

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4638160号  
(P4638160)

(45) 発行日 平成23年2月23日(2011.2.23)

(24) 登録日 平成22年12月3日(2010.12.3)

(51) Int. Cl.		F I			
<b>H04L</b>	<b>9/08</b>	<b>(2006.01)</b>	<b>H04L</b>	9/00	<b>601B</b>
<b>G06F</b>	<b>21/24</b>	<b>(2006.01)</b>	<b>G06F</b>	12/14	<b>520F</b>
<b>G11B</b>	<b>20/10</b>	<b>(2006.01)</b>	<b>G06F</b>	12/14	<b>520P</b>
			<b>G11B</b>	20/10	<b>H</b>

請求項の数 9 (全 57 頁)

(21) 出願番号	特願2004-66181 (P2004-66181)	(73) 特許権者	000005821
(22) 出願日	平成16年3月9日(2004.3.9)		パナソニック株式会社
(65) 公開番号	特開2005-20703 (P2005-20703A)		大阪府門真市大字門真1006番地
(43) 公開日	平成17年1月20日(2005.1.20)	(74) 代理人	100090446
審査請求日	平成19年2月16日(2007.2.16)		弁理士 中島 司朗
(31) 優先権主張番号	特願2003-65591 (P2003-65591)	(72) 発明者	中野 稔久
(32) 優先日	平成15年3月11日(2003.3.11)		大阪府門真市大字門真1006番地 松下
(33) 優先権主張国	日本国(JP)		電器産業株式会社内
(31) 優先権主張番号	特願2003-158927 (P2003-158927)	(72) 発明者	山道 将人
(32) 優先日	平成15年6月4日(2003.6.4)		大阪府門真市大字門真1006番地 松下
(33) 優先権主張国	日本国(JP)		電器産業株式会社内
		(72) 発明者	布田 裕一
			大阪府門真市大字門真1006番地 松下
			電器産業株式会社内

最終頁に続く

(54) 【発明の名称】 著作物保護システム、記録装置、再生装置及び記録媒体

(57) 【特許請求の範囲】

【請求項1】

記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置であって、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記記録装置は、

無効化されていない複数の再生装置の各々について、メディア鍵が、当該再生装置に割り当てられたデバイス鍵に基づいて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、

前記コンテンツを前記記録媒体に書き込む際に、前記メディア鍵データが、前記記録媒体に存在するか否かを確認する存否確認手段と、

コンテンツ鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化手段と、

前記記憶手段に記憶されているメディア鍵データから得られるメディア鍵に基づき前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する鍵暗号化手段と、

前記暗号化コンテンツと前記暗号化コンテンツ鍵とを前記記録媒体の前記書換可能領域に書き込み、前記存否確認手段が前記記録媒体に前記メディア鍵データが存在しないことを確認した場合に、前記記憶手段が記憶するメディア鍵データを前記記録媒体の前記書換

可能領域に書き込む書込手段と  
を備えることを特徴とする記録装置。

【請求項 2】

別の記録媒体は、無効化されていない各再生装置についてメディア鍵が、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶しており、

前記記録装置は、さらに、

前記別の記録媒体に記憶されている別のメディア鍵データと、前記記憶手段に記憶されている前記メディア鍵データとの新旧を比較する比較手段と、

前記別のメディア鍵データの方が新しいと判断される場合に、前記別の記録媒体から前記別のメディア鍵データを読み出し、読み出した前記別のメディア鍵データを、前記記憶手段に記憶されている前記メディア鍵データに、上書きする更新手段と

を備えることを特徴とする請求項 1 に記載の記録装置。

【請求項 3】

前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データの世代を示す第 1 バージョン情報を含み、

前記別の記録媒体に記録されている前記別のメディア鍵データは、当該別のメディア鍵データの世代を示す第 2 バージョン情報を含み、

前記比較手段は、前記第 1 バージョン情報と前記第 2 バージョン情報とを比較することにより、前記記憶手段に記憶されているメディア鍵データと前記別の記録媒体に記録されている別のメディア鍵データとの新旧を比較する

ことを特徴とする請求項 2 に記載の記録装置。

【請求項 4】

前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データが生成された日時を示す第 1 日時情報を含み、

前記別の記録媒体に記録されている前記別のメディア鍵データは、当該別のメディア鍵データが生成された日時を示す第 2 日時情報を含み、

前記比較手段は、前記第 1 日時情報と前記第 2 日時情報とを比較することにより、前記記憶手段に記憶されているメディア鍵データと前記別の記録媒体に記録されている別のメディア鍵データとの新旧を比較する

ことを特徴とする請求項 2 に記載の記録装置。

【請求項 5】

前記記憶手段に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別する第 1 データ識別子を含み、

前記書込手段は、前記第 1 データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記第 1 データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込む

ことを特徴とする請求項 1 に記載の記録装置。

【請求項 6】

記録媒体にコンテンツを暗号化して書き込み、無効化されていない複数の再生装置の各々について、メディア鍵が、当該再生装置に割り当てられたデバイス鍵に基づいて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶する記憶手段を有する記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置で用いられる記録方法であって、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記記録方法は、

前記コンテンツを前記記録媒体に書き込む際に、前記メディア鍵データが、前記記録媒体に存在するか否かを確認する存否確認ステップと、

10

20

30

40

50

コンテンツ鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化ステップと、

前記記憶手段に記憶されているメディア鍵データから得られるメディア鍵に基づき前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する鍵暗号化ステップと、

前記暗号化コンテンツと前記暗号化コンテンツ鍵とを前記記録媒体の前記書換可能領域に書き込み、前記存否確認手段が前記記録媒体に前記メディア鍵データが存在しないことを確認した場合に、前記記憶手段が記憶するメディア鍵データを前記記録媒体の前記書換可能領域に書き込む書込ステップと

を有することを特徴とする記録方法。

【請求項 7】

記録媒体にコンテンツを暗号化して書き込み、無効化されていない複数の再生装置の各々について、メディア鍵が、当該再生装置に固有のデバイス鍵に基づいて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶する記憶手段を有する記録装置で用いられる記録用のコンピュータプログラムであって、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

コンピュータに、

前記コンテンツを前記記録媒体に書き込む際に、前記メディア鍵データが、前記コンテンツ記録媒体に存在するか否かを確認する存否確認ステップと、

コンテンツ鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化ステップと、

前記記憶手段に記憶されているメディア鍵データから得られるメディア鍵に基づき前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する鍵暗号化ステップと、

前記暗号化コンテンツと前記暗号化コンテンツ鍵とを前記コンテンツ記録媒体の前記書換可能領域に書き込み、前記存否確認手段が前記コンテンツ記録媒体に前記メディア鍵データが存在しないことを確認した場合に、前記記憶手段が記憶するメディア鍵データを前記コンテンツ記録媒体の前記書換可能領域に書き込む書込ステップと

を実行させるためのコンピュータプログラム。

【請求項 8】

コンテンツ記録媒体にコンテンツを暗号化して書き込み、無効化されていない複数の再生装置の各々について、メディア鍵が、当該再生装置に固有のデバイス鍵に基づいて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶する記憶手段を有する記録装置で用いられる記録用のコンピュータプログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、

前記コンテンツ記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

コンピュータに、

前記コンテンツを前記記録媒体に書き込む際に、前記メディア鍵データが、前記コンテンツ記録媒体に存在するか否かを確認する存否確認ステップと、

コンテンツ鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化ステップと、

前記記憶手段に記憶されているメディア鍵データから得られるメディア鍵に基づき前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する鍵暗号化ステップと、

前記暗号化コンテンツと前記暗号化コンテンツ鍵とを前記コンテンツ記録媒体の前記書換可能領域に書き込み、前記存否確認手段が前記コンテンツ記録媒体に前記メディア鍵データが存在しないことを確認した場合に、前記記憶手段が記憶するメディア鍵データを前記コンテンツ記録媒体の前記書換可能領域に書き込む書込ステップと

を実行させるためのコンピュータプログラムを記録しているプログラム記録媒体。

【請求項 9】

記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されてい

10

20

30

40

50

る暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムであって、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記書換可能領域は、メディア鍵データと暗号化コンテンツとが記録される領域であり、

前記メディア鍵データは、無効化されていない複数の再生装置の各々について、メディア鍵が、当該再生装置に割り当てられたデバイス鍵に基づいて、暗号化されて生成された複数の暗号化メディア鍵から構成され、

前記暗号化コンテンツは、コンテンツ鍵に基づいて、デジタルデータであるコンテンツを暗号化して生成したものであり、

前記記録装置は、

無効化されていない複数の再生装置の各々について、メディア鍵が、当該再生装置に割り当てられたデバイス鍵に基づいて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、

前記コンテンツを前記記録媒体に書き込む際に、前記メディア鍵データが、前記記録媒体に存在するか否かを確認する存否確認手段と、

コンテンツ鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化手段と、

前記記憶手段に記憶されているメディア鍵データから得られるメディア鍵に基づき前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成する鍵暗号化手段と、

前記暗号化コンテンツと前記暗号化コンテンツ鍵とを前記記録媒体の前記書換可能領域に書き込み、前記存否確認手段が前記記録媒体に前記メディア鍵データが存在しないことを確認した場合に、前記記憶手段が記憶するメディア鍵データを前記記録媒体の前記書換可能領域に書き込む書込手段と

を備え、

前記再生装置は、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データ、又はその一部を読み出す読出手段と、

当該再生装置に割り当てられたデバイス鍵を用いて、読み出された前記メディア鍵データ、又はその一部を復号して復号メディア鍵を生成する復号手段と、

前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備えることを特徴とする著作権保護システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、デジタルデータを大容量の記録媒体に記録し再生する技術に関し、特に不正装置によるコンテンツの不正な記録及び不正な再生を防止する技術に関する。

【背景技術】

【0002】

近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布し、又はネットワークを介して配布するシステムが普及しつつある。

配布されたコンテンツは、コンピュータや再生装置等で読み出され、再生、又は複製の対象となる。

【0003】

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーなどの不正利用を防止するために暗号化技術が用いられる。具体的には、記録装置は、

10

20

30

40

50

コンテンツを暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する再生装置のみが、記録媒体から読み出した暗号化コンテンツをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる。

【0004】

なお、コンテンツを暗号化して記録媒体に記録する際には、再生装置が保有する復号鍵に対応する暗号化鍵を用いて、コンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、再生装置が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等が用いられる。

このとき、再生装置が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による当該再生装置内部の不正な解析により、復号鍵が外部に暴露される危険性がある。復号鍵が一旦不正者により暴露されてしまうと、前記不正者は、コンテンツを不正利用する記録装置、再生装置を製造して不法に販売したり、又はコンテンツを不正利用するためのコンピュータプログラムを作成し、インターネット等によりこのようなプログラムを流布することが考えられる。

【0005】

このような場合、著作権者は一旦暴露された復号鍵では、次から提供するコンテンツを扱えないようにしたいと考える。このようなことを実現する技術を鍵無効化技術と呼び、特許文献1により鍵無効化を実現するシステムが開示されている。

従来の鍵無効化技術では、予め、記録媒体の書き換え不可領域に、装置の保有する鍵が無効化されていることを示す鍵無効化情報を記録している。装置は、記録媒体に記録されている鍵無効化情報を用いて、当該装置の保有する鍵が無効化されているか否かを判断し、無効化された鍵を保有する場合には、当該装置は、前記記録媒体を利用することができないようにしている。また、新たに鍵の無効化が発生すると、前記の鍵無効化情報は更新され、この無効化発生以降に製造される新たな記録媒体には更新後の鍵無効化情報が記録される。こうして無効化された鍵では新たな記録媒体を利用できない仕組みとなっている。

【0006】

一方、光ディスク等の記録媒体に記録されているコンテンツの読み出し、あるいは書き込みは、光ディスクドライブと称されるパソコン周辺機器で行われることが一般的であるが、機器の互換性を達成するためにその入出力の方法は公開の情報として標準化され、秘密にされないことが一般的である。このため、記録媒体に記録されているコンテンツは、パソコン等により、容易に読み出すことが可能であり、また、読み出したデータを他の記録媒体に書き込むことも容易である。したがって、コンテンツの著作権を保護するシステムにおいては、記録媒体上のデータを読み出し、他の記録媒体に書き込むという、通常のユーザが行い得る行為に対して、それを防止する有効な機能を備えるシステムでなければならない。記録媒体から読み出したデータが他の記録媒体に書き込まれることを防止する技術をメディアバインド技術と呼び、特許文献2により、メディアバインドを実現するメカニズムが開示されている。

【0007】

従来のメディアバインド技術を利用して著作権保護を実現するために、予め、記録媒体の書き換え不可領域には、記録媒体を識別する媒体識別子が記録されており、当該記録媒体に記録されている暗号化コンテンツは、この媒体識別子に基づいて、暗号化されている。従って、暗号化コンテンツだけを他の記録媒体に複製しても、他の記録媒体は、別の媒体識別子を記録しており、この別の媒体識別子に基づいて、暗号化コンテンツを正しく復号することはできない。

【特許文献1】特開2002-281013号公報

【特許文献2】特許第3073590号公報

【特許文献3】特開平09-160492号公報

【発明の開示】

10

20

30

40

50

**【発明が解決しようとする課題】****【0008】**

しかしながら、コンテンツの不正な利用の拡大を防ぐために、多様な不正防止技術の実現が要望されている。

本発明は、上記の要望に対処するために、コンテンツの不正利用を防止することができる著作物保護システム、記録装置、記録方法、再生装置、再生方法、コンピュータプログラム及び記録媒体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】****【0009】**

上記目的を達成するために本発明は、記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムである。

前記複数の再生装置のうちいずれか1台以上は、無効化されている。

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されている。

**【0010】**

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、前記記憶手段から前記メディア鍵データを読み出す読出手段と、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段とを備えている。

**【0011】**

各再生装置は、前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

**【発明の効果】****【0012】**

この構成によると、前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記録媒体に書き込み、また、媒体固有番号及びメディア鍵に基づいて、生成された暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、生成された暗号化コンテンツを記録媒体に書き込む。また、再生装置は、デバイス鍵を用いて、暗号化メディア鍵を復号して復号メディア鍵を生成し、生成した復号メディア鍵が、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止する。

**【0013】**

このように構成されているので、無効化された再生装置を排除することができる。

ここで、別の記録媒体は、無効化されていない各再生装置についてメディア鍵が、無効

10

20

30

40

50

化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶している。前記記録装置は、さらに、前記別の記録媒体に記憶されている別のメディア鍵データと、前記記憶手段に記憶されている前記メディア鍵データとの新旧を比較する比較手段と、前記別のメディア鍵データの方が新しいと判断される場合に、前記別の記録媒体から前記別のメディア鍵データを読み出し、読み出した前記別のメディア鍵データを、前記記憶手段に記憶されている前記メディア鍵データに、上書きする更新手段とを備え、前記読出手段は、前記メディア鍵データの読出しに代えて、前記記憶手段から前記別のメディア鍵データを読み出し、前記書込手段は、前記メディア鍵データの書込みに代えて、読み出された前記別のメディア鍵データを前記記録媒体の前記書換可能領域に書き込む。

10

**【 0 0 1 4 】**

この構成によると、記録装置は、内部に記憶しているメディア鍵データを、別の記録媒体から取得した別の暗号化メディア鍵に更新することができる。

ここで、前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して検証情報を生成する署名生成手段を備え、前記書込手段は、さらに、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込む。また、前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成し、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込み、前記読出手段は、さらに、前記記録媒体の前記書換可能領域に書き込まれた前記検証情報を読み出し、前記再生装置は、さらに、読み出した前記検証情報に基づいて、署名検証を施して、検証の成功又は失敗を示す検証結果を出力する検証手段を備え、前記制御手段は、さらに、前記検証結果が検証の失敗を示す場合に、前記暗号化コンテンツの復号を禁止し、前記検証結果が検証の成功を示す場合に、前記暗号化コンテンツの復号を許可する。

20

**【 0 0 1 5 】**

この構成によると、記録装置は、さらに、デジタル署名により生成した検証情報を記録媒体に書き込むので、再生装置において、検証情報を検証することにより、不正な再生装置を排除することができる。

30

ここで、前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む。また、前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込み、前記再生装置は、さらに、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第1無効化データを記憶している記憶手段と、前記記録媒体から前記公開鍵証明書を読み出す証明書読出手段と、読み出した公開鍵証明書に含まれる公開鍵が、前記第1無効化データにより、無効化されていることを示しているか否かを検証する公開鍵検証手段とを含み、前記制御手段は、さらに、前記公開鍵が無効化されている場合に、前記暗号化コンテンツの復号を禁止し、前記公開鍵が無効化されていない場合に、前記暗号化コンテンツの復号を許可する。

40

**【 0 0 1 6 】**

この構成によると、記録装置は、公開鍵証明書を記録媒体に書き込み、再生装置は、記録媒体から公開鍵証明書を読み出し、公開鍵が無効化されている場合に、暗号化コンテンツの復号を禁止できる。

ここで、別の記録媒体は、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第2無効化データを記憶しており、前記再生装置は、さらに、前記別の記録媒体に記憶されている前記第2無効化データと、前記記憶

50

手段に記憶されている前記第 1 無効化データとの新旧を比較する比較手段と、前記第 2 無効化データの方が新しいと判断される場合に、前記別の記録媒体から前記第 2 無効化データを読み出し、読み出した前記第 2 無効化データを、前記記憶手段に記憶されている前記第 1 無効化データに、上書きする更新手段とを含む。

【 0 0 1 7 】

この構成によると、再生装置は、無効化データを最新の状態に更新することができる。

ここで、前記記憶手段は、さらに、当該記録装置を識別する装置識別子を記憶しており、前記記録装置は、さらに、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記コンテンツに電子透かしとして埋め込む埋込手段を備え、前記暗号化手段は、前記装置識別子が埋め込まれたコンテンツを暗号化する。また、前記再生装置は、さらに、当該再生装置を識別する装置識別子を記憶している前記記憶手段と、復号が許可された場合に、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記暗号化コンテンツに電子透かしとして埋め込む埋込手段と、前記装置識別子が埋め込まれた前記暗号化コンテンツを前記記録媒体に書き込む。

10

【 0 0 1 8 】

記録装置及び再生装置は、装置識別子が埋め込まれたコンテンツを記録媒体に書き込むので、前記コンテンツが不正に流通した場合に、前記コンテンツから、埋め込まれた装置識別子を抽出することにより、そのコンテンツを記録した記録装置及び再生装置を特定することができる。

ここで、前記記憶手段に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記書込手段は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込む。また、前記記録装置に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込み、前記再生装置は、さらに、前記記録媒体に記録されている前記暗号化コンテンツの指定を受け付ける受付手段と、指定が受け付けられた前記暗号化コンテンツに対応付けられた前記データ識別子を前記記録媒体から読み出す読出手段と、読み出した前記データ識別子を含む前記メディア鍵データを前記記録媒体から読み出す読出手段とを含み、前記制御手段は、読み出した前記メディア鍵データに基づいて、前記暗号化コンテンツの復号の可否を判断する。

20

30

【 0 0 1 9 】

記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体に書き込み、前記データ識別子を含む前記メディア鍵データを前記記録媒体に書き込むので、再生装置において、データ識別子を介して、暗号化コンテンツに対応するメディア鍵データを取得し、取得したメディア鍵データに基づいて、暗号化コンテンツの復号の可否を判断できる。

【 発明を実施するための最良の形態 】

【 0 0 2 0 】

1. 第 1 の実施の形態

本発明に係る 1 の実施の形態としてのコンテンツ供給システム 10 について説明する。

1. 1 コンテンツ供給システム 10 の構成

コンテンツ供給システム 10 は、図 1 に示すように、コンテンツサーバ装置 500、記録装置 100 及び再生装置 200 a、200 b、200 c、200 d、200 e、・・・から構成されている。記録装置 100 及び再生装置 200 a、200 b、200 c、200 d、200 e、・・・の台数の合計は、n 台である。記録装置 100 には、装置番号「1」が割り当てられており、再生装置 200 a、200 b、200 c、200 d、200 e、・・・には、それぞれ、装置番号「2」、「3」、「4」、・・・、「n」が割り当てられている。各装置は、割り当てられた各装置番号により識別される。

40

50

## 【 0 0 2 1 】

これらの n 台の装置のうち、再生装置 2 0 0 b 及び再生装置 2 0 0 c は、不正な第三者による不正な攻撃を受けたために、本来秘密に内蔵すべき鍵が暴露されており、このため、再生装置 2 0 0 b 及び再生装置 2 0 0 c は、無効化されている。

音楽や映画などのコンテンツの供給業者は、コンテンツサーバ装置 5 0 0 及び記録装置 1 0 0 を有しており、コンテンツサーバ装置 5 0 0 と記録装置 1 0 0 とは、専用回線 3 0 を介して接続されている。

## 【 0 0 2 2 】

コンテンツサーバ装置 5 0 0 は、コンテンツ及び前記コンテンツを暗号化する際に用いられるコンテンツ鍵を有しており、記録装置 1 0 0 からの要求により、コンテンツ及び対応するコンテンツ鍵を、専用回線 3 0 を介して、記録装置 1 0 0 へ送信する。

記録装置 1 0 0 は、コンテンツサーバ装置 5 0 0 から、専用回線 3 0 を介して、コンテンツ及び対応するコンテンツ鍵を受信し、受信したコンテンツとコンテンツ鍵を暗号化し、暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報をして記録媒体 1 2 0 に書き込む。

## 【 0 0 2 3 】

暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報が記録された記録媒体 1 2 0 は、販売店で売られ、利用者は、記録媒体 1 2 0 を購入する。

利用者の有する再生装置 2 0 0 a は、記録媒体 1 2 0 が装着されると、記録媒体 1 2 0 から暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報を読み出し、読み出したその他の関連する情報を用いて、コンテンツの復号の可否を判断し、復号可能であると判断する場合に、暗号化コンテンツ鍵から復号コンテンツ鍵を生成し、復号コンテンツ鍵を用いて復号コンテンツを生成し、生成した復号コンテンツから映画や音楽を生成し、出力する。

## 【 0 0 2 4 】

## 1 . 2 コンテンツサーバ装置 5 0 0

コンテンツサーバ装置 5 0 0 は、情報記憶部 5 0 1、制御部 5 0 2、入力部 5 0 3、表示部 5 0 4 及び送受信部 5 0 5 から構成されている（図示していない）。

コンテンツサーバ装置 5 0 0 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、通信ユニット、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 又は前記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従って動作することにより、コンテンツサーバ装置 5 0 0 の各構成要素は、その機能を達成する。

## 【 0 0 2 5 】

送受信部 5 0 5 は、専用回線 3 0 を介して、記録装置 1 0 0 に接続されており、記録装置 1 0 0 と制御部 5 0 2 との間で情報の送受信を行う。

情報記憶部 5 0 1 は、映像情報及び音声情報が高効率で圧縮符号化されて生成されたコンテンツと当該コンテンツを暗号化する際に鍵として用いられるコンテンツ鍵との組を複数個予め記憶している。

## 【 0 0 2 6 】

制御部 5 0 2 は、記録装置 1 0 0 から、専用回線 3 0 及び送受信部 5 0 5 を介して、いずれかのコンテンツの取得要求を受け取る。前記取得要求を受け取ると、制御部 5 0 2 は、情報記憶部 5 0 1 から、前記取得要求により示されるコンテンツ及びコンテンツ鍵を読み出し、読み出したコンテンツ及びコンテンツ鍵を、送受信部 5 0 5 及び専用回線 3 0 を介して、記録装置 1 0 0 へ送信する。

