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

特許第5678804号
(P5678804)

(45)発行日　平成27年3月4日(2015.3.4)　(24)登録日　平成27年1月16日(2015.1.16)

(51)Int.Cl.		F I		
G06F 21/10	(2013.01)	G06F	21/10	
H04N 5/93	(2006.01)	H04N	5/93	Z
H04N 5/91	(2006.01)	H04N	5/91	P
H04N 5/92	(2006.01)	H04N	5/92	H
G11B 20/10	(2006.01)	G11B	20/10	H

請求項の数 16　(全 40 頁)　最終頁に続く

(21)出願番号　特願2011-118575 (P2011-118575)
(22)出願日　平成23年5月27日 (2011.5.27)
(65)公開番号　特開2012-247961 (P2012-247961A)
(43)公開日　平成24年12月13日 (2012.12.13)
審査請求日　平成26年4月3日 (2014.4.3)

(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】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】
利用管理対象となるコンテンツを出力するコンテンツ出力装置と、
前記コンテンツを前記コンテンツ出力装置から入力して格納するメディアと、
前記メディアを装着して前記コンテンツの再生を行う再生装置と、
コンテンツの前記メディアに対する記録処理の管理を実行する管理サーバを有するコンテンツ利用システムであり、
前記コンテンツ出力装置は、
暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵を前記メディアに出力し、
前記管理サーバは、
前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を生成して前記メディアに送信し、
前記メディアは、
前記暗号化コンテンツと、前記暗号鍵と、前記メディアＩＤ検証値を記憶部に格納し、
前記再生装置は、
前記メディアを装着し、前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行するコンテンツ利用システム。

【請求項２】
前記メディアは、
メディアの記憶部に対するアクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域を有し、
前記コンテンツ出力装置の証明書検証に基づいてアクセス許容判定のなされた保護領域に前記暗号鍵を格納し、
前記再生装置による前記暗号鍵の読み取り要求に応じて、前記再生装置の証明書検証に基づいてアクセス許容判定のなされた保護領域に記録された前記暗号鍵を前記再生装置に出力する請求項１に記載のコンテンツ利用システム。
【請求項３】
前記暗号化コンテンツは、タイトルキーで暗号化された暗号化コンテンツであり、
前記暗号鍵は、前記タイトルキーの暗号化および復号処理に適用されるドメインキーまたはドメインキーの変換キーであり、
前記コンテンツ出力装置は、
前記暗号化コンテンツと、
前記ドメインキーで暗号化された暗号化タイトルキーを前記メディアに出力する請求項１に記載のコンテンツ利用システム。
【請求項４】
前記ドメインキーは、
コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供する暗号鍵である請求項３に記載のコンテンツ利用システム。
【請求項５】
前記コンテンツ出力装置は、
前記ドメインキーを保持するコンテンツ利用を許容されたドメイン機器であり、
前記再生装置は、
前記ドメインキーを保持しない非ドメイン機器である請求項４に記載のコンテンツ利用システム。
【請求項６】
データ処理部と記憶部を有し、
前記記憶部は、
アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分され、
前記汎用領域に暗号化コンテンツと、自装置の識別子であるメディアＩＤに基づいて生成されたメディアＩＤ検証値を格納し、
前記保護領域に、前記暗号化コンテンツの利用処理に適用する暗号鍵を格納し、
前記データ処理部は、
前記暗号化コンテンツの利用予定の再生装置から提供される証明書を検証して、前記保護領域に対するアクセス権の確認に応じて前記再生装置による前記暗号鍵の読み取りを許容し、
前記再生装置に対してメディアＩＤを出力し、再生装置におけるメディアＩＤに基づく算出検証値と前記汎用領域に格納されたメディアＩＤ検証値の照合処理に基づくコンテツ再生可否判定を実行させることを可能とした情報処理装置。
【請求項７】
前記データ処理部は、
前記汎用領域に対する暗号化コンテンツの記録処理に際して、
前記メディアＩＤを管理サーバに送信し、管理サーバの生成したメディアＩＤ検証値を受信して前記汎用領域に格納する請求項６に記載の情報処理装置。
【請求項８】

前記データ処理部は、
コンテンツ出力装置から提供される暗号化コンテンツと、前記暗号化コンテンツの暗号化キーであるタイトルキーを暗号化した暗号化タイトルキーを前記汎用領域に格納し、
前記暗号化タイトルキーの暗号鍵であり、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供するドメインキーを前記保護領域に格納する請求項６に記載の情報処理装置。
【請求項９】
記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行するデータ処理部を有し、
前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、
前記データ処理部は、
前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化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】
前記メディアは、
メディアの記憶部に対するアクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域を有し、
前記データ処理部は、
前記メディアに対して、再生装置の証明書であり、前記保護領域に対するアクセス許容情報の記録された証明書の提供処理を行う請求項９に記載の情報処理装置。
【請求項１１】
前記暗号化コンテンツは、タイトルキーで暗号化された暗号化コンテンツであり、
前記暗号鍵は、前記タイトルキーの暗号化および復号処理に適用されるドメインキーまたはドメインキーの変換キーである請求項９に記載の情報処理装置。
【請求項１２】
前記ドメインキーは、
コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供する暗号鍵である請求項１１に記載の情報処理装置。
【請求項１３】
暗号化コンテンツと、該暗号化コンテンツの利用処理に適用する暗号鍵を格納した記憶部と、データ処理部を有し、
前記データ処理部は、
コンテンツ出力対象となるメモリカードに対して、前記暗号化コンテンツと前記暗号鍵を出力して記録させる構成であり、
前記メモリカードは、
アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分された記憶部を有し、
前記データ処理部は、
自装置の証明書を前記メモリカードに提示し、前記メモリカードによる証明書検証に基づいてアクセスの許容された保護領域に前記暗号鍵の書き込みを行う情報処理装置。
【請求項１４】
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、
アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容され

る保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分され、
前記汎用領域に暗号化コンテンツと、自装置の識別子であるメディアＩＤに基づいて生成されたメディアＩＤ検証値を格納し、
前記保護領域に、前記暗号化コンテンツの利用処理に適用する暗号鍵を格納し、
前記データ処理部は、
前記暗号化コンテンツの利用予定の再生装置から提供される証明書を検証して、前記保護領域に対するアクセス権の確認に応じて前記再生装置による前記暗号鍵の読み取りを許容し、
前記再生装置に対してメディアＩＤを出力し、再生装置におけるメディアＩＤに基づく算出検証値と前記汎用領域に格納されたメディアＩＤ検証値の照合処理に基づくコンテツ再生可否判定を実行させることを可能とした情報処理方法。
【請求項１５】
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、記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行するデータ処理ステップを実行し、
前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、
前記データ処理ステップは、
前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行するステップである情報処理方法。
【請求項１６】
情報処理装置において実行する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、記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行させるデータ処理ステップを実行し、
前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、
前記データ処理ステップにおいて、
前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化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。特に例えばハードディスク等の第１メディアに記録したコンテンツを例えばメモリカード等の第２メディアに記録して利用する構成におけるコンテンツの不正利用を防止した情報処理装置、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－ｒａｙ 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メ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規定がないという問題がある。

【００１０】
例えばコンテンツ提供サーバからダウンロードしたコンテンツや、放送コンテンツなどは、ユーザ装置としてのＰＣやＢＤレコーダなどのハードディスクに記録される場合が多い。しかし、このようなコンテンツを携帯機器において利用しようとする場合、このハードディスクの記録コンテンツを例えばフラッシュメモリやＵＳＢハードディスクなどの小型のメディアであるメモリカード等に移す処理が必要となる。
このようなコンテンツ出力処理は、一般的にエクスポート（ｅｘｐｏｒｔ）と呼ばれる。
【００１１】
例えばハードディスクに一旦記録したダウンロードコンテンツやストリーミングコンテンツは、他の記録メディアに対してコピー（ｂｉｔ－ｆｏｒ－ｂｉｔ　ｃｏｐｙ）を行えば無制限にコピーが作成できてしまう。
このような無制限のコピーを許容してしまうと、コンテンツの著作権保護の観点から好ましくない。
【００１２】
このような無秩序なコピーを制限するための構成について、すでにいくつか提案され、利用されている。
例えば外部から入力するデジタルデータをハードディスク等に記録した場合、その記録コンテンツの再生を、例えばデータ記録処理を実行した１つの機器（デバイス）など特定の機器にのみ許容する構成がある。この構成は、コンテンツ利用を１つの機器（デバイス）に結びつける構成であり、いわゆるデバイスバインド（ｄｅｖｉｃｅ－ｂｉｎｄ）と呼ばれる。
しかし、このような制限は、バックアップコピーが作成できないなど、ユーザの利便性を欠くものであるとも言える。
【００１３】
なお、コンテンツの転送制御構成として従来から提案または利用されている構成として例えば、以下のものがある。
ＤＶＤ等の記録メディアに関する著作権保護技術を規定したＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ）において規定されているＳＤカード対応の規格であるＣＰＲＭ／ＳＤ－Ｃａｒｄには、特定のＩＤを持つメディア上でのみコンテンツ再生を許容しないコンテンツ利用制御構成を規定している。
【００１４】
また、ホームネットワークにおけるコンテンツの利用構成について規定しているＤＬＮＡ（Ｄｉｇｉｔａｌ　Ｌｉｖｉｎｇ　Ｎｅｔｗｏｒｋ　Ａｌｌｉａｎｃｅ）では、セキュア通信路を利用し外部漏えいを防止してネットワーク接続機器間でコンテンツをストリーミング配信する構成について規定している。
この構成では、例えば１階のレコーダに記録したコンテンツを２階のＰＣにストリーミング配信するといった処理が可能となる。
【００１５】
また、ＢＤ（ブルーレイディスク）の規格においては、「オンラインでメディアとコンテンツを紐付けるデータ（電子署名、など）を記録することで、コンテンツをＢＤに記録する処理を許容し、署名検証等の検証処理をコンテンツ利用の条件とすることでコンテンツの不正利用を排除する」仕様について規定している。これは、例えばプリペアイビデオ（Ｐｒｅｐａｒｅｄ　Ｖｉｄｅｏ）として規格化されている。
【００１６】
このように、特定のコンテンツ利用構成に限定した範囲において、様々な規格や仕様が策定されているにすぎない。しかし、上記の様々な規格化されたコンテンツの利用構成以外の設定でコンテンツ利用を行う場合には、上記の各規格の適用外となり、必ずしも十分な著作権保護が行われないという問題がある。
【先行技術文献】

【特許文献】
【００１７】
【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】
【００１８】
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、利用制御が必要となるコンテンツをメディア間で移動させて利用する構成において、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】
【００１９】
本発明の第１の側面は、
利用管理対象となるコンテンツを出力するコンテンツ出力装置と、
前記コンテンツを前記コンテンツ出力装置から入力して格納するメディアと、
前記メディアを装着して前記コンテンツの再生を行う再生装置と、
コンテンツの前記メディアに対する記録処理の管理を実行する管理サーバを有するコンテンツ利用システムであり、
前記コンテンツ出力装置は、
暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵を前記メディアに出力し、
前記管理サーバは、
前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を生成して前記メディアに送信し、
前記メディアは、
前記暗号化コンテンツと、前記暗号鍵と、前記メディアＩＤ検証値を記憶部に格納し、
前記再生装置は、
前記メディアを装着し、前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行するコンテンツ利用システムにある。
【００２０】
さらに、本開示のコンテンツ利用システムの一実施態様において、前記メディアは、メディアの記憶部に対するアクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域を有し、前記コンテンツ出力装置の証明書検証に基づいてアクセス許容判定のなされた保護領域に前記暗号鍵を格納し、前記再生装置による前記暗号鍵読み取り要求に応じて、前記再生装置の証明書検証に基づいてアクセス許容判定のなされた保護領域に記録された前記暗号鍵を前記再生装置に出力する。
【００２１】
さらに、本開示のコンテンツ利用システムの一実施態様において、前記暗号化コンテンツは、タイトルキーで暗号化された暗号化コンテンツであり、前記暗号鍵は、前記タイトルキーの暗号化および復号処理に適用されるドメインキーまたはドメインキーの変換キーであり、前記コンテンツ出力装置は、前記暗号化コンテンツと、前記ドメインキーで暗号化された暗号化タイトルキーを前記メディアに出力する。
【００２２】
さらに、本開示のコンテンツ利用システムの一実施態様において、前記ドメインキーは、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供する暗号鍵である。
【００２３】

