(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2012-249035
(P2012-249035A)
(43)公開日　平成24年12月13日(2012.12.13)

| (51)Int.Cl. | | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| H04N | 7/167 | (2011.01) | H04N | 7/167 | Z | 5C164 |
| H04L | 9/08 | (2006.01) | H04L | 9/00 | 601B | 5J104 |
| | | | H04L | 9/00 | 601E | |

審査請求 未請求　請求項の数 17　ＯＬ　（全 41 頁）

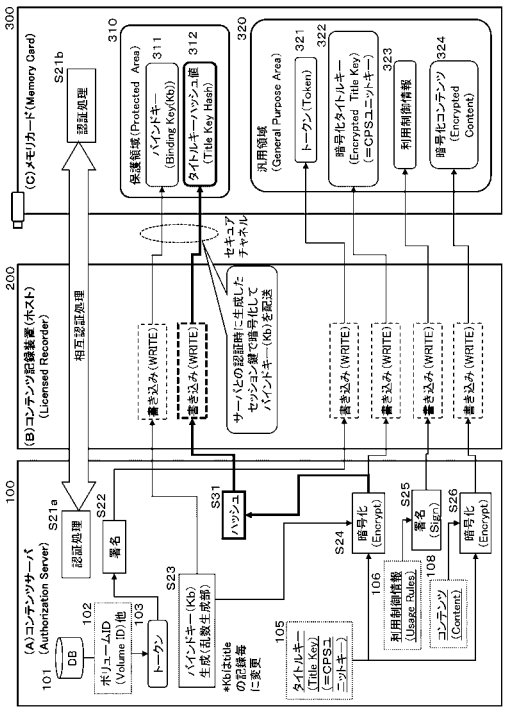
(21)出願番号　特願2011-118576 (P2011-118576)
(22)出願日　平成23年5月27日 (2011.5.27)

(71)出願人　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】情報処理装置、および情報処理方法、並びにプログラム

(57)【要約】
【課題】暗号化コンテンツの復号処理に際して適用する鍵の漏えいに基づくコンテンツ不正利用を防止する。
【解決手段】例えばサーバの提供コンテンツを格納するメモリカードに、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域と設定する。サーバは、タイトルキーで暗号化した暗号化コンテンツと、タイトルキーの暗号化キーであるバインドキーと、タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、暗号化タイトルキーのハッシュ値を生成して、メモリカードに出力する。メモリカードは、汎用領域に暗号化コンテンツと暗号化タイトルキーを格納し、保護領域に、バインドキーと暗号化タイトルキーのハッシュ値を格納し、コンテンツ再生時にハッシュ値の検証に基づいてコンテンツ再生許容判定を実行させる。
【選択図】図８



【特許請求の範囲】
【請求項１】
データ処理部と、記憶部を有し、
前記記憶部は、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記汎用領域に暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納し、
前記保護領域に、前記タイトルキーの暗号化に適用したバインドキーと、前記暗号化タイトルキーのハッシュ値を格納し、
前記データ処理部は、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容する情報処理装置。
【請求項２】
前記情報処理装置はメモリカードであり、
該メモリカードを装着した再生装置に、前記保護領域の格納ハッシュ値と、前記暗号化タイトルキーに基づく算出ハッシュ値との照合処理結果に基づく前記暗号化コンテンツの再生許容判定を実行させることを可能とした請求項１に記載の情報処理装置。
【請求項３】
前記データ処理部は、
前記暗号化コンテンツを提供するサーバの提供するサーバ証明書の記録情報に応じて、前記保護領域に対するサーバのアクセス許容判定を実行し、
前記サーバの提供する前記暗号化タイトルキーのハッシュ値を前記保護領域に格納する請求項１に記載の情報処理装置。
【請求項４】
前記サーバ証明書は、前記サーバの公開鍵を格納した公開鍵証明書であり、前記保護領域の区分領域単位のアクセス許容情報が記録された証明書である請求項３に記載の情報処理装置。
【請求項５】
コンテンツ再生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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行し、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出し、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応じてコンテンツの再生許容判定を行う情報処理装置。
【請求項６】
前記メモリカードは、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記データ処理部は、
前記汎用領域から、前記暗号化タイトルキーを読み出し、
前記保護領域から、前記照合用ハッシュ値を読み出す請求項５に記載の情報処理装置。
【請求項７】
前記データ処理部は、
前記メモリカードとの認証処理に際して、前記メモリカードに対して、前記保護領域に対するアクセス許容情報を記録した証明書を出力する請求項５に記載の情報処理装置。
【請求項８】
メモリカードに対するコンテンツ提供処理を実行するサーバ装置であり、
データ処理部が、

タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力して記録させる処理を実行し、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせるサーバ装置。
【請求項９】
前記サーバ装置は、
前記メモリカードの保護領域に対するアクセス許容情報を記録したサーバ証明書を保持し、
該サーバ証明書を前記メモリカードに提供して、前記メモリカードにアクセス可否判定を実行させる請求項８に記載のサーバ装置。
【請求項１０】
コンテンツ提供サーバと、
前記コンテンツ提供サーバの提供するコンテンツを格納するメモリカードを有する情報処理システムであり、
前記コンテンツ提供サーバは、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力し、
前記メモリカードは、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分された記憶部を有し、
前記汎用領域に前記暗号化コンテンツと、前記暗号化タイトルキーを格納し、
前記保護領域に、前記バインドキーと、前記暗号化タイトルキーのハッシュ値を格納し、
前記保護領域に対する前記コンテンツ提供サーバからのアクセス要求に応じて、前記コンテンツ提供サーバの提供する証明書を検証してアクセスを許容するか否かのアクセス可否判定を行う情報処理システム。
【請求項１１】
前記コンテンツ提供サーバは、
前記メモリカードの保護領域に対するアクセス許容情報を記録したサーバ証明書を保持し、
該サーバ証明書を前記メモリカードに提供して、前記メモリカードにアクセス可否判定を実行させる請求項１０に記載の情報処理システム。
【請求項１２】
データ処理部と、記憶部を有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、
前記記憶部は、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記データ処理部は、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容するアクセス許容判定処理を実行し、
前記アクセス許容判定処理においてアクセス許容判定がなされた場合に、前記アクセス前記保護領域に、前記外部装置の提供データである、
前記タイトルキーの暗号化に適用したバインドキーと、

前記暗号化タイトルキーのハッシュ値を格納し、
前記汎用領域に、前記外部装置の提供データである、
暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納する処理を行う情報処理方法。
【請求項１３】
情報処理装置においてコンテンツ再生処理を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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行し、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出し、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応じてコンテンツの再生許容判定を行う情報処理方法。
【請求項１４】
メモリカードに対するコンテンツ提供処理を実行するサーバ装置において実行する情報処理方法であり、
前サーバ装置のデータ処理部が、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力して記録させる処理を実行し、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせる情報処理方法。
【請求項１５】
データ処理部と、記憶部を有する情報処理装置において情報処理を実行させるプログラムであり、
前記記憶部は、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記データ処理部に、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容するアクセス許容判定処理を実行させ、
前記アクセス許容判定処理においてアクセス許容判定がなされた場合に、前記アクセス前記保護領域に、前記外部装置の提供データである、
前記タイトルキーの暗号化に適用したバインドキーと、
前記暗号化タイトルキーのハッシュ値を格納させ、
前記汎用領域に、前記外部装置の提供データである、
暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納させる処理を実行させるプログラム。
【請求項１６】
情報処理装置においてコンテンツ再生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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行させ、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出させ、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応じてコンテンツの再生許容判定を行わせるプログラム。

【請求項１７】
メモリカードに対するコンテンツ提供処理を実行するサーバ装置において情報処理を実行させるプログラムであり、
前サーバ装置のデータ処理部に、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力して記録させる処理を実行させ、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、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、例えばメモリカード等の記録メディアに記録するコンテンツの不正利用を効果的に防止する情報処理装置、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、情報記録媒体として、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】
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。
【０００４】
例えば、コンテンツの利用制御に関する規格としてＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）が知られている。ＡＡＣＳの規格は、例えばＢｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）の記録コンテンツに対する利用制御構成を定義している。具体的には例えばＢｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）に記録するコンテンツを暗号化コンテンツとして、その暗号鍵を取得できるユーザを正規ユーザにのみ限定することを可能とするアルゴリズムなどを規定している。
【０００５】
しかし、現行のＡＡＣＳ規定には、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）等のディスク記録コンテンツに対する利用制御構成についての規定は存在するが、例えばメモリカードなどのフラッシュメモリに記録されるコンテンツ等については、十分な規定がない。従って、このようなメモリカードの記録コンテンツについては、著作権の保護が不十分になる恐れがあり、これらメモリカード等のメディアを利用したコンテンツ利用に対する利用制御構成を構築することが要請されている。
【０００６】
例えばＡＡＣＳ規定では、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）等のディスク記録コンテンツに対する利用制御構成として以下のような規定がある。
（ａ）既にコンテンツの記録されたメディア（例えばＲＯＭディスク）からＢｌｕ－ｒ

ａｙ　Ｄｉｓｃ（登録商標）等のディスクにコピーされたコンテンツに対する利用規定、
（ｂ）サーバからダウンロードしてＢｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）等のディスクに記録されたコンテンツの利用規定、
例えば、このようなコンテンツの利用制御について規定している。
【０００７】
ＡＡＣＳでは、例えば上記（ａ）のメディア間のコンテンツコピーを実行する場合、管理サーバからコピー許可情報を取得することを条件としたマネージドコピー（ＭＣ：Ｍａｎａｇｅｄ　Ｃｏｐｙ）について規定している。
【０００８】
また、上記の（ｂ）のサーバからのコンテンツのダウンロード処理として、ＡＡＣＳでは、
ＰＣ等のユーザ装置を利用したＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓｅｌｌ　Ｔｈｒｏｕｇｈ）や、
コンビニ等に設置された共用端末を利用したＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎ　Ｄｅｍａｎｄ）、
これらの各種のダウンロード形態を規定して、これらの各ダウンロード処理によりディスクにコンテンツを記録して利用する場合についても、所定のルールに従った処理を行うことを義務付けている。
なお、これらの処理については、例えば特許文献１（特開２００８－９８７６５号公報）に記載されている。
【０００９】
しかし、前述したように、ＡＡＣＳの規定は、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）等のディスク記録コンテンツを利用制御対象として想定しているものであり、ＵＳＢルモリなどを含むフラッシュメモリタイプ等のメモリカードに記録されるコンテンツについては十分な利用制御に関する規定がないという問題がある。
【先行技術文献】
【特許文献】
【００１０】
【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】
【００１１】
本開示は、例えば上記問題点に鑑みてなされたものであり、フラッシュメモリ等のディスク以外の情報記録媒体（メディア）にコンテンツを記録して利用する場合の利用制御構成を確立して不正なコンテンツ利用を防止する構成を実現する情報処理装置、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】
【００１２】
本開示の第１の側面は、
データ処理部と、記憶部を有し、
前記記憶部は、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記汎用領域に暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納し、
前記保護領域に、前記タイトルキーの暗号化に適用したバインドキーと、前記暗号化タイトルキーのハッシュ値を格納し、
前記データ処理部は、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容する情報処理装置にある。

【００１３】
さらに、本開示の情報処理装置の一実施態様において、前記情報処理装置はメモリカードであり、該メモリカードを装着した再生装置に、前記保護領域の格納ハッシュ値と、前記暗号化タイトルキーに基づく算出ハッシュ値との照合処理結果に基づく前記暗号化コンテンツの再生許容判定を実行させることを可能とした。
【００１４】
さらに、本開示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、前記暗号化コンテンツを提供するサーバの提供するサーバ証明書の記録情報に応じて、前記保護領域に対するサーバのアクセス許容判定を実行し、前記サーバの提供する前記暗号化タイトルキーのハッシュ値を前記保護領域に格納する。
【００１５】
さらに、本開示の情報処理装置の一実施態様において、前記サーバ証明書は、前記サーバの公開鍵を格納した公開鍵証明書であり、前記保護領域の区分領域単位のアクセス許容情報が記録された証明書である。
【００１６】
さらに、本開示の第２の側面は、
コンテンツ再生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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行し、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出し、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応じてコンテンツの再生許容判定を行う情報処理装置にある。
【００１７】
さらに、本開示の情報処理装置の一実施態様において、前記メモリカードは、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、前記データ処理部は、前記汎用領域から、前記暗号化タイトルキーを読み出し、前記保護領域から、前記照合用ハッシュ値を読み出す。
【００１８】
さらに、本開示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、前記メモリカードとの認証処理に際して、前記メモリカードに対して、前記保護領域に対するアクセス許容情報を記録した証明書を出力する。
【００１９】
さらに、本開示の第３の側面は、
メモリカードに対するコンテンツ提供処理を実行するサーバ装置であり、
データ処理部が、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力して記録させる処理を実行し、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせるサーバ装置にある。
【００２０】
さらに、本開示のサーバ装置の一実施態様において、前記サーバ装置は、前記メモリカードの保護領域に対するアクセス許容情報を記録したサーバ証明書を保持し、該サーバ証明書を前記メモリカードに提供して、前記メモリカードにアクセス可否判定を実行させる。

