(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5664236号
(P5664236)

(45)発行日　平成27年2月4日(2015.2.4)　(24)登録日　平成26年12月19日(2014.12.19)

(51)Int.Cl.		F I		
G06K 19/073	(2006.01)	G06K	19/00	P
G06K 17/00	(2006.01)	G06K	17/00	T
G06F 21/62	(2013.01)	G06F	21/24	166C
H04L 9/32	(2006.01)	H04L	9/00	675A

請求項の数 17　(全 28 頁)

(21)出願番号　特願2010-294477 (P2010-294477)
(22)出願日　平成22年12月29日 (2010.12.29)
(65)公開番号　特開2012-141821 (P2012-141821A)
(43)公開日　平成24年7月26日 (2012.7.26)
審査請求日　平成25年11月12日 (2013.11.12)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(74)代理人　110000763
特許業務法人大同特許事務所

最終頁に続く

(54)【発明の名称】データ記憶装置、情報処理装置、および情報処理方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
データ記憶領域と制御部を有するフラッシュメモリ部と、
前記フラッシュメモリ部に対するデータ記録と読み出し制御を実行するコントローラ部を有し、
前記コントローラ部が読み出し処理を行うコントローラＩＤと、
前記フラッシュメモリ部の制御部が読み出し処理を行うフラッシュＩＤを記録したメモリ部を有し、
前記コントローラ部は、外部装置からのコントローラＩＤ読み出し要求に応じて、コントローラＩＤを外部装置に対して出力し、
前記フラッシュメモリ部の制御部は、外部装置からのフラッシュＩＤ読み出し要求に応じて、フラッシュＩＤを外部装置に対して出力し、
前記コントローラ部は、前記コントローラＩＤおよび前記フラッシュＩＤの２つのＩＤに基づいて生成された検証値を外部装置から入力して前記データ記憶領域に格納する処理を実行するデータ記憶装置。
【請求項２】
前記コントローラ部は、
認証処理を実行する認証機能を有し、前記外部装置との認証処理の成立を条件として前記コントローラＩＤを外部装置に出力する処理を実行する請求項１に記載のデータ記憶装置。

【請求項３】
前記フラッシュメモリ部の制御部は、
認証処理を実行する認証機能を有し、前記外部装置との認証処理の成立を条件として前記フラッシュＩＤを外部装置に出力する処理を実行する請求項１に記載のデータ記憶装置。
【請求項４】
メモリカードに対するコンテンツ記録を実行する情報処理装置であり、
前記メモリカードに対するコンテンツ記録処理を実行するデータ処理部を有し、
前記データ処理部は、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を生成して前記メモリカードに記録する処理を実行する情報処理装置。
【請求項５】
前記データ処理部は、
前記検証値として、前記コントローラＩＤとフラッシュＩＤを含むデータに対するＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成して前記メモリカードに記録する処理を実行する請求項４に記載の情報処理装置。
【請求項６】
前記データ処理部は、
前記検証値として、前記コントローラＩＤに対するＭＡＣと、前記フラッシュＩＤに対するＭＡＣを個別に生成して前記メモリカードに記録する処理を実行する請求項４に記載の情報処理装置。
【請求項７】
前記データ処理部は、
前記検証値として、前記コントローラＩＤとフラッシュＩＤを含むデータに対する署名データ（トークン）を生成して前記メモリカードに記録する処理を実行する請求項４に記載の情報処理装置。
【請求項８】
前記データ処理部は、
前記検証値として、前記コントローラＩＤに対する署名データと、前記フラッシュＩＤに対する署名データを個別に生成して前記メモリカードに記録する処理を実行する請求項４に記載の情報処理装置。
【請求項９】
メモリカードに記録されたコンテンツを再生する情報処理装置であり、
前記メモリカードに記録されたコンテンツを読み出して再生するデータ処理部を有し、
前記データ処理部は、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を算出し、前記メモリカードに予め記録された照合用検証値との比較を実行して照合が成立したことを条件として、前記メモリカードに記録されたコンテンツの再生処理を実行する情報処理装置。
【請求項１０】
前記データ処理部は、
前記検証値の算出処理において、前記コントローラＩＤとフラッシュＩＤを含むデータに対するＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を算出する請求項９に記載の情報処理装置。
【請求項１１】

前記データ処理部は、
前記検証値の算出処理において、前記コントローラＩＤに対するＭＡＣと、前記フラッシュＩＤに対するＭＡＣを個別に算出する請求項９に記載の情報処理装置。
【請求項１２】
前記データ処理部は、
前記検証値の算出処理において、前記コントローラＩＤとフラッシュＩＤを含むデータに対する署名データ（トークン）を算出する請求項９に記載の情報処理装置。
【請求項１３】
前記データ処理部は、
前記検証値の算出処理において、前記コントローラＩＤに対する署名データと、前記フラッシュＩＤに対する署名データを個別に算出する請求項９に記載の情報処理装置。
【請求項１４】
メモリカードに対するコンテンツ記録を実行する情報処理装置において実行する情報処理方法であり、
前記情報処理装置のデータ処理部が、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を生成して前記メモリカードに記録する処理を実行する情報処理方法。
【請求項１５】
メモリカードに記録されたコンテンツを再生する情報処理装置において実行する情報処理方法であり、
前記情報処理装置のデータ処理部が、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を算出し、前記メモリカードに予め記録された照合用検証値との比較を実行して照合が成立したことを条件として、前記メモリカードに記録されたコンテンツの再生処理を実行する情報処理方法。
【請求項１６】
メモリカードに対するコンテンツ記録を実行する情報処理装置に情報処理を実行させるプログラムであり、
前記情報処理装置のデータ処理部に、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得させ、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を生成して前記メモリカードに記録する処理を実行させるプログラム。
【請求項１７】
メモリカードに記録されたコンテンツを再生する情報処理装置に情報処理を実行させるプログラムであり、
前記情報処理装置のデータ処理部に、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得させ、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を算出し、前記メモリカードに予め記録された照合用検証値との比較を実行して照合が成立したことを条件として、前記メモリカードに記録されたコンテンツの再生処理を実行させるプログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、データ記憶装置、情報処理装置、および情報処理方法、並びにプログラムに関する。特に、コンテンツの不正利用の防止構成を実現するデータ記憶装置、情報処理装置、および情報処理方法、並びにプログラムに関する。
【背景技術】
【０００２】
昨今、データ記録媒体として、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）や、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）、あるいはフラッシュメモリなど、様々なメディアが利用されている。特に、昨今は、大容量のフラッシュメモリを搭載したメモリースティック（登録商標）、ＳＤカード、ＵＳＢメモリなどのメモリカードの利用が盛んになっている。ユーザは、このような様々な情報記録媒体（メディア）に音楽や映画などのコンテンツを記録して再生装置（プレーヤ）に装着してコンテンツの再生を行うことができる。
【０００３】
また、近年、ネットワークを介したコンテンツの流通が盛んになり、ユーザによるコンテンツ購入処理の形態は、コンテンツを予め記録したディスクの購入処理から、ネットワーク接続したサーバからダウンロードする処理に次第にシフトしている。
【０００４】
具体的なコンテンツ購入形態としては、ＲＯＭディスク等のメディアの購入を行う処理の他、例えば、以下のようなコンテンツ購入形態がある。
（ａ）ネットワーク接続可能な端末やＰＣ等のユーザ装置を利用してコンテンツ提供サーバに接続して、コンテンツをダウンロードして購入するＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓｅｌｌ　Ｔｈｒｏｕｇｈ）。
（ｂ）コンビニや、駅等の公共スペースに設置された共用端末を利用して、ユーザのメディア（メモリカード等）にコンテンツを記録するＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎ　Ｄｅｍａｎｄ）。
【０００５】
このように、ユーザは、コンテンツ記録用のメモリカードなどのメディアを有していれば、様々なコンテンツ提供プロバイダ等のコンテンツソースから自由に様々なコンテンツを選択購入し、自分のメディアに記録することができる。
なお、ＥＳＴ、ＭｏＤ等の処理については、例えば特許文献１（特開２００８－９８７６５号公報）に記載されている。
【０００６】
しかし、音楽データ、画像データ等の多くのコンテンツは、その作成者あるいは販売者に著作権、頒布権等が保有されている。従って、ユーザにコンテンツを提供する場合には、一定の利用制限、すなわち正規な利用権を持つユーザのみにコンテンツの利用を許諾し、許可のないコピー等の無秩序な利用が行われないような制御を行うのが一般的となっている。
【０００７】
コンテンツ利用制御の規定の１つにＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ）がある。これは、例えばメモリカードなどのデータ記録メディアにコンテンツを暗号化して記録し、さらにメディア固有のＩＤ（メディアＩＤ）に基づく検証値を記録し、メディアからのコンテンツの読み出し時にこの検証値に基づく検証処理を実行させてコンテンツの利用制御を実行する制御構成である。ここでメディアＩＤは、各メディア個別に異なるＩＤが記録されていることが前提である。
【０００８】
しかし、例えばＳＤカード等のメモリカードの１枚ごとに異なる固有ＩＤを記録するという管理が確実に行われているとは言えないのが現状である。

図１に一般的なメモリカードの製造シーケンスを示す。図１に示すようにメモリカード１０には、コントローラ部１１とフラッシュメモリ部１２を有する。
コントローラ部１１は、コントローラを製造するコントローラ製造会社（コントローラベンダー）２０において製造される。
また、フラッシュメモリ部１２は、フラッシュメモリ部を製造するフラッシュメモリ製造会社（フラッシュメモリベンダー）３０において製造される。
それぞれのベンダーの製造したパーツを最終工程で組み立ててメディア１０を完成させるのが一般的な工程となる。
【０００９】
メディアＩＤは、コントローラ部１１の製造者であるコントローラベンダー２０の管理の下に記録されることが多い。コントローラベンダー２０側において正しい管理の下でメディアＩＤの記録が実行されれば問題はないが、正しい管理がなされない場合、例えば同じメディアＩＤを持つ複数のメディアが大量に生産されユーザに供給される恐れもある。
【００１０】
このような事態が発生すると、上述のＣＰＲＭに基づくコンテンツ管理、すなわちメディアＩＤが各メディア固有の値（固有値）であることに依存したコンテンツ利用制御が不可能となる。結果として、コンテンツの不正利用が行われる可能性を引き起こすという問題を発生させる。
【先行技術文献】
【特許文献】
【００１１】
【特許文献１】特開２００８－９８７６５号公報
【発明の概要】
【発明が解決しようとする課題】
【００１２】
本発明は、例えば上記問題点に鑑みてなされたものであり、メディアＩＤを利用したコンテンツの利用制御を持つ構成において、より厳格なコンテンツ利用制御を実現するデータ記憶装置、情報処理装置、および情報処理方法、並びにプログラム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】
【００１３】
本発明の第１の側面は、
データ記憶領域と制御部を有するフラッシュメモリ部と、
前記フラッシュメモリ部に対するデータ記録と読み出し制御を実行するコントローラ部を有し、
前記コントローラ部が読み出し処理を行うコントローラＩＤと、
前記フラッシュメモリ部の制御部が読み出し処理を行うフラッシュＩＤを記録したメモリ部を有し、
前記コントローラ部は、外部装置からのコントローラＩＤ読み出し要求に応じて、コントローラＩＤを外部装置に対して出力し、
前記フラッシュメモリ部の制御部は、外部装置からのフラッシュＩＤ読み出し要求に応じて、フラッシュＩＤを外部装置に対して出力するデータ記憶装置にある。
【００１４】
さらに、本発明のデータ記憶装置の一実施態様において、前記コントローラ部は、認証処理を実行する認証機能を有し、前記外部装置との認証処理の成立を条件として前記コントローラＩＤを外部装置に出力する処理を実行する。
【００１５】
さらに、本発明のデータ記憶装置の一実施態様において、前記フラッシュメモリ部の制御部は、認証処理を実行する認証機能を有し、前記外部装置との認証処理の成立を条件として前記フラッシュＩＤを外部装置に出力する処理を実行する。