## 【 0 0 2 7 】

入力部 5 0 3 は、コンテンツサーバ装置 5 0 0 の操作者の指示を受け付け、受け付けた指示を制御部 5 0 2 へ出力する。

表示部 5 0 4 は、制御部 5 0 2 の制御により、様々な情報を表示する。

10

20

30

40

50

### 1.3 記録装置100

記録装置100は、図2に示すように、デバイス鍵格納部101、メディア鍵データ格納部102、鍵計算部103、鍵計算部104、暗号化部105、暗号化部106、秘密鍵格納部107、証明書格納部108、CRL格納部109、署名生成部110、ドライブ部111、制御部112及び送受信部113から構成されている。

#### 【0028】

記録装置100は、具体的には、コンテンツサーバ装置500と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニット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又は前記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従って動作することにより、記録装置100は、その機能を達成する。

10

#### 【0029】

##### (1) デバイス鍵格納部101

デバイス鍵格納部101は、外部の装置からアクセスできないように、デバイス鍵DK\_\_1を秘密に記憶している。デバイス鍵DK\_\_1は、記録装置100に固有の鍵である。なお、本明細書において、装置mが保有するデバイス鍵をDK\_\_mと表現している。

##### (2) メディア鍵データ格納部102

メディア鍵データ格納部102は、メディア鍵データMDATAを記憶している。メディア鍵データMDATAは、n個の組を含み、各組は、暗号化メディア鍵及び装置番号から構成されている。各組に含まれている暗号化メディア鍵と装置番号とは対応している。ここで、nは、上述したように、記録装置100及び再生装置200a、200b、・・・の台数の合計値である。

20

#### 【0030】

n個の組のうち、第1の組は、第1の暗号化メディア鍵及び装置番号「1」から構成されている。装置番号「1」は、記録装置100を識別する識別情報である。第1の暗号化メディア鍵は、装置番号「1」により識別される装置、つまり、記録装置100に割り当てられたデバイス鍵DK\_\_1を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

#### 【0031】

第1の暗号化メディア鍵 = E1 (DK\_\_1, MK)

30

ここで、暗号化アルゴリズムE1は、一例として、DES (Data Encryption Standard) によるものである。また、E(A, B)は、鍵Aを用いて、平文Bに対して暗号化アルゴリズムEを施して得られた暗号文を示している。

また、メディア鍵MKは、記録媒体120に固有の鍵である。

#### 【0032】

また、n個の組のうち、第2の組は、それぞれ、第2の暗号化メディア鍵及び装置番号「2」から構成されている。ここで、装置番号「2」は、再生装置200aを識別する。また、第2の暗号化メディア鍵は、装置番号「2」の装置、つまり、再生装置200aに割り当てられたデバイス鍵DK\_\_2を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

40

#### 【0033】

第2の暗号化メディア鍵 = E1 (DK\_\_2, MK)

また、n個の組のうち、第3、第4の組は、それぞれ、第3の暗号化メディア鍵及び装置番号「3」、第4の暗号化メディア鍵及び装置番号「4」から構成されている。ここで、装置番号「3」及び「4」は、それぞれ、再生装置200b、200cを識別する。また、第3、第4の暗号化メディア鍵は、それぞれ、装置番号「3」、「4」により識別される装置、つまり、再生装置200b、200cに割り当てられたデバイス鍵DK\_\_3、DK\_\_4を用いて、メディア鍵MKの代わりに、値「0」に暗号化アルゴリズムE1を施して生成されたものである。

#### 【0034】

50

第3の暗号化メディア鍵 =  $E1(DK\_3, 0)$

第4の暗号化メディア鍵 =  $E1(DK\_4, 0)$

ここで、値「0」は、メディア鍵(MK)とは全く無関係のデータである。メディア鍵MKの代わりに、値「0」を用いるのは、第3及び第4の暗号化メディア鍵に、それぞれ、対応する再生装置200b及び200cが無効化されているからであり、再生装置200b及び200cが無効化されていることを知るための検知情報として用いられる。

【0035】

無効化された装置について、無効化された装置のデバイス鍵を用いて、メディア鍵MKとは全く無関係のデータ、つまり値「0」を暗号化して暗号化メディア鍵を生成することにより、無効化された装置以外の全ての装置だけがメディア鍵MKを共有できる。また、無効化された装置をこのシステムから排除することができる。

10

ここで、値「0」を用いるとしているが、メディア鍵MKとは、全く無関係の他のデータであるとしてもよい。例えば、他の固定値である「0xFFFF」、暗号化メディア鍵を生成する時点の日付や時刻を示す情報、当該無効化された装置のデバイス鍵などであるとしてもよい。

【0036】

なお、装置の無効化方法は他の方法を利用してもよく、例えば、特許文献1には木構造を利用した無効化方法が開示されている。

また、n個の組のうち、第5、・・・、第nの組は、それぞれ、第5の暗号化メディア鍵及び装置番号「5」、・・・、第nの暗号化メディア鍵及び装置番号「n」から構成されている。ここで、装置番号「5」、・・・、「n」は、それぞれ、再生装置200d、200e、・・・を識別する。また、第5、・・・、第nの暗号化メディア鍵は、それぞれ、装置番号「5」、・・・「n」の装置、つまり、再生装置200d、200e、・・・に割り当てられたデバイス鍵DK\_5、・・・、DK\_nを用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

20

【0037】

第5の暗号化メディア鍵 =  $E1(DK\_5, MK)$

・・・

第nの暗号化メディア鍵 =  $E1(DK\_n, MK)$

(3) 鍵計算部103

鍵計算部103は、記録装置100に割り当てられた装置番号「1」を予め記憶している。

30

【0038】

鍵計算部103は、メディア鍵データ格納部102に記憶されているメディア鍵データMDATAを構成するn個の組から、予め記憶している装置番号「1」を含む組を探して読み出し、読み出した組から装置番号「1」に対応する暗号化メディア鍵 $E1(DK\_1, MK)$ を抽出する。

次に、鍵計算部103は、デバイス鍵格納部101からデバイス鍵DK\_1を読み出し、読み出したデバイス鍵DK\_1を用いて、抽出した暗号化メディア鍵 $E1(DK\_1, MK)$ に復号アルゴリズムD1を施して、メディア鍵MKを生成する。

40

【0039】

メディア鍵MK =  $D1(DK\_1, (E1(DK\_1, MK)))$

ここで、復号アルゴリズムD1は、暗号化アルゴリズムE1を施して生成された暗号文を復号するアルゴリズムであり、一例として、DESによるものである。また、D(A, B)は、鍵Aを用いて、暗号文Bに対して復号アルゴリズムDを施して得られた復号文を示している。

【0040】

次に、鍵計算部103は、生成したメディア鍵MKを鍵計算部104へ出力する。

なお、図2において、記録装置100の各構成部を示す各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線

50

は、信号や情報が伝達される経路を示している。また、鍵計算部 103 を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが描かれているものは、鍵計算部 103 へ鍵としての情報が伝達される経路を示している。他の構成要素を示すブロックについても同様である。また、他の図面についても同様である。

【0041】

(4) 鍵計算部 104

鍵計算部 104 は、鍵計算部 103 からメディア鍵 MK を受け取り、ドライブ部 111 を介して、記録媒体 120 の固有番号記録領域 121 から媒体固有番号 MID を読み出す。

次に、鍵計算部 104 は、受け取ったメディア鍵 MK と読み出した媒体固有番号 MID を、この順序で、結合して、結合値 (MK || MID) を生成する。ここで、「A || B」は、データ A とデータ B とをこの順序でビット結合することを示す。次に、鍵計算部 104 は、生成した結合値 (MK || MID) にハッシュ関数 SHA-1 を施して、ハッシュ値  $H = \text{SHA-1}(MK || MID)$  を得、得られたハッシュ値 H を鍵暗号化鍵 KEK とし、鍵暗号化鍵 KEK を暗号化部 105 及び署名生成部 110 へ出力する。

10

【0042】

ここで、SHA-1(A) は、情報 A に対してハッシュ関数 SHA-1 を施して得られたハッシュ値を示している。

なお、鍵計算部 104 は、ハッシュ関数 SHA-1 を施して得られたハッシュ値を鍵暗号化鍵 KEK としているが、これに限定されることはない。得られたハッシュ値の一部分を鍵暗号化鍵 KEK としてもよい。

20

【0043】

また、ハッシュ関数 SHA-1 については、公知であるので、説明を省略する。なお、他のハッシュ関数を使用してもよい。

(5) 暗号化部 105

暗号化部 105 は、コンテンツサーバ装置 500 から送受信部 113 を介して、コンテンツ鍵 CK を受け取り、鍵計算部 104 から鍵暗号化鍵 KEK を受け取る。

【0044】

次に、暗号化部 105 は、受け取った鍵暗号化鍵 KEK を用いて、受け取ったコンテンツ鍵 CK に暗号化アルゴリズム E2 を施して、暗号化コンテンツ鍵 ECK を生成する。

30

暗号化コンテンツ鍵  $ECK = E2(KEK, CK)$

ここで、暗号化アルゴリズム E2 は、一例として、DES によるものである。

次に、暗号化部 105 は、ドライブ部 111 を介して、記録媒体 120 上に鍵記録領域 123 を確保し、次に、生成した暗号化コンテンツ鍵 ECK を、ドライブ部 111 を介して、記録媒体 120 の鍵記録領域 123 へ書き込む。

【0045】

(6) 暗号化部 106

暗号化部 106 は、コンテンツサーバ装置 500 から送受信部 113 を介して、コンテンツ鍵 CK 及びコンテンツ CNT を受け取り、受け取ったコンテンツ鍵 CK を用いて、受け取ったコンテンツ CNT に暗号化アルゴリズム E3 を施して暗号化コンテンツ ECNT を生成する。

40

【0046】

暗号化コンテンツ  $ECNT = E3(CK, CNT)$

ここで、暗号化アルゴリズム E3 は、一例として、DES によるものである。

次に、暗号化部 106 は、ドライブ部 111 を介して、記録媒体 120 上にコンテンツ記録領域 124 を確保し、次に、生成した暗号化コンテンツ ECNT を、ドライブ部 111 を介して、記録媒体 120 のコンテンツ記録領域 124 へ書き込む。

【0047】

(7) 秘密鍵格納部 107

秘密鍵格納部 107 は、外部の装置からアクセスできないように、記録装置 100 の秘

50

密鍵  $SK\_1$  を記憶している。秘密鍵  $SK\_1$  は、公開鍵暗号方式によるものである。ここで、前記公開鍵暗号方式は、一例として、RSA (Rivest Shamir Adleman) 暗号方式である。

#### 【0048】

##### (8) 証明書格納部 108

証明書格納部 108 は、公開鍵証明書 PKC を記憶している。公開鍵証明書 PKC は、証明書識別子 ID\_1、公開鍵 PK\_1 及び署名データ Sig\_1 を含んで構成される。

証明書識別子 ID\_1 は、公開鍵証明書 PKC を一意に識別する識別情報である。公開鍵 PK\_1 は、秘密鍵格納部 107 に記憶されている秘密鍵  $SK\_1$  に対応する公開鍵である。また、署名データ Sig\_1 は、認証局 CA (Certificate Authority) の秘密鍵  $SK\_CA$  を用いて、証明書識別子 ID\_1 及び公開鍵 PK\_1 の結合値 (ID\_1 || PK\_1) に対してデジタル署名 Sig を施して生成されたものである。

10

#### 【0049】

署名データ  $Sig\_1 = Sig(SK\_CA, ID\_1 || PK\_1)$

ここで、 $Sig(A, B)$  は、鍵 A を用いて、データ B に対して、デジタル署名 Sig を施して得られた署名データを示している。また、デジタル署名 Sig の一例は、ハッシュ関数 SHA-1 を使った RSA を用いるデジタル署名である。

##### (9) CRL 格納部 109

CRL 格納部 109 は、第 1 の時点における無効化された公開鍵証明書を示す公開鍵証明書無効化リスト (以下、無効化リスト CRL と呼ぶ。) を記録している。

20

#### 【0050】

無効化リスト CRL は、1 個以上の証明書識別子と、署名データ Sig ID と、版数とを含んでいる。

各証明書識別子は、無効化された公開鍵証明書を識別する識別情報である。

署名データ Sig ID は、認証局 CA の秘密鍵  $SK\_CA$  を用いて、無効化リスト CRL に含まれる全ての証明書識別子の結合値に対して (無効化リスト CRL に 1 個の証明書識別子が含まれている場合には、前記 1 個の証明書識別子に対して)、デジタル署名 Sig を施して生成されたものである。

#### 【0051】

署名データ  $Sig\ ID = Sig(SK\_CA, \text{全ての証明書識別子の結合値})$

30

例えば、証明書識別子 ID\_3 及び ID\_4 により識別される公開鍵証明書が無効化されている場合には、無効化リスト CRL は、証明書識別子 ID\_3、ID\_4、署名データ  $Sig\ ID = Sig(SK\_CA, (ID\_3 || ID\_4))$  及び版数を含む。

版数は、無効化リスト CRL の世代を示す情報であり、無効化リスト CRL が前記第 1 の時点におけるものであることを示す。版数は、公開鍵証明書無効化リストの世代が新しいほど、大きい値をとる。

#### 【0052】

##### (10) 署名生成部 110

署名生成部 110 は、秘密鍵格納部 107 から秘密鍵  $SK\_1$  を読み出し、CRL 格納部 109 から無効化リスト CRL を読み出し、鍵計算部 104 から鍵暗号化鍵 KEK を受け取る。

40

次に、署名生成部 110 は、受け取った鍵暗号化鍵 KEK と読み出した無効化リスト CRL とをこの順序で結合して結合値 (KEK || CRL) を生成し、読み出した秘密鍵  $SK\_1$  を用いて、生成した結合値 (KEK || CRL) にデジタル署名 Sig を施して署名データ Sig CRL を生成する。

#### 【0053】

署名データ  $Sig\ CRL = Sig(SK\_1, (KEK || CRL))$

次に、署名生成部 110 は、ドライブ部 111 を介して、記録媒体 120 上に署名記録領域 125 を確保し、次に、生成した署名データ Sig CRL を、ドライブ部 111 を介して、記録媒体 120 の署名記録領域 125 へ書き込む。

50

## ( 1 1 ) 制御部 1 1 2

制御部 1 1 2 は、送受信部 1 1 3 を介して、コンテンツサーバ装置 5 0 0 に対して、コンテンツの取得要求を送信する。

## 【 0 0 5 4 】

また、制御部 1 1 2 は、証明書格納部 1 0 8 から公開鍵証明書 P K C を読み出し、ドライブ部 1 1 1 を介して、記録媒体 1 2 0 上に証明書記録領域 1 2 7 を確保し、次に、読み出した公開鍵証明書 P K C をドライブ部 1 1 1 を介して、記録媒体 1 2 0 の証明書記録領域 1 2 7 へ書き込む。

また、制御部 1 1 2 は、メディア鍵データ格納部 1 0 2 からメディア鍵データ M D A T A を読み出し、ドライブ部 1 1 1 を介して、記録媒体 1 2 0 上にメディア鍵データ記録領域 1 2 2 を確保し、次に、読み出したメディア鍵データ M D A T A をドライブ部 1 1 1 を介して、記録媒体 1 2 0 のメディア鍵データ記録領域 1 2 2 へ書き込む。

## 【 0 0 5 5 】

また、制御部 1 1 2 は、C R L 格納部 1 0 9 から無効化リスト C R L を読み出し、ドライブ部 1 1 1 を介して、記録媒体 1 2 0 上に C R L 記録領域 1 2 6 を確保し、次に、読み出した無効化リスト C R L をドライブ部 1 1 1 を介して、記録媒体 1 2 0 の C R L 記録領域 1 2 6 へ書き込む。

制御部 1 1 2 は、記録装置 1 0 0 の操作者の操作指示によりキーボード 1 8 0 から指示情報を受け取り、指示情報に従って動作する。また、記録装置 1 0 0 を構成する他の構成要素の動作を制御する。

## 【 0 0 5 6 】

## ( 1 2 ) 送受信部 1 1 3

送受信部 1 1 3 は、専用回線 3 0 を介して、コンテンツサーバ装置 5 0 0 と接続されており、コンテンツサーバ装置 5 0 0 と制御部 1 1 2 との間で情報の送受信を行う。また、制御部 1 1 2 の制御の基に、コンテンツサーバ装置 5 0 0 と暗号化部 1 0 5 との間で、及びコンテンツサーバ装置 5 0 0 と暗号化部 1 0 6 との間で、情報の送受信を行う。

## 【 0 0 5 7 】

## ( 1 3 ) ドライブ部 1 1 1

ドライブ部 1 1 1 は、制御部 1 1 2 の制御の基に、記録媒体 1 2 0 の固有番号記録領域 1 2 1 から媒体固有番号 M I D を読み出し、読み出した媒体固有番号 M I D を鍵計算部 1 0 4 へ出力する。

また、ドライブ部 1 1 1 は、制御部 1 1 2 の制御の基に、暗号化部 1 0 5、暗号化部 1 0 6、署名生成部 1 1 0 から各情報を受け取り、受け取った情報を書き込むための各領域を記録媒体 1 2 0 上に確保し、確保した領域に前記情報を書き込む。

## 【 0 0 5 8 】

また、ドライブ部 1 1 1 は、制御部 1 1 2 から情報を受け取り、受け取った情報を書き込むための各領域を記録媒体 1 2 0 上に確保し、確保した領域に前記情報を書き込む。

## ( 1 4 ) キーボード 1 8 0 及びモニタ 1 9 0

キーボード 1 8 0 は、記録装置 1 0 0 の操作者の操作指示を受け付け、受け付けた操作指示に対応する指示情報を制御部 1 1 2 へ出力する。

## 【 0 0 5 9 】

モニタ 1 9 0 は、制御部 1 1 2 の制御により様々な情報を表示する。

## 1 . 4 記録媒体 1 2 0

記録媒体 1 2 0 は、光ディスクメディアであり、図 3 に示すように、固有番号記録領域 1 2 1 と、一般領域 1 2 9 とから構成されている。

固有番号記録領域 1 2 1 には、記録媒体 1 2 0 を識別する固有の番号である媒体固有番号 M I D が予め記録されている。固有番号記録領域 1 2 1 は、他の情報の書き込みや記録されている媒体固有番号 M I D の書き換えができない書換不可領域である。媒体固有番号 M I D は、一例として、1 6 進数 8 桁で表現されており、「0 x 0 0 0 0 0 0 0 6」である。なお、本明細書において、「0 x」は、以降の表示が 1 6 進数によるものであること

10

20

30

40

50

を示している。

【 0 0 6 0 】

一般領域 1 2 9 は、他の情報の書き込みが可能な領域であり、当初、一般領域 1 2 9 には、何らの情報も書き込まれていない。

記録装置 1 0 0 の上述した動作の終了後において、一般領域 1 2 9 には、図 3 に示すように、メディア鍵データ記録領域 1 2 2、鍵記録領域 1 2 3、コンテンツ記録領域 1 2 4、署名記録領域 1 2 5、C R L 記録領域 1 2 6 及び証明書記録領域 1 2 7 が確保される。

【 0 0 6 1 】

上述したように、第 1 の実施の形態では、記録装置 1 0 0 及び再生装置 2 0 0 a、2 0 0 b、2 0 0 c、2 0 0 d、2 0 0 e、・・・の台数の合計が n 台であり、これらの装置のうち、再生装置 2 0 0 b 及び再生装置 2 0 0 c が無効化されており、n 台の装置はそれぞれ固有のデバイス鍵を 1 つだけ保有している、と仮定している。このような仮定に基づいて、記録媒体 1 2 0 の一般領域 1 2 9 に含まれている各領域には、具体例としての各種データが記録されている。

【 0 0 6 2 】

(メディア鍵データ記録領域 1 2 2 )

メディア鍵データ記録領域 1 2 2 には、メディア鍵データ M D A T A が記録されている。メディア鍵データ M D A T A は、n 個の組から構成され、各組は、暗号化メディア鍵及び装置番号を含む。

装置番号は、装置を識別する識別情報である。

【 0 0 6 3 】

暗号化メディア鍵は、対応する装置番号「m」により示される装置 m に割り当てられたデバイス鍵 D K \_ m を用いて、メディア鍵 M K 又は値「0」に暗号化アルゴリズム E 1 を施して生成されたものである。ここで、装置 m が無効化されている場合には、値「0」を用いる。また、装置 m が無効化されていない場合には、メディア鍵 M K を用いる。

暗号化メディア鍵 = E 1 ( D K \_ m、M K ) 又は

暗号化メディア鍵 = E 1 ( D K \_ m、0 )

( 鍵記録領域 1 2 3 )

鍵記録領域 1 2 3 には、暗号化コンテンツ鍵 E C K が記録されている。暗号化コンテンツ鍵 E C K は、鍵暗号化鍵 K E K を用いて、コンテンツ鍵 C K に暗号化アルゴリズム E 2 を施して生成されたものである。

【 0 0 6 4 】

暗号化コンテンツ鍵 E C K = E 2 ( K E K、C K )

ここで、鍵暗号化鍵 K E K は、メディア鍵 M K と媒体固有番号 M I D を結合した値を入力値として、ハッシュ関数の出力値を利用して算出される鍵である。

鍵暗号化鍵 K E K = S H A - 1 ( M K | | M I D )

( コンテンツ記録領域 1 2 4 )

コンテンツ記録領域 1 2 4 には、暗号化コンテンツ E C N T が記録されている。暗号化コンテンツ E C N T は、コンテンツ鍵 C K を用いて、コンテンツに暗号化アルゴリズム E 3 を施して生成されたものである。

【 0 0 6 5 】

暗号化コンテンツ E C N T = E 3 ( C K、C N T )

( 署名記録領域 1 2 5 )

署名記録領域 1 2 5 には、署名データ S i g C R L が記録されている。

署名データ S i g C R L は、秘密鍵 S K \_ 1 を用いて、鍵暗号化鍵 K E K と無効化リスト C R L との結合値 ( K E K | | C R L ) にデジタル署名 S i g を施して生成されたものである。

【 0 0 6 6 】

署名データ S i g C R L = S i g ( S K \_ 1、( K E K | | C R L ) )

( C R L 記録領域 1 2 6 )

CRL記録領域126には、無効化リストCRLが記録されており、無効化リストCRLには、無効化するべき証明書のIDが記載されている。無効化リストCRLは、一例として、証明書識別子ID\_\_3、ID\_\_4、署名データSigID及び版数を含んでいる。

【0067】

証明書識別子ID\_\_3、ID\_\_4は、無効化された公開鍵証明書を識別する識別情報である。

署名データSigIDは、認証局CAの秘密鍵SK\_\_CAを用いて、無効化リストCRLに含まれる全ての証明書識別子の結合値に対して（無効化リストCRLに1個の証明書識別子が含まれている場合には、前記1個の証明書識別子に対して）、デジタル署名Sigを施して生成されたものである。

10

【0068】

署名データSigID = Sig (SK\_\_CA、全ての証明書識別子の結合値)

認証局CAによる署名データが含まれているのは、無効化リストCRLの正当性を保証するためである。

版数は、無効化リストCRLの世代を示す情報である。

なお、CRLのフォーマットは公知のものであってもよいし、また、あるシステムに特化したフォーマットであってもよい。

【0069】

(証明書記録領域127)

証明書記録領域127には、公開鍵証明書PKCが記録されている。公開鍵証明書PKCは、証明書識別子ID\_\_1、公開鍵PK\_\_1及び署名データSig\_\_1を含んでいる。

