(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2005-242871
(P2005-242871A)
(43)公開日　平成17年9月8日(2005.9.8)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	560C	5B017
G06F 1/00	G06F 12/14	560E	5B076
H04L 9/32	H04L 9/00	675A	5J104
	G06F 9/06	660J	

審査請求 未請求　請求項の数 7　OL　（全 16 頁）

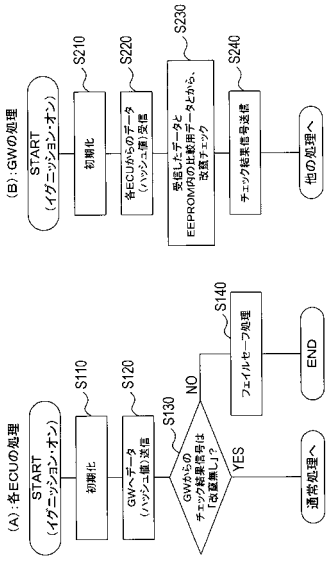
(21)出願番号　特願2004-54251(P2004-54251)
(22)出願日　平成16年2月27日(2004.2.27)

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(74)代理人　100082500
弁理士　足立　勉
(72)発明者　脇山　賢一
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内

Fターム(参考)　5B017 AA08　BB02　CA12
5B076 FC01　FD02
5J104 LA05　NA12　NA42

(54)【発明の名称】通信システム

(57)【要約】
【課題】　通信システムを構成する電子装置の内蔵データが改竄されたことを検出する。
【解決手段】　車両内の通信ラインに複数のＥＣＵと１つのゲートウェイが接続された通信システムにおいて、各ＥＣＵは、イグニッションスイッチ（以下、ＩＧ）のオフに伴い動作を停止する直前に、自装置に内蔵されているデータのハッシュ値をゲートウェイへ送信し、ゲートウェイが、その各ＥＣＵからのハッシュ値を比較用データとして自己のＥＥＰＲＯＭに記憶する。そして、ＩＧがオンされて各ＥＣＵが動作を開始した際に、その各ＥＣＵが、自装置に内蔵されているデータのハッシュ値をゲートウェイへ送信し（Ｓ１２０）、ゲートウェイが、各ＥＣＵについて、そのＥＣＵからのハッシュ値と、自己のＥＥＰＲＯＭ内の上記比較用データとを比較して、両値が不一致ならば、そのＥＣＵの内蔵データは改竄されていると判定する（Ｓ２２０，Ｓ２３０）。
【選択図】　図２



【特許請求の範囲】
【請求項１】
通信ラインに複数の電子装置が接続された通信システムにおいて、
前記複数の電子装置のうちの特定の電子装置（以下、親電子装置という）が、他の電子装置（以下、子電子装置という）から、該子電子装置に内蔵されている改竄検出対象のメモリデータの特徴を表す情報を受信し、その子電子装置からの前記情報と、当該親電子装置の記憶手段に事前に記憶されている改竄有無判定用基準情報とを比較することにより、前記子電子装置に内蔵されている前記メモリデータが改竄されたか否かを判定すること、
を特徴とする通信システム。
【請求項２】
請求項１に記載の通信システムにおいて、
前記子電子装置が動作を停止する直前に、該子電子装置が、前記親電子装置へ、自装置が現在内蔵している前記メモリデータの特徴を表す情報を送信すると共に、前記親電子装置が、その子電子装置からの情報を前記改竄有無判定用基準情報として前記記憶手段に記憶し、
前記子電子装置が動作を開始した際に、該子電子装置が、前記親電子装置へ、自装置が現在内蔵している前記メモリデータの特徴を表す情報を送信すると共に、前記親電子装置が、その子電子装置からの情報と、前記記憶手段に記憶されている前記改竄有無判定用基準情報とを比較して、その両情報が一致していなければ、前記子電子装置に内蔵されている前記メモリデータが改竄されたと判定すること、
を特徴とする通信システム。
【請求項３】
請求項１又は請求項２に記載の通信システムにおいて、
前記メモリデータの特徴を表す情報は、前記メモリデータそのものであること、
を特徴とする通信システム。
【請求項４】
請求項１又は請求項２に記載の通信システムにおいて、
前記メモリデータの特徴を表す情報は、前記メモリデータの所定の関数による関数値であること、
を特徴とする通信システム。
【請求項５】
請求項１に記載の通信システムにおいて、
前記改竄検出対象のメモリデータは、前記子電子装置の動作中に値が所定の変化傾向で更新されていくデータであると共に、前記メモリデータの特徴を表す情報は、前記メモリデータそのものであり、
前記子電子装置は、予め定められたタイミング毎に、前記親電子装置へ、自装置が現在内蔵している前記メモリデータを送信し、
前記親電子装置は、前記子電子装置からの前記メモリデータを受信すると共に、今回受信した前記メモリデータの値と、前回受信して前記記憶手段に前記改竄有無判定用基準情報として記憶しておいた前記メモリデータの値との関係が、前記変化傾向に合った関係になっていなければ、前記子電子装置に内蔵されている前記メモリデータが改竄されたと判定すること、
を特徴とする通信システム。
【請求項６】
請求項１に記載の通信システムにおいて、
前記メモリデータの特徴を表す情報は、前記メモリデータの一方向性関数による関数値であり、
前記子電子装置は、予め定められたタイミング毎に、自装置が現在内蔵している前記メモリデータの一方向性関数による関数値を算出すると共に、前回算出した関数値（以下、旧関数値という）を前記メモリデータの格納先である記憶媒体から読み出して、その読み

出した旧関数値と、今回算出した関数値（以下、新関数値という）とを、前記親電子装置に送信し、更に、前記新関数値を次回に送信する旧関数値として前記記憶媒体に更新記憶し、

前記親電子装置は、前記子電子装置からの前記新関数値及び前記旧関数値を受信すると共に、今回受信した前記旧関数値と、前回受信して前記記憶手段に前記改竄有無判定用基準情報として記憶しておいた前記新関数値とを比較して、その両関数値が一致していなければ、前記子電子装置に内蔵されている前記メモリデータが改竄されたと判定すること、

を特徴とする通信システム。

【請求項７】

請求項１ないし請求項６の何れか１項に記載の通信システムにおいて、

前記親電子装置の記憶手段は、耐タンパ性の記憶装置であること、

を特徴とする通信システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、通信ラインに複数の電子装置が接続された通信システムに関する。

【背景技術】

【０００２】

従来より、例えば自動車においては、複数の電子制御装置（以下、ＥＣＵという）間で情報提供や連係動作のためのデータ通信ができるように、図６に例示する如く各ＥＣＵを通信ライン１００で接続して、通信システム（所謂車載ＬＡＮ）を構築している。

【０００３】

ここで、図６に例示する通信システムは、自動変速機を制御するＥＣＴ・ＥＣＵ１０１と、エンジンを制御するエンジンＥＣＵ１０２と、メータの表示を制御するメータＥＣＵ１０３と、車両の走行距離を積算する距離積算ＥＣＵ１０４とからなっている。

【０００４】

そして、距離積算ＥＣＵ１０４は、他のＥＣＵ（例えばＥＣＴ・ＥＣＵ１０１）から送信される車速値（詳しくは、車速値のデータ）を受信して、その車速値から車両の総走行距離を積算し、その距離積算値（詳しくは、距離積算値のデータ）を、メータＥＣＵ１０３へ送信する。すると、メータＥＣＵ１０３は、その距離積算ＥＣＵ１０４からの距離積算値をオドメータ（総走行距離計）に表示させることとなる。

