(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2019-61663
(P2019-61663A)
(43)公開日　平成31年4月18日(2019.4.18)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/44	(2013.01)	G06F	21/44	
B60R 16/023	(2006.01)	B60R	16/023	P

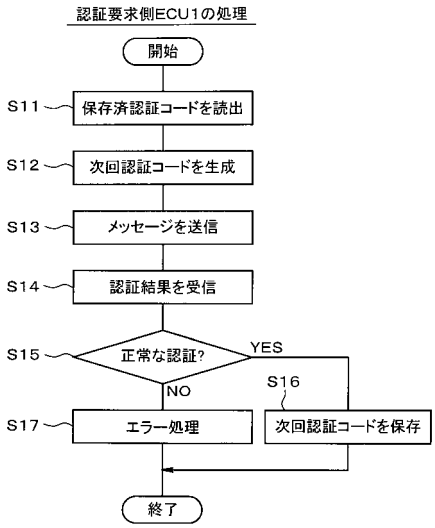
審査請求 未請求　請求項の数 8　ＯＬ　（全 11 頁）

(21)出願番号　特願2018-165972 (P2018-165972)
(22)出願日　平成30年9月5日 (2018.9.5)
(31)優先権主張番号　特願2017-186403 (P2017-186403)
(32)優先日　平成29年9月27日 (2017.9.27)
(33)優先権主張国　日本国 (JP)

(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　110000567
特許業務法人　サトー国際特許事務所
(72)発明者　安藤　友樹
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内

(54)【発明の名称】電子制御装置

(57)【要約】　（修正有）
【課題】なりすましを極力防止できるようにした電子制御装置を提供する。
【解決手段】ＥＣＵ１は、認証コードを生成し、ＥＣＵ２との間で予め共有された認証コードを保存済認証コードとして不揮発性メモリに記憶している。ＥＣＵ１は、Ｓ１１～Ｓ１３において保存済認証コードと改めて生成された次回認証コードとをＥＣＵ２に送信する。ＥＣＵ１は、Ｓ１５、Ｓ１６において、送信された保存済認証コード及び次回認証コードが認証受付側のＥＣＵ２にて正常に認証されたことを条件として次回認証コードを不揮発性メモリに保存する。
【選択図】図４



【特許請求の範囲】
【請求項１】
複数の電子制御装置の間で認証処理を実施する認証システムを構成する認証要求側の第１電子制御装置（１）であって、
認証コードを生成する認証コード生成部（１１、Ｓ１）と、
第２電子制御装置との間で予め共有された認証コードを保存済認証コードとして記憶する第１記憶部（１２，１５、Ｓ４、Ｓ１６）と、
前記第１記憶部に記憶された保存済認証コードと、前記認証コード生成部により生成された次回認証コードとを、前記第２電子制御装置に送信する送信部（１３、Ｓ１３）と、
前記送信された保存済認証コード及び次回認証コードが前記第２電子制御装置において正常に認証されたことを条件として前記次回認証コードを保存する第１保存部（１２，１５、Ｓ１６）と、
を備える電子制御装置。
【請求項２】
前記認証コード生成部は、認証処理を実施する度に、前記次回認証コードをランダムに生成する請求項１記載の電子制御装置。
【請求項３】
前記第２電子制御装置における認証コードの認証結果が認証エラーとなるときにはエラー処理を実行する認証要求側エラー処理実行部（１１、Ｓ１７）、をさらに備える請求項１または２記載の電子制御装置。
【請求項４】
複数の電子制御装置の間で認証処理を実施する認証システムを構成する認証受付側の第２電子制御装置（２）であって、
第１電子制御装置（１）から送信される前回認証コード及び次回認証コードを受信する第１受信部（２３、Ｔ１）と、
前記第１電子制御装置から前回受信された認証コードを保存済認証コードとして記憶する第２記憶部（２２，２５、Ｔ２、Ｔ１５）と、
前記第２記憶部に記憶された保存済認証コードが、前記第１受信部により受信した前回認証コードに含まれるときに正常な認証と判断し前記第１受信部により受信した前記次回認証コードを保存する第２保存部（２２，２５、Ｔ１５）と、
を備える電子制御装置。
【請求項５】
前記第２記憶部に記憶された保存済認証コードが、前記受信部により受信した前回認証コードに含まれないときには認証エラーと判断し、認証エラー処理を実行する認証受付側エラー処理実行部（２１、Ｔ１６）、をさらに備える請求項４記載の電子制御装置。
【請求項６】
前記第２記憶部に記憶された保存済認証コードと、前記受信部により受信した前回認証コードとの認証結果を、前記第１電子制御装置に送信する認証結果送信部（２３、Ｔ１７）、をさらに備える請求項５記載の電子制御装置。
【請求項７】
請求項１から３の何れか一項に記載の認証要求側の第１電子制御装置（１）であって、
第２電子制御装置（２）から前回認証コード及び次回認証コードを受信する第２受信部（１３、Ｔ１１）と、
前記第２電子制御装置から前回受信された認証コードを保存済認証コードとして記憶する第３記憶部（１２，１５、Ｔ２）と、
前記第３記憶部に記憶された保存済認証コードと、前記第２受信部により受信した前回認証コードとに応じて認証する認証部（１１、Ｔ１３）と、
を備える電子制御装置。
【請求項８】
前記第３記憶部に記憶された保存済認証コードが、前記第２受信部により受信した前回

