

(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2005-190040
(P2005-190040A)

(43) 公開日 平成17年7月14日(2005.7.14)

(51) Int. Cl.⁷
G06K 17/00

F I
G06K 17/00

テーマコード(参考)
5B058

審査請求 未請求 請求項の数 5 O L (全 15 頁)

(21) 出願番号 特願2003-428651 (P2003-428651)
(22) 出願日 平成15年12月25日(2003.12.25)

(71) 出願人 000005326
本田技研工業株式会社
東京都港区南青山二丁目1番1号
(74) 代理人 100064908
弁理士 志賀 正武
(74) 代理人 100108578
弁理士 高橋 詔男
(74) 代理人 100101465
弁理士 青山 正和
(74) 代理人 100094400
弁理士 鈴木 三義
(74) 代理人 100107836
弁理士 西 和哉
(74) 代理人 100108453
弁理士 村山 靖彦

最終頁に続く

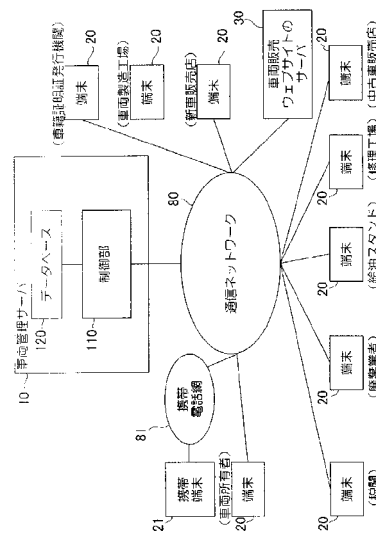
(54) 【発明の名称】 商品管理システム

(57) 【要約】

【課題】 販売済みの商品が正当な所有者以外の者によって不正に使用、あるいは、取引されることを防止する。

【解決手段】 商品に関わるキー情報と当該商品の所有者に関わる所有者情報とを関連付けて記憶するデータベースと、商品に取り付けられ、当該商品に関わるキー情報を記憶したICタグから前記キー情報を読み取り、読み取ったキー情報に関連付けられた所有者情報を前記データベースから読み出す所有者認証手段と、を備える商品管理システムにおいて、前記キー情報を記憶する記憶媒体を備えたカードを発行するカード発行手段と、前記カードから読み取ったキー情報と前記ICタグから読み取ったキー情報と前記データベースから読み出したキー情報とを照合する照合手段とを備え、所有者を認証する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

商品に関わるキー情報と当該商品の所有者に関わる所有者情報とを関連付けて記憶するデータベースと、

商品に取り付けられ、当該商品に関わるキー情報を記憶した IC タグから前記キー情報を読み取り、読み取ったキー情報に関連付けられた所有者情報を前記データベースから読み出す所有者認証手段と、

を備える商品管理システムにおいて、

前記キー情報を記憶する記憶媒体を備えたカードを発行するカード発行手段と、

カードから読み取ったキー情報と前記 IC タグから読み取ったキー情報と前記データベースから読み出したキー情報の 3 者のキー情報の照合を行い、前記商品の正規所有者を認証する認証手段と

を備えることを特徴とする商品管理システム。

【請求項 2】

前記 IC タグの前記キー情報は、無線通信によりやりとりされることを特徴とする請求項 1 に記載の商品管理システム。

【請求項 3】

前記カードの前記キー情報は、無線通信によりやりとりされることを特徴とする請求項 1 に記載の商品管理システム。

【請求項 4】

前記カードおよび前記 IC タグは前記所有者情報を記憶し、

前記所有者認証手段は、前記カードから読み取った前記キー情報および前記所有者情報と、前記 IC タグから読み取った前記キー情報および前記所有者情報とが一致したときに、前記データベースから前記キー情報を読み出し可能とされる、

ことを特徴とする請求項 1 に記載の商品管理システム。

【請求項 5】

前記カードはカードを識別するカード ID を記憶し、

前記データベースは前記カード ID を記憶し、

前記所有者認証手段は、前記カードから読み出した前記カード ID と前記データベースから読み出した前記カード ID とが一致し且つ前記 IC タグから読み出した前記所有者情報と前記データベースから読み出した前記所有者情報とが一致したことにより、正規所有者を認証する、

ことを特徴とする請求項 4 に記載の商品管理システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、商品管理システムに関する。

【背景技術】

【0002】

従来技術として、特許文献 1 には、試着室内に持ち込まれる商品に取り付けられた商品タグ内に格納されている商品固有の識別情報を検知し、検知した識別情報に基づいた商品に関する情報を試着室に設置された表示装置に表示することにより、試着室に持ち込まれた商品の盗難を防止することが記載されている。

また、特許文献 2 には、商品が未清算のまま店外に持ち出される事態を検知する盗難防止システムと、この盗難防止システムに用いられ、製造コストが安価であり、目立ちにくく、商品の美観を損なうことのない盗難防止タグについて記載されている。

【特許文献 1】特開平 11 - 66445 号公報

【特許文献 2】特開 2003 - 36485 号公報

10

20

30

40

50

【発明の開示】

【発明が解決しようとする課題】

【0003】

特許文献1及び2の技術によれば、販売前の商品が盗難されることを防止することができる。しかし、商品の販売後に、当該商品が正当な所有者以外の者によって不正に使用されたり、取引されたりすることを防止することはできない。

