(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5479408号
(P5479408)

(45)発行日　平成26年4月23日(2014.4.23)　(24)登録日　平成26年2月21日(2014.2.21)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
B60R 16/023	(2006.01)	B60R	16/02	665Z
G06F 21/44	(2013.01)	G06F	21/20	144C

請求項の数 14　(全 24 頁)

(21)出願番号　特願2011-150357(P2011-150357)
(22)出願日　平成23年7月6日(2011.7.6)
(65)公開番号　特開2013-17140(P2013-17140A)
(43)公開日　平成25年1月24日(2013.1.24)
審査請求日　平成25年2月13日(2013.2.13)

(73)特許権者　509186579
日立オートモティブシステムズ株式会社
茨城県ひたちなか市高場２５２０番地
(74)代理人　100091096
弁理士　平木　祐輔
(74)代理人　100105463
弁理士　関谷　三男
(74)代理人　100102576
弁理士　渡辺　敏章
(72)発明者　三宅　淳司
茨城県ひたちなか市高場２５２０番地　日立オートモティブシステムズ株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】車載ネットワークシステム

(57)【特許請求の範囲】
【請求項１】
車両の動作を制御する車載制御装置と、
前記車載制御装置が前記車両の車載ネットワークに参加する正当権限を有するか否かを認証する構成管理装置と、
を備え、
前記構成管理装置は、
前記車載制御装置を前記車載ネットワークに参加させる登録装置から、前記車載制御装置を前記車載ネットワークに参加させるよう要求する登録要求を受け取ると、前記登録装置に対する認証を実施した上で、前記車載制御装置に固有の構成証明データを作成して前記登録装置に返信し、
前記登録装置は、
前記車載制御装置を前記車載ネットワークに参加させるときのみ前記車載ネットワークに対して接続される装置として構成されており、
前記登録要求に対する前記構成管理装置からの返信において前記構成管理装置から前記構成証明データを受け取って前記車載制御装置に中継し、
前記車載制御装置は、
前記登録装置から前記構成証明データを受け取ってメモリ内に格納し、
前記構成管理装置はさらに、
前記構成証明データを用いて前記車載制御装置を認証する

ことを特徴とする車載ネットワークシステム。
【請求項２】
前記構成管理装置は、
前記車載制御装置を認証する認証手順とは異なる認証手順によって前記登録装置を認証する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項３】
前記構成証明データは、
前記構成管理装置が前記車載制御装置を認証する際のパスワード、または
前記構成管理装置が前記車載制御装置を認証する際に実施するチャレンジ＆レスポンス認証において前記車載制御装置がレスポンスを生成する際に用いる共通鍵
のうち少なくともいずれかを含む
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項４】
前記構成証明データは、
前記車載制御装置が前記車載ネットワーク上でメッセージ認証符号を送受信する際に、メッセージからデジタル署名を作成するために用いる共通鍵、または
前記車載制御装置が前記車載ネットワーク上で暗号化通信を実施するために用いる共通鍵
のうち少なくともいずれかを含む
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項５】
前記構成管理装置は、
前記車載制御装置毎、前記車載制御装置が備えるソフトウェアのバージョン毎、前記車両の車種毎、または前記車両を個体毎に識別する車両識別番号毎に異なる値を出力する一方向性関数を用いて、前記構成証明データを生成する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項６】
前記構成管理装置は、
前記車載ネットワークに参加している前記車載制御装置から、前記構成証明データまたは前記構成証明データを用いて生成された認証データを受信することにより、前記車載ネットワークに参加している前記車載制御装置を認証し、
前記車載ネットワークに参加している前記車載制御装置に対して前記構成証明データまたは前記認証データを送信するように要求してもその応答として前記構成証明データまたは前記認証データを受信することができない場合、前記車載ネットワークに参加している前記車載制御装置から定期的に前記構成証明データまたは前記認証データを受信することができない場合、または前記車載制御装置の認証に失敗した場合は、
前記車載制御装置が改竄された旨を示す警告信号を出力するか、または前記車載制御装置が改竄された旨を記述した通信パケットを前記車載ネットワークに対してブロードキャストする
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項７】
前記車載制御装置は、前記構成証明データまたは前記構成証明データを用いて生成された認証データを用いて前記構成管理装置を認証する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項８】
前記車載制御装置は、
前記構成管理装置から前記構成証明データまたは前記認証データを受信することにより、前記構成管理装置を認証し、
前記構成管理装置に対して前記構成証明データまたは前記認証データを送信するよう

に要求してもその応答として前記構成証明データまたは前記認証データを受信することができない場合、前記構成管理装置から定期的に前記構成証明データまたは前記認証データを受信することができない場合、または前記構成管理装置の認証に失敗した場合は、
　前記構成管理装置が改竄された旨を示す警告信号を出力するか、または前記構成管理装置が改竄された旨を記述した通信パケットを前記車載ネットワークに対してブロードキャストするか、または以後の前記構成管理装置からの指示に従わない
ことを特徴とする請求項７記載の車載ネットワークシステム。
【請求項９】
前記構成証明データは、前記構成管理装置と前記車載制御装置の間で送受信する通信データの種別を記述した識別番号を含み、
前記構成管理装置と前記車載制御装置は、前記識別番号を指定した通信データによって前記構成証明データを送受信する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項１０】
前記構成管理装置は、
　前記車載ネットワークに接続する装置間の通信を中継する通信ゲートウェイとして動作し、
　前記登録装置の認証に失敗した場合は、前記登録装置と前記車載制御装置との間の通信を遮断する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項１１】
前記登録装置は、前記車載制御装置が搭載しているソフトウェアを書き換える書換装置としての機能を備える
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項１２】
前記登録装置は、前記車載ネットワークに一時的に接続する通信装置である
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項１３】
前記登録装置は、前記車両の外部に配置され、前記車載ネットワークを経由して前記構成管理装置または前記車載制御装置と通信する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【請求項１４】
前記構成管理装置は、
　前記車載ネットワークに接続する前記車載制御装置の種別および搭載しているソフトウェアのバージョンを管理するデータベースを備え、
　前記登録装置からの要求に応じて前記データベースが格納しているデータを更新し、
　前記登録装置または前記車載制御装置から前記データベースが格納しているデータに対する問い合わせを受け取って前記データベースが格納しているデータを返信する
ことを特徴とする請求項１記載の車載ネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車載ネットワークシステムに関する。
【背景技術】
【０００２】
近年、乗用車、トラック、バス等には、各機能部を制御する車載ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）が多数搭載されている。各ＥＣＵは車載ネットワークを介して相互接続し、協調動作する。
【０００３】
通常、車載ＥＣＵが搭載している制御プログラムは、車載ＥＣＵに内蔵されているマイ

クロコンピュータのフラッシュＲＯＭ（Ｒｅａｄ　Ｏｎｌｅ　Ｍｅｍｏｒｙ）などの記憶装置に格納されている。この制御プログラムのバージョンは、製造者によって管理されており、正規のソフトウェアバージョンを組み合わせることにより、単独機能および車載ネットワークを通じての協調機能が正常に動作するように意図されている。

【０００４】

したがって、意図しないソフトウェアを搭載した車載ＥＣＵ、または意図的に改竄された車載ＥＣＵが車載ネットワークに接続されることは、車両のセキュリティの観点から看過できない。

【０００５】

各車載ＥＣＵが自局のソフトウェアの真正性を外部に証明すること、さらには全ての関連する車載ＥＣＵの真正性を証明することを、構成証明と呼ぶ。構成証明が得られた場合は、製造者によって提供された正しいプログラムを組み合わせ、意図した制御が実施されているという確証となる。

【０００６】

下記特許文献１には、共通鍵または共通鍵生成源を複数の車載ＥＣＵ間で共有し、この情報を共有していると推定されているＥＣＵ間で暗号化通信が成立するか否かにより、上記構成証明を実施する手法が開示されている。

【０００７】

下記特許文献２には、ＫＰＳ（Ｋｅｙ　Ｐｒｅｄｉｓｔｒｉｂｕｔｉｏｎ　Ｓｙｓｔｅｍ）方式の共通鍵配信手法が開示されている。同方式は、特許文献１において共通鍵生成源として利用することができる。

【先行技術文献】

【特許文献】

【０００８】

【特許文献１】特開２０１０－１１４００号公報

【特許文献２】特公平５－４８９８０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００９】

上記特許文献１では、共通鍵または共通鍵生成源を複数のＥＣＵ間で共有させるため、センターサーバなどの外部インフラが必要である。また、車載ＥＣＵ間で暗号化通信が成立することをもって構成証明に代えるため、暗号化通信を実施する際に多大な計算機パワーが必要となる。以下、これら２点の課題について詳述する。

【００１０】

（１）センターサーバについて

（１．１）情報集約について

センターサーバは、全車の鍵情報が集約されている外部サーバであり、車載ネットワークを構成する各車載ＥＣＵはそれぞれセンターサーバに接続して鍵情報を受け取らなければならない。鍵情報の全てがセンターサーバに集約されているため、車載ＥＣＵとセンターサーバとの間の通信が妨害されたり、センターサーバ自体が攻撃されたり、悪意の第３者がセンターサーバになりすましたりした場合は、システム全体が崩壊しかねない。

【００１１】

（１．２）センターサーバとの間の通信について

ＫＰＳ方式によって配信する共通鍵生成源は、車載ネットワークに参加しているＥＣＵ間で通信するために用いるものである。したがって、ＥＣＵ間で安全に通信するためには、まず初期化処理としてセンターサーバから共通鍵生成源を取得する必要がある。このとき各ＥＣＵがセンターサーバと通信するために用いる暗号化鍵は、ＥＣＵ毎に固有の暗号化鍵ではなく、固定の暗号化鍵を使わざるを得ない。なぜなら、車載ＥＣＵは、部品メーカにより量産され組み立てメーカに納入されるものであり、初期化処理のための暗号化鍵は、車種単位、同一部品番号単位、またはＩＤの等しいロット単位で、必然的にバリエー

ションが固定されるためである。暗号化鍵が固定であると、悪意の第３者にとってはＥＣＵとセンターサーバの間の通信を盗聴しやすくなるので、これを利用して初期化鍵を不正入手される可能性がある。初期化鍵が不正入手されると、センターサーバの情報が不正に引き出される可能性がある。また、車載ＥＣＵに対して偽りの共通鍵を配信し、他の車載ＥＣＵとの間の通信を妨害される可能性もある。