さらに、本開示のコンテンツ利用システムの一実施態様において、前記コンテンツ出力装置は、前記ドメインキーを保持するたコンテンツ利用を許容されたドメイン機器であり、前記再生装置は、前記ドメインキーを保持しない非ドメイン機器である。

【００２４】

さらに、本開示の第２の側面は、

データ処理部と記憶部を有し、

前記記憶部は、

アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分され、

前記汎用領域に暗号化コンテンツと、自装置の識別子であるメディアＩＤに基づいて生成されたメディアＩＤ検証値を格納し、

前記保護領域に、前記暗号化コンテンツの利用処理に適用する暗号鍵を格納し、

前記データ処理部は、

前記暗号化コンテンツの利用予定の再生装置から提供される証明書を検証して、前記保護領域に対するアクセス権の確認に応じて前記再生装置による前記暗号鍵の読み取りを許容し、

前記再生装置に対してメディアＩＤを出力し、再生装置におけるメディアＩＤに基づく算出検証値と前記汎用領域に格納されたメディアＩＤ検証値の照合処理に基づくコンテツ再生可否判定を実行させることを可能とした情報処理装置にある。

【００２５】

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、前記汎用領域に対する暗号化コンテンツの記録処理に際して、前記メディアＩＤを管理サーバに送信し、管理サーバの生成したメディアＩＤ検証値を受信して前記汎用領域に格納する。

【００２６】

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、コンテンツ出力装置から提供される暗号化コンテンツと、前記暗号化コンテンツの暗号化キーであるタイトルキーを暗号化した暗号化タイトルキーを前記汎用領域に格納し、前記暗号化タイトルキーの暗号鍵であり、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供するドメインキーを前記保護領域に格納する。

【００２７】

さらに、本開示の第３の側面は、

記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行するデータ処理部を有し、

前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、

前記データ処理部は、

前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行する情報処理装置にある。

【００２８】

さらに、本開示の情報処理装置の一実施態様において、前記メディアは、メディアの記憶部に対するアクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域を有し、前記データ処理部は、前記メディアに対して、再生装置の証明書であり、前記保護領域に対するアクセス許容情報の記録された証明書の提供処理を行う。

【００２９】

さらに、本開示の情報処理装置の一実施態様において、前記暗号化コンテンツは、タイ

トルキーで暗号化された暗号化コンテンツであり、前記暗号鍵は、前記タイトルキーの暗号化および復号処理に適用されるドメインキーまたはドメインキーの変換キーである。

【００３０】

さらに、本開示の情報処理装置の一実施態様において、前記ドメインキーは、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供する暗号鍵である。

【００３１】

さらに、本開示の第４の側面は、

暗号化コンテンツと、該暗号化コンテンツの利用処理に適用する暗号鍵を格納した記憶部と、データ処理部を有し、

前記データ処理部は、

コンテンツ出力対象となるメディアに対して、前記暗号化コンテンツと前記暗号鍵を出力して記録させる構成であり、

前記メディアは、

アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分された記憶部を有し、

前記データ処理部は、

自装置の証明書を前記メモリカードに提示し、メモリカードによる証明書検証に基づいてアクセスの許容された保護領域に前記暗号鍵の書き込みを行う情報処理装置にある。

【００３２】

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、

アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分され、

前記汎用領域に暗号化コンテンツと、自装置の識別子であるメディアＩＤに基づいて生成されたメディアＩＤ検証値を格納し、

前記保護領域に、前記暗号化コンテンツの利用処理に適用する暗号鍵を格納し、

前記データ処理部は、

前記暗号化コンテンツの利用予定の再生装置から提供される証明書を検証して、前記保護領域に対するアクセス権の確認に応じて前記再生装置による前記暗号鍵の読み取りを許容し、

前記再生装置に対してメディアＩＤを出力し、再生装置におけるメディアＩＤに基づく算出検証値と前記汎用領域に格納されたメディアＩＤ検証値の照合処理に基づくコンテツ再生可否判定を実行させることを可能とした情報処理方法にある。

【００３３】

さらに、本開示の第６の側面は、

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、記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行するデータ処理ステップを実行し、

前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、

前記データ処理ステップは、

前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行するステップである情報処理方法にある。

【００３４】

さらに、本開示の第７の側面は、
情報処理装置において実行する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、記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行させるデータ処理ステップを実行し、
前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、
前記データ処理ステップにおいて、
前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行させるプログラムにある。

【００３５】
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。

【００３６】
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】

【００３７】
本開示の一実施例の構成によれば、コンテンツの利用制御の下でメディアに対するコンテンツ出力とメディア格納コンテンツの利用を行う構成が実現される。
具体的には、コンテンツ出力装置が、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵を前記メディアに出力し、管理サーバが、メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を生成してメディアに送信する。メディアは、暗号化コンテンツと、暗号鍵と、メディアＩＤ検証値を記憶部に格納する。再生装置は、メディアを装着し、メディアから取得したメディアＩＤに基づいて検証値を算出し、メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、暗号鍵を適用したデータ処理によってメディアに格納された暗号化コンテンツの再生処理を実行する。
この処理によりメディアバインド型のコンテンツ利用制御が実現される。

【図面の簡単な説明】

【００３８】
【図１】コンテンツ利用制御規格であるマーリンに従ったコンテンツ利用処理の概要について説明する図である。
【図２】コンテンツ利用制御規格であるマーリンに従ったコンテンツ利用処理の概要について説明する図である。
【図３】コンテンツ利用制御規格であるマーリンに従ったコンテンツ利用処理の問題点について説明する図である。
【図４】本開示の構成において想定されるコンテンツ利用構成例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について説明する図である。
【図６】ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）について説明する図である。
【図７】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８】メモリカードの格納データの例について説明する図である。
【図９】コンテンツ提供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１０】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】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１３】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１４】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】
【００３９】
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．デバイスバインド型のコンテンツ利用制御構成の概要
２．コンテンツ提供処理および利用処理の概要について
３．メモリカードの構成例について
４．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
５．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
６．メモリカードに対する記録データの構成例について
７．デバイスからメモリカードに対するコンテンツ記録シーケンスについて
８．メモリカード格納コンテンツの再生シーケンスについて
９．各装置のハードウェア構成例について
１０．本開示の構成のまとめ
【００４０】
［１．デバイスバインド型のコンテンツ利用制御構成の概要］
本開示の構成についての説明の前に、デバイスバインド型のコンテンツ利用制御構成の概要について説明する。
図１は、デバイスバインド型のコンテンツ利用制御構成の一例であるマーリンＤＲＭ（Ｍａｒｌｉｎ　Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）に従ったドメイン単位のコンテンツ利用制御構成について説明する図である。
マーリンはソニー（株）他のメーカーが規定したデジタルコンテンツの利用制御を実現する仕様である。
【００４１】
マーリンでは、例えばあるユーザの利用している複数の再生機器の集合をドメインとして規定する。ドメイン機器には例えばユーザの利用するＰＣ２１、再生機器２２、テレビ２３等、様々なユーザ機器が含まれる。これらのドメイン機器２１～２３は管理サーバ１１に機器ＩＤ等の登録情報を提供し、管理サーバ１１にドメイン機器として登録される。管理サーバ１１は登録されたドメイン機器２１～２３に暗号鍵であるドメインキーを提供する。各ドメイン機器２１～２３は管理サーバ１１から提供されたドメインキーを記憶部に格納する。
【００４２】
図２にドメイン機器２１～２３の格納データ例を示す。
ドメイン機器には、記憶部４０に、例えば映画や音楽等の再生対象とするコンテンツの暗号化データである暗号化コンテンツ４１と、暗号化コンテンツの暗号化、復号処理に適用するコンテンツキーを暗号化した暗号化コンテンツキー４２、さらに、コンテンツの利用条件、例えばコンテンツの利用が許可されていることを証明する情報や、コンテンツの

コピー可否情報、出力可否情報などを記録したライセンス情報４３が記録される。これらは、例えばコンテンツ提供サーバなどから提供される。

【００４３】

さらに、外部からのアクセスを困難化したセキュア記憶部５０に、前述したドメインキー５１が格納される。

ドメインキー５１は、暗号化コンテンツキー４２の暗号化および復号処理に適用される鍵である。

ドメイン機器２１～２３において、コンテンツ再生を行う場合、以下の処理が実行される。

（１）ドメインキー５１を用いて暗号化コンテンツキー４２の復号を実行してコンテンツキーを取得、

（２）取得したコンテンツキーを利用して暗号化コンテンツ４１を復号してコンテンツを取得、

（３）取得したコンテンツをライセンス情報４３に認められた範囲で再生、利用。

このようなシーケンスに従って、ドメイン機器でのコンテンツ利用が可能となる。

【００４４】

このようにコンテンツはドメイン機器として登録された特定の機器（デバイス）でのみ利用が可能となる。すなわちマーリンＤＲＭでは、デバイスバインド型のコンテンツ利用制御を実現している。

【００４５】

しかしながら、このようなデバイスバインド型のコンテンツ利用制御構成では、ドメイン機器として登録された機器以外では、コンテンツが全く利用できなくなるという問題が発生する。

昨今、大容量の小型メモリ例えばフラッシュメモリや小型ハードディスク等を備えたメモリカードの利用が盛んとなっている。

例えば図３に示すように、このようなメモリカード７０にコンテンツをドメイン機器１２１～１２３から移動またはコピーして、メモリカード７０をドメイン機器以外の小型デバイス８０に装着して利用したいといった場合、上記のデバイスバインド型のコンテンツ利用制御構成では対応できない。すなわちコンテンツの利用ができないという問題がある。

【００４６】

小型デバイス８０においてコンテンツ利用を可能とするためには、ユーザは、所定の手続きを実行して、小型デバイス８０をドメイン機器として管理サーバ１１に登録し、管理サーバ１１から新たに追加のドメインキーを入手して小型デバイス８０に格納することが必要となる。

このように、デバイスバインド型のコンテンツ利用制御構成では、新たな再生機器でコンテンツを利用するためには、新たな再生機器を管理サーバに登録して、その新たな再生機器にドメインキーを新たに格納するという処理が必要となってしまう。

【００４７】

以下では、このような新たな機器登録処理を必要とすることなく、メモリカード等にコンテンツを移動またはコピーし、メモリカードを装着した機器においてコンテンツを利用可能とし、かつ不正なコンテンツ利用を防止する構成について説明する。

【００４８】

［２．コンテンツ提供処理および利用処理の概要について］

まず、図４以下を参照して、コンテンツの提供処理および利用処理の概要について説明する。

図４には、ユーザ機器としてのコンテンツ再生装置であり、前述した管理サーバへの登録がなされたドメイン機器であるＰＣ１２１、再生機器１２２、テレビ１２３を示している。

