【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23年1月6日(2011.1.6)

【公開番号】特開2006-135931(P2006-135931A)
【公開日】平成18年5月25日(2006.5.25)
【年通号数】公開・登録公報2006-020
【出願番号】特願2005-210643(P2005-210643)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成22年11月15日(2010.11.15)
【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】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報を送受信する方法であって、
前記コンテンツ利用情報を送受信するための暗号通信路を確立する第１ステップと、
前記暗号通信路を用いて前記コンテンツ利用情報を送受信する第２ステップと、を含み、
前記第１ステップは、
前記コンテンツ利用情報の送信元装置が前記コンテンツ利用情報の送信先装置を認証するステップと、
前記送信先装置が承認されたときに、前記送信元装置と前記送信先装置の間で公開鍵暗号方式を用いて第１の対称鍵を共有するステップと、を含み、
前記第２ステップは、
前記コンテンツ利用情報を送信するタイミングが到来したときに、前記送信元装置と前記送信先装置の間で第２の対称鍵を共有するステップと、
前記送信元装置が、前記第１の対称鍵及び前記第２の対称鍵により前記コンテンツ利用情報を暗号化して前記送信先装置へ送信するステップと、を含む
ことを特徴とするコンテンツ利用情報送信方法。
【請求項２】
前記第１ステップは、前記第２の対称鍵を共有するために使用する第３の対称鍵を前記送信元装置と前記送信先装置との間で共有するステップを更に含み、
前記第２の対称鍵を共有するステップは、前記第２の対称鍵を前記第３の対称鍵で暗号化して送受信することにより前記第２の対称鍵を共有することを特徴とする請求項１に記載のコンテンツ利用情報送信方法。
【請求項３】
前記第１の対称鍵は、前記送信元装置及び前記送信先装置のうちいずれか一方が発行し、前記第２の対称鍵は、他方が発行することを特徴とする請求項１又は２に記載のコンテンツ利用情報送信方法。
【請求項４】

前記第２の対称鍵は、前記第２ステップの終了後に、次のコンテンツ利用情報を送信するときには新たに発行され、前記送信元装置及び前記送信先装置の間で共有されることを特徴とする請求項１から３のいずれかに記載のコンテンツ利用情報送信方法。
【請求項５】
前記第１ステップは、前記送信先装置が前記送信元装置を認証するステップを更に含み、
前記送信先装置及び前記送信元装置が互いに承認されたときに、前記第１の対称鍵を交換するステップが実行されることを特徴とする請求項１から４のいずれかに記載のコンテンツ利用情報送信方法。
【請求項６】
前記送信元装置及び前記送信先装置の一方は、ストレージデバイスであることを特徴とする請求項１から５のいずれかに記載のコンテンツ利用情報送信方法。
【請求項７】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、
前記コンテンツ利用情報享受装置から認証情報を取得して、その認証情報の正当性を検証する検証手段と、
前記検証手段が前記コンテンツ利用情報享受装置を承認したときに、前記コンテンツ利用情報享受装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、
前記コンテンツ利用情報を送信するタイミングが到来したときに、前記コンテンツ利用情報享受装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、
前記コンテンツ利用情報を、前記第１の対称鍵及び前記第２の対称鍵により暗号化する暗号化手段と、
前記暗号化手段により暗号化された前記コンテンツ利用情報享受装置へ送信するコンテンツ利用情報送信手段と、
