

(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2018-166310

(P2018-166310A)

(43) 公開日 平成30年10月25日(2018.10.25)

(51) Int.Cl.	F I	テーマコード (参考)
H O 4 L 9/14 (2006.01)	H O 4 L 9/00 6 4 1	5 J 1 0 4
B 6 O R 16/023 (2006.01)	B 6 O R 16/023 P	5 K 0 3 2
H O 4 L 12/40 (2006.01)	H O 4 L 12/40 Z	5 K 0 3 3
H O 4 L 12/28 (2006.01)	H O 4 L 12/28 2 0 0 M	
H O 4 L 9/32 (2006.01)	H O 4 L 9/00 6 7 5 A	
審査請求 未請求 請求項の数 5 O L (全 14 頁) 最終頁に続く		

(21) 出願番号 特願2017-63802 (P2017-63802)
 (22) 出願日 平成29年3月28日 (2017. 3. 28)

(71) 出願人 314012076
 パナソニック I P マネジメント株式会社
 大阪府大阪市中央区域見 2 丁目 1 番 6 1 号
 (74) 代理人 100123102
 弁理士 宗田 悟志
 (72) 発明者 小泉 朋洋
 大阪府門真市大字門真 1 〇 〇 6 番地 パナ
 ソニック株式会社内
 (72) 発明者 岩見 良太郎
 大阪府門真市大字門真 1 〇 〇 6 番地 パナ
 ソニック株式会社内
 (72) 発明者 千賀 久司
 大阪府門真市大字門真 1 〇 〇 6 番地 パナ
 ソニック株式会社内

最終頁に続く

(54) 【発明の名称】 送信装置、車載通信システム、通信方法およびコンピュータプログラム

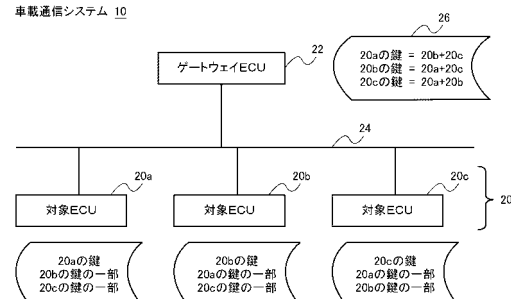
(57) 【要約】

【課題】 車載装置のセキュリティを向上させる。

【解決手段】 複数の対象 ECU 20 のそれぞれは、ゲートウェイ ECU 22 から送信されたデータの正当性を認証するための自装置の鍵である第 1 鍵を記憶し、他の対象 ECU 20 の第 1 鍵の一部に対応する第 2 鍵をさらに記憶する。ゲートウェイ ECU 22 は、特定の対象 ECU 20 の第 1 鍵を生成するための、他の対象 ECU 20 に記憶された複数の第 2 鍵の組み合わせ態様を定めた組み合わせテーブル 26 を記憶する。ゲートウェイ ECU 22 は、特定の対象 ECU 20 へデータを送信すべき場合、他の複数の対象 ECU 20 から複数の第 2 鍵を取得し、複数の第 2 鍵を、組み合わせテーブル 26 が定める態様で組み合わせることにより、特定の対象 ECU 20 の第 1 鍵を生成する。ゲートウェイ ECU 22 は、生成した第 1 鍵を使用して、特定の対象 ECU 20 へデータを送信する。

【選択図】 図 1

車載通信システム 10



【特許請求の範囲】

【請求項 1】

車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置であって、
前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を
認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵
の一部に対応する第 2 鍵を記憶し、

前記送信装置は、

特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記
憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部と、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複
数の第 2 鍵を取得する鍵取得部と、

前記鍵取得部により取得された複数の第 2 鍵を、前記記憶部に記憶された態様で組み合
わせることにより、前記特定の電子制御装置の第 1 鍵を生成する鍵生成部と、

前記鍵生成部により生成された第 1 鍵を使用して、前記特定の電子制御装置へデータを送
信する送信部と、

を備える送信装置。

【請求項 2】

前記記憶部は、前記複数の電子制御装置の異なる第 1 鍵を生成するための、前記複数の
第 2 鍵の異なる組み合わせ態様を記憶し、

前記鍵生成部は、前記異なる組み合わせ態様のうちデータ送信先の電子制御装置に応じ
た態様で前記複数の第 2 鍵を組み合わせることにより、前記データ送信先の電子制御装置
の第 1 鍵を生成する、

請求項 1 に記載の送信装置。

【請求項 3】

複数の電子制御装置と、

車載ネットワークを介して前記複数の電子制御装置へデータを送信する送信装置と、
を備え、

前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を
認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵
の一部に対応する第 2 鍵を記憶し、

前記送信装置は、

特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記
憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部と、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複
数の第 2 鍵を取得する鍵取得部と、

前記鍵取得部により取得された複数の第 2 鍵を、前記記憶部に記憶された態様で組み合
わせることにより、前記特定の電子制御装置の第 1 鍵を生成する鍵生成部と、

前記鍵生成部により生成された第 1 鍵を使用して、前記特定の電子制御装置へデータを送
信する送信部と、を含む車載通信システム。

【請求項 4】

車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置が実行する
通信方法であって、

前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を
認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵
の一部に対応する第 2 鍵を記憶し、

