(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2019-9509
(P2019-9509A)
(43)公開日　平成31年1月17日(2019.1.17)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640E	
H04L	9/08	(2006.01)	H04L	9/00	601F	

審査請求 未請求　請求項の数 13　ＯＬ　（全 30 頁）

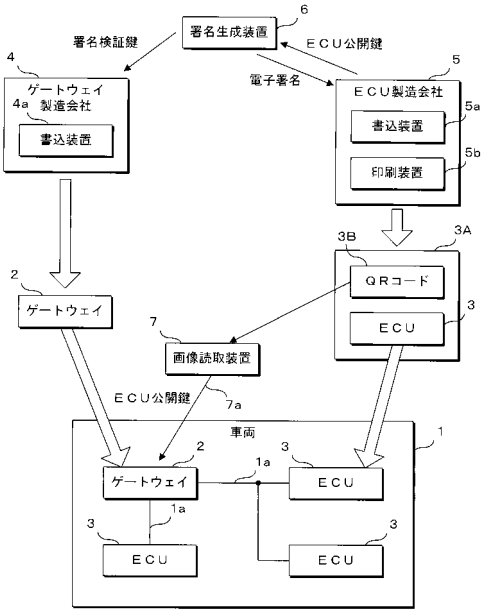
(21)出願番号　特願2017-120830 (P2017-120830)
(22)出願日　平成29年6月20日 (2017.6.20)

(71)出願人　504139662
国立大学法人名古屋大学
愛知県名古屋市千種区不老町１番
(71)出願人　395011665
株式会社オートネットワーク技術研究所
三重県四日市市西末広町１番１４号
(71)出願人　000183406
住友電装株式会社
三重県四日市市西末広町１番１４号
(71)出願人　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(74)代理人　100114557
弁理士　河野　英仁

最終頁に続く

(54)【発明の名称】車載認証システム、通信装置、車載認証装置、コンピュータプログラム、通信装置の認証方法及び通信装置の製造方法

(57)【要約】　（修正有）
【課題】車両外の装置との無線通信などを必要とせずに通信装置を認証することができる車載認証システムを提供する。
【解決手段】車両に搭載されるＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）３は第１秘密鍵及び第１公開鍵を記憶し、ゲートウェイ２は第２秘密鍵、第２公開鍵及び署名検証鍵を記憶する。ゲートウェイ２は、電子署名が付された第１公開鍵を取得して署名検証鍵にて検証し、正当な第１公開鍵を用いて第２公開鍵を暗号化してＥＣＵ３へ送信する。ＥＣＵ３は、暗号化された第２公開鍵を受信して第１秘密鍵にて復号し、第１秘密鍵を用いて復号して得た第２公開鍵を用いて第１公開鍵を暗号化してゲートウェイ２へ送信する。ゲートウェイ２は、暗号化された第１公開鍵を受信して第２秘密鍵にて復号し、復号した第１公開鍵が別途取得した第１公開鍵と比較して正当であると判定した場合に、ＥＣＵ３が正当な装置であると認証する。
【選択図】図１



【特許請求の範囲】
【請求項１】
車両内のネットワークに新たに接続された通信装置を車載認証装置が認証する車載認証システムにおいて、
前記通信装置は、第１秘密鍵及び第１公開鍵が記憶された第１記憶部を有し、
前記車載認証装置は、
第２秘密鍵及び第２公開鍵、並びに、前記第１公開鍵に付された電子署名の正否を検証する署名検証鍵が記憶された第２記憶部と、
前記電子署名が付された前記第１公開鍵を取得する第１公開鍵取得部と、
前記第１公開鍵取得部が取得した前記第１公開鍵に付された前記電子署名の正否を、前記第２記憶部に記憶された前記署名検証鍵を用いて検証する署名検証部と、
前記署名検証部により正当であると判定された電子署名が付された第１公開鍵を用いて、前記第２記憶部に記憶された第２公開鍵を暗号化する第２公開鍵暗号化部と、
前記第２公開鍵暗号化部が暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信する第２公開鍵送信部と
を有し、
前記通信装置は、
前記車載認証装置から暗号化された前記第２公開鍵を受信する第２公開鍵受信部と、
前記第２公開鍵受信部が受信した前記第２公開鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号する第２公開鍵復号部と、
前記第２公開鍵復号部が復号した前記第２公開鍵を用いて、前記第１記憶部に記憶された前記第１公開鍵を暗号化する第１公開鍵暗号化部と、
前記第１公開鍵暗号化部が暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信する第１公開鍵送信部と
を更に有し、
前記車載認証装置は、
前記通信装置から暗号化された前記第１公開鍵を受信する第１公開鍵受信部と、
前記第１公開鍵受信部が受信した前記第１公開鍵を、前記第２記憶部に記憶された前記第２秘密鍵を用いて復号する第１公開鍵復号部と、
前記第１公開鍵復号部が復号した前記第１公開鍵の正否を判定する第１公開鍵判定部と
を更に有し、
前記第１公開鍵判定部が前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証すること
を特徴とする車載認証システム。
【請求項２】
前記車載認証装置の前記第２記憶部は、前記ネットワークを介した前記車両内の通信に用いられる共通鍵を記憶し、
前記車載認証装置は、
前記第１公開鍵判定部が正当であると判定した前記第１公開鍵を用いて、前記第２記憶部に記憶された前記共通鍵を暗号化する共通鍵暗号化部と、
前記共通鍵暗号化部が暗号化した前記共通鍵を、前記ネットワークを介して前記通信装置へ送信する共通鍵送信部と
を有し、
前記通信装置は、
前記車載認証装置から暗号化された前記共通鍵を受信する共通鍵受信部と、
前記共通鍵受信部が受信した前記共通鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号する共通鍵復号部と
を有し、
前記通信装置の前記第１記憶部は、前記共通鍵復号部が復号した前記共通鍵を記憶すること

を特徴とする請求項１に記載の車載認証システム。
【請求項３】
前記通信装置又は前記通信装置の付随物には、前記電子署名が付された前記第１公開鍵を可視化した情報が描かれており、
前記情報を取得する可視化情報取得装置を更に備え、
前記車載認証装置は、前記可視化情報取得装置が取得した情報に基づいて前記電子署名が付された前記第１公開鍵を取得すること
を特徴とする請求項１又は請求項２に記載の車載認証システム。
【請求項４】
前記署名検証鍵と対になる署名生成鍵を記憶した記憶部と、入力された前記第１公開鍵に対して前記記憶部に記憶された前記署名生成鍵を用いて電子署名を生成する署名生成部とを有する署名生成装置を備えること
を特徴とする請求項１乃至請求項３のいずれか１つに記載の車載認証システム。
【請求項５】
前記車載認証装置の前記第１公開鍵取得部は、前記電子署名が付された前記第１公開鍵と共に、該第１公開鍵と対になる前記第１秘密鍵を記憶した前記通信装置の識別情報を取得し、
前記車載認証装置は、前記第１公開鍵取得部が取得した前記電子署名が付された前記第１公開鍵を、前記識別情報に対応付けて前記第２記憶部に記憶し、
前記通信装置は、前記ネットワークに接続された際に、自身の識別情報を前記車載認証装置へ送信する識別情報送信部を有し、
前記車載認証装置は、前記通信装置から前記識別情報を受信する識別情報受信部を有し、
前記車載認証装置の前記第２公開鍵暗号化部は、前記識別情報受信部が受信した識別情報に対応付けられた前記第１公開鍵を用いて前記第２公開鍵を暗号化すること
を特徴とする請求項１乃至請求項４のいずれか１つに記載の車載認証システム。
【請求項６】
車両内のネットワークに接続される通信装置において、
第１秘密鍵及び第１公開鍵が記憶された記憶部と、
前記ネットワークに接続された車載認証装置から暗号化された第２公開鍵を受信する第２公開鍵受信部と、
前記第２公開鍵受信部が受信した前記第２公開鍵を、前記記憶部に記憶された前記第１秘密鍵を用いて復号する第２公開鍵復号部と、
前記第２公開鍵復号部が復号した前記第２公開鍵を用いて、前記記憶部に記憶された前記第１公開鍵を暗号化する第１公開鍵暗号化部と、
前記第１公開鍵暗号化部が暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信する第１公開鍵送信部と
を備えることを特徴とする通信装置。
【請求項７】
車両内のネットワークに接続される通信装置において、
第１秘密鍵が記憶された記憶部を備え、
装置本体又は装置の付随物には、前記第１秘密鍵と対になる第１公開鍵及び該第１公開鍵の正当性を示す電子署名を可視化した情報が描かれていること
を特徴とする通信装置。
【請求項８】
車両内のネットワークに新たに接続された通信装置を認証する車載認証装置において、
前記通信装置が記憶している第１秘密鍵と対になる第１公開鍵に付された電子署名の正否を検証する署名検証鍵、並びに、第２秘密鍵及び第２公開鍵が記憶された記憶部と、
前記電子署名が付された前記第１公開鍵を取得する第１公開鍵取得部と、
前記第１公開鍵取得部が取得した前記第１公開鍵に付された前記電子署名の正否を、前

記記憶部に記憶された前記署名検証鍵を用いて検証する署名検証部と、
前記署名検証部により正当であると判定された電子署名が付された第１公開鍵を用いて、前記記憶部に記憶された第２公開鍵を暗号化する第２公開鍵暗号化部と、
前記第２公開鍵暗号化部が暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信する第２公開鍵送信部と、
前記通信装置から暗号化された前記第１公開鍵を受信する第１公開鍵受信部と、
前記第１公開鍵受信部が受信した前記第１公開鍵を、前記記憶部に記憶された前記第２秘密鍵を用いて復号する第１公開鍵復号部と、
前記第１公開鍵復号部が復号した前記第１公開鍵の正否を判定する第１公開鍵判定部と
を備え、
前記第１公開鍵判定部が前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証すること
を特徴とする車載認証装置。
【請求項９】
第１秘密鍵及び第１公開鍵が記憶された記憶部を有するコンピュータに、
車両内のネットワークに接続された車載認証装置から暗号化された第２公開鍵を受信させ、
受信した前記第２公開鍵を、前記記憶部に記憶された前記第１秘密鍵を用いて復号させ、
復号した前記第２公開鍵を用いて、前記記憶部に記憶された前記第１公開鍵を暗号化させ、
暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信させること
を特徴とするコンピュータプログラム。
【請求項１０】
車両内のネットワークに接続された通信装置が記憶している第１秘密鍵と対になる第１公開鍵に付された電子署名の正否を検証する署名検証鍵、並びに、第２秘密鍵及び第２公開鍵が記憶された記憶部を有するコンピュータに、
前記電子署名が付された前記第１公開鍵を取得させ、
取得した前記第１公開鍵に付された前記電子署名の正否を、前記記憶部に記憶された前記署名検証鍵を用いて検証させ、
検証により正当であると判定された電子署名が付された第１公開鍵を用いて、前記記憶部に記憶された第２公開鍵を暗号化させ、
暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信させ、
前記通信装置から暗号化された前記第１公開鍵を受信させ、
受信した前記第１公開鍵を、前記記憶部に記憶された前記第２秘密鍵を用いて復号させ、
復号した前記第１公開鍵の正否を判定させ、
前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証させること
を特徴とするコンピュータプログラム。
【請求項１１】
第１秘密鍵及び第１公開鍵を車両内のネットワークに接続される通信装置の第１記憶部に記憶し、
第２秘密鍵及び第２公開鍵、並びに、前記第１公開鍵に付された電子署名の正否を検証する署名検証鍵を車載認証装置の第２記憶部に記憶し、
前記車載認証装置が、前記電子署名が付された前記第１公開鍵を取得し、取得した前記第１公開鍵に付された前記電子署名の正否を、前記第２記憶部に記憶された前記署名検証鍵を用いて検証し、検証により正当であると判定された電子署名が付された第１公開鍵を用いて、前記第２記憶部に記憶された第２公開鍵を暗号化し、暗号化した前記第２公開鍵

を、前記ネットワークを介して前記通信装置へ送信し、
前記通信装置が、前記車載認証装置から暗号化された前記第２公開鍵を受信し、受信した前記第２公開鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号し、復号した前記第２公開鍵を用いて、前記第１記憶部に記憶された前記第１公開鍵を暗号化し、暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信し、
前記車載認証装置が、前記通信装置から暗号化された前記第１公開鍵を受信し、受信した前記第１公開鍵を、前記第２記憶部に記憶された前記第２秘密鍵を用いて復号し、復号した前記第１公開鍵の正否を判定し、前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証すること
を特徴とする通信装置の認証方法。

【請求項１２】
署名生成装置が、第１公開鍵の電子署名を生成し、
情報書込装置が、前記第１公開鍵及び該第１公開鍵と対になる第１秘密鍵を、車両内のネットワークに接続される通信装置の第１記憶部に書き込み、
印刷装置が、前記通信装置又は前記通信装置の付随物に、前記電子署名が付された前記第１公開鍵を可視化した情報を印刷し、
情報書込装置が、第２秘密鍵及び第２公開鍵、並びに、前記第１公開鍵に付された電子署名の正否を検証する署名検証鍵を車載認証装置の第２記憶部に書き込み、
可視化情報取得装置が、印刷された前記情報を取得し、
前記車載認証装置が、前記可視化情報取得装置が取得した情報に基づいて前記電子署名が付された前記第１公開鍵を取得し、取得した前記第１公開鍵に付された前記電子署名の正否を、前記第２記憶部に記憶された前記署名検証鍵を用いて検証し、検証により正当であると判定された電子署名が付された第１公開鍵を用いて、前記第２記憶部に記憶された第２公開鍵を暗号化し、暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信し、
前記通信装置が、前記車載認証装置から暗号化された前記第２公開鍵を受信し、受信した前記第２公開鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号し、復号した前記第２公開鍵を用いて、前記第１記憶部に記憶された前記第１公開鍵を暗号化し、暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信し、
前記車載認証装置が、前記通信装置から暗号化された前記第１公開鍵を受信し、受信した前記第１公開鍵を、前記第２記憶部に記憶された前記第２秘密鍵を用いて復号し、復号した前記第１公開鍵の正否を判定し、前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証すること
を特徴とする通信装置の認証方法。

