(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2016 年 12 月 29 日(29.12.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/208227 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G06F 21/60* (2013.01)
G06F 21/44 (2013.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2016/057087

(22) 国際出願日: 2016 年 3 月 8 日(08.03.2016)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2015-124781 2015 年 6 月 22 日(22.06.2015) JP

(71) 出願人: ＫＤＤＩ株式会社(KDDI CORPORATION) [JP/JP]; 〒1638003 東京都新宿区西新宿二丁目３番２号 Tokyo (JP).

(72) 発明者: 竹森　敬祐(TAKEMORI Keisuke); 〒3568502 埼玉県ふじみ野市大原２丁目１番１５号　株式会社ＫＤＤＩ研究所内 Saitama (JP).

(74) 代理人: 棚井　澄雄，外(TANAI Sumio et al.); 〒1006620 東京都千代田区丸の内一丁目９番２号 Tokyo (JP).

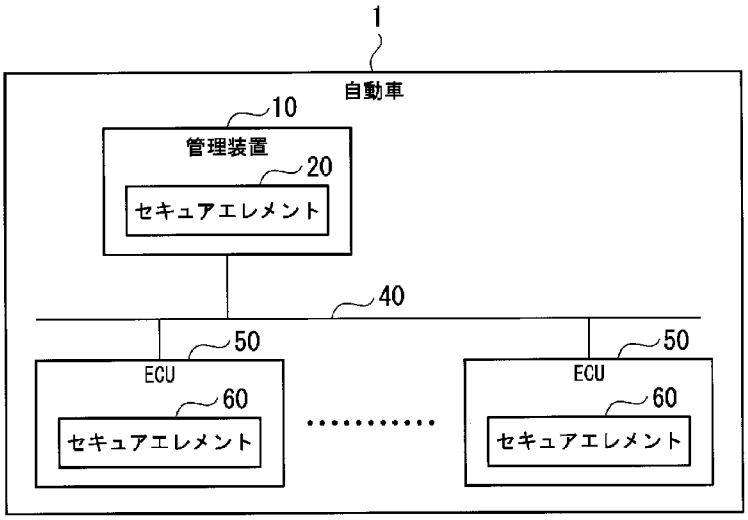
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: MANAGEMENT SYSTEM, VEHICLE, MANAGEMENT DEVICE, VEHICLE-MOUNTED COMPUTER, MANAGEMENT METHOD, AND COMPUTER PROGRAM

(54) 発明の名称 : 管理システム、車両、管理装置、車載コンピュータ、管理方法、及びコンピュータプログラム



1 Automobile
10 Management device
20, 60 Secure element

(57) **Abstract**: This management system is provided with a vehicle-related management device and a vehicle-mounted computer, the management device and the vehicle-mounted computer communicating with one another by way of a communication network provided in a vehicle. The management device and the vehicle-mounted computer are provided in common with a key storage unit which stores a root private key and a root certificate, which is a public key certificate of a root public key forming a pair with the root private key. The management system uses the pair comprising the root certificate and the root private key stored in the key storage unit to issue a public key certificate to be used in a public key encryption scheme.

(57) 要約: 管理システムは、車両に備わる管理装置と車載コンピュータを備え、前記管理装置と前記車載コンピュータとが前記車両に備わる通信ネットワークを介して通信する管理システムであって、前記管理装置と前記車載コンピュータとが、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、共通して備え、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する。

WO 2016/208227 A1

明　細　書

発明の名称 ：

管理システム、車両、管理装置、車載コンピュータ、管理方法、及びコンピュータプログラム

技術分野

[0001] 本発明は、管理システム、車両、管理装置、車載コンピュータ、管理方法、及びコンピュータプログラムに関する。

本願は、２０１５年６月２２日に、日本に出願された特願２０１５－１２４７８１号に基づき優先権を主張し、その内容をここに援用する。

背景技術

[0002] 近年、自動車は、ＥＣＵ（Electronic Control Unit）を有し、ＥＣＵによってエンジン制御等の機能を実現する。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。既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は、通常、自動車の検査時や定期点検時などに、一般の自動車整備工場で行われる。

[0003] 従来、ＥＣＵのコンピュータプログラムの更新では、作業者が、自動車のＯＢＤ（On-board Diagnostics）ポートと呼ばれる診断ポートにメンテナンス専用の診断端末を接続し、該診断端末から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。これ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

[0004] 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：高田広章、松本勉、“車載組込みシステムの情報セキュリティ強化に関する提言”、2013年9月、インターネット＜ＵＲＬ：https://www.ipa.go.jp/files/000034668.pdf＞

非特許文献3：Trusted Computing Group、インターネット＜ＵＲＬ：http://www.trustedcomputinggroup.org/＞

発明の概要

発明が解決しようとする課題

[0005] 上述した非特許文献１、２では、セキュリティの向上を実現する手段については記載されない。このため、自動車等の車両に備わるＥＣＵ等の車載コンピュータ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が起動した後に、ＥＣＵが保持する鍵を使用してデータの交換相手を相互認証することによって、車載コンピュータシステムの防御能力を向上させることが考えられる。また、例えば、ＥＣＵが保持する鍵を使用して、ＥＣＵ間で交換するデータの正当性を検証することが考えられる。また、例えば、ＥＣＵに使用されるコンピュータプログラム等のデータに電子署名を付して自動車の管理装置へ配布し、管理装置が保持する鍵を使用して、配布されたデータの電子署名を検証することにより、ＥＣＵに使用されるコンピュータプログラム等のデータを検査することが考えられる。ここで、自動車に保持される鍵の管理や更新をどのようにして実現するのかが、鍵の保安上の課題である。

[0006] 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、自動車等の車両に保持される鍵の管理や更新に寄与できる、管理システム、車両、管理装置、車載コンピュータ、管理方法、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

[0007] （１）：本発明の一態様は、車両に備わる管理装置と車載コンピュータを備え、前記管理装置と前記車載コンピュータとが前記車両に備わる通信ネットワークを介して通信する管理システムであって、前記管理装置と前記車載コンピュータとが、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、共通

して備え、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する。

（２）：本発明の一態様は、上記（１）の管理システムであって、前記管理装置は、公開鍵と秘密鍵のペアを生成する鍵生成部と、前記管理装置の鍵記憶部に記憶されるＲｏｏｔ秘密鍵を使用して、前記鍵生成部により生成された公開鍵の電子署名を生成する暗号処理部と、を備え、前記鍵生成部により生成された公開鍵と前記暗号処理部により生成された電子署名とから構成される公開鍵証明書を前記車載コンピュータへ送信し、前記車載コンピュータは、前記管理装置から受信した公開鍵証明書を、前記車載コンピュータの鍵記憶部に記憶されるＲｏｏｔ証明書を使用して検証する検証部を備えていてもよい。

（３）：本発明の一態様は、上記（２）の管理システムであって、前記車載コンピュータは、公開鍵と秘密鍵のペアを生成する鍵生成部と、前記車載コンピュータの鍵記憶部に記憶されるＲｏｏｔ秘密鍵を使用して、前記車載コンピュータの鍵生成部により生成された公開鍵の電子署名を生成する暗号処理部と、を備え、前記車載コンピュータの鍵生成部により生成された公開鍵と前記車載コンピュータの暗号処理部により生成された電子署名とから構成される公開鍵証明書を前記管理装置へ送信し、前記管理装置は、前記車載コンピュータから受信した公開鍵証明書を、前記管理装置の鍵記憶部に記憶されるＲｏｏｔ証明書を使用して検証する検証部を備えていてもよい。

（４）：本発明の一態様は、上記（３）の管理システムであって、前記管理装置の鍵生成部は鍵を生成し、前記管理装置の暗号処理部は、前記車載コンピュータへ送信した公開鍵証明書の公開鍵とペアの秘密鍵を使用して、前記管理装置の鍵生成部により生成された鍵の電子署名を生成し、当該鍵と当該電子署名とから構成される鍵証明書を前記車載コンピュータから受信した公開鍵証明書の公開鍵で暗号化し、前記管理装置は前記鍵証明書の暗号化データを前記車載コンピュータへ送信し、前記車載コンピュータの暗号処理部は、前記管理装置から受信した鍵証明書の暗号化データを、前記管理装置へ

送信した公開鍵証明書の公開鍵とペアの秘密鍵で復号化し、前記車載コンピュータの検証部は、前記鍵証明書の暗号化データの復号化データを、前記管理装置から受信した公開鍵証明書の公開鍵を使用して検証してもよい。

（５）：本発明の一態様は、上記（１）から（４）のいずれかの管理システムであって、前記管理装置の鍵生成部は、新Ｒｏｏｔ公開鍵と新Ｒｏｏｔ秘密鍵のペアを生成し、前記管理装置の暗号処理部は、前記管理装置の鍵記憶部に記憶されるＲｏｏｔ秘密鍵を使用して前記新Ｒｏｏｔ公開鍵の電子署名を生成し、前記管理装置の鍵記憶部は、前記新Ｒｏｏｔ秘密鍵と、前記新Ｒｏｏｔ公開鍵と当該新Ｒｏｏｔ公開鍵の電子署名とから構成される公開鍵証明書である新Ｒｏｏｔ証明書とを記憶し、前記管理装置は、前記新Ｒｏｏｔ秘密鍵と前記新Ｒｏｏｔ証明書を、前記車載コンピュータとの間で共有する暗号路鍵で暗号化して前記車載コンピュータへ送信し、前記車載コンピュータは、前記管理装置から受信した前記新Ｒｏｏｔ秘密鍵と前記新Ｒｏｏｔ証明書の暗号化データを前記暗号路鍵で復号化し、前記車載コンピュータの検証部は、復号化された前記新Ｒｏｏｔ証明書を、前記車載コンピュータの鍵記憶部に記憶されるＲｏｏｔ証明書を使用して検証し、前記車載コンピュータの鍵記憶部は、前記新Ｒｏｏｔ証明書の検証が成功である場合に、前記新Ｒｏｏｔ秘密鍵と前記新Ｒｏｏｔ証明書を記憶してもよい。

[0008] （６）：本発明の一態様は、上記（１）から（５）のいずれかの管理システムを備える車両である。

[0009] （７）：本発明の一態様は、車両に備わる通信ネットワークを介して前記車両に備わる車載コンピュータと通信する前記車両に備わる管理装置であって、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、前記車載コンピュータと共通して備え、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する。

[0010] （８）：本発明の一態様は、車両に備わる通信ネットワークを介して前記

車両に備わる管理装置と通信する前記車両に備わる車載コンピュータであって、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、前記管理装置と共通して備え、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する。

[0011] （９）：本発明の一態様は、車両に備わる管理装置と車載コンピュータを備え、前記管理装置と前記車載コンピュータとが前記車両に備わる通信ネットワークを介して通信する管理システムの管理方法であって、前記管理装置と前記車載コンピュータとが、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを、共通して各々の鍵記憶部に記憶するステップと、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行するステップと、を含む。

[0012] （１０）：本発明の一態様は、車両に備わる通信ネットワークを介して前記車両に備わる車載コンピュータと通信する前記車両に備わる管理装置のコンピュータに、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを、前記車載コンピュータと共通して鍵記憶部に記憶するステップと、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行するステップと、を実行させるためのコンピュータプログラムである。

[0013] （１１）：本発明の一態様は、車両に備わる通信ネットワークを介して前記車両に備わる管理装置と通信する前記車両に備わる車載コンピュータに、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを、前記管理装置と共通して鍵記憶部に記憶するステップと、前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行するステップと、を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

