(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5591076号
(P5591076)

(45)発行日　平成26年9月17日(2014.9.17)　(24)登録日　平成26年8月8日(2014.8.8)

(51)Int.Cl.			F I		
H04W	12/06	(2009.01)	H04W	12/06	
H04W	4/04	(2009.01)	H04W	4/04	１１１
H04L	9/08	(2006.01)	H04W	4/04	１１３
G08G	1/09	(2006.01)	H04L	9/00	６０１Ｂ
			G08G	1/09	Ｈ

請求項の数 15　(全 37 頁)　最終頁に続く

(21)出願番号　特願2010-262391 (P2010-262391)
(22)出願日　平成22年11月25日 (2010.11.25)
(65)公開番号　特開2012-114702 (P2012-114702A)
(43)公開日　平成24年6月14日 (2012.6.14)
審査請求日　平成25年9月5日 (2013.9.5)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100152881
弁理士　山地　博人
(72)発明者　泉　幸雄
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　三澤　学
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】通信装置及び通信方法及びプログラム

(57)【特許請求の範囲】

【請求項１】

配信情報と、前記配信情報の検証に用いられる第二の認証情報とを繰り返し送信するとともに、前記第二の認証情報の検証に用いられる第一の認証情報を繰り返し送信する通信装置であって、

繰り返し到来する送信タイミングごとに、前記第一の認証情報を送信するか、前記第一の認証情報に代えて前記第一の認証情報の識別情報を送信するかを指定する送信対象指定部と、

前記送信対象指定部により前記第一の認証情報の送信が指定された送信タイミングでは、少なくとも前記第一の認証情報を送信し、前記送信対象指定部により前記第一の認証情報の識別情報の送信が指定された送信タイミングでは、前記第一の認証情報の識別情報と前記配信情報と前記第二の認証情報とを対応付けて送信する通信部とを有することを特徴とする通信装置。

【請求項２】

前記通信装置は、更に、

送信タイミングが到来する度に、送信タイミングの到来回数をカウントするカウンタを有し、

前記送信対象指定部は、

前記カウンタのカウンタ値を参照し、Ｎ（Ｎは２以上の任意の整数）回に１回は前記第一の認証情報の送信を指定し、（Ｎ－１）回は前記第一の認証情報の識別情報の送信を指

定することを特徴とする請求項１に記載の通信装置。
【請求項３】
前記通信装置は、更に、
送信タイミングの合間の期間において前記配信情報を受信できる状況にある通信機器を検出するとともに、未検出であった通信機器を新たに検出した場合に、新たな通信機器を検出したことを前記送信対象指定部に通知する機器検出部を有し、
前記送信対象指定部は、
前記機器検出部により新たな通信機器の検出が通知された後に到来する送信タイミングに対して、前記第一の認証情報の送信を指定することを特徴とする請求項１に記載の通信装置。
【請求項４】
前記送信対象指定部は、
送信タイミングが到来した際に前記機器検出部により新たな通信機器の検出が通知されていない場合に、当該送信タイミングに対して、前記第一の認証情報の識別情報の送信を指定することを特徴とする請求項３に記載の通信装置。
【請求項５】
前記機器検出部は、
新たな通信機器を１つ検出した以降は、新たな通信機器を検出する動作を停止することを特徴とする請求項３に記載の通信装置。
【請求項６】
前記送信対象指定部は、
前記機器検出部により新たな通信機器の検出が通知された後であって前記第一の認証情報の識別情報の送信が指定された送信タイミングの次の送信タイミングに対して、前記第一の認証情報の送信を指定することを特徴とする請求項３に記載の通信装置。
【請求項７】
前記送信対象指定部は、
前記機器検出部により新たな通信機器の検出が通知された次の送信タイミングに対して、前記第一の認証情報の送信を指定することを特徴とする請求項３に記載の通信装置。
【請求項８】
前記通信部は、
前記送信対象指定部により前記第一の認証情報の送信が指定された送信タイミングでは、前記配信情報と前記第二の認証情報とを送信することなく、前記第一の認証情報を送信することを特徴とする請求項１に記載の通信装置。
【請求項９】
前記通信部は、
前記送信対象指定部により前記第一の認証情報の送信が指定された送信タイミングでは、前記第一の認証情報と前記配信情報と前記第二の認証情報とを対応付けて送信することを特徴とする請求項１に記載の通信装置。
【請求項１０】
前記通信装置は、
通信機器から、配信情報と、前記配信情報の検証に用いられる第二の認証情報とを受信し、
受信した配信情報のうち所定の条件に合致する配信情報を選択し、選択した配信情報にのみ前記第二の認証情報を用いた検証を行うことを特徴とする請求項１に記載の通信装置。
【請求項１１】
前記通信装置は、
通信機器から、配信情報と、前記配信情報の検証に用いられる第二の認証情報とを受信し、
前記第二の認証情報の検証に用いられる第一の認証情報を保有している場合に、保有し

ている第一の認証情報の有効期限を確認し、有効期限内であれば前記第一の認証情報を用いて前記第二の認証情報の検証を行い、有効期限外であれば前記第一の認証情報を削除することを特徴とする請求項１に記載の通信装置。
【請求項１２】
前記通信装置は、
道路の路側に設置されている路側機に搭載されており、
前記道路を通行する車両に搭載されている通信機器に対して、配信情報を送信することを特徴とする請求項１に記載の通信装置。
【請求項１３】
前記通信装置は、
道路を走行する車両に搭載されており、
前記道路を通行する他の車両に搭載されている通信機器及び前記道路の路側に設置されている路側機に搭載されている通信機器の少なくともいずれかに対して、配信情報を送信することを特徴とする請求項１に記載の通信装置。
【請求項１４】
配信情報と、前記配信情報の検証に用いられる第二の認証情報とを繰り返し送信するとともに、前記第二の認証情報の検証に用いられる第一の認証情報を繰り返し送信するコンピュータが行う通信方法であって、
前記コンピュータが、繰り返し到来する送信タイミングごとに、前記第一の認証情報を送信するか、前記第一の認証情報に代えて前記第一の認証情報の識別情報を送信するかを指定する送信対象指定ステップと、
前記コンピュータが、前記送信対象指定ステップにより前記第一の認証情報の送信が指定された送信タイミングでは、少なくとも前記第一の認証情報を送信し、前記送信対象指定ステップにより前記第一の認証情報の識別情報の送信が指定された送信タイミングでは、前記第一の認証情報の識別情報と前記配信情報と前記第二の認証情報とを対応付けて送信する通信ステップとを有することを特徴とする通信方法。
【請求項１５】
配信情報と、前記配信情報の検証に用いられる第二の認証情報とを繰り返し送信するとともに、前記第二の認証情報の検証に用いられる第一の認証情報を繰り返し送信するコンピュータに、
繰り返し到来する送信タイミングごとに、前記第一の認証情報を送信するか、前記第一の認証情報に代えて前記第一の認証情報の識別情報を送信するかを指定する送信対象指定ステップと、
前記送信対象指定ステップにより前記第一の認証情報の送信が指定された送信タイミングでは、少なくとも前記第一の認証情報を送信し、前記送信対象指定ステップにより前記第一の認証情報の識別情報の送信が指定された送信タイミングでは、前記第一の認証情報の識別情報と前記配信情報と前記第二の認証情報とを対応付けて送信する通信ステップとを実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信装置間で配信情報を送受信するとととともに、配信情報に関連する関連情報を送受信する通信システムに関する。
例えば、車両に搭載された車載器間、車載器と路側に設置された路側機との間で配信情報を送受信するとともに、配信情報の正当性を検証するための認証情報を送受信する通信システムに関する。
【背景技術】
【０００２】
近年、放送型の路車間通信や車車間通信によって、路側に設置された路側機や車両に搭載された車載器から他の車載器に対して、交通渋滞や信号に関わる情報や車両の速度、位

置など走行状態に関する情報、救急車等の緊急車両接近情報、隊列走行時の車両制御情報等（以下、これらをまとめて配信情報という）を送信して、安全運転や効率的な運転に役立てる運転支援システムが検討されている。

【０００３】

図２５は、一般的な運転支援システムの構成図を示す。

路側機は周囲の車載器に配信情報を配信し、同様に車載器は他の車載器に配信情報を配信する。

このようなシステムにおいて、悪意のある利用者が車載器（ＣやＤ）を悪用して、路側機や緊急車両になりすまし、他の車載器に対して偽の情報を配信し、混乱を引き起こしたり、交通事故を引き起こしたりすることが考えられる。

従って、情報を配信している送信側、つまり、情報を配信している路側機や車載器の正当性を受信側が確認できるセキュリティ手段が必要となる。

このような対策の例として、特許文献１に公開鍵暗号アルゴリズムのデジタル署名を用いた路車間通信システムが記載されている。

以下、図２６と図２７を用いて、特許文献１記載のシステムを説明する。

【０００４】

特許文献１のシステムでは、認証局が路側機に対して公開鍵証明書Ａを発行する。

路側機は、公開鍵証明書Ａを発行した認証局の公開鍵証明書Ｂを車載器に配信する。

また、路側機は、図２７に示すように配信する情報のデジタル署名を生成して、配信する情報、そのデジタル署名、及びその署名を検証できる公開鍵証明書Ａを車載器に配信する。

車載器は受信した公開鍵証明書Ａを認証局の公開鍵証明書Ｂで検証するとともに、配信された情報のデジタル署名を公開鍵証明書Ａで検証することにより、正当な路側機から配信された情報であることを確認する。

特許文献１では、路車間通信システムを対象に記述されているが、車車間通信でも同様のセキュリティ対策は適用でき、緊急車両になりすました車載器から配信された情報や証明書を検証することで、一般の車載器が緊急車両になりすましていることが検出できる。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００７－８８７３７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、上記のような従来のシステムでは、送信側である路側機は、配信する情報の他に受信側が送信側の正当性を確認する認証情報を配信する必要がある。

上記システムでの認証情報は、認証局の公開鍵証明書Ｂ、配信情報の署名と路側機の公開鍵証明書Ａである。

認証局の証明書Ｂは、その数が少ないため、あらかじめ受信側である車載器に格納しておくという手段をとることができるが、路側機の数は非常に多数であり、あらかじめ格納しておくことは現実的ではない。

また、車車間通信を含めた場合、受信側である車載器に送信側であるすべての路側機と車載器の証明書をあらかじめ格納しておくことはできない。

従って、配信のたびに送信側の証明書を、配信情報とその署名と共に送信する必要がある。

ここで、公開鍵暗号アルゴリズムとして、鍵長１０２４ｂｉｔのＲＳＡ（登録商標）（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ）を用いたデジタル署名を考える。

公開鍵証明書には、公開鍵とそれに対する認証局の署名が含まれるので、送信側の証明書は、送信側の公開鍵（１０２４ｂｉｔ）と認証局の署名（１０２４ｂｉｔ）が少なくとも含まれる。

また、配信情報の署名は１０２４ｂｉｔとなる。
これより、配信情報以外に少なくとも３０７２ｂｉｔの認証情報が必要となる。
また、受信側は受信した公開鍵証明書の検証と配信情報の署名検証を実施するため、高い処理能力が必要である。
さらに、配信情報の署名検証を実施した後、配信情報を利用する構成になっているため、受信したすべての配信情報の署名検証をしなければならないので、高い処理能力が必要であり、無駄が多い。

【０００７】
この発明は、上記のような課題を解決することを主な目的の一つとしており、配信情報の送受信に付随して送受信されるデータのデータ量を削減することを主な目的とする。

【課題を解決するための手段】

【０００８】
本発明に係る通信装置は、
配信情報を繰り返し送信するとともに、配信情報に関連する関連情報を繰り返し送信する通信装置であって、
繰り返し到来する送信タイミングごとに、前記関連情報を送信するか、前記関連情報に代えて前記関連情報の識別情報を送信するかを指定する送信対象指定部と、
前記送信対象指定部により前記関連情報の送信が指定された送信タイミングでは、少なくとも前記関連情報を送信し、前記送信対象指定部により前記関連情報の識別情報の送信が指定された送信タイミングでは、前記関連情報の識別情報と前記配信情報とを対応付けて送信する通信部とを有することを特徴とする。

【発明の効果】

【０００９】
本発明によれば、関連情報の送信に代えて、関連情報よりもデータ量が少ない関連情報の識別情報を送信するので、送信するデータ量を削減することができる。

【図面の簡単な説明】

【００１０】
【図１】実施の形態１に係る通信装置の構成例を示す図。
【図２】実施の形態１に係る通信装置の送信時の処理を示すフローチャート図。
【図３】実施の形態１に係る通信データの構成例を示す図。
【図４】実施の形態１に係る通信装置の受信時の処理を示すフローチャート図。
【図５】実施の形態１に係る第１の認証情報の記憶方法の一例を示す図。
【図６】実施の形態２に係る通信装置の送信時の処理を示すフローチャート図。
【図７】実施の形態２に係る通信データの構成例を示す図。
【図８】実施の形態２に係る通信装置の受信時の処理を示すフローチャート図。
【図９】実施の形態３に係る通信装置の構成例を示す図。
【図１０】実施の形態３に係る通信装置の送信時の処理を示すフローチャート図。
【図１１】実施の形態３に係る通信データの構成例を示す図。
【図１２】実施の形態３に係る通信装置の受信時の処理を示すフローチャート図。
【図１３】実施の形態３に係るＩＤ記録処理とＩＤ比較処理の具体例を示す図。
【図１４】実施の形態４に係る通信装置の送信時の処理を示すフローチャート図。
【図１５】実施の形態４に係る通信データの構成例を示す図。
【図１６】実施の形態４に係る通信装置の受信時の処理を示すフローチャート図。
【図１７】実施の形態５に係る通信装置の構成例を示す図。
【図１８】実施の形態５に係る通信装置の送信時の処理を示すフローチャート図。
【図１９】実施の形態５に係る通信装置の受信時の処理を示すフローチャート図。
【図２０】実施の形態５に係るＩＤ記録処理とＩＤ比較処理の具体例を示す図。
【図２１】実施の形態１に係る回数Ｎの決定方法の一例を示す図。
【図２２】実施の形態１に係る回数Ｎの決定方法の一例を示す図。
【図２３】実施の形態２に係る回数Ｎの決定方法の一例を示す図。

【図２４】実施の形態１に係る通信装置の構成例を示す図。
【図２５】従来技術を説明する図。
【図２６】従来技術を説明する図。
【図２７】従来技術を説明する図。
【図２８】実施の形態１～５に係る通信装置のハードウェア構成例を示す図。
【発明を実施するための形態】
【００１１】
実施の形態１.
実施の形態１～５では、配信情報を繰り返し送受信するとともに、配信情報の正当性を検証するために用いる第二の認証情報と、第二の認証情報の正当性を検証するための第一の認証情報（関連情報の例）を繰り返し送受信する路車間・車車間通信システムを説明する。
また、本実施の形態では、あらかじめ決められた通信回数Ｎ（Ｎは２以上の任意の整数）に対して、１回は第一の認証情報のみを送信し（配信情報は送信しない）、残りのＮ－１回は配信情報と第二の認証情報を送信する例を説明する。
【００１２】
図１は、本実施の形態に係る通信装置１の構成例を示す図である。
路車間及び車車間通信の場合、路側に設置される路側機は車両に搭載される車載器と、車載器は路側機及び他の車載器と通信する。
本実施の形態では、路側機と車載器を通信装置１として記述する。
また、通信装置１にとっての他の通信装置２は通信機器の例である。
【００１３】
通信装置１は配信情報を他の通信装置２に送信し、他の通信装置２が送信した配信情報を受信する。
通信装置１は、他の通信装置２に送信する配信情報を生成し、他の通信装置２から受信した配信情報を処理する配信情報処理部３を有する。
また、通信装置１は、受信側が送信側の正当性を確認する認証情報を、配信情報やあらかじめ格納されている鍵情報を用いて生成・検証する認証情報処理部４を有する。
また、通信装置１は、他の通信装置２とＤＳＲＣ（Ｄｅｄｉｃａｔｅｄ　Ｓｈｏｒｔ　Ｒａｎｇｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）や無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの無線通信を行う通信部５を有する。
【００１４】
配信情報処理部３は、自身のデータ送信回数をカウントするカウンタ６を内部に持ち、繰り返し到来する送信タイミングごとにカウンタ６のカウンタ値を参照して、第一の認証情報を送信するか、第一の認証情報に代えて第一の認証情報の識別情報を送信するかを指定する。
配信情報処理部３は、送信対象指定部の例である。
認証情報処理部４には、認証情報処理部４が読み書き可能なメモリである記憶部７が設けられ、認証情報を生成・検証するために使用される鍵情報が格納されている。
鍵情報は、例えば公開鍵アルゴリズムによるデジタル署名を適用した場合は、認証局が発行した公開鍵証明書や公開鍵証明書に含まれる公開鍵に対応する秘密鍵、認証局の公開鍵証明書などであり、共通鍵アルゴリズムを適用した場合は通信で使用する共通鍵などである。
なお、図示していないが、通信装置１は現在の位置情報、日付や時間を表す日時情報が、搭載されている路側機や車両から入力されている。
これらは、路側機や車両に設置されているＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）受信装置、ジャイロスコープや時計などで生成される。
【００１５】
また、車両に搭載される通信装置１では、例えば図２４に示すように、図１に示す各構成要素がナビゲーション装置７０と車載器８０とに分離されて配置されていてもよい。