前記送信装置は、特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の
電子制御装置に記憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部を備えており

、

前記送信装置が、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複

10

20

30

40

50

数の第 2 鍵を取得し、

取得した複数の第 2 鍵を、前記記憶部に記憶された態様で組み合わせることにより、前記特定の電子制御装置の第 1 鍵を生成し、

生成した第 1 鍵を使用して、前記特定の電子制御装置へデータを送信する、通信方法。

【請求項 5】

車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置が実行するコンピュータプログラムであって、

前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵の一部に対応する第 2 鍵を記憶し、

前記送信装置は、特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部を備えており、

前記送信装置に、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複数の第 2 鍵を取得し、

取得した複数の第 2 鍵を、前記記憶部に記憶された態様で組み合わせることにより、前記特定の電子制御装置の第 1 鍵を生成し、

生成した第 1 鍵を使用して、前記特定の電子制御装置へデータを送信する、

ことを実行させるためのコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明はデータ通信技術に関し、特に送信装置、車載通信システム、通信方法およびコンピュータプログラムに関する。

【背景技術】

【0002】

従来技術として、車載通信システムにおいて中継器となるゲートウェイが、各 ECU (Electronic Control Unit) の照合コードを記憶すること、ECU が、プログラムの書換要求の送信元がゲートウェイか否かを照合コードを用いて判定し、送信元がゲートウェイの場合にプログラムの書換を許可することが知られている。

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2013-112120 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

従来の車載通信システムでは、ゲートウェイが攻撃され、ゲートウェイが記憶する各 ECU の照合コードが盗竊された場合、各 ECU が記憶するプログラムの不正書換が容易になされてしまう場合があった。

【0005】

本発明は上記課題に鑑みたもので、1 つの目的は、車載装置のセキュリティを向上させることである。

【課題を解決するための手段】

【0006】

上記課題を解決するために、本発明のある態様の送信装置は、車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置であって、複数の電子制御装置のそれぞれは、送信装置から送信されたデータの正当性を認証するための自装置の鍵である第 1

10

20

30

40

50

鍵を記憶するとともに、他の電子制御装置の第1鍵の一部に対応する第2鍵を記憶し、送信装置は、特定の電子制御装置の第1鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第2鍵の組み合わせ態様を記憶する記憶部と、特定の電子制御装置へデータを送信する場合、他の複数の電子制御装置から複数の第2鍵を取得する鍵取得部と、鍵取得部により取得された複数の第2鍵を、記憶部に記憶された態様で組み合わせることにより、特定の電子制御装置の第1鍵を生成する鍵生成部と、鍵生成部により生成された第1鍵を使用して、特定の電子制御装置へデータを送信する送信部と、を備える。

【0007】

本発明の別の態様は、車載通信システムである。この車載通信システムは、複数の電子制御装置と、車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置と、を備える。複数の電子制御装置のそれぞれは、送信装置から送信されたデータの正当性を認証するための自装置の鍵である第1鍵を記憶するとともに、他の電子制御装置の第1鍵の一部に対応する第2鍵を記憶し、送信装置は、特定の電子制御装置の第1鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第2鍵の組み合わせ態様を記憶する記憶部と、特定の電子制御装置へデータを送信する場合、他の複数の電子制御装置から複数の第2鍵を取得する鍵取得部と、鍵取得部により取得された複数の第2鍵を、記憶部に記憶された態様で組み合わせることにより、特定の電子制御装置の第1鍵を生成する鍵生成部と、鍵生成部により生成された第1鍵を使用して、特定の電子制御装置へデータを送信する送信部と、を含む。

【0008】

本発明のさらに別の態様は、通信方法である。この方法は、車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置が実行する通信方法であって、複数の電子制御装置のそれぞれは、送信装置から送信されたデータの正当性を認証するための自装置の鍵である第1鍵を記憶するとともに、他の電子制御装置の第1鍵の一部に対応する第2鍵を記憶し、送信装置は、特定の電子制御装置の第1鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第2鍵の組み合わせ態様を記憶する記憶部を備えており、送信装置が、特定の電子制御装置へデータを送信する場合、他の複数の電子制御装置から複数の第2鍵を取得し、取得した複数の第2鍵を、記憶部に記憶された態様で組み合わせることにより、特定の電子制御装置の第1鍵を生成し、生成した第1鍵を使用して、特定の電子制御装置へデータを送信する。

【0009】

なお、以上の構成要素の任意の組合せ、本発明の表現を、コンピュータプログラム、コンピュータプログラムを記録した記録媒体、本装置を搭載した車両などの間で変換したものもまた、本発明の態様として有効である。

【発明の効果】

【0010】

本発明によれば、車載装置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】

【0011】

【図1】実施例の車載通信システムの概要を説明する図である。

【図2】実施例の車載通信システムの構成を示す図である。

【図3】図2の対象ECUの動作を示すフローチャートである。

【図4】図2のゲートウェイECUの動作を示すフローチャートである。

【発明を実施するための形態】

【0012】

図1は、実施例の車載通信システム10の概要を説明する図である。実施例の車載通信システム10では、プログラム更新（言い換えればリプログラミング）の対象となるECUである対象ECU20a、対象ECU20b、対象ECU20cが、車載ネットワーク24を介して、ゲートウェイECU22に接続される。

