(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2010-92498
(P2010-92498A)
(43)公開日　平成22年4月22日(2010.4.22)

(51)Int.Cl.		F I		テーマコード（参考）
G06K 17/00	(2006.01)	G06K 17/00	V	2C005
G06K 7/00	(2006.01)	G06K 17/00	L	5B035
G06K 19/10	(2006.01)	G06K 7/00	U	5B058
G06K 19/00	(2006.01)	G06K 19/00	S	5B072
B42D 15/10	(2006.01)	G06K 19/00	U	

審査請求 有　請求項の数 8　ＯＬ　（全 25 頁）　最終頁に続く

(21)出願番号　特願2009-288672 (P2009-288672)
(22)出願日　平成21年12月21日 (2009.12.21)
(62)分割の表示　特願2007-134033 (P2007-134033)の分割
原出願日　平成11年4月28日 (1999.4.28)

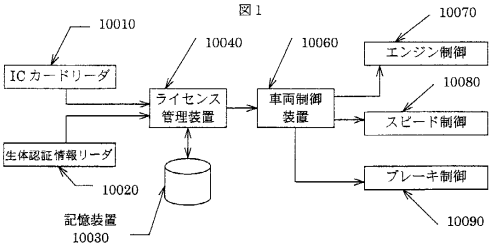
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000442
特許業務法人　武和国際特許事務所
(72)発明者　清水　宏
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内
(72)発明者　小俣　隆
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所デジタルメディア開発本部内

最終頁に続く

(54)【発明の名称】機器操作権管理システムおよび電子機器

(57)【要約】
【課題】機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うようにすること。
【解決手段】免許証としてメモリチップ等を搭載したＩＣカードなどを用い、自動車に、ＩＣカードまたは同等の機能を有する免許証を挿入する端末を設けると共に、乗車した運転手の指紋・虹彩等の生体認証情報を検知する生体認証情報検出手段を設け、また、ＩＣカードまたは同等の機能を有する免許証のメモリに、免許証の所有者の生体認証情報を表わす情報を記載する。そして例えば、運転者の生体認証情報と免許証記載の生体認証情報との照合が一致し、かつ免許証の内容が運転する自動車に合わない限り、運転を不可能とする。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
前記許可表示手段に記載されている権利者と、機器を操作する操作者との一致を、操作者の生体認証情報を用いて確認することを特徴とする機器操作権管理システム。
【請求項２】
請求項１に記載の機器操作権管理システムにおいて、
前記許可表示手段は、メモリもしくはＣＰＵを有するＩＣチップを搭載していることを特徴とする機器操作権管理システム。
【請求項３】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報は、指紋情報であることを特徴とする機器操作権管理システム。
【請求項４】
請求項３に記載の機器操作権管理システムにおいて、
前記生体認証情報を検出するセンサを、機器を最初に作動させるスイッチ上に設けたことを特徴とする機器操作権管理システム。
【請求項５】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報は、網膜もしくは虹彩形状を示す情報であることを特徴とする機器操作権管理システム。
【請求項６】
請求項５に記載の機器操作権管理システムにおいて、
前記生体認証情報を検出するセンサを、機器のステータス情報を表示するパネルに設置することを特徴とする機器操作権管理システム。
【請求項７】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
操作機器内に、前記許可表示手段の読み取り装置と、前記生体認証情報を検出するセンサとを設置することを特徴とする機器操作権管理システム。
【請求項８】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
操作機器とは別体の携帯端末装置に、前記許可表示手段の読み取り装置と、前記生体認証情報を検出するセンサとを設置することを特徴とする機器操作権管理システム。
【請求項９】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
操作機器内に、前記生体認証情報を記憶する記憶装置を有することを特徴とする機器操作権管理システム。
【請求項１０】
請求項２に記載の機器操作権管理システムにおいて、
前記許可表示手段に搭載したＩＣチップに、前記生体認証情報を記憶することを特徴とする機器操作権管理システム。
【請求項１１】
請求項１０に記載の機器操作権管理システムにおいて、
記憶している前記生体認証情報は複数種であり、操作する機器が、照合に使用する前記生体認証情報をそれぞれ自由に選択可能であることを特徴とする機器操作権管理システム。
【請求項１２】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証精度を、操作する機器の種類に応じて変化させることを特徴とする機器操作権管理システム。

【請求項１３】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器の起動前毎に行うことを特徴とする機器操作権管理システム。
【請求項１４】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器の起動後に一定時間間隔で行うことを特徴とする機器操作権管理システム。
【請求項１５】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器に搭乗する扉の開閉時毎に行うことを特徴とする機器操作権管理システム。
【請求項１６】
請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器の動作終了時毎に行うことを特徴とする機器操作権管理システム。
【請求項１７】
機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
機器の操作許可を得ている者に発行した前記許可表示手段に記載されているＩＤ番号を、少なくとも１つ以上記憶する記憶装置を有することを特徴とする機器操作権管理システム。
【請求項１８】
請求項１７に記載の機器操作権管理システムにおいて、
前記許可表示手段は紙等の非電子手段により構成され、前記ＩＤ番号は該許可表示手段上に光学的に読み取り可能な形態で記載されており、前記機器制御手段は、前記許可表示手段に記載されたＩＤ番号を読み取る読み取り手段を有することを特徴とする機器操作権管理システム。
【請求項１９】
請求項１７もしくは１８に記載の機器操作権管理システムにおいて、
前記許可表示手段に記載されたＩＤ番号が、前記機器制御手段内の記憶装置に記憶されているＩＤ番号と一致しない限り、機器の操作を不可能とすることを特徴とする機器操作権管理システム。
【請求項２０】
請求項１７から１９の何れか１つに記載の機器操作権管理システムにおいて、
前記機器制御手段内の記憶装置に記憶されているＩＤ番号と一致したＩＤ番号の前記許可表示手段を有する者に、前記記憶装置に新たなＩＤ番号を追加もしくは変更もしくは削除する手順の操作許可を与えることを特徴とする機器操作権管理システム。
【請求項２１】
機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
前記許可表示手段に記載されている操作可能機器情報を読み取る読み取り手段を有し、前記機器制御手段は、前記許可表示手段に記載されている前記操作可能機器情報が自身の機器と一致しているかの判断を行い、一致していれば機器の操作を可能とすることを特徴とする機器操作権管理システム。
【請求項２２】
請求項２１に記載の機器操作権管理システムにおいて、
前記許可表示手段は紙等の非電子手段により構成され、前記操作可能機器情報は該許可表示手段上に光学的に読み取り可能な形態で記載されており、前記機器制御手段は、前記許可表示手段に記載された操作可能機器情報を読み取る光学的読み取り手段を有すること

を特徴とする機器操作権管理システム。
【請求項２３】
請求項２１に記載の機器操作権管理システムにおいて、
前記操作可能機器情報に従って、機器の操作可能範囲を変更することを特徴とする機器操作権管理システム。
【請求項２４】
請求項２に記載の機器操作権管理システムにおいて、
前記許可表示手段に搭載したＩＣチップは、複数のアプリケーションの実行が可能なＣＰＵカードであることを特徴とする機器操作権管理システム。
【請求項２５】
請求項２４に記載の機器操作権管理システムにおいて、
前記ＣＰＵカードは、電子マネー機能を含むカードであることを特徴とする機器操作権管理システム。
【請求項２６】
請求項２もしくは２４に記載の機器操作権管理システムにおいて、
前記許可表示手段に搭載したＩＣチップは、機器が搭乗および移動可能な機器である場合に、機器の移動に伴う位置や、該位置に到達した時刻等の情報を記録することが可能であることを特徴とする機器操作権管理システム。
【請求項２７】
請求項２もしくは２４に記載の機器操作権管理システムにおいて、
機器の使用におけるルール違反等に対する罰則として、機器の使用制限を行うことを特徴とする機器操作権管理システム。
【請求項２８】
請求項２７に記載の機器操作権管理システムにおいて、
前記罰則は機器操作の一定期間の禁止を含み、時間軸に沿って、機器の使用許可および使用禁止の設定を複数回設定することが可能であることを特徴とする機器操作権管理システム。
【請求項２９】
請求項２７もしくは２８に記載の機器操作権管理システムにおいて、
前記罰則は機器操作における機能の制限を含み、時間軸に沿って、機器の使用許可および禁止を含めて、機器の使用機能制限を複数回にわたって設定することが可能であることを特徴とする機器操作権管理システム。
【請求項３０】
請求項２７から２９の何れか１つに記載の機器操作権管理システムにおいて、
前記罰則施行時期を管理する時計は、保証された時刻情報以外の情報により、機器の使用者が改変することを不可能とすることを特徴とする機器操作権管理システム。
【請求項３１】
機器操作許可情報を有するＩＣチップであって、
該ＩＣチップには、機器操作許可を有するＩＣカードの所有者のＩＤ番号および操作可能機器情報が記載されていることを特徴とするＩＣチップ。
【請求項３２】
請求項３１に記載のＩＣチップにおいて、
前記ＩＣチップには、機器操作許可を有するＩＣカードの所有者の指紋や網膜・虹彩等の生体認証情報が記載されていることを特徴とするＩＣチップ。
【請求項３３】
請求項３１に記載のＩＣチップにおいて、
前記ＩＣチップには、電子マネー機能も併せて含むことを特徴とするＩＣチップ。
【請求項３４】
請求項３１に記載のＩＣチップにおいて、
前記ＩＣチップには、機器が搭乗および移動可能な機器である場合に、機器の移動に伴

