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

特許第4140624号
(P4140624)

(45)発行日　平成20年8月27日(2008.8.27)　(24)登録日　平成20年6月20日(2008.6.20)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	H
G11B 27/00	(2006.01)	G11B	20/10	301Z
H04L 9/32	(2006.01)	G11B	27/00	D
		H04L	9/00	675B

請求項の数 30　(全 52 頁)

(21)出願番号　特願2005-270484(P2005-270484)
(22)出願日　平成17年9月16日(2005.9.16)
(65)公開番号　特開2007-80458(P2007-80458A)
(43)公開日　平成19年3月29日(2007.3.29)
審査請求日　平成18年6月1日(2006.6.1)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　高島　芳和
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　高野　美帆子

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法、並びにコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理装置であり、
情報記録媒体の記録コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードファイルを複数記録した情報記録媒体から、コンテンツコードファイルを取得して、該取得コンテンツコードファイルに従ったデータ処理を実行するデータ処理部を有し、
前記コンテンツコードファイルは、管理センタによる電子署名が付与されており、
前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されており、
前記データ処理部は、
前記コンテンツコードファイルに含まれるコンテンツコード全体の改ざん検証を可能とした前記管理センタによる電子署名の検証処理を実行し、該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに含まれるプログラムに従ったデータ処理を実行する構成であり、更に前記情報記録媒体に記録された複数のコンテンツコードファイルから、前記プレーヤ固有のプログラムを含むコンテンツコードファイルを取得してプレーヤ固有の秘密鍵による署名の検証処理を実行し、該検証の結果、プレーヤ署名設定コンテンツコードファイルの正当性が確認されたことを条件として、前記プレーヤ固有のプログラム処理を実行する構成であることを特徴とする情報処理装

置。
【請求項２】
前記データ処理部は、
前記電子署名の検証処理として、
管理センタの付与する電子署名の検証処理を実行し、
さらに、プレーヤ製造者に固有のプレーヤ秘密鍵を適用して生成された電子署名の検証処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置
【請求項３】
前記データ処理部は、
情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル各々について、各ファイルに設定された電子署名に基づく署名検証処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記データ処理部は、
情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル中、１つのコンテンツコードファイルに設定された電子署名に基づく署名検証処理を実行し、その他の利用コンテンツコードファイルについては、電子署名検証と異なる検証処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記データ処理部は、
前記その他の利用コンテンツコードファイルについては、ハッシュ値に基づく検証処理を実行する構成であることを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記データ処理部は、
前記コンテンツコードに含まれる変換テーブルを適用した、コンテンツの一部データの置き換え処理に伴って必要となるデータ処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記データ処理部は、
情報記録媒体に記録されたコンテンツの区分領域として設定されたセグメント毎に異なるパラメータであり、前記変換テーブルに含まれる変換エントリの復元に適用するパラメータを算出する処理を実行する構成であることを特徴とする請求項６に記載の情報処理装置。
【請求項８】
情報記録媒体製造装置であり、
情報記録媒体に記録するコンテンツデータを格納したコンテンツファイルを生成するコンテンツファイル生成手段と、
コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードを格納し、さらに改ざん検証用データとしての電子署名を含む複数のコンテンツコードファイルを生成するコンテンツコードファイル生成手段と、
前記コンテンツファイル生成手段において生成したコンテンツファイル、および前記コンテンツコードファイル生成手段において生成したコンテンツコードファイルを情報記録媒体に記録する記録手段と、
を有し、
前記コンテンツコードファイル生成手段は、管理センタによる電子署名の設定されたコンテンツコードファイルを複数生成し、複数のコンテンツコードファイルのうちの少なくとも一つは、プレーヤ固有のプログラムを含むコンテンツコードを格納し、プレーヤ固有の秘密鍵による署名を更に設定したファイルとして生成する処理を実行することを特徴とする情報記録媒体製造装置。

【請求項９】
前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名であることを特徴とする請求項８に記載の情報記録媒体製造装置。
【請求項１０】
前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値であることを特徴とする請求項８に記載の情報記録媒体製造装置。
【請求項１１】
前記コンテンツコードファイル生成手段は、
複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する処理を実行する構成であり、
前記記録手段は、
前記コンテンツコードファイル生成手段において生成された複数の異なるカテゴリのコンテンツコードファイルを情報記録媒体に記録する処理を実行する構成であることを特徴とする請求項８に記載の情報記録媒体製造装置。
【請求項１２】
前記コンテンツコードファイル生成手段は、
複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する構成であり、
各コンテンツコードファイルを、各ファイルに含まれるコンテンツコードの製作者または提供エンティティの電子署名を含むファイルとして生成する処理を実行する構成であることを特徴とする請求項８に記載の情報記録媒体製造装置。
【請求項１３】
情報記録媒体であり、
コンテンツデータを格納したコンテンツファイルと、
コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードを格納し、さらに改ざん検証用データを含む複数のコンテンツコードファイルと、
を格納データとして有し、
前記複数のコンテンツコードファイルは、管理センタによる電子署名が付与されており、前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されているプレーヤ署名設定コンテンツコードファイルであることを特徴とする情報記録媒体。
【請求項１４】
前記プレーヤ署名設定コンテンツコードファイルは、
プレーヤ特有のコードに対して、プレーヤ製造者の秘密鍵を用いて署名を付加されたデータに対して、更に、管理センタにより署名が付加されたファイルであることを特徴とする請求項１３に記載の情報記録媒体。
【請求項１５】
前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名であることを特徴とする請求項１３に記載の情報記録媒体。
【請求項１６】
前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値であることを特徴とする請求項１３に記載の情報記録媒体。
【請求項１７】
前記コンテンツコードファイルは、

複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルによって構成されていることを特徴とする請求項１３に記載の情報記録媒体。

【請求項１８】

前記コンテンツコードファイルは、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルによって構成され、各コンテンツコードファイルには、各ファイルに含まれるコンテンツコードの製作者または提供エンティテイの電子署名が含まれる構成であることを特徴とする請求項１３に記載の情報記録媒体。

【請求項１９】

情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理方法であり、

情報記録媒体の記録コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードファイルを複数記録した情報記録媒体から、コンテンツコードファイルを取得して、コンテンツコードファイルに含まれるコンテンツコード全体の改ざん検証を可能とした電子署名の検証処理を実行する検証処理ステップと、

前記コンテンツコード該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに従ったデータ処理を実行するコード実行ステップと、

を有し、

前記コンテンツコードファイルは、管理センタによる電子署名が付与されており、

前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されており、

前記検証処理ステップは、

前記情報記録媒体に記録された複数のコンテンツコードファイルから、前記プレーヤ固有のプログラムを含むコンテンツコードファイルを取得してプレーヤ固有の秘密鍵による署名の検証処理を実行するステップを含み、

前記コード実行ステップは、

プレーヤ署名設定コンテンツコードファイルの正当性が確認されたことを条件として、前記プレーヤ固有のプログラム処理を実行するステップを含むことを特徴とする情報処理方法。

【請求項２０】

前記検証処理ステップは、

情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル各々について、各ファイルに設定された電子署名に基づく署名検証処理を実行するステップであることを特徴とする請求項１９に記載の情報処理方法。

【請求項２１】

前記検証処理ステップは、

情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル中、１つのコンテンツコードファイルに設定された電子署名に基づく署名検証処理を実行し、その他の利用コンテンツコードファイルについては、電子署名検証と異なる検証処理を実行するステップであることを特徴とする請求項１９に記載の情報処理方法。

【請求項２２】

前記検証処理ステップは、

前記その他の利用コンテンツコードファイルについては、ハッシュ値に基づく検証処理を実行するステップであることを特徴とする請求項２１に記載の情報処理方法。

【請求項２３】

前記コード実行ステップは、

前記コンテンツコードに含まれる変換テーブルを適用した、コンテンツの一部データの置き換え処理に伴って必要となるデータ処理を実行するステップであることを特徴とする請求項１９に記載の情報処理方法。

【請求項２４】
前記コード実行ステップは、
情報記録媒体に記録されたコンテンツの区分領域として設定されたセグメント毎に異なるパラメータであり、前記変換テーブルに含まれる変換エントリの復元に適用するパラメータを算出する処理を実行するステップであることを特徴とする請求項２３に記載の情報処理方法。
【請求項２５】
情報記録媒体製造方法であり、
情報記録媒体に記録するコンテンツデータを格納したコンテンツファイルを生成するコンテンツファイル生成ステップと、
コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードを格納し、さらに改ざん検証用データとしての電子署名を含む複数のコンテンツコードファイルを生成するコンテンツコードファイル生成ステップと、
前記コンテンツファイル生成ステップにおいて生成したコンテンツファイル、および前記コンテンツコードファイル生成ステップにおいて生成したコンテンツコードファイルを情報記録媒体に記録する記録ステップと、
を有し、
前記コンテンツコードファイル生成ステップは、管理センタによる電子署名の設定されたコンテンツコードファイルを複数生成し、複数のコンテンツコードファイルのうちの少なくとも一つは、プレーヤ固有のプログラムを含むコンテンツコードを格納し、プレーヤ固有の秘密鍵による署名を更に設定したファイルとして生成する処理を実行するステップを含むことを特徴とする情報記録媒体製造方法。
【請求項２６】
前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名であることを特徴とする請求項２５に記載の情報記録媒体製造方法。
【請求項２７】
前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値であることを特徴とする請求項２５に記載の情報記録媒体製造方法。
【請求項２８】
前記コンテンツコードファイル生成ステップは、
複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する処理を実行するステップであり、
前記記録ステップは、
前記コンテンツコードファイル生成ステップにおいて生成された複数の異なるカテゴリのコンテンツコードファイルを情報記録媒体に記録する処理を実行するステップであることを特徴とする請求項２５に記載の情報記録媒体製造方法。
【請求項２９】
前記コンテンツコードファイル生成ステップは、
複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成するステップであり、
各コンテンツコードファイルを、各ファイルに含まれるコンテンツコードの製作者または提供エンティティの電子署名を含むファイルとして生成する処理を実行するステップであることを特徴とする請求項２５に記載の情報記録媒体製造方法。
【請求項３０】
情報記録媒体に記録されたコンテンツの再生処理を情報処理装置において実行させるコンピュータ・プログラムであり、
情報記録媒体の記録コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードファイルを複数記録した情報記録媒体から、コンテ

ンツコードファイルを取得して、コンテンツコードファイルに含まれるコンテンツコード全体の改ざん検証を可能とした電子署名の検証処理を実行する検証処理ステップと、
前記コンテンツコード該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに従ったデータ処理を実行するコード実行ステップと、
を有し、
前記コンテンツコードファイルは、管理センタによる電子署名が付与されており、
前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されており、
前記検証処理ステップは、
前記情報記録媒体に記録された複数のコンテンツコードファイルから、前記プレーヤ固有のプログラムを含むコンテンツコードファイルを取得してプレーヤ固有の秘密鍵による署名の検証処理を実行するステップを含み、
前記コード実行ステップは、
プレーヤ署名設定コンテンツコードファイルの正当性が確認されたことを条件として、前記プレーヤ固有のプログラム処理を実行するステップを含むことを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、コンテンツの利用制御プログラムとして、コンテンツと共に情報記録媒体に記録されるコンテンツコードの厳格な管理構成を実現する情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法、並びにコンピュータ・プログラムに関する。

