(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6775702号
(P6775702)
(45)発行日　令和2年10月28日(2020.10.28)　(24)登録日　令和2年10月8日(2020.10.8)

(51)Int.Cl.		F I		
G07C 5/00	(2006.01)	G07C	5/00	Z
G06F 21/60	(2013.01)	G06F	21/60	340
G08G 1/00	(2006.01)	G08G	1/00	D

請求項の数 2　(全 17 頁)

(21)出願番号　特願2020-90364(P2020-90364)
(22)出願日　令和2年5月25日(2020.5.25)
(62)分割の表示　特願2015-224322(P2015-224322)の分割
原出願日　平成27年11月16日(2015.11.16)
(65)公開番号　特開2020-149713(P2020-149713A)
(43)公開日　令和2年9月17日(2020.9.17)
審査請求日　令和2年6月1日(2020.6.1)

早期審査対象出願

(73)特許権者　000237592
株式会社デンソーテン
兵庫県神戸市兵庫区御所通１丁目２番２８号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　古石　朋久
兵庫県神戸市兵庫区御所通１丁目２番２８号　株式会社デンソーテン内

審査官　毛利　太郎

最終頁に続く

(54)【発明の名称】記憶装置および走行映像アクセス方法

(57)【特許請求の範囲】
【請求項１】
車両の外部を撮像する撮像部と、
前記撮像部によって撮像され、記憶媒体へ記憶される前記車両の走行映像に対し、認証により前記記憶媒体へ記憶される前記車両の走行映像へのアクセスを制限するアクセス制限を設定するアクセス制御部と、
を備え、
前記アクセス制御部は、
前記車両に関して生じたイベントが少なくとも緊急性の高さを示す所定の条件を満たす場合に、前記アクセス制限を解除すること
を特徴とする記憶装置。
【請求項２】
車両の外部を撮像する撮像部によって撮像され、記憶媒体へ記憶される走行映像へのアクセスを制限する走行映像アクセス方法において、
アクセス制御部が、認証により前記記憶媒体に記憶される前記車両の走行映像へのアクセスを制限するアクセス制限を設定するアクセス制御ステップと、
前記アクセス制御部が、車両に関して生じたイベントが少なくとも緊急性の高さを示す所定の条件を満たす場合に、前記アクセス制限を解除するアクセス制限解除ステップと
を含むことを特徴とする走行映像アクセス方法。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、記憶装置および走行映像アクセス方法に関する。
【背景技術】
【０００２】
従来、車両に搭載され、車両の外部を撮像した走行映像を走行情報として記録するドライブレコーダが知られている。かかるドライブレコーダで記録された走行情報は、例えば、車両が衝突事故を起こした場合などに、事故当時の状況を客観的に示す情報として利用される。
【０００３】
また、ドライブレコーダでは、記録した走行情報に対して搭乗者ごとの認証コードを設定することで、走行情報が他者に不正に読み出されるのを防止する個人情報保護のための技術が提案されている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１５－０９０５１９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述した従来技術では、記憶した走行情報へのアクセス権を搭乗者ごとに設定しているため、例えば、衝突事故などの緊急性の高い走行映像を搭乗者以外が閲覧できないおそれがあった。
【０００６】
本発明は、上記に鑑みてなされたものであって、個人情報を保護しつつ、緊急性の高い走行映像は搭乗者以外でも閲覧することができる記憶装置および走行映像アクセス方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
上述した課題を解決し、目的を達成するために、本発明に係る記憶装置は、撮像部と、アクセス制御部とを備える。前記撮像部は、車両の外部を撮像する。前記アクセス制御部は、前記撮像部によって撮像され、記憶媒体へ記憶される前記車両の走行映像に対し、認証により前記記憶媒体へ記憶される前記車両の走行映像へのアクセスを制限するアクセス制限を設定する。前記アクセス制御部は、前記車両に関して生じたイベントが少なくとも緊急性の高さを示す所定の条件を満たす場合に、前記アクセス制限を解除する。
【発明の効果】
【０００８】
本発明によれば、個人情報を保護しつつ、緊急性の高い走行映像は搭乗者以外でも閲覧することができる。
【図面の簡単な説明】
【０００９】
【図１】図１は、実施形態に係るドライブレコーダの記録方法の概要を示す図である。
【図２】図２は、実施形態に係る表示システムの概要を示す図である。
【図３】図３は、実施形態に係る表示システムの構成を示すブロック図である。
【図４】図４は、識別情報を示す図である。
【図５】図５は、アクセス制限設定の処理を説明する図である。
【図６】図６は、走行情報を示す図である。
【図７】図７は、イベント情報を示す図である。
【図８Ａ】図８Ａは、管理者権限を説明する図（その１）である。
【図８Ｂ】図８Ｂは、管理者権限を説明する図（その２）である。

