

(43) 国際公開日
2007 年 9 月 20 日 (20.09.2007)

PCT

(10) 国際公開番号
WO 2007/105338 A1

(51) 国際特許分類:

G11B 19/04 (2006.01) G11B 31/00 (2006.01)
B60R 11/02 (2006.01) G11B 33/02 (2006.01)

(21) 国際出願番号: PCT/JP2006/323111

(22) 国際出願日: 2006 年 11 月 20 日 (20.11.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2006-068048 2006 年 3 月 13 日 (13.03.2006) JP

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 7 番 3 号 Tokyo (JP).

(72) 発明者: および

(75) 発明者/出願人 (米国についてのみ): 妹尾 孝志 (SENOO, Takashi) [JP/JP]; 〒1020073 東京都千代田

区九段北一丁目 1 3 番 5 号 三菱電機エンジニアリング株式会社内 Tokyo (JP).

(74) 代理人: 田澤 博昭, 外 (TAZAWA, Hiroaki et al.); 〒1000013 東京都千代田区霞が関三丁目 7 番 1 号 大東ビル 7 階 Tokyo (JP).

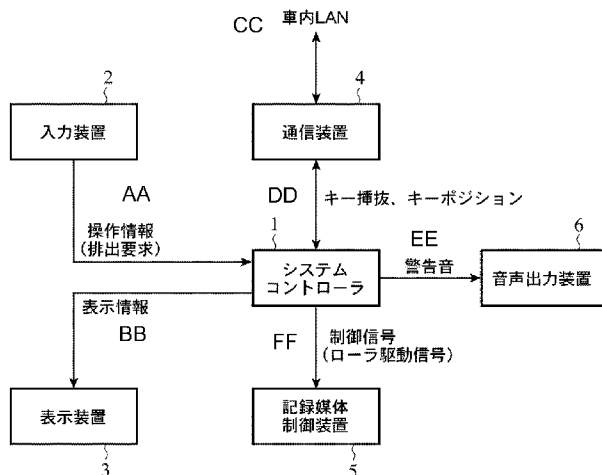
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: ANTITHEFT DEVICE AND METHOD FOR RECORDING MEDIUM

(54) 発明の名称: 記録媒体の盗難防止装置および方法



- 2 INPUT DEVICE
AA OPERATION INFORMATION
(UNLOAD REQUEST)
BB DISPLAY INFORMATION
3 DISPLAY
CC IN-CAR LAN
4 COMMUNICATION DEVICE
DD KEY INSERTION AND REMOVAL, KEY POSITION
1 SYSTEM CONTROLLER
EE ALARM SOUND
FF CONTROL SIGNAL
(ROLLER DRIVING SIGNAL)
5 RECORDING MEDIUM CONTROLLER
6 SOUND OUTPUT DEVICE

(57) Abstract: When it is judged from acquired key information that the user is absent, a system controller (1 (a control means)) sets a recording medium such as an HD to an unload forbidden state. When it is judged that the user is present, the system controller controls a security function so as to cancel the unload forbidden state of the recording medium. Further, when it is judged that the user is absent, the system controller sets the recording medium such as an HD to an access forbidden state. When it is judged that the user is present, the system controller controls the security function so as to cancel the access forbidden state of the recording medium.

(57) 要約: システムコントローラ 1 (制御手段) は、取得したキー情報からユーザが不在であると判定されたとき、HD等記録媒体を排出禁止状態に設定し、ユーザが居在すると判定されたとき、記録媒体の排出禁止状態を解除するようにセキュリティ機能を制御する。また、取得したキー情報からユーザが不在であると判定されたとき、HD等記録媒体をアクセス禁止状態に設定し、ユーザが居在すると判定されたとき、記録媒体のアクセス禁止状態を解除するようにセキュリティ機能を制御する。



KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

明 細 書

記録媒体の盗難防止装置および方法

技術分野

- [0001] 本発明は、セキュリティ機能を備えた車載用オーディオ・ビジュアル機器に用いて好適な記録媒体の盗難防止装置および方法に関する。

背景技術

- [0002] 現在流通している車載用オーディオ・ビジュアル機器(以下、車載用AV機器という)には、盗難防止対策として、他車から窃盗した車載用AV機器を自車に取り付け動作させようとしてもセキュリティ機能が働き、操作を無効にすることで動作しないような仕組みが採用されている。

しかしながら、この仕組みによれば、記録媒体の挿入は禁止されても排出が可能であることから記録媒体のみを窃盗することは容易である。

- [0003] このことを解決するために、従来、セキュリティモード時にあつては記録媒体の挿入を可能とする一方、記録媒体の排出を禁止し、AV機器を破壊しない限り記録媒体の取出しを不能とする技術が提案されている(例えば、特許文献1参照)。また、本体が電源から切り離されたことを検出してセキュリティモードが設定される車載用オーディオプレーヤにおいて、セキュリティモードが一旦設定されると、記録媒体を排出禁止モードに固定する技術も提案されている(例えば、特許文献2参照)。

- [0004] 特許文献1:特開平5-14461号公報

特許文献2:実開平3-11952号公報

- [0005] 上記した特許文献1、特許文献2に開示された技術によれば、記録媒体の盗難は防止されるものの、正規の所有者であるユーザが乗車している場合であっても同じセキュリティ機能が働き、従って、このセキュリティ機能を頻繁に用いた場合は、操作性が悪化するという問題が新たに生じることになるという課題があった。

また、将来的に、AV機器にPC(Personal Computer)等、データ採取装置が接続された場合を想定すれば、記録媒体に記録されたデータのみ窃盗されることも考えられ、この場合についての盗難防止対策はとられていないのが現状である。

[0006] 本発明は上記のような課題を解決するためになされたもので、ユーザの在不在によりセキュリティ機能を制御し、盗難防止が必要な場合にのみセキュリティ機能を働かせることで操作性の向上をはかった、記録媒体の盗難防止装置および方法を提供することを目的とする。

また、記録媒体の盗難防止対策は勿論のこと、記録媒体に記録されたデータの盗難防止対策も施すことで、記録媒体のハード、ソフト両面にわたりセキュリティ保護をはかった、記録媒体の盗難防止装置および方法を提供することを目的とする。

発明の開示

[0007] 本発明に係る記録媒体の盗難防止装置は、セキュリティ機能を備えた車載オーディオ・ビジュアル機器に挿入される記録媒体の盗難防止装置であって、操作入力に基づく前記記録媒体の排出要求を取得し、通信により取得されるイグニッションキーのキー情報からユーザが不在であると判定したときに前記記録媒体を排出禁止状態に設定し、前記セキュリティ機能を有効にする制御手段、を備えたものである。

[0008] また、本発明に係る記録媒体の盗難防止方法は、操作入力に基づく記録媒体のアクセス要求を取得し、通信により取得されるイグニッションキーのキー情報からユーザが不在であると判定したときに前記記録媒体をアクセス禁止状態に設定し、前記セキュリティ機能を有効にする制御手段、を備えたものである。

[0009] また、本発明に係る記録媒体の盗難防止方法は、車載オーディオ・ビジュアル機器は、操作入力により前記記録媒体の排出要求を取得するステップと、前記排出要求の取得を契機に、通信によりイグニッションキーのキー情報を取得するステップと、前記取得されたキー情報からユーザが不在であると判定したとき、前記記録媒体を排出禁止状態に設定し、前記取得されたキー情報からユーザが居在すると判定したとき、前記記録媒体の排出禁止状態を解除するように前記セキュリティ機能を制御するステップと、を有するものである。

[0010] また、本発明に係る記録媒体の盗難防止方法は車載オーディオ・ビジュアル機器は、操作入力により前記記録媒体のアクセス要求を取得するステップと、前記アクセス要求の取得を契機に、通信によりイグニッションキーのキー情報を取得するステップと、前記取得したキー情報からユーザが不在であると判定したとき、前記記録媒体

をアクセス禁止状態に設定し、前記取得されたキー情報からユーザが居在すると判定したとき、前記記録媒体のアクセス禁止状態を解除するように前記セキュリティ機能を制御するステップと、を有するものである。

- [0011] 本発明によれば、ユーザが不在でセキュリティ機能が必要である場合にのみセキュリティ機能を有効にすることができ、ユーザが居在する場合に操作性を優先してセキュリティ機能を働かせることができる。また、記録媒体の盗難防止対策は勿論のこと、記録媒体に記録されたデータの盗難防止対策も施すことができ、この場合、記録媒体のハード、ソフトの両面にわたってセキュリティ保護が可能になる。

図面の簡単な説明

- [0012] [図1]本発明の実施の形態1にかかわる記録媒体の盗難防止装置の構成を示すブロック図である。
- [図2]図1に示すシステムコントローラの内部構成を機能展開して示したブロック図である。
- [図3]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における基本動作の流れを説明するために引用したフローチャートである。
- [図4]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。
- [図5]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。
- [図6]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。
- [図7]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。
- [図8]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。
- [図9]本発明の実施の形態1にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。
- [図10]本発明の実施の形態2にかかわる記録媒体の盗難防止装置の構成を示すブ

ロック図である。

[図11]図10に示すシステムコントローラの内部構成を機能展開して示したブロック図である。

[図12]本発明の実施の形態2にかかわる記録媒体の盗難防止装置の基本動作について説明するために引用したフローチャートである。

[図13]本発明の実施の形態2にかかわる記録媒体の盗難防止装置における応用例の動作を説明するために引用したフローチャートである。

発明を実施するための最良の形態

[0013] 以下、この発明をより詳細に説明するために、この発明を実施するための最良の形態について、添付の図面に従って説明する。

実施の形態1.

図1は、本発明の実施の形態1にかかわる記録媒体の盗難防止装置の構成を示すブロック図である。ここではAV機器に適用した例が示されている。

本発明の第1の実施形態にかかわる記録媒体の盗難防止装置は、AV機器の制御中枢となるシステムコントローラ1を核に、入力装置2、表示装置3、通信装置4、記録媒体制御装置5、音声出力装置6が周辺装置として接続され構成されて成る。

[0014] システムコントローラ1にはCPUが内蔵され、同じく内蔵されるRAMを作業領域として用い、ROMに記録されたプログラムを逐次読み出し、実行することにより周辺装置2～6をコントロールするものである。

システムコントローラ1は、後述するように、操作入力に基づく記録媒体の排出要求を取得し、通信により取得されるイグニッションキー（以下、IGキーという）のキー情報からユーザが不在であると判定したときに記録媒体を排出禁止状態に設定し、セキュリティ機能を有効にする、本発明の制御手段として機能する。ここで、取得されるキー情報とは、IGキーの挿抜状態、キーポジション（OFF、ACC、ON）をいう。

[0015] なお、ここで使用される入力装置2はAV機器の操作ボタン、表示装置2はAV機器の液晶表示モニタとする。また、通信装置4は、車両の各部に分散配置されるECU（Engine Control Unit）と情報交換するために使用される車内LAN（Local Area Network）との間でデータを送受信するために設けられ、ここでは、エンジンを駆

動するときに用いられるIGキーの挿抜状態、もしくは挿入されたときのキーポジションをシステムコントローラ1が認識するために設けられる。

- [0016] 記録媒体制御装置5は、例えば、HD(Hard Disc)、CD(Compact Disc)、DVD(Digital Versatile Disc)、SD(Secure Digital)メモ리카ード等の記録媒体が挿入され、挿入された記録媒体に記録されたデータをアクセスするドライブであり、ここでは、記録媒体としてHDが挿入されるものとする。このため、記録媒体制御装置5には、CPU制御の下でHDをローディングして挿入し、あるいは排出するローディング機構が備えられているものとする。

また、音声出力装置6は、CPU制御の下、ここでは図示せぬスピーカを介して警告音(ビープ音)を出力しユーザに注意喚起する意味で設けられる。

- [0017] 図2は、図1に示すシステムコントローラ1の内部構成を機能展開して示したブロック図である。

図2に示されるように、システムコントローラ1の内部構成を機能的に大別すれば、排出要求取得部11と、キー情報取得部12と、セキュリティモード判定部13と、警告音生成部14と、タイマ監視部15と、UI(User Interface)部16と、セキュリティ情報照合部17と、セキュリティ情報記憶部18とから成る。