図２４（ａ）は、認証情報処理部４が車載器８０に配置されている構成を示し、図２４（ｂ）は、認証情報処理部４がナビゲーション装置７０に配置されている構成を示す。
ナビゲーション装置７０で車載器通信部７１が設けられ、車載器８０にはナビ通信部８１が設けられ、ナビゲーション装置７０と車載器８０の間の通信が可能である。

【００１６】

次に図２と図３を用いて、通信装置１のデータ送信時の処理フローを説明する。
図２はデータ送信時の処理フロー図であり、図３は通信データの構成図である。

【００１７】

通信装置１の電源投入時又は送信タイミングの到来時に、配信情報処理部３はカウンタ６のカウンタ値を確認する（Ｓ１００）。
本実施の形態では、通信装置１に電源が入った直後のカウンタの初期値は１で、その後送信する度にカウントアップしていくカウンタとしている。
カウンタ値が１の場合、通信装置１の配信情報処理部３は、第一の認証情報を送信すると決定し（送信対象指定ステップ）、認証情報処理部４から第一の認証情報を取得する（Ｓ１０１）。
この時、認証情報処理部４は、第一の認証情報を記憶部７に保持している場合は生成する必要がないが、保持していない場合、第一の認証情報を生成して配信情報処理部３に出力する。
第一の認証情報は、例えば、公開鍵アルゴリズムによるデジタル署名の場合は、当該通信装置１の公開鍵証明書などであり、この場合生成する必要はない。
また、共通鍵アルゴリズムの場合は、一時的に利用するセッション鍵を共通鍵で暗号化したセッション鍵情報やセッション鍵にメッセージ認証コードを追加したものを共通鍵で暗号化したセッション鍵情報などであり、この場合はセッション鍵情報を生成する必要がある。
また、第一の認証情報を一意に識別する第一の認証情報の識別情報や第一の認証情報が有効である期間を示す有効期限が第一の認証情報に含まれていてもよい。
そして、通信データに配信情報を含むか否かを表す情報であるデータ識別情報２１に“配信情報なし”を設定し（Ｓ１０２）、図３（ａ）に示す１回目の構成にて通信データを通信部５から送信する（Ｓ１０３）（通信ステップ）。

【００１８】

一方、Ｓ１０１の判断においてカウンタ値が１以外であった場合は、配信情報処理部３は、第一の認証情報に代えて第一の認証情報の識別情報を送信することを決定し（送信対象指定ステップ）、配信情報を生成する（Ｓ１０４）。
そして、生成した配信情報を認証情報処理部４に入力する。
認証情報処理部４では、記憶部７の鍵情報と第一の認証情報を利用して、第二の認証情報を生成する（Ｓ１０５）。
第二の認証情報は、例えば公開鍵アルゴリズムの場合は、通信装置１の秘密鍵によって生成された配信情報のデジタル署名などであり、共通鍵アルゴリズムの場合、セッション鍵によって生成されたメッセージ認証コードなどがある。
そして、認証情報処理部４は、第二の認証情報の生成に利用した第一の認証情報を一意に識別する第一の認証情報の識別情報を配信情報処理部３に応答する（Ｓ１０６）。
第一の認証情報の識別情報は、第一の認証情報を一意に識別できればよく、公開鍵証明書に含まれるＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）や、ハッシュ関数を用いて算出した証明書のハッシュ値（ダイジェスト）やその一部、セッション鍵情報に含まれるＩＤ、セッション鍵のダイジェストやその一部でもよい。
なお、第一の認証情報の識別情報が証明書のダイジェストである場合、通信装置１は、通信装置１の公開鍵証明書が格納された際に生成して記憶部７に保持しておけば、通信時に生成する必要がなく、通信時の処理の負荷を減少させることができる。
この場合、証明書格納時や電源投入後の通信前に配信情報処理部３が認証情報処理部４から取得して保持して、その情報を用いて通信データを構成するようにしてもよい。

そして、配信情報処理部３は、データ識別情報２１に“配信情報あり”を設定し（Ｓ１０７）、図３（ｂ）に示す２回目の構成で通信データを通信部５から送信する（Ｓ１０３）。

【００１９】

配信情報処理部３は、通信データを送信後、カウンタ値があらかじめ決められた通信回数Ｎに達しているか否かを確認する（Ｓ１０８）。

通信回数Ｎは、通信装置の通信フレーム間隔、通信装置で必要な配信情報の時間間隔、対応するシステムの特性などから決められる。

また、適用するシステムに依存して通信回数Ｎを無限大、すなわち一度第一の認証情報を送信後、常にその情報を用いるようにしてもよい。

【００２０】

なお、通信回数Ｎの決定方法としては、図２１及び図２２に示す方法が考えられる。

図２１は、路側機の場合に、路側機の通信エリア半径Ｌ、車両の速度Ｖ、配信情報の受信のための最低距離Ｒ、送信周期Ｆから通信回数Ｎを決定する例を示している。

なお、図２１では、通信回数Ｎを２５回又は２０回以下とする例を示しているが、通信回数Ｎは例えば３～１０回程度でもよい。

また、図２２は、配信情報の分割回数＋１を通信回数Ｎとする例を示している。

図２２では、１つの配信情報をＭ（Ｍは２以上の任意の整数）分割して送信するケースを示しており、この場合には、配信情報がＭ回にわたって送信されるので、第一の認証情報の１回の送信を加えて、データ送信の機会が（Ｍ＋１）回となる。

つまり、図２２では、通信回数Ｎ＝（Ｍ＋１）回となる。

なお、通信回数Ｎは、図２１及び図２２に示した以外の方法によって決定してもよい。

【００２１】

図２のＳ１０８の判断において、カウンタ値が通信回数Ｎに達していなければ、配信情報処理部３は、カウンタ値をカウントアップし（Ｓ１０９）、カウンタ値が通信回数Ｎに達していればカウンタ値を初期値に戻す（Ｓ１１０）。

このようにして、図３に示す通信データが送信される。

なお、図示していないが、システムに応じて、通信データや配信情報を暗号化して送信してもよい。

【００２２】

次に図４を用いて通信装置１の受信時のフローについて説明する。

図４は受信時の処理フロー図である。

【００２３】

通信装置１は、通信部５によって通信データを受信する（Ｓ１５０）。

そして、通信部５は通信データを配信情報処理部３に送り、配信情報処理部３は通信データ内のデータ識別情報２１を確認する（Ｓ１５１）。

データ識別情報２１が“配信情報なし”の場合、通信データに含まれている第一の認証情報２０を認証情報処理部４に送り、認証情報処理部４は、第一の認証情報２０が記憶部７に格納されていることを確認する（Ｓ１５２）。

第一の認証情報２０が記憶部７に保有されている場合は何もしないで受信処理を終了する。

保有していない場合、認証情報処理部４は、記憶部７にあらかじめ記録された鍵情報を用いて第一の認証情報２０を検証する（Ｓ１５３）。

検証は、例えば、公開鍵アルゴリズムの場合、あらかじめ記録されている認証局の公開鍵証明書を用いて受信した証明書の署名検証、あらかじめ記録されているＣＲＬ（証明書失効リスト）の検索などである。

共通鍵アルゴリズムの場合、あらかじめ記録されている共通鍵を用いた復号やメッセージ認証コードの検証、復号結果内のパディング値の確認などである。

また、第一の認証情報２０に有効期限が設けられている場合、現在の日時と比較することで、その有効期限を確認し、期限内であれば上記と合わせて正当と判断し、期限が切れ

ていたらその第一の認証情報は削除する。
そして、検証の結果を判断し（Ｓ１５４）、第一の認証情報２０の正当性が確認できたら、第一の認証情報２０を記憶部７に格納する（Ｓ１５５）。
この際、必要に応じて第一の認証情報２０の識別情報を作成して第一の認証情報２０と共に記録する。
第一の認証情報２０に、第一の認証情報の識別情報が含まれている場合はその情報を共に記録する。
一方、第一の認証情報２０の正当性が確認できない場合、第一の認証情報を破棄する（Ｓ１５６）。

【００２４】
ここで、図５に記憶部７における第一の認証情報２０の記憶方法の例を示す。
図５の構成では、第一の認証情報２０と、その識別情報２４、第一の認証情報を使用した日付２５、第一の認証情報を使用した回数２６を記録している。
また、図示していないが、第一の認証情報２０を受信した日付や第一の認証情報２０を検証した日付を記録してもよい。
使用した日付２５は、記憶部７の容量が限界に達したとき、新しい第一の認証情報を記録するために、一番古い日付の情報を検索して、上書きや削除するために使用することができる。
これにより、記憶部７を有効に使用することができる。
また、使用した回数は、前述と同様に、記憶部７の容量が限界に達したとき、新しい第一の認証情報を記録するために、使用回数が低いものを上書きや削除し、記憶部７の空き記憶量を増やすことができる。
これらの項目は、システムや使用する暗号アルゴリズムに応じて省略してもよい。

【００２５】
次に、受信した通信データのデータ識別情報２１が“配信情報あり”の場合、配信情報処理部３は暗号化されていない部分の配信情報２２、すなわち全部もしくは一部の配信情報２２を確認して、その情報の必要性を決定する（Ｓ１５７）。
決定は、配信情報２２に含まれる位置や時間、送信先や送信元の通信装置を一意に識別する通信装置ＩＤなどから決定する。
例えば、反対車線における渋滞に関する情報は、車両の進行方向とは逆の車線の情報なので、不必要と決定することもできる。
受信した配信情報２２が必要な場合、配信情報２２の検証を行う必要があり、不必要の場合、検証は不要である。
このように、受信したすべての情報に対して検証を行うのではなく、必要な情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。
また、この必要性の決定には、第一の認証情報の識別情報２４を用いてもよい。
例えば、車両に設けられた運転者の操作を受付ける入力部（不図示）を介して、運転者から指定された第一の認証情報の識別情報２４を含む場合に、その配信情報２２を必要と判断するようにしてもよい。
そして、配信情報処理部３は配信情報２２の必要性から検証の必要性を判断し（Ｓ１５８）、不必要の場合は配信情報２２を破棄する（Ｓ１５９）。
必要の場合は、認証情報処理部４に第一の認証情報の識別情報２４、配信情報２２と第二の認証情報２３を送り、認証情報処理部４は第一の認証情報２０を記憶部に保有していることを確認する（Ｓ１６０）。
第一の認証情報２０を保有していない場合、配信情報処理部３にその結果を応答し、配信情報２２を破棄する（Ｓ１５９）。
なお、この場合、配信情報処理部３は、配信情報２２を破棄せずに、参考情報として使用する場合も想定されるので、実際に破棄するか否かはサービスやシステムに依存する。
なお、本明細書では以降、配信情報２２を破棄する例にて説明を行う。

【００２６】
一方、第一の認証情報２０を保有している場合、認証情報処理部４は第二の認証情報２３の検証を第一の認証情報２０を用いて行う（Ｓ１６１）。
検証は、例えば、公開鍵アルゴリズムの場合、第一の認証情報である送信側の公開鍵証明書を用いて受信した配信情報の署名検証などである。
共通鍵の場合、第一の認証情報２０に含まれるセッション鍵を用いた配信情報のメッセージ認証コードの検証、復号した結果内のパディング値の確認などである。
また、この際、第一の認証情報２０に有効期限が設けられている場合、現在日時と比較することで、その有効期限が切れていないことの確認も行い、期限内であれば上記と合わせて正当と判断し、期限が切れていたらその第一の認証情報は削除する。
そして、認証情報処理部４は検証の結果を判断し（Ｓ１６２）、第二の認証情報２３の正当性が確認できない場合には、その結果を配信情報処理部３に伝え、配信情報処理部３は配信情報２２を破棄する（Ｓ１５９）。
なお、この場合、前述と同様に、配信情報処理部３は、配信情報２２を破棄せずに、参考情報として使用する場合も想定されるので、実際に破棄するか否かはサービスやシステムに依存する。
なお、本明細書では以降、配信情報２２を破棄する例にて説明を行う。
【００２７】
第二の認証情報２３の正当性が確認できた場合、認証情報処理部４はその結果を配信情報処理部３に送り、配信情報処理部３は配信情報２２を処理する（Ｓ１６３）。
この際、必要に応じて、配信情報２２も配信情報処理部３に送る。
配信情報２２の処理は、図示されていないが、運転者が確認可能な表示装置に送信し、運転者に注意や警告を促したり、車両の制御部に送信して、速度調整やステアリング調整を行ったりする。
また、複数の通信データから総合的に判断して上記処理を行ってもよい。
【００２８】
このようにして、通信回数Ｎにおいて、１回は第一の認証情報を送信し、残りの（Ｎ－１）回は第二の認証情報、第一の認証情報の識別情報、配信情報を送信する構成によって、通信データ長を短くすることができる。
ここで、公開鍵暗号アルゴリズム鍵長１０２４ｂｉｔのＲＳＡ（登録商標）を用いたデジタル署名を利用した場合を考える。
配信情報を送信しない場合、第一の認証情報は通信装置の証明書に含まれる公開鍵（１０２４ｂｉｔ）と認証局の署名（１０２４ｂｉｔ）となる。
配信情報を送信する場合には、第二の認証情報が配信情報の署名（１０２４ｂｉｔ）であり、第一の認証情報の識別情報はハッシュ関数ＳＨＡ－１を用いた公開鍵証明書のハッシュ値とすると１６０ｂｉｔであり、従来に比べて少なくとも１０２４ｂｉｔ通信データ長を短くすることができる。
これにより、より長い配信情報の通信や通信品質の向上が可能となる。
また、共通鍵アルゴリズムの場合、通信回数Ｎ回毎に検証で使用する共通鍵を変えることができるので、セキュリティレベルが向上する。
また、第一の認証情報の識別情報を第二の認証情報と共に送信しているため、複数の通信装置と通信する場合でも、通信装置では正確かつ簡単に第一の認証情報と第二の認証情報を関連付けすることができる。
さらに、従来受信の際に第一の認証情報と第二の認証情報の両方の検証を実施していたが、第一の認証情報と第二の認証情報を分けて受信するようにしているため、検証を分けて実施することができ、処理の負荷を減らすことができ、処理能力の低い装置での実現が可能となり、コスト削減が可能となる。
また、受信したすべての配信情報に対して検証を行うのではなく、必要な配信情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。

また、検証して正当であることを確認した第一の認証情報を記憶部に記録し、再度同じ第一の認証情報を受信した際には保有していることを確認し、第一の認証情報に有効期限がある場合にはその有効期限を確認する構成であるので、無駄な検証を省略することができ、処理の負荷を減らすことができる。

この結果、処理能力の低い通信装置であっても効率的にセキュリティ強度を高めることができる。

【００２９】

なお、通信装置１において、送信時と受信時の構成を変えてもよい。

例えば、通信部５は配信情報処理部３とのみ接続されている構成になっているが、送信時、通信部５を認証情報処理部４に接続する構成にして、配信情報処理部３で生成された配信情報から認証情報処理部４で認証情報を生成し、配信情報と認証情報をあわせて通信部５から送信する構成でもよい。

また、通信部５は配信情報処理部３の配信情報と認証情報処理部４の認証情報をあわせて送信する形態でもよい。

受信時は、上記実施の形態では、配信情報処理部３で必要と判断された第二の認証情報の検証を実施していたが、通信部５から認証情報処理部４を経て、正当性が確認された配信情報のみを配信情報処理部３に送る構成にした場合、受信した通信データすべてを検証する構成にすることもできる。

また、通信装置１は、通信部５にてデータ識別情報を判断し、配信情報が無い場合には、第一の認証情報を認証情報処理部４へ送信し、配信情報がある場合には、通信データを配信情報処理部３へ送信する構成でもよい。

さらに、配信情報処理部３にあったカウンタを認証情報処理部４に設けてもよい。

【００３０】

また、本実施の形態を適用するのは低コストがより厳しく要求される車載器のみに適用し、路側機は従来と同じ構成の路車間・車車間通信システムとしてもよい。

さらに、複数のチャネルを持つ路車間・車車間通信システムの場合、あるチャネルには第一の認証情報を送信して、別のチャネルにて配信情報、第一の認証情報の識別情報、第二の認証情報を送信してもよい。

また、配信情報を含む通信データの場合は通信データ全体もしくは配信情報のみを暗号化を施し、配信情報を含まない第一の認証情報のみを送信する場合は暗号化をしないで送信する構成にしてもよい。

なお、本実施の形態では電源投入後、カウンタ値が１で送信から開始する構成を示したが、異なるカウンタや受信から開始する場合にも適用できることは言うまでもない。

【００３１】

実施の形態２.