【請求項１３】
署名生成装置が、第１公開鍵の電子署名を生成し、
情報書込装置が、前記第１公開鍵及び該第１公開鍵と対になる第１秘密鍵を、車両内のネットワークに接続される通信装置の第１記憶部に書き込み、
印刷装置が、前記通信装置又は前記通信装置の付随物に、前記電子署名が付された前記第１公開鍵を可視化した情報を印刷すること
を特徴とする通信装置の製造方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両内のネットワークに接続された通信装置を認証するための車載認証システム、通信装置、車載認証装置、コンピュータプログラム、通信装置の認証方法及び通信装置の製造方法に関する。

【背景技術】
【０００２】
近年、車両の自動運転又は運転補助等の技術が研究開発されており、車両の高機能化が

推し進められている。車両の高機能化に伴って、車両に搭載されるＥＣＵ（Electronic Control Unit）などの制御装置においては、ハードウェア及びソフトウェアが高機能化及び複雑化している。これに対して、車両の制御システムに不正な装置又はソフトウェアの注入を行うことによって、例えば車両の乗っ取りなどの攻撃が行われ得るという問題がある。車両に対する不正な攻撃を防ぐため、例えば通信の暗号化などの種々の対策が検討されている。

【０００３】

特許文献１においては、車両の電子キーを交換後に再登録する際のセキュリティ性を確保することを目的とした電子キー登録システムが提案されている。この電子キー登録システムでは、車両に搭載されたＥＣＵが車両外のセンターとの通信を行って、交換する電子キーが正当なものであるか否かの照合を行うことによって、セキュリティ性を高めている。また特許文献２においては、故障などによりＥＣＵを交換した場合に、交換後のＥＣＵに電子キーを登録する電子キー登録システムが提案されている。この電子キー登録システムでは、交換後のＥＣＵが電子キーから読み出した情報を車両外のセンターへ送信して照合を行い、照合が成立した場合に電子キーを登録することによって、セキュリティ性を高めている。

【０００４】

特許文献３においては、管理装置及びＥＣＵの間で共通のデータを生成し、このデータを通信のメッセージ認証コードの生成又は暗号鍵に使用することでセキュリティ性を向上することを目的とした車載制御システムが提案されている。この車載制御システムでは、管理装置及びＥＣＵが共通の第１データを記憶し、管理装置が第２データを生成してＥＣＵへ送信し、管理装置及びＥＣＵが第１データ及び第２データを用いて共通の第３データを生成する。

【０００５】

非特許文献１においては、車両に対して新たなＥＣＵを追加する際に、車内ネットワークを介した通信にて必要となる暗号処理用の鍵を、車両に搭載されたセキュリティゲートウェイと新たなＥＣＵとの間で安全に授受するための方法が提案されている。この方法では、セキュリティゲートウェイが有するマスターキー及び初期マスターキーと、新たなＥＣＵに書き込まれた初期マスターキーとを利用して、最終的にセキュリティゲートウェイが通信用のセッションキーをＥＣＵへ送信する。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２０１４－１５６７２３号公報

【特許文献２】特開２０１４－０７７２８１号公報

【特許文献３】特開２０１７－０６００３１号公報

【非特許文献】

【０００７】

【非特許文献１】Takaya Kubota, Mitsuru Shiozaki and Takeshi Fujino, "Proposal and Implementation of Key Exchange Protocol suitable for In-Vehicle Network based on Symmetric Key Cipher using PUF as Key Storage", escarEU2016, 2016.

【発明の概要】

【発明が解決しようとする課題】

【０００８】

特許文献１，２に記載された電子キー登録システムでは、車両外のセンターを利用して電子キーの照合を行う必要があるが、車両は必ずしも車両外の装置と通信を行うことができる環境にあるとは限らず、センターとの通信を行うことができない場合にはこのシステムを利用できないという問題がある。

【０００９】

特許文献３に記載の車載制御システムでは、センターなどとの通信を行う必要はないが

、管理装置と共通の第１データをＥＣＵのメモリなどに予め書き込んでおく必要がある。例えばＥＣＵの故障による交換又は機能追加のための新たなＥＣＵの追加等を行う場合には、交換又は追加される新たなＥＣＵのメモリに共通の第１データを書き込む必要がある。このため、ＥＣＵの交換又は追加等の作業を行う作業者が、第１データを不正に取得することが可能である。不正に第１データを取得した悪意の作業者は、例えば第１データを不正な装置のメモリに書き込み、不正な装置を車両に取り付けるなどの行為を行う虞がある。非特許文献１に記載の技術も同様に、新たなＥＣＵに対して共通の初期マスターキーの書き込みを行う必要があり、この際に初期マスターキーが漏洩する可能性がある。

【００１０】

本発明は、斯かる事情に鑑みてなされたものであって、その目的とするところは、車両外の装置との無線通信などを必要とせずに、車両に対する通信装置の交換又は追加等を行った際にこの通信装置を認証することができる車載認証システム、通信装置、車載認証装置、コンピュータプログラム、通信装置の認証方法及び通信装置の製造方法を提供することにある。

【課題を解決するための手段】

【００１１】

本発明に係る車載認証システムは、車両内のネットワークに新たに接続された通信装置を車載認証装置が認証する車載認証システムにおいて、前記通信装置は、第１秘密鍵及び第１公開鍵が記憶された第１記憶部を有し、前記車載認証装置は、第２秘密鍵及び第２公開鍵、並びに、前記第１公開鍵に付された電子署名の正否を検証する署名検証鍵が記憶された第２記憶部と、前記電子署名が付された前記第１公開鍵を取得する第１公開鍵取得部と、前記第１公開鍵取得部が取得した前記第１公開鍵に付された前記電子署名の正否を、前記第２記憶部に記憶された前記署名検証鍵を用いて検証する署名検証部と、前記署名検証部により正当であると判定された電子署名が付された第１公開鍵を用いて、前記第２記憶部に記憶された第２公開鍵を暗号化する第２公開鍵暗号化部と、前記第２公開鍵暗号化部が暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信する第２公開鍵送信部とを有し、前記通信装置は、前記車載認証装置から暗号化された前記第２公開鍵を受信する第２公開鍵受信部と、前記第２公開鍵受信部が受信した前記第２公開鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号する第２公開鍵復号部と、前記第２公開鍵復号部が復号した前記第２公開鍵を用いて、前記第１記憶部に記憶された前記第１公開鍵を暗号化する第１公開鍵暗号化部と、前記第１公開鍵暗号化部が暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信する第１公開鍵送信部とを更に有し、前記車載認証装置は、前記通信装置から暗号化された前記第１公開鍵を受信する第１公開鍵受信部と、前記第１公開鍵受信部が受信した前記第１公開鍵を、前記第２記憶部に記憶された前記第２秘密鍵を用いて復号する第１公開鍵復号部と、前記第１公開鍵復号部が復号した前記第１公開鍵の正否を判定する第１公開鍵判定部とを更に有し、前記第１公開鍵判定部が前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証することを特徴とする。

【００１２】

また、本発明に係る車載認証システムは、前記車載認証装置の前記第２記憶部が、前記ネットワークを介した前記車両内の通信に用いられる共通鍵を記憶し、前記車載認証装置は、前記第１公開鍵判定部が正当であると判定した前記第１公開鍵を用いて、前記第２記憶部に記憶された前記共通鍵を暗号化する共通鍵暗号化部と、前記共通鍵暗号化部が暗号化した前記共通鍵を、前記ネットワークを介して前記通信装置へ送信する共通鍵送信部とを有し、前記通信装置は、前記車載認証装置から暗号化された前記共通鍵を受信する共通鍵受信部と、前記共通鍵受信部が受信した前記共通鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号する共通鍵復号部とを有し、前記通信装置の前記第１記憶部は、前記共通鍵復号部が復号した前記共通鍵を記憶することを特徴とする。

【００１３】

また、本発明に係る車載認証システムは、前記通信装置又は前記通信装置の付随物には

、前記電子署名が付された前記第１公開鍵を可視化した情報が描かれており、前記情報を取得する可視化情報取得装置を更に備え、前記車載認証装置は、前記可視化情報取得装置が取得した情報に基づいて前記電子署名が付された前記第１公開鍵を取得することを特徴とする。

【００１４】

また、本発明に係る車載認証システムは、前記署名検証鍵と対になる署名生成鍵を記憶した記憶部と、入力された前記第１公開鍵に対して前記記憶部に記憶された前記署名生成鍵を用いて電子署名を生成する署名生成部とを有する署名生成装置を備えることを特徴とする。

【００１５】

また、本発明に係る車載認証システムは、前記車載認証装置の前記第１公開鍵取得部は、前記電子署名が付された前記第１公開鍵と共に、該第１公開鍵と対になる前記第１秘密鍵を記憶した前記通信装置の識別情報を取得し、前記車載認証装置は、前記第１公開鍵取得部が取得した前記電子署名が付された前記第１公開鍵を、前記識別情報に対応付けて前記第２記憶部に記憶し、前記通信装置は、前記ネットワークに接続された際に、自身の識別情報を前記車載認証装置へ送信する識別情報送信部を有し、前記車載認証装置は、前記通信装置から前記識別情報を受信する識別情報受信部を有し、前記車載認証装置の前記第２公開鍵暗号化部は、前記識別情報受信部が受信した識別情報に対応付けられた前記第１公開鍵を用いて前記第２公開鍵を暗号化することを特徴とする。

【００１６】

また、本発明に係る通信装置は、車両内のネットワークに接続される通信装置において、第１秘密鍵及び第１公開鍵が記憶された記憶部と、前記ネットワークに接続された車載認証装置から暗号化された第２公開鍵を受信する第２公開鍵受信部と、前記第２公開鍵受信部が受信した前記第２公開鍵を、前記記憶部に記憶された前記第１秘密鍵を用いて復号する第２公開鍵復号部と、前記第２公開鍵復号部が復号した前記第２公開鍵を用いて、前記記憶部に記憶された前記第１公開鍵を暗号化する第１公開鍵暗号化部と、前記第１公開鍵暗号化部が暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信する第１公開鍵送信部とを備えることを特徴とする。

【００１７】

また、本発明に係る通信装置は、車両内のネットワークに接続される通信装置において、第１秘密鍵が記憶された記憶部を備え、装置本体又は装置の付随物には、前記第１秘密鍵と対になる第１公開鍵及び該第１公開鍵の正当性を示す電子署名を可視化した情報が描かれていることを特徴とする。

【００１８】

また、本発明に係る車載認証装置は、車両内のネットワークに新たに接続された通信装置を認証する車載認証装置において、前記通信装置が記憶している第１秘密鍵と対になる第１公開鍵に付された電子署名の正否を検証する署名検証鍵、並びに、第２秘密鍵及び第２公開鍵が記憶された記憶部と、前記電子署名が付された前記第１公開鍵を取得する第１公開鍵取得部と、前記第１公開鍵取得部が取得した前記第１公開鍵に付された前記電子署名の正否を、前記記憶部に記憶された前記署名検証鍵を用いて検証する署名検証部と、前記署名検証部により正当であると判定された電子署名が付された第１公開鍵を用いて、前記記憶部に記憶された第２公開鍵を暗号化する第２公開鍵暗号化部と、前記第２公開鍵暗号化部が暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信する第２公開鍵送信部と、前記通信装置から暗号化された前記第１公開鍵を受信する第１公開鍵受信部と、前記第１公開鍵受信部が受信した前記第１公開鍵を、前記記憶部に記憶された前記第２秘密鍵を用いて復号する第１公開鍵復号部と、前記第１公開鍵復号部が復号した前記第１公開鍵の正否を判定する第１公開鍵判定部とを備え、前記第１公開鍵判定部が前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証することを特徴とする。

【００１９】

また、本発明に係るコンピュータプログラムは、第１秘密鍵及び第１公開鍵が記憶された記憶部を有するコンピュータに、車両内のネットワークに接続された車載認証装置から暗号化された第２公開鍵を受信させ、受信した前記第２公開鍵を、前記記憶部に記憶された前記第１秘密鍵を用いて復号させ、復号した前記第２公開鍵を用いて、前記記憶部に記憶された前記第１公開鍵を暗号化させ、暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信させることを特徴とする。

【００２０】

また、本発明に係るコンピュータプログラムは、車両内のネットワークに接続された通信装置が記憶している第１秘密鍵と対になる第１公開鍵に付された電子署名の正否を検証する署名検証鍵、並びに、第２秘密鍵及び第２公開鍵が記憶された記憶部を有するコンピュータに、前記電子署名が付された前記第１公開鍵を取得させ、取得した前記第１公開鍵に付された前記電子署名の正否を、前記記憶部に記憶された前記署名検証鍵を用いて検証させ、検証により正当であると判定された電子署名が付された第１公開鍵を用いて、前記記憶部に記憶された第２公開鍵を暗号化させ、暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信させ、前記通信装置から暗号化された前記第１公開鍵を受信させ、受信した前記第１公開鍵を、前記記憶部に記憶された前記第２秘密鍵を用いて復号させ、復号した前記第１公開鍵の正否を判定させ、前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証させることを特徴とする。

【００２１】

また、本発明に係る通信装置の認証方法は、第１秘密鍵及び第１公開鍵を車両内のネットワークに接続される通信装置の第１記憶部に記憶し、第２秘密鍵及び第２公開鍵、並びに、前記第１公開鍵に付された電子署名の正否を検証する署名検証鍵を車載認証装置の第２記憶部に記憶し、前記車載認証装置が、前記電子署名が付された前記第１公開鍵を取得し、取得した前記第１公開鍵に付された前記電子署名の正否を、前記第２記憶部に記憶された前記署名検証鍵を用いて検証し、検証により正当であると判定された電子署名が付された第１公開鍵を用いて、前記第２記憶部に記憶された第２公開鍵を暗号化し、暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信し、前記通信装置が、前記車載認証装置から暗号化された前記第２公開鍵を受信し、受信した前記第２公開鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号し、復号した前記第２公開鍵を用いて、前記第１記憶部に記憶された前記第１公開鍵を暗号化し、暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信し、前記車載認証装置が、前記通信装置から暗号化された前記第１公開鍵を受信し、受信した前記第１公開鍵を、前記第２記憶部に記憶された前記第２秘密鍵を用いて復号し、復号した前記第１公開鍵の正否を判定し、前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証することを特徴とする。

