(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-182946
(P2009-182946A)
(43)公開日　平成21年8月13日(2009.8.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 17　OL　（全 31 頁）

(21)出願番号　特願2008-22842(P2008-22842)
(22)出願日　平成20年2月1日(2008.2.1)

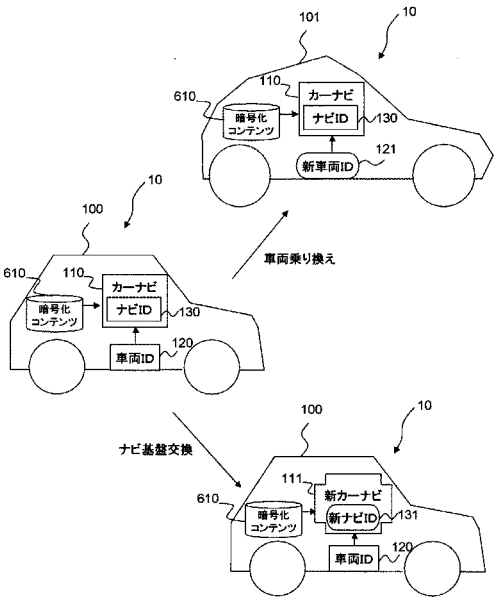
(71)出願人　591132335
株式会社ザナヴィ・インフォマティクス
神奈川県座間市広野台二丁目６番３５号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　関口　隆昭
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　加藤　博光
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】コンテンツ暗号化装置と暗号化プログラム、コンテンツ引継ぎ装置と引継ぎプログラム、コンテンツ引継ぎシステム、コンテンツの流用防止方法

(57)【要約】　（修正有）
【課題】機器を別環境に設置した場合には、コンテンツの引継ぎを行わない限り正常にコンテンツを再生できないようにすることを可能とする。
【解決手段】車両に搭載されたコンテンツ暗号化装置であって、記憶部には、コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施したコンテンツを記憶する領域と、権利情報を記憶する領域と、を備え、制御部は、コンテンツを記憶部に暗号化されたコンテンツとして取り込むコンテンツ取り込み部を備え、コンテンツ取り込み部は、コンテンツに対して所定の暗号鍵による暗号を施して記憶部に記憶し、暗号化装置識別子と、車両に搭載された車両制御装置から取得した車両識別子と、を用いて暗号鍵を算出するための権利情報を作成して記憶部に記憶する装置を提供する。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
車両に搭載されたコンテンツ暗号化装置であって、記憶部と、制御部と、を備え、
前記記憶部は、前記コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施した前記コンテンツを記憶する領域と、権利情報を記憶する領域と、を備え、
前記制御部は、前記コンテンツを前記記憶部に暗号化されたコンテンツとして取り込むコンテンツ取り込み部を備え、
前記コンテンツ取り込み部は、前記コンテンツに対して所定の暗号鍵による暗号を施して前記記憶部に記憶し、前記暗号化装置識別子と、前記車両に搭載された車両制御装置から取得した車両識別子と、を用いて前記暗号鍵を算出するための前記権利情報を作成して前記記憶部に記憶する、
ことを特徴とするコンテンツ暗号化装置。
【請求項２】
請求項１に記載のコンテンツ暗号化装置であって、
前記コンテンツ取り込み部は、前記暗号鍵を算出するための前記権利情報を作成する処理において、前記暗号鍵のうち第一の部分を前記暗号化装置識別子に基づいて作成し、前記暗号鍵のうち第二の部分を前記車両に搭載された車両制御装置から取得した車両識別子に基づいて作成する、
ことを特徴とするコンテンツ暗号化装置。
【請求項３】
請求項１に記載のコンテンツ暗号化装置であって、さらに、
前記制御部は、前記暗号化されたコンテンツの暗号を解除して再生するコンテンツ再生部を備え、
前記コンテンツ再生部は、前記暗号化装置識別子と、前記車両識別子と、を用いて前記権利情報から前記所定の暗号鍵を算出し、前記暗号化されたコンテンツの暗号を解除して再生する、
ことを特徴とするコンテンツ暗号化装置。
【請求項４】
請求項３に記載のコンテンツ暗号化装置であって、
前記コンテンツ暗号化装置の記憶部は、さらに、所定のブロック鍵を記憶した領域と、権利情報ブロックを記憶する領域と、を備え、
前記コンテンツ取り込み部は、前記権利情報を作成する処理において、前記暗号鍵に対して前記車両識別子と前記暗号化装置識別子とを用いて暗号を施して前記権利情報を作成し、前記暗号鍵と前記ブロック鍵とを用いて前記権利情報ブロックを作成し、前記権利情報と前記権利情報ブロックとを前記コンテンツ暗号化装置の記憶部に記憶する、
ことを特徴とするコンテンツ暗号化装置。
【請求項５】
コンテンツ引継ぎ装置であって、
記憶部と、外部記憶装置接続部と、入力受付部と、制御部と、を備え、
前記記憶部は、部分ブロック鍵を記憶した領域を備え、
前記外部記憶装置接続部は接続された外部記憶装置に対し入出力を行い、
前記入力受付部は、識別子の入力を受け付け、
前記制御部は、前記入力受付部から受け付けた識別子と、前記記憶部に記憶された部分ブロック鍵とを用いて、前記外部記憶装置に記憶された権利情報ブロックから権利情報を作成して前記外部記憶装置に記憶させる、
ことを特徴とするコンテンツ引継ぎ装置。
【請求項６】
請求項５に記載のコンテンツ引継ぎ装置であって、
前記制御部は、前記権利情報ブロックから前記権利情報を作成する処理において、前記

入力受付部から受け付けた識別子を暗号鍵として前記部分ブロック鍵情報の所定の桁に暗号を施し、暗号を施した前記部分ブロック鍵情報の所定の桁の値を元に前記権利情報を作成する、
ことを特徴とするコンテンツ引継ぎ装置。
【請求項７】
車両に搭載されたコンテンツ暗号化装置のコンテンツ暗号化プログラムであって、
前記コンテンツ暗号化装置は、
記憶部と、制御部と、を備え、
前記記憶部は、前記コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施した前記コンテンツを記憶する領域と、権利情報を記憶する領域と、を備え、
前記制御部に、
前記コンテンツに対して所定の暗号鍵による暗号を施して前記記憶部に記憶する手順と、
前記暗号化装置識別子と、前記車両に搭載された車両制御装置から取得した車両識別子と、を用いて前記暗号鍵を算出するための前記権利情報を作成して前記記憶部に記憶する手順と、
を実行させることを特徴とするコンテンツ暗号化プログラム。
【請求項８】
請求項７に記載のコンテンツ暗号化プログラムであって、さらに、
前記制御部に、
前記暗号化装置識別子と、前記車両識別子と、を用いて前記権利情報から前記所定の暗号鍵を算出する手順と、
前記暗号化されたコンテンツの暗号を解除して再生する手順と、
を実行させることを特徴とする特徴とするコンテンツ暗号化プログラム。
【請求項９】
請求項８に記載のコンテンツ暗号化プログラムであって、
前記コンテンツ暗号化装置の記憶部は、さらに、所定のブロック鍵を記憶した領域と、権利情報ブロックを記憶する領域と、を備え、
前記制御部に、
前記権利情報を作成する手順において、前記暗号鍵に対して前記車両識別子と前記暗号化装置識別子とを用いて暗号を施して前記権利情報を作成する手順と、
前記暗号鍵と前記ブロック鍵とを用いて前記権利情報ブロックを作成する手順と、
前記権利情報と前記権利情報ブロックとを前記コンテンツ暗号化装置の記憶部に記憶する手順と、
を実行させることを特徴とするコンテンツ暗号化プログラム。
【請求項１０】
コンテンツ引継ぎ装置のコンテンツ引継ぎプログラムであって、
前記コンテンツ引継ぎ装置は、
記憶部と、外部記憶装置接続部と、入力受付部と、制御部と、を備え、
前記記憶部は、部分ブロック鍵を記憶した領域を備え、
前記外部記憶装置接続部に、接続された外部記憶装置に対し入出力を行う手順と、
前記入力受付部に、識別子の入力を受け付ける手順と、
前記制御部に、前記入力受付部から受け付けた識別子と、前記記憶部に記憶された部分ブロック鍵とを用いて、前記外部記憶装置に記憶された権利情報ブロックから権利情報を作成して前記外部記憶装置に記憶させる手順と、
を実行させることを特徴とするコンテンツ引継ぎプログラム。
【請求項１１】
請求項１０に記載のコンテンツ引継ぎプログラムであって、
前記制御部に、前記権利情報ブロックから前記権利情報を作成させる手順において、前

記入力受付部から受け付けた識別子を暗号鍵として前記部分ブロック鍵情報の所定の桁に暗号を施し、暗号を施した前記部分ブロック鍵情報の所定の桁の値を元に前記権利情報を作成する手順、
を実行させることを特徴とするコンテンツ引継ぎプログラム。
【請求項１２】
コンテンツ引継ぎシステムであって、
車両制御装置は、
車両を識別する車両識別子を記憶した記憶部を備え、
前記車両制御装置が搭載された車両に搭載されたコンテンツ暗号化装置は、記憶部と、制御部と、を備え、
前記コンテンツ暗号化装置の記憶部は、前記コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施した前記コンテンツを記憶する領域と、権利情報を記憶する領域と、所定のブロック鍵を記憶した領域と、権利情報ブロックを記憶する領域と、を備え、
前記コンテンツ暗号化装置の制御部は、
前記コンテンツに対して所定の暗号鍵による暗号を施して前記コンテンツ暗号化装置の記憶部に記憶させ、
前記暗号化装置識別子と、前記車両識別子と、を用いて前記暗号鍵に暗号を施して前記暗号鍵を算出するための前記権利情報を作成して前記コンテンツ暗号化装置の記憶部に記憶させ、
前記暗号鍵と前記ブロック鍵とを用いて前記権利情報ブロックを作成させ、
前記権利情報と前記権利情報ブロックとを前記コンテンツ暗号化装置の記憶部に記憶させ、
さらに、コンテンツ引継ぎ装置は、制御部と、部分ブロック鍵を記憶した領域を備える記憶部を備え、
前記コンテンツ引継ぎ装置の制御部は、新たな車両識別子の入力を受け付け、
受け付けた前記新たな車両識別子と、前記部分ブロック鍵と、を用いて、前記権利情報ブロックから新たな権利情報を作成して前記コンテンツ暗号化装置の記憶部に記憶する、
ことを特徴とするコンテンツ引継ぎシステム。
【請求項１３】
コンテンツ引継ぎシステムであって、
車両制御装置は、
車両を識別する車両識別子を記憶した記憶部を備え、
前記車両制御装置が搭載された車両に搭載されたコンテンツ暗号化装置は、記憶部と、制御部と、を備え、
前記コンテンツ暗号化装置の記憶部は、前記コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施した前記コンテンツを記憶する領域と、権利情報を記憶する領域と、所定のブロック鍵を記憶した領域と、権利情報ブロックを記憶する領域と、を備え、
前記コンテンツ暗号化装置の制御部は、
前記コンテンツに対して所定の暗号鍵による暗号を施して前記コンテンツ暗号化装置の記憶部に記憶させ、
前記暗号化装置識別子と、前記車両識別子と、を用いて前記暗号鍵に暗号を施して前記暗号鍵を算出するための前記権利情報を作成して前記コンテンツ暗号化装置の記憶部に記憶させ、
前記暗号鍵と前記ブロック鍵とを用いて前記権利情報ブロックを作成させ、
前記権利情報と前記権利情報ブロックとを前記コンテンツ暗号化装置の記憶部に記憶させ、
さらに、コンテンツ引継ぎ装置は、制御部と、部分ブロック鍵を記憶した領域を備える記憶部を備え、

