【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17年10月27日(2005.10.27)

【公開番号】特開2004-72134(P2004-72134A)
【公開日】平成16年3月4日(2004.3.4)
【年通号数】公開・登録公報2004-009
【出願番号】特願2002-224321(P2002-224321)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/08
　Ｇ０９Ｃ　 1/00
　Ｇ１１Ｂ　20/10
　Ｈ０４Ｌ　 9/10
　Ｈ０４Ｌ　 9/32
　Ｈ０４Ｎ　 5/91
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６０１Ａ
　Ｇ０９Ｃ　 1/00　　６４０Ｅ
　Ｇ１１Ｂ　20/10　　Ｄ
　Ｇ１１Ｂ　20/10　　Ｈ
　Ｇ１１Ｂ　20/10　　３２１Ｚ
　Ｈ０４Ｌ　 9/00　　６７３Ｂ
　Ｈ０４Ｌ　 9/00　　６２１Ａ
　Ｈ０４Ｎ　 5/91　　Ｐ

【手続補正書】
【提出日】平成17年7月29日(2005.7.29)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】情報処理システム、記録媒体再生装置および記録媒体再生方法、情報処理装置および方法、プログラム格納媒体、情報記録媒体、並びにプログラム
【手続補正２】
【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】
　記録媒体を再生する記録媒体再生装置と、前記記録媒体再生装置との間で情報を授受する情報処理装置からなる情報処理システムにおいて、
　前記記録媒体再生装置は、
　　前記記録媒体再生装置を証明する証明書を取得する第１の取得手段と、
　　前記記録媒体に固有の記録媒体ＩＤを、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化する第１の暗号化手段と、
　　前記記録媒体ＩＤを、前記記録媒体再生装置が有する第３の鍵で暗号化する第２の暗号化手段と、
　　前記第１の取得手段により取得した前記記録媒体再生装置の証明書、前記第１の暗号

化手段により暗号化された記録媒体ＩＤ、および前記第２の暗号化手段により暗号化された記録媒体ＩＤを前記情報処理装置へ送信する送信手段とを備え、
前記情報処理装置は、
前記記録媒体再生装置の前記送信手段が送信した前記第１の取得手段により取得した前記記録媒体再生装置の証明書、前記第１の暗号化手段により暗号化された記録媒体ＩＤ、および前記第２の暗号化手段により暗号化された記録媒体ＩＤを取得する第２の取得手段と、
前記記録媒体再生装置から送信され、前記第２の取得手段により取得された、前記第１の暗号化手段により暗号化された記録媒体ＩＤを前記情報処理装置が有する前記第１の鍵で復号する第１の復号手段と、
前記記録媒体再生装置から送信され、前記第２の取得手段により取得された、前記第２の暗号化手段により暗号化された記録媒体ＩＤを、前記情報処理装置が有する第４の鍵で復号する第２の復号手段と、
前記第１の復号手段により取得された記録媒体ＩＤと、前記第２の復号手段により取得された記録媒体ＩＤが同一であるか否かを判定する判定手段と、
前記判定手段により、前記第１の復号手段により取得された記録媒体ＩＤと、前記第２の復号手段により取得された記録媒体ＩＤが同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする情報処理システム。
【請求項２】
前記記録媒体再生装置を証明する証明書と、前記情報処理装置を証明する証明書を発行する認証装置をさらに備え、
前記記録媒体再生装置を証明する証明書は、前記記録媒体再生装置の証明内容を、前記認証装置が有する秘密鍵により暗号化したものであり、
前記情報処理装置を証明する証明書は、前記情報処理装置の証明内容を、前記認証装置が有する前記秘密鍵により暗号化したものである
ことを特徴とする請求項１に記載の情報処理システム。
【請求項３】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置において、
前記記録媒体再生装置を証明する証明書を取得する取得手段と、
前記記録媒体に固有の記録媒体ＩＤを、情報処理装置が有する第１の鍵に対応する第２の鍵を用いて暗号化する第１の暗号化手段と、
前記記録媒体ＩＤを、前記記録媒体再生装置が有する第３の鍵を用いて暗号化する第２の暗号化手段と、
前記取得手段により取得した前記記録媒体再生装置の証明書、前記第１の暗号化手段により暗号化された記録媒体ＩＤ、および前記第２の暗号化手段により暗号化された記録媒体ＩＤを、前記情報処理装置へ送信する送信手段と
を備えることを特徴とする記録媒体再生装置。
【請求項４】
前記記録媒体再生装置を証明する前記証明書は、前記記録媒体再生装置の電子証明書であり、
前記第１の鍵は、前記情報処理装置の秘密鍵であり、
前記第２の鍵は、前記情報処理装置の公開鍵であり、
前記第３の鍵は、前記記録媒体再生装置の秘密鍵である
ことを特徴とする請求項３に記載の記録媒体再生装置。
【請求項５】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置の記録媒体再生方法において、
前記記録媒体再生装置を証明する証明書を取得する取得ステップと、
前記記録媒体に固有の記録媒体ＩＤを、情報処理装置が有する第１の鍵に対応する第２

