(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-176684
(P2010-176684A)
(43)公開日　平成22年8月12日(2010.8.12)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	520D	5B017
H04L 9/14	(2006.01)	G06F	12/14	540A	5J104
H04L 9/08	(2006.01)	H04L	9/00	641	
		H04L	9/00	601B	

審査請求 有　請求項の数 78　OL　（全 25 頁）

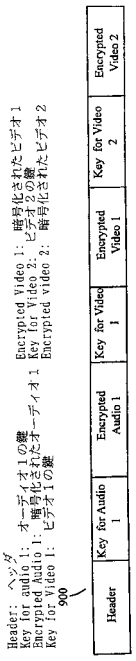
(21)出願番号　特願2010-42116(P2010-42116)
(22)出願日　平成22年2月26日(2010.2.26)
(62)分割の表示　特願2008-535657(P2008-535657)の分割
原出願日　平成18年10月10日(2006.10.10)
(31)優先権主張番号　11/249,123
(32)優先日　平成17年10月11日(2005.10.11)
(33)優先権主張国　米国(US)

(71)出願人　503260918
アップル　インコーポレイテッド
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　インフィニット　ループ　１
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　ファルジア，オーギュスタン・ジェイ
アメリカ合衆国・９５０１４・カリフォルニア州・クーペルティノ・トゥラ　レーン・１０４１１

最終頁に続く

(54)【発明の名称】コンテンツ配信システムにおける複数のコンテンツのピースを伴うメディア・ストレージ構造の使用

(57)【要約】　（修正有）
【課題】ネットワークにわたってコンテンツを配信するための方法を提供する。
【解決手段】方法は、第１の暗号化されたコンテンツのピースをストアする第１のコンテンツ・セクションと、第２の暗号化されたコンテンツのピースをストアする第２のコンテンツ・セクションを含むメディア・ストレージ構造が、第１及び第２の暗号化されたコンテンツのピースを平文化するための第１及び第２の鍵をそれぞれストアするための第１及び第２の鍵セクションも含み、そのメディア・ストレージ構造を、第１及び第２の鍵を配信する１つ又は複数のコンピュータとは別のコンピュータから配信し、第１及び第２の鍵をメディア・ストレージ構造内の第１及び第２の鍵セクションに挿入する。この鍵に基づいて、メディア・ストレージ構造内の２つのコンテンツのピースのうちのいずれか１つ又は両方の暗号化されたコンテンツのピースを平文化し、アクセスが可能になる。
【選択図】図９



【特許請求の範囲】
【請求項１】
ａ）少なくとも２つの暗号化されたメディア部分のセットを含む、単一メディア・ストレージ構造をデバイスに対し提供するステップと、
ｂ）前記デバイスがアクセス権を有する前記メディア部分に基づいて、第２の鍵セットの中から第１の鍵セットを選択するステップであって、前記第１の鍵セットは前記デバイスがアクセス権を有する前記暗号化されたメディア部分のみに前記デバイスがアクセス出来るようにする、ステップと、
ｃ）どのメディア部分に前記デバイスがアクセス可能かを制御するために、前記デバイスに前記第１の鍵セットを提供するステップと、
から成ることを特徴とするコンテンツの配信方法。
【請求項２】
第１のコンピュータのセットは前記単一メディア・ストレージ構造を提供し、第２のコンピュータのセットは前記第１の鍵のセットを提供することを特徴とする請求項１記載の方法。
【請求項３】
前記第１と第２のコンピュータのセットは同じであることを特徴とする請求項１記載の方法。
【請求項４】
前記第１と第２のコンピュータのセットは共有するコンピュータを持たないことを特徴とする請求項１記載の方法。
【請求項５】
前記コンピュータのセットのうち少なくとも１つは、２つ以上のコンピュータを有することを特徴とする請求項１記載の方法。
【請求項６】
前記コンピュータのセットのうち少なくとも１つは、コンピュータを１つのみを有することを特徴とする請求項１記載の方法。
【請求項７】
前記第１の鍵セットは、前記第２の鍵セットより少ない鍵を有することを特徴とする請求項１記載の方法。
【請求項８】
前記メディア・ストレージ構造は各鍵に対するスロットを有し、それぞれのスロットは前記メディア・ストレージ構造の特定のメディア部分に対する特定の鍵を格納するためのものであることを特徴とする請求項１記載の方法。
【請求項９】
前記デバイスの前記メディア部分のセットへのアクセス権を取得するための要求を受信するステップと、
前記要求されたアクセス権を取得するために財務取引を実行するステップと、
から成ることを特徴とする請求項１記載の方法。
【請求項１０】
前記第２の鍵セットの中から、前記第１の鍵セットを選択することは、前記財務取引を介して取得されたアクセス権に基づくことを特徴とする請求項１記載の方法。
【請求項１１】
第１のコンピュータのセットは前記財務取引を実行するために使用され、第２のコンピュータのセットは前記メディア・ストレージ構造を提供するために使用され、第３のコンピュータのセットは前記第１の鍵のセットを選択するために使用されることを特徴とする請求項１記載の方法。
【請求項１２】
前記第１と前記第３のコンピュータのセットは少なくとも１つのコンピュータを共有することを特徴とする請求項１記載の方法。

【請求項１３】
前記第１の鍵セットは、前記デバイスがアクセス権を有する前記メディア・ストレージ構造内の各メディア部分を復号化するための暗号鍵を含むことを特徴とする請求項１記載の方法。
【請求項１４】
前記メディア・ストレージ構造を提供するステップの前に、前記メディア・ストレージ構造内の特定のメディア部分へのアクセス権を取得する財務取引を完了するステップをさらに含むことを特徴とする請求項１記載の方法。
【請求項１５】
コンテンツを受信するデバイスと、
暗号化されたメディア部分を備えるメディア・ストレージ構造と鍵のセットを前記デバイスに配信するコンピュータのセットと、
を備え、
前記鍵のセットの特定の鍵は前記暗号化されたメディア部分内の特定のメディア部分を復号化するためのものであり、
前記鍵のセットはそれぞれのメディア部分に対し１つの鍵を含むのではなく、前記デバイスがアクセス権を有する各メディア部分に対し１つの鍵を有することを特徴とするコンテンツ配信システム。
【請求項１６】
前記コンピュータのセットは、前記暗号化されたコンテンツを配信するための第１のコンピュータと、前記鍵を配信するための第２のコンピュータを有することを特徴とする請求項１５記載のコンテンツ配信システム。
【請求項１７】
前記第２のコンピュータは、特定のデバイスが前記メディア部分の少なくとも一部へのアクセス権を取得した後、特定のメディア部分に対する鍵のセットを配信し、前記特定のメディア部分に対して配信された前記鍵のセットにより、前記特定のデバイスはアクセス権が取得された前記メディア部分の一部にアクセスすることが可能になることを特徴とする請求項１６記載のコンテンツ配信システム。
【請求項１８】
前記メディア・ストレージ構造は各鍵に対するスロットを含み、各スロットは前記メディア・ストレージ構造の特定のメディア部分に対する特定の鍵を格納することを特徴とする請求項１５記載のコンテンツ配信システム。
【請求項１９】
コンピュータ可読媒体に格納されたデータ構造であって、
ａ）ヘッダー情報と、
ｂ）複数の暗号化されたメディア部分と、
ｃ）鍵のセットと、
を備え、それぞれの鍵は前記複数の暗号化されたメディア部分のうちの１つを復号化し、
前記鍵のセットは、暗号化された各メディア部分に対する鍵は含まないことを特徴とするデータ構造。
【請求項２０】
デバイス上のメディア・コンテンツにアクセスする方法であって、
ａ）複数の保護されたメディア部分を伴う単一メディア・ストレージ構造を受信するステップと、
ｂ）前記デバイスがアクセス権を有する前記複数の保護されたメディア部分のそれぞれに対する鍵を受信するステップであって、少なくとも１つの保護されたメディア部分に対する少なくとも１つの鍵は前記単一メディア・ストレージ構造とは別に受信される、ステップと、
ｃ）前記単一メディア・ストレージ構造に受信した各鍵を格納するステップと、
ｄ）前記デバイスがアクセス権を有する保護されたメディア部分にアクセスするため、受

信した鍵を使用するステップと、
から成ることを特徴とする方法。
【請求項２１】
前記単一メディア・ストレージ構造は、保護された各コンテンツの各鍵とは別に受信されることを特徴とする請求項２０の方法。
【請求項２２】
前記保護された各メディア部分に対する各鍵が、前記コンテンツ配信用の第１のコンピュータのセットとは異なるライセンス付与用の第２のコンピュータセットから受信される間に、前記単一メディア・ストレージ構造はコンテンツ配信用の第１のコンピュータセットから受信されることを特徴とする請求項２０の方法。
【請求項２３】
前記保護されたメディア部分の１つはオーディオ・コンテンツであり、前記保護されたメディア部分のうちもう一つは前記オーディオ・コンテンツに関連したビデオ・コンテンツであることを特徴とする請求項２０記載の方法。
【請求項２４】
前記オーディオ・コンテンツはソングであり、前記ビデオ・コンテンツは前記ソングに関連した音楽ビデオであることを特徴とする請求項２１記載の方法。
【請求項２５】
前記保護されたメディア部分の１つはオーディオ・コンテンツであり、前記保護されたメディア部分のもう１つは前記オーディオ・コンテンツに関連したテキスト・コンテンツであることを特徴とする請求項２０記載の方法。
【請求項２６】
前記オーディオ・コンテンツはソングであり、前記テキスト・コンテンツは前記ソングの歌詞であることを特徴とする請求項２０記載の方法。
【請求項２７】
前記保護されたメディア部分の１つはビデオ・コンテンツであり、前記保護されたメディア部分のもう一つは前記ビデオ・コンテンツに関連したテキスト・コンテンツであることを特徴とする請求項２０記載の方法。
【請求項２８】
前記テキスト・コンテンツは前記ビデオ・コンテンツに関連した会話であることを特徴とする請求項２７記載の方法。
【請求項２９】
第２のデバイスが、前記第１のデバイスに格納された前記第１の単一メディア・ストレージ構造から保護されている前記複数のメディア部分へのアクセス権を有するか否かを判定するステップと、
前記第１の単一メディア・ストレージ構造から、少なくとも１つの保護されたメディア部分に関連した少なくとも１つの鍵を削除するステップであって、前記削除された鍵は、前記第２のデバイスがアクセス権を持たない特定の保護されたメディア部分に関連した特定の鍵である、ステップと、
前記第２のデバイスに第２の単一メディア・ストレージ構造を提供するステップと、
をさらに有し、
前記第２の単一メディア・ストレージ構造は、前記第１の単一メディア・ストレージ構造から削除された前記少なくとも１つの鍵を除いた、前記第１の単一メディア・ストレージ構造から保護されている前記複数のメディア部分と格納された鍵を含み、
前記デバイスは第１のデバイスであり、前記単一メディア・ストレージ構造は第１の単一メディア・ストレージ構造であることを特徴とする請求項２０記載の方法。
【請求項３０】
前記第２の単一メディア・ストレージ構造は前記第１の単一メディア・ストレージ構造と同一であることを特徴とする請求項２０記載の方法。
【請求項３１】

