(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 1 日(01.12.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/189796 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04W 12/04* (2009.01)
H04W 4/04 (2009.01)

(21) 国際出願番号: PCT/JP2016/002062

(22) 国際出願日: 2016 年 4 月 15 日(15.04.2016)

(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 2015-104516 2015 年 5 月 22 日(22.05.2015) JP

(71) 出願人: 株式会社デンソー(DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町１丁目１番地 Aichi (JP).

(72) 発明者: 成本　洋介(NARIMOTO, Yousuke); 〒4488661 愛知県刈谷市昭和町１丁目１番地株式会社デンソー内 Aichi (JP). 長尾　悟志(NAGAO, Satoshi); 〒4488661 愛知県刈谷市昭和町１丁目１番地株式会社デンソー内 Aichi (JP). 井本　礼一郎(IMOTO, Reiichirou); 〒4488661 愛知県刈谷市昭和町１丁目１番地株式会社デンソー内 Aichi (JP). 菅島　健司(SUGASHIMA, Takeshi); 〒4488661 愛知県刈谷市昭和町１丁目１番地株式会社デンソー内 Aichi (JP).

(74) 代理人: 金　順姫(KIN, Junhi); 〒4600003 愛知県名古屋市中区錦２丁目１３番１９号　瀧定ビル６階 Aichi (JP).

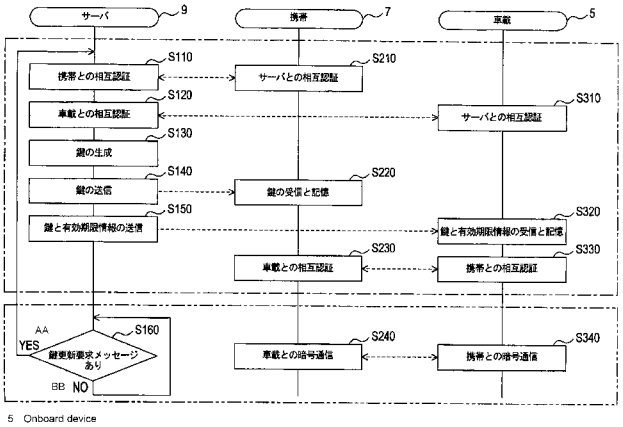
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, 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).

[続葉有]

(54) **Title**: VEHICLE COMMUNICATION SYSTEM, ONBOARD DEVICE, AND KEY ISSUING DEVICE

(54) 発明の名称 : 車両用通信システム、車載装置及び鍵発行装置



5 Onboard device
7 Portable device
9 Server
S110, S330 Mutual authentication with portable device
S120 Mutual authentication with onboard device
S130 Generation of key
S140 Transmission of key
S150 Transmission of key and validity period information
S160 Does key update request message exist?
S210 Mutual authentication with server
S220 Reception and storage of key
S230 Mutual authentication with onboard device
S240 Encrypted communication with onboard device
S310 Mutual authentication with server
S320 Reception and storage of key and validity period information
S340 Encrypted communication with portable device
AA YES
BB NO

(57) **Abstract**: A vehicle communication system is provided with an onboard device (5), a portable device (7), and a key-issuing device (9) provided outside the vehicle for issuing a key for encrypted communication between the portable device and the onboard device. The portable device and the onboard device store the key, and perform encrypted communication using the stored key. The onboard device is issued the key and validity period information by the key-issuing device. The onboard device is provided with a determination unit for determining whether a validity period has started, and an update request unit for transmitting a key update request to request the issuance of a new key. When the key update request has been received, the key-issuing device issues a new key to the portable device, and issues a new key and validity period information for the new key to the onboard device (S160, S130-S150).

(57) 要約: 車両用通信システムは、車載装置（５）と、携帯機器（７）と、車両の外部に設けられ、携帯機器と車載装置とに暗号通信用の鍵を発行する鍵発行装置（９）と、を備える。携帯機器と車載装置とが、鍵を記憶し、記憶した鍵を用いて暗号通信を行う。鍵発行装置から車載装置には、鍵と、有効期限情報とが発行される。車載装置は、有効期限が到来したか否かを判定する判定部と、新たな鍵の発行を要求するための鍵更新要求を送信する更新要求部と、を備える。鍵発行装置は、鍵更新要求を受信した場合には、新たな鍵を携帯機器に発行すると共に、新たな鍵と新たな鍵についての有効期限情報とを車載装置に発行する（Ｓ１６０，Ｓ１３０～Ｓ１５０）。

WO 2016/189796 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： 車両用通信システム、車載装置及び鍵発行装置

関連出願の相互参照

[0001] 本出願は、２０１５年５月２２日に出願された日本国特許出願２０１５－１０４５１６号に基づくものであり、ここにその記載内容を参照により援用する。

技術分野

[0002] 本開示は、携帯機器と車載装置とが鍵発行装置から発行された鍵を用いて暗号通信を行う車両用通信システムに関する。

背景技術

[0003] 車両の使用者に携帯される携帯機器と、車両に搭載された車載装置とが、暗号通信を行う通信システムとして、例えば特許文献１に記載のものがある。

[0004] 特許文献１の通信システムは、携帯機器として、ドアを施解錠するためのスマートキーを備え、車載装置として、ドアの施解錠を実施するドアロック装置を備える。そして、特許文献１の通信システムにおいて、スマートキーとドアロック装置は、通信網を介して通信可能な鍵発行装置から発行される暗号通信用の鍵を、複数記憶する。更に、スマートキーとドアロック装置は、記憶した複数の鍵の１つを暗号通信に使用するが、使用する鍵を暗号通信に成功するまで切り換えていくことにより、双方において一致する鍵を特定している。特許文献１では、このような手法により、スマートキー及びドアロック装置が鍵発行装置と常時通信しなくても、暗号通信に使用される鍵が更新されるようにして、暗号通信の安全性を確保している。

先行技術文献

特許文献

[0005] 特許文献1：ＪＰ２０１１－２５６５６１Ａ

発明の概要

[0006] 特許文献１の技術では、携帯機器と車載装置とにおいて、鍵を複数記憶しなければならず、鍵を記憶するためのリソースが増加するおそれがある。このため、リソースの乏しい車載装置や携帯機器へ適用しづらいおそれがある。

[0007] そこで、本開示は、携帯機器及び車載装置が鍵発行装置と通信しなければならない頻度を下げることと、暗号通信用の鍵の更新による安全性確保と、鍵を記憶するのに必要なリソースの低減とを、実現することを目的としている。

[0008] 本開示の一態様による車両用通信システムは、車両に搭載された車載装置と、車両の使用者に携帯される携帯機器と、車両の外部に設けられ、携帯機器と車載装置とに暗号通信用の鍵を発行する鍵発行装置と、を備える。