【００１２】

（２）暗号化通信について

特許文献１に記載されている技術では、ＫＰＳ方式に基づいて通信相手方の鍵を復元する計算資源と、その鍵を用いて暗号化通信するための共通鍵暗号処理（例えば、ＤＥＳ：Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ方式の暗号処理）を実行する計算資源とが必要になる。これらの処理は、現状の車載ＥＣＵの能力（ＣＰＵの計算能力、ＲＯＭ／ＲＡＭの容量など）にとって非常に大きなリソースを要求する。したがって、特許文献１に記載されている暗号化通信を実現するためには、車載ＥＣＵのコスト上昇が避けられない。

【００１３】

現状の車載ＥＣＵを設計する際には、各ＥＣＵおよびその構成部品の原価低減を積み上げて、車両システム全体の価格戦略を摺り合わせている。車載ＥＣＵの構成証明という目的に対して、これら構成部品の価格が上昇することは、到底許容できるものではない。

【００１４】

本発明は、上記のような課題を解決するためになされたものであり、各車載制御装置の処理負荷（およびコスト）の上昇を抑えつつ、構成証明を実施する機能を備えた車載ネットワークを提供し、車両のセキュリティを向上させることを目的とする。

【課題を解決するための手段】

【００１５】

本発明に係る車載ネットワークシステムは、車載制御装置を認証する構成管理装置を備え、構成管理装置は、構成証明を実施するために用いる構成証明データを、車載ネットワークに接続する登録装置を介して車載制御装置に配信する。

【発明の効果】

【００１６】

本発明に係る車載ネットワークシステムは、車載制御装置を認証する構成管理装置が車載ネットワーク内に配置されているため、車内の鍵情報を車両外で保持する必要がない。したがって、安全でない通信方式を用いて車外と通信する必要がなくなり、セキュリティが向上する。また、登録装置は必ずしも車載ネットワークに常時接続されている必要はなく、車載制御装置を新規に登録する際に、オペレータが手作業で登録装置を車載ネットワークに接続させることができる。そのため、登録装置の処理能力を高めても、車載ネットワーク自体のコストは増加しないので、登録装置と構成管理装置の間では強固な認証方式を用いることができる。これにより、車載ネットワーク全体としてのコストを抑えつつセキュリティを向上させることができる。

【図面の簡単な説明】

【００１７】

【図１】実施形態１に係る車載ネットワークシステム１０００の構成図である。

【図２】構成管理サーバ１０３がネットワーク登録装置１０２を認証するシーケンスを説明する図である。

【図３】特許文献１に記載されている車載ネットワークの構成例を示す図である。

【図４】実施形態２に係る車載ネットワークシステム１０００の構成例を示す図である。

【図５】構成管理サーバ１０３と目標ＥＣＵ１０１の間で構成証明情報（共通鍵）を共有する形態を示す図である。

【図６】構成管理サーバ１０３が構成証明用鍵（共通鍵）を生成する方法を示す図である。

【図７】構成管理サーバ１０３が目標ＥＣＵ１０１を認証する手順を説明するシーケンス

図である。
【図８】構成管理サーバ１０３が目標ＥＣＵ１０１を認証する手順を示す別方式のシーケンス図である。
【図９】構成管理サーバ１０３の内部で実行される処理を示すフローチャートである。
【図１０】目標ＥＣＵ１０１の内部で実行される処理を示すフローチャートである。
【図１１】実施形態１～３で説明した構成証明手法を、構成証明以外の用途に応用した動作例を説明する図である。
【図１２】近年の代表的な高機能車両が備えている車載ネットワークのネットワークトポロジー例を示す図である。
【発明を実施するための形態】
【００１８】
＜実施の形態１＞
図１は、本発明の実施形態１に係る車載ネットワークシステム１０００の構成図である。車載ネットワークシステム１０００は、車両の動作を制御するＥＣＵを接続する車内ネットワークである。ここでは、構成証明の対象である目標ＥＣＵ１０１を１台のみ例示したが、車載ネットワークシステム１０００に接続することができるＥＣＵは、これに限られるものではない。
【００１９】
車載ネットワークシステム１０００には、目標ＥＣＵ１０１と構成管理サーバ１０３が車載ネットワークを介して接続されている。また、目標ＥＣＵ１０１を車載ネットワークに参加させるため、必要に応じてネットワーク登録装置１０２が車載ネットワークシステム１０００に接続される。
【００２０】
構成管理サーバ１０３は、車載ネットワークを介して目標ＥＣＵ１０１およびネットワーク登録装置１０２と通信することのできる装置である。構成管理サーバ１０３は、ＥＣＵの１種として構成してもよいし、その他任意の通信装置として構成してもよい。構成管理サーバ１０３は、目標ＥＣＵ１０１とネットワーク登録装置１０２を認証する。目標ＥＣＵ１０１を認証する目的は、目標ＥＣＵ１０１が車載ネットワークに参加する正当権限を有しているか否かを確認することである。ネットワーク登録装置１０２を認証する目的は、ネットワーク登録装置１０２が目標ＥＣＵ１０１を車載ネットワークに参加させる正当権限を有しているか否かを確認することである。
【００２１】
ネットワーク登録装置１０２は、目標ＥＣＵ１０１を車載ネットワークに参加させる装置である。車載ネットワークに参加させるとは、目標ＥＣＵ１０１が車載ネットワークを介して他のＥＣＵと通信するために必要な構成証明データを目標ＥＣＵ１０１に配信することである。ネットワーク登録装置１０２が目標ＥＣＵ１０１を車載ネットワークに参加させるためには、あらかじめ構成管理サーバ１０３による認証を受ける必要がある。
【００２２】
ネットワーク登録装置１０２は、必ずしも車載ネットワークに常時接続されている必要はない。例えば、車両の製造工程において車載ネットワークシステム１０００を構築する際に、目標ＥＣＵ１０１を車載ネットワークに参加させる作業を実施するときのみ、ネットワーク登録装置１０２を手作業で車載ネットワークに接続することができる。
【００２３】
以下、図１にしたがって、ネットワーク登録装置１０２が目標ＥＣＵ１０１を車載ネットワークに参加させる手順を説明する。
【００２４】
（図１：ステップＳ１１１：認証要求）
オペレータは、ネットワーク登録装置１０２を操作して、目標ＥＣＵ１０１を車載ネットワークに参加させる作業（登録処理）を開始する。ネットワーク登録装置１０２は、登録処理を開始すると、構成管理サーバ１０３に対し、自己を認証するように車載ネットワ

ークを介して要求する。
【００２５】
（図１：ステップＳ１１１：認証要求：補足）
ネットワーク登録装置１０２は、構成管理サーバ１０３に認証要求を出すと同時に、車載ネットワークに参加させる目標ＥＣＵ１０１の識別情報（詳細は後述の図５で説明）を構成管理サーバ１０３に通知する。この識別情報としては、例えばＥＣＵ－ＩＤ（部品番号）、ソフトウェアバージョンなどが挙げられる。これらの識別情報は、オペレータがネットワーク登録装置１０２上で手動入力するなどして与えることができる。
【００２６】
（図１：ステップＳ１１２：構成証明鍵の配布）
構成管理サーバ１０３は、ネットワーク登録装置１０２から認証要求を受け取ると、所定の認証アルゴリズム（詳細は後述の図２で説明）にしたがってネットワーク登録装置１０２を認証する。構成管理サーバ１０３は、ネットワーク登録装置１０２の真正性を確認した場合は、認証要求時にネットワーク登録装置１０２から受け取った情報を用いて内部のデータベース（詳細は後述の図５で説明）を更新し、目標ＥＣＵ１０１固有の構成証明用鍵（共通鍵）（詳細は後述の図６で説明）を生成して、ネットワーク登録装置１０２に配信する。
【００２７】
（図１：ステップＳ１１３：鍵格納指令）
ネットワーク登録装置１０２は、目標ＥＣＵ１０１に対して、構成管理サーバ１０３から配信された目標ＥＣＵ１０１固有の構成証明用鍵（共通鍵）を中継し、目標ＥＣＵ１０１にこれを格納するよう指示する。
【００２８】
（図１：ステップＳ１１４：格納完了通知）
目標ＥＣＵ１０１は、ステップＳ１１３で受け取った目標ＥＣＵ１０１固有の構成証明用鍵（共通鍵）を自局のメモリに格納し、車載ネットワークに正常に参加した旨をネットワーク登録装置１０２に通知する。
【００２９】
（図１：ステップＳ１１５：構成証明要求）
構成管理サーバ１０３は、ステップＳ１１２でネットワーク登録装置１０２を経由して配布しておいた構成証明用鍵（共通鍵）が目標ＥＣＵ１０１内に保持されている、との推定に基づいて、目標ＥＣＵ１０１に対して自局の真正性を証明するよう要求する。
【００３０】
（図１：ステップＳ１１６：構成証明回答）
目標ＥＣＵ１０１は、構成管理サーバ１０３に対して構成証明用鍵（共通鍵）の共有知識に基づいた回答を返信し、自局の真正性を証明する。
【００３１】
（図１：ステップＳ１１６：構成証明回答：補足）
ステップＳ１１５～Ｓ１１６における構成証明要求と回答は、構成管理サーバ１０３と目標ＥＣＵ１０１の間で相互になされるべきものである。したがって、図１に図示するステップＳ１１５とステップＳ１１６の矢印方向とは逆に、目標ＥＣＵ１０１が構成管理サーバ１０３に対して構成証明を要求し、構成管理サーバ１０３が回答してもよい。また、上記双方向のやり取りを合成して、目標ＥＣＵ１０１が構成管理サーバ１０３に対して構成証明を開示する前に、構成管理サーバ１０３の構成証明を要求し、目標ＥＣＵ１０１が構成管理サーバ１０３の真正性を確認しておいてから構成管理サーバ１０３に対して回答するように、相互的なハンドシェイクの形態を取ってもよい。
【００３２】
＜実施の形態１：ネットワーク登録装置の認証＞
図２は、構成管理サーバ１０３がネットワーク登録装置１０２を認証するシーケンスを説明する図である。図２の認証シーケンスは、図１のステップＳ１１１の詳細を示すもの

である。ここでは、公開鍵暗号方式に基づくデジタル署名を用いてネットワーク登録装置１０２を認証する手法を例示するが、チャレンジ＆レスポンス認証など別の認証方式を用いることもできる。なお、あらかじめネットワーク登録装置１０２の公開鍵と秘密鍵のペアを生成し、公開鍵を構成管理サーバ１０３に配信しておくものとする。以下、図２の各ステップについて説明する。