認証コードに含まれるときに正常な認証と判断し前記第２受信部により受信した前記次回認証コードを保存する第３保存部（１２，１５、Ｔ１５）、をさらに備える請求項７記載の電子制御装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子制御装置に関する。
【背景技術】
【０００２】
車載ネットワークシステムは、複数のＥＣＵ（Electronic Control Unit）をネットワーク接続して連携動作して車両用機器を制御するシステムである。この種の車載ネットワークシステムでは、各ＥＣＵは、工場出荷時の初回の起動時に、各ＥＣＵに一意の識別情報を有するメッセージを送信すると共に、他のＥＣＵからメッセージを受信し、当該メッセージから抽出した識別情報が登録されたリストを作成する。工場出荷後に起動した各ＥＣＵは、他のＥＣＵから受信したメッセージから抽出した識別情報がリストに登録されていない場合、異常検知処理を行うようにする技術が提供されている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開平１１－１７４１０５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
前述した特許文献１記載の技術を適用したときには、例えば識別情報が漏えいしてしまうと、識別情報が漏洩したＥＣＵを、任意のＥＣＵに変更可能になってしまうという問題を生じる。任意のＥＣＵに変更可能になると、所謂なりすましできるようになってしまう。
本発明の目的は、識別情報が漏洩したとしても、なりすましを極力防止できるようにした電子制御装置を提供することにある。
【課題を解決するための手段】
【０００５】
請求項１記載の発明は、認証処理を実施する認証システムを構成する認証要求側の第１電子制御装置を対象としている。この請求項１記載の発明によれば、認証コード生成部と、第１記憶部と、送信部と、第１保存部と、を備える。認証コード生成部は認証コードを生成し、第１記憶部は第２電子制御装置との間で予め共有された認証コードを保存済認証コードとして記憶する。送信部は、記憶部に記憶された保存済認証コードと、認証コード生成部により生成された次回認証コードとを第２電子制御装置に送信する。第１保存部は、送信された保存済認証コード及び次回認証コードが第２電子制御装置において正常に認証されたことを条件として次回認証コードを保存する。認証要求側において、次回認証コードを次の認証に用いることができるようになるため、これらの処理が繰り返されることで認証コードを次々に変更できるようになる。したがって、たとえ古い識別コードが漏洩したとしても当該古い識別コードを用いて認証処理できなくなり、意図しない電子制御装置に変更されたことを検出できるようになり、なりすましを極力防止できるようになる。
【０００６】
請求項４記載の発明は、認証処理を実施する認証システムを構成する認証受付側の第２電子制御装置を対象としている。この請求項４記載の発明によれば、受信部と、第２記憶部と、第２保存部と、を備える。受信部は、第１電子制御装置から送信される前回認証コード及び次回認証コードを受信する。第２記憶部は、第１電子制御装置から前回受信され

た認証コードを保存済認証コードとして記憶する。第２保存部は、第２記憶部に記憶された保存済認証コードに、受信部により受信した前回認証コードが含まれるときに正常な認証と判断し次回認証コードを保存する。認証受付側において、次回認証コードを次の認証に用いることができるようになるため、これらの処理が繰り返されることで認証コードを次々に変更できるようになる。したがって、たとえ古い識別コードが漏洩したとしても当該古い識別コードを用いて認証処理できなくなり、意図しない電子制御装置に変更されたことを検出できるようになり、なりすましを極力防止できるようになる。

【図面の簡単な説明】

【０００７】

【図１】一実施形態における車載ネットワークシステムの構成例

【図２】認証要求側の第１電子制御装置の初期化処理を概略的に示すフローチャート

【図３】認証受付側の第２電子制御装置の初期化処理を概略的に示すフローチャート

【図４】認証要求側の第１電子制御装置の認証時処理を概略的に示すフローチャート

【図５】認証受付側の第２電子制御装置の認証時処理を概略的に示すフローチャート

【図６】第１及び第２電子制御装置間の認証時処理の流れの一例を示すシーケンス図

【図７】第１及び第２電子制御装置間の認証時処理の流れの一例を示すタイミングチャート

【発明を実施するための形態】

【０００８】

以下、本発明の電子制御装置の実施形態について図面を参照しながら説明する。

図１は車載ネットワークシステムの中の認証システムの構成例を示している。車両内には、複数のＥＣＵ（Electronic Control Unit：電子制御装置）１、２…３が、車載ネットワーク（例えばＣＡＮバス）４に接続されており、互いに各種情報を送受信可能に構成されており、これらのＥＣＵ１、２…３により認証システムが構成されている。ＣＡＮは登録商標である。

