(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2017-17616
(P2017-17616A)
(43)公開日　平成29年1月19日(2017.1.19)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/16	(2006.01)	H04L	9/00	643	5J104
H04L	9/32	(2006.01)	H04L	9/00	675A	
G09C	1/00	(2006.01)	G09C	1/00	640D	
G06F	21/64	(2013.01)	G06F	21/64		
B60R	16/02	(2006.01)	H04L	9/00	675B	

審査請求 未請求　請求項の数 7　OL　（全 16 頁）　最終頁に続く

(21)出願番号　特願2015-134427 (P2015-134427)
(22)出願日　平成27年7月3日 (2015.7.3)

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100106909
弁理士　棚井　澄雄
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100146835
弁理士　佐伯　義文
(72)発明者　川端　秀明
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内
(72)発明者　溝口　誠一郎
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内
最終頁に続く

(54)【発明の名称】ソフトウェア配布処理装置、車両、ソフトウェア配布処理方法及びコンピュータプログラム

(57)【要約】
【課題】ＥＣＵ等のコンピュータのコンピュータプログラムの更新の際にコンピュータの共通鍵で検証することによる負担を軽減すること。
【解決手段】ソフトウェア配布処理装置２は、ソフトウェアの更新データの電子署名の検証鍵とＥＣＵ３０の共通鍵を記憶し、管理サーバ装置７０から受信した更新データの電子署名を、検証鍵を使用して検証し、電子署名の検証が成功した更新データに対してＥＣＵ３０の共通鍵を使用して電子署名を施し、ＥＣＵ３０の共通鍵を使用して電子署名が施された更新データをＥＣＵ３０へ送信する。
【選択図】図１

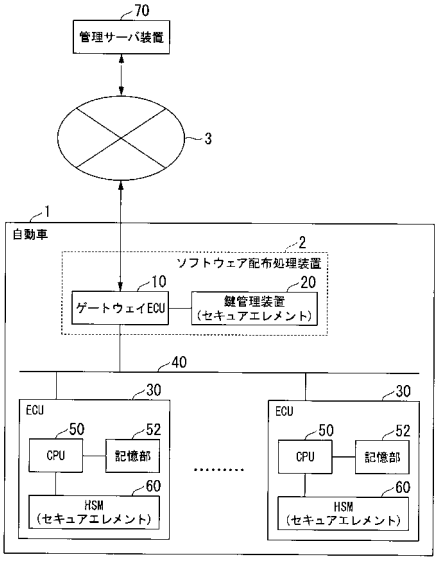

図1

【特許請求の範囲】
【請求項１】
ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を記憶する鍵記憶部と、
電子署名が施された前記更新データを受信する受信部と、
前記受信部で受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証部と、
前記検証部による電子署名の検証が成功した前記更新データに対して前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名部と、
前記共通鍵を使用して電子署名が施された前記更新データを前記コンピュータへ送信する送信部と、
を備えるソフトウェア配布処理装置。
【請求項２】
ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を記憶する鍵記憶部と、
電子署名が施された前記更新データを受信する受信部と、
前記受信部で受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証部と、
前記検証部による電子署名の検証が成功した前記更新データについての期待値を計算する期待値計算部と、
前記検証部による電子署名の検証が成功した前記更新データについて計算された前記期待値を、前記鍵記憶部に記憶される前記共通鍵を使用して暗号化する暗号処理部と、
前記検証部による電子署名の検証が成功した前記更新データと当該更新データについて計算された前記期待値が前記共通鍵を使用して暗号化された暗号化データに対して、前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名部と、
前記共通鍵を使用して電子署名が施された前記更新データと前記暗号化データを前記コンピュータへ送信する送信部と、
を備えるソフトウェア配布処理装置。
【請求項３】
請求項１又は２のいずれか１項に記載のソフトウェア配布処理装置と、
通信ネットワークと、
前記通信ネットワークを介して前記ソフトウェア配布処理装置と通信する車載コンピュータと、
を備える車両。
【請求項４】
ソフトウェア配布処理装置が、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、
前記ソフトウェア配布処理装置が、電子署名が施された前記更新データを受信する受信ステップと、
前記ソフトウェア配布処理装置が、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データに対して前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、
前記ソフトウェア配布処理装置が、前記共通鍵を使用して電子署名が施された前記更新データを前記コンピュータへ送信する送信ステップと、
を含むソフトウェア配布処理方法。
【請求項５】
ソフトウェア配布処理装置が、ソフトウェアの更新データの電子署名の検証に使用され