【図８Ｃ】図８Ｃは、管理者権限を説明する図（その３）である。
【図９】図９は、実施形態に係るドライブレコーダが実行する記録処理の処理手順を示すフローチャートである。
【図１０】図１０は、ドライブレコーダの機能を実現するコンピュータの一例を示すハードウェア構成図である。
【発明を実施するための形態】
【００１０】
以下、添付図面を参照して、本願の開示するドライブレコーダ、表示システム、ドライブレコーダの記録方法およびプログラムの実施形態を詳細に説明する。なお、以下に示す実施形態によりこの発明が限定されるものではない。
【００１１】
＜ドライブレコーダの記録方法の概要＞
図１は、実施形態に係るドライブレコーダの記録方法の概要を示す図である。実施形態に係るドライブレコーダの記録方法は、例えば、車両１１に搭載されるドライブレコーダ１によって実行される。
【００１２】
なお、図１には、搭乗者Ａが車両１１に搭乗する場合について示している。搭乗者Ａは、例えば、車両１１の運転者であるが、運転者に限定されず、車両１１の助手席や後部座席に着座する搭乗者であってもよい。
【００１３】
実施形態に係るドライブレコーダ１の記録方法では、車両１１の外部を撮像した走行映像に対し、車両１１の搭乗者Ａにアクセス権を付与する一方で、搭乗者Ａ以外のアクセスを制限するアクセス制限を設定する。また、車両１１の衝突事故など所定のイベントが生じた場合には、かかるアクセス制限を解除する。
【００１４】
具体的には、図１に示すように、ドライブレコーダ１はまず、ドライブレコーダ１自体や車両１１などに設けられた撮像部（図示せず）によって車両１１の外部を所定のフレームレート（単位時間あたりの処理フレーム数）で撮像する。撮像部によって撮像された、例えば、走行映像Ｖ１は、搭乗者Ａ以外からのアクセスを制限するアクセス制限が設定され、走行情報Ｆ１として記憶媒体に記録される。
【００１５】
走行情報Ｆ１は、搭乗者Ａを識別する識別情報を含む情報である。識別情報には、例えば、搭乗者Ａを識別するＩＤ、走行情報Ｆ１へのアクセスを許可するためのパスワード（図１の例では、「１２３４」）、管理者権限を有する管理者に関する情報などが含まれる。
【００１６】
つまり、ドライブレコーダ１は、走行映像Ｖ１へ、パスワードを付与することで搭乗者Ａ以外からのアクセスを制限する走行情報Ｆ１を記録する。これにより、搭乗者Ａが車両１１へ搭乗した際の走行映像Ｖ１を、搭乗者Ａのパスワードを知らない他者（図１の例では、閲覧者Ｂ）が閲覧できないため、搭乗者Ａの個人情報が保護される。
【００１７】
なお、アクセスの制限は、パスワードに限定されず、例えば搭乗者Ａの指紋情報を識別情報に含ませることで、搭乗者Ａから受け付けた指紋と指紋情報とを照合する指紋認証を用いてもよい。
【００１８】
一方、車両１１が、例えば、他車両と衝突事故を起こした場合、かかる衝突事故の走行映像Ｖ２に対して搭乗者Ａ以外からのアクセスを制限するアクセス制限が設定されると、警察や保険会社などの閲覧者Ｂは、衝突事故の状況が撮像された走行映像Ｖ２を閲覧できず、事故原因を正確に解析できないおそれがある。
【００１９】

そこで、実施形態に係るドライブレコーダ１の記録方法では、車両１１に関して生じたイベントが少なくとも緊急性の高さを示す所定の条件を満たす場合に、かかる搭乗者Ａ以外からのアクセス制限を解除した走行情報Ｆ２を記録することとした。

【００２０】

これにより、実施形態に係るドライブレコーダ１の記録方法によれば、例えば、緊急性の低い走行映像については搭乗者Ａの個人情報を保護しつつ、緊急性の高い走行映像については搭乗者Ａ以外でも閲覧することができるようになる。つまり、警察や保険会社などの閲覧者Ｂは、走行情報Ｆ２に記録された衝突事故の走行映像Ｖ２を閲覧できるため、事故原因を正確に解析することができる。

【００２１】

＜表示システムの概要＞

次に、図１を用いて説明したドライブレコーダ１を含む表示システム１００について図２を参照して説明する。図２は、実施形態に係る表示システム１００の概要を示す図である。図２に示すように、実施形態に係る表示システム１００は、携帯装置Ｐ１～Ｐｎと、ドライブレコーダ１と、表示装置１０とを備える。なお、以下では、携帯装置Ｐ１～Ｐｎを総称する場合、携帯装置Ｐと記載する。

【００２２】

携帯装置Ｐは、例えば、車両１１の搭乗者が所有する携帯電話やスマートフォンなどの可搬性の電子機器である。なお、携帯装置Ｐは、携帯電話やスマートフォンに限定されず、搭乗者を識別できればよく、例えば、車両１１のドアの開錠やエンジン始動を制御する電子キーなどであってもよい。

【００２３】

携帯装置Ｐは、ドライブレコーダ１と、通信可能に接続される。例えば携帯装置Ｐとドライブレコーダ１とは、無線で通信を行い、互いに識別情報、認証要求および認証結果などの送受信を行う。無線通信は、例えば、デジタル機器用の近距離無線通信規格であるＢｌｕｅｔｏｏｔｈ（登録商標）やＷｉＦｉ（登録商標）などが利用される。

【００２４】

ドライブレコーダ１は、撮像部（図示せず）を備え、かかる撮像部によって車両１１の外部を撮像できる箇所、例えば、撮像部の撮像方向が車両１１の前方を向くように、フロントガラスの車室内側の面に設けられる。

【００２５】

なお、ドライブレコーダ１は、フロントガラス以外にも、車両１１のリアガラスや車室内の天井、ダッシュボード上等、車両１１の外部を撮像できる箇所であれば任意の箇所に設置することができる。また、ドライブレコーダ１から撮像部が分離されており、かかる撮像部を撮像方向に応じて車両１１の任意の箇所に設置する構成としてもよい。

【００２６】

また、ドライブレコーダ１には、可搬型の記憶媒体Ｍ（例えば、ＳＤカードなど）が着脱可能である。記憶媒体Ｍには、アクセス制限が設定された走行映像を含む走行情報が記録される。

【００２７】

なお、記憶媒体Ｍは、可搬型の記憶媒体に限定されず、例えば、ドライブレコーダ１に内蔵されるＨＤＤ（Hard Disk Drive）であってもよく、あるいは、クラウドコンピューティングにおけるサーバ装置であってもよい。

【００２８】

表示装置１０は、例えば、ディスプレイを含み、かかるディスプレイへ記憶媒体Ｍに記録された走行映像を表示させる。また、表示装置１０は、走行情報に設定されたパスワードなどを入力するための入力部（図示せず）を備える。なお、表示装置１０は、携帯装置Ｐが表示装置１０の機能を兼用してもよい。

【００２９】

＜表示システムのブロック図＞

かかる表示システム１００の構成について、さらに具体的に図３を用いて説明する。図３は、実施形態に係る表示システム１００の構成を示すブロック図である。

【００３０】

＜携帯装置Ｐ＞

携帯装置Ｐは、搭乗者Ａを識別する識別情報をドライブレコーダ１へ送信することで、搭乗者Ａを認証対象者として登録するための初期設定を行う。かかる初期設定において、搭乗者Ａは、識別情報であるＩＤおよびパスワードとして、例えば、搭乗者Ａを識別可能な任意の文字列をそれぞれ設定する。

【００３１】

また、携帯装置Ｐは、初期設定が完了した搭乗者Ａが車両１１に搭乗すると、搭乗者Ａを個人認証する認証要求をドライブレコーダ１へ送信する。認証要求は、例えば、初期設定で登録したＩＤおよびパスワードを送信することによって認証を要求する。携帯装置Ｐは、ドライブレコーダ１が、送信した搭乗者ＡのＩＤおよびパスワードを認証した場合、かかる認証結果をドライブレコーダ１から受信する。