【背景技術】

【０００２】

音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーション・プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）は、記録メディア、例えば、青色レーザを適用したＢｌｕ－ｒａｙ Ｄｉｓｃ（商標）、あるいはＤＶＤ(Digital Versatile Disc)、ＭＤ(Mini Disc)、ＣＤ(Compact Disc)にデジタルデータとして格納することができる。特に、青色レーザを利用したＢｌｕ－ｒａｙ Ｄｉｓｃ（商標）は、高密度記録可能なディスクであり大容量の映像コンテンツなどを高画質データとして記録することができる。

【０００３】

これら様々な情報記録媒体（記録メディア）にデジタルコンテンツが格納され、ユーザに提供される。ユーザは、所有するＰＣ（Personal Computer）、ディスクプレーヤ等の再生装置においてコンテンツの再生、利用を行う。

【０００４】

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

【０００５】

デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクの流通や、ＰＣ等のハードディスクに格納したコピーコンテンツの利用が蔓延しているといった問題が発生している。

【０００６】
ＤＶＤ、あるいは近年開発が進んでいる青色レーザを利用した記録媒体等の大容量型記録媒体は、１枚の媒体に例えば映画１本～数本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。
【０００７】
コンテンツの不正コピーを防止して著作権者の保護を図る１つの手法としてコンテンツの暗号化処理がある。しかし、コンテンツを暗号化しても、暗号鍵の漏洩が発生してしまうと、不正に復号されたコンテンツが流出するという問題が発生する。このような問題を解決する１つの構成を開示した従来技術として、特許文献１に記載の構成がある。特許文献１は、コンテンツの一部をダミーデータに置き換えて記録することで、コンテンツの不正再生を防止した構成を開示している。
【０００８】
コンテンツをダミーデータに置き換えたコンテンツの再生処理に際しては、ダミーデータを正常なコンテンツデータに再度、置き換える処理が必要になる。このデータ変換処理は、正常コンテンツの外部への漏洩を発生させることなく行なわれることが必要であり、またダミーデータの配置位置などや変換方法などの処理情報についても漏洩を防止することが好ましい。
【０００９】
このように、コンテンツの再生に際しては、コンテンツの復号処理やデータ変換処理などを実行することが必要であり、また、コンテンツを利用しようとする情報処理装置や再生（プレーヤ）プログラムが正当なライセンスを受けた機器やプログラムであるかといった正当性確認処理などを行なう場合がある。このようなデータ処理は、コンテンツの利用制御プログラムとして、コンテンツと共に情報記録媒体に記録されるコンテンツコードを実行することで行なわれる。なお、コンテンツコードを利用したコンテンツ利用処理例については、例えば特許文献１に記載がある。
【００１０】
コンテンツコードは、コンテンツとは独立したファイルとして設定し、情報記録媒体に記録される。従って、コンテンツコードのみを他の情報記録媒体に移動させる処理や、コピーするといった処理も可能となる。コンテンツコードの漏洩が発生し、不正に流通し、不正な利用が行なわれると、多くのコンテンツが不正に再生、利用される可能性があり、大きな損害を発生させる可能性がある。
【特許文献１】ＷＯ２００５／００８３８５
【発明の開示】
【発明が解決しようとする課題】
【００１１】
本発明は、このような状況に鑑みてなされたものであり、コンテンツの利用制御プログラムとしてコンテンツと共に情報記録媒体に記録されるコンテンツコードの厳格な管理構成を実現する情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法、並びにコンピュータ・プログラムを提供することを目的とするものである。さらに、例えばコンテンツコードをある特定の再生装置用に作成した場合であって、複数の異なるコンテンツが載った媒体に同じコンテンツコードを記録をする場合に、複数のある特定再生装置用、または、複数のコンテンツで使用可能なコンテンツコードの再利用を容易にすることで、記録媒体のオーサリング時の負担を軽減することを目的とするものである。
【課題を解決するための手段】
【００１２】
本発明の第１の側面は、
情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理装置であり、

情報記録媒体の記録コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードファイルを複数記録した情報記録媒体から、コンテンツコードファイルを取得して、該取得コンテンツコードファイルに従ったデータ処理を実行するデータ処理部を有し、

前記コンテンツコードファイルは、管理センタによる電子署名が付与されており、

前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されており、

前記データ処理部は、

前記コンテンツコードファイルに含まれるコンテンツコード全体の改ざん検証を可能とした前記管理センタによる電子署名の検証処理を実行し、該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに含まれるプログラムに従ったデータ処理を実行する構成であり、更に前記情報記録媒体に記録された複数のコンテンツコードファイルから、前記プレーヤ固有のプログラムを含むコンテンツコードファイルを取得してプレーヤ固有の秘密鍵による署名の検証処理を実行し、該検証の結果、プレーヤ署名設定コンテンツコードファイルの正当性が確認されたことを条件として、前記プレーヤ固有のプログラム処理を実行する構成であることを特徴とする情報処理装置にある。

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記電子署名の検証処理として、管理センタの付与する電子署名の検証処理を実行し、さらに、プレーヤ製造者に固有のプレーヤ秘密鍵を適用して生成された電子署名の検証処理を実行する構成であることを特徴とする。

【００１３】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル各々について、各ファイルに設定された電子署名に基づく署名検証処理を実行する構成であることを特徴とする。

【００１４】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル中、１つのコンテンツコードファイルに設定された電子署名に基づく署名検証処理を実行し、その他の利用コンテンツコードファイルについては、電子署名検証と異なる検証処理を実行する構成であることを特徴とする。

【００１５】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記その他の利用コンテンツコードファイルについては、ハッシュ値に基づく検証処理を実行する構成であることを特徴とする。

【００１６】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記コンテンツコードに含まれる変換テーブルを適用した、コンテンツの一部データの置き換え処理に伴って必要となるデータ処理を実行する構成であることを特徴とする。

【００１７】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、情報記録媒体に記録されたコンテンツの区分領域として設定されたセグメント毎に異なるパラメータであり、前記変換テーブルに含まれる変換エントリの復元に適用するパラメータを算出する処理を実行する構成であることを特徴とする。

【００１８】

さらに、本発明の第２の側面は、

情報記録媒体製造装置であり、

情報記録媒体に記録するコンテンツデータを格納したコンテンツファイルを生成するコ

ンテンツファイル生成手段と、
コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードを格納し、さらに改ざん検証用データとしての電子署名を含む複数のコンテンツコードファイルを生成するコンテンツコードファイル生成手段と、
前記コンテンツファイル生成手段において生成したコンテンツファイル、および前記コンテンツコードファイル生成手段において生成したコンテンツコードファイルを情報記録媒体に記録する記録手段と、
を有し、
前記コンテンツコードファイル生成手段は、管理センタによる電子署名の設定されたコンテンツコードファイルを複数生成し、複数のコンテンツコードファイルのうちの少なくとも一つは、プレーヤ固有のプログラムを含むコンテンツコードを格納し、プレーヤ固有の秘密鍵による署名を更に設定したファイルとして生成する処理を実行することを特徴とする情報記録媒体製造装置にある。

【００１９】
さらに、本発明の情報記録媒体製造装置の一実施態様において、前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名であることを特徴とする。

【００２０】
さらに、本発明の情報記録媒体製造装置の一実施態様において、前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値であることを特徴とする。

【００２１】
さらに、本発明の情報記録媒体製造装置の一実施態様において、前記コンテンツコードファイル生成手段は、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する処理を実行する構成であり、前記記録手段は、前記コンテンツコードファイル生成手段において生成された複数の異なるカテゴリのコンテンツコードファイルを情報記録媒体に記録する処理を実行する構成であることを特徴とする。

【００２３】
さらに、本発明の情報記録媒体製造装置の一実施態様において、前記コンテンツコードファイル生成手段は、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する構成であり、各コンテンツコードファイルを、各ファイルに含まれるコンテンツコードの製作者または提供エンティテイの電子署名を含むファイルとして生成する処理を実行する構成であることを特徴とする。

【００２４】
さらに、本発明の第３の側面は、
情報記録媒体であり、
コンテンツデータを格納したコンテンツファイルと、
コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードを格納し、さらに改ざん検証用データを含む複数のコンテンツコードファイルと、
を格納データとして有し、
前記複数のコンテンツコードファイルは、管理センタによる電子署名が付与されており、前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されているプレーヤ署名設定コンテンツコードファイルであることを特徴とする情報記録媒体にある。
さらに、本発明の情報記録媒体の一実施態様において、前記プレーヤ署名設定コンテンツコードファイルは、プレーヤ特有のコードに対して、プレーヤ製造者の秘密鍵を用いて署名を付加されたデータに対して、更に、管理センタにより署名が付加されたファイルで

あることを特徴とする。

【００２５】

さらに、本発明の情報記録媒体の一実施態様において、前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名であることを特徴とする。

【００２６】

さらに、本発明の情報記録媒体の一実施態様において、前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値であることを特徴とする。

【００２７】

さらに、本発明の情報記録媒体の一実施態様において、前記コンテンツコードファイルは、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルによって構成されていることを特徴とする。

【００２９】

さらに、本発明の情報記録媒体の一実施態様において、前記コンテンツコードファイルは、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルによって構成され、各コンテンツコードファイルには、各ファイルに含まれるコンテンツコードの製作者または提供エンティティの電子署名が含まれる構成であることを特徴とする。

【００３０】

さらに、本発明の第４の側面は、

情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理方法であり、

情報記録媒体の記録コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードファイルを複数記録した情報記録媒体から、コンテンツコードファイルを取得して、コンテンツコードファイルに含まれるコンテンツコード全体の改ざん検証を可能とした電子署名の検証処理を実行する検証処理ステップと、

前記コンテンツコード該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに従ったデータ処理を実行するコード実行ステップと、

を有し、

前記コンテンツコードファイルは、管理センタによる電子署名が付与されており、

前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されており、

前記検証処理ステップは、

前記情報記録媒体に記録された複数のコンテンツコードファイルから、前記プレーヤ固有のプログラムを含むコンテンツコードファイルを取得してプレーヤ固有の秘密鍵による署名の検証処理を実行するステップを含み、

前記コード実行ステップは、

プレーヤ署名設定コンテンツコードファイルの正当性が確認されたことを条件として、前記プレーヤ固有のプログラム処理を実行するステップを含むことを特徴とする情報処理方法にある。

【００３１】

さらに、本発明の情報処理方法の一実施態様において、前記検証処理ステップは、情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテンツコードファイル各々について、各ファイルに設定された電子署名に基づく署名検証処理を実行するステップであることを特徴とする。

【００３２】

さらに、本発明の情報処理方法の一実施態様において、前記検証処理ステップは、情報記録媒体に記録された複数のコンテンツコードファイルから選択される利用対象のコンテ

ンツコードファイル中、１つのコンテンツコードファイルに設定された電子署名に基づく署名検証処理を実行し、その他の利用コンテンツコードファイルについては、電子署名検証と異なる検証処理を実行するステップであることを特徴とする。

