(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2004-326278
(P2004-326278A)
(43)公開日　平成16年11月18日(2004.11.18)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320F	5B017
G06K 17/00	G06K 17/00	E	5B035
G06K 19/073	G06K 19/00	P	5B058

審査請求 未請求　請求項の数 30　ＯＬ　（全 24 頁）

(21)出願番号　特願2003-117822(P2003-117822)
(22)出願日　平成15年4月23日(2003.4.23)

(71)出願人　503121103
株式会社ルネサステクノロジ
東京都千代田区丸の内二丁目４番１号
(74)代理人　100089071
弁理士　玉村　静世
(72)発明者　今井　勉
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内
(72)発明者　兼平　晃
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内
(72)発明者　片山　国弘
東京都千代田区丸の内二丁目４番１号　株式会社ルネサステクノロジ内

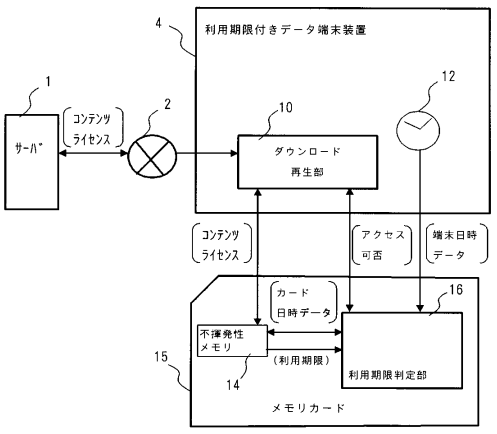
Ｆターム(参考)　5B017 AA03　BB10　CA14　CA16

最終頁に続く

(54)【発明の名称】不揮発性記憶装置及びデータ処理装置

(57)【要約】
【課題】再生装置や端末装置内部の時計の操作による期限付きデータの不正アクセスを効果的に抑制する。
【解決手段】不揮発性記憶装置は、制御回路（１６）と不揮発性記憶回路（１４）とを有する。不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有する。制限情報にはアクセス期限情報とアクセス時間情報とを含む。制御回路は、外部より供給される時刻情報と前記制限情報とに基いて利用情報のアクセス可否を判定し、時刻情報に基づいてアクセス時間情報を更新するアクセス判定動作を行なう。アクセス可否の判定において時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は時刻情報がアクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否とする。アクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。
【選択図】　図２

図２



【特許請求の範囲】
【請求項１】
制御回路と不揮発性記憶回路とを有し、
前記不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有し、
前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、
前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、
前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とする不揮発性記憶装置。
【請求項２】
制御回路と不揮発性記憶回路とを有し、
前記不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有し、
前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、
前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、
前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、前記制御回路によるアクセス判定動作を少なくとも不揮発性記憶装置へ動作電源を投入するときと動作電源を遮断するときに行なうことを特徴とする不揮発性記憶装置。
【請求項３】
前記不揮発性記憶回路は前記利用情報の格納領域を有し、前記不揮発性記憶装置は前記利用情報を複数に分割してアクセスを行ない、
アクセス開始時の前記アクセス判定動作においてアクセス可と判定された後、分割された前記利用情報のアクセス毎又は所定の複数アクセス毎に前記アクセス判定動作を行なうことを特徴とする請求項１又は２記載の不揮発性記憶装置。
【請求項４】
分割された前記利用情報のアクセス単位はセクタであることを特徴とする請求項３記載の不揮発性記憶装置。
【請求項５】
前記分割された利用情報のアクセスに対するアクセス判定動作において、第２回目以降のアクセス判定動作では、時刻情報が前記アクセス期限情報により示されるアクセス期限より後であってもアクセス可と判定することを特徴とする請求項３記載の不揮発性記憶装置。
【請求項６】
前記不揮発性記憶装置は前記時刻情報を出力可能な外部装置に接続され使用されるものであり、前記外部装置へ前記分割された利用情報を出力可能であることを特徴とする請求項３記載の不揮発性記憶装置。
【請求項７】
前記不揮発性記憶回路は不揮発性半導体メモリであり、外部装置に接続されるインタフェース端子を有する所定のメモリカードケーシングに内蔵されて成ることを特徴とする請求項３記載の不揮発性記憶装置。
【請求項８】

前記制限情報は前記制御回路により暗号化されて前記不揮発性記憶回路に格納されることを特徴とする請求項１又は２記載の不揮発性記憶装置。
【請求項９】
前記制限情報の暗号化に用いる暗号鍵は不揮発性記憶装置固有の属性情報であることを特徴とする請求項８記載の不揮発性記憶装置。
【請求項１０】
前記制御回路は前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために証明情報を外部に出力可能であることを特徴とする請求項１又は２記載の不揮発性記憶装置。
【請求項１１】
前記制御回路は、前記利用情報ライセンスを外部から受領して前記不揮発性記憶回路に格納することを特徴とする請求項１０記載の不揮発性記憶装置。
【請求項１２】
前記制御回路は前記コンテンツ鍵とともに入力される時間情報を前記アクセス時間情報の初期値として前記不揮発性記憶回路に格納することを特徴とする請求項１１記載の不揮発性記憶装置。
【請求項１３】
前記不揮発性記憶回路はアクセス制限領域とアクセス非制限領域とを有し、
前記制限情報はアクセス制限領域に格納され、
前記利用情報はアクセス非制限領域に格納されることを特徴とする請求項１又は２記載の不揮発性記憶装置。
【請求項１４】
前記制御回路は外部からの認証を受けて前記アクセス制限領域に対する書き込みが可能にされることを特徴とする請求項１３記載の不揮発性記装置。
【請求項１５】
前記アクセス制限領域は前記利用情報ライセンスの格納領域とされることを特徴とする請求項１４記載の不揮発性記憶装置。
【請求項１６】
前記制御回路は外部から与えられる証明情報に対する認証を行なって前記アクセス制限領域に対する読み出しを可能にすることを特徴とする請求項１３又は１４記載の不揮発性記装置。
【請求項１７】
再生部と利用制限部とを有し、利用情報に対するアクセス制限を行なう制限情報を格納する書換え可能な記憶媒体をアクセスして前記利用情報を再生可能なデータ処理装置であって、
前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、
前記利用制限部は、データ処理装置で生成される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記記憶媒体上の前記アクセス時間情報を更新するアクセス判定動作を行ない、
前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、
前記利用制限部によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とするデータ処理装置。
【請求項１８】
再生部と利用制限部とを有し、利用情報に対するアクセス制限を行なう制限情報を格納する書換え可能な記憶媒体をアクセスして前記利用情報を再生可能なデータ処理装置であって、
前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、
前記利用制限部は、データ処理装置で生成される時刻情報と前記制限情報とに基いて前記

利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記記憶媒体上の前記アクセス時間情報を更新するアクセス判定動作を行ない、
前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、
前記利用制限部によるアクセス判定動作を少なくとも再生部へ記憶媒体を装着するときと再生部から記憶媒体を離脱するときに行なうことを特徴とするデータ処理装置。
【請求項１９】
前記利用制限部は、再生部に記憶媒体が装着された状態で動作電源が投入されるときと、再生部に記憶媒体が装着された状態で動作電源が遮断されるときに前記アクセス判定動作を行なうことを特徴とする請求項１８記載のデータ処理装置。
【請求項２０】
前記利用制限部は、記憶媒体固有の属性情報を暗号鍵とする暗号化を行なってアクセス時間情報の更新を行なうことを特徴とする請求項１７乃至１９の何れか１項記載のデータ処理装置。
【請求項２１】
前記記憶媒体は書換え可能な不揮発性記憶装置であることを特徴とする請求項１７乃至１９の何れか１項記載のデータ処理装置。
【請求項２２】
前記不揮発性記憶装置はアクセス制限領域とアクセス非制限領域とを有し、
前記利用制限判定部はアクセス制限領域に対して制限情報のアクセスを行ない、
前記再生部はアクセス非制限領域に対して利用情報のアクセスを行なうことを特徴とする請求項２１記載のデータ処理装置。
【請求項２３】
前記利用制限部は不揮発性記憶装置から与えられる証明情報に対して認証を行なった後に前記アクセス制限領域に書き込みが可能にされることを特徴とする請求項２２記載のデータ処理装置。
【請求項２４】
前記アクセス制限領域は前記利用情報を復号するための利用情報ライセンスの格納領域とされることを特徴とする請求項２３記載のデータ処理装置。
【請求項２５】
前記利用制限部は不揮発性記憶装置に証明情報を与えて認証を受けた後に前記アクセス制限領域に対する読み出しが可能にされることを特徴とする請求項２４記載のデータ処理装置。
【請求項２６】
ホストインタフェース制御部を有し、当該ホストインタフェース制御部は、前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために前記記憶媒体が保有する証明情報をホスト装置に向けて出力可能であることを特徴とする請求項１７乃至１９の何れか１項記載のデータ処理装置。
【請求項２７】
前記ホストインタフェース制御回路は、前記利用情報ライセンスをホスト装置から受領して前記記憶媒体に格納可能であることを特徴とする請求項２６記載のデータ処理装置。
【請求項２８】
前記ホストインタフェース制御回路は、前記コンテンツ鍵とともに入力される時間情報を前記制アクセス時間情報の初期値として前記記憶媒体に格納可能であることを特徴とする請求項２７記載のデータ処理装置。
【請求項２９】
ホストインタフェース部、媒体インタフェース部、及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納するデータ処理装置であって、
前記データ処理部は、復号鍵の受領要求と共に記憶媒体が保有する証明情報をホストイン

