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

特許第5395036号
(P5395036)

(45)発行日　平成26年1月22日(2014.1.22)　(24)登録日　平成25年10月25日(2013.10.25)

(51)Int.Cl.		F I		
G06F 21/57	(2013.01)	G06F	21/00	157B
G06F 21/44	(2013.01)	G06F	21/20	144C
G06F 21/62	(2013.01)	G06F	21/24	165E
B60R 16/023	(2006.01)	B60R	16/02	665P
H04L 12/28	(2006.01)	H04L	12/28	200Z

請求項の数 9　(全 22 頁)

(21)出願番号　特願2010-254123 (P2010-254123)
(22)出願日　平成22年11月12日 (2010.11.12)
(65)公開番号　特開2012-104049 (P2012-104049A)
(43)公開日　平成24年5月31日 (2012.5.31)
審査請求日　平成25年1月23日 (2013.1.23)

(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　宮司　卓佳

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】
データを格納するメモリを備えた車載制御装置と、
前記車載制御装置が備える前記メモリが格納しているデータに対して読込要求または書込要求を発行する通信装置を認証する認証装置と、
を有し、
前記認証装置は、
前記通信装置が前記読込要求または前記書込要求を発行する前に前記通信装置に対する認証処理を実施してその結果を保持しておき、
前記車載制御装置は、
前記通信装置から前記読込要求または前記書込要求を受け取ると、前記通信装置に対する前記認証処理の結果を前記認証装置に対して照会し、
前記認証装置が前記通信装置を認証許可した場合は前記読込要求または前記書込要求を受け入れ、
前記認証装置が前記通信装置を認証許可しなかった場合は前記読込要求または前記書込要求を拒否する
ことを特徴とする車載ネットワークシステム。
【請求項２】
前記認証装置は、
前記認証処理が完了した旨を前記通信装置に応答する際に、認証許可したか否かを示

す情報を前記応答内に含めずに前記応答を送信する
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３】
前記認証装置は、
前記車載ネットワークシステムに接続する機器間の通信を中継する通信ゲートウェイとして動作して、前記車載制御装置と前記通信装置の間の通信を中継し、
前記通信装置に対する認証処理において前記通信装置を認証許可しなかった場合は、前記通信装置から前記車載制御装置に対する通信を中継しない
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】
前記車載制御装置は、
前記認証装置との間の接続が確立されているか否かを周期的に確認し、
前記認証装置との間の接続が確認できないときは、前記通信装置からの前記読込要求または前記書込要求を拒否する
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５】
前記認証装置は、
前記車載制御装置との間の接続が確立されているか否かを周期的に確認し、
前記車載制御装置との間の接続が確認できないときは、前記通信装置に対する認証処理において前記通信装置を認証許可しない
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】
前記認証装置は、
前記車載制御装置との間の接続が確立されているか否かを周期的に確認し、
前記車載制御装置との間の接続が確認できないときは、その旨の警告を発信する
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７】
前記認証装置は、
前記車載制御装置と前記認証装置の間の通信を監視し、
前記車載制御装置と前記認証装置の間の通信に対する他機器からの干渉もしくは妨害を検出したとき、または他機器が前記認証装置に成り済ましている旨を検出したときは、その旨の警告を発信する
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８】
前記認証装置は、
前記通信装置に対する前記認証処理において認証許可した後、前記車載制御装置と前記通信装置が通信中であるときは、前記車載ネットワークシステムに接続している他機器にその旨を通知する
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９】
前記認証装置は、
前記認証処理において前記通信装置を認証許可するとき、認証許可した旨を示す通信識別子を前記通信装置に対して配布し、
前記車載制御装置は、
前記通信装置から前記読込要求または前記書込要求を受け取ると、前記通信装置が前記通信識別子を保持しているか否かを確認し、
前記通信装置が前記通信識別子を保持している場合は前記読込要求または前記書込要求を受け入れ、
前記通信装置が前記通信識別子を保持していない場合は前記読込要求または前記書込要求を拒否する

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、各機能部の制御を行う車載ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）が搭載されている。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】

各ＥＣＵは、その開発フェーズにおいて、キャリブレーション、適合、またはマッチングと称する工程を実施する。同工程では、制御用パラメータをＥＣＵの外部からモニタしつつ、内部プログラムが参照する制御定数を変更し、各ＥＣＵに書き戻し設定する。

【０００４】

また、開発フェーズに限らず、車両が市場に出てからも、リコールもしくはサービスキャンペーンなどの機会において、ソフトウェアを書き換える場合がある。これは、制御プログラムの不具合が製品の市場投入後に発覚した場合、ディーラーが車両を回収した後、該当車載ＥＣＵのプログラムを書き換えることを指す。

【０００５】

車載ＥＣＵ外部からの制御パラメータ調整もしくはプログラム本体の書き換えは、ＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、ＦｌｅｘＲａｙ等の車載ネットワークを通じて行われる。このとき、専用の書き換え端末を車載ネットワークに接続するか、またはインターネット等の車外通信網と車載ネットワークを電気的に接続して書き換え作業を実施する。このとき、不正な書き換えを排除するため上記書き換え端末や、車載ネットワークに接続して書き換え指令を発行する装置が正規のものであるか否かを認証することが必要となる。

【０００６】

通常、車載ＥＣＵの制御プログラムは、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。これを書き換えるためには、旧プログラムを含む該当領域の全記憶データを一旦物理的に消去し、その後の初期化済み領域に新たにプログラムを書き込む必要がある。

【０００７】

上記書き換え端末等が悪意あるものである場合、該当ＥＣＵの旧プログラムを消去し、新たなプログラムを転送しないことにより、容易に該当ＥＣＵを機能停止させることができる。また、機能停止させるだけでなく、新たに悪意を持ったプログラムに書き換えることもできる。これにより、制御的に不安全な挙動を故意に引き起こすプログラムが仕組まれる可能性がある。さらには、書き換え対象のＥＣＵ以外にも問題を引き起こす可能性がある。例えば、故意に車載ネットワークの通信トラフィックを飽和させるプログラムが仕組まれる可能性がある。その他、特定ＥＣＵが故障した旨の情報を車載ネットワークに流すことによって、他の正常なＥＣＵにフェールセーフ動作を故意に実施させるような妨害行為も考えられる。

【０００８】

上記ではプログラムの書き換えについて述べたが、その他にも、開発フェーズにおいてＥＣＵ内部の変数を確認するために設けた機能を悪用し、ＥＣＵ内部のデータを不正に取得される可能性もある。例えば、車載ネットワークを介して特定ＥＣＵの制御パラメータの動きを不正にモニタする、その結果を元にリバースエンジニアリングを実施して当該ＥＣＵの技術情報を収集する、カーナビゲーション・ＥＴＣ（Ｅｌｅｃｔｒｏｎｉｃ　Ｔｏｌｌ　Ｃｏｌｌｅｃｔｉｏｎ）・携帯電話等の情報系ＥＣＵより個人情報を入手する、などの手口が考えられる。

【０００９】
下記特許文献１には、上記のような悪意ある端末から、車載ネットワーク、およびそれを構成するＥＣＵを防衛する技術として、外部端末と通信するＥＣＵが相手方端末を個別に認証し、車載ネットワークを介した不正侵入を排除する手法が開示されている。
【先行技術文献】
【特許文献】
【００１０】
【特許文献１】特開２０１０－２３５５６号公報
【発明の概要】
【発明が解決しようとする課題】
【００１１】
車載ネットワークのトラフィック飽和攻撃などの事例では、車載ネットワーク全体のセキュリティは、最もセキュリティの脆弱なＥＣＵによって決まる。そのため、個別ＥＣＵがセキュリティを向上させても、他の脆弱なＥＣＵによって車載ネットワーク全体のセキュリティが向上しない可能性がある。
【００１２】
しかし車載ＥＣＵは、搭載されるマイクロコンピュータの計算能力やＲＯＭ／ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）などのリソースが比較的低機能であるため、高度な認証アルゴリズムを採用することは難しい。
【００１３】
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のできる手法を提供することを目的とする。
【課題を解決するための手段】
【００１４】
本発明に係る車載ネットワークシステムにおいて、車載制御装置が保持しているデータに対して読取要求または書込要求を発行する通信装置は、あらかじめ認証装置による認証許可を受ける。
【発明の効果】
【００１５】
本発明に係る車載ネットワークシステムによれば、認証装置が一括して認証処理を実施するので、各車載制御装置の処理負荷を上げることなく、高度な認証手法を実装することができる。これにより、各車載制御装置の処理負荷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。
【図面の簡単な説明】
【００１６】
【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】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３】車載ネットワークシステム１０００の別構成例を示す図である。
【図４】目標ＥＣＵ１０１、書換装置１０２、認証サーバ１０３の間の通信手順を示すシーケンス図である。
【図５】目標ＥＣＵ１０１、書換装置１０２、認証サーバ１０３の間の別の通信手順を示すシーケンス図である。
【図６】認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されているか否かを確認する処理シーケンスを示す図である。
【図７】認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されているか否かを確認する別の処理シーケンスを示す図である。
【図８】認証サーバ１０３が車載ネットワーク上で認証サーバ１０３に成り済ました動作を実施している機器を検出した場合の動作を説明する図である。
【図９】実施形態１～４において目標ＥＣＵ１０１が書換装置１０２からセッション開始