【００２２】

また、本発明に係る通信装置の認証方法は、署名生成装置が、第１公開鍵の電子署名を生成し、情報書込装置が、前記第１公開鍵及び該第１公開鍵と対になる第１秘密鍵を、車両内のネットワークに接続される通信装置の第１記憶部に書き込み、印刷装置が、前記通信装置又は前記通信装置の付随物に、前記電子署名が付された前記第１公開鍵を可視化した情報を印刷し、情報書込装置が、第２秘密鍵及び第２公開鍵、並びに、前記第１公開鍵に付された電子署名の正否を検証する署名検証鍵を車載認証装置の第２記憶部に書き込み、可視化情報取得装置が、印刷された前記情報を取得し、前記車載認証装置が、前記可視化情報取得装置が取得した情報に基づいて前記電子署名が付された前記第１公開鍵を取得し、取得した前記第１公開鍵に付された前記電子署名の正否を、前記第２記憶部に記憶された前記署名検証鍵を用いて検証し、検証により正当であると判定された電子署名が付された第１公開鍵を用いて、前記第２記憶部に記憶された第２公開鍵を暗号化し、暗号化した前記第２公開鍵を、前記ネットワークを介して前記通信装置へ送信し、前記通信装置が、前記車載認証装置から暗号化された前記第２公開鍵を受信し、受信した前記第２公開鍵を、前記第１記憶部に記憶された前記第１秘密鍵を用いて復号し、復号した前記第２公開

鍵を用いて、前記第１記憶部に記憶された前記第１公開鍵を暗号化し、暗号化した前記第１公開鍵を、前記ネットワークを介して前記車載認証装置へ送信し、前記車載認証装置が、前記通信装置から暗号化された前記第１公開鍵を受信し、受信した前記第１公開鍵を、前記第２記憶部に記憶された前記第２秘密鍵を用いて復号し、復号した前記第１公開鍵の正否を判定し、前記第１公開鍵が正当であると判定した場合に、前記通信装置が正当な装置であると認証することを特徴とする。

【００２３】

また、本発明に係る通信装置の製造方法は、署名生成装置が、第１公開鍵の電子署名を生成し、情報書込装置が、前記第１公開鍵及び該第１公開鍵と対になる第１秘密鍵を、車両内のネットワークに接続される通信装置の第１記憶部に書き込み、印刷装置が、前記通信装置又は前記通信装置の付随物に、前記電子署名が付された前記第１公開鍵を可視化した情報を印刷することを特徴とする。

【００２４】

本発明においては、車両内のネットワークに新たに接続された通信装置を、車両に搭載された車載認証装置が認証する（即ち、この通信装置が正当な装置であるか否かを判断する）。

通信装置は、第１秘密鍵及び第１公開鍵を記憶しておく。車載認証装置は、第２秘密鍵及び第２公開鍵と、電子署名の正否を検証する署名検証鍵とを記憶しておく。通信装置及び車載認証装置は、共通の鍵情報を記憶しておく必要がないため、装置の製造後に共通の鍵情報が扱われることはなく、共通の鍵情報が漏えいすることはない。本発明の手法では、これらの鍵情報の記憶は装置の製造段階で予め行われる。

【００２５】

まず車載認証装置は、車両内のネットワークに対して新たに接続される通信装置の第１公開鍵を取得する。公開鍵は外部に漏えいしても問題がない情報であるため、車載認証装置による第１公開鍵の取得はどのような方法で行われてもよい。ただし第１公開鍵には電子署名が付され、車載認証装置は、予め記憶した署名検証鍵を用いて取得した第１公開鍵の正否を検証する。第１公開鍵が正当なものである場合、この第１公開鍵を用いて、自身が記憶している第２公開鍵を暗号化し、暗号化した第２公開鍵を、車両内のネットワークを介して新たに接続された通信装置へ送信する。このときに送信される第２公開鍵を復号することができるのは、暗号化に用いた第１公開鍵と対になる第１秘密鍵を有する通信装置のみである。

【００２６】

車載認証装置から暗号化された第２公開鍵を受信した通信装置は、自身が記憶している第１秘密鍵を用いて第２公開鍵を復号する。この第２公開鍵を用いて通信装置は、自身が記憶している第１公開鍵を暗号化し、暗号化した第１公開鍵を、車両内のネットワークを介して車載認証装置へ送信する。このときに送信される第１公開鍵を復号することができるのは、暗号化に用いた第２公開鍵と対になる第２秘密鍵を有する車載認証装置のみである。

【００２７】

通信装置から暗号化された第１公開鍵を受信した車載認証装置は、自身が記憶している第２秘密鍵を用いて第１公開鍵を復号し、復号した第１公開鍵の正否を判定する。このときに車載認証装置は、例えば復号した第１公開鍵が、電子署名付きで取得した第１公開鍵と一致する場合に、この第１公開鍵を正当なものであると判定する構成とすることができる。第１公開鍵が正当であると判定した場合、車載認証装置は、この第１公開鍵の送信元である通信装置を正当な装置であると判断する。

このように本発明に係る車載認証システムでは、新たに車両内のネットワークに接続された通信装置を認証するために、車載認証装置が車両外のサーバ装置などとの間で通信を行う必要がない。また漏洩を防止すべき第１秘密鍵及び第２秘密鍵は、例えば装置の製造段階等において各装置のメモリなどに予め書き込んでおけばよいため、通信装置を接続する作業を行う作業者が第１秘密鍵及び第２秘密鍵を扱う必要はなく、悪意の作業者が第１

秘密鍵及び第２秘密鍵を不正に取得することを防止できる。

【００２８】

また本発明においては、車両内のネットワークを介した通信に用いられる共通鍵を車載認証装置が記憶し、正当な装置であると判定した新規の通信装置に対してこの共通鍵を送信する処理を行う。共通鍵は、車両内のネットワークに接続された全ての装置が有する共通の鍵であり、例えば送受信する情報の暗号化／復号の処理又はメッセージ認証子の生成／検証の処理等を行う際に用いられる。

車載認証装置は、通信装置の第１公開鍵を用いて共通鍵を暗号化し、暗号化した共通鍵を通信装置へ送信する。暗号化された共通鍵を受信した通信装置は、自身が記憶している第１秘密鍵を用いて共通鍵を復号する。以降、通信装置は、車両内のネットワークに接続された他の装置との間で、共通鍵を用いた通信を行うことが可能となる。

【００２９】

また本発明においては、第１公開鍵に電子署名を付したものを可視化した情報、例えば２次元バーコード若しくはＱＲコード（登録商標）等の画像、又は、数字若しくは文字等を複数並べた文字列などの可視化情報を生成し、通信装置の本体又は通信装置の付随物等に可視化情報を描く（印刷する）。通信装置の本体に可視化情報を描く場合、例えば通信装置を覆う外装部品などに可視化情報を描くことができる。通信装置の付随物は、例えば通信装置が梱包される箱、パッケージ又は取扱説明書等とすることができる。

通信装置を車両内のネットワークに接続する際、可視化情報取得装置にて通信装置の本体又は付随物に描かれた可視化情報の取得を行う。取得した可視化情報を電子署名付きの第１公開鍵の情報に変換することによって、車載認証装置は電子署名付きの第１公開鍵を取得することができる。なお可視化情報から第１公開鍵への変換は、可視化情報取得装置が行ってもよく、車載認証装置が行ってもよい。

【００３０】

また本発明においては、通信装置の第１公開鍵の電子署名を署名生成装置が生成する。署名生成装置は、車載認証装置が記憶している署名検証鍵と対になる署名生成鍵を記憶しており、この署名生成鍵を用いて通信装置の第１公開鍵の電子署名を生成する。署名生成装置は例えば通信装置の製造前の段階で署名の生成を行い、生成された電子署名付きの第１公開鍵に基づいて、通信装置の製造工程において上述の可視化情報の印刷が行われる。

【００３１】

また本発明において車載認証装置は、通信装置の電子署名付の第１公開鍵を取得する際に、通信装置の識別情報を取得する。例えば通信装置の識別情報は、電子署名付の第１公開鍵と共に可視化情報として可視化情報取得装置を介して車載認証装置が取得する構成とすることができる。車載認証装置は、通信装置の識別情報に対応付けて第１公開鍵を記憶しておく。通信装置は、車両内のネットワークに接続された際に、自身の識別情報を車載認証装置へ送信する。この識別情報を受信した車載認証装置は、受信した識別情報に対応付けられた第１公開鍵を用いて自身の第２公開鍵を暗号化し、通信装置へ送信する。これにより車載認証装置は、複数の通信装置に関する第１公開鍵を取得し、複数の通信装置に対して並列的に認証を行うことが可能となる。

【発明の効果】

【００３２】

本発明による場合は、車載認証装置及び通信装置が車両外の装置との無線通信などを行うことを必要とせずに、車両内のネットワークに接続された通信装置が正当な装置であるか否かを車載認証装置が判断することができると共に、秘匿性の高い情報が漏えいする可能性を低減することができる。

【図面の簡単な説明】

【００３３】

【図１】本実施の形態に係る車載認証システムを説明するための模式図である。

【図２】セッション鍵を授受するためにゲートウェイ及びＥＣＵの間で行われる処理を説明するための模式図である。

【図３】ゲートウェイの構成を示すブロック図である。
【図４】ＥＣＵ公開鍵ＤＢの一構成例を示す模式図である。
【図５】ＥＣＵの構成を示すブロック図である。
【図６】署名生成装置の構成を示すブロック図である。
【図７】画像読取装置の構成を示すブロック図である。
【図８】ＥＣＵ製造会社によるＥＣＵの製造方法を説明するためのフローチャートである。
【図９】ＥＣＵの車両への取り付け方法を説明するためのフローチャートである。
【図１０】ゲートウェイが行うＥＣＵ公開鍵の取得処理の手順を示すフローチャートである。
【図１１】ＥＣＵが行う認証処理の手順を示すフローチャートである。
【図１２】ゲートウェイが行う認証処理の手順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】
【００３４】
＜システム構成及び概要＞
図１は、本実施の形態に係る車載認証システムを説明するための模式図である。本実施の形態に係る車載認証システムは、車両１に搭載されたゲートウェイ２に複数の通信線１ａが接続され、各通信線１ａに対して一又は複数のＥＣＵ３が接続され、ＥＣＵ３が通信線１ａ及びゲートウェイ２を介して他のＥＣＵ３との通信を行う構成の車載通信システムにおいて、いずれかのＥＣＵ３の交換又は新規のＥＣＵ３の追加等を目的として通信線１ａに対して新たなＥＣＵ３が接続された場合に、このＥＣＵ３が正当な装置であるか否かをゲートウェイ２が判定する構成である。
【００３５】
通信線１ａを介して行われる車両１内の通信においては、ゲートウェイ２及びＥＣＵ３は、送信するメッセージに対してメッセージ認証子を付す。なお本実施の形態においてはメッセージにメッセージ認証子を付す構成を採用するが、これに限るものではない。例えばメッセージに電子署名を付してもよく、また例えばメッセージを暗号化して送信してもよい。
【００３６】
メッセージを受信したゲートウェイ２及びＥＣＵ３は、メッセージ認証子の正否を判定することによって受信したメッセージの正否を判定し、受信したメッセージが正当なものではないと判定した場合には、このメッセージを破棄する処理を行う。メッセージ認証子の生成及び判定を行うために、全てのゲートウェイ２及びＥＣＵ３は共通のセッション鍵を有している。例えばゲートウェイ２及びＥＣＵ３は、送信するメッセージに含まれるデータをセッション鍵にて暗号化することでメッセージ認証子を生成することができる。またメッセージを受信したゲートウェイ２及びＥＣＵ３は、メッセージに付されたメッセージ認証子をセッション鍵にて復号し、復号して得られたデータとメッセージに含まれるデータとが一致するか否かに応じて、このメッセージが正当なものであるか否かを判定することができる。
【００３７】
セッション鍵は、ゲートウェイ２の製造工程などにおいてゲートウェイ２の記憶部に予め書き込まれるか、又は、ゲートウェイ２により生成される。ＥＣＵ３は、工場出荷後の初期状態においてセッション鍵を有しておらず、車両１の通信線１ａに接続された後、ゲートウェイ２から送信されるセッション鍵を取得することにより、車両１内の他のＥＣＵ３とのメッセージ送受信を行うことが可能となる。ゲートウェイ２は、車両１内の通信線１ａに新たに接続されたＥＣＵ３が正当な装置であると判断した場合に、このＥＣＵ３に対してセッション鍵を送信する。
【００３８】
本実施の形態に係る車載認証システムでは、ゲートウェイ２からＥＣＵ３へのセッション鍵の授受を安全に行うために、公開鍵方式の暗号化技術を用いたＥＣＵ３の認証方式を

採用している。公開鍵方式では、秘密鍵及び公開鍵の一組の鍵が用いられ、例えば公開鍵で暗号化された情報を秘密鍵で復号し、また例えば秘密鍵で生成された電子署名を公開鍵で検証するなどの処理が行われる。本実施の形態に係る車載認証システムでは、ゲートウェイ２のＧＷ（ゲートウェイ）秘密鍵及びＧＷ公開鍵と、各ＥＣＵ３のＥＣＵ秘密鍵及びＥＣＵ公開鍵と、電子署名の作成／検証用の署名生成鍵及び署名検証鍵との３組の鍵が用いられる。なお署名生成鍵が秘密鍵であり、署名検証鍵が公開鍵である。

【００３９】

ゲートウェイ２の製造及び販売等を行うゲートウェイ製造会社４は、電子署名の検証に必要な署名検証鍵を予め取得している。電子署名を生成する署名生成装置６は、例えば車両１の製造会社又は販売会社等が管理運営する装置であり、電子署名の生成に署名生成鍵を用いる。署名検証鍵は、この署名生成鍵と対になる鍵である。ゲートウェイ製造会社４は、署名生成装置６を管理運営する会社から配布された署名検証鍵を予め取得することができる。ゲートウェイ製造会社４は、ゲートウェイ２の製造工程において書込装置４ａを用い、ゲートウェイ２の記憶部にＧＷ秘密鍵及びＧＷ公開鍵と、署名検証鍵とを書き込む。なお本実施の形態においてゲートウェイ２の記憶部には、署名検証鍵を書き込むための特別な領域が設けられている。この署名検証鍵を記憶する領域は、データの書き込みを１回のみ行うことができる領域である。この領域に書き込まれた署名検証鍵は、以降に書き換えることはできない。製造されたゲートウェイ２は、例えば車両１の製造工場に運ばれ、製造工場にて車両１に搭載される。

