(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2009-93731
(P2009-93731A)
(43)公開日　平成21年4月30日(2009.4.30)

(51)Int.Cl.		F I			テーマコード（参考）
G11B 20/10	(2006.01)	G11B	20/10	H	5B017
G11B 23/30	(2006.01)	G11B	20/10	D	5B035
G06K 19/00	(2006.01)	G11B	23/30	B	5B058
G06K 19/07	(2006.01)	G06K	19/00	Q	5D044
G06K 17/00	(2006.01)	G06K	19/00	H	

審査請求 未請求　請求項の数 18　ＯＬ　（全 32 頁）　最終頁に続く

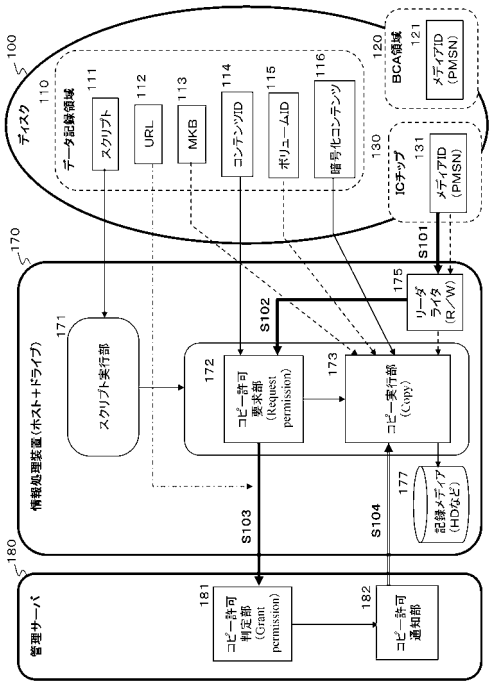
(21)出願番号　特願2007-261781 (P2007-261781)
(22)出願日　平成19年10月5日 (2007.10.5)

(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
(72)発明者　千秋　進
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)　5B017 AA06　BB09　CA06　CA16
最終頁に続く

(54)【発明の名称】情報処理装置、ディスク、および情報処理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】メディアＩＤの迅速な読み取りによるコピー許可情報の取得を可能とする。
【解決手段】コンテンツの記録されたディスクにディスクの固有識別情報であるメディアＩＤ（ＰＭＳＮ）を記録したＩＣチップを設け、ＩＣチップから読み取ったメディアＩＤをサーバに送信してディスク格納コンテンツのコピー許可情報を取得する。本構成によれば、例えばＡＡＣＳ規定に従ったコンテンツ記録ディスクにおいてメディアＩＤ（ＰＭＳＮ）の記録されたＢＣＡ領域からＰＭＳＮデータを読み取る処理が省略可能となり、迅速なＩＣチップからのデータ読み取りによってメディアＩＤを取得可能となり、効率的なコピー許可情報取得処理を行うことが可能となる。
【選択図】図４



【特許請求の範囲】
【請求項１】
ディスクに設けられたＩＣチップからディスクの固有識別子であるメディアＩＤを読み取るデータ読み取り手段と、
前記データ読み取り手段において読み取られたメディアＩＤを含むデータを管理サーバに送信するコピー許可要求手段と、
前記管理サーバからのコピー許可情報の受領を条件として、ディスクに記録されたコンテンツを読み取り、前記ディスク以外のデータ記録手段に対するコピー記録処理を実行するコピー実行手段と、
を有することを特徴とする情報処理装置。
【請求項２】
前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）ディスク記録コンテンツの識別子であるコンテンツＩＤと、
を記録した構成であり、
前記コピー許可要求手段は、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤとコンテンツＩＤを、前記管理サーバに送信する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記情報処理装置は、さらに、
ディスクに記録された簡易プログラムであるスクリプトを実行するスクリプト実行手段を有し、
前記スクリプト実行手段の実行するプログラムに従って、前記コピー許可要求手段および前記コピー実行手段の処理が行われることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）簡易プログラムであるスクリプトと、
（ｃ）前記管理サーバのアドレスを示すＵＲＬと、
を記録した構成であり、
前記スクリプト実行手段は、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったスクリプトを実行し、
前記コピー許可要求手段は、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤを含むデータを、前記ＵＲＬの指定する管理サーバに送信する処理を実行する構成であることを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記情報処理装置は、さらに、
認証処理を実行する認証処理部を有し、
前記認証処理部は、
前記ディスクに設けられたＩＣチップ内に構成された認証処理部との認証処理を行い、
前記情報処理装置は、前記認証処理の成立を条件としてＩＣチップ内の記録データの利用処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記メディアＩＤはＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）において規定されるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ Ｍｅｄｉａ Ｓｅｒｉａｌ Ｎｕｍｂｅｒ）であることを特徴とする請求項１～５いずれかに記載の情報

処理装置。
【請求項７】
コンテンツを記録したディスクであり、
コンテンツを記録したデータ記録部と、
ディスクの固有識別子であるメディアＩＤを記録したＩＣチップを備え、
前記ＩＣチップは、非接触のデータ読み取り手段によるメディアＩＤ読み取りが可能な構成を有し、情報処理装置におけるディスク記録コンテンツの利用に際して、前記ＩＣチップからのメディアＩＤの読み取りおよびメディアＩＤを利用したデータ処理を実行させることを可能とした構成を持つことを特徴とするディスク。
【請求項８】
前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）ディスク記録コンテンツの識別子であるコンテンツＩＤと、
を記録した構成であり、情報処理装置におけるディスク記録コンテンツの利用に際して、前記ＩＣチップからのメディアＩＤおよびコンテンツＩＤの読み取りおよび読み取りデータを利用した処理を実行させることを可能とした構成を持つことを特徴とする請求項７に記載のディスク。
【請求項９】
前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）簡易プログラムであるスクリプトと、
（ｃ）前記管理サーバのアドレスを示すＵＲＬと、
を記録した構成であり、情報処理装置におけるディスク記録コンテンツの利用に際して、前記ＩＣチップからのデータ読み取りを行わせ、スクリプトの実行により前記ＵＲＬによって指定されるサーバに対する前記メディアＩＤの送信処理を行わせる構成としたことを特徴とする請求項７に記載のディスク。
【請求項１０】
前記ＩＣチップは、
認証処理を実行する認証処理部を有し、
前記認証処理部は、
ディスク記録コンテンツの利用を行う情報処理装置との認証処理を行う構成であることを特徴とする請求項７に記載のディスク。
【請求項１１】
前記メディアＩＤはＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）において規定されるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ　Ｍｅｄｉａ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）であることを特徴とする請求項７～１０いずれかに記載のディスク。
【請求項１２】
情報処理装置において、ディスク記録コンテンツの利用処理を行う情報処理方法であり、
データ読み取り手段が、ディスクに設けられたＩＣチップからディスクの固有識別子であるメディアＩＤを読み取るデータ読み取りステップと、
コピー許可要求手段が、前記データ読み取り手段において読み取られたメディアＩＤを含むデータを管理サーバに送信するコピー許可要求ステップと、
コピー実行手段が、前記管理サーバからのコピー許可情報の受領を条件として、ディスクに記録されたコンテンツを読み取り、前記ディスク以外のデータ記録手段に対するコピー記録処理を実行するコピー実行ステップと、
を有することを特徴とする情報処理方法。
【請求項１３】
前記ＩＣチップは、

（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）ディスク記録コンテンツの識別子であるコンテンツＩＤと、
を記録した構成であり、
前記コピー許可要求ステップは、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤとコンテンツＩＤを、前記管理サーバに送信する処理を実行するステップであることを特徴とする請求項１２に記載の情報処理方法。
【請求項１４】
前記情報処理方法は、さらに、
スクリプト実行手段が、ディスクに記録された簡易プログラムであるスクリプトを実行するスクリプト実行ステップを有し、
前記スクリプト実行ステップにおいて実行するプログラムに従って、前記コピー許可要求ステップおよび前記コピー実行ステップの各処理が行われることを特徴とする請求項１２に記載の情報処理方法。
【請求項１５】
前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）簡易プログラムであるスクリプトと、
（ｃ）前記管理サーバのアドレスを示すＵＲＬと、
を記録した構成であり、
前記スクリプト実行ステップは、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったスクリプトを実行し、
前記コピー許可要求ステップは、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤを含むデータを、前記ＵＲＬの指定する管理サーバに送信する処理を実行することを特徴とする請求項１４に記載の情報処理方法。
【請求項１６】
前記情報処理方法は、さらに、
認証処理部が、前記ディスクに設けられたＩＣチップ内に構成された認証処理部との認証処理を行う認証ステップを有し、
前記情報処理装置は、前記認証処理の成立を条件としてＩＣチップ内の記録データの利用処理を実行することを特徴とする請求項１２に記載の情報処理方法。
【請求項１７】
前記メディアＩＤはＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）において規定されるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ Ｍｅｄｉａ Ｓｅｒｉａｌ Ｎｕｍｂｅｒ）であることを特徴とする請求項１２～１６いずれかに記載の情報処理方法。
【請求項１８】
情報処理装置において、ディスク記録コンテンツの利用処理を行わせるコンピュータ・プログラムであり、
データ読み取り手段に、ディスクに設けられたＩＣチップからディスクの固有識別子であるメディアＩＤを読み取らせるデータ読み取りステップと、
コピー許可要求手段に、前記データ読み取り手段において読み取られたメディアＩＤを含むデータを管理サーバに送信させるコピー許可要求ステップと、
コピー実行手段に、前記管理サーバからのコピー許可情報の受領を条件として、ディスクに記録されたコンテンツを読み取らせて、前記ディスク以外のデータ記録手段に対するコピー記録処理を実行させるコピー実行ステップと、
を有することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、情報処理装置、ディスク、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、情報記録媒体の格納コンテンツの利用制御を行う情報処理装置、ディスク、および情報処理方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００２】
コンテンツの記録媒体としてＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクが利用されている。例えば映画コンテンツなどがディスク（例えばＲＯＭディスク）に記録されてユーザに提供されるが、これらのディスク記録コンテンツは、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たコンテンツである場合が多い。このようなコンテンツについては例えば許可のないコピー（複製）等を防止するため、一定の利用制御構成が採用されている。
【０００３】
コンテンツ著作権保護に関する規格としてＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）がある。ＡＡＣＳは高度な共通鍵暗号（ＡＥＳ暗号）を基本とした著作権保護技術を規定している。ＡＡＣＳの規定では、コンテンツ利用処理、例えばディスクからのコンテンツ再生やコンテンツのコピー記録処理等を行なう場合、ディスクに記録された識別情報、例えばディスク固有の識別情報であるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ　Ｍｅｄｉａ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）などの識別情報を読み取り、ＡＡＣＳで規定するシーケンスに従った処理、例えば認証処理や暗号処理を行なうことが必要となる。ＡＡＣＳ規定に従ったコンテンツ格納ディスクの場合、ディスクのＢＣＡ（Ｂｕｒｓｔ　Ｃｕｔｔｉｎｇ　Ａｒｅａ）にディスク固有の識別情報であるＰＭＳＮが記録されている。
【０００４】
ＢＣＡ領域は、通常のデータ記録領域と異なる領域であり、通常のデータ記録方式と異なる物理的なカッティングによってデータが記録される。従ってＢＣＡ領域の記録データは書き換えが困難であり、再生処理においても通常のデータ再生処理とは異なる特殊な読み取り処理が必要となる。
【０００５】
ＡＡＣＳ規定に従ったディスク記録コンテンツの再生処理、および、ディスク記録コンテンツの他のメディア、例えばハードディスクなどの他メディアに対するコピー処理シーケンスについて、図１、図２を参照して説明する。
【０００６】
図１は、ＡＡＣＳ規定に従ったディスク記録コンテンツの再生シーケンスを説明する図である。図１には、左からコンテンツを格納したディスク１０、ディスク１０を装着してディスクからのデータ読み取りを実行するドライブ２０、ドライブ２０を介してディスク１０の記録データを取得してコンテンツの復号、再生を行うホスト３０を示している。なお、図はドライブ２０とホスト３０を別構成として示してあるが、ドライブとホストは１つの装置、例えば再生装置などの一体となった構成である場合もある。左端のディスク（情報記録媒体）１０はＡＡＣＳ規格に対応するディスク１０であり、予め映画などのコンテンツが暗号化コンテンツ１７として記録されている。
【０００７】
ディスク１０には、暗号化コンテンツ１７の識別情報であるコンテンツＩＤ１４、ディスク１０の製造単位毎の識別子であるボリュームＩＤ１５、ディスク固有の識別情報であるメディアＩＤ１６としてＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ　Ｍｅｄｉａ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）が記録されている。メディアＩＤ（ＰＭＳＮ）は前述したようにＢＣＡ領域に記録されている。
【０００８】

ディスク１０は、さらに、
ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト１１、
例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ１２、
暗号化コンテンツ１７の復号処理に適用する鍵情報を格納した暗号鍵ブロックであるＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）１３、
これらのデータが記録されている。

【０００９】

ＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）１３は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号情報（暗号鍵）ブロックである。ＭＫＢ１３は、コンテンツの復号に必要なキーであるメディアキー［Ｋｍ］が暗号化されて格納された暗号情報ブロックであり、有効なライセンスを持つユーザ装置に格納されたデバイスキー［Ｋｄ］を利用した処理（復号）によってメディアキー［Ｋｍ］を取得することができる。

【００１０】

ドライブ２０は、ＡＡＣＳ管理センタの公開鍵と、ドライブ公開鍵とドライブ秘密鍵を含む鍵データ２１、ホストリボケーションリスト２２を有する。ホストリボケーションリスト２２は、ＡＡＣＳの管理センタが不正なホストであると判定したホストの識別情報を記録したリスト、すなわちブラックリストである。例えばホストの識別情報としてホストに対応するホスト公開鍵証明書の識別番号が記録される。ホストリボケーションリスト２２は改ざんがなされないようにＡＡＣＳ管理センタの秘密鍵による署名が付与されている。

