

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4220213号  
(P4220213)

(45) 発行日 平成21年2月4日(2009.2.4)

(24) 登録日 平成20年11月21日(2008.11.21)

(51) Int.Cl.

F I

H04L 9/08 (2006.01)

H04L 9/00 601B

H04L 9/00 601A

請求項の数 23 (全 70 頁)

(21) 出願番号 特願2002-303509 (P2002-303509)  
 (22) 出願日 平成14年10月17日(2002.10.17)  
 (65) 公開番号 特開2003-204320 (P2003-204320A)  
 (43) 公開日 平成15年7月18日(2003.7.18)  
 審査請求日 平成17年8月17日(2005.8.17)  
 (31) 優先権主張番号 特願2001-329863 (P2001-329863)  
 (32) 優先日 平成13年10月26日(2001.10.26)  
 (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 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  
 (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

最終頁に続く

(54) 【発明の名称】 著作物保護システム、鍵管理装置及び利用者装置

(57) 【特許請求の範囲】

【請求項1】

n分木(nは、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置と、1以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、

前記鍵管理装置は、

n分木においてルートから一部のリーフへの経路上に存在する複数のノードは無効化されており、n分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス

10

鍵を記憶しているデバイス鍵記憶手段と、  
 複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、

リーフを除き、無効化されたノードについて、下位のn個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、

20

前記利用者装置は、

前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と

10

を備えることを特徴とする著作物保護システム。

【請求項 2】

n 分木 (n は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、

n 分木においてルートから一部のリーフへの経路上に存在する複数のノードは無効化されており、n 分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、

複数の共通デバイス鍵をそれぞれ用いて 1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、

20

リーフを除き、無効化されたノードについて、下位の n 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段と

を備えることを特徴とする鍵管理装置。

【請求項 3】

前記 n 分木は、複数のレイヤから構成され、

前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、

30

前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む

ことを特徴とする請求項 2 に記載の鍵管理装置。

【請求項 4】

前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、

前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む

40

ことを特徴とする請求項 2 に記載の鍵管理装置。

【請求項 5】

前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成する

ことを特徴とする請求項 2 に記載の鍵管理装置。

【請求項 6】

前記無効化情報生成手段は、

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特

50

別無効化情報を生成し、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し

、  
リーフを除く他の無効化されたノードについて、下位の  $n$  個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成する

ことを特徴とする請求項 2 に記載の鍵管理装置。

【請求項 7】

前記無効化情報生成手段は、

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第 1 付加情報と、下位の  $n$  個のノードのそれぞれが無効化されていることを示す  $n$  桁の情報とから構成される特別無効化情報を生成し、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し

、  
リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第 2 付加情報と、下位の  $n$  個のノードのそれぞれが無効化されているか否かを示す  $n$  桁の情報とから構成される無効化情報を生成する

ことを特徴とする請求項 6 に記載の鍵管理装置。

【請求項 8】

前記無効化情報生成手段は、

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位の  $n$  個のノードのそれぞれが無効化されていることを示す  $n$  桁の特別値から構成される特別無効化情報を生成し、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し

、  
リーフを除く他の無効化されたノードについて、下位の  $n$  個のノードのそれぞれが無効化されているか否かを示す  $n$  桁の無効化情報を生成する

ことを特徴とする請求項 6 に記載の鍵管理装置。

【請求項 9】

$n$  分木 ( $n$  は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、

$n$  分木において一部のノードは、無効化されており、 $n$  分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、

複数の共通デバイス鍵をそれぞれ用いて 1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$  分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、

リーフを除き、無効化された各ノードについて、

下位の  $n$  個のノードの少なくとも 1 個が無効化されている場合に、それぞれが無効化されているか否かを示す第 1 無効化情報を生成し、

下位の  $n$  個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第 2 無効化情報を生成し、

その結果、1 個以上の第 1 無効化情報、1 個以上の第 2 無効化情報、又は 1 個以上の第 1 無効化情報及び 1 個以上の第 2 無効化情報が得られ、

得られた 1 個以上の第 1 無効化情報、1 個以上の第 2 無効化情報、又は 1 個以上の第 1 無効化情報及び 1 個以上の第 2 無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段と

を備えることを特徴とする鍵管理装置。

【請求項 10】

n 分木 (n は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有する鍵管理装置により、1 個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の 1 個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、

前記鍵管理装置は、n 分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて 1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位の n 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

10

前記利用者装置は、

前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、

20

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と

を備えることを特徴とする利用者装置。

#### 【請求項 11】

前記 n 分木は、複数のレイヤから構成され、

前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、

前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、

30

前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する

ことを特徴とする請求項 10 に記載の利用者装置。

#### 【請求項 12】

前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、

前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、

前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する

40

ことを特徴とする請求項 10 に記載の利用者装置。

#### 【請求項 13】

リーフを除き、無効化された全てのノードについて、無効化情報が生成されて前記記録媒体に書き込まれ、

前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定する

ことを特徴とする請求項 10 に記載の利用者装置。

#### 【請求項 14】

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化

50

されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、

リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、

前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する

ことを特徴とする請求項10に記載の利用者装置。

【請求項15】

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第1付加情報と、下位の $n$ 個のノードのそれぞれが無効化されていることを示す $n$ 桁の情報とから構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、

リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第2付加情報と、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す $n$ 桁の情報とから構成される無効化情報が生成されて前記記録媒体に書き込まれ、

前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する

ことを特徴とする請求項14に記載の利用者装置。

【請求項16】

リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位の $n$ 個のノードのそれぞれが無効化されていることを示す $n$ 桁の特別値から構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、

前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、

リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す $n$ 桁の無効化情報が生成されて前記記録媒体に書き込まれ、

前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する

ことを特徴とする請求項14に記載の利用者装置。

【請求項17】

$n$ 分木( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置により、1個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の1個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、

前記鍵管理装置は、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しており、一部のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化された各ノードについて、下位の $n$ 個のノードの少なくとも1個が無効化されている場合に、それぞれが無効化されているか否かを示す第1無効化情報を生成し、下位の $n$ 個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第2無効化情報を生成し、その結果、1個以上の第1無効化情報、1個以上の第2無効化情報、又は1個以上の第1無効

10

20

30

40

50

化情報及び1個以上の第2無効化情報が得られ、得られた1個以上の第1無効化情報、1個以上の第2無効化情報、又は1個以上の第1無効化情報及び1個以上の第2無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

前記利用者装置は、

前記記録媒体に前記配列順序に従って書き込まれた前記第1無効化情報、前記第2無効化情報、又は前記第1無効化情報及び前記第2無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、

特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、

10

生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段と

を備えることを特徴とする利用者装置。

【請求項18】

n分木(nは、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理プログラムであって、

前記鍵管理装置は、n分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、n分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段、鍵情報生成手段及び無効化情報生成手段を備えるコンピュータであり、

20

鍵情報生成手段により、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、

無効化情報生成手段により、リーフを除き、無効化されたノードについて、下位のn個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと

30

をコンピュータに実行させるための鍵管理プログラム。

【請求項19】

n分木(nは、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置により、1以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の1個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者プログラムであって、

前記鍵管理装置は、n分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位のn個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

40

前記利用者装置は、特定手段、復号手段及び暗号復号手段を備えるコンピュータであり

50

特定手段により、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、

復号手段により、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、

暗号復号手段により、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと

10

をコンピュータに実行させるための利用者プログラム。

【請求項 2 0】

n 分木 (n は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理方法であって、前記鍵管理装置は、n 分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、n 分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しているデバイス鍵記憶手段、鍵情報生成手段及び無効化情報生成手段を備え、

前記鍵管理方法は、

鍵情報生成手段により、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵をそれぞれ用いて、1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を n 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと

20

無効化情報生成手段により、リーフを除き、無効化されたノードについて、下位の n 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと

を含むことを特徴とする鍵管理方法。

【請求項 2 1】

30

n 分木 (n は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有する鍵管理装置により、1 以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の 1 個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用方法であって、

前記鍵管理装置は、n 分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて 1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位の n 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

40

前記利用者装置は、特定手段、復号手段及び暗号復号手段を備え、

前記利用方法は、

特定手段により、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化

50

メディア鍵を特定する特定ステップと、

復号手段により、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、

暗号復号手段により、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと

を含むことを特徴とする利用方法。

【請求項 2 2】

n 分木 (n は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有する鍵管理装置で用いられる鍵管理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、

前記鍵管理装置は、n 分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、前記デバイス鍵を各利用者装置に割り当て、n 分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しているデバイス鍵記憶手段、鍵情報生成手段及び無効化情報生成手段を備えるコンピュータであり、

鍵情報生成手段により、複数の共通デバイス鍵をそれぞれ用いて 1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成ステップと、

無効化情報生成手段により、リーフを除き、無効化されたノードについて、下位の n 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成ステップと

を前記コンピュータに実行させるための前記鍵管理プログラムを記録していることを特徴とする記録媒体。

【請求項 2 3】

n 分木 (n は、2 以上の整数) に関連付けて 1 個以上のデバイス鍵を有する鍵管理装置により、1 以上のデバイス鍵が割り当てられ、割り当てられた複数のデバイス鍵の中の 1 個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置で用いられる利用者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、

前記鍵管理装置は、n 分木を構成する 1 個以上のノードにそれぞれ対応付けて 1 個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて 1 個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1 以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、n 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位の n 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、

前記利用者装置は、特定手段、復号手段及び暗号復号手段を備えるコンピュータであり

特定手段により、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定ステップと、

10

20

30

40

50



復号手段により、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号ステップと、

暗号復号手段により、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号ステップと

を前記コンピュータに実行させるための前記利用者プログラムを記録していることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

10

【発明の属する技術分野】

本発明は、デジタル著作物を記録媒体に記録し、記録媒体を配布し、配布された記録媒体からデジタル著作物を再生する技術に関し、特に、著作権を保護するためのコンテンツ暗号化のための鍵情報を管理する技術に関する。

【0002】

【従来の技術】

近年、デジタル処理、蓄積、通信等の技術の発展に伴い、映画などのデジタルコンテンツを格納している大容量記録媒体を販売又はレンタルによりユーザに提供するサービスが普及している。また、デジタル化されたコンテンツが放送され、受信装置がデジタルコンテンツを受信し、受信したデジタルコンテンツを記録型デジタル光ディスク等の記録媒体に格納し、再生装置が記録媒体に格納されたデジタルコンテンツを再生するというシステムも普及しつつある。

20

【0003】

こうしたサービスやシステムが提供される際には、コンテンツが不正に使用されないように、コンテンツの著作権が保護され、著作権者との合意による制限の下でのみコンテンツの再生や複製などが行われる必要がある。

一般的には、次に示すようにして、著作物を著作権者の許可のない不正コピー等から保護する。記録装置がデジタルコンテンツをある暗号化鍵により暗号化し、暗号化コンテンツをディスクに記録する。前記暗号化鍵に対応する復号鍵を持つ再生装置だけが暗号化コンテンツを復号できる。記録装置や再生装置などの製造業者と著作権者との間で著作権保護に対する規定が取り決められ、その規定の遵守を条件として、製造業者は、暗号化鍵又は復号鍵（以降、これらを単に、鍵と称する。）を入手できる。製造業者は、入手した鍵が外部に露見しないように厳重に管理しなければならない。

30

【0004】

しかし、製造業者が鍵を厳重に管理したとしても、不正な第三者（以下、不正者）が、何らかの手段により鍵を取得することがあるかもしれない。こうして鍵が一旦不正者により暴露されてしまうと、この不正者は、製造業者と著作権者との合意による規定を逃れて、鍵自体を流布したり、コンテンツを不正に扱う記録装置又は再生装置を製造したり、又はコンテンツを不正に扱うコンピュータプログラムを作成しインターネット等を介して流布することが考えられる。このような場合、著作権者は、一旦暴露された鍵では、次から提供

40

【0005】

著作権者のこのような要求に答えるための最も単純な方法を次に示す。

鍵管理機関は、複数のデバイス鍵及び複数のメディア鍵からなる集合を有している。鍵管理機関は、複数の記録装置及び複数の再生装置のそれぞれに、1個のデバイス鍵及びそのデバイス鍵の鍵識別番号を割り当て、割り当てたデバイス鍵及び鍵識別番号を記録装置又は再生装置に与える。また、記録媒体に、1個のメディア鍵を割り当てる。次に、鍵管理機関は、前記記録装置及び前記再生装置のそれぞれに割り当てられた各デバイス鍵を用いてメディア鍵を暗号化して暗号化メディア鍵を作成し、全てのデバイス鍵に対する暗号化メディア鍵と鍵識別番号からなるリストを鍵情報として記録媒体に格納する。記録媒体が

50

装着された記録装置又は再生装置は、自らに割り当てられた鍵識別番号に対応する暗号化メディア鍵を、前記記録媒体の鍵情報から取り出し、自らに割り当てられたデバイス鍵を用いて、取り出した暗号化メディア鍵を復号してメディア鍵を獲得する。次に、記録装置は、獲得したメディア鍵を用いてコンテンツを暗号化して記録媒体に記録する。一方、再生装置は、同様にして獲得したメディア鍵を用いて暗号化コンテンツを復号する。このようにして、正規にデバイス鍵が割り当てられた記録装置又は再生装置であれば、1個の記録媒体からは必ず同じメディア鍵が獲得できるので、機器間の互換性が保たれる。

#### 【0006】

ここで、ある記録装置又は再生装置のデバイス鍵が暴露されたと想定する。デバイス鍵が暴露された後、鍵管理機関が鍵情報を新たな記録媒体に格納するときに、鍵管理機関は、暴露されたデバイス鍵を除いて鍵情報を作成し、記録媒体に格納する。このようにすると、暴露されたデバイス鍵を知っている不正な装置は、記録媒体に格納されている鍵情報に、暴露されたデバイス鍵を用いて暗号化された暗号化メディア鍵が含まれていないので、鍵情報から正しいメディア鍵を獲得することができない。この結果、不正な装置は、コンテンツの不正な使用をすることができない。例えば、その不正な装置が記録装置であれば、その記録装置で記録した暗号化コンテンツは、正しいメディア鍵を用いて暗号化されていないので、他の正規の再生装置では復号することができない。また、その不正な装置が再生装置であれば、正しいメディア鍵を獲得することができないので、他の正規の記録装置で記録された暗号化コンテンツを正しく復号することができない。このようにして、暴露された鍵を無効化することができる。

#### 【0007】

しかし、この単純な方法では、装置の台数が大量になると鍵情報のデータサイズが非現実的な大きな値になるという欠点がある。例えば、あるデジタル機器が世界的に普及し、全世界で10億台の機器が存在するものとする。また、上述した暗号化コンテンツの生成に用いる暗号アルゴリズムとして、米国の標準暗号であるトリプルDES暗号を用いるものとする、メディア鍵の長さは、パディングも含めて、16[B(バイト)]となる。従って暗号化メディア鍵の長さも16[B]となる。さらに鍵識別番号として4[B]の値を持つとすると、全体の鍵情報サイズは20[B]×10億台=200億[B]=20[GB]となる。これは現在の記録型光ディスクの容量からすると非現実的な大きな値である。

#### 【0008】

そこで、このようなシステムは、記録媒体に記録する鍵情報サイズが記録媒体の記録容量に比べわずかである、という条件を満たすものでなければならない。

このような条件を満たすシステムの一例として、文献(1)「デジタルコンテンツ保護用鍵管理方式」(中野、大森、館林、2001年暗号と情報セキュリティシンポジウム、SCIS2001 5A-5、Jan. 2001)には、木構造を用いた著作権保護用鍵管理方式が開示されている。

#### 【0009】

##### 【特許文献1】

「デジタルコンテンツ保護用鍵管理方式」(中野、大森、館林、2001年暗号と情報セキュリティシンポジウム、SCIS2001 5A-5、Jan. 2001)

ここで、文献(1)において開示されている方式について説明する前に、木構造について若干の解説を行う。

形式的に、木構造は、1個以上のノードを要素とする有限集合Tであって、次の条件を満たすものとして定義される。

#### 【0010】

(a) 木構造のルートと呼ばれるノードが、1個だけ指定されている。

(b) ルートを除く他のノードは、m個(m>0)の共通部分を持たない集合T<sub>1</sub>、・・・、T<sub>m</sub>に分割され、各T<sub>i</sub>(i=1、・・・、m)は再び木構造であり、これらは、Tよりも高さが「1」だけ小さい部分木である。この木構造T<sub>1</sub>、・・・、T<sub>m</sub>を、そのルートに対する部分木という。

## 【0011】

また、木構造Tにおける水準 (= レイヤ) とは、次のように定義された数である。Tのルートの水準は0である。このルートに対する部分木をT<sub>j</sub> とする場合、T<sub>j</sub> に含まれるノードのTにおける水準は、T<sub>j</sub> における水準より1だけ大きい。

以下では、文献(1)により開示されている木構造を用いた著作権保護用鍵管理方式について説明する。

## 【0012】

前記著作権保護用鍵管理方式において、鍵管理機関は、一例として、レイヤ数4の2分木である木構造を構築し、構築した木構造に含まれるノードと同じ数のデバイス鍵を生成し、生成したデバイス鍵を構築した前記木構造の各ノードに割り当てる。鍵管理機関は、木構造の各リーフに各プレーヤ(以降、上述の再生装置と同義で使用)を対応させ、リーフからルートに至るまでの経路上に割り当てられた複数のデバイス鍵を1個のデバイス鍵セットとして、各リーフに1対1で対応するプレーヤに対して、配布する。こうして各プレーヤに配布されたデバイス鍵セットは、プレーヤごとに全て異なる。

## 【0013】

ここで、1個のプレーヤに割り当てられたデバイス鍵セットが暴露された場合において、鍵管理機関は、木構造において、暴露されたデバイス鍵セットに含まれるデバイス鍵が割り当てられているノードを削除する。次に、デバイス鍵が暴露されていないプレーヤの中で、最も多くのプレーヤが共有しているデバイス鍵を、次に使うべきデバイス鍵とする。

## 【0014】

この方式によれば、10億台の装置のうち、任意の1万台を無効化するためには、概ね3[MB]程度の鍵情報サイズでよいことが文献(1)に示されている。

また、文献(2)「Manipulation of Trees in Information Retrieval」(G. Salton、Communication of the ACM 5、1962)及び文献(3)「基本算法/情報構造」(米田、寛記、サイエンス社、昭53)は、木構造を1次元で表現する表現方法を開示している。木構造の各ノードをある規則に従って並べることで、木構造は1次元で表現される。例えば、文献(3)のp. 136には、水準順の並べ方が示されている。これによると、水準については小さい方から大きい方へ順に並べ、それぞれの水準については、その水準内の各ノードを左から右への順に従って並べる。このような特定の規則に基づく並べ方を利用することにより、プレーヤ側で、1次元に並べた情報から木構造を構築することができる。

## 【0015】

## 【特許文献2】

「Manipulation of Trees in Information Retrieval」(G. Salton、Communication of the ACM 5、1962)

## 【0016】

## 【特許文献3】

「基本算法/情報構造」(米田、寛記、サイエンス社、昭53)

## 【0017】

## 【発明が解決しようとする課題】

上述の著作権保護用鍵管理方式では、記録媒体に記録する鍵情報サイズが記録媒体の記録容量に比べわずかであるという条件を満たすものの、木構造により構築された鍵において、無効化されたものを含む場合に、プレーヤにおいて自らに割り当てられた鍵を効率良く決定することが要求されている。

そこで本発明は、前記の要求に対処するために、利用者が有する利用者装置において、割り当てられた鍵を効率良く決定することができる著作物保護システム、鍵管理装置、利用者装置、鍵管理方法、鍵管理プログラム及び鍵管理プログラムを記録している記録媒体を提供することを目的とする。

## 【0018】

## 【課題を解決するための手段】

上記目的を達成するために、本発明は、n分木(nは、2以上の整数)に関連付けて1個

10

20

30

40

50

以上のデバイス鍵を有する鍵管理装置と、1以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、前記鍵管理装置は、 $n$ 分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

10

20

**【0019】**

また、本発明は、 $n$ 分木( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、 $n$ 分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする。

30

**【0020】**

ここで、前記 $n$ 分木は、複数のレイヤから構成され、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むように構成してもよい。

40

**【0021】**

ここで、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込むように構成してもよい。

**【0022】**

50

ここで、前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成するように構成してもよい。

ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成するように構成してもよい。

【0023】

ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第1付加情報と、下位の $n$ 個のノードのそれぞれが無効化されていることを示す $n$ 桁の情報とから構成される特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第2付加情報と、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す $n$ 桁の情報とから構成される無効化情報を生成するように構成してもよい。

【0024】

ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位の $n$ 個のノードのそれぞれが無効化されていることを示す $n$ 桁の特別値から構成される特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す $n$ 桁の無効化情報を生成するように構成してもよい。

【0025】

また、本発明は、 $n$ 分木( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、 $n$ 分木において一部のノードは、無効化されており、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化された各ノードについて、下位の $n$ 個のノードの少なくとも1個が無効化されている場合に、それぞれが無効化されているか否かを示す第1無効化情報を生成し、下位の $n$ 個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第2無効化情報を生成し、その結果、1個以上の第1無効化情報、1個以上の第2無効化情報、又は1個以上の第1無効化情報及び1個以上の第2無効化情報が得られ、得られた1個以上の第1無効化情報、1個以上の第2無効化情報、又は1個以上の第1無効化情報及び1個以上の第2無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備えることを特徴とする。

【0026】

また、本発明は、 $n$ 分木( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、 $n$ 分木を構成する全てのノードは、有効であり、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、各利用者装置に共通に割り当てられた1個のデバイス鍵に基づいて、1個のメディア鍵を暗号化して1個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込む鍵情報生成手段と、 $n$ 分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込

10

20

30

40

50

む無効化情報生成手段とを備えることを特徴とする。

【0027】

また、本発明は、 $n$ 分木 ( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置により、1個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の1個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

【0028】

ここで、前記 $n$ 分木は、複数のレイヤから構成され、前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定するように構成してもよい。

【0029】

ここで、前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定するように構成してもよい。

【0030】

ここで、リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

ここで、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

## 【0031】

ここで、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す第1付加情報と、下位の $n$ 個のノードのそれぞれが無効化されていることを示す $n$ 桁の情報とから構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位側に接続する全てのノードが無効化されていない旨を示す第2付加情報と、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す $n$ 桁の情報とから構成される無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

10

## 【0032】

ここで、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位の $n$ 個のノードのそれぞれが無効化されていることを示す $n$ 桁の特別値から構成される特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す $n$ 桁の無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定するように構成してもよい。

20

## 【0033】

また、本発明は、 $n$ 分木（ $n$ は、2以上の整数）に関連付けて1個以上のデバイス鍵を有する鍵管理装置により、1個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の1個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しており、一部のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化された各ノードについて、下位の $n$ 個のノードの少なくとも1個が無効化されている場合に、それぞれが無効化されているか否かを示す第1無効化情報を生成し、下位の $n$ 個のノードのいずれも無効化されていない場合に、いずれのノードも無効化されていないことを示す第2無効化情報を生成し、その結果、1個以上の第1無効化情報、1個以上の第2無効化情報、又は1個以上の第1無効化情報及び1個以上の第2無効化情報が得られ、得られた1個以上の第1無効化情報、1個以上の第2無効化情報、又は1個以上の第1無効化情報及び1個以上の第2無効化情報を、前記配列順序に従って前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記第1無効化情報、前記第2無効化情報、又は前記第1無効化情報及び前記第2無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

30

40

## 【0034】

また、本発明は、 $n$ 分木（ $n$ は、2以上の整数）に関連付けて1個以上のデバイス鍵を有

50

する鍵管理装置により、１個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の１個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、 $n$ 分木を構成する１個以上のノードにそれぞれ対応付けて１個以上のデバイス鍵を記憶しており、 $n$ 分木を構成する全てのノードは、有効であり、各利用者装置に共通に割り当てられた１個のデバイス鍵に基づいて、１個のメディア鍵を暗号化して１個の暗号化メディア鍵を生成し、生成した前記暗号化メディア鍵を、記録媒体に書き込み、 $n$ 分木を構成する全てのノードが有効であることを示す情報を前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に有効であることを示す前記情報が記録されていると判断する場合に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出す読出手段と、読み出した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備えることを特徴とする。

10

#### 【００３５】

##### 【発明の実施の形態】

##### 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著作物保護システム１０について説明する。

20

##### １．１ 著作物保護システム１０の構成

著作物保護システム１０は、図１に示すように、鍵管理装置１００、鍵情報記録装置２００、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・から構成されている。

#### 【００３６】

鍵管理装置１００は、鍵情報記録装置２００により、ＤＶＤ－ＲＡＭ等のレコーダブルメディアであって、今だ何らの情報も記録されていない記録媒体５００ａに鍵情報を記録して、鍵情報が記録された記録媒体５００ｂを予め生成しておく。また、鍵管理装置１００は、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・のそれぞれに対して鍵情報を復号するためのデバイス鍵を割り当て、割り当てられたデバイス鍵と、デバイス鍵を識別するデバイス鍵識別情報と、記録装置３００