[0009] 車両用通信システムは、携帯機器と車載装置とが、鍵発行装置によって発行された鍵を記憶し、その記憶した鍵を用いて暗号通信を行う。

[0010] 鍵発行装置から車載装置には、鍵と、その鍵の有効期限を示す有効期限情報とが発行される。

[0011] 車載装置は、判定部と、更新要求部とを備える。判定部は、前記発行された有効期限情報が示す有効期限が、到来したか否かを判定する。更新要求部は、判定部により有効期限が到来したと判定されると、鍵発行装置に対して、新たな鍵の発行を要求するための鍵更新要求を送信する。

[0012] 鍵発行装置は、車載装置からの鍵更新要求を受信した場合には、新たな鍵を携帯機器に発行すると共に、その新たな鍵と当該鍵についての有効期限情報とを車載装置に発行する。

[0013] 本開示の車両用通信システムによれば、下記の効果が得られる。

[0014] 鍵発行装置から携帯機器と車載装置とに鍵を発行するのは、有効期限情報が示す有効期限が到来する毎で良い。このため、携帯機器及び車載装置が鍵発行装置と通信しなければならない頻度を下げることができる。

[0015] 携帯機器と車載装置とが暗号通信に用いる鍵は、有効期限情報が示す有効期限が到来する毎に更新されるため、暗号通信の安全性を確保することがで

きる。

[0016] 携帯機器と車載装置とは、暗号通信用の鍵を１つ記憶すれば良い。つまり、複数の鍵を記憶する必要がない。このため、携帯機器と車載装置とにおいて、鍵を記憶するのに必要なリソース（即ち、メモリ資源）を低減することができる。

[0017] 携帯機器は、車両の使用者ではない者に持ち去られる可能性があるが、その携帯機器には鍵の有効期限情報が記憶されない。このため、悪意のある者が有効期限情報を改ざんすることを防止することができ、延いては暗号通信の安全性を高めることができる。

[0018] 本開示の別の態様による車載装置は、車両に搭載されて、車両の使用者に携帯される携帯機器と暗号通信を行う。車載装置には、暗号通信に用いる鍵が、車両の外部の鍵発行装置によって発行される。

[0019] 鍵発行装置から当該車載装置には、鍵と、その鍵の有効期限を示す有効期限情報とが発行される。

[0020] 車載装置は、判定部と、更新要求部とを備える。判定部は、前記発行された有効期限情報が示す有効期限が、到来したか否かを判定する。更新要求部は、判定部により有効期限が到来したと判定されると、鍵発行装置に対して、新たな鍵の発行を要求するための鍵更新要求を送信する。

[0021] 本開示の車載装置は、車両用通信システムにおける車載装置として使用することができる。

[0022] 本開示の別の態様による鍵発行装置は、車両の使用者に携帯される携帯機器と、車両に搭載された車載装置とに、暗号通信用の鍵を発行する。

[0023] 鍵発行装置は、第１の発行部と、第２の発行部と、鍵更新部と、を備える。第１の発行部は、携帯機器に鍵を発行する。第２の発行部は、車載装置に、鍵と、その鍵の有効期限を示す有効期限情報とを発行する。鍵更新部は、車載装置に発行された有効期限情報が示す有効期限が到来すると車載装置から送信されて来る鍵更新要求を受信したか否かを判定し、鍵更新要求を受信したと判定した場合には、新たな鍵を第１の発行部に発行させると共に、そ

の新たな鍵と当該鍵についての有効期限情報とを第２の発行部に発行させる。

[0024] 本開示の鍵発行装置は、車両用通信システムにおける鍵発行装置として使用することができる。

[0025] 本開示によれば、携帯機器及び車載装置が鍵発行装置と通信しなければならない頻度を下げることと、暗号通信用の鍵の更新による安全性確保と、鍵を記憶するのに必要なリソースの低減とを、実現できる。

図面の簡単な説明

[0026] 本開示についての上記および他の目的、特徴や利点は、添付図面を参照した下記詳細な説明から、より明確になる。添付図面において、

[図1]図１は、実施形態の車両用通信システムを表す構成図であり、

[図2]図２は、鍵発行サーバと携帯機器と車載装置との各処理を表すフローチャートであり、

[図3]図３は、鍵更新要求処理を表すフローチャートである。

発明を実施するための形態

[0027] 以下に、本開示が適用された実施形態の車両用通信システムについて説明する。

[0028] （構成）

図１に示すように、本実施形態の車両用通信システム１は、車両３に搭載された装置である車載装置５と、車両３の使用者に携帯される携帯機器７と、車両３の外部に設けられた鍵発行装置としての鍵発行サーバ（鍵発行装置に相当する）９と、を備える。

[0029] 携帯機器７は、本実施形態では多機能携帯電話（いわゆるスマートフォン）である。鍵発行サーバ９は、車載装置５と携帯機器７とに暗号通信用の鍵を発行するためのセンターとして機能する。

[0030] 鍵発行サーバ９と車載装置５との間、および鍵発行サーバ９と携帯機器７との間は、携帯電話網やインターネットや広域ネットワーク等の通信網１０を介して、通信が可能となっている。そして、車載装置５と携帯機器７との

各々は、鍵発行サーバ９と無線で通信するようになっている。

[0031] また、携帯機器７と車載装置５との間は、例えばＵＨＦ（Ultra High Frequency）帯等を用いる近距離無線通信によって通信可能となっている。本実施形態において、携帯機器７と車載装置５との間の無線通信方式は、例えばブルートゥース（登録商標）であるが、赤外線通信等、他の方式であってもよい。尚、携帯機器７と車載装置５との間の通信であっても、通信網１０を介した通信が行われてもよい。

[0032] 車載装置５は、通信網１０を介して少なくも鍵発行サーバ９と通信するためのネットワークインターフェース１１と、携帯機器７との間で無線通信を行うための近距離通信装置１２とを備える。そして、車載装置５は、ＣＰＵ（Central Processing Unit）１３と、ＲＯＭ（Read Only Memory）１４と、ＲＡＭ（Random Access Memory）１５と、記憶装置１６とを備える。記憶装置１６は、例えば、ＥＥＰＲＯＭ（Electrically Erasable Programmable ROM）やフラッシュメモリ等の書き換え可能不揮発性メモリであるが、ハードディスクドライブ等でも良い。更に、車載装置５は、車両３に関する各種情報を入力するための入力回路１７と、車両３に搭載された機器を制御するための出力回路１８とを備える。