20

証明書識別子ID\_\_1は、公開鍵証明書PKCを識別する識別情報である。

公開鍵PK\_\_1は、公開鍵暗号方式によるものであり、秘密鍵SK\_\_1に対応している。

【0070】

署名データSig\_\_1は、認証局CAの秘密鍵SK\_\_CAを用いて、証明書識別子ID\_\_1及び公開鍵PK\_\_1の結合値(ID\_\_1 || PK\_\_1)に対してデジタル署名Sigを施して生成されたものである。

署名データSig\_\_1 = Sig (SK\_\_CA、ID\_\_1 || PK\_\_1)

なお、認証局CAによる署名データが含まれているのは、公開鍵証明書の正当性を保証するためである。

30

【0071】

また、公開鍵証明書のフォーマットは公知のものであってもよいし、またあるシステムに特化したフォーマットであってもよい。

1.5 再生装置200

再生装置200a、200b、200c、・・・は、同様の構成を有しているので、ここでは、再生装置200として説明する。

【0072】

再生装置200は、図4に示すように、デバイス鍵格納部201、鍵計算部202、鍵計算部203、復号部204、復号部205、CA公開鍵格納部206、証明書検証部207、CRL格納部208、CRL検証部209、CRL比較更新部210、証明書判定部211、署名検証部212、スイッチ213、再生部214、制御部215、入力部216、表示部217及びドライブ部218から構成されている。

40

【0073】

再生装置200は、具体的には、コンテンツサーバ装置500と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニット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又は前記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従って動作することにより、再生装置200は、その機能を達成する。

【0074】

50

## (1) デバイス鍵格納部 201

デバイス鍵格納部 201 は、外部の装置からアクセスできないように、デバイス鍵  $DK\_x$  を秘密に記憶している。デバイス鍵  $DK\_x$  は、再生装置 200 に固有の鍵である。

なお、デバイス鍵格納部 201 が記憶しているデバイス鍵  $DK\_x$  は、再生装置 200 a、200 b、200 c、200 d、200 e、・・・により異なる。再生装置 200 a、200 b、200 c、200 d、200 e、・・・の各デバイス鍵格納部 201 は、それぞれ、デバイス鍵  $DK\_2$ 、 $DK\_3$ 、 $DK\_4$ 、 $DK\_5$ 、 $DK\_6$ 、・・・を記憶している。

## 【0075】

## (2) 鍵計算部 202

鍵計算部 202 は、再生装置 200 に割り当てられた装置番号「x」を予め記憶している。なお、鍵計算部 202 が記憶している装置番号「x」は、再生装置 200 a、200 b、200 c、200 d、200 e、・・・により異なる。再生装置 200 a、200 b、200 c、200 d、200 e、・・・の各鍵計算部 202 は、それぞれ、装置番号「2」、「3」、「4」、「5」、「6」・・・を記憶している。

## 【0076】

鍵計算部 202 は、記録媒体 120 のメディア鍵データ記録領域 122 から、ドライブ部 218 を介して、メディア鍵データ  $MEDIA$  を構成する  $n$  個の組を順に読み出し、読み出した組の中から、記憶している装置番号「x」を含む組を探す。装置番号「x」を含む組を発見すると、発見した組から装置番号「x」に対応する暗号化メディア鍵  $E1(DK\_x, y)$  を抽出する。ここで、再生装置 200 が、再生装置 200 b 又は 200 c である場合には、 $y$  は、値「0」である。また、再生装置 200 が、再生装置 200 b 及び 200 c を除く他の再生装置である場合には、 $y$  は、メディア鍵  $MEDIA$  である。

## 【0077】

次に、鍵計算部 202 は、デバイス鍵格納部 201 からデバイス鍵  $DK\_x$  を読み出し、読み出したデバイス鍵  $DK\_x$  を用いて、抽出した暗号化メディア鍵  $E1(DK\_x, y)$  に復号アルゴリズム  $D1$  を施して、復号メディア鍵  $y$  を生成する。

復号メディア鍵  $y = D1(DK\_x, (E1(DK\_x, y)))$

ここで、復号メディア鍵  $y$  は、メディア鍵  $MEDIA$  及び値「0」のいずれかである。

## 【0078】

次に、鍵計算部 202 は、生成した復号メディア鍵  $y$  を鍵計算部 203 へ出力する。

## (3) 鍵計算部 203

鍵計算部 203 は、鍵計算部 104 と同様に動作する。

鍵計算部 203 は、鍵計算部 202 から復号メディア鍵  $y$  を受け取り、ドライブ部 218 を介して、記録媒体 120 の固有番号記録領域 121 から媒体固有番号  $MEDIA$  を読み出す。

## 【0079】

次に、鍵計算部 203 は、受け取った復号メディア鍵  $y$  と読み出した媒体固有番号  $MEDIA$  を、この順序で、結合して、結合値  $(y || MEDIA)$  を生成する。次に、鍵計算部 203 は、生成した結合値  $(y || MEDIA)$  にハッシュ関数  $SHA-1$  を施して、ハッシュ値  $H' = SHA-1(y || MEDIA)$  を得、得られたハッシュ値  $H'$  を鍵復号鍵  $KDK$  とし、鍵復号鍵  $KDK$  を復号部 204 及び署名検証部 212 へ出力する。

## 【0080】

なお、上述したように、鍵計算部 104 が、得られたハッシュ値の一部分を鍵暗号化鍵  $KEK$  とする場合には、鍵計算部 203 も得られたハッシュ値の前記一部分と同じ部分を鍵復号鍵  $KDK$  とする。

## (4) 復号部 204

復号部 204 は、記録媒体 120 の鍵記録領域 123 から、ドライブ部 218 を介して、暗号化コンテンツ鍵  $ECK$  を読み出し、鍵計算部 203 から鍵復号鍵  $KDK$  を受け取る。

10

20

30

40

50

## 【 0 0 8 1 】

次に、復号部 2 0 4 は、受け取った鍵復号鍵  $KDK$  を用いて、読み出した暗号化コンテンツ鍵  $ECK$  に復号アルゴリズム  $D2$  を施して、復号コンテンツ鍵  $DCK$  を生成する。

復号コンテンツ鍵  $DCK = D2(KDK, ECK)$

ここで、復号アルゴリズム  $D2$  は、暗号化アルゴリズム  $E2$  を施して生成された暗号文を復号するアルゴリズムであり、一例として、 $DES$  によるものである。

## 【 0 0 8 2 】

次に、復号部 2 0 4 は、生成した復号コンテンツ鍵  $DCK$  を復号部 2 0 5 へ出力する。

( 5 ) 復号部 2 0 5

復号部 2 0 5 は、記録媒体 1 2 0 のコンテンツ記録領域 1 2 4 から、ドライブ部 2 1 8 を介して、暗号化コンテンツ  $ECNT$  を読み出し、復号部 2 0 4 から復号コンテンツ鍵  $DCK$  を受け取る。

## 【 0 0 8 3 】

次に、復号部 2 0 5 は、受け取った復号コンテンツ鍵  $DCK$  を用いて、読み出した暗号化コンテンツ  $ECNT$  に復号アルゴリズム  $D3$  を施して復号コンテンツ  $DCNT$  を生成する。

復号コンテンツ  $DCNT = D3(DCK, ECNT)$

ここで、復号アルゴリズム  $D3$  は、暗号化アルゴリズム  $E3$  を施して生成された暗号文を復号するアルゴリズムであり、一例として、 $DES$  によるものである。

## 【 0 0 8 4 】

次に、復号部 2 0 5 は、生成した復号コンテンツ  $DCNT$  をスイッチ 2 1 3 へ出力する。

( 6 )  $CA$  公開鍵格納部 2 0 6

$CA$  公開鍵格納部 2 0 6 は、認証局  $CA$  の公開鍵  $PK\_CA$  を予め記憶している。

( 7 ) 証明書検証部 2 0 7

証明書検証部 2 0 7 は、 $CA$  公開鍵格納部 2 0 6 から公開鍵  $PK\_CA$  を読み出し、記録媒体 1 2 0 の証明書記録領域 1 2 7 から、ドライブ部 2 1 8 を介して、公開鍵証明書  $PKC$  を読み出す。

## 【 0 0 8 5 】

次に、証明書検証部 2 0 7 は、読み出した公開鍵証明書  $PKC$  から、証明書識別子  $ID\_1$ 、公開鍵  $PK\_1$  及び署名データ  $Sig\_1$  を抽出し、抽出した証明書識別子  $ID\_1$  及び公開鍵  $PK\_1$  をこの順序で結合して結合値 ( $ID\_1 || PK\_1$ ) を生成する。

次に、証明書検証部 2 0 7 は、読み出した公開鍵  $PK\_CA$  を用いて、抽出した署名データ  $Sig\_1$  及び生成した結合値 ( $ID\_1 || PK\_1$ ) に、署名検証アルゴリズム  $Vrfy$  を施して、検証結果  $RS L 2$  を得る。検証結果  $RS L 2$  は、検証成功及び検証失敗のいずれかを示す情報である。

## 【 0 0 8 6 】

ここで、署名検証アルゴリズム  $Vrfy$  は、デジタル署名  $Sig$  により生成された署名データを検証するアルゴリズムである。

次に、証明書検証部 2 0 7 は、検証結果  $RS L 2$  をスイッチ 2 1 3 へ出力する。

( 8 )  $CRL$  格納部 2 0 8

$CRL$  格納部 2 0 8 は、第 2 の時点における無効化された公開鍵証明書を示す公開鍵証明書無効化リスト (以下、蓄積無効化リスト  $CRL\_ST$  と呼ぶ。) を記録している。

## 【 0 0 8 7 】

蓄積無効化リスト  $CRL\_ST$  は、第 1 の時点における無効化された公開鍵証明書を示すリストである無効化リスト  $CRL$  と同様に、1 個以上の証明書識別子と、署名データ  $SigID$  と、版数とを含んでいる。

証明書識別子及び署名データ  $SigID$  については、上述した通りである。

版数は、蓄積無効化リスト  $CRL\_ST$  の世代を示す情報であり、蓄積無効化リスト  $C$

10

20

30

40

50

R L \_\_ S T が前記第 2 の時点におけるものであることを示す。版数は、公開鍵証明書無効化リストの世代が新しいほど、大きい値をとる。

【 0 0 8 8 】

( 9 ) C R L 検証部 2 0 9

C R L 検証部 2 0 9 は、C A 公開鍵格納部 2 0 6 から公開鍵 P K \_\_ C A を読み出し、記録媒体 1 2 0 の C R L 記録領域 1 2 6 から、ドライブ部 2 1 8 を介して、無効化リスト C R L を読み出す。

次に、C R L 検証部 2 0 9 は、読み出した無効化リスト C R L から 1 個以上の証明書識別子と署名データ S i g I D とを抽出する。ここで、複数の証明書識別子が抽出された場合には、これらが無効化リスト C R L 内に配置されている順序で結合して結合値を生成する。また、1 個の証明書識別子のみが抽出された場合には、抽出された 1 個の証明書識別子を前記結合値とする。

10

【 0 0 8 9 】

次に、C R L 検証部 2 0 9 は、読み出した公開鍵 P K \_\_ C A を用いて、抽出した署名データ S i g I D と生成した前記結合値とに、署名検証アルゴリズム V r f y を施して、検証結果 R S L 3 を得る。検証結果 R S L 3 は、検証成功及び検証失敗のいずれかである。

得られた検証結果 R S L 3 が検証成功を示す場合には、C R L 検証部 2 0 9 は、読み出した無効化リスト C R L を署名検証部 2 1 2 及び C R L 比較更新部 2 1 0 へ出力する。

【 0 0 9 0 】

( 1 0 ) C R L 比較更新部 2 1 0

C R L 比較更新部 2 1 0 は、C R L 検証部 2 0 9 から無効化リスト C R L を受け取る。

無効化リスト C R L を受け取った場合に、C R L 比較更新部 2 1 0 は、受け取った無効化リスト C R L から版数を抽出し、C R L 格納部 2 0 8 から蓄積無効化リスト C R L \_\_ S T を読み出し、読み出した蓄積無効化リスト C R L \_\_ S T から版数を抽出する。次に、無効化リスト C R L から抽出した版数が、蓄積無効化リスト C R L \_\_ S T から抽出した版数より大きいか、否かを判断する。

20

【 0 0 9 1 】

無効化リスト C R L から抽出した版数が、蓄積無効化リスト C R L \_\_ S T から抽出した版数より大きいと判断した場合に、C R L 比較更新部 2 1 0 は、無効化リスト C R L の世代は、蓄積無効化リスト C R L \_\_ S T の世代より新しいとみなし、無効化リスト C R L を、蓄積無効化リスト C R L \_\_ S T として、C R L 格納部 2 0 8 に上書きする。

30

無効化リスト C R L から抽出した版数が、蓄積無効化リスト C R L \_\_ S T から抽出した版数より小さいか又は等しいと判断した場合に、無効化リスト C R L の世代は、蓄積無効化リスト C R L \_\_ S T の世代より古いか又は同じとみなされ、上記の上書きは行われない。

【 0 0 9 2 】

( 1 1 ) 証明書判定部 2 1 1

証明書判定部 2 1 1 は、C R L 格納部 2 0 8 から蓄積無効化リスト C R L \_\_ S T を読み出す。ここで、C R L 格納部 2 0 8 に記憶されている蓄積無効化リスト C R L \_\_ S T は、C R L 比較更新部 2 1 0 により、最新のものに更新されている。また、証明書判定部 2 1 1 は、記録媒体 1 2 0 の証明書記録領域 1 2 7 から、ドライブ部 2 1 8 を介して、公開鍵証明書 P K C を読み出す。

40

【 0 0 9 3 】

次に、証明書判定部 2 1 1 は、読み出した公開鍵証明書 P K C から証明書識別子 I D \_\_ 1 を抽出し、抽出した証明書識別子 I D \_\_ 1 が、蓄積無効化リスト C R L \_\_ S T に含まれているか否かを判断する。次に、判断結果 J D G をスイッチ 2 1 3 へ出力する。ここで、判断結果 J D G は、証明書識別子 I D \_\_ 1 が蓄積無効化リスト C R L \_\_ S T に含まれているか否かを示す情報である。

【 0 0 9 4 】

( 1 2 ) 署名検証部 2 1 2

50

署名検証部 212 は、鍵計算部 203 から鍵復号鍵 KDK を受け取る。また、記録媒体 120 の署名記録領域 125 から、ドライブ部 218 を介して、署名データ S i g C R L を読み出し、記録媒体 120 の証明書記録領域 127 から、ドライブ部 218 を介して、公開鍵証明書 P K C を読み出す。また、C R L 検証部 209 から無効化リスト C R L を受け取る。

【 0095 】

次に、署名検証部 212 は、読み出した公開鍵証明書 P K C から公開鍵 P K \_ 1 を抽出し、受け取った鍵復号鍵 KDK と受け取った無効化リスト C R L を結合して結合値 ( K D K | | C R L ) を生成し、抽出した公開鍵 P K \_ 1 を用いて、読み出した署名データ S i g C R L 及び生成した結合値 ( K D K | | C R L ) に署名検証アルゴリズム V r f y を施して、検証結果 R S L 1 を得る。検証結果 R S L 1 は、検証成功及び検証失敗のいずれかを示す情報である。

10

【 0096 】

次に、署名検証部 212 は、検証結果 R S L 1 をスイッチ 213 へ出力する。

( 13 ) スイッチ 213

スイッチ 213 は、復号部 205 から復号コンテンツ D C N T を受け取る。また、証明書判定部 211 から判断結果 J D G を受け取り、証明書検証部 207 から検証結果 R S L 2 を受け取り、署名検証部 212 から検証結果 R S L 1 を受け取る。

【 0097 】

受け取った検証結果 R S L 1 が検証成功を示し、かつ受け取った検証結果 R S L 2 が検証成功を示し、かつ受け取った判断結果 J D G が、証明書識別子 I D \_ 1 が蓄積無効化リスト C R L \_ S T に含まれていないことを示す場合に限り、スイッチ 213 は、受け取った復号コンテンツ D C N T を再生部 214 へ出力する。

20

受け取った検証結果 R S L 1 が検証失敗を示し、又は受け取った検証結果 R S L 2 が検証失敗を示し、又は受け取った判断結果 J D G が、証明書識別子 I D \_ 1 が蓄積無効化リスト C R L \_ S T に含まれていることを示す場合に、スイッチ 213 は、受け取った復号コンテンツ D C N T を再生部 214 へ出力しない。

【 0098 】

( 14 ) 再生部 214

再生部 214 は、スイッチ 213 から復号コンテンツ D C N T を受け取り、受け取った復号コンテンツ D C N T から映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモニタ 290 へ出力する。

30

【 0099 】

( 15 ) 制御部 215、入力部 216、表示部 217、ドライブ部 218、モニタ 290 及びリモコン 280

制御部 215 は、再生装置 200 を構成する各構成要素の動作を制御する。

リモコン 280 は、各種のボタンを備え、操作者の前記ボタンの操作に応じた操作指示情報を生成し、生成した操作指示情報を赤外線に乗せて出力する。

【 0100 】

40

入力部 216 は、リモコン 280 から、操作指示情報が乗せられた赤外線を受け取り、受け取った赤外線から操作指示情報を抽出し、抽出した操作指示情報を制御部 215 へ出力する。

表示部 217 は、制御部 215 の制御の基に、様々な情報を表示する。

ドライブ部 218 は、記録媒体 120 からの情報の読み出しを行う。

【 0101 】

モニタ 290 は、C R T 及びスピーカを備え、再生部 214 からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声信号に基づいて音声を出力する。

コンテンツ供給システム 10 の動作について、特に、記録装置 100 による記録媒体 120 へのデータの書き込みの動作及び再生装置 200 による記録媒体 120 に記録されているデータの再生の動作について、説明する。

【0102】

(1) 記録装置 100 による書き込みの動作

記録装置 100 による記録媒体 120 へのデータの書き込みの動作について、図 5 に示すフローチャートを用いて説明する。

鍵計算部 103 は、デバイス鍵格納部 101 及びメディア鍵データ格納部 102 から、それぞれ、デバイス鍵  $DK\_1$  及びメディア鍵データ  $MDATA$  を読み出し (ステップ S301)、次に、読み出したデバイス鍵  $DK\_1$  及びメディア鍵データ  $MDATA$  を用いて、メディア鍵  $MK$  を生成する (ステップ S302)。

10

【0103】

次に、鍵計算部 104 は、記録媒体 120 の固有番号記録領域 121 から媒体固有番号  $MID$  を読み出し (ステップ S303)、生成されたメディア鍵  $MID$  と読み出した媒体固有番号  $MID$  を用いて、鍵暗号化鍵  $KEK$  を算出する (ステップ S304)。

次に、暗号化部 105 は、算出された鍵暗号化鍵  $KEK$  を用いて、コンテンツサーバ装置 500 から取得したコンテンツ鍵  $CK$  を暗号化して、暗号化コンテンツ鍵  $ECK$  を生成する (ステップ S305)。

【0104】

次に、暗号化部 106 は、コンテンツサーバ装置 500 から取得したコンテンツ鍵  $CK$  を用いて、コンテンツサーバ装置 500 から取得したコンテンツ  $CNT$  を暗号化して暗号化コンテンツ  $ECNT$  を生成する (ステップ S306)。

20

次に、署名生成部 110 は、秘密鍵格納部 107 から秘密鍵  $SK\_1$  を読み出し (ステップ S307)、読み出した秘密鍵  $SK\_1$  を用いて、鍵暗号化鍵  $KEK$  及び無効化リスト  $CRL$  に対する署名データ  $Si g C R L$  を生成する (ステップ S308)。

【0105】

次に、記録装置 100 は、メディア鍵データ  $MDATA$ 、暗号化コンテンツ鍵  $ECK$ 、暗号化コンテンツ  $ECNT$ 、署名データ  $Si g C R L$ 、無効化リスト  $CRL$  及び公開鍵証明書  $PKC$  を、ドライブ部 111 を介して、記録媒体 120 に記録する (ステップ S309)。

30

(2) 再生装置 200 による再生の動作

再生装置 200 による記録媒体 120 に記録されているデータの再生の動作について、図 6 ~ 図 7 に示すフローチャートを用いて説明する。

【0106】

再生装置 200 は、記録媒体 120 から、メディア鍵データ  $MDATA$ 、媒体固有番号  $MID$ 、暗号化コンテンツ鍵  $ECK$ 、暗号化コンテンツ  $ECNT$ 、署名データ  $Si g C R L$ 、無効化リスト  $CRL$  及び公開鍵証明書  $PKC$  を読み出す (ステップ S401)。

次に、鍵計算部 202 は、デバイス鍵格納部 201 からデバイス鍵  $DK\_x$  を読み出し (ステップ S402)、読み出したメディア鍵データ  $MDATA$  及びデバイス鍵  $DK\_x$  を用いて、復号メディア鍵  $y$  を得る (ステップ S403)。

40

【0107】

次に、鍵計算部 203 は、読み出した媒体固有番号  $MID$  及び得られた復号メディア鍵  $y$  から鍵復号鍵  $KDK$  を算出する (ステップ S404)。

次に、復号部 204 は、算出された鍵復号鍵  $KDK$  を用いて、読み出した暗号化コンテンツ鍵  $ECK$  を復号して復号コンテンツ鍵  $DCK$  を得る (ステップ S405)。

次に、復号部 205 は、読み出した暗号化コンテンツ  $ECNT$  を、得られた復号コンテンツ鍵  $DCK$  を用いて、復号して、復号コンテンツ  $DCNT$  を得る (ステップ S406)。

。

【0108】

次に、証明書検証部 207 は、 $CA$  公開鍵格納部 206 から認証局  $CA$  の公開鍵  $PK\_$

50

CAを読み出し(ステップS407)、読み出した認証局CAの公開鍵PK\_CAを用いて、読み出した公開鍵証明書PKCの正当性を検証する(ステップS408)。

公開鍵証明書PKCの正当性の検証に失敗した場合には(ステップS409)、ステップS422へ制御が移る。公開鍵証明書PKCの正当性の検証に成功した場合には(ステップS409)、CRL検証部209は、認証局CAの公開鍵PK\_CAを用いて、読み出した無効化リストCRLの正当性を検証する(ステップS410)。

#### 【0109】

無効化リストCRLの正当性の検証に失敗した場合には(ステップS411)、ステップS422へ制御が移る。無効化リストCRLの正当性の検証に成功した場合には(ステップS411)、CRL比較更新部210は、CRL格納部208から蓄積無効化リストCRL\_STを読み出し(ステップS412)、記録媒体120から読み出した無効化リストCRLと、CRL格納部208から読み出した蓄積無効化リストCRL\_STとの新旧を比較する(ステップS413)。

#### 【0110】

CRL比較更新部210は、上記の比較の結果、無効化リストCRLの方が、蓄積無効化リストCRL\_STより新しいと判断される場合に(ステップS414)、新しいと判断した無効化リストCRLを蓄積無効化リストCRL\_STととして、CRL格納部208に上書きする(ステップS415)。無効化リストCRLの方が、蓄積無効化リストCRL\_STより古いと判断される場合(ステップS414)、ステップS416へ制御が移る。

#### 【0111】

次に、証明書判定部211は、CRL格納部208から蓄積無効化リストCRL\_STを読み出し(ステップS416)、読み出した公開鍵証明書PKCから抽出した証明書識別子ID\_1が、蓄積無効化リストCRL\_STに含まれているか否かを判断することにより、読み出した蓄積無効化リストCRL\_STに公開鍵証明書PKCが登録されているか否かを判定する(ステップS417)。