う位置や、該位置に到達した時刻等の情報が記録されることを特徴とするＩＣチップ。
【請求項３５】
請求項３１に記載のＩＣチップにおいて、
前記ＩＣチップには、機器の使用におけるルール違反等に対する罰則として、機器操作の一定期間の禁止を含み、時間軸に沿って、機器の使用許可および使用禁止の設定を複数回設定することが可能な情報を含むことを特徴とするＩＣチップ。
【請求項３６】
請求項３１に記載のＩＣチップにおいて、
ＩＣチップには、機器の使用におけるルール違反等に対する罰則として、機能の制限を含み、時間軸に沿って機器の使用許可および禁止を含めて、機器の使用機能制限を複数回にわたって設定することが可能な情報を含むことを特徴とするＩＣチップ。
【請求項３７】
請求項３１から３６の何れか１つに記載のＩＣチップにおいて、
前記ＩＣチップは、ＩＣカード内のＩＣチップであることを特徴とするＩＣチップ。
【請求項３８】
請求項３１から３６の何れか１つに記載のＩＣチップにおいて、
前記ＩＣチップは、機器を始動する鍵に内蔵されることを特徴とするＩＣチップ。
【請求項３９】
請求項３１から３６の何れか１つに記載のＩＣチップにおいて、
前記ＩＣチップには、前記罰則施行時期を管理する時計を内蔵し、この時計は保証された時刻情報以外の情報により、機器の使用者が改変することを不可能とすることを特徴とするＩＣチップ。
【請求項４０】
請求項３９に記載のＩＣチップにおいて、
前記時計を駆動する電池の寿命は、機器操作許可の期限と略等しい寿命であることを特徴とするＩＣチップ。
【請求項４１】
機器を取り扱う権利を表示する許可表示手段に記載した情報を読み取る読み取り手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理端末において、
機器の操作許可を得ている者に発行した前記許可表示手段に記載されているＩＤ番号を少なくとも１つ以上記憶する記憶装置を有することを特徴とする機器操作権管理端末。
【請求項４２】
請求項４１に記載の機器操作権管理端末において、
前記機器操作権管理端末内の前記記憶装置に記憶されているＩＤ番号と一致したＩＤ番号の前記許可表示手段を有する者に、前記記憶装置に新たなＩＤ番号を追加もしくは変更もしくは削除する手順の操作許可を与えることを特徴とする機器操作権管理端末。
【請求項４３】
半導体メモリもしくはＣＰＵで構成されたＩＣチップを内蔵したＩＣチップケースであって、
ＩＣカード内の前記ＩＣチップは電気的な接点部分を除いて絶縁体にて封印されており、前記ＩＣチップの電気的な接点の露出部のみを除くように、前記絶縁体の外面全体を導電体で覆った形状で構成されることを特徴とするＩＣチップケース。
【請求項４４】
請求項４３記載のＩＣチップケースにおいて、
前記ＩＣチップの電気的な接点の露出部と、前記導電体を結ぶ直線の間には、前記絶縁体が必ず存在することを特徴とするＩＣチップケース。
【請求項４５】
半導体メモリもしくはＣＰＵで構成されたＩＣチップを内蔵する、機器を取り扱う権利を表示する許可表示手段と、該表示許可手段と接続可能なインタフェースを有する、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、

前記ＩＣチップは、情報の暗号化・復号化を行う機能を有し、前記インタフェースには、前記ＩＣチップと同等の機能を有するＩＣチップもしくはアプリケーションソフトウェアを搭載し、前記許可表示手段に内蔵したＩＣチップと、前記インタフェースとの間の通信を、暗号化された信号により行うことを特徴とする機器操作権管理システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、機器の操作の可否を管理・制御する機器操作権管理システムにかかわる技術に関し、特に、自動車の免許証等に代表されるライセンスカード形態の機器操作権を表記する機能を有するデバイスと、同デバイスと連携して機器操作者本人であることを生体認証情報を用いて照合する機能などを有する、機器操作権管理システムにかかわる技術に関するものである。

【背景技術】

【０００２】

機器を操作する権利を有することを証明する証明書を発行し、その証明書を保有する者のみが、当該機器の操作を可能とするような、機器操作権管理方法は、各所で利用されている。例えば運転免許証の場合、免許証を持つ者のみが自動車を運転する権利を有し、警察官による運転免許証の提示指示が出たときは、速やかにこれに従い、従えない場合は罰則を科すシステムとして実運用されている。

【０００３】

しかし、自動車の運転免許証は、警察官の提示指示があるとき以外は、その効力を発揮することはなく、免許証を持っていなくても、実際には自動車の運転は可能であり、機器操作権を確実に管理するには至っていない。

【０００４】

この問題を解決するために、特開平６－８７２８５号公報（特許文献１）に開示された技術では、運転免許証としてＩＣカードを用い、このＩＣカードには、ドライバーのＩＤ等の免許証に記載されている事項を電子情報として記入し、自動車にはこの情報を読み取る端末を設け、有効な免許証でない限り、この自動車の運転が出来ないようにし、且つ、ＩＣカード内に運行記録を記入して、後に各ドライバーの稼動状況を集計する方式が記載されている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開平６－８７２８５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

上記した特許文献１に開示された技術においては、警察官に提示するとき以外に効力を持たなかった免許証を、自動車が常に判別することで、自動車を運転する権利を示す免許証としての確実な運用が可能になり、併せてＩＣカードのメモリ機能の特徴を生かして、運行状況のログを取り、最適な運行計画に反映させることも可能になる。

【０００７】

しかし、前記特許文献１に開示された技術では、下記に示すような問題があり、これらの点への配慮がなされていない。

【０００８】

（１）まず、前記特許文献１では、自動車にＩＣカード免許証を挿入した者が、本当に免許証の所有者かどうかを確認することに関しては、何らの配慮も払われていない。したがって、免許証の交付を受けた者と運転者とが同一人でない場合でも、すなわち、実際には免許が与えられていない者でも、免許証を所持さえしていれば、運転が可能になる。

【０００９】

（２）また、前記特許文献１では、交通違反等により免許証を失効したときの対応については、交通事故や交通違反時に、データ管理装置を用いて、免許証内に事故や違反データを書き込みすることや、出頭命令書や反則金納付書を発行することや、あるいは、免許停止・失効中には、免許証を自動車の端末に差し込んでもエンジンがかからないようにすることに関する記述はあるものの、これらは現行の免許証運用方法にのっとったものであって、ＩＣカードを利用することにより初めて得られるメリットを罰則に適用した検討についてはなされていない。

【００１０】

（３）また、前記特許文献１では、自動車のＩＣカード端末に、この自動車を運転することが出来る運転手のＩＤリストを有し、このＩＤと一致する運転手のみが運転できる旨は記載されてはいるものの、免許証の種類と運転可能な自動車の種類及び運転モード種類との連携については、その検討が全くなされていない。

【００１１】

（４）さらに、前記特許文献１では、ＩＣカード内容の違法な変更に対して防護を施すことに関しても、何らの配慮も払われていない。

【００１２】

本発明は上記の点に鑑みなされたもので、その目的とするところは、機器を操作するライセンスとその所有者が同一であることを、確実に認証可能とすることにある。また、本発明の目的とするところは、操作の違反を行った場合の操作制限について、木目細かく、より実質に沿った処置が可能なようにすることにある。また、本発明の目的とするところは、ライセンスのレベルにより機器操作の制限を細かく設定することを可能とし、以って、確実な機器操作者の管理と、誤操作を防止できるようにすることにある。また、本発明の目的とするところは、ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止することにある。

【課題を解決するための手段】

【００１３】

上記した目的を達成するために、本発明では、例えば以下のような手段を用いる。

【００１４】

（１）自動車にＩＣカードまたは同等の機能を有する免許証を挿入する端末を設けると共に、乗車した運転手の指紋や虹彩等の生体認証情報を検知する生体認証情報の検出手段を設け、前記ＩＣカードまたは同等の機能を有する免許証のメモリに、免許証の所有者の生体認証情報を表わす情報を記載する。

【００１５】

（２）特に自動車の場合は、通行中に違反を受けて、前記先願公報に記載のような処理を受けると、違反を起こした場所で自動車の運転が不可能になり、車の移動が不可能となってしまう。そこで、ＩＣカード内に、違反時の自動車の運転許可パターンを細かく時間軸に沿って設定することで、例えば、実際の免許停止処分の発行を２日後に設定し、自動車の端末もその指示に沿って動作する。

