

【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 2 区分

【発行日】平成22年4月15日 (2010.4.15)

【公開番号】特開2009-20401(P2009-20401A)

【公開日】平成21年1月29日 (2009.1.29)

【年通号数】公開・登録公報2009-004

【出願番号】特願2007-184177(P2007-184177)

【国際特許分類】

G 0 9 C 1/00 (2006.01)

H 0 4 N 5/91 (2006.01)

G 0 6 F 21/24 (2006.01)

H 0 4 N 7/167 (2006.01)

H 0 4 N 7/173 (2006.01)

H 0 4 N 5/93 (2006.01)

【 F I 】

G 0 9 C 1/00 6 6 0 D

H 0 4 N 5/91 N

G 0 6 F 12/14 5 4 0 A

G 0 6 F 12/14 5 6 0 C

H 0 4 N 7/167 Z

H 0 4 N 7/173 6 3 0

H 0 4 N 5/93 Z

【手続補正書】

【提出日】平成22年3月2日 (2010.3.2)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】暗号化コンテンツ編集方法およびコンテンツ管理装置

【手続補正 2】

【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】

情報機器が、第 1 の記憶装置にコンテンツを暗号化して格納し、アクセス制御がされた第 2 の記憶装置に前記コンテンツの挿げ替えや改竄を防止するための対象データをコンテンツ利用データとして格納して管理することにより前記コンテンツの保護を行う暗号化コンテンツ編集方法であって、

前記情報機器は、前記コンテンツを暗号化する際に復号時にランダムアクセス可能な暗号化を施し、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツと前記コンテンツ利用データについての再暗号化をすることなく行うことを特徴とする暗号化コンテンツ編集方法。

【請求項 2】

情報機器が、第 1 の記憶装置にコンテンツを暗号化して格納し、前記第 1 の記憶装置またはアクセス制御がされた第 2 の記憶装置に前記コンテンツの挿げ替えや改竄を防止する

ための対象データをコンテンツ利用データとして格納し、前記第2の記憶装置に前記コンテンツ利用データから算出したメッセージ認証値を格納して管理し、前記コンテンツを利用する際に、前記コンテンツ利用データから算出したメッセージ認証値と、前記第2の記憶装置に格納された前記メッセージ認証値とが一致しない場合は、前記コンテンツの利用を許可しないことにより前記コンテンツの保護を行う暗号化コンテンツ編集方法であって、

前記情報機器は、前記コンテンツを暗号化する際に復号時にランダムアクセス可能な暗号化を施し、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツと前記コンテンツ利用データについての再暗号化をすることなく行うことを特徴とする暗号化コンテンツ編集方法。

【請求項3】

請求項1または2記載の暗号化コンテンツ編集方法において、

前記情報機器は、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツについての一つまたは複数のプレイリストを作成することで代行し、作成された前記プレイリストに従って、前記コンテンツ利用データの分割・結合・削除・並べ替えを行なうことにより、新たな一つまたは複数の前記コンテンツ利用データとすることを特徴とする暗号化コンテンツ編集方法。

【請求項4】

請求項1または2記載の暗号化コンテンツ編集方法において、

前記情報機器は、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツについての一つまたは複数のプレイリストを作成することで代行し、作成された前記プレイリストに前記コンテンツ利用データを結合することにより、新たな一つまたは複数の前記コンテンツ利用データとすることを特徴とする暗号化コンテンツ編集方法。

【請求項5】

請求項4記載の暗号化コンテンツ編集方法において、

新たな前記コンテンツ利用データには、前記プレイリストが1つのみ含まれることを特徴とする暗号化コンテンツ編集方法。

【請求項6】

請求項4記載の暗号化コンテンツ編集方法において、

新たな前記コンテンツ利用データには、前記プレイリストが1つに限定されず存在することを特徴とする暗号化コンテンツ編集方法。

【請求項7】

請求項3～6のいずれか1項記載の暗号化コンテンツ編集方法において、

前記情報機器は、暗号化された前記コンテンツ自体に対する分割・結合・削除・並べ替えによる編集処理を行わないことを特徴とする暗号化コンテンツ編集方法。

【請求項8】

請求項1～7のいずれか1項記載の暗号化コンテンツ編集方法において、

前記コンテンツ利用データが、暗号化された前記コンテンツ自体であることを特徴とする暗号化コンテンツ編集方法。

【請求項9】

請求項1～7のいずれか1項記載の暗号化コンテンツ編集方法において、

前記コンテンツ利用データが、暗号化された前記コンテンツの暗号鍵または暗号鍵導出データであることを特徴とする暗号化コンテンツ編集方法。

【請求項10】

請求項1～7のいずれか1項記載の暗号化コンテンツ編集方法において、

前記コンテンツ利用データが、暗号化された前記コンテンツのデータを間引いて抽出したデータであり、前記情報機器は、前記コンテンツを利用または編集する際に、前記コンテンツ利用データが前記コンテンツ内に存在しているかどうかを随時確認することを特徴とする暗号化コンテンツ編集方法。