タフェース部から外部に出力し、これに応答してホストインタフェース部に返される情報を受領し、これに基いて、媒体インタフェース部から前記記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納し、
前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、
前記アクセス時間情報の初期値は前記受領した情報に含まれる時間情報であり、
前記証明情報は特定の記憶媒体であることを表す情報であり、
前記特定の記憶媒体は、制御回路と不揮発性記憶回路とを有し、
前記不揮発性記憶回路は前記制限情報の格納領域を有し、
前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、
前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、
前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とするデータ処理装置。
【請求項３０】
媒体インタフェース部、及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納するデータ処理装置であって、
前記データ処理部は、復号鍵の発行要求に応答して記憶媒体から証明情報を取得し、記憶媒体を認証した後に、媒体インタフェース部から記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納し、
前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、
前記アクセス時間情報の初期値は所定に時間情報であり、
前記証明情報は特定の記憶媒体であることを表す情報であり、
前記特定の記憶媒体は、制御回路と不揮発性記憶回路とを有し、
前記不揮発性記憶回路は前記制限情報の格納領域を有し、
前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、
前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、
前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とするデータ処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、記憶媒体に格納された動画や音楽などのコンテンツデータなどに対する再生期限管理に係り、再生期限管理の制御を適用した不揮発性記憶装置、再生端末装置及び頒布端末装置に関する。
【０００２】
【従来の技術】
メモリカードなどの記憶媒体に記憶された画像データおよび音楽データレンタルされる場合、予め設定された再生期限内であれば、ユーザは、再生装置を用いて画像および音楽を再生できる。ユーザの再生装置において検知された時刻と、記憶媒体にデジタルデータを記憶する時に書込まれた再生期限情報とに基づいて、再生が管理される。ユーザの再生装置により検知される現在時刻が改ざんされると、再生期限を経過しているにもかかわらず

、コンテンツを再生することができる。
【０００３】
再生装置の時刻改ざんに対する対策として、例えば特許文献１に記載された技術が有る。すなわち、データ書込み装置は、データ読取り装置によりデータを出力可能な期限を設定して、記憶媒体に、データと、期限と、記憶媒体へのデータおよび期限の書込み日時とを書込む。データ読取り装置は、記憶媒体から読取った期限と書込み日時と、検知した現在日時とに基づいて、記憶媒体に書込まれたデータの出力の可否を判断して、データの出力が可能であると、記憶媒体からデータを読取って出力する。データを出力できる期限が経過したときに、データ読取り装置の検知手段により検知される現在日時を書込み日時以前に変更して、不正にデータの出力を行なおうとする場合を想定する。この場合、不正に変更された現在日時が、データが書込まれた日時以前であるため、判断手段は、データの出力が可能と判断しない。更に前記書き込み日時は再生処理の終了時に現在時刻に更新するようになっている。
【０００４】
【特許文献１】
特開２００２－２５９９１７号公報（段落９９、図７）
【０００５】
【発明が解決しようとする課題】
上記特許文献１の技術によればメモリカード等の記憶媒体に日時データを記録することによって端末内部の時計を操作されても期限付きコンテンツの不正な再生を抑制することができるが、充分ではないことが本発明者によって見出された。第１に、記憶媒体の現在時刻を再生終了時点で更新するだけでは不十分な場合が想定される。例えばコンテンツ再生終了直前に電源が遮断された場合には記憶媒体の現在時刻が全く更新されない虞がある。第２に、期限付きコンテンツの不正再生抑制機能は再生装置側が備えるので、再生装置を変えれば依然として不正アクセスが可能になる。
【０００６】
本発明の目的は、再生装置や端末装置内部の時計の操作による期限付きデータの不正アクセスを効果的に抑制する技術を提供することにある。
【０００７】
本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。
【０００８】
【課題を解決するための手段】
本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。
【０００９】
《不揮発性記憶装置》
本発明の第１の観点は、期限付きデータの不正アクセス抑止機能を記憶媒体としての不揮発性記憶装置が備える観点である。
【００１０】
〔１〕本発明に係る不揮発性記憶装置は、制御回路と不揮発性記憶回路とを有する。前記不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有する。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれる。前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行なう。前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【００１１】
上記手段により、メモリカード等の不揮発性記憶装置にアクセス時間情報のような日時データを更新して記録するから、更新毎に、アクセス時間情報により示される時間と期限情報により示される時間差は狭められ、最後にアクセス時間情報により示される時間が期限情報により示される時間を超える。一端超えれば利用不可にされる。最早、ユーザーは端末内の時計を利用制限より前の日時に戻しても再生は不可とされる。これにより、再生装置などの端末内部の時計が操作されても期限付き利用情報の不正な再生を抑制することが可能になる。アクセス時間情報の更新はアクセス終了時点だけでなくアクセス開始時点でも行なわれるから、利用情報の再生終了直前に電源が遮断されても少なくとも１回のアクセス時間情報の更新は保証される。期限付き利用情報の不正再生抑制機能は不揮発性記憶装置が備えるので、再生装置を変えても依然として不正アクセス抑止機能を働かせることは容易である。
【００１２】
〔２〕アクセス判定動作は、少なくとも不揮発性記憶装置へ動作電源を投入するときと動作電源を遮断するときに行なうようにしてもよい。
【００１３】
〔３〕更にアクセス判定動作を別のタイミングで行なってもよい。即ち、利用情報を複数に分割してアクセスを行なうとき、アクセス開始時の前記アクセス判定動作においてアクセス可と判定された後は、分割された前記利用情報のアクセス毎又は所定の複数アクセス毎に前記アクセス判定動作を行なってもよい。
【００１４】
〔４〕分割された前記利用情報のアクセス単位は例えばセクタである。
【００１５】
〔５〕前記分割された利用情報のアクセスに対するアクセス判定動作において、第２回目以降のアクセス判定動作では、時刻情報が前記アクセス期限情報により示されるアクセス期限より後であってもアクセス可と判定するようにしてよい。アクセス判定動作を何回も行なうとき、利用情報の再生途中などで期限が到来して再生が中断される不都合を簡単に解消することができる。
【００１６】
〔６〕前記不揮発性記憶装置は、例えば前記時刻情報を出力可能な外部装置に接続され使用されるものであり、前記外部装置へ前記分割された利用情報を出力可能である。
【００１７】
〔７〕前記不揮発性記憶回路は、例えば不揮発性半導体メモリであり、外部装置に接続されるインタフェース端子を有する所定のメモリカードケーシングに内蔵されて成る。
【００１８】
〔８〕前記制限情報は前記制御回路により暗号化されて前記不揮発性記憶回路に格納される。アクセス制限が行なわれていない領域に格納される場合に、簡便で好適である。
【００１９】
〔９〕前記制限情報の暗号化に用いる暗号鍵は、例えば不揮発性記憶装置固有の属性情報にすればよい。
【００２０】
〔１０〕著作権保護の観点が考慮される場合には、前記制御回路は前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために証明情報を外部に出力可能であることがよい。
【００２１】
〔１１〕その証明情報に対して外部で認証されれば、前記制御回路は、前記利用情報ライセンスを外部から受領することができ、受領したライセンスを前記不揮発性記憶回路に格納するのがよい。
【００２２】
〔１２〕前記制御回路は前記コンテンツ鍵とともに入力される時間情報を前記アクセス時