[0014] 本発明によれば、自動車等の車両に保持される鍵の管理や更新に寄与できるという効果が得られる。

図面の簡単な説明

[0015] [図1]第１実施形態に係る自動車を示す図である。

[図2]第１実施形態に係る管理装置を示す構成図である。

[図3]図２に示す鍵記憶部の構成を示す図である。

[図4]第１実施形態に係るＥＣＵを示す構成図である。

[図5]図４に示す鍵記憶部の構成を示す図である。

[図6]第１の実施形態に係る管理方法のシーケンスチャートである。

[図7]第１の実施形態に係る管理方法のシーケンスチャートである。

[図8]第１の実施形態に係る管理方法のシーケンスチャートである。

[図9]第１の実施形態に係る管理方法のシーケンスチャートである。

[図10]第２実施形態に係る管理システムを示す図である。

[図11]第２実施形態に係る管理装置を示す構成図である。

発明を実施するための形態

[0016] 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。

[0017] ［第１実施形態］

図１は、第１実施形態に係る自動車１を示す図である。図１において、自動車１は管理装置１０とＥＣＵ５０を備える。管理装置１０は制御用車載ネットワーク４０に接続される。制御用車載ネットワーク４０として、例えばＣＡＮ（Controller Area Network）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、制御用車載ネットワーク４０はＣＡＮである。制御用車載ネットワーク４０には、各種のＥＣＵ５０が接続される。ＥＣＵ５０は、自動車１に備わる車載コンピュータである。ＥＣＵ５０は、例えば、駆動系ＥＣＵ、車体系ＥＣＵ、安全制御系ＥＣＵなどである。管理装置１０は、制御用車載ネットワーク４０を

介して、各ＥＣＵ５０との間でデータを交換する。ＥＣＵ５０は、制御用車載ネットワーク４０を介して、他のＥＣＵ５０との間でデータを交換する。

[0018] 管理装置１０はセキュアエレメント２０を備える。ＥＣＵ５０はセキュアエレメント６０を備える。

[0019] 図２は、第１実施形態に係る管理装置１０を示す構成図である。図２において、管理装置１０は、制御部１１とＣＡＮインタフェース１２とセキュアエレメント２０を備える。

これら各部はデータを交換できるように構成される。セキュアエレメント２０は、鍵生成部２１と鍵記憶部２２と検証部２３と暗号処理部２４を備える。

[0020] 制御部１１は管理装置１０の制御機能を有する。ＣＡＮインタフェース１２は、ＥＣＵ５０と通信する通信部である。ＣＡＮインタフェース１２は、制御用車載ネットワーク４０と接続し、制御用車載ネットワーク４０を介して各ＥＣＵ５０とデータを交換する。セキュアエレメント２０は耐タンパー性（Tamper Resistant）を有する。

[0021] セキュアエレメント２０において、鍵生成部２１は鍵を生成する。鍵記憶部２２は鍵を記憶する。検証部２３は、データの交換についての検証を行う。暗号処理部２４は、データの暗号化と暗号化データの復号化とを行う。

[0022] 図３は、図２に示す鍵記憶部２２の構成を示す図である。図３において、鍵記憶部２２は、Ｒｏｏｔ証明書記憶部３１とＲｏｏｔ秘密鍵記憶部３２とＳ公開鍵証明書記憶部３３とＳ秘密鍵記憶部３４とＣ公開鍵証明書記憶部３５とＭＡＣ鍵記憶部３６を備える。

[0023] Ｒｏｏｔ証明書記憶部３１はＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐを記憶する。Ｒｏｏｔ秘密鍵記憶部３２はＲｏｏｔ秘密鍵ＫＲｓを記憶する。Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐは公開鍵の証明書である。Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐが証明する公開鍵はＲｏｏｔ公開鍵ＫＲｐである。Ｒｏｏｔ秘密鍵ＫＲｓは、Ｒｏｏｔ公開鍵ＫＲｐとペアの秘密鍵である。Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓとは、例えば管理装置１０の製造時

などに、安全にセキュアエレメント２０に書き込まれる。セキュアエレメント２０に書き込まれたＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐは、Ｒｏｏｔ証明書記憶部３１に記憶される。セキュアエレメント２０に書き込まれたＲｏｏｔ秘密鍵ＫＲｓは、Ｒｏｏｔ秘密鍵記憶部３２に記憶される。Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ及びＲｏｏｔ秘密鍵ＫＲｓについては、平文のままでセキュアエレメント２０から外部に出力させないように管理し秘匿することが好ましい。

[0024] Ｓ公開鍵証明書記憶部３３はＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐを記憶する。Ｓ秘密鍵記憶部３４はＳ秘密鍵ＫＳｓを記憶する。Ｓ公開鍵証明書ＫＳｐは公開鍵の証明書である。

Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐが証明する公開鍵はＳ公開鍵ＫＳｐである。Ｓ秘密鍵ＫＳｓは、Ｓ公開鍵ＫＳｐとペアの秘密鍵である。Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐとＳ秘密鍵ＫＳｓとは鍵生成部２１によって生成される。鍵生成部２１によって生成されたＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐは、Ｓ公開鍵証明書記憶部３３に記憶される。鍵生成部２１によって生成されたＳ秘密鍵ＫＳｓは、Ｓ秘密鍵記憶部３４に記憶される。

[0025] Ｃ公開鍵証明書記憶部３５はＣ公開鍵証明書を記憶する。Ｃ公開鍵証明書は、ＥＣＵ５０毎に存在する。Ｃ公開鍵証明書記憶部３５は、各ＥＣＵ５０のＣ公開鍵証明書を記憶する。あるＥＣＵ５０のＣ公開鍵証明書は、当該ＥＣＵ５０の公開鍵の証明書である。例えば、自動車１に備わるＥＣＵ５０のうちの一つである第１のＥＣＵ５０のＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐが証明する公開鍵はＣ公開鍵ＫＣ１ｐである。Ｃ公開鍵ＫＣ１ｐは、第１のＥＣＵ５０の公開鍵である。Ｃ公開鍵ＫＣ１ｐは、第１のＥＣＵ５０の秘密鍵であるＣ秘密鍵ＫＣ１ｓとペアである。各ＥＣＵ５０から受信されたＣ公開鍵証明書は、Ｃ公開鍵証明書記憶部３５に記憶される。

[0026] ＭＡＣ鍵記憶部３６はＭＡＣ鍵Ｋｍを記憶する。ＭＡＣ鍵Ｋｍは鍵生成部２１によって生成される共通鍵である。鍵生成部２１によって生成されたＭＡＣ鍵Ｋｍは、ＭＡＣ鍵記憶部３６に記憶される。ＭＡＣ鍵Ｋｍは、例えば

、ＥＣＵ５０間のデータ交換の際に使用される。

[0027] 図４は、第１実施形態に係るＥＣＵ５０を示す構成図である。図４において、ＥＣＵ５０は、制御部５１とＣＡＮインタフェース５２とセキュアエレメント６０を備える。これら各部はデータを交換できるように構成される。セキュアエレメント６０は、鍵生成部６１と鍵記憶部６２と検証部６３と暗号処理部６４を備える。

[0028] 制御部５１は、ＥＣＵ５０に対応する所定の制御機能を備える。ＣＡＮインタフェース５２は、管理装置１０や他のＥＣＵ５０と通信する通信部である。ＣＡＮインタフェース５２は、制御用車載ネットワーク４０と接続し、制御用車載ネットワーク４０を介して管理装置１０や他のＥＣＵ５０とデータを交換する。セキュアエレメント６０は耐タンパー性を有する。

[0029] セキュアエレメント６０において、鍵生成部６１は鍵を生成する。鍵記憶部６２は鍵を記憶する。検証部６３は、データの交換についての検証を行う。暗号処理部６４は、データの暗号化と暗号化データの復号化とを行う。

[0030] 図５は、図４に示す鍵記憶部６２の構成を示す図である。図５において、鍵記憶部６２は、Ｒｏｏｔ証明書記憶部７１とＲｏｏｔ秘密鍵記憶部７２とＣ公開鍵証明書記憶部７３とＣ秘密鍵記憶部７４とＳ公開鍵証明書記憶部７５とＭＡＣ鍵記憶部７６を備える。

[0031] Ｒｏｏｔ証明書記憶部７１は、管理装置１０と同じＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐを記憶する。Ｒｏｏｔ秘密鍵記憶部７２は、管理装置１０と同じＲｏｏｔ秘密鍵ＫＲｓを記憶する。したがって、管理装置１０と各ＥＣＵ５０とは、同一のＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓのペアを備える。Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓとは、例えばＥＣＵ５０の製造時などに、安全にセキュアエレメント６０に書き込まれる。セキュアエレメント６０に書き込まれたＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐは、Ｒｏｏｔ証明書記憶部７１に記憶される。セキュアエレメント６０に書き込まれたＲｏｏｔ秘密鍵ＫＲｓは、Ｒｏｏｔ秘密鍵記憶部７２に記憶される。Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ及びＲｏｏｔ秘密鍵ＫＲｓ

については、平文のままでセキュアエレメント６０から外部に出力させないように管理し秘匿することが好ましい。

[0032] Ｃ公開鍵証明書記憶部７３はＣ公開鍵証明書を記憶する。Ｃ秘密鍵記憶部７４はＣ秘密鍵を記憶する。Ｃ公開鍵証明書は公開鍵の証明書である。Ｃ秘密鍵は、Ｃ公開鍵証明書の公開鍵とペアの秘密鍵である。Ｃ公開鍵証明書とＣ秘密鍵とは鍵生成部６１によって生成される。鍵生成部６１によって生成されたＣ公開鍵証明書は、Ｃ公開鍵証明書記憶部７３に記憶される。鍵生成部６１によって生成されたＣ秘密鍵は、Ｃ秘密鍵記憶部７４に記憶される。例えば、第１のＥＣＵ５０のＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐは、第１のＥＣＵ５０のＣ公開鍵ＫＣ１ｐの証明書である。Ｃ公開鍵ＫＣ１ｐは、第１のＥＣＵ５０のＣ秘密鍵ＫＣ１ｓとペアである。第１のＥＣＵ５０の鍵生成部６１によって生成されたＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐは、第１のＥＣＵ５０のＣ公開鍵証明書記憶部７３に記憶される。第１のＥＣＵ５０の鍵生成部６１によって生成されたＣ秘密鍵ＫＣ１ｓは、第１のＥＣＵ５０のＣ秘密鍵記憶部７４に記憶される。

[0033] Ｓ公開鍵証明書記憶部７５は管理装置１０のＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐを記憶する。管理装置１０から受信されたＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐは、Ｓ公開鍵証明書記憶部７５に記憶される。

[0034] ＭＡＣ鍵記憶部７６はＭＡＣ鍵Ｋｍを記憶する。管理装置１０から受信されたＭＡＣ鍵Ｋｍは、ＭＡＣ鍵記憶部７６に記憶される。

[0035] 次に、図６から図９を参照して第１実施形態に係る管理方法を説明する。なお、以下の説明において、管理装置１０とＥＣＵ５０とは、制御用車載ネットワーク４０を介してデータを送受する。管理装置１０のセキュアエレメント２０は、ＣＡＮインタフェース１２を介して、ＥＣＵ５０のセキュアエレメント６０とデータを送受する。ＥＣＵ５０のセキュアエレメント６０は、ＣＡＮインタフェース５２を介して、管理装置１０のセキュアエレメント２０とデータを送受する。これにより、管理装置１０のセキュアエレメント２０とＥＣＵ５０のセキュアエレメント６０との間でデータの交換が行われ

る。

[0036] ［公開鍵証明書の更新段階］

図６を参照して、公開鍵証明書の更新段階を説明する。図６は、第１の実施形態に係る管理方法のシーケンスチャートである。ここでは、説明の便宜上、自動車１に備わるＥＣＵ５０のうちの一つである第１のＥＣＵ５０を例に挙げて説明するが、他のＥＣＵ５０についても同様である。