30

０ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・を識別するＩＤ情報とを、記録装置３００ａ、３００ｂ、３００ｃ、・・・及び再生装置４００ａ、４００ｂ、４００ｃ、・・・のそれぞれに予め配布しておく。

#### 【００３７】

記録装置３００ａは、それぞれ、デジタル化されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成した暗号化コンテンツを記録媒体５００ｂに記録して、記録媒体５００ｃを生成する。再生装置４００ａは、記録媒体５００ｃから暗号化コンテンツを取り出し、取り出した暗号化コンテンツを復号して、元のコンテンツを得る。記録装置３００

40

ｂ、３００ｃ、・・・は、記録装置３００ａと同様に動作し、再生装置４００ｂ、４００

ｃ、・・・は、再生装置４００ａと同様に動作する。

#### 【００３８】

なお、以下において、記録装置３００ｂ、３００ｃ、・・・及び再生装置４００ｂ、４００

#### 【００３９】

ｃ、・・・をユーザ装置と呼ぶことがある。

50

１．１．１ 鍵管理装置１００  
鍵管理装置１００は、図２に示すように、木構造構築部１０１、木構造格納部１０２、デバイス鍵割当部１０３、無効化装置指定部１０４、木構造更新部１０５、鍵情報ヘッダ生成部１０６及び鍵情報生成部１０７から構成されている。



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、鍵管理装置100は、その機能を達成する。

#### 【0040】

##### (1) 木構造格納部102

木構造格納部102は、具体的にはハードディスクユニットから構成されており、図3に一例として示すように、木構造テーブルD100を有している。

木構造テーブルD100は、図4に一例として示す木構造T100に対応しており、木構造T100を表現するためのデータ構造を示す。後述するように、木構造構築部101により木構造T100を表現するためのデータ構造が、木構造テーブルD100として生成され、木構造格納部102に書き込まれる。

10

#### 【0041】

##### (木構造T100)

木構造T100は、図4に示すように、レイヤ0からレイヤ4までの5階層からなる2分木である。木構造T100は、2分木であるので、木構造T100が有する各ノード(リーフを除く)は、2本の経路を介して下位側の2個のノードにそれぞれ接続されている。レイヤ0にはルートである1個のノードが含まれ、レイヤ1には2個のノードが含まれ、レイヤ2には4個のノードが含まれ、レイヤ3には8個のノードが含まれ、レイヤ4にはリーフである16個のノードが含まれている。なお、木構造において下位側とはリーフ側を示し、上位側とはルート側を示している。

20

#### 【0042】

木構造T100が有する各ノード(リーフを除く)と、下位側のノードとを接続する2本の経路のうち、一方である左の経路には、「0」の番号が割り当てられており、他方である右の経路には「1」の番号が割り当てられている。ここで、図4の紙面において、各ノードを中心として当該ノードから左側下方に接続されている経路を左の経路と称し、当該ノードから右側下方に接続されている経路を右の経路と称している。

#### 【0043】

各ノードには、ノード名が付されている。ルートであるノードのノード名は、「ルート」である。また、レイヤ1を含め、レイヤ1より下位にあるレイヤに属するノードに対しては、レイヤ数が示す値と同じ文字数からなる文字列がノード名として付されている。この文字列は、ルートから当該ノードに至るまでの経路に割り当てられた番号を、上位から順に並べて生成されたものである。例えば、レイヤ1に属する2個のノードのノード名は、それぞれ「0」及び「1」である。また、レイヤ2に属する4個のノードのノード名は、それぞれ「00」、「01」、「10」及び「11」である。また、レイヤ3に属する8個のノードのノード名は、それぞれ「000」、「001」、「010」、「011」、・・・、「101」、「110」及び「111」である。また、レイヤ4に属する16個のノードのノード名は、それぞれ「0000」、「0001」、「0010」、「0011」、・・・、「1100」、「1101」、「1110」及び「1111」である。

30

#### 【0044】

##### (木構造テーブルD100)

木構造テーブルD100は、木構造T100に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造T100を構成する各ノードにそれぞれ対応している。

40

各ノード情報は、ノード名、デバイス鍵及び無効化フラグを含む。

#### 【0045】

ノード名は、当該ノード情報に対応するノードを識別するための名称である。

デバイス鍵は、当該ノード情報に対応するノードに対して割り当てられた鍵である。

また、無効化フラグは、当該ノード情報に対応するデバイス鍵が無効化されているか否かを示すフラグであり、無効化フラグが「0」である場合には、無効化されていないことを示し、無効化フラグが「1」である場合には、無効化されていることを示す。

50

## 【 0 0 4 6 】

木構造テーブル D 1 0 0 内には、次に示す順序規則 1 に従った順序により各ノード情報が記憶される。ここに示す順序規則 1 は、記録装置 3 0 0 a、3 0 0 b、3 0 0 c、・・・、再生装置 4 0 0 a、4 0 0 b、4 0 0 c、・・・により、木構造テーブル D 1 0 0 から各ノード情報がシーケンシャルに読み出される場合においても適用される。

## 【 0 0 4 7 】

( a ) 木構造テーブル D 1 0 0 内には、木構造 T 1 0 0 のレイヤ数の昇順に、各レイヤに属するノードに対応するノード情報が記憶される。具体的には、木構造テーブル D 1 0 0 内には、最初にレイヤ 0 に属する 1 個のルートに対応する 1 個のノード情報が記憶され、次に、レイヤ 1 に属する 2 個のノードに対応する 2 個のノード情報が記憶され、次に、レイヤ 2 に属する 4 個のノードに対応する 4 個のノード情報が記憶される。以下同様である。

10

## 【 0 0 4 8 】

( b ) 各レイヤに属するノードについては、各ノードを識別するノード名の昇順により、対応するノード情報が記憶される。

具体的には、図 3 に示す木構造テーブル D 1 0 0 内には、次に示す順序により各ノード情報が記憶される。

「ルート」、「0」、「1」、「0 0」、「0 1」、「1 0」、「1 1」、「0 0 0」、「0 0 1」、「0 1 0」、「0 1 1」、・・・、「1 0 1」、「1 1 0」、「1 1 1」、「0 0 0 0」、「0 0 0 1」、「0 0 1 0」、「0 0 1 1」、・・・、「1 1 0 0」、「1 1 0 1」、「1 1 1 0」、「1 1 1 1」

20

ここでは、各ノード情報に含まれるノード名により、各ノード情報が記憶されている順序を示している。

## 【 0 0 4 9 】

## ( 2 ) 木構造構築部 1 0 1

木構造構築部 1 0 1 は、以下に示すようにして、デバイス鍵を管理するための n 分木のデータ構造を構築し、木構造格納部 1 0 2 に構築した木構造を格納する。ここで、n は 2 以上の整数であり、一例として、n = 2 である。

木構造構築部 1 0 1 は、最初に、ノード名として「ルート」を含むノード情報を生成し、木構造格納部 1 0 2 が有している木構造テーブルへ書き込む。

30

## 【 0 0 5 0 】

次に、木構造構築部 1 0 1 は、レイヤ 1 について、2 個のノードを識別するノード名「0」及び「1」を生成し、生成したノード名「0」及び「1」をそれぞれ含む 2 個のノード情報を生成し、生成した 2 個のノード情報をこの順序で、木構造格納部 1 0 2 が有している木構造テーブルへ追加して書き込む。

次に、木構造構築部 1 0 1 は、レイヤ 2 について、4 個のノードを識別するノード名「0 0」、「0 1」、「1 0」及び「1 1」を生成し、生成したノード名「0 0」、「0 1」、「1 0」及び「1 1」をそれぞれ含む 4 個のノード情報を生成し、生成した 4 個のノード情報をこの順序で、木構造格納部 1 0 2 が有している木構造テーブルへ追加して書き込む。

40

## 【 0 0 5 1 】

以降、木構造構築部 1 0 1 は、レイヤ 3 及びレイヤ 4 について、この順序で、上記と同様にして、ノード情報の生成と、木構造テーブルへの書き込みとを行う。

木構造構築部 1 0 1 は、次に、木構造のノード毎に乱数を用いてデバイス鍵を生成し、生成したデバイス鍵を各ノードに対応付けて木構造テーブル内に書き込む。

## 【 0 0 5 2 】

## ( 3 ) デバイス鍵割当部 1 0 3

デバイス鍵割当部 1 0 3 は、以下に示すようにして、木構造格納部 1 0 2 に格納されている木構造から、ユーザ装置が割り当てられていないリーフと、デバイス鍵を与えるべきユーザ装置を対応付けて適当なデバイス鍵を選択し、選択したデバイス鍵をユーザ装置へ出

50

力する。

【 0 0 5 3 】

デバイス鍵割当部 1 0 3 は、4 ビット長の変数 I D を有している。

デバイス鍵割当部 1 0 3 は、以下に示す処理 ( a ) ~ ( f ) を 1 6 回繰り返す。1 6 回の繰り返しのそれぞれにおいて、変数 I D は、「 0 0 0 0 」、「 0 0 0 1 」、「 0 0 1 0 」、  
・ ・ ・、「 1 1 1 0 」、「 1 1 1 1 」の値を保持する。1 6 回の繰り返しにより、デバイス鍵割当部 1 0 3 は、1 6 台のユーザ装置のそれぞれに I D 情報と 5 個のデバイス鍵とを割り当てる。

【 0 0 5 4 】

( a ) デバイス鍵割当部 1 0 3 は、木構造格納部 1 0 2 が有する木構造テーブルから、「  
ルート」のノード名を含むノード情報を取得し、取得したノード情報に含まれるデバイス  
鍵を抽出する。抽出したデバイス鍵が、ルートに割り当てられたデバイス鍵である。 10

( b ) デバイス鍵割当部 1 0 3 は、木構造格納部 1 0 2 が有する木構造テーブルから、変  
数 I D の先頭 1 ビットからなるノード名を含むノード情報を取得し、取得したノード情報  
に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵 A とする。

【 0 0 5 5 】

( c ) デバイス鍵割当部 1 0 3 は、木構造格納部 1 0 2 が有する木構造テーブルから、変  
数 I D の先頭 2 ビットからなるノード名を含むノード情報を取得し、取得したノード情報  
に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵 B とする。

( d ) デバイス鍵割当部 1 0 3 は、木構造格納部 1 0 2 が有する木構造テーブルから、変  
数 I D の先頭 3 ビットからなるノード名を含むノード情報を取得し、取得したノード情報  
に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵 C とする。 20

【 0 0 5 6 】

( e ) デバイス鍵割当部 1 0 3 は、木構造格納部 1 0 2 が有する木構造テーブルから、変  
数 I D の先頭 4 ビットからなるノード名を含むノード情報を取得し、取得したノード情報  
に含まれるデバイス鍵を抽出する。ここで、抽出したデバイス鍵をデバイス鍵 D とする。

( f ) デバイス鍵割当部 1 0 3 は、I D 情報としての変数 I D、ルートに割り当てられた  
デバイス鍵、各ノードに割り当てられたデバイス鍵 A、B、C、D、及び前記 5 個のデ  
バイス鍵をそれぞれ識別する 5 個のデバイス鍵識別情報を、ユーザ装置が有する鍵情報記  
憶部へ書き込む。 30

【 0 0 5 7 】

こうして、各ユーザ装置の鍵情報記憶部は、図 8 に一例として示すように、I D 情報、5  
個のデバイス鍵識別情報及び 5 個のデバイス鍵を記憶する。ここで、5 個のデバイス鍵識  
別情報と 5 個のデバイス鍵とは、それぞれ対応付けられている。各デバイス鍵識別情報は  
、対応するデバイス鍵が割り当てられているノードが属するレイアの数 ( レイア数 ) であ  
る。

【 0 0 5 8 】

以上のようにして、1 6 台のユーザ装置のそれぞれに、I D 情報及び 5 個のデバイス鍵が  
割り当てられる。

一例として、図 4 に示す木構造 T 1 0 0 は、上述したように、レイヤ数 5 の 2 分木であり  
、1 6 個のリーフを含んでいる。ここで、ユーザ装置は、1 6 台あるものとし、1 6 台の  
ユーザ装置は、各々 1 6 個のリーフに対応している。各ユーザ装置には、木構造 T 1 0 0  
において、対応するリーフからルートに至るまでの経路上に位置するノードに割り当てら  
れたデバイス鍵がそれぞれ与えられる。例えば、ユーザ装置 1 には、I K 1、Key H、  
Key D、Key B、Key A の 5 つのデバイス鍵が与えられる。また、例えば、ユーザ  
装置 1 には、I D 情報「 0 0 0 0 」が与えられ、ユーザ装置 1 4 には、I D 情報「 1 1 0  
1 」が与えられる。 40

【 0 0 5 9 】

( 4 ) 無効化装置指定部 1 0 4

無効化装置指定部 1 0 4 は、鍵管理装置 1 0 0 の運営管理者から、無効化する 1 台以上の 50

ユーザ装置をそれぞれ識別する 1 個以上の ID 情報を受け付け、受け付けた ID 情報を木構造更新部 105 へ出力する。

(5) 木構造更新部 105

木構造更新部 105 は、無効化装置指定部 104 から 1 個以上の ID 情報を受け取る。ID 情報を受け取ると、受け取った 1 個以上の ID 情報のそれぞれについて、次に示す処理 (a) ~ (d) を繰り返す。

【0060】

(a) 木構造更新部 105 は、受け取った ID 情報をノード名として含むノード情報を木構造格納部 102 が有する木構造テーブルから取得し、取得したノード情報に無効化フラグ「1」を付加し、無効化フラグ「1」が付加されたノード情報を、木構造テーブル上において、取得した前記ノード情報が記憶されていた位置に上書きする。

10

【0061】

(b) 木構造更新部 105 は、受け取った ID 情報の先頭 3 ビットをノード名として含むノード情報を木構造格納部 102 が有する木構造テーブルから取得し、上記と同様にして、取得したノード情報に無効化フラグ「1」を付加して木構造テーブルに上書きする。

(c) 木構造更新部 105 は、受け取った ID 情報の先頭 2 ビットをノード名として含むノード情報を木構造格納部 102 が有する木構造テーブルから取得し、上記と同様にして、取得したノード情報に無効化フラグ「1」を付加して木構造テーブルに上書きする。

【0062】

(d) 木構造更新部 105 は、「ルート」をノード名として含むノード情報を木構造格納部 102 が有する木構造テーブルから取得し、上記と同様にして、取得したノード情報に無効化フラグ「1」を付加して木構造テーブルに上書きする。

20

以上説明したように、木構造更新部 105 は、無効化装置指定部 104 から受け取った ID 情報に基づいて、木構造において、受け取った ID 情報が示すリーフから、ノードまでの経路上に存在する全てのノードを無効化する。

【0063】

図 4 に示す木構造 T100 において、ID 情報「0000」、「1010」及び「1011」により示されるユーザ装置が無効化されると想定する場合、上記のようにしてノードが無効化された木構造 T200 を図 5 に示す。

また、木構造テーブル D100 は、木構造 T200 に対応して無効化フラグが付加されたものである。

30

【0064】

木構造 T200 において、ID 情報「0000」により示されるユーザ装置 1 に対応するリーフからルートまでの経路に存在する全てのノード、ID 情報「1010」により示されるユーザ装置 1 に対応するリーフからルートまでの経路に存在する全てのノード、及び ID 情報「1011」により示されるユーザ装置 12 に対応するリーフからルートまでの経路に存在する全てのノードに、×印が付されているが、これらのノードは、無効化されたノードを示している。

【0065】

木構造テーブル D100 において、上記の無効化されたノードに対応するノード情報には、無効化フラグが付加されている。

40

(6) 鍵情報ヘッダ生成部 106

鍵情報ヘッダ生成部 106 は、レイヤ数を示す変数 i 及びレイヤに含まれるノード名を示す変数 j を有している。

【0066】

鍵情報ヘッダ生成部 106 は、次に示す処理 (a) を、木構造に含まれるレイヤ数分、繰り返す。レイヤ数分の繰り返しのそれぞれにおいて、レイヤ数を示す変数 i は、「0」、「1」、「2」、「3」の値を保持する。

(a) 鍵情報ヘッダ生成部 106 は、変数 i によりレイヤ数が示されるレイヤに含まれる全てのノードの数だけ、ノード毎に次に示す処理 (a-1) ~ (a-3) を繰り返す。こ

50

ここで、処理 ( a - 1 ) ~ ( a - 3 ) の対象となる対象ノード名を変数 j により示す。

【 0 0 6 7 】

( a - 1 ) 鍵情報ヘッダ生成部 1 0 6 は、木構造格納部 1 0 2 が有する木構造テーブルから、変数 j に「 0 」を結合して得られるノード名を含むノード情報を取得し、変数 j に「 1 」を結合して得られるノード名を含むノード情報を取得する。

このようにして得られた 2 個のノード情報は、それぞれ、変数 j により示される対象ノードの直下に接続されている 2 個の下位ノードに対応している。

【 0 0 6 8 】

( a - 2 ) 鍵情報ヘッダ生成部 1 0 6 は、取得した 2 個の前記ノード情報のそれぞれに含まれている無効化フラグの両方が「 0 」であるか、否かを調べ、両方が「 0 」でない場合に、取得した 2 個の前記ノード情報のそれぞれに含まれている 2 個の無効化フラグを、2 個の前記ノード情報が木構造テーブルに格納されている順序で並べて、ノード無効化パターン ( Node Revocation Pattern、以下、NRP と呼ぶ。 ) を生成する。

【 0 0 6 9 】

具体的には、取得した 2 個の前記ノード情報のそれぞれに含まれている無効化フラグが「 0 」及び「 0 」である場合には、ノード無効化パターンを生成しない。

また、取得した 2 個の前記ノード情報のそれぞれに含まれている無効化フラグが「 1 」及び「 0 」である場合には、NRP { 1 0 } を生成する。

【 0 0 7 0 】

取得した 2 個の前記ノード情報のそれぞれに含まれている無効化フラグが「 0 」及び「 1 」である場合には、NRP { 0 1 } を生成する。

取得した 2 個の前記ノード情報のそれぞれに含まれている無効化フラグが「 1 」及び「 1 」である場合には、NRP { 1 1 } を生成する。

( a - 3 ) 鍵情報ヘッダ生成部 1 0 6 は、生成した NRP を鍵情報記録装置 2 0 0 へ出力する。

【 0 0 7 1 】

以上説明したように、鍵情報ヘッダ生成部 1 0 6 は、木構造のレイヤ内のノード毎に、当該ノードの下位側に直接接続されている 2 個の下位ノードが無効化されているか否かを調べ、2 個の下位ノードのいずれか一方が無効化されている場合には、上記に示すようにして NRP を生成する。図 5 に示す木構造 T 2 0 0 において、×印が付されたノードの近辺に、当該ノードに対応して生成した NRP を示している。

【 0 0 7 2 】

また、鍵情報ヘッダ生成部 1 0 6 は、上記に示すような繰り返しにおいて、NRP を出力するので、図 5 に示す場合には、図 6 に一例として示す複数個の NRP が生成されて出力される。鍵情報ヘッダ生成部 1 0 6 は、これらの複数個の NRP をヘッダ情報として出力する。

図 5 に示す木構造 T 2 0 0 において、ユーザ装置 1、ユーザ装置 1 1 及びユーザ装置 1 2 がそれぞれ無効化されている。ここで、無効化されるべき各ユーザ装置に対応するリーフから、ルートに至るまでの経路上に存在するノード ( 図 5 において、×印が付されたノード ) を無効化ノードと称する。また、1 個のノードの子ノードが無効化ノードである場合を「 1」、そうでない場合を「 0」で表現し、それら子ノードの状態を左から順に連結したものが、そのノードの NRP である。NRP は、n 分木の場合、n ビットの情報である。図 5 における木構造 T 2 0 0 のルート T 2 0 1 について、2 つの子ノードが共に無効化ノードであるため、NRP は、{ 1 1 } と表現される。また、ノード T 2 0 2 に付された NRP は、{ 1 0 } と表現される。また、ノード T 2 0 3 は、無効化ノードであるが、子ノードが存在しないリーフであるため、NRP は付加されない。

【 0 0 7 3 】

図 6 に一例として示すように、ヘッダ情報 D 2 0 0 は、NRP { 1 1 }、{ 1 0 }、{ 1 0 }、{ 1 0 }、{ 0 1 }、{ 1 0 }、{ 1 1 } から構成され、各 NRP をこの順序で含

10

20

30

40

50

んでいる。

なお、これらの複数個のNRPのそれぞれは、ヘッダ情報D200内において格納される位置が定められている。この位置は、上記の繰り返しにより定まるものである。図6に示すように、ヘッダ情報D200内に「0」、「1」、「2」、「3」、「4」、「5」及び「6」により定まる位置において、それぞれ、NRP{11}、{10}、{10}、{10}、{01}、{10}、{11}が配置されている。

#### 【0074】

以上説明したように、鍵情報ヘッダ生成部106は、無効化ノードの1以上のNRPを抽出し、抽出したNRPを鍵情報のヘッダ情報として、鍵情報記録装置200へ出力する。このとき、鍵情報ヘッダ生成部106は、複数のNRPを水準順に並べる。すなわち、複数のNRPを上位レイヤから下位レイヤの順に並べ、レイヤが同じNRPについては、左から右への順に並べる。なお、NRPの並べ方はある規則に基づいていればよく、例えば、レイヤが同じ場合に右から左の順に並べるとしてもよい。

#### 【0075】

##### (7) 鍵情報生成部107

鍵情報生成部107は、鍵情報ヘッダ生成部106と同様に、レイヤ数を示す変数i及びレイヤに含まれるノード名を示す変数jを有している。

鍵情報生成部107は、次に示す処理(a)を、木構造に含まれ、レイヤ0を除くレイヤ数分、繰り返す。レイヤ数分の繰り返しのそれぞれにおいて、レイヤ数を示す変数iは、「1」、「2」、「3」の値を保持する。

#### 【0076】

(a) 鍵情報生成部107は、変数iによりレイヤ数が示されるレイヤに含まれる全てのノードの数だけ、ノード毎に次に示す処理(a-1)~(a-3)を繰り返す。ここで、処理(a-1)~(a-3)の対象となる対象ノード名を変数jにより示す。

(a-1) 鍵情報生成部107は、木構造格納部102が有する木構造テーブルから、変数jをノード名として含むノード情報を取得し、取得したノード情報に含まれる無効化フラグが「1」であるか又は「0」であるかを判断する。

#### 【0077】

(a-2) 無効化フラグが「0」である場合に、鍵情報生成部107は、さらに、対象ノードの上位に接続されている上位ノードに対応するデバイス鍵による暗号化がされているか否かを判断する。

(a-3) 暗号化がされていない場合に、鍵情報生成部107は、取得したノード情報に含まれるデバイス鍵を抽出し、暗号化アルゴリズムE1を適用して、抽出したデバイス鍵を用いて、生成されたメディア鍵を暗号化して、暗号化メディア鍵を生成する。

#### 【0078】

暗号化メディア鍵 = E1(デバイス鍵、メディア鍵)

ここで、E(A、B)は、暗号化アルゴリズムEを適用して、鍵Aを用いて、データBを暗号化することを示している。

また、暗号化アルゴリズムE1は、一例として、DES(Data Encryption Standard)である。

#### 【0079】

次に、鍵情報生成部107は、生成した暗号化メディア鍵を鍵情報記録装置200へ出力する。

なお、無効化フラグ「1」が付されている場合、又は暗号化がされている場合には、処理(a-3)は、行われない。

以上説明したように、鍵情報生成部107は、上記に示すような繰り返しにおいて、暗号化メディア鍵を出力するので、図5に示す場合には、図7に一例として示す複数個の暗号化メディア鍵が生成されて出力される。鍵情報生成部107は、これらの複数個の暗号化メディア鍵を鍵情報D300として出力する。

#### 【0080】

なお、これらの複数の暗号化メディア鍵のそれぞれは、鍵情報 D 3 0 0 内において格納されている位置が定められている。この位置は、上記の繰り返しにより定まるものである。図 7 に示すように、鍵情報 D 3 0 0 内に「0」、「1」、「2」、「3」及び「4」により定まる位置において、それぞれ、暗号化メディア鍵 E 1 (Key E、メディア鍵)、E 1 (Key G、メディア鍵)、E 1 (Key I、メディア鍵)、E 1 (Key L、メディア鍵)、E 1 (IK 2、メディア鍵) が配置されている。

#### 【0081】

##### 1.1.2 鍵情報記録装置 200

鍵情報記録装置 200 は、鍵情報ヘッダ生成部 106 からヘッダ情報を受け取り、鍵情報生成部 107 から鍵情報を受け取り、受け取ったヘッダ情報と鍵情報とを記録媒体 500 a に書き込む。