る検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、
前記ソフトウェア配布処理装置が、電子署名が施された前記更新データを受信する受信ステップと、
前記ソフトウェア配布処理装置が、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについての期待値を計算する期待値計算ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについて計算された前記期待値を、前記鍵記憶部に記憶される前記共通鍵を使用して暗号化する暗号処理ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データと当該更新データについて計算された前記期待値が前記共通鍵を使用して暗号化された暗号化データに対して、前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、
前記ソフトウェア配布処理装置が、前記共通鍵を使用して電子署名が施された前記更新データと前記暗号化データを前記コンピュータへ送信する送信ステップと、
を含むソフトウェア配布処理方法。
【請求項６】
ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、
電子署名が施された前記更新データを受信する受信ステップと、
前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、
前記検証ステップによる電子署名の検証が成功した前記更新データに対して前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、
前記共通鍵を使用して電子署名が施された前記更新データを前記コンピュータへ送信する送信ステップと、
をコンピュータに実行させるためのコンピュータプログラム。
【請求項７】
ソフトウェア配布処理装置が、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、
前記ソフトウェア配布処理装置が、電子署名が施された前記更新データを受信する受信ステップと、
前記ソフトウェア配布処理装置が、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについての期待値を計算する期待値計算ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについて計算された前記期待値を、前記鍵記憶部に記憶される前記共通鍵を使用して暗号化する暗号処理ステップと、
前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データと当該更新データについて計算された前記期待値が前記共通鍵を使用して暗号化された暗号化データに対して、前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、
前記ソフトウェア配布処理装置が、前記共通鍵を使用して電子署名が施された前記更新データと前記暗号化データを前記コンピュータへ送信する送信ステップと、
をコンピュータに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、ソフトウェア配布処理装置、車両、ソフトウェア配布処理方法及びコンピュータプログラムに関する。
【背景技術】
【０００２】
近年、自動車は、車載制御システムを備え、車載制御システムによって、走る、止まる、曲がるといった自動車の基本的な動作の制御や、その他の応用的な制御を行っている。車載制御システムは、一般に、ＥＣＵ（Electronic Control Unit）と呼ばれる車載制御マイコンを２０個～１００個程度備える。ＥＣＵは、コンピュータの一種であり、コンピュータプログラムによって所望の機能を実現する。それらＥＣＵは、自動車に搭載される通信ネットワークであるＣＡＮ（Controller Area Network）に接続し、各ＥＣＵが互いに連携する。
【０００３】
また、自動車には、ＥＣＵに繋がるＯＢＤ（On-board Diagnostics）ポートと呼ばれる診断ポートのインタフェースが設けられている。このＯＢＤポートに、メンテナンス専用の診断端末を接続して、該診断端末からＥＣＵに対して更新プログラムのインストール及びデータの設定変更などを行うことができる。すでに使用されている自動車について、ＥＣＵのコンピュータプログラムの更新等をする場合には、通常、車検時や自動車の定期点検時などに、正規販売店（ディーラー）や一般の自動車整備工場の工員によって更新がなされる。
【０００４】
自動車の車載制御システムに関し、例えば非特許文献１、２にはセキュリティについて記載されている。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】C. Miller、C. Valasek、“Adventures in Automotive Networks and Control Units”、DEF CON 21、2013年8月
【非特許文献２】吉岡顕、小熊寿、西川真、繁富利恵、大塚玲、今井秀樹、“構成証明機能を持つ車内通信プロトコルの提案”、情報処理学会、DICOMO2008、pp.1270-1275、2008年7月
【発明の概要】
【発明が解決しようとする課題】
【０００６】
自動車の車載制御システムのＥＣＵに使用されるコンピュータプログラム等のデータの適用についての信頼性を向上させることが望まれる。例えば、ＥＣＵがファームウェアの更新を実施する際にＥＣＵの共通鍵で検証することが考えられる。この場合、更新ファームウェアを配布するサーバがＥＣＵの共通鍵を有することになる。しかしながら、更新ファームウェアを配布するサーバが複数存在する場合、ＥＣＵの共通鍵を複数のサーバで共有することから、ＥＣＵの共通鍵のサーバ間共有におけるコスト面や、共通鍵の漏洩時に漏洩元の特定が難しいなどの共通鍵のセキュリティ面における負担が問題となる可能性がある。
【０００７】
本発明は、このような事情を考慮してなされたものであり、ＥＣＵ等のコンピュータのコンピュータプログラムの更新の際にコンピュータの共通鍵で検証することによる負担を軽減することができる、ソフトウェア配布処理装置、車両、ソフトウェア配布処理方法及びコンピュータプログラムを提供することを課題とする。
【課題を解決するための手段】
【０００８】

（１）本発明の一態様は、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を記憶する鍵記憶部と、電子署名が施された前記更新データを受信する受信部と、前記受信部で受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証部と、前記検証部による電子署名の検証が成功した前記更新データに対して前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名部と、前記共通鍵を使用して電子署名が施された前記更新データを前記コンピュータへ送信する送信部と、を備えるソフトウェア配布処理装置である。

【０００９】

（２）本発明の一態様は、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を記憶する鍵記憶部と、電子署名が施された前記更新データを受信する受信部と、前記受信部で受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証部と、前記検証部による電子署名の検証が成功した前記更新データについての期待値を計算する期待値計算部と、前記検証部による電子署名の検証が成功した前記更新データについて計算された前記期待値を、前記鍵記憶部に記憶される前記共通鍵を使用して暗号化する暗号処理部と、前記検証部による電子署名の検証が成功した前記更新データと当該更新データについて計算された前記期待値が前記共通鍵を使用して暗号化された暗号化データに対して、前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名部と、前記共通鍵を使用して電子署名が施された前記更新データと前記暗号化データを前記コンピュータへ送信する送信部と、を備えるソフトウェア配布処理装置である。

【００１０】

（３）本発明の一態様は、上記（１）又は（２）のいずれかのソフトウェア配布処理装置と、通信ネットワークと、前記通信ネットワークを介して前記ソフトウェア配布処理装置と通信する車載コンピュータと、を備える車両である。

【００１１】

（４）本発明の一態様は、ソフトウェア配布処理装置が、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、前記ソフトウェア配布処理装置が、電子署名が施された前記更新データを受信する受信ステップと、前記ソフトウェア配布処理装置が、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データに対して前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、前記ソフトウェア配布処理装置が、前記共通鍵を使用して電子署名が施された前記更新データを前記コンピュータへ送信する送信ステップと、を含むソフトウェア配布処理方法である。

【００１２】

（５）本発明の一態様は、ソフトウェア配布処理装置が、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、前記ソフトウェア配布処理装置が、電子署名が施された前記更新データを受信する受信ステップと、前記ソフトウェア配布処理装置が、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについての期待値を計算する期待値計算ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについて計算された前記期待値を、前記鍵記憶部に記憶される前記共通鍵を使用して暗号化する暗号処理ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データと当該更新データについて計算された前記期待値が前記共通鍵を使用して暗号化された暗号化データに対して、前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署

名ステップと、前記ソフトウェア配布処理装置が、前記共通鍵を使用して電子署名が施された前記更新データと前記暗号化データを前記コンピュータへ送信する送信ステップと、を含むソフトウェア配布処理方法である。

