

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5031994号
(P5031994)

(45) 発行日 平成24年9月26日 (2012. 9. 26)

(24) 登録日 平成24年7月6日 (2012. 7. 6)

(51) Int.Cl.

H04L 9/32 (2006.01)

F I

H04L 9/00 675B

請求項の数 9 (全 64 頁)

(21) 出願番号	特願2005-77860 (P2005-77860)	(73) 特許権者	000006013
(22) 出願日	平成17年3月17日 (2005. 3. 17)		三菱電機株式会社
(65) 公開番号	特開2006-262184 (P2006-262184A)		東京都千代田区丸の内二丁目7番3号
(43) 公開日	平成18年9月28日 (2006. 9. 28)	(74) 代理人	100099461
審査請求日	平成19年11月12日 (2007. 11. 12)		弁理士 溝井 章司
		(72) 発明者	齋藤 和美
			東京都千代田区丸の内二丁目2番3号 三
			菱電機株式会社内
		(72) 発明者	米田 健
			東京都千代田区丸の内二丁目2番3号 三
			菱電機株式会社内
		(72) 発明者	辻 宏郷
			東京都千代田区丸の内二丁目2番3号 三
			菱電機株式会社内

最終頁に続く

(54) 【発明の名称】 権限委譲システムおよび制御装置および権限委譲方法

(57) 【特許請求の範囲】

【請求項1】

所定の装置を制御する制御装置と、上記制御装置に対して指示する権限を有する権限所有装置と、上記権限所有装置から上記権限を借用することにより、上記制御装置に対して指示可能となる権限借用装置とを備える権限委譲システムにおいて、

上記権限借用装置は、

上記権限借用装置を識別可能な借用装置識別情報を上記権限所有装置へ送信する第1借用装置送信部と、

上記借用装置識別情報と指示とを上記制御装置へ送信する第2借用装置送信部とを備え、

上記権限所有装置は、

上記第1借用装置送信部が送信した上記借用装置識別情報を受信する所有装置受信部と、

上記所有装置受信部が受信した上記借用装置識別情報と、上記権限借用装置に委譲する権限に関する権限情報とを含むチケットを生成するチケット生成部と、

上記チケット生成部が生成した上記チケットを上記制御装置へ送信する所有装置送信部とを備え、

上記制御装置は、

上記所有装置送信部が送信した上記チケットを受信する第1制御装置受信部と、

上記第2借用装置送信部が送信した上記借用装置識別情報と上記指示とを受信する第2

制御装置受信部と、

上記第1制御装置受信部が受信したチケットを参照し、上記第2制御装置受信部が受信した上記借用装置識別情報を含むチケットが存在するかを判定する制御装置判定部と、

上記借用装置識別情報を含むチケットが存在すると上記制御装置判定部が判定した場合、上記チケットに含まれる上記権限情報に基づき、上記権限借用装置から受信した上記指示に従い、上記所定の装置を制御する制御部と
を備えることを特徴とする権限委譲システム。

【請求項2】

上記チケット生成部は、上記権限所有装置が有する権限のうち、一部の権限だけがあることを示す情報を、上記権限情報として含むチケットを生成する
ことを特徴とする請求項1記載の権限委譲システム。

10

【請求項3】

上記チケット生成部は、上記権限所有装置が上記制御装置に対して指示することが可能な操作を制限する制限情報を、上記権限情報として含むチケットを生成する
ことを特徴とする請求項2記載の権限委譲システム。

【請求項4】

上記チケット生成部は、上記権限所有装置が上記制御装置に対して指示することにより、制御することが可能な装置を制限する制限情報を、上記権限情報として含むチケットを生成する
ことを特徴とする請求項2記載の権限委譲システム。

20

【請求項5】

上記チケット生成部は、上記権限所有装置が上記制御装置に対して指示することが可能な操作のうち、上記権限借用装置が指示することができる操作を示す許可情報を、上記権限情報として含むチケットを生成する
ことを特徴とする請求項2記載の権限委譲システム。

【請求項6】

上記権限所有装置は、さらに、

上記チケット生成部が上記チケットを生成した場合、上記チケットを記憶する所有装置記憶部

を備えることを特徴とする請求項1に記載の権限委譲システム。

30

【請求項7】

上記チケット生成部は、上記権限借用装置が制御装置へ指示をすることができる期限である有効期限を含む上記チケットを生成し、

上記権限所有装置は、さらに、

上記所有装置記憶部が記憶した上記チケットに含まれる上記有効期限が有効でなくなった場合、そのチケットを削除する所有装置削除部
を備えることを特徴とする請求項6記載の権限委譲システム。

【請求項8】

所定の装置を制御する制御装置において、

権限借用装置を識別可能な借用装置識別情報と、制御装置に対して指示する権限を有する権限所有装置から上記権限借用装置に委譲される権限に関する権限情報とを含むチケットを、上記権限所有装置から受信する第1制御装置受信部と、

40

上記借用装置識別情報と指示とを上記権限借用装置から受信する第2制御装置受信部と、

上記第1制御装置受信部が受信したチケットを参照し、上記第2制御装置受信部が受信した上記借用装置識別情報を含むチケットが存在するかを判定する制御装置判定部と、

上記借用装置識別情報を含むチケットが存在すると上記制御装置判定部が判定した場合、上記チケットに含まれる上記権限情報に基づき、上記権限借用装置から受信した上記指示に従い、上記所定の装置を制御する制御部と
を備えることを特徴とする制御装置。

50

【請求項 9】

所定の装置を制御する制御装置と、上記制御装置に対して指示する権限を有する権限所有装置と、上記権限所有装置から上記権限を借用することにより、上記制御装置に対して指示可能となる権限借用装置とを備える権限委譲システムの権限委譲方法において、

上記権限借用装置が、上記権限借用装置を識別可能な借用装置識別情報を上記権限所有装置へ送信する第 1 借用装置送信工程と、

上記権限借用装置が、上記借用装置識別情報と指示とを上記制御装置へ送信する第 2 借用装置送信工程と、

上記権限所有装置が、上記第 1 借用装置送信工程で送信した上記借用装置識別情報を受信する所有装置受信工程と、

上記権限所有装置が、上記所有装置受信工程で受信した上記借用装置識別情報と、上記権限借用装置に委譲する権限に関する権限情報とを含むチケットを生成するチケット生成工程と、

上記権限所有装置が、上記チケット生成工程で生成した上記チケットを上記制御装置へ送信する所有装置送信工程と、

上記制御装置が、上記所有装置送信工程で送信した上記チケットを受信する第 1 制御装置受信工程と、

上記制御装置が、上記第 2 借用装置送信工程で送信した上記借用装置識別情報と上記指示とを受信する第 2 制御装置受信工程と、

上記制御装置が、上記第 1 制御装置受信工程で受信したチケットを参照し、上記第 2 制御装置受信工程で受信した上記借用装置識別情報を含むチケットが存在するかを判定する制御装置判定工程と、

上記制御装置が、上記借用装置識別情報を含むチケットが存在すると上記制御装置判定工程で判定した場合、上記チケットに含まれる上記権限情報に基づき、上記権限借用装置から受信した上記指示に従い、上記所定の装置を制御する制御工程とを備えることを特徴とする権限委譲方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、例えば、権限所有装置の有する権限を権限借用装置へ委譲する権限所有装置および権限借用装置および制御装置および権限委譲システムおよび権限所有プログラムおよび権限所有方法に関するものである。

【背景技術】

【0002】

例えば、特開 2004-88339 号公報では、スマートキーシステムは、車両の借用者が車両の所有者から通知された登録情報を用いて接続した管理サーバから識別コードを取得することによって、所有者は借用者へ車両のキーの貸与を行っていた。ここで、登録情報とは、パスワードなどである。また識別コードとは、車両のキーなどである。

【特許文献 1】特開 2004-88339 号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

従来のスマートキーシステムは、車両の借用者が車両のキーを取得するために必ず管理サーバに接続する。そのため、管理サーバが停止した場合や、管理サーバへ負荷が集中して管理サーバとの接続ができない状態が発生した場合には、車両の借用者が識別コードを取得することは困難となるという課題があった。

【課題を解決するための手段】

【0004】

本発明にかかる権限所有装置は、所定の装置を制御する制御装置に対して指示する権限があることを識別可能なチケットを取得して上記制御装置へ指示をする権限借用装置に対

10

20

30

40

50

してネットワークを介してチケットを送信する上記権限所有装置において、上記権限があることを識別可能な署名を付けたチケットを生成するチケット生成部と、上記チケット生成部が生成した上記チケットを上記権限借用装置へ送信する所有装置送信部とを備えることを特徴とする。

【発明の効果】

【0005】

本発明による権限委譲システムによれば、権限所有装置から権限借用装置へチケットを送信する。そのため、管理サーバを介することなく、権限所有装置から権限借用装置へ権限を委譲することが可能である。

【発明を実施するための最良の形態】

10

【0006】

以下、本発明の一例を図面に示す実施の形態に基づいて説明する。

【0007】

図1は、実施の形態にかかる権限所有装置100と権限借用装置200と制御装置300とのハードウェア構成図の一例である。ここでは、権限所有装置100と権限借用装置200とは携帯電話機であるとする。権限所有装置100と権限借用装置200とは、これに限るものではなく、PHS (Personal Handyphone System、登録商標)やPDA (Personal Digital Assistance)などに代表される携帯端末や、スマートキー、パーソナルコンピュータやワークステーションなどに代表されるコンピュータなどでも構わない。また、ここでは、制御装置300は、車両であるとする。制御装置300は、これに限るものではなく、玄関ドア、建物の入退場口、コンピュータ、電化製品、その他一般の制御機器などでも構わない。

20

【0008】

車両所有者の携帯電話11001は車両11201を所有する者(以下、車両所有者)が保持している携帯電話である。ここでは、権限所有装置100は、車両所有者の携帯電話11001であるとする。

車両借用者の携帯電話11101は車両11201を借用する者(以下、車両借用者)が所有している携帯電話である。ここでは、権限借用装置200は、車両借用者の携帯電話11101であるとする。

車両11201は車両所有者が保持しており、車両借用者に貸与する車両である。ここでは、制御装置300は、車両11201であるとする。

30

【0009】

車両所有者の携帯電話11001は、通信部11002、表示部11003、入力部11004、制御部11005、記憶部11006、カード部11007を備える。

通信部11002は、無線通信や赤外線通信などを用いて他の機器との通信を行う。通信部11002は、例えば、通信ボードやアンテナなどを備える。

表示部11003は、制御部11005から送信された情報を画面に表示する。表示部11003は、例えば、LCD (Liquid Crystal Display) などである。

入力部11004は、車両所有者に情報を入力させる。入力部11004は、例えば、操作ボタンやタッチパネルなどである。

40

制御部11005は、車両所有者の携帯電話11001の処理を制御する。

記憶部11006は、車両所有者の携帯電話11001の処理に必要なプログラムやデータを格納する。記憶部11006は、RAMなどの揮発性メモリやROMなどの不揮発性メモリなどである。

カード部11007は、内部にUIM (User Identity Module) 11008などを装着可能である。カード部11007は、SD (Secure Digital) スロットとSDメモリカードとなどでも構わない。また、UIM 11008は、その他の記憶装置や携帯電話の記憶部を用いて情報を格納してもよい。

UIM 11008は、通信部11009、制御部11010、記憶部11011を備え

50

る。

通信部11009は、無線通信やその他の通信手段を用いて他の機器との通信を担う。
通信部11009は、例えば、通信ボードやアンテナなどを備える。

制御部11010は、UIM11008の処理を制御する。

記憶部11011は、UIM11008の処理に必要なプログラムやデータを格納する。
記憶部11011は、RAMなどの揮発性メモリやROMなどの不揮発性メモリなどである。また、記憶部11011に記憶したプログラムは、車両所有者の携帯電話11001に備えたCPU(Central Processing Unit)で処理される。

例えば、車両所有者は、車両を購入する際に、車両を操作するために必要なプログラムやデータを車両所有者の携帯電話11001に格納する。格納方法としては、販売店の専用端末に車両所有者の携帯電話11001を接続してダウンロードする方法がある。また、別の格納方法としては、販売店が作成したCD-ROM(Compact Disk Read-Only Memory)などの外部記憶媒体を車両所有者の計算機に設置し、計算機に車両所有者の携帯電話11001を接続してダウンロードする方法がある。

【0010】

車両借用者の携帯電話11101は、通信部11102、表示部11103、入力部11104、制御部11105、記憶部11106、カード部11107を備える。車両借用者の携帯電話11101についての各部の機能は、車両所有者の携帯電話11001と同様の構成である。

【0011】

車両11201は、通信部11202、制御部11203、記憶部11204を備える。

通信部11202は、無線通信や赤外線通信などを用いて他の機器との通信を行う。通信部11202は、例えば、通信ボードやアンテナなどを備える。

制御部11203は、車両11201の動作を制御する。

記憶部11204は、車両11201が動作するために必要なプログラムやデータを格納する。記憶部11204は、RAMなどの揮発性メモリやROMなどの不揮発性メモリなどである。プログラムやデータなどの格納方法としては、例えば、車両メーカーの専用機器や専用端末などに記憶部11204を接続してダウンロードする。記憶部11204が記憶したプログラムは、車両11201に備えたCPUで処理される。

【0012】

実施の形態1.

まず、実施の形態1について説明する。実施の形態1では、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話11101が車両11201を操作する動作とを説明する。

【0013】

図2は、実施の形態1にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。つまり、図2は、車両所有者の携帯電話11001と車両借用者の携帯電話11101と車両11201との機能ブロック図である。

【0014】

権限所有装置100は、チケット生成部101、所有装置送信部102、所有装置受信部103、所有装置記憶部104を備える。

チケット生成部101は、制御装置に対して指示する権限があることを識別可能なチケットを生成する。つまり、ここでは、チケット生成部101は、車両11201に対して指示する権限があることを識別可能なチケットを生成する。

所有装置送信部102は、チケット生成部101が生成したチケットを権限借用装置200へ送信する。

所有装置受信部103は、権限借用装置200が送信した情報などを受信する。

所有装置記憶部104は、権限所有装置100の処理に必要なプログラムやデータを格

10

20

30

40

50

納する。また、所有装置記憶部104は、チケット生成部101が生成したチケットを記憶しても構わない。ここでは、所有装置記憶部104は、記憶部11006やUIM11008の記憶部11011などである。

【0015】

権限借用装置200は、借用装置送信部201、借用装置受信部202、借用装置記憶部203、借用装置指示部204、借用装置判定部205を備える。

借用装置送信部201は、後述する借用装置記憶部203が記憶したチケットを制御装置300へ送信する。

借用装置受信部202は、権限があることを識別可能な署名を付けたチケットを権限所有装置100から受信する。

借用装置記憶部203は、借用装置受信部202が受信した上記チケットを記憶する。

借用装置指示部204は、制御装置300へ指示をする。つまり、借用装置指示部204は、車両11201へ指示をする。

借用装置判定部205は、権限所有装置100から受信したチケットなどを検証する。

【0016】

制御装置300は、制御装置送信部301、制御装置受信部302、制御装置記憶部303、制御装置判定部304、制御部305を備える。

制御装置送信部301は、権限所有装置100、権限借用装置200などへ情報を送信する。

制御装置受信部302は、権限があることを識別可能な署名を付けたチケットなどを権限借用装置200から受信する。また、制御装置受信部302は、権限所有装置100と権限借用装置200とから指示を受信する。

制御装置記憶部303は、チケットが正しいかを判定するための情報などを記憶する。

制御装置判定部304は、制御装置記憶部303が記憶した情報に基づいて、チケットが正しいかを判定する。

制御部305は、制御装置判定部304が、チケットが正しいと判定した場合、権限借用装置200から受信した指示を受付ける。また、制御部305は、権限所有装置100からの指示を受付ける。

【0017】

ここでは、権限所有装置100である車両所有者の携帯電話11001と、権限借用装置200である車両借用者の携帯電話11101と、制御装置300である車両11201とが記憶したプログラムが、上述したの各部を制御して動作するものとして説明する。

【0018】

図3は、車両所有者の携帯電話11001の記憶部11006に格納されたプログラムである。車両操作権限貸与プログラム21001は車両11201の操作権限を車両借用者の携帯電話11101に貸与するための処理を行うプログラムである。車両操作権限借用プログラム21002は車両11201の操作権限を車両所有者の携帯電話11001から借用するための処理を行うプログラムである。端末側車両操作プログラム21003は車両11201を操作するための処理を行うプログラムである。

図4は、車両所有者の携帯電話11001におけるUIM11008の記憶部11011に格納されたデータである。車両所有者の秘密鍵31001は公開鍵暗号方式における秘密鍵であり、車両所有者の携帯電話11001に対応する。車両所有者の公開鍵31002は公開鍵暗号方式における公開鍵であり、車両所有者の秘密鍵31001と対をなす。

【0019】

図5は、車両借用者の携帯電話11101の記憶部11106に格納されたプログラムである。図6は、車両借用者の携帯電話11101におけるUIM11108の記憶部11111に格納されたデータである。各プログラムおよび各データの機能は、車両所有者の携帯電話11001の場合と同様であるので、ここでは省略する。

【0020】

10

20

30

40

50

図7は、車両11201の記憶部11204に格納されたプログラムおよびデータである。車両の秘密鍵61001は公開鍵暗号方式における秘密鍵であり、車両11201に対応する。車両の公開鍵61002は公開鍵暗号方式における公開鍵であり、車両の秘密鍵61001と対をなす。車両所有者の公開鍵31002は公開鍵暗号方式における公開鍵であり、車両所有者の公開鍵31002と同一のものである。車両側車両操作プログラム61004は車両11201が動作するための処理を行うプログラムである。

【0021】

次に、上記のように構成された実施の形態1の動作について説明する。実施の形態1の動作は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話11101が車両11201を操作する動作とを備える。

10

【0022】

まず、車両操作権限を委譲する動作について図8、図9、図10を用いて説明する。図8は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。図9は、車両所有者の携帯電話11001の車両操作権限貸与プログラム21001の一連の動作を示すフローチャートである。図10は、車両借用者の携帯電話11101の車両操作権限借用プログラム41002の一連の動作を示すフローチャートである。

【0023】

まず、車両所有者の携帯電話11001は、車両操作権限貸与プログラム21001を起動する。また、車両借用者の携帯電話11101は、車両操作権限借用プログラム41002を起動する。

20

【0024】

所有装置公開鍵要求ステップS91001では、所有装置送信部102は、車両借用者の携帯電話11101に対して車両借用者の公開鍵要求を送信する。

【0025】

借用装置公開鍵要求受信ステップS101001では、借用装置受信部202は、車両借用者の公開鍵要求を受信する。

【0026】

借用装置公開鍵送信ステップS101002では、借用装置送信部201は、車両所有者の携帯電話11001に対して車両借用者の公開鍵51002を送信する。

30

【0027】

所有装置公開鍵受信ステップS91002では、所有装置受信部103は、車両借用者の公開鍵51002を受信する。所有装置記憶部104は、受信した公開鍵を一時的に記憶する。例えば、図1に示すUIM11008の記憶部11011は、受信した公開鍵を一時的に格納する。

【0028】

所有装置公開鍵送信ステップS91003では、所有装置送信部102は、車両借用者の携帯電話11101に対して車両所有者の公開鍵31002を送信する。

【0029】

借用装置公開鍵受信ステップS101003では、借用装置受信部202は、車両所有者の公開鍵31002を受信する。借用装置記憶部203は、受信した公開鍵を一時的に記憶する。例えば、図1に示すUIMの記憶部11111は、受信した公開鍵を一時的に格納する。

40

【0030】

借用装置公開鍵受信完了通知ステップS101004では、借用装置送信部201は、車両所有者の携帯電話11001に対して公開鍵受信完了通知を送信する。

【0031】

所有装置公開鍵受信完了受信ステップS91004では、所有装置受信部103は、公開鍵受信完了通知を受信する。

50

【0032】

チケット生成ステップS91005では、チケット生成部101は、車両借用者のチケットを作成する。チケット生成部101が生成したチケットは、車両借用者の公開鍵51002と車両借用者の操作許可情報111112と操作制限情報111113とを備える。ここで、所有装置記憶部104は、チケット生成部101が生成したチケットを記憶しても構わない。

車両借用者の操作許可情報111112と操作制限情報111113とは、車両操作権限を委譲する前に、あらかじめ車両所有者により設定されている。例えば、車両所有者の携帯電話11001は、車両借用者の操作許可情報111112や操作制限情報111113の入力画面を表示し、車両所有者に入力を促す。操作許可情報111112は、車両借用者に許可する車両操作を含む情報である。例えば、操作許可情報111112は、ドアのロックとアンロック、エンジンの始動、トランクのロックとアンロック、カーナビやオーディオなど車載器の使用の有無などである。操作制限情報111113は、車両借用者に許可する車両操作の範囲を含む情報である。例えば、操作制限情報111113は、走行距離、走行範囲、利用時間などである。図11は、車両借用者の操作許可情報111112や操作制限情報111113の入力画面の一例である。

車両借用者の操作許可情報111112や操作制限情報111113の入力は、車両11201の操作権限を委譲する処理の必ずしも最初に行う必要はない。車両借用者の操作許可情報111112や操作制限情報111113の入力は、車両所有者が事前に操作許可情報111112、操作制限情報111113を入力し、車両所有者の携帯電話11001の記憶部11006に保管しておいてもよい。この場合において、車両11201の操作権限を委譲する場合は、入力処理を省略したり、いくつかの登録情報の中から車両所有者が最適な情報を選択したりすることができ、車両所有者の利便性が向上する。

【0033】

チケット署名ステップS91006では、チケット生成部101は、車両所有者の秘密鍵31001を用いてチケットの署名情報を作成する。

【0034】

チケット送信ステップ（所有装置送信ステップ）S91007では、所有装置送信部102は、署名付きチケットを車両借用者の携帯電話11101へ送信する。

【0035】

チケット受信ステップS101005では、借用装置受信部202は、署名付きチケットを受信する。

【0036】

借用装置チケット検証ステップS101006では、借用装置判定部205は、車両所有者の公開鍵31002を用いて署名情報を検証する。

【0037】

借用装置チケット検証ステップS101007では、借用装置判定部205は、検証に成功した場合、次のステップへ進む。借用装置判定部205は、検証に失敗した場合、プログラムを終了する。

【0038】

借用装置チケット記憶ステップS101008では、借用装置記憶部203は、署名付きチケットを記憶する。つまり、図1に示すUIMの記憶部11111は、署名付きチケットを格納する。

【0039】

チケット受信完了通知ステップS101009では、借用装置送信部201は、車両所有者の携帯電話11001に対してチケット受信完了通知を送信する。車両借用者の携帯電話11101は、チケット受信完了通知を借用装置送信部201が送信後、プログラムを終了する。

【0040】

チケット受信完了通知受信ステップS91008では、所有装置受信部103は、チケ

10

20

30

40

50

ット受信完了通知を受信する。車両所有者の携帯電話１１００１は、チケット受信完了通知を所有装置受信部１０３が受信後、プログラムを終了する。

【００４１】

車両所有者の携帯電話１１００１と車両借用者の携帯電話１１１０１とは、安全な通信経路上で通信する。例えば、携帯電話の暗号機能付きのメールを用いた通信や、非接触ＩＣカードとリーダー／ライター一体型携帯電話などのように非接触ＩＣカード機能を利用して携帯電話と携帯電話とを接触させて行うデータ交換機能を用いた通信などを行う。

【００４２】

図１２は、車両所有者の携帯電話１１００１が車両借用者の携帯電話１１１０１に対して車両操作権限を委譲した後、車両借用者の携帯電話１１１０１のＵＩＭ１１１０８の記憶部１１１１１に格納されている情報である。ＵＩＭ１１１０８の記憶部１１１１１には、車両操作権限を委譲する前と比較して、車両所有者の署名付きチケット１１１００１が加わっている。

10

【００４３】

次に、車両所有者の携帯電話１１００１が車両１１２０１を操作する動作について図１３、図１４、図１５を用いて説明する。図１３は、車両所有者の携帯電話１１００１が車両１１２０１を操作する一連の動作を示すメッセージのシーケンス図である。図１４は、車両所有者または車両借用者（以下、車両利用者）の携帯電話１１００１または１１１０１の端末側車両操作プログラム２１００３または４１００３の一連の動作を示すフローチャートである。図１５は、車両１１２０１の車両側車両操作プログラム６１００４の一連の動作を示すフローチャートである。

20

【００４４】

通信リンク確立ステップＳ１３１００１およびＳ１４１００１では、車両側車両操作プログラム６１００４は、制御装置送信部３０１を介し、携帯電話に対して応答要求を送信する。車両所有者の携帯電話１１００１が車両１１２０１に近づき、車両所有者の携帯電話１１００１の端末側車両操作プログラム２１００３が応答要求を受信することによって、車両１１２０１と車両所有者の携帯電話１１００１間の通信リンクを確立する。

【００４５】

制御装置公開鍵要求ステップＳ１４１００２では、制御装置送信部３０１は、車両所有者の携帯電話１１００１と車両１１２０１とが通信リンク確立したら、車両所有者の携帯電話１１００１に対して公開鍵要求を送信する。

30

例えば、車両側車両操作プログラム６１００４は、車両所有者が車両１１２０１のドア、エンジン、トランクのノブを回した時にステップＳ１４１００２以降の認証処理を実行する。ＥＴＣ、カーナビ、オーディオなど頻繁に操作する装置については操作毎に認証処理を行わず、直前に行われた認証処理の結果に基づいてステップＳ１４１００７の操作可能状態へ移行するなどしても構わない。

【００４６】

利用装置公開鍵要求受信ステップＳ１３１００２では、所有装置受信部１０３は、公開鍵要求を受信する。

【００４７】

40

利用装置データ送信ステップＳ１３１００３では、所有装置送信部１０２は、車両１１２０１に対して車両所有者の公開鍵３１００２を送信する。車両所有者の携帯電話１１００１は、車両所有者の公開鍵３１００２を送信後、プログラムを終了する。

【００４８】

制御装置データ受信ステップＳ１４１００３では、制御装置受信部３０２は、車両所有者の公開鍵３１００２を受信する。

【００４９】

データ解析ステップＳ１４１００４では、制御装置判定部３０４は、受信したデータの種類を解析する。

【００５０】

50

制御装置署名検証ステップS141105では、制御装置判定部304は、車両所有者の携帯電話11001からのデータであった場合、制御装置記憶部303に記憶している車両利用者の公開鍵と照合する。つまり、制御装置判定部304は、車両11201の記憶部11204に格納している車両利用者の公開鍵と照合する。

【0051】

制御装置署名検証ステップS141106では、制御装置判定部304は、照合が成功した場合、次のステップに進む。制御装置判定部304は、照合が失敗した場合、プログラムを終了する。

【0052】

操作可能状態移行ステップS141007では、車両側車両操作プログラム61004は、車両操作可能状態へ移行する。車両側車両操作プログラム61004は、例えば、ドアのアンロック、エンジン始動などの操作を可能な状態とする。

【0053】

車両所有者の携帯電話11001と車両11201とは、赤外線通信などにより通信が行われる。

【0054】

次に、車両借用者の携帯電話11101が車両11201を操作する動作について図16、図14、図15を用いて説明する。図16は、車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【0055】

ステップS131001からステップS131002とステップS141001からステップS141002は、上述した車両所有者の携帯電話11001が車両11201を操作する動作の場合と同様であるので、ここでは省略する。

【0056】

利用装置データ送信ステップS131003では、借用装置送信部201は、車両11201に対して署名付きチケットを送信する。車両借用者の携帯電話11101は、署名付きチケットを送信後、プログラムを終了する。

【0057】

制御装置データ受信ステップS141003では、制御装置受信部302は、署名付きチケットを受信する。

【0058】

データ解析ステップS141004では、制御装置判定部304は、受信したデータの種類を解析する。

【0059】

制御装置署名検証ステップS141105では、制御装置判定部304は、車両借用者の携帯電話11101からのデータであった場合、記憶部11204に格納されている利用者の公開鍵を用いて署名を検証する。

【0060】

制御装置署名検証ステップS141106では、制御装置判定部304は、検証に成功した場合、次のステップへ進む。制御装置判定部304は、検証に失敗した場合、プログラムを終了する。

【0061】

操作可能状態移行ステップS141007では、車両側車両操作プログラム61004は、操作許可情報111112と操作制限情報111113に基づいて、車両操作可能状態へ移行する。

例えば、車両側車両操作プログラム61004は、操作許可情報111112にはドアとエンジンの操作許可が含まれ、操作制限情報111113には利用時間と走行距離が含まれている場合、まず、車両側車両操作プログラム61004は現在時刻を取得し利用時間と比較する。現在時刻が利用時間内の場合、車両側車両操作プログラム61004は、ドアとエンジンの操作を実行可能とする。現在時刻が利用時間を過ぎていれば、車両側車

10

20

30

40

50

両操作プログラム 61004 は、ドアとエンジンの操作を実行可能としない。また、車両側車両操作プログラム 61004 は、車両借用者が車両 11201 を走行させた総距離を計算し操作制限情報 11113 の走行距離と比較する。総距離が走行距離を超過した場合、車両側車両操作プログラム 61004 は、エンジンの操作を実行可能としない。

【0062】

車両借用者の携帯電話 11101 と車両 11201 とは、赤外線通信などにより通信が行われる。

【0063】

以上のように、実施の形態 1 では、車両所有者の携帯電話 11001 と車両借用者の携帯電話 11101 との間で通信を行う。そして、車両所有者の携帯電話 11001 は、車両借用者の携帯電話 11101 へ、車両 11201 を操作するために必要な情報（チケット）を送信している。そのため、実施の形態 1 では、管理サーバを介さずに車両所有者の携帯電話 11001 と車両借用者の携帯電話 11101 との間で車両操作権限を委譲することができる。

10

【0064】

また、車両の所有者は利便性の高い操作により、車両の借用者が操作できる権限の範囲をきめ細かく設定できる。

【0065】

実施の形態 2 .