【００３３】

（図２：ステップＳ２０１）

ネットワーク登録装置１０２は、例えば車載ネットワークに最初に接続した時点など、目標ＥＣＵ１０１をネットワーク登録する動作に先立って、構成管理サーバ１０３に対し自己が正規端末であることを認証するように要求する。このとき、ネットワーク登録装置１０２の識別コード（またはそれに類する情報）を併せて送信し、自身を固有に識別する情報を構成管理サーバ１０３に対して明らかにする。

【００３４】

（図２：ステップＳ２０１：補足）

本ステップでいう正規端末とは、ネットワーク登録装置１０２が当該車両のメーカによって認定された正規のものであること、改竄されたものでないこと、別の装置が正規のネットワーク登録端末１０２になりすましたものでないこと、などを保証された端末のことである。すなわち、目標ＥＣＵ１０１を車載ネットワークに参加させる正当権限を有する端末である。

【００３５】

（図２：ステップＳ２０２～Ｓ２０３）

構成管理サーバ１０３は、認証開始処理を実行する（Ｓ２０２）。具体的には、疑似乱数を用いて種コードを生成し、ネットワーク登録装置１０２に返送する（Ｓ２０３）。また、ステップＳ２０１でネットワーク登録装置１０２から受け取った識別コードを用いて、ネットワーク登録装置１０２に対応する公開鍵を特定しておく。

【００３６】

（図２：ステップＳ２０４～Ｓ２０５）

ネットワーク登録装置１０２は、ステップＳ２０３で認証サーバから受け取った種コードを自身の秘密鍵で署名し（Ｓ２０４）、署名済みコードとして構成管理サーバ１０３に返送する（Ｓ２０５）。

【００３７】

（図２：ステップＳ２０６）

構成管理サーバ１０３は、ステップＳ２０２で特定しておいた公開鍵を読み出し、これを用いてステップＳ２０５でネットワーク登録装置１０２から受け取った署名済みコードを復号する。構成管理サーバ１０３は、その復号結果とステップＳ２０３でネットワーク登録装置１０２に送信した種コードを比較し、両者が一致すればネットワーク登録装置１０２が正規端末であると判断する。両者が一致しなければ、ネットワーク登録装置１０２は認証許可されなかったことになる。

【００３８】

（図２：ステップＳ２０７～Ｓ２０８）

構成管理サーバ１０３は、認証シーケンスが終了した旨を、確認応答としてネットワーク登録装置１０２に対して送信する（Ｓ２０７）。その後、ネットワーク登録装置１０２は、これから車載ネットワークに参加させる予定の目標ＥＣＵ１０１の｛ＥＣＵ－ＩＤ，ソフトウェアバージョン｝を構成管理サーバ１０３に通知する（Ｓ２０８）。

【００３９】

＜実施の形態１：まとめ＞

以上のように、本実施形態１に係る車載ネットワークシステム１０００において、構成管理サーバ１０３は、厳密に真正性を検証することができるネットワーク登録装置１０２を経由して、目標ＥＣＵ１０１に構成証明用鍵（共通鍵）を配布する。これにより、目標ＥＣＵ１０１は、多大な計算資源を消費するＫＰＳ方式のように高度な計算を実施するこ

となく、簡便に構成証明用鍵（共通鍵）を共有することができるので、ＥＣＵコストを抑えつつ車載ネットワークのセキュリティを向上させることができる。

【００４０】

また、本実施形態１に係る車載ネットワークシステム１０００において、ネットワーク登録装置１０２は必ずしも車載ネットワークシステム１０００に常時接続する必要はないので、車載ネットワークシステム１０００から独立した高性能な装置を用いてネットワーク登録装置１０２を構成することができる。これにより、車載ネットワークシステム１０００を構成するＥＣＵのコストを抑えつつ、構成管理サーバ１０３とネットワーク登録装置１０２の間で強固な認証処理を実施することができる。この認証処理には、構成管理サーバ１０３と目標ＥＣＵ１０１の間の認証処理よりも強固な手法を用いることができる。すなわち、ネットワーク登録装置１０２の性能を目標ＥＣＵ１０１よりも高くすることができるので、多大なリソースを消費する強固な認証処理を実施することができる。

【００４１】

また、本実施形態１に係る車載ネットワークシステム１０００において、目標ＥＣＵ１０１およびネットワーク登録装置１０２を認証する構成管理サーバ１０３は、車載ネットワーク内部に配置されている。これにより、各装置は認証処理を実施するために車外と通信する必要がなくなり、セキュリティを向上させることができる。また、認証処理を実施するためのリソースを構成管理サーバ１０３に集約させることにより、他のＥＣＵのコストを抑えることができる。

【００４２】

＜実施の形態２＞

本発明の実施形態２では、実施形態１で説明した車載ネットワークシステム１０００の具体的な構成例について説明する。

【００４３】

以下、本実施形態２に係る車載ネットワークシステム１０００（図４）と、特許文献１に記載されている従来例（図３）とを比較し、両者の構成とセキュリティに関する違いを説明する。

【００４４】

＜実施の形態２：従来例の説明＞

図３は、特許文献１に記載されている車載ネットワークの構成例を示す図であり、本実施形態２と対比するために記載したものである。図３において、車載ネットワーク２０２の中にＥＣＵマスタ１０５が存在しており、これが車両ごとの識別番号｛車両ＩＤ｝を保持している。

【００４５】

ＥＣＵマスタ１０５は、初期化処理を実施するとき、車載ネットワーク２０２の外部に設置されているセンターサーバ２０３に対して、｛車両ＩＤ，ＥＣＵ－ＩＤ，ソフトウェアバージョン｝の情報をセットにして、｛共通鍵生成源｝を配信するよう要求する（ステップＳ３１１）。ＥＣＵ－ＩＤはＥＣＵマスタ１０５の識別子であり、ソフトウェアバージョンはＥＣＵマスタ１０５が搭載しているソフトウェアのバージョンである。

【００４６】

センターサーバ２０３は、その要求に応じて｛共通鍵生成源｝を配布する（ステップＳ３１２）。これらのやり取りは、ＥＣＵマスタ１０５内部に固定的に設定された初期化鍵によって暗号化されている（外部通信Ｆ２２１）。

【００４７】

センターサーバ２０３より配布される｛共通鍵生成源｝は、車載ネットワーク２０２に属するＥＣＵ間の通信のみに使われる「共通鍵を導出する情報源」である。｛共通鍵生成源｝は、センターサーバ２０３と通信する際には用いられない。

【００４８】

ＥＣＵマスタ１０５以外の車載ネットワークに属する目標ＥＣＵ１０１は、ＥＣＵマスタ１０５より｛車両ＩＤ｝を入手する。この時点では、目標ＥＣＵ１０１は｛共通鍵生成

源｝を入手していないので、目標ＥＣＵ１０１は暗号化を実施せずにＥＣＵマスタ１０５と通信する（ステップＳ３１３）。

【００４９】

目標ＥＣＵ１０１は、ＥＣＵマスタ１０５より受け取った｛車両ＩＤ｝を用いて、｛車両ＩＤ，ＥＣＵ－ＩＤ，ソフトウェアバージョン｝のセットを組み立て、センターサーバ２０３に対して、｛共通鍵生成源｝を配信するよう要求する（ステップＳ３１４）。ＥＣＵ－ＩＤは目標ＥＣＵ１０１の識別子であり、ソフトウェアバージョンは目標ＥＣＵ１０１が搭載しているソフトウェアのバージョンである。

【００５０】

センターサーバ２０３は、その要求に応じて｛共通鍵生成源｝を配布する（ステップＳ３１５）。これらのやり取りは、目標ＥＣＵ１０１内部に固定的に設定された初期化鍵によって暗号化されている（外部通信Ｆ２２２）。

【００５１】

以上の構成より、特許文献１における方式には次のような脆弱性が存在することが明らかとなる。

（脆弱性１）車載ネットワーク２０２に属する全てのＥＣＵは、初期化処理を実施するとき、車載ネットワーク２０２の外部に配置されているセンターサーバ２０３と接続して｛共通鍵生成源｝の配布を受ける。そのため、初期化処理中にセンターサーバ２０３との間の接続が断たれた場合は、有効な車載ネットワークを構成することができない。

（脆弱性２）センターサーバ２０３は、全ての車両の｛車両ＩＤ，ＥＣＵ－ＩＤ，ソフトウェアバージョン｝と｛共通鍵生成源｝のセットを管理している。そのため、センターサーバ２０３が不正に侵入されると、全ての車両の鍵が流出する。また、故意・過失を問わずセンターサーバ２０３に障害が発生すると、全ての車両の鍵が紛失する危険を伴う。

（脆弱性３）初期化処理を実施するときの暗号化通信（外部通信Ｆ２２１および外部通信Ｆ２２２）が脆弱である。そのため、｛共通鍵生成源｝の配布をうける際に、ＥＣＵとセンターサーバ２０３との間の相互認証がセキュアではない。これは、部品として量産されるＥＣＵハードウェアの制約上、固定的でバリエーションの少ない暗号化鍵を使わざるを得ない特性に起因する。したがって、この暗号化鍵が破られると、センターサーバ２０３については特定車両の鍵情報が流出するおそれがあり、車載ＥＣＵについては悪意の第３者が偽りの鍵情報を配布することにより車載ネットワークへの妨害などが発生し得る。

（脆弱性４）初期化処理を実施するときのＥＣＵマスタ１０５から目標ＥＣＵ１０１の間の｛車両ＩＤ｝の流れ（ステップＳ３１３）は暗号化されていないので、車載ネットワーク２０２の外部から容易にキャプチャすることができる。これは、｛車両ＩＤ，ＥＣＵ－ＩＤ，ソフトウェアバージョン｝のセット（ステップＳ３１１およびステップＳ３１４で使用）を悪意の第３者が類推する糸口になる。

【００５２】

＜実施の形態２：本発明の説明＞

図４は、本実施形態２に係る車載ネットワークシステム１０００の構成例を示す図である。車載ネットワーク２０２に、構成管理サーバ１０３が設置されている。この車載ネットワーク２０２に新たな目標ＥＣＵ１０１を参加させる手順を詳述する。