前記コンテンツ引継ぎ装置の制御部は、新たなコンテンツ暗号化装置の識別子の入力を受け付け、
受け付けた前記新たなコンテンツ暗号化装置の識別子と、前記部分ブロック鍵と、を用いて、前記権利情報ブロックから新たな権利情報を作成して前記コンテンツ暗号化装置の記憶部に記憶する、
ことを特徴とするコンテンツ引継ぎシステム。
【請求項１４】
コンテンツの流用防止方法であって、
車両制御装置は、
車両を識別する車両識別子を記憶した記憶部を備え、
前記車両制御装置が搭載された車両に搭載されたコンテンツ暗号化装置は、記憶部と、制御部と、を備え、
前記コンテンツ暗号化装置の記憶部は、前記コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施した前記コンテンツを記憶する領域と、権利情報を記憶する領域と、を備え、
前記コンテンツ暗号化装置の制御部は、
前記コンテンツに対して所定の暗号鍵による暗号を施して前記コンテンツ暗号化装置の記憶部に記憶するステップと、
前記暗号化装置識別子と、前記車両識別子と、を用いて前記暗号鍵を算出するための前記権利情報を作成し、前記コンテンツ暗号化装置の記憶部に記憶するステップと、
を実行することを特徴とするコンテンツの流用防止方法。
【請求項１５】
請求項１４に記載のコンテンツの流用防止方法であって、さらに、
前記コンテンツ暗号化装置の制御部は、
前記暗号化装置識別子と、前記車両識別子と、を用いて前記権利情報から前記所定の暗号鍵を算出し、前記暗号化されたコンテンツの暗号を解除して再生するステップ、
を実行することを特徴とするコンテンツの流用防止方法。
【請求項１６】
請求項１４または１５に記載のコンテンツの流用防止方法であって、
前記コンテンツ暗号化装置の記憶部は、さらに、所定のブロック鍵を記憶した領域と、権利情報ブロックを記憶する領域と、を備え、
前記制御部は、前記権利情報を作成するステップにおいて、
前記暗号鍵に対して前記車両識別子と前記暗号化装置識別子とを用いて暗号を施して前記権利情報を作成するステップと、
前記暗号鍵と前記ブロック鍵とを用いて前記権利情報ブロックを作成するステップと、
前記権利情報と前記権利情報ブロックとを前記コンテンツ暗号化装置の記憶部に記憶するステップと、
を実行し、
さらに、コンテンツ引継ぎ装置は、部分ブロック鍵を記憶した領域を備える記憶部を備え、
前記コンテンツ引継ぎ装置は、
新たな車両識別子の入力を受け付ける入力受付ステップと、
前記入力受付ステップにて受け付けた前記新たな車両識別子と、前記部分ブロック鍵と、を用いて、前記権利情報ブロックから新たな権利情報を作成して前記コンテンツ暗号化装置の記憶部に記憶するステップと、
を実行することを特徴とするコンテンツの流用防止方法。
【請求項１７】
請求項１４または１５に記載のコンテンツの流用防止方法であって、
前記コンテンツ暗号化装置の記憶部は、さらに、所定のブロック鍵を記憶した領域と、権利情報ブロックを記憶する領域と、を備え、

前記制御部は、前記権利情報を作成するステップにおいて、
前記暗号鍵に対して前記車両識別子と前記暗号化装置識別子とを用いて暗号を施して前記権利情報を作成するステップと、
前記暗号鍵と前記ブロック鍵とを用いて前記権利情報ブロックを作成するステップと、
前記権利情報と前記権利情報ブロックとを前記コンテンツ暗号化装置の記憶部に記憶するステップと、
を実行し、
さらに、コンテンツ引継ぎ装置は、部分ブロック鍵を記憶した領域を備える記憶部を備え、
前記コンテンツ引継ぎ装置は、
新たな暗号化装置識別子の入力を受け付ける入力受付ステップと、
前記入力受付ステップにて受け付けた前記新たな暗号化装置識別子と、前記部分ブロック鍵と、を用いて、前記権利情報ブロックから新たな権利情報を作成して前記コンテンツ暗号化装置の記憶部に記憶するステップと、
を実行することを特徴とするコンテンツの流用防止方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツを暗号化する技術に関する。
【背景技術】
【０００２】
従来、リッピング等により記憶装置に取り込まれた音楽コンテンツ等は、著作権を保護するために、特定の機器で無ければ利用できないよう、機器毎に異なる鍵情報を用いて暗号化する場合があった。しかし、当該機器の買い替え等により移設が必要となる場合には、著作権を保護しつつ買い替えた機器での利用を実現する必要がある。このような場合には、例えば、特許文献１のように、異なる機器に当該音楽コンテンツ等を移設する際に、サーバが移設先の機器に固有の暗号鍵を発行し、移設元の暗号鍵を無効にする技術を用いることで、コンテンツを無制限にコピーされるのを防ぐことができる。
【０００３】
【特許文献１】特許公開２００７－１８８１２０号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかし、上記特許文献１に記載の技術では、コンテンツを記憶した機器が別の環境で再生可能であるため、例えばコンテンツを記憶した機器を再販された場合等に、著作権の保護が不十分となる可能性がある。
【０００５】
そこで、本発明は、機器を別環境に設置した場合には、コンテンツの引継ぎを行わない限り正常にコンテンツを再生できないようにする技術の提供を目的とする。
【課題を解決するための手段】
【０００６】
本願に係るコンテンツ引継ぎの技術は、車両に搭載されたコンテンツ暗号化装置において、コンテンツを暗号化して取り込むと共に、その暗号化に用いた暗号鍵を車両固有の識別子とコンテンツ暗号化装置固有の識別子との両方を用いて暗号化する。
【０００７】
具体的には、車両に搭載されたコンテンツ暗号化装置であって、記憶部と、制御部と、を備え、前記記憶部は、前記コンテンツ暗号化装置を識別する暗号化装置識別子を記憶した領域と、暗号を施した前記コンテンツを記憶する領域と、権利情報を記憶する領域と、を備え、前記制御部は、前記コンテンツを前記記憶部に暗号化されたコンテンツとして取り込むコンテンツ取り込み部を備え、前記コンテンツ取り込み部は、前記コンテンツに対

して所定の暗号鍵による暗号を施して前記記憶部に記憶し、前記暗号化装置識別子と、前記車両に搭載された車両制御装置から取得した車両識別子と、を用いて前記暗号鍵を算出するための前記権利情報を作成して前記記憶部に記憶する、ことを特徴とする。

【発明の効果】

【０００８】

本発明によれば、機器を別環境に設置した場合には、記憶されたコンテンツを再生できないよう制限することが可能となる。

【発明を実施するための最良の形態】

【０００９】

以下に、本発明の実施形態について図１～図２３を用いて説明する。

【００１０】

まず、図１～図６を用いて、本発明の概要について説明する。

【００１１】

まず、図１に示すように、車両１００は、カーナビ（カーナビゲーション装置）１１０と、車両１００に固有の車両ＩＤ（車両識別子）１２０と、暗号が施された暗号化コンテンツ６１０と、を備える。暗号化コンテンツ６１０は、カーナビ１１０により再生される楽曲データ等に暗号を施したものである。

【００１２】

カーナビ１１０は、暗号化コンテンツ６１０を再生する際に、車両ＩＤ１２０と、カーナビに備えられたナビＩＤ（ナビ識別子）１３０と、を用いて暗号化コンテンツ６１０に施された暗号を解除して復号する。

【００１３】

すなわち、車両１００を車両１０１に乗り換えた場合や、カーナビ１１０のナビ基盤を部品交換して新カーナビ１１１に変更した場合には、新車両ＩＤ１２１あるいは新ナビＩＤ１３１を用いて暗号を解除することになる。

【００１４】

しかし、新車両ＩＤ１２１や、新ナビＩＤ１３１をそのまま使用して暗号化コンテンツ６１０の暗号の解除を試みた場合には、新車両ＩＤ１２１あるいは新ナビＩＤ１３１では、もとの車両ＩＤ１２０とナビＩＤ１３０の組み合わせを再現できないため、暗号化コンテンツ６１０の暗号の解除に失敗してしまう。

【００１５】

つまり、車両１０１への乗り換えの際に車両販売店を経由しない場合や、カーナビ１１０の交換が正当な修理業者でない場合には、このように暗号の解除に失敗してしまうことにより、コンテンツの流用を実態的に抑止することができるため、著作権の保護が実現される。

【００１６】

しかし、正当な車両１０１への乗り換え（例えば販売店での車両の買い替え）、カーナビ１１０の正当な交換（カーナビ修理業者による正規品の修理交換）の場合には、暗号の解除を失敗してしまうことは、利用者の正当な使用を阻害することを意味する。

【００１７】

そのため、正当な乗り換えや修理の場合には、新車両ＩＤ１２１あるいは新ナビＩＤ１３１を用いて暗号化コンテンツ６１０の暗号を解除することができるようにする必要がある。

【００１８】

図２～図６に、本願におけるコンテンツの暗号化および暗号の解除に必要な情報の流れを示す。

【００１９】

図２には、コンテンツ暗号化装置２００がコンテンツ６００に対し可逆的に暗号を施して暗号化コンテンツ６１０を作成する際の情報の流れと、暗号化コンテンツ６１０の暗号を解除してコンテンツ６００を得る際の情報の流れが記載されている。

【００２０】
カーナビゲーション装置やオーディオ再生装置を含むコンテンツ暗号化装置２００がコンテンツ６００に暗号を施す際には、暗号鍵（コンテンツ暗号鍵）４を用いる。
【００２１】
そして、コンテンツ暗号化装置２００は、後述するブロック鍵（ＢＬＫ）６５０を元に決定したデータ構成のパターンに従って、暗号鍵４を暗号化した値を生成して、後述する権利情報ブロック（ＲＩＢ）６３０として記憶する。
【００２２】
また、コンテンツ暗号化装置２００は、車両ＩＤ１２０（後述する車両識別子ＶＩＤ３１１に相当する）とナビＩＤ１３０（後述する暗号化装置識別子ＮＩＤ６４０に相当する）を合成した値を鍵として暗号鍵４に暗号を施し、権利情報（ＲＩ）６２０として記憶する。
【００２３】
コンテンツ暗号化装置２００は、暗号化コンテンツ６１０の暗号を解除する際には、車両ＩＤ１２０とナビＩＤ１３０を合成した値を鍵として権利情報（ＲＩ）６２０の暗号を解除し、復号鍵４（暗号鍵４と同一のもの）を取得する。そして、取得した復号鍵４を用いて暗号化コンテンツ６１０の暗号を解除し、コンテンツ６００を取得する。
【００２４】
以上が、正常な状態でのコンテンツ６００の暗号化・暗号の解除の際の情報の流れである。
【００２５】
図３には、車両１００を車両１０１に乗り換え、コンテンツ暗号化装置２００はそのまま流用して設置した場合の情報の流れが示されている。
【００２６】
図１に示すのと同様に、車両を乗り換えて、コンテンツ暗号化装置２００を流用する場合には、コンテンツ暗号化装置２００は、乗り換え前の車両１００において記憶された暗号化コンテンツ６１０の暗号を解除するために必要な復号鍵４を得る必要がある。
【００２７】
復号鍵４を得るために、コンテンツ暗号化装置２００は、乗換え後の車両１０１に備えられた新車両ＩＤ１２１を用いて権利情報（ＲＩ）６２０から暗号鍵４を取得する。
【００２８】
しかし、権利情報（ＲＩ）６２０を作成した際、すなわち暗号化を行った際の車両ＩＤ１２０と異なる値である新たな車両ＩＤ１２１を用いて暗号を解除することになるため、暗号化コンテンツ６１０を正常に暗号を解除できず、コンテンツ暗号化装置２００は誤りのある復号鍵４を得る。誤りのある復号鍵４を用いて暗号化コンテンツ６１０の暗号を解除すると、解除に失敗し、コンテンツ６００を正常に取得することはできない。
【００２９】
図３では、車両１０１に乗り換えた場合に暗号化コンテンツ６１０の暗号の解除が失敗することを示しているが、同様に、コンテンツ暗号化装置２００の制御基盤装置を交換した場合には、車両識別子１２０には変更はないが、コンテンツ暗号化装置２００は別のコンテンツ暗号化装置２００となってしまうため、暗号化を行った際のナビＩＤ１３０と異なる新ナビＩＤ１３１を用いて暗号の解除を行うことになる。そのため、正常に暗号の解除を行うことができない。
【００３０】
そこで、利用者の正当な使用を阻害しないため、正当な車両の乗り換えやコンテンツ暗号化装置の修理の場合には、新車両ＩＤ１２１あるいは新ナビＩＤ１３１を用いて暗号化コンテンツ６１０の暗号を解除することができるようにする技術が必要となる。この技術について、図４～図６を用いて説明する。
【００３１】
図４は、図３に示した暗号化コンテンツ６１０の暗号解除の失敗を回避する暗号解除の

処理におけるデータの流れを示す図である。

【００３２】

図４に示すように、車両１０１に乗り換えがあった場合に、新車両ＩＤ１２１を用いて暗号化コンテンツ６１０の暗号の解除を行う場合のデータの流れは、以下となる。

【００３３】

コンテンツ暗号化装置２００は、暗号化コンテンツ６１０の暗号を解除する際に、車両ＩＤ１２１と、ナビＩＤ１３０と、を合成した値を鍵としてブロック鍵（ＢＬＫ）６５０に対して可逆に暗号を施し、得られた値をデータ構成のパターンとして用いて権利情報ブロック（ＲＩＢ）６３０から値を取り出し、新たな権利情報（ＲＩ）６２０を作成する。