次に実施の形態 2 について説明する。上述した実施の形態 1 では、車両所有者の携帯電話 11001 から車両借用者の携帯電話 11101 に対してチケットを送信することによって、車両所有者の携帯電話 11001 から車両借用者の携帯電話 11101 へ車両操作権限を委譲するようにした。実施の形態 2 では、車両操作権限を委譲する場合に車両借用者のなりすましを防ぐ動作と、更に車両 11201 を操作する場合に車両利用者のなりすましを防ぐ動作とを説明する。

20

【0066】

実施の形態 2 では、実施の形態 1 における車両操作権限委譲システムで車両操作権限を委譲する場合に、車両借用者の署名を車両所有者の携帯電話 11001 が検証する手順を加える。そのため、実施の形態 2 では、実施の形態 1 の効果に加えて、車両操作権限委譲時に第三者が車両借用者になりすまして不正な車両操作権限委譲を行うことを防ぐことができる。

30

【0067】

また、実施の形態 2 では、車両利用者の携帯電話が車両 11201 を操作する時に車両利用者の署名を車両 11201 が検証する手順を加える。そのため、実施の形態 2 では、チケットを入手した第三者が車両借用者になりすますなどにより不正に車両 11201 を操作することを防ぐことができる。

【0068】

図 17 は、実施の形態 2 にかかる権限所有装置 100 と権限借用装置 200 と制御装置 300 との機能ブロック図である。図 17 に示す機能ブロック図は、図 2 に示す機能ブロック図と概ね同様であるため、差分についてのみ説明する。

40

【0069】

権限所有装置 100 は、さらに、所有装置判定部 105、所有装置識別情報作成部 106 を備える。所有装置判定部 105 は、権限借用装置 200 などから受信した識別情報を判定する。所有装置識別情報作成部 106 は、権限所有装置 100 の識別情報を作成する。所有装置識別情報作成部 106 が作成する識別情報は、権限所有装置であることを認証可能な所有装置認証情報である。

【0070】

権限借用装置 200 は、さらに、借用装置識別情報作成部 206 を備える。借用装置識別情報作成部 206 は、権限借用装置 200 の識別情報を作成する。借用装置識別情報作成部 206 が作成する識別情報は、権限借用装置であることを認証可能な借用装置認証情

50

報である。

制御装置 300 は、さらに、制御装置識別情報作成部 306 を備える。制御装置識別情報作成部 306 は、制御装置 300 の識別情報を作成する。制御装置識別情報作成部 306 が作成する識別情報は、制御装置であることを認証可能な制御装置認証情報である。

【0071】

実施の形態 2 における車両操作権限委譲システムの記憶部の構成は、車両所有者の携帯電話 11001 の UIM 11008 の記憶部 11011 を除いて、実施の形態 1 と同様である。そのため、ここでは差分についてのみ説明する。

【0072】

図 18 は、実施の形態 2 における車両所有者の携帯電話 11001 の UIM 11008 の記憶部 11011 に格納されたデータである。車両所有者の秘密鍵 31001 は公開鍵暗号方式における秘密鍵であり、車両所有者の携帯電話 11001 に対応する。車両所有者の公開鍵 31002 は公開鍵暗号方式における公開鍵であり、車両所有者の秘密鍵 31001 と対をなす。車両 11201 の識別情報は車両 11201 を識別するための情報である。

10

【0073】

次に、上記のように構成された実施の形態 2 の動作について説明する。実施の形態 2 の動作は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話 11101 が車両 11201 を操作する動作とを備える。

20

【0074】

まず、車両操作権限を委譲する動作について図 19、図 20、図 21 を用いて説明する。図 19 は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。図 20 は、車両所有者の携帯電話 11001 の車両操作権限貸与プログラム 21001 の一連の動作を示すフローチャートである。図 21 は、車両借用者の携帯電話 11101 の車両操作権限借用プログラム 41002 の一連の動作を示すフローチャートである。

【0075】

ステップ S92001、ステップ S102001 からステップ S102002 は、実施の形態 1 のステップ S91001、ステップ S101001 からステップ S101002 と同様なので、ここでは説明を省略する。

30

【0076】

所有装置公開鍵受信ステップ S92002 では、所有装置受信部 103 は、車両借用者の公開鍵 51002 を受信する。所有装置記憶部 104 は、受信した公開鍵を一時的に記憶する。例えば、図 1 に示す UIM 11008 の記憶部 11011 は、受信した公開鍵を一時的に格納する。

【0077】

所有装置公開鍵送信ステップ S92003 では、所有装置送信部 102 は、車両借用者の携帯電話 11101 に対して車両所有者の公開鍵 31002 を送信する。

【0078】

40

借用装置公開鍵受信ステップ S102003 では、借用装置受信部 202 は、車両所有者の公開鍵 31002 を受信する。借用装置記憶部 203 は、受信した公開鍵を一時的に記憶する。例えば、図 1 に示す UIM の記憶部 11111 は、受信した公開鍵を一時的に格納する。

【0079】

借用装置公開鍵受信完了通知ステップ S102004 では、借用装置送信部 201 は、車両所有者の携帯電話 11001 に対して公開鍵受信完了通知を送信する。

【0080】

所有装置公開鍵受信完了受信ステップ S92004 では、所有装置受信部 103 は、公開鍵受信完了通知を受信する。

50

【0081】

所有装置乱数生成ステップS92005では、所有装置識別情報作成部106は、乱数を生成する。

【0082】

所有装置乱数送信ステップS92006では、所有装置送信部102は、車両借用者の携帯電話11101に対して乱数を送信する。

【0083】

借用装置乱数受信ステップS102005では、借用装置受信部202は、乱数を受信する。

【0084】

借用装置識別情報作成ステップS102006では、借用装置識別情報作成部206は、車両所有者の携帯電話11001の識別情報を作成する。ここでは、車両所有者の公開鍵31002のハッシュ値を生成し、車両所有者の携帯電話11001の識別情報とする。

10

【0085】

借用装置署名作成ステップS102007では、借用装置識別情報作成部206は、車両借用者の秘密鍵51001を用いて、車両所有者の携帯電話11001の識別情報と受信した乱数とに署名を付け、署名情報を作成する。

【0086】

借用装置識別情報送信ステップS102008では、借用装置送信部201は、署名情報を車両所有者の携帯電話11001に対して送信する。

20

【0087】

所有装置識別情報受信ステップS92007では、所有装置受信部103は、署名情報を受信する。

【0088】

所有装置識別情報検証ステップS92008では、所有装置判定部105は、受信した署名情報の検証を行う。所有装置判定部105は、例えば、まず、車両所有者の公開鍵31002から車両所有者の携帯電話11001の識別情報を作成する。次に、所有装置判定部105は、車両所有者の携帯電話11001の識別情報と乱数とから署名対象情報を作成する。次に、所有装置判定部105は、車両借用者の公開鍵51002を用いて受信した署名情報から署名対象情報を作成し、前記署名対象情報と比較する。

30

【0089】

所有装置識別情報検証ステップS92009では、所有装置判定部105は、検証が成功した場合、次のステップに進む。所有装置判定部105は、検証が失敗した場合、プログラムを終了する。

【0090】

チケット生成ステップS92010では、チケット生成部101は、チケットを作成する。

【0091】

チケット署名ステップS92011では、チケット生成部101は、車両所有者の秘密鍵31001を用いて、チケットと車両11201の識別情報の署名情報を作成する。

40

【0092】

ステップS92012からステップS92013、ステップS102009からステップS102013は、実施の形態1のステップS91007からステップS91008、ステップS101005からステップS101009と同様なので、ここでは説明を省略する。

【0093】

車両所有者の携帯電話11001と車両借用者の携帯電話11101とは、実施の形態1と同様に安全な通信経路で通信する。

【0094】

50

図 2 2 は、車両所有者の携帯電話 1 1 0 0 1 が車両借用者の携帯電話 1 1 1 0 1 に対して車両操作権限を委譲した後、車両借用者の携帯電話 1 1 1 0 1 の U I M 1 1 1 0 8 の記憶部 1 1 1 1 1 に格納される情報である。

【0 0 9 5】

次に、車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する動作について図 2 3、図 2 4、図 2 5 を用いて説明する。図 2 3 は、車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。図 2 4 は、車両所有者または車両借用者（以下、車両利用者）の携帯電話 1 1 0 0 1 または 1 1 1 0 1 の端末側車両操作プログラム 2 1 0 0 3 または 4 1 0 0 3 の一連の動作を示すフローチャートである。図 2 5 は、車両 1 1 2 0 1 の車両側車両操作プログラム 6 1 0 0 4 の一連の動作を示すフローチャートである。

10

【0 0 9 6】

ステップ S 1 3 2 0 0 1 からステップ S 1 3 2 0 0 3、ステップ S 1 4 2 0 0 1 からステップ S 1 4 2 0 0 6 は、実施の形態 1 のステップ S 1 3 1 0 0 1 からステップ S 1 3 1 0 0 3、ステップ S 1 4 1 0 0 1 からステップ S 1 4 1 1 0 6 と同様なので、ここでは説明を省略する。

【0 0 9 7】

制御装置乱数生成ステップ S 1 4 2 0 0 7 では、制御装置識別情報作成部 3 0 6 は、乱数を生成する。

【0 0 9 8】

20

制御装置乱数送信ステップ S 1 4 2 0 0 8 では、制御装置送信部 3 0 1 は、車両所有者の携帯電話 1 1 0 0 1 に対して乱数を送信する。

【0 0 9 9】

利用装置乱数受信ステップ S 1 3 2 0 0 4 では、所有装置受信部 1 0 3 は、乱数を受信する。

【0 1 0 0】

利用装置署名作成ステップ S 1 3 2 0 0 5 では、所有装置識別情報作成部 1 0 6 は、車両所有者の秘密鍵 3 1 0 0 1 を用いて車両 1 1 2 0 1 の識別情報と乱数とに署名を付け、署名情報を作成する。

【0 1 0 1】

30

利用装置識別情報送信ステップ S 1 3 2 0 0 6 では、所有装置送信部 1 0 2 は、署名情報を車両 1 1 2 0 1 に対して送信する。車両所有者の携帯電話 1 1 0 0 1 は、署名情報送信後、プログラムを終了する。

【0 1 0 2】

制御装置識別情報受信ステップ S 1 4 2 0 0 9 では、制御装置受信部 3 0 2 は、署名情報を受信する。

【0 1 0 3】

制御装置識別情報検証ステップ S 1 4 2 0 1 0 では、制御装置判定部 3 0 4 は、署名情報の検証を行う。制御装置判定部 3 0 4 は、例えば、まず、車両の公開鍵 6 1 0 0 2 から車両 1 1 2 0 1 の識別情報を作成する。次に、制御装置判定部 3 0 4 は、車両 1 1 2 0 1 の識別情報と乱数とから署名対象情報を作成する。次に、制御装置判定部 3 0 4 は、車両所有者の公開鍵 3 1 0 0 2 を用いて受信した署名情報から署名対象情報を作成し、前記署名対象情報と比較する。

40

【0 1 0 4】

制御装置識別情報検証ステップ S 1 4 2 0 1 1 では、制御装置判定部 3 0 4 は、検証が成功した場合、次のステップに進む。制御装置判定部 3 0 4 は、検証が失敗した場合、プログラムを終了する。

【0 1 0 5】

ステップ S 1 4 2 0 1 2 は、実施の形態 1 のステップ S 1 4 1 0 0 7 と同様なので、ここでは説明を省略する。

50

【0106】

車両所有者の携帯電話11001と車両11201とは、赤外線通信などにより通信が行われる。

【0107】

次に、車両借用者の携帯電話11101が車両11201を操作する動作について図26、図24、図25を用いて説明する。図26は、車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【0108】

ステップS132001からステップS132003、ステップS142001からステップS142006は、実施の形態1のステップS131001からステップS131003、ステップS141001からステップS141106と同様なので、ここでは説明を省略する。また、ステップS142007からステップS142012は、車両所有者の携帯電話11001が車両11201を操作する場合と同様なので、ここでは説明を省略する。ただし、利用装置署名作成ステップS132005で署名をするのに用いる秘密鍵は、車両所有者の秘密鍵31001ではなく、車両借用者の秘密鍵51001である。

10

車両借用者の携帯電話11101と車両11201とは、赤外線通信などにより通信が行われる。

【0109】

上記で発生させた乱数には、現在時刻やメッセージカウンタなどのデータ送信毎に変化するデータを用いてもよい。以下乱数を発生させる場合に同様である。

20

【0110】

実施の形態2では、車両11201の操作権限委譲時および車両11201の操作時において各々認証を行ったが、車両11201の操作権限委譲時または車両11201の操作時いずれかのみ認証を行ってもよい。

また、実施の形態2では、上述の認証手順以外でも同等の効果を得られるその他の認証手順を用いてもよい。

【0111】

以上のように、実施の形態2では、実施の形態1における車両操作権限委譲システムの車両操作権限委譲時に車両借用者の携帯電話11101の署名を車両所有者の携帯電話11001が検証する手順を加えている。そのため、実施の形態2では、実施の形態1の効果に加えて、車両操作権限委譲時に第三者が車両借用者の携帯電話11101になりすまして不正な車両操作権限委譲を行うことを防ぐことができる。

30

【0112】

また、実施の形態2では、車両利用者が車両11201を操作する時に車両利用者の署名を車両11201が検証する手順を加えることにより、チケットを入手した第三者が車両借用者になりすますなどにより不正に車両11201を操作することを防ぐことができる。

【0113】

実施の形態3.

40

次に実施の形態3について説明する。上述した実施の形態2では、車両所有者の携帯電話11001から車両借用者の携帯電話11101へ車両操作権限を委譲する時に車両借用者の署名を車両所有者の携帯電話11001が検証した。そのため、車両操作権限委譲時の車両借用者になりすます行為を防いだ。また、車両利用者が車両11201を操作する時に車両利用者の署名を車両11201が検証することによって、車両操作時の車両利用者のなりすましを防ぐようにしたものである。実施の形態3では、車両操作権限を委譲する場合には車両借用者と車両所有者との相互のなりすましを防ぎ、車両11201を操作する場合には車両利用者と車両との相互のなりすましを防ぐ動作を説明する。

【0114】

実施の形態3では、実施の形態2における車両操作権限委譲システムの車両操作権限委

50

譲時に車両借用者の署名を車両所有者の携帯電話11001が検証する手順の代わりに、車両借用者の携帯電話11101と車両所有者の携帯電話11001がお互い相手の署名を検証する手順を実行する。そのため、実施の形態3では、実施の形態2の効果に加えて、車両操作権限委譲時に第三者が車両所有者になりすまして不正な車両操作権限委譲を与えることを防ぐことができる。

【0115】

また、実施の形態3では、車両利用者が車両11201を操作する時に車両利用者の署名を車両11201が検証する手順の代わりに、車両利用者の携帯電話と車両11201がお互い相手の署名を検証する手順を実行する。そのため、実施の形態3では、実施の形態2の効果に加えて、車両利用者が不正な車両を操作することを防ぐことができる。

10

【0116】

実施の形態3における機能ブロック図および車両操作権限委譲システムの記憶部の構成は、実施の形態2と同様であるので、ここでは説明を省略する。

【0117】

次に、上記のように構成された実施の形態3の動作について説明する。実施の形態3の動作は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話11101が車両11201を操作する動作とを備える。

【0118】

まず、車両操作権限を委譲する動作について図27、図28、図29を用いて説明する。図27は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。図28は、車両所有者の携帯電話11001の車両操作権限貸与プログラム21001の一連の動作を示すフローチャートである。図29は、車両借用者の携帯電話11101の車両操作権限借用プログラム41002の一連の動作を示すフローチャートである。

20

【0119】

ステップS93001からステップS93006、ステップS103001からステップS103005は、実施の形態2のステップS92001からステップS92006、ステップS102001からステップS102005と同様なので、ここでは説明を省略する。

30

【0120】

借用装置乱数生成ステップS103006では、借用装置識別情報作成部206は、乱数を生成する。

【0121】

借用装置識別情報作成ステップS103007では、借用装置識別情報作成部206は、車両所有者の携帯電話11001の識別情報を作成する。

【0122】

借用装置署名作成ステップS103008では、借用装置識別情報作成部206は、車両借用者の秘密鍵51001を用いて、生成した乱数（以下、乱数b）、受信した乱数（以下、乱数a）、車両所有者の携帯電話11001の識別情報に署名を付け、署名情報を作成する。

40

【0123】

借用装置識別情報送信ステップS103009では、借用装置送信部201は、乱数bと乱数aと車両所有者の携帯電話11001の識別情報と署名情報とを車両所有者の携帯電話11001に対して送信する。

【0124】

所有装置識別情報受信ステップS93007では、所有装置受信部103は、乱数bと乱数aと車両所有者の携帯電話11001の識別情報と署名情報とを受信する。

【0125】

所有装置識別情報検証ステップS93008では、所有装置判定部105は、受信した

50

署名情報の検証を行う。所有装置判定部105は、例えば、まず、乱数b、乱数a、車両所有者の携帯電話11001の識別情報とから署名対象情報を作成する。次に、所有装置判定部105は、車両借用者の公開鍵51002を用いて署名情報から署名対象情報を作成し、前記署名対象情報と比較する。

【0126】

所有装置識別情報検証ステップS93009では、所有装置判定部105は、検証が成功した場合、次のステップに進む。所有装置判定部105は、検証が失敗した場合、プログラムを終了する。

【0127】

所有装置乱数検証ステップS93010では、所有装置判定部105は、乱数aと車両所有者の携帯電話11001の識別情報とを検証する。所有装置判定部105は、例えば、まず、ステップS93005において生成した乱数と乱数aとを照合する。次に、所有装置判定部105は、車両所有者の携帯電話11001の識別情報を作成し、受信した車両所有者の携帯電話11001の識別情報と照合する。

10

【0128】

所有装置乱数検証ステップS93011では、所有装置判定部105は、所有装置判定部105が比較した結果、いずれも一致したら検証は成功とみなし、次のステップに進む。所有装置判定部105は、所有装置判定部105が比較した結果、いずれかが一致しなければ検証は失敗とみなし、プログラムを終了する。

【0129】

20

所有装置識別情報作成ステップS93012では、所有装置識別情報作成部106は、車両借用者の携帯電話11101の識別情報を作成する。

【0130】

所有装置署名作成ステップS93013では、車両所有者の秘密鍵31001を用いて乱数aと乱数bと車両借用者の携帯電話11101の識別情報とに署名を付け、署名情報を作成する。

【0131】

所有装置識別情報送信ステップS93014では、所有装置送信部102は、乱数aと乱数bと車両借用者の携帯電話11101の識別情報と署名情報とを車両借用者の携帯電話11101に対して送信する。

30

【0132】

借用装置識別情報受信ステップS103010では、借用装置受信部202は、乱数aと乱数bと車両借用者の携帯電話11101の識別情報と署名情報とを受信する。

【0133】

借用装置識別情報検証ステップS103011では、借用装置判定部205は、受信した署名情報の検証を行う。借用装置判定部205は、例えば、まず、乱数a、乱数b、車両借用者の識別情報から署名対象情報を作成する。次に、借用装置判定部205は、車両所有者の公開鍵31002を用いて署名情報から署名対象情報を作成し、前記署名対象情報と比較する。

【0134】

40

借用装置識別情報検証ステップS103012では、借用装置判定部205は、検証が成功した場合、次のステップに進む。借用装置判定部205は、検証が失敗した場合、プログラムを終了する。

【0135】

借用装置乱数検証ステップS103013では、借用装置判定部205は、乱数aと乱数bと車両借用者の携帯電話11101の識別情報とを検証する。借用装置判定部205は、例えば、まず、ステップS103005において受信した乱数と乱数aとを照合する。次に、借用装置判定部205は、ステップS103006において生成した乱数と乱数bとを照合する。次に、借用装置判定部205は、車両借用者の携帯電話11101の識別情報を作成し、受信した車両借用者の携帯電話11101の識別情報と照合する。

50

【0136】

借用装置乱数検証ステップS103014では、借用装置判定部205は、借用装置判定部205が比較した結果、いずれも一致したら検証は成功とみなし、次のステップに進む。借用装置判定部205は、借用装置判定部205が比較した結果、いずれかが一致しなければ検証は失敗とみなし、プログラムを終了する。

【0137】

チケット要求送信ステップS103015では、借用装置送信部201は、車両所有者の携帯電話11001に対して、チケット要求を送信する。

【0138】

チケット要求受信ステップS93015では、所有装置受信部103は、チケット要求を受信する。

10

【0139】

ステップS93016からステップS93019、ステップS103016からステップS103020は、実施の形態2のステップS92010からステップS92013、ステップS102009からステップS102013と同様なので、ここでは説明を省略する。

【0140】

車両所有者の携帯電話11001と車両借用者の携帯電話11101とは、実施の形態2と同様に安全な通信経路で通信する。

【0141】

20

図22は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲した後、車両借用者の携帯電話11101の記憶部に格納される情報である。

【0142】

次に、車両所有者の携帯電話11001が車両11201を操作する動作について図30、図31、図32を用いて説明する。図30は、車両所有者の携帯電話11001が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。図31は、車両所有者または車両借用者（以下、車両利用者）の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。図32は、車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

30

【0143】

ステップS133001からステップS133004、ステップS143001からステップS143008は、実施の形態2のステップS132001からステップS132004、ステップS142001からS142008と同様なので、ここでは説明を省略する。

【0144】

利用装置乱数生成ステップS133005において、所有装置識別情報作成部106は、乱数を生成する。

【0145】

40

利用装置署名作成ステップS133006では、所有装置識別情報作成部106は、車両所有者の秘密鍵31001を用いて、生成した乱数（以下、乱数b）と受信した乱数（以下、乱数a）と車両11201の識別情報とに署名を付け、の署名情報を作成する。

【0146】

利用装置識別情報送信ステップS133007では、乱数bと乱数aと車両11201の識別情報と署名情報とを車両11201に対して送信する。

【0147】

制御装置識別情報受信ステップS143009では、制御装置受信部302は、乱数bと乱数aと車両11201の識別情報と署名情報とを受信する。

【0148】

50

制御装置識別情報検証ステップS 1 4 3 0 1 0では、制御装置判定部3 0 4は、署名情報の検証を行う。制御装置判定部3 0 4は、例えば、まず、乱数b、乱数a、車両1 1 2 0 1の識別情報から署名対象情報を作成する。次に、制御装置判定部3 0 4は、車両借用者の公開鍵5 1 0 0 2を用いて署名情報から署名対象情報を作成し、前記署名対象情報と比較する。

【0 1 4 9】

制御装置識別情報検証ステップS 1 4 3 0 1 1では、制御装置判定部3 0 4は、検証が成功した場合、次のステップに進む。制御装置判定部3 0 4は、検証が失敗した場合、プログラムを終了する。

【0 1 5 0】

10

制御装置乱数検証ステップS 1 4 3 0 1 2では、制御装置判定部3 0 4は、乱数aと車両1 1 2 0 1の識別情報を検証する。制御装置判定部3 0 4は、例えば、まず、ステップS 1 4 3 0 0 7において生成した乱数と乱数aとを照合する。次に、制御装置判定部3 0 4は、車両1 1 2 0 1の識別情報を作成し、受信した車両所有者の携帯電話1 1 0 0 1の識別情報と照合する。

【0 1 5 1】

制御装置乱数検証ステップS 1 4 3 0 1 3では、制御装置判定部3 0 4は、制御装置判定部3 0 4が比較した結果、いずれも一致したら検証は成功とみなし、次のステップに進む。制御装置判定部3 0 4は、制御装置判定部3 0 4が比較した結果、いずれかが一致しなければ検証は失敗とみなし、プログラムを終了する。

20

【0 1 5 2】

制御装置識別情報作成ステップS 1 4 3 0 1 4では、制御装置識別情報作成部3 0 6は、車両所有者の携帯電話1 1 0 0 1の識別情報を作成する。

【0 1 5 3】

制御装置署名作成ステップS 1 4 3 0 1 5では、制御装置識別情報作成部3 0 6は、車両の秘密鍵6 1 0 0 1を用いて乱数aと乱数bと車両所有者の携帯電話1 1 0 0 1の識別情報とに署名を付け、署名情報を作成する。

【0 1 5 4】

制御装置識別情報送信ステップS 1 4 3 0 1 6では、制御装置送信部3 0 1は、乱数aと乱数bと車両所有者の携帯電話1 1 0 0 1の識別情報と署名情報とを車両所有者の携帯電話1 1 0 0 1に対して送信する。

30

【0 1 5 5】

利用装置識別情報受信ステップS 1 3 3 0 0 8では、所有装置受信部1 0 3は、乱数aと乱数bと車両所有者の携帯電話1 1 0 0 1の識別情報と署名情報とを受信する。

【0 1 5 6】

利用装置識別情報検証ステップS 1 3 3 0 0 9では、所有装置判定部1 0 5は、受信した署名情報の検証を行う。所有装置判定部1 0 5は、例えば、まず、乱数a、乱数b、車両所有者の携帯電話1 1 0 0 1の識別情報から署名対象情報を作成する。次に、所有装置判定部1 0 5は、車両所有者の公開鍵3 1 0 0 2を用いて署名情報から署名対象情報を作成し、前記署名対象情報と比較する。

40

【0 1 5 7】

利用装置識別情報検証ステップS 1 3 3 0 1 0では、所有装置判定部1 0 5は、検証が成功した場合、次のステップに進む。所有装置判定部1 0 5は、検証が失敗した場合、プログラムを終了する。