【００４０】

ＥＣＵ３の製造及び販売等を行うＥＣＵ製造会社５は、製造するＥＣＵ３毎に異なるＥＣＵ秘密鍵及びＥＣＵ公開鍵の組を、例えば社内のサーバ装置などにて生成する。ＥＣＵ製造会社５は、生成したＥＣＵ公開鍵を、署名生成装置６を管理運営する会社などへ送信して電子署名の生成を依頼する。この依頼に応じて署名生成装置６ではＥＣＵ公開鍵毎に電子署名が生成され、ＥＣＵ公開鍵に電子署名を付した情報（ＥＣＵ公開鍵証明書）がＥＣＵ製造会社５に与えられる。ＥＣＵ製造会社５は、ＥＣＵ３の製造工程において書込装置５ａを用い、ＥＣＵ３の記憶部にＥＣＵ秘密鍵及びＥＣＵ公開鍵を書き込む。

【００４１】

またＥＣＵ製造会社５は、署名生成装置６から取得した電子署名付きのＥＣＵ公開鍵と、これと対になるＥＣＵ秘密鍵が書き込まれたＥＣＵ３のＩＤなどの情報とをＱＲコード（可視化情報）３Ｂに変換する。なおＥＣＵ３のＩＤは、例えば製造番号などのＥＣＵ３に対して一意的に付される識別情報である。ＥＣＵ製造会社５は、ＥＣＵ３の製造工程などにおいて印刷装置５ｂを用い、ＥＣＵ３が収容される箱３Ａの表面などにＱＲコード３Ｂを印刷する。その後、製造されたＥＣＵ３は箱３Ａに収められて出荷される。

【００４２】

出荷されたＥＣＵ３は、例えば車両１の製造工程において車両１に取り付けられるか、又は、例えば故障による交換などで車両１のディーラ若しくは修理工場等において車両１に取り付けられる。いずれの場合であっても、ＥＣＵ３を車両１に取り付ける作業者は、ＥＣＵ３の車両１の取り付けに先立って、ＥＣＵ３を収容した箱３Ａに印刷されたＱＲコード３ｂの読み取りを画像読取装置７にて行う。画像読取装置７は、読み取ったＱＲコード３Ｂをデジタルデータに変換し、ＥＣＵ３のＥＣＵ公開鍵、このＥＣＵ公開鍵に付された電子署名、及び、このＥＣＵ公開鍵を記憶しているＥＣＵ３のＩＤ等の情報を取得する。画像読取装置７は、通信ケーブル７ａなどを介してゲートウェイ２に着脱可能に接続することができ、ＱＲコード３Ｂを変換して得られたＥＣＵ公開鍵、電子署名及びＩＤ等の情報をゲートウェイ２に与える。ゲートウェイ２は、自身が予め記憶している署名検証鍵を用いてＥＣＵ公開鍵に付された電子署名が正当なものであるか否かを判定することにより、画像読取装置７から与えられたＥＣＵ公開鍵が正当なものであるか否かを判定する。ＥＣＵ公開鍵が正当なものである場合、ゲートウェイ２は、ＥＣＵ公開鍵及び電子署名をＥＣＵ３のＩＤと対応付けて記憶する。

【００４３】

その後、ＥＣＵ３が車両１の通信線１ａに接続された場合に、このＥＣＵ３とゲートウェイ２との間で所定の手順で処理が行われ、最終的にゲートウェイ２からＥＣＵ３へセッション鍵が与えられる。図２は、セッション鍵を授受するためにゲートウェイ２及びＥＣＵ３の間で行われる処理を説明するための模式図である。車両１の通信線１ａに接続されたＥＣＵ３は、通信線１ａを介して自身のＩＤをゲートウェイ２へ送信する。なおこのときにＥＣＵ３はセッション鍵を有しておらず、ＥＣＵ３及びゲートウェイ２の間で行われるメッセージの送受信にはメッセージ認証子が付されていないため、ゲートウェイ２はＥＣＵ３がセッション鍵を保有するまでの間はメッセージ認証子なしの通信をこのＥＣＵ３との間で行うことを認めるものとする。

【００４４】

ＥＣＵ３からＩＤを通知されたゲートウェイ２は、このＩＤに対応するＥＣＵ公開鍵を読み出し、読み出したＥＣＵ公開鍵を用いて、自身が記憶しているＧＷ公開鍵を暗号化する。ゲートウェイ２は、暗号化したＧＷ公開鍵をＥＣＵ３へ送信する。暗号化されたＧＷ公開鍵を受信したＥＣＵ３は、自身が記憶しているＥＣＵ秘密鍵を用いてＧＷ公開鍵を復号する。ＥＣＵ３は、復号したＧＷ公開鍵を用いて、自身が記憶しているＥＣＵ公開鍵を暗号化する。ＥＣＵ３は、暗号化したＥＣＵ公開鍵をゲートウェイ２へ送信する。暗号化されたＥＣＵ公開鍵を受信したゲートウェイ２は、自身が記憶しているＧＷ秘密鍵を用いて、ＥＣＵ公開鍵を復号する。

【００４５】

これらによりゲートウェイ２は、ＱＲコード３Ｂを画像読取装置７にて読み取って取得したＥＣＵ公開鍵と、通信線１ａに接続されたＥＣＵ３から通信により取得したＥＣＵ公開鍵とを有することとなる。ゲートウェイ２は２つのＥＣＵ公開鍵が一致するか否かを判定することにより、取得したＥＣＵ公開鍵が正当なものであるか否かを判定する。２つのＥＣＵ公開鍵が一致する場合、ゲートウェイ２は、このＥＣＵ公開鍵が正当なものであると判定し、このＥＣＵ公開鍵の送信元のＥＣＵ３が正当な装置であると判定する。

【００４６】

ＥＣＵ３が正当な装置であると判定した場合、ゲートウェイ２は、このＥＣＵ３に対応するＥＣＵ公開鍵を用いて、自身が記憶しているセッション鍵を暗号化する。ゲートウェイ２は、暗号化したセッション鍵をＥＣＵ３へ送信する。暗号化されたセッション鍵を受信したＥＣＵ３は、自身が記憶しているＥＣＵ秘密鍵を用いてセッション鍵を復号する。これによりＥＣＵ３はセッション鍵を取得することができ、以降の通信ではセッション鍵を利用してメッセージ認証子の生成／検証を行うことができる。

【００４７】

＜装置構成＞

図３は、ゲートウェイ２の構成を示すブロック図である。なお図３においては、ゲートウェイ２の機能のうち、ＥＣＵ３の認証機能に関する機能ブロックを抽出して図示し、メッセージの中継機能などの他の機能については機能ブロックの図示を省略してある。本実施の形態に係るゲートウェイ２は、処理部（プロセッサ）２１、記憶部（ストレージ）２２、通信部（トランシーバ）２３及び接続端子（コネクタ）２４等を備えて構成されている。処理部２１は、例えばＣＰＵ（Central Processing Unit）又はＭＰＵ（Micro-Processing Unit）等の演算処理装置を用いて構成されており、記憶部２２に記憶されたプログラムを読み出して実行することにより、種々の演算処理及び制御処理等を行うことができる。例えば処理部２１は、車両１内に設けられた複数の通信線１ａ間で送受信されるメッセージを中継する処理を行う。また本実施の形態において処理部２１は、記憶部２２に記憶された認証処理プログラム２２ａを実行することにより、通信線１ａに新たに接続されたＥＣＵ３の認証に係る処理を行う。

【００４８】

記憶部２２は、例えばフラッシュメモリ又はＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）等の不揮発性のメモリ素子を用いて構成されている。記憶部２２は、処理部２１が実行するプログラム及び処理に必要な各種のデータ等が記憶さ

れている。本実施の形態において記憶部２２は、ＥＣＵ３の認証に係る処理を行う認証処理プログラム２２ａと、このプログラムによる処理に必要なＧＷ秘密鍵２２ｂ、ＧＷ公開鍵２２ｃ、署名検証鍵２２ｄ及びセッション鍵２２ｅとを記憶している。また記憶部２２には、一又は複数のＥＣＵ３についてのＥＣＵ公開鍵を記憶したＥＣＵ公開鍵ＤＢ（データベース）２２ｆが設けられている。

【００４９】

記憶部２２のＧＷ秘密鍵２２ｂ及びＧＷ公開鍵２２ｃは、公開鍵方式での暗号化／復号を行うための一組の鍵であり、ゲートウェイ２毎に異なる値が設定される。署名検証鍵２２ｄは、ＥＣＵ３が有するＥＣＵ公開鍵に付された電子署名の正否を検証する際に用いられる鍵であり、署名生成装置６が使用する署名生成鍵と対になる鍵である。署名検証鍵２２ｄは、複数のゲートウェイ２に同じ値が設定される。ＧＷ秘密鍵２２ｂ、ＧＷ公開鍵２２ｃ及び署名検証鍵２２ｄは、例えばゲートウェイ２の製造工程においてゲートウェイ製造会社４の書込装置４ａにより記憶部２２に書き込まれる。

【００５０】

本実施の形態において、記憶部２２に記憶された署名検証鍵２２ｄは、読み出しのみが許可され、値を書き換えることができない。即ち記憶部２２には、１回のみデータを書き込むことができ、データを書き込んだ後にそのデータを書き換えることができない記憶領域が設けられている。署名検証鍵２２ｄは記憶部２２のこの記憶領域に書き込まれることによって、改変不可能な情報となる。なお署名検証鍵２２ｄは、記憶部２２とは異なるＲＯＭ（Read Only Memory）などの記憶素子に書き込まれてもよい。また署名検証鍵２２ｄ以外の例えばＧＷ秘密鍵２２ｂ及びＧＷ公開鍵２２ｃ等の鍵についても同様に、改変不可能な情報としてもよい。

【００５１】

セッション鍵２２ｅは、車両１内のネットワークにて送受信されるメッセージに付されるメッセージ認証子の生成及び正否判定に用いられる鍵であり、共通鍵方式で暗号化／復号を行うための鍵である。車両１に搭載されたゲートウェイ２及びＥＣＵ３は、同じセッション鍵２２ｅを有している必要がある。セッション鍵２２ｅは、例えばゲートウェイ２の製造工程で記憶部２２に書き込まれる構成であってもよいが、本実施の形態においてはゲートウェイ２が乱数発生などのアルゴリズムを用いて生成するものとする。ゲートウェイ２は、例えば周期的にセッション鍵２２ｅを生成して更新し、更新したセッション鍵２２ｅを車両１内の全てのＥＣＵ３へ送信する処理を行ってもよい。

【００５２】

ＥＣＵ公開鍵ＤＢ２２ｆは、車両１に搭載されたＥＣＵ３のＥＣＵ公開鍵を記憶している。図４は、ＥＣＵ公開鍵ＤＢ２２ｆの一構成例を示す模式図である。記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆには、ＥＣＵ３に対して一意に付されるＩＤと、ＥＣＵ３のＥＣＵ公開鍵と、このＥＣＵ公開鍵の正当性を証明する電子署名とが対応付けて記憶されている。ゲートウェイ２は、ＥＣＵ３が収められた箱３ＡのＱＲコード３Ｂから画像読取装置７にて読み取った情報を取得し、取得した情報に含まれるＥＣＵ公開鍵が正当なものであるか否かを電子署名に基づいて判定し、正当であると判定した場合にこれらの情報をＥＣＵ公開鍵ＤＢ２２ｆに登録する。なお本実施の形態においてはＥＣＵ公開鍵の電子署名を記憶しておく構成としているが、これに限るものではなく、ＥＣＵ公開鍵が正当なものであると電子署名に基づいて判定した後は、この電子署名を破棄してもよい。

【００５３】

ゲートウェイ２の通信部２３は、通信線１ａを介して他の装置との間でメッセージを送受信する処理を行う。通信部２３は、例えばＣＡＮ（Controller Area Network）又はイーサネット（登録商標）等の通信プロトコルに従って、メッセージの送受信を行う。通信部２３は、処理部２１から与えられた送信用のメッセージを電気信号に変換して通信線１ａへ出力することによりメッセージの送信を行う。通信部２３は、通信線１ａ上の電気信号をサンプリングして取得することによりメッセージを受信し、受信したメッセージを処理部２１へ与える。またゲートウェイ２は、複数の通信部２３を備えており、一の通信部

２３にて受信したメッセージを他の通信部２３から送信するメッセージの中継を行っている。なおメッセージに付されるメッセージ認証子に基づいた正否判定は、通信部２３ではなく、処理部２１にて行われる。

【００５４】

接続端子２４は、通信ケーブル７ａを着脱可能に接続することができる端子であり、例えばＯＢＤ（On Board Diagnostics）又はＵＳＢ（Universal Serial Bus）等の規格による端子を採用することができる。本実施の形態においては、接続端子２４に通信ケーブル７ａを介して画像読取装置７を接続することができる。ゲートウェイ２は、接続端子２４に接続された画像読取装置７から、ＥＣＵ３の箱３Ａに印刷されたＱＲコード３Ｂを読み取ったデータを取得することができる。

【００５５】

また本実施の形態に係るゲートウェイ２の処理部２１には、記憶部２２に記憶された認証処理プログラム２２ａを実行することによって、ＥＣＵ公開鍵取得部２１ａ、署名検証部２１ｂ、識別情報受信部２１ｃ、ＧＷ公開鍵暗号化部２１ｄ、ＧＷ公開鍵送信部２１ｅ、ＥＣＵ公開鍵受信部２１ｆ、ＥＣＵ公開鍵復号部２１ｇ、ＥＣＵ公開鍵判定部２１ｈ、セッション鍵暗号化部２１ｉ及びセッション鍵送信部２１ｊ等がソフトウェア的な機能ブロックとして実現される。