要求を受け取ったときに実施する処理フローの１例を示す図である。
【図１０】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】
【００１７】
＜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、制御プログラムを書き換える対象である目標ＥＣＵ１０１のみを例示したが、車載ネットワークシステム１０００に接続するＥＣＵの数はこれに限られるものではない。
【００１８】
車載ネットワークシステム１０００には、目標ＥＣＵ１０１と認証サーバ１０３が通信ネットワークを介して接続されている。また、目標ＥＣＵ１０１がフラッシュＲＯＭ等のメモリ上に格納している制御プログラムを書き換えるため、または目標ＥＣＵ１０１の内部データを取得するため、必要に応じて書換装置１０２が車載ネットワークシステム１０００に接続される。
【００１９】
認証サーバ１０３は、車載ネットワークを介して目標ＥＣＵ１０１および書換装置１０２と通信することのできる装置である。認証サーバ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。
【００２０】
書換装置１０２が目標ＥＣＵ１０１に対して上記処理を実施するためには、あらかじめ認証サーバ１０３による認証を受ける必要がある。ここでいう認証とは、書換装置１０２が目標ＥＣＵ１０１に対して上記処理を実施する権限を有するか否かを検証する処理である。以下図１にしたがって、書換装置１０２が目標ＥＣＵ１０１に対して上記処理を実施するまでの手順を説明する。
【００２１】
（図１：ステップＳ１０１：認証要求）
書換装置１０２は、目標ＥＣＵ１０１に対してプログラム書換要求またはデータ取得要求を発行する前に、認証サーバ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。このとき書換装置１０２の識別子などの書換装置１０２に固有の情報を併せて送信する。
【００２２】
（図１：ステップＳ１０２：確認応答）
認証サーバ１０３は、書換装置１０２から認証要求を受け取ると、所定の認証アルゴリズムを用いて書換装置１０２を認証する。認証サーバ１０３は、書換装置１０２の識別子と認証結果を対応付けて、メモリなどの記憶装置上に保持しておく。認証サーバ１０３は、認証処理が完了すると、その旨の確認応答を書換装置１０２へ送信する。
【００２３】
（図１：ステップＳ１０２：確認応答：補足）
認証サーバ１０３は、本ステップにおいて書換装置１０２に確認応答を送信する際に、認証許可するか否かを示す情報を確認応答内に含めずに確認応答を送信する。これは、書換装置１０２が認証を多数回数試行して認証処理を突破する手法から、認証アルゴリズムを防衛するためである。
【００２４】
（図１：ステップＳ１０３：リクエスト）
書換装置１０２は、目標ＥＣＵ１０１に対して、目標ＥＣＵ１０１のメモリ上に格納している制御プログラムを書き換える要求、または目標ＥＣＵ１０１の内部データを取得する要求を送信する。

【００２５】
（図１：ステップＳ１０４：認証結果照会）
目標ＥＣＵ１０１は、ステップＳ１０３の要求送信元が正規端末であるか否かを、認証サーバ１０３に問い合わせる。
【００２６】
（図１：ステップＳ１０５：認証結果回答）
認証サーバ１０３は、ステップＳ１０２で保持しておいた書換装置１０２の認証結果を検索し、その結果を目標ＥＣＵ１０１に送信する。
【００２７】
（図１：ステップＳ１０６：リクエスト受諾または拒否）
目標ＥＣＵ１０１は、ステップＳ１０５で認証サーバ１０３より認証許可した旨の回答を得た場合は、ステップＳ１０３で書換装置１０２から受け取った要求を受け入れる。認証許可しなかった旨の回答を得た場合は、書換装置１０２から受け取った要求を拒否する。目標ＥＣＵ１０１は、要求を受け入れるか否かの回答を、書換装置１０２に回答する。
【００２８】
＜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、認証サーバ１０３は、ＥＣＵ１０１内部のデータに対して読取要求または書込要求を発行する書換装置１０２の認証を一括して行う。これにより、各ＥＣＵ１０１は認証処理を実行する必要がなくなり、認証結果を認証サーバ１０３に問い合わせるのみで済むので、各ＥＣＵ１０１の処理負荷を増加させずに認証処理を実施することができる。
【００２９】
また、本実施形態１に係る車載ネットワークシステム１０００によれば、認証処理を認証サーバ１０３に集約することができるので、認証サーバ１０３において、例えば公開鍵暗号などの高度な認証技術を採用することができる。これにより、各ＥＣＵ１０１のリソースなどの制約を受けることなく、車載ネットワークシステム１０００のセキュリティを向上させることができる。また、従来のようにセキュリティを向上させるため各ＥＣＵ１０１のハードウェア性能を向上させる必要がなくなり、セキュリティ向上のためのコストアップを抑制することができる。
【００３０】
また、本実施形態１に係る車載ネットワークシステム１０００では、認証処理を実施するのは認証サーバ１０３のみであるため、認証処理に係る技術情報を外部メーカなどに公開する必要がなくなり、技術情報の拡散によるセキュリティ上の情報漏洩を未然に防ぐことができる。すなわち、通常の車載ＥＣＵは、同一仕様のものであっても、部品調達リスクを分散させる観点、または車両トータルコストを最適化する観点から、車種や仕向け地の違いによって複数のＥＣＵメーカに並列的に発注する場合がある。この分業形態をとった場合、従来のように各ＥＣＵ１０１が書換装置１０２を認証する方式では、認証処理に係る技術情報を外部の複数のＥＣＵメーカに公開する必要がある。本発明ではかかる必要がなくなる点で有利である。
【００３１】
また、本実施形態１に係る車載ネットワークシステム１０００によれば、車載ネットワーク全体のセキュリティレベルが認証サーバ１０３のセキュリティ強度によって定まるため、従来のように各ＥＣＵ１０１が認証処理を実施する場合と比較して、脆弱なＥＣＵが車載ネットワーク全体のセキュリティレベルを低下させるおそれがなくなる。
【００３２】
また、本実施形態１に係る車載ネットワークシステム１０００によれば、新たな脆弱性が発見された場合などにおいて認証機能を更新する際に、認証サーバ１０３の認証アルゴリズムを書き換えるのみで済む。この点、従来のように各ＥＣＵ１０１が認証処理を実施する場合には、各ＥＣＵ１０１の認証アルゴリズムを書き換える必要があるので、その間の車両動作を停止せざるを得ず、ユーザにとって不便である。本発明によれば、認証サー

バ１０３の動作自体は通常の車両制御とは無関係であるため、車両動作を停止させずに認証アルゴリズムを更新することができる。例えば、当該車両が走行中状態であっても、電話網・インターネット配信等を通じてセキュリティパッチを配布し、認証アルゴリズムを書き換えることができる。これにより、認証アルゴリズムを更新するために車両を回収する手続きが必要なくなるので、例えばリコールやサービスキャンペーンなどの名目で車両を回収する必要がなくなり、更新コストを安価に押さえて迅速に更新作業を行うことができる。

【００３３】

＜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。

【００３４】

図２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。図２において、目標ＥＣＵ１０１と認証サーバ１０３は、ＣＡＮ等の車載ネットワーク１０５に接続され、車両内部に搭載されている。

