(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5406199号
(P5406199)

(45)発行日　平成26年2月5日(2014.2.5)　(24)登録日　平成25年11月8日(2013.11.8)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/24	165E
G06F 21/44	(2013.01)	G06F	21/20	144C
G06F 21/34	(2013.01)	G06F	21/20	134
		G06F	21/24	166A

請求項の数 28　(全 85 頁)

(21)出願番号　特願2010-530722 (P2010-530722)
(86)(22)出願日　平成21年9月18日 (2009.9.18)
(86)国際出願番号　PCT/JP2009/004733
(87)国際公開番号　WO2010/035449
(87)国際公開日　平成22年4月1日 (2010.4.1)
審査請求日　平成24年6月4日 (2012.6.4)
(31)優先権主張番号　特願2008-244376 (P2008-244376)
(32)優先日　平成20年9月24日 (2008.9.24)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2008-295503 (P2008-295503)
(32)優先日　平成20年11月19日 (2008.11.19)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(74)代理人　100125597
弁理士　小林　国人
(74)代理人　100146798
弁理士　川畑　孝二
(74)代理人　100121027
弁理士　木村　公一
(72)発明者　原田　俊治
大阪府門真市大字門真１００６番地　パナソニック株式会社内

最終頁に続く

(54)【発明の名称】記録再生システム、記録媒体装置及び記録再生装置

(57)【特許請求の範囲】
【請求項１】
記録媒体装置と記録再生装置とから構成される記録再生システムであって、
前記記録媒体装置は、耐タンパー手段及びメモリ手段を備え、
前記耐タンパー手段は、
耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、
前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、
前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、
前記記録再生装置は、
前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、
前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段と
を備えることを特徴とする記録再生システム。
【請求項２】
前記メモリ手段は、さらに、暗号化デバイス鍵を格納している暗号化デバイス鍵格納部

と、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化デバイス鍵は、前記記録媒体装置に固有のデバイス鍵を、コントローラ鍵で暗号化して生成されたものであり、前記暗号化メディア鍵群に含まれる複数の暗号化メディア鍵は、記録媒体装置のデバイス鍵又は記録再生装置のデバイス鍵それぞれを用いて、１個のメディア鍵を暗号化して生成されたものであり、

前記耐タンパー手段は、半導体デバイスであるコントローラであり、

前記証明手段は、さらに、

コントローラに固有の、又は所定数のコントローラの集合に固有のコントローラ鍵を格納しているコントローラ鍵格納部と、

前記暗号化デバイス鍵格納部から取得した前記暗号化デバイス鍵を、前記コントローラ鍵格納部に格納されている前記コントローラ鍵を用いて復号する復号部と、

前記復号部により生成されたデバイス鍵と、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群に基づき、メディア鍵を生成する第１メディア鍵生成部と

前記第１メディア鍵生成部により生成された前記メディア鍵と、前記識別情報格納手段に格納されている前記識別情報に基づき、メディア固有鍵を生成する第１メディア固有鍵生成部とを備え、

前記検証手段は、

前記記録再生装置に固有のデバイス鍵を格納しているデバイス鍵格納部と、

前記デバイス鍵格納部に格納されている前記デバイス鍵と、前記暗号化メディア鍵群格納部から取得した前記暗号化メディア鍵群に基づき、メディア鍵を生成する第２メディア鍵生成部と、

前記第２メディア鍵生成部により生成されたメディア鍵と、前記記録媒体装置から取得した前記識別情報に基づき、メディア固有鍵を生成する第２メディア固有鍵生成部とを備え、

前記証明手段は、前記第１メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報を生成し、

前記検証手段は、前記第２メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報に基づき、前記記録媒体装置の正当性を検証する

ことを特徴とする請求項１記載の記録再生システム。

【請求項３】

前記メモリ手段は、さらに、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化メディア鍵群に含まれる複数の暗号化メディア鍵は、前記記録媒体装置のデバイス鍵又は前記記録再生装置のデバイス鍵それぞれを用いて、１個のメディア鍵を暗号化して生成されたものであり、

前記証明手段は、さらに、

前記耐タンパー手段に固有のデバイス鍵を格納する第１デバイス鍵格納部と、

前記第１デバイス鍵格納部に格納されている前記デバイス鍵と、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群に基づき、メディア鍵を生成する第１メディア鍵生成部と、

前記第１メディア鍵生成部により生成された前記メディア鍵と、前記識別情報格納手段に格納されている前記識別情報に基づき、メディア固有鍵を生成する第１メディア固有鍵生成部とを備え、

前記検証手段は、さらに、

前記記録再生装置に固有のデバイス鍵を格納している第２デバイス鍵格納部と、

前記第２デバイス鍵格納部に格納されている前記デバイス鍵と、前記暗号化メディア鍵群格納部から取得した前記暗号化メディア鍵群に基づき、メディア鍵を生成する第２メディア鍵生成部と、

前記第２メディア鍵生成部により生成された前記メディア鍵と、前記記録媒体装置から取得した前記識別情報に基づき、メディア固有鍵を生成する第２メディア固有鍵生成部とを備え、

前記証明手段は、前記第１メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報を生成し、
前記検証手段は、前記第２メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報に基づき、前記記録媒体装置の正当性を検証する
ことを特徴とする請求項１記載の記録再生システム。
【請求項４】
前記証明手段は、さらに、
前記記録媒体装置のメーカーに固有のメーカー秘密鍵を格納しているメーカー秘密鍵格納部と、
前記記録再生装置の前記検証手段から乱数を受け取り、前記メーカー秘密鍵を用いて、受け取った前記乱数及び前記識別情報格納手段に格納されている前記識別情報に対する署名データを生成する署名生成部とを備え、
前記メモリ手段は、さらに、
信頼できるセンターにより、当該センターのセンター秘密鍵を用いて、前記メーカー秘密鍵に対応するメーカー公開鍵に対して発行されたメーカー公開鍵証明書を格納しているメーカー公開鍵証明書格納部を備え、
前記検証手段は、さらに、
前記乱数を生成し前記記録媒体装置へ送る乱数生成部と、
前記センターのセンター秘密鍵に対応するセンター公開鍵を格納しているセンター公開鍵格納部と、
前記センター公開鍵格納部に格納されている前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する第１署名検証部と、
正当性が検証された前記メーカー公開鍵を用いて、前記記録媒体装置から受け取った前記署名データの正当性を検証することにより、前記記録媒体装置の正当性を検証する第２署名検証部と
を備えることを特徴とする請求項１記載の記録再生システム。
【請求項５】
前記証明手段は、
前記識別情報を用いて、当該耐タンパー手段のメディア固有鍵を生成する第１メディア固有鍵生成手段と、
前記メディア固有鍵を鍵として用いて、前記記録再生装置からのチャレンジデータからレスポンスデータとしての前記証明情報を生成し、生成したレスポンスデータとしての前記証明情報を出力する証明生成手段とを含み、
前記検証手段は、
前記記録媒体装置の前記識別情報を用いて、前記メディア固有鍵と同一のメディア固有鍵を生成する第２メディア固有鍵生成手段と、
前記チャレンジデータを生成して出力し、前記記録媒体装置から取得したレスポンスデータとしての前記証明情報と、前記チャレンジデータとを用いて、前記記録媒体装置の正当性を検証する検証部とを備える
ことを特徴とする請求項１に記載の記録再生システム。
【請求項６】
前記証明手段は、さらに、メディア鍵を生成する第１メディア鍵生成手段を備え、
前記第１メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いてメディア固有鍵を生成し、
前記検証手段は、さらに、前記第１メディア鍵生成手段にて生成されたメディア鍵と同一のメディア鍵を生成する第２メディア鍵生成手段を備え、
前記第２メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いて前記メディア固有鍵を生成する
ことを特徴とする請求項５に記載の記録再生システム。

【請求項７】
前記証明手段は、
前記記録媒体装置の製造者のメーカー秘密鍵を格納しているメーカー秘密鍵格納部と、
前記識別情報格納手段から前記識別情報を取得し、前記メーカー秘密鍵を用いて、取得した前記識別情報に対して、デジタル署名を施して、前記証明情報として署名データを生成する署名生成部とを含み、
前記検証手段は、
前記記録媒体装置の製造者のメーカー公開鍵を格納しているメーカー公開鍵格納部と、
前記記録媒体装置から前記証明情報として前記署名データを取得し、前記メーカー公開鍵を用いて、取得した前記証明情報としての前記署名データに対して、デジタル署名検証を施し、検証に失敗した場合には、暗号化コンテンツの復号又はコンテンツの暗号化を禁止し、検証に成功した場合には、前記署名データから前記識別情報を取得する署名検証部とを含み、
前記コンテンツ暗復号手段は、検証に成功した場合に、取得された前記識別情報に基づき、前記コンテンツを暗号化し、又は前記暗号化コンテンツを復号する
ことを特徴とする請求項１に記載の記録再生システム。
【請求項８】
暗号化されたコンテンツを格納するための記録媒体装置であって、
耐タンパー手段及びメモリ手段を備え、
前記耐タンパー手段は、
耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、
前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、
前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、
前記証明手段は、
前記識別情報を用いて、メディア固有鍵を生成する第１メディア固有鍵生成手段と、
前記メディア固有鍵を鍵として用いて、記録再生装置からのチャレンジデータからレスポンスデータとしての前記証明情報を生成し、生成したレスポンスデータとしての前記証明情報を出力する証明生成手段とを含む
ことを特徴とする記録媒体装置。
【請求項９】
前記証明手段は、さらに、メディア鍵を生成する第１メディア鍵生成手段を備え、
前記第１メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いてメディア固有鍵を生成する
ことを特徴とする請求項８に記載の記録媒体装置。
【請求項１０】
前記メモリ手段は、さらに、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化メディア鍵群は、複数の暗号化メディア鍵を含み、複数の暗号化メディア鍵は、複数の装置に対応し、複数の暗号化メディア鍵のそれぞれは、各装置に割り当てられたデバイス鍵を用いて、前記記録媒体装置のメディア鍵を暗号化して生成されたものであり、
前記証明手段は、さらに、当該記録媒体装置に割り当てられたデバイス鍵を格納しているデバイス鍵格納手段を備え、
前記第１メディア鍵生成手段は、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群から、当該記録媒体装置の暗号化メディア鍵を特定し、特定した暗号化メディア鍵を前記デバイス鍵を用いて復号して、前記メディア鍵を生成する
ことを特徴とする請求項９に記載の記録媒体装置。
【請求項１１】
前記耐タンパー手段は、半導体デバイスであるコントローラであり、

前記メモリ手段は、さらに、暗号化された前記デバイス鍵を格納している暗号化デバイス鍵格納手段を備え、
前記証明手段は、さらに、
コントローラである当該耐タンパー手段に割り当てられたコントローラ鍵を格納しているコントローラ鍵格納手段と、
前記暗号化デバイス鍵格納手段に格納されている暗号化された前記デバイスを、前記コントローラ鍵を用いて復号して、前記デバイス鍵を生成する復号手段と
を備えることを特徴とする請求項１０に記載の記録媒体装置。
【請求項１２】
前記メモリ手段は、さらに、暗号化された前記デバイス鍵を格納している暗号化デバイス鍵格納手段を備え、
前記証明手段は、さらに、
当該耐タンパー手段に固有の固有鍵を生成する固有鍵生成手段と、
前記暗号化デバイス鍵格納手段に格納されている暗号化された前記デバイス鍵を、前記固有鍵を用いて復号して、前記デバイス鍵を生成する復号手段と
を備えることを特徴とする請求項１０に記載の記録媒体装置。
【請求項１３】
暗号化されたコンテンツを格納するための記録媒体装置であって、
耐タンパー手段及びメモリ手段を備え、
前記耐タンパー手段は、
耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、
前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、
前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、
前記証明手段は、
前記記録媒体装置の製造者のメーカー秘密鍵を格納しているメーカー秘密鍵格納部と、
前記識別情報格納手段から前記識別情報を取得し、前記メーカー秘密鍵を用いて、取得した前記識別情報に対して、デジタル署名を施して、前記証明情報として署名データを生成する署名生成部とを含む
ことを特徴とする記録媒体装置。
【請求項１４】
前記署名生成部は、記録再生装置から乱数を取得し、取得した前記識別情報及び取得した乱数の結合体に対して、デジタル署名を施す
ことを特徴とする請求項１３に記載の記録媒体装置。
【請求項１５】
前記記録媒体装置のメモリ手段は、さらに、信頼できるセンターにより、当該センターのセンター秘密鍵を用いて、前記メーカー秘密鍵に対応するメーカー公開鍵に対して発行されたメーカー公開鍵証明書を格納するメーカー公開鍵証明書格納部を備える
ことを特徴とする請求項１３に記載の記録媒体装置。
【請求項１６】
暗号化コンテンツを復号し、又はコンテンツを暗号化する記録再生装置であって、
暗号化されたコンテンツを格納するための記録媒体装置から、当該記録媒体装置の識別情報に基づいて当該記録媒体装置の正当性を証明する証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、
前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記記録媒体装置に記録し、又は、前記識別情報に基づき、前記記録媒体装置から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段と
を備えることを特徴とする記録再生装置。

【請求項１７】
前記記録媒体装置は、耐タンパー手段及びメモリ手段を備え、メディア固有鍵を生成し前記メディア固有鍵を鍵として用いて、前記記録再生装置からのチャレンジデータからレスポンスデータとしての前記証明情報を生成して出力し、
前記検証手段は、
前記記録媒体装置の前記識別情報を用いて、前記記録媒体装置で生成されたメディア固有鍵と同一のメディア固有鍵を生成する第２メディア固有鍵生成手段と、
前記チャレンジデータを生成して出力し、前記記録媒体装置から取得したレスポンスデータとしての前記証明情報と、前記チャレンジデータとを用いて、前記記録媒体装置の正当性を検証する検証部とを備える
ことを特徴とする請求項１６に記載の記録再生装置。
【請求項１８】
前記記録媒体装置は、さらに、メディア鍵を生成し、前記識別情報及び生成された前記メディア鍵を用いてメディア固有鍵を生成し、
前記検証手段は、さらに、前記記録媒体装置に生成されたメディア鍵と同一のメディア鍵を生成する第２メディア鍵生成手段を備え、
前記第２メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いて前記メディア固有鍵を生成する
ことを特徴とする請求項１７に記載の記録再生装置。
【請求項１９】
前記記録媒体装置のメモリ手段は、さらに、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化メディア鍵群は、複数の暗号化メディア鍵を含み複数の暗号化メディア鍵は、複数の装置に対応し、複数の暗号化メディア鍵のそれぞれは各装置に割り当てられたデバイス鍵を用いて、前記記録媒体装置のメディア鍵を暗号化して生成されたものであり、
前記検証手段は、さらに、当該記録再生装置に割り当てられたデバイス鍵を格納しているデバイス鍵格納手段を備え、
前記第２メディア鍵生成手段は、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群から、当該記録再生装置の暗号化メディア鍵を特定し、特定した暗号化メディア鍵を前記デバイス鍵を用いて復号して、前記メディア鍵を生成する
ことを特徴とする請求項１８に記載の記録再生装置。
【請求項２０】
前記検証手段は、
前記記録媒体装置の製造者のメーカー公開鍵を格納しているメーカー公開鍵格納部と、
前記記録媒体装置の製造者のメーカー秘密鍵を用いて、前記識別情報に対して、デジタル署名を施して生成された前記証明情報としての署名データを取得し、前記メーカー公開鍵を用いて、取得した前記証明情報としての前記署名データに対して、デジタル署名検証を施し、検証に失敗した場合には、前記暗号化コンテンツの復号又は前記コンテンツの暗号化を禁止し、検証に成功した場合には、前記署名データから前記識別情報を取得する署名検証部とを含み、
前記コンテンツ暗復号手段は、検証に成功した場合に、取得された前記識別情報に基づき、前記コンテンツを暗号化し、又は前記暗号化コンテンツを復号する
ことを特徴とする請求項１６に記載の記録再生装置。
【請求項２１】
前記記録再生装置の前記検証手段は、さらに、乱数を生成し前記記録媒体装置へ送る乱数生成部を備え、
前記検証手段は、前記識別情報及び前記乱数の結合体に対してデジタル署名が施されて生成された署名データを取得し、取得した前記証明情報と生成した乱数の結合体に基づき前記記録媒体装置の正当性を検証する
ことを特徴とする請求項２０記載の記録再生装置。

【請求項２２】
前記検証手段は、さらに、
信頼できるセンターのセンター秘密鍵に対応するセンター公開鍵を格納するセンター公開鍵格納部と、
前記センター公開鍵格納部の前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する署名検証部とを含む
ことを特徴とする請求項２０に記載の記録再生装置。
【請求項２３】
暗号化コンテンツを復号し、又はコンテンツを暗号化する記録再生装置において用いられる記録再生方法であって、
記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、
前記記録再生方法は、
前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証ステップと、
前記検証ステップによる検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号ステップと
を含むことを特徴とする記録再生方法。
【請求項２４】
暗号化コンテンツを復号し、又はコンテンツを暗号化する記録再生装置において用いられる記録再生のためのコンピュータプログラムであって、
記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、
コンピュータに、
前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証ステップと、
前記検証ステップによる検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号ステップと
を実行させるための前記コンピュータプログラム。
【請求項２５】
前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項２４に記載のコンピュータプログラム。
【請求項２６】
集積回路であって、
記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを

含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、
前記集積回路は、
前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、
前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段と
を備えることを特徴とする集積回路。

【請求項２７】
半製品であるコントローラから記録媒体装置に組み込まれるべきコントローラを製造する製造方法であって、
半製品であるコントローラは、耐タンパー性を有する半導体デバイスであり、識別情報格納手段と、前記識別情報格納手段に格納されるべき識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記証明手段は、コントローラ鍵格納部と、暗号化デバイス鍵を前記コントローラ鍵格納部に格納されるべきコントローラ鍵を用いて復号する復号部と、前記復号部により生成されたデバイス鍵及び暗号化メディア鍵群に基づき、メディア鍵を生成する第１メディア鍵生成部と、前記第１メディア鍵生成部で生成された前記メディア鍵と、前記識別情報格納手段に格納されている前記識別情報に基づき、メディア固有鍵を生成する第１メディア固有鍵生成部と、前記第１メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報を生成する証明生成手段とを備え、
（ａ）コントローラベンダのコンピュータにより、製造対象のコントローラに固有の識別情報を生成するステップと、
（ｂ）コントローラベンダのコンピュータにより、コントローラに固有の、又は、所定数のコントローラの集合に固有のコントローラ鍵を生成するステップと、
（ｃ）コントローラベンダの実装手段により、生成した前記識別情報を前記識別情報格納手段に格納するステップと、
（ｄ）コントローラベンダの実装手段により、生成した前記コントローラ鍵を前記コントローラ鍵格納部に格納するステップと
含むことを特徴とする製造方法。

【請求項２８】
請求項２７の製造方法により製造されたコントローラを組み込んで記録媒体装置を製造する製造方法であって、
（ｅ）コントローラベンダのコンピュータにより、コントローラベンダを識別するベンダＩＤと、前記コントローラ鍵を識別するコントローラ鍵識別情報と、前記コントローラ鍵とを鍵発行局であるセンターに送付するステップと、
（ｆ）前記センターのコンピュータにより、前記ベンダＩＤと前記コントローラ鍵識別情報と前記コントローラ鍵を受け取るステップと、
（ｇ）前記センターのコンピュータにより、受け取った前記ベンダＩＤと前記コントローラ鍵識別情報と前記コントローラ鍵とを前記センターのコンピュータの格納手段に格納するステップと、
（ｈ）前記記録媒体装置メーカーのコンピュータにより、コントローラベンダに対してコントローラの注文情報を送るステップと、
（ｉ）前記コントローラベンダのコンピュータにより、コントローラの前記注文情報を受け付けるステップと、
（ｊ）前記コントローラベンダにより、前記記録媒体装置メーカーに対して、前記コントローラを発行するステップと、
（ｋ）前記コントローラベンダのコンピュータにより、前記記録媒体装置メーカーに対

して、コントローラベンダのベンダＩＤと、前記コントローラに格納されたコントローラ鍵のコントローラ鍵識別情報を、発行するステップと、
（ｌ）前記記録媒体装置メーカーにより、前記コントローラベンダから、前記コントローラを受け取るステップと、
（ｍ）前記記録媒体装置メーカーのコンピュータにより、前記コントローラベンダから前記ベンダＩＤと、前記コントローラ鍵識別情報とを受け取るステップと、
（ｎ）前記記録媒体装置メーカーの組込装置により、受け取ったコントローラを前記記録媒体装置に実装するステップと、
（ｏ）前記記録媒体装置メーカーのコンピュータにより、センターに対して、コントローラベンダから受け取った前記ベンダＩＤと、前記コントローラ鍵識別情報とを含むカードデバイス鍵注文情報を送るステップと、
（ｐ）センターのコンピュータにより、前記記録媒体装置メーカーから、前記カードデバイス鍵注文情報を受け付けるステップと、
（ｑ）センターのコンピュータにより、前記カードデバイス鍵注文情報に応じたデバイス鍵を生成するステップと、
（ｒ）センターのコンピュータにより、前記格納手段から前記ベンダＩＤと、前記コントローラ鍵識別情報に対応するコントローラ鍵とを前記格納手段より取得し、取得したコントローラ鍵を用いて、生成したデバイス鍵を暗号化して、暗号化デバイス鍵を生成するステップと、
（ｓ）センターのコンピュータにより、メディア鍵を複数の記録媒体装置のデバイス鍵もしくは記録再生装置のデバイス鍵それぞれを用いて暗号化して得られる暗号化メディア鍵群を生成するステップと、
（ｔ）センターのコンピュータにより、前記記録媒体装置メーカーに対して、生成した前記暗号化デバイス鍵と、前記暗号化メディア鍵群とを、記録媒体装置のメーカーに発行するステップと、
（ｕ）前記記録媒体装置のメーカーのコンピュータにより、前記センターから前記暗号化デバイス鍵と、前記暗号化メディア鍵群とを受け取るステップと、
（ｖ）前記記録媒体装置のメーカーの実装手段により、記録媒体装置のメモリの暗号化カードデバイス鍵格納部及び暗号化メディア鍵群格納部に、センターから受け取った暗号化カードデバイス鍵及び暗号化メディア鍵群を格納するステップと
を含むことを特徴とする記録媒体装置の製造方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタルコンテンツの不正利用を防止する技術に関する。
【背景技術】
【０００２】
デジタル放送されるデジタルコンテンツを、記録媒体、例えば、記録型ＤＶＤ（DigitalVersatile Disk）、メモリカード等に記録する記録再生装置が普及しつつある。前記記録再生装置の具体例は、ＤＶＤレコーダ、１セグ放送（1 segment broadcasting）録画に対応した携帯電話等である。また、映画や音楽等のデジタルコンテンツを、ネットワーク経由で、記録装置に、デジタル配信し、前記記録装置を用いて記録媒体に記録するサービスが普及しつつある。前記記録装置の具体例は、ＫＩＯＳＫ端末、パーソナルコンピュータ等である。さらに、デジタルコンテンツを、ネットワーク経由で、再生装置にデジタル配信し再生するといったデジタルコンテンツ配信サービスが普及しつつある。再生装置の具体例は、音楽プレーヤ、映像表示用の携帯端末等である。
【０００３】
この場合、デジタルコンテンツの著作権者の権利を保護するため、一度、記録媒体に記録されたデジタルコンテンツが、他の記録媒体にコピーされて再生されることを防止する技術が必要である。

【０００４】
特許文献１によると、記録媒体に、当該記録媒体固有の書き換え不可能な一意の媒体固有番号を格納する。許諾側では、この記録媒体の媒体固有番号をもとに媒体固有鍵を生成し、この媒体固有鍵を用いて、暗号化データを復号するための復号鍵を暗号化して許諾情報として記録媒体に書き込む。使用側では、記録媒体から媒体固有番号を読み込み、読み込んだ媒体固有番号をもとに媒体固有鍵を生成する。次に、この媒体固有鍵によって許諾情報である暗号化された復号鍵を復号して元の復号鍵を生成する。そして、この復号鍵によって暗号化データを復号して、平文の電子化データを生成している。
【０００５】
この技術によると、使用者は、正規の記録媒体に記録された暗号化データ及び許諾情報を他の不正な記録媒体にコピーし、不正な記録媒体から暗号化データを復号しようとしても、正規の記録媒体の媒体固有番号を不正な記録媒体にコピーできない。したがって、使用者は、前記他の記録媒体から、正規の記録媒体の媒体固有番号を取得できず、許諾情報である暗号化された復号鍵を正しく復号できない。その結果、使用者は暗号化データを正しく復号できない。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】日本国特開平０５－２５７８１６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ここで、カードメーカーが、各メモリカードに同じメディアＩＤを格納する場合を想定する。つまり、第１及び第２のメモリカードに、カードメーカーにより、同じメディアＩＤが格納されているものとする。また、第１メモリカードには、正規の暗号化コンテンツが格納されているものとする。この暗号化コンテンツは、メディアＩＤから生成されたコンテンツ鍵を用いて、コンテンツを暗号化して生成したものである。
【０００８】
この場合に、第１メモリカードに格納されている暗号化コンテンツが第２メモリカードに不正にコピーされたとする。第２メモリカードにコピーされた暗号化コンテンツを不正に再生するために、第２メモリカードからメディアＩＤを取得し、取得したメディアＩＤからコンテンツ鍵を生成する。第２メモリカードに格納されているメディアＩＤは、第１メモリカードに格納されているメディアＩＤと同一である。したがって、第２メモリカードのメディアＩＤから生成したコンテンツ鍵は、第１メモリカードのメディアＩＤから生成したコンテンツ鍵と同一である。したがって、生成したコンテンツ鍵を用いて、第２メモリカードにコピーされた暗号化コンテンツを復号しようとすると、復号が正しく行える
このように、従来の技術では、カードメーカーが、複数のメモリカードに同じメディアＩＤを格納するという不正を行った場合、デジタルコンテンツの著作権者の権利が保護できないという問題点がある。
【０００９】
本発明は、上記問題点を解決するため、記録媒体装置のメーカーが、複数の記録媒体装置に、一の記録媒体装置を識別する一の識別情報を格納するという不正を防止することができる記録再生システム、記録媒体装置、記録再生装置、方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１０】
上記目的を達成するために、本発明は、記録媒体装置と記録再生装置とから構成される記録再生システムであって、前記記録媒体装置は、耐タンパー手段及びメモリ手段を備え前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明

情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、前記記録再生装置は、前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段とを備えることを特徴とする。

【発明の効果】

【００１１】

本発明の記録再生システムによれば、記録再生装置の検証手段が、記録媒体装置の耐タンパー手段に格納されている識別情報に基づいて証明手段により生成された証明情報を用いて、記録媒体装置の正当性を検証する。検証が失敗した場合には、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する。検証が成功した場合には、コンテンツの暗号化又は暗号化コンテンツの復号が許される。

【００１２】

そのため、もし、記録媒体装置のメーカーが不正に記録媒体装置の識別情報を複数の記録媒体装置に複製したとしても、そのメーカーは、その不正な記録媒体装置に耐タンパー手段を複製できない。これにより、記録媒体装置は、識別情報に基づく証明情報を出力できず、正当な記録再生装置との間の認証に失敗する。

【００１３】

これにより、記録媒体装置のメーカーが不正に識別情報を複製した場合であっても、その記録媒体装置を使って、コンテンツを暗号化したり、暗号化されたコンテンツを復号したりすることはできない。こうして、記録媒体装置のメーカーによる不正行為を防止できるという効果が発揮される。

【図面の簡単な説明】

【００１４】

【図１】実施の形態１における記録再生システム３００、センター６００、カードメーカー４００及び装置メーカー５００を表す全体構成図である。

【図２】実施の形態１におけるセンター６００、カードメーカー４００及び装置メーカー５００の各構成を示す構成図である。

【図３】実施の形態１におけるセンター６００及びカードメーカー４００の動作を示すフローチャートである。

【図４】実施の形態１におけるメーカー公開鍵証明書／メディアＩＤ格納モジュール注文書８１０の例を示す。

【図５】実施の形態１におけるメーカー公開鍵証明書８２０の例を示す。

【図６】実施の形態１におけるメディアＩＤ格納モジュール部６１０の構成を示す構成図である。

【図７】実施の形態１におけるメディアＩＤ署名データ８３０の例を示す。

【図８】実施の形態１におけるセンター６００と装置メーカー５００の動作を示すフローチャートである。

【図９】実施の形態１におけるセンター公開鍵注文書８４０の例を示す。

【図１０】実施の形態１における記録再生システム３００（メモリカード１００と記録再生装置２００）の構成を示す構成図である。

【図１１】実施の形態１における記録再生システム３００（メモリカード１００と記録再生装置２００）の記録時の動作を示すフローチャートである。

【図１２】実施の形態１における記録再生システム３００（メモリカード１００と記録再生装置２００）の再生時の動作を示すフローチャートである。

【図１３】実施の形態１における記録再生システム３００による効果を説明するための説明図である。

【図１４】実施の形態２における記録再生システム３００ａ、センター６００ａ、カードメーカー４００ａ及び装置メーカー５００ａの構成を示す全体構成図である。
【図１５】実施の形態２におけるセンター６００ａ、カードメーカー４００ａ及び装置メーカー５００ａの構成を示す構成図である。
【図１６】実施の形態２におけるセンター６００ａ及びカードメーカー４００ａの動作を示すフローチャートである。
【図１７】実施の形態２におけるメディアＩＤ格納モジュール注文書８５０の例を示す。
【図１８】実施の形態２におけるメディアＩＤ格納モジュール部６１０ａの構成を示す構成図である。
【図１９】実施の形態２における暗号化メディア鍵群８６０のデータ構造を示す。
【図２０】実施の形態２におけるセンター６００ａ及び装置メーカー５００ａの動作を示すフローチャートである。
【図２１】実施の形態２における装置デバイス鍵注文書８７０のデータ構造の一例を示す。
【図２２】実施の形態２における記録再生システム３００ａ（メモリカード１００ａ及び記録再生装置２００ａ）の構成を示す構成図である。
【図２３】実施の形態２における記録再生システム３００ａ（メモリカード１００ａ及び記録再生装置２００ａ）の記録時の動作を示すフローチャートである。
【図２４】実施の形態２における記録再生システム３００ａ（メモリカード１００ａ及び記録再生装置２００ａ）における認証処理の例を示す。
【図２５】実施の形態２における記録再生システム３００ａ（メモリカード１００ａ及び記録再生装置２００ａ）の再生時の動作を示すフローチャートである。
【図２６】実施の形態２における記録再生システム３００ａによる効果を説明するための説明図である。
【図２７】実施の形態１の変形例としての記録再生システム３００ｃ（メモリカード１００ｃ及び記録再生装置２００ｃ）の構成を示す構成図である。
【図２８】実施の形態２の変形例としての記録再生システム（メモリカード１００ａ及び記録再生装置２００ａ）の構成を示す構成図である。
【図２９】実施の形態３における記録再生システム１３００、センター１６００、コントローラベンダ１７００、カードメーカー１４００及び装置メーカー１５００の構成を示す全体構成図である。
【図３０】実施の形態３におけるセンター１６００、コントローラベンダ１７００及びカードメーカー１４００の構成を示す構成図である。
【図３１】実施の形態３におけるセンター１６００及び装置メーカー１５００の構成を示す構成図である。
【図３２】実施の形態３におけるセンター１６００、コントローラベンダ１７００及びカードメーカー１４００の動作を示すフローチャートである。
【図３３】実施の形態３におけるセンター１６００が管理するコントローラ鍵情報１８１０のデータ構造の一例を示す。
【図３４】実施の形態３におけるコントローラ注文書１８２０のデータ構造の一例を示す。
【図３５】実施の形態３におけるカードデバイス鍵注文書１８３０のデータ構造の一例を示す。
【図３６】実施の形態３におけるコントローラ１９１０の構成を示す構成図である。
【図３７】実施の形態３における暗号化メディア鍵群１８４０のデータ構造の一例を示す。
【図３８】実施の形態３におけるセンター１６００及び装置メーカー１５００の動作を示すフローチャートである。
【図３９】実施の形態３における装置デバイス鍵注文書１８５０のデータ構造の一例を示す。

【図４０】実施の形態３における記録再生システム１３００（メモリカード１１００及び記録再生装置１２００）の構成を示す構成図である。
【図４１】実施の形態３における記録再生システム１３００（メモリカード１１００及び記録再生装置１２００）の記録時の動作を示すフローチャートである。
【図４２】実施の形態３における記録再生システム１３００（メモリカード１１００及び記録再生装置１２００）における認証処理の例を示す。
【図４３】実施の形態３における記録再生システム１３００（メモリカード１１００及び記録再生装置１２００）の再生時の動作を示すフローチャートである。
【図４４】実施の形態３における記録再生システム１３００による効果を説明するための説明図である。
【図４５】変形例としての記録再生システム２３００（メモリカード２１００及び記録再生装置２２００）の構成を示す構成図である。
【図４６】変形例としての記録再生システム２３００（メモリカード２１００及び記録再生装置２２００）の動作を示すフローチャートである。
【図４７】実施の形態２におけるカードデバイス鍵／暗号化メディア鍵群注文書８５５の例を示す。
【発明を実施するための形態】
【００１５】
本発明の第１の態様に係る記録再生システムは、記録媒体装置と記録再生装置とから構成される記録再生システムであって、前記記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、前記記録再生装置は、前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段とを備えることを特徴とする。
【００１６】
本発明の第２の態様に係る記録再生システムにおいて、前記メモリ手段は、さらに、暗号化デバイス鍵を格納している暗号化デバイス鍵格納部と、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化デバイス鍵は、前記記録媒体装置に固有のデバイス鍵を、コントローラ鍵で暗号化して生成されたものであり、前記暗号化メディア鍵群に含まれる複数の暗号化メディア鍵は、記録媒体装置のデバイス鍵又は記録再生装置のデバイス鍵それぞれを用いて、１個のメディア鍵を暗号化して生成されたものであり、前記耐タンパー手段は、半導体デバイスであるコントローラであり、前記証明手段は、さらに、コントローラに固有の、又は所定数のコントローラの集合に固有のコントローラ鍵を格納しているコントローラ鍵格納部と、前記暗号化デバイス鍵格納部から取得した前記暗号化デバイス鍵を、前記コントローラ鍵格納部に格納されている前記コントローラ鍵を用いて復号する復号部と、前記復号部により生成されたデバイス鍵と、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群に基づき、メディア鍵を生成する第１メディア鍵生成部と、前記第１メディア鍵生成部により生成された前記メディア鍵と、前記識別情報格納手段に格納されている前記識別情報に基づき、メディア固有鍵を生成する第１メディア固有鍵生成部とを備え、前記検証手段は、前記記録再生装置に固有のデバイス鍵を格納しているデバイス鍵格納部と、前記デバイス鍵格納部に格納されている前記デバイス鍵と、前記暗号化メディア鍵群格納部から取得した前記暗号化メディア鍵群に基づき、メディア鍵を生成する第２メディア鍵生成部と、前記第２メディア鍵生成部により生成されたメディア鍵と、前記記録媒体装置から取得した前記識別情報に基づき

メディア固有鍵を生成する第２メディア固有鍵生成部とを備え、前記証明手段は、前記第１メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報を生成し、前記検証手段は、前記第２メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報に基づき、前記記録媒体装置の正当性を検証することを特徴とする。

【００１７】

この構成によると、記録媒体装置の耐タンパー手段は、証明手段を備え、前記証明手段は、コントローラ鍵格納部、復号部、第１メディア鍵生成部及び第１メディア固有鍵生成部を備えるので、もし、記録媒体装置のメーカーが不正に記録媒体装置の識別情報を複数の記録媒体装置に複製したとしても、そのメーカーは、その不正な記録媒体装置に耐タンパー手段を複製できず、記録媒体装置は、識別情報に基づく証明情報を出力できず、正当な記録再生装置との間の認証に失敗する。こうして、記録媒体装置のメーカーによる不正行為を防止できる。

