【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３区分
【発行日】平成26年12月4日(2014.12.4)

【公開番号】特開2013-109399(P2013-109399A)
【公開日】平成25年6月6日(2013.6.6)
【年通号数】公開・登録公報2013-028
【出願番号】特願2011-251735(P2011-251735)
【国際特許分類】
Ｇ０６Ｆ　21/62　　(2013.01)
Ｇ０６Ｆ　21/64　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/24　　１６６Ｅ
Ｇ０６Ｆ　21/24　　１６６Ｂ
Ｇ０６Ｆ　21/24　　１６７Ａ
Ｇ０６Ｆ　21/24　　１６６Ｃ

【手続補正書】
【提出日】平成26年10月20日(2014.10.20)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００３０
【補正方法】変更
【補正の内容】
【００３０】
例えば、特許文献１（特開２００２－３５８０１１号公報）には、再生予定のコンテンツファイルからハッシュ値を計算し、予め用意された照合用ハッシュ値、すなわち正当なコンテンツデータに基づいて予め計算済みの照合用ハッシュ値との比較を実行し、新たに算出したハッシュ値が照合用ハッシュ値と一致した場合には、コンテンツの改ざんは無いと判定して、コンテンツの再生処理に移行する制御構成を開示している。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００６０
【補正方法】変更
【補正の内容】
【００６０】
利用制御対象となるコンテンツとは、例えば無秩序なコピーやコピーデータ配布等が禁止されたコンテンツや、利用期間が制限されたコンテンツ等である。なお、メモリカード３１に対して、利用制御コンテンツを記録する場合、そのコンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）が合わせて記録される。
利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）には、例えば許容されるコンテンツ利用期間や許容されるコピー回数などのコンテンツ利用に関する情報が記録される。
コンテンツ提供装置は、コンテンツに併せてコンテンツ対応の利用制御情報を提供する。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０１００
【補正方法】変更
【補正の内容】
【０１００】

図６には、左から、メモリカードに対するアクセス要求装置であるサーバＡ６１、サーバＢ６２、ホスト機器６３、メモリカード７０を示している。
サーバＡ６１、サーバＢ６２は、例えば、メモリカード７０に対する記録コンテンツである暗号化コンテンツ（Ｃｏｎ１，Ｃｏｎ２，Ｃｏｎ３・・・）を提供する。
これらのサーバは、さらに、暗号化コンテンツの復号用の鍵であるタイトルキー（Ｋｔ１，Ｋｔ２・・・）、コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ：ＵＲ１，ＵＲ２・・・）を提供する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０１６２
【補正方法】変更
【補正の内容】
【０１６２】
［９．ＥＣＳファイル、ＥＣＳ発行装置証明書の日時情報を適用した処理について］
次に、ＥＣＳファイル、ＥＣＳ発行装置証明書の日時情報を適用した処理について説明する。
（１）ＥＣＳ発行装置１０２が生成し、コンテンツ提供装置に提供されるＥＣＳファイル、
（２）ライセンス発行装置（ＬＡ）１０１が生成し、ＥＣＳ発行装置１０２に提供されるＥＣＳ発行装置証明書、
これらには、図９を参照して説明したように、様々な日時情報が記録される。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０１８９
【補正方法】変更
【補正の内容】
【０１８９】
コンテンツ提供装置は、
暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）を読み出す。さらに、
ＥＣＳ発行装置証明書の記録データであるＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）を読み出す。
さらに、これらの日時情報を比較し、
ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前であるか否かを判定する。
ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前である場合（Ｙｅｓ）は、ステップＳ１５６に進み、暗号化コンテンツの配布を停止する。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０１９０
【補正方法】変更
【補正の内容】
【０１９０】
ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前でない場合（Ｎｏ）は、ステップＳ１５２に進み、ステップＳ１５３以下において暗号化コンテンツ署名ファイル（ＥＣＳファイル）とＥＣＳ発行装置証明書に記録された日時情報（タイムスタンプ）を適用したコンテンツ提供可否判定処理を開始する。
【手続補正７】

【補正対象書類名】明細書
【補正対象項目名】０２００
【補正方法】変更
【補正の内容】
【０２００】
次に、図１８に示すフローチャートを参照して、先に図１５のステップＳ１３２～Ｓ１３５を参照して説明したユーザ装置１０４における暗号化コンテンツ署名ファイル（ＥＣＳファイル）を適用したコンテンツ再生許容判定処理の詳細について説明する。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】０２６５
【補正方法】変更
【補正の内容】
【０２６５】
図２４（ａ）に示す正当データ格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ａ１）コンテンツ（Ｃ１）に対する正当なタイトルキー（Ｋｔ１）で暗号化された暗号化コンテンツ（Ｃ１（Ｋｔ１））
（ａ２）コンテンツ（Ｃ１）に対する正当な利用制御情報（ＵＲ１）
（ａ３）コンテンツ（Ｃ１）に対する正当な暗号化コンテンツ署名ファイル（ＥＣＳファイル：ＥＣＳ１（Ｃ１，Ｋｔ１））
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】０２６９
【補正方法】変更
【補正の内容】
【０２６９】
図２４（ｂ）に示す「すげ替えデータ」格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ｂ１）コンテンツ（Ｃ２）に対する不正なタイトルキー（Ｋｔ１）で暗号化された不正暗号化コンテンツ（Ｃ２（Ｋｔ１））
（ｂ２）コンテンツ（Ｃ２）に不正に対応付けた利用制御情報（ＵＲ１）［＝コンテン（Ｃ１）対応の利用制御情報（ＵＲ１）］
（ｂ３）コンテンツ（Ｃ２）に対応させて不正に生成した暗号化コンテンツ署名ファイル（ＥＣＳ２［＝ＥＣＳ２（Ｃ２，Ｋｔ１）］
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】０２９３
【補正方法】変更
【補正の内容】
【０２９３】
図２７（ａ）に示す正当データ格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ａ１）コンテンツ（Ｃ１）に対する正当なタイトルキー（Ｋｔ１）で暗号化された暗号化コンテンツ（Ｃ１（Ｋｔ１））
（ａ２）コンテンツ（Ｃ１）に対する正当な利用制御情報（ＵＲ１）
（ａ３）コンテンツ（Ｃ１）に対する正当な暗号化コンテンツ署名ファイル（ＥＣＳファイル：ＥＣＳ１（Ｃ１，Ｋｔ１））
【手続補正１１】
【補正対象書類名】明細書