を備えることを特徴とするコンテンツ利用情報提供装置。
【請求項８】
前記第２の対称鍵を交換するために使用する第３の対称鍵を前記コンテンツ利用情報享受装置との間で共有する第３の対称鍵共有手段を更に備え、
前記第２の対称鍵共有手段は、前記第３の対称鍵により暗号化された前記第２の対称鍵を前記コンテンツ利用情報享受装置へ送信又は前記コンテンツ利用情報享受装置から受信することにより、前記第２の対称鍵を前記コンテンツ利用情報享受装置との間で共有することを特徴とする請求項７に記載のコンテンツ利用情報提供装置。
【請求項９】
前記第１の対称鍵は、前記コンテンツ利用情報提供装置及び前記コンテンツ利用情報享受装置のうちいずれか一方が発行したものであり、前記第２の対称鍵は、他方が発行したものであることを特徴とする請求項７又は８に記載のコンテンツ利用情報提供装置。
【請求項１０】
前記第２の対称鍵は、前記コンテンツ利用情報を前記コンテンツ利用情報享受装置へ送信した後に、次のコンテンツ利用情報を送信するときには新たに発行され、前記コンテンツ利用情報享受装置との間で共有されることを特徴とする請求項７から９のいずれかに記載のコンテンツ利用情報提供装置。
【請求項１１】
前記コンテンツ利用情報享受装置に、自身の認証情報を送信する認証情報送信部を更に備え、
前記第１の対称鍵共有手段は、前記検証手段が前記コンテンツ利用情報享受装置を承認し、かつ、前記コンテンツ利用情報享受装置が前記自身の認証情報を承認したときに、前記コンテンツ利用情報享受装置との間で第１の対称鍵を共有することを特徴とする請求項７から１０のいずれかに記載のコンテンツ利用情報提供装置。

【請求項１２】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、
前記コンテンツ利用情報享受装置との間でデータの授受を制御するインタフェースと、
前記コンテンツ利用情報の提供に際して、テンポラルに第１の対称鍵および第２の対称鍵を生成する対称鍵生成部と、
前記コンテンツ利用情報享受装置に設定された第１の公開鍵によって、データを暗号化する第１の暗号部と、
前記コンテンツ利用情報享受装置に設定された第２の公開鍵によって、データを暗号化する第２の暗号部と、
前記コンテンツ利用情報享受装置で生成された第３の対称鍵によって、前記第２の暗号部において暗号化されたデータをさらに暗号化する第３の暗号部と、
前記コンテンツ利用情報享受装置で生成された第４の対称鍵によって、データを暗号化する第４の暗号部と、
前記第２の対称鍵によって、データをさらに暗号化する第５の暗号部と、
第１の対称鍵あるいは第２の対称鍵によって、データを復号する復号部と、
制御部とを備え、
前記制御部は、
前記第１の対称鍵を生成するように前記対称鍵生成部に指示し、
前記第１の公開鍵を前記インタフェースを介して受け取って前記第１の暗号部に与え、
前記第１の公開鍵によって暗号化された前記第１の対称鍵を前記第１の暗号部から受け取って前記インタフェースを介して出力し、
前記第１の対称鍵によって暗号化された前記第３の対称鍵および前記第２の公開鍵を、前記インタフェースを介して受け取って前記復号部に与え、
前記第２の対称鍵を生成し、前記第２の対称鍵を前記第２の暗号部に与えるように前記対称鍵生成部に指示し、
前記第２の公開鍵又は前記第３の対称鍵によって暗号化された前記第２の対称鍵を、前記第２又は第３の暗号部から受け取って前記インタフェースを介して出力し、
前記第１の対称鍵あるいは第２の対称鍵によって暗号化された前記第４の対称鍵を、前記インタフェースを介して前記コンテンツ利用情報享受装置から受け取って前記復号部に与え、
前記第４の対称鍵と前記第２の対称鍵とによって暗号化されたコンテンツ利用情報を前記４の暗号部または前記第５の暗号部から受け取って前記インタフェースを介して出力する、
ことを特徴とするコンテンツ利用情報提供装置。
【請求項１３】
前記制御部は、
同じ前記コンテンツ利用情報享受装置に対して、前記コンテンツ利用情報を連続して提供する処理において、