[0033] 携帯機器７は、通信網１０を介して少なくも鍵発行サーバ９と通信するためのネットワークインターフェース２１と、車載装置５との間で無線通信を行うための近距離通信装置２２と、ＣＰＵ２３と、ＲＯＭ２４と、ＲＡＭ２５と、記憶装置２６と、表示装置２７とを備える。表示装置２７は、例えば、入力装置としての機能を兼ね備えたタッチパネルである。また、記憶装置２６は、例えば、ＥＥＰＲＯＭやフラッシュメモリ等の書き換え可能不揮発性メモリであるが、ハードディスクドライブ等でも良い。

[0034] 鍵発行サーバ９は、通信網１０を介して少なくも車載装置５及び携帯機器７と通信するためのネットワークインターフェース３１と、ＣＰＵ３３と、ＲＯＭ３４と、ＲＡＭ３５と、記憶装置３６とを備える。記憶装置３６は、例えば、ハードディスクドライブであるが、ＥＥＰＲＯＭやフラッシュメモ

リ等の書き換え可能不揮発性メモリ等でも良い。

[0035] 鍵発行サーバ９と携帯機器７と車載装置５との各々は、ＣＰＵ、ＲＯＭ及びＲＡＭを備えるため、コンピュータとして機能する。

[0036] （処理）

次に、鍵発行サーバ９と携帯機器７と車載装置５との各々が行う処理について、図２，図３を用い説明する。尚、鍵発行サーバ９の動作は、ＣＰＵ３３が例えばＲＯＭ３４又は記憶装置３６に記憶されているプログラムを実行することで実現される。ＲＯＭ３４および記憶装置３６はコンピュータ読取り可能な非一時的な記憶媒体の一例に相当する。車載装置５の動作は、ＣＰＵ１３が例えばＲＯＭ１４又は記憶装置１６に記憶されているプログラムを実行することで実現される。携帯機器７の動作は、ＣＰＵ２３が例えばＲＯＭ２４又は記憶装置２６に記憶されているプログラムを実行することで実現される。特に、以下に説明する携帯機器７の動作は、例えば記憶装置２６に記憶されたアプリケーションソフトをＣＰＵ２３が実行することで実現される。そのアプリケーションソフトは、例えば鍵発行サーバ９からダウンロードされる。

[0037] 図２に示すように、鍵発行サーバ９は携帯機器７との相互認証のための処理を行う（Ｓ１１０）。すると、携帯機器７も鍵発行サーバ９との相互認証のための処理を行う（Ｓ２１０）。つまり、鍵発行サーバ９と携帯機器７とが相互認証を実施する（Ｓ１１０，Ｓ２１０）。

[0038] 鍵発行サーバ９と携帯機器７は、例えばチャレンジ・レスポンス方式によって相互認証を行う。

[0039] 鍵発行サーバ９と携帯機器７とが相互認証を行うために用いる認証用鍵を、認証用鍵Ａと言うことにすると、その認証用鍵Ａは、事前に鍵発行サーバ９から携帯機器７に配付されている。例えば、認証用鍵Ａは、鍵発行サーバ９から携帯機器７にダウンロードされるアプリケーションソフトに埋め込まれていても良い。また、使用者が携帯機器７を操作して鍵発行サーバ９へユーザＩＤとパスワード等を送信することで、鍵発行サーバ９から携帯機器７

へ認証用鍵Ａが送信されるようになっていても良い。携帯機器７への認証用鍵Ａの配付方法は、鍵発行サーバ９と携帯機器７とが認証用鍵Ａを共有できるのであれば、どのような方法でも良い。

[0040] そして、鍵発行サーバ９と携帯機器７との相互認証においては、まず、鍵発行サーバ９が、毎回変化するランダムなデータを、「チャレンジ」として携帯機器７に送信する。携帯機器７は、鍵発行サーバ９から受信したデータと、自身が保有している認証用鍵Ａとを用いて、予め定められた演算を行い、その演算結果のデータを、「レスポンス」として鍵発行サーバ９に送信する。鍵発行サーバ９は、携帯機器７に送信した「チャレンジ」と、自身が保有している認証用鍵Ａと用いて、携帯機器７側と同じ演算行うことにより、「レスポンス」を算出し、その算出結果と、携帯機器７から受信した「レスポンス」とが一致すれば、携帯機器７を認証する。その後更に、携帯機器７が「チャレンジ」の送り側となり、鍵発行サーバ９が「レスポンス」の送り側となることで、携帯機器７が鍵発行サーバ９を認証する。尚、鍵発行サーバ９と携帯機器７との相互認証の方式は、チャレンジ・レスポンス方式以外の方式であっても良い。

[0041] 次に、鍵発行サーバ９は車載装置５との相互認証のための処理を行う（Ｓ１２０）。すると、車載装置５も鍵発行サーバ９との相互認証のための処理を行う（Ｓ３１０）。つまり、鍵発行サーバ９と車載装置５とが相互認証を実施する（Ｓ１２０，Ｓ３１０）。

[0042] 鍵発行サーバ９と車載装置５も、例えば、鍵発行サーバ９と携帯機器７との相互認証と同様に、チャレンジ・レスポンス方式によって相互認証を行う。

[0043] 鍵発行サーバ９と車載装置５とが相互認証を行うために用いる認証用鍵を、認証用鍵Ｂと言うことにすると、その認証用鍵Ｂは、例えば、マスタ鍵と車載装置５に固有のＩＤとから生成される。

[0044] 具体的には、車両３の製造工場と鍵発行サーバ９とでマスタ鍵が共有されている。そして、車両３の製造工場では、車両３の製造工程において、車載

装置５のＩＤとマスタ鍵とから所定の生成規則で認証用鍵Ｂが生成され、その生成された認証用鍵Ｂが、車載装置５の例えば記憶装置１６に書き込まれる。このため、車載装置５は、記憶装置１６に記憶された認証用鍵Ｂを用いて、鍵発行サーバ９との相互認証を行う。

[0045] また、鍵発行サーバ９は、車載装置５との認証過程において、車載装置５からＩＤを取得し、その取得したＩＤとマスタ鍵とから、車両３の製造工場での上記生成規則と同じ規則で認証用鍵Ｂを生成する。そして、鍵発行サーバ９は、その生成した認証用鍵Ｂを用いて、車載装置５との相互認証を行う。

[0046] 鍵発行サーバ９は、携帯機器７及び車載装置５との相互認証が完了すると、携帯機器７及び車載装置５に発行する暗号通信用の鍵を生成する（Ｓ１３０）。このＳ１３０で生成される鍵は、毎回異なる。

[0047] そして、鍵発行サーバ９は、Ｓ１３０で生成した鍵を、携帯機器７との間で共有している認証用鍵Ａを用いて暗号化し、その暗号化した鍵を携帯機器７に送信する（Ｓ１４０）。鍵を携帯機器７に送信することは、携帯機器７に鍵を発行することに相当する。