前記第１のデバイスに格納された前記第１の単一メディア・ストレージ構造から保護されている複数のメディア部分へ、第２のデバイスがアクセス権を有する否かを判定するステップと、
前記第２のデバイスに第２の単一メディア・ストレージ構造を提供するステップと、
から成り、
前記第２の単一メディア・ストレージ構造は、前記第２のデバイスがアクセス権を持たない特定の保護されたメディア部分に関連した少なくとも１つの鍵を除いた、前記第１の単一メディア・ストレージ構造から保護された複数のメディア部分および格納された鍵を含み、
前記デバイスは第１のデバイスであり、前記単一メディア・ストレージ構造は第１の単一メディア・ストレージ構造であることを特徴とする請求項２０記載の方法。
【請求項３２】
前記第１のデバイスに格納されている前記第１の単一メディア・ストレージ構造から保護されている前記複数のメディア部分へ、第２のデバイスがアクセス権を有するか否かを判定するステップと、
前記第２のデバイスがアクセス権を持たない少なくとも１つの保護されたメディア部分を除く、前記格納された鍵、および前記第１の単一メディア・ストレージ構造から保護されている前記複数のメディア部分を含んだ第２の単一メディア・ストレージ構造を、前記第２のデバイスに提供するステップと、
をさらに有し、
前記デバイスは第１のデバイスであり、前記単一メディア・ストレージ構造は第１の単一メディア・ストレージ構造であることを特徴とする請求項２０記載の方法。
【請求項３３】
前記第２の単一メディア・ストレージ構造は、前記第２のデバイスがアクセス権を持たない、前記少なくとも１つの保護されたメディア部分に関連した少なくとも１つの鍵を含まないことを特徴とする請求項３２記載の方法。
【請求項３４】
ａ）複数の保護されたメディア部分を伴う単一メディア・ストレージ構造をデバイスに提供するステップと、
ｂ）前記デバイスがアクセス権を有する各保護されたメディア部分に対する鍵を、前記デバイスに供給するステップと、
から成り、
各鍵は前記デバイスがアクセス権を有するメディア部分にアクセスするためのものであって、前記単一メディア・ストレージ構造は、前記デバイスがアクセス権を有する少なくとも１つの保護されたメディア部分に対する少なくとも１つの鍵とは別に、提供されることを特徴とする、メディア・コンテンツへのアクセス許可を与える方法。
【請求項３５】
前記単一メディア・ストレージ構造は前記単一メディア・ストレージ構造の前記保護されたメディア・ピースにアクセスするための鍵を挿入するスロットを含むことを特徴とする請求項３４記載の方法。
【請求項３６】
前記単一メディア・ストレージ構造は、保護されたメディア部分のそれぞれとは別に提供されることを特徴とする請求項３４記載の方法。
【請求項３７】
前記単一メディア・ストレージ構造の保護された各メディア部分に対する各鍵が前記コンピュータの第１のセットとは異なるコンピュータの第２のセットによって提供される間に、前記単一メディア・ストレージ構造はコンピュータの第１のセットによって提供されることを特徴とする請求項３４記載の方法。
【請求項３８】
コンテンツを受信するためのデバイスと、

暗号化されたメディア部分のセットを前記デバイスに配信するためのコンピュータの第１のセットと、
鍵のセットを前記デバイスに配信するためのコンピュータの第２のセットと、
を備え、
前記鍵のセット内の特定の鍵は、前記暗号化された特定のメディア部分を復号化するためのものであり、
コンピュータの第１と第２のセットは異なることを特徴とするコンテンツ配信システム。
【請求項３９】
前記デバイスは、前記暗号化されたメディア部分のセットと、前記鍵のセットをメディア・ストレージ構造内に格納することを特徴とする請求項３８記載のシステム。
【請求項４０】
前記デバイスは、前記鍵のセットを除く、前記メディア・ストレージ構造に前記暗号化されたメディア部分のセットを受信し、前記鍵のセットは前記メディア・ストレージ構造内に組み込むことを特徴とする請求項３９記載のシステム。
【請求項４１】
前記デバイスは前記メディア・ストレージ構造を格納し、前記暗号化されたメディア部分のセットにアクセスするために、前記デバイスは前記メディア・ストレージ構造を獲得し、前記鍵のセットを用いて復号化し、そうすることによって前記暗号化されたメディア部分にアクセスすることを特徴とする請求項３９記載のシステム。
【請求項４２】
前記デバイスはコンピュータであることを特徴とする請求項１５または３８記載のコンテンツ配信システム。
【請求項４３】
前記メディア・ストレージ構造を受信するために前記コンピュータを同期させるためのポータブル・プレーヤをさらに備えることを特徴とする請求項４２記載のコンテンツ配信システム。
【請求項４４】
前記デバイスはポータブル・プレーヤであることを特徴とする請求項１５または３８記載のコンテンツ配信システム。
【請求項４５】
コンピュータ可読媒体に格納されたデータ構造であって、前記データ構造は
ａ）ヘッダ情報と、
ｂ）複数の暗号化されたメディア部分と、
ｃ）前記暗号化されたメディア部分の１つを復号化するための各鍵を入れるための複数のスロットと、
を備え、
前記データ構造は、前記鍵を除いて、第１のコンピュータセットによって配信され、前記鍵は前記第１のコンピュータとは異なる第２のコンピュータセットによって配信されることを特徴とするデータ構造。
【請求項４６】
前記複数のスロットのセットに挿入された鍵のセットをさらに備えることを特徴とする請求項４５記載のデータ構造。
【請求項４７】
前記暗号化されたメディア部分の１つはオーディオ・コンテンツであり、前記暗号化されたメディア部分のもう一つは前記オーディオ・コンテンツに関係したビデオ・コンテンツでることを特徴とする請求項１９または４５記載のデータ構造。
【請求項４８】
前記オーディオ・コンテンツはソングであり、前記ビデオ・コンテンツは前記ソングにい関連した音楽ビデオであることを特徴とする請求項４７記載のデータ構造。

【請求項４９】
前記暗号化されたメディア部分の１つはオーディオ・コンテンツであり、前記暗号化されたメディア部分のもう一つは前記オーディオ・コンテンツに関連したテキスト・コンテンツであることを特徴とする請求項１９または４５記載のデータ構造。
【請求項５０】
前記オーディオ・コンテンツはソングであり、前記テキスト・コンテンツはソングの歌詞であることを特徴とする請求項４９記載のデータ構造。
【請求項５１】
前記暗号化されたメディア部分の１つはビデオ・コンテンツであり、前記暗号化されたメディア部分のもう一つは前記ビデオ・コンテンツに関連したテキスト・コンテンツであることを特徴とする請求項１９または４５記載のデータ構造。
【請求項５２】
前記テキスト・コンテンツは前記ビデオの会話であることを特徴とする請求項５１記載のデータ構造。
【請求項５３】
複数のデバイスにメディアコンテンツを配信する方法であって、この方法は、
第１のコンピュータのセットにおいて、複数の保護されたメディア部分を備える単一メディア・ストレージ構造を第１のデバイスに提供するステップと、
第２のコンピュータのセットにおいて、前記第１のデバイスがアクセス権を有する前記複数の保護されたメディア部分のそれぞれに対する鍵を提供するステップと、
前記第１のコンピュータのセットにおいて、前記単一メディア・ストレージ構造を第２のデバイスに提供するステップと、
前記第２のコンピュータのセットにおいて、前記第２のデバイスがアクセス権を有する前記複数のメディア部分のそれぞれに対する鍵を提供するステップと、
から成り、
前記第２のデバイスは、前記第１のデバイスとは異なる前記単一メディア・ストレージ構造のメディア部分へのアクセス権を有することを特徴とする方法。
【請求項５４】
前記第１のデバイスがアクセス権を有する、第１の特定のメディア部分は第１の財務取引に基づくことを特徴とする請求項５３記載の方法。
【請求項５５】
前記第２のデバイスがアクセス権を有する、第２の特定のメディア部分は第２の財務取引に基づくことを特徴とする請求項５４記載の方法。
【請求項５６】
前記第１と第２のデバイスに提供された前記単一メディア・ストレージ構造は、前記第１と第２のデバイスがアクセス権を有する前記メディア部分に依存しないことを特徴とする請求項５３記載の方法。
【請求項５７】
前記複数の保護されたメディア部分は、対称暗号スキームを使用して暗号化された第１のメディア部分と、非対称暗号スキームによって暗号化された第２のメディア部分を有することを特徴とする請求項５３記載の方法。
【請求項５８】
デバイスにメディアコンテンツを配信する方法であって、この方法は、
複数の保護されたメディア部分を含んだ単一メディア・ストレージ構造を前記デバイスに提供するために、第１のソースから第２のソースへ要求を送るステップと、
前記単一メディア・ストレージ構造が前記第１のソースとは異なる前記第２のソースから無事に受信されたことの確認を前記第１のソースで受けるステップと、
前記デバイスがアクセス権を有する前記複数の保護されたメディア部分のそれぞれに対する特定の鍵を、前記第１のソースから前記デバイスに提供するステップと、
から成り、

