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

特許第4722945号
(P4722945)

(45)発行日　平成23年7月13日(2011.7.13)　(24)登録日　平成23年4月15日(2011.4.15)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G06Q 50/00	(2006.01)	H04L	9/00	601E
G06Q 30/00	(2006.01)	G06F	17/60	142
G06Q 10/00	(2006.01)	G06F	17/60	302E
		G06F	17/60	512

請求項の数 14　(全 25 頁)

(21)出願番号　特願2007-551853 (P2007-551853)
(86)(22)出願日　平成18年8月24日 (2006.8.24)
(86)国際出願番号　PCT/JP2006/316623
(87)国際公開番号　WO2007/074557
(87)国際公開日　平成19年7月5日 (2007.7.5)
審査請求日　平成20年2月14日 (2008.2.14)
(31)優先権主張番号　特願2005-372721 (P2005-372721)
(32)優先日　平成17年12月26日 (2005.12.26)
(33)優先権主張国　日本国(JP)

(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　100123434
弁理士　田澤　英昭
(74)代理人　100101133
弁理士　濱田　初音
(72)発明者　子安　健彦
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　河野　篤
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】コンテンツ配信システムおよび端末およびサーバ

(57)【特許請求の範囲】

【請求項１】

コンテンツ暗号化鍵によって暗号化されたコンテンツが記憶された第１記録媒体と、

持ち運び可能な第２記録媒体と、

前記第１記録媒体および前記第２記録媒体の着脱が可能な端末と、

前記第２記録媒体の着脱が可能な通信装置と、

前記通信装置にネットワークを介して接続されるサーバ

とを備えたコンテンツ配信システムにおいて、

前記端末は、

通信鍵を生成する鍵生成部と、

前記サーバに記憶された秘密鍵と対をなす公開鍵を記憶する公開鍵記憶部と、

当該端末が有するＩＤと前記鍵生成部で生成された通信鍵とを、前記公開鍵記憶部に記憶されている公開鍵によって暗号化して第１暗号データを生成するＩＤ暗号化部と、

前記第２記録媒体が装着されることにより、前記ＩＤ暗号化部で生成された第１暗号データを該第２記録媒体に書き込む書込部と、

前記通信装置によって第２暗号データが書き込まれた第２記録媒体が装着されることにより、該第２記録媒体から第２暗号データを読み出す読出部と、

前記読出部で読み出された第２暗号データを前記鍵生成部で生成された通信鍵で復号する鍵復号部と、

前記第１記録媒体が装着されることにより、前記鍵復号部で復号することにより得られ

たコンテンツ復号鍵を用いて該第１記録媒体に記憶されているコンテンツを復号するコンテンツ復号部
とを備え、
前記通信装置は、
前記端末において第１暗号データが書き込まれた第２記録媒体の装着に応答して該第２記録媒体から第１暗号データを読み出して前記サーバに送信することによりライセンス取得要求を行い、且つ、該ライセンス取得要求に応答して前記サーバから送信されてくる第２暗号データを受信して前記第２記録媒体に書き込む制御部
を備え、
前記サーバは、
前記端末に記憶された公開鍵と対をなす秘密鍵を記憶する秘密鍵記憶部と、
コンテンツ復号鍵を記憶する鍵記憶部と、
前記通信装置からネットワークを介してライセンス取得要求として送信されてくる第１暗号データを受信する受信部と、
前記受信部で受信された第１暗号データを、前記秘密鍵記憶部に記憶されている秘密鍵で復号するＩＤ復号部と、
前記鍵記憶部に記憶されているコンテンツ復号鍵を、前記ＩＤ復号部で復号することにより得られた通信鍵によって暗号化して第２暗号データを生成する鍵暗号化部と、
前記鍵暗号化部で生成された第２暗号データを、前記ライセンス取得要求に対する応答として、前記通信装置に送信する送信部
とを備えたコンテンツ配信システム。
【請求項２】
通信鍵を生成する鍵生成部と、
サーバに記憶された秘密鍵と対をなす公開鍵を記憶する公開鍵記憶部と、
当該端末が有するＩＤと前記鍵生成部で生成された通信鍵とを、前記公開鍵記憶部に記憶されている公開鍵によって暗号化して第１暗号データを生成するＩＤ暗号化部と、
持ち運び可能な第２記録媒体が装着されることにより、前記ＩＤ暗号化部で生成された第１暗号データを該第２記録媒体に書き込む書込部と、
前記サーバで生成された第２暗号データが書き込まれた第２記録媒体が装着されることにより、該第２記録媒体から第２暗号データを読み出す読出部と、
前記読出部で読み出された第２暗号データを前記鍵生成部で生成された通信鍵で復号する鍵復号部と、
コンテンツ暗号化鍵によって暗号化されたコンテンツが記憶された第１記録媒体が装着されることにより、前記鍵復号部で復号することにより得られたコンテンツ復号鍵を用いて該第１記録媒体に記憶されているコンテンツを復号するコンテンツ復号部
とを備えた端末。
【請求項３】
端末が有するＩＤは、第１記録媒体に付与されたＩＤである
ことを特徴とする請求項２記載の端末。
【請求項４】
端末が有するＩＤは、当該端末に付与されたＩＤである
ことを特徴とする請求項２記載の端末。
【請求項５】
端末が有するＩＤは、第１記録媒体に付与されたＩＤおよび当該端末に付与されたＩＤから成る
ことを特徴とする請求項２記載の端末。
【請求項６】
書込部は、コンテンツ復号部によって前記第１記録媒体に記録されているコンテンツが復号された後に、第２記録媒体に記憶されている内容を消去する
ことを特徴とする請求項２記載の端末。

【請求項７】
鍵生成部で生成された通信鍵を記憶する鍵記憶部を備え、
前記鍵復号部は、読出部で読み出された第２暗号データを前記鍵記憶部に記憶されている通信鍵で復号し、
前記コンテンツ復号部は、コンテンツを復号した後に、前記鍵記憶部に記憶されている内容を消去する
ことを特徴とする請求項２記載の端末。
【請求項８】
秘密鍵を記憶する秘密鍵記憶部と、
第１記録媒体に記憶されているコンテンツを復号するために用いられるコンテンツ復号鍵を記憶する鍵記憶部と、
前記秘密鍵と対をなす公開鍵によって暗号化された第１暗号データが記憶された第２記録媒体が装着された通信装置からライセンス取得要求として送信されてくる、該第１暗号データを受信する受信部と、
前記受信部で受信された第１暗号データを、前記秘密鍵記憶部に記憶されている秘密鍵で復号するＩＤ復号部と、
前記鍵記憶部に記憶されているコンテンツ復号鍵を、前記ＩＤ復号部で復号することにより得られた通信鍵によって暗号化して第２暗号データを生成する鍵暗号化部と、
前記鍵暗号化部で生成された第２暗号データを、前記ライセンス取得要求に対する応答として、前記通信装置に送信する送信部
とを備えたサーバ。
【請求項９】
送信部は、ＩＤ復号部により第１暗号データが復号された後に、通信装置に消去指令を送信することにより、該通信装置に装着された第２記録媒体に書き込まれている第１暗号データを消去させ、その後、鍵暗号化部で生成された第２暗号データを前記通信装置に送信する
ことを特徴とする請求項８記載のサーバ。
【請求項１０】
端末のＩＤ、該端末のＩＤの使用可否を表す情報および通信鍵を記憶するＩＤ記憶部を備え、
鍵暗号化部は、ＩＤ復号部で復号することにより得られたＩＤおよび通信鍵が前記ＩＤ記憶部に記憶されているＩＤおよび通信鍵とそれぞれ一致する場合、または、前記ＩＤ復号部で復号することにより得られたＩＤが前記ＩＤ記憶部に記憶されている使用可否の情報により使用可になっている場合に、鍵記憶部に記憶されているコンテンツ復号鍵を、前記通信鍵によって暗号化して第２暗号データを生成する
ことを特徴とする請求項８記載のサーバ
【請求項１１】
端末のＩＤは、第１記録媒体に付与されたＩＤである
ことを特徴とする請求項１０記載のサーバ。
【請求項１２】
端末のＩＤは、端末に付与されたＩＤである
ことを特徴とする請求項１０記載のサーバ。
【請求項１３】
端末のＩＤは、第１記録媒体に付与されたＩＤおよび端末に付与されたＩＤから成る
ことを特徴とする請求項１０記載のサーバ。
【請求項１４】
鍵記憶部は、複数のコンテンツ復号鍵を記憶し、
鍵暗号化部は、
前記鍵記憶部に記憶された複数のコンテンツ復号鍵のいずれかを、ＩＤ復号部で復号することにより得られたＩＤまたは通信鍵に応じて選択し、該選択したコンテンツ復号鍵を

通信鍵によって暗号化する
ことを特徴とする請求項１０記載のサーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、サーバからユーザの端末にコンテンツを配信するコンテンツ配信システムおよび端末およびサーバに関し、特に、通信機能を使用できない端末にコンテンツを配信する技術に関する。
【背景技術】
【０００２】
近年、インターネットの普及や記憶メディアの性能向上と低価格化に伴い、音楽データやプログラムデータといった大容量のコンテンツを記憶メディアに書き込んでユーザに配布し、その記憶メディアに記憶されているコンテンツを利用する権利として与えられる鍵は、ユーザがインターネットを介して専用のサーバに接続し、該サーバから通信により取得するといったコンテンツ配信システムが利用されている。
【０００３】
このようなコンテンツ配信システムとして、例えば特許文献１は、携帯端末プレーヤ対応のコンテンツ配信システムを開示している。この特許文献１に開示されたコンテンツ配信システムは、コンテンツサーバとユーザのダウンロード情報および権利情報を含むユーザ情報データベースとを備えて通信網を介してＳＤＭＩのチェックイン・チェックアウトルールで配信を行うコンテンツプロバイダと、記録媒体にダウンロードしたコンテンツを再生する記録媒体再生機能と再生できる権利をコンテンツプロバイダへ戻すチェックイン機能を備えたユーザの携帯端末プレーヤと、から構成されている。コンテンツプロバイダは携帯端末プレーヤへの配信の際に、ユーザに対するコンテンツのチェックアウト数の管理を行い、ユーザが配信されたコンテンツをチェックインする場合に、携帯端末プレーヤは当該コンテンツ再生の暗号化鍵およびファイル名登録を消去するようにしてコンテンツ配信管理を行う。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００２－８３１５２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
上述した特許文献１に開示されたコンテンツ配信システムは、コンテンツ配信管理を行うコンテンツプロバイダに対して、コンテンツを利用する権利として与えられる鍵の取得や返送を通信によって行うように構成されているので、コンテンツを利用する機器が通信機能を有することが前提である。したがって、通信機能を使用できない機器では、このようなコンテンツ配信システムを利用することができない。
【０００６】
今、上記のようなコンテンツ配信システムをカーナビゲーション装置に適用することを考える。近年の殆どのカーナビゲーション装置は通信機能を有するが、多くのカーナビゲーション装置では、通信手段として携帯電話が使用されている。ところが、携帯電話とカーナビゲーション装置とでは、それらの使用期間（使用サイクル）に大きな差があるので、ユーザが携帯電話を買い換えることによって、その携帯電話をカーナビゲーション装置の通信手段として使用できなくなることがある。また、携帯電話とカーナビゲーション装置との接続には専用のケーブルが必要な場合があり、ケーブルがないためにカーナビゲーション装置の通信機能を使用していないユーザもいる。このような現状にあって、カーナビゲーション装置に対して上述したコンテンツ配信システムをそのまま適用することは難しいという問題がある。

