルールに従って加工または選別する蓄積制御部と、を備える車載ゲートウェイ装置。
【請求項２】
前記複数の内部通信処理部のうちの少なくとも一つは、インターネットに接続された外部通信処理部と通信を行う、請求項１に記載の車載ゲートウェイ装置。
【請求項３】
前記蓄積制御部によるデータの加工は暗号処理を含む、請求項１に記載の車載ゲートウェイ装置。
【請求項４】
前記暗号処理に用いる鍵がデータの出力先に応じて異なる、請求項２に記載の車載ゲートウェイ装置。
【請求項５】
電子制御ユニットが出力するデータを外部機器に送信する診断用通信部をさらに備え、
前記蓄積制御部は、前記蓄積部から出力するデータの出力先が前記外部機器である場合は、当該データを暗号化する、請求項１乃至４のいずれか一項に記載の車載ゲートウェイ装置。
【請求項６】
前記蓄積制御部は、データの加工または選別を行うか否かの設定、または、データの加工または選別を行う際の前記ルールを変更する設定を行うモード設定部を備える、請求項１乃至５のいずれか一項に記載の車載ゲートウェイ装置。
【請求項７】
前記所定のルールは、電子制御ユニットが出力するデータが伝送されるバスに応じて、前記蓄積部へのデータの入力を許可または禁止するルールを含む、請求項１乃至６のいずれか一項に記載の車載ゲートウェイ装置。
【請求項８】
前記所定のルールは、同一のセンサ信号を取得して異なるバスに出力する複数の電子制御ユニットが出力するデータが一致するか否かにより、複数の電子制御ユニットが出力するデータを前記蓄積部に蓄積するか、いずれかの電子制御ユニットが出力するデータのみを前記蓄積部に蓄積するかを判定するルールを含む、請求項１乃至７のいずれか一項に記載の車載ゲートウェイ装置。
【請求項９】
前記電子制御ユニットのファームウェアに関する情報を取得する情報取得部をさらに備え、
前記蓄積部は、前記電子制御ユニットが出力するデータと、前記情報取得部が取得した前記ファームウェアに関する情報とを蓄積する、請求項１乃至８のいずれか一項に記載の車載ゲートウェイ装置。
【請求項１０】
前記情報取得部は、前記車載システムを介した前記ファームウェアのアップデートを監視して、前記ファームウェアに関する情報を取得する、請求項９に記載の車載ゲートウェイ装置。
【請求項１１】

前記情報取得部は、前記電子制御ユニットに対して前記ファームウェアに関する情報を問い合わせることにより、前記ファームウェアに関する情報を取得する、請求項９に記載の車載ゲートウェイ装置。
【請求項１２】
前記ルーティング処理部は、外部装置から暗号化されて送信された前記ファームウェアを復号して前記電子制御ユニットが接続される内部通信処理部に転送し、
前記情報取得部は、復号した前記ファームウェアが、前記電子制御ユニットが接続される内部通信処理部に転送される際に前記ファームウェアに関する情報を取得する、請求項９に記載の車載ゲートウェイ装置。
【請求項１３】
前記ファームウェアに関する情報は、前記ファームウェアのバージョン情報または前記ファームウェアのハッシュ値である、請求項９乃至１２のいずれか一項に記載の車載ゲートウェイ装置。
【請求項１４】
前記蓄積部が蓄積するデータを削除または無効化するデータ管理部をさらに備える、請求項１乃至１３のいずれか一項に記載の車載ゲートウェイ装置。
【請求項１５】
前記データ管理部は、前記蓄積部が蓄積するデータの種類に応じて当該データを削除または無効化するタイミングを決定する、請求項１４に記載の車載ゲートウェイ装置。
【請求項１６】
前記データ管理部は、前記蓄積部が蓄積するデータが外部装置に出力されると、当該データを削除または無効化する、請求項１４に記載の車載ゲートウェイ装置。
【請求項１７】
前記データ管理部は、前記車載システムを搭載した車両のオペレータが変更された場合に、前記蓄積部が蓄積するデータを削除または無効化する、請求項１４に記載の車載ゲートウェイ装置。
【請求項１８】
前記蓄積制御部は、前記電子制御ユニットが出力するデータを、所定単位のグループごとに共通の鍵を用いて暗号化し、
前記データ管理部は、前記鍵を削除または上書きすることで、前記蓄積部が蓄積する、前記鍵を用いて暗号化されたデータを無効化する、請求項１４乃至１７のいずれか一項に記載の車載ゲートウェイ装置。
【請求項１９】
前記蓄積制御部は、さらに複数の前記鍵を共通の鍵暗号化鍵を用いて暗号化し、
前記データ管理部は、前記暗号化鍵を削除または上書きすることで、前記蓄積部が蓄積する、前記鍵を用いて暗号化されたデータを無効化する、請求項１８に記載の車載ゲートウェイ装置。
【請求項２０】
前記蓄積部に蓄積するデータを選別する前記ルールの変更が要求された場合に、該変更の要因となるイベントが実際に発生しているかを確認する監視部をさらに備える、請求項１乃至１９のいずれか一項に記載の車載ゲートウェイ装置。
【請求項２１】
車載システムに搭載される車載ゲートウェイ装置において実行される蓄積制御方法であって、
前記車載ゲートウェイ装置は、
前記車載システムに含まれる電子制御ユニットが出力するデータを蓄積する蓄積部を備え、
少なくとも一つの電子制御ユニットが接続される内部通信処理部を含む複数の内部通信処理部の間でデータを転送するとともに、転送したデータの少なくとも一部を前記蓄積部に蓄積可能に出力する工程と、

前記蓄積部に蓄積するデータと前記蓄積部から出力するデータとの少なくともいずれかを所定のルールに従って加工または選別する工程と、を含む蓄積制御方法。
【請求項２２】
車載システムに搭載される車載ゲートウェイ装置に、
前記車載システムに含まれる電子制御ユニットが出力するデータを蓄積する蓄積部の機能と、
少なくとも一つの電子制御ユニットが接続される内部通信処理部を含む複数の内部通信処理部の機能と、
前記複数の内部通信処理部の間でデータを転送するとともに、転送したデータの少なくとも一部を前記蓄積部に蓄積可能に出力するルーティング処理部の機能と、
前記蓄積部に蓄積するデータと前記蓄積部から出力するデータとの少なくともいずれかを所定のルールに従って加工または選別する蓄積制御部の機能と、を実現させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、車載ゲートウェイ装置、蓄積制御方法およびプログラムに関する。
【背景技術】
【０００２】
従来、車載システムにおいてデータを記録するための記録装置が存在した。それらの記録装置は、ドライブレコーダに代表されるようにカメラで撮影した映像データをハードディスクドライブ（ＨＤＤ）やＳＤカードなどの記録媒体に記録する機能を備えている。また、車載システムに搭載された電子制御ユニット（ＥＣＵ：Electronic Control Unit）が出力するデータを収集し、車外のサーバにログとして記録するシステムも提案されている。
【０００３】
しかし、従来の技術では、車載システムが外部装置とネットワークを介して接続され、不正な外部装置から攻撃を受けたり、車載システムの内部に悪意のある装置やプログラムが存在したりすることを想定していない。このため、攻撃者または悪意ある利用者から記録媒体に記録されたデータを不正に取得されたり、不正に改変されたり、不正に消去されたりする脅威には対応していなかった。
【０００４】
また、車載システム内部で発生した異常やセキュリティ上の検証処理が失敗したことを検出し、ログに記録する仕組みも提案されている。しかしこの場合も、車載システム内部の不正モジュールや不正プログラムから記録媒体に記録されたデータを不正に操作されることは想定していない。このため、セキュリティ事故が発生したとしても、その痕跡を残すための具体的な実現方法は明らかになっていなかった。
【０００５】
また、ＥＣＵが出力するデータには完成車メーカのノウハウが含まれているため、完成車メーカにとって保護対象のデータとなり得る。例えば、完成車メーカ自身もしくは保険会社や、裁判所などの法的機関など完成車メーカが許可した第３者にはＥＣＵが出力して車載システム内部に蓄積した全てのデータを開示する一方で、一般ユーザや競合の完成車メーカに対してはデータの取得や解析を防止したり、蓄積したデータを部分的に公開したりする仕組みが求められる。しかし、その具体的な実現方法は明らかになっていなかった。
【０００６】
以上のことから、ＥＣＵが出力するデータを車載システム内部に蓄積する場合、蓄積するデータを保護しながら、データの用途に応じてその出力を制限できる仕組みを構築することが求められる。

【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２０１１－１２１４２５号公報
【非特許文献】
【０００８】
【非特許文献１】D. K. Nilsson and U. E. Larson, “A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure”, in Journal of Networks, vol. 4, no. 7, 2009
【発明の概要】
【発明が解決しようとする課題】
【０００９】
本発明が解決しようとする課題は、蓄積するデータを保護しながら、データの用途に応じてその出力を制限できる車載ゲートウェイ装置、蓄積制御方法およびプログラムを提供することである。
【課題を解決するための手段】
【００１０】
実施形態の車載ゲートウェイ装置は、車載システムに搭載される車載ゲートウェイ装置であって、蓄積部と、複数の内部通信処理部と、ルーティング処理部と、蓄積制御部と、を備える。蓄積部は、前記車載システムに含まれる電子制御ユニットが出力するデータを蓄積する。複数の内部通信処理部は、少なくとも一つの電子制御ユニットが接続される内部通信処理部を含む。ルーティング処理部は、前記複数の内部通信処理部の間でデータを転送するとともに、転送したデータの少なくとも一部を前記蓄積部に蓄積可能に出力する。蓄積制御部は、前記蓄積部に蓄積するデータと前記蓄積部から出力するデータとの少なくともいずれかを所定のルールに従って加工または選別する。
【図面の簡単な説明】
【００１１】
【図１】車載システムの概略構成を示すブロック図。
【図２】第１実施形態の車載ゲートウェイ装置の機能的な構成例を示すブロック図。
【図３－１】入力制御部の内部構成例を示す図。
【図３－２】入力制御部の内部構成例を示す図。
【図３－３】入力制御部の内部構成例を示す図。
【図４－１】出力制御部の内部構成例を示す図。
【図４－２】出力制御部の内部構成例を示す図。
【図４－３】出力制御部の内部構成例を示す図。
【図４－４】出力制御部の内部構成例を示す図。
【図４－５】出力制御部の内部構成例を示す図。
【図４－６】出力制御部の内部構成例を示す図。
【図５】第３外部通信処理部を備える車載システムの概略例を示すブロック図。
【図６】図５の車載システムに対応する車載ゲートウェイ装置の構成例を示すブロック図。
【図７】蓄積制御部をルーティング処理部内に組み込んだ車載ゲートウェイ装置の構成例を示すブロック図。
【図８】第２実施形態の車載ゲートウェイ装置の機能的な構成例を示すブロック図。
【図９】システム情報取得部を蓄積制御部内に組み込んだ車載ゲートウェイ装置の構成例を示すブロック図。
【図１０】システム情報取得部をルーティング処理部内に組み込んだ車載ゲートウェイ装置の構成例を示すブロック図。
【図１１】暗号化されたファームウェアの復号を行う車載ゲートウェイ装置の構成例を示すブロック図。

【図１２】ファームウェアの検証を行う車載ゲートウェイ装置の構成例を示すブロック図。
【図１３】ファームウェアの検証および復号を行う車載ゲートウェイ装置の構成例を示すブロック図。
【図１４】第３実施形態の車載ゲートウェイ装置の機能的な構成例を示すブロック図。
【図１５】プライバシを考慮した車載ゲートウェイ装置の構成例を示すブロック図。
【図１６】認証が成功した場合にプライバシ情報を削除する車載ゲートウェイ装置の構成例を示すブロック図。
【図１７】暗号鍵記録部を備える車載ゲートウェイ装置の構成例を示すブロック図。
【図１８】鍵蓄積部に暗号鍵記録部を設けた車載ゲートウェイ装置の構成例を示すブロック図。
【図１９】第４実施形態の車載ゲートウェイ装置の機能的な構成例を示すブロック図。
【発明を実施するための形態】
【００１２】
実施形態の車載ゲートウェイ装置は、ＥＣＵが出力するデータを効率よく蓄積し、改変されることを防止しつつ、蓄積したデータをセキュリティ事故が発生した後などに選択的に出力するものである。以下では、このような車載ゲートウェイ装置の具体的な構成例について、図面を参照しながら詳細に説明する。
【００１３】
＜第１実施形態＞
まず、実施形態の車載ゲートウェイ装置を搭載した車載システムについて説明する。図１は、車載システム１０の概略構成を示すブロック図である。この車載システム１０は、例えば自動車やバス、トラック、バイクなどの車両に搭載されることを想定している。なお、図１に示す車載システム１０の構成は一例であり、これに限らない。例えば、車載システム１０に含まれるＥＣＵの数や各ＥＣＵの役割分担、車載ゲートウェイ装置１００との接続関係などは、車両の構成などに応じて任意に変更することができる。また、信頼性向上のために特定のＥＣＵを複数のバスに接続し、一方のバスが故障しても他方のバスでデータを送受信できる冗長な構成とすることもある。
【００１４】
図１に示す車載システム１０は、車載ゲートウェイ装置１００と、診断用通信部１１と、エンジン制御ＥＣＵ１２と、ステアリング制御ＥＣＵ１３と、ブレーキ制御ＥＣＵ１４と、ライト制御ＥＣＵ１５と、エアバッグ制御ＥＣＵ１６と、空調制御ＥＣＵ１７と、センサＥＣＵ１８と、座席制御ＥＣＵ１９と、映像処理ＥＣＵ２０と、第１外部通信処理部２１と、運転支援制御ＥＣＵ２２と、第２外部通信処理部２３とを備えている。
【００１５】
エンジン制御ＥＣＵ１２は、車両のエンジンを制御するＥＣＵである。ステアリング制御ＥＣＵ１３は、車両のステアリング操作を制御するＥＣＵである。ブレーキ制御ＥＣＵ１４は、車両のブレーキを制御するＥＣＵである。ライト制御ＥＣＵ１５は、車両のライト（電燈）の動作を制御するＥＣＵである。エアバッグ制御ＥＣＵ１６は、車両のエアバッグの動作を制御するＥＣＵである。
【００１６】
これらエンジン制御ＥＣＵ１２、ステアリング制御ＥＣＵ１３、ブレーキ制御ＥＣＵ１４、ライト制御ＥＣＵ１５およびエアバッグ制御ＥＣＵ１６は、例えば、ＣＡＮ（Controller Area Network）の規格に準拠した第１バスＢ１に接続され、パワートレインＣＡＮと呼ばれるネットワークを構成する。このパワートレインＣＡＮの各ＥＣＵは、第１バスＢ１を介して、車載ゲートウェイ装置１００に接続されている。
【００１７】
空調制御ＥＣＵ１７は、車両の空調を制御するＥＣＵである。センサＥＣＵ１８は、車両の温度センサや圧力センサなど車両内外の状態を計測する各種センサを含むＥＣＵである。座席制御ＥＣＵ１９は、車両の座席の位置を制御するＥＣＵである。