間情報の初期値として前記不揮発性記憶回路に格納することが望ましい。そのような時間情報については改ざんされている可能性は非常に低い。

【００２３】

〔１３〕セキュア領域のようなアクセス制限領域について考慮する。前記不揮発性記憶回路はアクセス制限領域とアクセス非制限領域とを有するとき、前記制限情報はアクセス制限領域に格納し、前記利用情報はアクセス非制限領域に格納すればよい。

【００２４】

〔１４〕アクセス制限領域に対する書き込み認証について考慮する。前記制御回路は外部からの認証を受けて前記アクセス制限領域に対する書き込みが可能にされればよい。アクセス制限領域に対する不正な書き込みが阻止される。

【００２５】

〔１５〕前記アクセス制限領域は例えば前記利用情報ライセンス等の格納領域とされる。

【００２６】

〔１６〕アクセス制限領域に対する読み出し認証について考慮する。前記制御回路は外部から与えられる証明情報に対する認証を行なって前記アクセス制限領域に対する読み出しを可能にする。アクセス制限領域に対する不正な読み出しを阻止できる。

【００２７】

《再生端末装置》

本発明の第２の観点は、期限付きデータの不正アクセス抑止機能を再生端末などのデータ処理装置を備える観点である。

【００２８】

〔１７〕本発明に係るデータ処理装置は、再生部と利用制限部とを有し、利用情報に対するアクセス制限を行なう制限情報を書換え可能に格納する記憶媒体をアクセスして前記利用情報を再生可能である。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれる。前記利用制限部は、データ処理装置で生成される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記記憶媒体上の前記アクセス時間情報を更新するアクセス判定動作を行なう。前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。前記利用制限部によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【００２９】

上記手段により、メモリカード等の記憶媒体にアクセス時間情報のような日時データを更新して記録するから、更新毎に、アクセス時間情報により示される時間と期限情報により示される時間差は狭められ、最後にアクセス時間情報により示される時間が期限情報により示される時間を超える。一端超えれば利用不可にされる。最早、ユーザーは端末内の時計を利用制限より前の日時に戻しても再生は不可とされる。これにより、再生装置などの端末内部の時計が操作されても期限付きコンテンツの不正な再生を抑制することが可能になる。アクセス時間情報の更新はアクセス終了時点だけでなくアクセス開始時点でも行なわれるから、利用情報の再生終了直前に電源が遮断されても少なくとも１回のアクセス時間情報の更新は保証される。

【００３０】

〔１８〕アクセス判定動作は、少なくとも再生部へ記憶媒体を装着するときと再生部から記憶媒体を離脱するときに行なうようにしてもよい。

【００３１】

〔１９〕また別の大要としてアクセス判定動作は、再生部に記憶媒体が装着された状態で動作電源が投入されるときと、再生部に記憶媒体が装着された状態で動作電源が遮断されるときに行なうようにしてもよい。

【００３２】

〔２０〕前記利用制限部は、記憶媒体固有の属性情報を暗号鍵として暗号化を行なってアクセス時間情報の更新を行なう。アクセス制限が行なわれていない領域に格納される場合に、簡便で好適である。

【００３３】

〔２１〕前記記憶媒体は例えば書換え可能な不揮発性記憶装置である。

【００３４】

〔２２〕セキュア領域のようなアクセス制限領域について考慮する。前記不揮発性記憶装置はアクセス制限領域とアクセス非制限領域とを有するとき、前記利用制限判定部はアクセス制限領域に対して制限情報のアクセスを行ない、前記再生部はアクセス非制限領域に対して利用情報のアクセスを行なう。

【００３５】

〔２３〕アクセス制限領域に対する書き込み認証について考慮する。前記利用制限部は不揮発性記憶装置から出力される証明情報に対して認証を行なった後にアクセス制限領域に書き込みが可能にされるのがよい。アクセス制限領域に対する不正な書き込みが阻止される。

【００３６】

〔２４〕前記アクセス制限領域は前記利用情報を復号するための利用情報ライセンスの格納領域とされる。

【００３７】

〔２５〕アクセス制限領域に対する読み出し認証について考慮する。前記利用制限部は不揮発性記憶装置に証明情報を与えて認証を受けた後に前記アクセス制限領域に対する読み出しが可能にされるのがよい。アクセス制限領域対する不正読み出しを阻止できる。

【００３８】

〔２６〕ホストインタフェース制御部を有するとき、著作権保護の観点が考慮される場合には、当該ホストインタフェース制御部は、前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために前記記憶媒体が保有する証明情報をホスト装置に向けて出力可能であることが望ましい。

【００３９】

〔２７〕その証明情報に対してホスト送致で認証されれば、前記ホストインタフェース制御回路は、前記利用情報ライセンスをホスト装置から受領して前記記憶媒体に格納可能であることが望ましい。

【００４０】

〔２８〕前記ホストインタフェース制御回路は、前記コンテンツ鍵とともに入力される時間情報を前記制アクセス時間情報の初期値として前記記憶媒体に格納可能であることが望ましい。そのような時間情報については改ざんされている可能性は非常に低い。

【００４１】

《ダウンロード端末装置》

本発明の第３の観点は、期限付きデータの不正アクセス抑止機能をダウンロード端末装置等のデータ処理装置が支援する観点である。

【００４２】

〔２９〕本発明に係るデータ処理装置はホストインタフェース部、媒体インタフェース部、及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納する。前記データ処理部は、復号鍵の受領要求と共に記憶媒体が保有する証明情報をホストインタフェース部から外部に出力し、これに応答してホストインタフェース部に返される情報を受領し、これに基いて、媒体インタフェース部から前記記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納する。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれる。前記アクセス時間情報の初期値は前記受領した情報に含まれる時間情報である。前記証明情報は特定の記憶媒体であることを表す情報である。前記特定の記憶媒体は、制御回路と不揮発性記憶回路とを有し、前記不揮発性記憶回路は前記制限情報の格納領域

を有する。前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行なう。前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【００４３】

《頒布端末装置》

本発明の第４の観点は、期限付きデータの不正アクセス抑止機能を頒布端末装置等のデータ処理装置が支援する観点である。

【００４４】

〔３０〕本発明に係るデータ処理装置は、媒体インタフェース部及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納する。前記データ処理部は、復号鍵の発行要求に応答して記憶媒体から証明情報を取得し、記憶媒体を認証した後に、媒体インタフェース部から記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納する。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、前記アクセス時間情報の初期値は所定に時間情報である。前記証明情報は特定の記憶媒体であることを表す情報である。特定の記憶媒体は上記項目〔２９〕の記憶媒体と同じである。

【００４５】

【発明の実施の形態】

図１にはコンテンツデータ配信システムが例示される。コンテンツサーバ１が接続するネットワーク２には代表的に示される利用期限付きデータ端末装置（データ処理装置）３が接続される。利用期限付きデータ端末装置（単にデータ端末装置とも称する）３はダウンロード再生部（ダウンロード部及び再生部）１０、利用期限判定部（利用制限部）１１、及び端末内部時計１２を有する。データ端末装置３には記憶媒体として不揮発性記憶装置（単にメモリカードとも称する）１３が着脱自在にされる。メモリカード１３はフラッシュメモリなどの電気的に消去及び書き込み可能な不揮発性メモリ（不揮発性記憶回路）１４を備える。

【００４６】

データ端末装置３によるコンテンツデータのダウンロード機能の概略を説明する。データ端末装置３にメモリカード１３が装着されて、データ端末装置３にコンテンツデータのダウンロードが指示されると、データ端末装置３は、コンテンツサーバ１から利用期限付きコンテンツデータ（利用情報）とそれに対応した再生ライセンス（利用情報ライセンス）をダウンロードし、メモリカードに書き込む。更に、サーバ１からダウンロードの日時データを取得し、メモリカード１３に書き込む。メモリカード１３に書き込まれた日時データがカード日時データである。特に制限されないが、ダウンロードされた日時データは利用制限判定部でライセンスフォーマットに組み込まれてセキュアライセンスとして不揮発性メモリ１４のセキュア領域に格納される。特に制限されないが、利用期限もセキュアライセンスが保有する。また、特に制限されないが、再生ライセンスも不揮発性メモリ１４のセキュア領域に格納される。

【００４７】

データ端末装置３による期限付きコンテンツデータの再生機能について概略を説明する。データ端末装置３に再生が指示されるとデータ端末装置３はメモリカード１３から再生ライセンスを読み出す。読み出した再生ライセンスから利用期限を取出し、コンテンツデータの利用期限を利用期限判定部１１に送る。利用期限部１１は、コンテンツデータの利用期限（アクセス期限情報）、端末内部時計１２が示す端末日時データ（時刻情報）、カードが保有するカード日時データ（アクセス時間情報）とによって、アクセス可否を判定する。即ち、前記端末日時データにより示される日時がアクセス期限情報により示されるア

