

【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21年11月5日(2009.11.5)

【公表番号】特表2009-508412(P2009-508412A)

【公表日】平成21年2月26日(2009.2.26)

【年通号数】公開・登録公報2009-008

【出願番号】特願2008-530239(P2008-530239)

【国際特許分類】

H 0 4 L 9/08 (2006.01)

H 0 4 N 7/173 (2006.01)

G 0 6 Q 30/00 (2006.01)

G 0 6 Q 50/00 (2006.01)

G 0 6 Q 10/00 (2006.01)

G 0 6 F 21/24 (2006.01)

G 0 6 F 21/00 (2006.01)

【 F I 】

H 0 4 L 9/00 6 0 1 B

H 0 4 N 7/173 6 3 0

H 0 4 L 9/00 6 0 1 E

G 0 6 F 17/60 3 0 2 E

G 0 6 F 17/60 1 4 2

G 0 6 F 17/60 5 1 2

G 0 6 F 12/14 5 2 0 D

G 0 6 F 12/14 5 4 0 A

G 0 6 F 12/14 5 2 0 F

G 0 6 F 15/00 3 3 0 Z

【手続補正書】

【提出日】平成21年9月7日(2009.9.7)

【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】

セキュアメモリ領域及び少なくとももう 1 つのメモリ領域を有している不揮発性書換可能メモリデバイスにより、メディアタイトルを配信する方法であって、前記デバイスは、前記セキュア領域に記憶されている 1 つ又は複数のコンテンツ暗号化鍵と、

前記デバイスのメモリ領域に記憶され、前記コンテンツ暗号化鍵（複数鍵）により暗号化されているメディアタイトル、前記メディアタイトルの選択された部分、及び／又は当該タイトルの制約無しにアクセスできる低品質バージョンを含んでいるコンテンツと、を備えており、前記方法は、

権利及び／又は規則に関する情報を受け取る段階と、

前記デバイスの前記セキュアメモリ領域に、認証情報が前記デバイスにより受け取られると前記デバイスに記憶されている選択された暗号化されているメディアタイトルを復号するためのコンテンツ暗号化鍵（複数鍵）へのアクセスを許可する、前記権利及び／又は規則を記憶する段階と、

少なくとも幾つかの前記メディアタイトルの前記選択された部分又は当該タイトルの低

品質バージョンを、レンダリングするためにホストに供給する段階と、から成る方法。

【請求項 2】

前記認証情報を受け取る段階と、前記デバイスに記憶されている選択された暗号化されているメディアタイトルを、コンテンツ暗号化鍵を使用して復号する段階と、を更に含んでいる、請求項 1 に記載の方法。

【請求項 3】

当該認証情報が受け取られる前に、前記認証情報をセッション鍵で暗号化する段階を更に備えている、請求項 1 に記載の方法。

【請求項 4】

前記ホストが、前記暗号化されているメディアタイトルをレンダリングするために前記デバイス进行操作する方法であって、前記方法は、

前記ホストをサーバに接続する段階と、

購入認証を前記ホストから前記サーバに送る段階と、

前記ホスト側で、前記サーバから前記認証情報及び前記権利及び / 又は規則に関する情報を受け取る段階と、

前記認証情報及び前記権利及び / 又は規則に関する情報を前記デバイスに供給する段階と、を更に含んでいる、請求項 1 に記載の方法。

【請求項 5】

前記デバイスに記憶されている前記選択された暗号化されているメディアタイトルを復号する段階と、

前記復号されたメディアタイトルをユーザー向けにレンダリングするために前記ホストに送る段階と、を更に含んでいる、請求項 4 に記載の方法。

【請求項 6】

前記復号された、選択された暗号化されているメディアタイトルをセッション鍵で暗号化する段階を更に含んでいる、請求項 5 に記載の方法。

【請求項 7】

前記ユーザーに当該メディアタイトルを購入するように促す段階を更に含んでいる、請求項 1 に記載の方法。

【請求項 8】

前記メディアタイトルはファイルに編成され、各ファイルは対応するコンテンツ暗号化鍵により暗号化され、前記デバイスは、前記ファイルの内の少なくとも幾つかのそれぞれについて、当該ファイルの前記対応するコンテンツ暗号化鍵を使用するための許可及び / 又は制約を含むアクセス制御記録を更に備えており、前記ファイルの内の 1 つの第 1 アクセス制御記録は、前記認証情報が提示されたとき、前記対応するコンテンツ暗号化鍵にアクセスする前記許可の委譲を別のアクセス制御記録に許可するものであって、前記方法は、