【０００９】

ＥＣＵ１は、ＣＰＵ１１、メモリ１２、及び通信回路１３などバス１４に接続して構成された第１電子制御装置に相当するものであり、車両内の各種センサ、アクチュエータ（何れも図示せず）などを制御するように構成される。メモリ１２は、不揮発性メモリ１５及び揮発性メモリ（図示せず）によるもので、ＣＰＵ１１は、メモリ１２に記憶された制御プログラムに基づいて動作する。メモリ１２は非遷移的実効的記録媒体として用いられる。通信回路１３は、車載ネットワークに対応したトランシーバ（例えばＣＡＮトランシーバ）により構成され、ＥＣＵ１は通信回路１３を通じてネットワーク４を介して他のＥＣＵ（例えば２）との間でデータを送受信する。本実施形態では、ＣＰＵ１１が認証コード生成部、認証要求側エラー処理実行部、として用いられると共に、通信回路１３が送信部、第２受信部として用いられ、不揮発性メモリ１５が第１記憶部、第１保存部、第３記憶部、第３保存部に相当するメモリとして用いられる。

【００１０】

ＥＣＵ２もＥＣＵ１と同様の構成とされている。説明の便宜上、符号を変更して図示しているが、ＥＣＵ２は、ＣＰＵ２１、メモリ２２、及び通信回路２３などバス２４に接続して構成された第２電子制御装置に相当するものであり、車両内の各種センサ、アクチュエータ（何れも図示せず）などを制御するように構成される。メモリ２２もまた、不揮発性メモリ２５及び揮発性メモリ（図示せず）によるもので、ＣＰＵ２１は、メモリ２２に記憶された制御プログラムに基づいて動作する。メモリ２２もまた非遷移的実効的記録媒体として用いられる。通信回路２３は、車載ネットワークに対応したトランシーバ（例えばＣＡＮトランシーバ）により構成され、ＥＣＵ２は、通信回路２３を通じてネットワーク４を介して他のＥＣＵ（例えばＥＣＵ１）との間でデータを送受信する。本実施形態では、ＣＰＵ２１が認証部、認証受付側エラー処理実行部として用いられ、通信回路２３が第１受信部、認証結果送信部として用いられ、不揮発性メモリ２５が第２記憶部、第２保存部に相当するメモリとして用いられる。以下では、前述のＣＰＵ１１、２１が各メモリ

１２、２２に記憶されたプログラムに応じて実行する動作を、各ＥＣＵ１、２の動作と表記して説明を行う。

【００１１】

上記構成の作用、動作を説明する。本実施形態では、ネットワーク接続によるＥＣＵのなりすましを防止するため、複数のＥＣＵ１、２の間で認証処理を実施するところに特徴を備える。以下では、その詳細説明を行う。

【００１２】

図２及び図３は、それぞれ、ＥＣＵ１、ＥＣＵ２の各初期化処理をフローチャートにより示している。ＥＣＵ１が認証要求側のＥＣＵであり、ＥＣＵ２が認証受付側のＥＣＵであることを前提として説明する。ＥＣＵ１はまず、Ｓ１において次回の認証に利用する次回認証コードをランダムに生成し、Ｓ２にてこの次回認証コードをメッセージとしてネットワーク４に送信する。

【００１３】

ＥＣＵ２は、図２のＳ２で送信されたメッセージを図３のＴ１において受信し、Ｔ２において次回認証コードとして不揮発性メモリ２５に保存する。その後、ＥＣＵ２は、Ｔ３において処理終了通知をメッセージとしてネットワーク４に送信する。これによりＥＣＵ２の初期化処理を終了する。

【００１４】

ＥＣＵ１は、図３のＴ３で送信された処理終了通知に係るメッセージを図２のＳ３において受信する。するとＥＣＵ１は、このメッセージによりＥＣＵ２が次回認証コードを不揮発性メモリ２５に保存したことを確認できる。ＥＣＵ１は、ＥＣＵ２が次回認証コードを不揮発性メモリ１５に正常に保存したことを確認した後、Ｓ４において生成した次回認証コードを不揮発性メモリ２５に記憶、保存する。これによりＥＣＵ１の初期化処理を終了する。これにより、認証要求側のＥＣＵ１が生成した認証コードをＥＣＵ１及び２の間で共有できる。この各不揮発性メモリ１５、２５に保存された認証コードを保存済認証コードと称する。