【0013】

対象 ECU 20 a、対象 ECU 20 b、対象 ECU 20 c は、各種アクチュエータ（ステアリング、ブレーキ等）を制御する ECU であってもよく、各種センサ（温度センサ、加速度センサ等）に接続された ECU であってもよい。以下、対象 ECU 20 a、対象 ECU 20 b、対象 ECU 20 c を総称する場合、対象 ECU 20 と呼ぶ。車載ネットワーク 24 は、例えば、CAN（Controller Area Network）であってもよい。

【0014】

複数の対象 ECU 20 のそれぞれは、予め定められた自装置の鍵（以下「第 1 鍵」とも呼ぶ。）を使用したチャレンジレスポンス認証により、データ送信元装置の正当性を判定する。複数の対象 ECU 20 のそれぞれは、第 1 鍵を記憶するとともに、他の対象 ECU の第 1 鍵の一部に対応するデータ（以下「第 2 鍵」とも呼ぶ。）を記憶する。例えば、第 2 鍵は、第 1 鍵のデータ全体のうちの一部を構成するデータであってもよい。このように、車載通信システム 10 では、ある対象 ECU 20 の第 1 鍵を、他の複数の対象 ECU 20 で分散管理する。

【0015】

ゲートウェイ ECU 22 は、各対象 ECU の第 1 鍵を生成するための、第 2 鍵の組み合わせ態様を定めた組み合わせテーブル 26 を記憶する。ゲートウェイ ECU 22 は、対象 ECU 20 a ヘデータを送信すべき場合、対象 ECU 20 b が記憶する第 2 鍵と、対象 ECU 20 c が記憶する第 2 鍵を取得して組み合わせることにより、対象 ECU 20 a の第 1 鍵を生成する。ゲートウェイ ECU 22 は、生成した第 1 鍵を使用して、対象 ECU 20 a ヘデータを送信することによりチャレンジレスポンス認証をクリアする。この構成によると、車載通信システム 10 のセキュリティを向上でき、例えば、対象 ECU 20 の鍵の安全性を高めることができる。

【0016】

図 2 は、実施例の車載通信システム 10 の構成を示す。車載通信システム 10 は、車両 12 の内部に構築され、また、車両 12 の外部に存在する外部機器 14 と接続される。外部機器 14 は、複数の対象 ECU 20 に記憶されたプログラムの書換・更新を指示するデータ（以下「書換指示」とも呼ぶ。）を車両 12 へ入力する。

【0017】

車両 12 は、対象 ECU 20 a、対象 ECU 20 b、対象 ECU 20 c、ゲートウェイ ECU 22、コネクタ 28 を備える。既述したように、複数の対象 ECU 20 とゲートウェイ ECU 22 は、車載ネットワーク 24 に接続される。コネクタ 28 は、外部機器 14 とのインタフェースを提供する。

【0018】

図 2 は、対象 ECU 20 a の機能構成を示すブロック図を含む。本明細書のブロック図において示される各ブロックは、ハードウェア的には、コンピュータの CPU・メモリをはじめとする素子や機械装置で実現でき、ソフトウェア的にはコンピュータプログラム等によって実現されるが、ここでは、それらの連携によって実現される機能ブロックを描いている。これらの機能ブロックはハードウェア、ソフトウェアの組合せによっていろいろなかたちで実現できることは、当業者には理解されるところである。

【0019】

対象 ECU 20 a は、通信部 30、記憶部 32、制御部 34 を備える。対象 ECU 20 b、対象 ECU 20 c の構成も対象 ECU 20 a と同様である。

【0020】

通信部 30 は、所定の通信プロトコルにしたがって、車載ネットワーク 24 ヘデータを送信し、また、車載ネットワーク 24 を流れるデータを受信する。制御部 34 は、各種データ処理を制御する。制御部 34 に含まれる機能ブロックは、対象 ECU 20 a の CPU がプログラムを実行することにより実現されてよい。記憶部 32 は、制御部 34 により参照または更新されるデータを記憶する。記憶部 32 は、例えばフラッシュメモリにより実現されてよい。

【0021】

記憶部 32 は、プログラム記憶部 36、第 1 鍵記憶部 38、第 2 鍵記憶部 40、配送鍵記憶部 41 を含む。プログラム記憶部 36 は、対象 ECU 20a が担当する車両 12 の走行に関するデータ処理を実行するためのプログラム（以下「データ処理プログラム」とも呼ぶ。）を記憶する。データ処理プログラムは、例えば、センサによる検知内容の通知処理、または、アクチュエータの制御処理を規定してもよい。第 1 鍵記憶部 38 は、外部装置（実施例ではゲートウェイ ECU 22）から送信されたデータの正当性を共通鍵方式で認証するための第 1 鍵を記憶する。

【0022】

第 2 鍵記憶部 40 は、他の対象 ECU 20（例えば対象 ECU 20b、対象 ECU 20c）の第 1 鍵の一部に対応する第 2 鍵を記憶する。実施例では、第 2 鍵記憶部 40 は、他の複数の対象 ECU 20 それぞれの第 2 鍵であり、対象 ECU 20 ごとに異なる第 2 鍵を記憶する。例えば、対象 ECU 20a の第 2 鍵記憶部 40 は、対象 ECU 20b 用の第 2 鍵と、対象 ECU 20c 用の第 2 鍵の両方を記憶する。