【００２１】
さらに、本開示の第４の側面は、
コンテンツ提供サーバと、
前記コンテンツ提供サーバの提供するコンテンツを格納するメモリカードを有する情報処理システムであり、
前記コンテンツ提供サーバは、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力し、
前記メモリカードは、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分された記憶部を有し、
前記汎用領域に前記暗号化コンテンツと、前記暗号化タイトルキーを格納し、
前記保護領域に、前記バインドキーと、前記暗号化タイトルキーのハッシュ値を格納し、
前記保護領域に対する前記コンテンツ提供サーバからのアクセス要求に応じて、前記コンテンツ提供サーバの提供する証明書を検証してアクセスを許容するか否かのアクセス可否判定を行う情報処理システムにある。
【００２２】
さらに、本開示の情報処理システムの一実施態様において、前記コンテンツ提供サーバは、前記メモリカードの保護領域に対するアクセス許容情報を記録したサーバ証明書を保持し、該サーバ証明書を前記メモリカードに提供して、前記メモリカードにアクセス可否判定を実行させる。
【００２３】
さらに、本開示の第５の側面は、
データ処理部と、記憶部を有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、
前記記憶部は、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記データ処理部は、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容するアクセス許容判定処理を実行し、
前記アクセス許容判定処理においてアクセス許容判定がなされた場合に、前記アクセス前記保護領域に、前記外部装置の提供データである、
前記タイトルキーの暗号化に適用したバインドキーと、
前記暗号化タイトルキーのハッシュ値を格納し、
前記汎用領域に、前記外部装置の提供データである、
暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納する処理を行う情報処理方法にある。
【００２４】
さらに、本開示の第６の側面は、
情報処理装置においてコンテンツ再生処理を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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行し、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出し、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応

じてコンテンツの再生許容判定を行う情報処理方法にある。
【００２５】
さらに、本開示の第７の側面は、
メモリカードに対するコンテンツ提供処理を実行するサーバ装置において実行する情報処理方法であり、
前サーバ装置のデータ処理部が、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力して記録させる処理を実行し、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせる情報処理方法にある。
【００２６】
さらに、本開示の第８の側面は、
データ処理部と、記憶部を有する情報処理装置において情報処理を実行させるプログラムであり、
前記記憶部は、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記データ処理部に、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容するアクセス許容判定処理を実行させ、
前記アクセス許容判定処理においてアクセス許容判定がなされた場合に、前記アクセス前記保護領域に、前記外部装置の提供データである、
前記タイトルキーの暗号化に適用したバインドキーと、
前記暗号化タイトルキーのハッシュ値を格納させ、
前記汎用領域に、前記外部装置の提供データである、
暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納させる処理を実行させるプログラムにある。
【００２７】
さらに、本開示の第９の側面は、
情報処理装置においてコンテンツ再生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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行させ、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出させ、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応じてコンテンツの再生許容判定を行わせるプログラムにある。
【００２８】
さらに、本開示の第１０の側面は、
メモリカードに対するコンテンツ提供処理を実行するサーバ装置において情報処理を実行させるプログラムであり、
前サーバ装置のデータ処理部に、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、

生成データを前記メモリカードに出力して記録させる処理を実行させ、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせるプログラムにある。

【００２９】

なお、本開示のプログラムは、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。

【００３０】

本開示のさらに他の目的、特徴や利点は、後述する本開示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】

【００３１】

本開示の一実施例の構成によれば、暗号化コンテンツの復号処理に際して適用する鍵の漏えいに基づくコンテンツ不正利用を防止する構成が実現される。

具体的には、例えばサーバの提供コンテンツを格納するメモリカードに、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域と設定する。サーバは、タイトルキーで暗号化した暗号化コンテンツと、タイトルキーの暗号化キーであるバインドキーと、タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、暗号化タイトルキーのハッシュ値を生成して、メモリカードに出力する。メモリカードは、汎用領域に暗号化コンテンツと暗号化タイトルキーを格納し、保護領域に、バインドキーと暗号化タイトルキーのハッシュ値を格納し、コンテンツ再生時にハッシュ値の検証に基づいてコンテンツ再生許容判定を実行させる。

これらの構成により、万が一、バインドキーの漏えい等が発生した場合でも、暗号化タイトルキーを漏えいバインドキーで暗号化する等の不正処理を行った場合、ハッシュ値検証によって、その不正が検出可能となり、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】

【００３２】

【図１】コンテンツ提供処理および利用処理の概要について説明する図である。
【図２】メモリカードに記録されたコンテンツの利用形態について説明する図である。
【図３】メモリカードの記憶領域の具体的構成例について説明する図である。
【図４】サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）について説明する図である。
【図５】メモリカードの記憶領域の具体的構成例とアクセス制御処理の一例について説明する図である。
【図６】コンテンツサーバから提供されるコンテンツをメモリカードに記録する場合の処理シーケンスについて説明する図である。
【図７】コンテンツサーバが生成して提供するトークンの具体的なデータ構成例について説明する図である。
【図８】コンテンツサーバから提供されるコンテンツをメモリカードに記録する場合の処理シーケンスについて説明する図である。
【図９】暗号化タイトルキーのハッシュ値生成処理例について説明する図である。
【図１０】コンテンツの再生処理シーケンスについて説明するフローチャートを示す図である。
【図１１】コンテンツの再生処理シーケンスについて説明するフローチャートを示す図で

ある。
【図１２】メモリカードを装着してデータの記録や再生処理を行うホスト機器のハードウェア構成例について説明する図である。
【図１３】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】
【００３３】
以下、図面を参照しながら本開示の情報処理装置、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．コンテンツ提供処理および利用処理の概要について
２．メモリカードの構成例と利用例について
３．保護領域に対するアクセス許容情報を持つ証明書について
４．各装置の証明書を適用したメモリカードに対するアクセス処理例について
５．メモリカードに対するコンテンツや鍵情報等の書き込み処理例と問題点について
６．コンテンツの不正利用を防止可能とした構成について
７．コンテンツ再生処理について
８．各装置のハードウェア構成例について
９．本開示の構成のまとめ
【００３４】
［１．コンテンツ提供処理および利用処理の概要について］
【００３５】
以下、図面を参照しながら本発明の情報処理装置、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。
【００３６】
まず、図１以下を参照して、コンテンツ提供処理および利用処理の概要について説明する。
図１には、左から、
（ａ）コンテンツ提供元
（ｂ）コンテンツ記録装置（ホスト）
（ｃ）コンテンツ記録メディア
これらを示している。
【００３７】
（ｃ）コンテンツ記録メディアはユーザがコンテンツを記録して、コンテンツの再生処理に利用するメディアである。ここでは例えばフラッシュメモリ等の情報記録装置であるメモリカード３１を示している。
【００３８】
ユーザは、例えば音楽や映画などの様々なコンテンツをメモリカード３１に記録して利用する。これらのコンテンツは例えば著作権管理コンテンツ等、利用制御対象となるコンテンツである。所定の利用条件下での利用のみが許容され、基本的に無秩序なコピー処理やコピーデータの無制限な配布等は禁止される。なお、後述するがメモリカード３１に対して、コンテンツを記録する場合、そのコンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）、具体的には、許容されるコピー回数などのコピー制限情報などを規定した利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）も併せて記録される。
【００３９】
（ａ）コンテンツ提供元は、利用制限のなされた音楽や映画等のコンテンツの提供元である。図１には、コンテンツサーバ１１と、予めコンテンツの記録されたＲＯＭディスク等のコンテンツ記録ディスク１２を示している。
コンテンツサーバ１１は、音楽や映画等のコンテンツを提供するサーバである。コンテンツ記録ディスク１２は予め音楽や映画等のコンテンツを記録したＲＯＭディスク等のディスクである。
【００４０】

ユーザは、（ｃ）コンテンツ記録メディアであるメモリカード３１を（ｂ）コンテンツ記録装置（ホスト）に装着し、（ｂ）コンテンツ記録装置（ホスト）を介してコンテンツサーバ１１に接続して、コンテンツを受信（ダウンロード）してメモリカード３１に記録することができる。

【００４１】

なお、コンテンツサーバ１１は、このダウンロード処理に際して、所定のシーケンスに従った処理を行い、暗号化コンテンツの他、利用制御情報やトークン、さらに鍵情報（バインドキー）等のコンテンツ管理情報を提供する。これらの処理、および提供データについては、後段で詳細に説明する。

【００４２】

あるいは、（ｃ）コンテンツ記録メディアであるメモリカード３１を装着した（ｂ）コンテンツ記録装置（ホスト）に、予めコンテンツの記録されたＲＯＭディスク等のコンテンツ記録ディスク１２を装着してコンテンツ記録ディスク１２の記録コンテンツをメモリカード３１にコピーすることができる。ただし、このコピー処理を実行する場合にも、コンテンツサーバ１１に接続して所定のシーケンスに従った処理が必要となる。コンテンツサーバ１１は、このディスクからのコンテンツコピー処理に際して、コピーコンテンツに対応する利用制御情報やトークン、さらに鍵情報（バインドキー）等のコンテンツ管理情報を提供する。

【００４３】

（ｂ）コンテンツ記録装置（ホスト）は、（ｃ）コンテンツ記録メディアであるメモリカード３１を装着して、（ａ）コンテンツ提供元であるコンテンツサーバ１１からネットワークを介して受信（ダウンロード）したコンテンツ、あるいは、コンテンツ記録ディスク１２から読み取ったコンテンツをメモリカード３１に記録する。

【００４４】

（ｂ）コンテンツ記録装置（ホスト）としては、不特定多数のユーザが利用可能な公共スペース、例えば駅やコンビニ等に設置された共用端末２１、ユーザ機器としての記録再生器（ＣＥ（Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器）２２、ＰＣ２３などがある。これらはすべて（ｃ）コンテンツ記録メディアであるメモリカード３１を装着可能な装置である。

また、これらの（ｂ）コンテンツ記録装置（ホスト）は、コンテンツサーバ１１からのダウンロード処理を実行する構成である場合は、ネットワークを介したデータ送受信処理を実行することが可能な構成である。

コンテンツ記録ディスク１２を利用する構成の場合は、ディスクの再生可能な装置であることが必要である。

【００４５】

図１に示すように、ユーザは、

（ａ）コンテンツ提供元であるコンテンツサーバ１１からのダウンロードコンテンツ、あるいはＲＯＭディスク等のコンテンツ記録ディスク１２に記録されたコンテンツを（ｂ）コンテンツ記録装置（ホスト）を介して、（ｃ）コンテンツ記録メディアとしてのメモリカード３１に記録する。

【００４６】

このメモリカード３１に記録されたコンテンツの利用形態について図２を参照して説明する。

ユーザは、コンテンツを記録したメモリカード３１を、例えば、図１（ｂ）を参照して説明した（ｂ）コンテンツ記録装置（ホスト）としてのユーザ機器である記録再生器（ＣＥ機器）２２やＰＣ２３等に装着してメモリカード３１に記録されたコンテンツを読み取り、再生する。

【００４７】

なお、多くの場合、これらのコンテンツは暗号化コンテンツとして記録されており、記録再生器（ＣＥ機器）２２やＰＣ２３等の再生装置は、所定のシーケンスに従った復号処

理を実行した後、コンテンツ再生を行う。
なお、メモリカード３１に記録されたコンテンツを再生する機器は、図１（ｂ）を参照して説明した（ｂ）コンテンツ記録装置（ホスト）に限られず、その他の再生装置（プレーヤ）であってもよい。ただし、例えば予め規定されたシーケンスに従った暗号化コンテンツの復号処理等を実行可能な機器、すなわち予め規定された再生処理シーケンスを実行するプログラムを格納した機器であることが必要となる。なお、コンテンツ再生シーケンスの詳細については、後段で説明する。
【００４８】
［２．メモリカードの構成例と利用例について］
次に、コンテンツの記録メディアとして利用されるフラッシュメモリ等のメモリカードの構成例と利用例について説明する。
メモリカード３１の記憶領域の具体的構成例を図３に示す。
メモリカード３１の記憶領域は、図３に示すように、
（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１、
（ｂ）汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）５２、
これら２つの領域によって構成される。
【００４９】
（ｂ）汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）５２はユーザの利用する記録再生装置によって、自由にアクセス可能な領域であり、コンテンツや一般のコンテンツ管理データ等が記録される。ユーザによって自由にデータの書き込みや読み取りを行うことか可能な領域である。
【００５０】
一方、（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１は、自由なアクセスが許容されない領域である。
例えば、ユーザの利用する記録再生装置、再生装置、あるいはネットワークを介して接続されるサーバ等によってデータの書き込みあるいは読み取りを行おうとする場合、メモリカード３１のデータ処理部が、メモリカード３１に予め格納されたプログラムに従って、各装置に応じて読み取り（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）の可否を決定する。
【００５１】
メモリカード３１は、予め格納されたプログラムを実行するためのデータ処理部や認証処理を実行する認証処理部を備えており、メモリカード３１は、まず、メモリカード３１に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。
【００５２】
この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書（たとえばサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ））を受信し、その証明書に記載された情報を用いて、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１の各区分領域のアクセスが許容されるか否かを判定する。この判定処理は、図３に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１内の区分領域（図に示す領域＃０，＃１，＃２・・・）単位で判定処理が行われ、許可された区分領域で許可された処理（データの読み取り／書き込み等の処理）のみが実行される。
【００５３】
このメディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）は、例えば、アクセスしようとする装置、例えばコンテンツサーバ、あるいは記録再生装置（ホスト）単位で設定される。これらの情報は各装置対応のサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録される。
【００５４】
メモリカード３１は、メモリカード３１に予め格納された規定のプログラムに従って、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）の記録データを検証して、アクセス許可のなされた領域についてのみアクセスを許容する処理

