【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第４区分
【発行日】平成22年5月6日(2010.5.6)

【公開番号】特開2009-93731(P2009-93731A)
【公開日】平成21年4月30日(2009.4.30)
【年通号数】公開・登録公報2009-017
【出願番号】特願2007-261781(P2007-261781)
【国際特許分類】
Ｇ１１Ｂ　20/10　(2006.01)
Ｇ１１Ｂ　23/30　(2006.01)
Ｇ０６Ｋ　19/00　(2006.01)
Ｇ０６Ｋ　19/07　(2006.01)
Ｇ０６Ｋ　17/00　(2006.01)
Ｇ０６Ｆ　21/24　(2006.01)
【ＦＩ】
Ｇ１１Ｂ　20/10　Ｈ
Ｇ１１Ｂ　20/10　Ｄ
Ｇ１１Ｂ　23/30　Ｂ
Ｇ０６Ｋ　19/00　Ｑ
Ｇ０６Ｋ　19/00　Ｈ
Ｇ０６Ｋ　17/00　Ｌ
Ｇ０６Ｋ　17/00　Ｆ
Ｇ０６Ｆ　12/14　５３０Ｃ

【手続補正書】
【提出日】平成22年3月18日(2010.3.18)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】変更
【補正の内容】
【００２４】
管理サーバ５０のコピー許可判定部５１は、情報処理装置４０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。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００５６
【補正方法】変更
【補正の内容】
【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、ＡＡＣＳ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。
【手続補正３】
【補正対象書類名】明細書

【補正対象項目名】０１０５
【補正方法】変更
【補正の内容】
【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３３０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３３０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。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０１０７
【補正方法】変更
【補正の内容】
【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３２０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。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０１１０
【補正方法】変更
【補正の内容】
【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３１５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。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０１２３
【補正方法】変更
【補正の内容】
【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４３６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。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】０１２５

【補正方法】変更
【補正の内容】
【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４３６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。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】０１３２
【補正方法】変更
【補正の内容】
【０１３２】
本実施例では、ＩＣチップ５３０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。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】０１３３
【補正方法】変更
【補正の内容】
【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５００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。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】０１４３
【補正方法】変更
【補正の内容】
【０１４３】
ホスト５６０のＭＡＣ算出部５６４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。
【手続補正１１】
【補正対象書類名】明細書

【補正対象項目名】０１４８
【補正方法】変更
【補正の内容】
【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）５７５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。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】０１５０
【補正方法】変更
【補正の内容】
【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ＩＤ５３４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。