【0023】

配送鍵記憶部 41 は、対象 ECU 20a とゲートウェイ ECU 22 の間での第 2 鍵交換時に第 2 鍵を暗号化するための共通鍵（以下「配送鍵」と呼ぶ。）を記憶する。配送鍵は、対象 ECU 20 ごとに異なるデータが設定される。

【0024】

制御部 34 は、データ処理部 42、照合部 44、書換実行部 46、第 2 鍵提供部 48 を含む。データ処理部 42 は、プログラム記憶部 36 に記憶されたデータ処理プログラムを実行することにより、対象 ECU 20a が担当するデータ処理を実行する。照合部 44 は、第 1 鍵記憶部 38 に記憶された第 1 鍵を使用して、書換要求の送信元を認証し、言い換えれば、ゲートウェイ ECU 22 から送信された書換要求の正当性を認証する。

【0025】

書換実行部 46 は、照合部 44 により書換要求の正当性が確認された場合に、ゲートウェイ ECU 22 から送信された書換プログラムをプログラム記憶部 36 に保存することにより、既存のデータ処理プログラムを書換プログラムに置き換える。

【0026】

第 2 鍵提供部 48 は、ゲートウェイ ECU 22 から送信された鍵提供要求に応じて、第 2 鍵記憶部 40 に記憶された第 2 鍵をゲートウェイ ECU 22 へ送信する。実施例の鍵提供要求のフレームには、要求する第 2 鍵の種類（対象 ECU 20a～対象 ECU 20c のいずれか）ごとに異なるフレーム ID が設定される。第 2 鍵提供部 48 は、フレーム ID に対応する第 2 鍵を、配送鍵記憶部 41 に記憶された配送鍵で暗号化し、暗号化したデータを含む応答フレームをゲートウェイ ECU 22 へ送信する。応答フレームには、送信元の対象 ECU 20（対象 ECU 20a～対象 ECU 20c のいずれか）を示すフレーム ID が設定される。

【0027】

図 2 は、ゲートウェイ ECU 22 の機能構成を示すブロック図を含む。ゲートウェイ ECU 22 は、通信部 50、記憶部 52、制御部 54 を備える。これらの機能ブロックは、対象 ECU 20a の通信部 30、記憶部 32、制御部 34 に対応する。

【0028】

記憶部 52 は、プログラム記憶部 56、鍵生成規則記憶部 58、配送鍵記憶部 59 を含む。プログラム記憶部 56 は、外部機器 14 から受信した書換指示に含まれる書換プログラムを一時的に記憶する。配送鍵記憶部 59 は、複数の対象 ECU 20 との通信で使用する複数の配送鍵を記憶し、すなわち、各対象 ECU 20 用の配送鍵を記憶する。

【0029】

鍵生成規則記憶部 58 は、複数の対象 ECU 20 それぞれの第 1 鍵を生成するための規則であり、複数の対象 ECU 20 に記憶された複数の第 2 鍵の組み合わせ態様を記憶する。実施例では、鍵生成規則記憶部 58 は、図 1 の組み合わせテーブル 26 を記憶する。

【0030】

10

20

30

40

50

組み合わせテーブル 26 には、複数の対象 ECU 20 それぞれの第 1 鍵であり、対象 ECU 20 ごとに異なる第 1 鍵を生成するための、複数の第 2 鍵の異なる組み合わせ態様が定められる。例えば、図 1 の組み合わせテーブル 26 では、対象 ECU 20 a の第 1 鍵を、対象 ECU 20 b から提供された第 2 鍵と、対象 ECU 20 c から提供された第 2 鍵とを組み合わせ生成することが定められている。また、対象 ECU 20 b の第 1 鍵を、対象 ECU 20 a から提供された第 2 鍵と、対象 ECU 20 c から提供された第 2 鍵とを組み合わせ生成することが定められている。

【0031】

制御部 54 は、書換指示受信部 60、書換要求部 62、第 2 鍵取得部 64、第 1 鍵生成部 66 を含む。書換指示受信部 60 は、外部機器 14 からコネクタ 28 を介して入力された書換指示を受信する。書換指示は、プログラム書換対象となる対象 ECU 20（以下、「特定 ECU」と呼ぶ。）の ID を含む。さらに書換要求は、特定 ECU に記憶された既存のプログラムに置き換えるべき新たなプログラムのデータ（以下「書換プログラム」とも呼ぶ。）を含む。

【0032】

変形例として、クラウド上のサーバ（不図示）が、インターネット等、車両 12 外部のネットワークを介して、書換指示を車両 12 へ送信してもよい。この場合、通信部 50 は、車両 12 外部のネットワークと通信し、書換指示受信部 60 は、通信部 50 を介して、サーバから送信された書換指示を受信してもよい。

【0033】

書換要求部 62 は、書換指示受信部 60 により書換指示が受信された場合、データ処理プログラムの書換要求を対象 ECU 20 へ送信する。書換要求部 62 は、対象 ECU 20 へ送信する書換要求のフレームに対して、特定 ECU の種類（例えば対象 ECU 20 a、対象 ECU 20 b、または対象 ECU 20 c）ごとに異なるフレーム ID を設定する。なお、当該フレームのペイロードに、特定 ECU の ID を指定してもよい。