【００５３】

オペレータは、ネットワーク登録装置１０２を接続用車両コネクタ１０４に接続し、構成管理サーバ１０３と通信して認証を受ける。このときオペレータは、これから車載ネットワーク２０２に参加させようとしている目標ＥＣＵ１０１のＥＣＵＩ－ＩＤなどをネットワーク登録装置１０２上で入力し、構成管理サーバ１０３に送信する。この手順は、図１のステップＳ１１１に相当する。

【００５４】

構成管理サーバ１０３は、ネットワーク登録装置１０２の真正性を厳密に審査・検証する。構成管理サーバ１０３は、ネットワーク登録装置１０２が正規のものであることを確認した場合は、目標ＥＣＵ１０１固有の｛共通鍵｝を発行する（ステップＳ１１２）。

【００５５】
ネットワーク登録装置１０２は、この｛共通鍵｝を目標ＥＣＵ１０１に中継して格納させる（ステップＳ１１３）。以上の手順により、構成管理サーバ１０３と目標ＥＣＵ１０１の間で｛共通鍵｝が安全に共有される。
【００５６】
以上説明した本発明のメカニズムにより、先に説明した従来例における脆弱性は、以下に示すように改善される。先に説明した脆弱性に対応する改善点を、脆弱性と同じ順番で説明する。
（改善点１）各ＥＣＵが実施する通信は、車載ネットワーク２０２内部でクローズしており、車両外部との間の通信は実施されない。したがって、車載ネットワーク２０２に対して不正侵入を受ける機会も、情報漏洩を発生させる機会も少ない。
（改善点２）車載ネットワーク２０２内の鍵情報は、車両ごとに内蔵されている構成管理サーバ１０３が管理する。したがって、センターサーバ２０３に全車両の情報を集約させることによる脆弱性は存在しない。また、｛共通鍵｝は車両ごとに独立してユニークであり、これが流出しても他車両に対するセキュリティ上の懸案事項は発生しない。
（改善点３）初期化処理を実施するときの｛共通鍵｝の発行および中継は、厳密に相互認証を実施した構成管理サーバ１０３とネットワーク登録装置１０２の間で実施される。したがって、悪意の第３者による妨害などのセキュリティリスクは少ない。
（改善点４）車載ネットワーク２０２のメンバを構成するＥＣＵの識別情報、例えば｛車両ＩＤ，ＥＣＵ－ＩＤ，ソフトウェアバージョン｝は、構成管理サーバ１０３の内部のみで管理されている。そのため、車載ネットワーク２０２を介して他ＥＣＵにこれら識別情報を開示する必要がない。したがって、これら情報の漏洩リスクに対して頑健である。
【００５７】
＜実施の形態２：共通鍵の共有形態＞
ネットワーク登録装置１０２は、目標ＥＣＵ１０１上の不揮発性メモリ（ＥＥＰＲＯＭ：Ｅｌｅｃｔｒｏｎｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　ａｎｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙ）に上記共通鍵情報を記憶させる機能のみを有する簡易装置として構成してもよいし、制御ソフトウェアを記憶するフラッシュＲＯＭに上記共通鍵情報を直接書き込むプログラム書換装置として構成してもよい。
【００５８】
車両が市場に出た後に制御プログラムの不具合が発覚した場合、ディーラーは車両を回収して該当車載ＥＣＵのプログラムを書き換える。このとき、このプログラム書換装置を用いて、目標ＥＣＵのソフトバージョンアップ、構成証明用鍵（共通鍵）の更新、構成管理サーバ１０３の登録情報（ＥＣＵ－ＩＤ，ソフトウェアバージョンなど）の更新が同時に実施できるようにしておけば、作業者にとって便宜である。そのため、ネットワーク登録装置１０２はプログラム書換装置としての機能を兼ね備えていることが望ましいといえる。
【００５９】
なお図４において、ネットワーク登録装置１０２は、車載ネットワーク２０２に直接接続するように図示されているが、無線通信などの有線以外の信号結合方式を用いて車外の通信網と接続し、ネットワーク登録装置１０２をその通信網の一要素として構成してもよい。この場合も、車内の構成管理サーバ１０３とネットワーク登録装置１０２との間の認証は厳密に実行される。
【００６０】
図５は、構成管理サーバ１０３と目標ＥＣＵ１０１の間で構成証明情報（共通鍵）を共有する形態（情報分布形態）を示す図である。ここでは目標ＥＣＵ１０１が複数存在する例を示した。
【００６１】
図５（ａ）は、構成管理サーバ１０３内のデータベース４１０が格納しているデータ例を示す。各車載ＥＣＵの識別情報（ＥＣＵ－ＩＤ，ソフトウェアバージョンなど）がデー

タ４１２で示すように保持されている。データ４１１は、構成管理サーバ自体の認証鍵であり、車載ＥＣＵ全てに等しく配布される。

【００６２】

図５（ｂ）～（ｄ）に示すデータベース４２０、４３０、４４０は、目標ＥＣＵ１０１ａ～１０１ｃのメモリ上にそれぞれ記憶されている構成証明用鍵（共通鍵）のデータ例を示す。各目標ＥＣＵ１０１が保持している共通鍵は、構成管理サーバ１０３が発行し、ネットワーク登録装置１０２を経由して設定されたものである。

【００６３】

すなわち、構成管理サーバ内データベース４１０のデータ４１２のうちＥＣＵ－ＩＤとソフトウェアバージョンを除いた情報が、各目標ＥＣＵ１０１に転写される。この共通鍵は、各目標ＥＣＵ１０１が構成管理サーバ１０３に対して自己の真正性を証明するために用いる鍵情報である。以降、この情報を「ＥＣＵ鍵」と呼ぶ。

【００６４】

また、構成管理サーバ内データベース４１０のデータ４１１のうちＥＣＵ－ＩＤとソフトウェアバージョンを除いた共通鍵情報も、各目標ＥＣＵ１０１に転写される。この共通鍵は、構成管理サーバ１０３が目標ＥＣＵ１０１に対して自己の真正性を証明するために用いる鍵情報である。以降、この情報を「サーバ鍵」と呼ぶ。

【００６５】

上述したＥＣＵ鍵とサーバ鍵に加えて、構成管理サーバ１０３と各目標ＥＣＵ１０１とが通信する際に用いるチャンネル番号またはメッセージＩＤなどの通信識別情報４１３を各目標ＥＣＵ１０１に配信することもできる。

【００６６】

通信識別情報４１３は、通信データの種別を指定する情報である。例えば、構成管理サーバ１０３が目標ＥＣＵ１０１ａに共通鍵を送信するときはメッセージＩＤ０ｘ１５を用い、目標ＥＣＵ１０１ｂに共通鍵を送信するときはメッセージＩＤ０ｘ１７を用いる、といった使い分けをすることができる。各目標ＥＣＵ１０１は、受信したデータが何を記述しているのかを、メッセージＩＤの値によって識別することができる。

【００６７】

各目標ＥＣＵ１０１は、車載ネットワーク２０２に参加する前は、構成証明において用いられる通信チャンネルを把握していない。そこで、構成証明用鍵（共通鍵）を配布するとともに各目標ＥＣＵ１０１にメッセージＩＤを配布することができる。メッセージＩＤは、各目標ＥＣＵ１０１のデータベース内に、それぞれデータ４２１、４３１、４４１として格納される。

【００６８】

通信データの種別毎にメッセージＩＤを変えることにより、通信の秘匿性がより一層高まる。すなわち、悪意の第３者はどのメッセージＩＤを用いて共通鍵が配信されているかを知らないため、通信データのなかから共通鍵を抽出することが困難である。

【００６９】

上述の各情報の他、構成管理サーバ内データベース４１０が格納している、ＥＣＵ－ＩＤ、ソフトウェアバージョンなどの属性情報を、各目標ＥＣＵ１０１に配信することもできる。これら情報は、ネットワーク登録装置１０２や目標ＥＣＵ１０１にとって有用な情報である。

【００７０】

ネットワーク登録装置１０２は、車両のＥＣＵが現在どのようなＥＣＵ群・ソフトウェア群で構成されているのかを調査したい場合がある。また、車載ＥＣＵは、協調制御の相手方となる他の車載ＥＣＵのソフトウェアバージョンが自局の制御ソフトと対応しているのかを調査したい場合がある。このような要求に答えるため、構成管理サーバ１０３は、データベース４１０が保持しているこれら情報を、ネットワーク登録装置１０２や目標ＥＣＵ１０１に配信してもよい。

【００７１】

ただしセキュリティの観点から、これら情報の開示は、ネットワーク登録装置１０２については前述の認証が厳密に実施された後、車載ＥＣＵについては当該ＥＣＵの構成証明が厳密に実施された後になされる。

【００７２】

図５に示すデータベース４１０は、オペレータがネットワーク登録装置１０２を用いて内容を閲覧し、更新することができるように構成してもよい。閲覧または更新に先立って構成管理サーバ１０３がネットワーク登録装置１０２を認証するのは、構成証明の場合と同様である。

【００７３】

＜実施の形態２：共通鍵の生成手段＞

図６は、構成管理サーバ１０３が構成証明用鍵（共通鍵）を生成する方法を示す図である。以下図６にしたがって、構成証明用鍵を生成する手順を説明する。

【００７４】

車両識別番号５０１は、車両個々にユニークに付けられる番号であり、構成管理サーバ１０３が内部的に情報を保持している。ＥＣＵ－ＩＤ（部品番号）５０２とソフトウェアバージョン５０３は、車載ネットワーク２０２に参加させようとしている目標ＥＣＵ１０１のＥＣＵ－ＩＤ（部品番号）とソフトウェアバージョンである。乱数５０４は、構成管理サーバ１０３内部で適宜発生させた乱数である。例えば、半導体閾値のホワイトノイズ的な揺らぎで一様乱数を生成するデバイスを用いて生成することができる。簡易的には、例えばマイコンのフリーランカウンタなどを適当なタイミングでキャプチャした数値列を乱数５０４として採用してもよい。

【００７５】

構成管理サーバ１０３は、これらの値を一方向性ハッシュ関数５０５に入力する。一方向性ハッシュ関数５０５は、固定長のＥＣＵ固有の共通鍵５０６を出力する。この共通鍵５０６またはこれを用いて算出した値を、構成証明用鍵として用いることができる。

【００７６】

一方向性ハッシュ関数５０５は、ＥＣＵ固有の共通鍵５０６から、車両識別番号５０１、ＥＣＵ－ＩＤ（部品番号）５０２、ソフトウェアバージョン５０３などの情報を復元することが不可能となるようにするために用いる。また、入力値が少しでも変わると共通鍵５０６も変化し、生成値が衝突しにくく、同一の出力値を与える入力値の組み合わせが予見不可能であることも重要である。