【００３２】

＜車両１１＞

車両１１は、ドライブレコーダ１と、車両センサ３とを備える。まず、車両センサ３について説明する。車両センサ３は、車両１１の走行に関する状態を検知するセンサである。

【００３３】

車両センサ３は、例えば、車両１１の加速度を検出する加速度センサ、電波を放射するミリ波レーダーなどによって車両１１と他車両との距離を検出するセンサ、車両１１の盗難などを検知する防犯センサなどである。車両センサ３は、車両１１の状態を示す検出結果をドライブレコーダ１へ出力する。

【００３４】

＜ドライブレコーダ１＞

ドライブレコーダ１は、撮像部２と、制御部４と、記憶部５とを備える。制御部４は、認証部４ａと、アクセス制御部４ｂとを備える。

【００３５】

撮像部２は、例えば、ＣＣＤ（Charge Coupled Device）やＣＭＯＳ（Complementary Metal Oxide Semiconductor）などの撮像素子を備える。撮像部２は、かかる撮像素子によって車両１１の外部を所定のフレームレート（例えば、３０ｆｐｓ）で撮像した撮像画像を走行映像として制御部４へ出力する。

【００３６】

制御部４は、例えば、ＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）およびＲＯＭ（Read Only Memory）を備えるマイクロコンピュータである。かかるＣＰＵは、たとえば、ＲＯＭに予め記憶されたプログラムに従い、演算処理を行うことで、上述した認証部４ａ、アクセス制御部４ｂとして機能する。

【００３７】

＜認証部４ａ＞

認証部４ａは、初期設定において携帯装置Ｐから送信される、搭乗者Ａを識別するＩＤおよびパスワードを含む識別情報５ａを記憶部５へ記憶する。また、認証部４ａは、搭乗者Ａが車両１１に搭乗した際に、携帯装置Ｐから認証要求を受信し、搭乗者Ａを識別するＩＤおよびパスワードに基づいて搭乗者Ａの個人認証を行う。

【００３８】

具体的には、認証部４ａは、携帯装置Ｐから送信されるＩＤおよびパスワードと、記憶部５に記憶される識別情報５ａのＩＤおよびパスワードとが一致するか否かを判定する。認証部４ａは、双方のＩＤおよびパスワードが一致する場合、搭乗者Ａを認証し、認証した旨を示す認証結果を携帯装置Ｐへ送信する。

【００３９】

ここで、図４を参照して、認証部４ａによって記憶される識別情報５ａについて説明する。図４は、識別情報５ａを示す図である。なお、図４に示す識別情報５ａは一例であり、これに限定されない。

【００４０】

図４に示すように、識別情報５ａは、「ＩＤ」、「パスワード」、「管理者フラグ」および「準管理者フラグ」といった項目を含む情報である。「ＩＤ」は、車両１１に搭乗する搭乗者を識別する情報であり、例えば、ユーザ名などである。「パスワード」は、アクセスを許可するためのパスワードであり、例えば、任意の４つの数字からなる。

【００４１】

「管理者フラグ」および「準管理者フラグ」は、走行情報に対する処理について特権的機能を実行可能な管理者およびこれに準ずる準管理者であるかを、「０」か「１」かの２値で示す情報である。つまり、認証対象者が管理者または準管理者として登録される場合、「管理者フラグ」または「準管理者フラグ」はそれぞれ「１」となる。なお、管理者および準管理者については、図８を参照して後述する。

【００４２】

図４に示すように、識別情報５ａには、複数の認証者を登録することができ、例えば、識別情報５ａは、車両１１がレンタカーや社用車などである場合に、１台の車両１１を複数の認証者で共有可能であることを示している。すなわち、各認証者は、それぞれ異なるパスワードを設定することで、本人以外からのアクセスを制限する。

【００４３】

図３に戻り、認証部４ａの説明を続ける。認証部４ａは、搭乗者Ａを認証すると、認証結果を携帯装置Ｐへ送信するとともに、識別情報５ａに含まれる搭乗者Ａに関する情報をアクセス制御部４ｂへ出力する。

【００４４】

＜アクセス制御部４ｂ＞

アクセス制御部４ｂは、認証部４ａから取得した搭乗者Ａに関する情報に基づき、撮像部２から入力される走行映像に対して、搭乗者Ａにアクセス権を付与するとともに、搭乗者Ａ以外からのアクセスを制限するアクセス制限を設定する。具体的には、アクセス制御部４ｂは、走行映像に対して、認証部４ａから取得した搭乗者Ａのパスワードを付与することでアクセス制限を設定する。また、アクセス制御部４ｂは、走行映像に対するパスワードを解除もしくは付与しないようにすることで、走行映像へのアクセス制限を解除する。

【００４５】

ここで、図５を参照して、アクセス制限設定の処理について説明する。図５は、アクセス制限設定の処理を説明する図である。図５に示すように、実施形態に係るドライブレコーダ１は、例えば、撮像部２から入力される撮像画像Ｇを順次記録していく常時録画方式を用いている。

【００４６】

かかる方式では、アクセス制御部４ｂは、撮像部２から順次入力される各撮像画像に対してアクセス制限を設定していく。具体的には、アクセス制御部４ｂは、搭乗者Ａが認証されている時刻ｔ１において撮像画像Ｇ１が撮像されると、撮像画像Ｇ１に対して搭乗者ＡのＩＤに対応するパスワード（例えば、１２３４）を付与する。

【００４７】

なお、アクセス制御部４ｂは、搭乗者Ａが車両１１を降車する、つまり、搭乗者Ａの携帯装置Ｐと、ドライブレコーダ１との通信が途絶えると、搭乗者Ａの認証を解除し、かかる認証解除以降の撮像画像に対しては、搭乗者ＡのＩＤに対応するパスワードを付与しない。

【００４８】

そして、アクセス制御部４ｂは、搭乗者ＡのＩＤに対応するパスワードが付与された各撮像画像を、例えば搭乗者Ａに関する走行情報を格納するためのフォルダＦＡへ格納する

。つまり、フォルダＦＡに格納される走行映像を閲覧するためには、搭乗者ＡのＩＤに対応するパスワードが必要となる。

【００４９】

また、アクセス制御部４ｂは、搭乗者Ｂが認証されている時刻ｔ１０において撮像画像Ｇ１０が撮像されると、撮像画像Ｇ１０に対して搭乗者ＢのＩＤに対応するパスワード（例えば、５６７８）を付与する。