クセス期限よりも後であり、又は前記端末日時データにより示される日時がカード日時データにより示される日時よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。アクセス可であればメモリカード１３のコンテンツデータを読み出して再生する。アクセス否であれば再生ライセンスなどを消去する。利用期限判定部１１は前記アクセス可否判定と共に、前記端末日時データに基づいてメモリカード１３内のカード日時データを更新する。

【００４８】

カード日時データの更新は、上記アクセス可否判定時に代表されるアクセス開始時だけでなく、アクセス終了時にも行なう。また、例えば、少なくともメモリカードへ動作電源を投入するときと動作電源を遮断するときに行なうようにしてもよい。

【００４９】

図２にはコンテンツデータ配信システムに別のデータ端末装置４が接続されている例が示される。データ端末装置４はダウンロード再生部（ダウンロード部及び再生部）１０と端末内部時計１２を有する。データ端末装置３には記憶媒体として不揮発性記憶装置（単にメモリカードとも称する）１５が着脱自在にされる。メモリカード１５は利用期限判定部（利用制限部）１６と不揮発性メモリ１４を備える。

【００５０】

データ端末装置４によるコンテンツデータのダウンロード機能の概略を説明する。データ端末装置４にメモリカード１５が装着されて、データ端末装置４にコンテンツデータのダウンロードが指示されると、データ端末装置４は、コンテンツサーバ１から利用期限付きコンテンツデータ（利用情報）とそれに対応した再生ライセンス（利用情報ライセンス）をダウンロードし、メモリカード１５に書き込む。更に、サーバ１からダウンロードの日時データを取得し、メモリカード１５に書き込む。メモリカード１５に書き込まれた日時データがカード日時データである。特に制限されないが、ダウンロードされた日時データは利用制限判定部でライセンスフォーマットに組み込まれてセキュアライセンスとして不揮発性メモリ１４のセキュア領域に格納される。特に制限されないが、再生ライセンスも不揮発性メモリ１４のセキュア領域に格納される。

【００５１】

期限付きコンテンツデータの再生機能について概略を説明する。データ端末装置４に再生が指示されるとデータ端末装置４は利用期限判定部１６にメモリカード１５の再生ライセンスを取得させる。利用期限判定部１６は読み出した再生ライセンスから利用期限を取出す。利用期限判定部１６は、コンテンツデータの利用期限（アクセス期限情報）、端末内部時計１２が示す端末日時データ（時刻情報）、不揮発性メモリ１４が保有するカード日時データ（アクセス時間情報）とによって、アクセス可否を判定する。即ち、前記端末日時データにより示される日時がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記端末日時データにより示される日時がカード日時データにより示される日時よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。アクセス可であれば利用期限判定部１６はダウンロード再生部１０にメモリカード１３のコンテンツデータを読み出させて再生可能とする。利用期限判定部１６は前記アクセス可否判定と共に、前記端末日時データに基づいてメモリカード内のカード日時データを更新する。

【００５２】

カード日時データの更新は、上記アクセス可否判定時に代表されるアクセス開始時だけでなく、アクセス終了時にも行なう。また、例えば、少なくともメモリカードへ動作電源を投入するときと動作電源を遮断するときに行なうようにしてもよい。

【００５３】

図３には前記端末日時データに基づいて更新されるカード日時データによる利用制限の概要が例示される。コンテンツデータをダウンロードした日時（借りた日）Ｔｓ、利用期限（返却日）Ｔｅは固定である。現在とある時間は端末日時データが示す時間Ｔｃである。アクセス日時とあるのがカード日時データが示す時間Ｔａｃｓである。カード日時データ

が更新されなければそれが示す日時はコンテンツデータをダウンロードした日時（借りた日）Ｔｓに固定される。仮に（ａ）のように、カード日時データＴａｃｓが更新されなければ現在日時Ｔｃが借りた日Ｔｓと利用期限Ｔｅの間の何処にあっても利用可能となり、例えば（ｂ）のように現在日時Ｔｃが利用期限Ｔｅを過ぎれば利用不可になる。しかし、端末時計を操作して現在日時を借りた日と利用期限の間に移動すれば、コンテンツデータは不正に利用可能になる。これに対し図１、図２では前記端末日時データに基づいてメモリカード内のカード日時データを更新するから、（ｃ）のようにアクセス日時とあるカード日時データＴａｃｓが示す日時から利用期限までの時間は更新毎に狭められ、最後に利用期限Ｔｅを超える。一端超えれば利用不可にされる。最早、ユーザーは端末内の時計を利用制限より前の日時に戻しても再生は不可とされる。これにより、データ端末装置内部の時計が操作されても期限付きコンテンツの不正な再生を充分に抑制することが可能になる。

【００５４】

カード日時データの更新は、アクセス終了時点だけでなくアクセス開始時点でも行なわれるから、利用情報の再生終了直前に電源が遮断されても少なくとも１回のアクセス時間情報の更新は保証される。図２のように、期限付き利用情報の不正再生抑制機能は不揮発性記憶装置が備えるので、再生装置を変えても依然として不正アクセス抑止機能を働かせることは容易である。

【００５５】

図４には前記利用期限判定部１１と端末内部時計１２の具体例が示される。２０で示される回路ブロックは、少なくとも前記利用期限判定部１１と端末内部時計１２を実現するマイクロコンピュータとされる。図４にはマイクロコンピュータ２０の内部を機能ブロックによって示している。マイクロコンピュータ２０は、日時データ取得作成部２１、暗号化部２２、ライセンス作成部２３、セキュア領域アクセス部２４、日時データ取り出し部２５、復号部２６、利用制限判定部２６、及び端末内時計回路２７を有する。

【００５６】

不揮発性メモリ１４はセキュア領域（アクセス制限領域）１４Ａと非セキュア領域（アクセス非制限領域）１４Ｂを有する。セキュア領域１４Ａに対する書き込みアクセスはメモリカード１３内の証明情報に対しメモリカード外部例えば端末装置２０やサーバ１による認証を受けて可能にされる。外部からセキュア領域１４Ａに対する読み出しは外部から与えられる証明情報に対して認証を得ることを条件に許可される。図示は省略するが、メモリカード１３は不揮発性メモリ１４のアクセス制御と外部とのインタフェース制御を行なうカードコントローラを有している。セキュア領域アクセス部２４はそのカードコントローラを介してインタフェースされる。

【００５７】

この例では、カード日時データ暗号化部２２で暗号化した後、これをライセンス作成部２３でセキュアライセンスに埋め込んで、セキュア領域アクセス部２４の制御で不揮発性メモリ１４のセキュア領域１４Ａに記録するようになっている。

【００５８】

前記日時データ取得作成部２１はサーバ１がコンテンツデータやライセンスをダウンロードしたときサーバ１から日時データ（ダウンロード日時データ）を取得する回路である。取得した日時データのフォーマットは図５に例示されるように、１６バイトのデータで構成される。

【００５９】

前記暗号化部２２はサーバから取得した前記日時データを暗号化する。暗号化方式は、特に制限されないが、コンテンツの暗号化復号処理で用いているのと同じＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式を用いる。日時データを暗号化する鍵はメモリカード固有の属性情報、例えば、カードのシリアル番号等を用いる。

【００６０】

前記ライセンス作成部２３は、取得して暗号化した日時データを例えばライセンスフォー

マット中のコンテンツ鍵の部分に埋め込んでセキュアライセンスを作成する。

【００６１】

前記セキュア領域アクセス部２４は日時データが含まれているセキュアライセンスを不揮発性メモリのセキュア領域１４Ａに書き込む。セキュア領域１４Ａへの書き込みには前記書き込み認証が必要とされる。前記日時データ取り出し部２５は暗号化された日時データが含まれるライセンスをセキュア領域から読み出し、暗号化された日時データを取出す。セキュア領域１４Ａの読み出しには前記読み出し認証が必要とされる。

【００６２】

復号部２６はセキュアライセンスから取出した暗号化された日時データをＡＥＳで復号する。復号する鍵は暗号部２２で用いた鍵と同じものを使用する。

【００６３】

前記利用制限判定部２７は、前述の如く、利用期限が切れていないのかを判定すると共に、端末内の時計がユーザーによって操作されていないかを判定する。その判定内容は図１を参照して既に説明した。操作されていると判定したら、カード内のライセンスを全て消去する。端末内時計回路２８は端末内の時計から年月日時間を取得する。