【００３５】

書換装置１０２は、車両の外面に設けられた接続用車両コネクタ１０４を介して車載ネットワーク１０５に接続する。これにより、目標ＥＣＵ１０１を車外に取り出すことなく目標ＥＣＵ１０１に接続し、目標ＥＣＵ１０１が保持しているプログラムの書き換え、内部データの取得などの処理を実行する。

【００３６】

図３は、車載ネットワークシステム１０００の別構成例を示す図である。図３に示す構成では、車載ネットワーク１０５に加えて新たに車載ネットワーク２０２が設けられており、車載ネットワーク１０５と車載ネットワーク２０２の間は通信ゲートウェイ２０１によって接続されている。

【００３７】

目標ＥＣＵ１０１は車載ネットワーク１０５の配下、書換装置１０２と認証サーバ１０３は、車載ネットワーク２０２の配下にそれぞれ配置されており、各々別ネットワークに属する。車載ネットワーク１０５と車載ネットワーク２０２は、通信ゲートウェイ２０１により電気的に接続されているので、各機器は相互に通信することができる。

【００３８】

図４は、目標ＥＣＵ１０１、書換装置１０２、認証サーバ１０３の間の通信手順を示すシーケンス図である。ここでは、プログラムの不具合によるリコールの対応などで、書換装置１０２が目標ＥＣＵ１０１のフラッシュＲＯＭに格納されているプログラムを書き換える作業を想定している。以下、図４の各ステップについて説明する。

【００３９】

（図４：ステップＳ４１０）

書換装置１０２と認証サーバ１０３は、以下に説明するステップＳ４１１～Ｓ４１５からなる認証シーケンスＳ４１０を実行する。認証シーケンスＳ４１０は、図１のステップＳ１０１～Ｓ１０２に相当するものである。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書換装置１０２を認証する手法を例示するが、別の認証方式を用いることもできる。なお、あらかじめ書換装置１０２の公開鍵と秘密鍵のペアを生成し、公開鍵を認証装置１０３に配信しておくものとする。

【００４０】

（図４：ステップＳ４１１）

書換装置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に対して読取要求または書込要求を発行する前の段階で、認証サーバ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、書換装置１０２の識別コード（またはそれに類する情報、以下同様）を併せて送信し、自身を固有に識別する情報を認証サーバ１０３に対して明らかにする。

【００４１】
（図４：ステップＳ４１１：補足）
ここでいう正規端末とは、書換装置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、別の装置が正規の書換端末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。
【００４２】
（図４：ステップＳ４１２）
認証サーバ１０３は、認証開始処理を実行する。具体的には、疑似乱数を用いて種コードを生成し、書換装置１０２に返送する。また、ステップＳ４１１で書換装置１０２から受け取った識別コードを用いて、書換装置１０２に対応する公開鍵を特定しておく。
【００４３】
（図４：ステップＳ４１３）
書換装置１０２は、ステップＳ４１２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、署名済みコードとして認証サーバ１０３に返送する。
【００４４】
（図４：ステップＳ４１４）
認証サーバ１０３は、ステップＳ４１１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Ｓ４１３で書換装置１０２から受け取った署名済みコードを復号する。認証サーバ１０３は、その復号結果とステップＳ４１２で書換装置１０２に送信した種コードを比較し、両者が一致すれば書換装置１０２が正規端末であると判断する。認証サーバ１０３は、書換装置１０２を認証許可した旨の情報を、内部の認証済み機器リストに格納する。両者が一致しなければ、書換装置１０２は認証許可されなかったことになる。
【００４５】
（図４：ステップＳ４１５）
認証サーバ１０３は、認証シーケンスＳ４１０が終了した旨を、確認応答として書換装置１０２に対して送信する。このとき、書換装置１０２を認証許可したか否かについての情報を確認応答のなかに含めないこととする。理由は実施形態１のステップＳ１０２で述べた通りである。
【００４６】
（図４：ステップＳ４２０）
書換装置１０２は、目標ＥＣＵ１０１に対してセッション開始要求を送信する。本ステップは、図１のステップＳ１０３に相当する。セッション開始要求には、書換装置１０２の識別コードが含まれているものとする。
【００４７】
（図４：ステップＳ４３０）
書換装置１０２と目標ＥＣＵ１０１は、以下に説明するステップＳ４３１～Ｓ４３２からなる認証照会シーケンスＳ４３０を実行する。認証照会シーケンスＳ４３０は、図１のステップＳ１０４～Ｓ１０５に相当するものである。
【００４８】
（図４：ステップＳ４３１）
目標ＥＵＣ１０１は、書換装置１０２からセッション開始要求を受け取ると、書換装置１０２の認証結果を確認する処理を開始する。目標ＥＵＣ１０１は、ステップＳ４２０で受け取った書換装置１０２の識別コードを用いて、認証サーバ１０３に対し、書換装置１０２が認証済みであるか否かを照会する。
【００４９】
（図４：ステップＳ４３２）
認証サーバ１０３では、ステップＳ４３１で受け取った書換装置１０２の識別コードが認証済み機器リストに登録されているか否かを照合する。該当する識別コードが見つかれば、書換装置１０２は認証済みである旨の回答を目標ＥＣＵ１０１に送信し、見つからなければ書換装置１０２は認証許可されなかった旨の回答を目標ＥＣＵ１０１に送信する。

【００５０】
（図４：ステップＳ４４０）
目標ＥＣＵ１０１は、書換装置１０２との間の正規セッションを開始する。目標ＥＣＵ１０１は、ステップＳ４３２において書換装置１０２が認証許可されている旨の応答を受け取った場合は、書換装置１０２からのセッション開始要求を受け入れ、セッション受諾通知を書換装置１０２に対して発行する。ステップＳ４３２において書換装置１０２が認証許可されていない旨の応答を受け取った場合は、書換装置１０２からのセッション開始要求を拒否する。例えば、セッション開始要求を無視して書換装置１０２に対して何も応答しないなどの対応を取る。
【００５１】
（図４：ステップＳ４５０）
ステップＳ４４０の結果、書換装置１０２と目標ＥＣＵ１０１の間のセッションが確立する。書換装置１０２は、目標ＥＣＵ１０１が保持しているプログラムの書き換え、内部データの取得、などの処理を実行する。
【００５２】
（図４：ステップＳ４６０）
認証サーバ１０３は、認証シーケンスＳ４１０を正常完了し認証済み機器リストに書換装置１０２を登録した後、目標ＥＣＵ１０１から照会を受けたときに備えて、認証済み機器リストの内容をそのまま保持する。認証サーバ１０３は、例えば１回のドライビングサイクルの間のみ認証済み機器リストを保持する、もしくは所定時間が経過するまでの間のみ認証済み機器リストを保持する、もしくは車両のイグニッション・キーがＯＦＦされるまでの間のみ認証済み機器リストを保持する、などの基準に基づき、古くなった認証済み機器リストを破棄する。
【００５３】
（図４：ステップＳ４６０：補足）
ドライビングサイクルは、ＯＢＤ　ＩＩ（Ｏｎ－Ｂｏａｒｄ　Ｄｉａｇｎｏｓｔｉｃｓ，ＩＩ　ｇｅｎｅｒａｔｉｏｎ，ＩＳＯ－９１４１－２）などの車両の自己診断技術において提示された概念である。同技術において、ドライビングサイクルとは、エンジン始動（アイドリングストップ対応自動車等におけるエンジン自動停止に続く始動を除く）、運行状態およびエンジン停止状態（アイドリングストップ対応自動車等におけるエンジン自動停止を除く）を各１回含む期間のことを指す。
【００５４】
図５は、目標ＥＣＵ１０１、書換装置１０２、認証サーバ１０３の間の別の通信手順を示すシーケンス図である。ここでは図４とは異なり、認証シーケンスＳ４１０に代えてチャレンジ＆レスポンス方式によるワンタイムパスワードを用いた認証シーケンスＳ５１０を採用した。以下、図４との違いを中心に図５の各ステップについて説明する。
【００５５】
（図５：ステップＳ５１０）
書換装置１０２と認証サーバ１０３は、以下に説明するステップＳ５１１～Ｓ５１７からなる認証シーケンスＳ５１０を実行する。なお、あらかじめ書換装置１０２と認証装置１０３の間で、後述するステップＳ５１３～Ｓ５１５で用いる既定関数を共用しておくものとする。
【００５６】
（図５：ステップＳ５１１）
本ステップは、図４のステップＳ４１１と同様である。
【００５７】
（図５：ステップＳ５１２）
認証サーバ１０３は、認証開始処理を実行する。具体的には、疑似乱数を用いて種コードを生成し、書換装置１０２に返送する。また、ステップＳ５１１で書換装置１０２から受け取った識別コードを用いて、書換装置１０２に対応する既定関数を特定しておく。