の鍵を用いて暗号化する第１の暗号化ステップと、
前記記録媒体ＩＤを、前記記録媒体再生装置が有する第３の鍵を用いて暗号化する第２の暗号化ステップと、
前記取得ステップの処理により取得した前記記録媒体再生装置の証明書、前記第１の暗号化ステップの処理により暗号化された記録媒体ＩＤ、および前記第２の暗号化ステップの処理により暗号化された記録媒体ＩＤを、前記情報処理装置へ送信する送信ステップと
を含むことを特徴とする記録媒体再生方法。
【請求項６】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するプログラムであって、
前記記録媒体再生装置を証明する証明書を取得する取得ステップと、
前記記録媒体に固有の記録媒体ＩＤを、情報処理装置が有する第１の鍵に対応する第２の鍵を用いて暗号化する第１の暗号化ステップと、
前記記録媒体ＩＤを、前記記録媒体再生装置が有する第３の鍵を用いて暗号化する第２の暗号化ステップと、
前記取得ステップの処理により取得した前記記録媒体再生装置の証明書、前記第１の暗号化ステップの処理により暗号化された記録媒体ＩＤ、および前記第２の暗号化ステップの処理により暗号化された記録媒体ＩＤを、前記情報処理装置へ送信する送信ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項７】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するコンピュータに、
前記記録媒体再生装置を証明する証明書を取得する取得ステップと、
前記記録媒体に固有の記録媒体ＩＤを、情報処理装置が有する第１の鍵に対応する第２の鍵を用いて暗号化する第１の暗号化ステップと、
前記記録媒体ＩＤを、前記記録媒体再生装置が有する第３の鍵を用いて暗号化する第２の暗号化ステップと、
前記取得ステップの処理により取得した前記記録媒体再生装置の証明書、前記第１の暗号化ステップの処理により暗号化された記録媒体ＩＤ、および前記第２の暗号化ステップの処理により暗号化された記録媒体ＩＤを、前記情報処理装置へ送信する送信ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項８】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置において、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記記録媒体に固有の記録媒体ＩＤ、および前記記録媒体再生装置が有する第３の鍵で暗号化された前記記録媒体ＩＤを取得する取得手段と、
前記取得手段により取得された、前記情報処理装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている記録媒体ＩＤを、前記第１の鍵で復号する第１の復号手段と、
前記取得手段により取得された、前記記録媒体再生装置が有する第３の鍵を用いて暗号化されている記録媒体ＩＤを、第４の鍵で復号する第２の復号手段と、
前記第１の復号手段により取得された記録媒体ＩＤと、前記第２の復号手段により取得された記録媒体ＩＤが同一であるか否かを判定する判定手段と、
前記判定手段により、前記第１の復号手段により取得された記録媒体ＩＤと、前記第２の復号手段により取得された記録媒体ＩＤが同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする情報処理装置。
【請求項９】