- [0018] 排出要求取得部11は、ユーザが入力装置2のボタン操作(イジェクト操作)を行うことにより生成されるHDの排出要求を取得してセキュリティモード判定部13へ供給する。セキュリティモード判定部13には、更に、キー情報取得部12を介してIGキーの挿抜状態、もしくはキーポジションに関する情報も供給されている。IGキーの挿抜状態、もしくはキーポジションに関する情報は、上記したように車内LANから通信装置4を介してキー情報として通信され、キー情報取得部12に設定される。

セキュリティモード判定部13は、排出要求取得部11を介してHDの排出要求があったことを検知すると、更に、キー情報取得部12を介して取得されるキー情報からユーザが不在であると判定したときに、HDを排出禁止状態に設定してセキュリティ機能を有効にし、記録媒体制御装置5に対し、例えば、ローディング機構のローラ駆動を禁止するための制御信号を供給する。また、警告音発生部14による警告音生成処理を起動し、音声出力装置6を介して警告音発生を指示することも可能である。

[0019] セキュリティモード判定部13はまた、キー情報からユーザが不在であると判定したとき、UI部16を介して表示装置3にセキュリティ情報入力を促すためのメッセージを表示し、続いてユーザが入力装置2を操作することによりボタン入力されるID等のセキュリティ情報を取込み、セキュリティ情報照合部17に対してセキュリティ情報の照合を指示する機能もあわせ持つ。

セキュリティ情報照合部17は、UI部16を介して取込まれるID等のセキュリティ情報と、車載AV機器毎に設定される固有のセキュリティ情報、ここではセキュリティ情報記憶部18に格納されるID等のセキュリティ情報とを比較照合し、この照合の結果をセキュリティモード判定部13へ供給する。セキュリティモード判定部13は、セキュリティ情報照合部17によって出力される照合の結果によってはHDの排出禁止状態を解除してセキュリティ機能を無効にすることができる。

[0020] なお、セキュリティ情報照合部17は、照合の結果によってはUI部16を再度起動し、表示装置3によるメッセージ表示、および入力装置2のセキュリティ情報の取り込みによる照合を所定回数試行し、都度その結果をセキュリティモード判定部13へ供給する。

セキュリティモード判定部13は、セキュリティ情報照合部17による所定回数の試行の結果に変化がないとき、HDの排出禁止状態を継続してセキュリティ機能を有効にする。

[0021] 一方、タイマ監視部15は、キーポジション検知部12によりIGキーの抜去が検知されたときに内蔵のタイマに所定の値を設定し、キー情報取得部12によるキー情報の取得を契機にタイマスタートさせてタイマ監視を行い、タイムオーバを検出したときにセキュリティモード判定部13を起動する。

このとき、セキュリティモード判定部13は、設定された時間分のカウントが終了するまでの間、HDの排出禁止状態の設定を遅延させ、この間セキュリティ機能の実行を無効にすることができる。このことは、ユーザがIGキーを抜いても数秒間は車内に居ることを配慮しての措置である。

[0022] なお、UI部16は、表示装置3にセキュリティ状態変更設定画面を表示し、セキュリティ機能を有効にするか無効にするかについての指示入力を促す機能も合わせ持

つ。このとき、セキュリティモード判定部13は、UI部16を介してユーザが入力装置2を操作することにより入力され取込まれる、セキュリティ機能の有効、無効に関する指示入力に従い、HDを排出禁止状態に設定してセキュリティ機能を有効にするか、HDの排出禁止状態を解除してセキュリティ機能を無効にするように制御する。

この機能は、セキュリティ機能のON/OFFを自動化する他に、ユーザ自身が任意にセキュリティ機能をコントロールするためになされた措置である。

[0023] 図3は、本発明の実施の形態1にかかわる記録媒体の盗難防止装置の基本動作の流れを説明するために引用したフローチャートである。

以下、図3に示すフローチャートを参照しながら図1、図2に示す記録媒体の盗難防止装置の動作について詳細に説明する。

[0024] 図3において、システムコントローラ1は、まず、排出要求受信部11により入力装置2を介して到来するHDの排出要求の有無を判定する(ステップST301)。HDの排出要求の有無に関する情報は、セキュリティモード判定部13へ出力される。システムコントローラ1は更に、キー情報取得部12により取得されるIGキーの挿抜状態、もしくはキーポジションを示すキー情報をセキュリティモード判定部13へ出力する。このとき、セキュリティモード判定部13は、ユーザからHDの排出要求があり(ステップST301“YES”)、例えば、IGキーが挿入され、ACC電源が有効になっている状態にあると判定された場合(ステップST302“YES”)、ユーザが居在すると判定してセキュリティ機能を無効とし、HD排出禁止状態を解除する(ステップST311)。そして、セキュリティモード判定部13は、記録媒体制御装置5に対してHD排出要求を出力する(ステップST312)。このことにより、記録媒体制御装置5は、挿入されてあるHDを排出することができる(ステップST313)。

[0025] 一方、セキュリティモード判定部13は、キー情報によりユーザが不在であると判定した場合、更に、現在セキュリティ機能が有効となっており、HD排出禁止状態にあるか否かを判定する(ステップST303)。

ステップST303において、セキュリティモード判定部13は、システムがHD排出禁止状態になっていた場合(ステップST303“YES”)、ステップST301の処理に戻り、一方、システムがHD排出禁止状態になっていない場合(ステップST303“NO”)、セ

セキュリティ情報照合部17を起動する。

[0026] このとき、セキュリティ情報照合部17は、まず、ユーザのID誤入力回数をカウントするために割り当てられ内蔵カウンタ(CNT)をクリアし(ステップST304)、表示装置3に対し、ユーザにHD禁止状態を解除するためのID入力を促すメッセージ(ID入力要求)を表示するようにUI部16を起動する。このことにより、UI部16は、ID入力を促すメッセージを表示装置3に表示し(ステップST305)、ユーザが入力装置2を操作することによって入力されるIDの到来を待つ(ステップST306)。

[0027] ここで、ユーザによりID入力があった場合、セキュリティ情報照合部17は、UI部16を介して出力されるIDと、セキュリティ情報記憶部18に記録された車両もしくはAV機器に固有のIDとを比較照合する(ステップST307)。

IDの比較照合の結果、一致した場合(ステップST307“YES”)、セキュリティ情報照合部17はセキュリティモード判定部13を起動し、セキュリティモード判定部13は、記録媒体制御装置5に対してHD排出要求を出力する(ステップST312)。このことにより、記録媒体制御装置5は、挿入されてあるHDを排出することができる(ステップST313)。

[0028] 一方、ステップST307において、ID不一致と判定された場合(ステップST307“NO”)、セキュリティ情報照合部17は、内蔵カウンタ(CNT)を+1更新する(ステップST308)。

ここで、IDの誤入力は2回まで許されるものとし、カウンタ(CNT)が“3”をカウントした時点で(ステップST309“YES”)、セキュリティ情報照合部17はセキュリティモード判定部13を起動し、セキュリティモードを有効にするように制御する。すなわち、セキュリティモード判定部13は、記録媒体制御装置5に、例えばローラ駆動禁止信号を出力してHD排出禁止状態に設定し(ステップST310)、ステップST301の処理に戻る。すなわち、ユーザの居在が確認できるまではHDの排出は禁止される。

[0029] 図4は、図3に示す基本動作の流れに従いHDの排出を禁止するとき、警告音を同時に鳴らしてユーザに注意喚起する、本発明の実施の形態1の応用例の動作を説明するために引用したフローチャートである。

図3に示す基本動作との差異は、記録媒体制御装置5がHD排出禁止状態に設定

された後(ステップST410)、システムコントローラ1は、音声出力装置6を起動して警告音の発生を要求し(ステップST411)、音声出力装置6は、例えば、警告音の出力を1分継続(ステップST412)した後音声出力を停止する(ステップST413)ことにある。

[0030] なお、図4のフローチャートにおいて、ユーザからHD排出要求があり、取得されたキー情報からユーザが不在であると判定されたときにHDを排出禁止状態に設定し(ステップST401～ステップST410)、ユーザが居在すると判定されたときHDの排出禁止状態を解除してセキュリティ機能を制御する処理(ステップST402、ステップST414～ステップST416)は、図3のフローチャートを用いて説明した基本動作の流れを踏襲するものである。

[0031] 図5は、図3に示す基本動作の流れに、更に、IGキーが抜去されても所定時間(数十秒間)はユーザが車両に居在するとシステムに認識させ、セキュリティ機能の実行を遅延させることによって利便性をはかる、本発明の実施の形態1の応用例の動作を説明するために引用したフローチャートである。

図5において、システムコントローラ1は、まずIGキーの挿抜を検知し(ステップST501)、IGキーが抜去(ステップST501“YES”)されたことを契機にタイマ監視部15に対して所定時間に相当する初期値(ここでは30秒)を設定する(ステップST502)。以降、HDの排出要求を受信し、到来する鍵情報からユーザが不在であると判定(ステップST503“NO”)したときにタイマ監視部15を起動してタイマをスタートさせ、タイムアウトを検出(ステップST505)するまでセキュリティ機能を無効とし、HD排出禁止状態に設定するための処理を遅延させている。

[0032] なお、取得されたキー情報からユーザが不在であると判定されたときHDを排出禁止状態に設定し、ユーザが居在すると判定されたときID入力を促しHDの排出禁止状態を解除してセキュリティ機能を制御する処理(ステップST506～ステップST513、およびステップST504、ステップST514～ステップST516)は、図3のフローチャートを用いて説明した基本動作の流れを踏襲するものである。

[0033] 図6、図7は、図5に示す応用例に、更に、図4に示すフローチャートを用いて説明した警告音を出力する機能を付加し、ユーザにセキュリティ機能が有効になったこと

を告知する意味で示した実施の形態1の応用例である。

図4、図5の説明と重複するため、冗長を回避する意味で、ここでの説明は省略する。

[0034] 図8、図9は、図3に示す基本動作に対して、セキュリティ機能のON/OFF設定をユーザが制御できるようにしてユーザに利便性を提供するとともに、一層の操作性向上をはかる意味で示した本発明の実施の形態1の応用例である。

ここでは、システムコントローラ1は最初にUI部16を介してユーザが入力装置2を操作することにより生成されるセキュリティ設定変更要求の有無を判定する(ステップST801)。具体的に、UI部16は、表示装置3に対してセキュリティ変更設定画面を表示してユーザにセキュリティ機能を有効にするか否かについての指示入力を促し、ユーザによる指示入力の到来を待つ。

[0035] システムコントローラ1は、ユーザが入力装置2を操作することにより入力され、UI部16によって取込まれる、セキュリティ機能を有効にするか否かに関する指示入力に基づき、「セキュリティ設定変更要求なし」と判定した場合(ステップST801“NO”)、図9に示すステップST809の処理に進む。

一方、「セキュリティ設定変更要求あり」と判定した場合(ステップST801“YES”)、更に、キー情報取得部12により取得されるキー情報に基づきユーザが不在か否かを判定する(ステップST802)。

[0036] ステップST802の処理においてユーザが居在すると判定された場合(ステップST802“YES”)、システムコントローラ1は、UI部16を介して表示装置3に対して現在のセキュリティ状態(セキュリティ機能が有効か否か)を表示するように指示する(ステップST803)。

続いて、システムコントローラ1は、ユーザが表示装置3に表示された現在のセキュリティ状態を確認した後に入力装置2を操作して入力される設定終了要求を、UI部16を介して取込む。ここで、「設定終了要求あり」と判定された場合(ステップST804“YES”)、後述する図9のステップST809の処理に進み、「設定終了要求無し」と判定された場合(ステップST804“NO”)、更に、セキュリティ設定変更要求の有無を判定する(ステップST805)。