【００５８】
（図５：ステップＳ５１３～Ｓ５１４）
書換装置１０２は、ステップＳ５１２で受け取った種コードを既定関数に適用して演算結果を算出する（Ｓ５１３）。書換装置１０２は、算出結果を認証サーバ１０３に送信する（Ｓ５１４）。
【００５９】
（図５：ステップＳ５１５）
認証サーバ１０３は、ステップＳ５１２で特定しておいた既定関数を読み出し、ステップＳ５１５で書換装置１０２に対して送信したものと同じコードをこの既定関数に適用して演算結果を算出する。
【００６０】
（図５：ステップＳ５１６）
認証サーバ１０３は、ステップＳ５１４で書換装置１０２から受け取った演算結果と、ステップＳ５１５で算出した演算結果とを比較する。両者が一致すれば書換装置１０２が正規端末であると判断する。認証サーバ１０３は、書換装置１０２を認証許可した旨の情報を、内部の認証済み機器リストに格納する。両者が一致しなければ、書換装置１０２は認証許可されなかったことになる。
【００６１】
（図５：ステップＳ５１７）
認証サーバ１０３は、認証シーケンスＳ５１０が終了した旨を、確認応答として書換装置１０２に対して送信する。このとき、書換装置１０２を認証許可したか否かについての情報を確認応答のなかに含めないこととする。理由は実施形態１のステップＳ１０２で述べた通りである。
【００６２】
（図５：ステップＳ５２０～Ｓ５６０）
これらのステップは、図４のステップＳ４２０～Ｓ４６０と同様である。
【００６３】
＜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、認証サーバ１０３は、公開鍵暗号方式に基づくデジタル署名を用いて書換装置１０２を認証することができる。公開鍵暗号方式では、書換装置１０２の秘密鍵をネットワークに流さなくて済み、また認証サーバ１０３にも書換装置１０２の秘密鍵を開示しなくてよい。これにより、正規の書換装置１０２の秘密鍵を第３者に対して秘匿することができ、車載ネットワークシステム１０００のセキュリティを高めることができる。
【００６４】
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、認証サーバ１０３は、チャレンジ＆レスポンス方式によるワンタイムパスワードを用いて書換装置１０２を認証することができる。チャレンジ＆レスポンス方式によるワンタイムパスワードでは、認証サーバ１０３が生成する種コードが毎回変化するので、書換装置１０２と認証サーバ１０３の間で共有している既定関数を予測することが難しい。これにより、認証処理の内容を第３者に対して秘匿することができ、車載ネットワークシステム１０００のセキュリティを高めることができる。
【００６５】
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、図３で言及した通信ゲートウェイ２０１が認証サーバ１０３としての役割を兼ねることもできる。この構成の下では、図４および図５の各認証シーケンスＳ４１０およびＳ５１０が失敗したとき、書換装置１０２からの通信を、目標ＥＣＵ１０１が属する車載ネットワーク１０５から電気的に切り離すことができる。この構成を用いる場合、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。
【００６６】
＜実施の形態３＞
本発明の実施形態３では、認証サーバ１０３が車載ネットワークシステム１０００から切り離されることによって認証処理が妨害されたり、他機器が認証サーバ１０３に成り済まして不正な認証処理を実施したりすることを防止する構成を説明する。
【００６７】
以上説明した実施形態１～２では、認証処理を認証サーバ１０３に集約してセキュリティレベルを向上させることを図っている。しかしその反面、認証サーバ１０３自体のセキュリティ機能が妨害されると、車載ネットワークシステム１０００全体をセキュリティの脅威にさらすおそれがある。
【００６８】
例えば、目標ＥＣＵ１０１と認証サーバ１０３の間の不可分性が破られ、他機器が認証サーバ１０３に成り済ました場合を考える。すなわち、認証サーバ１０３が車載ネットワークから除去されるか、または車載ネットワークに対する接続を妨害され、悪意ある書換装置１０２と、認証サーバ１０３に成り済ました第３者機器とによって目標ＥＣＵ１０１が騙されてしまうという状況である。
【００６９】
上記のような状況を回避するためには、目標ＥＣＵ１０１と認証サーバ１０３との間の接続が遮断されたり、通信が妨害されたりすることを防止しなければならない。この脆弱性に対抗する手段として、以下の３つが考えられる。
【００７０】
（対策その１：目標ＥＣＵ１０１側の対策）
目標ＥＣＵ１０１は、認証サーバ１０３との間の接続が確保されているか否かを常時監視し、認証サーバ１０３から切り離されていること検知したときには、書換装置１０２からメモリ内部のデータに対する読取要求や書込要求を受け取っても、これを拒否する。
【００７１】
（対策その２：認証サーバ１０３側の対策）
認証サーバ１０３は、目標ＥＣＵ１０１との間の接続が確保されているか否かを常時監視し、目標ＥＣＵ１０１から切り離されていることを検知したときには、ネットワークの構成が不正に変更された、または認証サーバ１０３が単体で車載ネットワークから取り出されている、などの状況が生じていると判断する。このとき認証サーバ１０３は、認証処理を停止し、外部からのいかなる要求に対しても、認証拒否する。

【００７２】
（対策その２：認証サーバ１０３側の対策：補足）
一般に認証サーバ１０３は、複数のＥＣＵに対する接続を監視している立場なので、特定ＥＣＵの取り外しだけでなく、ネットワーク全体の構成変化を検出することができる。この機能を利用して、ネットワーク構成の不正な変更を検出した場合、他のＥＣＵに対してその旨を通知したり、不正な変更によって引き起こされている機能不全状況を通知したりしてもよい。
【００７３】
（対策その３：警告を発信する）
認証サーバ１０３が、車載ネットワーク上に認証サーバ１０３に成り済ましている機器を検出した場合には、不正アクセスされようとしている目標ＥＣＵを防衛するため、目標ＥＣＵに対して積極的に強制中断通知などの警告メッセージを発信する。
【００７４】
図６は、認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されているか否かを確認する処理シーケンスを示す図である。ここでは認証サーバ１０３が主体となって接続確認を実施する例を示す。図６に示す処理シーケンスでは、チャレンジ＆レスポンス方式に

基づくワンタイムパスワードを用いて、接続確認を実施する。以下、図６に示す各ステップについて説明する。

【００７５】

（図６：ステップＳ６１０）

認証サーバ１０３と目標ＥＣＵ１０１は、以下に説明するステップＳ６１１～Ｓ６１９からなる接続確認シーケンスＳ６１０を実行する。なお、あらかじめ目標ＥＣＵ１０１と認証装置１０３の間で、後述するステップＳ６１２～Ｓ６１４で用いる既定関数を共用しておくものとする。

【００７６】

（図６：ステップＳ６１１～Ｓ６１４）

認証サーバ１０３は、接続確認処理を開始する。例えば所定の時間間隔で周期的に本ステップを開始することにより、周期的に接続確認を実施することができる。具体的な処理手順は図５のステップＳ５１２～Ｓ５１６と同様であるが、ここでは認証サーバ１０３と目標ＥＣＵ１０１の間で処理を実施する点が異なる。

【００７７】

（図６：ステップＳ６１５）

認証サーバ１０３は、目標ＥＣＵ１０１における演算結果と認証サーバ１０３における演算結果を比較する。両者が一致した場合は、認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されていることを確認できたものとし、タイムアウトを計測するためのタイマをリセットする。一致しなかった場合は、接続が確認できなかったものとする。

【００７８】

（図６：ステップＳ６１５：補足その１）

接続確認処理は周期的に起動されるので、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が確立されていれば、同じ周期で両者の間の接続を確認できるはずである。そこで、両者の間の接続が確認できない期間が所定のタイムアウト時間を超過した場合、認証サーバ１０３は、両者が切断されていると判断する。本ステップにおいて両者の間の接続が確認できた場合、改めてタイムアウト時間を計測するため、タイマをリセットする。