【００１８】
これら空調制御ＥＣＵ１７、センサＥＣＵ１８および座席制御ＥＣＵ１９は、例えば、ＣＡＮの規格に準拠した第２バスＢ２に接続され、ボディＣＡＮと呼ばれるネットワークを構成する。このボディＣＡＮの各ＥＣＵは、第２バスＢ２を介して、車載ゲートウェイ装置１００に接続されている。なお、上述の冗長な構成の一例として、センサＥＣＵ１８は、各々が異なるバスに接続された複数のＥＣＵを含み、これら複数のＥＣＵが同一のセンサ信号を取得して異なるバスに出力する場合もある。
【００１９】
映像処理ＥＣＵ２０は、例えば、地図情報や車両の状態を液晶モニタなどの表示装置に表示する処理を行うＥＣＵである。映像処理ＥＣＵ２０は、外部から地図情報や渋滞情報などを取得するために、第１外部通信処理部２１と接続されている。第１外部通信処理部２１は、例えば、３ＧＰＰ（3rd Generation Partnership Project；登録商標）やＬＴＥ（Long Term Evolution；登録商標）などの移動体通信網や、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの無線を用いてインターネットと通信する処理を行う。
【００２０】
映像処理ＥＣＵ２０および第１外部通信処理部２１は、例えば、ＩＢＤ１３９４やＭＯＳＴ（Media Oriented Systems Transport；登録商標）などの規格に準拠した第３バスＢ３に接続され、ＡＶ（Audio-Visual）ネットワークと呼ばれるネットワークを構成する。映像処理ＥＣＵ２０および第１外部通信処理部２１は、第３バスＢ３を介して、車載ゲートウェイ装置１００に接続されている。
【００２１】
運転支援制御ＥＣＵ２２は、先進運転支援システム（ＡＤＡＳ：Advanced Driving Assistant System）または自動運転に必要な経路選択制御などの処理を行うＥＣＵである。運転支援制御ＥＣＵ２２は、例えばＡＤＡＳに必要な情報を取得するために、第２外部通信処理部２３と接続されている。第２外部通信処理部２３は、例えば、８０２．１１ｐなどの無線を用いて道路上の路側機や他の外部装置と通信し、信号の状態や他の情報記録装置との距離などを受信する処理を行う。
【００２２】
運転支援制御ＥＣＵ２２および第２外部通信処理部２３は、例えば、ＬＩＮ（Local Interconnect Network）の規格に準拠した第４バスＢ４に接続され、ＬＩＮと呼ばれるネットワークを構成する。運転支援制御ＥＣＵ２２および第２外部通信処理部２３は、第４バスＢ４を介して、車載ゲートウェイ装置１００に接続されている。
【００２３】
診断用通信部１１は、車載システム１０が自己故障診断を行うために、車載システム１０に含まれる各ＥＣＵから収集した診断情報を外部機器に送信する処理を行うものである。この診断用通信部１１は、例えば、ＯＤＢ（ＯＤＢ，ＯＤＢ１．５，ＯＤＢＩＩ）などの規格に準拠した通信処理を行う。診断用通信部１１は、車載ゲートウェイ装置１００に接続され、車載システム１０に含まれる各ＥＣＵの診断情報は、車載ゲートウェイ装置１００を介して診断用通信部１１から外部機器に送信される。
【００２４】
なお、第１バスＢ１、第２バスＢ２、第３バスＢ３および第４バスＢ４は、それぞれ異なる通信規格、異なる通信速度、異なる通信レート、異なるレイテンシのバスであってもよいし、同じ通信規格、同じ性能を備えていてもよい。これらのバスが同じ通信規格、同じ性能を備えている場合は、必ずしも物理的に別々の通信線になっている必要はなく、同じ通信線で各ＥＣＵが接続されていてもよい。
【００２５】
次に、本実施形態の車載ゲートウェイ装置１００の詳細について説明する。図２は、車載ゲートウェイ装置１００の機能的な構成例を示すブロック図である。本実施形態の車載ゲートウェイ装置１００は、図２に示すように、通信処理部１１０と、ルーティング処理

部１２０と、蓄積部１３０と、蓄積制御部１４０とを備える。

【００２６】

通信処理部１１０は、複数の内部通信処理部として、第１通信処理部１１１と、第２通信処理部１１２と、第３通信処理部１１３と、第４通信処理部１１４と、第５通信処理部１１５とを含む。第１通信処理部１１１は、第１バスＢ１に接続されたエンジン制御ＥＣＵ１２、ステアリング制御ＥＣＵ１３、ブレーキ制御ＥＣＵ１４、ライト制御ＥＣＵ１５およびエアバッグ制御ＥＣＵ１６と通信する処理を行う。第２通信処理部１１２は、第２バスＢ２に接続された空調制御ＥＣＵ１７、センサＥＣＵ１８および座席制御ＥＣＵ１９と通信する処理を行う。第３通信処理部１１３は、第３バスＢ３に接続された映像処理ＥＣＵ２０および第１外部通信処理部２１と通信する処理を行う。第４通信処理部１１４は、第４バスＢ４に接続された運転支援制御ＥＣＵ２２および第２外部通信処理部２３と通信する処理を行う。第５通信処理部１１５は、診断用通信部１１と通信する処理を行う。

【００２７】

ルーティング処理部１２０は、通信処理部１１０に含まれるいずれかの通信処理部が入力したデータを他の通信処理部に転送し、バスを跨がる通信や診断用通信部１１との間の通信を中継する処理を行う。すなわち、ルーティング処理部１２０は、どのバスから入力したデータをどのバスに出力するか、どのバスに接続されたどのＥＣＵから入力したデータをどのバスに出力するか、どのバスに接続されたどのＥＣＵから入力したデータをどのバスに接続されたどのＥＣＵに出力するかなどを決定する処理を行う。このとき、ルーティング処理部１２０は、バスの規格やプロトコル、データフォーマットが異なる場合は、プロトコル・フォーマットを変換する処理を行う。

【００２８】

ルーティング処理部１２０は、内部にフィルタリング処理部１２１を備える。フィルタリング処理部１２１は、設定されたポリシーに従って、ルーティング処理部１２０に入力されるデータの一部を蓄積制御部１４０に送信する処理を行う。

【００２９】

ルーティング処理部１２０は、上述のように、バスを跨がる通信を中継するため、バスを跨がってＥＣＵ間で送受信されるデータはルーティング処理部１２０に入力される。また、バスを跨がない通信であっても、バス上にブロードキャストされたデータは通信処理部１１０によって受信されるため、ルーティング処理部１２０にそのデータを入力することができる。ここで、車載システム１０を搭載する車両のイグニッションスイッチがオフか、走行中か、停車中か、外部装置と通信を行っているかといったように、車両の状態にも依存するが、車載システム１０においては、多数のＥＣＵから制御コマンドや制御データが出力されるため、ルーティング処理部１２０が受信したり処理したりするデータも膨大な量になる。したがって、ルーティング処理部１２０が受信した全てのデータを蓄積部１３０に蓄積することは現実的ではない。そこで、フィルタリング処理部１２１は、設定されたポリシーに従って、必要なデータのみ蓄積制御部１４０に送信する。

【００３０】

なお、フィルタリング処理部１２１は、予め設定された固定のポリシーに従って蓄積制御部１４０に送信するデータを判定してもよいし、フィルタリング処理部１２１のポリシーを可変とし、蓄積制御部１４０に送信するデータをその都度判定してもよい。また、フィルタリング処理部１２１に設定するポリシーを、蓄積制御部１４０から更新できるように構成されていてもよい。

【００３１】

蓄積部１３０は、車載システム１０に含まれる各ＥＣＵが出力するデータを蓄積する。この蓄積部１３０としては、例えばＮＡＮＤフラッシュメモリやＨＤＤなど、データを記録する媒体を用いることができる。

【００３２】

蓄積制御部１４０は、蓄積部１３０に蓄積するデータと蓄積部１３０から出力するデータとの少なくともいずれかを、所定のルールに従って加工または選別する処理を行う。

【００３３】
本実施形態では、車載システム１０に含まれる各ＥＣＵが出力するデータが蓄積部１３０に蓄積される。この蓄積部１３０に蓄積されたデータの用途は多様である。例えば、車載システム１０を搭載する車両に事故が発生した場合、オペレータ（車両の運転者）のミスによって発生した事故か、ソフトウェアの不具合によって発生した事故かを後から検証するための情報として利用することが考えられる。場合によっては、オペレータのミスによって発生した事故であることを車両の製造ベンダが証明するために、警察や裁判所などの公的機関にデータの提出が必要になる場合も想定される。また、オペレータが急加速や急発進といった事故につながりやすい操作をしていないかどうかをモニタリングし、燃費や安全運転に配慮した操作のアドバイスや保険額の割引など様々なサービスに利用することも考えられる。また、車両の製造ベンダが車載システム１０の実試験を行い、改善に向けた評価を行うための情報として利用することも考えられる。
【００３４】
また、車載システム１０は様々な外部装置と通信することを想定している。したがって、様々な外部装置から攻撃を受ける可能性がある。一般的に、情報通信システムでは、設計者や実装者が意図していない不具合を悪用して攻撃がなされるが、すべての攻撃を事前に予測して、不具合を完全に排除した車載システム１０を設計、実装することは困難である。車載システム１０も不正な命令や不正なデータを排除する機能を備えていることが望ましいが、それらの対策を施していたとしても残念ながら攻撃が成立してしまう場合もある。このとき、仮に車載システム１０の不具合により不正な命令や不正なデータを受け付けてしまったとしても、どのような情報が外部装置から送信されたのか記録できていれば、それを後から解析して不具合の修正に利用することができる。このため、ＥＣＵが出力するデータを車載システム１０内に蓄積しておくことは、事後対応として有用である。
【００３５】
一般的に、車載システム１０に含まれるＥＣＵは様々なものがあり、ＥＣＵやそこに搭載されるソフトウェアによって、車載システム１０の品質や特性が変化する。このため、ＥＣＵが出力するデータには、オペレータにとって利用しやすい車載システム１０を構成するためのノウハウが多々含まれている。したがって、車両の製造ベンダにとって、ＥＣＵが出力するデータを競争相手の製造ベンダに秘匿する必要がある。
【００３６】
また、ＥＣＵが出力するデータ群は上述のように様々な用途が考えられるため、例えば車両の製造ベンダや、警察、裁判所などの公的機関には蓄積部１３０に蓄積したデータをすべて公開し、保険会社には一部のデータを公開し、一般ユーザには最小限のデータを公開するといったように、データの開示範囲を制限する機能を備えておくことが望まれる。
【００３７】
また、車両の製造ベンダがデータを改変していないことを証明するか、車載ゲートウェイ装置１００から出力した後にデータが何者かによって改変されることを防ぐ仕組みを備えている必要がある。
【００３８】
本実施形態の車載ゲートウェイ装置１００は、これらの要求を満足するために、蓄積部１３０へのデータの入力や蓄積部１３０からのデータの出力を制御する蓄積制御部１４０を備える。
【００３９】
蓄積制御部１４０は、記録通信部１４１と、入力制御部１４２と、出力制御部１４３と、蓄積通信部１４４と、を備える。記録通信部１４１は、ルーティング処理部１２０と通信する処理を行う。入力制御部１４２は、蓄積部１３０にデータを入力するときに加工・選別する処理を行う。出力制御部１４３は、蓄積部１３０からデータを出力するときに加工・選別する処理を行う。入力制御部１４２と出力制御部１４３の詳細は後述する。蓄積通信部１４４は、蓄積部１３０にデータを送信したり、蓄積部１３０からデータを受信したりする処理を行う。

【００４０】
なお、ルーティング処理部１２０から蓄積制御部１４０に送信されるデータは、上述したようにフィルタリング処理部１２１によって選別されたデータであるが、蓄積制御部１４０が、どのデータを送信するかをルーティング処理部１２０に指示する構成としてもよい。例えば、蓄積制御部１４０が蓄積部１３０の容量を監視し、一定以上の容量になった場合には蓄積部１３０でデータが溢れることを防ぐため、蓄積部１３０に記録するデータを制限するように、フィルタリング処理部１２１のポリシーの変更をルーティング処理部１２０に依頼してもよい。
【００４１】
ここで、入力制御部１４２の具体例について説明する。図３－１乃至図３－３は、入力制御部１４２の内部構成例を示す図である。入力制御部１４２は、図３－１に示すように、内部に選別処理部２０１を備える構成と、図３－２に示すように、内部に第１暗号処理部２０２および鍵管理部２０３を備える構成と、図３－３に示すように、内部に選別処理部２０１、第１暗号処理部２０２および鍵管理部２０３を備える構成とがある。車載システム１０に要求される性能や蓄積部１３０の容量サイズなどに応じて、最適な構成の入力制御部１４２を選択すればよい。
【００４２】
選別処理部２０１は、ルーティング処理部１２０から入力されたデータに対し、蓄積部１３０に蓄積するデータか否かを判定して、データの加工や選別を行う処理部である。選別処理部２０１は、予め設定された固定のルールに従って、ルーティング処理部１２０から入力されたデータが蓄積部１３０に蓄積するデータか否かを判定してもよいし、選別処理部２０１のルールを可変とし、ルーティング処理部１２０から入力されたデータが蓄積部１３０に蓄積するデータか否かを判定するルールが更新できるようになっていてもよい。
【００４３】
選別処理部２０１が用いるルールの例を以下に挙げる。
【００４４】
ルール１－１：ルーティング処理部１２０から入力されたデータのビットレートに基づき、蓄積部１３０に蓄積するデータか否かを判定する。例えば、選別処理部２０１は、ルーティング処理部１２０から入力されたデータのビットレートを計測し、予め定めた上限を超える場合は、データを間引いて蓄積部１３０に入力するように制御する。
【００４５】
ルール１－２：ルーティング処理部１２０から入力されたデータが、どのバスからのデータであるかによって、蓄積部１３０に蓄積するデータか否かを判定する。例えば、選別処理部２０１は、ルーティング処理部１２０から入力されたデータが第１バスＢ１からのデータであった場合は蓄積部１３０への入力を禁止するが、第２バスＢ２からのデータであった場合は蓄積部１３０への入力を許可するといったように、蓄積部１３０へのデータの入力を制御する。
【００４６】
ルール１－３：ルーティング処理部１２０から入力されたデータの種類に基づき、蓄積部１３０に蓄積するデータか否かを判定する。例えば、選別処理部２０１は、ルーティング処理部１２０から入力されたデータが動画データの場合は蓄積部１３０への入力を禁止するが、テキストデータ（数値データを含む）の場合は蓄積部１３０への入力を許可するといったように、蓄積部１３０へのデータの入力を制御する。他にも、例えば時間情報（時刻情報）は蓄積部１３０への入力を禁止するが、それ以外のデータは蓄積部１３０への入力を許可するといったように、データの種類に応じて蓄積部１３０へのデータの入力を制御する。
【００４７】
ルール１－４：ルーティング処理部１２０から入力されたデータのサイズに基づき、蓄積部１３０に蓄積するデータか否かを判定する。例えば、選別処理部２０１は、ルーティ

ング処理部１２０から入力されたデータのサイズがＮキロバイト以上の場合は蓄積部１３０への入力を禁止するが、それより小さい場合は蓄積部１３０への入力を許可するといったように、蓄積部１３０へのデータの入力を制御する。

【００４８】

ルール１－５：ルーティング処理部１２０から入力されたデータが、どのＥＣＵが出力したデータであるかによって、蓄積部１３０に蓄積するデータか否かを判定する。例えば、選別処理部２０１は、空調制御ＥＣＵ１７が出力したデータは蓄積部１３０への入力を許可するが、エンジン制御ＥＣＵ１２が出力したデータは蓄積部１３０への入力を禁止するといったように、蓄積部１３０へのデータの入力を制御する。

【００４９】

ルール１－６：センサＥＣＵ１８が物理的に異なる複数のＥＣＵを含み、これら複数のＥＣＵが同一のセンサ信号を取得して異なるバスに出力する場合、複数のＥＣＵが出力するデータが一致するか否かにより、蓄積部１３０に蓄積するデータか否かを判定する。例えば、センサ信号に冗長性を持たせるため、センサＥＣＵ１８に含まれる複数のＥＣＵを異なるバスに接続し、これら複数のＥＣＵが同一のセンサ信号を取得して、異なるバスに出力する構成とする場合がある。このような構成の場合、選別処理部２０１は、例えば、それら複数のＥＣＵが出力するデータが一致する間はいずれかのＥＣＵが出力するデータのみ蓄積部１３０に入力し、異なる場合はそれら複数のＥＣＵが出力するデータを蓄積部１３０に入力するといったように、蓄積部１３０へのデータの入力を制御する。これにより、故障あるいは不正アクセスによる問題の発生を検知することができ、原因追及に際して有用である。

【００５０】

ルール１－７：外部装置との間で認証が成功したか否かによって、ルーティング処理部１２０から入力されたデータを蓄積部１３０に蓄積するか否かを判定する。例えば、選別処理部２０１は、外部装置から第１外部通信処理部２１、第２外部通信処理部２３、あるいは診断用通信部１１を経由して、予め設定したパスワード（ＰＩＮコード）と一致する値が送信されてきた場合は、ルーティング処理部１２０から入力されたデータを蓄積部１３０に入力することを許可するが、予め設定したパスワード（ＰＩＮコード）と一致する値が送信されない場合は、ルーティング処理部１２０から入力されたデータを蓄積部１３０に入力することを禁止するといったように、蓄積部１３０へのデータの入力を制御する。