【００７７】

一方向性ハッシュ関数５０５の入力値として、車両識別番号５０１を用いているので、同じＥＣＵ－ＩＤ（部品番号）５０２の目標ＥＣＵ１０１をネットワーク登録しても、車両ごとに共通鍵５０６の値は異なる。また、一方向性ハッシュ関数５０５の入力値として乱数５０４を用いているので、同一車両の車載ネットワーク２０２に、同一のＥＣＵ－ＩＤ（部品番号）５０２および同一のソフトウェアバージョン５０３の車載ＥＣＵを参加させても、参加を実施する毎に共通鍵５０６の値は異なる。

【００７８】

この仕組みにより、ＥＣＵ改竄やＥＣＵ不正入れ換えを検出する能力を向上させることができる。同様の効果を発揮することができれば、一方向性ハッシュ関数５０５以外の関数を用いてもよいが、共通鍵５０６に基づき元の値を推測することができないようにする観点からは、一方向性関数を採用することが望ましい。

【００７９】

＜実施の形態２：構成証明の手順＞

図７は、構成管理サーバ１０３が目標ＥＣＵ１０１を認証する手順を説明するシーケンス図である。ここでは上述のサーバ鍵とＥＣＵ鍵をパスワードとして用いる例を示した。以下、図７の各ステップについて説明する。

【００８０】

（図７：ステップＳ７０１～Ｓ７０２：構成証明の開始）

構成管理サーバ１０３は、目標ＥＣＵ１０１に対して、構成証明要求を送信する（Ｓ７０１）。この構成証明要求は、車両が特定の状態時（始動直後、アイドリング時、イグニッションオフ直後など）に実施してもよいし、定期的に実施してもよい。目標ＥＣＵ１０１は、証明を要求しているのが本当に正規の構成管理サーバ１０３であるかを確かめるため、サーバ認証要求を返信する（Ｓ７０２）。

【００８１】

（図７：ステップＳ７０１～Ｓ７０２：補足）

前述の構成証明用鍵（共通鍵）とともに通信識別情報４１３を配布する場合は、図７に示す通信シーケンスは、各ＥＣＵが記憶している通信チャンネルまたはメッセージＩＤを用いて実施される。

【００８２】

（図７：ステップＳ７０３～Ｓ７０４：サーバ側認証）

構成管理サーバ１０３は、自分の真正性を目標ＥＣＵ１０１に示すため、サーバ鍵をサーバ側パスワードとして開示する（Ｓ７０３）。このサーバ鍵と、目標ＥＣＵ１０１が内部に保持しているサーバ鍵とが一致した場合、構成管理サーバ１０３が真正であると結論付けられる（Ｓ７０４）。

【００８３】

（図７：ステップＳ７０５～Ｓ７０７：ＥＣＵ側構成証明）

構成管理サーバ１０３が真正である旨を目標ＥＣＵ１０１が確認した場合、目標ＥＣＵ１０１は、ＥＣＵ鍵をＥＣＵ側パスワードとして構成管理サーバ１０３に送信する（Ｓ７０５）。構成管理サーバ１０３は、データベース４１０が保持している鍵と受信したＥＣＵ鍵が一致した場合、目標ＥＣＵ１０１は改竄されていないと判断する（Ｓ７０６）。以上の手順によって構成証明が完了し、構成管理サーバ１０３はセッション終了通知を目標ＥＣＵ１０１に送信する（Ｓ７０７）。

【００８４】

＜実施の形態２：構成証明の手順その２＞

図７で説明した手順によれば、サーバ認証とＥＣＵ構成証明を簡便に実行することができる。ただし、サーバ鍵とＥＣＵ鍵が直接車載ネットワーク２０２上に流れるので、これをキャプチャすれば、改竄された目標ＥＣＵ１０１（もしくは構成管理サーバ１０３）を作成して車載ネットワーク２０２に接続することができる。

【００８５】

このような状況を防止し、セキュリティ性能を向上させるため、構成証明用鍵（共通鍵）を直接車載ネットワーク２０２に流すことに代えて、チャレンジ＆レスポンス認証の共通鍵として構成証明用鍵を用いることもできる。図８を用いてその手順を説明する。

【００８６】

図８は、構成管理サーバ１０３が目標ＥＣＵ１０１を認証する手順を示す別方式のシーケンス図である。以下、図８の各ステップについて説明する。

【００８７】

（図８：ステップＳ８０１：構成証明要求）

構成管理サーバ１０３は、目標ＥＣＵ１０１に対して、構成証明要求を送信する（Ｓ８０１）。この構成証明要求は、車両が特定の状態時（始動直後、アイドリング時、イグニッションオフ直後など）に実施してもよいし、定期的に実施してもよい。目標ＥＣＵ１０１は、証明を要求しているのが本当に正規の構成管理サーバ１０３であるかを確かめる認証処理を開始する。

【００８８】

（図８：ステップＳ８０２～Ｓ８０３）

目標ＥＣＵ１０１は、乱数を発生させ（Ｓ８０２）、サーバ認証用のチャレンジデータとして構成管理サーバ１０３に送信する（Ｓ８０３）。

【００８９】

（図８：ステップＳ８０４～Ｓ８０５）

構成管理サーバ１０３は、ステップＳ８０３のサーバ認証用チャレンジを受け取り、このデータとサーバ鍵を入力として、一方向性ハッシュ関数を用いてレスポンスを計算する（Ｓ８０４）。構成管理サーバ１０３は、算出したレスポンスをサーバ側レスポンスとして目標ＥＣＵ１０１に送信する（Ｓ８０５）。

【００９０】

（図８：ステップＳ８０６）

目標ＥＣＵ１０１は、ステップＳ８０２で生成した乱数と、構成管理サーバ１０３との間で共有しているサーバ鍵とを一方向性ハッシュ関数に入力し、レスポンスとして構成管理サーバ１０３から帰ってくるであろうと予測される期待値を計算する。構成管理サーバ１０３と目標ＥＣＵ１０１は、規約によりそれぞれ同じアルゴリズムの一方向性ハッシュ関数を採用していると推定されるので、同じデータを入力とする一方向性ハッシュ関数の出力値は一致するはずである。

【００９１】

（図８：ステップＳ８０７～Ｓ８０８）

目標ＥＣＵ１０１は、ステップＳ８０６で計算した値と、構成管理サーバ１０３から受け取った値とを比較する（Ｓ８０７）。両者の値が一致すれば、構成管理サーバ１０３の真正性が証明されたことになるので、目標ＥＣＵ１０１は構成証明用チャレンジ要求を構成管理サーバに送信する（Ｓ８０８）。

【００９２】

（図８：ステップＳ８０９～Ｓ８１０）

構成管理サーバ１０３は、ステップＳ８０８で目標ＥＣＵ１０１が送信した構成証明用チャレンジ要求を受信すると、乱数を発生させ（Ｓ８０９）、目標ＥＣＵ１０１に対して構成証明用チャレンジデータとして送信する（Ｓ８１０）。乱数発生の手段は、目標ＥＣＵ１０１と同様である。

【００９３】

（図８：ステップＳ８１１～Ｓ８１３）

構成管理サーバ１０３は、ステップＳ８１０で送信したチャレンジデータとＥＣＵ鍵を用いて、ステップＳ８０６と同様の手順でレスポンスの期待値を計算しておく（Ｓ８１１）。目標ＥＣＵ１０１は、ステップＳ８１０で構成管理サーバ１０３が送信したチャレンジデータとＥＣＵ鍵を用いて、ステップＳ８０４と同様の手順でレスポンスを計算し（Ｓ８１２）、構成管理サーバ１０３に返信する（Ｓ８１３）。

【００９４】

（図８：ステップＳ８１４～Ｓ８１５）

構成管理サーバ１０３は、ステップＳ８１３で目標ＥＣＵ１０１から返信された構成証明用レスポンスとステップＳ８１１で計算した期待値を比較する。両者が一致すれば、目標ＥＣＵ１０１の構成証明が得られたことになる（Ｓ８１４）。その後、構成管理サーバ１０３は、目標ＥＣＵ１０１に対してセッション終了通知を送信する（Ｓ８１５）。

【００９５】

＜実施の形態２：まとめ＞

以上のように、本実施形態２に係る車載ネットワークシステム１０００において、構成管理サーバ１０３は、車載ネットワークに２０２に接続される全ての車載ＥＣＵの識別情報（ＥＣＵ－ＩＤ（部品番号）、ソフトウェアバージョン等）を管理する。この管理形態は、全車両の情報を集約する外部サーバなどを用いず、各車両が自己の識別情報を個別に保持する分散制御として構成される。したがって、情報管理形態としてロバストであり、個別車両の構成管理サーバ１０３が破られても、セキュリティ危機が全車両に波及することがない。

【００９６】

また、本実施形態２に係る車載ネットワークシステム１０００において、目標ＥＣＵ１０１を車載ネットワーク２０２に参加させる際に、信頼できるネットワーク登録装置１０２の力を借りて、安全に構成証明用鍵（共通鍵）を配信することができる。これにより、

上述のように簡単なチャレンジ＆レスポンス認証で、構成管理サーバ１０３と目標ＥＣＵ１０１が互いに相手方を認証し、構成の真正性を互いに証明し合うことができる。

【００９７】

また、本実施形態２に係る車載ネットワークシステム１０００においては、構成証明を実施する際に、高度な暗号化通信（一般の共通鍵暗号や公開鍵暗号）や共通鍵配信技術（ＫＰＳ方式など）を使う必要がない。すなわち、現状のＥＣＵにおけるＣＰＵ／ＲＯＭ／ＲＡＭ等の計算リソースを構成証明のために浪費する必要がなくなり、ひいては実装コストが増加しない。したがって本手法は、構成証明機能を車載ネットワークシステム１０００に簡便に付加し、ＥＣＵの改竄に対抗する手法として、非常にコストパフォーマンスに優れた方式であると言える。

【００９８】

＜実施の形態３＞

本発明の実施形態３では、実施形態２で開示した車載ネットワークシステム１０００の具体的なソフトウェア実装例について説明する。図９と図１０は、図８で示したチャレンジ＆レスポンス方式の構成証明手順を、ソフトウェア実装の観点でフローチャートとして開示したものである。したがって、機能として図８のシーケンスとは完全に等価というわけではなく、異常系処理と診断ＮＧ時の警告系処理を含んでいる。