を行う。

【００５５】

［３．保護領域に対するアクセス許容情報を持つ証明書について］

次に、上述したメモリカード３１の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１に対するアクセスを行う場合に、メモリカードに提示が必要となる証明書の構成例について図４を参照して説明する。

【００５６】

上述したように、メモリカード３１は、メモリカード３１に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書（たとえばサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ））を受信し、その証明書に記載された情報を用いて、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１の各区分領域のアクセスを許容するか否かを判定する。

【００５７】

この認証処理に利用される装置証明書の一例として、サーバに提供されるサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）の構成例について図４を参照して説明する。

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、例えば、公開鍵証明書発行主体である認証局によって例えば、コンテンツ提供を行うコンテンツサーバ等の各サーバに提供される。例えば、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、認証局がコンテンツ提供処理を認めたサーバに対して発行するサーバの証明書であり、サーバ公開鍵等を格納した証明書である。サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、認証局秘密鍵によって署名が設定され、改ざんの防止されたデータとして構成される。

【００５８】

図４に認証局が各コンテンツサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）の具体例を示す。

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）には、図４に示すように、以下のデータが含まれる。

（１）タイプ情報

（２）サーバＩＤ

（３）サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）

（４）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）

（５）その他の情報

（６）署名（Ｓｉｇｎａｕｒｅ）

【００５９】

以下、上記（１）～（６）の各データについて説明する。

（１）タイプ情報

タイプ情報は、証明書のタイプやコンテンツサーバのタイプを示す情報であり、例えば本証明書がサーバ証明書であることを示すデータや、サーバの種類、例えば音楽コンテンツの提供サーバであるとか、映画コンテンツの提供サーバであるといったサーバの種類などを示す情報が記録される。

【００６０】

（２）サーバＩＤ

サーバＩＤはサーバ識別情報としてのサーバＩＤを記録する領域である。

（３）サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）

サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）はサーバの公開鍵である。サーバに提供されるサーバ秘密鍵とともに公開鍵暗号方式に従った鍵ペアを構成する。

【００６１】

（４）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒ

ｉｔｅ）
メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）は、コンテンツを記録するメディア、例えば図１、図２に示すメモリカード３１、あるいは図３に示すメモリカード３１の記憶領域中に設定される保護領域（ＰＤＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）内のデータ読み取り（Ｒｅａｄ）や、書き込み（Ｗｒｉｔｅ）が許容された区分領域についての情報が記録される。
【００６２】
（５）その他の情報、（６）書名（Ｓｉｇｎａｔｕｒｅ）
サーバ証明書には、上記（１）～（４）の他、様々な情報が記録され、（１）～（５）の情報に対する署名データが記録される。
署名は、認証局の秘密鍵によって実行される。サーバ証明書に記録された情報、例えばサーバ公開鍵を取り出して利用する場合には、まず認証局の公開鍵を適用した署名検証処理を実行して、サーバ証明書の改ざんがないことを確認し、その確認がなされたことを条件として、サーバ公開鍵等の証明書格納データの利用が行われることになる。
【００６３】
［４．各装置の証明書を適用したメモリカードに対するアクセス処理例について］
図４を参照して説明したように、メモリカード３１の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１に対してアクセスを行う場合には、図４に示すような証明書をメモリカードに提示することが必要となる。
メモリカードは、図４に示す証明書を確認して、図３に示すメモリカード３１の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１に対するアクセス可否を判定する。
【００６４】
サーバは、例えば図４を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）を保持し、コンテンツの再生等を行う記録再生装置等のホスト機器はホスト機器に対応する証明書（ホスト証明書）を保持している。
これらの各装置が、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセスを行う場合には、証明書をメモリカードに提供してメモリカード側の検証に基づくアクセス可否の判定を受けることが必要となる。
【００６５】
図５を参照して、メモリカードに対するアクセス要求装置がサーバである場合と、記録再生装置等のホスト機器である場合のアクセス制限の設定例について説明する。
【００６６】
図５には、左から、メモリカードに対するアクセス要求装置であるサーバ６１、ホスト機器６２、メモリカード７０を示している。
サーバ６１は、例えば、メモリカード７０に対する記録コンテンツであるダウンロードコンテンツや、ディスクからのコピーコンテンツの再生時に必要となる鍵情報（バインドキーなど）の書き込み処理を、メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に対して実行するサーバである。
ホスト機器６２は、メモリカード７０に格納されたコンテンツの再生処理を行う装置であり、コンテンツの復号処理のために、メモリカード７０に記録されたバインドキーを取得する必要がある機器である。
【００６７】
メモリカード７０は、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０と、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０を有し、暗号化コンテンツ等は汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０に記録される。
コンテンツ再生に際して必要とする鍵であるバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）は保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に記録される。
【００６８】
先に図３を参照して説明したように、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０は、複数の領域に区分されている。

図５に示す例では、
区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１、
区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２、
これらの２つの区分領域を持つ例を示している。

【００６９】

これらの区分領域の設定態様としては様々な設定が可能である。
図５に示す例では、一例として、区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１は、放送コンテンツの鍵データとしてのバインドキー記録領域、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２は、ダウンロード、コピーコンテンツの鍵データとしてのバインドキー記録領域として設定された例を示している。

【００７０】

このような設定において、例えばダウンロードコンテンツの提供サーバは、提供コンテンツの復号に必要となるバインドキーを、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２に記録する。
この場合、サーバ６１のサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）に記録される書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）は、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に対する書き込み（Ｗｒｉｔｅ）許可が設定された証明書として構成される。
なお、図に示す例では、書き込み（Ｗｒｉｔｅ）の許容された区分領域に対しては、読み取り（Ｒｅａｄ）についても許容された設定として示している。

【００７１】

また、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２に記録されたバインドキーを読み取ってコンテンツ再生を実行する再生装置であるホスト機器６２の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に対する読み取り（Ｒｅａｄ）許可のみが設定された証明書として構成される。

【００７２】

ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に対する書き込み（Ｗｒｉｔｅ）許可は設定されない。
ただし、コンテンツ削除時に、削除コンテンツに対応するバインドキーの削除が可能な設定とするため、削除処理については許可する設定としてもよい。

【００７３】

すなわち、メモリカードのデータ処理部は、アクセス要求装置からの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に対するデータ書き込みとデータ読み取りについては、書く装置の装置証明書に基づいて許可するか否かを判定するが、削除要求についてはすべて許可する設定としてもよい。

【００７４】

あるいは、アクセス要求装置の証明書に、区分領域単位の書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の各処理についての許容情報に加えて、削除（ｄｅｌｅｔｅ）についての許容情報を記録して、この記録情報に基づいて削除の可否を判定する構成としてもよい。

【００７５】

図５に示すメモリカード７０の区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１は、放送コンテンツの鍵データとしてのバインドキー記録領域として設定された例を示している。
放送コンテンツは、例えば、レコーダ、あるいはＰＣ等、放送データの受信、記録機能を持つホスト機器６２が放送局からのコンテンツを受信してメディアに記録する。

【００７６】

この場合、放送コンテンツの復号のために適用する鍵情報であるバインドキーは、放送局が提供し、ホスト機器６２が受信する。ホスト機器６２はメモリカード７０にアクセス

を行い、メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に放送コンテンツ用の鍵データを記録する。

【００７７】

この例では、放送コンテンツ用の鍵データを記録する領域は、区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１として予め規定されている。

メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０は、このように、区分領域（＃０，＃１，＃２・・・）単位で、記録するデータの種類を予め規定することが可能である。

【００７８】

メモリカードは、アクセス要求装置からのデータ書き込みや読み取り要求の入力に応じて、書き込みあるいは読み取り要求データの種類を判別し、データ書き込み先あるいは読み取り先としての区分領域（＃０，＃１，＃２・・・）を選別する。

【００７９】

放送コンテンツの復号のために適用する鍵情報であるバインドキーは、ホスト機器６２が書き込み処理を実行し、再生処理においても、ホスト機器６２が読み取り処理を実行する。

【００８０】

従って、ホスト機器６２の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、放送コンテンツ用の鍵データの記録領域として規定された区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１については、書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の双方の処理許可が設定された証明書として構成される。

【００８１】

図５に示すホスト機器６２の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒ）は、図に示すように、

読み取り（Ｒｅａｄ）許容領域：＃０，＃１

書き込み（Ｗｒｉｔｅ）許容領域：＃０

これらの設定のなされた証明書となる。

【００８２】

一方、サーバ６１はこの放送コンテンツ用の鍵データの記録領域として規定された区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１に対しては、データ書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）のいずれも許可されておらず、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）にはデータ書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の非許可情報が記録される。

【００８３】

図５に示すサーバ６１の保持するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒ）は、図に示すように、

読み取り（Ｒｅａｄ）許容領域：＃１

書き込み（Ｗｒｉｔｅ）許容領域：＃１

これらの設定のなされた証明書となる。

【００８４】

このように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）は、アクセス要求装置単位、かつ区分領域（＃０，＃１，＃２・・・）単位で、データの書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の許容、非許容がアクセス制御情報として設定される。

【００８５】

このアクセス制御情報は、各アクセス要求装置の証明書（サーバ証明書、ホスト証明書など）に記録され、メモリカードは、アクセス要求装置から受領した証明書について、まず署名検証を行い、正当性を確認した後、証明書に記載されたアクセス制御情報、すなわち、以下の情報を読み取る。

読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）、

書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）、
これらの情報に基づいて、アクセス要求装置に対して認められた処理のみを許容して実行する。
【００８６】
なお、ホスト機器にも、例えばレコーダ、プレーヤ等のＣＥ機器や、ＰＣ等、様々な機器の種類がある。
装置証明書は、これらの各装置が個別に保持する証明書であり、これらの装置の種類に応じて異なる設定とすることができる。
また、メモリカードのデータ処理部は、装置証明書に記録された以下の情報、すなわち、
読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）、
書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）、
これらの情報のみならず、例えば、図４を参照して説明した証明書に含まれるタイプ情報（Ｔｙｐｅ）に基づいて、保護領域の区分領域単位のアクセスの許容判定を行ってもよい。
【００８７】
［５．メモリカードに対するコンテンツや鍵情報等の書き込み処理例と問題点について］
次に、図６を参照して、メモリカードに対するコンテンツや鍵情報等の書き込み処理例と問題点について説明する。
なお、図６を参照して説明する処理例は、コンテンツの不正利用の排除が困難になってしまう問題点を含む処理例である。後段で図８を参照して説明する本開示に従った処理例は、この問題点を解決する構成を持つ。
【００８８】
まず、図６を参照して問題点を含む処理シーケンスについて説明する。
図６には、左から、
（Ａ）コンテンツサーバ１００
（Ｂ）コンテンツ記録装置（ホスト）２００
（Ｃ）メモリカード３００
これらを示している。
【００８９】
（Ａ）コンテンツサーバ１００は、メモリカード３００に記録するコンテンツの提供を行うサーバである。
（Ｂ）コンテンツ記録装置２００は、メモリカード３００を装着して、メモリカード３００に対するデータ記録や読み出しを実行するＰＣや、記録再生機器等の装置である。
（Ｃ）メモリカード３００はコンテンツおよびコンテンツの再生時に適用する鍵情報等を記録する例えばフラッシュメモリによって構成される記憶装置（メディア）であり、先に図３、図５を参照して説明したように、保護領域と汎用領域を持つ記憶装置である。
【００９０】
図６には、コンテンツサーバ１００がメモリカード３００に対して、コンテンツと、コンテンツ以外のコンテンツ管理情報を提供して記録させる場合の処理シーケンスを示している。
なお、コンテンツを図１に示すディスク１２からコピーしてメモリカードに記録する場合は、コンテンツはディスクからメモリカード３００に記録されるが、その他のトークンを含む管理データについては、コンテンツサーバ１００からメモリカード３００に送信されて記録される。
【００９１】
なお、図６に示す（Ｃ）メモリカード３００は、（Ｂ）コンテンツ記録装置（ホスト）２００に装着し、（Ｂ）コンテンツ記録装置（ホスト）２００の通信部を介して（Ａ）コンテンツサーバ１００との通信を実行し、（Ａ）コンテンツサーバ１００から受信する各

種のデータを（Ｂ）コンテンツ記録装置（ホスト）２００を介して受信してメモリカード３００に記録する。

【００９２】

図６を参照して処理シーケンスについて説明する。

まず、ステップＳ２１において、コンテンツサーバ１００とメモリカード３００間で相互認証処理を実行する。例えば公開鍵暗号方式に従って、双方の公開鍵証明書の交換処理等を含む相互認証処理を行う。コンテンツサーバ１００は先に説明したように、認証局の発行した公開鍵を格納したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）と秘密鍵を保持している。メモリカード３００も予め認証局から公開鍵証明書と秘密鍵のペアを受信し自己の記憶部に格納している。

