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

特許第4574175号
(P4574175)

(45)発行日　平成22年11月4日(2010.11.4)　(24)登録日　平成22年8月27日(2010.8.27)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E
H04L 9/00 601A

請求項の数 12　(全 27 頁)

(21)出願番号　特願2004-7060(P2004-7060)
(22)出願日　平成16年1月14日(2004.1.14)
(65)公開番号　特開2004-320719(P2004-320719A)
(43)公開日　平成16年11月11日(2004.11.11)
審査請求日　平成18年12月21日(2006.12.21)
(31)優先権主張番号　特願2003-7349(P2003-7349)
(32)優先日　平成15年1月15日(2003.1.15)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2003-101455(P2003-101455)
(32)優先日　平成15年4月4日(2003.4.4)
(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
(72)発明者　中野　稔久
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　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　松崎　なつめ
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、鍵データ生成装置及び端末装置

(57)【特許請求の範囲】
【請求項１】
（ａ）木構造を利用して端末装置が保有するデバイス鍵を管理している鍵データ生成装置により、コンテンツを利用するために用いる第１鍵データを、前記デバイス鍵に対して生成した変換情報を用いて、予め定められた変換規則に基づいて変換した第２鍵データを、前記デバイス鍵を用いて暗号化することで生成された暗号化鍵データと、（ｂ）前記暗号化鍵データの生成に用いられたデバイス鍵の前記木構造での位置情報に基づいて生成された、前記変換情報を生成するための情報であるヘッダ情報とを取得する取得手段と、
複数のデバイス鍵を保持している保持手段と、
前記木構造における当該端末装置の位置情報を保持している保持手段と、
前記暗号化鍵データを、当該端末装置が保持するデバイス鍵のうちの一つを用いて復号し、第２鍵データを生成する復号手段と、
前記ヘッダ情報と前記位置情報とから変換情報を生成し、前記第２鍵データを、前記生成した変換情報を用いて、予め定められた変換規則に基づいて変換することで第１鍵データを生成する変換手段と、
前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用手段と
を備えることを特徴とする端末装置。
【請求項２】
前記暗号化鍵データの生成に用いられたデバイス鍵は、正当な端末装置のみが保有するデバイス鍵を含み、

前記ヘッダ情報は、正当な端末装置のみが保有するデバイス鍵の前記木構造での位置情報に基づいて生成された情報である
ことを特徴とする請求項１に記載の端末装置。
【請求項３】
前記暗号化鍵データは、前記鍵データ生成装置により、前記デバイス鍵に対して生成した変換情報と前記第１鍵データとで逆変換可能な演算を行って生成された前記第２鍵データを暗号化して生成された情報である
ことを特徴とする請求項１に記載の端末装置。
【請求項４】
前記端末装置は、更に
前記複数のデバイス鍵から、一つのデバイス鍵を選択する選択手段を備え、
前記復号手段は、前記選択されたデバイス鍵を用いて復号し、
前記変換手段は、前記復号された第２鍵データに対する変換情報を生成し、前記変換情報を用いて前記選択されたデバイス鍵に所定の演算を施して前記第１鍵データを生成し、前記暗号化鍵データに付随するヘッダ情報から前記変換情報を生成し、
前記ヘッダ情報は、木構造を利用してデバイス鍵を管理している前記鍵データ生成装置が、前記木構造において、前記正当な端末装置のみが保有するデバイス鍵の内、最上位層に位置するノードに対応付けられている１以上のデバイス鍵を選択し、選択した前記デバイス鍵の木構造における位置情報に基づいて生成した、前記変換情報を生成するための情報である
ことを特徴とする請求項３に記載の端末装置。
【請求項５】
前記ヘッダ情報は、木構造の各ノードに１以上のデバイス鍵を対応付けて、各端末装置が保持するデバイス鍵と、それらのデバイス鍵が無効化されているか否かを管理し、前記木構造において、無効化されていない前記正当な端末装置のみが保有するデバイス鍵の内、最上位層に位置するノードに対応付けられている１以上のデバイス鍵を選択し、選択したデバイス鍵が対応するノードと、他のノードの無効化の状態とに基づいて定義された無効化情報に基づいて生成された、前記変換情報を生成するための情報である
ことを特徴とする請求項１に記載の端末装置。
【請求項６】
前記第２鍵データは、前記鍵データ生成装置によって、前記デバイス鍵に対して生成された変換情報を、前記第１鍵データの冗長部分の少なくとも一部に埋め込み生成され、
前記変換手段は、前記第２鍵データの冗長部分を削除して、前記第１鍵データを生成する
ことを特徴とする請求項１に記載の端末装置。
【請求項７】
前記コンテンツ利用手段は、
前記第１鍵データに基づいて、前記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、
前記暗号化コンテンツを出力する出力部とを備える
ことを特徴とする請求項１に記載の端末装置。
【請求項８】
前記コンテンツ利用手段は、
暗号化されたコンテンツを取得するコンテンツ取得部と、
前記第１鍵データに基づいて、前記暗号化コンテンツを復号し、コンテンツを生成する復号部と
前記コンテンツを再生する再生部とを備える
ことを特徴とする請求項１に記載の端末装置。
【請求項９】
木構造を利用して端末装置が保有するデバイス鍵を管理している鍵データ生成装置と端

末装置とからなる著作物保護システムであって、
前記鍵データ生成装置は、
コンテンツを利用するために用いる第１鍵データを、前記デバイス鍵に対して生成した変換情報を用いて、予め定められた変換規則に基づいて変換することで第２鍵データを生成する変換手段と、
前記デバイス鍵を用いて前記第２鍵データを暗号化し、暗号化鍵データを生成する暗号化手段と、
前記暗号化鍵データの生成に用いられたデバイス鍵の前記木構造での位置情報に基づいて生成された、前記変換情報を生成するための情報であるヘッダ情報を生成するヘッダ情報生成手段と、
前記ヘッダ情報を付随させた前記暗号化鍵データを出力する出力手段とを備え、
前記端末装置は、
複数のデバイス鍵を保持している保持手段と、
前記木構造における当該端末装置の位置情報を保持している保持手段と、
前記暗号化鍵データと前記暗号化鍵データに付随するヘッダ情報とを取得する取得手段と、
前記暗号化鍵データを、前記端末装置が保持するデバイス鍵のうちの一つを用いて復号し、第２鍵データを生成する復号手段と、
前記ヘッダ情報と前記位置情報とから変換情報を生成し、前記第２鍵データを、前記生成した変換情報を用いて、予め定められた変換規則に基づいて変換することで第１鍵データを生成する変換手段と、
前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用手段とを備える。
【請求項１０】
コンテンツを利用する端末装置で用いられる方法であって、
前記端末装置は、
複数のデバイス鍵を保持している保持手段と、
木構造における当該端末装置の位置情報を保持している保持手段とを備え、
前記方法は、
（ａ）木構造を利用して端末装置が保有するデバイス鍵を管理している鍵データ生成装置により、コンテンツを利用するために用いる第１鍵データを、前記デバイス鍵に対して生成した変換情報を用いて、予め定められた変換規則に基づいて変換した第２鍵データを、前記デバイス鍵を用いて暗号化することで生成された暗号化鍵データと、（ｂ）前記暗号化鍵データの生成に用いられたデバイス鍵の前記木構造での位置情報に基づいて生成された、前記変換情報を生成するための情報であるヘッダ情報とを取得する取得ステップと、
前記暗号化鍵データを、当該端末装置が保持するデバイス鍵のうちの一つを用いて復号し、第２鍵データを生成する復号ステップと、
前記ヘッダ情報と前記位置情報とから変換情報を生成し、前記第２鍵データを、前記生成した変換情報を用いて、予め定められた変換規則に基づいて変換することで第１鍵データを生成する変換ステップと、
前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用ステップと
を含むことを特徴とする方法。
【請求項１１】
コンテンツを利用する端末装置で用いられるコンピュータプログラムであって、
前記端末装置は、
複数のデバイス鍵を保持している保持手段と、
木構造における当該端末装置の位置情報を保持している保持手段とを備え、
前記コンピュータプログラムは、
（ａ）木構造を利用して端末装置が保有するデバイス鍵を管理している鍵データ生成装置により、コンテンツを利用するために用いる第１鍵データを、前記デバイス鍵に対して

生成した変換情報を用いて、予め定められた変換規則に基づいて変換した第２鍵データを、前記デバイス鍵を用いて暗号化することで生成された暗号化鍵データと、（ｂ）前記暗号化鍵データの生成に用いられたデバイス鍵の前記木構造での位置情報に基づいて生成された、前記変換情報を生成するための情報であるヘッダ情報とを取得する取得ステップと、

前記暗号化鍵データを、当該端末装置が保持するデバイス鍵のうちの一つを用いて復号し、第２鍵データを生成する復号ステップと、

前記ヘッダ情報と前記位置情報とから変換情報を生成し、前記第２鍵データを、前記生成した変換情報を用いて、予め定められた変換規則に基づいて変換することで第１鍵データを生成する変換ステップと、

前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用ステップと

を含むことを特徴とするコンピュータプログラム。

【請求項１２】

コンテンツを利用する端末装置で用いられる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記録媒体であって、

前記端末装置は、

複数のデバイス鍵を保持している保持手段と、

木構造における当該端末装置の位置情報を保持している保持手段とを備え、

前記コンピュータプログラムは、

（ａ）木構造を利用して端末装置が保有するデバイス鍵を管理している鍵データ生成装置により、コンテンツを利用するために用いる第１鍵データを、前記デバイス鍵に対して生成した変換情報を用いて、予め定められた変換規則に基づいて変換した第２鍵データを、前記デバイス鍵を用いて暗号化することで生成された暗号化鍵データと、（ｂ）前記暗号化鍵データの生成に用いられたデバイス鍵の前記木構造での位置情報に基づいて生成された、前記変換情報を生成するための情報であるヘッダ情報とを取得する取得ステップと、

前記暗号化鍵データを、当該端末装置が保持するデバイス鍵のうちの一つを用いて復号し、第２鍵データを生成する復号ステップと、

前記ヘッダ情報と前記位置情報とから変換情報を生成し、前記第２鍵データを、前記生成した変換情報を用いて、予め定められた変換規則に基づいて変換することで第１鍵データを生成する変換ステップと、

前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用ステップと

を含むことを特徴とする記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、映画などの著作物であるコンテンツのデジタル化データを、光ディスク等の大容量記録媒体へ記録、再生するシステムに関する。

【背景技術】

【０００２】

映画、音楽などの著作物であるコンテンツの著作権を保護するために、再生装置には、それぞれ複数のデバイス鍵を与え、記録媒体には、暗号化されたコンテンツと、再生を許可された再生装置のみがコンテンツを復号するための鍵を獲得できる鍵データが記録されている。このような鍵データを生成する鍵管理方式の一手法として、木構造を用いた鍵管理方式が提案されている。

【０００３】

非特許文献１には、木構造を用いた鍵管理方式において、個別の無効化に対応した、鍵情報の少ない鍵管理方式に関する技術が開示されている。また、非特許文献２は、非特許文献１の技術を基に、予め再生装置が保有しておくデバイス鍵の増加を抑えつつ、記録媒体に記録する鍵情報サイズを小さく出来る、デジタルコンテンツ保護用鍵管理方式に関す

る技術が開示されている。

【０００４】

ここで、非特許文献１に開示されている鍵管理方式について、概要を説明する。

鍵管理機関は、図１１に示すように、木構造の各リーフに１対１で再生装置を対応させてデバイス鍵を管理している。各再生装置は、ルートから、対応するリーフに至るまでの経路上に位置する各ノードに対応付けられているデバイス鍵を、それぞれ保持している。鍵管理機関は、コンテンツの暗号化、復号に用いるメディア鍵ＭＫを、管理しているデバイス鍵の内、最も多くの再生装置が共有しているデバイス鍵Ｋを用いて暗号化する。そして、暗号化メディア鍵Ｅ（Ｋ，ＭＫ）を記録媒体に書き込む。ただし、E(X,Y)は、データYを鍵データXで暗号化したときの暗号文を意味する。