【0004】

この発明は、このような事情を考慮してなされたもので、その目的は、販売済みの商品の所有者が正当な所有者であるか否かを検出することにより、商品が正当な所有者以外の者に不正に使用、あるいは、取引されることを防止することのできる商品管理システムを提供することにある。

10

【課題を解決するための手段】

【0005】

この発明は、上記の課題を解決すべくなされたもので、商品に関わるキー情報と当該商品の所有者に関わる所有者情報とを関連付けて記憶するデータベース(120)と、商品に取り付けられ、当該商品に関わるキー情報を記憶したICタグから前記キー情報を読み取り、読み取ったキー情報に関連付けられた所有者情報を前記データベース(120)から読み出す所有者認証手段と、を備える商品管理システムにおいて、前記キー情報を記憶する記憶媒体(72)を備えたカード(50)を発行するカード発行手段と、前記カード(50)から読み取ったキー情報と前記ICタグから読み取ったキー情報と前記データベース(120)から読み出したキー情報とを照合する照合手段とを、さらに備えることを特徴とする商品管理システムである。

20

このような構成により、商品に関わるキー情報と当該商品の所有者に関わる所有者情報とを関連付けてデータベースに記憶しておき、商品に取り付けられたICタグ内のキー情報を基に、当該商品の所有者情報を読み出す。また、商品に取り付けられるICタグから読み出したキー情報と、当該商品の所有者に対して発行したカードから読み出したキー情報と、データベース内から読み出した当該商品のキー情報とを照合することにより、商品が正当な所有者により使用あるいは取引されているものであるか否かを確認する。

【0006】

また、本発明は、上述する商品管理システムであって、前記ICタグの前記キー情報は、無線通信によりやりとりされることを特徴とする。

30

このような構成では、無線を用いて商品の外部または内部に取り付けられたICタグからキー情報を読み取る。ここで、無線通信とは、電磁波や超音波などを用いた通信である。電磁波とは、いわゆる電波、赤外線、光(可視光)などであり、適宜適切な周波数帯域の電磁波を用いることとする。また、ICタグとしては、例えばRFID(Radio Frequency Identification)タグなどを用いる。

また、本発明は、上述する商品管理システムであって、前記カードの前記キー情報は、無線通信によりやりとりされることを特徴とする。

このような構成では、他のICタグ(例えば、商品に取り付けられたICタグなど)から情報を読み取る装置を用いて、カードが備えるICタグからキー情報を読み取ることができる。つまり、ICタグから情報を読み取る装置を共通化できる。ここで、無線通信とは、電磁波や超音波などを用いた通信である。電磁波とは、いわゆる電波、赤外線、光(可視光)などであり、適宜適切な周波数帯域の電磁波を用いることとする。また、ICタグとしては、例えばRFIDタグなどを用いる。

40

また、本発明は、上述する商品管理システムであって、前記カードおよび前記ICタグは前記所有者情報を記憶し、前記所有者認証手段は、前記カードから読み取った前記キー情報および前記所有者情報と、前記ICタグから読み取った前記キー情報および前記所有者情報とが一致したときに、前記データベースから前記キー情報を読み出し可能とされることを特徴とする。

このような構成では、ICカードから読み取った情報とカードから読み取った情報とが

50

一致しない場合には、データベースにアクセスする必要がない。

また、本発明は、上述する商品管理システムであって、前記カードはカードを識別するカードIDを記憶し、前記データベースは前記カードIDを記憶し、前記所有者認証手段は、前記カードから読み出した前記カードIDと前記データベースから読み出した前記カードIDとが一致し且つ前記ICカードから読み出した前記所有者情報と前記データベースから読み出した前記所有者情報とが一致したことにより、正規所有者を認証することを特徴とする。

このような構成では、例えば不正なカードが偽造された場合には、即ちカードIDの異なるカードに前記キー情報および前記所有者情報を書き込んだ場合には、その(偽造等の)カードを用いて正規所有者を認証してしまうことはない。つまり、偽造カードの使用を防止できる。

【発明の効果】

【0007】

本発明によれば、商品に取り付けられたICタグから読み出したキー情報と、カードから読み出したキー情報と、データベース内から読み出したキー情報とを照合することにより、簡易に商品が正当な所有者により使用あるいは取引されているものであるか否かを確認し、また、本来の所有者を確認するための情報を取得することができる。これにより、商品が盗難された場合でも、被害にあった商品を早期に発見するとともに、真の所有者の割り出しに役立てることができ、さらには、盗難を防止あるいは抑制することができる。また、消費者は、不正に取引された商品ではないことを確認し、安心して中古の商品を購入することができる。

また、商品に取り付けるICタグとしてRFIDタグを用いることにより、商品からの情報の読み出しが容易となる。

【発明を実施するための最良の形態】

【0008】

以下、図面を参照しこの発明の一実施形態について説明する。なお、ここでは、商品として車両を想定する。

図1は、同実施形態による商品管理システムの構成を示すブロック図である。図1において、符号10は車両管理サーバであり、この車両管理サーバ10は内部に制御部110(所有者認証手段、カード発行手段、照合手段)とデータベース120とを備えている。また、20は、車両製造工場や、車籍証明証発行機関、新車あるいは中古車販売店、車両の修理工場、給油スタンド、車両の廃棄業者、税関、車両所有者宅などにそれぞれ設けられた端末である。なお、端末20には必要に応じてタグリーダ/ライタが接続されており、車両に取り付けられたICタグや車籍証明証(カード)50に埋め込まれたICタグ(記憶媒体)内のメモリの情報を読み書きできるようになっている。21は、例えば車両所有者が保有する携帯端末である。また、30は、通信ネットワーク80を介していわゆるウェブインタフェースを用いて車両を販売するために設けられている車両販売ウェブサイトのサーバである。