【００１１】

ホスト３０は、ＡＡＣＳ管理センタの公開鍵と、ホスト公開鍵とホスト秘密鍵を含む鍵データ３１、ドライブリボケーションリスト３２を有する。ドライブリボケーションリスト３２は、ＡＡＣＳ管理センタが不正なドライブ装置であると判定したドライブの識別情報を記録したリスト、すなわちブラックリストである。例えばドライブの識別情報としてドライブに対応するドライブ公開鍵証明書の識別番号が記録される。ドライブリボケーションリスト３２も改ざんがなされないようにＡＡＣＳ管理センタの秘密鍵による署名が付与されている。なお、ホストリボケーションリスト２２や、ドライブリボケーションリスト３２は、ディスク１０に記録して、ドライブ２０およびホスト３０は、ディスク１０に記録されたデータを読み取って利用する構成としてもよい。

【００１２】

ホスト３０がコンテンツの再生を行なう場合のシーケンスについて説明する。ホスト３０とドライブ２０は、まず、ホスト３０の認証処理部３３とドライブ２０の認証処理部２３との間で認証処理を実行する。この認証処理はＡＡＣＳの規定する処理シーケンスに従って実行される。この処理において各装置の実行する主な処理は以下の通りである。

【００１３】

ドライブ２０は、ホストリボケーションリスト２２を読み取り、ＡＡＣＳ管理センタ公開鍵を適用してホストリボケーションリスト２２の署名検証を行なって改ざんのないことを確認し、ホストリボケーションリスト２２にホスト３０の識別情報が記載されていないこと、すなわち、ホスト３０がリボークされていないことを確認する。

【００１４】

ホスト３０においても、ドライブリボケーションリスト３２を読み取り、ＡＡＣＳ管理センタ公開鍵を適用してドライブリボケーションリスト３２の署名検証を行なって改ざんのないことを確認し、ドライブリボケーションリスト３２にドライブ２０の識別情報が記載されていないこと、すなわち、ドライブ２０がリボークされていないことを確認する。

【００１５】

ドライブ２０とホスト３０の両者ともリボークされていないことが確認された場合は、

ドライブ２０とホスト３０間で、ＡＡＣＳ規定に従った暗号データの通信を実行して、共有秘密鍵を生成してドライブ２０とホスト３０で共有する。

【００１６】

このホストとドライブ間の認証が完了すると、ドライブ２０は、ディスク１０からメディアＩＤ（ＰＭＳＮ）１６を読み取り、ＭＡＣ算出部２４において認証処理に際して生成した共有鍵を適用したＭＡＣ生成処理を実行して、生成ＭＡＣ値と、メディアＩＤ（ＰＭＳＮ）１６をホスト３０に送信する。

【００１７】

なお、メディアＩＤ（ＰＭＳＮ）１６は、前述したように、通常のデータ記録領域と異なるＢＣＡ領域に記録され、通常のデータ再生処理とは異なる特殊な読み取り処理を行うことが必要となる。

【００１８】

ホスト３０のＭＡＣ算出部３４は、認証処理に際して生成した共有鍵を適用したＭＡＣ検証処理を実行する。すなわち、ドライブ２０から受信したメディアＩＤに対して共有鍵を適用したＭＡＣ生成処理を行い、生成ＭＡＣ値とドライプ２０から受信したＭＡＣ値とを照合する。２つのＭＡＣ値が一致した場合に、検証成立と判断し、暗号処理モジュール３６においてＡＡＣＳ規定に従ったコンテンツ復号、再生処理を実行する。

【００１９】

暗号処理モジュール３６において実行するＡＡＣＳ規定に従ったコンテンツ復号においては、デバイスキー［Ｋｄ］３５を適用したＭＫＢ１３の処理により、ＭＫＢ１３からメディアキー［Ｋｍ］を取得し、メディアキー［Ｋｍ］を適用した処理によって、コンテンツの復号用の鍵を取得してコンテンツ復号処理が実行されることになる。

【００２０】

次に、図２を参照して、ディスク記録コンテンツを他のメディア、例えばハードディスクなどの他メディアに対するコピー処理シーケンスについて説明する。ＡＡＣＳ規定に従ったディスク記録コンテンツのコピーに際しては、ＡＡＣＳ規定に従って管理サーバからコピー許可情報を得ることが必要となる。この許可に基づくコピー処理はマネージドコピー（Ｍａｎａｇｅｄ　Ｃｏｐｙ）と呼ばれる。

【００２１】

図２には、左からコピー許可情報を出力する管理サーバ５０、コピー処理を実行する情報処理装置４０、コピー対象のコンテンツを格納したディスク１０を示している。なお、情報処理装置４０は、図１を参照して説明したホストとドライブの双方の機能を持つ装置である。ディスク１０は図１を参照して説明したディスク１０と同じくＡＡＣＳ規格に対応するディスク１０であり、予め映画などのコンテンツが暗号化コンテンツ１７として記録されている。ディスク１０のその他の記情報は、図１を参照して説明したと同様の情報である。

【００２２】

情報処理装置４０は、ディスク１０に記録された暗号化コンテンツ１７を記録メディア４４、例えば情報処理装置４０の保有するハードディスクなどの記録メディア４４にコピーする場合、情報処理装置４０は、管理サーバ５０からコピー許可情報を得るため、ディスク１０に記録されたスクリプト１１（簡易プログラム）をスクリプト実行部４１において実行する。

【００２３】

スクリプト１１には、コピー処理を実行する際の一連の手続きを実行するプログラムが記録されている。情報処理装置４０のコピー許可要求部４２は、ディスク１０からコンテンツＩＤ１４と、メディアＩＤ（ＰＭＳＮ）１６を読み取り、これらのＩＤ情報を、ディスク１０に記録されたＵＲＬ１２に従って管理サーバ５０に送信する。なお、メディアＩＤ（ＰＭＳＮ）１６は、前述したように、通常のデータ記録領域と異なるＢＣＡ領域に記録され、通常のデータ再生処理とは異なる特殊な処理よって読み取ることが必要となる。

【００２４】

管理サーバ５０のコピー許可判定部５１は、情報処理装置５０からコンテンツＩＤ１４と、メディアＩＤ（ＰＭＳＮ）１６を受信し、コピー対象コンテンツとその記録ディスクを確認し、コピーが許容されるか否かを判定する。管理サーバ５０は、ディスクおよびコンテンツ単位のコピー許容情報を保持している。例えば、特定のディスクのあるコンテンツＡは１回のコピー処理を許容するコンテンツであるといった情報である。

【００２５】

管理サーバ５０のコピー許可判定部５１は、このようなコピー許容情報に従って、情報処理装置４０からのコピー要求を許可するか否かを判定し、コピー可否判定情報を、コピー許可通知部５２を介して情報処理装置４０に通知する。

【００２６】

情報処理装置４０は、管理サーバ５０からコピー許可情報を受信すると、コピー実行部４３において、ディスク１０に記録された暗号化コンテンツ１７を読み取り、情報処理装置４０の保有するハードディスクなどの記録メディア４４にコピーする処理を実行する。なお、このコピー処理に際しては、暗号化コンテンツ１７の復号処理を実行して復号コンテンツとして記録することが可能であり、この場合は、ＭＫＢ１３、ボリュームＩＤ１５をディスク１０から読み取り、これらの読み取りデータを適用してＡＡＣＳ規定に従った復号シーケンスを実行して取得した復号コンテンツを記録メディア４４に記録する。

【００２７】

以上、ＡＡＣＳ規定に従ったディスク記録コンテンツの再生処理、および、ディスク記録コンテンツのコピー処理シーケンスについて、図１、図２を参照して説明した。上述したシーケンスでは、コンテンツ再生、コピー処理のいずれにおいても、各処理を行うためにディスクから様々なデータを読み取ることが必要となる。すなわちコンテンツの再生やコピー処理を開始する以前にディスクに記録された複数のＩＤなどの読み取りが必要であり、このためにディスク再生処理を行うことが必要となる。さらに、いずれの処理においても、メディアＩＤ（ＰＭＳＮ）１６の読み取りが必須となっている。

【００２８】

メディアＩＤ（ＰＭＳＮ）１６は、前述したように、通常のデータ記録領域と異なるＢＣＡ領域に記録され、通常のデータ再生処理とは異なる特殊な処理よって読み取ることが必要となり、コンテンツ再生やコピーを行う装置は、このＢＣＡ読み取りを行う機能を備えることが必須となる。

【００２９】

このように、コンテンツ再生やコピーを行う従来のシーケンスでは、ディスク再生やＢＣＡ領域のデータ読み取りが必須であり、とくにコンテンツのコピーを行う場合には、管理サーバとの送受信の前にＢＣＡ領域のデータ読み取りを行い、管理サーバとの送受信の後に通常のデータ記録領域のデータ読み取りを行うというように、実際のコピー処理を開始する前に必要となる処理の負荷が大きく、またこれらの処理に必要とする時間も増大するという問題がある。

【００３０】

一部のデータをディスクに記録せず、高速なデータ読み取りが可能な素子、例えば高周波による近接通信を可能としたＩＣチップに記録する構成を開示した従来技術として例えば特許文献１がある。特許文献１には、光ディスクにＩＣチップを埋め込み、光ディスクに記録されたソフトウェアのインストールに必要とするソフトウェアの識別情報や利用制御情報をＩＣチップに記録して、ＩＣチップの記録情報を利用してソフトウェアインストール前の事前処理を実行する構成が記載されている。また、特許文献２には、ＲＦＩＤタグを光ディスクに埋め込み、ＲＦＩＤタグに鍵情報を記録しておく構成を開示している。しかし、これらいずれの従来技術にも、ディスク記録コンテンツのコピー処理などにおいて必要とするデータのＩＣチップへの記録や読み取り処理については開示していない。

【特許文献１】特開２００７－１３３６０８号公報

【特許文献２】特開２００５－３１６９９４号公報

【発明の開示】

【発明が解決しようとする課題】
【００３１】
本発明は、ディスク記録コンテンツのコピー処理に際して、管理サーバからの許可情報を取得するために必要とする情報の高速取得を可能とし、コピー許可の取得処理を迅速に行うことを可能とする情報処理装置、ディスク、および情報処理方法、並びにコンピュータ・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】
【００３２】
本発明の第１の側面は、
ディスクに設けられたＩＣチップからディスクの固有識別子であるメディアＩＤを読み取るデータ読み取り手段と、
前記データ読み取り手段において読み取られたメディアＩＤを含むデータを管理サーバに送信するコピー許可要求手段と、
前記管理サーバからのコピー許可情報の受領を条件として、ディスクに記録されたコンテンツを読み取り、前記ディスク以外のデータ記録手段に対するコピー記録処理を実行するコピー実行手段と、
を有することを特徴とする情報処理装置にある。
【００３３】
さらに、本発明の情報処理装置の一実施態様において、前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）ディスク記録コンテンツの識別子であるコンテンツＩＤと、
を記録した構成であり、
前記コピー許可要求手段は、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤとコンテンツＩＤを、前記管理サーバに送信する処理を実行する構成であることを特徴とする。
【００３４】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、ディスクに記録された簡易プログラムであるスクリプトを実行するスクリプト実行手段を有し、前記スクリプト実行手段の実行するプログラムに従って、前記コピー許可要求手段および前記コピー実行手段の処理が行われることを特徴とする。
【００３５】
さらに、本発明の情報処理装置の一実施態様において、前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）簡易プログラムであるスクリプトと、
（ｃ）前記管理サーバのアドレスを示すＵＲＬと、
を記録した構成であり、
前記スクリプト実行手段は、前記データ読み取り手段を介して、前記ＩＣチップから読み取ったスクリプトを実行し、前記コピー許可要求手段は、前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤを含むデータを、前記ＵＲＬの指定する管理サーバに送信する処理を実行する構成であることを特徴とする。
【００３６】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、認証処理を実行する認証処理部を有し、前記認証処理部は、前記ディスクに設けられたＩＣチップ内に構成された認証処理部との認証処理を行い、前記情報処理装置は、前記認証処理の成立を条件としてＩＣチップ内の記録データの利用処理を実行する構成であることを特徴とする。
【００３７】
さらに、本発明の情報処理装置の一実施態様において、前記メディアＩＤはＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）において規定されるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ Ｍｅｄｉａ Ｓｅｒｉａｌ Ｎｕｍｂｅｒ）であ

ることを特徴とする。
【００３８】
さらに、本発明の第２の側面は、
コンテンツを記録したディスクであり、
コンテンツを記録したデータ記録部と、
ディスクの固有識別子であるメディアＩＤを記録したＩＣチップを備え、
前記ＩＣチップは、非接触のデータ読み取り手段によるメディアＩＤ読み取りが可能な構成を有し、情報処理装置におけるディスク記録コンテンツの利用に際して、前記ＩＣチップからのメディアＩＤの読み取りおよびメディアＩＤを利用したデータ処理を実行させることを可能とした構成を持つことを特徴とするディスクにある。
【００３９】
さらに、本発明のディスクの一実施態様において、前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）ディスク記録コンテンツの識別子であるコンテンツＩＤと、
を記録した構成であり、情報処理装置におけるディスク記録コンテンツの利用に際して、前記ＩＣチップからのメディアＩＤおよびコンテンツＩＤの読み取りおよび読み取りデータを利用した処理を実行させることを可能とした構成を持つことを特徴とする。
【００４０】
さらに、本発明のディスクの一実施態様において、前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）簡易プログラムであるスクリプトと、
（ｃ）前記管理サーバのアドレスを示すＵＲＬと、
を記録した構成であり、情報処理装置におけるディスク記録コンテンツの利用に際して、前記ＩＣチップからのデータ読み取りを行わせ、スクリプトの実行により前記ＵＲＬによって指定されるサーバに対する前記メディアＩＤの送信処理を行わせる構成としたことを特徴とする。
【００４１】
さらに、本発明のディスクの一実施態様において、前記ＩＣチップは、認証処理を実行する認証処理部を有し、前記認証処理部は、ディスク記録コンテンツの利用を行う情報処理装置との認証処理を行う構成であることを特徴とする。
【００４２】
さらに、本発明のディスクの一実施態様において、前記メディアＩＤはＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）において規定されるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ Ｍｅｄｉａ Ｓｅｒｉａｌ Ｎｕｍｂｅｒ）であることを特徴とする。
【００４３】
さらに、本発明の第３の側面は、
情報処理装置において、ディスク記録コンテンツの利用処理を行う情報処理方法であり、
データ読み取り手段が、ディスクに設けられたＩＣチップからディスクの固有識別子であるメディアＩＤを読み取るデータ読み取りステップと、
コピー許可要求手段が、前記データ読み取り手段において読み取られたメディアＩＤを含むデータを管理サーバに送信するコピー許可要求ステップと、
コピー実行手段が、前記管理サーバからのコピー許可情報の受領を条件として、ディスクに記録されたコンテンツを読み取り、前記ディスク以外のデータ記録手段に対するコピー記録処理を実行するコピー実行ステップと、
を有することを特徴とする情報処理方法にある。
【００４４】
さらに、本発明の情報処理方法の一実施態様において、前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、