【０００５】

ここで、再生装置の内部が解析され、その再生装置が持つ全てのデバイス鍵が暴露された場合、鍵管理機関は暴露されたデバイス鍵を無効化し、残りのデバイス鍵から最も多くの再生装置が共有しているデバイス鍵を選択して、メディア鍵ＭＫの暗号化に用いる。

図１１のように、再生装置０が無効化された場合、デバイス鍵Ｋｆ，Ｋｂ，Ｋ１をそれぞれ用いてメディア鍵ＭＫを暗号化し、暗号文Ｅ（Ｋｆ，ＭＫ）、Ｅ（Ｋｂ，ＭＫ）及びＥ（Ｋ１，ＭＫ）を生成し、記録媒体に書き込む。

【０００６】

これにより、無効化された再生装置０はデバイス鍵Ｋｆ，Ｋｂ，Ｋ１を保持していないため、メディア鍵ＭＫを取得出来ず、デバイス鍵Ｋｆ，Ｋｂ，Ｋ１を保持する再生装置のみがメディア鍵ＭＫを取得可能になる。

【非特許文献１】中野、大森、館林、“デジタルコンテンツ保護用鍵管理方式”、２００１年暗号と情報セキュリティシンポジウム講演論文集、ＳＣＩＳ２００１　５Ａ－５、Ｊａｎ．２００１

【非特許文献２】中野、大森、松崎、館林、“デジタルコンテンツ保護用鍵管理方式－機構造パターン分割方式”、２００２年暗号と情報セキュリティシンポジウム講演論文集、ＳＣＩＳ２００２　１０Ｃ－１、Ｊａｎ．２００２

【発明の開示】

【発明が解決しようとする課題】

【０００７】

ここで、デバイス鍵のユニーク性が損なわれ、例えばデバイス鍵ＫｆとデバイスＫ１とが同一の値である場合、記録媒体に書き込まれている暗号文Ｅ（Ｋｆ，ＭＫ）とＥ（Ｋ１，ＭＫ）とは同一の値となる。これにより、デバイス鍵Ｋｆ及びＫ１が同一の値であることが公知となる。

その後、図１２に示すように、再生装置７が無効化された場合、鍵管理機関は、デバイス鍵Ｋｂ，Ｋｃ，Ｋ１，Ｋ６を用いてメディア鍵ＭＫを暗号化する。記録媒体には、暗号文Ｅ（Ｋｂ，ＭＫ）、Ｅ（Ｋｃ，ＭＫ）、Ｅ（Ｋ１，ＭＫ）及びＥ（Ｋ６，ＭＫ）の４つが記録される。

【０００８】

ここで、再生装置７が保持するデバイス鍵Ｋｆは既に暴露されており、且つＫｆ＝Ｋ１の事実は公知であるため、不正者が暴露されているＫｆを利用して、暗号文Ｅ（Ｋ１，ＭＫ）を復号してメディア鍵ＭＫを不正に入手する危険性がある。また、前記不正を防止するために、暗号文Ｅ（Ｋ１，ＭＫ）を記録媒体に記録しないという対策を施すと、正当な再生装置１がメディア鍵ＭＫを得られなくなり、不当に無効化されてしまう。

【０００９】

不正にメディア鍵を入手したり、無効化されるべきでない再生装置が不当に無効化されたりすることを防ぐための一手法としては、デバイス鍵のユニーク性を確保（保証）することが挙げられる。具体的には、一般的にデバイス鍵は、乱数列を生成する乱数生成器を用いて生成されるため、１つのデバイス鍵を生成する度に、それ以前に生成した全てのデバイス鍵と一致するか否かをチェックして、一致した場合はその系列を破棄し、一致しな

い場合は、その系列をデバイス鍵として採用する、という方法が考えられる。

【００１０】

しかしながら、再生装置の総数が億単位の大規模なシステムである場合、デバイス鍵生成の度にデバイス鍵の一致／不一致のチェックを行うと、膨大な時間的コストが費やされる。また、非特許文献２の鍵管理方式を利用しても同様に時間が掛かる。

そこで本発明はかかる問題点に鑑みてなされたものであり、デバイス鍵のユニーク性のチェック無しで、不正者が不正にメディア鍵を入手したり、無効化されるべきでない再生装置が不当に無効化されたりすることを防止する著作物保護システ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】

【００１１】

上記目的を達成するために本発明は、正当な端末装置のみがコンテンツを利用可能となる著作物保護システムであって、コンテンツを利用するために用いる第１鍵データを、予め定められた変換規則に基づいて変換して第２鍵データを生成する変換手段と、正当な端末装置のみが保持するデバイス鍵を用いて前記第２鍵データを暗号化し、暗号化鍵データを生成する暗号化手段と、前記暗号化鍵データを出力する出力手段とから構成される鍵データ生成装置と、暗号化鍵データを取得する取得手段と、前記暗号化鍵データを、当該端末装置が保持するデバイス鍵を用いて復号し、第２鍵データを生成する復号手段と、前記第２鍵データを、予め定められた変換規則に基づいて変換し、第１鍵データ生成する変換手段と、前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用手段とから構成される端末装置とから構成されることを特徴とする著作物保護システム。

【発明の効果】

【００１２】

本発明は、上記構成の著作物保護システムである。

また、正当な端末装置のみがコンテンツを利用可能となるように鍵データを生成する鍵データ生成装置であって、コンテンツを利用するために用いる第１鍵データを、予め定められた変換規則に基づいて変換して第２鍵データを生成する変換手段と、正当な端末装置のみが保持するデバイス鍵を用いて前記第２鍵データを暗号化し、暗号化鍵データを生成する暗号化手段と、前記暗号化鍵データを出力する出力手段とから構成されることを特徴とする鍵データ生成装置である。

【００１３】

また、コンテンツを利用する端末装置であって、鍵データ生成装置により、コンテンツを利用するために用いる第１鍵データを、予め定められた変換規則に基づいて変換した第２鍵データを、前記デバイス鍵を用いて暗号化し、生成された暗号化鍵データを取得する取得手段と、前記暗号化鍵データを、当該端末装置が保持するデバイス鍵を用いて復号し、第２鍵データを生成する復号手段と、前記第２鍵データを、予め定められた変換規則に基づいて変換し、第１鍵データ生成する変換手段と、前記第１鍵データを用いて、コンテンツを利用するコンテンツ利用手段とから構成されることを特徴とする端末装置である。

【００１４】

この構成によると、デバイス鍵が同じ値であったとしても、暗号化鍵データが同じ値になるとは限らず、暗号化鍵データからデバイス鍵の値が同一であるか否かを判断することが出来ないので、第１鍵データの不正な入手を防止することが出来る。これにより、無効化されるべきでない再生装置が不当に無効化されることが無くなる。

ここで、前記鍵データ生成装置の前記変換手段は、前記デバイス鍵に対して変換情報を生成し、生成した変換情報と、前記第１鍵データとで逆変換可能な演算を行い、前記第２鍵データを生成し、前記出力手段は、更に、前記変換情報を出力するとしても良い。

【００１５】

また、前記端末装置は、更に、複数のデバイス鍵を保持している保持手段と、前記複数のデバイス鍵から、一つのデバイス鍵を選択する選択手段とを備え、前記取得手段は、前記鍵データ生成装置により、前記デバイス鍵に対して生成した変換情報と前記第１鍵デー

タとで逆変換可能な演算を行って生成された前記第２鍵データを暗号化して生成された前記暗号化鍵データを取得し、前記復号手段は、前記選択されたデバイス鍵を用いて復号し、前記変換手段は、前記選択されたデバイス鍵に対する変換情報を生成し、前記変換情報を用いて前記選択されたデバイス鍵に所定の演算を施して前記第１鍵データを生成するとしても良い。

【００１６】

この構成によると、鍵データ生成装置は、選択したデバイス鍵に対して生成する変換情報を用いて、逆変換可能な演算を第1鍵データに施して、前記第2鍵データを生成するため、前記デバイス鍵を保持する端末装置のみが、第2鍵データを再変換し、前記第1鍵データを生成することが出来る。

ここで、前記鍵データ生成装置は、更に、木構造の各ノードに１以上のデバイス鍵を対応付けて、各端末装置が有するデバイス鍵を規定する鍵管理手段と、前記木構造において、前記正当な端末装置のみが保有するデバイス鍵の内、最上位層に位置するノードに対応付けられている１以上のデバイス鍵を選択する選択手段とを備え、前記変換手段は、選択した前記デバイス鍵の木構造における位置情報に基づいて前記変換情報を生成し、前記暗号化手段は、前記選択したデバイス鍵を用いて前記第２鍵データを暗号化するとしても良い。

【００１７】

また、前記端末装置の前記変換手段は、前記暗号化鍵データに付随するヘッダ情報から前記変換情報を生成するとしても良い。前記ヘッダ情報は、木構造を利用してデバイス鍵を管理している前記鍵データ生成装置が、前記木構造において、前記正当な端末装置のみが保有するデバイス鍵の内、最上位層に位置するノードに対応付けられている１以上のデバイス鍵を選択し、選択した前記デバイス鍵の木構造における位置情報に基づいて生成した、前記変換情報を生成するための情報であり、前記端末装置において、前記保持手段は、前記木構造での当該端末装置の位置情報を保持しており、前記変換手段は、前記ヘッダ情報と前記位置情報とから前記変換情報を生成するとしても良い。

【００１８】

この構成によると、鍵データ生成装置は、選択したデバイス鍵の、木構造での位置に基づいて生成した変換情報を利用して、前記第1鍵データを変換するため、デバイス鍵の値が同じであったとしても、木構造での位置が異なるデバイス鍵は、第2鍵データを正しく再変換できない。これにより、第１鍵データの不正な入手を防ぐことが可能となる。

ここで、前記鍵データ生成装置は、更に、木構造の各ノードに１以上のデバイス鍵を対応付けて、各端末装置が保持するデバイス鍵と、それらのデバイス鍵が無効化されているか否かとを規定する鍵管理手段と、前記木構造において、無効化されていない前記正当な端末装置のみが保有するデバイス鍵の内、最上位層に位置するノードに対応付けられている１以上のデバイス鍵を選択する選択手段とを備え、前記変換手段は、前記選択したデバイス鍵が対応するノードと、他のノードの無効化の状態とに基づいて定義された無効化情報に基づいて変換情報を生成するとしても良い。

【００１９】

また、前記ヘッダ情報は、木構造の各ノードに１以上のデバイス鍵を対応付けて、各端末装置が保持するデバイス鍵と、それらのデバイス鍵が無効化されているか否かを管理し、前記木構造において、無効化されていない前記正当な端末装置のみが保有するデバイス鍵の内、最上位層に位置するノードに対応付けられている１以上のデバイス鍵を選択し、選択したデバイス鍵が対応するノードと、他のノードの無効化の状態とに基づいて定義された無効化情報に基づいて生成された、前記変換情報を生成するための情報であり、前記端末装置において、前記保持手段は、鍵データ生成装置において端末装置のデバイス鍵を管理している木構造での当該端末装置の位置情報を保持しており、前記変換手段は、前記ヘッダ情報と、前記位置情報とから前記変換情報を生成するとしても良い。

【００２０】

この構成によると、変換情報は、無効化されたデバイス鍵の、木構造における位置関係

により生成されるので、木構造での位置が異なるデバイス鍵は、第2鍵データを正しく再変換できない。これにより、第１鍵データの不正な入手を防ぐことが可能となる。

ここで、前記鍵データ生成装置の前記変換手段は、ルートから、選択した前記デバイス鍵が対応しているノードに至るまでの経路を構成するパスを識別するID情報を連結して前記変換情報を生成するとしても良い。