【００１６】
さらに、本発明の第２の側面は、
メモリカードに対するコンテンツ記録を実行する情報処理装置であり、
前記メモリカードに対するコンテンツ記録処理を実行するデータ処理部を有し、
前記データ処理部は、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を生成して前記メモリカードに記録する処理を実行する情報処理装置にある。
【００１７】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値として、前記コントローラＩＤとフラッシュＩＤを含むデータに対するＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成して前記メモリカードに記録する処理を実行する。
【００１８】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値として、前記コントローラＩＤに対するＭＡＣと、前記フラッシュＩＤに対するＭＡＣを個別に生成して前記メモリカードに記録する処理を実行する。
【００１９】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値として、前記コントローラＩＤとフラッシュＩＤを含むデータに対する署名データ（トークン）を生成して前記メモリカードに記録する処理を実行する。
【００２０】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値として、前記コントローラＩＤに対する署名データと、前記フラッシュＩＤに対する署名データを個別に生成して前記メモリカードに記録する処理を実行する。
【００２１】
さらに、本発明の第３の側面は、
メモリカードに記録されたコンテンツを再生する情報処理装置であり、
前記メモリカードに記録されたコンテンツを読み出して再生するデータ処理部を有し、
前記データ処理部は、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を算出し、前記メモリカードに予め記録された照合用検証値との比較を実行して照合が成立したことを条件として、前記メモリカードに記録されたコンテンツの再生処理を実行する情報処理装置にある。
【００２２】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値の算出処理において、前記コントローラＩＤとフラッシュＩＤを含むデータに対するＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を算出する。
【００２３】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値の算出処理において、前記コントローラＩＤに対するＭＡＣと、前記フラッシュＩＤに対するＭＡＣを個別に算出する。
【００２４】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値の算出処理において、前記コントローラＩＤとフラッシュＩＤを含むデータに対する署名データ（トークン）を算出する。

【００２５】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記検証値の算出処理において、前記コントローラＩＤに対する署名データと、前記フラッシュＩＤに対する署名データを個別に算出する。
【００２６】
さらに、本発明の第４の側面は、
メモリカードに対するコンテンツ記録を実行する情報処理装置において実行する情報処理方法であり、
前記情報処理装置のデータ処理部が、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を生成して前記メモリカードに記録する処理を実行する情報処理方法にある。
【００２７】
さらに、本発明の第５の側面は、
メモリカードに記録されたコンテンツを再生する情報処理装置において実行する情報処理方法であり、
前記情報処理装置のデータ処理部が、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得し、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を算出し、前記メモリカードに予め記録された照合用検証値との比較を実行して照合が成立したことを条件として、前記メモリカードに記録されたコンテンツの再生処理を実行する情報処理方法にある。
【００２８】
さらに、本発明の第６の側面は、
メモリカードに対するコンテンツ記録を実行する情報処理装置に情報処理を実行させるプログラムであり、
前記情報処理装置のデータ処理部に、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得させ、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を生成して前記メモリカードに記録する処理を実行させるプログラムにある。
【００２９】
さらに、本発明の第７の側面は、
メモリカードに記録されたコンテンツを再生する情報処理装置に情報処理を実行させるプログラムであり、
前記情報処理装置のデータ処理部に、
前記メモリカードのコントローラ部が読み出し処理を行うコントローラＩＤと、
前記メモリカードのフラッシュメモリ部内制御部が読み出し処理を行うフラッシュＩＤを取得させ、
取得したコントローラＩＤとフラッシュＩＤを適用した検証値を算出し、前記メモリカードに予め記録された照合用検証値との比較を実行して照合が成立したことを条件として、前記メモリカードに記録されたコンテンツの再生処理を実行させるプログラムにある。
【００３０】
なお、本発明のプログラムは、例えば、様々なプログラム・コードを実行可能な情報処理装置やコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体によって提供可能なプログラムである。このようなプログラムをコンピュータ

可読な形式で提供することにより、情報処理装置やコンピュータ・システム上でプログラムに応じた処理が実現される。

【００３１】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００３２】

本発明の一実施例の構成によれば、ＩＤに基づく検証値を利用してコンテンツの不正利用を防止する構成が実現される。具体的には、データ記憶領域と制御部を有するフラッシュメモリ部と、フラッシュメモリ部に対するデータ記録と読み出し制御を実行するコントローラ部を有するメモリカードにコントローラ部が読み出すコントローラＩＤ（ＣＩＤ）と、フラッシュメモリ部の制御部が読み出すフラッシュＩＤ（ＦＩＤ）を記録する。コンテンツ記録処理を実行する記録装置は、ＣＩＤとＦＩＤを利用したＭＡＣ等の検証値を生成してメモリカードに記録し、コンテンツ再生を実行する再生装置は、ＣＩＤとＦＩＤに基づく算出検証値と照合用検証値を比較する検証処理を実行して検証成立を条件としてコンテンツ再生を行う。

【００３３】

本構成により、コントローラ部の製造主体であるコントローラベンダー、またはフラッシュメモリ部の製造主体であるフラッシュメモリベンダーのいずれか一方が不正なＩＤ設定を行っても、いずれか一方が正しいＩＤ管理を行っている限り、コンテンツの不正利用を防止することが可能となる。

【図面の簡単な説明】

【００３４】

【図１】メモリカードの製造プロセスについて説明する図である。

【図２】メモリカードの構成例について説明する図である。

【図３】本発明に従った検証値の生成と記録処理の概要について説明する図である。

【図４】本発明の情報処理装置の実行するコンテンツ記録処理における検証値の生成と記録処理の第１実施例について説明する図である。

【図５】本発明の情報処理装置の実行するコンテンツ記録処理における検証値の生成と記録処理の第１実施例の変形例について説明する図である。

【図６】本発明の情報処理装置の実行するコンテンツ記録処理における検証値の生成と記録処理の第２実施例について説明する図である。

【図７】本発明の情報処理装置の実行するコンテンツ記録処理における検証値の生成と記録処理の第３実施例について説明する図である。

【図８】本発明の情報処理装置の実行するコンテンツ記録処理における検証値の生成と記録処理の第４実施例について説明する図である。

【図９】本発明の情報処理装置の実行するコンテンツ再生処理のシーケンスを説明するフローチャートを示す図である。

【図１０】情報処理装置のハードウェア構成例について説明する図である。

【図１１】メモリカードのハードウェア構成例について説明する図である。

【発明を実施するための形態】

【００３５】

以下、図面を参照しながら本発明のデータ記憶装置、情報処理装置、および情報処理方法、並びにプログラムの詳細について説明する。なお、説明は以下の項目に従って行う。

１．データ記憶装置（メモリカード）の構成例について

２．コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の利用処理の概要について

３．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例１

４．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例２
５．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例３
６．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例４
７．コンテンツ再生処理シーケンスについて
８．各装置のハードウェア構成例について

【００３６】

［１．データ記憶装置（メモリカード）の構成例について］

【００３７】

以下、図面を参照しながら本発明のデータ記憶装置、情報処理装置、および情報処理方法、並びにプログラムの詳細について説明する。

【００３８】

まず、図２以下を参照して、データ記憶装置（メモリカード）の構成例について説明する。

図２は、本発明において適用可能なデータ記憶装置であるフラッシュメモリを備えたデータ記憶装置（メモリカード）１００の構成例を示す図である。データ記憶装置（メモリカード）１００は、例えばＳＤカード、ＵＳＢメモリ、メモリースティック（登録商標）等である。

【００３９】

先に図１を参照して簡単に説明したように、メモリカード１００はコントローラ部１１０とフラッシュメモリ部１２０を有する。

コントローラ部１１０は、フラッシュメモリ部１２０に対するデータ記録と読み出し制御を実行する。また、例えばメモリカード１００を装着した情報処理装置（ホスト）との通信制御や、フラッシュメモリ部１２０に対するアクセス制御などの制御処理を実行する。コントローラ部１１０は、ＣＰＵやＲＡＭ，ＲＯＭ等のハードウェアによって構成される。

【００４０】

さらに、コントローラ部１１０は、メモリカード１００を装着した情報処理装置（ホスト）との認証処理や通信データの暗号化処理等を実行する。

また、後段で詳細に説明するが、コントローラ部１１０は、コントローラ部１１０の管理するＩＤであるコントローラＩＤ（ＣＩＤ）の読み出しを実行する。

【００４１】

フラッシュメモリ部１２０は、データ記憶領域を有し、さらにフラッシュメモリ部内制御部１２１を有する。

データ記憶領域は、図に示すように保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１２２と汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）１２３によって構成される。

フラッシュメモリ部内制御部１２１は、例えばフラッシュメモリ部１２０の管理するＩＤであるフラッシュメモリＩＤ（ＦＩＤ）の読み出し処理を実行する。

【００４２】

例えば、コントローラＩＤ（ＣＩＤ）は、先に図１を参照して説明したコントローラベンダーの管理下で設定されたＩＤであり、フラッシュメモリＩＤ（ＦＩＤ）は、フラッシュメモリベンダーの管理下で設定されたＩＤとなる。すなわち、これら２つのＩＤは、独自に個別管理されたＩＤとして設定される。

【００４３】

コントローラＩＤ（ＣＩＤ）は、コントローラ部１１０によってのみ読み取り可能なＩＤであり、フラッシュメモリＩＤ（ＦＩＤ）はフラッシュメモリ部内制御部１２１によってのみ読み取り可能なＩＤとされる。

【００４４】

なお、各ＩＤの記録領域は特に限定されない。例えばコントローラＩＤ（ＣＩＤ）はコントローラ部内のメモリに記録してもよいし、フラッシュメモリ部１２０データ記憶領域内に記録してもよい。フラッシュメモリＩＤ（ＦＩＤ）は、フラッシュメモリ部１２０デ