前記第１の対称鍵あるいは第２の対称鍵によって暗号化された、新たな前記第４の対称鍵を、前記インタフェースを介して受け取って前記復号部に与え、
新たな前記第４の対称鍵と前記第２の対称鍵とによって暗号化されたコンテンツ利用情報を、前記インタフェースを介して出力する
ことを特徴とする請求項１２に記載のコンテンツ利用情報提供装置。
【請求項１４】
前記コンテンツ利用情報提供装置は、
前記コンテンツ利用情報を生成するコンテンツ利用情報生成部と、
前記コンテンツデータを前記コンテンツ鍵によって暗号化し、前記暗号化コンテンツデータを出力するコンテンツデータ暗号部と、
を更に備えることを特徴とする請求項７から１３のいずれかに記載のコンテンツ利用情

報提供装置。
【請求項１５】
前記コンテンツ利用情報提供装置は、
前記暗号化コンテンツデータを格納する第１の格納部と、
前記コンテンツ利用情報を格納する第２の格納部と、を更に備え、
前記第２の格納部は、耐タンパ構造によって構成されることを特徴とする請求項７から１４のいずれかに記載のコンテンツ利用情報提供装置。
【請求項１６】
本コンテンツ利用情報提供装置は、ストレージデバイスであることを特徴とする請求項７から１５のいずれかに記載のコンテンツ利用情報提供装置。
【請求項１７】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報提供装置から享受するコンテンツ利用情報享受装置であって、
前記コンテンツ利用情報提供装置に自身の認証情報を送信する認証情報送信手段と、
前記コンテンツ利用情報提供装置が前記認証情報を承認したときに、前記コンテンツ利用情報提供装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、
前記コンテンツ利用情報を受信するタイミングが到来したときに、前記コンテンツ利用情報提供装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、
前記第１の対称鍵及び前記第２の対称鍵により暗号化された前記コンテンツ利用情報を前記コンテンツ利用情報提供装置から受信するコンテンツ利用情報受信手段と、
前記暗号化された前記コンテンツ利用情報を前記第１の対称鍵及び前記第２の対称鍵により復号する復号手段と、
を備えることを特徴とするコンテンツ利用情報享受装置。
【請求項１８】
前記第２の対称鍵を交換するために使用する第３の対称鍵を前記コンテンツ利用情報提供装置との間で共有する第３の対称鍵共有手段を更に備え、
前記第２の対称鍵共有手段は、前記第３の対称鍵により暗号化された前記第２の対称鍵を前記コンテンツ利用情報提供装置へ送信又は前記コンテンツ利用情報提供装置から受信することにより、前記第２の対称鍵を前記コンテンツ利用情報提供装置との間で共有することを特徴とする請求項１７に記載のコンテンツ利用情報享受装置。
【請求項１９】
前記第１の対称鍵は、前記コンテンツ利用情報提供装置及び前記コンテンツ利用情報享受装置のうちいずれか一方が発行したものであり、前記第２の対称鍵は、他方が発行したものであることを特徴とする請求項１７又は１８に記載のコンテンツ利用情報享受装置。
【請求項２０】
前記第２の対称鍵は、前記コンテンツ利用情報を前記コンテンツ利用情報提供装置から受信した後に、次のコンテンツ利用情報を受信するときには新たに発行され、前記コンテンツ利用情報提供装置との間で共有されることを特徴とする請求項１７から１９のいずれかに記載のコンテンツ利用情報享受装置。
【請求項２１】
前記コンテンツ利用情報提供装置から認証情報を取得して、その認証情報の正当性を検証する検証手段を更に備え、
前記第１の対称鍵共有手段は、前記検証手段が前記コンテンツ利用情報提供装置を承認し、かつ、前記コンテンツ利用情報提供装置が自身の認証情報を承認したときに、前記コンテンツ利用情報提供装置との間で第１の対称鍵を共有することを特徴とする請求項１７から２０のいずれかに記載のコンテンツ利用情報享受装置。
【請求項２２】