【0034】

第 2 鍵取得部 64 は、複数の対象 ECU 20 から複数の第 2 鍵を取得する。具体的には、第 2 鍵取得部 64 は、鍵提供要求を複数の対象 ECU 20（少なくとも特定 ECU 以外の対象 ECU 20）へ送信し、鍵提供要求に対する応答フレーム（第 2 鍵を含む）を複数の対象 ECU 20 から取得する。第 2 鍵取得部 64 は、応答フレームのフレーム ID に基づいて、複数の第 2 鍵それぞれの提供元（例えば対象 ECU 20 a、対象 ECU 20 b、または対象 ECU 20 c）を識別する。

【0035】

第 1 鍵生成部 66 は、第 2 鍵取得部 64 により取得された複数の第 2 鍵を、鍵生成規則記憶部 58 の組み合わせテーブル 26 が示す態様で組み合わせることにより、特定 ECU の第 1 鍵を生成する。組み合わせテーブル 26 は、複数の第 2 鍵の連結順序を定めてもよい。第 1 鍵生成部 66 は、組み合わせテーブル 26 が示す順序で複数の第 2 鍵のデータを連結することにより、特定 ECU の第 1 鍵を生成してもよい。例えば、第 1 鍵生成部 66 は、図 1 の組み合わせテーブル 26 を参照して、対象 ECU 20 b から提供された第 2 鍵の後に対象 ECU 20 c から提供された第 2 鍵を連結することにより、特定 ECU である対象 ECU 20 a の第 1 鍵を生成してもよい。

【0036】

また、第 1 鍵生成部 66 は、組み合わせテーブル 26 に規定された第 2 鍵の複数の組み合わせ態様のうち、データ送信先（言い換えればプログラム書換先）となる特定 ECU に応じた態様で複数の第 2 鍵を組み合わせる。これにより、第 1 鍵生成部 66 は、特定 ECU ごとに異なる第 1 鍵を生成する。

【0037】

書換要求部 62 は、第 1 鍵生成部 66 により生成された特定 ECU の第 1 鍵を使用して特定 ECU へデータを送信する。実施例では、書換要求部 62 は、特定 ECU から受信したチャレンジ（乱数）に対するレスポンスを、特定 ECU の第 1 鍵に基づいて生成し、当

10

20

30

40

50

該レスポンスを特定 ECU へ送信する。また、書換要求部 62 は、特定 ECU から書換開始要求を受信した場合、特定 ECU へ書換プログラムを送信する。

【0038】

以上の構成による車載通信システム 10 の動作を説明する。

図 3 は、図 2 の対象 ECU 20 の動作を示すフローチャートである。対象 ECU 20 a、対象 ECU 20 b、対象 ECU 20 c のいずれも同様の動作になる。図 3 には不図示だが、対象 ECU 20 が起動中（例えば電源オンの間）、データ処理部 42 は、プログラム記憶部 36 に記憶されたデータ処理プログラムを実行することにより、対象 ECU 20 が担当するデータ処理を実行する。

【0039】

通信部 30 が、ゲートウェイ ECU 22 から送信された鍵提供要求を受信すると（S10 の Y）、第 2 鍵提供部 48 は、鍵提供要求の ID が示す対象 ECU 20 の第 2 鍵（すなわち特定 ECU の第 1 鍵の一部）を取得する。第 2 鍵提供部 48 は、取得した第 2 鍵を、配送鍵記憶部 41 に記憶された配送鍵により暗号化する。第 2 鍵提供部 48 は、第 2 鍵の暗号化データと、自装置を示す ID とを含む応答フレームをゲートウェイ ECU 22 へ送信する（S12）。鍵提供要求を未受信であれば（S10 の N）、S12 をスキップする。

【0040】

通信部 30 が、ゲートウェイ ECU 22 から送信された書換要求を受信すると（S14 の Y）、照合部 44 は、所定の乱数生成器から乱数を取得し、取得した乱数をゲートウェイ ECU 22 へ送信する（S16）。照合部 44 は、取得した乱数に対して、第 1 鍵記憶部 38 に記憶された第 1 鍵を使用して演算し、演算結果を照合コードとして取得する（S18）。また、照合部 44 は、通信部 30 を介して、ゲートウェイ ECU 22 から送信された照合コードを取得する（S20）。S18 で取得した照合コードと、S20 で取得した照合コードが一致する場合（S22 の Y）、照合部 44 は、自 ECU を書換許可状態へ移行させる（S24）。

【0041】

書換許可状態へ移行されると、書換実行部 46 は、書換プログラムの提供を要求する書換開始要求をゲートウェイ ECU 22 へ送信し（S26）、ゲートウェイ ECU 22 から送信された書換プログラムを取得する（S28）。書換実行部 46 は、取得した書換プログラムをプログラム記憶部 36 へ格納し、既存のデータ処理プログラムを更新する（S30）。書換実行部 46 は、データ処理プログラムの書換完了通知をゲートウェイ ECU 22 へ送信する（S32）。