ータ記憶領域内に記録される。
【００４５】
なお、フラッシュメモリ部１２０のデータ記憶領域に設定される保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１２２は、アクセス権限が認められた特定の装置のみがアクセス（データ書き込みやデータ読み取り）を実行することを可能としたアクセス制限領域である。
汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）１２３は、アクセス制限のないデータ記録領域である。
【００４６】
なお、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１２２に対してアクセスを実行しようとする情報処理装置は、コントローラ部１１０との間で所定の認証処理を実行し、例えば保護領域内の各区分領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０，＃１・・・）に対するアクセス権限を記載した証明書（Ｃｅｒｔ）をコントローラ部１１０に提示して、コントローラ部１１０の確認を受けることが必要となる。
【００４７】
［２．コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の利用処理の概要について］
次に、図３を参照して、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の利用処理の概要について説明する。
【００４８】
本発明の構成では、メモリカード１００に対するコンテンツ等のデータ記録処理に際して、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の２つのＩＤを利用した検証値を生成して記録コンテンツに併せてメモリカード１００に記録する。
また、メモリカード１００からのコンテンツの読み出し、再生処理を実行する場合には、コンテンツに併せて記録した検証値に基づく検証処理を実行し、検証処理が成立した場合にのみコンテンツの読み取り、再生処理を許容する構成とする。
【００４９】
本発明の構成では、独自に管理される２つの異なるＩＤであるコントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の双方を利用した検証値を利用した構成としている。
なお、コントローラＩＤ（ＣＩＤ）は、メモリカード１００のコントローラ部が読み出し処理を実行する。
フラッシュＩＤ（ＦＩＤ）はフラッシュメモリ部内の制御部が読み出し処理を実行する。
【００５０】
この独自に管理される２つのコントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の双方を利用した検証値を利用した構成によって、例えばＣＩＤまたはＦＩＤのいずれかが不正な管理の下に不正に設定されたＩＤであっても、少なくとも一方が正しく管理されたＩＤであれば、その正しい管理下に基づくＩＤに従ったコンテンツ利用制御を実現可能とする。
【００５１】
図３は、データ記憶装置（メモリカード）１００に対するコンテンツ記録処理時に実行する処理シーケンスの概要を説明する図である。
図３には、
データ記憶装置（メモリカード）１００と、
データ記憶装置（メモリカード）１００に対するコンテンツ記録処理を実行する情報処理装置（ホスト）２００、
を示している。
なお、情報処理装置（ホスト）２００は、例えばユーザのＰＣ、レコーダ等、メモリカード１００を装着可能な装置である。あるいはユーザのＰＣ等にネットワークを介して接

続されたコンテンツ提供サーバ等であってもよい。

【００５２】

情報処理装置（ホスト）２００は、データ記憶装置（メモリカード）１００に対するコンテンツ記録に先立ち、コントローラ部１１０の読み出し可能なＩＤであるコントローラＩＤ（ＣＩＤ）１５１と、フラッシュメモリ部１２０の制御部（図２に示すフラッシュメモリ部内制御部１２１）によって読み出し可能なＩＤであるフラッシュメモリＩＤ（ＦＩＤ）１６１を読み出す。

【００５３】

なお、情報処理装置（ホスト）２００は、コントローラＩＤ（ＣＩＤ）１５１をコントローラ部１１０から受領するために、情報処理装置（ホスト）２００とコントローラ部１１０間で、予め規定された相互認証処理を実行し、認証処理が成立し、相互が信頼できることを確認する処理を実行する。すなわち、相互認証の成立を条件として情報処理装置（ホスト）２００は、コントローラＩＤ（ＣＩＤ）１５１をコントローラ部１１０から受領する。

【００５４】

情報処理装置（ホスト）２００は、フラッシュメモリＩＤ（ＦＩＤ）１６１を、フラッシュメモリ部１２０の制御部（フラッシュメモリ部内制御部１２１）から受領する場合、同様に、情報処理装置（ホスト）２００とフラッシュメモリ部内制御部１２１間で、予め規定された相互認証処理を実行して相互認証の成立を条件としてフラッシュメモリＩＤ（ＦＩＤ）１６１をコントローラ部１１０から受領する構成とすることが好ましい。

ただし、フラッシュメモリ部内制御部１２１に認証処理機能を有していない場合は、この認証処理は省略可能である。

【００５５】

ただし、フラッシュメモリＩＤ（ＦＩＤ）１６１は、フラッシュメモリ部内制御部１２１によって読み取り可能なデータであり、コントローラ部１１０が、フラッシュメモリ部内制御部１２１の介在なしに直接読み出すことができない。例えば、フラッシュメモリＩＤ（ＦＩＤ）は、フラッシュメモリ部内制御部１２１のみが利用可能な特定アドレスの記憶領域に記録されている。

【００５６】

情報処理装置（ホスト）２００は、このように、データ記憶装置（メモリカード）１００に対するコンテンツ記録に先立ち、コントローラ部１１０の読み出し可能なＩＤであるコントローラＩＤ（ＣＩＤ）１５１と、フラッシュメモリ部１２０の制御部（図２に示すフラッシュメモリ部内制御部１２１）によって読み出し可能なＩＤであるフラッシュメモリＩＤ（ＦＩＤ）１６１を読み出す。

【００５７】

情報処理装置（ホスト）２００は、ステップＳ１１において、コントローラＩＤ（ＣＩＤ）１５１と、フラッシュメモリＩＤ（ＦＩＤ）１６１、これら２つのＩＤを適用した検証値を生成し、生成した検証値をメモリカード１００に記録する。図に示す検証値１８１である。

【００５８】

なお、検証値としては、例えばＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）や特定の署名鍵を適用した署名データとしてのトークン（Ｔｏｋｅｎ）などが利用可能である。これらの具体的処理については後述する。

【００５９】

さらに、情報処理装置（ホスト）２００は、ステップＳ１２においてメモリカード１００に対するコンテンツ記録処理を実行する。図に示すコンテンツ１８２である。なお、このコンテンツは暗号化データとして記録することが好ましい。

【００６０】

［３．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例１］

次に、図４を参照してメモリカードに対するコンテンツ記録処理に際して実行する検証

値の生成、記録処理の第１実施例について説明する。
【００６１】
この第１実施例は、メモリカードに対するコンテンツ記録処理に際して検証値として、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の２つのＩＤに基づく１つのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を検証値として生成して記録する処理例である。
【００６２】
図４には、
データ記憶装置（メモリカード）１００と、
データ記憶装置（メモリカード）１００に対するコンテンツ記録処理を実行する情報処理装置（ホスト）２００、
これらを示している。
なお、情報処理装置（ホスト）２００は、例えばユーザのＰＣ、レコーダ等、メモリカード１００を装着可能な装置である。あるいはユーザのＰＣ等にネットワークを介して接続されたコンテンツ提供サーバ等であってもよい。
【００６３】
メモリカード１００には、
メモリカードのコントローラ部によってのみ読み取り可能なメモリカード識別子としてのコントローラＩＤ（ＣＩＤ）３０１、
メモリカードのフラッシュメモリ内制御部によってのみ読み取り可能なメモリカード識別子としてのフラッシュＩＤ（ＦＩＤ）３０２、
これら２つのＩＤが記録されている。これらのＩＤは不揮発性メモリに記録されている。
【００６４】
メモリカード１００は、所定のアクセス権の確認処理に基づいてアクセスの許容される保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１２２と、アクセス権確認処理を実行することなくアクセスの許容される汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）１２３を有する。
【００６５】
メモリカード１００に対してコンテンツを記録する情報処理装置（ホスト）２００は、まず、メモリカード１００のコントローラ部が読み出し可能なＩＤであるコントローラＩＤ（ＣＩＤ）３０１と、フラッシュメモリ部の制御部（図２に示すフラッシュメモリ部内制御部１２１）が読み出し可能なＩＤであるフラッシュメモリＩＤ（ＦＩＤ）３０２をメモリカード１００から取得する。
【００６６】
なお、情報処理装置（ホスト）２００は、コントローラＩＤ（ＣＩＤ）３０１をメモリカード１００から受領する前提として、情報処理装置（ホスト）２００とメモリカード内のコントローラ部間で予め規定された相互認証処理を実行し、認証処理が成立し相互が信頼できることを確認する処理を実行する。すなわち、相互認証の成立を条件として情報処理装置（ホスト）２００は、コントローラＩＤ（ＣＩＤ）３０１をメモリカード１００のコントローラ部から受領する。
【００６７】
フラッシュメモリＩＤ（ＦＩＤ）３０２の取得処理においては、図２を参照して説明したフラッシュメモリ内制御部１２１によるフラッシュメモリＩＤの読み取りが必要となる。情報処理装置（ホスト）２００は、メモリカード１００のコントローラ部を介してフラッシュメモリ内制御部１２１に対してフラッシュメモリＩＤの読み取り要求を出力する。フラッシュメモリ内制御部１２１が読み取ったフラッシュメモリＩＤは認証されたコントローラ部を介してを取得する。この場合、メモリカード１００のコントローラ部はこれらの通信処理の通過点となるのみとなる。
【００６８】

なお、フラッシュメモリ部内制御部１２１が認証機能を有する設定と有しない設定のいずれの構成の場合もあり得る。認証機能を有さない場合は、情報処理装置（ホスト）２００と、フラッシュメモリ部内制御部１２１間の認証処理は実行しない。認証機能を有する場合は、情報処理装置（ホスト）２００と、フラッシュメモリ部内制御部１２１間で、予め規定された相互認証処理を実行して相互認証の成立を条件としてフラッシュメモリＩＤ（ＦＩＤ）３０２をメモリカード１００から受領する。

【００６９】

情報処理装置（ホスト）２００は、ステップＳ１０１において、メモリカード１００から取得したコントローラＩＤ（ＣＩＤ）３０１と、フラッシュメモリＩＤ（ＦＩＤ）３０２に基づいて検証値としてのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成する。

【００７０】

ここでは、ＭＡＣ生成アルゴリズムの１つであるＣＭＡＣを適用し、

ＭＡＣ＝ＣＭＡＣ（Ｋｔ，ＣＩＤ||ＦＩＤ）

上記式に従って検証値を生成する。

なお、上記式において、

Ｋｔは、メモリカード１００に格納するコンテンツの暗号化に適用する鍵であるタイトル鍵である。

ＣＩＤ||ＦＩＤは、コントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の連結データを意味する。

ＣＭＡＣ（Ｋｔ，ＣＩＤ||ＦＩＤ）は、コントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の連結データに対してタイトル鍵（Ｋｔ）を適用したＣＭＡＣアルゴリズムを適用した暗号処理（ＭＡＣ生成処理）を意味する。

【００７１】

情報処理装置（ホスト）２００が、ステップＳ１０１において生成した検証値（ＭＡＣ）は、データ記憶装置（メモリカード）１００の汎用領域１２３に格納する。図４に示す検証値（ＭＡＣ）３０３である。

【００７２】

次に、情報処理装置（ホスト）２００は、ステップＳ１０２において、乱数生成処理によりバインド鍵（Ｋｂ）３２１を生成する。

バインド鍵（Ｋｂ）３２１は、コンテンツの暗号化に適用するタイトル鍵（Ｋｔ）３２３の暗号化処理に適用する鍵として生成される。

【００７３】

なお、生成したバインド鍵（Ｋｂ）はメモリカード１００の保護領域１２２に格納する。この保護領域に対するバインド鍵（Ｋｂ）の記録処理に際しては、メモリカード１００のコントローラ部において情報処理装置（ホスト）２００の保護領域１２２に対するアクセス権の確認処理が実行される。