【００１８】

本発明の第３の態様に係る記録再生システムにおいて、前記メモリ手段は、さらに、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化メディア鍵群に含まれる複数の暗号化メディア鍵は、前記記録媒体装置のデバイス鍵又は前記記録再生装置のデバイス鍵それぞれを用いて、１個のメディア鍵を暗号化して生成されたものであり、前記証明手段は、さらに、前記耐タンパー手段に固有のデバイス鍵を格納する第１デバイス鍵格納部と、前記第１デバイス鍵格納部に格納されている前記デバイス鍵と、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群に基づき、メディア鍵を生成する第１メディア鍵生成部と、前記第１メディア鍵生成部により生成された前記メディア鍵と、前記識別情報格納手段に格納されている前記識別情報に基づき、メディア固有鍵を生成する第１メディア固有鍵生成部とを備え、前記検証手段は、さらに、前記記録再生装置に固有のデバイス鍵を格納している第２デバイス鍵格納部と、前記第２デバイス鍵格納部に格納されている前記デバイス鍵と、前記暗号化メディア鍵群格納部から取得した前記暗号化メディア鍵群に基づき、メディア鍵を生成する第２メディア鍵生成部と、前記第２メディア鍵生成部により生成された前記メディア鍵と、前記記録媒体装置から取得した前記識別情報に基づき、メディア固有鍵を生成する第２メディア固有鍵生成部とを備え、前記証明手段は、前記第１メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報を生成し、前記検証手段は、前記第２メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報に基づき、前記記録媒体装置の正当性を検証することを特徴とする。

【００１９】

この構成によると、記録媒体装置の耐タンパー手段は、証明手段を備え、前記証明手段は、第１デバイス鍵格納部、第１メディア鍵生成部及び第１メディア固有鍵生成部を備えるので、もし、記録媒体装置のメーカーが不正に記録媒体装置の識別情報を複数の記録媒体装置に複製したとしても、そのメーカーは、その不正な記録媒体装置に耐タンパー手段を複製できず、記録媒体装置は、識別情報に基づく証明情報を出力できず、正当な記録再生装置との間の認証に失敗する。こうして、記録媒体装置のメーカーによる不正行為を防止できる。

【００２０】

本発明の第４の態様に係る記録再生システムにおいて、前記証明手段は、さらに、前記記録媒体装置のメーカーに固有のメーカー秘密鍵を格納しているメーカー秘密鍵格納部と前記記録再生装置の前記検証手段から乱数を受け取り、前記メーカー秘密鍵を用いて、受け取った前記乱数及び前記識別情報格納手段に格納されている前記識別情報に対する署名データを生成する署名生成部とを備え、前記メモリ手段は、さらに、信頼できるセンターにより、当該センターのセンター秘密鍵を用いて、前記メーカー秘密鍵に対応するメーカー公開鍵に対して発行されたメーカー公開鍵証明書を格納しているメーカー公開鍵証明書格納部を備え、前記検証手段は、さらに、前記乱数を生成し前記記録媒体装置へ送る乱数

生成部と、前記センターのセンター秘密鍵に対応するセンター公開鍵を格納しているセンター公開鍵格納部と、前記センター公開鍵格納部に格納されている前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する第１署名検証部と、正当性が検証された前記メーカー公開鍵を用いて、前記記録媒体装置から受け取った前記署名データの正当性を検証することにより、前記記録媒体装置の正当性を検証する第２署名検証部とを備えることを特徴とする。

【００２１】

この構成によると、記録媒体装置の耐タンパー手段は、証明手段を備え、前記証明手段は、メーカー秘密鍵格納部、署名生成部とを備えるので、もし、記録媒体装置のメーカーが不正に記録媒体装置の識別情報を複数の記録媒体装置に複製したとしても、そのメーカーは、その不正な記録媒体装置に耐タンパー手段を複製できず、記録媒体装置は、識別情報に基づく証明情報を出力できず、正当な記録再生装置との間の認証に失敗する。こうして、記録媒体装置のメーカーによる不正行為を防止できる。

【００２２】

本発明の第５の態様に係る記録再生システムにおいて、前記証明手段は、前記識別情報を用いて、当該耐タンパー手段のメディア固有鍵を生成する第１メディア固有鍵生成手段と、前記メディア固有鍵を鍵として用いて、前記記録再生装置からのチャレンジデータからレスポンスデータとしての前記証明情報を生成し、生成したレスポンスデータとしての前記証明情報を出力する証明生成手段とを含み、前記検証手段は、前記記録媒体装置の前記識別情報を用いて、前記メディア固有鍵と同一のメディア固有鍵を生成する第２メディア固有鍵生成手段と、前記チャレンジデータを生成して出力し、前記記録媒体装置から取得したレスポンスデータとしての前記証明情報と、前記チャレンジデータとを用いて、前記記録媒体装置の正当性を検証する検証部とを備える。

【００２３】

本発明の第６の態様に係る記録再生システムにおいて、前記証明手段は、さらに、メディア鍵を生成する第１メディア鍵生成手段を備え、前記第１メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いてメディア固有鍵を生成し、前記検証手段は、さらに、前記第１メディア鍵生成手段にて生成されたメディア鍵と同一のメディア鍵を生成する第２メディア鍵生成手段を備え、前記第２メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いて前記メディア固有鍵を生成する。

【００２４】

本発明の第７の態様に係る記録再生システムにおいて、前記証明手段は、前記記録媒体装置の製造者のメーカー秘密鍵を格納しているメーカー秘密鍵格納部と、前記識別情報格納手段から前記識別情報を取得し、前記メーカー秘密鍵を用いて、取得した前記識別情報に対して、デジタル署名を施して、前記証明情報として署名データを生成する署名生成部とを含み、前記検証手段は、前記記録媒体装置の製造者のメーカー公開鍵を格納しているメーカー公開鍵格納部と、前記記録媒体装置から前記証明情報として前記署名データを取得し、前記メーカー公開鍵を用いて、取得した前記証明情報としての前記署名データに対して、デジタル署名検証を施し、検証に失敗した場合には、暗号化コンテンツの復号又はコンテンツの暗号化を禁止し、検証に成功した場合には、前記署名データから前記識別情報を取得する署名検証部とを含み、前記コンテンツ暗復号手段は、検証に成功した場合に取得された前記識別情報に基づき、前記コンテンツを暗号化し、又は前記暗号化コンテンツを復号する。

【００２６】

本発明の第８の態様に係る記録媒体装置は、暗号化されたコンテンツを格納するための記録媒体装置であって、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、前記証明手段は、前記識別情報を用いて、メディア固有鍵を生成する第

１メディア固有鍵生成手段と、前記メディア固有鍵を鍵として用いて、記録再生装置からのチャレンジデータからレスポンスデータとしての前記証明情報を生成し、生成したレスポンスデータとしての前記証明情報を出力する証明生成手段とを含む。

【００２７】

本発明の第９の態様に係る記録媒体装置において、前記証明手段は、さらに、メディア鍵を生成する第１メディア鍵生成手段を備え、前記第１メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いてメディア固有鍵を生成する。

【００２８】

本発明の第１０の態様に係る記録媒体装置において、前記メモリ手段は、さらに、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化メディア鍵群は、複数の暗号化メディア鍵を含み、複数の暗号化メディア鍵は、複数の装置に対応し複数の暗号化メディア鍵のそれぞれは、各装置に割り当てられたデバイス鍵を用いて、前記記録媒体装置のメディア鍵を暗号化して生成されたものであり、前記証明手段は、さらに、当該記録媒体装置に割り当てられたデバイス鍵を格納しているデバイス鍵格納手段を備え、前記第１メディア鍵生成手段は、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群から、当該記録媒体装置の暗号化メディア鍵を特定し、特定した暗号化メディア鍵を前記デバイス鍵を用いて復号して、前記メディア鍵を生成する。

【００２９】

本発明の第１１の態様に係る記録媒体装置において、前記耐タンパー手段は、半導体デバイスであるコントローラであり、前記メモリ手段は、さらに、暗号化された前記デバイス鍵を格納している暗号化デバイス鍵格納手段を備え、前記証明手段は、さらに、コントローラである当該耐タンパー手段に割り当てられたコントローラ鍵を格納しているコントローラ鍵格納手段と、前記暗号化デバイス鍵格納手段に格納されている暗号化された前記デバイスを、前記コントローラ鍵を用いて復号して、前記デバイス鍵を生成する復号手段とを備える。

【００３０】

本発明の第１２の態様に係る記録媒体装置において、前記メモリ手段は、さらに、暗号化された前記デバイス鍵を格納している暗号化デバイス鍵格納手段を備え、前記証明手段は、さらに、当該耐タンパー手段に固有の固有鍵を生成する固有鍵生成手段と、前記暗号化デバイス鍵格納手段に格納されている暗号化された前記デバイス鍵を、前記固有鍵を用いて復号して、前記デバイス鍵を生成する復号手段とを備える。

【００３１】

本発明の第１３の態様に係る記録媒体装置は、暗号化されたコンテンツを格納するための記録媒体装置であって、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、前記証明手段は、前記記録媒体装置の製造者のメーカー秘密鍵を格納しているメーカー秘密鍵格納部と、前記識別情報格納手段から前記識別情報を取得し、前記メーカー秘密鍵を用いて、取得した前記識別情報に対して、デジタル署名を施して、前記証明情報として署名データを生成する署名生成部とを含むことを特徴とする。

【００３２】

本発明の第１４の態様に係る記録媒体装置において、前記署名生成部は、記録再生装置から乱数を取得し、取得した前記識別情報及び取得した乱数の結合体に対して、デジタル署名を施す。

【００３３】

本発明の第１５の態様に係る記録媒体装置において、前記記録媒体装置のメモリ手段はさらに、信頼できるセンターにより、当該センターのセンター秘密鍵を用いて、前記メーカー秘密鍵に対応するメーカー公開鍵に対して発行されたメーカー公開鍵証明書を格納するメーカー公開鍵証明書格納部を備える。

【００３４】
本発明の第１６の態様に係る記録再生装置は、暗号化コンテンツを復号し、又はコンテンツを暗号化する記録再生装置であって、暗号化されたコンテンツを格納するための記録媒体装置から、当該記録媒体装置の識別情報に基づいて当該記録媒体装置の正当性を証明する証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記記録媒体装置に記録し、又は、前記識別情報に基づき、前記記録媒体装置から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段とを備えることを特徴とする。
【００３５】
本発明の第１７の態様に係る記録再生装置において、前記記録媒体装置は、耐タンパー手段及びメモリ手段を備え、メディア固有鍵を生成し、前記メディア固有鍵を鍵として用いて、前記記録再生装置からのチャレンジデータからレスポンスデータとしての前記証明情報を生成して出力し、前記検証手段は、前記記録媒体装置の前記識別情報を用いて、前記記録媒体装置で生成されたメディア固有鍵と同一のメディア固有鍵を生成する第２メディア固有鍵生成手段と、前記チャレンジデータを生成して出力し、前記記録媒体装置から取得したレスポンスデータとしての前記証明情報と、前記チャレンジデータとを用いて、前記記録媒体装置の正当性を検証する検証部とを備える。
【００３６】
本発明の第１８の態様に係る記録再生装置において、前記記録媒体装置は、さらに、メディア鍵を生成し、前記識別情報及び生成された前記メディア鍵を用いてメディア固有鍵を生成し、前記検証手段は、さらに、前記記録媒体装置に生成されたメディア鍵と同一のメディア鍵を生成する第２メディア鍵生成手段を備え、前記第２メディア固有鍵生成手段は、前記識別情報及び生成された前記メディア鍵を用いて前記メディア固有鍵を生成する
本発明の第１９の態様に係る記録再生装置において、前記記録媒体装置のメモリ手段はさらに、暗号化メディア鍵群を格納している暗号化メディア鍵群格納部を備え、前記暗号化メディア鍵群は、複数の暗号化メディア鍵を含み、複数の暗号化メディア鍵は、複数の装置に対応し、複数の暗号化メディア鍵のそれぞれは、各装置に割り当てられたデバイス鍵を用いて、前記記録媒体装置のメディア鍵を暗号化して生成されたものであり、前記検証手段は、さらに、当該記録再生装置に割り当てられたデバイス鍵を格納しているデバイス鍵格納手段を備え、前記第２メディア鍵生成手段は、前記暗号化メディア鍵群格納部に格納されている前記暗号化メディア鍵群から、当該記録再生装置の暗号化メディア鍵を特定し、特定した暗号化メディア鍵を前記デバイス鍵を用いて復号して、前記メディア鍵を生成する。
【００３７】
本発明の第２０の態様に係る記録再生装置において、前記検証手段は、前記記録媒体装置の製造者のメーカー公開鍵を格納しているメーカー公開鍵格納部と、前記記録媒体装置の製造者のメーカー秘密鍵を用いて、前記識別情報に対して、デジタル署名を施して生成された前記証明情報としての署名データを取得し、前記メーカー公開鍵を用いて、取得した前記証明情報としての前記署名データに対して、デジタル署名検証を施し、検証に失敗した場合には、前記暗号化コンテンツの復号又は前記コンテンツの暗号化を禁止し、検証に成功した場合には、前記署名データから前記識別情報を取得する署名検証部とを含み、前記コンテンツ暗復号手段は、検証に成功した場合に、取得された前記識別情報に基づき前記コンテンツを暗号化し、又は前記暗号化コンテンツを復号する。
【００３８】
本発明の第２１の態様に係る記録再生装置において、前記記録再生装置の前記検証手段は、さらに、乱数を生成し前記記録媒体装置へ送る乱数生成部を備え、前記検証手段は、前記識別情報及び前記乱数の結合体に対してデジタル署名が施されて生成された署名データを取得し、取得した前記証明情報と生成した乱数の結合体に基づき、前記記録媒体装置

の正当性を検証する。

【００３９】

本発明の第２２の態様に係る記録再生装置において、前記検証手段は、さらに、信頼できるセンターのセンター秘密鍵に対応するセンター公開鍵を格納するセンター公開鍵格納部と、前記センター公開鍵格納部の前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する署名検証部とを含む。

【００４０】

本発明の第２３の態様に係る記録再生方法は、暗号化コンテンツを復号し、又はコンテンツを暗号化する記録再生装置において用いられる記録再生方法であって、記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、前記記録再生方法は、前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証ステップと、前記検証ステップによる検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号ステップとを含むことを特徴とする。

【００４１】

本発明の第２４の態様に係るコンピュータプログラムは、暗号化コンテンツを復号し、又はコンテンツを暗号化する記録再生装置において用いられる記録再生のためのコンピュータプログラムであって、記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、コンピュータに、前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証ステップと、前記検証ステップによる検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号ステップとを実行させるための前記コンピュータプログラムであることを特徴とする。

【００４２】

本発明の第２５の態様に係るコンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている。

本発明の第２６の態様に係る集積回路において、記録媒体装置は、耐タンパー手段及びメモリ手段を備え、前記耐タンパー手段は、耐タンパー手段に固有の識別情報を格納している識別情報格納手段と、前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明手段とを含み、前記メモリ手段は、暗号化されたコンテンツを格納するための暗号化コンテンツ格納部を備え、前記集積回路は、前記記録媒体装置から前記証明情報を取得し、取得した前記証明情報に基づき、前記記録媒体装置の正当性を検証し、検証に失敗した場合に、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証手段と、前記検証手段による検証が成功した場合に、前記識別情報に基づき、コンテンツを暗号化して前記暗号化コンテンツ格納部に記録し、又は、前記識別情報に基づき、前記暗号化コンテンツ格納部から読み出した暗号化コンテンツを復号するコンテンツ暗復号手段とを備えることを特徴とする。

【００４３】

本発明の第２７の態様に係る製造方法は、半製品であるコントローラから記録媒体装置に組み込まれるべきコントローラを製造する製造方法であって、半製品であるコントローラは、耐タンパー性を有する半導体デバイスであり、識別情報格納手段と、前記識別情報格納手段に格納されるべき識別情報に基づいて自己の正当性を証明する証明情報を生成し生成した証明情報を出力する証明手段とを含み、前記証明手段は、コントローラ鍵格納部と、暗号化デバイス鍵を前記コントローラ鍵格納部に格納されるべきコントローラ鍵を用いて復号する復号部と、前記復号部により生成されたデバイス鍵及び暗号化メディア鍵群に基づき、メディア鍵を生成する第１メディア鍵生成部と、前記第１メディア鍵生成部で生成された前記メディア鍵と、前記識別情報格納手段に格納されている前記識別情報に基づき、メディア固有鍵を生成する第１メディア固有鍵生成部と、前記第１メディア固有鍵生成部により生成された前記メディア固有鍵を用いて、前記証明情報を生成する証明生成手段とを備え、（ａ）コントローラベンダのコンピュータにより、製造対象のコントローラに固有の識別情報を生成するステップと、（ｂ）コントローラベンダのコンピュータにより、コントローラに固有の、又は、所定数のコントローラの集合に固有のコントローラ鍵を生成するステップと、（ｃ）コントローラベンダの実装手段により、生成した前記識別情報を前記識別情報格納手段に格納するステップと、（ｄ）コントローラベンダの実装手段により、生成した前記コントローラ鍵を前記コントローラ鍵格納部に格納するステップと含むことを特徴とする。

【００４４】

本発明の第２８の態様に係る製造方法は、前記製造方法により製造されたコントローラを組み込んで記録媒体装置を製造する製造方法であって、（ｅ）コントローラベンダのコンピュータにより、コントローラベンダを識別するベンダＩＤと、前記コントローラ鍵を識別するコントローラ鍵識別情報と、前記コントローラ鍵とを鍵発行局であるセンターに送付するステップと、（ｆ）前記センターのコンピュータにより、前記ベンダＩＤと前記コントローラ鍵識別情報と前記コントローラ鍵を受け取るステップと、（ｇ）前記センターのコンピュータにより、受け取った前記ベンダＩＤと前記コントローラ鍵識別情報と前記コントローラ鍵とを前記センターのコンピュータの格納手段に格納するステップと、（ｈ）前記記録媒体装置メーカーのコンピュータにより、コントローラベンダに対して、コントローラの注文情報を送るステップと、（ｉ）前記コントローラベンダのコンピュータにより、コントローラの前記注文情報を受け付けるステップと、（ｊ）前記コントローラベンダにより、前記記録媒体装置メーカーに対して、前記コントローラを発行するステップと、（ｋ）前記コントローラベンダのコンピュータにより、前記記録媒体装置メーカーに対して、コントローラベンダのベンダＩＤと、前記コントローラに格納されたコントローラ鍵のコントローラ鍵識別情報を、発行するステップと、（ｌ）前記記録媒体装置メーカーにより、前記コントローラベンダから、前記コントローラを受け取るステップと、（ｍ）前記記録媒体装置メーカーのコンピュータにより、前記コントローラベンダから、前記ベンダＩＤと、前記コントローラ鍵識別情報とを受け取るステップと、（ｎ）前記記録媒体装置メーカーの組込装置により、受け取ったコントローラを前記記録媒体装置に実装するステップと、（ｏ）前記記録媒体装置メーカーのコンピュータにより、センターに対して、コントローラベンダから受け取った前記ベンダＩＤと、前記コントローラ鍵識別情報とを含むカードデバイス鍵注文情報を送るステップと、（ｐ）センターのコンピュータにより、前記記録媒体装置メーカーから、前記カードデバイス鍵注文情報を受け付けるステップと、（ｑ）センターのコンピュータにより、前記カードデバイス鍵注文情報に応じたデバイス鍵を生成するステップと、（ｒ）センターのコンピュータにより、前記格納手段から前記ベンダＩＤと、前記コントローラ鍵識別情報に対応するコントローラ鍵とを前記格納手段より取得し、取得したコントローラ鍵を用いて、生成したデバイス鍵を暗号化して、暗号化デバイス鍵を生成するステップと、（ｓ）センターのコンピュータによりメディア鍵を複数の記録媒体装置のデバイス鍵もしくは記録再生装置のデバイス鍵それぞれを用いて暗号化して得られる暗号化メディア鍵群を生成するステップと、（ｔ）センターのコンピュータにより、前記記録媒体装置メーカーに対して、生成した前記暗号化デバイ

ス鍵と、前記暗号化メディア鍵群とを、記録媒体装置のメーカーに発行するステップと（ｕ）前記記録媒体装置のメーカーのコンピュータにより、前記センターから前記暗号化デバイス鍵と、前記暗号化メディア鍵群とを受け取るステップと、（ｖ）前記記録媒体装置のメーカーの実装手段により、記録媒体装置のメモリの暗号化カードデバイス鍵格納部及び暗号化メディア鍵群格納部に、センターから受け取った暗号化カードデバイス鍵及び暗号化メディア鍵群を格納するステップとを含むことを特徴とする。

１．実施の形態１

以下、本発明に係る１の実施の形態について、図面を参照しながら説明する。

１．１　全体構成

図１は、本発明の実施の形態１における記録再生システム３００と、記録再生システムの製造に係るカードメーカー４００、装置メーカー５００、センター（鍵発行局）６００の全体関係を示す図である。記録再生システム３００は、複数のメモリカード１００、・・・及び複数の記録再生装置２００、・・・から構成される。なお、カードメーカー４００、装置メーカー５００及びセンター６００は、それぞれ、カードメーカー、装置メーカー及びセンターが有する装置を表している。

【００４５】

ここで、センター６００は、メモリカード１００の製造に関するライセンスを締結したカードメーカー４００に対して、メモリカード１００の製造に必要な複数のメディアＩＤ格納モジュール部６１０、・・・とメーカー公開鍵証明書６２０とを発行する。また、センター６００は、記録再生装置２００の製造に関するライセンスを締結した装置メーカー５００に対して、記録再生装置２００の製造に必要なセンター公開鍵６３０を発行する。メディアＩＤ格納モジュール部６１０、メーカー公開鍵証明書６２０、センター公開鍵６３０の詳細については後述する。

【００４６】

カードメーカー４００は、複数のメモリカード１００、・・・を製造し、センター６００から受け取ったメディアＩＤ格納モジュール部６１０と、メーカー公開鍵証明書６２０を、メモリカード１００、・・・に実装する。

【００４７】

装置メーカー５００は、センター６００から受け取ったセンター公開鍵６３０を記録再生装置２００に実装する。

１．２　センター６００、カードメーカー４００及び装置メーカー５００の構成

図２に、センター６００、カードメーカー４００及び装置メーカー５００の構成を示す

センター６００は、図２に示すように、メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書受付手段６４０、メディアＩＤ格納モジュール発行手段６５０、メーカー公開鍵証明書発行手段６６０、センター公開鍵注文書受付手段６７０及びセンター公開鍵発行手段６８０を備える。

【００４８】

カードメーカー４００は、図２に示すように、メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書送付手段４１０、メディアＩＤ格納モジュール受取手段４２０、メディアＩＤ格納モジュール実装手段４３０、メーカー公開鍵証明書受取手段４４０及びメーカー公開鍵証明書実装手段４５０を備える。

【００４９】

装置メーカー５００は、図２に示すように、センター公開鍵注文書送付手段５１０、センター公開鍵受取手段５２０及びセンター公開鍵実装手段５３０を備える。

１．３　センターとカードメーカー間の動作

センター６００とカードメーカー４００との間の動作について、図３に示すフローチャートを用いて説明する。

【００５０】

図３に示すように、カードメーカー４００のメーカー公開鍵証明書／メディアＩＤ格納モジュール注文書送付手段４１０は、センター６００に対して、メーカー公開鍵証明書／

メディアＩＤ格納モジュール注文書を送付する（Ｓ１０１）。
【００５１】
ここで、メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書の一例を図４に示す。図４に示すように、メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書８１０には、カードメーカーＩＤ、メーカー公開鍵証明書の要否、メディアＩＤ格納モジュール部の注文数（製造するメモリカードの数）等が記載される。ここで、カードメーカーＩＤは、カードメーカー毎に異なる固有の値であり、センター６００によりライセンス契約時に付与される。メーカー公開鍵証明書の要否欄は、通常、初回の注文時にのみ“要”とする。メディアＩＤ格納モジュール部の注文数欄には、カードメーカー４００が必要とするメディアＩＤ格納モジュール部の注文数を記載する。このようにして、カードメーカー４００は、必要に応じて、その都度、メディアＩＤ格納モジュール部を注文することができる。
【００５２】
次に、センター６００のメーカー公開鍵証明書／メディアＩＤ格納モジュール注文書受付手段６４０は、カードメーカー４００からメーカー公開鍵証明書／メディアＩＤ格納モジュール注文書を受け付ける（Ｓ１０２）。メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書のメーカー公開鍵証明書の要否欄が“要”である場合は、カードメーカー４００に対して、メーカー公開鍵証明書発行手段６６０は、メーカー公開鍵証明書を発行する（Ｓ１０３）。そして、メディアＩＤ格納モジュール発行手段６５０は、メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書のメディアＩＤ格納モジュール部の注文数欄の数に応じて、メディアＩＤ格納モジュール部をカードメーカー４００に発行する（Ｓ１０４）。
【００５３】
なお、メディアＩＤ格納モジュール部の発行形態については、後述するように、センター６００がカードメーカー４００に、ＬＳＩ等の半導体デバイスであるメディアＩＤ格納デバイスとして提供する方法と、ＬＳＩ等の半導体デバイスを製造するのに必要な回路ＩＰであるメディアＩＤ格納回路ＩＰとして提供する方法がある。前者の場合は、ステップＳ１０４で、メディアＩＤ格納モジュール部の注文数欄の数に応じて、注文数のメディアＩＤ格納モジュール部としてメディアＩＤ格納デバイスをカードメーカーに発行する。後者の場合には、注文数に係らず、メディアＩＤ格納モジュール部として、メディアＩＤ格納回路ＩＰを発行する。
【００５４】
次に、カードメーカー４００のメーカー公開鍵証明書受取手段４４０は、センター６００から、メーカー公開鍵証明書を受け取る（Ｓ１０５）。カードメーカー４００のメディアＩＤ格納モジュール受取手段４２０は、センター６００から、メディアＩＤ格納モジュール部を受け取る（Ｓ１０６）。
【００５５】
そして、カードメーカー４００のメディアＩＤ格納モジュール実装手段４３０及びメーカー公開鍵証明書実装手段４５０は、メモリカード１００の製造において、各メモリカードに、それぞれ、メーカー公開鍵証明書と、メディアＩＤ格納モジュール部とを実装する（Ｓ１０７、Ｓ１０８）。具体的には、ステップＳ１０６において、メディアＩＤ格納モジュール部としてメディアＩＤ格納デバイスをセンター６００から受け取った場合は、ステップＳ１０８において、受け取ったメディアＩＤ格納デバイスを各メモリカードに実装する。また、メディアＩＤ格納モジュール部としてメディアＩＤ格納回路ＩＰをセンター６００から受け取った場合は、カードメーカーが、当該メディアＩＤ格納回路ＩＰに基づき製造したメディアＩＤ格納デバイスを各メモリカード１００に実装する。
カードメーカー４００は、メディアＩＤ格納モジュール部のストックが少なくなれば、（又は、無くなれば）、センター６００に、再び、メーカー公開鍵証明書／メディアＩＤ格納モジュール注文書を送付する。
【００５６】

図５に、メーカー公開鍵証明書の構成を示す。図５に示すように、メーカー公開鍵証明書８２０は、カードメーカー４００を識別するためのカードメーカーＩＤと、カードメーカー毎に異なる公開鍵であるメーカー公開鍵と、カードメーカーＩＤとメーカー公開鍵に対してセンター６００が発行するデジタル署名であるセンター発行署名とを含んで構成される。

【００５７】

ここで、センター発行署名の生成には、ＲＳＡ（Rivest Shamir Adleman）署名関数を用いる。ＲＳＡ署名関数については、広く知られているので説明は省略する。

なお、ここではＲＳＡ署名アルゴリズムを用いる場合を示すが、他のデジタル署名アルゴリズムを用いてもよい。

【００５８】

また、センター６００は、センター発行署名の生成に用いるセンター秘密鍵と、それに対応し、後述するセンター発行署名の検証に用いるセンター公開鍵を予め生成し管理しているものとする。また、センター６００は、カードメーカー毎に、メーカー公開鍵と、それに対応し、後述するメディアＩＤ格納モジュール部に格納されるメーカー秘密鍵を、予め生成し管理しているものとする。

【００５９】

ここでは、ＲＳＡ署名生成関数を、ＲＳＡ－ＳＩＧＮ（秘密鍵、被署名データ）、ＲＳＡ署名検証関数を、ＲＳＡ－ＶＥＲＩＦＹ（公開鍵、署名データ）と表す。このとき、センター発行署名＝ＲＳＡ－ＳＩＧＮ（センター秘密鍵、メーカーＩＤ‖メーカー公開鍵）となる。ここで、Ａ‖Ｂは、データＡとデータＢの連結を示す。

１．４　メディアＩＤ格納モジュール部６１０の構成

図６に、メディアＩＤ格納モジュール部６１０の構成を示す。図６に示すように、メディアＩＤ格納モジュール部６１０は、耐タンパー（tamper resistant）モジュールでありメディアＩＤ格納部６１１、メーカー秘密鍵格納部６１２及び署名生成部６１３から構成される。メーカー秘密鍵格納部６１２及び署名生成部６１３は、証明部６０９を構成し、証明部６０９は、後述するように、メディアＩＤ格納モジュール部６１０の正当性を示す証明情報を生成する。

【００６０】

センター６００からカードメーカー４００に発行される耐タンパー化されたメディアＩＤ格納モジュール部６１０の実現手段、及び発行形態として以下の２通りがある。

（ａ）センター６００が、メディアＩＤ格納モジュール部をＬＳＩ等の半導体デバイスであるメディアＩＤ格納デバイスとして実現し、カードメーカー４００に発行する。このとき、センター６００は、カードメーカー４００からの注文数に応じて、その注文数のメディアＩＤ格納デバイスを発行する。すなわち、注文数が１０００の場合、１０００個のメディアＩＤ格納デバイスを発行する。カードメーカー４００において、発行されたメディアＩＤ格納デバイスを、各メモリカードに１つずつ実装する。

【００６１】

（ｂ）センター６００が、メディアＩＤ格納モジュール部を、（ａ）のメディアＩＤ格納デバイスを製造するために必要な設計情報である回路ＩＰであるメディアＩＤ格納回路ＩＰとして実現し、メディアＩＤ格納回路ＩＰをカードメーカー４００に発行する。この場合、カードメーカー４００において、センター６００から発行されたメディアＩＤ格納回路ＩＰに基づき、製造するメモリカードの数のメディアＩＤ格納デバイスを製造し、製造したメディアＩＤ格納デバイスを各メモリカードに、１つずつ実装する。

【００６２】

なお、（ａ）の場合、メディアＩＤ格納モジュール部はハードウェア的に耐タンパー化されたＬＳＩ等の半導体デバイスとして実現される。そのため、カードメーカー４００がメディアＩＤ格納モジュール部の内部のメディアＩＤ格納部６１１の解析が困難となり、メディアＩＤを書き換えることは困難となる。また、後述するように、メディアＩＤ格納部６１１を電気ヒューズやＰＵＦ（Ｐｈｙｓｉｃａｌ　Ｕｎｃｌｏａｎａｂｌｅ　Ｆｕｎ

ｃｔｉｏｎ）等の技術を用いて実現するため、同じメディアＩＤを生成するようにＬＳＩを複製することは困難となる。

【００６３】

また、（ｂ）の場合は、メディアＩＤ格納モジュール部は、回路ＩＰとして実現されるそのため、カードメーカー４００が、メディアＩＤ格納モジュール部の内部のメディアＩＤを書き換えることを困難とするよう、回路ＩＰを必要に応じて難読化するものとする。このため、カードメーカー４００が、メディアＩＤ格納モジュール部の内部のメディアＩＤ格納部６１１の解析が困難となり、メディアＩＤを書き換えることは困難となる。また後述の通りメディアＩＤ格納部６１１をＰＵＦ等の技術を用いて実現するため、同じメディアＩＤを生成するようにＬＳＩを複製することは困難となる。

【００６４】

次に、メディアＩＤ格納モジュール部６１０のメディアＩＤ格納部６１１は、各メモリカードに実装されたときに、それぞれ、メディアＩＤ格納モジュール部毎に異なる固有のメディアＩＤ（言い換えると、メディア識別情報）として１２８ビットの異なる数値を格納するよう構成される。一般に、ＬＳＩ等の半導体デバイスにおいて、半導体デバイス毎に異なる固有のデータを生成する手段としては、電気ヒューズ等により固有データを半導体デバイス毎に設定する手段や、ＰＵＦ（Ｐｈｙｓｉｃａｌ　Ｕｎｃｌｏａｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ）等を半導体デバイスに実装し、半導体デバイス毎に、ＰＵＦの実装のばらつきを利用して、異なるデータを生成する手段がある。メディアＩＤ格納部６１１はこれらの手段を用いて実現する。

【００６５】

メーカー秘密鍵格納部６１２は、カードメーカー毎に異なるメーカー秘密鍵（ＲＳＡ署名生成用の秘密鍵）を格納する。

署名生成部６１３は、ＲＳＡ署名生成関数を用いて、メディアＩＤ署名データを生成する。メディアＩＤ署名データを図７に示す。図７に示すように、メディアＩＤ署名データ８３０は、乱数、メディアＩＤ、メモリカード発行署名からなる。メディアＩＤ署名データは、前記証明情報である。

【００６６】

ここで、メディアＩＤは、メディアＩＤ格納部６１１に格納されたメディアＩＤである乱数は、後述するように、記録再生装置２００から受け取る乱数である。メモリカード発行署名は、ＲＳＡ－ＳＩＧＮ（メーカー秘密鍵、乱数‖メディアＩＤ）にて生成される。

１．５　センター６００と装置メーカー５００との間の動作

センター６００と装置メーカー５００と間の動作について、図８に示すフローチャートを用いて説明する。

【００６７】

図８に示すように、記録再生装置の製造ライセンスを締結した装置メーカー５００のセンター公開鍵注文書送付手段５１０が、センター６００に対して、センター公開鍵注文書を送付する（Ｓ２０１）。

【００６８】

図９に、センター公開鍵注文書の一例を示す。図９に示すように、センター公開鍵注文書８４０には、装置メーカーＩＤ、センター公開鍵の要否及び、センター公開鍵を実装する記録再生装置の数（製造する記録再生装置数）が記載される。ここで、装置メーカーＩＤは、装置メーカー毎に異なる固有の値であり、センター６００によりライセンス契約時に付与される。センター公開鍵の要否欄は、通常、初回の注文時にのみ“要”とする。製造する記録再生装置の数欄は、装置メーカー５００がセンター公開鍵を実装して製造する記録再生装置の数を記載する。このようにして、装置メーカー５００は、センター公開鍵を注文することができる。

【００６９】

次に、センター６００のセンター公開鍵注文書受付手段６７０は、装置メーカー５００からセンター公開鍵注文書を受け付ける（Ｓ２０２）。センター６００のセンター公開鍵

発行手段６８０は、センター公開鍵注文書のセンター公開鍵の要否欄が“要”の場合は、装置メーカー５００に対して、センター公開鍵を発行する（Ｓ２０３）。

【００７０】

次に、装置メーカー５００のセンター公開鍵受取手段５２０は、センター６００から、センター公開鍵を受け取る（Ｓ２０４）。

そして、装置メーカー５００のセンター公開鍵実装手段５３０は、記録再生装置２００を製造する際、各記録再生装置２００に、それぞれ、センター公開鍵を実装する（Ｓ２０５）。

１．６　記録再生システム３００の構成

記録再生システム３００は、図１に示すように、複数のメモリカード１００、・・・及び複数の記録再生装置２００、・・・から構成される。代表例として、図１０に、記録再生システム３００を構成するメモリカード１００及び記録再生装置２００の詳細の構成を示す。

（１）メモリカード１００の詳細の構成

図１０に示すように、メモリカード１００は、制御部１１０、メモリ部１２０、メディアＩＤ格納モジュール部６１０から構成される。

【００７１】

制御部１１０は、メディアＩＤ格納モジュール部６１０、及び、メモリ部１２０に対する所定の制御処理を行うとともに、記録再生装置２００からの要求に応じて、所定の制御処理を行う。具体的には、制御部１１０は、記録再生装置２００からの要求に応じて、メディアＩＤ格納モジュール部６１０に対して、メディアＩＤ署名データの生成を要求し、生成されたメディアＩＤ署名データを取得し、記録再生装置２００に送ったり、記録再生装置２００から受け取った暗号化コンテンツをメモリ部１２０に格納したりという制御処理を行う。

【００７２】

メモリ部１２０は、さらに、メーカー公開鍵証明書格納部１２１、暗号化コンテンツ格納部１２２で構成される。メモリ部１２０のメーカー公開鍵証明書格納部１２１は、記録再生装置２００からのデータの読み出しのみが可能な領域であり、メモリカード製造時にカードメーカー４００が、センター６００から受け取ったメーカー公開鍵証明書を格納する。メモリ部１２０の暗号化コンテンツ格納部１２２は、記録再生装置２００からデータの読み書きができる領域であり、記録再生装置２００によって暗号化されたコンテンツが格納される。