[0037] （ステップＳ１）：管理装置１０のセキュアエレメント２０において、鍵生成部２１が、Ｓ公開鍵ＫＳｐとＳ秘密鍵ＫＳｓのペアを生成する。公開鍵と秘密鍵のペアの生成方法として、例えば、ＲＳＡ（Rivest Shamir Adleman）やＥＣＣ（Elliptic Curve Cryptosystems）などが利用可能である。さらに、鍵生成部２１が、生成したＳ公開鍵ＫＳｐのＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐを生成する。Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐは、Ｓ公開鍵ＫＳｐと、Ｓ公開鍵ＫＳｐの電子署名とから構成される。Ｓ公開鍵ＫＳｐの電子署名は、Ｓ公開鍵ＫＳｐのハッシュ値をＲｏｏｔ秘密鍵ＫＲｓで暗号化した結果の暗号化データである。

[0038] Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐの生成において、まず鍵生成部２１が、Ｓ公開鍵ＫＳｐのハッシュ値ｈａｓｈ（ＫＳｐ）を算出する。次いで、暗号処理部２４が、鍵生成部２１により算出されたハッシュ値ｈａｓｈ（ＫＳｐ）を、Ｒｏｏｔ秘密鍵記憶部３２に記憶されるＲｏｏｔ秘密鍵ＫＲｓで暗号化する。この暗号化データＫＲｓ（ｈａｓｈ（ＫＳｐ））はＳ公開鍵ＫＳｐの電子署名である。次いで、鍵生成部２１が、Ｓ公開鍵ＫＳｐとＳ公開鍵ＫＳｐの電子署名ＫＲｓ（ｈａｓｈ（ＫＳｐ））とからＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」を構成する。

[0039] Ｓ公開鍵証明書記憶部３３は、鍵生成部２１により生成されたＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」を記憶する。Ｓ秘密鍵記憶部３４は、鍵生成部２１により生成されたＳ秘密鍵ＫＳｓを記憶する。また、Ｓ公開鍵証明書記憶部３３に記憶されるＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」とＳ秘密鍵記

憶部３４に記憶されるＳ秘密鍵ＫＳｓとがペアであることを示す関連付け情報を設定する。

[0040] （ステップＳ２）：第１のＥＣＵ５０のセキュアエレメント６０において、鍵生成部６１が、Ｃ公開鍵ＫＣ１ｐとＣ秘密鍵ＫＣ１ｓのペアを生成する。さらに、鍵生成部６１が、生成したＣ秘密鍵ＫＣ１ｓのＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐを生成する。Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐは、Ｃ公開鍵ＫＣ１ｐと、Ｃ公開鍵ＫＣ１ｐの電子署名とから構成される。Ｃ公開鍵ＫＣ１ｐの電子署名は、Ｃ公開鍵ＫＣ１ｐのハッシュ値をＲｏｏｔ秘密鍵ＫＲｓで暗号化した結果の暗号化データである。

[0041] Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐの生成において、まず鍵生成部６１が、Ｃ公開鍵ＫＣ１ｐのハッシュ値ｈａｓｈ（ＫＣ１ｐ）を算出する。次いで、暗号処理部６４が、鍵生成部６１により算出されたハッシュ値ｈａｓｈ（ＫＣ１ｐ）を、Ｒｏｏｔ秘密鍵記憶部７２に記憶されるＲｏｏｔ秘密鍵ＫＲｓで暗号化する。この暗号化データＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））はＣ公開鍵ＫＣ１ｐの電子署名である。次いで、鍵生成部６１が、Ｃ公開鍵ＫＣ１ｐとＣ公開鍵ＫＣ１ｐの電子署名ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））とからＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」を構成する。

[0042] Ｃ公開鍵証明書記憶部７３は、鍵生成部６１により生成されたＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」を記憶する。Ｃ秘密鍵記憶部７４は、鍵生成部６１により生成されたＣ秘密鍵ＫＣ１ｓを記憶する。また、Ｃ公開鍵証明書記憶部７３に記憶されるＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」とＣ秘密鍵記憶部７４に記憶されるＣ秘密鍵ＫＣ１ｓとがペアであることを示す関連付け情報を設定する。

[0043] （ステップＳ３:公開鍵証明書の送付）：管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、上記のステップＳ１で生成されたＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ

））」を第１のＥＣＵ５０のセキュアエレメント６０へ送信する。

[0044] （ステップＳ４）：第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、管理装置１０のセキュアエレメント２０からＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」を受信する。第１のＥＣＵ５０のセキュアエレメント６０において、検証部６３が、管理装置１０のセキュアエレメント２０から受信したＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」を検証する。

[0045] Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」の検証において、まず検証部６３が、Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」からＳ公開鍵ＫＳｐを取得し、取得したＳ公開鍵ＫＳｐのハッシュ値ｈａｓｈ（ＫＳｐ）を算出する。次いで、検証部６３が、Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」から電子署名ＫＲｓ（ｈａｓｈ（ＫＳｐ））を取得し、取得した電子署名ＫＲｓ（ｈａｓｈ（ＫＳｐ））を、Ｒｏｏｔ証明書記憶部７１に記憶されるＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐのＲｏｏｔ公開鍵ＫＲｐで復号化する。

この復号化により、復号化データ「ＫＲｐ・ＫＲｓ（ｈａｓｈ（ＫＳｐ））」が得られる。次いで、検証部６３が、算出したハッシュ値ｈａｓｈ（ＫＳｐ）と、復号化データ「ＫＲｐ・ＫＲｓ（ｈａｓｈ（ＫＳｐ））」とが一致するかを判定する。この判定の結果、一致する場合にはＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」の検証が成功であり、不一致する場合にはＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」の検証が失敗である。

[0046] Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」の検証が成功である場合には、検証部６３が、Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」をＳ公開鍵証明書記憶部７５に記憶させる。この後、ステップＳ５に進む。

[0047] 一方、Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」の検証が失敗である場合には、図６の処理を終了する。よって、Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」は、Ｓ公開鍵証明書記憶部７５に記憶されない。また、Ｓ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」の検証が失敗である場合に、制御部５１が所定のエラー処理を実行してもよい。

[0048] （ステップＳ５：公開鍵証明書の送付）：第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、上記のステップＳ２で生成されたＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」を管理装置１０のセキュアエレメント２０へ送信する。

[0049] （ステップＳ６）：管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、第１のＥＣＵ５０のセキュアエレメント６０からＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」を受信する。管理装置１０のセキュアエレメント２０において、検証部２３が、第１のＥＣＵ５０のセキュアエレメント６０から受信したＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」を検証する。

[0050] Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」の検証において、まず検証部２３が、Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」からＣ公開鍵ＫＣ１ｐを取得し、取得したＣ公開鍵ＫＣ１ｐのハッシュ値ｈａｓｈ（ＫＣ１ｐ）を算出する。次いで、検証部２３が、Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」から電子署名ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））を取得し、取得した電子署名ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））を、Ｒｏｏｔ証明書記憶部３１に記憶されるＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐのＲｏｏｔ公開鍵ＫＲｐで復号化する。この復号化により、復号化データ「ＫＲｐ・ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」が得られる。次いで、検証部２３が、算出したハッシュ値ｈａｓｈ（ＫＣ１ｐ）と、復号化データ「

ＫＲｐ・ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」とが一致するかを判定する。この判定の結果、一致する場合にはＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」の検証が成功であり、不一致する場合にはＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」の検証が失敗である。

[0051] Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」の検証が成功である場合には、検証部２３が、Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」をＣ公開鍵証明書記憶部３５に記憶させる。この後、図６の処理を終了する。

[0052] 一方、Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」の検証が失敗である場合には、図６の処理を終了する。よって、Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」は、Ｃ公開鍵証明書記憶部３５に記憶されない。また、Ｃ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」の検証が失敗である場合に、制御部１１が所定のエラー処理を実行してもよい。

[0053] 上述した公開鍵証明書の更新段階によれば、自動車１の内部に閉じて、管理装置１０がＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐを発行し、また、ＥＣＵ５０がＣ公開鍵証明書を発行することができる。このため、一般のＰＫＩ（Public Key Infrastructure、公開鍵基盤）を使用することなく、自動車１の内部に閉じて公開鍵証明書の発行を行うことができる。

これにより、一般のＰＫＩを使用することなく自動車１の内部に閉じた公開鍵暗号方式を実現することができる。また、公開鍵暗号方式を使用して自動車１の内部のデータの秘匿を図る際に、自動車１の外部に存在するＰＫＩを使用するための通信が不要となるので、通信装置を削減すること、通信ができない環境に適用すること、公開鍵証明書の発行頻度を容易に増加させることなどの効果が得られる。

[0054] なお、管理装置１０及びＥＣＵ５０は、比較的短い周期で繰り返し公開鍵

と秘密鍵のペアを生成して公開鍵証明書を発行し、公開鍵証明書の発行の度に公開鍵証明書を新しいものに交換するようにしてもよい。これにより、公開鍵の失効リスト（リボケーションリスト）の管理を省略してもよい。

[0055] ［ＭＡＣ鍵の更新段階］

図７を参照して、ＭＡＣ鍵の更新段階を説明する。図７は、第１の実施形態に係る管理方法のシーケンスチャートである。ここでは、説明の便宜上、自動車１に備わるＥＣＵ５０のうちの一つである第１のＥＣＵ５０を例に挙げて説明するが、他のＥＣＵ５０についても同様である。

[0056] （ステップＳ１１）：管理装置１０のセキュアエレメント２０において、鍵生成部２１が、ＭＡＣ鍵Ｋｍを生成する。次いで、鍵生成部２１が、生成したＭＡＣ鍵Ｋｍに対して電子署名を施す。ＭＡＣ鍵Ｋｍに対する電子署名では、まず鍵生成部２１が、ＭＡＣ鍵Ｋｍのハッシュ値ｈａｓｈ（Ｋｍ）を算出する。次いで、暗号処理部２４が、鍵生成部２１により算出されたハッシュ値ｈａｓｈ（Ｋｍ）を、Ｓ秘密鍵記憶部３４に記憶されるＳ秘密鍵ＫＳｓで暗号化する。この暗号化データＫＳｓ（ｈａｓｈ（Ｋｍ））はＭＡＣ鍵Ｋｍの電子署名である。次いで、鍵生成部２１が、ＭＡＣ鍵ＫｍとＭＡＣ鍵Ｋｍの電子署名ＫＳｓ（ｈａｓｈ（Ｋｍ））とからＭＡＣ鍵証明書「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」を構成する。ＭＡＣ鍵記憶部３６は、鍵生成部２１により生成されたＭＡＣ鍵Ｋｍを記憶する。

[0057] （ステップＳ１２：暗号路鍵の送付）：管理装置１０のセキュアエレメント２０において、暗号処理部２４が、Ｃ公開鍵証明書記憶部３５に記憶されるＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」からＣ公開鍵ＫＣ１ｐを取得する。次いで、暗号処理部２４が、取得したＣ公開鍵ＫＣ１ｐで、鍵生成部２１により生成されたＭＡＣ鍵証明書「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」を暗号化する。この暗号化データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）は暗号路鍵の送付データである。次いで、管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（

ｈａｓｈ（Ｋｍ））」）を第１のＥＣＵ５０のセキュアエレメント６０へ送信する。

[0058] （ステップＳ１３）：第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、管理装置１０のセキュアエレメント２０から暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）を受信する。第１のＥＣＵ５０のセキュアエレメント６０において、検証部６３が、管理装置１０のセキュアエレメント２０から受信した暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）を検証する。

[0059] 暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）の検証において、まず暗号処理部６４が、Ｃ秘密鍵記憶部７４に記憶されるＣ秘密鍵ＫＣ１ｓで、暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）を復号化する。