【００２１】

また、前記鍵データ生成装置の前記変換手段は、前記選択したデバイス鍵が対応するノードの位置を、前記木構造における階層、及び同一階層の各ノードの位置関係で表現したものを前記変換情報として生成するとしても良い。

また、前記鍵データ生成装置の前記変換手段は、ルートから、選択した前記デバイス鍵が対応しているノードまでの経路に位置する各ノードに対する無効化情報を連結して前記変換情報を生成するとしても良い。

【００２２】

また、前記鍵データ生成装置の前記変換手段は、所定の順序で並べた各ノードに対応付けられた無効化情報を、先頭の無効化情報から前記選択されたデバイス鍵が対応するノードの無効化情報までを連結して前記変換情報を生成するとしても良い。

この構成によると、デバイス鍵の、木構造での位置によって、多くのパターンが存在するため、正当なデバイス鍵の木構造での位置情報を持たない端末装置は、変換情報を生成することが出来ず、第1鍵データを入手することが出来ない。

【００２３】

ここで、前記鍵データ生成装置の前記変換手段は、前記デバイス鍵に対して変換情報を生成し、当該変換情報を、前記第１鍵データに含まれる冗長部分の少なくとも一部に埋め込んで前記第２鍵データを生成するとしても良い。

また、前記鍵データ生成装置の前記変換手段は、前記デバイス鍵に対して乱数を生成し、生成した乱数を、前記第１鍵データに含まれる冗長部分の少なくとも一部分に埋め込み、前記第２鍵データを生成するとしても良い。

【００２４】

また、前記端末装置において、前記変換手段は、前記第２鍵データの冗長部分を削除して、前記第１鍵データを生成するとしても良い。

この構成によると、第1鍵データに冗長ビットが含まれる場合、変換情報又は変換の度に異なる値を冗長ビットに埋め込むため、記録されている暗号化鍵データの値から、同一の値のデバイス鍵で暗号化した鍵データを探すことは困難になるため、正しい鍵データの位置を特定できる端末装置のみが前記第1鍵データを入手することが出来る。

【００２５】

ここで、前記鍵データ生成装置の前記変換手段は、前記冗長部分のうち、前記乱数を埋め込んでいない部分を、他の情報の伝達に用いるとしても良い。

この構成によると、一部の冗長ビットに乱数を埋め込み、残りの部分を情報伝達用に利用するため、他の情報を伝達しつつ、不正な第1鍵データの入手を防止することが出来る。

【発明を実施するための最良の形態】

【００２６】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

（実施の形態１）

１．　著作権保護システムの構成

著作権保護システムは、図1及び図６に示すように、鍵データ生成装置１００、複数の再生装置２００ａ、２００ｂ、・・・及びDVD３００から構成される。なお、図６には、再生装置２００ａ、２００ｂ、・・・に共通の構成を、再生装置２００として図示している。

【００２７】

鍵データ生成装置１００は、管理機関が保持し、コンテンツと、当該コンテンツを再生

するための鍵データとをDVD３００に記録する。鍵データは、正当な再生装置のみが前記コンテンツを再生可能となるように、選択された鍵データであり、木構造を利用して管理している。

再生装置２００ａ、２００ｂ、・・・は、それぞれユーザが有し、鍵データ生成装置１００によって予め割り当てられている複数のデバイス鍵を保持している。また、デバイス鍵から適切なデバイス鍵を選択し、選択したデバイス鍵を用いてDVD３００に記録されている暗号化コンテンツを復号し、再生する。

【００２８】

以下、各構成について説明する。

１．１　鍵データ生成装置１００

鍵データ生成装置１００は図１に示すように、デバイス鍵格納部１０１、デバイス鍵選択部１０２、変換部１０３、変換情報生成部１０４、メディア鍵暗号化部１０５、コンテンツ鍵暗号化部１０６、コンテンツ暗号化部１０７、入力部１０８、制御部１０９及びドライブ部１１０から構成される。

【００２９】

鍵データ生成装置１００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、ディスプレィユニット、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。

【００３０】

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、鍵データ生成装置１００は、その機能を達成する。

（１）入力部１０８、ドライブ部１１０

入力部１０８は、外部から、メディア鍵MK、コンテンツ鍵CK及びコンテンツの入力を受け付ける。メディア鍵MKは、変換部１０３及びコンテンツ鍵暗号化部１０６へ出力し、コンテンツ鍵CKは、コンテンツ鍵暗号化部１０６及びコンテンツ暗号化部１０７へ出力し、コンテンツは、コンテンツ暗号化部１０７へ出力する。

【００３１】

なお、メディア鍵は、DVD３００に固有の情報であっても良いし、固有の情報から生成される鍵データであっても良い。

ドライブ部１１０は、制御部１０９の制御の基、変換情報、暗号化された鍵データ及び暗号化コンテンツをDVD３００に書き込む。

（２）制御部１０９

制御部１０９は、デバイス鍵選択部１０２を制御して、管理しているデバイス鍵の中で、最も多くの再生装置が共有している１以上のデバイス鍵を選択させる。

【００３２】

また、変換情報生成部１０４を制御して、選択したそれぞれのデバイス鍵に対する変換情報を生成させる。

次に、制御部１０９は、変換部１０３を制御し、変換情報生成部１０４により生成された変換情報をそれぞれ用いて、メディア鍵MKを変換させる。

また、メディア鍵暗号化部１０５を制御して、選択したそれぞれのデバイス鍵を用いて、変換後のメディア鍵MKを暗号化させる。また、コンテンツ鍵暗号化部１０６を制御し、メディア鍵MKを用いて受け取ったコンテンツを暗号化させる。また、コンテンツ暗号化部１０７を制御してコンテンツを暗号化させる。

【００３３】

それぞれ暗号化した鍵データ、変換情報及び暗号化コンテンツをドライブ部１１０を介してDVD３００へ書き込む。

（３）デバイス鍵格納部１０１

デバイス鍵格納部１０１は、著作権保護システムに属する全ての再生装置に与えられる

デバイス鍵を格納している。

【００３４】

デバイス鍵格納部１０１が格納しているデバイス鍵は、図２に示す木構造鍵管理方式を利用して生成され、各再生装置に割り当てられている。

なお、本実施の形態では３階層の３分木として説明するが、３分木でなくてもよく、更に多数の階層から構成されるとしても良い。木構造鍵管理方式については、非特許文献２に詳しく記述されている。

【００３５】

ここで、木構造について簡単に説明する。

木構造は、ノードとパスにより構成される。木構造における各節をノードと呼び、ノードとノードとは、パスにより連結されている。木構造におけるノードの位置する各層をレイヤと呼ぶ。あるノードから上に伸びる１つのパスにより連結されているノードを、そのノードの親ノードと呼ぶ。また、下に派生した複数のパスにより連結されるノードを、そのノードの子ノードと呼ぶ。

【００３６】

また、最上位層に位置するノードをルートと呼び、最下位層に位置するノードをリーフと呼ぶ。リーフには、1対１で再生装置が割り当てられている。図２では、再生装置を０～８の番号を付して示している。

また、各ノードは、ノードIDを割り当てられている。ノードIDとは、各ノードから派生するパスに、左から順に００、０１、１０のパス番号を振っていき、ルートからそのノードまでのパス番号を連結したものをノードIDと呼ぶ。例えば、再生装置６が割り当てられているリーフのノードIDは、「１０００」となる。

【００３７】

ここで、著作権保護システムにおける、デバイス鍵の割り当て方について簡単に説明する。

（ルート）

ルートには、複数のデバイス鍵が割り当てられている。図２では、これらのデバイス鍵を、Ka－0000、Ka－0001、Ka－0010、Ka－0011、Ka－0100、Ka－0101及びKa－0110のように、識別情報で表している。識別情報は、Ka－の部分がルートに割り当てられていることを示す。Ka－の後に付されている４ビットがNRP（Node Revocation Pattern）であり、このNRPの内、上位１ビットは、リーフに対して親ノードであるかを識別する。「１」のときはリーフの親ノードであることを示し、「０」のときは、それ以外のノードであることを示す。

【００３８】

また、4ビットのNRPの内、下位３ビットは無効化情報を表している。無効化情報は、ルートの各子ノードに対応付けられたデバイス鍵の中に、無効化すべきデバイス鍵が存在する子ノードを「１」、そうでない子ノードを「０」と表現し、木構造の左から順に連結したものである。

ここで、無効化とは、内部を解析され、再生装置が保持しているデバイス鍵が暴露された場合などに、当該再生装置及びデバイス鍵を無効にすることを示す。このような無効化されたデバイス鍵が対応するノードは無効化し、無効化されたノードを無効化ノードと呼ぶ。

【００３９】

Ka－0000は、木構造に属する全ての再生装置が備える鍵であり、木構造に属する何れの再生装置も無効化されていない初期状態では、このデバイス鍵が使用される。

また、その他のデバイス鍵は、子ノードに無効化されたデバイス鍵が存在する場合に、メディア鍵の暗号化に使用される鍵である。

例えば、ルートに対して左側の子ノードの下位に無効化された再生装置が属し、他の子ノードには無効化された再生装置が属していない場合、無効化情報「100」の、Ka－0100で識別されるデバイス鍵が使用される。このように、各無効化情報に対応するデバイス鍵

が割り当てられており、無効化された再生装置の木構造での位置によって、以降、何れの無効化情報で識別するデバイス鍵を使用するか選択される。

【００４０】

また、全ての子ノードに無効化された再生装置が属する場合、下位のレイヤのノードに割り当てられたデバイス鍵を使用するため、「111」の無効化情報が付されたデバイス鍵は、割り当てられていない。

（ノード）

レイヤ１の左側のノードには、Kb－1001、Kb－1010、Kb－1011、Kb－1100、Kb－1101及びKb－1110の6個のデバイス鍵が割り当てられている。Kbは、レイヤ１の左側のノードに割り当てられていることを示し、ルートのデバイス鍵と同様に、子ノードの無効化情報によって、識別される。また、ノードの下位に位置するノードに無効化された再生装置が存在しない場合、ノードの上位のノードであるルートに割り当てられているデバイス鍵を使用するため、無効化情報が「000」のデバイス鍵は割り当てられていない。また、子ノードである3つのリーフに対応するの全ての再生装置が無効化されている場合、そのノードに割り当てられているデバイス鍵は使用されないため、無効化情報が「111」のデバイス鍵は割り当てられない。

【００４１】

また、他のノードも同様の無効化情報で識別される6個のデバイス鍵を割り当てられている。

（リーフ）

各リーフには、それぞれ再生装置が割り当てられている。ここでは０～８の番号で識別する。

【００４２】

レイヤ２で左側のリーフには、デバイス鍵Ka－0000、Ka－0001、Ka－0010、Ka－0011、Kb－1001、Kb－1010及びKb－1011が割り当てられている。

前記リーフには、リーフからルートに至るパス上に位置する全てのノードに割り当てられているデバイス鍵の内、当該リーフに対応する再生装置０が無効化されているときの無効化パターンに対応するデバイス鍵を除くデバイス鍵を割り当てる。つまり、ルート及びレイヤ１の左側ノードに割り当てられているデバイス鍵の内、Ka－0100、Ka－0101、Ka－0110、Kb－1100、Kb－1101及びKb－1110は、再生装置０が無効化されている場合に利用される鍵であるため、前記リーフには割り当てられない。

