【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2月1日(2007.2.1)

【公開番号】特開2002-33725(P2002-33725A)
【公開日】平成14年1月31日(2002.1.31)
【出願番号】特願2000-370416(P2000-370416)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｈ　1/00　(2006.01)
Ｈ０４Ｎ　7/173　(2006.01)
Ｈ０４Ｎ　7/167　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｈ　1/00　Ｆ
Ｈ０４Ｎ　7/173　６２０Ａ
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｎ　7/167　Ｚ

【手続補正書】
【提出日】平成18年12月13日(2006.12.13)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンテンツと該コンテンツの視聴のために必要なコンテンツ関連情報であるメタデータとをコンテンツ受信側へ送信する送信方法であって、
イベントを構成するコンテンツを、コンテンツ単位で第１のコンテンツ鍵（Kk）で暗号化して暗号化コンテンツを生成し、送信するステップと、
第１のコンテンツ鍵（Kk）を第１のワーク鍵(Kwc)で暗号化して第１の暗号化コンテンツ鍵（Kk'）を生成して、共通情報として送信するステップと、
コンテンツに関連する内容情報及び制御情報を含むメタデータを第１のワーク鍵(Kwc)で暗号化して暗号化メタデータを生成し、送信するステップと
を含む送信方法。
【請求項２】
コンテンツと該コンテンツの視聴のために必要なコンテンツ関連情報であるメタデータとをコンテンツ受信側へ送信する送信方法であって、
イベントを構成するコンテンツを、コンテンツ単位で第１のコンテンツ鍵（Kk）で暗号化して暗号化コンテンツを生成し、送信するステップと、
コンテンツに関連する内容情報及び制御情報を含むメタデータに第１のコンテンツ鍵(Kk)を含め、第１のワーク鍵(Kwc)で暗号化して暗号化メタデータを生成し、送信するステップと
を含む送信方法。
【請求項３】
第１のワーク鍵(Kwc)は、第１の個人鍵(Kmc)で暗号化されて第１の暗号化ワーク鍵(Kwc')として個別情報として送信されることを特徴とする請求項1又は２に記載の送信方法。

【請求項４】
暗号化されたコンテンツ及びメタデータは、衛星回線又は地上波回線を介してその回線の伝送暗号方式で暗号化された後、伝送されることを特徴とする請求項１乃至３のいずれかに記載の送信方法。
【請求項５】
暗号化コンテンツ及び暗号化メタデータを受信し、該暗号化メタデータを復号化し、該復号化メタデータをもって上記暗号化コンテンツを制御し、該コンテンツの視聴を可能とする受信方法であって、
受信機内に記憶された第１の個人鍵(Kmc)を用いて、受信された第１の暗号化ワーク鍵(Kwc')を復号化して第１のワーク鍵(Kwc)を生成するステップと、
復号化された第１のワーク鍵(Kwc)を用いて、共通情報として受信された第１の暗号化コンテンツ鍵（Kk'）を復号化して第１のコンテンツ鍵（Kk）を生成するステップと、
復号化された第１のコンテンツ鍵（Kk）を用いて暗号化コンテンツを復号化してコンテンツを生成するステップと、
暗号化メタデータを第１のワーク鍵(Kwc)で復号化してメタデータを生成するステップと
を含む受信方法。
【請求項６】
暗号化コンテンツ及び暗号化メタデータを受信し、該暗号化メタデータを復号化し、該復号化メタデータをもって上記暗号化コンテンツを制御し、該コンテンツの視聴を可能とする受信方法であって、
受信機内に記憶された第１の個人鍵(Kmc)を用いて、上記暗号化コンテンツ及び暗号化メタデータとともに受信された第１の暗号化ワーク鍵(Kwc')を復号化し第１のワーク鍵(Kwc)を生成するステップと、
復号化された第１のワーク鍵(Kwc)を用いて、暗号化メタデータを復号化し、そこに含まれた第１のコンテンツ鍵（Kk）を求めるステップと、
求められた第１のコンテンツ鍵（Kk）を用いて暗号化コンテンツを復号化してコンテンツを生成するステップと
を含む受信方法。
【請求項７】
メタデータに第１のコンテンツ鍵(Kk)を含めるステップと、
第１の再暗号化鍵(Kt)を生成するステップと、
メタデータを第１の再暗号化鍵(Kt)で暗号化して暗号化メタデータを生成するステップと、
第１のコンテンツ鍵(Kk)で暗号化された暗号化コンテンツ及び生成された暗号化メタデータを記録媒体に蓄積するステップと
をさらに含む請求項５又は６に記載の受信方法。
【請求項８】
メタデータから検索処理に用いられる情報を抽出し、検索テーブルに記憶するステップをさらに含む請求項５乃至７のいずれかに記載の受信方法。
【請求項９】
選択されたコンテンツに対応する暗号化メタデータを第１の再暗号化鍵（Kt）で復号するステップと、
復号メタデータに基づきコンテンツの視聴可否を判断し、課金情報を含む契約情報を作成し、復号メタデータに含めるステップと、
復号メタデータを第１及び第２の分離メタデータに分離するステップと、
第２の再暗号化鍵(Kt')を生成するステップと、
第２の分離メタデータを第２の再暗号化鍵(Kt')で暗号化した第２の分離メタデータを生成し、記録媒体に蓄積するステップと、
第１の分離メタデータに第２の再暗号化鍵(Kt')を含め、入力された第３の個人鍵(Km2)