【００３４】

そして、コンテンツ暗号化装置２００は、新車両ＩＤ１２１と、ナビＩＤ１３０と、を合成した値を鍵として、新たな権利情報（ＲＩ）６２０の暗号を解除し、暗号化コンテンツ６１０を作成した際に用いた暗号鍵と同一の鍵である復号鍵４を得る。そして、コンテンツ暗号化装置２００は、復号鍵４を用いて暗号化コンテンツ６１０の暗号を解除し、コンテンツ６００を取得する。

【００３５】

図５は、図４と同様、暗号解除の失敗を回避した暗号解除の処理におけるデータの流れを示す図である。

【００３６】

図５では、基盤を交換して新たなコンテンツ暗号化装置を用いる場合に、新たなナビＩＤ１３１を用いて暗号化コンテンツ６１０の暗号を解除する場合のデータの流れを示す。

【００３７】

コンテンツ暗号化装置２００は、暗号化コンテンツ６１０の暗号を解除する際に、車両ＩＤ１２０と、新ナビＩＤ１３１と、を合成した値を鍵としてブロック鍵（ＢＬＫ）６５０に対して可逆に暗号を施し、得られた値をデータ構成のパターンとして用いて権利情報ブロック（ＲＩＢ）６３０から値を取り出し、新たな権利情報（ＲＩ）６２０を作成する。

【００３８】

そして、コンテンツ暗号化装置２００は、車両ＩＤ１２０と、新ナビＩＤ１３１と、を合成した値を鍵として、新たな権利情報（ＲＩ）６２０の暗号を解除することで、暗号化コンテンツ６１０を作成した際に用いた暗号鍵と同一の復号鍵４を得る。そして、コンテンツ暗号化装置２００は、復号鍵４を用いて暗号化コンテンツ６１０の暗号を解除してコンテンツ６００を取得することに成功する。

【００３９】

図６（ａ）と図６（ｂ）と、は、それぞれ、図４、図５に示す暗号の解除を実現する仕組みを示す図である。

【００４０】

図６（ａ）には、暗号化装置提供者（コンテンツ暗号化装置２００の提供者、製造者）１から車両販売店（ディーラー）３に対して部分ブロック鍵（ディーラー用）４２４を提供することが記載されている。部分ブロック鍵（ディーラー用）４２４は、ブロック鍵（ＢＬＫ）６５０のうち車両ＩＤにより暗号を施される桁以外の桁についてマスクデータを格納した鍵である。この部分ブロック鍵（ディーラー用）４２４を用いることで、権利情報（ＲＩ）６２０の、車両ＩＤを用いて暗号を解除する桁の情報を更新して新たな権利情報（ＲＩ）６２０を作成することができる。ただし、権利情報（ＲＩ）６２０のナビＩＤを用いて暗号を解除する桁の情報を更新することはできない。

【００４１】

これにより、車両販売店３は、車両ＩＤの変更に伴う権利情報の更新を正当に行うことができる、すなわち車両乗り換えの際にコンテンツ暗号化装置２００を流用することが可能となる上、コンテンツ暗号化装置２００の制御基盤装置の交換の際にはコンテンツを流用することができるように対応することはできない。

【００４２】
図６（ｂ）には、暗号化装置提供者（コンテンツ暗号化装置２００の提供者、製造者）１から暗号化装置修理業者２に対して部分ブロック鍵（暗号化装置修理業者用）４２３を提供することが記載されている。部分ブロック鍵（暗号化装置修理業者用）４２３は、ブロック鍵（ＢＬＫ）６５０のうちナビＩＤにより暗号される桁以外の桁についてマスクデータを格納した鍵である。この部分ブロック鍵（暗号化装置修理業者用）４２３を用いることで、権利情報（ＲＩ）６２０の、ナビＩＤを用いて暗号を解除する桁の情報を更新して新たな権利情報（ＲＩ）６２０を作成することができる。ただし、権利情報（ＲＩ）６２０の車両ＩＤを用いて暗号を解除する桁の情報を更新することはできない。
【００４３】
これにより、暗号化装置修理業者２は、コンテンツ暗号化装置２００の制御基盤装置の変更に伴う権利情報の更新を正当に行うことができる、すなわち制御基盤装置交換の際にコンテンツを流用することが可能となるが、車両乗り換えの際にはコンテンツ暗号化装置を流用することができるように対応することはできない。
【００４４】
図７～図２３を用いて、本発明の第一の実施形態のコンテンツ引継ぎシステム１０の詳細について説明する。
【００４５】
図７は、本発明の第一の実施形態のコンテンツ引継ぎシステム１０を示す図である。コンテンツ引継ぎシステム１０は、車両１００内に設置されたコンテンツ暗号化装置２００と、車両外の車両販売店等に設置されるコンテンツ引継ぎ装置４００と、を有する。
【００４６】
コンテンツ引継ぎ装置４００は、ＰＣ（パーソナルコンピュータ）や、ワークステーション、各種携帯電話端末、ＰＤＡ（Personal Digital Assistant）などの端末装置である。
【００４７】
コンテンツ暗号化装置２００は、車体ネットワーク５００を介して車両制御装置３００と接続する。
【００４８】
コンテンツ暗号化装置２００は、例えば、カーナビゲーション装置やカーオーディオ装置などであり、音楽や動画などをリッピングして記憶装置に記憶し、再生することができる。車両制御装置３００は、車両の制御を行うことのできる装置であり、例えば、ＥＣＵ（Electronic Control Unit）等の自動車用デバイスの制御用マイクロコンピュータユニットである。
【００４９】
車体ネットワーク５００は、車体に取り付けられた各種電子デバイスの間で通信や同期を行うためのネットワークであり、例えば、ＣＡＮ（Controller Area Network）などのプロトコルにより通信を行うことができるネットワークである。
【００５０】
次に、コンテンツ暗号化装置２００について説明する。
【００５１】
コンテンツ暗号化装置２００は、図８に示すように、制御部２１０と、通信部２２０と、記憶部２３０と、を有する。
【００５２】
制御部２１０は、楽曲や映像のコンテンツの取り込みを行うコンテンツ取り込み部２１１と、取り込んだコンテンツを再生するコンテンツ再生部２１２と、を有する。
【００５３】
コンテンツ取り込み部２１１は、図示しない記憶媒体読取装置を介して、ＣＤ，ＤＶＤ，またはその他の記憶媒体から音楽や映像等のコンテンツを取得して、記憶部２３０のコンテンツ記憶領域２３１に記憶させる。その際に、著作権の保護を目的として、コンテン

ツに暗号を施して暗号化コンテンツとして記憶させる。
【００５４】
コンテンツ再生部２１２は、コンテンツ取り込み部２１１によって記憶装置２３０のコンテンツ記憶領域２３１に記憶された暗号化コンテンツの暗号を解除して、楽曲や映像を再生する。
【００５５】
通信部２２０は、車体ネットワーク５００に接続された他の機器に対して、ＣＡＮ等のプロトコルに準拠するデータの送信、受信を行う。
【００５６】
記憶部２３０は、コンテンツ記憶領域２３１と、権利情報記憶領域２３２と、権利情報ブロック記憶領域２３３と、暗号化装置識別子記憶領域２３４と、ブロック鍵記憶領域２３５と、を備える。
【００５７】
図９は、記憶部２３０の構成を示す図である。
【００５８】
コンテンツ記憶領域２３１は、暗号化されたコンテンツである暗号化コンテンツ６１０を複数記憶する記憶領域である。
【００５９】
権利情報記憶領域２３２は、暗号化コンテンツ６１０と対応する権利情報（ＲＩ）６２０を複数記憶する記憶領域である。
【００６０】
権利情報ブロック記憶領域２３３は、暗号化コンテンツ６１０と対応する権利情報ブロック（ＲＩＢ）６３０を複数記憶する記憶領域である。
【００６１】
暗号化装置識別子記憶領域２３４は、コンテンツ暗号化装置２００の制御基盤装置毎に備えるシリアル番号などの暗号化装置識別子（ＮＩＤ）６４０を記憶する記憶領域である。
【００６２】
ブロック鍵記憶領域２３５は、ブロック鍵２００を記憶する記憶領域である。
【００６３】
図８の説明に戻り、車両制御装置３００について説明する。
【００６４】
車両制御装置３００は、車両識別子記憶領域３１０と、通信部３２０と、を有する。
【００６５】
車両識別子記憶領域３１０は、車両固有の情報である車体番号等の車両識別子（ＶＩＤ）３１１を記憶する記憶領域である。
【００６６】
通信部３２０は、車体ネットワーク５００に接続された他の機器に対してＣＡＮ等のプロトコルに準拠するデータの送信、受信を行う。
【００６７】
次に、コンテンツ引継ぎ装置４００について説明する。
【００６８】
コンテンツ引継ぎ装置４００は、制御部４１０と、記憶部４２０と、外部記憶装置接続部４３０と、を有する。
【００６９】
制御部４１０は、記憶装置に記憶されたコンテンツを再生可能に引き継ぐための処理を行うコンテンツ引継ぎ部４１１と、使用者からの入力操作を受付ける入力受付部４１２と、表示を行う出力表示部４１３と、を備える。
【００７０】
コンテンツ暗号化装置２００の制御基盤装置を修理等により交換する場合には、コンテ

ンツ引継ぎ部４１１は、記憶装置２３０を乗せ換える先の新たなコンテンツ暗号化装置２００が備える暗号化装置識別子（ＮＩＤ）６４０と、車両１００が備える車両識別子（ＶＩＤ）３１１と、を元に、権利情報ブロック（ＲＩＢ）６３０から所定のパターンに従って１６バイトの情報を特定する。

【００７１】

そして、コンテンツ引継ぎ部４１１は、特定した１６バイトのデータを記憶装置２３０の権利情報記憶領域２３２に、権利情報（ＲＩ）６２０として記憶する。

【００７２】

または、車両１００を乗り換えてコンテンツ暗号化装置２００を流用する場合には、コンテンツ引継ぎ部４１１は、コンテンツ暗号化装置２００を乗せ換える先の新たな車両１０１が備える車両識別子（ＶＩＤ）３１１と、コンテンツ暗号化装置２００が備える暗号化装置識別子（ＮＩＤ）６４０と、を元に、権利情報ブロック（ＲＩＢ）６３０から所定の１６バイトを特定する。

【００７３】

そして、コンテンツ引継ぎ部４１１は、特定した１６バイトのデータを記憶装置２３０の権利情報記憶領域２３２に、権利情報（ＲＩ）６２０として記憶し、新たな権利情報とする。

【００７４】

入力受付部４１２は、コンテンツ引継ぎ装置４００が備える入力装置であるキーボードやマウス、マイクロフォン等からの入力情報を受け付ける。

【００７５】

出力表示部４１３は、コンテンツ引継ぎ装置４００が備える出力装置であるディスプレイ装置やスピーカ装置等に出力情報を表示する。

【００７６】

記憶部４２０は、ブロック鍵記憶領域４２１と、部分ブロック鍵４２２を記憶するブロック鍵記憶領域４２１と、を有する。

【００７７】

外部記憶装置接続部４３０は、記憶装置を接続するためのインターフェイスを備えた接続部であり、インターフェイスに接続した記憶装置からの読み出しと、インターフェイスに接続した記憶装置への書き込みを行うことができる。

【００７８】

次に、権利情報記憶領域２３２に記憶された権利情報（ＲＩ）６２０のデータ構造について、図１０を用いて説明する。

【００７９】

権利情報（ＲＩ）６２０は、オフセット位置が１６進数表示でゼロからＦまでで表される１６バイトのデータ長を持つ。１６バイトのうち、最上位バイト、すなわち左端のバイト（オフセット０）から８バイト（オフセット（７））までは、暗号化装置識別子用権利情報（ＲＩ＿Ｎ）６２１を格納し、最下位バイト、すなわち右端のバイト（オフセットＦ）から８バイト（オフセット（８））までは、車両識別子用権利情報（ＲＩ＿Ｖ）６２２を格納するものである。

【００８０】

次に、権利情報ブロック記憶領域２３３に記憶された権利情報ブロック（ＲＩＢ）６３０のデータ構造について、図１１を用いて説明する。

【００８１】

権利情報ブロック（ＲＩＢ）６３０は、１行あたり１６バイトのデータ長を２５６行備えた（１６×２５６の）二次元配列のデータ構造を持つ。各行を構成する１６バイトのうち、最上位バイト、すなわち左端のバイト（オフセット０）から８バイト（オフセット（７））までは、暗号化装置識別子用権利情報ブロック（ＲＩＢ＿Ｎ）６３１を格納し、最下位バイト、すなわち右端のバイト（オフセットＦ）から８バイト（オフセット（８））までは、車両識別子用権利情報ブロック（ＲＩＢ＿Ｖ）６３２を格納するものである。