【０００５】

そして更に、距離積算ＥＣＵ１０４は、車両のバッテリが外されても距離積算値を失わないように、その距離積算値を電気的にデータの書き換えが可能なＥＥＰＲＯＭ１０５に更新記憶するようにしている。尚、こうした動作は、ＣＰＵ１０６がプログラムを実行することで実現される。また、ＥＥＰＲＯＭ等のデータ書き換え可能な不揮発性メモリには、データの書き込み／消去の回数に制限があるため、ＥＥＰＲＯＭ１０５への距離積算値の更新記憶は、算出される値が所定値（例えば１ｋｍ分）だけ増加する毎に行われる（例えば、非特許文献１参照）。

【非特許文献１】水谷集治監修，カーエレクトロニクス研究会編著，「新カーエレクトロニクス」，株式会社山海堂，平成４年４月，ｐ．１１７－１２２

【発明の開示】

【発明が解決しようとする課題】

【０００６】

ところで、上記図６の通信システムでは、距離積算ＥＣＵ１０４のＥＥＰＲＯＭ１０５が不正に交換されることで、オドメータに表示される総走行距離の値が改竄されてしまうという問題がある。つまり、距離積算ＥＣＵ１０４に内蔵される距離積算値が、ＥＥＰＲＯＭ１０５の交換によって改竄されてしまうということであり、このような改竄行為が起こると、車両の価値が不正に変わってしまうこととなる。

【０００７】

また近年では、ＥＣＵに盗難防止用などの様々なセキュリティ機能が組み込まれているが、距離積算値のような演算データに限らず、各ＥＣＵに内蔵されたプログラムが改竄されることで、そのようなセキュリティ機能を無効にされてしまう可能性もある。

【０００８】

そこで本発明は、通信システムを構成する電子装置のプログラムやデータが改竄されたことを検出できるようにすることを目的としている。

【課題を解決するための手段】

【０００９】

上記目的を達成するためになされた請求項１の通信システムでは、通信ラインに接続された複数の電子装置のうちの特定の電子装置である親電子装置が、他の電子装置である子電子装置から、その子電子装置に内蔵されている改竄検出対象のメモリデータの特徴を表す情報（以下、特徴情報ともいう）を受信する。そして更に、親電子装置は、その子電子装置から受信した特徴情報と、当該親電子装置の記憶手段に事前に記憶されている改竄有無判定用基準情報とを比較することにより、その子電子装置に内蔵されているメモリデータが改竄されたか否かを判定する。

【００１０】

尚、親電子装置の記憶手段に事前に記憶しておく改竄有無判定用基準情報としては、子電子装置からの特徴情報と比較することで、その子電子装置に内蔵されているメモリデータが改竄されたか否かを判別できる情報であれば良く、例えば、子電子装置に内蔵されたプログラムや固定のデータを改竄検出対象のメモリデータとするのであれば、子電子装置が送信するはずの特徴情報と同じものを、親電子装置の製造時等において、記憶手段に改竄有無判定用基準情報として記憶しておけば良い。この場合、親電子装置は、子電子装置からの特徴情報と、記憶手段内の改竄有無判定用基準情報とが不一致ならば、子電子装置のメモリデータが改竄されたと判定することができる。

【００１１】

このような通信システムによれば、子電子装置に内蔵された改竄検出対象のメモリデータが改竄されたことを確実に検出することができる。

また特に、請求項２の通信システムでは、子電子装置が動作を停止する直前に、該子電子装置が、親電子装置へ、自装置が現在内蔵しているメモリデータの特徴を表す情報を送信すると共に、親電子装置が、その子電子装置からの情報（特徴情報）を改竄有無判定用基準情報として記憶手段に記憶する。

【００１２】

そして、子電子装置が動作を開始した際に、該子電子装置が、親電子装置へ、自装置が現在内蔵しているメモリデータの特徴を表す情報を送信すると共に、親電子装置が、その子電子装置からの情報と、記憶手段に記憶されている改竄有無判定用基準情報（即ち、子電子装置が動作を停止する直前に送信して来た特徴情報）とを比較して、その両情報が一致していなければ、子電子装置に内蔵されているメモリデータが改竄されたと判定するようになっている。

【００１３】

つまり、この通信システムでは、子電子装置が動作を停止する直前の最終状態でのメモリデータの特徴を表す特徴情報が、親電子装置の記憶手段に改竄有無判定用基準情報として記憶され、その改竄有無判定用基準情報と、子電子装置が動作を開始した時点でのメモリデータの特徴を表す特徴情報とが不一致ならば、子電子装置のメモリデータが改竄されたと判定するようにしている。

【００１４】

この構成によれば、改竄検出対象のメモリデータが、プログラムや固定のデータのみならず、子電子装置の動作中に値が変化する演算データであっても、効率良く改竄検出を行うことができる。改竄検出対象のメモリデータが、どのようなものであっても、子電子装置が動作を停止している間に違う内容に改竄されたならば、その子電子装置が動作を再開した際に、メモリデータの改竄が親電子装置にて確実に検出することができるからである

。
【００１５】
尚、親電子装置は、常時動作するように構成されていても良いし、また、子電子装置が動作を停止する直前に送信する特徴情報を記憶手段に記憶したら動作を停止し、その後、子電子装置と共に動作を開始するように構成されていても良い。
【００１６】
ところで、メモリデータの特徴を表す情報（特徴情報）としては、請求項３に記載の如く、そのメモリデータそのものであっても良い。
また、メモリデータの特徴情報としては、請求項４に記載の如く、メモリデータの所定の関数による関数値（即ち、メモリデータを引数として所定の関数の処理を行った結果の値）であっても良い。そして、特徴情報として、こうした関数値を用いたならば、元のメモリデータよりも関数値の方が一般にデータ量が小さいため、子電子装置から親電子装置に送信するデータ量や親電子装置側で記憶する改竄有無判定用基準情報のデータ量を抑えることができる。
【００１７】
一方、請求項５の通信システムでは、改竄検出対象のメモリデータが、子電子装置の動作中に値が所定の変化傾向で更新されていくデータ（演算データ）であり、また、メモリデータの特徴を表す情報（特徴情報）として、メモリデータそのものを用いている。
【００１８】
そして、この通信システムにおいて、子電子装置は、予め定められたタイミング毎に、親電子装置へ、自装置が現在内蔵しているメモリデータを送信し、親電子装置は、その子電子装置からのメモリデータを受信すると共に、今回受信したメモリデータの値Ｄ[n]と、前回受信して記憶手段に改竄有無判定用基準情報として記憶しておいたメモリデータの値Ｄ[n-1]との関係が、前記変化傾向に合った関係になっていなければ、子電子装置に内蔵されているメモリデータが改竄されたと判定する。
【００１９】
例えば、メモリデータの変化傾向が増加であるならば、「Ｄ[n]＜Ｄ[n-1]」の関係になっている場合に、改竄と判定することができ、逆に、メモリデータの変化傾向が減少であるならば、「Ｄ[n]＞Ｄ[n-1]」の関係になっている場合に、改竄と判定することができる。
【００２０】
このような通信システムによれば、子電子装置の動作中に値が更新される演算データが、その子電子装置の動作中に改竄されたとしても、その改竄を確実に検出することができる。
【００２１】
次に、請求項６の通信システムでは、メモリデータの特徴を表す情報として、そのメモリデータの一方向性関数による関数値（メモリデータを引数として一方向性関数の処理を行った結果の値）を用いている。
【００２２】
そして、この通信システムにおいて、子電子装置は、予め定められたタイミング毎に、自装置が現在内蔵しているメモリデータの一方向性関数による関数値を算出すると共に、前回算出した関数値（以下、旧関数値という）Ｖoldを前記メモリデータの格納先である記憶媒体から読み出して、その読み出した旧関数値Ｖoldと、今回算出した関数値（以下、新関数値という）Ｖnewとを、親電子装置に送信し、更に、今回算出した新関数値Ｖnewを次回に送信する旧関数値Ｖoldとして前記記憶媒体に更新記憶する。
【００２３】
また、親電子装置は、子電子装置からの新関数値Ｖnew及び旧関数値Ｖoldを受信すると共に、今回受信した旧関数値Ｖold[n]と、前回受信して記憶手段に改竄有無判定用基準情報として記憶しておいた新関数値（即ち、前回の新関数値）Ｖnew[n-1]とを比較して、その両関数値Ｖold[n], Ｖnew[n-1]が一致していなければ、子電子装置に内蔵されているメ