[0037] ステップST805の処理において、「セキュリティ設定変更要求あり」と判定された場合(ステップST805“YES”)、セキュリティモード判定部13は、例えば、内蔵のフラグを参照することにより、現在、セキュリティ機能がON状態になっているか否かを判定し(ステップST806)、ON状態になっている場合(ステップST806“YES”)、内蔵フラグをセキュリティOFF状態に(ステップST808)、OFF状態になっている場合はセキュリティ機能ON状態に設定を変更し(ステップST807)、それぞれ、ステップST803の処理に戻る。

[0038] 一方、ステップST801の処理において、「セキュリティ設定変更要求無し」と判定された場合(ST801“NO”)、およびステップST804の処理において、「設定終了要求無し」と判定された場合(ステップST804“YES”)ともに、セキュリティモード判定部13は、排出要求取得部11を介し、ユーザが入力装置2を操作することにより生成されるHDの排出要求の取得を待つ(図9のステップST809)。

セキュリティモード判定部13は、排出要求取得部11によりHDの排出要求が到来したことを検知したときに、内蔵フラグを参照することにより、現在セキュリティ機能がON状態になっているか否かを判定し(ステップST810)、OFF状態になっている場合(ステップST810“NO”)、セキュリティ機能を無効にするためにHD排出禁止状態を解除し(ステップST820)、ON状態になっている場合(ステップST810“YES”)、更にキー情報取得部12により取得されるキー情報を判定する(ステップST811)。

[0039] 以降、取得されたキー情報からユーザが不在であると判定されたときHDを排出禁止状態に設定し、ユーザが居在すると判定されたときID入力を促しHDの排出禁止状態を解除してセキュリティ機能を制御する処理(ステップST812～ステップST819、およびステップST810、ステップST820～ステップST822)は、図3のフローチャートを用いて説明した基本動作の流れを踏襲するものである。

[0040] 以上説明のように本発明の実施の形態1によれば、ユーザが不在のときにHD等の記録媒体を排出禁止状態に設定する、セキュリティ機能が必要である場合にのみセキュリティ機能を有効にすることができ、このことにより、ユーザが居在する場合に操作性を優先させることができる。

また、記録媒体を排出禁止状態に設定してセキュリティ機能を有効にするとき、同

時に警告音を出力することでユーザに注意を喚起することができ、更に、システムに対し、IGキーを抜いても一定期間ユーザは居在するものと強制的に認識させることによりセキュリティ動作を遅延させることができ、これらにより、ユーザに利便性を提供することができる。また、ユーザにセキュリティ機能のON/OFF設定を手動で制御させることのできるUI環境を提供することで操作性を一層向上させることができる。

[0041] 実施の形態2.

図10は、本発明の実施の形態2にかかわる記録媒体の盗難防止装置の構成を示すブロック図である。

図1に示す実施の形態1との差異は、車載AV機器に特殊な接続インタフェースを介してPCを接続し、記録媒体制御装置5に挿入される記録媒体に記録されたデータを採取することにある。車載AV機器は、図1に示す実施の形態1と同様、AV機器の制御中枢となるシステムコントローラ1を核に、入力装置2、表示装置3、通信装置4、記録媒体制御装置5、音声出力装置6が周辺装置として接続され構成されるが、入力装置1からは、実施の形態1で示した排出要求に代わってアクセス要求が入力され、取込まれる。

[0042] 図11は、図10に示すシステムコントローラ1の内部構成を機能展開して示したブロック図である。

図10に示されるように、システムコントローラ1の内部構成を機能的に大別すれば、アクセス要求取得部19と、キー情報取得部12と、セキュリティモード判定部13と、警告音生成部14と、タイマ監視部15と、UI部16と、セキュリティ情報照合部17と、セキュリティ情報記憶部18とから成る。

[0043] アクセス要求取得部19は、ユーザが入力装置2のボタン操作(R/W操作)を行うことにより生成されるHDのアクセス要求を取得してセキュリティモード判定部13へ供給する。セキュリティモード判定部13には、他に、キー情報取得部12を介してIGキーの挿抜状態、もしくはキーポジションに関するキー情報が供給されている。IGキーの挿抜状態、もしくはキーポジションに関する情報は、上記したように車内LANから通信装置4を介してキー情報として通信されキー情報取得部12に設定される。

セキュリティモード判定部13は、アクセス要求取得部19を介してHDのアクセス要

求があったことを検知すると、更に、キー情報取得部12を介して取得されるキー情報からユーザが不在であると判定したときに、HDをアクセス禁止状態に設定してセキュリティ機能を有効にし、記録媒体制御装置5に対し、アクセスを禁止するための制御信号を供給する。また、警告音発生部14による警告音生成処理を起動し、音声出力装置6を介して警告音発生を指示することも可能である。

[0044] セキュリティモード判定部13はまた、キー情報からユーザが不在であると判定したとき、UI部16を介して表示装置3にセキュリティ情報入力を促すためのメッセージを表示し、続いてユーザが入力装置2を操作することによりボタン入力されるID等のセキュリティ情報を取込み、セキュリティ情報照合部17に対してセキュリティ情報の照合を指示する機能もあわせ持つ。

セキュリティ情報照合部17は、UI部16を介して取込まれるID等のセキュリティ情報と、車載AV機器毎に設定される固有のセキュリティ情報、ここではセキュリティ情報記憶部18に格納されるID等のセキュリティ情報とを比較照合し、この照合の結果をセキュリティモード判定部13へ供給する。セキュリティモード判定部13は、セキュリティ情報照合部17によって出力される照合の結果によってはHDのアクセス禁止状態を解除してセキュリティ機能を無効にすることができる。

[0045] なお、セキュリティ情報照合部17は、照合の結果によってはUI部16を再度起動し、表示装置3によるメッセージ表示、および入力装置2のセキュリティ情報の取り込みによる照合を所定回数試行し、都度その結果をセキュリティモード判定部13へ供給する。セキュリティモード判定部13は、セキュリティ情報照合部17による所定回数の試行の結果に変化がないとき、HDのアクセス禁止状態を継続してセキュリティ機能を有効にする。

[0046] 図12は、本発明の実施の形態2にかかわる記録媒体の盗難防止装置の基本動作について説明するために引用したフローチャートである。

以下、図12に示すフローチャートを参照しながら図10、図11に示す記録媒体の盗難防止装置の動作について詳細に説明する。

[0047] 図12において、システムコントローラ1は、まず、アクセス要求受信部19により入力装置2を介して到来するHDのアクセス要求、ここではデータREADの有無を判定す

る(ステップST121)。HDのアクセス要求の有無に関する情報は、セキュリティモード判定部13へ出力される。システムコントローラ1は更に、キー情報取得部12により取得されるIGキーの挿抜状態、もしくはキーポジションを示すキー情報をセキュリティモード判定部13へ出力する。

このとき、セキュリティモード判定部13は、ユーザからHDのデータREAD要求があり、キーが挿入された状態にあることが検知された場合(ステップST122“YES”)、ユーザが居在すると判定してセキュリティ機能を無効とし、HDアクセス禁止状態を解除する(ステップST131)。そして、セキュリティモード判定部13は、記録媒体制御装置5に対してアクセス要求を許可する信号を出力し(ステップST132:データREAD許可)、PC10へのデータ送信を許可する(ステップST133)。

[0048] 一方、ステップST122の処理において、キー情報によりユーザが不在であると判定された場合(ステップST122“NO”)、セキュリティモード判定部13は、更に、現在セキュリティ機能が有効となっており、HDアクセス禁止状態にあるか否かを判定する(ステップST123)。

セキュリティモード判定部13は、ステップST123の処理において、HDアクセス禁止状態に設定されていると判定した場合(ステップST123“YES”)、ステップST121の処理に戻り、一方、HDアクセス禁止状態に設定されていないと判定した場合(ステップST123“NO”)、セキュリティ情報照合部17を起動する。このとき、セキュリティ情報照合部17は、まず、ユーザのID誤入力回数をカウントするために割り当てられ内蔵カウンタ(CNT)をクリアし(ステップST124)、表示装置3に対し、ユーザにHDアクセス禁止状態を解除するためのID入力を促すメッセージ(ID入力要求)を表示するようにUI部16を起動する。このことにより、UI部16は、ID入力を促すメッセージを表示装置3に表示し(ステップST125)、ユーザが入力装置2を操作することによって入力されるIDの到来を待つ(ステップST126)。

[0049] ここで、ユーザによりID入力があった場合、セキュリティ情報照合部17は、UI部16を介して出力されるIDと、セキュリティ情報記憶部18に記録されたAV機器に固有のIDとを比較照合する(ステップST127)。IDの比較照合の結果、一致した場合(ステップST127“YES”)、セキュリティ情報照合部17は、セキュリティモード判定部13を

起動し、セキュリティモード判定部13は、記録媒体制御装置5に対してHDアクセス要求(データREAD)を許可する(ステップST132)。このことにより、PC10は、挿入されてあるHDに記録されたデータをREADすることができる(ステップST133)。

一方、ステップST127の処理において、ID不一致と判定された場合(ステップST127“NO”)、セキュリティ情報照合部17は、内蔵カウンタ(CNT)を+1更新する(ステップST128)。ここで、IDの誤入力回数は2回まで許されるものとし、カウンタ(CNT)が“3”をカウントした時点で(ステップST129“YES”)、セキュリティ情報照合部17はセキュリティモード判定部13を起動し、セキュリティモードを有効にするように制御する。すなわち、セキュリティモード判定部13は、記録媒体制御装置5にアクセス禁止信号を出力してHDアクセス禁止状態に設定し(ステップST130)、ステップST121の処理に戻る。すなわち、ユーザの居在が確認できるまでHDのアクセスは禁止される。

[0050] 図13は、図12に示す基本動作の流れに従いHDのアクセスを禁止するとき、警告音を同時に鳴らすことでユーザに注意喚起する場合の実施の形態2の応用例の動作を説明するために引用したフローチャートである。

図12に示すフローチャートとの差異は、記録媒体制御装置5がHDアクセス禁止状態に設定された後(ステップST150)、システムコントローラ1は、音声出力装置6を起動して警告音の発生を要求し(ステップST151)、音声出力装置6は、例えば、警告音の出力を1分継続(ステップST152)した後音声出力を停止する(ステップST153)ことにある。

[0051] なお、アクセス要求(データREAD)があり、取得されたキー情報からユーザが不在であると判定されたときにHDをアクセス禁止状態に設定し(ステップST141～ステップST150)、ユーザが居在すると判定されたときHDのアクセス禁止状態を解除してセキュリティ機能を制御する処理(ステップST142、ステップST154～ステップST157)は、図12で説明した基本動作の流れを踏襲するものである。

[0052] 以上説明のように本発明の実施の形態2によれば、記録媒体の盗難防止対策は勿論のこと、HD等の記録媒体に記録されたデータの盗難防止対策も施すことができ、記録媒体のハード、ソフトの両面にわたってセキュリティ保護が可能になる。また、HD等記録媒体をアクセス禁止状態に設定しセキュリティ機能を有効にするとき、同時

に警告音を出力することでユーザに注意を喚起することもできる。

[0053] 以上説明のように本発明は、取得されたキー情報からユーザが不在であると判定されたとき、HD等記録媒体を排出禁止状態に設定し、ユーザが居在すると判定されたとき、記録媒体の排出禁止状態を解除するようにセキュリティ機能を制御することでユーザが居在する場合の操作性の向上をはかるものである。

また、取得したキー情報からユーザが不在であると判定されたとき、HD等記録媒体をアクセス禁止状態に設定し、ユーザが居在すると判定されたとき、記録媒体のアクセス禁止状態を解除するようにセキュリティ機能を制御することで、記録媒体に記録されたデータの盗難防止対策も施し、記録媒体のハード、ソフトの両面にわたるセキュリティ保護を実現するものである。