10

##### 1.1.3 記録媒体 500 a、b、c

記録媒体 500 a は、DVD-RAM 等のレコーダブルメディアであって、今だ何らの情報も記録されていないものである。

#### 【0082】

記録媒体 500 b は、記録媒体 500 a に、鍵管理装置 100 及び鍵情報記録装置 200 により、上記に述べたようにして、ヘッダ情報が付加された鍵情報が書き込まれたものである。

記録媒体 500 c は、記録媒体 500 b に、記録装置 300 a、300 b、300 c、・・・の何れかにより、上記に述べたようにして、暗号化コンテンツが書き込まれたものである。

20

#### 【0083】

図 8 に示すように、記録媒体 500 c は、ヘッダ情報が付加された鍵情報と暗号化コンテンツとを記録している。

##### 1.1.4 記録装置 300 a、300 b、300 c、・・・

記録装置 300 a は、図 8 に示すように、鍵情報記憶部 301、復号部 302、特定部 303、暗号部 304 及びコンテンツ記憶部 305 から構成されている。なお、記録装置 300 b、300 c、・・・は、記録装置 300 a と同様の構成を有しているので、これらについて説明を省略する。

#### 【0084】

30

記録装置 300 a は、具体的には、マイクロプロセッサ、ROM、RAM などを含んで構成され、前記 RAM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置 300 a は、その機能を達成する。

記録装置 300 a には、記録媒体 500 b が装着される。記録装置 300 a は、自らが記憶している ID 情報を元に記録媒体 500 b に記憶されているヘッダ情報の解析を行って、復号すべき暗号化メディア鍵の位置と、使用すべきデバイス鍵を特定し、特定したデバイス鍵を用いて復号してメディア鍵を獲得する。次に、獲得したメディア鍵を用いて、デジタル化されたコンテンツを暗号化し、暗号化コンテンツを記録媒体 500 b に記録する。

40

#### 【0085】

##### (1) 鍵情報記憶部 301

鍵情報記憶部 301 は、ID 情報と、5 個のデバイス鍵と、5 個のデバイス鍵をそれぞれ識別するための 5 個のデバイス鍵識別情報とを記憶するための領域を備えている。

##### (2) 特定部 303

特定部 303 は、鍵管理装置 100 が有する鍵情報ヘッダ生成部 106 が、鍵情報のヘッダ情報を上述した順序規則 1 に従って生成したものと想定して動作する。

#### 【0086】

特定部 303 は、鍵情報記憶部 301 から ID 情報を読み出す。また、記録媒体 500 b からヘッダ情報及び鍵情報を読み出す。次に、特定部 303 は、読み出した ID 情報及び

50

読み出したヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から1個の暗号化メディア鍵が存在する位置Xと、前記暗号化メディア鍵の復号に使用するデバイス鍵を識別するためのデータ鍵識別情報とを特定する。なお、暗号化メディア鍵が存在する位置X及びデバイス鍵識別情報を特定する場合の詳細の動作については、後述する。

【0087】

次に、特定部303は、特定した1個の暗号化メディア鍵及び決定した1個のデバイス鍵識別情報を復号部302へ出力する。

(3) 復号部302

復号部302は、特定部303から1個の暗号化メディア鍵及び1個のデバイス鍵識別情報を受け取る。1個の暗号化メディア鍵及び1個のデバイス鍵識別情報を受け取ると、受け取ったデバイス鍵識別情報により識別されるデバイス鍵を鍵情報記憶部301から読み出し、復号アルゴリズムD1を適用して、読み出したデバイス鍵を用いて、受け取った暗号化メディア鍵を復号して、メディア鍵を生成する。

【0088】

メディア鍵 = D1 (デバイス鍵、暗号化メディア鍵)

ここで、D(A、B)は、復号アルゴリズムDを適用して、鍵Aを用いて、暗号化データBを復号して元のデータを生成することを意味する。

また、復号アルゴリズムD1は、暗号化アルゴリズムE1に対応するものであり、暗号化アルゴリズムE1を適用して暗号化されたデータを復号するためのアルゴリズムである。

【0089】

次に、復号部302は、生成したメディア鍵を暗号部304へ出力する。

なお、図8に記載されている各ブロックは、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、各接続線は、信号や情報が伝達される経路を示している。また、復号部302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付されているものは、復号部302へ鍵としての情報が伝達される経路を示している。暗号部304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。

【0090】

(4) コンテンツ記憶部305

コンテンツ記憶部305は、デジタル化された音楽などの著作物であるコンテンツを記憶している。

(5) 暗号部304

暗号部304は、復号部302からメディア鍵を受け取り、コンテンツ記憶部305からコンテンツを読み出す。次に、暗号部304は、暗号化アルゴリズムE2を適用して、受け取ったメディア鍵を用いて、読み出したコンテンツを暗号化して暗号化コンテンツを生成する。

【0091】

暗号化コンテンツ = E2 (メディア鍵、コンテンツ)

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

次に、暗号部304は、生成した暗号化コンテンツを記録媒体500bへ書き込む。このようにして、暗号化コンテンツが書き込まれた記録媒体500cが生成される。

【0092】

1.1.5 再生装置400a、400b、400c、・・・

再生装置400aは、図9に示すように、鍵情報記憶部401、特定部402、復号部403、復号部404及び再生部405から構成されている。なお、再生装置400b、400c、・・・は、再生装置400aと同様の構成を有しているので、これらについて説明を省略する。

【0093】



再生装置 400a は、具体的には、マイクロプロセッサ、ROM、RAM などを含んで構成され、前記 RAM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置 400a は、その機能を達成する。

ここで、鍵情報記憶部 401、特定部 402 及び復号部 403 は、それぞれ、記録装置 300a が有している鍵情報記憶部 301、特定部 303 及び復号部 302 と同様の構成を有しているので、説明を省略する。

#### 【0094】

再生装置 400a に記録媒体 500c が装着される。再生装置 400a は、自ら記憶している ID 情報を元に、記録媒体 500c に記憶されているヘッダ情報の解析を行って、復号すべき暗号化メディア鍵の位置と、使用すべきデバイス鍵を特定し、特定したデバイス鍵を用いて復号してメディア鍵を獲得する。次に、再生装置 400a は、獲得したメディア鍵を用いて、記録媒体 500c に記録されている暗号化コンテンツを復号してコンテンツを再生する

##### (1) 復号部 404

復号部 404 は、復号部 403 からメディア鍵を受け取り、記録媒体 500c から暗号化コンテンツを読み出し、復号アルゴリズム D2 を適用して、受け取ったメディア鍵を用いて、読み出した前記暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生部 405 へ出力する。

#### 【0095】

コンテンツ = D2 (メディア鍵、暗号化コンテンツ)

ここで、復号アルゴリズム D2 は、暗号化アルゴリズム E2 に対応するものであり、暗号化アルゴリズム E2 を適用して暗号化されたデータを復号するためのアルゴリズムである。

##### (2) 再生部 405

再生部 405 は、復号部 404 からコンテンツを受け取り、受け取ったコンテンツを再生する。例えば、コンテンツが音楽の場合には、再生部 405 は、コンテンツを音声に変換して出力する。

#### 【0096】

##### 1.2. 著作物保護システム 10 の動作

著作物保護システム 10 の動作について説明する。

##### 1.2.1 デバイス鍵の割り当て、記録媒体の生成及びコンテンツの暗号化又は復号の動作

ここでは、ユーザ装置へデバイス鍵を割り当てる動作、鍵情報の生成と記録媒体への書き込みの動作及びユーザ装置によるコンテンツの暗号化又は復号の動作について、図 10 に示すフローチャートを用いて説明する。特に、デバイス鍵が不正な第三者により暴露されるまでの、各装置の動作について説明する。

#### 【0097】

鍵管理装置 100 の木構造構築部 101 は、木構造を表す木構造テーブルを生成し、生成した木構造テーブルを木構造格納部 102 へ書き込み (ステップ S101)、次に、木構造のノード毎にデバイス鍵を生成し、生成したデバイス鍵を各ノードに対応付けて木構造テーブル内に書き込む (ステップ S102)。次に、デバイス鍵割当部 103 は、デバイス鍵、デバイス鍵識別情報及び ID 情報を対応するユーザ装置へ出力する (ステップ S103 ~ S104)。ユーザ装置が有する鍵情報記憶部は、デバイス鍵、デバイス鍵識別情報及び ID 情報を受け取り (ステップ S104)、受け取ったデバイス鍵、デバイス鍵識別情報及び ID 情報を記録する (ステップ S111)。

#### 【0098】

このようにして、デバイス鍵、デバイス鍵識別情報及び ID 情報を記録しているユーザ装置が生産され、生産されたユーザ装置がユーザに対して販売される。

次に、鍵情報生成部 107 は、メディア鍵を生成し (ステップ S105)、鍵情報を生成

10

20

30

40

50

し(ステップS106)、生成した鍵情報を鍵情報記録装置200を介して記録媒体500aに出力し(ステップS107~S108)、記録媒体500aは、鍵情報を記録する(ステップS121)。

#### 【0099】

このようにして、鍵情報が記録された記録媒体500bが生成され、生成された記録媒体500bが販売などされることにより、利用者に配布される。

次に、鍵情報が記録された記録媒体が、ユーザ装置に装着され、ユーザ装置は、記録媒体から鍵情報を読み出し(ステップS131)、読み出した鍵情報を用いて、当該ユーザ装置自身に割り当てられた暗号化メディア鍵を特定し(ステップS132)、メディア鍵を復号し(ステップS133)、復号したメディア鍵を用いて、コンテンツを暗号化して記録媒体500bに書き込み、又は暗号化コンテンツの記録されている記録媒体500cから暗号化コンテンツを読み出し、読み出した暗号化コンテンツを復号したメディア鍵を用いて復号して、コンテンツを生成する(ステップS134)。

10

#### 【0100】

以上のように、ユーザ装置により暗号化コンテンツを記録媒体500bに書き込み、ユーザ装置により暗号化コンテンツの記録されている記録媒体500cから暗号化コンテンツを読み出して復号し、コンテンツを再生する。

次に、不正な第三者が、ユーザ装置に割り当てられたデバイス鍵を、何らかの手段により不正に取得する。不正な第三者は、前記コンテンツを不正に流通させたり、正規のユーザ装置を模倣する不正な装置を生産して販売する。

20

#### 【0101】

鍵管理装置100の運営管理者は、又は前記コンテンツの著作権者は、コンテンツが不正に流通していること、又は不正な装置が流通していることを知り、前記デバイス鍵が漏洩したことを知る。

#### 1.2.2 デバイス鍵が暴露された後の動作

ここでは、デバイス鍵が不正な第三者により暴露された後における、暴露されたデバイス鍵に対応する木構造の内のノードの無効化の動作、新たな鍵情報の生成と記録媒体への書き込みの動作、及びユーザ装置によるコンテンツの暗号化又は復号の動作について、図11に示すフローチャートを用いて説明する。

#### 【0102】

30

鍵管理装置100の無効化装置指定部104は、無効化する1台以上のユーザ装置の1個以上のID情報を受け付け、受け付けたID情報を木構造更新部105へ出力する(ステップS151)。次に、木構造更新部105は、ID情報を受け取り、受け取ったID情報を用いて、木構造を更新し(ステップS152)、鍵情報ヘッダ生成部106は、ヘッダ情報を生成し、生成したヘッダ情報を鍵情報記録装置200へ出力し(ステップS153)、鍵情報生成部は、メディア鍵を生成し(ステップS154)、鍵情報を生成し(ステップS155)、生成した鍵情報を鍵情報記録装置200を介して出力し(ステップS156~S157)、記録媒体500aは、鍵情報を記録する(ステップS161)。

#### 【0103】

このようにして、新たな鍵情報が記録された記録媒体500bが生成され、生成された記録媒体500bが販売などされることにより、利用者に配布される。

40

次に、新たな鍵情報が記録された記録媒体が、ユーザ装置に装着され、ユーザ装置は、記録媒体から鍵情報を読み出し(ステップS171)、読み出した鍵情報を用いて、当該ユーザ装置自身に割り当てられた暗号化メディア鍵を特定し(ステップS172)、メディア鍵を復号し(ステップS173)、復号したメディア鍵を用いて、コンテンツを暗号化して記録媒体500bに書き込み、又は暗号化コンテンツの記録されている記録媒体500cから暗号化コンテンツを読み出し読み出した暗号化コンテンツを復号したメディア鍵を用いて復号して、コンテンツを生成する(ステップS174)。

#### 【0104】

以上のように、ユーザ装置により暗号化コンテンツを記録媒体500bに書き込み、又は

50

ユーザ装置により暗号化コンテンツの記録されている記録媒体 5 0 0 c から暗号化コンテンツを読み出して復号し、コンテンツを再生する。

#### 1 . 2 . 3 木構造を構築して格納する動作

ここでは、木構造構築部 1 0 1 による木構造テーブルの生成と木構造格納部 1 0 2 への木構造テーブルの書き込みの動作について、図 1 2 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 0 に示すフローチャートにおけるステップ S 1 0 1 の詳細である。

##### 【 0 1 0 5 】

木構造構築部 1 0 1 は、最初に、ノード名として「ルート」を含むノード情報を生成し、木構造格納部 1 0 2 が有している木構造テーブルへ書き込む（ステップ S 1 9 1）。次に、木構造構築部 1 0 1 は、レイヤ  $i$  ( $i = 1, 2, 3, 4$ ) について、次に示すステップ S 1 9 3 ~ S 1 9 4 を繰り返す。

##### 【 0 1 0 6 】

木構造構築部 1 0 1 は、 $2i$  個の文字列をノード名として生成し（ステップ S 1 9 3）、生成した  $2i$  個の文字列をノード名として含むノード情報を、順に木構造テーブルへ書き込む（ステップ S 1 9 4）。

#### 1 . 2 . 4 デバイス鍵と ID 情報とを各ユーザ装置へ出力する動作

ここでは、デバイス鍵割当部 1 0 3 によるデバイス鍵と ID 情報とを各ユーザ装置へ出力する動作について、図 1 3 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 0 に示すフローチャートにおけるステップ S 1 0 3 の詳細である。

##### 【 0 1 0 7 】

デバイス鍵割当部 1 0 3 は、変数 ID を「0 0 0 0」、「0 0 0 1」、「0 0 1 0」、・・・、「1 1 1 0」、「1 1 1 1」のように変化させ、それぞれの変数 ID について、次に示すステップ S 2 2 2 ~ S 2 2 7 を繰り返す。

デバイス鍵割当部 1 0 3 は、ルートに割り当てられたデバイス鍵を取得し（ステップ S 2 2 2）、変数 ID の先頭 1 ビットをノード名とするノードに割り当てられたデバイス鍵 A を取得し（ステップ S 2 2 3）、変数 ID の先頭 2 ビットをノード名とするノードに割り当てられたデバイス鍵 B を取得し（ステップ S 2 2 4）、変数 ID の先頭 3 ビットをノード名とするノードに割り当てられたデバイス鍵 C を取得し（ステップ S 2 2 5）、変数 ID の先頭 4 ビットをノード名とするノードに割り当てられたデバイス鍵 D を取得し（ステップ S 2 2 6）、ID 情報としての変数 ID、ルートに割り当てられたデバイス鍵、各ノードに割り当てられたデバイス鍵 A、B、C、D をユーザ装置へ出力する（ステップ S 2 2 7）。

##### 【 0 1 0 8 】

#### 1 . 2 . 5 木構造の更新の動作

ここでは、木構造更新部 1 0 5 による木構造の更新の動作について、図 1 4 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 1 に示すフローチャートにおけるステップ S 1 5 2 の詳細である。

木構造更新部 1 0 5 は、無効化装置指定部 1 0 4 から受け取った 1 個以上の ID 情報のそれぞれについて、次に示すステップ S 2 4 2 ~ S 2 4 6 を繰り返す。

##### 【 0 1 0 9 】

木構造更新部 1 0 5 は、受け取った ID 情報をノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「1」を付加する（ステップ S 2 4 2）。次に、木構造更新部 1 0 5 は、受け取った ID 情報の先頭 3 ビットをノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「1」を付加する（ステップ S 2 4 3）。

##### 【 0 1 1 0 】

次に、木構造更新部 1 0 5 は、受け取った ID 情報の先頭 2 ビットをノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「1」を付加する（ステップ S 2 4 4）。

次に、木構造更新部 105 は、受け取った ID 情報の先頭 1 ビットをノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「1」を付加する（ステップ S245）。

【0111】

次に、木構造更新部 105 は、「ルート」をノード名として含むノード情報を取得し、取得したノード情報に無効化フラグ「1」を付加する（ステップ S246）。

1.2.6 ヘッド情報の生成の動作

ここでは、鍵情報ヘッド生成部 106 によるヘッド情報の生成の動作について、図 15 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 11 に示すフローチャートにおけるステップ S153 の詳細である。

【0112】

鍵情報ヘッド生成部 106 は、レイヤ 0 からレイヤ 3 までの各レイヤについて、ステップ S262 ~ S266 を繰り返す。さらに、鍵情報ヘッド生成部 106 は、各レイヤに含まれる対象ノード毎に、ステップ S263 ~ S265 を繰り返す。

鍵情報ヘッド生成部 106 は、当該対象ノードの直下に接続されている 2 個の下位ノードを選択し（ステップ S263）、次に選択した 2 個の下位ノードのそれぞれに無効化フラグが付されているか否かを調べて NRP を生成し（ステップ S264）、生成した NRP を出力する（ステップ S265）。

【0113】

1.2.7 鍵情報の生成の動作

ここでは、鍵情報生成部 107 による鍵情報の生成の動作について、図 16 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 11 に示すフローチャートにおけるステップ S155 の詳細である。

鍵情報生成部 107 は、レイヤ 1 からレイヤ 3 までの各レイヤについて、ステップ S282 ~ S287 を繰り返す。さらに、鍵情報生成部 107 は、各レイヤに含まれる対象ノード毎に、ステップ S283 ~ S286 を繰り返す。

【0114】

鍵情報生成部 107 は、対象ノードに無効化フラグ「1」が付されているか否かを判断する。無効化フラグ「1」が付されていない場合には（ステップ S283）、さらに対象ノードの上位に接続されている上位ノードに対応するデバイス鍵による暗号化がされているか否かを判断する。暗号化がされていない場合に（ステップ S284）、対象ノードに対応するデバイス鍵を木構造テーブルから取得し（ステップ S285）、取得したデバイス鍵を用いて、生成されたメディア鍵を暗号化して、暗号化メディア鍵を生成し、生成した暗号化メディア鍵を出力する（ステップ S286）。

【0115】

無効化フラグ「1」が付されている場合（ステップ S283）、又は暗号化がされている場合（ステップ S284）、ステップ S285 ~ S286 は行われない。

1.2.8 鍵情報の特定の動作

ここでは、記録装置 300a が有する特定部 303 により、記録媒体 500b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作について、図 17 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 11 に示すフローチャートにおけるステップ S172 の詳細である。

【0116】

また、再生装置 400a が有する特定部 402 による動作は、特定部 303 による動作と同じであるので、説明を省略する。

特定部 303 は、暗号化メディア鍵の位置を示す変数 X、ユーザ装置自身に関する 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、ユーザ装置自身に関する NRP（Node Revocation Pattern、以下、NRP と呼ぶ。）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

10

20

30

40

50

ドのN R Pを示す。

【0117】

特定部303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。  
特定部303は、初期値として、それぞれ変数 $A = 0$ 、変数 $W = 1$ 、変数 $i = 0$ とする（ステップS301）。

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S302）、このユーザ装置は、無効化されているので、次に、特定部303は、処理を終了する。

【0118】

変数 $i$ が値 $D$ より小さいか又は等しい場合（ステップS302）、特定部303は、A番目のN R Pを構成する左右2ビットのうち、ID情報の上位 $i$ 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S303）。ここで、対応するビット位置とは、図4に示すように、木構造において左の経路に「0」、右の経路に「1」が割り当てられ、これらの規則に基づいてID情報が構成されているので、ID情報の上位 $i$ ビット目の値「0」は、A番目のN R Pの左ビットに対応し、 $i$ ビット目の値「1」は、A番目のN R Pの右ビットに対応する。

【0119】

値 $B = 0$ の場合（ステップS303）、特定部303は、これまでにチェックしたN R Pのうち、オール「1」でないN R Pの数をカウントし、カウントした値を、変数 $X$ に代入する。こうして得られた変数 $X$ が、暗号化メディア鍵の位置を示している。また、この時点の変数 $i$ は、デバイス鍵を識別するためのデバイス鍵識別情報である（ステップS307）。次に、特定部303は、処理を終了する。

【0120】

値 $B = 1$ の場合（ステップS303）、特定部303は、レイヤ $i$ に存在する $W$ 個の全N R Pの「1」の数をカウントし、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N R Pの数を示す（ステップS304）。

次に、特定部303は、レイヤ $i$ に存在するN R Pのうちの最初のN R Pから、対応するビット位置までのN R Pをカウントし、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N R Pのうち、ユーザ装置自身に関するN R Pの位置を示す（ステップS305）。

【0121】

次に、特定部303は、変数 $i = i + 1$ を演算し（ステップS306）、次にステップS302へ制御を移し、上述の処理を繰り返す。

#### 1.2.9 鍵情報の特定の動作の具体例

一具体例として、図6及び図7に示すヘッダ情報及び鍵情報を用いて、図5に示す無効化されていないユーザ装置14が暗号化メディア鍵を特定するまでの動作について以下に説明する。ユーザ装置14には、ID情報「1101」が割り当てられ、デバイス鍵「Key A」、「Key C」、「Key G」、「Key N」及び「IK14」が割り当てられているものとする。

【0122】

（ステップ1）特定部303は、ユーザ装置14に割り当てられたID情報「1101」の最上位ビットの値が「1」であるため、最初のN R P { 11 } の右ビットをチェックする（ステップS303）。

（ステップ2）最初のN R P { 11 } の右ビットの値が「1」であるため、特定部303は、解析を続ける（ステップS303で、 $B = 1$ ）。

【0123】

（ステップ3）特定部303は、レイヤ0に存在する1個のN R P { 11 } の「1」の数をカウントする。そのカウントした値が「2」であるので、次のレイヤ1には2個のN R Pが存在することが分かる（ステップS304）。

（ステップ4）特定部303は、対応するビット位置までのN R P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。そのカウントした値が「1

」であるため、次のレイヤ 1 の対応する N R P の位置は、レイヤ 1 内で、1 番目である（ステップ S 3 0 5 ）。

【 0 1 2 4 】

（ステップ 5 ）次に、特定部 3 0 3 は、I D 情報「 1 1 0 1 」の上位から 2 ビット目の値が「 1 」であるため、レイヤ 1 の 1 番目の N R P { 1 0 } の右ビットをチェックする（ステップ S 3 0 3 ）。

（ステップ 6 ）ここで、レイヤ 1 の 1 番目の N R P { 1 0 } の右ビットの値が「 0 」であるため、特定部 3 0 3 は、解析を終了する（ステップ S 3 0 3 で、B = 0 ）。

【 0 1 2 5 】

（ステップ 7 ）特定部 3 0 3 は、これまでの N R P のうち、オール「 1 」でない N R P の数をカウントする。ただし、最後にチェックした N R P はカウントしない。カウントした値が「 1 」であるため、暗号化メディア鍵の位置は、鍵情報内において、1 番目である（ステップ S 3 0 7 ）。

（ステップ 8 ）図 7 に示すように、鍵情報の 1 番目の位置に格納されている暗号化メディア鍵は、E 1（K e y G，メディア鍵）である。

【 0 1 2 6 】

ユーザ装置 1 4 は、K e y G を保持している。よって、ユーザ装置 1 4 は、K e y G を用いて暗号化メディア鍵を復号してメディア鍵を獲得することができる。

1 . 3 まとめ

以上説明したように、第 1 の実施の形態によると、記録媒体に予め記録されている鍵情報のヘッダ情報内には、複数の N R P が水準順に並べられているので、鍵情報がコンパクトになる。また、プレーヤは、復号すべき暗号化メディア鍵を効率よく特定することができる。

【 0 1 2 7 】

2 . 第 2 の実施の形態

ここでは、第 1 の実施の形態の変形例としての第 2 の実施の形態について説明する。

第 1 の実施の形態において、一例として図 1 8 に示すように、無効化されるユーザ装置が木構造の中で特定のリーフに偏って発生する可能性がある。この場合、鍵管理装置 1 0 0 が記録媒体に書き込む鍵情報のヘッダ情報内において、{ 1 1 } である N R P が多くなる。図 1 8 に示す例では、木構造 T 3 0 0 の左半分のリーフは、全て無効化された装置に対応するので、鍵情報内のヘッダ情報は、1 1 個の N R P を含むが、そのうち 8 個は { 1 1 } である。

【 0 1 2 8 】

図 1 8 に示す例では、木構造 T 3 0 0 の左半分は全て無効化された装置であるので、レイヤ 1 の左のノードから下は全て無効化ノードであると表現すれば、左半分の各ノードに対応した N R P をヘッダ情報として記録媒体に記録する必要がなくなる。