【００５０】

アクセス制御部４ｂは、搭乗者ＢのＩＤに対応するパスワードが付与された各撮像画像を、例えば搭乗者Ｂに関する走行情報を格納するためのフォルダＦＢへ格納する。つまり、フォルダＦＢに格納される走行映像を閲覧するためには、搭乗者ＢのＩＤに対応するパスワードが必要となる。

【００５１】

これにより、搭乗者Ａおよび搭乗者Ｂが車両１１を共有する場合、それぞれの走行映像に対して、各搭乗者に対応するパスワードを設定することで、本人以外から無断でアクセスされるのを制限することができる。

【００５２】

また、アクセス制御部４ｂは、例えば、時刻ｔ３０において車両１１を運転する搭乗者Ｂが衝突事故を起こした場合、時刻ｔ３０に撮像された撮像画像Ｇ３０を含む所定期間の走行映像に対し、搭乗者Ｂ以外からのアクセスを制限するアクセス制限を解除する。

【００５３】

具体的には、アクセス制御部４ｂは、時刻ｔ２０から時刻ｔ３０までの過去の期間の各撮像画像に対しては、付与されていたパスワードを解除する。また、アクセス制御部４ｂは、時刻ｔ３０から時刻ｔ４０までの先の期間の各撮像画像に対しては、パスワードを付与しないようにする。

【００５４】

これにより、認証者である搭乗者Ｂ以外の者（例えば、認証されていない搭乗者Ａや閲覧者Ｃ）が時刻ｔ３０における衝突事故の前後の期間の走行映像を閲覧することができる。

【００５５】

また、アクセス制御部４ｂは、パスワードが設定されない各撮像画像を例えばフォルダＦへ格納する。つまり、フォルダＦに格納される走行映像を閲覧するためのパスワードが必要なくなるため、誰でも閲覧することができる。

【００５６】

次に、記憶部５に記憶される走行情報５ｂについて図６を参照して説明する。図６は、走行情報５ｂを示す図である。なお、図６に示す走行情報５ｂは一例であり、これに限定されない。

【００５７】

図６に示すように、走行情報５ｂは、「画像Ｎｏ」、「時刻」、「認証ＩＤ」、「ＰＷフラグ」および「パスワード」といった項目を含む情報である。「画像Ｎｏ」は、撮像された撮像画像の識別ＩＤであり、例えば撮像画像それぞれに付与されたナンバリング情報である。「時刻」は、撮像画像が撮像された時刻である。「認証ＩＤ」は、対応する時刻において認証されていた搭乗者のＩＤである。

【００５８】

「ＰＷフラグ」は、撮像画像に対してパスワードを付与するか否かを、「０」か「１」かの２値で示す情報である。「ＰＷフラグ」には、車両１１に関して生じたイベントが少なくとも緊急性の高さを示す所定の条件を満たす場合には、パスワードを付与しないことを示す「１」が格納され、それ以外の場合には、「０」が格納される。「パスワード」は、認証ＩＤの搭乗者に対応するパスワードである。

【００５９】

例えば、時刻ｔ３０において衝突事故を起こした場合、時刻ｔ２０から時刻ｔ４０まで

のＰＷフラグを「１」とすることで、対応する「画像Ｎｏ」の撮像画像に対してはパスワードが付与されない。

【００６０】

また、アクセス制御部４ｂは、パスワードを付与するか否かを決定するにあたり、車両１１に関して緊急性が高いイベントが生じたか否かを判定する。具体的には、アクセス制御部４ｂは、車両センサ３から入力される検出結果に基づいて、緊急性が高いイベントを含むイベント情報５ｃのうち、いずれのイベントが生じたかを判定する。

【００６１】

ここで、イベント情報５ｃについて図７を参照して説明する。図７は、イベント情報５ｃを示す図である。図７に示すイベント情報５ｃは、記憶部５に予め記憶される。なお、図７に示すイベント情報５ｃは一例であり、これに限定されるものではない。イベント情報５ｃは、車両１１に生じることが想定される各種のイベントそれぞれに関する設定等の情報を表すものである。車両１１に生じることが想定されるイベントには、緊急性が高いイベントと、緊急性が低いイベントとが含まれる。

【００６２】

図７に示すように、イベント情報には、「イベント」、「記録開始」、「ＰＷ有無」、「上書き防止」および「その他」といった項目を含む。「イベント」は、車両１１の周辺で起こりうるイベントのパターンを示す。

【００６３】

「記録開始」は、走行情報５ｂの記録を開始する方法を示し、「自動」と「手動」に分類される。「自動」は、認証者の意思とは無関係に走行情報５ｂを記録することを示す。「手動」は、認証者から所定の操作を受け付けた場合に、走行情報５ｂを記録することを示す。

【００６４】

「ＰＷ有無」は、記録する走行情報５ｂに対してパスワードを付与するか否かを示す。「ＰＷ有無」が「無」となるイベントの場合は走行情報５ｂに対するパスワードを解除することを表している。通常、緊急性が高いイベントに関しては「ＰＷ有無」が「無」となる。また、「ＰＷ有無」が「選択」となる特定イベントの場合は、走行情報５ｂへパスワードを付与するか解除するかを選択する搭乗者からの操作を受け付け、該操作に応じてパスワードの付与及び解除（アクセス制限の設定及び解除）が切り替えられる。「上書き防止」は、記録した走行情報５ｂのデータ量過多により、記憶部５の記録容量が不足した場合に、新しい走行情報５ｂを記録するための上書きの可否、すなわち古い走行情報５ｂを削除するか否かを示す。「その他」は、その他の付帯情報を示す。

【００６５】

実施形態に係るドライブレコーダ１では、通常時には、撮像された走行映像をすべて記録する常時録画方式が用いられる。つまり、アクセス制御部４ｂは、図７に示す「常時録画」を通常パターンとし、「常時録画」では「ＰＷ有無」を「有」、すなわち、記録する走行情報５ｂに対してパスワードを付与する。

【００６６】

また、アクセス制御部４ｂは、「常時録画」の場合に、「上書き防止」の「無」に従って、記録する走行情報５ｂに対して古い走行情報５ｂを新しい走行情報５ｂに書き換えられるようにする。これにより、ドライブレコーダ１は、記憶部５の記録容量を無駄なく使用することができる。