[0054] なお、上記した本発明の実施の形態1、実施の形態2によれば、記録媒体としてHDを使用した場合についてのみ説明したが、他に、CDやDVDの光ディスクやSDカード等の半導体メモリを記録媒体として用いたAV機器に適用してもよい。但し、SDカードの場合は、記録媒体制御装置5にローディング機構を持たないため、セキュリティ機能を有効にするためには、例えば、SDのポップアップ機構をロックするための機械的な手段が必要になる。

産業上の利用可能性

[0055] 以上のように、この発明に係る、記録媒体のハード、ソフト両面にわたって盗難を防止するセキュリティ機能を備えた、記録媒体の盗難防止装置および方法は、車載用オーディオ・ビジュアル機器などに用いるのに適している。

請求の範囲

- [1] セキュリティ機能を備えた、車載オーディオ・ビジュアル機器に挿入される記録媒体の盗難防止装置であって、
- 操作入力に基づく前記記録媒体の排出要求を取得し、通信により取得されるイグニッションキーのキー情報からユーザが不在であると判定したときに、前記記録媒体を排出禁止状態に設定し前記セキュリティ機能を有効にする制御手段、
- を備えたことを特徴とする記録媒体の盗難防止装置。
- [2] セキュリティ機能を備えた、車載オーディオ・ビジュアル機器に挿入される記録媒体の盗難防止装置であって、
- 操作入力に基づく前記記録媒体のアクセス要求を取得し、通信により取得されるイグニッションキーのキー情報からユーザが不在であると判定したときに、前記記録媒体をアクセス禁止状態に設定し前記セキュリティ機能を有効にする制御手段、
- を備えたことを特徴とする記録媒体の盗難防止装置。
- [3] 前記制御手段は、
- 前記キー情報からユーザが不在であると判定したとき、表示装置にセキュリティ情報入力を促すためのメッセージを表示し、続いてユーザが入力装置を操作することにより入力されるセキュリティ情報を取込んで前記車載オーディオ・ビジュアル機器毎に設定される固有のセキュリティ情報と照合し、前記照合の結果によっては前記記録媒体の排出禁止状態、もしくはアクセス禁止状態を解除して前記セキュリティ機能を無効にすることを特徴とする請求項1記載の記録媒体の盗難防止装置。
- [4] 前記制御手段は、
- 前記照合の結果によっては、前記メッセージの表示、およびセキュリティ情報の取り込みによる前記照合を所定回数試行し、前記所定回数の照合を試行した結果に変化がないとき、前記記録媒体の排出禁止状態、もしくはアクセス禁止状態を継続して前記セキュリティ機能を有効にすることを特徴とする請求項3記載の記録媒体の盗難防止装置。
- [5] 前記制御手段は、
- 前記記録媒体を排出禁止状態、もしくはアクセス禁止状態に設定するとき、同時に

所定の時間だけ警告音を出力することを特徴とする請求項1記載の記録媒体の盗難防止装置。

[6] 前記制御手段は、

前記イグニッションキーの抜去が検知されたときに所定の値が設定されるタイマを、前記記録媒体の排出要求を取得したことを契機にスタートさせ、前記タイマのタイムアウトを検出するまでの間、前記記録媒体の排出禁止状態の設定を遅延させ、前記セキュリティ機能を無効にすることを特徴とする請求項1記載の記録媒体の盗難防止装置。

[7] 前記制御手段は、

前記記録媒体を排出禁止状態に設定するとき、同時に所定の時間だけ警告音を出力することを特徴とする請求項6記載の記録媒体の盗難防止装置。

[8] 前記制御手段は、

表示装置にセキュリティ状態変更設定画面を表示し、前記セキュリティ機能を有効にするか否かについての指示入力进行促し、ユーザが入力装置を操作することにより入力され、取込まれる前記セキュリティ機能を有効にするか否かに関する指示入力に従い、前記記録媒体を排出禁止状態に設定し前記セキュリティ機能を有効にするか、前記記録媒体の排出禁止状態を解除して前記セキュリティ機能を無効にするかを制御することを特徴とする請求項1記載の記録媒体の盗難防止装置。

[9] 前記制御手段は、

前記キー情報からユーザが不在であると判定したとき、表示装置にセキュリティ情報入力を促すためのメッセージを表示し、続いてユーザが入力装置を操作することにより入力されるセキュリティ情報を取込んで前記車載オーディオ・ビジュアル機器毎に設定される固有のセキュリティ情報と照合し、前記照合の結果によっては前記記録媒体の排出禁止状態、もしくはアクセス禁止状態を解除して前記セキュリティ機能を無効にすることを特徴とする請求項2記載の記録媒体の盗難防止装置。

[10] 前記制御手段は、

前記照合の結果によっては、前記メッセージの表示、およびセキュリティ情報の取り込みによる前記照合を所定回数試行し、前記所定回数の照合を試行した結果に変

化がないとき、前記記録媒体の排出禁止状態、もしくはアクセス禁止状態を継続して前記セキュリティ機能を有効にすることを特徴とする請求項9記載の記録媒体の盗難防止装置。

[11] 前記制御手段は、

前記記録媒体を排出禁止状態、もしくはアクセス禁止状態に設定するとき、同時に所定の時間だけ警告音を出力することを特徴とする請求項2記載の記録媒体の盗難防止装置。

[12] セキュリティ機能を備えた、車載オーディオ・ビジュアル機器に挿入される記録媒体の盗難防止方法であって、

前記車載オーディオ・ビジュアル機器は、

操作入力により前記記録媒体の排出要求を取得するステップと、

前記記録媒体の排出要求の取得を契機に、通信によりイグニッションキーのキー情報を取得するステップと、

前記取得されたキー情報からユーザが不在であると判定したとき、前記記録媒体を排出禁止状態に設定し、前記取得されたキー情報からユーザが居在すると判定したとき、前記記録媒体の排出禁止状態を解除するように前記セキュリティ機能を制御するステップと、

を有することを特徴とする記録媒体の盗難防止方法。

[13] セキュリティ機能を備えた、車載オーディオ・ビジュアル機器に挿入された記録媒体の盗難防止方法であって、

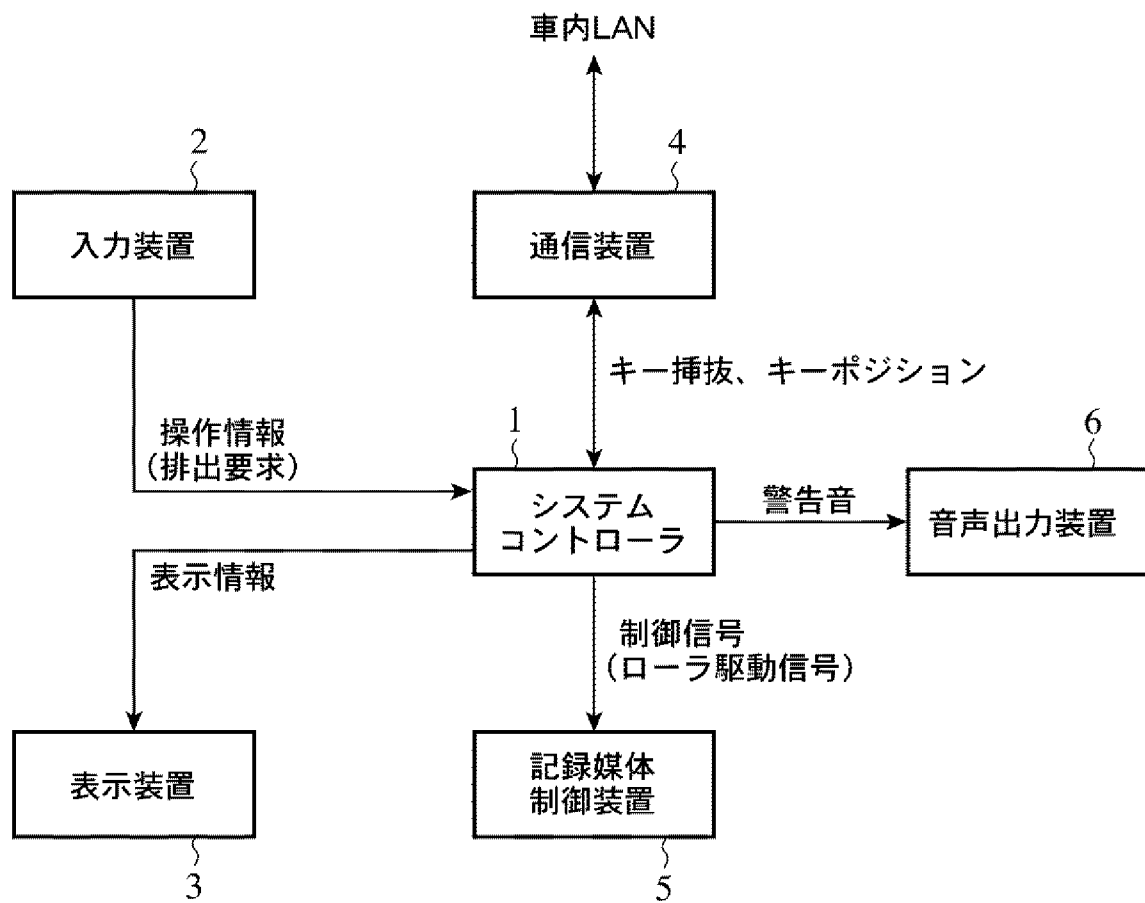
前記車載オーディオ・ビジュアル機器は、

操作入力により前記記録媒体のアクセス要求を取得するステップと、

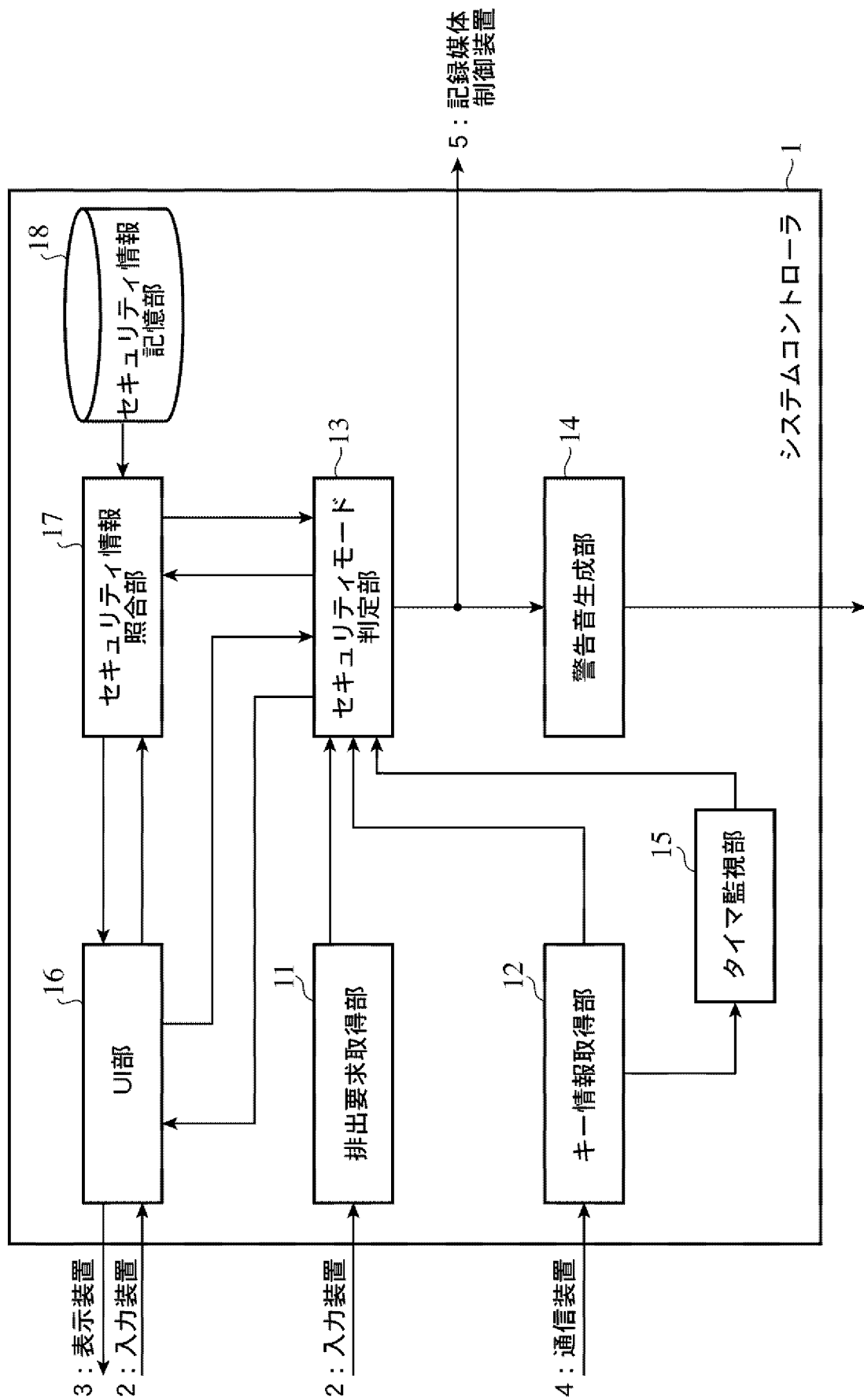
前記アクセス要求の取得を契機に、通信によりイグニッションキーのキー情報を取得するステップと、