【００３３】

さらに、本発明の情報処理方法の一実施態様において、前記検証処理ステップは、前記その他の利用コンテンツコードファイルについては、ハッシュ値に基づく検証処理を実行するステップであることを特徴とする。

【００３４】

さらに、本発明の情報処理方法の一実施態様において、前記コード実行ステップは、前記コンテンツコードに含まれる変換テーブルを適用した、コンテンツの一部データの置き換え処理に伴って必要となるデータ処理を実行するステップであることを特徴とする。

【００３５】

さらに、本発明の情報処理方法の一実施態様において、前記コード実行ステップは、情報記録媒体に記録されたコンテンツの区分領域として設定されたセグメント毎に異なるパラメータであり、前記変換テーブルに含まれる変換エントリの復元に適用するパラメータを算出する処理を実行するステップであることを特徴とする。

【００３６】

さらに、本発明の第５の側面は、

情報記録媒体製造方法であり、

情報記録媒体に記録するコンテンツデータを格納したコンテンツファイルを生成するコンテンツファイル生成ステップと、

コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードを格納し、さらに改ざん検証用データとしての電子署名を含む複数のコンテンツコードファイルを生成するコンテンツコードファイル生成ステップと、

前記コンテンツファイル生成ステップにおいて生成したコンテンツファイル、および前記コンテンツコードファイル生成ステップにおいて生成したコンテンツコードファイルを情報記録媒体に記録する記録ステップと、

を有し、

前記コンテンツコードファイル生成ステップは、管理センタによる電子署名の設定されたコンテンツコードファイルを複数生成し、複数のコンテンツコードファイルのうちの少なくとも一つは、プレーヤ固有のプログラムを含むコンテンツコードを格納し、プレーヤ固有の秘密鍵による署名を更に設定したファイルとして生成する処理を実行するステップを含むことを特徴とする情報記録媒体製造方法にある。

【００３７】

さらに、本発明の情報記録媒体製造方法の一実施態様において、前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名であることを特徴とする。

【００３８】

さらに、本発明の情報記録媒体製造方法の一実施態様において、前記改ざん検証用データは、前記コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値であることを特徴とする。

【００３９】

さらに、本発明の情報記録媒体製造方法の一実施態様において、前記コンテンツコードファイル生成ステップは、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する処理を実行するステップであり、前記記録ステップは、前記コンテンツコードファイル生成ステップにおいて生成された複数の異なるカテゴリのコンテンツコードファイルを情報記録媒体に記録する処理を実行するステップであることを特徴とする。

【００４１】

さらに、本発明の情報記録媒体製造方法の一実施態様において、前記コンテンツコード

ファイル生成ステップは、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成するステップであり、各コンテンツコードファイルを、各ファイルに含まれるコンテンツコードの製作者または提供エンティティの電子署名を含むファイルとして生成する処理を実行するステップであることを特徴とする。

【００４２】

さらに、本発明の第６の側面は、

情報記録媒体に記録されたコンテンツの再生処理を情報処理装置において実行させるコンピュータ・プログラムであり、

情報記録媒体の記録コンテンツの利用の際に実行するプログラムまたはコンテンツ置き換え用データを含むコンテンツコードファイルを複数記録した情報記録媒体から、コンテンツコードファイルを取得して、コンテンツコードファイルに含まれるコンテンツコード全体の改ざん検証を可能とした電子署名の検証処理を実行する検証処理ステップと、

前記コンテンツコード該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに従ったデータ処理を実行するコード実行ステップと、

を有し、

前記コンテンツコードファイルは、管理センタによる電子署名が付与されており、

前記複数のコンテンツコードファイルのうちの少なくとも一つに含まれる前記プログラムはプレーヤ固有のプログラムであり、前記プレーヤ固有のプログラムを含むコンテンツコードファイルには、プレーヤ固有の秘密鍵による署名が更に付与されており、

前記検証処理ステップは、

前記情報記録媒体に記録された複数のコンテンツコードファイルから、前記プレーヤ固有のプログラムを含むコンテンツコードファイルを取得してプレーヤ固有の秘密鍵による署名の検証処理を実行するステップを含み、

前記コード実行ステップは、

プレーヤ署名設定コンテンツコードファイルの正当性が確認されたことを条件として、前記プレーヤ固有のプログラム処理を実行するステップを含むことを特徴とするコンピュータ・プログラムにある。

【００４３】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００４４】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００４５】

本発明の一実施例の構成によれば、情報記録媒体に記録されたコンテンツの再生処理を実行する際に、コンテンツの利用に適用するプログラムまたは適用情報を含むコンテンツコードを取得し、取得コンテンツコードに従ったデータ処理を実行する前の段階において、コンテンツコードを格納したコンテンツコードファイルに設定された電子署名の検証処理を実行し、該検証の結果、コンテンツコードファイルの正当性が確認されたことを条件として、コンテンツコードに従ったデータ処理を実行する構成としたので、不正なコンテンツコードの実行が防止され、コンテンツコードの不正利用によるコンテンツの不正再生、利用を防止することが可能となる。

【００４６】
また、本発明の一実施例の構成によれば、情報記録媒体に記録され情報処理装置において利用されるコンテンツコードファイルが複数設定される場合においても、少なくとも１つのファイルに電子署名を設定して、電子署名の検証による検証の成立を条件としてコンテンツコードの利用を可能とする構成としたので、厳格なコンテンツコードの利用制御が実現される。
【発明を実施するための最良の形態】
【００４７】
以下、図面を参照しながら本発明の情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の記載項目に従って行う。
１．情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要
２．コンテンツ管理ユニット（ＣＰＳユニット）について
３．情報記録媒体の格納データ管理構成
４．変形データを含むコンテンツのデータ構成およびデータ変換処理の概要
５，再生（プレーヤ）アプリケーションとセキュアＶＭ間の処理
６．コンテンツ再生処理
７．コンテンツコードの管理構成
８．情報処理装置の構成
９．情報記録媒体製造装置および情報記録媒体
【００４８】
［１．情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要］
まず、情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要について説明する。図１に、コンテンツの格納された情報記録媒体１００、ドライブ１２０およびホスト１４０の構成を示す。ホスト１４０は、例えばＰＣ等の情報処理装置で実行されるデータ再生（または記録）アプリケーションであり、所定のデータ処理シーケンスに従ってＰＣ等の情報処理装置のハードウェアを利用した処理を行なう。
【００４９】
情報記録媒体１００は、例えば、Ｂｌｕ－ｒａｙ Ｄｉｓｃ（商標）、ＤＶＤなどの情報記録媒体であり、正当なコンテンツ著作権、あるいは頒布権を持ついわゆるコンテンツ権利者の許可の下にディスク製造工場において製造された正当なコンテンツを格納した情報記録媒体（ＲＯＭディスクなど）、あるいはデータ記録可能な情報記録媒体（ＲＥディスクなど）である。なお、以下の実施例では、情報記録媒体の例としてディスク型の媒体を例として説明するが、本発明は様々な態様の情報記録媒体を用いた構成において適用可能である。
【００５０】
図１に示すように、情報記録媒体１００には、暗号化処理および一部データの置き換え処理の施された暗号化コンテンツ１０１と、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのＭＫＢ（Media Key Block）１０２、コンテンツ復号処理に適用するタイトル鍵を暗号化したデータ（Encrypted CPS Unit Key）等から構成されるタイトル鍵ファイル１０３、コンテンツのコピー・再生制御情報としてのＣＣＩ（Copy Control Information）等を含む使用許諾情報１０４、暗号化コンテンツ１０１の利用に際して実行されるデータ処理プログラムを含むコンテンツコード１０５が格納される。
【００５１】
コンテンツコード１０５には、コンテンツ中の所定領域の置き換えデータに対応する変換データを登録した変換テーブル（Ｆｉｘ－ｕｐ Ｔａｂｌｅ）１０６が含まれる。コンテンツの再生を実行する情報処理装置は、コンテンツコード１０５に含まれるデータ変換処理プログラムに従って、コンテンツコード１０５に含まれる変換テーブル（Ｆｉｘ－ｕｐ Ｔａｂｌｅ）１０６に記録された変換データを取り出して、コンテンツの構成データ

の置き換え処理を行なう。

【００５２】

コンテンツコードは、変換データを適用した変換処理プログラムの他、スタートアップ処理や、セキュリティチェック処理などの様々な処理を実行するための情報やプログラムが含まれる。コンテンツコードの詳細については、後段で詳細に説明する。なお、図に示す情報記録媒体格納データ例は一例であり、格納データは、ディスクの種類などによって多少異なる。以下、これらの各種情報の概要について説明する。

【００５３】

（１）暗号化コンテンツ１０１

情報記録媒体１００には、様々なコンテンツが格納される。例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツのＡＶ(Audio Visual)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。これらのコンテンツは、特定のＡＶフォーマット規格データであり、特定のＡＶデータフォーマットに従って格納される。具体的には、例えばＢｌｕ－ｒａｙ　Ｄｉｓｃ（商標）ＲＯＭ規格データとして、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（商標）ＲＯＭ規格フォーマットに従って格納される。

【００５４】

さらに、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどが格納される場合もある。これらのコンテンツは、特定のＡＶデータフォーマットに従わないデータフォーマットを持つデータとして格納される場合もある。

【００５５】

コンテンツの種類としては、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなど、様々なコンテンツが含まれ、これらのコンテンツには、情報記録媒体１００からのデータのみによって利用可能なコンテンツ情報と、情報記録媒体１００からのデータと、ネットワーク接続されたサーバから提供されるデータとを併せて利用可能となるコンテンツ情報など、様々な態様の情報が含まれる。情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵（ＣＰＳユニット鍵またはユニット鍵（あるいはタイトル鍵と呼ぶ場合もある））が割り当てられ暗号化されて格納される。１つのユニット鍵を割り当てる単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。さらに、コンテンツは、構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録されたデータに置き換える処理が必要となる。これらの処理は後段で詳細に説明する。

【００５６】

（２）ＭＫＢ

ＭＫＢ（Media Key Block）１０２は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。ＭＫＢ１０２は有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式を適用したものであり、ユーザデバイス（情報処理装置）が有効なライセンスを持つ場合にのみ、メディア鍵［Ｋｍ］の取得を可能とし、無効化（リボーク処理）されたユーザデバイスにおいては、メディア鍵［Ｋｍ］の取得が不可能となる。

【００５７】

ライセンスエンティテイとしての管理センタはＭＫＢに格納する鍵情報の暗号化に用いるデバイス鍵の変更により、特定のユーザデバイスに格納されたデバイス鍵では復号できない、すなわちコンテンツ復号に必要なメディア鍵を取得できない構成を持つＭＫＢを生成することができる。従って、任意タイミングで不正デバイスを排除（リボーク）して、