（ｂ）ディスク記録コンテンツの識別子であるコンテンツＩＤと、
を記録した構成であり、
前記コピー許可要求ステップは、
前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤとコンテンツＩＤを、前記管理サーバに送信する処理を実行するステップであることを特徴とする。

【００４５】
さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、スクリプト実行手段が、ディスクに記録された簡易プログラムであるスクリプトを実行するスクリプト実行ステップを有し、前記スクリプト実行ステップにおいて実行するプログラムに従って、前記コピー許可要求ステップおよび前記コピー実行ステップの各処理が行われることを特徴とする。

【００４６】
さらに、本発明の情報処理方法の一実施態様において、前記ＩＣチップは、
（ａ）ディスクの固有識別子であるメディアＩＤと、
（ｂ）簡易プログラムであるスクリプトと、
（ｃ）前記管理サーバのアドレスを示すＵＲＬと、
を記録した構成であり、
前記スクリプト実行ステップは、前記データ読み取り手段を介して、前記ＩＣチップから読み取ったスクリプトを実行し、前記コピー許可要求ステップは、前記データ読み取り手段を介して、前記ＩＣチップから読み取ったメディアＩＤを含むデータを、前記ＵＲＬの指定する管理サーバに送信する処理を実行することを特徴とする。

【００４７】
さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、認証処理部が、前記ディスクに設けられたＩＣチップ内に構成された認証処理部との認証処理を行う認証ステップを有し、前記情報処理装置は、前記認証処理の成立を条件としてＩＣチップ内の記録データの利用処理を実行することを特徴とする。

【００４８】
さらに、本発明の情報処理方法の一実施態様において、前記メディアＩＤはＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）において規定されるＰＭＳＮ（Ｐｒｅ－ｒｅｃｏｒｄｅｄ Ｍｅｄｉａ Ｓｅｒｉａｌ Ｎｕｍｂｅｒ）であることを特徴とする。

【００４９】
さらに、本発明の第４の側面は、
情報処理装置において、ディスク記録コンテンツの利用処理を行わせるコンピュータ・プログラムであり、
データ読み取り手段に、ディスクに設けられたＩＣチップからディスクの固有識別子であるメディアＩＤを読み取らせるデータ読み取りステップと、
コピー許可要求手段に、前記データ読み取り手段において読み取られたメディアＩＤを含むデータを管理サーバに送信させるコピー許可要求ステップと、
コピー実行手段に、前記管理サーバからのコピー許可情報の受領を条件として、ディスクに記録されたコンテンツを読み取らせて、前記ディスク以外のデータ記録手段に対するコピー記録処理を実行させるコピー実行ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

【００５０】
なお、本発明のコンピュータ・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汎用コンピュータ・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コンピュータ・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、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。

【００５１】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【発明の効果】
【００５２】
本発明の一実施例の構成によれば、コンテンツの記録されたディスクにディスクの固有識別情報であるメディアＩＤ（ＰＭＳＮ）を記録したＩＣチップを設け、ＩＣチップから読み取ったメディアＩＤをサーバに送信してディスク格納コンテンツのコピー許可情報を取得する構成とした。本構成によれば、例えばＡＡＣＳ規定に従ったコンテンツ記録ディスクにおいてメディアＩＤ（ＰＭＳＮ）の記録されたＢＣＡ領域からＰＭＳＮデータを読み取る処理が省略可能となり、迅速なＩＣチップからのデータ読み取りによってメディアＩＤを取得可能となり、効率的なコピー許可情報取得処理を行うことが可能となる。
【発明を実施するための最良の形態】
【００５３】
以下、図面を参照しながら本発明の情報処理装置、ディスク、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。
以下、本発明の複数の実施例について順次説明する。
【００５４】
［実施例１］
まず、図３、図４を参照して本発明の第１実施例の構成および処理について説明する。図３は、コンテンツを記録したディスク（情報記録媒体）１００の記録データを説明する図である。ディスク１００は、例えば、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクであり、データ記録領域に映画などのコンテンツが記録されている。
【００５５】
ディスク１００は、コンテンツなどを記録したデータ記録領域１１０と、ディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ：Ｐｒｅ－ｒｅｃｏｒｄｅｄ　Ｍｅｄｉａ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）１２１を記録したＢＣＡ領域（バーストカッテイング領域）１２０を有し、さらにＢＣＡ領域１２０に記録されたメディアＩＤと同一のデータであるメディアＩＤ（ＰＭＳＮ）１３１を記録したＩＣチップ１３０が設けられた構成となっている。
【００５６】
ディスク１００は、コンテンツ著作権保護に関する規格であるＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）規格に従って製造されたディスクであり、データ記録領域１１０、およびＢＣＡ領域１２０には、ＡＡＣＡ規格に従ったコンテンツ利用を行うためのデータが記録されている。
【００５７】
ディスク１００のデータ記録領域１１０には以下のデータが記録されている。
ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト１１１、
例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ１１２、
暗号化コンテンツ１１６の復号処理に適用する鍵情報を格納した暗号鍵ブロックであるＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）１１３、
暗号化コンテンツ１１６の識別情報であるコンテンツＩＤ１１４、
ディスク１００の製造単位毎の識別子であるボリュームＩＤ１１５、
例えば映画などのコンテンツを暗号化したデータである暗号化コンテンツ１１６、
以上のデータがデータ記録領域１１０に記録されている。

【００５８】
さらに、ディスク１００のＢＣＡ領域１２０には、
ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）１２１が記録されている。
前述したようにＢＣＡ領域は、通常のデータ記録領域と異なる領域であり、通常のデータ記録方式と異なる物理的なカッティングによってデータが記録される。従ってＢＣＡ領域の記録データは書き換えが困難であり、再生処理においても通常のデータ再生処理とは異なる特殊な読み取り処理が必要となる。
【００５９】
さらに、ディスク１００に設けられたＩＣチップ１３０には、
ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）１３１が記録されている。
このＩＣチップ１３０に記録されたメディアＩＤ（ＰＭＳＮ）１３１と、ＢＣＡ領域１２０に記録されたメディアＩＤ（ＰＭＳＮ）１２１は同一のデータである。
【００６０】
ＩＣチップ１３０は、ＩＣチップ１３０と接触または非接触状態に置かれたリーダライタ（またはリーダ）との通信を行う通信機能を有する例えばＲＦＩＣ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　ＩＣ）と呼ばれるＩＣチップである。ＩＣチップ１３０内のメモリに格納されたメディアＩＤ（ＰＭＳＮ）１３１をリーダライタに対して出力する機能を持つ。このＩＣチップは、リーダライタの出力する電波あるいは磁界をアンテナで受信し、電力に変換してメモリに格納されたメディアＩＤ（ＰＭＳＮ）１３１をリーダライタに対して出力する処理を実行する。
【００６１】
この図３に示すデータ格納構成を持つディスクに格納されたコンテンツの再生処理は、先に図１を参照して説明したＡＡＣＳ規定に従った処理と全く同様の処理として実行可能である。
【００６２】
次に、図４を参照して、図３に示すデータ格納構成を持つディスクに格納されたコンテンツのコピー処理シーケンスについて説明する。すなわち、ディスク記録コンテンツを他のメディア、例えばハードディスクなどの他メディアに対するコピー処理シーケンスである。先に説明したようにＡＡＣＳ規定に従ったディスク記録コンテンツのコピーに際しては、ＡＡＣＳ規定に従って管理サーバからコピー許可情報を得ることが必要となる。この許可に基づくコピー処理はマネージドコピー（Ｍａｎａｇｅｄ　Ｃｏｐｙ）と呼ばれる。
【００６３】
図４には、左からコピー許可情報を出力する管理サーバ１８０、コピー処理を実行する情報処理装置１７０、コピー対象のコンテンツを格納したディスク１００を示している。ディスク１００は、図３を参照して説明したデータ記録構成を持つディスクであり、同一のメディアＩＤ（ＰＭＳＮ）をＢＣＡ領域１２０とＩＣチップ１３０に記録した構成を有する。
【００６４】
情報処理装置１７０は、コンテンツ再生処理やコピー処理を実行するホストとしての機能とディスクの駆動、データ読み取りを行うドライブ機能の双方の機能を持つ装置である。
【００６５】
情報処理装置１７０は、ディスク１００に記録された暗号化コンテンツ１１６を記録メディア１７７、例えば情報処理装置１７０の保有するハードディスクなどの記録メディア１７７にコピーする場合、まず、管理サーバ１８０からコピー許可情報を得るため、ディスク１００に記録されたスクリプト１１１（簡易プログラム）をスクリプト実行部１７１において実行する。
【００６６】
スクリプト１１１には、コピー処理を実行する際の一連の手続きを実行するプログラムが記録されている。情報処理装置１７０のコピー許可要求部１７２は、ディスク１００の

データ記録領域１１０からコンテンツＩＤ１１４を読み取り、さらに、ＩＣチップ１３０に記録されたメディアＩＤ（ＰＭＳＮ）１３１をリーダライタ（Ｒ／Ｗ）１７５を介して読み取り、これらのＩＤ情報を、ディスク１００のデータ記録領域に記録されたＵＲＬ１１２に従って管理サーバ１８０に送信する。

【００６７】

なお、ＩＣチップ１３０から読み取られるメディアＩＤ（ＰＭＳＮ）の転送シーケンスは、図４に示す太線のステップＳ１０１～Ｓ１０３である。本処理例において、メディアＩＤ（ＰＭＳＮ）は、ＩＣチップ１３０から読み取られるので、ＢＣＡ領域１２０からの読み取り処理は省略することができる。ＢＣＡ領域のデータ読み取りは、通常のデータ記録領域１１０と異なる特殊な読み取り処理が必要であるが、本処理例では、このＢＣＡからのデータ読み取りが省略できる。

【００６８】

このようにして、情報処理装置１７０のコピー許可要求部１７２は、コンテンツＩＤ１１４と、ＩＣチップ１３０から読み取ったメディアＩＤ（ＰＭＳＮ）１３１を、ディスク１００のデータ記録領域に記録されたＵＲＬ１１２に従って管理サーバ１８０に送信する。

【００６９】

管理サーバ１８０のコピー許可判定部１８１は、情報処理装置１７０からコンテンツＩＤ１１４と、メディアＩＤ（ＰＭＳＮ）１３１を受信し、コピー対象コンテンツとその記録ディスクを確認し、コピーが許容されるか否かを判定する。管理サーバ１８０は、管理情報として、例えばディスクおよびコンテンツ単位のコピー許容情報などを保持し、この管理情報に基づいてコピーの許可の可否を判定し、コピー可否判定情報を、コピー許可通知部１８２を介して情報処理装置１７０に通知（図４のステップＳ１０４）する。

【００７０】

情報処理装置１７０は、管理サーバ１８０からコピー許可情報を受信すると、コピー実行部１７３において、ディスク１００のデータ記録領域１１０に記録された暗号化コンテンツ１１６を読み取り、情報処理装置１７０の保有するハードディスクなどの記録メディア１７７にコピーする処理を実行する。なお、このコピー処理に際しては、暗号化コンテンツ１１６の復号処理を実行して復号コンテンツとして記録することが可能であり、この場合は、復号処理に必要とする情報、例えば、データ記録領域１１０に記録されたＭＫＢ１１３、ボリュームＩＤ１１５、ＩＣチップ１３０に記録されたメディアＩＤ（ＰＭＳＮ）１３１などを読み取り、これらの読み取りデータを適用してＡＡＣＳ規定に従った復号シーケンスを実行して取得した復号コンテンツを記録メディア１７７に記録する。なお、メディアＩＤ（ＰＭＳＮ）１３１については、コピー許可情報取得処理に際して読み取った情報を情報処理装置１７０内のメモリに記録しておき、この読み取り済み情報を利用することが可能である。

【００７１】

このように、本実施例に従ったコンテンツコピー処理においては、ＢＣＡ領域１２０に記録されたメディアＩＤ（ＰＭＳＮ）１２１の読み取り処理を全く行わないで処理を進行させることが可能となり、管理サーバ１８０からのコピー許可情報の取得を迅速に行うことが可能となる。

【００７２】

なお、ディスク１００は、ＩＣチップ１３０に重複してメディアＩＤ（ＰＭＳＮ）を記録しているが、その他のデータ記録構成はＡＡＣＳ規格に従ったものであり、ＡＡＣＳ規格に従ったコンテンツ再生処理を実行することが可能である。

【００７３】

［実施例２］

次に、図５、図６を参照して本発明の第２実施例の構成および処理について説明する。図５は、コンテンツを記録したディスク（情報記録媒体）２００の記録データを説明する図である。ディスク２００は、例えば、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ

Ｄｉｓｃ）、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクであり、データ記録領域に映画などのコンテンツが記録されている。

【００７４】

ディスク２００は、図３を参照して説明したと実施例１と同様、コンテンツなどを記録したデータ記録領域２１０と、ディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ）２２１を記録したＢＣＡ領域（バーストカッテイング領域）２２０を有し、さらにＢＣＡ領域２２０に記録されたメディアＩＤと同一のデータであるメディアＩＤ（ＰＭＳＮ）２３１を記録したＩＣチップ２３０が設けられた構成となっている。

【００７５】

本実施例では、さらに、ＩＣチップ２３０に、

（ａ）ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト２３２、

（ｂ）例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ２３３、

これらのデータを記録している。

実施例１においては、これらのデータは、データ記録領域に記録していたが、本実施例２では、これらの（ａ），（ｂ）データをデータ記録領域２１０に記録せず、ＩＣチップ２３０に記録している。

【００７６】

ディスク２００のデータ記録領域２１０には以下のデータが記録されている。

暗号化コンテンツ２１４の復号処理に適用する鍵情報を格納した暗号鍵ブロックであるＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）２１１、