【0042】

S18 で取得した照合コードと、S20 で取得した照合コードとが不一致であれば（S22 の N）、照合部 44 は、自 ECU を書換禁止状態へ移行させ、または、自 ECU の書換禁止状態を維持する（S34）。図 3 には不図示だが、S34 の後、照合部 44 は、所定の異常時処理を実行してもよい。例えば、照合部 44 は、書換禁止状態あること、または、照合コードの検証に失敗したことを示すデータをゲートウェイ ECU 22 へ送信してもよい。また、照合部 44 は、照合コードの検証に失敗したことを所定のログファイルへ記録してもよい。書換要求を未受信であれば（S14 の N）、S16 以降の処理をスキップし、本図のフローを終了する。

【0043】

図 4 は、図 2 のゲートウェイ ECU 22 の動作を示すフローチャートである。図 3 には不図示だが、ゲートウェイ ECU 22 は、起動中（例えば電源オンの間）、車載ネットワーク 24 を流れるフレームの中継処理およびルーティング処理を実行する。

【0044】

書換指示受信部 60 は、外部機器 14 から入力された書換指示を受信すると（S40 の Y）、書換指示が含む書換プログラムをプログラム記憶部 56 へ格納する。書換要求部 62 は、書換指示が示す特定 ECU へデータ処理プログラムの書換要求を送信する（S42

10

20

30

40

50

）。第2鍵取得部64は、特定ECUに対応するフレームIDを設定したフレームであり、特定ECUの第2鍵の提供を要求するフレームを複数の対象ECU20（実施例では特定ECUを含む）へ送信する（S44）。例えば、第2鍵取得部64は、車載ネットワーク24のバスへ上記フレームをブロードキャストしてもよい。

【0045】

第2鍵取得部64は、複数の対象ECU20から送信された複数の第2鍵（暗号化データ）を取得して、配送鍵記憶部59に記憶された配送鍵によりそれらの暗号化データを復号し、複数の第2鍵（平文）を取得する（S46）。第1鍵生成部66は、鍵生成規則記憶部58の組み合わせテーブル26を参照し、特定ECUの第1鍵の生成規則にしたがって複数の第2鍵を組み合わせることにより、特定ECUの第1鍵を生成する（S48）。書換要求部62は、特定ECUから送信された乱数を取得する（S50）。書換要求部62は、S50で取得した乱数と、S48で生成した第1鍵とに基づいて所定の演算を実行し、演算結果を照合コードとして取得する（S52）。書換要求部62は、照合コードを特定ECUへ送信する（S54）。

【0046】

既述したように、照合コードが正しければ、特定ECUからゲートウェイECU22へ書換開始要求が送信される。通信部50が、特定ECUから送信された書換開始要求を受信すると（S56のY）、書換要求部62は、書換プログラムを特定ECUへ送信する（S58）。書換要求部62は、特定ECUから書換完了通知を受信すると、所定の後処理を実行し、例えば、リプログラミングの完了を外部機器14へ通知する（S60）。書換開始要求を未受信であれば（S56のN）、S58以降をスキップして本図のフローを終了する。外部機器14から書換指示を未受信であれば（S40のN）、S42以降をスキップして本図のフローを終了する。

【0047】

実施例の車載通信システム10によると、リプログラミングの対象となる対象ECU20が、ゲートウェイECU22から送信されたデータの正当性を第1鍵を用いて認証することを実現しつつ、鍵の秘密性を向上することができる。ゲートウェイECU22は、第2鍵の組み合わせ態様のデータを記憶するだけであるため、仮にゲートウェイECU22が攻撃されても、各電子制御装置の第1鍵が漏洩することを防止できる。また仮に、ある対象ECU20が攻撃されても、盗まれるのは当該ECUの第1鍵と他の対象ECU20の第1鍵の一部となり、鍵の漏洩を最小限に抑えることができる。

【0048】

以上、本発明を実施例をもとに説明した。この実施例は例示であり、それらの各構成要素あるいは各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0049】

変形例を説明する。上記実施例では、対象ECU20のそれぞれは、他の複数の対象ECU20それぞれの第2鍵を記憶した。例えば、対象ECU20aは、対象ECU20bの第2鍵と、その第2鍵とは異なる対象ECU20cの第2鍵を記憶した。変形例として、対象ECU20のそれぞれは、他の対象ECU20に依存しない共通の第2鍵（典型的には単一の第2鍵）を記憶してもよい。例えば、対象ECU20aは、対象ECU20bと対象ECU20cに共通の第2鍵を記憶してもよい。

【0050】

本変形例のゲートウェイECU22の組み合わせテーブル26には、複数の対象ECU20から取得された複数の第2鍵の組み合わせ態様として、特定ECUごとに異なる組み合わせ態様が定められる。この態様によると、対象ECU20が記憶する第2鍵は単一であっても、複数の第2鍵の組み合わせ態様を異ならせることで、対象ECU20ごとに異なる第1鍵を生成することができる。本変形例も上記実施例と同様の効果を奏する。

【0051】

別の変形例を説明する。上記実施例では、対象ECU20のリプログラミング時に、ゲ

ートウェイ ECU 22 が、複数の第 2 鍵を組み合わせて第 1 鍵を生成することを例示した。ただし、実施例に記載の技術はこれに制限されない。実施例に記載の技術は、複数の ECU と、複数の ECU のいずれかに対して何らかのデータを送信する送信装置（実施例のゲートウェイ ECU 22 に対応）を含むシステムであり、ECU が第 1 鍵を使用して送信元の正当性を検証するシステムに広く適用可能である。