これらのドメイン機器は、管理サーバ１０１にコンテンツ利用機器として登録された機

器であり、先に図２を参照して説明したようにドメインキーを保持している。
【００４９】
これらのドメイン機器１２１～１２３の機器情報を管理情報として保持し、これらの機器に対してドメインキーを提供するのが管理サーバ１０１である。
また、ドメイン機器１２１～１２３に対して暗号化コンテンツを提供するのがコンテンツ提供サーバ１０２ａ，１０２ｂである。
【００５０】
ユーザ機器には、管理サーバ１０１に登録されたドメイン機器１２１～１２３以外に再生装置１３１がある。この再生装置１３１はドメイン機器として登録されていない機器（非ドメイン機器）である。
【００５１】
ユーザは、ドメイン機器１２１～１２３のいずれかに例えばフラッシュメモリや小型ハードディスクの記憶部を持つメモリカード２００を装着して、暗号化コンテンツおよびコンテンツ再生に必要となる各種情報をドメイン機器からメモリカードに移動またはコピーする。
このメモリカード２００を非ドメイン機器である再生装置１３１に装着して、再生装置１３１においてコンテンツ再生等、コンテンツの利用を行う。
このようなコンテンツ利用をコンテンツの漏えいや不正利用を防止した構成として実現する。
【００５２】
［３．メモリカードの構成例について］
次に、図４に示すメモリカード２００の具体的構成例と利用例について説明する。
図５は、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具体的構成例を示す図である。
メモリカード２００の記憶領域は、図５に示すように、
（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０、
（ｂ）汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２２０、
これら２つの領域によって構成される。
【００５３】
（ｂ）汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２２０はユーザの利用する記録装置や再生装置等によって、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。
【００５４】
一方、（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０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２００のデータ処理部は、メモリカード２００に予め格納されたプログラムに従ってアクセス許容判定処理を実行する。この判定処理によって、アクセスを要求する各装置に応じて読み取り（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）の可否が決定される。
【００５５】
メモリカード２００は、予め格納されたプログラムの実行や認証処理を行うデータ処理部を備えており、メモリカード２００は、メモリカード２００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。
【００５６】
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　Ｃｅｒｔｉｆｉｃａｔｅ））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）２１０の各区分領域に対するアクセス許容判定を行う。この判定処理は、図５に示す保護領

域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０内の区分領域（図に示す領域＃０，＃１，＃２・・・）単位で行われ、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、アクセス要求装置に対する許容処理として設定される。

【００５７】

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、例えばサーバや、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　Ｃｅｒｔｉｆｉｃａｔｅ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）に記録される。

【００５８】

メモリカード２００は、メモリカード２００に予め格納された既定のプログラムに従って、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）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。

【００５９】

［４．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２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０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６を参照して説明する。

【００６０】

上述したように、メモリカード２００は、メモリカード２００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　Ｃｅｒｔｉｆｉｃａｔｅ）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）２１０の各区分領域のアクセスを許容するか否かを判定する。

【００６１】

この認証処理に利用される装置証明書の一例として、図４に示すドメイン機器１２１～１２３や、再生装置１３１等のユーザ機器（ホスト機器）に提供され、これらの機器に格納されるホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）の構成例について図６を参照して説明する。

【００６２】

ホスト証明書（Ｈｏｓｔ　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各ユーザ機器（ホスト機器）に提供される。例えば、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、認証局がコンテンツ利用処理を認めたユーザ機器（ホスト機器）に対して発行するユーザ機器の証明書であり、公開鍵等を格納した証明書である。ホスト証明書（Ｈｏｓｔ　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。

【００６３】

なお、メモリカード２００の保護領域に対するアクセスを行うサーバに対しても、ホスト証明書と同様の構成を持つサーバ公開鍵とメモリカードのアクセス許容情報が記録されたサーバ証明書（Ｓｅｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）が提供される。

【００６４】

図６に認証局が各ホスト機器（ユーザ機器）に提供するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）の具体例を示す。

ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、図６に示すように、以下のデータが含まれる。

（１）タイプ情報

（２）ホストＩＤ（ユーザ機器ＩＤ）

（３）ホスト公開鍵（Ｈｏｓｔ　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）
【００６５】
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、証明書のタイプやユーザ機器のタイプを示す情報であり、例えば本証明書がホスト証明書であることを示すデータや、機器の種類、例えばＰＣであるとか、音楽再生プレーヤであるといった機器の種類などを示す情報が記録される。
【００６６】
（２）ホストＩＤ
ホストＩＤは機器識別情報としての機器ＩＤを記録する領域である。
（３）ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）
ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）はホスト機器の公開鍵である。ホスト機器（ユーザ機器）に提供される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。
【００６７】
（４）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）
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４、図５に示すメモリカード２００の記憶領域中に設定される保護領域（ＰＤＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０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。
【００６８】
（５）その他の情報、（６）署名（Ｓｉｇｎａｔｕｒｅ）
ホスト証明書には、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。ホスト証明書に記録された情報、例えばホスト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、ホスト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、ホスト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。
【００６９】
なお、図６は、メモリカードの保護領域に対するユーザ機器（ホスト機器）のアクセス許容情報を記録したホスト証明書であるが、例えばメモリカードにコンテンツを提供するコンテンツ提供サーバなど、保護領域に対するアクセスが必要となるサーバに対しては、図６に示すホスト証明書と同様、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証明書（サーバ証明書（サーバ公開鍵証明書））が提供される。
【００７０】
［５．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６を参照して説明したように、メモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０に対してアクセスを行う場合には、図５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６に示す証明書を確認して、図５に示すメモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０に対するアクセス可否を判定する。
【００７１】
ホスト機器は、例えば図６を参照して説明したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）を保持し、コンテンツの提供等を行うサーバは、サーバに対応する証明書（サーバ証明書：Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）を保持している。

【００７２】
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、各装置が保有している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。
【００７３】
図７を参照して、メモリカードに対するアクセス要求装置が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。
【００７４】
図７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ホスト機器２２２と、メモリカード２００を示している。
ホスト機器２２２は、例えば、図４に示すドメイン機器１２１～１２３や再生装置１３１等のユーザ機器であり、メモリカード２００に対するコンテンツの出力処理や、メモリカード２００に記録されたコンテンツ再生を実行する装置である。
【００７５】
例えばドメイン機器１２１～１２３は、自装置の記憶部に格納された暗号化コンテンツをメモリカード２００に出力する際に、自装置に格納されたドメインキーをメモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０に書き込む処理を実行する。
また、再生装置１３１はメモリカード２１０に記録された暗号化コンテンツを利用して再生する場合に、メモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０に書き込まれたドメインキーを取得する処理を実行する。
ドメイン機器１２１～１２３や非ドメイン機器である再生装置１３１は、これらの処理においてメモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０に対するアクセスが必要となる。
【００７６】
メモリカード２００は、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０と、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２２０を有し、暗号化コンテンツ等は汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２２０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ドメインキーは保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０に記録される。
【００７７】
先に図５を参照して説明したように、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０は、複数の領域に区分されている。
図７に示す例では、
区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）２１１、
区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）２１２、
これらの２つの区分領域を持つ例を示している。
【００７８】
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７に示す例では、ホスト機器２２２の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、
区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）に対しては、データの記録（Ｗｒｉｔｅ）と読み取り（Ｒｅａｄ）の双方の処理が許可、
区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に対しては、読み取り（Ｒｅａｄ）処理のみが許可、
これらの設定がなされた証明書である。
【００７９】
図７に示すホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に対する書き込み（Ｗｒｉｔｅ）許可が設定されていない。
例えば、このようなアクセス許容情報が記録された証明書がユーザ機器に提供されるこ

とになる。
【００８０】
メモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０をアクセスしようとする装置は、このアクセス許容情報が記録された証明書をメモリカードに出力して、メモリカード内のデータ処理部における証明書検証処理に基づいて、アクセス可否が決定され、決定情報に従ってメモリカード２００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０をアクセスすることになる。
【００８１】
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。
【００８２】
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。
【００８３】
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６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。
【００８４】
［６．メモリカードに対する記録データの構成例について］
次に、例えば図４に示すドメイン機器１２１～１２３のいずれかに記録されたコンテンツをメモリカード２００に移動またはコピーし、メモリカード２００に格納されたコンテンツを非ドメイン機器としての再生装置１３１において利用する場合、ドメイン機器１２１～１２３がメモリカード２００に記録するデータの一例について図８を参照して説明する。
【００８５】
図８には、メモリカード２００に記録されたデータ例を示している。
メモリカード２００は、各アクセス機器の保有する証明書（図６参照）に記録されたアクセス許容情報に応じてアクセスの許容される保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０と、証明書のアクセス許容情報に基づくことなくアクセスの許容される汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２２０を有する。
【００８６】
図８に示すように、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１０には、ドメインキー３８１が記録される。
このドメインキー３８１は、図４に示すドメイン機器１２１～１２３が管理サーバ１０

１に対するドメイン機器の登録を条件として管理サーバ１０１から受領した鍵である。このドメインキー３８１は、暗号化コンテンツの暗号化／復号鍵として利用されるタイトルキーの暗号化／復号処理に適用される鍵である。

【００８７】

このドメインキー３８１以外のデータ、すなわち暗号化コンテンツ他のデータは、汎用領域２２０に記録される。

図８には、例えば映画や音楽データ等、再生対象となるコンテンツの暗号化データであり、圧縮フォーマットとしてＭＰＥＧ４（ＭＰ４）形式を持つデータファイルである暗号化コンテンツファイル＃１，３１０，暗号化コンテンツファイル＃２，３２０の２つの暗号化コンテンツファイルを記録した例を示している。

【００８８】

これらの暗号化コンテンツファイルにはコンテンツ識別子としてのＩＤ情報が設定され、各コンテンツファイル内に設定されるセキュリティボックス内にＩＤ情報が記録される。このＩＤ情報は、各コンテンツファイルに対応する鍵情報などの格納領域に設定されたインデックスとしてのＩＤ情報に対応している。

例えばこのメモリカード２００を装着してメモリカード２００に格納されたコンテンツを再生する再生装置は、再生対象コンテンツを選択すると、その選択したコンテンツファイル内のセキュリティボックスからＩＤ情報を取得して取得したＩＤに従って、選択コンテンツに対応する管理情報を取得することができる。

【００８９】

なお、これらのＩＤ情報は、例えば図４に示すドメイン機器１２１～１２３からのコンテンツの移動またはコピー処理に際してメモリカード２００内のデータ処理部が管理情報記録領域のインデックスとして設定する。

【００９０】

図８に示す例では、暗号化コンテンツファイル３１０のセキュリティボックス３１１にコンテンツ識別子（ＩＤ１）が記録されており、このコンテンツ識別子（ＩＤ１）に対応する管理情報３３０が、インデックス（ＩＤ１）によって識別可能な記録領域に記録される。

また、暗号化コンテンツファイル３２０のセキュリティボックス３２１にコンテンツ識別子（ＩＤ２）が記録されており、このコンテンツ識別子（ＩＤ２）に対応する管理情報３４０が、インデックス（ＩＤ２）の記録領域に記録されている。

【００９１】

管理情報３３０は、暗号化コンテンツファイル＃１，３１０対応のインデックス（ＩＤ１）によって特定可能な記録領域に記録され、ここには、暗号化コンテンツファイル＃１，３１０の再生処理に利用する情報が記録される。具体的には、図８に示すように、

（ａ）トークン（Ｔｏｋｅｎ）３３１、
（ｂ）利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）３３２、
（ｃ）メディアＩＤ検証値（ＭＡＣ　ｏｆ　Ｍｅｄｉａ　ＩＤ）３３３、
（ｄ）暗号化タイトルキー（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）３３４、

これらの情報が暗号化コンテンツファイル３１０に対応する管理情報３３０として記録される。

【００９２】

同様に、インデックス（ＩＤ２）の記録領域には、暗号化コンテンツファイル＃２，３２０の再生処理に利用する管理情報３４０が記録される。具体的には、図８に示すように、

（ａ）トークン（Ｔｏｋｅｎ）３４１、
（ｂ）利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）３４２、
（ｃ）メディアＩＤ検証値（ＭＡＣ　ｏｆ　Ｍｅｄｉａ　ＩＤ）３４３、
（ｄ）暗号化タイトルキー（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）３４４、