【００６４】

図４の各機能ブロックは、特に図示はしないが、中央処理装置、浮動小数点演算ユニット、それらの処理プログラムを保有するＲＯＭ（リード・オンリ・メモリ）、中央処理装置のワーク領域などに利用されるＲＡＭ（ランダム・アクセス・メモリ）、リアルタイムクロック回路、タイマ、及び入出力回路などによって構成される。

【００６５】

図４の回路の動作を説明する。最初に、サーバ１と通信したときやコンテンツ、ライセンスをダウンロードしたときの動作を説明する。

【００６６】

サーバ１と接続したとき、サーバ１から日時データを日時データ取得・作成部２１で取得する。取得した日時データはライセンスフォーマット中のコンテンツ鍵の領域に組込み可能にするために、日時データは例えば図５に例示する１６バイトのデータ構成とされる。日時が２００２年１０月１０日（木）１５時３０分４５秒００のとき、この日時データを１６進で表すと、“０７Ｄ２　０００Ａ　０００Ａ　０００４　０００Ｆ　００１Ｅ　００２Ｄ　００００　ｈ”となる。

【００６７】

暗号化部２２で、日時データ取得・作成部２１で作成した１６バイトの日時データをＡＥＳ方式で暗号する。暗号化する鍵はカード固有のシリアル番号を使用する。

【００６８】

ライセンス作成部２３で、暗号化した日時データをライセンス内のコンテンツ鍵の部分に埋め込み、１つのライセンスを作成する。作成されたライセンスは、セキュア領域アクセス部２４によってメモリカードのセキュア領域に書き込まれる。セキュア領域が１２８個のライセンスを記録できる場合には、最後の１２８番目に日時データを含むライセンスを書き込む。セキュア領域１４Ａに対する書き込みは前記書き込み認証を受けて可能にされる。

【００６９】

次に利用制限判定処理の動作について説明する。セキュア領域アクセス部２４で、セキュア領域１４Ａから暗号化されている日時データが含まれているセキュアライセンスを読み出す。セキュア領域に対するリードアクセスは前記読み出し認証を受けて可能にされる。日時データ取出し部２５で、読み出したライセンスから暗号化されている日時データ１６バイトを取出す。復号化部２６で、１６バイトの日時データをＡＥＳ方式で復号する。復号化する鍵は暗号化したときと同じカード固有のシリアル番号を使用する。次いで、端末内時計取得部２８で、端末内の日時を取得する。利用制限判定部２７で、利用期限、端末の日時データ、カードの日時データを用いて期限が切れていないのか、不正な操作が行われていないのかを判定する。

【００７０】
次に日時データの更新処理動作について説明する。カード内には電源がないため、カード自身では日時データを更新することはできない。したがって、上記で説明したようにサーバーとの接続時やコンテンツの再生、表示時（利用制限判定処理のとき）に日時データを更新する。しかし、サーバーと接続をしない場合やコンテンツの再生表示を行わない場合には長時間更新されない場合がある。日時データを更新するタイミングは、前述のアクセス開始時と終了時の他に、メモリカードがデータ端末に挿入されたときと離脱されたとき、或はメモリカードがデータ端末に装着されている状態でデータ端末の電源オンが指示されたときと、電源オフが指示されたとき等であってよい。データ端末の電源をオフにするときには、マイクロコンピュータ内部のタイマーで測定した時間をカードに記録されている日時データに加算することにより更新すればよい。

【００７１】
図６には前記メモリカード１５に内蔵された前記利用期限判定部１６の具体例が示される。前記利用期限判定部１６はマイクロコンピュータ３０によって構成される。図６ではマイクロコンピュータ３０は外部インタフェースコントローラ３１及びメモリコントローラ３２と共にカードコントローラを構成する。図６にはマイクロコンピュータ３０をその一部の機能である利用期限判定部１６を構成する機能ブロックによって図示している。マイクロコンピュータ３０によって実現される図示された機能ブロックは、暗号化部３３、ライセンス作成部３４、日時データ取り出し部３５、復号部３６、利用期限取り出し部３７、及び利用制限判定部３８である。

【００７２】
外部インタフェースコントローラ３１はマイクロコンピュータ３０の指示に従って所定のメモリカードインタフェース仕様に準拠した外部インタフェース制御を行なう。メモリコントローラ３２はマイクロコンピュータ３０の指示に従って不揮発性メモリ１４に対する消去、書き込み及び読み出しのアクセス制御を行なう。

【００７３】
特に図示はしないが、マイクロコンピュータ３０は中央処理装置、浮動小数点演算ユニット、それらの処理プログラムを保有するＲＯＭ（リード・オンリ・メモリ）、中央処理装置のワーク領域などに利用されるＲＡＭ（ランダム・アクセス・メモリ）、リアルタイムクロック回路、タイマ、及び入出力回路などによって構成される。マイクロコンピュータ３０は前記利用期限判定部１６を実現すると共に、その動作プログラムに従って認証のための演算処理や不揮発性メモリ１４をアクセスするためのアドレス演算処理等を行なう機能を有する。

【００７４】
不揮発性メモリ１４はセキュア領域（アクセス制限領域）１４Ａと非セキュア領域（アクセス非制限領域）１４Ｂを有する。セキュア領域１４Ａに対する書き込みアクセスはメモリカード１５内の証明情報に対しメモリカード外部例えば端末装置２０やサーバ１による認証を受けて可能にされる。外部からセキュア領域１４Ａに対する読み出しは外部から与えられる証明情報に対して認証を得ることを条件に許可される。メモリカード１５内の前記証明情報は、そのメモリカード１５が図２及び図６で説明した利用期限判定機能などを備えたメモリカードであり、その他のメモリカードと区別可能な情報を含んでいる。

【００７５】
この例では、カード日時データ暗号化部３３で暗号化した後、これをライセンス作成部３４でセキュアライセンスに埋め込み、メモリコントローラ３２を介して不揮発性メモリ１４のセキュア領域１４Ａに記録するようになっている。特に制限されないが、コンテンツの利用期限もセキュアライセンスが保有する。

【００７６】
図２のダウンロード再生部１０がコンテンツデータやライセンスをサーバからダウンロードしたときサーバ１から日時データ（ダウンロード日時データ）が取得される。日時データはコンテンツライセンスに付随する。取得した日時データのフォーマットは図５に例示

されるように、１６バイトのデータで構成される。

【００７７】

前記暗号化部３３はサーバから取得した前記日時データを受取って暗号化する。暗号化方式は、特に制限されないが、コンテンツの暗号化復号処理で用いているのと同じＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式を用いる。日時データを暗号化する鍵はメモリカード固有の属性情報、例えば、カードのシリアル番号等を用いる。

【００７８】

前記ライセンス作成部３４は、取得して暗号化した日時データを例えばライセンスフォーマット中のコンテンツ鍵の部分に埋め込んでセキュアライセンスを作成する。

【００７９】

作成されたセキュアライセンスはメモリコントローラ３２を介して不揮発性メモリのセキュア領域１４Ａに書き込まれる。セキュア領域１４Ａへの書き込みには前記書き込み認証が必要とされる。前記日時データ取り出し部３６は暗号化された日時データが含まれるセキュアライセンスがセキュア領域１４Ａから読み出されたとき、そこから暗号化された日時データを抽出する。利用期限取り出し部３７はセキュアライセンスがセキュア領域１４Ａから読み出されたとき、そこから利用期限データを抽出する。セキュア領域１４Ａの読み出しには前記読み出し認証が必要とされる。

【００８０】

復号部３６はセキュアライセンスから取出した暗号化された日時データをＡＥＳで復号する。復号する鍵は暗号部３３で用いた鍵と同じものを使用する。

【００８１】

前記利用制限判定部２７は、前述の如く、利用期限が切れていないのかを判定すると共に、データ端末４内の時計１２がユーザーによって操作されていないかを判定する。その判定内容は図２を参照して既に説明した。操作されていると判定したら、セキュア領域１４Ａ内のライセンスを全て消去する。

【００８２】

図６の回路の動作を説明する。最初に、サーバ１と通信したときやコンテンツ、ライセンスをダウンロードしたときの動作を説明する。

【００８３】

データ端末装置４がサーバ１に接続したとき、サーバ１からの日時データを外部インタフェースコントローラ３１を介して入力する。併せて再生期限日データも入力する。再生期限日は例えば再生ライセンスに含まれるものを利用する。入力した日時データは図５に例示する１６バイトのデータ構成とされる。日時データは暗号化部３３によって例えばＡＥＳ方式で暗号される。暗号化する鍵はカード固有のシリアル番号を使用する。