この復号化により、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）」が得られる。次いで、検証部６３が、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）」からＭＡＣ鍵Ｋｍを取得し、取得したＭＡＣ鍵Ｋｍのハッシュ値ｈａｓｈ（Ｋｍ）を算出する。

[0060] 次いで、検証部６３が、Ｓ公開鍵証明書記憶部７５に記憶されるＳ公開鍵証明書Ｃｅｒｔ＿ＫＳｐ「ＫＳｐ，ＫＲｓ（ｈａｓｈ（ＫＳｐ））」からＳ公開鍵ＫＳｐを取得する。

次いで、検証部６３が、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）」から電子署名ＫＳｓ（ｈａｓｈ（Ｋｍ））を取得し、取得した電子署名ＫＳｓ（ｈａｓｈ（Ｋｍ））をＳ公開鍵ＫＳｐで復号化する。この復号化により、復号化データ「ＫＳｐ・ＫＳｓ（ｈａｓｈ（Ｋｍ））」が得られる。

[0061] 次いで、検証部６３が、算出したハッシュ値ｈａｓｈ（Ｋｍ）と、復号化データ「ＫＳｐ・ＫＳｓ（ｈａｓｈ（Ｋｍ））」とが一致するかを判定する

。この判定の結果、一致する場合には暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）の検証が成功であり、不一致する場合には暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）の検証が失敗である。

[0062] 暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）の検証が成功である場合には、検証部６３が、暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）から取得したＭＡＣ鍵ＫｍをＭＡＣ鍵記憶部７６に記憶させる。この後、図７の処理を終了する。

[0063] 一方、暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）の検証が失敗である場合には、図７の処理を終了する。よって、暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）に含まれるＭＡＣ鍵Ｋｍは、ＭＡＣ鍵記憶部７６に記憶されない。また、暗号路鍵の送付データＫＣ１ｐ（「Ｋｍ，ＫＳｓ（ｈａｓｈ（Ｋｍ））」）の検証が失敗である場合に、制御部５１が所定のエラー処理を実行してもよい。

[0064] 上述したＭＡＣ鍵の更新段階によれば、自動車１で使用されるＭＡＣ鍵Ｋｍの更新を、自動車１の内部に閉じて、公開鍵暗号方式により安全に行うことができる。

[0065] ［Ｒｏｏｔ証明書の更新段階］

図８及び図９を参照して、Ｒｏｏｔ証明書の更新段階を説明する。図８及び図９は、第１の実施形態に係る管理方法のシーケンスチャートである。

[0066] （Ｒｏｏｔ証明書の初回更新段階）

まず図８を参照して、Ｒｏｏｔ証明書の初回更新段階を説明する。ここでは、説明の便宜上、管理装置１０及びＥＣＵ５０に最初に保持されるＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓのペアにおいて、Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐを初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐと称し、Ｒｏｏｔ公開鍵ＫＲｐを初期Ｒｏｏｔ公開鍵ＫＲｐと称し、Ｒｏｏｔ秘密鍵ＫＲｓを初期Ｒｏｏｔ秘密鍵ＫＲｓと称する。また、新規に生成されるＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓのペアにおいて、Ｒｏ

ｏｔ証明書Ｃｅｒｔ＿ＫＲｐを新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗと称し、Ｒｏｏｔ公開鍵ＫＲｐを新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと称し、Ｒｏｏｔ秘密鍵ＫＲｓを新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと称する。また、ここでは、自動車１に備わるＥＣＵ５０のうちの一つである第１のＥＣＵ５０を例に挙げて説明するが、他のＥＣＵ５０についても同様である。

[0067] （ステップＳ２１）：管理装置１０のセキュアエレメント２０において、鍵生成部２１が、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗのペアを生成する。

さらに、鍵生成部２１が、生成した新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの証明書である新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗを生成する。新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗは、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名とから構成される。新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名は、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗのハッシュ値を初期Ｒｏｏｔ秘密鍵ＫＲｓで暗号化した結果の暗号化データである。

[0068] 新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗの生成において、まず鍵生成部２１が、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗのハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）を算出する。次いで、暗号処理部２４が、鍵生成部２１により算出されたハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）を、Ｒｏｏｔ秘密鍵記憶部３２に記憶される初期Ｒｏｏｔ秘密鍵ＫＲｓで暗号化する。この暗号化データＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））は新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名である。次いで、鍵生成部２１が、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））とから新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を構成する。

[0069] Ｒｏｏｔ証明書記憶部３１は、鍵生成部２１により生成された新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を記憶する。Ｒｏｏｔ秘密鍵記憶部３２は、鍵生成部２

１により生成された新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗを記憶する。また、Ｒｏｏｔ証明書記憶部３１に記憶される新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とＲｏｏｔ秘密鍵記憶部３２に記憶される新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗとがペアであることを示す関連付け情報を設定する。

[0070] （ステップＳ２２：暗号路鍵の送付）：管理装置１０のセキュアエレメント２０において、鍵生成部２１が、暗号路鍵Ｋｃを生成する。次いで、暗号処理部２４が、Ｃ公開鍵証明書記憶部３５に記憶されるＣ公開鍵証明書Ｃｅｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」からＣ公開鍵ＫＣ１ｐを取得する。次いで、暗号処理部２４が、取得したＣ公開鍵ＫＣ１ｐで、鍵生成部２１により生成された暗号路鍵Ｋｃを暗号化する。この暗号化データＫＣ１ｐ（Ｋｃ）は暗号路鍵の送付データである。次いで、管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）を第１のＥＣＵ５０のセキュアエレメント６０へ送信する。

[0071] 第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、管理装置１０のセキュアエレメント２０から暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）を受信する。第１のＥＣＵ５０のセキュアエレメント６０において、暗号処理部６４が、管理装置１０のセキュアエレメント２０から受信した暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）を、Ｃ秘密鍵記憶部７４に記憶されるＣ秘密鍵ＫＣ１ｓで復号化する。この復号化により、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（Ｋｃ）」が得られる。暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）の復号化が成功すれば、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（Ｋｃ）」は暗号路鍵Ｋｃである。ここでは、暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）の復号化が成功し、暗号路鍵Ｋｃが得られたとする。

[0072] （ステップＳ２３：新Ｒｏｏｔ秘密鍵、新Ｒｏｏｔ証明書の送付）：管理装置１０のセキュアエレメント２０において、暗号処理部２４が、上記のステップＳ２２で鍵生成部２１により生成された暗号路鍵Ｋｃで、新Ｒｏｏｔ

秘密鍵ＫＲｓ＿ｎｅｗと、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とを暗号化する。これにより、暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）が得られる。次いで、管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）を第１のＥＣＵ５０のセキュアエレメント６０へ送信する。

[0073] （ステップＳ２４）：第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、管理装置１０のセキュアエレメント２０から暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）を受信する。第１のＥＣＵ５０のセキュアエレメント６０において、暗号処理部６４が、管理装置１０のセキュアエレメント２０から受信した暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）を、上記のステップＳ２２で暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）の復号化により得られた暗号路鍵Ｋｃで復号化する。この復号化により、復号化データ「Ｋｃ・Ｋｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）」が得られる。暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）の復号化が成功すれば、復号化データ「Ｋｃ・Ｋｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）」から、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とが得られる。ここでは、暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）の復号化が成功し、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とが得られたとする。次いで、検証部６３が、得られた新

Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を検証する。

[0074] 新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証において、まず検証部６３が、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」から新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗを取得し、取得した新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗのハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）を算出する。次いで、検証部６３が、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」から電子署名ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））を取得し、取得した電子署名ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））を、Ｒｏｏｔ証明書記憶部７１に記憶される初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐの初期Ｒｏｏｔ公開鍵ＫＲｐで復号化する。この復号化により、復号化データ「ＫＲｐ・ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」が得られる。

[0075] 次いで、検証部６３が、算出したハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）と、復号化データ「ＫＲｐ・ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とが一致するかを判定する。この判定の結果、一致する場合には新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が成功であり、不一致する場合には新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が失敗である。

[0076] 新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が成功である場合には、Ｒｏｏｔ証明書記憶部７１が、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を記憶する。Ｒｏｏｔ秘密鍵記憶部７２が、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗを記憶する。また、Ｒｏｏｔ証明書記憶部７１に記憶される新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とＲｏ

ｏｔ秘密鍵記憶部７２に記憶される新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗとがペアであることを示す関連付け情報を設定する。この後、図８の処理を終了する。

[0077] 一方、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が失敗である場合には、図８の処理を終了する。よって、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」は、Ｒｏｏｔ証明書記憶部７１に記憶されない。また、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が失敗である場合に、制御部５１が所定のエラー処理を実行してもよい。

[0078] （Ｒｏｏｔ証明書の２回目以降の更新段階）

次に図９を参照して、Ｒｏｏｔ証明書の２回目以降の更新段階を説明する。ここでは、説明の便宜上、管理装置１０及びＥＣＵ５０に保持される更新前のＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓのペアにおいて、Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐを旧Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｏｌｄと称し、Ｒｏｏｔ公開鍵ＫＲｐを旧Ｒｏｏｔ公開鍵ＫＲｐ＿ｏｌｄと称し、Ｒｏｏｔ秘密鍵ＫＲｓを旧Ｒｏｏｔ秘密鍵ＫＲｓ＿ｏｌｄと称する。また、新規に生成されるＲｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐとＲｏｏｔ秘密鍵ＫＲｓのペアにおいて、Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐを新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗと称し、Ｒｏｏｔ公開鍵ＫＲｐを新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと称し、Ｒｏｏｔ秘密鍵ＫＲｓを新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと称する。また、ここでは、自動車１に備わるＥＣＵ５０のうちの一つである第１のＥＣＵ５０を例に挙げて説明するが、他のＥＣＵ５０についても同様である。

[0079] （ステップＳ３１）：管理装置１０のセキュアエレメント２０において、鍵生成部２１が、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗのペアを生成する。

さらに、鍵生成部２１が、生成した新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの証

明書である新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗを生成する。新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗは、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名とから構成される。新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名は、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗのハッシュ値を旧Ｒｏｏｔ秘密鍵ＫＲｓ＿ｏｌｄで暗号化した結果の暗号化データである。

[0080] 新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗの生成において、まず鍵生成部２１が、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗのハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）を算出する。次いで、暗号処理部２４が、鍵生成部２１により算出されたハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）を、Ｒｏｏｔ秘密鍵記憶部３２に記憶される旧Ｒｏｏｔ秘密鍵ＫＲｓ＿ｏｌｄで暗号化する。この暗号化データＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））は新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名である。次いで、鍵生成部２１が、新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗと新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗの電子署名ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））とから新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を構成する。

[0081] Ｒｏｏｔ証明書記憶部３１は、鍵生成部２１により生成された新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を記憶する。Ｒｏｏｔ秘密鍵記憶部３２は、鍵生成部２１により生成された新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗを記憶する。また、Ｒｏｏｔ証明書記憶部３１に記憶される新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とＲｏｏｔ秘密鍵記憶部３２に記憶される新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗとがペアであることを示す関連付け情報を設定する。

[0082] （ステップＳ３２：暗号路鍵の送付）：管理装置１０のセキュアエレメント２０において、鍵生成部２１が、暗号路鍵Ｋｃを生成する。次いで、暗号処理部２４が、Ｃ公開鍵証明書記憶部３５に記憶されるＣ公開鍵証明書Ｃｅ

ｒｔ＿ＫＣ１ｐ「ＫＣ１ｐ，ＫＲｓ（ｈａｓｈ（ＫＣ１ｐ））」からＣ公開鍵ＫＣ１ｐを取得する。次いで、暗号処理部２４が、取得したＣ公開鍵ＫＣ１ｐで、鍵生成部２１により生成された暗号路鍵Ｋｃを暗号化する。この暗号化データＫＣ１ｐ（Ｋｃ）は暗号路鍵の送付データである。次いで、管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）を第１のＥＣＵ５０のセキュアエレメント６０へ送信する。