【0009】

通信ネットワーク80はインターネットやVPN(Virtual Private Network)、LAN(Local Area Network)などのネットワークである。車両管理サーバ10と、端末20及び車両販売ウェブサイトのサーバ30とは、この通信ネットワーク80を介して、また、携帯端末21とは、携帯電話網81及び通信ネットワーク80を介して相互に通信することが可能となっている。

【0010】

車両管理サーバ10内において、データベース120は、各車両に関して、その車両の識別情報と、カード(車籍証明証50)の識別情報と、所有者に関する情報を示す所有者情報と、車両に関する情報を示す車両情報と、車両の履歴を示す車両履歴情報とを関連させて記憶している。また、制御部110は、後述するように、端末20や携帯端末21や車両販売ウェブサイトのサーバ30などとデータのやり取りを行いながら、データベース

10

20

30

40

50

120に格納されているデータを参照したり、データベース120にデータを書き込んだりする。さらに、車籍証明証50、車両に取り付けられたICタグ、及び、データベース120から読み出した車両に関わるキー情報を照合し、不正に使用あるいは取引される車両ではないかを確認する。このキー情報は、車両の識別情報、カードの識別情報、所有者情報、車両履歴情報のいずれかまたは任意の組み合わせでありうる。

【0011】

なお、車両管理サーバ10や端末20や車両販売ウェブサイトのサーバ30は、コンピュータを用いて実現する。また、携帯端末21としては、携帯型電話端末（携帯電話端末あるいはPHS（登録商標、パーソナル・ハンディフォン・システム）端末）やPDA（パーソナル・デジタル・アシスタント）などを用いる。これらの各装置は、内部にCPU（中央処理装置）を備えている。そして、これら各装置が行う処理の過程は、コンピュータプログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをCPUが読み出して実行することによって、上記処理が行われる。ここでコンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、CD-ROM、DVD-ROM、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータに設けられたCPUが当該プログラムを実行するようにしても良い。

10

【0012】

車両に取り付けられるICタグは、外部とのインターフェースと、メモリとを備え、メモリ内の情報の読み書きや保持を行うことができる。ICタグには、当該ICタグを識別するためのIDが予め記憶される。本実施の形態では、ICタグとしてRFID（Radio Frequency Identification）タグを用いる。RFIDタグは、無線周波数を通信に利用するためのアンテナと、半導体メモリとが内蔵されており、この半導体メモリには書き替え禁止領域と書き替え可能領域との両方が存在している。そして、この書き替え禁止領域には、IDが予め書き込まれており車両ID（車両の識別情報）として使用される。また、書き替え可能領域には、所有者情報、車両情報、車両履歴情報などが書き込まれる。

20

【0013】

図2は、車両が自動二輪車である場合にRFIDタグを取り付ける場所の概略を示す概略図である。図2において、符号90は人が乗るためのシートであり、このシートは樹脂部材によってできている。そして、前記のRFIDタグを、このシートの内部に設けることとする。

30

【0014】

図3は、シートの長手方向の断面図であり、この図において符号71a、71b、71c、71d、71e、71fはそれぞれRFIDタグを固着する位置の例を示している。これら71a～71fのいずれにRFIDタグを取り付けても良いが、特に、71aや71fの位置に取り付けた場合には、シート表面からRFIDタグまでの距離が短いため、より近くまでRFIDリーダ/ライタを近付けることができる。なお、図3のAA部でのシートの断面図が図4である。

なお、図3に示すように、シートを構成する樹脂部材は乗る人のための緩衝の役割を果たすために上下方向にある程度の厚みを持っている。従って、71b、71c、71d、71eの位置にRFIDタグを取り付けた場合には、シート表面までの距離が比較的長くなる。一方、71a又は71fのように、シート内の前方又は後方の部分にRFIDタグを取り付けた場合には、それぞれ前方又は後方のシート表面までの距離が比較的短くなる。従って、RFIDタグの読み書き信号（電磁波）の到達距離が比較的短い場合には、71aあるいは71fといったシート表面までの距離が相対的に短い位置にRFIDタグを設けることによって、RFIDタグにより近い場所まで読取装置を持っていくことが可能となり、読み書きがし易くなる。

40

【0015】

なお、図2～図4では自動二輪車（原動機付き自転車も同様）の場合についてRFIDタグの取り付け位置を示したが、自動二輪車以外にも、自転車やパーソナルウォーターク

50

ラフト（PWC）や4輪バギー車などのくら乗り型の乗り物においてシート内にRFIDタグを設けるようにすることができる。シートは電磁波を通す樹脂部材でできているため、このようにシート内部にRFIDタグを取り付けることは、電磁波の信号を用いてRFIDタグの記憶情報を読んだり書いたりするために好都合である。また、くら乗り型の乗り物では、通常、シートの上方を覆う金属製の屋根などがいないため、例えば、給油スタンドや修理工場や道路上などにおいて車両の停止位置などの上方にRFIDリーダー/ライター（タグリーダー/ライター）を設置することもでき、好都合である。また、RFIDタグは、車両の製造から廃棄に至るまで車両に固着されるようにするが、RFIDタグをシート内に設けることによってRFIDタグが容易にはずれてしまうことがないという利点もある。