【００９３】

なお、メモリカード３００は相互認証処理や、図３や図５を参照して説明した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセス可否判定を行うプログラムを格納し、これらのプログラムを実行するデータ処理部を有する。

【００９４】

コンテンツサーバ１００とメモリカード３００間の相互認証が成立し、双方の正当性が確認されると、サーバ１００はメモリカード３００に対して様々なデータを提供する。相互認証が成立しない場合は、サーバ１００からのデータ提供処理は行われない。

【００９５】

相互認証の成立後、コンテンツサーバ１００は、データベース１０１に記録されたボリュームＩＤ等のデータを取得して、トークン１０３を生成し、ステップＳ２２においてトークンに対する署名を実行して、これをメモリカード３００に対する書き込みデータとして、コンテンツ記録装置（ホスト）２００に送信する。

【００９６】

トークン１０３について、図７を参照して説明する。トークン１０３は、図７に示すように例えば以下のデータを含むデータである。

（１）ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）

（２）コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）

（３）コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））

（４）利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）

（５）タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）

（６）その他の情報

（７）署名（Ｓｉｇｎａｔｕｒｅ）

【００９７】

以下、上記の各データについて説明する。

（１）ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）

ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）は、所定単位（例えばタイトル単位）のコンテンツに対応する識別子（ＩＤ）である。このＩＤは、例えばコンテンツ再生時に利用可能性のあるＪａｖａ（登録商標）アプリケーションであるＢＤ－Ｊ／ＡＰＩやＢＤ＋ＡＰＩ等によって参照される場合があるデータである。

【００９８】

（２）コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）

コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）はコンテンツを識別する識別子であるが、トークンに記録されるコンテンツＩＤは、コンテンツまたはコンテンツ管理データ（トークンを含む）を提供したサーバＩＤを含むデータとして設定される。すなわち、

コンテンツＩＤ＝サーバＩＤ（Ｓｅｒｖｅｒ　ＩＤ）＋コンテンツ固有ＩＤ（Ｕｎｉｑｕｅ　Ｃｏｎｔｅｎｔ　ＩＤ）

上記のようにサーバＩＤを含むデータとしてコンテンツＩＤが記録される。

【００９９】

サーバＩＤは、認証局が各コンテンツサーバに設定したＩＤである。先に図４を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録されたサーバＩＤと同じＩＤである。

コンテンツ固有ＩＤは、コンテンツサーバが独自に設定するコンテンツ対応の識別子（ＩＤ）である。

トークンに記録されるコンテンツＩＤは、このように認証局の設定したサーバＩＤとコンテンツサーバの設定したコンテンツ固有ＩＤの組み合わせとして構成される。

【０１００】

なお、コンテンツＩＤの構成ビット数や、サーバＩＤのビット数、コンテンツ固有ＩＤのビット数は予め規定されており、コンテンツを再生する再生装置は、トークンに記録されたコンテンツＩＤから所定ビット数の上位ビットを取得してサーバＩＤを取得し、コンテンツＩＤから所定の下位ビットを取得することでコンテンツ固有ＩＤを得ることが可能となる。

【０１０１】

（３）コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））

コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））は、メモリカードに格納されるコンテンツのハッシュ値を記録したデータである。このデータは、コンテンツが改ざん検証処理に利用される。

【０１０２】

コンテンツを再生する再生装置は、メモリカードに記録された再生予定のコンテンツのハッシュ値を計算し、トークンに記録されたコンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））の記録値との比較を実行する。計算データと登録データとが一致としていればコンテンツの改ざんはないと判定されコンテンツ再生が可能となる。一致しない場合は、コンテンツは改ざんされている可能性があると判定され、再生は禁止される。

【０１０３】

（４）利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）

利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）はサーバがコンテンツの管理データとしてユーザに提供しメモリカードに記録させる利用制御情報のハッシュ値である。

利用制御情報は、例えばコンテンツのコピーを許容するか否か、コピーの許容回数、他機器への出力可否などのコンテンツの利用形態の許容情報などを記録したデータであり、コンテンツとともにメモリカードに記録される情報である。

利用制御情報ハッシュ値は、この利用制御情報の改ざん検証用のデータとして利用されるハッシュ値である。

【０１０４】

コンテンツを再生する再生装置は、メモリカードに記録された再生予定のコンテンツに対応する利用制御情報のハッシュ値を計算し、トークンに記録された利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）の記録値との比較を実行する。計算データと登録データとが一致としていれば利用制御情報の改ざんはないと判定され、利用制御情報に従ったコンテンツ利用が可能となる。一致しない場合は、利用制御情報は改ざんされている可能性があると判定され、コンテンツの再生等の利用処理は禁止される。

【０１０５】

（５）タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）

タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）は、このトークンの作成日時、例えば図７の（７）に示す署名の作成日時情報である。

【０１０６】

トークン（Ｔｏｋｅｎ）には、上述したデータの他、図７に示すように［（６）その他の情報］が記録され、さらに、（１）～（６）の各データに対してサーバの秘密鍵によっ

て生成された（７）署名（Ｓｉｇｎａｔｕｒｅ）が記録される。この署名によりトークンの改ざん防止構成が実現される。

【０１０７】

トークン（Ｔｏｋｅｎ）を利用する場合は、署名検証を実行して、トークン（Ｔｏｋｅｎ）が改ざんのない正当なトークンであることを確認した上で利用が行われる。なお、署名検証は、サーバの公開鍵を利用して実行される。サーバの公開鍵は、先に図４を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）から取得可能である。

【０１０８】

図６に戻り、コンテンツの記録処理シーケンスについての説明を続ける。

図７を参照して説明したデータを含むトークンが、（Ａ）コンテンツサーバ１００から（Ｂ）コンテンツ記録装置（ホスト）２００を介して（Ｃ）メモリカード３００に送信され、メモリカード３００に記録される。この記録データが図６の（Ｃ）メモリカード３００中に示すトークン（Ｔｏｋｅｎ）３２１である。

【０１０９】

なお、メモリカード３００は、先に図３、図５を参照して説明したように保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）と汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に分割されている。

図６に示す（Ｃ）メモリカード３００の保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）３１０には、図に示すようにバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１が記録される。その他のデータは、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）３２０に記録される。

【０１１０】

なお、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１は暗号化コンテンツの復号に適用するタイトルキー（ＣＰＳユニットキーとも呼ばれる）の暗号化処理に利用される鍵であり、コンテンツサーバにおいて乱数生成処理等によって生成される。

【０１１１】

図６（Ａ）コンテンツサーバ１００のステップＳ２３の処理として示すように、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））は、コンテンツサーバにおいて生成される。この鍵は、コンテンツのメモリカードに対する提供処理、あるいはディスクからのコンテンツのコピー処理が実行される毎に、サーバが、逐次、乱数生成等を実行して生成してメモリカードに提供する。従って、コンテンツの提供あるいはコピー処理ごとに異なるバインドキーが生成されることになる。

【０１１２】

サーバ１００の生成したバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））は、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に書き込まれる。

なお、先に図５を参照して説明したように、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に対するデータの書き込み（Ｗｒｉｔｅ）、あるいは保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）からのデータ読み込み（Ｒｅａｄ）処理は、アクセス許可を持つ装置によって実行可能となる制限された処理として行われる。

【０１１３】

アクセス要求装置（サーバや、記録再生装置（ホスト））単位、および各区分領域（＃１，＃２・・・）単位で書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の可否が設定されている。この設定情報はサーバであればサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）、記録再生装置（ホスト）であればホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録されている。

【０１１４】

メモリカード３００は、アクセス要求装置から受領した証明書、本例ではサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を参照して、書き込みの許容された保護領域内の区分領域にバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））を記録する。図６に示すバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１である。なお、図６では、保護領域（Ｐｒｏ

ｔｅｃｔｅｄ　Ａｒｅａ）３１０の内部を詳細に示していないが、この保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０は図３を参照して説明したように複数の区分領域（＃０，＃１，＃２・・・）に区分されており、サーバ証明書に書き込み許容領域として記録された区分領域にバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１が記録される。

【０１１５】

なお、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）はステップＳ２１の認証処理に際して、メモリカード３００がコンテンツサーバ１００から受領した証明書を参照することができる。なお、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）には認証局の署名が設定され、メモリカード３００は認証局の公開鍵を適用して署名検証を実行し、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）の正当性を確認していることが前提となる。

【０１１６】

なお、コンテンツサーバ１００からメモリカード３００へのバインドキーの送信は、セッションキーで暗号化したデータとして安全な通信路であるセキュアチャンネルを介して行われる。

セッションキーは、サーバ１００とメモリカード３００間の相互認証処理（ステップＳ２１）時に生成され、双方で共有する鍵である。メモリカード３００は、暗号化されたバインドキーをセッションキーで復号してメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０の所定の区分領域に記録する。

【０１１７】

図６に示す（Ａ）コンテンツサーバ１００は、次に、生成したバインドキー（Ｋｂ）を利用して、ステップＳ２４において、コンテンツの暗号化キーであるタイトルキー１０５を暗号化して暗号化タイトルキーを生成する。

【０１１８】

（Ａ）コンテンツサーバ１００は生成した暗号化タイトルキーを（Ｂ）コンテンツ記録装置（ホスト）２００を介して（Ｃ）メモリカード３００に送信する。メモリカード３００は、受信した暗号化タイトルキーをメモリカードに記録する。この記録データが図６の（Ｃ）メモリカード３００中の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）３２０に示す暗号化タイトルキー３２２である。なお、タイトルキーはＣＰＳユニットキーとも呼ばれる。

【０１１９】

さらに、コンテンツサーバ１００は、コンテンツに対応する利用制御情報１０６を生成して、ステップＳ２５でコンテンツサーバ１００の秘密鍵で署名処理を実行してメモリカード３００に提供する。

また、コンテンツサーバ１００は、ステップＳ２６において、コンテンツ１０８をタイトルキー１０５で暗号化してメモリカード３００に提供する。コンテンツ１０８は、例えば映画等、ユーザが再生装置のディスプレイに表示、あるいはスピーカに出力して視聴する再生対象コンテンツである。

【０１２０】

メモリカード３００は、これらのサーバ１００からの提供データを記録する。この記録データが図６の（Ｃ）メモリカード３００中に示す利用制御情報３２３、暗号化コンテンツ３２４である。

【０１２１】

なお、図６に示す処理シーケンス中には示していないが、コンテンツサーバ１００は、これらのデータの他、例えば、

（１）コンテンツリボケーションリスト（ＣＲＬ）

（２）サーバリボケーションリスト（ＳＲＬ）

これらのデータをメモリカード３００に提供し、メモリカード３００はこれらのデータをメモリカード３００に記録する。

【０１２２】

コンテンツリボケーションリスト（ＣＲＬ）とは、無効化されたコンテンツの識別情報

を記載したリストであり、サーバリボケーションリスト（ＳＲＬ）は無効化されたサーバの識別情報を記載したリストである。

ユーザ装置において、コンテンツ再生やコンテンツ取得を行う際に、これらのリストを参照して、再生予定のコンテンツが無効化されているか否かを確認し、またコンテンツを取得したサーバが無効化されていないかを確認し、無効化されている場合には、コンテンツの再生やコンテンツ取得を中止する処理が行われることになる。

【０１２３】

次に、図６を参照して説明したコンテンツ記録シーケンスにおける問題点について説明する。

図６に示す処理において、メモリカード３００に記録された暗号化コンテンツ３２４の復号処理において適用する鍵情報であるバインドキー３１１は、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に格納され、一見すると安全に格納されているように見える。

【０１２４】

しかし、このバインドキー３１１は、コンテンツ再生を実行する再生装置によって、再生装置の証明書を提示すれば、メモリカード３００の保護領域３１０から読み取って利用される。

従って、例えば、この証明書と、メモリカード３００との認証処理に適用する秘密鍵が漏えいし、不正装置がこれらの漏えいデータを取得した場合、その不正装置は、メモリカードとの認証に成功し、メモリカードの保護領域からバインドキー３１１を不正に取得することが可能となる。

このように、何らかの方法でバインドキーの漏えいが発生してしまった場合、次のような不正処理が行われる可能性がある。

【０１２５】

様々なコンテンツに対応するタイトルキーを取得して、漏えいバインドキーを利用して暗号化する。この処理によって、

（ａ）漏えいバインドキーと、

（ｂ）漏えいバインドキーによって暗号化されたタイトルキー

（ｃ）タイトルキーによって暗号化された暗号化コンテンツ

この３つの組み合わせが完成してしまう。

【０１２６】

上記３つの組み合わせが設定されれば、再生装置は、以下の予め既定された正常なコンテンツ再生シーケンス（（Ｓ１）～（Ｓ２））に従って、暗号化コンテンツの復号、再生を行うことが可能になる。

（Ｓ１）漏えいバインドキーによって暗号化された暗号化タイトルキーを、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に格納された漏えいバインドキーで復号してタイトルキーを取得する。

