【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３区分
【発行日】平成18年5月11日(2006.5.11)

【公開番号】特開2001-175605(P2001-175605A)
【公開日】平成13年6月29日(2001.6.29)
【出願番号】特願平11-359896
【国際特許分類】
Ｇ０６Ｆ　21/00　(2006.01)
Ｈ０４Ｈ　1/00　(2006.01)
Ｈ０４Ｎ　7/173　(2006.01)
Ｇ１０Ｌ　11/00　(2006.01)
Ｈ０４Ｌ　9/10　(2006.01)
Ｈ０４Ｎ　7/167　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　３３０Ｚ
Ｈ０４Ｈ　1/00　Ｆ
Ｈ０４Ｎ　7/173　６４０Ａ
Ｇ１０Ｌ　9/00　Ｅ
Ｈ０４Ｌ　9/00　６２１Ａ
Ｈ０４Ｎ　7/167　Ｚ

【手続補正書】
【提出日】平成18年3月17日(2006.3.17)
【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】
コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、
前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、
前記決定の結果を示す履歴データを生成する履歴データ生成手段と、
前記コンテンツ鍵データを復号する復号手段と
を耐タンパ性の回路モジュール内に有する
データ処理装置。
【請求項２】
前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、
前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と
を前記耐タンパ性の回路モジュール内にさらに有する
請求項１に記載のデータ処理装置。
【請求項３】
前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらに行い、

前記データ処理装置は、
前記署名データの正当性を検証する署名処理手段
を耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う
請求項１に記載のデータ処理装置。
【請求項４】
前記入力処理手段は、前記コンテンツデータの署名データを入力する処理をさらに行い、
前記データ処理装置は、
前記署名データの正当性を検証する署名処理手段
を耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う
請求項１に記載のデータ処理装置。
【請求項５】
前記入力処理手段は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて秘密鍵データを用いて作成された署名データと、前記秘密鍵データに対応する公開鍵データとを入力する処理をさらに行い、
前記データ処理装置は、
前記公開鍵データを用いて、前記署名データの正当性を検証する署名処理手段を前記耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う
請求項１に記載のデータ処理装置。
【請求項６】
前記コンテンツ鍵データは、ライセンス鍵データを用いて暗号化されており、
前記データ処理装置は、
前記ライセンス鍵データを記憶する記憶手段
をさらに有し、
前記復号手段は、前記記憶手段から読み出した前記ライセンス鍵データを用いて前記コンテンツ鍵データを復号する
請求項１に記載のデータ処理装置。
【請求項７】
前記データ処理装置は、他の装置との間で、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一のデータをオンラインで送受信する場合に、前記他の装置との間で相互認証を行う相互認証手段と、
前記相互認証によって得られたセッション鍵データを用いて、前記送受信を行うデータの暗号化および復号を行う暗号化・復号手段と
を前記耐タンパ性の回路モジュール内にさらに有する
請求項１に記載のデータ処理装置。
【請求項８】
コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、
当該データ処理装置の秘密鍵データを記憶する記憶回路と、
前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、
前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、
前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、
前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路と
を耐タンパ性の回路モジュール内に有するデータ処理装置。
【請求項９】
コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、
他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、
前記相互認証を行うために乱数を生成する乱数生成回路と、
演算処理回路と、
データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、
前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路と
を耐タンパ性の回路モジュール内に有するデータ処理装置。
【請求項１０】
ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、
他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、
他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、
前記相互認証を行うために乱数を生成する乱数生成回路と、
演算処理回路と、
前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路と
を耐タンパ性の回路モジュール内に有するデータ処理装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】削除
【補正の内容】
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】削除
【補正の内容】
【手続補正４】

【補正対象書類名】明細書
【補正対象項目名】００１７
【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】００１８
【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】００１９
【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】００２０
【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】００２１
【補正方法】削除
【補正の内容】
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】削除
【補正の内容】
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】削除
【補正の内容】
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】削除
【補正の内容】
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】削除
【補正の内容】
【手続補正１４】

【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】削除
【補正の内容】
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】削除
【補正の内容】
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】削除
【補正の内容】
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００３０
【補正方法】削除
【補正の内容】
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】削除
【補正の内容】
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】００３２
【補正方法】変更
【補正の内容】
【００３２】
本発明のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有する。
【手続補正２０】

【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】削除
【補正の内容】
【手続補正２１】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】削除
【補正の内容】
【手続補正２２】
【補正対象書類名】明細書
【補正対象項目名】００３５
【補正方法】削除
【補正の内容】
【手続補正２３】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】削除
【補正の内容】
【手続補正２４】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】削除
【補正の内容】
【手続補正２５】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】削除
【補正の内容】
【手続補正２６】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】削除
【補正の内容】
【手続補正２７】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】削除
【補正の内容】
【手続補正２８】
【補正対象書類名】明細書
【補正対象項目名】００４１
【補正方法】削除
【補正の内容】
【手続補正２９】
【補正対象書類名】明細書
【補正対象項目名】００４２
【補正方法】削除
【補正の内容】
【手続補正３０】

【補正対象書類名】明細書
【補正対象項目名】００４３
【補正方法】削除
【補正の内容】
【手続補正３１】
【補正対象書類名】明細書
【補正対象項目名】００４４
【補正方法】削除
【補正の内容】
【手続補正３２】
【補正対象書類名】明細書
【補正対象項目名】００４５
【補正方法】削除
【補正の内容】
【手続補正３３】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】削除
【補正の内容】
【手続補正３４】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】変更
【補正の内容】
【００４７】
また、本発明のデータ処理装置は、コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有する。
【手続補正３５】
【補正対象書類名】明細書
【補正対象項目名】００４８
【補正方法】削除
【補正の内容】
【手続補正３６】
【補正対象書類名】明細書
【補正対象項目名】００４９
【補正方法】変更
【補正の内容】
【００４９】
また、本発明のデータ処理装置は、ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記

記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。
【手続補正３７】
【補正対象書類名】明細書
【補正対象項目名】００５０
【補正方法】削除
【補正の内容】
【手続補正３８】
【補正対象書類名】明細書
【補正対象項目名】００５１
【補正方法】削除
【補正の内容】
【手続補正３９】
【補正対象書類名】明細書
【補正対象項目名】００５２
【補正方法】削除
【補正の内容】
【手続補正４０】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】削除
【補正の内容】