【００１３】

（６）本発明の一態様は、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、電子署名が施された前記更新データを受信する受信ステップと、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、前記検証ステップによる電子署名の検証が成功した前記更新データに対して前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、前記共通鍵を使用して電子署名が施された前記更新データを前記コンピュータへ送信する送信ステップと、をコンピュータに実行させるためのコンピュータプログラムである。

【００１４】

（７）本発明の一態様は、ソフトウェア配布処理装置が、ソフトウェアの更新データの電子署名の検証に使用される検証鍵と前記ソフトウェアがインストールされたコンピュータの共通鍵を鍵記憶部に記憶する鍵記憶ステップと、前記ソフトウェア配布処理装置が、電子署名が施された前記更新データを受信する受信ステップと、前記ソフトウェア配布処理装置が、前記受信ステップで受信された前記更新データの電子署名を前記鍵記憶部に記憶される前記検証鍵を使用して検証する検証ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについての期待値を計算する期待値計算ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データについて計算された前記期待値を、前記鍵記憶部に記憶される前記共通鍵を使用して暗号化する暗号処理ステップと、前記ソフトウェア配布処理装置が、前記検証ステップによる電子署名の検証が成功した前記更新データと当該更新データについて計算された前記期待値が前記共通鍵を使用して暗号化された暗号化データに対して、前記鍵記憶部に記憶される前記共通鍵を使用して電子署名を施す署名ステップと、前記ソフトウェア配布処理装置が、前記共通鍵を使用して電子署名が施された前記更新データと前記暗号化データを前記コンピュータへ送信する送信ステップと、をコンピュータに実行させるためのコンピュータプログラムである。

【発明の効果】

【００１５】

本発明によれば、ＥＣＵ等のコンピュータのコンピュータプログラムの更新の際にコンピュータの共通鍵で検証することによる負担を軽減することができるという効果が得られる。

【図面の簡単な説明】

【００１６】

【図１】第１実施形態に係る自動車１及び管理システムを示す図である。
【図２】図１に示すゲートウェイＥＣＵ１０の構成図である。
【図３】図１に示す鍵管理装置２０の構成図である。
【図４】第１実施形態のソフトウェア配布処理方法のシーケンスチャートである。
【図５】セキュアブート方法の説明図である。
【図６】第２実施形態に係る鍵管理装置２０の構成図である。
【図７】第２実施形態のソフトウェア配布処理方法のシーケンスチャートである。

【発明を実施するための形態】

【００１７】

以下、図面を参照し、本発明の実施形態について説明する。なお、以下に示す実施形態では、車両として自動車を例に挙げて説明する。

【００１８】

［第１実施形態］

図１は、第１実施形態に係る自動車１及び管理システムを示す図である。図１において、自動車１は、ゲートウェイＥＣＵ１０と鍵管理装置２０と複数のＥＣＵ３０と車載ネットワーク４０を備える。本実施形態では、ソフトウェア配布処理装置２はゲートウェイＥＣＵ１０と鍵管理装置２０から構成される。ゲートウェイＥＣＵ１０とＥＣＵ３０は車載ネットワーク４０に接続される。車載ネットワーク４０として、例えばＣＡＮが使用される。ＣＡＮは車両に搭載される通信ネットワークの一つとして知られている。本実施形態では、車載ネットワーク４０はＣＡＮである。ゲートウェイＥＣＵ１０と各ＥＣＵ３０とは、車載ネットワーク４０を介してデータを交換する。ＥＣＵ３０は、車載ネットワーク４０を介して、他のＥＣＵ３０との間でデータを交換する。

【００１９】

ＥＣＵ３０は、自動車１に備わる車載コンピュータである。ＥＣＵ３０は、ＣＰＵ（Central Processing Unit）５０と記憶部５２とＨＳＭ（Hardware Security Module）６０を備える。ＣＰＵ＿５０は、ＥＣＵ３０にインストールされたファームウェアを実行する。ファームウェアはソフトウェアつまりコンピュータプログラムの一種である。記憶部５２はファームウェアやデータ等を記憶する。記憶部５２は、ＲＯＭ（リードオンリメモリ）やＲＡＭ（ランダムアクセスメモリ）、フラッシュメモリ（flash memory）などから構成される。ＨＳＭ＿６０は暗号処理等を実行する。本実施形態では、セキュアエレメントの一例としてＨＳＭ＿６０を使用する。セキュアエレメントは耐タンパー性を有する。

【００２０】

ゲートウェイＥＣＵ１０は、無線通信ネットワーク３を介して管理サーバ装置７０と通信する。管理サーバ装置７０はＥＣＵ３０のファームウェアを管理する。鍵管理装置２０は、管理サーバ装置７０の鍵とＥＣＵ３０の鍵を管理する。鍵管理装置２０はセキュアエレメントにより実現される。

【００２１】

図２は、図１に示すゲートウェイＥＣＵ１０の構成図である。図２において、ゲートウェイＥＣＵ１０は無線通信部１１とＣＡＮインタフェース１２と制御部１３とユーザインタフェース１４を備える。無線通信部１１は無線通信ネットワーク３を介して管理サーバ装置７０とデータを送受する。ＣＡＮインタフェース１２は、車載ネットワーク４０を介して各ＥＣＵ３０とデータを送受する。制御部１３は、ゲートウェイＥＣＵ１０の制御を実行する。ユーザインタフェース１４は、利用者の操作を受け付ける。