暗号化コンテンツ２１４の識別情報であるコンテンツＩＤ２１２、

ディスク２００の製造単位毎の識別子であるボリュームＩＤ２１３、

例えば映画などのコンテンツを暗号化したデータである暗号化コンテンツ２１４、

以上のデータがデータ記録領域２１０に記録されている。

【００７７】

さらに、ディスク２００のＢＣＡ領域２２０には、

ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）２２１が記録されている。

前述したようにＢＣＡ領域は、通常のデータ記録領域と異なる領域であり、通常のデータ記録方式と異なる物理的なカッティングによってデータが記録される。従ってＢＣＡ領域の記録データは書き換えが困難であり、再生処理においても通常のデータ再生処理とは異なる特殊な読み取り処理が必要となる。

【００７８】

さらに、ディスク２００に設けられたＩＣチップ２３０には、前述したように、

ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）２３１、

ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト２３２、

例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ２３３、

これらのデータを記録している。

ＩＣチップ２３０に記録されたメディアＩＤ（ＰＭＳＮ）２３１と、ＢＣＡ領域２２０に記録されたメディアＩＤ（ＰＭＳＮ）２２１は同一のデータである。

【００７９】

この図５に示すデータ格納構成を持つディスクに格納されたコンテンツの再生処理は、先に図１を参照して説明したＡＡＣＳ規定に従った処理と全く同様の処理として実行可能である。

【００８０】

次に、図６を参照して、図５に示すデータ格納構成を持つディスクに格納されたコンテンツのコピー処理シーケンスについて説明する。すなわち、ディスク記録コンテンツを他

のメディア、例えばハードディスクなどの他メディアに対するコピー処理シーケンスである。

【００８１】

図６には、左からコピー許可情報を出力する管理サーバ２８０、コピー処理を実行する情報処理装置２７０、コピー対象のコンテンツを格納したディスク２００を示している。ディスク２００は、図５を参照して説明したデータ記録構成を持つディスクであり、同一のメディアＩＤ（ＰＭＳＮ）をＢＣＡ領域２２０とＩＣチップ２３０に記録した構成を有する。

【００８２】

情報処理装置２７０は、コンテンツ再生処理やコピー処理を実行するホストとしての機能とディスクの駆動、データ読み取りを行うドライブ機能の双方の機能を持つ装置である。

【００８３】

情報処理装置２７０は、ディスク２００に記録された暗号化コンテンツ２１４を記録メディア２７７、例えば情報処理装置２７０の保有するハードディスクなどの記録メディア２７７にコピーする場合、まず、管理サーバ２８０からコピー許可情報を得るため、ディスク２００に記録されたスクリプト（簡易プログラム）２３２をスクリプト実行部２７１において実行する。

【００８４】

本実施例では、スクリプト２３２はＩＣチップ２３０に記録されており、情報処理装置２７０は、リーダライタ（Ｒ／Ｗ）２７５を介してＩＣチップ２３０からスクリプト２３２を取得してスクリプト実行部２７１において実行する。図に示すステップＳ２０１はスクリプト２３２の読み取り処理を示している。

【００８５】

スクリプト２３２には、コピー処理を実行する際の一連の手続きを実行するプログラムが記録されている。情報処理装置２７０のコピー許可要求部２７２は、ディスク２００のデータ記録領域２１０からコンテンツＩＤ２１２を読み取り、さらに、ＩＣチップ２３０に記録されたメディアＩＤ（ＰＭＳＮ）２３１をリーダライタ（Ｒ／Ｗ）２７５を介して読み取る。さらに、ＩＣチップ２３０に記録されたＵＲＬ２３３をリーダライタ（Ｒ／Ｗ）２７５を介して読み取る。図に示すステップＳ２０２はＵＲＬ２３３の読み取り、利用処理を示している。

【００８６】

情報処理装置２７０はＵＲＬ２３３に従って、管理サーバ２８０にコンテンツＩＤ２１２とメディアＩＤ（ＰＭＳＮ）２３１を送信する。図に示すステップＳ２０３はコンテンツＩＤ２１２とメディアＩＤ（ＰＭＳＮ）２３１の送信処理を示している。

【００８７】

本処理例においても、メディアＩＤ（ＰＭＳＮ）は、ＩＣチップ２３０から読み取られるので、ＢＣＡ領域２２０からの読み取り処理は省略することができる。ＢＣＡ領域のデータ読み取りは、通常のデータ記録領域２１０と異なる特殊な読み取り処理が必要であるが、本処理例では、このＢＣＡからのデータ読み取りが省略できる。

【００８８】

このようにして、情報処理装置２７０のコピー許可要求部２７２は、コンテンツＩＤ２１２と、ＩＣチップ２３０から読み取ったメディアＩＤ（ＰＭＳＮ）２３１を、ＩＣチップ２３０から読み取ったＵＲＬ２３３に従って管理サーバ２８０に送信する。

【００８９】

管理サーバ２８０のコピー許可判定部２８１は、情報処理装置２７０からコンテンツＩＤ２１２と、メディアＩＤ（ＰＭＳＮ）２３１を受信し、コピー対象コンテンツとその記録ディスクを確認し、コピーが許容されるか否かを判定し、コピー可否判定情報を、コピー許可通知部２８２を介して情報処理装置２７０に通知（図６のステップＳ２０４）する。

【００９０】
情報処理装置２７０は、管理サーバ２８０からコピー許可情報を受信すると、コピー実行部２７３において、ディスク２００のデータ記録領域２１０に記録された暗号化コンテンツ２１４を読み取り、情報処理装置２７０の保有するハードディスクなどの記録メディア２７７にコピーする処理を実行する。なお、このコピー処理に際しては、暗号化コンテンツ２１６の復号処理を実行して復号コンテンツとして記録することが可能であり、この場合は、復号処理に必要とする情報、例えば、データ記録領域２１０に記録されたＭＫＢ２１１、ボリュームＩＤ２１３、ＩＣチップ２３０に記録されたメディアＩＤ（ＰＭＳＮ）２３１などを読み取り、これらの読み取りデータを適用してＡＡＣＳ規定に従った復号シーケンスを実行して取得した復号コンテンツを記録メディア２７７に記録する。なお、メディアＩＤ（ＰＭＳＮ）２３１については、コピー許可情報取得処理に際して読み取った情報を情報処理装置２７０内のメモリに記録しておき、この読み取り済み情報を利用することが可能である。
【００９１】
このように、本実施例に従ったコンテンツコピー処理においても、実施例１と同様ＢＣＡ領域２２０に記録されたメディアＩＤ（ＰＭＳＮ）２２１の読み取り処理を全く行わないで処理を進行させることが可能となり、管理サーバ２８０からのコピー許可情報の取得を迅速に行うことが可能となる。
【００９２】
また、本実施例では、ＩＣチップ２３０に、
（ａ）ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト２３２、
（ｂ）例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ２３３、
これらのデータを記録した構成としているが、ＩＣチップ２３０は、データの記録消去が可能な構成であるため、サーバ接続処理方法などを規定したスクリプトや接続サキサーバを規定したＵＲＬの書き換えが必要となった場合にデータの再書き込みによるデータ変更が可能であるというメリットがある。
【００９３】
従来型のＡＡＣＳ規定のディスクでは、スクリプトやＵＲＬはデータ記録領域に記録され、ディスクがデータ再記録のできないＲＯＭディスクのような場合には、一度記録されたデータの変更ができないという問題があったが、本例のようにＩＣチップにスクリプトやＵＲＬを書き込む構成とすることで、スクリプトの変更があった場合や接続先サーバのＵＲＬの変更があった場合など、任意のタイミングにおいてデータの書き換えが可能となる。
【００９４】
［実施例３］
次に、図７、図８を参照して本発明の第３実施例の構成および処理について説明する。図７は、コンテンツを記録したディスク（情報記録媒体）３００の記録データを説明する図である。ディスク３００は、例えば、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクであり、データ記録領域に映画などのコンテンツが記録されている。
【００９５】
ディスク３００は、図３を参照して説明したと実施例１と同様、コンテンツなどを記録したデータ記録領域３１０と、ディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ）３２１を記録したＢＣＡ領域（バーストカッテイング領域）３２０を有し、さらにＢＣＡ領域３２０に記録されたメディアＩＤと同一のデータであるメディアＩＤ（ＰＭＳＮ）３３１を記録したＩＣチップ３３０が設けられた構成となっている。
【００９６】
本実施例では、さらに、ＩＣチップ３３０に、

暗号化コンテンツ３１５の識別情報であるコンテンツＩＤ３３２を記録している。
実施例１においては、コンテンツＩＤは、データ記録領域に記録していたが、本実施例３では、このデータをデータ記録領域３１０に記録せず、ＩＣチップ３３０に記録している。

【００９７】
ディスク３００のデータ記録領域３１０には以下のデータが記録されている。
ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト３１１、
例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ３１２、
暗号化コンテンツ３１５の復号処理に適用する鍵情報を格納した暗号鍵ブロックであるＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）３１３、
ディスク３００の製造単位毎の識別子であるボリュームＩＤ３１４、
例えば映画などのコンテンツを暗号化したデータである暗号化コンテンツ３１５、
以上のデータがデータ記録領域３１０に記録されている。

【００９８】
さらに、ディスク３００のＢＣＡ領域３２０には、
ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）３２１が記録されている。
前述したようにＢＣＡ領域は、通常のデータ記録領域と異なる領域であり、通常のデータ記録方式と異なる物理的なカッティングによってデータが記録される。従ってＢＣＡ領域の記録データは書き換えが困難であり、再生処理においても通常のデータ再生処理とは異なる特殊な読み取り処理が必要となる。

【００９９】
さらに、ディスク３００に設けられたＩＣチップ３３０には、前述したように、
ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）３３１、
暗号化コンテンツ３１５の識別情報であるコンテンツＩＤ３３２、
これらのデータを記録している。
ＩＣチップ３３０に記録されたメディアＩＤ（ＰＭＳＮ）３３１と、ＢＣＡ領域３２０に記録されたメディアＩＤ（ＰＭＳＮ）３２１は同一のデータである。

【０１００】
この図７に示すデータ格納構成を持つディスクに格納されたコンテンツの再生処理は、先に図１を参照して説明したＡＡＣＳ規定に従った処理と全く同様の処理として実行可能である。

【０１０１】
次に、図８を参照して、図７に示すデータ格納構成を持つディスクに格納されたコンテンツのコピー処理シーケンスについて説明する。すなわち、ディスク記録コンテンツを他のメディア、例えばハードディスクなどの他メディアに対するコピー処理シーケンスである。

【０１０２】
図８には、左からコピー許可情報を出力する管理サーバ３８０、コピー処理を実行する情報処理装置３７０、コピー対象のコンテンツを格納したディスク３００を示している。ディスク３００は、図７を参照して説明したデータ記録構成を持つディスクであり、同一のメディアＩＤ（ＰＭＳＮ）をＢＣＡ領域３２０とＩＣチップ３３０に記録した構成を有する。

【０１０３】
情報処理装置３７０は、コンテンツ再生処理やコピー処理を実行するホストとしての機能とディスクの駆動、データ読み取りを行うドライブ機能の双方の機能を持つ装置である。

【０１０４】
情報処理装置３７０は、ディスク３００に記録された暗号化コンテンツ３１５を記録メ

ディア３７７、例えば情報処理装置３７０の保有するハードディスクなどの記録メディア３７７にコピーする場合、まず、管理サーバ３８０からコピー許可情報を得るため、ディスク３００に記録されたスクリプト（簡易プログラム）３１１をスクリプト実行部３７１において実行する。

【０１０５】

スクリプト３１１には、コピー処理を実行する際の一連の手続きを実行するプログラムが記録されている。情報処理装置３７０のコピー許可要求部３７２は、ＩＣチップ１３０に記録されたメディアＩＤ（ＰＭＳＮ）３３１と、コンテンツＩＤ３３２をリーダライタ（Ｒ／Ｗ）３７５を介して読み取る。図に示すステップＳ３０１，Ｓ３０２はＩＣチップ１３０に記録されたメディアＩＤ（ＰＭＳＮ）３３１と、コンテンツＩＤ３３２をリーダライタ（Ｒ／Ｗ）３７５を介して読み取る処理を示している。

【０１０６】

情報処理装置３７０のコピー許可要求部３７２は、データ記録領域３１０に記録されたＵＲＬ３１２に従って、管理サーバ３８０にコンテンツＩＤ３３２とメディアＩＤ（ＰＭＳＮ）３３１を送信する。図に示すステップＳ３０３はコンテンツＩＤ３３２とメディアＩＤ（ＰＭＳＮ）３３１の送信処理を示している。

【０１０７】

本処理例においては、メディアＩＤ（ＰＭＳＮ）のみならずコンテンツＩＤもＩＣチップ３３０から読み取る構成であり、ＢＣＡ領域２２０からの読み取り処理が省略され、データ記録領域からのデータ読み取り処理時間も削減可能となる。

【０１０８】

このようにして、情報処理装置３７０のコピー許可要求部３７２は、コンテンツＩＤ３３２と、ＩＣチップ３３０から読み取ったメディアＩＤ（ＰＭＳＮ）３３１を、ＵＲＬ３１２に従って管理サーバ３８０に送信する。

【０１０９】

管理サーバ２８０のコピー許可判定部３８１は、情報処理装置３７０からコンテンツＩＤ３３２と、メディアＩＤ（ＰＭＳＮ）３３１を受信し、コピー対象コンテンツとその記録ディスクを確認し、コピーが許容されるか否かを判定し、コピー可否判定情報を、コピー許可通知部３８２を介して情報処理装置３７０に通知（図６のステップＳ３０４）する。

【０１１０】

情報処理装置３７０は、管理サーバ３８０からコピー許可情報を受信すると、コピー実行部３７３において、ディスク３００のデータ記録領域３１０に記録された暗号化コンテンツ３１５を読み取り、情報処理装置３７０の保有するハードディスクなどの記録メディア３７７にコピーする処理を実行する。なお、このコピー処理に際しては、暗号化コンテンツ３１６の復号処理を実行して復号コンテンツとして記録することが可能であり、この場合は、復号処理に必要とする情報、例えば、データ記録領域３１０に記録されたＭＫＢ３１３、ボリュームＩＤ３１４、ＩＣチップ３３０に記録されたメディアＩＤ（ＰＭＳＮ）３３１などを読み取り、これらの読み取りデータを適用してＡＡＣＳ規定に従った復号シーケンスを実行して取得した復号コンテンツを記録メディア３７７に記録する。なお、メディアＩＤ（ＰＭＳＮ）３３１については、コピー許可情報取得処理に際して読み取った情報を情報処理装置３７０内のメモリに記録しておき、この読み取り済み情報を利用することが可能である。