（Ｓ２）取得したタイトルキーを利用して暗号化コンテンツを復号、再生する。

【０１２７】

上記の処理は、様々なコンテンツに対して実行可能であり、各コンテンツに対応するタイトルキーを漏えいしたバインドキーで暗号化することで、様々なコンテンツの不正利用の可能性が高まることになる。

すなわち、例えば以下のような処理が想定される。

コンテンツＡに対応して設定されたタイトルキーａ、

コンテンツＢに対応して設定されたタイトルキーｂ、

コンテンツＣに対応して設定されたタイトルキーｃ、

：

上記の様々なコンテンツ対応のタイトルキーを漏えいしたバインドキーを適用して暗号化してメモリカードの汎用領域に格納する。

【０１２８】

この処理によってあらゆる暗号化コンテンツＡ，Ｂ，Ｃ・・・を上記の正常なコンテンツ再生シーケンス（（Ｓ１）～（Ｓ２））に従って復号、再生を行うことが可能になる。
例えば、漏えいバインドキーを不特定多数のクライアントであるメモリカードを持つユーザの再生装置に提供することで、これらのクライアント集団では、不正なコンテンツ利用が可能となる。

【０１２９】
なお、各コンテンツに対応するタイトルキーは、正常な処理シーケンスにおいては、サーバから配信単位で生成される固有のバインドキーによって暗号化されてクライアント側のメモリカードに提供される。しかし、不正なバインドキーの読み出しを行う不正再生装置によって、バインドキーの読み出しが実行されて、暗号化タイトルキーを復号してタイトルキーを取得し、不特定多数のクライアントに提供済みの漏えいバインドキーを用いて再暗号化して、これらのクライアントに提供する処理が行われると、それらのコンテンツに対して上記の正常なコンテンツ再生シーケンス（（Ｓ１）～（Ｓ２））に従って復号、再生を行うことが可能になり、多くのコンテンツの不正利用が行われてしまうことになる。

【０１３０】
このように、１つのバインドキーを様々なコンテンツ対応のタイトルキーの暗号化キーとして適用してタイトルキーの再暗号化処理を行い、これらの再暗号化タイトルキーと暗号化コンテンツを記録したメディアなどが海賊版として流通するといった事態も想定し得る。

【０１３１】
このように、図６に示す設定では、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に格納されたバインドキー３１１が、一旦、漏えいしてしまうと、不正なコンテンツ利用が行われる可能性が高まるという問題点がある。

【０１３２】
［６．コンテンツの不正利用を防止可能とした構成について］
次に、上述したバインドキーの漏えいによるコンテンツの不正利用を防止可能とした構成について説明する。
本構成におけるコンテンツ記録シーケンスについて、図８を参照して説明する。
図８には、図６と同様、左から、
（Ａ）コンテンツサーバ１００
（Ｂ）コンテンツ記録装置（ホスト）２００
（Ｃ）メモリカード３００
これらを示している。

【０１３３】
（Ａ）コンテンツサーバ１００は、メモリカード３００に記録するコンテンツの提供を行うサーバである。
（Ｂ）コンテンツ記録装置２００は、メモリカード３００を装着して、メモリカード３００に対するデータ記録や読み出しを実行するＰＣや、記録再生機器等の装置である。
（Ｃ）メモリカード３００はコンテンツおよびコンテンツの再生時に適用する鍵情報等を記録する例えばフラッシュメモリによって構成される記憶装置（メディア）であり、先に図３、図５を参照して説明したように、保護領域と汎用領域を持つ記憶装置である。

【０１３４】
図８には、コンテンツサーバ１００がメモリカード３００に対して、コンテンツと、コンテンツ以外のコンテンツ管理情報を提供して記録させる場合の処理シーケンスを示している。
なお、コンテンツを図１に示すディスク１２からコピーしてメモリカードに記録する場合は、コンテンツはディスクからメモリカードに記録されるが、その他のトークンを含む管理データについては、コンテンツサーバ１００からメモリカード３００に送信されて記録される。

【０１３５】
なお、図８に示す（Ｃ）メモリカード３００は、（Ｂ）コンテンツ記録装置（ホスト）２００に装着し、（Ｂ）コンテンツ記録装置（ホスト）２００の通信部を介して（Ａ）コンテンツサーバ１００との通信を実行し、（Ａ）コンテンツサーバ１００から受信する各種のデータを（Ｂ）コンテンツ記録装置（ホスト）２００を介して受信してメモリカード３００に記録する。
【０１３６】
図８を参照して処理シーケンスについて説明する。
なお、図８において、図６と同様のデータについては同じ参照番号を設定し、同じ処理については、同じ処理番号（Ｓｘｘ）を設定している。
【０１３７】
まず、ステップＳ２１において、コンテンツサーバ１００とメモリカード３００間で相互認証処理を実行する。例えば公開鍵暗号方式に従って、双方の公開鍵証明書の交換処理等を含む相互認証処理を行う。コンテンツサーバ１００は先に説明したように、認証局の発行した公開鍵を格納したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）と秘密鍵を保持している。メモリカード３００も予め認証局から公開鍵証明書と秘密鍵のペアを受信し自己の記憶部に格納している。
【０１３８】
なお、メモリカード３００は相互認証処理や、図３や図５を参照して説明した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセス可否判定を行うプログラムを格納し、これらのプログラムを実行するデータ処理部を有する。
【０１３９】
コンテンツサーバ１００とメモリカード３００間の相互認証が成立し、双方の正当性が確認されると、サーバ１００はメモリカード３００に対して様々なデータを提供する。相互認証が成立しない場合は、サーバ１００からのデータ提供処理は行われない。
【０１４０】
相互認証の成立後、コンテンツサーバ１００は、データベース１０１に記録されたボリュームＩＤ等のデータを取得して、トークン１０３を生成し、ステップＳ２２においてトークンに対する署名を実行して、これをメモリカード３００に対する書き込みデータとして、コンテンツ記録装置（ホスト）２００に送信する。
【０１４１】
トークン１０３については、先に図７を参照して説明した通り、例えば以下のデータを含むデータである。
（１）ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）
（２）コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）
（３）コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））
（４）利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）
（５）タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）
（６）その他の情報
（７）署名（Ｓｉｇｎａｔｕｒｅ）
【０１４２】
トークン（Ｔｏｋｅｎ）は、（１）～（６）の各データに対してサーバの秘密鍵によって生成された（７）署名（Ｓｉｇｎａｔｕｒｅ）が記録される。この署名によりトークンの改ざん防止構成が実現される。
【０１４３】
トークン（Ｔｏｋｅｎ）を利用する場合は、署名検証を実行して、トークン（Ｔｏｋｅｎ）が改ざんのない正当なトークンであることを確認した上で利用が行われる。なお、署名検証は、サーバの公開鍵を利用して実行される。サーバの公開鍵は、先に図４を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）から取得可能である

。
【０１４４】
図７を参照して説明したデータを含むトークンが、（Ａ）コンテンツサーバ１００から（Ｂ）コンテンツ記録装置（ホスト）２００を介して（Ｃ）メモリカード３００に送信され、メモリカード３００に記録される。この記録データが図８の（Ｃ）メモリカード３００中に示すトークン（Ｔｏｋｅｎ）３２１である。
【０１４５】
なお、メモリカード３００は、先に図３、図５を参照して説明したように保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）と汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に分割されている。
図８に示す（Ｃ）メモリカード３００の保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）３１０には、図に示すようにバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１が記録される。その他のデータは、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）３２０に記録される。
【０１４６】
なお、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１は暗号化コンテンツの復号に適用するタイトルキー（ＣＰＳユニットキーとも呼ばれる）の暗号化処理に利用される鍵であり、コンテンツサーバにおいて乱数生成処理等によって生成される。
【０１４７】
図８（Ａ）コンテンツサーバ１００のステップＳ２３の処理として示すように、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））は、コンテンツサーバにおいて生成される。この鍵は、コンテンツのメモリカードに対する提供処理、あるいはディスクからのコンテンツのコピー処理が実行される毎に、サーバが、逐次、乱数生成等を実行して生成してメモリカードに提供する。従って、コンテンツの提供あるいはコピー処理ごとに異なるバインドキーが生成されることになる。
【０１４８】
サーバ１００の生成したバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））は、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に書き込まれる。
なお、先に図３、図５を参照して説明したように、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に対するデータの書き込み（Ｗｒｉｔｅ）、あるいは保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）からのデータ読み込み（Ｒｅａｄ）処理は、アクセス許可を持つ装置によって実行可能となる制限された処理として行われる。
【０１４９】
メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０は、アクセス要求装置（サーバや、記録再生装置（ホスト））単位、および各区分領域（＃１，＃２・・・）単位で書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の可否が設定されている。この設定情報はサーバであればサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）、記録再生装置（ホスト）であればホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録されている。
【０１５０】
メモリカード３００は、アクセス要求装置から受領した証明書、本例ではサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を参照して、書き込みの許容された保護領域内の区分領域にバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））を記録する。図８に示すバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１である。なお、図８では、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０の内部を詳細に示していないが、この保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０は図３を参照して説明したように複数の区分領域（＃０，＃１，＃２・・・）に区分されており、サーバ証明書に書き込み許容領域として記録された区分領域にバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））３１１が記録される。
【０１５１】
なお、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）はステップＳ２１の認証処理に際して、メモリカード３００がコンテンツサーバ１００から受領した証明書を参照することがで

きる。なお、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）には認証局の署名が設定され、メモリカード３００は認証局の公開鍵を適用して署名検証を実行し、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）の正当性を確認していることが前提となる。

【０１５２】

なお、コンテンツサーバ１００からメモリカード３００へのバインドキーの送信は、セッションキーで暗号化したデータとして安全な通信路としてのセキュアチャンネルを介して行われる。

セッションキーは、サーバ１００とメモリカード３００間の相互認証処理（ステップＳ２１）時に生成され、双方で共有する鍵である。メモリカード３００は、暗号化されたバインドキーをセッションキーで復号してメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０の所定の区分領域に記録する。

【０１５３】

図８に示す（Ａ）コンテンツサーバ１００は、次に、生成したバインドキー（Ｋｂ）を適用してステップＳ２４において、コンテンツの暗号化キーであるタイトルキー１０５を暗号化して暗号化タイトルキーを生成する。

【０１５４】

（Ａ）コンテンツサーバ１００は生成した暗号化タイトルキーを（Ｂ）コンテンツ記録装置（ホスト）２００を介して（Ｃ）メモリカード３００に送信する。メモリカード３００は、受信した暗号化タイトルキーをメモリカードに記録する。この記録データが図８の（Ｃ）メモリカード３００中の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）３２０に示す暗号化タイトルキー３２２である。なお、タイトルキーはＣＰＳユニットキーとも呼ばれる。

【０１５５】

さらに、コンテンツサーバ１００は、コンテンツに対応する利用制御情報１０６を生成して、ステップＳ２５でコンテンツサーバ１００の秘密鍵で署名処理を実行してメモリカード３００に提供する。

また、コンテンツサーバ１００は、ステップＳ２６において、コンテンツ１０８をタイトルキー１０５で暗号化してメモリカード３００に提供する。コンテンツ１０８は、例えば映画等、ユーザが再生装置のディスプレイに表示、あるいはスピーカに出力して視聴する再生対象コンテンツである。

【０１５６】

メモリカード３００は、これらのサーバ１００からの提供データを記録する。この記録データが図８の（Ｃ）メモリカード３００中に示す利用制御情報３２３、暗号化コンテンツ３２４である。