#### 【0112】

登録されていると判定された場合(ステップS418)、ステップS422へ制御が移る。登録されていないと判定された場合(ステップS418)、署名検証部212は、鍵復号鍵KDK、公開鍵証明書PKC及び無効化リストCRLを用いて、署名データSigCRLの正当性を検証する(ステップS419)。

署名データSigCRLの正当性の検証に失敗した場合(ステップS420)、スイッチ213は、開かれ、コンテンツは再生されず(ステップS422)、再生装置200の再生動作が終了する。

#### 【0113】

一方、署名データSigCRLの正当性の検証に成功した場合(ステップS420)、スイッチ213は、閉じられ、復号コンテンツDCNTを再生部214へ出力し、再生部214は、復号コンテンツDCNTを再生し(ステップS421)、再生装置200の再生動作が終了する。

#### 1.7 その他の変形例

(1)第1の実施の形態では、記録媒体を介して、無効化リストCRLを伝播する仕組みを実現するために、記録装置が、無効化リストCRLを署名対象として署名データSigCRLを生成し、生成した署名データSigCRLを記録媒体に書き込むとしているが、本発明は、この構成に限定されるものではない。

#### 【0114】

例えば、記録装置は、無効化リストCRLのハッシュ値を算出して、そのハッシュ値に対して署名データを生成するとしてもよい。

署名データ = Sig(SK\_1, HASH(CRL))

ここで、HASH(A)は、データAに対してハッシュ関数HASHを施して得られたハッシュ値である。

10

20

30

40

50

## 【 0 1 1 5 】

また、記録装置は、無効化リストCRLのハッシュ値を算出して、そのハッシュ値とメディア鍵MKをXOR（排他的論理和）演算し、その演算結果に対して署名データを生成するとしてもよい。

署名データ =  $Sig(SK\_1, (HASH(CRL)) XOR (MK))$

このように、記録装置は、無効化リストCRL及びコンテンツに対して署名データを生成したり、無効化リストCRL及び各種鍵データに対して署名データを生成したりし、生成した署名データを記録媒体に書き込むことにより、記録媒体上の無効化リストCRLの改ざんや削除を防止することができる。

## 【 0 1 1 6 】

また、これらの場合に、再生装置は、それぞれ、対応するデータを用いて、署名検証を行う。

(2) 第1の実施の形態では、外部から取得する無効化リストCRL及び内部に記憶している無効化リストCRLの新旧を比較する際に、バージョン番号を比較するとしているが、本発明は、この構成に限定されるものではない。

## 【 0 1 1 7 】

例えば、無効化リストCRLが更新されるにつれて、無効化リストCRLのサイズが単調に増加すると仮定できれば、CRLのサイズが大きい方を新しいと判断してもよい。

同様に、無効化リストCRLが更新されるにつれて、無効化される装置の数が単調に増加すると仮定できれば、無効化する装置の台数の比較により、無効化台数が多い方を新しいと判断してもよい。

## 【 0 1 1 8 】

以上のように、CRLから新旧比較できる情報を得ることができる構成であれば、如何なる構成であってもよい。

(3) 別の記録媒体を介して、メディア鍵データの最新版が、記録装置に対して、伝播する構成であってもよい。

前記別の記録媒体には、最新版のメディア鍵データが記録されている。

## 【 0 1 1 9 】

記録装置は、内部に予めメディア鍵データを保有している。メディア鍵データが記録されている前記別の記録媒体が装着されると、記録装置は、自身が保有しているメディア鍵データと、記録媒体に記録されているメディア鍵データとの新旧を比較し、自身が保有するメディア鍵データよりも、記録媒体に記録されているメディア鍵データの方が、新しければ、自ら保有しているメディア鍵データに代えて、記録媒体に記録されているメディア鍵データを内部に書き込む。

## 【 0 1 2 0 】

ここで、各メディア鍵データには、その世代を示すバージョン番号が付与されており、記録装置は、各バージョン番号を用いて、各メディア鍵データの新旧を比較する。

また、メディア鍵データから算出されるメディア鍵の一部はバージョン番号であり、残りの部分は、乱数を用いて生成されるとしてもよい。記録装置は、各メディア鍵データからメディア鍵の一部のバージョン番号を抽出し、抽出した各バージョン番号を用いて、各メディア鍵データの新旧を比較する。

## 【 0 1 2 1 】

また、メディア鍵データにおいて無効化されている装置の台数、つまり、メディア鍵MKに代えて値「0」が暗号化の対象となっている暗号化メディア鍵の数は、メディア鍵データの更新につれて、単調に増加すると仮定し、記録装置は、メディア鍵データに含まれている無効化されている装置の台数を用いて、各メディア鍵データの新旧を比較するとしてもよい。

## 【 0 1 2 2 】

また、各メディア鍵データには、当該メディア鍵データが生成された時刻情報（年月日時分秒）が付与されており、記録装置は、各時刻情報を用いて、各メディア鍵データの新

10

20

30

40

50

旧を比較するとしてもよい。

以上のように、メディア鍵データの新旧を正しく比較できる構成であれば、如何なる構成であってもよい。

【 0 1 2 3 】

また、各メディア鍵データには、改ざん防止のための認証局 C A の署名が付与されているとしてもよい。記録装置は、署名を検証することにより、メディア鍵データの正当性を確認する。

( 4 ) メディア鍵データ及び暗号化コンテンツ鍵などが予め記録されている記録媒体に対して、さらに、別の暗号化コンテンツ鍵を追加して書き込む場合に、記録装置は、自身が保有するメディア鍵データに基づいて、又は前記記録媒体に記録されているメディア鍵データに基づいて、外部（例えば、コンテンツサーバ装置）から取得したコンテンツ鍵を暗号化して、別の暗号化コンテンツ鍵を生成し、生成した別の暗号化コンテンツ鍵を前記記録媒体に書き込むとしてもよい。

10

【 0 1 2 4 】

この場合、前記記録媒体上には、複数のメディア鍵データ、複数の公開鍵証明書、複数の無効化リスト C R L が存在する場合がある。

また、記録装置は、前記記録媒体上のメディア鍵データと、記録装置が保有しているメディア鍵データとの新旧を比較し、記録装置が保有しているメディア鍵データの方が新しければ、前記記録媒体に記録されている暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を自身が保有する新しいメディア鍵に基づいて暗号化して、再暗号化コンテンツ鍵を生成し、生成した再暗号化コンテンツ鍵を前記記録媒体に書き込むとしてもよい。このとき、前記記録媒体に記録されている暗号化コンテンツ鍵を削除するとしてもよい。

20

【 0 1 2 5 】

( 5 ) 第 1 の実施の形態では、鍵暗号化鍵 K E K に対して、デジタル署名を施して署名データを生成するとしているが、本発明はこの構成に限定されるものではない。

例えば、コンテンツ C N T 全体のハッシュ値に対して、デジタル署名を施して署名データを生成するとしてもよい。

署名データ = S i g ( S K \_ 1 , ( H A S H ( C N T ) )

即ち、署名は、コンテンツを記録した記録装置の正当性の確認が目的であるため、署名の対象となるデータは、コンテンツに関連する情報や暗号化の際に用いる鍵に関連する情報であれば、如何なる情報であってもよい。

30

【 0 1 2 6 】

( 6 ) 第 1 の実施の形態では、記録装置 1 0 0 は、図 2 に示すように、デバイス鍵格納部 1 0 1、メディア鍵データ格納部 1 0 2、鍵計算部 1 0 3、鍵計算部 1 0 4、暗号化部 1 0 5、暗号化部 1 0 6、秘密鍵格納部 1 0 7、証明書格納部 1 0 8、C R L 格納部 1 0 9、署名生成部 1 1 0、ドライブ部 1 1 1、制御部 1 1 2 及び送受信部 1 1 3 から構成される一体の装置であるとしているが、本発明は、この構成には限定されない。

【 0 1 2 7 】

例えば、デバイス鍵格納部 1 0 1、メディア鍵データ格納部 1 0 2、鍵計算部 1 0 3、鍵計算部 1 0 4、暗号化部 1 0 5、暗号化部 1 0 6、秘密鍵格納部 1 0 7、証明書格納部 1 0 8、C R L 格納部 1 0 9、署名生成部 1 1 0、ドライブ部 1 1 1 及び制御部 1 1 2 の一部が一体となったドライブ装置から構成され、制御部 1 1 2 の他の一部及び送受信部 1 1 3 が一体となった処理装置から構成されているとしてもよい。この構成では、記録媒体に対するデータの読出 / 書込及び暗号処理を行うドライブ装置と、他の処理を行う処理装置とに分離している。

40

【 0 1 2 8 】

また、デバイス鍵格納部 1 0 1、メディア鍵データ格納部 1 0 2、秘密鍵格納部 1 0 7、証明書格納部 1 0 8 及び C R L 格納部 1 0 9 は、外部の記憶装置の記憶領域上に構成されているとしてもよい。ここで、前記外部の記憶装置の一例は、可搬型のセキュアなメモ

50

リカードである。

また、第1の実施の形態では、再生装置200は、図4に示すように、デバイス鍵格納部201、鍵計算部202、鍵計算部203、復号部204、復号部205、CA公開鍵格納部206、証明書検証部207、CRL格納部208、CRL検証部209、CRL比較更新部210、証明書判定部211、署名検証部212、スイッチ213、再生部214、制御部215、入力部216、表示部217及びドライブ部218から構成される一体の装置であるとしているが、本発明は、この構成には限定されない。

【0129】

デバイス鍵格納部201、鍵計算部202、鍵計算部203、復号部204、復号部205、CA公開鍵格納部206、証明書検証部207、CRL格納部208、CRL検証部209、CRL比較更新部210、証明書判定部211、署名検証部212、スイッチ213及びドライブ部218から構成される一体となったドライブ装置から構成され、再生部214、制御部215、入力部216及び表示部217から構成される一体となった処理装置から構成されているとしてもよい。この構成では、記録媒体に対するデータの読出/書込及び暗号処理を行うドライブ装置と、他の処理を行う処理装置とに分離している。

10

【0130】

また、デバイス鍵格納部201、CA公開鍵格納部206及びCRL格納部208は、外部の記憶装置の記憶領域上に構成されているとしてもよい。ここで、前記外部の記憶装置の一例は、可搬型のセキュアなメモリカードである。

20

以上のように、記録装置及び再生装置は、それぞれ、一体の装置ではなく、データ読出/書込装置及び処理装置の別々の構成であってもよい。この場合、データ読出/書込装置で暗号処理を行ってもよいし、処理装置で暗号処理を行ってもよい。

【0131】

(7)第1の実施の形態では、メディア鍵データMDATA、暗号化コンテンツ鍵ECK、暗号化コンテンツECNT、署名データSigCRL、無効化リストCRL及び公開鍵証明書PKCを全て同一の記録媒体に記録しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置100は、署名データSigCRL、無効化リストCRL、公開鍵証明書PKCなどのデータの一部を、記録媒体120とは別の記録媒体に記録し、記録媒体120及びこの別の記録媒体が配布されるとしてもよい。

30

【0132】

また、記録装置100は、インターネットを代表とするネットワークに接続されており、これらのデータの一部を、ネットワークを介して配布するとしてもよい。再生装置200も、ネットワークに接続されており、記録装置100から、ネットワークを介して、これらのデータの一部を取得する。

以上のように、メディア鍵データMDATA、暗号化コンテンツ鍵ECK、暗号化コンテンツECNT、署名データSigCRL、無効化リストCRL及び公開鍵証明書PKCが、1個以上の記録媒体に記録されて配布され、又は、1個以上の記録媒体に記録されかつネットワークを介して配布されるとしてもよい。

40

【0133】

(8)第1の実施の形態では、デバイス鍵に基づいて、コンテンツを暗号化し、また暗号化コンテンツを復号しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置及び再生装置が利用条件を取得しており、その利用条件に基づいて記録及び再生を制御する構成であってもよい。ここで、利用条件とは、コンテンツに付随する管理情報であり、例えば、コンテンツの記録及び再生を許可する日付、時間、又は回数である。

【0134】

(9)第1の実施の形態では、再生装置がCRL格納部から無効化リストCRLを読み出して新旧比較を行い、新しい無効化リストCRLをCRL格納部に格納し、公開鍵証明

50

書の登録有無の確認時に再度、無効化リストCRLを読み出すとしているが、本発明は、この構成に限定されるものではない。

例えば、再生装置は、無効化リストCRLの新旧比較を行うことなく、また、新しいと判断した無効化リストCRLをCRL格納部に格納することなく、公開鍵証明書が無効化リストCRLでの登録の有無を判定した後に、記録媒体120から読み出した無効化リストCRLをCRL格納部へ格納するとしてもよい。

【0135】

また、署名検証、CRL検証、公開鍵証明書判定の順序も、第1の実施の形態に記載の如く限定されず、再生装置は、種々の順序により、署名検証、CRL検証、公開鍵証明書判定を行い、コンテンツの再生を制御するとしてもよい。

(10)記録装置及び再生装置が電子透かしを生成して埋め込む電子透かし処理部を備える構成であってもよい。

【0136】

例えば、記録装置がその装置を特定する装置IDを記憶しており、コンテンツの記録媒体への記録時に、コンテンツに対して、その装置IDを電子透かしとして埋め込むとしてもよい。

このとき、装置IDが電子透かしとして埋め込まれたコンテンツが不正流出した場合に、コンテンツから、埋め込まれた装置IDを抽出することにより、そのコンテンツを記録した記録装置を特定することができる。

【0137】

また、同様に再生装置が再生時に、自身の装置IDを電子透かしとして、記録媒体上のコンテンツに埋め込む構成であってもよい。このとき、装置IDが埋め込まれたコンテンツが不正流出した場合に、コンテンツから、埋め込まれた装置IDを抽出することにより、そのコンテンツを再生した再生装置を特定することができる。

(11)コンテンツ供給システムは、暴露されたデバイス鍵を持つ不正装置が発見された場合に、内部に格納されているデバイス鍵を特定することができるデバイス鍵発見装置を含むとしてもよい。この不正装置は、再生装置200と同じ構成を有している。

【0138】

デバイス鍵発見装置は、図8に示すように、n枚の記録媒体MD1、MD2、MD3、・・・、MDnを生成する。なお、図8では、メディア鍵データ以外の他のデータについては、図示を省略している。

記録媒体MD1、MD2、MD3、・・・、MDnは、以下の点を除いて、第3に示す記録媒体120と同じ内容のデータを記録している。

【0139】

(a)記録媒体MD1、MD2、MD3、・・・、MDnに記録されている無効化リストCRLに登録されている無効化された公開鍵証明書はない。つまり、無効化リストCRLは、公開鍵証明書の識別子を含んでいない。

(b)記録媒体MD1、MD2、MD3、・・・、MDnに記録されている各メディア鍵データは、記録媒体120に記録されているメディア鍵データとは異なるものである。記録媒体MD1、MD2、MD3、・・・、MDnに記録されている各メディア鍵データの一例を図8に示す。

【0140】

(b-1)記録媒体MD1に記録されているメディア鍵データは、n個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第1の実施の形態において説明した通りである。

第1の暗号化メディア鍵は、デバイス鍵DK\_\_1を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

【0141】

第2、第3、・・・、第nの暗号化メディア鍵は、それぞれ、デバイス鍵DK\_\_2、DK\_\_3、・・・、DK\_\_nを用いて、値「0」に暗号化アルゴリズムE1を施して生成さ

10

20

30

40

50

れたものである。

(b-2) 記録媒体MD2に記録されているメディア鍵データは、n個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第1の実施の形態において説明した通りである。

【0142】

第1の暗号化メディア鍵は、デバイス鍵DK\_\_1を用いて、値「0」に暗号化アルゴリズムE1を施して生成されたものである。

第2の暗号化メディア鍵は、デバイス鍵DK\_\_2を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

第3、・・・、第nの暗号化メディア鍵は、それぞれ、デバイス鍵DK\_\_3、・・・、DK\_\_nを用いて、値「0」に暗号化アルゴリズムE1を施して生成されたものである。

10

【0143】

(b-3) 記録媒体MD3、・・・、MDnについて、上記と同様である。

整数i(1 ≤ i ≤ n)について、記録媒体MDiに記録されているメディア鍵データは、n個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第1の実施の形態において説明した通りである。

第iの暗号化メディア鍵は、デバイス鍵DK\_\_iを用いて、値「0」に暗号化アルゴリズムE1を施して生成されたものである。

【0144】

その他の暗号化メディア鍵は、対応するデバイス鍵を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

20

次に、操作者は、記録媒体MD1、MD2、MD3、・・・、MDnを一枚ずつ順に、不正装置に装着し、コンテンツの再生を不正装置に対して指示する。

こうして、n枚の記録媒体が不正装置により試される。

【0145】

不正装置によりコンテンツが正しく再生された場合に、装着された記録媒体により、不正装置が内蔵するであろうデバイス鍵を特定することができる。

例えば、記録媒体MD1が装着された場合に、不正装置によりコンテンツが正しく再生されたのであれば、不正装置が内蔵するデバイス鍵は、DK\_\_1である。

一般化して言うと、記録媒体MDiが装着された場合に、不正装置によりコンテンツが正しく再生されたのであれば、不正装置が内蔵するデバイス鍵は、DK\_\_iである。

30

【0146】

不正装置は、再生装置200と同じ構成を有しており、図6～図7に示すように動作するので、記録媒体MD1、MD2、MD3、・・・、MDnのいずれか一枚が装着された場合に限り、コンテンツを正しく再生する。

(12) 第1の実施の形態では、署名生成アルゴリズムとして、署名対象データにその署名を付与する付録型署名を用いるとしているが、本発明は、この構成に限定されるものではない。

【0147】

例えば、メッセージ付録型署名ではなく、メッセージ回復型署名を使用するとしてもよい。なお、メッセージ回復型署名については、特許文献3に開示されている。

40

メッセージ回復型署名では、署名者が、生成する署名に秘密情報を埋め込むことが可能であり、検証者が、署名検証後にその秘密情報を得ることが可能である。この特徴を利用して、記録装置は、秘密情報と鍵データ(例えばコンテンツ鍵)とにXOR演算(排他的論理和)を施し、演算結果に対して、メッセージ回復型署名を施して署名データを生成する。このとき、再生装置は、署名検証をし、検証が成功した場合に、前記演算結果を得、内蔵している秘密情報と演算結果に対して、XOR演算(排他的論理和)を施して、鍵データ(例えばコンテンツ鍵)を得る。

【0148】

なお、秘密情報と鍵データとの間の演算は、XOR演算に限定する必要はなく、加算演

50

算や、両データを結合したデータを入力値として、ハッシュ関数の出力値を利用する構成であってもよい。

また、秘密情報を作用させる情報は、コンテンツ鍵である必要はなく、鍵暗号化鍵などの他の鍵であってもよい。

【0149】

以上のように、署名検証することで得られる秘密情報を獲得しない限り、コンテンツの再生が行えない構成であれば如何なる構成であってもよい。このように、メッセージ回復型署名を利用することで、コンテンツの再生には署名検証が必須となる。

(13)第1の実施の形態では、コンテンツ鍵及びコンテンツは、記録装置の外部から取得するとしているが、本発明は、この構成に限定されるものではない。

10

【0150】

例えば、コンテンツ記録装置内部に、予めコンテンツ鍵及びコンテンツを対応付けて格納しているとしてもよい。また、コンテンツ鍵を、利用の都度、記録装置内部で生成するとしてもよい。

(14)第1の実施の形態では、種々の検証、並びに判定結果に基づいて制御されるスイッチ213は、復号部205と再生部214との間に備えられ、再生部214に対して復号コンテンツの出力を行うか否かを制御するとしているが、本発明は、この構成に限定されるものではない。

【0151】

例えば、スイッチ213は、復号部204と復号部205との間に備えられ、復号部205に対して復号コンテンツ鍵の出力を行うか否かを制御するとしてもよい。

20

また、スイッチ213は、鍵計算部203と復号部204との間に備えられ、復号部204に対して、鍵復号鍵KDKの出力を行うか否かを制御するとしてもよい。

このように、各検証の結果に基づき、最終的なコンテンツの再生を制御できる構成であれば如何なる構成であってもよい。さらに、スイッチ213は物理的なスイッチである必要はなく、再生制御を行える構成であれば、ソフトウェアによる構成であってもよい。

【0152】

また、鍵計算部202は、生成した復号メディア鍵yが、検知情報である値「0」であるか否かを判断し、復号メディア鍵yが値「0」であると判断する場合に、スイッチ213に対して、復号コンテンツDCNTを再生部214へ出力しないように指示するとしてもよい。

30

また、鍵計算部202は、復号メディア鍵yが値「0」であると判断する場合に、鍵計算部203、復号部204、復号部205の全て又はいずれかに対して、鍵復号鍵の生成、復号コンテンツ鍵の生成、復号コンテンツの生成を行わないように指示するとしてもよい。

【0153】

また、鍵計算部202は、復号メディア鍵yが値「0」であると判断する場合に、制御部215に対して、復号メディア鍵yが値「0」である旨のメッセージを通知し、制御部215は、前記メッセージを受け取ると、再生装置200を構成する他の構成要素に対して、暗号化コンテンツの復号及び再生を中止するように指示するとしてもよい。

40

(15)第1の実施の形態では、メディア鍵、鍵暗号化鍵及びコンテンツ鍵の3階層から暗号化システムを採用しているが、本発明は、この構成に限定されるものではない。

【0154】

例えば、コンテンツ鍵を省き、鍵暗号化鍵で直接コンテンツを暗号化する構成であってもよい。あるいは、新たな鍵を導入してその階層を1階層増やす構成であってもよい。

(16)記録装置又は再生装置は、インターネットに代表されるネットワークを介して、メディア鍵データ及び無効化リストCRLの最新版を取得し、内蔵するデータを更新する構成であってもよい。

【0155】

(17)第1の実施の形態では、記録装置が無効化リストCRLを記録媒体に記録する

50

としているが、本発明は、この構成に限定されるものではない。

例えば、再生装置は、無効化リストCRLを、ネットワークを介して取得するものとして、記録装置は、CRLを記録媒体に記録しない構成であってもよい。

(18)第1の実施の形態では、記録装置が、記録媒体に記録するコンテンツ又はコンテンツに関連する情報に対して署名データを生成し、生成した署名データを記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

【0156】

例えば、記録装置は、署名生成を行わないとしてもよい。このとき、記録装置は、自身が保有するメディア鍵データ及び媒体固有番号に基づいてコンテンツを暗号化して、暗号化に使用したメディア鍵データと、暗号化されたコンテンツを記録媒体に記録するとしてもよい。このとき、再生装置は、記録媒体からメディア鍵データ、媒体固有番号、及び暗号化コンテンツを読み出し、メディア鍵データ、及び媒体固有番号に基づいてコンテンツを復号する。

10

【0157】

(19)第1の実施の形態では、記録装置は、メディア鍵及び媒体固有番号から鍵暗号化鍵を生成することにより、メディアバインドを実現しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、メディア鍵及び媒体固有番号に基づいて認証子を生成して、生成した認証子を記録媒体に記録することにより、メディアバインドを実現するとしてもよい。このとき、再生装置は、同じく、メディア鍵及び媒体固有番号から認証子を生成し、記録媒体に記録された認証子と、生成した認証子が一致するか否かを判定してコンテンツの再生を制御する。