【０００７】
この発明は、上述した問題を解決するためになされたものであり、その課題は、通信機能を有しない端末に対して安全に鍵を配布してコンテンツを利用可能にするコンテンツ配信システムおよび端末およびサーバを提供することにある。
【課題を解決するための手段】
【０００８】
上記課題を解決するために、この発明に係るコンテンツ配信システムは、コンテンツ暗号化鍵によって暗号化されたコンテンツが記憶された第１記録媒体と、持ち運び可能な第２記録媒体と、第１記録媒体および第２記録媒体の着脱が可能な端末と、第２記録媒体の着脱が可能な通信装置と、通信装置にネットワークを介して接続されるサーバとを備えたコンテンツ配信システムにおいて、端末は、通信鍵を生成する鍵生成部と、サーバに記憶された秘密鍵と対をなす公開鍵を記憶する公開鍵記憶部と、当該端末が有するＩＤと鍵生成部で生成された通信鍵とを、公開鍵記憶部に記憶されている公開鍵によって暗号化して第１暗号データを生成するＩＤ暗号化部と、第２記録媒体が装着されることにより、ＩＤ暗号化部で生成された第１暗号データを該第２記録媒体に書き込む書込部と、通信装置によって第２暗号データが書き込まれた第２記録媒体が装着されることにより、該第２記録媒体から第２暗号データを読み出す読出部と、読出部で読み出された第２暗号データを鍵生成部で生成された通信鍵で復号する鍵復号部と、第１記録媒体が装着されることにより、鍵復号部で復号することにより得られたコンテンツ復号鍵を用いて該第１記録媒体に記憶されているコンテンツを復号するコンテンツ復号部とを備え、通信装置は、端末において第１暗号データが書き込まれた第２記録媒体の装着に応答して該第２記録媒体から第１暗号データを読み出してサーバに送信することによりライセンス取得要求を行い、且つ、該ライセンス取得要求に応答してサーバから送信されてくる第２暗号データを受信して第２記録媒体に書き込む制御部を備え、サーバは、端末に記憶された公開鍵と対をなす秘密鍵を記憶する秘密鍵記憶部と、コンテンツ復号鍵を記憶する鍵記憶部と、通信装置からネットワークを介してライセンス取得要求として送信されてくる第１暗号データを受信する受信部と、受信部で受信された第１暗号データを、秘密鍵記憶部に記憶されている秘密鍵で復号するＩＤ復号部と、鍵記憶部に記憶されているコンテンツ復号鍵を、ＩＤ復号部で復号することにより得られた通信鍵によって暗号化して第２暗号データを生成する鍵暗号化部と、鍵暗号化部で生成された第２暗号データを、ライセンス取得要求に対する応答として、通信装置に送信する送信部とを備えている。
【発明の効果】
【０００９】
この発明に係るコンテンツ配信システムによれば、ネットワークへの接続ができない端末であっても、第２記録媒体を用いることにより、ライセンスを管理するサーバと通信装置を経由して通信し、第１記録媒体に記憶されている暗号化されたデータを復号するためのコンテンツ復号鍵を取得することができるので、サーバは安全にコンテンツ復号鍵を配布することができる。したがって、通信機能を有しない端末であってもコンテンツを利用することが可能になる。
【図面の簡単な説明】
【００１０】
【図１】この発明の実施の形態１に係るコンテンツ配信システムの構成を示すブロック図である。
【図２】この発明の実施の形態１に係るコンテンツ配信システムを構成するカーナビゲーション装置の詳細な構成を示すブロック図である。
【図３】この発明の実施の形態１に係るコンテンツ配信システムを構成するパーソナルコンピュータの詳細な構成を示すブロック図である。
【図４】この発明の実施の形態１に係るコンテンツ配信システムを構成するサーバの詳細な構成を示すブロック図である。
【図５】この発明の実施の形態１に係るコンテンツ配信システムを構成するサーバで使用

されるライセンス管理リストを示す図である。
【図６】この発明の実施の形態１に係るコンテンツ配信システムの動作を示すシーケンスチャートである。
【図７】この発明の実施の形態１に係るコンテンツ配信システムを構成するサーバで実行されるライセンス確認処理の詳細を示すフローチャートである。
【図８】この発明の実施の形態２に係るコンテンツ配信システムを構成するサーバで使用されるライセンス管理リストを示す図である。
【図９】この発明の実施の形態２に係るコンテンツ配信システムを構成するサーバで実行されるライセンス確認処理の詳細を示すフローチャートである。
【図１０】この発明の実施の形態３に係るコンテンツ配信システムを構成するサーバで使用されるライセンス管理リストを示す図である。
【図１１】この発明の実施の形態３に係るコンテンツ配信システムを構成するサーバで実行されるライセンス確認処理の詳細を示すフローチャートである。
【図１２】この発明の実施の形態４に係るコンテンツ配信システムを構成するサーバで使用されるライセンス管理リストを示す図である。
【図１３】この発明の実施の形態４に係るコンテンツ配信システムを構成するサーバで実行されるライセンス確認処理の詳細を示すフローチャートである。
【図１４】この発明の実施の形態５に係るコンテンツ配信システムを構成するサーバで使用されるライセンス管理リストを示す図である。
【図１５】この発明の実施の形態５に係るコンテンツ配信システムを構成するサーバで実行されるライセンス確認処理の詳細を示すフローチャートである。
【図１６】この発明の実施の形態６に係るコンテンツ配信システムを構成するサーバで使用されるライセンス管理リストを示す図である。
【図１７】この発明の実施の形態７に係るコンテンツ配信システムを構成するサーバで実行されるライセンス確認処理の詳細を示すフローチャートである。
【発明を実施するための形態】
【００１１】
以下、この発明をより詳細に説明するために、この発明を実施するための形態について、添付の図面に従って説明する。
実施の形態１.
図１は、この発明の実施の形態１に係るコンテンツ配信システムの構成を示すブロック図である。このコンテンツ配信システムは、ＤＶＤ（Digital Versatile Disk）１、ＰＣカード（PC Card）２、カーナビゲーション装置１０、パーソナルコンピュータ２０、ネットワーク３０およびサーバ４０から構成されている。ネットワーク３０としては、例えばインターネットが使用される。
【００１２】
ＤＶＤ１は、この発明の第１記録媒体に対応し、ナビゲーション用の地図を更新するための地図更新データがデータ保護用の鍵Ｋｃｒｙによって暗号化された暗号化地図更新データ（コンテンツ）を記憶している。ここで、鍵Ｋｃｒｙは、この発明のコンテンツ暗号化鍵およびコンテンツ復号鍵に対応し、コンテンツを暗号化する時はコンテンツ暗号化鍵、コンテンツを復号する時はコンテンツ復号鍵と呼ばれる。また、ＤＶＤ１には、ライセンスを管理するための固有のシリアル番号が付されており、このシリアル番号は、所有者ＩＤとして使用される。このＤＶＤ１は、カーナビゲーション装置１０に装着される。
【００１３】
ＰＣカード２は、この発明の第２記録媒体に対応し、カーナビゲーション装置１０およびパーソナルコンピュータ２０の双方に着脱可能になっている。カーナビゲーション装置１０およびパーソナルコンピュータ２０は、ＰＣカード２が装着された場合に、この装着されたＰＣカード２にデータを書き込み、また、ＰＣカード２からデータを読み出すことができる。
【００１４】

カーナビゲーション装置１０は、この発明の端末に対応し、自己が保持している地図データを、ＤＶＤ１によって配布される暗号化地図更新データを復号して得られる地図更新データを用いて更新する。図２は、カーナビゲーション装置１０の詳細な構成を示すブロック図である。このカーナビゲーション装置１０は、ディスクドライブ１１、ＰＣスロット１２、公開鍵記憶部１３、地図データ記憶部１４、入力部１５、制御部１６および鍵記憶部１７を備えている。

【００１５】

ディスクドライブ１１は、ＤＶＤ１が装着された場合に、該ＤＶＤ１に記憶されている内容を読み取って制御部１６に送る。ＰＣスロット１２にはＰＣカード２が着脱される。このＰＣスロット１２に装着されたＰＣカード２には、詳細は後述するが、制御部１６から第１暗号データＸが書き込まれるとともに、ＰＣカード２に記憶されている第２暗号データＹが制御部１６によって読み取られる。

【００１６】

公開鍵記憶部１３は、例えばＨＤＤ（Hard Disk Drive）の一部によって構成されている。この公開鍵記憶部１３には、当該カーナビゲーション装置１０の製造時に、サーバ４０に保持されている秘密鍵Ｓｐｒｉと対をなす公開鍵Ｓｐｕｂが格納される。したがって、カーナビゲーション装置１０が製品としてユーザに届いた時点では、既に公開鍵Ｓｐｕｂは公開鍵記憶部１３に記憶された状態にある。この公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂは、制御部１６によって読み出される。

【００１７】

地図データ記憶部１４は、例えばＨＤＤの他の一部によって構成されており、ナビゲーション用の地図を表示するための地図データを記憶する。この地図データ記憶部１４に記憶されている地図データは、制御部１６から送られてくる地図更新データによって更新される。入力部１５は、例えばリモートコントローラ、タッチパネル、操作ボタンまたは音声入力装置などから構成されており、ユーザがシリアル番号を入力するために使用される。この入力部１５から入力されたシリアル番号は、制御部１６に送られる。

【００１８】

制御部１６は、例えばマイクロコンピュータから構成されている。この制御部１６は、例えばマイクロコンピュータによるソフトウェア処理によって実現された鍵生成部１６１、ＩＤ暗号化部１６２、ＰＣカード書込部１６３、ＰＣカード読出部１６４、鍵復号部１６５およびコンテンツ復号部１６６から構成されている。ＰＣカード書込部１６３は、この発明の書込部に対応し、ＰＣカード読出部１６４は、この発明の読出部に対応する。