[0083] 第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、管理装置１０のセキュアエレメント２０から暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）を受信する。第１のＥＣＵ５０のセキュアエレメント６０において、暗号処理部６４が、管理装置１０のセキュアエレメント２０から受信した暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）を、Ｃ秘密鍵記憶部７４に記憶されるＣ秘密鍵ＫＣ１ｓで復号化する。この復号化により、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（Ｋｃ）」が得られる。暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）の復号化が成功すれば、復号化データ「ＫＣ１ｓ・ＫＣ１ｐ（Ｋｃ）」は暗号路鍵Ｋｃである。ここでは、暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）の復号化が成功し、暗号路鍵Ｋｃが得られたとする。

[0084] （ステップＳ３３：新Ｒｏｏｔ秘密鍵、新Ｒｏｏｔ証明書の送付）：管理装置１０のセキュアエレメント２０において、暗号処理部２４が、上記のステップＳ３２で鍵生成部２１により生成された暗号路鍵Ｋｃで、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とを暗号化する。これにより、暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）が得られる。次いで、管理装置１０のセキュアエレメント２０が、ＣＡＮインタフェース１２により、暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）を第１のＥＣＵ５０のセキュアエレメント６０へ送信する。

[0085] （ステップＳ３４）：第１のＥＣＵ５０のセキュアエレメント６０が、ＣＡＮインタフェース５２により、管理装置１０のセキュアエレメント２０から暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）を受信する。第１のＥＣＵ５０のセキュアエレメント６０において、暗号処理部６４が、管理装置１０のセキュアエレメント２０から受信した暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）を、上記のステップＳ３２で暗号路鍵の送付データＫＣ１ｐ（Ｋｃ）の復号化により得られた暗号路鍵Ｋｃで復号化する。この復号化により、復号化データ「Ｋｃ・Ｋｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）」が得られる。暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）の復号化が成功すれば、復号化データ「Ｋｃ・Ｋｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）」から、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とが得られる。ここでは、暗号化データＫｃ（ＫＲｓ＿ｎｅｗ，「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」）の復号化が成功し、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗと、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とが得られたとする。次いで、検証部６３が、得られた新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を検証する。

[0086] 新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証において、まず検証部６３が、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」から新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗを取得し、取得した新Ｒｏｏｔ公開鍵ＫＲｐ＿ｎｅｗのハッシュ値ｈ

ａｓｈ（ＫＲｐ＿ｎｅｗ）を算出する。次いで、検証部６３が、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」から電子署名ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））を取得し、取得した電子署名ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））を、Ｒｏｏｔ証明書記憶部７１に記憶される旧Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｏｌｄの旧Ｒｏｏｔ公開鍵ＫＲｐ＿ｏｌｄで復号化する。この復号化により、復号化データ「ＫＲｐ＿ｏｌｄ・ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」が得られる。

[0087] 次いで、検証部６３が、算出したハッシュ値ｈａｓｈ（ＫＲｐ＿ｎｅｗ）と、復号化データ「ＫＲｐ＿ｏｌｄ・ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とが一致するかを判定する。この判定の結果、一致する場合には新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が成功であり、不一致する場合には新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が失敗である。

[0088] 新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が成功である場合には、Ｒｏｏｔ証明書記憶部７１が、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」を記憶する。Ｒｏｏｔ秘密鍵記憶部７２が、新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗを記憶する。また、Ｒｏｏｔ証明書記憶部７１に記憶される新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」とＲｏｏｔ秘密鍵記憶部７２に記憶される新Ｒｏｏｔ秘密鍵ＫＲｓ＿ｎｅｗとがペアであることを示す関連付け情報を設定する。この後、図９の処理を終了する。

[0089] 一方、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が失敗である場合には、図９の処理を終了する。よって、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿

ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」は、Ｒｏｏｔ証明書記憶部７１に記憶されない。また、新Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐ＿ｎｅｗ「ＫＲｐ＿ｎｅｗ，ＫＲｓ＿ｏｌｄ（ｈａｓｈ（ＫＲｐ＿ｎｅｗ））」の検証が失敗である場合に、制御部５１が所定のエラー処理を実行してもよい。

[0090] 上述したＲｏｏｔ証明書の更新段階によれば、自動車１の内部に閉じて、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを更新することができる。このため、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを定期的に更新することにより、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアの信頼性を高めることができるので、一般のＰＫＩを使用することなく自動車１の内部に閉じた公開鍵暗号方式を実現する際の安全性が向上する。例えば、初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐと初期Ｒｏｏｔ秘密鍵ＫＲｓのペアを更新することなく使い続ける場合、耐タンパー性を有するセキュアエレメントであっても、漏洩電磁波解析の結果として初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐと初期Ｒｏｏｔ秘密鍵ＫＲｓのペアが漏洩する可能性を否定できない。このため、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを定期的に更新することは好ましい。また、初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐと初期Ｒｏｏｔ秘密鍵ＫＲｓのペアについては、信頼性の向上のために、できる限り使用回数を少なくすることは好ましい。例えば、初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐと初期Ｒｏｏｔ秘密鍵ＫＲｓのペアの使用は、所定回数（例えば１回のみ）に限定してもよい。

[0091] また、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアは自動車１毎に異なることが好ましい。

上述したＲｏｏｔ証明書の更新段階によれば、自動車１の内部に閉じてＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを更新することができるので、初期Ｒｏｏｔ証明書Ｃｅｒｔ＿ＫＲｐと初期Ｒｏｏｔ秘密鍵ＫＲｓのペアが各自動車１に共通であったとしても、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアの更新により、各自動車１のＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアが異なるようにすることができる。

[0092] ［第２実施形態］

図１０は、第２実施形態に係る管理システムを示す図である。図１０において図１の各部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。図１０において、管理システムは、管理装置１０ａと管理サーバ装置８０を備える。管理装置１０ａは自動車１に備わる。管理サーバ装置８０は、無線通信ネットワーク２の通信事業者に備わる。

[0093] 無線通信ネットワーク２を利用するためには、無線通信ネットワーク２の契約者情報が書き込まれたＳＩＭ（Subscriber Identity Module）又はｅＳＩＭ（Embedded Subscriber Identity Module）が必要である。管理装置１０ａは、ＳＩＭ＿２０ａを備える。ＳＩＭ＿２０ａは、無線通信ネットワーク２の契約者情報が書き込まれたＳＩＭである。よって、管理装置１０ａは、ＳＩＭ＿２０ａを使用することにより無線通信ネットワーク２を利用できる。管理装置１０ａは、ＳＩＭ＿２０ａを使用して確立される無線通信回線３により無線通信ネットワーク２に接続する。ＳＩＭ＿２０ａはセキュアエレメントである。

[0094] 管理サーバ装置８０は、無線通信ネットワーク２の通信事業者の通信回線４により無線通信ネットワーク２に接続する。管理装置１０ａと管理サーバ装置８０とは、無線通信ネットワーク２を介して通信する。

[0095] なお、管理装置１０ａと管理サーバ装置８０との間に無線通信ネットワーク２を介した専用線を確立し、管理装置１０ａと管理サーバ装置８０とが専用線を介してデータを送受するようにしてもよい。

[0096] 自動車１において、管理装置１０ａは制御用車載ネットワーク４０に接続される。本実施形態では、制御用車載ネットワーク４０はＣＡＮである。制御用車載ネットワーク４０には、各種のＥＣＵ５０が接続される。管理装置１０ａは、制御用車載ネットワーク４０を介して、各ＥＣＵ５０との間でデータを交換する。

[0097] 図１１は、第２実施形態に係る管理装置１０ａを示す構成図である。図１１において図２の各部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。図１１において、管理装置１０ａは、制御部１１とＣＡＮインタフェース１２と無線通信部１３とＳＩＭ＿２０ａを備える。これら各部はデータを交換できるように構成される。ＳＩＭ＿２０ａは、鍵生成部２１と鍵記憶部２２と検証部２３と暗号処理部２４を備える。第２実施形態においても、鍵記憶部２２の構成は上記の図３に示される構成と同じである。

[0098] ＳＩＭ＿２０ａは、セキュアエレメントであり、耐タンパー性を有する。なお、セキュアエレメントとして、ＳＩＭ＿２０ａの代わりにｅＳＩＭを利用してもよい。ＳＩＭ及びｅＳＩＭ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。

[0099] 無線通信部１３は無線通信によりデータを送受する。ＳＩＭ＿２０ａは、無線通信ネットワーク２の契約者情報が書き込まれたＳＩＭである。よって、無線通信部１３は、ＳＩＭ＿２０ａを使用することにより、無線通信回線３を介して無線通信ネットワーク２に接続する。

[0100] ＳＩＭ＿２０ａは、上記の図２に示すセキュアエレメント２０と同様の機能を実現する。これにより、上記の図６から図９を参照して説明した第１実施形態の管理方法が実現される。

[0101] 本実施形態では、ＳＩＭ＿２０ａは、無線通信部１３により、無線通信ネットワーク２を介して管理サーバ装置８０とデータを交換する。管理サーバ装置８０は、ＳＩＭ＿２０ａへ、Ｒｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを送信する。管理サーバ装置８０からＳＩＭ＿２０ａへＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを送信する際には、管理装置１０ａと管理サーバ装置８０との間に無線通信ネットワーク２を介した専用線を確立し、確立した専用線を介してデータを送受することが好ましい。

[0102] ＳＩＭ＿２０ａは、管理サーバ装置８０から受信したＲｏｏｔ証明書を、Ｒｏｏｔ証明書記憶部３１に記憶させる。ＳＩＭ＿２０ａは、管理サーバ装置８０から受信したＲｏｏｔ秘密鍵を、Ｒｏｏｔ秘密鍵記憶部３２に記憶させる。

[0103] 本実施形態によれば、無線通信により、管理サーバ装置８０から自動車１

へＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを送信することができる。これにより、自動車１に保持されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを、管理サーバ装置８０から更新することができる。

[0104] なお、無線通信ネットワーク２の電波が届かない等の理由により管理装置１０ａが無線通信ネットワーク２を介して管理サーバ装置８０と通信できない場合には、必要に応じて、自動車１に対し、新たなＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを保持する管理装置１０ａ及びＥＣＵ５０に交換してもよい。

[0105] 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。

[0106] 例えば、セキュアエレメントとして、ＳＩＭ又はｅＳＩＭを使用する例を挙げたが、これに限定されない。セキュアエレメントとして、例えば、耐タンパー性のある暗号処理チップを使用してもよい。耐タンパー性のある暗号処理チップとして、例えば、ＨＳＭ（Hardware Security Module）やＴＰＭ（Trusted Platform Module）と呼ばれる暗号処理チップが知られている。ＴＰＭについては、例えば非特許文献３に記載されている。例えば、管理装置１０のセキュアエレメント２０及びＥＣＵ５０のセキュアエレメント６０にＨＳＭ又はＴＰＭを使用してもよい。又は、管理装置１０，１０ａのセキュアエレメント２０，２０ａ及びＥＣＵ５０のセキュアエレメント６０にＳＩＭ又はｅＳＩＭを使用してもよい。又は、管理装置１０，１０ａのセキュアエレメント２０，２０ａとしてＳＩＭ又はｅＳＩＭを使用し、ＥＣＵ５０のセキュアエレメント６０としてＨＳＭ又はＴＰＭを使用してもよい。