有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。コンテンツの復号処理については後述する。

【００５８】

（３）タイトル鍵ファイル

前述したように各コンテンツまたは複数コンテンツの集合は、コンテンツの利用管理のため、各々、個別の暗号鍵（タイトル鍵（ＣＰＳユニット鍵））を適用した暗号化がなされて情報記録媒体１００に格納される。すなわち、コンテンツを構成するＡＶ(Audio Visual)ストリーム、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なるタイトル鍵を生成して、復号処理を行なうことが必要となる。このタイトル鍵を生成するための情報がタイトル鍵データであり、例えばメディア鍵等によって生成された鍵で暗号化タイトル鍵を復号することによってタイトル鍵を得る。タイトル鍵データを適用した所定の暗号鍵生成シーケンスに従って、各ユニット対応のタイトル鍵が生成され、コンテンツの復号が実行される。

【００５９】

（４）使用許諾情報

使用許諾情報には、例えばコピー・再生制御情報（ＣＣＩ）が含まれる。すなわち、情報記録媒体１００に格納された暗号化コンテンツ１０１に対応する利用制御のためのコピー制限情報や、再生制限情報である。このコピー・再生制御情報（ＣＣＩ）は、コンテンツ管理ユニットとして設定されるＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。

【００６０】

（５）コンテンツコード

コンテンツコード１０５は、暗号化コンテンツ１０１の利用に際して実行されるデータ処理プログラムを含むデータである。コンテンツ再生を実行するホストは、データ変換処理を実行するバーチャルマシン（ＶＭ）を設定し、バーチャルマシン（ＶＭ）において、情報記録媒体１００から読み出したコンテンツコードに従って、データ変換処理を実行して、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０６の登録エントリを適用して、コンテンツの一部構成データのデータ変換処理を実行する。

【００６１】

情報記録媒体１００に格納された暗号化コンテンツ１０１は、所定の暗号化が施されているとともに、コンテンツ構成データの一部が、正しいデータと異なるブロークンデータによって構成されている。コンテンツ再生に際しては、このブロークンデータを正しいコンテンツデータである変換データに置き換えるデータ上書き処理が必要となる。この変換データを登録したテーブルが変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０６である。ブロークンデータはコンテンツ中に散在して多数設定され、コンテンツ再生に際しては、これらの複数のブロークンデータを変換テーブルに登録された変換データに置き換える（上書き）する処理が必要となる。この変換データを適用することにより、例えば、暗号鍵が漏洩しコンテンツの復号が不正に行なわれた場合であっても、コンテンツの復号のみでは、置き換えデータの存在によって正しいコンテンツの再生が不可能となり、不正なコンテンツ利用を防止することができる。

【００６２】

なお、変換テーブル１０６には、通常の変換データに加え、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータを含む変換データが含まれる。具体的には、例えば、プレーヤ（ホストアプリケーションを実行する装置）の識別データとしてのプレーヤＩＤあるいはプレーヤＩＤに基づいて生成された識別情報が記録された「識別マークを含む変換データ」が含まれる。識別マークを含む変換データは、コンテンツの再生に影響を与えないレベルで、正しいコンテンツデータのビット値をわずかに変更したデータである。

【００６３】

なお、コンテンツコード１０５には、上述した変換テーブル１０６を適用したデータ変換処理プログラムの他、スタートアップ処理や、セキュリティチェック処理などの様々な処理を実行するための情報やプログラムが含まれる。コンテンツコードの詳細については、後段で詳細に説明する。

【００６４】

次に、ホスト１４０とドライブ１２０の構成、処理の概要について、図１を参照して説明する。情報記録媒体１００に格納されたコンテンツの再生処理は、ドライブ１２０を介してホスト１４０にデータが転送されて実行される。

【００６５】

ホスト１４０には、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０が設定される。再生（プレーヤ）アプリケーション１５０は、コンテンツ再生処理部であり、コンテンツ再生処理において実行するドライブとの認証処理、コンテンツ復号、デコード処理などの処理を実行する。セキュアＶＭ１６０は、例えば、コンテンツ再生処理部である再生（プレーヤ）アプリケーション１５０の実行するコンテンツ再生処理において実行するデータ変換処理において適用するパラメータを提供するパラメータ生成部として機能する。セキュアＶＭ１６０は、ホスト１４０内にバーチャルマシンとして設定される。バーチャルマシン（ＶＭ）は中間言語を直接解釈して実行する仮想コンピュータであり、プラットホームに依存しない中間言語での命令コード情報を情報記録媒体１００から読み出して解釈実行する。

【００６６】

セキュアＶＭ１６０は、情報記録媒体１００に記録された暗号化コンテンツ１０１の利用に適用するプログラムまたは適用情報を含むコンテンツコード１０５を取得して、取得したコンテンツコード１０５に従ってコードを実行し、データ処理を行なうデータ処理部として機能する。

【００６７】

再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間の情報伝達、あるいは処理要求は、再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理のシーケンスによって実行される。アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理のシーケンスによって、コンテンツ再生処理において実行するデータ変換処理において適用するパラメータの算出要求、およびパラメータ提供が行われる。これらの処理シーケンスの詳細については後段で説明する。

【００６８】

ホスト１４０の実行する主な処理について説明する。コンテンツの利用に先立ち、ドライブ１２０と、ホスト１４０間では相互認証処理が実行され、この認証処理の成立によって双方の正当性が確認された後、ドライブからホストに暗号化コンテンツが転送され、ホスト側でコンテンツの復号処理が行なわれ、さらに上述の変換テーブルによるデータ変換処理が実行されてコンテンツ再生が行なわれる。

【００６９】

ホスト１４０と、ドライブ１２０間において実行する相互認証においては、各機器またはアプリケーションが不正な機器またはアプリケーションとして登録されていないかを示す管理センタの発行したリボケーション（無効化）リストを参照して、正当性を判定する処理を実行する。

【００７０】

ドライブ１２０は、ホストの証明書（公開鍵証明書）のリボーク（無効化）情報を格納したホストＣＲＬ（Certificate Revocation List）を格納するためのメモリ１２２を有する。一方、ホスト１４０は、ドライブの証明書（公開鍵証明書）のリボーク（無効化）情報を格納したドライブＣＲＬ（Certificate Revocation List）を格納するためのメモ

リ１５２を有する。メモリは不揮発性メモリ（ＮＶＲＡＭ）であり、例えば、情報記録媒体１００から読み出されるＣＲＬがより新しいバージョンである場合には、それぞれのデータ処理部１２１，１５１は、メモリ１２２．１５２に新しいバージョンのホストＣＲＬまたはドライブＣＲＬを格納する更新処理を行なう。

【００７１】

ホストＣＲＬ、ドライブＣＲＬ等のＣＲＬは管理センタが逐次更新する。すなわち新たな不正機器が発覚した場合、その不正機器に対して発行された証明書のＩＤまたは機器ＩＤなどを新規エントリとし追加した更新ＣＲＬを発行する。各ＣＲＬにはバージョン番号が付与されており、新旧比較が可能な構成となっている。例えばドライブが装着した情報記録媒体から読み出されたＣＲＬが、ドライブ内のメモリ１２２に格納されたＣＲＬより新しい場合、ドライブは、ＣＲＬの更新処理を実行する。ホスト１４０も同様に、ドライブＣＲＬの更新を実行する。

【００７２】

ドライブ１２０のデータ処理部１２１は、このＣＲＬの更新処理の他、コンテンツ利用に際して実行されるホストとの認証処理、さらに、情報記録媒体からのデータ読み出し、ホストへのデータ転送処理などを実行する。

【００７３】

ホスト１４０の再生（プレーや）アプリケーション１５０は、例えばＰＣ等の情報処理装置で実行されるデータ再生（または記録）アプリケーションであり、所定のデータ処理シーケンスに従ってＰＣ等の情報処理装置のハードウェアを利用した処理を行なう。

【００７４】

ホスト１４０は、ドライブ１２０との相互認証処理や、データ転送制御などを実行するデータ処理部１５１、暗号化コンテンツの復号処理を実行する復号処理部１５３、前述の変換テーブル１０５の登録データに基づくデータ変換処理を実行するデータ変換処理部１５４、デコード（例えばＭＰＥＧデコード）処理を実行するデコード処理部１５５を有する。

【００７５】

データ処理部１５１は、ホスト－ドライブ間の認証処理を実行し、認証処理においては、不揮発性メモリ（ＮＶＲＡＭ）としてのメモリａ１５２に格納されたドライブＣＲＬを参照して、ドライブがリボークされたドライブでないことを確認する。ホストも、また、メモリａ１５２に新しいバージョンのドライブＣＲＬを格納する更新処理を行なう。

【００７６】

復号処理部１５３では、メモリｂ１５６に格納された各種情報、および、情報記録媒体１００からの読み取りデータを適用して、コンテンツの復号に適用する鍵を生成し、暗号化コンテンツ１０１の復号処理を実行する。データ変換処理部１５４は、情報記録媒体１００から取得されるデータ変換処理プログラムに従って、情報記録媒体１００から取得される変換テーブルに登録された変換データを適用してコンテンツの構成データの置き換え処理（上書き）を実行する。デコード処理部１５５は、デコード（例えばＭＰＥＧデコード）処理を実行する。

【００７７】

情報処理装置１５０のメモリｂ１５６には、デバイス鍵：Ｋｄや、相互認証処理に適用する鍵情報や復号に適用する鍵情報などが格納される。なお、コンテンツの復号処理の詳細については後述する。デバイス鍵：Ｋｄは、先に説明したＭＫＢの処理に適用する鍵である。ＭＫＢは有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックであり、暗号化コンテンツの復号に際して、情報処理装置１５０は、メモリｂ１５６に格納されたデバイス鍵：Ｋｄを適用してＭＫＢの処理を実行することになる。なお、コンテンツの復号処理の詳細については後述する。

【００７８】

［２．コンテンツ管理ユニット（ＣＰＳユニット）について］

前述したように、情報記録媒体に格納されるコンテンツは、ユニット毎の異なる利用制御を実現するため、ユニット毎に異なる鍵が割り当てられ暗号化処理がなされて格納される。すなわち、コンテンツはコンテンツ管理ユニット（ＣＰＳユニット）に区分されて、個別の暗号化処理がなされ、個別の利用管理がなされる。

【００７９】

コンテンツ利用に際しては、まず、各ユニットに割り当てられたＣＰＳユニット鍵（タイトル鍵とも呼ばれる）を取得することが必要であり、さらに、その他の必要な鍵、鍵生成情報等を適用して予め定められた復号処理シーケンスに基づくデータ処理を実行して再生を行う。コンテンツ管理ユニット（ＣＰＳユニット）の設定態様について、図２を参照して説明する。

【００８０】

図２に示すように、コンテンツは、（Ａ）インデックス２１０、（Ｂ）ムービーオブジェクト２２０、（Ｃ）プレイリスト２３０、（Ｄ）クリップ２４０の階層構成を有する。再生アプリケーションによってアクセスされるタイトルなどのインデックスを指定すると、例えばタイトルに関連付けられた再生プログラムが指定され、指定された再生プログラムのプログラム情報に従ってコンテンツの再生順等を規定したプレイリストが選択される。