前記取得されたキー情報からユーザが不在であると判定したとき、前記記録媒体をアクセス禁止状態に設定し、前記取得されたキー情報からユーザが居在すると判定したとき、前記記録媒体のアクセス禁止状態を解除するように前記セキュリティ機能を制御するステップと、を有することを特徴とする記録媒体の盗難防止方法。

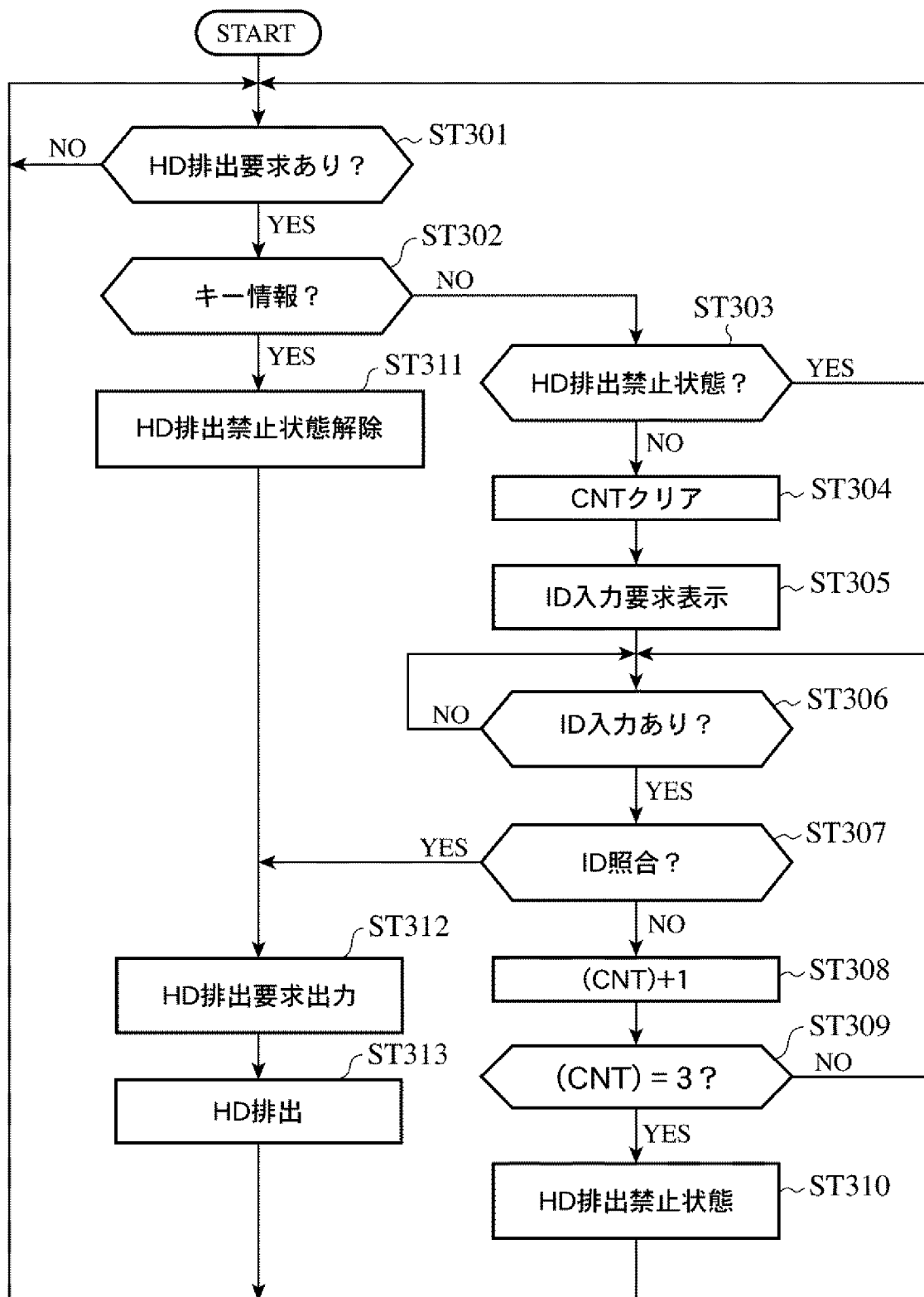
[図1]



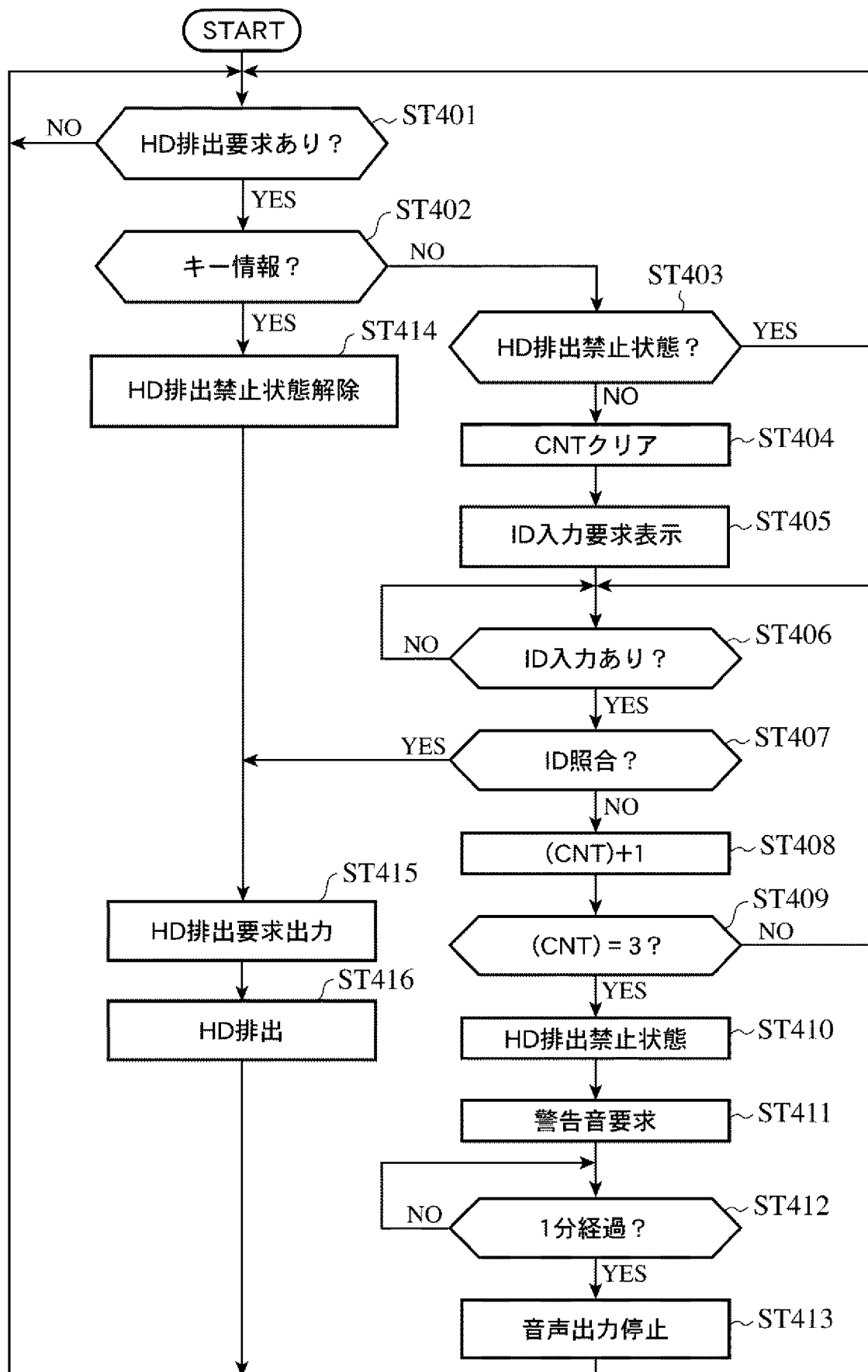
[図2]



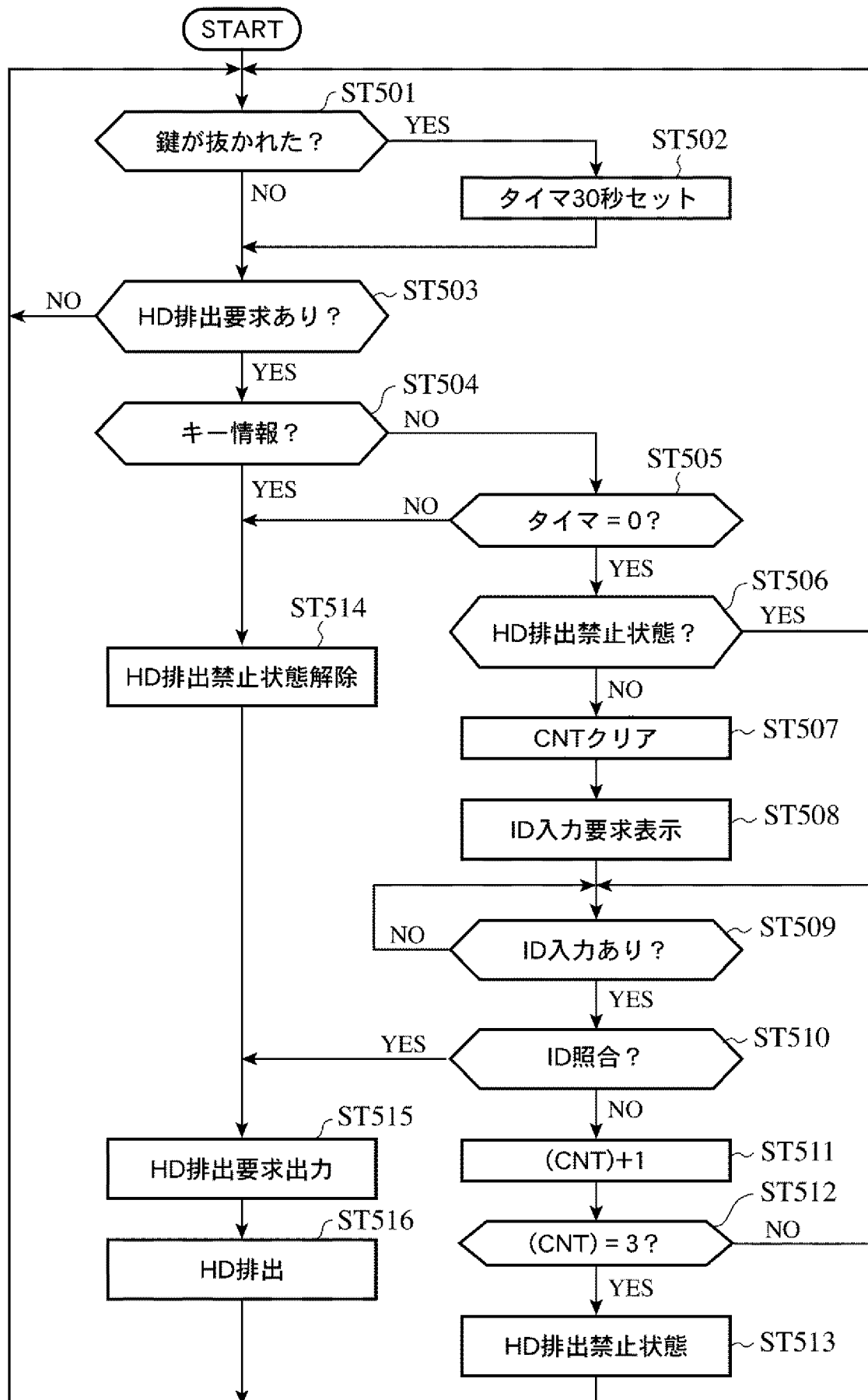
[図3]