例えば、メモリカード１００のコントローラ部は、情報処理装置（ホスト）２００の保持する公開鍵証明書などの証明書（Ｃｅｒｔ）を取得し、証明書（Ｃｅｒｔ）の記録情報に従って、情報処理装置（ホスト）２００の保護領域１２２に対するアクセス権の確認処理を実行する。

【００７４】

情報処理装置（ホスト）２００の保護領域１２２に対するアクセス権が確認されたことを条件として、バインド鍵（Ｋｂ）の書き込みが実行される。

情報処理装置（ホスト）２００の保護領域１２２に対するアクセス権が確認されない場合は、バインド鍵（Ｋｂ）の書き込みが実行されず、その後のコンテンツ記録処理も実行されないことになる。

【００７５】

情報処理装置（ホスト）２００の保護領域１２２に対するアクセス権が確認され、バインド鍵（Ｋｂ）の書き込みが完了した後、情報処理装置（ホスト）２００はコンテンツの

暗号化に適用するタイトル鍵の暗号化とメモリカードに対する書き込み処理を実行する。この処理は、図４に示すステップＳ１０３～Ｓ１０５の処理である。

【００７６】

まず、ステップＳ１０３において、利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）３２２のハッシュ値算出（ＡＥＳ－Ｈ）を実行する。利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）３２２は、メモリカード１００に対して記録するコンテンツ３２４に対応する利用制御情報ファイルである。例えばコンテンツのコピー許容回数などのコンテンツの利用ルールを記録したファイルである。

【００７７】

ステップＳ１０３において、利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）３２２のハッシュ値算出（ＡＥＳ－Ｈ）を実行し、ステップＳ１０４において、タイトル鍵（Ｋｔ）３２３との排他的論理和演算処理を実行する。

【００７８】

さらに、ステップＳ１０５において、排他的論理和演算結果に対してバインド鍵（Ｋｂ）３２１を適用した暗号化処理（ＡＥＳ－Ｅ）を実行して暗号化タイトル鍵を生成してメモリカード１００の汎用領域１２３に記録する。図４に示す暗号化タイトル鍵（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）３０５である。また、利用制御情報もメモリカード１００の汎用領域１２３に記録する。図４に示す利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）３０４である。

【００７９】

ステップＳ１０５における暗号化タイトル鍵（ＥｎｃＫｔ）の生成は、例えば以下の式に従って実行される。

ＥｎｃＫｔ＝ＡＥＳ－１２８Ｅ（Ｋｂ，ＫｔｘｏｒＡＥＳ－Ｈ（Ｕｓａｇｅ））

上記式において、

ＫｔｘｏｒＡＥＳ－Ｈ（Ｕｓａｇｅ）は、利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）のハッシュ値とタイトル鍵（Ｋｔ）の排他的論理和演算（ｘｏｒ）を示している、

この排他的論理和演算結果に対してバインド鍵（Ｋｂ）を適用して暗号化アルゴリズム（ＡＥＳ－１２８Ｅ）を適用した暗号化処理を実行して暗号化タイトル鍵（ＥｎｃＫｔ）を生成する。

【００８０】

次に、情報処理装置（ホスト）２００は、ステップＳ１０６においてコンテンツ３２４に対して、タイトル鍵（Ｋｔ）３２３を適用した暗号化処理を実行し、暗号化コンテンツをメモリカード１００の汎用領域１２３に記録する。図４に示す暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ）３０６である。

【００８１】

このように、情報処理装置（ホスト）２００は、メモリカード１００に対して暗号化コンテンツ３０６を記録する際に、暗号化コンテンツ３０６に対応する検証値３０３としてのＭＡＣをコントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の２つのＩＤに基づいて生成してメモリカード１００に記録する。

【００８２】

メモリカード１００に格納された暗号化コンテンツ３０６を読み出して再生する再生装置は、この検証値３０３に基づく検証処理を実行する。

すなわち、再生装置はコンテンツの読み出し前の処理として、検証値３０３に基づく検証処理を実行する。検証が成立した場合にのみコンテンツの読み出し、再生が実行される。検証が不成立の場合は、コンテンツの読み出し、再生は許容されない。なお、コンテンツ再生処理の詳細シーケンスについては後述する。

【００８３】

（実施例１の変形例）

次に、図４を参照して説明したメモリカードに対するコンテンツ記録処理に際して実行する検証値の生成、記録処理の第１実施例の変形例について図５を参照して説明する。

【００８４】
図５に示す処理例は、図４を参照して説明した処理と同様、メモリカードに対するコンテンツ記録処理に際して検証値として、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の２つのＩＤに基づく１つのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を検証値として生成して記録する処理例である。
【００８５】
図５に示す処理例は、図４を参照して説明した処理ステップであるステップＳ１０１～Ｓ１０６のステップ中、ステップＳ１０３～Ｓ１０５の処理を、図５に示すステップＳ１２１～Ｓ１２２に変更した点のみが異なる。
【００８６】
図５に示す処理では、ステップＳ１２１において、利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）３２２に対する秘密鍵に基づく署名処理を実行し、署名を付加した利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）を生成する。
この署名付きの利用制御情報をメモリカード１００の汎用領域１２３に記録する。図５に示す利用制御情報（Ｕｓａｇｅ　ｆｉｌｅ）３０４である。
【００８７】
さらに、ステップＳ１２２において、タイトル鍵３２３に対して、バインド鍵（Ｋｂ）３２１を適用した暗号化処理を実行して暗号化タイトル鍵を生成してメモリカード１００の汎用領域１２３に記録する。図５に示す暗号化タイトル鍵（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）３０５である。
【００８８】
その後のステップＳ１０６の処理は、図４を参照して説明したと同様の処理であり、ステップＳ１０６においてコンテンツ３２４に対して、タイトル鍵（Ｋｔ）３２３を適用した暗号化処理を実行し、暗号化コンテンツをメモリカード１００の汎用領域１２３に記録する。図４に示す暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ）３０６である。
本処理例では、利用制御情報に署名を設定して記録する構成としており、利用制御情報の改ざん検証、改ざん防止の効果がもたらされる。
【００８９】
［４．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例２］
次に、図６を参照してメモリカードに対するコンテンツ記録処理に際して実行する検証値の生成、記録処理の第２実施例について説明する。
【００９０】
この第２実施例は、メモリカードに対するコンテンツ記録処理に際して検証値として、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の２つのＩＤに基づいて、それぞれ個別のＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を検証値として生成して記録する処理例である。
【００９１】
図６には、図４と同様、
データ記憶装置（メモリカード）１００と、
データ記憶装置（メモリカード）１００に対するコンテンツ記録処理を実行する情報処理装置（ホスト）２００、
これらを示している。
なお、情報処理装置（ホスト）２００は、例えばユーザのＰＣ、レコーダ等、メモリカード１００を装着可能な装置である。あるいはユーザのＰＣ等にネットワークを介して接続されたコンテンツ提供サーバ等であってもよい。
【００９２】
メモリカード１００には、
メモリカードのコントローラ部によってのみ読み取り可能なメモリカード識別子としてのコントローラＩＤ（ＣＩＤ）３０１、

メモリカードのフラッシュメモリ内制御部によってのみ読み取り可能なメモリカード識別子としてのフラッシュＩＤ（ＦＩＤ）３０２、
これら２つのＩＤが記録されている。これらのＩＤは不揮発性メモリに記録されている。

【００９３】
図６に示す処理シーケンスと、図４に示す処理シーケンスとの差異は、
図４におけるステップＳ１０１の処理が、
図６においては、ステップＳ１０１ａとステップＳ１０１ｂの２つの処理として設定されている点である。これら２つのステップにおいて、それぞれ、
（ａ）コントローラＩＤ（ＣＩＤ）に基づく第１検証値（ＭＡＣ）、
（ｂ）フラッシュＩＤ（ＦＩＤ）に基づく第２検証値（ＭＡＣ）、
これら２つの検証値を生成してメモリカード１００の汎用領域１２３に記録する。
その他の処理については、図４を参照して説明した処理と同様である。

【００９４】
情報処理装置（ホスト）２００は、まず、ステップＳ１０１ａにおいて、メモリカード１００から読み出したコントローラＩＤ（ＣＩＤ）３０１に基づいて第１検証値としてのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成する。
ここでは、ＭＡＣ生成アルゴリズムの１つであるＣＭＡＣを適用し、
ＭＡＣ＝ＣＭＡＣ（Ｋｔ，ＣＩＤ）
上記式に従ってコントローラＩＤ（ＣＩＤ）に基づく第１検証値を生成する。

【００９５】
情報処理装置（ホスト）２００が、ステップＳ１０１ａにおいて生成した第１検証値（ＭＡＣ）は、データ記憶装置（メモリカード）１００の汎用領域１２３に格納する。図６に示す第１検証値（ＭＡＣ）３０３ａである。

【００９６】
さらに、情報処理装置（ホスト）２００は、ステップＳ１０１ｂにおいて、メモリカード１００から読み出したフラッシュＩＤ（ＦＩＤ）３０２に基づいて第２検証値としてのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成する。
ＣＩＤに対する処理と同様に、ＭＡＣ生成アルゴリズムの１つであるＣＭＡＣを適用し、
ＭＡＣ＝ＣＭＡＣ（Ｋｔ，ＦＩＤ）
上記式に従ってフラッシュＩＤ（ＦＩＤ）に基づく第２検証値を生成する。

【００９７】
情報処理装置（ホスト）２００が、ステップＳ１０１ｂにおいて生成した第２検証値（ＭＡＣ）は、データ記憶装置（メモリカード）１００の汎用領域１２３に格納する。図６に示す第２検証値（ＭＡＣ）３０３ｂである。

【００９８】
ステップＳ１０２～ステップＳ１０６の処理は、図４を参照して説明した第１実施例の処理と同様の処理である。

【００９９】
本処理例において情報処理装置（ホスト）２００は、メモリカード１００に対して暗号化コンテンツ３０６を記録する際に、暗号化コンテンツ３０６に対応する検証値３０３として、
（ａ）コントローラＩＤ（ＣＩＤ）に基づく第１検証値（ＭＡＣ）、
（ｂ）フラッシュＩＤ（ＦＩＤ）に基づく第２検証値（ＭＡＣ）、
これらの２つの検証値を個別に生成してメモリカード１００に記録する。

【０１００】
メモリカード１００に格納された暗号化コンテンツ３０６を読み出して再生する再生装置は、このこの２つの検証値である第１検証値３０３ａと第２検証値３０３ｂに基づく検証処理を実行する。

すなわち、再生装置はコンテンツの読み出し前の処理として、第１検証値３０３ａと第２検証値３０３ｂに基づく検証処理を実行する。検証が成立した場合にのみコンテンツの読み出し、再生が実行される。検証が不成立の場合は、コンテンツの読み出し、再生は許容されない。なお、コンテンツ再生処理の詳細シーケンスについては後述する。

【０１０１】

なお、本処理例においても、先に図５を参照して説明したステップＳ１２１～Ｓ１２２の処理と同様の処理を適用して、利用制御情報に対して署名を設定して記録する構成としてもよい。