【0 1 5 8】

利用装置乱数検証ステップS 1 3 3 0 1 1では、所有装置判定部1 0 5は、乱数aと乱数bと車両所有者の携帯電話1 1 0 0 1の識別情報とを検証する。所有装置判定部1 0 5は、例えば、まず、ステップS 1 3 3 0 0 4において受信した乱数と乱数aとを照合する。次に、所有装置判定部1 0 5は、ステップS 1 3 3 0 0 5において生成した乱数と乱数bとを照合する。次に、所有装置判定部1 0 5は、車両所有者の携帯電話1 1 0 0 1の識

50

別情報を作成し、受信した車両所有者の携帯電話 1 1 0 0 1 の識別情報と照合する。

【0159】

利用装置乱数検証ステップ S 1 3 3 0 1 2 では、所有装置判定部 1 0 5 は、所有装置判定部 1 0 5 が比較した結果、いずれも一致したら検証は成功とみなし、次のステップに進む。所有装置判定部 1 0 5 は、所有装置判定部 1 0 5 が比較した結果、いずれかが一致しなければ検証は失敗とみなし、プログラムを終了する。

【0160】

操作開始要求送信ステップ S 1 3 3 0 1 3 では、所有装置送信部 1 0 2 は、車両 1 1 2 0 1 に対して操作開始要求を送信する。車両所有者の携帯電話 1 1 0 0 1 は、操作開始要求を送信後、プログラムを終了する。

10

【0161】

操作開始要求受信ステップ S 1 4 3 0 1 7 では、制御装置受信部 3 0 2 は、操作開始要求を受信する。

【0162】

操作可能状態移行ステップ S 1 4 3 0 1 8 では、車両側車両操作プログラム 6 1 0 0 4 は、操作可能状態に移行する。車両 1 1 2 0 1 は、操作可能状態に移行後、プログラムを終了する。

【0163】

車両所有者の携帯電話 1 1 0 0 1 と車両 1 1 2 0 1 とは、赤外線通信などにより通信が行われる。

20

【0164】

次に、車両借用者の携帯電話 1 1 1 0 1 が車両 1 1 2 0 1 を操作する動作について図 3 3、図 3 1、図 3 2 を用いて説明する。図 3 3 は、車両借用者の携帯電話 1 1 1 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

【0165】

ステップ S 1 3 3 0 0 1 からステップ S 1 3 3 0 0 4、ステップ S 1 4 3 0 0 1 からステップ S 1 4 3 0 0 8 は、実施の形態 2 のステップ S 1 3 2 0 0 1 からステップ S 1 3 2 0 0 4、ステップ S 1 4 2 0 0 1 から S 1 4 2 0 0 8 と同様なので、ここでは説明を省略する。また、ステップ S 1 3 3 0 0 5 からステップ S 1 3 3 0 1 3、ステップ S 1 4 3 0 0 9 からステップ S 1 4 3 0 1 8 は、車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する場合と同様なので、ここでは説明を省略する。

30

【0166】

車両借用者の携帯電話 1 1 1 0 1 と車両 1 1 2 0 1 とは、赤外線通信などにより通信が行われる。

【0167】

実施の形態 3 では、車両の操作権限委譲時および車両 1 1 2 0 1 の操作時において各々認証を行ったが、車両 1 1 2 0 1 の操作権限委譲時または車両 1 1 2 0 1 の操作時いずれかのみ認証を行ってもよい。

【0168】

また、実施の形態 3 では、ISO/IEC 98970-3 three-pass mutual authentication に示される認証手順を使用しているが、同等の効果を得られるその他の認証手順を用いてもよい。

40

【0169】

以上のように、実施の形態 3 では、実施の形態 2 における車両操作権限委譲システムの車両操作権限委譲時に車両借用者の携帯電話 1 1 1 0 1 の署名を車両所有者の携帯電話 1 1 0 0 1 が検証する手順の代わりに、車両借用者の携帯電話 1 1 1 0 1 と車両所有者の携帯電話 1 1 0 0 1 がお互い相手の署名を検証する手順を実行した。そのため、実施の形態 3 では、実施の形態 2 の効果に加えて、車両操作権限委譲時に第三者が車両所有者の携帯電話 1 1 0 0 1 になりすまして不正な車両操作権限委譲を与えることを防ぐことができる。

50

【0170】

また、実施の形態3では、車両利用者が車両11201を操作する時に車両利用者の署名を車両11201が検証する手順の代わりに、車両利用者の携帯電話と車両11201がお互い相手の署名を検証する手順を実行した。そのため、実施の形態3では、実施の形態2の効果に加えて、車両利用者が不正な車両を操作することを防ぐことができる。

【0171】

実施の形態4.

次に実施の形態4について説明する。上述した実施の形態では、車両所有者の携帯電話11001と車両借用者の携帯電話11101との通信や、車両利用者の携帯電話と車両11201との通信において送信される情報は特別な処理は施されていないと考えることも可能である。実施の形態4では、送信される情報を暗号化し第三者からの盗聴や割り込み利用を防ぐ動作を説明する。

10

【0172】

実施の形態4では、上述した実施の形態における車両操作権限委譲システムの車両操作権限委譲時において、車両所有者の携帯電話11001と車両借用者の携帯電話11101との間でメッセージを暗号化するための共通鍵を共有する。そのため、実施の形態4では、これまでの実施の形態の効果に加えて車両操作権限委譲時に第三者からの盗聴や割り込み利用を防ぐことができる。

【0173】

また、実施の形態4では、車両操作時においては車両11201と車両利用者の間でメッセージを暗号化するための共通鍵を共有する。そのため、実施の形態4では、上述した実施の形態の効果に加えて車両操作時に第三者からの盗聴や割り込み利用を防ぐことができる。

20

【0174】

さらに、実施の形態4では、車両所有者の公開鍵31002、車両借用者の公開鍵51002、車両の公開鍵61002の代わりに車両所有者の証明書34002、車両借用者の証明書54002、車両の証明書64002を用いることにより、パーソナルコンピュータなど計算機向けの既存の認証システムを利用することができる。よって、実施の形態4では、車両所有者の携帯電話11001と車両借用者の携帯電話11101とが遠隔地に離れていても安全に権限を委譲できる。

30

【0175】

図34は、実施の形態4にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。図34に示す機能ブロック図は、図17に示す機能ブロック図と概ね同様であるため、差分についてのみ説明する。

【0176】

権限所有装置100は、さらに、所有装置暗号化部107、所有装置鍵生成部108、所有装置復号部109を備える。所有装置暗号化部107は、チケット生成部101が生成したチケットなどを暗号化し暗号チケットとする。所有装置鍵生成部108は、権限借用装置200の任意の情報である借用装置任意情報と、権限所有装置の任意の情報である所有装置任意情報となどから鍵を生成する。所有装置復号部109は、暗号チケットなどを復号する。

40

【0177】

権限借用装置200は、さらに、借用装置暗号化部207、借用装置鍵生成部208、借用装置復号部209を備える。借用装置暗号化部207は、権限所有装置100から受信したチケットなどを暗号化し暗号チケットとする。借用装置鍵生成部208は、権限借用装置200の任意の情報である借用装置任意情報と、権限所有装置の任意の情報である所有装置任意情報となどから鍵を生成する。借用装置復号部209は、暗号チケットなどを復号する。

【0178】

制御装置300は、さらに、制御装置鍵生成部307、制御装置暗号化部308、制御

50

装置復号部 309 を備える。制御装置鍵生成部 307 は、制御装置 300 の任意の情報である制御装置任意情報と、権限借用装置 200 の任意の情報である借用装置任意情報となどから鍵を生成する。制御装置暗号化部 308 は、制御装置 300 の証明書などを暗号化する。制御装置復号部 309 は、暗号チケットなどを復号する。

【0179】

実施の形態 4 における車両操作権限委譲システムの記憶部の構成は、車両所有者の携帯電話 11001 の UIM11008 の記憶部 11011、車両借用者の携帯電話 11101 の UIM11108 の記憶部 11111、車両 11201 の記憶部 11204 を除いて、実施の形態 1 と同様であるので、ここでは差分についてのみ説明する。

【0180】

図 35 は、車両所有者の携帯電話 11001 の UIM11008 の記憶部 11011 に格納されたデータである。車両所有者の秘密鍵 31001 は公開鍵暗号方式における秘密鍵であり、車両所有者の携帯電話 11001 に対応する。車両所有者の証明書 34002 は公開鍵証明書であり、車両所有者の秘密鍵 31001 と対なす公開鍵を含む。

【0181】

図 36 は、車両借用者の携帯電話 11101 の UIM11108 の記憶部 11111 に格納されたデータである。各プログラムおよび各データの機能は、車両所有者の携帯電話 11001 の場合と同様であるので、ここでは省略する。

【0182】

図 37 は、車両 11201 の記憶部 11204 に格納されたプログラムおよびデータである。車両側車両操作プログラム 61004 は、車両 11201 が動作するための処理を行うプログラムである。車両の秘密鍵 61001 は公開鍵暗号方式における秘密鍵であり、車両 11201 に対応する。車両の証明書 64002 は公開鍵証明書であり、車両の秘密鍵 61001 と対をなす公開鍵を含む。車両所有者の証明書 34002 は公開鍵証明書であり、車両所有者の証明書 34002 と同一のものである。

【0183】

次に、上記のように構成された実施の形態 4 の動作について説明する。実施の形態 4 の動作は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話 11101 が車両 11201 を操作する動作とを備える。

【0184】

まず、車両操作権限を委譲する動作について図 38、図 39、図 40、図 41 を用いて説明する。図 38 は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。図 39 は、車両所有者の携帯電話 11001 の車両操作権限貸与プログラム 21001 の一連の動作を示すフローチャートである。図 40 と図 41 とは、車両借用者の携帯電話 11101 の車両操作権限借用プログラム 41002 の一連の動作を示すフローチャートである。

【0185】

まず、車両所有者の携帯電話 11001 は、車両操作権限貸与プログラム 21001 を起動する。また、車両借用者の携帯電話 11101 は、車両操作権限借用プログラム 41002 を起動する。

【0186】

所有装置証明書要求ステップ S94001 では、所有装置送信部 102 は、車両借用者の携帯電話 11101 に対して車両借用者の証明書要求を送信する。

【0187】

借用装置証明書要求受信ステップ S104101 では、借用装置受信部 202 は、車両借用者の証明書要求を受信する。

【0188】

借用装置証明書送信ステップ S104102 では、借用装置送信部 201 は、車両所有

10

20

30

40

50

者の携帯電話 1 1 0 0 1 に対して車両借用者の証明書 5 4 0 0 2 を送信する。

【0 1 8 9】

所有装置証明書受信ステップ S 9 4 0 0 2 では、所有装置受信部 1 0 3 は、車両借用者の証明書 5 4 0 0 2 を受信する。

【0 1 9 0】

所有装置証明書検証ステップ S 9 4 0 0 3 では、所有装置判定部 1 0 5 は、証明書の検証を行う。所有装置判定部 1 0 5 は、例えば、証明書の検証はパソコンなどの計算機向けの既存のプログラムやサーバを用いて行う。所有装置判定部 1 0 5 は、証明書検証サーバに接続し、証明書検証を依頼し、検証結果を得るなどする。

【0 1 9 1】

所有装置証明書検証ステップ S 9 4 0 0 4 では、所有装置判定部 1 0 5 は、検証が成功した場合、証明書を一時的に U I M 1 1 0 0 8 の記憶部 1 1 0 1 1 に格納し、次のステップに進む。所有装置判定部 1 0 5 は、検証が失敗した場合、プログラムを終了する。

【0 1 9 2】

所有装置証明書送信ステップ S 9 4 0 0 5 では、所有装置送信部 1 0 2 は、車両借用者の携帯電話 1 1 1 0 1 に対して車両所有者の証明書 3 4 0 0 2 を送信する。

【0 1 9 3】

借用装置証明書受信ステップ S 1 0 4 1 0 3 では、借用装置受信部 2 0 2 は、車両所有者の証明書 3 4 0 0 2 を受信する。

【0 1 9 4】

借用装置証明書検証ステップ S 1 0 4 1 0 4 では、借用装置判定部 2 0 5 は、証明書検証を行う。検証方法については、上記の所有装置証明書検証ステップ S 9 4 0 0 3 と同様の方法が考えられる。

【0 1 9 5】

借用装置証明書検証ステップ S 1 0 4 1 0 5 では、借用装置判定部 2 0 5 は、検証が成功した場合、証明書を一時的に U I M 1 1 1 0 8 の記憶部 1 1 1 1 1 に格納し、次のステップに進む。借用装置判定部 2 0 5 は、検証が失敗した場合、プログラムを終了する。

【0 1 9 6】

借用装置証明書受信完了通知ステップ S 1 0 4 1 0 6 では、借用装置送信部 2 0 1 は、車両所有者の携帯電話 1 1 0 0 1 に対して証明書受信完了通知を送信する。

【0 1 9 7】

所有装置証明書受信完了受信ステップ S 9 4 0 0 6 では、所有装置受信部 1 0 3 は、証明書受信完了通知を受信する。

【0 1 9 8】

所有装置鍵用乱数生成ステップ S 9 4 0 0 7 では、所有装置鍵生成部 1 0 8 は、共通鍵生成用乱数を生成する。

【0 1 9 9】

所有装置乱数生成ステップ S 9 4 0 0 8 では、所有装置識別情報作成部 1 0 6 は、乱数を生成する。

【0 2 0 0】

所有装置乱数暗号化ステップ S 9 4 0 0 9 では、所有装置暗号化部 1 0 7 は、車両所有者の携帯電話 1 1 0 0 1 の識別情報と共通鍵生成用乱数と乱数とを車両借用者の公開鍵 5 1 0 0 2 で暗号化する。

【0 2 0 1】

所有装置乱数送信ステップ S 9 4 0 1 0 では、所有装置送信部 1 0 2 は、車両借用者の携帯電話 1 1 1 0 1 に対して、所有装置乱数暗号化ステップ S 9 4 0 0 9 で暗号化したデータを送信する。ここでは、車両所有者の携帯電話 1 1 0 0 1 の識別情報は、車両所有者の証明書 3 4 0 0 2 に含まれる発行者名とシリアルナンバーなどとする。また、車両借用者の公開鍵 5 1 0 0 2 は、車両借用者の証明書 5 4 0 0 2 から取得する。

【0 2 0 2】

10

20

30

40

50

借用装置乱数受信ステップS104107では、借用装置受信部202は、暗号化された車両所有者の携帯電話11001の識別情報と共通鍵生成用乱数と乱数とを受信する。

【0203】

借用装置識別情報復号ステップS104108では、借用装置復号部209は、暗号化された車両所有者の携帯電話11001の識別情報と共通鍵生成用乱数と乱数とを、車両借用者の秘密鍵51001を用いて復号する。

【0204】

借用装置識別情報検証ステップS104109では、借用装置判定部205は、車両所有者の証明書34002を用いて、車両所有者の携帯電話11001の識別情報を検証する。

10

【0205】

借用装置識別情報検証ステップS104110では、借用装置判定部205は、検証に成功した場合、次のステップに進む。借用装置判定部205は、検証に失敗した場合、プログラムを終了する。

【0206】

借用装置鍵用乱数生成ステップS104111では、借用装置鍵生成部208は、共通鍵生成用乱数を生成する。

【0207】

借用装置乱数生成ステップS104112では、借用装置識別情報作成部206は、乱数を生成する。

20

【0208】

借用装置乱数暗号化ステップS104113では、借用装置暗号化部207は、車両借用者の携帯電話11101の識別情報と借用装置鍵用乱数生成ステップS104111で生成した共通鍵生成用乱数と借用装置乱数生成ステップS104112で生成した乱数とを車両所有者の公開鍵31002で暗号化する。

【0209】

借用装置乱数送信ステップS104114では、借用装置送信部201は、借用装置乱数暗号化ステップS104113で暗号化した車両借用者の携帯電話11101の識別情報と共通鍵生成用乱数と乱数とを、車両所有者の携帯電話11001に対して送信する。ここでは、車両借用者の携帯電話11101の識別情報は、車両借用者の証明書54002に含まれる発行者名とシリアルナンバーとする。また、車両所有者の公開鍵31002は、車両所有者の証明書34002から取得する。

30

【0210】

所有装置乱数受信ステップS94011では、所有装置受信部103は、暗号化された車両借用者の携帯電話11101の識別情報と共通鍵生成用乱数と乱数とを受信する。

【0211】

所有装置識別情報復号ステップS94012では、所有装置復号部109は、暗号化された車両借用者の携帯電話11101の識別情報と共通鍵生成用乱数と乱数とを、車両所有者の秘密鍵31001を用いて復号する。

【0212】

40

所有装置識別情報検証ステップS94013では、所有装置判定部105は、車両借用者の証明書54002を用いて、車両借用者の携帯電話11101の識別情報を検証する。

【0213】

所有装置識別情報検証ステップS94014では、所有装置判定部105は、検証に成功した場合、次のステップに進む。所有装置判定部105は、検証に失敗した場合、プログラムを終了する。

【0214】

所有装置共通鍵生成ステップS94015では、所有装置鍵生成部108は、ステップS94007において生成した共通鍵生成用乱数とステップS94011において受信し

50

た共通鍵生成用乱数とから共通鍵を生成する。所有装置鍵生成部108は、例えば、共通鍵生成用乱数を連結して取得したハッシュ値の先頭から鍵長までの長さの値を共通鍵とする。

【0215】

所有装置乱数再送信ステップS94016では、所有装置送信部102は、車両借用者の携帯電話11101に対して、ステップS94011において受信した乱数を送信する。

【0216】

借用装置乱数再受信ステップS104115では、借用装置受信部202は、乱数を受信する。

10

【0217】

借用装置乱数検証ステップS104116では、借用装置判定部205は、受信した乱数を、ステップS104112において生成した乱数と照合して検証する。

【0218】

借用装置乱数検証ステップS104117では、借用装置判定部205は、検証が成功した場合、次のステップに進む。借用装置判定部205は、検証が失敗した場合、プログラムを終了する。

【0219】

借用装置共通鍵生成ステップS104118では、借用装置鍵生成部208は、ステップS104107において受信した共通鍵生成用乱数とステップS104111において生成した共通鍵生成用乱数から共通鍵を生成する。

20

【0220】

チケット要求暗号化ステップS104191では、借用装置暗号化部207は、チケット要求を共通鍵で暗号化する。

【0221】

チケット要求送信ステップS104192では、借用装置送信部201は、暗号化したチケット要求を車両所有者の携帯電話11001に対して送信する。

【0222】

チケット要求受信ステップS94017では、所有装置受信部103は、暗号化されたチケット要求を受信する。

30

【0223】

チケット要求復号ステップS94018では、所有装置復号部109は、暗号化されたチケット要求を共通鍵で復号する。

【0224】

チケット生成ステップS94019では、チケット生成部101は、車両借用者のチケットを作成する。チケット生成部101が生成したチケットは、車両借用者の証明書54002、車両借用者の操作許可情報111112と操作制限情報111113とを備える。

【0225】

チケット署名ステップS94020では、チケット生成部101は、車両所有者の秘密鍵31001を用いてチケットの署名情報を作成する。

40

【0226】

チケット暗号化ステップS94021では、所有装置暗号化部107は、チケット生成部101が作成した署名付きチケットを共通鍵で暗号化する。

【0227】

チケット送信ステップS94022では、所有装置送信部102は、暗号化した署名付きチケットを車両借用者の携帯電話11101に送信する。

【0228】

チケット受信ステップS104193では、借用装置受信部202は、暗号化された署名付きチケットを受信する。

50

【0229】

チケット復号ステップS104194では、借用装置復号部209は、暗号化された署名付きチケットを共通鍵で復号する。

【0230】

チケット検証ステップS104195では、借用装置判定部205は、車両所有者の公開鍵31002を用いて署名情報を検証する。

【0231】

チケット検証ステップS104196では、借用装置判定部205は、検証に成功した場合、次のステップに進む。借用装置判定部205は、検証に失敗した場合、プログラムを終了する。

10

【0232】

チケット記憶ステップS104197では、借用装置記憶部203は、署名付きチケットを記憶する。

【0233】

チケット受信完了通知暗号化ステップS104198では、借用装置暗号化部207は、チケット受信完了通知を共通鍵で暗号化する。

【0234】

チケット受信完了通知ステップS104199では、借用装置送信部201は、車両所有者の携帯電話11001に対して暗号化したチケット受信完了通知を送信する。車両借用者の携帯電話11101は、暗号化したチケット受信完了通知を送信後、プログラムを終了する。

20

【0235】

チケット受信完了通知受信ステップS94023では、所有装置受信部103は、暗号化されたチケット受信完了通知を受信する。

【0236】

チケット受信完了通知復号ステップS94024では、所有装置復号部109は、暗号化されたチケット受信完了通知を共通鍵で復号する。車両所有者の携帯電話11001は、暗号化されたチケット受信完了通知を共通鍵で復号後、プログラムを終了する。

【0237】

車両所有者の携帯電話11001と車両借用者の携帯電話11101とは、実施の形態1と同様に安全な通信経路で通信する。

30

【0238】

図42は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲した後、車両借用者の携帯電話11101のUIM11108の記憶部11111に格納される情報である。UIM11108の記憶部11111には、車両操作権限を委譲する前と比較して、車両借用者の証明書54002を含む車両所有者の署名付きチケット111001が加わっている。

【0239】

次に、車両所有者の携帯電話11001が車両11201を操作する動作について図43、図44、図45を用いて説明する。図43は、車両所有者の携帯電話11001が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。図44は、車両所有者または車両借用者（以下、車両利用者）の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。図45は、車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

40

【0240】

通信リンク確立ステップS134001およびS144001では、車両側車両操作プログラム61004は、制御装置送信部301を介し、定期的に携帯電話に対して応答要求を送信する。車両所有者の携帯電話11001が車両11201に近づき、車両所有者の携帯電話11001の端末側車両操作プログラム21003が応答要求を受信すること

50

によって、車両 1 1 2 0 1 と車両所有者の携帯電話 1 1 0 0 1 との通信リンクを確立する。

【0 2 4 1】

制御装置証明書要求ステップ S 1 4 4 0 0 2 では、制御装置送信部 3 0 1 は、車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 の操作を開始したら、車両所有者の携帯電話 1 1 0 0 1 に対して証明書要求を送信する。

【0 2 4 2】

利用装置証明書要求受信ステップ S 1 3 4 0 0 2 では、所有装置受信部 1 0 3 は、車両所有者の証明書 3 4 0 0 2 要求を受信する。

【0 2 4 3】

利用装置証明書送信ステップ S 1 3 4 0 0 3 では、所有装置送信部 1 0 2 は、車両 1 1 2 0 1 に対して車両所有者の証明書 3 4 0 0 2 を送信する。

【0 2 4 4】

制御装置証明書受信ステップ S 1 4 4 0 0 3 では、制御装置受信部 3 0 2 は、車両借用者の証明書 3 4 0 0 2 を受信する。

【0 2 4 5】

制御装置証明書解析ステップ S 1 4 4 0 0 4 では、制御装置判定部 3 0 4 は、受信したデータの種別を解析する。

【0 2 4 6】

制御装置証明書照合ステップ S 1 4 4 1 0 5 では、制御装置判定部 3 0 4 は、受信した証明書と記憶部 1 1 2 0 4 に格納している車両利用者の証明書とを照合する。

【0 2 4 7】

制御装置証明書照合ステップ S 1 4 4 1 0 6 では、制御装置判定部 3 0 4 は、照合に成功した場合、次のステップに進む。制御装置判定部 3 0 4 は、照合に失敗した場合、プログラムを終了する。

【0 2 4 8】

制御装置証明書検証ステップ S 1 4 4 0 0 7 では、制御装置判定部 3 0 4 は、照合に成功した場合、車両所有者の証明書 3 4 0 0 2 を検証する。

【0 2 4 9】

制御装置証明書検証ステップ S 1 4 4 0 0 8 では、制御装置判定部 3 0 4 は、制御装置判定部 3 0 4 が検証に成功した場合、次のステップに進む。制御装置判定部 3 0 4 は、制御装置判定部 3 0 4 が検証に失敗した場合、プログラムを終了する。

【0 2 5 0】

制御装置証明書送信ステップ S 1 4 4 0 0 9 では、制御装置送信部 3 0 1 は、車両所有者の携帯電話 1 1 0 0 1 に対して車両の証明書 6 4 0 0 2 を送信する。

【0 2 5 1】

利用装置証明書受信ステップ S 1 3 4 0 0 4 では、所有装置受信部 1 0 3 は、車両の証明書 6 4 0 0 2 を受信する。

【0 2 5 2】

利用装置証明書検証ステップ S 1 3 4 0 0 5 では、所有装置判定部 1 0 5 は、証明書を検証する。

【0 2 5 3】

利用装置証明書検証ステップ S 1 3 4 0 0 6 では、所有装置判定部 1 0 5 は、検証が成功した場合、次のステップに進む。所有装置判定部 1 0 5 は、検証が失敗した場合、プログラムを終了する。

【0 2 5 4】

利用装置証明書受信完了通知ステップ S 1 3 4 0 0 7 では、所有装置送信部 1 0 2 は、車両 1 1 2 0 1 に対して証明書受信完了通知を送信する。

【0 2 5 5】

制御装置証明書受信完了受信ステップ S 1 4 4 0 1 0 では、制御装置受信部 3 0 2 は、

10

20

30

40

50

証明書受信完了通知を受信する。

【0256】

制御装置鍵用乱数生成ステップS144011では、制御装置鍵生成部307は、共通鍵生成用乱数を生成する。

【0257】

制御装置乱数生成ステップS144012では、制御装置識別情報作成部306は乱数を生成する。

【0258】

制御装置乱数暗号化ステップS144013では、車両11201の識別情報と共通鍵生成用乱数と乱数とを車両所有者の公開鍵31002で暗号化する。

10

【0259】

制御装置乱数送信ステップS144014では、制御装置送信部301は、暗号化した車両11201の識別情報と共通鍵生成用乱数と乱数とを車両所有者の携帯電話11001に対して送信する。ここでは、車両11201の識別情報は車両の証明書64002に含まれる発行者名とシリアルナンバーとする。また、車両所有者の公開鍵31002は、車両所有者の証明書34002から取得する。

【0260】

利用装置乱数受信ステップS134008では、所有装置受信部103は、暗号化された車両11201の識別情報と共通鍵生成用乱数と乱数とを受信する。

【0261】

20

利用装置識別情報復号ステップS134009では、所有装置復号部109は、暗号化された車両11201の識別情報と共通鍵生成用乱数と乱数とを、車両所有者の秘密鍵31001を用いて復号する。

【0262】

利用装置識別情報検証ステップS134010では、所有装置判定部105は、車両の証明書64002を用いて、車両11201の識別情報を検証する。

【0263】

利用装置識別情報検証ステップS134011では、所有装置判定部105は、検証に成功した場合、次のステップに進む。所有装置判定部105は、検証に失敗した場合、プログラムを終了する。

30

【0264】

利用装置鍵用乱数生成ステップS134012では、所有装置鍵生成部108は、共通鍵生成用乱数を生成する。

【0265】

利用装置乱数生成ステップS134013では、所有装置識別情報作成部106は、乱数を生成する。

【0266】

利用装置乱数暗号化ステップS134014では、所有装置暗号化部107は、車両所有者の携帯電話11001の識別情報と共通鍵生成用乱数と乱数とを、車両の公開鍵61002で暗号化する。

40

【0267】

利用装置乱数送信ステップS134015では、所有装置送信部102は、暗号化した車両所有者の携帯電話11001の識別情報と共通鍵生成用乱数と乱数とを、車両11201に対して送信する。ここでは、車両所有者の携帯電話11001の識別情報は車両所有者の証明書34002に含まれる発行者名とシリアルナンバーとする。また、車両の公開鍵61002は、車両の証明書64002から取得する。