【００５６】

ＥＣＵ公開鍵取得部２１ａは、接続端子２４に通信ケーブル７ａを介して接続された画像読取装置７から、ＥＣＵ３の箱３Ａに印刷されたＱＲコード３Ｂを読み取ったデータを取得することにより、このＥＣＵ３のＥＣＵ公開鍵をＩＤ及び電子署名等の情報と共に取得する処理を行う。署名検証部２１ｂは、ＥＣＵ公開鍵取得部２１ａが取得したＥＣＵ公開鍵に付された電子署名の正否を検証することにより、ＥＣＵ公開鍵の正否を検証する処理を行う。例えば署名検証部２１ｂは、記憶部２２に記憶した署名検証鍵２２ｄを用いて電子署名を復号し、復号して得られたデータがＥＣＵ公開鍵の一部又は全部と一致するか否かに応じて、電子署名の正否を判定する構成とすることができる。署名検証鍵２２ｄは、正当な電子署名が付されていると判断したＥＣＵ公開鍵を、記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆに登録する。

【００５７】

識別情報受信部２１ｃは、車両１の通信線１ａに新たなＥＣＵ３が接続された場合に、この新たなＥＣＵ３から送信される認証要求と、この認証要求と共に送信されるＥＣＵ３のＩＤとを、通信部２３にて受信する処理を行う。ＧＷ公開鍵暗号化部２１ｄは、識別情報受信部２１ｃがＥＣＵ３からの認証要求及びＩＤを受信した場合に、受信したＩＤに対応付けられたＥＣＵ公開鍵を記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆから読み出し、読み出したＥＣＵ公開鍵を用いて、記憶部２２に記憶されたＧＷ公開鍵２２ｃを暗号化する。ＧＷ公開鍵送信部２１ｅは、ＧＷ公開鍵暗号化部２１ｄが暗号化したＧＷ公開鍵２２ｃを、認証要求を送信したＥＣＵ３（が接続された通信線１ａ）へ送信する。

【００５８】

ＥＣＵ公開鍵受信部２１ｆは、ＧＷ公開鍵送信部２１ｅによるＧＷ公開鍵２２ｃの送信に応じてＥＣＵ３から送信されるＥＣＵ３のＥＣＵ公開鍵を通信部２３にて受信する。受信したＥＣＵ公開鍵は、ＧＷ公開鍵を用いて暗号化されているため、ＥＣＵ公開鍵復号部２１ｇは、記憶部２２からＧＷ秘密鍵２２ｂを読み出し、読み出したＧＷ秘密鍵２２ｂを用いて、ＥＣＵ３から受信したＥＣＵ公開鍵を復号する。ＥＣＵ公開鍵判定部２１ｈは、ＥＣＵ公開鍵復号部２１ｇが復号したＥＣＵ公開鍵と、ＥＣＵ公開鍵取得部２１ａが取得してＥＣＵ公開鍵ＤＢ２２ｆに登録したＥＣＵ公開鍵とを比較し、両ＥＣＵ公開鍵が一致するか否かを判定することにより、新たなＥＣＵ３から受信したＥＣＵ公開鍵が正当なものであるか否かを判定する。ＥＣＵ公開鍵判定部２１ｈが、ＥＣＵ公開鍵が正当なものであると判定した場合、ゲートウェイ２は、このＥＣＵ公開鍵の送信元のＥＣＵ３が正当な装置であると判定する（即ち、このＥＣＵ３を認証する）。

【００５９】

セッション鍵暗号化部２１ｉは、ＥＣＵ公開鍵判定部２１ｈが正当と判定したＥＣＵ公開鍵を用いて、記憶部２２に記憶されたセッション鍵２２ｅを暗号化する。セッション鍵送信部２１ｊは、セッション鍵暗号化部２１ｉが暗号化したセッション鍵２２ｅを、正当な装置と判定したＥＣＵ３へ送信する。これにより車両１の通信線１ａに新たに接続されたＥＣＵ３は、車両１内の通信に用いるセッション鍵２２ｅを取得することができ、以降の通信はセッション鍵２２ｅを用いて生成したメッセージ認証子を送信メッセージに付すことが可能となる。

【００６０】

図５は、ＥＣＵ３の構成を示すブロック図である。なお図５においては、車両１に搭載される複数のＥＣＵ３が有する機能のうち、ＥＣＵ３の認証機能に関する共通の機能ブロックを抽出した図示し、各ＥＣＵ３に個別の制御処理などの機能については機能ブロックの図示を省略してある。本実施の形態に係るＥＣＵ３は、処理部（プロセッサ）３１、記憶部（ストレージ）３２及び通信部（トランシーバ）３３等を備えて構成されている。処理部３１は、例えばＣＰＵ又はＭＰＵ等の演算処理装置を用いて構成されており、記憶部３２に記憶されたプログラムを読み出して実行することにより、種々の演算処理及び制御処理等を行うことができる。本実施の形態において処理部３１は、記憶部３２に記憶された認証処理プログラム３２ａを実行することにより、ゲートウェイ２との間でＥＣＵ３の認証に係る処理を行う。

【００６１】

記憶部３２は、例えばフラッシュメモリ又はＥＥＰＲＯＭ等の不揮発性のメモリ素子を用いて構成されている。記憶部３２は、処理部３１が実行するプログラム及び処理に必要な各種のデータ等が記憶されている。本実施の形態において記憶部３２は、ＥＣＵ３の認証に係る処理を行う認証処理プログラム３２ａと、このプログラムによる処理に必要なＥＣＵ秘密鍵３２ｂ、ＥＣＵ公開鍵３２ｃ及びセッション鍵３２ｄとを記憶している。記憶部３２のＥＣＵ秘密鍵３２ｂ及びＥＣＵ公開鍵３２ｃは、公開鍵方式で暗号化／復号を行うための一組の鍵であり、ＥＣＵ３毎に異なる値が設定される。ＥＣＵ秘密鍵３２ｂ及びＥＣＵ公開鍵３２ｃは、例えばＥＣＵ３の製造工程においてＥＣＵ製造会社５の書込装置５ａにより記憶部３２に書き込まれる。

【００６２】

セッション鍵３２ｄは、車両１内のネットワークにて送受信されるメッセージに付されるメッセージ認証子の生成及び正否判定に用いられる鍵であり、共通鍵方式で暗号化／復号を行うための鍵である。車両１に搭載されたゲートウェイ２及びＥＣＵ３は、同じセッション鍵を有している必要がある。セッション鍵３２ｄは、ＥＣＵ３の製造工程で書き込まれることはなく、ＥＣＵ３が車両１に搭載された後にゲートウェイ２から送信されたものを受信し、受信したセッション鍵３２ｄが記憶部３２に書き込まれる。

【００６３】

通信部３３は、通信線１ａを介して他の装置との間でメッセージを送受信する処理を行う。通信部３３は、例えばＣＡＮ又はイーサネット等の通信プロトコルに従って、メッセージの送受信を行う。通信部３３は、処理部３１から与えられた送信用のメッセージを電気信号に変換して通信線１ａへ出力することによりメッセージの送信を行う。通信部３３は、通信線１ａ上の電気信号をサンプリングして取得することによりメッセージを受信し、受信したメッセージを処理部３１へ与える。なおメッセージに付されるメッセージ認証子に基づいた正否判定は、通信部３３ではなく、処理部３１にて行われる。

【００６４】

また本実施の形態に係るＥＣＵ３の処理部３１には、記憶部３２に記憶された認証処理プログラム３２ａを実行することによって、識別情報送信部３１ａ、ＧＷ公開鍵受信部３１ｂ、ＧＷ公開鍵復号部３１ｃ、ＥＣＵ公開鍵暗号化部３１ｄ、ＥＣＵ公開鍵送信部３１ｅ、セッション鍵受信部３１ｆ及びセッション鍵復号部３１ｇ等がソフトウェア的な機能ブロックとして実現される。識別情報送信部３１ａは、ＥＣＵ３が車両１の通信線１ａに対して新たに接続された場合に、この車両１に搭載されたゲートウェイ２に対して認証要

求と共に自装置のＩＤを送信する処理を行う。識別情報送信部３１ａは、例えばＥＣＵ３の起動後に記憶部３２がセッション鍵３２ｄを記憶していない場合に、ゲートウェイ２に対して認証要求及びＩＤを自動的に送信してもよく、また例えばＥＣＵ３を車両１に搭載する作業を行った作業者の操作に応じて認証要求及びＩＤを送信してもよい。

【００６５】

ＧＷ公開鍵受信部３１ｂは、識別情報送信部３１ａが送信した認証要求及びＩＤに応じてゲートウェイ２が送信するＧＷ公開鍵を通信部３３にて受信する処理を行う。なおこのＧＷ公開鍵は、ＥＣＵ３のＥＣＵ公開鍵にて暗号化されている。ＧＷ公開鍵復号部３１ｃは、ＧＷ公開鍵受信部３１ｂが受信したＧＷ公開鍵を、記憶部３２に記憶されたＥＣＵ秘密鍵３２ｂを用いて復号する。ＥＣＵ公開鍵暗号化部３１ｄは、ＧＷ公開鍵復号部３１ｃが復号したＧＷ公開鍵を用いて、記憶部３２に記憶されたＥＣＵ公開鍵３２ｃを暗号化する。ＥＣＵ公開鍵送信部３１ｅは、ＥＣＵ公開鍵暗号化部３１ｄが暗号化したＥＣＵ公開鍵３２ｃを、通信部３３にてゲートウェイ２へ送信する。

【００６６】

ＥＣＵ３からＥＣＵ公開鍵を受信したゲートウェイ２は、受信したＥＣＵ公開鍵が正当なものであると判定し、ＥＣＵ３が正当な装置であると判定した場合に、自身が記憶しているセッション鍵をＥＣＵ３へ送信する。ＥＣＵ３のセッション鍵受信部３１ｆは、ゲートウェイ２から送信されたセッション鍵を通信部３３にて受信する。このセッション鍵はゲートウェイ２によりＥＣＵ公開鍵を用いて暗号化されているため、セッション鍵復号部３１ｇは、記憶部３２に記憶されたＥＣＵ秘密鍵３２ｂを用いてセッション鍵を復号し、復号したセッション鍵３２ｄを記憶部３２に記憶する。これにより車両１の通信線１ａに新たに接続されたＥＣＵ３は、車両１内の通信に用いるセッション鍵３２ｄを記憶部３２に記憶することができ、以降の通信では記憶部３２に記憶したセッション鍵３２ｄを用いて生成したメッセージ認証子を送信メッセージに付すことが可能となり、メッセージ認証子が付されたメッセージを受信することが可能となる。

【００６７】

図６は、署名生成装置６の構成を示すブロック図である。本実施の形態に係る署名生成装置６は、例えば車両１の製造会社又は販売会社等が管理運営するサーバ装置として実現される。ただし署名生成装置６は、署名生成のサービスを提供する会社、ゲートウェイ２の製造会社又はＥＣＵ３の製造会社等が管理運営する装置であってもよい。また署名生成装置６は、汎用のコンピュータに署名生成プログラム６２ａをインストールすることによって実現される。署名生成プログラム６２ａは、例えば光ディスク又はメモリカード等の記録媒体６５に記録されて提供され、コンピュータにより記録媒体６５から読み出されてハードディスクなどにインストールされる。

【００６８】

本実施の形態に係る署名生成装置６は、処理部６１、記憶部６２及び通信部６３等を備えて構成されている。処理部６１は、ＣＰＵ又はＭＰＵ等の演算処理装置を用いて構成されており、記憶部６２に記憶されたプログラムを読み出して実行することにより、種々の演算処理を行うことができる。本実施の形態において処理部６１は、記憶部６２に記憶された署名生成プログラム６２ａを実行することにより、与えられたデータの正当性を証明するための電子署名を生成する処理を行う。

【００６９】

記憶部６２は、例えばハードディスクなどの大容量の記憶装置を用いて構成されている。記憶部６２は、処理部６１が実行するプログラム及び処理に必要な各種のデータ等が記憶されている。本実施の形態において記憶部６２は、電子署名の生成に係る処理を行う署名生成プログラム６２ａと、このプログラムによる処理に必要な署名生成鍵６２ｂとを記憶している。署名生成鍵６２ｂは、ゲートウェイ２が記憶している署名検証鍵２２ｄと対になる鍵であり、電子署名を生成するために所定のデータを暗号化する際に用いられる鍵である。

【００７０】

通信部６３は、例えばインターネットなどの広域ネットワークを介して他の装置との間でメッセージを送受信する処理を行う。本実施の形態において通信部６３は、例えばゲートウェイ製造会社に設置された通信装置、及び、ＥＣＵ製造会社５に設置された通信装置との間で、例えばイーサネットの通信プロトコルによるメッセージの送受信を行う。通信部６３は、処理部６１から与えられた送信用のメッセージを他の装置へ送信すると共に、他の装置から受信したメッセージを処理部６１へ与える。本実施の形態において署名生成装置６は、ゲートウェイ製造会社４の通信装置に対して、ゲートウェイ２が記憶する署名検証鍵２２ｄを送信してもよい。また署名生成装置６は、ＥＣＵ製造会社５から署名生成依頼と共にＥＣＵ公開鍵を受信し、受信したＥＣＵ公開鍵の正当性を証明する電子署名を生成してＥＣＵ製造会社５へ送信する。

【００７１】

また本実施の形態に係る署名生成装置６の処理部６１には、記憶部６２に記憶された署名生成プログラム６２ａを実行することによって、ＥＣＵ公開鍵受信部６１ａ、署名生成部６１ｂ及び署名送信部６１ｃ等がソフトウェア的な機能ブロックとして実現される。ＥＣＵ公開鍵受信部６１ａは、ＥＣＵ製造会社５の通信装置などから送信される署名生成依頼及びＥＣＵ公開鍵を通信部６３にて受信する処理を行う。署名生成部６１ｂは、署名作成を依頼されたＥＣＵ公開鍵について、記憶部６２の署名生成鍵６２ｂを用いて電子署名を生成する。署名送信部６１ｃは、署名生成部６１ｂが生成した電子署名を含む情報を、署名作成依頼及びＥＣＵ公開鍵の送信元であるＥＣＵ製造会社５の通信装置へ送信する処理を行う。

