

【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 7 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2013-110459(P2013-110459A)

【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2011-251733(P2011-251733)

【国際特許分類】

H 0 4 L 9/32 (2006.01)

G 0 9 C 1/00 (2006.01)

【 F I 】

H 0 4 L 9/00 6 7 5 B

G 0 9 C 1/00 6 4 0 D

【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】0 1 0 5

【補正方法】変更

【補正の内容】

【 0 1 0 5 】

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 A 6 1、サーバ B 6 2、ホスト機器 6 3、メモリカード 7 0 を示している。

サーバ A 6 1、サーバ B 6 2 は、例えば、メモリカード 7 0 に対する記録コンテンツである暗号化コンテンツ (Con 1, Con 2, Con 3...) 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 (Kt 1, Kt 2...)、コンテンツに対応する利用制御情報 (Usage Rule: UR 1, UR 2...) を提供する。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0 1 6 7

【補正方法】変更

【補正の内容】

【 0 1 6 7 】

[9 . E C S ファイル、E C S 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、E C S ファイル、E C S 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) E C S 発行装置 1 0 2 が生成し、コンテンツ提供装置に提供される E C S ファイル、

(2) ライセンス発行装置 (L A) 1 0 1 が生成し、E C S 発行装置 1 0 2 に提供される E C S 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 3】

【補正対象書類名】明細書

【補正対象項目名】0 2 0 5

【補正方法】変更

【補正の内容】

【 0 2 0 5 】

次に、図 1 8 に示すフローチャートを参照して、先に図 1 5 のステップ S 1 3 2 ~ S 1 3 5 を参照して説明したユーザ装置 1 0 4 における暗号化コンテンツ署名ファイル (E C S 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 4】

【補正対象書類名】明細書

【補正対象項目名】0 2 7 0

【補正方法】変更

【補正の内容】

【0 2 7 0】

図 2 4 (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。

(a 1) コンテンツ (C 1) に対する正当なタイトルキー (K t 1) で暗号化された暗号化コンテンツ (C 1 (K t 1))

(a 2) コンテンツ (C 1) に対する正当な利用制御情報 (U R 1)

(a 3) コンテンツ (C 1) に対する正当な暗号化コンテンツ署名ファイル (E C S ファイル : E C S 1 (C 1 , K t 1))

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0 2 7 4

【補正方法】変更

【補正の内容】

【0 2 7 4】

図 2 4 (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。

(b 1) コンテンツ (C 2) に対する不正なタイトルキー (K t 1) で暗号化された不正暗号化コンテンツ (C 2 (K t 1))

(b 2) コンテンツ (C 2) に不正に対応付けた利用制御情報 (U R 1) [= コンテンツ (C 1) 対応の利用制御情報 (U R 1)]

(b 3) コンテンツ (C 2) 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 (E C S 2 [= E C S 2 (C 2 , K t 1)])

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0 2 9 8

【補正方法】変更

【補正の内容】

【0 2 9 8】

図 2 7 (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。

(a 1) コンテンツ (C 1) に対する正当なタイトルキー (K t 1) で暗号化された暗号化コンテンツ (C 1 (K t 1))

(a 2) コンテンツ (C 1) に対する正当な利用制御情報 (U R 1)

(a 3) コンテンツ (C 1) に対する正当な暗号化コンテンツ署名ファイル (E C S ファイル : E C S 1 (C 1 , K t 1))

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0 3 0 2

【補正方法】変更

【補正の内容】

【0 3 0 2】

図 2 7 (b) に示す「すげ替えデータ」格納構成では、

メモ리카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8】

【補正対象書類名】明細書

【補正対象項目名】0310

【補正方法】変更

【補正の内容】

【0310】

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9】

【補正対象書類名】明細書

【補正対象項目名】0311

【補正方法】変更

【補正の内容】

【0311】

次に、ステップS245において、暗号化コンテンツC1(Kt2)をメモ리카ードの汎用領域に記録する。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0313

【補正方法】変更

【補正の内容】

【0313】

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리카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11】

【補正対象書類名】明細書

【補正対象項目名】0332

【補正方法】変更

【補正の内容】

【0332】

図30に示すように、メモ리카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、
 $K_t(+)UR || (ECSSig)hash$
が格納される。

【手続補正 12】

【補正対象書類名】明細書

【補正対象項目名】0333

【補正方法】変更

【補正の内容】

【0333】

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、ECSS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 13】

【補正対象書類名】明細書

【補正対象項目名】0341

【補正方法】変更

【補正の内容】

【0341】

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0xFFFFFFF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。