そこで、第 2 の実施の形態では、無効化された装置が木構造の中で特定のリーフに集中する場合に、ヘッダ情報のデータ量を少なく抑えることができる著作物保護システム 1 0 b（図示していない）について説明する。

【 0 1 2 9 】

鍵管理装置 1 0 0 は、第 1 の実施の形態において説明したように、鍵情報のヘッダ情報として、N R P を生成する。ここで、鍵管理装置 1 0 0 は、N R P の先頭に 1 ビットを追加する。追加したビットが「 1 」である場合には、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示す。図 1 9 において、ノード T 4 0 1 及びノード T 4 0 2 は、これらのノードの子孫のノードに割り当てられた装置が全て無効化装置ではないので、先頭ビットは「 0 」であり、N R P は、それぞれ、{ 0 1 1 }、{ 0 1 0 } と表現される。ノード T 4 0 3 の子孫のノードに割り当てられた装置は、全て無効化装置であるため、N R P は { 1 1 1 } と表現される。鍵管理装置 1 0 0 は、ノード T 4 0 3 の子孫のノードについての N R P を記録媒体に書き込まない。

【 0 1 3 0 】

## 2.1 著作物保護システム10bの構成

著作物保護システム10bは、著作物保護システム10と同様の構成を有している。ここでは、著作物保護システム10との相違点を中心として説明する。

第2の実施の形態では、図19に示すように、ユーザ装置1～ユーザ装置8及びユーザ装置12がそれぞれ無効化されているとする。

### 【0131】

#### 2.1.1 鍵管理装置100

著作物保護システム10bの鍵管理装置100は、第1の実施の形態において述べた鍵管理装置100と同様の構成を有している。ここでは、その相違点を中心として説明する。

##### (1) 木構造格納部102

木構造格納部102は、木構造テーブルD100に代えて、一例として図20に示す木構造テーブルD400を有している。

### 【0132】

木構造テーブルD400は、図19に一例として示す木構造T400に対応しており、木構造T400を表現するためのデータ構造を示す。

木構造テーブルD400は、木構造T400に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造T400を構成する各ノードにそれぞれ対応している。

### 【0133】

各ノード情報は、ノード名、デバイス鍵、無効化フラグ及びNRPを含む。

ノード名、デバイス鍵及び無効化フラグについては、第1の実施の形態で説明したとおりであるので、説明を省略する。

NRPは、3ビットから構成され、上位の1ビットは、上述したように、対応するノード名により示されるノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示す。下位の2ビットは、第1の実施の形態で説明したNRPと同じ内容のものである。

### 【0134】

#### (2) 鍵情報ヘッダ生成部106

鍵情報ヘッダ生成部106は、NRPの先頭の1ビットが「1」である場合には、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示すNRPを生成し、生成したNRPを鍵情報記録装置200へ出力する。なお、NRPの生成の詳細については、後述する。

### 【0135】

鍵情報ヘッダ生成部106は、一例として、図21に示すヘッダ情報D500を生成する。ヘッダ情報D500は、NRP{011}、{111}、{010}、{001}及び{001}から構成され、各NRPをこの順序で含んでいる。また、この図に示すように、ヘッダ情報D500内に「0」、「1」、「2」、「3」及び「4」により定まる位置において、それぞれ、NRP{011}、{111}、{010}、{001}及び{001}が配置されている。

### 【0136】

#### (3) 鍵情報生成部107

鍵情報生成部107は、一例として、図22に示す鍵情報D600を生成する。鍵情報D600は、3個の暗号化メディア鍵を含んでいる。3個の暗号化メディア鍵は、それぞれデバイス鍵KeyG、KeyL、IK11を用いてメディア鍵を暗号化したものである。

### 【0137】

これらの複数個の暗号化メディア鍵のそれぞれは、鍵情報D600内において格納されている位置が定められている。この図に示すように、鍵情報D600内に「0」、「1」及び「2」により定まる位置において、それぞれ、暗号化メディア鍵E1(KeyG、メディア鍵)、E1(KeyL、メディア鍵)及びE1(IK11、メディア鍵)が配置されている。

10

20

30

40

50

## 【 0 1 3 8 】

## 2 . 1 . 2 記録装置 3 0 0 a

記録装置 3 0 0 a は、第 1 の実施の形態において述べた記録装置 3 0 0 a と同様の構成を有している。ここでは、その相違点を中心として説明する。

## ( 1 ) 特定部 3 0 3

特定部 3 0 3 は、ID 情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から 1 個の暗号化メディア鍵が存在する位置 X を特定する。なお、暗号化メディア鍵が存在する位置 X を特定する場合の詳細の動作については、後述する。

## 【 0 1 3 9 】

## 2 . 2 著作物保護システム 1 0 b の動作

著作物保護システム 1 0 b の動作について、著作物保護システム 1 0 の動作との相違点を中心として説明する。

## 2 . 2 . 1 ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作について、図 2 3 ~ 図 2 6 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 1 に示すフローチャートにおけるステップ S 1 5 3 の詳細である。

## 【 0 1 4 0 】

鍵情報ヘッダ生成部 1 0 6 は、レイヤ 0 からレイヤ 3 までの各レイヤについて、ステップ S 3 2 2 ~ S 3 2 7 を繰り返す。さらに、鍵情報ヘッダ生成部 1 0 6 は、各レイヤに含まれる対象ノード毎に、ステップ S 3 2 3 ~ S 3 2 6 を繰り返す。

鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードの直下に接続される 2 個の下位ノードを選択し (ステップ S 3 2 3 )、選択した 2 個の下位ノードのそれぞれに無効化フラグが付されているか否かを調べて、NRP を生成し (ステップ S 3 2 4 )、値「0」を有する拡張ビットを生成した NRP の先頭に付加し (ステップ S 3 2 5 )、拡張ビットが付加された NRP を木構造テーブル内の当該対象ノードに対応するノード情報内に付加する (ステップ S 3 2 6 )。

## 【 0 1 4 1 】

以上のようにして、ステップ S 3 2 1 ~ S 3 2 8 の繰返しが終了すると、第 1 の実施の形態において説明した方法と同様に、各ノード情報内に NRP が付加される。ここで、各 NRP の先頭には、値「0」(1 ビット) が付加されている。次に、鍵情報ヘッダ生成部 1 0 6 は、レイヤ 3 からレイヤ 0 までの各レイヤについて、ステップ S 3 3 0 ~ S 3 3 5 を繰り返す。さらに、鍵情報ヘッダ生成部 1 0 6 は、各レイヤに含まれる対象ノード毎に、ステップ S 3 3 1 ~ S 3 3 4 を繰り返す。

## 【 0 1 4 2 】

鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードの直下に接続される 2 個の下位ノードを選択し (ステップ S 3 3 1 )、選択した 2 個のノードの両方にそれぞれ NRP { 1 1 1 } が付加されているか否かを調べる。ただし、選択した 2 個のノードがリーフである場合には、選択した 2 個のノードの両方に無効化フラグが付されているか否かを調べる (ステップ S 3 3 2 )。

## 【 0 1 4 3 】

選択した 2 個の下位ノードの両方にそれぞれ NRP { 1 1 1 } が付されている場合にのみ、ただし選択した 2 個のノードがリーフである場合には、選択した 2 個の下位ノードの両方に無効化フラグが付されている場合にのみ (ステップ S 3 3 3 )、鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードに付加された NRP の先頭ビットを「1」に書き換える (ステップ S 3 3 4 )。

## 【 0 1 4 4 】

以上のようにして、ステップ S 3 2 9 ~ S 3 3 6 の繰返しが終了すると、それぞれ NRP { 1 1 1 } が付加されている 2 個の下位ノードに接続する上位のノードには、{ 1 1 1 } が付加されることになる。

10

20

30

40

50



次に、鍵情報ヘッダ生成部 106 は、レイヤ 2 からレイヤ 0 までの各レイヤについて、ステップ S 338 ~ S 343 を繰り返す。さらに、鍵情報ヘッダ生成部 106 は、各レイヤに含まれる対象ノード毎に、ステップ S 339 ~ S 342 を繰り返す。

#### 【0145】

鍵情報ヘッダ生成部 106 は、当該対象ノードの直下に接続される 2 個の下位ノードを選択し（ステップ S 339）、選択した 2 個の下位ノードの両方に NRP { 111 } が付加されているか否かを調べる（ステップ S 340）。

選択した 2 個の下位ノードの両方に NRP { 111 } が付加されている場合にのみ（ステップ S 341）、鍵情報ヘッダ生成部 106 は、選択した 2 個の下位ノードにそれぞれ付加された NRP を木構造テーブルから削除する（ステップ S 342）。 10

#### 【0146】

次に、鍵情報ヘッダ生成部 106 は、木構造テーブルに記憶されている NRP をルートから順に読み出して、出力する（ステップ S 345）。

以上のようにして、NRP の先頭の 1 ビットが「1」である場合に、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示す NRP が生成される。

#### 【0147】

##### 2.2.2 鍵情報の特定の動作

ここでは、記録装置 300a が有する特定部 303 により、記録媒体 500b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作について、図 27 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 11 に示すフローチャートにおけるステップ S 172 の詳細である。 20

#### 【0148】

また、特定部 303 による 1 個の暗号化メディア鍵を特定する動作は、第 1 の実施の形態において説明した動作と同様であり、ここでは、その相違点を中心として説明する。

値 B = 0 の場合（ステップ S 303）、特定部 303 は、これまでにチェックした NRP のうち、下位 2 ビットがオール「1」でない NRP の数をカウントし、カウントした値を、変数 X に代入する。こうして得られた変数 X が、暗号化メディア鍵の位置を示している（ステップ S 307a）。次に、特定部 303 は、処理を終了する。

#### 【0149】

値 B = 1 の場合（ステップ S 303）、特定部 303 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 S 304a）。 30

#### 【0150】

次に、特定部 303 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 のうち、ユーザ装置自身に関する NRP の位置を示す（ステップ S 305a）。 40

#### 【0151】

##### 2.2.3 鍵情報の特定の動作の具体例

一具体例として、図 21 及び図 22 に示す鍵情報を用いて、図 19 に示す無効化されていないユーザ装置 10 が暗号化メディア鍵を特定するまでの動作について以下に説明する。ユーザ装置 10 には、ID 情報「1001」が割り当てられ、デバイス鍵「Key A」、「Key C」、「Key F」、「Key L」及び「IK10」が割り当てられているものとする。

#### 【0152】

（ステップ 1）特定部 303 は、ユーザ装置 10 に割り当てられた ID 情報「1001」の最上位ビットの値が「1」であるため、最初の NRP { 011 } の下位 2 ビットのうち 50

の右ビットをチェックする（ステップS 3 0 3）。

（ステップ2）最初のN R P { 0 1 1 } の下位2ビットのうちの右ビットの値が「1」であるため、特定部3 0 3は、解析を続ける（ステップS 3 0 3で、B = 1）。

【0 1 5 3】

（ステップ3）特定部3 0 3は、レイヤ0に存在する1個のN R P { 0 1 1 } の下位2ビットのうちの「1」の数をカウントする。そのカウントした値が「2」であるため、次のレイヤ1には2個のN R Pが存在することが分かる（ステップS 3 0 4 a）。

（ステップ4）特定部3 0 3は、対応するビット位置までのN R P { 0 1 1 } の下位2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。そのカウントした値が「1」であるため、次のレイヤ1の対応するN R Pの位置は、レイヤ1内において、1番目である（ステップS 3 0 5 a）。

10

【0 1 5 4】

（ステップ5）次に、特定部3 0 3は、ID情報「1 0 0 1」の上位から2ビット目の値が「0」であるため、レイヤ1の1番目のN R P { 0 1 0 } の下位2ビットのうちの左ビットをチェックする（ステップS 3 0 3）。

（ステップ6）ここで、レイヤ1の1番目のN R P { 0 1 0 } の下位2ビットのうちの左ビットの値が「1」であるため、特定部3 0 3は、解析を続ける（ステップS 3 0 3で、B = 1）。

【0 1 5 5】

（ステップ7）特定部3 0 3は、レイヤ1に存在する2個のN R P { 1 1 1 }、{ 0 1 0 } の下位2ビットのうちの「1」の数をカウントする。ただし、N R Pの最上位ビットが「1」であるN R Pについては、カウントしない。そのカウントした値が「1」であるため、次のレイヤ2には1個のN R Pが存在することが分かる（ステップS 3 0 4 a）。

20

【0 1 5 6】

（ステップ8）特定部3 0 3は、対応するビット位置までのN R P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。そのカウントした値が「0」であるため、次のレイヤ2の対応するN R Pの位置は、レイヤ2内において、0番目である（ステップS 3 0 5 a）。

（ステップ9）次に、特定部3 0 3は、ID情報「1 0 0 1」の上位から3ビット目の値が「0」であるため、レイヤ2の0番目のN R P { 0 0 1 } の下位2ビットのうちの左ビットをチェックする（ステップS 3 0 3）。

30

【0 1 5 7】

（ステップ10）ここで、レイヤ2の0番目のN R P { 0 0 1 } の下位2ビットのうちの左ビットの値が「0」であるため、特定部3 0 3は、解析を終了する（ステップS 3 0 3で、B = 0）。

（ステップ11）特定部3 0 3は、これまでに解析したN R Pのうち、下位2ビットが、オール「1」でないN R Pの数をカウントする。なお、最後にチェックしたN R Pは、カウントしない。カウントした値が「1」であるため、暗号化メディア鍵の位置は、鍵情報内において、1番目である（ステップS 3 0 7 a）。

【0 1 5 8】

40

（ステップ12）図2 2より、鍵情報の1番目の位置に格納されている暗号化メディア鍵は、E 1（Key L，メディア鍵）である。

ユーザ装置1 0は、Key Lを保持している。よって、ユーザ装置1 0は、Key Lを用いて暗号化メディア鍵を復号してメディア鍵を獲得することができる。

【0 1 5 9】

なお、上述した第2の実施の形態においては、あるノードの子孫に存在するユーザ装置が全て無効化装置である場合に、追加するビットを「1」としている。しかし、リーフのレイヤ数がそれぞれ異なるような木構造がある場合、あるノードの子孫にN R Pが存在しない場合は、追加したビットを「1」にすることで終端を意味するフラグとしても使用することができる。

50

## 【 0 1 6 0 】

## 3 . 第 3 の 実 施 の 形 態

上記の第 2 の実施の形態においては、あるノードの子孫が全て無効化装置であるか否かを示すビットを N R P の先頭に追加することで、無効化装置が集中した場合に、ヘッダ情報をさらに少なく抑える方法を示している。

次に述べる第 3 の実施の形態では、N R P にビットを追加する代わりに、特定のパターン { 0 0 } を有する N R P を用いて、1 個のノードの子孫が全て無効化装置であるか否かを判断する。これは、レイヤ 0 を除く全てのレイヤにおいては、N R P { 0 0 } が使われないことに着目したものである。これにより、第 2 の実施の形態よりも、さらにヘッダ情報を少なく抑えることができる著作物保護システム 1 0 c ( 図示していない ) について説明する。

10

- ここでは、図 2 8 に示すように、ユーザ装置 1 ~ ユーザ装置 8、ユーザ装置 1 2 がそれぞれ無効化されているとする。第 3 の実施の形態では、N R P は第 1 の実施の形態に示す通りであるが、あるノードの子孫のユーザ装置が全て無効化装置である場合には、そのノードの N R P を { 0 0 } で表現する。図 2 8 におけるノード T 5 0 1 について、そのノードの子孫が全て無効化装置であるため、N R P は { 0 0 } と表現されている。

## 【 0 1 6 1 】

## 3 . 1 著作物保護システム 1 0 c の構成

著作物保護システム 1 0 c は、著作物保護システム 1 0 と同様の構成を有している。ここでは、著作物保護システム 1 0 との相違点を中心として説明する。

20

## 3 . 1 . 1 鍵管理装置 1 0 0

著作物保護システム 1 0 c の鍵管理装置 1 0 0 は、第 1 の実施の形態において述べた鍵管理装置 1 0 0 と同様の構成を有している。ここでは、その相違点を中心として説明する。

## 【 0 1 6 2 】

## ( 1 ) 鍵情報ヘッダ生成部 1 0 6

鍵情報ヘッダ生成部 1 0 6 は、N R P が { 0 0 } である場合には、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示す N R P を生成し、生成した N R P を鍵情報記録装置 2 0 0 へ出力する。なお、N R P の生成の詳細については、後述する。

## 【 0 1 6 3 】

鍵情報ヘッダ生成部 1 0 6 は、一例として、図 2 9 に示すヘッダ情報 D 7 0 0 を生成する。ヘッダ情報 D 7 0 0 は、N R P { 1 1 }、{ 0 0 }、{ 1 0 }、{ 0 1 } 及び { 0 1 } から構成され、各 N R P をこの順序で含んでいる。また、この図に示すように、ヘッダ情報 D 7 0 0 内に「 0 」、「 1 」、「 2 」、「 3 」及び「 4 」により定まる位置において、それぞれ、N R P { 1 1 }、{ 0 0 }、{ 1 0 }、{ 0 1 } 及び { 0 1 } が配置されている。

30

## 【 0 1 6 4 】

## ( 2 ) 鍵情報生成部 1 0 7

鍵情報生成部 1 0 7 は、一例として、図 3 0 に示す鍵情報 D 8 0 0 を生成する。鍵情報 D 8 0 0 は、3 個の暗号化メディア鍵を含んでいる。3 個の暗号化メディア鍵は、それぞれデバイス鍵 K e y G、K e y L、I K 1 1 を用いてメディア鍵を暗号化したものである。

40

## 【 0 1 6 5 】

これらの複数個の暗号化メディア鍵のそれぞれは、鍵情報 D 8 0 0 内において格納されている位置が定められている。この図に示すように、鍵情報 D 8 0 0 内に「 0 」、「 1 」及び「 2 」により定まる位置において、それぞれ、暗号化メディア鍵 E 1 ( K e y G、メディア鍵)、E 1 ( K e y L、メディア鍵) 及び E 1 ( I K 1 1、メディア鍵) が配置されている。

## 【 0 1 6 6 】

## 3 . 1 . 2 記録装置 3 0 0 a

著作物保護システム 1 0 c の記録装置 3 0 0 a は、第 1 の実施の形態において述べた記録

50

装置 3 0 0 a と同様の構成を有している。ここでは、その相違点を中心として説明する。

( 1 ) 特定部 3 0 3

特定部 3 0 3 は、ID 情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から 1 個の暗号化メディア鍵が存在する位置 X を特定する。なお、暗号化メディア鍵が存在する位置 X を特定する場合の詳細の動作については、後述する。

【 0 1 6 7 】

3 . 2 著作物保護システム 1 0 c の動作

著作物保護システム 1 0 c の動作について、著作物保護システム 1 0 の動作との相違点を中心として説明する。

10

3 . 2 . 1 ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作について、図 3 1 ~ 図 3 4 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 1 に示すフローチャートにおけるステップ S 1 5 3 の詳細である。

【 0 1 6 8 】

鍵情報ヘッダ生成部 1 0 6 は、レイヤ 0 からレイヤ 3 までの各レイヤについて、ステップ S 3 2 2 ~ S 3 2 7 を繰り返す。さらに、鍵情報ヘッダ生成部 1 0 6 は、各レイヤに含まれる対象ノード毎に、ステップ S 3 2 3 ~ S 3 2 6 a を繰り返す。

鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードの直下に接続される 2 個の下位ノードを選択し ( ステップ S 3 2 3 ) 、選択した 2 個の下位ノードのそれぞれに無効化フラグが付されているか否かを調べて、N R P を生成し ( ステップ S 3 2 4 ) 、生成された N R P を木構造テーブル内の当該対象ノードに対応するノード情報内に付加する ( ステップ S 2 3 6 a ) 。

20

【 0 1 6 9 】

以上のようにして、ステップ S 3 2 1 ~ S 3 2 8 の繰返しが終了すると、第 1 の実施の形態において説明した方法と同様に、各ノードに N R P が付加される。次に、鍵情報ヘッダ生成部 1 0 6 は、レイヤ 3 からレイヤ 0 までの各レイヤについて、ステップ S 3 3 0 ~ S 3 3 5 を繰り返す。さらに、鍵情報ヘッダ生成部 1 0 6 は、各レイヤに含まれる対象ノード毎に、ステップ S 3 3 1 ~ S 3 3 4 a を繰り返す。

【 0 1 7 0 】

30

鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードの直下に接続される 2 個の下位ノードを選択し ( ステップ S 3 3 1 ) 、選択した 2 個のノードの両方にそれぞれ N R P { 1 1 } が付加されているか否かを調べる。ただし、選択した 2 個のノードがリーフである場合には、選択した 2 個のノードの両方に無効化フラグが付されているか否かを調べる ( ステップ S 3 3 2 ) 。

【 0 1 7 1 】

選択した 2 個の下位ノードの両方にそれぞれ N R P { 1 1 } が付されている場合にのみ、ただし選択した 2 個のノードがリーフである場合には、選択した 2 個の下位ノードの両方に無効化フラグが付されている場合にのみ ( ステップ S 3 3 3 ) 、鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードに付加された N R P を { 0 0 } に書き換える ( ステップ S 3 3 4 a ) 。

40

【 0 1 7 2 】

以上のようにして、ステップ S 3 2 9 ~ S 3 3 6 の繰返しが終了すると、それぞれ N R P { 1 1 } が付加されている 2 個の下位ノードに接続する上位のノードには、{ 0 0 } が付加されることになる。

次に、鍵情報ヘッダ生成部 1 0 6 は、レイヤ 2 からレイヤ 0 までの各レイヤについて、ステップ S 3 3 8 ~ S 3 4 3 を繰り返す。さらに、鍵情報ヘッダ生成部 1 0 6 は、各レイヤに含まれる対象ノード毎に、ステップ S 3 3 9 ~ S 3 4 2 a を繰り返す。

【 0 1 7 3 】

鍵情報ヘッダ生成部 1 0 6 は、当該対象ノードの直下に接続される 2 個の下位ノードを選

50

折し（ステップS 3 3 9）、選択した2個の下位ノードの両方にN R P { 0 0 } が付加されているか否かを調べる（ステップS 3 4 0 a）。

選択した2個の下位ノードの両方にN R P { 0 0 } が付加されている場合にのみ（ステップS 3 4 1 a）、鍵情報ヘッダ生成部1 0 6は、選択した2個の下位ノードにそれぞれ付加されたN R P を木構造テーブルから削除する（ステップS 3 4 2 a）。

【0 1 7 4】

次に、鍵情報ヘッダ生成部1 0 6は、木構造テーブルに記憶されているN R P をルートから順に読み出して、出力する（ステップS 3 4 5）。

以上のようにして、N R P が { 0 0 } である場合に、そのノードの子孫のノードに割り当てられたユーザ装置は全て無効化装置であることを示すN R P が生成される。

10

【0 1 7 5】

### 3 . 2 . 2 鍵情報の特定の動作

ここでは、記録装置3 0 0 aが有する特定部3 0 3により、記録媒体5 0 0 bに記憶されている鍵情報から、1個の暗号化メディア鍵を特定する動作について、図3 5に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図1 1に示すフローチャートにおけるステップS 1 7 2の詳細である。

【0 1 7 6】

また、特定部3 0 3による1個の暗号化メディア鍵を特定する動作は、第1の実施の形態において説明した動作と同様であり、ここでは、その相違点を中心として説明する。

値B = 0の場合（ステップS 3 0 3）、特定部3 0 3は、これまでにチェックしたN R Pのうち、オール「1」でないN R Pの数とオール「0」でないN R Pの数とをカウントする。ただし、レイヤ0に関してのみ、オール「0」のN R Pもカウントする。カウントした値を、変数Xに代入する。こうして得られた変数Xが、暗号化メディア鍵の位置を示している。また、この時点の変数iは、デバイス鍵を識別するためのデバイス鍵識別情報である（ステップS 3 0 7 b）。次に、特定部3 0 3は、処理を終了する。

20

【0 1 7 7】

### 3 . 2 . 3 鍵情報の特定の動作の具体例

一具体例として、図2 9及び図3 0に示す鍵情報を用いて、図2 8に示す無効化されていないユーザ装置1 0が暗号化メディア鍵を特定するまでの動作について以下に説明する。

ユーザ装置1 0には、ID情報「1 0 0 1」が割り当てられ、デバイス鍵「Key A」、「Key C」、「Key F」、「Key L」及び「IK 1 0」が割り当てられているものとする。

30

【0 1 7 8】

（ステップ1）特定部3 0 3は、ユーザ装置1 0に割り当てられたID情報「1 0 0 1」の最上位ビットの値が「1」であるため、最初のN R P { 1 1 }の右ビットをチェックする（ステップS 3 0 3）。