【００１６】

（３）ライセンスのレベルにより、運転する車の動作モードを規定する。例えば、教習所等の専用コースや駐車場において、速度１０ｋｍ／ｈ未満の走行のみが行えるライセンスの設定を行い、自動車の端末もその指示に従って動作する。

【００１７】

（４）ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止しつつ、暗号処理の必要のないデータの簡単な読み出しを可能とする。具体的には、上記（２）、（３）記載の免許停止処分の発行日程やライセンスレベルを、外部に特別な暗号処理チップを用いることなく読み出せ、且つその情報の破壊・改変を防止する。

【発明の効果】

【００１８】

本発明によれば、機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うことが出来る。また、操作の違反を行った場合の操作制限も、時間軸に沿った木目細かい処理を行うことが出来、より実質に沿った処置をすることが出来る。また、ライセンスのレベルにより、機器操作の制限を細かく設定することが出来、確実な機器操作者の管理と誤操作を防止することが可能となる。さらに、ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止しつつ、暗号処理の必要のないデータの簡単な読み出しを可能となる。

【図面の簡単な説明】

【００１９】

【図１】本発明の第１実施形態に係る機器操作権管理システムの構成例を示すブロック図である。

【図２】本発明の第１実施形態に係る機器操作権管理システムにおける、自動車の操縦席近傍へのシステム配置の１例を示す説明図である。

【図３】本発明の第１実施形態に係る機器操作権管理システムにおいて用いる、ＩＣカードの内部構成の１例を示す説明図である。

【図４】本発明の第１実施形態に係る機器操作権管理システムにおける、違反時の罰則処理パターンの１例を表で示す説明図である。

【図５】本発明の第２実施形態に係る機器操作権管理システムにおける、ライセンス種類による動作モードの規定の１例を表で示した説明図である。

【図６】本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順の第１例を示すフローチャート図である。

【図７】本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順の第２例および第３例を示すフローチャート図である。

【図８】本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードリーダおよび生体認証情報リーダを具備してなる、機器の起動を行うためのリモコンの実施形態の例を示した説明図である。

【図９】本発明による機器操作権管理システムにおいて、機器の使用許可を出していない者に使用許可を出す方法例を示した説明図である。

【図１０】本発明による機器操作権管理システムにおいて、生体認証情報の認証の精度を操縦する機器によって変更するパターンの例を示した説明図である。

【図１１】本発明による機器操作権管理システムにおいて、ＩＣカードのメモリ機能を利用して、通行ルートの記録を行う例を示した説明図である。

【図１２】本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードの機能を自動車の鍵に内蔵した実施形態の例を示す説明図である。

【図１３】本発明による機器操作権管理システムにおいて、免許証の種類により運転する車種の限定を行うパターンを示した説明図である。

【図１４】本発明による機器操作権管理システムにおいて適用可能な、端末装置へのＩＣカード挿入時におけるＩＣチップの静電破壊を防止するための、ＩＣカードの実施形態の例を示した説明図である。

【図１５】本発明による機器操作権管理システムにおいて適用可能な、端末（端末装置）とＩＣカード間の情報の守秘を行う実施形態の例を示した説明図である。

【発明を実施するための形態】

【００２０】

以下、本発明の実施の形態を、図面を用いて説明する。

【００２１】

図１は、本発明の第１実施形態に係る機器操作権管理システムの構成を示すブロック図であり、本実施形態は、自動車における機器操作権管理システムへの適用例である。本システムは、機器（ここでは自動車）の動作の可否を制御する機器制御機能をもつ装置と、機器を取り扱う権利（ここでは運転免許であり、例えば、教習所内などの限定されたエリアのみでの運転を許可するものを含むものとする）を示す情報をもつ許可表示手段として

のＩＣカードとを、少なくとも含むものとなっている。

【００２２】

自動車にはＩＣカードリーダ10010 があり、ドライバーは自動車を運転する際に、自身のＩＣカードをＩＣカードリーダ10010 に差し込む。生体認証情報リーダ10020 は運転席に座ったドライバーの指紋もしくは虹彩・網膜などの人間自身のＩＤを示す生体認証情報を読み取る。ライセンス管理装置10040 は、前記ＩＣカードリーダ10010 によってＩＣカードから読取られた、該当免許証の所有者の情報と、同じく前記生体認証情報リーダ10020 によって読み取られた、運転席に座ったドライバーの生体認証情報とを比較し、同一であるかどうかの判断を行う。

【００２３】

記憶装置10030 は、例えばこの車両を運転してもよいドライバーを限定するときに、そのドライバーＩＤを記憶する。差し込まれたＩＣカードのドライバーＩＤが、この記憶装置10030 に記憶されたドライバーＩＤと一致しないときは、後述する車両制御装置10060 によりエンジン始動を抑制する。

【００２４】

ライセンス管理装置10040 が、差し込まれたＩＣカードからの情報と生体認証情報リーダ10020 からの情報とにより、運転席に座ったドライバーが確かにこの自動車を運転する資格を有する本人と判断したとき、ライセンス管理装置10040 は、車両制御装置10060 に動作許可を示すメッセージを送る。

【００２５】

車両制御装置10060 は、この許可メッセージに従って、エンジン始動の可否を含めてエンジンの制御を行うエンジン制御装置10070 や、自動車の走行速度のリミッターを制御するスピード制御装置10080 や、ＡＢＳ（Antilock Brake System ）の動作、レベルを設定するブレーキ制御装置10090に、それぞれ動作許可指示を送る。これによりエンジンの始動が可能になり、またドライバーの資格レベルに従った最高速度の設定、さらに、現行の免許証制度では存在しないがドライバーの技量に見合った形でＡＢＳのＯＮ／ＯＦＦ制御を行う。

【００２６】

図２は、本実施形態の機器操作権管理システムにおける、自動車の操縦席近傍へのシステム配置の１例を示した説明図である。

【００２７】

20000 はコックピットである。運転席右にＩＣカード挿入口20020 があり、この自動車を運転するドライバーは、自身の免許証であるＩＣカードをこの挿入口20020 に挿入する。次に、指紋読み取り部兼エンジン始動ボタン20030 を押すことで、ドライバーの指紋を読み取り、先のＩＣカードに記載したドライバーの生体認証情報との認証を行う。そして、紋読み取り部兼エンジン始動ボタン20030 を押した人が、確かにＩＣカードの示す本人であることを認識して、初めてエンジンの始動が行える。

【００２８】

このとき、記憶装置20050 に、この自動車を操縦してもよいドライバーのＩＤリストを持つことにより、挿入したＩＣカードのＩＤとの照合を行い、図１の説明と同様に、操縦許可のないドライバーでは、自動車のエンジン始動を含む操作が出来ないようにして、盗難防止等のセキュリティを確保することが出来る。

【００２９】

生体認証情報の確認手法としては、スピードメーター位置に網膜・虹彩センサ20010 を設ける方法もある。この場合、ドライバーが運転席に座らない限りは、このセンサを用いて検出することが出来ないので、例えば先の指紋読み取り部兼エンジン始動ボタン20030 を、ＩＣカード（免許証）を交付された本人が助手席から押して、免許証がない人が運転席に座って運転するようなことが、不可能になる。ここで、スピードメーターはドライバーの視線が必ず行くところであり、且つドライバーシートは頭の位置がほぼ固定されるので、網膜・虹彩センサ20010 を設置するのに適している。