10

なお、金属製の屋根を有する乗用車やバスやトラックなど車両等の場合には、シート内にRFIDタグを取り付けておいて、ハンディ型の読み書き装置を車両内部に持ち込むことによって、そのRFIDタグの情報を読み書きする。あるいは、乗用車のフロントウィンドウ付近あるいはリアウィンドウ付近にRFIDタグを取り付ける。例えば、ダッシュボード部分にRFIDタグを取り付けて、車外上方などから、RFIDタグの読み書きするようにしても良い。また、ダッシュボード部分を構成する樹脂部材の中にRFIDタグを取り付けるようにしても良い。

【0016】

次に、本システムで用いるカードとしての車籍証明証50について説明する。図5は、車籍証明証50の券面の一例を示す概略図である。この図において、車籍証明証50は、車両毎に1枚発行される証明証であり、図示するように、その表面に、対象の車両の車種や年式（「モデル 2003」と表示）、製造番号、製造会社名などの車両情報が記載されており、また、車両の写真が印刷又は貼付されている。また、符号72は、車籍証明証50内に埋め込まれている記憶媒体としてのICタグであり、ここではRFIDタグを用いることとする。このRFIDタグ72は、車両に取り付けられるRFIDタグと同様に構成されるが、RFIDタグ72の書き替え禁止領域に予め書き込まれているIDは、カードID（カードの識別情報）として使用される。また、書き替え禁止領域には、車籍証明証50の発行時に車両IDがさらに書き込まれる。書き替え可能領域には、車両に取り付けられるRFIDタグと同様、所有者情報、車両情報、及び、車両履歴情報が書き込まれる。

20

30

なお、上記のカードIDは、カードの製造時にカード個体毎に割り振られて予め書き込まれているIDであり、このカードIDによりカード個体を完全にユニークに識別可能である。

なお、この車籍証明証50は、車両を製造する製造業者や車籍を管理する公的機関等によって発行されるものとする。また、この車籍証明証50のサイズは、例えば、縦5.3センチメートル、横8.5センチメートルのクレジットカードサイズ程度で、その材質はプラスチック等とする。

【0017】

次に、車両に取り付けられたRFIDタグが保持する情報について説明する。図6は、車両に取り付けられたRFIDタグ内のメモリに記憶されているデータの構成を示す概略図である。図示するように、メモリ内には書き替え禁止領域と書き替え可能領域とが存在している。書き替え禁止領域は、例えば、ROM（リードオンリーメモリ）を用いることによって書き換え禁止とする。また、あるいは、RFIDタグが備える制御機能により、書き換え禁止領域を書き替えないように制御する。

40

【0018】

書き替え禁止領域には、タグ種別コードと車両IDとが記憶されており、さらに予備領域が設けられている。タグ種別コードは、当該RFIDタグが車両に取り付けられたRFIDタグであるか車籍証明証50に設けられたRFIDタグ72であるかを判別するためのコード情報であり、車両に取り付けられたRFIDタグであることを示すコードが設定される。

50

また、書き替え可能領域には、所有者データ、車両データ、及び、車両履歴データが記憶されており、さらに予備領域が設けられている。これら所有者データ、車両データ、及び、車両履歴データは、後述するように、車籍証明証50のRFIDタグ72及びデータベース120にも同様の情報が保持される。すなわち、本システムでは、通信ネットワーク80を介して車両管理サーバ10と端末20とが通信可能となっているため、データベース120に記憶され管理されるデータ（所有者データ、車両データ、及び、車両履歴データ）と車両に取り付けられたRFIDタグに記憶されるデータ（所有者データ、車両データ、及び、車両履歴データ）とは、必要に応じて適宜、同期的に更新される。さらに、このとき同時に、車籍証明証50のRFIDタグ72内のデータ（所有者データ、車両データ、及び、車両履歴データ）も更新される。また、RFIDタグの記憶容量には限りがあるため、データベース120にはこれらの各データのフルセットを持たせておき、RFIDタグにはこれらの各データのサブセットのみを持たせるようにしても良い。

なお、車籍証明証50のRFIDタグ72は、上述する車両に取り付けられたRFIDタグと同様のデータ構成によりデータを記憶しているが、書き替え禁止領域には、車籍証明証50に設けられたRFIDタグ72であることを示すコードが設定されたタグ種別コード及びカードIDと、車両IDとが記憶される。

【0019】

次に、図7及び図8を参照しながら、データベース120が保持する各データについて説明する。但し、図7及び図8に示すデータは、車両毎に、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72にもその一部又は全部が保持されている。

図7は、データベース120に含まれる所有者データのデータ構造を示す概略図である。図示するように、所有者データには、車両IDと対応付けられた所有者情報が含まれている。所有者情報とは、所有者の氏名、生年月日、住所等の情報である。