（ステップ2）最初のN R P { 1 1 }の右ビットの値が「1」であるため、特定部3 0 3は、解析を続ける（ステップS 3 0 3で、B = 1）。

【0 1 7 9】

（ステップ3）特定部3 0 3は、レイヤ0に存在する1個のN R P { 1 1 }の「1」の数をカウントする。そのカウントした値が「2」であるため、次のレイヤ1には2個のN R Pが存在することが分かる（ステップS 3 0 4）。

40

（ステップ4）特定部3 0 3は、対応するビット位置までのN R P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。そのカウントした値が「1」であるため、次のレイヤ1の対応するN R Pの位置は、レイヤ1内において、1番目である（ステップS 3 0 5）。

【0 1 8 0】

（ステップ5）次に、特定部3 0 3は、ID情報「1 0 0 1」の上位から2ビット目の値が「0」であるため、レイヤ1の1番目のN R P { 1 0 }の左ビットをチェックする（ステップS 3 0 3）。

50

(ステップ6) レイヤ1の1番目のNRP{10}の左ビットの値が「1」であるため、特定部303は、解析を続ける(ステップS303で、B=1)。

【0181】

(ステップ7) 特定部303は、レイヤ1に存在する2個のNRPの「1」の数をカウントする。ここで、NRP{00}は、カウントしない。そのカウントした値が「1」であるため、次のレイヤ2には1個のNRPが存在することが分かる(ステップS304)。

(ステップ8) 特定部303は、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、対応するビット位置の値はカウントしない。そのカウントした値が「0」であるため、次のレイヤ2の対応するNRPの位置は、レイヤ2内において、0番目である(ステップS305)。

10

【0182】

(ステップ9) 次に、特定部303は、ID情報「1001」の上位から3ビット目の値が「0」であるため、レイヤ2の0番目のNRP{01}の下位2ビットのうちの左ビットをチェックする(ステップS303)。

(ステップ10) ここで、レイヤ2の0番目のNRP{01}の下位2ビットのうちの左ビットの値が「0」であるため、特定部303は、解析を終了する(ステップS303で、B=0)。

【0183】

(ステップ11) 特定部303は、これまでに解析したNRPのうち、オール「1」でないNRPの数をカウントする。なお、最後にチェックしたNRPはカウントしない。カウントした値が「1」であるため、暗号化メディア鍵の位置は、鍵情報内において、1番目である。

20

(ステップ12) 図30より、鍵情報の1番目の位置に格納されている暗号化メディア鍵は、E1(KeyL, メディア鍵)である。

【0184】

ユーザ装置10は、KeyLを保持している。よって、ユーザ装置10は、KeyLを用いて暗号化メディア鍵を復号してメディア鍵を獲得することができる。

#### 4. 第4の実施の形態

上記の第1の実施の形態においては、複数のNRPを上位レイヤから下位レイヤの順に並べ、レイヤが同じNRPについては、左から右への順に並べるようにしている。

30

【0185】

次に述べる第4の実施の形態では、別の並べ方により複数のNRPを出力する著作物保護システム10d(図示していない)について説明する。

#### 4.1 著作物保護システム10dの構成

著作物保護システム10dは、著作物保護システム10と同様の構成を有している。ここでは、著作物保護システム10との相違点を中心として説明する。

【0186】

#### 4.1.1 鍵管理装置100

著作物保護システム10dの鍵管理装置100は、第1の実施の形態において述べた鍵管理装置100と同様の構成を有している。ここでは、その相違点を中心として説明する。

40

#### (1) 木構造格納部102

木構造格納部102は、具体的にはハードディスクユニットから構成されており、図37に一例として示すように木構造テーブルD1000を有している。

【0187】

木構造テーブルD1000は、図36に一例として示す木構造T600に対応しており、木構造T600を表現するためのデータ構造を示す。後述するように、木構造構築部101により木構造T600を表現するためのデータ構造が、木構造テーブルD1000として生成され、木構造格納部102に書き込まれる。

#### (木構造T600)

木構造T600は、図36に示すように、木構造T100と同様に、レイヤ0からレイヤ

50

4 までの 5 階層からなる 2 分木である。

#### 【 0 1 8 8 】

木構造 T 6 0 0 の各レイヤに含まれるノードの数は、木構造 T 1 0 0 と同じである。また、上位側のノードと下位側のノードを接続する経路に割り当てられる番号も、木構造 T 1 0 0 と同じである。木構造 T 6 0 0 において、× が付されているノードは、無効化されている。

木構造 T 6 0 0 のルートであるノードのノード名は、空白である。他のノードのノード名は、木構造 T 1 0 0 と同様に設定される。

#### 【 0 1 8 9 】

各ノード名は、4 桁の文字で表現される。ルートであるノードのノード名は、4 桁の空白文字からなる。ノード名「0」は、具体的には、文字「0」+ 1 桁の空白文字 + 1 桁の空白文字 + 1 桁の空白文字である。ノード名「00」は、文字「0」+ 文字「0」+ 1 桁の空白文字 + 1 桁の空白文字である。ノード名「101」は、文字「1」+ 文字「0」+ 文字「1」+ 1 桁の空白文字である。ノード名「1111」は、文字「1」+ 文字「1」+ 文字「1」+ 文字「1」である。その他のノード名についても同様である。

#### 【 0 1 9 0 】

木構造 T 6 0 0 において、各ノードの付近に付された { 1 0 } などは、N R P を示している。また、各ノードの付近に付された 印で囲まれた番号は、N R P が出力される順序を示している。

( 木構造テーブル D 1 0 0 0 )

木構造テーブル D 1 0 0 0 は、木構造 T 6 0 0 に含まれるノードと同じ数のノード情報を含んで構成されており、各ノード情報は、木構造 T 6 0 0 を構成する各ノードにそれぞれ対応している。

#### 【 0 1 9 1 】

各ノード情報は、ノード名、デバイス鍵及び無効化フラグを含んでいる。ノード名、デバイス鍵及び無効化フラグについては、木構造テーブル D 1 0 0 と同じであるので説明を省略する。

木構造テーブル D 1 0 0 0 内には、次に示す順序規則 2 に従った順序により各ノード情報が記憶される。ここに示す順序規則 2 は、記録装置 3 0 0 a、3 0 0 b、3 0 0 c、・・・、再生装置 4 0 0 a、4 0 0 b、4 0 0 c、・・・により、木構造テーブル D 1 0 0 0 から各ノード情報がシーケンシャルに読み出される場合においても適用される。

#### 【 0 1 9 2 】

( a ) 木構造テーブル D 1 0 0 0 内の先頭には、ルートであるノードに対応するノード情報が記憶される。

( b ) 1 個のノード ( 特定ノードと呼ぶ。 ) に対応するノード情報が木構造テーブル D 1 0 0 0 内に記憶された後において、前記特定ノードの下位側に接続する 2 個の下位ノードが存在する場合には、次に示すようにして、ノード情報が並べられる。前記特定ノードに対応するノード情報に続いて、前記 2 個の下位ノードのうち、左側のノード及び前記左側のノードのさらに下位側に接続する全てのノードに対応する各ノード情報が記憶される。続いて、前記 2 個の下位ノードのうち、右側のノード及び前記右側のノードのさらに下位側に接続する全てのノードに対応する各ノード情報が記憶される。

#### 【 0 1 9 3 】

( c ) ( b ) 内において、( b ) が再度、適用される。

具体的には、図 3 7 に示す木構造テーブル D 1 0 0 内には、次に示す順序により各ノード情報が記憶される。

空白 ( ルートを示す )、 「 0 」、 「 0 0 」、 「 0 0 0 」、 「 0 0 0 0 」、 「 0 0 0 1 」、 「 0 0 1 」、 「 0 0 1 0 」、 「 0 0 1 1 」、 「 0 1 」、 「 0 1 0 」、 ・・・、 「 1 1 」、 「 1 1 0 」、 「 1 1 0 0 」、 「 1 1 0 1 」、 「 1 1 1 」、 「 1 1 1 0 」、 「 1 1 1 1 」

( 2 ) 木構造構築部 1 0 1

木構造構築部 1 0 1 は、デバイス鍵を管理するための n 分木データ構造を構築し、木構造

10

20

30

40

50

格納部 102 に構築した木構造を格納する。ここで、 $n$  は 2 以上の整数であり、一例として、 $n = 2$  である。

#### 【0194】

木構造構築部 101 による木構造の構築及び木構造格納部 102 への格納の詳細の動作については、後述する。

木構造構築部 101 は、次に、木構造のノード毎に乱数を用いてデバイス鍵を生成し、生成したデバイス鍵を各ノードに対応付けて木構造テーブル内に書き込む。

#### 【0195】

##### (3) 鍵情報ヘッダ生成部 106

鍵情報ヘッダ生成部 106 は、複数の NRP を生成し、生成した複数の NRP をヘッダ情報として、鍵情報記録装置 200 へ出力する。NRP の生成の詳細の動作については、後述する。

鍵情報ヘッダ生成部 106 により生成されるヘッダ情報の一例を図 38 に示す。この図に示すヘッダ情報 D900 は、NRP {11}、{11}、{11}、{10}、{01}、{11}、{10}、{10}、{10}、{01}、{11} から構成され、各 NRP をこの順序で含んでいる。

#### 【0196】

なお、これらの複数の NRP のそれぞれは、ヘッダ情報 D900 内において格納されている位置が定められている。この図に示すように、ヘッダ情報 D900 内に「0」、「1」、「2」、「3」、「4」、「5」、「6」、「7」、「8」、「9」、「10」、により定まる位置において、それぞれ、NRP {11}、{11}、{11}、{10}、{01}、{11}、{10}、{10}、{10}、{01}、{11} が配置されている。

#### 【0197】

##### (4) 鍵情報生成部 107

鍵情報生成部 107 は、上記の木構造テーブルにノード情報が格納される順序と同じ順序で、無効化されていないノードに対応するデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成し、生成した暗号化メディア鍵を鍵情報として出力する。

#### 【0198】

鍵情報生成部 107 は、一例として次に示す鍵情報を生成して出力する。

鍵情報は、デバイス鍵「IK2」、「IK3」、「IK6」、「IK8」、「KeyL」及び「KeyG」をそれぞれ用いて、メディア鍵を暗号化することにより、生成された暗号化メディア鍵 E1 (IK2、メディア鍵)、E1 (IK3、メディア鍵)、E1 (IK6、メディア鍵)、E1 (IK8、メディア鍵)、E1 (KeyL、メディア鍵) 及び E1 (KeyG、メディア鍵) から構成されている。この鍵情報内に、「0」、「1」、「2」、「3」、「4」、「5」及び「6」により定まる位置において、それぞれ、暗号化メディア鍵 E1 (IK2、メディア鍵)、E1 (IK3、メディア鍵)、E1 (IK6、メディア鍵)、E1 (IK8、メディア鍵)、E1 (KeyL、メディア鍵) 及び E1 (KeyG、メディア鍵) が配置されている。

#### 【0199】

##### 4.1.2 記録装置 300a

著作物保護システム 10d の記録装置 300a は、第 1 の実施の形態において述べた記録装置 300a と同様の構成を有している。ここでは、その相違点を中心として説明する。

##### (1) 特定部 303

特定部 303 は、ID 情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から 1 個の暗号化メディア鍵が存在する位置 X を特定する。なお、暗号化メディア鍵が存在する位置 X を特定する場合の詳細の動作については、後述する。

#### 【0200】

##### 4.2 著作物保護システム 10d の動作



著作物保護システム 10 d の動作について、著作物保護システム 10 の動作との相違点を中心として説明する。

#### 4.2.1 木構造を構築して格納する動作

ここでは、木構造構築部 101 による木構造テーブルの生成と木構造格納部 102 への木構造テーブルの書き込みの動作について、図 39 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 10 に示すフローチャートにおけるステップ S101 の詳細である。

##### 【0201】

木構造構築部 101 は、空白のノード名を含むノード情報を生成して木構造テーブルに書き込む（ステップ S401）。

10

次に、木構造構築部 101 は、レイヤ  $i$  ( $i = 1, 2, 3, 4$ ) について、次に示すステップ S403 ~ ステップ S404 を繰り返す。

木構造構築部 101 は、 $2^i$  個の文字列をノード名として生成する。具体的には、 $i = 1$  のときは、 $2^1 = 2$  個の文字列「0」及び「1」を生成する。また、 $i = 2$  のときは、 $2^2 = 4$  個の文字列「00」、「01」、「10」及び「11」を生成する。また、 $i = 3$  のときは、 $2^3 = 8$  個の文字列「000」、「001」、「010」、・・・、「111」を生成する。また、 $i = 4$  のときは、 $2^4 = 16$  個の文字列「0000」、「0001」、「0010」、「0011」、・・・、「1111」を生成する（ステップ S403）。次に、木構造構築部 101 は、生成した各ノード名をそれぞれ含むノード情報を木構造テーブルに書き込む（ステップ S404）。

20

##### 【0202】

次に、木構造構築部 101 は、木構造テーブルに含まれている各ノード情報を、ノード名の昇順に並び換え、並び替えられた各ノード情報を再度、木構造テーブルに上書きする（ステップ S406）。

このようにして、図 37 に一例として示す木構造テーブル D1000 が生成される。生成された木構造テーブル D1000 は、上述した順序規則 2 により各ノード情報を含んでいる。なお、この段階では、木構造テーブル D1000 内に各デバイス鍵はまだ記録されていない。

##### 【0203】

#### 4.2.2 ヘッド情報の生成の動作

30

ここでは、鍵情報ヘッダ生成部 106 によるヘッド情報の生成の動作について、図 40 ~ 図 41 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 11 に示すフローチャートにおけるステップ S153 の詳細である。

##### 【0204】

鍵情報ヘッダ生成部 106 は、順序規則 2 に従って木構造テーブルから順に 1 個ずつノード情報の読出しを試みる（ステップ S421）。

ノード情報の終了を検出すると（ステップ S422）、鍵情報ヘッダ生成部 106 は、ステップ S427 へ制御を移す。

ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップ S422）、鍵情報ヘッダ生成部 106 は、読み出したノード情報に対応する対象ノードの下位側に接続されている 2 個の下位ノードに対応する 2 個のノード情報を読み出す（ステップ S423）。

40

##### 【0205】

下位ノードが存在する場合に（ステップ S424）、鍵情報ヘッダ生成部 106 は、読み出した 2 個の下位ノードに対応する 2 個のノード情報の両方に、無効化フラグが付されているか否かを調べて、NRP を生成し（ステップ S425）、次に、生成した NRP を読み出した対象ノードに対応するノード情報に付加する（ステップ S426）。次に、ステップ S421 へ戻って処理を繰り返す。

##### 【0206】

下位ノードが存在しない場合（ステップ S424）、ステップ S421 へ戻って処理を繰

50

り返す。

次に、鍵情報ヘッダ生成部 106 は、順序規則 2 に従って木構造テーブルから順に 1 個ずつノード情報の読出しを試みる（ステップ S 427）。

ノード情報の終了を検出すると（ステップ S 422）、鍵情報ヘッダ生成部 106 は、処理を終了する。

【0207】

ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップ S 428）、鍵情報ヘッダ生成部 106 は、読み出したノード情報に NRP が付加されているか否かを調べ、付加されている場合（ステップ S 429）、付加されている NRP を出力し（ステップ S 430）、次に、ステップ S 427 へ戻って処理を繰り返す。

10

【0208】

NRP が付加されていない場合（ステップ S 429）、鍵情報ヘッダ生成部 106 は、ステップ S 427 へ戻って処理を繰り返す。

4.2.3 鍵情報の特定の動作

ここでは、記録装置 300a が有する特定部 303 により、記録媒体 500b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作について、図 42 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 11 に示すフローチャートにおけるステップ S 172 の詳細である。

【0209】

また、再生装置 400a が有する特定部 402 による動作は、特定部 303 による動作と同じであるので、説明を省略する。

20

特定部 303 は、チェックする ID 情報のビット位置を示す変数  $i$ 、現在チェックしている NRP が含まれるレイヤを示す変数  $L$ 、分岐点のノードのレイヤを記憶する変数  $X$ 、NRP をチェックするか否かを判断するフラグ  $F$ （初期値、 $F = 0$ ）を有しており、木構造のレイヤ数を示す値  $D$  を有している。また、チェックする NRP の位置を示すポインタ  $A$  を有している。

【0210】

特定部 303 は、変数  $i = 0$ 、変数  $L = 0$ 、フラグ  $F = 0$ 、変数  $X = 0$ 、ポインタ  $A = 0$  とする（ステップ S 1300）。

次に、特定部 303 は、変数  $L$  がレイヤ数  $D - 1$  よりも小さいか否かを判定する。大きい場合又は等しい場合（ステップ S 1301）、特定部 303 は、変数  $L$  に対して、変数  $X$  の最後のレイヤ番号を入力する。変数  $X$  は、後入れ先出しの変数であり、出力した値は削除されるものとする。即ち、変数  $X$  にレイヤ 0、レイヤ 2、レイヤ 3 の順で入力されたとすると、最初に出力されるのはレイヤ 3 で、そのレイヤ 3 は削除され、次はレイヤ 2 が出力される（ステップ S 1313）。次に、ステップ S 1301 へ戻って処理を繰り返す。

30

【0211】

変数  $L$  がレイヤ数  $D - 1$  よりも小さい場合（ステップ S 1301）、特定部 303 は、変数  $i =$  変数  $L$  であるか否かを判定する。変数  $i =$  変数  $L$  でない場合（ステップ S 1302）、特定部 303 は、ステップ S 1310 へ制御を移す。

変数  $i =$  変数  $L$  である場合（ステップ S 1302）、特定部 303 は、さらに、フラグ  $F = 0$  であるか否かを判定する。フラグ  $F = 0$  でない場合（ステップ S 1303）、特定部 303 は、フラグ  $F = 0$  とし（ステップ S 1309）、特定部 303 は、ステップ S 1310 へ制御を移す。

40

【0212】

フラグ  $F = 0$  である場合（ステップ S 1303）、特定部 303 は、ID 情報の上位  $i$  ビット目の値に従って、 $A$  番目の NRP の対応するビット位置の値  $B$  をチェックし、変数  $i = i + 1$  とする（ステップ S 1304）。

次に、特定部 303 は、値  $B = 1$  であるか否かを調べ、値  $B = 1$  でない場合（ステップ S 1305）、この ID 情報が割り当てられた装置は無効化されていないものとして、特定部 303 は、処理を終了する。

50

## 【0213】

値  $B = 1$  である場合 (ステップ S 1305)、変数  $D - 1$  であるか否かを調べ、変数  $D - 1$  でない場合 (ステップ S 1306)、この ID 情報が割り当てられた装置は無効化されているものとして、特定部 303 は、処理を終了する。次に、変数  $D - 1$  である場合 (ステップ S 1306)、特定部 303 は、NRP が { 11 } であり、かつ ID 情報の  $i - 1$  番目の値が「1」であるか否かを判定する。No の場合 (ステップ S 1307)、特定部 303 は、ステップ S 1310 へ制御を移す。

## 【0214】

Yes の場合 (ステップ S 1307)、特定部 303 は、フラグ  $F = 1$  とし (ステップ S 1308)、次に、 $L = L + 1$  とし (ステップ S 1310)、NRP が { 11 } であれば、そのレイヤ番号を変数  $X$  に記憶し (ステップ S 1311)、 $A = A + 1$  とし (ステップ S 1312)、次に、ステップ S 1310 へ戻って処理を繰り返す。

## 【0215】

## 5. 第 5 の実施の形態

上記の第 4 の実施の形態においては、複数の NRP を順序規則 2 により並べるようにしている。

次に述べる第 5 の実施の形態では、第 4 の実施の形態において述べた著作物保護システム 10d と同様に、順序規則 2 により並べて複数の NRP を出力し、かつ、第 2 の実施の形態において述べた著作物保護システム 10b と同様に、無効化された装置が木構造の中で特定のリーフに集中する場合に、ヘッダ情報のデータ量を少なく抑えることができる著作物保護システム 10e (図示していない) について説明する。

## 【0216】

## 5.1 著作物保護システム 10e の構成

著作物保護システム 10e は、著作物保護システム 10d と同様の構成を有している。ここでは、著作物保護システム 10d との相違点を中心として説明する。

## 5.1.1 鍵管理装置 100

著作物保護システム 10e の鍵管理装置 100 は、第 4 の実施の形態において述べた鍵管理装置 100d と同様の構成を有している。ここでは、その相違点を中心として説明する。

## 【0217】

## (1) 木構造格納部 102

木構造格納部 102 は、木構造テーブルを有している。木構造格納部 102 が有する木構造テーブルは、第 4 の実施の形態において説明した木構造格納部 102 が有している木構造テーブル D 1000 と同様の構成を備えており、木構造テーブルに含まれる各ノード情報は、さらに、NRP を含む。

## 【0218】

## (2) 鍵情報ヘッダ生成部 106

鍵情報ヘッダ生成部 106 は、複数の NRP を生成し、生成した複数の NRP をヘッダ情報として、鍵情報記録装置 200 へ出力する。各 NRP は、第 2 の実施の形態において説明したように、3 ビットから構成される。

NRP の生成の詳細の動作については、後述する。

## 【0219】

## 5.1.2 記録装置 300a

著作物保護システム 10e の記録装置 300a は、第 4 の実施の形態において述べた記録装置 300a と同様の構成を有している。ここでは、その相違点を中心として説明する。

## (1) 特定部 303

特定部 303 は、ID 情報及びヘッダ情報を用いて、ヘッダ情報を上位からシーケンシャルに調べていくことにより、鍵情報の中から 1 個の暗号化メディア鍵が存在する位置  $X$  を特定する。なお、暗号化メディア鍵が存在する位置  $X$  を特定する場合の詳細の動作については、後述する。

## 【 0 2 2 0 】

## 5 . 2 著作物保護システム 1 0 e の動作

著作物保護システム 1 0 e の動作について、著作物保護システム 1 0 d の動作との相違点を中心として説明する。

## 5 . 2 . 1 ヘッダ情報の生成の動作

ここでは、鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作について、図 4 3 ~ 図 4 6 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 1 に示すフローチャートにおけるステップ S 1 5 3 の詳細である。

## 【 0 2 2 1 】

鍵情報ヘッダ生成部 1 0 6 は、順序規則 2 に従って木構造テーブルから順に 1 個ずつノード情報の読出しを試みる（ステップ S 4 5 1 ）。

ノード情報の終了を検出すると（ステップ S 4 5 2 ）、鍵情報ヘッダ生成部 1 0 6 は、ステップ S 4 5 8 へ制御を移す。

ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップ S 4 5 2 ）、鍵情報ヘッダ生成部 1 0 6 は、読み出したノード情報に対応する対象ノードの下位側に接続されている 2 個の下位ノードに対応する 2 個のノード情報を読み出す（ステップ S 4 5 3 ）。

## 【 0 2 2 2 】

下位ノードが存在する場合に（ステップ S 4 5 4 ）、鍵情報ヘッダ生成部 1 0 6 は、読み出した 2 個の下位ノードに対応する 2 個のノード情報の両方に、無効化フラグが付されているか否かを調べて、N R P を生成し（ステップ S 4 5 5 ）、値「 0 」を有する拡張ビットを生成した N R P の先頭に付加し（ステップ S 4 5 6 ）、次に、拡張ビットの付加された N R P を読み出した対象ノードに対応するノード情報に付加する（ステップ S 4 5 7 ）。

次に、ステップ S 4 5 1 へ戻って処理を繰り返す。

## 【 0 2 2 3 】

下位ノードが存在しない場合（ステップ S 4 5 4 ）、ステップ S 4 5 1 へ戻って処理を繰り返す。

次に、鍵情報ヘッダ生成部 1 0 6 は、順序規則 2 に従って木構造テーブルから順に 1 個ずつノード情報の読出しを試みる（ステップ S 4 5 8 ）。

ノード情報の終了を検出すると（ステップ S 4 5 9 ）、鍵情報ヘッダ生成部 1 0 6 は、ステップ S 4 6 5 へ制御を移す。

## 【 0 2 2 4 】

ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップ S 4 5 9 ）、鍵情報ヘッダ生成部 1 0 6 は、読み出したノード情報に対応する対象ノードの下位側に接続されている全ての下位ノードに対応する全てのノード情報を読み出す（ステップ S 4 6 0 ）。

下位ノードが存在する場合に（ステップ S 4 6 1 ）、鍵情報ヘッダ生成部 1 0 6 は、読み出した全ての下位ノードに対応する全てのノード情報に、無効化フラグが付されているか否かを調べ（ステップ S 4 6 2 ）、全てのノード情報に付加されている場合にのみ（ステップ S 4 6 3 ）、対象ノードに対応するノード情報に付加された N R P の先頭ビットを「 1 」に書き換える（ステップ S 4 6 4 ）。