【００３０】
また、ここで免許証として利用するデバイスは、ＩＣカードであり、電子マネー等で使用するマルチアプリケーション対応のＩＣカードである。これにより、同じＩＣカード内に、電子マネーや電子クレジット等のアプリケーションを同居させることが出来、自動車から料金自動支払いシステム20040 へのアクセスによって、高速道路の自動料金支払いや、ドライブスルーやガソリンスタンド等の必ず自動車に乗車している条件下で買物を行うシステムへの対応を行うことも出来る。
【００３１】
さらに、ここで使用する免許証がＩＣカードを用いずに、従来の印刷物による免許証を利用しても、カード挿入口に免許証を挿入して、ＩＤ番号等をイメージスキャナで読み取ることで、この自動車の操縦許可を得ているドライバーの免許証かどうかの判断を行うことが出来る。さらに記憶装置10030 に、ドライバーの生体認証情報を記録しておくことで、ＩＣカードを用いなくても、従来の免許証システムで、免許証と生体認証情報によるドライバー本人との照合を行うことも可能であり、ＩＣカードではなく従来の免許証システムをそのまま用いても、本発明の機能を実現することが出来る。
【００３２】
図３は、本実施形態の機器操作権管理システムにおいて用いるＩＣカードの内部構成（ＩＣカードに搭載したＩＣチップの内部構成）の１例を示す説明図である。
【００３３】
ＩＣカード30000 に搭載したＩＣチップ30005 は、ＭＦ30010 （Master File ）をルートとして、その下位に複数のＤＦ（Dedicated File）を有し、ＤＦ１(30020)は免許証、ＤＦ２(30060)は例えば電子マネーに用いられている。ＤＦ１(30020)の下には複数のＥＦ（Elementary File ）があり、電子免許証に関連する情報が記載されている。ＥＦ１(30030)には、免許証ＩＤ番号と、生体認証情報を示す指紋情報や虹彩情報などがある。この場合、生体認証情報は複数種類あってもよく、自動車の端末に装着された生体認証情報リーダ10020 が、例えば指紋スキャナであった場合は、指紋情報を用い、虹彩センサであるならば、虹彩情報を用いればよい。ＥＦ２(30040)には、この免許証のライセンス種類やレベルが、そしてＥＦ３(30050)には、違反履歴が記載される。ＣＰＵカードは、ＤＦやＥＦがプログラムになっており、外部から特定のコマンドを入力するときのみ、生体認証情報を読み出したり、違反履歴を書き換えたりすることが出来る。この特定のコマンドは、専用のソフトや後述する専用のチップのみが行い、これによりカードの内部情報の機密を保ち、改変を防止することが出来る。
【００３４】
また、ここでカード内に時計30070 を設け、前記生体認証情報や違反履歴と同様に、専用のソフトやチップを介さない限り、この時計の日付・時刻を改変出来ない仕掛けとすることで、図４にて後述する、違反時の罰則発行を日付に従って施行する際に、故意に時計を狂わせて罰則発行を免れるような行為を完全に防止することが出来る。カード上で単体で動作する時計のため、当然狂いが生じるが、これはカードを車載の端末に挿入したときに、専用のソフトもしくはチップがＧＰＳ等の確実に信頼できる時計により確認した正しい時刻を用いて、カード内の時計の狂いを修正する。この時刻の修正は、自動車に搭載した端末に限らず、図２に示した料金自動支払い時の通信において行ってもよく、また自動車に関係なく、電子マネー端末と連携して、電子マネーや電子クレジットによる買物を行った際に、端末から時計の修正を随時行ってもよい。また、ＩＣカード内に設置された時計は、ＩＣカードの駆動電源を外部から与えられなくても動作する必要があり、薄型電池をＩＣカード内に内蔵する。この電池の寿命は、基本的に免許の許可期限以上の寿命とするが、場合によっては、免許の許可期限と略同程度の寿命を持つようにしてもよい。時計の駆動以外ではこの電池は一切使用しないので、使用条件により寿命が短くなるという現象は起きず、正確に寿命の設定をすることが可能である。
【００３５】
図４は、本実施形態における、違反時の罰則処理パターンの１例を示す表図である。

【００３６】
罰則処理のパターンとして、本実施形態では、自動車を運転する際の動作モードを、(１)エンジン始動のみ、(２)１０ｋｍ／ｈ未満の走行、(３)通常走行可能の３つに分類した。例えば無違反の場合は、当然ながらこの３つの動作モードをすべて使うことが可能である。
【００３７】
まず、従来の免許停止に相当するスピード違反について示す。従来の免許証では、スピード違反による罰則すなわち免許停止は即時発行するが、例えば旅行途中でスピード違反をした場合には、そのまま乗って帰ることになり、さらに警察に見つからなければ、そのまま乗り続けることも現実には可能となってしまう。そこで、例えばＩＣカード等による電子情報として違反情報を記載し、自動車にこれに対応する端末を設け、免許停止を即時発行した場合は、その場で例えば半年間のあいだ、自動車を動かすことが出来なくなり、道の真ん中で車を置き去りにするという現象が発生する。本実施形態では、スピード違反をした後、その罰則の発行を違反時から例えば２日後からと設定し、その間に自動車を自宅に持ち帰ったり、貸出し元に返却したりする。その上で実際の罰則が発行されて、この免許証では運転が出来ないような処理をすることが出来る。
【００３８】
また、即時免許停止が必要なほど異常なスピード違反を行った場合、少なくとも高速道路のサービスエリア上の道端から、駐車エリアまでは車の移動が出来るように、１０ｋｍ／ｈ以下の走行のみを例えば２日間の一定期間だけ可能とし、一般道路の通常走行の禁止は即時発行する。
【００３９】
また、酒気帯び運転による免許停止発行の場合は、少なくとも摘発時点では車の走行は即時やめさせる必要があるので、１０ｋｍ／ｈ以下の走行は勿論、自動車のエンジン始動も不可能とする。これは摘発されたドライバーが酔いから醒めるまでの期間として、例えば６時間だけ完全な運転禁止とし、その後、前記したスピード違反と同様に２日間だけ通常走行を可能として、自宅に車を持ち帰った後、免許停止が初めて発行される。この期間はドライバーの自宅までの距離や情状酌量に応じて、摘発した担当者が決定することが出来る。
【００４０】
なお、ＩＣカードに書き込む罰則による制限事項は、時間軸に沿って、使用許可、使用禁止、使用機能制限などを複数回にわたって設定可能となっている。
【００４１】
本実施形態における罰則発行の時期・時刻は、ある基準となる時計に従って施行されるが、例えば通常の自動車に搭載された時計を用いた場合、ドライバーが勝手にその時計を変更し、例えば時計を半年進めてしまえば、すでに処分期間は過ぎているので、勝手に運転をすることが可能となってしまう。これを防ぐために、図３に示したように、外部から勝手に時刻の変更を行えないような時計をＩＣカード内に持ったり、同様な機能、すなわちＧＰＳ等の確実に信頼できる時計により時刻の修正を行う以外は、任意の時刻設定がまったく出来ないような時計を、車載の端末に持たせてもよい。
【００４２】
図５は、本発明の第２実施形態に係る機器操作権管理システムにおける、ライセンス種類による動作モードの規定の１例を記述した表図である。本実施形態はヘリコプターの操縦を想定した例であり、正規ライセンスのパイロット、訓練生、そしてメカニックそれぞれのライセンスと、それぞれに対する動作モードを示している。
【００４３】
正規ライセンスのパイロットは、当然ながらエンジン始動、ホバリング、低速飛行、高速飛行のすべてを行うことが出来る。訓練生の場合は、エンジン始動から低速飛行までが行え、高速飛行への制限がある。具体的には、例えばメインローター回転面の角度を、パイロットの意志では一定以上傾けることが出来ないような制御を入れる。勿論ジャイロ等

による自動姿勢制御はこの制限を受けずに、角度一杯まで倒すことが可能である。また、簡単な浮上試験が出来る資格を持つメカニック１級はエンジン始動及びホバリングまで可能とする。具体的には、極低速の前後左右移動までが可能な程度に、例えばメインローター回転面の角度の変更操作が不可能となるような制御を行う。整備資格のみを持つメカニック２級の場合はエンジン始動のみである。

【００４４】

このような制御の具体的な制限手法は、操縦する機器により異なるが、ＩＣカード免許にライセンスのレベルを記載し、実際に操作する機器側で、そのライセンスでどこまで操作出来るかを設定することで、例えば自動車を運転する際、同じ仮免許証でも、一般道路と専用コース内で動作モードを変えるような制御が可能である。

【００４５】

図６は、本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順を示したフローチャートの第１例である。

【００４６】

まず、操作する機器にＩＤカードを挿入し（ステップ60010 ）、次に指紋の入力を行う（ステップ60020 ）。次に、ステップ60030 にて、挿入したＩＤカードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者がＩＤカードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、ＩＤカードのEject を行う（ステップ60040 ）。照合結果が○であれば、エンジンスタートを行い（ステップ60050 ）、操縦する機器が自動車であれば、走行を行う（ステップ60060 ）。

【００４７】

ここで、例えばＩＤカードは前記した如く、メモリを持つＩＣチップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号等をイメージスキャナで読み取り、図１、図２で示した機器に搭載されている記憶装置から、該当免許証番号に対応した指紋情報を読み出して、操縦者が入力した指紋との一致判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【００４８】

図７は、本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順を示したフローチャートの第２例と第３例である。

【００４９】

図７の（ａ）は、ＩＤカードと操縦する機器の種類の照合を行う場合のフローチャートである。まず、操縦者は機器にＩＤカードを挿入し（ステップ70010 ）、操縦する機器は挿入されたＩＤカードからライセンスＩＤを読取る。そして、該当ライセンスＩＤが、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70020 ）、操縦が出来ない場合は運転不可表示を行い、且つＩＤカードのEject を行う（ステップ70030 ）。照合結果が○であれば、エンジンスタートを行い（ステップ70040 ）、操縦する機器が自動車であれば、走行を行う（ステップ70050 ）。

【００５０】

ここで、例えばＩＤカードは前記した如く、メモリを持つＩＣチップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号及び記載されている操縦可能機器の種類をイメージスキャナで読み取り、本機器を操縦できるライセンスかどうかの判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【００５１】