これらの情報が暗号化コンテンツファイル３１０に対応する管理情報３４０として記録

される。
【００９３】
これらのデータ（ａ）～（ｄ）中、
（ａ）トークン（Ｔｏｋｅｎ）３３１，３４１と、
（ｂ）利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）３３２，３４２と、
（ｄ）暗号化タイトルキー（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）３３４，３４４、
これらのデータは、例えば図４に示すドメイン機器１２１～１２３が、暗号化コンテンツとともに保持していたデータである。
すなわち、図４に示すドメイン機器１２１～１２３が、コンテンツをコンテンツ提供サーバ１０２から取得した際に、コンテンツとともに、コンテンツ提供サーバ１０２から受領したデータである。
【００９４】
一方、データ（ａ）～（ｄ）中、
（ｃ）メディアＩＤ検証値（ＭＡＣ　ｏｆ　Ｍｅｄｉａ　ＩＤ）３３３，３４３は、ドメイン機器１２１～１２３が保持しているデータではない。このメディアＩＤ検証値（ＭＡＣ　ｏｆ　Ｍｅｄｉａ　ＩＤ）３３３，３４３は、メディアであるメモリカード２００にコンテンツを記録する際に、管理サーバ１０１から予め設定されたシーケンスに従って、取得する情報である。
【００９５】
このメディアＩＤ検証値（ＭＡＣ　ｏｆ　Ｍｅｄｉａ　ＩＤ）３３３，３４３は、メディア（メモリカード２００）と、メディア（メモリカード２００）に記録されるコンテンツとを結びつけるためのデータ、すなわちコンテンツをメディアバインドするためのデータとして利用される。
【００９６】
汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２２０には、さらに、メディア証明書（Ｍｅｄｉａ　Ｃｅｒｔｉｆｉｃａｔｅ）３６０が記録される。このメディア証明書（Ｍｅｄｉａ　Ｃｅｒｔｉｆｉｃａｔｅ）は、例えばメディア（メモリカード２００）のメディアＩＤやメディア公開鍵を格納した公開鍵証明書である。例えば認証局から提供される証明書である。先に図６を参照して説明したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）と同様のデータ構成を有する。ただし、保護領域に対するアクセス許容情報についての記録データは持たない。
このメディア証明書は、例えば、メディア（メモリカード２００）を装着したデバイスとの認証処理において利用される。
【００９７】
管理情報に含まれるトークン（Ｔｏｋｅｎ）３３１，３４１は、対応コンテンツに関する管理情報を記録したデータであり、コンテンツ提供サーバが生成してコンテンツとともにデバイス（ドメイン機器１２１～１２３）に提供するデータである。
具体的なトークン構成データについて、図９を参照して説明する。
【００９８】
図９に示すようにトークンは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）
【００９９】

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。

【０１００】

（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。

【０１０１】

サーバＩＤは、認証局が各コンテンツ提供サーバに設定したＩＤである。先に図６を参照して説明したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）と同様のデータを有するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）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、コンテンツ提供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とコンテンツ提供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。

【０１０２】

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。

【０１０３】

（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。

【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。

【０１０５】

（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メモリカードに記録される利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）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。

【０１０６】

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。

【０１０７】

（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９の（７）に示す署名の作成日時情報である。

【０１０８】

トークン（Ｔｏｋｅｎ）には、上述したデータの他、図９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。

【０１０９】

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、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）から取得可能である。

【０１１０】

［７．デバイスからメモリカードに対するコンテンツ記録シーケンスについて］

次に、図１０に示すシーケンス図を参照して、例えば図４に示すドメイン機器１２１～１２３等のデバイスからメモリカード２００に対するコンテンツ記録シーケンスについて説明する。

【０１１１】

図１０には、左から、

コンテンツを保持するデバイス（例えば図４に示すドメイン機器１２１～１２３）、

コンテンツの記録対象となるメモリカード、

管理サーバ、

これらを示している。

【０１１２】

デバイスは、例えば図４に示すドメイン機器１２１～１２３であり、管理サーバ１０１からドメインキーを受領している機器である。また、コンテンツ提供サーバ１０２から暗号化コンテンツおよびその管理情報を保持しているデバイスである。

管理情報には、先に図８を参照して説明した以下の情報が含まれる。

（ａ）トークン（Ｔｏｋｅｎ）、

（ｂ）利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）、

（ｄ）暗号化タイトルキー（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）、

これらの情報が含まれる。

【０１１３】

図１０のシーケンス図に従って、各処理について説明する。

まず、デバイス（例えば図４に示すドメイン機器１２１～１２３）は、メモリカードを装着し、ステップＳ１０１においてデバイスとメモリカード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。

【０１１４】

デバイス、メモリカードとも、認証局の発行した公開鍵を格納した証明書（Ｃｅｒｔｉｆｉｃａｔｅ）と秘密鍵を保持している。デバイスの保持する証明書（Ｃｅｒｔｉｆｉｃａｔｅ）は先に図６を参照して説明したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）であり、公開鍵の他、メモリカードの保護領域に関するアクセス権情報が記録されている。

【０１１５】

なお、メモリカードは相互認証処理や、図５や図７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。

【０１１６】

デバイス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Ｓ１０２以下の処理が実行される。例えば、ステップＳ１０３におけるデバイスからメモリカードに対する暗号化コンテンツを含む様々なデータ提供処理が行われる。相互認証が成立しない場合は、ステップＳ１０２以下の処理は実行されない。すなわち、ステップＳ１０３におけるデバイスからメモリカードに対するデータ提供処理も行われない。

【０１１７】

デバイス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、メモリカードのデータ処理部は、ステップＳ１０２において、デバイスが認証処理に際してメモリカードに提供した公開鍵証明書（図６に示すホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ））を参照して、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセス権の確認を行う。

【０１１８】

先に図５、図６、図７を参照して説明したように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）は複数の区分領域に区分され、デバイスがメモリカードに提供したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には各区分領域単位のアクセス権情報（書き込み（Ｗｒｉｔｅ）／読み出し（Ｒｅａｄ）の許容情報）が記録されている。

【０１１９】

メモリカードのデータ処理部は、デバイスから受領した証明書（図６に示すホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）を参照して、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の各区分領域についてのアクセス権の確認を行う。

【０１２０】

なお、メモリカードに対するコンテンツの記録処理に際しては、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するドメインキーの書き込みを行うことが必要となる。従って、メモリカードのデータ処理部は、デバイスから受領した証明書（図６に示すホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）にメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の１つ以上の区分領域に対する書き込み（Ｗｒｉｔｅ）許容情報が記録されているか否かを確認する。

【０１２１】

区分領域に対する書き込み（Ｗｒｉｔｅ）許容情報がない場合、そのデバイスによるメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するドメインキーの書き込みは許容されない。この場合、ステップＳ１０３以下のメモリカードに対するコンテンツの提供処理は中止される。

【０１２２】

デバイスからメモリカードに提供された証明書（図６に示すホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）にメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の１つ以上の区分領域に対する書き込み（Ｗｒｉｔｅ）許容情報が記録されている場合には、デバイスの提供するドメインキーを保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録可能となり、この場合に限り、ステップＳ１０３以下の処理が実行される。

【０１２３】

ステップＳ１０３では、デバイスがメモリカードに対して、以下のデータを送信する。

（１）暗号化コンテンツ
（２）管理情報（トークン、利用制御情報、暗号化タイトルキー）
（３）ドメインキー
【０１２４】
これらの情報中、
（１）暗号化コンテンツ
（２）管理情報（トークン、利用制御情報、暗号化タイトルキー）
これらの情報は、デバイスがコンテンツ提供サーバからのコンテンツ取得処理に際して受領したデータである。
（３）ドメインキーは、デバイスが管理サーバから受領した鍵情報である。
【０１２５】
メモリカードは、ステップＳ１０４において、デバイスから受領したデータをメモリカードの記憶領域に書き込む処理を行う。
上記の（１）～（３）の受領データ中、
（１）暗号化コンテンツ
（２）管理情報（トークン、利用制御情報、暗号化タイトルキー）
これらの情報は、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に書き込む。
【０１２６】
さらに、上記の（１）～（３）の受領データ中、
（３）ドメインキー
は、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録する。なお、ドメインキーは、先のステップＳ１０２におけるデバイスの証明書（Ｈｐｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）に基づくアクセス権の確認処理において、書き込み（Ｗｒｉｔｅ）処理の許容された区分領域に書き込む処理が実行される。
【０１２７】
次に、メモリカードは管理サーバとの相互認証処理を開始する。なお、メモリカードとサーバ間の通信は、メモリカードを装着しているデバイスの通信部を介して実行する。
【０１２８】
管理サーバとメモリカード間の相互認証処理は、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。管理サーバも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。
【０１２９】
管理サーバ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Ｓ１０６において、サーバはメモリカードの証明書に記録されているメモリカードの識別情報であるメディアＩＤを取得してメディアＩＤの検証値としてのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成する。
管理サーバは、ステップＳ１０７において、生成したメディアＩＤの検証値としてのＭＡＣをメモリカードに送信する。
【０１３０】
メモリカードは、ステップＳ１０８において、管理サーバから受信したメディアＩＤ検証値（ＭＡＣ）をメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に書き込む。
以上の処理によって、メモリカードには、例えば先に図８を参照して説明したデータ、すなわち、具体的には、
暗号化コンテンツファイル３１０、
管理情報３３０、
ドメインキー３８１、

これらのデータが格納されることになる。
なお、先に図８を参照して説明したように、コンテンツとコンテンツに対応する管理情報は、識別情報（ＩＤ１，ＩＤ２，ＩＤ３・・・）によって関連付けられて記録される。
【０１３１】
メモリカードは、コンテンツの新たな記録処理に際して、コンテンツファイル中に含まれるセキュリティボックス内に記録された識別子（ＩＤ）を取得し、そのＩＤをインデックスとして設定した記憶領域をメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に設定し、設定した記憶領域にコンテンツファイルに対応する管理情報を記録する。
【０１３２】
また、デバイスは、デバイスがメモリカードに提供する管理情報に含まれる利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）にデバイス識別子を記録してメモリカードに提供する構成としてもよい。
すなわちコンテンツの移動元またはコピー元のデバイスを示す情報を利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）に記録してメモリカードに提供する構成としてもよい。
このような設定とすることで、メモリカードに記録されたコンテンツおよび管理情報を元のデバイスに返還する際、利用制御情報（Ｕｓａｇｅ　Ｆｉｌｅ）を参照してコンテンツの提供元を確認して、コンテンツの出力デバイスに対して誤りなくコンテンツを返却することが可能となる。
【０１３３】
また、図１０を参照して説明したシーケンスではデバイスからメモリカードに対してデバイスの保持するドメインキーをそのまま出力する構成として説明したが、そのまま出力するのではなく、予め設定した変換アルゴリズムに従ってドメインキーを変換して変換ドメインキーを生成し変換ドメインキーをメモリカードに提供して格納する構成としてもよい。
【０１３４】
ただし、この場合、コンテンツ再生を実行する再生装置では、上記の変換アルゴリズムと逆の変換アルゴリズムを実行して変換ドメインキーを元のドメインキーに戻して、その後の処理を行うことになる。
【０１３５】
また、デバイスがメモリカードに出力する管理情報として、さらに、
元のデバイスにおけるコンテンツの利用制御規格情報、例えば、
マーリン（Ｍａｒｌｉｎ　０ｘ００）
上記のような元のデバイスにおけるコンテンツの利用制御規格情報を記録する設定としてもよい。
【０１３６】
さらに、元のデバイスにおけるコンテンツの利用制御規格おいて許容されているコンテンツの同時利用可能な機器数についての情報や、今回のコンテンツ出力に基づく残りの利用可能な機器数の情報をデバイスに保持しメモリカードにも出力する構成としてもよい。
この処理によって、複数のメモリカードに対する出力を行う場合に、元のコンテンツ利用制御規定に従った範囲でのコンテンツ出力処理を行うように制御することが可能となる。
【０１３７】
［８．メモリカード格納コンテンツの再生シーケンスについて］
次に、図１０を参照して説明したシーケンスに従ってコンテンツ他の情報を記録したメモリカードを装着したデバイス、例えば図４に示す非ドメイン機器としての再生装置１３１がコンテンツを再生する処理のシーケンスについて図１１、図１２に示すフローチャートを参照して説明する。
なお、再生装置１３１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、管理情報の検証、管理情報を適用したコンテンツ検証等を実行する。

【０１３８】

図１０に示すステップＳ２０１において、再生装置は、再生対象となるコンテンツと管理情報、およびドメインキーを格納したメディア（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。

【０１３９】

ステップＳ２０２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。

【０１４０】

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Ｓ２０３の判定＝Ｎｏ）は、ステップＳ２５１に進みコンテンツ再生を中止する。