モリデータが改竄されたと判定する。つまり、子電子装置にて改竄検出対象のメモリデータが格納された記憶媒体が正常であれば、子電子装置から今回受信する旧関数値Ｖold[n]と、子電子装置から前回受信した新関数値Ｖnew[n-1]とは同じはずであるため、その関係が崩れたならば、改竄と判定している。

【００２４】

このような通信システムによれば、メモリデータの特徴を表す情報として一方向性関数による関数値を用いるにも拘わらず、子電子装置内の演算データが、その子電子装置の動作中に改竄されたことを検出することができるようになる。具体的には、第三者が、子電子装置内の演算データを改竄するために、その子電子装置の記憶媒体のデータを書き換えたり該記憶媒体を交換したりすると、親電子装置にて、メモリデータが改竄されたと判定されるからである。

【００２５】

つまり、一方向性関数の特性上、結果値である関数値からは引数である元のメモリデータを逆算することはできないため、前述した請求項５の通信システムにおいて、子電子装置から親電子装置へ、ただ単に、メモリデータの代わりに、そのメモリデータの一方向性関数による関数値を送信するようにしたのでは、改竄の有無を判定することができないが、請求項６の通信システムによれば改竄検出が可能となる。

【００２６】

ところで、親電子装置の記憶手段として、耐タンパ性の記憶装置（いわゆる耐タンパ性モジュール（Tamper Resistant Module））を用いれば、メモリデータの改竄に対する保護機能を一層高めることができる。つまり、子電子装置内のメモリデータの改竄に合わせて、親電子装置側の改竄有無判定用基準情報も改竄し、親電子装置にて改竄と判定されないようにする、といった第三者の不正行為を防止できるからである。

【発明を実施するための最良の形態】

【００２７】

以下に、本発明が適用された実施形態の通信システムについて説明する。尚、本実施形態の通信システムは、自動車に搭載された複数のＥＣＵをノードとした車載ＬＡＮを成すものである。

【００２８】

まず図１は、第１実施形態の通信システム１の構成を表すブロック図である。

本第１実施形態の通信システム１は、自動変速機を制御するＥＣＴ・ＥＣＵ１１、エンジンを制御するエンジンＥＣＵ１２、メータの表示を制御するメータＥＣＵ１３、及び車両の走行距離を積算する距離積算ＥＣＵ１４が、通信ラインＬ１に接続された制御系ネットワークＮ１と、ナビゲーション装置に関する制御を行うナビＥＣＵ１５、及び車両外部の情報センタに設置されている無線通信装置との通信を制御するテレマティクスＥＣＵ１６が、通信ラインＬ２に接続されたマルチメディア系ネットワークＮ２とを備えている。

【００２９】

更に、上記両通信ラインＬ１，Ｌ２には、ゲートウェイ（ＧＷ）２１が接続されており、制御系ネットワークＮ１のＥＣＵ１１～１４とマルチメディア系ネットワークＮ２のＥＣＵ１５，１６は、そのゲートウェイ２１を介して通信できるようになっている。

【００３０】

一方、各ＥＣＵ１１～１６には、自装置に関する各種処理を実行するマイコン（以下、ＣＰＵという）１１ａ～１６ａが搭載されている。尚、図示は省略しているが、ＣＰＵ１１ａ～１６ａには、実行対象のプログラムが格納されたＲＯＭやデータを一時記憶するためのＲＡＭなどが内蔵されている。更に、各ＥＣＵ１１～１６には、ＣＰＵ１１ａ～１６ａが演算するデータ（演算データ）の全部又は一部を継続的に保存するためのデータ書き換え可能な不揮発性メモリとして、ＥＥＰＲＯＭ１１ｂ～１６ｂも搭載されている。そして、そのＥＥＰＲＯＭ１１ｂ～１６ｂには、ＥＣＵ１１～１４毎に用途は異なるが、ＣＰＵ１１ａ～１６ａが実行するプログラムの一部や固定のデータも記憶される。また、ゲートウェイ２１にも、ＥＣＵ１１～１６と同様に、ＣＰＵ２１ａ及びＥＥＰＲＯＭ２１ｂが

搭載されている。

【００３１】

そして、本通信システム１では、例えば、ＥＣＴ・ＥＣＵ１１が、車速センサ３１からの信号に基づき車速を検出して、その検出した車速値を、自装置における制御処理に用いると共に、通信ラインＬ１へ定期的に送信する。また、エンジンＥＣＵ１２が、水温センサ３２からの信号に基づきエンジンの冷却水温を検出して、その検出した水温値を、自装置における制御処理に用いると共に、通信ラインＬ１へ定期的に送信する。また更に、距離積算ＥＣＵ１４が、ＥＣＴ・ＥＣＵ１１からの車速値を受信して、その車速値から車両の総走行距離を積算し、その距離積算値を通信ラインＬ１へ定期的に送信する。尚、「背景技術」の欄でも述べたように、距離積算ＥＣＵ１４では、算出した距離積算値をＥＥＰＲＯＭ１４ｂに記憶して継続的に保存する。そして、メータＥＣＵ１３が、距離積算ＥＣＵ１４からの距離積算値をオドメータに表示させると共に、ＥＣＴ・ＥＣＵ１１からの車速値を車速メータに表示させ、更に、エンジンＥＣＵ１２からの水温値を水温メータに表示させる。

【００３２】

また、本通信システム１において、制御系ネットワークＮ１のＥＣＵ１１～１４とゲートウェイ２１は、車両のイグニッションスイッチ（図示省略）がオンされると、バッテリからの電源供給が開始されて初期状態から動作を開始（いわゆるイニシャルスタート）するようになっている。

【００３３】

そして、イグニッションスイッチがオフされると、ＥＣＵ１１～１４及びゲートウェイ２１の各々にて終了処理が行われた後、その各ＥＣＵ１１～１４及びゲートウェイ２１への電源供給が停止されて、それらが動作を停止するようになっている。

【００３４】

尚、こうした電源供給の開始／停止は、例えば下記（１）～（５）の構成及び手順で実現されている。

（１）まず、ＥＣＵ１１～１４及びゲートウェイ２１には、バッテリからの電源が、電源供給用のリレー（以下、給電用リレーという）を介して供給されるようになっている。

【００３５】

そして、イグニッションスイッチがオンされると、上記給電用リレーがオンして、ＥＣＵ１１～１４及びゲートウェイ２１にバッテリからの電源が供給され、その結果、ＥＣＵ１１～１４及びゲートウェイ２１が動作を開始するようになっている。

【００３６】

（２）また、イグニッションスイッチのオンに伴いＥＣＵ１１～１４及びゲートウェイ２１が動作を開始すると、それらのうちの少なくとも１つ（本実施形態では例えばゲートウェイ２１）が、上記給電用リレーをオン状態に保持させる。尚、このように給電用リレーをオン状態に保持させる自己保持制御を担う電子装置（この例ではゲートウェイ２１）には、イグニッションスイッチのオン／オフ状態を示すイグニッションスイッチ信号が入力されている。