【0052】

実施例および変形例に記載の技術は、以下の項目によって特定されてもよい。

[項目 1]

車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置であって、前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵の一部に対応する第 2 鍵を記憶し、

10

前記送信装置は、

特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部と、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複数の第 2 鍵を取得する鍵取得部と、

前記鍵取得部により取得された複数の第 2 鍵を、前記記憶部に記憶された態様で組み合わせることにより、前記特定の電子制御装置の第 1 鍵を生成する鍵生成部と、

前記鍵生成部により生成された第 1 鍵を使用して、前記特定の電子制御装置へデータを送信する送信部と、を備える送信装置。

20

この構成によると、電子制御装置が、送信装置から送信されたデータの正当性を第 1 鍵を用いて認証することを実現しつつ、鍵の秘密性を向上することができる。送信装置は第 2 鍵の組み合わせ態様のデータを記憶するだけであるため、仮に送信装置が攻撃されても、各電子制御装置の鍵が漏洩することを防止できる。また仮に、ある電子制御装置が攻撃されても、盗まれうるのは当該電子制御装置の鍵と他の電子制御装置の鍵の一部であり、鍵の漏洩を最小限に抑えることができる。

[項目 2]

前記記憶部は、前記複数の電子制御装置の異なる第 1 鍵を生成するための、前記複数の第 2 鍵の異なる組み合わせ態様を記憶し、

30

前記鍵生成部は、前記異なる組み合わせ態様のうちデータ送信先の電子制御装置に応じた態様で前記複数の第 2 鍵を組み合わせることにより、前記データ送信先の電子制御装置の第 1 鍵を生成する、項目 1 に記載の送信装置。

この態様によると、複数の電子制御装置それぞれに異なる第 1 鍵を設定でき、セキュリティを一層向上させることができる。

[項目 3]

複数の電子制御装置と、

車載ネットワークを介して前記複数の電子制御装置へデータを送信する送信装置と、を備え、

前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵の一部に対応する第 2 鍵を記憶し、

40

前記送信装置は、

特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部と、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複数の第 2 鍵を取得する鍵取得部と、

前記鍵取得部により取得された複数の第 2 鍵を、前記記憶部に記憶された態様で組み合わせることにより、前記特定の電子制御装置の第 1 鍵を生成する鍵生成部と、

前記鍵生成部により生成された第 1 鍵を使用して、前記特定の電子制御装置へデータを

50

送信する送信部と、を含む車載通信システム。

この車載通信システムによると、項目 1 と同様に、電子制御装置が、送信装置から送信されたデータの正当性を第 1 鍵を用いて認証することを実現しつつ、鍵の秘密性を向上することができる。

〔項目 4〕

車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置が実行する通信方法であって、

前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵の一部に対応する第 2 鍵を記憶し、

前記送信装置は、特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部を備えており

、
前記送信装置が、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複数の第 2 鍵を取得し、

取得した複数の第 2 鍵を、前記記憶部に記憶された態様で組み合わせることにより、前記特定の電子制御装置の第 1 鍵を生成し、

生成した第 1 鍵を使用して、前記特定の電子制御装置へデータを送信する、通信方法。

この通信方法によると、項目 1 と同様に、電子制御装置が、送信装置から送信されたデータの正当性を第 1 鍵を用いて認証することを実現しつつ、鍵の秘密性を向上することができる。

〔項目 5〕

車載ネットワークを介して複数の電子制御装置へデータを送信する送信装置が実行するコンピュータプログラムであって、

前記複数の電子制御装置のそれぞれは、前記送信装置から送信されたデータの正当性を認証するための自装置の鍵である第 1 鍵を記憶するとともに、他の電子制御装置の第 1 鍵の一部に対応する第 2 鍵を記憶し、

前記送信装置は、特定の電子制御装置の第 1 鍵を生成するのに用いられる、他の複数の電子制御装置に記憶された複数の第 2 鍵の組み合わせ態様を記憶する記憶部を備えており

、
前記送信装置に、

前記特定の電子制御装置へデータを送信する場合、前記他の複数の電子制御装置から複数の第 2 鍵を取得し、

取得した複数の第 2 鍵を、前記記憶部に記憶された態様で組み合わせることにより、前記特定の電子制御装置の第 1 鍵を生成し、

生成した第 1 鍵を使用して、前記特定の電子制御装置へデータを送信する、ことを実行させるためのコンピュータプログラム。

このコンピュータプログラムによると、項目 1 と同様に、電子制御装置が、送信装置から送信されたデータの正当性を第 1 鍵を用いて認証することを実現しつつ、鍵の秘密性を向上することができる。

【0053】

上述した実施例および変形例の任意の組み合わせもまた本発明の実施の形態として有用である。組み合わせによって生じる新たな実施の形態は、組み合わせられる実施例および変形例それぞれの効果をあわせもつ。また、請求項に記載の各構成要件が果たすべき機能は、実施例および変形例において示された各構成要素の単体もしくはそれらの連携によって実現されることも当業者には理解されるところである。