【００５１】

なお、選別処理部２０１は、外部装置との間で認証が成功した場合、ルーティング処理部１２０から入力された全てのデータが蓄積部１３０に入力されるように制御してもよいが、上記のルール１－１からルール１－６のいずれかまたはその組み合わせに従って、蓄積部１３０に入力するデータを選別してもよい。また、外部装置との間の認証方式は、パスワード認証に限らず、ＲＳＡなどの公開鍵アルゴリズムを用いた公開鍵認証でもよい。その場合、選別処理部２０１が秘密鍵を管理する。

【００５２】

上記のルール１－７は、車載システム１０を搭載する車両の製造ベンダがテスト用のデータを収集し、解析する際に極めて有用である。テスト用のデータは、オペレータや保険会社など、通常の利用時には蓄積する必要のない、あるいは取得されたくないデータであるが、製造ベンダにとっては有用なデータである。すなわち、車載システム１０を再設計する際は、各種認定を再度取得するために実機でテストする場合がある。この場合、車載システム１０の各ＥＣＵがテスト用のデータを出力するが、このとき製造ベンダのみが知り得るパスワードや鍵情報を元に認証を行うようにすれば、製造ベンダがテストを行う場合に限り、ＥＣＵが出力するテスト用のデータを蓄積部１３０に蓄積させることができる。

【００５３】

ルール１－８：上記のルール１－１からルール１－７の任意の組み合わせ。

【００５４】
なお、上記のルール１－１からルール１－８で検出した結果に応じて、ＥＣＵが出力するデータを蓄積部１３０に蓄積するか否かについて異なるポリシーを適用し、システム状況に応じたデータの蓄積（ログ蓄積）を行えるようになっていてもよい。例えば、ルール１－６の場合、より多くのログを採取したり、あるいは、故障時の冗長系からのログ採取に切り替えたりしてもよい。
【００５５】
なお、入力制御部１４２は、ルーティング処理部１２０から入力されたデータを蓄積部１３０に入力する場合に、圧縮技術を用いて圧縮形式で蓄積部１３０に入力する構成としてもよい。例えば、同じデータの値が連続して同じ値だった場合に、同じデータを連続回数分送るのではなく圧縮して送る。
【００５６】
また、入力制御部１４２は、ルーティング処理部１２０から入力されたデータを蓄積部１３０に入力する場合に、そのデータに統計処理を施してもよい。例えば、同じＥＣＵからの同種のデータが時間Ｘ、Ｙ、Ｚでルーティング処理部１２０から入力された場合、３つのデータを蓄積部１３０に入力するのではなく、それら３つのデータの平均値を蓄積部１３０に入力してもよい。
【００５７】
また、入力制御部１４２は、ルーティング処理部１２０から入力されたデータを蓄積部１３０に入力する場合に、そのデータに車載システム１０を搭載した車両のオペレータを識別する情報を付与してもよい。オペレータの癖などによって、車両の操作方法が異なる可能性がある。蓄積部１３０に蓄積されたデータを解析する際、どのオペレータが操作したときにＥＣＵが出力したデータであるか区別できれば、燃費や安全運転に配慮した操作のアドバイスや保険額の割引など様々なサービスに利用することができる。オペレータを区別する方法としては、例えば、車内カメラで人物認識する方法、指紋や声紋などの生体情報で識別する、あるいは、運転免許証やクレジットカードなどオペレータを特定する所有物を読み込むリーダで認識する方法などがある。それらカメラやセンサ、カードリーダなどの各種リーダが読み込んだ情報を入力制御部１４２に伝える。
【００５８】
なお、上記のルール１－２やルール１－５に従った判定は、ルーティング処理部１２０のフィルタリング処理部１２１でも行う場合がある。上述のようにバスの規格によってはデータがブロードキャストされる場合がある。そのようなバスの規格では、送り主アドレスと送り先アドレスをフィルタリング処理部１２１で判定できない場合がある。このような場合に備え、本実施形態では、類似の処理をフィルタリング処理部１２１でも入力制御部１４２でも行う構成になっている。
【００５９】
また、以上の例では、蓄積部１３０に蓄積するデータの選別を選別処理部２０１が行う構成であるが、データの選別処理はフィルタリング処理部１２１で行う構成としてもよい。すなわち、選別処理部２０１は、上記のルール１－１からルール１－８のいずれかを保持し、そのルールに従ってフィルタリング処理部１２１のポリシーを設定し、選別処理部２０１が保持するルールに従ってフィルタリング処理部１２１が選別処理を行う構成としてもよい。
【００６０】
第１暗号処理部２０２は、ルーティング処理部１２０から入力されたデータに暗号処理を施す。鍵管理部２０３は、第１暗号処理部２０２が暗号処理に使用する鍵を管理する。なお、暗号アルゴリズムは、ＡＥＳのような共通鍵暗号でもよいし、ＲＳＡや楕円曲線暗号のような公開鍵暗号でもよい。入力制御部１４２が第１暗号処理部２０２と鍵管理部２０３を備える図３－２の構成の場合、蓄積部１３０には、暗号化されたデータが蓄積される。したがって、例えば攻撃者が蓄積部１３０のみを取り外してデータを取得したとしても、攻撃者は平文のデータを取得することはできない。

【００６１】
なお、暗号処理はデータの秘匿化に限らず、メッセージ認証コード（ＭＡＣ：Message Authentication Code）などによる完全性を保証する処理であってもよい。この場合、第１暗号処理部２０２は、例えばＨＭＡＣなどのアルゴリズムを用い、データにＭＡＣ値を付けて蓄積部１３０に入力する。さらに、暗号処理は署名を付与する処理であってもよい。この場合、第１暗号処理部２０２は、例えばＲＳＡのような公開鍵暗号を用いてデータに対する署名値を生成し、データに署名値を付けて蓄積部１３０に蓄積する。もちろんデータサイズが大きい場合は、例えばＳＨＡ－１などのハッシュアルゴリズムを用いてハッシュ値を計算し、そのハッシュ値に対する署名値を計算してもよい。
【００６２】
図３－３に示すように、内部に選別処理部２０１、第１暗号処理部２０２および鍵管理部２０３を備える構成の入力制御部１４２では、第１暗号処理部２０２がどのデータを暗号化するかが選別処理部２０１により選定される。この場合、ルーティング処理部１２０から入力されたデータは、選別処理部２０１によって、蓄積部１３０に蓄積しないか、第１暗号処理部２０２により暗号処理を施して蓄積部１３０に蓄積するか、平文のまま蓄積部１３０に蓄積するか判定される。選別処理部２０１による判定処理は、例えば、上述したルール１－１からルール１－８のいずれかに従って行うことができる。
【００６３】
なお、蓄積部１３０に蓄積するデータに対して第１暗号処理部２０２が暗号処理を行う場合は、データの出力先に応じて異なる鍵を用いた暗号処理を行うようにしてもよい。すなわち、暗号処理に用いる鍵を分けることによって、例えば、製造ベンダと公的機関のみが全てのデータを復号でき、保険会社は特定のデータのみを復号できるといったように、アクセス可能な対象者を区別するようにしてもよい。同様に、データの出力先に応じて異なる暗号アルゴリズムを用いた暗号処理を行うようにしてもよい。
【００６４】
次に、出力制御部１４３の具体例について説明する。図４－１乃至図４－６は、出力制御部１４３の内部構成例を示す図である。出力制御部１４３は、図４－１に示すように、内部にアクセス制御部３０１を備える構成と、図４－２に示すように、内部にアクセス制御部３０１、モード設定部３０２および認証処理部３０３を備える構成と、図４－３に示すように、内部に第２暗号処理部３０４および第２鍵管理部３０５を備える構成と、図４－４に示すように、内部にアクセス制御部３０１、第３暗号処理部３０６および第３鍵管理部３０７を備える構成と、図４－５に示すように、内部にアクセス制御部３０１および第３暗号処理部３０６を備える構成と、図４－６に示すように、内部にアクセス制御部３０１、第２暗号処理部３０４および第２鍵管理部３０５を備える構成とがある。車載システム１０に要求される性能やセキュリティレベルなどに応じて、最適な構成の出力制御部１４３を選択すればよい。
【００６５】
アクセス制御部３０１は、蓄積部１３０からの出力が要求されたデータに対し、出力できるデータか否かを判定して、出力するデータの加工や選別を行う処理部である。アクセス制御部３０１は、予め設定された固定のルールに従って、出力が要求されたデータが出力できるデータか否かを判定してもよいし、アクセス制御部３０１のルールを可変とし、出力が要求されたデータが出力できるデータか否かを判定するルールが更新できるようになっていてもよい。
【００６６】
アクセス制御部３０１が用いるルールの例を以下に挙げる。
【００６７】
ルール２－１：出力が要求されたデータをルーティング処理部１２０に送信する際のビットレートに基づき、出力できるデータか否かを判定する。例えば、アクセス制御部３０１は、出力が要求されたデータのビットレートを計測し、予め定めた上限を超える場合は、データを間引いてルーティング処理部１２０に送信するように制御する。

【００６８】
ルール２－２：出力が要求されたデータの出力先に応じて、出力できるデータか否かを判定する。例えば、アクセス制御部３０１は、出力が要求されたデータが診断用通信部１１から外部機器に送信される場合は出力を禁止するが、第２外部通信処理部２３から外部機器に送信される場合は出力を許可するといったように、蓄積部１３０に蓄積されたデータの出力を制御する。
【００６９】
ルール２－３：出力が要求されたデータの種類に基づき、出力できるデータか否かを判定する。例えば、アクセス制御部３０１は、出力が要求されたデータが動画データの場合は出力を禁止するが、テキストデータ（数値データを含む）の場合は出力を許可するといったように、蓄積部１３０に蓄積されたデータの出力を制御する。他にも、例えば時間情報（時刻情報）は出力を禁止するが、それ以外のデータは出力を許可するといったように、データの種類に応じて蓄積部１３０に蓄積されたデータの出力を制御する。
【００７０】
ルール２－４：出力が要求されたデータのサイズに基づき、出力できるデータか否かを判定する。例えば、アクセス制御部３０１は、出力が要求されたデータのサイズがＮキロバイト以上の場合は出力を禁止するが、それより小さい場合は出力を許可するといったように、蓄積部１３０に蓄積されたデータの出力を制御する。
【００７１】
ルール２－５：出力が要求されたデータが、どのＥＣＵが出力したデータであるかによって、出力できるデータか否かを判定する。例えば、アクセス制御部３０１は、出力が要求されたデータが空調制御ＥＣＵ１７が出力したデータであれば出力を許可するが、エンジン制御ＥＣＵ１２が出力したデータであれば出力を禁止するといったように、蓄積部１３０に蓄積されたデータの出力を制御する。なお、この場合、データを蓄積部１３０に蓄積する際に、入力制御部１４２がどのＥＣＵから入力したデータであるかを示す情報を付与して蓄積するようにしてもよい。
【００７２】
ルール２－６：センサＥＣＵ１８が物理的に異なる複数のＥＣＵを含み、これら複数のＥＣＵが同一のセンサ信号を取得して異なるバスに出力する構成において、複数のＥＣＵが同一のセンサ信号を取得して出力したデータが蓄積部１３０に蓄積されている場合、これら複数のＥＣＵが出力したデータが一致するか否かにより、出力できるデータか否かを判定する。例えば、アクセス制御部３０１は、複数のＥＣＵが出力したデータが異なる場合は攻撃やエラーの解析のため出力を許可し、一致する場合は出力を禁止するといったように、蓄積部１３０に蓄積されたデータの出力を制御する。なお、この場合、データを蓄積部１３０に蓄積する際に、入力制御部１４２が同一のセンサから入力したデータであることを示す情報を付与して蓄積するようにしてもよい。
【００７３】
ルール２－７：外部装置との間で認証が成功したか否かによって、出力が要求されたデータを出力するか否かを判定する。例えば、アクセス制御部３０１は、外部装置から第１外部通信処理部２１、第２外部通信処理部２３、あるいは診断用通信部１１を経由して、予め設定したパスワード（ＰＩＮコード）と一致する値が送信されてきた場合は、出力が要求されたデータの出力を許可するが、予め設定したパスワード（ＰＩＮコード）と一致する値が送信されない場合は、出力が要求されたデータの出力を禁止するといったように、蓄積部１３０に蓄積されたデータの出力を制御する。
【００７４】
なお、アクセス制御部３０１は、外部装置との間で認証が成功した場合、出力が要求された全てのデータの出力を許可してもよいが、上記のルール２－１からルール２－６のいずれかまたは組み合わせに従って、出力を許可するデータを選別してもよい。また、外部装置との間の認証方式は、パスワード認証に限らず、ＲＳＡなどの公開鍵アルゴリズムを用いた公開鍵認証でもよい。その場合、アクセス制御部３０１が秘密鍵を管理する。

【００７５】
ルール２－８：上記のルール２－１からルール２－７の任意の組み合わせ。
【００７６】
なお、出力制御部１４３は、蓄積部１３０に蓄積されたデータが圧縮技術によって圧縮されている場合、そのデータに対して伸長処理を施す。
【００７７】
また、出力制御部１４３は、蓄積部１３０に蓄積されたデータに対して統計処理を施して出力してもよい。例えば、同じＥＣＵからの同種のデータが時間Ｘ、Ｙ、Ｚで蓄積部１３０に記録されている場合、３つのデータを出力するのではなく、それら３つのデータの平均値を出力してもよい。
【００７８】
モード設定部３０２は、アクセス制御部３０１の動作を有効にするか無効にするか設定する処理を行う。モード設定部３０２によりアクセス制御部３０１が有効に設定されていれば、アクセス制御部３０１によって上記のルール２－１からルール２－８のいずれかに従ったデータの選別や加工が行われる。一方、アクセス制御部３０１が無効に設定されている場合は、出力が要求されたデータが蓄積部１３０からそのまま出力される。
【００７９】
認証処理部３０３は、モード設定部３０２の動作を制限するための認証処理を行う。すなわち、認証処理部３０３が認証成功としたときのみ、モード設定部３０２がアクセス制御部３０１を有効にしたり無効にしたり設定できる。これにより、パスワードや秘密鍵の値を知らない攻撃者によって不正にアクセス制御部３０１の設定が変更されることを防止できる。認証の方式としては、例えば、認証処理部３０３に予め設定されたパスワード（ＰＩＮコード）を用いる方法（パスワード認証）、ＲＳＡや楕円曲線暗号などの公開鍵アルゴリズムを用いて公開鍵認証を用いる方法などがある。
【００８０】
なお、モード設定部３０２は、アクセス制御部３０１の動作を有効にするか無効にするかの設定だけでなく、アクセス制御部３０１が用いるルールを変更する設定を行ってもよい。例えば、アクセス制御部３０１にルール２－１が適用されている場合、認証処理部３０３による認証が成功すると、モード設定部３０２は、アクセス制御部３０１にルール２－２を適用するように設定する構成としてもよい。
【００８１】
第２暗号処理部３０４は、蓄積部１３０からの出力が要求されたデータに暗号処理を施す。第２鍵管理部３０５は、第２暗号処理部３０４が暗号処理に使用する鍵を管理する。なお、暗号アルゴリズムは、ＡＥＳのような共通鍵暗号でもよいし、ＲＳＡや楕円曲線暗号のような公開鍵暗号でもよい。出力制御部１４３が第２暗号処理部３０４と第２鍵管理部３０５を備える図４－３の構成の場合、蓄積部１３０から出力されるデータは暗号化される。そして、共通鍵の場合は第２鍵管理部３０５が管理する鍵と同じ値を、公開鍵の場合は第２鍵管理部３０５の公開鍵に対応する秘密鍵の値を持っている場合に限り、蓄積部１３０から出力されたデータを平文に復号することができる。したがって、鍵の値を知らない攻撃者は暗号化されたデータを復号することができないため、蓄積部１３０のデータが平文で攻撃者に取得されることを防止できる。
【００８２】
なお、暗号処理はデータの秘匿化に限らず、メッセージ認証コード（ＭＡＣ）などによる完全性を保証する処理であってもよい。この場合、第２暗号処理部３０４は、例えばＨＭＡＣなどのアルゴリズムを用い、蓄積部１３０から出力されるデータにＭＡＣ値を付ける。さらに、暗号処理は署名を付与する処理であってもよい。この場合、第２暗号処理部３０４は、例えばＲＳＡのような公開鍵暗号を用いてデータに対する署名値を生成し、蓄積部１３０から出力されるデータに署名値を付ける。もちろんデータサイズが大きい場合は、例えばＳＨＡ－１などのハッシュアルゴリズムを用いてハッシュ値を計算し、そのハッシュ値に対する署名値を計算してもよい。