【００８１】

プレイリストには、再生対象データ情報としてのプレイアイテムが含まれる。プレイリストに含まれるプレイアイテムによって規定される再生区間としてのクリップ情報によって、コンテンツ実データとしてのＡＶストリームあるいはコマンドが選択的に読み出されて、ＡＶストリームの再生、コマンドの実行処理が行われる。なお、プレイリスト、プレイアイテムは多数、存在し、それぞれに識別情報としてのプレイリストＩＤ、プレイアイテムＩＤが対応付けられている。

【００８２】

図２には、２つのＣＰＳユニットを示している。これらは、情報記録媒体に格納されたコンテンツの一部を構成している。ＣＰＳユニット１，２７１、ＣＰＳユニット２，２７２の各々は、インデックスとしてのタイトルと、再生プログラムファイルとしてのムービーオブジェクトと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイルを含むクリップを含むユニットとして設定されたＣＰＳユニットである。

【００８３】

コンテンツ管理ユニット（ＣＰＳユニット）１，２７１には、タイトル１，２１１とタイトル２，２１２、再生プログラム２２１，２２２、プレイリスト２３１，２３２、クリップ２４１、クリップ２４２が含まれ、これらの２つのクリップ２４１，２４２に含まれるコンテンツの実データであるＡＶストリームデータファイル２６１，２６２が、少なくとも暗号化対象データであり、原則的にコンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定される暗号鍵であるタイトル鍵（Ｋｔ１）（ＣＰＳユニット鍵とも呼ばれる）を適用して暗号化されたデータとして設定される。

【００８４】

コンテンツ管理ユニット（ＣＰＳユニット）２，２７２には、インデックスとしてアプリケーション１，２１３、再生プログラム２２４、プレイリスト２３３、クリップ２４３が含まれ、クリップ２４３に含まれるコンテンツの実データであるＡＶストリームデータファイル２６３がコンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定される暗号鍵である暗号鍵であるタイトル鍵（Ｋｔ２）適用して暗号化される。

【００８５】

例えば、ユーザがコンテンツ管理ユニット１，２７１に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定された暗号鍵としてのタイトル鍵：Ｋｔ１を取得して復号処理を実行することが必要となる。コンテンツ管理ユニット２，２７２に対応する

アプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定された暗号鍵としてのタイトル鍵：Ｋｔ２を取得して復号処理を実行することが必要となる。

【００８６】

ＣＰＳユニットの設定構成、およびタイトル鍵の対応例を図３に示す。図３には、情報記録媒体に格納される暗号化コンテンツの利用管理単位としてのＣＰＳユニット設定単位と、各ＣＰＳユニットに適用するタイトル鍵（ＣＰＳユニット鍵）の対応を示している。なお、予め後発データ用のＣＰＳユニットおよびタイトル鍵を格納して設定しておくことも可能である。例えばデータ部２８１が後発データ用のエントリである。

【００８７】

ＣＰＳユニット設定単位は、コンテンツのタイトル、アプリケーション、データグループなど、様々であり、ＣＰＳユニット管理テーブルには、それぞれのＣＰＳユニットに対応する識別子としてのＣＰＳユニットＩＤが設定される。

【００８８】

図３において、例えばタイトル１はＣＰＳユニット１であり、ＣＰＳユニット１に属する暗号化コンテンツの復号に際しては、タイトル鍵Ｋｔ１を生成し、生成したタイトル鍵Ｋｔ１に基づく復号処理を行なうことが必用となる。

【００８９】

このように、情報記録媒体１００に格納されるコンテンツは、ユニット毎の異なる利用制御を実現するため、ユニット毎に異なる鍵が割り当てられ暗号化処理がなされて格納される。各コンテンツ管理ユニット（ＣＰＳユニット）に対する個別の利用管理のために、各コンテンツ管理ユニット（ＣＰＳユニット）に対する使用許諾情報（ＵＲ：Ｕｓａｇｅ Ｒｕｌｅ）が設定されている。使用許諾情報は、前述したように、コンテンツに対する例えばコピー・再生制御情報（ＣＣＩ）を含む情報であり、各コンテンツ管理ユニット（ＣＰＳユニット）に含まれる暗号化コンテンツのコピー制限情報や、再生制限情報である。

【００９０】

なお、タイトル鍵の生成には、情報記録媒体に格納された様々な情報を適用したデータ処理が必要となる。これらの処理の具体例についは、後段で詳細に説明する。

【００９１】

［３．情報記録媒体の格納データ管理構成］

次に、情報記録媒体の格納データ管理構成について説明する。図２を参照して説明した階層構造を持つコンテンツを情報記録媒体に格納する場合、様々なデータ、あるいはコンテンツコード等のプログラムなどは、個別のファイルとして記録される。図４を参照して、情報記録媒体に格納される各データに対応するディレクトリ構成について説明する。

（Ａ）図２におけるインデックス２１０は、図４に示すディレクトリ中のindex.bdmvファイル

（Ｂ）図２におけるムービーオブジェクト２２０は図４に示すディレクトリ中のMovieObject.bdmvファイル

（Ｃ）図２におけるプレイリスト２３０は図４に示すディレクトリ中のPLAYLISTディレクトリ下のファイル、

（Ｄ）図２におけるクリップ２４０は図４に示すディレクトリ中のCLIPINFディレクトリ下のファイルとSTREAMディレクトリ下のファイルで同じファイル番号を持つものに対応する。

（Ｅ）その他、音声データやフォントデータを格納したＡＵＸＤＡＴＡファイル、メタデータを格納したＭＥＴＡファイル、ＢＤ－Ｊオブジェクトを格納したＢＤＯＪファイルなどが情報記録媒体に格納される。

【００９２】

情報記録媒体に格納されるコンテンツは、前述したように、コンテンツの構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデー

タとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録されたデータ（変換データ）に置き換える処理が必要となる。この置き換え処理には、情報記録媒体に格納されたコンテンツコード１０５を適用して、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０６の登録データによるデータ変換処理を実行する。

【００９３】

この変換テーブルを含むコンテンツコードについても、個別のファイルとして情報記録媒体に格納される。コンテンツコードを設定したディレクトリ構成を図５に示す。図５は、例えば、図４のディレクトリ構造を持つＡＶコンテンツに対して作成されるコンテンツコードのディレクトリ構成である。

【００９４】

コンテンツコードは、前述したように変換テーブルを含み、変換テーブルを適用したデータ変換処理プログラムの他、スタートアップ処理や、セキュリティチェック処理などの様々な処理を実行するための情報やプログラムが含まれる。これらのコンテンツコードは、大きく分けると、

（ａ）全コンテンツ＆全プレーヤ（装置または再生アプリ）共通のコンテンツコード

（ｂ）コンテンツ固有のコンテンツコード

（ｃ）プレーヤ（装置または再生アプリ）固有のコンテンツコード

（ｄ）コンテンツ＆プレーヤ（装置または再生アプリ）固有のコンテンツコード

の各カテゴリに分類され、各コンテンツコードは、その製作エンティテイ、提供エンティが異なっている。従って、これらの異なるカテゴリのコンテンツコードは独立したファイルとしてそれぞれ設定することが、例えばファイルの再利用等の観点から好ましい。

【００９５】

図５に示すコンテンツコードファイル［００００００．ｓｖｍ］～［００００３．ｓｖｍ］は、これらの異なるエンティテイによって生成された異なるカテゴリの独立したコンテンツコードファイルを示している。なお、コンテンツコードファイルの具体的な例については、後段で詳細に説明する。

【００９６】

図５に示すように、コンテンツコードは、ＢＤＳＶＭディレクテリに、複数の個別のファイルとして設定され、さらに、ＢＡＣＫＵＰディレクトリにコピーデータとしてのバックアップデータが設定される。

【００９７】

［４．変形データを含むコンテンツのデータ構成およびデータ変換処理の概要］

次に、変形データを含むコンテンツの構成およびデータ変換処理の概要について説明する。情報記録媒体１００に含まれる暗号化コンテンツ１０１は、前述したように、構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録された変換データに置き換える処理が必要となる。

【００９８】

図６を参照して、情報記録媒体に格納されるコンテンツの構成および再生処理の概要について説明する。情報記録媒体１００には例えば映画などのＡＶ（Audio Visual）コンテンツが格納される。これらのコンテンツは暗号化が施され、所定のライランスを持つ再生装置においてのみ取得可能な暗号鍵を適用した処理によって復号の後、コンテンツ再生が可能となる。具体的なコンテンツ再生処理については後段で説明する。情報記録媒体１００に格納されるコンテンツは、暗号化のみならず、コンテンツの構成データが変形データによって置き換えられた構成を持つ。

【００９９】

図６には、情報記録媒体１００に格納される記録コンテンツ２９１の構成例を示している。記録コンテンツ２９１は変形のされていない正常なコンテンツデータ２９２と、変形

が加えられ破壊されたコンテンツであるブロークンデータ２９３によって構成される。ブロークンデータ２９３は、本来のコンテンツに対してデータ処理によって破壊が施されたデータである。従って、このブロークンデータを含むコンテンツ２９１を適用して正常なコンテンツ再生は実行できない。

【０１００】

コンテンツ再生を行なうためには、記録コンテンツ２９１に含まれるブロークンデータ２９３を正常なコンテンツデータに置き換える処理を行なって再生コンテンツ２９６を生成することが必要となる。各ブロークンデータ領域に対応する正常なコンテンツデータとしての変換用のデータ（変換データ）は、情報記録媒体１００に記録されたコンテンツコード１０５内の変換テーブル（ＦＵＴ(Fix-Up Table)）１０６（図１参照）に登録された変換エントリ２９５から変換データを取得して、ブロークンデータ領域のデータを置き換える処理を実行して、再生コンテンツ２９６を生成して再生を実行する。

【０１０１】

なお、再生コンテンツ２９６の生成に際しては、ブロークンデータ２９３を正常なコンテンツデータとしての変換データ２９７に置き換える処理に加え、記録コンテンツ２９１の一部領域を、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報（例えばプレーヤＩＤ）の構成ビットを解析可能としたデータを含む識別子設定変換データ２９８によって置き換える処理を行なう。例えば、不正にコピーされたコンテンツが流出した場合、流出コンテンツ中の識別子設定変換データ２９８の解析によって、不正コンテンツの流出源を特定することが可能となる。

【０１０２】

なお、変換データを含む変換テーブルの構成データとしての変換エントリは、コンテンツの構成データ中の特定パケットに分散して重複記録する構成としてもよい。すなわち、変換データは、図１に示す変換テーブル１０６に格納されるとともに、暗号化コンテンツ１０１にも分散記録され、重複して記録される。コンテンツ再生を実行する情報処理装置は、変換テーブル１０６に格納された変換データを取得してデータ置き換えを実行するか、あるいはコンテンツに分散は記録された変換エントリを取得してデータ置き換えを実行するかのいずれかの処理を行なう。

【０１０３】

図７を参照して、情報記録媒体１００に格納される暗号化コンテンツ３００と、データ変換処理実行プログラムと変換テーブルを含むコンテンツコード３０２の構成例について説明する。情報記録媒体１００に記録されるコンテンツコード３０２－０～ｎは、例えば各コンテンツあるいは各クリップ対応の独立したファイルイデータとして情報記録媒体に記録される。図に示す例では、ｎ＋１個のコンテンツコード３０２－０～ｎが情報記録媒体１００に記録された例を示している。