【００８２】
なお、権利情報ブロック（ＲＩＢ）６３０に含まれる要素を示すために、二次元座標を用いて表現する。例えば、（Ｄ，Ｃ）という座標は、権利情報ブロック（ＲＩＢ）６３０のうち、１３行目の、最上位桁から１２番目の要素を示す。すなわち、権利情報ブロック（ＲＩＢ）の座標は、（０，０）～（ＦＦ，Ｆ）の範囲により、含まれる全ての情報の座標をあらわすことができる。
【００８３】
次に、ブロック鍵記憶領域２３５に記憶されたブロック鍵（ＢＬＫ）６５０のデータ構造について、図１２を用いて説明する。
【００８４】
ブロック鍵（ＢＬＫ）６５０は、オフセット位置が１６進数表示でゼロからＦまでで表される１６バイトのデータ長を持つ。１６バイトのうち、最上位バイト、すなわち左端のバイト（オフセット０）から８バイト（オフセット（７））までは、暗号化装置識別子用ブロック鍵（ＢＬＫ＿Ｎ）６５１を格納し、最下位バイト、すなわち右端のバイト（オフセットＦ）から８バイト（オフセット（８））までは、車両識別子用ブロック鍵情報（ＢＬＫ＿Ｖ）６５２を格納するものである。
【００８５】
図１２に示すように、ブロック鍵６５３は、最上位バイトから８バイトまでは、例えば、Ｆ２，８７，Ｄ３，０１，ＥＡ，６７，９Ａ，８８，の値が格納されており、続く８バイトは、２１，Ａ６，３２，５Ｃ，３１，２０，ＥＣ，Ａ８，の値が格納されている。
【００８６】
次に、コンテンツ引継ぎ装置４００の記憶部４２０のブロック鍵記憶領域４２１に記憶される部分ブロック鍵４２２のデータ構造について、図１３を用いて説明する。
【００８７】
図１３（ａ）に示すように、部分ブロック鍵４２２は、１６バイトのデータ長を備える。
【００８８】
すなわち、部分ブロック鍵４２２は、オフセット位置を１６進数表示でゼロからＦまでの値で表すことができる。
【００８９】
部分ブロック鍵４２２は、コンテンツ引継ぎ装置４００の使用者によって予め値が決められ、記憶部４２０に記憶される。
【００９０】
例えば、図１３（ｂ）に示すように、暗号化装置修理業者が保持するコンテンツ引継ぎ装置４００に記憶される部分ブロック鍵４２３は、部分ブロック鍵長１６バイトのうち、最上位バイト、すなわち左端のバイト（オフセット０）から８バイト目（オフセット（７））までは、ブロック鍵（ＢＬＫ）６５０の同じオフセット位置にある値と同じ値（０ｘＦ２，０ｘ８７，０ｘＤ３，０ｘ０１，０ｘＥＡ，０ｘ６７，０ｘ９Ａ，０ｘ８８）を格納するものである。
【００９１】
そして、部分ブロック鍵４２３の先頭から９バイト目（オフセット（８））から最下位バイト、すなわち右端のバイト（オフセットＦ）までは、無意味なデータ、例えば０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦの値を格納するものである。
【００９２】
また例えば、図１３（ｃ）に示すように、ディーラーが保持するコンテンツ引継ぎ装置４００に記憶される部分ブロック鍵４２４は、部分ブロック鍵長１６バイトのうち、最上位バイト、すなわち左端のバイト（オフセット０）から８バイト目（オフセット（７））までは、無意味なデータ、例えば０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦを格納するものである。

【００９３】
そして、部分ブロック鍵４２４の先頭から９バイト目（オフセット（８））から最下位バイト、すなわち右端のバイト（オフセットＦ）までは、ブロック鍵（ＢＬＫ）６５０の同じオフセット位置にある値と同じ値（０ｘ２１，０ｘＡ６，０ｘ３２，０ｘ５Ｃ，０ｘ３１，０ｘ２０，０ｘＥＣ，０ｘＡ８）を格納するものである。
【００９４】
次に、本発明の方法の一実施の形態を示すコンテンツ引継ぎシステム１０を構成するハードウェアについて、図１４を用いて説明する。
【００９５】
図１４に示すコンテンツ引継ぎシステム１０では、コンテンツ暗号化装置２００は、車体ネットワーク５００を介して、車両制御装置３００と接続することができる。
【００９６】
コンテンツ暗号化装置２００は、ＣＰＵ（Central Processing Unit）２５０と、ＲＡＭ（Random Access Memory）２５１と、不揮発性メモリ２５２と、可搬記憶媒体読取装置２５３と、補助記憶装置２５４と、通信Ｉ／Ｆ（インターフェイス）２５５と、を有する。
【００９７】
不揮発性メモリ２５２は、例えばフラッシュメモリなど、外部から通電しなくとも記憶データが消滅しないメモリ装置である。
【００９８】
可搬記憶媒体読み取り装置２５３は、ＣＤ（Compact Disk）、ＤＶＤ（Digital Versatile Disk）などの記憶媒体２６０を読み取る装置である。
【００９９】
補助記憶装置２５４は、例えばハードディスク装置やフラッシュメモリなどの書き込みが可能な記憶装置を用いて実現され、ＲＡＭ２５１の記憶領域を補助的に拡張する記憶装置である。
【０１００】
通信Ｉ／Ｆ２５５は、車体ネットワーク５００などのネットワークを介して他の装置と通信を行う制御装置である。通信Ｉ／Ｆ２５５は、例えば、ＣＡＮ（Controller Area Network）やＬＩＮ（Local Interconnect Network）などの通信プロトコルに従って通信する。
【０１０１】
車両制御装置３００は、ＣＰＵ３５０と、ＲＯＭ（Read Only Memory）３５１と、通信Ｉ／Ｆ３５２と、を有する。
【０１０２】
ＲＯＭ３５１は、読み取り専用で、書き換えが不可能なメモリ装置である。
【０１０３】
通信Ｉ／Ｆ３５２は、車体ネットワーク５００などのネットワークを介して他の装置と通信を行う制御装置である。通信Ｉ／Ｆ２５５は、例えば、ＣＡＮやＬＩＮなどの通信プロトコルに従って通信する。
【０１０４】
コンテンツ引継ぎ装置４００は、ＣＰＵ４５０と、ＲＡＭ４５１と、不揮発性メモリ４５２と、補助記憶装置４５３と、入力装置４５４と、出力装置４５５と、外部記憶装置Ｉ／Ｆ４５６と、を有する。
【０１０５】
入力装置４５４はキーボードやマウス、あるいはタッチペン、その他ポインティングデバイスやマイクロフォンなどの入力を受け付ける装置である。
【０１０６】
出力装置４５５はディスプレイ装置やスピーカなど、視覚あるいは聴覚を通して情報を表示する装置である。

【０１０７】
外部記憶装置Ｉ／Ｆ４５６は、例えば引き継ぐ対象となるハードディスク装置やフラッシュメモリなどの不揮発性記憶装置と接続するためのインターフェイス装置である。
【０１０８】
コンテンツ暗号化装置２００のコンテンツ取り込み部２１１と、コンテンツ再生部２１２と、は、コンテンツ暗号化装置２００のＣＰＵ２５０に処理を行わせるプログラムによって実現される。
【０１０９】
プログラムはＲＡＭ２５１、不揮発性メモリ２５２、補助記憶装置２５４または記憶媒体２６０内に記憶され、実行にあたってＲＡＭ２５１上にロードされ、ＣＰＵ２５０により実行される。
【０１１０】
コンテンツ記憶領域２３１と、権利情報記憶領域２３２と、権利情報ブロック記憶領域２３３と、ブロック鍵記憶領域２３５と、は、コンテンツ暗号化装置２００の補助記憶装置２５４により実現される。
【０１１１】
暗号化装置識別子記憶領域２３４は、コンテンツ暗号化装置２００の不揮発性メモリ２５２により実現される。
【０１１２】
車両識別子記憶領域３１０は、車両制御装置３００のＲＯＭ３５１により実現される。
【０１１３】
コンテンツ引継ぎ装置４００のコンテンツ引継ぎ部４１１は、コンテンツ引継ぎ装置４００のＣＰＵ４５０に処理を行わせるプログラムによって実現される。
【０１１４】
プログラムはＲＡＭ４５１、不揮発性メモリ４５２または補助記憶装置４５３内に記憶され、実行にあたってＲＡＭ４５１上にロードされ、ＣＰＵ４５０により実行される。
【０１１５】
ブロック鍵記憶領域４２１は、コンテンツ引継ぎ装置４００の補助記憶装置４５３により実現される。また、不揮発性メモリ４５２により実現されてもよい。
【０１１６】
次に、本実施形態におけるコンテンツ取り込み、コンテンツ再生、コンテンツ引継ぎに関する処理のフローについて、図１５～図２３を用いて説明する。
【０１１７】
図１５は、本実施形態のコンテンツ取り込み処理の例を示すフロー図である。
【０１１８】
コンテンツ取り込み処理は、コンテンツを取り込む指示が使用者からなされると開始される。または、これに限らず、例えばコンテンツが記憶されたＣＤやＤＶＤを再生させる際に処理を開始されるものであってもよい。
【０１１９】
まず、コンテンツ取り込み部２１１は、記憶媒体２６０などに記憶された楽曲や映像などの暗号化されていないコンテンツを読み出す（ステップＳ１０１）。
【０１２０】
そして、コンテンツ取り込み部２１１は、例えば１６バイト長のコンテンツ暗号鍵４（以降、ＣＥＫという）を、日時等の情報をシードとして生成する乱数を用いて作成する（ステップＳ１０２）。
【０１２１】
そして、コンテンツ取り込み部２１１は、ステップＳ１０２で作成したＣＥＫ４を用いて、ステップＳ１０１で読み出したコンテンツに暗号を施し、暗号化したコンテンツのデータを記憶部２３０のコンテンツ記憶領域２３１に暗号化コンテンツ６１０として記憶する（ステップＳ１０３）。

【０１２２】
そして、コンテンツ取り込み部２１１は、ＣＥＫ４と、記憶装置２３０のブロック鍵記憶領域２３５に記憶されたブロック鍵（ＢＬＫ）６５０と、を用いて、権利情報ブロック（ＲＩＢ）６３０を作成し、記憶装置２３０の権利情報ブロック記憶領域２３３に記憶する（ステップＳ１０４）。
【０１２３】
具体的には、コンテンツ取り込み部２１１は、図１６に示すように、ＣＥＫ４の各桁（各バイト）の値に０ｘ００～０ｘＦＦまでの２５６通りの可逆の暗号化を施して得られた２５６通りの値を、権利情報ブロック（ＲＩＢ）６３０の各行の同オフセットに重複無く格納することで、権利情報ブロック（ＲＩＢ）６３０を作成する。
【０１２４】
本実施例では、コンテンツ取り込み部２１１は、重複無く権利情報ブロック（ＲＩＢ）６３０の各行にＣＥＫ４の暗号値を格納するために、ブロック鍵（ＢＬＫ）６５０の各桁（各バイト）の値に応じて、０ｘ００～０ｘＦＦまでの２５６通りの可逆の暗号化を施して得られた値をその格納先の行とする（ステップＳ１０４１～ステップＳ１０４７）。
【０１２５】
より具体的には、まず、コンテンツ取り込み部２１１は、ループ制御用の整数ｉとｊとを０で初期化する（ステップＳ１０４１）。
【０１２６】
そして、コンテンツ取り込み部２１１は、ｉの値が１６進数「ＦＦ」を超えるか否かを判定する（ステップＳ１０４２）。
【０１２７】
ｉの値が１６進数「ＦＦ」を超えない場合（ステップＳ１０４２の判定で「Ｎｏ」）には、コンテンツ取り込み部２１１は、ｊの値が１６進数「Ｆ」を超えるか否かを判定する（ステップＳ１０４３）。
【０１２８】
ｊの値が１６進数「Ｆ」を超えない場合（ステップＳ１０４３の判定で「Ｎｏ」）には、コンテンツ取り込み部２１１は、ブロック鍵（ＢＬＫ）６５０のｊ番目のオフセットに格納された値を変数ｉを鍵にして暗号化した値を、整数ｋに格納し、ＣＥＫのｊ番目のオフセットに格納された値を変数ｉを鍵にして暗号化した値を、権利情報ブロック（ＲＩＢ）６３０のｋ行目のオフセットｊ番目に格納する（ステップＳ１０４４）。
【０１２９】
そして、コンテンツ取り込み部２１１は、ｊの値を１増加させ、ステップＳ１０４３に処理を戻す（ステップＳ１０４５）。
【０１３０】
ｊの値が１６進数「Ｆ」を超える場合（ステップＳ１０４３の判定で「Ｙｅｓ」）には、コンテンツ取り込み部２１１は、ｉの値を１増加させる（ステップＳ１０４６）。
【０１３１】
そして、コンテンツ取り込み部２１１は、ｊの値を０に設定し、ステップＳ１０４２に処理を戻す（ステップＳ１０４７）。
【０１３２】
ｉの値が１６進数「ＦＦ」を超える場合（ステップＳ１０４２の判定で「Ｙｅｓ」）には、コンテンツ取り込み部２１１は、権利情報ブロック作成処理を終了させる。
【０１３３】
なお、図１６にて用いるｉ，ｊは、整数型変数であり、ＥＮＣと表す関数は、２つの引数を受付けて、第２引数である１バイトの情報に対して、第１引数をキーとして可逆変換を行い、１バイトの情報を返却する関数、すなわち暗号化関数である。
【０１３４】
図１７は、図１６の処理について、具体的な値を用いて説明する図である。
【０１３５】