【００１５】

図４及び図５はＥＣＵ１、ＥＣＵ２の各認証時処理をフローチャートにより示しており、図６はＥＣＵ１、ＥＣＵ２の間で行われる認証時処理の流れの一例をシーケンス図で示しており、図７はＥＣＵ１、ＥＣＵ２の間で行われる認証時処理の流れの一例をタイミングチャートで示している。

【００１６】

ＥＣＵ１はまず、図４のＳ１１においてＥＣＵ２に予め通知すると共に保存した保存済認証コードを不揮発性メモリ１５から読出す。図６のＳ１１も参照。そしてＥＣＵ１は、Ｓ１２において、次回の認証に利用する次回認証コードをランダムに生成する。その後、ＥＣＵ１は、Ｓ１３において、不揮発性メモリ１５から読み出した保存済認証コードを前回認証コードとし、この前回認証コードとランダムに生成した次回認証コードとを合わせたメッセージを生成してネットワーク４に送信する。

【００１７】

他方、ＥＣＵ２は、図７に示すように、ＥＣＵ１がＳ１３にてメッセージを送信する前にはメッセージを待機している。ＥＣＵ１が図４のＳ１３で送信したメッセージをＥＣＵ２は図５のＴ１１にて受信する。図６のＴ１１も参照。するとＥＣＵ２は、図５のＴ１２において、ＥＣＵ１から前回受信して不揮発性メモリ２５に保存した保存済認証コードを読出し、図５のＴ１３において、当該読出した保存済認証コードと受信した前回認証コードとを比較する。

【００１８】

ＥＣＵ２は、これらの保存済認証コードと前回認証コードとが一致していればＴ１３でＹＥＳと判断し、図５のＴ１４において正常な認証と判断し、図５のＴ１５において受信した次回認証コードを不揮発性メモリ２５に保存する。他方ＥＣＵ２は、図５のＴ１３において、これらの保存済認証コードと受信した前回認証コードとが一致しないと判断した

ときには、ＥＣＵ１が変更されたと判定し、図５のＴ１６において認証エラー処理を実行する。ＥＣＵ２は、このＴ１６の認証エラー処理において、例えばＥＣＵ２が、ＥＣＵ１以外のＥＣＵ３などに対し、ＥＣＵ１が不正な電子制御装置であることを通知したり、ＥＣＵ１から受信した情報をリセット、すなわち初期化したり、今後ＥＣＵ１から様々な要求を受けたとしても無視する旨のフラグを立てたりする。これによりＥＣＵ２側では、図６のＴ１３～Ｔ１６において認証コードの適否に応じた処理を実行できる。

【００１９】

これによりＥＣＵ１が、様々ななりすまし行為を過去に行っていた、又は将来に渡り行うとしても、このなりすまし行為による被害を過去に遡って検出できると共に将来に渡る被害を未然に防ぐことができる。そしてＥＣＵ２は、図５のＴ１７において、これらのＴ１４又はＴ１５における認証結果をＥＣＵ１に送信する。図６及び図７のＴ１７も参照。これにより、ＥＣＵ２は処理終了となる。

【００２０】

ＥＣＵ１は、図７に示すように、Ｓ１３においてメッセージを送信してから認証結果を受信するまで認証結果の受信を待機している。ＥＣＵ１は、図４のＳ１４においてＥＣＵ２から認証結果を受信すると、Ｓ１５において正常認証されたか否かを判定し、認証結果が正常な認証とされていればＳ１５でＹＥＳと判定することで、Ｓ１２にて生成した次回認証コードをＳ１６において不揮発性メモリ１５に保存し、正常な認証とされていなければＳ１５でＮＯと判定することでＳ１７においてエラー処理を実行する。

このエラー処理は、なりすましていないＥＣＵ１により実行される処理である。このためＥＣＵ１は、ネットワーク４におけるトラフィックエラーによる可能性があると判断し、Ｓ１１に処理を戻して再度認証処理を繰り返すようにしても良いし、所定（例えば複数）回以上繰り返し実行してもＳ１７のエラー処理に移行してしまう場合には、ネットワーク４に問題があると断定して終了しても良い。これによりＥＣＵ１は処理終了となる。ＥＣＵ１、２が共に正常な認証であると判断すれば、ＥＣＵ１、２が不揮発性メモリ１５、２５に共有される認証コードは次回認証コードに更新されることになる。

【００２１】

したがって、次回、ＥＣＵ１、２が認証処理を実施するときには、この不揮発性メモリ１５、２５に保存された次回認証コードを共有した認証コードとすると共に、さらに新たな次々回認証コードを生成して認証処理を繰り返し実行できるようになる。したがって、ＥＣＵ１、２は共有する認証コードを例えば認証処理する度に毎回更新できるようになり、たとえ古い識別コードが漏洩したとしても当該古い識別コードを用いて認証できなくなる。この結果、ＥＣＵが意図しないＥＣＵに変更されたことを検出できるようになり、なりすましを極力防止できるようになる。