【００３７】

（３）その後、イグニッションスイッチがオフされると、そのことをゲートウェイ２１が検知する。そして、ゲートウェイ２１は、イグニッションスイッチがオフされたことを示すスイッチ情報を通信ラインＬ１に送信して、そのこと（即ち、イグニッションスイッチがオフされたこと）をＥＣＵ１１～１４に報知すると共に、自装置の終了処理を実行する。

【００３８】

（４）また、ＥＣＵ１１～１４は、ゲートウェイ２１からの上記スイッチ情報によって、イグニッションスイッチがオフされたことを検知すると、各自の終了処理を実行し、その終了処理が完了すると、その旨を示す処理完了信号をゲートウェイ２１へ送信する。

【００３９】

（５）そして、ゲートウェイ２１は、ＥＣＵ１１～１４の全てから上記処理完了信号が送信されたことを検知し、且つ、自装置の終了処理も完了したならば、上記給電用リレーをオフさせる。すると、ＥＣＵ１１～１４及びゲートウェイ２１への電源供給が停止されることとなる。

【００４０】

一方、マルチメディア系ネットワークＮ２のＥＣＵ１５，１６には、車両のアクセサリ系電源ライン（即ち、車両のキーがキーシリンダにおけるアクセサリ位置又はイグニッション位置に操作されている時にバッテリと接続される電源ライン）から電源が供給されるようになっている。また、ゲートウェイ２１への電源供給が停止されて該ゲートウェイ２１が動作を停止している時（即ち、制御系ネットワークＮ１の休止時）には、そのゲートウェイ２１においてマルチメディア系ネットワークＮ２の通信ラインＬ２に接続された通信回路（図示省略）の出力がハイインピーダンス状態となり、その通信ラインＬ２に影響を与えないようになっている。

【００４１】

ここで特に、本通信システム１では、制御系ネットワークＮ１のＥＣＵ１１～１４に内蔵されているプログラムやデータが改竄されたことを検出するために、その各ＥＣＵ１１～１４とゲートウェイ２１とが図２及び図３に示す処理を実行するようになっている。

【００４２】

尚、それら改竄検出用の処理は、実際には、ＥＣＵ１１～１４とゲートウェイ２１の各々に搭載されたＣＰＵ１１ａ～１４ａ，２１ａが自己に内蔵のＲＯＭに格納されているプログラムを実行することで行われる。また、本第１実施形態では、各ＥＣＵ１１～１４のＥＥＰＲＯＭ１１ａ～１４ａ内の全データが改竄検出対象であるものとして説明するが、ＥＥＰＲＯＭ１１ｂ～１４ｂ内のデータの一部を改竄検出対象としても良い。

【００４３】

そこで次に、改竄検出のための処理について説明する。

まず、イグニッションスイッチがオンされてＥＣＵ１１～１４が動作を開始すると、その各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが、図２（Ａ）の処理をそれぞれ実行する。

【００４４】

そして、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが、図２（Ａ）の処理を開始すると、まずＳ１１０にて、ＲＡＭなどを初期化するための初期化処理を行い、続くＳ１２０にて、自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）に現在記憶されているデータ（即ち、演算データ，固定データ，プログラム）に対し一方向性関数であるハッシュ関数の処理を施して（つまり、そのデータを引数としてハッシュ関数の処理を行い）、そのデータのハッシュ関数による関数値（結果値）であるハッシュ値を算出し、その算出したハッシュ値を、ＥＥＰＲＯＭ内のデータの特徴を表す特徴情報としてゲートウェイ２１に送信する。

【００４５】

次に、続くＳ１３０にて、ゲートウェイ２１から後述する図２（Ｂ）の処理によって送信されて来るチェック結果信号を受信し、そのチェック結果信号が「改竄無し」を示しているか否かを判定する。

【００４６】

そして、チェック結果信号が「改竄無し」を示していたならば（Ｓ１３０：ＹＥＳ）、通常処理を実行する。尚、通常処理とは、そのＥＣＵに特有の処理であり、例えばエンジンＥＣＵ１２ならばエンジンを制御するための処理であり、距離積算ＥＣＵ１４ならば車両の総走行距離を表す距離積算値を算出する処理である。

【００４７】

また、ゲートウェイ２１からのチェック結果信号が「改竄有り」を示していれば（Ｓ１３０：ＮＯ）、Ｓ１４０に移行して、予め定められたフェイルセーフ処理を行う。

一方、イグニッションスイッチがオンされてゲートウェイ２１が動作を開始すると、そのゲートウェイ２１のＣＰＵ２１ａが、図２（Ｂ）の処理を実行する。

【００４８】
そして、ゲートウェイ２１のＣＰＵ２１ａが、図２（Ｂ）の処理を開始すると、まずＳ２１０にて、ＲＡＭなどを初期化するための初期化処理を行い、続くＳ２２０にて、各ＥＣＵ１１～１４から図２（Ａ）のＳ１２０の処理によって送信されて来るハッシュ値をそれぞれ受信する。
【００４９】
次に、続くＳ２３０にて、ＥＣＵ１１～１４の各々について、上記Ｓ２２０で受信したハッシュ値と、当該ゲートウェイ２１のＥＥＰＲＯＭ２１ｂに事前に記憶されている改竄有無判定用基準情報（以下、比較用データともいう）とに基づいて、そのＥＣＵのＥＥＰＲＯＭ内のデータが改竄されたか否かの改竄チェックを行う。
【００５０】
尚、ＥＥＰＲＯＭ２１ｂには、ＥＣＵ１１～１４の各々について、そのＥＣＵがイグニッションスイッチのオンに伴い動作を開始した時点で該ＥＣＵのＥＥＰＲＯＭに記憶されているはずのデータのハッシュ値が、比較用データとして、後述する図３の処理により記憶されている。そして、Ｓ２３０では、ＥＣＵ１１～１４の各々について、上記Ｓ２２０で受信したハッシュ値と、ＥＥＰＲＯＭ２１ｂに記憶されている比較用データとしてのハッシュ値とを比較し、その両ハッシュ値が一致していれば、そのＥＣＵのＥＥＰＲＯＭ内のデータは改竄されていない（改竄無し）と判定し、逆に、両ハッシュ値が不一致ならば、そのＥＣＵのＥＥＰＲＯＭ内のデータが改竄された（改竄有り）と判定する。
【００５１】
そして、続くＳ２４０にて、各ＥＣＵ１１～１４へ、そのＥＣＵについての改竄チェック結果を表すチェック結果信号を送信し、その後、他の処理を実行する。
次に、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａは、イグニッションスイッチがオフされたことを検知すると、図３（Ａ）の処理をそれぞれ実行する。
【００５２】
そして、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが図３（Ａ）の処理を開始すると、まずＳ３１０にて、前述したＳ１２０と同様に、自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）に現在記憶されているデータのハッシュ値を算出し、その算出したハッシュ値を、ＥＥＰＲＯＭ内のデータの特徴を表す特徴情報としてゲートウェイ２１に送信する。
【００５３】
そして、続くＳ３２０にて、自装置の終了処理を実行し、その後、ゲートウェイ２１へ前述した処理完了信号を送信する。すると、その後、ゲートウェイ２１の前述した（５）の機能により、当該ＥＣＵへの電源供給が停止されることとなる。
【００５４】
一方、ゲートウェイ２１のＣＰＵ２１ａは、イグニッションスイッチがオフされたことを検知すると、図３（Ｂ）の処理を実行する。
そして、ゲートウェイ２１のＣＰＵ２１ａが図３（Ｂ）の処理を開始すると、まずＳ４１０にて、各ＥＣＵ１１～１４から図３（Ａ）のＳ３１０の処理によって送信されて来るハッシュ値をそれぞれ受信する。
【００５５】
次に、続くＳ４２０にて、上記Ｓ４１０で受信した各ＥＣＵ１１～１４からのハッシュ値を、そのＥＣＵについての前述した比較用データとして、ＥＥＰＲＯＭ２１ｂにそれぞれ記憶する。そして、続くＳ４３０にて、自装置の終了処理を実行する。
【００５６】
尚、その後、ゲートウェイ２１のＣＰＵ２１ａは、前述した（５）の機能により、給電用リレーをオフさせて、当該ゲートウェイ２１及びＥＣＵ１１～１４への電源供給を停止させることとなる。
【００５７】
つまり、本通信システム１では、イグニッションスイッチがオフされてＥＣＵ１１～１４が動作を停止する直前に、その各ＥＣＵ１１～１４が、ゲートウェイ２１へ、自装置の