図７の（ｂ）は、図６と図７の（ａ）の両方の機能を実現した例を示すフローチャートである。すなわち、操縦者は機器にＩＤカードを挿入し（ステップ70010 ）、次に指紋の入力を行う（ステップ70060 ）。次に、ステップ70070 にて、挿入したＩＤカードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者がＩＤカードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、ＩＤカードのEject を行う（ステップ70031 ）。照合結果が○であれば、挿入されたＩＤカード

から読み取ったライセンスＩＤが、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70021 ）、操縦が出来ない場合は運転不可表示を行い、且つＩＤカードのEject を行う（ステップ70032 ）。照合結果が○であれば、エンジンスタートを行い（ステップ70041 ）、操縦する機器が自動車であれば、走行を行う（ステップ70051 ）。

【００５２】

ここで、指紋照合とライセンスＩＤの照合順序は、どちらでも構わないが、例えば自動車において、指名手配者等のライセンスＩＤをネットワーク等で自動車が常に受信している場合、この照合時点にて自動車は搭乗しているドライバーが犯罪者等であることを認識し、運転不可表示を行うと同時に、図示しない通信手段を用いて、犯罪者の存在を警察等に知らせるという仕掛けを実現することも出来る。この手順を一番最初に行うことで、確実な犯罪者の検知を行うことが可能となる。

【００５３】

なおまた、指紋照合などの生体認証情報の認証（照合）は、自動車等の乗り物の所定の扉の取っ手に指紋読み取りセンサを設けることなどにより、乗り物に搭乗する際の、扉の開閉操作と同時に行うようにしてもよい。

【００５４】

さらにまた、指紋や虹彩などの生体認証情報の認証（照合）は、自動車などの機器の起動前毎に行うだけでなく、機器の起動開始許可後に、一定時間毎に行うようにしたり、あるいは、機器の動作終了時毎に行うようにしてもよい。このようにすることで、機器の動作を立ち上げた後に、最初に認証した人物と異なる者が、途中で機器の運転や操縦などを交代したかどうかを監視することができる。そして、途中で運転や操縦などを交代した場合には、自動車等の機器がこの旨を警告したり、時と場合によるが警告後に機器の動作を徐々に停止させたり、あるいは、ＩＣカードや機器の記憶装置に、不正交代したことの情報と交代後の人物の生体認証情報とを併せて記録したり、または、不正交代したことの情報と交代後の人物の生体認証情報とを外部に自動報知したりするような、仕組みとすることもできる。したがって、タクシーなどにおいて、悪意の乗客が車を乗っ取って運転した時などにおいて、大いにその効力を発揮する。

【００５５】

図８は、本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードリーダおよび生体認証情報リーダを装着してなる、機器の起動を行うためのリモコンの実施形態の例を示した説明図である。

【００５６】

図８の（ａ）に示したリモコンは、リモコンにＩＣカードリーダと生体認証情報リーダとしての指紋スキャナとを具備させることにより、前記した第１実施形態における機器制御機能をもつ車載の装置（端末装置）と同等の機能を持たせたものである。

【００５７】

リモコン本体には、指紋スキャナ兼スターターボタン80020 があり、利用者がＩＣカード80030 を差し込んで、ボタン80020 に指を乗せることで指紋のスキャンを行い、ＩＣカード80030 内に記載した指紋情報とスキャンした利用者の指紋情報との照合を行って、照合が成立したときに初めて、赤外線／電波発射口80010 より、自動車のエンジンスタートやドアロック解除等の信号を、赤外線もしくは電波によって発射する。

【００５８】

図８の（ｂ）は、ＩＣカードの機能をリモコンの内部に内蔵した例である。この例の場合、汎用の自動車の免許証とは異なる使用形態になるが、ある機器を動かそうとしたときに、その機器を動かす資格のある者の指紋情報を記憶しているので、他の者が機器を動かそうとしてもスタート出来ない。また、ＩＣカードの差し込みがないのでカードの携帯による紛失を回避することも出来る。

【００５９】

図９は、本発明による機器操作権管理システムにおいて、機器の使用許可を出していない者に使用許可を出す方法例を示した説明図である。具体的な例として、ある自動車のオ

ーナーが、その自動車を運転する権利を他の人に与えるための操作フローを、操作画面を元に説明する。

【００６０】

まず、図９の（ａ）の操作画面で示すように、自動車は他人への運転許可を与える人が、確かにその車のオーナーかどうかの判定をするために、オーナーにＩＤカードの挿入を促す。ここで、図示しない指紋等の生体認証情報の照合により、オーナー本人であることを確認する。

【００６１】

次に、図９の（ｂ）に示す操作画面で、他人に与える運転許可モードを選択する。すなわち、「１」を選択することで当日のみ、「２」を選択することで指定日付を指定する。そして、「３」を選択することで、例えば家族などの永久ライセンスを与える。この選択の後、図９の（ａ）と同様な操作画面にて、運転許可を与えるドライバーのＩＤカードの挿入を促し、運転許可の登録を行う。

【００６２】

図９の（ｃ）の画面は、現在この車に既に登録されている運転可能ドライバーの一覧を表示したものを示す。ここで番号により選択を行うことで、図９の（ｄ）の操作画面に示すように、運転許可モードの変更を行うことが出来る。

【００６３】

図１０は、本発明による機器操作権管理システムにおいて、生体認証情報の認証の精度を操縦する機器によって変更するパターンの例を示した説明図である。生体認証情報の認証（照合）は、例えば指紋照合の方式では、現状、代表的なものとして次の３方式がある。

（１）．指紋の稜線の分岐点、端点の位置と方向を照合するマニーシャア方式。

（２）．（１）に加え、相対的な位置関係を用いるマニーシャアリレーション方式。データ量と処理負荷が大きいが、警察庁が犯人を割り出すのに使用している。

（３）．特徴点を含む画像片（チップ）を用いて照合する画像チップ方式。

【００６４】

方式としての認証精度は、（２）→（３）→（１）の順となっている。また、その各々に対して、どれだけサンプリングするかで照合精度が変化し、サンプリング数を上げると処理時間がかかる。照合精度の取り方としては、例えば、特徴点を１５箇所くらい選んで、これを順次照合し、７箇所連続して一致すれば照合作業完とする。このように特徴点の数と、照合をどこまでで止めるかで照合精度が決まり、例えば全部照合すると時間もかかり、逆に本人照合率が低下することもある。

【００６５】

基本的に、ライセンスの種類により操縦できる機器が確実に限定されるのが、目標であり理想であるが、上記の問題により認証精度を上げると、処理時間がかかったり、逆に本人でも認証してくれないという現象が発生する。操縦する機器の種類によっては、本人認証のレベルを下げてもよいものがあり、処理速度の向上やコストの削減に対応することが可能になる。

【００６６】

図１０の表は、操縦する車種とその重要度とライセンスの資格レベルを示す。重要度はＣがもっとも低く、Ａがもっとも重要度が高い。また、資格レベルはＥがもっとも低く、Ａがもっとも高くて、高いレベルのライセンスを持つ者は低いレベルのライセンスの運転資格も同時に有する。例えば普通免許証をＤとし、原動機付自転車の免許証をＥとすると、Ｄの免許証を持つ者は原動機付自転車の運転も可能である。

【００６７】

図１０の表において、重要度がＣの原動機付自転車は、その操縦資格レベルも最低のＥであるので、免許証を持っている者ならほとんどの者が操縦可能な機器である。そこで生体認証情報の認証も精密にやる必要がなく、生体認証レベルを最低のレベル「１」としてある。