【００２２】

図３は、図１に示す鍵管理装置２０の構成図である。図３において、鍵管理装置２０は、検証部２１と署名部２２と鍵記憶部２３を備える。検証部２１は、電子署名の検証を実行する。署名部２２は、電子署名の生成を実行する。鍵記憶部２３は、管理サーバ装置７０の電子署名の検証に使用される検証鍵と、ＥＣＵ３０の共通鍵を記憶する。管理サーバ装置７０の電子署名の検証に使用される検証鍵は、管理サーバ装置７０の電子署名の生成に使用される共通鍵であってもよく、又は、管理サーバ装置７０の電子署名の生成に使用される秘密鍵のペアの公開鍵であってもよい。鍵記憶部２３には、予め、管理サーバ装置７０の電子署名の検証に使用される検証鍵と、ＥＣＵ３０の共通鍵とが記憶される。

【００２３】

鍵管理装置２０はセキュアエレメントにより実現される。鍵管理装置２０を実現するセキュアエレメントとして、例えば、ＳＩＭ（Subscriber Identity Module）、ｅＳＩＭ（Embedded Subscriber Identity Module）又はＨＳＭなどが挙げられる。例えば、無線通信ネットワーク３を利用するためのＳＩＭ又はｅＳＩＭを使用して、鍵管理装置２０を実現してもよい。無線通信ネットワーク３を利用するためのＳＩＭ又はｅＳＩＭは、ゲートウェイＥＣＵ１０の無線通信部１１が無線通信ネットワーク３に接続する際に使用される。

【００２４】

次に図４を参照して、本実施形態の動作を説明する。図４は、第１実施形態のソフトウェア配布処理方法のシーケンスチャートである。

【００２５】
（ステップＳ１）利用者がゲートウェイＥＣＵ１０のユーザインタフェース１４を操作してＥＣＵ３０のアップデート確認を実施する。又は、管理サーバ装置７０がゲートウェイＥＣＵ１０に対してＥＣＵ３０のアップデート確認を要求する。
【００２６】
（ステップＳ２）ゲートウェイＥＣＵ１０は、ＥＣＵ３０に対してＥＣＵバージョンを問い合わせし、ＥＣＵ３０からＥＣＵバージョンの応答を得る。ゲートウェイＥＣＵ１０は、ＥＣＵ３０から得た応答のＥＣＵバージョンを管理サーバ装置７０へ送信する。
【００２７】
なお、管理サーバ装置７０が自動車１のＥＣＵ３０のＥＣＵバージョンを記録し管理する場合には、上記のステップＳ１及びＳ２は無くてもよい。
【００２８】
（ステップＳ３）管理サーバ装置７０が、自動車１のＥＣＵ３０について、更新ファームウェアの有無を確認する。管理サーバ装置７０は、ＥＣＵ３０のバージョン情報と電子署名付き更新ファームウェアを保持する。管理サーバ装置７０は、ＥＣＵ３０のバージョン情報に基づいて、自動車１のＥＣＵ３０のＥＣＵバージョンが最新バージョンであるかを判定する。
【００２９】
（ステップＳ４）管理サーバ装置７０は、ステップＳ３の結果、自動車１のＥＣＵ３０のＥＣＵバージョンが最新バージョンではない場合に、電子署名付き更新ファームウェアをゲートウェイＥＣＵ１０へ送信する。
【００３０】
（ステップＳ５）ゲートウェイＥＣＵ１０が、管理サーバ装置７０から受信した電子署名付き更新ファームウェアを鍵管理装置２０へ送信する。
【００３１】
（ステップＳ６）鍵管理装置２０の検証部２１が、ゲートウェイＥＣＵ１０から受信した電子署名付き更新ファームウェアの電子署名を、鍵記憶部２３に記憶される検証鍵を使用して検証する。
【００３２】
（ステップＳ７）鍵管理装置２０の署名部２２は、ステップＳ６の検証部２１による電子署名の検証が成功した電子署名付き更新ファームウェアの更新ファームウェアに対して、鍵記憶部２３に記憶される共通鍵を使用して電子署名を施す。これにより、ＥＣＵ３０の共通鍵を使用して電子署名が施された電子署名付き更新ファームウェアが生成される。このＥＣＵ３０の共通鍵を使用して電子署名が施された電子署名付き更新ファームウェアのことを、管理サーバ装置７０から受信した電子署名付き更新ファームウェアと区別するために、説明の便宜上、再署名更新ファームウェアと称する。
【００３３】
（ステップＳ８）鍵管理装置２０は、再署名更新ファームウェアをゲートウェイＥＣＵ１０へ送信する。なお、ステップＳ６の検証部２１による電子署名の検証が失敗した場合には、鍵管理装置２０は、エラーメッセージをゲートウェイＥＣＵ１０へ送信する。
【００３４】
（ステップＳ９）ゲートウェイＥＣＵ１０は、鍵管理装置２０から受信した再署名更新ファームウェアをＥＣＵ３０へ送信する。
【００３５】
（ステップＳ１０）ＥＣＵ３０のＣＰＵ＿５０は、ゲートウェイＥＣＵ１０から受信した再署名更新ファームウェアをＨＳＭ＿６０へ送信する。
【００３６】
（ステップＳ１１）ＥＣＵ３０のＨＳＭ＿６０は、ＥＣＵ３０の共通鍵を使用して、再署名更新ファームウェアの電子署名を検証する。ＨＳＭ＿６０は、予め、ＥＣＵ３０の共通鍵を保持する。ＨＳＭ＿６０は、再署名更新ファームウェアの電子署名の検証結果をＣＰ