[0107] また、自動車１に備わるいずれかのＥＣＵ５０を管理装置１０又は管理装置１０ａとして機能させてもよい。

[0108] 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。

[0109] また、上述した管理装置１０、管理装置１０ａ又はＥＣＵ５０が実行する

管理方法の各ステップ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。

[0110] 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。

産業上の利用可能性

[0111] 本発明は、管理システム、車両、管理装置、車載コンピュータ、管理方法、及びコンピュータプログラムに適用してもよい。

符号の説明

[0112] １…自動車

２…無線通信ネットワーク

３…無線通信回線

４…通信回線

１０，１０ａ…管理装置

１１，５１…制御部

１２，５２…ＣＡＮインタフェース

１３…無線通信部

２０，６０…セキュアエレメント

２０ａ…ＳＩＭ（セキュアエレメント）

２１，６１…鍵生成部

２２，６２…鍵記憶部

２３，６３…検証部

２４，６４…暗号処理部

３１，７１…Ｒｏｏｔ証明書記憶部

３２，７２…Ｒｏｏｔ秘密鍵記憶部

３３，７５…Ｓ公開鍵証明書記憶部

３４…Ｓ秘密鍵記憶部

３５，７３…Ｃ公開鍵証明書記憶部

３６，７６…ＭＡＣ鍵記憶部

８０…管理サーバ装置

請求の範囲

[請求項1] 車両に備わる管理装置と車載コンピュータを備え、前記管理装置と前記車載コンピュータとが前記車両に備わる通信ネットワークを介して通信する管理システムであって、

前記管理装置と前記車載コンピュータとが、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、共通して備え、

前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する、

管理システム。

[請求項2] 前記管理装置は、

公開鍵と秘密鍵のペアを生成する鍵生成部と、

前記管理装置の鍵記憶部に記憶されるＲｏｏｔ秘密鍵を使用して、前記鍵生成部により生成された公開鍵の電子署名を生成する暗号処理部と、を備え、

前記鍵生成部により生成された公開鍵と前記暗号処理部により生成された電子署名とから構成される公開鍵証明書を前記車載コンピュータへ送信し、

前記車載コンピュータは、

前記管理装置から受信した公開鍵証明書を、前記車載コンピュータの鍵記憶部に記憶されるＲｏｏｔ証明書を使用して検証する検証部を備える、

請求項１に記載の管理システム。

[請求項3] 前記車載コンピュータは、

公開鍵と秘密鍵のペアを生成する鍵生成部と、

前記車載コンピュータの鍵記憶部に記憶されるＲｏｏｔ秘密鍵を使用して、前記車載コンピュータの鍵生成部により生成された公開鍵の電子署名を生成する暗号処理部と、を備え、

前記車載コンピュータの鍵生成部により生成された公開鍵と前記車載コンピュータの暗号処理部により生成された電子署名とから構成される公開鍵証明書を前記管理装置へ送信し、

前記管理装置は、

前記車載コンピュータから受信した公開鍵証明書を、前記管理装置の鍵記憶部に記憶されるＲｏｏｔ証明書を使用して検証する検証部を備える、

請求項２に記載の管理システム。

[請求項4] 前記管理装置の鍵生成部は鍵を生成し、

前記管理装置の暗号処理部は、前記車載コンピュータへ送信した公開鍵証明書の公開鍵とペアの秘密鍵を使用して、前記管理装置の鍵生成部により生成された鍵の電子署名を生成し、当該鍵と当該電子署名とから構成される鍵証明書を前記車載コンピュータから受信した公開鍵証明書の公開鍵で暗号化し、

前記管理装置は前記鍵証明書の暗号化データを前記車載コンピュータへ送信し、

前記車載コンピュータの暗号処理部は、前記管理装置から受信した鍵証明書の暗号化データを、前記管理装置へ送信した公開鍵証明書の公開鍵とペアの秘密鍵で復号化し、

前記車載コンピュータの検証部は、前記鍵証明書の暗号化データの復号化データを、前記管理装置から受信した公開鍵証明書の公開鍵を使用して検証する、

請求項３に記載の管理システム。

[請求項5] 前記管理装置の鍵生成部は、新Ｒｏｏｔ公開鍵と新Ｒｏｏｔ秘密鍵のペアを生成し、

前記管理装置の暗号処理部は、前記管理装置の鍵記憶部に記憶されるＲｏｏｔ秘密鍵を使用して前記新Ｒｏｏｔ公開鍵の電子署名を生成し、

前記管理装置の鍵記憶部は、前記新Ｒｏｏｔ秘密鍵と、前記新Ｒｏｏｔ公開鍵と当該新Ｒｏｏｔ公開鍵の電子署名とから構成される公開鍵証明書である新Ｒｏｏｔ証明書とを記憶し、

前記管理装置は、前記新Ｒｏｏｔ秘密鍵と前記新Ｒｏｏｔ証明書を、前記車載コンピュータとの間で共有する暗号路鍵で暗号化して前記車載コンピュータへ送信し、

前記車載コンピュータは、前記管理装置から受信した前記新Ｒｏｏｔ秘密鍵と前記新Ｒｏｏｔ証明書の暗号化データを前記暗号路鍵で復号化し、

前記車載コンピュータの検証部は、復号化された前記新Ｒｏｏｔ証明書を、前記車載コンピュータの鍵記憶部に記憶されるＲｏｏｔ証明書を使用して検証し、

前記車載コンピュータの鍵記憶部は、前記新Ｒｏｏｔ証明書の検証が成功である場合に、前記新Ｒｏｏｔ秘密鍵と前記新Ｒｏｏｔ証明書を記憶する、

請求項１から４のいずれか１項に記載の管理システム。

[請求項6] 請求項１から５のいずれか１項に記載の管理システムを備える車両。

[請求項7] 車両に備わる通信ネットワークを介して前記車両に備わる車載コンピュータと通信する前記車両に備わる管理装置であって、

Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、前記車載コンピュータと共通して備え、

前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する、

管理装置。

[請求項8] 車両に備わる通信ネットワークを介して前記車両に備わる管理装置と通信する前記車両に備わる車載コンピュータであって、

Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを記憶する鍵記憶部を、前記管理装置と共通して備え、

前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行する、

車載コンピュータ。

[請求項9] 車両に備わる管理装置と車載コンピュータを備え、前記管理装置と前記車載コンピュータとが前記車両に備わる通信ネットワークを介して通信する管理システムの管理方法であって、

前記管理装置と前記車載コンピュータとが、Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを、共通して各々の鍵記憶部に記憶するステップと、

前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行するステップと、

を含む管理方法。

[請求項10] 車両に備わる通信ネットワークを介して前記車両に備わる車載コンピュータと通信する前記車両に備わる管理装置のコンピュータに、

Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公開鍵証明書であるＲｏｏｔ証明書とを、前記車載コンピュータと共通して鍵記憶部に記憶するステップと、

前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行するステップと、

を実行させるためのコンピュータプログラム。

[請求項11] 車両に備わる通信ネットワークを介して前記車両に備わる管理装置と通信する前記車両に備わる車載コンピュータに、

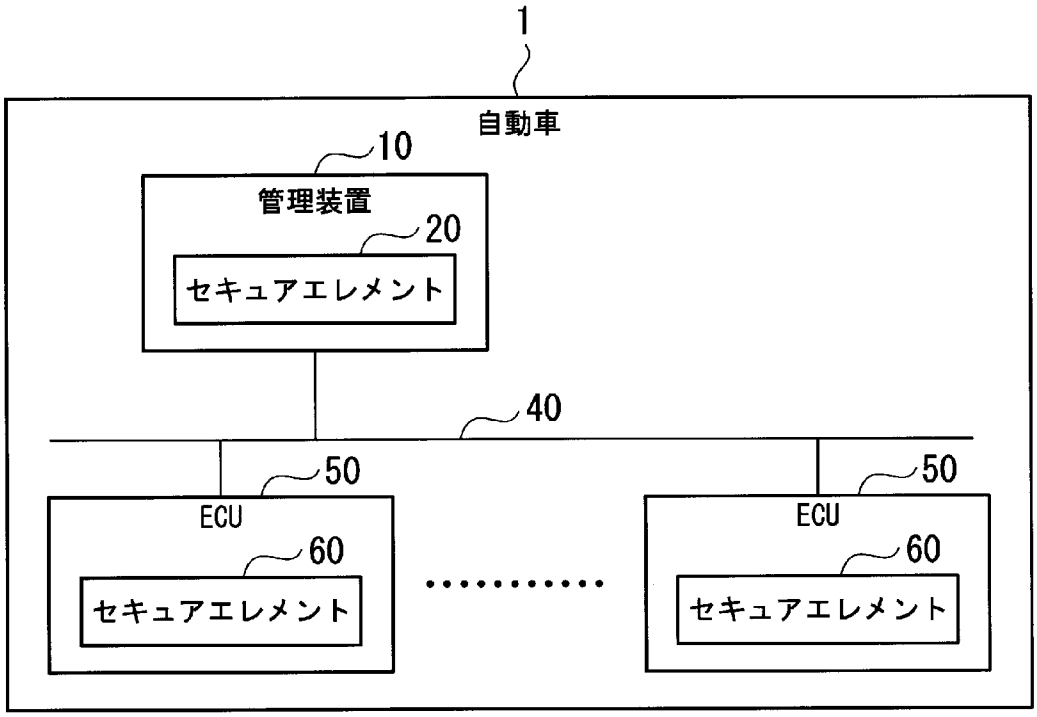
Ｒｏｏｔ秘密鍵と前記Ｒｏｏｔ秘密鍵のペアのＲｏｏｔ公開鍵の公

開鍵証明書であるＲｏｏｔ証明書とを、前記管理装置と共通して鍵記憶部に記憶するステップと、

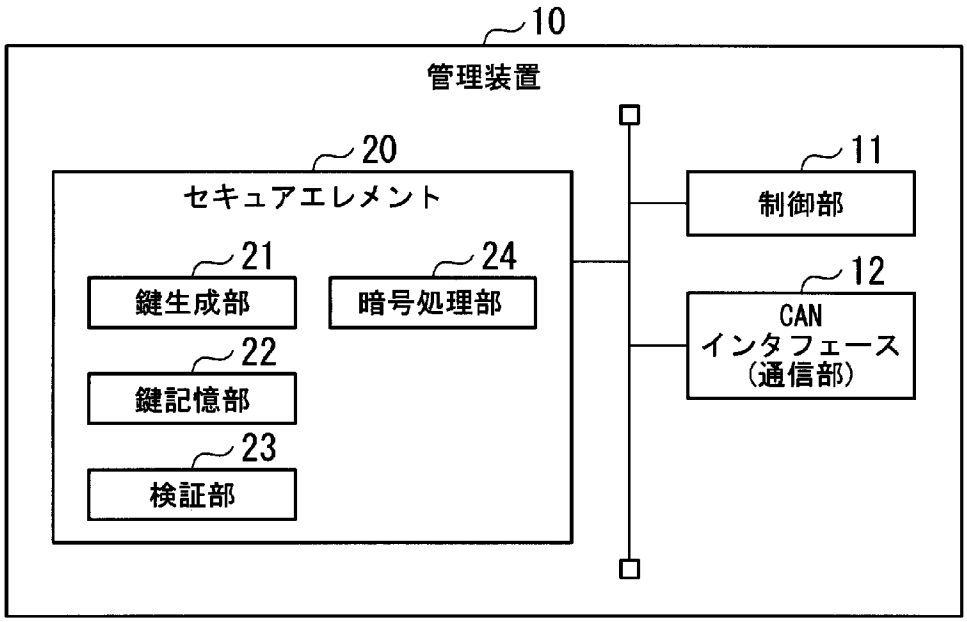
前記鍵記憶部に記憶されるＲｏｏｔ証明書とＲｏｏｔ秘密鍵のペアを使用して、公開鍵暗号方式に使用される公開鍵証明書を発行するステップと、