【００６８】
普通自動車やタクシー、大型車は、車両のコストも高価で盗難による影響も大きいので、重要度をＢとする。その中で普通車は一般個人車両であるので、その資格レベルはＤ、タクシーは業務車両であるので、その資格レベルをＣとする。この２つは、車両の大きさおよび操縦の難易度は同じであるため、生体認証レベルは同じとして、原動機付自転車よりも高いレベル「２」に設定する。
【００６９】
大型車は、前記２つの車両に比べて大きく、運転も難易度が高いため、より確実な資格が必要（資格レベルＢ）になるということで、生体認証レベルをさらに高いレベル「３」に設定する。
【００７０】
そして最後に、緊急自動車は、重要度がＡともっとも高く、特定の資格者のみが操縦するということで、資格レベルも最高のＡとする。そして盗難が発生したときの影響がもっとも大きいので、より確実なドライバーの確認を行うために、生体認証レベルを最高の「４」とする。この場合、緊急車両は緊急出動が必要となるため、確実な認証と同時に、有資格者を間違えずに短時間で確実に認証する必要がある。このため、生体認証のアルゴリズムもそれに適したものを利用することになる。
【００７１】
図１１は、本発明による機器操作権管理システムにおいて、ＩＣカードのメモリ機能を利用して、通行ルートの記録を行う例を示した説明図である。すなわち、図１に示した前記第１実施形態の機器操作管理システムを用いて自動車を運転する者が、その走行経路を自身の記録として、ＩＣカードに保存する方法を示した説明図である。
【００７２】
図１１の（ａ）は、ドライバーがたどる経路を示している。出発点11040 から、道路11030 を通過して交差点11020 を左折した後、Ｙ字分岐11010 を左折して、目的地11000 に到着する。この通行経路は、あらかじめカーナビゲーションシステムにより設定しておくが、通行時に、交差点11020 の様子を電子カメラで撮影する（11060 は、この撮影画像を示している）。画像上に重ねた矢印11070 は、実際に自動車が曲がった方向である。
【００７３】
図１１の（ｂ）は、ドライバーの通行経路をドライバーのＩＣカードに記録するフォーマットの例である。通行路を、交差点を主に、いくつかのチェックポイント別に分離し、始点座標と終点座標を緯度・経度で表記し、始点を通過した日付・時刻と、このルートを通行するのに要した時間とを記載する。さらに、交差点のマークとなるように、図１１の（ａ）で撮影した画像のファイル名を添付する。この記録は、走行中に一旦車載の記憶装置に記録して、最後にＩＣカードにダウンロードするようにしてもよい。
【００７４】
このような記録を行うことにより、ＩＣカード（特にＣＰＵカード）の守秘性により、改変しない正確な走行記録を、走行した個人の管理下に置くことが可能となり、個人的な管理および、例えば同一の車種および外観の自動車が犯罪を起こしたときに、この記録により自身が犯罪とは関係ないことを証明することも可能となる。
【００７５】
図１２は、本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードの機能を自動車の鍵に内蔵した実施形態の例を示す説明図である。
【００７６】
図１２の（ａ）は、鍵120010にＩＣチップ120020を内蔵させ、インタフェース端子120030によって、この鍵120010と鍵を挿入する自動車の端末とを接続するように構成した例である。この場合、免許証とは形態は異なるが、鍵自身に前述した如くドライバーのＩＤ番号や生体認証情報を入れておくことで、現状と同様の鍵の使用のみで、ＩＣカードの利用と同様な効果をもたせることができる。
【００７７】

図１２の（ｂ）は、鍵120011に、図１２の（ａ）の鍵120010の機能に加えて、さらに指紋センサ120040を内蔵させた例である。なお、図１２の（ｂ）において、120021はＩＣチップ、120031はインタフェース端子である。

【００７８】

この図１２の（ｂ）の例の場合には、鍵120011を自動車の鍵穴に挿入し、ひねってエンジンをかけるという現在の操作とまったく同じ操作で、前記した実施形態と同様の効果を得ることができる。ここで、指紋センサ120040に代替する生体認証情報センサとして、個人によって微妙に異なる指の荷重分布を情報として検出するセンサを用いてもよい。また、荷重分布も面方向だけではなく、鍵をひねる際の時間軸による荷重変化を生体認証情報として用いてもよい。鍵を持つ・ひねるという操作を利用することで、指紋センサという高度なセンサを用いなくても、生体認証情報の認証を行うことが可能である。

【００７９】

図１３は、本発明による機器操作権管理システムにおいて、免許証の種類により運転する車種の限定を行うパターンを示した説明図である。図１３の表のフォーマットは、図４、図５と同様のためここでの説明は省略する。

【００８０】

免許証の種類は練習生、仮免許、本免許、そしてＡＴ（オートマチック車）限定を示す。例えば、教習所内でのみの運転を行う練習生は、エンジン始動も含めてすべて△とする。これは、操作は可能であるが、助手席に本免許証を有するものが搭乗している条件で運転が可能ということを示す。助手席に本免許証を有するものがいることの証明は、教習専用の車で、運転席と同様のＩＣカードリーダーを助手席に設置する方法と、図９で示した運転許可を与えるのと同様に、事前に本免許証を運転席の端末に差し込んで、認証を行った上で、練習生に運転許可を与える方法がある。仮免許による運転許可も同様である。

【００８１】

本免許は当然すべての自動車の操縦ができるが、ここでＡＴ限定免許の者は、そのライセンスの種類により、ＡＴ車の走行は可能であるが、ＭＴ車の走行は不可能となる。具体的には、ギアを入れるとスロットルが開かないように、もしくはエンジンストールをするような仕掛けとする。ただし、緊急脱出用にスターターモーターによる走行を可能としたり、５分以内の速度１０ｋｍ／ｈ未満の走行のみを可能とするような制御を行ってもよい。

【００８２】

図１４は、本発明による機器操作権管理システムにおいて適用可能な、端末装置へのＩＣカード挿入時におけるＩＣチップの静電破壊を防止するための、ＩＣカードの実施形態の例を示した説明図である。

【００８３】

140060は端末（端末装置）側のＩＣカード挿入口であり、挿入時にコネクタ140061にて、ＩＣカード側の電極と接続する。ＩＣカード140000は、その芯が絶縁体で構成され、ＩＣチップ140010が封入されて電極部のみが表面に露出されている。そして、ＩＣカード140000はその周囲を導電体140030が覆っており、導電体とＩＣチップの間にはスパーク等が生じないように一定の間隔があくように、且つ、導電体とＩＣチップとの間にスパークが飛ぶような空間が存在せず、必ず絶縁体がさえぎる形で入るように絶縁体140020の形状が設定されている。

【００８４】

ＩＣカード140000を利用者が持つと、導電体140030は人体を通じてアースされる（140040）。ＩＣカードを端末に挿入するときに、特に自動車等の場合は、アースに相当する路面との間がゴムタイヤで絶縁されているため、帯電した自動車と挿入したＩＣカードとの間（140070）にスパークが生じる。このスパークがＩＣチップ140010に流れ込まないように、導電体140030を通して人体経由でアースさせることで、端末とＩＣカードの電位を等しくする。また、端末内のＩＣカードスロットには導電ブラシ140050を設け、特にＩＣカードの端子表面の除電や埃の清掃等を行う。これにより、特に自動車特有の高電圧静電気

によるＩＣカード（ＩＣチップ）の破損を防止することができる。

【００８５】

図１５は、本発明による機器操作権管理システムにおいて適用可能な、端末（端末装置）とＩＣカード間の情報の守秘を行う実施形態の例を示した説明図である。

【００８６】

端末150000（端末装置）とＩＣカード150100の間の情報は、例えば図１４に示した接点をモニターすることで、傍受が可能である。さらに傍受した信号を解析することで、この接点から擬似的な信号を入力して、ＩＣカード記載事項の改変を行うこともできる。

【００８７】

そこで、図１５に示した本例では、ＩＣカード150100のＩＣチップに、ＣＰＵ内蔵チップを用い、端末150000との間の信号の授受を暗号化した信号で行う。端末150000側には、ＩＣカードに内蔵したチップと同等の機能を持つＣＰＵ内蔵チップ150010、もしくは、専用アプリケーション150020があり、ＩＣカードとの通信をこれらのチップもしくはアプリケーション経由にて行う。ＩＣカード150100に内蔵のＩＣチップと、端末150000側のＩＣチップもしくはアプリケーションは同じ方式による暗号化・復号化機能を有し、ＩＣカード150100の情報の読み出し、書き換え等のコマンドおよび情報の傍受、並びにこれらに基づく改変や偽造を、確実に防止する。免許証番号や氏名等、通常の免許証の記載事項と同等で、秘密にする必要のない情報は、スルー経路150030を通して読み出すことができる。この場合は、例えば電子マネーの残高表示機と同様に、ごく簡単な構造の端末で情報の表示を行うことができる。また、暗号処理を行わなくても、ＣＰＵチップの使用により、ＩＣカードへの書き込みアクセスに特定のコマンドを使用することが可能となり、簡便に誤操作や破壊を防止することが可能となる。

【００８８】

以上、本発明を主として図示した実施形態によって説明したが、当業者には本発明の精神を逸脱しない範囲で種々の変形が可能であることは言うまでもなく、例えば、ＩＣカードとして接触式で情報を授受するもの以外にも、ＩＣカードに至近距離間での無線送受信が可能な機能を具備させて、非接触で情報を授受するタイプのものを用いることも可能である。この場合、本発明のＩＣチップの機能を、携帯電話や腕時計などの携帯機器に内蔵させることも可能である。

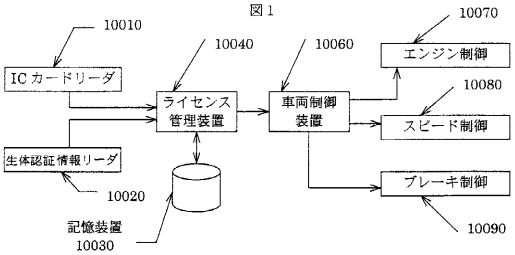
【符号の説明】

【００８９】

10010　ＩＣカードリーダ
10020　生体認証情報リーダ
10030　記憶装置
10040　ライセンス管理装置
10060　車両制御装置
10070　エンジン制御装置
10080　スピード制御装置
10090　ブレーキ制御装置
20000　コックピット
20010　網膜・虹彩センサ
20020　ＩＣカード挿入口
20030　指紋読み取り部兼エンジン始動ボタン
20040　料金自動支払いシステム
20050　記憶装置
30000　ＩＣカード
30005　ＩＣチップ