【００８４】

ライセンス作成部３４で、暗号化した日時データをライセンス内のコンテンツ鍵の部分に埋め込み、セキュアライセンスを作成する。作成されたライセンスは、メモリコントローラ３２を介してメモリカード１４のセキュア領域１４Ａに書き込まれる。セキュア領域が１２８個のライセンスを記録できる場合には、最後の１２８番目に前記セキュアライセンスを書き込む。セキュア領域１４Ａに対する書き込みは前記書き込み認証を受けて可能にされる。

【００８５】

次に利用制限判定処理の動作について説明する。メモリコントローラ３２を介してセキュア領域１４Ａからセキュアライセンスが読み出される。セキュア領域に対するリードアクセスは前記読み出し認証を受けて可能にされる。日時データ取出し部３５で、読み出したライセンスから暗号化されている日時データ１６バイトを取出す。利用期限取り出し部３７では利用期限を取出す。復号部３６で、１６バイトの日時データをＡＥＳ方式で復号する。復号する鍵は暗号化したときと同じカード固有のシリアル番号を使用する。次いで、端末内の日時を取得する。利用制限判定部３８で、利用期限、端末の日時データ、カード

の日時データを用いて期限が切れていないのか、不正な操作が行われていないのかを判定する。

【００８６】

次に日時データの更新処理動作について説明する。カード内には電源がないため、カード自身では日時データを更新することはできない。したがって、上記で説明したようにサーバーとの接続時やコンテンツの再生、表示時（利用制限判定処理のとき）に日時データを更新する。しかし、サーバーと接続をしない場合やコンテンツの再生表示を行わない場合には長時間更新されない場合がある。日時データを更新するタイミングは、前述のアクセス開始時と終了時の他に、メモリカードがデータ端末に挿入されたときと離脱されたとき、或はメモリカードがデータ端末に装着されている状態でデータ端末の電源オンが指示されたときと、電源オフが指示されたとき等であってよい。データ端末の電源をオフにするときには、マイクロコンピュータ内部のタイマーで測定した時間をカードに記録されている日時データに加算することにより更新すればよい。

【００８７】

更新処理を、更に別のタイミングで行なってもよい。即ち、メモリカードがファイルメモリ方式によるセクタ単位で分割してデータアクセスを行なう場合、アクセス開始時の前記アクセス判定動作においてアクセス可と判定された後は、後続セクタのアクセス毎又は所定の複数アクセス毎に前記アクセス判定動作を行なってもよい。このようにセクタ単位で分割されたデータのアクセスに対するアクセス判定動作において、第２回目以降のアクセス判定動作では、時刻情報が前記アクセス期限情報により示されるアクセス期限より後であってもアクセス可と判定するようにしてよい。アクセス判定動作を何回も行なうとき、利用情報の再生途中などで期限が到来して再生が中断される不都合を簡単に解消することができる。

【００８８】

図７には再生ライセンスのフォーマットが例示され、図８にはセキュアライセンスのフォーマットが例示される。コンテンツＩＤはコンテンツ毎にユニークに割り当てられる識別子である。トランザクションＩＤはトランザクション毎にユニークな識別子である。トランザクションＩＤには再生可能回数（ライセンスを読み出せる回数）、移動可能回数（ライセンスを移動できる回数）、及びセーフレベル（保護強度）の識別子を含む。メディアアクセス条件はメディア内部で強制可能なアクセス条件である。コンテンツ鍵はコンテンツを暗号化するときに用いた鍵であり、コンテンツを復号する時に利用する。デコーダアクセス条件は再生用デコーダの内部で強制可能なアクセス条件を示す。デコーダアクセス条件には再生サイズ（１つのライセンスで再生可能なコンテンツサイズ）と利用期限（利用可能な期限）とを含む。拡張メディアアクセス条件は証明書認証、ＰＩＮ認証を行うか否かを示すフラグとされる。再生ライセンスはコンテンツ鍵を有しているが、セキュアライセンスは、その再生ライセンスのコンテンツ鍵をカード日時データに入れ替えて構成される。

【００８９】

証明書認証例えばセキュア領域の書き込み認証を受けるための証明情報、そしれＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）による個人認証を行なうためのＰＩＮは不揮発性メモリ１４に格納されている。

【００９０】

図９にはライセンスの書き込み時の認証（書き込み認証）処理手順が例示される。先ず、証明認証を行なうか否かが判定され（Ｓ１）、行なう場合にはメモリカードから認証情報と公開暗号鍵を有する証明書（メディアクラス証明書）を読み出し（Ｓ２）、これをサーバに送信する（Ｓ３）。サーバはその証明書を検証し（Ｓ４）、それによって認証されれば、メモリカードのセキュア領域に対する再生ライセンス及びセキュアライセンスの書き込みが許容される（Ｓ５）。前記メディアクラス証明書は、例えば前記利用期限判定機能などを備えたメモリカード１５を、当該機能を備えていない他のメモリカードと区別することができる証明情報を有している。

【００９１】
図１０にはライセンスの読み出し時の認証（読み出し認証）処理手順が例示される。先ず、証明認証を行なうか否かが判定され（Ｓ１１）、行なう場合にはデータ端末からメモリカードに認証情報と公開暗号鍵を有する証明書（デコーダクラス証明書）を送信する（Ｓ１２）。メモリカードはその証明書を検証し（Ｓ３）、それによって認証されれば、メモリカードのセキュア領域から再生ライセンス及びセキュアライセンスの読み出しが許容される（Ｓ１４）。処理Ｓ１１の判別で証明認証を行なわない場合には、ＰＩＮ認証を行なうかの判別を行ない（Ｓ１５）、行なう場合にはデータ端末装置からＰＩＮをメモリカードに送信し（Ｓ１６）、メモリカード内でＰＩＮの検証を行なう。ＰＩＮが正当であればライセンスの読み出しを行なう（Ｓ１４）。ＰＩＮが不当である場合、ＰＩＮ認証を行なわない場合、証明認証を得られない場合にはそのまま処理を終了する。

【００９２】
図１１には利用期限付コンテンツの再生処理フローの一例が示される。再生ライセンスを利用して利用期限付コンテンツの再生を行なう場合、先ず利用期限判定処理Ｒ２１を行ない、再生可能であればカード日時データ更新処理Ｒ２２を行ない、利用期限付コンテンツの再生終了を判定し（Ｓ２３）、終了でなければ所定のインターバル毎にカード日時データ更新処理Ｒ２２を繰返す。再生終了を判別すると、最後にカード日時更新処理Ｒ２２を行なって終了する。

【００９３】
図１２には利用期限判定処理Ｒ２１の詳細な一例が示される。データ端末装置の日時情報を取得し、端末日時データを作成する（Ｓ３１）。次に、必要な証明認証又はＰＩＮ認証を行なってメモリカードから、カード日時データを取得し（Ｓ３２）、ライセンスから利用期限を取得する（Ｓ３３）。利用制限とカード日時データを比較し（Ｓ３４）、利用期限≦カード日時データの場合には期限切れと判定して処理を終了する。利用期限＞カード日時データの場合には端末日時データとカード日時データを比較する（Ｓ３５）。端末日時データ≦カード日時データの場合には端末日時データが不正と判定し、メモリカードが保有する全てのライセンスの消去を行なう（Ｓ３６）。端末日時データ＞カード日時データの場合にはカードの日時データを端末の日時データに更新する（Ｓ３７）。

【００９４】
図１３にはカード日時データ更新処理Ｒ２２の詳細な一例が示される。データ端末装置の日時情報を取得し、端末日時データを作成する（Ｓ４１）。次に、必要な証明認証又はＰＩＮ認証を行なってメモリカードから、カード日時データを取得する（Ｓ４２）。端末日時データとカード日時データを比較する（Ｓ４３）。端末日時データ≦カード日時データの場合には端末日時データが不正と判定し、メモリカードが保有する全てのライセンスの消去を行なう（Ｓ４４）。端末日時データ＞カード日時データの場合にはカードの日時データを端末の日時データに更新する（Ｓ４５）。図１３の処理は図１２に対して、ライセンスから利用期限を取得せず、利用期限≦カード日時データの場合に期限切れと判定して処理を終了することを行なわない。したがって、利用期限付コンテンツの再生途中などで再生期限が到来して再生が中断される不都合を解消することができる。

【００９５】
図１４には期限付きデータの再生端末装置４０が示される。同図に示される再生端末装置４０は再生部４１を有し、図２の端末装置４に対しコンテンツデータとライセンスのダウンロード機能が省かれた再生専用器として構成される。図１１乃至図１３に示されるコンテンツ再生処理を行なうことができる。