【００６７】

次に、イベントが「事故衝撃」である場合を例に説明する。アクセス制御部４ｂは、例えば、車両１１が他車両と衝突し、車両センサ３である加速度センサが所定の閾値以上の加速度を検出した場合、イベントとして「事故衝撃」が生じたと判定する。

【００６８】

そして、かかる場合、アクセス制御部４ｂは、イベント情報５ｃのうちの「事故衝撃」に対応する情報、例えば「ＰＷ有無」の「無」に従って、記録する走行情報５ｂに対する

パスワードを解除する。また、アクセス制御部４ｂは、例えば「上書き防止」の「有」に従って、記録する走行情報５ｂが書き換えられるのを防止する。

【００６９】

これにより、実施形態に係るドライブレコーダ１では、衝突事故などを起こした場合に、警察や保険会社などの閲覧者が衝突事故の映った走行情報５ｂを閲覧することが可能となるので、かかる事故原因を正確に解析することができる。

【００７０】

なお、イベントが「急ブレーキ」である場合の判定条件は、例えば、加速度センサによって検出される前方方向への加速度が所定の閾値以上、かつ、「事故衝突」と判定される加速度の閾値以下の場合である。

【００７１】

また、イベントが「防犯（不審者接近）」や「防犯（車体衝撃）」である場合の判定条件は、例えば、車両センサ３が車両１１に接近する不審者を検出した場合や、かかる不審者が車両１１の盗難を試みようと窓ガラスを割るのを検知した場合である。

【００７２】

また、イベントが「自動ブレーキ作動時」である場合の判定条件は、例えば、車両センサ３が、車両１１と前方車両との車間距離が所定距離以下であることを検出し、車両１１へ別途搭載されている車載装置が自動でブレーキを制御した場合である。また、イベントが「車線逸脱時」である場合の判定条件は、例えば、車両センサ３が車両１１の車線逸脱を検知した場合である。

【００７３】

また、イベントが「車両スタック時」である場合の判定条件は、例えば、車両１１が雪道でスタックした場合に、エンジンが高回転しているにも関わらず、加速度が検出されない場合である。

【００７４】

次に、「記録開始」が「手動」の場合について、イベントが「ドライブ風景」である場合を例に説明する。アクセス制御部４ｂは、例えば、認証者である搭乗者が、ドライブ中の風景を記録し保存しておきたい場合に、これに応じた所定操作をドライブレコーダ１に設けられたスイッチなどを介して行ったならば、かかる操作を「ドライブ風景」のイベントとして受け付ける。

【００７５】

そして、アクセス制御部４ｂは、「ドライブ風景」に対応する情報、例えば「ＰＷ有無」の「選択」に従って、搭乗者に対してドライブ風景の走行映像へパスワードを付与するか解除するかを選択させる。そして、アクセス制御部４ｂは、搭乗者の選択操作に応じてパスワードの付与および解除を切り替える。また、「上書き防止」の「有」に従って、ドライブ風景の走行映像へ削除不可のアクセス制限を設定する。

【００７６】

これにより、実施形態に係るドライブレコーダ１では、搭乗者が、走行映像へ任意のアクセス制限を設定することができ、例えば、ドライブ風景の走行映像へパスワード無しで他の閲覧者が閲覧可能としたり、誤って上書きされて消されるのを防止したりすることができる。

【００７７】

なお、「記録開始」が「手動」の場合のイベントとしては、例えば他に、「他者危険運転」や「他者交通違反」、「他者事故」の場合などがある。これらは、自車である車両１１へ危険が及ばない、すなわち緊急性は高くないものの、後に他の閲覧者が閲覧可能となるように走行映像へアクセス制限を設定するかを、搭乗者へ任意に設定可能とするものである。すなわち、搭乗者は、自分の視認した状況に応じ、現況の走行映像へパスワードを設定するか、あるいは、上書きを防止するかといったアクセス制限の設定を任意に行うことができる。

【００７８】

次に、「記録開始」が「自動」および「手動」である場合について、イベントが「他車急接近」である場合を例に説明する。アクセス制御部４ｂは、車両１１と車両１１に接近する他車両との距離が所定距離以下になったことを車両センサ３が検知した場合は、「記録開始」を「自動」で行う。つまり、ドライブレコーダ１は、車両センサ３が検知したイベントをトリガにして記録を開始する。

【００７９】

そして、アクセス制御部４ｂは、「記録開始」が「自動」の場合には、「ＰＷ有無」を「無」で、すなわち、記録される走行情報５ｂに対するパスワードを解除する。

【００８０】

また、アクセス制御部４ｂは、車両１１に搭乗する搭乗者が、車両１１に接近する他車両を危険と判断し、ドライブレコーダ１への所定の手動操作を行った場合には、「記録開始」を「手動」で行う。

【００８１】

そして、アクセス制御部４ｂは、「記録開始」が「手動」の場合には、「ＰＷ有無」を「選択」で、すなわち、搭乗者に対して走行映像へパスワードを付与するか解除するかを選択させる。

【００８２】

なお、アクセス制御部４ｂは、例えば、別途車両１１へ搭載され、車両１１へ接近する対象物を検知する検知装置の検知結果に応じて、接近物が、他車両や歩行者、飛来物などの移動体であるか、道路上の落下物などの物体であるかなどを判定することができる。そして、かかる判定結果に応じて、アクセス制御部４ｂは、「他車急接近」や「歩行者急接近」、「落下物／飛来物」といったイベントの判定を行うこととなる。

【００８３】

ところで、アクセス制御部４ｂは、例えば、車両１１がレンタカーや社用車である場合、認証者のみがアクセス可能なアクセス制限を設定すると、車両１１を保有する会社側で走行情報５ｂを管理するのが困難になるおそれがある。

【００８４】

そこで、アクセス制御部４ｂは、認証者が管理者である場合、走行映像のすべてに対する管理者権限に応じたアクセス権を認証者（管理者）に付与する。管理者権限とは、かかる走行映像に対して特権的機能を実行可能な権限である。

【００８５】

ここで、アクセス制御部４ｂが管理者に付与する管理者権限について図８Ａ～図８Ｃを参照して説明する。図８Ａ～図８Ｃは、管理者権限を説明する図（その１）～（その３）である。