【００７３】

また、メディアＩＤ格納モジュール部６１０には、カードメーカー４００がセンター６００からＬＳＩ等の半導体デバイスの形態でメディアＩＤ格納モジュール部を受け取った場合は、受け取ったメディアＩＤ格納モジュール部が、そのままメモリカード１００に実装される。カードメーカー４００がセンター６００から、メディアＩＤ格納モジュール部に代えて、回路ＩＰを受け取った場合は、カードメーカー４００が受け取った回路ＩＰに基づき製造したＬＳＩ等の半導体デバイスが、メモリカード１００に実装される。メディアＩＤ格納モジュール部６１０の内部構成については、既に説明済であるので省略する。

【００７４】

ここで、制御部１１０は、例えば、ＬＳＩ等の半導体デバイスで構成され、メモリ部１２０は、例えば、フラッシュメモリで構成され、メディアＩＤ格納モジュール部６１０はＬＳＩ等の半導体デバイスで構成される。

（２）記録再生装置２００の詳細の構成

記録再生装置２００は、図１０に示すように、メモリカード検証部２１１、メディアＩＤ取得部２０６、コンテンツ鍵生成部２０７、コンテンツ受信部２０８、コンテンツ暗復号部２０９及びコンテンツ再生部２１０から構成される。メモリカード検証部２１１は、署名検証部２０１、センター公開鍵格納部２０２、乱数生成部２０３、署名検証部２０４及びメーカー公開鍵格納部２０５から構成される。

【００７５】
メモリカード検証部２１１は、メモリカード１００から受け取ったメーカー公開鍵証明書及びメディアＩＤ署名データを検証する。この検証により、そのメモリカード１００が正しいメモリカードか、不正なメモリカードかを判別することができる。
【００７６】
以下、メモリカード検証部２１１を構成する署名検証部２０１、センター公開鍵格納部２０２、乱数生成部２０３、署名検証部２０４及びメーカー公開鍵格納部２０５について説明する。
【００７７】
署名検証部２０１は、メモリカード１００のメーカー公開鍵証明書格納部１２１からメーカー公開鍵証明書を受け取り、受け取ったメーカー公開鍵証明書に含まれるセンター発行署名をＲＳＡ署名検証関数を用いて検証する。検証が成功した場合は、受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵をメーカー公開鍵格納部２０５に送る。
【００７８】
なお、具体的な検証処理については、後述する。また、メーカー公開鍵証明書の構成については、既に説明済であるので説明を省略する（図５参照）。
センター公開鍵格納部２０２は、装置メーカー５００により、記録再生装置２００の製造時に、センターから受け取ったセンター公開鍵を格納している。
【００７９】
乱数生成部２０３は、乱数を生成し、メモリカードに送る。乱数の長さは、例えば、１２８ビットとする。
署名検証部２０４は、メーカー公開鍵格納部２０５から受け取ったメーカー公開鍵を用いて、メモリカード１００から受け取ったメディアＩＤ署名データを検証する。この場合における署名の検証は、回復型検証である。検証が成功した場合、検証の対象であるメディアＩＤ署名データからメディアＩＤが取り出され、取り出されたメディアＩＤをメディアＩＤ取得部２０６に送る。なお、具体的な検証処理については、後述する。
【００８０】
メーカー公開鍵格納部２０５は、署名検証部２０１から受け取ったメーカー公開鍵が格納される。
次に、メディアＩＤ取得部２０６は、署名検証部２０４において検証に成功したときのみ、署名検証部２０４からメディアＩＤを取得し、取得したメディアＩＤをコンテンツ鍵生成部２０７に送る。
【００８１】
コンテンツ鍵生成部２０７は、メディアＩＤ取得部から受け取ったメディアＩＤに基づいてコンテンツ鍵を生成する。具体的な、コンテンツ鍵生成法については、後述する。
コンテンツ受信部２０８は、デジタル放送されたデジタルコンテンツや、デジタル配信されたデジタルコンテンツを受信し、受信したデジタルコンテンツをコンテンツ暗復号部２０９に送る。
【００８２】
コンテンツ暗復号部２０９は、コンテンツ鍵生成部２０７から受け取ったコンテンツ鍵を用いて、コンテンツ受信部２０８より受け取ったデジタルコンテンツを暗号化してメモリカード１００に送る。又は、コンテンツ暗復号部２０９は、メモリカード１００から受け取った暗号化デジタルコンテンツを復号して、生成したデジタルコンテンツをコンテンツ再生部２１０に送る。コンテンツの暗復号の詳細については、後述する。
【００８３】
コンテンツ再生部２１０は、コンテンツ暗復号部２０９から復号されたデジタルコンテンツを受け取り、受け取ったデジタルコンテンツを再生する。ここで、デジタルコンテンツの再生とは、圧縮符号化された映像及び音声のデジタル信号を、伸張して映像及び音声のデジタル信号を生成し、生成した映像及び音声のデジタル信号を記録再生装置２００に接続された外部の表示装置へ出力することを言う。また、デジタルコンテンツの再生とは

コンテンツ再生部２１０が映像表示部及び音声出力部を備える場合には、圧縮符号化された映像及び音声のデジタル信号を、伸張して映像及び音声のデジタル信号を生成し、生成した映像及び音声のデジタル信号を映像表示部及び音声出力部へ出力し、映像表示部は映像を表示し、音声出力部は音声を出力することを言う。

１．７　記録再生システム３００の動作

（１）記録時の動作

記録再生装置２００がメモリカード１００にコンテンツを記録する際の動作について、図１１に示すフローチャートを用いて説明する。

【００８４】

図１１に示すように、記録再生装置２００の乱数生成部２０３は、１２８ビットの乱数を生成し、メモリカード１００に送付する（Ｓ３０１）。メモリカード１００の制御部１１０は、記録再生装置２００から、１２８ビットの乱数を受け取り（Ｓ３０２）、署名生成部６１３に送る。メモリカード１００の署名生成部６１３は、メーカー秘密鍵格納部６１２からメーカー秘密鍵を、メディアＩＤ格納部６１１から、１２８ビットのメモリカード毎に固有のメディアＩＤを受け取る。メモリカード１００の署名生成部６１３は、メーカー秘密鍵を用いて、乱数とメディアＩＤに対する署名（メモリカード発行署名）を以下の式により生成し、乱数、メディアＩＤ、及び、生成されたメモリカード発行署名からなるメディアＩＤ署名データを制御部１１０に送る（Ｓ３０３）。図７に、メディアＩＤ署名データの構成例を示す。

【００８５】

メモリカード発行署名＝ＲＳＡ－ＳＩＧＮ（メーカー秘密鍵、乱数‖メディアＩＤ）

ここで、ＲＳＡ－ＳＩＧＮは、これにより生成されたメディアＩＤ署名データの検証に成功した場合に、乱数‖メディアＩＤが取り出される回復型署名である。

【００８６】

次に、メモリカード１００の制御部１１０は、署名生成部６１３から受け取ったメディアＩＤ署名データと、メーカー公開鍵証明書格納部１２１から読み出したメーカー公開鍵証明書を記録再生装置２００に送る（Ｓ３０４）。

【００８７】

記録再生装置２００の署名検証部２０４は、メモリカード１００からメディアＩＤ署名データ及びメーカー公開鍵証明書を受け取る（Ｓ３０５）。記録再生装置の署名検証部２０１は、ステップＳ３０５でメモリカードから受け取ったメーカー公開鍵証明書と、センター公開鍵格納部２０２から読み出したセンター公開鍵を用いて以下の式が成り立つか否かを検証する（Ｓ３０６）。

【００８８】

（メーカーＩＤ‖メーカー公開鍵）＝

ＲＳＡ－ＶＥＲＩＦＹ（センター公開鍵、センター発行署名）

ここで、メーカー公開鍵とセンター発行署名は、図５に示す通り、メーカー公開鍵証明書に含まれており、センター発行署名は、既に説明の通り、以下の式で与えられる。

【００８９】

センター発行署名＝ＲＳＡ－ＳＩＧＮ（センター秘密鍵、メーカーＩＤ‖メーカー公開鍵）

そして、上記検証式が成り立つ場合、署名検証部２０１は、メーカー公開鍵格納部２０５にメーカー公開鍵を格納し、次のステップに進む。上記検証式が成り立たない場合、コンテンツの記録処理を終了する。

【００９０】

次に、署名検証部２０１は、ステップＳ３０６の検証式が成り立つ場合、ステップ３０５でメモリカード１００から受け取ったメディアＩＤ署名データと、メーカー公開鍵格納部２０５から取得したメーカー公開鍵（ステップＳ３０６で正当性が検証されたメーカー公開鍵）を用いて以下の式が成り立つか否かを検証する（Ｓ３０７）。

【００９１】

（乱数‖メディアＩＤ）＝
　ＲＳＡ－ＶＥＲＩＦＹ（メーカー公開鍵、メモリカード発行署名）
ここで、乱数とメディアＩＤは、図７に示す通り、メディアＩＤ署名データに含まれており、メモリカード発行署名は、既に説明の通り、以下の式で与えられる。
【００９２】
メモリカード発行署名＝ＲＳＡ－ＳＩＧＮ（メーカー秘密鍵、乱数‖メディアＩＤ）
そして、上記検証式が成り立つ場合、署名検証部２０４は、メディアＩＤをメディアＩＤ取得部２０６に送り、次のステップに進む。上記検証式が成り立たない場合、署名検証部２０４は、コンテンツの記録処理を終了する。これにより、署名検証部２０４は、暗号化コンテンツの復号又はコンテンツの暗号化を禁止している。
【００９３】
メディアＩＤ取得部２０６は、ステップＳ３０７で正当性が検証された場合、署名検証部２０４からメディアＩＤ（ステップＳ３０７で正当性が検証されたメディアＩＤ）を取得する（Ｓ３０８）。
【００９４】
コンテンツ鍵生成部２０７は、メディアＩＤ取得部２０６から取得したメディアＩＤに対して、次の式により、一方向性関数Ｆを用いて、コンテンツ鍵を生成し、コンテンツ鍵をコンテンツ暗復号部２０９に送る（Ｓ３０９）。
【００９５】
　コンテンツ鍵＝Ｆ（メディアＩＤ）
一方向性関数Ｆの具体例としては、例えば、ＡＥＳ（Advanced EncryptionStandard）暗号を用いて、以下の式で実現できる。
【００９６】
コンテンツ鍵＝
　ＡＥＳ－Ｅ（コンテンツ鍵生成用秘密鍵、メディアＩＤ）（＋）メディアＩＤ
ここで、（＋）は、排他的論理和演算を表す。また、コンテンツ鍵生成用秘密鍵は、１２８ビットであり、全ての記録再生装置に共通で秘密であり、予め、コンテンツ鍵生成部２０７が保持しているものとする。ＡＥＳ暗号については、広く知られているので説明は省略する。また、本明細書において、Ｘ＝ＡＥＳ－Ｅ（Ｙ、Ｚ）は、ＡＥＳ暗号関数により、鍵Ｙを用いて、平文Ｚを暗号化して暗号文Ｘを生成することを示す。Ｚ＝ＡＥＳ－Ｄ（Ｙ、Ｘ）は、ＡＥＳ復号関数により、鍵Ｙを用いて、暗号文Ｘを暗号化して復号文Ｚを生成することを示す。
【００９７】
なお、ここでは、コンテンツ鍵生成関数としてＡＥＳ暗号を用いる例を示したが、１２８ビットのメディアＩＤに基づき、１２８ビットのランダムな乱数を、コンテンツ鍵として生成する一方向性関数であればどんな構成でもよい。
【００９８】
コンテンツ暗復号部２０９は、コンテンツ受信部２０８にて受信されたデジタル放送されたデジタルコンテンツ、又は、デジタル配信されたデジタルコンテンツを、コンテンツ鍵生成部２０７から受け取ったコンテンツ鍵を用いて、暗号化し（Ｓ３１０）、メモリカード１００に暗号化されたデジタルコンテンツをメモリカード１００に送付する（Ｓ３１１）。
【００９９】
ここで、コンテンツの暗号化は、例えば、以下の式を用いて行う。
　暗号化されたデジタルコンテンツ＝ＡＥＳ－ＥＣＢＣ（コンテンツ鍵、デジタルコンテンツ）
ここで、ＡＥＳ－ＥＣＢＣとは、ＡＥＳ暗号をＣＢＣモード（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）で利用して暗号化することを示す。ＣＢＣモードについては、広く知られているので説明を省略する。また、本明細書において、Ｘ＝ＡＥＳ－ＥＣＢＣ（Ｙ、Ｚ）は、ＣＢＣモードでＡＥＳ暗号関数により、鍵Ｙを用いて、平文Ｚを暗号化して

暗号文Ｘを生成することを示す。Ｚ＝ＡＥＳ－ＤＣＢＣ（Ｙ、Ｘ）は、ＣＢＣモードでＡＥＳ復号関数により、鍵Ｙを用いて、暗号文Ｘを暗号化して復号文Ｚを生成することを示す。なお、ここでは、ＡＥＳ－ＥＣＢＣを用いる場合を示したが、この構成に限定されない。

【０１００】

メモリカード１００の制御部１１０は、記録再生装置２００から暗号化されたデジタルコンテンツを受け取り、暗号化されたデジタルコンテンツを暗号化コンテンツ格納部１２２に格納する（Ｓ３１２）。

【０１０１】

（２）再生時の動作

記録再生装置２００がメモリカード１００から暗号化コンテンツを読み出し再生する際の動作について、図１２に示すフローチャートを用いて説明する。

【０１０２】

なお、図１２のＳ４０１からＳ４０９は、それぞれ、図１１のＳ３０１からＳ３０９と全く同じ動作であるので、説明を省略する。

記録再生装置２００は、メモリカード１００に暗号化コンテンツの送付を要求する（Ｓ４１０）。メモリカード１００の制御部１１０は、記録再生装置２００からの暗号化コンテンツの送付要求に対応して、暗号化コンテンツ格納部１２２から暗号化コンテンツを読み出し、読み出した暗号化コンテンツを記録再生装置２００に送付する（Ｓ４１１）。コンテンツ暗復号部２０９は、メモリカード１００から、受け取った暗号化コンテンツを、コンテンツ鍵生成部２０７から受け取ったコンテンツ鍵を用いて復号し、復号したコンテンツをコンテンツ再生部２１０に送る（Ｓ４１２）。

【０１０３】

ここで、コンテンツの復号は、以下の式で表される。

復号されたコンテンツ＝ＡＥＳ－ＤＣＢＣ（コンテンツ鍵、暗号化されたデジタルコンテンツ）

ここで、ＡＥＳ－ＤＣＢＣとは、ＡＥＳ暗号をＣＢＣモード（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）で利用して復号することを示す。

【０１０４】

コンテンツ再生部２１０は、コンテンツ暗復号部２０９から受け取った、復号されたコンテンツを再生する（Ｓ４１３）。

１．８　不正の判別

以上の構成により、本発明の実施の形態１の構成によれば、カードメーカー４００が、不正なメモリカードを製造したとしても、記録再生装置２００のメモリカード検証部２１１により、正しく製造されたメモリカードか、不正なメモリーカードかの判別が可能となる。このことを、図１３を用いて説明する。

【０１０５】

図１３において、メモリカード１００は、本発明の実施の形態１に係るメモリカード（以下、正規のメモリカードと称する）、記録再生装置２００は、本発明の実施の形態１に係る記録再生装置（以下、正規の記録再生装置と称する）であり、メモリカード１０Ｃは、不正なカードメーカーが、本発明の実施の形態１に係るメモリカード１００と記録再生装置２００を動作させることにより、メディアＩＤを取得し、従来の構成のメモリカード１０Ｃのメディア ＩＤ格納部１３Ｃに格納して製造したメモリカード（以下、不正なメモリカードと称する）である。

【０１０６】

このとき、不正なメモリカード１０Ｃを用いて、正規の記録再生装置２００により記録再生処理を試みたとしても、不正なメモリカード１０Ｃは、正規の記録再生装置２００から受け取った乱数に対応するメディアＩＤ署名を生成できない。そのため、正規の記録再生装置２００において、メモリカード検証部２１１の署名検証部２０４は署名検証処理に失敗する。すなわち、カードメーカーが、不正なメモリカードを製造したとしても、正規

の記録再生装置２００により、正規のメモリカードか不正なメモリカードかの判別が可能となる。

２．実施の形態２

本発明に係る他の実施の形態について、図面を参照しながら説明する。

２．１　全体構成

図１４は、実施の形態２における記録再生システム３００ａ、記録再生システム３００ａの製造に係るカードメーカー４００ａ、装置メーカー５００ａ及びセンター（鍵発行局）６００ａの全体関係を示す図である。記録再生システム３００ａは、複数のメモリカード１００ａ、・・・及び複数の記録再生装置２００ａ、・・・から構成される。なお、カードメーカー４００ａ、装置メーカー５００ａ及びセンター６００ａは、それぞれ、カードメーカー、装置メーカー及びセンターが有する装置を表している。

【０１０７】

ここで、センター６００ａは、メモリカード１００ａの製造に関するライセンスを締結したカードメーカー４００ａに対して、メモリカード１００ａの製造に必要な１個以上のメディアＩＤ格納モジュール部６１０ａ、暗号化カードデバイス鍵６２５ａ及び暗号化メディア鍵群６２０ａを発行する。また、センター６００ａは、記録再生装置２００ａの製造に関するライセンスを締結した装置メーカー５００ａに対して、記録再生装置の製造に必要な装置デバイス鍵６３０ａを発行する。メディアＩＤ格納モジュール部６１０ａ、暗号化カードデバイス鍵６２５ａ、暗号化メディア鍵群６２０ａ、装置デバイス鍵６３０ａの詳細については後述する。

【０１０８】

カードメーカー４００ａは、センター６００ａから受け取ったメディアＩＤ格納モジュール部６１０ａ、暗号化カードデバイス鍵６２５ａ及び暗号化メディア鍵群６２０ａを、メモリカード１００aに実装する。

【０１０９】

また、装置メーカー５００ａは、センター６００ａから受け取った装置デバイス鍵６３０ａを記録再生装置２００aに実装する。

２．２　センター６００ａ、カードメーカー４００ａ及び装置メーカー５００ａの構成

図１５に、センター６００ａ、カードメーカー４００ａ及び装置メーカー５００ａの構成を示す。

【０１１０】

センター６００ａは、図１５に示すように、メディアＩＤ格納モジュール注文書受付手段６４０ａ、メディアＩＤ格納モジュール発行手段６５０ａ、カードデバイス鍵／暗号化メディア鍵群注文書受付手段６６０ａ、カードデバイス鍵／暗号化メディア鍵群発行手段６７０ａ、装置デバイス鍵注文書受付手段６８０ａ、装置デバイス鍵発行手段６９０ａ、暗号化カード固有鍵復号手段６２１ａ、暗号化カードデバイス鍵生成手段６２２ａ及びデバイス鍵／暗号化メディア群生成手段６２３ａを備える。

【０１１１】

カードメーカー４００ａは、図１５に示すように、メディアＩＤ格納モジュール注文書送付手段４１０ａ、メディアＩＤ格納モジュール受取手段４２０ａ、メディアＩＤ格納モジュール実装手段４３０ａ、カードデバイス鍵／暗号化メディア鍵群注文書送付手段４４０ａ、暗号化カード固有鍵取得手段４５０ａ、カードデバイス鍵／暗号化メディア鍵群受取手段４６０ａ及びカードデバイス鍵／暗号化メディア鍵群実装手段４７０ａを備える。

【０１１２】

装置メーカー５００ａは、図１５に示すように、装置デバイス鍵注文書送付手段５１０ａ、装置デバイス鍵受取手段５２０ａ及び装置デバイス鍵実装手段５３０ａを備える。

２．３　センターとカードメーカーとの間の動作

センター６００ａとカードメーカー４００ａとの間の動作について、図１６に示すフローチャートを用いて説明する。

【０１１３】

図１６に示すように、カードメーカー４００ａのメディアＩＤ格納モジュール注文書送付手段４１０ａは、センター６００ａに対して、メディアＩＤ格納モジュール注文書を送付する（Ｓ１０１ａ）。

【０１１４】

ここで、メディアＩＤ格納モジュール注文書の一例を図１７に示す。図１７に示すように、メディアＩＤ格納モジュール注文書８５０には、カードメーカーＩＤ、メディアＩＤ格納モジュール部の注文数（製造するメモリカードの数）等が記載される。ここで、カードメーカーＩＤは、カードメーカー毎に異なる固有の値であり、センター６００ａによりライセンス契約時に付与される。メディアＩＤ格納モジュールの注文数欄は、カードメーカー４００ａが必要とするメディアＩＤ格納モジュールの注文数を記載する。このようにして、カードメーカー４００ａは、必要に応じて、その都度、必要な個数のメディアＩＤ格納モジュール部を注文することができる。

【０１１５】

次に、センター６００ａのメディアＩＤ格納モジュール注文書受付手段６４０ａは、カードメーカー４００ａからメディアＩＤ格納モジュール注文書を受け付ける（Ｓ１０２ａ）。メディアＩＤ格納モジュール発行手段６５０ａは、メディアＩＤ格納モジュール部をカードメーカー４００ａに発行する（Ｓ１０３ａ）。

【０１１６】

なお、メディアＩＤ格納モジュール部の発行形態については、実施の形態１の場合と同様に、センター６００ａがカードメーカー４００ａに、ＬＳＩ等の半導体デバイスであるメディアＩＤ格納デバイスとして提供する方法と、ＬＳＩ等の半導体デバイスを製造するのに必要な回路ＩＰであるメディアＩＤ格納回路ＩＰとして提供する方法がある。前者の場合は、ステップＳ１０３ａで、メディアＩＤ格納モジュール部の注文数欄の数に応じて注文数のメディアＩＤ格納モジュール部（メディアＩＤ格納デバイス）をカードメーカー４００ａに発行（出荷）する。後者の場合には、注文数に係らず、メディアＩＤ格納モジュール部として、メディアＩＤ格納回路ＩＰを発行する。

【０１１７】

次に、カードメーカー４００ａのメディアＩＤ格納モジュール受取手段４２０ａは、センター６００ａから、メディアＩＤ格納モジュール部を受け取る（Ｓ１０４ａ）。

そして、カードメーカー４００ａのメディアＩＤ格納モジュール実装手段４３０ａは、各メモリカード１００ａに、メディアＩＤ格納モジュール部を実装する（Ｓ１０５ａ）。具体的には、ステップＳ１０４ａにおいて、メディアＩＤ格納モジュール部としてメディアＩＤ格納デバイスをセンター６００ａから受け取った場合は、ステップＳ１０５ａにおいて、受け取ったメディアＩＤ格納デバイスを各メモリカードに実装する。また、メディアＩＤ格納モジュール部としてメディアＩＤ格納回路ＩＰをセンター６００ａから受け取った場合は、カードメーカーが、当該メディアＩＤ格納回路ＩＰに基づき製造したメディアＩＤ格納デバイスを各メモリカード１００ａに実装する。

【０１１８】

次に、暗号化カード固有鍵取得手段４５０ａは、各メモリカード１００ａから暗号化カード固有鍵を取得する（Ｓ１０６ａ）。カードデバイス鍵／暗号化メディア鍵群注文書送付手段４４０ａは、センター６００ａに対して、暗号化カード固有鍵及びカードデバイス鍵／暗号化メディア鍵群注文書を送付する（Ｓ１０７ａ）。図４７に、カードデバイス鍵／暗号化メディア鍵群注文書の注文書の一例を示す。図４７に示すカードデバイス鍵／暗号化メディア鍵群注文書８５５は、カードデバイス鍵／暗号化メディア鍵群注文書送付手段４４０ａがセンター６００ａに対してカードデバイス鍵／暗号化メディア鍵群を注文する際に送信するデータである。図４７に示すように、カードデバイス鍵／暗号化メディア鍵群注文書８５５には、カードメーカー自身のカードメーカーＩＤと、カードデバイス鍵の注文数（製造するメモリカードの数）と、暗号化メディア鍵群の要否とが記載される。ここで、カードデバイス鍵の注文数欄は、カードメーカー１４００が必要とするカードデバイス鍵の注文数を記載する。暗号化メディア鍵群の要否欄は、必要なときに“要”とす

る。
【０１１９】
このようにして、カードメーカーは、必要な個数のカードデバイス鍵を注文することができる。なお、暗号化カード固有鍵、カードデバイス鍵、暗号化メディア鍵群の詳細については後述する。
【０１２０】
次に、センター６００ａのカードデバイス鍵／暗号化メディア鍵群注文書受付手段６６０ａは、カードメーカー４００ａから暗号化カード固有鍵及びカードデバイス鍵／暗号化メディア鍵群注文書を受け取る（Ｓ１０８ａ）。
【０１２１】
暗号化カード固有鍵復号手段６２１ａは、後述する共通鍵を用いて暗号化カード固有鍵を復号してカード固有鍵を生成する（Ｓ１０９ａ）。デバイス鍵／暗号化メディア群生成手段６２３ａは、カードデバイス鍵及び当該カードデバイス鍵を識別するカードデバイス鍵ＩＤ／装置デバイス鍵及び当該装置デバイス鍵を識別する装置デバイス鍵ＩＤ／暗号化メディア群を生成する（Ｓ１１０ａ）。デバイス鍵／暗号化メディア群生成手段６２３ａは、カード固有鍵を用いて、カードデバイス鍵を暗号化する（Ｓ１１１ａ）。カードデバイス鍵／暗号化メディア鍵群発行手段６７０ａは、暗号化カードデバイス鍵及びカードデバイス鍵ＩＤ／暗号化メディア鍵群を発行する（Ｓ１１２ａ）。なお、暗号化メディア鍵群の詳細については、後述する。装置デバイス鍵及び装置デバイス鍵ＩＤについては、後述するように、装置メーカーに対して発行される。ここでは、デバイス鍵／暗号化メディア群生成手段６２３ａは、カードデバイス鍵／暗号化メディア鍵群注文書を受け取った後に、カードデバイス鍵や暗号化メディア鍵群を生成する構成としたが、この構成に限定されない。例えば、センターのデバイス鍵／暗号化メディア群生成手段６２３ａは、カードデバイス鍵、後述する装置デバイス鍵、及び、暗号化メディア鍵群を予め生成して保持しておき、カードメーカーや装置メーカーからの注文に応じて、保持しているものを発行してもよい。
【０１２２】
カードメーカー４００ａのカードデバイス鍵／暗号化メディア鍵群受取手段４６０ａは暗号化カードデバイス鍵及びカードデバイス鍵ＩＤ／暗号化メディア鍵群を受け取る（Ｓ１１３ａ）。カードデバイス鍵／暗号化メディア鍵群実装手段４７０ａは、受け取った暗号化カードデバイス鍵及びカードデバイス鍵ＩＤ／暗号化メディア鍵群をメモリカード１００ａに実装する（Ｓ１１４ａ）。
２．４　メディアＩＤ格納モジュール部６１０ａの構成
図１８に、メディアＩＤ格納モジュール部６１０ａの構成を示す。
【０１２３】
メディアＩＤ格納モジュール部６１０ａは、耐タンパーモジュールであり、図１８に示すように、固有鍵生成部６１１ａ、カードデバイス鍵格納部６１２ａ、復号部６１３ａ、暗号化部６１４ａ、メディア鍵生成部６１５ａ、共通鍵格納部６１６ａ、メディア固有鍵生成部６１７ａ、メディアＩＤ格納部６１８ａ及び認証部６１９ａから構成される。固有鍵生成部６１１ａ、カードデバイス鍵格納部６１２ａ、復号部６１３ａ、メディア鍵生成部６１５ａ、メディア固有鍵生成部６１７ａ及び認証部６１９ａは、証明部６０９ａを構成する。証明部６０９ａは、後述するように、メディアＩＤ格納モジュール部６１０ａの正当性を示す証明情報を生成する。
【０１２４】
ここで、センター６００ａからカードメーカー４００ａに発行されるメディアＩＤ格納モジュール部６１０ａの実現手段、及び、発行形態としては、実施の形態１と同じであるので、ここでの説明は省略する。
【０１２５】
次に、メディアＩＤ格納モジュール部６１０ａの固有鍵生成部６１１ａは、メディアＩＤ格納モジュール部６１０ａが各メモリカード１００ａに実装されたときに、それぞれ、

メディアＩＤ格納モジュール部毎に異なるカード固有鍵として、１２８ビットの異なる数値を生成するよう構成される。一般に、ＬＳＩ等の半導体デバイスにおいて、半導体デバイス毎に異なる固有のデータを生成する手段としては、電気ヒューズ等により固有データを半導体デバイス毎に設定する手段や、ＰＵＦ（Ｐｈｙｓｉｃａｌ　Ｕｎｃｌｏａｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ）等を半導体デバイスに実装し、半導体デバイス毎に、ＰＵＦの実装のばらつきを利用して、異なるデータを生成する手段があり、固有鍵生成部６１１ａは、これらの手段を用いて実現する。

【０１２６】

カードデバイス鍵格納部６１２ａは、復号部６１３ａから受け取った、カード毎に異なる固有の１２８ビットのカードデバイス鍵を格納する。

復号部６１３ａは、ＡＥＳ復号関数を用いて、以下の式により暗号化カードデバイス鍵を復号する。

【０１２７】

カードデバイス鍵＝ＡＥＳ－Ｄ（カード固有鍵、暗号化カードデバイス鍵）

なお、ＡＥＳ暗号については広く知られているので説明は省略する。また、暗号化カードデバイス鍵は、センターから以下の式で与えられる。

【０１２８】

暗号化カードデバイス鍵＝ＡＥＳ－Ｅ（カード固有鍵、カードデバイス鍵）

ここで、カード固有鍵は、固有鍵生成部６１１ａにて生成された、メディアＩＤ格納モジュール部毎に異なる固有鍵である。

【０１２９】

暗号化部６１４ａは、ＡＥＳ暗号化関数を用いて、以下の式により、カード固有鍵を暗号化し、暗号化カード固有鍵を外部に出力する。

暗号化カード固有鍵＝ＡＥＳ－Ｅ（共通鍵、カード固有鍵）

メディア鍵生成部６１５ａは、暗号化メディア鍵群から、カードデバイス鍵を識別するカードデバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択する。次に、ＡＥＳ復号関数を用いて、以下の式により、暗号化メディア鍵群から選択した１個の暗号化メディア鍵を、カードデバイス鍵を用いて復号することによりメディア鍵を生成する。

【０１３０】

メディア鍵＝ＡＥＳ－Ｄ（カードデバイス鍵、暗号化メディア鍵）

ここで、暗号化メディア鍵群は、センターにより発行される。暗号化メディア鍵群の一例を図１９に示す。図１９に示す通り、暗号化メディア鍵群８６０は、複数の組を含み、各組は、ＩＤと暗号化メディア鍵とから構成される。ＩＤは、カードデバイス鍵ＩＤ又は装置デバイス鍵ＩＤである。カードデバイス鍵ＩＤは、カードデバイス鍵を一意に識別する識別情報であり、装置デバイス鍵ＩＤは、装置デバイス鍵を一意に識別する識別情報である。各暗号化メディア鍵は、ＡＥＳ暗号関数を用いて、当該暗号化メディア鍵に対応するカードデバイス鍵ＩＤにより識別される１２８ビットのカードデバイス鍵を用いて、又は当該暗号化メディア鍵に対応する装置デバイス鍵ＩＤにより識別される１２８ビットの装置デバイス鍵を用いて、１２８ビットのメディア鍵を暗号化して生成したものである。

【０１３１】

共通鍵格納部６１６ａは、予めセンター６００ａとの間で共有されている１２８ビットの共通鍵を格納する。

メディア固有鍵生成部６１７ａは、一方向性関数Ｇを用いて、メディア鍵とメディアＩＤ（言い換えると、メディア識別情報）から以下の式によりメディア固有鍵を生成する。

【０１３２】

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ暗号を利用して実現することができる。

【０１３３】

メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。
メディアＩＤ格納部６１８ａは、メディアＩＤ格納モジュール部が各メモリカード１００ａに実装されたときに、それぞれ、メディアＩＤ格納モジュール部毎に異なる固有のメディアＩＤとして、１２８ビットの異なる数値を生成するよう構成される。具体的な実現手段については、固有鍵生成部６１１ａの実現手段と同じである。
【０１３４】
認証部６１９ａは、記録再生装置２００ａの認証部との間で相互認証を行う。相互認証の詳細については後述する。
２．５　センター６００ａと装置メーカー５００ａとの間の動作
センター６００ａと装置メーカー５００ａとの間の動作について、図２０に示すフローチャートを用いて説明する。
【０１３５】
図２０に示すように、装置メーカー５００ａの装置デバイス鍵注文書送付手段５１０ａは、センター６００ａに対して、装置デバイス鍵注文書を送付する（Ｓ２０１ａ）。
図２１に、装置デバイス鍵注文書の一例を示す。図２１に示すように、装置デバイス鍵注文書８７０には、装置メーカーＩＤと、装置デバイス鍵の注文数（製造する記録再生装置の数）、暗号化メディア鍵群の要否が記載される。ここで、装置メーカーＩＤは、装置メーカー毎に異なる固有の値であり、センター６００ａによりライセンス契約時に付与される。装置デバイス鍵の注文数欄は、装置メーカー５００ａが、装置デバイス鍵を実装して製造する記録再生装置の数を記載する。暗号化メディア鍵群の要否欄は、必要なときに“要”とする。
【０１３６】
このようにして、装置メーカー５００ａは、装置デバイス鍵を注文することができる。
次に、センター６００ａの装置デバイス鍵注文書受付手段６８０ａは、装置メーカー５００ａから装置デバイス鍵注文書を受け付ける（Ｓ２０２ａ）。装置デバイス鍵発行手段６９０ａは、装置デバイス鍵注文書の装置デバイス鍵の注文数に応じて、ステップＳ１１０ａで生成した装置デバイス鍵及び当該装置デバイス鍵を識別する装置デバイス鍵ＩＤを装置メーカーに発行し、また、注文書の暗号化メディア鍵群の要否欄が“要”の場合は、暗号化メディア鍵群を、装置メーカーに発行する（Ｓ２０３ａ）。
【０１３７】

なお、注文書の暗号化メディア鍵群の要否欄が“不要”の場合も、センターが暗号化メディア鍵群を更新した場合には、装置メーカーに発行される場合がある。
【０１３８】
次に、装置メーカー５００ａの装置デバイス鍵受取手段５２０ａは、センター６００ａから、装置デバイス鍵及び装置デバイス鍵ＩＤと暗号化メディア鍵群を受け取る（Ｓ２０４ａ）。そして、装置メーカー５００ａの装置デバイス鍵実装手段５３０ａは、記録再生装置２００ａを製造する際、各記録再生装置２００ａに、それぞれ、装置デバイス鍵及び装置デバイス鍵ＩＤと、必要に応じて暗号化メディア鍵群を実装する（Ｓ２０５ａ）。
２．５　記録再生システム３００ａの構成
図２２に、記録再生システム３００ａを構成するメモリカード１００ａ及び記録再生装置２００ａの詳細の構成を示す。
（１）メモリカード１００ａの詳細の構成
メモリカード１００ａは、図２２に示すように、制御部１１０ａ、メモリ部１２０ａ及びメディアＩＤ格納モジュール部６１０ａから構成される。
【０１３９】
制御部１１０ａは、メディアＩＤ格納モジュール部６１０ａ及びメモリ部１２０ａに対する所定の制御処理を行うとともに、記録再生装置２００ａからの要求に応じて、所定の制御処理を行う。具体的には、制御部１１０ａは、記録再生装置２００ａからの要求に応じて、メディアＩＤ格納モジュール部６１０ａに対して、メディアＩＤを要求し、メディ

アＩＤを取得し、記録再生装置２００ａに送る。また、制御部１１０ａは、記録再生装置２００ａからの要求に応じて、メモリ部１２０ａから、暗号化メディア鍵群を取得し、記録再生装置２００ａに送る。また、制御部１１０ａは、記録再生装置から受け取った暗号化コンテンツをメモリ部１２０ａに格納する。