以上の実施の形態１では、あらかじめ決められた通信回数に対して、第一の認証情報のみを送信する場合と、第一の認証情報の識別情報と配信情報と第二の認証情報を送信する場合に分けて送信するようにしたものである。

次に、毎回配信情報を送信し、あらかじめ決められた通信回数Ｎに対して、１回は第一の認証情報と配信情報、第二の認証情報を送信し、残りの（Ｎ－１）回は第一の認証情報の識別情報と配信情報、第二の認証情報を送信する形態を示す。

このような構成は、実施の形態１と比較して、通信データ長は長くなるものの、配信情報を毎回送信することができ、配信情報の送信頻度低下に対応できる。

なお、本実施の形態に係る通信装置の構成は実施の形態１の図１と同じであるので、説明を省略する。

【００３２】

次に、送信時の処理について図６と図７を用いて説明する。

図６はデータ送信時の処理フロー図であり、図７は通信データの構成図である。

【００３３】

通信装置１の電源投入時又は送信タイミングの到来時に、配信情報処理部３は配信情報

を生成し（Ｓ２００）、認証情報処理部４に配信情報を出力する。
そして、認証情報処理部４は記憶部７に格納されている鍵情報を用いて、第二の認証情報を生成し（Ｓ２０１）、配信情報処理部３に応答する。
第二の認証情報は実施の形態１と同様である。
そして、配信情報処理部３はカウンタ６のカウンタ値を確認する（Ｓ２０２）。
本実施の形態では、実施の形態１と同様に通信装置１に電源が入った直後のカウンタの初期値は１で、その後送信する度にカウントアップしていくカウンタとしている。

【００３４】

カウンタ値が１の場合、配信情報処理部３は第一の認証情報を認証情報処理部４から取得する（Ｓ２０３）。
この時の認証情報処理部４での処理や第一の認証情報は実施の形態１と同じである。
そして、通信データに第一の認証情報を含むか、第一の認証情報の識別情報を含むかを表す情報であるデータ識別情報２１に“第一の認証情報”を設定し（Ｓ２０４）、図７（ａ）に示す１回目の構成で通信データを通信部５から送信する（Ｓ２０５）。
カウンタ値が１以外の場合、配信情報処理部３は、第二の認証情報の生成に利用した第一の認証情報の識別情報を取得する（Ｓ２０６）。
第一の認証情報の識別情報は、実施の形態１と同じである。
そして、配信情報処理部３は、データ識別情報２１に“第一の認証情報の識別情報”を設定し（Ｓ２０７）、図７（ｂ）に示す２回目の構成で通信データを通信部５から送信する（Ｓ２０５）。
通信データの送信後、配信情報処理部３は、カウンタ値があらかじめ決められた通信回数Ｎに達しているか否かを確認する（Ｓ２０８）。
そして、カウンタ値が通信回数Ｎに達していなければカウンタ値をカウントアップし（Ｓ２０９）、達していればカウンタ値を初期値に戻す（Ｓ２１０）。
このようにして、図７に示す通信データが送信される。
なお、図示していないが、システムに応じて、通信データや配信情報を暗号化して送信してもよい。

【００３５】

本実施の形態では、毎回配信情報を送信するため、通信回数Ｎは例えば図２３に示す方法により決定する。
図２３は、実施の形態１における図２２に相当する。
図２３では、配信情報の分割回数＝通信回数Ｎとする例を示している。
図２３では、１つの配信情報をＭ分割して送信するケースを示しており、この場合には、第一の認証情報も配信情報とともに送信されるので、データ送信の機会はＭ回となる。
つまり、図２３では、通信回数Ｎ＝Ｍ回となる。
図２３の方法に代えて図２１に示す方法によって通信回数Ｎを決定してもよいし、他の方法によって決定してもよい。

【００３６】

次に図８を用いて通信装置の受信時のフローについて説明する。
図８は受信時の処理フロー図である。

【００３７】

通信装置１は、通信部５によって通信データを受信する（Ｓ２５０）。
そして、通信部５は通信データを配信情報処理部３に送り、配信情報処理部３は暗号化されていない部分の配信情報２２、すなわち全部もしくは一部の配信情報２２を確認して、その情報の必要性を決定する（Ｓ２５１）。
決定は、実施の形態１と同様である。
そして、配信情報処理部３は配信情報２２の必要性から検証の必要性を判断し（Ｓ２５２）、不必要の場合は配信情報２２を破棄する（Ｓ２５３）。
必要の場合は、配信情報処理部３は認証情報処理部４に通信データを送り、認証情報処理部４は第一の認証情報２０を記憶部７に保有していることを確認する（Ｓ２５４）。

この際、第一の認証情報２０に有効期限が含まれている場合、現在日時と比較して、その有効期限が切れていないことを確認する。
このように、受信したすべての情報に対して検証を行うのではなく、必要な情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。
【００３８】
第一の認証情報２０を保有していない場合、データ識別情報２１を確認する（Ｓ２５５）。
データ識別情報２１が“第一の認証情報の識別情報”の場合、無効な通信データとして配信情報処理部３に応答して、配信情報処理部３は配信情報２２を破棄する（Ｓ２５３）。
データ識別情報２１が“第一の認証情報”の場合、認証情報処理部４は、記憶部７にあらかじめ記録された鍵情報を用いて第一の認証情報２０を検証する（Ｓ２５６）。
検証処理は、実施の形態１と同様である。
そして、検証の結果を判断し（Ｓ２５７）、第一の認証情報２０の正当性が確認できない場合、第一の認証情報を破棄し、その旨を配信情報処理部３に通知し、配信情報処理部３は配信情報２２を破棄する（Ｓ２５３）。
第一の認証情報２０の正当性が確認できたら、第一の認証情報２０を記憶部７に格納する（Ｓ２５８）。
この際、必要に応じて第一の認証情報の識別情報を作成して第一の認証情報２０と共に記録する。
第一の認証情報２０に、第一の認証情報の識別情報が含まれている場合はその情報を共に記録する。
そして、認証情報処理部４は、第二の認証情報２３の検証を第一の認証情報を用いて行う（Ｓ２５９）。
検証処理は、実施の形態１と同様である。
その後、認証情報処理部４は、検証の結果を判断し（Ｓ２６０）、第二の認証情報２３の正当性が確認できない場合には、その結果を配信情報処理部３に伝え、配信情報処理部３は配信情報２２を破棄する（Ｓ２５３）。
第二の認証情報２３の正当性を確認できた場合、認証情報処理部４は、その結果を配信情報処理部３に送り、配信情報処理部３は配信情報を処理する（Ｓ２６１）。
この際、必要に応じて、配信情報２２も配信情報処理部３に送る。
配信情報２２の処理は、実施の形態１と同様である。
Ｓ２５４にて、第一の認証情報を保有している場合、第一の認証情報を検証する必要がないので、上記第二の認証情報２３の検証（Ｓ２５９）を実施する。
これ以降の処理は上記と同じである。
【００３９】
このようにして、通信回数Ｎにおいて、１回は第一の認証情報、配信情報、第二の認証情報を送信し、残りの（Ｎ－１）回は第二の認証情報、第一の認証情報の識別情報、配信情報を送信する構成によって、配信情報の送信頻度を低下させずに、従来に比べて総合的に通信データ長を短くすることができる。
ここで、公開鍵暗号アルゴリズム鍵長１０２４ｂｉｔのＲＳＡ（登録商標）を用いたデジタル署名を利用した場合を考える。
第一の認証情報を送信する場合、通信装置の証明書に含まれる公開鍵（１０２４ｂｉｔ）と認証局の署名（１０２４ｂｉｔ）を含む第一の認証情報と、第二の認証情報である配信情報の署名（１０２４ｂｉｔ）となり、従来と同じであるが、第一の認証情報の識別情報を送信する場合、第一の認証情報（少なくとも２０４８ｂｉｔ）の代わりに第一の認証情報の識別情報であるハッシュ値１６０ｂｉｔであり、従来に比べて総合的に通信データ長を短くすることができる。
これにより、配信情報の送信頻度を低下させずに、通信品質の向上が可能となる。

また、共通鍵アルゴリズムの場合、通信回数Ｎ回毎に検証で使用する共通鍵を変えることができるので、セキュリティレベルが向上する。

また、第一の認証情報を送信しない場合、第一の認証情報の識別情報を第二の認証情報と共に送信しているため、複数の通信装置と通信する場合でも、通信装置では正確かつ簡単に第一の認証情報と第二の認証情報を関連付けすることができる。

さらに、第一の認証情報の識別情報を受信した際には、第二の認証情報のみ検証すればよい構成になっているので、配信情報の送信頻度を低下させずに、処理の負荷を減らすことができる。

また、受信したすべての配信情報に対して検証を行うのではなく、必要な配信情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。

また、検証して正当であることを確認した第一の認証情報を記憶部に記録し、再度同じ第一の認証情報を受信した際には保有していることを確認し、第一の認証情報に有効期限がある場合にはその有効期限を確認する構成であるので、無駄な検証を省略することができ、処理の負荷を減らすことができる。

【００４０】

なお、通信装置において、送信時と受信時の構成を変えてもよい。

例えば、通信部５は配信情報処理部３とのみ接続されている構成になっているが、送信時、通信部５を認証情報処理部４に接続する構成にして、配信情報処理部３で生成された配信情報から認証情報処理部４で認証情報を生成し、配信情報と認証情報をあわせて通信部５から送信する構成でもよい。

また、通信部５は配信情報処理部３の配信情報と認証情報処理部４の認証情報をあわせて送信する形態でもよい。

受信時は、上記実施の形態では、配信情報処理部３で必要と判断された第二の認証情報の検証を実施していたが、通信部５から認証情報処理部４を経て、正当性が確認された配信情報のみを配信情報処理部３に送る構成にした場合、受信した通信データすべてを検証する構成にすることもできる。

さらに、配信情報処理部３にあったカウンタ６を認証情報処理部４に設けてもよい。

また、本実施の形態を適用するのは低コストがより厳しく要求される車載器のみに適用し、路側機は従来と同じ構成の路車間・車車間通信システムとしてもよい。

また、通信データ全体もしくは配信情報のみを暗号化を施して送信する構成にしてもよい。

なお、本実施の形態では電源投入後、カウンタ値が１で送信から開始する構成を示したが、異なるカウンタや受信から開始する場合にも適用できることは言うまでもない。

【００４１】

実施の形態３．

以上の実施の形態１と２では、あらかじめ決められた通信回数に対して、第一の認証情報を送信する場合と、第一の認証情報の識別情報を送信する場合に分けて送信するようにしたものである。

次に、第一の認証情報を送信した直後に他の通信装置から受信した情報を元に、第一の認証情報を送信する場合と第一の認証情報の識別情報を送信する場合とを選択的に決定して送信する実施の形態を示す。

【００４２】

図９は、本実施の形態に係る通信装置１の構成を示す図である。

実施の形態１の図１と同じ番号は説明を省略する。

【００４３】

受信ＩＤ記憶部５０は、受信した通信データの送信元である他の通信装置を一意に識別できる通信装置ＩＤを記憶するもので、配信情報処理部３と接続されている。

受信ＩＤ記憶部５０は、読み書き可能なメモリで構成される。

通信装置ＩＤは、通信装置を一意に識別するためのもので、通信装置に設定されている

ＩＤや第一の認証情報の識別情報でよい。
本実施の形態では通信装置ＩＤを第一の認証情報の識別情報として説明する。
【００４４】
また、配信情報処理部３には、送信フラグ５１と受信フラグ５２が設けられ、これらは読み書き可能なメモリで構成される。
送信フラグ５１は、通信装置１が第一の認証情報を送信したかどうかを表すフラグであり、本実施の形態では第一の認証情報を送信した場合には“Ｈ”、第一の認証情報の識別情報を送信した場合には“Ｌ”で示し、電源投入直後の初期値は“Ｌ”としている。
受信フラグ５２は、通信装置１が受信した情報から次回の送信において第一の認証情報を送信すべきかどうかを表すフラグであり、本実施の形態では第一の認証情報を送信する必要がない、すなわち第一の認証情報の識別情報を送信する場合には“Ｈ”、第一の認証情報を送信する必要がある場合には“Ｌ”で示し、電源投入直後の初期値は“Ｌ”としている。
【００４５】
更に、配信情報処理部３には、送信処理部３１と受信処理部３２が設けられている。
通信装置１が車両に搭載されている車載器である場合には、他の通信装置２は他の車両に搭載されている車載器又は路側に設置されている路側機であり、通信装置１が搭載されている車両の移動又は他の通信装置２が搭載されている車両の移動に伴って通信装置１の通信可能範囲（無線通信用の電波の届く範囲）に所在する他の通信装置２が変化していく。
同様に、通信装置１が路側機である場合には、他の通信装置２は車両に搭載されている車載器であり、他の通信装置２が搭載されている車両の移動に伴って通信装置１の通信範囲（無線通信用の電波の届く範囲）に所在する他の通信装置２が変化していく。
また、本実施の形態では、通信装置１は周期的に通信データを送信するとともに、送信タイミングの合間の期間では、他の通信装置２からの通信データを受信する。
【００４６】
受信処理部３２は、送信タイミングの合間の期間において通信部５により受信された通信データに含まれている通信装置ＩＤを用いて、通信装置１からの通信データを受信できる状況にある通信装置２（通信装置１の通信可能範囲内にある他の通信装置２）を検出する。
また、受信処理部３２は、受信フラグ５２が“Ｈ”のときに、送信フラグが“Ｌ”であるという条件と、それまで未検出であった通信装置２を新たに検出したという条件という２つの条件が満たされた場合に、受信フラグ５２を“Ｌ”にして、新たな通信装置２が検出されたため第一の認証情報の送信が必要であることを送信処理部３１に通知する。
送信処理部３１は、送信タイミングが到来した際に送信フラグ５１が“Ｌ”であり、受信フラグ５２が“Ｌ”である場合、１つ前の送信タイミングで送信した情報が第一の認証情報の識別情報であるという条件と受信処理部３２により新たな通信装置２が検出されているという条件が満たされている場合は、送信処理部３１は第一の認証情報の送信を指定し、通信部５は、第一の認証情報が含まれる通信データを送信する。
一方、送信タイミングが到来した際に送信フラグが“Ｈ”である場合、すなわち、１つ前のの送信タイミングで送信した情報が第一の認証情報である場合、または送信フラグが“Ｌ”であっても受信フラグ５２が“Ｈ”である場合、すなわち１つ前の送信タイミングで送信した情報が第一の認証情報の識別情報であるという条件は満たすが受信処理部３２により新たな通信装置２が検出されていない場合には、送信処理部３１は第一の認証情報の識別情報の送信を指定し、通信部５は、第一の認証情報の識別情報と配信情報と第二の認証情報が含まれる通信データを送信する。
【００４７】
前述したように、送信処理部３１は、１つ前の送信タイミングにおいて第一の認証情報の識別情報が送信されており、更に受信処理部３２により新たな通信装置２が検出されている場合にのみ、第一の認証情報の送信を選択する。

換言すれば、１つ前の送信タイミングで第一の認証情報が送信されていれば、１つ前の送信タイミングの後に受信処理部３２により新たな通信装置２が検出されていても、次の送信タイミングでは第一の認証情報の識別情報が送信される。