【００７９】

（図６：ステップＳ６１５：補足その２）

認証サーバ１０３は、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が切断されていると判断した場合、認証処理を停止し、ネットワーク構成が不正に変更された旨の警告を発するなどの防衛手段を実行する。

【００８０】

（図６：ステップＳ６１６～Ｓ６１８）

認証サーバ１０３は、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が確立されていることを目標ＥＣＵ１０１の側でも確認させるため、ステップＳ６１４で得た演算結果に対して改めて既定関数を適用した演算結果を用いて、ステップＳ６１２～Ｓ６１４と同様の処理を反対方向で実施する。

【００８１】

（図６：ステップＳ６１９）

目標ＥＣＵ１０１は、目標ＥＣＵ１０１における演算結果と認証サーバ１０３における演算結果を比較する。両者が一致した場合は、認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されていることを確認できたものとし、タイムアウトを計測するためのタイマをリセットする。一致しなかった場合は、接続が確認できなかったものとする。

【００８２】

（図６：ステップＳ６１９：補足）

目標ＥＣＵ１０１は、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が切断されていると判断した場合、書換装置１０２からメモリ内部のデータに対する読取要求や書込要求を受け取っても、これを拒否する。

【００８３】

図７は、認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されているか否かを確認する別の処理シーケンスを示す図である。ここでは図６と同様に、認証サーバ１０３が主体となって接続確認を実施する例を示す。図７に示す処理シーケンスでは、メッセージＩＤホッピング方式を用いて、接続確認を実施する。

【００８４】

メッセージＩＤホッピングとは、所定のＩＤ値を有するメッセージを宛先へ送信し、送信側と受信側でそのＩＤ値を同じ値だけシフトした結果を送信側と受信側で相互に確認し合うことにより、互いを認証する方式である。以下、図７に示す各ステップについて説明する。

【００８５】

（図７：ステップＳ７１０）

認証サーバ１０３と目標ＥＣＵ１０１は、以下に説明するステップＳ７１１～Ｓ７１８からなる接続確認シーケンスＳ７１０を実行する。なお、あらかじめ目標ＥＣＵ１０１と認証装置１０３の間で、後述するステップＳ７１２～Ｓ７１３で用いるシフト値を共用しておくものとする。

【００８６】

（図７：ステップＳ７１１）

認証サーバ１０３は、所定のＩＤ値のメッセージを目標ＥＣＵ１０１に送信することにより、目標ＥＣＵ１０１に対して問いかけを発信する。

【００８７】

（図７：ステップＳ７１２）

目標ＥＣＵ１０１は、あらかじめ認証サーバ１０３と共有しておいたシフト値を用いて認証サーバ１０３から受け取ったＩＤ値をシフトし、ＥＣＵ側ＩＤとして認証サーバ１０３へ返信する。

【００８８】

（図７：ステップＳ７１３）

認証サーバ１０３は、目標ＥＣＵ１０１との間で共用しているシフト値を用いて、ステップＳ７１１で目標ＥＣＵ１０１に送信したＩＤ値をシフトし、目標ＥＣＵ１０１から返信されてくるＥＣＵ側ＩＤを予測する。

【００８９】

（図７：ステップＳ７１４）

認証サーバ１０３は、ステップＳ７１２で目標ＥＣＵ１０１が送信するＥＣＵ側ＩＤとステップＳ７１３で予測したＩＤとを比較する。両者が一致した場合は、認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されていることを確認できたものとし、タイムアウトを計測するためのタイマをリセットする。一致しなかった場合は、接続が確認できなかったものとする。タイムアウトについては図６と同様である。

【００９０】

（図７：ステップＳ７１４：補足）

認証サーバ１０３は、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が切断されていると判断した場合、認証処理を停止し、ネットワーク構成が不正に変更された旨の警告を発するなどの防衛手段を実行する。

【００９１】

（図７：ステップＳ７１５～Ｓ７１７）

目標ＥＣＵ１０１は、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が確立されていることを目標ＥＣＵ１０１の側でも確認するため、自己が保持している所定のＩＤ値を用いて、ステップＳ７１１～Ｓ７１３と同様の処理を反対方向で実施する。

【００９２】

（図７：ステップＳ７１８）

目標ＥＣＵ１０１は、ステップＳ７１６で認証サーバ１０３が返信するサーバ側ＩＤと

ステップＳ７１７で予測したＩＤとを比較する。両者が一致した場合は、認証サーバ１０３と目標ＥＣＵ１０１の間の接続が確立されていることを確認できたものとし、タイムアウトを計測するためのタイマをリセットする。一致しなかった場合は、接続が確認できなかったものとする。

【００９３】

（図７：ステップＳ７１８：補足）

目標ＥＣＵ１０１は、目標ＥＣＵ１０１と認証サーバ１０３の間の接続が切断されていると判断した場合、書換装置１０２からメモリ内部のデータに対する読取要求や書込要求を受け取っても、これを拒否する。

【００９４】

図８は、認証サーバ１０３が車載ネットワーク上で認証サーバ１０３に成り済ました動作を実施している機器（不正端末８０１）を検出した場合の動作を説明する図である。以下、図８の各ステップについて説明する。

【００９５】

（図８：ステップＳ８０１）

不正端末８０１は、認証サーバ１０３に対して認証要求せずに、目標ＥＣＵ１０１に対して直接アクセスしようと試みる。不正端末８０１は、目標ＥＣＵ１０１に対してセッション開始要求を送信する。

【００９６】

（図８：ステップＳ８０２）

目標ＥＣＵ１０１は、不正端末８０１からセッション開始要求を受け取ると、認証サーバ１０３に対し、不正端末８０１が認証許可済みであるか否かを照会する。このとき、車載ネットワークが一般にバス型構成を採用しているため、本照会は車載ネットワークに接続されている各機器に到達する。そのため、認証サーバ１０３と不正端末８０１ともに、目標ＥＣＵ１０１からの照会を捕捉することができる。

【００９７】

（図８：ステップＳ８０３）

認証サーバ１０３は、不正端末８０１が認証許可済みでない旨を、目標ＥＣＵ１０１に対して通知する。

【００９８】

（図８：ステップＳ８０４）

不正端末８０１は、偽の認証済通知を目標ＥＣＵ１０１に対して送信する準備を開始する。不正端末８０１は、認証サーバ１０３が送信する未認証通知が目標ＥＣＵ１０１に到達しないようにするため、ジャミング信号を送出する、または目標ＥＣＵ１０１と認証サーバ１０３の間のネットワーク接続を瞬断（図示せず）するなどして、未認証通知が目標ＥＣＵ１０１に到達することを妨害する。

【００９９】

（図８：ステップＳ８０５）

不正端末８０１は、認証サーバ１０３が送出したかのように装って、偽の認証済通知を目標ＥＣＵ１０１に対して送信する。このとき、ステップＳ８０２と同様に、偽の認証済通知は認証サーバ１０３にも到達する。これにより認証サーバ１０３は、不正端末８０１の存在を検出することができる。

【０１００】

（図８：ステップＳ８０６）

目標ＥＣＵ１０１は、偽の認証済通知を受け取り、不正端末８０１との間の正規セッションを開始する。このとき、不正端末８０１の識別コードを含むセッション受諾通知を発信する。

【０１０１】

（図８：ステップＳ８０７）

認証サーバ１０３は、偽の認証済通知を検出すると、目標ＥＣＵ１０１に対し、強制中

断するように通知する。これにより、不正端末８０１が目標ＥＣＵ１０１内部のデータを不正に取得したり、プログラムを不正に書き換えたりすることを防止することを図る。

【０１０２】

（図８：ステップＳ８０８）

ステップＳ８０７において認証サーバ１０３が偽の認証済通知を検出できなくても、目標ＥＣＵ１０１が不正端末８０１との間の正規セッションを開始するときにセッション受諾通知を発信するので、これに基づき不正端末８０１の存在を検出できる。具体的には、セッション受諾通知には不正端末８０１の識別コードが含まれているので、認証サーバ１０３は認証処理を介さずに目標ＥＣＵ１０１に対して直接アクセスしている端末を検出することができる。認証サーバ１０３は、不正端末８０１を検出すると、ステップＳ８０７と同様の処理を実施する。