【００８３】
図４－６に示すように、内部にアクセス制御部３０１、第２暗号処理部３０４および第２鍵管理部３０５を備える構成の出力制御部１４３では、蓄積部１３０に平文で蓄積されているデータのうち、第２暗号処理部３０４がどのデータを暗号化するかがアクセス制御部３０１により選定される。この場合、蓄積部１３０から出力されるデータは、アクセス制御部３０１によって、第２暗号処理部３０４により暗号処理を施して出力するか、平文のまま出力するかが判定される。アクセス制御部３０１による判定処理は、例えば、上述したルール２－１からルール２－８のいずれかに従って行うことができる。
【００８４】
なお、蓄積部１３０から出力するデータに対して第２暗号処理部３０４が暗号処理を行う場合は、データの出力先に応じて異なる鍵を用いた暗号処理を行うようにしてもよい。すなわち、暗号処理に用いる鍵を分けることによって、例えば、製造ベンダと公的機関のみが全てのデータを復号でき、保険会社は特定のデータのみを復号できるといったように、アクセス可能な対象者を区別するようにしてもよい。
【００８５】
第３暗号処理部３０６は、蓄積部１３０に蓄積されたデータが入力制御部１４２の第１暗号処理部２０２により暗号化されている場合に、蓄積部１３０から出力するデータに対して復号処理を施す。第３鍵管理部３０７は、第３暗号処理部３０６が使用する鍵を管理する。第１暗号処理部２０２で暗号化されたデータが蓄積部１３０に蓄積されている場合、蓄積部１３０に蓄積されているデータのうち、どのデータを第３暗号処理部３０６で復号するかがアクセス制御部３０１により選定される。すなわち、蓄積部１３０から出力されるデータは、アクセス制御部３０１によって、第３暗号処理部３０６により復号して平文として出力するか、暗号文のまま出力するかが判定される。アクセス制御部３０１による判定処理は、例えば、上述したルール２－１からルール２－８のいずれかに従って行うことができる。
【００８６】
なお、共通鍵暗号が用いられている場合は、入力制御部１４２の鍵管理部２０３に格納された値と同じ値を第３鍵管理部３０７に格納してもよいし、図４－５に示す構成のように、出力制御部１４３内部に第３鍵管理部３０７を設けずに、第３暗号処理部３０６が入力制御部１４２の鍵管理部２０３から鍵を取得してもよい。
【００８７】
蓄積部１３０に蓄積されたデータの出力を要求する方法としては、車載システム１０に含まれるＥＣＵが出力要求メッセージを送信する方法、外部装置が診断用通信部１１、第１外部通信処理部２１、第２外部通信処理部２３のいずれかを介して出力要求メッセージを送信する方法などがある。また、蓄積部１３０に蓄積されたデータの出力先としては、内部のバスを経由してＥＣＵに出力する、診断用通信部１１、第１外部通信処理部２１、第２外部通信処理部２３のいずれかを介して外部装置に出力するなどがある。外部装置へ出力する場合は有線の場合もあるし、無線の場合もある。蓄積部１３０に蓄積されたデータの出力を要求する出力要求メッセージに、出力先を指定する情報を付与してもよいし、車載ゲートウェイ装置１００に予め出力先が指定されていてもよい。出力先を指定する情報として、バスを指定する方法、ＥＣＵを指定する方法、診断用通信部１１を指定する方法などがある。
【００８８】
なお、いずれの認証または暗号化を施す場合も、どのバスまたはどのＥＣＵからの要求であるかをアクセス制御部３０１が判定する処理を行い、バスまたはＥＣＵによってアクセス制御部３０１の動作を変更できるようになっていてもよい。例えば、ルーティング処理部１２０を介して第１バスＢ１からアクセス制御部３０１の動作を変更する場合にはモード設定部３０２は無効になり、アクセス制御部３０１の動作を有効にしたり無効にしたり設定できるが、診断用通信部１１からアクセス制御部３０１の動作を変更する場合にはモード設定部３０２が有効となり、認証処理部３０３との認証が成功しない限りアクセス

制御部３０１の設定を変更できないといった構成になっていてもよい。同様に、ルーティング処理部１２０を介して第１バスＢ１から蓄積部１３０に蓄積されたデータの出力が要求された場合にはデータは平文のまま出力されるが、診断用通信部１１から蓄積部１３０に蓄積されたデータの出力が要求された場合には、データは第２暗号処理部３０４によって暗号化されて出力されるといった構成になっていてもよい。

【００８９】

なお、以上の例では、蓄積部１３０にデータを入力するときに入力制御部１４２がデータの加工・選別を行うとともに、蓄積部１３０からデータを出力するときに出力制御部１４３がデータの加工・選別を行うようにしているが、データの加工・選別は、蓄積部１３０にデータを入力するとき、あるいは、蓄積部１３０からデータを出力するときのいずれかのみ行う構成としてもよい。

【００９０】

以上、具体的な例を挙げながら詳細に説明したように、本実施形態の車載ゲートウェイ装置１００は、ＥＣＵが出力するデータを蓄積部１３０に蓄積し、蓄積部１３０に蓄積したデータを出力する際に、所定のルールに従ってデータを加工または選別するようにしている。したがって、この車載ゲートウェイ装置１００によれば、蓄積部１３０に蓄積するデータを保護しながら、データの用途に応じてその出力を制限することができる。これにより、蓄積部１３０に蓄積するデータが悪意の第３者に取得されたり、蓄積部１３０に蓄積するデータを不用意に開示してしまったりする不都合を有効に抑制することができる。

【００９１】

また、本実施形態によれば、蓄積部１３０に蓄積するデータを加工または選別することにより、蓄積部１３０のデータあふれを抑制することができるとともに、蓄積部１３０のバス幅を小さくすることができるため、蓄積部１３０のコストを削減することができる。

【００９２】

なお、図１に示した車載システム１０の構成では、映像処理ＥＣＵ２０と運転支援制御ＥＣＵ２２が外部と通信するために、それぞれ別々の通信処理部（第１外部通信処理部２１および第２外部通信処理部２３）と接続されている。しかし、外部と通信するための通信処理部をひとつにまとめた構成としてもよい。その場合の車載システム１０の構成例を図５に示す。

【００９３】

図５に示す車載システム１０は、図１の第１外部通信処理部２１と第２外部通信処理部２３との代わりに、車載ゲートウェイ装置１００に接続された第３外部通信処理部２４を備えている。第３外部通信処理部２４は、例えば、３ＧＰＰ（登録商標）やＬＴＥ（登録商標）などの移動体通信網や、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、８０２．１１ｐなどの無線を用いて、インターネット、路側機や他の外部装置と通信する処理を行う。

【００９４】

図１に示した構成の車載システム１０では、映像処理ＥＣＵ２０は車載ゲートウェイ装置１００を介さず直接、第１外部通信処理部２１を用いて外部と通信していた。同様に、運転支援制御ＥＣＵ２２も車載ゲートウェイ装置１００を介さず直接、第２外部通信処理部２３を用いて外部と通信していた。しかし、図５に示す構成の車載システム１０では、映像処理ＥＣＵ２０や運転支援制御ＥＣＵ２２は、第３外部通信処理部２４を用いて外部と通信するために車載ゲートウェイ装置１００を介す必要がある。その場合の車載ゲートウェイ装置１００の構成例を図６に示す。

【００９５】

図６に示す車載ゲートウェイ装置１００は、図２に示す構成と比較して、通信処理部１１０に第６通信処理部１１６が追加で含まれている点のみが異なる。第６通信処理部１１６は、第３外部通信処理部２４と通信する処理を行う。映像処理ＥＣＵ２０が第３外部通信処理部２４を用いて外部と通信する場合は、映像処理ＥＣＵ２０と第３外部通信処理部２４は、第３通信処理部１１３、ルーティング処理部１２０および第６通信処理部１１６

を介して接続される。また、運転支援制御ＥＣＵ２２が第３外部通信処理部２４を用いて外部と通信する場合は、運転支援制御ＥＣＵ２２と第３外部通信処理部２４は、第４通信処理部１１４、ルーティング処理部１２０および第６通信処理部１１６を介して接続される。

【００９６】

また、図２に示した車載ゲートウェイ装置１００の構成では、ルーティング処理部１２０と蓄積制御部１４０はそれぞれ個別に設けられている。しかし、ルーティング処理部１２０内に蓄積制御部１４０を組み込んだ構成とすることも可能である。その場合の車載ゲートウェイ装置１００の構成例を図７に示す。

【００９７】

図７に示す車載ゲートウェイ装置１００では、蓄積制御部１４０がルーティング処理部１２０内に組み込まれている。このため、蓄積制御部１４０に記録通信部１４１は設けられていない。

【００９８】

図２に示した構成の車載ゲートウェイ装置１００では、ルーティング処理部１２０が、設定されたポリシーに従って必要なデータのみ蓄積制御部１４０に送信する処理を行っていた。これに対し、図７に示す構成の車載ゲートウェイ装置１００では、蓄積制御部１４０の入力制御部１４２がこの処理を行う。すなわち、入力制御部１４２は、ルーティング処理部１２０に設定されたポリシーに従ってルーティング処理部１２０に入力されたデータの選別を行うとともに、上述したルール１－１からルール１－８のいずれかに従って、蓄積部１３０に蓄積するデータの加工・選別を行う。

【００９９】

また、図２に示した構成の車載ゲートウェイ装置１００では、蓄積部１３０から出力するデータを出力制御部１４３が加工・選別し、記録通信部１４１からルーティング処理部１２０に送信していた。これに対し、図７に示す構成の車載ゲートウェイ装置１００では、蓄積制御部１４０がルーティング処理部１２０に組み込まれているため、出力制御部１４３は、加工・選別したデータを直接ルーティング処理部１２０に受け渡す処理を行う。ルーティング処理部１２０は、そのデータを第１バスＢ１、第２バスＢ２、第３バスＢ３、第４バスＢ４、または診断用通信部１１に転送する処理を行う。

【０１００】

＜第２実施形態＞

次に、第２実施形態について説明する。第１実施形態では、車載システム１０に含まれるＥＣＵが出力するデータを蓄積部１３０に格納していた。これに対し第２実施形態では、ＥＣＵから出力されたデータに加え、ＥＣＵのファームウェアに関する情報をシステム情報として蓄積する点が、第１実施形態と異なる。以下、第１実施形態との相違点についてのみ説明する。

【０１０１】

一般的に、車載システム１０には数多くの様々な種類のＥＣＵが搭載されている。図１では、それら多数のＥＣＵの一例としてエンジン制御ＥＣＵ１２などを例示したが、これら以外にも様々なＥＣＵが搭載されている。車載システム１０は、複数の異なるベンダが提供するＥＣＵを搭載していることが一般的である。それらのＥＣＵの中には、ハードウェアのみで実現されているものと、ハードウェアとソフトウェア（ファームウェア）で構成されているものがある。ハードウェアとファームウェアで構成されているもののうち、ファームウェアが工場出荷時に組み込まれ、工場出荷後に更新（アップデート）することができないようになっているものもあるが、ファームウェアをＥＣＵ単体で工場から出荷後、あるいは車載システム１０としてアセンブルされた後に、機能追加、性能向上、不具合の改善などを目的として、後から新しいファームウェアにアップデートする機能を備えているものもある。

【０１０２】

このとき課題となるのが、ファームウェアの更新である。パーソナルコンピュータ（Ｐ

Ｃ）を中心としたＩＴシステムの場合、各ＰＣが常時インターネットに接続されている場合が多いため、各ＰＣは最新のファームウェアがサーバ上で配布されているか定期的に確認し、ファームウェアが提供されたと同時に更新することが可能である。

【０１０３】

しかし、車載システム１０はファームウェアを配布するサーバとネットワークで常時接続されているわけではない。例えば、車載システム１０を搭載した車両がトンネルや地下道路を走行中の場合、外部装置と通信できない場合もあるし、車両を週末のみ利用する（イグニッションをオンにする）といったこともあり得る。したがって、必ずしもすべての車載システム１０がすべてのＥＣＵに対して最新のファームウェアを取得し、インストールしているとは限らない。また、ＥＣＵの故障により、同一種類の車載システム１０であってもあるＥＣＵは最新のファームウェアがインストールされているが、別のＥＣＵは古いファームウェアがインストールされているという状況もあり得る。

【０１０４】

さらに、上述のようにＥＣＵを提供するベンダは異なり、各ＥＣＵの機能はそれぞれ異なるため、ＥＣＵごとに個別にアップデートされていくことが見込まれる。したがって、仮に同じベンダが提供する同じ種類の車載システム１０だとしても、ＥＣＵのファームウェアのバージョンの組み合わせは相当な数にのぼる。例えば、あるＥＣＵのバージョンがＸであり、別のＥＣＵのバージョンがＹの場合にのみ不具合が発生するといったように、特定のファームウェアのバージョンの組み合わせで不具合が発生する場合も考えらえる。

【０１０５】

また、セキュリティの観点からは、車載システム１０のシステム構成によって攻撃の成否が異なり、特定のファームウェアの組み合わせで特定の攻撃が成立する場合もある。このように、車載システム１０のシステム構成は、不具合や攻撃などの問題解決を進める上で、重要な手掛かりとなり得る。仮に事故が発生した場合、どのような不具合で生じたのかどうかを車両の製造ベンダが確認したり解析したりする作業が必要になるが、ファームウェアの組み合わせが分からなければ究明に多大なコストがかかる。

【０１０６】

以上のことから、車両の製造ベンダが、ＥＣＵが出力したデータとともに各ＥＣＵのファームウェアの状態を把握することができれば、再現も容易になるため、原因を究明するための解析が容易になると考えらえる。さらに、外部から有効な攻撃が発生しているか否かを車両の製造ベンダが事後的に効率よく解析するために、車載システム１０内にシステム構成に関する情報を蓄積しておく必要があるが、蓄積すべきデータの種類・管理方法、出力方法が明らかになっていない。

【０１０７】

本実施形態では、車載ゲートウェイ装置１００が、ＥＣＵが出力するデータに加えて、ＥＣＵのファームウェアに関する情報をシステム情報として蓄積し、データの解析を行う場合に各ＥＣＵのファームウェアの状態を把握できるようにすることで、データの解析を容易かつ効率よく行えるようにする。

【０１０８】

図８は、本実施形態の車載ゲートウェイ装置１００の機能的な構成例を示すブロック図である。図２に示した第１実施形態の構成と比較して、システム情報取得部１５０が追加されている点と、蓄積部１３０がログ蓄積部１３１とシステム情報蓄積部１３２とを備える点が異なる。

【０１０９】

システム情報取得部１５０は、車載システム１０に含まれる各ＥＣＵのファームウェアに関する情報を取得する処理を行う。ＥＣＵのファームウェアに関する情報とは、ファームウェアのバージョン情報であってもよいし、ファームウェアのハッシュ値であってもよい。また、ＥＣＵのファームウェアに関する情報は、日付などのファームウェアのメタデータ、ファームウェアのサイズ、ファームウェアに添付されている署名、ファームウェアを提供するベンダに関する情報などを含んでいてもよい。また、ファームウェアに関する