【０１０４】

各コンテンツコード３０２－０～ｎには、それぞれ変換テーブル３０３－０～ｎが含まれる。各変換テーブル３０３－０～ｎの各々には、実際にコンテンツの置き換えデータとして利用される変換データと、その記録位置情報を設定した変換エントリ３０４－０～ｎが記録される。なお、図に示す例では、暗号化コンテンツ３００－０～ｎとコンテンツコード３０２－０～ｎ、変換テーブル３０３－０～ｎとして、すべて変数［ｎ］を適用して示しているが、暗号化コンテンツ３００とコンテンツコード３０２の設定数は同一であることは必要でない。例えば、コンテンツコード３０２－０に、暗号化コンテンツ０～ｎに対応する全ての変換テーブルを記録する構成としてもよい。このように、暗号化コンテンツとコンテンツコードは必ずしも一対一に対応するものではない。

【０１０５】

変換エントリの各々には、置き換えデータとして適用される変換データと変換データの記録位置情報が含まれる。図８を参照して、変換テーブル中に記録される変換エントリのデータ構成について説明する。

【０１０６】

図８は、変換テーブブロックに含まれる１つの変換エントリ（FixUpEntry）のデータ構成例を示している。図８に示すように、変換エントリ（FixUpEntry）には以下のデータが含まれる。

type_indicator：タイプ識別子[00:変換なし，01b:変換データによる処理，10b,11b:識別子設定変換データによる処理]

FM_ID_bit_position：識別子設定変換データに対応するプレーヤＩＤの識別ビット位置

relative_SPN：変換データ適用パケット位置（プログラマブルマップテーブル（ＰＭＴ）格納パケットからのパケット数）

byte_position：パケット内の変換データ記録位置

overwrite_value：変換データ（識別子設定変換データも含む）

relative_SPN_2：第２変換データ適用パケット位置（ＰＭＴパケットからのパケット数）

byte_position_2：パケット内の変換データ記録位置（第２変換データ対応）

overwrite_value_2：第２変換データ（識別子設定変換データも含む）

これらのデータによって構成される。

【０１０７】

変換エントリは、コンテンツデータの一部の置き換え対象となる変換データと、該変換データのコンテンツに対する設定位置情報を記録したデータとして設定され、この変換エントリを変換テーブルから読み出して、コンテンツ構成データの置き換え処理実行命令を含む変換処理プログラムとしてのコンテンツコードを実行して、データ変換が行われる。

【０１０８】

図８に示す変換エントリ（FixUpEntry）情報に含まれる情報［type_indicator］は、変換データが、

（ａ）ブロークンデータを正当なコンテンツデータに変換するための変換データに関する登録情報であるか、または、

（ｂ）再生装置又はコンテンツ再生アプリケーションの識別情報を埋めこむための識別子設定変換データに関する登録情報であるか、

上記（ａ）、（ｂ）のいずれの登録情報であるかを識別するタイプ識別子である。

【０１０９】

登録情報［FM_ID_bit_position］は、複数ビットからなる再生装置又は再生アプリケーションの識別情報中、処理態様決定のために参照すべきビットの位置情報である。例えば、複数ビットからなる再生装置又は再生アプリケーションの識別情報中、処理態様決定のために参照すべきビットのビット値が１である場合、変換テーブルに登録された識別子設定変換データによってコンテンツ構成データの置き換えを実行し、参照すべきビットのビット値が０である場合には置き換えを実行しないといった処理態様が決定されてデータ変換が実行される。

【０１１０】

なお、参照ビットが０の場合に変換を実行し、１の場合に変換を実行しないとする設定も可能である。また参照ビットが０の場合の変換データと、１の場合の変換データをそれぞれ別の変換データとして設定し、参照ビットのビット値に応じて、適宜、変換データを選択して設定する構成としてもよい。

【０１１１】

図７に示すように、暗号化コンテンツ３００－０～ｎの各々にも、変換エントリ３０１－０～ｎが分散記録されている。暗号化コンテンツ３００は、ＴＳパケットのストリームとして設定され、その一部に変換エントリが散在して格納されたパケット、すなわち変換エントリ格納パケット３０７ａ～３０７ｄが設定される。

【０１１２】

これらの分散記録データとして設定される各変換エントリには、各変換エントリ格納パケットの近傍の変換データが記録されている。暗号化コンテンツ３００に分散記録された変換エントリと、変換テーブル３０３に含まれる変換エントリは同じものであり、コンテ

ンツ再生を実行する情報処理装置は、再生（プレーヤ）アプリケーションの仕様に応じて、コンテンツに分散記録された変換エントリ３０１から変換データを取得してデータ置き換えを実行するか、あるいは、変換テーブル３０３中の変換エントリ３０４から変換データを取得してデータ置き換えを実行するかいずれか一方の処理を実行する。

【０１１３】

コンテンツは、図７に示すように、所定データ単位ごとのセグメント（ＳＰセグメント）として区分されている。各変換データを含む変換エントリは、コンテンツの所定データ単位（セグメント単位）ごとに異なるパラメータ（ＳＰ：シークレットパラメータ）を適用した演算または暗号化処理が実行されて、変換テーブル３０３に格納されている。コンテンツ中のＴＳパケットに格納された変換エントリも、同様に、セグメント単位）ごとに異なるパラメータ（ＳＰ：シークレットパラメータ）を適用した演算または暗号化処理が実行されて記録されている。

【０１１４】

コンテンツ再生の際に実行するデータの置き換え処理としてのデータ変換処理を実行する情報処理装置は、各セグメントに対応するシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）順次、取得して、各セグメント位置に対応する変換エントリに対して、取得パラメータ（ＳＰｎ）を適用した演算または暗号処理を実行して、変換データを取得する処理を行なう。

【０１１５】

図９、図１０を参照して、変換データに基づくデータ置き換えの具体例について説明する。まず、図９を参照して、コンテンツに分散記録された変換データを含む変換テーブルブロック構成データを取得して、データ置き換えを実行する処理例について説明する。

【０１１６】

図９（ａ）は、情報記録媒体１００に記録されたコンテンツ構成を示している。変換データと記録位置情報を含む変換エントリが図に示すＴＳパケット３０７ａ～ｄに分散記録されている。

【０１１７】

データ置き換え処理シーケンスについて、図９（ｂ）を参照して説明する。図９（ｂ）に示す処理は、ホストの再生（プレーヤ）アプリケーションの実行する処理である。図９（ｂ）には、コンテンツ構成データ中の、セグメントＩＤ＝Ｎ，Ｎ＋１に属するコンテンツのＴＳパケット列の一部を示している。

【０１１８】

例えば、セグメントＩＤ＝Ｎに記録された変換エントリを含むパケット３１１には、シークレットパラメータ（ＳＰｘ）と排他論理和演算された結果データとしてのＸＯＲｅｄ変換エントリ３１５が格納されている。データ置き換え処理を実行するホストの再生（プレーヤ）アプリケーションは、ＸＯＲｅｄ変換エントリ３１５に対して、シークレットパラメータ（ＳＰｘ）３１６との排他論理和演算を実行して変換エントリ３１７を取得して、変換エントリ３１７から変換データと記録位置情報を取得し、データ置き換え対象位置のパケット３１２ａ，ｂとの置き換え処理を実行する。

【０１１９】

変換エントリ３１７を取得するための演算に適用するパラメータ（ＳＰｘ）は、セキュアＶＭ３２０から供給を受ける。例えば、再生（プレーヤ）アプリケーションは、コンテンツの各セグメントにおいて必要なシークレットパラメータ（ＳＰｎ）を取得するため、各セグメントに対応するシークレットパラメータ指定情報としてのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得して、シークレットパラメータＩＤの通知を含むシークレットパラメータ算出要求を、セキュアＶＭに対する割り込み（ＩＮＴＲＰ）要求として出力する。セキュアＶＭは、再生（プレーヤ）アプリケーションからのシークレットパラメータ算出要求に応じて、ＳＰ＿ＩＤ対応のシークレットパラメータ（ＳＰｘ）を算出し、応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーションに提供する。

【０１２０】

図９に示すように、セグメントが異なると、変換エントリを取得するための演算に適用するパラメータ（ＳＰｘ）は異なるパラメータとなる。例えば、１つのセグメントはコンテンツ再生時間として約１０秒程度に設定され、再生（プレーヤ）アプリケーションは、約１０秒の各セグメント毎に異なるパラメータをセキュアＶＭから受領して、変換エントリを復元して、復元した変換エントリから変換データを取得し、データ置き換え処理を実行する。

【０１２１】

次に、図１０を参照して、コンテンツ中に分散記録された変換エントリではなく情報記録媒体に格納されたコンテンツコード３０２の変換テーブル３０３内の変換エントリ３０４を適用して、コンテンツに対するデータ置き換えを行なう場合の処理概要について説明する。

【０１２２】

コンテンツは、図９を用いて説明したのと同様に、図１０（ａ）に示すように、所定データ単位ごとのセグメントとして区分されている。変換テーブル３０３に記録された変換データを含む変換エントリ３０４は、コンテンツの所定データ単位（セグメント単位）ごとに異なるパラメータ（ＳＰ：シークレットパラメータ）を適用した演算または暗号化処理が実行されている。

【０１２３】

コンテンツ再生の際に実行するデータの置き換え処理としてのデータ変換処理を実行する情報処理装置は、各セグメントに対応するシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）順次、取得して、各セグメント位置に対応する変換データを含む変換エントリに対して、取得パラメータ（ＳＰｎ）を適用した演算または暗号処理を実行して、変換データを取得する処理を行なう。

【０１２４】

データ置き換え処理シーケンスについて、図１０（ｂ）を参照して説明する。図１０（ｂ）に示す処理は、ホストの再生（プレーヤ）アプリケーションの実行する処理である。図１０（ｂ）には、コンテンツ構成データ中の、セグメントＩＤ＝Ｎ，Ｎ＋１に属するコンテンツのＴＳパケット列の一部を示している。

【０１２５】

例えば、セグメントＩＤ＝Ｎについてのデータ置き換えを実行する場合、変換テーブル３０３から変換エントリ３０４を取得し、変換エントリ３０４から、セグメントＩＤ＝Ｎに対応する変換エントリを選択する。しかし、この変換エントリｘ３１５は、セグメントＮに対応付けられたセグメント固有のシークレットパラメータ（ＳＰｘ）と排他論理和演算された結果データとしてのＸＯＲｅｄ変換エントリ３１５として変換テーブル３０３に記録されている。

【０１２６】

データ置き換え処理を実行するホストの再生（プレーヤ）アプリケーションは、ＸＯＲｅｄ変換エントリ３１５に対して、セキュアＶＭ３２０から提供されるシークレットパラメータ（ＳＰｘ）３１６との排他論理和演算を実行して変換エントリ３１７を取得して、変換エントリ３１７から変換データと記録位置情報を取得し、データ置き換え対象位置のパケット３１２ａ，ｂとの置き換え処理を実行する。