【００４３】

他のリーフも、同様にデバイス鍵が割り当てられている。

（４）デバイス鍵選択部１０２

デバイス鍵選択部１０２は、無効化された再生装置でコンテンツを利用できないように、デバイス鍵を選択し、選択したデバイス鍵をメディア鍵暗号化部１０５へ出力する。

初期状態では、「Ka－0000」を選択する。選択したデバイス鍵をメディア鍵暗号化部１０５へ出力する。

【００４４】

無効化された再生装置がある場合のデバイス鍵の選択方法を、図３を用いて説明する。

再生装置０及び８が無効化されている場合、ルートから再生装置０及び８が対応するリーフまでのパス上に位置する全てのノードを無効化する。図３では無効化ノードに×を付して表している。無効化すると、それまで使用していたデバイス鍵は使用できなくなる。つまり、初期状態で使用していたKa－0000は使用できない。

【００４５】

次に、全ての無効化ノードに対して、そのノードの無効化パターンに対応するデバイス鍵を選択する。ルートの場合、左右の子ノードが無効化されているため、無効化情報が「101」のデバイス鍵Ka－0101を選択する。

レイヤ１の左側ノードの場合、左側の子ノードが無効化されているため、無効化情報が「100」のデバイス鍵Kb－1100を選択する。ノードレイヤ１の中央ノードには、無効化さ

れている子ノードが無く、上位のレイヤ、この場合ルートに割り当てられているデバイス鍵Ka－0101が使用される。レイヤ１の右側ノードの場合、右側の子ノードが無効化されているため、無効化情報が「001」のデバイス鍵Ｋｄ－1001を選択する。

（５）変換情報生成部１０４

変換情報生成部１０４は、デバイス鍵選択部１０２によって選択された全てのデバイス鍵に対して、それぞれ変換情報を生成する。

【００４６】

ここで変換情報は、ルートから、選択されたデバイス鍵が割り当てられているノードまでのNRPを連結したものである。

図３のように、再生装置０及び８が無効化されている場合、変換情報生成部１０４は、デバイス鍵選択部１０２により選択されたデバイス鍵Ｋａ－0101、Kb－1100及びKd－1001に対して変換情報を生成する。

【００４７】

まず、再生装置３～５が共有するデバイス鍵Ka－0101に対する変換情報を生成する。ここで、ルートからデバイス鍵Ｋａ－0101が割り当てられているノードまでのNRPは、「１０１」のみであるため、「１０１」を変換情報とし、変換部１０３へ出力する。

次に、再生装置１，２が共有するデバイス鍵Kb－1100に対する変換情報を生成する。ルートからデバイス鍵Kb－1100が割り当てられているノードまでのNRPは、「１０１」及び「１００」であるため、これらを連結した変換情報「１０１１００」を生成する。生成した変換情報を、変換部１０３へ出力する。

【００４８】

次に、再生装置６，７が共有するデバイス鍵Ｋｄ－1001に対する変換情報を生成する。ルートからデバイス鍵Ｋｄ－1001が割り当てられているノードまでのNRPは、「１０１」及び「００１」であるため、これらを連結した変換情報「１０１００１」を生成する。生成した変換情報を、変換部１０３へ出力する。

また、変換情報の生成に用いた各NRPを、上位のレイヤに割り当てられている順に、ドライブ部１１０を介してDVD３００の変換情報記録領域３０１へ書き込む。

【００４９】

なお、暗号化メディア鍵又は暗号化コンテンツ鍵などに付随するヘッダ情報を変換情報として利用できる場合は、変換情報を記録しなくても良い。また、再生装置が変換情報を生成できる場合も、変換情報を記録しない構成であっても良い。

（６）変換部１０３

変換部１０３は、外部から入力部１０８を介してメディア鍵を受け取り、変換情報生成部１０４から変換情報を受け取る。受け取った変換情報をそれぞれ用いて、メディア鍵にＸＯＲ演算を施して変換する。

【００５０】

具体的には、図４（ａ）に示すように、まず、デバイス鍵Ka－0101に対応する変換情報「０１０１」を用いてメディア鍵MKを変換し、変換後メディア鍵MK’を生成する。次に、図４（ｂ）に示すように、デバイス鍵Kb-1100に対応する変換情報「０１０１１１００」を用いてメディア鍵MKを変換し、変換後メディア鍵ＭＫ”を生成する。また、図４（ｃ）に示すように、デバイス鍵Kd-1001に対応する変換情報「０１０１１００１」を用いてメディア鍵MKを変換し、変換後メディア鍵ＭＫ’’’を生成する。

【００５１】

変換部１０３は、生成した変換後メディア鍵MK’、ＭＫ”及びＭＫ’’’をメディア鍵暗号化部１０５へ出力する。

（７）メディア鍵暗号化部１０５

メディア鍵暗号化部１０５は、デバイス鍵選択部１０２からデバイス鍵を受け取り、変換部１０３から変換後メディア鍵を受け取る。受け取ったデバイス鍵をそれぞれ用いて、各変換後メディア鍵を暗号化する。

【００５２】

具体的には、図４（ａ）に示すように、まず、デバイス鍵Ka－0101を用いて変換後メディア鍵MK’に暗号化アルゴリズムE1を施し、暗号化メディア鍵E（Ka－0101, MK’）を生成する。ここで、暗号化アルゴリズムE1は、一例としてAES（Advanced Encryption Standard）である。AESについては、公知であるので説明を省略する。また、E(X,Y)は、データYを鍵データXで暗号化したときの暗号文を意味する。

【００５３】

同様に、図４（ｂ）に示すように、デバイス鍵Kb-1100を用いて変換後メディア鍵ＭＫ”に暗号化アルゴリズムE1を施して、暗号化メディア鍵E（Kb－1100, ＭＫ”）を生成する。次に、図４（ｃ）に示すように、デバイス鍵Kd-1001を用いて変換後メディア鍵ＭＫ’’’を暗号化し、暗号化メディア鍵E（Kd－1001, ＭＫ’’’）を生成する。

また、メディア鍵暗号化部１０５は、生成した暗号化メディア鍵E（Ka－0101, MK’）、E（Kb－1100, ＭＫ”）及びE（Kd－1001, ＭＫ’’’）を、ドライブ部１１０を介してDVD３００のメディア鍵データ記録領域３０２に書き込む。

（８）コンテンツ鍵暗号化部１０６

コンテンツ鍵暗号化部１０６は、入力部１０８を介してコンテンツ鍵CK及びメディア鍵MKを受け取る。受け取ったメディア鍵MKを用いてコンテンツ鍵CKに暗号化アルゴリズムＥ１を施して暗号化し、暗号化コンテンツ鍵E(MK,CK)を生成する。生成した暗号化コンテンツ鍵E(MK,CK)を、ドライブ部１１０を介してDVD３００のコンテンツ鍵データ記録領域３０３へ書き込む。

（９）コンテンツ暗号化部１０７

コンテンツ暗号化部１０７は、外部から入力部１０８を介してコンテンツ及びコンテンツ鍵CKを受け取る。受け取ったコンテンツ鍵CKを用いてコンテンツに暗号化アルゴリズムＥ１を施して暗号化し、暗号化コンテンツE(CK,コンテンツ)を生成する。生成した暗号化コンテンツE(CK,コンテンツ)を、ドライブ部１１０を介してDVD３００のコンテンツ記録領域３０４へ書き込む。

１．２　DVD３００

DVD３００は、図５に示すように、変換情報記録領域３０１、メディア鍵データ記録領域３０２、コンテンツ鍵データ記録領域３０３及びコンテンツ記録領域３０４を含む。

【００５４】

変換情報記録領域３０１は、変換情報の生成に用いた各NRPを、書き込む領域である。上位のレイヤに存在するノードに対応するNRPから順に書き込まれる。

メディア鍵データ記録領域３０２は、暗号化メディア鍵を記録する領域である。暗号化メディア鍵は、木構造で上位のレイヤに割り当てられているデバイス鍵を用いて暗号化された暗号化メディア鍵から順に記録される。

【００５５】

コンテンツ鍵データ記録領域３０３は、暗号化コンテンツ鍵を記録する領域である。

コンテンツ記録領域３０４は、暗号化コンテンツを記録する領域である。

１．３　再生装置２００

再生装置２００ａ、２００ｂ、・・・の共通の構成を示す再生装置２００は、木構造において、再生装置０～８の何れかに該当する。

【００５６】

再生装置２００は、図６に示すように、デバイス鍵選択部２０１、デバイス鍵格納部２０２、メディア鍵復号部２０３、変換部２０４、コンテンツ鍵復号部２０５、コンテンツ復号部２０６、ドライブ部２０７、再生部２０８、制御部２０９及び入力部２１０から構成される。また、再生部２０８には、モニタ２２０及びスピーカ２２１が接続されている。

【００５７】

再生装置２００は、鍵データ生成装置１００と同様に、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などから構成されるコンピュータシステムである。

前記マイクロプロセッサが、前記RAM又は前記ハードディスクユニットに記憶されておる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。

（１）ドライブ部２０７、入力部２１０

入力部２１０は、外部からの入力を受け付け、受け付けた入力情報を制御部２０９へ出力する。

【００５８】

ドライブ部２０７は、制御部２０９の制御の基、DVD３００から情報を読み出す。

まず、ドライブ部２０７は、制御部２０９の制御の基、ＤＶＤ３００の変換情報記録領域３０１から変換情報を読み出し、デバイス鍵選択部２０１へ出力する。

次に、メディア鍵データ記録領域３０２から暗号化メディア鍵を読み出して、メディア鍵復号部２０３へ出力する。

【００５９】

また、コンテンツ鍵データ記録領域３０３から暗号化コンテンツ鍵Ｅ（ＭＫ，ＣＫ）を読み出し、コンテンツ鍵復号部２０５へ出力する。

また、コンテンツ記録領域３０４から暗号化コンテンツＥ（ＣＫ，コンテンツ）を読み出し、コンテンツ復号部２０６へ出力する。

（２）再生部２０８

再生部２０８は、制御部２０９の制御の基、コンテンツ復号部２０６から受け取るコンテンツから映像信号を生成し、生成した映像信号をモニタ２２０へ出力する。また、受け取ったコンテンツから音声信号を生成し、生成した音声信号をスピーカ２２１へ出力する。

（３）制御部２０９

制御部２０９は、入力部２１０から、DVD３００に記録されているコンテンツの再生を指示する指示情報を受け取ると、DVD３００から各データを読み出すようにドライブ部２０７を制御する。

【００６０】

まず、デバイス鍵選択部２０１を制御して、デバイス鍵を選択し、暗号化メディア鍵の記録位置の特定及び変換情報の生成を行う。

次に、メディア鍵復号部２０３を制御し、暗号化メディア鍵を復号して変換後メディア鍵を生成し、変換後メディア鍵を変換部２０４で再度変換してメディア鍵を生成する。

また、コンテンツ鍵復号部２０５を制御し、メディア鍵を用いて、読み出した暗号化コンテンツ鍵を復号させ、コンテンツ鍵を生成する。生成したコンテンツ鍵を用いて、コンテンツ復号部２０６で読み出した暗号化コンテンツを復号させてコンテンツを生成し、再生部２０８を制御してコンテンツを再生させる。

（４）デバイス鍵格納部２０２

デバイス鍵格納部２０２は、管理者によって再生装置２００に割り当てられている複数のデバイス鍵を格納している。割り当てられている鍵は、図２の、再生装置０～８のそれぞれ下に示している識別子で示している。例えば再生装置６は、Ka‐0000、Ka‐0010、Ka‐0100、Ka‐0110、Kd－1001、Kd－1010及びKd－1011の識別情報で示されるデバイス鍵を保持している。

【００６１】

また、デバイス鍵格納部２０２は、木構造において、当該再生装置２００が対応付けられているルートの位置を示すID情報を記録している。

（５）デバイス鍵選択部２０１

デバイス鍵選択部２０１は、デバイス鍵を選択する。選択したデバイス鍵を、メディア鍵復号部２０３へ出力する。なお、デバイス鍵の選択方法としては、再生装置にデバイス鍵を割り当てる際に、それぞれのデバイス鍵に予め識別子を付しておき、鍵データ生成装置はDVDに選択すべきデバイス鍵の識別子を記録し、再生装置はDVDに記録されている識別子が示すデバイス鍵を選択する、などの方法があるが、デバイス鍵の選択方法は公知であ