【０１４０】

メモリ部１２０ａは、さらに、暗号化カードデバイス鍵格納部１２１ａ、暗号化メディア鍵群格納部１２２ａ及び暗号化コンテンツ格納部１２３ａから構成される。メモリ部１２０ａの暗号化カードデバイス鍵格納部１２１ａは、記録再生装置２００ａからの読み書きができない領域であり、メモリカード製造時に、カードメーカー４００ａが、センター６００ａから受け取った暗号化カードデバイス鍵及び当該カードデバイス鍵を識別するカードデバイス鍵ＩＤを格納する。なお、ここでは、暗号化カードデバイス鍵格納部１２１ａは、記録再生装置２００ａから読み書きできない領域であるとしたが、この構成に限定されない。例えば、暗号化カードデバイス鍵格納部は、記録再生装置２００ａから書き込みできない領域であるとしてもよい。

【０１４１】

メモリ部１２０ａの暗号化メディア鍵群格納部１２２ａは、記録再生装置２００ａからの読み出しのみが可能な領域であり、メモリカード製造時に、カードメーカー４００ａがセンター６００ａから受け取った暗号化メディア鍵群を格納する。なお、ここでは、暗号化メディア鍵群が更新されない場合を想定し、暗号化メディア鍵群格納部１２２ａは、記録再生装置２００ａからの読み出しのみが可能な領域としたがこの構成に限定されない。例えば、暗号化メディア鍵群が更新される場合を想定し、暗号化メディア鍵群格納部１２２ａは、記録再生装置２００ａからデータの読み書きが可能な領域であるとしてもよい。

【０１４２】

メモリ部１２０ａの暗号化コンテンツ格納部１２３ａは、記録再生装置２００ａからデータの読み書きができる領域であり、記録再生装置２００ａによって暗号化されたコンテンツが格納される。

【０１４３】

また、メディアＩＤ格納モジュール部６１０ａには、カードメーカー４００ａがセンター６００ａからＬＳＩ等の半導体デバイスの形態でメディアＩＤ格納モジュール部を受け取った場合は、受け取ったメディアＩＤ格納モジュール部が、そのまま実装される。またカードメーカー４００ａがセンター６００ａからメディアＩＤ格納モジュール部として、回路ＩＰを受け取った場合は、カードメーカー４００ａが回路ＩＰに基づき製造したＬＳＩ等の半導体デバイスが、実装される。メディアＩＤ格納モジュール部６１０ａの内部構成については既に説明済であるので省略する。

【０１４４】

ここで、制御部１１０ａは、例えば、ＬＳＩ等の半導体デバイスで構成され、メモリ部１２０ａは、例えば、フラッシュメモリで構成され、メディアＩＤ格納モジュール部６１０ａは、ＬＳＩ等の半導体デバイスで構成される。

（２）記録再生装置２００ａの詳細の構成

記録再生装置２００ａは、図２２に示すように、メモリカード検証部２１１ａ、メディアＩＤ取得部２０５ａ、コンテンツ鍵生成部２０６ａ、コンテンツ受信部２０７ａ、コンテンツ暗復号部２０８ａ及びコンテンツ再生部２０９ａから構成される。メモリカード検証部２１１ａは、装置デバイス鍵格納部２０１ａ、メディア鍵生成部２０２ａ、メディア固有鍵生成部２０３ａ及び認証部２０４ａから構成される。

【０１４５】

メモリカード検証部２１１ａは、メモリカード１００ａから受け取った暗号化メディア鍵群を用いて生成したメディア固有鍵を用いて、メモリカード１００ａとの間で相互認証処理を行う。この相互認証処理により、そのメモリカード１００ａが、正しいメモリカードか、不正なメモリカードかを判別することができる。

【０１４６】

以下、メモリカード検証部２１１ａを構成する装置デバイス鍵格納部２０１ａ、メディア鍵生成部２０２ａ、メディア固有鍵生成部２０３ａ及び認証部２０４ａについて説明する。

【０１４７】

装置デバイス鍵格納部２０１ａは、記録再生装置毎に異なる固有の１２８ビットの装置デバイス鍵及び当該装置デバイス鍵を識別する装置デバイス鍵ＩＤを格納している。

メディア鍵生成部２０２ａは、メモリカード１００ａのメディア鍵生成部６１５ａと同様の構成である。メディア鍵生成部２０２ａは、メモリカード１００ａの暗号化メディア鍵群格納部１２２ａから暗号化メディア鍵群を読み出すことにより取得し、取得した暗号化メディア鍵群から、装置デバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択する次に、メディア鍵生成部２０２ａは、ＡＥＳ復号関数を用いて、以下の式により、選択した暗号化メディア鍵を、装置デバイス鍵を鍵として用いて復号する。そして、これによりメディア鍵を生成し、生成したメディア鍵をメディア固有鍵生成部２０３ａへ出力する。

【０１４８】

メディア鍵＝ＡＥＳ－Ｄ（装置デバイス鍵、暗号化メディア鍵）

暗号化メディア鍵群の一例を図１９に示す。図１９に示す通り、暗号化メディア鍵群８６０に含まれる各暗号化メディア鍵は、ＡＥＳ暗号関数を用いて、１２８ビットのカードデバイス鍵を用いて、又は、装置デバイス鍵を用いて、１２８ビットのメディア鍵を暗号化したものである。

【０１４９】

メディア固有鍵生成部２０３ａは、メモリカード１００ａのメディア固有鍵生成部６１７ａと同様の構成である。メディア固有鍵生成部２０３ａは、メモリカード１００ａのメディアＩＤ格納部６１８ａから、制御部１１０ａを介して、メディアＩＤを取得し、メディア鍵生成部２０２ａからメディア鍵を取得し、一方向性関数Ｇを用いて、取得したメディア鍵と取得したメディアＩＤから以下の式によりメディア固有鍵を生成し、取得したメディアＩＤ及び生成したメディア固有鍵を認証部２０４ａへ出力する。

【０１５０】

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

なお、一方向性関数Ｇの具体例としては、次式に示すように、例えばＡＥＳ暗号を利用して実現することができる。

【０１５１】

メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。

認証部２０４ａは、メディア固有鍵生成部２０３ａからメディアＩＤ及びメディア固有鍵を受け取る。次に、認証部２０４ａは、受け取ったメディア固有鍵を用いて、メモリカード１００ａの認証部６１９ａとの間で相互認証処理を行う。相互認証処理の詳細については、後述する。認証部２０４ａは、メモリカード１００ａの認証部６１９ａとの間の相互認証に成功した場合に限り、メディア固有鍵生成部２０３ａから受け取ったメディアＩＤをメディアＩＤ取得部２０５ａへ出力する。

【０１５２】

メディアＩＤ取得部２０６は、認証部２０４ａにおいて相互認証に成功したときのみ、認証部２０４ａからメディアＩＤを取得し、取得したメディアＩＤをコンテンツ鍵生成部２０６ａに送る。

【０１５３】

コンテンツ鍵生成部２０６ａは、メディアＩＤ取得部２０５ａから受け取ったメディアＩＤに基づいてコンテンツ鍵を生成する。具体的なコンテンツ鍵の生成方法については、後述する。生成したコンテンツ鍵をコンテンツ暗復号部２０８ａへ出力する。

【０１５４】

コンテンツ受信部２０７ａは、デジタル放送されたデジタルコンテンツや、デジタル配信されたデジタルコンテンツを受信し、受信したデジタルコンテンツをコンテンツ暗復号

部２０８ａに送る。
【０１５５】
コンテンツ暗復号部２０８ａは、コンテンツ鍵生成部２０６ａからコンテンツ鍵を受け取る。次に、受け取ったコンテンツ鍵を用いてコンテンツ受信部２０７ａから受け取ったデジタルコンテンツを暗号化して暗号化デジタルコンテンツをメモリカード１００ａに送る。又は、メモリカード１００ａから暗号化デジタルコンテンツを受け取り、受け取ったコンテンツ鍵を用いて、受け取った暗号化デジタルコンテンツを復号して、デジタルコンテンツを生成し、生成したデジタルコンテンツをコンテンツ再生部２０９ａに送る。コンテンツの暗復号の詳細については、後述する。
【０１５６】
コンテンツ再生部２０９ａは、コンテンツ暗復号部２０８ａより受け取った復号されたデジタルコンテンツを再生する。
２．６　記録再生システム３００ａの動作
（１）記録再生システム３００ａの記録時の動作
記録再生装置２００ａがメモリカード１００ａにコンテンツを記録する際の動作について、図２３に示すフローチャートを用いて説明する。
【０１５７】
図２３に示すように、まず、記録再生装置２００ａのメディア固有鍵生成部２０３ａはメモリカード１００ａにメディアＩＤを要求する（Ｓ３０１ａ）。メモリカード１００ａの制御部１１０ａは、記録再生装置２００ａからのメディアＩＤの要求に対応して、メディアＩＤ格納部６１８ａからメディアＩＤを取得し、記録再生装置２００ａへ送る（Ｓ３０２ａ）。記録再生装置２００ａのメディア鍵生成部２０２ａは、メモリカード１００ａに暗号化メディア鍵群を要求する（Ｓ３０３ａ）。メモリカード１００ａの制御部１１０ａは、記録再生装置２００ａからの暗号化メディア鍵群の要求に対応して、メモリ部１２０ａの暗号化メディア鍵群格納部１２２ａから暗号化メディア鍵群を取得し記録再生装置２００ａに送る（Ｓ３０４ａ）。
【０１５８】
次に、記録再生装置２００ａのメディア鍵生成部２０２ａは、メモリカード１００ａから受け取った暗号化メディア鍵群から、装置デバイス鍵格納部２１０ａから取得した装置デバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択する。次に、暗号化メディア鍵群から選択した１個の暗号化メディア鍵と、装置デバイス鍵格納部２０１ａから取得した装置デバイス鍵を用いてＡＥＳ復号関数を用いて、以下の式によりメディア鍵を生成し、
メディア鍵＝ＡＥＳ－Ｄ（装置デバイス鍵、暗号化メディア鍵）
生成したメディア鍵をメディア固有鍵生成部２０３ａに送る（Ｓ３０５ａ）。
【０１５９】

記録再生装置２００ａのメディア固有鍵生成部２０３ａは、ステップＳ３０１ａで取得したメディアＩＤとメディア鍵生成部２０２ａから受け取ったメディア鍵と一方向性関数Ｇを用いて、以下の式よりメディア固有鍵を生成する。
【０１６０】
メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）
なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ暗号を利用して実現することができる。
【０１６１】
メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ
ここで、（＋）は、排他的論理和演算を表す。（Ｓ３０６ａ）
メモリカード１００ａのメディア鍵生成部６１５ａも、記録再生装置２００ａのメディア鍵生成部２０２ａと同様に、メモリ部１２０ａの暗号化メディア鍵群格納部１２２ａの暗号化メディア鍵群から、暗号化カードデバイス鍵格納部１２１ａから取得したカードデバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択する。次に、暗号化メディア鍵群

から選択した１個の暗号化メディア鍵と、カードデバイス鍵格納部６１２ａから取得したカードデバイス鍵を用いてＡＥＳ復号関数を用いて、以下の式によりメディア鍵を生成し

メディア鍵＝ＡＥＳ－Ｄ（カードデバイス鍵、暗号化メディア鍵）

生成したメディア鍵をメディア固有鍵生成部６１７ａに送る（Ｓ３０７ａ）。

【０１６２】

メモリカード１００ａのメディア固有鍵生成部６１７ａは、記録再生装置２００ａのメディア固有鍵生成部２０３ａと同様に、メディアＩＤ格納部６１８ａから取得したメディアＩＤとメディア鍵生成部６１５ａから受け取ったメディア鍵と一方向性関数Ｇを用いて以下の式よりメディア固有鍵を生成する。

【０１６３】

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ暗号を利用して実現することができる。

【０１６４】

メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。（Ｓ３０８ａ）

メモリカード１００ａの認証部６１９ａと記録再生装置２００ａの認証部２０４ａは、相互認証を行う（Ｓ３０９ａ）。相互認証の詳細については後述する。

【０１６５】

ステップＳ３０９ａの相互認証が失敗した場合、処理を終了する。これにより、暗号化コンテンツの復号を禁止し、又はコンテンツの暗号化を禁止している。

ステップＳ３０９ａの相互認証が成功した場合、メディアＩＤ取得部２０５ａは、認証部２０４ａからメディアＩＤを取得する（Ｓ３１０ａ）。

【０１６６】

コンテンツ鍵生成部２０６ａは、メディアＩＤ取得部２０５ａから取得したメディアＩＤに対して、次式により、一方向性関数Ｆを用いて、コンテンツ鍵を生成し、生成したコンテンツ鍵をコンテンツ暗復号部２０８ａに送る（Ｓ３１１ａ）。

【０１６７】

コンテンツ鍵＝Ｆ（メディアＩＤ）

一方向性関数Ｆの具体例としは、例えば、ＡＥＳ暗号を用いて以下の式で実現できる。

コンテンツ鍵＝

ＡＥＳ（コンテンツ鍵生成用秘密鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。また、コンテンツ鍵生成用秘密鍵は、１２８ビットであり、全ての記録再生装置に共通で秘密であり、予め、コンテンツ鍵生成部２０７が保持しているものとする。ＡＥＳ暗号については、広く知られているので説明は省略する。

【０１６８】

なお、ここでは、コンテンツ鍵生成関数としてＡＥＳ暗号を用いる例を示したが、１２８ビットのメディアＩＤに基づき、１２８ビットのランダムな乱数を、コンテンツ鍵として生成する一方向性関数であればどんな構成でもよい。

【０１６９】

コンテンツ暗復号部２０８ａは、コンテンツ受信部２０７ａにて受信されたデジタル放送されたデジタルコンテンツ、又はデジタル配信されたデジタルコンテンツを、コンテンツ鍵生成部２０６ａから受け取ったコンテンツ鍵を用いて、暗号化する（Ｓ３１２ａ）。コンテンツ暗復号部２０８ａは、メモリカード１００ａに暗号化されたデジタルコンテンツをメモリカードに送付する（Ｓ３１３ａ）。

【０１７０】

ここで、コンテンツの暗号化は、例えば、以下の式を用いて行う

暗号化されたデジタルコンテンツ＝ＡＥＳ－ＥＣＢＣ（コンテンツ鍵、デジタルコンテンツ）

ここで、ＡＥＳ－ＥＣＢＣとは、ＡＥＳ暗号をＣＢＣモード（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）で利用して暗号化することを示す。ＣＢＣモードについては、広く知られているので説明を省略する。なお、ここでは、ＡＥＳ－ＣＢＣを用いる場合を示したが、この構成には限定されない。

【０１７１】

次に、メモリカード１００ａの制御部１１０ａは、記録再生装置２００ａから暗号化されたデジタルコンテンツを受け取り、受け取った暗号化されたデジタルコンテンツを暗号化コンテンツ格納部１２３ａに格納する（Ｓ３１４ａ）。

（２）相互認証処理の一例

次に、相互認証処理の一例を、図２４に示すプロセスチャートを用いて説明する。ここで説明する相互認証処理は、チャレンジ・レスポンス型の認証（challenge and response authentication）である。

【０１７２】

メモリカード１００ａの認証部６１９ａは、チャレンジデータとしての乱数Ｒ１を生成する（Ｓ５０１）。メモリカード１００ａの認証部６１９ａは、生成した乱数Ｒ１をチャレンジデータとして記録再生装置２００ａに送る。記録再生装置２００ａの認証部２０４ａは、チャレンジデータとしての乱数Ｒ１を受け取る（Ｓ５０２）。

【０１７３】

記録再生装置２００ａの認証部２０４ａは、受け取ったチャレンジデータとしての乱数Ｒ１を、メディア固有鍵生成部２０３ａから受け取ったメディア固有鍵を用いて暗号化して、レスポンスデータとして暗号化乱数Ｅ１＝ＡＥＳ－Ｅ（メディア固有鍵、乱数Ｒ１）を生成する（Ｓ５０３）。ここで、暗号化乱数Ｅ１は、記録再生装置２００ａが自己の正当性を証明するための証明情報である。レスポンスデータとしての暗号化乱数Ｅ１をメモリカード１００ａに送り、メモリカード１００ａの認証部６１９ａは、レスポンスデータとしての暗号化乱数Ｅ１を受け取る（Ｓ５０４）。

【０１７４】

メモリカード１００ａの認証部６１９ａは、受け取ったレスポンスデータとしての暗号化乱数Ｅ１を、メディア固有鍵生成部６１７ａから取得したメディア固有鍵を用いて、復号して乱数Ｄ１＝ＡＥＳ－Ｄ（メディア固有鍵、暗号化乱数Ｅ１）を生成する（Ｓ５０５）。メモリカード１００ａの認証部６１９ａは、生成した乱数Ｄ１とＳ５０１で生成した乱数Ｒ１を比較し（Ｓ５０６）、一致すれば、次のＳ５１１に進み、一致しなければ、相互認証処理を終了する。

【０１７５】

記録再生装置２００ａの認証部２０４ａは、チャレンジデータとして乱数Ｒ２を生成する（Ｓ５１１）。記録再生装置２００ａの認証部２０４ａは、生成したチャレンジデータとしての乱数Ｒ２をメモリカード１００ａに送る。メモリカード１００ａの認証部６１９ａは、チャレンジデータとしての乱数Ｒ２を受け取る（Ｓ５１２）。

【０１７６】

メモリカード１００ａの認証部６１９ａは、受け取ったチャレンジデータとしての乱数Ｒ２を、メディア固有鍵生成部６１７ａから受け取ったメディア固有鍵を用いて暗号化してレスポンスデータとしての暗号化乱数Ｅ２＝ＡＥＳ－Ｅ（メディア固有鍵、乱数Ｒ２）を生成する（Ｓ５１３）。ここで、暗号化乱数Ｅ２は、メモリカード１００ａが自己の正当性を証明するための証明情報である。レスポンスデータとしての暗号化乱数Ｅ２を記録再生装置２００ａに送り、記録再生装置２００ａの認証部２０４ａは、レスポンスデータとしての暗号化乱数Ｅ２を受け取る（Ｓ５１４）。

【０１７７】

記録再生装置２００ａの認証部２０４ａは、受け取った暗号化乱数Ｅ２を、メディア固有鍵生成部２０３ａから取得したメディア固有鍵を用いて、復号して、乱数Ｄ２＝ＡＥＳ－Ｄ（メディア固有鍵、暗号化乱数Ｅ２）を生成する（Ｓ５１５）。記録再生装置２００ａの認証部２０４ａは、生成した乱数Ｄ２とＳ５１１で生成した乱数Ｒ２を比較し（Ｓ５

１６）、一致すれば、メディアＩＤ取得部２０５ａにメディアＩＤを送る。一致しなければ、相互認証処理を終了する。

【０１７８】

図２４に示すプロセスチャートにおいて、ステップＳ５０１、Ｓ５０２、Ｓ５０５、Ｓ５０６は、認証部６１９ａ内において、検証部６１９ｖを構成している。また、ステップＳ５０３、Ｓ５０４は、認証部２０４ａ内において、証明生成部２０４ｐを構成している

さらに、図２４に示すプロセスチャートにおいて、ステップＳ５１１、Ｓ５１２、Ｓ５１５、Ｓ５１６は、認証部２０４ａ内において、検証部２０４ｖを構成している。また、ステップＳ５１３、Ｓ５１４は、認証部６１９ａ内において、証明生成部６１９ｐを構成している。

【０１７９】

上記のＡＥＳ－Ｅは、ＡＥＳ暗号化関数であり、上記のＡＥＳ－Ｄは、ＡＥＳ復号関数である。なお、上記において、ＡＥＳを用いているが、これには限定されない。他の共通鍵暗号方式を用いるとしてもよい。また、上記において、チャレンジ・レスポンス型の認証プロトコルを用いているがこれには限定されない。他の認証プロトコルを用いてもよい

（３）記録再生システム３００ａの再生時の動作

記録再生装置２００ａがメモリカード１００ａから暗号化コンテンツを読み出し再生する際の動作について、図２５に示すフローチャートを用いて説明する。

【０１８０】

なお、図２５に示すＳ４０１ａからＳ４１１ａは、それぞれ、図２３に示すＳ３０１ａからＳ３１１ａと全く同じ動作であるので、説明を省略する。

記録再生装置２００ａのコンテンツ暗復号部２０８ａは、メモリカード１００ａに暗号化コンテンツの送付を要求する（Ｓ４１２ａ）。メモリカード１００ａの制御部１１０ａは、記録再生装置２００ａからの暗号化コンテンツの送付要求に対応し、暗号化コンテンツ格納部１２３ａから暗号化コンテンツを読み出し、記録再生装置２００ａへ送付する（Ｓ４１３ａ）。コンテンツ暗復号部２０８ａは、メモリカード１００ａから、受け取った暗号化コンテンツを、コンテンツ鍵生成部２０６ａから受け取ったコンテンツ鍵を用いて復号し、復号したコンテンツをコンテンツ再生部２０９ａへ送る（Ｓ４１４ａ）

ここで、コンテンツの復号は、以下の式で表される。

【０１８１】

復号されたデジタルコンテンツ＝ＡＥＳ－ＤＣＢＣ（コンテンツ鍵、暗号化されたデジタルコンテンツ）

ここで、ＡＥＳ－ＤＣＢＣとは、ＡＥＳ暗号をＣＢＣモード（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）で利用して復号することを示す。

【０１８２】

コンテンツ再生部２０９ａは、コンテンツ暗復号部２０８ａから受け取った、復号されたコンテンツを再生する（Ｓ４１５ａ）。

２．７　不正の判別

以上の説明したように、実施の形態２の構成によれば、カードメーカーが、不正なメモリカードを製造したとしても、記録再生装置２００ａのメモリカード検証部２１１ａにより、正しく製造されたメモリカードか、不正なメモリカードかの判別が可能となる。このことを、図２６を用いて説明する。

【０１８３】

図２６において、メモリカード１００ａは、実施の形態２に係るメモリカード（以下、正規のメモリカードと称する）であり、記録再生装置２００ａは、実施の形態２に係る記録再生装置（以下、正規の記録再生装置と称する）である。また、メモリカード１０Ｄは不正なカードメーカーが、実施の形態２に係るメモリカード１００ａと記録再生装置２００ａを動作させることにより、メディアＩＤを取得し、従来の構成のメモリカード１０Ｄのメディア ＩＤ格納部１３Ｃに格納して製造したメモリカード（以下、不正なメモリカードと称する）である。

【０１８４】
このとき、不正なメモリカード１０Ｄを用いて、正規の記録再生装置２００ａにより記録再生処理を試みたとしても、不正なメモリカード１０Ｄは、メディア固有鍵を生成できないため、正規の記録再生装置２００ａのメモリカード検証部２１１ａの認証部２０４ａにおける相互認証処理に失敗する。すなわち、カードメーカーが、不正なメモリカードを製造したとしても、正規の記録再生装置２００ａにより、正規のメモリカードか不正なメモリカードかの判別が可能となる。
２．８　変形例
（１）実施の形態１では、メーカー公開鍵証明書におけるセンター発行署名の生成、及びメディアＩＤ署名データにおけるメモリカード発行署名の生成において、回復型署名であるＲＳＡを用いる場合を説明したが、この構成には限定されない。
【０１８５】
例えば、回復型署名（署名データに対する署名検証の結果、被署名データが回復する方式）に代えて添付型署名（署名データと、署名データに添付される被署名データを用いて署名検証を行う方式）を用いてもよい。具体的には、例えば、ＲＳＡに代えて、楕円曲線暗号を用いてもよい。
【０１８６】
また、例えば、ＲＳＡや楕円曲線暗号のような公開鍵暗号系の署名アルゴリズムを用いるのに代えて、共通鍵暗号系の例えばＡＥＳ暗号を用いたＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）アルゴリズムを用いてもよい。この場合、メモリカード１００のメディアＩＤ格納モジュール部６１０に、メーカー秘密鍵格納部６１２に代えて、ＭＡＣ生成用秘密鍵格納部を持たせ、署名生成部６１３に代えてＭＡＣ生成部を持たせ、記録再生装置２００に、センター公開鍵格納部２０２やメーカー公開鍵格納部２０５に代えて、ＭＡＣ生成用秘密鍵格納部を持たせ、署名検証部２０４に代えてＭＡＣ検証部を持たせてもよい。ＭＡＣアルゴリズムについては公知であるので説明を省略する。なお、この場合は、記録再生装置２００のＭＡＣ生成用秘密鍵格納部及びＭＡＣ検証部は耐タンパーモジュールとしてセンターから発行してもよい。
（２）実施の形態１では、メモリカード１００のメディアＩＤ格納モジュール部６１０にメーカー秘密鍵格納部６１２を持たせ、メーカー秘密鍵を用いて、メディアＩＤ署名を生成する構成としたが、この構成には限定されない。
【０１８７】
例えば、図２７に示すように、メモリカード１００ｃのメディアＩＤ格納モジュール部６１０ｃにメーカー秘密鍵格納部６１２に代えてセンター秘密鍵格納部６１２ｃを持たせセンター秘密鍵を用いて、メディアＩＤ署名を生成してもよい。この場合、図２７に示すように、記録再生装置２００ｃは、メディアＩＤ署名を、センター公開鍵を用いて検証する。
【０１８８】
具体的には、図２７に示すように、センター６００をセンター６００ｃに代え、メモリカード１００をメモリカード１００ｃに代え、記録再生装置２００を記録再生装置２００ｃに代える。
【０１８９】
センター６００ｃは、センター６００と同様の構成を有しているが、メーカー公開鍵証明書発行手段６６０を備えていない。
また、メモリカード１００ｃは、メモリカード１００と同様の構成を有しているが、メディアＩＤ格納モジュール部６１０及びメモリ部１２０に代えて、メディアＩＤ格納モジュール部６１０ｃ及びメモリ部１２０ｃを備えている。メディアＩＤ格納モジュール部６１０ｃは、耐タンパーモジュールであり、メーカー秘密鍵格納部６１２及び署名生成部６１３に代えて、センター秘密鍵格納部６１２ｃ及び署名生成部６１３ｃを備えている。センター秘密鍵格納部６１２ｃ及び署名生成部６１３ｃは、証明部６０９ｃを構成しているメモリ部１２０ｃは、メーカー公開鍵証明書格納部１２１を備えておらず、暗号化コンテ

ンツ格納部１２２を備えている。
【０１９０】
記録再生装置２００ｃは、記録再生装置２００と同様の構成を有しているが、メモリカード検証部２１１に代えて、メモリカード検証部２１１ｃを備えている。メモリカード検証部２１１ｃは、センター公開鍵格納部２０２ｃ、乱数生成部２０３及び署名検証部２０４ｃを備えている。
【０１９１】
センター秘密鍵格納部６１２ｃは、センター秘密鍵を格納している。
署名生成部６１３ｃは、ＲＳＡ署名生成関数を用いて、メディアＩＤ署名データを生成する。メディアＩＤ署名データは、乱数、メディアＩＤ、メモリカード発行署名からなるここで、メディアＩＤは、メディアＩＤ格納部６１１に格納されたメディアＩＤである。乱数は、記録再生装置２００の乱数生成部２０３から受け取る乱数である。メモリカード発行署名は、ＲＳＡ－ＳＩＧＮ（センター秘密鍵、乱数‖メディアＩＤ）により生成される。署名生成部６１３ｃは、生成したメディアＩＤ署名データを、制御部１１０ｃを介して、記録再生装置２００ｃへ出力する。
【０１９２】
センター公開鍵格納部２０２ｃは、センター公開鍵を格納している。
署名検証部２０４ｃは、センター公開鍵格納部２０２ｃから取得したセンター公開鍵を用いて、メモリカード１００ｃから受け取ったメディアＩＤ署名データを検証する。この場合における署名の検証は、回復型検証である。検証が成功した場合、検証の対象であるメディアＩＤ署名データからメディアＩＤ（識別情報）が抽出され、抽出されたメディアＩＤをメディアＩＤ取得部２０６に送る。
【０１９３】
（３）実施の形態２では、図２２に示すように、メディアＩＤ格納モジュール部６１０ａに、固有鍵生成部６１１ａ、暗号化部６１４ａ、共通鍵格納部６１６ａを設け、図１５に示すように、カードメーカー４００ａにおいて、メディアＩＤ格納モジュール部をメモリカード１００ａに実装した後、カードメーカー４００ａは、メモリカード１００ａから暗号化カード固有鍵を取得し、暗号化カード固有鍵をセンター６００ａに送付し、センター６００ａにて暗号化カード固有鍵を復号し、カード固有鍵を用いてカードデバイス鍵を暗号化してカードメーカー４００ａに送り、カードメーカー４００ａがメモリカード１００ａに暗号化カードデバイス鍵を実装する構成としているが、センター６００ａからカードメーカー４００ａにメディアＩＤ格納モジュール部を半導体デバイスとして発行する場合は、この構成には限定されない。
【０１９４】
例えば、図２８に示すように、メディアＩＤ格納モジュール部６１０ａから、暗号化部６１４ａ及び共通鍵格納部６１６ａを省略し、センター６００ａにおいて、メディアＩＤ格納モジュール部を半導体デバイスとして実装し、センター６００ａは、メモリカード１００ａから固有鍵生成部６１１ａが生成するカード固有鍵を取得し、取得したカード固有鍵を用いて、カードデバイス鍵を暗号化し、暗号化したカードデバイス鍵を、メディアＩＤ格納モジュールとともに発行してもよい。
【０１９５】
（４）実施の形態１及び２では、デジタルコンテンツの記録及び再生の両方の機能を持つ装置を記録再生装置２００及び２００ａについて説明している。しかし、記録再生装置は、再生機能のみを持つ再生装置又は記録機能のみを持つ記録装置として実現してもよい
（５）実施の形態１及び２では、メモリカードの制御部と、メディアＩＤ格納モジュールをそれぞれ別々の半導体デバイスで実現するとしたが、この構成に限定されない。例えば、メディアＩＤ格納モジュールに、制御部の機能を組み込み、メモリカードの制御部とメディアＩＤ格納モジュールを１つの半導体で構成してもよい。
３．実施の形態３
本発明に係る他の実施の形態について、図面を参照しながら説明する。

３．１　全体構成

図２９は、実施の形態３における記録再生システム１３００と、記録再生システム１３００の製造に係るカードメーカー１４００、装置メーカー１５００、センター（鍵発行局）１６００及びコントローラベンダ１７００の全体関係を示す図である。コントローラベンダ１７００は、センター１６００から信頼されている。記録再生システム１３００は複数のメモリカード１１００、・・・、複数の記録再生装置１２００、・・・から構成される。なお、カードメーカー１４００、装置メーカー１５００、センター１６００及びコントローラベンダ１７００は、それぞれ、カードメーカー、装置メーカー、センター及びコントローラベンダが有する装置を表している。

【０１９６】

センター１６００は、以下の処理（ａ）～（ｄ）を行う。

（ａ）センター１６００は、コントローラベンダ１７００からコントローラ鍵１９４０を受け取る。コントローラベンダ１７００は、センター１６００がコントローラ１９１０の製造に関するライセンスを締結した相手である。コントローラ１９１０は、メモリカード１１００に実装される。

（ｂ）センター１６００は、暗号化カードデバイス鍵及び暗号化メディア鍵群を生成する暗号化カードデバイス鍵は、受け取ったコントローラ鍵を用いて、カードデバイス鍵を暗号化することにより、生成される。暗号化メディア鍵群は、複数の暗号化メディア鍵を含む。複数の暗号化メディア鍵は、複数のカードデバイス鍵及び複数の装置デバイス鍵のそれぞれを用いて、１個のメディア鍵を暗号化することにより、生成される。なお、カードデバイス鍵はメモリカード毎に異なる鍵であり、装置デバイス鍵は記録再生装置毎に異なる鍵である。

（ｃ）センター１６００は、カードメーカー１４００に対して、暗号化カードデバイス鍵１９６０及び暗号化メディア鍵群１９２０を発行する。カードメーカー１４００は、センター１６００がメモリカード１１００の製造に関するライセンスを締結した相手である。

（ｄ）センター１６００は、装置メーカー１５００に対して、記録再生装置１２００の製造に必要な装置デバイス鍵１９３０を発行する。装置メーカー１５００は、センター１６００が記録再生装置１２００の製造に関するライセンスを締結した相手である。

【０１９７】

なお、コントローラ１９１０、暗号化カードデバイス鍵１９６０、暗号化メディア鍵群１９２０、装置デバイス鍵１９３０及びコントローラ鍵１９４０の詳細については後述する。

【０１９８】

コントローラベンダ１７００は、コントローラ鍵１９４０を生成し、コントローラ鍵１９４０をセンター１６００に送付するとともに、コントローラ１９１０をカードメーカー１４００に発行する。ここで、コントローラ１９１０は、メモリカード１１００に搭載されるメモリを制御したり、メモリカード１１００が装着される記録再生装置１２００とのインターフェースを提供する半導体デバイスである。具体的には、コントローラ１９１０は、ＬＳＩなどの半導体チップとして構成される。また、コントローラ１９１０は、耐タンパー（tamper resistant）化されている耐タンパーモジュールである。そのため、コントローラ１９１０内部の情報や構成を、外から解析することはできない。

【０１９９】

カードメーカー１４００は、コントローラベンダ１７００から受け取ったコントローラ１９１０、センター１６００から受け取った暗号化カードデバイス鍵１９６０及び暗号化メディア鍵群１９２０を、メモリカード１１００に実装する。

【０２００】

装置メーカー１５００は、センター１６００から受け取った装置デバイス鍵１９３０を記録再生装置１２００に実装する。

３．２　センター１６００、コントローラベンダ１７００、カードメーカー１４００及び装置メーカー１５００の構成

図３０に、センター１６００、コントローラベンダ１７００及びカードメーカー１４００の構成を示す。また、図３１に、センター１６００及び装置メーカー１５００の構成を示す。

【０２０１】

センター１６００は、図３０に示すように、ベンダＩＤ／コントローラ鍵受取手段１６１０、ベンダＩＤ／コントローラ鍵格納手段１６１１、カードデバイス鍵生成手段１６２０、カードデバイス鍵暗号化手段１６３０、カードデバイス鍵注文受付手段１６４０、暗号化メディア鍵群生成手段１６５０、暗号化カードデバイス鍵発行手段１６６０、装置デバイス鍵注文受付手段１６７０、装置デバイス鍵生成手段１６８０及び装置デバイス鍵発行手段１６９０を備える。

【０２０２】

コントローラベンダ１７００は、図３０に示すように、メディアＩＤ生成手段１７１０メディアＩＤ実装手段１７２０、ベンダＩＤ／コントローラ鍵送付手段１７３０、コントローラ鍵生成手段１７４０、コントローラ鍵実装手段１７５０、ベンダＩＤ格納手段１７６０、コントローラ注文受付手段１７７０及びコントローラ発行手段１７８０を備える。

【０２０３】

カードメーカー１４００は、図３０に示すように、コントローラ注文手段１４１０、コントローラ／ベンダＩＤ受取手段１４２０、コントローラ実装手段１４３０、カードデバイス鍵注文手段１４４０、暗号化カードデバイス鍵受取手段１４５０及び暗号化カードデバイス鍵実装手段１４６０を備える。

【０２０４】

装置メーカー１５００は、図３１に示すように、装置デバイス鍵注文手段１５１０、装置デバイス鍵受取手段１５２０及び装置デバイス鍵実装手段１５３０を備える。

ここで、上記各手段は、例えば、ネットワークに接続されたＰＣなどのコンピュータ、コンピュータに接続されたハードディスク等の記憶装置、及び、半導体製造用治具、等により実現される。また、上記各手段が行う動作は、以下で述べる動作フローの説明にて詳述する。

３．３　センター１６００とコントローラベンダ１７００とカードメーカー１４００と間の動作

センター１６００とコントローラベンダ１７００とカードメーカー１４００と間の動作について、図３２に示すフローチャートを用いて説明する。

【０２０５】

図３２に示すように、コントローラベンダ１７００のメディアＩＤ生成手段１７１０は製造するコントローラ毎に異なる固有の値であるメディアＩＤ（言い換えると、メディア識別情報）を生成し、生成したメディアＩＤをメディアＩＤ実装手段１７２０へ出力する（Ｓ１１０１）。ここでメディアＩＤは、例えば１２８ビットの値である。

【０２０６】

なお、ここでは、コントローラベンダ１７００がメディアＩＤを生成するとしたがこの構成に限定されない（後述する変形例２参照）。

次に、コントローラベンダ１７００のコントローラ鍵生成手段１７４０は、ロット毎に異なるコントローラ鍵を生成し、生成したコントローラ鍵をコントローラ鍵実装手段１７５０及びベンダＩＤ／コントローラ鍵送付手段１７３０へ出力する（Ｓ１１０２）。