【００２２】

＜実施例＞

説明を理解し易くするため８ビットの認証コードの例を挙げて説明する。例えば、ＥＣＵ１及び２は、初期化処理においてそれぞれ保存済認証コードとして「＆ＨＡＡ」を不揮発性メモリ１５、２５に保存して当該コードを共有しているときに、ＥＣＵ１が、次回認証コードとして「＆ＨＢＢ」を生成したと仮定する。

【００２３】

ＥＣＵ１は、保存済認証コード「＆ＨＡＡ」を前回認証コードとして送信すると共に、次回認証コード「＆ＨＢＢ」を送信すると、ＥＣＵ２はこれらの前回認証コード「＆ＨＡＡ」及び次回認証コード「＆ＨＢＢ」を受信する。

【００２４】

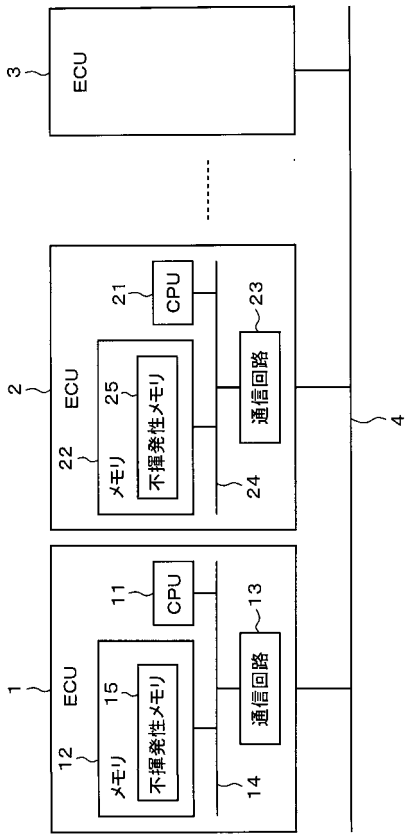
するとＥＣＵ２は、前回認証コード「＆ＨＡＡ」と、不揮発性メモリ２５に保存された保存済認証コード「＆ＨＡＡ」とを比較、照合し、これらが一致したときに、次回認証コード「＆ＨＢＢ」を不揮発性メモリ２５に保存する。ＥＣＵ２が、認証結果として正常な認証であることをＥＣＵ１に送信すると、ＥＣＵ１は、次回認証コード「＆ＨＢＢ」を不揮発性メモリ１５に保存する。これにより、次回認証コード「＆ＨＢＢ」はＥＣＵ１及び

２の間で共有されることになる。
【００２５】
ＥＣＵ１及び２は、次回の認証処理においてこの共有された次回認証コード「＆ＨＢＢ」を保存済認証コードとして用いる。この後、ＥＣＵ１が、さらなる次回認証コード「＆ＨＣＣ」を生成したと仮定する。ＥＣＵ１は、保存済認証コード「＆ＨＢＢ」を前回認証コードとして送信すると共に、次回認証コード「＆ＨＣＣ」を送信すると、ＥＣＵ２は、これらの前回認証コード「＆ＨＢＢ」及び次回認証コード「＆ＨＣＣ」を受信する。
【００２６】
するとＥＣＵ２は、前回認証コード「＆ＨＢＢ」と、不揮発性メモリ２５に保存された保存済認証コード「＆ＨＢＢ」とを比較、照合し、これらが一致したときに、次回認証コード「＆ＨＣＣ」を不揮発性メモリ２５に保存する。ＥＣＵ２が、認証結果として正常な認証であることをＥＣＵ１に送信すると、ＥＣＵ１は、次回認証コード「＆ＨＣＣ」を不揮発性メモリ１５に保存する。これにより、次回認証コード「＆ＨＣＣ」はＥＣＵ１及び２の間で共有される。このような処理を繰り返すことで、認証処理を実施する度に認証コードを更新できる。
【００２７】
この例では、説明の簡単化のため、８ビット＝１バイトを認証コードとして用いた例を示しているが、その情報量は限られるものではない。
【００２８】
＜本実施形態に係る概念的なまとめ＞
要するに、本実施形態によれば以下の構成を備えることで以下の効果を得られる。本実施形態によれば、ＥＣＵ１は認証コードを生成し、ＥＣＵ２との間で予め共有された認証コードを保存済認証コードとして不揮発性メモリ１５に記憶しており、ＥＣＵ１は、通信回路１３により、保存済認証コードと改めて生成された次回認証コードとをＥＣＵ２に送信する。ＥＣＵ１は、送信された保存済認証コード及び次回認証コードがＥＣＵ２において正常に認証されたことを条件として次回認証コードを不揮発性メモリ１５に保存するようにしている。
【００２９】
このときＥＣＵ１側では、ＥＣＵ２において正常に認証されたことを条件として次回認証コードを不揮発性メモリ１５に保存するようにしている。このため、ＥＣＵ１は、次回の認証に用いる次回認証コードを不揮発性メモリ２５に保存することで次の認証処理に用いることができる。次回認証コードを次の認証に用いることができるようになるため、これらの処理が繰り返されることで認証コードを次々に変更できるようになる。したがって、たとえ古い識別コードが漏洩したとしても当該古い識別コードを用いて認証処理できなくなる。この結果、ＥＣＵが意図しないＥＣＵに変更されたことを検出できるようになり、なりすましを極力防止できるようになる。
【００３０】
ＥＣＵ１は、認証処理を実施する度に、次回認証コードをランダムに生成しているため、認証処理を実施する度に認証コードを変更することができ、仮に認証コードが漏えいしてしまった場合であっても、ＥＣＵ１の変更は検知することが可能となり、なりすましを防止できる。
【００３１】
逆に、ＥＣＵ２は、通信回路２３を通じてＥＣＵ１から送信される前回認証コード及び次回認証コードを受信し、前回受信された認証コードを保存済認証コードとして不揮発性メモリ２５に記憶している。このとき、ＥＣＵ２は、不揮発性メモリ２５に記憶された保存済認証コードと、通信回路２３を通じて受信した前回認証コードとが一致するときに正常な認証と判断し、次回認証コードを不揮発性メモリ２５に保存するようにしているため、ＥＣＵ２は、ＥＣＵ１を認証することができ、当該ＥＣＵ１がなりすましではないことを確認できる。しかも、次回の認証に用いる次回認証コードを不揮発性メモリ２５に保存することで次の認証処理に用いることができるようになる。これにより、なりすましを極