ＥＥＰＲＯＭ（１１ｂ～１４ｂ）に格納されているデータ（内蔵データ）の特徴量であるハッシュ値を送信し（Ｓ３１０）、ゲートウェイ２１が、その各ＥＣＵ１１～１４からのハッシュ値を、改竄検出のための比較用データとして、当該ゲートウェイ２１のＥＥＰＲＯＭ２１ｂに記憶するようになっている（Ｓ４１０，４２０）。

【００５８】

そして、イグニッションスイッチがオンされてＥＣＵ１１～１４が動作を開始した際に、その各ＥＣＵ１１～１４が、ゲートウェイ２１へ、自装置のＥＥＰＲＯＭ（１１ｂ～１４ｂ）に格納されているデータの特徴量であるハッシュ値を送信し（Ｓ１２０）、ゲートウェイ２１が、各ＥＣＵ１１～１４について、そのＥＣＵから送信されて来たハッシュ値と、ＥＥＰＲＯＭ２１ｂに記憶されている比較用データ（即ち、そのＥＣＵが動作を停止する直前に送信して来たハッシュ値）とを比較して、その両ハッシュ値が一致していなければ、そのＥＣＵのＥＥＰＲＯＭ内のデータは改竄されていると判定するようになっている（Ｓ２２０，Ｓ２３０）。

【００５９】

このような本通信システム１によれば、各ＥＣＵ１１～１４におけるＥＥＰＲＯＭ（１１ｂ～１４ｂ）内のデータが改竄されたことを、そのデータが、プログラムや固定のデータのみならず、ＥＣＵの動作中に値が変化する演算データであっても、効率良く検出することができる。ＥＥＰＲＯＭ１１ｂ～１４ｂ内のデータが、どのようなものであっても、ＥＣＵ１１～１４が動作を停止している間に違う内容に改竄されたならば、そのＥＣＵが動作を再開した際に、データの改竄がゲートウェイ２１にて確実に検出されるからである。よって、例えば、距離積算ＥＣＵ１４のＥＥＰＲＯＭ１４ｂが不正に交換されて、メータＥＣＵ１３によりオドメータに表示される総走行距離が本当の値よりも小さい値に改竄されてしまう、といった不正行為の発生を確実に検出することができる。

【００６０】

尚、ゲートウェイ２１のＣＰＵ２１ａが図３（Ｂ）の処理を未だ一度も実行していないのに図２（Ｂ）の処理を実行した場合（即ち、車両が完成してから初めてイグニッションスイッチがオンされた場合）には、ＥＥＰＲＯＭ２１ｂには図３（Ｂ）の処理によって比較用データが未だ記憶されていないため、その場合にだけは、図２（Ｂ）におけるＳ２３０の改竄チェックをスキップし、続くＳ２４０では、各ＥＣＵ１１～１４へ、「改竄無し」を示すチェック結果信号を無条件で送信するように構成すれば良い。

【００６１】

また、Ｓ２３０の改竄チェックを１回目だけスキップするのではなく、例えば車両の製造時において、各ＥＣＵ１１～１４のＥＥＰＲＯＭ１１ｂ～１４ｂに記憶されるデータ（演算データ，固定データ，プログラム）の初期値から算出したハッシュ値を、ゲートウェイ２１のＥＥＰＲＯＭ２１ｂへ、比較用データの初期値として記憶しておいても良い。そして、このようにすれば、イグニッションスイッチが初めてオンされた時から、改竄チェックを実施することができる。

【００６２】

一方、本第１実施形態では、ゲートウェイ２１が親電子装置に相当し、ＥＣＵ１１～１４の各々が子電子装置に相当し、ゲートウェイ２１のＥＥＰＲＯＭ２１ｂが、親電子装置の記憶手段に相当している。

【００６３】

また、上記第１実施形態において、図２（Ａ）のＳ１２０と図３（Ａ）のＳ３１０とで、各ＥＣＵ１１～１４がゲートウェイ２１へ送信する特徴情報としては、ハッシュ値でなく、その時点で自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）に記憶されている改竄チェック対象（改竄検出対象）のデータそのものとするように構成しても良い。但し、このようにすると、各ＥＣＵ１１～１４からゲートウェイ２１へ送信されるデータ量が増加すると共に、図３（Ｂ）のＳ４２０でゲートウェイ２１のＥＥＰＲＯＭ２１ｂに記憶しなければならない比較用データの量も増加するため、前述したように、ＥＣＵ１１～１４からゲートウェイ２１へはハッシュ値を送信するようにした方が有利である。

【００６４】
　また、各ＥＣＵ１１～１４がゲートウェイ２１へ送信する特徴情報を算出するための関数としては、引数が異なれば必ず違う結果が得られる関数であれば、ハッシュ関数以外の他の関数を用いても良い。
【００６５】
　一方、ゲートウェイ２１は、例えば常時動作するように構成しても良い。
　また、ゲートウェイ２１は、各ＥＣＵ１１～１４から図３（Ａ）のＳ３１０で送信される特徴情報を確実に受信してＥＥＰＲＯＭ２１ｂに記憶できるのであれば、マルチメディア系ネットワークＮ２のＥＣＵ１５，１６と同様に、アクセサリ系電源ラインから電源が供給されて動作するようにしても良い。
【００６６】
　次に、第２実施形態の通信システムについて説明する。尚、第２実施形態の通信システムは、第１実施形態の通信システム１とハードウェア構成は同じであるため、以下の説明において、各部の符号は第１実施形態と同じものを用いる。
【００６７】
　第２実施形態の通信システム１は、第１実施形態と比較すると、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが、前述した処理に加えて更に図４（Ａ）の処理を実行し、ゲートウェイ２１のＣＰＵ２１ａが、前述した処理に加えて更に図４（Ｂ）の処理を実行する。尚、図４の処理も、ＣＰＵ１１ａ～１４ａ，２１ａが自己に内蔵のＲＯＭに格納されているプログラムを実行することで行われる。
【００６８】
　即ち、まず、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａは、イグニッションスイッチがオンされている動作期間中において、例えば一定周期の定期送信タイミングが到来する毎に、図４（Ａ）の処理をそれぞれ実行する。
【００６９】
　そして、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが、図４（Ａ）の処理を開始すると、Ｓ５１０にて、自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）に現在記憶されているデータのうち、自装置の動作中に値が所定の変化傾向で更新されていく演算データを、動作中に改竄チェックを行うべきデータ（以下、動作中改竄チェック対象データという）としてゲートウェイ２１に送信し、その後、当該図４（Ａ）の処理を終了する。例えば、距離積算ＥＣＵ１４ならば、上記Ｓ５１０の処理により、ＥＥＰＲＯＭ１４ｂに記憶されている距離積算値を送信することとなる。
【００７０】
　一方、ゲートウェイ２１のＣＰＵ２１ａは、イグニッションスイッチがオンされている期間中に図４（Ｂ）の処理を実行する。
　そして、ゲートウェイ２１のＣＰＵ２１ａが、図４（Ｂ）の処理を開始すると、まずＳ６１０にて、各ＥＣＵ１１～１４から上記図４（Ａ）の処理で送信されて来る動作中改竄チェック対象データの何れかを受信するまで待つ。
【００７１】
　そして、動作中改竄チェック対象データを受信したならば（Ｓ６１０：ＹＥＳ）、Ｓ６２０に進んで、今回受信した動作中改竄チェック対象データの値Ｄ[n]と、その動作中改竄チェック対象データを前回受信した際にＥＥＰＲＯＭ２１ｂに記憶しておいた該データの前回の受信値（改竄有無判定用基準情報に相当）Ｄ[n-1]とを比較することにより、その動作中改竄チェック対象データがＥＣＵ側で改竄されたか否かの改竄チェックを行う。
【００７２】
　具体的には、両値Ｄ[n]，Ｄ[n-1]の関係が、その動作中改竄チェック対象データの変化傾向に合った関係になっていなければ、改竄されたと判定する。例えば、受信した動作中改竄チェック対象データが距離積算ＥＣＵ１４からの距離積算値であったとすると、その距離積算値の変化傾向は増加であるため、「Ｄ[n]＜Ｄ[n-1]」の関係になっている場合に、「改竄有り」と判定する。