【０１１１】

このように、本実施例に従ったコンテンツコピー処理においても、実施例１，２と同様ＢＣＡ領域３２０に記録されたメディアＩＤ（ＰＭＳＮ）３２１の読み取り処理を全く行わないで処理を進行させることが可能となり、管理サーバ３８０からのコピー許可情報の取得を迅速に行うことが可能となる。

【０１１２】

また、本実施例では、ＩＣチップ３３０に、

暗号化コンテンツ３１５の識別情報であるコンテンツＩＤ３３２を記録した構成としており、ＢＣＡ領域２２０からの読み取り処理が省略可能となるとともにデータ記録領域からのデータ読み取り処理時間も削減できる。

【０１１３】

なお、実施例２では、ＩＣチップにメディアＩＤに加えて、

スクリプトと、ＵＲＬを記録した構成を説明し、

実施例３では、ＩＣチップにメディアＩＤに加えて、

コンテンツＩＤを記録した構成について説明したが、これらの実施例２，３を併せて、ＩＣチップに、メディアＩＤに加えて、

スクリプトと、ＵＲＬと、コンテンツＩＤを記録した構成としてもよい。この構成によれば、コピー許可情報の取得処理に際してディスクのデータ記録領域のデータ読み取りを省略することが可能となる。

【０１１４】

［実施例４］

次に、図９、図１０を参照して本発明の第４実施例の構成および処理について説明する。図９は、コンテンツを記録したディスク（情報記録媒体）４００の記録データを説明する図である。ディスク４００は、例えば、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクであり、データ記録領域に映画などのコンテンツが記録されている。

【０１１５】

ディスク４００は、図３を参照して説明したと実施例１と同様、コンテンツなどを記録したデータ記録領域４１０と、ディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ）４２１を記録したＢＣＡ領域（バーストカッテイング領域）４２０を有し、さらにＢＣＡ領域４２０に記録されたメディアＩＤと同一のデータであるメディアＩＤ（ＰＭＳＮ）４３１を記録したＩＣチップ４３０が設けられた構成となっている。

【０１１６】

本実施例では、さらに、ＩＣチップ４３０に、

（ａ）ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト４３２、

（ｂ）例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ４３３、

（ｃ）暗号化コンテンツ４１３の識別情報であるコンテンツＩＤ４３４、

（ｄ）認証用データ４３５、

（ｅ）認証処理部４３６、

これらのデータおよび機能を有している。

【０１１７】

ディスク４００のデータ記録領域４１０には以下のデータが記録されている。

暗号化コンテンツ４１３の復号処理に適用する鍵情報を格納した暗号鍵ブロックであるＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）４１１、

ディスク４００の製造単位毎の識別子であるボリュームＩＤ４１２、

例えば映画などのコンテンツを暗号化したデータである暗号化コンテンツ４１３、

以上のデータがデータ記録領域４１０に記録されている。

【０１１８】

さらに、ディスク４００のＢＣＡ領域４２０には、

ディスク固有の識別情報であるメディアＩＤ（ＰＭＳＮ）４２１が記録されている。

前述したようにＢＣＡ領域は、通常のデータ記録領域と異なる領域であり、通常のデータ記録方式と異なる物理的なカッティングによってデータが記録される。従ってＢＣＡ領域の記録データは書き換えが困難であり、再生処理においても通常のデータ再生処理とは異なる特殊な読み取り処理が必要となる。

【０１１９】

この図９に示すデータ格納構成を持つディスクを利用した認証処理シーケンスについて、図１０を参照して説明する。例えば図９に示すデータ格納構成を持つディスクに格納されたコンテンツのコピー処理、すなわち、ディスク記録コンテンツを他のメディア、例えばハードディスクなどの他メディアに対するコピー処理を行う場合、前述した実施例において説明したように、管理サーバと接続してコピー許可情報を取得する処理が必要となる。

【０１２０】

この管理サーバと接続して通信を実行する場合、管理サーバ４８０、情報処理装置４７０、ディスク４００、これら各々の正当性を確認するといった処理、すなわち認証処理を行って正当性が確認された場合に、処理を行うことが好ましい。

【０１２１】

例えば、

管理サーバ４８０と、ＩＣチップ４３０間の認証処理、

ＩＣチップ４３０の認証処理部４３６と情報処理装置４７０の認証処理部４７９との間での認証処理、

情報処理装置４７０の認証処理部４７９と、管理サーバ４８０の認証処理部４８６との間での認証処理、

これらの各部間の少なくともいずれかの認証処理を実行して、認証が成立したことを条件としてコピー許可情報の送信を行うといった設定とすることが可能である。

【０１２２】

情報処理装置４７０は認証処理部４７９と認証用データ４７８を備えており、これらのデータを適用した認証が可能な構成であり、ＩＣチップ４３０も、認証処理部４３６と認証用データ４３５を備えており、これらのデータを適用した認証が可能な構成となっている。

【０１２３】

例えば、情報処理装置４７０の認証処理部４７９は、ディスク４００に設けられたＩＣチップ４３０内に構成された認証処理部４３５との認証処理を行い、認証処理の成立を条件としてＩＣチップ４３０内の記録データの利用処理を実行するといった処理が可能となる。

【０１２４】

また、管理サーバ４８０と、ＩＣチップ４３０間の認証処理も可能であり、この場合、情報処理装置４７０の認証処理部４７９を介した処理が行われる。認証処理を実行して双方の正当性を確認し、暗号鍵の共有処理を行って通信データを共有した暗号鍵で暗号化して送受信することでセキュリティレベルの高い通信が可能となりデータ漏洩の可能性を低減した安全なデータ通信が可能となる。

【０１２５】

ＩＣチップ４３０には認証処理に必要なデータ、例えば、ＡＡＣＳ管理センタの公開鍵、ＩＣチップ４３０に対応して設定された公開鍵，秘密鍵などを含む認証用データ４３５が記録されており、ＩＣチップ４３０内の認証処理部４３５はこの認証用データ４３５を利用して管理サーバ４８０の認証処理部４８６との間で、情報処理装置４７０を介して通信を実行して認証処理を行う。この場合、情報処理装置４７０のリーダライタ（Ｒ／Ｗ）４７５、認証処理部４７９を介して通信が実行される。図に示すステップＳ４０１，Ｓ４０２のラインが認証処理時の通信を示している。管理サーバ４８０にも認証用データ４８５が格納され、この認証用データを利用して認証処理が実行される。

【０１２６】

この認証処理が完了し、管理サーバ４８０と、ＩＣチップ４３０の双方の正当性が確認された後、先の実施例で説明したコピー許可情報取得処理が行われることになる。認証処理において共有した暗号鍵を利用して通信データを暗号化することでセキュリティレベルの高い通信が可能となりデータ漏洩の可能性を低減した安全なデータ通信が可能となる。

【０１２７】

本実施例では、ＩＣチップ４３０に、メディアＩＤ（ＰＭＳＮ）４３１に加えて、スクリプト４３２と、ＵＲＬ４３３と、コンテンツＩＤ４３４を記録した構成であり、この構成によれば、コピー許可情報の取得処理に際してディスクのデータ記録領域のデータ読み取りを省略することが可能となる。

【０１２８】

なお、上述の説明では、管理サーバ４８０と、ＩＣチップ４３０間の認証を行う処理例を説明したが、ＩＣチップ４３０の認証処理部４３６と、情報処理装置４７０の認証処理部４７９との間で認証を実行し、さらに、情報処理装置４７０の認証処理部４７９と、管理サーバ４８０の認証処理部４８６との間で認証を実行してすべての認証が成立したことを条件としてコピー許可情報の送信を行うといった設定としてもよい。情報処理装置４７０も認証用データ４７８を備えており、これらのデータを適用した認証が可能な構成となっている。

【０１２９】

［実施例５］

次に、図１１、図１２、図１３を参照して本発明の第５実施例の構成および処理について説明する。図１１は、コンテンツを記録したディスク（情報記録媒体）５００の記録データを説明する図である。ディスク５００は、例えば、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクであり、データ記録領域に映画などのコンテンツが記録されている。

【０１３０】

ディスク５００は、実施例１～４において説明した構成と異なり、ＢＣＡ領域（バーストカッテイング領域）５２０にディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ）が記録されていない構成となっている。図にはＢＣＡ領域５２０を示しているが、本実施例では、ＢＣＡ領域自体が省略された構成であってもよい。

【０１３１】

ディスク５００は、コンテンツなどを記録したデータ記録領域５１０と、ディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ）５３１などを記録したＩＣチップ５３０が設けられた構成となっている。

【０１３２】

本実施例では、ＩＣチップ２３０には、

（ａ）ディスク固有の識別情報であるメディアＩＤ（例えばＰＭＳＮ）５３１、

（ｂ）ＡＡＣＳ規定に従った再生やコピー処理を実行させるための簡易プログラムであるスクリプト５３２、

（ｃ）例えばディスク格納コンテンツのコピー処理に際してコピー処理の許可を得るために接続するサーバのＵＲＬ５３３、

（ｄ）暗号化コンテンツ５１３の識別情報であるコンテンツＩＤ５３４、

これらのデータを記録している。

【０１３３】

ディスク５００のデータ記録領域５１０には以下のデータが記録されている。

暗号化コンテンツ５１３の復号処理に適用する鍵情報を格納した暗号鍵ブロックであるＭＫＢ（Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）５１１、

ディスク２００の製造単位毎の識別子であるボリュームＩＤ５１２、

例えば映画などのコンテンツを暗号化したデータである暗号化コンテンツ５１３、

以上のデータがデータ記録領域５１０に記録されている。

【０１３４】

この図１１に示すデータ格納構成を持つディスクに格納されたコンテンツの再生処理シーケンスについて、図１２を参照して説明する。図１２には、左からコンテンツを格納したディスク５００、ディスク５００を装着してディスクからのデータ読み取りを実行するドライブ５５０、ドライブ５５０を介してディスク５００の記録データを取得してコンテンツの復号、再生を行うホスト５６０を示している。なお、図はドライブ５５０とホスト

５６０を別構成として示してあるが、ドライブとホストは１つの装置、例えば再生装置などの一体となった構成である場合もある。左端のディスク（情報記録媒体）５００は、図１１を参照して説明したデータ記録構成を持つディスクである。

【０１３５】

ドライブ５５０は、ＡＡＣＳ管理センタの公開鍵と、ドライブ公開鍵とドライブ秘密鍵を含む鍵データ５５１、ホストリボケーションリスト５５２を有する。ホストリボケーションリスト５５２は、ＡＡＣＳの管理センタが不正なホストであると判定したホストの識別情報を記録したリスト、すなわちブラックリストである。例えばホストの識別情報としてホストに対応するホスト公開鍵証明書の識別番号が記録される。ホストリボケーションリスト５５２は改ざんがなされないようにＡＡＣＳ管理センタの秘密鍵による署名が付与されている。

【０１３６】

ホスト５６０は、ＡＡＣＳ管理センタの公開鍵と、ホスト公開鍵とホスト秘密鍵を含む鍵データ５６１、ドライブリボケーションリスト５６２を有する。ドライブリボケーションリスト５６２は、ＡＡＣＳ管理センタが不正なドライブ装置であると判定したドライブの識別情報を記録したリスト、すなわちブラックリストである。例えばドライブの識別情報としてドライブに対応するドライブ公開鍵証明書の識別番号が記録される。ドライブリボケーションリスト５６２も改ざんがなされないようにＡＡＣＳ管理センタの秘密鍵による署名が付与されている。なお、ホストリボケーションリスト５５２や、ドライブリボケーションリスト５６２は、ディスク５００に記録して、ドライブ５５０およびホスト５６０は、ディスク５００に記録されたデータを読み取って利用する構成としてもよい。

【０１３７】

ホスト５６０がコンテンツの再生を行なう場合のシーケンスについて説明する。ホスト５６０とドライブ５５０は、まず、ホスト５６０の認証処理部５６３とドライブ５５０の認証処理部５５３との間で認証処理を実行する。この認証処理はＡＡＣＳの規定する処理シーケンスに従って実行される。この処理において各装置の実行する主な処理は以下の通りである。

【０１３８】

ドライブ５５０は、ホストリボケーションリスト５５２を読み取り、ＡＡＣＳ管理センタ公開鍵を適用してホストリボケーションリスト５５２の署名検証を行なって改ざんのないことを確認し、ホストリボケーションリスト５５２にホスト５６０の識別情報が記載されていないこと、すなわち、ホスト５６０がリボークされていないことを確認する。

【０１３９】

ホスト５６０においても、ドライブリボケーションリスト５６２を読み取り、ＡＡＣＳ管理センタ公開鍵を適用してドライブリボケーションリスト５６２の署名検証を行なって改ざんのないことを確認し、ドライブリボケーションリスト５６２にドライブ５５０の識別情報が記載されていないこと、すなわち、ドライブ５５０がリボークされていないことを確認する。

【０１４０】

ドライブ５５０とホスト５６０の両者ともリボークされていないことが確認された場合は、ドライブ５５０とホスト５６０間で、ＡＡＣＳ規定に従った暗号データの通信を実行して、共有秘密鍵を生成してドライブ５５０とホスト５６０で共有する。

【０１４１】

このホストとドライブ間の認証が完了すると、ドライブ５５０は、ディスク５００からボリュームＩＤ５１２とメディアＩＤ（ＰＭＳＮ）５３１を読み取る。本実施例において、メディアＩＤ（ＰＭＳＮ）５３１は、ディスク５００に埋め込まれたＩＣチップ５３０に記録されており、ドライブ５５０は、リーダライタ５５５によって、ディスク５００のＩＣチップ５３０からメディアＩＤ（ＰＭＳＮ）５３１を読み取る。