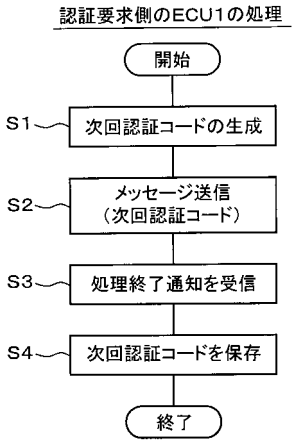
力防止できる。
【００３２】
ＥＣＵ２は、保存済認証コードと、通信回路２３を通じて受信した前回認証コードとの認証結果をＥＣＵ１に送信するようにしているため、ＥＣＵ１にその認証結果を伝えることができる。このため、ＥＣＵ１は、ＥＣＵ２に正常な認証がされたときにはこの確認をすることができ、ＥＣＵ１とＥＣＵ２との間で正常な認証確認を行うことができる。
【００３３】
（他の実施形態）
前述実施形態に限定されるものではなく、例えば、以下に示す変形又は拡張が可能である。
ＥＣＵ２は、メモリ２２に保存された保存済認証コードと受信した前回認証コードとが一致したことを条件として正常な認証と判断して次回認証コードを不揮発性メモリ２５に保存し、一致していないときには認証エラー処理を実行する形態を示したが、これに限定されるものではない。ＥＣＵ２は、例えば、保存済認証コードが送信された前回認証コードに含まれていれば正常な認証と判断して次回認証コードを保存するようにしても良い。
例えば、保存済認証コードが「＆ＨＡＡ」であったときに、ＥＣＵ１が前回認証コードとして「＆ＨＡＡＢ」をＥＣＵ２に送信し、ＥＣＵ２により「＆ＨＡＡ」が「＆ＨＡＡＢ」に含まれていることを条件として正常な認証と判断するようにしても良い。
【００３４】
前述実施形態では、ＥＣＵ１が認証要求しＥＣＵ２が認証受付する形態を示したが、これに限定されるものではなく、ＥＣＵ１が認証要求すると共に認証受付する機能を備えており、ＥＣＵ２が認証受付すると共に認証要求する機能を備えていても良い。
すなわち、ＥＣＵ１が、図２及び図４の処理を実行可能になっていると共に図３及び図５の処理を実行可能になっており、ＥＣＵ２が図３及び図５の処理を実行可能になっていると共に図２及び図４の処理を実行可能になっていても良い。
これらの処理内容は、前述実施形態と同様であるため図面の記載を省略しているが、例えば、ＥＣＵ２が、認証コードをランダムに次回認証コードとして生成する機能を備えており、この次回認証コードと共に、不揮発性メモリ２５に保存された保存済認証コードを前回認証コードとしてＥＣＵ１に送信する。そしてＥＣＵ１が、通信回路２３を通じて他のＥＣＵ２から前回認証コード及び次回認証コードを受信し、第３記憶部となる不揮発性メモリ１５に保存された保存済認証コードと、ＥＣＵ２から受信した前回認証コードとに応じて認証する。この認証は、ＣＰＵ１１が認証部としての機能を用いて実行される処理である。ＥＣＵ１は、保存済認証コードが前回認証コードに一致しているか、又は、含まれているかを判定することで、ＥＣＵ２の認証を行うことができる。
【００３５】
ここで、ＥＣＵ１は、保存済認証コードが前回認証コードに一致していたり、含まれていたりしたときには正常な認証と判断し、ＥＣＵ２がなりすましていない旨を確認することができ、さらにＥＣＵ２から受信した次回認証コードを不揮発性メモリ１５に保存する。これは第３保存部としての保存機能である。このように、前述実施形態で説明したＥＣＵ１及び２の各機能をＥＣＵ１及び２がそれぞれ備えて相互に認証できるようにしても良い。
【００３６】
前述実施形態では、認証処理を実施する度に、ランダムに認証コードを変更している形態を示したが、認証処理を実行する度に認証コードを変更しなくても良く、同じ認証コードを用いて相手方のＥＣＵの通常認証を行った上で、何回かに一度だけ認証コードを変更する形態にも適用できる。また、ランダムに認証コードを変更しなくても、規則的に認証コードを変更する形態にも適用できる。
不揮発性メモリ１５、２５に保存済認証コードを保存する形態を示したが、例えばバッテリ電源などが常時通電されていれば当該不揮発性メモリ１５、２５以外の例えばバックアップＲＡＭなどのメモリ１２に保存済認証コードを保存する形態に適用しても良い。