【００７３】
そして、続くＳ６３０にて、上記Ｓ６２０での改竄チェックの結果を判定し、改竄チェック結果が「改竄無し」であったならば、Ｓ６４０に進んで、今回受信して改竄無しと判定した動作中改竄チェック対象データの値Ｄ[n]を、その動作中改竄チェック対象データの前回の受信値Ｄ[n-1]としてＥＥＰＲＯＭ２１ｂに更新記憶し、その後Ｓ６１０に戻る。尚、このＳ６４０で記憶された値Ｄ[n-1]が、次に同じ種類の動作中改竄チェック対象データを受信した際に、上記Ｓ６２０での改竄チェックに用いられる。
【００７４】
また、上記Ｓ６３０にて、改竄チェック結果が「改竄有り」であったと判定したならば（Ｓ６３０：ＮＯ）、Ｓ６５０に移行し、今回受信して改竄有りと判定した動作中改竄チェック対象データの送信元であるＥＣＵ（或いは更にそのＥＣＵから情報が提供される他のＥＣＵ）へ、改竄報知信号を送信し、その後、Ｓ６１０へ戻る。
【００７５】
すると、その改竄報知信号を受信したＥＣＵでは、所定のフェイルセーフ処理を行うこととなる。
以上のような第２実施形態の通信システム１によれば、ＥＣＵ１１～１４の動作中に値が更新される演算データが、そのＥＣＵの動作中に改竄されたとしても、その改竄を確実に検出することができるようになる。
【００７６】
尚、図４（Ｂ）の処理において、Ｓ６４０では、今回受信した動作中改竄チェック対象データの値Ｄ[n]を、前回の受信値Ｄ[n-1]としてＲＡＭに記憶すると共に、Ｓ６２０では、そのＲＡＭから前回の受信値Ｄ[n-1]を読み出すようにしても良い。そして、この場合には、ゲートウェイ２１におけるＣＰＵ２１ａ内の上記ＲＡＭが、親電子装置の記憶手段（請求項５）に相当することとなる。
【００７７】
次に、第３実施形態の通信システムについて説明する。尚、第３実施形態の通信システムも、第１実施形態の通信システム１とハードウェア構成は同じであるため、以下の説明において、各部の符号は第１実施形態と同じものを用いる。
【００７８】
第３実施形態の通信システム１は、第１実施形態と比較すると、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが、前述した処理に加えて更に図５（Ａ）の処理を実行し、ゲートウェイ２１のＣＰＵ２１ａが、前述した処理に加えて更に図５（Ｂ）の処理を実行する。尚、図５の処理も、ＣＰＵ１１ａ～１４ａ，２１ａが自己に内蔵のＲＯＭに格納されているプログラムを実行することで行われる。
【００７９】
即ち、まず、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａは、イグニッションスイッチがオンされている動作期間中において、例えば一定周期の定期送信タイミングが到来する毎に、図５（Ａ）の処理をそれぞれ実行する。
【００８０】
そして、各ＥＣＵ１１～１４のＣＰＵ１１ａ～１４ａが、図５（Ａ）の処理を開始すると、まずＳ７１０にて、自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）に現在記憶されているデータに対しハッシュ関数の処理を施して、そのデータのハッシュ値を算出する。尚、ここでは、各ＥＣＵ１１～１４のＥＥＰＲＯＭ１１ａ～１４ａ内の全データを改竄検出対象として、その全データのハッシュ値を算出するものとするが、ＥＥＰＲＯＭ１１ｂ～１４ｂ内のデータの一部を改竄検出対象として、その一部のデータのハッシュ値を算出するようにしても良い。
【００８１】
次に、Ｓ７２０にて、前回のＳ７１０で算出したハッシュ値（以下、旧ハッシュ値という）Holdを自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）から読み出し、続くＳ７３０にて、その読み出した旧ハッシュ値Holdと、今回のＳ７１０で算出したハッシュ値（以下、

新ハッシュ値という）Hnewとを、ゲートウェイ２１に送信する。

【００８２】

そして、続くＳ７４０にて、今回のＳ７１０で算出した新ハッシュ値Hnewを、次回のＳ７２０で読み出す旧ハッシュ値Holdとして自装置のＥＥＰＲＯＭ（１１ａ～１４ａ）に更新記憶し、その後、当該図５（Ａ）の処理を終了する。

【００８３】

一方、ゲートウェイ２１のＣＰＵ２１ａは、イグニッションスイッチがオンされている期間中に図５（Ｂ）の処理を実行する。

そして、ゲートウェイ２１のＣＰＵ２１ａが、図５（Ｂ）の処理を開始すると、まずＳ８１０にて、各ＥＣＵ１１～１４から上記図５（Ａ）の処理で送信されて来る新・旧ハッシュ値Hnew, Holdを受信するまで待つ。

【００８４】

そして、ＥＣＵ１１～１４のうちの何れかからの新・旧ハッシュ値Hnew, Holdを受信したならば（Ｓ８１０：ＹＥＳ）、Ｓ８２０に進んで、その新・旧ハッシュ値Hnew, Holdの送信元であるＥＣＵについてのデータ改竄チェックを行う。

【００８５】

具体的には、今回受信した新・旧ハッシュ値Hnew[n], Hold[n], のうちの旧Hold[n]と、前回受信した新・旧ハッシュ値Hnew[n-1], Hold[n-1]のうちでＥＥＰＲＯＭ２１ａに記憶しておいた新ハッシュ値Hnew[n-1]とを比較し、その両ハッシュ値Hold[n], Hnew[n-1]が一致していなければ、今回受信した新・旧ハッシュ値Hnew[n], Hold[n]の送信元であるＥＣＵにて、ＥＥＰＲＯＭ内のデータが改竄されたと判定する。つまり、ＥＣＵ１１～１４にてＥＥＰＲＯＭ１１ａ～１４ａが正常であれば、そのＥＣＵから今回受信する旧ハッシュ値Hold[n]と、そのＥＣＵから前回受信した新ハッシュ値Hnew[n-1]とは同じはずであるため、その関係が崩れたならば、改竄と判定している。