【０１０３】

（図８：ステップＳ８０９）

目標ＥＣＵ１０１は、強制中断通知を受け取ると、不正端末８０１との間の通信セッションを強制終了させる。

【０１０４】

＜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によれば、認証サーバ１０３は、目標ＥＣＵ１０１との間の通信が確立されているか否かを周期的に確認し、接続が遮断されていることを検出したときは認証処理を停止する。これにより、認証サーバ１０３が車載ネットワークから不正に切り離されたような場合には、認証処理を実施することができなくなるので、不正アクセスを未然に防止することができる。

【０１０５】

また、本実施形態３に係る車載ネットワークシステム１０００によれば、目標ＥＣＵ１０１は、認証サーバ１０３との間の通信が確立されているか否かを周期的に確認し、接続が遮断されていることを検出したときは書換装置１０２からの読取要求および書込要求を拒否する。これにより、上記と同様の効果を発揮することができる。

【０１０６】

また、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、認証サーバ１０３と目標ＥＣＵ１０１の間の接続確認は、チャレンジ＆レスポンス方式やメッセージＩＤシフト方式によって実施される。これにより、両者の間の接続確認方式を第３者に対して秘匿することができるので、接続確認手続きを模倣しようとする不正端末を排除することができる。なお、メッセージＩＤのシフト量に関しては、接続確認する両ノード間であらかじめ共有しておいてもよいし、最初の問いかけメッセージ中にそのシフト量の種になるデータを忍び込ませておくなどして秘密裏に共有してもよい。

【０１０７】

また、本実施形態３に係る車載ネットワークシステム１０００によれば、認証サーバ１０３は、車載ネットワーク上で認証サーバ１０３に成り済ました機器を検出すると、目標ＥＣＵ１０１に対して強制中断通知を送信する。これにより、認証サーバ１０３と目標ＥＣＵ１０１の間の接続を切断することなく不正アクセスを試みる不正端末８０１を排除することができる。

【０１０８】

また、本実施形態３において、認証サーバ１０３が主体となって接続確認を実施することを説明したが、目標ＥＣＵ１０１が主体となって実施してもよい。いずれの場合でも、認証サーバ１０３と目標ＥＣＵ１０１双方が同様の接続確認を互いに実施することにより確実に接続を確認することができる。

【０１０９】

＜実施の形態４＞

以上の実施形態１～３において、認証サーバ１０３が書換装置１０２を認証許可するとき、目標ＥＣＵ１０１内部のデータに対して読み取りまたは書き込みを実施することので

きる権限を有する旨を示す、セッションチケットを発行することもできる。目標ＥＣＵ１０１は、認証サーバ１０３が認証許可済みである書換装置１０２であっても、権限を有するセッションチケットを保持していない書換装置１０２については、読取要求または書込要求を拒否するようにしてもよい。

【０１１０】

このセッションチケットは、認証サーバ１０３および目標ＥＣＵ１０１の間のみで共有されている通信識別子であり、書換装置１０２が目標ＥＣＵ１０１に対して書き込みまたは読み取りを実施する権限を有する旨の認証許可を受けたことを示す。書換装置１０２は、認証サーバ１０３によって認証許可された場合のみ、セッションチケットを得ることができる。

【０１１１】

実施形態１～３で説明した手法と併用して本実施形態４のセッションチケットを用いることにより、車載ネットワークシステム１０００のセキュリティレベルをさらに向上させることができる。

【０１１２】

＜実施の形態５＞

図９は、以上の実施形態１～４において目標ＥＣＵ１０１が書換装置１０２からセッション開始要求を受け取ったときに実施する処理フローの一例を示す図である。本発明では認証処理が認証サーバ１０３に集約されているので、目標ＥＣＵ１０１が実施すべき処理は簡略化されている。ここでは例として、書換装置１０２が目標ＥＣＵ１０１内部のフラッシュＲＯＭに格納されているプログラムを書き換えるように要求した場合を示す。以下図９の各ステップについて説明する。

【０１１３】

（図９：ステップＳ９０１～Ｓ９０２）

目標ＥＣＵ１０１は、図６または図７で例示したような接続確認処理を実施し、認証サーバ１０３との間の接続が確立されているか否かを判定する。目標ＥＣＵ１０１は、認証サーバ１０３との間の接続が切断されていることを検出したときはステップＳ９０８へ進み、接続が確立されていることを確認したときはステップＳ９０３へ進む。

【０１１４】

（図９：ステップＳ９０３）

目標ＥＣＵ１０１は、書換装置１０２からのセッション開始要求を受け取るまでの間はステップＳ９０１～Ｓ９０３を繰り返し実行し、セッション開始要求を受け取るとステップＳ９０４へ進む。

【０１１５】

（図９：ステップＳ９０４～Ｓ９０６）

目標ＥＣＵ１０１は、認証サーバ１０３に書換装置１０２の認証結果を照会する。認証許可済みである場合はステップＳ９０６へ進んで書換装置１０２との間の正規セッションを開始し、セッション受諾通知を発信する。認証許可済みでない場合は、ステップＳ９０８へ進む。

【０１１６】

（図９：ステップＳ９０７）

目標ＥＣＵ１０１は、書換装置１０２からの書込要求を処理する手続きを開始する。認証サーバ１０３は、ステップＳ９０６のセッション受諾通知を受信することによって、目標ＥＣＵ１０１が書込要求の処理を開始したことを認識することができる。目標ＥＣＵ１０１が本処理を実施している間は他のＥＣＵが目標ＥＣＵ１０１と通信しようとしても応答することができないので、認証サーバ１０３は、目標ＥＣＵ１０１が現在ビジー状態である旨を他のＥＣＵにブロードキャストなどで通知してもよい。

【０１１７】

（図９：ステップＳ９０８）

目標ＥＣＵ１０１は、車載ネットワークシステム１０００のセキュリティ異常が生じて

いると判断し、書換装置１０２からの書込要求を強制終了する。書込要求をまだ受け取っていない場合は、以後の受付を禁止する。

【０１１８】

（図９：ステップＳ９０９）

目標ＥＣＵ１０１は、ステップＳ９０７を開始した後も、認証サーバ１０３からの強制中断通知（アボート通知）を周期的にチェックしている。アボート通知があれば、ステップＳ９０８にスキップして書込要求を強制終了する。これは、図８ステップＳ８０９に相当する。アボート通知がなければ、ステップＳ９１０に進む。

【０１１９】

（図９：ステップＳ９１０～Ｓ９１１）

目標ＥＣＵ１０１は、書換装置１０２からの書込要求を所定の処理単位毎に処理する。書込要求を全て処理し終えた場合は本処理フローを終了し、残っている場合はステップＳ９０９に戻って同様の処理を繰り返す。

【０１２０】

＜実施の形態５：まとめ＞

ステップＳ９０７において、目標ＥＣＵ１０１がフラッシュＲＯＭ内のデータを書き換えていることを想定する。フラッシュＲＯＭ内のデータを書き換えるためには、それに用いる制御プログラムをそのままフラッシュＲＯＭに置いておくことができず、いったん該当プログラムをＲＡＭなどの揮発性メモリに展開する必要がある。一般のマイコンでは、フラッシュＲＯＭに比べてＲＡＭの容量は極端に少ないので、高度な認証プログラムやセキュリティ監視プログラムを書き換えプログラムとともに展開することができない。

また、フラッシュＲＯＭにデータを書き込む際には、所定の電荷量をフラッシュＲＯＭのメモリセルに対して印加する必要があり、これは制御プログラムによる時間変調で行われる。したがって、ステップＳ９０７における処理は、この厳密な時間的制約のため、予定通りの時間内で厳密に完了する必要があるといえる。

【０１２１】

そのため、ステップＳ９０７における目標ＥＣＵ１０１の処理負荷を軽減して本来の書込処理に専念させるため、認証手続きおよびセッション開始後のセキュリティ監視手続きについて認証サーバ１０３に委譲することは有用であるといえる。

【０１２２】

＜実施の形態６＞

以上の実施形態１～５では、目標ＥＣＵ１０１が備えているプログラムを書き換える手法を説明したが、同様の手法を用いて、認証サーバ１０３が保持しているプログラムを書き換えることもできる。これにより、認証アルゴリズムをより高度なものに更新するなどしてセキュリティレベルを向上させることができる。また、各ＥＣＵのプログラムを書き換えることなく認証処理を更新することができるので、コスト面で有利である。