【請求項 1 1】

第 1 の記憶装置と、

アクセスが制御された第 2 の記憶装置と、

前記第 1 の記憶装置にコンテンツを暗号化して格納し、前記第 2 の記憶装置に前記コンテンツの挿げ替えや改竄を防止するための対象データをコンテンツ利用データとして格納して管理することにより前記コンテンツの保護を行うコンテンツ関連データ処理部とを有するコンテンツ管理装置であって、

前記コンテンツ関連データ処理部は、前記コンテンツを暗号化する際に復号時にランダムアクセス可能な暗号化を施し、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツと前記コンテンツ利用データについての再暗号化をすることなく行うことを特徴とするコンテンツ管理装置。

【請求項 1 2】

第 1 の記憶装置と、

アクセスが制御された第 2 の記憶装置と、

前記第 1 の記憶装置にコンテンツを暗号化して格納し、前記第 1 の記憶装置または前記第 2 の記憶装置に前記コンテンツの挿げ替えや改竄を防止するための対象データをコンテンツ利用データとして格納し、前記第 2 の記憶装置に前記コンテンツ利用データから算出したメッセージ認証値を格納して管理し、前記コンテンツを利用する際に、前記コンテンツ利用データから算出したメッセージ認証値と、前記第 2 の記憶装置に格納された前記メッセージ認証値とが一致しない場合は、前記コンテンツの利用を許可しないことにより前記コンテンツの保護を行うコンテンツ関連データ処理部とを有するコンテンツ管理装置であって、

前記コンテンツ関連データ処理部は、前記コンテンツを暗号化する際に復号時にランダムアクセス可能な暗号化を施し、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツと前記コンテンツ利用データについての再暗号化をすることなく行うことを特徴とするコンテンツ管理装置。

【請求項 1 3】

請求項 1 1 または 1 2 記載のコンテンツ管理装置において、

前記コンテンツ関連データ処理部は、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツについての一つまたは複数のプレイリストを作成することで代行し、作成された前記プレイリストに従って、前記コンテンツ利用データの分割・結合・削除・並べ替えを行なうことにより、新たな一つまたは複数の前記コンテンツ利用データとすることを特徴とするコンテンツ管理装置。

【請求項 1 4】

請求項 1 1 または 1 2 記載のコンテンツ管理装置において、

前記コンテンツ関連データ処理部は、前記コンテンツの分割・結合・削除・並べ替えによる編集処理を、前記コンテンツについての一つまたは複数のプレイリストを作成することで代行し、作成された前記プレイリストに前記コンテンツ利用データを結合することにより、新たな一つまたは複数の前記コンテンツ利用データとすることを特徴とするコンテンツ管理装置。

【請求項 1 5】

請求項 1 4 記載のコンテンツ管理装置において、

新たな前記コンテンツ利用データには、前記プレイリストが 1 つのみ含まれることを特徴とするコンテンツ管理装置。

【請求項 1 6】

請求項 1 4 記載のコンテンツ管理装置において、

新たな前記コンテンツ利用データには、前記プレイリストが 1 つに限定されず存在することを特徴とするコンテンツ管理装置。

【請求項 1 7】

請求項 1 3 ~ 1 6 のいずれか 1 項記載のコンテンツ管理装置において、

前記コンテンツ関連データ処理部は、暗号化された前記コンテンツ自体に対する分割・結合・削除・並べ替えによる編集処理を行わないことを特徴とするコンテンツ管理装置。

【請求項 18】

請求項 11～17 のいずれか 1 項記載のコンテンツ管理装置において、
前記コンテンツ利用データが、暗号化された前記コンテンツ自体であることを特徴とするコンテンツ管理装置。

【請求項 19】

請求項 11～17 のいずれか 1 項記載のコンテンツ管理装置において、
前記コンテンツ利用データが、暗号化された前記コンテンツの暗号鍵または暗号鍵導出データであることを特徴とするコンテンツ管理装置。

【請求項 20】

請求項 11～17 のいずれか 1 項記載のコンテンツ管理装置において、
前記コンテンツ利用データが、暗号化された前記コンテンツのデータを間引いて抽出したデータであり、前記コンテンツ関連データ処理部は、前記コンテンツを利用または編集する際に、前記コンテンツ利用データが前記コンテンツ内に存在しているかどうかを随時確認することを特徴とするコンテンツ管理装置。