ＣＥＫ４は、図１７に記載のあるように、0x0123456789ABCDEF0123456789ABCDEFとし、ブロック鍵（ＢＬＫ）６５０は、0xF287D301EA679A8821A6325C3120ECA8とする。

【０１３６】

図１７の（１）に示すように、（ｉ，ｊ）の組が（0x00，0x0）の場合には、コンテンツ取り込み部２１１は、ｋの値を、ブロック鍵（ＢＬＫ）６５０のｊ番目のオフセット、即ち左端（ゼロ番目のオフセット）の「0xF2」をｉの値すなわちゼロで暗号化した値、例えば0x04として得る。

【０１３７】

そして、権利情報ブロック（ＲＩＢ）６３０のｋ行、ｊ番目のオフセット位置に、ＣＥＫのｊ番目のオフセット値をｉの値すなわちゼロで暗号化した値、例えば0xABを格納する。

【０１３８】

同様に、図１７の（２）、（３）に示すように、（ｉ，ｊ）の組が（0x00，0x1）、（ｉ，ｊ）の組が（0x00，0x2）の場合についても値を算出し、権利情報ブロック（ＲＩＢ）６３０のｋ行、ｊ番目のオフセット位置に格納する。

【０１３９】

そして、コンテンツ取り込み部２１１は、ＣＥＫ４と、記憶装置２３０の暗号化装置識別子記憶領域２３４に記憶された暗号化装置識別子（ＮＩＤ）６４０と、車両制御装置３００の車両識別子記憶領域３１０に記憶された車両識別子（ＶＩＤ）３１１と、を用いて、権利情報（ＲＩ）６２０を作成し、記憶装置２３０の権利情報記憶領域２３２に記憶する（ステップＳ１０５）。

【０１４０】

具体的には、コンテンツ取り込み部２１１は、図１８に示すように、暗号化装置識別子（ＮＩＤ）６４０と、車両識別子（ＶＩＤ）３１１と、を連結して得られる変数ＩＤを算出し（ステップＳ１０５１）、ＣＥＫ４の各桁（各バイト）の値に、変数ＩＤの対応するオフセット位置にある値をキーとして可逆の暗号化を施し、得られた値を、権利情報（ＲＩ）６２０の同じオフセット位置に格納することで、権利情報（ＲＩ）６２０を作成する（ステップＳ１０５４）。

【０１４１】

より具体的には、まず、コンテンツ取り込み部２１１は、８バイトのデータ長を持つ暗号化装置識別子（ＮＩＤ）６４０と、８バイトのデータ長を持つ車両識別子（ＶＩＤ）３１１と、を結合して１６バイトの変数ＩＤに代入する（ステップＳ１０５１）。

【０１４２】

次に、コンテンツ取り込み部２１１は、ループ制御用の整数ｊを０で初期化する（ステップＳ１０５２）。

【０１４３】

そして、コンテンツ取り込み部２１１は、ｊの値が１６進数「Ｆ」を超えるか否かを判定する（ステップＳ１０５３）。

【０１４４】

ｊの値が１６進数「Ｆ」を超えない場合（ステップＳ１０５３の判定で「Ｎｏ」）には、コンテンツ取り込み部２１１は、コンテンツ暗号鍵（ＣＥＫ）４のｊ番目のオフセットに格納された値を、変数ＩＤのｊ番目のオフセットに格納された値を鍵として暗号化した値を算出し、暗号化した値を、権利情報（ＲＩ）６２０のオフセットｊ番目に格納する（ステップＳ１０５４）。

【０１４５】

そして、コンテンツ取り込み部２１１は、ｊの値を１増加させ、ステップＳ１０５３に処理を戻す（ステップＳ１０５５）。

【０１４６】

ｊの値が１６進数「Ｆ」を超える場合（ステップＳ１０５３の判定で「Ｙｅｓ」）には、コンテンツ取り込み部２１１は、権利情報作成処理を終了させる。

【０１４７】
なお、図１８にて用いるｊは、整数型変数である。
【０１４８】
ＥＮＣで表される関数は、暗号を施す関数である。ＥＮＣで表される関数は、２つの引数を受付けて、第２引数である１バイトの情報に対して、第１引数をキーとして可逆変換を行い、１バイトの情報を返却する関数である。
【０１４９】
このように、ステップＳ１０１～Ｓ１０５の処理により、コンテンツ取り込み部２１１は、記憶媒体２６０などに記憶された楽曲や映像などのコンテンツを取り込む。
【０１５０】
次に、コンテンツ再生処理について、図１９を用いて説明する。
【０１５１】
図１９は、コンテンツ取り込み処理により取り込んだコンテンツを再生する処理である。
【０１５２】
コンテンツ再生部２１２は、再生する暗号化コンテンツ６１０の暗号を解除して再生する。
【０１５３】
その際に、コンテンツ再生部２１２は、コンテンツ取り込み処理のステップＳ１０５において算出した権利情報（ＲＩ）６２０を元情報として、暗号を施すのに用いたＣＥＫ４を算出し、暗号化コンテンツ６１０の暗号の解除を行う。
【０１５４】
まず、コンテンツ再生部２１２は、記憶装置２３０の暗号化装置識別子記憶領域２３４に記憶された暗号化装置識別子（ＮＩＤ）６４０と、車両制御装置３００の車両識別子記憶領域３１０に記憶された車両識別子（ＶＩＤ）３１１と、を連結して、変数ＩＤに格納する（ステップＳ２０１）。
【０１５５】
具体的には、コンテンツ再生部２１２は、８バイトのデータ長を持つ暗号化装置識別子（ＮＩＤ）６４０と、８バイトのデータ長を持つ車両識別子（ＶＩＤ）３１１と、を結合して１６バイトの変数ＩＤに代入する。
【０１５６】
そして、コンテンツ再生部２１２は、権利情報（ＲＩ）６２０のｊ番目のオフセット位置にある値に変数ＩＤのｊ番目のオフセット位置にある値をキーとして可逆の暗号化を施し、得られた値を、ＣＥＫ４のｊ番目のオフセット位置に格納することで、ＣＥＫ４を復元する（ステップＳ２０２～ステップＳ２０５）。
【０１５７】
具体的には、コンテンツ再生部２１２は、ループ制御用の整数ｊを０で初期化する（ステップＳ２０２）。
【０１５８】
そして、コンテンツ再生部２１２は、ｊの値が１６進数「Ｆ」を超えるか否かを判定する（ステップＳ２０３）。
【０１５９】
ｊの値が１６進数「Ｆ」を超えない場合（ステップＳ２０３の判定で「Ｎｏ」）には、コンテンツ再生部２１２は、権利情報（ＲＩ）６２０のｊ番目のオフセットに格納された値を、変数ＩＤのｊ番目のオフセットに格納された値を鍵として暗号化した値を算出し、暗号化した値を、ＣＥＫ４のオフセットｊ番目に格納する（ステップＳ２０４）。
【０１６０】
そして、コンテンツ再生部２１２は、ｊの値を１増加させ、ステップＳ２０３に処理を戻す（ステップＳ２０５）。
【０１６１】

ｊの値が１６進数「Ｆ」を超える場合（ステップＳ２０３の判定で「Ｙｅｓ」）には、コンテンツ再生部２１２は、ステップＳ２０２～ステップＳ２０５で得たＣＥＫ４を用いて、対象の暗号化コンテンツ６１０の暗号を解除し、復号したコンテンツ６００を取得する（ステップＳ２０６）。

【０１６２】

そして、コンテンツ再生部２１２は、ステップＳ２０６で取得したコンテンツ６００を再生する（ステップＳ２０７）。

【０１６３】

なお、図１９にて用いるｊは、整数型変数である。

【０１６４】

ＥＮＣで表される関数は、暗号を施す関数である。ＥＮＣで表される関数は、２つの引数を受付けて、第２引数である１バイトの情報に対して、第１引数をキーとして可逆変換を行い、１バイトの情報を返却する関数である。

【０１６５】

次に、コンテンツ引継ぎ処理について、図２０～図２３を用いて説明する。

【０１６６】

この処理の前提として、コンテンツ暗号化装置２００の補助記憶装置２５４を取り出し、コンテンツ引継ぎ装置４００の外部記憶装置Ｉ／Ｆ４５６に接続されているものとする。

【０１６７】

図２０は、コンテンツ引継ぎ処理の全体のフローを示す図である。

【０１６８】

コンテンツ引継ぎ処理は、車両の乗り換えの際には車両販売店等が備えるコンテンツ引継ぎ装置４００に、コンテンツ暗号化装置２００の補助記憶装置２５４が接続され、コンテンツ引継ぎ装置４００において入力受付部４１２が処理開始の指示を受け付けることで処理が開始される。

【０１６９】

まず、コンテンツ引継ぎ部４１１は、記憶部４２０の部分ブロック鍵４２２を読み込む。

【０１７０】

そして、コンテンツ引き継ぎ部４１１は、その部分ブロック鍵４２２はディーラー用の部分ブロック鍵４２４であるか、そうでないか、を判定する（ステップＳ３０１）。

【０１７１】

具体的には、コンテンツ引継ぎ部４１１は、部分ブロック鍵４２２の上位８バイトが０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦ，０ｘＦＦと一致するかどうかを判定する。

【０１７２】

判定の結果、一致する場合には、ディーラー用の部分ブロック鍵４２４であると判定する。

【０１７３】

ステップＳ３０１における判定の結果、一致する場合（すなわち、ステップＳ３０１で「Ｙｅｓ」の場合）には、図２１に示すディーラー用権利情報更新処理を実施する（ステップＳ３０２）。

【０１７４】

そうでない場合（すなわち、ステップＳ３０１で「Ｎｏ」の場合）には、図２２に示す暗号化装置修理業者用権利情報更新処理を実施する（ステップＳ３０３）。

【０１７５】

図２１は、ディーラー用権利情報更新処理の処理フローを示す図である。

【０１７６】

ディーラー用権利情報更新処理は、図２０に示したコンテンツ引継ぎ処理のステップＳ

３０２において呼び出されることで処理を開始する。
【０１７７】
コンテンツ引継ぎ部４１１は、コンテンツ暗号化装置２００が搭載される車両識別子の入力を操作者に促し、入力受付部４１２は、操作者からの入力を受け付ける（ステップＳ３０２１）。
【０１７８】
具体的には、コンテンツ引継ぎ部４１１は、出力表示部４１３を介して出力装置４５５に対して、後述する識別子入力画面３３１を表示させる。そして、入力装置４５４を介して、入力受付部４１２が入力された値を車両識別子として受け付ける。
【０１７９】
次に、コンテンツ引継ぎ部４１１は、ステップＳ３０２１で受け付けた車両識別子を、１６バイトの変数である変数ＩＤの先頭から９バイト目から最下位バイト、すなわち右端のバイトまでの位置に、順に格納する（ステップＳ３０２２）。
【０１８０】
そして、コンテンツ引継ぎ部４１１は、ブロック鍵（ＢＬＫ）６５０の９桁目以降の各桁（各バイト）の値に応じて、変数ＩＤの同一のオフセット位置にある値をキーとして可逆の暗号を施すことで変数ｋを求め、得られた値ｋを権利情報ブロック（ＲＩＢ）６３０の行番号とみなして該当する行の所定のオフセット位置にある値を取り出す。所定の位置とは、ブロック鍵（ＢＬＫ）６５０と対応するオフセット位置のことである。
【０１８１】
そして、コンテンツ引き継ぎ部４１１は、取り出した値を、権利情報（ＲＩ）６２０の同一のオフセット位置に格納する（ステップＳ３０２３～ステップＳ３０２６）。
【０１８２】
これを、ｊの値を９からＦまで１ずつ増加させながら繰り返す（Ｓ３０２７）。
【０１８３】
より具体的には、まず、コンテンツ引継ぎ部４１１は、ループ制御用の整数ｊを１６進数「８」の値で初期化する（ステップＳ３０２３）。
【０１８４】
そして、コンテンツ引継ぎ部４１１は、ｊの値が１６進数「Ｆ」を超えるか否かを判定する（ステップＳ３０２４）。
【０１８５】
ｊの値が１６進数「Ｆ」を超えない場合（ステップＳ３０２４の判定で「Ｎｏ」）には、コンテンツ引継ぎ部４１１は、ブロック鍵（ＢＬＫ）６５０のｊ番目のオフセットに格納された値を対象として、変数ＩＤのｊ番目のオフセットの値を鍵として暗号化した値を、整数ｋに格納する（ステップＳ３０２５）。
【０１８６】
そして、コンテンツ引継ぎ部４１１は、権利情報ブロック（ＲＩＢ）のｋ行ｊ番目の位置に格納された値を取り出し、権利情報（ＲＩ）６２０のオフセットｊ番目に格納する（ステップＳ３０２６）。
【０１８７】
そして、コンテンツ引継ぎ部４１１は、ｊの値を１増加させ、ステップＳ３０２４に処理を戻す（ステップＳ３０２７）。
【０１８８】
ｊの値が１６進数「Ｆ」を超える場合（ステップＳ３０２４の判定で「Ｙｅｓ」）には、コンテンツ引継ぎ部４１１は、処理を終了させる。
【０１８９】
なお、図２１にて用いているｊは、整数型変数である。
【０１９０】
ＥＮＣで表される関数は、入力された値に暗号を施し出力する関数である。ＥＮＣで表される関数は、２つの引数を受付けて、第２引数である１バイトの情報に対して、第１引