前記記録媒体再生装置を証明する前記証明書は、前記記録媒体再生装置の電子証明書であり、
前記第１の鍵は、前記情報処理装置の秘密鍵であり、
前記第２の鍵は、前記情報処理装置の公開鍵であり、
前記第３の鍵は、前記記録媒体再生装置の秘密鍵であり、
前記第４の鍵は、前記記録媒体再生装置の公開鍵である
ことを特徴とする請求項８に記載の記録媒体再生装置。
【請求項１０】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置の情報処理方法において、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記記録媒体に固有の記録媒体ＩＤ、および前記記録媒体再生装置が有する第３の鍵で暗号化された前記記録媒体ＩＤを取得する取得ステップと、
前記取得ステップの処理により取得された、前記情報処理装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている記録媒体ＩＤを、前記第１の鍵で復号する第１の復号ステップと、
前記取得ステップの処理により取得された、前記記録媒体再生装置が有する第３の鍵を用いて暗号化されている記録媒体ＩＤを、第４の鍵で復号する第２の復号ステップと、
前記第１の復号ステップの処理により取得された記録媒体ＩＤと、前記第２の復号ステップの処理により取得された記録媒体ＩＤが同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記第１の復号ステップの処理により取得された記録媒体ＩＤと、前記第２の復号ステップの処理により取得された記録媒体ＩＤが同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とする情報処理方法。
【請求項１１】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置を制御するプログラムであって、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記記録媒体に固有の記録媒体ＩＤ、および前記記録媒体再生装置が有する第３の鍵で暗号化された前記記録媒体ＩＤを取得する取得ステップと、
前記取得ステップの処理により取得された、前記情報処理装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている記録媒体ＩＤを、前記第１の鍵で復号する第１の復号ステップと、
前記取得ステップの処理により取得された、前記記録媒体再生装置が有する第３の鍵を用いて暗号化されている記録媒体ＩＤを、第４の鍵で復号する第２の復号ステップと、
前記第１の復号ステップの処理により取得された記録媒体ＩＤと、前記第２の復号ステップの処理により取得された記録媒体ＩＤが同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記第１の復号ステップの処理により取得された記録媒体ＩＤと、前記第２の復号ステップの処理により取得された記録媒体ＩＤが同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項１２】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置を制御するコンピュータに、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記情報

処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記記録媒体に固有の記録媒体ＩＤ、および前記記録媒体再生装置が有する第３の鍵で暗号化された前記記録媒体ＩＤを取得する取得ステップと、
前記取得ステップの処理により取得された、前記情報処理装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている記録媒体ＩＤを、前記第１の鍵で復号する第１の復号ステップと、
前記取得ステップの処理により取得された、前記記録媒体再生装置が有する第３の鍵を用いて暗号化されている記録媒体ＩＤを、第４の鍵で復号する第２の復号ステップと、
前記第１の復号ステップの処理により取得された記録媒体ＩＤと、前記第２の復号ステップの処理により取得された記録媒体ＩＤが同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記第１の復号ステップの処理により取得された記録媒体ＩＤと、前記第２の復号ステップの処理により取得された記録媒体ＩＤが同一であると判定された場合、所定の処理を実行する実行ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項１３】
情報を処理する情報処理装置と、記録媒体を再生し、前記情報処理装置との間で情報を授受する記録媒体再生装置からなる情報処理システムにおいて、
前記情報処理装置は、
前記情報処理装置を証明する証明書を取得する第１の取得手段と、
共通鍵を生成する共通鍵生成手段と、
前記共通鍵生成手段により生成された前記共通鍵を、前記記録媒体再生装置が有する第１の鍵に対応する第２の鍵で暗号化する第１の暗号化手段と、
前記共通鍵を、前記情報処理装置が有する第３の鍵で暗号化する第２の暗号化手段と、
前記第１の取得手段により取得した前記情報処理装置の証明書、前記第１の暗号化手段により暗号化された共通鍵、および前記第２の暗号化手段により暗号化された共通鍵を前記記録媒体再生装置へ送信する送信手段とを備え、
前記記録媒体再生装置は、
前記情報処理装置の前記送信手段が送信した前記第１の取得手段により取得した前記情報処理装置の証明書、前記第１の暗号化手段により暗号化された共通鍵、および前記第２の暗号化手段により暗号化された共通鍵を取得する第２の取得手段と、
前記情報処理装置から送信され、前記第２の取得手段により取得された、前記第１の暗号化手段により暗号化された共通鍵を前記記録媒体再生装置が有する前記第１の鍵で復号する第１の復号手段と、
前記情報処理装置から送信され、前記第２の取得手段により取得された、前記第２の暗号化手段により暗号化された共通鍵を、前記記録媒体再生装置が有する第４の鍵で復号する第２の復号手段と、
前記第１の復号手段により取得された共通鍵と、前記第２の復号手段により取得された共通鍵が同一であるか否かを判定する判定手段と、
前記判定手段により、前記第１の復号手段により取得された共通鍵と、前記第２の復号手段により取得された共通鍵が同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする情報処理システム。
【請求項１４】
前記情報処理装置を証明する証明書と、前記記録媒体再生装置を証明する証明書を発行する認証装置をさらに備え、
前記情報処理装置を証明する証明書は、前記情報処理装置の証明内容を、前記認証装置が有する前記秘密鍵により暗号化したものであり、
前記記録媒体再生装置を証明する証明書は、前記記録媒体再生装置の証明内容を、前記

