

【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19年12月20日(2007.12.20)

【公開番号】特開2006-203275(P2006-203275A)

【公開日】平成18年8月3日(2006.8.3)

【年通号数】公開・登録公報2006-030

【出願番号】特願2005-9735(P2005-9735)

【国際特許分類】

H 0 4 L 9/08 (2006.01)

【F I】

H 0 4 L 9/00 6 0 1 A

【手続補正書】

【提出日】平成19年11月7日(2007.11.7)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

コンテンツを記録する記録媒体であって、

コンテンツ鍵を用いてコンテンツが暗号化された暗号化コンテンツと、

複数個の媒体鍵それぞれを用いて媒体鍵ごとに前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵と、

前記複数個の媒体鍵ごとに對応付けられたデバイス鍵を用いて当該媒体鍵が暗号化された暗号化媒体鍵とを記録しており、

前記デバイス鍵は複数個あり、前記デバイス鍵のそれぞれは、前記コンテンツを再生する再生装置、又は複数の再生装置からなる再生装置群に対応しており、

前記複数個の媒体鍵それぞれは、前記複数個のデバイス鍵のうち1個のデバイス鍵に對応している

ことを特徴とする記録媒体。

【請求項2】

外部の記録媒体から取得する暗号化コンテンツを再生するコンテンツの再生装置であつて、

前記記録媒体は、コンテンツ鍵を用いてコンテンツが暗号化された暗号化コンテンツと、複数個の媒体鍵それぞれを用いて媒体鍵ごとに前記コンテンツ鍵が暗号化された暗号化コンテンツ鍵と、前記複数個の媒体鍵ごとに對応付けられたデバイス鍵を用いて当該媒体鍵が暗号化された暗号化媒体鍵とを記録しており、

前記デバイス鍵は複数個あり、前記デバイス鍵のそれぞれは、前記コンテンツを再生する再生装置、又は複数の再生装置からなる再生装置群に対応しており、

前記複数個の媒体鍵それぞれは、前記複数個のデバイス鍵のうち1個のデバイス鍵に對応しており、

前記再生装置は、

当該再生装置に對応するデバイス鍵を保持する保持手段と、

前記保持手段が保持するデバイス鍵に對応する暗号化媒体鍵を、前記記録媒体から取得する媒体鍵取得手段と、

取得した前記暗号化媒体鍵を、前記デバイス鍵を用いて復号して媒体鍵を生成する媒体鍵生成手段と、

前記複数の暗号化コンテンツ鍵のうち前記媒体鍵生成手段にて生成された前記媒体鍵に  
対応する暗号化コンテンツ鍵を、前記記録媒体から取得するコンテンツ鍵取得手段と、

前記暗号化コンテンツ鍵を、前記媒体鍵生成手段にて生成された前記媒体鍵を用いて復  
号して前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

前記暗号化コンテンツを、前記記録媒体から取得するコンテンツ取得手段と、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号する復号手  
段と

を有することを特徴とする再生装置。

#### 【請求項3】

外部の記録媒体から取得する暗号化コンテンツを再生するコンテンツの再生装置で用い  
られる再生方法であって、

前記記録媒体は、コンテンツ鍵を用いてコンテンツが暗号化された暗号化コンテンツと  
、複数個の媒体鍵それぞれを用いて当該媒体鍵ごとに前記コンテンツ鍵が暗号化された暗  
号化コンテンツ鍵と、前記複数個の媒体鍵ごとに對応付けられたデバイス鍵を用いて当該  
媒体鍵が暗号化された暗号化媒体鍵とを記録しており、

前記デバイス鍵は複数個あり、前記デバイス鍵のそれぞれは、前記コンテンツを再生す  
る再生装置、又は複数の再生装置からなる再生装置群に対応しており、

前記複数個の媒体鍵それぞれは、前記複数個のデバイス鍵のうち1個のデバイス鍵に対  
応しており、

前記再生装置は、

当該再生装置に対応するデバイス鍵を保持する保持手段を備え、

前記再生方法は、

前記保持手段が保持するデバイス鍵に対応する暗号化媒体鍵を、前記記録媒体から取得  
する媒体鍵取得ステップと、

取得した前記暗号化媒体鍵を、前記デバイス鍵を用いて復号して媒体鍵を生成する媒体  
鍵生成ステップと、

前記複数の暗号化コンテンツ鍵のうち前記媒体鍵生成ステップにて生成された前記媒体  
鍵に對応する暗号化コンテンツ鍵を、前記記録媒体から取得するコンテンツ鍵取得ステッ  
プと、

前記暗号化コンテンツ鍵を、前記媒体鍵生成ステップにて生成された前記媒体鍵を用い  
て復号して前記コンテンツ鍵を生成するコンテンツ鍵生成ステップと、

前記暗号化コンテンツを、前記記録媒体から取得するコンテンツ取得ステップと、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号する復号ス  
テップと