Ｕ＿５０へ応答する。
【００３７】
（ステップＳ１２）ＥＣＵ３０のＣＰＵ＿５０は、ＨＳＭ＿６０から受信した応答が検証の成功である場合に、ステップＳ９でゲートウェイＥＣＵ１０から受信した再署名更新ファームウェアの更新ファームウェアを使用して、ファームウェア更新処理を実行する。これにより、ＥＣＵ３０のＥＣＵバージョンが最新バージョンになる。一方、ＥＣＵ３０のＣＰＵ＿５０は、ＨＳＭ＿６０から受信した応答が検証の失敗である場合には、ファームウェア更新処理を実行しない。
【００３８】
（ステップＳ１３）ＥＣＵ３０のＣＰＵ＿５０は、ファームウェア更新処理の実行が完了した場合に、更新完了通知をゲートウェイＥＣＵ１０へ送信する。ゲートウェイＥＣＵ１０は、ＥＣＵ３０から更新完了通知を受信すると、ＥＣＵ３０のファームウェアの更新完了通知を管理サーバ装置７０へ送信する。
【００３９】
なお、ステップＳ１３の更新完了通知については、実行してもよく、又は、実行しなくてもよい。
【００４０】
また、ステップＳ２において、ＥＣＵバージョンを示すＥＣＵバージョン情報に対して、暗号化したり又は電子署名を施したりしてもよい。以下、ＥＣＵバージョン情報に対して暗号化する場合を説明する。ＥＣＵ３０のＨＳＭ＿６０がＥＣＵ３０の共通鍵を使用してＥＣＵバージョン情報を暗号化し、ＥＣＵバージョン情報の暗号化データをゲートウェイＥＣＵ１０へ送信する。ゲートウェイＥＣＵ１０はＥＣＵバージョン情報の暗号化データを鍵管理装置２０へ送信する。鍵管理装置２０は、鍵記憶部２３に記憶される共通鍵を使用してＥＣＵバージョン情報の暗号化データを復号化する。鍵管理装置２０は、この復号化データを鍵記憶部２３に記憶される検証鍵（管理サーバ装置７０の共通鍵又は公開鍵）を使用して暗号化し、この暗号化データをゲートウェイＥＣＵ１０へ送信する。ゲートウェイＥＣＵ１０は、鍵管理装置２０から受信した暗号化データを管理サーバ装置７０へ送信する。管理サーバ装置７０は、ゲートウェイＥＣＵ１０から受信した暗号化データを、共通鍵又は秘密鍵を使用して復号化する。この復号化によりＥＣＵバージョン情報が得られる。なお、ＥＣＵバージョン情報に対して電子署名を施す場合にも暗号化と同様の手順となる。
【００４１】
上述した第１実施形態によれば、ソフトウェア配布処理装置２が、管理サーバ装置７０から受信した電子署名付き更新ファームウェアの電子署名を検証する。次いで、ソフトウェア配布処理装置２が、電子署名の検証が成功した電子署名付き更新ファームウェアの更新ファームウェアに対して、ＥＣＵ３０の共通鍵を使用して電子署名を施す。次いで、ソフトウェア配布処理装置２が、ＥＣＵ３０の共通鍵を使用して電子署名が施された再署名更新ファームウェアをＥＣＵ３０へ送信する。ＥＣＵ３０は、ソフトウェア配布処理装置２から受信した再署名更新ファームウェアの電子署名を、自己の共通鍵で検証する。ＥＣＵ３０は、電子署名の検証が成功した再署名更新ファームウェアの更新ファームウェアのみを使用して、ファームウェア更新処理を実行する。
【００４２】
これにより、ＥＣＵ３０がファームウェアの更新を実施する際に、ＥＣＵ３０の共通鍵で検証することができる。さらに、管理サーバ装置７０はＥＣＵ３０の共通鍵を有する必要がないので、ＥＣＵ３０の共通鍵のサーバ間共有におけるコスト上の問題や、共通鍵の漏洩時に漏洩元の特定が難しいなどの共通鍵のセキュリティ上の問題が解消する。よって、ＥＣＵ３０のファームウェアの更新の際にＥＣＵ３０の共通鍵で検証することによる負担を軽減することができるという効果が得られる。
【００４３】
［第２実施形態］

第２実施形態において、自動車１及び管理システムの構成は上記の図１と同様である。第２実施形態では、ＥＣＵ３０がセキュアブートを実行する。

【００４４】

図５を参照してＥＣＵ３０のセキュアブートに係る動作を説明する。図５はセキュアブート方法の説明図である。ＥＣＵ３０において、ＣＰＵ＿５０は、ＥＣＵ３０のファームウェアのプログラムコードであるＥＣＵコード（ECU code）５２１を実行する。ＥＣＵコード５２１は、記憶部５２のフラッシュメモリに格納される。ＣＰＵ＿５０に対し、ブートローダ（Boot Loader）５２２によってＥＣＵコード５２１が起動される。ブートローダ５２２のプログラム（ブートプログラム）は、記憶部５２のＲＯＭに格納される。ＣＰＵ＿５０は、初期起動時に記憶部５２のＲＯＭからブートプログラムを起動し、ブートローダ５２２として機能する。ＨＳＭ＿６０は、ＥＣＵコード５２１のＣＭＡＣ（Cipher-based Message Authentication Code）の正解値である期待値ＢＯＯＴ＿ＭＡＣを保持する。期待値ＢＯＯＴ＿ＭＡＣは、予め、ＨＳＭ＿６０に設定される。

【００４５】

（ステップＳ２１）ブートローダ５２２はＥＣＵコード５２１をＨＳＭ＿６０へ送信する。

【００４６】

（ステップＳ２２）ＨＳＭ＿６０は、受信したＥＣＵコード５２１のＣＭＡＣ（Cipher-based Message Authentication Code）を計算する。

【００４７】

（ステップＳ２３）ＨＳＭ＿６０は、計算結果のＣＭＡＣの値と期待値ＢＯＯＴ＿ＭＡＣを比較する。この比較の結果、一致した場合にはＨＳＭ＿６０はブートローダ５２２へ検証の成功を応答し、不一致した場合にはＨＳＭ＿６０はブートローダ５２２へ検証の失敗を応答する。