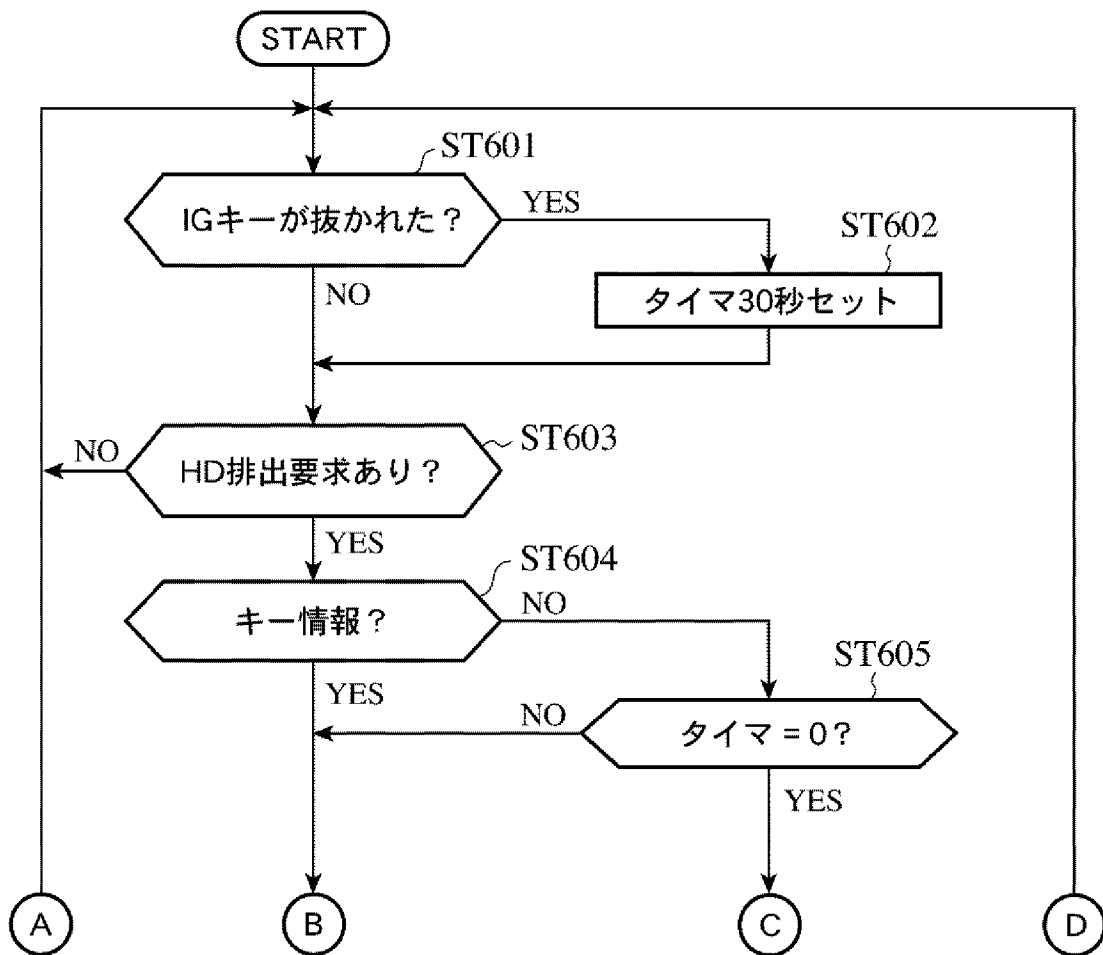
[図4]



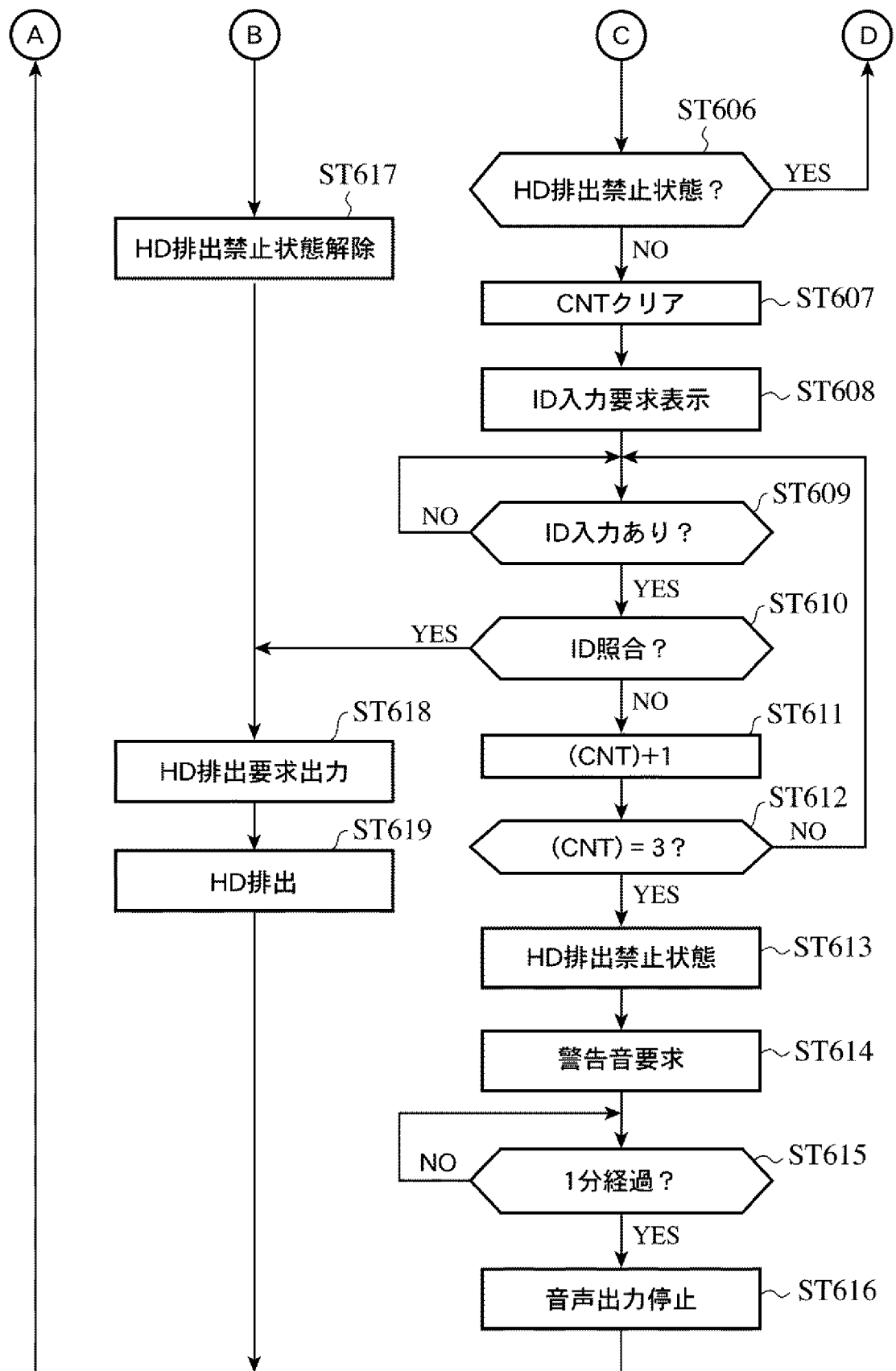
[図5]



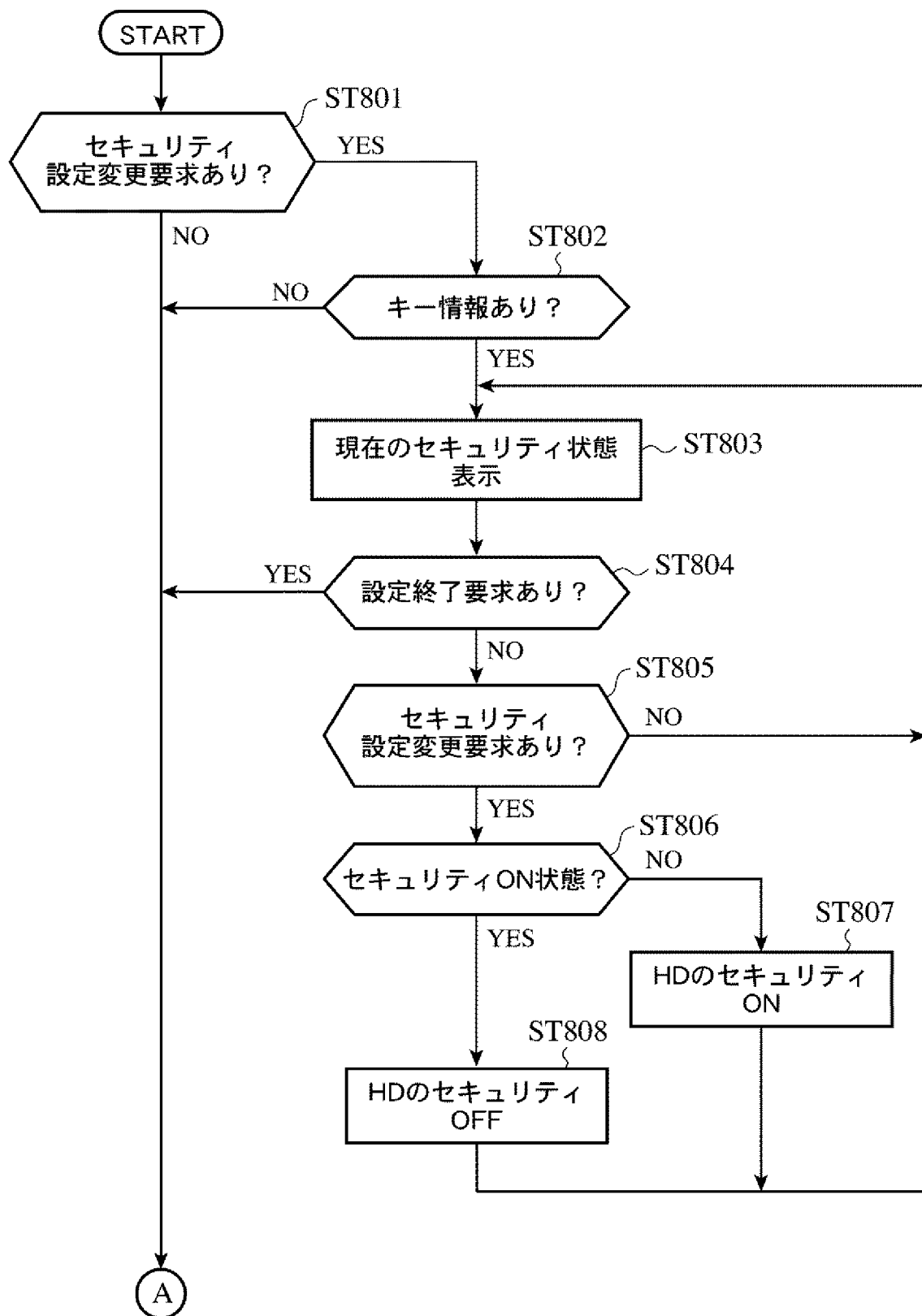
[図6]