【補正対象項目名】０２９７
【補正方法】変更
【補正の内容】
【０２９７】
図２７（ｂ）に示す「すげ替えデータ」格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ｂ１）コンテンツ（Ｃ１）に対する不正生成したタイトルキー（Ｋｔ２）で暗号化された不正暗号化コンテンツ（Ｃ１（Ｋｔ２））
（ｂ２）コンテンツ（Ｃ１）に対応させて不正に生成した利用制御情報（ＵＲ２）
（ｂ３）コンテンツ（Ｃ１）に対応させて不正に生成した暗号化コンテンツ署名ファイル（ＥＣＳ２［＝ＥＣＳ２（Ｃ１，Ｋｔ２）］
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】０３０４
【補正方法】変更
【補正の内容】
【０３０４】
さらに、コンテンツＣ２の暗号化と復号に適用するタイトルキーＫｔ２を以下の式に従って算出する。
Ｋｔ２＝（Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ（＋）（ＵＲ２｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】０３０５
【補正方法】変更
【補正の内容】
【０３０５】
次に、ステップＳ２４４において、ステップＳ２４３で生成したタイトルキーＫｔ１を適用してコンテンツＣ１（Ｋｔ１）を復号し、さらに、ステップＳ２４３で生成した新たなタイトルキーＫｔ２を適用してコンテンツＣ１暗号化して暗号化コンテンツＣ１（Ｋｔ２）を生成する。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】０３０６
【補正方法】変更
【補正の内容】
【０３０６】
次に、ステップＳ２４５において、暗号化コンテンツＣ１（Ｋｔ２）をメモリカードの汎用領域に記録する。
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】０３０８
【補正方法】変更
【補正の内容】
【０３０８】
次に、ステップＳ２４７において、ステップＳ２４６で不正に生成したＥＣＳ署名（ＥＣＳ２Ｓｉｇ（Ｃ１，Ｋｔ２））を含むＥＣＳファイルを生成してメモリカードの汎用領域に記録する。
最後に、ステップＳ２４８において、ステップＳ２４１で生成した利用制御情報ＵＲ２を汎用領域に記録する。

この図２８に示す一連の処理によって図２７（ｂ）に示す「すげ替えデータ」の記録処理が終了する。
このようなすげ替え処理によって、コンテンツＣ１に対して不正に生成した利用制御情報（ＵＲ２）が対応づけられる。なお、コンテンツＣ１は新たなタイトルキーＫｔ２によって暗号化されて記録される。
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】０３２７
【補正方法】変更
【補正の内容】
【０３２７】
図３０に示すように、メモリカードの汎用領域にはコンテンツに対応する、
暗号化コンテンツ署名（ＥＣＳ）ファイル、
利用制御情報（ＵＲ）、
これらのデータが格納される。
また、保護領域のブロックｋには、
コンテンツに対応するタイトルキーの変換データ、すなわち、
Ｋｔ（＋）ＵＲ｜｜（ＥＣＳＳｉｇ）ｈａｓｈ
が格納される。
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】０３２８
【補正方法】変更
【補正の内容】
【０３２８】
ユーザ装置に対して、コンテンツを提供するコンテンツ提供装置は、自己の有するホスト証明書（図４参照）に記録された保護領域アクセス権情報としてのブロック識別子と、ＥＣＳ発行装置証明書中のブロック識別子としての書き込み許容ブロック領域情報とを比較する。
この比較結果に応じて、コンテンツ提供の可否を判定する。
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】０３３６
【補正方法】変更
【補正の内容】
【０３３６】
ステップＳ４２２において、ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が０ｘＦＦＦＦＦＦＦＦであると判定した場合は、ステップＳ４２３に進み、メディアの保護領域に設定された全ブロックをアクセス許容ブロックとみなす。
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】０３５１
【補正方法】変更
【補正の内容】
【０３５１】
ステップＳ４５１は、先にコンテンツ提供装置の処理として説明した図３１に示すフローのステップＳ４０１の処理と同様の処理である。すなわち、図３２に示すフローを参照して詳細を説明したように、ＥＣＳ発行装置証明書内のブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）と、ブロック識別子範囲情報（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）を適用して、ＥＣＳ発行装置証明書において規

定されたアクセス許容範囲を算出しこれをアクセス許容ブロック識別子リストとして設定する。
【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】０３６４
【補正方法】変更
【補正の内容】
【０３６４】
入出力インタフェース８０５に接続されている通信部８０６は、例えばサーバやホスト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。