なお、本実施の形態では、送信処理部３１が送信対象指定部の例となり、受信処理部３２は機器検出部の例となる。

【００４８】

また、図９では図示していないが、通信装置１は現在の位置情報、日付や時間を表す日時情報が、搭載されている路側機や車両から入力されている。

これらは、路側機や車両に設置されているＧＰＳ信号通信装置や時計などで生成される。

【００４９】

次に図１０と図１１を用いて通信装置における送信時のフローについて説明する。

図１０は送信処理フロー図であり、図１１は通信データの構成図を示した図である。

【００５０】

送信処理部３１は、まず、送信フラグ５１を確認する（Ｓ３００）。

送信フラグ５１が“Ｈ”の場合、送信処理部３１にて配信情報２２を生成し（Ｓ３０１）、認証情報処理部４に出力する。

認証情報処理部４は、第二の認証情報２３を記憶部７に記録されている鍵情報と配信情報から生成して（Ｓ３０２）、配信情報処理部３へ応答する。

そして、配信情報処理部３では、送信処理部３１が、第一の認証情報の識別情報を取得する（Ｓ３０４）。

その後、送信処理部３１は、データ識別情報２１に“配信情報あり”を設定し（Ｓ３０５）、送信フラグを“Ｌ”に設定する（Ｓ３０６）。

そして、通信部５を介して他の通信装置２に図１１（ｂ）に示すように第一の認証情報の識別情報、配信情報と第二の認証情報を送信する（Ｓ３０７）。

【００５１】

一方、Ｓ３００において送信フラグが“Ｌ“の場合、送信処理部３１は、受信フラグ５２を確認する（Ｓ３０８）。

Ｓ３０８において受信フラグ５２が“Ｈ“の場合、第一の認証情報を送信する必要はないので、送信フラグが“Ｈ”の場合と同じ処理を行うことによって第一の認証情報の識別情報、配信情報と第二の認証情報を送信する。

Ｓ３０８において受信フラグが“Ｌ”の場合、送信処理部３１は第一の認証情報を取得する（Ｓ３０９）。

その後、送信処理部３１は、データ識別情報２１に“配信情報なし”を設定し（Ｓ３１０）、送信フラグを“Ｈ”に（Ｓ３１１）、受信フラグを“Ｈ”に（Ｓ３１２）設定する。

そして、受信ＩＤ記憶部５０に記録されている内容を消去して（Ｓ３１３）、通信部５を介して他の通信装置２に図１１（ａ）に示すように第一の認証情報を送信する（Ｓ３０７）。

このようにして、図１１に示す通信データが送信される。

なお、図示していないが、システムに応じて、通信データや配信情報を暗号化して送信してもよい。

【００５２】

次に図１２を用いて通信装置１における受信時のフローについて説明する。

【００５３】

図１２は受信処理フロー図であり、第一の認証情報や第二の認証情報の処理に関しては実施の形態１の図４と同じであるため、省略している。

本図では、図４に含まれていない送信フラグ、受信フラグ、受信ＩＤ記憶部に関する処理に焦点を当てて示している。

【００５４】

まず、通信部５によって他の通信装置２からの通信データを受信する（Ｓ１５０）。
そして、図４と同様の処理を行い、最終的に配信情報処理部３や認証情報処理部４の処理によって、配信情報の破棄（Ｓ１５９）、配信情報の処理（Ｓ１６３）、第一の認証情報の破棄（Ｓ１５６）、第一の認証情報の格納（Ｓ１５５）が実施される。
その後、配信情報処理部３の受信処理部３２は、送信フラグ５１を確認する（Ｓ３５０）。
送信フラグ５１が“Ｈ”の場合、直前に送信したのは第一の認証情報なので、受信処理部３２は、受信した通信装置ＩＤを受信ＩＤ記憶部５０に記憶し（Ｓ３５１）、終了する。
受信ＩＤ記憶部５０に記録されている通信装置ＩＤについて図１３を用いて説明する。
通信装置１はシステムで定められたある一定間隔で通信データを送信し（６０）、同様に他の通信装置２が送信した通信データを受信する（６１）。
受信ＩＤ記憶部５０には、図１３に示すように、自身が第一の認証情報を含む通信データを送信（６０ａ）した後、一送信周期後に自身が再び通信データを送信（６０ｂ）するまでの間（Ｔ１）に受信した他の通信装置２の通信データに含まれる通信装置ＩＤが記録される。

【００５５】

図１２のＳ３５０にて、送信フラグ５１が“Ｌ”の場合、受信処理部３２は、受信フラグ５２を確認する（Ｓ３５２）。
受信フラグ５２が“Ｌ”の場合、何も処理をせず終了する。
受信フラグ５２が“Ｈ”の場合、受信処理部３２は、受信した通信装置ＩＤと受信ＩＤ記憶部５０に記憶されている以前に受信した通信装置ＩＤを比較する（Ｓ３５３）。
比較について、図１３を用いて説明する。
送信フラグ５１が“Ｌ”の場合、これらの比較結果は以下の二通りに分類される。
Ａ）受信した通信装置ＩＤが受信ＩＤ記憶部５０に記録されているＩＤに含まれる場合
Ｂ）受信した通信装置ＩＤが受信ＩＤ記憶部５０に記録されているＩＤに含まれない場合、もしくは受信ＩＤ記憶部５０に通信装置ＩＤが記憶されていない場合（例えば、電源投入直後）
受信した通信装置ＩＤが受信ＩＤ記憶部５０内に含まれている場合（上記Ａ）の場合）、何も処理をせず終了する。
受信した通信装置ＩＤが受信ＩＤ記憶部５０内に含まれていない場合（上記Ｂ）の場合）、当該通信装置ＩＤで識別される通信装置２は新たに検出された通信装置であり、当該通信装置に対して第一の認証情報を送信する必要があるので、受信処理部３２は受信フラグ５２を“Ｌ”に設定して（Ｓ３５４）終了する。

【００５６】

上記の送信や受信の処理について図１３を用いて時系列で説明する。
通信装置１は、前述したように、システムで定められたある一定間隔で通信データを送信し（６０）、同様に他の通信装置２が送信した通信データを受信する（６１）。
図１３にて、通信装置１が第一の認証情報を含む通信データを送信（６０ａ）した後、送信フラグが“Ｈ”であるので、図１２より一送信周期後に自身が再び通信データを送信（６０ｂ）するまでの間（Ｔ１）に受信した他の通信装置２の通信データに含まれる通信装置ＩＤが記録される。
そして、通信装置１が送信する通信データ（６０ｂ）は、送信フラグが“Ｈ”であるので、図１０のフロー図より、第一の認証情報の識別情報が含まれる。
このように、第一の認証情報を送信した次の通信データには、必ず第一の認証情報の識別情報が含まれる。
通信装置１が第一の認証情報の識別情報を含む通信データ（６０ｂ）を送信した後は、図１０より送信フラグが“Ｌ”である。
受信フラグは“Ｈ”のままであるので、通信装置１は、図１２より一送信周期後に自身が再び通信データを送信（６０ｃ）するまでの間（Ｔ２）に受信した他の通信装置２の通

信データに含まれる通信装置ＩＤと受信ＩＤ記憶部５０内に記録されている通信装置ＩＤと比較する。

他の通信装置２の通信データ（６１ａ）を受信した際の比較の結果、受信した他の通信装置２の通信装置ＩＤが受信ＩＤ記憶部５０内の通信装置ＩＤに含まれている場合、通信装置１は何もせずに、その受信処理を終了する。

次に、他の通信装置の通信データ（６１ｂ）を受信した際の比較の結果、受信した他の通信装置２の通信装置ＩＤが受信ＩＤ記憶部５０内の通信装置ＩＤに含まれてない場合、通信装置１は受信フラグを“Ｌ”に設定して、受信処理を終了する。

これは、第一の認証情報を送信した後に受信した他の通信装置２以外に新たな通信装置２が通信エリアに入っていることを意味するので、再び第一の認証情報を送信する必要があることを意味している。

そして、他の通信装置の通信データ（６１ｃ）を受信した際、受信フラグが“Ｌ”であるので、比較はせずに受信処理を終了する。

これは、１台でも新たな通信装置２が通信エリアに入っている場合には、第一の認証情報を送信しなければならないので、複数の新たな通信装置２を検出する必要はなく、処理を効率化している。

このように、１台でも新たな通信装置２を検出した場合、検出後の比較を行わない構成にしているので、処理の負荷を低減し、効率化することができる。

そして、通信装置が通信データ（６０ｃ）を送信する際には、送信フラグが“Ｌ”、受信フラグが“Ｌ”に設定されているので、図１０より第一の認証情報を含む通信データを送信することができる。

また、他の通信装置の通信データ（６１ｂ）を受信した際の比較によって、受信ＩＤ記憶部５０に含まれる場合、次の他の通信装置の通信データ（６１ｃ）を受信した際に比較を実施する。

そして、通信装置が通信データ（６０ｃ）を送信するまでに、受信したすべての通信装置ＩＤが受信ＩＤ記憶部に含まれる場合、つまり、新たな他の通信装置２が検出できない場合、図１２より送信フラグは“Ｌ”、受信フラグは“Ｈ”であるので、図１０の送信フローより第一の認証情報の識別情報を含む通信データ（６０ｃ）を送信する。

このようにして、第一の認証情報を送信した直後に受信した情報と比較して、新たな通信装置を検出した場合、第一の認証情報を送信し、検出しない場合は、第一の認証情報の識別情報を送信する。

【００５７】

このように、周囲に存在する通信装置の状態を考慮し、新しい通信装置が存在する場合には第一の認証情報を用いて送信し、存在しない場合には第一の認証情報の識別情報を送信する構成にしているので、効率良く必要な情報を送信することができ、かつ通信データ長を短くすることができる。

また、第一の認証情報の識別情報を第二の認証情報と共に送信しているため、複数の通信装置と通信する場合でも、通信装置では正確かつ簡単に第一の認証情報と第二の認証情報を関連付けすることができる。

さらに、従来受信の際に第一の認証情報と第二の認証情報の両方の検証を実施していたが、第一の認証情報と第二の認証情報を分けて受信するようにしているため、検証を分けて実施することができ、処理の負荷を減らすことができ、処理能力の低い装置での実現が可能となり、コスト削減が可能となる。

また、受信したすべての配信情報に対して検証を行うのではなく、必要な配信情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。

また、検証して正当であることを確認した第一の認証情報を記憶部に記録し、再度同じ第一の認証情報を受信した際には保有していることを確認し、第一の認証情報に有効期限がある場合にはその有効期限を確認する構成であるので、無駄な検証を省略することができ、処理の負荷を減らすことができる。

また、送信フラグにより第一の認証情報を送信した後は、必ず第一の認証情報の識別情報を送信する構成にしているため、少なくとも２回に１回は確実に配信情報を送信することができる。

さらに、受信した配信情報を要否問わず、受信したＩＤを受信ＩＤ記憶部に記録しているので、より正確な周囲に存在する通信装置の状態を把握することができ、効率的に情報を送信することができる。

また、１台でも新たな通信装置を検出した場合、検出後の比較を行わない構成にしているので、処理の負荷を低減し、効率化することができる。

【００５８】

なお、通信装置１において、送信時と受信時の構成を変えてもよい。

例えば、通信部５は配信情報処理部３とのみ接続されている構成になっているが、送信時、通信部を認証情報処理部４に接続する構成にして、配信情報処理部３で生成された配信情報から認証情報処理部４で認証情報を生成し、配信情報と認証情報をあわせて通信部５から送信する構成でもよい。

また、通信部５は配信情報処理部３の配信情報と認証情報処理部４の認証情報をあわせて送信する形態でもよい。

受信時は、上記実施の形態では、配信情報処理部３で必要と判断された第二の認証情報の検証を実施していたが、通信部５から認証情報処理部４を経て、正当性が確認された配信情報のみを配信情報処理部３に送る構成にした場合、受信した通信データすべてを検証する構成にすることもできる。

また、通信装置１は、通信部５にてデータ識別情報を判断し、配信情報が無い場合には、第一の認証情報を認証情報処理部４へ送信し、配信情報がある場合には、通信データを配信情報処理部４へ送信する構成でもよい。

さらに、配信情報処理部３にあった送信フラグ５１、受信フラグ５２を認証情報処理部４に設け、受信ＩＤ記憶部５０を認証情報処理部４に接続する構成にしてもよい。

また、本実施の形態を適用するのは低コストがより厳しく要求される車載器のみに適用し、路側機は従来と同じ構成の路車間・車車間通信システムとしてもよい。

さらに、複数のチャネルを持つ路車間・車車間通信システムの場合、あるチャネルには第一の認証情報を送信して、別のチャネルにて配信情報、第一の認証情報の識別情報、第二の認証情報を送信してもよい。

また、配信情報を含む通信データの場合は通信データ全体もしくは配信情報のみを暗号化を施し、配信情報を含まない第一の認証情報のみを送信する場合は暗号化をしないで送信する構成にしてもよい。

なお、本実施の形態では電源投入後、各フラグの初期値が“Ｌ”で送信から開始する構成を示したが、異なるフラグや受信から開始する場合にも適用できることは言うまでもない。

【００５９】

実施の形態４.

以上の実施の形態３では、あらかじめ決められた通信回数に対して、第一の認証情報のみを送信する場合と、配信情報と第二の認証情報を送信する場合に分けて送信するようにしたものであるが、次に、毎回配信情報を送信する構成にした形態を示す。

つまり、実施の形態３と同様に、新たな他の通信装置を検出した際に、１つ前の送信タイミングにおいて第一の認証情報の識別情報を送信している場合は、第一の認証情報を送信するが、このとき配信情報と第二の認証情報も併せて送信する。

このような構成は、実施の形態１と実施の形態２との関係と同様に、実施の形態３と比較して、通信データ長は長くなるものの、配信情報を毎回送信することができ、配信情報の送信頻度低下に対応できる。

【００６０】

本実施の形態に係る通信装置は実施の形態３の図９と同じであるので、説明を省略する。

【００６１】
次に、送信時の処理について図１４と図１５を用いて説明する。
図１４は送信時の処理フロー図、図１５は通信データの構成図である。
【００６２】
通信装置１は、送信開始後、送信処理部３１にて配信情報を生成し（Ｓ４００）、認証情報処理部４に配信情報を送信して、認証情報処理部４は記憶部７に格納されている鍵情報を用いて、第二の認証情報を生成し（Ｓ４０１）、配信情報処理部３に応答する。
第二の認証情報は実施の形態１と同様である。
そして、送信処理部３１は、送信フラグ５１を確認する（Ｓ４０２）。
送信フラグが“Ｈ”の場合、送信処理部３１は第一の認証情報の識別情報を取得する（Ｓ４０３）。
その後、データ識別情報２１に“第一の認証情報の識別情報”を設定し（Ｓ４０４）、送信処理部３１は送信フラグ５１を“Ｌ”に設定する（Ｓ４０５）。
そして、通信部５を介して他の通信装置２に図１５の（ａ）に示すように第一の認証情報の識別情報２４、配信情報２２と第二の認証情報２３を送信する（Ｓ４０６）。
送信フラグ５１が“Ｌ”の場合、送信処理部３１は、受信フラグ５２を確認する（Ｓ４０７）。
受信フラグ５２が“Ｈ”の場合、第一の認証情報を送信する必要はないので、送信処理部３１は送信フラグ５１が“Ｈ”の場合の処理と同じ処理を行うことによって第一の認証情報の識別情報２４、配信情報２２と第二の認証情報２３を送信する。
受信フラグ５２が“Ｌ”の場合、配信情報処理部４は第一の認証情報を取得する（Ｓ４０８）。
その後、送信処理部３１は、データ識別情報２１に“第一の認証情報”を設定し（Ｓ４０９）、送信フラグ５１を“Ｈ”に（Ｓ４１０）、受信フラグ５２を“Ｈ”に（Ｓ４１１）設定する。
そして、受信ＩＤ記憶部５０に記録されている内容を消去して（Ｓ４１２）、通信部５を介して他の通信装置２に図１５の（ｂ）に示すように第一の認証情報２０、配信情報２２と第二の認証情報２３を送信する（Ｓ４０６）。
このようにして、図１５に示す通信データが送信される。
なお、図示していないが、システムに応じて、通信データや配信情報を暗号化して送信してもよい。
【００６３】
次に図１６を用いて通信装置１における受信時のフローについて説明する。
図１６は受信処理フロー図であり、第一の認証情報や第二の認証情報の処理に関しては実施の形態２の図８と同じであるため、省略している。
本図では、図８に含まれていない送信フラグ、受信フラグ、受信ＩＤ記憶部に関する処理に焦点を当てて示している。
【００６４】
まず、通信部５によって他の通信装置２からの通信データを受信する（Ｓ２５０）。
そして、図８と同様の処理を行い、最終的に配信情報処理部３や認証情報処理部４の処理によって、配信情報の破棄（Ｓ２５３）、配信情報の処理（Ｓ２６１）が実施される。
その後、配信情報処理部３の受信処理部３２は、送信フラグ５１を確認する（Ｓ４５０）。
送信フラグ５１が“Ｈ”の場合、直前に送信したのは第一の認証情報なので、受信した通信装置ＩＤを受信ＩＤ記憶部５０に記憶し（Ｓ４５１）、終了する。
受信ＩＤ記憶部５０に記録されている通信装置ＩＤについては実施の形態３の図１３と同じである。
送信フラグ５１が“Ｌ”の場合、受信処理部３２は、受信フラグ５２を確認する（Ｓ４５２）。
受信フラグ５２が“Ｌ”の場合、何も処理をせず終了する。