[0048] 一方、携帯機器７は、鍵発行サーバ９からの暗号化された鍵を受信して、その受信した鍵を、認証用鍵Ａを用いて復号し、その復号後の鍵を、例えば記憶装置２６に記憶する（Ｓ２２０）。

[0049] また、鍵発行サーバ９は、Ｓ１３０で生成した鍵に有効期限情報を付加し、その有効期限情報を付加した鍵（以下、情報付き鍵という）を、車載装置５との間で共有している認証用鍵Ｂを用いて暗号化する。そして、その暗号化した情報付き鍵を車載装置５に送信する（Ｓ１５０）。情報付き鍵を車載装置５に送信することは、車載装置５に鍵と有効期限情報とを発行することに相当する。有効期限情報は、鍵の有効期限を示す情報である。有効期限情報の具体的な内容については後で述べる。

[0050] 一方、車載装置５は、鍵発行サーバ９からの暗号化された情報付き鍵を受信して、その受信した情報付き鍵を、認証用鍵Ｂを用いて復号する。そして

、復号した鍵及び有効期限情報を、例えば記憶装置１６に記憶する（Ｓ３２０）。尚、鍵発行サーバ９から車載装置５へは、鍵と有効期限情報とが、情報付き鍵の形態ではなく、１つずつ順次送信されるようになっていても良い。

[0051] そして、携帯機器７と車載装置５は、鍵発行サーバ９から発行された鍵を用いて相互認証を実施する（Ｓ２３０，Ｓ３３０）。つまり、携帯機器７は、Ｓ２３０にて、車載装置５との相互認証のための処理を行い、車載装置５は、Ｓ３３０にて、携帯機器７との相互認証の処理を行う。

[0052] 携帯機器７と車載装置５は、例えば前述のチャレンジ・レスポンス方式によって相互認証を行うが、認証用鍵としては、鍵発行サーバ９から発行された鍵を用いる。

[0053] また、携帯機器７と車載装置５との相互認証が失敗した場合には、携帯機器７と車載装置５とに同じ鍵が記憶されていないと考えられるため、図２において一点鎖線で囲まれた処理が再び実施される。図２において一点鎖線で囲まれた処理（即ち、Ｓ１１０～Ｓ１５０，Ｓ２１０～Ｓ２３０，Ｓ３１０～Ｓ３３０の処理）は、鍵発行サーバ９から携帯機器７及び車載装置５への鍵の配付が完了するまでの処理である。例えば、携帯機器７と車載装置５と何れかが、相手の認証に失敗した場合には、鍵発行サーバ９に対して再試行要求を送信する。そして、その再試行要求を受信した鍵発行サーバ９は、Ｓ１１０の処理からやり直す。

[0054] 携帯機器７と車載装置５は、相互認証に成功した後は、鍵発行サーバ９から発行されて記憶した鍵を用いて暗号通信を行う（Ｓ２４０，Ｓ３４０）。そして、携帯機器７と車載装置は、暗号通信を行うことにより、使用者にサービスを提供する。尚、図２において二点鎖線で囲まれた処理は、使用者にサービスを提供する段階で実施される処理である。

[0055] 携帯機器７は、例えば、使用者が当該携帯機器７に入力した要求の内容を示すコマンドを、Ｓ２２０で記憶装置２６に記憶した鍵を用いて暗号化し、その暗号化したコマンドを、近距離通信装置２２によって車載装置５に送信

する。

[0056] 車載装置５は、携帯機器７からのコマンドを近距離通信装置１２によって受信し、その受信したコマンドを、Ｓ３２０で記憶装置１６に記憶した鍵を用いて復号する。そして、車載装置５は、復号したコマンドに応じた処理を行う。

[0057] 例えば、コマンドとしては、車両３における何れかの部分を動作させるサービスのためのコマンドがある。具体例を挙げると、携帯機器７から、車両３のドアの施錠を要求するコマンドが送信された場合、車載装置５は、車両３のドアロックアクチュエータを動作させてドアを施錠することとなる。逆に、携帯機器７からドアの解錠を要求するコマンドが送信された場合、車載装置５は、ドアロックアクチュエータを動作させてドアを解錠することとなる。尚、車両３における何れかの部分を動作させるサービスとしては、ドアの施解錠に限らず、例えば、パワーウィンドウを動かすことやエンジンを始動させること等でも良い。

[0058] また、コマンドとしては、車両３の状態を車載装置５から携帯機器７に通知させるサービスのためのコマンドもある。

[0059] その場合、車載装置５は、コマンドによって通知が要求された情報のデータを、Ｓ３２０で記憶装置１６に記憶した鍵を用いて暗号化し、その暗号化したデータを、近距離通信装置１２によって携帯機器７に送信する。そして、携帯機器７は、車載装置５からのデータを近距離通信装置２２によって受信し、その受信したデータを、Ｓ２２０で記憶装置２６に記憶した鍵を用いて復号する。そして、携帯機器７は、復号したデータの内容を表示装置２７に表示する。具体例を挙げると、携帯機器７から車載装置５へ、車両３における故障情報の通知を要求するコマンドが送信された場合、車載装置５から携帯機器７へ故障情報のデータが送信され、その故障情報の内容が携帯機器７の表示装置２７に表示されることとなる。

[0060] また、車載装置５は、図２のＳ３４０にて携帯機器７との相互認証に成功した後（つまり、鍵の受け取りに成功した後）は、図３に示す鍵更新要求処

理を例えば一定時間毎に実行する。

[0061] 図３に示すように、車載装置５は、鍵更新要求処理を開始すると、Ｓ４１０にて、図２のＳ３２０で鍵と共に記憶装置１６に記憶した有効期限情報が示す有効期限が、到来したか否かを判定する。

[0062] 本実施形態において、鍵発行サーバ９から車載装置５に送信される有効期限情報は、例えば、鍵の発行時からの経過時間を鍵の有効期限として示す情報である。

[0063] このため、車載装置５は、Ｓ４１０では、鍵発行サーバ９からの鍵を記憶装置１６に更新記憶した時点から、有効期限情報が示す時間が経過したか否かを判定し、その時間が経過したと判定したなら、鍵の有効期限が到来したと判定する。

[0064] 車載装置５は、Ｓ４１０にて、鍵の有効期限が到来していないと判定した場合には、そのまま当該鍵更新要求処理を終了するが、鍵の有効期限が到来したと判定した場合には、Ｓ４２０に進む。

[0065] 車載装置５は、Ｓ４２０では、鍵発行サーバ９に対して、新たな鍵の発行を要求するための鍵更新要求メッセージを送信する。例えば、車載装置５は、鍵更新要求メッセージを、前述の認証用鍵Ｂを用いて暗号化し、その暗号化した鍵更新要求メッセージを鍵発行サーバ９に送信する。そして、車載装置５は、その後、当該鍵更新要求処理を終了する。