【００１９】

鍵生成部１６１は、自己を特定するための鍵Ｋｃｏｍを生成する。この鍵Ｋｃｏｍは、この発明の通信鍵に対応し、カーナビゲーション装置１０がＤＶＤ１に記憶されている暗号化地図更新データを復号するための鍵Ｋｃｒｙをサーバ４０から取得する際に、サーバ４０において鍵Ｋｃｒｙを暗号化する鍵として使用される。この鍵生成部１６１で生成された鍵Ｋｃｏｍは、ＩＤ暗号化部１６２および鍵記憶部１７に送られる。

【００２０】

ＩＤ暗号化部１６２は、入力部１５から所有者ＩＤとして入力されたＤＶＤ１のシリアル番号と鍵生成部１６１から送られてくる鍵Ｋｃｏｍとを、公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂによって暗号化することにより第１暗号データＸを生成し、ＰＣカード書込部１６３に送る。ＰＣカード書込部１６３は、ＩＤ暗号化部１６２から送られてきた第１暗号データＸを、ＰＣスロット１２に装着されたＰＣカード２に書き込む。

【００２１】

ＰＣカード読出部１６４は、ＰＣスロット１２に装着されたＰＣカード２に記憶されている第２暗号データＹ（サーバ４０によって生成されて通信装置２０によって書き込まれる）を読み出し、鍵復号部１６５に送る。鍵復号部１６５は、ＰＣカード読出部１６４から送られてくる第２暗号データＹを、鍵記憶部１７に記憶されている鍵Ｋｃｏｍを用いて復号し、鍵Ｋｃｒｙを取得する。この鍵復号部１６５で取得された鍵Ｋｃｒｙは、コンテ

ンツ復号部１６６に送られる。

【００２２】

コンテンツ復号部１６６は、ディスクドライブ１１に装着されたＤＶＤ１から暗号化地図更新データを読み出し、鍵復号部１６５から送られてくる鍵Ｋｃｒｙを用いて復号する。また、コンテンツ復号部１６６は、暗号化地図更新データを復号した後に、鍵記憶部１７に記憶されている鍵Ｋｃｏｍを消去する。このコンテンツ復号部１６６における復号によって得られた地図更新データは、地図データ記憶部１４に送られて、該地図データ記憶部１４に既に記憶されている地図データを更新するために使用される。

【００２３】

鍵記憶部１７は、例えばＨＤＤの一部によって構成されており、鍵生成部１６１で生成された鍵Ｋｃｏｍを記憶する。この鍵記憶部１７に記憶された鍵Ｋｃｏｍは、鍵復号部１６５によって参照される。また、鍵記憶部１７に記憶されている内容は、コンテンツ復号部１６６からの指示により消去される。

【００２４】

パーソナルコンピュータ２０は、この発明の通信装置に対応し、カーナビゲーション装置１０とサーバ４０との間のデータの送受をＰＣカード２によって仲介する。図３は、パーソナルコンピュータ２０の詳細な構成を示すブロック図である。このパーソナルコンピュータ２０は、ＰＣスロット２１、通信部２２および制御部２３を備えている。ＰＣスロット２１、通信部２２および制御部２３は、この発明の制御部に対応する。なお、図３においては、この発明に関係しない構成要素は図示を省略してある。

【００２５】

ＰＣスロット２１にはＰＣカード２が着脱される。このＰＣスロット２１に装着されたＰＣカード２に記憶されている第１暗号データＸは制御部２３によって読み取られる。また、ＰＣスロット２１に装着されたＰＣカード２には、制御部２３から第２暗号データＹが書き込まれる。通信部２２は、ネットワーク３０を介してサーバ４０との間で行われる通信を制御する。

【００２６】

制御部２３は、パーソナルコンピュータ２０の全体を制御する。例えば、制御部２３は、ＰＣスロット２１に装着されたＰＣカード２から第１暗号データＸを読み出して通信部２２に送るとともに、通信部２２から送られてくる第２暗号データＹをＰＣスロット２１に装着されたＰＣカード２に書き込む。

【００２７】

サーバ４０は、例えばサーバコンピュータから構成されており、カーナビゲーション装置１０に保持される地図データのライセンスを管理する。図４は、サーバ４０の詳細な構成を示すブロック図である。サーバ４０は、秘密鍵記憶部４２、受信部４３、ＩＤ復号部４４、ライセンス管理リスト記憶部４５、鍵記憶部４６、鍵暗号化部４７および送信部４８を備えている。

【００２８】

秘密鍵記憶部４２は、後述するように、メーカから受け取った秘密鍵Ｓｐｒｉを記憶する。この秘密鍵記憶部４２に記憶されている秘密鍵Ｓｐｒｉは、ＩＤ復号部４４に送られる。受信部４３は、パーソナルコンピュータ２０からネットワーク３０を介して、ライセンス取得要求として送信されてくる第１暗号データＸを受信し、ＩＤ復号部４４に送る。ＩＤ復号部４４は、受信部４３から送られてくる第１暗号データＸを、秘密鍵記憶部４２から送られてくる秘密鍵Ｓｐｒｉを用いて復号し、シリアル番号および鍵Ｋｃｏｍを取得する。このＩＤ復号部４４で取得されたシリアル番号および鍵Ｋｃｏｍは、鍵暗号化部４７に送られる。

【００２９】

ライセンス管理リスト記憶部４５は、この発明のＩＤ記憶部に対応し、図５に示すように、ＤＶＤ１に付与されたシリアル番号と使用可否の情報とを対にしたライセンス管理リストを記憶する。ライセンス管理リスト中の使用可否の情報は、該使用可否の情報に対応

するシリアル番号を有するＤＶＤ１に使用権が存在するかどうか、つまりＤＶＤ１に記憶されている地図更新データを用いて既存の地図データを更新する権利が存在するかどうかを表し、初期状態、つまり、ＤＶＤ１を用いた地図データの更新が未だなされていない場合は使用可（「０」）に設定されており、１回でも地図データの更新がなされた場合は使用不可（「１」）に設定される。

【００３０】

鍵記憶部４６は、ＤＶＤ１に記憶されている暗号化地図更新データの作成に使用された鍵Ｋｃｒｙを記憶する。この鍵記憶部４６に記憶されている鍵Ｋｃｒｙは、鍵暗号化部４７によって読み出される。鍵暗号化部４７は、ライセンス管理リスト記憶部４５に記憶されているライセンス管理リストを参照することによってＤＶＤ１の使用権が存在することを確認した場合に、鍵記憶部４６に記憶されている鍵Ｋｃｒｙを、ＩＤ復号部４４において復号することにより得られた鍵Ｋｃｏｍによって暗号化することにより第２暗号データＹを生成し、送信部４８に送る。送信部４８は、鍵暗号化部４７から送られてきた第２暗号データＹを、ネットワーク３０を経由してパーソナルコンピュータ２０に送信する。

【００３１】

次に、上記のように構成される、この発明の実施の形態１に係るコンテンツ配信システムの動作を説明する。

【００３２】

まず、更新地図データを提供するメーカ、例えば自動車メーカやカーナビゲーション装置１０のメーカ等は、地図更新データを暗号化するための鍵Ｋｃｒｙを生成し、この生成した鍵Ｋｃｒｙにより地図更新データを暗号化することにより暗号化地図更新データを生成し、ＤＶＤ１に書き込む。そして、暗号化地図更新データが書き込まれたＤＶＤ１にシリアル番号を付与してユーザに配布する。

【００３３】

また、メーカは、生成した鍵Ｋｃｒｙおよびシリアル番号をサーバ４０に送付する。なお、この明細書で「送付」とは、例えば運送等といった内容が漏洩しにくい方法で送ることをいう。サーバ４０では、メーカから受け取った鍵Ｋｃｒｙを鍵記憶部４６に記憶するとともに、シリアル番号と使用可否の情報とが対になったライセンス管理リストを生成してライセンス管理リスト記憶部４５に記憶する。この場合、使用可否の情報は、全て使用可（「０」）に設定される。

【００３４】

また、メーカは、一対の公開鍵Ｓｐｕｂおよび秘密鍵Ｓｐｒｉを生成し、秘密鍵Ｓｐｒｉをサーバ４０に送付し、公開鍵Ｓｐｕｂをカーナビゲーション装置１０に送付する。サーバ４０は、受け取った秘密鍵Ｓｐｒｉを秘密鍵記憶部４２に格納する。また、カーナビゲーション装置１０は、受け取った公開鍵Ｓｐｕｂを公開鍵記憶部１３に格納する。なお、公開鍵Ｓｐｕｂの公開鍵記憶部１３への格納は、カーナビゲーション装置１０の製造時に行われる。

【００３５】

以上の状態において、ユーザがカーナビゲーション装置１０の地図データ記憶部１４に記憶されている地図データを更新する場合は、ユーザは、購入したＤＶＤ１をカーナビゲーション装置１０のディスクドライブ１１に装着する。これにより、地図データ更新処理が開始される。この場合、ＤＶＤ１に格納されている暗号化地図更新データを復号するための鍵Ｋｃｒｙが必要となるが、カーナビゲーション装置１０がネットワーク３０を介してサーバ４０に接続できない場合（例えば、ネットワーク３０への接続機能は有しているがユーザの携帯電話がカーナビゲーション装置１０の通信に対応していない場合等）は、以下の手順でサーバ４０から鍵Ｋｃｒｙを取得する処理が行われる。

【００３６】

以下、図６に示すシーケンスチャートを参照しながら、地図データ更新処理を説明する。カーナビゲーション装置１０では、ディスクドライブ１１にＤＶＤ１が装着されると、鍵Ｋｃｏｍが生成される（ステップＳＴ１１）。すなわち、制御部１６の鍵生成部１６１

は、鍵Ｋｃｒｙをサーバ４０から取得する際の暗号化に使用される鍵Ｋｃｏｍを生成し、ＩＤ暗号化部１６２に送るとともに、鍵記憶部１７に送る。鍵記憶部１７に記憶された鍵Ｋｃｏｍは、後に第２暗号データを復号する際に使用される。

【００３７】

次いで、ＤＶＤ１に記載されているシリアル番号が入力部１５から入力されると、第１暗号データＸが生成される（ステップＳＴ１２）。すなわち、ＩＤ暗号化部１６２は、ディスクドライブ１１に装着されるＤＶＤ１のシリアル番号と鍵生成部１６１から送られてくる鍵Ｋｃｏｍとを、公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂによって暗号化することにより第１暗号データＸを生成し、ＰＣカード書込部１６３に送る。なお、ＤＶＤ１の装着、鍵Ｋｃｏｍの生成およびシリアル番号の入力は、任意の順番で行うことができる。

【００３８】

次いで、第１暗号データＸがＰＣカード２に書き込まれる（ステップＳＴ１３）。すなわち、ＰＣカード書込部１６３は、ＩＤ暗号化部１６２から送られてきた第１暗号データＸを、ＰＣスロット１２に装着されているＰＣカード２に書き込む。その後、ユーザは、カーナビゲーション装置１０からＰＣカード２を引き抜き、パーソナルコンピュータ２０のＰＣスロット２１に装着する。