【0268】

制御装置乱数受信ステップS144015では、制御装置受信部302は、暗号化された車両11201の識別情報と共通鍵生成用乱数と乱数とを受信する。

【0269】

50

制御装置識別情報復号ステップS 1 4 4 0 1 6では、制御装置復号部3 0 9は、暗号化された車両1 1 2 0 1の識別情報と共通鍵生成用乱数と乱数とを、車両の秘密鍵6 1 0 0 1を用いて復号する。

【0 2 7 0】

制御装置識別情報検証ステップS 1 4 4 0 1 7では、制御装置判定部3 0 4は、車両借用者の証明書3 4 0 0 2を用いて、車両所有者の携帯電話1 1 0 0 1の識別情報を検証する。

【0 2 7 1】

制御装置識別情報検証ステップS 1 4 4 0 1 8では、制御装置判定部3 0 4は、検証に成功した場合、次のステップに進む。制御装置判定部3 0 4は、検証に失敗した場合、プログラムを終了する。

10

【0 2 7 2】

制御装置共通鍵生成ステップS 1 4 4 0 1 9では、制御装置鍵生成部3 0 7は、ステップS 1 4 4 0 1 1において生成した共通鍵生成用乱数とステップS 1 4 4 0 1 5において受信した共通鍵生成用乱数とから共通鍵を生成する。制御装置鍵生成部3 0 7は、例えば、共通鍵生成用乱数を連結して取得したハッシュ値の先頭から鍵長までの長さの値を共通鍵とする。

【0 2 7 3】

制御装置乱数再送信ステップS 1 4 4 0 2 0では、制御装置送信部3 0 1は、車両所有者の携帯電話1 1 0 0 1に対して、ステップS 1 4 4 0 1 5において受信した乱数を送信する。

20

【0 2 7 4】

利用装置乱数再受信ステップS 1 3 4 0 1 6では、所有装置受信部1 0 3は、乱数を受信する。

【0 2 7 5】

利用装置乱数検証ステップS 1 3 4 0 1 7では、所有装置判定部1 0 5は、受信した乱数を、ステップS 1 3 4 0 1 3において生成した乱数と照合して検証する。

【0 2 7 6】

利用装置乱数検証ステップS 1 3 4 0 1 8では、所有装置判定部1 0 5は、検証が成功した場合、次のステップに進む。所有装置判定部1 0 5は、検証が失敗した場合、プログラムを終了する。

30

【0 2 7 7】

利用装置共通鍵生成ステップS 1 3 4 0 1 9では、所有装置鍵生成部1 0 8は、ステップS 1 3 4 0 0 8において受信した共通鍵生成用乱数とステップS 1 3 4 0 1 2において生成した共通鍵生成用乱数から共通鍵を生成する。

【0 2 7 8】

操作開始要求暗号化ステップS 1 3 4 0 2 0では、所有装置暗号化部1 0 7は、共通鍵を用いて操作開始要求を暗号化する。

【0 2 7 9】

操作開始要求送信ステップS 1 3 4 0 2 1では、所有装置送信部1 0 2は、暗号化した操作開始要求を車両1 1 2 0 1に対して送信する。車両所有者の携帯電話1 1 0 0 1は、暗号化した操作開始要求を車両1 1 2 0 1に対して送信後、プログラムを終了する。

40

【0 2 8 0】

操作開始要求受信ステップS 1 4 4 0 2 1では、制御装置受信部3 0 2は、暗号化された操作開始要求を受信する。

【0 2 8 1】

操作開始要求復号ステップS 1 4 4 0 2 2では、制御装置復号部3 0 9は、暗号化された操作開始要求を共通鍵で復号する。

【0 2 8 2】

操作可能状態移行ステップS 1 4 4 0 2 3では、車両側車両操作プログラム6 1 0 0 4

50

は、車両操作可能状態へ移行する。車両 1 1 2 0 1 は、車両操作可能状態へ移行後、プログラムを終了する。

【0 2 8 3】

車両所有者の携帯電話 1 1 0 0 1 と車両 1 1 2 0 1 とは、実施の形態 1 と同様に赤外線通信などにより通信が行われる。

【0 2 8 4】

次に、車両借用者の携帯電話 1 1 1 0 1 が車両 1 1 2 0 1 を操作する動作について図 4 6、図 4 4、図 4 5 を用いて説明する。図 4 6 は、車両借用者の携帯電話 1 1 1 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

【0 2 8 5】

ステップ S 1 3 4 0 0 1 からステップ S 1 3 4 0 0 2、ステップ S 1 4 4 0 0 1 からステップ S 1 4 4 0 0 3 は、車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する動作の時と同様であるので、ここでは省略する。

【0 2 8 6】

利用装置証明書送信ステップ S 1 3 4 0 0 3 では、借用装置送信部 2 0 1 は、車両 1 1 2 0 1 に対して署名付きチケットを送信する。

【0 2 8 7】

制御装置証明書受信ステップ S 1 4 4 0 0 3 では、制御装置受信部 3 0 2 は、署名付きチケットを受信する。

【0 2 8 8】

制御装置証明書解析ステップ S 1 4 4 0 0 4 では、制御装置判定部 3 0 4 は、受信したデータの種別を解析する。

【0 2 8 9】

制御装置証明書照合ステップ S 1 4 4 0 0 5 では、制御装置判定部 3 0 4 は、記憶部 1 1 2 0 4 に格納されている利用者の証明書を用いて署名を検証する。

【0 2 9 0】

制御装置証明書照合ステップ S 1 4 4 0 0 6 では、制御装置判定部 3 0 4 は、検証に成功した場合、次のステップに進む。制御装置判定部 3 0 4 は、検証に失敗した場合、プログラムを終了する。

【0 2 9 1】

制御装置証明書検証ステップ S 1 4 4 0 0 7 では、制御装置判定部 3 0 4 は、検証に成功すると、チケットに含まれる車両借用者の証明書 5 4 0 0 2 を検証する。

【0 2 9 2】

以降、ステップ S 1 4 4 0 0 8 からステップ S 1 4 4 0 2 2 とステップ S 1 3 4 0 0 4 からステップ S 1 3 4 0 2 1 は、車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する動作の時と同様であるので、ここでは省略する。

【0 2 9 3】

操作可能状態移行ステップ S 1 4 4 0 2 3 では、車両側車両操作プログラム 6 1 0 0 4 は、操作許可情報 1 1 1 1 1 2 と操作制限情報 1 1 1 1 1 3 とに基づいて、車両操作可能状態へ移行する。車両側車両操作プログラム 6 1 0 0 4 は、車両操作可能状態へ移行後、プログラムを終了する。

【0 2 9 4】

車両借用者の携帯電話 1 1 1 0 1 と車両 1 1 2 0 1 とは、実施の形態 1 と赤外線通信などにより通信が行われる。

【0 2 9 5】

実施の形態 4 では、公開鍵証明書を用いているが、その他の実施の形態においても公開鍵の代わりに公開鍵証明書を使用してもよい。

【0 2 9 6】

また、実施の形態 4 は公開鍵証明書を用いているが、公開鍵を含む任意の情報であってもよい。

10

20

30

40

50

【0297】

実施の形態4では、ISO/IEC 11770-3 Key Transport Mechanism 6に示される認証手順を使用しているが、同等の効果を得られるその他の認証手順を用いてもよい。

【0298】

以上のように、実施の形態4では、上述した実施の形態における車両操作権限委譲システムの車両操作権限委譲時において、車両所有者の携帯電話11001と車両借用者の携帯電話11101との間でメッセージを暗号化するための共通鍵を共有した。そのため、上述した実施の形態の効果に加えて車両操作権限委譲時に第三者からの盗聴や割り込み利用を防ぐことができる。

10

【0299】

また、車両操作時においては車両11201と車両利用者の間でメッセージを暗号化するための共通鍵を共有した。そのため、上述した実施の形態の効果に加えて車両操作時に第三者からの盗聴や割り込み利用を防ぐことができる。

【0300】

さらに、車両所有者の公開鍵31002、車両借用者の公開鍵51002、車両の公開鍵61002の代わりに車両所有者の証明書34002、車両借用者の証明書54002、車両の証明書64002を用いることにより、パーソナルコンピュータなど計算機向けの既存の認証システムを利用することができ、車両所有者の携帯電話11001と車両借用者の携帯電話11101とが遠隔地に離れていても安全に権限を委譲できる。

20

【0301】

実施の形態5.

次に実施の形態5について説明する。上述したの実施の形態1では、車両所有者の携帯電話11001から車両借用者の携帯電話11101に対してチケットを送信することによって、車両所有者の携帯電話11001から車両借用者の携帯電話11101へ車両操作権限を委譲するようにした。実施の形態5では、車両所有者の携帯電話11001が指定した車両11201のみ車両借用者が操作することが可能である。そのため、実施の形態5では、複数の車両11201を効率よく操作できる。

【0302】

実施の形態5では、実施の形態1における車両操作権限委譲システムのチケットに車両の公開鍵61002を加える。そのため、実施の形態5では、実施の形態1の効果に加えて、車両所有者の携帯電話11001が指定した車両11201のみ車両借用者が操作することができる。

30

【0303】

また、実施の形態5では、車両利用者が車両11201を操作する時に車両の公開鍵61002を車両11201から受信する手順を加えることにより、車両利用者は複数の車両11201を効率よく操作することができる。

【0304】

図47は、実施の形態5にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。図47に示す機能ブロック図は、図2に示す機能ブロック図と概ね同様であるため、差分についてのみ説明する。

40

【0305】

権限所有装置100は、さらに、所有装置検索部110を備える。所有装置検索部110は、車両所有者の公開鍵31002から、操作する車両11201に対する公開鍵を検索する。

【0306】

権限借用装置200は、さらに、借用装置検索部210を備える。借用装置検索部210は、車両借用者の公開鍵51002から、操作する車両11201に対するチケットを検索する。

【0307】

50

実施の形態 5 における車両操作権限委譲システムの記憶部の構成は、車両所有者の携帯電話 11001 の UIM11008 の記憶部 11011 を除いて、実施の形態 1 と同様であるので、ここでは差分についてのみ説明する。

【0308】

図 48 は、車両所有者の携帯電話 11001 の UIM11008 の記憶部 11011 に格納されたデータである。車両所有者の秘密鍵 31001 は公開鍵暗号方式における秘密鍵であり、車両所有者に対応する。車両所有者の公開鍵 31002 は公開鍵暗号方式における公開鍵であり、車両所有者の秘密鍵 31001 と対をなす。車両の公開鍵 61002 は公開鍵暗号方式における公開鍵であり車両の秘密鍵 61001 と対をなす。

【0309】

次に、上記のように構成された実施の形態 5 の動作について説明する。実施の形態 5 の動作は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話 11101 が車両 11201 を操作する動作とを備える。

【0310】

まず、車両操作権限を委譲する動作について図 8、図 9、図 10 を用いて説明する。

【0311】

ステップ S91001 からステップ S91004、ステップ S101001 からステップ S101004 は、実施の形態 1 と同様であるので、ここでは説明を省略する。

【0312】

チケット生成ステップ S91005 では、チケット生成部 101、車両借用者のチケットを作成する。チケット生成部 101 が生成したチケットは、車両借用者の公開鍵 51002 と車両借用者の操作許可情報 111112 と操作制限情報 111113 とを備える。車両借用者の操作許可情報 111112 と操作制限情報 111113 とは、車両操作権限を委譲する前に、あらかじめ車両所有者により設定されている。

【0313】

チケット署名ステップ S91006 では、チケット生成部 101 は、車両所有者の秘密鍵 31001 を用いてチケットと車両の公開鍵 61002 との署名情報を作成する。ここで、車両の公開鍵 61002 は、このチケットで制御可能な車両を制限する制御装置制限情報である。

【0314】

チケット送信ステップ S91007 では、所有装置送信部 102 は、署名付きチケットを車両借用者の携帯電話 11101 に送信する。

【0315】

チケット受信ステップ S101005 では、借用装置受信部 202 は、署名付きチケットを受信する。

【0316】

ステップ S91008、ステップ S101006 からステップ S101009 は、実施の形態 1 と同様であるので、ここでは説明を省略する。

【0317】

車両所有者の携帯電話 11001 と車両借用者の携帯電話 11101 とは、安全な通信経路で通信する。

【0318】

図 49 は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲した後、車両借用者の携帯電話 11101 の UIM11108 の記憶部 11111 に格納される情報である。車両操作権限を委譲する前と比較して、車両借用者の公開鍵 51002 を含む車両所有者の署名付きチケット 111001 が加わっている。

【0319】

次に、車両所有者の携帯電話 11001 が車両 11201 を操作する動作について図 5

10

20

30

40

50

0、図51、図52を用いて説明する。図50は、車両所有者の携帯電話11001が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。図51は、車両所有者または車両借用者（以下、車両利用者）の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。図52は、車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

【0320】

ステップS135001、ステップS145001は、実施の形態1のステップS131001、S141001と同様なので、ここでは説明を省略する。

【0321】

制御装置公開鍵送信ステップS145002では、制御装置送信部301は、車両所有者の携帯電話11001に対して車両の公開鍵61002を送信する。

【0322】

利用装置公開鍵受信ステップS135002では、所有装置受信部103は、車両の公開鍵61002を受信する。

【0323】

利用装置検索ステップS135003では、所有装置検索部110は、車両の公開鍵61002に対応する車両所有者の公開鍵31002を検索する。

【0324】

利用装置データ送信ステップS135004では、所有装置送信部102は、車両11201に対して車両所有者の公開鍵31002を送信する。車両所有者の携帯電話11001は、公開鍵35002を送信後、プログラムを終了する。

【0325】

制御装置データ受信ステップS145003では、制御装置受信部302は、車両所有者の公開鍵31002を受信する。

【0326】

ステップS145004からステップS145009は、実施の形態1のステップS141004からステップS141007と同様なので、ここでは説明を省略する。

【0327】

車両所有者の携帯電話11001と車両11201とは、赤外線通信などにより通信が行われる。

【0328】

次に、車両借用者の携帯電話11101が車両11201を操作する動作について図53、図51、図52を用いて説明する。図53は、車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【0329】

ステップS135001からステップS135003、S145001からS145002は、車両所有者の携帯電話11001が車両11201を操作する場合と同様なので、ここでは説明を省略する。

【0330】

利用装置データ送信ステップS135004では、借用装置送信部201は、車両11201に対して署名付きチケットを送信する。車両借用者の携帯電話11101は、公開鍵35002を送信後、プログラムを終了する。

【0331】

制御装置データ受信ステップS145003では、制御装置受信部302は、署名付きチケットを受信する。

【0332】

データ解析ステップS145004では、制御装置判定部304は、受信したデータの種類を解析する。

【0333】

10

20

30

40

50

制御装置公開情報検証ステップS 1 4 5 0 0 5では、チケットに含まれる車両の公開鍵6 1 0 0 2を、記憶部1 1 2 0 4に格納している車両の公開鍵6 1 0 0 2と照合する。

【0 3 3 4】

制御装置公開情報検証ステップS 1 4 5 0 0 6では、制御装置判定部3 0 4は、照合が成功した場合、次のステップに進む。制御装置判定部3 0 4は、照合が失敗した場合、プログラムを終了する。

【0 3 3 5】

制御装置署名検証ステップS 1 4 5 0 0 7では、制御装置判定部3 0 4は、記憶部1 1 2 0 4に格納されている利用者の公開鍵を用いて署名を検証する。

【0 3 3 6】

制御装置署名検証ステップS 1 4 5 0 0 8では、制御装置判定部3 0 4は、検証に成功した場合、次のステップへ進み、制御装置判定部3 0 4は、検証に失敗した場合、プログラムを終了する。

【0 3 3 7】

操作可能状態移行ステップS 1 4 5 0 0 9では、車両側車両操作プログラム6 1 0 0 4は、操作許可情報1 1 1 1 1 2と操作制限情報1 1 1 1 1 3とに基づいて、車両操作可能状態へ移行する。車両1 1 2 0 1は、車両操作可能状態へ移行後、プログラムを終了する。

【0 3 3 8】

車両借用者の携帯電話1 1 1 0 1と車両1 1 2 0 1とは、赤外線通信などにより通信が行われる。

【0 3 3 9】

以上のように、実施の形態5では、実施の形態1における車両操作権限委譲システムのチケットに車両の公開鍵6 1 0 0 2を加えた。そのため、実施の形態5では、実施の形態1の効果に加えて、車両所有者の携帯電話1 1 0 0 1が指定した車両1 1 2 0 1のみ車両借用者が操作することができる。

【0 3 4 0】

また、実施の形態5では、車両利用者が車両1 1 2 0 1を操作する時に車両の公開鍵6 1 0 0 2を車両1 1 2 0 1から受信する手順を加えた。そのため、実施の形態5では、車両利用者は複数の車両1 1 2 0 1を効率よく操作することができる。

【0 3 4 1】

実施の形態6.

次に実施の形態6について説明する。上述した実施の形態1では、車両所有者の携帯電話1 1 0 0 1から車両借用者の携帯電話1 1 1 0 1に対してチケットを送信することによって、車両所有者の携帯電話1 1 0 0 1から車両借用者の携帯電話1 1 1 0 1へ車両操作権限を委譲するようにした。実施の形態6では、車両所有者の携帯電話1 1 0 0 1が指定した期間のみ車両借用者の携帯電話1 1 1 0 1が操作できる実施形態を示す。

【0 3 4 2】

実施の形態6では、実施の形態1における車両操作権限委譲システムのチケットにチケットの有効期限を加える。そのため、実施の形態6では、実施の形態1の効果に加えて、車両所有者の携帯電話1 1 0 0 1が指定した期間のみ車両借用者の携帯電話1 1 1 0 1が操作することができる。

【0 3 4 3】

実施の形態6における機能ブロック図および車両操作権限委譲システムの記憶部の構成は、実施の形態1と同様であるので、ここでは説明を省略する。

【0 3 4 4】

次に、上記のように構成された実施の形態6の動作について説明する。実施の形態6の動作は、車両所有者の携帯電話1 1 0 0 1が車両借用者の携帯電話1 1 1 0 1に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話1 1 1 0 1が車両1 1 2 0 1を操作する動作とを備える。

10

20

30

40

50

【0345】

まず、車両操作権限を委譲する動作について図8、図9、図10を用いて説明する。

【0346】

ステップS91001からステップS91004、ステップS101001からステップS101004は、実施の形態1と同様であるので、ここでは説明を省略する。

【0347】

チケット生成ステップS91005では、チケット生成部101は、車両借用者のチケットを作成する。チケットは、車両借用者の公開鍵51002と車両借用者の操作許可情報111112と操作制限情報111113とチケットの有効期限111114とを備える。車両借用者の操作許可情報111112と操作制限情報111113と有効期限111114とは、車両操作権限を委譲する前に、あらかじめ車両所有者により設定されている。

10

【0348】

チケット署名ステップS91006では、チケット生成部101は、車両所有者の秘密鍵31001を用いてチケットの署名情報を作成する。

【0349】

チケット送信ステップS91007では、所有装置送信部102は、署名付きチケットを車両借用者の携帯電話11101に送信する。

【0350】

チケット受信ステップS101005では、借用装置受信部202は、署名付きチケットを受信する。

20

【0351】

ステップS91008、ステップS101006からステップS101009は、実施の形態1と同様であるので、ここでは説明を省略する。

【0352】

車両所有者の携帯電話11001と車両借用者の携帯電話11101とは、安全な通信経路で通信する。

【0353】

図54は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲した後、車両借用者の携帯電話11101の記憶部に格納される情報である。UIM11108の記憶部11111には、車両操作権限を委譲する前と比較して、チケットの有効期限を含む車両所有者の署名付きチケット111001が加わっている。

30

【0354】

次に、車両所有者の携帯電話11001が車両11201を操作する動作については、実施の形態1のステップS141001からステップS141007と同様なので、ここでは説明を省略する。

【0355】

車両所有者の携帯電話11001と車両11201とは、赤外線通信などにより通信が行われる。

40

【0356】

次に、車両借用者の携帯電話11101が車両11201を操作する動作について図16、図14、図55を用いて説明する。図55は、車両所有者または車両借用者（以下、車両利用者）の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。

【0357】

ステップS146001からステップS146003は、車両所有者の携帯電話11001が車両11201を操作する場合と同様なので、ここでは説明を省略する。

【0358】

制御装置証明書解析ステップS146004では、制御装置判定部304は、受信した

50

データの種別を解析する。

【0359】

制御装置証明書照合ステップS146005では、制御装置判定部304は、記憶部11204に格納されている利用者の公開鍵を用いて署名を検証する。

【0360】

制御装置証明書照合ステップS146006では、制御装置判定部304は、照合に成功した場合、次のステップに進む。制御装置判定部304は、照合に失敗した場合、プログラムを終了する。

【0361】

時刻取得ステップS146007では、制御装置判定部304は、現在時刻を取得する。 10

【0362】

有効期限判定ステップS146008では、制御装置判定部304は、チケットに含まれる有効期限内であるか否かを判定する。制御装置判定部304は、有効期限内であれば次のステップへ進む。制御装置判定部304は、有効期限を超えていたらプログラムを終了する。

【0363】

操作可能状態移行ステップS146009では、操作許可情報111112と操作制限情報111113とに基づいて、車両操作可能状態へ移行する。車両側車両操作プログラム61004は、車両操作可能状態へ移行後、プログラムを終了する。 20

【0364】

車両借用者の携帯電話11101と車両11201とは、赤外線通信などにより通信が行われる。

【0365】

車両11201にチケットを格納した場合、有効期限切れのチケットは削除してもよい。この場合、車両11201の記憶部の使用容量を節約することができる。

【0366】

以上のように、実施の形態6では、実施の形態1における車両操作権限委譲システムのチケットに、チケットの有効期限を加えた。そのため、実施の形態6では、実施の形態1の効果に加えて、車両所有者が指定した期間のみ車両借用者の携帯電話11101が操作 30

【0367】

実施の形態7.

次に実施の形態7について説明する。上述した実施の形態では、車両11201の操作時に車両利用者は携帯電話の操作を行うことをしない。上述した実施の形態では、自動的に車両11201を操作するスマートキーシステムにおいて車両操作権限を委譲するようにしたものである。実施の形態7では、車両利用者が携帯電話を操作することにより車両11201を操作するリモコン型スマートキーシステムにおいて車両操作権限を委譲できる実施形態を示す。

【0368】

実施の形態7における車両操作権限委譲システムは、これまでの実施の形態における車両操作権限委譲システムの車両操作時において送付する車両所有者の署名付きチケットに車両操作コマンドを加える。そのため、実施の形態7における車両操作権限委譲システムは、車両利用者が携帯電話によって車両11201を操作するリモコン型スマートキーシステムにおいて車両操作権限を委譲できる。 40

【0369】

図56は、実施の形態7にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。図56に示す機能ブロック図は、図2に示す機能ブロック図と概ね同様であるため、差分についてのみ説明する。

【0370】

権限所有装置 100 は、さらに、所有装置入力部 111 を備える。所有装置入力部 111 は、制御装置 300 への指示を入力する。

権限借用装置 200 は、さらに、借用装置入力部 211 を備える。借用装置入力部 211 は、制御装置 300 への指示を入力する。

【0371】

実施の形態 7 における車両操作権限委譲システムの記憶部の構成は、実施の形態 1 と同様であるので、ここでは説明を省略する。

【0372】

次に、上記のように構成された実施の形態 7 の動作について説明する。実施の形態 7 の動作は、車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話 11101 が車両 11201 を操作する動作とを備える。

【0373】

車両操作権限を委譲する動作については、実施の形態 1 と同様であるので、ここでは説明を省略する。

【0374】

次に、車両所有者の携帯電話 11001 が車両 11201 を操作する動作について図 57、図 58、図 59 を用いて説明する。図 57 は、車両所有者の携帯電話 11001 が車両 11201 を操作する一連の動作を示すメッセージのシーケンス図である。図 58 は、車両所有者または車両借用者（以下、車両利用者）の携帯電話 11001 または 11101 の端末側車両操作プログラム 21003 または 41003 の一連の動作を示すフローチャートである。図 59 は、車両 11201 の車両側車両操作プログラム 61004 の一連の動作を示すフローチャートである。

【0375】

通信リンク確立ステップ S137001 および S147001 では、車両側車両操作プログラム 61004 は、制御装置送信部 301 を介し、定期的に携帯電話に対して応答要求を送信する。車両所有者の携帯電話 11001 が車両 11201 に近づき、車両所有者の携帯電話 11001 の端末側車両操作プログラム 21003 が応答要求を受信することによって、車両 11201 と車両所有者の携帯電話 11001 との通信リンクを確立する。

【0376】

操作コマンド入力ステップ S137002 では、所有装置入力部 111 は、車両 11201 の操作コマンドを入力する。所有装置入力部 111 は、例えば、車両所有者の携帯電話 11001 の操作ボタンに車両 11201 の操作コマンドが割り振られている場合に、車両所有者は携帯電話の操作ボタンを押下することによってドアのアンロックなどの車両 11201 の操作を行う。

【0377】

操作コマンド送信ステップ S137003 では、所有装置送信部 102 は、車両 11201 に対して、車両所有者の公開鍵 31002 と車両 11201 の操作コマンドとを送信する。車両所有者の携帯電話 11001 は、車両所有者の公開鍵 31002 と車両 11201 の操作コマンドとを送信後、プログラムを終了する。

【0378】

操作コマンド受信ステップ S147002 では、制御装置受信部 302 は、車両所有者の公開鍵 31002 と車両 11201 の操作コマンドとを受信する。

【0379】

制御装置データ解析ステップ S147003 では、制御装置判定部 304 は、受信したデータの種類を解析する。

【0380】

制御装置データ検証ステップ S147104 では、制御装置判定部 304 は、記憶部 11204 に格納している車両利用者の公開鍵と照合する。

【0381】

制御装置データ検証ステップS147105では、制御装置判定部304は、照合に成功した場合、次のステップに進む。制御装置判定部304は、照合に失敗した場合、プログラムを終了する。

【0382】

操作可能状態移行ステップS147006では、車両側車両操作プログラム61004は、車両11201の操作コマンドに基づいて、車両操作可能状態へ移行する。車両側車両操作プログラム61004は、例えば、ドアのアンロック、エンジン始動などの車両操作可能状態へ移行する。車両11201は、車両操作可能状態へ移行後、プログラムを終了する。

10

【0383】

車両所有者の携帯電話11001と車両11201とは、赤外線通信などにより通信が行われる。

【0384】

次に、車両借用者の携帯電話11101が車両11201を操作する動作について図60、図58、図59を用いて説明する。図60は、車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【0385】

ステップS137001からステップS137002、ステップS147001は、車両所有者の携帯電話11001が車両11201を操作する動作の時と同様であるので、ここでは省略する。

20

【0386】

操作コマンド送信ステップS137003では、借用装置送信部201は、車両11201に対して署名付きチケットと車両11201の操作コマンドとを送信する。車両借用者の携帯電話11101は、署名付きチケットと車両11201の操作コマンドとを送信後、プログラムを終了する。

【0387】

操作コマンド受信ステップS147002では、制御装置受信部302は、署名付きチケットを受信する。

【0388】

制御装置データ解析ステップS147003では、制御装置判定部304は、受信したデータの種別を解析する。

30

【0389】

制御装置データ検証ステップS147004では、制御装置判定部304は、記憶部11204に格納されている利用者の公開鍵を用いて署名を検証する。

【0390】

制御装置データ検証ステップS147005では、制御装置判定部304は、検証に成功した場合、次のステップに進む。制御装置判定部304は、検証に失敗した場合、プログラムを終了する。

【0391】

操作可能状態移行ステップS147006では、車両側車両操作プログラム61004は、操作コマンド、操作許可情報111112と操作制限情報111113とに基づいて、車両操作可能状態へ移行する。車両11201は、車両操作可能状態へ移行後、プログラムを終了する。

40

【0392】

車両借用者の携帯電話11101と車両11201とは、赤外線通信などにより通信が行われる。

【0393】

以上のように、実施の形態7では、上述した実施の形態における車両操作権限委譲システムの車両操作時において、送付する車両所有者の署名付きチケットに車両操作コマンド

50

を加えた。そのため、実施の形態7では、車両利用者が携帯電話によって車両11201を操作するリモコン型スマートキーシステムにおいて車両操作権限を委譲できる。

【0394】

実施の形態8.