[0066] 尚、鍵更新要求メッセージは、鍵更新要求に相当する。そして、車載装置５が行う処理のうち、Ｓ４１０は、判定部としての処理に相当し、Ｓ４２０は、更新要求部としての処理に相当する。

[0067] 一方、図２に示すように、鍵発行サーバ９は、車載装置５からの鍵更新要求メッセージを受信したか否かを判定する（Ｓ１６０）。具体的には、鍵発行サーバ９は、車載装置５からのメッセージを受信して、その受信したメッセージを、認証用鍵Ｂを用いて復号し、復号したメッセージが鍵更新要求メッセージであれば、車載装置５からの鍵更新要求メッセージを受信したと判定する。

[0068] そして、鍵発行サーバ９は、車載装置５からの鍵更新要求メッセージを受信したと判定した場合には（Ｓ１６０：ＹＥＳ）、図２におけるＳ１１０の処理からやり直す。よって、この場合には、図２において一点鎖線で囲まれた処理が再び実施される。

[0069] このため、鍵発行サーバ９は、車載装置５からの鍵更新要求メッセージを受信した場合には、新たな鍵を生成して（Ｓ１３０）、その新たな鍵を携帯機器７に発行すると共に（Ｓ１４０）、その新たな鍵と当該鍵についての有効期限情報とを車載装置５に発行することとなる（Ｓ１５０）。

[0070] 尚、鍵発行サーバ９が行う処理のうち、Ｓ１４０は、第１の発行部としての処理に相当し、Ｓ１５０は、第２の発行部としての処理に相当する。そして、Ｓ１３０とＳ１６０は、鍵更新部としての処理に相当する。

[0071] （効果）

本実施形態の車両用通信システム１では、鍵発行サーバ９から車載装置５には、鍵と共に有効期限情報が発行される。そして、その有効期限情報が示す有効期限が到来する毎に、鍵発行サーバ９から携帯機器７及び車載装置５への鍵が更新される。このため、下記（１）～（４）の効果が得られる。

[0072] （１）鍵発行サーバ９から携帯機器７と車載装置５とに鍵を発行するのは、有効期限情報が示す有効期限が到来する毎で良い。このため、携帯機器７及び車載装置５が鍵発行サーバ９と通信しなければならない頻度を下げることができる。

[0073] （２）携帯機器７と車載装置５とが暗号通信に用いる鍵は、有効期限情報が示す有効期限が到来する毎に更新されるため、暗号通信の安全性を確保することができる。

[0074] （３）携帯機器７と車載装置５とは、暗号通信用の鍵を１つ記憶すれば良い。つまり、複数の鍵を記憶する必要がない。このため、携帯機器７と車載装置５とにおいて、鍵を記憶するのに必要なリソース（即ち、メモリ資源）を低減することができる。

[0075] （４）携帯機器７は、車両３の使用者ではない者に持ち去られる可能性が

あるが、その携帯機器７には鍵の有効期限情報が記憶されない。このため、悪意のある者が有効期限情報を改ざんすることを防止することができ、延いては暗号通信の安全性を高めることができる。

[0076] また、上記実施形態では、有効期限情報が、鍵の発行時からの経過時間を鍵の有効期限として示す情報である。このため、同じ鍵が実際に使用される期間の長さ（即ち、鍵の有効時間）を、有効期限情報によって精度良く制御することができる。尚、鍵発行サーバ９が発行する有効期限情報は、いつも同じ値であっても良いが、鍵を更新する毎に異なる値としても良い。

[0077] （変形例１）

有効期限情報は、例えば、鍵の発行時から車両３に対して特定の操作が行われた回数を、鍵の有効期限として示す情報であっても良い。

[0078] その場合、車載装置５は、鍵発行サーバ９からの鍵を記憶装置１６に更新記憶した時点から、車両３に対して特定の操作が行われた回数を計数すれば良い。つまり、車載装置５は、図３のＳ４１０では、特定の操作が行われた回数の計数値が、有効期限情報が示す回数に達したか否かを判定し、その回数に達したと判定したなら、鍵の有効期限が到来したと判定すれば良い。また、特定の操作としては、例えば、車両３の電源スイッチをオンする操作や、車両３のドアを開閉する操作等が考えられる。

[0079] このように構成すれば、有効期限情報の値が同じであったとしても、車両の利用形態に応じて鍵の有効時間を変えることができる。例えば、有効期限が鍵発行時から１週間経過だった場合、車両を週末にしか利用しない使用者にとっては、車両の利用ごとに鍵を更新することになってしまい、鍵を記憶するメリットが薄れてしまうが、有効期限情報が例えば車両３の電源スイッチがオンされた回数やドアの開閉回数等であれば、一定の期間、鍵の利用を持続させることができる。

[0080] （変形例２）

有効期限情報は、例えば、鍵の発行時からの車両３の走行距離を、鍵の有効期限として示す情報であっても良い。

[0081] その場合、車載装置５は、鍵発行サーバ９からの鍵を記憶装置１６に更新記憶した時点からの、車両３の走行距離を計数すれば良い。つまり、車載装置５は、図３のＳ４１０では、走行距離の計数値が、有効期限情報が示す走行距離に達したか否かを判定し、その走行距離に達したと判定したなら、鍵の有効期限が到来したと判定すれば良い。このように構成しても、変形例１と同様の効果が得られる。

[0082] （変形例３）

有効期限情報は、例えば、鍵の発行時から車両３が特定の状態になった回数を、鍵の有効期限として示す情報であっても良い。

[0083] その場合、車載装置５は、鍵発行サーバ９からの鍵を記憶装置１６に更新記憶した時点から、車両３が特定の状態になった回数を計数すれば良い。つまり、車載装置５は、図３のＳ４１０では、車両３が特定の状態になった回数の計数値が、有効期限情報が示す回数に達したか否かを判定し、その回数に達したと判定したなら、鍵の有効期限が到来したと判定すれば良い。このように構成しても、変形例１と同様の効果が得られる。

[0084] また、車両３の特定の状態としては、例えば、車両３の燃料が補給されたという状態が考えられる。車両３の燃料は、車両３の動力源の燃料である。このため、燃料としては、例えば、ガソリンまたは軽油等の化石燃料や、植物油や、水素や、電気等が考えられるが、他の種類の燃料でも良い。

[0085] また、車両３の特定の状態としては、例えば、車両３が特定の場所に行ったという状態でも良い。そして、特定の場所としては、例えば、自宅の駐車場や、使用者が勤務する会社の駐車場等が考えられるが、他の場所でも良い。