前記少なくとも１つの鍵は前記デバイスから受信した確認に応答して提供されることを特徴とする方法。
【請求項５９】
前記要求は、前記第１のソースと前記デバイス間における財務取引が実行された後、送られることを特徴とする請求項５８記載の方法。
【請求項６０】
前記単一メディア・ストレージ構造は複数の空のスロットを備えることを特徴とする請求項５８記載の方法。
【請求項６１】
ある特定の鍵は特定の空のスロットに格納されることを特徴とする請求項６０記載の方法。
【請求項６２】
前記特定の鍵の前記特定のスロットへの格納は前記デバイスで実行されることを特徴とする請求項６１記載の方法。
【請求項６３】
デバイスにメディアコンテンツを配信する方法であって、この方法は、
第２のソースから前記デバイスに単一メディア・ストレージ構造を送るよう第１のソースで要求を受けるステップと、
前記第２のソースからの要求に応答して、前記第１のソースが、複数の保護されたメディア部分を有する前記単一メディア・ストレージ構造を、前記デバイスに提供するステップと、
から成ることを特徴とする方法。
【請求項６４】
前記第１と第２のソースは相互に直接連通していることを特徴とする請求項６３記載の方法。
【請求項６５】
前記要求は、前記第１のソースと前記デバイス間における財務取引が実行された後、送られることを特徴とする請求項６３記載の方法。
【請求項６６】
前記財務取引はライセンスを購入して、前記単一メディア・ストレージ構造の少なくとも１つのメディア部分にアクセスすることを特徴とする請求項６５記載の方法。
【請求項６７】
前記単一メディア・ストレージ構造は複数の空のスロットを有することを特徴とする請求項６３記載の方法。
【請求項６８】
ある特定の空のスロット特定はある特定の鍵の格納して、前記前記単一メディア・ストレージ構造から保護されたある特定のメディア部分を復号化するためのものであることを特徴とする請求項６７記載の方法。
【請求項６９】
デバイスにおいて、複数の保護されたメディア部分を含む単一メディア・ストレージ構造を第１のソースから受信するステップと、
前記デバイスにおいて、前記単一メディア・ストレージ構造が前記第１のソースに無事に受信されたことの確認を、前記第１のソースとは異なる前記第２のソースに提供するステップと、
から成ることを特徴とするデバイスでメディア部分を受信する方法。
【請求項７０】
前記デバイスにおいて、前記デバイスがアクセス権を有する前記複数の保護されたメディア部分のそれぞれに対する鍵を、前記第２のソースから受信するステップをさらに有し、少なくとも１つの鍵は前記第２のソースに提供された確認に応答して受信されることを特徴とする請求項６９記載の方法。

【請求項７１】
前記デバイスにおいて、前記単一メディア・ストレージ構造内に受信された鍵を格納するステップをさらに有することを特徴とする請求項７０記載の方法。
【請求項７２】
前記単一メディア・ストレージ構造は複数の空のスロットを有することを特徴とする請求項７１記載の方法。
【請求項７３】
前記複数の保護されたメディア部分は（ｉ）対称暗号スキームを使用して暗号化された第１の保護されたメディア部分と、（ｉｉ）非対称暗号スキームを使用して暗号化された第２の保護されたメディア部分と、を有することを特徴とする請求項６９記載の方法。
【請求項７４】
前記第１の保護されたメディア部分はオーディオ・コンテンツであり、前記第２の保護されたメディア部分はビデオ・コンテンツであることを特徴とする請求項７３記載の方法。
【請求項７５】
前記第１の保護されたメディア部分は、前記第１のソースが前記デバイスに前記単一メディア・ストレージ構造を提供するよう要求を受信してから、前記デバイスによって受信されることを特徴とする請求項６９記載の方法。
【請求項７６】
デバイスにおいて、複数の保護されたメディア部分を含む単一メディア・ストレージ構造が、第１のソースとは異なる第２のソースから無事に受信されたことの確認を第１のソースに提供するステップと、
前記デバイスにおいて、前記デバイスがアクセス権を有する前記複数の保護されたメディア部分のそれぞれに対する鍵を、前記第１のソースから受信するステップと、
から成り、前記第１のソースに提供された確認に応答して、少なくとも１つの鍵が受信されることを特徴とするデバイスでメディア部分を受信する方法。
【請求項７７】
前記単一メディア・ストレージ構造に少なくとも１つの鍵を格納するステップをさらに有することを特徴とする請求項７６記載の方法。
【請求項７８】
少なくとも１つのプロセッサによって実行可能なコンピュータプログラムを格納するコンピュータ可読媒体であって、前記コンピュータプログラムは前記請求項１乃至１４、２０乃至３７、および５３乃至７７に記載された方法を実行するための命令を備えることを特徴とするコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ディジタル著作権管理システムにおける複数のコンテンツのピースを伴う単一メディア・ストレージ構造の使用に関する。
【背景技術】
【０００２】
ネットワークにわたってコンピュータ間で転送されるディジタル・コンテンツの保護は、根本的に今日の多くの企業にとって重要である。企業は、何らかの形式のディジタル著作権管理（ＤＲＭ）プロセスを実装することによってこの保護の確保を試みている。ＤＲＭプロセスは、しばしばコンテンツのピースを暗号化（たとえば、コンテンツのバイナリ形式を暗号化）して利用をそのコンテンツに向けられた権利が与えられているユーザに制限することを伴う。
【０００３】
暗号は、ネットワークにわたる通過においてデータを保護する伝統的な方法である。その典型的な応用において、暗号は、相互に信頼している２当事者間の通信を、通過中のデ

ータに対する攻撃から保護する。しかしながら、今日の多くのディジタル・ファイル転送応用にとって（たとえば、オーディオ又はビデオ・コンテンツの転送にとって）、コンテンツを受け取る当事者（すなわち「受信側」）は、コンテンツを供給する当事者（すなわち「配信側」）がそのコンテンツに適用したＤＲＭ暗号を破ろうと試みるおそれがあることから、このパラダイムがシフトしてしまっている。それに加えて、ネットワーク侵入攻撃の増殖に伴い、第三者が、受信側のコンピュータに対する、したがって保護されたコンテンツに対するアクセスを獲得するおそれもある。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

既存のＤＲＭシステムにおいて配信されるいくつかのコンテンツのピースは互いに関連している。しかしながら既存のＤＲＭシステムは、しばしばコンテンツの受領者が、ＤＲＭコンテンツの関連セットからコンテンツのサブセットを購入するか、又はライセンスすることを許可しない。たとえば、１つの既存のＤＲＭシステムは、特定のソングを、それらの関連する音楽ビデオとともに配信する。ソングをそれの関連する音楽ビデオとともに配信することにおいて、このＤＲＭシステムは、受領者に（１）ソングとそれに関連する音楽ビデオをともに購入すること、又は（２）ソングとそれに関連する音楽ビデオ両方に対するアクセスを見合わせることのいずれかを厳格に要求する。したがって、この分野においては、コンテンツ受領者がＤＲＭコンテンツの関連セットからコンテンツのサブセットを購入するか、又はライセンスすることを柔軟に許可するＤＲＭシステムの必要性が存在する。

【課題を解決するための手段】

【０００５】

本発明の一部の実施態様は、ネットワークにわたってコンテンツを配信するための方法を提供する。この方法は、単一メディア・ストレージ構造を、ネットワークに接続するデバイス（たとえばコンピュータ、ポータブル・プレーヤ等）に配信する。メディア・ストレージ構造は、第１及び第２の暗号化されたコンテンツのピースを含む。第１のコンテンツのピース、第２のコンテンツのピースへのアクセス、又はその両方がデバイスに許可されているか否かに基づいて、この方法は、そのデバイスに、そのデバイスがアクセスすることができるコンテンツのピースを平文化するための鍵のセットを提供する。

【０００６】

提供される鍵のセットは、２つの暗号化されたコンテンツのピースのうちの１つだけを平文化するための１つ又は複数の鍵を含む。又は、両方の暗号化されたコンテンツのピースを平文化するための１つ又は複数の鍵を含んでもよい。たとえば、選択された鍵のセットが、第１の暗号化されたコンテンツのピースを平文化するための第１の鍵及び第２の暗号化されたコンテンツのピースを平文化するための第２の鍵を含む。提供される鍵のセットに基づいて、デバイスが、その後、メディア・ストレージ構造内の２つのコンテンツのピースのうちのいずれか１つ、又はメディア・ストレージ構造内の両方の暗号化されたコンテンツのピースを平文化し、アクセスすることが可能になる。

【０００７】

メディア・ストレージ構造は、第１の暗号化されたコンテンツのピースをストアする第１のコンテンツ・セクションと、第２の暗号化されたコンテンツのピースをストアする第２のコンテンツ・セクションを含む。一部の実施態様においては、メディア・ストレージ構造が、第１及び第２の暗号化されたコンテンツのピースを平文化するための第１及び第２の鍵をそれぞれストアするための第１及び第２の鍵セクションも含む。一部の実施態様の方法は、第１及び第２の暗号化されたコンテンツのピースを伴うメディア・ストレージ構造を、第１及び第２の鍵を配信する１つ又は複数のコンピュータとは別のコンピュータから配信する。一部の実施態様においては、メディア・ストレージ構造を受信するデバイスが、第１及び第２の鍵をメディア・ストレージ構造の第１及び第２の鍵セクションに挿入する。