るので、詳しい説明を省略する。

【００６２】

また、選択したデバイス鍵に対応する暗号化メディア鍵の記録位置の特定及び変換情報の生成を行い、記録位置をメディア鍵復号部２０３へ出力し、変換情報を変換部２０４へ出力する。なお、記録位置の特定及び変換情報の生成処理については後述する。

（６）メディア鍵復号部２０３

メディア鍵復号部２０３は、デバイス鍵選択部２０１からデバイス鍵及び暗号化メディア鍵の記録位置を受け取る。受け取った記録位置が示す領域に記録されている暗号化メディア鍵を、ドライブ部２０７を介してDVD３００から読み出す。

【００６３】

メディア鍵復号部２０３は、暗号化メディア鍵に、デバイス鍵を用いて復号アルゴリズムＤ１を施し、変換後メディア鍵を生成する。ここで、復号アルゴリズムD1は、暗号化アルゴリズムE1の逆の処理を行う。メディア鍵復号部２０３は、生成した変換後メディア鍵を変換部２０４へ出力する。

具体的には、選択したデバイス鍵がKa－0101の場合、図７（ａ）に示すように、選択したデバイス鍵Ka‐0101を用いて暗号化メディア鍵E（Ka－0101，MK’）を復号し、変換後メディア鍵MK’を生成する。選択したデバイス鍵がKb-1100の場合、図７（ｂ）に示すように、暗号化メディア鍵E（Kb－1100，ＭＫ”）を復号し、変換後メディア鍵ＭＫ”を生成する。また、選択したデバイス鍵がKd-1001の場合、図７（ｃ）に示すように、暗号化メディア鍵E（Kd－1001，ＭＫ’’’）を復号し、変換後メディア鍵ＭＫ’’’を生成する。

【００６４】

生成した変換後メディア鍵MK’、ＭＫ” 又はＭＫ’’’を、変換部２０４へ出力する。

（７）変換部２０４

変換部２０４は、メディア鍵復号部２０３から変換後メディア鍵を受け取り、デバイス鍵選択部２０１から変換情報を受け取る。

【００６５】

デバイス鍵選択部２０１により生成された変換情報で、受け取った変換後メディア鍵にＸＯＲ演算を行い、メディア鍵を生成する。

具体的には、選択したデバイス鍵がKa－0101の場合、図７（ａ）に示すように、デバイス鍵がKa－0101に対する変換情報「０１０１」を用いて変換後メディア鍵MK’を変換し、メディア鍵ＭＫを生成する。また、選択したデバイス鍵がKb-1100の場合、図７（ｂ）に示すように、対応する変換情報「０１０１１１００」を用いて変換後メディア鍵MK’を変換し、メディア鍵ＭＫを生成する。また、選択したデバイス鍵がKd－1001の場合、図７（ｃ）に示すように、対応する変換情報「０１０１１００１」を用いて変換後メディア鍵ＭＫ’’’を変換し、メディア鍵ＭＫを生成する。

【００６６】

変換して生成したメディア鍵MKを、コンテンツ鍵復号部２０５へ出力する。

（８）コンテンツ鍵復号部２０５

コンテンツ鍵復号部２０５は、ドライブ部２０７から暗号化コンテンツ鍵を受け取り、変換部２０４からメディア鍵を受け取る。受け取ったメディア鍵を用いて暗号化コンテンツ鍵に復号アルゴリズムD1を施してコンテンツ鍵を生成する。生成したコンテンツ鍵は、コンテンツ復号部２０６へ出力する。

（９）コンテンツ復号部２０６

コンテンツ復号部２０６は、ドライブ部２０７から暗号化コンテンツを受け取り、コンテンツ鍵復号部２０５からコンテンツ鍵を受け取る。受け取ったコンテンツ鍵を用いて暗号化コンテンツに復号アルゴリズムD1を施してコンテンツを生成し、生成したコンテンツを再生部２０８へ出力する。

２．　著作権保護システムの動作

２．１　鍵データ生成装置１００の動作

鍵データ生成装置１００の動作を、図８を用いて説明する。

【００６７】

デバイス鍵選択部１０２は、最も多くの、無効化されていない再生装置が共有しているデバイス鍵を１個以上選択する（ステップＳ４０１）。選択したデバイス鍵をメディア鍵暗号化部１０５及び変換情報生成部１０４へ出力する。

次に変換情報生成部１０４、変換部１０３及びメディア鍵暗号化部１０５は、選択したデバイス鍵それぞれに対して、以下の処理（ステップＳ４０３～４０５）を繰り返し行う。なお、図８でAは、選択したデバイス鍵の数を示す。

【００６８】

変換情報生成部１０４は、変換情報を生成し（ステップＳ４０３）、変換部１０３へ出力する。変換部１０３は、入力部１０８を介して取得したメディア鍵を変換して、変換後メディア鍵を生成し（ステップＳ４０４）、生成した変換後メディア鍵をメディア鍵暗号化部１０５へ出力する。メディア鍵暗号化部１０５は、選択したデバイス鍵と、変換後メディア鍵とを取得し、取得したデバイス鍵を用いて、変換後メディア鍵を暗号化し、暗号化メディア鍵を生成する（ステップＳ４０５）。

【００６９】

選択した全てのデバイス鍵に対してステップＳ４０３～４０５の処理を行うと、生成した変換情報及び暗号化メディア鍵をドライブ部１１０を介してDVD３００へ書き込む（ステップＳ４０６）。

次に、コンテンツ鍵暗号化部１０６は、変換前のメディア鍵を用いてコンテンツ鍵を暗号化し、暗号化コンテンツ鍵を生成する。生成した暗号化コンテンツ鍵をドライブ部１１０を介してDVD３００に書き込む（ステップＳ４０７）。

【００７０】

また、コンテンツ暗号化部１０７は、コンテンツ鍵を用いてコンテンツを暗号化し、暗号化コンテンツを生成する。生成した暗号化コンテンツをドライブ部１１０を介してDVD３００へ書き込む（ステップＳ４０８）。

２．２　再生装置の動作

再生装置２００がDVD３００に記録されているコンテンツを再生する際の動作を、図９を用いて説明する。

【００７１】

デバイス鍵選択部２０１は、ドライブ部２０７を介して読み出した変換情報に基づいて、デバイス鍵を選択し、暗号化メディア鍵の記録位置の特定及び変換情報の生成を行う（ステップＳ４１１）。選択したデバイス鍵及び記録位置をメディア鍵復号部２０３へ出力し、変換情報を変換部２０４へ出力する。

次にメディア鍵復号部２０３は、記録位置に従ってDVD３００から読み出した暗号化メディア鍵を、ドライブ部２０７を介して読み出し、デバイス鍵選択部２０１から受け取ったデバイス鍵を用いて暗号化メディア鍵を復号し、変換後メディア鍵を得る（ステップＳ４１２）。変換後メディア鍵を変換部２０４へ出力する。

【００７２】

変換部２０４は、デバイス鍵選択部２０１から受け取る変換情報を用いて、変換後メディア鍵にXOR演算を施し（ステップＳ４１３）、演算結果であるメディア鍵をコンテンツ鍵復号部２０５へ出力する。

コンテンツ鍵復号部２０５は、ドライブ部２０７を介してDVD３００から読み出した暗号化コンテンツ鍵を、メディア鍵を用いて復号し、コンテンツ鍵を得る（ステップＳ４１４）。コンテンツ鍵をコンテンツ復号部２０６へ出力する。

【００７３】

コンテンツ復号部２０６は、ドライブ部２０７を介してDVD３００から読み出した暗号化コンテンツを、コンテンツ鍵復号部２０５から受け取るコンテンツ鍵を用いて復号し、コンテンツを得る（ステップＳ４１５）。コンテンツを再生部２０８へ出力する。

再生部２０８は、受け取ったコンテンツを再生し、モニタ２２０及びスピーカ２２１へ出力する（ステップＳ４１６）。

２．３　暗号化メディア鍵の特定及び変換情報の生成

（１）上記ステップＳ４１１における暗号化メディア鍵の選択及び変換情報の生成について、図１０を用いて説明する。

【００７４】

デバイス鍵選択部２０１は、変換情報記録領域３０１に記録されているNRPを順にチェックする。デバイス鍵選択部２０１は、チェック中のNRPの位置を示す変数Y、暗号化メディア鍵の記録位置を示す変数Ｘ、再生装置２００自身に関係するNRPの位置を示す変数A、あるレイヤにおけるNRPの数を示す変数W、及び木構造のレイヤ数を示す値Ｄを有している。ここで、再生装置２００に関係するNRPとは、木構造において、ユーザ装置に割り当てられているリーフから、ルートに至るまでの経路上に存在するノードのＮＲＰを示す。

【００７５】

デバイス鍵選択部２０１は、レイヤｉ＝０から、レイヤｉ＝D－１まで、以下の手順で解析を行う。

デバイス鍵選択部２０１は、初期値として、それぞれ変数A＝０、変数W＝１、変数ｉ＝０、変数Y＝０及びX＝０とする（ステップＳ４２１）。

変数ｉと値Ｄとを比較し、変数ｉが値Ｄより大きい場合（ステップＳ４２２）、この再生装置２００は無効化されているので、デバイス鍵選択部２０１は、処理を終了する。

【００７６】

変数ｉが値Ｄより小さいか又は等しい場合（ステップＳ４２２）、変換情報記録領域３０１に記録されているNRPからY番目のNRPの下位３ビットが「１１１」であるか否かを判断する（ステップＳ４２３）。「１１１」である場合、Y=Y+1の演算を行い（ステップＳ４２６）、ステップＳ４２３の処理へ戻る。

下位３ビットが「１１１」でない場合、変数Yの値と変数Aの値とが等しいか否かを判断する（ステップＳ４２４）。値が異なる場合、X=X+1の演算（ステップＳ４２５）及びY=Y+1の演算（ステップＳ４２６）を行い、ステップＳ４２３の処理へ戻る。

【００７７】

変数Yの値と変数Aの値とが等しい場合、レイヤｉに存在するNRPの内、Ｙ番目のNRPの値を記憶する（ステップＳ４２７）。

次に、デバイス鍵選択部２０１は、Ｙ番目のNRPを構成する４ビットのうち、ID情報の上位２ｉビット目及び２ｉ－１ビット目の値に対応するビット位置にある値Ｂが「０」であるか、又は「１」であるかをチェックする（ステップＳ４２８）。ここで、対応するビット位置とは、ID情報の上位２ｉビット目及び２ｉ－１ビット目の値が「００」の場合、Y番目のＮＲＰの左ビットに対応し、「０１」の場合、Y番目のＮＲＰの中央ビットに対応し、「１０」の場合、Y番目のＮＲＰの右ビットに対応する。ID情報は、図２に示すように、木構造において左の経路に「００」、中央の経路に「０１」、右の経路に「１０」が割り当てられ、これらの規則に基づいて構成されているので、木構造におけるルートから、再生装置が対応するリーフに至るまでの経路を示している。

【００７８】

値Ｂが「１」の場合（ステップＳ４２８）、デバイス鍵選択部２０１は、レイヤｉに存在するW個の全ＮＲＰの「１」の数をカウントする。ただし、ＮＲＰの最上位のビットが「１」のＮＲＰについては、カウントしない。カウントした値を変数Wに代入する。こうして得られた変数Wが、次のレイヤｉ＋１に存在するNRPの数を示す。（ステップＳ４２９）。

【００７９】

次に、デバイス鍵選択部２０１は、最初のＮＲＰから数えて、対応するビット位置までのNRPの「１」の数をカウントする。ただし、NRPの最上位のビットが「１」のNRPについては、カウントしない。カウントした値を変数Ａに代入する。ここで、対応するビット位置の値はカウントしない。こうして得られた変数Ａが、次のレイヤｉ＋１のNRPの内、ユ