【００４８】

（ステップＳ２３）ブートローダ５２２は、ＨＳＭ＿６０からの応答が検証の成功である場合にＥＣＵコード５２１を起動する。一方、ブートローダ５２２は、ＨＳＭ＿６０からの応答が検証の失敗である場合にはＥＣＵコード５２１を起動しない。

【００４９】

ＥＣＵ３０のファームウェアを更新するとＥＣＵコード５２１が変わる。このため、ＥＣＵ３０が上述したセキュアブートを実行する場合には、ＥＣＵ３０のファームウェアを更新する際に、ＨＳＭ＿６０に保持される期待値ＢＯＯＴ＿ＭＡＣも更新する必要がある。

【００５０】

図６は、第２実施形態に係る鍵管理装置２０の構成図である。図６に示す鍵管理装置２０は、上記の図３の構成に対してさらに期待値計算部２４と暗号処理部２５を備える。期待値計算部２４はＣＭＡＣを計算する。暗号処理部２５は暗号処理を実行する。

【００５１】

図７を参照して本実施形態の動作を説明する。図７は、第２実施形態のソフトウェア配布処理方法のシーケンスチャートである。図７において、上記の図４の各ステップに対応する部分には同一の符号を付け、その説明を省略する。

【００５２】

ステップＳ１～Ｓ６までは上記の図４と同じである。ステップＳ６における電子署名付き更新ファームウェアの電子署名の検証が成功した場合にのみ、ステップＳ３１に進む。ステップＳ６における電子署名付き更新ファームウェアの電子署名の検証が失敗した場合には、鍵管理装置２０からゲートウェイＥＣＵ１０へ、エラーメッセージが送信される。

【００５３】

（ステップＳ３１）鍵管理装置２０の期待値計算部２４は、ステップＳ６における電子署名の検証が成功した電子署名付き更新ファームウェアの更新ファームウェアに対して、ＣＭＡＣを計算する。次いで、鍵管理装置２０の暗号処理部２５が、期待値計算部２４の計

算結果のＣＭＡＣの値を、鍵記憶部２３に記憶される共通鍵を使用して暗号化する。
【００５４】
（ステップＳ３２）鍵管理装置２０の署名部２２は、ステップＳ６における電子署名の検証が成功した電子署名付き更新ファームウェアの更新ファームウェアとステップＳ３１で暗号処理部２５の暗号化により生成された暗号化データであるＣＭＡＣ暗号化データに対して、鍵記憶部２３に記憶される共通鍵を使用して電子署名を施す。これにより、ＥＣＵ３０の共通鍵を使用して電子署名が施された電子署名付き更新ファームウェアとＣＭＡＣ暗号化データが生成される。このＥＣＵ３０の共通鍵を使用して電子署名が施された電子署名付き更新ファームウェアとＣＭＡＣ暗号化データのことを、管理サーバ装置７０から受信した電子署名付き更新ファームウェアと区別するために、説明の便宜上、再署名更新データと称する。
【００５５】
（ステップＳ３３）鍵管理装置２０は、再署名更新データをゲートウェイＥＣＵ１０へ送信する。
【００５６】
（ステップＳ３４）ゲートウェイＥＣＵ１０は、鍵管理装置２０から受信した再署名更新データをＥＣＵ３０へ送信する。
【００５７】
（ステップＳ３５）ＥＣＵ３０のＣＰＵ＿５０は、ゲートウェイＥＣＵ１０から受信した再署名更新データの電子署名の検証をＨＳＭ＿６０へ依頼する。
【００５８】
（ステップＳ３６）ＥＣＵ３０のＨＳＭ＿６０は、ＥＣＵ３０の共通鍵を使用して、再署名更新データの電子署名を検証する。ＨＳＭ＿６０は、予め、ＥＣＵ３０の共通鍵を保持する。
【００５９】
（ステップＳ３７）ＥＣＵ３０のＨＳＭ＿６０は、再署名更新データの電子署名の検証結果をＣＰＵ＿５０へ応答する。
【００６０】
（ステップＳ３８）ＥＣＵ３０のＣＰＵ＿５０は、ステップＳ３７でＨＳＭ＿６０から受信した応答が検証の成功である場合に、ステップＳ３４でゲートウェイＥＣＵ１０から受信した再署名更新データのＣＭＡＣ暗号化データをＨＳＭ＿６０へ送信し、期待値更新を依頼する。一方、ＥＣＵ３０のＣＰＵ＿５０は、ステップＳ３７でＨＳＭ＿６０から受信した応答が検証の失敗である場合には、ＨＳＭ＿６０に対して期待値更新を依頼しない。
【００６１】
（ステップＳ３９）ＥＣＵ３０のＨＳＭ＿６０は、ＣＰＵ＿５０からの期待値更新の依頼に応じて期待値更新処理を実行する。この期待値更新処理では、ＨＳＭ＿６０は、ＣＰＵ＿５０から受信した再署名更新データの更新ファームウェアのＣＭＡＣを計算する。また、ＨＳＭ＿６０は、ＣＰＵ＿５０から受信した再署名更新データのＣＭＡＣ暗号化データを、ＥＣＵ３０の共通鍵を使用して復号化する。次いで、ＨＳＭ＿６０は、計算結果のＣＭＡＣの値とＣＭＡＣ暗号化データの復号結果の値を比較する。この比較の結果、一致した場合には、ＨＳＭ＿６０は、ＣＭＡＣ暗号化データの復号結果の値を新しい期待値ＢＯＯＴ＿ＭＡＣとして保持する。この場合、期待値更新処理の結果が成功である。一方、その比較の結果、不一致した場合には、ＨＳＭ＿６０は、期待値ＢＯＯＴ＿ＭＡＣを更新しない。この場合、期待値更新処理の結果が失敗である。
【００６２】
（ステップＳ４０）ＥＣＵ３０のＨＳＭ＿６０は、期待値更新処理の結果をＣＰＵ＿５０へ応答する。
【００６３】
（ステップＳ４１）ＥＣＵ３０のＣＰＵ＿５０は、ステップＳ４０でＨＳＭ＿６０から受信した応答が期待値更新処理の成功である場合に、ステップＳ３４でゲートウェイＥＣＵ