【００３７】
特許請求の範囲に記載した括弧内の符号は、本発明の一つの態様として前述する実施形態に記載の具体的手段との対応関係を示すものであって、本発明の技術的範囲を限定するものではない。前述実施形態の一部を、課題を解決できる限りにおいて省略した態様も実施形態と見做すことが可能である。また、特許請求の範囲に記載した文言によって特定される発明の本質を逸脱しない限度において、考え得るあらゆる態様も実施形態と見做すことが可能である。
【００３８】
また本発明は、前述した実施形態に準拠して記述したが、本発明は当該実施形態や構造に限定されるものではないと理解される。本発明は、様々な変形例や均等範囲内の変形をも包含する。加えて、様々な組み合わせや形態、さらには、それらに一要素、それ以上、あるいはそれ以下、を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。
【符号の説明】
【００３９】
図面中、１はＥＣＵ（第１電子制御装置）、２はＥＣＵ（第２電子制御装置）、１１は認証要求側のＥＣＵのＣＰＵ（認証コード生成部、認証要求側エラー処理実行部）、１２はメモリ（第１記憶部、第１保存部、第３記憶部、第３保存部）、１３は通信回路（送信部、第２受信部）、１５は不揮発性メモリ（第１記憶部、第１保存部、第３記憶部、第３保存部）、２１は認証受付側のＥＣＵのＣＰＵ（認証部、認証受付側エラー処理実行部）、２２はメモリ（第２記憶部、第２保存部）、２３は通信回路（第１受信部、認証結果送信部）、２５は不揮発性メモリ（第２記憶部、第２保存部）、を示す。