【０００８】
一方の暗号化されたコンテンツのピースを特定のプレゼンテーション（たとえば音楽ビデオ、映画等）に関連するオーディオ・コンテンツ（たとえば、オーディオ・トラック、ソング、サウンド・トラック等）とし、他方の暗号化されたコンテンツのピースがその特定のプレゼンテーションに関連するビデオ・コンテンツ（たとえば、ビデオ・トラック、ビデオ・クリップ等）としてもよい。それに代えて両方のコンテンツのピースをビデオ・コンテンツ（たとえば、１つ又は複数のシーンの異なるアングルからのビデオ・クリップ）又はオーディオ・コンテンツ（たとえば、異なるバージョン又はミキシングのソング又は動画中の会話のための異なる言語）とすることも可能である。それに加えて、オーディオ又はビデオ以外のコンテンツをメディア・ストレージ構造内にストアすることができる。たとえば、一方のコンテンツのピースをオーディオ又はビデオ・コンテンツとし、他方のコンテンツのピースをそれらのオーディオ又はビデオ・コンテンツのピースに関連付けされる歌詞又は会話とする。

【０００９】
一部の実施態様における方法は、２つより多くのコンテンツのピースを含むメディア・ストレージ構造を配信する。たとえば、いくつかの場合においては、メディア・ストレージ構造が１つのオーディオ・コンテンツのピースを含むとともに、そのオーディオ・コンテンツに関連付けられた２つの異なるビデオ・クリップである（たとえば、あるソングに関連付けられた２つの異なる音楽ビデオである）２つのビデオ・コンテンツのピースをも含む。

【００１０】
一部の実施態様においては、メディア・ストレージ構造を受信するデバイス（たとえばコンピュータ）が、メディア・ストレージ構造を別のデバイス（たとえば、ポータブル・プレーヤ）に転送する。この転送においては、メディア・ストレージ構造からコンテンツのピースの一方を、ほかのデバイス（たとえば、ポータブル・プレーヤ）へのメディア・ストレージ構造の転送において削除できる。いくつかの場合においては、その相手のデバイス上のリソースの消費を低減すさせために、メディア・ストレージ構造からコンテンツが削除される。別の場合においては、その相手のデバイスがこの他方のコンテンツにアクセスする権利を有していないためにメディア・ストレージ構造からコンテンツが削除される。

【００１１】
本発明の新しい特徴は付随する請求の範囲に示されている。しかしながら説明の目的からいくつかの実施態様が添付図面内に示されている。

【図面の簡単な説明】

【００１２】
【図１】この種のメディア・ストレージ構造の例を示した説明図である。
【図２】選択された鍵のセットが第１の暗号化されたコンテンツのピースを平文化するための第１の鍵及び第２の暗号化されたコンテンツのピースを平文化するための第２の鍵を含む例を示した説明図である。
【図３】別のメディア・ストレージ構造の例を示した説明図である。
【図４】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。
【図５】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。
【図６】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。
【図７】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。
【図８】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。

【図９】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。
【図１０】いくつかの実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示した説明図である。
【図１１】一部の実施形態のコンテンツ配信システムを示した説明図である。
【図１２】コンピュータ、ＤＲＭサーバ、及びコンテンツ・キャッシング・サーバの間における１つの可能なインタラクションのセットの例を概念的に示した説明図である。
【図１３】メディア・ファイルを獲得するコンピュータの別の例を示した説明図である。
【図１４】コンピュータの、図１１に示されている例においてそれが受信する２つの鍵のストレージを示した説明図である。
【図１５】コンピュータの、図１３に示されている例においてそれが受信する鍵のストレージを示した説明図である。
【図１６】ポータブル・プレーヤとのＤＲＭコンテンツの同期を行うコンピュータの例を示した説明図である。
【図１７】一部の実施形態においてコンピュータが実行してプレーヤとコンテンツのセットを同期するプロセスを概念的に示した説明図である。
【発明を実施するための最良の形態】
【００１３】
以下の説明においては多くの詳細が説明の目的のために示されている。しかしながら当業者は認識することになろうが、それらの特定の詳細の使用を伴わずにも本発明を実施できることもある。一方、周知の構造やデバイスについては、不必要な詳細によって本発明の記述がわかりにくくならないようにブロック図形式で示されている。
【００１４】
Ｉ．メディア・ストレージ構造
本発明の一部の実施形態は、ネットワークに接続するデバイス（たとえば、コンピュータ、ポータブル・プレーヤ等）に単位メディア・ストレージ構造を配信するためのコンテンツ配信システムを提供する。各単位メディア・ストレージ構造は、関連するコンテンツのピースのセットを含む。一部の実施形態の少なくともいくつかの単位メディア・ストレージ構造内においては、各コンテンツのピースが別々に暗号化されて、無許可の使用からそれを保護する。コンテンツのピースの例は、ビデオ、オーディオ、テキスト、サウンド等を含む。
【００１５】
図１は、一部の実施形態の単位メディア・ストレージ構造１００の例を概念的に示している。この図に示されているとおり、メディア・ストレージ構造は、暗号化されたコンテンツの第１及び第２のピース１０５、１１０を含む。またそれは、コンテンツの第１及び第２のピース１０５、１１０を平文化する第１及び第２の暗号鍵を含む第１及び第２のセクション１１５、１２０も含む。このメディア・ストレージ構造は、このメディア・ストレージ構造内のコンテンツに関するメタデータを含むヘッダ１２５も含む。
【００１６】
第１のコンテンツのピース１０５、第２のコンテンツのピース１１０、又は両方へのアクセスがデバイスに許可されているか否かに基づいて、システムは、そのデバイスに、そのデバイスがアクセスすることができるコンテンツのピースを平文化するための鍵のセットを提供する。提供される鍵のセットは、２つの暗号化されたコンテンツのピースのうちの１つだけを平文化するための１つの鍵だけを含むことができる。両方の暗号化されたコンテンツのピースを平文化するための２つの鍵を含むことができる。
【００１７】
たとえば図２は、選択された鍵のセットが、第１の暗号化されたコンテンツのピース１０５を平文化するための第１の鍵２１５、第２の暗号化されたコンテンツのピース１１０を平文化するための第２の鍵２２０を含む例を示している。図３は、メディア・ストレージ構造１００の別の例を示している。この例においては、メディア・ストレージ構造１０

０が、第２の暗号化されたコンテンツのピース１１０を平文化するための第２の鍵２２０しか含んでいない。

【００１８】

システムがデバイスに提供する鍵のセットに基づいて、デバイスは、２つのコンテンツのピース１０５、１１０のうちのいずれか１つ、又は両方の暗号化されたコンテンツのピースを平文化し、アクセスすることが可能になる。一部の実施形態のシステムは、第１及び第２の暗号化されたコンテンツのピース１０５、１１０を伴うメディア・ストレージ構造を、第１及び第２の暗号化されたコンテンツのピースを平文化するための第１及び第２の鍵２１５、２２０を配信する１つ又は複数のコンピュータとは別のコンピュータから配信する。

【００１９】

この出願は、「鍵」の受信、ストア、操作、使用を述べているが、多数の公知技術を使用して鍵を隠蔽できることは理解されるであろう。たとえば、鍵を隠すこと、鍵を暗号化すること、１を超える数の断片に鍵を分けて別々にストアすること、読み出し／書き込み動作を曖昧化することは、すべて使用可能であり、「鍵」の受信、ストア、使用の一般的概念の中で考慮される。

【００２０】

上で述べたとおり、一部の実施形態によって配信される単一メディア・ストレージ構造は、関連するコンテンツのピースのセットを含む。一部の実施形態においては、２つのコンテンツのピースが、それらが同一のオーディオ及び／又はビデオ・プレゼンテーション（たとえば、ソング、動画、音楽ビデオ等）に関係するとき、関係があるとされる。いくつかの場合においては、２つの関係があるコンテンツのピースを同時に見ること又は再生することができる。別の場合においては、２つのコンテンツのピースを独立に見ること又は再生することができる。

【００２１】

図４～１０は、一部の実施形態のメディア・ストレージ構造内における関係があるコンテンツのピースの種々の例を示している。図４は、一方の暗号化されたコンテンツのピースが、特定のプレゼンテーション（たとえば、音楽ビデオ、映画等）に関係するオーディオ・コンテンツ４０５（たとえば、オーディオ・トラック、ソング、サウンド・トラック）となり、他方の暗号化されたコンテンツのピースがビデオ・コンテンツ４１０（たとえば、ビデオ・トラック、ビデオ・クリップ等）となるストレージ構造４００の例を示している。

【００２２】

図５は、２つのビデオ・コンテンツのピースを含むストレージ構造５００を示している。その種の２つのビデオ・コンテンツのピースの１つの例は、動画中の１つ又は複数のシーンをカバーするために異なるアングルから撮影された２つのビデオ・クリップとなろう。ビデオ・コンテンツのピースは、そのビデオ・コンテンツに関連付けられたオーディオ・コンテンツを含むこともあり、ビデオ・データしか含まないこともある。図６は、２つのオーディオ・コンテンツのピースを含むストレージ構造６００を示している。その種の２つのオーディオ・コンテンツのピースの１つの例は、２つの異なるバージョン又はミキシングのソングとなろう。

【００２３】

オーディオ又はビデオ以外のコンテンツを、本発明の一部の実施形態のメディア・ストレージ構造内にストアしてもよい。たとえば、図７は、１つはオーディオ・コンテンツのピース７０５で、他は、このオーディオ・コンテンツのピース７０５に関連付けられた歌詞、会話、又はそのほかのデータであるテキスト・コンテンツのピース７１０をストアしたメディア・ストレージ構造７００を示している。同様に図８は、ビデオ・コンテンツのピース８０５と、ビデオ・コンテンツのピース８０５に関連付けられた会話であるテキスト・コンテンツのピース８１０とをストアするメディア・ストレージ構造８００を示している。