【００８６】

そして、続くＳ８３０にて、上記Ｓ８２０での改竄チェックの結果を判定し、改竄チェック結果が「改竄無し」であったならば、Ｓ８４０に進んで、今回受信した新ハッシュ値Hnew[n]を、それの送信元のＥＣＵについての新ハッシュ値の前回受信値Hnew[n-1]としてＥＥＰＲＯＭ２１ｂに更新記憶し、その後Ｓ８１０に戻る。尚、このＳ８４０で記憶された値Hnew[n-1]が、次に同じＥＣＵについてのデータ改竄チェックを行う際に、上記Ｓ８２０で用いられることとなる。

【００８７】

また、上記Ｓ８３０にて、改竄チェック結果が「改竄有り」であったと判定したならば（Ｓ８３０：ＮＯ）、Ｓ８５０に移行し、今回受信した新・旧ハッシュ値Hnew, Holdの送信元であるＥＣＵ（或いは更にそのＥＣＵから情報が提供される他のＥＣＵ）へ、改竄報知信号を送信し、その後、Ｓ８１０へ戻る。

【００８８】

すると、その改竄報知信号を受信したＥＣＵでは、所定のフェイルセーフ処理を行うこととなる。

以上のような第３実施形態の通信システム１によれば、ＥＣＵ１１～１４からゲートウェイ２１へデータの特徴を表す特徴情報としてハッシュ値を送信するようにしているにも拘わらず、ＥＣＵ１１～１４内の演算データが、そのＥＣＵの動作中に改竄されたことを検出することができるようになる。具体的には、第三者が、ＥＣＵ１１～１４内の演算データを改竄するために、そのＥＣＵのＥＥＰＲＯＭのデータを書き換えたり該ＥＥＰＲＯＭを交換したりすると、ゲートウェイ２１にて、図５（Ｂ）のＳ８２０の処理により、データが改竄されたと判定されるからである。

【００８９】

つまり、ハッシュ関数の特性上、ハッシュ値からは元のデータを逆算することはできないため、仮に、前述した第２実施形態において、各ＥＣＵ１１～１４が図４（Ａ）の処理でゲートウェイ２１へ、ただ単に、演算データの代わりに、その演算データのハッシュ値

を送信するようにしたのでは、改竄の有無を判定することができないが、本第３実施形態の通信システム１によれば、動作中における演算データの改竄検出が可能となる。

【００９０】

尚、図５（Ａ）のＳ７１０では、各ＥＣＵ１１～１４のＥＥＰＲＯＭ１１ａ～１４ａ内のデータのうち、特定の演算データだけを改竄検出対象として、その演算データのハッシュ値を算出するようにしても良い。また、図５（Ａ）のＳ７１０で用いる関数は、ハッシュ関数に限らず、他の一方向性関数でも良い。

【００９１】

以上、本発明の一実施形態について説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲において、種々なる態様で実施し得ることは勿論である。

【００９２】

例えば、ＥＣＵ１１～１４に内蔵されたプログラムや固定のデータだけを改竄検出対象とするのであれば、下記（Ａ）～（Ｃ）のように構成することができる。

（Ａ）まず、車両の製造時やカーディーラーなどにおいて、ゲートウェイ２１のＥＥＰＲＯＭ２１ｂに、各ＥＣＵ１１～１４について、そのＥＣＵに内蔵される改竄検出対象のデータと同じデータ（又は該データの特徴を表す関数値（例えばハッシュ値））を、改竄有無判定用基準情報として予め記憶しておく。

【００９３】

（Ｂ）各ＥＣＵ１１～１４は、予め定められたタイミング毎（例えば一定時間毎や起動時毎）に、自装置に内蔵されている改竄検出対象のデータ（又は該データの特徴を表す関数値）をゲートウェイ２１へ送信する。

【００９４】

（Ｃ）ゲートウェイ２１は、何れかのＥＣＵ１１～１４から、改竄検出対象のデータ（又は該データの関数値）を受信すると、そのデータ（又は関数値）を送信したＥＣＵに該当する改竄有無判定用基準情報をＥＥＰＲＯＭ２１ａから読み出して、その改竄有無判定用基準情報と、上記受信したデータ（又は関数値）とを比較し、両者が不一致ならば、ＥＣＵにてデータが改竄されていると判定する。

【００９５】

つまり、プログラムや固定のデータだけを改竄検出対象とするのであれば、ゲートウェイ２１側の改竄有無判定用基準情報は特に更新する必要がなく、また、ゲートウェイ２１側で行う改竄有無の判定も、各ＥＣＵ１１～１４から送信されて来る情報と改竄有無判定用基準情報との一致／不一致を確認するだけで済む。

【００９６】

一方、ゲートウェイ２１のＥＥＰＲＯＭ２１ｂとして、耐タンパ性モジュールを用いれば、ＥＣＵ内のメモリデータの改竄に合わせて、ゲートウェイ２１側の改竄有無判定用基準情報も改竄し、ゲートウェイ２１にて改竄と判定されないようにする、といった第三者の不正行為を防止することができるため、データ改竄に対する保護機能を一層高めることができる。

【００９７】

また、データ改竄を検出するためのＥＣＵ１１～１４とゲートウェイ２１との間の通信として、通信データを暗号化する暗号化通信を用いても良い。

また更に、上記各実施形態では、制御系ネットワークＮ１のＥＣＵ１１～１４についてのみデータ改竄の検出を行うようにしていたが、マルチメディア系ネットワークＮ２のＥＣＵ１５，１６についても同様にデータ改竄の検出を実施するように構成しても良い。

【００９８】

また、上記各実施形態では、ゲートウェイ２１が改竄検出用の親電子装置となっていたが、ゲートウェイが存在しない通信システムならば、何れか１つのＥＣＵが親電子装置となるように構成すれば良い。但し、ゲートウェイを親電子装置にすれば、子電子装置としての各ＥＣＵから情報を収集し易いという点で有利である。

【図面の簡単な説明】

【００９９】

【図１】第１実施形態の通信システムの構成を表すブロック図である。

【図２】第１実施形態における各ＥＣＵのＣＰＵとゲートウェイのＣＰＵとが、イグニッションスイッチのオンに伴い動作を開始した際にそれぞれ実行する処理を表すフローチャートである。

【図３】第１実施形態における各ＥＣＵのＣＰＵとゲートウェイのＣＰＵとが、イグニッションスイッチのオフに伴い動作を停止する直前にそれぞれ実行する処理を表すフローチャートである。