次に実施の形態8について説明する。上述した実施の形態では、車両所有者の携帯電話11001から車両借用者の携帯電話11101にチケットを送付することによって、車両11201の操作権限を委譲するようにしたものである。実施の形態8では、車両所有者の携帯電話11001から車両11201にチケットを送付することによって、車両11201の操作権限を委譲する。

【0395】

実施の形態8では、上述した実施の形態における車両操作権限委譲システムの車両操作権限委譲時に車両所有者の携帯電話11001から車両借用者の携帯電話11101にチケットを送付する代わりに、車両所有者の携帯電話11001から車両11201にチケットを送付する。そのため、実施の形態8では、上述した実施の形態と同様に、管理サーバを必要とせずに車両11201の操作権限を委譲することができる。

【0396】

また、車両借用者の携帯電話11101には、車両操作権限を委譲するための付加情報を格納する必要がなく、車両借用者の手間を省くことができる。

【0397】

実施の形態8における機能ブロック図は、実施の形態1と同様であるので、ここでは説明を省略する。

【0398】

実施の形態8における車両操作権限委譲システムの記憶部の構成は、車両11201の記憶部11204を除いて、実施の形態1と同様であるので、ここでは差分についてのみ説明する。

【0399】

図61は、車両11201の記憶部11204に格納されたプログラムおよびデータである。車両操作権限設定プログラム61005は車両11201の操作権限を委譲するための設定を行うプログラムである。車両側車両操作プログラム61004は車両11201が動作するための処理を行うプログラムである。車両の秘密鍵61001は公開鍵暗号方式における秘密鍵であり、車両11201に対応する。車両の公開鍵61002は公開鍵暗号方式における公開鍵であり、車両の秘密鍵61001と対をなす。車両所有者の公開鍵31002は公開鍵暗号方式における公開鍵であり、車両所有者の公開鍵31002と同一のものである。

【0400】

次に、上記のように構成された実施の形態8の動作について説明する。実施の形態8の動作は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する動作と、車両操作権限を委譲された車両借用者の携帯電話11101が車両11201を操作する動作とを備える。

【0401】

まず、車両操作権限を委譲する動作について図62、図63、図64、図65を用いて説明する。図62は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。図63は、車両所有者の携帯電話11001の車両操作権限貸与プログラム21001の一連の動作を示すフローチャートである。図64は、車両借用者の携帯電話11101の車両操作権限借用プログラム41002の一連の動作を示すフローチャートである。図65は、車両11201の車両操作権限設定プログラム61005の一連の動作を示すフローチャートである。

【0402】

まず、車両所有者の携帯電話11001は、車両操作権限貸与プログラム21001を

10

20

30

40

50

起動する。車両借用者の携帯電話11101は、車両操作権限借用プログラム41001を起動する。

【0403】

所有装置公開鍵要求ステップS98001では、所有装置送信部102は、車両借用者の携帯電話11101に対して車両借用者の公開鍵要求を送信する。

【0404】

借用装置公開鍵要求受信ステップS108001では、借用装置受信部202は、車両借用者の公開鍵要求を受信する。

【0405】

借用装置公開鍵送信ステップS108002では、借用装置送信部201は、車両所有者の携帯電話11001に対して車両借用者の公開鍵51002を送信する。車両借用者の携帯電話11101は、車両借用者の公開鍵51002を送信後、プログラムを終了する。

10

【0406】

所有装置公開鍵受信ステップS98002では、所有装置受信部103は、車両借用者の公開鍵51002を受信する。所有装置記憶部104は、受信した公開鍵を一時的に記憶する。例えば、図1に示すUIM11008の記憶部11011は、受信した公開鍵を一時的に格納する。

【0407】

チケット生成ステップS98003では、チケット生成部101は、車両借用者のチケットを作成する。チケットは、車両借用者の公開鍵51002と車両借用者の操作許可情報111112と操作制限情報111113とを備える。車両借用者の操作許可情報111112と操作制限情報111113とは、車両操作権限を委譲する前に、あらかじめ車両所有者の携帯電話11001により設定されている。

20

【0408】

チケット署名ステップS98004では、チケット生成部101は、車両所有者の秘密鍵31001を用いてチケットの署名情報を作成する。

【0409】

通信リンク確立ステップS98005およびS178001では、車両操作権限貸与プログラム21001は、車両11201との通信リンクを確立する。

30

【0410】

チケット送信ステップS98006では、所有装置送信部102署名付きチケットを車両11201へ送信する。

【0411】

チケット受信ステップS178002では、制御装置受信部302は、署名付きチケットを受信する。

【0412】

制御装置チケット検証ステップS178003では、制御装置判定部304は、車両所有者の公開鍵31002を用いて署名情報を検証する。

【0413】

40

制御装置チケット検証ステップS178004では、制御装置判定部304は、検証に成功した場合、次のステップへ進む。制御装置判定部304は、検証に失敗した場合、プログラムを終了する。

【0414】

制御装置チケット記憶ステップS178005では、制御装置記憶部303は、署名付きチケットを記憶する。

【0415】

チケット受信完了通知ステップS178006では、制御装置送信部301は、車両所有者の携帯電話11001に対して署名付きチケット受信完了通知を送信する。車両11201は、署名付きチケット受信完了通知を送信後、プログラムを終了する。

50

【0416】

チケット受信完了通知受信ステップS98007では、所有装置受信部103は、チケット受信完了通知を受信する。車両所有者の携帯電話11001は、チケット受信完了通知を所有装置受信部103が受信後、プログラムを終了する。

【0417】

車両所有者の携帯電話11001と車両借用者の携帯電話11101とは、実施の形態1と同様に安全な通信経路で通信する。

【0418】

車両所有者の携帯電話11001と車両11201間は、実施の形態1と同様に赤外線通信などにより通信が行われる。

10

【0419】

図66は、車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲した後、車両11201の記憶部11204に格納される情報である。記憶部11204には、車両操作権限を委譲する前と比較して、チケット111101が加わっている。

【0420】

次に、車両所有者が車両11201を操作する動作について図13、図67、図68を用いて説明する。図67は、車両所有者または車両借用者（以下、車両利用者）の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。図68は、車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

20

【0421】

通信リンク確立ステップS138001およびS148001では、車両側車両操作プログラム61004は、制御装置送信部301を介し、例えば、定期的に携帯電話に対して応答要求を送信する。車両所有者の携帯電話11001が車両11201に近づき、車両所有者の携帯電話11001の端末側車両操作プログラム21003が応答要求を受信することによって、車両11201と車両所有者の携帯電話11001との通信リンクを確立する。

【0422】

制御装置公開鍵要求ステップS148002では、制御装置送信部301は、車両所有者の携帯電話11001が車両11201の操作を開始したら、車両所有者の携帯電話11001に対して公開鍵要求を送信する。

30

【0423】

利用装置公開鍵要求受信ステップS138002では、所有装置受信部103は、公開鍵要求を受信する。

【0424】

利用装置公開鍵送信ステップS138003では、所有装置送信部102は、車両11201に対して車両所有者の公開鍵31002を送信する。車両所有者の携帯電話11001は、車両所有者の公開鍵31002を送信後、プログラムを終了する。

【0425】

制御装置公開鍵受信ステップS148003では、制御装置受信部302は、車両所有者の公開鍵31002を受信する。

40

【0426】

制御装置証明書照合ステップS148004では、制御装置判定部304は、受信した車両所有者の公開鍵31002を、記憶部11204に格納している車両利用者の公開鍵と照合する。

【0427】

制御装置証明書照合ステップS148005では、制御装置判定部304は、照合に成功した場合、次のステップに進む。制御装置判定部304は、照合に失敗した場合、プログラムを終了する。

50

【0428】

操作可能状態移行ステップS148006では、車両側車両操作プログラム61004は、車両操作可能状態へ移行する。車両側車両操作プログラム61004は、例えば、ドアのアンロック、エンジン始動などの車両操作可能状態へ移行する。車両11201は、車両操作可能状態へ移行後、プログラムを終了する。

【0429】

車両所有者の携帯電話11001と車両11201とは、赤外線通信などにより通信が行われる。

【0430】

次に、車両借用者の携帯電話11101が車両11201を操作する動作については、車両所有者の携帯電話11001が車両11201を操作する場合と同様なので、ここでは説明を省略する。

10

【0431】

以上のように、実施の形態8では、上述した実施の形態における車両操作権限委譲システムの車両操作権限委譲時に、車両所有者の携帯電話11001から車両借用者の携帯電話11101にチケットを送付する代わりに、車両所有者の携帯電話11001から車両11201にチケットを送付する。そのため、実施の形態8では、管理サーバを必要とせずに車両11201の操作権限を委譲することができる。

【0432】

また、実施の形態8では、車両借用者の携帯電話11101には、車両操作権限を委譲するための付加情報を格納する必要がなく、車両借用者の手間を省くことができる。

20

【0433】

実施の形態9.

次に実施の形態9について説明する。実施の形態9では、実施の形態1における車両所有者の携帯電話11001は、生成したチケットを記憶する。そのため、実施の形態9では、車両所有者の携帯電話11001は、委譲した権限を確認することが可能である。

また、実施の形態9では、実施の形態7における車両所有者の携帯電話11001は、チケットの有効期限が切れた場合には、記憶したチケットを削除する。

さらに、実施の形態9では、実施の形態8における車両11201は、チケットの有効期限が切れた場合には、記憶したチケットを削除する。

30

【0434】

図69は、実施の形態9にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。図69に示す機能ブロック図は、図2に示す機能ブロック図と概ね同様であるため、差分についてのみ説明する。

【0435】

権限所有装置100は、さらに、所有装置入力部111、所有装置表示部112、所有装置削除部113を備える。

所有装置入力部111は、生成したチケットの参照要求を入力する。所有装置表示部112は、所有装置入力部111から要求があった場合、チケットの内容を表示する。所有装置削除部113は、有効期限がきれたチケットを削除する。

40

制御装置300は、さらに、制御装置削除部310を備える。制御装置削除部310は、有効期限が切れたチケットを削除する。

【0436】

次に実施の形態9の動作について説明する。

まず、実施の形態1におけるチケット生成ステップS91005において、所有装置記憶部104は、チケット生成部101が生成したチケットを記憶する。

【0437】

所有装置入力部111は、生成したチケットの参照要求を入力する。例えば、車両や車両借用者の携帯電話11101を指定して参照要求を入力する。そして、所有装置表示部112は、所有装置入力部111から要求があった場合、チケットの内容を表示する。

50

【0438】

また、実施の形態7で示したように、チケットに有効期限を持たせている場合、所有装置削除部113は、有効期限がきれたチケットを削除する。同様に、実施の形態8で示したように、車両11201がチケットを記憶している場合、制御装置削除部310は、有効期限が切れたチケットを削除する。

【0439】

以上のように、実施の形態9では、車両所有者の携帯電話11001は、権限の委譲の状況を確認することが可能である。生成したチケットの情報は、車両所有者の携帯電話11001が記憶するのに限らず、外部のコンピュータやサーバなどが記憶しても構わない。

10

【0440】

また、実施の形態9では、記憶したチケットを有効期限が切れた場合には削除する。そのため、記憶装置の容量の圧迫を防ぐことが可能である。例えば、車両所有者の携帯電話11001や車両11201からは、有効期限が切れたチケットを削除し、外部のコンピュータやサーバには残すことなども可能である。

【産業上の利用可能性】

【0441】

車両や入り口などの鍵などに応用することで、鍵などを使用する権限を他者へ、サーバなどを介することなく、委譲することが可能である。また、操作権限の貸与は、個人利用だけでなく、カーシェアリングやレンタカーなど権限を貸与する場面などへ応用することが可能である。

20

【図面の簡単な説明】

【0442】

【図1】実施の形態にかかると権限所有装置100と権限借用装置200と制御装置300とのハードウェア構成図の一例である。

【図2】実施の形態1にかかると権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。

【図3】車両所有者の携帯電話11001の記憶部11006に格納されたプログラムである。

【図4】車両所有者の携帯電話11001におけるUIM11008の記憶部11011に格納されたデータである。

30

【図5】車両借用者の携帯電話11101の記憶部11106に格納されたプログラムである。

【図6】車両借用者の携帯電話11101におけるUIM11108の記憶部11111に格納されたデータである。

【図7】車両11201の記憶部11204に格納されたプログラムおよびデータである。

【図8】車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。

【図9】車両所有者の携帯電話11001の車両操作権限貸与プログラム21001の一連の動作を示すフローチャートである。

40

【図10】車両借用者の携帯電話11101の車両操作権限借用プログラム41002の一連の動作を示すフローチャートである。

【図11】車両借用者の操作許可情報111112や操作制限情報111113の入力画面の一例である。

【図12】車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲した後、車両借用者の携帯電話11101のUIM11108の記憶部11111に格納されている情報である。

【図13】車両所有者の携帯電話11001が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

50

【図14】車両所有者または車両借用者の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。

【図15】車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

【図16】車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【図17】実施の形態2にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。

【図18】実施の形態2における車両所有者の携帯電話11001のUIM11008の記憶部11011に格納されたデータである。

10

【図19】車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。

【図20】車両所有者の携帯電話11001の車両操作権限貸与プログラム21001の一連の動作を示すフローチャートである。

【図21】車両借用者の携帯電話11101の車両操作権限借用プログラム41002の一連の動作を示すフローチャートである。

【図22】車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲した後、車両借用者の携帯電話11101のUIM11108の記憶部11111に格納される情報である。

20

【図23】車両所有者の携帯電話11001が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【図24】車両所有者または車両借用者の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。

【図25】車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

【図26】車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【図27】車両所有者の携帯電話11001が車両借用者の携帯電話11101に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。

30

【図28】車両所有者の携帯電話11001の車両操作権限貸与プログラム21001の一連の動作を示すフローチャートである。

【図29】車両借用者の携帯電話11101の車両操作権限借用プログラム41002の一連の動作を示すフローチャートである。

【図30】車両所有者の携帯電話11001が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【図31】車両所有者または車両借用者の携帯電話11001または11101の端末側車両操作プログラム21003または41003の一連の動作を示すフローチャートである。

40

【図32】車両11201の車両側車両操作プログラム61004の一連の動作を示すフローチャートである。

【図33】車両借用者の携帯電話11101が車両11201を操作する一連の動作を示すメッセージのシーケンス図である。

【図34】実施の形態4にかかる権限所有装置100と権限借用装置200と制御装置300との機能ブロック図である。

【図35】車両所有者の携帯電話11001のUIM11008の記憶部11011に格納されたデータである。

【図36】車両借用者の携帯電話11101のUIM11108の記憶部11111に格納されたデータである。

50

【図 3 7】車両 1 1 2 0 1 の記憶部 1 1 2 0 4 に格納されたプログラムおよびデータである。

【図 3 8】車両所有者の携帯電話 1 1 0 0 1 が車両借用者の携帯電話 1 1 1 0 1 に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。

【図 3 9】車両所有者の携帯電話 1 1 0 0 1 の車両操作権限貸与プログラム 2 1 0 0 1 の一連の動作を示すフローチャートである。

【図 4 0】車両借用者の携帯電話 1 1 1 0 1 の車両操作権限借用プログラム 4 1 0 0 2 の一連の動作を示すフローチャートである。

【図 4 1】車両借用者の携帯電話 1 1 1 0 1 の車両操作権限借用プログラム 4 1 0 0 2 の一連の動作を示すフローチャートである。

10

【図 4 2】車両所有者の携帯電話 1 1 0 0 1 が車両借用者の携帯電話 1 1 1 0 1 に対して車両操作権限を委譲した後、車両借用者の携帯電話 1 1 1 0 1 の U I M 1 1 1 0 8 の記憶部 1 1 1 1 1 に格納される情報である。

【図 4 3】車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

【図 4 4】車両所有者または車両借用者の携帯電話 1 1 0 0 1 または 1 1 1 0 1 の端末側車両操作プログラム 2 1 0 0 3 または 4 1 0 0 3 の一連の動作を示すフローチャートである。

【図 4 5】車両 1 1 2 0 1 の車両側車両操作プログラム 6 1 0 0 4 の一連の動作を示すフローチャートである。

20

【図 4 6】車両借用者の携帯電話 1 1 1 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

【図 4 7】実施の形態 5 にかかる権限所有装置 1 0 0 と権限借用装置 2 0 0 と制御装置 3 0 0 との機能ブロック図である。

【図 4 8】車両所有者の携帯電話 1 1 0 0 1 の U I M 1 1 0 0 8 の記憶部 1 1 0 1 1 に格納されたデータである。

【図 4 9】車両所有者の携帯電話 1 1 0 0 1 が車両借用者の携帯電話 1 1 1 0 1 に対して車両操作権限を委譲した後、車両借用者の携帯電話 1 1 1 0 1 の U I M 1 1 1 0 8 の記憶部 1 1 1 1 1 に格納される情報である。

【図 5 0】車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

30

【図 5 1】車両所有者または車両借用者の携帯電話 1 1 0 0 1 または 1 1 1 0 1 の端末側車両操作プログラム 2 1 0 0 3 または 4 1 0 0 3 の一連の動作を示すフローチャートである。

【図 5 2】車両 1 1 2 0 1 の車両側車両操作プログラム 6 1 0 0 4 の一連の動作を示すフローチャートである。

【図 5 3】車両借用者の携帯電話 1 1 1 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

【図 5 4】車両所有者の携帯電話 1 1 0 0 1 が車両借用者の携帯電話 1 1 1 0 1 に対して車両操作権限を委譲した後、車両借用者の携帯電話 1 1 1 0 1 の記憶部に格納される情報である。

40

【図 5 5】車両所有者または車両借用者の携帯電話 1 1 0 0 1 または 1 1 1 0 1 の端末側車両操作プログラム 2 1 0 0 3 または 4 1 0 0 3 の一連の動作を示すフローチャートである。

【図 5 6】実施の形態 7 にかかる権限所有装置 1 0 0 と権限借用装置 2 0 0 と制御装置 3 0 0 との機能ブロック図である。

【図 5 7】車両所有者の携帯電話 1 1 0 0 1 が車両 1 1 2 0 1 を操作する一連の動作を示すメッセージのシーケンス図である。

【図 5 8】車両所有者または車両借用者（以下、車両利用者）の携帯電話 1 1 0 0 1 または 1 1 1 0 1 の端末側車両操作プログラム 2 1 0 0 3 または 4 1 0 0 3 の一連の動作を示

50

すフローチャートである。

【図 59】車両 11201 の車両側車両操作プログラム 61004 の一連の動作を示すフローチャートである。

【図 60】車両借用者の携帯電話 11101 が車両 11201 を操作する一連の動作を示すメッセージのシーケンス図である。

【図 61】車両 11201 の記憶部 11204 に格納されたプログラムおよびデータである。

【図 62】車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲する一連の動作を示すメッセージのシーケンス図である。

【図 63】車両所有者の携帯電話 11001 の車両操作権限貸与プログラム 21001 の一連の動作を示すフローチャートである。

【図 64】車両借用者の携帯電話 11101 の車両操作権限借用プログラム 41001 の一連の動作を示すフローチャートである。

【図 65】車両 11201 の車両操作権限設定プログラム 61005 の一連の動作を示すフローチャートである。

【図 66】車両所有者の携帯電話 11001 が車両借用者の携帯電話 11101 に対して車両操作権限を委譲した後、車両 11201 の記憶部 11204 に格納される情報である。

【図 67】車両所有者または車両借用者の携帯電話 11001 または 11101 の端末側車両操作プログラム 21003 または 41003 の一連の動作を示すフローチャートである。

【図 68】車両 11201 の車両側車両操作プログラム 61004 の一連の動作を示すフローチャートである。

【図 69】実施の形態 9 にかかる権限所有装置 100 と権限借用装置 200 と制御装置 300 との機能ブロック図である。

【符号の説明】

【0443】

11001 車両所有者の携帯電話、11002 通信部、11003 表示部、11004 入力部、11005 制御部、11006 記憶部、11007 カード部、11008 UIM、11009 通信部、11010 制御部、11011 記憶部、11101 車両借用者の携帯電話、11102 通信部、11103 表示部、11104 入力部、11105 制御部、11106 記憶部、11107 カード部、11108 UIM、11109 通信部、11110 制御部、11111 記憶部、11201 車両、11202 通信部、11203 制御部、11204 記憶部、100 権限所有装置、101 チケット生成部、102 所有装置送信部、103 所有装置受信部、104 所有装置記憶部、105 所有装置判定部、106 所有装置識別情報作成部、107 所有装置暗号化部、108 所有装置鍵生成部、109 所有装置復号部、110 所有装置検索部、111 所有装置入力部、112 所有装置表示部、113 所有装置削除部、200 権限借用装置、201 借用装置送信部、202 借用装置受信部、203 借用装置記憶部、204 借用装置指示部、205 借用装置判定部、206 借用装置識別情報作成部、207 借用装置暗号化部、208 借用装置鍵生成部、209 借用装置復号部、210 借用装置検索部、211 借用装置入力部、300 制御装置、301 制御装置送信部、302 制御装置受信部、303 制御装置記憶部、304 制御装置判定部、305 制御部、306 制御装置識別情報作成部、307 制御装置鍵生成部、308 制御装置暗号化部、309 制御装置復号部、310 制御装置削除部。