受信フラグ５２が“Ｈ”の場合、受信処理部３２が受信した通信装置ＩＤと受信ＩＤ記憶部５０に記憶されている以前に受信した通信装置ＩＤを比較する（Ｓ４５３）。
比較処理については、実施の形態３と同じである。
受信ＩＤ記憶部５０内に含まれている場合、何も処理をせず終了する。
受信ＩＤ記憶部５０内に含まれていない場合、第一の認証情報を送信する必要があるので、受信フラグ５２を“Ｌ”に設定して（Ｓ４５４）終了する。

【００６５】

このように、周囲に存在する通信装置の状態を考慮し、新しい通信装置が存在する場合には第一の認証情報を用いて送信し、存在しない場合には第一の認証情報の識別情報を送信する構成にしているので、配信情報の送信頻度を低下させずに従来に比べて総合的に通信データ長を短くすることができる。
また、第一の認証情報を送信しない場合、第一の認証情報の識別情報を第二の認証情報と共に送信しているため、複数の通信装置と通信する場合でも、通信装置では正確かつ簡単に第一の認証情報と第二の認証情報を関連付けすることができる。
さらに、第一の認証情報の識別情報を受信した際には、第二の認証情報のみ検証すればよい構成になっているので、配信情報の送信頻度を低下させずに、処理の負荷を減らすことができる。
さらに、受信したすべての配信情報に対して検証を行うのではなく、必要な配信情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。
また、検証して正当であることを確認した第一の認証情報を記憶部に記録し、再度同じ第一の認証情報を受信した際には保有していることを確認し、第一の認証情報に有効期限がある場合にはその有効期限を確認する構成であるので、無駄な検証を省略することができ、処理の負荷を減らすことができる。
また、送信フラグにより第一の認証情報を送信した後は、必ず第一の認証情報の識別情報を送信する構成にしているため、少なくとも２回に１回は従来よりも短い通信データを送ることができる。
さらに、受信した配信情報を要否問わず、受信したＩＤを受信ＩＤ記憶部に記録しているので、より正確な周囲に存在する通信装置の状態を把握することができ、効率的に情報を送信することができる。
また、１台でも新たな通信装置を検出した場合、検出後の比較を行わない構成にしているので、処理の負荷を低減し、効率化することができる。

【００６６】

なお、通信装置１において、送信時と受信時の構成を変えてもよい。
例えば、通信部５は配信情報処理部３とのみ接続されている構成になっているが、送信時、通信部を認証情報処理部４に接続する構成にして、配信情報処理部３で生成された配信情報から認証情報処理部４で認証情報を生成し、配信情報と認証情報をあわせて通信部５から送信する構成でもよい。
また、通信部５は配信情報処理部３の配信情報と認証情報処理部４の認証情報をあわせて送信する形態でもよい。
受信時は、上記実施の形態では、配信情報処理部３で必要と判断された第二の認証情報の検証を実施していたが、通信部５から認証情報処理部４を経て、正当性が確認された配信情報のみを配信情報処理部３に送る構成にした場合、受信した通信データすべてを検証する構成にすることもできる。
さらに、配信情報処理部３にあった送信フラグ、受信フラグを認証情報処理部４に設け、認証情報処理部４が受信ＩＤ記憶部５０と接続される構成でもよい。
また、本実施の形態を適用するのは低コストがより厳しく要求される車載器のみに適用し、路側機は従来と同じ構成の路車間・車車間通信システムとしてもよい。
また、通信データ全体もしくは配信情報のみを暗号化を施して送信する構成にしてもよい。

なお、本実施の形態では電源投入後、各フラグの初期値が“Ｌ”で送信から開始する構成を示したが、異なるフラグや受信から開始する場合にも適用できることは言うまでもない。

【００６７】

実施の形態５.

以上の実施の形態３と４では、第一の認証情報を送信した後に受信した他の通信装置ＩＤと送信前に受信した他の通信装置ＩＤを比較することで第一の認証情報を送信する場合と第一の認証情報の識別情報を送信する場合とを選択的に決定して送信するようにしたものである。

実施の形態３と４の方式では、新たな他の通信装置を検出した場合であっても第一の認証情報を送信した次の送信タイミングでは第一の認証情報の識別情報を送信することとなっており、第一の認証情報を送信した後に通信エリアに入ってきた他の通信装置に対して直ちに第一の認証情報を送信することができない。

本実施の形態では、第一の認証情報を送信していても、新たな他の通信装置が検出された次の送信タイミングにおいて第一の認証情報を送信する形式を説明する。

より具体的には、本実施の形態では、第一の認証情報の送信の有無に関わらず、送信周期２回前に他の通信装置から受信した他の通信装置ＩＤと１回前に受信した他の通信装置ＩＤを比較することで、第一の認証情報を送信する場合と第一の認証情報の識別情報を送信する場合とを選択的に決定して送信する方式を示す。

【００６８】

図１７は、本実施の形態に係る通信装置１の構成を示す図である。

実施の形態１の図１や実施の形態３の図９と同じ番号は説明を省略する。

【００６９】

第一の受信ＩＤ記憶部５５と第二の受信ＩＤ記憶部５６は、受信した他の通信装置２のＩＤを記憶するもので、配信情報処理部３と接続されている。これらは読み書き可能なメモリで構成される。通信装置ＩＤは、実施の形態３と同じものでよい。

配信情報処理部３には、記録フラグ５７が設けられ、これは読み書き可能なメモリで構成される。

記録フラグ５７は、通信装置１が受信した他の通信装置２のＩＤの記録先、すなわち第一の受信ＩＤ記憶部５５もしくは第二の受信ＩＤ記憶部５６を示しているフラグであり、本実施の形態では第一の受信ＩＤ記憶部５５に記録すべき場合には“Ｈ”、第二の受信ＩＤ記憶部５６に記録すべき場合には“Ｌ”で示し、電源投入直後の初期値は“Ｌ”としている。

また、配信情報処理部３に設けられている受信フラグ５２は、実施の形態３と同じである。

図示していないが、通信装置１は現在の位置情報、日付や時間を表す日時情報が、搭載されている路側機や車両から入力されている。

これらは、路側機や車両に設置されているＧＰＳ信号通信装置や時計などで生成される。

【００７０】

次に図１８と図１５を用いて通信装置における送信時のフローについて説明する。

図１８は送信処理フロー図である。

【００７１】

配信情報処理部３の送信処理部３１は、まず、配信情報を生成し（Ｓ５００）、認証情報処理部４に配信情報を送信して、認証情報処理部４は記憶部７に格納されている鍵情報を用いて、第二の認証情報を生成し（Ｓ５０１）、配信情報処理部３に応答する。

第二の認証情報は実施の形態１と同様である。

そして、送信処理部３１は、受信フラグ５２を確認する（Ｓ５０２）。

受信フラグ５２が“Ｈ”の場合、送信処理部３１は、第一の認証情報の識別情報を取得する（Ｓ５０３）。

その後、送信処理部３１は、データ識別情報２１に“第一の認証情報の識別情報”を設定し（Ｓ５０４）、通信部５を介して他の通信装置に図１５の（ａ）に示すように第一の認証情報の識別情報２４、配信情報２２と第二の認証情報２３を送信する（Ｓ５０５）。

Ｓ５０２において受信フラグが“Ｌ”の場合、送信処理部３１は第一の認証情報を取得する（Ｓ５０６）。

その後、送信処理部３１はデータ識別情報２１に“第一の認証情報”を設定し（Ｓ５０７）、受信フラグ５２を“Ｈ”に設定する（Ｓ５０８）。

そして、通信部５を介して他の通信装置２に図１５の（ｂ）に示すように第一の認証情報２０、配信情報２２、第二の認証情報２３を送信する（Ｓ５０５）。

通信データを送信後、送信処理部３１は、記録フラグ５７を確認する（５０９）。

記録フラグ５７が“Ｌ”の場合、送信処理部３１は第一の受信ＩＤ記憶部５５をクリアし（Ｓ５１０）、記録フラグ５７を“Ｈ”に設定して（Ｓ５１１）終了する。

Ｓ５０９において記録フラグ５７が“Ｈ”の場合、送信処理部３１は第二の受信ＩＤ記憶部５６をクリアし（Ｓ５１２）、記録フラグ５７を“Ｌ”に設定して（Ｓ５１３）終了する。

このようにして、図１５に示す通信データが送信される。

なお、図示していないが、システムに応じて、通信データや配信情報を暗号化して送信してもよい。

【００７２】

次に図１９を用いて通信装置１における受信時のフローについて説明する。

図１９は受信処理フロー図であり、第一の認証情報や第二の認証情報の処理に関しては実施の形態２の図８と同じであるため、省略している。

本図では、図８に含まれていない記録フラグ、受信フラグ、第一の受信ＩＤ記憶部、第二の受信ＩＤ記憶部に関する処理に焦点を当てて示している。

【００７３】

まず、通信部５によって他の通信装置２からの通信データを受信する（Ｓ２５０）。

そして、図８と同様の処理を行い、最終的に配信情報処理部３や認証情報処理部４の処理によって、配信情報の破棄（Ｓ２５３）、配信情報の処理（Ｓ２６１）が実施される。

その後、受信処理部３２は、記録フラグ５７を確認する（Ｓ５５０）。

記録フラグ５７が“Ｈ”の場合、第一の受信ＩＤ記憶部５５に記録すべき場合であるので、受信処理部３２は、受信した通信装置ＩＤを第一の受信ＩＤ記憶部５５に記憶する（Ｓ５５１）。

そして、受信処理部３２は受信フラグ５２を確認する（Ｓ５５２）。

受信フラグ５２が“Ｌ”の場合、何も処理をせず終了する。

受信フラグ５２が“Ｈ”の場合、受信処理部３２は受信した通信装置ＩＤと第二の受信ＩＤ記憶部５６に記憶されている以前に受信した通信装置ＩＤを比較する（Ｓ５５３）。

これらの比較結果は以下の二通りに分類される。

Ａ）受信した通信装置ＩＤが第二の受信ＩＤ記憶部５６に記録されているＩＤに含まれる場合

Ｂ）受信した通信装置ＩＤが第二の受信ＩＤ記憶部５６に記録されているＩＤに含まれない場合、もしくは第二の受信ＩＤ記憶部５６に通信装置ＩＤが記憶されていない場合（例えば、電源投入直後）

第二の受信ＩＤ記憶部５６内に含まれている場合（上記Ａ）の場合）、受信処理部３２は何も処理をせず終了する。

第二の受信ＩＤ記憶部５６内に含まれていない場合（上記Ｂ）の場合）、第一の認証情報を送信する必要があるので、受信処理部３２は受信フラグ５２を“Ｌ”に設定して（Ｓ５５４）終了する。

Ｓ５５０にて記録フラグ５７が“Ｌ”の場合、第二の受信ＩＤ記憶部５６に記録すべき場合であるので、受信した通信装置ＩＤを第二の受信ＩＤ記憶部５６に記憶する（Ｓ５５５）。

そして、受信処理部３２は受信フラグ５２を確認する（Ｓ５５６）。
受信フラグ５２が“Ｌ”の場合、何も処理をせず終了する。
受信フラグ５２が“Ｈ”の場合、受信処理部３２は受信した通信装置ＩＤと第一の受信ＩＤ記憶部５５に記憶されている以前に受信した通信装置ＩＤを比較する（Ｓ５５７）。
第一の受信ＩＤ記憶部５５内に含まれている場合、受信処理部３２は何も処理をせず終了する。
第一の受信ＩＤ記憶部５５内に含まれていない場合、第一の認証情報を送信する必要があるので、受信処理部３２は受信フラグ５２を“Ｌ”に設定して（Ｓ５５８）終了する。
【００７４】
上記の送信や受信の処理について図２０を用いて時系列で説明する。
図２０は通信イメージ図である。
【００７５】
通信装置１は、前述したように、システムで定められたある一定間隔で通信データを送信し（６０）、同様に他の通信装置２が送信した通信データを受信する（６１）。
図２０は、通信装置１が通信データを送信（６０ｄ）する前の記録フラグ５７は“Ｌ”としている。
通信データを送信（６０ｄ）した後、図１８より第一の受信ＩＤ記憶部５５がクリアされ、記録フラグ５７は“Ｈ”になる。また、図１８より通信データを送信した後は、必ず受信フラグは“Ｈ”である。
そして、他の通信装置から通信データを受信する。
この際、図１９より一送信周期後に自身が再び通信データを送信（６０ｅ）するまでの間（Ｔ３）に受信した他の通信装置２の通信データに含まれる通信装置ＩＤは、記録フラグ５７が“Ｈ”なので、第一の受信ＩＤ記憶部５５に記録される。
その後、受信フラグ５２が“Ｈ”であるので、受信した通信装置ＩＤと、第二の受信ＩＤ記憶部５６に記録されている他の通信装置ＩＤを比較する。
比較の結果、受信した通信装置ＩＤが第二の受信ＩＤ記憶部５６に記録されている他の通信装置ＩＤに含まれている場合には、受信フラグ５２はそのままで“Ｈ”である。
含まれない場合、受信フラグ５２は“Ｌに設定される。
これらの動作については実施の形態３と同様に、含まれている場合は新たなほかの通信装置が無いので、第一の認証情報を送信する必要はなく、含まれている場合には新たな他の通信装置が存在するので、第一の認証情報を送信する必要があることを意味している。
そして、通信装置１が通信データ（６０ｅ）を送信する場合、図１８より、受信フラグ５２によって第一の認証情報、もしくは第一の認証情報の識別情報を含む通信データが送信される。
通信データ（６０ｅ）を送信した後、記録フラグ５７は“Ｈ”であるので、図１８より、第二の受信ＩＤ記憶部５６がクリアされ、記録フラグ５７が“Ｌ”に設定される。
上記と同様に受信フラグ５２は“Ｈ”である。
そして、他の通信装置２の通信データを受信する。
この際、図１９より一送信周期後に自身が再び通信データを送信（６０ｆ）するまでの間（Ｔ４）に受信した他の通信装置２の通信データに含まれる通信装置ＩＤは、記録フラグ５７が“Ｌ”なので、第二の受信ＩＤ記憶部５６に記録される。
その後、同様の処理を行い、新たな他の通信装置が無い場合には受信フラグは“Ｈ”のまま、新たな他の通信装置２が存在する場合には、受信フラグ５２は“Ｌ“となる。
そして、通信データ（６０ｆ）を送信した後、受信した他の通信装置ＩＤは第一の受信ＩＤ記憶部５５に記録され、第二の受信ＩＤ記憶部５６に記録されているＩＤと比較される。
このようにして、二回前に通信データを送信した直後に受信した情報と直前に受信した情報を比較して、新たな通信装置２を検出した場合、第一の認証情報を送信し、検出しない場合は、第一の認証情報の識別情報を送信する。
【００７６】

このように、周囲に存在する通信装置の状態を考慮し、新しい通信装置が存在する場合には第一の認証情報を用いて送信し、存在しない場合には第一の認証情報の識別情報を送信する構成にしているので、効率良く必要な情報を送信することができ、かつ通信データ長を短くすることができる。

また、二回前に通信データを送信した直後に受信した情報と直前に受信した情報を比較して、新たな通信装置を検出した場合、第一の認証情報を送信し、検出しない場合は、第一の認証情報の識別情報を送信するように構成しているため、より細かく送信すべき情報を選択することができ、通信効率を向上させることができる。

さらに、第一の認証情報の識別情報を受信した際には、第二の認証情報のみ検証すればよい構成になっているので、配信情報の送信頻度を低下させずに、処理の負荷を減らすことができる。

また、第一の認証情報を送信しない場合、第一の認証情報の識別情報を第二の認証情報と共に送信しているため、複数の通信装置と通信する場合でも、通信装置では正確かつ簡単に第一の認証情報と第二の認証情報を関連付けすることができる。

さらに、受信したすべての情報に対して検証を行うのではなく、必要な情報のみ検証を行うので、効率的な検証を実施することでき、通信装置に対する処理能力の仕様を下げることができ、コスト削減が可能となる。

また、検証して正当であることを確認した第一の認証情報を記憶部に記録し、再度同じ第一の認証情報を受信した際には保有していることを確認し、第一の認証情報に有効期限がある場合にはその有効期限を確認する構成であるので、無駄な検証を省略することができ、処理の負荷を減らすことができる。