１０から受信した再署名更新データの更新ファームウェアを使用して、ファームウェア更新処理を実行する。これにより、ＥＣＵ３０のＥＣＵバージョンが最新バージョンになる。また、ＨＳＭ＿６０に保持される期待値ＢＯＯＴ＿ＭＡＣが最新バージョンになるので、ＥＣＵ３０のセキュアブートに対応することができる。一方、ＥＣＵ３０のＣＰＵ＿５０は、ステップＳ４０でＨＳＭ＿６０から受信した応答が期待値更新処理の失敗である場合には、ファームウェア更新処理を実行しない。

【００６４】

（ステップＳ４２）ＥＣＵ３０のＣＰＵ＿５０は、ファームウェア更新処理の実行が完了した場合に、更新完了通知をゲートウェイＥＣＵ１０へ送信する。ゲートウェイＥＣＵ１０は、ＥＣＵ３０から更新完了通知を受信すると、ＥＣＵ３０のファームウェアの更新完了通知を管理サーバ装置７０へ送信する。

【００６５】

なお、ステップＳ４２の更新完了通知については、実行してもよく、又は、実行しなくてもよい。

【００６６】

上述した第２実施形態によれば、ＥＣＵ３０がセキュアブートを実行する場合に対応することができる。

【００６７】

なお、更新ファームウェアを所定の方法で複数に分割し、該分割ごとにＣＭＡＣの値を計算して期待値を生成してもよい。これにより、更新ファームウェア全体のＣＭＡＣを計算するには鍵管理装置２０の処理能力が不足し時間がかかる場合に、処理時間の短縮を図ることができる。この場合には、ＨＳＭ＿６０は、更新ファームウェアの分割毎にＣＭＡＣの期待値を保持する。そして、ＥＣＵ３０のセキュアブートの実行の際には、ブートローダ５２２が、ＥＣＵコード５２１を所定の方法で複数に分割し、ＥＣＵコード５２１の各分割をＨＳＭ＿６０へ送信する。ＨＳＭ＿６０は、ＥＣＵコード５２１の分割毎に、ＣＭＡＣを計算して期待値と比較する。

【００６８】

また、更新ファームウェアのハッシュ値に対して期待値を持つようにしてもよい。この場合、鍵管理装置２０は、更新ファームウェアのハッシュ値に対してＣＭＡＣを計算し、この計算結果のＣＭＡＣの値を期待値とする。そして、ＥＣＵ３０のセキュアブートの実行の際には、ブートローダ５２２が、ＥＣＵコード５２１のハッシュ値を計算してＨＳＭ＿６０へ送信する。これにより、ＨＳＭ＿６０は、ＥＣＵコード５２１のハッシュ値についてのＣＭＡＣの計算値と期待値の比較を行う。

【００６９】

以上、本発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

例えば、自動車１に備わるいずれかのＥＣＵ３０をゲートウェイＥＣＵ１０として機能させてもよい。

【００７０】

また、車両として自動車を例に挙げたが、原動機付自転車や鉄道車両等の自動車以外の他の車両にも適用可能である。

【００７１】

また、コンピュータとして自動車のＥＣＵを例に挙げたが、他のコンピュータにも適用可能である。例えば、通信ネットワークに接続される家電製品の内蔵コンピュータのファームウェアの更新に適用してもよい。

【００７２】

また、上述したソフトウェア配布処理装置２の機能を実現するためのコンピュータプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行するようにしてもよい。なお、ここ

でいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものであってもよい。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、フラッシュメモリ等の書き込み可能な不揮発性メモリ、ＤＶＤ（Digital Versatile Disk）等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００７３】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（例えばＤＲＡＭ（Dynamic Random Access Memory））のように、一定時間プログラムを保持しているものも含むものとする。

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【符号の説明】

【００７４】

１…自動車、２…ソフトウェア配布処理装置、１０…ゲートウェイＥＣＵ、１１…無線通信部、１２…ＣＡＮインタフェース、１３…制御部、１４…ユーザインタフェース、２０…鍵管理装置、２１…検証部、２２…署名部、２３…鍵記憶部、３０…ＥＣＵ、４０…車載ネットワーク、５０…ＣＰＵ、５２…記憶部、６０…ＨＳＭ、５２１…ＥＣＵコード、５２２…ブートローダ