ーザ装置自身に関係するNRPの位置を示す（ステップＳ４３０）。
【００８０】
次に、Ｘ＝Ｘ＋１（ステップＳ４３１）、Ｙ＝０（ステップＳ４３２）、及びｉ＝ｉ＋１（ステップＳ４３３）の演算を行い、ステップＳ４２２の処理に戻る。
ステップＳ４２８で値Ｂ＝０の場合、デバイス鍵選択部２０１は、変数Xの値を、暗号化メディア鍵の記録位置として、メディア鍵復号部２０３へ出力し、生成した変換情報を変換部２０４へ出力し（ステップＳ４３４）、処理を終了する。
（２）暗号化メディア鍵の選択及び変換情報の生成の具体的な処理を、図２の再生装置６の場合を例として説明する。
【００８１】
再生装置６は、デバイス鍵として、Ka-0000、Ka-0010 、Ka-0100 、Ka-0110、Kd-1001、Kd-1010、Kd-1011を予め保持している。また、ID情報として、「１０００」を保持している。
ａ）デバイス鍵選択部２０１は、変換情報記録領域３０１に記録されている０番目のNRP「０１０１」の下位３ビットが「１１１」であるか否かを判断する（ステップＳ４２３）。
【００８２】
ｂ）「１１１」でないので、変数Y及び変数Aの値を比較し（ステップＳ４２４）、値が等しいため、レイヤ０に存在する０番目のNRP「０１０１」の値を記憶する（ステップＳ４２７）。
ｃ）ID情報の、上位２ビットの値が「１０」であるので、０番目のNRPの下位３ビットのうち、右側のビットをチェックする（ステップＳ４２８）。右ビットが「１」であるので、ステップＳ４２９以降の処理を行う。
【００８３】
ｄ）レイヤ０に存在する１個のNRP「０１０１」の下位３ビットのうちの「１」の数をカウントする（ステップＳ４２９）。カウントした値が「２」であるので、次のレイヤ１には２個のNRPが存在することが分かる。
ｅ）次に、対応するビット位置までのNRPの「０１０１」の下位３ビットの「１」の数をカウントする。ただし、対応するビット位置の値はカウントしない。カウントした値が「１」であるため、次のレイヤ１の対応するNRPの位置Aは1番目である。
【００８４】
ｆ）X=X+1、Y＝０及びｉ＝ｉ＋１の処理を行う（ステップＳ４３１～４３３）。これにより、変数Ｘの値は「１」となる。
ｇ）変換情報記録領域３０１のレイヤ１に存在する０番目のＮＲＰ「１１００」の下位３ビットが「１１１」であるか否かを判断し（ステップＳ４２３）、「１１１」ではないので、変数Y及び変数Aの値を比較する（ステップＳ４２４）。
【００８５】
ｈ）値が異なるため、X=X+1の演算を行う（ステップＳ４２５）。この結果、Xの値は「２」となる。また、Y=Y+1の演算を行う（ステップＳ４２６）。この結果、Ｙの値は「１」となる。
ｉ）レイヤ１に存在する１番目のＮＲＰ「１００１」の下位3ビットが「１１１」であるか否かを判断し、「１１１」でないので、変数Y及び変数Aの値を比較する（ステップＳ４２４）。
【００８６】
ｊ）値が等しいため、レイヤ１に存在する１番目のNRP「１００１」の値を、前回記憶したＮＲＰ「０１０１」に連結して記憶する（ステップＳ４２７）。
ｋ）ID情報の、上位３及び４ビット目の値が「００」であるので、１番目のNRPの下位３ビットのうち、左側のビットをチェックする（ステップＳ４２８）。左ビットが「０」であるので、解析を終了する。
【００８７】

１）デバイス鍵選択部２０１は、記録位置として変数Ｘの値「２」をメディア鍵復号部２０３へ出力し、変換情報として、「０１０１１００１」を変換部２０４へ出力する（ステップＳ４３４）。

以上により、再生装置６は記録位置「２」から、暗号化メディア鍵Ｅ（Kd-1001）を特定し、変換情報「０１０１１００１」を生成することが出来る。

３．　その他の変形例

なお、本発明を上記の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はもちろんである。以下のような場合も本発明に含まれる。

（１）暗号化方式としてAESを利用するとしたが、他の暗号化方式を利用しても良い。

（２）実施の形態では、メディア鍵及びコンテンツ鍵は、外部から入力されるとしたが、鍵データ生成装置に格納されているとしても良い。また、利用する都度、メディア鍵及びコンテンツ鍵を生成するとしても良い。

（３）実施の形態ではコンテンツ鍵を用いてコンテンツを暗号化し、メディア鍵を用いてコンテンツ鍵を暗号化する２階層の構成としたが、メディア鍵でコンテンツを暗号化する１階層の構成であっても良いし、鍵を追加して、階層を更に増やす構成であっても良い。階層を増やした場合、暗号化の対象となる鍵のうち、少なくとも一つを変換して暗号化すれば良い。

（４）実施の形態では、変換情報として、NRPを用いるとしたが、本発明は、これに限定されない。変換情報は、デバイス鍵を割り当てられているノードの、木構造における位置、他のノードとの関係などに対して生成されるものであり、パス番号、ノードの位置情報、NRPなどを、予め定めた規則に従って生成されるものであれば良い。例として、以下に（ａ）～（ｆ）を示す。

【００８８】

（ａ）変換情報生成部１０４は、選択されたデバイス鍵が割り当てられているノードのノードIDを求める。また、NRPも合わせて求める。これらを連結した情報を変換情報とする。具体的には、以下のようになる。

図３のように、再生装置０、１及び８が無効化されている場合、デバイス鍵選択部１０２によって、デバイス鍵Ka-0101、Kb-1100及びKd-1001が選択される。

【００８９】

変換情報生成部１０４は、まず、デバイス鍵Ka-0101に対して変換情報を生成する。ここで、デバイス鍵Ka-0101が割り当てられているノードはルートであり、ノードIDが存在しないため、NRPである「０１０１」が変換情報となる。

次に、デバイス鍵Kb-1100に対して変換情報を生成する。ここで、デバイス鍵Kb-1100が割り当てられているノードのノードIDは「００」であり、NRPが「１１００」であるため、変換情報は、これらを連結した「００１１００」となる。

【００９０】

また、デバイス鍵Kd-1001に対して変換情報を生成する。ここでデバイス鍵Kd-1001が割り当てられているノードのノードIDは「１０」であり、NRPが「１００１」であるため、変換情報は、これらを連結した「１０１００１」となる。

また、NRPと連結させずに、ノードIDのみを変換情報としても良い。この場合、デバイス鍵Ka-0101に対する変換情報は存在しないため、メディア鍵を変換せずに暗号化するとしても良いし、予めルートの場合に使用する変換情報を設定しておいても良い。この場合、他の変換情報と一致しない値を変換情報として用いる。

【００９１】

（ｂ）図２に示すように、木構造のルートを起点として、上から下、左から右の順で、各ノードに対して、それぞれを識別するための識別番号を付与していき、その識別番号を変換情報とする。

つまり、図３のように、再生装置0，1及び８が無効化されている場合、デバイス鍵選択部１０２は、Ka-0101の変換情報は「０」となる。また、Kb-1100の変換情報は「０１」、Kd-1001の変換情報は、「１１」となる。

【００９２】
（ｃ）図２に示すように、木構造の各階層にはそれぞれを識別するレイヤ番号を付与し、同一のレイヤの複数のノードに対しては、左から順に相対ノード番号を付与する。ノードの位置情報を、レイヤ番号、及び相対ノード番号に基づいて生成する。生成した位置情報を変換情報とする。
（ｄ）図２に示すように、木構造をルートを起点として、各ノードを上位層から下位層、また、同一層においては、左から右の順に検索していき、選択したデバイス鍵が対応付けられているノードまでに存在する全てのNRPを連結したものを変換情報とする。また、このとき、必要であれば生成した変換情報を圧縮して任意長に変換した系列を変換情報とする。
【００９３】
（ｅ）ルートを起点として、各ノードを上位層から階層、また、同一層においては、左から右の順に検索していき、デバイス鍵が対応付けられているノードまでに存在する全てのNRPの「１」の数（「０」の数でも良い）をカウントした結果を変換情報としても良い。
また、カウントした値を2進数に変換して、変換したデータにNRPを連結した値を変換情報としても良い。
【００９４】
このとき、連結するNRPは、ルートから、デバイス鍵が割り当てられているノードまでの間に存在するNRPであっても、上記ルールに基づき検索した全NRPであっても良い。また、最後に検索した1つのNRPのみを連結する構成であっても良い。或いは使用するデバイス鍵を識別するための識別子を連結する構成であっても良い。
（ｆ）ルートを起点として検索し、デバイス鍵が対応付けられているノードまでに存在する全てのNRPを１０進数に変換して、それらの総和を変換情報としても良い。或いは、NRPを２進数としてXOR演算し、その結果を変換情報としても良い。
（５）実施の形態でNRPの上位１ビットは、リーフの一つ上のレイヤに存在するノードであるかを示すとしたが、他の情報の伝達に使用しても良い。例えば、そのノードの子孫に有効な装置が存在するか否かを示すフラグとして利用できる。また、これらを組み合わせても良い。また、４ビットのNRPのうち、下位３ビット或いは２ビットだけを利用する構成であっても良い。同様にパス番号も２ビットである必要は無く、NRPと同様に、他の情報を付加した構成であっても良い。また、それらの全ビットを利用する構成であっても、その一部分を利用する構成であっても良い。
（６）上位層から下位層、また、同一層においては、左から右の順に検索するとしたが、本発明はこれに限定されない。検索の方法は、予め定められたルールに基づいたものであれば如何なるものでも良く、例えば、木構造における左方向、及び深さ優先で検索する構成であっても良い。
（７）実施の形態では、変換情報とメディア鍵とをXOR演算を行うとしたが、本発明はこれに限定されない。逆変換可能な演算であれば如何なる演算であっても良く、例えば四則演算であっても良い。
（８）メディア鍵データにパリティビットを含むフォーマットの場合、メディア鍵と変換情報を演算するのではなく、メディア鍵のパリティビットに変換情報を埋め込む構成であっても良い。
【００９５】
例えば、DES暗号を利用する場合、６４ビット長のメディア鍵データのうち、８ビットがパリティビットであり、鍵データ生成装置１００は、この８ビットに変換情報を埋め込み、変換する。
再生装置２００は、変換情報を生成する必要が無く、DVD３００から暗号化メディア鍵を読み出して復号したメディア鍵データの８ビットのパリティビットをチェックせずに削除し、５６ビットの有効鍵データをメディア鍵として用いる。
【００９６】

また、デバイス鍵で暗号化する度に、異なる乱数をパリティビットに埋め込むことでメディア鍵を変換するとしても良い。この場合も、再生装置２００はパリティビットをチェックせずに削除し、５６ビットの有効鍵データをメディア鍵として用いる。

（９）上記（５）のようにパリティビットを含むフォーマットの場合、パリティビットの一部分に変換情報又は乱数を埋め込み、残りのパリティビットを情報伝送用として利用する構成であっても良い。

【００９７】

例えば、パリティビットが８ビットである場合、７ビットに乱数を埋め込み、残りの１ビットを情報伝送用として利用する。情報伝送用のビットの利用例としては、鍵データを記録する記録媒体に、無効化すべき鍵の識別子を記載したリストが存在するか否かなどを示すフラグとして利用する方法などがある。このとき、情報伝送用ビットは、その記録媒体において固定値となるが、他の７ビットのパリティビットに乱数が埋め込まれるため、変換後のメディア鍵は、デバイス鍵毎に異なる。