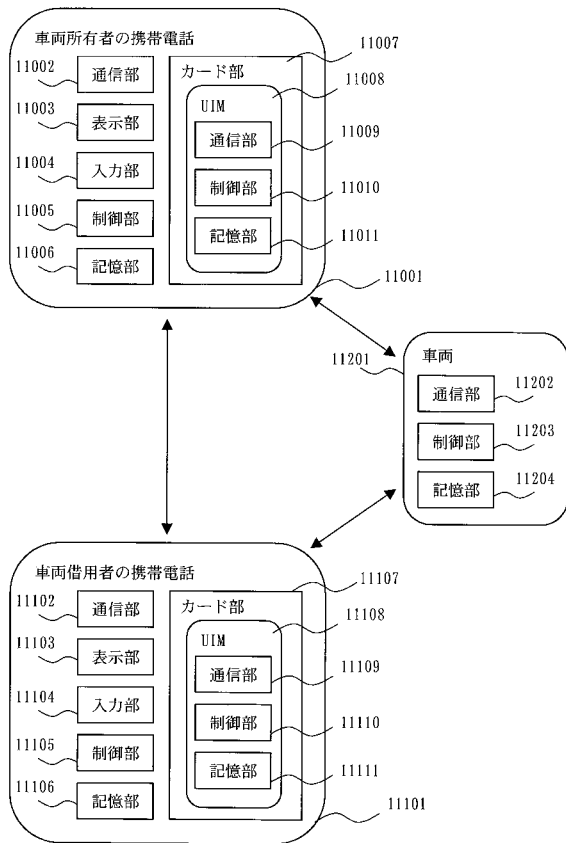
10

20

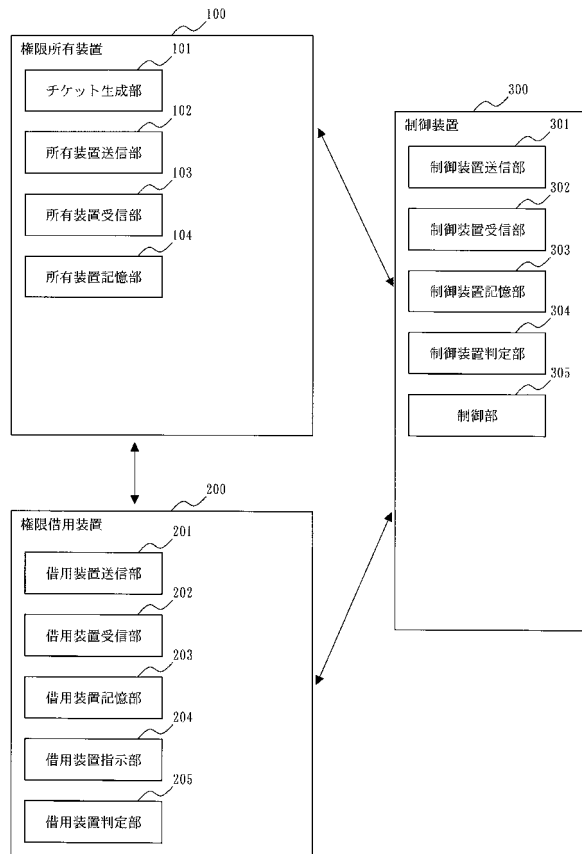
30

40

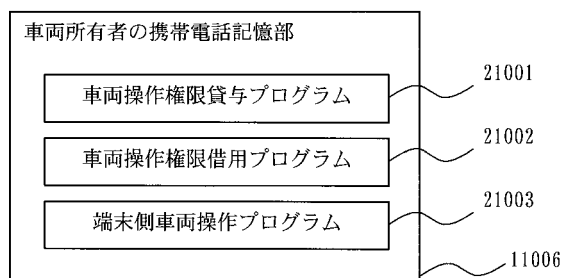
【図 1】



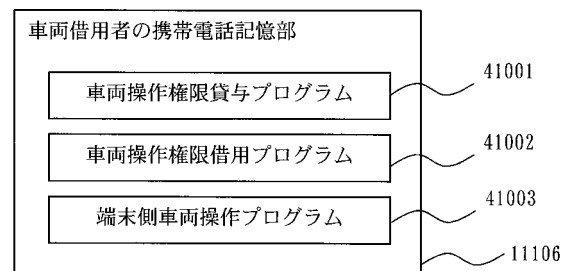
【図 2】



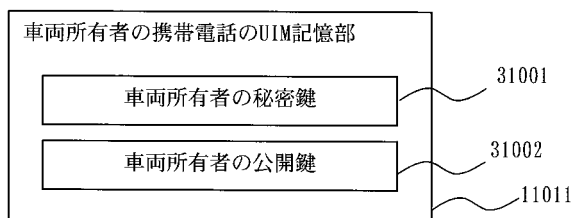
【図 3】



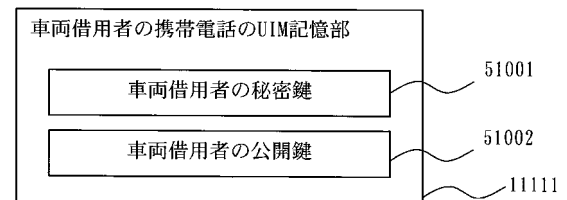
【図 5】



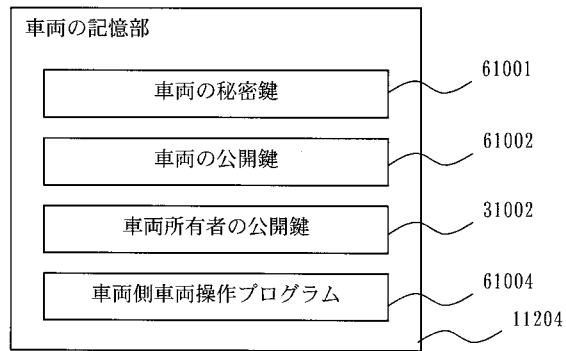
【図 4】



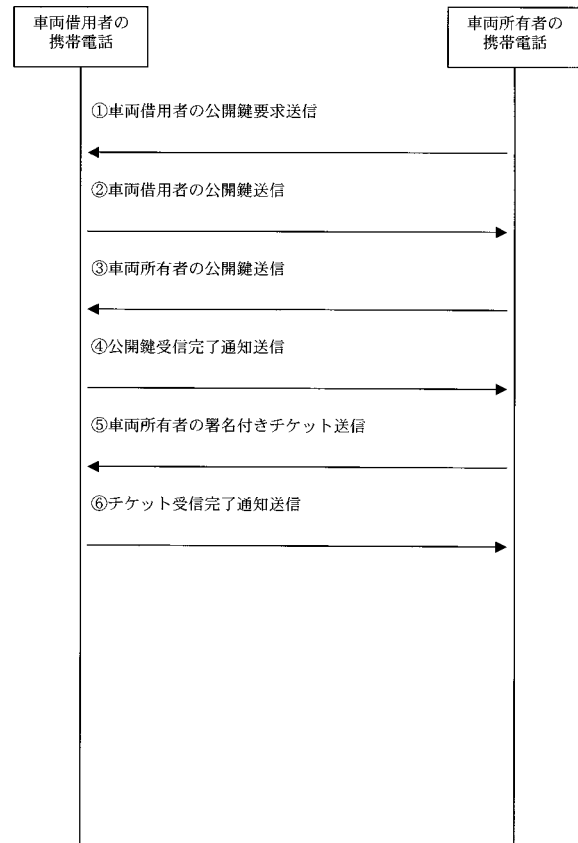
【図 6】



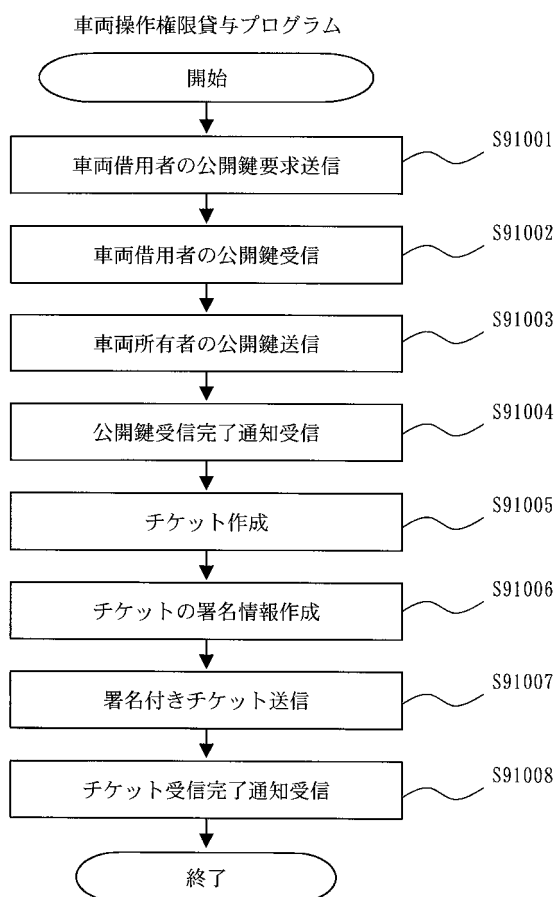
【図 7】



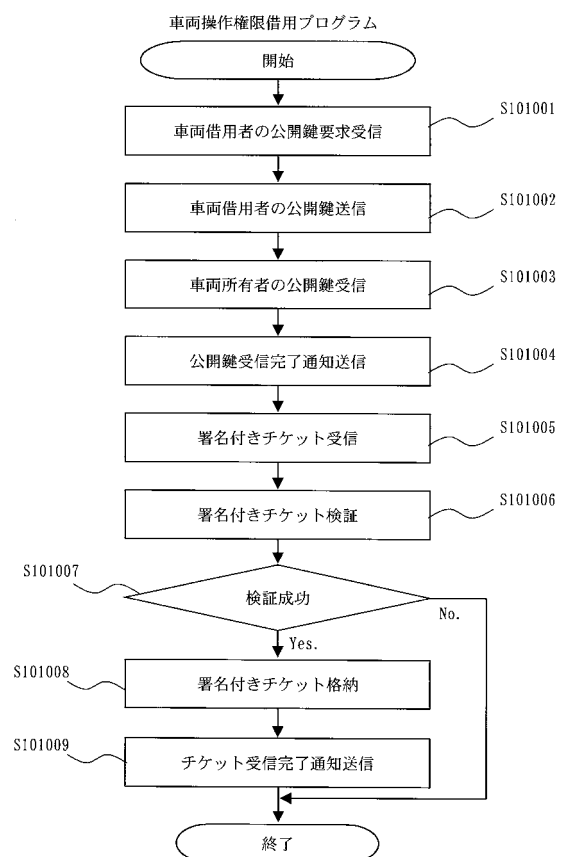
【図 8】



【図 9】



【図 10】



【図 1 1】

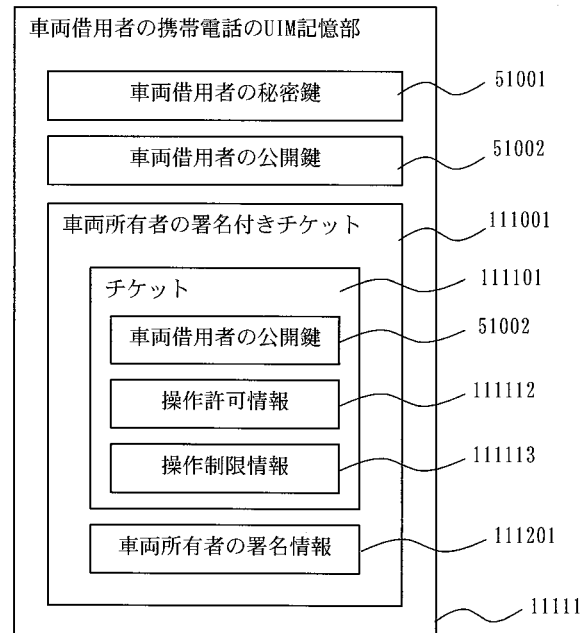
車を〇〇さんに貸します。
許可する操作を選んでください。

■ドア ■エンジン □トランク
□ETC □カーナビ □オーディオ

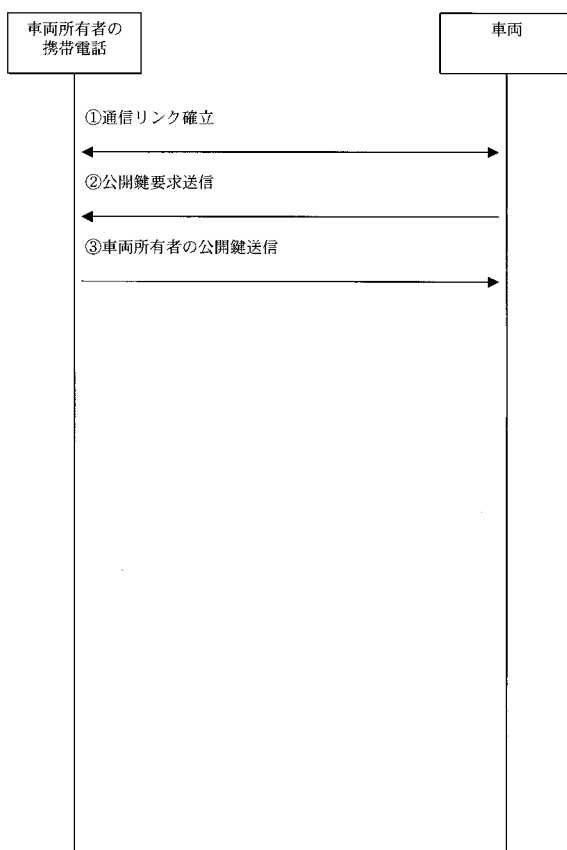
制約条件を入力してください。

走行距離 Km
走行範囲 半径 Km
利用時間 時まで

【図 1 2】

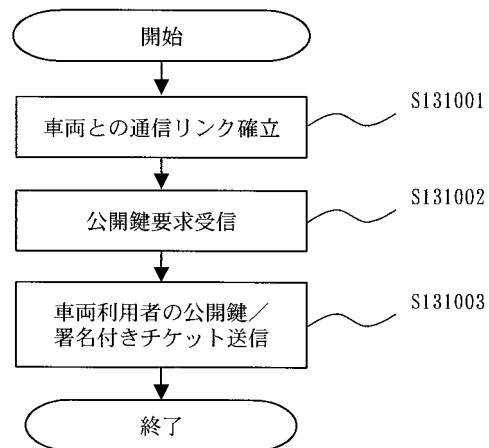


【図 1 3】

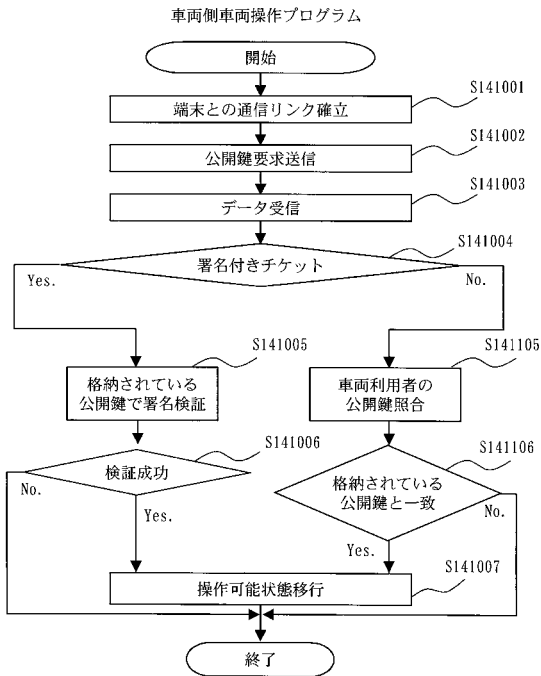


【図 1 4】

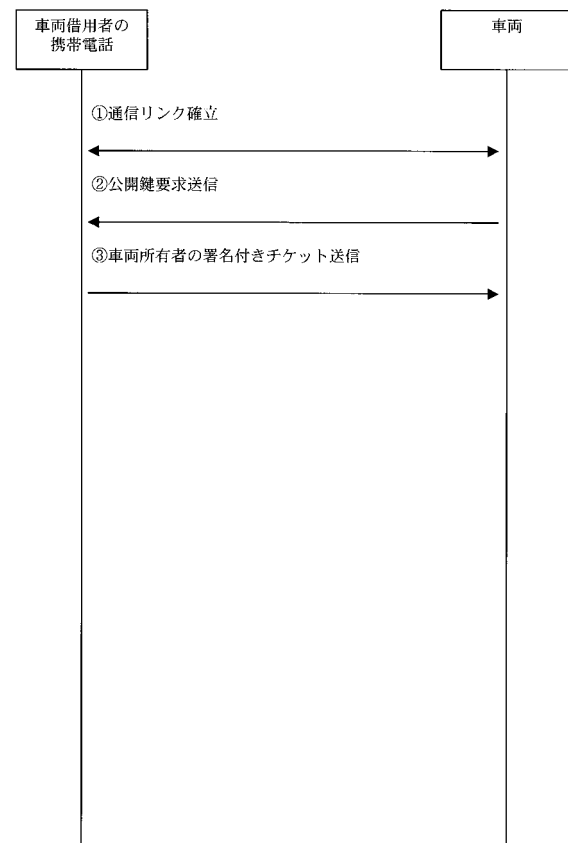
端末側車両操作プログラム



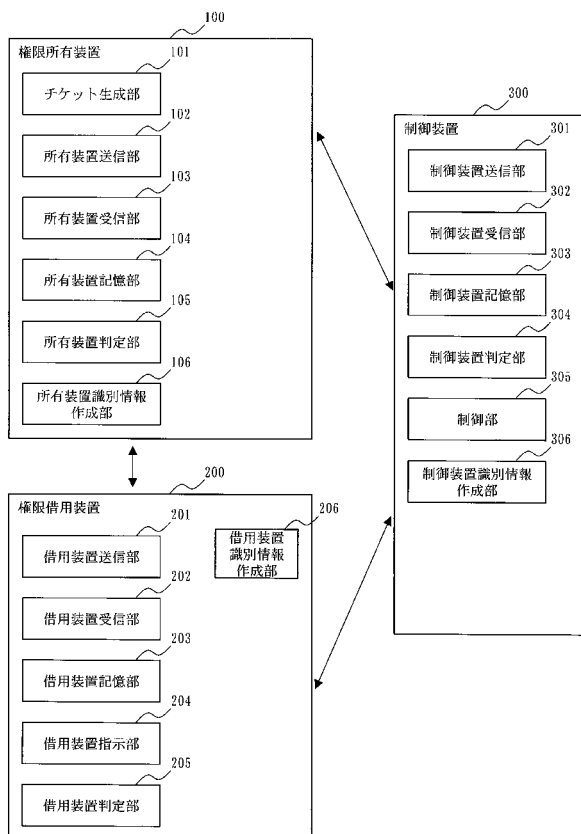
【図 15】



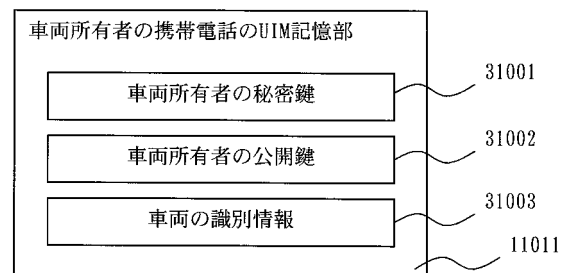
【図 16】



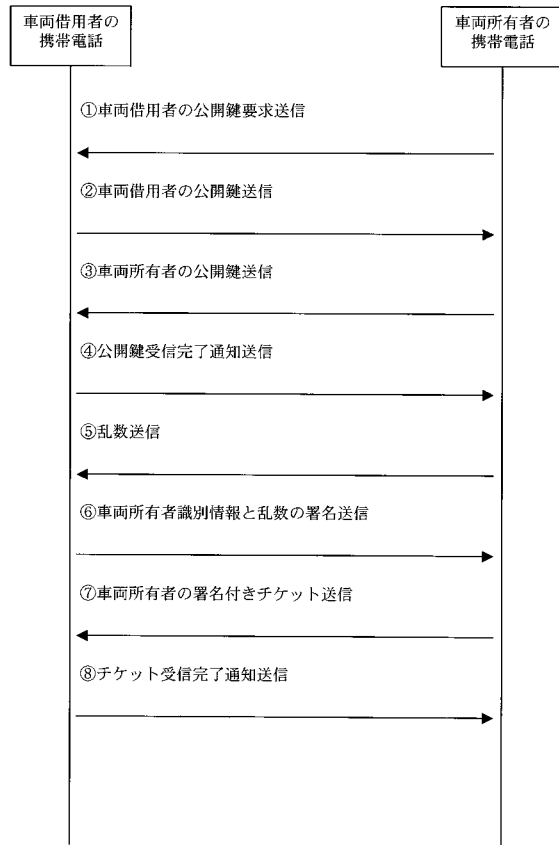
【図 17】



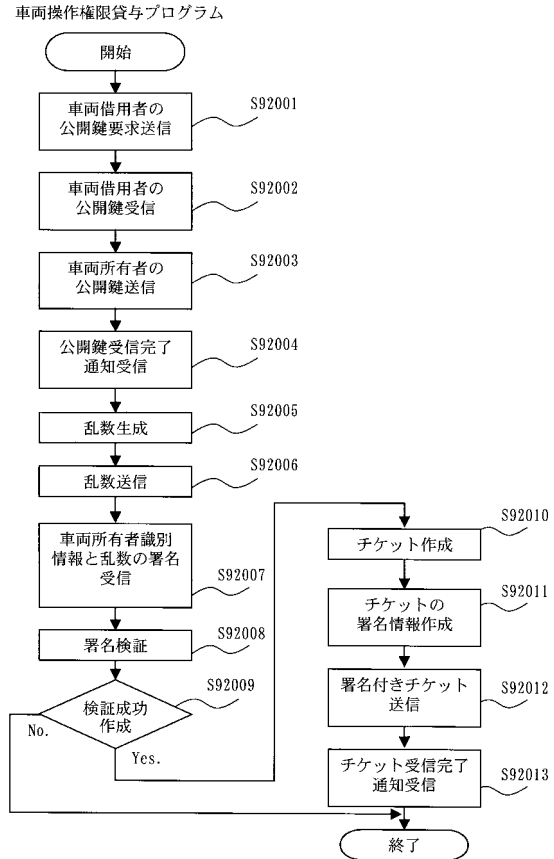
【図 18】



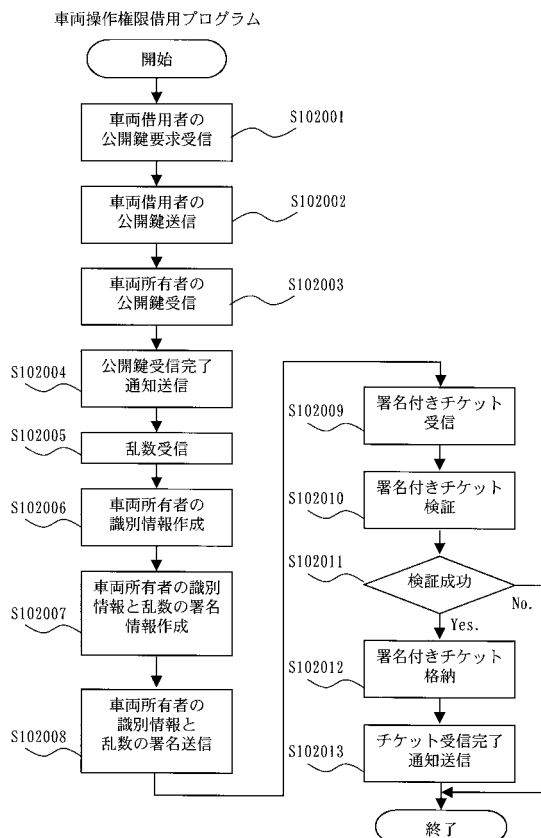
【図 19】



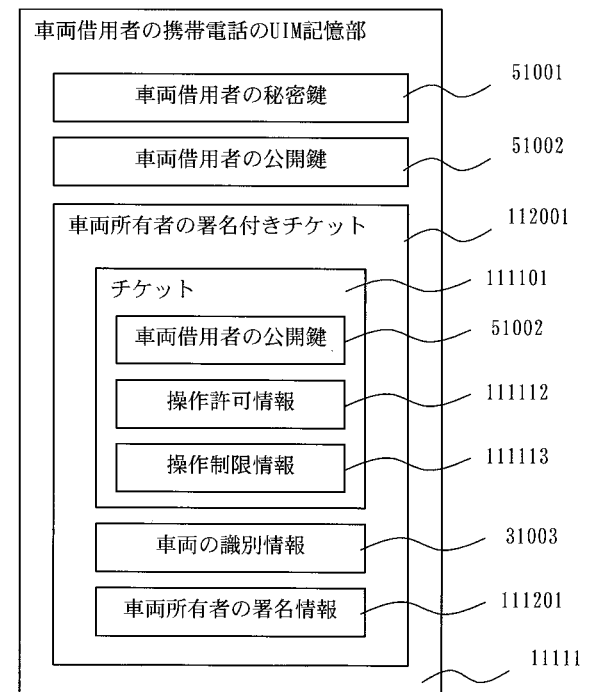
【図 20】



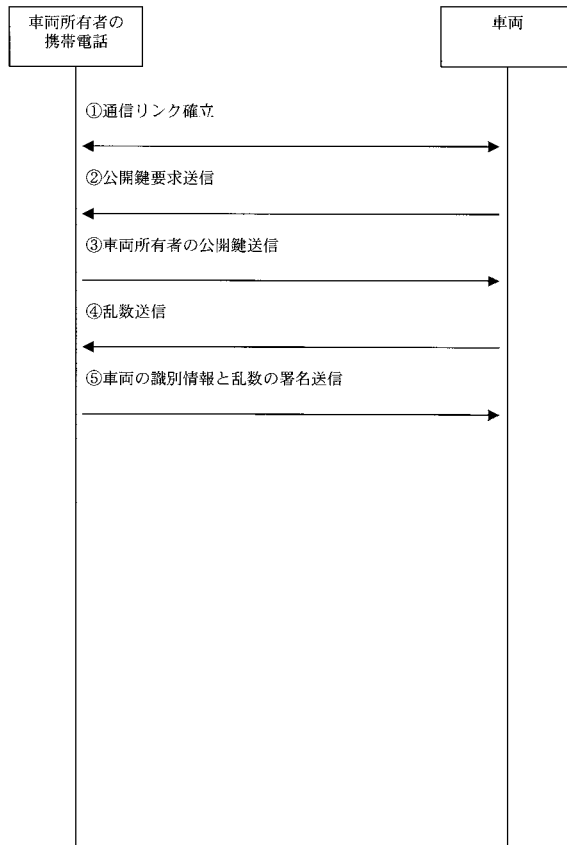
【図 21】



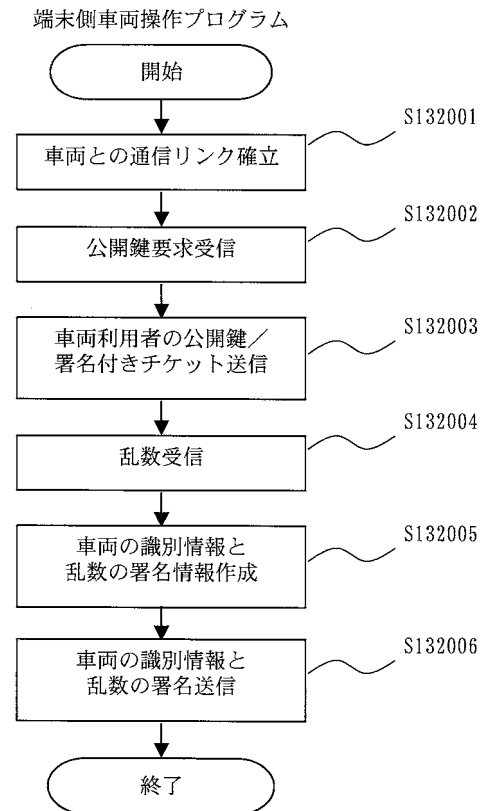
【図 22】



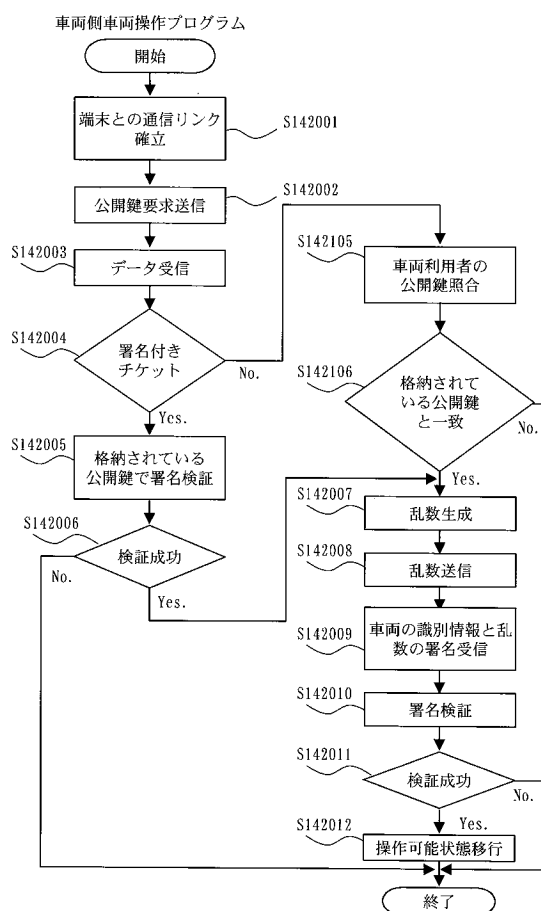
【図 2 3】