認証装置が有する秘密鍵により暗号化したものである
ことを特徴とする請求項１３に記載の情報処理システム。
【請求項１５】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置において、
前記情報処理装置を証明する証明書を取得する取得手段と、
共通鍵を生成する共通鍵生成手段と、
前記共通鍵生成手段により生成された前記共通鍵を、前記記録媒体再生装置が有する第１の鍵に対応する第２の鍵で暗号化する第１の暗号化手段と、
前記共通鍵を、前記情報処理装置が有する第３の鍵で暗号化する第２の暗号化手段と、
前記取得手段により取得した前記情報処理装置の証明書、前記第１の暗号化手段により暗号化された共通鍵、および前記第２の暗号化手段により暗号化された共通鍵を前記記録媒体再生装置へ送信する送信手段と
を備えることを特徴とする情報処理装置。
【請求項１６】
前記情報処理装置を証明する前記証明書は、前記情報処理装置の電子証明書であり、
前記第１の鍵は、前記記録媒体再生装置の秘密鍵であり、
前記第２の鍵は、前記記録媒体再生装置の公開鍵であり、
前記第３の鍵は、前記情報処理装置の秘密鍵である
ことを特徴とする請求項１５に記載の情報処理装置。
【請求項１７】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置の情報処理方法において、
前記情報処理装置を証明する証明書を取得する取得ステップと、
共通鍵を生成する共通鍵生成ステップと、
前記共通鍵生成ステップの処理により生成された前記共通鍵を、前記記録媒体再生装置が有する第１の鍵に対応する第２の鍵で暗号化する第１の暗号化ステップと、
前記共通鍵を、前記情報処理装置が有する第３の鍵で暗号化する第２の暗号化ステップと、
前記取得ステップの処理により取得した前記情報処理装置の証明書、前記第１の暗号化ステップの処理により暗号化された共通鍵、および前記第２の暗号化ステップの処理により暗号化された共通鍵を前記記録媒体再生装置へ送信する送信ステップと
を含むことを特徴とする情報処理方法。
【請求項１８】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置情報を処理する情報処理装置を制御するプログラムであって、
前記情報処理装置を証明する証明書を取得する取得ステップと、
共通鍵を生成する共通鍵生成ステップと、
前記共通鍵生成ステップの処理により生成された前記共通鍵を、前記記録媒体再生装置が有する第１の鍵に対応する第２の鍵で暗号化する第１の暗号化ステップと、
前記共通鍵を、前記情報処理装置が有する第３の鍵で暗号化する第２の暗号化ステップと、
前記取得ステップの処理により取得した前記情報処理装置の証明書、前記第１の暗号化ステップの処理により暗号化された共通鍵、および前記第２の暗号化ステップの処理により暗号化された共通鍵を前記記録媒体再生装置へ送信する送信ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項１９】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置情報を処理する情報処理装置を制御するコンピュータに、
前記情報処理装置を証明する証明書を取得する取得ステップと、