【０１５７】

なお、図８に示す処理シーケンス中には示していないが、コンテンツサーバ１００は、これらのデータの他、例えば、

（１）コンテンツリボケーションリスト（ＣＲＬ）

（２）サーバリボケーションリスト（ＳＲＬ）

これらのデータをメモリカード３００に提供し、メモリカード３００はこれらのデータをメモリカード３００に記録する。

【０１５８】

この図８に示す処理において、図６に示されない処理が、図８のステップＳ３１に示す処理である。

コンテンツサーバ１００は、ステップＳ３１において、ステップＳ２４で生成した暗号化タイトルキーのハッシュ値を算出する。

ハッシュ値算出に適用するハッシュアルゴリズムとしては、例えばＳＨＡ－１や、ＡＥＳ暗号を利用したハッシュ関数などが適用可能である。

【０１５９】

ハッシュ値算出処理例を図９に示す。

例えば図９（ａ）に示すように、コンテンツに対応して設定されるタイトルキーが１つである場合は、その１つのタイトルキーをバインドキーで暗号化した暗号化タイトルキーに対するハッシュ値算出を行う。
また、図９（ｂ）に示すように、コンテンツに対応して設定されるタイトルキーが複数ある場合は、各タイトルキーをバインドキーで暗号化した複数の暗号化タイトルキーに対するハッシュ値算出を行う。
【０１６０】
本実施例では、コンテンツサーバ１００は、ステップＳ３１において、ステップＳ２４で生成した暗号化タイトルキーのハッシュ値を算出し、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に格納する。
図８のメモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０内のタイトルキーハッシュ値（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）３１２である。
なお、コンテンツサーバ１００からメモリカード３００へのタイトルキーハッシュ値（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）の送信は、セッションキーで暗号化したデータとして安全な通信路としてのセキュアチャンネルを介して行われる。
【０１６１】
本実施例では、このように、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０内に、
バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）３１１、
タイトルキーハッシュ値（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）３１２、
これらのデータを格納する。
これらの各データは、コンテンツ再生を実行する再生装置によって読み取られ、予め設定された再生シーケンスの中で利用されることになる。
【０１６２】
［７．コンテンツ再生処理について］
次に、図８を参照して説明したコンテンツ記録シーケンス、すなわち、
バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）３１１、
タイトルキーハッシュ値（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）３１２、
これらのデータをメモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０内に格納した場合のコンテンツ再生シーケンスについて、図１０、図１１に示すフローチャートを参照して説明する。
【０１６３】
図１０、図１１に示すコンテンツ再生処理は、図８を参照して説明したコンテンツ記録シーケンスに従って、コンテンツや鍵情報等が記録されたメモリカード３００を装着した再生装置において実行される。
【０１６４】
再生装置は、例えば図２に示す記録再生器２２、ＰＣ２３、あるいは再生処理のみを行う再生装置等の様々な装置である。なお、これらの再生装置には、以下に説明するフローに従った再生シーケンスを実行するためのプログラムが格納されており、そのプログラムに従って再生伴う様々な処理、例えばコンテンツの復号処理や、管理データの検証、管理データを適用したコンテンツ検証等を実行する。
【０１６５】
図１０に示すフローチャートについて説明する。
ステップＳ１０１において、再生対象となるコンテンツと管理データを格納したメデイア（メモリカード）を装着し、再生対象コンテンツのユーザ指定等により再生コンテンツが選択される。
【０１６６】
ステップＳ１０２において、再生装置とメモリカード間において、相互認証処理を実行する。例えば公開鍵暗号方式に従って、双方の公開鍵証明書の交換処理等を含む相互認証処理を行う。なお、再生装置は、認証局の発行した公開鍵を格納した証明書と秘密鍵を保

持している。メモリカードも予め認証局から公開鍵証明書と秘密鍵のペアを受信し自己の記憶部に格納している。

【０１６７】

再生装置とメモリカード間の相互認証が成立しなかった場合（ステップＳ１０３の判定＝Ｎｏ）は、コンテンツ再生処理は中止される。

再生装置とメモリカード間の相互認証が成立し、双方の正当性が確認されると（ステップＳ１０３の判定＝Ｙｅｓ）、ステップＳ１０４に進む。

【０１６８】

再生装置は、ステップＳ１０４において、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）から、バインドキーと、タイトルキーハッシュを読み取る。

図８に示す、メモリカード３００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）３１０に格納された、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）３１１と、タイトルキーハッシュ（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）３１２である。

【０１６９】

次に、再生装置は、ステップＳ１０５において、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から、暗号化タイトルキーを読み取る。

図８に示すメモリカード３００の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）３２０に格納された暗号化タイトルキー（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）３２２である。

【０１７０】

次に、再生装置は、ステップＳ１０６において、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から読み取った暗号化タイトルキーのハッシュ値を算出する。このハッシュ算出アルゴリズムは、先に図８を参照して説明したステップＳ３１においてコンテンツサーバ１００が実行したハッシュ値算出処理と同じアルゴリズムを利用して行われる。

【０１７１】

次に、再生装置は、ステップＳ１０７において、ステップＳ１０６で算出したハッシュ値と、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）から読み取ったタイトルキーハッシュ（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）とを比較する。

【０１７２】

次に、図１１に示すステップＳ１０８において、

算出ハッシュ値＝保護領域に格納されたタイトルキーハッシュ（Ｔｉｔｌｅ　Ｋｅｙ　Ｈａｓｈ）

上記式が成立するか否かを判定する。

上記式が成立すれば、

暗号化タイトルキーは、正当な暗号化タイトルキーであると判定し、ステップＳ１０９に進む。

すなわち、上記式が成立した場合は、図８を参照して説明したコンテンツサーバ１００の提供した暗号化タイトルキーに間違いないと判定することができる。

【０１７３】

例えば、前述したように、暗号化タイトルキーが、漏えいしたバインドキーによって再暗号化されている場合、上記式は成立しない。

ステップＳ１０８のハッシュ値比較において、照合不成立の場合は、暗号化タイトルキーが不正に改ざんされている可能性があると判定し、ステップＳ１５１に進み、コンテンツ再生を中止する。

【０１７４】

ステップＳ１０８のハッシュ値比較において、照合成立の場合は、暗号化タイトルキーが改ざんのない正しい鍵であると判定し、ステップＳ１０９に進む。

ステップＳ１０９では、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）から読み取ったバインドキーを適用した暗号化タイトルキーの復号処理を実行して、タイト

ルキーを取得する。

【０１７５】

次に、再生装置は、ステップＳ１１０において、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）からトークン、利用制御情報を読み取り、これらのデータに設定された改ざん検証用の署名検証を実行する。

ステップＳ１１１において検証成立と判定されると、ステップＳ１１２に進み、検証不成立の場合は、ステップＳ１５１に進み再生処理を中止する。

【０１７６】

ステップＳ１１１において検証成立と判定され、トークン、利用制御情報の正当性が確認された場合は、ステップＳ１１２に進み、トークン、利用制御情報の構成データに基づくコンテンツの検証や許容処理の確認等を実行する。

次に、ステップＳ１１３において、再生装置は、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から読み取った暗号化コンテンツを、ステップＳ１０９において取得したタイトルキーを適用して復号し、コンテンツ再生を実行する。

【０１７７】

このように、再生装置は、コンテンツ再生処理に際して、

メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録されている暗号化タイトルキーのハッシュ値を算出し、

さらに、予めメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録されているタイトルキーハッシュ値との比較照合処理を実行する。

この照合において、両ハッシュ値が一致すれば、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録されている暗号化タイトルキーは、サーバが生成し、提供した暗号化タイトルキーであることが確認される。

【０１７８】

例えば、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録されている暗号化タイトルキーが、漏えいしたバインドキーによる再暗号化された不正なキーである場合は、ハッシュ値照合が不成立となり、コンテンツ再生が中止されることになり、不正なコンテンツ利用が防止されることになる。

【０１７９】

［８．各装置のハードウェア構成例について］

最後に、図１２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１２を参照して、メモリカードを装着してデータの記録や再生処理を行うホスト機器のハードウェア構成例について説明する。

【０１８０】

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サーバとの通信処理やサーバからの受信データのメモリカード(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。

【０１８１】

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。

【０１８２】
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。
【０１８３】
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等の各種データを取得する例えば、。取得されたコンテンツや鍵データを用いて、ＣＰＵによって実行する再生プログラムに従ってコンテンツの復号、再生処理などが行われる。
【０１８４】
図１３は、メモリカードのハードウェア構成例を示している。
ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）８０１は、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）８０２、または記憶部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サーバやホスト機器との通信処理やデータの記憶部８０７に対する書き込み、読み取り等の処理、記憶部８０７の保護領域８１１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。
【０１８５】
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、記憶部８０７が接続されている。
【０１８６】
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。記憶部８０７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 Ａｒｅａ）８１１、自由にデータ記録読み取りができる汎用領域（Ｇｅｎｅｒａｌ Ｐｕｒｐｏｓｅ Ａｒｅａ）８１２を有する。
【０１８７】
なお、サーバは、例えば図１２に示すホスト機器と同様のハードウェア構成を持つ装置によって実現可能である。
【０１８８】
［９．本開示の構成のまとめ］
以上、特定の実施例を参照しながら、本開示の実施例について詳解してきた。しかしながら、本開示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。本開示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。
【０１８９】
なお、本明細書において開示した技術は、以下のような構成をとることができる。
（１）データ処理部と、記憶部を有し、
前記記憶部は、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、
前記汎用領域に暗号化コンテンツと、該暗号化コンテンツの復号に適用するタイトルキーを暗号化した暗号化タイトルキーを格納し、
前記保護領域に、前記タイトルキーの暗号化に適用したバインドキーと、前記暗号化タイトルキーのハッシュ値を格納し、

前記データ処理部は、
前記保護領域に対する外部装置からのアクセス要求に応じて、アクセスを許容するか否かの判定処理を行い、アクセス許容判定がなされた場合にのみ、前記保護領域に対するアクセスを許容する情報処理装置。
【０１９０】
（２）前記情報処理装置はメモリカードであり、該メモリカードを装着した再生装置に、前記保護領域の格納ハッシュ値と、前記暗号化タイトルキーに基づく算出ハッシュ値との照合処理結果に基づく前記暗号化コンテンツの再生許容判定を実行させることを可能とした上記（１）に記載の情報処理装置。
（３）前記データ処理部は、前記暗号化コンテンツを提供するサーバの提供するサーバ証明書の記録情報に応じて、前記保護領域に対するサーバのアクセス許容判定を実行し、前記サーバの提供する前記暗号化タイトルキーのハッシュ値を前記保護領域に格納する上記（１）または（２）に記載の情報処理装置。
（４）前記サーバ証明書は、前記サーバの公開鍵を格納した公開鍵証明書であり、前記保護領域の区分領域単位のアクセス許容情報が記録された証明書である上記（１）～（３）いずれかに記載の情報処理装置。
【０１９１】
（５）コンテンツ再生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、
再生対象コンテンツを格納したメモリカードとの認証処理を実行し、
前記認証処理が成立したメモリカードから、暗号化コンテンツの暗号化に適用されたタイトルキーの暗号化データである暗号化タイトルキーを読み出して、暗号化タイトルキーのハッシュ値を算出し、
前記メモリカードから取得した照合用ハッシュ値との照合処理を実行して照合結果に応じてコンテンツの再生許容判定を行う情報処理装置。
【０１９２】
（６）前記メモリカードは、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分され、前記データ処理部は、前記汎用領域から、前記暗号化タイトルキーを読み出し、前記保護領域から、前記照合用ハッシュ値を読み出す上記（５）に記載の情報処理装置。
（７）前記データ処理部は、前記メモリカードとの認証処理に際して、前記メモリカードに対して、前記保護領域に対するアクセス許容情報を記録した証明書を出力する上記（５）または（６）に記載の情報処理装置。
【０１９３】
（８）　メモリカードに対するコンテンツ提供処理を実行するサーバ装置であり、
データ処理部が、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力して記録させる処理を実行し、
前記メモリカード内のアクセス制限記憶領域である保護領域に対するアクセス要求を出力し、該アクセス要求に対する前記メモリカードのアクセス許可に応じて前記ハッシュ値の前記保護領域に対する記録処理を行わせるサーバ装置。
（９）前記サーバ装置は、前記メモリカードの保護領域に対するアクセス許容情報を記録したサーバ証明書を保持し、該サーバ証明書を前記メモリカードに提供して、前記メモリカードにアクセス可否判定を実行させる上記（８）に記載のサーバ装置。
【０１９４】
（１０）　コンテンツ提供サーバと、
前記コンテンツ提供サーバの提供するコンテンツを格納するメモリカードを有する情報

処理システムであり、
前記コンテンツ提供サーバは、
タイトルキーで暗号化した暗号化コンテンツと、
前記タイトルキーの暗号化キーであるバインドキーと、
前記タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、
前記暗号化タイトルキーのハッシュ値を生成し、
生成データを前記メモリカードに出力し、
前記メモリカードは、
アクセス制限のなされた保護領域と、アクセス制限のない汎用領域とに区分された記憶部を有し、
前記汎用領域に前記暗号化コンテンツと、前記暗号化タイトルキーを格納し、
前記保護領域に、前記バインドキーと、前記暗号化タイトルキーのハッシュ値を格納し、
前記保護領域に対する前記コンテンツ提供サーバからのアクセス要求に応じて、前記コンテンツ提供サーバの提供する証明書を検証してアクセスを許容するか否かのアクセス可否判定を行う情報処理システム。