数をキーとして可逆変換を行い、１バイトの情報を返却する関数である。

【０１９１】

図２２は、暗号化装置修理業者用権利情報更新処理の処理フローを示す図である。

【０１９２】

暗号化装置修理業者用権利情報更新処理は、図２０に示したコンテンツ引継ぎ処理のステップＳ３０３において呼び出されることで処理を開始する。

【０１９３】

コンテンツ引継ぎ部４１１は、補助記憶装置２５４が新たに搭載されるコンテンツ暗号化装置２００が備える暗号化装置識別子（ＮＩＤ）６４０の入力を操作者に促し、入力受付部４１２は、操作者からの入力を受け付ける（ステップＳ３０３１）。

【０１９４】

具体的には、コンテンツ引継ぎ部４１１は、出力表示部４１３を介して出力装置４５５に対して、後述する識別子入力画面３３１を表示させる。そして、入力装置４５４を介して、入力受付部４１２が入力された値を暗号化装置識別子として受け付ける。

【０１９５】

次に、コンテンツ引継ぎ部４１１は、ステップＳ３０３１で受け付けた暗号化装置識別子を、１６バイトの変数である変数ＩＤの先頭すなわち左端のバイトから８バイト目までの位置に、順に格納する（ステップＳ３０３２）。

【０１９６】

そして、コンテンツ引継ぎ部４１１は、ブロック鍵（ＢＬＫ）６５０の先頭桁から８桁目までの各桁（各バイト）の値に応じて、変数ＩＤの同一のオフセット位置にある値をキーとして可逆の暗号を施すことで変数ｋを求め、得られた値ｋを権利情報ブロック（ＲＩＢ）６３０の行番号とみなして該当する行の所定のオフセット位置にある値を取り出す。所定の位置とは、ブロック鍵（ＢＬＫ）６５０と対応するオフセット位置のことである。

【０１９７】

そして、コンテンツ引き継ぎ部４１１は、取り出した値を、権利情報（ＲＩ）６２０の同一のオフセット位置に格納する（ステップＳ３０３３～ステップＳ３０３６）。

【０１９８】

これを、ｊの値を０から７まで１ずつ増加させながら繰り返す（Ｓ３０３７）。

【０１９９】

より具体的には、まず、コンテンツ引継ぎ部４１１は、ループ制御用の整数ｊを１６進数「０」の値で初期化する（ステップＳ３０３３）。

【０２００】

そして、コンテンツ引継ぎ部４１１は、ｊの値が１６進数「７」を超えるか否かを判定する（ステップＳ３０３４）。

【０２０１】

ｊの値が１６進数「７」を超えない場合（ステップＳ３０３４の判定で「Ｎｏ」）には、コンテンツ引継ぎ部４１１は、ブロック鍵（ＢＬＫ）６５０のｊ番目のオフセットに格納された値を対象として、変数ＩＤのｊ番目のオフセットの値を鍵として暗号化した値を、整数ｋに格納する（ステップＳ３０３５）。

【０２０２】

そして、コンテンツ引継ぎ部４１１は、権利情報ブロック（ＲＩＢ）のｋ行ｊ番目の位置に格納された値を取り出し、権利情報（ＲＩ）６２０のオフセットｊ番目に格納する（ステップＳ３０３６）。

【０２０３】

そして、コンテンツ引継ぎ部４１１は、ｊの値を１増加させ、ステップＳ３０３４に処理を戻す（ステップＳ３０３７）。

【０２０４】

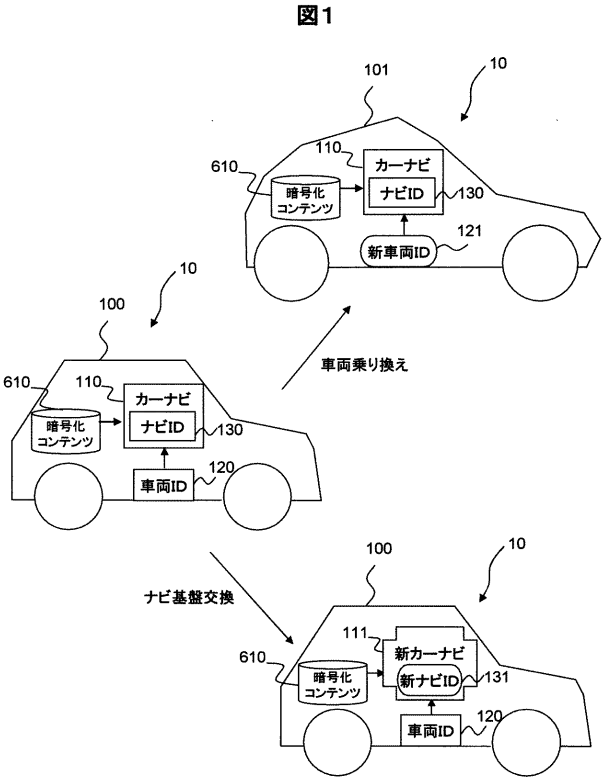
ｊの値が１６進数「７」を超える場合（ステップＳ３０３４の判定で「Ｙｅｓ」）には、コンテンツ引継ぎ部４１１は、処理を終了させる。

【０２０５】
なお、図２２にて用いているｊは、整数型変数である。
【０２０６】
ＥＮＣで表される関数は、入力された値に暗号を施し出力する関数である。ＥＮＣで表される関数は、２つの引数を受付けて、第２引数である１バイトの情報に対して、第１引数をキーとして可逆変換を行い、１バイトの情報を返却する関数である。
【０２０７】
ここで、図２３の識別子入力画面３３１について説明する。
【０２０８】
図２３に示す識別子入力画面３３１は、車両識別子の入力を受け付ける画面である。
【０２０９】
識別子入力画面３３１は、車両の識別子を入力する識別子入力領域３３２と、入力を確定するＯＫボタン３３３と、を有する。
【０２１０】
このうち、ＯＫボタン３３３は、車両識別子入力領域３３２に入力した車両識別子をコンテンツ引継ぎ部４１１に送信するよう指令を発生させるボタンである。
【０２１１】
なお、この車両識別子入力画面３３１は、車両識別子の入力に限らず、暗号化装置識別子の入力画面として用いることも可能である。
【０２１２】
暗号化装置識別子の入力画面として用いる場合には、例えば、識別子入力画面３３１は、暗号化装置の識別子を入力する識別子入力領域３３２と、入力を確定するＯＫボタン３３３と、を有する。
【０２１３】
このうち、ＯＫボタン３３３は、識別子入力領域３３２に入力した暗号化装置識別子をコンテンツ引継ぎ部４１１に送信するよう指令を発生させるボタンである。
【０２１４】
以上が、本実施例のコンテンツ引継ぎ処理のフローである。
【０２１５】
本実施形態によれば、コンテンツ暗号化装置２００を別の車両に移設する場合には、ディーラーがコンテンツ引継ぎ処理において新たな車両の識別子を入力することで権利情報（ＲＩ）６２０を書き換えることが可能である。
【０２１６】
書き換わった権利情報（ＲＩ）６２０を元にコンテンツ再生部２１２がＣＥＫ４を算出することで、暗号化コンテンツ６１０を復号することが可能となり、暗号を解除することができるようになる。
【０２１７】
また、コンテンツ暗号化装置２００の故障などの場合に、別の制御基盤装置あるいは筐体に補助記憶装置２５４を移設する場合には、暗号化装置修理業者がコンテンツ引継ぎ処理において新たな暗号化装置の識別子を入力することで権利情報（ＲＩ）６２０を書き換えることが可能である。
【０２１８】
書き換わった権利情報（ＲＩ）６２０を元にコンテンツ再生部２１２がＣＥＫ４を算出することで、暗号化コンテンツ６１０を復号することが可能となり、暗号を解除することができるようになる。
【０２１９】
なお、例えば、コンテンツ暗号化装置２００の故障などの場合に、別の制御基盤装置あるいは筐体に補助記憶装置２５４を移設する場合に補助記憶装置２５４を複製し、異なる車両の所有者に対して複製した補助記憶装置を販売して異なる車両に移設しようとしても、暗号化装置修理業者が保有するコンテンツ引継ぎ装置４００では、新たな車両の識別子

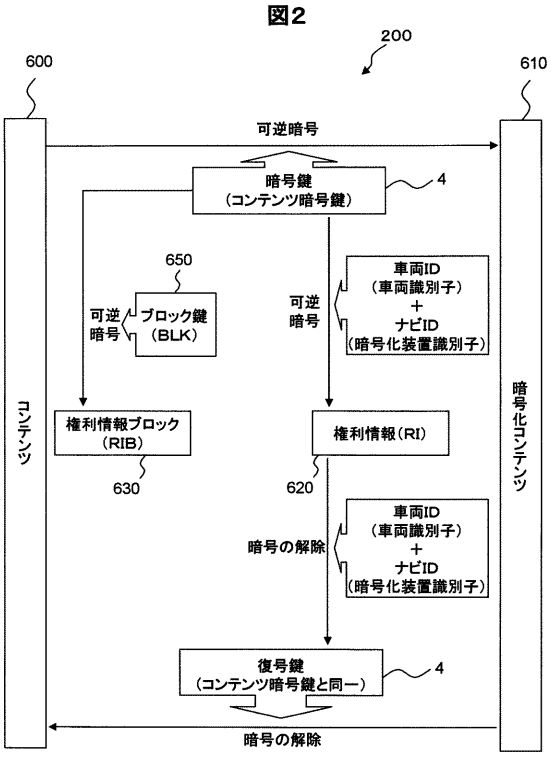
を用いて権利情報（ＲＩ）６２０を適切に書き換えることができない。
【０２２０】
そのため、コンテンツ再生部２１２は適切なＣＥＫ４を算出できずに暗号化コンテンツ６１０の暗号を解除できないため、複製したコンテンツを再生できない。
【０２２１】
以上、本発明の実施の形態について、その実施の形態に基づき具体的に説明したが、これに限定されるものではなく、その要旨を逸脱しない範囲で種々の変更が可能である。
【０２２２】
例えば、上記実施例では車両制御装置の車両識別子を用いているが、これに限らず、例えば車両に設置される他の機器に固有の番号等であってもよい。
【０２２３】
なお、上記のコンテンツ引継ぎシステム１０は、システムとして取引対象とするだけでなく、各機器単位、またはその機器の動作を実現するプログラム部品単位で取引対象とすることも可能である。
【０２２４】
以上が、本発明の実施形態である。
【図面の簡単な説明】
【０２２５】
【図１】本実施形態のコンテンツ引継ぎ技術の概略の構成図である。
【図２】本実施形態のコンテンツの暗号化／暗号の解除の際の情報の流れを示す図である。
【図３】本実施形態の車両乗り換えの際の、コンテンツ暗号化装置を流用した場合の情報の流れを示す図である。
【図４】本実施形態の車両乗り換えの際の、暗号化コンテンツの暗号解除の失敗を回避する処理における情報の流れを示す図である。
【図５】本実施形態のコンテンツ暗号化装置の修理の際の、暗号化コンテンツの暗号解除の失敗を回避する処理における情報の流れを示す図である。
【図６】本実施形態の暗号解除を実現する仕組みを示す図である。
【図７】本実施形態のコンテンツ引継ぎシステムの概略の構成図である。
【図８】本実施形態のコンテンツ引継ぎシステムの構成図である。
【図９】本実施形態のコンテンツ暗号化装置の記憶部の構成図である。
【図１０】本実施形態における権利情報のデータ構造を示す図である。
【図１１】本実施形態における権利情報ブロックのデータ構造を示す図である。
【図１２】本実施形態におけるブロック鍵のデータ構造を示す図である。
【図１３】本実施形態における部分ブロック鍵のデータ構造を示す図である。
【図１４】本実施形態におけるコンテンツ暗号化装置等のハードウェア構造を示す図である。
【図１５】本実施形態におけるコンテンツ取り込み処理のフローチャートである。
【図１６】本実施形態における権利情報ブロック作成処理のフローチャートである。
【図１７】本実施形態における権利情報ブロック作成処理を例示する図である。
【図１８】本実施形態における権利情報作成処理のフローチャートである。
【図１９】本実施形態におけるコンテンツ再生処理のフローチャートである。
【図２０】本実施形態におけるコンテンツ引継ぎ処理のフローチャートである。
【図２１】本実施形態におけるディーラー用権利情報更新処理のフローチャートである。
【図２２】本実施形態における暗号化装置修理業者用権利情報更新処理のフローチャートである。
【図２３】本実施形態の車両識別子の入力を受付ける画面を例示する図である。
【符号の説明】
【０２２６】
１０：コンテンツ引継ぎシステム、１００：車両、２００：コンテンツ暗号化装置、２１