共通鍵を生成する共通鍵生成ステップと、
前記共通鍵生成ステップの処理により生成された前記共通鍵を、前記記録媒体再生装置が有する第１の鍵に対応する第２の鍵で暗号化する第１の暗号化ステップと、
前記共通鍵を、前記情報処理装置が有する第３の鍵で暗号化する第２の暗号化ステップと、
前記取得ステップの処理により取得した前記情報処理装置の証明書、前記第１の暗号化ステップの処理により暗号化された共通鍵、および前記第２の暗号化ステップの処理により暗号化された共通鍵を前記記録媒体再生装置へ送信する送信ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項２０】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置において、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記情報処理装置に固有の共通鍵、および前記情報処理装置が有する第３の鍵で暗号化された前記共通鍵を取得する取得手段と、
前記取得手段により取得された、前記記録媒体再生装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている共通鍵を、前記第１の鍵で復号する第１の復号手段と、
前記取得手段により取得された、前記情報処理装置が有する第３の鍵を用いて暗号化されている共通鍵を、第４の鍵で復号する第２の復号手段と、
前記第１の復号手段により取得された共通鍵と、前記第２の復号手段により取得された共通鍵が同一であるか否かを判定する判定手段と、
前記判定手段により、前記第１の復号手段により取得された共通鍵と、前記第２の復号手段により取得された共通鍵が同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする記録媒体再生装置。
【請求項２１】
前記情報処理装置を証明する前記証明書は、前記情報処理装置の電子証明書であり、
前記第１の鍵は、前記記録媒体再生装置の秘密鍵であり、
前記第２の鍵は、前記記録媒体再生装置の公開鍵であり、
前記第３の鍵は、前記情報処理装置の秘密鍵であり、
前記第４の鍵は、前記情報処理装置の公開鍵である
ことを特徴とする請求項２０に記載の記録媒体再生装置。
【請求項２２】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置の記録媒体再生方法において、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記情報処理装置に固有の共通鍵、および前記情報処理装置が有する第３の鍵で暗号化された前記共通鍵を取得する取得ステップと、
前記取得ステップの処理により取得された、前記記録媒体再生装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている共通鍵を、前記第１の鍵で復号する第１の復号ステップと、
前記取得ステップの処理により取得された、前記情報処理装置が有する第３の鍵を用いて暗号化されている共通鍵を、第４の鍵で復号する第２の復号ステップと、
前記第１の復号ステップの処理により取得された共通鍵と、前記第２の復号ステップの処理により取得された共通鍵が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記第１の復号ステップの処理により取得された共通鍵と、前記第２の復号ステップの処理により取得された共通鍵が同一であると判定された場合、所定の処理を実行する実行ステップと

を含むことを特徴とする記録媒体再生方法。
【請求項２３】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するプログラムであって、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記情報処理装置に固有の共通鍵、および前記情報処理装置が有する第３の鍵で暗号化された前記共通鍵を取得する取得ステップと、
前記取得ステップの処理により取得された、前記記録媒体再生装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている共通鍵を、前記第１の鍵で復号する第１の復号ステップと、
前記取得ステップの処理により取得された、前記情報処理装置が有する第３の鍵を用いて暗号化されている共通鍵を、第４の鍵で復号する第２の復号ステップと、
前記第１の復号ステップの処理により取得された共通鍵と、前記第２の復号ステップの処理により取得された共通鍵が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記第１の復号ステップの処理により取得された共通鍵と、前記第２の復号ステップの処理により取得された共通鍵が同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項２４】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するコンピュータに、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化された前記情報処理装置に固有の共通鍵、および前記情報処理装置が有する第３の鍵で暗号化された前記共通鍵を取得する取得ステップと、
前記取得ステップの処理により取得された、前記記録媒体再生装置が有する前記第１の鍵に対応する前記第２の鍵を用いて暗号化されている共通鍵を、前記第１の鍵で復号する第１の復号ステップと、
前記取得ステップの処理により取得された、前記情報処理装置が有する第３の鍵を用いて暗号化されている共通鍵を、第４の鍵で復号する第２の復号ステップと、
前記第１の復号ステップの処理により取得された共通鍵と、前記第２の復号ステップの処理により取得された共通鍵が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記第１の復号ステップの処理により取得された共通鍵と、前記第２の復号ステップの処理により取得された共通鍵が同一であると判定された場合、所定の処理を実行する実行ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項２５】
情報を処理する情報処理装置と、記録媒体を再生し、前記情報処理装置との間で情報を授受する記録媒体再生装置からなる情報処理システムにおいて、
前記情報処理装置は、
前記情報処理装置を証明する証明書を取得する第１の取得手段と、
前記情報を共通鍵で暗号化する第１の暗号化手段と、
前記情報に所定の演算を施して、演算値を生成する第１の演算手段と、
前記第１の暗号化手段により暗号化した前記情報、前記第１の取得手段により取得した前記情報処理装置の証明書、および前記第１の演算手段により生成された前記演算値を送信する送信手段とを備え、
前記記録媒体再生装置は、
前記情報処理装置の前記送信手段が送信した前記第１の取得手段により取得した前記