【符号の説明】

【0054】

10 車載通信システム、 20 対象 ECU、 22 ゲートウェイ ECU、 24

10

20

30

40

50

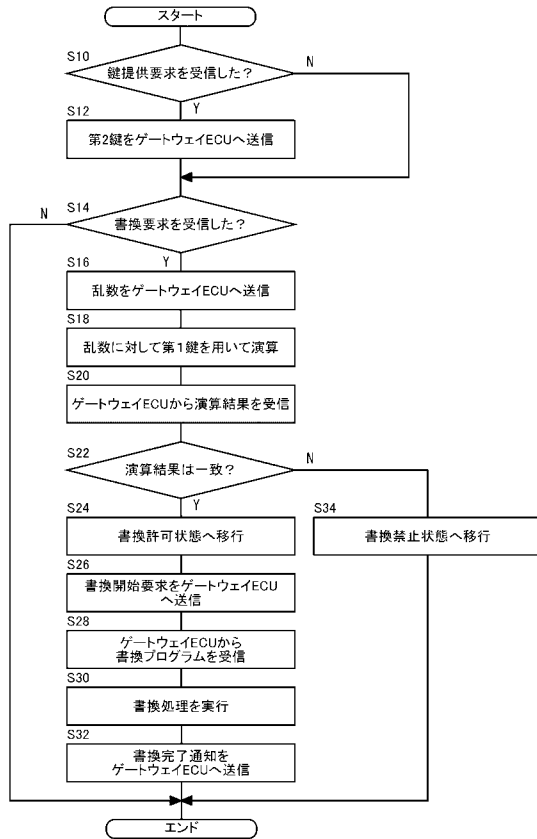
【図 1】

図1は、車両通信システム20の構成を示す。ゲートウェイECU22は、バス24を介して、対象ECU20a、対象ECU20b、対象ECU20cと接続されている。対象ECU20a、対象ECU20b、対象ECU20cは、それぞれ、20aの鍵、20bの鍵の一部、20cの鍵の一部を有する。ゲートウェイECU22は、20aの鍵、20bの鍵、20cの鍵を有する。

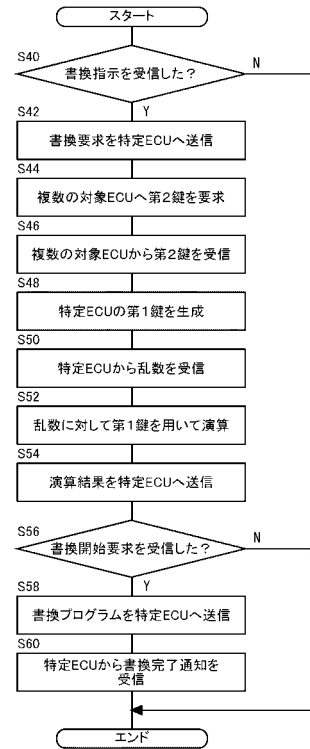
The diagram illustrates a vehicle system (10) with the following components and connections:

- ゲートウェイECU (Gateway ECU) 22**:
 - 通信部 (Communication Unit) 50
 - 制御部 (Control Unit) 54, containing:
 - 書換指示受信部 (Reception Unit for Rewrite Instruction) 60
 - 書換要求部 (Rewrite Request Unit) 62
 - 第2鍵取得部 (Second Key Acquisition Unit) 64
 - 第1鍵生成部 (First Key Generation Unit) 66
 - 記憶部 (Memory Unit) 52, containing:
 - プログラム記憶部 (Program Memory Unit) 56
 - 鍵生成規則記憶部 (Key Generation Rule Memory Unit) 58
 - 配送鍵記憶部 (Distribution Key Memory Unit) 59
- コネクタ (Connector) 28**: Connected to the Gateway ECU and the external device.
- 外部機器 (External Device) 14**: Connected to the system via the connector.
- 対象ECU (Target ECU) 20a**:
 - 通信部 (Communication Unit) 30
 - 制御部 (Control Unit) 34, containing:
 - データ処理部 (Data Processing Unit) 42
 - 照合部 (Verification Unit) 44
 - 書換実行部 (Rewrite Execution Unit) 46
 - 第2鍵提供部 (Second Key Provision Unit) 48
 - 記憶部 (Memory Unit) 32, containing:
 - プログラム記憶部 (Program Memory Unit) 36
 - 第1鍵記憶部 (First Key Memory Unit) 38
 - 第2鍵記憶部 (Second Key Memory Unit) 40
 - 配送鍵記憶部 (Distribution Key Memory Unit) 41
- 対象ECU 20b** and **対象ECU 20c**: Additional target ECUs connected to the system.

【図 3】



【図 4】



フロントページの続き

(51)Int.Cl. F I テーマコード (参考)
G 0 9 C 1/00 (2006.01) G 0 9 C 1/00 6 4 0 E

(72)発明者 竹内 政基
大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内

(72)発明者 小俣 皓司
大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内

(72)発明者 中西 智也
大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内

F ターム (参考) 5J104 AA07 AA16 EA02 EA13 EA18 KA04
5K032 AA08 BA06 DA01 DB28 EA03 EA06
5K033 AA08 BA06 DA01 DB20 EA03 EA06