【０１０２】

［５．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例３］

次に、図７を参照してメモリカードに対するコンテンツ記録処理に際して実行する検証値の生成、記録処理の第３実施例について説明する。

【０１０３】

この第３実施例は、メモリカードに対するコンテンツ記録処理に際して検証値として、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の２つのＩＤに基づいて、署名鍵（Ｋｓｉｇｎ）を適用した署名データを検証値（トークン（Ｔｏｋｅｎ））として生成して記録する処理例である。

【０１０４】

図７には、図４、図６と同様、

データ記憶装置（メモリカード）１００と、

データ記憶装置（メモリカード）１００に対するコンテンツ記録処理を実行する情報処理装置（ホスト）２００、

これらを示している。

なお、情報処理装置（ホスト）２００は、例えばユーザのＰＣ、レコーダ等、メモリカード１００を装着可能な装置である。あるいはユーザのＰＣ等にネットワークを介して接続されたコンテンツ提供サーバ等であってもよい。

【０１０５】

メモリカード１００には、

メモリカードのコントローラ部によってのみ読み取り可能なメモリカード識別子としてのコントローラＩＤ（ＣＩＤ）３０１、

メモリカードのフラッシュメモリ内制御部によってのみ読み取り可能なメモリカード識別子としてのフラッシュＩＤ（ＦＩＤ）３０２、

これら２つのＩＤが記録されている。これらのＩＤは不揮発性メモリに記録されている。

【０１０６】

図７に示す処理シーケンスと、図４に示す処理シーケンスとの差異は、

図４におけるステップＳ１０１の処理が、

図７においては、ステップＳ２０１の署名データ（ｓｉｇｎ）生成処理に置き換えられている点である。

【０１０７】

情報処理装置（ホスト）２００は、まず、ステップＳ２０１において、メモリカード１００から読み出したコントローラＩＤ（ＣＩＤ）３０１とフラッシュＩＤ（ＦＩＤ）３０２に対して、情報処理装置（ホスト）２００の保持する署名鍵（Ｋｓｉｇｎ）を適用した署名データを生成する。例えば公開鍵暗号方式に従った秘密鍵を署名鍵として利用した署名データ生成処理を実行する。

【０１０８】

署名データとしてのトークン（Ｔｏｋｅｎ）は例えば下記式に従って生成する。

Ｔｏｋｅｎ＝Ｓｉｇｎ（Ｋｓｉｇｎ，ＣＩＤ||ＦＩＤ）

なお、上記式において、

Ｋｓｉｇｎは、署名鍵である。

ＣＩＤ||ＦＩＤは、コントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の連結データを意味する。

Ｓｉｇｎ（Ｋｓｉｇｎ，ＣＩＤ||ＦＩＤ）は、コントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の連結データに対して署名鍵（Ｋｓｉｇｎ）を適用した署名アルゴリズム（Ｓｉｇｎ）を適用した署名処理を意味する。

【０１０９】

情報処理装置（ホスト）２００が、ステップＳ２０１において生成した検証値としてのトークン（Ｔｏｋｅｎ）は、データ記憶装置（メモリカード）１００の汎用領域１２３に格納する。図７に示す検証値（トークン）３１１である。

【０１１０】

ステップＳ２０２～ステップＳ２０６の処理は、図４を参照して説明した第１実施例の処理ステップＳ１０２～ステップＳ１０６の処理と同様の処理である。

【０１１１】

本処理例において情報処理装置（ホスト）２００は、メモリカード１００に対して暗号化コンテンツ３０６を記録する際に、暗号化コンテンツ３０６に対応する検証値３１１として、情報処理装置（ホスト）２００の保持する署名鍵（Ｋｓｉｇｎ）を適用した署名データ［トークン（Ｔｏｋｅｎ）］を生成してメモリカード１００に記録する。

【０１１２】

メモリカード１００に格納された暗号化コンテンツ３０６を読み出して再生する再生装置は、この検証値３１１に基づく検証処理を実行する。

すなわち、再生装置はコンテンツの読み出し前の処理として、検証値３１１に基づく検証処理を実行する。検証が成立した場合にのみコンテンツの読み出し、再生が実行される。検証が不成立の場合は、コンテンツの読み出し、再生は許容されない。なお、コンテンツ再生処理の詳細シーケンスについては後述する。

【０１１３】

なお、本処理例においても、先に図５を参照して説明したステップＳ１２１～Ｓ１２２の処理と同様の処理を適用して、利用制御情報に対して署名を設定して記録する構成としてもよい。

【０１１４】

［６．コンテンツ記録処理に際して実行する検証値の生成、記録処理の実施例４］

次に、図８を参照してメモリカードに対するコンテンツ記録処理に際して実行する検証値の生成、記録処理の第４実施例について説明する。

【０１１５】

この第４実施例は、メモリカードに対するコンテンツ記録処理に際して検証値として、コントローラＩＤ（ＣＩＤ）とフラッシュメモリＩＤ（ＦＩＤ）の２つのＩＤに基づいて、それぞれ署名鍵（Ｋｓｉｇｎ）を適用した署名データを個別に生成して２つの検証値（トークン（Ｔｏｋｅｎ））を生成して記録する処理例である。

【０１１６】

図８には、図４～図７と同様、

データ記憶装置（メモリカード）１００と、

データ記憶装置（メモリカード）１００に対するコンテンツ記録処理を実行する情報処理装置（ホスト）２００、

これらを示している。

なお、情報処理装置（ホスト）２００は、例えばユーザのＰＣ、レコーダ等、メモリカード１００を装着可能な装置である。あるいはユーザのＰＣ等にネットワークを介して接続されたコンテンツ提供サーバ等であってもよい。

【０１１７】

メモリカード１００には、

メモリカードのコントローラ部によってのみ読み取り可能なメモリカード識別子としてのコントローラＩＤ（ＣＩＤ）３０１、

メモリカードのフラッシュメモリ内制御部によってのみ読み取り可能なメモリカード識別子としてのフラッシュＩＤ（ＦＩＤ）３０２、
これら２つのＩＤが記録されている。これらのＩＤは不揮発性メモリに記録されている。

【０１１８】
図８に示す処理シーケンスと、図７に示す処理シーケンスとの差異は、
図７におけるステップＳ２０１の処理が、
図８においては、ステップＳ２０１ａとステップＳ２０１ｂの２つの処理として設定されている点である。これら２つのステップにおいて、それぞれ、
（ａ）コントローラＩＤ（ＣＩＤ）に基づく第１検証値（トークン）、
（ｂ）フラッシュＩＤ（ＦＩＤ）に基づく第２検証値（トークン）、
これら２つの検証値を生成してメモリカード１００の汎用領域１２３に記録する。
その他の処理については、図７を参照して説明した処理と同様である。

【０１１９】
情報処理装置（ホスト）２００は、まず、ステップＳ２０１ａにおいて、メモリカード１００から読み出したコントローラＩＤ（ＣＩＤ）３０１に対して署名鍵（Ｋｓｉｇｎ）を適用した署名データを第１検証値（Ｔｏｋｅｎ）として生成する。
署名データとしてのトークン（Ｔｏｋｅｎ）は例えば下記式に従って生成する。
Ｔｏｋｅｎ＝Ｓｉｇｎ（Ｋｓｉｇｎ，ＣＩＤ）
なお、上記式において、
Ｋｓｉｇｎは、署名鍵である。
Ｓｉｇｎ（Ｋｓｉｇｎ，ＣＩＤ）は、コントローラＩＤ（ＣＩＤ）に対して署名鍵（Ｋｓｉｇｎ）を適用した署名アルゴリズム（Ｓｉｇｎ）を適用した署名処理を意味する。

【０１２０】
情報処理装置（ホスト）２００が、ステップＳ２０１ａにおいて生成した第１検証値（トークン）は、データ記憶装置（メモリカード）１００の汎用領域１２３に格納する。図８に示す第１検証値（トークン）３１１ａである。

【０１２１】
さらに、情報処理装置（ホスト）２００は、ステップＳ２０１ｂにおいて、メモリカード１００から読み出したフラッシュＩＤ（ＦＩＤ）３０２に対して署名鍵（Ｋｓｉｇｎ）を適用した署名データを第２検証値（Ｔｏｋｅｎ）として生成する。
署名データとしてのトークン（Ｔｏｋｅｎ）は例えば下記式に従って生成する。
Ｔｏｋｅｎ＝Ｓｉｇｎ（Ｋｓｉｇｎ，ＦＩＤ）
なお、上記式において、
Ｋｓｉｇｎは、署名鍵である。
Ｓｉｇｎ（Ｋｓｉｇｎ，ＦＩＤ）は、フラッシュＩＤ（ＦＩＤ）に対して署名鍵（Ｋｓｉｇｎ）を適用した署名アルゴリズム（Ｓｉｇｎ）を適用した署名処理を意味する。

【０１２２】
情報処理装置（ホスト）２００が、ステップＳ２０１ｂにおいて生成した第２検証値（トークン）は、データ記憶装置（メモリカード）１００の汎用領域１２３に格納する。図８に示す第２検証値（トークン）３１１ｂである。

【０１２３】
ステップＳ２０２～ステップＳ２０６の処理は、図４を参照して説明した第１実施例の処理ステップＳ１０２～Ｓ１０６の処理と同様の処理である。

【０１２４】
本処理例において情報処理装置（ホスト）２００は、メモリカード１００に対して暗号化コンテンツ３０６を記録する際に、暗号化コンテンツ３０６に対応する検証値３０３として、
（ａ）コントローラＩＤ（ＣＩＤ）に基づく第１検証値（トークン）、
（ｂ）フラッシュＩＤ（ＦＩＤ）に基づく第２検証値（トークン）、

これらの２つの検証値を個別に生成してメモリカード１００に記録する。

【０１２５】

メモリカード１００に格納された暗号化コンテンツ３０６を読み出して再生する再生装置は、このこの２つの検証値である第１検証値３１１ａと第２検証値３１１ｂに基づく検証処理を実行する。

すなわち、再生装置はコンテンツの読み出し前の処理として、第１検証値３１１ａと第２検証値３１１ｂに基づく検証処理を実行する。検証が成立した場合にのみコンテンツの読み出し、再生が実行される。検証が不成立の場合は、コンテンツの読み出し、再生は許容されない。なお、コンテンツ再生処理の詳細シーケンスについては後述する。

【０１２６】

なお、本処理例においても、先に図５を参照して説明したステップＳ１２１～Ｓ１２２の処理と同様の処理を適用して、利用制御情報に対して署名を設定して記録する構成としてもよい。

【０１２７】

［７．コンテンツ再生処理シーケンスについて］

次に、図９に示すフローチャートを参照してメモリカードに記録されたコンテンツの再生処理における処理シーケンスについて説明する。

【０１２８】

図９に示す再生処理シーケンスは、図４～図８を先勝して説明した検証値のいずれかとコンテンツを格納したメモリカードを装着した再生装置において実行する処理シーケンスである。