【0020】

図8は、データベース120に含まれる車両履歴データのデータ構造を示す概略図である。図示する例のように、車両履歴データは、車両毎（車両ID毎）にその車両履歴情報を保持しており、日付と履歴概略と詳細の各データ項目を少なくとも含んでいる。履歴概略の項目の値は、例えば、「新車製造」、「所有者登録」、「所有者変更」、「給油」、「修理」、「登録抹消」、「廃棄物管理票発行」などである。これらの車両履歴情報は、それぞれの事象が発生する都度、端末20において情報が発生する。その情報は、車両に取り付けられたRFIDタグや車籍証明証50のRFIDタグ72に必要に応じて書き込まれるとともに、端末20から車両管理サーバ10に伝達される。車両管理サーバ10の制御部110は、その伝達された情報に基づいてデータベース120への書き込みを行う。

なお、履歴概略が「新車製造」の場合には、製造会社名や工場名が詳細データとして書き込まれている。履歴概略が「所有者登録」の場合には、所有者名や所有者住所などが詳細データとして書き込まれている。履歴概略が「給油」の場合には、給油所を特定する情報や給油量や給油時点の走行距離計情報などが詳細データとして書き込まれている。履歴概略が「修理」の場合には、修理工場名や修理内容の情報などが詳細データとして書き込まれている。履歴概略が「所有者変更」の場合には、新たな所有者名やその新たな所有者の住所などが詳細データとして書き込まれている。

【0021】

次に、車両管理サーバ10のデータベース120、車両に取り付けられるRFIDタグ、及び、車籍証明証50へのデータ登録処理の動作について説明する。図9は、データ登録処理におけるデータの流れを示す概略図である。

(1)まず、車両製造工場において車両が製造されたときに、新規車両を車両管理サーバ10のデータベース120に登録する。すなわち、車両製造工場の端末20は、新規車両に取り付けられるRFIDタグから車両IDを読み出す（ステップS110）。さらに、このRFIDタグを取り付ける車両の車両情報が入力されると、車両製造工場の端末20は、読み出した車両IDとともに車両管理サーバ10へ送信する（ステップS112）

10

20

30

40

50

。車両管理サーバ10の制御部110は、車両製造工場の端末20から車両ID及び車両情報を受信すると、これらに関連させて新規車両の車両データとしてデータベース120に登録する(ステップS114)。登録が成功した場合、車両製造工場の端末20は、データベース120に登録された車両情報をRFIDタグ内の車両データに書き込む(ステップS116)。このデータが書き込まれたRFIDタグは、出荷前までに当該車両に取り付けられる。

【0022】

(2) 販売店において新車が販売されると、所有者の新規登録を行う。販売店の端末20は、新規車両に取り付けられたRFIDタグから車両IDを読み出す(ステップS120)。さらに、この新規車両の所有者情報が入力されると、販売店の端末20は、読み出した車両IDとともに車両管理サーバ10へ送信する(ステップS122)。車両管理サーバ10の制御部110は、車両製造工場の端末20から車両ID及び所有者情報を受信すると、データベース120にこれらに関連させて所有者データとして登録する(ステップS124)。登録が成功した場合、販売店の端末20は、データベース120に登録された所有者データをRFIDタグに書き込む(ステップS126)。なお、車両管理サーバ10との情報の送受信は、車両販売ウェブサイトのサーバ30を介して行ってもよい。

10

また、車両が輸入された場合には、当該商品管理システムによる管理対象国(地域)からの輸入の場合には後述する中古車移転と同様の処理を行う。その他の国(地域)からの輸入の場合には、新たな車両として、車両データ及び所有者データ、ならびに過去の車両履歴データを、当該車両に取り付けられたRFIDタグから読み出した車両IDに関連させて車両管理サーバ10のデータベース120へ登録する。さらに、車両に取り付けられたRFIDタグに車両管理サーバ10のデータベース120へ登録した車両データ、所有者データ、及び、過去の車両履歴データが書き込まれる。このとき、必要な情報は、例えば税関の端末20から受信する。

20

【0023】

(3) 続いて、車籍証明証発行機関により、(2)において販売された車両の車籍証明証50が発行される。すなわち、車籍証明証発行機関の端末20は、発行する車籍証明証50のRFIDタグ72からカードIDを読み出す(ステップS130)。さらに、販売店から通知された車両IDが入力されると、車籍証明証発行機関の端末20は、読み出したカードIDとともに車両管理サーバ10へ送信する(ステップS132)。車両管理サーバ10の制御部110は、車籍証明証発行機関の端末20からカードID及び車両IDを受信すると、これらに関連させてデータベース120に登録する(ステップS134)。続いて、制御部110は、受信した車両IDに対応した所有者データ及び車両データを読み出して端末20へ通知し、車籍証明証50の発行を指示する(ステップS136)。車籍証明証発行機関の端末20は、入力された車両ID、及び、車両管理サーバ10から受信した所有者データ及び車両データを車籍証明証50のRFIDタグ72に書き込み、車籍証明証50を発行する(ステップS138)。なお、輸入された車両の場合には、車両管理サーバ10からさらに車両履歴データが通知され、車籍証明証50のRFIDタグ72に書き込まれる。発行された車籍証明証50は、直接あるいは販売店を通して車両所有者へ渡される。

30

40

【0024】

(4) 車両所有者が給油を行った場合、給油スタンドの端末20は、車両に取り付けられたRFIDタグから読み出した車両IDと、給油に関するデータ(給油量情報、走行距離計情報、給油地情報など)とを車両管理サーバ10へ送信する(ステップS140、ステップS142)。車両管理サーバ10の制御部110は、車両ID及び給油に関するデータ(給油データ)を受信すると、この車両IDに対応したデータベース120内の車両履歴データに、車両履歴情報として給油データを書き込む(ステップS144)。書き込みが成功した場合、給油スタンドの端末20は、登録した給油データを、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の車両履歴データに車両履歴情報として書き込む(ステップS146、ステップS148)。