【００７２】

なお署名生成装置６が行う署名生成鍵６２ｂを用いた署名生成処理については、既存の技術であるため、詳細な説明を省略する。またゲートウェイ２が行う署名検証鍵２２ｄを用いた署名検証処理については、既存の技術であるため、詳細な説明を省略する。同様に、秘密鍵及び公開鍵を用いた情報の暗号化及び復号の詳細な手順、共通鍵（セッション鍵）を用いた情報の暗号化及び復号の手順、並びに、セッション鍵によるメッセージ認証子を用いた通信の手順等については、既存の技術であるため、詳細な説明を省略する。

【００７３】

図７は、画像読取装置７の構成を示すブロック図である。本実施の形態に係る画像読取装置７は、例えば車両１のディーラ又は修理工場等に設けられ、車両１の整備又は修理等を行う作業者が持ち運ぶことが可能な大きさ及び形状の装置である。なお画像読取装置７は、例えばＥＣＵ３の取り付けなど車両１の整備及び修理等を行うための専用の装置であってよく、また例えば汎用のパーソナルコンピューター又はタブレット型端末装置等に画像読取及び車両１との通信を行う機能を有するプログラムをインストールした装置であってもよい。

【００７４】

本実施の形態に係る画像読取装置７は、処理部７１、記憶部７２、カメラ７３及び接続端子７４等を備えて構成されている。処理部７１は、ＣＰＵ又はＭＰＵ等の演算処理装置を用いて構成されており、記憶部７２に記憶されたプログラムを読み出して実行することにより、種々の演算処理を行うことができる。本実施の形態において処理部７１は、記憶部７２に記憶された変換プログラム７２ａを実行することにより、ＱＲコード３Ｂを読み取って情報に変換する処理を行う。

【００７５】

記憶部７２は、例えばフラッシュメモリ又はＥＥＰＲＯＭ等の不揮発性のメモリ素子を用いて構成されている。記憶部７２は、処理部７１が実行するプログラム及び処理に必要な各種のデータ等が記憶されている。本実施の形態において記憶部７２は、ＥＣＵ７の箱３Ａに印刷されたＱＲコード３Ｂを読み取って情報に変換する処理を行う変換プログラム７２ａと、このプログラムによる処理に必要な情報とを記憶している。

【００７６】

カメラ７３は、ＥＣＵ３の箱３Ａに印刷されたＱＲコード３Ｂを撮影するためのカメラ

である。カメラ７３は、例えば画像読取装置７の適所に設けられた撮影ボタンに対するユーザの操作に応じて撮影を行い、撮影により得られた画像を処理部７１へ与える。接続端子７４は、通信ケーブル７ａを着脱可能に接続することができる端子であり、例えばＯＢＤ又はＵＳＢ等の規格による端子を採用することができる。本実施の形態においては、接続端子７４に通信ケーブル７ａの一端を接続し、通信ケーブル７ａの他端をゲートウェイ２に接続することによって、ゲートウェイ２及び画像読取装置７が通信可能となる。

【００７７】

また本実施の形態に係る画像読取装置７の処理部７１には、記憶部７２に記憶された変換プログラム７２ａを実行することによって、変換処理部７１ａ等がソフトウェア的な機能ブロックとして実現される。変換処理部７１ａは、カメラ７３が撮影した画像からＱＲコード３Ｂを抽出し、抽出したＱＲコード３Ｂをデジタルデータ、本実施の形態においてはＥＣＵ３のＩＤ、ＥＣＵ公開鍵及び電子署名等のデータに変換する処理を行う。なおＱＲコード３Ｂからデジタルデータへの変換処理は、既存の技術であるため、詳細な説明を省略する。変換処理部７１ａにより変換されたデータは、接続端子７４に通信ケーブル７ａを介して接続されているゲートウェイ２へ送信される。

【００７８】

＜ＥＣＵの製造方法＞

次に、ＥＣＵ製造会社５にて行われるＥＣＵ３の製造方法について説明する。図８は、ＥＣＵ製造会社５によるＥＣＵ３の製造方法を説明するためのフローチャートである。ＥＣＵ製造会社５では、まず、製造するＥＣＵ３毎にＥＣＵ秘密鍵及びＥＣＵ公開鍵を生成する（ステップＳ１）。ＥＣＵ３毎のＥＣＵ秘密鍵及びＥＣＵ公開鍵は、例えばＥＣＵ製造会社５に設けられたコンピュータなどによって生成される。次いでＥＣＵ製造会社５では、コンピュータがインターネットなどのネットワークを介して署名生成装置６と通信を行い、ステップＳ１にて生成したＥＣＵ公開鍵に対する電子署名の生成依頼を行う（ステップＳ２）。この生成依頼に応じて署名生成装置６にてＥＣＵ公開鍵の電子署名が生成され、署名生成装置６から生成した電子署名が送信される。ＥＣＵ製造会社５のコンピュータは、署名生成装置６からの電子署名を受信して取得する（ステップＳ３）。

【００７９】

またＥＣＵ製造会社５では、書込装置５ａが、ステップＳ１にて生成したＥＣＵ秘密鍵及びＥＣＵ公開鍵を、ＥＣＵ３の記憶部３２に書き込む（ステップＳ４）。このときに書き込まれるＥＣＵ秘密鍵及びＥＣＵ公開鍵は、ＥＣＵ３毎に異なる値である。なおステップＳ４の処理は、ステップＳ２及びＳ３より先に行われてもよく、並行して行われてもよい。

【００８０】

ＥＣＵ製造会社５のコンピュータは、ステップＳ２にて署名生成装置６から取得した電子署名と、ＥＣＵ公開鍵及びこのＥＣＵ公開鍵が書き込まれたＥＣＵ３のＩＤとを含む情報を元にＱＲコード３Ｂを生成する（ステップＳ５）。次いでＥＣＵ製造会社５の印刷装置５ｂは、ステップＳ５にて生成したＱＲコード３Ｂを、ＥＣＵ３を収容する箱３Ａの所定箇所に印刷する（ステップＳ６）。その後、ＥＣＵ製造会社５の搬送装置などが、ステップＳ４にて記憶部３２にＥＣＵ秘密鍵及びＥＣＵ公開鍵が書き込まれたＥＣＵ３を、ステップＳ６にてＱＲコード３Ｂが印刷された箱３Ａ内に収容し（ステップＳ７）、ＥＣＵ３の製造が完了する。なおステップＳ７にてＥＣＵ３を箱３Ａ内に収容する際には、ＥＣＵ３の記憶部３２に記憶された公開鍵と、箱３Ａに印刷されたＱＲコード３Ｂに含まれるＥＣＵ公開鍵とが一致するように、ＥＣＵ３及び箱３Ａを組み合わせる必要がある。

【００８１】

＜ＥＣＵの車両への取り付け＞

図９は、ＥＣＵ３の車両１への取り付け方法を説明するためのフローチャートである。製造されたＥＣＵ３は、車両１の製造会社、ディーラ又は整備工場等にて車両１に取り付けられる。このときにＥＣＵ３の取り付けを行う作業者は、まず画像読取装置７を用いて、ＥＣＵ３が収容された箱３Ａに印刷されたＱＲコード３Ｂの読取作業を行う必要がある

。画像読取装置７は、作業者による撮影操作などに応じて、箱３Ａに印刷されたＱＲコード３Ｂのカメラ７３による撮影画像を取得する（ステップＳ１１）。次いで画像読取装置７は、カメラ７３にて取得した撮影画像に写されたＱＲコード３Ｂをデジタルデータに変換する処理を行う（ステップＳ１２）。

【００８２】

その後、画像読取装置７は、ステップＳ１２にて変換したデジタルデータに含まれるＥＣＵ３のＩＤ、ＥＣＵ公開鍵及び電子署名等の情報を、通信ケーブル７ａを介して接続されたゲートウェイ２へ送信し（ステップＳ１３）、処理を終了する。なおステップＳ１３を行う前に、作業者は車両１のゲートウェイ２と画像読取装置７とを通信ケーブル７ａにて接続する作業を行っておく必要がある。また通信ケーブル７ａを介して接続されたゲートウェイ２及び画像読取装置７が情報の送受信を開始する前に、例えば画像読取装置７を操作する作業者に対してパスワード等の入力を求めるなど、画像読取装置７又は作業者等が正当な権限を有するものであるか否かを確認する処理を行ってもよい。

【００８３】

図１０は、ゲートウェイ２が行うＥＣＵ公開鍵の取得処理の手順を示すフローチャートである。通信ケーブル７ａを介して画像読取装置７が接続されたゲートウェイ２の処理部２１のＥＣＵ公開鍵取得部２１ａは、画像読取装置７から送信されるＥＣＵ３のＩＤ、ＥＣＵ公開鍵及び電子署名等の情報を取得する（ステップＳ２１）。次いで処理部２１の署名検証部２１ｂは、記憶部２２に記憶された署名検証鍵２２ｄを読み出す（ステップＳ２２）。署名検証部２１ｂは、ステップＳ２１にて取得したＥＣＵ公開鍵及び電子署名と、ステップＳ２２にて読み出した署名検証鍵２２ｄとを用いて署名検証処理を行う（ステップＳ２３）。署名検証部２１ｂは、署名検証処理の結果から、ステップＳ２１にて取得した電子署名が正しい電子署名であるか否かを判定する（ステップＳ２４）。電子署名が正しいものである場合（Ｓ２４：ＹＥＳ）、署名検証部２１ｂは、ステップＳ２１にて取得したＥＣＵ３のＩＤ、ＥＣＵ公開鍵及び電子署名等の情報を、記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆに登録して（ステップＳ２５）、処理を終了する。電子署名が正しいものではない場合（Ｓ２４：ＮＯ）、署名検証部２１ｂは、ＩＤ、ＥＣＵ公開鍵及び電子署名等の情報を登録せずに、処理を終了する。

【００８４】

図１１は、ＥＣＵ３が行う認証処理の手順を示すフローチャートである。ＥＣＵ３の処理部３１の識別情報送信部３１ａは、ＥＣＵ３が車両１内の通信線１ａに接続され、例えば作業者により所定の操作がなされた場合に、ゲートウェイ２に対して認証要求及び自身のＩＤを送信する（ステップＳ３１）。その後、処理部３１のＧＷ公開鍵受信部３１ｂは、ゲートウェイ２から送信されるＧＷ公開鍵を通信部３３にて受信したか否かを判定する（ステップＳ３２）。ＧＷ公開鍵を受信していない場合（Ｓ３２：ＮＯ）、ＧＷ公開鍵受信部３１ｂは、ＧＷ公開鍵を受信するまで待機する。

【００８５】

ゲートウェイ２からＧＷ公開鍵を受信した場合（Ｓ３２：ＹＥＳ）、処理部３１のＧＷ公開鍵復号部３１ｃは、記憶部３２に記憶されたＥＣＵ秘密鍵３２ｂを用いて、受信したＧＷ公開鍵を復号する（ステップＳ３３）。ＧＷ公開鍵復号部３１ｃは、復号したＧＷ公開鍵を記憶部３２に記憶する（ステップＳ３４）。次いで処理部３１のＥＣＵ公開鍵暗号化部３１ｄは、記憶部３２に記憶されたＥＣＵ公開鍵３２ｃを、記憶部３２に記憶されたＧＷ公開鍵を用いて暗号化する（ステップＳ３５）。処理部３１のＥＣＵ公開鍵送信部３１ｅは、ステップＳ３５にて暗号化されたＥＣＵ公開鍵を、通信部３３にてゲートウェイ２へ送信する（ステップＳ３６）。

【００８６】

次いで処理部３１のセッション鍵受信部３１ｆは、ゲートウェイ２から送信されるセッション鍵を通信部３３にて受信したか否かを判定する（ステップＳ３７）。セッション鍵を受信していない場合（Ｓ３７：ＮＯ）、セッション鍵受信部３１ｆは、セッション鍵を受信するまで待機する。ゲートウェイ２からセッション鍵を受信した場合（Ｓ３７：ＹＥ

Ｓ）、処理部３１のセッション鍵復号部３１ｇは、記憶部３２に記憶されたＧＷ公開鍵を用いて、ステップＳ３７にて受信したセッション鍵を復号する（ステップＳ３８）。セッション鍵復号部３１ｇは、復号したセッション鍵を記憶部３２に記憶し（ステップＳ３９）、処理を終了する。

【００８７】

図１２は、ゲートウェイ２が行う認証処理の手順を示すフローチャートである。ゲートウェイ２の処理部２１の識別情報受信部２１ｃは、ＥＣＵ３が送信する認証要求及びＩＤを受信したか否かを判定する（ステップＳ５１）。認証要求及びＩＤを受信していない場合（Ｓ５１：ＮＯ）、識別情報受信部２１ｃは、認証要求及びＩＤを受信するまで待機する。ＥＣＵ３からの認証要求及びＩＤを受信した場合（Ｓ５１：ＹＥＳ）、処理部２１のＧＷ公開鍵暗号化部２１ｄは、受信したＩＤに対応するＥＣＵ公開鍵を、記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆから読み出す（ステップＳ５２）。ＧＷ公開鍵暗号化部２１ｄは、記憶部２２に記憶されたＧＷ公開鍵を、ステップＳ５２にて読み出したＥＣＵ公開鍵を用いて暗号化する（ステップＳ５３）。処理部２１のＧＷ公開鍵送信部２１ｅは、ステップＳ５３にて暗号化したＥＣＵ公開鍵を、通信部２３にて認証要求送信元のＥＣＵ３へ送信する（ステップＳ５４）。

【００８８】

次いで処理部２１のＥＣＵ公開鍵受信部２１ｆは、ＥＣＵ３から送信されるＥＣＵ公開鍵を受信したか否かを判定する（ステップＳ５５）。ＥＣＵ公開鍵を受信していない場合（Ｓ５５：ＮＯ）、ＥＣＵ公開鍵受信部２１ｆは、ＥＣＵ公開鍵を受信するまで待機する。ＥＣＵ３からＥＣＵ公開鍵を受信した場合（Ｓ５５：ＹＥＳ）、処理部２１のＥＣＵ公開鍵復号部２１ｇは、記憶部２２に記憶されたＧＷ秘密鍵２２ｂを用いて、ステップＳ５５にて受信したＥＣＵ公開鍵を復号する（ステップＳ５６）。処理部２１のＥＣＵ公開鍵判定部２１ｈは、ステップＳ５６にて復号したＥＣＵ公開鍵が、ステップＳ５２にて読み出したＥＣＵ公開鍵と一致するか否かを判定することにより、ステップＳ５６にて復号したＥＣＵ公開鍵が正しいものであるか否かを判定する（ステップＳ５７）。