[0086] また、車両３の特定の状態としては、例えば、車両３の走行速度が所定値以上になったという状態でも良い。走行速度の所定値としては、例えば、時速３０Ｋｍや時速８０Ｋｍといった値が考えられるが、他の値でも良い。

[0087] また、車両３の特定の状態としては、例えば、車両３のエンジンの冷却水温が所定値以上になったという状態でも良い。冷却水温の所定値としては、

例えば、４０℃や９０℃といった値が考えられるが、他の値でも良い。

[0088] （他の実施形態）

上記変形例１～３の内容は適宜組み合わせても良い。

[0089] また、携帯機器７は、スマートフォンに限らず、例えば、車両３のドアの施解錠やエンジンの始動等を行うための電子キーや、タブレット型パソコン等でも良い。

[0090] また、携帯機器７において、鍵の記憶場所は、アクセスにセキュリティ機能がある記憶装置が好ましい。例えば、携帯機器７がスマートフォンであれば、鍵がＳＩＭカード（Subscriber Identity Module Card）に記憶されるように構成することができる。また例えば、携帯機器７がタブレット型パソコンであれば、鍵がセキュリティチップに記憶されるように構成することができる。

[0091] また、車載装置５と鍵発行サーバ９との通信は、例えば、携帯機器７を介して（即ち、携帯機器７が中継装置となって）行われるようになっていても良い。

[0092] また、鍵発行サーバ９と携帯機器７と車載装置５との何れか同士の通信は、有線通信であっても良い。

[0093] また、鍵発行サーバ９から携帯機器７にも、鍵と共に有効期限情報が送信されても良い。その場合、携帯機器７は、鍵発行サーバ９からの有効期限情報は無視して破棄すれば良い。

[0094] 以上、本開示の実施形態について説明したが、本開示は上記実施形態に限定されることなく、種々の形態を採り得る。また、前述の数値も一例であり他の値でも良い。

[0095] 例えば、上記実施形態における１つの構成要素が有する機能を複数の構成要素として分散させたり、複数の構成要素が有する機能を１つの構成要素に統合させたりしてもよい。また、上記実施形態の構成の一部を省略してもよい。

[0096] また、上述した車両用通信システム１の他、当該車両用通信システム１を

構成する鍵発行サーバ９、携帯機器７及び車載装置５の各々や、その各々としてコンピュータを機能させるためのプログラム、このプログラムを記録した非一時的な記憶媒体、コンピュータ読み取り可能な非一時的な記憶媒体に保管されたプログラム製品、車両用通信システムの鍵管理方法など、種々の形態で本開示を実現することもできる。

[0097] ここで、この出願に記載されるフローチャート、あるいは、フローチャートの処理は、複数のステップ（あるいはセクションと言及される）から構成され、各ステップは、たとえば、Ｓ１１０と表現される。さらに、各ステップは、複数のサブステップに分割されることができる、一方、複数のステップが合わさって一つのステップにすることも可能である。

[0098] 以上、本開示に係る車両用通信システム、車載装置及び鍵発行装置の実施形態、構成、態様を例示したが、本開示に係る実施形態、構成、態様は、上述した各実施形態、各構成、各態様に限定されるものではない。例えば、異なる実施形態、構成、態様にそれぞれ開示された技術的部を適宜組み合わせて得られる実施形態、構成、態様についても本開示に係る実施形態、構成、態様の範囲に含まれる。

請求の範囲

[請求項1] 車両（３）に搭載された車載装置（５）と、

前記車両の使用者に携帯される携帯機器（７）と、

前記車両の外部に設けられ、前記携帯機器と前記車載装置とに暗号通信用の鍵を発行する鍵発行装置（９）と、を備え、

前記携帯機器と前記車載装置とが、前記鍵発行装置によって発行された前記鍵を記憶し、前記記憶した鍵を用いて暗号通信を行う車両用通信システム（１）において、

前記鍵発行装置から前記車載装置には、前記鍵と、前記鍵の有効期限を示す有効期限情報とが発行され、

前記車載装置は、

前記発行された有効期限情報が示す有効期限が到来したか否かを判定する判定部（Ｓ４１０）と、

前記判定部により前記有効期限が到来したと判定されると、前記鍵発行装置に対して、新たな鍵の発行を要求するための鍵更新要求を送信する更新要求部（Ｓ４２０）と、を備え、

前記鍵発行装置は、

前記鍵更新要求を受信した場合には、新たな鍵を前記携帯機器に発行すると共に、前記新たな鍵と前記新たな鍵についての前記有効期限情報とを前記車載装置に発行する（Ｓ１６０，Ｓ１３０～Ｓ１５０）、

車両用通信システム。

[請求項2] 請求項１に記載の車両用通信システムにおいて、

前記有効期限情報は、前記鍵の発行時からの経過時間を、前記鍵の有効期限として示す車両用通信システム。

[請求項3] 請求項１に記載の車両用通信システムにおいて、

前記有効期限情報は、前記鍵の発行時から前記車両に対して特定の操作が行われた回数を、前記鍵の有効期限として示す車両用通信シス

テム。

[請求項4] 請求項１に記載の車両用通信システムにおいて、

前記有効期限情報は、前記鍵の発行時からの前記車両の走行距離を、前記鍵の有効期限として示す車両用通信システム。

[請求項5] 請求項１に記載の車両用通信システムにおいて、

前記有効期限情報は、前記鍵の発行時から前記車両が特定の状態になった回数を、前記鍵の有効期限として示す車両用通信システム。

[請求項6] 請求項３に記載の車両用通信システムにおいて、

前記特定の操作は、前記車両の電源スイッチをオンする操作である、

車両用通信システム。

[請求項7] 請求項３に記載の車両用通信システムにおいて、

前記特定の操作は、前記車両のドアを開閉する操作である、

車両用通信システム。

[請求項8] 請求項５に記載の車両用通信システムにおいて、

前記特定の状態は、前記車両の燃料が補給されたことである、

車両用通信システム。

[請求項9] 請求項５に記載の車両用通信システムにおいて、

前記特定の状態は、前記車両が特定の場所に行ったことである、

車両用通信システム。

[請求項10] 請求項５に記載の車両用通信システムにおいて、

前記特定の状態は、前記車両の走行速度が所定値以上になったことである、

車両用通信システム。

[請求項11] 請求項５に記載の車両用通信システムにおいて、

前記特定の状態は、前記車両のエンジンの冷却水温が所定値以上になったことである、

車両用通信システム。

[請求項12] 車両（３）に搭載されて、前記車両の使用者に携帯される携帯機器（７）と暗号通信を行い、前記暗号通信に用いる鍵が、前記車両の外部の鍵発行装置（９）によって発行される車載装置（５）であって、