さらに、受信した配信情報を要否問わず、受信したＩＤを第一及び第二の受信ＩＤ記憶部に記録しているので、より正確な周囲に存在する通信装置の状態を把握することができ、効率的に情報を送信することができる。

また、１台でも新たな通信装置を検出した場合、検出後の比較を行わない構成にしているので、処理の負荷を低減し、効率化することができる。

【００７７】

なお、通信装置において、送信時と受信時の構成を変えてもよい。

例えば、通信部５は配信情報処理部３とのみ接続されている構成になっているが、送信時、通信部を認証情報処理部４に接続する構成にして、配信情報処理部３で生成された配信情報から認証情報処理部４で認証情報を生成し、配信情報と認証情報をあわせて通信部５から送信する構成でもよい。

また、通信部５は配信情報処理部３の配信情報と認証情報処理部４の認証情報をあわせて送信する形態でもよい。

受信時は、上記実施の形態では、配信情報処理部３で必要と判断された第二の認証情報の検証を実施していたが、通信部５から認証情報処理部４を経て、正当性が確認された配信情報のみを配信情報処理部３に送る構成にした場合、受信した通信データすべてを検証する構成にすることもできる。

また、通信装置１は、通信部５にてデータ識別情報を判断し、配信情報が無い場合には、第一の認証情報を認証情報処理部４へ送信し、配信情報がある場合には、通信データを配信情報処理部３へ送信する構成でもよい。

さらに、配信情報処理部３にあった記録フラグ５７、受信フラグ５２を認証情報処理部４に設け、第一及び第二の受信ＩＤ記憶部５５、５６を認証情報処理部４に接続する構成にしてもよい。

また、本実施の形態を適用するのは低コストがより厳しく要求される車載器のみに適用し、路側機は従来と同じ構成の路車間・車車間通信システムとしてもよい。

さらに、複数のチャネルを持つ路車間・車車間通信システムの場合、あるチャネルには第一の認証情報を送信して、別のチャネルにて配信情報、第一の認証情報の識別情報、第二の認証情報を送信してもよい。

また、配信情報を含む通信データの場合は通信データ全体もしくは配信情報のみを暗号

化を施し、配信情報を含まない第一の認証情報のみを送信する場合は暗号化をしないで送信する構成にしてもよい。

なお、本実施の形態では電源投入後、各フラグの初期値が“Ｌ”で送信から開始する構成を示したが、異なるフラグや受信から開始する場合にも適用できることは言うまでもない。

【００７８】

上述の実施の形態１～５では、

第一の認証情報を送信する場合と、第一の認証情報の識別情報、第二の認証情報、配信情報を送信する場合を分ける通信装置を説明した。

【００７９】

また、上述の実施の形態１～５では、

第一の認証情報、第二の認証情報、配信情報を送信する場合と、第一の認証情報の識別情報、第二の認証情報、配信情報を送信する場合を分ける通信装置を説明した。

【００８０】

また、上述の実施の形態１～５では、

Ｎ回に１回は第一の認証情報を送信し、残りのＮ－１回は第一の認証情報の識別情報を送信する通信装置を説明した。

【００８１】

また、上述の実施の形態１～５では、

第一の認証情報を送信した後に受信したＩＤと比較して、選択的に第一の認証情報と第一の認証情報の識別情報を送信する通信装置を説明した。

【００８２】

また、上述の実施の形態１～５では、

２回前に受信したＩＤと比較して、選択的に第一の認証情報と第一の認証情報の識別情報を送信する通信装置を説明した。

【００８３】

また、上述の実施の形態１～５では、

比較の際、新たな通信装置が１台でも存在した場合には、以降の比較処理を実施しない通信装置を説明した。

【００８４】

また、上述の実施の形態１～５では、

すべての通信データを検証せずに、選択的に検証する通信装置を説明した。

【００８５】

また、上述の実施の形態１～５では、

すでに検証済みの第一の認証情報を保有している場合、その有効期限を確認して、有効期限内であれば第二の認証情報の検証に用いて、期限切れの場合は、その第一の認証情報を削除する通信装置を説明した。

【００８６】

最後に、実施の形態１～５に示した通信装置１のハードウェア構成例について説明する。

図２８は、実施の形態１～５に示す通信装置１のハードウェア資源の一例を示す図である。

なお、図２８の構成は、あくまでも通信装置１のハードウェア構成の一例を示すものであり、通信装置１のハードウェア構成は図２８に記載の構成に限らず、他の構成であってもよい。

【００８７】

図２８において、通信装置１は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。

ＣＰＵ９１１は、バス９１２を介して、例えば、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍ

ｏｒｙ）９１３、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）９１４、通信ボード９１５、表示装置９０１、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。

また、通信装置１が車両に搭載されている場合は、例えば、入力のためのボタンやキーが配置されたコンソール９０２がＣＰＵ９１１に接続されていてもよい。

コンソール９０２はタッチパネル式であってもよい。

タッチパネル式の場合は、表示装置９０１とコンソール９０２が一体となっている。

更に、ＦＤＤ９０４（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ　Ｄｒｉｖｅ）、コンパクトディスク装置９０５（ＣＤＤ）等がＣＰＵ９１１に接続可能でもよい。

また、図示していないが、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）メモリ等であってもよい。

また、磁気ディスク装置９２０の代わりに、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）、光ディスク装置、メモリカード（登録商標）読み書き装置などの記憶装置でもよい。

ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３、ＦＤＤ９０４、ＣＤＤ９０５、磁気ディスク装置９２０の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。

実施の形態１～５で説明した「記憶部７」、「受信ＩＤ記憶部５０」、「第一の受信ＩＤ記憶部５５」及び「第二の受信ＩＤ記憶部５６」は、ＲＡＭ９１４、磁気ディスク装置９２０等により実現される。

通信ボード９１５、コンソール９０２、ＦＤＤ９０４などは、入力装置の一例である。

また、通信ボード９１５、表示装置９０１などは、出力装置の一例である。

【００８８】

通信ボード９１５は、前述したように、ＤＳＲＣの通信機能や無線ＬＡＮの通信機能を有する。

【００８９】

磁気ディスク装置９２０には、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。

プログラム群９２３のプログラムは、ＣＰＵ９１１がオペレーティングシステム９２１、ウィンドウシステム９２２を利用しながら実行する。

【００９０】

また、ＲＡＭ９１４には、ＣＰＵ９１１に実行させるオペレーティングシステム９２１のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。

また、ＲＡＭ９１４には、ＣＰＵ９１１による処理に必要な各種データが格納される。

【００９１】

また、ＲＯＭ９１３には、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）プログラムが格納され、磁気ディスク装置９２０にはブートプログラムが格納されている。

通信装置１の起動時には、ＲＯＭ９１３のＢＩＯＳプログラム及び磁気ディスク装置９２０のブートプログラムが実行され、ＢＩＯＳプログラム及びブートプログラムによりオペレーティングシステム９２１が起動される。

【００９２】

上記プログラム群９２３には、実施の形態１～５の説明において「～部」（「「記憶部７」、「受信ＩＤ記憶部５０」、「第一の受信ＩＤ記憶部５５」及び「第二の受信ＩＤ記憶部５６」以外、以下同様）として説明している機能を実行するプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

【００９３】

ファイル群９２４には、実施の形態１～５の説明において、「～の判断」、「～の生成」、「～の確認」、「～の比較」、「～の取得」、「～の更新」、「～の設定」、「～の登録」、「～の選択」、「～の入力」、「～の出力」等として説明している処理の結果を

示す情報やデータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。
「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。
ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出される。
そして、読み出された情報やデータや信号値や変数値やパラメータは、抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示などのＣＰＵの動作に用いられる。
抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示のＣＰＵの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリ、レジスタ、キャッシュメモリ、バッファメモリ等に一時的に記憶される。
また、実施の形態１～５で説明しているフローチャートの矢印の部分は主としてデータや信号の入出力を示す。
データや信号値は、ＲＡＭ９１４のメモリ、ＦＤＤ９０４のフレキシブルディスク、ＣＤＤ９０５のコンパクトディスク、磁気ディスク装置９２０の磁気ディスク、その他光ディスク、ミニディスク、ＤＶＤ等の記録媒体に記録される。
また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【００９４】

また、実施の形態１～５の説明において「～部」として説明しているものは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。
すなわち、実施の形態１～５で説明したフローチャートに示すステップ、手順、処理により、本発明に係る通信方法を実現することができる。
また、「～部」として説明しているものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。
或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。
ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、ＤＶＤ等の記録媒体に記憶される。
プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。
すなわち、プログラムは、実施の形態１～５の「～部」としてコンピュータを機能させるものである。あるいは、実施の形態１～５の「～部」の手順や方法をコンピュータに実行させるものである。

【００９５】

このように、実施の形態１～５に示す通信装置１は、処理装置たるＣＰＵ、記憶装置たるメモリ、磁気ディスク等、入力装置たるコンソール、通信ボード等、出力装置たる表示装置、通信ボード等を備えるコンピュータである。
そして、上記したように「～部」として示された機能をこれら処理装置、記憶装置、入力装置、出力装置を用いて実現するものである。

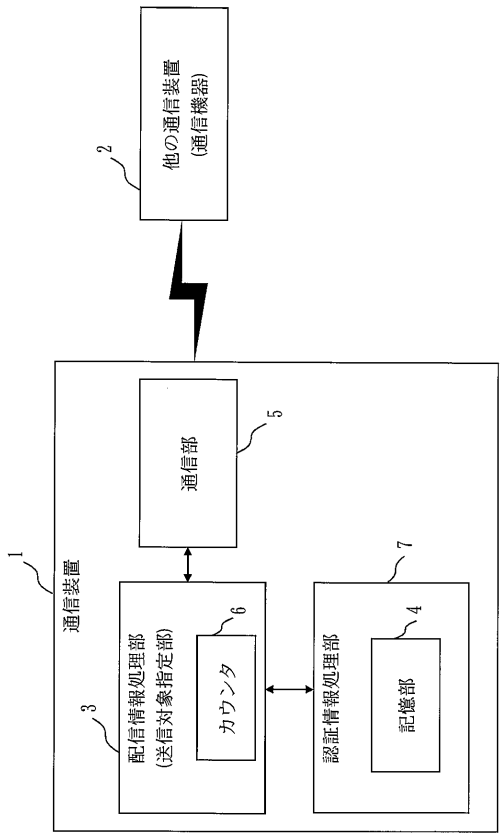
【符号の説明】

【００９６】

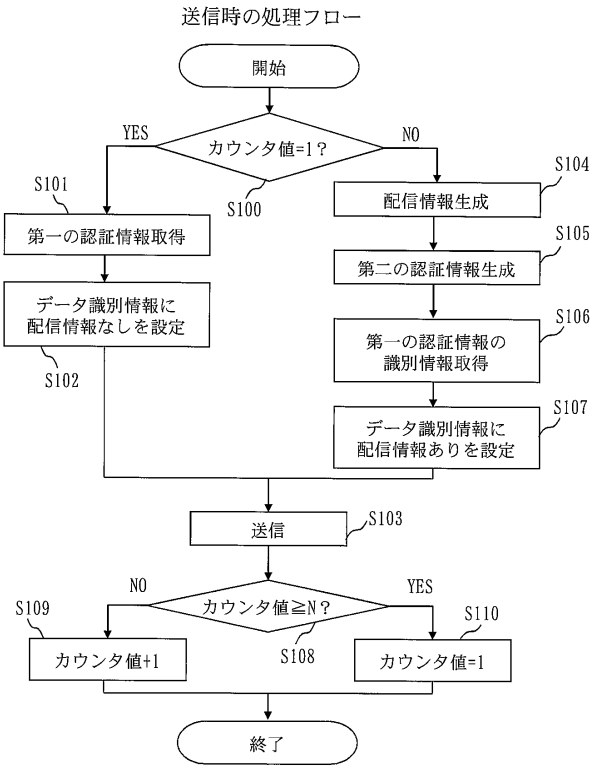
１　通信装置、２　通信装置、３　配信情報処理部、４　認証情報処理部、５　通信部、６　カウンタ、７　記憶部、２０　第一の認証情報、２１　データ識別情報、２２　配信情報、２３　第二の認証情報、２４　第一の認証情報の識別情報、３１　送信処理部、３２　受信処理部、５０　受信ＩＤ記憶部、５１　送信フラグ、５２　受信フラグ、５５

第一の受信ＩＤ記憶部、５６　第二の受信ＩＤ記憶部、５７　記録フラグ、７０　ナビゲーション装置、７１　車載器通信部、８０　車載器、８１　ナビ通信部。

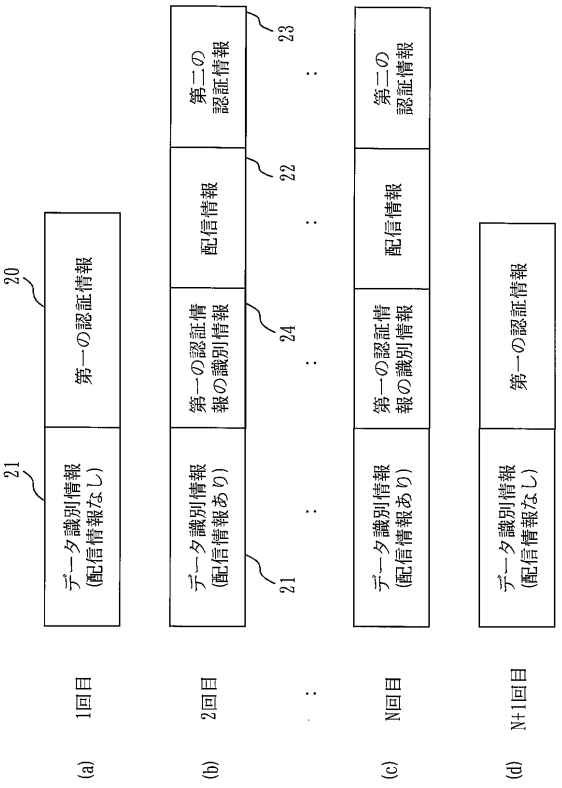
【図１】



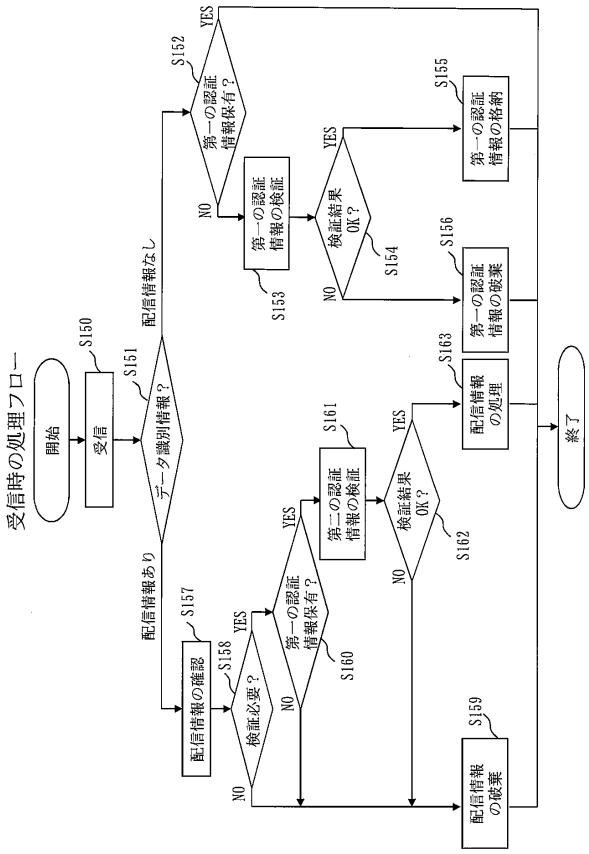
【図２】



【図３】



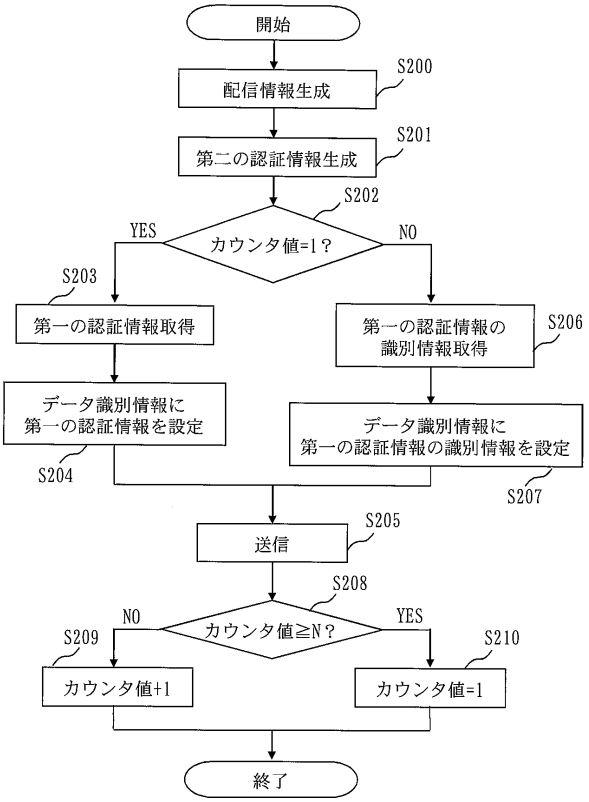
【図４】



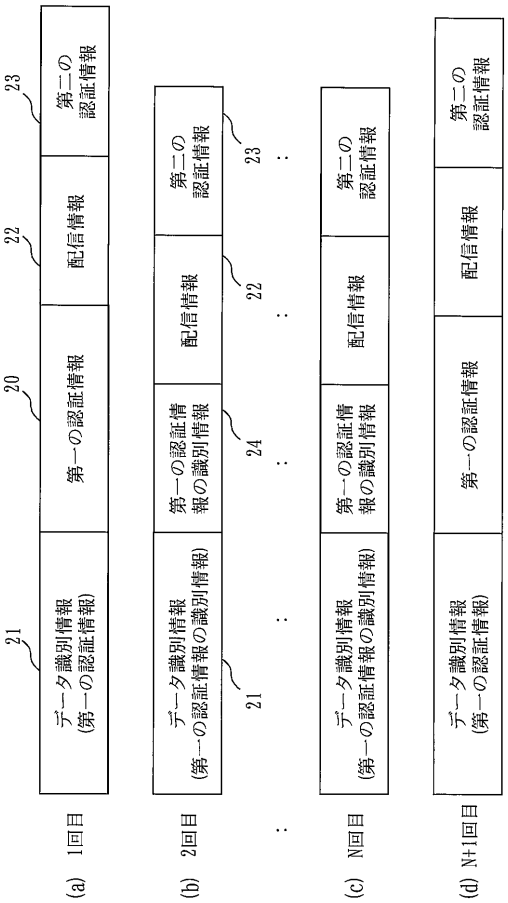
【図５】

24 第一の認証情報の識別情報	20 第一の認証情報	25 使用した日付	26 使用した回数
ID_1	第一の認証情報_1	2003/03/03 14：20：47	2
ID_2	第一の認証情報_2	2003/03/03 14：21：10	3
：	：	：	：