【００９６】
図１５にはダウンロード端末装置４５が示される。同図に示されるダウンロード端末装置４５は図２で説明した端末装置４におけるダウンロード再生部１０に対しコンテンツデータの再生機能が省かれた、コンテンツデータとライセンスのダウンロード専用端末装置とされる。ダウンロード専用端末装置４５は、ホストインタフェース部４６、メモリカードインタフェース部４７、及びデータ処理部４８を有し、メモリカードインタフェース部４

７に装着されたメモリカード１５に、コンテンツを復号するためのコンテンツライセンス、コンテンツに対するアクセス制限を行なう再生期限データ、及びカード日時データを初期的に格納する。前記データ処理部４８は、前記コンテンツライセンスの受領要求と共にメモリカード１５が保有する証明情報をホストインタフェース部４６から外部に出力し、これに応答して例えばサーバ１からホストインタフェース部４６に返される情報を受領してメモリカードインタフェース部４７から前記メモリカード１５に格納する。前記受領する情報は、コンテンツの復号に利用されるコンテンツ鍵、コンテンツに対するアクセス制限を行なう再生期限データ、及びカード日時データを含む。前記証明情報は利用期限判定機能を有するメモリカード１５であることを表す情報である。このダウンロード端末装置を用いてメモリカードにコンテンツ及びその再生ライセンスを頒布もしくは販売することにより、対象となる記憶媒体が前記利用期限判定機能を有するメモリカード１５に限定されるから、期限付きコンテンツデータに対する不正アクセスの抑止を支援することができる。

【００９７】

図１５の構成はネットワークに接続する端末装置としての構成に限定されない。特に図示はしないが、ダウンロード端末装置４５それ自体がコンテンツサーバであってもよく、見方を変えればスタンドアロンの頒布端末装置となる。

【００９８】

以上本発明者によってなされた発明を実施形態に基づいて具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【００９９】

例えば、今まで説明したダウンロード機能を有するデータ端末はコンテンツ及びコンテンツライセンスの双方をダウンロードして頒布する機能を有するものとして説明したが、本発明はそれに限定されず、コンテンツライセンスだけのダウンロード若しくは頒布であってもよい。また、再生機能を有するデータ端末装置において、コンテンツはライセンスと同じメモリカードに格納されていなくてもよい場合が有る。その場合、コンテンツデータはＣＤ－ＲＯＭやＤＶＤ－ＲＡＭ等のリムーバブルディスクドライブを用いてアクセスするようにしてもよい。或はハードディスクドライブからアクセスするようにしてもよい。

【０１００】

また、上記説明では、日時データを暗号化してライセンスに埋め込んでセキュア領域に記録する例を示したが、暗号化を省いても良い。日時データを暗号化しないでライセンスに埋め込むため処理量が少なくて済む。また、日時データを暗号化して非セキュア領域に記録してもよい。セキュア領域を持たない記憶媒体にも使用できる。また、日時データを暗号化せず且つ非セキュア領域に記録してもよい。セキュア領域を持たない記憶媒体にも使用でき、しかも、ＡＥＳの暗号／復号処理をする必要がないため最小の構成で実現できる。しかし、ユーザーにより日時データを操作される可能性が大きいことに注意を要する。

【０１０１】

【発明の効果】

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

【０１０２】

すなわち、メモリカード等の不揮発性記憶装置にアクセス時間情報のような日時データを更新して記録し、しかもアクセス時間情報の更新はアクセス終了時点だけでなく複数時点で行なうから、利用情報の再生終了直前に電源が遮断されても少なくとも１回のアクセス時間情報の更新は保証される。期限付き利用情報の不正再生抑制機能を不揮発性記憶装置が備えることにより、再生装置を変えても依然として不正アクセス抑止機能を働かせることが容易である。

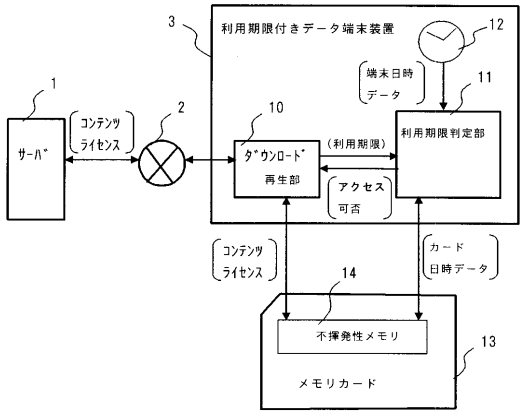
【図面の簡単な説明】

【図１】本発明を適用したコンテンツデータ配信システムのブロック図である。

【図２】本発明を適用したコンテンツデータ配信システムに別のデータ端末装置が接続されている例を示す説明図である。
【図３】端末日時データに基づいて更新されるカード日時データによる利用制限の概要を例示する説明図である。
【図４】図１における利用期限判定部と端末内部時計の具体例を示すブロック図である。
【図５】日時データのフォーマットを例示する説明図である。
【図６】図２のメモリカードに内蔵された利用期限判定部の具体例を示すブロック図である。
【図７】再生ライセンスのフォーマットを例示する説明図である。
【図８】セキュアライセンスのフォーマットを例示する説明図である。
【図９】ライセンスの書き込み時の認証（書き込み認証）処理手順を例示するフローチャートである。
【図１０】ライセンスの読み出し時の認証（読み出し認証）処理手順を例示するフローチャートである。
【図１１】利用期限付コンテンツの再生処理の一例を示すフローチャートである。
【図１２】図１１の利用期限判定処理Ｒ２１の詳細を例示するフローチャートである。
【図１３】図１１のカード日時データ更新処理Ｒ２２の詳細を例示するフローチャートである。
【図１４】期限付きデータの再生端末装置を例示するブロック図である。
【図１５】ダウンロード端末装置を例示するブロック図である。
【符号の説明】
１　サーバ
２　ネットワーク
３　データ端末装置
４　データ端末装置
１０　ダウンロード生成部
１１　利用期限判定部
１２　端末内部時計
１３　メモリカード
１４　不揮発性メモリ
１４Ａ　セキュア領域（アクセス制限領域）
１４Ｂ　非セキュア領域（アクセス非制限領域）
１５　メモリカード
１６　利用期限判定部
２０　マイクロコンピュータ
３０　マイクロコンピュータ
４０　再生端末装置
４１　再生部
４５　ダウンロード専用端末装置
４６　ホストインタフェース部
４７　メモリカードインタフェース部
４８　データ処理部