【００３９】

パーソナルコンピュータ２０においては、第１暗号データＸの送信が行われる（ステップＳＴ２１）。すなわち、パーソナルコンピュータ２０の制御部２３は、ＰＣスロット２１に装着されたＰＣカード２に記憶されている第１暗号データＸを読み取り、通信部２２に送る。通信部２２は、ネットワーク３０を介してサーバ４０に接続し、制御部２３から送られてくる第１暗号データＸをライセンス取得要求としてサーバ４０に送る。

【００４０】

サーバ４０においては、ライセンス取得要求として送られてくる第１暗号データＸが受信される（ステップＳＴ３１）。すなわち、サーバ４０の受信部４３は、パーソナルコンピュータ２０からネットワーク３０を介して送信されてくる第１暗号データＸを受信し、ＩＤ復号部４４に送る。

【００４１】

次いで、ライセンス確認処理が実行される（ステップＳＴ３２）。ここで、ライセンス確認処理の詳細を、図７に示すフローチャートを参照しながら説明する。このライセンス確認処理では、ライセンス取得要求としての第１暗号データＸが受信されると、まず、第１暗号データＸの復号が行われる（ステップＳＴ４１）。すなわち、ＩＤ復号部４４は、受信部４３から送られてくる第１暗号データＸを、秘密鍵記憶部４２に記憶されている秘密鍵Ｓｐｒｉを用いて復号し、シリアル番号および鍵Ｋｃｏｍを取得する。このＩＤ復号部４４で取得されたシリアル番号および鍵Ｋｃｏｍは、鍵暗号化部４７に送られる。

【００４２】

次いで、シリアル番号の使用可否がチェックされる（ステップＳＴ４２）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５からライセンス管理リストを読み出し、ステップＳＴ４１において復号することにより得られたシリアル番号に対応する使用可否の情報を取得する。次いで、ステップＳＴ４１において復号することにより得られたシリアル番号を有するＤＶＤ１が使用可であるかどうかが調べられる（ステップＳＴ４３）。すなわち、鍵暗号化部４７は、ステップＳＴ４２で取得した使用可否の情報が「０」であるか「１」であるかを調べる。

【００４３】

このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」であることが判断されると、鍵Ｋｃｏｍを用いて鍵Ｋｃｒｙが暗号化される（ステップＳＴ４４）。すなわち、鍵暗号化部４７は、鍵記憶部４６から鍵Ｋｃｒｙを読み出し、この読み出した鍵Ｋｃｒｙを、ＩＤ復号部４４から送られてくる鍵Ｋｃｏｍによって暗号化することにより第２暗号データＹを生成し、送信部４８に送る。

【００４４】
次いで、ライセンス管理リストの更新が行われる（ステップＳＴ４５）。すなわち、鍵暗号化部４７は、ステップＳＴ４２で取得したライセンス管理リストの使用可否の情報を「１」にセットし、ライセンス管理リスト記憶部４５に格納する。以上により、サーバ４０におけるライセンス確認処理は終了する。
【００４５】
上記ステップＳＴ４３において、使用不可である、つまり使用可否の情報が「１」であることが判断されると、鍵Ｋｃｏｍを用いて使用済ＩＤが暗号化される（ステップＳＴ４６）。すなわち、鍵暗号化部４７は、当該シリアル番号は使用済みであって使用権が存在しない旨を表す使用済ＩＤを生成し、この生成した使用済ＩＤを、ＩＤ復号部４４から送られてくる鍵Ｋｃｏｍによって暗号化することにより第２暗号データＹを生成し、送信部４８に送る。以上により、サーバ４０におけるライセンス確認処理は終了する。
【００４６】
ライセンス確認処理が終了すると、図６に示すように、送信が行われる（ステップＳＴ３３）。すなわち、サーバ４０の送信部４８は、鍵暗号化部４７から送られてくる第２暗号データＹを、ライセンス取得要求の応答として、ネットワーク３０を介してパーソナルコンピュータ２０に送信する。
【００４７】
パーソナルコンピュータ２０においては、第２暗号データＹの受信が行われる（ステップＳＴ２２）。すなわち、パーソナルコンピュータ２０の通信部２２は、サーバ４０からネットワーク３０を介して送信されてくる第２暗号データＹを受信し、制御部２３に送る。制御部２３は、通信部２２から受け取った第２暗号データＹを、ＰＣスロット２１に装着されているＰＣカード２に書き込む。その後、ユーザは、パーソナルコンピュータ２０のＰＣスロット２１からＰＣカード２を引き抜き、カーナビゲーション装置１０のＰＣスロット１２に装着する。
【００４８】
カーナビゲーション装置１０においては、鍵復号が行われる（ステップＳＴ１４）。すなわち、カーナビゲーション装置１０のＰＣカード読出部１６４は、ＰＣスロット１２に装着されたＰＣカード２に記憶されている第２暗号データＹを読み出し、鍵復号部１６５に送る。鍵復号部１６５は、ＰＣカード読出部４から送られてくる第２暗号データＹを、鍵記憶部１７に記憶されている鍵Ｋｃｏｍを用いて復号することにより鍵Ｋｃｒｙまたは使用済ＩＤを取得し、コンテンツ復号部１６６に送る。
【００４９】
次いで、コンテンツ復号が行われる（ステップＳＴ１５）。すなわち、コンテンツ復号部１６６は、鍵復号部１６５から鍵Ｋｃｒｙが送られてきた場合は、ディスクドライブ１１に装着されたＤＶＤ１から暗号化地図更新データを読み出し、鍵Ｋｃｒｙを用いて復号する。この復号が終了すると、コンテンツ復号部１６６は、鍵記憶部１７に記憶されている鍵Ｋｃｏｍを消去する。このコンテンツ復号部１６６における復号により得られた地図更新データは、地図データ記憶部１４に送られて、既存の地図データを更新するために使用される。
【００５０】
一方、コンテンツ復号部１６６は、鍵復号部１６５から使用済ＩＤが送られてきた場合は、カーナビゲーション装置１０に装着されたＤＶＤ１が複製されたもの（正規なものではない）とみなし、ユーザに対してその旨を通知する。したがって、ＤＶＤ１が正規である場合にはサーバ４０から鍵Ｋｃｒｙを取得することができるが、正規でない場合は鍵Ｋｃｒｙを取得することできないので、ＤＶＤ１の不正使用を防止できる。
【００５１】
以上説明したように、この実施の形態１に係るコンテンツ配信システムによれば、ネットワーク３０への接続ができないカーナビゲーション装置１０であっても、ＰＣカード２を用いることにより、ライセンスを管理するサーバ４０と通信し、ＤＶＤ１に記憶されて

いる暗号化地図更新データを復号するための鍵Ｋｃｒｙを取得することができ、サーバ４０は安全に鍵Ｋｃｒｙを配布することができる。

【００５２】

実施の形態２．

この発明の実施の形態２に係るコンテンツ配信システムは、実施の形態１に係るコンテンツ配信システムにおいて、鍵Ｋｃｒｙの配布を複数回できるようにしたものである。

【００５３】

この実施の形態２に係るコンテンツ配信システムは、サーバ４０のライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成およびサーバ４０の動作を除き、実施の形態１に係るコンテンツ配信システムと同じである。以下では、実施の形態１と相違する部分を中心に説明する。

【００５４】

図８は、ライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成を示す図である。このライセンス管理リストは、図５に示した実施の形態１に係るライセンス管理リストに、「鍵情報」という項目が追加されて構成されている。鍵情報としては、カーナビゲーション装置１０で生成された鍵Ｋｃｏｍが使用される。

【００５５】

次に、上記のように構成される、この発明の実施の形態２に係るコンテンツ配信システムの動作を説明する。このコンテンツ配信システムは、サーバ４０で行われるライセンス確認処理（図６のステップＳＴ３２に示す処理）のみが、実施の形態１と異なる。したがって、以下では、ライセンス確認処理の詳細を、図９に示すフローチャートを参照しながら説明する。なお、実施の形態１と同じ処理を行うステップには、実施の形態１と同じ符号を付して説明を簡略化する。

【００５６】

ライセンス確認処理では、ライセンス取得要求としての第１暗号データＸが受信されると、まず、第１暗号データＸの復号が行われる（ステップＳＴ４１）。次いで、シリアル番号の使用可否がチェックされる（ステップＳＴ４２）。次いで、ステップＳＴ４１において復号することにより得られたシリアル番号を有するＤＶＤ１が使用可であるかどうかが調べられる（ステップＳＴ４３）。このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」（未使用）であることが判断されると、鍵Ｋｃｏｍを用いて鍵Ｋｃｒｙが暗号化されて第２暗号データＹが生成される（ステップＳＴ４４）。このステップＳＴ４４において生成された第２暗号データＹは送信部４８に送られる。次いで、ライセンス管理リストの更新が行われる（ステップＳＴ４５）。すなわち、ライセンス管理リスト記憶部４５に記憶されているライセンス管理リストの使用可否の情報が「１」（使用不可）に設定されるとともに、鍵情報として鍵Ｋｃｏｍの値が記憶される。以上により、サーバ４０におけるライセンス確認処理は終了する。

【００５７】

上記ステップＳＴ４３において、使用不可である、つまり使用可否の情報が「１」（使用済み）であることが判断されると、鍵情報のチェックが行われる（ステップＳＴ５１）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５に記憶されているライセンス管理リストから鍵情報を取得する。次いで、同じ鍵であるかどうかが調べられる（ステップＳＴ５２）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５から取得した鍵情報と、カーナビゲーション装置１０から受け取った鍵Ｋｃｏｍとが同じであるかどうかを調べる。

【００５８】

このステップＳＴ５２において、同じあることが判断されると、シーケンスはステップＳＴ４４に進み、上述した処理が行われる。一方、ステップＳＴ５２において、同じでないことが判断されると、鍵Ｋｃｏｍを用いて使用済ＩＤが暗号化されて第２暗号データが生成される（ステップＳＴ４６）。このステップＳＴ４６において生成された第２暗号データＹは、送信部４８に送られる。

【００５９】
以上説明したように、この発明の実施の形態２に係るコンテンツ配信システムによれば、サーバ４０においてライセンス管理リストに鍵情報を対応付けて記録するように構成したので、同一の鍵Ｋｃｏｍでライセンス取得要求があった場合は複数回の鍵配布を許可することが可能である。これにより、サーバ４０からカーナビゲーション装置１０に鍵Ｋｃｒｙを配布する処理の途中で、誤ってＰＣカード２に記憶されているデータを削除してしまった場合やＰＣカード２を破損してしまった場合に、カーナビゲーション装置１０から再度第１暗号データＸをサーバ４０に送信することにより、サーバ４０から再度鍵Ｋｃｒｙの配布を受けることが可能となる。但し、カーナビゲーション装置１０は、再度第１暗号データＸをＰＣカード２に記録する際には、新たに鍵生成は行わず、生成済みの鍵Ｋｃｏｍを用いる。