情報は、動作中のＲＡＭイメージに関する情報であってもよい。

【０１１０】

システム情報取得部１５０は、取得したＥＣＵのファームウェアに関する情報を、蓄積部１３０に送信する。システム情報取得部１５０がＥＣＵのファームウェアに関する情報を取得するタイミングとしては、各ＥＣＵから定期的に取得する方法、車両のイグニッションがオンしたときに取得する方法、外部装置からの指示に応じて取得する方法、ＥＣＵの故障など異常を検出したときに取得する方法、特定のＥＣＵからの指示に応じて収集する方法などがある。特定のＥＣＵからの指示とは、例えば、エアバッグ制御ＥＣＵ１６が車載システム１０の衝突などのイベントを検出したときにシステム情報取得部１５０に指示を送信する場合などを指す。また、ＥＣＵのファームウェアに関する情報が更新された場合には、更新前のファームウェアに関する情報を上書きしてもよいし、更新前の情報を消さずに履歴として残しておき、追記してもよい。

【０１１１】

本実施形態の車載ゲートウェイ装置１００では、蓄積部１３０が、ログ蓄積部１３１とシステム情報蓄積部１３２とから構成される。ログ蓄積部１３１は、第１実施形態における蓄積部１３０と同一の機能を持つ。すなわち、ログ蓄積部１３１は、ＥＣＵが出力するデータであって、蓄積制御部１４０の入力制御部１４２により加工・選別されたデータを蓄積する。一方、システム情報蓄積部１３２は、システム情報取得部１５０が取得したＥＣＵのファームウェアに関する情報をシステム情報として蓄積する。

【０１１２】

第１の実施形態では、ＥＣＵが出力するデータを入力制御部１４２により加工・選別して蓄積部１３０に蓄積する仕組みを説明したが、ＥＣＵのファームウェアに関する情報についても同様に、加工・選別してシステム情報蓄積部１３２に蓄積する構成としてもよい。例えば、入力制御部１４２の選別処理部２０１が、システム情報取得部１５０が取得したＥＣＵのファームウェアに関する情報について、どのバスに出力するか、どのバスから入力されたか、どのＥＣＵから取得されたかなどによって、システム情報蓄積部１３２に蓄積すべきか否かを判定し、蓄積すべきと判定したもののみ蓄積するようにしてもよい。また、この判定は、ＥＣＵが出力するデータと独立に行ってもよい。すなわち、あるＥＣＵが出力するデータはログ蓄積部１３１に蓄積することを禁止するが、そのＥＣＵのファームウェアに関する情報はシステム情報蓄積部１３２に蓄積することを許可するといった判定を行ってもよい。

【０１１３】

同様に、あるＥＣＵが出力するデータを第１暗号処理部２０２により暗号化するか否かと、そのＥＣＵのファームウェアに関する情報を第１暗号処理部２０２により暗号化するか否かを別々に決めてもよい。また、双方を暗号化する場合は別々の鍵で暗号化するように、複数の鍵を鍵管理部２０３が管理するように構成してもよい。

【０１１４】

また、第１の実施形態では、蓄積部１３０から出力するデータを出力制御部１４３により加工・選別する仕組みを説明したが、ＥＣＵのファームウェアに関する情報についても同様に、システム情報蓄積部１３２から出力するデータを加工・選別する構成としてもよい。例えば、出力制御部１４３のアクセス制御部３０１が、システム情報蓄積部１３２からの出力が要求されたファームウェアに関する情報について、どのバスに出力するか、どのバスから入力されたか、どのＥＣＵから取得されたかなどによって、出力を許可するか否かを判定し、出力を許可すると判定したもののみ出力するようにしてもよい。また、この判定は、ＥＣＵが出力するデータと独立に行ってもよい。すなわち、あるＥＣＵが出力するデータはログ蓄積部１３１から出力することを禁止するが、そのＥＣＵのファームウェアに関する情報はシステム情報蓄積部１３２から出力することを許可するといった判定を行ってもよい。

【０１１５】

同様に、あるＥＣＵが出力するデータと、そのＥＣＵのファームウェアに関する情報に

ついて、第２暗号処理部３０４により暗号化するか否か、第３暗号処理部３０６により復号するか否かなども別々に決めてもよい。また、双方を暗号化、復号する場合は別々の鍵で暗号化するように、複数の鍵を第２鍵管理部３０５や第３鍵管理部３０７が管理するように構成してもよい。さらに、モード設定部３０２の設定についても、あるＥＣＵが出力するデータと、そのＥＣＵのファームウェアに関する情報とで別々に行ってもよい。

【０１１６】

以上のように、本実施形態の車載ゲートウェイ装置１００は、ＥＣＵが出力するデータをログ蓄積部１３１に蓄積するとともに、ＥＣＵのファームウェアに関する情報をシステム情報蓄積部１３２に蓄積する。したがって、例えば車両の製造ベンダがＥＣＵが出力したデータを解析する際に、ＥＣＵのファームウェアに関する情報も取得して解析を行うことができ、データの解析を容易かつ効率よく行うことができる。

【０１１７】

なお、図８に示した車載ゲートウェイ装置１００の構成では、システム情報取得部１５０がルーティング処理部１２０と接続されていたが、システム情報取得部１５０を蓄積制御部１４０内に組み込んだ構成としてもよい。その場合の車載ゲートウェイ装置１００の構成例を図９に示す。

【０１１８】

図９に示す車載ゲートウェイ装置１００では、システム情報取得部１５０が蓄積制御部１４０内に組み込まれている。この構成の場合、システム情報取得部１５０が取得したＥＣＵのファームウェアに関する情報は、記録通信部１４１、入力制御部１４２、蓄積通信部１４４を介して蓄積部１３０に送信され、システム情報蓄積部１３２に蓄積される。

【０１１９】

また、システム情報取得部１５０をルーティング処理部１２０内に組み込んだ構成とすることも可能である。その場合の車載ゲートウェイ装置１００の構成例を図１０に示す。

【０１２０】

図１０に示す車載ゲートウェイ装置１００では、システム情報取得部１５０がルーティング制御部１２０内に組み込まれている。この構成の場合、ＥＣＵのファームウェアをアップデートするために車載システム１０が取得した新しいファームウェアをルーティング処理部１２０が転送する際に、システム情報取得部１５０がそのファームウェアに関する情報を取得することができる。

【０１２１】

車載システム１０が新しいファームウェアを取得するトリガとしては、修理業者やメンテナンス業者が専用装置を用いてインストール指示を各ＥＣＵに送信する方法、車載システム１０が定期的に外部と通信し、更新すべきファームウェアの有無を確認する方法、車両のオペレータがスマートフォンなどの端末を利用し、無線ネットワークなどを通じて車載システム１０と通信してファームウェアを送信する方法、車両のオペレータが端末を利用して車載システム１０と通信し、車載システム１０にアップデートサーバと通信して最新のファームウェアがないか確認を促す方法などがある。

【０１２２】

新しいファームウェアを取得する経路は車載システム１０によって異なるが、図１に示した第１外部通信処理部２１もしくは第２外部通信処理部２３を経由する方法、図５に示した第３外部通信処理部２４を経由する方法、診断用通信部１１を経由する方法がある。いずれの入手経路でも、各ＥＣＵにファームウェアをインストールするには、車載ゲートウェイ装置１００のルーティング処理部１２０を介す必要がある。例えば、ファームウェアを第３外部通信処理部２４から入手してエンジン制御ＥＣＵ１２にインストールする場合、外部装置と第３外部通信処理部２４が通信を確立し、ファームウェアを取得し、ルーティング処理部１２０を介してエンジン制御ＥＣＵ１２に転送する。そして、エンジン制御ＥＣＵ１２が、受信したファームウェアをインストールするといった手順でＥＣＵのファームウェアの更新がなされる。

【０１２３】

図１０に示す構成の車載ゲートウェイ装置１００では、システム情報取得部１５０は、ルーティング処理部１２０で転送される情報を監視し、転送される情報がＥＣＵのファームウェアであった場合には、そのファームウェアに関する情報を取得する。

【０１２４】

なお、図８や図９に示す構成の車載ゲートウェイ装置１００では、システム情報取得部１５０は、能動的にＥＣＵに対してファームウェアに関する情報を問い合わせることにより、システム情報蓄積部１３２に蓄積するＥＣＵのファームウェアに関する情報を取得する。これは、ルーティング処理部１２０を介さずにＥＣＵのファームウェアが更新される場合に特に有用である。例えば、ＥＣＵを物理的に交換した場合などがこれに該当する。すなわち、ＥＣＵが故障した場合などは、最新のファームウェアがインストールされたＥＣＵを物理的に交換する可能性がある。このとき、ファームウェアはルーティング処理部１２０で転送されないため、システム情報取得部１５０が能動的にＥＣＵのファームウェアに関する情報を取得する方法が有用である。

【０１２５】

図１０に示す構成の車載ゲートウェイ装置１００においても、システム情報取得部１５０が、ルーティング処理部１２０で転送される情報を監視してＥＣＵのファームウェアに関する情報を取得することに加えて、能動的にＥＣＵのファームウェアに関する情報を取得するように構成してもよい。

【０１２６】

なお、ＥＣＵのファームウェアには、ＥＣＵに関する仕様やＥＣＵの効率的な利用方法など、ＥＣＵを提供するベンダのノウハウや秘密情報が含まれている場合がある。これらノウハウや情報を盗聴や改変による攻撃から保護するために、外部装置から配信されるＥＣＵのファームウェアは暗号化されている場合がある。ＥＣＵのファームウェアが暗号化されている場合に対応した車載ゲートウェイ装置１００の構成例を図１１に示す。

【０１２７】

図１１に示す車載ゲートウェイ装置１００では、ルーティング処理部１２０内に、システム情報取得部１５０に加えて、復号処理部１５１と第４鍵管理部１５２とが組み込まれている。復号処理部１５１は、暗号化されたＥＣＵのファームウェアを復号する処理を行う。第４鍵管理部１５２は、復号処理部１５１が使用する鍵を管理する。なお、暗号アルゴリズムはＡＥＳのような共通鍵暗号でもよいし、ＲＳＡや楕円曲線暗号のような公開鍵暗号でもよい。

【０１２８】

この構成の場合、外部装置から第１外部通信処理部２１、第２外部通信処理部２３、第３外部通信処理部２４、診断用通信部１１のいずれかを経由して取得した暗号化されたＥＣＵのファームウェアは、ルーティング処理部１２０において復号処理部１５１で復号された後、ターゲットとなるＥＣＵに転送される。ターゲットとなるＥＣＵは、平文となったファームウェアをインストールし、ファームウェアを更新する。

【０１２９】

本例は、正当なファームウェアは第４鍵管理部１５２で管理される鍵と対となる鍵を用いて暗号化されて車載システム１０に配信されることを前提としている。もしファームウェアが改変されていたり、異なる鍵で暗号化されていたりした場合には、復号処理部１５１で正常に復号することができないため、ターゲットとなるＥＣＵにインストールされることもない。

【０１３０】

なお、以上はＥＣＵのファームウェアが暗号化されて配信される例を示したが、ＥＣＵのファームウェアは暗号化される代わりに、ＭＡＣや署名が付与されて配信される場合もある。ＥＣＵのファームウェアにＭＡＣや署名を付与することで、データの完全性を保証することができる。そのような場合に対応した車載ゲートウェイ装置１００の構成例を図１２に示す。

【０１３１】

図１２に示す車載ゲートウェイ装置１００では、図１１の復号処理部１５１の代わりに、検証処理部１５３がルーティング処理部１２０内に組み込まれている。この構成の場合、ルーティング処理部１２０は、外部装置から入力したＥＣＵのファームウェアをターゲットとなるＥＣＵに転送する前に、検証処理部１５３によりファームウェアに付与されたＭＡＣまたは署名の検証を行う。そして、ルーティング処理部１２０は、検証処理部１５３による検証に成功したファームウェアのみをターゲットとなるＥＣＵに転送する。これにより、車載システム１０に送信される途中でＥＣＵのファームウェアが改ざんされているかどうかを確認することができ、改ざんされていない正当なファームウェアに限り、ＥＣＵにインストールしてアップデートすることができる。

【０１３２】

なお、ＥＣＵのファームウェアは暗号化され、かつ、ＭＡＣや署名が付与されて配信される場合もある。そのような場合に対応した車載ゲートウェイ装置１００の構成例を図１３に示す。

【０１３３】

図１３に示す車載ゲートウェイ装置１００では、復号処理部１５１と検証処理部１５３の双方が、ルーティング処理部１２０内に組み込まれている。この構成の場合、ルーティング処理部１２０は、外部装置から入力したＥＣＵのファームウェアをターゲットとなるＥＣＵに転送する前に、検証処理部１５３によりファームウェアに付与されたＭＡＣまたは署名の検証を行う。そして、ルーティング処理部１２０は、検証処理部１５３による検証に成功したファームウェアのみを復号処理部１５１で復号し、ターゲットとなるＥＣＵに転送する。これにより、車載システム１０に送信される途中でＥＣＵのファームウェアが改ざんされているかどうかを確認することができるとともに、ファームウェアの盗聴を防ぐことができるため、ファームウェアに含まれる秘密情報を保護しながら、改ざんされていない正当なファームウェアに限り、ＥＣＵにインストールしてアップデートすることができる。

【０１３４】

＜第３実施形態＞

次に、第３実施形態について説明する。第３実施形態は、蓄積部１３０に蓄積したデータを削除する点が、第１実施形態や第２実施形態と異なる。以下、第１実施形態や第２実施形態との相違点についてのみ説明する。

【０１３５】

図１４は、本実施形態の車載ゲートウェイ装置１００の機能的な構成例を示すブロック図である。本実施形態の車載ゲートウェイ装置１００では、図１４に示すように、データ管理部１６０が追加されている。データ管理部１６０は、蓄積部１３０に蓄積されたＥＣＵが出力するデータやＥＣＵのファームウェアに関する情報を削除する処理を行う。なお、図１４では、データ管理部１６０が蓄積制御部１４０に組み込まれた例を示しているが、データ管理部１６０は蓄積部１３０に蓄積されたＥＣＵが出力するデータやＥＣＵのファームウェアに関する情報を削除できる構成であればよい。また、図１４は、図１３に示した構成の車載ゲートウェイ装置１００にデータ管理部１６０を追加した構成例を示しているが、第１実施形態や第２実施形態において開示したいずれの構成の車載ゲートウェイ装置１００にデータ管理部１６０を追加してもよい。

【０１３６】

上述したように、ＥＣＵが出力するデータは膨大な量になるが蓄積部１３０の容量は有限であるため、すべてのデータを蓄積し続けることはできない。また、ＥＣＵによっては定期的にデータを出力するものもある。それらのＥＣＵが出力するデータの種類は動画データや数値データなど様々なものがある。一般的に動画データは容量が大きく、数値データは容量が小さいといったように、データサイズはデータの種類によって異なるため、同じ時間のデータであってもＥＣＵによって出力するデータサイズが異なる。例えば、数値データを出力するＥＣＵと動画データを出力するＥＣＵがあり、これらのＥＣＵが同一時間内に出力するデータを蓄積部１３０に蓄積すると、動画データを出力するＥＣＵが出力