暗号化コンテンツデータを復号および再生するためのコンテンツ鍵を含むコンテンツ利用情報を記録したコンテンツ利用情報提供装置から享受するコンテンツ利用情報享受装置

であって、
前記コンテンツ利用情報提供装置との間でデータの授受を制御するインタフェースと、
前記コンテンツ利用情報享受装置に設定された第１の公開鍵を保持する第１公開鍵保持部と、
前記第１の公開鍵によって暗号化されたデータを復号するための第１の秘密鍵を保持する第１秘密鍵保持部と、
前記コンテンツ利用情報享受装置に設定された第２の公開鍵を保持する第２公開鍵保持部と、
前記第２の公開鍵によって暗号化されたデータを復号するための第２の秘密鍵を保持する第２秘密鍵保持部と、
前記コンテンツ利用情報提供装置からコンテンツ利用情報の提供を受けるに際し、テンポラルに第１の対称鍵と第２の対称鍵を生成する対称鍵生成部と、
前記コンテンツ利用情報提供装置で生成された第３の対称鍵によって、データを暗号化する暗号部と、
前記第１の公開鍵によって暗号化されたデータを前記第１の秘密鍵によって復号する第１の復号部と、
前記第１の対称鍵によって暗号化されたデータを復号する第２の復号部と、
前記第２の公開鍵によって暗号化されたデータを第２の秘密鍵によって復号する第３の復号部と、
前記第２の対称鍵によって暗号化されたデータを復号する第４の復号部と、
前記コンテンツ利用情報提供装置で生成された第４の対称鍵によってデータを復号する第５の復号部と、
制御部とを備え、
前記制御部は、
前記第１の公開鍵を前記インタフェースを介して出力し、
前記第１の公開鍵によって暗号化された前記第３の対称鍵を、前記インタフェースを介して受け取り、
前記第１の対称鍵を生成し、前記暗号部に与えるように前記対称鍵生成部に指示し、
前記第１の復号部において復号された前記第３の対称鍵により暗号化された前記第１の対称鍵と前記第２の公開鍵とを前記暗号部から受け取って、前記インタフェースを介して出力し、
前記第２の公開鍵または前記第１の対称鍵によって暗号化された第４の対称鍵を、前記インタフェースを介して受け取り、
前記第２の対称鍵を生成し、前記暗号部に与えるように前記対称鍵生成部に指示し、
前記第２の復号部または前記３の復号部において復号された前記第４の対称鍵または前記第３の対称鍵により暗号化された前記第２の対称鍵を前記暗号部から受け取って、前記インタフェースを介して出力し、
前記第２の対称鍵および前記第４の対称鍵によって暗号化されたコンテンツ利用情報を、前記インタフェースを介して受け取る
ことを特徴とするコンテンツ利用情報享受装置。
【請求項２３】
前記制御部は、
前記コンテンツ利用情報を、同じ前記コンテンツ利用情報提供装置から連続して享受する処理において、
新たな前記第２の対称鍵を生成し、前記暗号部に与えるように前記対称鍵生成部に指示し、
前記暗号部において前記第１の対称鍵あるいは前記第４の対称鍵によって暗号化された新たな前記第２の対称鍵を前記インタフェースを介して出力し、
前記第２の対称鍵および前記第４の対称鍵によって暗号化されたコンテンツ利用情報を、前記インタフェースを介して受け取る

ことを特徴とする請求項２２に記載のコンテンツ利用情報享受装置。
【請求項２４】
前記コンテンツ利用情報享受装置は、
前記暗号化コンテンツデータを前記コンテンツ鍵により復号するコンテンツデータ復号部と、
前記コンテンツデータ復号部により復号されたコンテンツデータを再生する再生部と、
を更に備えることを特徴とする請求項１７から２３のいずれかに記載のコンテンツ利用情報享受装置。
【請求項２５】
前記コンテンツ利用情報享受装置は、
前記暗号化コンテンツデータを格納する第１の格納部と、
前記コンテンツ利用情報を格納する第２の格納部とを含み、
前記第２の格納部は、耐タンパ構造によって構成されることを特徴とする請求項１７から２４のいずれかに記載のコンテンツ利用情報享受装置。
【請求項２６】
本コンテンツ利用情報享受装置は、ストレージデバイスであることを特徴とする請求項１７から２５のいずれかに記載のコンテンツ利用情報享受装置。