【００６０】
実施の形態３．
上述した実施の形態１および実施の形態２では、所有者ＩＤとして、ＤＶＤ１に付与されたシリアル番号を用いたが、この実施の形態３に係るコンテンツ配信システムでは、所有者ＩＤとして、車（カーナビゲーション装置１０）に固有に割り当てられている「車ＩＤ番号」を用いるようにしたものである。

【００６１】
この実施の形態３に係るコンテンツ配信システムは、サーバ４０のライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成、カーナビゲーション装置１０の制御部１６に含まれるＩＤ暗号化部１６２の機能およびサーバ４０の動作が、実施の形態１に係るコンテンツ配信システムと相違する。以下では、実施の形態１と相違する部分を中心に説明する。

【００６２】
図１０は、ライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成を示す図である。このライセンス管理リストは、図５に示した実施の形態１に係るライセンス管理リストのシリアル番号が、「車ＩＤ番号」に置き換えられて構成されている。

【００６３】
また、ＩＤ暗号化部１６２は、入力部１５から所有者ＩＤとして入力された車ＩＤ番号と鍵生成部１６１から送られてくる鍵Ｋｃｏｍとを、公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂによって暗号化することにより第１暗号データＸを生成し、ＰＣカード書込部１６３に送る。

【００６４】
次に、上記のように構成される、この発明の実施の形態３に係るコンテンツ配信システムの動作を説明する。このコンテンツ配信システムは、カーナビゲーション装置１０で行われる第１暗号データＸの生成処理（図６のステップＳＴ１２）およびサーバ４０で行われるライセンス確認処理（図６のステップＳＴ３２に示す処理）のみが、実施の形態１と異なる。したがって、以下では、異なる部分のみを説明する。

【００６５】
図６に示すステップＳＴ１２では、車ＩＤ番号が入力部１５から入力されると、第１暗号データＸが生成される。すなわち、ＩＤ暗号化部１６２は、入力部１５から入力された車ＩＤ番号と鍵生成部１６１から送られてくる鍵Ｋｃｏｍとを、公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂによって暗号化することにより第１暗号データＸを生成し、ＰＣカード書込部１６３に送る。以後の処理は、実施の形態１と同じである。

【００６６】
次に、サーバ４０で行われるライセンス確認処理の詳細を、図１１に示すフローチャートを参照しながら説明する。なお、実施の形態１と同じ処理を行うステップには、実施の形態１と同じ符号を付して説明を簡略化する。

【００６７】
ライセンス確認処理では、ライセンス取得要求としての第１暗号データＸが受信される

と、まず、第１暗号データＸの復号が行われる（ステップＳＴ４１）。次いで、車ＩＤ番号の使用可否がチェックされる（ステップＳＴ６１）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５からライセンス管理リストを読み出し、ステップＳＴ４１において復号することにより得られた車ＩＤ番号に対応する使用可否の情報を取得する。次いで、ステップＳＴ４１において復号することにより得られた車ＩＤ番号を有するカーナビゲーション装置１０がＤＶＤ１を使用可であるかどうかが調べられる（ステップＳＴ４３）。

【００６８】

このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」（未使用）であることが判断されると、鍵Ｋｃｏｍを用いて鍵Ｋｃｒｙが暗号化されて第２暗号データＹが生成される（ステップＳＴ４４）。このステップＳＴ４４において生成された第２暗号データＹは送信部４８に送られる。次いで、ライセンス管理リストの更新が行われる（ステップＳＴ４５）。以上により、サーバ４０におけるライセンス確認処理は終了する。

【００６９】

上記ステップＳＴ４３において、使用不可である、つまり使用可否の情報が「１」（使用済み）であることが判断されると、鍵Ｋｃｏｍを用いて使用済ＩＤが暗号化されて第２暗号データが生成される（ステップＳＴ４６）。このステップＳＴ４６において生成された第２暗号データＹは、送信部４８に送られる。

【００７０】

以上説明したように、この発明の実施の形態３に係るコンテンツ配信システムによれば、ネットワーク３０への接続ができないカーナビゲーション装置１０であっても、ＰＣカード２を用いることにより、ライセンスを管理するサーバ４０と通信し、ＤＶＤ１に記憶されている暗号化地図更新データを復号するための鍵Ｋｃｒｙを取得することができ、サーバ４０は安全に鍵Ｋｃｒｙを配布することができる。この場合、サーバ４０は、車毎に付与された車ＩＤ番号によってライセンスの管理を行うため、上述した実施の形態１および実施の形態２に係るコンテンツ配信システムのように、ＤＶＤ１の個別のシリアル番号を割り当てる必要がない。

【００７１】

実施の形態４．

この発明の実施の形態４に係るコンテンツ配信システムは、実施の形態３に係るコンテンツ配信システムにおいて、鍵Ｋｃｒｙの配布を複数回できるようにしたものである。

【００７２】

この実施の形態４に係るコンテンツ配信システムは、サーバ４０のライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成およびサーバ４０の動作を除き、実施の形態３に係るコンテンツ配信システムと同じである。以下では、実施の形態３と相違する部分を中心に説明する。

【００７３】

図１２は、ライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成を示す図である。このライセンス管理リストは、図１０に示した実施の形態３に係るライセンス管理リストに、「鍵情報」という項目が追加されて構成されている。鍵情報としては、カーナビゲーション装置１０で生成された鍵Ｋｃｏｍが使用される。

【００７４】

次に、上記のように構成される、この発明の実施の形態４に係るコンテンツ配信システムの動作を説明する。このコンテンツ配信システムは、サーバ４０で行われるライセンス確認処理（図６のステップＳＴ３２に示す処理）のみが、実施の形態３と異なる。したがって、以下では、ライセンス確認処理の詳細を、図１３に示すフローチャートを参照しながら説明する。なお、実施の形態３と同じ処理を行うステップには、実施の形態３と同じ符号を付して説明を簡略化する。

【００７５】

ライセンス確認処理では、ライセンス取得要求としての第１暗号データＸが受信されると、まず、第１暗号データＸの復号が行われる（ステップＳＴ４１）。次いで、車ＩＤ番号の使用可否がチェックされる（ステップＳＴ６１）。次いで、ステップＳＴ４１において復号することにより得られた車ＩＤ番号を有するカーナビゲーション装置１０がＤＶＤ１を使用可であるかどうかが調べられる（ステップＳＴ４３）。

【００７６】

このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」（未使用）であることが判断されると、鍵Ｋｃｏｍを用いて鍵Ｋｃｒｙが暗号化されて第２暗号データＹが生成される（ステップＳＴ４４）。このステップＳＴ４４において生成された第２暗号データＹは送信部４８に送られる。次いで、ライセンス管理リストの更新が行われる（ステップＳＴ４５）。以上により、サーバ４０におけるライセンス確認処理は終了する。

【００７７】

上記ステップＳＴ４３において、使用不可である、つまり使用可否の情報が「１」（使用済み）であることが判断されると、鍵情報のチェックが行われる（ステップＳＴ５１）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５に記憶されているライセンス管理リストから鍵情報を取得する。次いで、同じ鍵であるかどうかが調べられる（ステップＳＴ５２）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５から取得した鍵情報と、カーナビゲーション装置１０から受け取った鍵Ｋｃｏｍとが同じであるかどうかを調べる。

【００７８】

このステップＳＴ５２において、同じあることが判断されると、シーケンスはステップＳＴ４４に進み、上述した処理が行われる。一方、ステップＳＴ５２において、同じでないことが判断されると、鍵Ｋｃｏｍを用いて使用済ＩＤが暗号化されて第２暗号データが生成される（ステップＳＴ４６）。このステップＳＴ４６において生成された第２暗号データＹは、送信部４８に送られる。

【００７９】

以上説明したように、この発明の実施の形態４に係るコンテンツ配信システムによれば、サーバ４０においてライセンス管理リストに鍵情報を対応付けて記録するように構成したので、実施の形態３により得られる効果に加え、同一の鍵Ｋｃｏｍでライセンス取得要求があった場合は複数回の鍵配布を許可することが可能である。これにより、サーバ４０からカーナビゲーション装置１０に鍵Ｋｃｒｙを配布する処理の途中で、誤ってＰＣカード２に記憶されているデータを削除してしまった場合やＰＣカード２を破損してしまった場合に、カーナビゲーション装置１０から再度第１暗号データＸをサーバ４０に送信することにより、サーバ４０から再度鍵Ｋｃｒｙの配布を受けることが可能となる。但し、カーナビゲーション装置１０は、再度第１暗号データＸをＰＣカード２に記録する際には、新たに鍵生成は行わず、生成済みの鍵Ｋｃｏｍを用いる。

【００８０】

実施の形態５．

この実施の形態５に係るコンテンツ配信システムでは、所有者ＩＤとして、ＤＶＤ１に付与されたシリアル番号および車ＩＤ番号の両方を用いるようにしたものである。

【００８１】

この実施の形態５に係るコンテンツ配信システムは、サーバ４０のライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成、カーナビゲーション装置１０の制御部１６に含まれるＩＤ暗号化部１６２の機能およびサーバ４０の動作が、実施の形態１および実施の形態３に係るコンテンツ配信システムと相違する。以下では、実施の形態１および実施の形態３と相違する部分を中心に説明する。

【００８２】

図１４は、ライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成を示す図である。このライセンス管理リストは、図１４（ａ）に示す車ＩＤ番号リスト、

図１４（ｂ）に示すシリアル番号リストおよび図１４（ｃ）に示す対応管理リストから構成されている。車ＩＤ番号リストは、図１０に示した実施の形態３のライセンス管理リストに車ＩＤ番号インデックス（Ｉｎｄｅｘ）の項目が追加されて構成されている。シリアル号リストは、図５に示した実施の形態１のライセンス管理リストにシリアル番号インデックス（Ｉｎｄｅｘ）の項目が追加されて構成されている。対応管理リストは、車ＩＤ番号インデックスとシリアル番号インデックスとによって車ＩＤ番号とシリアル番号との対応関係を規定する。この対応管理リストの初期値は空である。

【００８３】

また、ＩＤ暗号化部１６２は、入力部１５から所有者ＩＤとして入力された車ＩＤ番号、シリアル番号および鍵生成部１６１から送られてくる鍵Ｋｃｏｍを、公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂによって暗号化することにより第１暗号データＸを生成し、ＰＣカード書込部１６３に送る。