20

【0158】

上記の認証子の生成方法は、一例として、次の通りである。

メディア鍵、媒体固有番号及び暗号化コンテンツ鍵を結合した値に、ハッシュ関数を施し、得られたハッシュ値、又はハッシュ値の特定の一部を認証子とする。

(20)第1の実施の形態では、1枚の記録媒体は、1個のコンテンツ供給システムのみに対応しているが、本発明は、この構成に限定されるものではない。

【0159】

複数のコンテンツ供給システムが存在し、例えば、1のコンテンツ供給システムは、映画のコンテンツを供給するシステムである。別のコンテンツ供給システムは、コンピュータソフトウェアを供給するシステムである。さらに別のコンテンツ供給システムは、音楽を供給するシステムである。このように、供給されるコンテンツの種類により、異なるコンテンツ供給システムが用いられる。

30

【0160】

また、例えば、1のコンテンツ供給システムは、映画供給業者Aにより、映画のコンテンツを供給するシステムである。別のコンテンツ供給システムは、映画供給業者Bにより、映画のコンテンツを供給するシステムである。さらに別のコンテンツ供給システムは、映画供給業者Cにより、映画のコンテンツを供給するシステムである。このように、コンテンツの供給者により、異なるコンテンツ供給システムが用いられることもある。

40

【0161】

ここでは、1枚の記録媒体が、異なる複数のコンテンツ供給システムにおいて利用される仕組みについて、説明する。

記録媒体の書き換え不可領域には、記録媒体に固有の媒体固有番号に加え、鍵の無効化データが予め記録されている。このとき、第1のコンテンツ供給システムは、予め書き換え不可領域に記録されている鍵の無効化データを使用することにより、著作物保護の仕組みを実現する。また、第2のコンテンツ供給システムは、第1の実施の形態に示した構成で、著作物保護の仕組みを実現する。

【0162】

図9に、前記記録媒体に記録されるデータの一例を示す。

50

記録媒体 700 には、書き換え不可領域 710 と、書き換え可能領域 720 が存在し、書き換え不可領域 710 には、第 1 のコンテンツ供給システム用の鍵無効化データ記録領域 711 と、固有番号記録領域 712 が存在する。また、書き換え可能領域 720 には、第 2 のコンテンツ供給システム用の鍵無効化データ記録領域 721 と、第 1 の暗号化コンテンツ鍵記録領域 722 と、第 2 の暗号化コンテンツ鍵記録領域 723 と、その他の暗号化コンテンツ記録領域（図示していない）とが存在する。

【0163】

ここで、第 2 のコンテンツ供給システム用の鍵無効化データ記録領域 721 は、第 1 の実施の形態におけるメディア鍵データ記録領域 122 に相当する。さらに、第 1 の暗号化コンテンツ鍵記録領域 722 には、第 1 のコンテンツ供給システム用の鍵無効化データに基づいて暗号化されたデータが記録され、同様に、第 2 の暗号化コンテンツ鍵記録領域 723 には、第 2 のコンテンツ供給システム用の鍵無効化データに基づいて暗号化されたデータが記録される。

10

【0164】

このように、1 つの記録媒体が複数のコンテンツ供給システムをサポートする場合、媒体固有番号はシステムごとに複数存在する必要はなく、記録媒体に唯一でよく、各コンテンツ供給システムが同一の媒体固有番号、あるいはその一部分を共通に使用する構成であってもよい。

ここで、媒体固有番号の一部を使用するとは、例えば 128 ビットの媒体固有番号が存在した場合に、上位 32 ビットは使用せず、下位 96 ビットを媒体固有番号として使用したり、媒体固有番号の上位 32 ビットをオール 0 に置き換え、128 ビットの媒体固有番号として使用したりすることを意味する。

20

【0165】

以上のように、記録媒体に予め記録されている媒体固有番号を複数のコンテンツ供給システムで共通に使用することにより、既に市販され利用されている媒体固有番号のみを記録した記録媒体においても、著作物の著作権を保護することができるシステムの実現が可能となる。また、システムごとに媒体固有番号を記録する必要がないことにより、書き換え不可領域の容量削減も可能である。

【0166】

以上のように、本発明は、少なくとも第 1 及び第 2 のコンテンツ供給システムに対して著作物保護の仕組みを提供する著作物保護システムである。

30

記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号と、第 1 のコンテンツ供給システム用に鍵無効化データとが予め記録されている。

【0167】

第 1 のコンテンツ供給システムは、前記記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成されている。前記複数の再生装置のうちいずれか 1 台以上は、無効化されている。前記記録媒体の前記書換不可領域に記録されている前記鍵無効化データは、前記無効化された再生装置の鍵を示している。

40

【0168】

前記記録装置は、前記書換不可領域に記録されている前記無効化データを用いて、コンテンツを暗号化する暗号化部と、生成した暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込部とを備える。

前記再生装置は、前記記録媒体の前記書換不可領域に記録されている前記鍵無効化データと、前記記録媒体に記録されている前記暗号化コンテンツを読み出す読出部と、読み出した前記鍵無効化データを用いて、前記暗号化コンテンツの復号を許可するか否かを判断する判断部と、復号が許可されない場合に、前記暗号化コンテンツの復号を禁止し、復号が許可される場合に、前記暗号化コンテンツを復号して、復号コンテンツを生成する復号部とを備える。

50

## 【0169】

また、第2のコンテンツ供給システムは、前記記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成されている。前記複数の再生装置のうちいずれか1台以上は、無効化されている。

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶部と、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出部と、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成部と、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化部と、前記記憶部から前記メディア鍵データを読み出す読出部と、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込部とを備える。

10

## 【0170】

各再生装置は、前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出部と、当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号部と、生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御部と、復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号部とを備える。

20

## 【0171】

## 1.8 まとめ

以上説明したように、本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体から暗号化コンテンツを読み出して復号する再生装置からなる著作権保護システムである。

前記記録装置は、特定装置が保有する鍵を無効化するための無効化データを保持して、前記無効化データに基づいて前記コンテンツを暗号化して、前記記録媒体に、前記無効化データ、並びに前記暗号化コンテンツを記録して、さらに、前記コンテンツ、あるいは前記コンテンツの暗号化に関連するデータに対して署名を生成して、前記生成した署名を前記記録媒体に記録する。

30

## 【0172】

前記記録媒体は、ユーザにより書き換えできない領域に、前記記録媒体を一意に識別する識別番号を記録して、さらに、前記無効化データ、前記暗号化コンテンツ、並びに前記署名を記録する。

前記再生装置は、前記記録媒体から、前記無効化データ、前記暗号化コンテンツ、並びに前記署名を読み出して、前記無効化データに基づいて前記コンテンツを復号して、前記署名の正当性を検証した結果に基づいて、前記復号したコンテンツの再生を制御するとしてもよい。

40

## 【0173】

ここで、前記著作権保護システムにおいて、前記記録媒体は、前記無効化データ、並びに前記暗号化コンテンツを記録して、前記署名は、前記記録媒体とは異なる記録媒体、あるいは通信媒体を介して配布されるとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、2つ以上の装置の組み合わせで処理を行い、前記装置ごとに処理を分担するとしてもよい。

## 【0174】

ここで、前記著作権保護システムにおいて、前記再生装置は、2つ以上の装置の組み合

50

わせで処理を行い、前記装置ごとに処理を分担するとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、コンテンツの利用条件に基づいてコンテンツを記録するとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、コンテンツの利用条件に基づいてコンテンツを再生するとしてもよい。

【0175】

ここで、前記著作権保護システムにおいて、前記記録装置は、前記記録装置を一意に識別する装置特定番号を保持して、コンテンツの記録に際して、前記装置特定番号を電子透かしとして前記コンテンツに埋め込むとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、前記再生装置を一意に識別する装置特定番号を保持して、コンテンツの再生に際して、前記装置特定番号を電子透かしとして前記コンテンツに埋め込むとしてもよい。

【0176】

ここで、前記著作権保護システムにおいて、不正装置が発見された際に、前記不正装置が保有する鍵の種類を判定する鍵発見装置を含むとしてもよい。

また、本発明は、コンテンツを暗号化して記録する記録装置である。前記記録装置は、特定装置が保有する鍵を無効化するための無効化データを保持して、前記無効化データに基づいて前記コンテンツを暗号化して、記録媒体に、前記無効化データ、並びに前記暗号化コンテンツを記録して、さらに、前記コンテンツ、あるいは前記コンテンツの暗号化に関連するデータに対して署名を生成して、前記生成した署名を前記記録媒体に記録する。

【0177】

ここで、前記記録装置は、前記無効化データに加えて、前記記録媒体を一意に識別する識別番号に基づいて前記コンテンツを暗号化するとしてもよい。

ここで、前記記録装置は、前記署名の生成に使用した秘密鍵に対応する公開鍵を前記記録媒体に記録するとしてもよい。

ここで、前記記録装置は、公開鍵の無効化リストを署名対象として署名生成を行うとしてもよい。

【0178】

ここで、前記記録装置は、前記コンテンツを記録する記録媒体に無効化データが存在する場合に、前記記録装置が保有する無効化データと、前記記録媒体に存在する無効化データの新旧を比較して、新しい無効化データを保有するとしてもよい。

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化データのサイズの比較で行い、サイズの大きい無効化データを新しいと判断するとしてもよい。

【0179】

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化している鍵数の比較で行い、無効化している鍵数が多い無効化データを新しいと判断するとしてもよい。

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化データの生成日、あるいはバージョン番号の比較で行い、前記生成日、あるいは前記バージョン番号は、改ざんから保護されているとしてもよい。

【0180】

ここで、前記記録装置は、前記コンテンツを記録する記録媒体に無効化データ、並びに暗号化コンテンツが存在して、かつ、前記記録装置が保有する無効化データが、前記記録媒体に記録されている無効化データと比較して新しい場合に、前記記録媒体に記録された前記暗号化コンテンツを、同様に、前記記録媒体に記録された無効化データに基づいて一旦復号して、前記記録装置が保有する無効化データに基づいて再暗号化するとしてもよい。

【0181】

ここで、前記記録装置は、前記記録装置内部で秘密情報を生成して、前記秘密情報と前記無効化データに基づいて前記コンテンツを暗号化して、前記秘密情報を署名に埋め込む情報として署名を生成するとしてもよい。

10

20

30

40

50

また、本発明は、記録媒体から暗号化コンテンツを読み出して復号する再生装置である。前記再生装置は、前記記録媒体から、無効化データ、前記暗号化コンテンツ、並びに署名を読み出して、前記無効化データに基づいて前記コンテンツを復号して、前記署名の正当性を検証した結果に基づいて、前記復号したコンテンツの再生を制御する。

【0182】

ここで、前記再生装置は、前記無効化データに加えて、前記記録媒体を一意に識別する識別番号に基づいて前記暗号化コンテンツを復号するとしてもよい。

ここで、前記再生装置は、公開鍵の無効化リストを保有して、前記無効化リストを使用して、前記署名の正当性の検証に使用する公開鍵が、前記無効化リストに登録されているか否かを判断して、前記判断した結果に基づいて、前記復号したコンテンツの再生を制御するとしてもよい。

10

【0183】

ここで、前記再生装置は、前記記録媒体に前記無効化リストが存在する場合に、前記再生装置が保有する無効化リストと、前記記録媒体に存在する無効化リストの新旧を比較して、新しい無効化リストを保有するとしてもよい。

ここで、前記再生装置は、前記無効化リストの新旧の比較を、無効化リストのサイズの比較で行い、サイズの大きい無効化リストを新しいと判断するとしてもよい。

【0184】

ここで、前記再生装置は、前記無効化リストの新旧の比較を、無効化している公開鍵数の比較で行い、無効化している公開鍵数が多い無効化リストを新しいと判断するとしてもよい。

20

ここで、前記再生装置は、前記署名の正当性の検証を行うことにより秘密情報を獲得して、前記獲得した秘密情報、並びに無効化データに基づいて、前記暗号化コンテンツを復号するとしてもよい。

【0185】

また、本発明は、暗号化コンテンツを記録する記録媒体である。前記記録媒体は、ユーザにより書き換えできない領域に、前記記録媒体を一意に識別する識別番号を記録して、さらに、無効化データ、暗号化コンテンツ、並びに署名を記録している。

ここで、前記記録媒体は、前記無効化データ、並びに識別番号に基づいて暗号化されたコンテンツを記録しているとしてもよい。

30

【0186】

ここで、前記記録媒体は、前記署名の生成に使用した秘密鍵に対応する公開鍵を記録しているとしてもよい。

ここで、前記記録媒体は、2つ以上の記録装置により記録された場合に、2つ以上の無効化データ、並びに2つ以上の公開鍵を記録しているとしてもよい。

以上、説明したように、第1の実施の形態においては、記録装置が、メディア鍵データから算出されるメディア鍵に基づいてコンテンツを暗号化し、かつ記録装置自身の公開鍵証明書及び生成した署名を合わせて記録媒体に記録することで、記録媒体の書き換え不可領域に鍵無効化情報が記録されていない記録媒体であっても、鍵無効化及びメディアバインドを実現して、不正装置を使ったコンテンツの記録又は再生による著作物侵害の防止を実現することができる。

40

【0187】

具体的には、正規の記録装置及び不正な再生装置が存在する場合、正規の記録装置は、不正な再生装置の無効化を示すメディア鍵データに基づいてコンテンツを暗号化して記録媒体に記録する。その記録媒体を挿入した不正な再生装置は、記録されているメディア鍵データからはメディア鍵を復号することができないため、不正な再生装置によるコンテンツの再生を防止できる。

【0188】

また、不正な記録装置及び正規の再生装置が存在する場合、不正な記録装置は、自身が無効化されていない古いメディア鍵データに基づいてコンテンツを暗号化して記録媒体に

50

記録する。このとき、記録装置自身の公開鍵証明書及び生成した署名データも記録する。その記録媒体を挿入した正規の再生装置は、記録されているメディア鍵データからメディア鍵を復号することができる。しかし、コンテンツの再生前に記録装置の公開鍵証明書が無効化リストCRLに登録されているか否かを判断するため、無効化リストCRLに登録されている不正な記録装置により記録されたコンテンツであれば、その再生を止めることができる。

#### 【0189】

##### 2. 第2の実施の形態

本発明に係る別の実施の形態としてのコンテンツ供給システム20について説明する。

##### 2.1 コンテンツ供給システム20の構成

コンテンツ供給システム20は、コンテンツ供給システム10と類似した構成を有しており、図10に示すように、配信局装置1400、コンテンツサーバ装置1500、記録装置1100及び再生装置1200a、1200b、1200c、1200d、1200e、・・・から構成されている。

#### 【0190】

第1の実施の形態と同様に、再生装置のうちの一部は、無効化されている。

##### 2.2 配信局装置1400

配信局装置1400は、情報記憶部1401、制御部1402、入力部1403、表示部1404及び送受信部1405から構成されている(図示していない)。

配信局装置1400は、具体的には、第1の実施の形態のコンテンツサーバ装置500と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、通信ユニット、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又は前記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従って動作することにより、配信局装置1400の各構成要素は、その機能を達成する。

#### 【0191】

送受信部1405は、インターネット40を介して、記録装置1100と接続されており、記録装置1100と制御部1402との間で情報の送受信を行う。

情報記憶部1401は、鍵無効化データRDATAとバージョン番号VRとを対応付けて予め記憶している。

鍵無効化データRDATAは、第1の実施の形態のメディア鍵データMDATAと同一である。ここでは、詳細の説明を省略する。

#### 【0192】

バージョン番号VRは、当該バージョン番号VRに対応する鍵無効化データRDATAの世代を示す情報である。

制御部1402は、記録装置1100から、インターネット40及び送受信部1405を介して、鍵無効化データRDATAの取得要求を受け取る。前記取得要求を受け取ると、制御部1402は、情報記憶部1401から、鍵無効化データRDATAとバージョン番号VRとを読み出し、読み出した鍵無効化データRDATAとバージョン番号VRとを、送受信部1405及びインターネット40を介して、記録装置1100へ送信する。

#### 【0193】

入力部1403は、配信局装置1400の操作者の指示を受け付け、受け付けた指示を制御部1402へ出力する。

表示部1404は、制御部1402の制御により、様々な情報を表示する。

##### 2.3 コンテンツサーバ装置1500

コンテンツサーバ装置1500は、第1の実施の形態のコンテンツサーバ装置500と同一の構成を有している。ここでは、説明を省略する。

#### 【0194】

##### 2.4 記録装置1100

記録装置1100は、図11に示すように、デバイス鍵格納部1101、無効化データ

10

20

30

40

50

格納部 1102、鍵計算部 1103、暗号化部 1105、暗号化部 1106、認証子生成部 1104、割当部 1107、比較部 1108、制御部 1109、ドライブ部 1110 及び送受信部 1111 から構成されている。

【0195】

記録装置 1100 は、具体的には、記録装置 100 と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニット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 又は前記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従って動作することにより、記録装置 1100 は、その機能を達成する。

【0196】

(1) デバイス鍵格納部 1101

デバイス鍵格納部 1101 は、外部の装置からアクセスできないように、デバイス鍵 DK\_\_1 を秘密に記憶している。デバイス鍵 DK\_\_1 は、記録装置 1100 に固有の鍵である。

(2) 無効化データ格納部 1102

無効化データ格納部 1102 は、配信局装置 1400 から取得した鍵無効化データ RDATA とバージョン番号 VR とを記憶するための領域を有している。

【0197】

(3) 鍵計算部 1103

鍵計算部 1103 は、第 1 の実施の形態の鍵計算部 103 と同様の構成を有している。鍵計算部 1103 は、無効化データ格納部 1102 から鍵無効化データ RDATA を読み出し、デバイス鍵格納部 1101 からデバイス鍵 DK\_\_1 を読み出す。次に、鍵計算部 103 と同様に、読み出したデバイス鍵 DK\_\_1 を用いて、読み出した鍵無効化データ RDATA に復号アルゴリズム D1 を施してメディア鍵 MK を生成し、生成したメディア鍵 MK を認証子生成部 1104 及び暗号化部 1105 へ出力する。

【0198】

(4) 暗号化部 1105

暗号化部 1105 は、コンテンツサーバ装置 1500 から、送受信部 1111 を介して、コンテンツ鍵 CK を受け取り、鍵計算部 1103 からメディア鍵 MK を受け取る。

次に、暗号化部 1105 は、受け取ったメディア鍵 MK を用いて、受け取ったコンテンツ鍵 CK に暗号化アルゴリズム E2 を施して、暗号化コンテンツ鍵 ECK を生成する。

【0199】

暗号化コンテンツ鍵  $ECK = E2(MK, CK)$

次に、暗号化部 1105 は、ドライブ部 1110 を介して、記録媒体 1300 上の暗号化コンテンツファイル 1320 内に鍵記録部 1323 を確保し、次に、生成した暗号化コンテンツ鍵 ECK を、ドライブ部 1110 を介して、鍵記録部 1323 へ書き込む。

また、暗号化部 1105 は、生成した暗号化コンテンツ鍵 ECK を認証子生成部 1104 へ出力する。

【0200】

(5) 暗号化部 1106

暗号化部 1106 は、コンテンツサーバ装置 1500 から、送受信部 1111 を介して、コンテンツ鍵 CK 及びコンテンツ CNT を受け取り、受け取ったコンテンツ鍵 CK を用いて、受け取ったコンテンツ CNT に暗号化アルゴリズム E3 を施して暗号化コンテンツ ECNT を生成する。

【0201】

暗号化コンテンツ  $ECNT = E3(CK, CNT)$

次に、暗号化部 1106 は、ドライブ部 1110 を介して、記録媒体 1300 上の暗号化コンテンツファイル 1320 内にコンテンツ記録部 1324 を確保し、次に、生成した暗号化コンテンツ ECNT を、ドライブ部 1110 を介して、コンテンツ記録領域 124 へ書き込む。

10

20

30

40

50

【 0 2 0 2 】

( 6 ) 認証子生成部 1 1 0 4

認証子生成部 1 1 0 4 は、鍵計算部 1 1 0 3 からメディア鍵 M K を受け取り、暗号化部 1 1 0 5 から暗号化コンテンツ鍵 E C K を受け取り、記録媒体 1 3 0 0 の固有番号記録領域 1 3 0 1 から媒体固有番号 M I D を読み出す。

次に、認証子生成部 1 1 0 4 は、受け取ったメディア鍵 M K と、読み出した媒体固有番号 M I D と、受け取った暗号化コンテンツ鍵 E C K とをこの順序で結合して、結合データを生成し、生成した結合データに一方方向性関数 F を施して、認証子 M A C ( Message Authentication Code ) を生成する。

【 0 2 0 3 】

$$M A C = F ( M K \parallel E C K \parallel M I D )$$

ここで、F ( A ) は、データ A に対して一方方向性関数 F を施して得られた値を示している。また、一方方向性関数 F の一例は、ハッシュ関数 S H A - 1 である。

次に、認証子生成部 1 1 0 4 は、ドライブ部 1 1 1 0 を介して、記録媒体 1 3 0 0 上の暗号化コンテンツファイル 1 3 2 0 内に認証子記録部 1 3 2 2 を確保し、生成した認証子 M A C を、ドライブ部 1 1 1 0 を介して、認証子記録部 1 3 2 2 に書き込む。

【 0 2 0 4 】

このようにして生成された認証子 M A C は、再生装置 1 2 0 0 においてコンテンツの正当性を判定する際に用いられる。

( 7 ) 割当部 1 1 0 7

割当部 1 1 0 7 は、記録媒体 1 3 0 0 に記録する鍵無効化データ R D A T A に対して、記録媒体 1 3 0 0 においてその鍵無効化データ R D A T A を一意に識別する鍵無効化データ識別子 R I D を生成する。次に、ドライブ部 1 1 1 0 を介して、記録媒体 1 3 0 0 上の暗号化コンテンツファイル 1 3 2 0 内に識別子記録部 1 3 2 1 を確保し、生成した鍵無効化データ識別子 R I D を、ドライブ部 1 1 1 0 を介して、識別子記録部 1 3 2 1 に書き込む。

【 0 2 0 5 】

なお、割当部 1 1 0 7 による鍵無効化データ識別子 R I D の具体的な割当方法については後述する。

( 8 ) 比較部 1 1 0 8

比較部 1 1 0 8 は、制御部 1 1 0 9 の指示により、ドライブ部 1 1 1 0 を介して、記録媒体 1 3 0 0 に鍵無効化データファイルが存在するか否かを確認する。次に、ドライブ部 1 1 1 0 から鍵無効化データファイルが存在するか否かを示す存否情報を受け取る。

【 0 2 0 6 】

受け取った存否情報が、記録媒体 1 3 0 0 に鍵無効化データファイルが存在しないことを示す場合には、比較部 1 1 0 8 は、割当部 1 1 0 7 に対して、鍵無効化データ識別子 R I D の生成を指示し、また、ドライブ部 1 1 1 0 に対して、無効化データ格納部 1 1 0 2 に記録されている鍵無効化データ R D A T A と、そのバージョン番号 V R と、割当部 1 1 0 7 により生成された鍵無効化データ識別子 R I D とから構成される鍵無効化データファイルを記録媒体 1 3 0 0 に書き込むように指示する。

【 0 2 0 7 】

前記存否情報が、記録媒体 1 3 0 0 に鍵無効化データファイルが存在することを示す場合には、比較部 1 1 0 8 は、ドライブ部 1 1 1 0 を介して、記録媒体 1 3 0 0 上の各鍵無効化データファイルから鍵無効化データ F D A T A に含まれているバージョン番号 V F を読み出す。この場合に、1 個以上のバージョン番号 V F が読み出される。また、無効化データ格納部 1 1 0 2 から鍵無効化データ R D A T A に対応するバージョン番号 V R を読み出す。

【 0 2 0 8 】

次に、比較部 1 1 0 8 は、読み出したバージョン番号 V R と同じ内容のバージョン番号が、読み出した 1 個以上のバージョン番号 V F の中に存在するか否かを判断し、存在しな