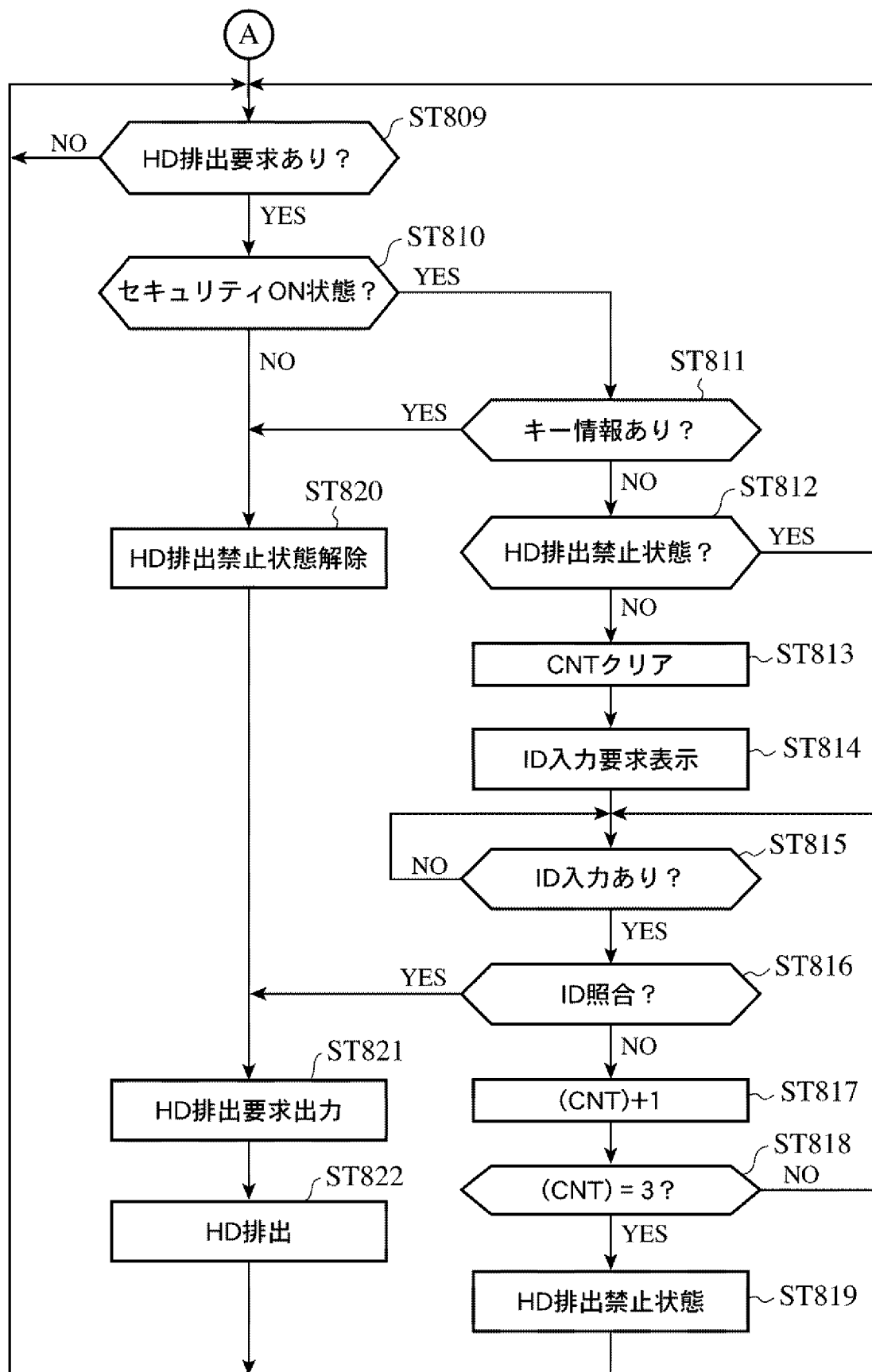
[図7]



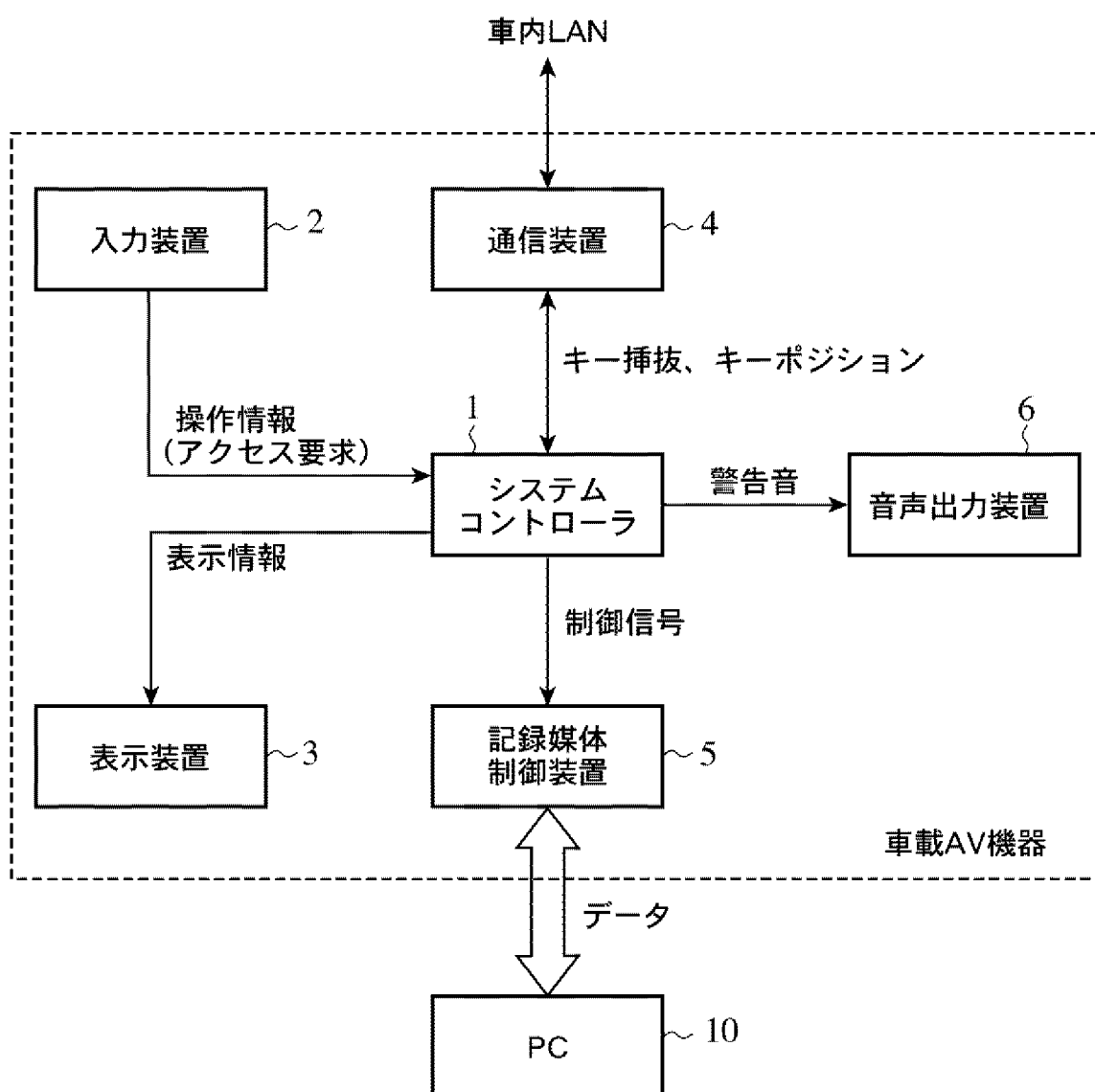
[図8]



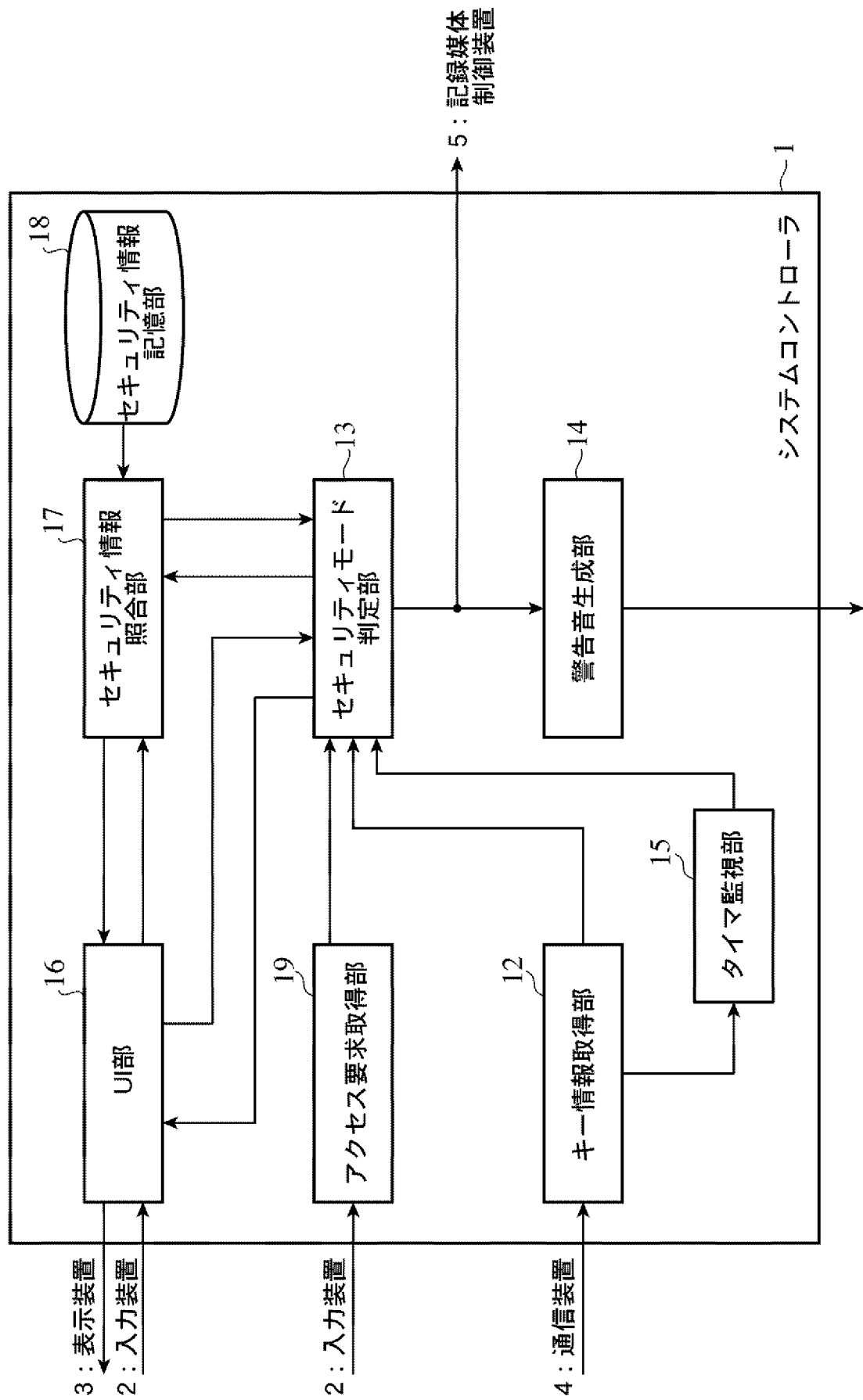
[図9]