【０２０７】

ここで、ロットとは、予め定められた製造時の最小製造数単位である。“ロット毎にコントローラ鍵が異なる”とは、同じロットで製造される複数のコントローラ間では、コントローラ鍵が共通であるが、異なるロットで製造される複数のコントローラ間では、コントローラ鍵が異なることを意味する。コントローラ鍵は、例えば１２８ビットの値であるなお、ここではコントローラ鍵はロット毎に異なるものとしたがこの構成に限定されない（後述する変形例６参照）。

【０２０８】

次に、コントローラベンダ１７００のメディアＩＤ実装手段１７２０は、メディアＩＤ生成手段１７１０により生成されたメディアＩＤをコントローラ１９１０に実装する（Ｓ１１０３）。なお、コントローラ毎に異なる固有のメディアＩＤを、コントローラに実装（格納）する手段としては、以下の方法を用いることができる。例えば、コントローラ１９１０に実装された電気ヒューズによりコントローラ１９１０固有のメディアＩＤを格納する方法や、コントローラ１９１０に実装された内蔵メモリにコントローラ１９１０固有のメディアＩＤを格納する方法や、コントローラ１９１０に実装されたＰＵＦ（Ｐｈｙｓｉｃａｌ Ｕｎｃｌｏａｎａｂｌｅ Ｆｕｎｃｔｉｏｎ）によりコントローラ１９１０固有のメディアＩＤを格納する方法などを用いることができる。また、これら以外の構成により、コントローラ毎に固有のメディアＩＤを実装してもよい。

【０２０９】

次に、コントローラ鍵実装手段１７５０は、コントローラ鍵生成手段１７４０により生成されたコントローラ鍵をコントローラ１９１０に実装する（Ｓ１１０４）。これにより半製品であったコントローラは、完成品のコントローラとなる。コントローラにロット毎に異なるコントローラ鍵を実装する手段としては、例えば、マスクＲＯＭで実現することができる。また、マスクＲＯＭ以外の構成により、ロット毎に固有のコントローラ鍵を実装してもよい。

【０２１０】

次に、コントローラベンダ１７００のベンダＩＤ／コントローラ鍵送付手段１７３０はベンダＩＤ格納手段１７６０からベンダＩＤを読み出し、内部に記憶しているコントローラ鍵識別情報を読み出し、コントローラ鍵生成手段１７４０からコントローラ鍵を受け取り、読み出したベンダＩＤ、読み出したコントローラ鍵識別情報及び受け取ったコントローラ鍵をセンター１６００へ送付する（Ｓ１１０５）。ここで、ベンダＩＤは、ベンダＩＤ格納手段１７６０に格納され、コントローラベンダ１７００を識別する情報である。また、コントローラ鍵識別情報は、コントローラベンダ１７００が生成したコントローラ鍵を識別する情報である。ここでは、コントローラ鍵識別情報については、内部に記憶しているコントローラ鍵識別情報を読み出すものとしたが、この構成に限定されない。例えばコントローラ鍵生成手段１７４０が、コントローラ鍵とともに、そのコントローラ鍵を識別する情報であるコントローラ鍵識別情報を生成し、コントローラ鍵生成手段１７４０から、生成されたコントローラ鍵及びコントローラ鍵識別情報を受け取る構成としてもよいここで、コントローラ鍵識別情報としては、コントローラ鍵がロット毎に異なる場合、ロット番号を用いることができる。また、ベンダＩＤは、コントローラベンダ毎に異なる固有の値であり、例えば、センター１６００によりライセンス契約時に付与される。

【０２１１】

ここで、コントローラベンダ１７００は、センター１６００に対して、コントローラ鍵を、秘密に送付する必要がある。このために、例えば、コントローラベンダ１７００は、市販の暗号化ソフトウェアにより、コントローラ鍵を暗号化し、暗号化コントローラ鍵をセンター１６００に送るものとする。ここで、暗号化の一例は、ＡＥＳである。

【０２１２】

次に、センター１６００のベンダＩＤ／コントローラ鍵受取手段１６１０は、コントローラベンダ１７００から、ベンダＩＤ、コントローラ鍵識別情報及びコントローラ鍵を受け取る（Ｓ１１０６）。そして、ベンダＩＤ／コントローラ鍵受取手段１６１０は、ベンダＩＤ／コントローラ鍵格納手段１６１１に、受け取ったベンダＩＤ、コントローラ鍵識別情報及びコントローラ鍵を格納する（Ｓ１１０７）。

【０２１３】

図３３にセンター１６００にて格納されるコントローラ鍵情報１８１０の一例を示す。コントローラ鍵情報１８１０は、複数の組から構成され、各組は、１個のベンダＩＤ、１個又は２個のコントローラ鍵識別情報（ロット番号）及び１個のコントローラ鍵を含む。

【０２１４】

図３３に示す例では、ベンダＩＤ＝００１のコントローラベンダについては、ロット番

号＝００３のコントローラ鍵Ｋｃ００１－００３が格納されている。またベンダＩＤ＝００２のコントローラベンダについては、ロット番号＝００１と００２のコントローラ鍵Ｋｃ００２－００１、Ｋｃ００２－００２がそれぞれ格納されている。またベンダＩＤ＝００３のコントローラベンダについては、ロット番号＝００１のコントローラ鍵Ｋｃ００３－００１が格納されている。格納されたコントローラ鍵は、後述するＳ１１６のデバイス鍵の暗号化において使用される。

【０２１５】

次に、カードメーカー１４００のコントローラ注文手段１４１０は、コントローラベンダ１７００に対して、コントローラを注文する（Ｓ１１０８）。

ここで、コントローラを注文する際に用いるコントローラ注文書の一例を図３４に示す図３４に示すコントローラ注文書１８２０は、コントローラ注文手段１４１０がコントローラベンダ１７００に対してコントローラを注文する際に送信するデータである。図３４に示すように、コントローラ注文書には、カードメーカーＩＤ、コントローラの注文数（製造するメモリカードの数）等が記載される。ここで、カードメーカーＩＤは、カードメーカー毎に異なる固有の値であり、例えば、センター１６００によりライセンス契約時に付与される。コントローラの注文数欄は、カードメーカー１４００が必要とするコントローラの注文数を記載する。このようにして、カードメーカー１４００は、必要に応じてその都度、コントローラベンダ１７００に対して、コントローラ１９１０を注文することができる。

【０２１６】

次に、コントローラベンダ１７００のコントローラ注文受付手段１７７０は、カードメーカー１４００からコントローラの注文を受け付ける（Ｓ１１０９）。コントローラ発行手段１７８０は、コントローラ１９１０と、コントローラベンダ自身のベンダＩＤと、コントローラ１９１０に実装されたコントローラ鍵のコントローラ鍵識別情報とをカードメーカー１４００に発行する（Ｓ１１１０）。

【０２１７】

次に、カードメーカー１４００のコントローラ／ベンダＩＤ受取手段１４２０は、コントローラベンダ１７００から、コントローラ１９１０とベンダＩＤとコントローラに対応するコントローラ鍵識別情報とを受け取る（Ｓ１１１１）。

【０２１８】

次に、カードメーカー１４００のコントローラ実装手段１４３０は、各メモリカード１１００に、それぞれ、コントローラベンダ１７００から受け取ったコントローラ１９１０を実装する（Ｓ１１１２）。

【０２１９】

次に、カードメーカー１４００のカードデバイス鍵注文手段１４４０は、センター１６００に対して、カードデバイス鍵を注文する（Ｓ１１１３）。

図３５に、カードデバイス鍵の注文書の一例を示す。図３５に示すカードデバイス鍵注文書１８３０は、カードデバイス鍵注文手段１４４０がセンター１６００に対してカードデバイス鍵を注文する際に送信するデータである。図３５に示すように、カードデバイス鍵注文書１８３０には、カードメーカー自身のカードメーカーＩＤと、Ｓ１１１１で受け取ったコントローラベンダ１７００のベンダＩＤと、コントローラ鍵識別情報（ロット番号）と、カードデバイス鍵の注文数（製造するメモリカードの数）と、暗号化メディア鍵群の要否とが記載される。ここで、カードメーカーＩＤは、カードメーカー毎に異なる固有の値であり、例えば、センター１６００によりライセンス契約時に付与される。カードデバイス鍵の注文数欄は、カードメーカー１４００が、カードデバイス鍵を実装して製造するメモリカードの数を記載する。暗号化メディア鍵群の要否欄は、必要なときに“要”とする。

【０２２０】

このようにして、カードメーカーは、カードデバイス鍵を注文することができる。

次に、センターのカードデバイス鍵注文受付手段１６４０は、カードメーカー１４００

からカードデバイス鍵の注文書を受け付ける（Ｓ１１１４）。そして、カードデバイス鍵生成手段１６２０は、カードデバイス鍵の注文書のカードデバイス鍵の注文数に応じてカードデバイス鍵及び当該カードデバイス鍵を識別するカードデバイス鍵ＩＤを生成する（Ｓ１１１５）。
そして、カードデバイス鍵暗号化手段１６３０は、カードデバイス鍵の注文書のベンダＩＤとコントローラ識別情報（ロット番号）に対応するコントローラ鍵を、ベンダＩＤ／コントローラ鍵格納手段１６１１から取得する。カードデバイス鍵暗号化手段１６３０は、取得したコントローラ鍵を用いて、Ｓ１１１５にて生成したカードデバイス鍵を暗号化する（Ｓ１１１６）。例えば、図３５に示すカードデバイス鍵注文書１８３０の例では、ベンダＩＤが００２で、コントローラ鍵識別情報が００１であるので、図３３に示すコントローラ鍵情報１８１０から、コントローラ鍵としてＫＣ００２－００１が取得される。

【０２２１】

次に、カードデバイス鍵の注文書の暗号化メディア鍵群の要否欄が“要”の場合は、暗号化メディア鍵群生成手段１６５０は、暗号化メディア鍵群を生成する（Ｓ１１１７）。

なお、ここでは、カードデバイス鍵生成手段１６２０、及び、暗号化メディア鍵群生成手段１６５０は、カードデバイス鍵の注文書を受け付けた後に、注文書の内容に応じてカードデバイス鍵や暗号化メディア鍵群を生成する構成としたが、この構成に限定されない例えば、カードデバイス鍵生成手段１６２０、及び、暗号化メディア鍵群生成手段１６５０は、予め、カードデバイス鍵や暗号化メディア鍵群を生成して保持しておき、カードメーカーからの注文に応じて、保持しているものを発行してもよい。

【０２２２】

次に、暗号化カードデバイス鍵発行手段１６６０は、カードメーカー１４００に対して暗号化カードデバイス鍵、カードデバイス鍵ＩＤ及び必要に応じて暗号化メディア鍵群を発行する（Ｓ１１１８）。

【０２２３】

なお、注文書の暗号化メディア鍵群の要否欄が“不要”の場合も、センターが暗号化メディア鍵群を更新した場合には、カードメーカー１４００に発行される場合がある。

暗号化メディア鍵群の一例を図３７に示す。図３７に示す通り、暗号化メディア鍵群１８４０は、複数の組を含み、各組は、ＩＤと暗号化メディア鍵とから構成される。ＩＤはカードデバイス鍵ＩＤ又は装置デバイス鍵ＩＤである。カードデバイス鍵ＩＤは、カードデバイス鍵を一意に識別する識別情報であり、装置デバイス鍵ＩＤは、装置デバイス鍵を一意に識別する識別情報である。各暗号化メディア鍵は、ＡＥＳ暗号関数を用いて、当該暗号化メディア鍵に対応するカードデバイス鍵ＩＤにより識別される１２８ビットのカードデバイス鍵を用いて、又は当該暗号化メディア鍵に対応する装置デバイス鍵ＩＤにより識別される１２８ビットの装置デバイス鍵を用いて、１２８ビットのメディア鍵を暗号化して生成したものである。

【０２２４】

次に、カードメーカー１４００の暗号化カードデバイス鍵受取手段１４５０は、センター１６００から、暗号化カードデバイス鍵、カードデバイス鍵ＩＤ及び必要に応じて暗号化メディア鍵群を受け取る（Ｓ１１１９）。

【０２２５】

次に、カードメーカー１４００の暗号化カードデバイス鍵実装手段１４６０は、メモリカード１１００を製造する際、各メモリカード１１００に、それぞれ、Ｓ１１１２において、各メモリカードに実装されたコントローラに対応付けて実装すべき暗号化カードデバイス鍵、カードデバイス鍵ＩＤ及び暗号化メディア鍵群を実装する（Ｓ１１２０）。
このように実装することにより、メモリカードに実装されたコントローラにおいて、そのコントローラに格納されているコントローラ鍵により、当該メモリカードに実装された暗号化カードデバイス鍵が正しく復号可能となる。

３．４　センター１６００と装置メーカー１５００と間の動作

センター１６００と装置メーカー１５００と間の動作について、図３８に示すフローチ

ャートを用いて説明する。

【０２２６】

図３８に示すように、装置メーカー１５００の装置デバイス鍵注文手段１５１０は、センター１６００に対して、装置デバイス鍵を注文する（Ｓ１２０１）。

図３９に、装置デバイス鍵の注文書の一例を示す。図３９に示す装置デバイス鍵注文書１８５０は、装置デバイス鍵注文手段１５１０がセンター１６００に対して装置デバイス鍵を注文する際に送信するデータである。図３９に示すように、装置デバイス鍵注文書１８５０には、装置メーカー自身の装置メーカーＩＤと、装置デバイス鍵の注文数（製造する記録再生装置の数）と、暗号化メディア鍵群の要否とが記載される。ここで、装置メーカーＩＤは、装置メーカー毎に異なる固有の値であり、例えば、センター１６００によりライセンス契約時に付与される。装置デバイス鍵の注文数欄は、装置メーカー１５００が装置デバイス鍵を実装して製造する記録再生装置の数を記載する。暗号化メディア鍵群の要否欄は、必要なときに“要”とする。

【０２２７】

このようにして、装置メーカー１５００は、装置デバイス鍵を注文することができる。

次に、センター１６００の装置デバイス鍵注文受付手段１６７０は、装置メーカー１５００から装置デバイス鍵の注文書を受け付ける（Ｓ１２０２）。そして、装置デバイス鍵生成手段１６８０は、装置デバイス鍵の注文書の装置デバイス鍵の注文数に応じて装置デバイス鍵及び当該装置デバイス鍵を識別する装置デバイス鍵ＩＤを生成する（Ｓ１２０３）。ここでは、装置デバイス鍵生成手段１６８０は、装置デバイス鍵の注文書を受け付けた後に、装置デバイス鍵を生成する構成としたが、この構成に限定されない。例えば、装置デバイス鍵生成手段１６８０は、予め、装置デバイス鍵を生成して保持しておき、装置メーカーからの注文に応じて、保持しているものを発行してもよい。そして、装置デバイス鍵発行手段１６９０は、装置メーカー１５００に対して装置デバイス鍵及び装置デバイス鍵ＩＤを発行する（Ｓ１２０４）。また、注文書の暗号化メディア鍵群の要否欄が“要”の場合は、暗号化メディア鍵群を発行する。

【０２２８】

なお、注文書の暗号化メディア鍵群の要否欄が“不要”の場合も、センター１６００が暗号化メディア鍵群を更新した場合には、装置メーカー１５００に発行される場合がある

次に、装置メーカー１５００の装置デバイス鍵受取手段１５２０は、センター１６００から、装置デバイス鍵、装置デバイス鍵ＩＤ及び必要に応じて暗号化メディア鍵群を受け取る（Ｓ１２０５）。

【０２２９】

ここで、センター１６００は、装置メーカー１５００に対して、装置デバイス鍵を、秘密に発行する必要がある。このために、例えば、センター１６００は、市販の暗号化ソフトウェアにより、装置デバイス鍵を暗号化して、暗号化装置デバイス鍵を生成し、暗号化装置デバイス鍵を装置メーカー１５００に送るものとする。ここで、暗号化において用いられる暗号方式の一例は、ＡＥＳである。

【０２３０】

次に、装置メーカー１５００の装置デバイス鍵実装手段１５３０は、記録再生装置１２００を製造する際、各記録再生装置１２００に、それぞれ、装置デバイス鍵及び装置デバイス鍵ＩＤと、必要に応じて暗号化メディア鍵群を実装する（Ｓ１２０６）。ここで、装置デバイス鍵は、外部から容易に読み書きできないように実装するものとする。

３．５　記録再生システム１３００の構成

記録再生システム１３００を構成するメモリカード１１００及び記録再生装置１２００の詳細の構成を図４０に示す。

（１）メモリカード１１００の詳細の構成

図４０に示すように、メモリカード１１００は、メモリ部１１２０及びコントローラ１９１０から構成される。

（ａ）コントローラ１９１０の構成

図３６に、コントローラ１９１０の構成を示す。この図に示すように、コントローラ１９１０は、コントローラ鍵格納部１９１１、カードデバイス鍵格納部１９１２、復号部１９１３、メディア鍵生成部１９１４、メディア固有鍵生成部１９１５、メディアＩＤ格納部１９１６、認証部１９１７及び制御部１９１８から構成される。コントローラ１９１０は、ＬＳＩ等の半導体デバイスで構成される。コントローラ鍵格納部１９１１、カードデバイス鍵格納部１９１２、復号部１９１３、メディア鍵生成部１９１４、メディア固有鍵生成部１９１５及び認証部１９１７は、証明部１９０９を構成している。

【０２３１】

コントローラ鍵格納部１９１１には、コントローラベンダ１７００により、ロット毎に異なるコントローラ鍵が格納される。コントローラ鍵格納部１９１１は、具体的にはマスクＲＯＭなどで実現する。

【０２３２】

カードデバイス鍵格納部１９１２は、後述する復号部１９１３から受け取ったカード毎に異なるカードデバイス鍵を格納する。

復号部１９１３は、コントローラ鍵格納部１９９１から取得したコントローラ鍵を用いて、メモリカード１１００のメモリ部１１２０から取得した暗号化カードデバイス鍵を、ＡＥＳ復号関数を用いて、以下の式により復号してカードデバイス鍵を生成する。

【０２３３】

カードデバイス鍵＝ＡＥＳ－Ｄ（コントローラ鍵、暗号化カードデバイス鍵）

なお、ＡＥＳ暗号方式については広く知られているので説明は省略する。

次に、復号部１９１３は、生成したカードデバイス鍵をカードデバイス鍵格納部１９１２に送る。

【０２３４】

なお、暗号化カードデバイス鍵は、センター１６００により、ＡＥＳ暗号関数を用いて以下の式で生成され、カードメーカー１４００に与えられ、カードメーカー１４００は、メモリカード１１００のメモリ部１１２０に実装する。

【０２３５】

暗号化カードデバイス鍵＝ＡＥＳ－Ｅ（コントローラ鍵、カードデバイス鍵）

メディア鍵生成部１９１４は、メモリカード１１００のメモリ部１１２０の暗号化メディア鍵群格納部１１２２から暗号化メディア鍵群を取得し、カードデバイス鍵格納部１９１２からカードデバイス鍵ＩＤを取得し、取得した暗号化メディア鍵群の中から、取得したカードデバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択し、カードデバイス鍵格納部１９１２からカードデバイス鍵を取得し、ＡＥＳ復号関数を用いて、以下の式により、選択した暗号化メディア鍵を、取得したカードデバイス鍵を用いて復号することによりメディア鍵を生成し、生成したメディア鍵をメディア固有鍵生成部１９１５へ出力する

メディア鍵＝ＡＥＳ－Ｄ（カードデバイス鍵、暗号化メディア鍵）

ここで、暗号化メディア鍵群は、センター１６００により発行される。暗号化メディア鍵群の一例として、暗号化メディア鍵群１８４０を図３７に示す。

【０２３６】

メディア固有鍵生成部１９１５は、メディア鍵生成部１９１４からメディア鍵を取得し後述するメディアＩＤ格納部１９１６からメディアＩＤを取得する。メディア固有鍵生成部１９１５は、一方向性関数Ｇを用いて、メディア鍵生成部１９１４により生成されたメディア鍵と、メディアＩＤ格納部１９１６から取得したメディアＩＤとを用いて、以下の式によりメディア固有鍵を生成し、生成したメディア固有鍵を認証部１９１７へ出力する

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ復号関数を利用して以下の式により実現することができる。

【０２３７】

メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。

メディアＩＤ格納部１９１６には、前述の通り、コントローラベンダ１７００が、コントローラ毎に異なる固有のメディアＩＤとして、１２８ビットの異なる数値を格納する。メディアＩＤ格納部１９１６は、具体的には、電気ヒューズや、ＰＵＦや、半導体デバイスの内蔵メモリ等を用いて実現される。

【０２３８】

認証部１９１７は、記録再生装置１２００の認証部１２０４との間で相互認証を行う。相互認証の詳細については後述する。

制御部１９１８は、メモリカード１１００のメモリ部１１２０に対する所定の制御処理を行うとともに、記録再生装置１２００からの要求に応じて、所定の制御処理を行う。具体的には、記録再生装置１２００からの要求に応じて、メディアＩＤを記録再生装置１２００に送る。制御部１９１８は、記録再生装置１２００からの要求に応じて、メモリ部１１２０から、暗号化メディア鍵群を取得し、取得した暗号化メディア鍵群を記録再生装置１２００に送る。また、制御部１９１８は、記録再生装置１２００から受け取った暗号化コンテンツをメモリ部１１２０に格納する。

（ｂ）メモリ部１１２０の構成

メモリ部１１２０は、図４０に示すように、暗号化カードデバイス鍵格納部１１２１、暗号化メディア鍵群格納部１１２２及び暗号化コンテンツ格納部１１２３により構成される。メモリ部１１２０は、例えば、フラッシュメモリで構成される。

【０２３９】

暗号化カードデバイス鍵格納部１１２１は、例えば記録再生装置１２００からの書き込みができない領域である。暗号化カードデバイス鍵格納部１１２１には、メモリカード１１００の製造時に、カードメーカー１４００により、センター１６００から受け取った暗号化カードデバイス鍵、カードデバイス鍵ＩＤが格納される。

【０２４０】

なお、ここでは、暗号化カードデバイス鍵格納部１１２１は、記録再生装置１２００から書き込みできない領域であるとしたが、この構成に限定されない。例えば、暗号化カードデバイス鍵格納部１１２１は、記録再生装置１２００から読み書きできない領域であるとしてもよい。

【０２４１】

暗号化メディア鍵群格納部１１２２は、例えば記録再生装置１２００からデータの読み書きが可能な領域である。暗号化メディア鍵群格納部１１２２には、メモリカード１１００の製造時に、カードメーカー１４００により、センター１６００から受け取った暗号化メディア鍵群が格納される。

【０２４２】

なお、ここでは、暗号化メディア鍵群が更新される場合を想定し、暗号化メディア鍵群格納部１１２２は、記録再生装置１２００からデータの読み書きが可能な領域であるとしているが、この構成に限定されない。例えば、暗号化メディア鍵群が更新されない場合は暗号化メディア鍵群格納部１１２２は、記録再生装置１２００からデータの読み出しのみ可能な領域であるとしてもよい。

【０２４３】

暗号化コンテンツ格納部１１２３は、記録再生装置１２００からデータの読み書きが可能な領域である。暗号化コンテンツ格納部１１２３には、記録再生装置１２００によって暗号化されたコンテンツが格納される。

（２）記録再生装置１２００の詳細の構成

記録再生装置１２００は、図４０に示すように、メモリカード検証部１２１１、メディアＩＤ取得部１２０５、コンテンツ鍵生成部１２０６、コンテンツ受信部１２０７、コンテンツ暗復号部１２０８及びコンテンツ再生部１２０９から構成される。メモリカード検証部１２１１は、装置デバイス鍵格納部１２０１、メディア鍵生成部１２０２、メディア固有鍵生成部１２０３及び認証部１２０４から構成される。

（ａ）メモリカード検証部１２１１

メモリカード検証部１２１１は、メモリカード１１００から受け取った暗号化メディア鍵群を用いて生成したメディア固有鍵を用いて、メモリカード１１００との間で相互認証処理を行う。この相互認証処理により、そのメモリカード１１００が、正しいメモリカードか、不正なメモリカードかを判別することができる。

【０２４４】

以下、メモリカード検証部１２１１を構成する装置デバイス鍵格納部１２０１、メディア鍵生成部１２０２、メディア固有鍵生成部１２０３及び認証部１２０４について説明する。

【０２４５】

装置デバイス鍵格納部１２０１には、記録再生装置毎に異なる１２８ビットの装置デバイス鍵及び当該装置デバイス鍵を識別する装置デバイス鍵ＩＤが、外部から読み書きできないように、格納されている。

【０２４６】

メディア鍵生成部１２０２は、メモリカード１１００のメディア鍵生成部１９１４と同様の構成を有している。メディア鍵生成部１２０２は、メモリカード１１００のメモリ部１１２０の暗号化メディア鍵群格納部１１２２から暗号化メディア鍵群を取得し、装置デバイス鍵格納部１２０１から装置デバイス鍵ＩＤを取得し、取得した暗号化メディア鍵群の中から、取得した装置デバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択し、装置デバイス鍵格納部１２０１から装置デバイス鍵を取得する。メディア鍵生成部１２０２は、ＡＥＳ復号関数を用いて、以下の式により、選択した暗号化メディア鍵を、取得した装置デバイス鍵を用いて復号することによりメディア鍵を生成し、生成したメディア鍵をメディア固有鍵生成部１２０３へ出力する。

【０２４７】

メディア鍵＝ＡＥＳ－Ｄ（装置デバイス鍵、暗号化メディア鍵）

ここで、暗号化メディア鍵群は、メモリカード１１００より取得される。暗号化メディア鍵群の一例として、暗号化メディア鍵群１８４０を図３７に示している。

【０２４８】

メディア固有鍵生成部１２０３は、メモリカード１１００のメディア固有鍵生成部１９１５と同様の構成を有している。メディア固有鍵生成部１２０３は、メディア鍵生成部１２０２からメディア鍵を取得し、メモリカード１１００のコントローラ１９１０のメディアＩＤ格納部１９１６からメディアＩＤを取得する。メディア固有鍵生成部１２０３は、一方向性関数Ｇを用いて、取得したメディア鍵と取得したメディアＩＤから以下の式によりメディア固有鍵を生成し、生成したメディア固有鍵を認証部１２０４へ出力する。

【０２４９】

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ復号関数を利用して実現することができる。

【０２５０】

メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。

認証部１２０４は、メモリカード１１００の認証部１９１７との間で相互認証処理を行う。相互認証処理の詳細は、後述する。

（ｂ）メディアＩＤ取得部１２０５、コンテンツ鍵生成部１２０６、コンテンツ受信部１２０７、コンテンツ暗復号部１２０８及びコンテンツ再生部１２０９

メディアＩＤ取得部１２０５は、認証部１２０４において相互認証に成功したときのみ認証部１２０４からメディアＩＤを取得し、取得したメディアＩＤをコンテンツ鍵生成部１２０６に送る。

【０２５１】

コンテンツ鍵生成部１２０６は、メディアＩＤ取得部１２０５からメディアＩＤを受け取り、受け取ったメディアＩＤに基づいてコンテンツ鍵を生成する。具体的な、コンテン

ツ鍵の生成方法については、後述する。次に、生成したコンテンツ鍵をコンテンツ暗復号部１２０８へ出力する。

【０２５２】

コンテンツ受信部１２０７は、デジタル放送されたデジタルコンテンツや、デジタル配信されたデジタルコンテンツを受信し、受信したデジタルコンテンツをコンテンツ暗復号部１２０８に送る。

【０２５３】

コンテンツ暗復号部１２０８は、コンテンツ鍵生成部１２０６からコンテンツ鍵を受け取る。次に、コンテンツ暗復号部１２０８は、コンテンツ鍵生成部１２０６から受け取ったコンテンツ鍵を用いて、コンテンツ受信部１２０７より受け取ったデジタルコンテンツを暗号化してメモリカード１１００に送る。又は、コンテンツ暗復号部１２０８は、コンテンツ鍵生成部１２０６から受け取ったコンテンツ鍵を用いて、メモリカード１１００から受け取った暗号化デジタルコンテンツを復号して、デジタルコンテンツを生成し、生成したデジタルコンテンツをコンテンツ再生部１２０９に送る。コンテンツの暗復号の詳細については、後述する。

【０２５４】

コンテンツ再生部１２０９は、コンテンツ暗復号部１２０８からデジタルコンテンツを受け取り、受け取ったデジタルコンテンツを再生する。

３．６　記録再生システム１３００の動作

（１）記録再生装置１２００による記録時の動作

記録再生装置１２００がメモリカード１１００にコンテンツを記録する際の動作について、図４１に示すフローチャートを用いて説明する。

【０２５５】

図４１に示すように、まず、記録再生装置１２００のメディア固有鍵生成部１２０３はメモリカード１１００にメディアＩＤを要求する（Ｓ１３０１）。メモリカード１１００の制御部１９１８は、記録再生装置１２００からのメディアＩＤの要求に対応して、メディアＩＤ格納部１９１６からメディアＩＤを取得し、取得したメディアＩＤを記録再生装置１２００に送る（Ｓ１３０２）。記録再生装置１２００のメディア鍵生成部１２０２はメモリカード１１００に暗号化メディア鍵群を要求する（Ｓ１３０３）。メモリカード１１００の制御部１９１８は、記録再生装置１２００からの暗号化メディア鍵群の要求に対応して、メモリ部１１２０の暗号化メディア鍵群格納部１１２２から暗号化メディア鍵群を取得し、取得した暗号化メディア鍵群を記録再生装置１２００に送る（Ｓ１３０４）。

【０２５６】

記録再生装置１２００のメディア鍵生成部１２０２は、メモリカード１１００から受け取った暗号化メディア鍵群から、装置デバイス鍵格納部１２０１から取得した装置デバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択する。次に、暗号化メディア鍵群から選択した１個の暗号化メディア鍵と、装置デバイス鍵格納部１２０１から取得した装置デバイス鍵を用いてＡＥＳ復号関数を用いて、以下の式によりメディア鍵を生成する。

【０２５７】

メディア鍵＝ＡＥＳ－Ｄ（装置デバイス鍵、暗号化メディア鍵）

そして、生成したメディア鍵をメディア固有鍵生成部１２０３に送る（Ｓ１３０５）。

記録再生装置１２００のメディア固有鍵生成部１２０３は、ステップＳ１３０２で取得したメディアＩＤとメディア鍵生成部１２０２から受け取ったメディア鍵とを用いて、一方向性関数Ｇにより、以下の式よりメディア固有鍵を生成する。

【０２５８】

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ暗号を利用して実現することができる。

【０２５９】

メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ

ここで、（＋）は、排他的論理和演算を表す。（Ｓ１３０６）
一方、メモリカード１１００の制御部１９１８は、メモリ部１１２０の暗号化カードデバイス鍵格納部１１２１から暗号化カードデバイス鍵を取得し、取得した暗号化カードデバイス鍵を復号部１９１３に送る。
【０２６０】
そして、復号部１９１３は、受け取った暗号化カードデバイス鍵を、コントローラ鍵格納部９１１から取得したコントローラ鍵を用いて以下の式で復号する。
カードデバイス鍵＝ＡＥＳ－Ｄ（コントローラ鍵、暗号化カードデバイス鍵）
次に、復号部１９１３は、カードデバイス鍵格納部１９１２に復号したカードデバイス鍵を送る。次に、メモリカード１１００の制御部１９１８は、メモリ部１１２０の暗号化メディア鍵群格納部１１２２から暗号化メディア鍵群を取得し、取得した暗号化メディア鍵群をメディア鍵生成部１９１４に送る。
【０２６１】
次に、メディア鍵生成部１９１４は、記録再生装置１２００のメディア鍵生成部１２０２と同様に、受け取った暗号化メディア鍵群から、暗号化カードデバイス鍵格納部１１２１から取得したカードデバイス鍵ＩＤに対応する１個の暗号化メディア鍵を選択する。次に、暗号化メディア鍵群から選択した１個の暗号化メディア鍵と、カードデバイス鍵格納部１９１２から取得したカードデバイス鍵を用いてＡＥＳ復号関数を用いて、以下の式によりメディア鍵を生成する。
【０２６２】
メディア鍵＝ＡＥＳ－Ｄ（カードデバイス鍵、暗号化メディア鍵）
次に、メディア鍵生成部１９１４は、生成したメディア鍵をメディア固有鍵生成部１９１５に送る（Ｓ１３０７）。
【０２６３】
メモリカード１１００のメディア固有鍵生成部１９１５は、記録再生装置１２００のメディア固有鍵生成部１２０３と同様に、メディアＩＤ格納部１９１６から取得したメディアＩＤとメディア鍵生成部１９１４から受け取ったメディア鍵とを用いて、一方向性関数Ｇにより、以下の式よりメディア固有鍵を生成する。
【０２６４】
メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）
なお、一方向性関数Ｇの具体例としては、例えばＡＥＳ暗号を利用して実現することができる。
【０２６５】
メディア固有鍵＝ＡＥＳ－Ｄ（メディア鍵、メディアＩＤ）（＋）メディアＩＤ
ここで、（＋）は、排他的論理和演算を表す。（Ｓ１３０８）
メモリカード１１００の認証部１９１７と記録再生装置１２００の認証部１２０４は、相互認証を行う（Ｓ１３０９）。相互認証の詳細については後述する。
【０２６６】
ステップＳ１３０９の相互認証が失敗した場合、処理を終了する。こうして、暗号化コンテンツの復号を禁止し、又はコンテンツの暗号化を禁止している。
ステップＳ１３０９の相互認証が成功した場合、メディアＩＤ取得部１２０５は、認証部１２０４からメディアＩＤを取得する（Ｓ１３１０）。
【０２６７】
コンテンツ鍵生成部１２０６は、メディアＩＤ取得部２０５から取得したメディアＩＤに対して、例えば、一方向性関数Ｆを用いて、以下の式によりコンテンツ鍵を生成し、生成したコンテンツ鍵をコンテンツ暗復号部１２０８に送る（Ｓ１３１１）。
【０２６８】
コンテンツ鍵＝Ｆ（メディアＩＤ）
一方向性関数Ｆの具体例としは、例えば、ＡＥＳ暗号を用いて以下の式で実現できる。
コンテンツ鍵＝ＡＥＳ（コンテンツ鍵生成用秘密鍵、メディアＩＤ）（＋）メディアＩ

D
ここで、（＋）は、排他的論理和演算を表す。また、コンテンツ鍵生成用秘密鍵は、１２８ビットであり、全ての記録再生装置に共通で秘密であり、予め、コンテンツ鍵生成部１２０６が保持しているものとする。ＡＥＳ暗号については、広く知られているので説明は省略する。

【０２６９】
なお、ここでは、コンテンツ鍵生成関数としてＡＥＳ暗号を用いる例を示したが、１２８ビットのメディアＩＤに基づき、１２８ビットのランダムな乱数を、コンテンツ鍵として生成する一方向性関数であればどんな構成でもよい。

【０２７０】
コンテンツ暗復号部１２０８は、コンテンツ受信部１２０７にて受信されたデジタル放送されたデジタルコンテンツ、もしくは、デジタル配信されたデジタルコンテンツを、コンテンツ鍵生成部１２０６から受け取ったコンテンツ鍵を用いて、暗号化する（Ｓ１３１２）。そして、暗号化されたデジタルコンテンツをメモリカード１１００に送付する（Ｓ１３１３）。

【０２７１】
ここで、コンテンツの暗号化は、例えば、以下の式を用いて行う
暗号化されたデジタルコンテンツ＝ＡＥＳ－ＥＣＢＣ（コンテンツ鍵、デジタルコンテンツ）
ここで、ＡＥＳ－ＥＣＢＣとは、ＡＥＳ暗号をＣＢＣモード（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）で利用して暗号化することを示す。ＣＢＣモードについては、広く知られているので説明を省略する。なお、ここでは、ＡＥＳ－ＣＢＣを用いる場合を示したがこの構成に限定されない。

【０２７２】
メモリカード１１００の制御部１９１８は、記録再生装置１２００から暗号化されたデジタルコンテンツを受け取り、受け取った暗号化デジタルコンテンツを暗号化コンテンツ格納部１１２３に格納する（Ｓ１３１４）。

（２）相互認証処理の一例
次に、相互認証処理の一例を、図４２に示すプロセスチャートを用いて説明する。ここで説明する相互認証処理は、チャレンジ・レスポンス型の認証である。