【００２４】
いくつかの場合においては、システムが２より多くのコンテンツのピースを含むメディア・ストレージ構造を配信する。たとえば図９は、１つのオーディオ・コンテンツのピース（たとえばソング）を、そのオーディオ・コンテンツに関連付けられた２つの異なるビデオ・クリップである（たとえば、ソングに関連付けられた２つの異なる音楽ビデオ）２つのビデオ・コンテンツのピースとともに含むメディア・ストレージ構造９００を示している。同様に図１０は、１つのビデオ・コンテンツのピース（たとえば動画）を、２つの異なる言語によるそのビデオのオーディオ構成部分である２つのオーディオ・コンテンツのピースとともに含むメディア・ストレージ構造１０００を示している。

【００２５】
図４～１０に示されている種々の例では、メディア・ストレージ構造が、メディア・ストレージ構造内にストアされている各コンテンツのピースを平文化するための鍵を含む。前述したとおり、一部の実施形態のコンテンツ配信システムは、特定のデバイス上のメディア・ストレージ構造にアクセスするために異なる鍵のセットの獲得（たとえば、購入されるか又はライセンスされる）を許可する。一部の実施形態においては、デバイスがメディア・ストレージ構造内に、獲得済みの鍵のセットをストアし、その獲得済みの鍵のセットを、そのデバイス上におけるアクセスのために購入されたか又はライセンスされた、そのメディア・ストレージ構造のコンテンツの平文化とアクセスに使用する。平文化された後は、そのデバイスが、平文化されたコンテンツのピースを個別に、又は同時に見ること又は再生することができる。

【００２６】
一部の実施形態においては、メディア・ストレージ構造を受信したデバイス（たとえばコンピュータ）が、そのメディア・ストレージ構造を別のデバイス（たとえば、ポータブル・プレーヤ）に転送する。この転送においては、メディア・ストレージ構造からコンテンツのピースの１つが、その相手のデバイス（たとえば、ポータブル・プレーヤ内）へのメディア・ストレージ構造の転送において削除されることがある。いくつかの場合においては、その相手のデバイス上のリソースの消費を低減するためにコンテンツのピースの１つが削除される。

【００２７】
上に挙げたいくつかの実施形態は、それ自体が鍵のストレージに利用可能な複数のセクションを含むメディア・ストレージ構造を参照して例示されている。その種のストレージ・セクションは、クイックタイム（Ｑｕｉｃｋｔｉｍｅ）ファイル・フォーマット、ウインドウズ・メディア（Ｗｉｎｄｏｗｓ（登録商標）　Ｍｅｄｉａ）ファイル・フォーマット、リアル（Ｒｅａｌ）メディア・フォーマット、ＩＳＯ／ＩＥＣ　１４４９６‐１２、モーションＪＰＥＧ等を含む多くのメディア・ファイル・フォーマット内に組み込まれることが可能である。当業者は認識することになろうが、一部の実施形態においては、それに代わって鍵が、それらが関係する単位メディア・ファイルとは別にストアされ、転送される。

【００２８】
II．コンテンツ配信システム
図１１は、一部の実施形態のコンテンツ配信システム１１００を示している。このコンテンツ配信システムは、コンテンツのディジタル著作権を保護する（すなわち、合法的使用を保証する）態様でコンテンツを配信する。関係のあるコンテンツを配信するために、システムは、複数の関連するコンテンツのピースを伴う単一メディア・ストレージ構造を配信する。この例においては、メディア・ストレージ構造はメディア・ファイルである。当業者は認識することになろうが、ほかの実施形態がほかのタイプのストレージ構造を使用することもある。

【００２９】
図１１に示されているとおり、コンテンツ配信システム１１００は、コンテンツ・キャッシング・サーバ１１０５、ＤＲＭサーバ１１１０、コンテンツ受信コンピュータ１１１

５を含む。コンピュータ１１１５は、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、ネットワークのネットワーク（たとえば、インターネット）等のコンピュータ・ネットワークを通じてサーバ１１０５、１１１０に接続する。

【００３０】

この接続を通じてコンピュータ１１１５は、ＤＲＭサーバ１１１０と通信し、コンテンツを獲得する。一部の実施形態においては、コンテンツ配信システム１１００がコンテンツの販売又はライセンス付与を伴わない。したがって、それらの実施形態においては、ＤＲＭサーバ１１１０が、財務上の目的を考慮することなく、許可されたコンピュータへのコンテンツの配信を単に遵守させる。

【００３１】

しかしながら例示する目的のため、以下に述べるコンテンツ配信システム１１００のいくつかの実施形態は、コンテンツの販売又はライセンス付与を伴う。したがって、それらの実施形態においては、ＤＲＭサーバ１１１０が、そこからコンピュータ１１１５のユーザがコンテンツを購入するか、又はライセンスできるサーバである。言い替えると一部の実施形態のＤＲＭサーバ１１１０は、コンテンツの購入又はライセンス付与のための財務取引を取り扱うサーバになる。いくつかの場合においては、特定のコンテンツの購入又はライセンスを無料にできる。

【００３２】

コンピュータ１１１５がコンテンツを獲得できるとＤＲＭサーバ１１１０が決定した後、コンテンツ配信システム１１００は、コンテンツ・キャッシング・サーバ１１０５を使用し、ネットワーク１１２０を介して１つ又は複数のＤＲＭコンテンツのピースを含むメディア・ストレージ・ファイルをコンピュータ１１１５に提供する。一部の実施形態においては、システム１１００は、ネットワークにわたるコンテンツのダウンロードの速度と効率を向上させるために、複数のコンテンツ・キャッシング・サーバ１１０５を使用してネットワーク上の種々の場所にコンテンツをキャッシュする。ＤＲＭサーバ１１１０がコンテンツ・キャッシング・サーバ１１０５にコンピュータ１１１５への提供を指示する各メディア・ストレージ・ファイルに対して、ＤＲＭサーバ１１１０は、そのコンピュータがメディア・ストレージ・ファイル内にストアされているコンテンツの平文化に使用するための鍵のセットを提供する。

【００３３】

図１２は、コンピュータ１１１５、ＤＲＭサーバ１１１０、コンテンツ・キャッシング・サーバ１１０５の間における１つの可能なインタラクションのセットの例を概念的に示している。このインタラクションのセットは、本発明の一部の実施形態のコンテンツ獲得プロセス１２００を表す。この図に示されているとおり、獲得プロセス１２００は、コンピュータ１１１５が、特定のメディア・ファイル内にストアされている１つ又は複数のコンテンツのピースを購入するか、ライセンスする要求をＤＲＭサーバ１１１０に（１２０５において）送信するときに開始する。１２１０においては、ＤＲＭサーバがこの要求を受信する。

【００３４】

獲得プロセスは、その後、ＤＲＭサーバ１１１０及び／又は購入側のコンピュータ１１１５に、購入又はライセンス取引を完了する１つ又は複数の動作を（１２１５において）実行させる。取引が完了した後、ＤＲＭサーバ１１１０は、購入されたか又はライセンスされたコンテンツのためのメディア・ファイルをコンピュータ１１１５に送信する要求を（１２１５において）コンテンツ・キャッシング・サーバ１１０５に送信する。

【００３５】

コンテンツ・キャッシング・サーバ１１０５は、この要求を１２２５において受信し、それに応答して購入側のコンピュータ１１１５へのメディア・ファイルのダウンロードを（１２３０において）開始する。図１１は、コンテンツ・キャッシング・サーバ１１０５がコンピュータ１１１５にダウンロードするメディア・ファイル１１２５の例を示している。この例においては、メディア・ファイルが５つのセクションを有する。第１及び第２

のセクション１１４５、１１５５が２つの暗号化されたコンテンツのピースを含む。各コンテンツのピースは、特定のコンテンツ鍵を使用して暗号化されている。第３及び第４のセクション１１５０及び１１６０は、ファイル内の空セクションであり、コンテンツ鍵がコンピュータ１１１５によって購入されるかライセンスされる場合に、その種のコンテンツ鍵を挿入するためのセクションである。最後の第５のセクション１１６５は、コンテンツ及び／又はコンテンツ鍵に関係するメタデータを含むヘッダ・フィールドである。

【００３６】

コンピュータ１１１５は、キャッシング・サーバによって提供されたメディア・ファイルを（１２３５において）受信する。その後コンピュータ１１１５は、ダウンロードの確認をＤＲＭサーバ１１１０に（１２４０において）送信する。１２２０の後に、ＤＲＭサーバ１１１０は、待機状態１２４５に遷移して、コンピュータ１１１５から確認が受信されるのを待つ。

【００３７】

ＤＲＭサーバ１１１０は、１２４５においてダウンロードの確認を受信すると、コンピュータ１１１５が購入したか又はライセンスしたコンテンツのピースに基づいて鍵のセットをコンピュータ１１１５に（１２５０において）送信する。図１１に示されている例においては、コンピュータ１１１５がメディア・ファイル内にストアされているコンテンツのピースを両方ともに獲得している。したがって、この例においては、ＤＲＭサーバ１１１０が、コンピュータ１１１５がメディア・ファイル１１２５内の両方のコンテンツのピースにアクセスすることを許可する鍵のセットを（１２５０において）送信する。

【００３８】

図１１に示されている例においては、この鍵のセットが２つのコンテンツ鍵１１３０、１１３２を含む。一部の実施形態においては、各コンテンツのピース（たとえば、１１４５又は１１５５）が特定のコンテンツ鍵（たとえば、１１３０又は１１３２）に基づいて暗号化される。したがって、コンピュータ１１１５は、コンテンツ鍵１１３０を使用して暗号化されたコンテンツ１１４５を平文化し、コンテンツ鍵１１３２を使用して暗号化されたコンテンツ１１５５を平文化する。