【００９９】

図９は、構成管理サーバ１０３の内部で実行される処理を示すフローチャートである。以下、図９の各ステップについて説明する。

【０１００】

（図９：ステップＳ９０１～Ｓ９０５：構成証明開始）

構成管理サーバ１０３は、データベース４１０より、検証すべき目標ＥＣＵ１０１の共通鍵を読み出し、構成証明に備える（Ｓ９０１）。その後、該当する目標ＥＣＵ１０１に対して構成証明要求を送信し（Ｓ９０２）、タイムアウト計測に備えてタイマを初期化する（Ｓ９０３）。構成管理サーバ１０３は、サーバ認証用チャレンジデータの到来を待ち受け（Ｓ９０４）、データが到来すればステップＳ９０６に遷移する。サーバ認証用チャレンジデータが到来せずタイムアウトと判定された場合は（Ｓ９０５）、目標ＥＣＵ１０１が反応していないと判断し、ステップＳ９１７に遷移する。

【０１０１】

（図９：ステップＳ９０６～Ｓ９１０：サーバ側認証）

構成管理サーバ１０３は、サーバ認証用チャレンジデータを受信すると、サーバ鍵を用いてレスポンスを計算し（Ｓ９０６）、目標ＥＣＵ１０１にレスポンスを返信する（Ｓ９０７）。その後、ＥＣＵ側の判定を待ち受けるためのタイムアウト計測に備えてタイマを初期化する（Ｓ９０８）。構成管理サーバ１０３は、目標ＥＣＵ１０１から構成証明用チャレンジ要求を待ち受け（Ｓ９０９）、要求を受信すると、目標ＥＣＵ１０１がサーバ認証を受け入れたということなので、ステップＳ９１１に遷移する。構成証明用チャレンジ要求が到来せずタイムアウトと判定された場合は（Ｓ９１０）、目標ＥＣＵ１０１がサーバ認証を受け入れなかったか、または目標ＥＣＵ１０１が改竄され手続きを知らない可能性があると判断し、ステップＳ９１７に遷移する。

【０１０２】

（図９：ステップＳ９１１～Ｓ９１６：ＥＣＵ側証明要求）

ステップＳ９１１～Ｓ９１６は、目標ＥＣＵ１０１の構成証明を実施するためのデータを準備するステップである。構成管理サーバ１０３は、乱数を発生させ（Ｓ９１１）、構成証明用チャレンジデータとして目標ＥＣＵ１０１に送信する（Ｓ９１２）。その後、タイムアウト計測用タイマを初期化し（Ｓ９１３）、ステップＳ９０１で検索済みの目標ＥＣＵ１０１のＥＣＵ鍵を用いて、レスポンスの期待値を計算する（Ｓ９１４）。構成管理サーバ１０３は、目標ＥＣＵ１０１から構成証明用レスポンスを待ち受け（Ｓ９１５）、レスポンスがあった場合はステップＳ９１８に遷移する。構成証明用レスポンスが到来せずタイムアウトと判定された場合は（Ｓ９１６）、目標ＥＣＵ１０１が改竄され手続きを

知らない可能性があると判断し、ステップＳ９１７に遷移する。
【０１０３】
（図９：ステップＳ９１７：ＥＣＵ不正検出＆警告処理）
構成管理サーバ１０３は、適当なインターフェースを介して、目標ＥＣＵ１０１が改竄されている旨の警告信号を出力するか、またはその旨を記述した通信データを車載ネットワーク２０２に対してブロードキャストする。
【０１０４】
（図９：ステップＳ９１８～Ｓ９２０：構成証明結果）
構成管理サーバ１０３は、ステップＳ９１４で計算した期待値と、目標ＥＣＵ１０１から受信した構成証明用レスポンスとを比較する（Ｓ９１８）。両者が一致すれば構成証明が完了したということなので、目標ＥＣＵ１０１にセッション終了通知を送信し（Ｓ９１９）、構成証明が終了したことを通知する。その後、全ての検査すべき車載ＥＣＵについて構成証明が完了したか否かをチェックする（Ｓ９２０）。完了している場合は図９の処理を終了し、未完である場合はステップＳ９０１に戻る。期待値と構成証明用レスポンスとが一致しなかった場合は、目標ＥＣＵ１０１が他の車両のものと取り換えられたり、車載ネットワーク２０２に参加する処理を実行しないまま車載ネットワーク２０２に接続されたりするなど、不正な改竄が行われた可能性があると判断し、ステップＳ９１７に遷移する。
【０１０５】
図１０は、目標ＥＣＵ１０１の内部で実行される処理を示すフローチャートである。以下、図１０の各ステップについて説明する。
【０１０６】
（図１０：ステップＳ１００１～Ｓ１００７：サーバ側認証開始）
目標ＥＣＵ１０１は、構成管理サーバ１０３からの構成証明要求を待ち受け、要求が到着するとステップＳ１００２に遷移する（Ｓ１００１）。目標ＥＣＵ１０１は、構成管理サーバ１０３が改竄されていないか（悪意の盗聴装置ではないか）を確認するために乱数を発生し（Ｓ１００２）、サーバ認証用チャレンジデータとして送信する（Ｓ１００３）。目標ＥＣＵ１０１は、タイムアウト計測用タイマを初期化し（Ｓ１００４）、サーバ鍵を用いて構成管理サーバ１０３からのレスポンスの期待値を計算する（Ｓ１００５）。目標ＥＣＵ１０１は、構成管理サーバ１０３からのサーバ認証用レスポンスを待ち受け（Ｓ１００６）、返信を受け取るとステップＳ１００８に遷移する。サーバ認証用レスポンスが到来せずタイムアウトと判定された場合は（Ｓ１００７）、構成管理サーバ１０３が改竄されるか、または悪意の盗聴装置と交換されている可能性があると判断し、ステップＳ１０１８に遷移する。
【０１０７】
（図１０：ステップＳ１００８～Ｓ１０１２：ＥＣＵ側構成証明開始）
目標ＥＣＵ１０１は、ステップＳ１００５で計算した期待値と、構成管理サーバ１０３から受信したサーバ認証用レスポンスとを比較する（Ｓ１００８）。両者が一致すれば、構成管理サーバ１０３の真正性が確認されたということなので、ステップＳ１００９に遷移する。期待値とサーバ認証用レスポンスとが一致しなかった場合は、構成管理サーバ１０３が他の車両のものと取り換えられるか、または不正な改竄が行われた可能性があると判断し、ステップＳ１０１８に遷移する。目標ＥＣＵ１０１は、構成管理サーバ１０３に対して、自局の真正性を証明するための構成証明用チャレンジデータを送信するよう要求する（Ｓ１００９）。その後、構成管理サーバ１０３から構成証明用チャレンジデータを待ち受けるためのタイムアウト計測に備えてタイマを初期化する（Ｓ１０１０）。目標ＥＣＵ１０１は、構成管理サーバ１０３から構成証明用チャレンジデータを待ち受け、返信を受け取るとステップＳ１０１３に遷移する。構成証明用チャレンジデータが到来せずタイムアウトと判定された場合は（Ｓ１０１２）、構成管理サーバ１０３が改竄され手続きを知らない可能性があると判断し、ステップＳ１０１８に遷移する。
【０１０８】

（図１０：ステップＳ１０１３～Ｓ１０１７：構成証明結果）
目標ＥＣＵ１０１は、構成管理サーバ１０３から受信した構成証明用チャレンジデータとＥＣＵ鍵を用いてレスポンスを計算し（Ｓ１０１３）、構成管理サーバに返信する（Ｓ１０１４）。また、構成管理サーバ１０３からの応答を監視するためのタイムアウト計測に備えてタイマを初期化する（Ｓ１０１５）。目標ＥＣＵ１０１は、構成管理サーバ１０３からセッション終了通知を待ち受け、返信を受け取ると、構成管理サーバ１０３が構成証明を完了したことを意味しているので、図１０の処理を終了する（Ｓ１０１６）。構成証明用チャレンジデータが到来せずタイムアウトと判定された場合は（Ｓ１０１７）、構成管理サーバ１０３が他の車両のものと取り換えられるか、または不正な改竄が行われた可能性があると判断し、ステップＳ１０１８に遷移する。

【０１０９】
（図１０：ステップＳ１０１８：構成管理サーバ不正検出＆警告処理）
目標ＥＣＵ１０１は、適当なインターフェースを介して、構成管理サーバ１０３が改竄されている旨の警告信号を出力するか、またはその旨を記述した通信データを車載ネットワーク２０２に対してブロードキャストする。

【０１１０】
＜実施の形態３：まとめ＞
以上のように、本実施形態３に係る車載ネットワークシステム１０００において、構成証明は、構成管理サーバ１０３と目標ＥＣＵ１０１の間の相互認証によって実施される。これにより、構成管理サーバ１０３または目標ＥＣＵ１０１が改竄されたことを検知し、その旨の警告を発信することができる。

【０１１１】
＜実施の形態４＞
図１１は、実施形態１～３で説明した構成証明手法を、構成証明以外の用途に応用した動作例を説明する図である。図１１では、ＥＣＵ１０１が２台存在し（ＥＣＵ１０１ａと１０１ｂ）、これらＥＣＵの間でデジタル署名付きのメッセージを送受信する動作を想定する。

【０１１２】
ＥＣＵ鍵は、構成管理サーバ１０３と特定の車載ＥＣＵのペア間のみで共有される情報であるが、サーバ鍵は複数の車載ＥＣＵが共有する情報である。したがって、サーバ鍵を用いて複数の車載ＥＣＵ間でメッセージ認証符号（ＭＡＣ：Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を送受信し、メッセージの真正性を保証することが考えられる。

【０１１３】
サーバ鍵は、目標ＥＣＵ１０１が車載ネットワーク２０２に参加するときに、構成管理サーバ１０３から安全に配布されたものであり、車載ネットワーク２０２に属する正規ＥＣＵ以外には流出しない。よって、このサーバ鍵を用いてデジタル署名（メッセージ認証符号を添付すること）を実施すれば、構成管理サーバ１０３により認証を受けた車載ＥＣＵからのメッセージであることを、他ＥＣＵが確認することができる。

【０１１４】
ＥＣＵ１０１ａは、送りたいメッセージ１０１１ａとサーバ鍵１０１２ａを一方向性ハッシュ関数１０１３ａに入力してメッセージ認証符号（ＭＡＣ）１０１４ａを生成する。メッセージ１０１１ａとメッセージ認証符号（ＭＡＣ）１０１４ａをパッキング（Ｓ１１０１）して送信バッファ１０１５ａに格納し、車載ネットワーク２０２に送り出す（Ｓ１１０２）。