前記鍵発行装置から当該車載装置には、前記鍵と、前記鍵の有効期限を示す有効期限情報とが発行され、

前記発行された有効期限情報が示す有効期限が到来したか否かを判定する判定部（Ｓ４１０）と、

前記判定部により前記有効期限が到来したと判定されると、前記鍵発行装置に対して、新たな鍵の発行を要求するための鍵更新要求を送信する更新要求部（Ｓ４２０）と、

を備える車載装置。

[請求項13] 車両（３）の使用者に携帯される携帯機器（７）と、前記車両に搭載された車載装置（５）とに、暗号通信用の鍵を発行する鍵発行装置（９）であって、

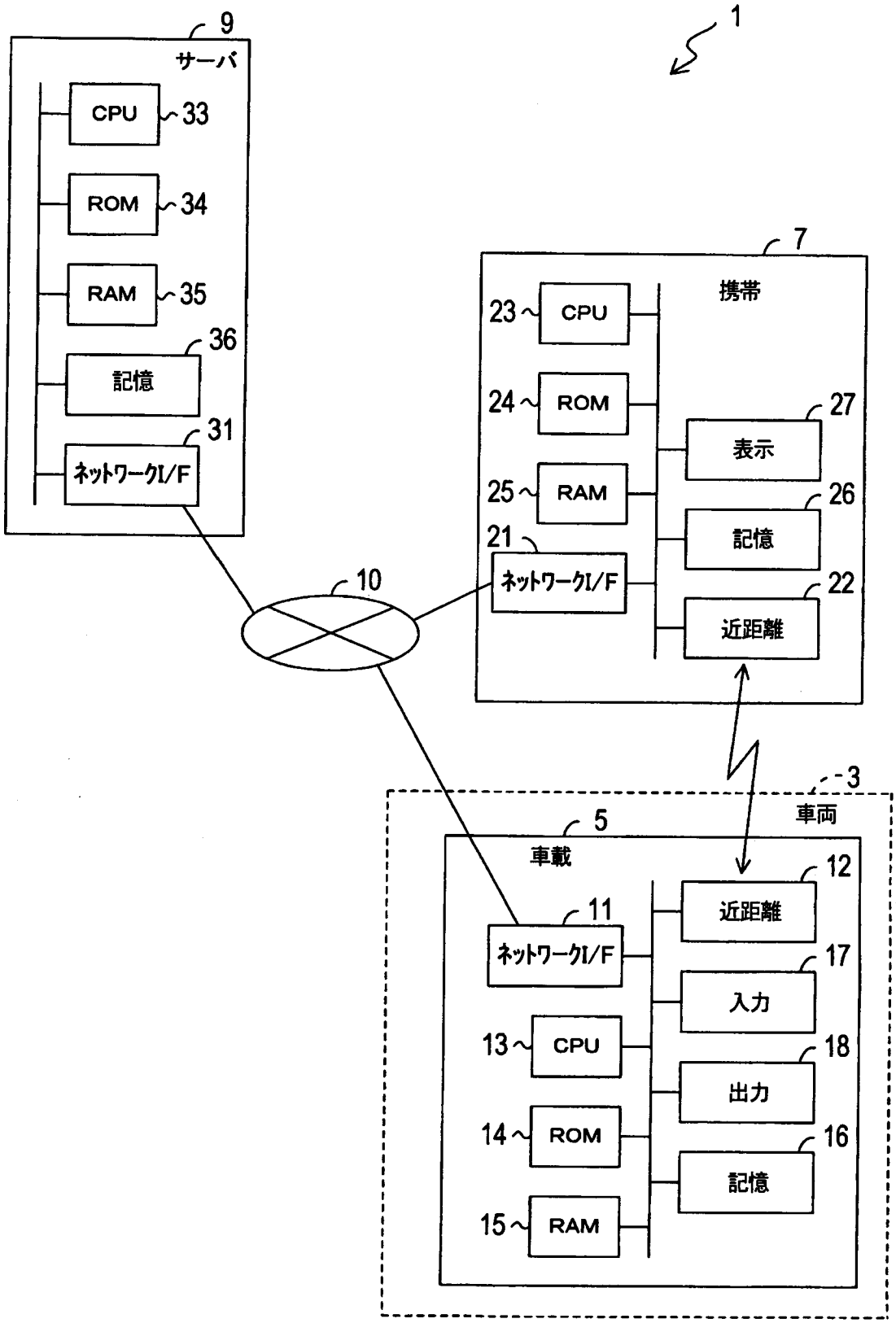
前記携帯機器に、前記鍵を発行する第１の発行部（Ｓ１４０）と、

前記車載装置に、前記鍵と、前記鍵の有効期限を示す有効期限情報とを発行する第２の発行部（Ｓ１５０）と、

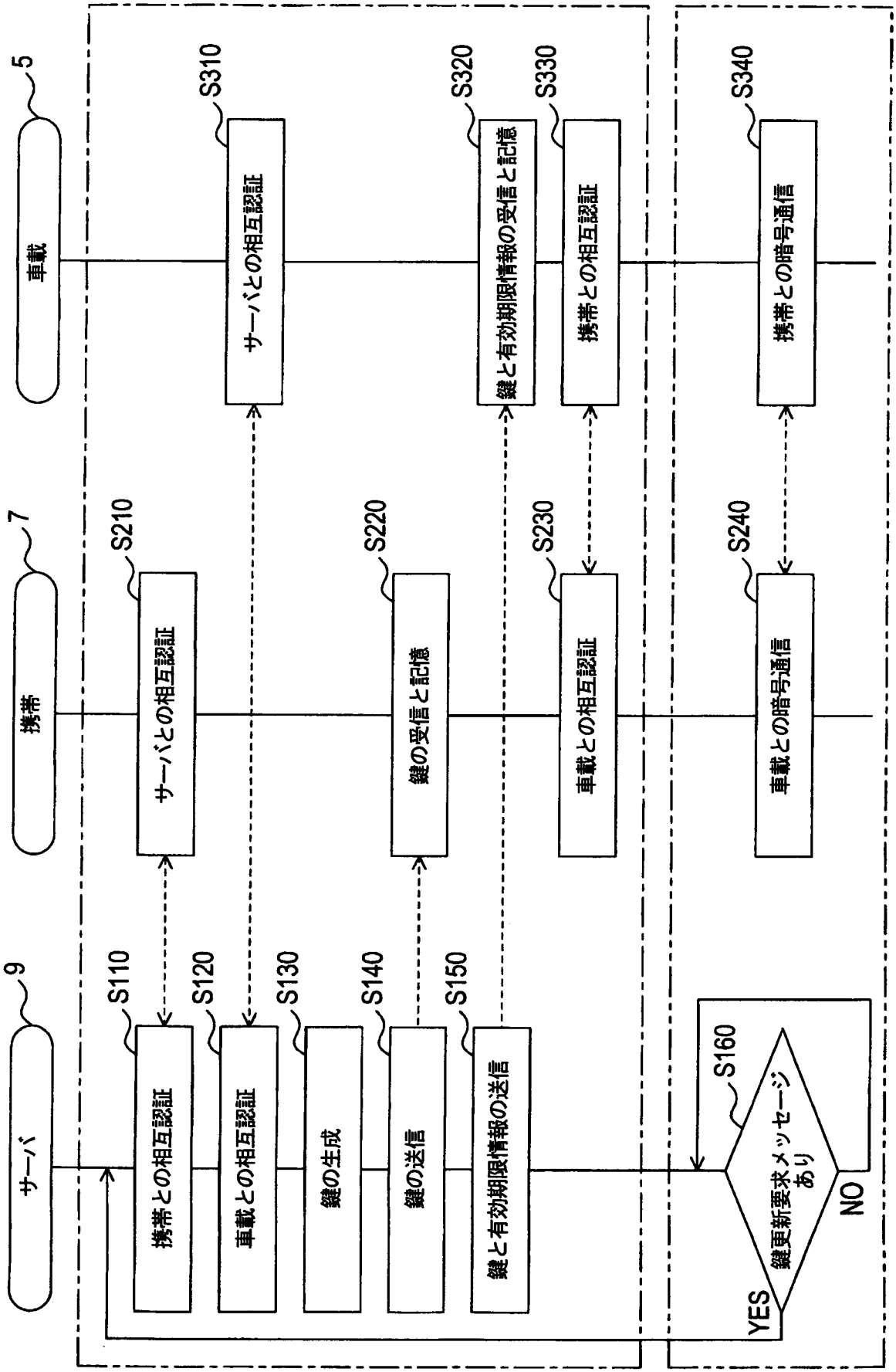
前記車載装置に発行された前記有効期限情報が示す有効期限が到来すると前記車載装置から送信されて来る鍵更新要求を受信したか否かを判定し、前記鍵更新要求を受信したと判定した場合には、新たな前記鍵を前記第１の発行部に発行させると共に、前記新たな鍵と前記新たな鍵についての前記有効期限情報とを前記第２の発行部に発行させる鍵更新部（Ｓ１３０，Ｓ１６０）と、

を備える鍵発行装置。

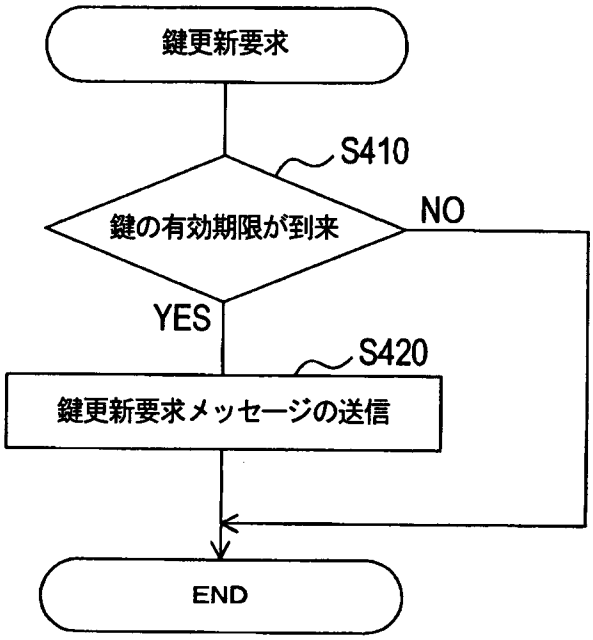
[図1]


1
9
サーバ
CPU
33
ROM
34
RAM
35
36
記憶
31
ネットワークI/F
10
7
携帯
23
CPU
24
ROM
25
RAM
21
ネットワークI/F
27
表示
26
記憶
22
近距離
3
車両
5
車載
11
ネットワークI/F
12
近距離
17
入力
13
CPU
18
出力
14
ROM
16
記憶
15
RAM

[図2]


5
車載
S310
サーバとの相互認証
S320
鍵と有効期限情報の受信と記憶
S330
携帯との相互認証
S340
携帯との暗号通信
7
携帯
S210
サーバとの相互認証
S220
鍵の受信と記憶
S230
車載との相互認証
S240
車載との暗号通信
9
サーバ
S110
携帯との相互認証
S120
車載との相互認証
S130
鍵の生成
S140
鍵の送信
S150
鍵と有効期限情報の送信
S160
鍵更新要求メッセージ
あり
YES
NO

[図3]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/002062

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *H04W4/04*(2009.01)i, *H04W12/04*(2009.01)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, H04W4/04, H04W12/04

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.
Y	JP 2009-275363 A (Tokai Rika Co., Ltd.), 26 November 2009 (26.11.2009), paragraphs [0014] to [0041]; fig. 1, 2 (Family: none)	1-13