【０２７３】
メモリカード１１００の認証部１９１７は、チャレンジデータとして乱数Ｒ１を生成する（Ｓ１５０１）。メモリカード１１００の認証部１９１７は、生成したチャレンジデータとしての乱数Ｒ１を記録再生装置１２００に送る。記録再生装置１２００の認証部１２０４は、チャレンジデータとしての乱数Ｒ１を受け取る（Ｓ１５０２）。

【０２７４】
記録再生装置１２００の認証部１２０４は、受け取ったチャレンジデータとしての乱数Ｒ１を、メディア固有鍵生成部１２０３から受け取ったメディア固有鍵を用いて暗号化して、レスポンスデータとしての暗号化乱数Ｅ１＝ＡＥＳ－Ｅ（メディア固有鍵、乱数Ｒ１）を生成する（Ｓ１５０３）。ここで、レスポンスデータとしての暗号化乱数Ｅ１は、記録再生装置１２００が自己の正当性を証明するための証明情報である。レスポンスデータとしての暗号化乱数Ｅ１をメモリカード１１００に送り、メモリカード１１００の認証部１９１７は、レスポンスデータとしての暗号化乱数Ｅ１を受け取る（Ｓ１５０４）。

【０２７５】
メモリカード１１００の認証部１９１７は、受け取ったレスポンスデータとしての暗号化乱数Ｅ１を、メディア固有鍵生成部１９１５から取得したメディア固有鍵を用いて、復号して乱数Ｄ１＝ＡＥＳ－Ｄ（メディア固有鍵、暗号化乱数Ｅ１）を生成する（Ｓ１５０５）。メモリカード１１００の認証部１９１７は、生成した乱数Ｄ１とＳ１５０１で生成した乱数Ｒ１を比較し（Ｓ１５０６）、一致すれば、次のＳ１５１１に進み、一致しなければ、相互認証処理を終了する。

【０２７６】
記録再生装置１２００の認証部１２０４は、チャレンジデータとして乱数Ｒ２を生成する（Ｓ１５１１）。記録再生装置１２００の認証部１２０４は、生成したチャレンジデータとしての乱数Ｒ２をメモリカード１１００に送る。メモリカード１１００の認証部１９１７は、チャレンジデータとしての乱数Ｒ２を受け取る（Ｓ１５１２）。
【０２７７】
メモリカード１１００の認証部１９１７は、受け取ったチャレンジデータとしての乱数Ｒ２を、メディア固有鍵生成部１９１５から受け取ったメディア固有鍵を用いて暗号化してレスポンスデータとしての暗号化乱数Ｅ２＝ＡＥＳ－Ｅ（メディア固有鍵、乱数Ｒ２）を生成する（Ｓ１５１３）。ここで、レスポンスデータとしての暗号化乱数Ｅ２は、メモリカード１１００が自己の正当性を証明するための証明情報である。レスポンスデータとしての暗号化乱数Ｅ２を記録再生装置１２００に送り、記録再生装置１２００の認証部１２０４は、レスポンスデータとしての暗号化乱数Ｅ２を受け取る（Ｓ１５１４）。
【０２７８】
記録再生装置１２００の認証部１２０４は、受け取ったレスポンスデータとしての暗号化乱数Ｅ２を、メディア固有鍵生成部１２０３から取得したメディア固有鍵を用いて、復号して、乱数Ｄ２＝ＡＥＳ－Ｄ（メディア固有鍵、暗号化乱数Ｅ２）を生成する（Ｓ１５１５）。記録再生装置１２００の認証部１２０４は、生成した乱数Ｄ２とＳ１５１１で生成した乱数Ｒ２を比較し（Ｓ１５１６）、一致すれば、メディアＩＤ取得部１２０５にメディアＩＤを送る。一致しなければ、相互認証処理を終了する。
【０２７９】
図４２に示すプロセスチャートにおいて、ステップＳ１５０１、Ｓ１５０２、Ｓ１５０５、Ｓ１５０６は、認証部１９１７内において、検証部１９１７ｖを構成している。またステップＳ１５０３、Ｓ１５０４は、認証部１２０４内において、証明生成部１２０４ｐを構成している。
【０２８０】
さらに、図４２に示すプロセスチャートにおいて、ステップＳ１５１１、Ｓ１５１２、Ｓ１５１５、Ｓ１５１６は、認証部１２０４内において、検証部１２０４ｖを構成している。また、ステップＳ１５１３、Ｓ１５１４は、認証部１９１７内において、証明生成部１９１７ｐを構成している。
【０２８１】
上記のＡＥＳ－Ｅは、ＡＥＳ暗号化関数であり、上記のＡＥＳ－Ｄは、ＡＥＳ復号関数である。なお、上記において、ＡＥＳを用いているが、これには限定されない。他の共通鍵暗号方式を用いるとしてもよい。また、上記において、チャレンジ・レスポンス型の認証プロトコルを用いているがこれには限定されない。他の認証プロトコルを用いてもよい
（３）記録再生装置１２００による再生時の動作
記録再生装置１２００がメモリカード１１００から暗号化コンテンツを読み出し再生する際の動作について、図４３に示すフローチャートを用いて説明する。
【０２８２】
なお、図４３のＳ１４０１からＳ１４１１は、それぞれ、図４１のＳ１３０１からＳ１３１１と全く同じ動作であるので説明を省略する。
記録再生装置１２００のコンテンツ暗復号部１２０８は、メモリカード１１００に暗号化コンテンツの送付を要求する（Ｓ１４１２）。メモリカード１１００のコントローラ１９１０の制御部１９１８は、記録再生装置１２００からの暗号化コンテンツの送付要求に対応し、暗号化コンテンツ格納部１１２３から暗号化コンテンツを読み出し、読み出した暗号化コンテンツを記録再生装置１２００に送付する（Ｓ１４１３）。コンテンツ暗復号部１２０８は、メモリカード１１００から暗号化コンテンツを受け取り、受け取った暗号化コンテンツを、コンテンツ鍵生成部１２０６から受け取ったコンテンツ鍵を用いて復号してコンテンツを生成し、生成したコンテンツをコンテンツ再生部に送る（Ｓ１４１４）
ここで、コンテンツの復号は、以下の式で表される。

【０２８３】
　復号されたデジタルコンテンツ＝ＡＥＳ－ＤＣＢＣ（コンテンツ鍵、暗号化されたデジタルコンテンツ）
　ここで、ＡＥＳ－ＤＣＢＣとは、ＡＥＳ暗号をＣＢＣモード（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）で利用して復号することを示す。
【０２８４】
　コンテンツ再生部１２０９は、コンテンツ暗復号部１２０８からコンテンツを受け取り受け取ったコンテンツを再生する（Ｓ１４１５）。
３．７　不正の判別
　実施の形態３の構成によれば、カードメーカー１４００が、不正なメモリカードを製造したとしても、記録再生装置１２００のメモリカード検証部１２１１により、正しく製造されたメモリカードか、不正なメモリカードかの判別が可能となる。このことを、図４４を用いて説明する。
【０２８５】
　図４４において、メモリカード１１００は、実施の形態３に係るメモリカード（以下、正規のメモリカードと称する）であり、記録再生装置１２００は、実施の形態３に係る記録再生装置（以下、正規の記録再生装置と称する）である。また、メモリカード１０１０Ｄは、不正なカードメーカーが、実施の形態３に係るメモリカード１１００と記録再生装置１２００を動作させることにより、メディアＩＤを取得し、従来の構成のメモリカード１０１０Ｄのメディアｉｄ格納部に格納して製造したメモリカード（以下、不正なメモリカードと称する）である。
【０２８６】
　このとき、不正なメモリカード１０１０Ｄを用いて、正規の記録再生装置１２００により記録再生処理を試みたとしても、不正なメモリカード１０１０Ｄは、メディア固有鍵を生成できない。したがって、正規の記録再生装置１２００のメモリカード検証部１２１１の認証部１２０４における相互認証処理に失敗する。すなわち、カードメーカーが、不正なメモリカードを製造したとしても、正規の記録再生装置１２００により、正規のメモリカードか不正なメモリカードかの判別が可能となる。
【０２８７】
　また、コントローラは、耐タンパー化されている。そのため、メディアＩＤ格納部１９１６、メディア固有鍵生成部１９１５及び認証部１９１７のそれぞれの動作や記録内容を外部から解析することはできない。したがって、不正なメモリカードの製造時にこれらの構成を複製することはできない。すなわち、カードメーカーが不正なメモリカードにコピーすることのできる情報は、記録もしくは再生処理のため、記録再生装置１２００に送られるメディアＩＤのみとなる。したがって、相互認証処理を不正なメモリカードを用いてエミュレートするような不正をも防止することができる。
３．８　変形例
（１）変形例１
　実施の形態３では、カードメーカー１４００が、センター１６００に対して、カードデバイス鍵の注文を行い、センター１６００がカードメーカー１４００に暗号化カードデバイス鍵を発行しているが、この構成には限定されない。
【０２８８】
　例えば、（ａ）コントローラベンダ１７００が、センター１６００に対して、カードデバイス鍵の注文を行い、（ｂ）センター１６００がコントローラベンダ１７００に暗号化カードデバイス鍵を発行し、（ｃ）カードメーカー１４００がコントローラベンダ１７００に対してコントローラの注文を行い、（ｄ）コントローラベンダ１７００が、カードメーカー１４００に、コントローラとともに、センター１６００から受け取った暗号化カードデバイス鍵を発行する構成としてもよい。上記構成によれば、カードメーカー１４００は、コントローラベンダ１７００から、コントローラと、そのコントローラに対応付けて実装すべき暗号化カードデバイス鍵を一緒に受け取るため、コントローラと、そのコント

ローラに対応付けてメモリカードに実装すべき暗号化カードデバイス鍵の管理、及び、メモリカードへの実装が容易となる。

【０２８９】

また、（ａ）カードメーカー１４００がコントローラベンダ１７００に対してコントローラの注文を行い、（ｂ）コントローラベンダ１７００が、センター１６００に対して、注文を受けたカードメーカー用のカードデバイス鍵の注文を行い、（ｃ）センター１６００がコントローラベンダ１７００に暗号化カードデバイス鍵を発行し、（ｄ）コントローラベンダ１７００が、カードメーカー１４００に、コントローラとともに、センター１６００から受け取った暗号化カードデバイス鍵を発行する構成としてもよい。上記構成によれば、カードメーカー１４００は、コントローラベンダ１７００から、コントローラと、そのコントローラに対応付けて実装すべき暗号化カードデバイス鍵を一緒に受け取るためコントローラと、そのコントローラに対応付けてメモリカードに実装すべき暗号化カードデバイス鍵の管理、及び、メモリカードへの実装が容易となる。

【０２９０】

（２）変形例２

実施の形態３では、コントローラベンダ１７００がメディアＩＤを生成しているが、この構成には限定されない。

【０２９１】

例えば、（ａ）センター１６００がメディアＩＤを生成し、（ｂ）コントローラベンダ１７００に通知し、（ｃ）コントローラベンダ１７００が、センター１６００から通知されたメディアＩＤをコントローラに実装する構成としてもよい。

【０２９２】

また、（ａ）カードメーカー１４００がメディアＩＤを生成し、（ｂ）コントローラベンダ１７００に通知し、（ｃ）コントローラベンダ１７００が、メディアＩＤのユニーク性をチェックした後、（ｄ）コントローラベンダ１７００がカードメーカー１４００から通知されたメディアＩＤをコントローラに実装する構成としてもよい。

【０２９３】

また、（ａ）センター１６００がメディアＩＤの少なくとも一部を生成し、（ｂ）生成したメディアＩＤの少なくとも一部をコントローラベンダ１７００に通知し、（ｃ）コントローラベンダ１７００が、メディアＩＤの残りの部分を生成し、（ｄ）コントローラベンダ１７００がセンター１６００から受け取ったメディアＩＤの少なくとも一部と自身の生成したメディアＩＤの残りの部分を連結してメディアＩＤを成形し、（ｅ）メディアＩＤをコントローラに実装する構成としてもよい。

【０２９４】

より具体的には、センター１６００が発行するメディアＩＤの一部として、センター１６００が発行するコントローラベンダ毎に異なる固有のベンダＩＤを用いてもよい。この場合、コントローラベンダ１７００が自由にメディアＩＤの残り部分を生成したとしてもメディアＩＤが、センター１６００が発行するベンダＩＤと、コントローラベンダ１７００が生成する値を連結したものとなるため、メディアＩＤのユニーク性が容易に保証される。

【０２９５】

また、（ａ）センター１６００がメディアＩＤの少なくとも一部をカードメーカー１４００に発行し、（ｂ）カードメーカー１４００がメディアＩＤの残りの部分を生成し、（ｃ）カードメーカー１４００が、センター１６００から受け取ったメディアＩＤの少なくとも一部と自身の生成したメディアＩＤの残りの部分を連結してメディアＩＤを成形し（ｄ）カードメーカー１４００が成形されたメディアＩＤをコントローラベンダ１７００に通知し、（ｅ）コントローラベンダ１７００がカードメーカー１４００から通知されたメディアＩＤのユニーク性をチェックした後、（ｆ）メディアＩＤをコントローラに実装する構成としてもよい。

【０２９６】

より具体的には、センター１６００が発行するメディアＩＤの一部として、センター１６００が発行するカードメーカー毎に異なる固有のカードメーカーＩＤを用いてもよい。この場合、カードメーカー１４００が自由にメディアＩＤの残り部分を生成したとしてもメディアＩＤが、センター１６００が発行するカードメーカーＩＤと、コントローラベンダ１７００が生成する値を連結したものとなるため、メディアＩＤのユニーク性が容易に保証される。

【０２９７】

また、（ａ）コントローラベンダ１７００がメディアＩＤの少なくとも一部を生成し、（ｂ）カードメーカー１４００が、メディアＩＤの残りの部分を生成し、（ｃ）カードメーカー１４００が、生成したメディアＩＤの残りの部分をコントローラベンダ１７００に通知し、（ｄ）コントローラベンダ１７００が自身の生成したメディアＩＤの少なくとも一部とカードメーカー１４００から受け取ったメディアＩＤの残り部分とを連結してメディアＩＤを成形し、（ｅ）メディアＩＤをコントローラに実装する構成としてもよい。また、上記の構成の組み合わせにより、構成してもよい。

【０２９８】

（３）変形例３

実施の形態３、及び、上記変形例２では、コントローラベンダ１７００がメディアＩＤ全体をコントローラに実装する構成としたが、この構成に限定されない。

【０２９９】

例えば、（ａ）コントローラベンダ１７００が、メディアＩＤのいずれかの一部のみをコントローラに実装し、（ｂ）カードメーカー１４００が、メディアＩＤの残り部分を、メモリカードのメモリ部に格納し、（ｃ）コントローラ内において、コントローラに実装されたメディアＩＤの一部とメモリ部に格納されたメディアＩＤの残り部分が連結されてメディアＩＤが成形されるとしてもよい。この構成によれば、コントローラ内に実装するデータ量を小さくできるため、コントローラの製造コストを削減することができる。またこの構成によれば、コントローラには、コントローラベンダ１７００自身が生成した情報（メディアＩＤのいずれかの一部）のみを実装すればよいため、コントローラの製造処理と、センターからの情報（メディアＩＤの残りの部分）の取得処理を切り離すことができる。

【０３００】

より具体的には、（ａ）コントローラベンダ１７００はメディアＩＤの少なくとも一部を生成し、（ｂ）生成したメディアＩＤの少なくとも一部のみをコントローラに実装し、（ｃ）センター１６００が、カードメーカー１４００に対して、メディアＩＤの残りの部分を発行し、（ｄ）カードメーカー１４００がセンター１６００から受け取ったメディアＩＤの残り部分をメモリカードのメモリ部に格納し、（ｅ）コントローラ内において、コントローラに実装されたメディアＩＤの一部と、メモリ部に格納されたメディアＩＤの残りの一部が連結されるとしてもよい。

【０３０１】

（４）変形例４

実施の形態３もしくは上記変形例３において、メディアＩＤの少なくとも一部を、カードデバイス鍵に関連する情報としてもよい。この構成により、コントローラに実装されるメディアＩＤと、そのコントローラが実装されるメモリカードのメモリ部に実装される暗号化カードデバイス鍵の対応付けの確認が可能となる。

【０３０２】

より具体的には、例えば、ＳＨＡハッシュ関数を用いて計算したカードデバイス鍵のハッシュ値をメディアＩＤの一部に含めてもよい。この場合、コントローラ内で、そのメディアＩＤの一部と、復号されたカードデバイス鍵のハッシュ値とがマッチするかを確認しマッチし、かつ認証が成功した場合のみメディアＩＤ取得部がメディアＩＤを取得するように構成してもよい。この構成によれば、万一、暗号化デバイス鍵が、当該暗号化デバイス鍵に対応する“カードデバイス鍵に関連する情報”を含むメディアＩＤとは異なるメデ

ィアＩＤが実装されたコントローラを実装したメモリカードのメモリ部にコピーされたとしも、コントローラ内で、メディアＩＤの一部と、復号されたカードデバイス鍵のハッシュ値とがマッチしない。したがって、不正にコピーされた暗号化デバイス鍵では、コンテンツの記録再生処理が行えないという効果が得られる。

【０３０３】

（５）変形例５

実施の形態３では、記録動作の際に、都度、メモリカード１１００が、図４１に示すＳ１３０７及びＳ１３０８の各ステップを実行して、メディア固有鍵を生成し、又は、再生動作の際に、都度、メモリカード１１００が、図４３に示すＳ１４０７、Ｓ１４０８の各ステップを実行して、メディア固有鍵を生成しているが、この構成には限定されない。

【０３０４】

例えば、コントローラ１９１０に、さらに暗号部を設け、

（ａ）メモリカードの初回の記録動作の際にのみ、図４１に示すＳ１３０７、Ｓ１３０８の各ステップを実行し、又は、初回の再生動作の際にのみ、図４３に示すＳ１４０７、Ｓ１４０８の各ステップを実行して、メディア固有鍵を生成し、

（ｂ）生成したメディア固有鍵を、２回目以降の記録もしくは再生の際に利用するために、暗号部にて、コントローラ１９１０のコントローラ鍵格納部１９１１に格納されたコントローラ鍵を用いて、以下の式で暗号化し、

暗号化メディア固有鍵＝ＡＥＳ－Ｅ（コントローラ鍵、メディア固有鍵）

（ｃ）暗号化されたメディア固有鍵をメモリカード１１００のメモリ部１１２０に格納し、

（ｄ）２回目以降の記録動作の際に、又は、２回目以降の再生動作の際に、コントローラ１９１０のコントローラ鍵格納部１９１１に格納されたコントローラ鍵を用いて、以下の式で復号し、

メディア固有鍵＝ＡＥＳ－Ｄ（コントローラ鍵、暗号化メディア固有鍵）

メディア固有鍵を生成するとしてもよい。

【０３０５】

また、メモリカード１１００のメモリ部１１２０に格納される暗号化メディア鍵群が更新される場合、暗号化メディア鍵群が更新されるときに、上記初回の記録動作又は初回の再生動作の場合と同様の動作を行うとしてもよい。すなわち、暗号化メディア鍵群が更新される際に、上記（ａ）と同様に、更新される暗号化メディア鍵群を用いて、図４１に示すステップＳ１３０７、Ｓ１３０８と同様のステップを実行して、新しいメディア固有鍵を生成し、次に、上記（ｂ）（ｃ）の処理を実行して、新しい暗号化されたメディア固有鍵を生成し、これをメモリカード１１００のメモリ部１１２０に格納し、以降の記録動作の際に、又は、再生動作の際に、上記（ｄ）を実行して新しいメディア固有鍵を生成してもよい。

【０３０６】

この構成によれば、記録動作又は再生動作におけるメディア固有鍵の生成処理が初回のみ、又は、暗号化メディア鍵群が更新されるときのみで済み、それ以降はメディア固有鍵の生成処理を軽減することができる。

【０３０７】

また、（ａ）コントローラベンダ１７００が生成したメディアＩＤをセンター１６００に送付し、

（ｂ）センター１６００が、メディア固有鍵を以下の式で生成し

メディア固有鍵＝Ｇ（メディア鍵、メディアＩＤ）

（ｃ）センター１６００が、デバイス鍵と同様の手順で、以下の式で暗号化メディア固有鍵を生成し

暗号化メディア固有鍵＝ＡＥＳ－Ｅ（コントローラ鍵、メディア固有鍵）

（ｄ）センター１６００が、カードメーカー１４００に対して、暗号化デバイス鍵と同様に、暗号化メディア固有鍵を発行し、

（ｅ）カードメーカー１４００が、メモリカード１１００のメモリ部１１２０に、暗号化メディア固有鍵を実装し、
（ｆ）メモリカード１１００が、記録動作、もしくは、再生動作の際に、コントローラ１９１０のコントローラ鍵格納部１９１１に格納されたコントローラ鍵を用いて、以下の式で復号し、
メディア固有鍵＝ＡＥＳ－Ｄ（コントローラ鍵、暗号化メディア固有鍵）
メディア固有鍵を生成するとしてもよい。

【０３０８】
この構成によれば、記録動作又は再生動作におけるメディア固有鍵の生成処理を軽減することができる。

（６）変形例６
実施の形態３では、コントローラ鍵は、ロット毎（予め定められた数量単位で製造されるコントローラの集合毎）に異なるとしたが、この構成に限定されない。

【０３０９】
例えば、コントローラ鍵は、所定数のロット毎に異なるとしてもよい。
また、コントローラ鍵は、ロット単位ではなく、コントローラの種別毎に固有としてもよい。この場合、コントローラ鍵識別情報としてコントローラの機種識別情報を用いることができる。

【０３１０】
また、コントローラを発行するカードメーカー毎に固有としてもよい。
また、メディアＩＤと同様に、コントローラ鍵は、コントローラ毎に異なるとしてもよい。この場合、コントローラ鍵識別情報としてメディアＩＤを用いることができる。

【０３１１】
（７）変形例７
実施の形態３では、メディアＩＤ、及びコントローラ鍵のサイズを１２８ビットとしたが、それに限定されない。他のサイズであるとしてもよい。

【０３１２】
（８）変形例８
実施の形態３では、図３２に示すステップＳ１１１０において、コントローラベンダ１７００が、カードメーカー１４００に対して、コントローラ、ベンダＩＤ及びコントローラ鍵識別情報を同時に発行しているが、この構成には限定されない。

【０３１３】
例えば、（ａ）コントローラベンダ１７００が、ベンダＩＤとコントローラ鍵識別情報とについては、カードメーカー１４００から注文を受け付け次第発行し、（ｂ）コントローラベンダ１７００が、コントローラについては、コントローラが製造され次第、発行するようにしてもよい。

【０３１４】
また、ベンダＩＤについては、カードメーカー１４００から初めてコントローラの注文を受け付けたときに１度だけ発行するとしてもよい。

（９）変形例９
実施の形態３では、図３２のステップＳ１１１５、ステップＳ１１１７、図３８のステップＳ１２０３において、センター１６００が、カードデバイス鍵、装置デバイス鍵、及び暗号化メディア鍵群をカードメーカー１４００や装置メーカー１５００からの注文に応じて生成しているが、この構成には限定されない。

【０３１５】
例えば、（ａ）センター１６００が、カードデバイス鍵、装置デバイス鍵、及び暗号化メディア鍵群を予め生成して保持しておき、（ｂ）カードメーカー１４００や装置メーカー１５００からの注文に応じて、保持しているものを発行してもよい。この構成により、センター１６００は、カードメーカー１４００や装置メーカー１５００からの注文に対して、迅速に、カードデバイス鍵、装置デバイス鍵、及び暗号化メディア鍵群を発行するこ

とができる。

【０３１６】

（１０）変形例１０

実施の形態３では、カードメーカー１４００が、コントローラ１９１０をメモリカード１１００に実装（図３２のＳ１１１２）した後、カードデバイス鍵を注文している（図３２のＳ１１１３）が、この構成には限定されない。

【０３１７】

例えば、（ａ）カードメーカー１４００が、ベンダＩＤ及びコントローラ鍵識別情報をコントローラベンダ１７００から受け取り次第（図３２のＳ１１１１）、カードメーカー１４００がセンター１６００に対して、カードデバイス鍵の注文を行うとしてもよい。

【０３１８】

（１１）変形例１１

実施の形態３では、記録媒体がメモリカードである場合を例として説明したが、記録媒体は、メモリ部と、メモリ制御用半導体デバイスで構成される記録媒体であれば何でもよい。

【０３１９】

（１２）変形例１２

実施の形態２～３及びこれらの変形例では、暗号化メディア鍵群１８４０が、複数の組を含み、各組は、カードデバイス鍵ＩＤ又は装置デバイス鍵ＩＤと、暗号化メディア鍵とから構成され、カードデバイス鍵ＩＤ又は装置デバイス鍵ＩＤに基づいて、復号すべき暗号化メディア鍵を選択するものとしたがこの構成に限定されない。例えば、暗号化メディア鍵群１８４０は、複数のエントリからなり、各エントリには暗号化メディア鍵が格納されるものとし、カードデバイス鍵ＩＤ又は装置デバイス鍵ＩＤより計算される、上記エントリのアドレス情報に基づき、暗号化メディア鍵群１８４０から、カードデバイス鍵ＩＤ又は装置デバイス鍵ＩＤに対応する暗号化メディア鍵を選択する構成としてもよい。また実施の形態２～３及びこれらの変形例では、暗号化メディア鍵群は、カードデバイス鍵又は、装置デバイス鍵を用いてメディア鍵を暗号化したものとしたがこの構成に限定されない。例えば、カードデバイス鍵又は、装置デバイス鍵に基づいて生成される暗号鍵を用いて、メディア鍵を暗号化することにより構成してもよい。この場合、カードデバイス鍵又は、装置デバイス鍵に基づいて暗号鍵を生成し、生成した暗号鍵を用いて暗号化メディア鍵を復号するものとする。

【０３２０】

また、実施の形態２～３及びこれらの変形例では、メモリカード、又は、記録再生装置に、それぞれ１つのデバイス鍵を格納する構成としたがこの構成に限定されない。例えばメモリカード、又は、記録再生装置に、複数のデバイス鍵からなるデバイス鍵セットを格納し、デバイス鍵セットから１つのデバイス鍵を選択し、選択したデバイス鍵を用いて、暗号化メディア鍵を復号する構成としてもよい。また、暗号化メディア鍵群を、ＤＶＤやＳＤメモリカード向けの著作権保護技術であるＣＰＲＭ、あるいは、Ｂｌｕ－ｒａｙ Ｄｉｓｋ向けの著作権保護技術であるＡＡＣＳで用いられているＭＫＢ（Ｍｅｄｉａ Ｋｅｙ Ｂｌｏｃｋ）の技術を適用して構成するとしてもよい。

【０３２１】

（１３）変形例１３

実施の形態２～３及びこれらの変形例において、暗号化メディア鍵群１８４０に、暗号化メディア鍵群のバージョンを示す情報を含め、記録再生装置において、自身に実装された暗号化メディア鍵群と、メモリカードから読み出した暗号化メディア鍵群のバージョンを比較し、自身に実装された暗号化メディア鍵群のバージョンの方が新しい場合に、自身に実装された暗号化メディア鍵群を用いて、メモリカードの暗号化メディア鍵群を更新する構成を持たせてもよい。また、暗号化メディア鍵群１８４０に、暗号化メディア鍵群のバージョンを示す情報を含め、記録再生装置において、自身に実装された暗号化メディア鍵群と、メモリカードから読み出した暗号化メディア鍵群のバージョンを比較し、自身に

実装された暗号化メディア鍵群のバージョンの方が古い場合に、メモリカードから読み出した暗号化メディア鍵群を用いて、自身の暗号化メディア鍵群を更新する構成を持たせてもよい。

（１４）変形例１４

実施の形態２～３及びこれらの変形例では、メモリカード又は記録再生装置のメディア鍵生成部及びメディア固有鍵生成部において、暗号化メディア鍵群をカードデバイス鍵又は装置デバイス鍵を用いて復号し、得られたメディア鍵とメディアＩＤを用いてメディア固有鍵を生成し、このメディア固有鍵を用いて相互認証する構成としたが、この構成に限定されない。例えば、メモリカード又は記録再生装置において、それぞれ、メディアＩＤに基づいて認証用の鍵を生成、その認証用の鍵を用いて相互認証する構成としてもよい。

（１５）変形例１５

実施の形態２～３及びこれらの変形例では、記録再生装置が、所得したメディアＩＤに基づいてコンテンツ鍵を生成し、コンテンツ鍵に基づいてデジタルコンテンツを暗号化する、又は、コンテンツ鍵に基づいて暗号化されたデジタルコンテンツを復号する構成としたがこの構成に限定されない。例えば、記録再生装置が、１）ランダムにコンテンツ鍵を生成し、２）コンテンツ鍵に基づいて、デジタルコンテンツを暗号化し、３）取得したメディアＩＤに基づいて暗号鍵を生成し、４）この暗号鍵に基づいてコンテンツ鍵を暗号化し、５）暗号化されたデジタルコンテンツと暗号化されたコンテンツ鍵をメモリカードに格納する、又は、５）メモリカードから、暗号化されたデジタルコンテンツと暗号化されたコンテンツ鍵を読み出し、６）取得したメディアＩＤに基づいて暗号鍵を生成し、７）この暗号鍵に基づいて暗号化されたコンテンツ鍵を復号し、８）復号されたコンテンツ鍵に基づいて、暗号化されたデジタルコンテンツを復号する構成としてもよい。

４．その他の変形例

（１）その他の変形例としての記録再生システムについて説明する。

【０３２２】

記録再生システム２３００は、図４５に示すように、記録媒体装置であるメモリカード２１００と、記録再生装置２２００とから構成される。

メモリカード２１００は、耐タンパーモジュールブロック２６１０とメモリ部２１２０を備えている。耐タンパーモジュールブロック２６１０は、耐タンパーモジュールブロック２６１０毎に異なる固有の識別情報を格納している識別情報格納部２６１１と、識別情報格納部２６１１に格納されている前記識別情報に基づいて自己の正当性を証明する証明情報を生成し、生成した証明情報を出力する証明部２６０９とを含む。

【０３２３】

メモリ部２１２０は、暗号化されたデジタルコンテンツを格納するための暗号化コンテンツ格納部２１２２を備えている。

記録再生装置２２００は、メモリカード２１００から前記証明情報を取得し、取得した前記証明情報に基づき、メモリカード２１００の正当性を検証し、検証に失敗した場合に暗号化コンテンツの復号又はコンテンツの暗号化を禁止する検証部２２１１と、検証部２２１１による検証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化してメモリカード２１００の暗号化コンテンツ格納部２１２２に記録し、又は、前記識別情報に基づき、メモリカード２１００の暗号化コンテンツ格納部２１２２から読み出した前記暗号化デジタルコンテンツを復号するコンテンツ暗復号部２２０９とを備える。

【０３２４】

次に、記録再生システム２３００の動作について、図４６に示すフローチャートを用いて説明する。

メモリカード２１００の証明部２６０９は、識別情報格納部２６１１から識別情報を読み出す（ステップＳ２１０１）。メモリカード２１００の証明部２６０９は、読み出した識別情報に基づいて自己の正当性を証明する証明情報を生成する（ステップＳ２１０２）メモリカード２１００の証明部２６０９は、生成した証明情報を記録再生装置２２００へ出力する（ステップＳ２２０３）。

【０３２５】
記録再生装置２２００の検証部２２１１は、メモリカード２１００から証明情報を取得し（ステップＳ２１０３）、取得した前記証明情報に基づき、メモリカード２１００の正当性を検証する（ステップＳ２１０４）。検証に失敗した場合に（ステップＳ２１０４で「失敗」）、暗号化コンテンツの復号又はコンテンツの暗号化を禁止する。検証部２２１１による検証が成功した場合に（ステップＳ２１０４で「成功」）、コンテンツ暗復号部２２０９は、前記識別情報に基づき、デジタルコンテンツを暗号化してメモリカード２１００の暗号化コンテンツ格納部２１２２に記録し、又は、前記識別情報に基づき、メモリカード２１００の暗号化コンテンツ格納部２１２２から読み出した前記暗号化デジタルコンテンツを復号する（ステップＳ２１０５）。

【０３２６】
（２）実施の形態１～３及びこれらの変形例では、ＡＥＳを用いる場合を説明したがこの構成に限定されない。例えば、ＡＥＳに代えて、他の暗号アルゴリズムでもよい。
（３）実施の形態１～３及びこれらの変形例では、デジタルコンテンツの記録及び再生の両方の機能を持つ装置を記録再生装置として説明した。しかし、記録再生装置は、再生機能のみを持つ再生装置及び記録機能のみを持つ記録装置として実現してもよい。

【０３２７】
（４）実施の形態１～３及びこれらの変形例では、記録再生装置は、コンテンツ再生部を備えるとしている。しかし、記録再生装置は、コンテンツ再生部を備えていないとしてもよい。このとき、記録再生装置は、コンテンツ暗復号部により暗号化コンテンツを復号して生成したコンテンツを外部の表示装置へ出力するとしてもよい。

【０３２８】
（５）実施の形態１及び２では、センターがカードメーカーにメディアＩＤ格納モジュール部を提供している。しかし、これには限定されない。
センターから委託されたメディアＩＤ格納モジュールベンダが、メディアＩＤ格納モジュール部を製造し、カードメーカーに提供するとしてもよい。

【０３２９】
この場合に、実施の形態３のコントローラベンダがメディアＩＤ格納モジュールベンダを兼ねるとしてもよい。
また、実施の形態１のメディアＩＤモジュール部６１０と制御部１１０とを一体化して耐タンパー部を製造し、センターから、あるいは、センターから委託されたメディアＩＤ格納モジュールベンダから、あるいは、メディアＩＤ格納モジュールベンダを兼ねるコントローラベンダから、一体化された耐タンパー部を提供してもよい。

【０３３０】
（６）実施の形態３では、所定単位毎に異なるコントローラ鍵を、マスクＲＯＭ等のハードウェアロジックにより実現するとしているが、この構成には限定されない。例えば、コントローラ鍵を、マスクＲＯＭ等のハードウェアロジックにより格納された所定単位毎に異なる固有のパラメータと、電気ヒューズ等により格納されたコントローラ毎に異なる固有のパラメータとにより、個々のコントローラ毎に生成するとしてもよい。

【０３３１】
（７）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。なお、各装置は、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどの全てを含むコンピュータシステムには限らず、これらの一部から構成されているコンピュータシステムであってもよい。

【０３３２】
（８）上記の各装置を構成する構成要素の一部又は全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。
【０３３３】
また、上記の各装置を構成する構成要素の各部は、個別に１チップ化されていてもよいし、一部又は全てを含むように１チップ化されてもよい。
また、ここでは、システムＬＳＩとしたが、集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。
【０３３４】
さらに、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。
【０３３５】
（９）上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしてもよい。前記ＩＣカード又は前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカード又は前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカード又は前記モジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパ性を有するとしてもよい。
【０３３６】
（１０）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。
【０３３７】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ　ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。
【０３３８】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。
【０３３９】
また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは前記コンピュータプログラムにしたがって動作するとしてもよい。
【０３４０】
また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送す