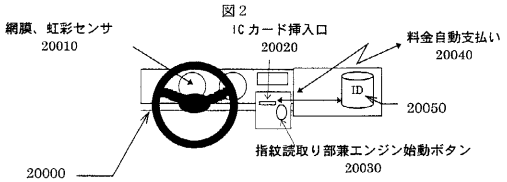
【図１】

図１



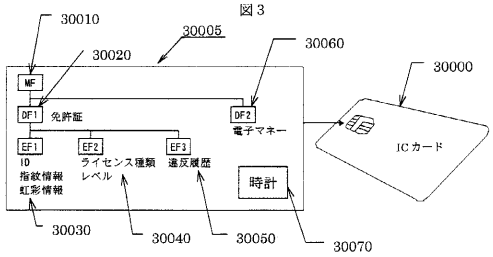
【図２】

図２



【図３】

図３



【図４】

図４

#	事項	動作モード		
		エンジン始動	10km/h 未満	通常走行
1	無違反	○	○	○
2	スピード違反	○	○	○(但２日間)
3	重大スピード違反	○	○(但２日間)	×
4	酒気帯び運転	×(但６時間)	×(但６時間)	○ (但６時間以降２日間)

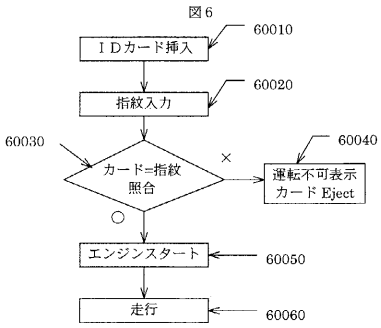
【図５】

図５

#	事項	動作モード			
		エンジン始動	ホバリング	低速飛行	高速飛行
1	パイロット	○	○	○	○
2	訓練生	○	○	○	×
3	メカニック１級	○	○	×	×
4	メカニック２級	○	×	×	×

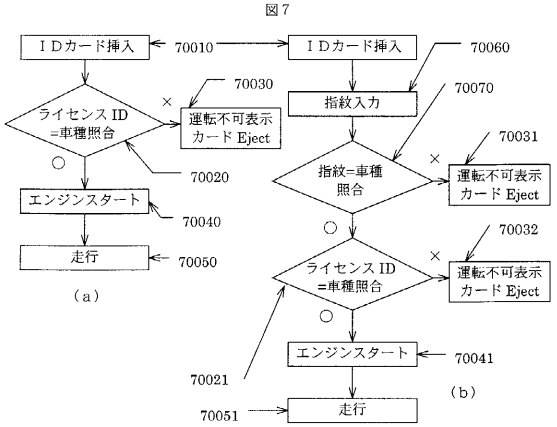
【図６】

図６



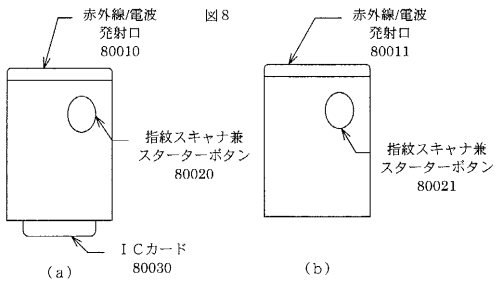
【図７】

図７



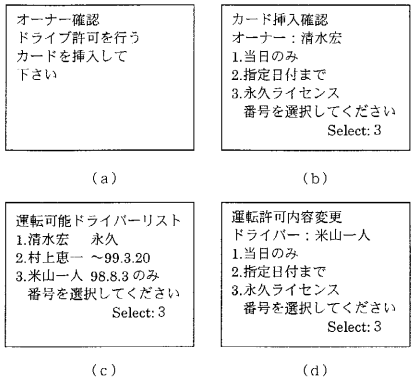
【図８】

図８



【図９】

図9



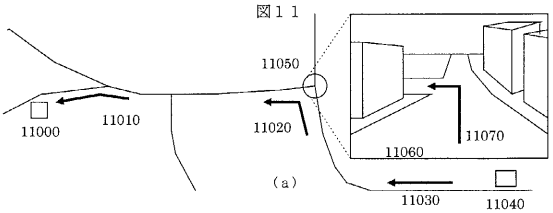
【図１０】

図１０

#	車種	ライセンス管理レベル		
		重要度	資格レベル	生体認証レベル
1	原動機付自転車	C	E	1
2	普通車	B	D	2
3	タクシー等	B	C	2
4	大型車	B	B	3
5	緊急自動車	A	A	4

【図１１】

図１１

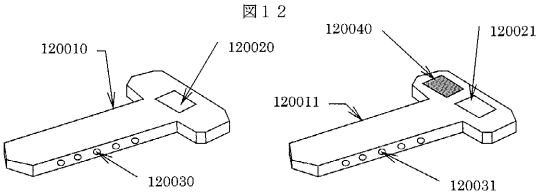


ルート#	終点座標	始点座標	日付	時刻	所要時間	画像ファイル名
1	110.25-540.12	111.32-538.00	H10.7.30	14:00	8分	W0001.GIF
2	111.32-538.00	112.21-535.86	H10.7.30	14:08	7分	W0002.GIF
.....						
8	120.00-532.65	122.37-533.77	H10.8.2	07:59	１２分	W0008.GIF
.....						
22	131.88-525.07	130.02-522.98	H10.8.5	16:45	１５分	W0022.GIF
23	130.02-522.98	129.25-521.45	H10.8.5	17:00	１６分	W0023.GIF

(b)

【図１２】

図１２



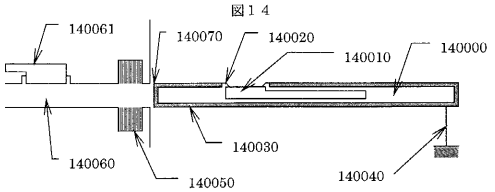
【図１３】

図１３

#	事項	動作モード		
		エンジン始動	ＭＴ	ＡＴ
1	練習生	△	△	△
2	仮免許	○	△	△
3	本免許	○	○	○
4	ＡＴ限定	○	×	○

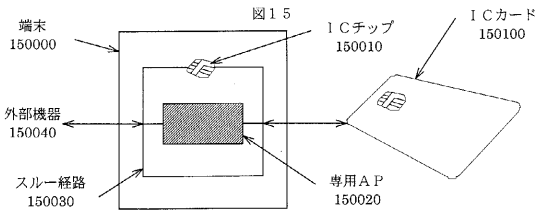
【図１４】

図１４



【図１５】

図１５



【手続補正書】
【提出日】平成22年1月20日(2010.1.20)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ＩＣカードに書き込まれた情報を読み取るＩＣカードリーダと、該ＩＣカードリーダから読み取った後に特定機器の機器操作を不許可にする電子情報と該特定機器を操作する権利を示す情報とに応じて該特定機器の動作可否を制御する特定機器制御手段とを具備した機器操作権管理システムにおいて、
該ＩＣカードリーダで該ＩＣカードから読み取った該ＩＣカードの所有者の生体認証情報を記憶する第１の記憶手段と、
該所有者から生体認証情報を検出するセンサ手段と
を有し、
該センサ手段の検出情報と該第１の記憶手段に記憶された該生体認証情報とを照合して一致した場合、該特定機器の操作権を認めることを特徴とする機器操作権管理システム。
【請求項２】
ＩＣカードに書き込まれた情報を読み取るＩＣカードリーダと、該ＩＣカードリーダから読み取った後に特定機器の機器操作を不許可にする電子情報と該特定機器を操作する権利を示す情報とに応じて該特定機器の動作可否を制御する特定機器制御手段とを具備した機器操作権管理システムにおいて、
該ＩＣカードリーダで該ＩＣカードから読み取った該ＩＣカードの所有者の生体認証情報を記憶する第１の記憶手段と、
該所有者から生体認証情報を検出するセンサ手段と
を有し、
該ＩＣカードが、該ＩＣカードリーダで該ＩＣカードから読み取った情報がネットワークを介して指定された操作権が認められない特定のＩＣカードでない場合であって、該センサ手段の検出情報と該第１の記憶手段に記憶された該生体認証情報とを照合して一致した場合、該特定機器の操作権を認めることを特徴とする機器操作権管理システム。
【請求項３】
請求項１に記載の機器操作権管理システムにおいて、
ネットワークで情報を取得する手段を設け、
前記ＩＣカードが、前記ＩＣカードリーダで前記ＩＣカードから読み取った情報が該ネットワークを介して指定された操作権が認められない特定のＩＣカードである場合には、前記特定機器の操作権を認めない不可表示を行なうことを特徴とする機器操作権管理システム。
【請求項４】
請求項１に記載の機器操作権管理システムにおいて、
ネットワークで情報を取得する手段を設け、
前記センサ手段の検出情報が該ネットワークを介して指定された操作権が認められない情報である場合には、前記特定機器の操作権を認めない不可表示を行なうことを特徴とする機器操作権管理システム。
【請求項５】
ＩＣカードに書き込まれた情報を読み取るＩＣカードリーダと、該ＩＣカードリーダから読み取った後に機器操作を不許可にする電子情報と該機器を操作する権利を示す情報とに応じて機器の動作可否を制御する機器制御手段とを具備した電子機器において、
該ＩＣカードリーダで該ＩＣカードから読み取った該ＩＣカードの所有者の生体認証情