（１０）実施の形態では、鍵データ生成装置１００が鍵データを生成し、コンテンツを暗号化し、鍵データ及び暗号化コンテンツを記録媒体に書き込むとしたが、全てを鍵データ生成装置１００が行う必要は無く、鍵データの生成、鍵データの記録及びコンテンツの記録を、それぞれ異なる装置が行うとしても良い。

【００９８】

また、鍵データ生成装置１００は、再生装置のほか、記録装置のデバイス鍵を管理するとしても良い。

この場合、記録装置は、木構造のリーフに割り当てられたデバイス鍵を保持している。鍵データ生成装置１００は、実施の形態と同様の処理を行い、変換情報及びメディア鍵データを生成してDVDに記録する。

【００９９】

記録装置は、コンテンツを暗号化するコンテンツ鍵を暗号化する際、再生装置２００と同様の処理を行い、保持しているデバイス鍵から適切なデバイス鍵を選択してメディア鍵を取得する。取得したメディア鍵を用いてコンテンツ鍵を暗号化し、暗号化コンテンツ鍵及び暗号化コンテンツをDVDに書き込む。

また、記録装置は、鍵データ生成装置１００が記録した鍵データをコンテンツ鍵としてコンテンツを暗号化するとしても良い。

（１１）鍵データの記録はDVDに限定されない。可搬型で鍵データ生成装置１００及び再生装置２００の両方に装着可能な記録媒体であればよく、例えば、CD、MD、MO、BD（Blu－ray Disc）などであっても良い。また、鍵データ生成装置１００からインターネットなどの通信を利用して再生装置へ鍵データ及びコンテンツを送信するとしても良い。

（１２）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。

【０１００】

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。

【０１０１】

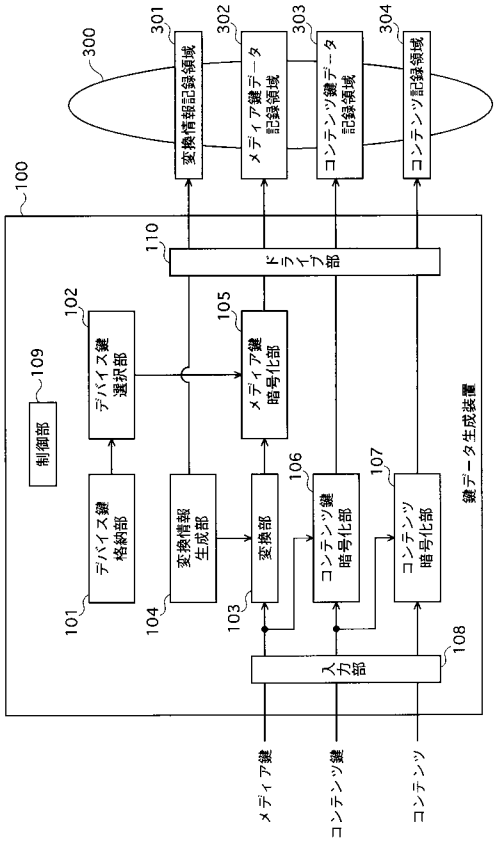
また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

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としてもよい。

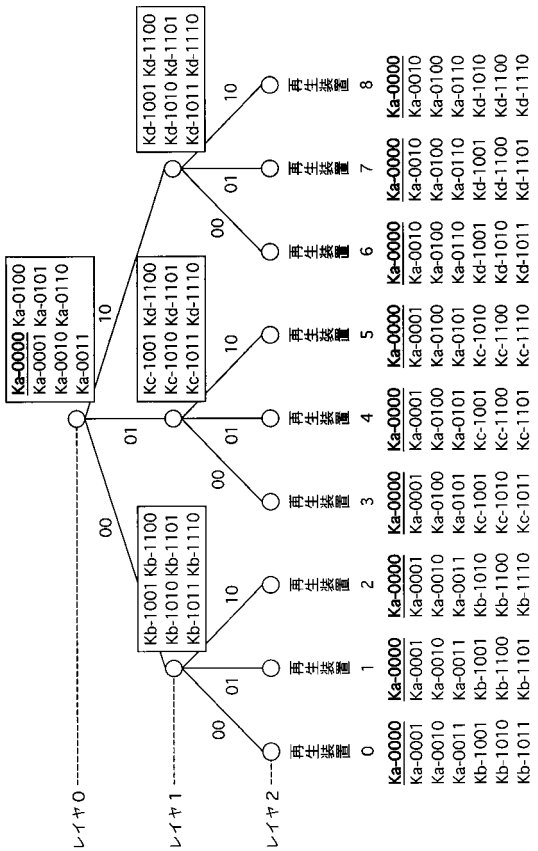
【０１０２】
また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。
（１３）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。
【産業上の利用可能性】
【０１０３】
木構造を利用した鍵管理方式に利用できる。特に、鍵データの不正入手防止に好適である。
【図面の簡単な説明】
【０１０４】
【図１】鍵データ生成装置１００とDVD３００との構成を示すブロック図である。
【図２】鍵データ生成装置１００において、デバイス鍵の対応関係を表す木構造を示す。
【図３】無効化すべきデバイス鍵が発生した場合のデバイス鍵の対応関係を示す。
【図４】メディア鍵の変換及び暗号化の処理内容を示す。
【図５】DVD３００の記録領域の構成を示す。
【図６】DVD３００と再生装置２００の構成を示すブロック図である。
【図７】暗号化メディア鍵の復号及び再変換の処理内容を示す。
【図８】鍵データ生成装置１００における鍵データの生成処理を示すフローチャートである。
【図９】再生装置２００の動作を示すフローチャートである。
【図１０】再生装置２００での、記録位置の特定及び変換情報の生成の動作を示すフローチャートである。
【図１１】木構造を利用した鍵管理方式の一例を示す。
【図１２】木構造を利用した鍵管理方式の一例を示す。
【符号の説明】
【０１０５】
１００　鍵データ生成装置
１０１　デバイス鍵格納部
１０２　デバイス鍵選択部
１０３　変換部
１０４　変換情報生成部
１０５　メディア鍵暗号化部
１０６　コンテンツ鍵暗号化部
１０７　コンテンツ暗号化部
１０８　入力部
１０９　制御部
１１０　ドライブ部
２００　再生装置
２０１　デバイス鍵選択部
２０２　デバイス鍵格納部
２０３　メディア鍵復号部
２０４　変換部
２０５　コンテンツ鍵復号部
２０６　コンテンツ復号部
２０７　ドライブ部
２０８　再生部
２０９　制御部
２１０　入力部
２２０　モニタ

２２１　スピーカ
３００　ＤＶＤ
３０１　変換情報記録領域
３０２　メディア鍵データ記録領域
３０３　コンテンツ鍵データ記録領域
３０４　コンテンツ記録領域

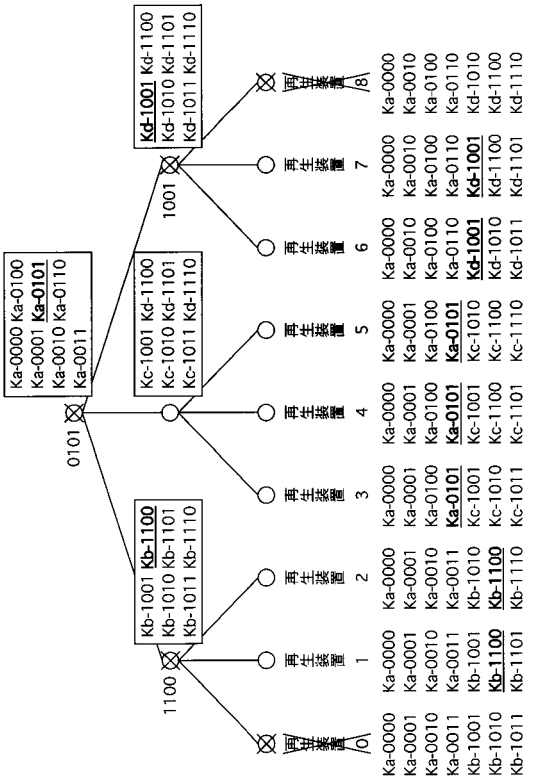
【図１】



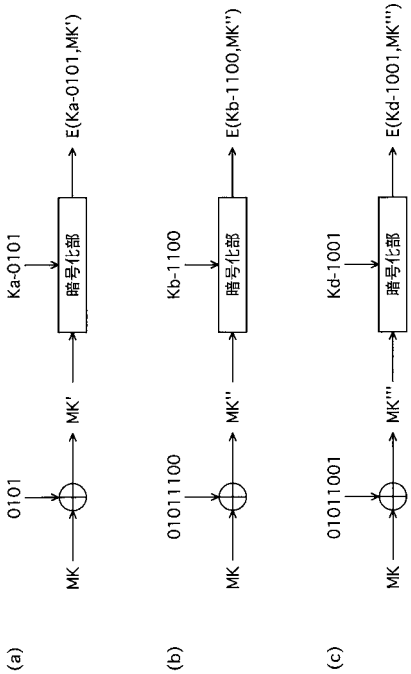
【図２】



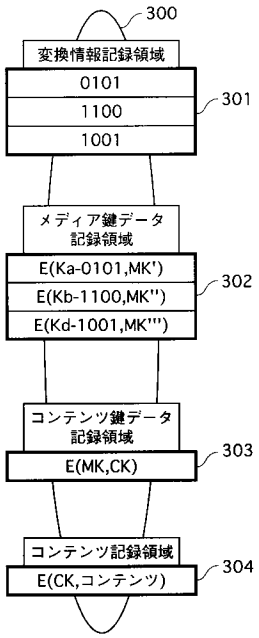
【図３】


Ka-0000 Ka-0100
Ka-0001 Ka-0101
Ka-0010 Ka-0110
Ka-0011
0101
Kb-1001 Kb-1100
Kb-1010 Kb-1101
Kb-1011 Kb-1110
1100
Kc-1001 Kd-1100
Kc-1010 Kd-1101
Kc-1011 Kd-1110
1001
Kd-1001 Kd-1100
Kd-1010 Kd-1101
Kd-1011 Kd-1110
再生装置 0
再生装置 1
再生装置 2
再生装置 3
再生装置 4
再生装置 5
再生装置 6
再生装置 7
再生装置 8
Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000
Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0010 Ka-0010 Ka-0010
Ka-0010 Ka-0010 Ka-0010 Ka-0100 Ka-0100 Ka-0100 Ka-0100 Ka-0100 Ka-0100
Ka-0011 Ka-0011 Ka-0011 Ka-0101 Ka-0101 Ka-0101 Ka-0110 Ka-0110 Ka-0110
Kb-1001 Kb-1001 Kb-1010 Kc-1001 Kc-1001 Kc-1010 Kc-1010 Kd-1001 Kd-1010
Kb-1010 Kb-1100 Kb-1100 Kc-1010 Kc-1100 Kc-1100 Kd-1010 Kd-1100 Kd-1100
Kb-1011 Kb-1101 Kb-1110 Kc-1011 Kc-1101 Kc-1110 Kd-1011 Kd-1101 Kd-1110