【０１２７】

変換エントリ３１７を取得するための演算に適用するパラメータ（ＳＰｘ）は、セキュアＶＭ３２０から供給を受ける。例えば、再生（プレーヤ）アプリケーションは、コンテンツの各セグメントにおいて必要なシークレットパラメータ（ＳＰｎ）を取得するため、各セグメントに対応するシークレットパラメータ指定情報としてのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得して、シークレットパラメータＩＤの通知を含むシークレットパラメータ算出要求を、セキュアＶＭに対する割り込み（ＩＮＴＲＰ）要求として出力する。なお、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得するために必要な情報は、例えば変換テーブル３０３に記録されている。

【０１２８】
セキュアＶＭは、再生（プレーヤ）アプリケーションからのシークレットパラメータ算出要求に応じて、ＳＰ＿ＩＤ対応のシークレットパラメータ（ＳＰｘ）を算出し、応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーションに提供する。
【０１２９】
図１０に示すように、セグメントが異なると、変換エントリを取得するための演算に適用するパラメータ（ＳＰｘ）は異なるパラメータとなる。例えば、１つのセグメントはコンテンツ再生時間として約１０秒程度に設定され、再生（プレーヤ）アプリケーションは、約１０秒の各セグメント毎に異なるパラメータをセキュアＶＭから受領して、変換エントリを復元して、復元した変換エントリから変換データを取得し、データ置き換え処理を実行する。
【０１３０】
このように、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、各セグメント単位で、セキュアＶＭからシークレットパラメータを受領して、演算を実行して、変換テーブルブロックの構成データとしてり変換エントリの復元を実行し、復元した変換エントリを取得してデータ置き換えを行なう。なお、上述の処理例では、シークレットパラメータを適用した演算として排他論理和（ＸＯＲ）を例示したが、その他の演算処理を適用する設定としてもよい。またシークレットパラメータを適用した暗号処理等を実行する構成としてもよい。
【０１３１】
［５，再生（プレーヤ）アプリケーションとセキュアＶＭ間の処理］
上述した処理を実行する場合、再生（プレーヤ）アプリケーションは、コンテンツの再生を実行中、一定のセグメント単位で、異なるシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を順次取得するため、セキュアＶＭに対して、再生セグメントが切り替わる毎にシークレットパラメータを取得してデータ置き換えを行なうことが必要となる。
【０１３２】
このシークレットパラメータ（ＳＰ）の取得処理を実行する場合に、再生（プレーヤ）アプリケーションは、セキュアＶＭに対してシークレットパラメータ指定情報としてのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を通知して、必要なＳＰを特定する。このシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得するための情報は、例えば、変換テーブルに記録されており、再生（プレーヤ）アプリケーションは、変換テーブルに記録された情報に基づいて、セグメント対応のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得する。
【０１３３】
再生（プレーヤ）アプリケーションは、このシークレットパラメータ（ＳＰ）の取得処理などにおいてセキュアＶＭ間とのでデータ処理要求、応答を送受信する。再生アプリケーションと、セキュアＶＭ間において実行される一連の処理シーケンスについて、図１１を参照して説明する。
【０１３４】
先に、図１を参照して説明したように、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間の情報伝達、あるいは処理要求は、再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理のシーケンスによって実行される。
【０１３５】
図１１に示す処理シーケンスは、コンテンツを記録した情報記録媒体の挿入から、取り出しに至るまでに再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間において実行される処理の種類を示した図である。
【０１３６】
例えば、ステップＳ１１は、情報記録媒体（Ｄｉｓｃ）挿入時の処理として実行される

メディア初期化（Ｍｅｄｉａ　Ｉｎｉｔｉａｌｉｚｅ）処理であり、再生（プレーヤ）アプリケーション１５０は、最初の再生処理に必要となるコード情報を格納したコンテンツコードファイル（Ｃｏｎｔｅｎｔ　Ｃｏｄｅ　Ｆｉｌｅ）をメモリにロードして、実行を開始する。コンテンツコードファイル（Ｃｏｎｔｅｎｔ　Ｃｏｄｅ　Ｆｉｌｅ）は、再生（プレーヤ）アプリケーションのメーカー、モデル名などを特定する。

【０１３７】

例えば、セキュアＶＭ１６０は、取得したモデル名が、過去にセキュリティ問題が発生したことがあるモデルであるか否かを判定し、過去にセキュリティ問題が発生したことがあるモデルである場合、同様のセキュリティ問題が発生していないかをコンテンツコード（ＣｏｎｔｅｎｔＣｏｄｅ）の実行により調査する。例えば情報処理装置のＲＡＭ上の特定の値や、特定のデバイスの動作を調べて、正しい状態であるかを検査する。なお、モデルごとの調査プログラムは、最初にロードしたコンテンツコードファイルには入っていないことがあり、その場合は別の必要なコンテンツコードファイルへのアクセスを行う。セキュアＶＭ１６０による初期化処理が終了すると、応答（Ｃａｌｌ）が再生アプリケーション１５０に通知され、次のステップＳ１２に進む。

【０１３８】

ステップＳ１２では、タイトル初期化処理（Ｔｉｔｌｅ　Ｉｎｉｔｉａｌｉｚｅ）を実行する。タイトルは再生対象コンテンツの指定情報として適用され、ユーザの指定などに基づいて、特定の再生対象コンテンツに対応するタイトルが選択され、タイトル情報とともに、タイトル初期化処理要求が再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に出力される。

【０１３９】

セキュアＶＭ１６０は、タイトル再生に必要な全クリップ対応の変換データ情報を集めた変換テーブルをセキュアＶＭ１６０のメモリ上に生成し、再生（プレーヤ）アプリケーション１５０がテーブルを取得できるようにテーブルがストアされたメモリの位置を再生（プレーヤ）アプリケーション１５０に知らせる。なお、タイトル初期化中もステップＳ１１のメディア初期化と同様のセキュリティチェックを行うことが可能である。

【０１４０】

タイトル初期化処理において実行される。タイトル再生に必要な全クリップ対応の変換データ情報を集めた変換テーブルをセキュアＶＭ１６０のメモリ上に生成する処理例について、図１２を参照して説明する。図１２には、セキュアＶＭ１６０の利用可能なメモリ領域（例えば2ＭＢ）を示している。ここには、セキュアＶＭ１６０が、情報記録媒体から取得したデータ変換処理プログラムを含むコード情報としてのコンテンツコードが格納される。なお、このコンテンツコードには暗号化等の難読化処理のなされた変換テーブルが含まれる。また、データ変換処理プログラムは、この難読化（obfascated）処理のなされた変換テーブルを平文に変更するための鍵（ＳＰ：シークレットパラメータ）を導出するためのプログラムが一例である。すなわち、変換テーブルを取得して、その位置情報（relative packet number）、上書き情報（overwrite_value）を適用するプログラムについては、情報記録媒体ではなく、再生装置（再生アプリケーション）が保持していても良い。

【０１４１】

再生（プレーヤ）アプリケーション１５０からのタイトル初期化要求が入力されると、セキュアＶＭ１６０は、コンテンツコードから、タイトル再生に必要な全クリップ対応の変換データ情報を集めた変換テーブルを、必要に応じて復号処理を行い、前述したＸＯＲｅｄ等の処理のなされた状態（マスク状態）でメモリに格納し、このメモリ格納位置を再生（プレーヤ）アプリケーション１５０に通知する。この通知処理は、再生（プレーヤ）アプリケーション１５０からのタイトル初期化要求（ＩＮＴＲＰ）に対する応答（Ｃａｌｌ）として実行される。

【０１４２】

再生（プレーヤ）アプリケーション１５０は、セキュアＶＭ１６０から、タイトル初期

化要求（ＩＮＴＲＰ）に対する応答（Ｃａｌｌ）を受領すると、セキュアＶＭ１６０利用メモリ領域の変換テーブル格納領域から、必要なデータ部分を、再生（プレーヤ）アプリケーション１５０の利用可能なメモリ領域にコピーして格納する。例えば、先に、図６～図９を参照して説明したコンテンツのセグメント対応のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得するためのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）特定テーブルを抽出して再生（プレーヤ）アプリケーション１５０の利用可能なメモリ領域にコピーして格納する。

【０１４３】

再生（プレーヤ）アプリケーション１５０は、このコピー処理において、変換エントリを格納した変換テーブルの構成データや、変換テーブル中に含まれるセグメント対応のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を特定するための情報など、コンテンツ変換処理、再生処理に必要となる情報をすべて再生（プレーヤ）アプリケーション１５０の利用可能なメモリ領域に格納する。

【０１４４】

図１１に戻り、再生（プレーヤ）アプリケーション１５０とセキュアＶＭ１６０間の処理シーケンスについて説明を続ける。ステップＳ１３は、シークレットパラメータ（ＳＰ）計算に（Ｃｏｍｐｕｔｅ＿ＳＰ）に対応する処理であり、再生（プレーヤ）アプリケーション１５０は、ＳＰ計算要求（ＩＮＴＲＰ）をセキュアＶＭ１６０に出力し、セキュアＶＭ１６０は計算結果（ＳＰ）を応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーション１５０に返す。再生（プレーヤ）アプリケーション１５０は、ＳＰ計算要求（ＩＮＴＲＰ）をセキュアＶＭ１６０に出力する場合、ＳＰ指定情報としてのＳＰ＿ＩＤを通知する。

【０１４５】

ステップＳ１４の処理は、シークレットパラメータの計算とは異なる再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する要求処理である。例えば、セキュリティチェックの実行などの要求処理であり、セキュアＶＭ１６０は、これらの要求があった場合、その要求に応じた処理を実行して、処理結果を応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーション１５０に通知する。なお、この際の情報伝達には、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０の双方が書き込み読み取り可能なレジスタ、例えばプレイヤ・ステータスレジスタ、レジスタ（ＰＳＲ）が利用される。

【０１４６】

ステップＳ１５の処理は、情報記録媒体（Ｄｉｓｃ）取出の際のメディアファイナライズ（Ｍｅｄｉａ　Ｆｉｎａｌｉｚｅ）処理であり、コンテンツコード（Ｃｏｎｔｅｎｔ　Ｃｏｄｅ）の処理状況を、不揮発メモリに記録する。この処理によって、次回のディスク挿入時に過去のセキュリティチェックの情報を継続して使用することが可能となる。

【０１４７】

上述したように、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間の情報伝達、あるいは処理要求、応答は、再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理によって実行される。

【０１４８】

［６．コンテンツ再生処理］

次に、図１３を参照して、ホストの実行するコンテンツ再生処理について説明する。図１３には、左から暗号化コンテンツの格納された情報記録媒体３３０、情報記録媒体３３０をセットし、データの読み取りを実行するドライブ３４０、ドライブとデータ通信可能に接続され、情報記録媒体３３０に格納されたコンテンツをドライブ３４０を介して取得して再生処理を実行する再生アプリケーションを実行するホスト３４５を示している。

【０１４９】

なお、図１３に示すホスト３４５は、コンテンツの復号、デコード、データ変換処理な

どを実行する再生（プレーヤ）アプリケーションブロック３５０と、シークレットパラメータ（ＳＰ）の算出処理などを実行するセキュアＶＭ３６０を有するセキュアＶＭ３６０ブロックを区分して示してある。