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Ｓ２０３の判定＝Ｙｅｓ）、ステップＳ２０４に進む。

【０１４１】

再生装置は、ステップＳ２０４において、認証処理においてメモリカードから受領した証明書からメモリカードの識別情報であるメディアＩＤを取り出してＭＡＣを算出する。

【０１４２】

次に、再生装置は、ステップＳ２０５において算出ＭＡＣ値と、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から読み出したメディアＩＤ検証値（ＭＡＣ）との照合処理を行う。２つのＭＡＣ値が一致すれば、メモリカードは、先に図１０を参照して説明した正しいシーケンスに従ってコンテンツが記録されたメディアであると判定（ステップＳ２０５の判定＝Ｙｅｓ）し、ステップＳ２０６に進む。

【０１４３】

２つのＭＡＣ値が一致しない場合は、メモリカードは、先に図１０を参照して説明した正しいシーケンスに従ってコンテンツが記録されたメディアでないと判定（ステップＳ２０５の判定＝Ｎｏ）し、ステップＳ２５１に進みコンテンツ再生を中止する。

【０１４４】

ステップＳ２０５の判定＝Ｙｅｓと判定され、メモリカードが、先に図１０を参照して説明した正しいシーケンスに従ってコンテンツが記録されたメディアであると判定した場合は、ステップＳ２０６に進み、再生装置は、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）からドメインキーの読み取り処理を実行する。

【０１４５】

なお、先に説明したように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセスに際しては、証明書の提示に基づくメモリカードによるアクセス権判定処理が必要となる。

メモリカードは、再生装置からのドメインキー読み取り要求に応じて、認証処理に際して再生装置から受領した証明書を参照して、証明書に記録された保護領域に対するアクセス権の記録を確認する。アクセス権情報としてドメインキーが記録された保護領域の区分領域に対する読み取り（Ｒｅａｄ）許容情報が記録されている場合に限り、再生装置のドメインキー読み取りが実行される。記録されていな場合は、ドメインキーの読み取りは実行されないことになり、コンテンツ再生処理は実行されないことになる。

【０１４６】

再生装置のアクセス権確認に基づくドメインキー読み取り処理が行われると、再生装置は、ステップＳ２０７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。

【０１４７】

次に、再生装置は、図１２に示すステップＳ２０８において、取得したドメインキーを利用し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復号処理を実行しタイトルキーを取得する。

【０１４８】

次に、再生装置は、ステップＳ２０９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Ｓ２１０において検証成立と判定されると、ステップＳ２１１に進み、検証不成立の場合は、ステップＳ２５１に進み再生処理を中止する。

【０１４９】

ステップＳ２１０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Ｓ２１１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Ｓ２１２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Ｓ２０８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。

【０１５０】

このように、再生装置は、コンテンツ再生処理に際して、

メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録されているドメインキーを取得することが可能であり、

取得したドメインキーによる暗号化タイトルキーの復号によるタイトルキー取得、

取得したタイトルキーによる暗号化コンテンツの復号によるコンテンツの取得、

これらの処理を行うことが可能となり、コンテンツ再生を実行することができる。

【０１５１】

本処理において、メディアＩＤのＭＡＣの検証によって、コンテンツが管理サーバによる監視下の正当なシーケンスでメディアに記録されたことが確認可能となる。

例えば図１０に示すシーケンス以外の処理によって管理サーバによる監視外でコンテンツが記録されたメディアを利用した場合は、ステップＳ２０５におけるメディアＩＤのＭＡＣ検証が不成立となり、コンテンツ再生は中止され、コンテンツの不正利用が防止される。

【０１５２】

［９．各装置のハードウェア構成例について］

最後に、図１３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１３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。

【０１５３】

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。

【０１５４】

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。

【０１５５】

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。

【０１５６】

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。

【０１５７】

図１４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。

【０１５８】

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。

【０１５９】

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。

【０１６０】

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。

【０１６１】

［１０．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。

【０１６２】

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）利用管理対象となるコンテンツを出力するコンテンツ出力装置と、

前記コンテンツを前記コンテンツ出力装置から入力して格納するメディアと、

前記メディアを装着して前記コンテンツの再生を行う再生装置と、

コンテンツの前記メディアに対する記録処理の管理を実行する管理サーバを有するコンテンツ利用システムであり、

前記コンテンツ出力装置は、
暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵を前記メディアに出力し、
前記管理サーバは、
前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を生成して前記メディアに送信し、
前記メディアは、
前記暗号化コンテンツと、前記暗号鍵と、前記メディアＩＤ検証値を記憶部に格納し、
前記再生装置は、
前記メディアを装着し、前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行するコンテンツ利用システム。

【０１６３】

（２）前記メディアは、メディアの記憶部に対するアクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域を有し、前記コンテンツ出力装置の証明書検証に基づいてアクセス許容判定のなされた保護領域に前記暗号鍵を格納し、前記再生装置による前記暗号鍵読み取り要求に応じて、前記再生装置の証明書検証に基づいてアクセス許容判定のなされた保護領域に記録された前記暗号鍵を前記再生装置に出力する前記（１）に記載のコンテンツ利用システム。

【０１６４】

（３）前記暗号化コンテンツは、タイトルキーで暗号化された暗号化コンテンツであり、前記暗号鍵は、前記タイトルキーの暗号化および復号処理に適用されるドメインキーまたはドメインキーの変換キーであり、前記コンテンツ出力装置は、前記暗号化コンテンツと、前記ドメインキーで暗号化された暗号化タイトルキーを前記メディアに出力する前記（１）または（２）に記載のコンテンツ利用システム。

【０１６５】

（４）前記ドメインキーは、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供する暗号鍵である前記（１）～（３）いずれかに記載のコンテンツ利用システム。

【０１６６】

（５）前記コンテンツ出力装置は、前記ドメインキーを保持するたコンテンツ利用を許容されたドメイン機器であり、前記再生装置は、前記ドメインキーを保持しない非ドメイン機器である前記（１）～（３）いずれかに記載のコンテンツ利用システム。

【０１６７】

（６）データ処理部と記憶部を有し、
前記記憶部は、
アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分され、
前記汎用領域に暗号化コンテンツと、自装置の識別子であるメディアＩＤに基づいて生成されたメディアＩＤ検証値を格納し、
前記保護領域に、前記暗号化コンテンツの利用処理に適用する暗号鍵を格納し、
前記データ処理部は、
前記暗号化コンテンツの利用予定の再生装置から提供される証明書を検証して、前記保護領域に対するアクセス権の確認に応じて前記再生装置による前記暗号鍵の読み取りを許容し、
前記再生装置に対してメディアＩＤを出力し、再生装置におけるメディアＩＤに基づく算出検証値と前記汎用領域に格納されたメディアＩＤ検証値の照合処理に基づくコンテツ

再生可否判定を実行させることを可能とした情報処理装置。

【０１６８】

（７）前記データ処理部は、前記汎用領域に対する暗号化コンテンツの記録処理に際して、前記メディアＩＤを管理サーバに送信し、管理サーバの生成したメディアＩＤ検証値を受信して前記汎用領域に格納する前記（６）に記載の情報処理装置。

【０１６９】

（８）前記データ処理部は、コンテンツ出力装置から提供される暗号化コンテンツと、前記暗号化コンテンツの暗号化キーであるタイトルキーを暗号化した暗号化タイトルキーを前記汎用領域に格納し、前記暗号化タイトルキーをの暗号鍵であり、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供するドメインキーを前記保護領域に格納する前記（６）または（７）に記載の情報処理装置。

【０１７０】

（９）記憶部を有するメディアに格納された暗号化コンテンツを読み出して、復号、再生処理を実行するデータ処理部を有し、

前記メディアは、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵と、前記メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を格納し、

前記データ処理部は、

前記メディアから取得したメディアＩＤに基づいて検証値を算出し、前記メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、前記暗号鍵を適用したデータ処理によって前記メディアに格納された前記暗号化コンテンツの再生処理を実行する情報処理装置。

【０１７１】

（１０）前記メディアは、メディアの記憶部に対するアクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域を有し、前記データ処理部は、前記メディアに対して、再生装置の証明書であり、前記保護領域に対するアクセス許容情報の記録された証明書の提供処理を行う前記（９）に記載の情報処理装置。

【０１７２】

（１１）前記暗号化コンテンツは、タイトルキーで暗号化された暗号化コンテンツであり、前記暗号鍵は、前記タイトルキーの暗号化および復号処理に適用されるドメインキーまたはドメインキーの変換キーである前記（９）または（１０）に記載の情報処理装置。

（１２）前記ドメインキーは、コンテンツ利用を許容されたドメイン機器に対して管理サーバの提供する暗号鍵である前記（９）～（１１）いずれかに記載の情報処理装置。

【０１７３】

（１３）暗号化コンテンツと、該暗号化コンテンツの利用処理に適用する暗号鍵を格納した記憶部と、データ処理部を有し、

前記データ処理部は、

コンテンツ出力対象となるメディアに対して、前記暗号化コンテンツと前記暗号鍵を出力して記録させる構成であり、

前記メディアは、

アクセス要求装置の証明書検証によるアクセス可否判定に基づいてアクセスの許容される保護領域と、アクセス要求装置の証明書検証によるアクセス可否判定の不要な汎用領域に区分された記憶部を有し、

前記データ処理部は、

自装置の証明書を前記メモリカードに提示し、メモリカードによる証明書検証に基づいてアクセスの許容された保護領域に前記暗号鍵の書き込みを行う情報処理装置。

【０１７４】

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。

【０１７５】
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。

【０１７６】
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】

【０１７７】
以上、説明したように、本開示の一実施例の構成によれば、コンテンツの利用制御の下でメディアに対するコンテンツ出力とメディア格納コンテンツの利用を行う構成が実現される。

具体的には、コンテンツ出力装置が、暗号化コンテンツと、暗号化コンテンツの利用処理に適用する暗号鍵を前記メディアに出力し、管理サーバが、メディアの識別子であるメディアＩＤに基づく検証値であるメディアＩＤ検証値を生成してメディアに送信する。メディアは、暗号化コンテンツと、暗号鍵と、メディアＩＤ検証値を記憶部に格納する。再生装置は、メディアを装着し、メディアから取得したメディアＩＤに基づいて検証値を算出し、メディアに格納済みのメディアＩＤ検証値との照合処理の成立を条件として、暗号鍵を適用したデータ処理によってメディアに格納された暗号化コンテンツの再生処理を実行する。