【００８９】

ＥＣＵ公開鍵が正しいものである場合（Ｓ５７：ＹＥＳ）、処理部２１のセッション鍵暗号化部２１ｉは、記憶部２２に記憶されたセッション鍵を読み出して暗号化する（ステップＳ５８）。処理部２１のセッション鍵送信部２１ｊは、ステップＳ５８にて暗号化されたセッション鍵を、通信部２３にてＥＣＵ３へ送信し（ステップＳ５９）、処理を終了する。ＥＣＵ公開鍵が正しいものでない場合（Ｓ５７：ＮＯ）、処理部２１はセッション鍵の暗号化及び送信を行うことなく、処理を終了する。

【００９０】

＜まとめ＞

以上の構成の本実施の形態に係る車載認証システムは、車両１内のネットワーク（通信線１ａ）に新たに接続されたＥＣＵ３を、車両１に搭載されたゲートウェイ２が認証する（即ち、ＥＣＵ３が正当な装置であるか否かを判断する）。ＥＣＵ３は、ＥＣＵ秘密鍵及びＥＣＵ公開鍵を記憶部３２に記憶しておく。ゲートウェイ２は、ＧＷ秘密鍵及びＧＷ公開鍵と、電子署名の正否を検証するための署名検証鍵とを記憶部２２に記憶しておく。ＥＣＵ３及びゲートウェイ２は、共通の鍵情報を予め記憶しておく必要がないため、これらの鍵情報は例えば各装置の製造段階などにて予め記憶させておくことができ、ＥＣＵ３を車両１に取り付ける際に鍵情報を書き込む作業が不要となる。

【００９１】

まずゲートウェイ２は、車両１内のネットワークに対して新たに接続されるＥＣＵ３のＥＣＵ公開鍵を取得する。このときのゲートウェイ２によるＥＣＵ公開鍵の取得はどのような方法が採用されてもよいが、本実施の形態においてはＥＣＵ３を収容する箱３Ａに印刷されたＱＲコード３Ｂを画像読取装置７にて読み取ることによってゲートウェイ２がＥＣＵ公開鍵を取得する方法を採用する。ＥＣＵ公開鍵を取得したゲートウェイ２は、ＥＣＵ公開鍵に付された電子署名の正否を、記憶部２２に記憶した署名検証鍵を用いて検証し

、正当なＥＣＵ公開鍵を記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆに記憶しておく。
【００９２】
ゲートウェイ２は、ＥＣＵ公開鍵ＤＢ２２ｆに記憶したＥＣＵ公開鍵を用いて、記憶部２２に記憶しているＧＷ公開鍵を暗号化し、暗号化したＧＷ公開鍵を新たに接続されたＥＣＵ３へ送信する。このときに送信されるＧＷ公開鍵を復号することができるのは、暗号化に用いたＥＣＵ公開鍵と対になるＥＣＵ秘密鍵を有するＥＣＵ３のみである。ゲートウェイ２から暗号化されたＧＷ公開鍵を受信したＥＣＵ３は、記憶部３２に記憶されたＥＣＵ秘密鍵を用いて受信したＧＷ公開鍵を復号する。ＥＣＵ３は、復号したＧＷ公開鍵を用いて、記憶部３２に記憶されたＥＣＵ公開鍵を暗号化し、暗号化したＥＣＵ公開鍵をゲートウェイ２へ送信する。このときに送信されるＥＣＵ公開鍵を復号できるのは、暗号化に用いたＧＷ公開鍵と対になるＧＷ秘密鍵を有するゲートウェイ２のみである。
【００９３】
ＥＣＵ３から暗号化されたＥＣＵ公開鍵を受信したゲートウェイ２は、記憶部２２に記憶しているＧＷ秘密鍵を用いてＥＣＵ公開鍵を復号し、復号したＥＣＵ公開鍵の正否を判定する。このときにゲートウェイ２は、例えばＥＣＵ３から受信したＥＣＵ公開鍵が、ＱＲコード３Ｂから取得したＥＣＵ公開鍵と一致する場合に、ＥＣＵ３から受信したＥＣＵ公開鍵が正当なものであると判定する。ＥＣＵ公開鍵が正当なものであると判定した場合、ゲートウェイ２は、このＥＣＵ公開鍵の送信元であるＥＣＵ３を正当な装置であると判断する（認証する）。
【００９４】
このように本実施の形態に係る車載認証システムでは、新たに車両１内のネットワークに接続されたＥＣＵ３を認証するために、ゲートウェイ２又はＥＣＵ３が車両１外のサーバ装置などとの通信を行う必要がない。また漏洩を防止すべきＥＣＵ秘密鍵及びＧＷ秘密鍵は、例えば各装置の製造段階などにおいて各装置の記憶部に予め書き込んでおけばよいため、ＥＣＵ３を接続する作業を行う作業者がＥＣＵ秘密鍵及びＧＷ秘密鍵を扱う必要はなく、悪意の作業者がＥＣＵ秘密鍵及びＧＷ秘密鍵を不正に取得することを防止できる。
【００９５】
また本実施の形態においては、車両１内のネットワークを介した通信に用いられるセッション鍵をゲートウェイ２が記憶し、正当であると判定した新規のＥＣＵ３に対してこのセッション鍵を送信する処理を行う。セッション鍵は、車両１内のネットワークに接続された全ての装置が共有する共通鍵であり、例えば送受信情報の暗号化／復号の処理、又は、メッセージ認証子の生成／検証の処理等を行う際に用いられる。ゲートウェイ２は、ＥＣＵ３のＥＣＵ公開鍵を用いてセッション鍵を暗号化し、暗号化したセッション鍵をＥＣＵ３へ送信する。暗号化されたセッション鍵を受信したＥＣＵ３は、記憶部３２に記憶されたＥＣＵ秘密鍵を用いてセッション鍵を復号する。以降、ＥＣＵ３は、車両１内のネットワークに接続された他のＥＣＵ３との間で、セッション鍵を用いた通信を行うことが可能となる。
【００９６】
また本実施の形態においては、ＥＣＵ公開鍵に電子署名を付したものを可視化したＱＲコード３Ｂを生成し、ＥＣＵ３を収容する箱３ＡにＱＲコード３Ｂを印刷しておく。ＱＲコード３Ｂは、箱３Ａ以外の場所に印刷されてもよく、例えばＥＣＵ３の外装部品などにＱＲコード３Ｂを印刷してもよく、また例えばＥＣＵ３に付属する説明書など、ＥＣＵ３と共に箱３Ａに収められた他の付属品にＱＲコード３Ｂを印刷してもよい。ＥＣＵ３を車両１内のネットワークに接続する際、画像読取装置７にてＥＣＵ３の本体又は付属物に描かれたＱＲコード３Ｂの読み取りを行う。読み取った画像を電子署名付きのＥＣＵ公開鍵の情報へ変換することによって、ゲートウェイ２は電子署名付きのＥＣＵ公開鍵を取得することができる。なおＱＲコード３ＢからＥＣＵ公開鍵のへの変換は、画像読取装置７が行ってもよく、ゲートウェイ２が行ってもよい。
【００９７】
また本実施の形態においては、ＥＣＵ３のＥＣＵ公開鍵の電子署名を署名生成装置６が

生成する。署名生成装置６は、ゲートウェイ２が記憶している署名検証鍵と対になる署名生成鍵を記憶しており、この署名生成鍵を用いてＥＣＵ３のＥＣＵ公開鍵の電子署名を生成する。署名生成装置６は例えばＥＣＵ３の製造前の段階で電子署名の生成を行い、生成された電子署名が付されたＥＣＵ公開鍵の情報を元にＱＲコード３Ｂを生成し、ＥＣＵ３の製造工程においてＱＲコード３Ｂの印刷が行われる。

【００９８】

また本実施の形態においてゲートウェイ２は、ＥＣＵ３の電子署名付きのＥＣＵ公開鍵を取得する際に、ＥＣＵ３を識別するＩＤを取得する。例えばＥＣＵ３のＩＤは、電子署名付きのＥＣＵ公開鍵と共にＱＲコード３Ｂとして画像読取装置７を介してゲートウェイ２に取得される。ゲートウェイ２は、ＥＣＵ３のＩＤに対応付けてＥＣＵ公開鍵を記憶部２２のＥＣＵ公開鍵ＤＢ２２ｆに記憶しておく。ＥＣＵ３は、車両１内のネットワークに接続された際に、自身のＩＤをゲートウェイ２へ送信する。このＩＤを受信したゲートウェイ２は、受信したＩＤに対応付けられたＥＣＵ公開鍵を用いて自身のＧＷ公開鍵を暗号化し、暗号化したＧＷ公開鍵をＥＣＵ３へ送信する。これによりゲートウェイ２は、複数のＥＣＵ３に関するＥＣＵ公開鍵を取得し、複数のＥＣＵ３に対して並列的に認証を行うことが可能となる。

【００９９】

なお本実施の形態においては、車両１に搭載されたゲートウェイ２が、新たに接続されたＥＣＵ３の認証を行う構成としたが、これに限るものではない。例えば車両１に搭載されたいずれかのＥＣＵ３が新たに接続されたＥＣＵ３の認証を行う構成としてもよく、ゲートウェイ２及びＥＣＵ３以外の車載装置が認証を行う構成としてもよい。

【０１００】

また本実施の形態においては、ＥＣＵ３の箱３Ａに印刷されたＱＲコード３Ｂを画像読取装置７にて読み取ることでゲートウェイ２がＥＣＵ公開鍵を取得する構成としたが、これに限るものではない。ＥＣＵ公開鍵は、ＱＲコード３Ｂ以外の画像に変換されて印刷されてもよい。またＱＲコード３Ｂは、ＥＣＵ３の箱３Ａ以外に印刷されてもよい。また、画像を読み取ることでＥＣＵ公開鍵を取得するのではなく、例えばＥＣＵ３に付属するメモリカードなどの記録媒体にＥＣＵ公開鍵及び電子署名の情報を記録しておき、ゲートウェイ２が記録媒体からＥＣＵ公開鍵及び電子署名を取得する構成としてもよい。この構成の場合、ゲートウェイ２及び記録媒体がＮＦＣ（Near Field Communication）などの無線通信を行って情報を授受する構成としてもよい。また例えば、ＥＣＵ公開鍵などの情報を数字又は文字等を複数並べた文字列としてＥＣＵ３の箱３Ａ又は取扱説明書等に印刷しておく構成としてもよい。この構成の場合、画像読取装置７にて文字列を読み取る構成としてもよいが、作業者がキーボードなどの入力デバイスを用いて文字列を入力し、ゲートウェイ２が入力された文字列を取得してＥＣＵ公開鍵などの情報に変換する構成としてもよい。

【０１０１】

また本実施の形態においては、ＥＣＵ製造会社５から署名生成装置６へインターネットなどのネットワークを介してＥＣＵ公開鍵を送信し、署名生成装置６からＥＣＵ製造会社５へネットワークを介して電子署名を送信する構成としたが、これに限るものではない。ＥＣＵ製造会社５及び署名生成装置６の間の情報授受は、例えば情報を記録した記録媒体を郵送で授受するなどの方法を採用してもよい。ゲートウェイ製造会社４及び署名生成装置６の間の情報授受も同様である。

【０１０２】

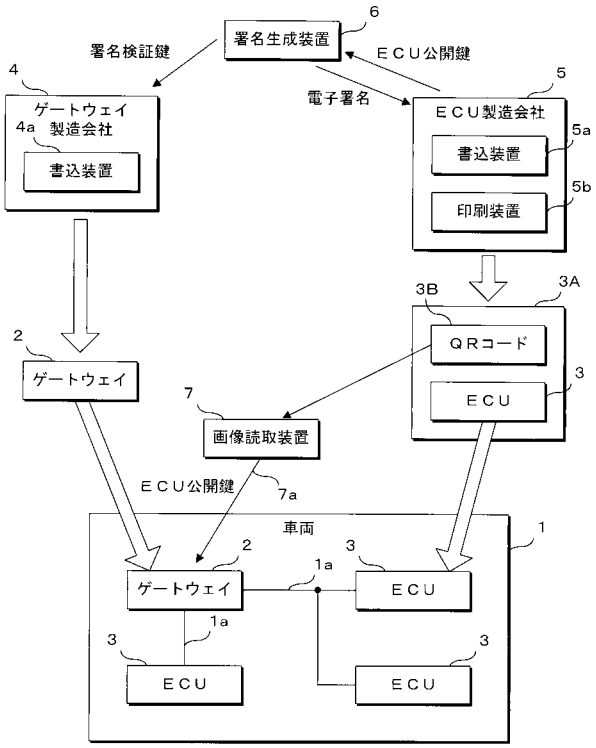
また本実施の形態においてゲートウェイ２の処理部２１が実行する認証処理プログラム２２ａ、ＥＣＵ３の処理部３１が実行する認証処理プログラム３２ａ、署名生成装置６の処理部６１が実行する署名生成プログラム６２ａ及び画像読取装置７の処理部７１が実行する変換プログラム７２ａ等のプログラムは、光ディスク又はメモリカード等の記録媒体に記録された態様で提供され得る。