Y	JP 2008-291566 A (NTT Docomo Inc.), 04 December 2008 (04.12.2008), paragraphs [0006] to [0044]; fig. 1, 3 (Family: none)	1-13
Y	JP 2012-49993 A (Toyota InfoTechnology Center, Co., Ltd.), 08 March 2012 (08.03.2012), paragraphs [0025] to [0048]; fig. 1 (Family: none)	1-13

☒ 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
28 June 2016 (28.06.16)	05 July 2016 (05.07.16)

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/002062

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2009-302848 A (Tokai Rika Co., Ltd.), 24 December 2009 (24.12.2009), paragraphs [0018] to [0052] (Family: none)	2-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／００２０６２

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, H04W4/04(2009.01)i, H04W12/04(2009.01)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, H04W4/04, H04W12/04

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
Y	JP 2009-275363 A (株式会社東海理化電機製作所) 2009.11.26, 段落 [0014] － [0041], 図 1, 2 (ファミリーなし)	1-13
Y	JP 2008-291566 A (株式会社エヌ・ティ・ティ・ドコモ) 2008.12.04, 段落 [0006] － [0044], 図 1, 3 (ファミリーなし)	1-13

☑　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
２８．０６．２０１６	０５．０７．２０１６

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　６３０４
青木　重徳
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
Y	JP 2012-49993 A (株式会社トヨタＩＴ開発センター) 2012.03.08, 段落［0025］－［0048］, 図１ (ファミリーなし)	1-13
Y	JP 2009-302848 A (株式会社東海理化電機製作所) 2009.12.24, 段落［0018］－［0052］ (ファミリーなし)	2-11