【０１９５】
さらに、上記した装置およびシステムにおいて実行する処理の方法や、処理を実行させるプログラムも本開示の構成に含まれる。

【０１９６】
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。

【０１９７】
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。

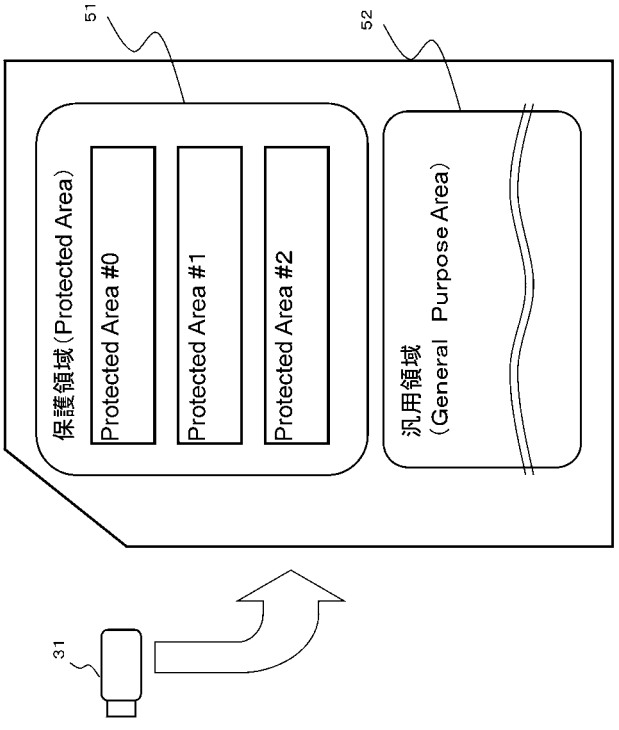
【産業上の利用可能性】

【０１９８】
以上、説明したように、本開示の一実施例の構成によれば、暗号化コンテンツの復号処理に際して適用する鍵の漏えいに基づくコンテンツ不正利用を防止する構成が実現される。
具体的には、例えばサーバの提供コンテンツを格納するメモリカードに、アクセス制限のなされた保護領域と、アクセス制限のない汎用領域と設定する。サーバは、タイトルキーで暗号化した暗号化コンテンツと、タイトルキーの暗号化キーであるバインドキーと、タイトルキーを前記バインドキーで暗号化したした暗号化タイトルキーと、暗号化タイトルキーのハッシュ値を生成して、メモリカードに出力する。メモリカードは、汎用領域に暗号化コンテンツと暗号化タイトルキーを格納し、保護領域に、バインドキーと暗号化タイトルキーのハッシュ値を格納し、コンテンツ再生時にハッシュ値の検証に基づいてコンテンツ再生許容判定を実行させる。
これらの構成により、万が一、バインドキーの漏えい等が発生した場合でも、暗号化タイトルキーを漏えいバインドキーで暗号化する等の不正処理を行った場合、ハッシュ値検証によって、その不正が検出可能となり、コンテンツの不正利用を防止することが可能と

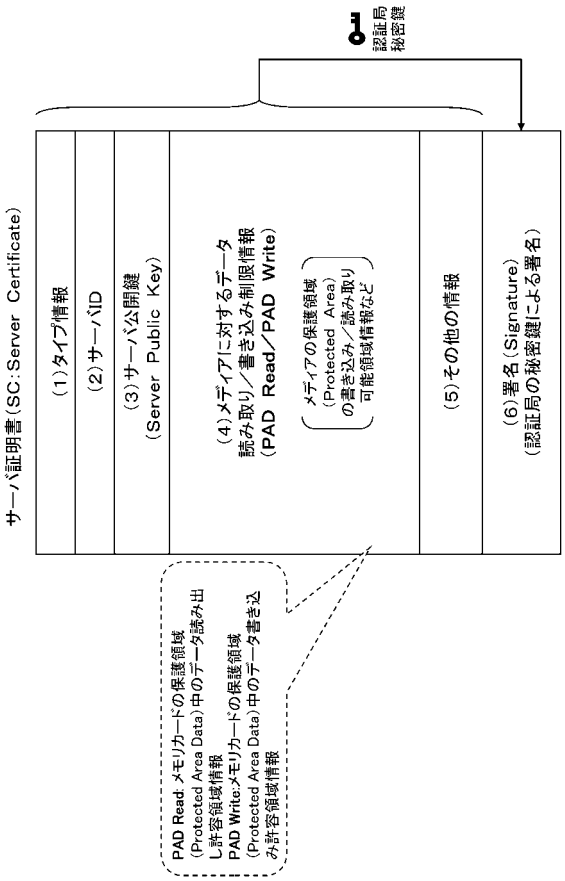
なる。
【符号の説明】
【０１９９】
１１　コンテンツサーバ
１２　コンテンツ記録ディスク
２１　共用端末
２２　記録再生器（ＣＥ機器）
２３　ＰＣ
３１　メモリカード
５１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
５２　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
６１　サーバ
６２　ホスト機器
７０　メモリカード
８０　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
８１，８２　区分領域
９０　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
１００　コンテンツサーバ
１０１　データベース（ＤＢ）
１０２　ボリュームＩＤ
１０３　トークン
１０５　タイトルキー（ＣＰＳユニットキー）
１０６　利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）
１０８　コンテンツ
２００　コンテンツ記録装置（ホスト）
３００　メモリカード
３１０　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
３１１　バインドキー
３１２　タイトルキーハッシュ値
３２０　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
３２１　トークン
３２２　暗号化タイトルキー
３２３　利用制御情報
３２４　暗号化コンテンツ
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
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　記憶部
８１１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
８１２　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）

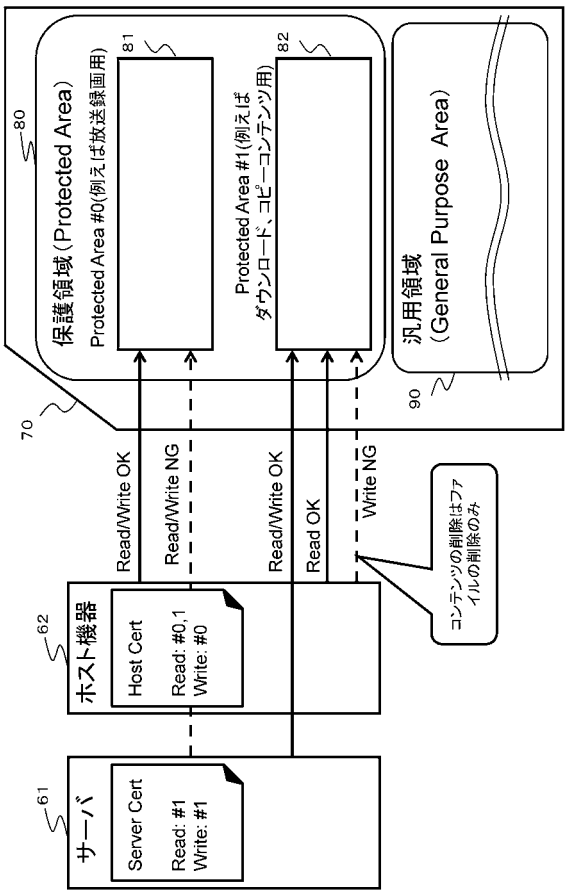
【図３】



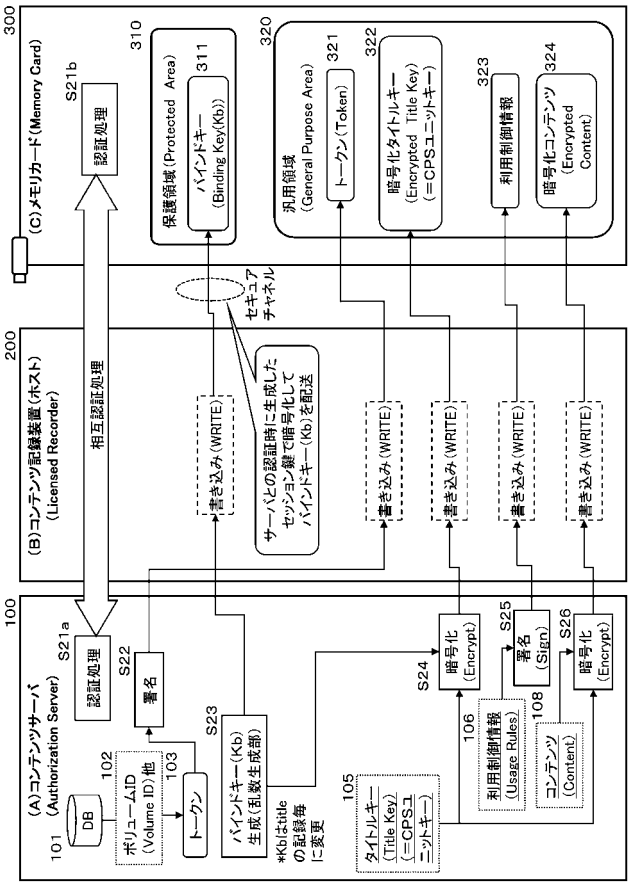

【図４】



【図５】




【図６】

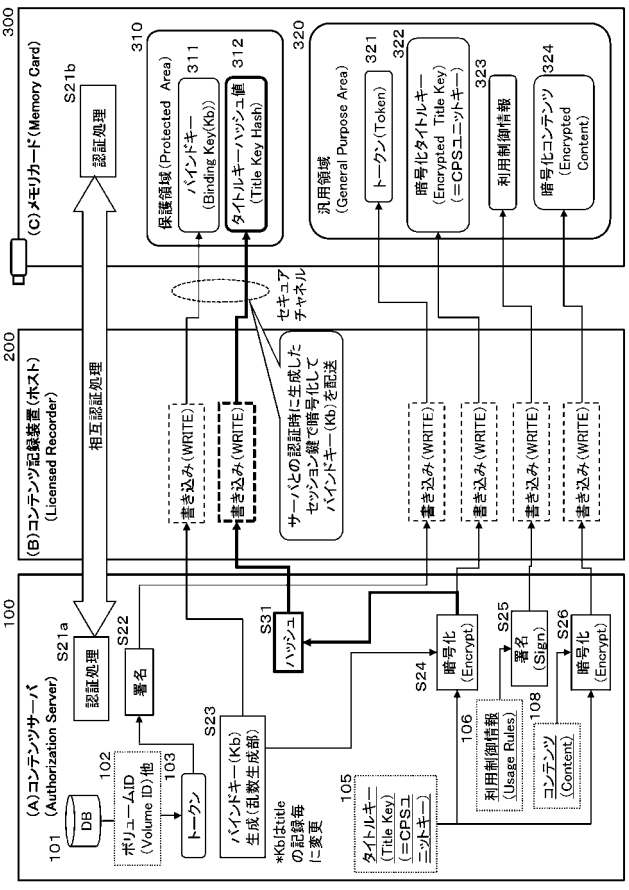



【図７】

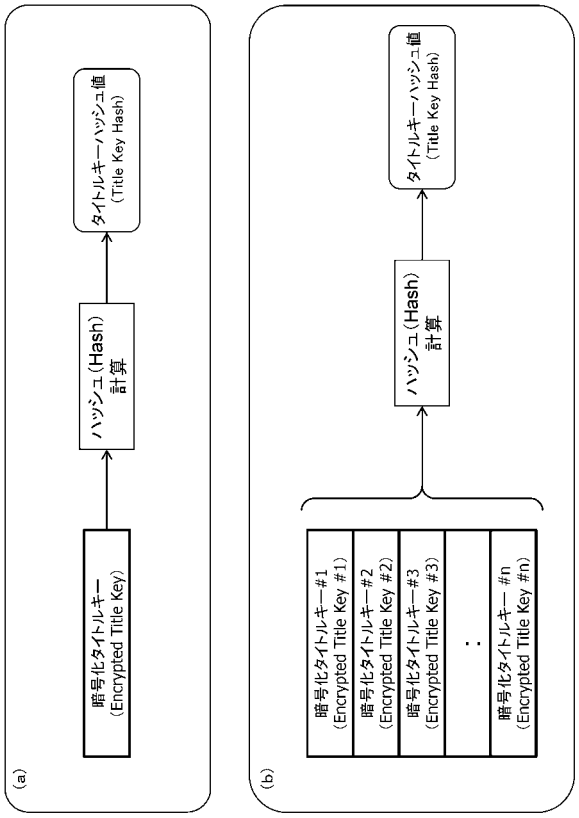
| | トークン記録データ | 説明, 具体例 |
|---|---|---|
| (1) | ボリュームID(PV Volume ID) | 所定単位(例えばタイトル単位コンテンツ)に対応する識別子(ID)である。記録データに含まれるBD-J API(やBD+ API)等によって利用される可能性有り |
| (2) | コンテンツID(Content ID) | サーバID(Server ID)+コンテンツID(Unique Content ID)<br>サーバIDは認証局が設定<br>コンテンツIDは、コンテンツサーバが設定 |
| (3) | コンテンツハッシュテーブルダイジェスト<br>(Content Hash Table Digest(s)) | コンテンツのハッシュ値のダイジェスト(要約値) |
| (4) | 利用制御情報ハッシュ値<br>(Usage Rule Hash) | 利用制御情報のハッシュ値 |
| (5) | タイムスタンプ<br>(Timestamp) | 署名を設定した日時情報 |
| (6) | その他の情報 | |
| (7) | 署名<br>(Signature) | 認証局の発行したコンテンツサーバの秘密鍵による署名<br>(トークン構成データに対する署名) |