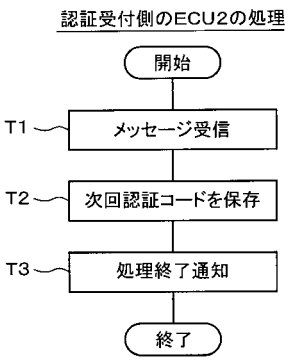
【図１】



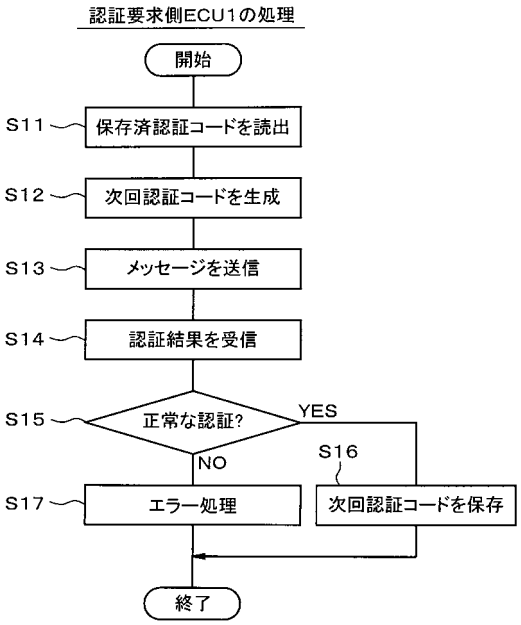
【図２】



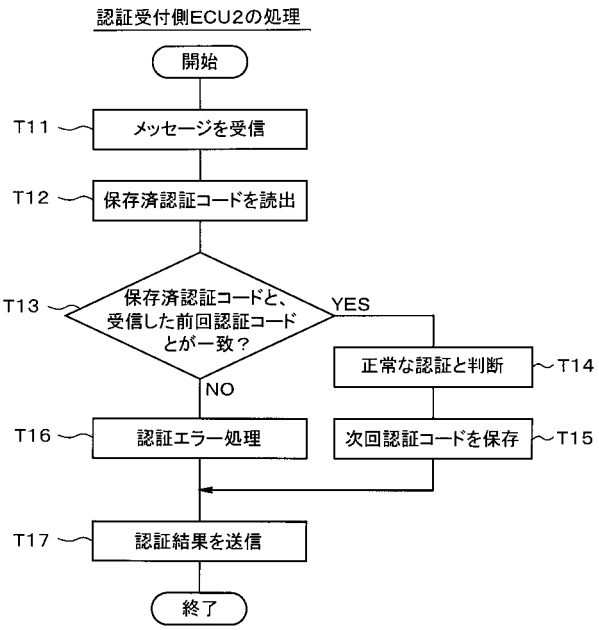
【図３】


認証受付側のECU2の処理
開始
T1
メッセージ受信
T2
次回認証コードを保存
T3
処理終了通知
終了

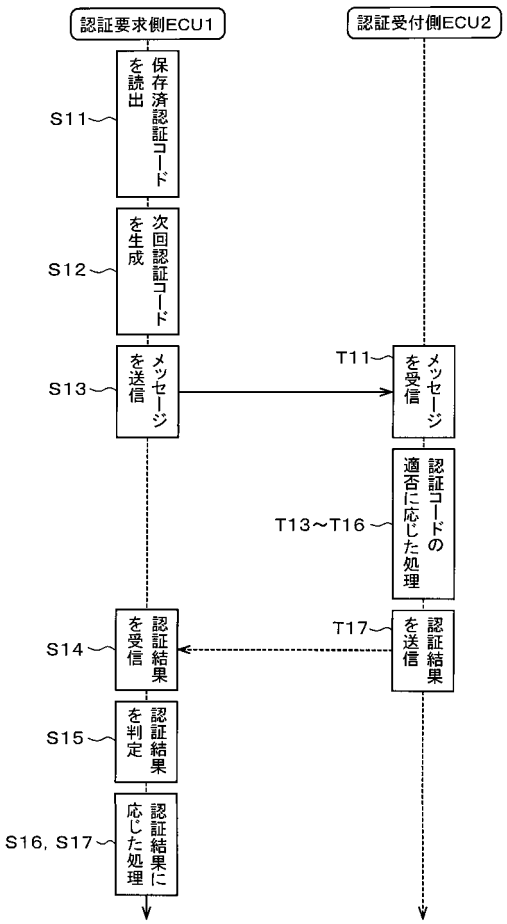
【図４】


認証要求側ECU1の処理
開始
S11
保存済認証コードを読出
S12
次回認証コードを生成
S13
メッセージを送信
S14
認証結果を受信
S15
正常な認証?
YES
NO
S16
S17
エラー処理
次回認証コードを保存
終了

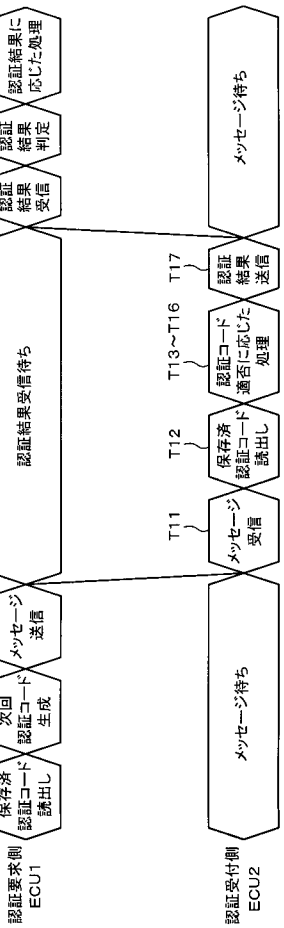
【図５】


認証受付側ECU2の処理
開始
T11
メッセージを受信
T12
保存済認証コードを読出
T13
保存済認証コードと、受信した前回認証コードとが一致?
YES
NO
正常な認証と判断
T14
T16
認証エラー処理
次回認証コードを保存
T15
T17
認証結果を送信
終了

【図６】


認証要求側ECU1
認証受付側ECU2
S11
保存済認証コードを読出
S12
次回認証コードを生成
S13
メッセージを送信
T11
メッセージを受信
T13〜T16
認証コードの適否に応じた処理
S14
認証結果を受信
T17
認証結果を送信
S15
認証結果を判定
S16, S17
認証結果に応じた処理

【図７】


認証要求側
ECU1
認証受付側
ECU2
S11
保存済認証コード読出し
S12
次回認証コード生成
S13
メッセージ送信
S14
認証結果受信
S15
認証結果判定
S16、S17
認証結果に応じた処理
認証結果受信待ち
T11
メッセージ受信
T12
保存済認証コード読出し
T13～T16
認証コード適否に応じた処理
T17
認証結果送信
メッセージ待ち
メッセージ待ち