【０１２３】

また、認証サーバ１０３の機能は、各ＥＣＵの通常の制御動作とは無関係であるので、車載ネットワークを停止せず、すなわち車両動作を停止せずに、認証アルゴリズムのみを書き換えることができる点も有利である。

【０１２４】

なお、認証サーバ１０３のプログラムを書き換える処理も、実施形態１～５と同様に書換装置１０２によって実施することができる。この場合の認証処理は、目標ＥＣＵ１０１は関与せず、認証サーバ１０３と書換装置１０２の間のみでの処理となる。

【０１２５】

＜実施の形態７＞

図１０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。認証サーバ１０３、ゲートウェイ装置２０１、各ＥＣＵなどの構成および動作は、実施形態１～６と同様である。

【０１２６】

図１０において、４群のネットワークが搭載されており、各々図３で説明した通信ゲートウェイ（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１０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。

【０１２７】

図１０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。

【０１２８】

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。

【０１２９】

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。

【０１３０】

書換装置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。

【０１３１】

電話用無線機３２１を通じて外部から特定の車載ＥＣＵの内部データまたはプログラムを書き換えることもできる。この場合において、電話網越しに車載ＥＣＵに書込要求を発行する機器を認証する際にも、実施形態１～６と同様の手法を用いることができる。

【０１３２】

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。この場合も、本発明で開示する技術は、車載ネットワークへの不正な侵入を防止し、真正な（改竄から保護された）ソフトウェアの配布と書き換えを保証することができる。

【０１３３】

図１０では、認証サーバ１０３を通信ゲートウェイＥＣＵ２０１の配下に直接接続したが、認証サーバ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、書換装置１０２と同様に、他のネットワークに直接接続してもよい。

【０１３４】

ただし、書換装置１０２と異なる点は、目標ＥＣＵ１０１（図１０においては、同図に示す各ＥＣＵ）との間の電気的な切り離しを防ぐ必要がある。その観点では、通信ゲート

ウェイＥＣＵ２０１が認証サーバ１０３の役割を兼ねることが望ましい。認証サーバ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。

【０１３５】

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。

【０１３６】

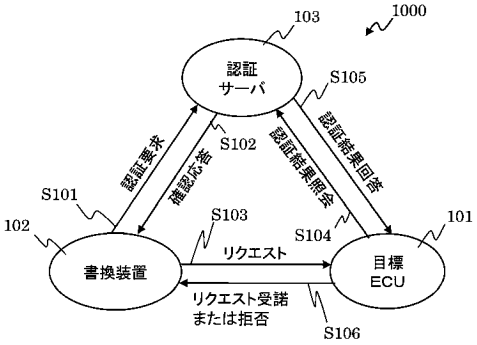
また、上記各構成、機能、処理部などは、それらの全部または一部を、例えば集積回路で設計することによりハードウェアとして実現することもできるし、プロセッサがそれぞれの機能を実現するプログラムを実行することによりソフトウェアとして実現することもできる。各機能を実現するプログラム、テーブルなどの情報は、メモリやハードディスクなどの記憶装置、ＩＣカード、ＤＶＤなどの記憶媒体に格納することができる。

【符号の説明】

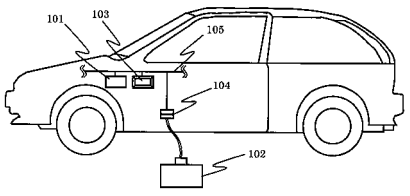
【０１３７】

１０１：目標ＥＣＵ、１０２：書換装置、１０３：認証サーバ、１０４：接続用車両コネクタ、１０５：車載ネットワーク、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、１０００：車載ネットワークシステム。