前記認証情報を前記第 1 アクセス制御記録に提示する段階と、

前記第 1 アクセス制御記録に、その対応するコンテンツ暗号化鍵にアクセスする許可を、前記第 1 アクセス制御記録とは異なる第 2 アクセス制御記録に委譲させる段階と、を更に含んでいる、請求項 1 に記載の方法。

【請求項 9】

複数のアクセス制御記録のそれぞれに、その対応するコンテンツ暗号化鍵にアクセスする許可を、前記第 1 及び前記複数のアクセス制御記録とは異なる第 2 アクセス制御記録に委譲させる段階を更に含んでいる、請求項 8 に記載の方法。

【請求項 10】

不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、前記デバイスは、

対応するコンテンツ暗号化鍵によりそれぞれに暗号化されるメディアファイルと、前記ファイルの内の少なくとも幾つかのそれぞれのための制御構造を備え、前記構造は、当該ファイルの前記対応するコンテンツ暗号化鍵を使用するための許可及び / 又は制約を含み

、前記ファイルの内の１つの第１制御構造は、認証情報が提示されたときに、前記対応するコンテンツ暗号化鍵にアクセスするための許可の委譲を別の制御構造に許可するものであって、前記方法は、

前記認証情報を前記第１制御構造に提示する段階と、

前記第１制御構造に、その対応するコンテンツ暗号化鍵にアクセスする許可を、前記第１制御構造とは異なる第２制御構造に委譲させる段階と、を含んでいる方法。

【請求項１１】

前記第１及び第２制御構造は、アクセス制御記録を備えている、請求項１０に記載の方法。

【請求項１２】

セキュアメモリ領域と少なくとももう１つのメモリ領域とを有する不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、前記デバイスは、

前記デバイスに記憶されている暗号化されたコンテンツが関与し、前記セキュアメモリ領域に記憶されている、１つ又は複数のコンテンツ暗号化鍵及び権利及び／又は規則と、

前記デバイスのメモリ領域に記憶され、前記１つ又は複数のコンテンツ暗号化キーにより暗号化されているメディアタイトルを含み、前記権利及び／又は規則は、前記メディアタイトルの内の少なくとも幾つかの選択された部分又は当該タイトルの低品質バージョンだけが制約無しにアクセスできることを、又は当該タイトルが制限回数だけ再生され得ることを指定するコンテンツと、

を備え、

前記方法は、

前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供するための権利及び／又は規則に関する情報を受け取る段階と、

前記デバイスに記憶された、選択され暗号化されているメディアタイトルへのアクセスを許可するために、認証情報に応じて前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供する前記権利及び／又は規則を変更する段階と、から成る方法。

【請求項１３】

ホストが、前記暗号化されているメディアタイトルをレンダリングするために前記デバイスを操作する方法であって、前記方法は、

前記ホストをサービスプロバイダに接続する段階と、

前記ホストからの購入認証を前記サービスプロバイダに送る段階と、

前記認証情報と、前記サービスプロバイダから、前記デバイス内の前記権利及び／又は規則を変更して前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供できるようにする情報を受け取る段階と、を更に含んでいる、請求項１２に記載の方法。

【請求項１４】

前記受け取った情報に応じて前記１つ又は複数のコンテンツ暗号化鍵（複数鍵）の内の少なくとも１つへのアクセスを提供するために、前記デバイスに記憶されている前記権利及び／又は規則を変更する段階を更に含んでいる、請求項１３に記載の方法。

【請求項１５】

前記デバイスに記憶されている選択された暗号化されているメディアタイトルを復号する段階と、

前記復号されたメディアタイトルをユーザー向けにレンダリングするために前記ホストに送る段階と、を更に含んでいる、請求項１４に記載の方法。

【請求項１６】

前記復号された、選択された暗号化されているメディアタイトルをセッション鍵で暗号化する段階を更に含んでいる、請求項１５に記載の方法。

【請求項１７】

ユーザー向けに、前記メディアタイトルの内の少なくとも幾つかの前記選択された部分又は当該タイトルの低品質バージョンを再生するか、又は当該タイトルを制限回数だけ再生する段階と、