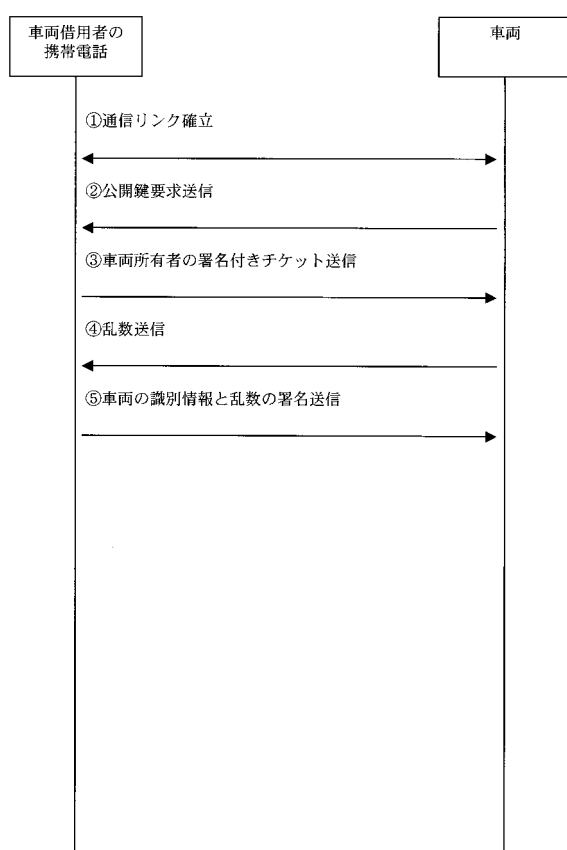
【図 2 4】



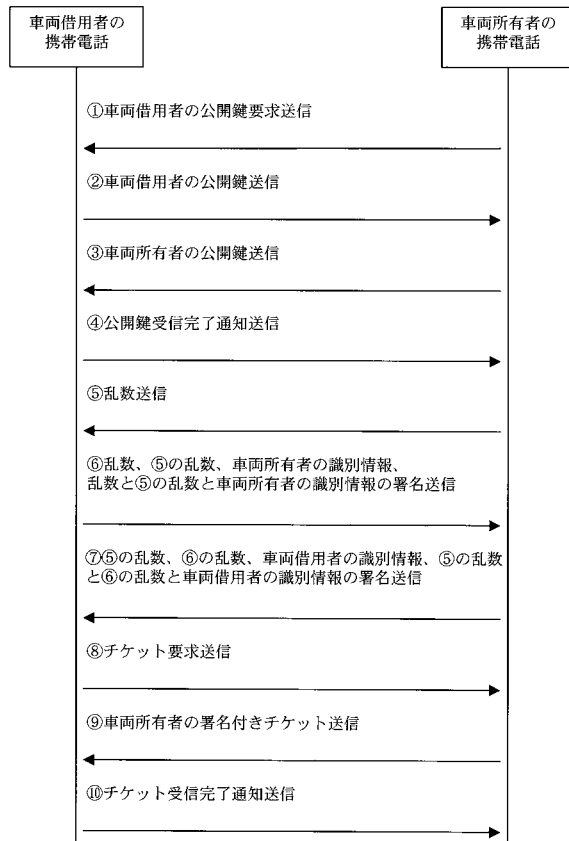
【図 2 5】



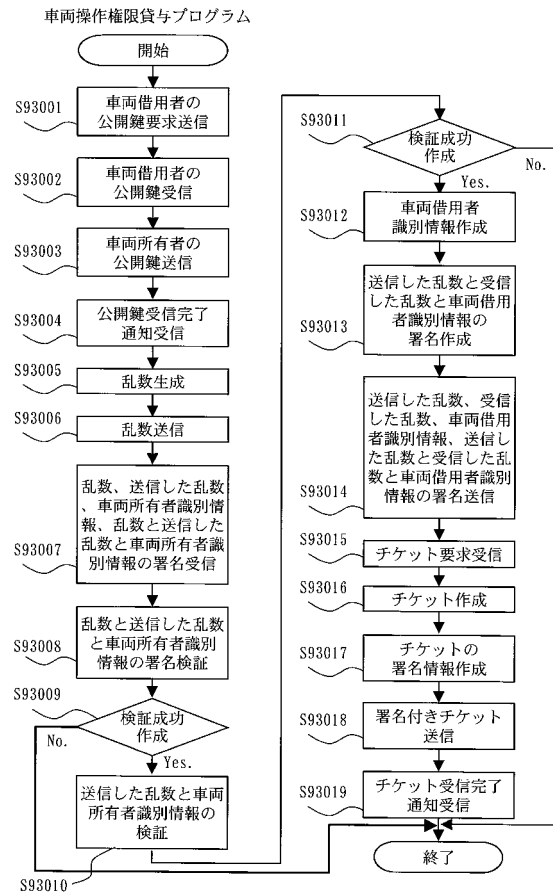
【図 2 6】



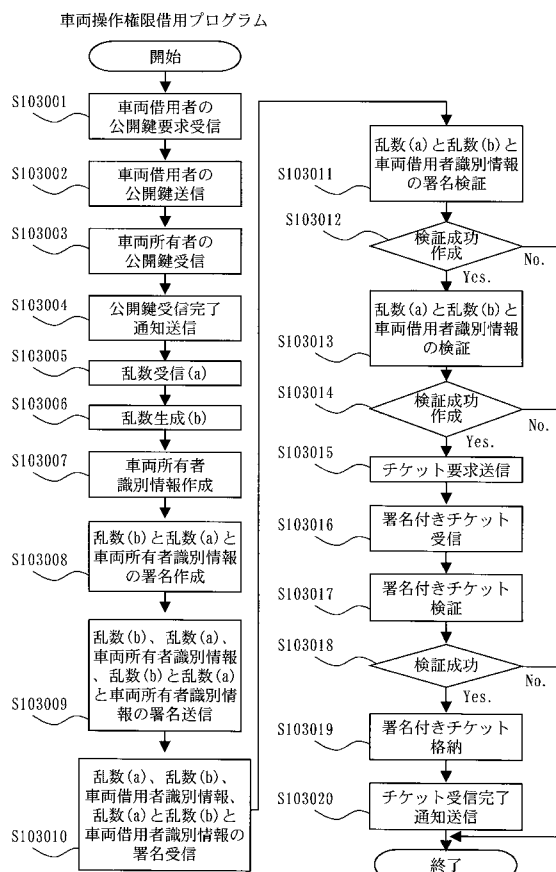
【図 27】



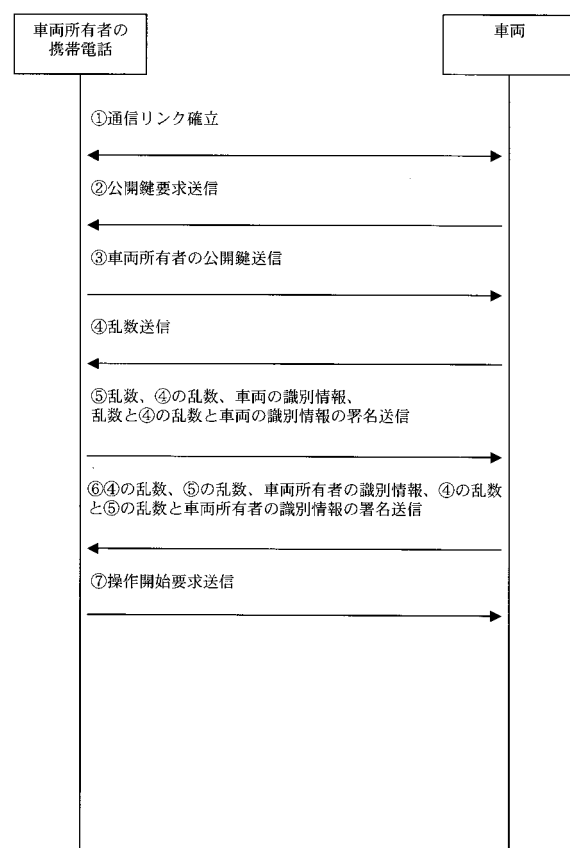
【図 28】



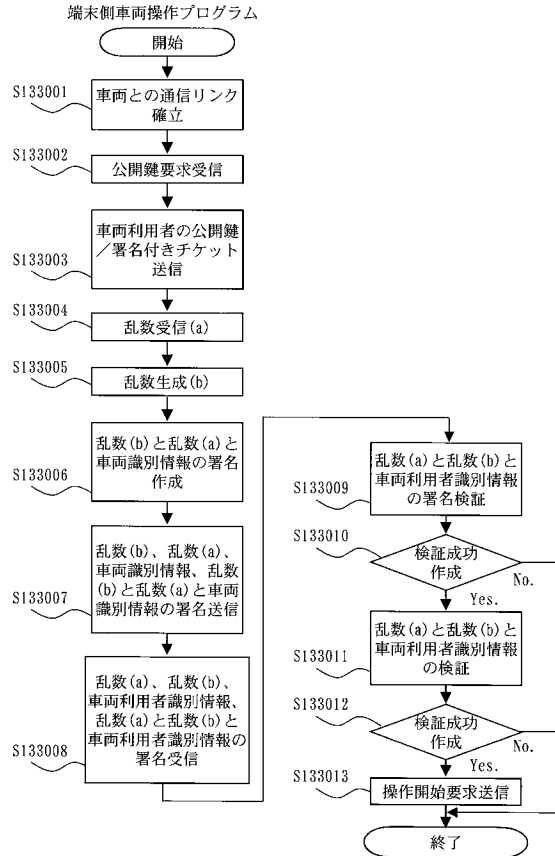
【図 29】



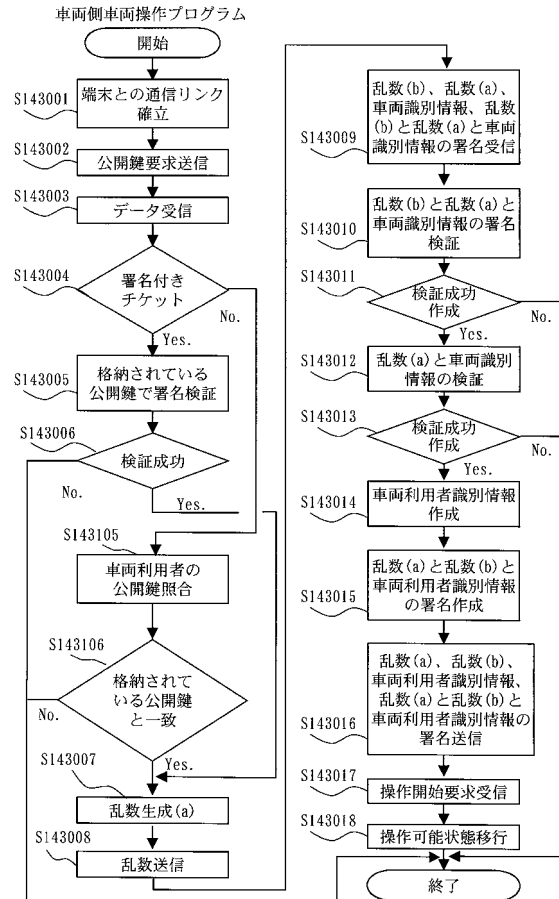
【図 30】



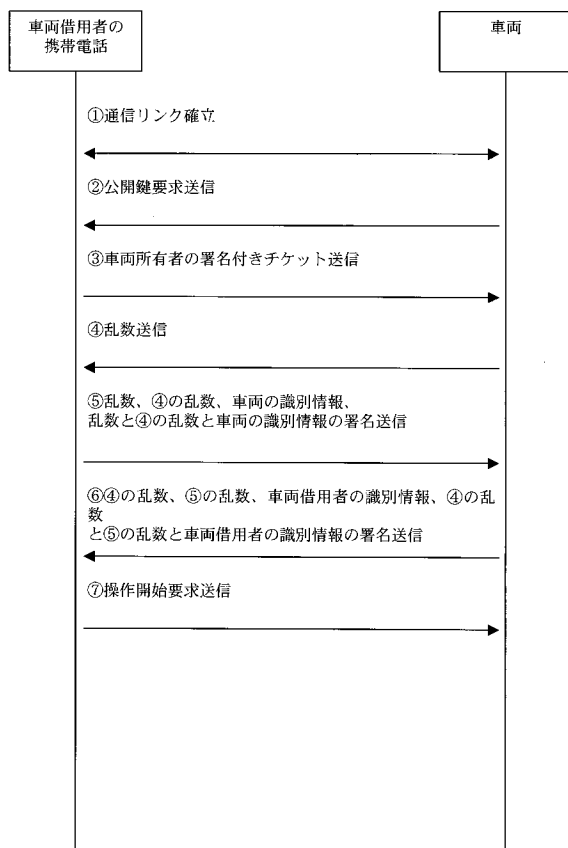
【図 3 1】



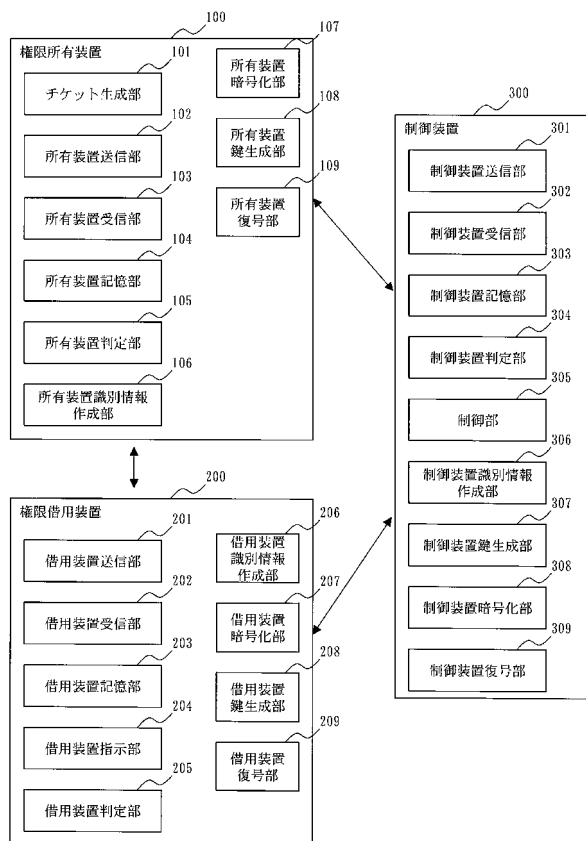
【図 3 2】



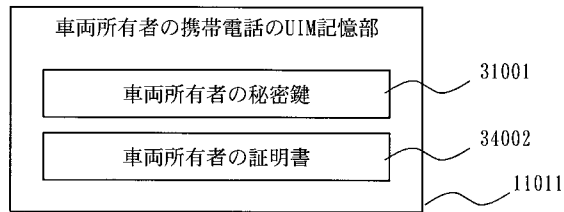
【図 3 3】



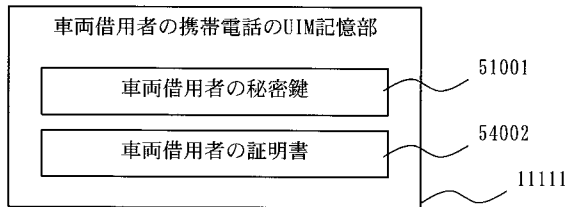
【図 3 4】



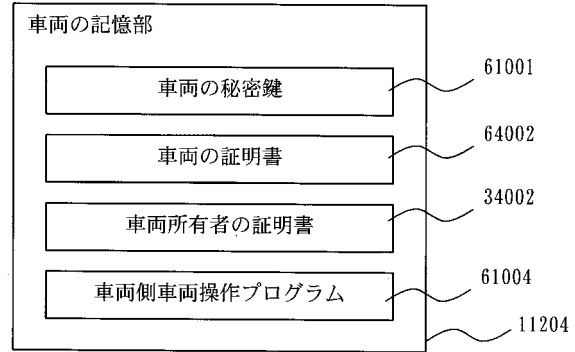
【図 3 5】



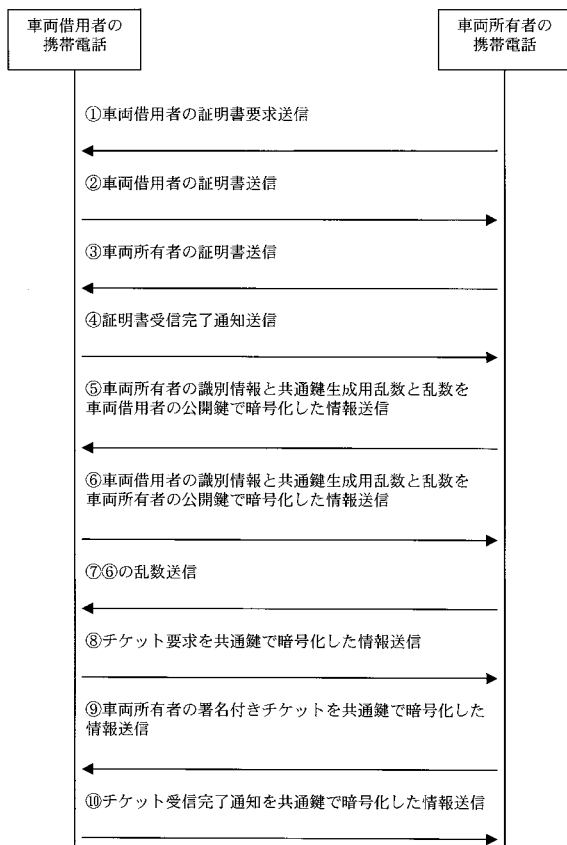
【図 3 6】



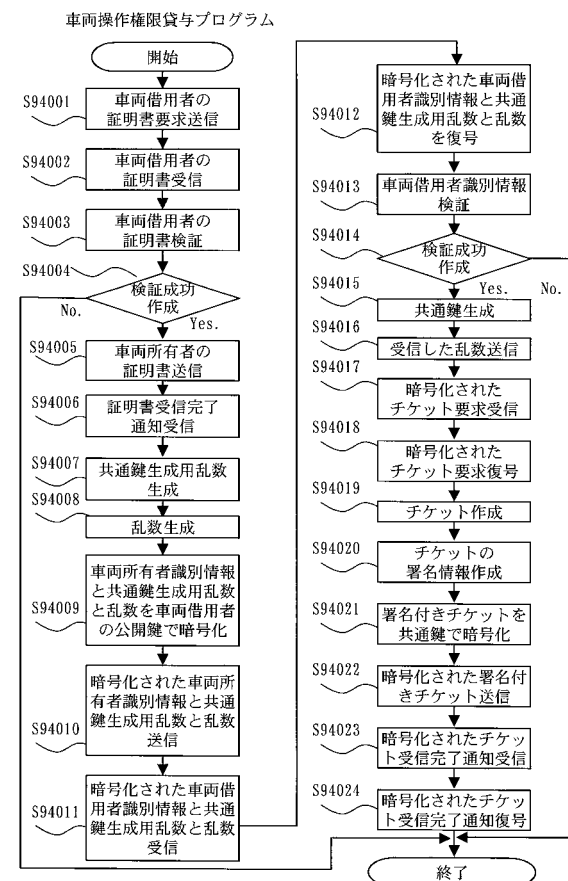
【図 3 7】



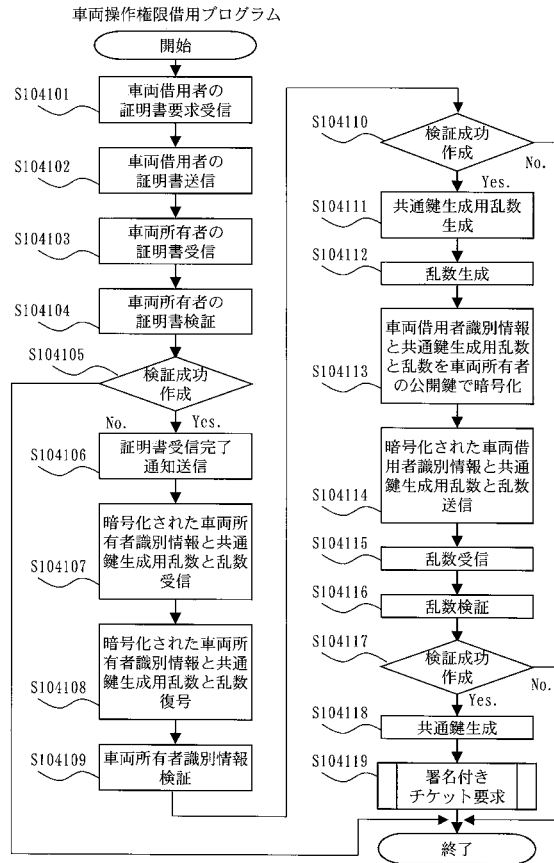
【図 3 8】



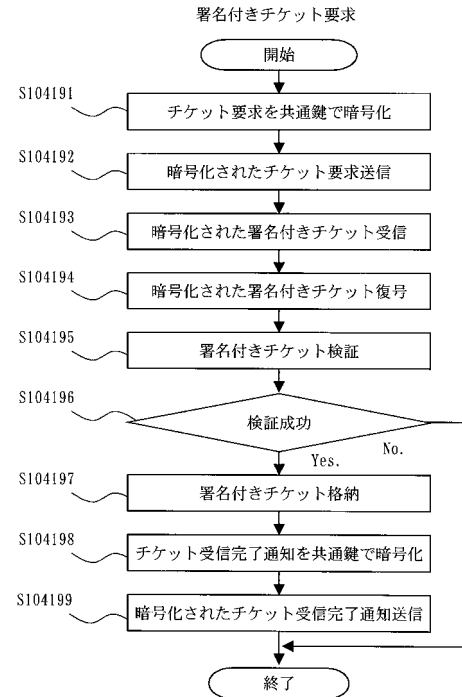
【図 3 9】



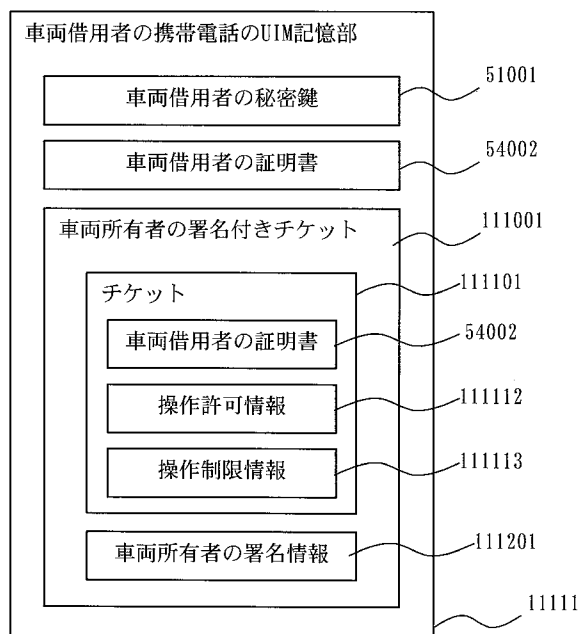
【図 40】



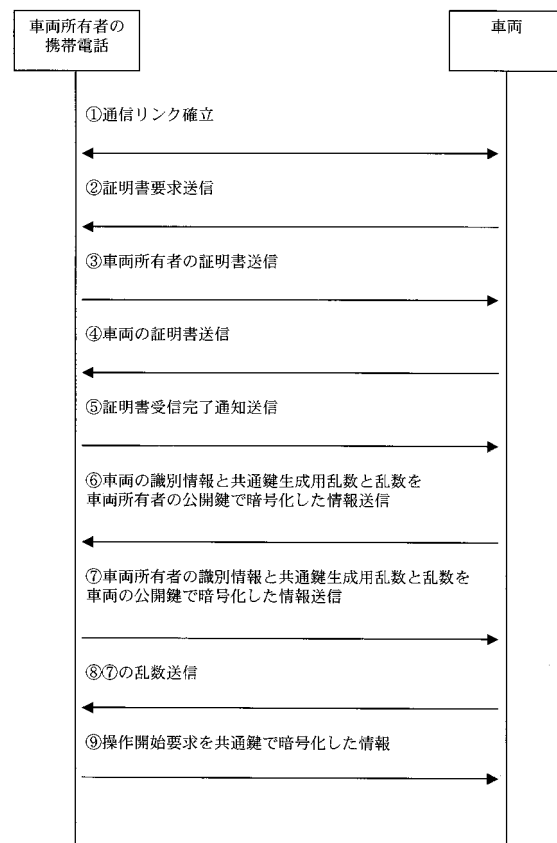
【図 41】



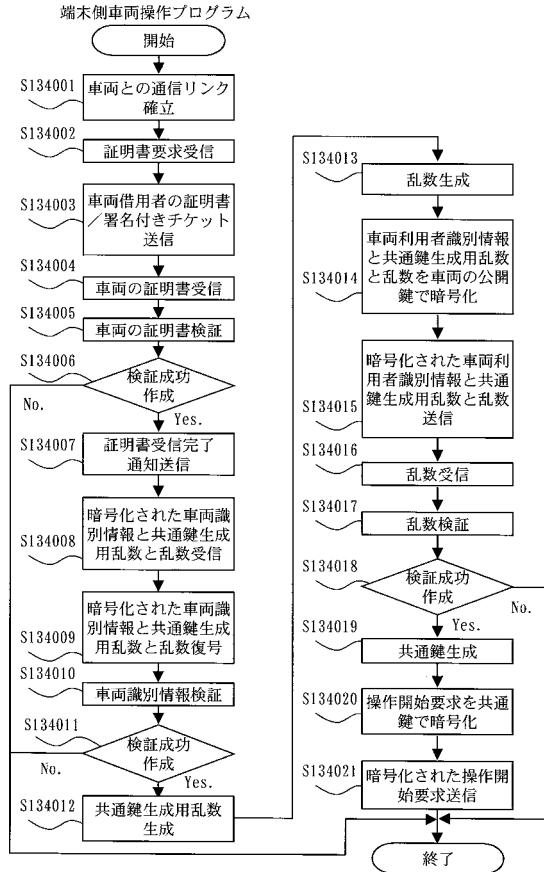
【図 42】



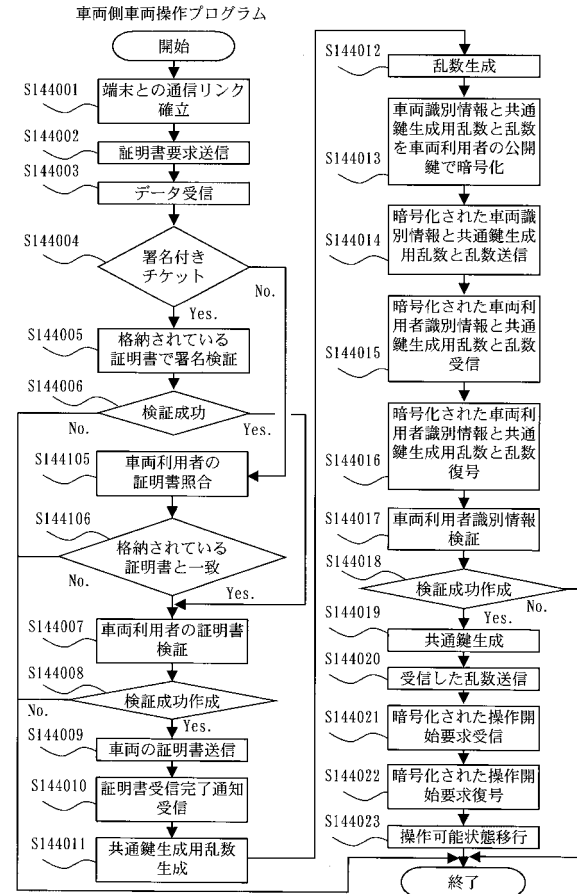
【図 43】



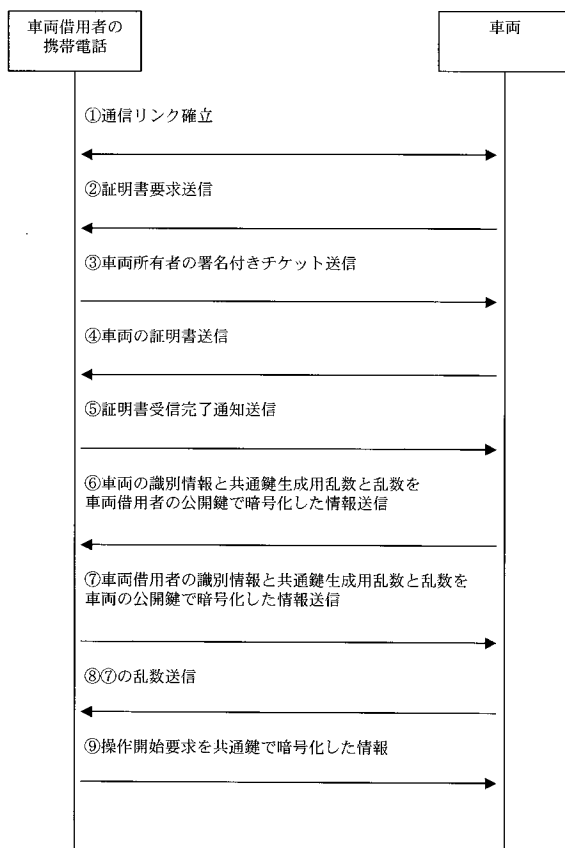
【図 4 4】



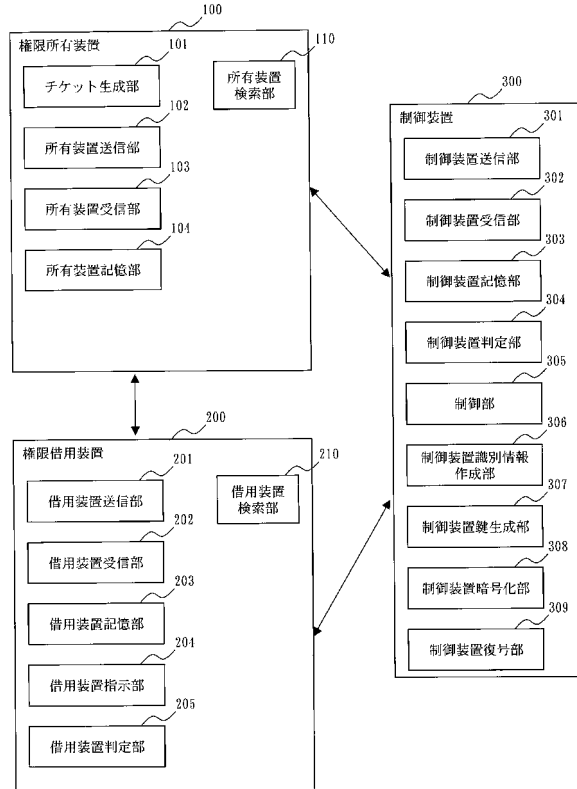
【図 4 5】



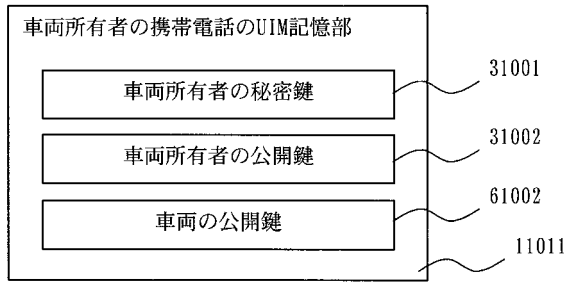
【図 4 6】



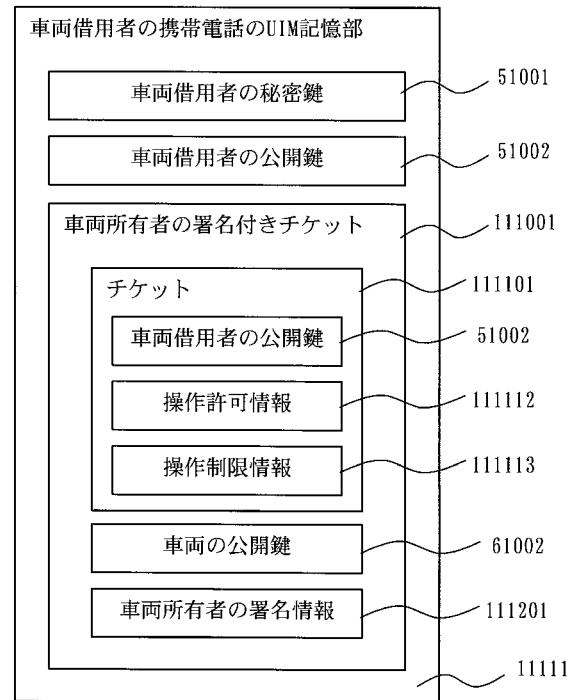
【図 4 7】



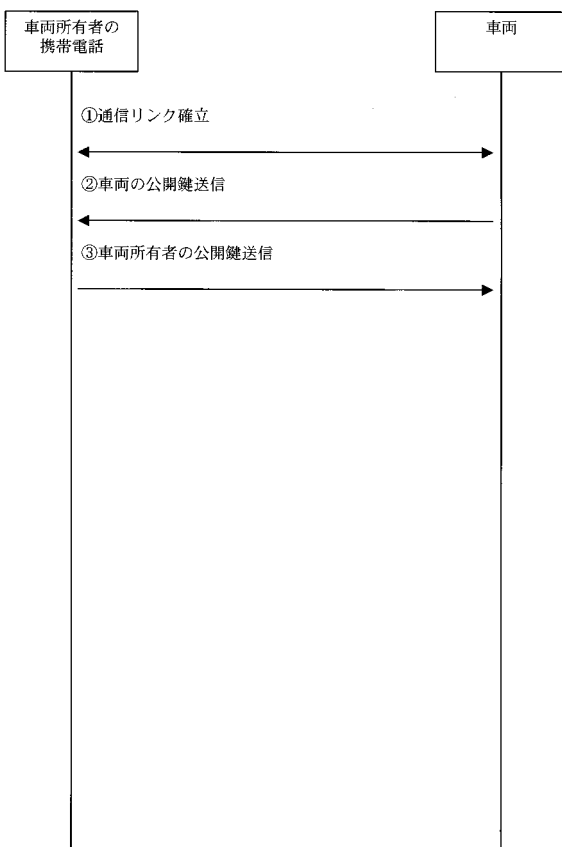
【図 48】



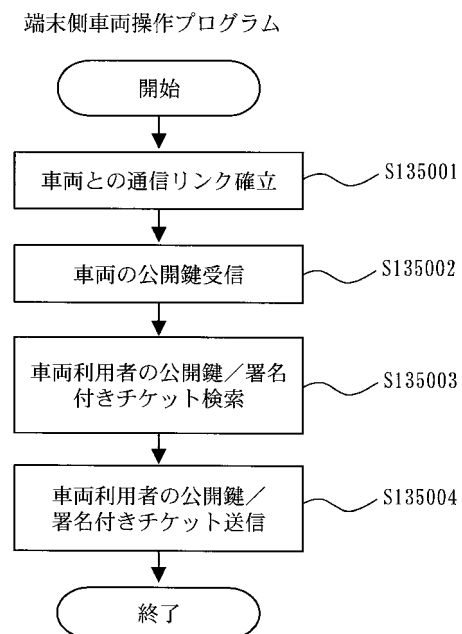
【図 49】



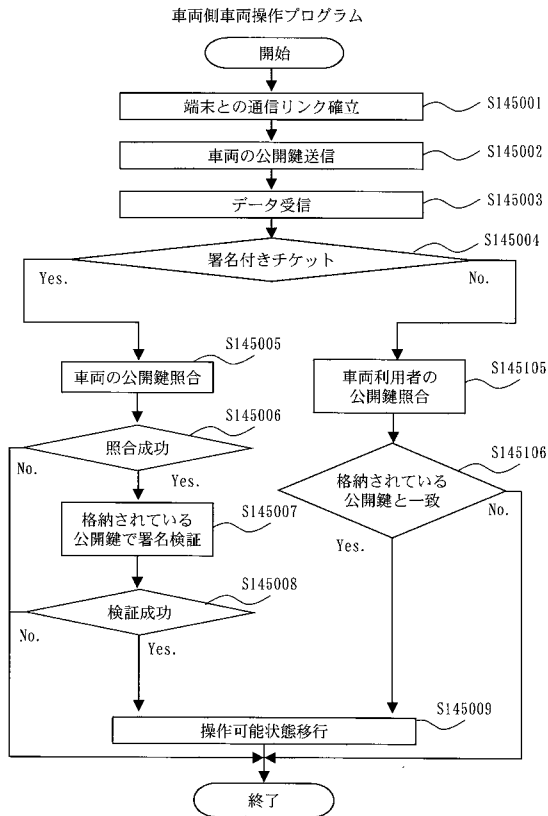