報を記憶する第１の記憶手段と、
該所有者から生体認証情報を検出するセンサ手段と
を有し、
該センサ手段の検出情報と該第１の記憶手段に記憶された該生体認証情報とを照合して一致した場合に、当該電子機器の操作権を認めることを特徴とする電子機器。
【請求項６】
ＩＣカードに書き込まれた情報を読み取るＩＣカードリーダと、該ＩＣカードリーダから読み取った後に機器操作を不許可にする電子情報と該機器を操作する権利を示す情報とに応じて機器の動作可否を制御する機器制御手段とを具備した電子機器において、
該ＩＣカードリーダで該ＩＣカードから読み取った該ＩＣカードの所有者の生体認証情報を記憶する第１の記憶手段と、
該所有者から生体認証情報を検出するセンサ手段と
を有し、
該ＩＣカードが、該ＩＣカードリーダで該ＩＣカードから読み取った情報がネットワークを介して指定された操作権が認められない特定のＩＣカードでない場合であって、該センサ手段の検出情報と該第１の記憶手段に記憶された該生体認証情報とを照合して一致した場合に、当該電子機器の操作権を認めることを特徴とする電子機器。
【請求項７】
請求項５に記載の電子機器において、
ネットワークで情報を取得する手段を設け、
前記ＩＣカードが、前記ＩＣカードリーダで前記ＩＣカードから読み取った情報が該ネットワークを介して指定された操作権が認められない特定のＩＣカードである場合には、当該電子機器の操作権を認めない不可表示を行なうことを特徴とする電子機器。
【請求項８】
請求項５に記載の電子機器において、
ネットワークで情報を取得する手段を設け、
前記センサ手段の検出情報が該ネットワークを介して指定された操作権が認められない情報である場合には、当該電子機器の操作権を認めない不可表示を行なうことを特徴とする電子機器。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
本発明は、機器の操作の可否を管理・制御する機器操作権管理システムにかかわる技術に関し、特に、ライセンスカード形態の機器操作権を表記する機能を有するデバイスと、同デバイスと連携して機器操作者本人であることを生体認証情報を用いて照合する機能などを有する、機器操作権管理システムにかかわる技術に関するものである。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
本発明は上記の点に鑑みなされたもので、その目的とするところは、機器を操作するライセンスとその所有者が同一であることを、確実に認証可能とすることにある。また、本発明の目的とするところは、ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止することにある。
【手続補正５】

【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更
【補正の内容】
【００１４】
（１）ＩＣカードに書き込まれた情報を読み取るＩＣカードリーダと、ＩＣカードリーダから読み取った後に特定機器の機器操作を不許可にする電子情報と特定機器を操作する権利を示す情報とに応じて特定機器の動作可否を制御する特定機器制御手段とを具備しており、ＩＣカードリーダでＩＣカードから読み取ったＩＣカードの所有者の生体認証情報を記憶する第１の記憶手段と、所有者から生体認証情報を検出するセンサ手段とを有し、センサ手段の検出情報と第１の記憶手段に記憶された生体認証情報とを照合して一致した場合、特定機器の操作権を認める。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
（２）ＩＣカードに書き込まれた情報を読み取るＩＣカードリーダと、ＩＣカードリーダから読み取った後に特定機器の機器操作を不許可にする電子情報と特定機器を操作する権利を示す情報とに応じて特定機器の動作可否を制御する特定機器制御手段とを具備しており、ＩＣカードリーダでＩＣカードから読み取ったＩＣカードの所有者の生体認証情報を記憶する第１の記憶手段と、所有者から生体認証情報を検出するセンサ手段とを有し、ＩＣカードが、ＩＣカードリーダでＩＣカードから読み取った情報がネットワークを介して指定された操作権が認められない特定のＩＣカードでない場合であって、センサ手段の検出情報と第１の記憶手段に記憶された生体認証情報とを照合して一致した場合、特定機器の操作権を認める。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
（３）上記（１）において、ネットワークで情報を取得する手段を設け、ＩＣカードが、ＩＣカードリーダでＩＣカードから読み取った情報がネットワークを介して指定された操作権が認められない特定のＩＣカードである場合には、特定機器の操作権を認めない不可表示を行なう。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
（４）上記（１）において、ネットワークで情報を取得する手段を設け、センサ手段の検出情報がネットワークを介して指定された操作権が認められない情報である場合には、特定機器の操作権を認めない不可表示を行なう。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更

【補正の内容】
【００１８】
本発明によれば、機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うことが出来る。また、ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止し、簡単な読み出しを可能となる。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】変更
【補正の内容】
【００４６】
まず、操作する機器にＩＣカードを挿入し（ステップ60010 ）、次に指紋の入力を行う（ステップ60020 ）。次に、ステップ60030 にて、挿入したＩＣカードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者がＩＣカードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、ＩＣカードのEject を行う（ステップ60040 ）。照合結果が○であれば、エンジンスタートを行い（ステップ60050 ）、操縦する機器が自動車であれば、走行を行う（ステップ60060 ）。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】変更
【補正の内容】
【００４７】
ここで、例えばＩＣカードは前記した如く、メモリを持つＩＣチップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号等をイメージスキャナで読み取り、図１、図２で示した機器に搭載されている記憶装置から、該当免許証番号に対応した指紋情報を読み出して、操縦者が入力した指紋との一致判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００４９
【補正方法】変更
【補正の内容】
【００４９】
図７の（ａ）は、ＩＣカードと操縦する機器の種類の照合を行う場合のフローチャートである。まず、操縦者は機器にＩＣカードを挿入し（ステップ70010 ）、操縦する機器は挿入されたＩＣカードからライセンスＩＤを読取る。そして、該当ライセンスＩＤが、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70020 ）、操縦が出来ない場合は運転不可表示を行い、且つＩＣカードのEject を行う（ステップ70030 ）。照合結果が○であれば、エンジンスタートを行い（ステップ70040 ）、操縦する機器が自動車であれば、走行を行う（ステップ70050 ）。
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００５０
【補正方法】変更
【補正の内容】
【００５０】
ここで、例えばＩＣカードは前記した如く、メモリを持つＩＣチップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号及び記載されている

操縦可能機器の種類をイメージスキャナで読み取り、本機器を操縦できるライセンスかどうかの判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００５１
【補正方法】変更
【補正の内容】
【００５１】
図７の（ｂ）は、図６と図７の（ａ）の両方の機能を実現した例を示すフローチャートである。すなわち、操縦者は機器にＩＣカードを挿入し（ステップ70010 ）、次に指紋の入力を行う（ステップ70060 ）。次に、ステップ70070 にて、挿入したＩＣカードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者がＩＣカードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、ＩＣカードのEject を行う（ステップ70031 ）。照合結果が○であれば、挿入されたＩＣカードから読み取ったライセンスＩＤが、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70021 ）、操縦が出来ない場合は運転不可表示を行い、且つＩＣカードのEject を行う（ステップ70032 ）。照合結果が○であれば、エンジンスタートを行い（ステップ70041 ）、操縦する機器が自動車であれば、走行を行う（ステップ70051 ）。

【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００６０
【補正方法】変更
【補正の内容】
【００６０】
まず、図９の（ａ）の操作画面で示すように、自動車は他人への運転許可を与える人が、確かにその車のオーナーかどうかの判定をするために、オーナーにＩＣカードの挿入を促す。ここで、図示しない指紋等の生体認証情報の照合により、オーナー本人であることを確認する。

【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００６１
【補正方法】変更
【補正の内容】
【００６１】
次に、図９の（ｂ）に示す操作画面で、他人に与える運転許可モードを選択する。すなわち、「１」を選択することで当日のみ、「２」を選択することで指定日付を指定する。そして、「３」を選択することで、例えば家族などの永久ライセンスを与える。この選択の後、図９の（ａ）と同様な操作画面にて、運転許可を与えるドライバーのＩＣカードの挿入を促し、運転許可の登録を行う。

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	Ｂ４２Ｄ 15/10 ５２１	

(72)発明者 松本 健司
神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考) 2C005 MA01 MB01 NB01 SA13 SA15 TA11
5B035 AA13 BB09 BC01 BC02 BC03 CA22
5B058 CA27 KA02 KA38 YA13
5B072 BB05 CC21 DD01