前記ユーザーに当該メディアタイトルを購入するように促す段階と、を更に含んでいる、請求項 1 2 に記載の方法。

【請求項 1 8】

前記デバイスに記憶されている前記選択された暗号化されているメディアタイトルを、前記 1 つ又は複数のコンテンツ暗号化鍵により復号する段階と、

前記復号されたメディアタイトルをユーザー向けにレンダリングする段階と、を更に含んでいる、請求項 1 2 に記載の方法。

【請求項 1 9】

当該情報が受け取られる前に、前記認証情報をセッション鍵で暗号化する段階を更に含んでいる、請求項 1 2 に記載の方法。

【請求項 2 0】

複数の不揮発性書換可能メモリデバイスに記憶されている、暗号化されているメディアコンテンツの配信を制御するための方法にあって、前記デバイスは、固有の識別コードを有しており、前記デバイスは、それぞれが N 個のデバイスを含んでいるセットに分割され、前記セットのそれぞれは、セット識別コードと、当該セットの前記デバイス内の暗号化されているコンテンツへのアクセスを制御するための対応する権利オブジェクトとを有し、

前記デバイスの少なくとも 1 つの前記セット識別コードを、その固有の識別コードから導き出す段階と、

前記導き出された識別コードから、前記少なくとも 1 つのデバイス内の暗号化されているコンテンツへのアクセスを制御するための前記権利オブジェクトを識別する段階と、

前記識別された権利オブジェクトをローディング用に前記少なくとも 1 つのデバイスに提供する段階と、から成る方法。

【請求項 2 1】

各デバイスの前記識別コードはそのシリアル番号であり、前記セット識別コードを導き出すことは、前記シリアル番号を事前に決められた数で割る段階を含んでいる、請求項 2 0 に記載の方法。

【請求項 2 2】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法にあって、前記カードはメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されている第 1 メディアコンテンツを備え、前記コンテンツは、少なくとも幾つかのメディアタイトルの選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンだけを含み、前記方法は、

少なくとも幾つかのメディアタイトルの前記選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンをユーザーにレンダリングする段階と、

前記少なくとも幾つかのメディアタイトルのノーカットの又は高品質のバージョン（複数バージョン）にアクセスする権利の購入に関してユーザーに問い合わせを送る段階と、から成る方法。

【請求項 2 3】

前記メディアタイトルは、前記少なくとも幾つかのメディアタイトルの暗号化されているノーカットの又は高品質のバージョン（複数バージョン）にアクセスする権利の購入に関するコンテンツ情報を含み、前記方法は、前記メディアタイトルから前記情報を取得する段階を更に含み、前記送る段階は、前記問い合わせの一環として前記情報を前記ユーザーに送る、請求項 2 2 に記載の方法。

【請求項 2 4】

前記少なくとも幾つかのメディアタイトルの前記暗号化されているノーカットの又は高品質のバージョン（複数のバージョン）を受け取る段階と、購入の証明が提供された後、前記少なくとも幾つかのメディアタイトルの前記暗号化されているバージョン（複数のバージョン）に関する前記権利及び / 又は規則を実行する段階を更に含んでいる、請求項 2

3に記載の方法。

【請求項 2 5】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法であって、前記カードはメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されているメディアコンテンツを備え、前記コンテンツは、少なくとも幾つかのメディアタイトルを含み、前記方法は、

前記少なくとも幾つかのメディアタイトルに時間制限内にアクセスすることを許容する段階と、

前記少なくとも幾つかのメディアタイへのアクセスを追跡する段階と、

前記追跡されたアクセスに基づいてアクセスプロファイルをコンパイルする段階と、から成る方法。

【請求項 2 6】

前記少なくとも幾つかのメディアタイトルは、1つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化され、前記カードは、前記アクセスプロファイルがダウンロードされると、少なくとも幾つかのメディアタイトルへの時間制限アクセスに対して延長を提供する権利及び/又は規則を記憶している、請求項 2 5 に記載の方法。

【請求項 2 7】

前記少なくとも幾つかのメディアタイトルは、1つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化され、前記時間制限又はその延長中に、前記1つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスを許可することによって、時間制限アクセスが許容されるか延長される、請求項 2 6 に記載の方法。

【請求項 2 8】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信できるようにするための方法であって、

不揮発性書換可能メモリカードにアクセスしているアプリケーションの証明書を、それがそうすることを認可されているか否かを判定するために照合する段階と、

前記アプリケーションの前記証明書が要件を満たさない場合は、前記アプリケーションが前記不揮発性書換可能メモリカードにアクセスすることを認可されていないことを示す表示を提供する段階と、から成る方法。

【請求項 2 9】

コンピュータシステムにより実行され、前記システムは、エンティティにより提供されているアプリケーションの事前に決められている証明書の一覧を保存し、前記コンピュータは、前記アプリケーションの証明書を前記事前に決められている証明書の一覧と照合する、請求項 2 8 に記載の方法。