【００８４】

次に、上記のように構成される、この発明の実施の形態５に係るコンテンツ配信システムの動作を説明する。このコンテンツ配信システムは、カーナビゲーション装置１０で行われる第１暗号データＸの生成処理（図６のステップＳＴ１２）およびサーバ４０で行われるライセンス確認処理（図６のステップＳＴ３２に示す処理）のみが、実施の形態１および実施の形態３と異なる。したがって、以下では、異なる部分のみを説明する。

【００８５】

図６に示すステップＳＴ１２では、車ＩＤ番号およびシリアル番号が入力部１５から入力されると、第１暗号データＸが生成される。すなわち、ＩＤ暗号化部１６２は、入力部１５から入力された車ＩＤ番号、シリアル番号および鍵生成部１６１から送られてくる鍵Ｋｃｏｍを、公開鍵記憶部１３に記憶されている公開鍵Ｓｐｕｂによって暗号化することにより第１暗号データＸを生成し、ＰＣカード書込部１６３に送る。以後の処理は、実施の形態１および実施の形態３と同じである。

【００８６】

次に、サーバ４０で行われるライセンス確認処理の詳細を、図１５に示すフローチャートを参照しながら説明する。なお、実施の形態１と同じ処理を行うステップには、実施の形態１および実施の形態３と同じ符号を付して説明を簡略化する。

【００８７】

ライセンス確認処理では、ライセンス取得要求としての第１暗号データＸが受信されると、まず、第１暗号データＸの復号が行われる（ステップＳＴ４１）。次いで、車ＩＤ番号の使用可否がチェックされる（ステップＳＴ６１）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５からライセンス管理リストの車ＩＤ番号リストを読み出し、ステップＳＴ４１において復号することにより得られた車ＩＤ番号に対応する使用可否の情報を取得する。次いで、ステップＳＴ４１において復号することにより得られた車ＩＤ番号を有するカーナビゲーション装置１０がＤＶＤ１を使用可であるかどうかが調べられる（ステップＳＴ４３）。

【００８８】

このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」（未使用）であることが判断されると、次いで、シリアル番号の使用可否がチェックされる（ステップＳＴ４２）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５からライセンス管理リストのシステム番号リストを読み出し、ステップＳＴ４１において復号することにより得られたシリアル番号に対応する使用可否の情報を取得する。次いで、ステップＳＴ４１において復号することにより得られたシリアル番号を有するＤＶＤ１が使用可であるかどうかが調べられる（ステップＳＴ４３）。すなわち、鍵暗号化部４７は、ステップＳＴ４２で取得した使用可否の情報が「０」であるか「１」であるかを調べる。

【００８９】

このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」であることが判断されると、鍵Ｋｃｏｍを用いて鍵Ｋｃｒｙが暗号化されて第２暗号データＹが

生成される（ステップＳＴ４４）。このステップＳＴ４４において生成された第２暗号データＹは送信部４８に送られる。次いで、ライセンス管理リストの更新が行われる（ステップＳＴ４５）。すなわち、鍵暗号化部４７は、ステップＳＴ６１で取得したライセンス管理リストうちの車ＩＤ番号リストの使用可否の情報を「１」にセットするとともに、ステップＳＴ４２で取得したライセンス管理リストの使用可否の情報を「１」にセットし、さらに、対応管理リストに車ＩＤインデックスとシリアル番号インデックスとの対応をセットし、ライセンス管理リスト記憶部４５に格納する。以上により、サーバ４０におけるライセンス確認処理は終了する。

【００９０】

上記ステップＳＴ４３およびステップＳＴ６１において、使用不可である、つまり使用可否の情報が「１」（使用済み）であることが判断されると、鍵Ｋｃｏｍを用いて使用済ＩＤが暗号化されて第２暗号データが生成される（ステップＳＴ４６）。このステップＳＴ４６において生成された第２暗号データＹは、送信部４８に送られる。

【００９１】

以上説明したように、この発明の実施の形態５に係るコンテンツ配信システムによれば、上述した実施の形態１および実施の形態３に係るコンテンツ配信システムによる効果に加え、サーバ４０は、各車で使用しているＤＶＤ１を対応管理リストに記憶できるので、車とＤＶＤ１の両方を管理することができる。

【００９２】

実施の形態６．

この発明の実施の形態６に係るコンテンツ配信システムは、実施の形態５に係るコンテンツ配信システムにおいて、鍵Ｋｃｒｙの配布を複数回できるようにしたものである。

【００９３】

この実施の形態６に係るコンテンツ配信システムは、サーバ４０のライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成およびサーバ４０の動作を除き、実施の形態５に係るコンテンツ配信システムと同じである。以下では、実施の形態５と相違する部分を中心に説明する。

【００９４】

図１６は、ライセンス管理リスト記憶部４５に格納されるライセンス管理リストの構成を示す図である。このライセンス管理リストは、図１４に示した実施の形態５に係るライセンス管理リストの対応管理リストに、「鍵情報」という項目が追加されて構成されている。鍵情報としては、カーナビゲーション装置１０で生成された鍵Ｋｃｏｍが使用される。

【００９５】

次に、上記のように構成される、この発明の実施の形態６に係るコンテンツ配信システムの動作を説明する。このコンテンツ配信システムは、サーバ４０で行われるライセンス確認処理（図６のステップＳＴ３２に示す処理）のみが、実施の形態５と異なる。したがって、以下では、ライセンス確認処理の詳細を、図１７に示すフローチャートを参照しながら説明する。なお、実施の形態５と同じ処理を行うステップには、実施の形態５と同じ符号を付して説明を簡略化する。

【００９６】

ライセンス確認処理では、ライセンス取得要求としての第１暗号データＸが受信されると、まず、第１暗号データＸの復号が行われる（ステップＳＴ４１）。次いで、車ＩＤ番号の使用可否がチェックされる（ステップＳＴ６１）。次いで、ステップＳＴ４１において復号することにより得られた車ＩＤ番号を有するカーナビゲーション装置１０がＤＶＤ１を使用可であるかどうかが調べられる（ステップＳＴ４３）。

【００９７】

このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」（未使用）であることが判断されると、次いで、シリアル番号の使用可否がチェックされる（ステップＳＴ６１）。次いで、ステップＳＴ４１において復号することにより得られたシリ

アル番号を有するＤＶＤ１を使用可であるかどうかが調べられる（ステップＳＴ４３）。このステップＳＴ４３において、使用可である、つまり使用可否の情報が「０」（未使用）であることが判断されると、鍵Ｋｃｏｍを用いて鍵Ｋｃｒｙが暗号化されて第２暗号データＹが生成される（ステップＳＴ４４）。このステップＳＴ４４において生成された第２暗号データＹは送信部４８に送られる。

【００９８】

次いで、ライセンス管理リストの更新が行われる（ステップＳＴ４５）。すなわち、鍵暗号化部４７は、ステップＳＴ６１で取得したライセンス管理リストうちの車ＩＤ番号リストの使用可否の情報を「１」にセットするとともに、ステップＳＴ４２で取得したライセンス管理リストの使用可否の情報を「１」にセットし、また、対応管理リストに車ＩＤインデックスとシリアル番号インデックスとの対応をセットし、さらに、対応管理リストに鍵情報として鍵Ｋｃｏｍの値を記憶する。以上により、サーバ４０におけるライセンス確認処理は終了する。

【００９９】

上記ステップＳＴ４３またはステップＳＴ６１において、使用不可である、つまり車ＩＤ番号リストまたはシリアル番号リストの使用可否の情報が「１」（使用済み）であることが判断されると、鍵情報のチェックが行われる（ステップＳＴ５１）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５に記憶されているライセンス管理リストの対応管理リストから鍵情報を取得する。次いで、同じ鍵であるかどうかが調べられる（ステップＳＴ５２）。すなわち、鍵暗号化部４７は、ライセンス管理リスト記憶部４５の対応管理リストから取得した鍵情報と、カーナビゲーション装置１０から受け取った鍵Ｋｃｏｍとが同じであるかどうかを調べる。

【０１００】

このステップＳＴ５２において、同じあることが判断されると、シーケンスはステップＳＴ４４に進み、上述した処理が行われる。一方、ステップＳＴ５２において、同じでないことが判断されると、鍵Ｋｃｏｍを用いて使用済ＩＤが暗号化されて第２暗号データが生成される（ステップＳＴ４６）。このステップＳＴ４６において生成された第２暗号データＹは、送信部４８に送られる。

【０１０１】

以上説明したように、この発明の実施の形態６に係るコンテンツ配信システムによれば、上述した実施の形態５に係るコンテンツ配信システムによる効果に加え、正規のユーザからのライセンス再発行を許可することができる。

【０１０２】

なお、上述した実施の形態１～実施の形態６では、ユーザがカーナビゲーション装置１０を操作して地図データの更新を行うものとして説明したが、特別な権限を有する者、例えばディーラにおける管理者のみがカーナビゲーション装置１０の管理者設定画面からのみ地図データの更新を可能にするように構成することができる。この構成によれば、ユーザは、自ら地図データを更新するための更新操作を行う必要がないので、ユーザの負担が軽減される。また、ユーザは更新操作に関与できないので、ユーザによる不正行為を防ぐことができる。

【０１０３】

また、第１記録媒体としてＤＶＤ１を用いたが、第１記録媒体としては、ＤＶＤ１に限らず、ＵＳＢメモリ、ＰＣカード、ＳＤカードといった他の記録媒体を用いることもできる。要は、カーナビゲーション装置１０でデータを読み出すことができるデバイスであれば、種々のタイプのデバイスを用いることができる。

【０１０４】

また、第２記録媒体としてＰＣカード２を用いたが、第２記録媒体としては、ＰＣカード２に限らず、ＵＳＢメモリ、ＳＤカード、ＤＶＤといった他の持ち運び可能な記録媒体を用いることもできる。要は、カーナビゲーション装置１０およびパーソナルコンピュータ２０の両者がデータの書き込みおよび読み出しをできるデバイスであれば、種々のタイ

プのデバイスを用いることができる。

【０１０５】

また、第１記録媒体としてＤＶＤ１を、第２記憶媒体としてＰＣカード２を用いたが、同一に記録媒体を用いることもできる。これにより、サーバ４０からライセンスを発行するとともに、コンテンツデータを発行する事もできる。

【０１０６】

また、ＤＶＤ１に書き込む地図更新データの暗号化用の鍵Ｋｃｒｙを作成する機関、サーバ４０を管理する機関およびサーバ４０に送付する秘密鍵とカーナビゲーション装置１０に記憶する公開鍵を生成する機関は同一である必要はない。要は、上述した処理によってサーバ４０からカーナビゲーション装置１０に鍵Ｋｃｒｙを配布できればよい。