【図 50】



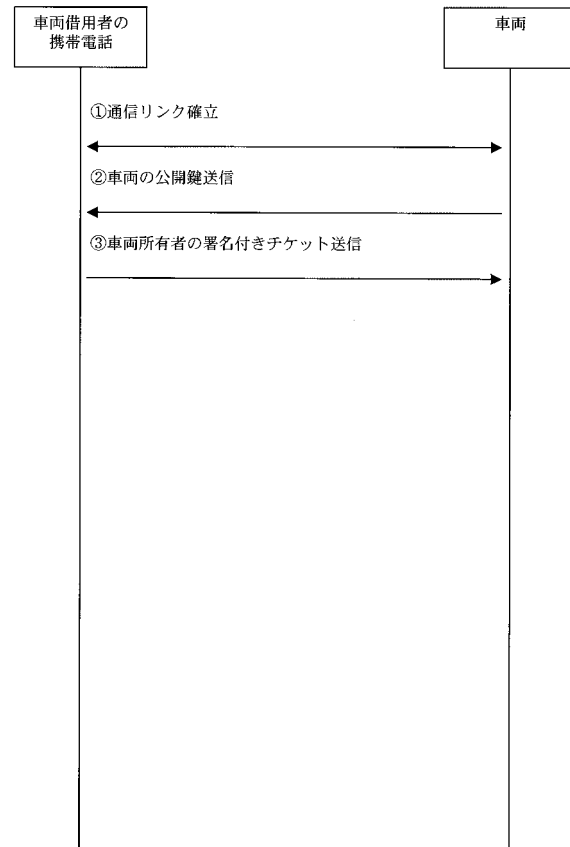
【図 51】



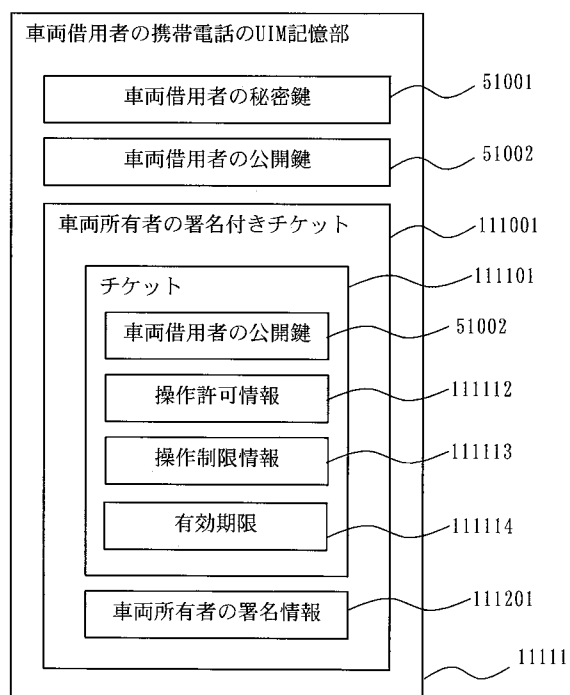
【図 5 2】



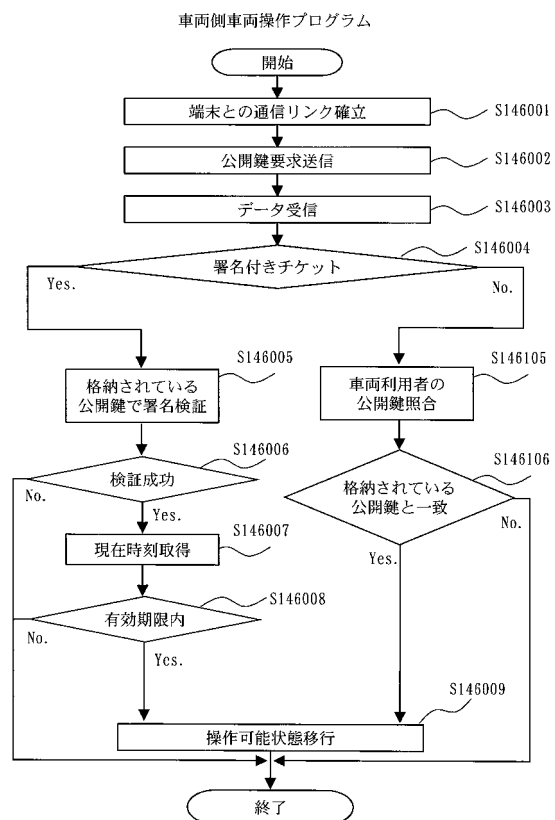
【図 5 3】



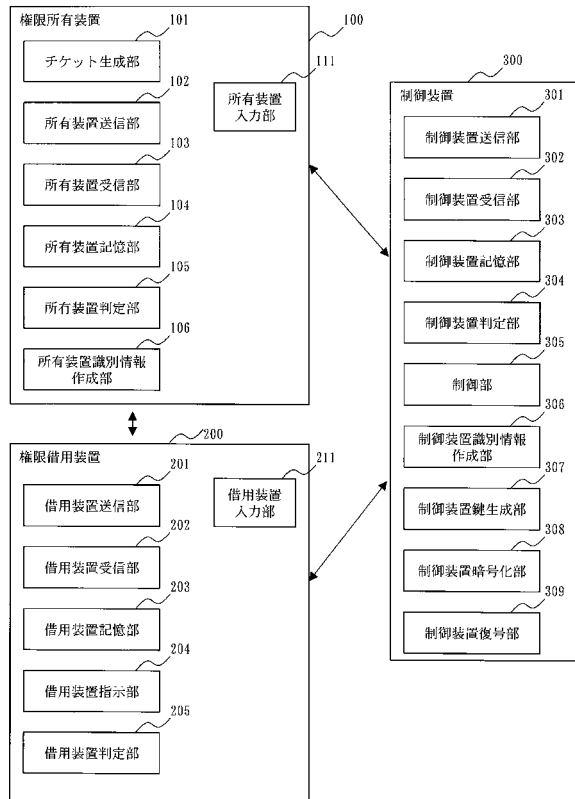
【図 5 4】



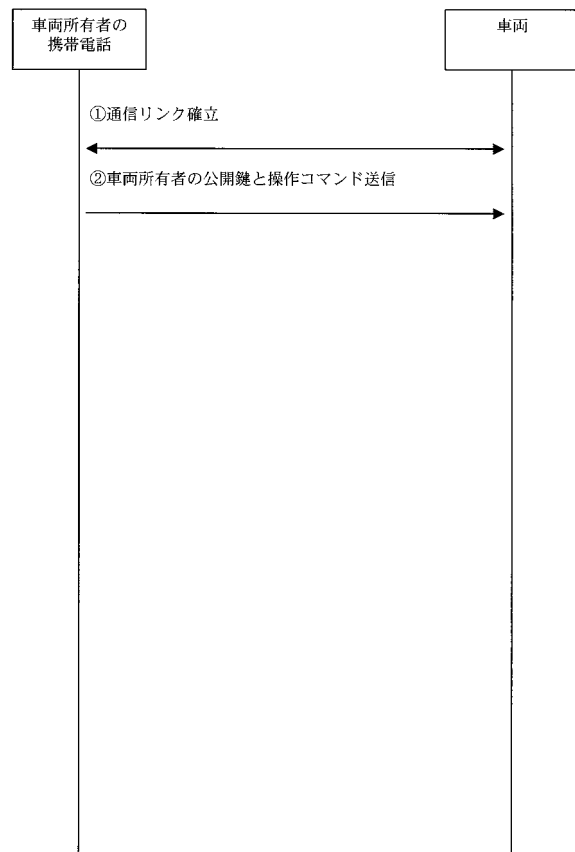
【図 5 5】



【図 56】

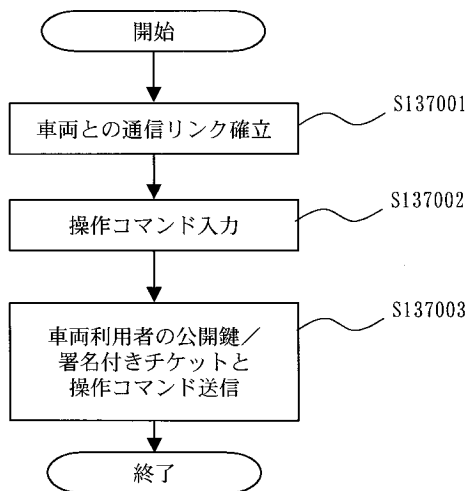


【図 57】



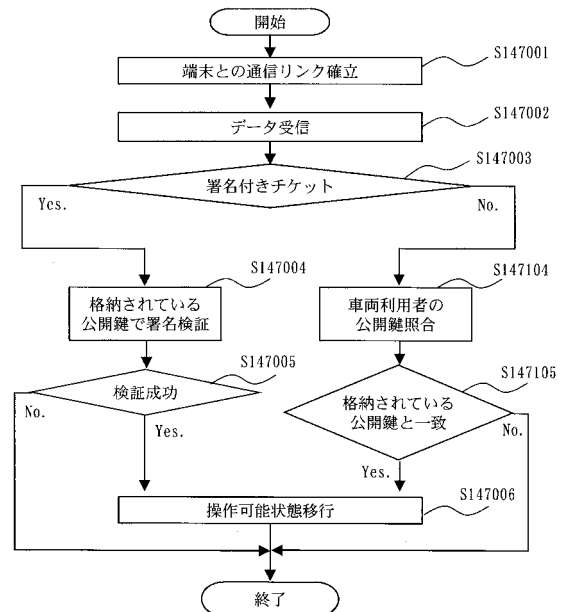
【図 58】

端末側車両操作プログラム

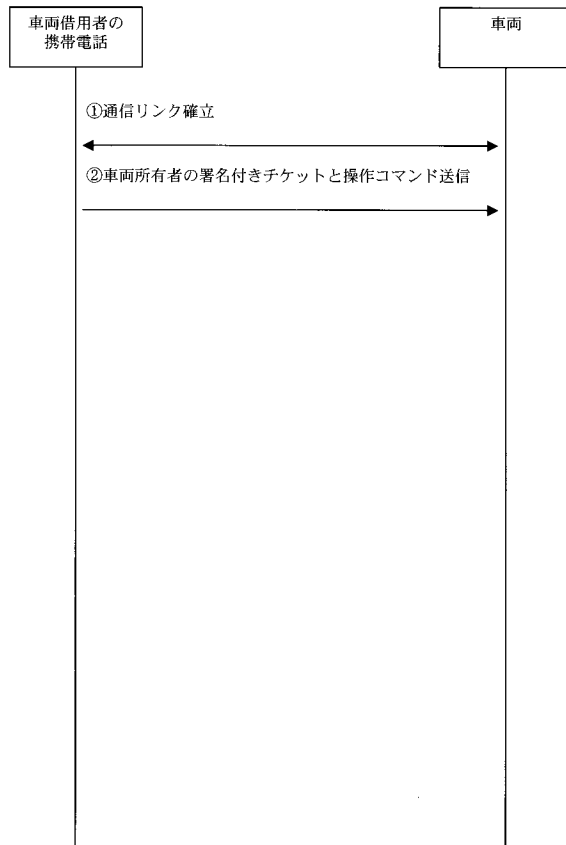


【図 59】

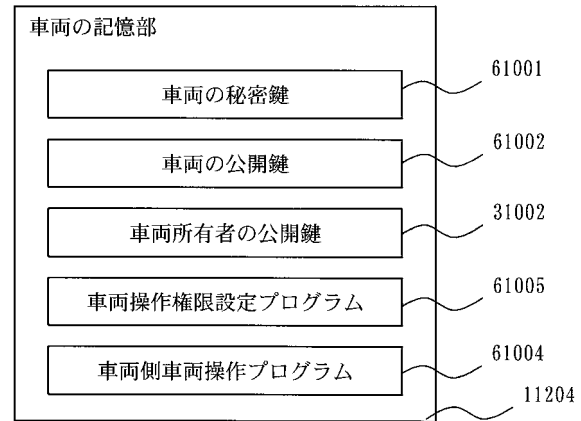
車両側車両操作プログラム



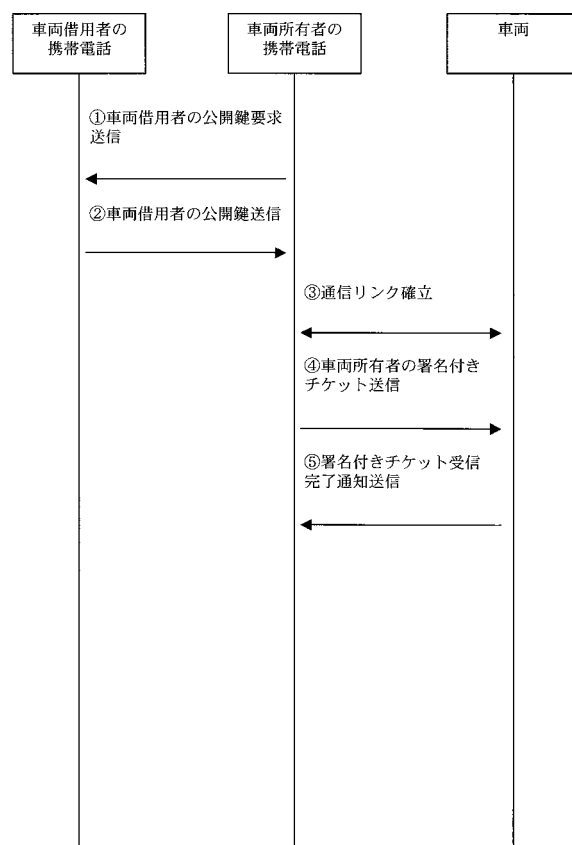
【図 6 0】



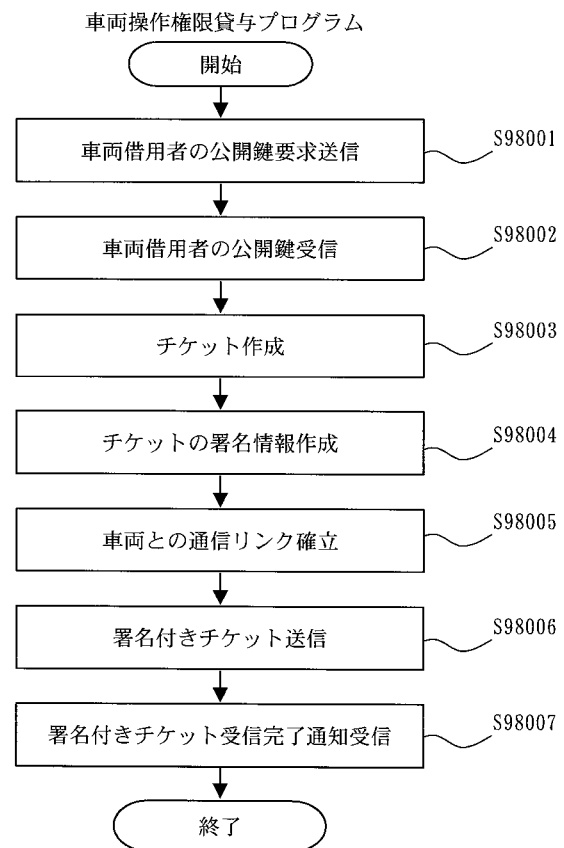
【図 6 1】



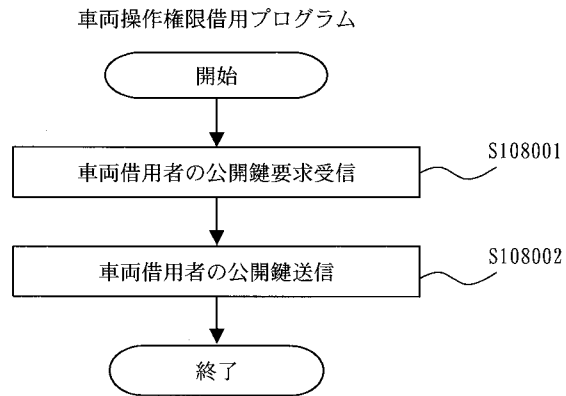
【図 6 2】



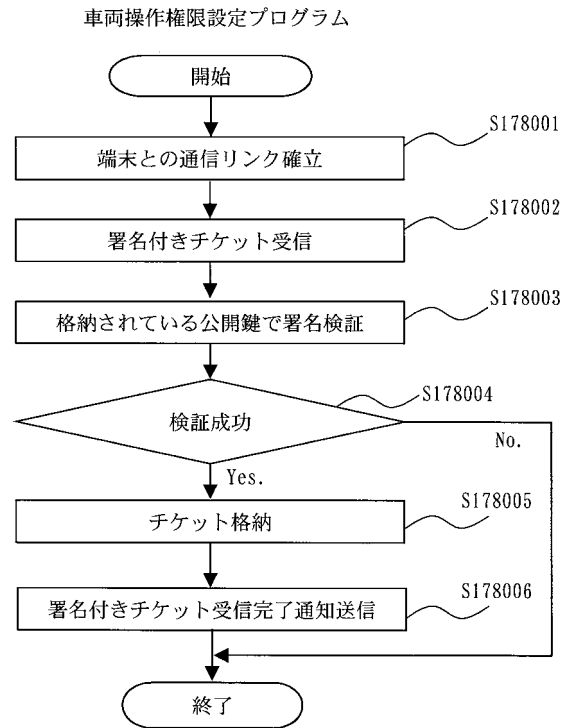
【図 6 3】



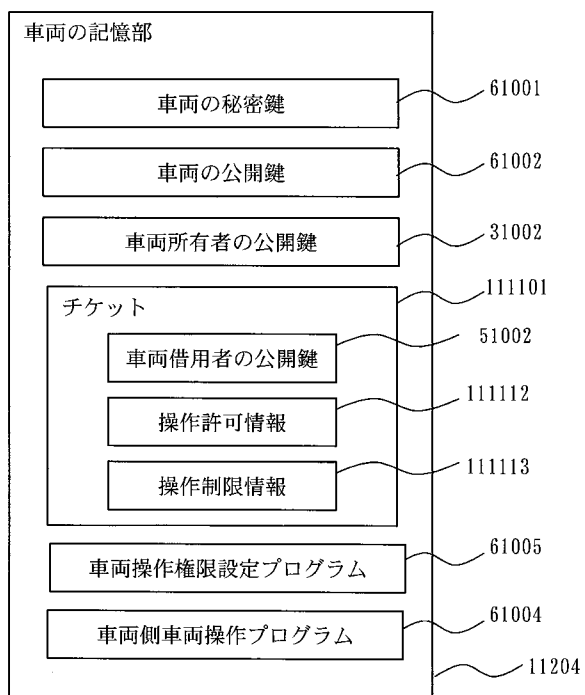
【図 6 4】



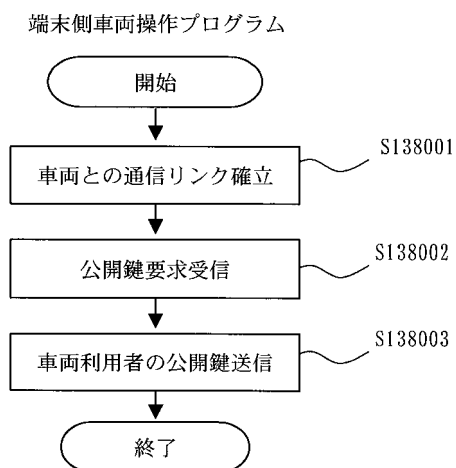
【図 6 5】



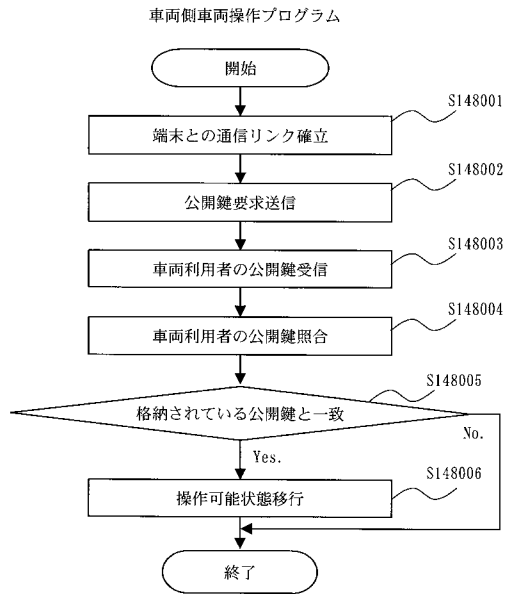
【図 6 6】



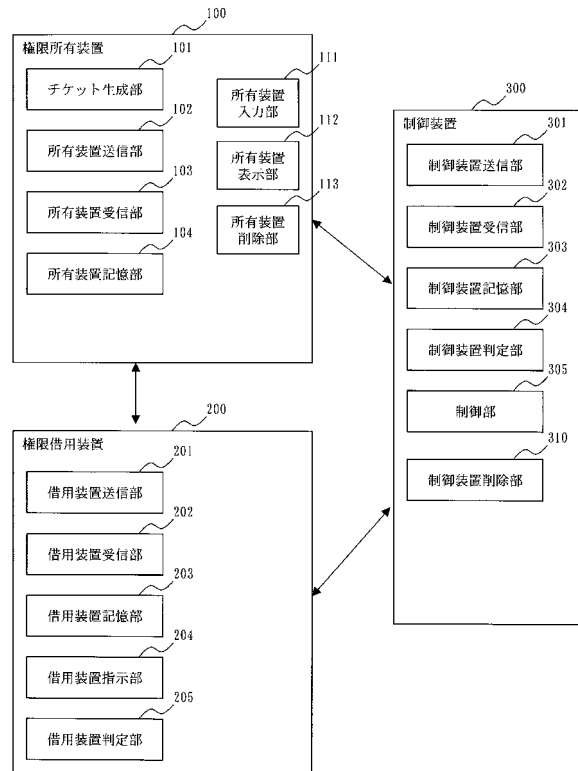
【図 6 7】



【図 68】



【図 69】



フロントページの続き

- (72)発明者 太田 英憲
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 松田 規
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 伊藤 隆
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

審査官 青木 重徳

- (56)参考文献 特開2001-101054 (JP, A)
特開2001-350732 (JP, A)
特開2004-348208 (JP, A)
特開2002-175589 (JP, A)
特開2004-304751 (JP, A)
特開平11-052851 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
H04L 9/32