【０１２９】

再生装置は、まずステップＳ３０１において、データ記憶装置（メモリカード）からコントローラＩＤ（ＣＩＤ）と、フラッシュＩＤ（ＦＩＤ）の読み出し処理を実行する。

なお、再生装置は、メモリカードからコントローラＩＤ（ＣＩＤ）を読み出す前に、再生装置とメモリカードのコントローラ部との相互認証を実行し相互認証が成立したことを条件としてコントローラＩＤを読み出す構成とすることが望ましい。

同様に、再生装置は、メモリカードからフラッシュＩＤ（ＦＩＤ）を読み出す前に、再生装置とメモリカードのフラッシュメモリ部内制御部との相互認証を実行し相互認証が成立したことを条件としてフラッシュＩＤを読み出す構成とすることが望ましい。

【０１３０】

次に、ステップＳ３０２において、再生装置はメモリカードから読み出したコントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）を適用した検証値を算出する。

ここで算出する検証値は、先に図４～図８を参照して説明した実施例１～４のいずれかの検証値である。具体的には、以下のいずれかの検証値となる。

（１）ＣＩＤとＦＩＤの連結データに基づくＭＡＣ（実施例１（図４、図５）対応）

（２）ＣＩＤとＦＩＤの個別データに基づく２つのＭＡＣ（実施例２（図６）対応）

（３）ＣＩＤとＦＩＤの連結データに基づく署名データ（トークン）（実施例３（図７）対応）

（４）ＣＩＤとＦＩＤの個別データに基づく２つの署名データ（トークン）（実施例４（図８）対応）

【０１３１】

次に、再生装置は、ステップＳ３０３において、メモリカードから照合用の検証値を読み取る。これは、先に図４～図８を参照して説明した実施例１～４のいずれかの検証値である。具体的には、以下のいずれかの検証値となる。

（１）図４、図５に示す実施例１の構成の場合、検証値（ＭＡＣ）３０３となる。

（２）図６に示す実施例２の構成の場合、第１検証値（ＭＡＣ）３０３ａと、第２検証値（ＭＡＣ）３０３ｂとなる。

（３）図７に示す実施例３の構成の場合、検証値（トークン）３１１となる。

（４）図８に示す実施例４の構成の場合、第１検証値（トークン）３１１ａと、第２検

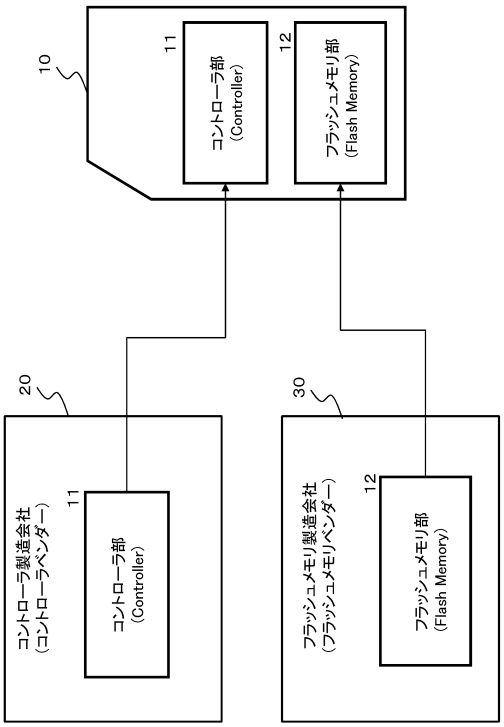
証値（トークン）３１１ｂとなる。
【０１３２】
次に、再生装置は、ステップＳ３０４において、ステップＳ３０２で算出した算出検証値ともステップＳ３０３でメモリカードから読み出した照合用検証値を比較する。
【０１３３】
ステップＳ３０５において、
算出検証値＝照合用検証値
上記式が成立するか否かを判定する。
上記式が成立する場合は、検証成功と判定し、ステップＳ３０６に進み、メモリカードから暗号化コンテンツを読み取り、復号、再生処理を実行する。
一方、上記式が成立しない場合は、検証失敗と判定し、ステップＳ３０６のコンテンツ再生処理を実行することなく処理を終了する。この場合、コンテンツ再生は許容されない。
【０１３４】
このように、本発明の構成では、メモリカードに、メモリカード内のコントローラ部が管理し、コントローラ部の管理の下に読み出し可能なコントローラＩＤ（ＣＩＤ）と、フラッシュメモリ部が管理し、フラッシュメモリ部内の制御部の管理の下で読み出し可能なフラッシュＩＤ（ＦＩＤ）を記録する構成とした。
【０１３５】
コンテンツ記録処理に際して、これらコントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の２つのＩＤに基づく検証値を生成してコンテンツに併せて記録し、コンテンツ再生時には、コントローラＩＤ（ＣＩＤ）とフラッシュＩＤ（ＦＩＤ）の２つのＩＤに基づく検証値を算出して照合する検証処理を実行して検証の成立を条件としてコンテンツ再生を許容する構成とした。
【０１３６】
この構成により、コントローラ部の製造主体であるコントローラベンダー、またはフラッシュメモリ部の製造主体であるフラッシュメモリベンダーのいずれか一方が不正なＩＤ設定を行っても、いずれか一方が正しいＩＤ管理を行っている限り、コンテンツの不正利用を防止することが可能となる。
【０１３７】
［８．各装置のハードウェア構成例について］
最後に、図１０以下を参照して、上述した処理を実行する各装置のハードウェア構成例について説明する。
まず、図１０を参照して、メモリカードに対するコンテンツ記録処理または再生処理を実行する情報記録装置や情報再生装置のハードウェア構成例について説明する。
【０１３８】
ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）７０１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）７０２、または記憶部７０８に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述の各実施例において説明したメモリカード(図中のリムーバブルメディア７１１)に対する記録処理、メモリカード(図中のリムーバブルメディア７１１)からのデータ再生処理等を実行する。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）７０３には、ＣＰＵ７０１が実行するプログラムやデータなどが適宜記憶される。これらのＣＰＵ７０１、ＲＯＭ７０２、およびＲＡＭ７０３は、バス７０４により相互に接続されている。
【０１３９】
ＣＰＵ７０１はバス７０４を介して入出力インタフェース７０５に接続され、入出力インタフェース７０５には、各種スイッチ、キーボード、マウス、マイクロホンなどよりなる入力部７０６、ディスプレイ、スピーカなどよりなる出力部７０７が接続されている。ＣＰＵ７０１は、入力部７０６から入力される指令に対応して各種の処理を実行し、処理結果を例えば出力部７０７に出力する。

【０１４０】
入出力インタフェース７０５に接続されている記憶部７０８は、例えばハードディスク等からなり、ＣＰＵ７０１が実行するプログラムや各種のデータを記憶する。通信部７０９は、インターネットやローカルエリアネットワークなどのネットワークを介して外部の装置と通信する。
【０１４１】
入出力インタフェース７０５に接続されているドライブ７１０は、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア７１１を駆動し、記録されているコンテンツや鍵情報、プログラム等の各種データを取得する。例えば、取得されたプログラムに従ったデータ処理、あるいはコンテンツや鍵データを用いて、ＣＰＵによって実行するデータ処理、記録再生プログラムに従って鍵生成、コンテンツの暗号化、記録処理、復号、再生処理などが行われる。
【０１４２】
図１１は、メモリカードのハードウェア構成例を示している。
先に、図２を参照して説明したようにメモリカードは、コントローラ部８００とフラッシュメモリ部８０７を有する。データ記憶装置（メモリカード）１００は、例えばＳＤカード、ＵＳＢメモリ、メモリースティック（登録商標）等により構成される。
【０１４３】
コントローラ部８００はＣＰＵ８０１、ＲＯＭ８０２、ＲＡＭ８０３を有する。
ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）８０１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）８０２、またはフラッシュメモリ部８０７に記憶されているプログラムに従って各種の処理を実行する。
【０１４４】
コントローラ部８００は、例えば、先に説明したコントローラＩＤ（ＣＩＤ）の読み取りを実行する。なお、コントローラＩＤ（ＣＩＤ）は、コントローラ部８００内のメモリに記録された設定としてもよいし、フラッシュメモリ部８０７の記憶素子領域８１２に記録された設定としてもよい。
【０１４５】
コントローラ部８００は、さらに、サーバや記録装置や再生装置等のホスト機器との通信処理やデータのフラッシュメモリ部８０７に対する書き込み、読み取り等の処理、フラッシュメモリ部８０７の保護領域の区分領域単位のアクセス可否判定処理等を実行する。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）８０３には、ＣＰＵ８０１が実行するプログラムやデータなどが適宜記憶される。これらのＣＰＵ８０１、ＲＯＭ８０２、およびＲＡＭ８０３は、バス８０４により相互に接続されている。
【０１４６】
ＣＰＵ８０１はバス８０４を介して入出力インタフェース８０５に接続され、入出力インタフェース８０５には、通信部８０６、フラッシュメモリ部８０７が接続されている。入出力インタフェース８０５に接続されている通信部８０４は、例えばサーバ、ホスト機器との通信を実行する。
【０１４７】
フラッシュメモリ部８０７は、図２に示すフラッシュメモリ部１２０に対応し、フラッシュメモリ部内の制御部８１１とも記憶素子領域８１２を有する。制御部８１１は、フラッシュＩＤ（ＦＩＤ）の読み取り処理を実行する。フラッシュＩＤ（ＦＩＤ）は、例えば記憶素子領域８１２に記録されている。
記憶素子領域８１２は、データの記憶領域であり、先に説明したようにアクセス制限のある保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｅａ）と、自由にデータ記録読み取りができる汎用領域を有する。
【０１４８】
なお、上述の実施例は、特定のフラッシュメモリ型のメモリカードを例として説明したが、ＵＳＢメモリ等の様々な形態のメモリにおいても本発明の適用は可能である。