を有することを特徴とする再生方法。

#### 【請求項4】

請求項3に含まれる各ステップをコンピュータに実行させることを特徴とする再生プロ  
グラム。

#### 【請求項5】

請求項3に含まれる各ステップをコンピュータに実行させるためのプログラムを記録し  
たコンピュータ読み取り可能な記録媒体。

#### 【請求項6】

コンテンツを記録する記録媒体であって、

複数個のコンテンツ鍵それぞれを用いて当該コンテンツ鍵ごとにコンテンツが暗号化さ  
れた暗号化コンテンツと、

媒体鍵を用いて前記複数個のコンテンツ鍵それが暗号化された暗号化コンテンツ鍵  
と、

複数個のデバイス鍵それぞれを用いて当該デバイス鍵ごとに前記媒体鍵が暗号化され  
た暗号化媒体鍵とを記録しており、

前記複数個のデバイス鍵それぞれは、前記コンテンツを再生する再生装置、又は複数の

再生装置からなる再生装置群に対応しており、

前記複数個のコンテンツ鍵それぞれは、少なくとも1以上の再生装置に対応していることを特徴とする記録媒体。

**【請求項7】**

外部の記録媒体から取得する暗号化コンテンツを再生するコンテンツの再生装置であって、

前記記録媒体は、複数個のコンテンツ鍵それぞれを用いて当該コンテンツ鍵ごとにコンテンツが暗号化された暗号化コンテンツと、媒体鍵を用いて前記複数個のコンテンツ鍵それぞれが暗号化された暗号化コンテンツ鍵と、複数個のデバイス鍵それぞれを用いて当該デバイス鍵ごとに前記媒体鍵が暗号化された暗号化媒体鍵とを記録しており、

前記複数個のデバイス鍵それぞれは、前記コンテンツを再生する再生装置、又は複数の再生装置からなる再生装置群に対応しており、

前記複数個のコンテンツ鍵それぞれは、少なくとも1以上の再生装置に対応しており、前記再生装置は、

当該再生装置に対応するデバイス鍵を保持する保持手段と、

前記保持手段にて保持されている前記デバイス鍵にて暗号化された暗号化媒体鍵を、前記記録媒体から取得する媒体鍵取得手段と、

取得した前記暗号化媒体鍵を、前記保持手段にて保持されている前記デバイス鍵を用いて復号して媒体鍵を生成する媒体鍵生成手段と、

当該再生装置に対応する暗号化コンテンツ鍵を、前記記録媒体から取得するコンテンツ鍵取得手段と、

前記暗号化コンテンツ鍵を、生成された前記媒体鍵を用いて復号して前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

当該再生装置に対応するコンテンツ鍵にて暗号化された暗号化コンテンツを、前記記録媒体から取得するコンテンツ取得手段と、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号する復号手段と

を有することを特徴とする再生装置。

**【請求項8】**

外部の記録媒体から取得する暗号化コンテンツを再生するコンテンツの再生装置で用いられる再生方法であって、

前記記録媒体は、複数個のコンテンツ鍵それぞれを用いて当該コンテンツ鍵ごとにコンテンツが暗号化された暗号化コンテンツと、媒体鍵を用いて前記複数個のコンテンツ鍵それぞれが暗号化された暗号化コンテンツ鍵と、複数個のデバイス鍵それぞれを用いて当該デバイス鍵ごとに前記媒体鍵が暗号化された暗号化媒体鍵とを記録しており、

前記複数個のデバイス鍵それぞれは、前記コンテンツを再生する再生装置、又は複数の再生装置からなる再生装置群に対応しており、

前記複数個のコンテンツ鍵それぞれは、少なくとも1以上の再生装置に対応しており、前記再生装置は、

当該再生装置に対応するデバイス鍵を保持する保持手段を備え、

前記再生方法は、

前記保持手段にて保持されている前記デバイス鍵にて暗号化された暗号化媒体鍵を、前記記録媒体から取得する媒体鍵取得ステップと、

取得した前記暗号化媒体鍵を、前記保持手段にて保持されている前記デバイス鍵を用いて復号して媒体鍵を生成する媒体鍵生成ステップと、

当該再生装置に対応する暗号化コンテンツ鍵を、前記記録媒体から取得するコンテンツ鍵取得ステップと、

前記暗号化コンテンツ鍵を、生成された前記媒体鍵を用いて復号して前記コンテンツ鍵を生成するコンテンツ鍵生成ステップと、

当該再生装置に対応するコンテンツ鍵にて暗号化された暗号化コンテンツを、前記記録

媒体から取得するコンテンツ取得ステップと、

生成した前記コンテンツ鍵を用いて、取得した前記暗号化コンテンツを復号する復号ステップと

を有することを特徴とする再生方法。

**【請求項 9】**

請求項 8に含まれる各ステップをコンピュータに実行させることを特徴とする再生プログラム。

**【請求項 10】**

請求項 8に含まれる各ステップをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。