したデータが蓄積部１３０の容量の大半を占めるといったようなことが起き得る。
【０１３７】
そこで、データ管理部１６０は、データの種類に応じて蓄積部１３０に蓄積されたデータを削除するタイミングを制御し、データを削除する処理を行う。例えば、動画データはＸ時間が経過したら削除し、数値データはＹ時間が経過したら削除するといったように、データの種類に応じて削除するタイミングを制御する。
【０１３８】
他にも、データの種類に応じて蓄積部１３０に蓄積するデータサイズの上限を予め定めておき、上限を超えた分については古いデータから削除していく方法を取ってもよい。例えば、動画データの場合には上限のデータサイズＸ、数値データの場合には上限のデータサイズＹを定めておく。このとき、動画データについて上限のデータサイズＸに達しているが、数値データについては上限のデータサイズＹに達していないとする。ここで新しい動画データを蓄積部１３０に蓄積する場合は、仮に数値データ用の容量に空きがあったとしても古い動画データを削除し、その代わりに新しい動画データを蓄積する。
【０１３９】
なお、以上はデータの種類に応じて蓄積部１３０に蓄積されたデータを削除するタイミングを制御する例を説明したが、蓄積部１３０に蓄積されたデータがどのＥＣＵから出力されたデータであるかによって、そのデータを削除するタイミングを制御してもよい。つまり、あるＥＣＵが出力するデータはＸ時間が経過したら削除し、別のＥＣＵが出力するデータはＹ時間が経過したら削除するといったように、ＥＣＵごとにデータを削除するタイミングを制御してもよい。
【０１４０】
また、ログ蓄積部１３１とシステム情報蓄積部１３２に蓄積された各データの削除を別々に制御してもよい。ログ蓄積部１３１に蓄積されるデータはＥＣＵが出力するデータであり、特に車載システム１０が動作している間は新しいデータが次々に入力され、故障が起きたり攻撃を受けたりしたことを確認するために用いられる。一方、システム情報蓄積部１３２に蓄積されるデータはＥＣＵのファームウェアに関する情報であるが、ＥＣＵのファームウェアがアップデートされる頻度は高くない。そこで、データ管理部１６０は、これらのデータを削除するタイミングを別々に管理してもよい。
【０１４１】
また、以上は蓄積部１３０に蓄積するデータのサイズが容量を超えた場合を想定していたが、蓄積部１３０から外部装置に出力したデータを削除するようにしてもよい。車載システム１０は、第１外部通信処理部２１、第２外部通信処理部２３、第３外部通信処理部２４、または診断用通信部１１を介して外部装置と接続することができる。そこで、ネットワークを介して外部装置に蓄積部１３０のデータを送信することで、蓄積部１３０の容量が一杯になることを避けることができる。この外部装置はＰＣやスマートフォン、ＵＳＢメモリのような装置であってもよいし、クラウドサーバのようなサーバシステムであってもよい。
【０１４２】
データ管理部１６０は、蓄積部１３０に蓄積されたデータがルーティング処理部１２０を介して外部装置に送信された場合に、その送信したデータを蓄積部１３０から削除する処理を行う。なお、データ管理部１６０は、ログ蓄積部１３１に蓄積されたデータは削除するが、システム情報蓄積部１３２に蓄積されたＥＣＵのファームウェアに関する情報は、外部装置に送信したとしても削除しないことが望ましい。ＥＣＵのファームウェアに関する情報は、車載システム１０内で管理されていることが望まれるためである。
【０１４３】
また、車載システム１０を搭載した車両の所有者が変わることも考えられ、このような場合にはプライバシを考慮した対策が求められる。すなわち、ログ蓄積部１３１に蓄積されたＥＣＵが出力するデータには、様々なプライバシに関する情報が含まれる場合がある。例えば、車両の位置情報（ＧＰＳ情報）と車両を運転した時刻情報が蓄積されていると

、その所有者がどの時刻にどの場所にいたかが分かってしまう。他にも、ログ蓄積部１３１には車両がどの経路で走行したか、映像処理ＥＣＵ２０でどのようなルート検索を行ったか、映像処理ＥＣＵ２０でどのようなレストランの検索を行ったか、映像処理ＥＣＵ２０でどのような映像コンテンツを閲覧したか、シート調整をどのように行ったのかといった情報が、ログ蓄積部１３１に蓄積されたデータに含まれている場合がある。したがって、車載システム１０を搭載した車両の所有者が変わる場合には、以前の所有者のプライバシに関する情報を完全に削除できることが望ましい。

【０１４４】

プライバシを考慮した車載ゲートウェイ装置１００の構成例を図１５に示す。図１５に示す車載ゲートウェイ装置１００は、図１４に示した構成に対してプライバシ情報管理部１７０が追加されている。

【０１４５】

プライバシ情報管理部１７０は、ログ蓄積部１３１に蓄積されたプライバシに関連する情報を削除するようログ蓄積部１３１に指示する。ログ蓄積部１３１に蓄積されているＥＣＵが出力したデータのうち、どのデータがプライバシに関連するデータに該当するかは、予めプライバシ情報管理部１７０に設定していてもよいし、ＥＣＵから該当するデータを選定してもよいし、ルーティング処理部１２０を経由して外部装置から指示してもよい。

【０１４６】

また、不正にプライバシ情報が削除されることを防止するために、第１外部通信処理部２１、第２外部通信処理部２３、第３外部通信処理部２４、あるいは診断用通信部１１を経由して外部装置と認証処理を行い、認証が成功した場合のみプライバシ情報の削除を許可するように構成してもよい。その場合の車載ゲートウェイ装置１００の構成例を図１６に示す。

【０１４７】

図１６に示す車載ゲートウェイ装置１００は、図１５に示した構成に対して認証処理部１８０が追加されている。認証処理部１８０は、ＥＣＵまたは外部装置に対する認証処理を行う。認証方式としては、パスワード認証やＲＳＡなどの公開鍵アルゴリズムを用いた公開鍵認証を用いればよい。認証処理部１８０は、認証が成功した場合に、認証が成功したことをプライバシ情報管理部１７０に通知する。プライバシ情報管理部１７０は、認証処理部１８０から認証成功の通知を受けた場合に限り、ログ蓄積部１３１に対してプライバシ情報を削除するよう指示する。

【０１４８】

さらに、オペレータが別な種類の車両に買い換えたり、故障によって同じ種類の車両に乗り換えたりする場合も考えられる。このような場合には、ログ蓄積部１３１に蓄積されたプライバシ情報を他の車両の車載システム１０に移行できるようにすることが求められる。すなわち、運転支援制御ＥＣＵ２２はオペレータの操作の癖の情報を入力とし、学習アルゴリズムによって快適な運転ができるように制御する。オペレータが車両を乗り換えた場合、これらの癖の情報がリセットされてしまい、新たに学習を始めると乗り換え当初は快適な運転制御が実現できなくなる。そこで、ログ蓄積部１３１に蓄積されたプライバシ情報を新しい車両に引き継ぐことが求められる。

【０１４９】

このような場合、プライバシ情報管理部１７０がログ蓄積部１３１からプライバシ情報を取得し、外部装置などに送信する。一方、別の車両に搭載された車載システム１０は、外部装置からオペレータのプライバシ情報を入力し、ログ蓄積部１３１に格納する。このとき、プライバシ情報の漏えいを防止するため、プライバシ情報の送信に先立ち、認証処理部１８０による認証処理を行ってもよい。また、プライバシ情報を送信した後、ログ蓄積部１３１から送信した情報を削除してもよい。

【０１５０】

以上のように、本実施形態の車載ゲートウェイ装置１００は、蓄積部１３０に蓄積した

データを削除する機能を備えることで、蓄積部１３０のデータあふれを有効に防止することができる。また、プライバシ情報の削除や引き継ぎを行う機能を備えることで、プライバシに配慮しつつ、車両の所有者が変更されたり、車両を乗り換えたりする場合にも適切な対応を図ることができる。

【０１５１】

＜変形例＞

さて、信頼性の高いデータ削除方式を規模の大きなデータに適用する場合、所要時間がかかったり、媒体疲弊を招いたりする場合がある。そこで、本変形例では、所定単位のグループごとに共通の暗号鍵を用いて、ログ蓄積部１３１に蓄積するデータを暗号化し、その暗号化処理に利用した暗号鍵を削除（あるいは新しい鍵で上書き）する構成とすることで、高速かつ信頼性の高いデータの無効化を可能とする。ここでのデータの無効化とは、データを復号できない状態にすることであり、上述したデータの削除と同様の効果がある。所定単位は、所定サイズのデータ単位であってもよいし、データ種類やデータの用途あるいは蓄積部１３０の領域ごとなどでグルーピングして暗号鍵を用意してもよい。このようにすることで、鍵自体の更新頻度を下げることができる。

【０１５２】

本変形例の入力制御部１４２は、少なくとも、第１暗号処理部２０２と鍵管理部２０３とを有する。そして、鍵管理部２０３は、データ管理部１６０からの削除要求に応じて当該データの暗号処理に利用する鍵を更新・削除する。真正性・完全性を確保するための暗号処理とは異なる単位で暗号鍵を利用してもよい。このようにすることで、削除される単位と、ログの正当性を主張する単位とが異なる場合にも対応できる。

【０１５３】

鍵管理部２０３は、暗号鍵生成を高速に実施するための乱数生成部を備えていたり、多くの暗号鍵を事前に生成し、蓄積しておく機能を備えていたりしてもよい。

【０１５４】

このような構成とすることで、鍵データという少量のデータを削除するだけで、それによって暗号化されたデータを無効化できる。データの消去に時間のかかる記憶媒体にデータが蓄積されている場合に有効である。また、蓄積部１３０の物理的な記録箇所が離れて記録されていたとしても一度にデータを無効化できる。この性質は、例えばデータ消去オペレーションがブロックごとに必要なフラッシュメモリなどの記憶媒体において、複数ブロックに分散したデータを無効化するのに特に有効である。ログ蓄積部１３１に蓄積されるデータは時系列に書き込まれるが、消去したいデータが時系列に生じるとは限らない。この場合は、管理対象のデータが複数のブロックに分散することが起こりえるが、このような場合でも、データの無効化を効率的に実施できる。

【０１５５】

また、ログ蓄積部１３１に蓄積するデータを暗号化するための暗号鍵（便宜上、データ暗号鍵と呼ぶ）に加えて、このデータ暗号鍵を暗号・復号するための暗号鍵（便宜上、鍵暗号鍵と呼ぶ）を考える。この場合の構成を図１７に示す。図１７に示す構成例は、蓄積部１３０に暗号鍵記録部１３３が新たに備わっている点が図１６とは異なる。

【０１５６】

これまでの構成では鍵管理部２０３でデータ暗号鍵を管理していたが、図１７に示す構成の場合は、鍵暗号鍵を鍵管理部２０３で管理する。そして、暗号化されたデータ暗号鍵を、蓄積部１３０の暗号鍵記録部１３３で管理する。鍵管理部２０３では、暗号鍵記録部１３３に蓄積された暗号化されたデータ暗号鍵を、鍵暗号鍵により復号した上で第１暗号処理部２０２や第３暗号処理部３０６に供給したり、暗号鍵記録部１３３に蓄積するデータ暗号鍵を鍵暗号鍵で暗号してから蓄積したり、データ管理部１６０からの要求に応じてデータ鍵を削除したりする。

【０１５７】

データ暗号鍵を複数用意し、データはデータ種別やデータの用途あるいは蓄積部の領域ごとなどでグルーピングして、それぞれ異なるデータ暗号鍵で暗号化する。複数のデータ

暗号鍵は同一の鍵暗号鍵で暗号、復号される。これにより、単一の鍵暗号鍵を消去することで、その鍵暗号鍵で暗号化された複数の暗号鍵を用いて暗号化されたデータを一括して無効化することができる。また、少量データである鍵暗号鍵をＬＳＩチップ内など比較的物理攻撃（低速バスのプローブ、データ改ざん、チップ取り外して付け替え・不正利用）に対して強固な箇所（オンチップフラッシュなど）に記憶して、暗号化されたデータ暗号鍵を相対的に物理攻撃に弱い記録媒体に配置しても安全性を確保することができる。

【０１５８】

なお、図１７では暗号鍵記録部１３３は蓄積部１３０に設けられていたが、暗号化されたデータ暗号鍵を蓄積部１３０とは別の領域に格納してもよい。その場合の構成を図１８に示す。図１８に示す構成例は、鍵蓄積部１９０を新たに備え、この鍵蓄積部１９０に、暗号化されたデータ暗号鍵を蓄積する暗号鍵記録部１９１が設けられている点が図１７とは異なる。

【０１５９】

図１８に示す構成例では、暗号化されたデータ暗号鍵を、ログ蓄積部１３１やシステム情報蓄積部１３２を有する蓄積部１３０とは異なる記憶媒体である鍵蓄積部１９０に記録する。その上で、各記憶媒体の特性を考慮して、暗号鍵とデータの蓄積媒体を使い分けることで、最適かつ信頼性の高い車載ゲートウェイ装置１００を実現できる。一例としては、重要なデータだが小容量である暗号鍵をビットコストが高く書き換え可能回数などの特性に優れた記録媒体に記録し、大容量であるログデータをより安価な記録媒体に記録する。

【０１６０】

上記のような削除方式に対する配慮は、特に信頼性とリアルタイム性が要求される車載向けの情報記録部を実現する上で特に効果が大きい。

【０１６１】

＜第４実施形態＞

車載システム１０において車載ゲートウェイ装置１００が処理すべきデータ量は多いため、第１実施形態のように、ルーティング処理部１２０内のフィルタリング処理部１２１や蓄積制御部１４０内の入力制御部１４２によって、蓄積部１３０に蓄積するデータを選別することは必要である。また、この処理を固定的なものではなく、データ量に応じて変更することでログ機構の可用性を確保することもできる。本実施形態は、このような処理の変更を悪用した攻撃を防ぐための構成例である。

【０１６２】

攻撃者は、目的の達成に向けて自身が攻撃できる範囲を拡大しようとすることがある。ここでは、車載ゲートウェイ装置１００に不正アクセスした攻撃者が、自身の不正アクセスできる範囲を拡大しようとする場面を想定する。この攻撃者は、フィルタリング処理部１２１によるデータ選別のポリシーや入力制御部１４２によるデータ選別のルールがデータ量に応じて変更されるように、実際には受信していないデータを直接ルーティング処理部１２０や蓄積制御部１４０に入力する。これにより、車載ゲートウェイ装置１００は、攻撃者によって入力された架空のデータをもとに、フィルタリング処理部１２１や入力制御部１４２が蓄積部１３０に蓄積するデータを選別するような新たな動作をする。攻撃者は、この新たな動作では蓄積部１３０にデータが蓄積されないような不正アクセスを実施する。このように、ログ機構の可用性のための機構を悪用する攻撃がある。本実施形態は、このような攻撃への対策を鑑みたものである。

【０１６３】

図１９は、本実施形態の車載ゲートウェイ装置１００の機能的な構成例を示すブロック図である。図２に示した第１実施形態の構成と比較して、監視部４００が追加されている点が異なる。監視部４００は、車載ゲートウェイ装置１００の各部と接続されるが、通信処理部１１０、ルーティング処理部１２０、蓄積部１３０および蓄積制御部１４０とは、独立したＣＰＵコアとメモリあるいはＨＷ機構により実現される。

【０１６４】

本実施形態の車載ゲートウェイ装置１００において、監視部４００は各バスをモニタリングし、例えばフィルタリング処理部１２１のポリシーや入力制御部１４２のルールを変更する前に、そのポリシー変更やルール変更の要因となるイベントが実際に発生しているかを確認する。例えば、蓄積部１３０の容量監視に伴うポリシーの変更が要求された場合には、監視部４００が、独立に蓄積部１３０の容量を確認することで、ルーティング処理部１２０が不正アクセスされていないことを確認する。また、例えば、ルーティング処理部１２０からのデータ入力量が大きいために、入力制御部１４２が蓄積部１３０に送るデータ種類やデータ量を減らしたりするようにルールの変更が要求された場合には、監視部４００が、通信処理部１１０の入出力のデータ量を確認することで、蓄積制御部１４０が不正にアクセスされていないことを確認する。また、監視部４００が蓄積部１３０の容量を確認することで、データ消去のきっかけとなるイベントの情報を蓄積制御部１４０に捏造して送ってデータを消去させるような攻撃にも対応できる。

【０１６５】

以上のように、本実施形態の車載ゲートウェイ装置１００は、蓄積部１３０に蓄積するデータを選別するポリシーやルールの変更が要求された場合に、監視部４００が、そのポリシー変更やルール変更の要因となるイベントが実際に発生しているかを確認するようにしている。したがって、車載ゲートウェイ装置１００に不正アクセスした攻撃者による攻撃の痕跡消去のための試みを防ぐことができる。

【０１６６】

＜補足説明＞

以上説明した実施形態の車載ゲートウェイ装置１００の機能的な構成要素は、例えば、ハードウェアとソフトウェア（プログラム）との協働により実現することができる。ハードウェアとしては、各種のハードウェアプロセッサ、揮発、不揮発のメモリ、メモリコントローラ、通信モジュールなど、車載ゲートウェイ装置１００をコンピュータシステムとして動作させるものがある。このようなコンピュータシステム上で所定のプログラムが実行されることにより、上述した車載ゲートウェイ装置１００の機能的な構成要素を実現することができる。