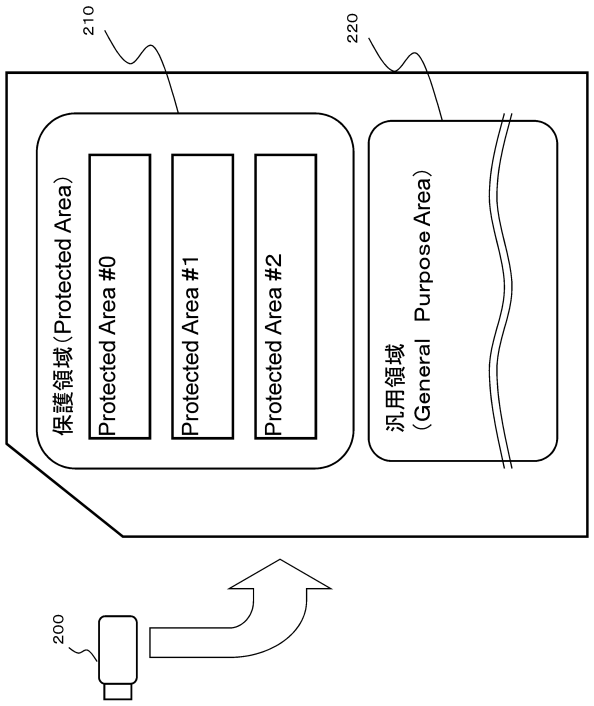
この処理によりメディアバインド型のコンテンツ利用制御が実現される。

【符号の説明】

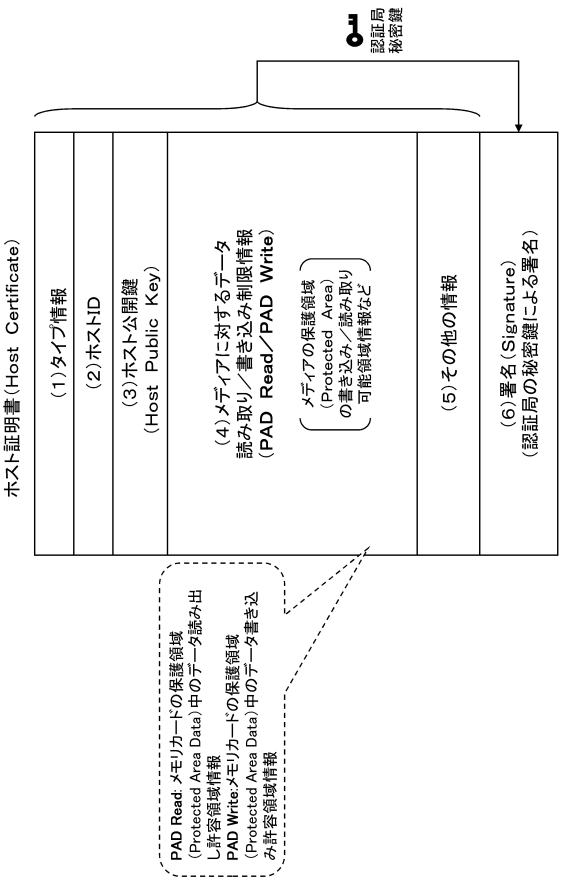
【０１７８】
１１　管理サーバ
２１　ＰＣ
２２　再生装置
２３　テレビ
３０
４０　記憶部
４１　暗号化コンテンツ
４２　暗号化コンテンツキー
４３　ライセンス情報
５０　セキュア記憶部
５１　ドメインキー
７０　メモリカード
１０１　管理サーバ
１０２　コンテンツ提供サーバ
１２１　ＰＣ
１２２　再生装置
１２３　テレビ
１３１　再生装置
２００　メモリカード

２１０　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
２２０　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
２１１，２１２　区分領域
３１０，３２０　暗号化コンテンツファイル
３１１，３２１　セキュリティボックス
３３０，３４０　管理情報
３３１，３４１　トークン
３３２，３４２　利用制御情報
３３３，３４３　メディアＩＤ検証値（ＭＡＣ）
３３４，３４４　暗号化タイトルキー
３６０　メディア証明書
３８１　ドメインキー
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）

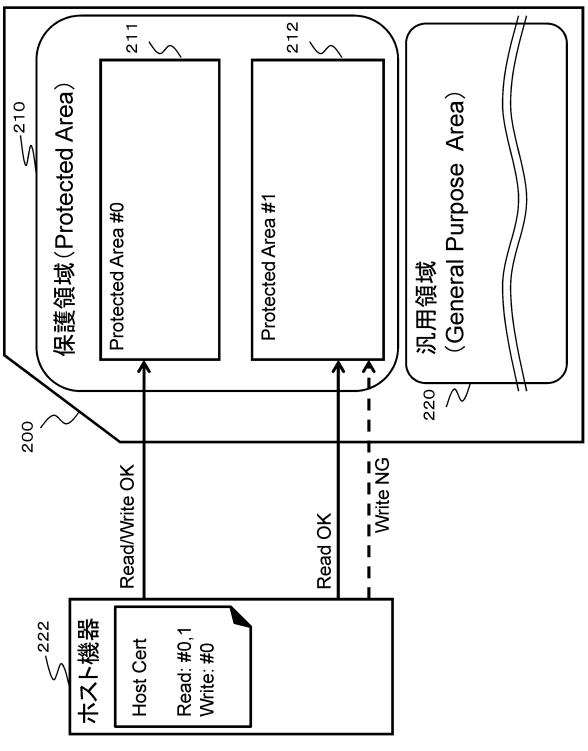
【図５】


210
220
保護領域(Protected Area)
Protected Area #0
Protected Area #1
Protected Area #2
汎用領域
(General Purpose Area)
200

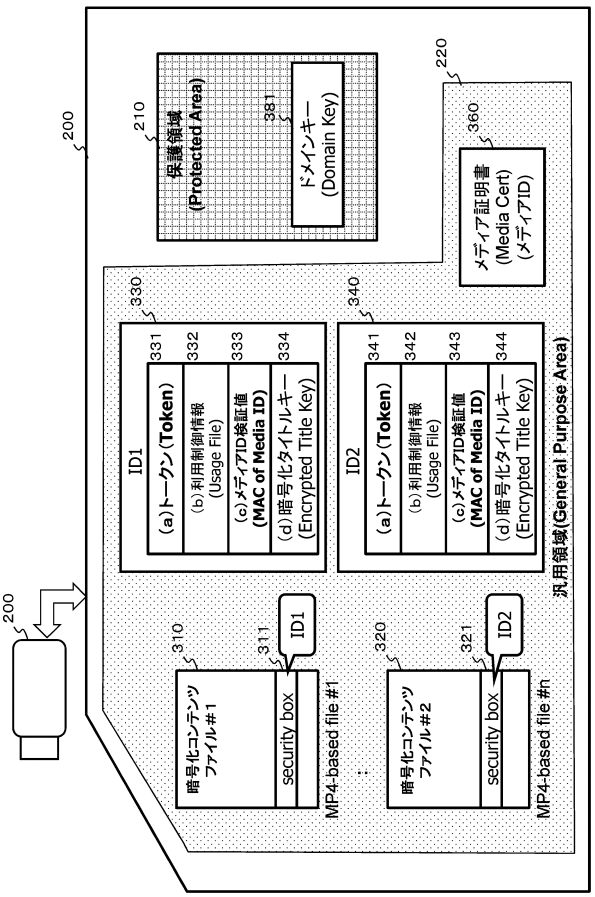
【図６】


認証局
秘密鍵
ホスト証明書(Host Certificate)
(1)タイプ情報
(2)ホストID
(3)ホスト公開鍵
(Host Public Key)
(4)メディアに対するデータ
読み取り／書き込み制限情報
(PAD Read／PAD Write)
メディアの保護領域
(Protected Area)
の書き込み／読み取り
可能領域情報など
(5)その他の情報
(6)署名(Signature)
(認証局の秘密鍵による署名)
PAD Read:メモリカードの保護領域
(Protected Area Data)中のデータ読み出
し許容領域情報
PAD Write:メモリカードの保護領域
(Protected Area Data)中のデータ書き込
み許容領域情報

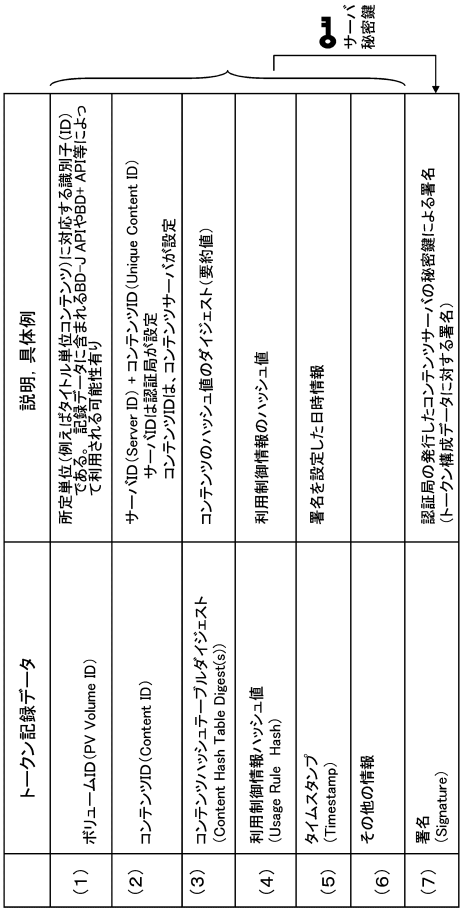
【図７】


200
210
211
212
220
保護領域(Protected Area)
Protected Area #0
Protected Area #1
汎用領域
(General Purpose Area)
Read/Write OK
Read OK
Write NG
222
ホスト機器
Host Cert
Read: #0,1
Write: #0

【図８】


200
210
保護領域
(Protected Area)
381
ドメインキー
(Domain Key)
220
360
メディア証明書
(Media Cert)
(メディアID)
330
ID1
(a)トークン(Token)
331
(b)利用制御情報
(Usage File)
332
(c)メディアID検証値
(MAC of Media ID)
333
(d)暗号化タイトルキー
(Encrypted Title Key)
334
340
ID2
341
342
343
344
310
暗号化コンテンツ
ファイル#1
311
ID1
security box
MP4-based file #1
320
暗号化コンテンツ
ファイル#2
321
ID2
MP4-based file #n
汎用領域(General Purpose Area)

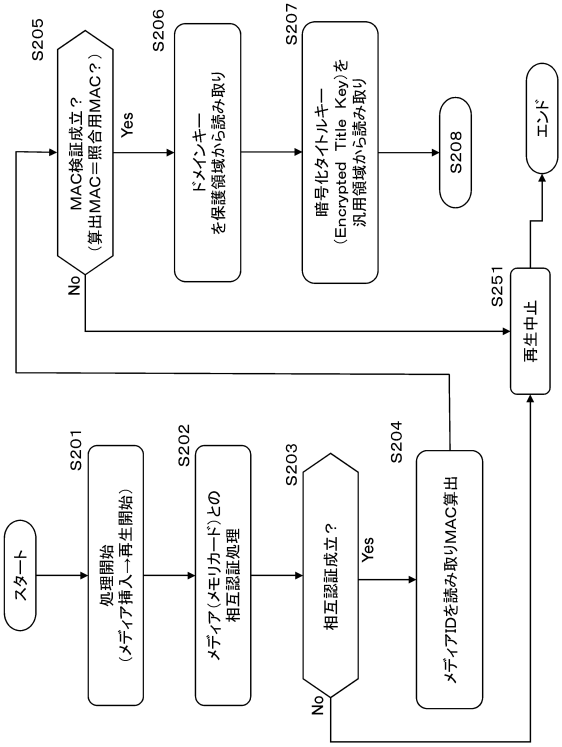
【図９】



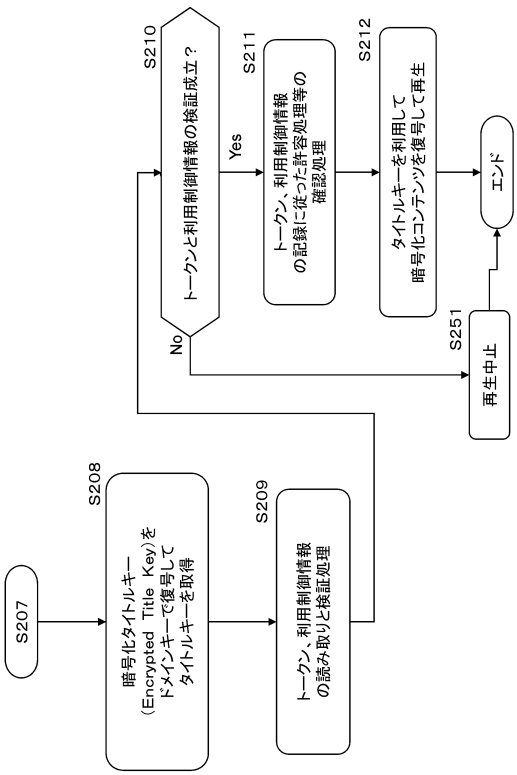
	トークン記録データ	説明、具体例
（1）	ボリュームID（PV Volume ID）	所定単位（例えばタイトル単位コンテンツ）に対応する識別子（ID）である。記録データに含まれるBD-J APIやBD+ API等によって利用される可能性有り
（2）	コンテンツID（Content ID）	サーバID（Server ID）＋コンテンツID（Unique Content ID） サーバIDは認証局が設定 コンテンツIDは、コンテンツサーバが設定
（3）	コンテンツのハッシュテーブルダイジェスト（Content Hash Table Digest(s)）	コンテンツのハッシュ値のダイジェスト（要約値）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