【００８６】

なお、図８Ａ～図８Ｃに示す管理者権限は一例であり、これに限定されるものではない。また、図８Ａ～図８Ｃに示す認証者Ａ、Ｂは、例えば、図５における搭乗者Ａ、Ｂであり、認証者Ｃは、例えば図５における閲覧者Ｃである。

【００８７】

また、図８Ａ～図８Ｃの説明の前提として、図４に示した識別情報５ａの認証者Ａが、管理者であり、認証者Ｂが準管理者であり、認証者Ｃは、いずれにも該当しないこととする。なお、準管理者は、例えば、管理者である認証者Ａより下位、かつ、認証者Ｃより上位の管理者権限を有する。

【００８８】

図８Ａに示すように、アクセス制御部４ｂは、例えば管理者である認証者Ａに対しては、認証者Ａ、認証者Ｂおよび認証者Ｃいずれの走行情報５ｂも閲覧可能なアクセス権を付与する。また、アクセス制御部４ｂは、準管理者である認証者Ｂに対しては、認証者Ｂおよび認証者Ｃの走行情報５ｂが閲覧可能なアクセス権を付与する。

【００８９】

また、図８Ｂに示すように、アクセス制御部４ｂは、管理者である認証者Ａに対しては

、認証者Ａ、認証者Ｂおよび認証者Ｃいずれの走行情報５ｂも削除可能なアクセス権を付与する。なお、走行映像を削除する権限は、不正な情報操作を防止する観点から、管理者のみに対して付与されることが好ましい。

【００９０】

また、図８Ｃに示すように、アクセス制御部４ｂは、管理者である認証者Ａに対しては、認証者Ａ、認証者Ｂおよび認証者Ｃいずれの走行情報５ｂも他の記憶媒体などへ転送可能なアクセス権を付与する。また、アクセス制御部４ｂは、認証者Ｂおよび認証者Ｃに対して、それぞれの走行情報５ｂのみ転送可能なアクセス権を付与する。

【００９１】

図８Ａ～図８Ｃで示したような管理者権限を設定することにより、管理者である認証者Ａが、走行情報５ｂを容易に管理することができる。

【００９２】

＜記憶部５＞

図３の説明に戻り、つづいて記憶部５について説明する。記憶部５は、例えばＳＤカードやＵＳＢメモリなど可搬型の記憶媒体である。あるいは、記憶部５を例えばＲＡＭ（Random Access Memory)、フラッシュメモリ等の半導体メモリ素子、または、ＨＤＤ、光ディスク等の記憶媒体としてもよい。記憶部５は、上述した識別情報５ａ、走行情報５ｂおよびイベント情報５ｃを記憶する。

【００９３】

＜表示装置１０＞

表示装置１０は、記憶部５に記憶された走行情報５ｂを読み出し、上述のディスプレイなどの表示部（図示せず）へ表示する。なお、表示装置１０は、閲覧者が走行情報５ｂを閲覧する場合、閲覧者に対してパスワードを要求する画像を表示部へ表示する。

【００９４】

また、表示装置１０は、閲覧者から入力されたパスワードが走行情報５ｂに付与されたパスワードと一致するか否かを判定し、パスワードが一致する場合には、指定された走行映像を表示する。

【００９５】

次に、実施形態に係るドライブレコーダ１が実行する記録処理の処理手順について、図９を用いて説明する。図９は、実施形態に係るドライブレコーダ１が実行する記録処理の処理手順を示すフローチャートである。ドライブレコーダ１の動作中は、図９の処理手順が所定周期で繰り返される。

【００９６】

図９に示すように、認証部４ａは、携帯装置Ｐから送信されるＩＤおよびパスワードと、記憶部５に記憶される識別情報５ａに含まれるＩＤおよびパスワードに基づいて搭乗者の個人認証を行う（ステップＳ１０１）。なお、このステップＳ１０１の個人認証は、ドライブレコーダ１の起動直後に１回のみ行えばよい。つづいて、撮像部２は、車両１１の外部を撮像する（ステップＳ１０２）。

【００９７】

つづいて、アクセス制御部４ｂは、少なくとも緊急性の高さを示す所定の条件を満たすイベントが発生したか否かを判定する（ステップＳ１０３）。この判定処理において、アクセス制御部４ｂは、かかるイベントが発生していないと判定した場合（ステップＳ１０３，Ｎｏ）、搭乗者以外からのアクセスを制限するアクセス制限を走行情報５ｂに設定し（ステップＳ１０５）、処理を終了する。

【００９８】

一方、ステップＳ１０３の判定処理において、アクセス制御部４ｂは、かかるイベントが発生したと判定した場合（ステップＳ１０３，Ｙｅｓ）、走行情報５ｂに付与したアクセス制限を解除し（ステップＳ１０４）、処理を終了する。

【００９９】

実施形態に係るドライブレコーダ１は、図１０に一例として示す構成のコンピュータ２

００で実現することができる。図１０は、ドライブレコーダ１の機能を実現するコンピュータの一例を示すハードウェア構成図である。

【０１００】

コンピュータ２００は、ＣＰＵ（Central Processing Unit）２１０と、ＲＯＭ（Read Only Memory）２２０と、ＲＡＭ（Random Access Memory）２３０と、ＨＤＤ（Hard Disk Drive）２４０とを備える。また、コンピュータ２００は、メディアインターフェイス（Ｉ／Ｆ）２５０と、通信インターフェイス（Ｉ／Ｆ）２６０と、入出力インターフェイス（Ｉ／Ｆ）２７０とを備える。

【０１０１】

なお、コンピュータ２００は、ＳＳＤ（Solid State Drive）を備え、かかるＳＳＤがＨＤＤ２４０の一部または全ての機能を実行するようにしてもよい。また、ＨＤＤ２４０に代えてＳＳＤを設けることとしてもよい。

【０１０２】

ＣＰＵ２１０は、ＲＯＭ２２０およびＨＤＤ２４０の少なくとも一方に格納されるプログラムに基づいて動作し、各部の制御を行う。ＲＯＭ２２０は、コンピュータ２００の起動時にＣＰＵ２１０によって実行されるブートプログラムや、コンピュータ２００のハードウェアに依存するプログラムなどを格納する。ＨＤＤ２４０は、ＣＰＵ２１０によって実行されるプログラムおよびかかるプログラムによって使用されるデータ等を格納する。