ることにより、独立した他のコンピュータシステムにより実施するとしてもよい。
【０３４１】
（１１）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。
５．その他
（ａ）以上説明したように、本発明の第１の態様に係る記録再生システムは、記録媒体装置と、記録再生装置とから構成される記録再生システムであって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を生成する生成部と、前記識別情報に基づいて前記再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備え、前記記録再生装置は、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証手段と、前記認証手段による認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号手段とを備えることを特徴とする。
【０３４２】
本発明の記録再生システムによれば、記録再生装置の認証手段が、記録媒体装置の耐タンパー化された識別情報格納手段の認証手段との間で、記録媒体装置の耐タンパー化された識別情報格納手段の識別情報生成手段にて生成された識別情報に基づき認証処理を行うそして、認証処理が成功した場合にのみ、前記識別情報に基づきデジタルコンテンツを暗号化して記録媒体装置に記録する、もしくは、記録媒体装置に記録された暗号化されたデジタルコンテンツを読み出し、前記識別情報に基づき、暗号化されたデジタルコンテンツを復号し、再生する。
【０３４３】
そのため、もし、記録媒体装置のメーカーが不正に記録媒体装置の識別情報を複数の記録媒体装置に複製したとしても、その不正な記録媒体装置に識別情報格納手段まで複製しない限り、正当な記録再生装置との間の認証に失敗する。また、識別情報格納手段は耐タンパー化されているため、いかに記録媒体装置のメーカーであってもその内容を解析することはできない。これにより、記録媒体装置のメーカーが不正に識別情報を複製した場合であっても、その記録媒体装置を使って、デジタルコンテンツを暗号化して記録したり、暗号化されたコンテンツを読み出して復号することはできない。すなわち、記録媒体装置のメーカーによる不正行為を防止できるという効果が発揮される。
【０３４４】
本発明の第２の態様に係る記録再生システムは、前記記録媒体装置の認証手段は、前記記録媒体装置のメーカー毎に異なるメーカー秘密鍵を格納するメーカー秘密鍵格納部と、前記記録再生装置の認証手段から乱数を受け取る受信部と、前記乱数と前記識別情報とに対するデジタル署名データを前記メーカー秘密鍵を用いて生成する署名生成部とを備え、前記記録媒体装置は、さらに、信頼できるセンターが、前記メーカー秘密鍵に対応するメーカー公開鍵に対して、前記センターのセンター秘密鍵を用いて発行したメーカー公開鍵証明書を格納する証明書格納手段と、前記メーカー公開鍵証明書を前記記録再生装置に送信する送信手段とを備え、前記記録再生装置の認証手段は、前記乱数を生成し前記記録媒体装置に送る乱数生成部と、前記信頼できるセンターのセンター秘密鍵に対応するセンター公開鍵を格納するセンター公開鍵格納部と、前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する署名検証部と、前記正当性が検証されたメーカー公開鍵を用いて、前記記録媒体から受け取った前記デジタル署名データの正当性を検証することで、前記記録媒体装置との間での認証処理を行う署名検証手段と、を備えることを特徴とする。
【０３４５】
この構成によれば、記録再生装置には、記録媒体装置との間での認証処理を行うために公開の情報であるセンター公開鍵のみを格納すればよく、記録媒体装置に、秘密の情報（記録再生装置に固有の装置デバイス鍵など）を格納する必要がない。そのためため、鍵格

納部の実装が簡単になるという効果を有する。なぜなら、センター公開鍵は、公開された情報であり、不正者に読み出されてもセキュリティ上の問題が生じない情報だからである。そのため、公開の情報であるセンター公開鍵格納部は、書き込みに対して保護する必要があるが読み出しに対して保護する必要がない。一方、秘密の情報である装置デバイス鍵格納部は、書き込みと読み出しの両方に対して保護する必要がある。したがって、保護を簡単にできる分、秘密の情報を使う場合よりも容易に実装することができる。

【０３４６】

本発明の第３の態様に係る記録再生システムは、前記記録媒体装置は、さらに、メディア鍵を複数のデバイス鍵を用いて暗号化して得られる暗号化メディア鍵群を格納する暗号化メディア鍵群格納手段を備え、前記記録媒体装置の認証手段は、前記記録媒体装置毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記記録媒体装置自身のデバイス鍵を用いて、前記暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、前記記録再生装置との間で相互認証を行う相互認証部とを備え、前記記録再生装置は、さらに、前記暗号化メディア鍵群を前記記録媒体装置から読み出す読出手段を備え、前記記録再生装置の認証手段は、前記記録再生装置毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記記録再生装置自身のデバイス鍵を用いて、前記暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、前記記録媒体装置との間で相互認証を行う相互認証部とを備えることを特徴とする。

【０３４７】

この構成によれば、記録再生装置は、記録媒体装置との間での認証処理を行うために、暗号化メディア鍵群の復号を行えばよい。そのため、復号に使うアルゴリズムとしてＡＥＳ暗号等の共通鍵暗号系を用いることができる。一方、デジタル署名を使って認証を行うシステムでは、記録再生装置は、記録媒体装置との間での認証処理（署名検証処理）を行うために、ＲＳＡ暗号などの公開鍵暗号系を用いる必要がある。共通鍵暗号系の実装は公開鍵暗号系の実装よりも簡単な構成になるため、公開鍵暗号系を使う記録再生システムに比較して、認証部の実装が簡単になるという効果を有する。

【０３４８】

本発明の第４の態様に係る記録媒体装置は、記録媒体装置と、記録媒体装置にデジタルコンテンツを記録する、もしくは、記録媒体装置に記録したデジタルコンテンツを読み出して再生する記録再生装置から構成される記録再生システムにおける記録媒体装置であって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を生成する生成部と、前記識別情報に基づいて前記記録再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備えることを特徴とする。

【０３４９】

本発明の第５の態様に係る記録媒体装置は、前記記録媒体装置の認証手段は、前記記録媒体装置のメーカー毎に異なるメーカー秘密鍵を格納するメーカー秘密鍵格納部と、前記記録再生装置の認証手段から乱数を受け取る受信部と、前記メーカー秘密鍵を用いて、前記乱数と前記識別情報とに対するデジタル署名データを生成する署名生成部を備え、前記記録媒体装置は、さらに、信頼できるセンターが、前記メーカー秘密鍵に対応するメーカー公開鍵に対して、前記センターのセンター秘密鍵を用いて発行したメーカー公開鍵証明書を格納する証明書格納手段とを備えることを特徴とする。

【０３５０】

本発明の第６の態様に係る記録媒体装置は、前記記録媒体装置は、さらに、メディア鍵を複数のデバイス鍵を用いて暗号化して得られる暗号化メディア鍵群を格納する暗号化メディア鍵群格納手段を備え、前記記録媒体装置の認証手段は、前記記録媒体装置毎に異なるデバイス鍵を格納するデバイス鍵格部と、前記記録媒体装置自身のデバイス鍵を用いて

前記暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、記録再生装置との間で相互認証を行う相互認証部とを備えることを特徴とする。

【０３５１】

本発明の第７の態様に係る記録再生装置は、記録媒体装置と記録再生装置とから構成される記録再生システムにおける記録再生装置であって、前記記録再生装置は、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証手段と、前記認証手段による認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号手段と、復号されたデジタルコンテンツを再生する再生手段とを備えることを特徴とする。

【０３５２】

本発明の第８の態様に係る記録再生装置は、前記記録再生装置の認証手段は、前記乱数を生成し前記記録媒体装置に送る乱数生成部と、前記信頼できるセンターのセンター秘密鍵に対応するセンター公開鍵を格納するセンター公開鍵格納部と、前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する署名検証部と、前記正当性が検証されたメーカー公開鍵を用いて、前記記録媒体から受け取った前記識別情報と前記乱数に対する署名データの正当性を検証する前記再生装置との間での認証処理を行う署名検証手段とを備えることを特徴とする。

【０３５３】

本発明の第９の態様に係る記録再生装置は、前記記録再生装置は、さらに、メディア鍵を複数のデバイス鍵を用いて暗号化して得られる暗号化メディア鍵群を読み出す読出手段を備え、前記記録再生装置の認証手段は、前記記録再生装置毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記デバイス鍵を用いて、信頼できるセンターが発行した暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、前記記録媒体装置との間で相互認証を行う相互認証部とを備えることを特徴とする。

【０３５４】

本発明の第１０の態様に係る記録再生方法は、記録媒体装置と、記録再生装置とから構成される記録再生システムで用いられる記録再生方法であって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を生成する生成部と、前記識別情報に基づいて前記再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備え、前記記録再生方法は、前記記録再生装置が、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証ステップと、前記記録再生装置が、前記認証ステップによる認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号ステップとを含むことを特徴とする。

【０３５５】

本発明の第１１の態様に係る記録再生プログラムは、記録媒体装置と、記録再生装置とから構成される記録再生システムで用いられる記録再生プログラムであって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を生成する生成部と、前記識別情報に基づいて前記再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段と備え、前記記録再生プログラムは、前記記録再生装置が、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証ステップと、前記記録再生装置が、前記認証ステップによる認証が成功した場合に、前記識別情報に基づき、

デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号ステップとを含むことを特徴とする。

【０３５６】

本発明の第１２の態様に係る記録再生プログラムは、前記記録再生プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする。

本発明の第１３の態様に係る集積回路は、記録媒体装置と、記録媒体装置にデジタルコンテンツを記録する、もしくは、記録媒体装置に記録したデジタルコンテンツを読み出して再生する記録再生装置から構成される記録再生システムにおける記録媒体装置で用いられる集積回路であって、前記集積回路は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を生成する生成部と、前記識別情報に基づいて前記記録再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備えることを特徴とする。

（ｂ）また、以上説明したように、本発明の第１の態様に係る記録再生システムは、記録媒体装置と、記録再生装置とから構成される記録再生システムであって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を格納する格納部と、前記識別情報に基づいて前記再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備え、前記記録再生装置は、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証手段と、前記認証手段による認証が成功した場合に前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号手段とを備えることを特徴とする。

【０３５７】

本発明の記録再生システムによれば、記録再生装置の認証手段が、記録媒体装置の耐タンパー化された識別情報格納手段の認証手段との間で、記録媒体装置の耐タンパー化された識別情報格納手段の識別情報格納手段にて格納された識別情報に基づき認証処理を行うそして、認証処理が成功した場合にのみ、前記識別情報に基づきデジタルコンテンツを暗号化して記録媒体装置に記録する、もしくは、記録媒体装置に記録された暗号化されたデジタルコンテンツを読み出し、前記識別情報に基づき、暗号化されたデジタルコンテンツを復号し、再生する。

【０３５８】

そのため、もし、記録媒体装置のメーカーが不正に記録媒体装置の識別情報を複数の記録媒体装置に複製したとしても、その不正な記録媒体装置に識別情報格納手段まで複製しない限り、正当な記録再生装置との間の認証に失敗する。また、識別情報格納手段は耐タンパー化されているため、いかに記録媒体装置のメーカーであってもその内容を解析することはできない。これにより、記録媒体装置のメーカーが不正に識別情報を複製した場合であっても、その記録媒体装置を使って、デジタルコンテンツを暗号化して記録したり、暗号化されたコンテンツを読み出して復号することはできない。すなわち、記録媒体装置のメーカーによる不正行為を防止できるという効果が発揮される。

【０３５９】

本発明の第２の態様に係る記録再生システムは、前記記録媒体装置は、さらに、前記記録媒体装置毎に異なるデバイス鍵を、前記記録媒体装置毎に異なる、もしくは、所定の記録媒体装置の集合毎に異なるコントローラ鍵で暗号化して得られる暗号化デバイス鍵を格納する暗号化デバイス鍵格納手段と、メディア鍵を複数のデバイス鍵のそれぞれを用いて暗号化して得られる暗号化メディア鍵群を格納する暗号化メディア鍵群格納手段を備え、前記記録媒体装置の認証部は、前記コントローラ鍵を格納するコントローラ鍵格納部と、前記暗号化デバイス鍵を前記コントローラ鍵を用いて復号する復号部と、前記復号部で復号されたデバイス鍵を格納するデバイス鍵格納部と、前記デバイス鍵格納部のデバイス鍵を用いて、前記暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前

記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、前記記録再生装置との間で相互認証を行う相互認証部とを備え、前記記録再生装置は、さらに、前記暗号化メディア鍵群を前記記録媒体装置から読み出す読出手段を備え、前記記録再生装置の認証手段は、前記記録再生装置毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記記録再生装置自身のデバイス鍵を用いて、前記暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と前記メディア固有鍵を用いて、前記記録媒体装置との間で相互認証を行う相互認証部とを備えることを特徴とする。

【０３６０】

この構成によれば、記録再生装置は、記録媒体装置との間での認証処理を行うために、暗号化メディア鍵群の復号を行えばよい。そのため、復号に使うアルゴリズムとしてＡＥＳ暗号等の共通鍵暗号系を用いることができる。一方、デジタル署名を使って認証を行うシステムでは、記録再生装置は、記録媒体装置との間での認証処理（署名検証処理）を行うために、ＲＳＡ暗号などの公開鍵暗号系を用いる必要がある。共通鍵暗号系の実装は公開鍵暗号系の実装よりも簡単な構成になるため、公開鍵暗号系を使う記録再生システムに比較して、認証部の実装が簡単になるという効果を有する。

【０３６１】

本発明の第３の態様に係る記録媒体装置は、記録媒体装置と、記録媒体装置にデジタルコンテンツを記録する、もしくは、記録媒体装置に記録したデジタルコンテンツを読み出して再生する記録再生装置から構成される記録再生システムにおける記録媒体装置であって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を格納する格納部と、前記識別情報に基づいて前記記録再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備えることを特徴とする。

【０３６２】

本発明の第４の態様に係る記録媒体装置は、前記記録媒体装置は、さらに、前記記録媒体装置毎に異なるデバイス鍵を、前記記録媒体装置毎に異なる、もしくは、所定の記録媒体装置の集合毎に異なるコントローラ鍵で暗号化して得られる暗号化デバイス鍵を格納する暗号化デバイス鍵格納手段と、メディア鍵を複数のデバイス鍵のそれぞれを用いて暗号化して得られる暗号化メディア鍵群を格納する暗号化メディア鍵群格納手段を備え、前記記録媒体装置の認証部は、前記コントローラ鍵を格納するコントローラ鍵格納部と、前記暗号化デバイス鍵を前記コントローラ鍵を用いて復号する復号部と、前記復号部で復号されたデバイス鍵を格納するデバイス鍵格部と、前記デバイス鍵格納部のデバイス鍵を用いて、前記暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、記録再生装置との間で相互認証を行う相互認証部とを備えることを特徴とする。

【０３６３】

本発明の第５の態様に係る記録再生装置は、記録媒体装置と記録再生装置とから構成される記録再生システムにおける記録再生装置であって、前記記録再生装置は、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証手段と、前記認証手段による認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号手段と、復号されたデジタルコンテンツを再生する再生手段とを備えることを特徴とする。

【０３６４】

本発明の第６の態様に係る記録再生装置は、前記記録再生装置は、さらに、メディア鍵を複数のデバイス鍵のそれぞれを用いて暗号化して得られる暗号化メディア鍵群を読み出す読出手段を備え、前記記録再生装置の認証手段は、前記記録再生装置毎に異なるデバイ

ス鍵を格納するデバイス鍵格納部と、前記デバイス鍵を用いて、信頼できるセンターが発行した暗号化メディア鍵群を復号しメディア鍵を生成するメディア鍵生成部と前記メディア鍵と、前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、前記メディア固有鍵を用いて、前記記録媒体装置との間で相互認証を行う相互認証部とを備えることを特徴とする。

【０３６５】

本発明の第７の態様に係る記録再生方法は、記録媒体装置と、記録再生装置とから構成される記録再生システムで用いられる記録再生方法であって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を格納する格納部と前記識別情報に基づいて前記再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備え、前記記録再生方法は、前記記録再生装置が、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証ステップと、前記記録再生装置が、前記認証ステップによる認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号ステップとを含むことを特徴とする。

【０３６６】

本発明の第８の態様に係る記録再生プログラムは、記録媒体装置と、記録再生装置とから構成される記録再生システムで用いられる記録再生プログラムであって、前記記録媒体装置は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を格納する格納部と、前記識別情報に基づいて前記再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段と備え、前記記録再生プログラムは、前記記録再生装置が、前記記録媒体装置の識別情報に基づき前記記録媒体装置との間で認証処理を行う認証ステップと、前記記録再生装置が、前記認証ステップによる認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号ステップとを含むことを特徴とする。

【０３６７】

本発明の第９の態様に係る記録再生プログラムは、前記記録再生プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする。

本発明の第１０の態様に係る集積回路は、記録媒体装置と、記録媒体装置にデジタルコンテンツを記録する、もしくは、記録媒体装置に記録したデジタルコンテンツを読み出して再生する記録再生装置から構成される記録再生システムにおける記録媒体装置で用いられる集積回路であって、前記集積回路は、耐タンパー化されており、内部に、前記記録媒体装置毎に固有の識別情報を格納する格納部と、前記識別情報に基づいて前記記録再生装置との間で認証処理を行う認証部とを備えた識別情報格納手段と、暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納手段とを備えることを特徴とする。

（Ｃ）また以上説明したように、本発明の一の実施態様は、記録媒体装置と、記録再生装置とから構成される記録再生システムである。前記記録媒体装置は、識別情報格納手段と暗号化されたデジタルコンテンツを格納する暗号化コンテンツ格納部を備えたメモリ手段と、を備える。前記記録再生装置は、前記記録媒体装置から取得した前記識別情報に基づき前記記録媒体装置との間で認証処理を行う認証部を備えた前記記録媒体装置の検証手段と、前記認証部による認証が成功した場合に、前記識別情報に基づき、デジタルコンテンツを暗号化して前記記録媒体装置の暗号化コンテンツ格納部に記録する、もしくは、前記識別情報に基づき、前記記録媒体装置の暗号化コンテンツ格納部から読み出した前記暗号化デジタルコンテンツを復号して再生するコンテンツ暗復号手段と、を備える。前記識別情報格納手段は、耐タンパー化されており、内部に、識別情報格納手段毎に異なる識別情報を格納する識別情報格納部と、前記識別情報に基づいて前記記録再生装置との間で認証

処理を行う認証部と、を備える。

【０３６８】

ここで、前記記録媒体装置における、前記メモリ手段は、さらに、暗号化デバイス鍵を格納する暗号化デバイス鍵格納部と、暗号化メディア鍵群を格納する暗号化メディア鍵群格納部を備える。前記識別情報格納手段は、半導体デバイスであるコントローラである。前記コントローラは、前記識別情報格納部と前記認証部に加え、コントローラ毎に異なるもしくは、所定のコントローラの集合毎に異なるコントローラ鍵を格納するコントローラ鍵格納部と、前記メモリ手段の暗号化デバイス鍵格納部から取得した前記暗号化デバイス鍵を、前記コントローラ鍵格納部の前記コントローラ鍵を用いて復号する復号部と、前記復号部で復号されたデバイス鍵と、前記メモリ手段の暗号化メディア鍵群格納部の前記暗号化メディア鍵群に基づき、メディア鍵を生成するメディア鍵生成部と、前記メディア鍵生成部で生成された前記メディア鍵と、前記識別情報格納部の識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、を備える。前記記録再生装置における、前記検証手段は、前記認証部に加え、前記記録再生装置毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記デバイス鍵格納部のデバイス鍵と、前記記録媒体装置の前記暗号化メディア鍵群格納部から取得した前記暗号化メディア鍵群に基づき、メディア鍵を生成するメディア鍵生成部と、前記メディア鍵生成部で生成されたメディア鍵と、前記記録媒体装置から取得した前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、を備える。前記暗号化デバイス鍵は、前記記録媒体装置毎に異なるデバイス鍵を前記コントローラ鍵で暗号化したものとする。前記暗号化メディア鍵群は、記録媒体装置のデバイス鍵もしくは記録再生装置のデバイス鍵それぞれを用いて、前記メディア鍵を暗号化したものとする。前記記録媒体装置の認証部と、前記記録再生装置の認証部は、それぞれ、それぞれの前記メディア固有鍵生成部で生成された前記メディア固有鍵を用いて、相互に認証を行うとしてもよい。

【０３６９】

ここで、前記記録媒体装置における、前記メモリ手段は、さらに、暗号化メディア鍵群を格納する暗号化メディア鍵群格納部を備える。前記識別情報格納手段は、前記識別情報格納部と前記認証部に加え、前記識別情報格納手段毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記デバイス鍵格納部のデバイス鍵と、前記メモリ手段の暗号化メディア鍵群格納部の前記暗号化メディア鍵群に基づき、メディア鍵を生成するメディア鍵生成部と、前記メディア鍵生成部で生成された前記メディア鍵と、前記識別情報格納部の識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、を備える。前記記録再生装置は、さらに、前記暗号化メディア鍵群を前記記録媒体装置から読み出す読出手段を備える。前記記録再生装置における、前記検証手段は、前記認証部に加え、前記記録再生装置毎に異なるデバイス鍵を格納するデバイス鍵格納部と、前記デバイス鍵格納部のデバイス鍵と、前記記録媒体装置の前記暗号化メディア鍵群格納部から取得した前記暗号化メディア鍵群に基づき、メディア鍵を生成するメディア鍵生成部と、前記メディア鍵生成部で生成されたメディア鍵と、前記記録媒体装置から取得した前記識別情報に基づき、メディア固有鍵を生成するメディア固有鍵生成部と、を備える。前記暗号化メディア鍵群は記録媒体装置のデバイス鍵もしくは記録再生装置のデバイス鍵それぞれを用いて、前記メディア鍵を暗号化したものとする。前記記録媒体装置の認証部と、前記記録再生装置の認証部は、それぞれ、それぞれの前記メディア固有鍵生成部で生成された前記メディア固有鍵を用いて、相互に認証を行うとしてもよい。

【０３７０】

ここで、前記記録媒体装置の識別情報格納手段は、前記識別情報格納部と前記認証部に加え、前記記録媒体装置のメーカー毎に異なるメーカー秘密鍵を格納するメーカー秘密鍵格納部と、前記記録再生装置の検証手段から乱数を受け取り、前記乱数と前記識別情報格納部の識別情報とに対するデジタル署名データを前記メーカー秘密鍵を用いて生成する署名生成部とを備える。前記記録媒体装置のメモリ手段は、さらに、信頼できるセンターが前記メーカー秘密鍵に対応するメーカー公開鍵に対して、前記センターのセンター秘密鍵

を用いて発行したメーカー公開鍵証明書を格納するメーカー公開鍵証明書格納部を備える前記記録再生装置の検証手段は、さらに、前記乱数を生成し前記記録媒体装置に送る乱数生成部と、前記信頼できるセンターのセンター秘密鍵に対応するセンター公関鍵を格納するセンター公開鍵格納部と、前記センター公開鍵格納部の前記センター公開鍵を用いて、前記記録媒体装置から受け取ったメーカー公開鍵証明書に含まれるメーカー公開鍵の正当性を検証する署名検証部と、前記署名検証部にて、正当性が検証された前記メーカー公開鍵を用いて、前記記録媒体から受け取った前記デジタル署名データの正当性を検証することで、前記記録媒体装置との間での認証処理を行う署名検証部と、を備えるとしてもよい

別の態様は、鍵発行局であるセンターに備えられたコンピュータ及び記憶装置、コントローラベンダに備えられたコンピュータ及び記憶装置及びコントローラの製造装置、記録媒体装置のメーカーに備えられたコンピュータ及び記憶装置及び記録媒体装置の製造装置及び、各コンピュータが接続されたネットワークからなるシステムにおいて、前記記録媒体装置を製造する方法である。この方法は、（ａ）コントローラベンダが、1)製造するコントローラ毎に異なる前記識別情報を生成するステップと、2)コントローラ毎に異なる、もしくは、所定のコントローラの集合毎に異なる前記コントローラ鍵を生成するステップと、3)生成した前記識別情報を、コントローラの前記識別情報格納部に格納するステップと、4)生成した前記コントローラ鍵を、コントローラの前記コントローラ鍵格納部に格納するステップと、5)コントローラベンダを識別する情報であるベンダIDと、前記コントローラ鍵を識別する情報であるコントローラ鍵識別情報と、前記コントローラ鍵とを鍵発行局であるセンターに送付するステップと、（ｂ）前記センターが、6)コントローラベンダから前記ベンダIDと前記コントローラ鍵識別情報と前記コントローラ鍵を受け取るステップと、7)受け取った前記ベンダIDと前記コントローラ鍵識別情報と前記コントローラ鍵を格納手段に格納するステップと、（ｃ）前記記録媒体装置メーカーが、8)コントローラベンダに対して、コントローラの注文情報を送るステップと、（ｄ）前記コントローラベンダが、9)前記記録媒体装置メーカーからコントローラの前記注文情報を受け付けるステップと、10)前記記録媒体装置メーカーに対して、前記コントローラと、コントローラベンダ自身のベンダIDと、前記コントローラに格納されたコントローラ鍵のコントローラ鍵識別情報を、発行するステップと、（ｅ）前記記録媒体装置メーカーが、11)前記コントローラベンダから、前記コントローラと、前記ベンダIDと、前記コントローラ鍵識別情報を受け取るステップと、12)受け取ったコントローラを前記記録媒体装置に実装するステップと、13)センターに対して、コントローラベンダから受け取った前記ベンダIDと、前記コントローラ鍵識別情報とを含むカードデバイス鍵注文情報を送るステップと、（ｆ）センターが、14)前記記録媒体装置メーカーから、前記カードデバイス鍵注文情報を受け付けるステップと、15)前記カードデバイス鍵注文情報に応じたデバイス鍵を生成するステップと、16)前記カードデバイス鍵注文情報に含まれる前記ベンダIDと、前記コントローラ鍵識別情報に対応するコントローラ鍵を前記格納手段より取得し、取得したコントローラ鍵を用いて、生成したデバイス鍵を暗号化して、暗号化コントローラ鍵を生成するステップと、17)メディア鍵を複数の記録媒体装置のデバイス鍵もしくは記録再生装置のデバイス鍵それぞれを用いて暗号化して得られる暗号化メディア鍵群を生成するステップと、18）前記記録媒体装置メーカーに対して、生成した前記暗号化デバイス鍵と、前記暗号化メディア鍵群を、記録媒体装置のメーカーに発行するステップと、（ｇ）前記記録媒体装置のメーカーが、19）前記センターから前記暗号化デバイス鍵と、前記暗号化メディア鍵群を受け取るステップと、20）記録媒体装置のメモリの暗号化カードデバイス鍵格納部、及び、暗号化メディア鍵群格納部に、センターから受け取った前記暗号化カードデバイス鍵と暗号化メディア鍵群を格納するステップとを含む。

【産業上の利用可能性】

【０３７１】

本発明に係る記録再生システムは、カードメーカーが不正なメモリカードを製造したとしても、不正なメモリカードか、正規のメモリカードかを判別し、正規のメモリカードにのみに、デジタル放送又はデジタル配信されるデジタルコンテンツの著作権を保護しつつ

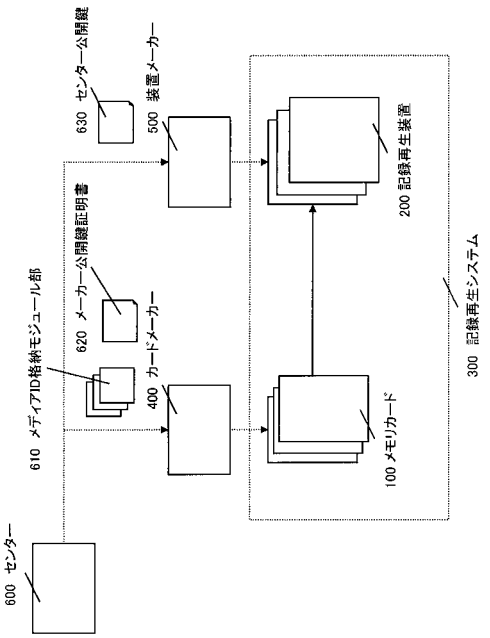
記録し、また、記録したデジタルコンテンツを再生する機能を有し、デジタル放送され、又はデジタル配信されるデジタルコンテンツの記録再生システムとして有用である。

【符号の説明】

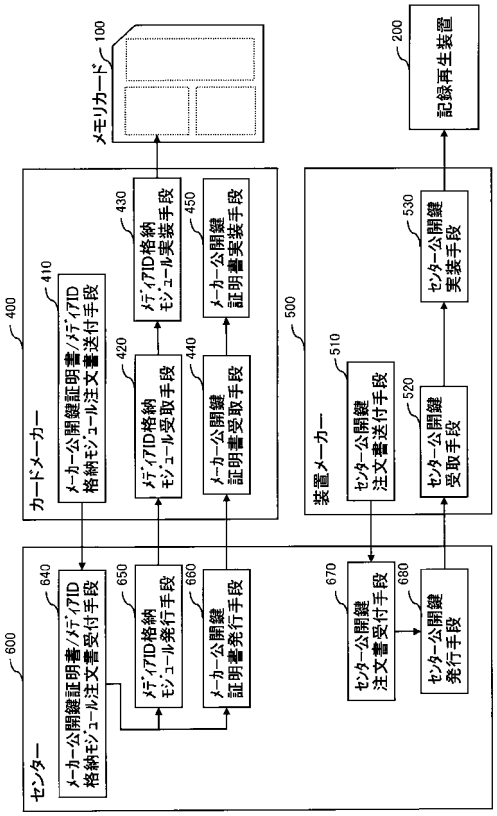
【０３７２】

１００　メモリカード
１００ａ　メモリカード
１００ｃ　メモリカード
３００　記録再生システム
３００ａ　記録再生システム
３００ｃ　記録再生システム
４００　カードメーカー
４００ａ　カードメーカー
５００　装置メーカー
５００ａ　装置メーカー
６００　センター
６００ａ　センター
６００ｃ　センター
１１００　メモリカード
１２００　記録再生装置
１３００　記録再生システム
１４００　カードメーカー
１５００　装置メーカー
１６００　センター
１７００　コントローラベンダ
２１００　メモリカード
２２００　記録再生装置
２３００　記録再生システム

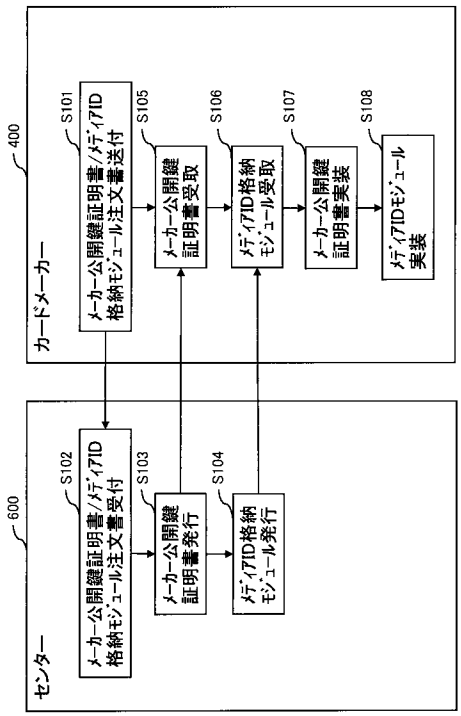
【図１】


600 センター
610 メディアID格納モジュール部
620 メーカー公開鍵証明書
400 カードメーカー
630 センター公開鍵
500 装置メーカー
100 メモリカード
200 記録再生装置
300 記録再生システム

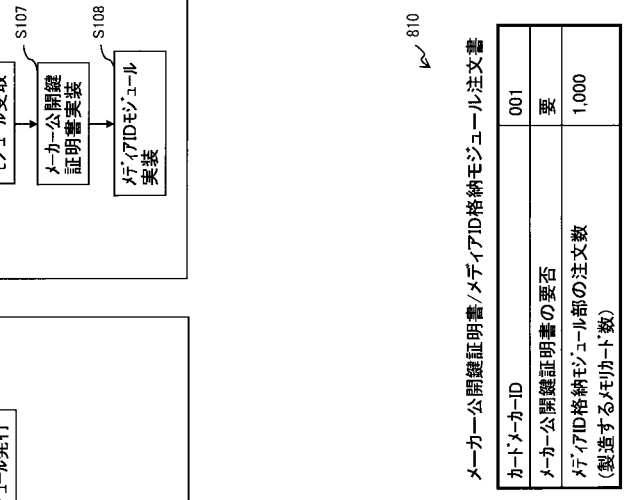
【図２】


メモリカード 100
200 記録再生装置
400 カードメーカー
410 メーカー公開鍵証明書/メディアID格納モジュール注文書送付手段
420 メディアID格納モジュール受取手段
430 メディアID格納モジュール実装手段
440 メーカー公開鍵証明書受取手段
450 メーカー公開鍵証明書実装手段
500 装置メーカー
510 センター公開鍵注文書送付手段
520 センター公開鍵受取手段
530 センター公開鍵実装手段
600 センター
640 メーカー公開鍵証明書/メディアID格納モジュール注文書受付手段
650 メディアID格納モジュール発行手段
660 メーカー公開鍵証明書発行手段
670 センター公開鍵注文書受付手段
680 センター公開鍵発行手段

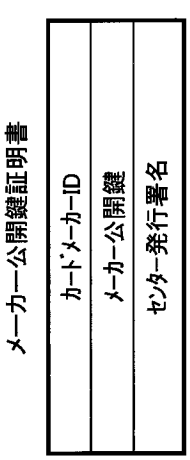
【図３】


400 カードメーカー
600 センター
S101 メーカー公開鍵証明書/メディアID格納モジュール注文書送付
S102 メーカー公開鍵証明書/メディアID格納モジュール注文書受付
S103 メーカー公開鍵証明書発行
S104 メディアID格納モジュール発行
S105 メーカー公開鍵証明書受取
S106 メディアID格納モジュール受取
S107 メーカー公開鍵証明書実装
S108 メディアIDモジュール実装

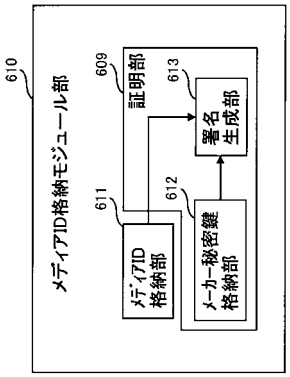
【図４】


810
メーカー公開鍵証明書/メディアID格納モジュール注文書
カードメーカーID 001
メーカー公開鍵証明書の要否 要
メディアID格納モジュール部の注文数（製造するメモリカード数） 1,000

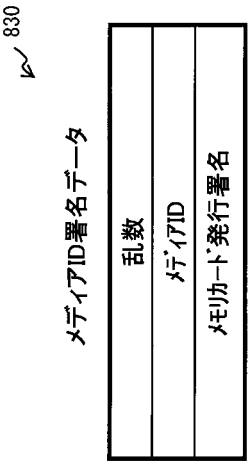
【図５】


820
メーカー公開鍵証明書
カードメーカーID
メーカー公開鍵
センター発行署名

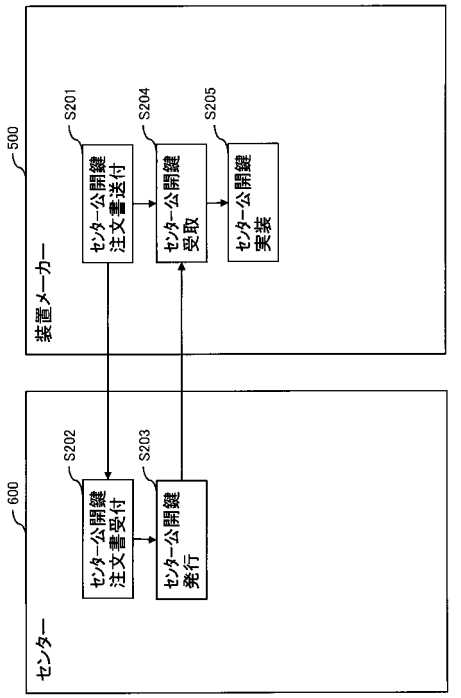
【図６】


610
メディアID格納モジュール部
609
証明部
613
署名生成部
611
メディアID格納部
612
メーカー秘密鍵格納部

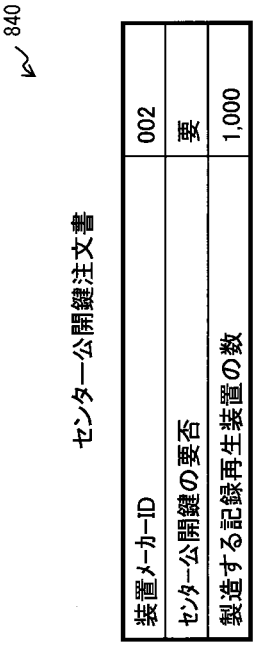
【図７】


830
メディアID署名データ
乱数
メディアID
メモリカード発行署名

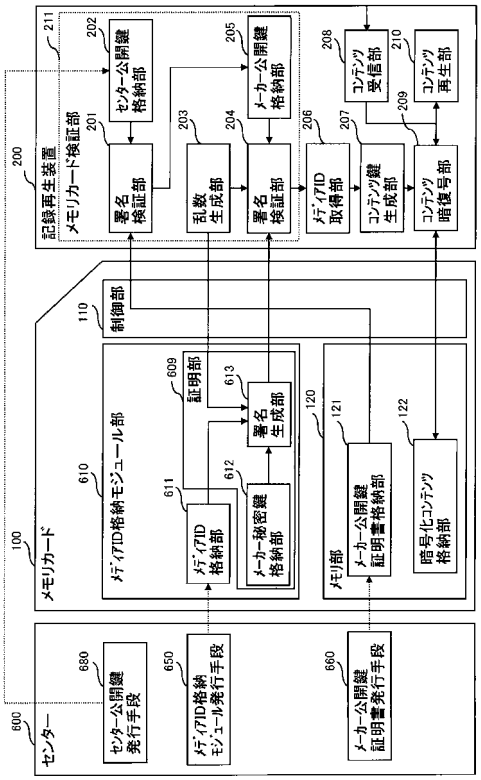
【図８】


500
装置メーカー
S201
センター公開鍵注文書送付
S204
センター公開鍵受取
S205
センター公開鍵実装
600
センター
S202
センター公開鍵注文書受付
S203
センター公開鍵発行