を実行させるためのコンピュータプログラム。

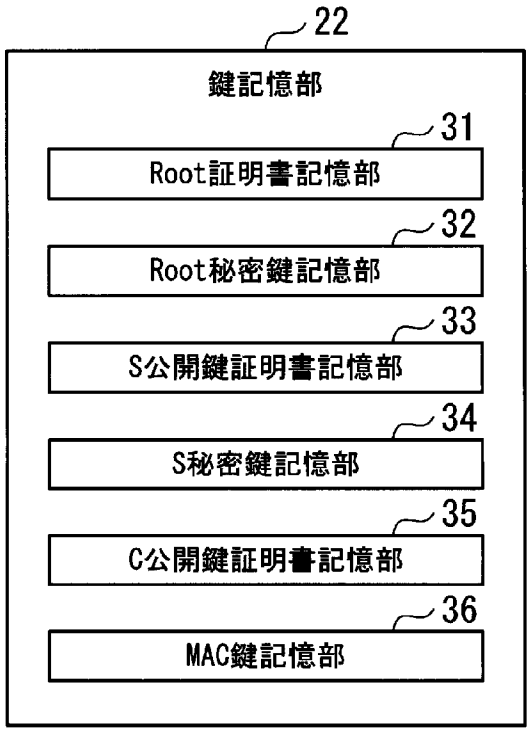
[図1]


1
自動車
10
管理装置
20
セキュアエレメント
40
50
ECU
60
セキュアエレメント
50
ECU
60
セキュアエレメント

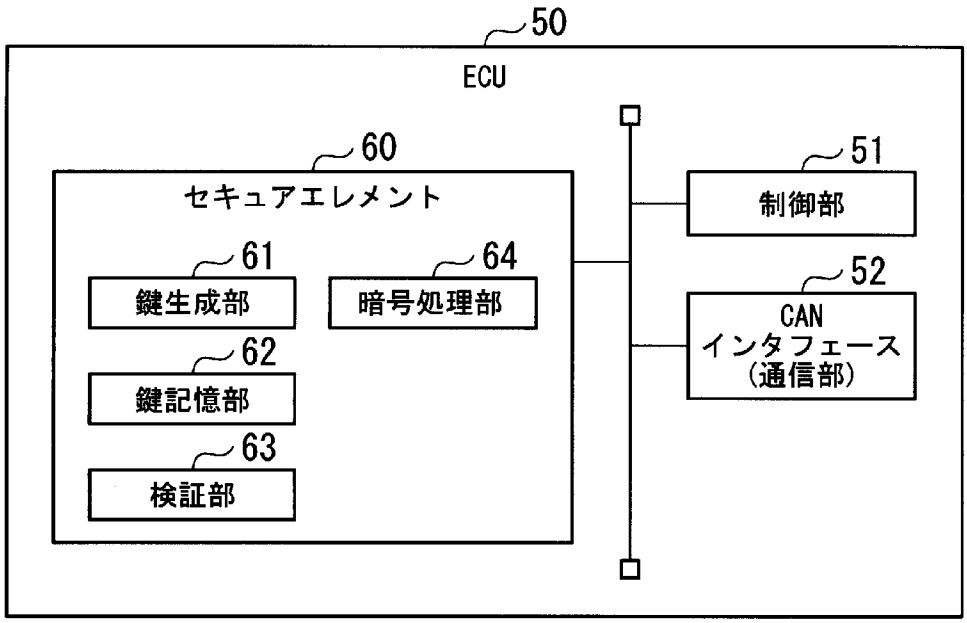
[図2]


10
管理装置
20
セキュアエレメント
21
鍵生成部
24
暗号処理部
22
鍵記憶部
23
検証部
11
制御部
12
CAN
インタフェース
(通信部)

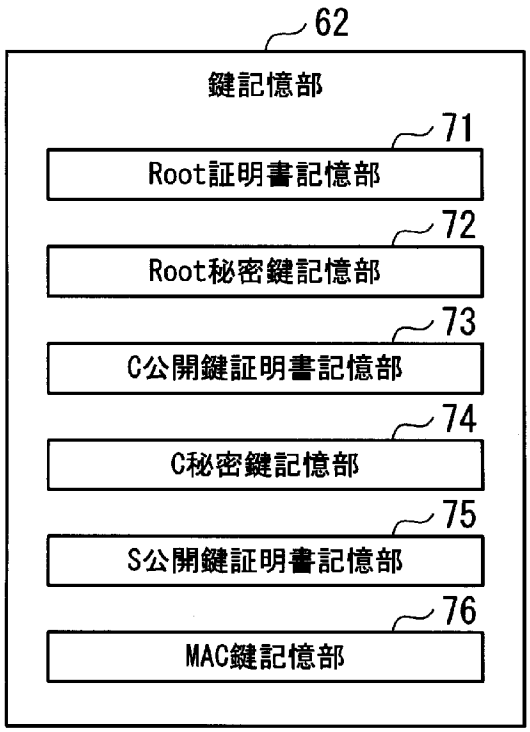
[図3]


22
鍵記憶部
31
Root証明書記憶部
32
Root秘密鍵記憶部
33
S公開鍵証明書記憶部
34
S秘密鍵記憶部
35
C公開鍵証明書記憶部
36
MAC鍵記憶部

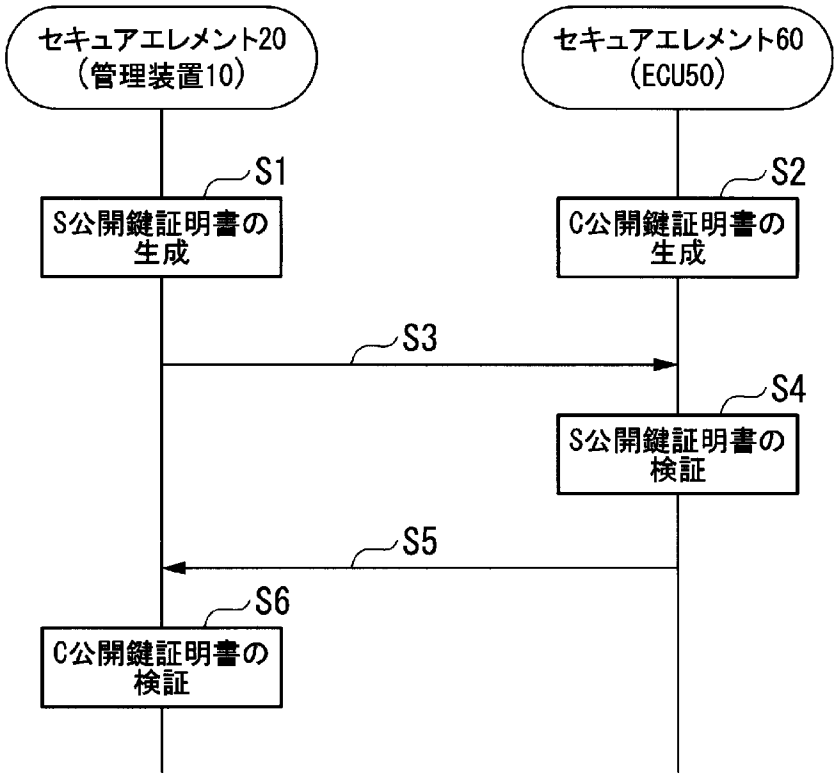
[図4]


50
ECU
60
セキュアエレメント
61
鍵生成部
64
暗号処理部
62
鍵記憶部
63
検証部
51
制御部
52
CAN
インタフェース
(通信部)

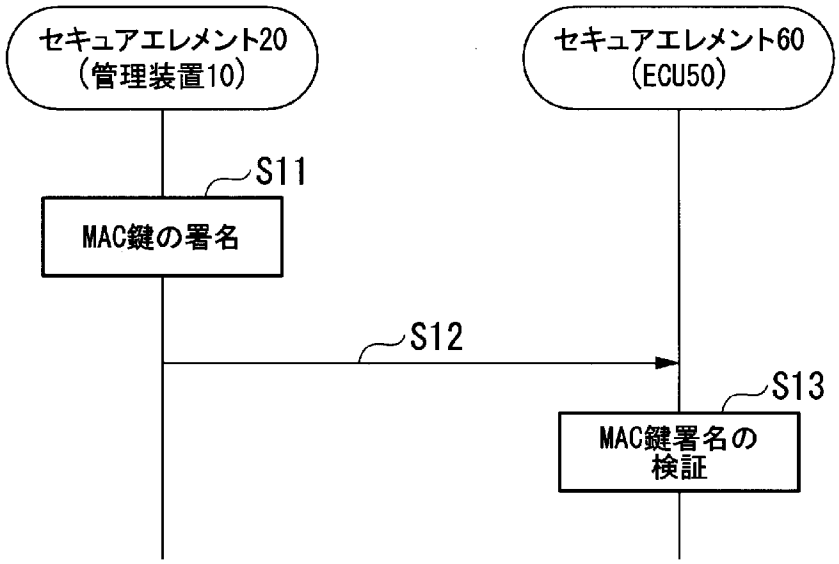
[図5]


62
鍵記憶部
71
Root証明書記憶部
72
Root秘密鍵記憶部
73
C公開鍵証明書記憶部
74
C秘密鍵記憶部
75
S公開鍵証明書記憶部
76
MAC鍵記憶部

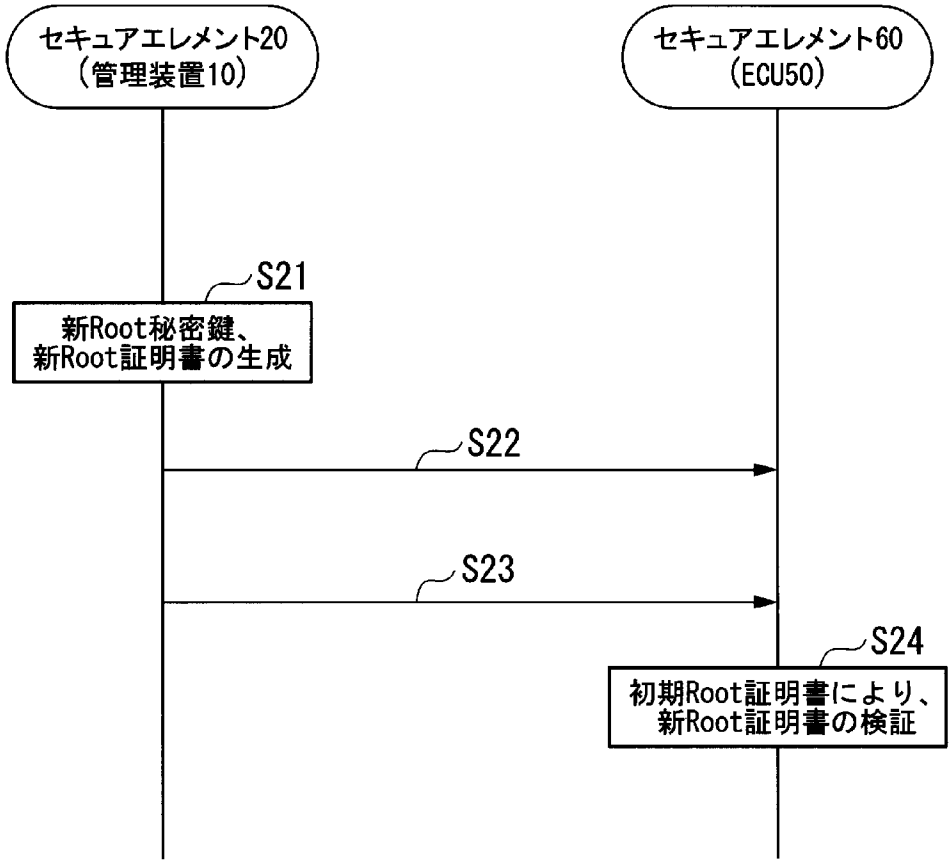
[図6]