【０１０３】

メディアＩ／Ｆ２５０は、記憶媒体２８０に格納されたプログラムやデータを読み取り、ＲＡＭ２３０を介してＣＰＵ２１０に提供する。ＣＰＵ２１０は、かかるプログラムを、メディアＩ／Ｆ２５０を介して記憶媒体２８０からＲＡＭ２３０上にロードし、ロードしたプログラムを実行する。あるいは、ＣＰＵ２１０は、かかるデータを用いてプログラムを実行する。記憶媒体２８０は、例えばＤＶＤ（Digital Versatile Disc）などの光磁気記録媒体やＳＤカード、ＵＳＢメモリなどである。

【０１０４】

通信Ｉ／Ｆ２６０は、ネットワーク２９０を介して他の機器からデータを受信してＣＰＵ２１０に送り、ＣＰＵ２１０が生成したデータを、ネットワーク２９０を介して他の機器へ送信する。あるいは、通信Ｉ／Ｆ２６０は、ネットワーク２９０を介して他の機器からプログラムを受信してＣＰＵ２１０に送り、ＣＰＵ２１０がかかるプログラムを実行する。

【０１０５】

ＣＰＵ２１０は、入出力Ｉ／Ｆ２７０を介して、ディスプレイ等の表示部、キーボードやマウス、ボタン等の入力部を制御する。ＣＰＵ２１０は、入出力Ｉ／Ｆ２７０を介して、入力部からデータを取得する。また、ＣＰＵ２１０は、生成したデータを入出力Ｉ／Ｆ２７０を介して表示装置１０に出力する。

【０１０６】

例えば、コンピュータ２００がドライブレコーダ１として機能する場合、コンピュータ２００のＣＰＵ２１０は、ＲＡＭ２３０上にロードされたプログラムを実行することにより、認証部４ａおよびアクセス制御部４ｂの各機能を実現する。

【０１０７】

コンピュータ２００のＣＰＵ２１０は、例えばこれらのプログラムを記憶媒体２８０から読み取って実行するが、他の例として、他の装置からネットワーク２９０を介してこれらのプログラムを取得してもよい。また、ＨＤＤ２４０は、記憶部５が記憶する識別情報５ａ、走行情報５ｂおよびイベント情報５ｃを記憶することができる。

【０１０８】

上述してきたように、実施形態に係るドライブレコーダ１は、撮像部２と、アクセス制御部４ｂとを備える。撮像部２は、車両１１の外部を撮像する。アクセス制御部４ｂは、撮像部２によって撮像され、記憶部５に記憶される車両１１の走行映像に対し、車両１１の搭乗者以外からのアクセスを制限するアクセス制限を設定する。また、アクセス制御部

４ｂは、車両１１に関して生じたイベントが少なくとも緊急性の高さを示す所定の条件を満たす場合に、アクセス制限を解除する。

【０１０９】

したがって、実施形態に係るドライブレコーダ１によれば、個人情報を保護しつつ、緊急性の高い走行映像は搭乗者以外でも閲覧することができる。

【０１１０】

また、上述した実施形態では、ドライブレコーダ１に着脱可能な可搬型の記憶媒体Ｍ（例えば、ＳＤカードなど）にアクセス制限が設定された走行映像を含む走行情報５ｂを記録した例を示したが、これに限定されるものではない。

【０１１１】

例えば、記憶媒体Ｍを、クラウドコンピューティングにおけるサーバ装置とした場合、ドライブレコーダ１は、サーバ装置と通信可能な通信部をさらに備える。アクセス制御部４ｂは、車両１１の走行映像に対し、車両１１の搭乗者以外からのアクセスを制限するアクセス制限を設定または解除し、通信部を介してサーバ装置の記憶部へ記憶する。

【０１１２】

そして、表示装置１０は、かかるサーバ装置と通信可能な通信部をさらに備え、通信部を介して、走行情報５ｂを取得し、表示部に表示する。これにより、表示システム１００では、搭乗者が走行情報５ｂの読み出しなど煩雑な作業をなくすことができ、さらに、走行情報５ｂを記憶する記憶装置のスペースをなくすことができる。

【０１１３】

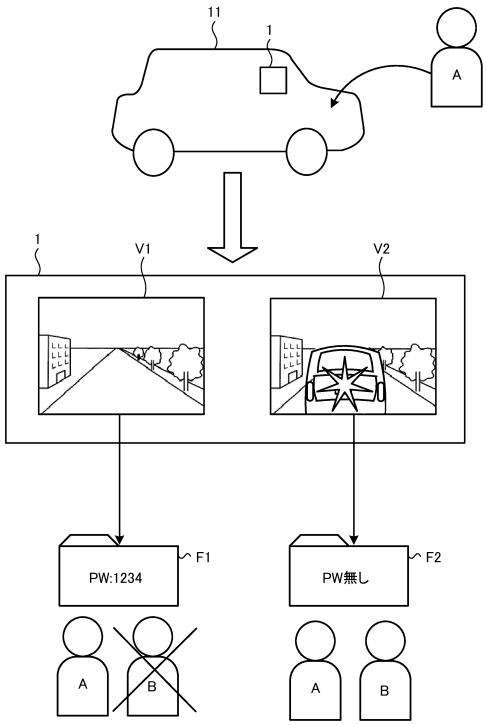
さらなる効果や変形例は、当業者によって容易に導き出すことができる。このため、本発明のより広範な態様は、以上のように表しかつ記述した特定の詳細および代表的な実施形態に限定されるものではない。したがって、添付の特許請求の範囲およびその均等物によって定義される総括的な発明の概念の精神または範囲から逸脱することなく、様々な変更が可能である。