サーバ秘密鍵

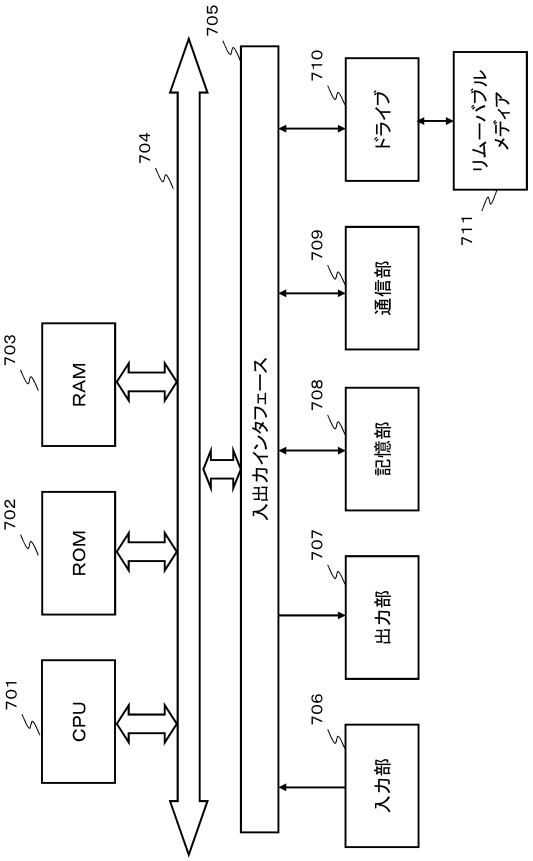
【図１１】



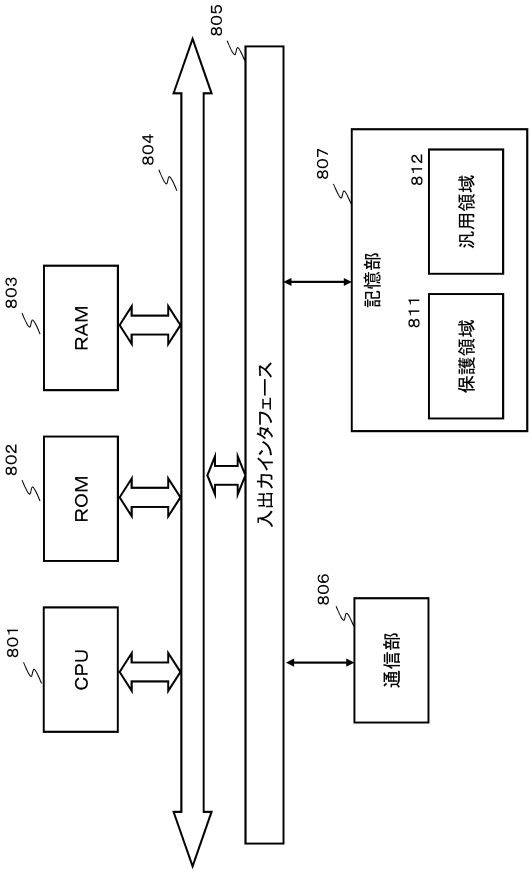
【図１２】



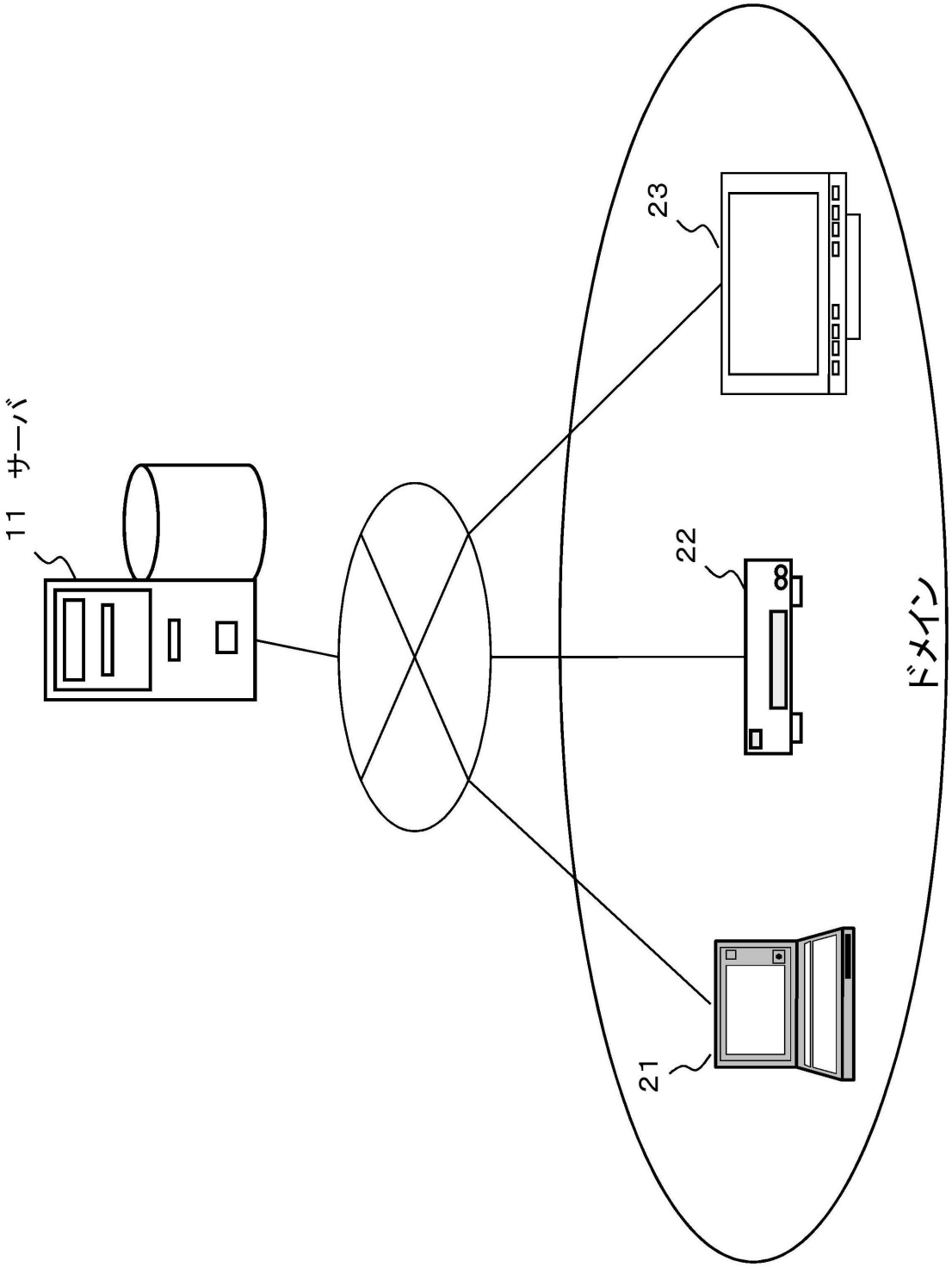
【図１３】



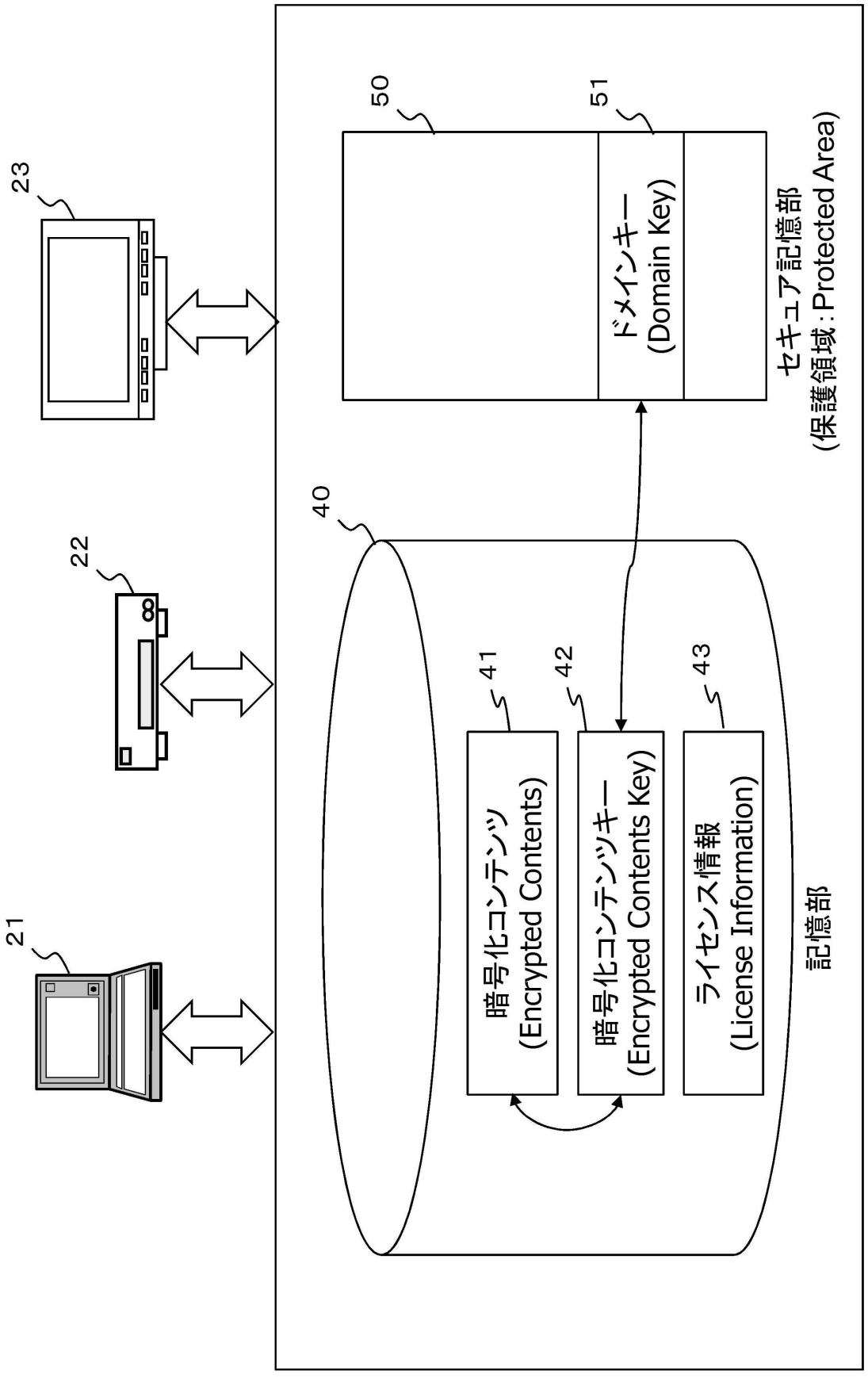
【図１４】


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

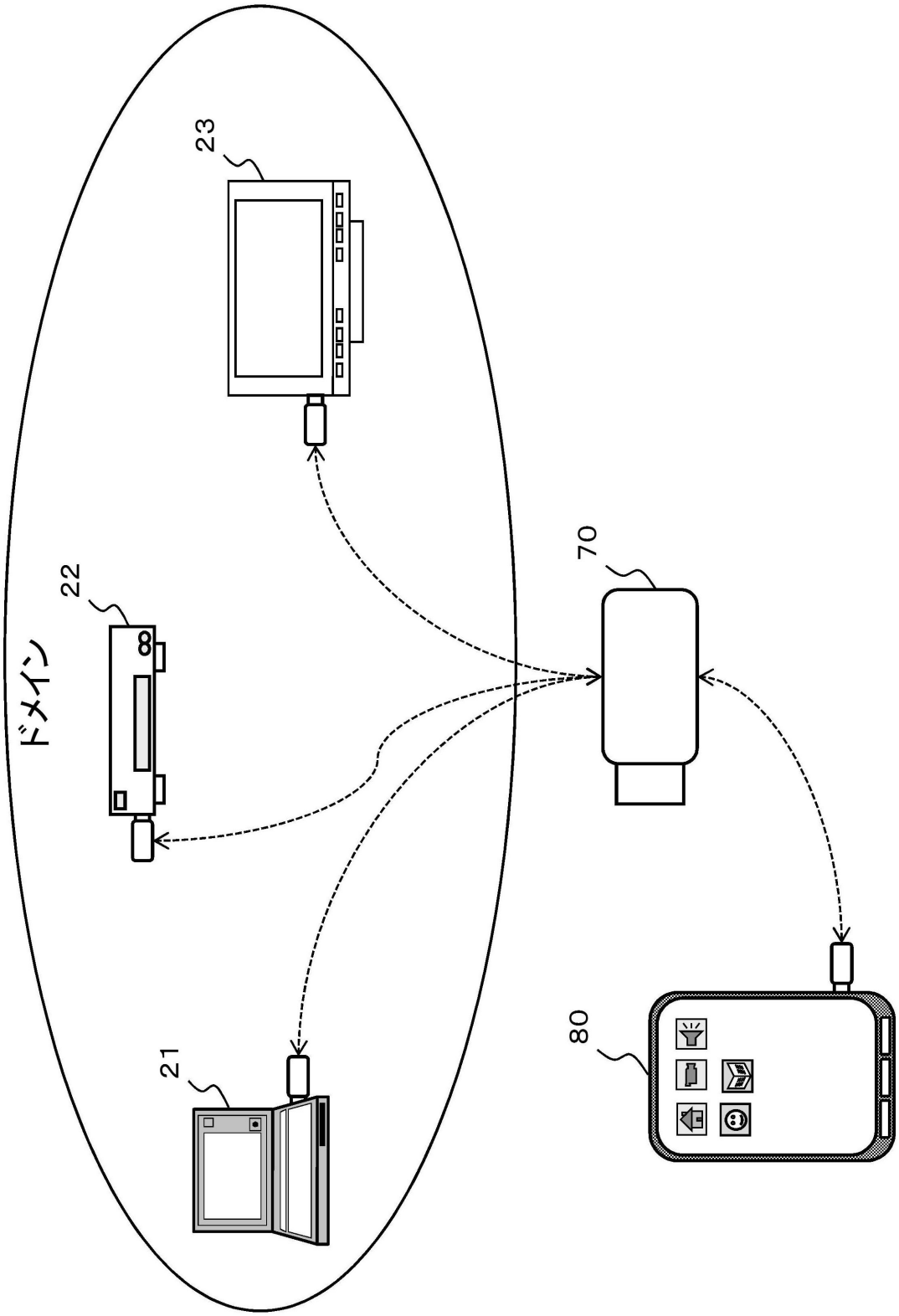
【図１】



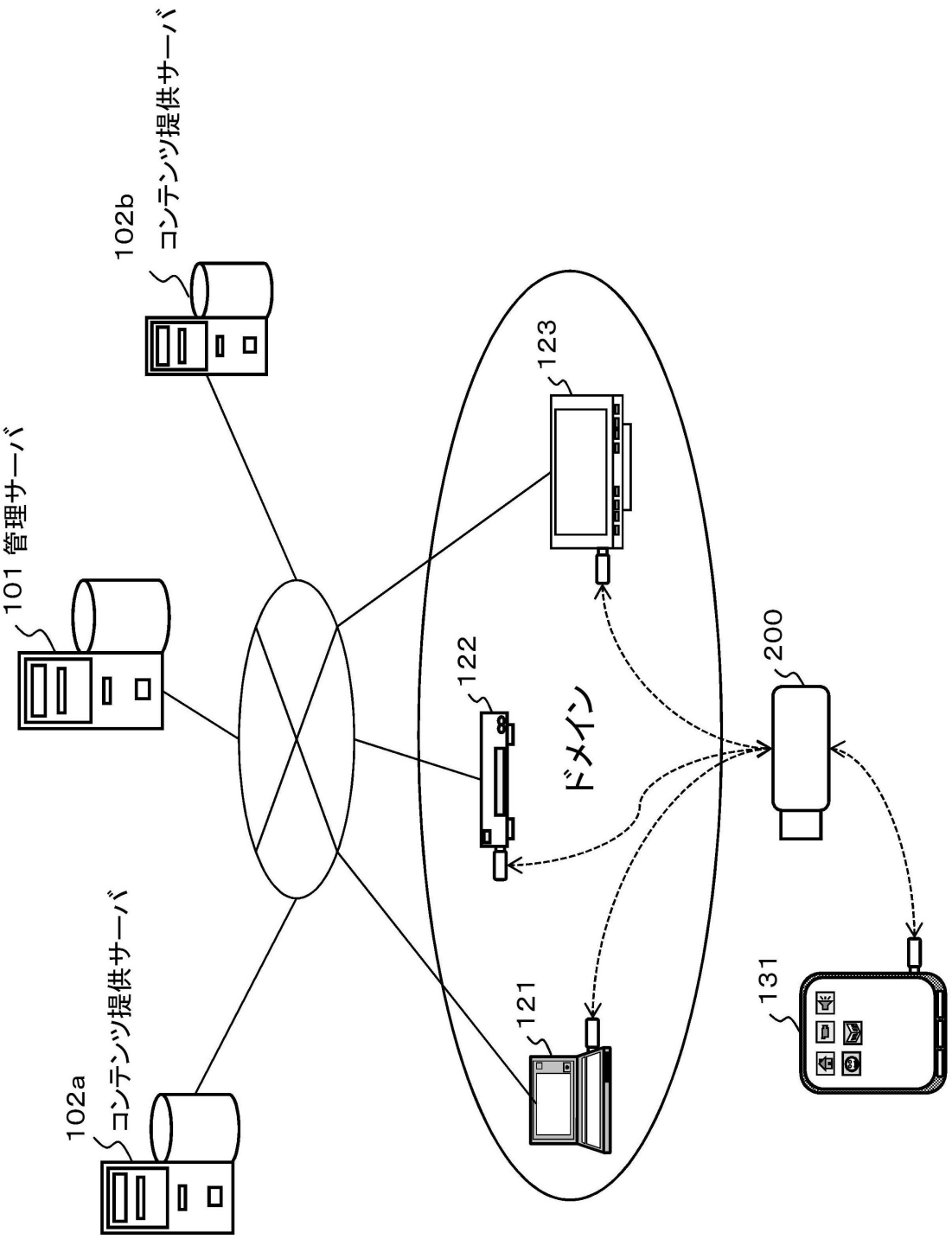
【図２】


23
22
21
50
51
ドメインキー
(Domain Key)
セキュア記憶部
(保護領域:Protected Area)
40
41
42
43
暗号化コンテンツ
(Encrypted Contents)
暗号化コンテンツキー
(Encrypted Contents Key)
ライセンス情報
(License Information)
記憶部

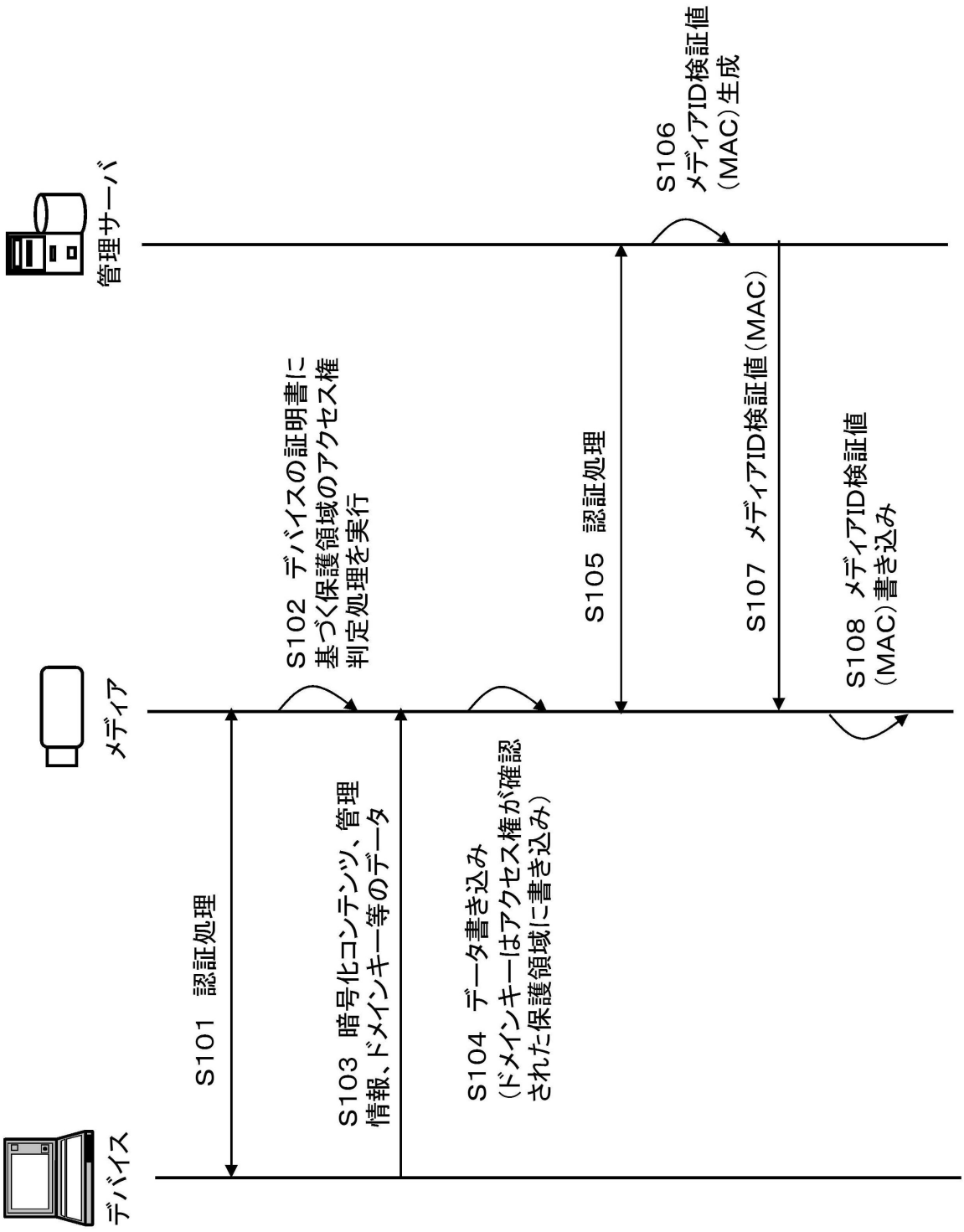
【図３】



【図４】


102b
コンテンツ提供サーバ
101 管理サーバ
123
122
ドメイン
200
102a
コンテンツ提供サーバ
121
131

【図１０】


管理サーバ
メディア
デバイス
S101 認証処理
S102 デバイスの証明書に基づく保護領域のアクセス権判定処理を実行
S103 暗号化コンテンツ、管理情報、ドメインキー等のデータ
S104 データ書き込み（ドメインキーはアクセス権が確認された保護領域に書き込み）
S105 認証処理
S106 メディアID検証値（MAC）生成
S107 メディアID検証値（MAC）
S108 メディアID検証値（MAC）書き込み

フロントページの続き

(51)Int.Cl.			FI		
H04L 9/08	*(2006.01)*		G11B	20/10	D
G09C 1/00	*(2006.01)*		G11B	20/10	F
			G11B	20/10	311
			H04L	9/00	601B
			G09C	1/00	640E

(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
(72)発明者 加藤 元樹
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 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

審査官 岸野 徹

(56)参考文献 特表２００９－５２４３３４（ＪＰ，Ａ）
特開２００５－１２９０５８（ＪＰ，Ａ）
特開２００９－１９９４９０（ＪＰ，Ａ）
特開２００８－０１５６２２（ＪＰ，Ａ）
特開２０１２－０４４５７７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／１０
Ｇ０９Ｃ １／００
Ｇ１１Ｂ ２０／１０
Ｈ０４Ｌ ９／０８
Ｈ０４Ｎ ５／９１
Ｈ０４Ｎ ５／９２
Ｈ０４Ｎ ５／９３