【０１１５】
ＥＣＵ１０１ｂは、ＥＣＵ１０１ａが送信した信号を受信（Ｓ１１０３）して受信バッファ１０１６ｂに格納し、送信側と申し合わせた規約によりアンパック（Ｓ１１０４）して、メッセージ１０１１ｂとメッセージ認証符号（ＭＡＣ）１０１４ｂとに分離する。

【０１１６】

ＥＣＵ１０１ｂは、メッセージ１０１１ｂとサーバ鍵１０１２ｂ（サーバ鍵１０１２ａと等しいと推定される）を一方向性ハッシュ関数１０１３ｂに入力して受信側メッセージ認証符号（ＭＡＣ）を作成し（Ｓ１１０５）、ＭＡＣ１０１４ｂと受信側メッセージ認証符号（ＭＡＣ）を比較器１０１７ｂにより比較する。両者が一致する旨の判定結果１０１８ｂが得られれば、メッセージ１０１１ｂの内容が確かにＥＣＵ１０１ａによって作成されたものであり、途中で改竄されていないと判断できる。

【０１１７】

なお、一方向性ハッシュ関数１０１３ａと１０１３ｂは、ＥＣＵ間の規約にしたがって同一のアルゴリズムを採用するものとする。

【０１１８】

図１１では、ネットワーク登録装置１０２により正規に車載ネットワーク２０２へ参加したＥＣＵが共通して保持するサーバ鍵を用いてメッセージ認証符号（ＭＡＣ）を実現する実施例を開示したが、この用途はメッセージ認証符号に限られるものではなく、共通鍵暗号方式（例えば、ＤＥＳ方式、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）方式など）による車載ＥＣＵ間の暗号化通信に応用してもよい。

【０１１９】

＜実施の形態４：まとめ＞

以上のように、本発明による車載ＥＣＵ間で共通鍵を共有する手法は、構成証明用途のみならず、任意の車載ＥＣＵ間での高信頼度通信についても有効であることが分かる。

【０１２０】

＜実施の形態５＞

図１２は、近年の代表的な高機能車両が備えている車載ネットワークのネットワークトポロジー例を示す図である。ネットワーク登録装置（ソフトウェア書換装置が兼任）１０２、構成管理サーバ１０３、各ＥＣＵなどの構成および動作は、実施形態１～４と同様である。

【０１２１】

図１２において、４群のネットワークが搭載されており、各々通信ゲートウェイ（ゲートウェイＥＣＵ）２０１によってネットワークが束ねられている。図１２では、ゲートウェイＥＣＵ２０１を中心にしてスター型のネットワーク配置を採用しているが、ゲートウェイＥＣＵ２０１を複数段設けてカスケード型の接続形態を採用してもよい。

【０１２２】

図１２に示す車載ネットワークには、駆動系ネットワーク３０１、シャーシ／安全系ネットワーク３０５、ボディ／電装系ネットワーク３０９、ＡＶ／情報系ネットワーク３１３が搭載されている。

【０１２３】

駆動系ネットワーク３０１の配下には、エンジン制御ＥＣＵ３０２、ＡＴ（Ａｕｔｏｍａｔｉｃ Ｔｒａｎｓｍｉｓｓｉｏｎ）制御ＥＣＵ３０３、ＨＥＶ（Ｈｙｂｒｉｄ Ｅｌｅｃｔｒｉｃ Ｖｅｈｉｃｌｅ）制御ＥＣＵ３０４が接続されている。シャーシ／安全系ネットワーク３０５の配下には、ブレーキ制御ＥＣＵ３０６、シャーシ制御ＥＣＵ３０７、ステアリング制御ＥＣＵ３０８が接続されている。ボディ／電装系ネットワーク３０９の配下には、計器表示ＥＣＵ３１０、エアコン制御ＥＣＵ３１１、盗難防止制御ＥＣＵ３１２が接続されている。ＡＶ／情報系ネットワーク３１３の配下には、ナビゲーションＥＣＵ３１４、オーディオＥＣＵ３１５、ＥＴＣ／電話ＥＣＵ３１６が接続されている。

【０１２４】

また、車両と外部との間で情報を送受信するため、車外通信部３１７が車外情報用ネットワーク３２２によってゲートウェイＥＣＵ２０１に接続されている。車外通信部３１７には、ＥＴＣ無線機３１８、ＶＩＣＳ（Ｖｅｈｉｃｌｅ Ｉｎｆｏｒｍａｔｉｏｎ ａｎｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｓｙｓｔｅｍ）無線機３１９、ＴＶ／ＦＭ無線機３２０、電話用無線機３２１が接続されている。

【０１２５】

ネットワーク登録装置１０２は、車両が備えている接続用車両コネクタ１０４を介して、車外情報用ネットワーク３２２の１ノードとして接続するように構成されている。これに代えて、他のネットワーク（駆動系ネットワーク３０１、シャーシ／安全系ネットワーク３０５、ボディ／電装系ネットワーク３０９、ＡＶ／情報系ネットワーク３１３）またはゲートウェイＥＣＵ２０１に単独で接続してもよい。すなわち、機械的な配置は無関係であって、直接もしくはゲートウェイＥＣＵ２０１を介して目標ＥＣＵに対して電気信号が到達すればよい。

【０１２６】

電話用無線機３２１を通じてネットワーク越しに車外通信網からネットワーク登録装置１０２の機能を実施することもできる。例えば、構成管理サーバ１０３のデータベース検索や目標ＥＣＵ１０１の構成証明用データのメンテナンスなどが考えられる。この場合においても、上述の実施形態１～４と同様の手法を用いることができる。

【０１２７】

電話網越しやインターネット越しにＥＣＵのソフトウェアを書き換える手法は、リコールなどの不具合対応に際してその実施コストを下げる重要技術であって、将来的にありふれた行為になることが予想される。

【０１２８】

したがって、本発明で開示する技術を用いることによって、このソフトウェア書き換え後に引き続いて、リモートで構成管理サーバ１０３のデータベース内容を更新し、リモートでソフトウェア書き換え後の車載ＥＣＵを正しくネットワークに再登録することができる。

【０１２９】

図１２では、構成管理サーバ１０３を通信ゲートウェイＥＣＵ２０１の配下に直接接続したが、構成管理サーバ１０３のネットワーク上の位置は任意でよい。すなわち、電気信号的な接続が確保できるのであれば、他のネットワーク（駆動系ネットワーク３０１、シャーシ／安全系ネットワーク３０５、ボディ／電装系ネットワーク３０９、ＡＶ／情報系ネットワーク３１３、車外情報用ネットワーク３２２など）に直接接続してもよい。

【０１３０】

ただし、以下の２つの観点で通信ゲートウェイＥＣＵ２０１が構成管理サーバ１０３の役割を兼ねることが望ましい。

（１）図１の認証シーケンスＳ１１１が失敗したとき、ネットワーク登録装置１０２からの通信を、目標ＥＣＵ１０１が属する車載ネットワーク（駆動系ネットワーク３０１、シャーシ／安全系ネットワーク３０５、ボディ／電装系ネットワーク３０９、ＡＶ／情報系ネットワーク３１３）から電気的に切り離すことができる。この構成を用いることによって、いわゆるファイヤーウォール（防火壁）機能を通信ゲートウェイ２０１に付与することになるので、車載ネットワークに対する外部からの侵入リスクを低下させ、セキュリティをさらに向上させることができる。

（２）車両の不正改造・特定車載ＥＣＵの改竄などの目的で、構成管理サーバ１０３が車載ネットワークから除去される行為を防がなければならない。その目的では、通信ゲートウェイＥＣＵ２０１と構成管理サーバ１０３が機能統合されており、１つのＥＣＵであることは望ましい。なぜなら、構成管理サーバ１０３を除去すると、複数の車載ネットワークにまたがる相互の通信が実施できなくなるからである。

【０１３１】

以上、本発明者によってなされた発明を実施形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。

【０１３２】

また、上記各構成、機能、処理部などは、それらの全部または一部を、例えば集積回路で設計することによりハードウェアとして実現することもできるし、プロセッサがそれぞれの機能を実現するプログラムを実行することによりソフトウェアとして実現することも

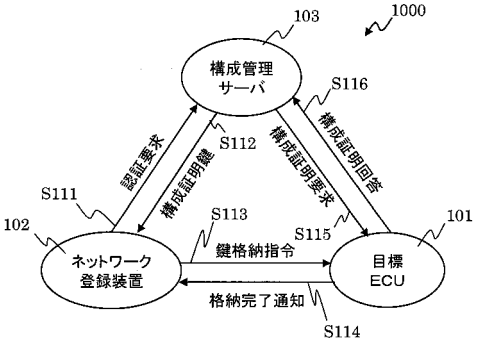
できる。各機能を実現するプログラム、テーブルなどの情報は、メモリやハードディスクなどの記憶装置、ＩＣカード、ＤＶＤなどの記憶媒体に格納することができる。

【符号の説明】

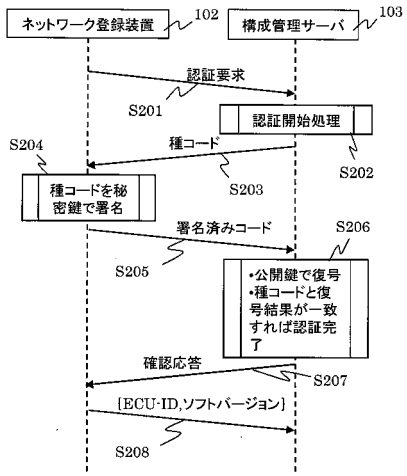
【０１３３】

１０１：目標ＥＣＵ、１０２：ネットワーク登録装置、１０３：構成管理サーバ、１０４：接続用車両コネクタ、２０１：通信ゲートウェイ、２０２：車載ネットワーク、３０１：駆動系ネットワーク、３０２：エンジン制御ＥＣＵ、３０３：ＡＴ制御ＥＣＵ、３０４：ＨＥＶ制御ＥＣＵ、３０５：シャーシ／安全系ネットワーク、３０６：ブレーキ制御ＥＣＵ、３０７：シャーシ制御ＥＣＵ、３０８：ステアリング制御ＥＣＵ、３０９：ボディ／電装系ネットワーク、３１０：計器表示ＥＣＵ、３１１：エアコン制御ＥＣＵ、３１２：盗難防止制御ＥＣＵ、３１３：ＡＶ／情報系ネットワーク、３１４：ナビゲーションＥＣＵ、３１５：オーディオＥＣＵ、３１６：ＥＴＣ／電話ＥＣＵ、３１７：車外通信部、３１８：ＥＴＣ無線機、３１９：ＶＩＣＳ無線機、３２０：ＴＶ／ＦＭ無線機、３２１：電話用無線機、３２２：車外情報用ネットワーク、１０００：車載ネットワークシステム。