【００３９】

図１３は、メディア・ファイル１１２５を獲得するコンピュータ１１１５の別の例を示している。この例においては、コンピュータ１１１５が第１の暗号化されたコンテンツ１１４５だけを獲得する。したがって、コンテンツ・キャッシング・サーバ１１０５がコンピュータ１１１５に両方のコンテンツのピースを含むメディア・ファイルを供給する場合であっても、ＤＲＭサーバ１１１０は、暗号化されたコンテンツ１１４５のためのコンテンツ鍵１１３０しか供給しない。

【００４０】

したがって、この例においては、コンピュータがコンテンツ鍵１１３０を使用することによってメディア・ファイル内の暗号化されたコンテンツ１１４５にアクセスできる。しかしながら、コンピュータ１１１５がメディア・ファイル１１２５内の暗号化されたコンテンツ１１５５のための暗号化されたコンテンツを受信していないことから、そのコンピュータは、暗号化されたコンテンツ１１５５を平文化することができない。

【００４１】

図１２に示されているとおり、コンピュータ１１１５は、ＤＲＭサーバ１１１０によって供給される鍵のセットを（１２５５において）受信する。図１２に示されているとおり、コンピュータ１１１５は、この鍵のセットを（１２６０において）メディア・ファイル内にストアする。図１４は、コンピュータの、図１１に示されている例の中でそれが受信する２つの鍵のストレージを示している。この図に示されているとおり、コンピュータ１１１５は、当初、コンテンツ鍵１１３０と１１３２を一時ストレージ１４０５、１４０７にストアする。その後、それらのコンテンツ鍵を、１２３５において受信して一時ストレージ１４１０内に一時的にストアしているメディア・ファイル１１２５と組み合わせる。その後、コンピュータは、この組合せの結果として得られたメディア・ファイルをコンテ

ンツ・ライブラリ・ストレージ１４１５内にストアする。

【００４２】

図１５は、コンピュータの、図１３に示されている例の中でそれが受信する鍵のストレージを示している。図１５に示されているストレージ動作は、コンピュータがこのコンテンツ鍵の獲得及び受信を行わなかったので、組合せファイル（コンテンツ・ライブラリ・ストレージ１４１５内にストアされる）が第２の暗号化されたコンテンツのためのコンテンツ鍵１１３２を含まないことを除けば、図１４に示されているストレージ動作に類似である。

【００４３】

上記の実施形態においては、コンテンツ配信システム１１００が、暗号化されたコンテンツの提供に１つのコンピュータを使用し、暗号化されたコンテンツの平文化に必要な鍵の提供に別のコンピュータを使用している。当業者は認識することになろうが、別の実施形態においては、コンテンツ配信システムが、暗号化されたコンテンツとその暗号化されたコンテンツを平文化するための鍵の提供に１つのコンピュータを使用する。

【００４４】

それに代わるものとして別の実施形態においては、コンテンツ配信システムが、コンテンツのための暗号鍵の提供に１より多くのコンピュータを使用する。たとえば、オーディオ・コンテンツのための鍵が１つのサーバから使用可能となり、同じメディア・ストレージ構造内にストアされる関係するビデオ・コンテンツのための鍵が別のサーバから利用可能となることがある。複数のサーバが異なる当事者によって所有され、管理されることさえ、それらが管理する著作権の場合と同様に考えられる。

【００４５】

また、上記の実施形態においては、コンテンツ配信システム１１００が、異なるコンテンツのピースの平文化のために異なる暗号鍵を用意する。別の実施形態においては、コンテンツ配信システムが、異なるコンテンツのピースの暗号化に異なるエンコーディング・スキームを使用することができる。たとえばシステムは、オーディオ・コンテンツの暗号化に対称暗号スキームを使用するが、ビデオ・コンテンツの暗号化に非対称暗号スキームを使用することが考えられる。それに代えてシステムが、オーディオ・コンテンツは完全に暗号化するが、ビデオ・コンテンツは部分だけを暗号化するといったことも考えられる。

【００４６】

また図１２は、コンピュータ１１１５、ＤＲＭサーバ１１１０、コンテンツ・キャッシング・サーバ１１０５の間における１つの可能なインタラクションのセットを示している。当業者は認識することになろうが、ほかの実施形態においてはそれらのコンピュータが異なるインタラクションを行うことができる。たとえば一部の実施形態においては、コンピュータ１１１５が、ＤＲＭサーバに対してメディア・ファイルの受信の確認を送信しない。それらの実施形態のいくつかにおいては、ＤＲＭサーバ自体が鍵のセットをコンピュータ１１１５に送信する。

【００４７】

単純化したネットワーク構成を参照して一部の実施形態を説明してきたが、ここで述べた枠組の中で多くの変形が存在することは理解されるであろう。たとえばＤＲＭサーバが単一のコンピュータとして示されているが、この特許の目的のためには、その種のサーバが多くの相互接続されたコンピュータ及び／又はメモリ及び／又は相互接続された装置の部分を含むことができる。同様にコンテンツ・キャッシング・サーバを単一のコンピュータ又は全体でサーバを構成するネットワークされたコンピュータとメモリの集合とすることも可能である。それに加えて、コンテンツはコンテンツ・キャッシング・サーバから特定のクライアント・コンピュータに直接又は間接的に供給できるが、ほかの転送方法は、コンピュータが、それがピア・コンピュータ、ポータブル・ストレージ・デバイス、又は何らかのそのほかの転送メカニズムから利用できるコンテンツをアンロックするための鍵を必要とする結果に帰することもある。

【００４８】
III．プレーヤとの同期
一部の実施形態においては、コンピュータ１１１５が、それ自体のＤＲＭコンテンツを、そのＤＲＭコンテンツへのアクセスが許可されたポータブル・プレーヤに同期させることができる。いくつかの場合においては、この同期が、コンピュータがポータブル・プレーヤにダウンロードするメディア・ファイルから１つ又は複数のコンテンツのピースを削除する。いくつかの場合においては、その相手のデバイス上のリソースの消費を低減するためにそれらのコンテンツが削除される。別の場合においてはその相手のデバイスがこの他方のコンテンツにアクセスする権利を有していないためにメディア・ストレージ構造からコンテンツが削除される。
【００４９】
図１６は、ポータブル・プレーヤ１６０５とのＤＲＭコンテンツの同期を行うコンピュータ１１１５の例を示している。ポータブル・プレーヤは、音楽プレーヤ、オーディオ／ビデオ・プレーヤ等とすることが可能である。コンピュータ１１１５がそれ自体のＤＲＭコンテンツの同期をポータブル・プレーヤ１６０５と行うとき、一部の実施形態におけるポータブル・プレーヤ１６０５は、（１）コンピュータ１１１５からＤＲＭコンテンツを受信し、かつ（２）それが受信する各ＤＲＭコンテンツのピースを平文化するためのコンテンツ鍵を受信する。ポータブルは、その後、受信した暗号化されたＤＲＭコンテンツと関連する鍵をストアする。
【００５０】
図１７は、一部の実施形態においてコンピュータ１１１５が実行してプレーヤ１６０５とコンテンツのセットを同期するプロセス１７００を概念的に示している。この図に示されているとおり、プロセス１７００は、それが、プレーヤ１６０５とのコンテンツのセットの同期を行う要求を受信するときに（１７０５において）開始する。その後プロセスは、プレーヤのユーザ・アカウントＩＤに関連付けられたメディア・ファイルのセットを（１７１０において）識別する。
【００５１】
次にプロセスは、コンピュータ１１１５がプレーヤにまだダウンロードしていない、そのプレーヤのためのメディア・ファイルをストアしているか否かを（すなわち、コンピュータとプレーヤの間において同期される必要があるメディア・ファイルがあるか否かを）（１７１５において）決定する。存在しない場合にはプロセスが終了する。
【００５２】
それ以外は、プロセスが、同期される必要のあるメディア・ファイルを（１７２０において）選択する。１７２０においては、プロセスが、そのポータブル・プレーヤにダウンロードされるべきでないコンテンツとして指定されているコンテンツのピースがあれば、メディア・ファイルから削除する。一部の実施形態においては、コンピュータが、ユーザがポータブル・プレーヤとの同期を希望しているコンテンツをユーザが指定することを可能にするアプリケーションを使用する。
【００５３】
プロセスがメディア・ファイルからコンテンツを（１７２０において）削除する場合に、本発明の一部の実施形態においては、メディア・ファイルからそのコンテンツの関連するコンテンツ鍵とメタデータも削除する。図１６は、ビデオ・コンテンツ及びそれに関連するコンテンツ鍵を、ポータブル・プレーヤ１６０５にダウンロードされるメディア・ファイル１６００から削除する例を示している。
【００５４】
１７２０の後、プロセスが、プレーヤと同期されなければならない暗号化されたコンテンツのみを含むメディア・ファイルを（１７２５において）ダウンロードする（すなわち、プレーヤにダウンロードされるべきでないコンテンツが削除された後のメディア・ファイルをダウンロードする）。一部の実施形態においては、ダウンロードされるメディア・ファイルが１つ又は複数の暗号化されたコンテンツのピースを含むだけでなく、そのコン

テンツの平文化に使用可能な１つ又は複数のコンテンツ鍵も含む。一部の実施形態においては、メディア・ファイル内においてプレーヤにダウンロードされる鍵のセットがコンピュータ１１１５上においてそのコンテンツの平文化に使用される鍵のセットと同一になる。別の実施形態においては、ダウンロードされるメディア・ファイル内の鍵が異なる鍵のセットになる。

【００５５】

その後プレーヤは、ダウンロードされたメディア・ファイルを、それ自体の内蔵ストレージ（たとえば、それの不揮発性ストレージ、ハードドライブ、フラッシュ・メモリ等）上に（１７２５において）ストアする。１７２５の後、プロセスが、プレーヤにまだダウンロードされていない、そのプレーヤのための追加のコンテンツが残っているか否かを（すなわち、コンピュータとプレーヤの間において同期される必要のある追加のコンテンツが存在するか否かを）（１７３０において）決定する。該当すれば、プロセスが、同期される必要があるコンテンツのピースについて１７２０と１７２５を反復する。該当しなければプロセスが終了する。