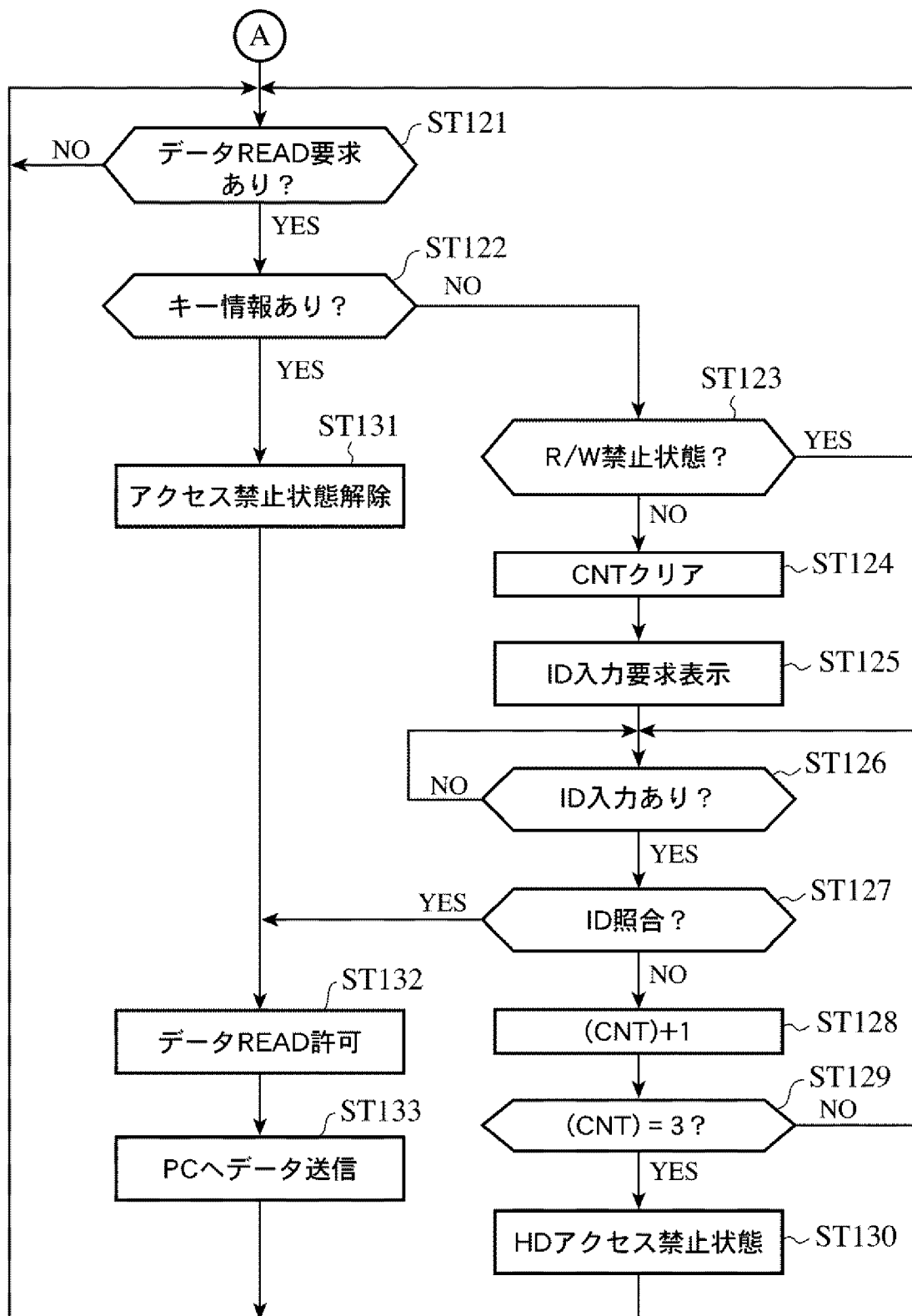
[図10]



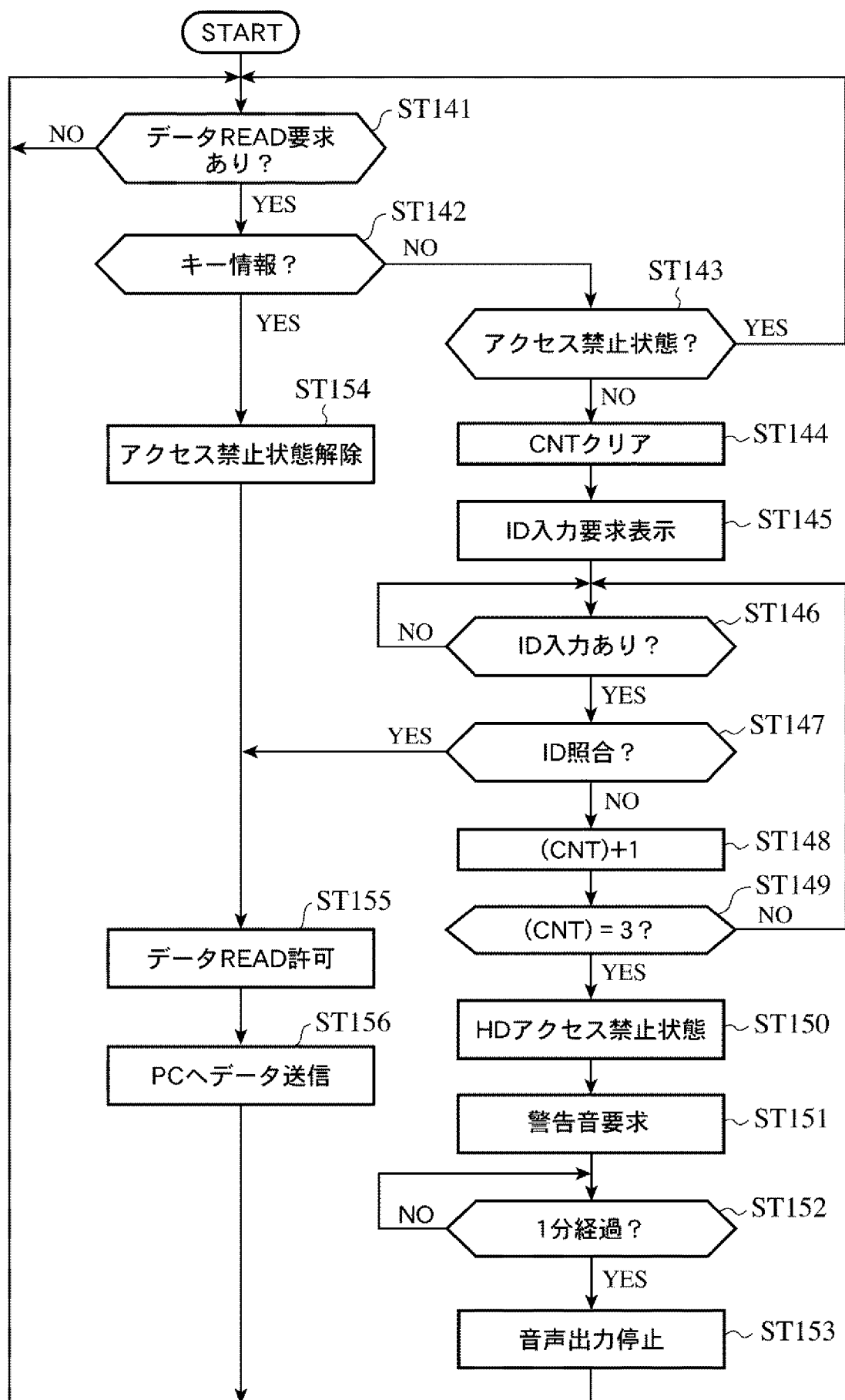
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/323111

A. CLASSIFICATION OF SUBJECT MATTER

G11B19/04(2006.01)i, B60R11/02(2006.01)i, G11B31/00(2006.01)i, G11B33/02(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G11B19/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-12087 A (Mitsubishi Electric Corp.), 15 January, 2002 (15.01.02), Full text; all drawings (Family: none)	1, 5-8, 12 2-4, 9-11, 13
Y A	JP 3-52675 B2 (Alpine Electronics, Inc.), 12 August, 1991 (12.08.91), Full text; all drawings & US 4734896 A	2-4, 9-11, 13 1, 5-8, 12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
19 December, 2006 (19.12.06)

Date of mailing of the international search report
26 December, 2006 (26.12.06)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/323111

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Microfilm of the specification and drawings annexed to the request of Japanese Utility Model Application No. 2365/1990 (Laid-open No. 94660/1991) (Kenwood Corp.), 26 September, 1991 (26.09.91), Full text; all drawings (Family: none)	4, 10 1-3, 5-9, 11-13
A	JP 5-144161 A (Fujitsu Ten Ltd.), 11 June, 1993 (11.06.93), Full text; all drawings (Family: none)	1-13
A	JP 7-37320 A (Nakamichi Corp.), 07 February, 1995 (07.02.95), Full text; all drawings (Family: none)	1-13
A	JP 2552978 Y2 (Mitsumi Electric Co., Ltd.), 15 November, 1997 (15.11.97), Full text; all drawings (Family: none)	1-13
A	WO 2005/069291 A1 (Matsushita Electric Industrial Co., Ltd.), 28 July, 2005 (28.07.05), Full text; all drawings & JP 2005-209237 A	1-13
A	Microfilm of the specification and drawings annexed to the request of Japanese Utility Model Application No. 72894/1989 (Laid-open No. 11952/1991) (Clarion Co., Ltd.), 06 February, 1991 (06.02.91), Full text; all drawings (Family: none)	1-13
A	JP 3085946 U (Funai Electric Co., Ltd.), 31 May, 2002 (31.05.02), Full text; all drawings (Family: none)	1-13

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G11B19/04(2006.01)i, B60R11/02(2006.01)i, G11B31/00(2006.01)i, G11B33/02(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. G11B19/04

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 6 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 6 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 6 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP 2002-12087 A (三菱電機株式会社) 2002.01.15, 全文, 全図 (ファミリーなし)	1, 5-8, 12 2-4, 9-11, 13
Y A	JP 3-52675 B2 (アルパイン株式会社) 1991.08.12, 全文, 全図 & US 4734896 A	2-4, 9-11, 13 1, 5-8, 12

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

1 9 . 1 2 . 2 0 0 6

国際調査報告の発送日

2 6 . 1 2 . 2 0 0 6

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官 (権限のある職員)

松尾 淳一

5 Q

8 8 4 2

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 9 1

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	日本国実用新案登録出願 2-2365 号(日本国実用新案登録出願公開 3-94660 号)の願書に添付した明細書及び図面の内容を撮影したマイ クロフィルム (株式会社ケンウッド) , 1991. 09. 26, 全文, 全図 (フ ァミリーなし)	4, 10 1-3, 5-9, 11-13
A	JP 5-144161 A (富士通テン株式会社) 1993. 06. 11, 全文, 全図 (フ ァミリーなし)	1-13
A	JP 7-37320 A (ナカミチ株式会社) 1995. 02. 07, 全文, 全図 (フ ァミリーなし)	1-13
A	JP 2552978 Y2 (ミツミ電機株式会社) 1997. 11. 15, 全文, 全図 (フ ァミリーなし)	1-13
A	WO 2005/069291 A1 (松下電器産業株式会社) 2005. 07. 28, 全文, 全 図 & JP 2005-209237 A	1-13
A	日本国実用新案登録出願 1-72894 号(日本国実用新案登録出願公開 3-11952 号)の願書に添付した明細書及び図面の内容を撮影したマイ クロフィルム (クラリオン株式会社) , 1991. 02. 06, 全文, 全図 (フ ァミリーなし)	1-13
A	JP 3085946 U (船井電機株式会社) 2002. 05. 31, 全文, 全図 (フ ァミリーなし)	1-13