【０１６７】

車載ゲートウェイ装置１００の機能的な構成要素を実現するプログラムは、例えば、不揮発のメモリに予め組み込んで提供される。また、上記プログラムは、インストール可能な形式または実行可能な形式のファイルでコンピュータ読み取り可能な記録媒体に記録されて提供されるようにしてもよい。また、上記プログラムを、インターネットなどのネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、上記プログラムを、インターネットなどのネットワーク経由で提供または配布するように構成してもよい。なお、車載ゲートウェイ装置１００における上述した機能的な構成要素は、その一部または全部を、ＡＳＩＣやＦＰＧＡなどの専用のハードウェアを用いて実現することも可能である。

【０１６８】

以上、本発明の実施形態を説明したが、この実施形態は例として提示したものであり、発明の範囲を限定することは意図していない。この新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

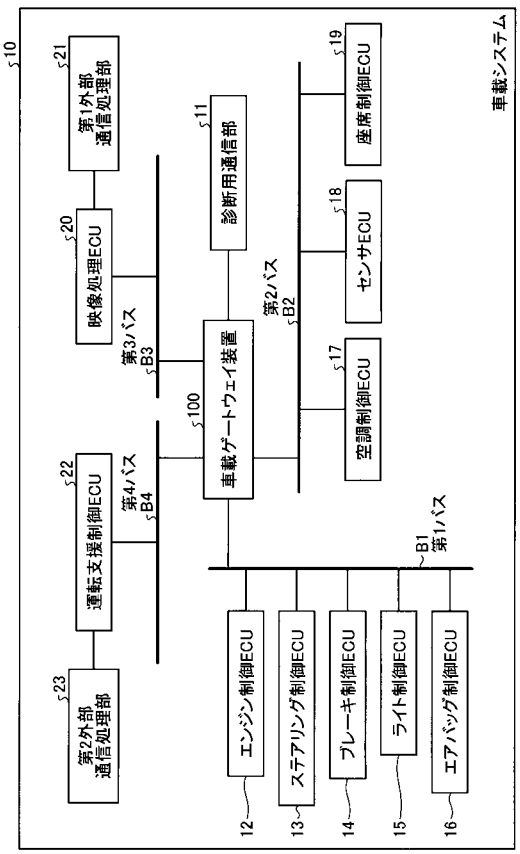
【符号の説明】

【０１６９】

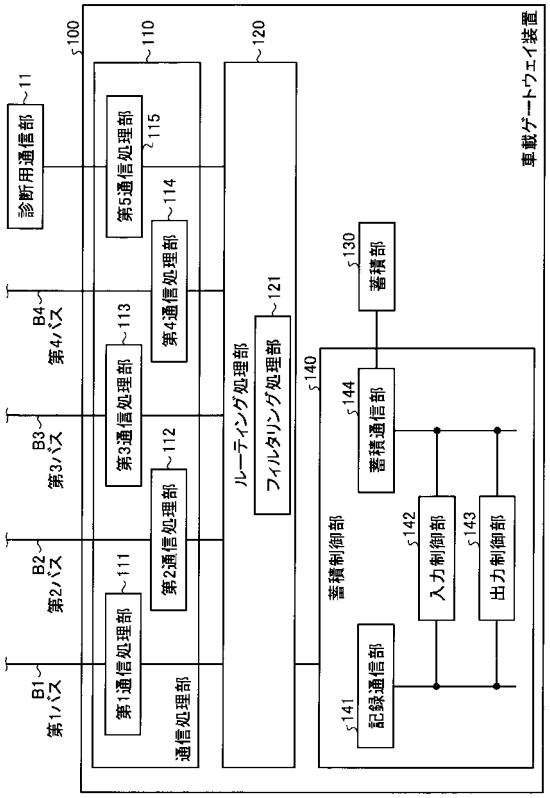
１０　車載システム
１２　エンジン制御ＥＣＵ
１３　ステアリング制御ＥＣＵ
１４　ブレーキ制御ＥＣＵ
１５　ライト制御ＥＣＵ

１６　エアバッグ制御ＥＣＵ
１７　空調制御ＥＣＵ
１８　センサＥＣＵ
１９　座席制御ＥＣＵ
２０　映像処理ＥＣＵ
２２　運転支援制御ＥＣＵ
１００　車載ゲートウェイ装置
１１０　通信処理部
１２０　ルーティング処理部
１３０　蓄積部
１３１　ログ蓄積部
１３２　システム情報蓄積部
１４０　蓄積制御部
１４２　入力制御部
１４３　出力制御部
１５０　システム情報取得部
１６０　データ管理部
１７０　プライバシ情報管理部
２０１　選別処理部
２０２　第１暗号処理部
３０１　アクセス制御部
３０２　モード設定部
３０４　第２暗号処理部
３０６　第３暗号処理部
４００　監視部

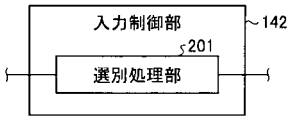
【図１】



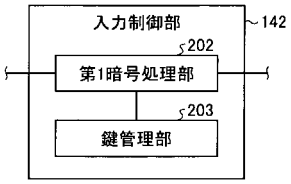
【図２】



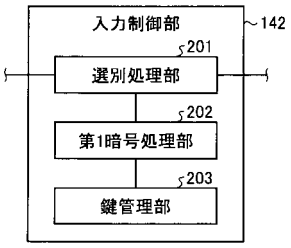
【図３－１】



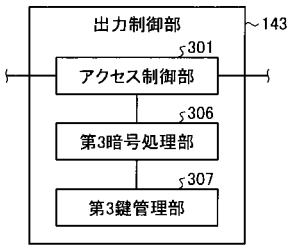
【図３－２】



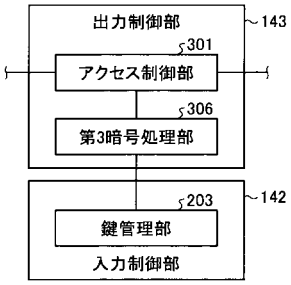
【図３－３】



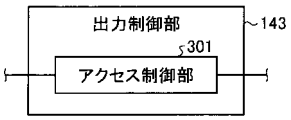
【図４－４】



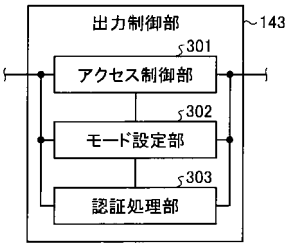
【図４－５】



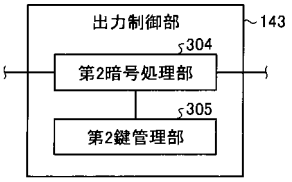
【図４－１】



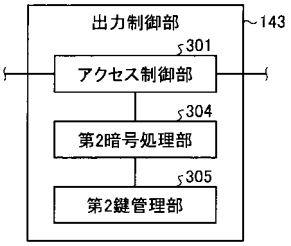
【図４－２】



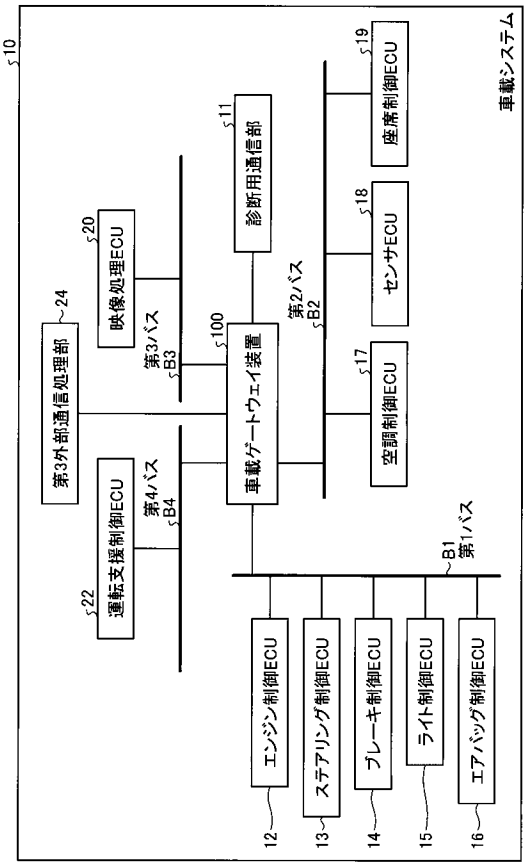
【図４－３】



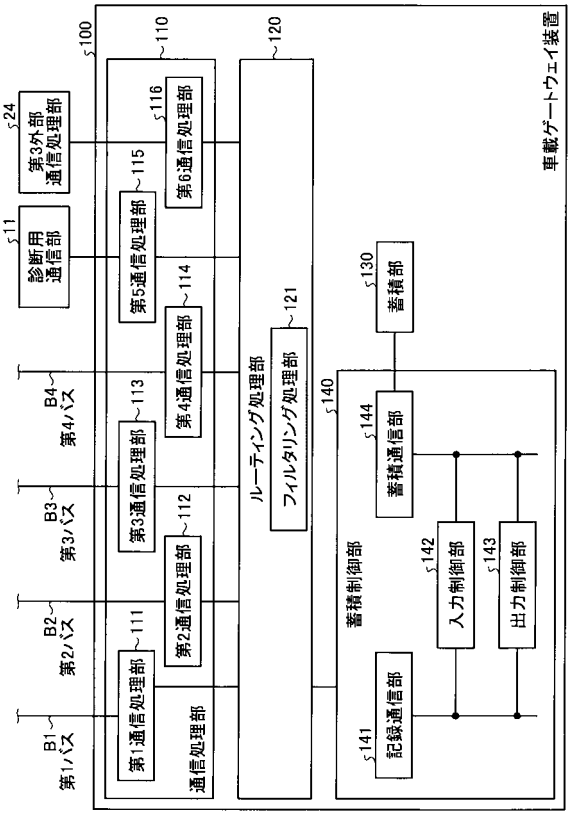
【図４－６】



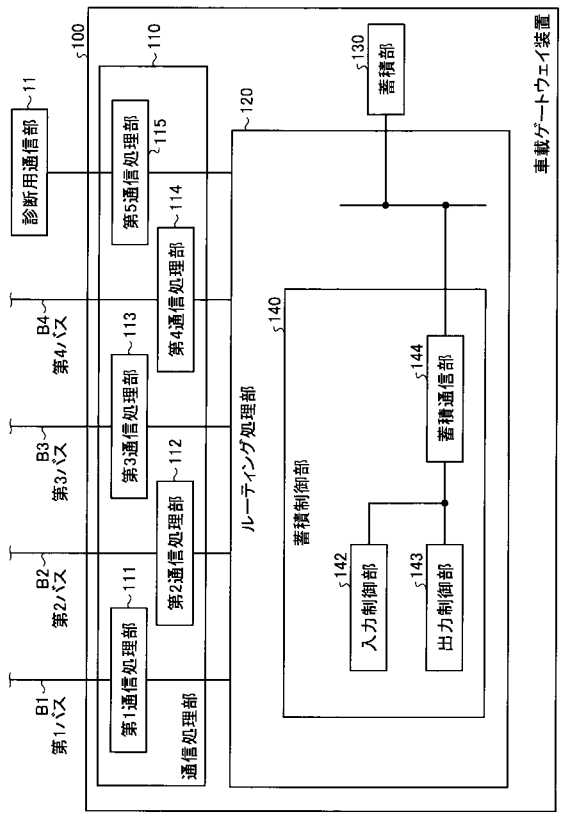
【図５】


車載システム
10
第3外部通信処理部
24
運転支援制御ECU
22
第4バス
B4
映像処理ECU
20
第3バス
B3
車載ゲートウェイ装置
100
診断用通信部
11
第2バス
B2
センサECU
18
座席制御ECU
19
空調制御ECU
17
第1バス
B1
エンジン制御ECU
12
ステアリング制御ECU
13
ブレーキ制御ECU
14
ライト制御ECU
15
エアバッグ制御ECU
16

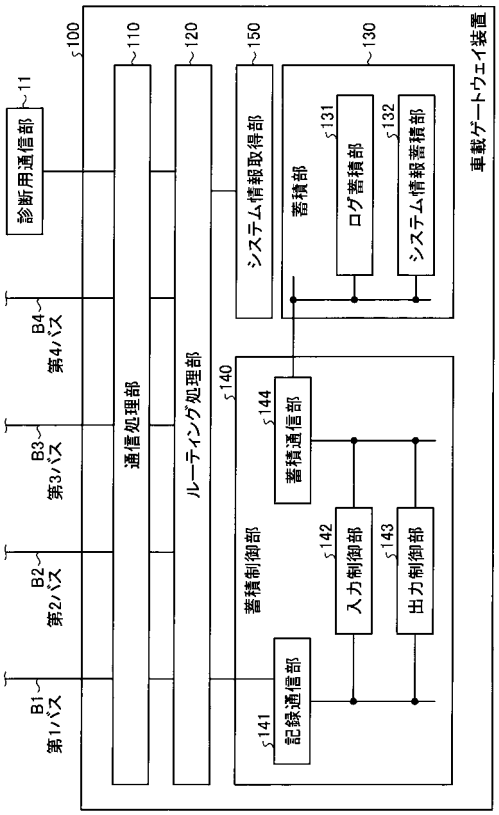
【図６】


車載ゲートウェイ装置
100
第3外部通信処理部
24
診断用通信部
11
第1バス
B1
第2バス
B2
第3バス
B3
第4バス
B4
第1通信処理部
111
第2通信処理部
112
第3通信処理部
113
第4通信処理部
114
第5通信処理部
115
第6通信処理部
116
通信処理部
110
ルーティング処理部
120
フィルタリング処理部
121
蓄積制御部
140
記録通信部
141
入力制御部
142
出力制御部
143
蓄積通信部
144
蓄積部
130

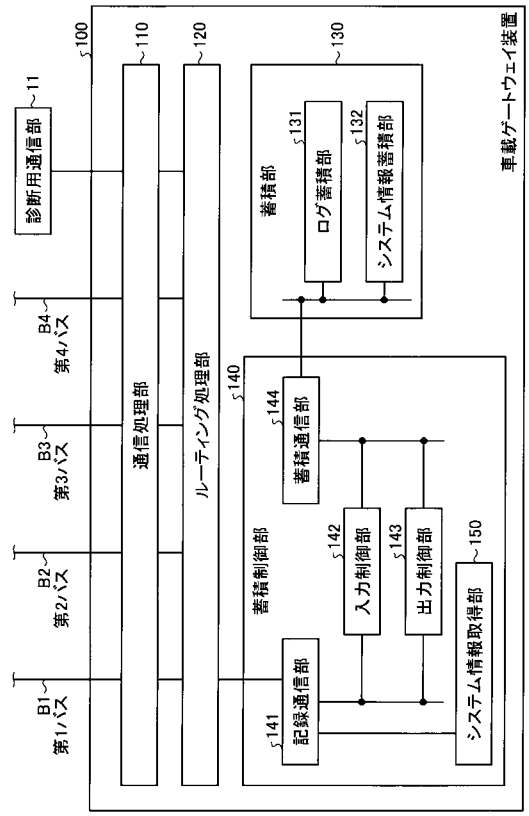
【図７】


車載ゲートウェイ装置
100
診断用通信部
11
第1バス
B1
第2バス
B2
第3バス
B3
第4バス
B4
第1通信処理部
111
第2通信処理部
112
第3通信処理部
113
第4通信処理部
114
第5通信処理部
115
通信処理部
110
ルーティング処理部
120
蓄積制御部
140
入力制御部
142
出力制御部
143
蓄積通信部
144
蓄積部
130