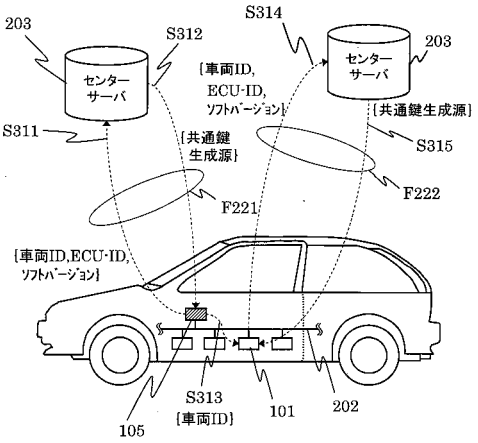
【図１】



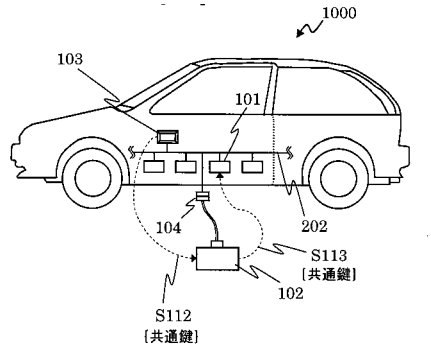
【図２】



【図３】



【図４】



【図５】

(a)構成管理サーバ

410 / 411 / 412 / 413

ECU-ID	ソフトウェアバージョン	共通鍵	メッセージID 送信	メッセージID 受信
自局(サーバ)	1.15.03	uCnz8o9H		
ECU-XXX	1.35.22	MbYUXhlY	0x15	0x16
ECU-YYY	2.00.01	bfkSXI7s	0x17	0x18
ECU-ZZZ	1.00.00	4CtXgogY	0x19	0x1a

(b)目標ECU 101a (ECU-XXX)

420 / 421

用途	共通鍵	メッセージID 送信	メッセージID 受信
自局証明用	MbYUXhlY	0x16	0x15
サーバ検証用	uCnz8o9H		

(c)目標ECU 101b (ECU-YYY)

430 / 431

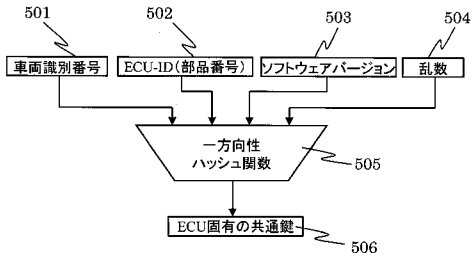
用途	共通鍵	メッセージID 送信	メッセージID 受信
自局証明用	bfkSXI7s	0x18	0x17
サーバ検証用	uCnz8o9H		

(d)目標ECU 101c (ECU-ZZZ)

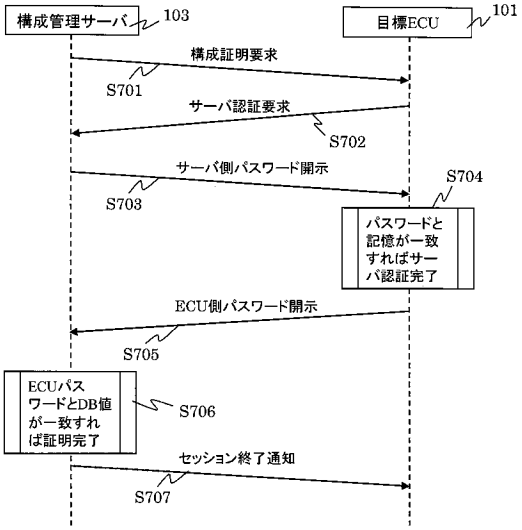
440 / 441

用途	共通鍵	メッセージID 送信	メッセージID 受信
自局証明用	4CtXgogY	0x1a	0x19
サーバ検証用	uCnz8o9H		

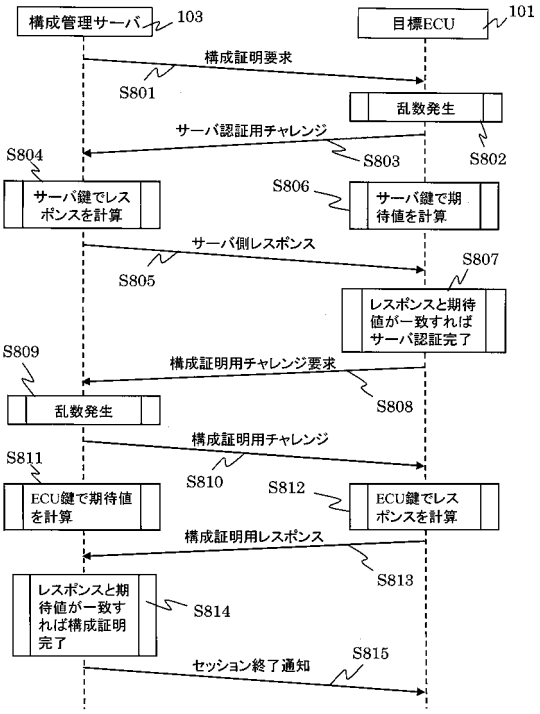
【図６】



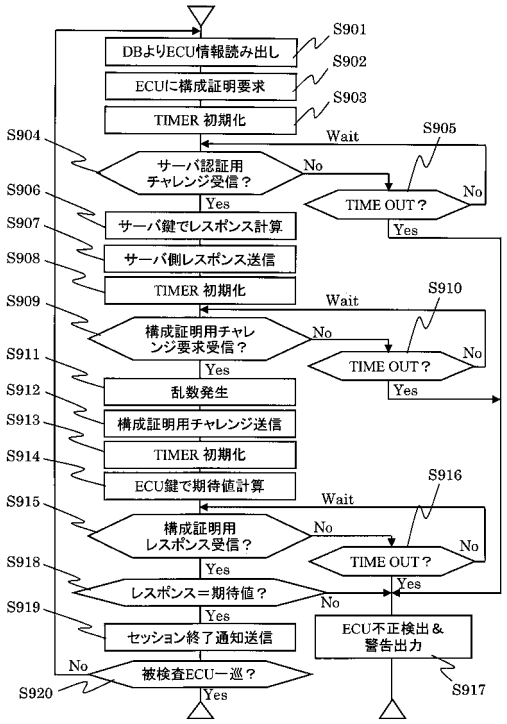
【図７】



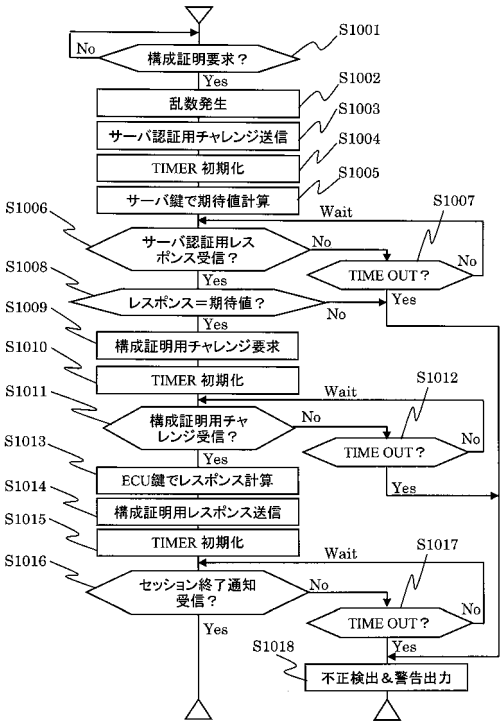
【図８】



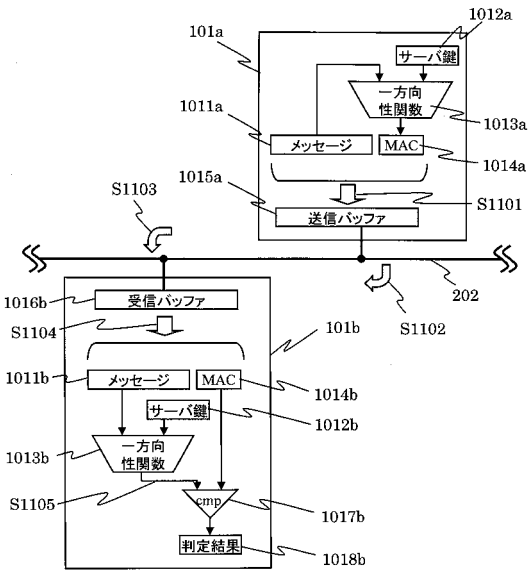
【図９】



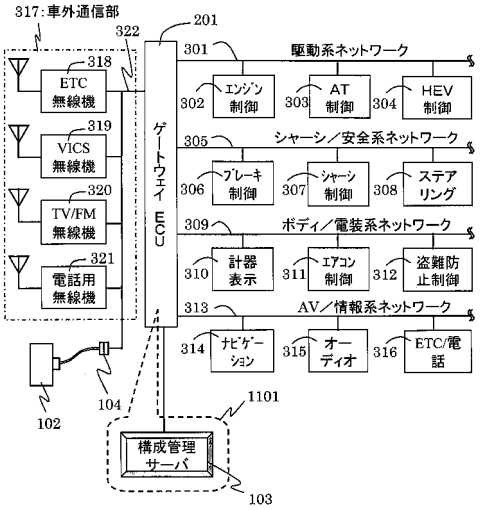
【図１０】



【図１１】



【図１２】



フロントページの続き

(56)参考文献 特開２００７－１５３０２１（ＪＰ，Ａ）
特開２０１０－１０３６９３（ＪＰ，Ａ）
特開２００５－３４１５２８（ＪＰ，Ａ）
特開２００６－０２５２９８（ＪＰ，Ａ）
特開平０６－１９５０２４（ＪＰ，Ａ）
特開２００７－２１４６９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｂ６０Ｒ　１６／０２３
Ｇ０６Ｆ　２１／４４