50

【 0 0 2 5 】

(5) 車両の所有者が修理工場で車両の修理を行った場合、修理工場の端末20は、車両に取り付けられたRFIDタグから読み出した車両IDと、修理に関するデータ(修理データ)とを車両管理サーバ10へ送信する(ステップS150、ステップS152)。車両管理サーバ10の制御部110は、車両ID及び修理データを受信すると、この車両IDに対応したデータベース120内の車両履歴データに、車両履歴情報として修理データを書き込む(ステップS154)。書き込みが成功した場合、修理工場の端末20は、登録した修理データを、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の車両履歴データに車両履歴情報として書き込む(ステップS156、ステップS158)。

10

【 0 0 2 6 】

(6) 中古車移転が行われると、所有者変更登録を行う。中古車販売店の端末20は、移転が行われる車両に取り付けられたRFIDタグから車両IDを読み出す(ステップS160)。さらに、移転後の所有者の氏名・住所などの所有者情報が入力されると、中古車販売店の端末20は、読み出した車両IDとともに車両管理サーバ10へ送信する(ステップS162)。車両管理サーバ10の制御部110は、中古車販売店の端末20から車両ID及び所有者情報を受信すると、この車両IDに対応したデータベース120内の所有者データに新たな所有者の所有者情報を登録する(ステップS164)。登録が成功した場合、中古車販売店の端末20は、登録した所有者情報を車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の所有者データに書き込む(ステップS166、ステップS168)。

20

また、輸出が行われる場合には、当該商品管理システムによる管理対象国(地域)への輸出の場合には前述の中古車移転と同様の処理を行う。その他の国(地域)への輸出の場合には、車両管理サーバ10のデータベース120、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の所有者データを更新又は抹消するとともに、輸出の記録の車両履歴情報を車両履歴データに追加する。輸出機能の処理に必要な情報は、例えば税関の端末20から受信する。

【 0 0 2 7 】

(7) 車両登録抹消を行う場合、廃棄業者の端末20は、車両登録が抹消される車両に取り付けられたRFIDタグから車両IDを読み出す(ステップS170)。さらに、登録抹消日などの登録抹消データが入力されると、廃棄業者の端末20は、読み出した車両IDとともに車両管理サーバ10へ送信する(ステップS170、ステップS172)。車両管理サーバ10の制御部110は、廃棄業者の端末20から車両ID及び登録抹消データを受信すると、この車両IDに対応したデータベース120内の車両履歴データに、車両履歴情報として登録抹消データを書き込む(ステップS174)。登録が成功した場合、廃棄業者の端末20は、登録抹消データを車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の車両履歴データに車両履歴情報として書き込む(ステップS176、ステップS178)。

30

また、廃棄物管理票が発行された場合などには、同様の処理により、車両管理サーバ10のデータベース120、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の車両履歴データが更新される。

40

【 0 0 2 8 】

次に、商品管理システムにおける正当性確認処理の動作について説明する。この正当性確認処理は、上記(4)~(7)のデータ登録の前など、必要に応じて行われる。図10は、商品管理システムにおける正当性確認処理の動作フローを示す。

まず、端末20のタグリーダ/ライターにより、車両に取り付けられたRFIDタグから、車両ID及び所有者データを読み出し、さらに、車籍証明証50のRFIDタグ72からカードID、車両ID及び所有者データを読み出す。端末20は、読み出したこれらのデータを、車両管理サーバ10へ送信する。

【 0 0 2 9 】

50

車両管理サーバ10は、車両に取り付けられたRFIDタグから読み出した車両ID及び所有者データと、車籍証明証50のRFIDタグ72から読み出したカードID、車両ID及び所有者データとを受信する(ステップS210)。すると、車両管理サーバ10の制御部110は、車両に取り付けられたRFIDタグから読み出した車両IDと、車籍証明証50のRFIDタグ72から読み出した車両IDが一致するか否かを確認する(ステップS220)。一致している場合は、この車両IDによりデータベース120を検索して、当該車両IDに対応するカードID及び所有者データを読み出す(ステップS230)。

【0030】

続いて、制御部110は、データベース120から読み出したカードIDと、車籍証明証50のRFIDタグ72から読み出したカードIDとが一致するか否かを確認する(ステップS240)。一致する場合は、さらに、データベース120から読み出した所有者データと、車両に取り付けられたRFIDタグから読み出した所有者データと、車籍証明証50のRFIDタグ72から読み出した所有者データとが一致するか否かを確認する(ステップS250)。一致した場合には、車両管理サーバ10は、この車両が正当な所有者により使用あるいは取引された車両であると判断する(ステップS260)。

そして、制御部110は、この判断した結果を示す照合結果と所有者データとを端末20へ返送する。このとき、データベース120から読み出した車両データ及び車両履歴データのすべてまたは一部を同時に返送してもよい(ステップS270)。

端末20は、車両管理サーバ10から受信した照合結果、所有者データ、車両データ、車両履歴データ、ならびに、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の情報を表示する。これにより、端末20の操作者は、正当な所有者により使用あるいは取引された車両であることを認識することができる。