【００５６】

図１７は、本発明の一部の実施形態におけるコンピュータとプレーヤの間のメディア・ファイルの同期の説明する例を提供している。当業者は認識することになろうが、ほかの実施形態は、メディア・ファイルの同期のための別のプロセスを使用する。また、一部の実施形態においては、ポータブル・プレーヤがＤＲＭサーバ及び／又はコンテンツ・キャッシング・サーバと直接通信してコンテンツを獲得する。

【００５７】

IV.　暗号化

上で述べたとおり、本発明のいくつかの実施形態は、コンテンツを配信するためのＤＲＭプロセスとシステムを提供する。それらのプロセスとシステムは、暗号鍵に基づいてコンテンツの暗号化と平文化を行う。コンテンツの暗号化は、１つ又は複数の暗号鍵に基づいて平文化可能な形式（平文と呼ばれる）から平文化不可能な形式（暗号文と呼ばれる）へのコンテンツの変換を伴う。コンテンツの平文化は、１つ又は複数の暗号鍵の使用によって、暗号化されたコンテンツを平文化可能な形式に変換することを含む。

【００５８】

暗号鍵は、暗号アルゴリズムの動作を制御する情報の一部である。対称暗号化テクノロジにおいては、コンテンツの暗号化に使用される鍵がコンテンツの平文化に使用される鍵と同一になる。非対称暗号化テクノロジにおいては、コンテンツの暗号化と平文化に同一の鍵が使用されない。たとえば、１つのスキームにおいては、暗号化デバイスが受領側の公開鍵を使用してコンテンツを暗号化し、受領側は、それ自体の秘密鍵を使用して暗号化されたコンテンツを平文化する。

【００５９】

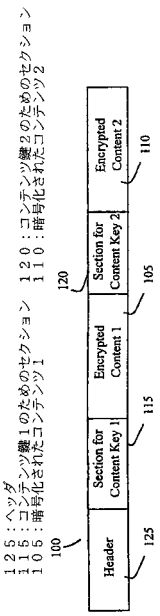
上で述べた実施形態の特徴の多くは、対称又は非対称暗号化アプローチに従って実装可能である。また一部の実施形態においては、暗号化がコンテンツのバイナリ・フォーマットに適用される。暗号化されていないコンテンツのピースのバイナリ・フォーマットは、人間にとって解読が困難であるが、アプリケーション又はオペレーティング・システムによっては解読可能である。それに対し、暗号化されたコンテンツのピースのバイナリ・フォーマットは、理想的には、１つ又は複数の暗号鍵を使用することによって最初に平文化しない限り、あらゆるアプリケーション又はオペレーティング・システムによっても解読できないものとなる。

【００６０】

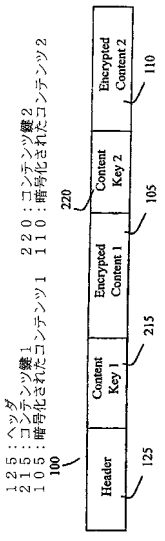
以上、多くの特定の詳細を参照して本発明を説明してきたが、当業者であれば、本発明の精神から逸脱することなしにほかの特定の形式において本発明の具体化が可能であることを認識するであろう。たとえば、一部の実施形態のメディア・ストレージ・ファイルについて１セットの鍵が上に述べられているが、ほかの実施形態は、異なるデバイス上におけるメディア・ストレージ・ファイルのコンテンツに対する異なるレベルのアクセスを定

義するために異なるセットの鍵を提供する。したがって、当業者は理解することになろうが、本発明が以上の例示的な詳細によって限定されることはなく、付随する特許請求の範囲によって定義される。

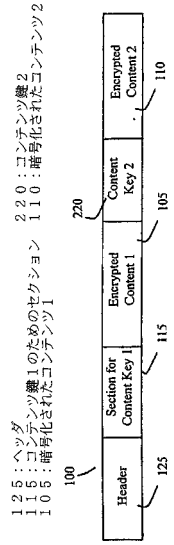
【図１】



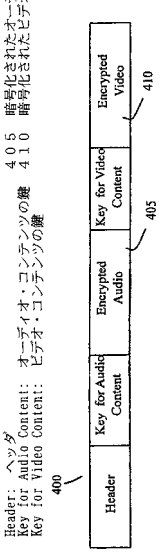
【図２】



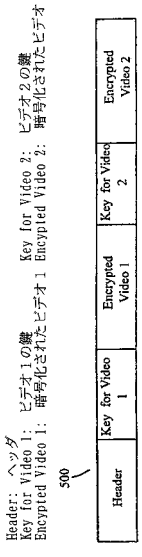
【図３】


１２５：ヘッダ
１１５：コンテンツ鍵１のためのセクション　２２０：コンテンツ鍵２
１０５：暗号化されたコンテンツ１　１１０：暗号化されたコンテンツ２
100
Header
Section for Content Key 1
Encrypted Content 1
Content Key 2
Encrypted Content 2
125
115
105
220
110

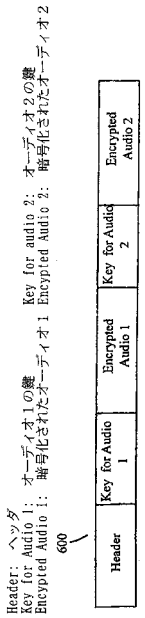
【図４】


Header: ヘッダ
Key for Audio Content: オーディオ・コンテンツの鍵　４０５　暗号化されたオーディオ
Key for Video Content: ビデオ・コンテンツの鍵　４１０　暗号化されたビデオ
400
Header
Key for Audio Content
Encrypted Audio
Key for Video Content
Encrypted Video
405
410

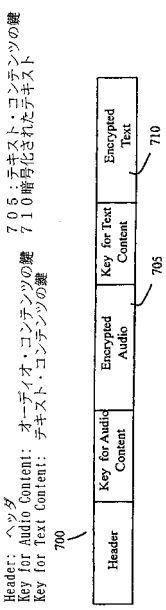
【図５】


Header: ヘッダ
Key for Video 1: ビデオ１の鍵　Key for Video 2: ビデオ２の鍵
Encrypted Video 1: 暗号化されたビデオ１　Encrypted Video 2: 暗号化されたビデオ２
500
Header
Key for Video 1
Encrypted Video 1
Key for Video 2
Encrypted Video 2

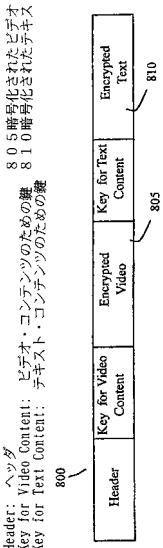
【図６】


Header: ヘッダ
Key for Audio 1: オーディオ１の鍵　Key for audio 2: オーディオ２の鍵
Encrypted Audio 1: 暗号化されたオーディオ１　Encrypted Audio 2: 暗号化されたオーディオ２
600
Header
Key for Audio 1
Encrypted Audio 1
Key for Audio 2
Encrypted Audio 2

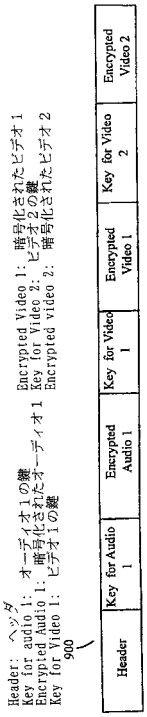
【図７】


Header: ヘッダ
Key for Audio Content: オーディオ・コンテンツの鍵
Key for Text Content: テキスト・コンテンツの鍵
700
Header
Key for Audio Content
Encrypted Audio
Key for Text Content
Encrypted Text
705
710
７０５：テキスト・コンテンツの鍵
７１０暗号化されたテキスト

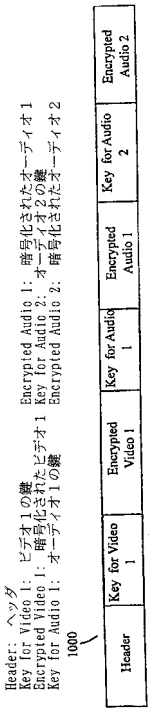
【図８】


Header: ヘッダ
Key for Video Content: ビデオ・コンテンツのための鍵
Key for Text Content: テキスト・コンテンツのための鍵
800
Header
Key for Video Content
Encrypted Video
Key for Text Content
Encrypted Text
805
810
８０５暗号化されたビデオ
８１０暗号化されたテキスト

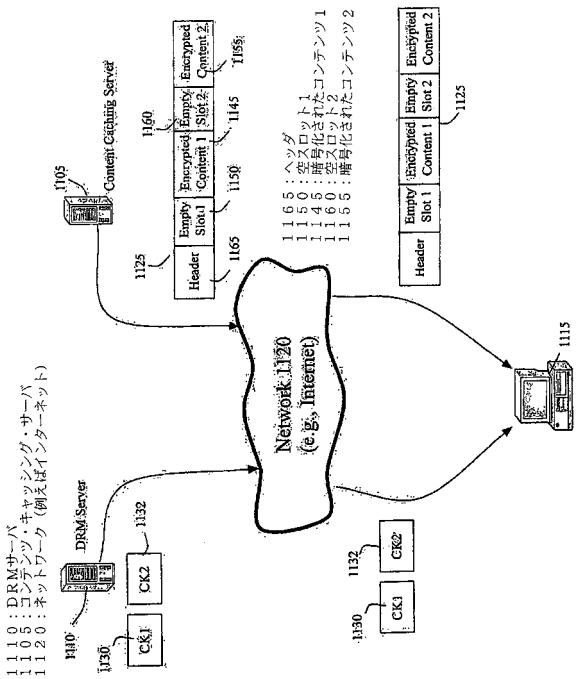
【図９】


Header: ヘッダ
Key for audio 1: オーディオ１の鍵
Encrypted Audio 1: 暗号化されたオーディオ１
Key for Video 1: ビデオ１の鍵
Encrypted Video 1: 暗号化されたビデオ１
Key for Video 2: ビデオ２の鍵
Encrypted video 2: 暗号化されたビデオ２
900
Header
Key for Audio 1
Encrypted Audio 1
Key for Video 1
Encrypted Video 1
Key for Video 2
Encrypted Video 2