【図１】

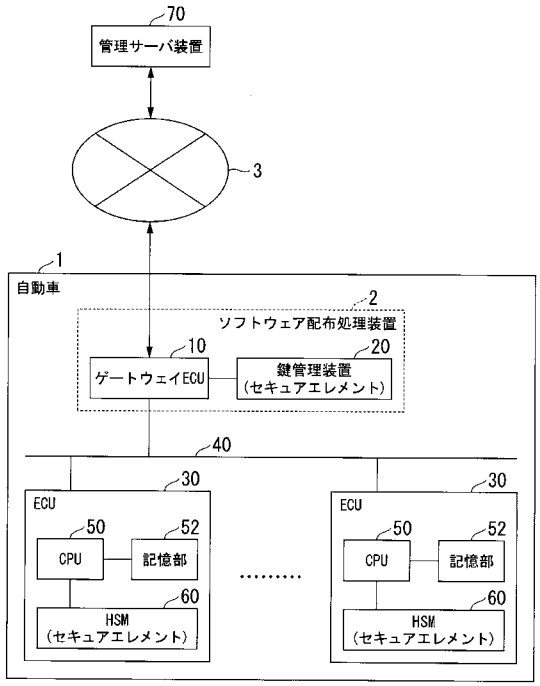

図１

【図２】

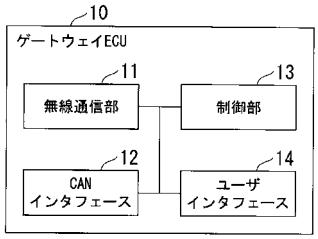

図２

【図３】

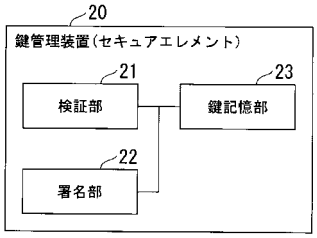

図３

【図４】

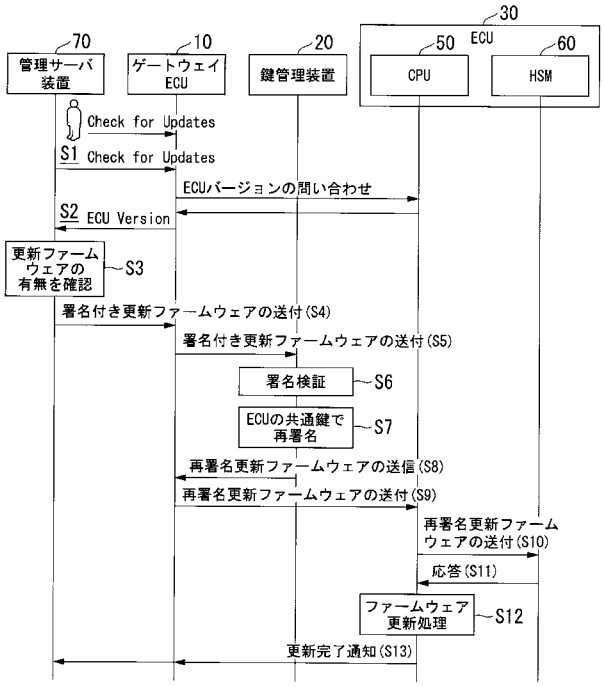

図４

【図５】

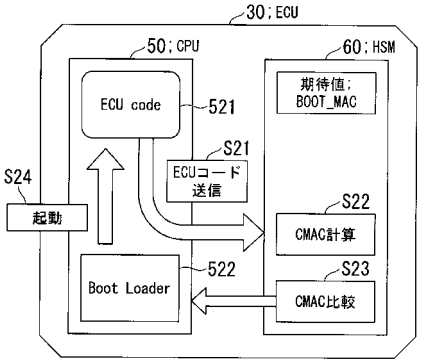

図５

【図６】

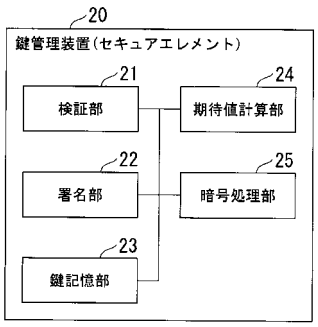

図６

【図７】

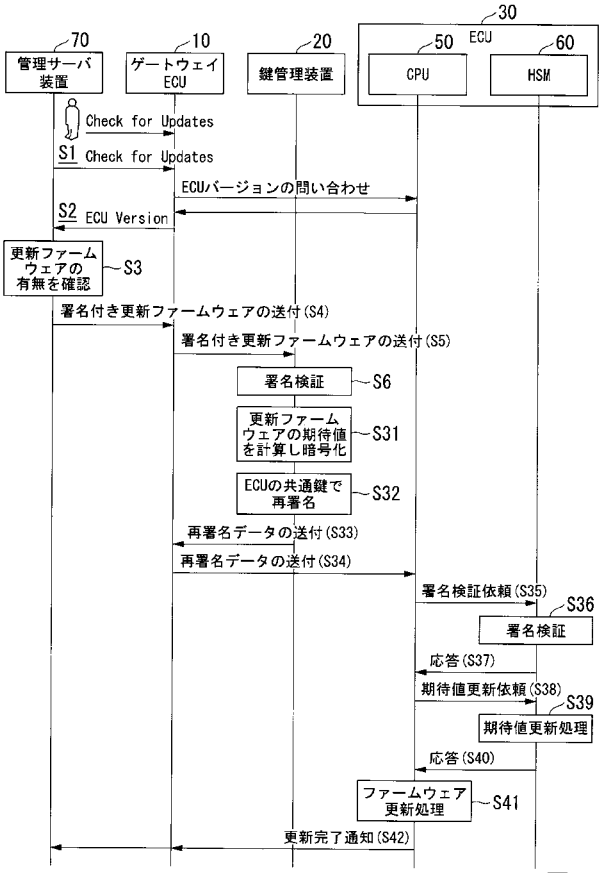
70
管理サーバ装置
10
ゲートウェイECU
20
鍵管理装置
30
ECU
50
CPU
60
HSM
Check for Updates
S1 Check for Updates
ECUバージョンの問い合わせ
S2 ECU Version
更新ファームウェアの有無を確認
S3
署名付き更新ファームウェアの送付(S4)
署名付き更新ファームウェアの送付(S5)
署名検証
S6
更新ファームウェアの期待値を計算し暗号化
S31
ECUの共通鍵で再署名
S32
再署名データの送付(S33)
再署名データの送付(S34)
署名検証依頼(S35)
S36
署名検証
応答(S37)
期待値更新依頼(S38)
S39
期待値更新処理
応答(S40)
ファームウェア更新処理
S41
更新完了通知(S42)

図７

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	Ｂ６０Ｒ　16/02　　６６０Ｕ	

(72)発明者　窪田　歩
埼玉県ふじみ野市大原二丁目１番１５号　株式会社ＫＤＤＩ研究所内

Ｆターム(参考) 5J104 AA08 AA12 AA18 JA03 JA21 LA02 LA03 LA06 MA02 NA37 NA42