【０１４２】

ドライブ５５０は、ディスクからの読み取りデータを利用してＭＡＣ算出部５５４にお

いて認証処理に際して生成した共有鍵を適用したＭＡＣ生成処理を実行して、生成ＭＡＣ値と、メディアＩＤ（ＰＭＳＮ）５３１をホスト５６０に送信する。

【０１４３】

ホスト５６０のＭＡＣ算出部５５４は、共有鍵を適用したＭＡＣ検証処理を実行する。すなわち、ドライブ５５０から受信したメディアＩＤに対して認証処理に際して生成した共有鍵を適用したＭＡＣ生成処理を行い、生成ＭＡＣ値とドライブ５５０から受信したＭＡＣ値とを照合する。２つのＭＡＣ値が一致した場合に、検証成立と判断し、暗号処理モジュール５６６においてコンテンツ復号、再生処理を実行する。

【０１４４】

暗号処理モジュール５６６において実行するコンテンツ復号においては、デバイスキー［Ｋｄ］５６５を適用したＭＫＢ５１１の処理により、ＭＫＢ５１１からメディアキー［Ｋｍ］を取得し、メディアキー［Ｋｍ］を適用した処理によって、コンテンツの復号用の鍵を取得してコンテンツ復号処理が実行されることになる。

【０１４５】

次に、図１３を参照して、図１１に示すデータ格納構成を持つディスクに格納されたコンテンツのコピー処理シーケンスについて説明する。すなわち、ディスク記録コンテンツを他のメディア、例えばハードディスクなどの他メディアに対するコピー処理シーケンスである。

【０１４６】

図１３には、左からコピー許可情報を出力する管理サーバ５８０、コピー処理を実行する情報処理装置５７０、コピー対象のコンテンツを格納したディスク５００を示している。ディスク５００は、図１１を参照して説明したデータ記録構成を持つディスクであり、メディアＩＤ（ＰＭＳＮ）をＩＣチップ５３０のみに記録した構成を有する。

【０１４７】

情報処理装置５７０は、コンテンツ再生処理やコピー処理を実行するホストとしての機能とディスクの駆動、データ読み取りを行うドライブ機能の双方の機能を持つ装置である。

【０１４８】

情報処理装置５７０は、ディスク５００に記録された暗号化コンテンツ５１３を記録メディア５７７、例えば情報処理装置５７０の保有するハードディスクなどの記録メディア５７７にコピーする場合、まず、管理サーバ５８０からコピー許可情報を得るため、ディスク５００のＩＣチップ５３０に記録されたスクリプト（簡易プログラム）５３２をリーダライタ（Ｒ／Ｗ）２７５を介して読み取りスクリプト実行部５７１において実行する。

【０１４９】

本実施例では、スクリプト５３２はＩＣチップ５３０に記録されており、情報処理装置５７０は、リーダライタ（Ｒ／Ｗ）５７５を介してＩＣチップ５３０からスクリプト５３２を取得してスクリプト実行部５７１において実行する。図に示すステップＳ５０１はスクリプト５３２の読み取り処理を示している。

【０１５０】

スクリプト５３２には、コピー処理を実行する際の一連の手続きを実行するプログラムが記録されている。情報処理装置５７０のコピー許可要求部５７２は、ディスク５００のＩＣチップ５３０に記録されたコンテンツＩＤ２１２と、メディアＩＤ（ＰＭＳＮ）５３１をリーダライタ（Ｒ／Ｗ）５７５を介して読み取る。さらに、ＩＣチップ５３０に記録されたＵＲＬ５３３をリーダライタ（Ｒ／Ｗ）５７５を介して読み取る。図に示すステップＳ５０２はＵＲＬ５３３の読み取り、利用処理を示している。

【０１５１】

情報処理装置５７０はＵＲＬ５３３に従って、管理サーバ５８０にコンテンツＩＤ５３４とメディアＩＤ（ＰＭＳＮ）５３１を送信する。図に示すステップＳ５０３はコンテンツＩＤ５３４とメディアＩＤ（ＰＭＳＮ）５３１の送信処理を示している。

【０１５２】

本処理例においては、
スクリプト５３２、ＵＲＬ５３３、さらに、
コンテンツＩＤ５３４とメディアＩＤ（ＰＭＳＮ）５３１、
これらのデータのすべてがＩＣチップ５３０から読み取られるので、ＢＣＡ領域やデータ記録領域からの読み取り処理を行うことなく、コピー許可情報の取得処理が可能となる。

【０１５３】
このようにして、情報処理装置５７０のコピー許可要求部５７２は、ＩＣチップ５３０から読み取ったコンテンツＩＤ５３４と、メディアＩＤ（ＰＭＳＮ）５３１を、ＩＣチップ５３０から読み取ったＵＲＬ５３３に従って管理サーバ５８０に送信する。

【０１５４】
管理サーバ５８０のコピー許可判定部５８１は、情報処理装置５７０からコンテンツＩＤ５３４と、メディアＩＤ（ＰＭＳＮ）５３１を受信し、コピー対象コンテンツとその記録ディスクを確認し、コピーが許容されるか否かを判定し、コピー可否判定情報を、コピー許可通知部５８２を介して情報処理装置５７０に通知（図１３のステップＳ５０４）する。

【０１５５】
情報処理装置５７０は、管理サーバ５８０からコピー許可情報を受信すると、コピー実行部５７３において、ディスク５００のデータ記録領域５１０に記録された暗号化コンテンツ５１３を読み取り、情報処理装置５７０の保有するハードディスクなどの記録メディア５７７にコピーする処理を実行する。なお、このコピー処理に際しては、暗号化コンテンツ５１３の復号処理を実行して復号コンテンツとして記録することが可能であり、この場合は、復号処理に必要とする情報、例えば、データ記録領域５１０に記録されたＭＫＢ５１１、ボリュームＩＤ５１２、ＩＣチップ５３０に記録されたメディアＩＤ（ＰＭＳＮ）５３１などを読み取り、これらの読み取りデータを適用してＡＡＣＳ規定に従った復号シーケンスを実行して取得した復号コンテンツを記録メディア５７７に記録する。なお、メディアＩＤ（ＰＭＳＮ）５３１については、コピー許可情報取得処理に際して読み取った情報を情報処理装置５７０内のメモリに記録しておき、この読み取り済み情報を利用することが可能である。

【０１５６】
このように、本実施例に従ったコンテンツコピー処理においては、スクリプト５３２、ＵＲＬ５３３、さらに、コンテンツＩＤ５３４とメディアＩＤ（ＰＭＳＮ）５３１、これらのデータのすべてがＩＣチップ５３０から読み取られるので、ＢＣＡ領域やデータ記録領域からの読み取り処理を行うことなく、コピー許可情報の取得処理が可能となり、コピー許可情報の取得を迅速に行うことが可能となる。

【０１５７】
また、本実施例では、ＩＣチップに、スクリプト５３２、ＵＲＬ５３３を記録した構成としており、サーバ接続処理方法などを規定したスクリプトや接続サキサーバを規定したＵＲＬの書き換えが必要となった場合にデータの再書き込みによるデータ変更が可能となり、任意のタイミングにおいてデータの書き換えが可能となる。

【０１５８】
なお、ＡＡＣＳ規定によれば、メディアＩＤ（ＰＭＳＮ）はディスクに記録されていることが必要であり、現状の規定ではＢＣＡ領域に記録する設定となっている。従って本実施例５の構成は現状のＡＡＣＳ規定に従った構成ではない。ただし、メディアＩＤ（ＰＭＳＮ）を記録したＩＣチップを埋め込んだディスクを製造し、ＡＡＣＳ規定に従ったディスクに設定する必要がある場合にのみ、ＩＣチップ内に記録済みのメディアＩＤ（ＰＭＳＮ）を後発的にＢＣＡ領域に書き込むといった処理を行ってＡＡＣＳ規定に従ったディスクとしてユーザに提供することも可能である。

【０１５９】
以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本

発明の要旨を逸脱しない範囲で当業者が実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

【０１６０】

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。

【０１６１】

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】

【０１６２】

以上、説明したように、本発明の一実施例の構成によれば、コンテンツの記録されたディスクにディスクの固有識別情報であるメディアＩＤ（ＰＭＳＮ）を記録したＩＣチップを設け、ＩＣチップから読み取ったメディアＩＤをサーバに送信してディスク格納コンテンツのコピー許可情報を取得する構成とした。本構成によれば、例えばＡＡＣＳ規定に従ったコンテンツ記録ディスクにおいてメディアＩＤ（ＰＭＳＮ）の記録されたＢＣＡ領域からＰＭＳＮデータを読み取る処理が省略可能となり、迅速なＩＣチップからのデータ読み取りによってメディアＩＤを取得可能となり、効率的なコピー許可情報取得処理を行うことが可能となる。