10

20

30

40

50

いと判断する場合に、上記と同様に、割当部 1 1 0 7 に対して、鍵無効化データ識別子 R I D の生成を指示し、また、ドライブ部 1 1 1 0 に対して、無効化データ格納部 1 1 0 2 に記録されている鍵無効化データ R D A T A と、そのバージョン番号 V R と、割当部 1 1 0 7 により生成された鍵無効化データ識別子 R I D とから構成される鍵無効化データファイルを記録媒体 1 3 0 0 に書き込むように指示する。

【 0 2 0 9 】

存在すると判断する場合に、比較部 1 1 0 8 は、読み出したバージョン番号 V R と同じ内容のバージョン番号が存在することを示す情報を制御部 1 1 0 9 へ出力する。

( 9 ) 制御部 1 1 0 9

制御部 1 1 0 9 は、送受信部 1 1 1 1 及びインターネット 4 0 を介して、配信局装置 1 4 0 0 に対して、鍵無効化データ R D A T A の取得要求を送信する。また、制御部 1 1 0 9 は、送受信部 1 1 1 1 を介して、コンテンツサーバ装置 1 5 0 0 に対して、コンテンツの取得要求を送信する。

【 0 2 1 0 】

制御部 1 1 0 9 は、比較部 1 1 0 8 に対して、記録媒体 1 3 0 0 に鍵無効化データファイルが存在するか否かを確認するように指示する。

比較部 1 1 0 8 からバージョン番号 V R と同じ内容のバージョン番号が存在することを示す情報を受け取った場合には、ドライブ部 1 1 1 0 に対して、記録媒体 1 3 0 0 上において、バージョン番号 V R と同じ内容のバージョン番号を含む鍵無効化データファイルから鍵無効化データ識別子 R I D を読み出すように指示し、ドライブ部 1 1 1 0 から鍵無効化データ識別子 R I D を受け取る。

【 0 2 1 1 】

次に、制御部 1 1 0 9 は、鍵計算部 1 1 0 3 に対して、デバイス鍵 D K \_ 1 と鍵無効化データ R D A T A とを読み出してメディア鍵 M K を生成するように指示し、暗号化部 1 1 0 5 に対して、コンテンツ鍵 C K を暗号化するように指示し、認証子生成部 1 1 0 4 に対して、媒体固有番号 M I D を読み出して、認証子 M A C を生成するように指示し、暗号化部 1 1 0 6 に対して、コンテンツ C N T を暗号化するように指示し、次に、ドライブ部 1 1 1 0 に対して、記録媒体 1 3 0 0 上に暗号化コンテンツファイルを確保するように指示し、認証子生成部 1 1 0 4、暗号化部 1 1 0 5 及び暗号化部 1 1 0 6 に対して、それぞれ、生成された認証子 M A C と、生成された暗号化コンテンツ鍵 E C K と、生成された暗号化コンテンツ E C N T とを記録媒体 1 3 0 0 上の暗号化コンテンツファイル内に書き込むように指示する。また、ドライブ部 1 1 1 0 に対して、記録媒体 1 3 0 0 上の暗号化コンテンツファイル内に、識別子記録部 1 3 0 3 を確保するように指示し、割当部 1 1 0 7 により生成された又はドライブ部 1 1 1 0 から受け取った鍵無効化データ識別子 R I D を識別子記録部 1 3 0 3 に書き込むように指示する。

【 0 2 1 2 】

( 1 0 ) 送受信部 1 1 1 1

送受信部 1 1 1 1 は、インターネット 4 0 を介して、配信局装置 1 4 0 0 と接続されている。また、専用回線 3 0 を介して、コンテンツサーバ装置 1 5 0 0 と接続されている。

送受信部 1 1 1 1 は、配信局装置 1 4 0 0 から、インターネット 4 0 を介して、鍵無効化データ R D A T A とバージョン番号 V R とを受信する。鍵無効化データ R D A T A とバージョン番号 V R とを受信すると、受信した鍵無効化データ R D A T A 及びバージョン番号 V R を、対応付けて、無効化データ格納部 1 1 0 2 へ書き込む。

【 0 2 1 3 】

また、送受信部 1 1 1 1 は、専用回線 3 0 を介して、コンテンツサーバ装置 1 5 0 0 から、コンテンツ鍵 C K 及びコンテンツ C N T を受信し、受信したコンテンツ鍵 C K 及びコンテンツ C N T を暗号化部 1 1 0 6 へ出力し、受信したコンテンツ鍵 C K を暗号化部 1 1 0 5 へ出力する。

( 1 1 ) ドライブ部 1 1 1 0

ドライブ部 1 1 1 0 は、記録装置 1 1 0 0 を構成する各構成要素の指示により、記録媒

10

20

30

40

50

体 1 3 0 0 から情報を読み出し、読み出した情報を当該構成要素へ出力する。

【 0 2 1 4 】

また、ドライブ部 1 1 1 0 は、記録装置 1 1 0 0 を構成する各構成要素の指示により、記録媒体 1 3 0 0 に各領域を確保し、また、各構成要素から情報を受け取り、確保した領域に受け取った前記情報を書き込む。

( 1 2 ) キーボード 1 1 8 0 及びモニタ 1 1 9 0

キーボード 1 1 8 0 は、記録装置 1 1 0 0 の操作者の操作指示を受け付け、受け付けた操作指示に対応する指示情報を制御部 1 1 0 9 へ出力する。

【 0 2 1 5 】

モニタ 1 1 9 0 は、制御部 1 1 0 9 の制御により様々な情報を表示する。

10

2 . 5 記録媒体 1 3 0 0

記録媒体 1 3 0 0 は、記録媒体 1 2 0 と同様に、光ディスクメディアであり、図 1 2 に示すように、書換不可領域 1 3 0 8 と、書換可能領域 1 3 0 9 とから構成されている。

書換不可領域 1 3 0 8 は、図 1 2 に示すように、固有番号記録領域 1 3 0 1 を有している。記録媒体 1 3 0 0 の製造時に、固有番号記録領域 1 3 0 1 には、記録媒体 1 3 0 0 に固有の媒体固有番号 M I D が記録される。このとき、書換可能領域 1 3 0 9 には、何も記録されていない。この図では、媒体固有番号 M I D は 1 6 進数 8 桁で表現されており、具体的には、「 5 」である。

【 0 2 1 6 】

その後、上述したように、記録装置 1 1 0 0 により記録媒体 1 3 0 0 上に情報が書き込まれると、書換可能領域 1 3 0 9 には、記録装置 1 1 0 0 により記録領域 1 3 0 5 と記録領域 1 3 0 6 とが確保され、記録領域 1 3 0 5 には、1 個以上の鍵無効化データファイルが記録され、記録領域 1 3 0 6 には、1 個以上の暗号化コンテンツファイルが記録される。

20

【 0 2 1 7 】

一例として、図 1 2 に示すように、記録領域 1 3 0 5 には、鍵無効化データファイル 1 3 1 0 が記録され、記録領域 1 3 0 6 には、暗号化コンテンツファイル 1 3 2 0 が記録される。なお、図 1 2 に示す記録媒体 1 3 0 0 には、一例として、1 個の鍵無効化データファイルと 1 個の暗号化コンテンツファイルとが記録されているが、1 個以上の鍵無効化データファイルと 1 個以上の暗号化コンテンツファイルとが記録媒体上に記録されることも

30

【 0 2 1 8 】

鍵無効化データファイル 1 3 1 0 は、図 1 2 に示すように、版数記録部 1 3 1 1、識別子記録部 1 3 1 2 及びデータ記録部 1 3 1 3 から構成されている。

版数記録部 1 3 1 1 には、鍵無効化データ R D A T A の世代を示すバージョン番号が記録されており、識別子記録部 1 3 1 2 には、記録装置 1 1 0 0 の割当部 1 1 0 7 により割り当てられた鍵無効化データ識別子 R I D が記録されており、データ記録部 1 3 1 3 には、鍵無効化データ R D A T A が記録されている。

【 0 2 1 9 】

ここで、バージョン番号、鍵無効化データ識別子 R I D 及び鍵無効化データ R D A T A については、上述した通りである。

40

図 1 2 において、バージョン番号は、1 6 進数 4 桁で表現されており、具体的には、「 3 」である。第 2 の実施の形態では、配信局装置 1 4 0 0 から、鍵無効化データのバージョン番号が割当てられる。

【 0 2 2 0 】

図 1 2 において、鍵無効化データ識別子は、1 6 進数 4 桁で表現されており、鍵無効化データ識別子 R I D は、具体的には、「 1 」である。

また、暗号化コンテンツファイル 1 3 2 0 は、図 1 2 に示すように、識別子記録部 1 3 2 1、認証子記録部 1 3 2 2、鍵記録部 1 3 2 3 及びコンテンツ記録部 1 3 2 4 から構成されている。また、暗号化コンテンツファイル 1 3 2 0 には、当該ファイルに含まれてい

50

る暗号化コンテンツを識別するコンテンツ番号が付加されている（図示していない）。

【0221】

識別子記録部1321には、鍵無効化データ識別子RIDが記録されている。鍵無効化データ識別子RIDは、コンテンツの暗号化において使用された鍵無効化データに対して、記録装置1100の割当部1107により割り当てられたものである。

認証子記録部1322には、認証子MACが記録されている。認証子MACは、記録装置1100の認証子生成部1104により生成されたものである。

【0222】

鍵記録部1323には、記録装置1100の暗号化部1105により、生成された暗号化コンテンツ鍵ECKが記録されている。

コンテンツ記録部1324には、記録装置1100の暗号化部1106により、生成された暗号化コンテンツCNTが記録されている。

2.6 再生装置1200

再生装置1200a、1200b、1200c、・・・は、同様の構成を有しているの  
で、ここでは、再生装置1200として説明する。

【0223】

再生装置1200は、図13に示すように、デバイス鍵格納部1201、鍵計算部1202、認証子生成部1203、復号部1204、復号部1205、比較部1206、指定受付部1207、取得部1208、検索部1209、スイッチ1211、ドライブ部1213、再生部1214、制御部1215、入力部1216及び表示部1217から構成されている。

【0224】

再生装置1200は、具体的には、再生装置200と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニット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又は前記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従って動作することにより、再生装置1200は、その機能を達成する。

【0225】

(1) 指定受付部1207

指定受付部1207は、利用者から、リモコン1280及び入力部1216を介して、再生すべきコンテンツの指定を受け付け、指定を受け付けたコンテンツを識別するコンテンツ番号を取得部1208及び認証子生成部1203へ出力する。

(2) 取得部1208

取得部1208は、指定受付部1207からコンテンツ番号を受け取り、ドライブ部1213を介して、記録媒体1300の記録領域1305より、受け取ったコンテンツ番号が付加された暗号化コンテンツファイル1320を見出し、見出した暗号化コンテンツファイル1320の識別子記録部1321から、鍵無効化データ識別子RIDを読み出す。次に、読み出した鍵無効化データ識別子RIDを検索部1209へ出力する。

【0226】

(3) 検索部1209

検索部1209は、取得部1208から鍵無効化データ識別子RIDを受け取る。鍵無効化データ識別子RIDを受け取ると、ドライブ部1213を介して、記録媒体1300の記録領域1305に記録された1個以上の鍵無効化データファイルから、受け取った鍵無効化データ識別子RIDと同じ内容の鍵無効化データ識別子を識別子記録部に含む鍵無効化データファイルを検索し、検索された鍵無効化データファイルのデータ記録部より、鍵無効化データRDATAを読み出す。

【0227】

次に、検索部1209は、読み出した鍵無効化データRDATAを鍵計算部1202へ出力する。

(4) デバイス鍵格納部1201

10

20

30

40

50

デバイス鍵格納部 1201 は、デバイス鍵格納部 201 と同様に、外部の装置からアクセスできないように、デバイス鍵  $DK\_x$  を秘密に記憶している。デバイス鍵  $DK\_x$  は、再生装置 1200 に固有の鍵である。

【0228】

(5) 鍵計算部 1202

鍵計算部 1202 は、検索部 1209 から鍵無効化データ  $RDATA$  を受け取り、デバイス鍵格納部 1201 からデバイス鍵  $DK\_x$  を読み出す。

次に、鍵計算部 1202 は、鍵計算部 202 と同様にして、読み出したデバイス鍵  $DK\_x$  を用いて、受け取った鍵無効化データ  $RDATA$  に復号アルゴリズム  $D1$  を施して、復号メディア鍵  $y$  を生成する。

10

【0229】

ここで、復号メディア鍵  $y$  は、メディア鍵  $MK$  及び値「0」のいずれかである。

次に、鍵計算部 1202 は、生成した復号メディア鍵  $y$  を認証子生成部 1203 及びスイッチ 1211 へ出力する。

(6) 認証子生成部 1203

認証子生成部 1203 は、鍵計算部 1202 から復号メディア鍵  $y$  を受け取り、ドライブ部 1213 を介して、記録媒体 1300 の固有番号記録領域 1301 から媒体固有番号  $MID$  を読み出す。また、指定受付部 1207 からコンテンツ番号を受け取り、ドライブ部 1213 を介して、記録媒体 1300 上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル 1320 を特定し、特定された暗号化コンテンツファイル 1320 の鍵記録部 1323 から暗号化コンテンツ鍵  $ECK$  を読み出す。

20

【0230】

次に、受け取った復号メディア鍵  $y$  と、読み出した暗号化コンテンツ鍵  $ECK$  と、読み出した媒体固有番号  $MID$  とをこの順序で結合して、結合データを生成し、生成した結合データに一方方向関数  $F$  を施して、復号認証子  $DMAC$  を生成する。

$$DMAC = F(y || ECK || MID)$$

次に、認証子生成部 1203 は、生成した復号認証子  $DMAC$  を比較部 1206 へ出力する。

【0231】

(7) 比較部 1206

比較部 1206 は、認証子生成部 1203 から復号認証子  $DMAC$  を受け取る。また、比較部 1206 は、指定受付部 1207 からコンテンツ番号を受け取り、ドライブ部 1213 を介して、記録媒体 1300 上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル 1320 を特定し、特定された暗号化コンテンツファイル 1320 の認証子記録部 1322 に記録されている認証子  $MAC$  を読み出す。

30

【0232】

次に、比較部 1206 は、受け取った復号認証子  $DMAC$  と読み出した認証子  $MAC$  とが一致するか否かを判断する。一致すると判断する場合に、スイッチ 1211 へ、閉じる指示を出力し、一致しないと判断する場合に、スイッチ 1211 へ、開く指示を出力する。

40

(8) スイッチ 1211

スイッチ 1211 は、比較部 1206 からの指示により、開閉が制御される。スイッチ 1211 は、比較部 1206 から閉じる指示を受け取った場合に、閉じ、開く指示を受け取った場合に、開く。

【0233】

また、スイッチ 1211 は、鍵計算部 1202 から復号メディア鍵  $y$  を受け取る。閉じる指示を受け取った場合に、受け取った復号メディア鍵  $y$  を復号部 1204 へ出力する。開く指示を受け取った場合に、復号メディア鍵  $y$  は、外部へ出力されない。

(9) 復号部 1204

復号部 1204 は、スイッチ 1211 から復号メディア鍵  $y$  を受け取る。また、指定受

50

付部 1 2 0 7 からコンテンツ番号を受け取り、ドライブ部 1 2 1 3 を介して、記録媒体 1 3 0 0 上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル 1 3 2 0 を特定し、特定された暗号化コンテンツファイル 1 3 2 0 の鍵記録部 1 3 2 3 に記録されている暗号化コンテンツ鍵 E C K を読み出し、受け取った復号メディア鍵 y を用いて、読み出した暗号化コンテンツ鍵 E C K に復号アルゴリズム D 2 を施して復号コンテンツ鍵 D C K を生成し、生成した復号コンテンツ鍵 D C K を復号部 1 2 0 5 へ出力する。

#### 【 0 2 3 4 】

( 1 0 ) 復号部 1 2 0 5

復号部 1 2 0 5 は、復号部 1 2 0 4 から復号コンテンツ鍵 D C K を受け取る。また、指定受付部 1 2 0 7 からコンテンツ番号を受け取り、ドライブ部 1 2 1 3 を介して、記録媒体 1 3 0 0 上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル 1 3 2 0 を特定し、特定された暗号化コンテンツファイル 1 3 2 0 のコンテンツ記録部 1 3 2 4 に記録されている暗号化コンテンツ E C N T を読み出し、受け取った復号コンテンツ鍵 D C K を用いて、読み出した暗号化コンテンツ E C N T に復号アルゴリズム D 3 を施して復号コンテンツ D C N T を生成し、生成した復号コンテンツ D C N T を再生部 1 2 1 4 へ出力する。

10

#### 【 0 2 3 5 】

( 1 1 ) 再生部 1 2 1 4

再生部 1 2 1 4 は、復号部 1 2 0 5 から復号コンテンツ D C N T を受け取り、受け取った復号コンテンツ D C N T から映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモニタ 1 2 9 0 へ出力する。

20

#### 【 0 2 3 6 】

( 1 2 ) 制御部 1 2 1 5、入力部 1 2 1 6、表示部 1 2 1 7、ドライブ部 1 2 1 3、モニタ 1 2 9 0 及びリモコン 1 2 8 0

制御部 1 2 1 5 は、再生装置 1 2 0 0 を構成する各構成要素の動作を制御する。

リモコン 1 2 8 0 は、各種のボタンを備え、操作者の前記ボタンの操作に応じた操作指示情報を生成し、生成した操作指示情報を赤外線に乗せて出力する。

30

#### 【 0 2 3 7 】

入力部 1 2 1 6 は、リモコン 1 2 8 0 から、操作指示情報が乗せられた赤外線を受け取り、受け取った赤外線から操作指示情報を抽出し、抽出した操作指示情報を制御部 1 2 1 5 又は指定受付部 1 2 0 7 へ出力する。

表示部 1 2 1 7 は、制御部 1 2 1 5 の制御の基に、様々な情報を表示する。

ドライブ部 1 2 1 3 は、記録媒体 1 3 0 0 からの情報の読み出しを行う。

#### 【 0 2 3 8 】

モニタ 1 2 9 0 は、C R T 及びスピーカを備え、再生部 1 2 1 4 からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声信号に基づいて音声を出力する。

### 2 . 7 記録媒体に記録されるデータの構造と関連処理

40

( 1 ) バージョン番号

図 1 2 において、バージョン番号は、1 6 進数 4 桁で表現されており、具体的には、「 3 」である。第 2 の実施の形態では、配信局装置 1 4 0 0 から、鍵無効化データのバージョン番号が割当てられる。

#### 【 0 2 3 9 】

具体的には、最初に発行された鍵無効化データには、バージョン番号として「 1 」が割当てられ、その後、発行される鍵無効化データには、バージョン番号が「 2 」、「 3 」、・・・というように割当てられる。

鍵無効化が発生した場合、新しい鍵無効化データが発行され、その際に新しいバージョン番号が付与される。なお、新しい鍵無効化データの発行は、鍵無効化が発生した場合の

50

みに限定されない。例えば、セキュリティの観点から、予め定められた一定期間ごとに新しい鍵無効化データの発行を行うとしてもよい。

【0240】

(2) 鍵無効化データ識別子

図12において、識別子記録部1312に記録されている鍵無効化データ識別子は、16進数4桁で表現されており、鍵無効化データ識別子RIDは、「1」である。

ここで、鍵無効化データ識別子RIDは、記録媒体毎に、それぞれ記録される鍵無効化データを一意に識別するための情報である。従って、記録媒体毎に独立した体系により、鍵無効化データ識別子を割り当てることができる。

【0241】

記録装置1100の割当部1107による鍵無効化データ識別子RIDの具体的な割当て方法としては、割当部1107は、既に記録媒体に記録されている鍵無効化データに割当てられた鍵無効化データ識別子とは異なる値を割り当てる。

例えば、図14に示すように、記録媒体1300aに、既に鍵無効化データファイル1と鍵無効化データファイル2とが記録されており、それぞれの鍵無効化データ識別子は、「1」及び「2」であるとする。

【0242】

このとき、この記録媒体に新たな鍵無効化データファイル3を記録する際、割当部1107は、鍵無効化データ識別子RIDとして、「1」及び「2」以外の値、例えば「3」を割当てる。

(3) デバイス鍵とメディア鍵

図12において、データ記録部1313には、 $n$ 個のデバイス鍵 $DK\_i$  ( $i = 1, 2, \dots, n$ )を用いて、メディア鍵 $MK$ を、それぞれ暗号化することにより得られる暗号化メディア鍵 $E(DK\_i, MK)$ が記録されている。

【0243】

また、図12において、装置 $n$ が保有するデバイス鍵を $DK\_n$ と表現している。この図の例では、装置3、並びに装置4が無効化されているため、それぞれが保有する $DK\_3$ 、及び $DK\_4$ では、メディア鍵 $MK$ とは全く無関係のデータ「0」が暗号化されて記録されている。

鍵無効化データをこのように生成することで、例えば、デバイス鍵 $DK\_1$ を保有する装置1は、鍵無効化データの $E(DK\_1, MK)$ をデバイス鍵 $DK\_1$ で復号することにより、メディア鍵 $MK$ を得ることができるが、デバイス鍵 $DK\_3$ を保有する装置3は、鍵無効化データの $E(DK\_3, 0)$ をデバイス鍵 $DK\_3$ で復号したとしても、メディア鍵 $MK$ を得ることができない。

【0244】

このように、図12の例では、装置3及び装置4以外の全ての装置だけが正しいメディア鍵 $MK$ を共有でき、装置3及び装置4は、正しいメディア鍵 $MK$ が得られない。こうして、無効化された装置3及び装置4を、システムから排除することができる。

なお、装置の無効化方法は他の方法を利用してもよく、例えば、特許文献1には木構造を利用した無効化方法が開示されている。

【0245】

(4) 暗号化コンテンツファイル

図12において、暗号化コンテンツファイル1320は、識別子記録部1321、認証子記録部1322、鍵記録部1323及びコンテンツ記録部1324からなる。

この図において、識別子記録部1321に記録されている鍵無効化データ識別子は、16進数4桁で表現されており、鍵無効化データ識別子RIDは、具体的には、「1」である。

【0246】

鍵無効化データ識別子RIDは、以下で説明するように、再生装置1200において、再生したい暗号化コンテンツを復号するために使用する鍵無効化データファイル310を

10

20

30

40

50

記録媒体 1300 から取得するために使用される。

即ち、再生装置 1200 において、記録媒体 1300 に記録された暗号化コンテンツを復号再生する際、再生したい暗号化コンテンツファイル 1320 の識別子記録部 1321 に記録されている鍵無効化データ識別子 R I D と同じ鍵無効化 I D を識別子記録部 1312 に含む鍵無効化データファイル 310 を、記録媒体 1300 から取得する。

#### 【0247】

ここで、図 15 を用いてより具体的に説明する。図 15 に示すように、記録媒体 1300 b には、鍵無効化データファイル 1、鍵無効化データファイル 2、暗号化コンテンツファイル A、暗号化コンテンツファイル B 及び暗号化コンテンツファイル C が記録されている。

10

この図に示すように、鍵無効化データファイル 1 及び鍵無効化データファイルの鍵無効化データ識別子は、それぞれ、「1」及び「2」である。また、暗号化コンテンツファイル A、暗号化コンテンツファイル B 及び暗号化コンテンツファイル C の鍵無効化データ識別子は、それぞれ、「1」、「1」及び「2」である。