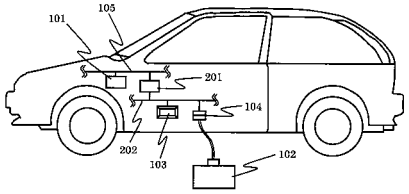
【図１】



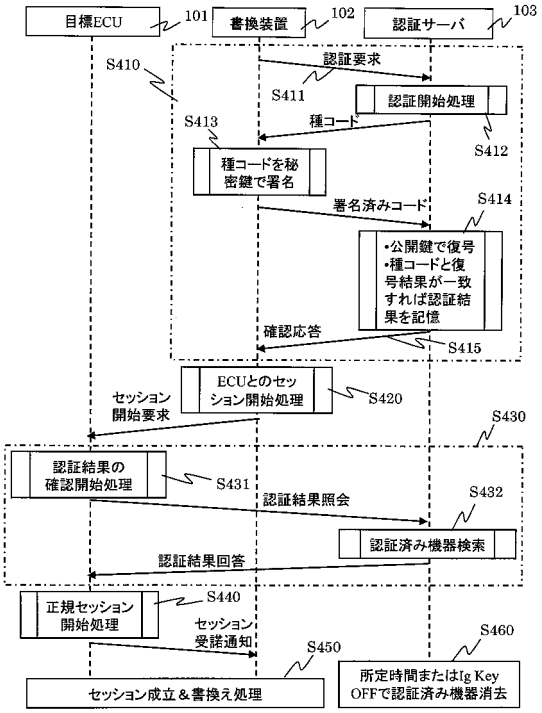
【図２】



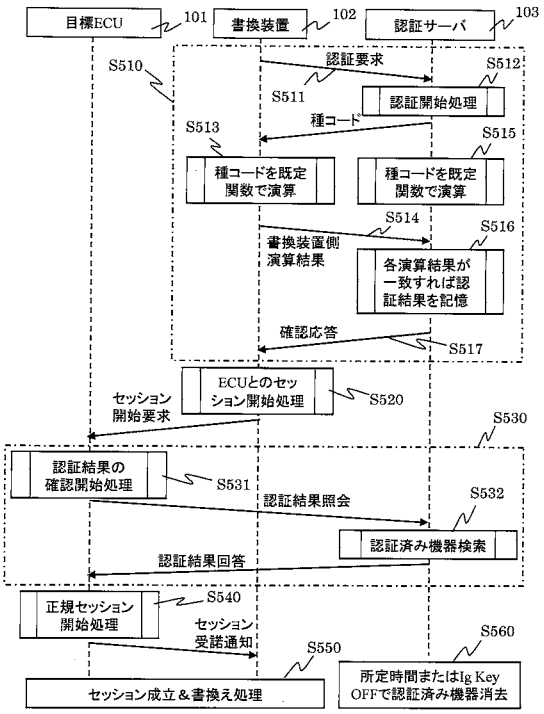
【図３】



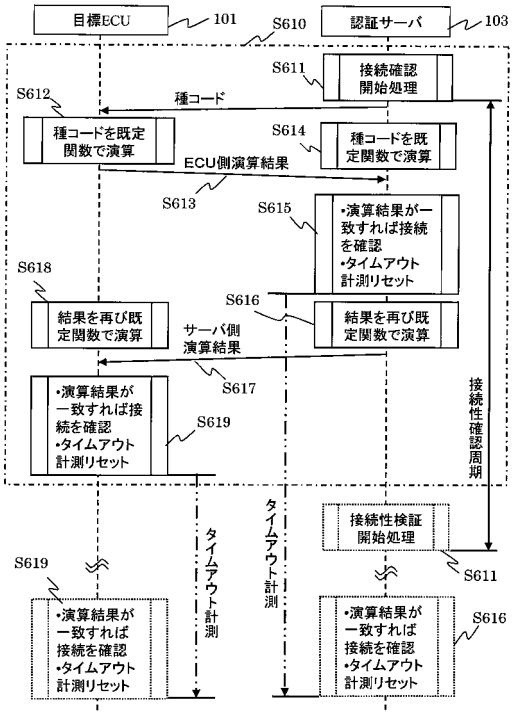
【図４】



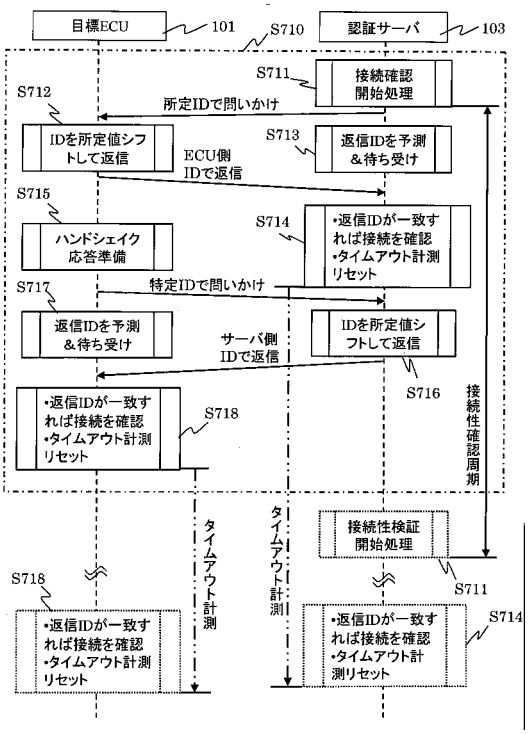
【図５】


目標ECU
101
書換装置
102
認証サーバ
103
S510
認証要求
S511
S512
認証開始処理
種コード
S513
S515
種コードを既定関数で演算
種コードを既定関数で演算
S514
書換装置側演算結果
S516
各演算結果が一致すれば認証結果を記憶
確認応答
S517
ECUとのセッション開始処理
S520
セッション開始要求
S530
認証結果の確認開始処理
S531
認証結果照会
S532
認証済み機器検索
認証結果回答
正規セッション開始処理
S540
セッション受諾通知
S550
S560
セッション成立＆書換え処理
所定時間またはIg Key OFFで認証済み機器消去

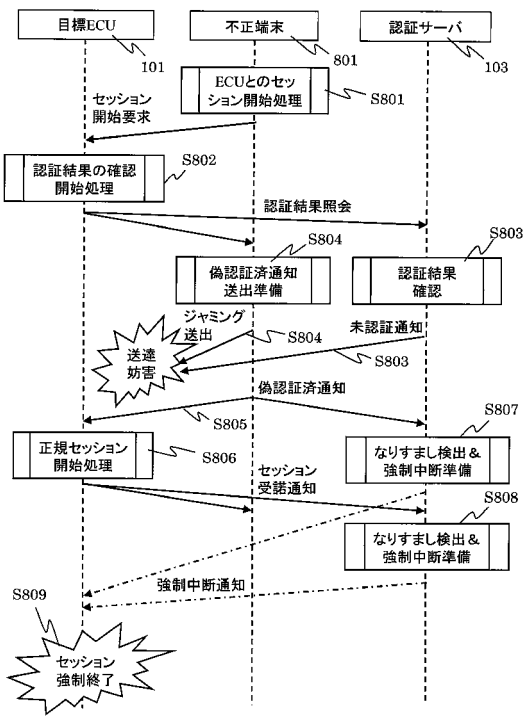
【図６】


目標ECU
101
S610
認証サーバ
103
S611
接続確認開始処理
S612
種コード
種コードを既定関数で演算
S614
種コードを既定関数で演算
ECU側演算結果
S613
S615
•演算結果が一致すれば接続を確認
•タイムアウト計測リセット
S618
S616
結果を再び既定関数で演算
結果を再び既定関数で演算
サーバ側演算結果
S617
•演算結果が一致すれば接続を確認
•タイムアウト計測リセット
S619
接続性確認周期
タイムアウト計測
タイムアウト計測
接続性検証開始処理
S611
S619
•演算結果が一致すれば接続を確認
•タイムアウト計測リセット
•演算結果が一致すれば接続を確認
•タイムアウト計測リセット
S616

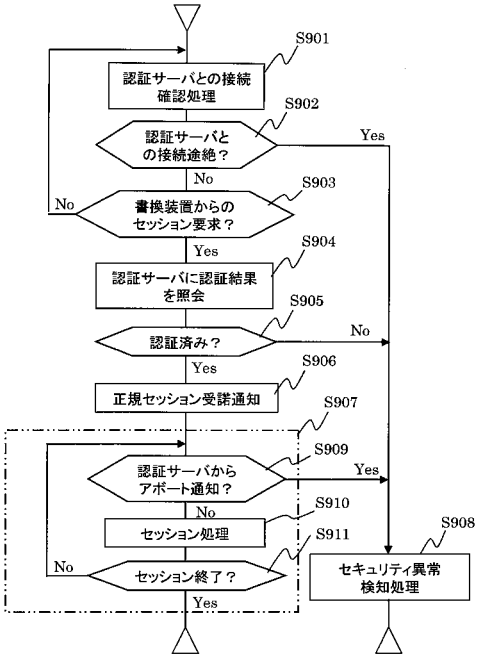
【図７】


目標ECU
101
S710
認証サーバ
103
S711
接続確認開始処理
S712
所定IDで問いかけ
IDを所定値シフトして返信
S713
返信IDを予測＆待ち受け
ECU側IDで返信
S715
ハンドシェイク応答準備
S714
•返信IDが一致すれば接続を確認
•タイムアウト計測リセット
S717
特定IDで問いかけ
返信IDを予測＆待ち受け
IDを所定値シフトして返信
サーバ側IDで返信
S716
•返信IDが一致すれば接続を確認
•タイムアウト計測リセット
S718
接続性確認周期
タイムアウト計測
タイムアウト計測
接続性検証開始処理
S711
S718
•返信IDが一致すれば接続を確認
•タイムアウト計測リセット
•返信IDが一致すれば接続を確認
•タイムアウト計測リセット
S714

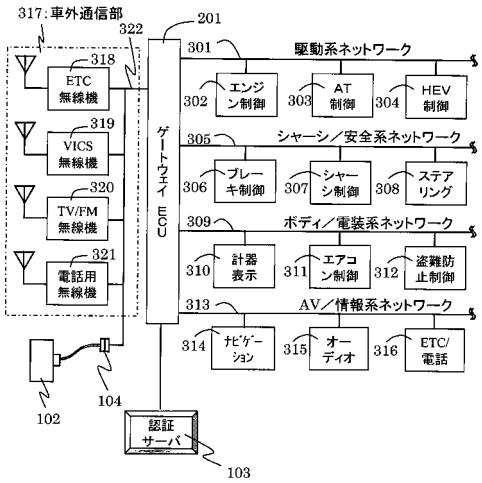
【図８】


目標ECU
101
不正端末
801
認証サーバ
103
ECUとのセッション開始処理
S801
セッション開始要求
S802
認証結果の確認開始処理
認証結果照会
S804
S803
偽認証済通知送出準備
認証結果確認
ジャミング送出
S804
未認証通知
S803
送達妨害
偽認証済通知
S805
S807
正規セッション開始処理
S806
なりすまし検出＆強制中断準備
セッション受諾通知
S808
なりすまし検出＆強制中断準備
強制中断通知
S809
セッション強制終了

【図９】


S901
認証サーバとの接続確認処理
S902
認証サーバとの接続途絶？
Yes
No
S903
No
書換装置からのセッション要求？
Yes
S904
認証サーバに認証結果を照会
S905
認証済み？
No
Yes
S906
正規セッション受諾通知
S907
S909
認証サーバからアボート通知？
Yes
No
S910
セッション処理
S911
No
セッション終了？
Yes
S908
セキュリティ異常検知処理

【図１０】


317:車外通信部
322
201
301
駆動系ネットワーク
318
ETC無線機
302
エンジン制御
303
AT制御
304
HEV制御
319
VICS無線機
305
シャーシ／安全系ネットワーク
320
TV/FM無線機
306
ブレーキ制御
307
シャーシ制御
308
ステアリング
309
ボディ／電装系ネットワーク
321
電話用無線機
310
計器表示
311
エアコン制御
312
盗難防止制御
313
AV／情報系ネットワーク
ゲートウェイECU
314
ナビゲーション
315
オーディオ
316
ETC/電話
102
104
認証サーバ
103

フロントページの続き

(56)参考文献 特開２００２－１５７１６５（ＪＰ，Ａ）
特開２００４－１３３８２４（ＪＰ，Ａ）
特開２００１－２５５９５２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－Ｇ０６Ｆ２１／８８
Ｂ６０Ｒ　１６／０２３
Ｈ０４Ｌ　１２／２８