【符号の説明】

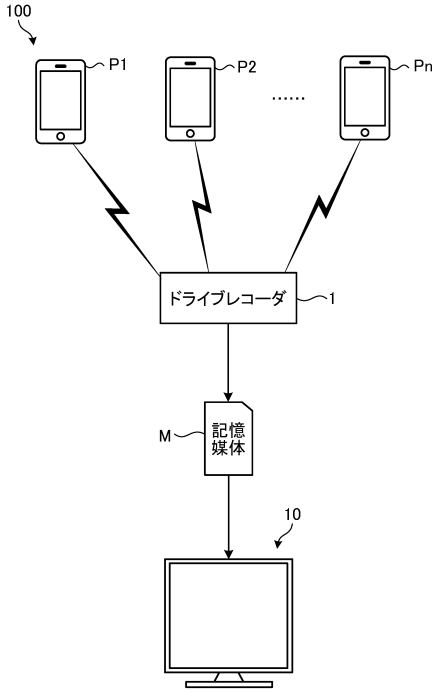
【０１１４】

１　ドライブレコーダ
２　撮像部
４ａ　認証部
４ｂ　アクセス制御部
５ａ　識別情報
５ｂ　走行情報
５ｃ　イベント情報
１０　表示装置
１１　車両

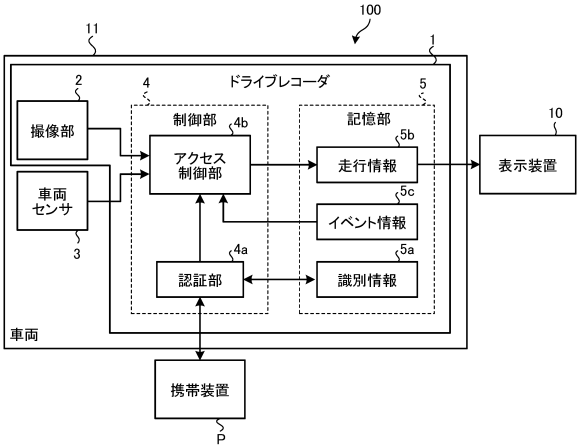
【図１】



【図２】



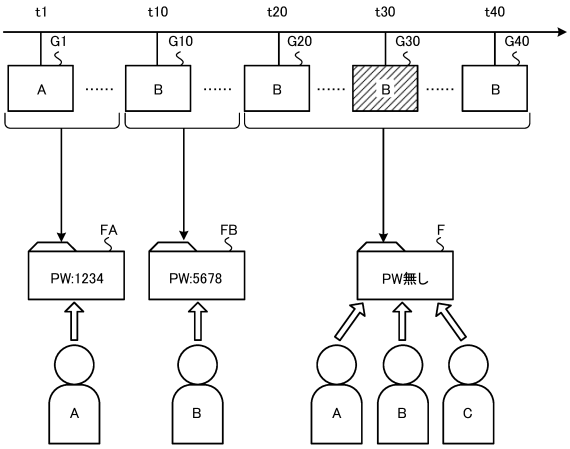
【図３】



【図４】

ID	パスワード	管理者フラグ	準管理者フラグ	
A	1234	1	0	
B	5678	0	1	
C	9999	0	0	
⋮	⋮	⋮	⋮	

【図５】



【図６】

画像No	時刻	認証ID	PWフラグ	パスワード
1	t1	A	0	1234
⋮	⋮	⋮	0	⋮
10	t10	B	0	5678
⋮	⋮	⋮	0	⋮
19	t19	B	0	5678
20	t20	B	1	無し
⋮	⋮	⋮	⋮	⋮
30	t30	B	1	無し
⋮	⋮	⋮	⋮	⋮
40	t40	B	1	無し
41	t41	B	0	5678
⋮	⋮	⋮	⋮	⋮

【図７】

イベント	記録開始		PW有無	上書き防止	その他
	自動	手動			
常時録画	●		有	無	
事故衝撃	●		無	有	
急ブレーキ	●		無	有	
防犯(不審者接近)	●		無	有	
防犯(車体衝撃)	●		無	有	
自動ブレーキ作動時	●		無	有	
車線逸脱時	●		無	有	
車両スタック時	●		無	有	
ドライブ風景		●	選択	有	
他車危険運転		●	選択	有	
他車交通違反		●	選択	有	
他車事故		●	選択	有	
他車急接近	●	●	選択	有	自動の場合はPW無し
歩行者急接近	●	●	選択	有	自動の場合はPW無し
落下物/飛来物	●	●	選択	有	自動の場合はPW無し

【図８Ａ】

		閲覧可能な走行情報		
		Aさん	Bさん	Cさん
認証者	Aさん	●	●	●
	Bさん		●	●
	Cさん			●

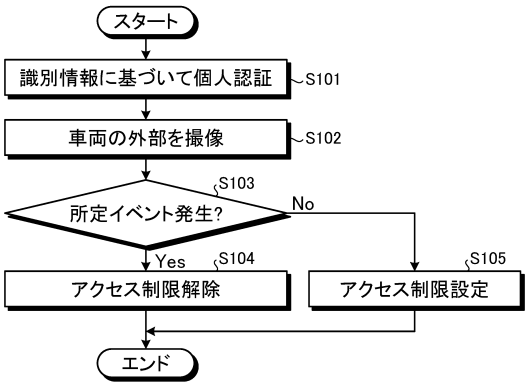
【図８Ｂ】

		削除可能な走行情報		
		Aさん	Bさん	Cさん
認証者	Aさん	●	●	●
	Bさん			
	Cさん			

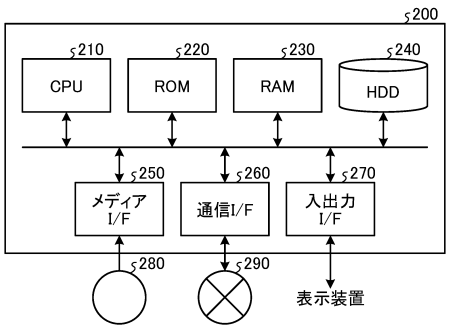
【図８Ｃ】

		データ転送可能な走行情報		
		Aさん	Bさん	Cさん
認証者	Aさん	●	●	●
	Bさん		●	
	Cさん			●

【図９】



【図１０】



フロントページの続き

(56)参考文献 特開２００４－３２２７８５（ＪＰ，Ａ）
特開２０１２－００３４０８（ＪＰ，Ａ）
特開２００６－３４５４９１（ＪＰ，Ａ）
特開２００４－２９１７６１（ＪＰ，Ａ）
特開２００９－２７１５７３（ＪＰ，Ａ）
特開２００６－３４７４９３（ＪＰ，Ａ）
特表平１０－５１２０７４（ＪＰ，Ａ）
米国特許出願公開第２０１２／０１６１９５２（ＵＳ，Ａ１）
特開２０１１－０７７８９９（ＪＰ，Ａ）
特開２００３－０３０１５２（ＪＰ，Ａ）
特開２０１１－２５７９０８（ＪＰ，Ａ）
特開２００５－１８２１７１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０７Ｃ　　１／００－　９／３８
Ｇ０６Ｆ　２１／６０
Ｇ０８Ｇ　　１／００