#### 【0248】

これは、記録装置 1100 において、暗号化コンテンツファイル A を生成し記録する際、鍵無効化データファイル 1 の鍵無効化データを使用し、暗号化コンテンツファイル B を生成し記録する際、鍵無効化データファイル 1 の鍵無効化データを使用し、暗号化コンテンツファイル C を生成し記録する際、鍵無効化データファイル 2 の鍵無効化データを使用したことを表している。

20

#### 【0249】

このとき、再生装置 1200 は、例えば、図 15 に示す記録媒体 1300 b における暗号化コンテンツファイル B を復号して再生する場合には、暗号化コンテンツファイル B の鍵無効化データ識別子は「1」であるから、鍵無効化データ識別子が「1」である鍵無効化データファイル 1 を取得し、所得した鍵無効化データファイル 1 に含まれている鍵無効化データを使用して、暗号化コンテンツファイル B に格納されている暗号化コンテンツを復号する。

#### 【0250】

##### 2.8 コンテンツ供給システム 20 の動作

コンテンツ供給システム 20 の動作について、特に、記録装置 1100 による記録媒体 1300 へのデータの書き込みの動作及び再生装置 1200 による記録媒体 1300 に記録されているデータの再生の動作について、説明する。

30

##### (1) 記録装置 1100 による書き込みの動作

記録装置 1100 による記録媒体 1300 へのデータの書き込みの動作について、図 16 ~ 図 18 に示すフローチャートを用いて説明する。

#### 【0251】

記録装置 1100 の送受信部 1111 は、配信局装置 1400 から、インターネット 40 を介して、鍵無効化データ R D A T A 及びバージョン番号 V R を受信し、受信した鍵無効化データ R D A T A 及びバージョン番号 V R を、対応付けて、無効化データ格納部 1102 に格納する (ステップ S 1501)。

40

なお、ステップ S 1501 における鍵無効化データ R D A T A 及びバージョン番号 V R の受信は、配信局装置 1400 により、新しい鍵無効化データ R D A T A が発行された時に行われる。鍵無効化データ R D A T A には、上述したように、その発行順序を示すバージョン番号 V R が付加されている。記録装置 1100 は、このバージョン番号 V R に基づいて、受信した鍵無効化データ R D A T A が新しいものかどうかを確認する。

#### 【0252】

例えば、記録装置 1100 の無効化データ格納部 1102 が、バージョン番号「1」が付加された鍵無効化データを保持している場合、配信局装置 1400 からバージョン番号「2」が付加された鍵無効化データを受信したと想定するとき、記録装置 1100 の制御部 1109 は、受信した鍵無効化データに付加されたバージョン番号「2」と、無効化デ

50

ータ格納部 1102 に保持されている鍵無効化データに付加されたバージョン番号「1」とを比較する。受信した鍵無効化データに付加されたバージョン番号「2」の方が新しいので、制御部 1109 は、受信した鍵無効化データは、新しいものであるとして、受信した鍵無効化データとバージョン番号「2」とを無効化データ格納部 1102 に格納するように送受信部 1111 へ指示を行う。ここで、バージョン番号は、その値が大きいほど、新しいことを示しているものとする。

#### 【0253】

なお、ここでは鍵無効化データの新旧の比較にバージョン番号を用いる場合について説明したが、この方法には限定されない。例えば、バージョン番号の代わりに、鍵無効化データには、その発行日時が付加されており、鍵無効化データの発行日時を用いて、鍵無効化データの新旧を比較する構成としてもよい。また、ここでは、配信局装置 1400 から鍵無効化データを入手するとしたが、鍵無効化データの取得方法はこの構成に限定されない。例えば、鍵無効化データとバージョン番号とが記録された記録媒体が配布され、記録装置 1100 は、この記録媒体から鍵無効化データとバージョン番号とを読み出すとしてもよい。

#### 【0254】

次に、記録装置 1100 の比較部 1108 は、ドライブ部 1110 を介して、記録媒体 1300 の記録領域 1305 に鍵無効化データファイルが存在するか否かを確認する。鍵無効化データファイルが存在しないと確認された場合は（ステップ S1502）、後述するステップ S1505a に進む。

鍵無効化データファイル 310 が存在すると確認された場合は（ステップ S1502）、比較部 1108 は、存在する全ての鍵無効化データファイルの版数記録部に記録されているバージョン番号について、ステップ S1501 で入手した鍵無効化データに付加されたバージョン番号と同じ内容のものが存在するか否かを確認する（ステップ S1503）。

#### 【0255】

ステップ S1503 において、上記条件を満たすバージョン番号が存在しない場合は（ステップ S1504）、後述するステップ S1505a に進む。

ステップ S1504 において、上記条件を満たすバージョン番号が存在する場合は（ステップ S1504）、制御部 1109 は、ドライブ部 1110 を介して、上記条件を満たすバージョン番号を含む鍵無効化データファイル 1310 の識別子記録部 1312 より、鍵無効化データ識別子 R I D を読み出す（ステップ S1505）。

#### 【0256】

鍵計算部 1103 は、デバイス鍵格納部 101 からデバイス鍵を読み出し、無効化データ格納部 1102 から鍵無効化データを読み出し（ステップ S1506）、読み出した鍵無効化データを読み出したデバイス鍵で復号することによりメディア鍵 M K を算出する（ステップ S1507）。

次に、暗号化部 1105 は、算出されたメディア鍵を用いて、コンテンツサーバ装置 1500 から受信したコンテンツ鍵 C K を暗号化して、暗号化コンテンツ鍵 E C K を生成する（ステップ S1508）。

#### 【0257】

認証子生成部 1104 は、記録媒体 1300 の固有番号記録領域 1301 から媒体固有番号 M I D を読み出し（ステップ S1509）、鍵計算部 1103 により算出されたメディア鍵 M K と、暗号化部 1105 により生成された暗号化コンテンツ鍵 E C K と、読み出した媒体固有番号 M I D とを結合した値をハッシュ関数の入力値としたときの出力値として、認証子 M A C を生成する（ステップ S1510）。なお、ここで使用するハッシュ関数は、公知の技術で実現可能である。例えばハッシュ関数として S H A - 1 を使用してもよい。なお、S H A - 1 には限定されない。

#### 【0258】

次に、暗号化部 1106 は、コンテンツサーバ装置 1500 から受信したコンテンツ鍵

10

20

30

40

50

CKを用いて、同じく受信したコンテンツCNTを暗号化する(ステップS1511)。

記録装置1100は、ステップS1505で取得した、又はステップS1505aで割当てられた鍵無効化データ識別子RIDと、ステップS1510で生成した認証子MACと、ステップS1508で生成した暗号化コンテンツ鍵と、ステップS1511で生成した暗号化コンテンツとを含む暗号化コンテンツファイルを、記録媒体1300の記録領域1305に記録し(ステップS1512)、処理を終了する。

#### 【0259】

また、記録媒体1300に鍵無効化データファイル1310が存在しないと確認された場合(ステップS1502)、及びステップS1503において条件を満たすバージョン番号が存在しない場合は(ステップS1504)、割当部1107は、ステップS1501で入手した鍵無効化データに対して、記録媒体1300の記録領域1305に記録されている全ての鍵無効化データファイルに既に割当てられた鍵無効化データ識別子RIDとは異なる値を、鍵無効化データ識別子として、割当てる(ステップS1505a)。

#### 【0260】

例えば、記録媒体1300に、鍵無効化データファイルが一切存在しない場合には、割当部1107は、任意の値、例えば「1」を割当る。また、図14に示す例のように、記録媒体1300aに、鍵無効化データ識別子RIDが「1」及び「2」の鍵無効化データファイル1及び2が存在する場合には、割当部1107は、「1」及び「2」とは異なる値、例えば「3」を割当てる。

#### 【0261】

次に、記録装置1100のドライブ部1110は、ステップS1501で入手した鍵無効化データと、その鍵無効化データのバージョン番号と、ステップS1505aで割当てられた鍵無効化データ識別子とを有する鍵無効化データファイルを、記録媒体1300の鍵無効化データファイル1302に記録する(ステップS1505b)。このとき、鍵無効化データ、バージョン番号及び鍵無効化データ識別子RIDを、それぞれ、鍵無効化データファイル310のデータ記録部1313、版数記録部1311及び識別子記録部1312に記録する。次に、ステップS1506へ制御が移り、以降、前述したステップS1506からステップS1512までが実行される。

#### 【0262】

(2)再生装置1200による再生の動作

再生装置1200による記録媒体1300に記録されているデータの再生の動作について、図19～図20に示すフローチャートを用いて説明する。

再生装置1200の指定受付部1207は、再生すべきコンテンツの指定を受け付ける(ステップS1601)。

#### 【0263】

取得部1208は、記録媒体1300の記録領域1305より、ステップS1601で指定されたコンテンツに対応する暗号化コンテンツファイルを見出す(ステップS1602)。

なお、指定受付部1207における再生すべきコンテンツの指定方法、及び、指定されたコンテンツに対応する暗号化コンテンツファイルの見出し方法としては、例えば、再生装置1200は、記録媒体1300の記録領域1305に記録されている全ての暗号化コンテンツファイルの属性を示す情報(例えば、暗号化コンテンツのファイル名、コンテンツのタイトル名、コンテンツの記録日時、コンテンツの要約情報、コンテンツのサムネイル画像、コンテンツを示すアイコンなど)の一覧を、再生装置1200の表示部1217に表示し、利用者に、その一覧の中から、再生したいコンテンツを選択させることにより、再生すべきコンテンツの指定を受け付ける。また、再生装置1200は、指定されたコンテンツの属性情報から、指定されたコンテンツが格納された暗号化コンテンツファイルのファイル名を知り、記録媒体1300の記録領域1305から、該当のファイル名の暗号化コンテンツファイルを見出す。

#### 【0264】

なお、暗号化コンテンツファイルの見出し方法としては、上述の方法に限定されるものではなく、他の方法を用いてもよい。

取得部 1208 は、ステップ S1602 で見出した暗号化コンテンツファイル 1320 の識別子記録部 1321 より鍵無効化データ識別子を読み出す（ステップ S1603）。

検索部 1209 は、記録媒体 1300 の記録領域 1305 より、ステップ S1603 で読み出した鍵無効化データ識別子 R I D と同じ値が、識別子記録部 1312 に記録されている鍵無効化データファイル 310 を見出す（ステップ S1604）。次に、検索部 1209 は、ステップ S1604 で見出した鍵無効化データファイル 1310 を取得する（ステップ S1605）。

#### 【0265】

鍵計算部 1202 は、デバイス鍵格納部 1201 からデバイス鍵を読み出し、検索部 1209 から鍵無効化データを受け取る（ステップ S1606）。

鍵計算部 1202 は、ステップ S1606 で受け取った鍵無効化データを、デバイス鍵を用いて復号することにより復号メディア鍵  $y$  を算出する（ステップ S1607）。

認証子生成部 1203 は、記録媒体 1300 の固有番号記録領域 1301 から媒体固有番号 M I D を読み出し（ステップ S1608）、ステップ S1602 で見出した暗号化コンテンツファイル 1320 の鍵記録部 1323 より暗号化コンテンツ鍵 E C K を読み出し（ステップ S1609）、ステップ S1607 で取得した復号メディア鍵  $y$  と、ステップ S1609 で読み出した暗号化コンテンツ鍵 E C K と、ステップ S1608 で取得した媒体固有番号 M I D とを結合した値をハッシュ関数の入力値としたときの出力値として、復号認証子 D M A C を生成する（ステップ S1610）。ここで使用するハッシュ関数は、記録装置 1100 で用いたものと同じハッシュ関数 S H A - 1 である。

#### 【0266】

比較部 1206 は、ステップ S1602 で見出した暗号化コンテンツファイル 1320 の認証子記録部 322 より、認証子 M A C を読み出し（ステップ S1611）、ステップ S1610 で算出された復号認証子 D M A C とステップ S1611 で読み出した認証子 M A C が一致するかどうか確認する（ステップ S1612）。

復号認証子 D M A C と認証子 M A C とが一致しなければ（ステップ S1613）、再生動作は、終了する。

#### 【0267】

復号認証子 D M A C と認証子 M A C とが一致すれば（ステップ S1613）、復号部 1204 は、暗号化コンテンツ鍵を、ステップ S1607 で算出した復号メディア鍵  $y$  で復号し、復号コンテンツ鍵 D C K を取得する（ステップ S1614）。

復号部 1205 は、ステップ S1602 で見出した暗号化コンテンツファイル 1320 のコンテンツ記録部 1324 より、暗号化コンテンツを読み出し（ステップ S1615）、ステップ S1615 で読み出した暗号化コンテンツを、ステップ S1614 で復号した復号コンテンツ鍵 D C K を用いて、復号して復号コンテンツし、再生部 1214 は、復号コンテンツを再生する（ステップ S1616）。

#### 【0268】

##### 2.9 その他の変形例

以下に示すように構成してもよい。

(1) 第2の実施の形態においては、鍵無効化データの世代を示すバージョン番号及び鍵無効化データを識別する鍵無効化データ識別子を、それぞれ、鍵無効化データファイルにおける版数記録部及び識別子記録部に記録するとしたが、この方法に限定されない。

#### 【0269】

例えば、鍵無効化データファイルを識別するファイル名の一部に、鍵無効化データのバージョン番号と鍵無効化データ識別子の両者、又は少なくとも1つを含む構成としてもよい。具体的には、鍵無効化データファイルのファイル名を、“K R D \_\_ n \_\_ m”としてもよい。ここで、n はバージョン番号であり、m は鍵無効化データ識別子である。この場合、例えば、“K R D \_\_ 0 0 0 1 \_\_ 0 0 0 2”というファイル名により識別される鍵無効化

10

20

30

40

50

データファイルのバージョン番号は「1」であり、鍵無効化データ識別子R I Dは「2」である。

【0270】

このようにファイル名にバージョン番号や鍵無効化データ識別子の両者、又は少なくとも1つ含むことにより、再生装置は、ファイル名を見れば、鍵無効化データファイルのバージョン番号や鍵無効化データ識別子R I Dを知ることができ、再生装置におけるファイルを検索する際の処理が軽減できるというメリットがある。

(2)第2の実施の形態においては、鍵無効化データ識別子を、暗号化コンテンツファイルにおける識別子記録部に記録するとしたが、この方法に限定されない。

【0271】

例えば、暗号化コンテンツファイルを識別するファイル名の一部に鍵無効化データ識別子を含める構成としても良い。具体的には、暗号化コンテンツを識別するファイル名を、“ECNT\_m”としてもよい。ここで、mは、鍵無効化データ識別子である。例えば“ECNT\_0002”というファイル名の暗号化コンテンツファイルの鍵無効化データ識別子R I Dは「2」である。

【0272】

このようにファイル名に鍵無効化データ識別子を含めることにより、再生装置において、ファイル名を見れば、鍵無効化データ識別子を知ることができ、再生装置における鍵無効化データ識別子の取得する際の処理が軽減できるというメリットがある。

(3)第2の実施の形態においては、鍵無効化データを鍵無効化データ識別子と関連づけるため、また暗号化コンテンツを前記鍵無効化データ識別子R I Dと関連づけるために、鍵無効化データファイル1310に、版数記録部1311と、識別子記録部1312を設け、それぞれ、バージョン番号と鍵無効化データ識別子とを記録し、暗号化コンテンツファイル1320に識別子記録部1321を設け、鍵無効化データ識別子を記録する構成としているが、この構成に限定されない。

【0273】

例えば、記録装置は、記録媒体1300上に、1個以上の鍵無効化データファイルと、1個以上の暗号化コンテンツファイルと、1個の鍵無効化データ管理ファイルとを記録するとしてもよい。この鍵無効化データ管理ファイルには、鍵無効化データファイル毎に、その鍵無効化データのバージョン番号と、鍵無効化データ識別子と、記録媒体上で該鍵無効化データファイルを一意に特定するための情報(例えば、鍵無効化データファイルが記録されているディレクトリ名やファイル名など)と、該鍵無効化データファイルを用いて暗号化した暗号化コンテンツファイルを記録媒体上で一意に特定するための情報(例えば、暗号化コンテンツファイルが記録されているディレクトリ名やファイル名など)とが含まれる。再生装置は、この鍵無効化データ管理ファイルに記録されている上記情報に基づいて、再生が指定された暗号化コンテンツに関連する鍵無効化データファイルを取得する。

【0274】

また、本実施の形態の構成と、鍵無効化データ管理ファイルを設ける構成を組み合わせた構成としても良い。

(4)第2の実施の形態では、鍵無効化データのバージョン番号と、鍵無効化データ識別子の両方が存在する構成としたが、この構成には限定されず、鍵無効化データ識別子だけが存在する構成でもよい。

【0275】

(5)第2の実施の形態では、鍵無効化技術として、記録媒体の書き換え可能領域に記録する鍵無効化データを、無効化されていない装置が保有するデバイス鍵を用いてメディア鍵を暗号化したものと、無効化された装置が保有するデバイス鍵を用いてメディア鍵とは無関係な値(例えば「0」)を暗号化したものとし、記録媒体の書き換え可能領域に記録する暗号化コンテンツを、コンテンツを前記メディア鍵に基づいて暗号化したものとする場合について説明したが、この構成に限定されるものではない。

10

20

30

40

50

## 【0276】

例えば、記録媒体の書き換え可能領域に記録する鍵無効化データと暗号化コンテンツとして、無効化されていない装置においては、鍵無効化データに基づいて暗号化コンテンツが復号再生でき、無効化された装置においては、鍵無効化データに基づいて暗号化コンテンツが復号再生できないという条件を満たすものであればどんな構成であってもよい。

(6)第2の実施の形態では、メディアバインド技術として、記録装置1100において媒体固有番号MIDを用いて認証子MACを生成して、再生装置1200において認証子MACの比較を行うとしているが、この構成に限定されるものではない。

## 【0277】

例えば、記録装置1100において媒体固有番号MIDを用いてコンテンツを暗号化して記録媒体に記録し、再生装置1200において媒体固有番号MIDを用いて暗号化されたコンテンツを復号する構成としても良い。

(7)第2の実施の形態では、鍵無効化データ識別子を割り当てる際、記録装置1100に既に記録されている鍵無効化データに割り当てられていない値を、鍵無効化IDとして割り当てる構成としているが、この構成に限定されるものではない。

## 【0278】

例えば、記録装置1100は、既に割り当てた鍵無効化データ識別子を媒体固有番号MIDとともに記憶しておき、記録装置1100に記憶している上記情報に基づいて、鍵無効化データ識別子を割り当てる構成としても良い。

## 2.10 まとめ

以上の説明から明らかなように、本発明に係る記録装置は、特定装置が保有する鍵を無効化するための鍵無効化データを格納する鍵無効化データ格納手段と、前記鍵無効化データに基づいて前記コンテンツを暗号化するコンテンツ暗号化手段と、前記鍵無効化データに対して、前記記録媒体において前記鍵無効化データを一意に識別するための鍵無効化データ識別情報を割り当てる鍵無効化データ識別情報割当手段と、前記記録媒体に、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ記録手段と、前記暗号化コンテンツを前記鍵無効化データ識別情報と関連づけて記録する暗号化コンテンツ記録手段とを備える。

## 【0279】

また、本発明の記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データに既に割り当てられた鍵無効化データ識別情報とは異なる値を、鍵無効化データ識別情報情報として割り当てる。

また、本発明の記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データと、前記鍵無効化データ格納手段に格納されている鍵無効化データの新旧を比較し、前記鍵無効化データ格納手段に格納されている鍵無効化データが新しい場合のみ、鍵無効化データ識別情報の割当てを行うことを特徴とする。

## 【0280】

また、本発明における記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データと、前記鍵無効化データ格納手段に格納されている鍵無効化データの新旧の比較を、各鍵無効化データが生成された日時に関連する情報、もしくは、各鍵無効化データが生成された順序に関連する情報に基づいて行う。

また、本発明に係る再生装置は、前記記録媒体から、暗号化コンテンツと、前記暗号化コンテンツに関連づけて記録された鍵無効化データ識別情報を読み出す暗号化コンテンツ読出手段と、前記記録媒体から、前記暗号化コンテンツ読出手段にて読み出した鍵無効化データ識別情報と同じ鍵無効化データ識別情報が関連づけて記録されている鍵無効化データを読み出す鍵無効化データ読出手段と、前記鍵無効化データ読出手段にて読み出した鍵無効化データに基づいて前記暗号化コンテンツ読出手段で読み出した前記暗号化コンテンツを復号するコンテンツ復号手段とを備える。

## 【0281】

また、本発明における記録媒体は、鍵無効化データを、前記記録媒体においてこの鍵無

10

20

30

40

50

効化データを一意に識別するための鍵無効化データ識別情報と関連づけて記録する鍵無効化データ格納手段と、前記鍵無効化データに基づいて暗号化された暗号化コンテンツを前記無効化データ識別情報と関連づけて記録する暗号化コンテンツ格納手段とを備える。

また、本発明における前記記録媒体は、さらに、鍵無効化データの新旧を示す情報を、鍵無効化データと関連づけて記録する。

#### 【0282】

また、本発明における著作権保護システムは、記録装置と、記録媒体と、再生装置からなり、前記記録装置は、特定装置が保有する鍵を無効化するための鍵無効化データを格納する鍵無効化データ格納手段と、前記鍵無効化データに基づいて前記コンテンツを暗号化するコンテンツ暗号化手段と、前記鍵無効化データに対して、前記記録媒体において前記鍵無効化データを一意に識別するための鍵無効化データ識別情報を割当てる鍵無効化データ識別情報割当手段と、前記記録媒体に、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ記録手段と、前記暗号化コンテンツを前記鍵無効化データ識別情報と関連づけて記録する暗号化コンテンツ記録手段とを備え、前記記録媒体は、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ格納手段と、前記暗号化コンテンツを前記無効化データ識別情報と関連づけて記録する暗号化コンテンツ格納手段とを備え、前記再生装置は、前記記録媒体から、暗号化コンテンツと、前記暗号化コンテンツに関連づけて記録された鍵無効化データ識別情報を読み出す暗号化コンテンツ読出手段と、前記暗号化コンテンツ読出手段にて読み出した鍵無効化データ識別情報と同じ鍵無効化データ識別情報が関連づけて記録されている鍵無効化データを読み出す鍵無効化データ読出手段と、前記鍵無効化データ読出手段にて読み出した鍵無効化データに基づいて前記暗号化コンテンツ読出手段で読み出した前記暗号化コンテンツを復号するコンテンツ復号手段とを備える。

#### 【0283】

このように、第2の実施の形態に係る記録装置、記録媒体、再生装置、及び、著作権保護システムにおいては、記録媒体に記録する鍵無効化データに対して、記録媒体においてその鍵無効化データを一意に識別するための鍵無効化データIDを割当て、この鍵無効化データIDを、記録媒体に記録する鍵無効化データと関連づけて鍵無効化データファイルとして記録するとともに、この鍵無効化データIDを、該鍵無効化データを使用して暗号化したコンテンツと関連づけて、暗号化コンテンツファイルとして、記録することにより、再生装置において、該暗号化コンテンツを復号再生する場合に、記録媒体に、複数の暗号化コンテンツファイルと、複数の鍵無効化データファイルが記録されている場合においても、該暗号化コンテンツファイルに含まれる鍵無効化データIDと同じ鍵無効化データIDを含む鍵無効化データファイルを検索取得することができ、暗号化コンテンツファイルを取得した鍵無効化データファイルを用いて復号再生することが可能となる。

#### 【0284】

##### 3. その他の変形例

なお、本発明を上記の各実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのももちろんである。以下のような場合も本発明に含まれる。