セキュアエレメント20
(管理装置10)
セキュアエレメント60
(ECU50)
S1
S公開鍵証明書の
生成
S2
C公開鍵証明書の
生成
S3
S4
S公開鍵証明書の
検証
S5
S6
C公開鍵証明書の
検証

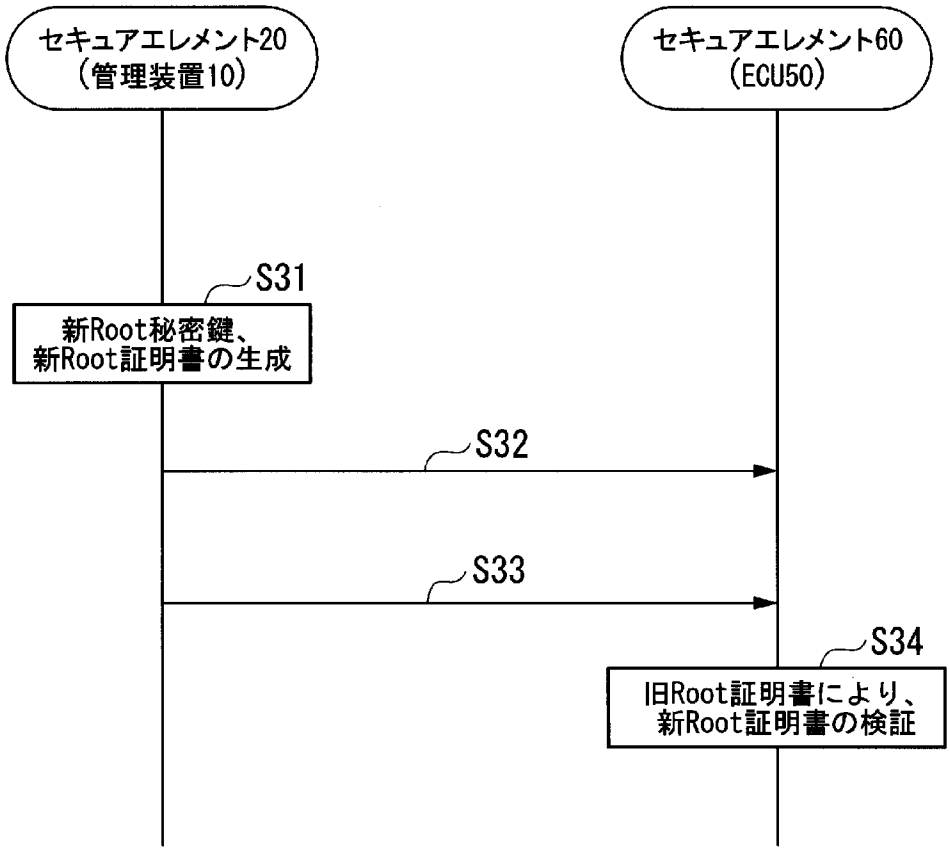
[図7]


セキュアエレメント20
(管理装置10)
セキュアエレメント60
(ECU50)
S11
MAC鍵の署名
S12
S13
MAC鍵署名の
検証

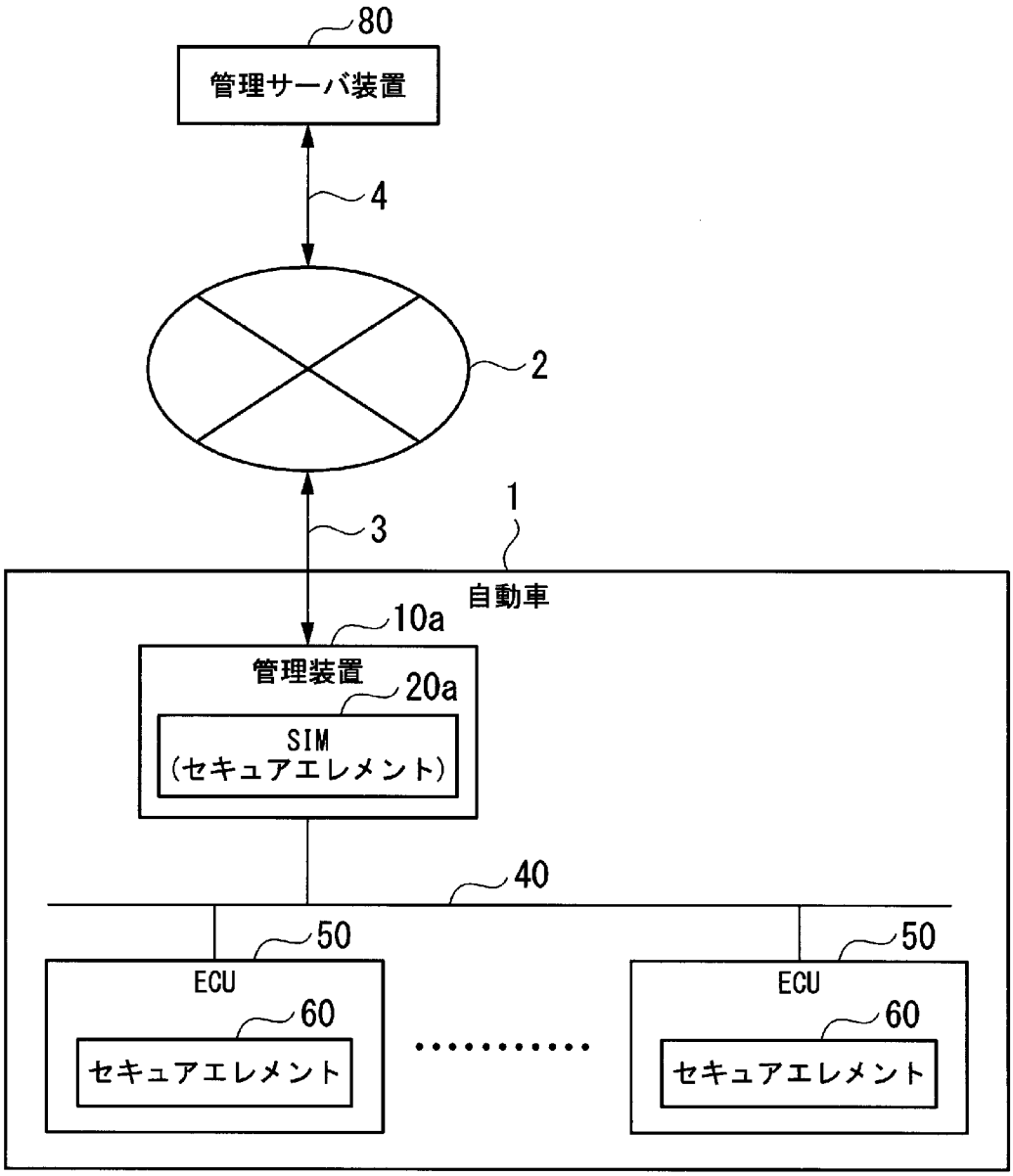
[図8]


セキュアエレメント20
(管理装置10)
セキュアエレメント60
(ECU50)
S21
新Root秘密鍵、
新Root証明書の生成
S22
S23
S24
初期Root証明書により、
新Root証明書の検証

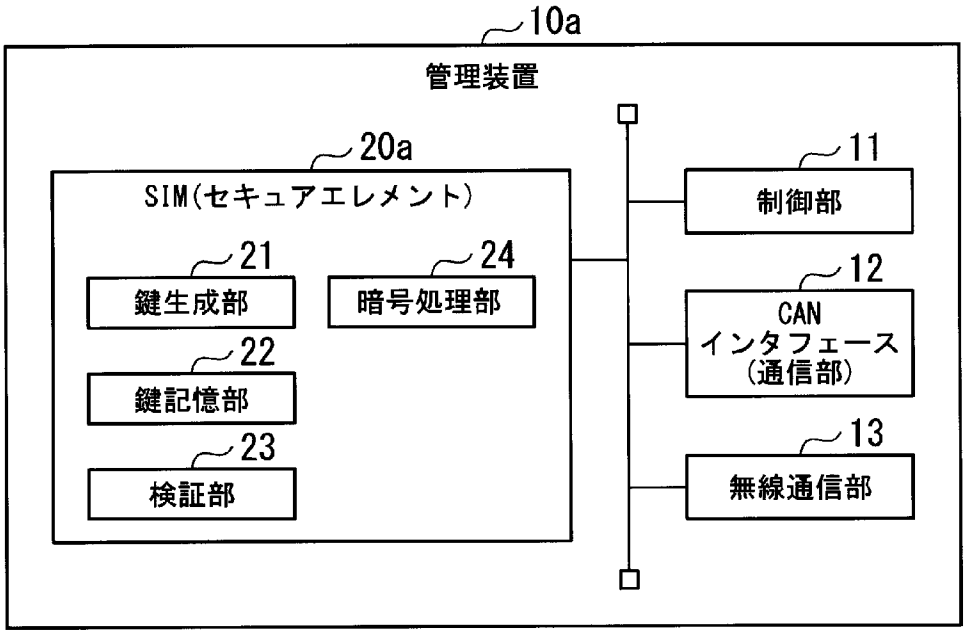
[図9]


セキュアエレメント20
(管理装置10)
セキュアエレメント60
(ECU50)
S31
新Root秘密鍵、
新Root証明書の生成
S32
S33
S34
旧Root証明書により、
新Root証明書の検証

[図10]


80
管理サーバ装置
4
2
3
1
自動車
10a
管理装置
20a
SIM
(セキュアエレメント)
40
50
ECU
60
セキュアエレメント
50
ECU
60
セキュアエレメント

[図11]


10a
管理装置
20a
SIM(セキュアエレメント)
21
鍵生成部
24
暗号処理部
22
鍵記憶部
23
検証部
11
制御部
12
CAN
インタフェース
(通信部)
13
無線通信部

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/057087

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F21/44*(2013.01)i, *G06F21/60*(2013.01)i, *H04L9/32*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, G06F21/44, G06F21/60, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-186635 A (Toyota Motor Corp.), 27 September 2012 (27.09.2012), & US 2014/0040992 A1 & WO 2012/120350 A2 & EP 2681901 A2 & CN 103404112 A	1-11
A	WO 2011/148744 A1 (Renesas Electronics Corp.), 01 December 2011 (01.12.2011), & JP 5261614 B2 & US 2013/0067220 A1 & US 2014/0303881 A1 & US 2015/0358170 A1 & EP 2579498 A1 & CN 102907039 A	1-11
A	JP 2014-107744 A (Hitachi Industrial Equipment System Co., Ltd.), 09 June 2014 (09.06.2014), (Family: None)	1-11

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 May 2016 (23.05.16)	31 May 2016 (31.05.16)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０５７０８７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/44(2013.01)i, G06F21/60(2013.01)i, H04L9/32(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, G06F21/44, G06F21/60, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2012-186635 A (トヨタ自動車株式会社) 2012.09.27 & US 2014/0040992 A1 & WO 2012/120350 A2 & EP 2681901 A2 & CN 103404112 A	1-11
A	WO 2011/148744 A1 (ルネサスエレクトロニクス株式会社) 2011.12.01 & JP 5261614 B2 & US 2013/0067220 A1 & US 2014/0303881 A1 & US 2015/0358170 A1 & EP 2579498 A1 & CN 102907039 A	1-11

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２３．０５．２０１６	３１．０５．２０１６

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４８７６
金木　陽一
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2014-107744 A (株式会社日立産機システム) 2014.06.09 (Family: None)	1-11