【０１０７】

また、ＤＶＤ１に書き込む地図更新データを暗号化するための鍵Ｋｃｒｙは、自動車メーカまたはカーナビゲーション装置１０のメーカで生成するようにしたが、サーバ４０で生成することもできる。この場合、鍵Ｋｃｒｙは、サーバ４０からＤＶＤ１に書き込む暗号化地図更新データを作成する機関に送付される。これにより、鍵Ｋｃｒｙをサーバ４０に送付する必要がなくなるので、鍵漏洩のリスクを低減させることができる。また、その他の機関で鍵Ｋｃｒｙを生成し、ＤＶＤ１に書き込む暗号化地図更新データを作成する機関およびサーバ４０に送付することもできる。要は、最終的にＤＶＤ１に書き込まれた暗号化地図更新データを復号するための鍵Ｋｃｒｙをサーバ４０が保持することができればよい。

【０１０８】

また、秘密鍵Ｓｐｒｉと公開鍵Ｓｐｕｂの生成は、自動車メーカまたはカーナビゲーション装置１０のメーカで行われるので、公開鍵Ｓｐｕｂをメーカから持ち出す必要がなくなり、鍵漏洩のリスクを低減させることができる。なお、秘密鍵Ｓｐｒｉと公開鍵Ｓｐｕｂの生成は、サーバ４０で行うこともできる。この場合は、公開鍵Ｓｐｕｂをサーバ４０から自動車メーカまたはカーナビゲーション装置１０のメーカに送付することになる。これにより、秘密鍵Ｓｐｒｉをサーバ４０の内部から持ち出す必要がないので、鍵漏洩のリスクを低減させることができる。

【０１０９】

また、サーバ４０は、ＰＣカード２から第１暗号データＸを読み込んだ後に、ＰＣカード２に記憶されている第１暗号データＸを消去するように構成することができる。この場合、サーバ４０の送信部４８は、ＩＤ復号部４４により第１暗号データが復号された後に、通信装置２０に消去指令を送る。通信装置２０の制御部２３は、サーバ４０から通信部２２を介して送られてくる消去指令に応じて、ＰＣスロット２１に装着されたＰＣカード２に記憶されている内容を消去する。この構成により、ライセンスの取得に使用されるデータの無用な流出を防止することができる。

【０１１０】

また、カーナビゲーション装置１０は、ＰＣカード２から第２暗号データＹを読み込んだ後に、ＰＣカード２に記憶されている第２暗号データＹを消去するように構成することもできる。この場合、ＰＣカード読出部１６４は、第２暗号データＹの読み込みが完了すると、その旨をＰＣカード書込部１６３に通知する。ＰＣカード書込部１６３は、この通知に応答して、ＰＣカードに記憶されている第２暗号データＹを消去する。この構成により、ライセンスの取得に使用されるデータの無用な流出を防止することができる。

【０１１１】

また、カーナビゲーション装置１０は、サーバ４０から鍵Ｋｃｒｙを受け取ってＤＶＤ１に記憶されている暗号化地図更新データを復号した後に、鍵Ｋｃｒｙを削除するように構成することもできる。この構成により、鍵Ｋｃｒｙが外部に漏れるリスクを低減させることができる。

【０１１２】

また、サーバ４０に記憶される秘密鍵Ｓｐｒｉとカーナビゲーション装置１０に記憶さ

れる公開鍵Ｓｐｕｂのペアは１種類のみではなく、車種やカーナビゲーション装置１０の型番毎に異ならせるように構成することができる。この場合、カーナビゲーション装置１０で生成する第１暗号データＸに車種やカーナビゲーション装置１０の型番を表す情報も含めるように構成する。この構成により、万が一、公開鍵Ｓｐｕｂが外部に漏れた際のリスクを低減させることができる。

【０１１３】

また、ＤＶＤ１に書き込む地図更新データの暗号化に使用された鍵Ｋｃｒｙも１種類のみではなく、生産月毎や生産枚数毎に異ならせるように構成できる。この場合、サーバ４０に、シリアル番号または車ＩＤ番号と鍵Ｋｃｒｙとの対応情報を保持しておく。この構成により、万が一、鍵Ｋｃｒｙが外部に漏れた際のリスクを低減させることができる。

【０１１４】

また、カーナビゲーション装置１０では、鍵生成部１６１において鍵Ｋｃｏｍを生成するように構成したが、公開鍵Ｓｐｕｂおよび秘密鍵Ｓｐｒｉのペアを生成するように構成することもできる。この場合、カーナビゲーション装置１０で作成する第１暗号データＸに鍵Ｋｃｏｍの代わりに公開鍵Ｓｐｕｂを含め、ＰＣカード２から読み込んだ第２暗号データＹを、カーナビゲーション装置１０で生成した秘密鍵Ｓｐｒｉにより復号する。この構成により、万が一、ＰＣカード２からカーナビゲーション装置１０が生成した公開鍵Ｓｐｕｂが漏洩した場合でも、その漏洩した公開鍵Ｓｐｕｂを用いて第２暗号データＹの復号はできないので、公開鍵Ｓｐｕｂが外部に漏れた際のリスクを低減させることができる。

【０１１５】

また、上述した実施の形態２、実施の形態４および実施の形態６において、第１暗号データＸを再度ＰＣカード２に記録する際には、新たに鍵生成は行わず、生成済みの鍵Ｋｃｏｍを用いるように構成したが、この鍵Ｋｃｏｍの消去のタイミングは、暗号化地図更新データを復号した後ではなく、地図データの更新が終了した時点とすることができる。この構成によれば、地図更新処理中にエラーが発生して地図更新処理の継続が不可能になった場合であっても、ライセンスの再発行が可能になる。

【０１１６】

また、上述した実施の形態１～実施の形態６では、この発明の端末としてカーナビゲーション装置が使用される場合について説明したが、この発明の端末としては、カーナビゲーション装置に限らず、例えば携帯電話、ＰＤＡ（Personal Digital Assistant）、携帯オーディオ機器といったコンテンツの配布を受けて動作する種々の機器を用いることができる。

【０１１７】

また、上述した実施の形態１～実施の形態６では、通信機能を有しないカーナビゲーション装置１０とサーバ４０との間の情報の送受をＰＣカード２を介して行うように構成したが、ＰＣカード２を介して送受される情報を、カーナビゲーション装置１０とサーバ４０との間で通信により直接に送受するように構成することもできる。

【０１１８】

また、上述した実施の形態１～実施の形態６では、暗号データＸの暗号化／復号に秘密鍵と公開鍵を用いた公開鍵暗号方式を採用したが、暗号化および復号で同じ鍵を用いる共通鍵暗号方式を採用することもできる。

【０１１９】

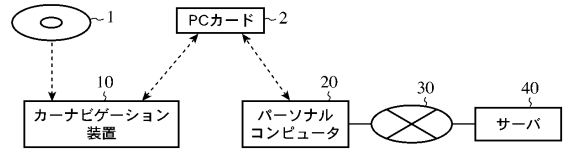
また、上述した実施の形態１～実施の形態６では、コンテンツ暗号化鍵およびコンテンツ復号鍵として同一の鍵Ｋｃｒｙを用いる共通鍵暗号方式を採用したが、コンテンツ暗号化鍵およびコンテンツ復号鍵として別個の鍵を用いる公開鍵暗号方式を採用することもできる。

【０１２０】

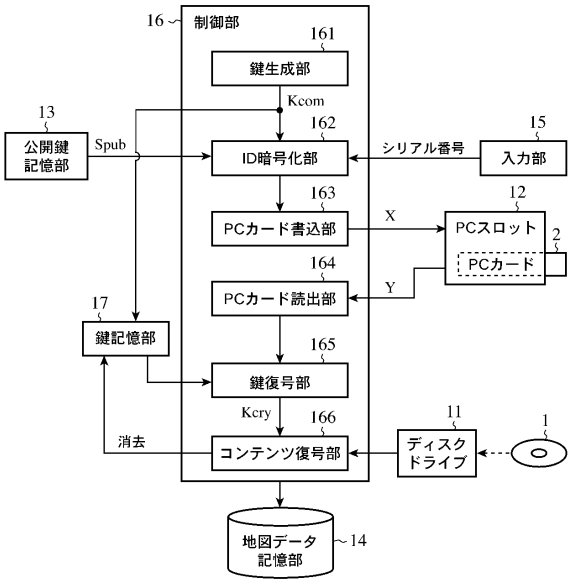
以上のように、この発明に係るコンテンツ配信システムおよび端末およびサーバは、ネットワークへの接続ができない端末であっても、サーバは安全にコンテンツ復号鍵を配布