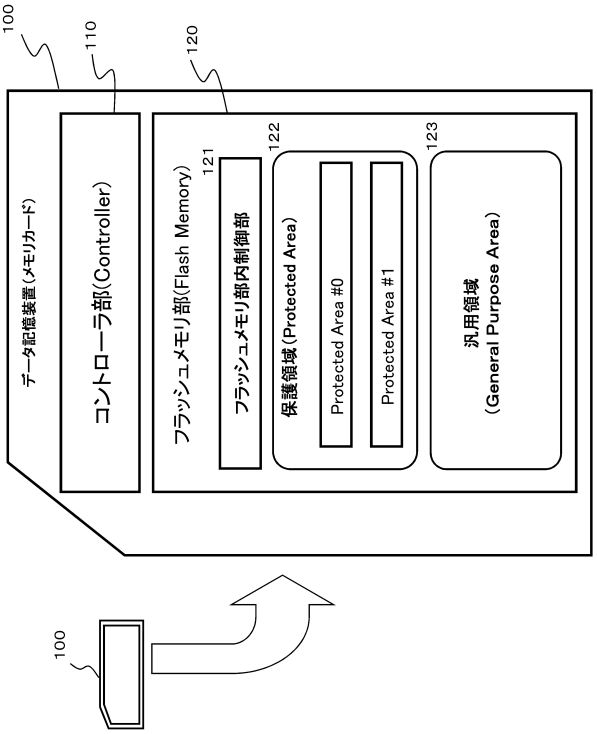
【０１４９】
以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。
【０１５０】
また、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。例えば、プログラムは記録媒体に予め記録しておくことができる。記録媒体からコンピュータにインストールする他、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介してプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。
【０１５１】
なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【産業上の利用可能性】
【０１５２】
以上、説明したように、本発明の一実施例の構成によれば、ＩＤに基づく検証値を利用してコンテンツの不正利用を防止する構成が実現される。具体的には、データ記憶領域と制御部を有するフラッシュメモリ部と、フラッシュメモリ部に対するデータ記録と読み出し制御を実行するコントローラ部を有するメモリカードにコントローラ部が読み出すコントローラＩＤ（ＣＩＤ）と、フラッシュメモリ部の制御部が読み出すフラッシュＩＤ（ＦＩＤ）を記録する。コンテンツ記録処理を実行する記録装置は、ＣＩＤとＦＩＤを利用したＭＡＣ等の検証値を生成してメモリカードに記録し、コンテンツ再生を実行する再生装置は、ＣＩＤとＦＩＤに基づく算出検証値と照合用検証値を比較する検証処理を実行して検証成立を条件としてコンテンツ再生を行う。
【０１５３】
本構成により、コントローラ部の製造主体であるコントローラベンダー、またはフラッシュメモリ部の製造主体であるフラッシュメモリベンダーのいずれか一方が不正なＩＤ設定を行っても、いずれか一方が正しいＩＤ管理を行っている限り、コンテンツの不正利用を防止することが可能となる。
【符号の説明】
【０１５４】
１０　メモリカード
１１　コントローラ部
１２　フラッシュメモリ部
２０　コントローラ製造会社（コントローラベンダー）
３０　フラッシュメモリ製造会社（フラッシュメモリベンダー）
１００　データ記憶装置（メモリカード）
１１０　コントローラ部
１２０　フラッシュメモリ部
１２１　フラッシュメモリ部内制御部
１２２　保護領域
１２３　汎用領域
１５１　コントローラＩＤ（ＣＩＤ）

１６１　フラッシュＩＤ（ＦＩＤ）
１８１　検証値
１８２　コンテンツ
２００　情報処理装置
３０１　コントローラＩＤ（ＣＩＤ）
３０２　フラッシュＩＤ（ＦＩＤ）
３０３　検証値
３０４　利用制御情報
３０５　暗号化タイトル鍵
３０６　暗号化コンテンツ
３１１　検証値
３２１　バインド鍵
３２２　利用制御情報
３２３　タイトル鍵
３２４　コンテンツ
３２５　署名鍵
７０１　ＣＰＵ
７０２　ＲＯＭ
７０３　ＲＡＭ
７０４　バス
７０５　入出力インタフェース
７０６　入力部
７０７　出力部
７０８　記憶部
７０９　通信部
７１０　ドライブ
７１１　リムーバブルメディア
８００　コントローラ部
８０１　ＣＰＵ
８０２　ＲＯＭ
８０３　ＲＡＭ
８０４　バス
８０５　入出力インタフェース
８０６　通信部
８０７　フラッシュメモリ部
８１１　制御部
８１２　記憶素子領域

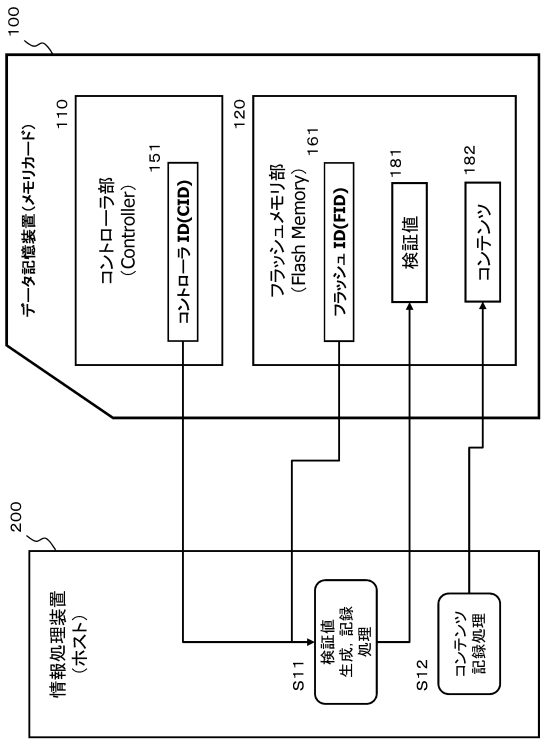
【図１】


10
11
コントローラ部
(Controller)
12
フラッシュメモリ部
(Flash Memory)
20
コントローラ製造会社
(コントローラベンダー)
11
コントローラ部
(Controller)
30
フラッシュメモリ製造会社
(フラッシュメモリベンダー)
12
フラッシュメモリ部
(Flash Memory)

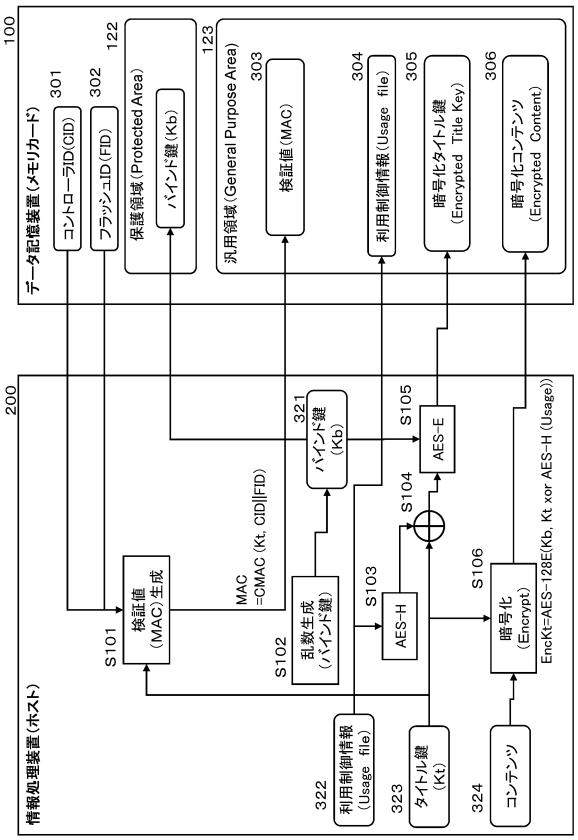
【図２】


100
110
120
データ記憶装置(メモリカード)
コントローラ部(Controller)
フラッシュメモリ部(Flash Memory)
121
フラッシュメモリ部内制御部
122
保護領域(Protected Area)
Protected Area #0
Protected Area #1
123
汎用領域
(General Purpose Area)
100

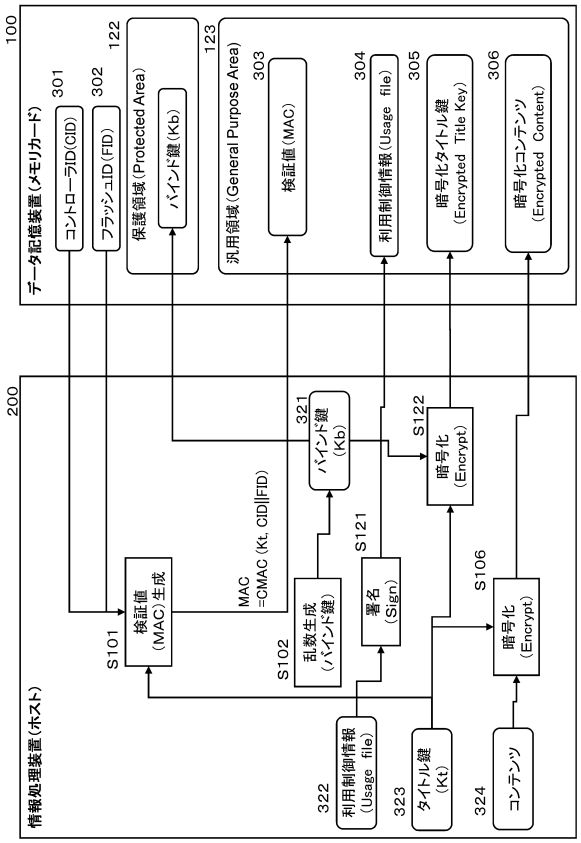
【図３】


100
データ記憶装置(メモリカード)
110
コントローラ部
(Controller)
151
コントローラ ID(CID)
120
フラッシュメモリ部
(Flash Memory)
161
フラッシュ ID(FID)
181
検証値
182
コンテンツ
200
情報処理装置
(ホスト)
S11
検証値
生成, 記録
処理
S12
コンテンツ
記録処理

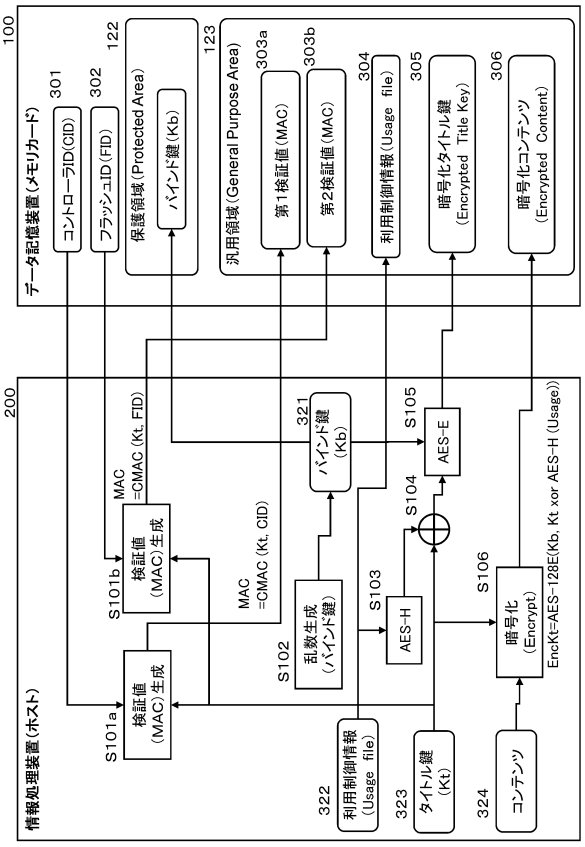
【図４】


100
データ記憶装置(メモリカード)
301
コントローラID(CID)
302
フラッシュID(FID)
122
保護領域(Protected Area)
バインド鍵(Kb)
123
汎用領域(General Purpose Area)
303
検証値(MAC)
304
利用制御情報(Usage file)
305
暗号化タイトル鍵
(Encrypted Title Key)
306
暗号化コンテンツ
(Encrypted Content)
200
情報処理装置(ホスト)
S101
検証値
(MAC)生成
MAC
=CMAC (Kt, CID)|FID)
S102
乱数生成
(バインド鍵)
321
バインド鍵
(Kb)
S103
AES-H
S104
S105
AES-E
S106
暗号化
(Encrypt)
EncKt=AES-128E(Kb, Kt xor AES-H (Usage))
322
利用制御情報
(Usage file)
323
タイトル鍵
(Kt)
324
コンテンツ