## 【 0 2 2 5 】

次に、ステップ S 4 5 8 へ戻って処理を繰り返す。

下位ノードが存在しない場合（ステップ S 4 6 1 ）、ステップ S 4 5 8 へ戻って処理を繰り返す。

次に、鍵情報ヘッダ生成部 1 0 6 は、順序規則 2 に従って木構造テーブルから順に 1 個ずつノード情報の読出しを試みる（ステップ S 4 6 5 ）。

## 【 0 2 2 6 】

ノード情報の終了を検出すると（ステップ S 4 6 6 ）、鍵情報ヘッダ生成部 1 0 6 は、ステップ S 4 7 2 へ制御を移す。

10

20

30

40

50

ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップS 4 6 6）、鍵情報ヘッダ生成部 1 0 6 は、読み出したノード情報に対応する対象ノードの下位側に接続されている全ての下位ノードに対応する全てのノード情報を読み出す（ステップS 4 6 7）。

【0 2 2 7】

下位ノードが存在する場合に（ステップS 4 6 8）、鍵情報ヘッダ生成部 1 0 6 は、読み出した全ての下位ノードに対応する全てのノード情報に、それぞれN R P { 1 1 1 } が付加されているか否かを調べ（ステップS 4 6 9）、全てのノード情報に付加されている場合にのみ（ステップS 4 7 0）、前記全てのノード情報に、それぞれ削除フラグを付加する（ステップS 4 7 1）。

10

【0 2 2 8】

次に、ステップS 4 6 5 へ戻って処理を繰り返す。

下位ノードが存在しない場合（ステップS 4 6 8）、ステップS 4 6 5 へ戻って処理を繰り返す。

次に、鍵情報ヘッダ生成部 1 0 6 は、順序規則 2 に従って木構造テーブルから順に 1 個ずつノード情報の読出しを試みる（ステップS 4 7 2）。

【0 2 2 9】

ノード情報の終了を検出すると（ステップS 4 7 3）、鍵情報ヘッダ生成部 1 0 6 は、処理を終了する。

ノード情報の終了を検出せず、ノード情報が読み出せた場合には（ステップS 4 7 3）、鍵情報ヘッダ生成部 1 0 6 は、読み出したノード情報にN R P が付加されているか否かを調べ、付加されている場合（ステップS 4 7 4）、さらに、削除フラグが付加されているか否かを調べ、削除フラグが付加されていない場合には（ステップS 4 7 5）、付加されているN R P を出力し（ステップS 4 7 6）、次に、ステップS 4 7 2 へ戻って処理を繰り返す。

20

【0 2 3 0】

N R P が付加されていない場合（ステップS 4 7 4）、又は、削除フラグが付加されている場合（ステップS 4 7 5）、鍵情報ヘッダ生成部 1 0 6 は、ステップS 4 7 2 へ戻って処理を繰り返す。

5 . 2 . 2 鍵情報の特定の動作

30

ここでは、記録装置 3 0 0 a が有する特定部 3 0 3 により、記録媒体 5 0 0 b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作について、図 4 7 に示すフローチャートを用いて説明する。なお、ここで説明する動作は、図 1 1 に示すフローチャートにおけるステップS 1 7 2 の詳細である。

【0 2 3 1】

また、再生装置 4 0 0 a が有する特定部 4 0 2 による動作は、特定部 3 0 3 による動作と同じであるので、説明を省略する。

また、ここでは、図 4 2 に示すフローチャートとの相違点を中心として説明する。

特定部 3 0 3 は、第 4 の実施の形態の場合と同様に、チェックする I D 情報のビット位置を示す変数  $i$ 、現在チェックしているN R P が含まれるレイヤを示す変数  $L$ 、分岐点のノードのレイヤを記憶する変数  $X$ 、N R P をチェックするか否かを判断するフラグ  $F$ （初期値、 $F = 0$ ）を有しており、木構造のレイヤ数を示す値  $D$  を有している。また、チェックするN R P の位置を示すポインタ  $A$  を有している。

40

【0 2 3 2】

値  $B = 1$  である場合（ステップS 1 3 0 5）、N R P の最上位ビットが「1」であるときにのみ（ステップS 1 3 1 6）、特定部 3 0 3 は、変数  $i = D - 1$  とし、変数  $L = D - 1$  とする（ステップS 1 3 1 7）。

また、特定部 3 0 3 は、N R P が { 1 1 } であり、かつN R P の最上位ビットが「1」でないとき、そのレイヤ番号を変数  $X$  に記憶する（ステップS 1 3 1 1）。

【0 2 3 3】

50

## 6. 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) 本発明の実施の形態として、従来方式による無効化方法を例として説明したが、本発明は上記の実施の形態に限定されるものではない。鍵管理装置がある木構造を保持し、この木構造のリーフに記録装置又は再生装置を割り当て、ノードに付随するあるデバイス鍵を各記録装置又は各再生装置に割り当てるものであり、鍵管理装置がこの木構造を用いて前記デバイス鍵の無効化と、前記鍵情報の作成を行うものであれば、前記ノードに付随するデバイス鍵の割り当て方や、各装置へのデバイス鍵の割り当て方はどのようなものであってもよい。

10

### 【0234】

(2) また、本発明の実施の形態として、2分木の木構造を例として説明したが、本発明は2分木に限定されるものではない。一般にn分木でも実現可能である。このときID情報は、あるノードから下に派生するn本の経路に対して、0~n-1を割り当て、上述した実施の形態と同様に、リーフからルートに至るまでの経路上に割り当てられた値を上位から順に連結することにより、設定される。

### 【0235】

(3) 以上で述べた本発明の実施の形態においては、DVD-RAM等のレコーダブルメディアについて説明した。しかし、DVD-Video等のプレレコーディッドメディアについても、同様の方法で実現することができる。

20

プレレコーディッドメディアにおける著作物保護システム10fについて、説明する。

### 【0236】

著作物保護システム10fは、図48に示すように、鍵管理装置100、データ記録装置1701、データ再生装置1703a、1703b、1703c、・・・から構成されている。

鍵管理装置100は、上記の実施の形態において説明したように、ヘッダ情報が付加された鍵情報とコンテンツ鍵とをデータ記録装置1701へ出力し、複数のデバイス鍵と各デバイス鍵識別情報とID情報とをデータ再生装置1703a、1703b、1703c、・・・へ出力する。

### 【0237】

30

データ記録装置1701に、プレレコーディッドメディアである記録媒体500aが装着される。データ記録装置1701は、鍵管理装置100から鍵情報とメディア鍵とを受け取り、メディア鍵を用いてコンテンツを暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツと受け取った鍵情報とを記録媒体500aに書き込む。こうして、暗号化コンテンツと鍵情報とが書き込まれた記録媒体500dが生産される。

### 【0238】

記録媒体500dは、市場を流通し、利用者は、記録媒体500dを入手する。利用者は、記録媒体500dをデータ再生装置1703aに装着する。

データ再生装置1703aは、鍵管理装置100から複数のデバイス鍵と各デバイス鍵識別情報とID情報とを予め受け取っており、記録媒体500dが装着されると、記録媒体500dから鍵情報と暗号化コンテンツとを読み出し、鍵情報から暗号化メディア鍵を特定し、特定した暗号化メディア鍵をデバイス鍵を用いて復号し、得られたメディア鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成する。

40

### 【0239】

このようなシステムにおいても、実施の形態で示した鍵管理装置100と同様の動作により、記録媒体に記録するヘッダ情報を少なく抑えつつ、各データ再生装置で効率よく復号すべき暗号化メディア鍵を特定することができる。

(4) 以上では本発明をデジタルコンテンツの著作権保護のために用いる場合を例示したが、本発明の応用はこれに限定されるものではなく、例えば、会員制の情報提供システムにおいて、ある特定の会員以外に情報を提供するという、いわゆるコンディショナルアク

50

セスの目的にも利用できる。

【0240】

(5) 本発明の実施の形態においては、鍵情報あるいは暗号化コンテンツを、記録媒体を用いて配布する例を示したが、記録媒体の代わりに、インターネットに代表されるような通信媒体を用いてもよい。

(6) 鍵管理装置と鍵情報記録装置が一体の装置から構成されているとしてもよい。

【0241】

(7) 上記の実施の形態では、 $n$ 分木を構成する全てのノードに予めデバイス鍵を割り当てておき、リーフからルートへの経路上に存在する全てのデバイス鍵を、前記リーフに対応する利用装置に割り当てるとしているが、本発明は、このようなデバイス鍵の割り当て方法には、限定されない。

$n$ 分木を構成する全てのノードに予めデバイス鍵を割り当てておくのではなく、一部のノードにのみ、予めデバイス鍵を割り当てておくとしてもよい。

【0242】

また、リーフからルートへの経路上に存在する全てのデバイス鍵を、前記リーフに対応する利用装置に割り当ててのではなく、リーフからルートへの経路上に存在する全てのデバイス鍵のうちの一部のデバイス鍵を前記利用装置に割り当てるとしてもよい。

(8) 一例として図4に示す木構造を想定する。デバイス鍵が漏洩していない初期状態では、メディア鍵は、デバイス鍵  $Key A$  を用いて暗号化され、暗号化メディア鍵が生成される。

【0243】

このとき、ユーザ装置1～16のいずれかの装置が、悪意のある第三者によりハックされて、デバイス鍵  $Key A$  が暴露され、デバイス鍵  $Key A$  だけを内部に有するクローン機器が製造されたとする。このとき、前記クローン機器は、デバイス鍵  $Key A$  だけを有するので、ユーザ装置1～16のうちのどの装置がハックされた装置であるかを特定することはできない。一方で、前記クローン機器は、デバイス鍵  $Key A$  を有しているので、正しいメディア鍵を不正に得ることができる。

【0244】

このような状況では、デバイス鍵  $Key A$  のみを無効化し、かつ、全ての機器がカバーされるようなデバイス鍵を用いて、言い換えると、全ての機器が共有しているデバイス鍵を用いて、メディア鍵を暗号化しなければならない。ここで、全ての機器をカバーする理由は、このような状況では、ハックされた機器がどの機器か断定できないためである。

【0245】

そこで、デバイス鍵  $Key B$  及び  $Key C$  をそれぞれ用いて、メディア鍵を暗号化して2個の暗号化メディア鍵を生成する。

次に、デバイス鍵  $Key B$  が暴露された場合には、デバイス鍵  $Key B$  を無効化し、さらに、デバイス鍵  $Key C$ 、 $Key D$  及び  $Key E$  をそれぞれ用いて、メディア鍵を暗号化して3個の暗号化メディア鍵を生成する。

【0246】

このような操作が、木の高さ分だけ繰り返されると、最終的には、ハックされた機器が特定される。

以上説明したような状況に対応するために、デバイス鍵  $Key A$  のみを無効化する場合、鍵管理装置は、デバイス鍵  $Key A$  が対応するノードに対して、 $NRP\{100\}$  を付加する。図4に示す木構造の場合には、ルートに対して、 $NRP\{100\}$  を付加する。

【0247】

$NRP\{100\}$  の先頭のビット「1」は、このノードが無効化されていることを示し、また、先頭のビット「1」に続くビット列「00」は、このノードの下に接続されている2個のノードは、両方とも、無効化されていないことを示している。

つまり、図4に示す木構造の場合に、ルートに対して、 $NRP\{100\}$  が付加されているならば、デバイス鍵  $Key B$  及び  $Key C$  を用いて、メディア鍵を暗号化して生成され

10

20

30

40

50

た2個の暗号化メディア鍵が存在することとなる。このように、NRPの先頭のビット「1」は、このノードの下には、暗号化メディア鍵が2個存在することを意味するフラグであるといえる。

#### 【0248】

一方、第2の実施の形態で説明したように、NRPが{111}であるときの先頭のビット「1」は、このノードの下には、NRPが存在しないことを示している。

以下において、さらに詳細に説明する。

#### (鍵管理装置100)

ここでは、鍵管理装置100は、図4に示す木構造T100を生成し、この図に示すように、各ノードにデバイス鍵を割り当て、各リーフにユーザ装置を割り当てたものとする。

10

#### 【0249】

この後、図49に示すように、ルートT701、ノードT702及びノードT703にそれぞれ割り当てられたデバイス鍵Key A、Key B及びKey Eが、上記に示すように漏洩したため、鍵管理装置100は、以下に示すようにして、デバイス鍵Key A、Key B及びKey Eを無効化し、ヘッダ情報及び鍵情報を生成し、生成したヘッダ情報及び鍵情報を、鍵情報記録装置200を介して、記録媒体に書き込む。

#### 【0250】

##### (a) デバイス鍵Key A、Key B及びKey Eの無効化

鍵管理装置100は、木構造テーブルにおいて、デバイス鍵Key A、Key B及びKey Eがそれぞれ含まれるノード情報に無効化フラグ「1」を付加する。

20

##### (b) ヘッダ情報の生成

鍵管理装置100は、無効化フラグが付加されたノード情報を含む前記木構造テーブルを用いて、ルートT701に付加するNRP{010}を生成し、生成したNRP{010}をヘッダ情報の一部として、鍵情報記録装置200を介して、記録媒体に書き込む。ここで、NRPの先頭のビット「0」は、ルートT701の直下に接続される2個の下位のノードのいずれか一方が無効化され、他方は無効化されていないことを示している。また、NRPの下位の2ビット「10」は、上記の実施の形態においても説明したように、ルートT701の直下に接続される2個の下位のノードのうち、左側のノードT702は、無効化されており、右側のノードT704は、無効化されていないことを示している。

#### 【0251】

30

次に、鍵管理装置100は、ノードT702に付加するNRP{001}を生成し、生成したNRP{001}をヘッダ情報の一部として、鍵情報記録装置200を介して、記録媒体に書き込む。ここで、NRPの先頭のビット「0」は、ノードT702の直下に接続される2個の下位のノードのいずれか一方が無効化され、他方は無効化されていないことを示している。また、NRPの下位の2ビット「01」は、ノードT702の直下に接続される2個の下位のノードのうち、左側のノードT705は、無効化されておらず、右側のノードT703は、無効化されていることを示している。

#### 【0252】

次に、鍵管理装置100は、ノードT703に付加するNRP{100}を生成し、生成したNRP{100}をヘッダ情報の一部として、鍵情報記録装置200を介して、記録媒体に書き込む。NRP{100}は、上記において説明したように、ノードT703の直下に接続される2個の下位のノードT706、T707の両方とも無効化されておらず、これら2個のノードT706、T707には、それぞれ暗号化メディア鍵が存在することを示している。

40

#### 【0253】

このようにして、図50に示すヘッダ情報D1000が記録媒体に書き込まれる。ヘッダ情報D1000は、この図に示すように、NRP{010}、{001}、{100}をこの順序で含んで構成されている。

##### (c) 鍵情報の生成

次に、鍵管理装置100は、以下に示すようにして、無効化されていないデバイス鍵のう

50



ちの一部のデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成し、生成した暗号化メディア鍵を含む鍵情報とNRPを含むヘッダ情報とを、鍵情報記録装置200を介して、記録媒体に書き込む。

【0254】

最初に、鍵管理装置100は、無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成する。ここで、図49に示すように、無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵は、ノードT704に割り当てられたデバイス鍵KeyCであるので、鍵管理装置100は、デバイス鍵KeyCを用いて、メディア鍵を暗号化して、暗号化メディア鍵E1(KeyC、メディア鍵)を生成し、生成した暗号化メディア鍵E1(KeyC、メディア鍵)を、鍵情報記録装置200を介して、記録媒体に書き込む。

10

【0255】

次に、鍵管理装置100は、上記のデバイス鍵KeyCが割り当てられたノードT704及びノードT704の下位側の全てのノードを除く他のノードについて、これらの他のノードに割り当てられた無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成する。ここで、該当するノードは、ノードT705であるので、鍵管理装置100は、ノードT705に割り当てられたデバイス鍵KeyDを用いて、メディア鍵を暗号化して、暗号化メディア鍵E1(KeyD、メディア鍵)を生成し、生成した暗号化メディア鍵E1(KeyD、メディア鍵)を、鍵情報記録装置200を介して、記録媒体に書き込む。

20

【0256】

次に、鍵管理装置100は、上記のデバイス鍵KeyCが割り当てられたノードT704及びノードT704の下位側の全てのノード、及び上記のデバイス鍵KeyDが割り当てられたノードT705及びノードT705の下位側の全てのノードを除く他のノードについて、これらの他のノードに割り当てられた無効化されていないデバイス鍵のうち、最上位のレイヤに存在するノードに割り当てられているデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成する。ここで、該当するノードは、ノードT706であるので、鍵管理装置100は、ノードT706に割り当てられたデバイス鍵KeyJを用いて、メディア鍵を暗号化して、暗号化メディア鍵E1(KeyJ、メディア鍵)を生成し、生成した暗号化メディア鍵E1(KeyJ、メディア鍵)を、鍵情報記録装置200を介して、記録媒体に書き込む。

30

【0257】

次に、鍵管理装置100は、上記と同様にして、ノードt707に割り当てられたデバイス鍵KeyKを用いて、メディア鍵を暗号化して、暗号化メディア鍵E1(KeyK、メディア鍵)を生成し、生成した暗号化メディア鍵E1(KeyK、メディア鍵)を、鍵情報記録装置200を介して、記録媒体に書き込む。このようにして、図50に示す鍵情報D1010が記録媒体に書き込まれる。鍵情報D1010は、この図に示すように、暗号化メディア鍵E1(KeyC、メディア鍵)、E1(KeyD、メディア鍵)、E1(KeyJ、メディア鍵)及びE1(KeyK、メディア鍵)を、この順序で含んで構成されている。

40

【0258】

(記録装置300a)

次に、記録装置300aが有する特定部303により、上記のようにして記録媒体に記憶されたヘッダ情報及び鍵情報から、1個の暗号化メディア鍵を特定する動作について、図51に示すフローチャートを用いて説明する。

特定部303は、暗号化メディア鍵の位置を示す変数X、ユーザ装置自身に関する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、及び処理対象となるレイヤ数を示す変数iを有している。

50

## 【0259】

特定部303は、初期値として、それぞれ変数  $A = 0$ 、変数  $W = 1$ 、変数  $i = 0$  とする（ステップS301）。

次に、特定部303は、A番目のNRPの下位2ビットのうち、ID情報の上位  $i$  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S303）。ここで、対応するビット位置とは、上記の実施の形態においても説明したように、図4に示す木構造において左の経路に「0」、右の経路に「1」が割り当てられ、これらの規則に基づいてID情報が構成されているので、ID情報の上位  $i$  ビット目の値「0」は、A番目のNRPの下位2ビットのうちの左ビットに対応し、 $i$  ビット目の値「1」は、A番目のNRPの下位2ビットのうちの右ビットに対応する。

10

## 【0260】

次に、値  $B = 0$  の場合（ステップS303）、特定部303は、先頭のNRPから、最後にチェックしたNRPまでの各NRPについて、以下の通りチェックする。ただしA番目のNRPは含まない。

（a）NRPの最上位ビットが「0」であり、かつ下位2ビットが「11」でないとき、変数  $X$  に「1」を加算する。

## 【0261】

（b）NRPの最上位ビットが「1」であるとき、下位2ビットに含まれる「0」の数を、変数  $X$  に加算する。

最後にチェックしたA番目のNRPについては、NRPの最上位ビットが「1」であるときのみ、対応するビット位置までの「0」の数を変数  $X$  に加算する。ここで、対応するビット自身は含まないものとする。こうして得られた変数  $X$  が、暗号化メディア鍵の位置を示している。また、この時点の変数  $i$  は、デバイス鍵を識別するためのデバイス鍵識別情報である（ステップS307c）。次に、特定部303は、処理を終了する。

20

## 【0262】

一方、値  $B = 1$  の場合（ステップS303）、さらに、特定部303は、NRPの最上位ビットが「1」でないか否かを判断し、NRPの最上位ビットが「1」であると判断する場合には（ステップS308）、このユーザ装置は、無効化されているので、次に、特定部303は、処理を終了する。

NRPの最上位ビットが「1」でないと判断する場合に（ステップS308）、特定部303は、レイヤ  $i$  に存在する  $W$  個の全NRPの下位2ビットに含まれる「1」の数をカウントし、カウントした値を変数  $W$  に代入する。ただし、NRPの最上位ビットが「1」のNRPは、カウントの対象とはしない。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S304c）。

30

## 【0263】

次に、特定部303は、レイヤ  $i$  に存在するNRPのうちの最初のNRPから、対応するビット位置までの各NRPについて、NRPの下位2ビットに含まれる「1」の数をカウントし、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。また、NRPの最上位ビットが「1」であるNRPは、カウントの対象とはしない。こうして得られた変数  $A$  が、次のレイヤ  $i + 1$  のNRPのうち、ユーザ装置自身に

40

## 【0264】

次に、特定部303は、変数  $i = i + 1$  を演算し（ステップS306）、次にステップS303へ制御を移し、上述の処理を繰り返す。

以上に示すようにして、木構造のリーフからルートへの経路上に存在するデバイス鍵が無効化された場合に限らず、木構造の一部のノードに割り当てられたデバイス鍵が無効化された場合であっても、鍵管理装置によるヘッダ情報及び鍵情報の記録媒体への書込みと、再生装置による暗号化メディア鍵の特定とが行える。

## 【0265】

（9）一例として図4に示す木構造を想定し、デバイス鍵が全く漏洩していない初期状態

50

であり、前記木構造には無効化されたノードがないものとする。

この場合に、鍵管理装置は、ルートに対応付けられているデバイス鍵 *Key A* を用いて、メディア鍵を暗号化して 1 個の暗号化メディア鍵を生成する。次に、鍵管理装置は、前記木構造には無効化されたノードがなく、全てのノードが有効であることを示す特別な *NRP { 0 0 }* を 1 個生成する。次に、鍵管理装置は、生成した前記暗号化メディア鍵と生成した *NRP { 0 0 }* を、鍵情報記録装置を介して、記録媒体に書き込む。

【 0 2 6 6 】

また、この場合に、再生装置は、前記記録媒体から *NRP* を読み出し、読み出した *NRP* が *{ 0 0 }* のみであり、この他に *NRP* が前記記録媒体に記録されていないと判断する場合に、再生装置は、木構造において無効化されているノードが全く存在しないものと判断し、次に、前記記録媒体に記録されている前記暗号化メディア鍵を読み出し、再生装置自身が記憶しているデバイス鍵のうち、ルートに対応付けられているデバイス鍵 *Key A* を用いて、読み出した前記暗号化メディア鍵を復号して、メディア鍵を生成する。

10

【 0 2 6 7 】

また、この場合に、記録装置も、前記再生装置と同様に動作する。

( 1 0 ) 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*、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。

20

【 0 2 6 8 】

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。

30

【 0 2 6 9 】

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。

( 1 1 ) 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。

【 0 2 7 0 】

7. まとめ

以上の説明から明かなように、第 1 の実施の形態において開示した発明によると、予め記録媒体に記録される鍵情報のヘッダ情報として、*NRP* を水準順に並べることにより、鍵情報をコンパクトにでき、プレーヤが効率よく復号すべき暗号化メディア鍵を特定することもできる。

40

【 0 2 7 1 】

また、第 2 の実施の形態において開示した発明によると、ヘッダ情報として、あるノードの子孫が全て無効化装置であるか否かを示すビットを *NRP* の先頭に追加することで、無効化装置が集中した場合にヘッダ情報を少なくすることができる。

また、第 3 の実施の形態において開示した発明によると、ある特定のパターンで、あるノードの子孫が全て無効化装置であるか否かを判断することで、さらにヘッダ情報を少なく抑えることができる。

【 0 2 7 2 】

また、第 4 の実施の形態及び第 5 の実施の形態において開示した発明によると、*NRP* の

50

順序を、第 1 ～ 第 3 の実施の形態において開示した順序以外のものとすることができる。

#### 8. 産業上の利用の可能性

上記において説明した鍵管理装置及び利用者装置から構成される著作物保護システムは、音楽、映画、小説などのデジタル化された著作物を DVD などの記録媒体に格納して市場を流通させる場合において、コンテンツの不正な使用を防ぐための仕組みとして好適である。

##### 【0273】

##### 【発明の効果】

上記目的を達成するために本発明は、 $n$ 分木 ( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置と、1以上の利用者装置とからなる著作物保護システムであって、前記鍵管理装置は、デバイス鍵を各利用者装置に割り当て、各利用者装置は、割り当てられたデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号し、前記鍵管理装置は、 $n$ 分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備え、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備える。

##### 【0274】

この構成によると、鍵管理装置は、複数の暗号化メディア鍵及び複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、利用者装置は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から暗号化メディア鍵を特定するので、利用者装置は、自らに割り当てられた暗号化メディア鍵を効率良く決定することができる。

##### 【0275】

また、本発明は、 $n$ 分木 ( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有し、前記デバイス鍵を利用者装置に割り当てる鍵管理装置であって、 $n$ 分木においてルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しているデバイス鍵記憶手段と、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込む鍵情報生成手段と、リーフを除き、無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得ら