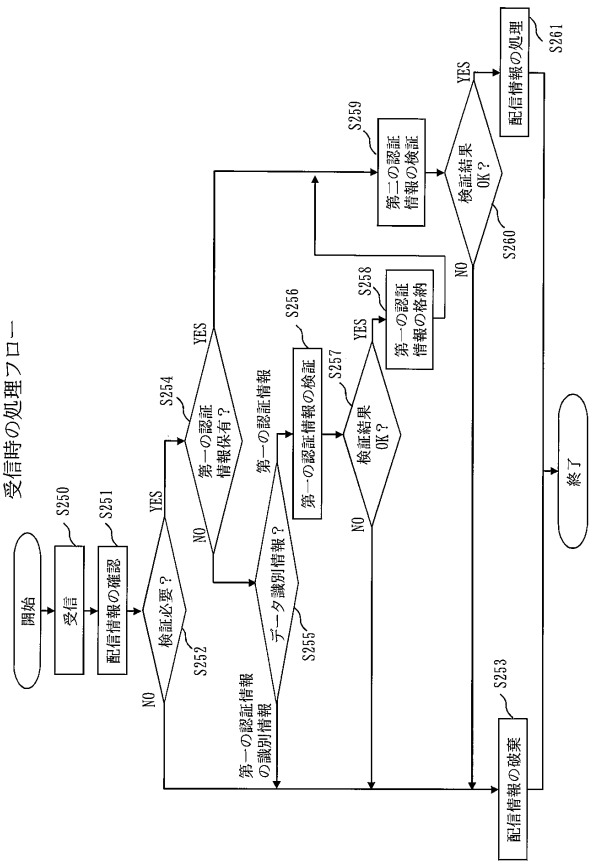
【図６】



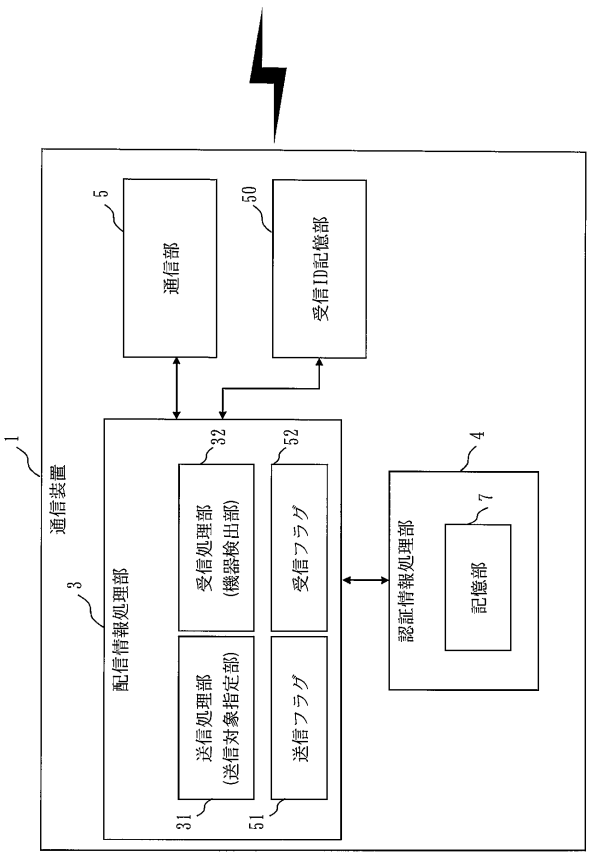
【図７】


21
20
22
23
データ識別情報
(第一の認証情報)
第一の認証情報
配信情報
第二の
認証情報
(a) 1回目
(b) 2回目
(c) N回目
(d) N+1回目
第一の認証情
報の識別情報

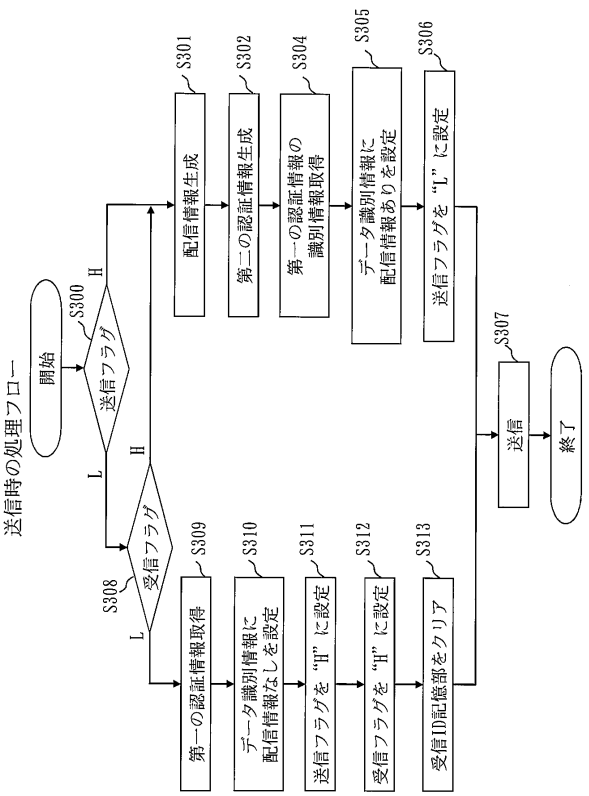
【図８】


受信時の処理フロー
開始
S250
受信
S251
配信情報の確認
検証必要？
S252
YES
NO
第一の認証情報
の識別情報
S254
第一の認証
情報保有？
YES
NO
S255
データ識別情報？
第一の認証情報
S256
第一の認証情報の検証
S257
検証結果
OK？
YES
NO
S258
第一の認証
情報の格納
S259
第二の認証
情報の検証
S260
検証結果
OK？
YES
NO
S261
配信情報の処理
S253
配信情報の破棄
終了

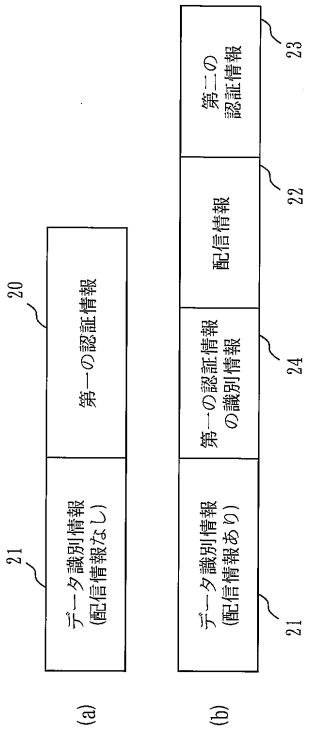
【図９】


1
通信装置
3
配信情報処理部
5
通信部
50
受信ID記憶部
32
受信処理部
(機器検出部)
52
受信フラグ
31
送信処理部
(送信対象指定部)
51
送信フラグ
4
認証情報処理部
7
記憶部

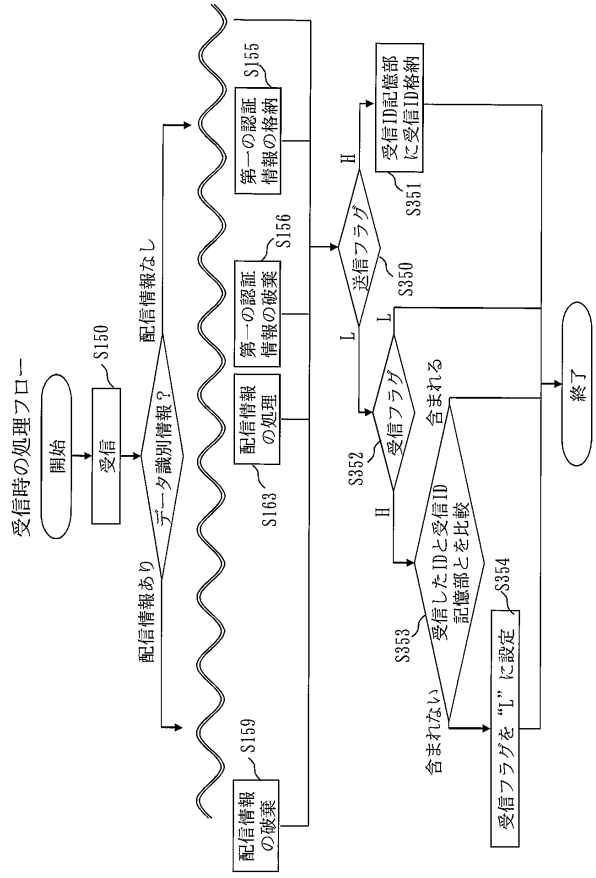
【図１０】


送信時の処理フロー
開始
S300
送信フラグ
H
L
S301
配信情報生成
S302
第二の認証情報生成
S304
第一の認証情報の
識別情報取得
S305
データ識別情報に
配信情報ありを設定
S306
送信フラグを“L”に設定
S307
送信
終了
受信フラグ
L
H
S308
S309
第一の認証情報取得
S310
データ識別情報に
配信情報なしを設定
S311
送信フラグを“H”に設定
S312
受信フラグを“H”に設定
S313
受信ID記憶部をクリア