【0031】

一方、ステップS220において、車両に取り付けられたRFIDタグから読み出した車両IDと、車籍証明証50のRFIDタグ72から読み出した車両IDとが一致しないと判断した場合、ステップS240において、データベース120から読み出したカードIDと、車籍証明証50のRFIDタグ72から読み出したカードIDとが一致しないと判断した場合、あるいは、データベース120から読み出した所有者データと、車両に取り付けられたRFIDタグから読み出した所有者データと、車籍証明証50のRFIDタグ72から読み出した所有者データとが不一致であると判断した場合には、この車両が正当な所有者により使用あるいは取引された車両ではないと判断する(ステップS280)。

そして、この判断した結果を示す照合結果と、データベース120から読み出した所有者データや車両データ、車両データ、車両履歴データを端末20へ返送する(ステップS270)。端末20は、車両管理サーバ10から受信した照合結果、所有者データ、車両データ、車両履歴データ、ならびに、車両に取り付けられたRFIDタグ及び車籍証明証50のRFIDタグ72内の情報を表示する。これにより、端末20の操作者は、正当な所有者により使用あるいは取引された車両ではないことを認識するとともに、正当な所有者を確認するための情報を得ることができる。

なお、上記の正当性確認処理において、所有者データに加えて、データベース120、車両に取り付けられたRFIDタグ、及び、車籍証明証50のRFIDタグ72から読み出した車両データ、車両履歴データの一部または全ての情報を照合してもよい。また、車両に取り付けられたRFIDタグにカードIDを記憶しておき、カードIDによる照合を行っても良い。

【0032】

また、車籍証明証50により、車両に対する操作の許可を行う構成としてもよい。すなわち、車両に設けられた書き替え不可の記憶手段に、車籍証明証50のカードIDを記憶しておく。そして、車両に対するキー操作などの各種操作の前に、車両に備えられたタグリーダー/ライターにより、車籍証明証50からカードID及び車両IDを読み込ませる。そ

10

20

30

40

50

して、読み込んだカードIDが自身の記憶しているカードIDと一致しており、さらに、読み込んだ車両IDが、当該車両の車両IDと一致していると判断した場合に、車両は操作を受け付ける。

【0033】

上記実施形態によれば、車両が正当な所有者により使用あるいは取引されているものであるか否かを確認し、また、本来の所有者を確認するための情報を取得することができる。これにより、車両が盗難されてしまった場合でも、被害にあった車両を早期に発見するとともに、真の所有者の割り出しに役立てることができ、さらには、盗難を防止あるいは抑制することができる。

また、不正に取引された車両ではないことの確認に加え、給油の履歴、修理の状況、走行距離などの車両履歴の確認を容易に行うことができるため、消費者は、安心して中古車を購入することができる。また、車両に対応して発行されたカードにより車両のキー操作などの認証を行うことで、車両のみが盗難されてもこの車両を操作することができず、盗難を抑止することができる。

また、車両に取り付けるICタグとしてRFIDタグを用いることにより、車両からの情報の読み出しが容易となる。

【0034】

上述の車両管理サーバ10、端末20、携帯端末21、及び、車両販売ウェブサイトのサーバ30は内部に、コンピュータシステムを有している。そして、上述した各装置の処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。ここでコンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、CD-ROM、DVD-ROM、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしても良い。

【0035】

以上、図面を参照してこの発明の実施形態を詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【0036】

他の実施形態として、例えば、カードおよびICタグは前記所有者情報を記憶し、所有者認証手段は、前記カードから読み取ったキー情報および所有者情報と、前記ICタグから読み取ったキー情報および所有者情報とが一致したときに、データベースからキー情報を読み出し可能とするようにする。

また、このような商品管理システムにおいて、さらに、カードはカードを識別するカードIDを記憶し、データベースは前記カードIDを記憶し、所有者認証手段は、カードから読み出したカードIDとデータベースから読み出したカードIDとが一致し且つICカードから読み出した所有者情報とデータベースから読み出した所有者情報とが一致したことにより、正規所有者を認証するようにする。