【図４】第２実施形態における各ＥＣＵのＣＰＵとゲートウェイのＣＰＵとがそれぞれ実行する処理を表すフローチャートである。

【図５】第３実施形態における各ＥＣＵのＣＰＵとゲートウェイのＣＰＵとがそれぞれ実行する処理を表すフローチャートである。

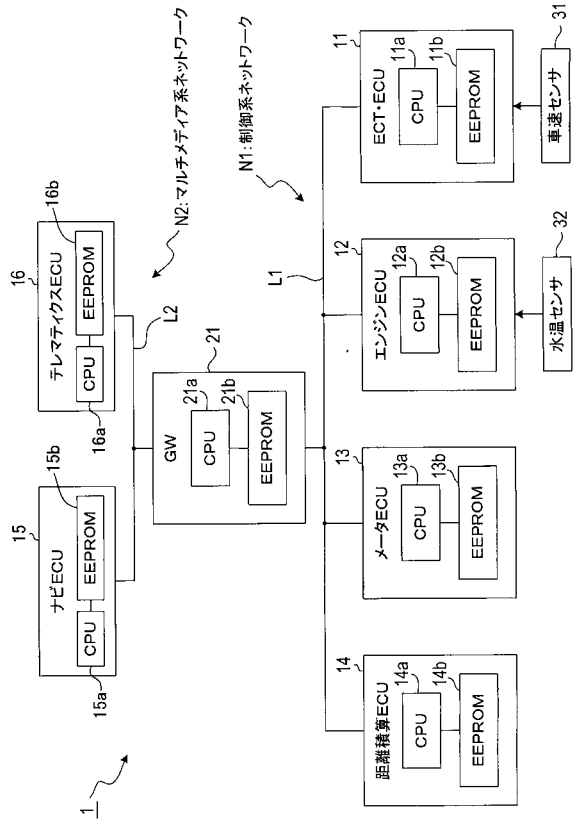
【図６】従来技術を説明する説明図である。

【符号の説明】

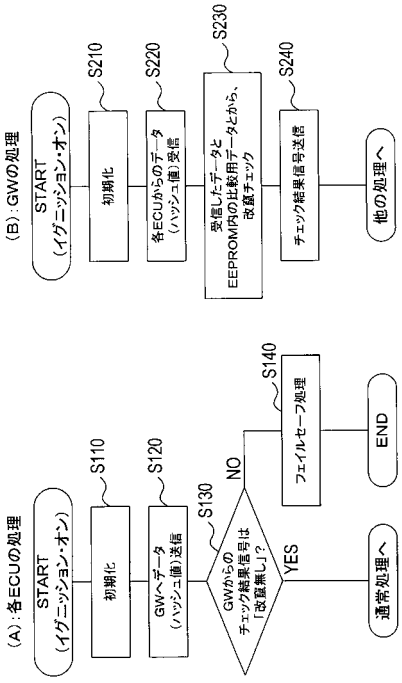
【０１００】

１…通信システム、Ｌ１，Ｌ２…通信ライン、Ｎ１…制御系ネットワーク、Ｎ２…マルチメディア系ネットワーク、１１…ＥＣＴ・ＥＣＵ、１２…エンジンＥＣＵ、１３…メータＥＣＵ、１４…距離積算ＥＣＵ、１５…ナビＥＣＵ、１６…テレマティクスＥＣＵ、２１…ゲートウェイ、３１…車速センサ、３２…水温センサ、１１ａ～１６ａ，２１ａ…ＣＰＵ、１１ｂ～１６ｂ，２１ｂ…ＥＥＰＲＯＭ

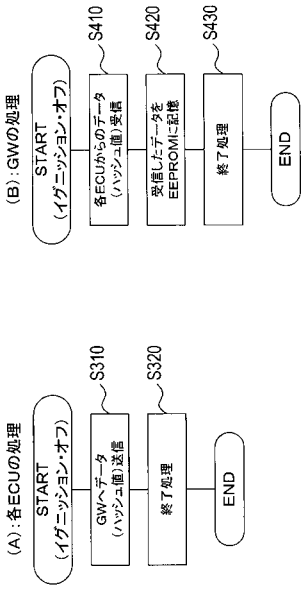
【図１】



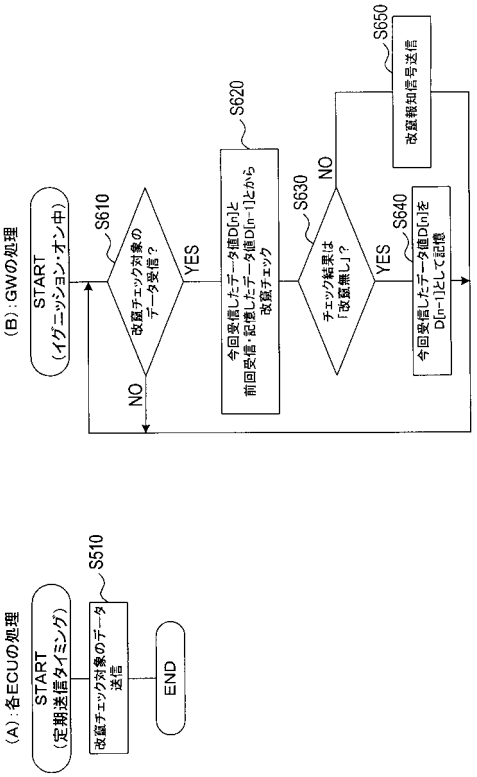
【図２】



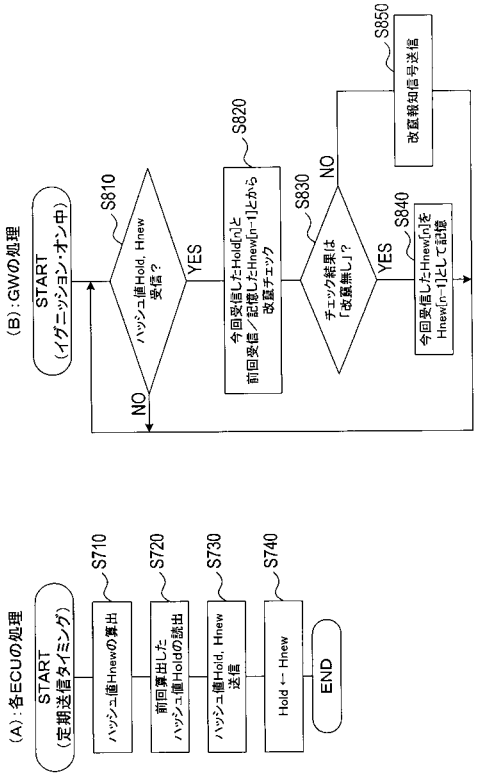
【図３】


(A):各ECUの処理
START
(イグニッション・オフ)
S310
GWハッシュ値データ送信
S320
終了処理
END
(B):GWの処理
START
(イグニッション・オフ)
S410
各ECUからのハッシュ値データ受信
S420
受信したデータをEEPROMに記憶
S430
終了処理
END

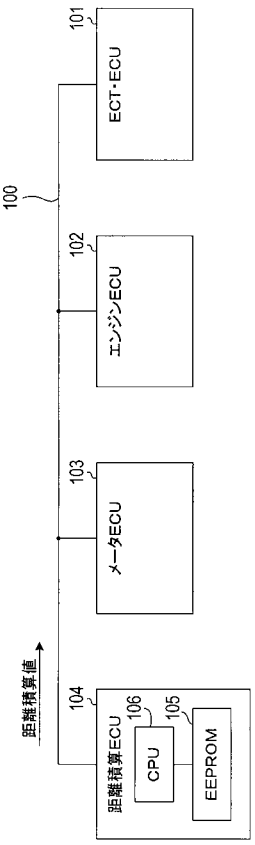
【図４】


(A):各ECUの処理
START
(定期送信タイミング)
S510
改竄チェック対象のデータ送信
END
(B):GWの処理
START
(イグニッション・オン中)
S610
改竄チェック対象のデータ受信？
NO
YES
S620
今回受信したデータ値D[n]と前回受信・記憶したデータ値D[n-1]とから改竄チェック
S630
チェック結果は「改竄無し」？
NO
YES
S640
今回受信したデータ値D[n]をD[n-1]として記憶
S650
改竄報知信号送信

【図５】


(A):各ECUの処理
START
(定期送信タイミング)
S710
ハッシュ値Hnewの算出
S720
前回算出したハッシュ値Holdの読出
S730
ハッシュ値Hold, Hnewの送信
S740
Hold ← Hnew
END
(B):GWの処理
START
(イグニッション・オン中)
S810
ハッシュ値Hold, Hnewの受信？
NO
YES
S820
今回受信したHold[n]と前回受信／記憶したHnew[n-1]とから改竄チェック
S830
チェック結果は「改竄無し」？
NO
YES
S840
今回受信したHnew[n]をHnew[n-1]として記憶
S850
改竄報知信号送信

【図６】


100
101
ECT-ECU
102
エンジンECU
103
メータECU
104
距離積算ECU
106
CPU
105
EEPROM
距離積算値