サーバ秘密鍵

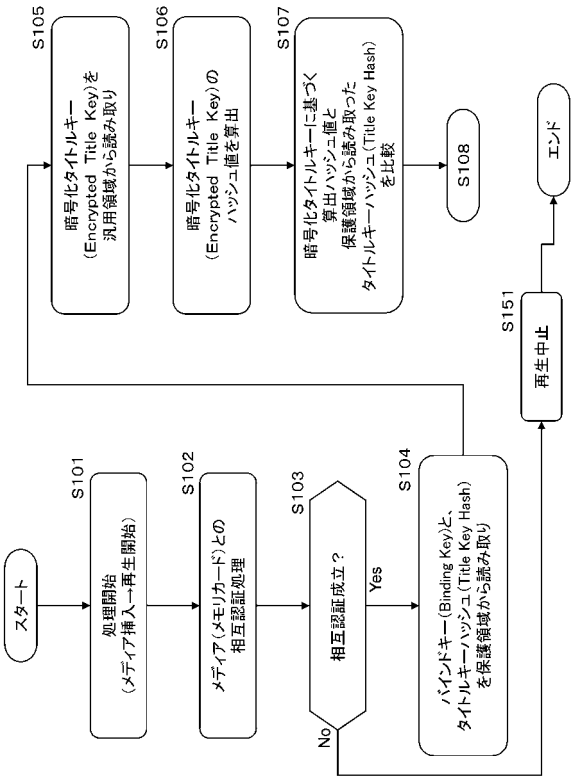
【図８】



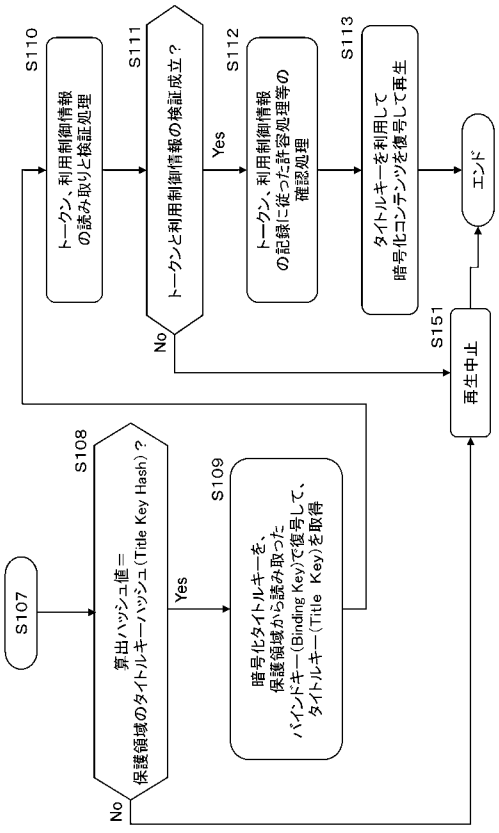
【図９】



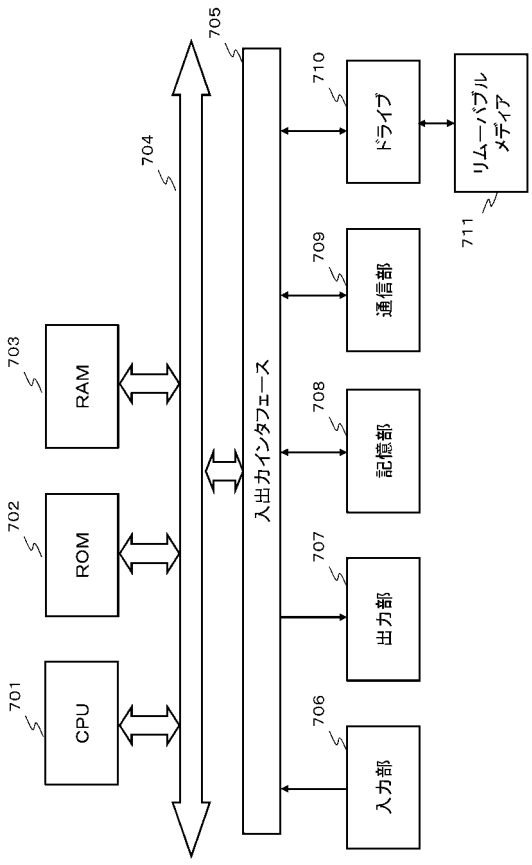

【図１０】



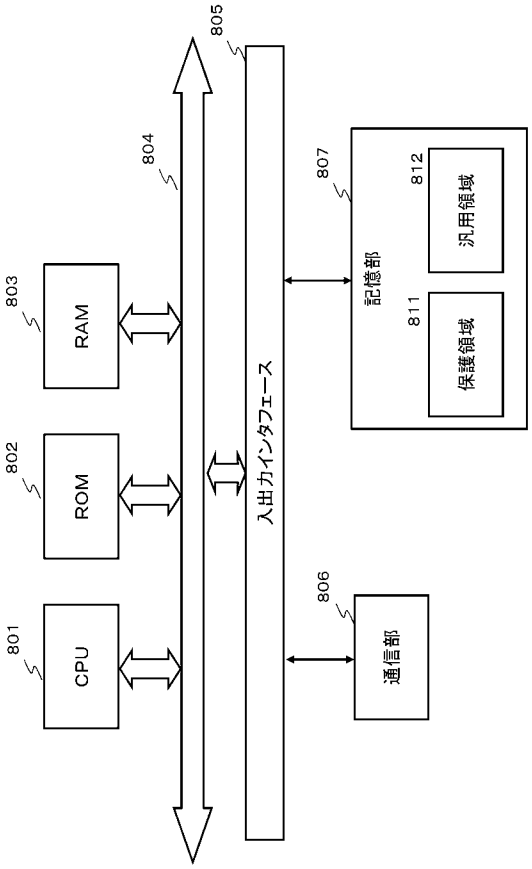

【図１１】



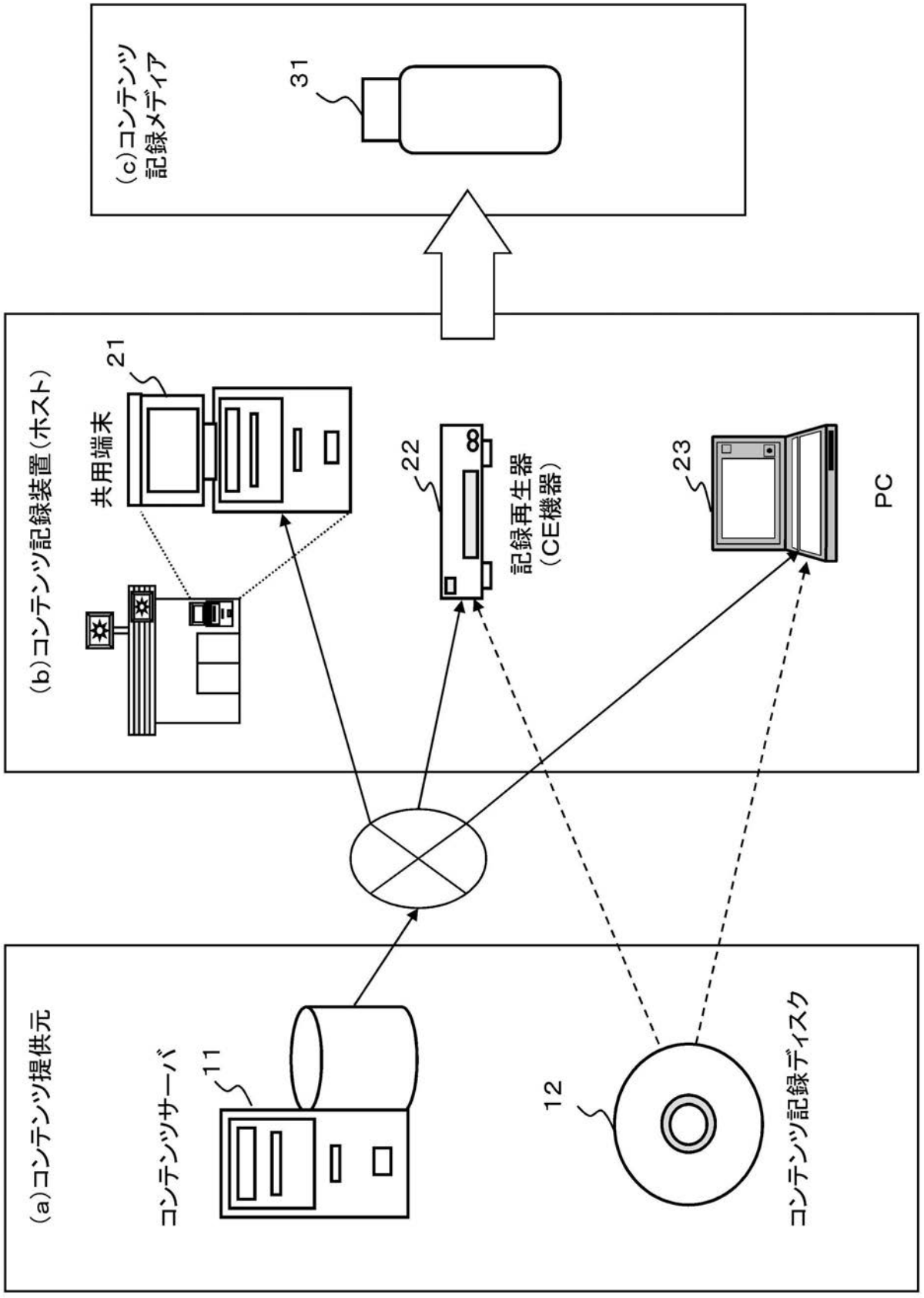

【図１２】



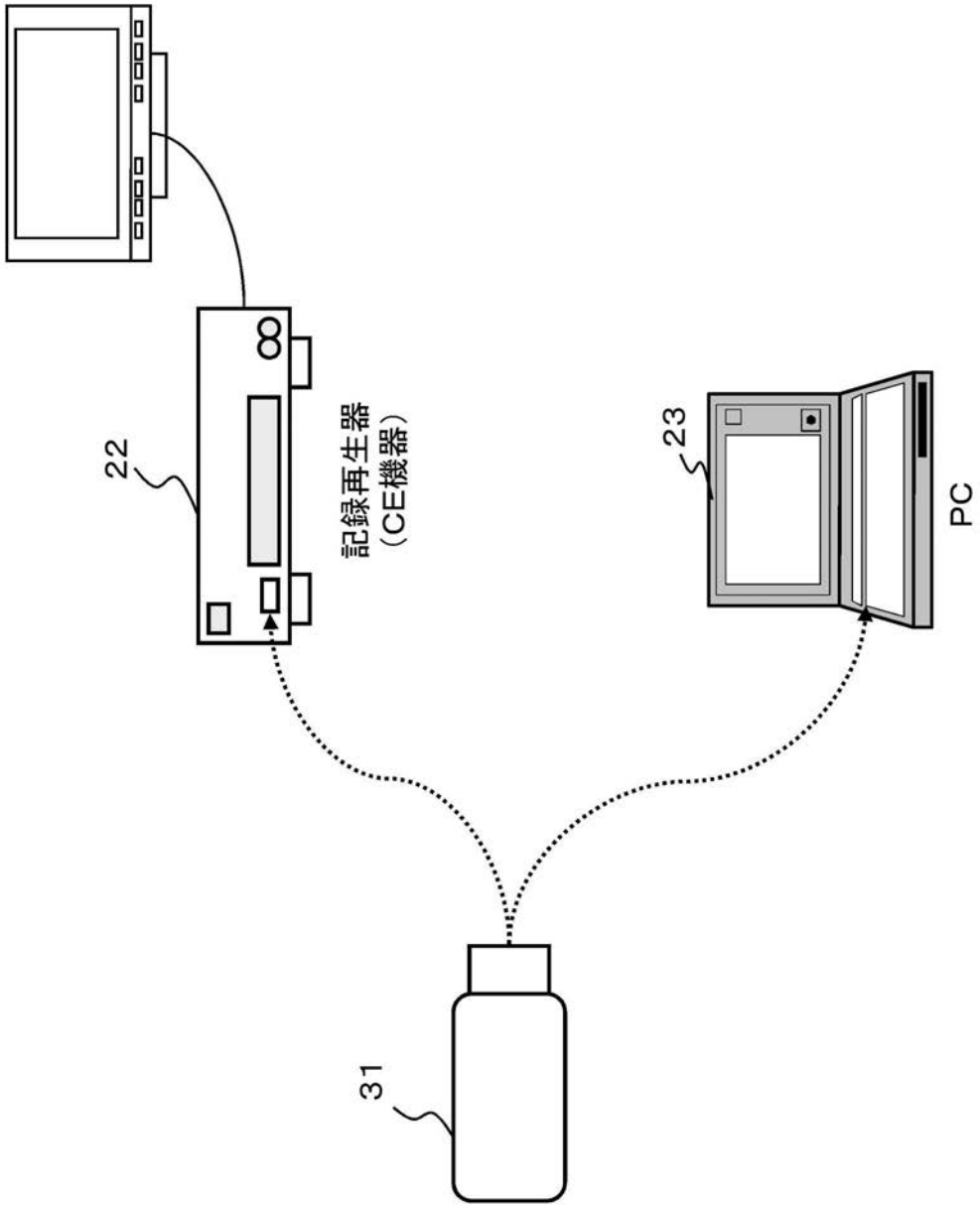
【図１３】


801
CPU
802
ROM
803
RAM
804
805
入出力インタフェース
806
通信部
807
記憶部
811
保護領域
812
汎用領域

【図１】


(a)コンテンツ提供元
コンテンツサーバ
11
12
コンテンツ記録ディスク
(b)コンテンツ記録装置(ホスト)
共用端末
21
22
記録再生器
(CE機器)
23
PC
(c)コンテンツ
記録メディア
31

【図２】



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　小林　義行
東京都港区港南１丁目７番１号　ソニー株式会社内

Ｆターム(参考) 5C164 PA23 PA24 PA27 SB25S SC02P TB23P UA12P YA09
5J104 AA12 AA16 EA04 EA15 EA16 EA17 JA03 JA21 NA02 NA12
NA27 NA37 PA14