【図面の簡単な説明】

【0037】

【図1】この発明の一実施形態による商品管理システムの構成を示すブロック図である。

【図2】同実施形態において、車両（自動二輪車）にRFIDタグを取り付ける場所の概略を示す概略図である。

【図3】同実施形態において、RFIDタグを取り付ける場所をより詳細に示したシートの断面図である。

【図4】同実施形態において、RFIDタグを取り付ける場所をより詳細に示したシートの断面図である。

【図5】同実施形態における車籍証明証の券面の一例を示す概略図である。

【図6】同実施形態における車両に取り付けられるRFIDタグ内のメモリに記憶される

10

20

30

40

50

データ構成を示す概略図である。

【図7】同実施形態におけるデータベースに含まれる所有者データのデータ構造を示す概略図である。

【図8】同実施形態におけるデータベースに含まれる車両履歴データのデータ構造を示す概略図である。

【図9】同実施形態におけるデータ登録処理のデータの流れを示す概略図である。

【図10】同実施形態における正当性確認処理の動作フローを示す。

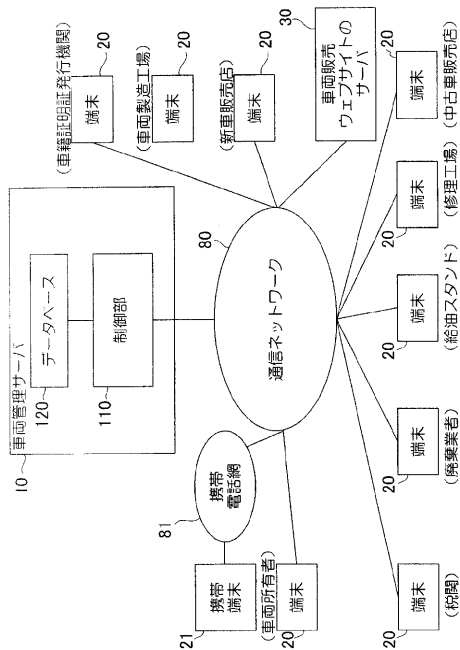
【符号の説明】

【0038】

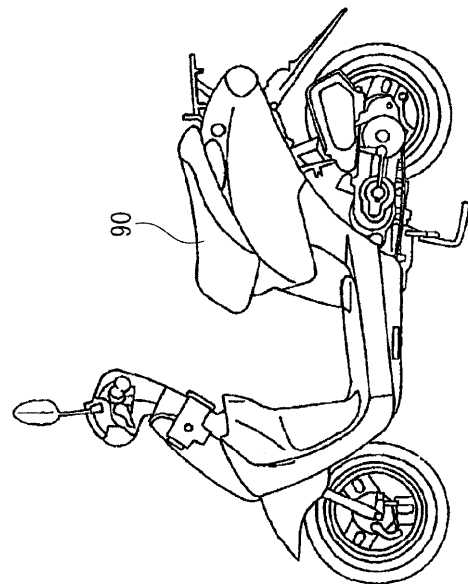
10 ... 車両管理サーバ、 50 ... 車籍証明証(カード)、 72 ... R F I D タグ(記憶媒体)、 110 ... 制御部(所有者認証手段、カード発行手段、照合手段)、 120 ... データベース

10

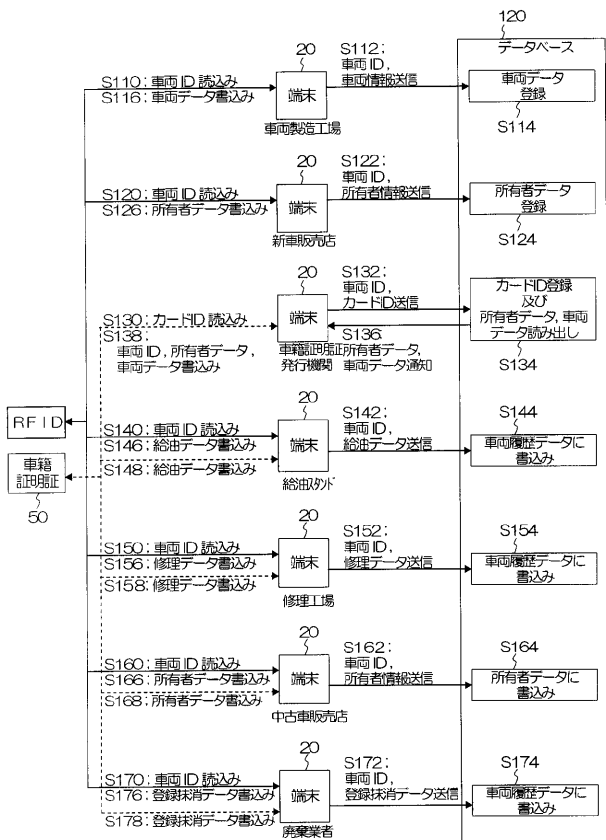
【図1】



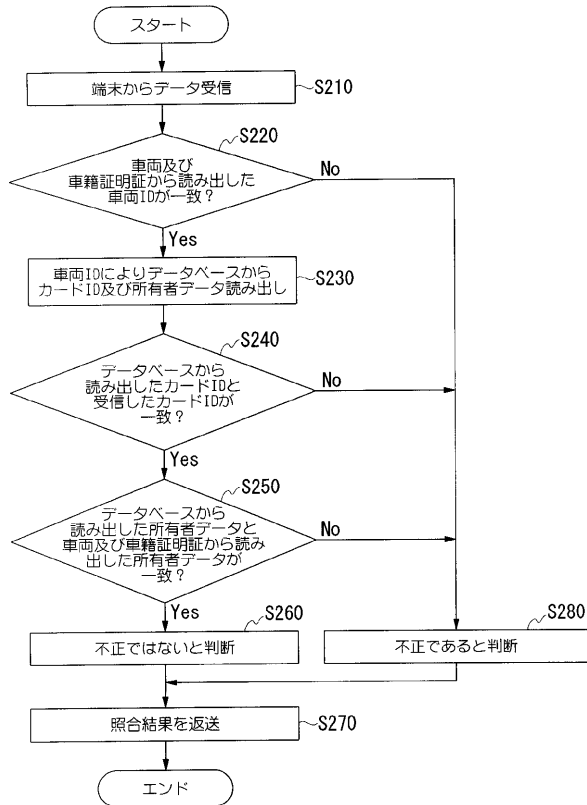
【図2】



【 図 9 】



【 図 10 】



フロントページの続き

(72)発明者 山際 登志夫

埼玉県和光市中央1丁目4番1号 株式会社本田技術研究所内

Fターム(参考) 5B058 CA17 KA11 KA31 YA01