【図面の簡単な説明】

【０１６３】

【図１】ＡＡＣＳ規定に従ったディスク記録コンテンツの再生シーケンスについて説明する図である。

【図２】ＡＡＣＳ規定に従ったディスク記録コンテンツのコピーシーケンスについて説明する図である。

【図３】本発明の第１実施例に従ったディスクのデータ記録構成例について説明する図である。

【図４】本発明の第１実施例に従ったディスク記録コンテンツのコピーシーケンスについて説明する図である。

【図５】本発明の第２実施例に従ったディスクのデータ記録構成例について説明する図である。

【図６】本発明の第２実施例に従ったディスク記録コンテンツのコピーシーケンスについて説明する図である。

【図７】本発明の第３実施例に従ったディスクのデータ記録構成例について説明する図である。

【図８】本発明の第３実施例に従ったディスク記録コンテンツのコピーシーケンスについて説明する図である。

【図９】本発明の第４実施例に従ったディスクのデータ記録構成例について説明する図である。

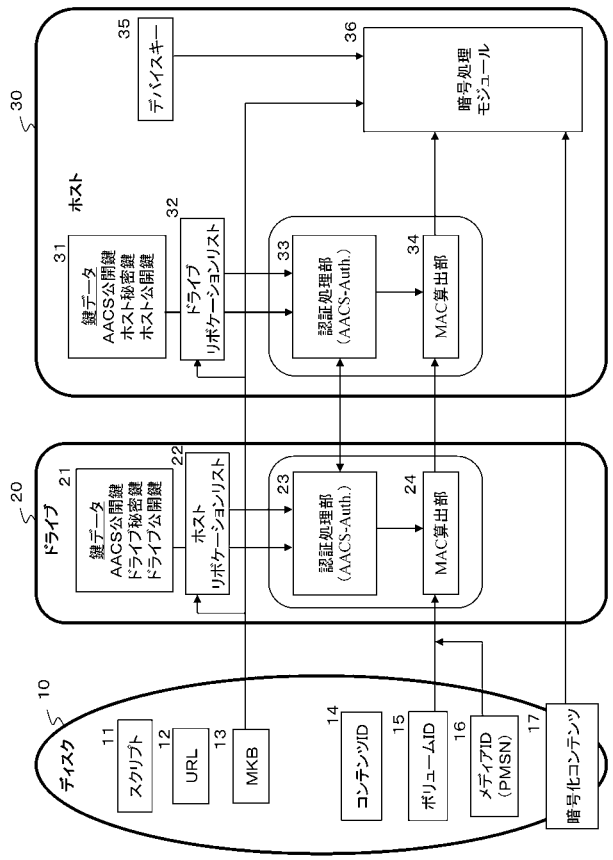
【図１０】本発明の第４実施例に従った認証シーケンスについて説明する図である。

【図１１】本発明の第５実施例に従ったディスクのデータ記録構成例について説明する図

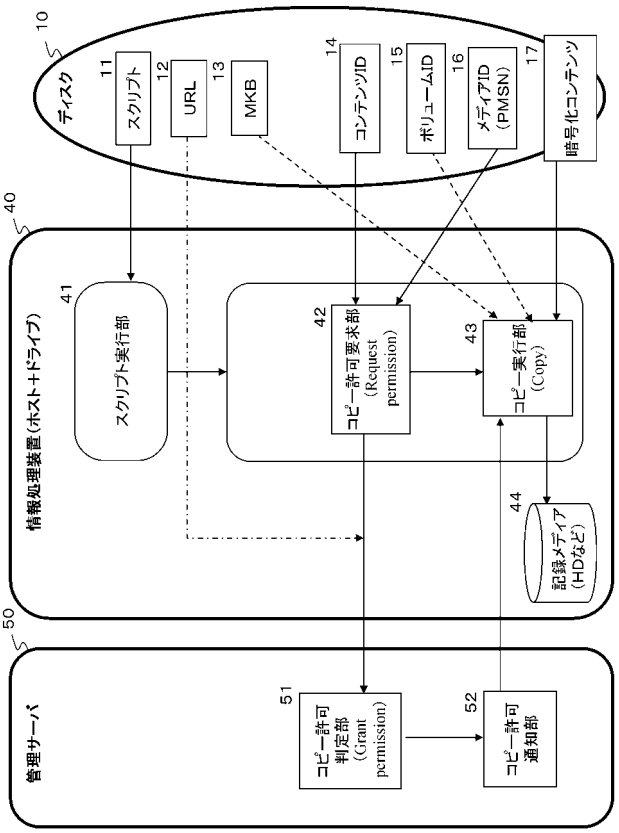
である。
【図１２】本発明の第５実施例に従ったディスク記録コンテンツの再生シーケンスについて説明する図である。
【図１３】本発明の第５実施例に従ったディスク記録コンテンツのコピーシーケンスについて説明する図である。
【符号の説明】
【０１６４】
１０・・・ディスク（情報記録媒体）、１１・・・スクリプト、１２・・・ＵＲＬ、１３・・・ＭＫＢ、１４・・・コンテンツＩＤ、１５・・・ボリュームＩＤ、１６・・・メディアＩＤ（ＰＭＳＮ）、１７・・・暗号化コンテンツ、２０・・・ドライブ、２１・・・鍵データ、２２・・・ホストリボケーションリスト、２３・・・認証処理部、２４・・・ＭＡＣ算出部、３０・・・ホスト、３１・・・鍵データ、３２・・・ドライブリボケーションリスト、３３・・・認証処理部、３４・・・ＭＡＣ算出部、３５・・・デジイスキー、３６・・・暗号処理モジュール、４０・・・情報処理装置、４１・・・スクリプト実行部、４２・・・コピー許可要求部、４３・・・コピー実行部、４４・・・記録メディア、５０・・・管理サーバ、５１・・・コピー許可判定部、５２・・・コピー許可通知部、１００・・・ディスク、１１０・・・データ記録領域、１１１・・・スクリプト、１１２・・・ＵＲＬ、１１３・・・ＭＫＢ、１１４・・・コンテンツＩＤ、１１５・・・ボリュームＩＤ、１１６・・・暗号化コンテンツ、１２０・・・ＢＣＡ領域、１２１・・・メディアＩＤ（ＰＭＳＮ）、１３０・・・ＩＣチップ、１３１・・・メディアＩＤ（ＰＭＳＮ）、１７０・・・情報処理装置、１７１・・・スクリプト実行部、１７２・・・コピー許可要求部、１７３・・・コピー実行部、１７５・・・リーダライタ（Ｒ／Ｗ）、１７７・・・記録メディア、１８０・・・管理サーバ、１８１・・・コピー許可判定部、１８２・・・コピー許可通知部、２００・・・ディスク、２１０・・・データ記録領域、２１１・・・ＭＫＢ、２１２・・・コンテンツＩＤ、２１３・・・ボリュームＩＤ、２１４・・・暗号化コンテンツ、２２０・・・ＢＣＡ領域、２２１・・・メディアＩＤ（ＰＭＳＮ）、２３０・・・ＩＣチップ、２３１・・・メディアＩＤ（ＰＭＳＮ）、２３２・・・スクリプト、２３３・・・ＵＲＬ、２７０・・・情報処理装置、２７１・・・スクリプト実行部、２７２・・・コピー許可要求部、２７３・・・コピー実行部、２７５・・・リーダライタ（Ｒ／Ｗ）、２７７・・・記録メディア、２８０・・・管理サーバ、２８１・・・コピー許可判定部、２８２・・・コピー許可通知部、３００・・・ディスク、３１０・・・データ記録領域、３１１・・・スクリプト、３１２・・・ＵＲＬ、３１３・・・ＭＫＢ、３１４・・・ボリュームＩＤ、３１５・・・暗号化コンテンツ、３２０・・・ＢＣＡ領域、３２１・・・メディアＩＤ（ＰＭＳＮ）、３３０・・・ＩＣチップ、３３１・・・メディアＩＤ（ＰＭＳＮ）、３３２・・・コンテンツＩＤ、３７０・・・情報処理装置、３７１・・・スクリプト実行部、３７２・・・コピー許可要求部、３７３・・・コピー実行部、３７５・・・リーダライタ（Ｒ／Ｗ）、３７７・・・記録メディア、３８０・・・管理サーバ、３８１・・・コピー許可判定部、３８２・・・コピー許可通知部、４００・・・ディスク、４１０・・・データ記録領域、４１１・・・ＭＫＢ、４１２・・・ボリュームＩＤ、４１３・・・暗号化コンテンツ、４２０・・・ＢＣＡ領域、４２１・・・メディアＩＤ（ＰＭＳＮ）、４３０・・・ＩＣチップ、４３１・・・メディアＩＤ（ＰＭＳＮ）、４３２・・・スクリプト、４３３・・・ＵＲＬ、４３４・・・コンテンツＩＤ、４３５・・・認証用データ、４３６・・・認証処理部、４７０・・・情報処理装置、４７１・・・スクリプト実行部、４７２・・・コピー許可要求部、４７３・・・コピー実行部、４７５・・・リーダライタ（Ｒ／Ｗ）、４７７・・・記録メディア、４８０・・・管理サーバ、４８１・・・コピー許可判定部、４８２・・・コピー許可通知部、５００・・・ディスク、５１０・・・データ記録領域、５１１・・・ＭＫＢ、５１２・・・ボリュームＩＤ、５１３・・・暗号化コンテンツ、５２０・・・ＢＣＡ領域、５３０・・・ＩＣチップ、５３１・・・メディアＩＤ（ＰＭＳＮ）、５３２・・・スクリプト、５３３・・・ＵＲＬ、５３４・・・コンテンツＩＤ、５５０・・・ドライブ、５５１・・・鍵データ、５５２・・・

ホストリボケーションリスト、５５３・・・認証処理部、５５４・・・ＭＡＣ算出部、５６０・・・ホスト、５６１・・・鍵データ、５６２・・・ドライブリボケーションリスト、５６３・・・認証処理部、５６４・・・ＭＡＣ算出部、５６５・・・デジイスキー、５６６・・・暗号処理モジュール、５７０・・・情報処理装置、５７１・・・スクリプト実行部、５７２・・・コピー許可要求部、５７３・・・コピー実行部、５７５・・・リーダライタ（Ｒ／Ｗ）、５７７・・・記録メディア、５８０・・・管理サーバ、５８１・・・コピー許可判定部、５８２・・・コピー許可通知部、

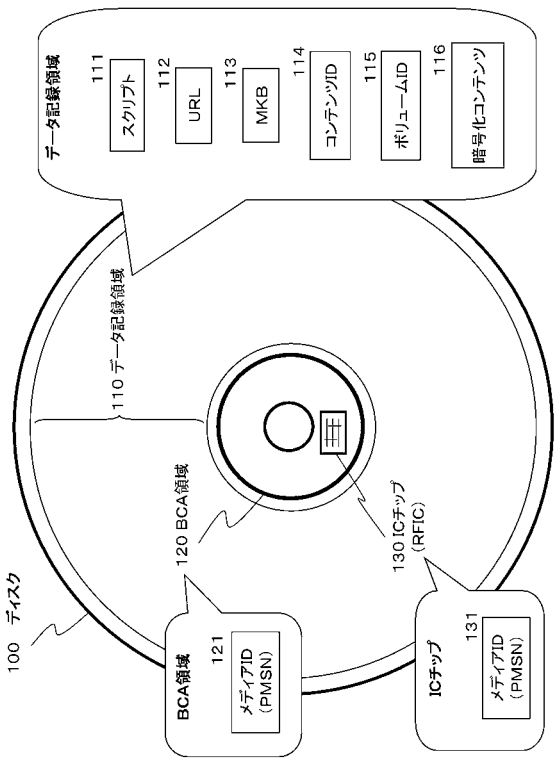
【図１】



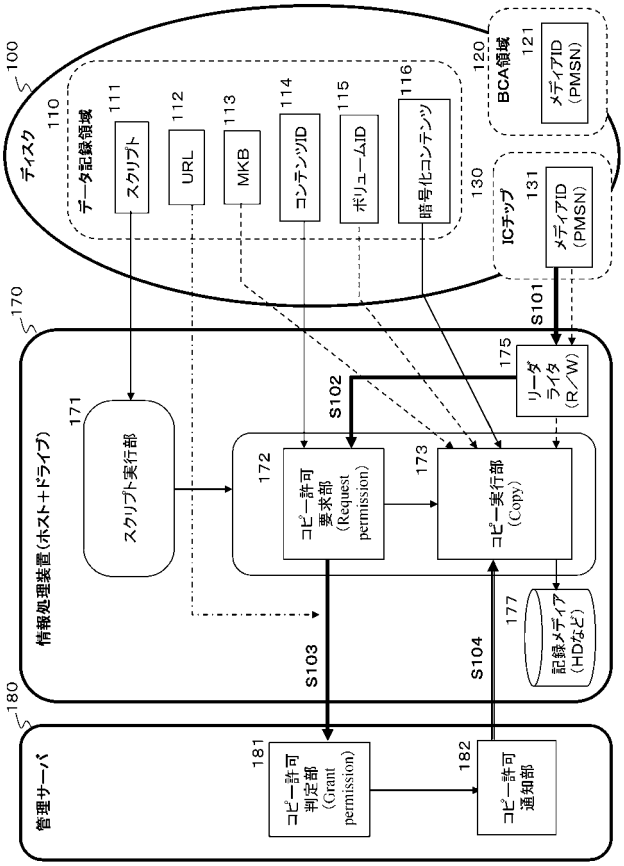
【図２】



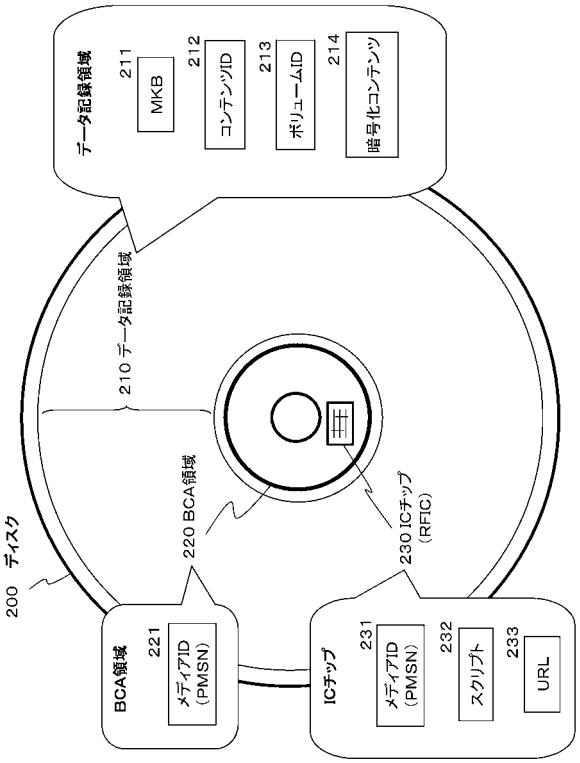
【図３】


100 ディスク
110 データ記録領域
120 BCA領域
130 ICチップ (RFIC)
データ記録領域
111 スクリプト
112 URL
113 MKB
114 コンテンツID
115 ボリュームID
116 暗号化コンテンツ
BCA領域
121 メディアID (PMSN)
ICチップ
131 メディアID (PMSN)

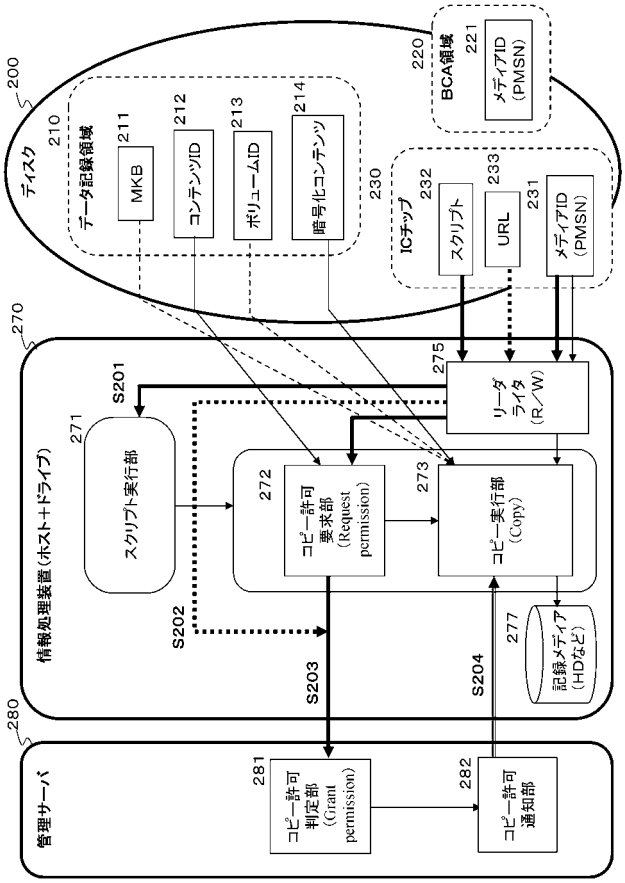
【図４】


100 ディスク
110 データ記録領域
111 スクリプト
112 URL
113 MKB
114 コンテンツID
115 ボリュームID
116 暗号化コンテンツ
120 BCA領域
121 メディアID (PMSN)
130 ICチップ
131 メディアID (PMSN)
170 情報処理装置(ホストドライブ)
171 スクリプト実行部
172 コピー許可要求部 (Request permission)
173 コピー実行部 (Copy)
175 リーダライタ (R／W)
177 記録メディア (HDなど)
180 管理サーバ
181 コピー許可判定部 (Grant permission)
182 コピー許可通知部
S101
S102
S103
S104

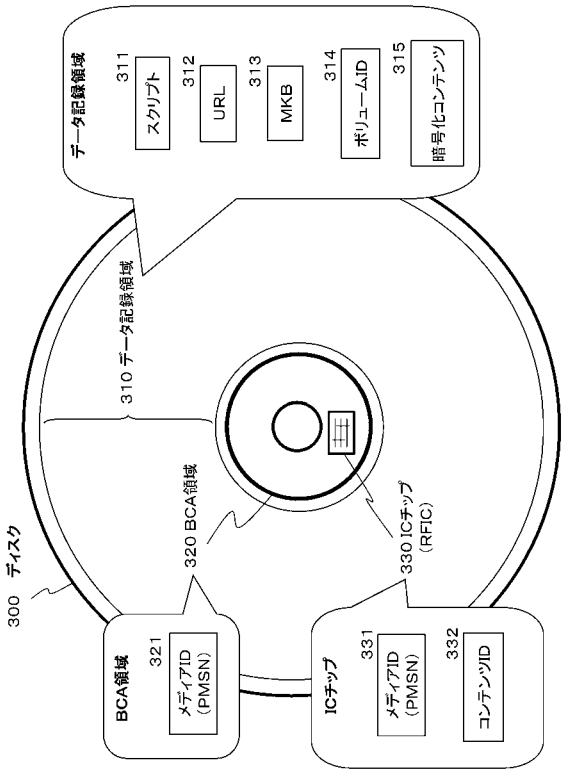
【図５】


200 ディスク
210 データ記録領域
220 BCA領域
230 ICチップ (RFIC)
データ記録領域
211 MKB
212 コンテンツID
213 ボリュームID
214 暗号化コンテンツ
BCA領域
221 メディアID (PMSN)
ICチップ
231 メディアID (PMSN)
232 スクリプト
233 URL