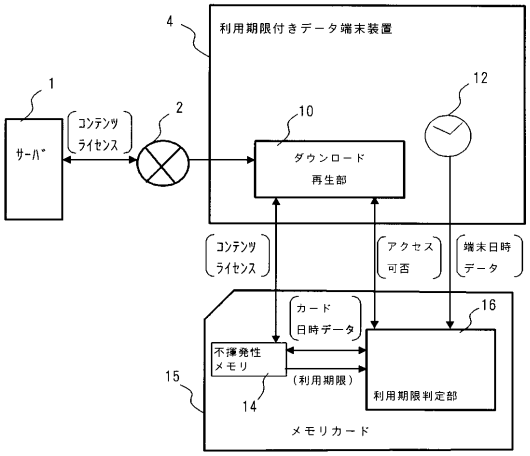
【図１】

図１



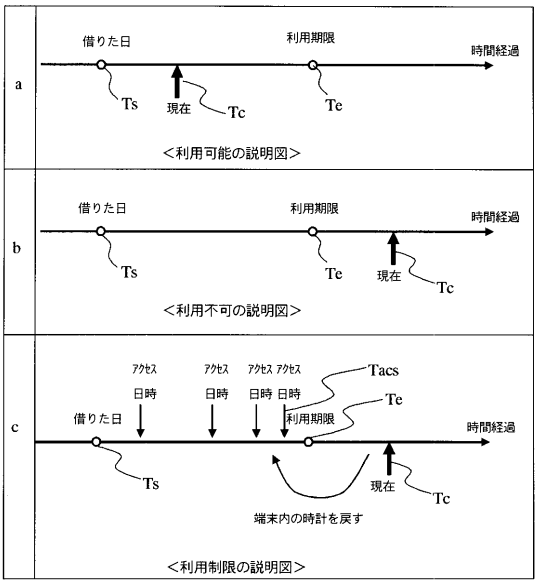
【図２】

図２



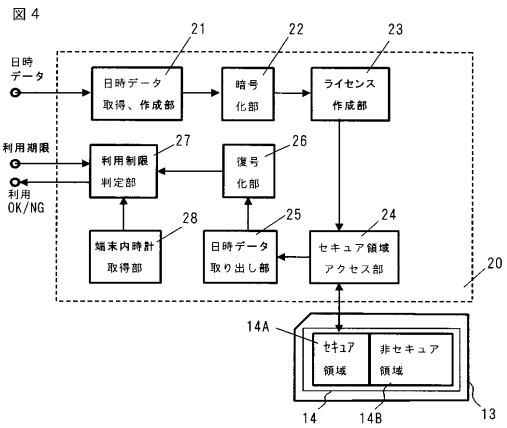
【図３】

図３



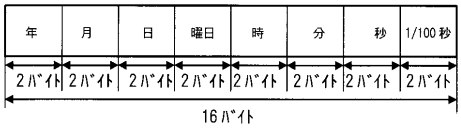
【図４】

図４



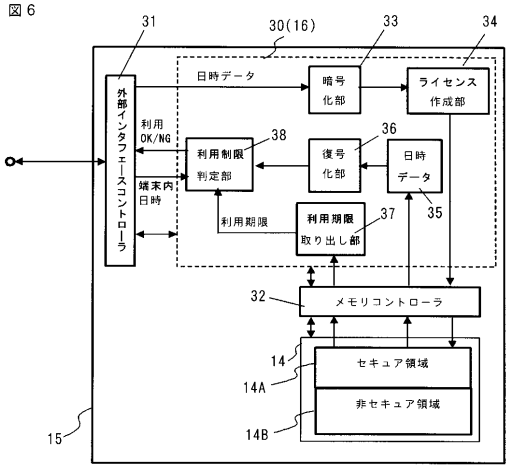
【図５】

図５



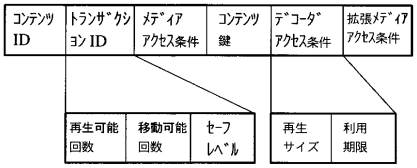
【図６】

図６



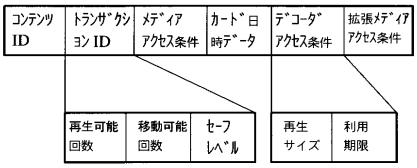
【図７】

図７



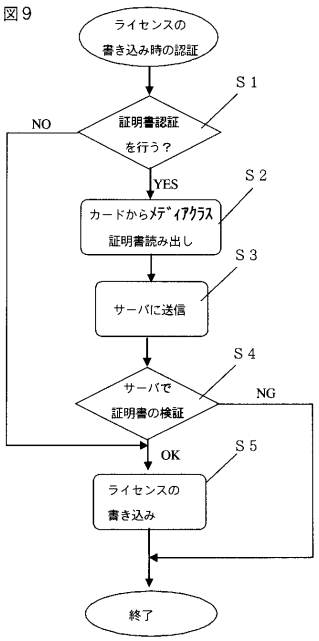
【図８】

図８



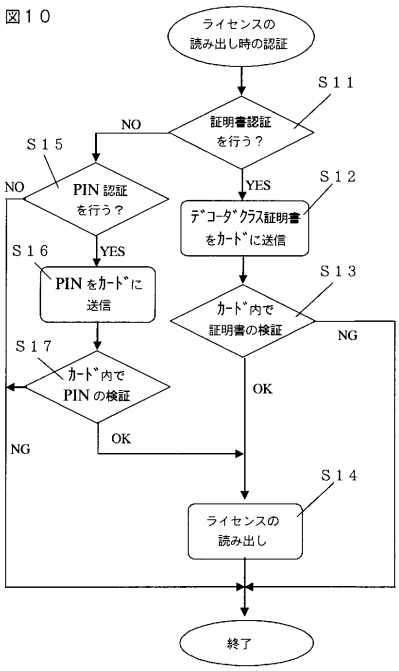
【図９】

図９



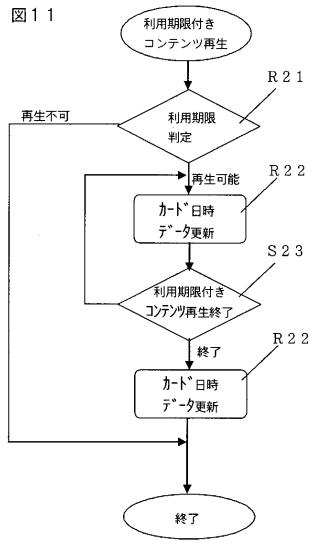
【図１０】

図１０



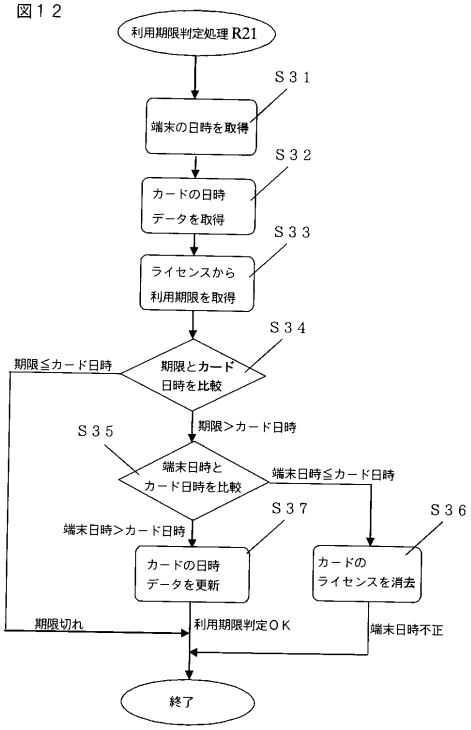
【図１１】

図１１



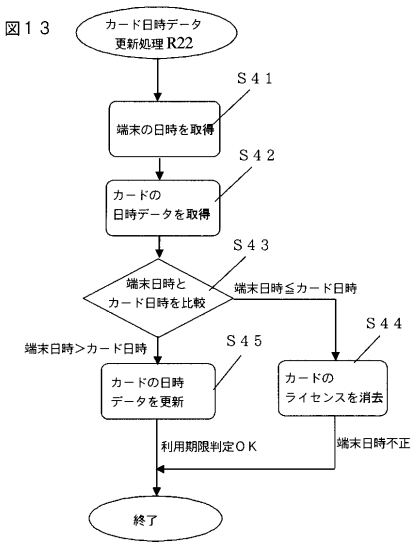
【図１２】

図１２



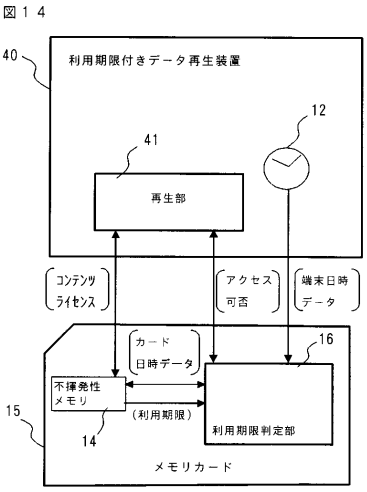
【図１３】

図１３



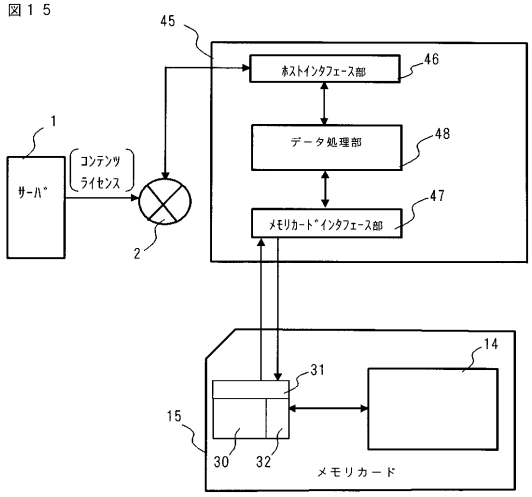
【図１４】

図１４



【図１５】

図１５


45
ﾎｽﾄｲﾝﾀﾌｪｰｽ部
46
1
ｻｰﾊﾞ
ｺﾝﾃﾝﾂ
ﾗｲｾﾝｽ
データ処理部
48
47
ﾒﾓﾘｶｰﾄﾞｲﾝﾀﾌｪｰｽ部
2
14
31
15
30
32
メモリカード

フロントページの続き

Ｆターム(参考) 5B035 BB09 BB11 CA11 CA38
5B058 CA13 CA27 KA01 KA04 KA35