することができるので、例えば、カーナビゲーション、携帯電話、ＰＤＡ、通信機能を有しない端末等に用いるのに適している。

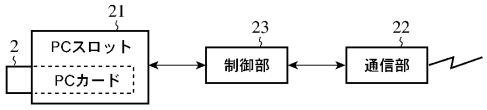
【図１】



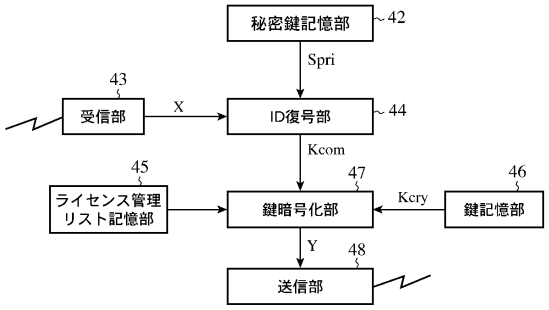
【図２】



【図３】



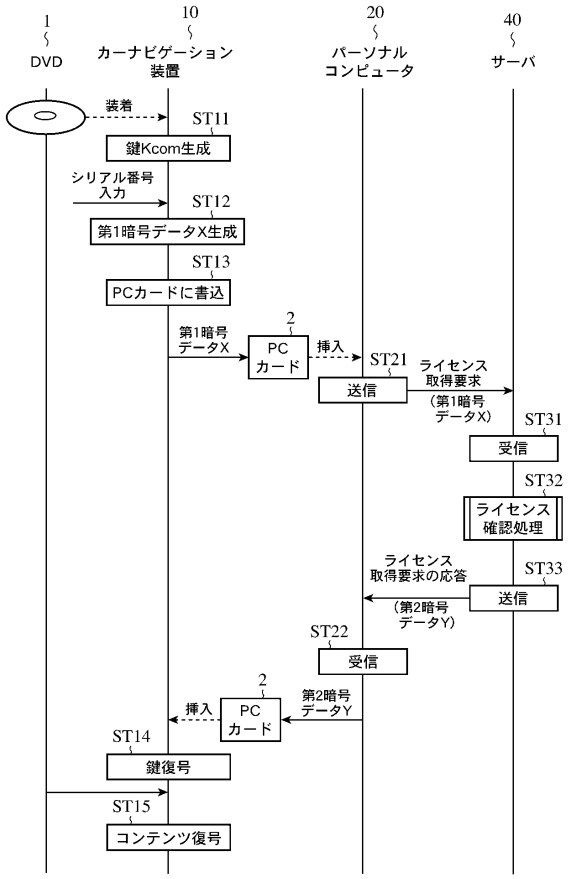
【図４】



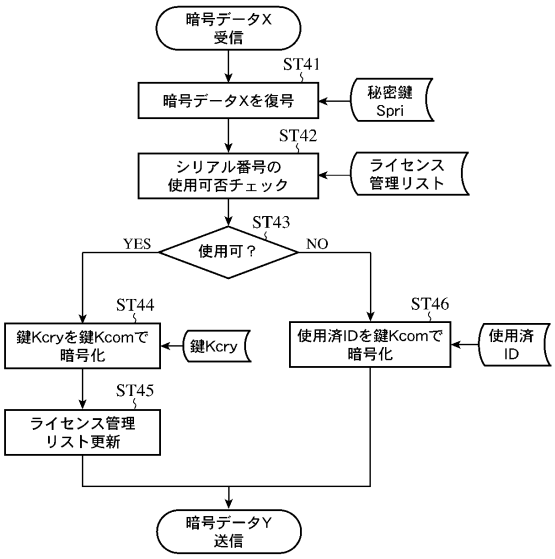
【図５】

シリアル番号	使用可否
0000-0000-000	0
0000-0000-001	0
0000-0000-002	0
0000-0000-003	1
⋮	⋮

【図６】



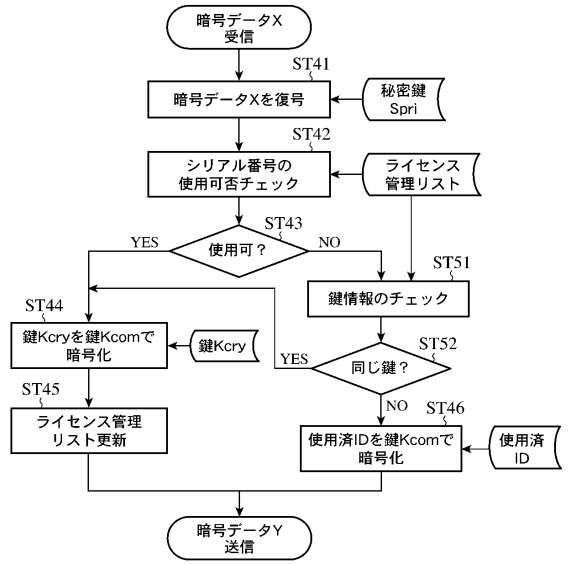
【図７】



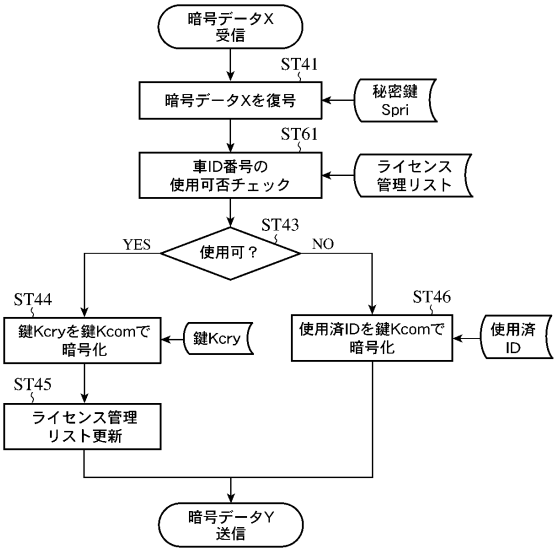
【図８】

シリアル番号	使用可否	鍵情報
0000-0000-000	0	da90-92d1-0s32-0bcc
0000-0000-001	0	79da-002f-9b73-2ee9
0000-0000-002	0	0543-aabc-de40-0054
0000-0000-003	1	e878-f318-acde-7763
⋮	⋮	⋮

【図９】



【図１１】



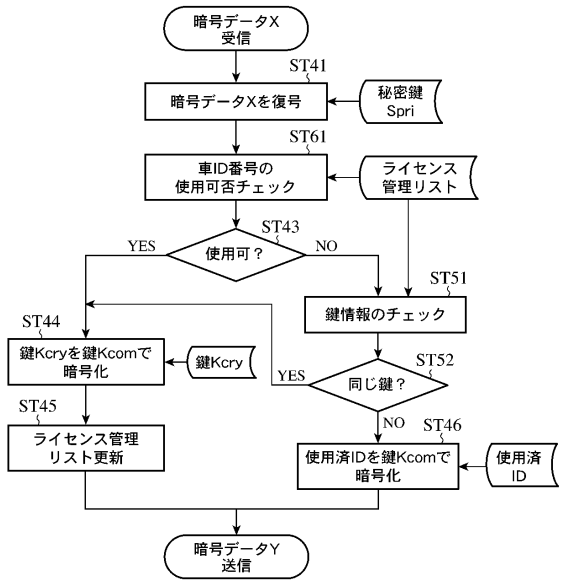
【図１０】

車ID番号	使用可否
AAAA-0000-000	0
BBBB-0000-001	0
CCCC-0000-002	0
DDDD-0000-003	1
⋮	⋮

【図１２】

車ID番号	使用可否	鍵情報
AAAA-0000-000	0	da90-92d1-0s32-0bcc
BBBB-0000-001	0	79da-002f-9b73-2ee9
CCCC-0000-002	0	0543-aabc-de40-0054
DDDD-0000-003	1	e878-f318-acde-7763
⋮	⋮	⋮

【図１３】



【図１４】

車ID 番号リスト

（ａ）

車ID 番号 Index	車ID 番号	使用可否
0	AAAA-0000-0000	0
1	BBBB-0000-0001	0
2	CCCC-0000-0002	0
3	DDDD-0000-0003	1
⋮	⋮	⋮

シリアル番号リスト

（ｂ）

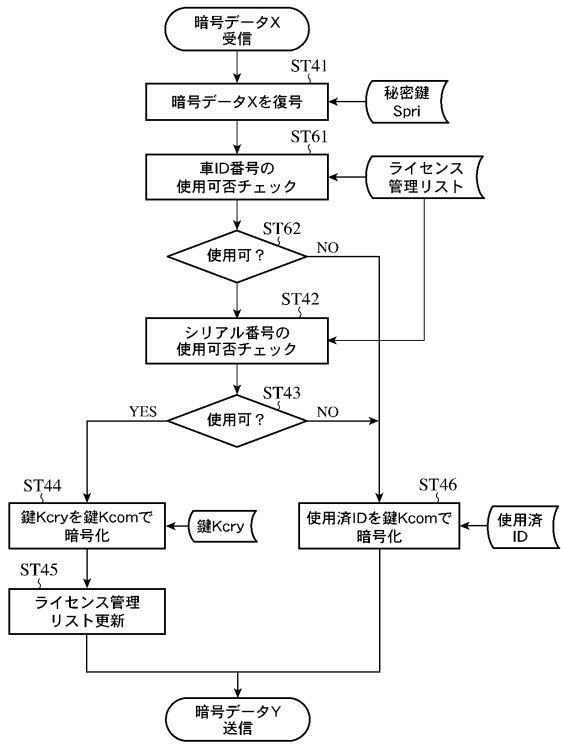
シリアル番号 Index	シリアル番号	使用可否
0	0000-0000-000	0
1	0000-0000-001	0
2	0000-0000-002	0
3	0000-0000-003	1
⋮	⋮	⋮

対応管理リスト

（ｃ）

車ID 番号 Index	シリアル番号 Index
0	3
1	2
2	0
3	1
⋮	⋮

【図１５】



【図１６】

車ID 番号リスト

（ａ）

車ID 番号 Index	車ID 番号	使用可否
0	AAAA-0000-0000	0
1	BBBB-0000-0001	0
2	CCCC-0000-0002	0
3	DDDD-0000-0003	1
⋮	⋮	⋮

シリアル番号リスト

（ｂ）

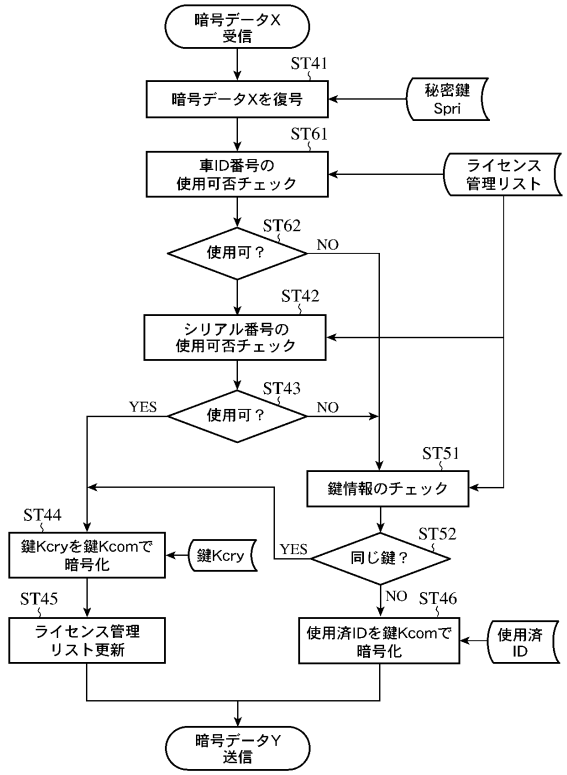
シリアル番号 Index	シリアル番号	使用可否
0	0000-0000-000	0
1	0000-0000-001	0
2	0000-0000-002	0
3	0000-0000-003	1
⋮	⋮	⋮

対応管理リスト

（ｃ）

車ID番号 Ind ex	シリアル番号 Index	鍵情報
0	3	da90-92d1-0s32-0bcc
1	2	79da-002f-9b73-2ee9
2	0	0543-aabc-de40-0054
3	1	e878-f318-acde-7763
⋮	⋮	⋮

【図１７】


暗号データX
受信
ST41
暗号データXを復号
秘密鍵
Spri
ST61
車ID番号の
使用可否チェック
ライセンス
管理リスト
ST62
使用可？
NO
ST42
シリアル番号の
使用可否チェック
ST43
YES
使用可？
NO
ST51
鍵情報のチェック
ST44
鍵Kcryを鍵Kcomで
暗号化
鍵Kcry
YES
ST52
同じ鍵？
NO
ST46
ST45
ライセンス管理
リスト更新
使用済IDを鍵Kcomで
暗号化
使用済
ID
暗号データY
送信

フロントページの続き

(72)発明者　井崎　公彦
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　松田　規
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　鶴川　達也
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　新田　亮

(56)参考文献　特開２００２－１６９４６５（ＪＰ，Ａ）
特開２００２－０８３１５２（ＪＰ，Ａ）
特開２００５－１９８３３６（ＪＰ，Ａ）
特開２００２－３１９９３２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08
G06Q　10/00
G06Q　30/00
G06Q　50/00