０：制御部、２２０：通信部、２３０：記憶部、３００：車両制御装置、３１０：車両識別子記憶領域、３２０：通信部、４００：コンテンツ引継ぎ装置、４１０：制御部、４２０：記憶部、４３０：外部記憶装置接続部、５００：車体ネットワーク、６２０：権利情報（ＲＩ）、６３０：権利情報ブロック（ＲＩＢ）、６４０：暗号化装置識別子（ＮＩＤ）、６５０：ブロック鍵（ＢＬＫ）

【図１】

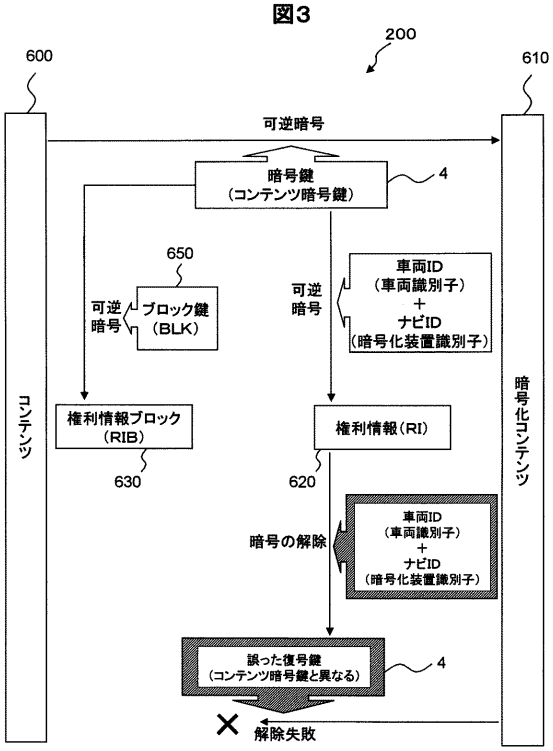


【図２】



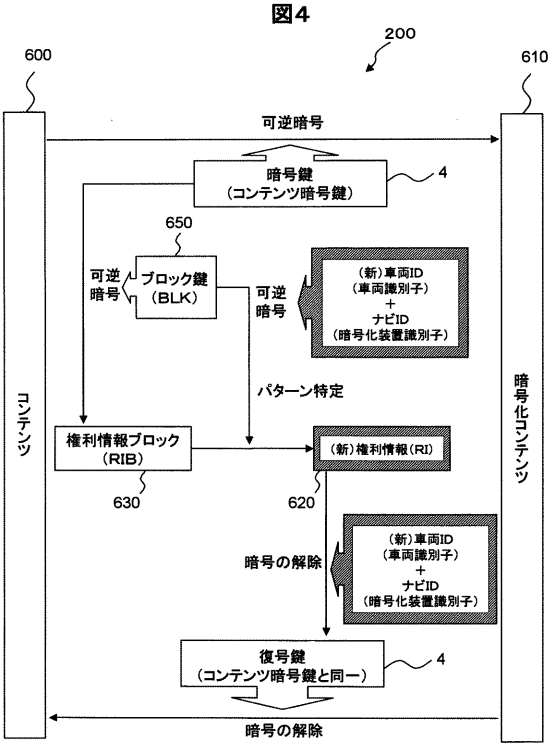
【図３】

図3



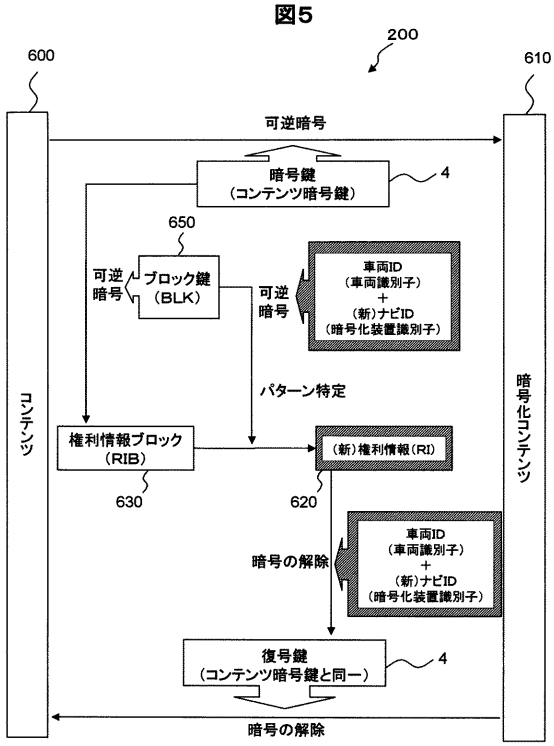
【図４】

図4



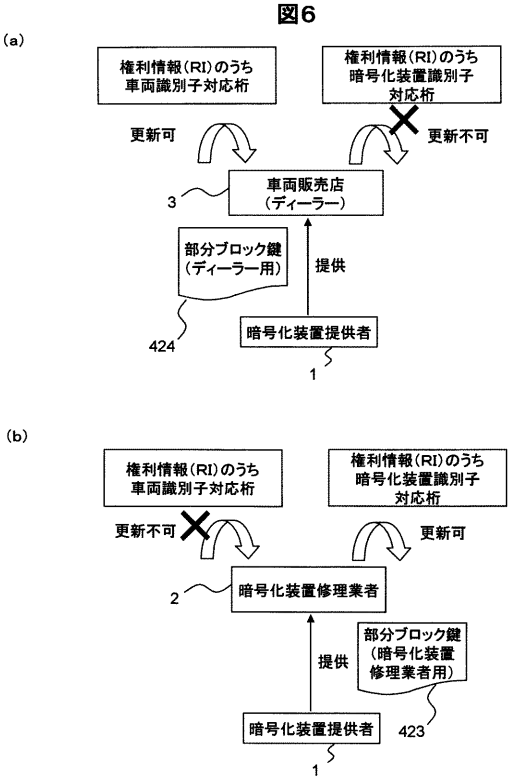
【図５】

図5



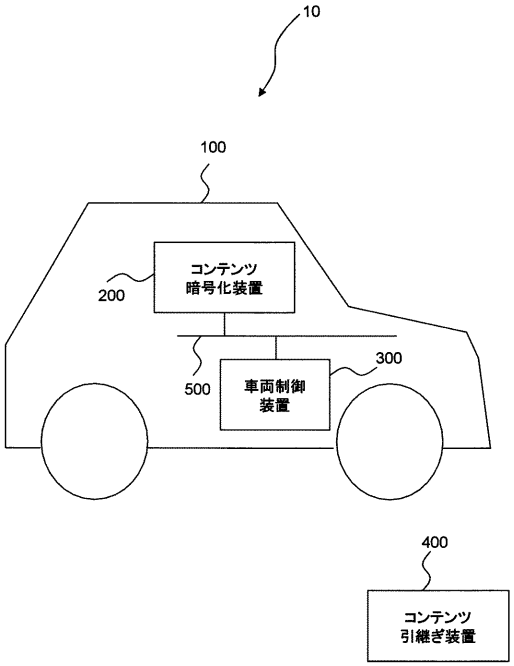
【図６】

図6



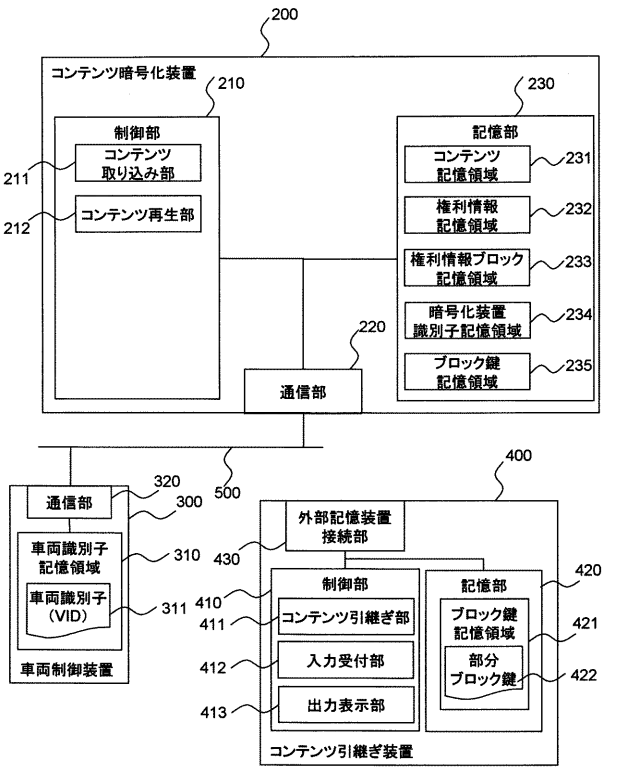
【図７】

図7



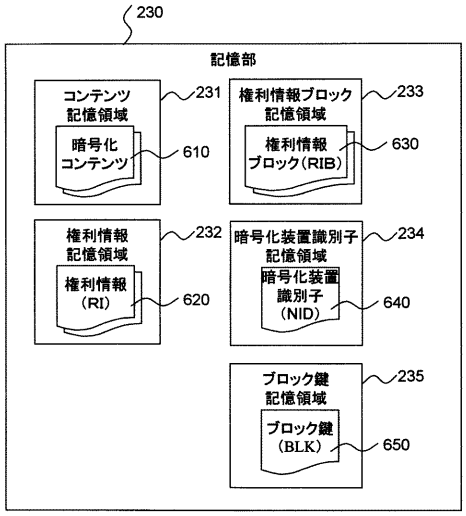
【図８】

図8



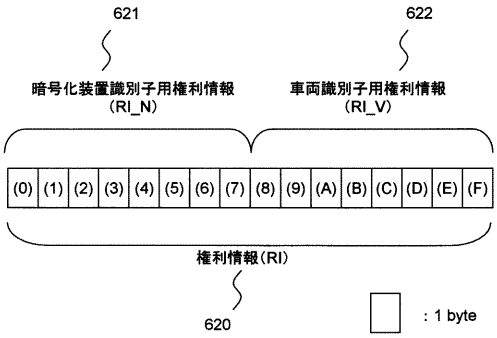
【図９】

図9



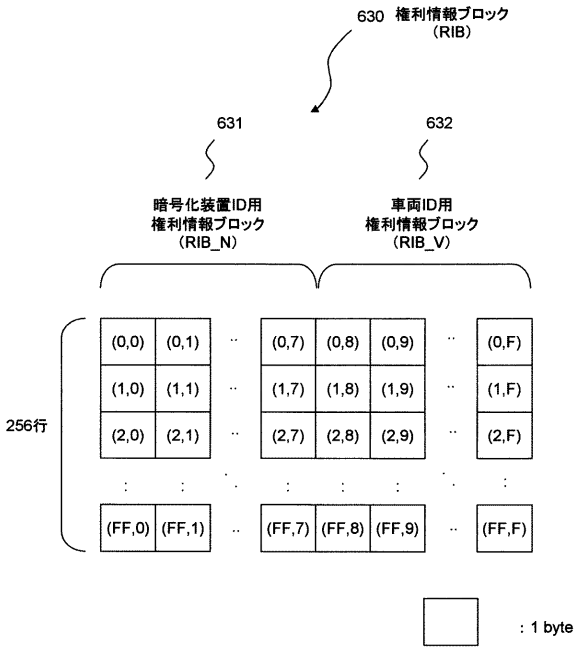
【図１０】

図10



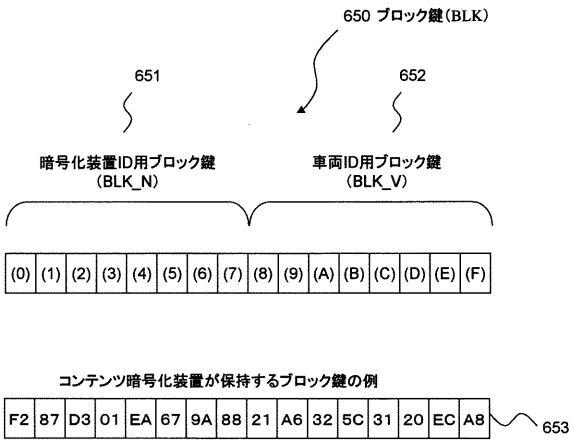
【図１１】

図11



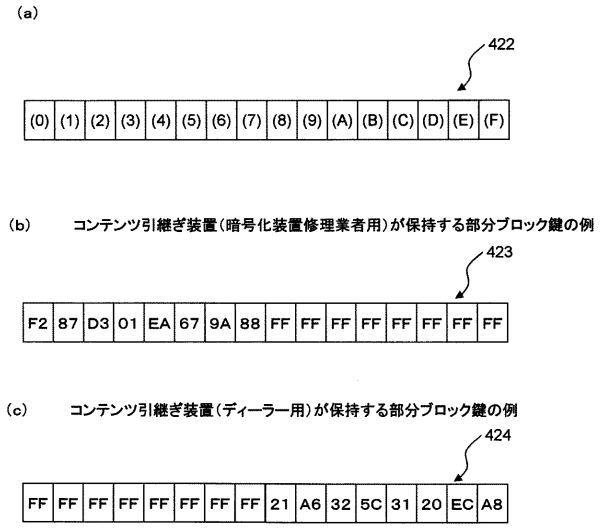
【図１２】

図12



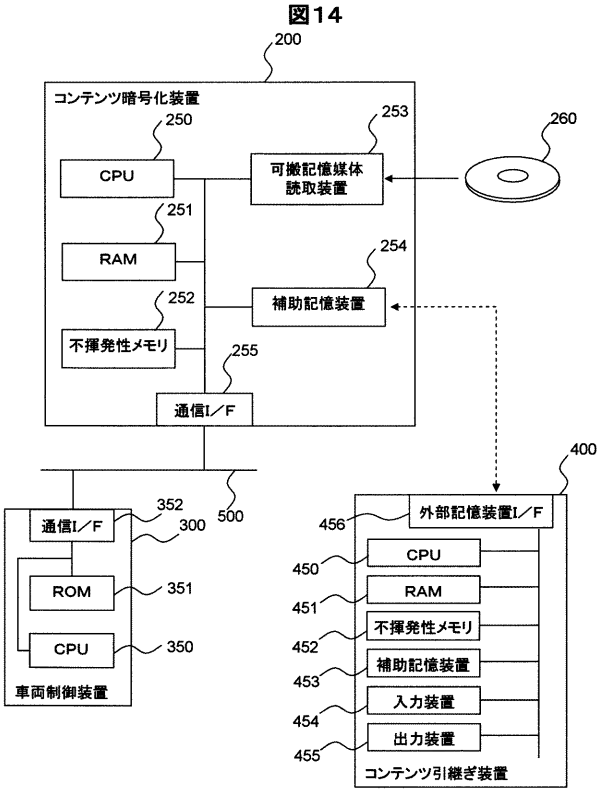
【図１３】

図13



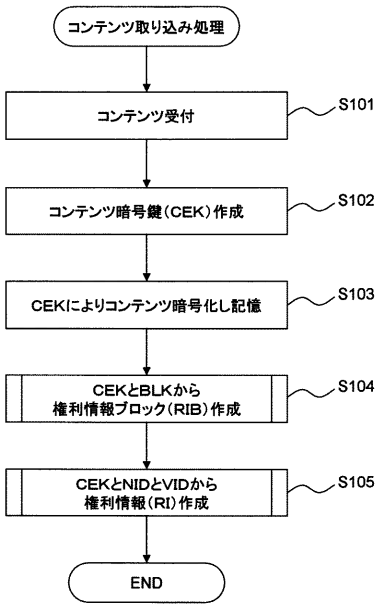
【図１４】

図14



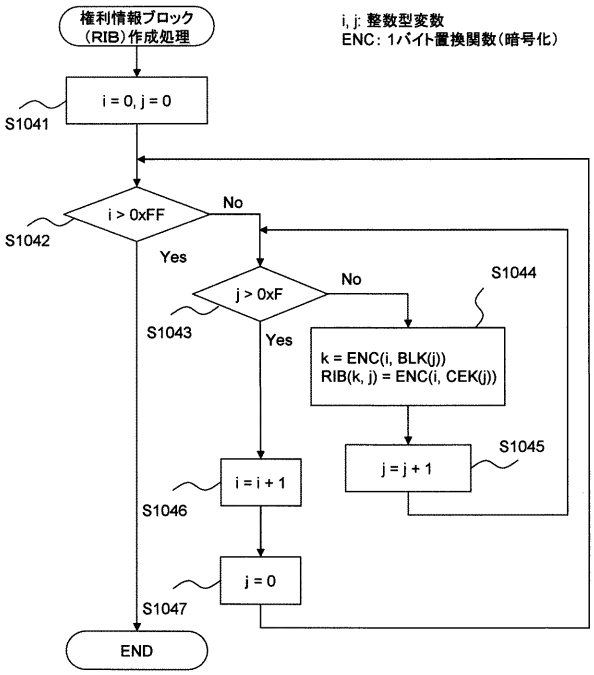
【図１５】

図15



【図１６】

図16



【図１７】

図17