情報処理装置の証明書、前記第１の暗号化手段により暗号化された前記情報、および前記第１の演算手段により生成された前記演算値を取得する第２の取得手段と、

前記情報処理装置から送信され、前記第２の取得手段により取得された前記第１の暗号化手段により暗号化された前記情報を、前記記録媒体再生装置が有する前記共通鍵で復号する復号手段と、

前記復号手段により復号された前記情報に所定の演算を施して、演算値を生成する第２の演算手段と、

前記情報処理装置から送信され、前記第２の取得手段により取得された前記第１の演算手段により生成された前記演算値と、前記第２の演算手段により生成された前記演算値が同一であるか否かを判定する判定手段と、

前記判定手段により、前記第１の演算手段により生成された前記演算値と、前記第２の演算手段により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行手段と

を備えることを特徴とする情報処理システム。

【請求項２６】

記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置において、

前記情報処理装置を証明する証明書を取得する取得手段と、

前記情報を共通鍵で暗号化する暗号化手段と、

前記情報に所定の演算を施して、演算値を生成する演算手段と、

前記暗号化手段により暗号化した前記情報、前記取得手段により取得した前記情報処理装置の証明書、および前記演算手段により生成された前記演算値を送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項２７】

記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置の情報処理方法において、

前記情報処理装置を証明する証明書を取得する取得ステップと、

前記情報を共通鍵で暗号化する暗号化ステップと、

前記情報に所定の演算を施して、演算値を生成する演算ステップと、

前記暗号化ステップの処理により暗号化した前記情報、前記取得ステップの処理により取得した前記情報処理装置の証明書、および前記演算ステップの処理により生成された前記演算値を送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項２８】

記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置を制御するプログラムであって、

前記情報処理装置を証明する証明書を取得する取得ステップと、

前記情報を共通鍵で暗号化する暗号化ステップと、

前記情報に所定の演算を施して、演算値を生成する演算ステップと、

前記暗号化ステップの処理により暗号化した前記情報、前記取得ステップの処理により取得した前記情報処理装置の証明書、および前記演算ステップの処理により生成された前記演算値を送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項２９】

記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置を制御するコンピュータに、

前記情報処理装置を証明する証明書を取得する取得ステップと、

前記情報を共通鍵で暗号化する暗号化ステップと、

前記情報に所定の演算を施して、演算値を生成する演算ステップと、

前記暗号化ステップの処理により暗号化した前記情報、前記取得ステップの処理により

取得した前記情報処理装置の証明書、および前記演算ステップの処理により生成された前記演算値を送信する送信ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項３０】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置において、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置により共通鍵で暗号化された前記情報、および前記情報処置装置により生成された演算値を取得する取得手段と、
前記取得手段により取得された共通鍵で暗号化されている前記情報を、前記記録媒体再生装置が有する前記共通鍵で復号する復号手段と、
前記復号手段により復号された前記情報に所定の演算を施して、演算値を生成する演算手段と、
前記取得手段により取得された前記演算値と、前記演算手段により生成された前記演算値が同一であるか否かを判定する判定手段と、
前記判定手段により、前記取得手段により取得された前記演算値と、前記演算手段により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする記録媒体再生装置。
【請求項３１】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置の記録媒体再生方法において、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置により共通鍵で暗号化された前記情報、および前記情報処置装置により生成された演算値を取得する取得ステップと、
前記取得ステップの処理により取得された共通鍵で暗号化されている前記情報を、前記記録媒体再生装置が有する前記共通鍵で復号する復号ステップと、
前記復号ステップの処理により復号された前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とする記録媒体再生方法。
【請求項３２】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するプログラムであって、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置により共通鍵で暗号化された前記情報、および前記情報処置装置により生成された演算値を取得する取得ステップと、
前記取得ステップの処理により取得された共通鍵で暗号化されている前記情報を、前記記録媒体再生装置が有する前記共通鍵で復号する復号ステップと、
前記復号ステップの処理により復号された前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプ

ログラム格納媒体。
【請求項３３】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するコンピュータに、
前記情報処理装置が送信した、前記情報処理装置を証明する証明書、前記情報処理装置により共通鍵で暗号化された前記情報、および前記情報処置装置により生成された演算値を取得する取得ステップと、
前記取得ステップの処理により取得された共通鍵で暗号化されている前記情報を、前記記録媒体再生装置が有する前記共通鍵で復号する復号ステップと、
前記復号ステップの処理により復号された前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項３４】
記録媒体を再生する記録媒体再生装置と、前記記録媒体再生装置との間で情報を授受する情報処理装置からなる情報処理システムにおいて、
前記記録媒体再生装置は、
前記記録媒体再生装置を証明する証明書を取得する第１の取得手段と、
前記情報を共通鍵で暗号化する第１の暗号化手段と、
前記情報に所定の演算を施して、演算値を生成する第１の演算手段と、
前記第１の暗号化手段により暗号化した前記情報、前記第１の取得手段により取得した前記記録媒体再生装置の証明書、および前記第１の演算手段により生成された前記演算値を送信する送信手段とを備え、
前記情報処理装置は、
前記記録媒体再生装置の前記送信手段が送信した、前記第１の取得手段により取得した前記記録媒体再生装置の証明書、前記第１の暗号化手段により暗号化された前記情報、および前記第１の演算手段により生成された前記演算値を取得する第２の取得手段と、
前記情報処理装置から送信され、前記第２の取得手段により取得された前記第１の暗号化手段により暗号化された前記情報を、前記情報処理装置が有する前記共通鍵で復号する復号手段と、
前記復号手段により復号された前記情報に所定の演算を施して、演算値を生成する第２の演算手段と、
前記記録媒体再生装置から送信され、前記第２の取得手段により取得された前記第１の演算手段により生成された前記演算値と、前記第２の演算手段により生成された前記演算値が同一であるか否かを判定する判定手段と、
前記判定手段により、前記第１の演算手段により生成された前記演算値と、前記第２の演算手段により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする情報処理システム。
【請求項３５】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置において、
前記記録媒体再生装置を証明する証明書を取得する取得手段と、
前記情報を共通鍵で暗号化する暗号化手段と、
前記情報に所定の演算を施して、演算値を生成する演算手段と、
前記暗号化手段により暗号化した前記情報、前記取得手段により取得した前記記録媒体再生装置の証明書、および前記演算手段により生成された前記演算値を送信する送信手段

と
を備えることを特徴とする記録媒体再生装置。
【請求項３６】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置の記録媒体再生方法において、
前記記録媒体再生装置を証明する証明書を取得する取得ステップと、
前記情報を共通鍵で暗号化する暗号化ステップと、
前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記暗号化ステップの処理により暗号化した前記情報、前記取得ステップの処理により取得した前記記録媒体再生装置の証明書、および前記演算ステップの処理により生成された前記演算値を送信する送信ステップと
を含むことを特徴とする記録媒体再生方法。
【請求項３７】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するプログラムであって、
前記記録媒体再生装置を証明する証明書を取得する取得ステップと、
前記情報を共通鍵で暗号化する暗号化ステップと、
前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記暗号化ステップの処理により暗号化した前記情報、前記取得ステップの処理により取得した前記記録媒体再生装置の証明書、および前記演算ステップの処理により生成された前記演算値を送信する送信ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項３８】
記録媒体を再生し、情報処理装置との間で情報を授受する記録媒体再生装置を制御するコンピュータに、
前記記録媒体再生装置を証明する証明書を取得する取得ステップと、
前記情報を共通鍵で暗号化する暗号化ステップと、
前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記暗号化ステップの処理により暗号化した前記情報、前記取得ステップの処理により取得した前記記録媒体再生装置の証明書、および前記演算ステップの処理により生成された前記演算値を送信する送信ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項３９】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置において、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記記録媒体再生装置により共通鍵で暗号化された前記情報、および前記記録媒体再生装置により生成された演算値を取得する取得手段と、
取得手段により取得された共通鍵で暗号化されている前記情報を、前記情報処理装置が有する前記共通鍵で復号する復号手段と、
前記復号手段により復号された前記情報に所定の演算を施して、演算値を生成する演算手段と、
前記取得手段により取得された前記演算値と、前記演算手段により生成された前記演算値が同一であるか否かを判定する判定手段と、
前記判定手段により、前記取得手段により取得された前記演算値と、前記演算手段により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行手段と
を備えることを特徴とする情報処理装置。
【請求項４０】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置の情報処理