(1) 各実施の形態において、コンテンツは、映像データと音声データとが高效率で圧縮符号化されたデータであるとしているが、これには、限定されない。例えば、コンテンツは、小説、静止画像、音声などがデジタル化されたコンピュータデータであるとしてもよい。

#### 【0285】

また、例えば、コンテンツは、コンピュータを構成するマイクロプロセッサの動作を制御する複数の命令から構成されるコンピュータプログラムであるとしてもよい。また、表計算ソフトにより生成される表データであるとしてもよいし、データベースソフトにより生成されるデータベースであるとしてもよい。

(2) 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

10

20

30

40

50

ュータシステムである。前記RAM又は前記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従って動作することにより、各装置は、その機能を達成する。

【0286】

(3)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。

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、に記録したものであるとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

10

【0287】

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。

また、本発明は、マイクロプロセッサとメモリと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従って動作するものとしてもよい。

【0288】

20

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ものとしてもよい。

(4)上記各実施の形態及び上記各変形例をそれぞれ組み合わせるものとしてもよい。

【産業上の利用可能性】

【0289】

本発明を構成する各装置及び記録媒体は、コンテンツを制作し、配給するコンテンツ配給産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

30

【図面の簡単な説明】

【0290】

【図1】図1は、コンテンツ供給システム10の構成を示す構成図である。

【図2】図2は、記録装置100の構成を示すブロック図である。

【図3】図3は、記録媒体120に記録されているデータの構造を示すデータ構造図である。

【図4】図4は、再生装置200の構成を示すブロック図である。

【図5】図5は、記録装置100による記録媒体120へのデータの書き込みの動作を示すフローチャートである。

【図6】図6は、再生装置200による記録媒体120に記録されているデータの再生の動作を示すフローチャートである。図7へ続く。

40

【図7】図7は、再生装置200による記録媒体120に記録されているデータの再生の動作を示すフローチャートである。図6から続く。

【図8】図8は、第1の実施の形態の変形例におけるn枚の記録媒体に記録されているデータの構造を示すデータ構造図である。

【図9】図9は、第1の実施の形態の変形例における記録媒体に記録されているデータの構造を示すデータ構造図である。

【図10】図10は、コンテンツ供給システム20の構成を示す構成図である。

【図11】図11は、記録装置1100の構成を示すブロック図である。

【図12】図12は、記録媒体1300に記録されているデータの構造を示すデータ構造

50

図である。

【図 1 3】図 1 3 は、再生装置 1 2 0 0 の構成を示すブロック図である。

【図 1 4】図 1 4 は、記録媒体 1 3 0 0 a に記録されているデータの構造を示すデータ構造図である。

【図 1 5】図 1 5 は、記録媒体 1 3 0 0 b に記録されているデータの構造を示すデータ構造図である。

【図 1 6】図 1 6 は、記録装置 1 1 0 0 による記録媒体 1 3 0 0 へのデータの書き込みの動作を示すフローチャートである。図 1 7 へ続く。

【図 1 7】図 1 7 は、記録装置 1 1 0 0 による記録媒体 1 3 0 0 へのデータの書き込みの動作を示すフローチャートである。図 1 8 へ続く。

【図 1 8】図 1 8 は、記録装置 1 1 0 0 による記録媒体 1 3 0 0 へのデータの書き込みの動作を示すフローチャートである。図 1 7 から続く。

【図 1 9】図 1 9 は、再生装置 1 2 0 0 による記録媒体 1 3 0 0 に記録されているデータの再生の動作を示すフローチャートである。図 2 0 へ続く。

【図 2 0】図 2 0 は、再生装置 1 2 0 0 による記録媒体 1 3 0 0 に記録されているデータの再生の動作を示すフローチャートである。図 1 9 から続く。

【符号の説明】

【 0 2 9 1 】

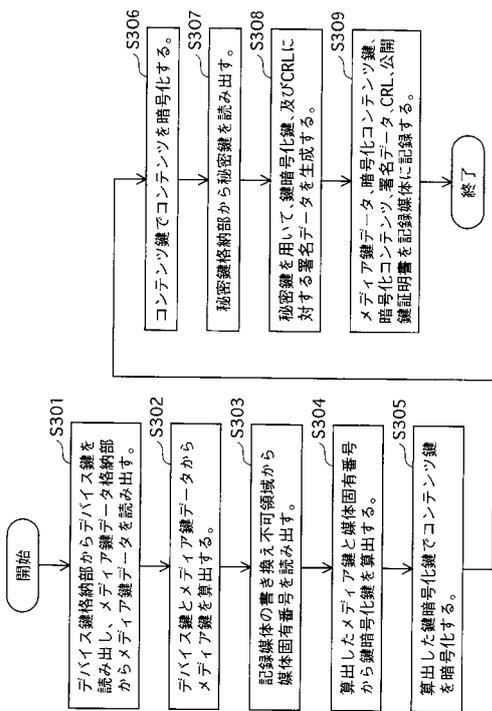
- 1 0      コンテンツ供給システム
  - 1 0 0     記録装置
  - 2 0 0 a ~ 2 0 0 e      再生装置
  - 5 0 0     コンテンツサーバ装置
  - 2 0      コンテンツ供給システム
  - 1 1 0 0    記録装置
  - 1 2 0 0 a ~ 1 2 0 0 e      再生装置
  - 1 4 0 0    配信局装置
  - 1 5 0 0    コンテンツサーバ装置
- ことを特徴とする記録媒体。

10

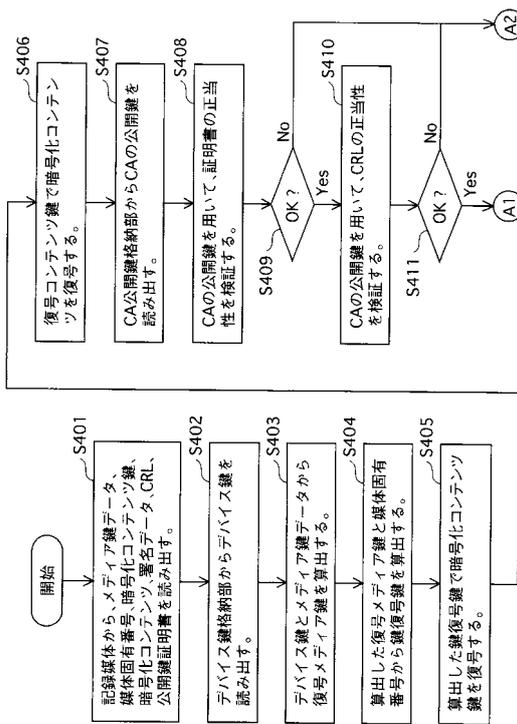
20



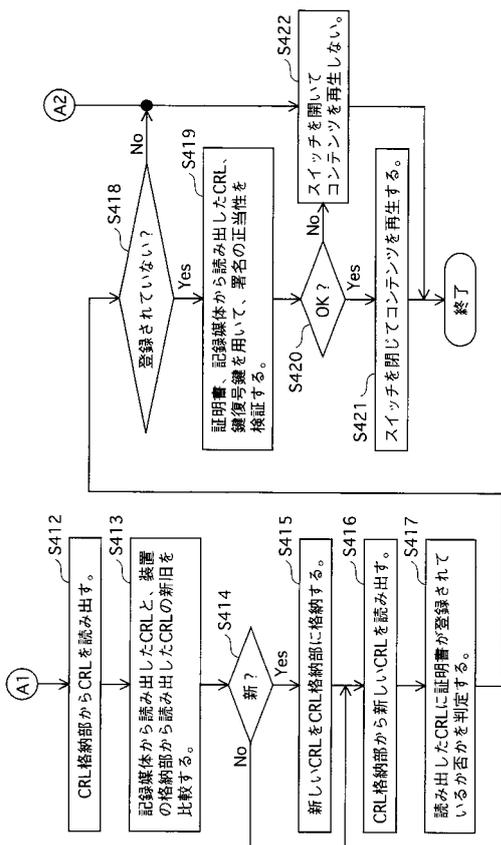
【 図 5 】



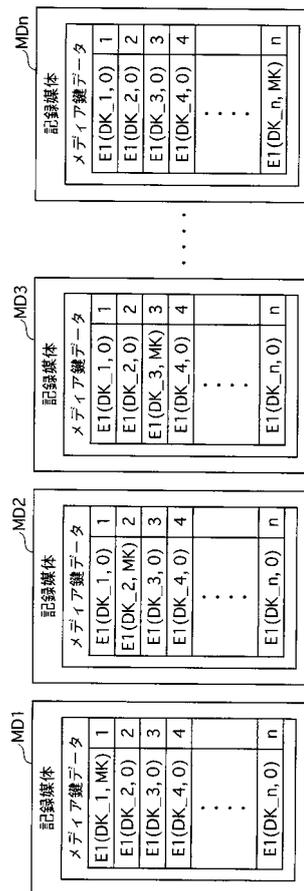
【 図 6 】



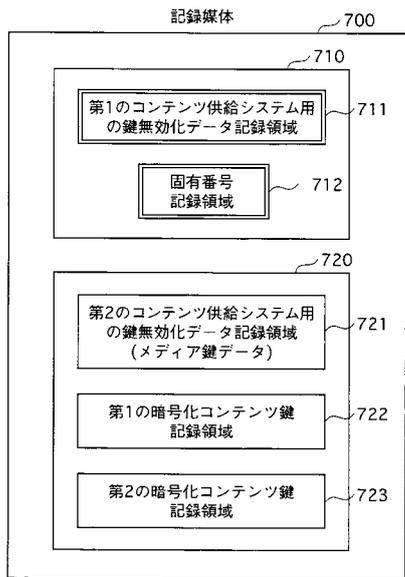
【 図 7 】



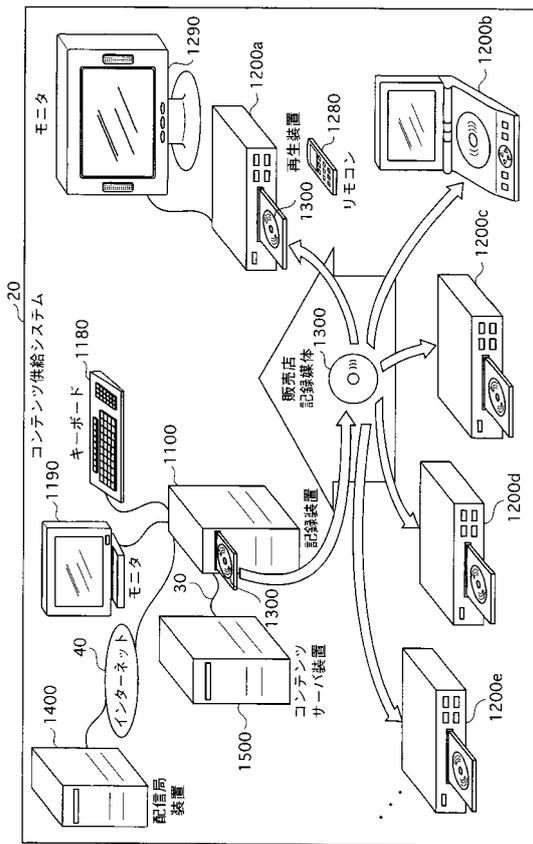
【 図 8 】



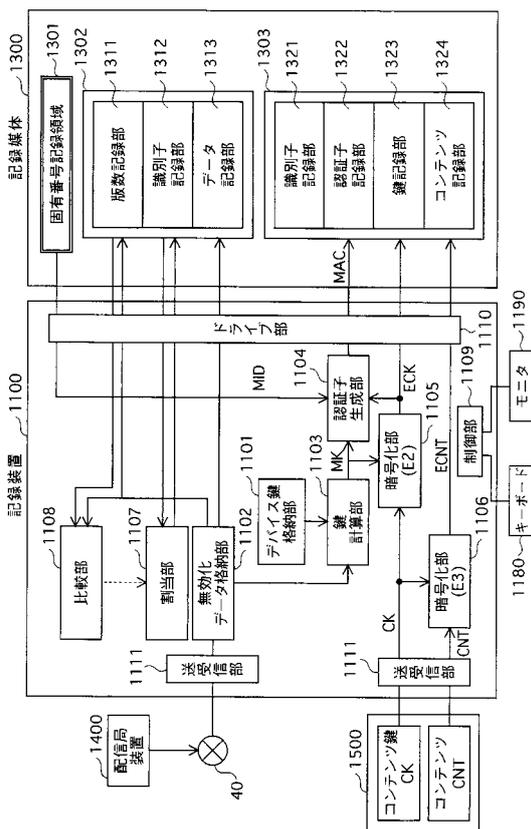
【図9】



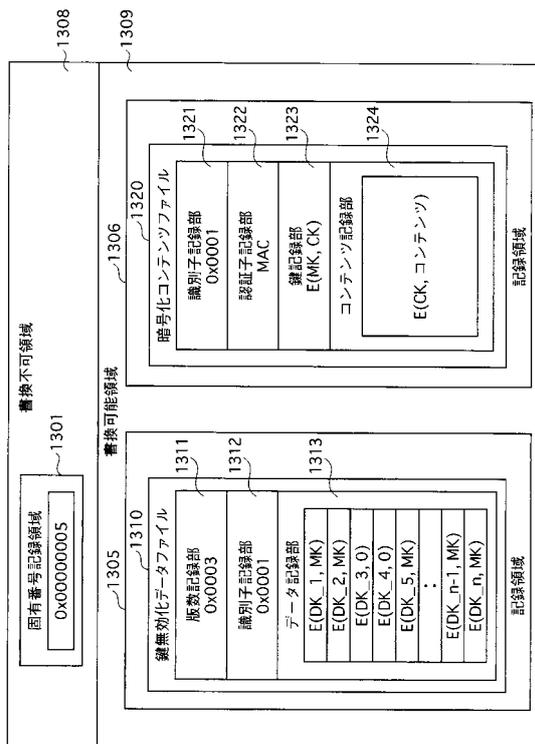
【図10】



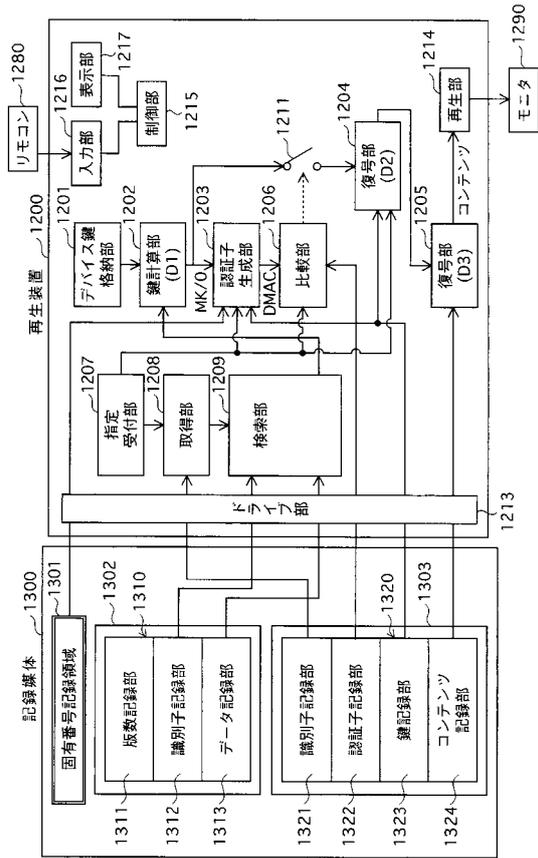
【図11】



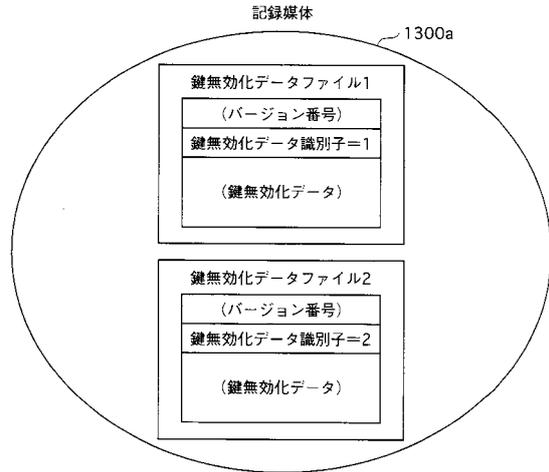
【図12】



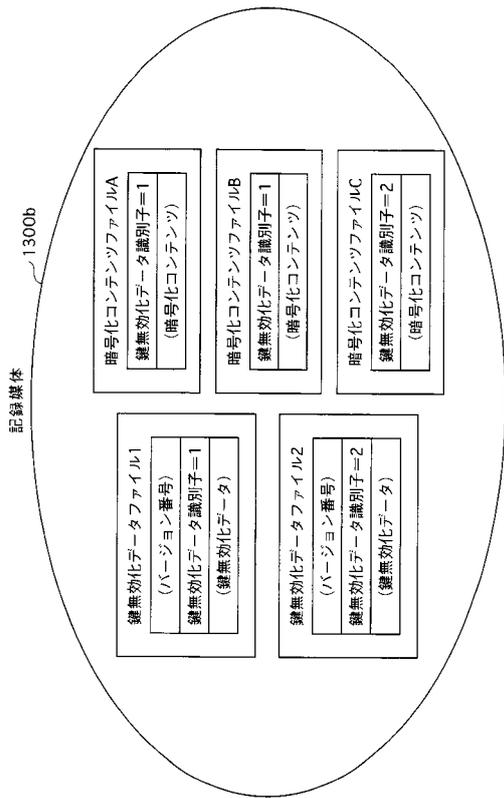
【図13】



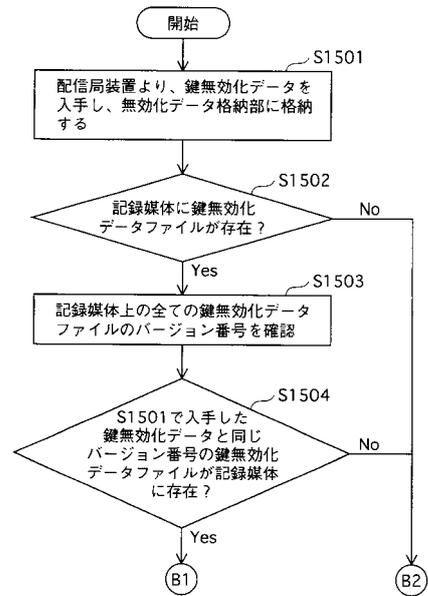
【図14】



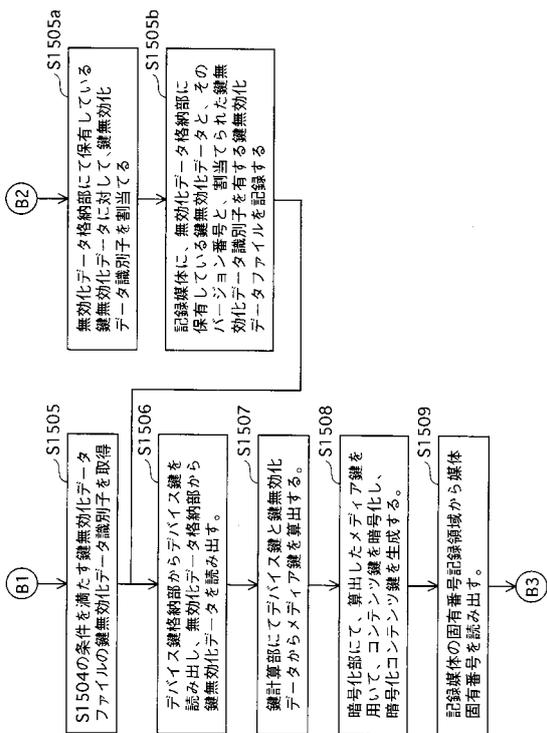
【図15】



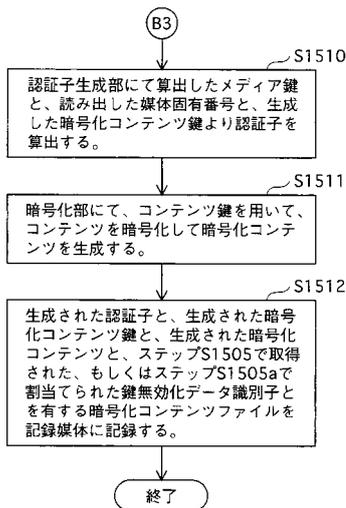
【図16】



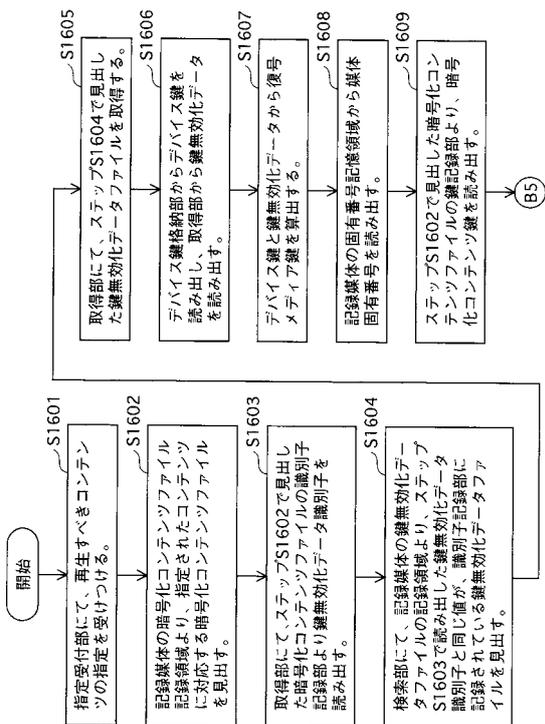
【図 17】



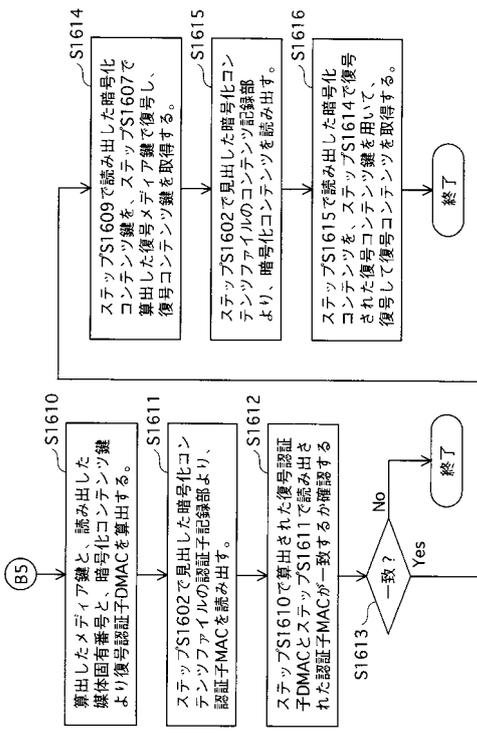
【図 18】



【図 19】



【図 20】



---

フロントページの続き

- (72)発明者 大森 基司  
大阪府門真市大字門真1006番地 松下電器産業株式会社内
- (72)発明者 館林 誠  
大阪府門真市大字門真1006番地 松下電器産業株式会社内
- (72)発明者 原田 俊治  
大阪府門真市大字門真1006番地 松下電器産業株式会社内
- (72)発明者 村瀬 薫  
大阪府門真市大字門真1006番地 松下電器産業株式会社内

審査官 中里 裕正

- (56)参考文献 特開2002-009753(JP,A)  
特開2002-009754(JP,A)  
特開2003-008567(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/08

G06F 21/24

G11B 20/10

JSTPlus/JMEDPlus/JST7580(JDreamII)