れた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む無効化情報生成手段とを備える。また、 $n$ 分木 ( $n$ は、2以上の整数)に関連付けて1個以上のデバイス鍵を有する鍵管理装置により、1個以上のデバイス鍵が割り当てられ、割り当てられた前記デバイス鍵の中の1個のデバイス鍵に基づいて、コンテンツを暗号化して記録媒体に書き込み又は前記記録媒体から読み出した暗号化コンテンツを復号する利用者装置であって、前記鍵管理装置は、 $n$ 分木を構成する1個以上のノードにそれぞれ対応付けて1個以上のデバイス鍵を記憶しており、ルートから一部のリーフへの経路上に存在する複数のノードは、無効化されており、複数の共通デバイス鍵をそれぞれ用いて1個のメディア鍵を暗号化して複数の暗号化メディア鍵を生成し、各共通デバイス鍵は、無効化されていないノードに対応付けられた複数のデバイス鍵のうち、1以上の利用者装置に共通に割り当てられたデバイス鍵であり、その結果複数の暗号化メディア鍵が得られ、得られた複数の暗号化メディア鍵を、 $n$ 分木の構成に係る配列順序に従って記録媒体に書き込み、リーフを除き、無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成し、その結果複数の無効化情報が得られ、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、前記利用者装置は、前記記録媒体に前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記記録媒体に前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、当該利用者装置に割り当てられたデバイス鍵により暗号化された暗号化メディア鍵を特定する特定手段と、特定した暗号化メディア鍵を、当該利用者装置に割り当てられたデバイス鍵に基づいて復号して、メディア鍵を生成する復号手段と、生成した前記メディア鍵に基づいてコンテンツを暗号化して前記記録媒体に書き込み、又は前記記録媒体から暗号化コンテンツを読み出し読み出した暗号化コンテンツを生成した前記メディア鍵に基づいて復号してコンテンツを生成する暗号復号手段とを備える。

#### 【0276】

この構成によると、鍵管理装置は、複数の暗号化メディア鍵及び複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込み、利用者装置は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から暗号化メディア鍵を特定するので、利用者装置は、自らに割り当てられた暗号化メディア鍵を効率良く決定することができる。

#### 【0277】

ここで、前記 $n$ 分木は、複数のレイヤから構成され、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む。また、前記 $n$ 分木は、複数のレイヤから構成され、前記複数の暗号化メディア鍵は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序である前記配列順序に従って記録媒体に書き込まれ、前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する。

#### 【0278】

この構成によると、前記配列順序は、ルートを起点とし、ルート側のレイヤからリーフ側のレイヤへの順序であるので、鍵管理装置及び利用者装置において前記配列順序を確実に決定することができる。

ここで、前記鍵情報生成手段は、得られた複数の暗号化メディア鍵を、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込み、前記無効化情報生成手段は、得られた複数の無効化情報を、前記配列順序に従って前記記録媒体に書き込む。また、前記複数の暗号化メディア鍵は、ルートを起点とし、ルートから各リーフへ至る経路上に配されるノードの順序であって、重複して配列されない前記配列順序に従って記録媒体に書き込まれ、

10

20

30

40

50

前記複数の無効化情報は、前記配列順序に従って前記記録媒体に書き込まれ、前記特定手段は、前記配列順序に従って書き込まれた前記複数の無効化情報を用いて、前記配列順序に従って書き込まれた前記複数の暗号化メディア鍵の中から、前記暗号化メディア鍵を特定する。

#### 【0279】

この構成によると、前記配列順序は、ルートを起点とし、重複して配列されないように、ルートから各リーフへ至る経路上に配されるノードの順序であるので、鍵管理装置及び利用者装置において前記配列順序を確実に決定することができる。

ここで、前記無効化情報生成手段は、リーフを除き、無効化された全てのノードについて、無効化情報を生成する。また、リーフを除き、無効化された全てのノードについて、無効化情報が生成されて、前記記録媒体に書き込まれ、前記特定手段は、前記複数の無効化情報を用いて、前記暗号化メディア鍵を特定する。

10

#### 【0280】

この構成によると、無効化された全てのノードについて、無効化情報を生成するので、鍵管理装置及び利用者装置において無効化されたノードを確実に決定することができる。

ここで、前記無効化情報生成手段は、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報を生成し、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成を抑制し、リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報を生成する。また、リーフを除き、無効化されたノードであって、下位側に接続する全てのノードが無効化されているものについて、下位側に接続する全てのノードが無効化されている旨を示す特別無効化情報が生成されて前記記録媒体に書き込まれ、前記下位側に接続する全ての無効化されたノードについて、無効化情報の生成が抑制され、リーフを除く他の無効化されたノードについて、下位の $n$ 個のノードのそれぞれが無効化されているか否かを示す無効化情報が生成されて前記記録媒体に書き込まれ、前記特定手段は、前記特別無効化情報及び前記無効化情報を用いて、前記暗号化メディア鍵を特定する。

20

#### 【0281】

この構成によると、下位側に接続する全てのノードが無効化されていることを示す特別な無効化情報を生成するので、下位側に接続する全てのノードが無効化されているものが多い場合に、記録媒体の容量を節約することができる。

30

#### 【図面の簡単な説明】

【図1】著作物保護システム10の構成を示すブロック図である。

【図2】鍵管理装置100の構成を示すブロック図である。

【図3】木構造テーブルD100のデータ構造の一例を示す。

【図4】木構造T100を示す概念図である。

【図5】無効化されたノードを含む木構造T200を示す概念図である。

【図6】ノード無効化パターンの一例を示すデータ構造図である。

【図7】複数の暗号化メディア鍵を含む鍵情報の一例を示すデータ構造図である。

【図8】記録装置300aの構成を示すブロック図である。

40

【図9】再生装置400aの構成を示すブロック図である。

【図10】ユーザ装置へデバイス鍵を割り当てる動作、鍵情報の生成と記録媒体への書き込みの動作及びユーザ装置によるコンテンツの暗号化又は復号の動作を示すフローチャートである。特に、デバイス鍵が特に、デバイス鍵が不正な第三者により暴露されるまでの、各装置の動作を示すフローチャートである。

【図11】デバイス鍵が不正な第三者により暴露された後における、暴露されたデバイス鍵に対応する木構造の内のノードの無効化の動作、新たな鍵情報の生成と記録媒体への書き込みの動作、及びユーザ装置によるコンテンツの暗号化又は復号の動作を示すフローチャートである。

【図12】木構造構築部101による木構造テーブルの生成と木構造格納部102への木

50

構造テーブルの書き込みの動作を示すフローチャートである。

【図 1 3】デバイス鍵割当部 1 0 3 によるデバイス鍵と I D 情報とを各ユーザ装置へ出力する動作を示すフローチャートである。

【図 1 4】木構造更新部 1 0 5 による木構造の更新の動作を示すフローチャートである。

【図 1 5】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。

【図 1 6】鍵情報生成部 1 0 7 による鍵情報の生成の動作を示すフローチャートである。

【図 1 7】記録装置 3 0 0 a が有する特定部 3 0 3 により、記録媒体 5 0 0 b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作を示すフローチャートである。

10

【図 1 8】第 1 の実施の形態において、一例として無効化されるユーザ装置が木構造の中で特定のリーフに集中して発生する可能性がある場合の木構造の一例を示す。

【図 1 9】第 2 の実施の形態において、無効化されるユーザ装置が木構造の中で特定のリーフに集中して発生した場合における特別なノード無効化パターンを示す木構造である。

【図 2 0】木構造テーブル D 4 0 0 のデータ構造の一例を示す。

【図 2 1】ヘッダ情報 D 5 0 0 のデータ構造の一例を示す。

【図 2 2】鍵情報 D 6 0 0 のデータ構造の一例を示す。

【図 2 3】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。図 2 4 へ続く。

【図 2 4】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。図 2 5 へ続く。

20

【図 2 5】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。図 2 6 へ続く。

【図 2 6】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。図 2 5 から続く。

【図 2 7】記録装置 3 0 0 a が有する特定部 3 0 3 により、記録媒体 5 0 0 b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作を示すフローチャートである。

【図 2 8】第 3 の実施の形態において、特別なノード無効化パターンを示す木構造である。

30

【図 2 9】ヘッダ情報 D 7 0 0 のデータ構造の一例を示す。

【図 3 0】鍵情報 D 8 0 0 のデータ構造の一例を示す。

【図 3 1】ヘッダ情報の生成の動作を示すフローチャートである。図 3 2 へ続く。

【図 3 2】ヘッダ情報の生成の動作を示すフローチャートである。図 3 3 へ続く。

【図 3 3】ヘッダ情報の生成の動作を示すフローチャートである。図 3 4 へ続く。

【図 3 4】ヘッダ情報の生成の動作を示すフローチャートである。図 3 3 から続く。

【図 3 5】記録装置 3 0 0 a が有する特定部 3 0 3 により、記録媒体 5 0 0 b に記憶されている鍵情報から、1 個の暗号化メディア鍵を特定する動作を示すフローチャートである。

【図 3 6】第 4 の実施の形態における複数のノード無効化パターンの並べ方を示す木構造である。

40

【図 3 7】木構造テーブル D 1 0 0 のデータ構造の一例を示す。

【図 3 8】ヘッダ情報 D 9 0 0 のデータ構造の一例を示す。

【図 3 9】木構造構築部 1 0 1 による木構造テーブルの生成と木構造格納部 1 0 2 への木構造テーブルの書き込みの動作を示すフローチャートである。

【図 4 0】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。図 4 1 へ続く。

【図 4 1】鍵情報ヘッダ生成部 1 0 6 によるヘッダ情報の生成の動作を示すフローチャートである。図 4 0 から続く。

【図 4 2】記録装置 3 0 0 a が有する特定部 3 0 3 により、記録媒体 5 0 0 b に記憶され

50

ている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。

【図４３】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４４へ続く。

【図４４】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４５へ続く。

【図４５】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４６へ続く。

【図４６】鍵情報ヘッダ生成部１０６によるヘッダ情報の生成の動作を示すフローチャートである。図４５から続く。

【図４７】記録装置３００ａが有する特定部３０３により、記録媒体５００ｂに記憶されている鍵情報から、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。

【図４８】著作物保護システム１０ｆの構成を示すブロック図である。

【図４９】無効化されたデバイス鍵Key A、Key B及びKey Eが割り当てられたノードを含む木構造T700を示す概念図である。

【図５０】ヘッダ情報D1000及び鍵情報D1010の構成を示すデータ構造図である。

【図５１】記録装置３００ａが有する特定部３０３により、１個の暗号化メディア鍵を特定する動作を示すフローチャートである。

【符号の説明】

１０、１０ｂ～１０ｆ 著作物保護システム

１００ 鍵管理装置

１００ｄ 鍵管理装置

１０１ 木構造構築部

１０２ 木構造格納部

１０３ デバイス鍵割当部

１０４ 無効化装置指定部

１０５ 木構造更新部

１０６ 鍵情報ヘッダ生成部

１０７ 鍵情報生成部

２００ 鍵情報記録装置

３００ａ、３００ｂ、３００ｃ 記録装置

３０１ 鍵情報記憶部

３０２ 復号部

３０３ 特定部

３０４ 暗号部

３０５ コンテンツ記憶部

４００ａ、４００ｂ、４００ｃ 再生装置

４０１ 鍵情報記憶部

４０２ 特定部

４０３ 復号部

４０４ 復号部

４０５ 再生部

５００ａ、５００ｂ、５００ｃ、５００ｄ 記録媒体

１７０１ データ記録装置

１７０３ａ、１７０３ｂ、１７０３ｃ データ再生装置

10

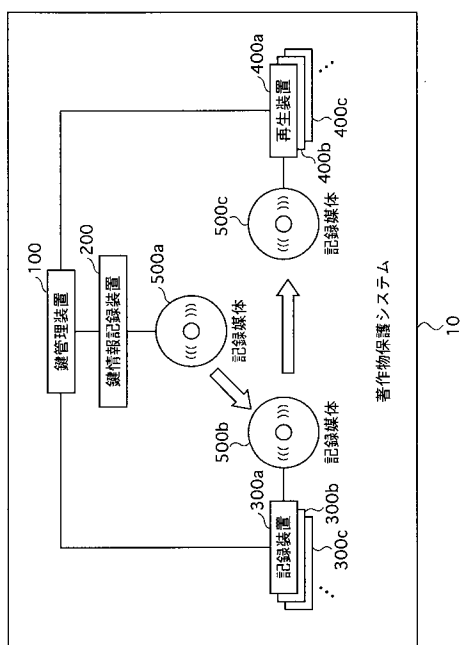
20

30

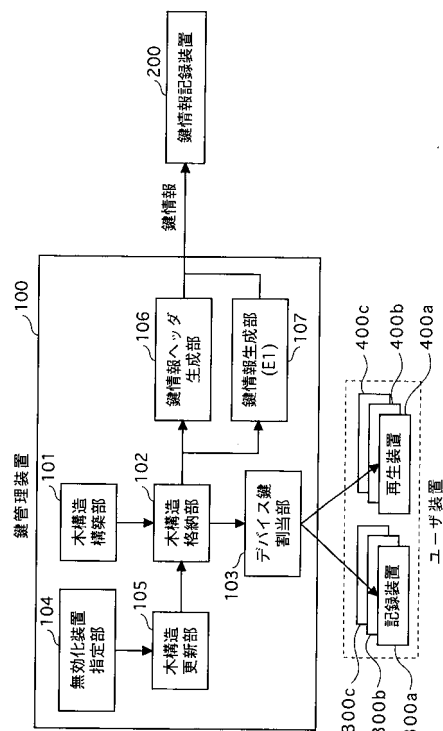
40



【圖 1】



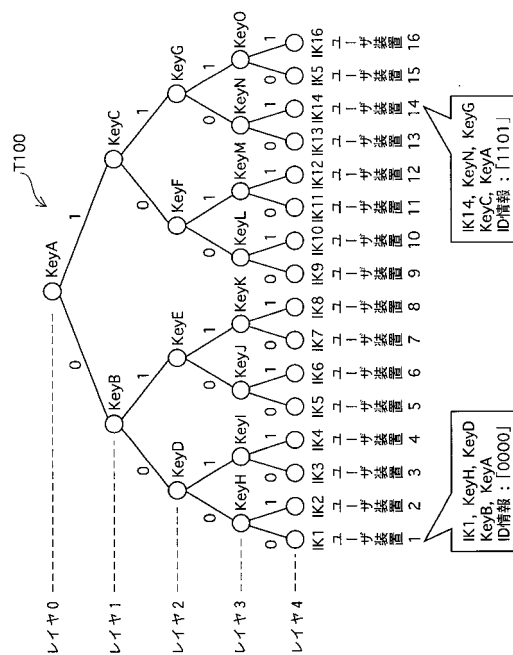
【圖 2】



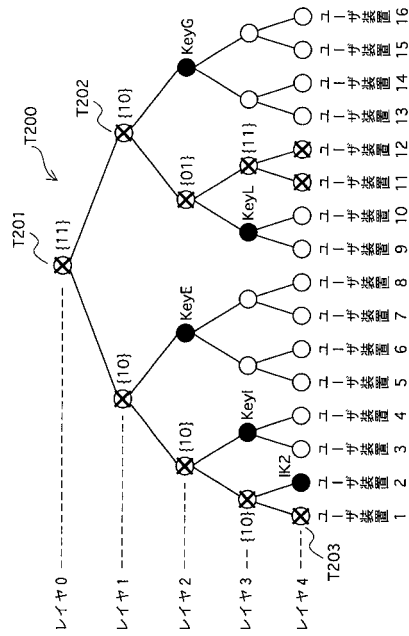
【 図 3 】

木構造テーブル			D100
ノード情報			
ノード名	デバイス鍵	無効化フラグ	
ルート	KeyA	1	
0	KeyB	1	
1	KeyC	1	
00	KeyD	1	
01	KeyE	0	
10	KeyF	1	
11	KeyG	0	
000	KeyH	1	
001	KeyI	0	
010	KeyJ	0	
⋮	⋮	⋮	
111	KeyO	0	
0000	IK1	1	
0001	IK2	0	
0010	IK3	0	
0011	IK4	0	
⋮	⋮	⋮	
1111	IK16	0	