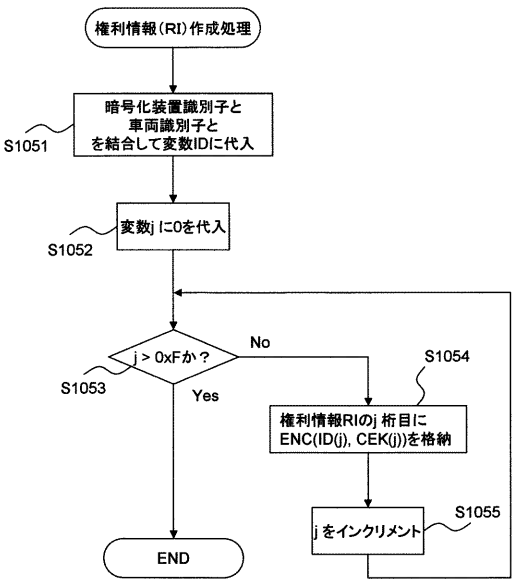
CEK: 0x0123456789ABCDEF0123456789ABCDEF
BLK: 0xF287D301EA679A8821A6325C3120ECA8

(1) (i, j) = (0x00, 0x0)
k = ENC(0x00, 0xF2) = 0x04 RIB(0x04, 0x0) = ENC(0x00, 0x01) = 0xAB
(2) (i, j) = (0x00, 0x1)
k = ENC(0x00, 0x87) = 0xEF RIB(0xEF, 0x1) = ENC(0x00, 0x23) = 0x2C
(3) (i, j) = (0x00, 0x2)
k = ENC(0x00, 0xD3) = 0x44 RIB(0x44, 0x2) = ENC(0x00, 0x45) = 0x8B
i BLK k j i CEK

	0x0	0x1	0x2	・・	0xF
0x00	-	-	-	・・	-
0x04	AB	-	-	・・	-
0x44	-	-	8B	・・	-
0xEF	-	2C	-	・・	-

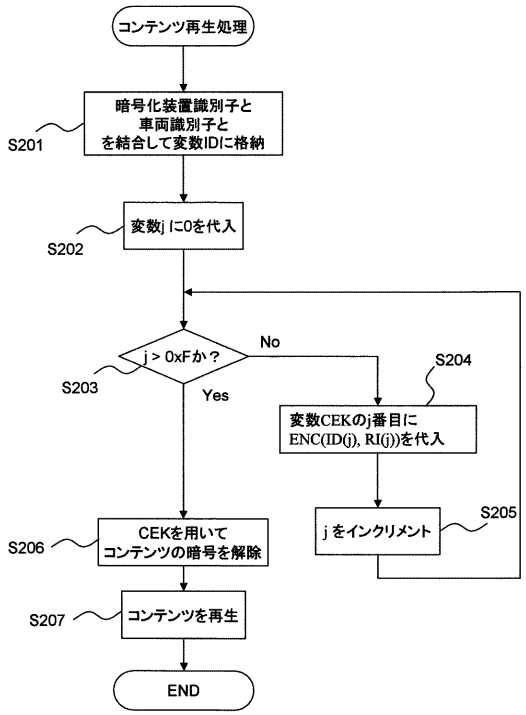
【図１８】

図18



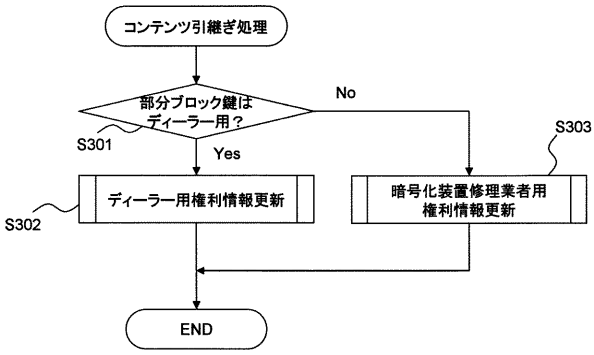
【図１９】

図19



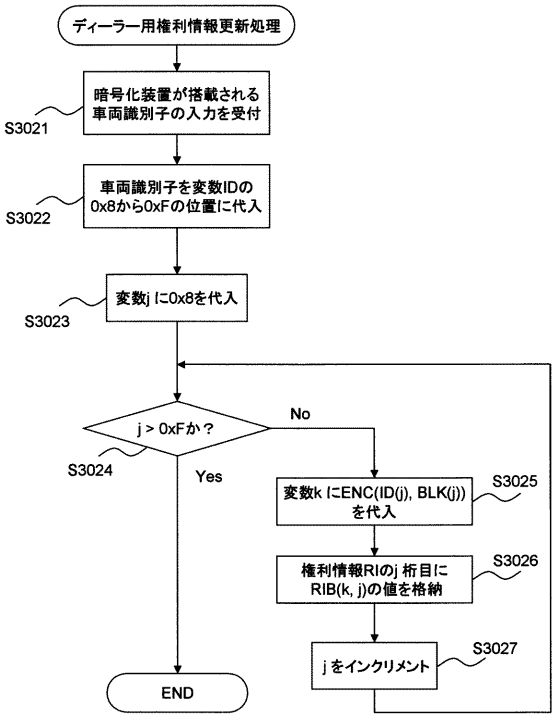
【図２０】

図20



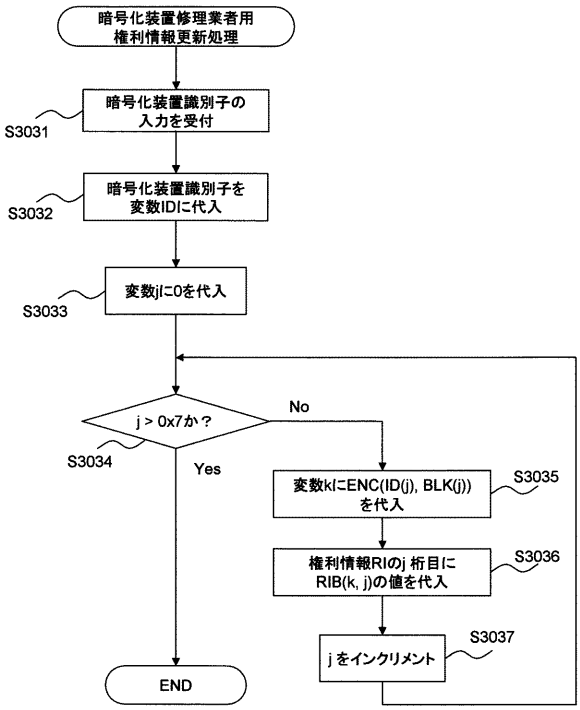
【図２１】

図21



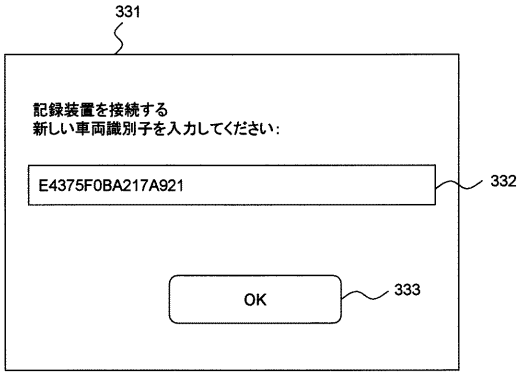
【図２２】

図22



【図２３】

図23


331
記録装置を接続する
新しい車両識別子を入力してください:
E4375F0BA217A921
332
OK
333

フロントページの続き

(72)発明者　相薗　岳生
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考) 5J104 AA16　AA32　EA04　EA15　EA16　JA03　NA02　NA37