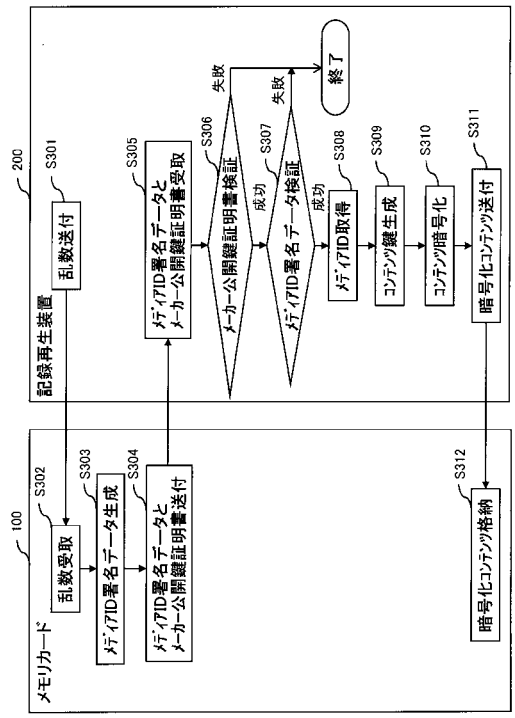
【図９】



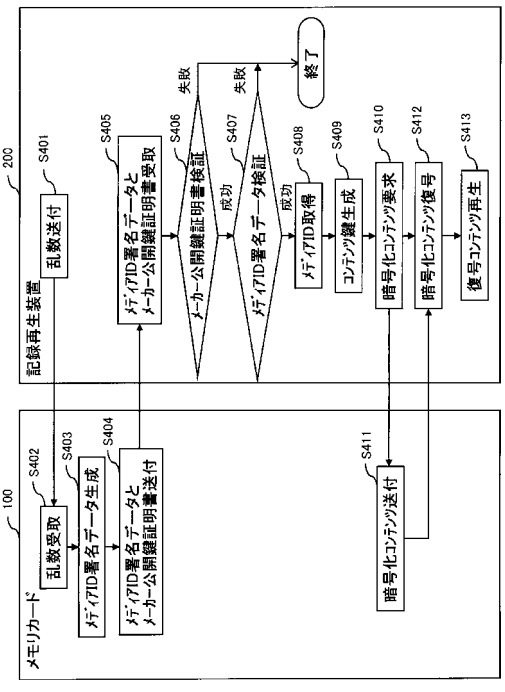
【図１０】



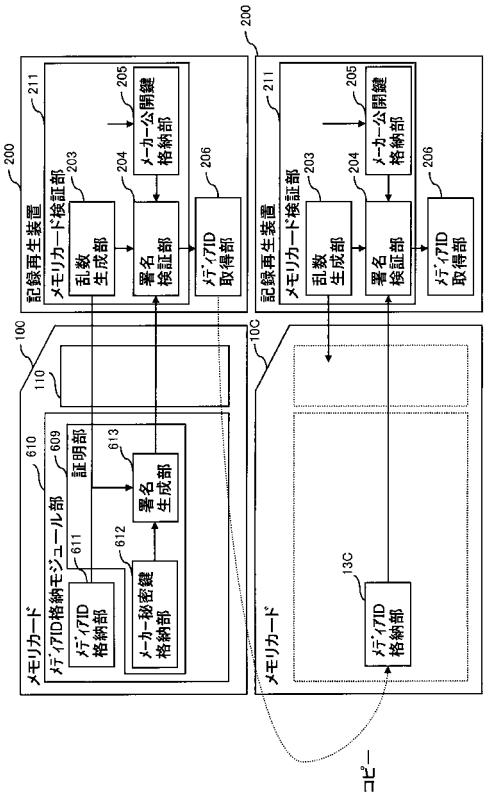
【図１１】



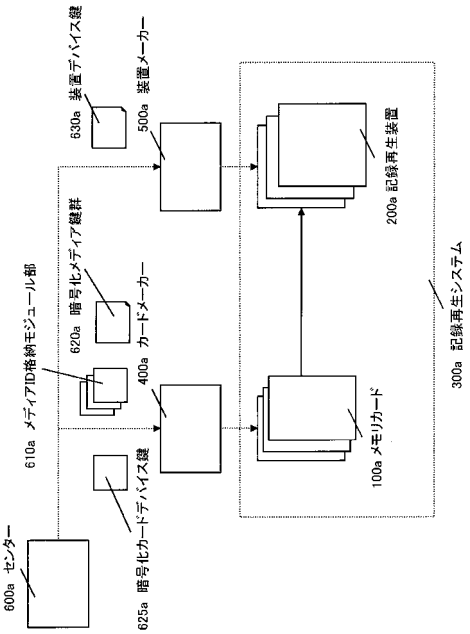
【図１２】



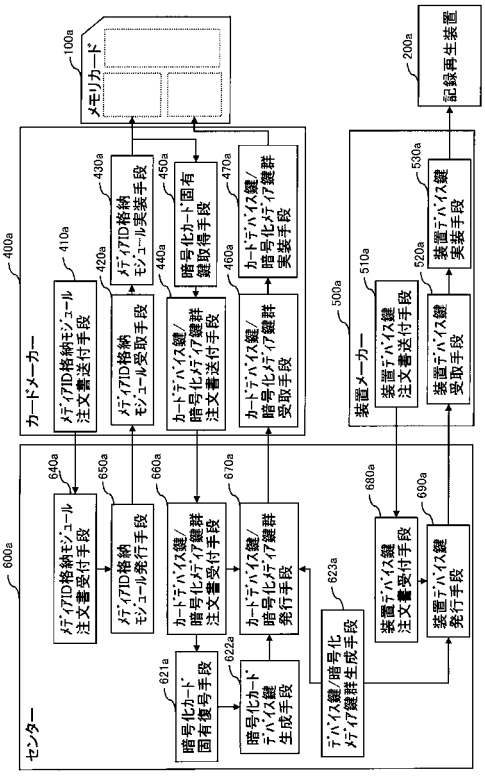
【図１３】



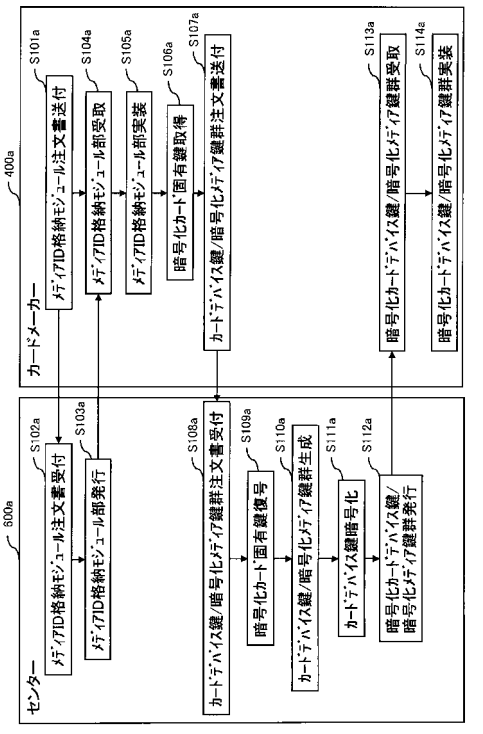
【図１４】



【図１５】



【図１６】



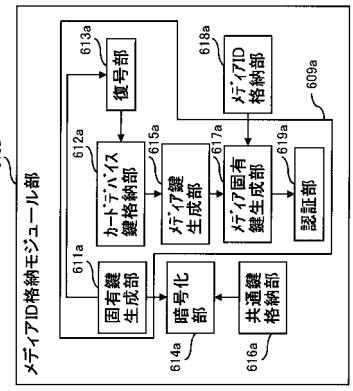
【図１７】

850

メディアID格納モジュール注文書

ｶｰﾄﾞﾒｰｶｰID	001
ﾒﾃﾞｨｱID格納ﾓｼﾞｭｰﾙ部の注文数 (製造するﾒﾓﾘｶｰﾄﾞ数)	1,000

【図１８】



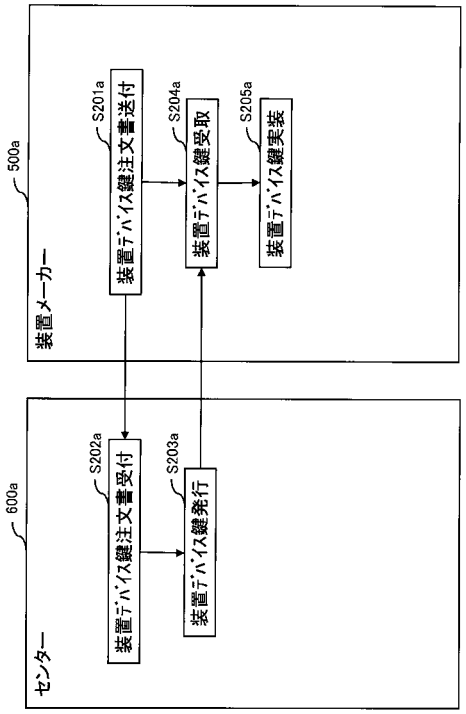
【図１９】

860

暗号化メディア鍵群

ｶｰﾄﾞﾃﾞﾊﾞｲｽ鍵ID=1	AES_E(ｶｰﾄﾞﾃﾞﾊﾞｲｽ鍵1、ﾒﾃﾞｨｱ鍵)
ｶｰﾄﾞﾃﾞﾊﾞｲｽ鍵ID=2	AES_E(ｶｰﾄﾞﾃﾞﾊﾞｲｽ鍵2、ﾒﾃﾞｨｱ鍵)
ｶｰﾄﾞﾃﾞﾊﾞｲｽ鍵ID=N	AES_E(ｶｰﾄﾞﾃﾞﾊﾞｲｽ鍵N、ﾒﾃﾞｨｱ鍵)
装置ﾃﾞﾊﾞｲｽ鍵ID=1	AES_E(装置ﾃﾞﾊﾞｲｽ鍵1、ﾒﾃﾞｨｱ鍵)
装置ﾃﾞﾊﾞｲｽ鍵ID=2	AES_E(装置ﾃﾞﾊﾞｲｽ鍵2、ﾒﾃﾞｨｱ鍵)
装置ﾃﾞﾊﾞｲｽ鍵ID=M	AES_E(装置ﾃﾞﾊﾞｲｽ鍵M、ﾒﾃﾞｨｱ鍵)

【図２０】



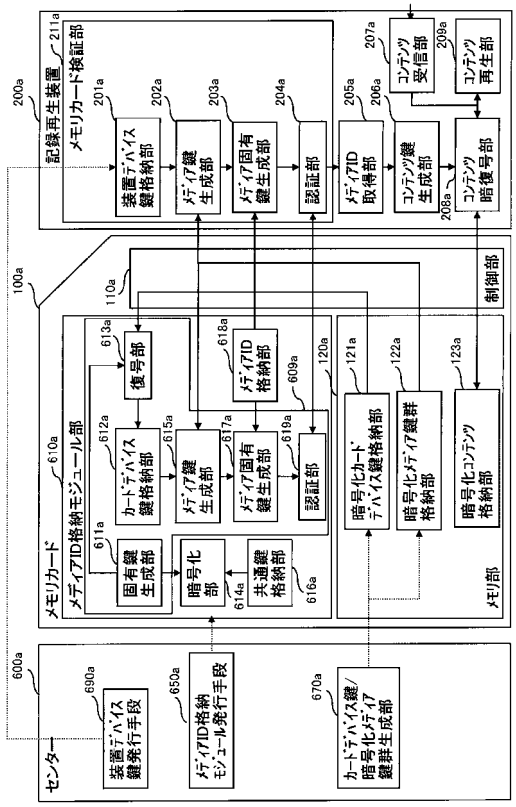
【図２１】

870

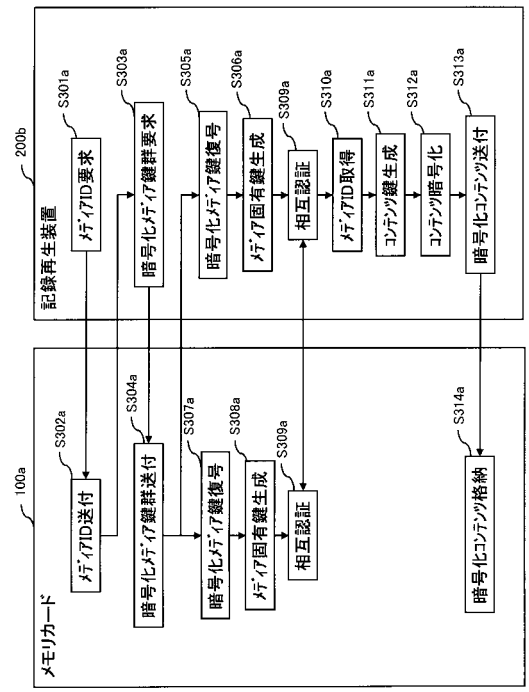
装置デバイス鍵注文書

装置メーカーID	002
装置デバイス鍵の注文数 (製造する記録再生装置の数)	1,000
暗号化メディア鍵群の要否	要

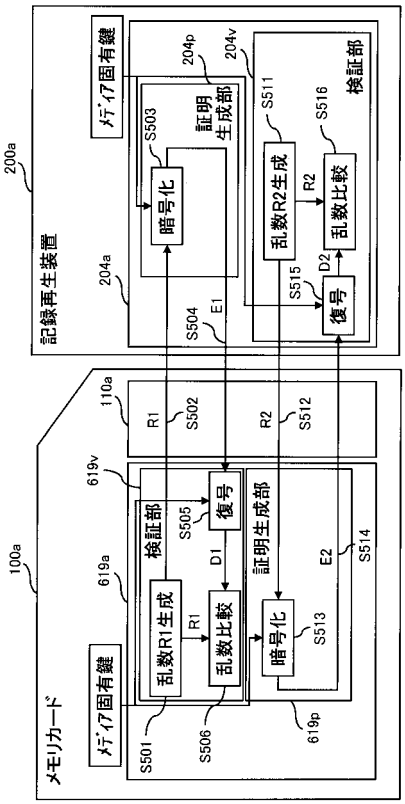
【図２２】



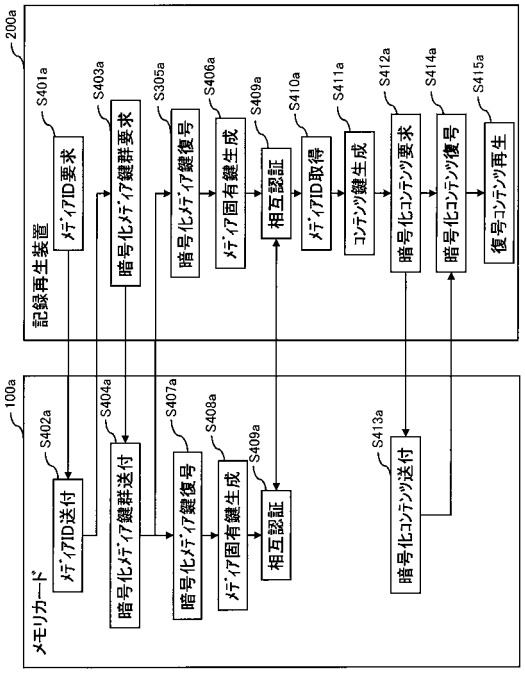
【図２３】



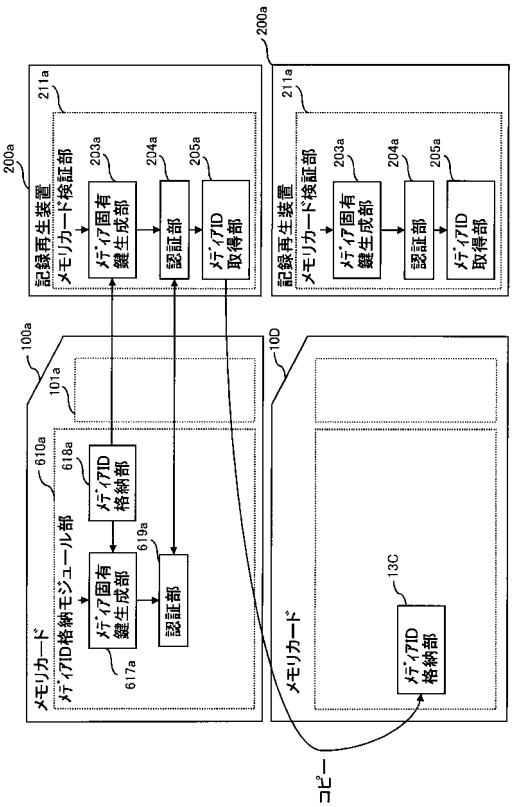
【図２４】



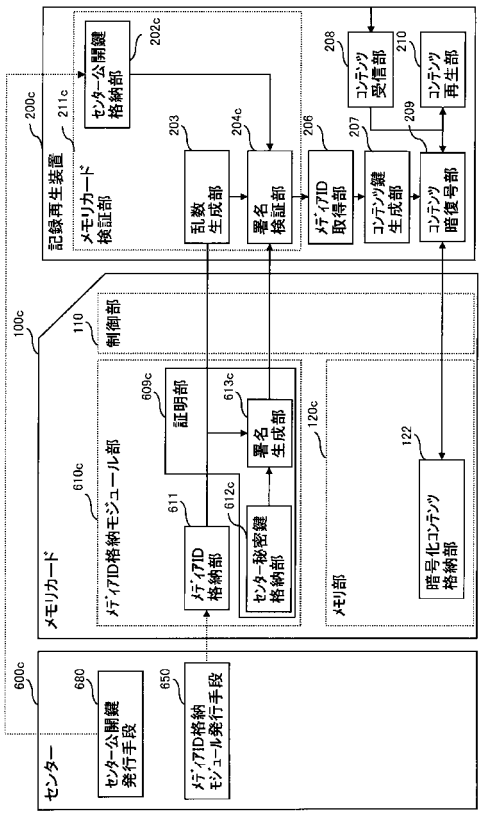
【図２５】



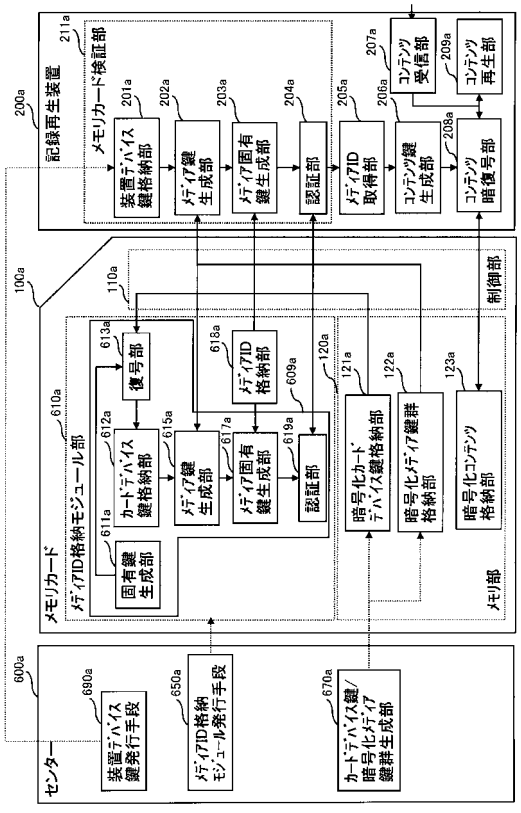
【図２６】



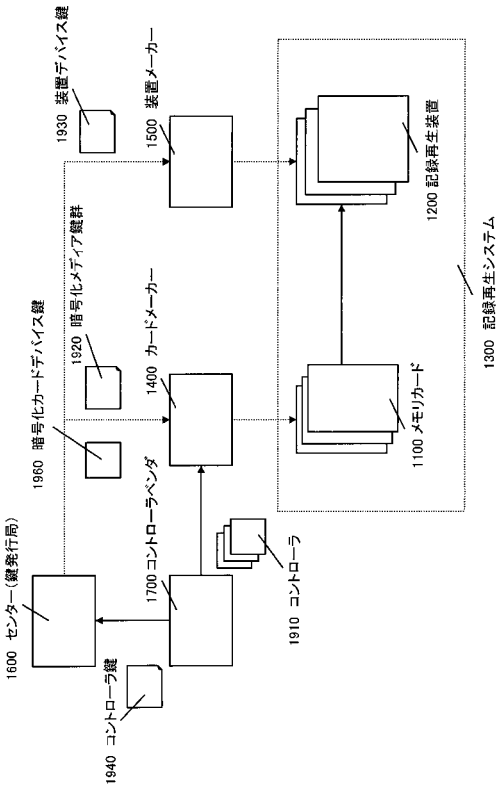
【図２７】



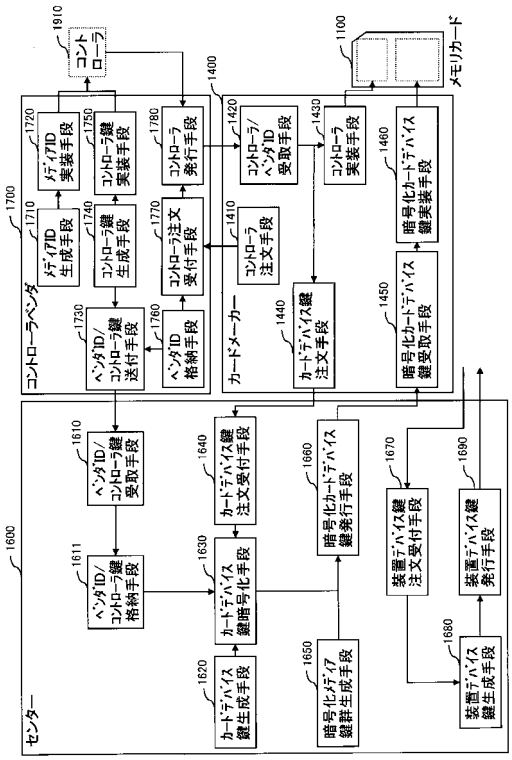
【図２８】



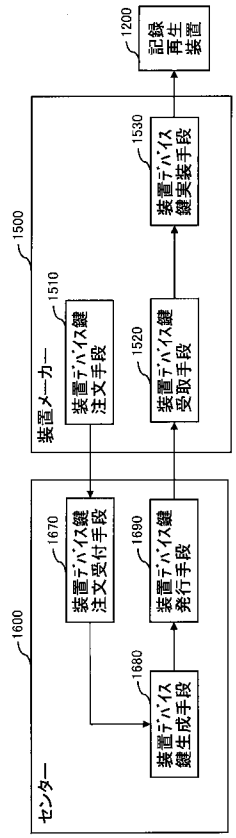
【図２９】



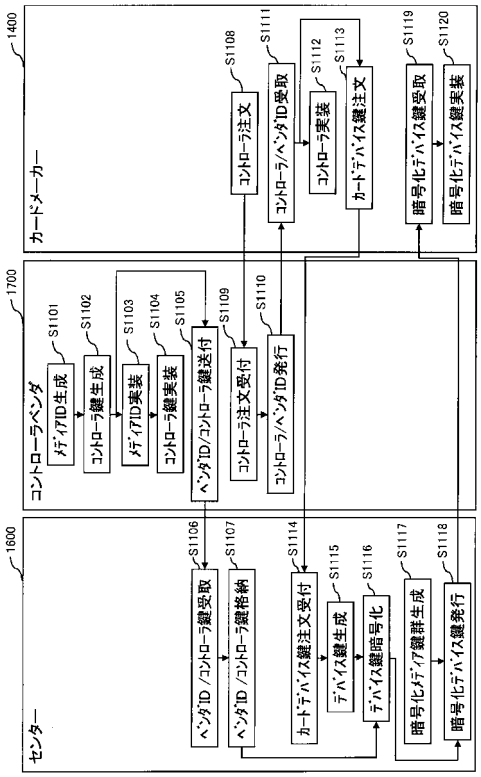
【図３０】



【図３１】



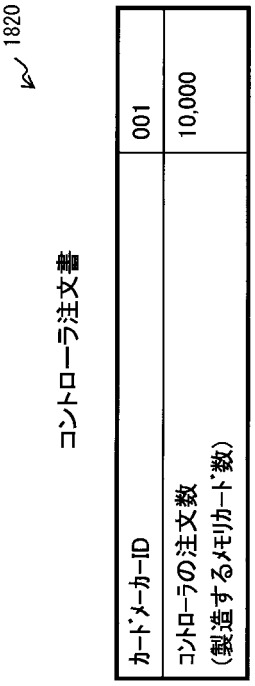
【図３２】



【図３３】

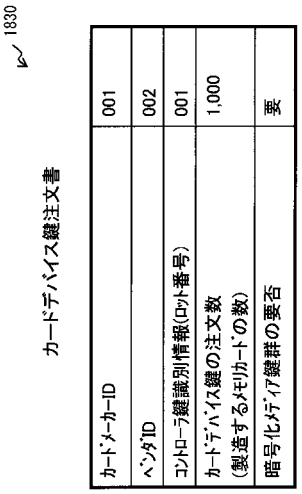
ベンダID	コントローラ鍵識別情報（ロット番号）	コントローラ鍵
001	003	Kc001-003
002	001	Kc002-001
	002	Kc002-002
003	001	Kc003-001

【図３４】



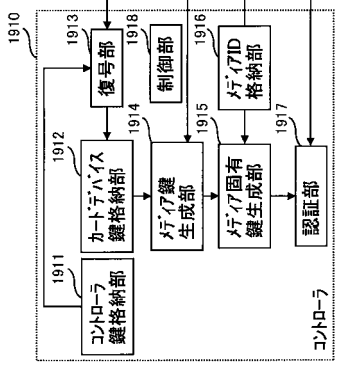
カードメーカーID	001
コントローラの注文数（製造するメモリカード数）	10,000

【図３５】

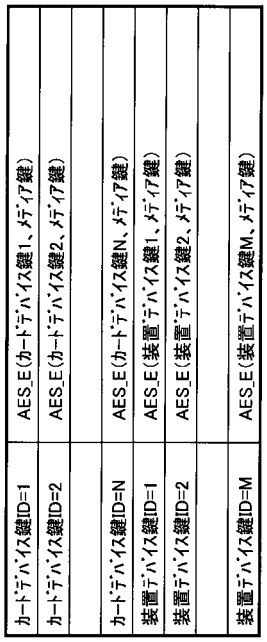


カードメーカーID	001
ベンダID	002
コントローラ鍵識別情報(ロット番号)	001
カードデバイス鍵の注文数（製造するメモリカードの数）	1,000
暗号化メディア鍵群の要否	要

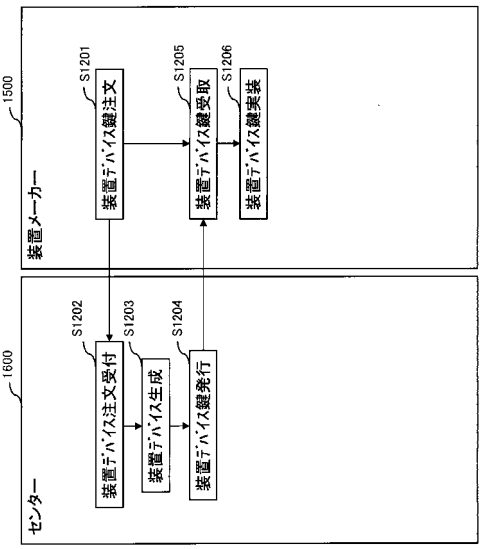
【図３６】



【図３７】



【図３８】



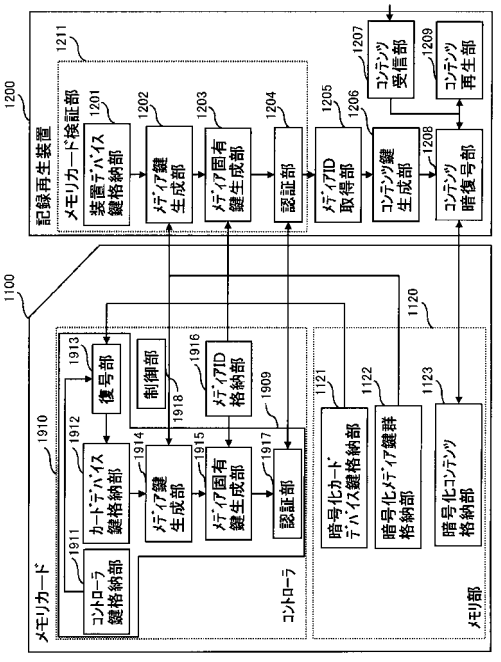
【図３９】

1850

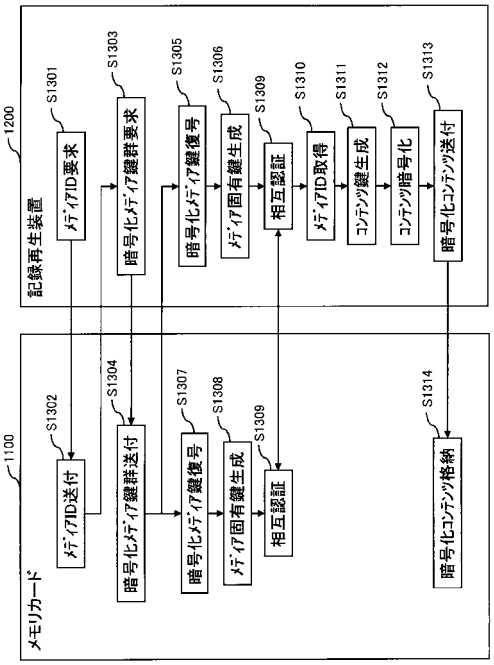
装置デバイス鍵注文書

装置メーカーID	002
装置デバイス鍵の注文数 （製造する記録再生装置の数）	1,000
暗号化メディア鍵群の要否	要

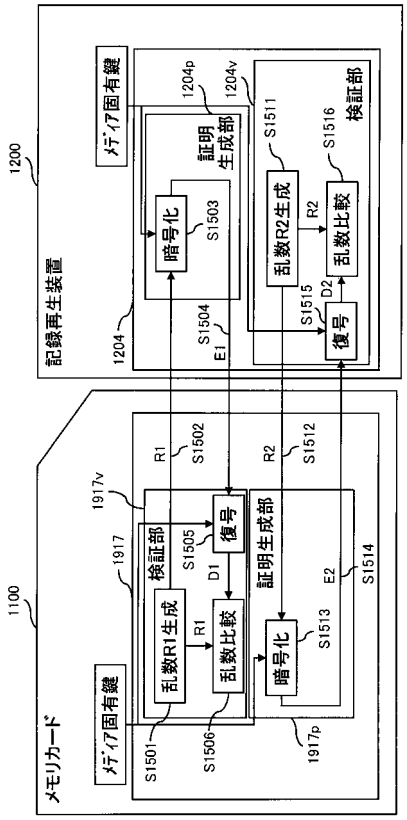
【図４０】



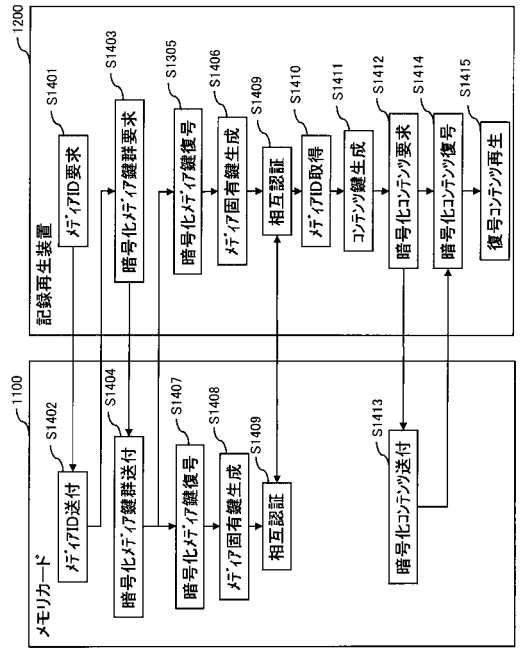
【図４１】



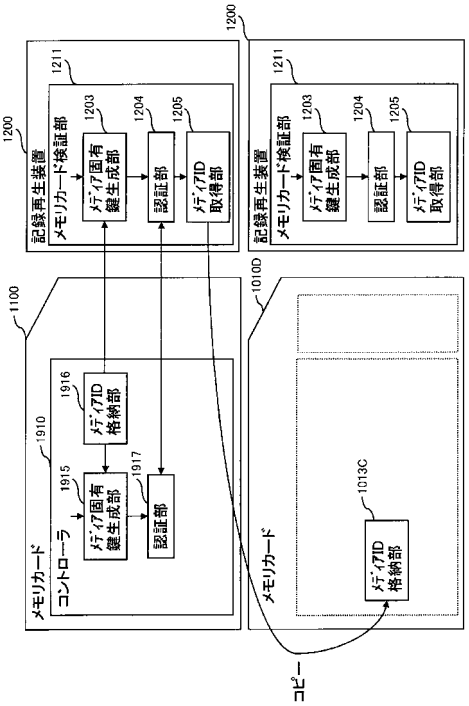
【図４２】



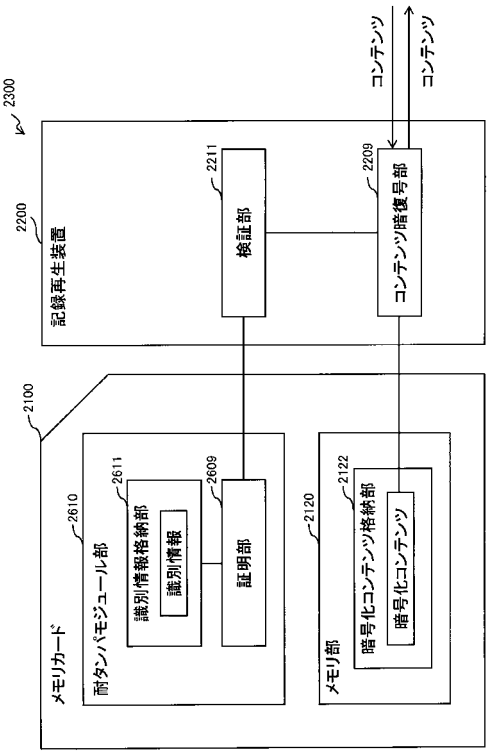
【図４３】



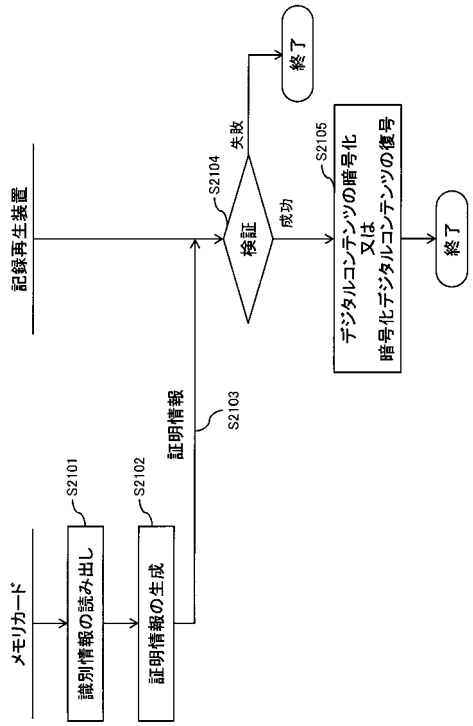
【図４４】



【図４５】



【図４６】



【図４７】

855

カードデバイス鍵／暗号化メディア鍵群注文書

カードメーカーID	001
カードデバイス鍵の注文数 （製造するメモリカードの数）	1,000
暗号化メディア鍵群の要否	要

フロントページの続き

(72)発明者　山本　雅哉
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　永田　峰久
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　山口　高弘
大阪府門真市大字門真１００６番地　パナソニック株式会社内

審査官　岸野　徹

(56)参考文献　特開２００５－１２２４０２（ＪＰ，Ａ）
特開２００４－２７２８９３（ＪＰ，Ａ）
特開２０００－１９６５８８（ＪＰ，Ａ）
特開２００１－１１９３９０（ＪＰ，Ａ）
特開２００１－２３０７６８（ＪＰ，Ａ）
特開平０７－１３５６８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／３４
Ｇ０６Ｆ　２１／４４