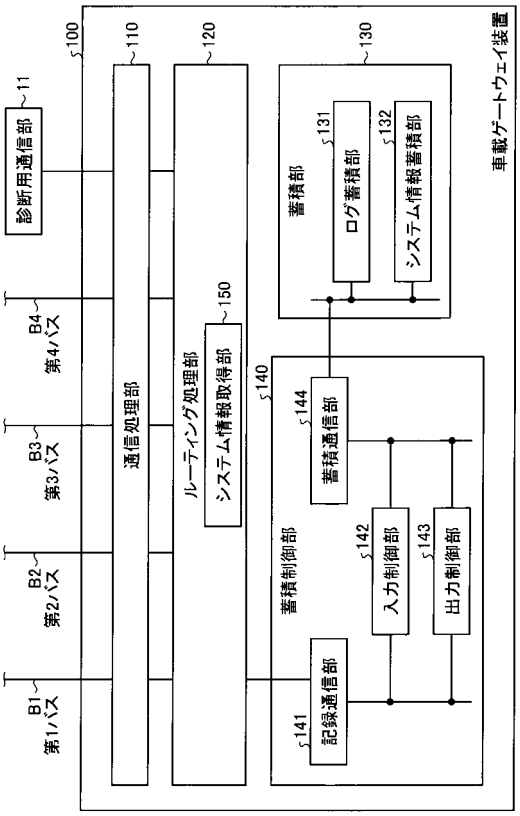
【図８】


車載ゲートウェイ装置
100
診断用通信部
11
第1バス
B1
第2バス
B2
第3バス
B3
第4バス
B4
通信処理部
110
ルーティング処理部
120
システム情報取得部
150
蓄積制御部
140
記録通信部
141
入力制御部
142
出力制御部
143
蓄積通信部
144
蓄積部
130
ログ蓄積部
131
システム情報蓄積部
132

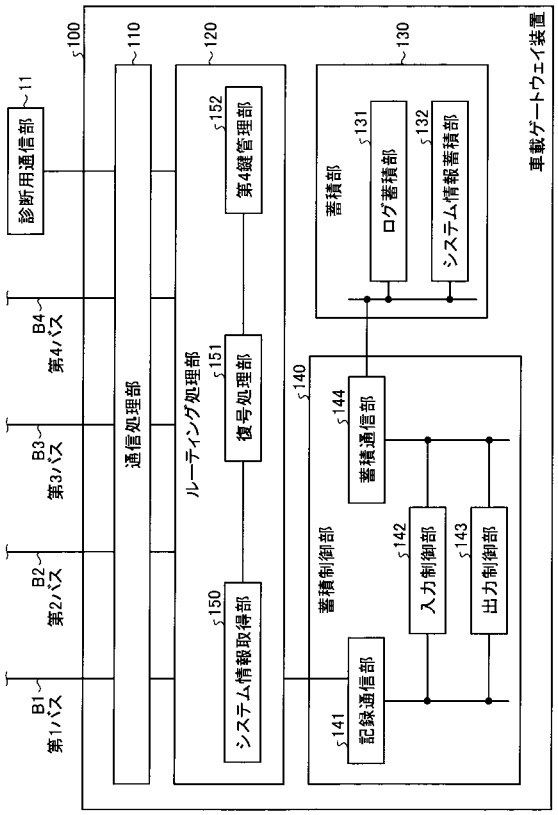
【図９】



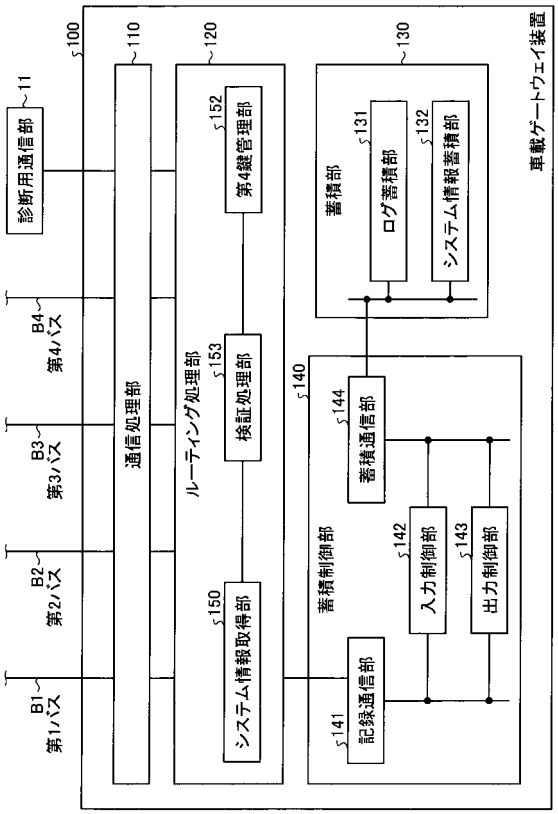
【図１０】



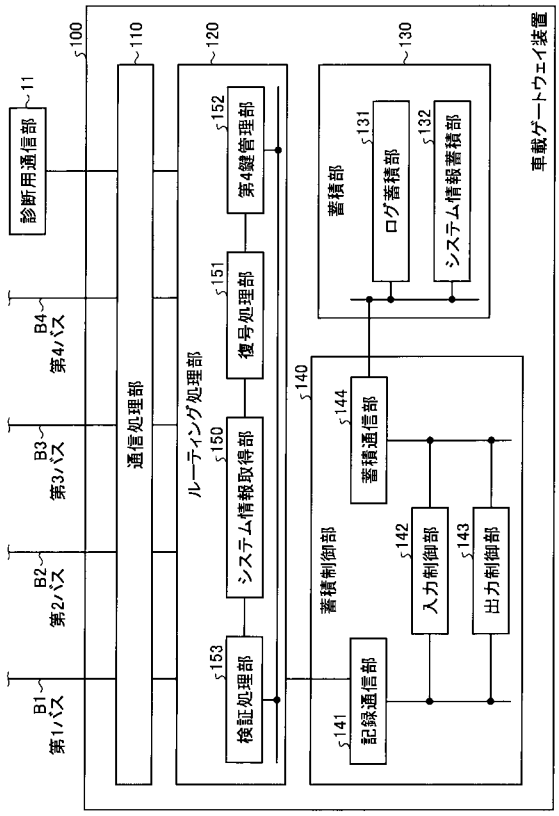
【図１１】



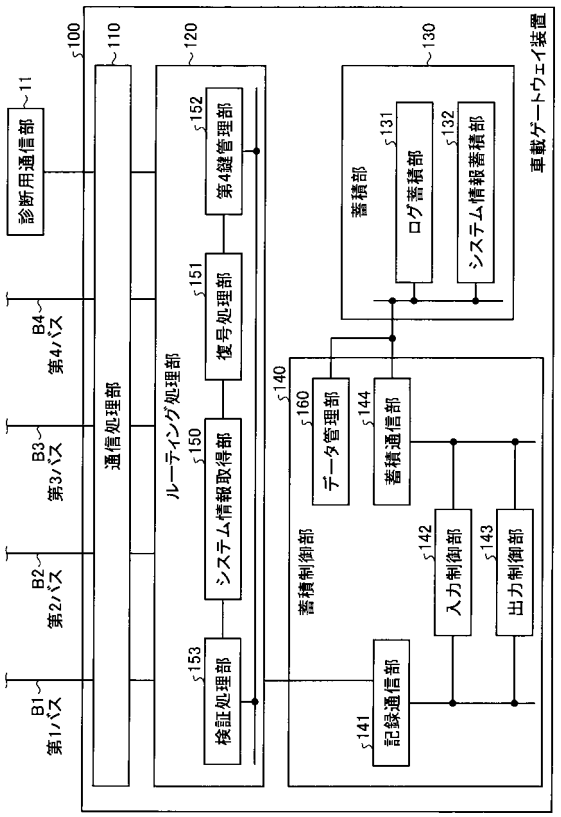
【図１２】



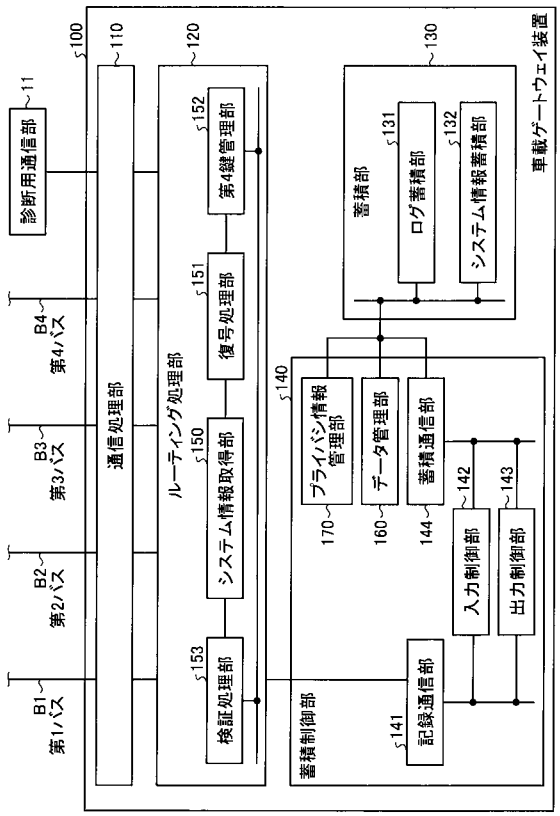
【図１３】



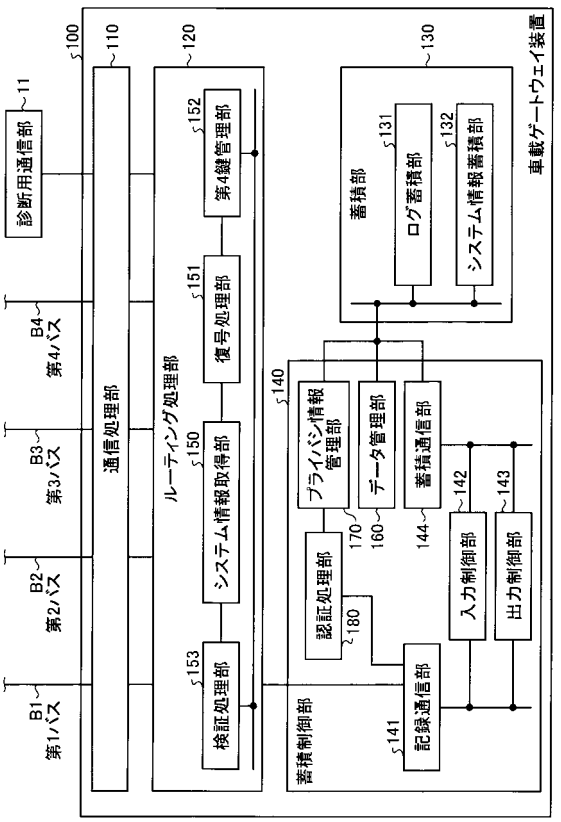
【図１４】



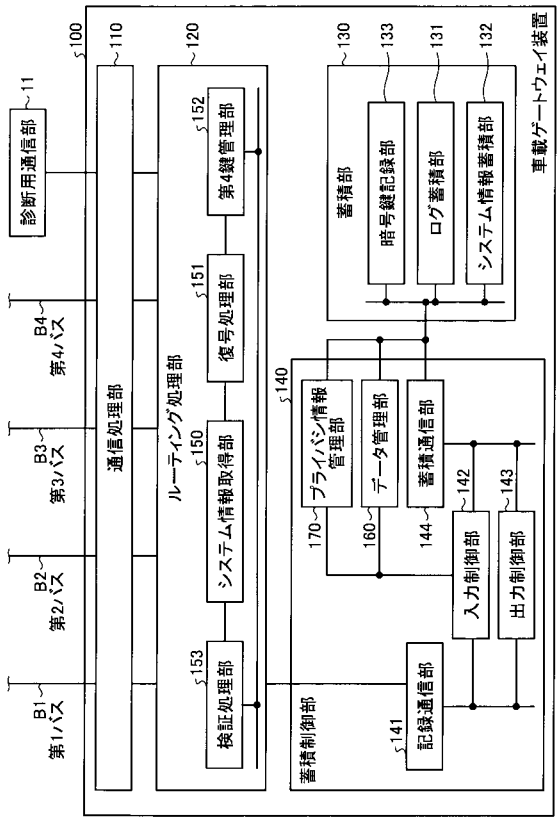
【図１５】



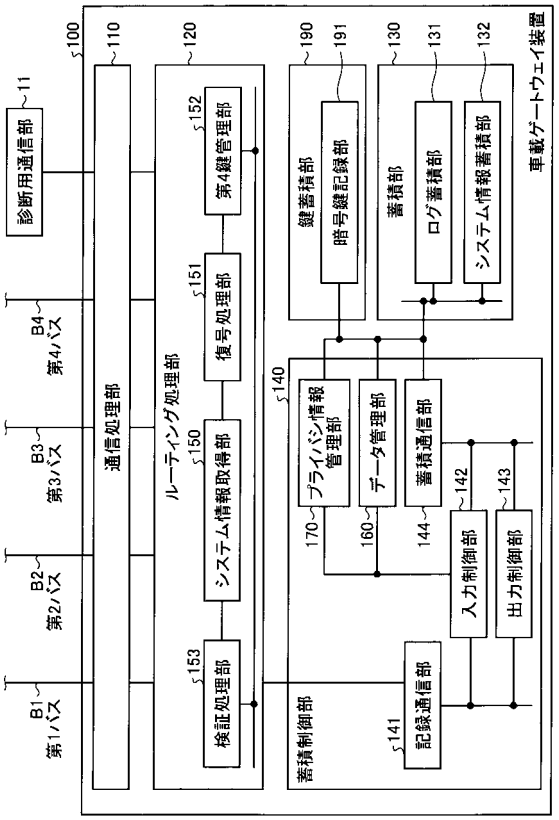
【図１６】



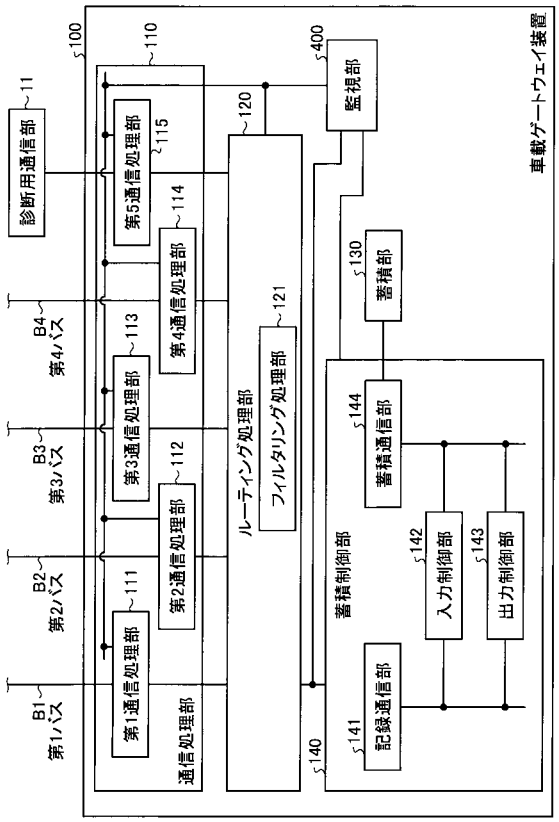
【図１７】


車載ゲートウェイ装置
診断用通信部
通信処理部
ルーティング処理部
蓄積制御部
蓄積部
暗号鍵記録部
ログ蓄積部
システム情報蓄積部
第4鍵管理部
復号処理部
システム情報取得部
検証処理部
プライバシ情報管理部
データ管理部
蓄積通信部
入力制御部
出力制御部
記録通信部
第1バス
第2バス
第3バス
第4バス

【図１８】


車載ゲートウェイ装置
診断用通信部
通信処理部
ルーティング処理部
蓄積制御部
鍵蓄積部
暗号鍵記録部
蓄積部
ログ蓄積部
システム情報蓄積部
第4鍵管理部
復号処理部
システム情報取得部
検証処理部
プライバシ情報管理部
データ管理部
蓄積通信部
入力制御部
出力制御部
記録通信部
第1バス
第2バス
第3バス
第4バス

【図１９】


車載ゲートウェイ装置
診断用通信部
通信処理部
第1通信処理部
第2通信処理部
第3通信処理部
第4通信処理部
第5通信処理部
ルーティング処理部
フィルタリング処理部
蓄積制御部
蓄積部
監視部
蓄積通信部
入力制御部
出力制御部
記録通信部
第1バス
第2バス
第3バス
第4バス

フロントページの続き

(72)発明者　山田　菜穂子
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　梅澤　健太郎
東京都港区芝浦一丁目１番１号　株式会社東芝内

Ｆターム(参考) 5K033 AA09　BA06　CC01　DA05　DA13　DB12　DB16　DB18