【符号の説明】

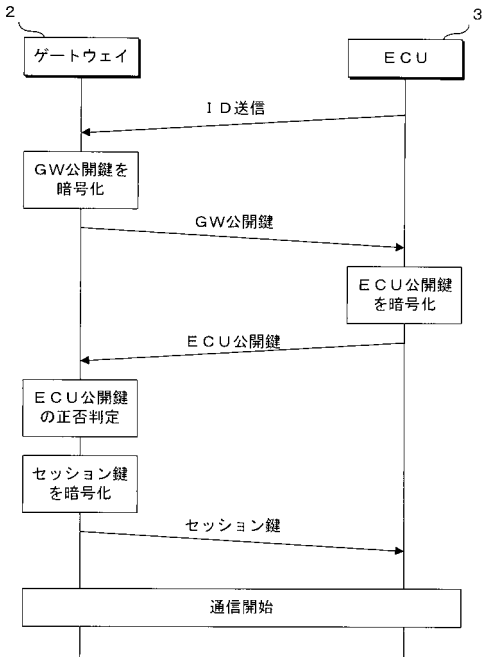
【０１０３】
１　車両
１ａ　通信線
２　ゲートウェイ（車載認証装置）
３　ＥＣＵ（通信装置）
３Ａ　箱（付随物）
３Ｂ　ＱＲコード（可視化情報）
４　ゲートウェイ製造会社
４ａ　書込装置
５　ＥＣＵ製造会社
５ａ　書込装置
５ｂ　印刷装置
６　署名生成装置
７　画像読取装置（可視化情報取得装置）
７ａ　通信ケーブル
２１　処理部
２１ａ　ＥＣＵ公開鍵取得部（第１公開鍵取得部）
２１ｂ　署名検証部
２１ｃ　識別情報受信部
２１ｄ　ＧＷ公開鍵暗号化部（第２公開鍵暗号化部）
２１ｅ　ＧＷ公開鍵送信部（第２公開鍵送信部）
２１ｆ　ＥＣＵ公開鍵受信部（第１公開鍵受信部）
２１ｇ　ＥＣＵ公開鍵復号部（第１公開鍵復号部）
２１ｈ　ＥＣＵ公開鍵判定部（第１公開鍵判定部）
２１ｉ　セッション鍵暗号化部（共通鍵暗号化部）
２１ｊ　セッション鍵送信部（共通鍵送信部）
２２　記憶部（第２記憶部）
２２ａ　認証処理プログラム
２２ｂ　ＧＷ秘密鍵（第２秘密鍵）
２２ｃ　ＧＷ公開鍵（第２公開鍵）
２２ｄ　署名検証鍵
２２ｅ　セッション鍵（共通鍵）
２２ｆ　ＥＣＵ公開鍵ＤＢ
２３　通信部
２４　接続端子
３１　処理部
３１ａ　識別情報送信部
３１ｂ　ＧＷ公開鍵受信部（第２公開鍵受信部）
３１ｃ　ＧＷ公開鍵復号部（第２公開鍵復号部）
３１ｄ　ＥＣＵ公開鍵暗号化部（第１公開鍵暗号化部）
３１ｅ　ＥＣＵ公開鍵送信部（第１公開鍵送信部）
３１ｆ　セッション鍵受信部（共通鍵受信部）
３１ｇ　セッション鍵復号部（共通鍵復号部）
３２　記憶部（第１記憶部）
３２ａ　認証処理プログラム
３２ｂ　ＥＣＵ秘密鍵（第１秘密鍵）
３２ｃ　ＥＣＵ公開鍵（第２秘密鍵）
３２ｄ　セッション鍵（共通鍵）
３３　通信部
６１　処理部

６１ａ　ＥＣＵ公開鍵受信部
６１ｂ　署名生成部
６１ｃ　署名送信部
６２　記憶部
６２ａ　署名生成プログラム
６２ｂ　署名生成鍵
６３　通信部
７１　処理部
７１ａ　変換処理部
７２　記憶部
７２ａ　変換プログラム
７３　カメラ
７４　接続端子

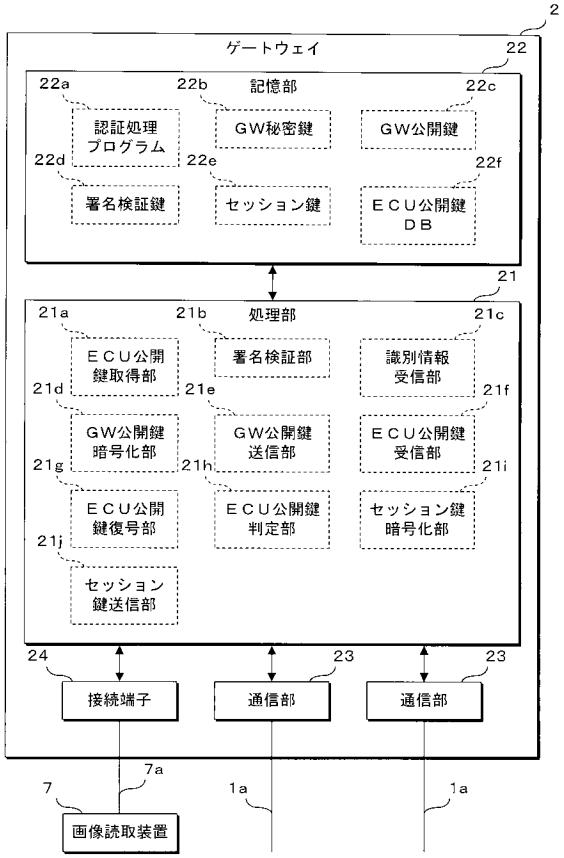
【図１】



【図２】



【図３】

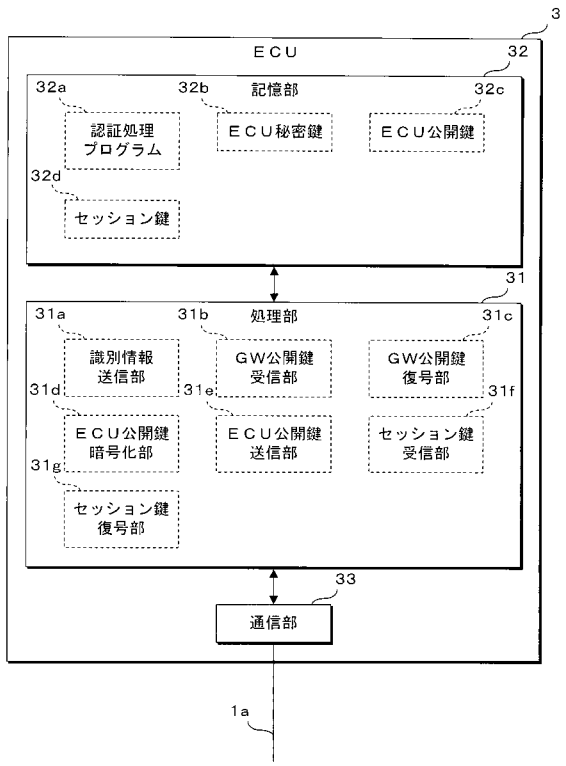


【図４】

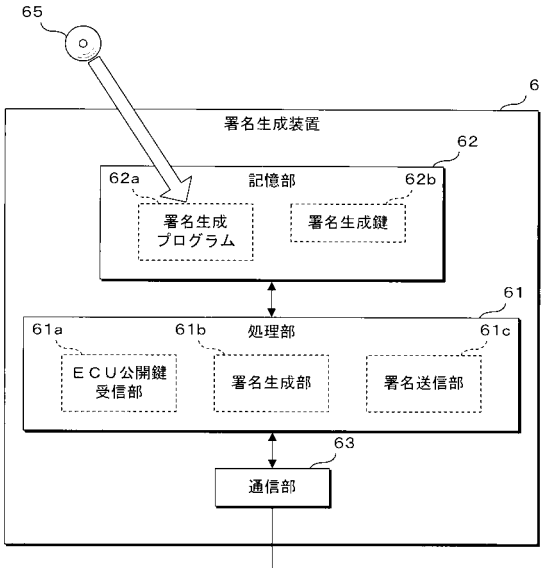
ECU公開鍵DB

ID	ECU公開鍵	電子署名
⋮	⋮	⋮

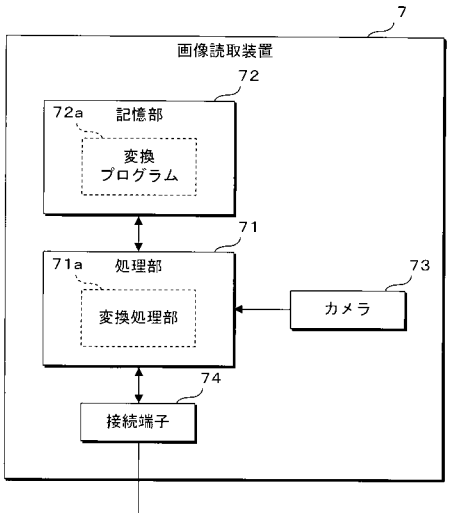
【図５】



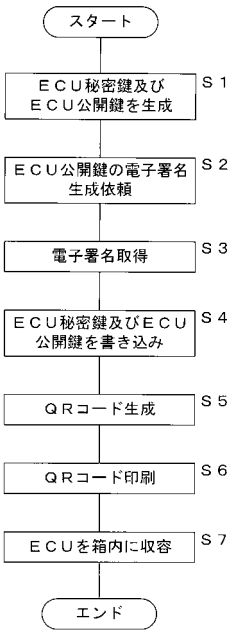
【図６】



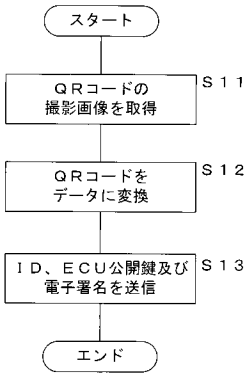
【図７】


7
画像読取装置
72
72a
記憶部
変換
プログラム
71
71a
処理部
変換処理部
73
カメラ
74
接続端子

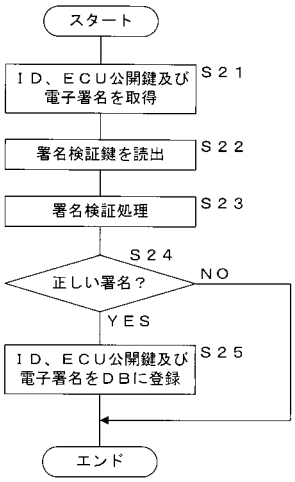
【図８】


スタート
ＥＣＵ秘密鍵及び
ＥＣＵ公開鍵を生成
Ｓ１
ＥＣＵ公開鍵の電子署名
生成依頼
Ｓ２
電子署名取得
Ｓ３
ＥＣＵ秘密鍵及びＥＣＵ
公開鍵を書き込み
Ｓ４
ＱＲコード生成
Ｓ５
ＱＲコード印刷
Ｓ６
ＥＣＵを箱内に収容
Ｓ７
エンド

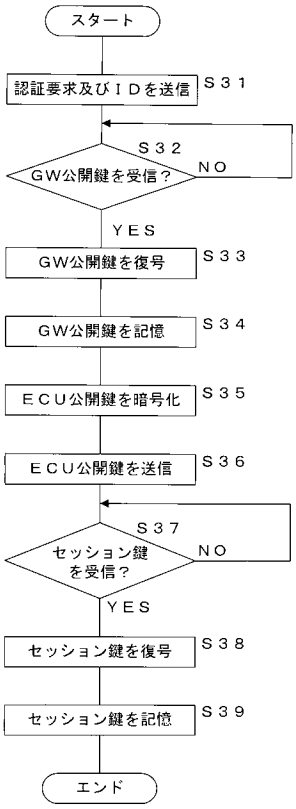
【図９】


スタート
ＱＲコードの
撮影画像を取得
Ｓ１１
ＱＲコードを
データに変換
Ｓ１２
ＩＤ、ＥＣＵ公開鍵及び
電子署名を送信
Ｓ１３
エンド

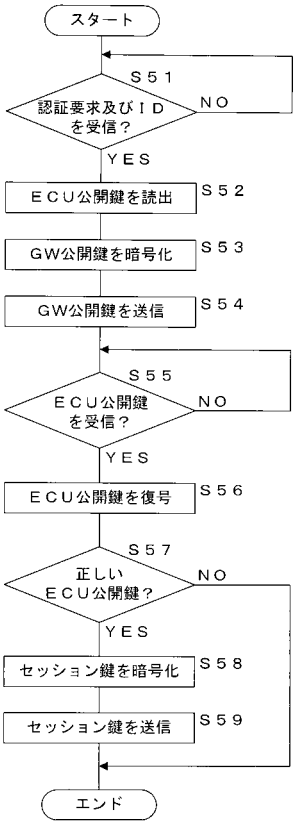
【図１０】


スタート
ＩＤ、ＥＣＵ公開鍵及び
電子署名を取得
Ｓ２１
署名検証鍵を読出
Ｓ２２
署名検証処理
Ｓ２３
Ｓ２４
正しい署名？
ＮＯ
ＹＥＳ
ＩＤ、ＥＣＵ公開鍵及び
電子署名をＤＢに登録
Ｓ２５
エンド

【図１１】


スタート
認証要求及びＩＤを送信
Ｓ３１
Ｓ３２
GW公開鍵を受信？
ＮＯ
ＹＥＳ
GW公開鍵を復号
Ｓ３３
GW公開鍵を記憶
Ｓ３４
ＥＣＵ公開鍵を暗号化
Ｓ３５
ＥＣＵ公開鍵を送信
Ｓ３６
Ｓ３７
セッション鍵
を受信？
ＮＯ
ＹＥＳ
セッション鍵を復号
Ｓ３８
セッション鍵を記憶
Ｓ３９
エンド

【図１２】


スタート
Ｓ５１
認証要求及びＩＤ
を受信？
ＮＯ
ＹＥＳ
ＥＣＵ公開鍵を読出
Ｓ５２
GW公開鍵を暗号化
Ｓ５３
GW公開鍵を送信
Ｓ５４
Ｓ５５
ＥＣＵ公開鍵
を受信？
ＮＯ
ＹＥＳ
ＥＣＵ公開鍵を復号
Ｓ５６
Ｓ５７
正しい
ＥＣＵ公開鍵？
ＮＯ
ＹＥＳ
セッション鍵を暗号化
Ｓ５８
セッション鍵を送信
Ｓ５９
エンド

フロントページの続き

(74)代理人　100078868
弁理士　河野　登夫
(72)発明者　高田　広章
愛知県名古屋市千種区不老町１番　国立大学法人名古屋大学内
(72)発明者　倉地　亮
愛知県名古屋市千種区不老町１番　国立大学法人名古屋大学内
(72)発明者　上田　浩史
三重県四日市市西末広町１番１４号　株式会社オートネットワーク技術研究所内
Ｆターム(参考) 5J104 AA07　AA16　EA16　KA05　NA02　NA38　PA07