で暗号化し、第３の個人鍵(Km2)及び第３の個人鍵(Km2)で暗号化された第１の分離メタデータを第２のモジュールに記録するステップと
を含む請求項５乃至８のいずれかに記載の受信方法。
【請求項１０】
暗号化された第２の分離メタデータを、さらにリムーバブルメディアに蓄積するステップと、記録媒体に蓄積された暗号化コンテンツをリムーバブルメディアに蓄積するステップとを含む請求項５乃至９のいずれかに記載の受信方法。
【請求項１１】
メタデータは、検索情報及び／又は課金情報を含む契約情報を含み、契約情報に従い、コンテンツ毎に課金処理を行うことを特徴とする請求項９又は１０に記載の受信方法。
【請求項１２】
リムーバブルメディアに記録された暗号化された第２の分離データを復号化し、第２の分離メタデータを生成するステップと、
第２のモジュールに記録された暗号化された第１の分離メタデータを復号化し、第１の分離メタデータを生成するステップと、
第１及び第２の分離メタデータに基づき、コンテンツの視聴可否を判断するステップと、
リムーバブルメディアに記録された暗号化コンテンツを、コンテンツ鍵で復号化してコンテンツを生成するステップと
を含む請求項１０又は１１に記載の受信方法。
【請求項１３】
第１のモジュールは受信機内に備えられ、第２のモジュールは可搬形で受信機に脱着可能であることを特徴とする請求項１乃至１２のいずれかに記載の受信方法。
【請求項１４】
ECMもしくはメタデータに第１のコンテンツ鍵（Kk）に関連する情報を記載し、その情報を元に第１のコンテンツ鍵（Kk）を取得するステップとをさらに含む請求項５又は６に記載の受信方法。
【請求項１５】
コンテンツと該コンテンツの視聴のために必要なコンテンツ関連情報であるメタデータとを送信するコンテンツ送信装置であって、
イベントを構成するコンテンツを、コンテンツ単位で第１のコンテンツ鍵（Kk）で暗号化して暗号化コンテンツを生成し、送信する手段と、
第１のコンテンツ鍵（Kk）を第１のワーク鍵(Kwc)で暗号化して第１の暗号化コンテンツ鍵（Kk'）を生成して、共通情報として送信する手段と、
コンテンツに関連する内容情報及び制御情報を含むメタデータを第１のワーク鍵(Kwc)で暗号化して暗号化メタデータを生成し、送信する手段と
を備えたコンテンツ送信装置。
【請求項１６】
暗号化コンテンツ及び暗号化メタデータを受信し、該暗号化メタデータを復号化し、該復号化メタデータをもって上記暗号化コンテンツを制御し、該コンテンツの視聴を可能とするコンテンツ受信装置であって、
受信機内に記憶された第１の個人鍵(Kmc)を用いて、上記暗号化コンテンツ及び暗号化メタデータとともに受信された第１の暗号化ワーク鍵(Kwc')を復号化し第１のワーク鍵(Kwc)を生成する手段と、
復号化された第１のワーク鍵(Kwc)を用いて、暗号化メタデータを復号化し、そこに含まれた第１のコンテンツ鍵（Kk）を求める手段と、
求められた第１のコンテンツ鍵（Kk）を用いて暗号化コンテンツを復号化してコンテンツを生成する手段と
を備えたコンテンツ受信装置。
【手続補正２】

【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【０００７】
本願発明は、以上のような点に鑑み、コンテンツの蓄積時における暗号化等の鍵の扱いが容易であり、暗号化蓄積時の信頼性向上が図れるコンテンツ送信方法、受信方法等を提供することを目的とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】
本願発明は、コンテンツ鍵を共通情報、例えばECM、またはメタデータに格納し、該コンテンツ鍵をワーク鍵で暗号化して配信する。または、ワーク鍵で暗号化、又は復号化されたコンテンツ鍵を用いて暗号化コンテンツを復号化してコンテンツを生成してなるものである。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】削除
【補正の内容】
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００７９
【補正方法】変更
【補正の内容】
【００７９】
【発明の効果】
本発明によると、コンテンツ蓄積時の暗号鍵、復号鍵の扱いが容易になり、かつ、暗号鍵、復号鍵の信頼性の向上が図れる。