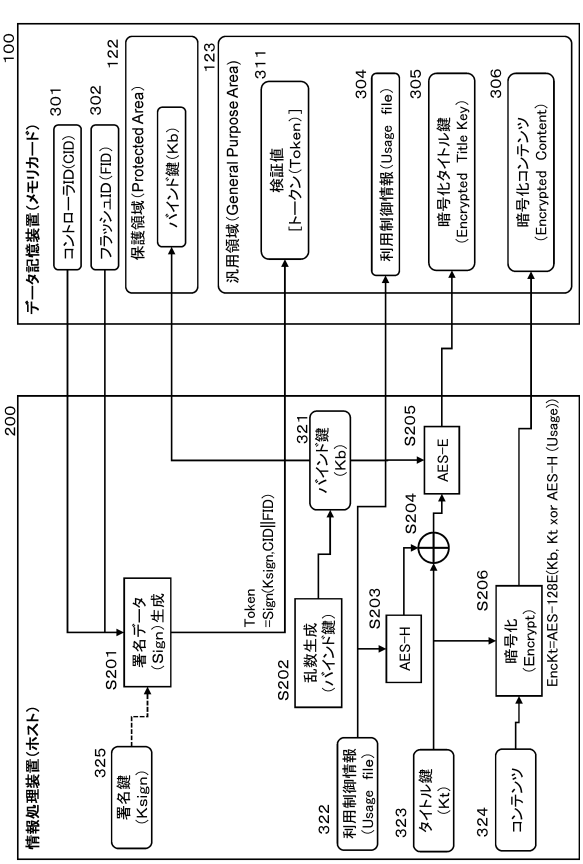
【図５】


100
データ記憶装置(メモリカード)
301
コントローラID(CID)
302
フラッシュID(FID)
122
保護領域(Protected Area)
バインド鍵(Kb)
123
汎用領域(General Purpose Area)
303
検証値(MAC)
304
利用制御情報(Usage file)
305
暗号化タイトル鍵(Encrypted Title Key)
306
暗号化コンテンツ(Encrypted Content)
200
情報処理装置(ホスト)
S101
検証値(MAC)生成
MAC=CMAC(Kt, CID||FID)
S102
乱数生成(バインド鍵)
S121
署名(Sign)
321
バインド鍵(Kb)
S122
暗号化(Encrypt)
S106
暗号化(Encrypt)
322
利用制御情報(Usage file)
323
タイトル鍵(Kt)
324
コンテンツ

【図６】


100
データ記憶装置(メモリカード)
301
コントローラID(CID)
302
フラッシュID(FID)
122
保護領域(Protected Area)
バインド鍵(Kb)
123
汎用領域(General Purpose Area)
303a
第1検証値(MAC)
303b
第2検証値(MAC)
304
利用制御情報(Usage file)
305
暗号化タイトル鍵(Encrypted Title Key)
306
暗号化コンテンツ(Encrypted Content)
200
情報処理装置(ホスト)
S101a
検証値(MAC)生成
S101b
検証値(MAC)生成
MAC=CMAC(Kt, FID)
MAC=CMAC(Kt, CID)
S102
乱数生成(バインド鍵)
321
バインド鍵(Kb)
S103
AES-H
S104
S105
AES-E
S106
暗号化(Encrypt)
EncKt=AES-128E(Kb, Kt xor AES-H(Usage))
322
利用制御情報(Usage file)
323
タイトル鍵(Kt)
324
コンテンツ

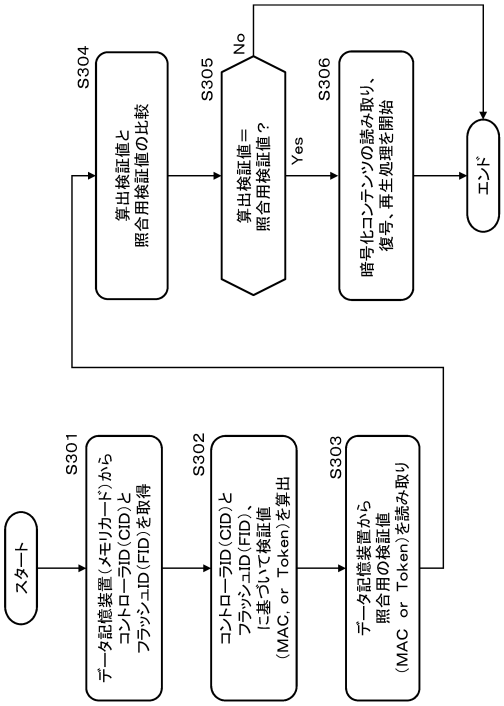
【図７】


100
データ記憶装置(メモリカード)
301
コントローラID(CID)
302
フラッシュID(FID)
122
保護領域(Protected Area)
バインド鍵(Kb)
123
汎用領域(General Purpose Area)
311
検証値[トークン(Token)]
304
利用制御情報(Usage file)
305
暗号化タイトル鍵(Encrypted Title Key)
306
暗号化コンテンツ(Encrypted Content)
200
情報処理装置(ホスト)
325
署名鍵(Ksign)
S201
署名データ(Sign)生成
Token=Sign(Ksign,CID||FID)
S202
乱数生成(バインド鍵)
321
バインド鍵(Kb)
S203
AES-H
S204
S205
AES-E
S206
暗号化(Encrypt)
EncKt=AES-128E(Kb, Kt xor AES-H(Usage))
322
利用制御情報(Usage file)
323
タイトル鍵(Kt)
324
コンテンツ

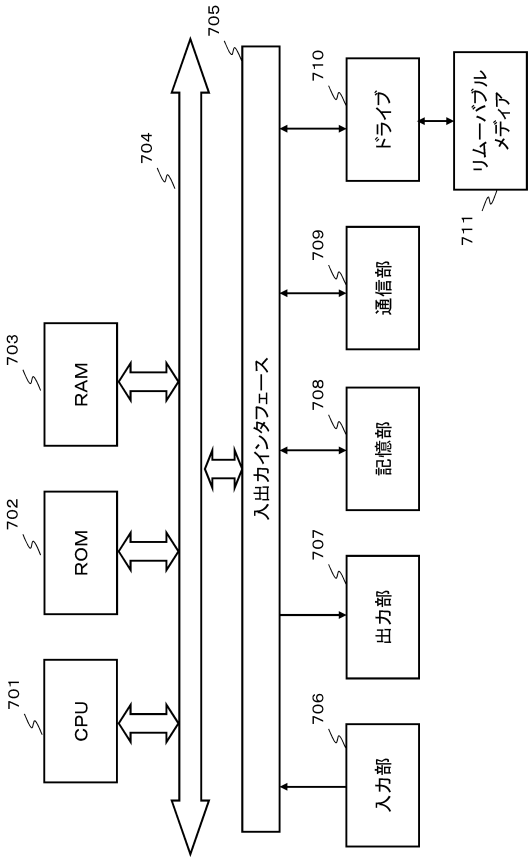
【図８】

100
データ記憶装置(メモリカード)
301
コントローラID(CID)
302
フラッシュID(FID)
122
保護領域(Protected Area)
バインド鍵(Kb)
123
汎用領域(General Purpose Area)
311a
第1検証値(トークン)
311b
第2検証値(トークン)
304
利用制御情報(Usage file)
305
暗号化タイトル鍵(Encrypted Title Key)
306
暗号化コンテンツ(Encrypted Content)
200
情報処理装置(ホスト)
325
署名鍵(Ksign)
S201a
署名データ(Sign)生成
S201b
署名データ(Sign)生成
Token=Sign(Ksign,FID)
Token=Sign(Ksign,CID)
S202
乱数生成(バインド鍵)
321
バインド鍵(Kb)
S203
AES-H
S204
S205
AES-E
S206
暗号化(Encrypt)
EncKt=AES-128E(Kb, Kt xor AES-H(Usage))
322
利用制御情報(Usage file)
323
タイトル鍵(Kt)
324
コンテンツ

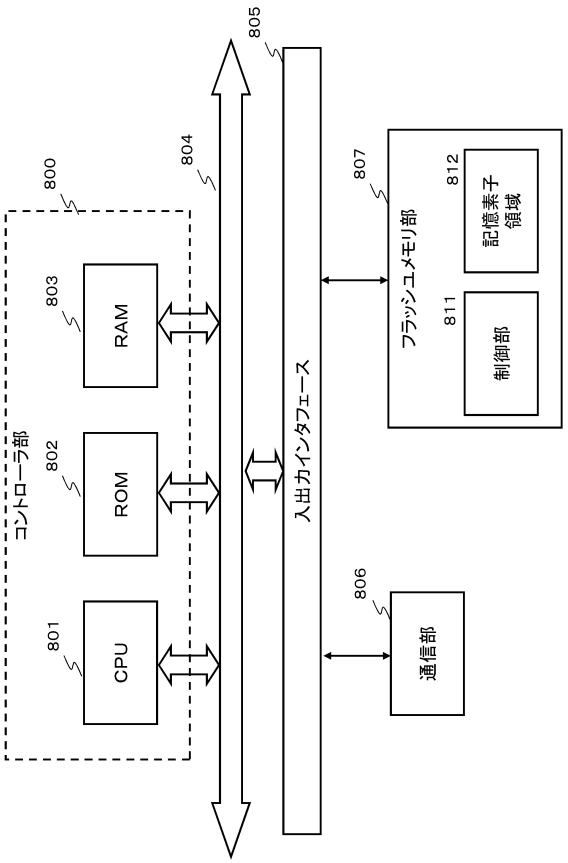
【図９】


スタート
S301
データ記憶装置（メモリカード）から
コントローラID（CID）と
フラッシュID（FID）を取得
S302
コントローラID（CID）と
フラッシュID（FID）、
に基づいて検証値
（MAC, or Token）を算出
S303
データ記憶装置から
照合用の検証値
（MAC or Token）を読み取り
S304
算出検証値と
照合用検証値の比較
S305
算出検証値＝
照合用検証値？
No
Yes
S306
暗号化コンテンツの読み取り、
復号、再生処理を開始
エンド

【図１０】


701
CPU
702
ROM
703
RAM
704
705
入出力インタフェース
706
入力部
707
出力部
708
記憶部
709
通信部
710
ドライブ
711
リムーバブル
メディア

【図１１】


800
コントローラ部
801
CPU
802
ROM
803
RAM
804
805
入出力インタフェース
806
通信部
807
フラッシュメモリ部
811
制御部
812
記憶素子
領域

フロントページの続き

(72)発明者　久野　浩
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　林　隆道
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　海老原　宗毅
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　上田　健二朗
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　吉村　光司
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　甲斐　哲雄

(56)参考文献　特開２００５－０１８４４５（ＪＰ，Ａ）
特開平０９－１３４３１１（ＪＰ，Ａ）
特開２００７－３１０７３２（ＪＰ，Ａ）
特開２００１－２５００９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｋ　１９／００－１９／１８
Ｇ０６Ｋ　１７／００
Ｇ０６Ｆ　２１／６０－２１／６４
Ｈ０４Ｌ　９／３２