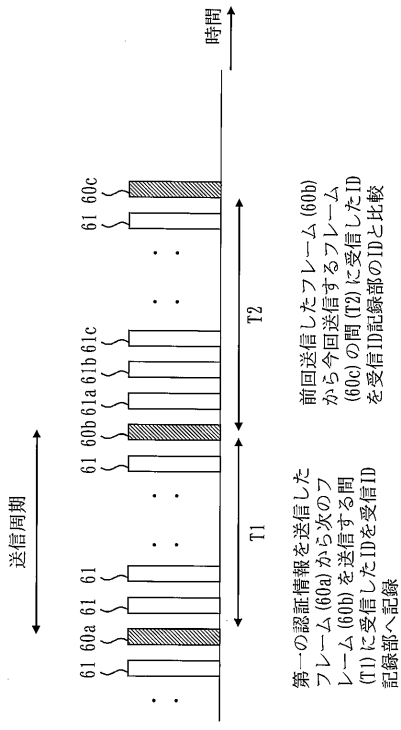
【図１１】



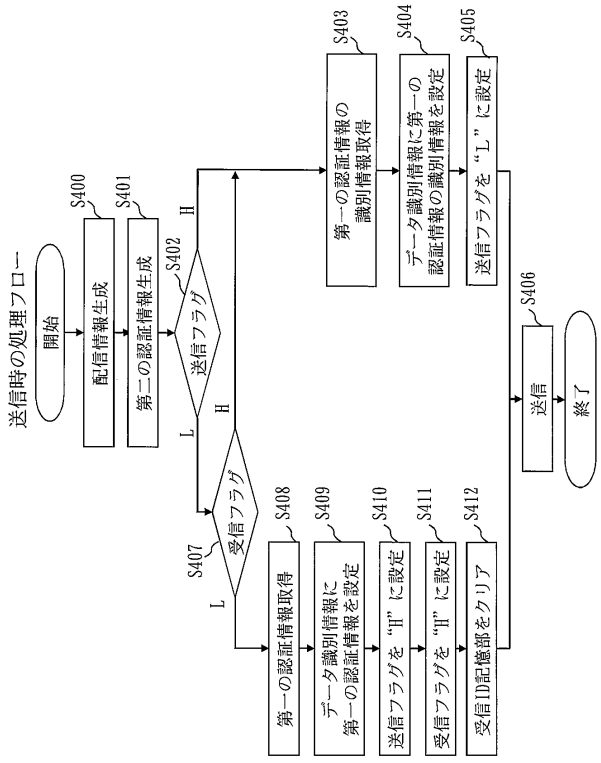
【図１２】



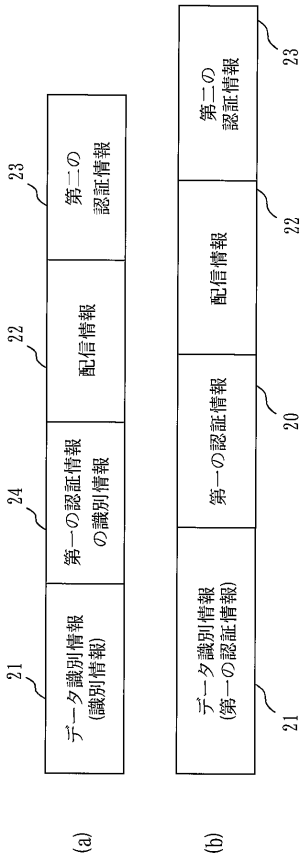
【図１３】



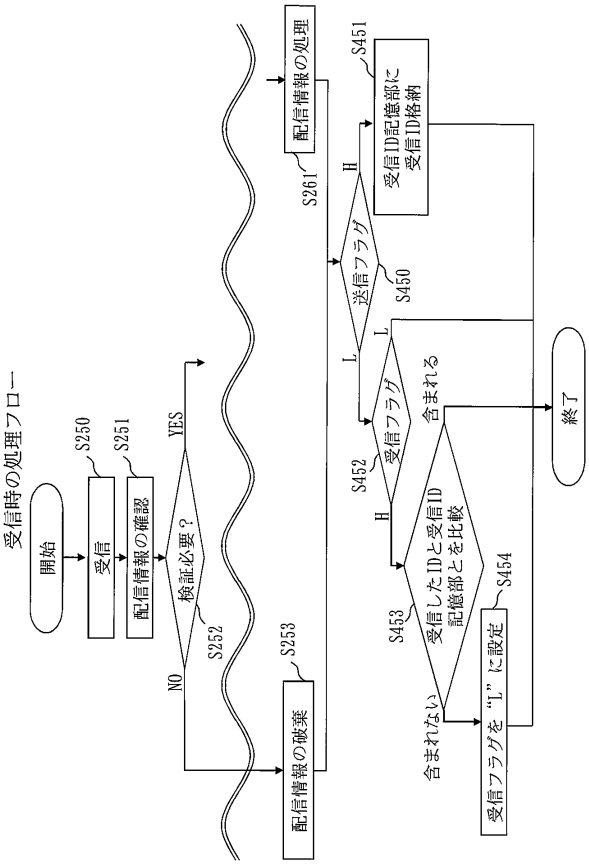
【図１４】



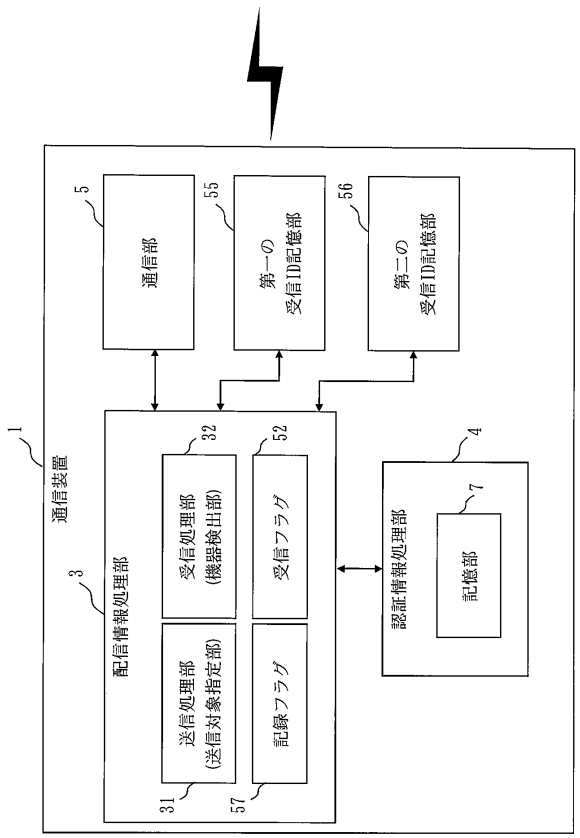
【図１５】



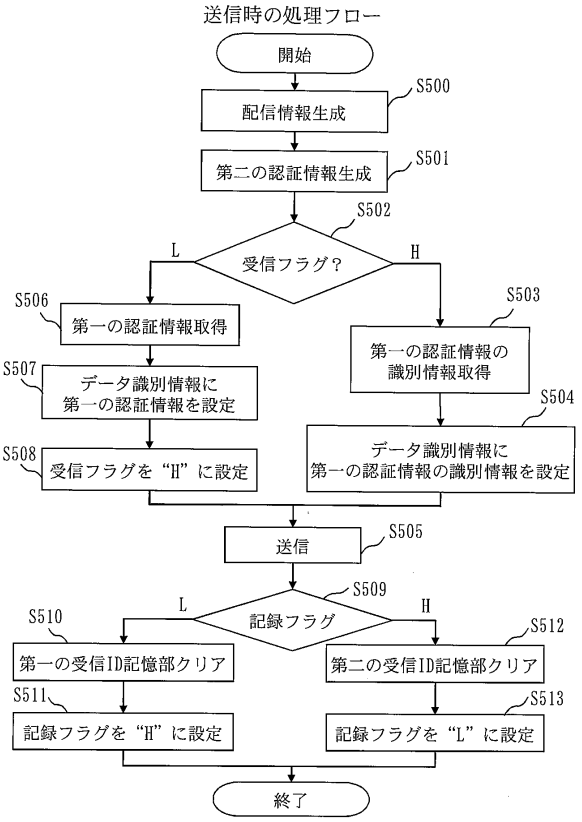
【図１６】



【図１７】



【図１８】



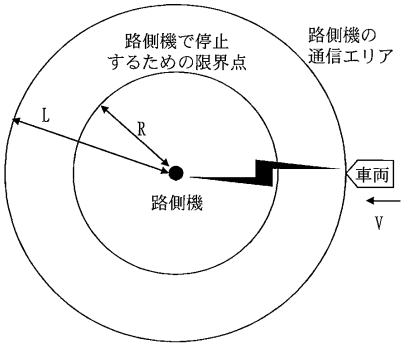
【図２１】

回数Nについて

(1) 路側機のNを通信距離や送信間隔などから算出される値以下に設定する

交差点等に設置されている路側機において、

- その通信エリアの半径 → L (m)
- その交差点で安全に停止するために、路側機から配信情報を受信しなければならない最低距離
  (想定する車両の速度や、運転者のブレーキ操作時間、車載器の表示時間等から想定) → R (m)
- 想定する車両の速度(e.g. 法定速度の2倍) → V (m/sec)
- 送信周期 → F (sec)



この時の通信回数Nを以下の式を満たす値に設定する

$N \leqq (L-R)/V/F$

例えば、L=300m、R=200m、V=20m/s(約70km/h)、F=0.05(sec) とすると、Nを25回以下に設定

また、上の発展形として、本通信システムのパケット到達率をPとした時、通信回数Nを以下の式を満たす値に設定する

$N \leqq (L-R)/V/F \times P$

上記例において、P=0.8(80%)とすると、Nを20回以下に設定

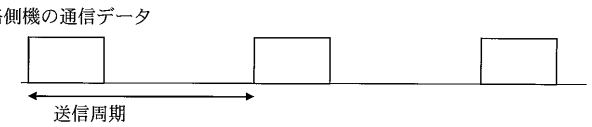
【図２２】

回数Nについて

(2) 路側機は、配信情報を分割して送信することを想定して、分割した先頭の通信データには
第一の認証情報を、他の通信データには第一の認証情報の識別情報を設定

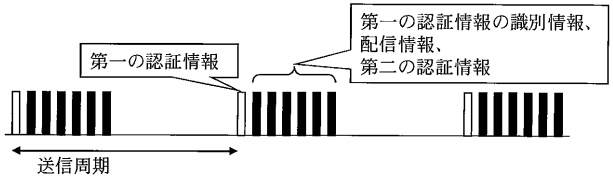
路側機の配信情報が車載器に比べて長い場合、1つの配信情報を分割(M分割)して送信する場合もありうる。

■実施の形態1の
通信イメージ



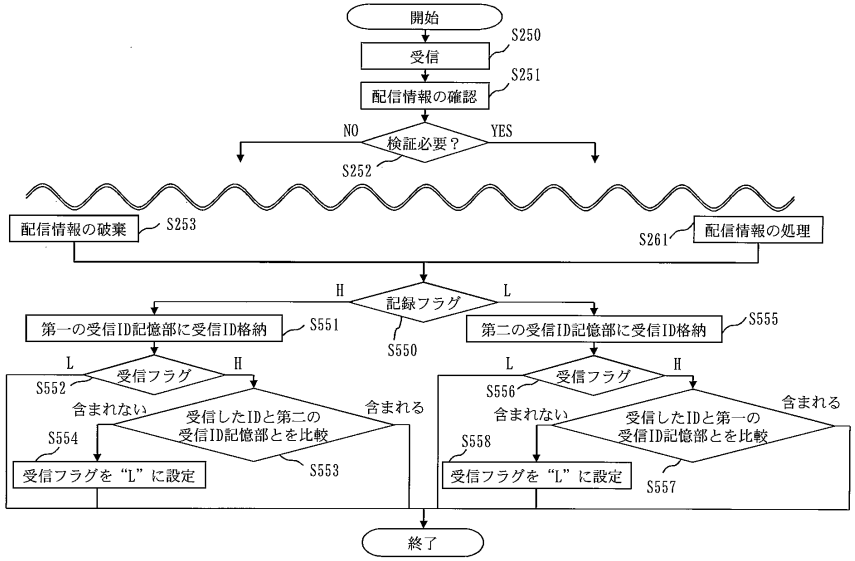
■路側機の配信情報を
M分割して連続的に送信

M+1回のデータ送信
(N=M+1)

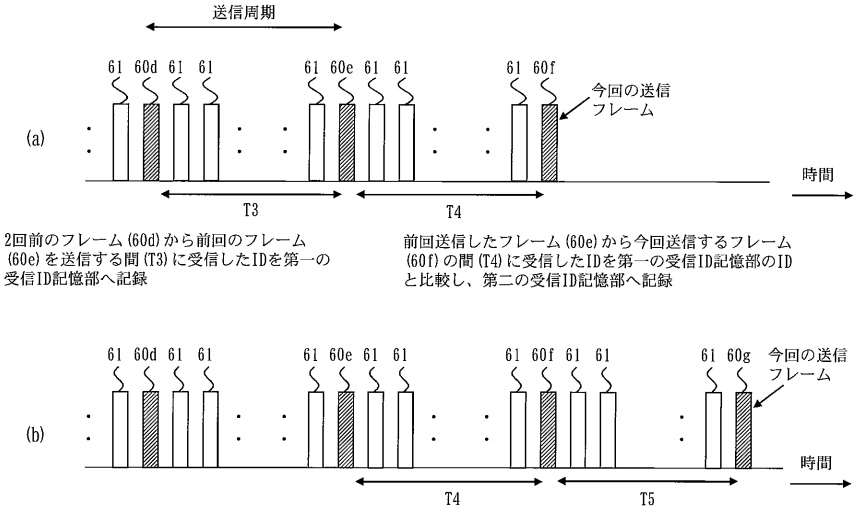


【図１９】

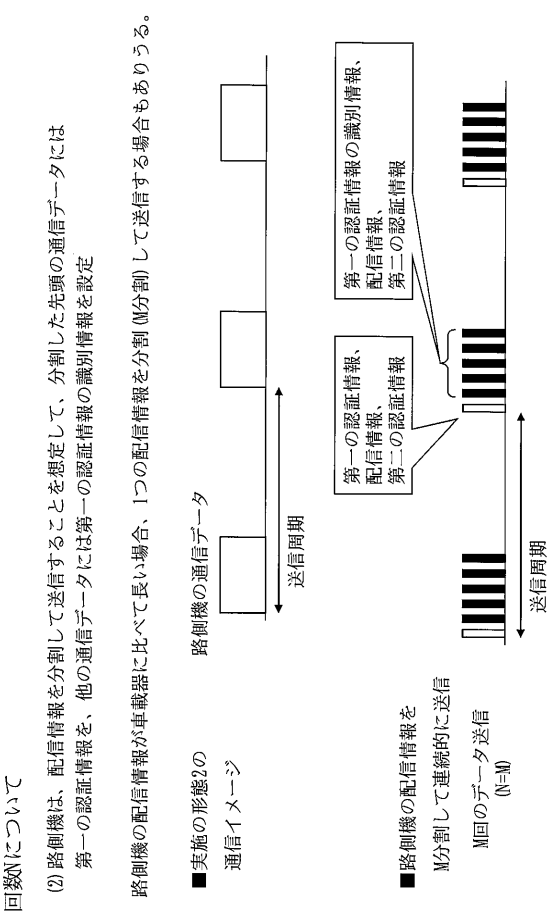
受信時の処理フロー



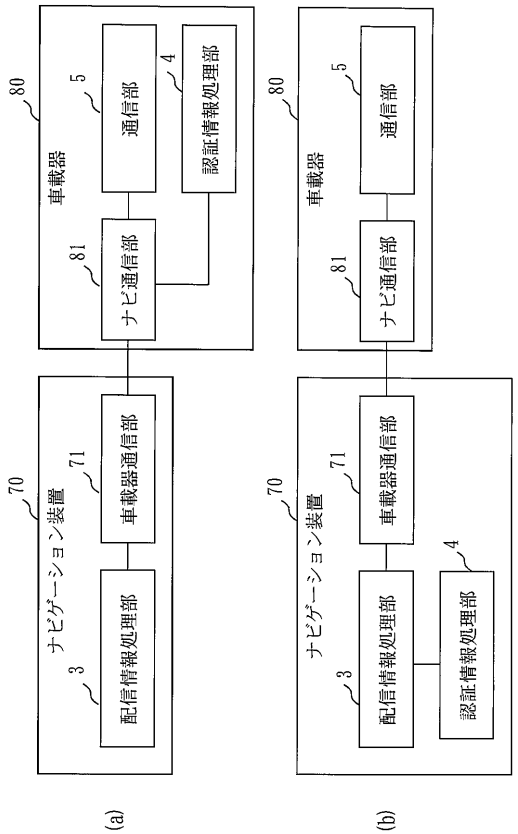
【図２０】



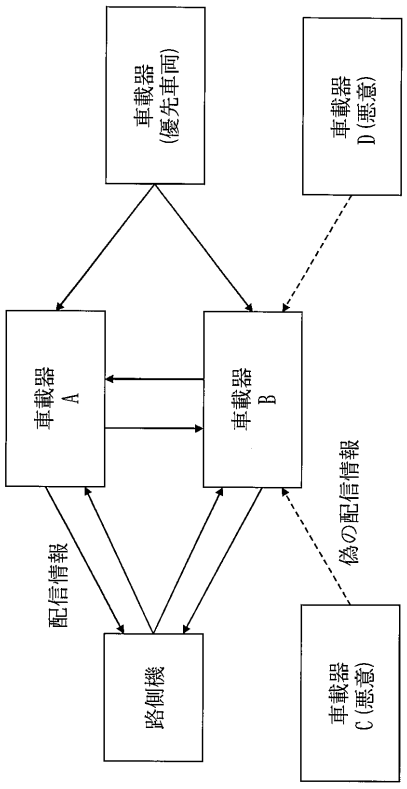
【図２３】



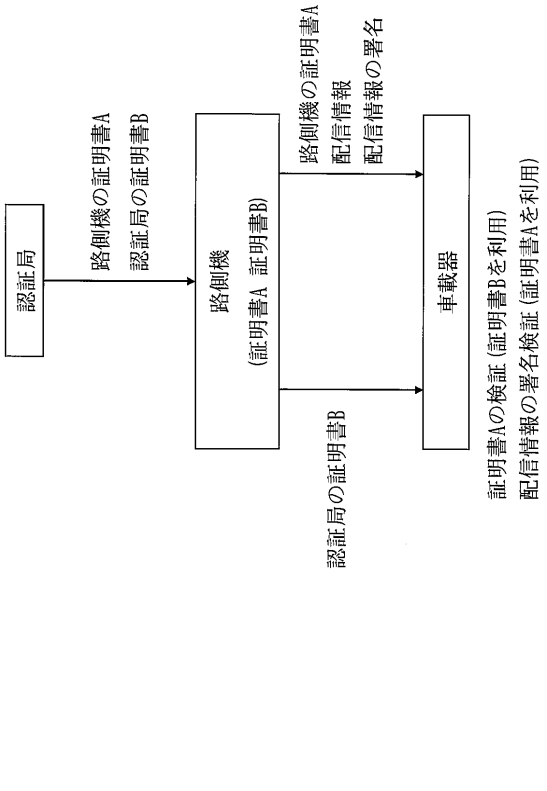
【図２４】



【図２５】



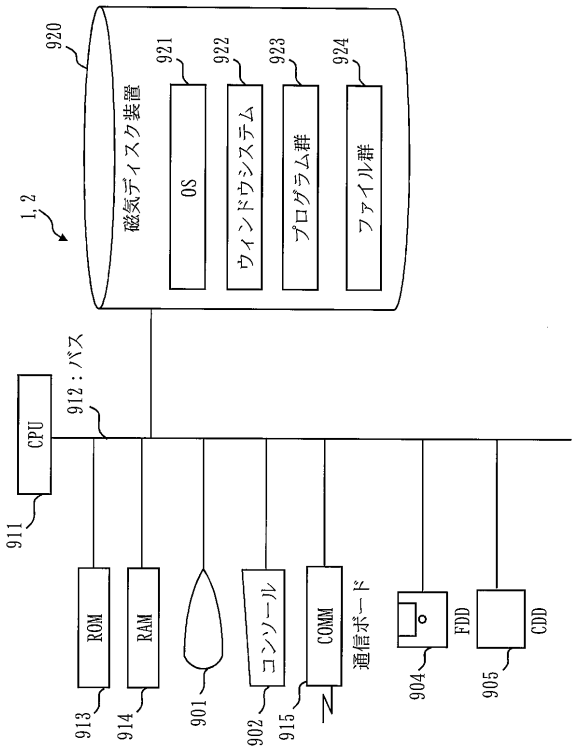
【図２６】



【図２７】


公開鍵証明書A
配信情報
配信情報の署名

【図２８】


920
磁気ディスク装置
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
1.2
CPU
911
912：バス
ROM
913
RAM
914
901
コンソール
902
COMM
915
通信ボード
FDD
904
CDD
905

フロントページの続き

(51)Int.Cl.　　ＦＩ
　　Ｇ０８Ｇ　1/09　　Ｆ

(72)発明者　佐藤　恒夫
　　東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　桑原　聡一

(56)参考文献　特開２００７－０８８７３７（ＪＰ，Ａ）
　　特開２００４－１６８０５２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｂ　７／２４－７／２６
　　Ｈ０４Ｗ　４／００－９９／００
　　Ｇ０９Ｃ　１／００－５／００
　　Ｈ０４Ｋ　１／００－３／００
　　Ｈ０４Ｌ　９／００－９／３８
　　Ｇ０８Ｇ　１／００－９９／００