方法において、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記記録媒体再生装置により共通鍵で暗号化された前記情報、および前記記録媒体再生装置により生成された演算値を取得する取得ステップと、
取得ステップの処理により取得された共通鍵で暗号化されている前記情報を、前記情報処理装置が有する前記共通鍵で復号する復号ステップと、
前記復号ステップの処理により復号された前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とする情報処理方法。
【請求項４１】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置を制御するプログラムであって、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記記録媒体再生装置により共通鍵で暗号化された前記情報、および前記記録媒体再生装置により生成された演算値を取得する取得ステップと、
取得ステップの処理により取得された共通鍵で暗号化されている前記情報を、前記情報処理装置が有する前記共通鍵で復号する復号ステップと、
前記復号ステップの処理により復号された前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項４２】
記録媒体を再生する記録媒体再生装置との間で情報を授受する情報処理装置を制御するコンピュータに、
前記記録媒体再生装置が送信した、前記記録媒体再生装置を証明する証明書、前記記録媒体再生装置により共通鍵で暗号化された前記情報、および前記記録媒体再生装置により生成された演算値を取得する取得ステップと、
取得ステップの処理により取得された共通鍵で暗号化されている前記情報を、前記情報処理装置が有する前記共通鍵で復号する復号ステップと、
前記復号ステップの処理により復号された前記情報に所定の演算を施して、演算値を生成する演算ステップと、
前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であるか否かを判定する判定ステップと、
前記判定ステップの処理により、前記取得ステップの処理により取得された前記演算値と、前記演算ステップの処理により生成された前記演算値が同一であると判定された場合、所定の処理を実行する実行ステップと
を含む処理を実行させることを特徴とするプログラム。
【請求項４３】
自分に固有の記録媒体IDと、前記記録媒体IDを用いて暗号化されたコンテンツを含む情報が記録されている情報記録媒体であって、

前記記録媒体IDは、記録媒体再生装置により、前記情報記録媒体から取得され、情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化されるとともに、記録媒体再生装置が有する第３の鍵で暗号化され、

前記第２の鍵で暗号化された前記記録媒体IDおよび前記第３の鍵で暗号化された記録媒体IDは、前記記録媒体再生装置により前記情報処理装置に送信され、前記情報処理装置により復号され、

復号された前記記録媒体IDは、前記情報処理装置により、前記情報処理装置が所定の処理を行うか否かを判定するために、同一であるか否かが判定される

ことを特徴とする情報記録媒体。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
【発明の属する技術分野】
本発明は、情報処理システム、記録媒体再生装置および記録媒体再生方法、情報処理装置および方法、プログラム格納媒体、情報記録媒体、並びにプログラムに関し、特に、コンテンツを安全に転送できるようにした情報処理システム、記録媒体再生装置および記録媒体再生方法、情報処理装置および方法、プログラム格納媒体、情報記録媒体、並びにプログラムに関する。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００６２
【補正方法】変更
【補正の内容】
【００６２】
本発明の第２のプログラムは、記録媒体再生装置が送信した、記録媒体再生装置を証明する証明書、記録媒体再生装置により共通鍵で暗号化された情報、および記録媒体再生装置により生成された演算値を取得する取得ステップと、取得ステップの処理により取得された共通鍵で暗号化されている情報を、情報処理装置が有する共通鍵で復号する復号ステップと、復号ステップの処理により復号された情報に所定の演算を施して、演算値を生成する演算ステップと、取得ステップの処理により取得された演算値と、演算ステップの処理により生成された演算値が同一であるか否かを判定する判定ステップと、判定ステップの処理により、取得ステップの処理により取得された演算値と、演算ステップの処理により生成された演算値が同一であると判定された場合、所定の処理を実行する実行ステップとを含む処理をコンピュータに実行させることを特徴とする。

本発明の情報記録媒体は、自分に固有の記録媒体IDと、記録媒体IDを用いて暗号化されたコンテンツを含む情報が記録されている情報記録媒体であって、記録媒体IDは、記録媒体再生装置により、情報記録媒体から取得され、情報処理装置が有する第１の鍵に対応する第２の鍵で暗号化されるとともに、記録媒体再生装置が有する第３の鍵で暗号化され、第２の鍵で暗号化された記録媒体IDおよび第３の鍵で暗号化された記録媒体IDは、記録媒体再生装置により情報処理装置に送信され、情報処理装置により復号され、復号された記録媒体IDは、情報処理装置により、情報処理装置が所定の処理を行うか否かを判定するために、同一であるか否かが判定されることを特徴とする。