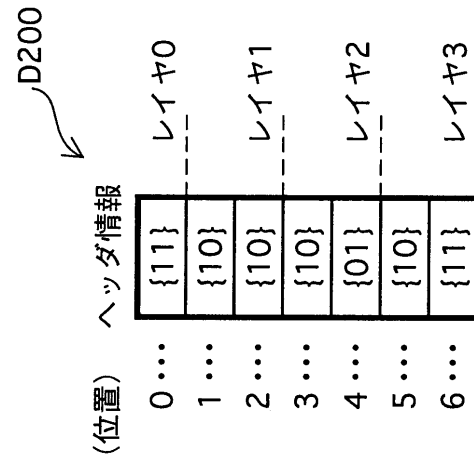
【 図 4 】



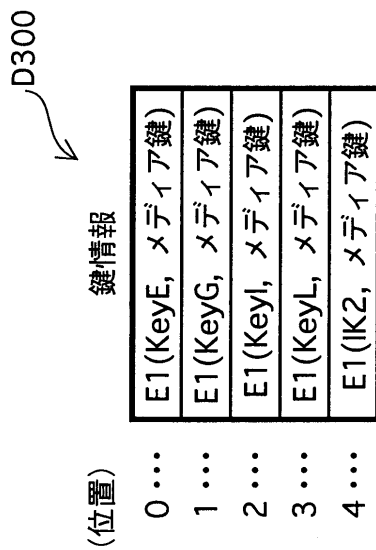
【図 5】



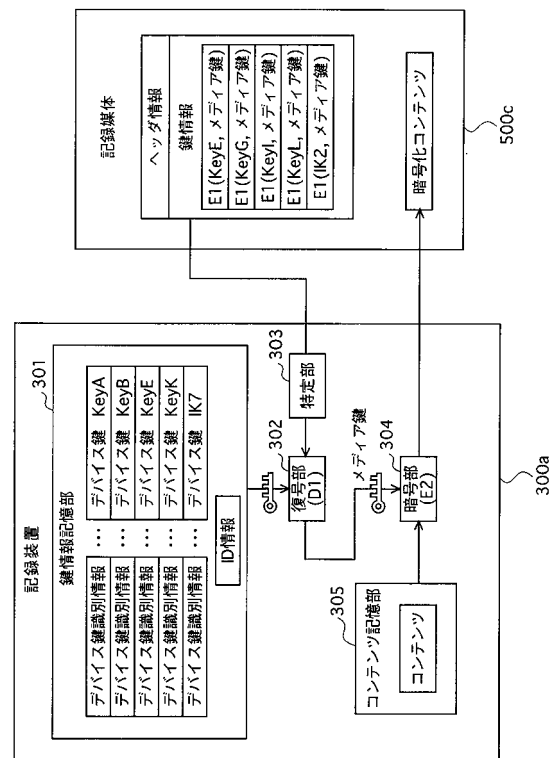
【図 6】



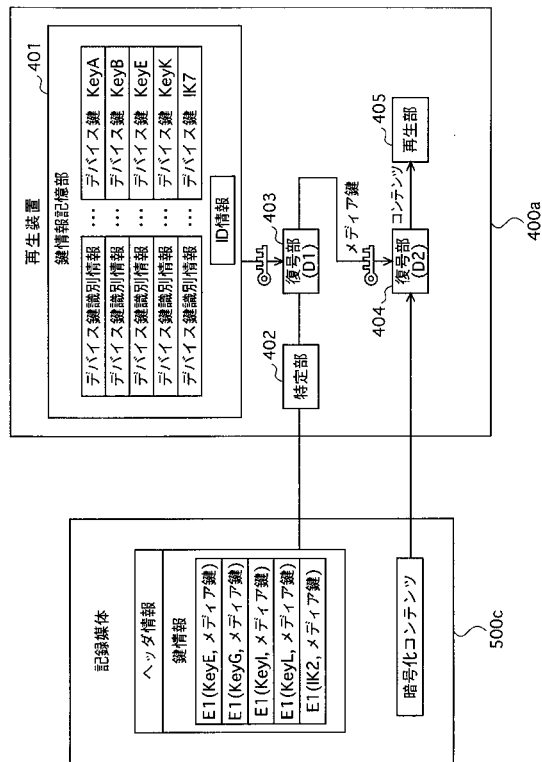
【図 7】



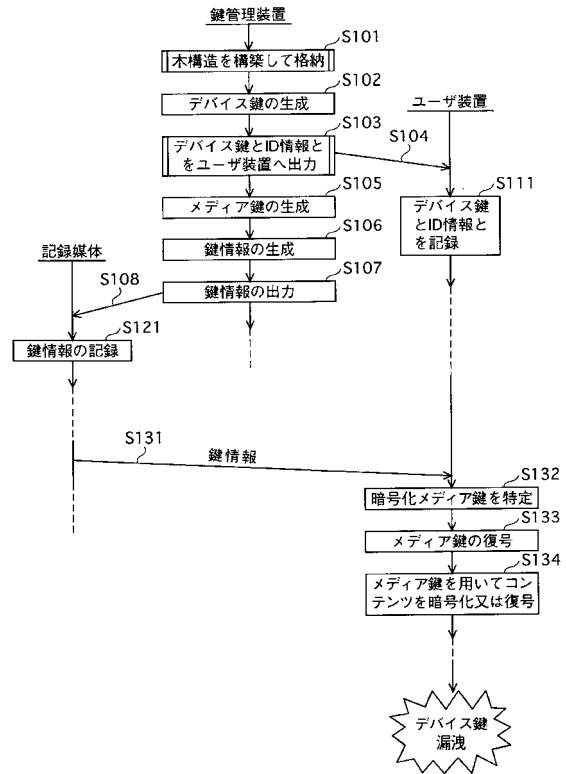
【図 8】



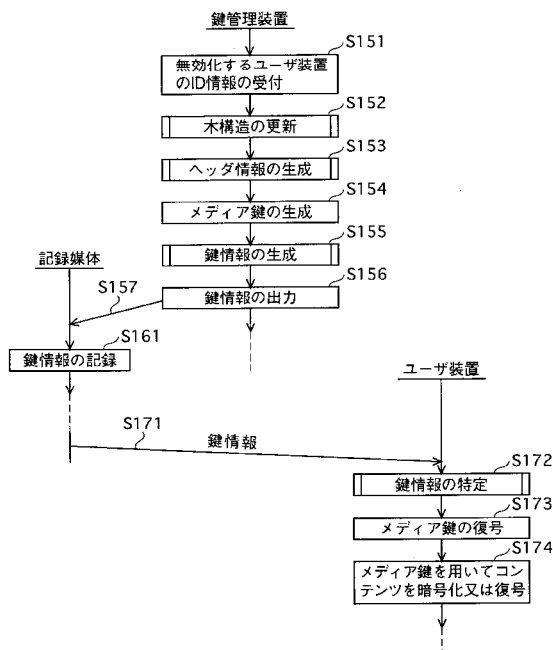
【図 9】



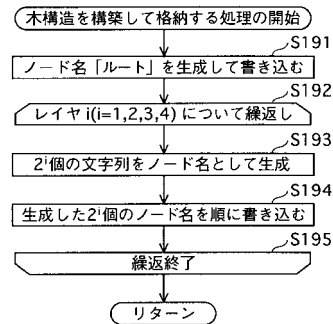
【図 10】



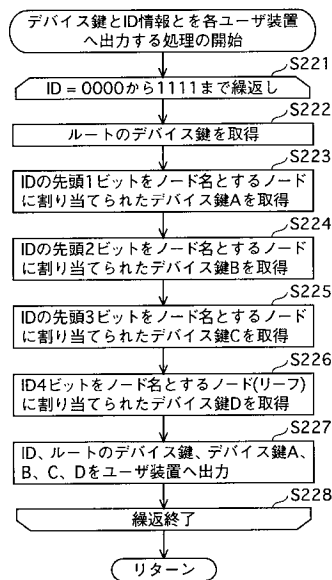
【図 11】



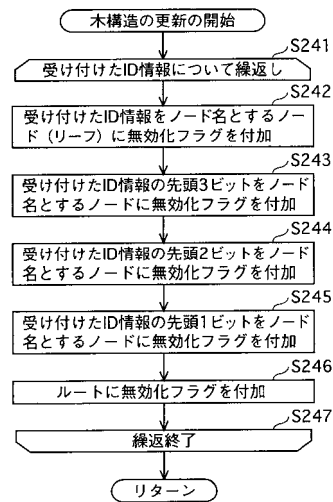
【図 12】



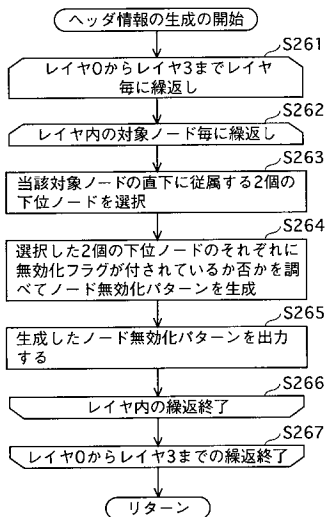
【図 13】



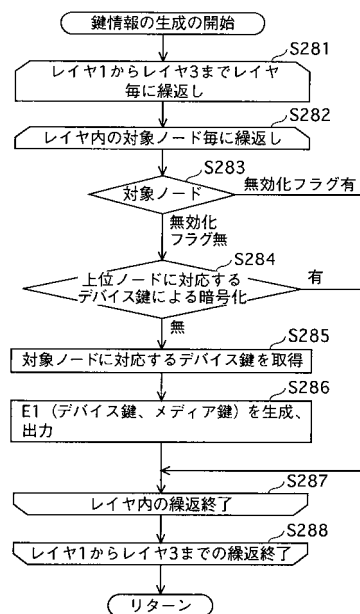
【図 14】



【図 15】

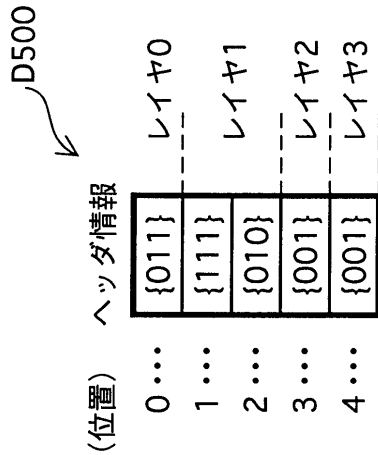


【図 16】

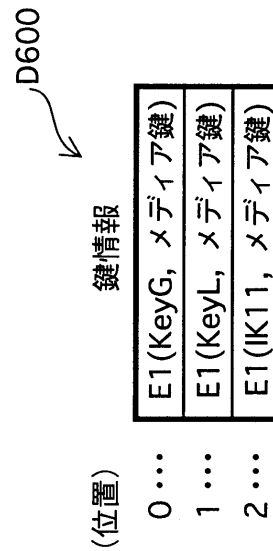




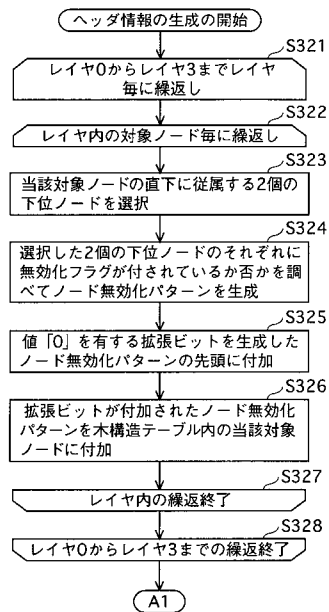
【図 2 1】



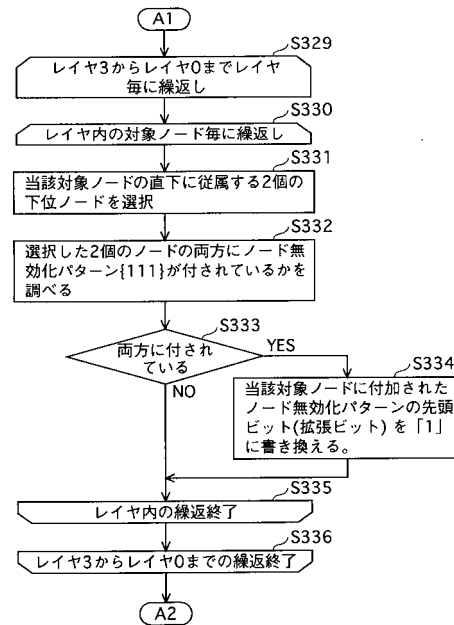
【図 2 2】



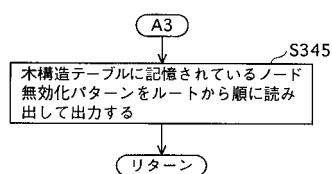
【図 2 3】



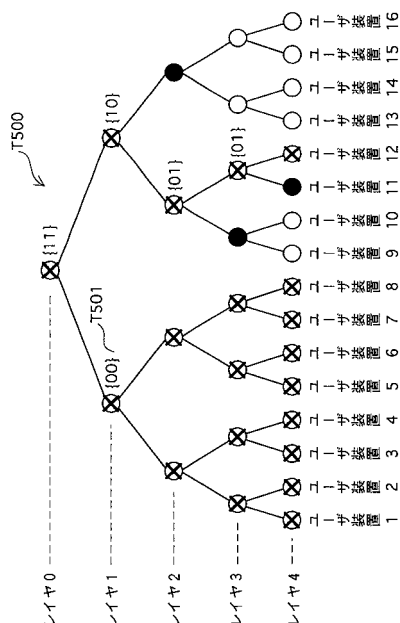
【図 2 4】



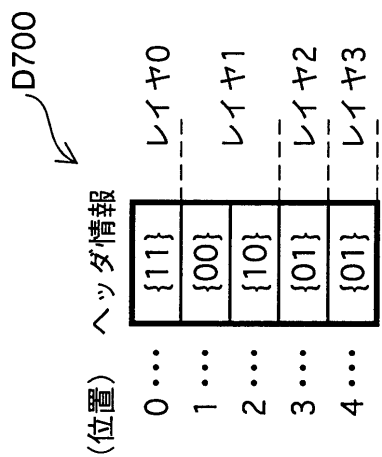
【 ㊦ 2 6 】



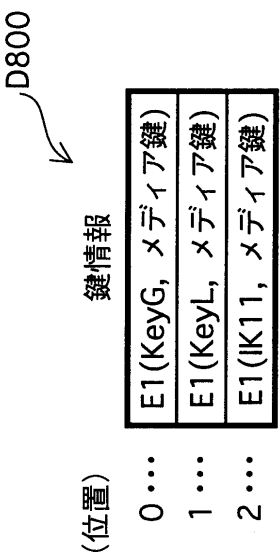
【 ㄨ 2 8 】



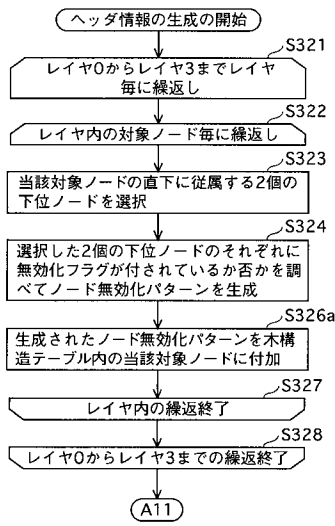
【図 29】



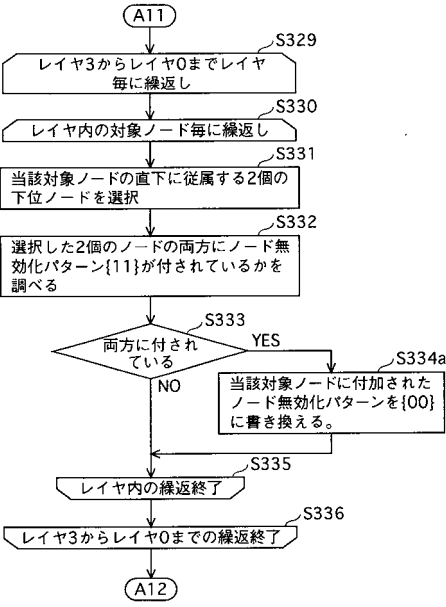
【図 30】



【図 31】

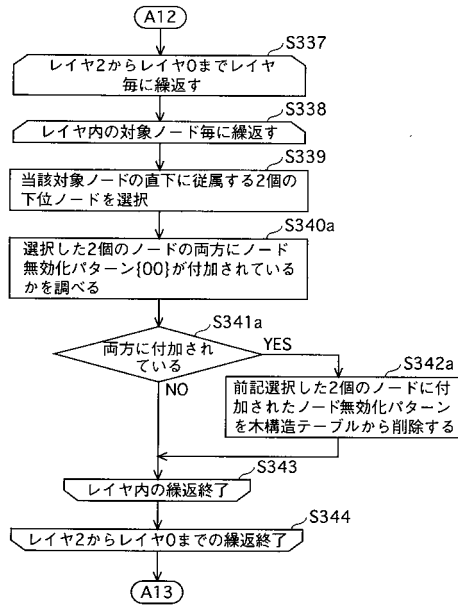


【図 32】

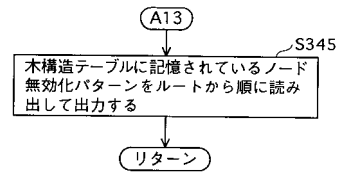




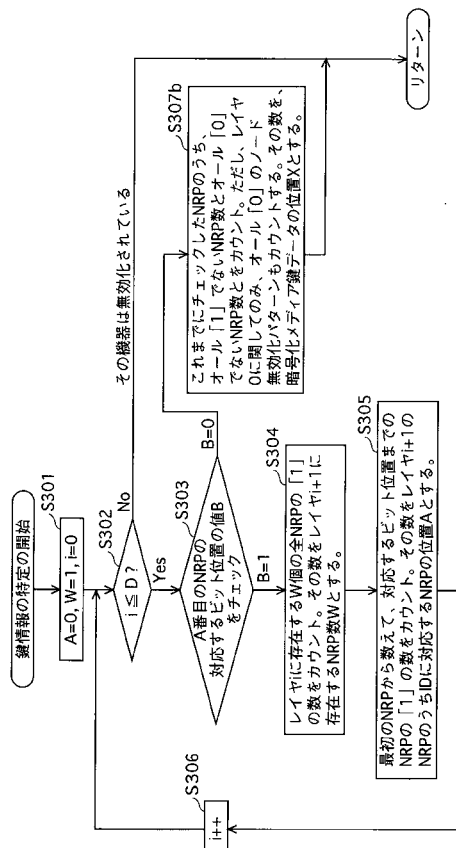
【図 33】



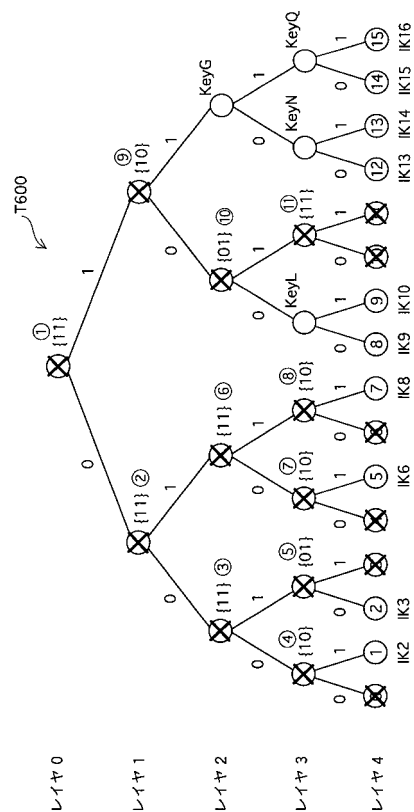
【図 34】



【図 35】



【図 36】



【図 3 7】

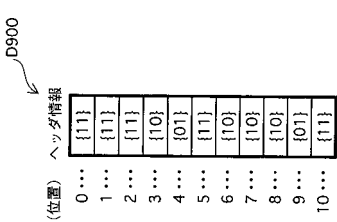
木構造テーブル

D1000

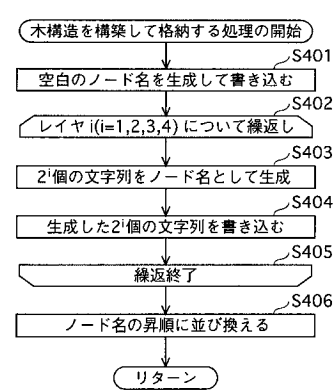
ノード情報		
ノード名	デバイス鍵	無効化フラグ
(空白)	KeyA	
0	KeyB	
00	KeyD	
000	KeyH	
0000	IK1	
0001	IK2	
001	KeyI	
0010	IK3	
0011	IK4	
01	KeyE	
010	KeyJ	
0100	IK5	
0101	IK6	
011	KeyK	
0110	IK7	
0111	IK8	

ノード情報		
ノード名	デバイス鍵	無効化フラグ
1	KeyC	
10	KeyF	
100	KeyL	
1000	IK9	
1001	IK10	
101	KeyM	
1010	IK11	
1011	IK12	
11	KeyG	
110	KeyN	
1100	IK13	
1101	IK14	
111	KeyO	
1110	IK15	
1111	IK16	

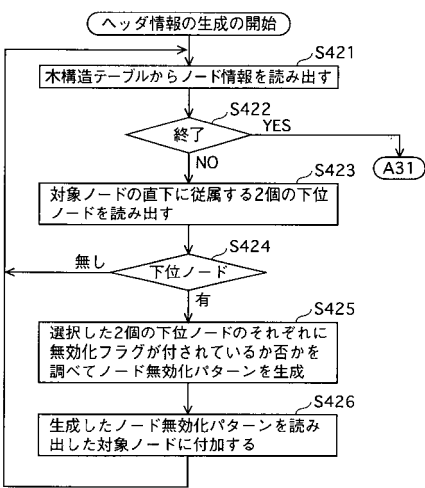
【図 3 8】



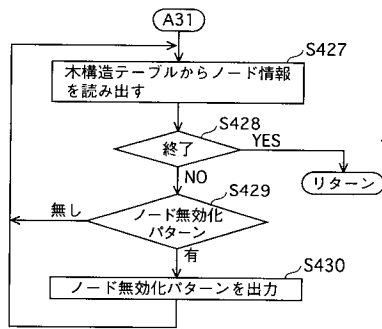
【図 3 9】



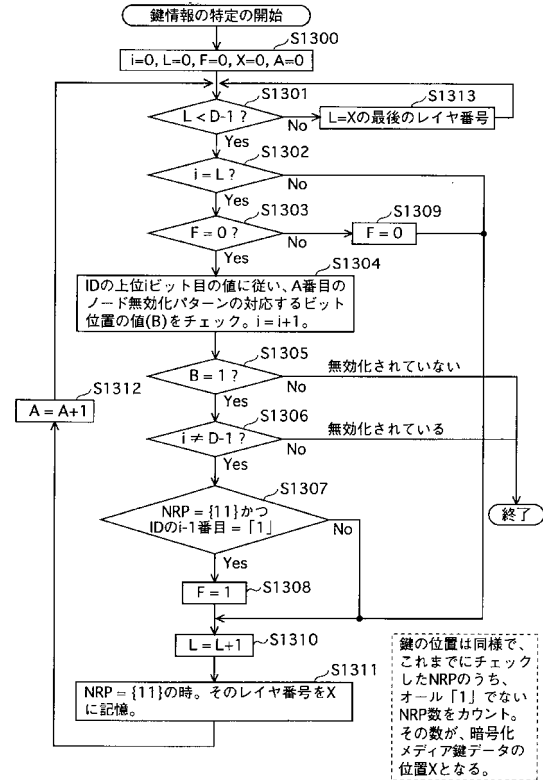
【図 4 0】



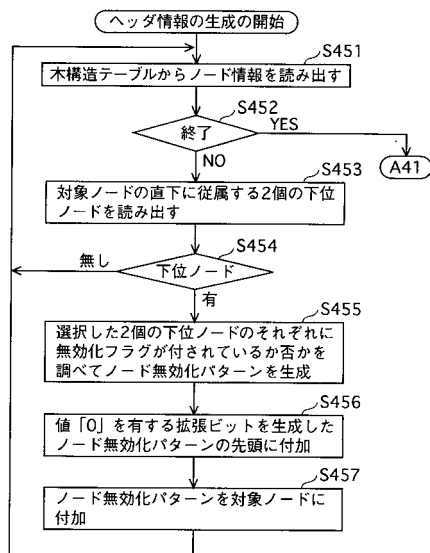
【図 4 1】



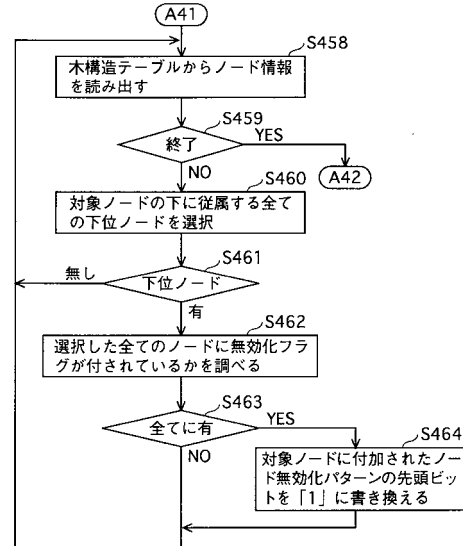
【図 4 2】



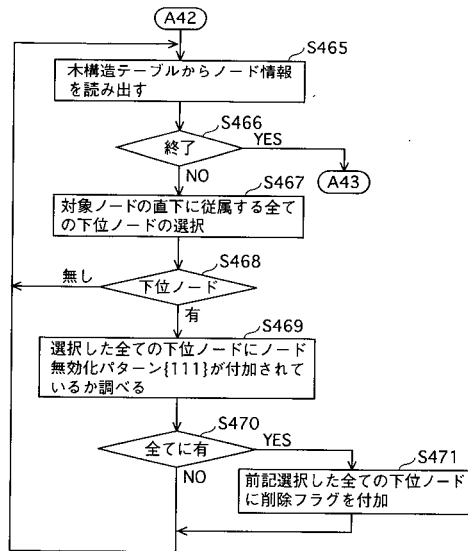
【図 4 3】



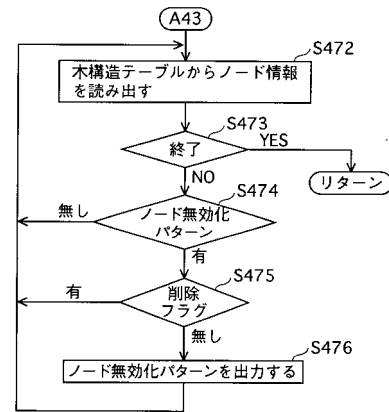
【図 4 4】



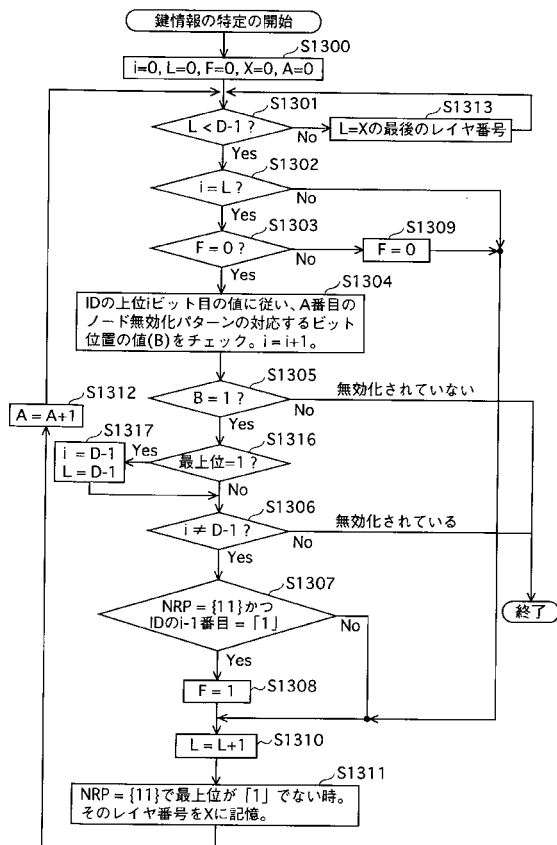
【図 45】



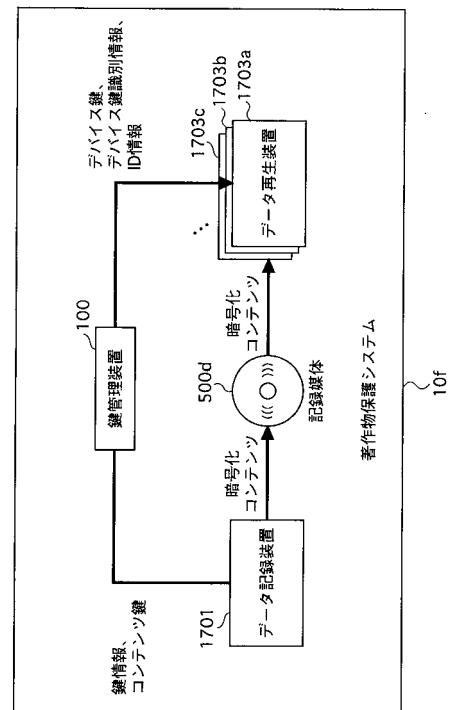
【図 46】



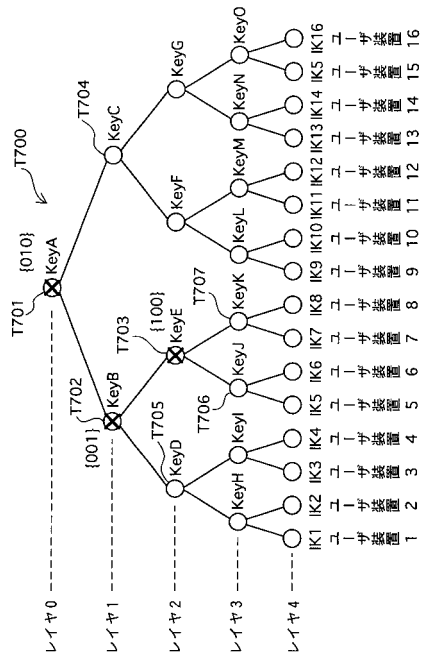
【図 47】



【図 48】



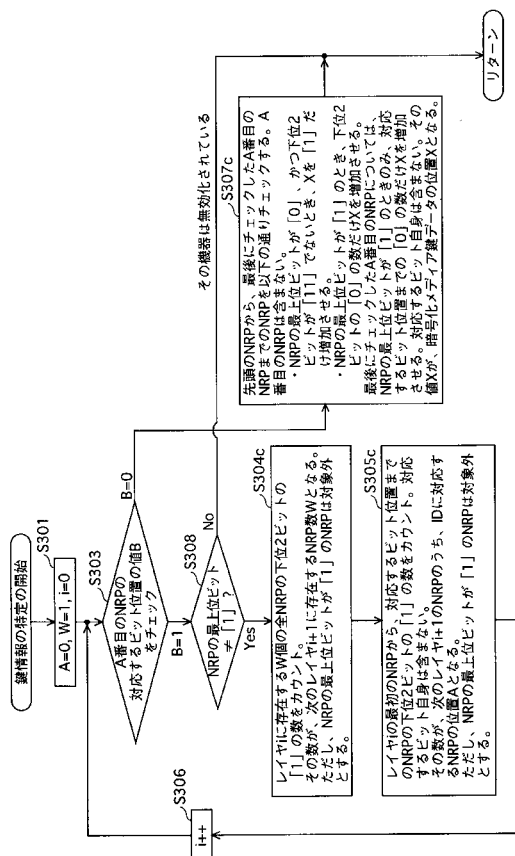
【図 49】



【図 50】



【図 51】



## フロントページの続き

審査官 青木 重徳

(56)参考文献 特開平 1 1 - 1 8 7 0 1 3 ( J P , A )

特開 2 0 0 1 - 1 8 6 1 1 9 ( J P , A )

Chung Kei Wong, Mohamed Gouda, and Simon S. Lam, "Secure Group Communications Using Key Graphs", IEEE/ACM Transactions on Networking, 2 0 0 0 年 2 月, VOL.8, NO.1, p.16-30, URL, <http://ieeexplore.ieee.org/xpls/absprintf.jsp?arnumber=836475>

中野稔久, 大森基司, 松崎なつめ, 館林誠, " デジタルコンテンツ保護用鍵管理方式-木構造パターン分割方式-", 暗号と情報セキュリティシンポジウム ( S C I S 2 0 0 2 ) 講演論文集 C D - R O M , 日本, 電子情報通信学会情報セキュリティ研究専門委員会, 2 0 0 2 年 1 月 2 9 日, 1 0 C 鍵配送・管理 ( 2 ) , 1 0 C - 1

松崎なつめ, 中野稔久, 松本勉, " 複数システムに対応した木構造鍵管理方法 ", 暗号と情報セキュリティシンポジウム ( S C I S 2 0 0 2 ) 講演論文集 C D - R O M , 日本, 電子情報通信学会情報セキュリティ研究専門委員会, 2 0 0 2 年 1 月 2 9 日, 1 0 C 鍵配送・管理 ( 2 ) , 1 0 C - 2

中野稔久, 松崎なつめ, 館林誠, " デジタルコンテンツ保護用鍵管理方式 - 木構造パターン分割方式の一般化検討 - ", 電子情報通信学会技術研究報告 ( I S E C 2 0 0 2 - 3 4 ~ 5 6 ) , 日本, 社団法人電子情報通信学会, 2 0 0 2 年 7 月 1 2 日, V o l . 1 0 2 , N o . 2 1 2 , p . 3 1 - 3 8

(58)調査した分野(Int.Cl., D B 名)

H04L 9/08