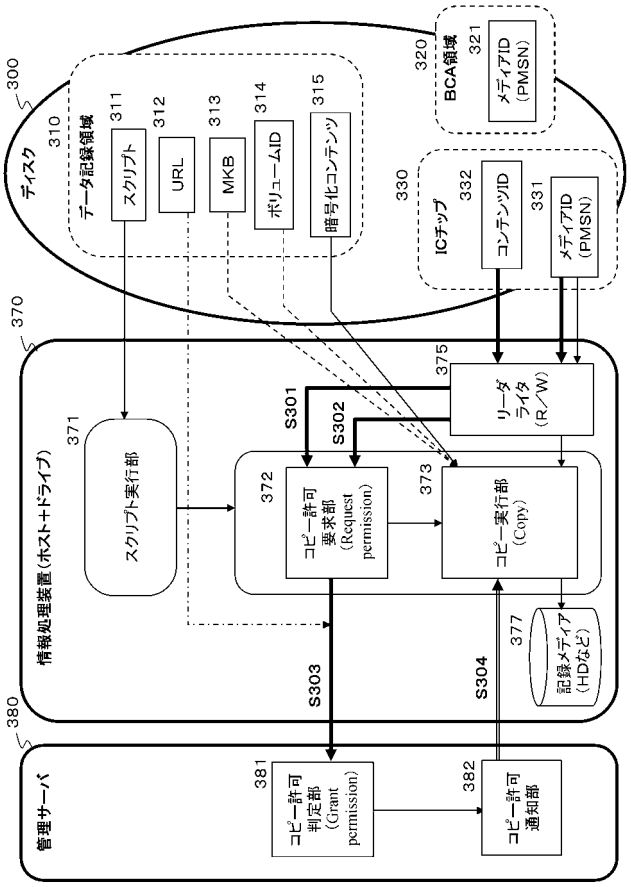
【図６】


200 ディスク
210 データ記録領域
211 MKB
212 コンテンツID
213 ボリュームID
214 暗号化コンテンツ
220 BCA領域
221 メディアID (PMSN)
230 ICチップ
231 メディアID (PMSN)
232 スクリプト
233 URL
270 情報処理装置(ホストドライブ)
271 スクリプト実行部
272 コピー許可要求部 (Request permission)
273 コピー実行部 (Copy)
275 リーダライタ (R／W)
277 記録メディア (HDなど)
280 管理サーバ
281 コピー許可判定部 (Grant permission)
282 コピー許可通知部
S201
S202
S203
S204

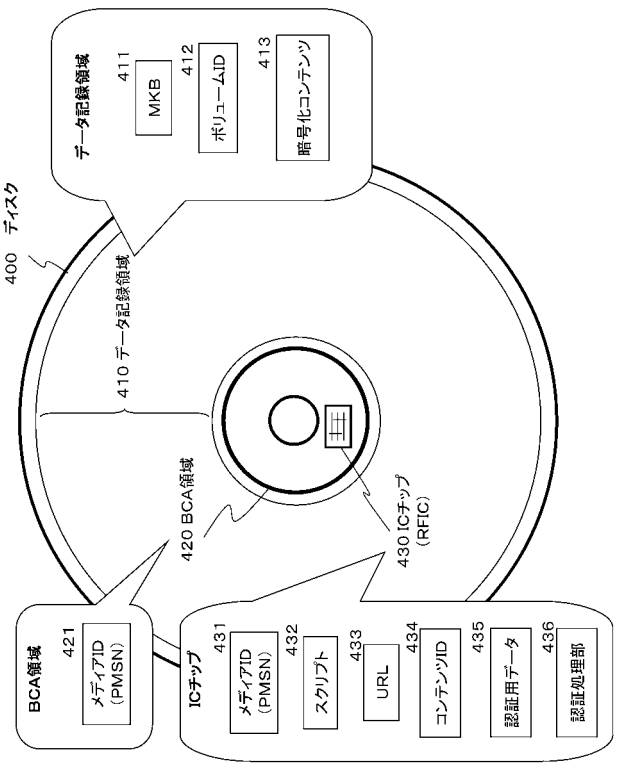
【図７】


300 ディスク
310 データ記録領域
311 スクリプト
312 URL
313 MKB
314 ボリュームID
315 暗号化コンテンツ
320 BCA領域
321 メディアID (PMSN)
330 ICチップ (RFIC)
331 メディアID (PMSN)
332 コンテンツID

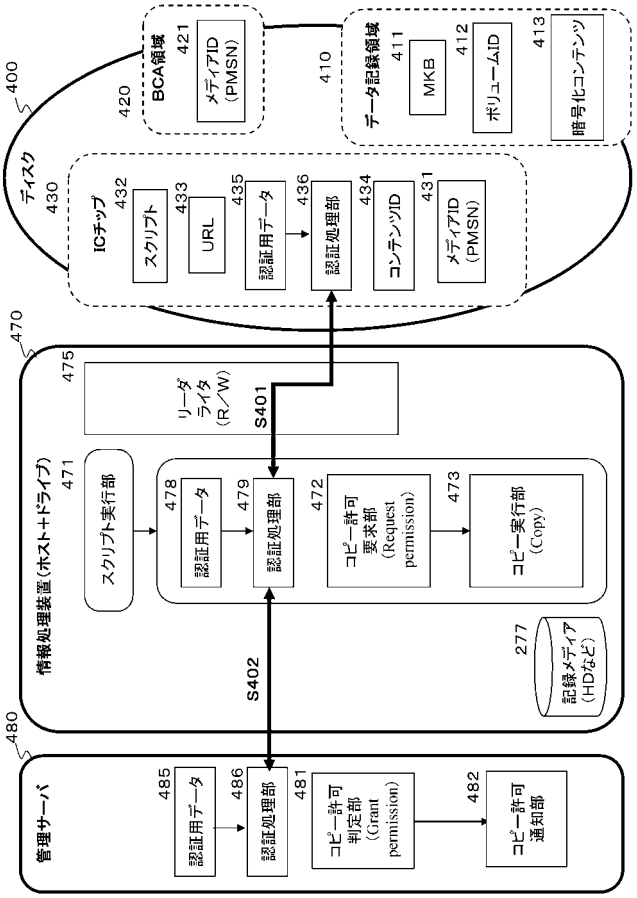
【図８】


300 ディスク
310 データ記録領域
311 スクリプト
312 URL
313 MKB
314 ボリュームID
315 暗号化コンテンツ
320 BCA領域
321 メディアID (PMSN)
330 ICチップ
331 メディアID (PMSN)
332 コンテンツID
370 情報処理装置（ホスト＋ドライブ）
371 スクリプト実行部
372 コピー許可要求部 (Request permission)
373 コピー実行部 (Copy)
375 リーダライタ (R／W)
377 記録メディア (HDなど)
S301
S302
S303
S304
380 管理サーバ
381 コピー許可判定部 (Grant permission)
382 コピー許可通知部

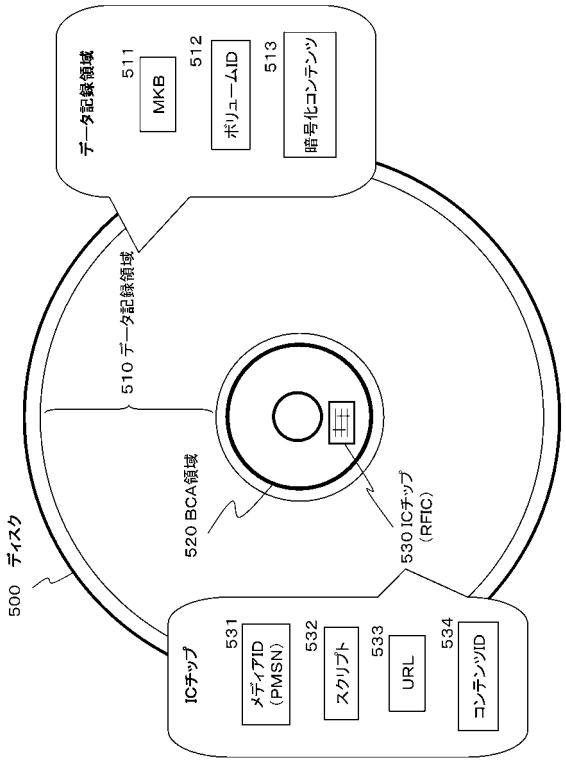
【図９】


400 ディスク
410 データ記録領域
411 MKB
412 ボリュームID
413 暗号化コンテンツ
420 BCA領域
421 メディアID (PMSN)
430 ICチップ (RFIC)
431 メディアID (PMSN)
432 スクリプト
433 URL
434 コンテンツID
435 認証用データ
436 認証処理部

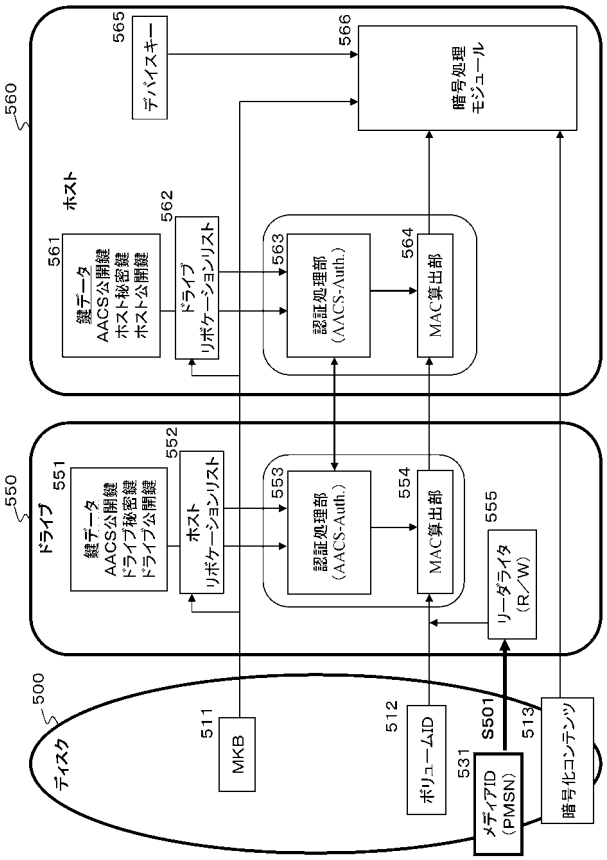
【図１０】


400 ディスク
410 データ記録領域
411 MKB
412 ボリュームID
413 暗号化コンテンツ
420 BCA領域
421 メディアID (PMSN)
430 ICチップ
431 メディアID (PMSN)
432 スクリプト
433 URL
434 コンテンツID
435 認証用データ
436 認証処理部
470 情報処理装置（ホスト＋ドライブ）
471 スクリプト実行部
472 コピー許可要求部 (Request permission)
473 コピー実行部 (Copy)
475 リーダライタ (R／W)
277 記録メディア (HDなど)
S401
S402
478 認証用データ
479 認証処理部
480 管理サーバ
481 コピー許可判定部 (Grant permission)
482 コピー許可通知部
485 認証用データ
486 認証処理部

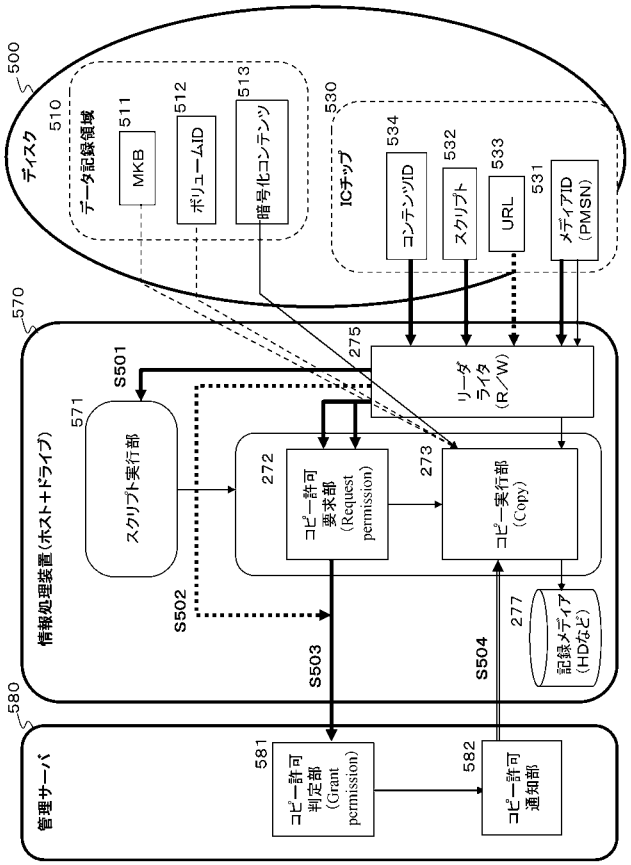
【図１１】


500 ディスク
510 データ記録領域
511 MKB
512 ボリュームID
513 暗号化コンテンツ
520 BCA領域
530 ICチップ (RFIC)
ICチップ
531 メディアID (PMSN)
532 スクリプト
533 URL
534 コンテンツID

【図１２】


560 ホスト
561 鍵データ AACS公開鍵 ホスト秘密鍵 ホスト公開鍵
562 ドライブ リボケーションリスト
563 認証処理部 (AACS-Auth.)
564 MAC算出部
565 デバイスキー
566 暗号処理モジュール
550 ドライブ
551 鍵データ AACS公開鍵 ドライブ秘密鍵 ドライブ公開鍵
552 ホスト リボケーションリスト
553 認証処理部 (AACS-Auth.)
554 MAC算出部
555 リーダライタ (R／W)
500 ディスク
511 MKB
512 ボリュームID
531 メディアID (PMSN)
S501
513 暗号化コンテンツ

【図１３】


500 ディスク
510 データ記録領域
511 MKB
512 ボリュームID
513 暗号化コンテンツ
530 ICチップ
534 コンテンツID
532 スクリプト
533 URL
531 メディアID (PMSN)
570 情報処理装置（ホスト＋ドライブ）
275 リーダライタ (R／W)
S501
571 スクリプト実行部
272 コピー許可要求部 (Request permission)
273 コピー実行部 (Copy)
277 記録メディア (HDなど)
S502
S503
S504
580 管理サーバ
581 コピー許可判定部 (Grant permission)
582 コピー許可通知部

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
Ｇ０６Ｆ　21/24	*(2006.01)*	Ｇ０６Ｋ　17/00	Ｌ	
		Ｇ０６Ｋ　17/00	Ｆ	
		Ｇ０６Ｆ　12/14	５３０Ｃ	

Ｆターム(参考) 5B035 AA13 BA06 BB09 CA23
5B058 CA17 CA23 KA02 KA04 KA31 YA13
5D044 BC02 CC04 DE49 DE50 DE57 DE58 FG18 GK12 HL08