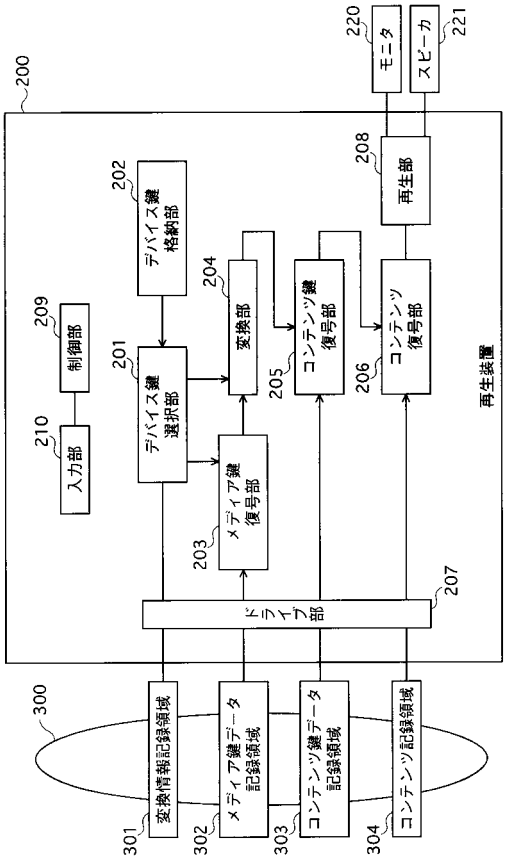
【図４】


Ka-0101
暗号化部
E(Ka-0101,MK')
0101
MK
MK'
(a)
Kb-1100
暗号化部
E(Kb-1100,MK'')
01011100
MK
MK''
(b)
Kd-1001
暗号化部
E(Kd-1001,MK''')
01011001
MK
MK'''
(c)

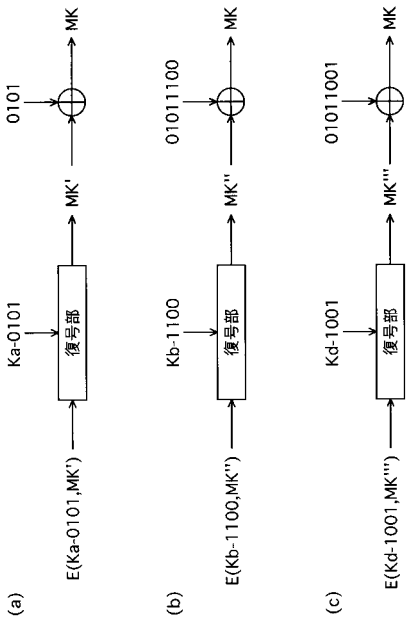
【図５】


300
変換情報記録領域
0101
1100
1001
301
メディア鍵データ
記録領域
E(Ka-0101,MK')
E(Kb-1100,MK'')
E(Kd-1001,MK''')
302
コンテンツ鍵データ
記録領域
E(MK,CK)
303
コンテンツ記録領域
E(CK,コンテンツ)
304

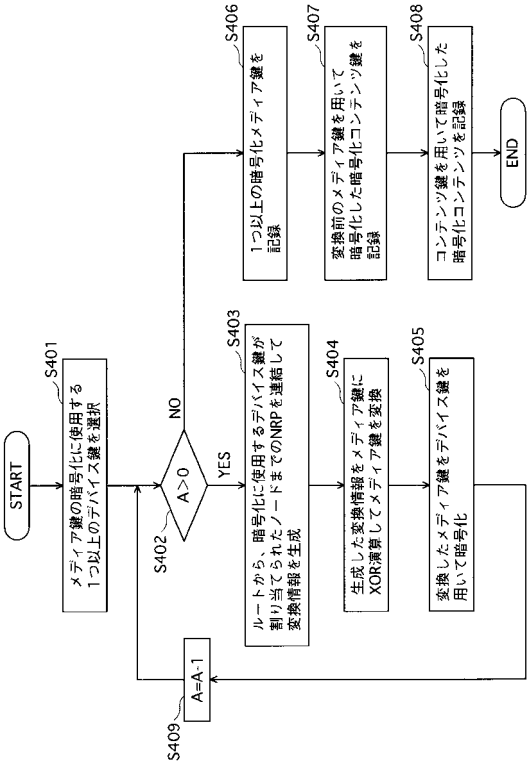
【図６】


200
220
モニタ
221
スピーカ
208
再生部
202
デバイス鍵
格納部
204
変換部
209
制御部
201
デバイス鍵
選択部
205
コンテンツ鍵
復号部
206
コンテンツ
復号部
210
入力部
203
メディア鍵
復号部
207
ドライブ部
再生装置
300
変換情報記録領域
メディア鍵データ
記録領域
コンテンツ鍵データ
記録領域
コンテンツ記録領域
301
302
303
304

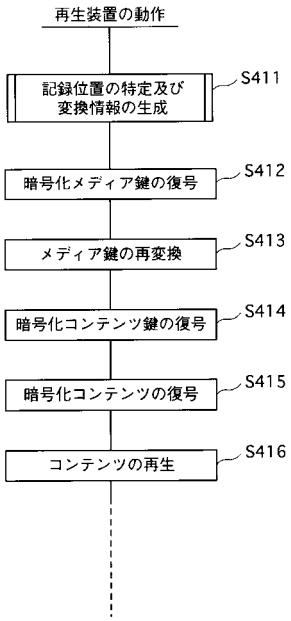
【図７】


0101
MK
MK'
Ka-0101
復号部
E(Ka-0101,MK')
(a)
01011100
MK
MK''
Kb-1100
復号部
E(Kb-1100,MK'')
(b)
01011001
MK
MK'''
Kd-1001
復号部
E(Kd-1001,MK''')
(c)

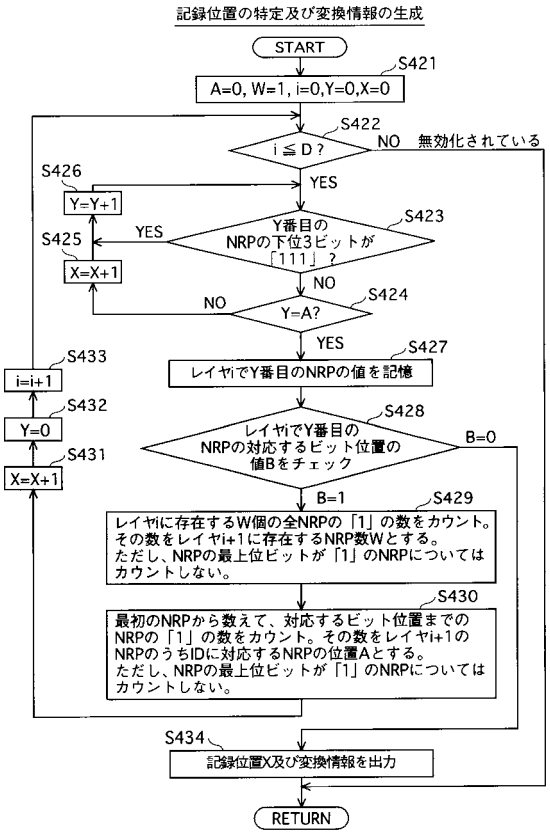
【図８】


START
S401
メディア鍵の暗号化に使用する1つ以上のデバイス鍵を選択
S402
A>0
NO
YES
S403
ルートから、暗号化に使用するデバイス鍵が割り当てられたノードまでのNRPを連結して変換情報を生成
S404
生成した変換情報をメディア鍵にXOR演算してメディア鍵を変換
S405
変換したメディア鍵をデバイス鍵を用いて暗号化
S406
1つ以上の暗号化メディア鍵を記録
S407
変換前のメディア鍵を用いて暗号化した暗号化コンテンツ鍵を記録
S408
コンテンツ鍵を用いて暗号化した暗号化コンテンツを記録
END
S409
A=A-1

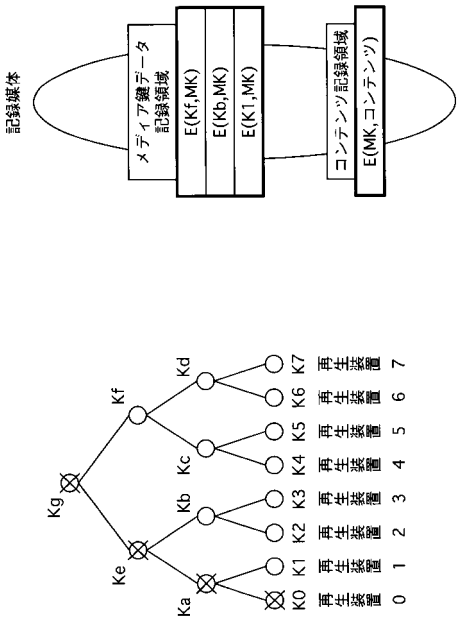
【図９】


再生装置の動作
記録位置の特定及び変換情報の生成
S411
暗号化メディア鍵の復号
S412
メディア鍵の再変換
S413
暗号化コンテンツ鍵の復号
S414
暗号化コンテンツの復号
S415
コンテンツの再生
S416

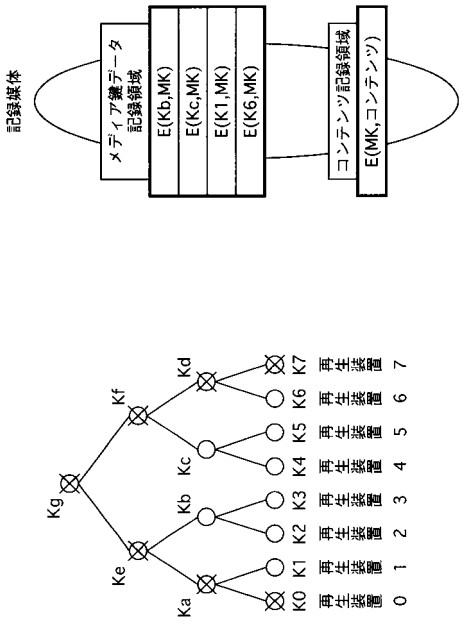
【図１０】


記録位置の特定及び変換情報の生成
START
S421
A=0, W=1, i=0,Y=0,X=0
S422
i≦D?
NO 無効化されている
YES
S426
Y=Y+1
S423
Y番目のNRPの下位3ビットが「111」?
YES
S425
X=X+1
NO
NO
S424
Y=A?
YES
S427
レイヤiでY番目のNRPの値を記憶
S428
レイヤiでY番目のNRPの対応するビット位置の値Bをチェック
B=0
B=1
S429
レイヤiに存在するW個の全NRPの「1」の数をカウント。その数をレイヤi+1に存在するNRP数Wとする。ただし、NRPの最上位ビットが「1」のNRPについてはカウントしない。
S430
最初のNRPから数えて、対応するビット位置までのNRPの「1」の数をカウント。その数をレイヤi+1のNRPのうちIDに対応するNRPの位置Aとする。ただし、NRPの最上位ビットが「1」のNRPについてはカウントしない。
S433
i=i+1
S432
Y=0
S431
X=X+1
S434
記録位置X及び変換情報を出力
RETURN

【図１１】


記録媒体
メディア鍵データ記録領域
E(Kf,MK)
E(Kb,MK)
E(K1,MK)
コンテンツ記録領域
E(MK,コンテンツ)
Kg
Kf
Ke
Kd
Kc
Kb
Ka
K0 K1 K2 K3 K4 K5 K6 K7
再生装置 0 1 2 3 4 5 6 7

【図１２】


記録媒体
メディア鍵データ記録領域
E(Kb,MK)
E(Kc,MK)
E(K1,MK)
E(K6,MK)
コンテンツ記録領域
E(MK,コンテンツ)
Kg
Kf
Ke
Kd
Kc
Kb
Ka
K0 K1 K2 K3 K4 K5 K6 K7
再生装置 0 1 2 3 4 5 6 7

フロントページの続き

(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　山本　直紀
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　石原　秀志
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２００２－２８１０１３（ＪＰ，Ａ）
特表２００４－５１５１８０（ＪＰ，Ａ）
国際公開第０２／０７８４１９（WO，Ａ１）
特開平０７－０２８４０７（ＪＰ，Ａ）
国際公開第０２／０４４８７５（WO，Ａ１）
特開２００３－０２６８９１（ＪＰ，Ａ）
D.W. Davies and W.L. Price，ネットワーク・セキュリティ，日経マグロウヒル社，１９８５年１２月　5日，p.85-92

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
ＪＭＥＤＰｌｕｓ（ＪＤｒｅａｍＩＩ）