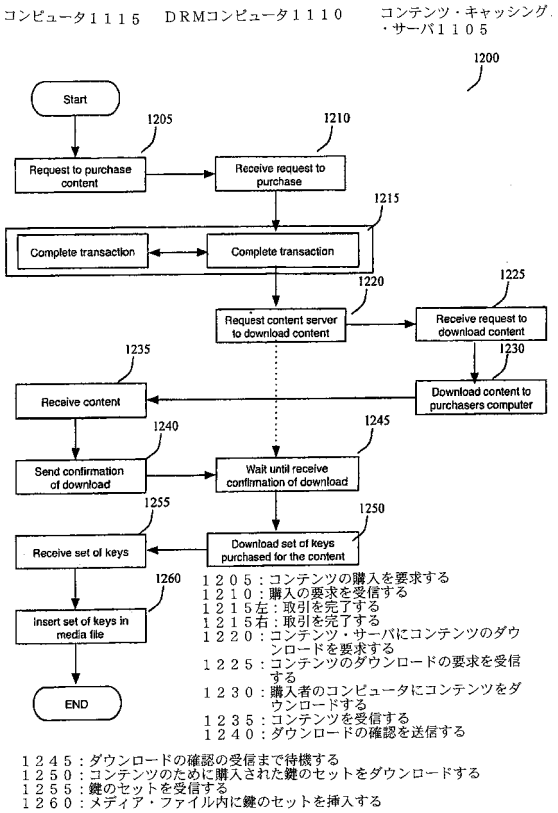
【図１０】


Header: ヘッダ
Key for Video 1: ビデオ１の鍵
Encrypted Video 1: 暗号化されたビデオ１
Key for Audio 1: オーディオ１の鍵
Encrypted Audio 1: 暗号化されたオーディオ１
Key for Audio 2: オーディオ２の鍵
Encrypted Audio 2: 暗号化されたオーディオ２
1000
Header
Key for Video 1
Encrypted Video 1
Key for Audio 1
Encrypted Audio 1
Key for Audio 2
Encrypted Audio 2

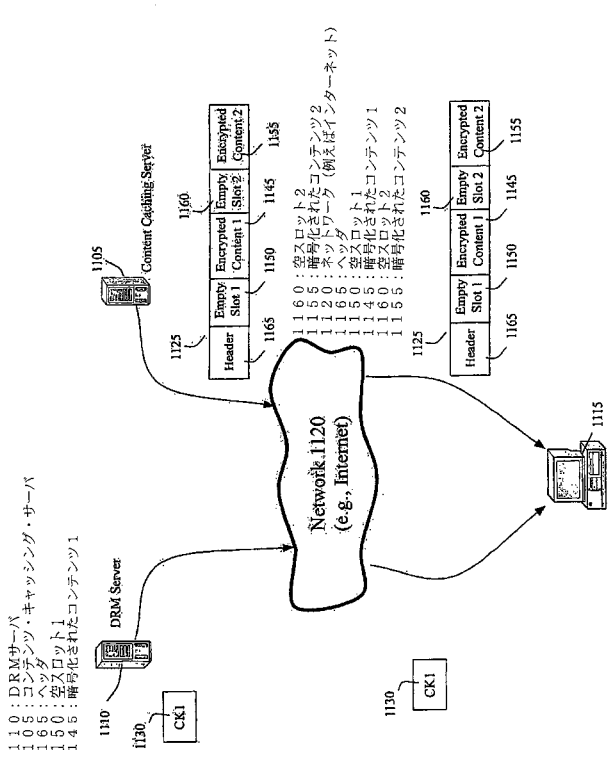
【図１１】



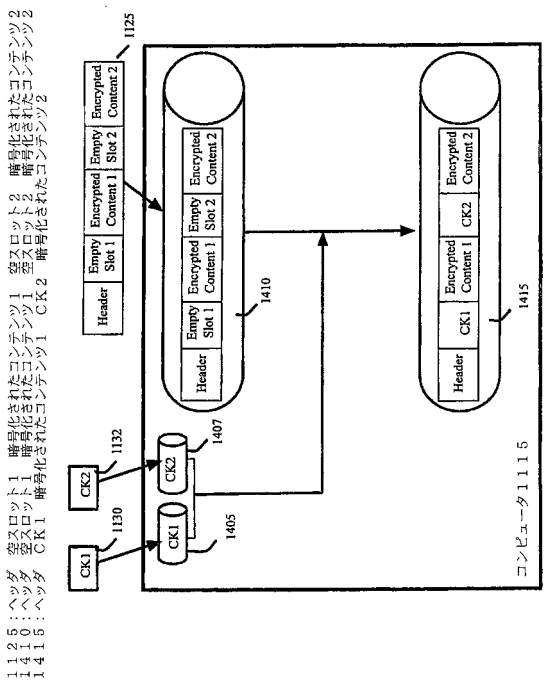
【図１２】



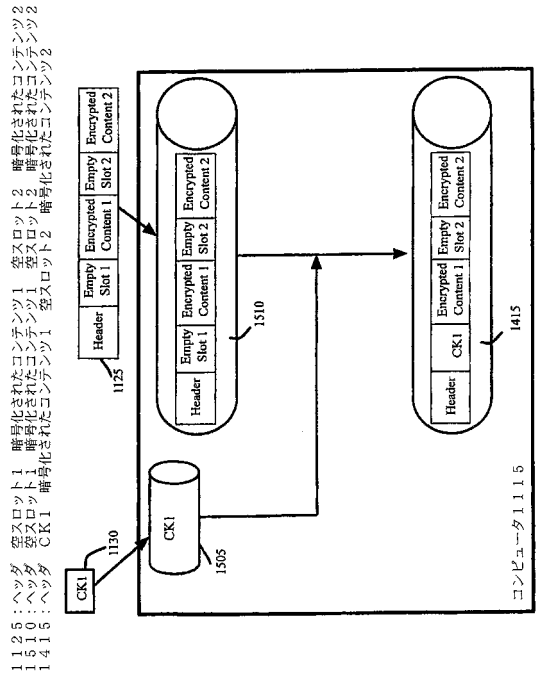
【図１３】



【図１４】

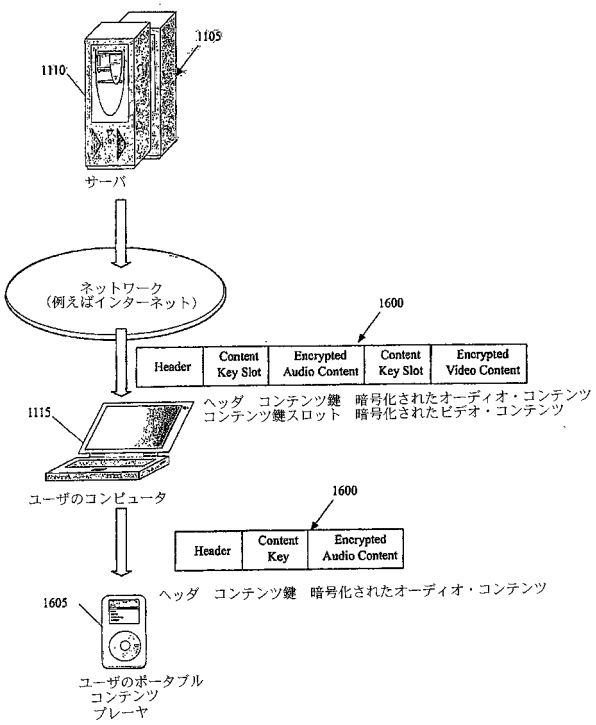


【図１５】

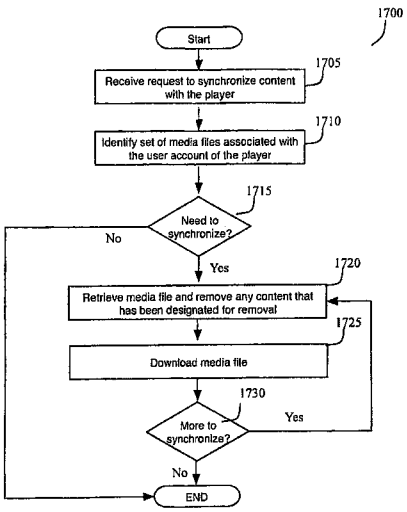


１１２５：ヘッダ　空スロット１　暗号化されたコンテンツ１　空スロット２　暗号化されたコンテンツ２
１５１０：ヘッダ　空スロット１　暗号化されたコンテンツ１　暗号化されたコンテンツ２
１４１５：ヘッダ　ＣＫ１　暗号化されたコンテンツ１　空スロット２　暗号化されたコンテンツ２

【図１６】



【図１７】



１７０５：プレーヤとコンテンツを同期する要求を受信する
１７１０：プレーヤのユーザ・アカウントに関連付けされている
　　メディア・ファイルのセットを識別する
１７１５：同期が必要か？
１７２０：メディア・ファイルを検索し、削除が指定された
　　コンテンツがあれば削除する
１７２５：メディア・ファイルをダウンロードする
１７３０：追加の同期はあるか？

フロントページの続き

(72)発明者　ダウディ，トーマス
アメリカ合衆国・９４０８７・カリフォルニア州・サニイベイル・カムサック　ドライブ・１６１０
(72)発明者　ファゾーリ，ジャンパオロ
アメリカ合衆国・９４３０１・カリフォルニア州・パロアルト・ホーソン　アベニュ・６８４

Ｆターム(参考) 5B017 AA07 BA07 BB09 CA16
5J104 AA16 AA32 EA04 EA08 EA17 JA03 JA21 NA02 NA37 PA14