【０１５０】

情報記録媒体３３０には、ＭＫＢ（Media Key Block）３３１、タイトル鍵ファイル３３２、暗号化コンテンツ３３３、変換処理プログラムを含むコンテンツコード３３４が記録され、暗号化コンテンツ３３３は、分散記録された変換エントリ３３５を含み、コンテンツコード３３４は、同様の変換エントリを含む変換テーブル３３６を含む構成である。ホスト３４５は、ＭＫＢの処理に適用するデバイス鍵３５１を保持している。

【０１５１】

図１３に示すホスト３４５がドライブ３４０を介して情報記録媒体３３０の格納コンテンツを取得して再生する処理シーケンスについて説明する。まず、情報記録媒体３３０の格納コンテンツの読み出しに先立ち、ホスト３４５とドライブ３４０は、ステップＳ１０１において、相互認証を実行する。この相互認証は、ホストおよびドライブがそれぞれ正当な機器またはアプリケーションソフトであるかを確認する処理である。この相互認証処理シーケンスとしては、様々な処理が適用可能である。相互認証処理によって、ドライブ３４０とホスト３４５は共通の秘密鍵としてのセッション鍵（Ｋｓ）を共有する。

【０１５２】

ステップＳ１０１において、ホストドライブ間の相互認証が実行され、セッション鍵（Ｋｓ）を共有した後、ホスト３４５の再生（プレーヤ）アプリケーション３５０は、ステップＳ１０２において、情報記録媒体３３０に記録されたＭＫＢ３３１を、ドライブを介して取得して、メモリに格納されたデバイス鍵３５１を適用したＭＫＢ３３１の処理を実行して、ＭＫＢからメディア鍵（Ｋｍ）を取得する。

【０１５３】

前述したように、ＭＫＢ（Media Key Block）３３１は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックであり、有効なライセンスを持つ装置に格納されたデバイス鍵（Ｋｄ）に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵（Ｋｍ）の取得を可能とした鍵情報ブロックである。

【０１５４】

次に、ステップＳ１０３において、ステップＳ１０２におけるＭＫＢ処理で取得したメディア鍵（Ｋｍ）を適用して、情報記録媒体３３０から読み取ったタイトル鍵ファイル３３２の復号を実行して、タイトル鍵（Ｋｔ）を取得する。情報記録媒体３３０に格納されるタイトル鍵ファイル３３２はメディア鍵によって暗号化されたデータを含むファイルであり、メディア鍵を適用した処理によってコンテンツ復号に適用するタイトル鍵（Ｋｔ）を取得することができる。なお、ステップＳ１０３の復号処理は、例えばＡＥＳ暗号アルゴリズムが適用される。

【０１５５】

次に、ホスト３４５の再生（プレーヤ）アプリケーション３５０は、ドライブ３４０を介して情報記録媒体３３０に格納された暗号化コンテンツ３３３を読み出して、トラックバッファ３５２に読み出しコンテンツを格納し、このバッファ格納コンテンツについて、ステップＳ１０４において、タイトル鍵（Ｋｔ）を適用した復号処理を実行し、復号コンテンツを取得する。

【０１５６】

復号コンテンツは、平文ＴＳバッファ３５３に格納する。（Ｐｌａｉｎ　ＴＳ）は復号された平文トランスポートストリームを意味する。ここで、平文ＴＳバッファ３５３に格納される復号コンテンツは、前述したブロークンデータを含むコンテンツであり、このままでは再生できず、所定のデータ変換（上書きによるデータ置き換え）を行なう必要がある。

【０１５７】

図１３に示す処理例では、暗号化コンテンツの構成データ中の特定パケットに分散されて記録された変換エントリを取得して、ここから変換データを抽出してデータ置き換えを行なう処理例である。すなわち、先に、図９を参照して説明したデータ変換処理に相当する。

【０１５８】

コンテンツ中に分割記録された変換エントリは、復号コンテンツに対して置き換え処理を行なう変換データ（または識別子設定変換データ）とその変換データの記録位置を記録したデータである。

【０１５９】

セキュアＶＭ３６１は、命令コード情報を含むデータ変換処理プログラムを含むコンテンツコード３３４を情報記録媒体３３０から読み出して、コンテンツ再生あるいは出力処理前および処理実行中に間欠的に、イベントハンドラ３５４の制御、プレーヤ情報３５５の入力に基づいて、情報記録媒体３３０にコンテンツとともに記録された変換テーブルを平文変換テーブルにするために必要なシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を生成して出力する。この処理は間欠的に行なわれる。

【０１６０】

シークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）は、前述したように所定のコンテンツデータ単位に対応するセグメントごとに切り替わる演算または暗号処理パラメータであり、具体的には、例えば、排他論理和（ＸＯＲ）演算パラメータである。セキュアＶＭ３６１は、再生（プレーヤ）アプリケーションからの要求に応じて、演算処理または暗号処理によって変形された変換テーブルブロックの構成データである変換エントリを復元するために必要なパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を間欠的に生成して出力する処理を実行する。

【０１６１】

再生（プレーヤ）アプリケーション３５０は、ステップＳ１０４において、変換エントリを含む暗号化コンテンツ３３３の復号が実行され、ステップＳ１０５におけるデマルチプレクサの処理によって、コンテンツ中に記録された変換テーブルの構成データである変換エントリが分離され、リアルタイムイベントハンドラ３５６の制御によって、ステップＳ１０６におけるテーブル復元＆データ変換処理が実行される。リアルタイムイベントハンドラ３５６の制御により、再生（プレーヤ）アプリケーション３５０は、セグメントの切り替えに応じたシークレットパラメータ算出要求をセキュアＶＭ３６１に割り込み（ＩＮＴＲＰ）として出力し、セキュアＶＭ３６１からセキュアパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を受領し、変換テーブルブロックの復号または演算を実行して平文変換テーブルブロックを取得し、取得した変換テーブルブロックに含まれる変換エントリを取得する。

【０１６２】

変換エントリには、変換データ、すなわち、

（ａ）変換データ

（ｂ）識別子設定変換データ

と、これらの変換データのコンテンツにおける記録位置指定情報が記録されており、再生（プレーヤ）アプリケーション３５０は、ステップＳ１０６において、指定位置に書き込むデータ変換処理をコンテンツ再生処理または外部出力処理に並行したリアルタイム処理として実行する。

【０１６３】

例えば、パラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）は所定のコンテンツ部分データ単位であるセグメントに対応する変換エントリとの排他論理和（ＸＯＲ）演算パラメータである場合、ステップＳ１０６におけるテーブル復元処理としては、

［変換エントリ１］（ＸＯＲ）［ＳＰ１］、

［変換エントリ２］（ＸＯＲ）［ＳＰ２］、

［変換エントリ３］（ＸＯＲ）［ＳＰ３］、

：　　：

これらの排他論理和演算処理を実行して、変換テーブルブロックデータに含まれる変換エントリを取得する。なお、上記式において、［Ａ］（ＸＯＲ）［Ｂ］は、ＡとＢの排他論理和演算を意味するものとする。

【０１６４】

このように、情報記録媒体に記録されたコンテンツ３３３に含まれる変換エントリは、シークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）と排他論理和演算されて格納されている。このパラメータは、セキュアＶＭ３６１によって逐次、取得され出力される。

【０１６５】

ステップＳ１０６のテーブル復元＆データ変換処理においては、シークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を適用した演算または暗号処理よって取得した復元された変換エントリから変換データを取得して、コンテンツに含まれるブロークンデータを正当なコンテンツ構成データである変換データに置き換え、さらに、識別子設定変換データをコンテンツの一部データと入れ替えるデータ上書き処理を実行し、平文ＴＳバッファ３５３の格納データを変換処理済みデータに変更する。このデータ変換処理の概要について、図１４を参照して説明する。

【０１６６】

情報記録媒体に格納された暗号化コンテンツ３３３が、一旦、ホスト側のトラックバッファ３５２に格納される。図１４（１）に示すトラックバッファ格納データ４０１である。ホスト側の復号処理によって、トラックバッファ格納データ４０１としての暗号化コンテンツの復号が実行されて、復号結果データが平文ＴＳバッファ３５３に格納される。図１４（２）に示す復号結果データ４０２である。

【０１６７】

復号結果データ４０２には、正常なコンテンツ構成データではない、ブロークンデータ４０３が含まれる。ホストのデータ変換処理部は、このブロークンデータ４０３を、正しいコンテンツ構成データとしての変換データ４０４に置き換える処理を実行する。この置き換え処理は、例えば平文ＴＳバッファ３５３に書き込み済みのデータに対する一部データの再書き込み（上書き）処理として実行される。

【０１６８】

さらに、ホストの実行するデータ変換処理は、ブロークンデータを正常なコンテンツデータである変換データに置き換える処理のみならず、図１４に示すように、識別子設定変換データ４０５によって、復号結果データ４０２の一部構成データを置き換える処理を実行する。

【０１６９】

識別子は、前述したようにコンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータである。具体的には例えば、ホストアプリケーションを実行するプレーヤとしての情報処理装置の識別情報（プレーヤＩＤ）の構成データまたは、プレーヤＩＤに基づいて生成される識別マークである。識別子設定変換データは、先に説明したようにコンテンツの再生に影響を与えないレベルで、正しいコンテンツデータのビット値をわずかに変更したデータである。

【０１７０】

識別子設定変換データ４０５は、コンテンツ中に多数設定され、これら複数の識別子設定変換データ４０５を集積して解析することで、例えばプレーヤＩＤが判別される。識別子設定変換データ４０５は、コンテンツとして通常再生可能なレベルで正常コンテンツデータの構成ビットを変更したデータであり、ＭＰＥＧビットストリーム解析によりビット（識別マーク構成ビット）判別が可能なデータである。

【０１７１】

情報記録媒体に格納される変換テーブルには、図１４に示す変換データ４０４、識別子設定変換データ４０５が多数登録されており、さらに、これらの書き込み位置情報につい

ても登録されている。この変換テーブル格納情報に基づくデータ変換処理を実行することで、平文ＴＳバッファ３５３に格納されたデータは、図１４（３）に示す変換処理済みデータ４０６に置き換えられることになる。

【０１７２】

その後、変換済みのＴＳ（トランスポートストリーム）は、ネットワークなどを介して外部出力され、外部の再生機器において再生される。あるいは、ステップＳ１０７において、デマルチプレクサによる処理によって、トランスポートストリーム（ＴＳ）からエレメンタリストリーム（ＥＳ）への変換が実行され、さらに、デコード処理（ステップＳ１０８）が行なわれた後、ディスプレイスピーカを介して再生される。

【０１７３】

［７．コンテンツコードの管理構成］

上述したように、情報記録媒体に記録されたコンテンツの再生においては、コンテンツコードを情報記録媒体から読み出して、コンテンツコードに含まれる変換テーブルを適用して、コンテンツコードに含まれる変換処理プログラムを適用して処理を実行することが必要である。コンテンツコードには、更にスタートアップ処理、セキュリティチェック処理などの実行に適用されるプログラムや、情報が含まれ、コンテンツ利用に際しては、コンテンツコードが取得間され、実行される。

【０１７４】

コンテンツコードの実行処理は、主に、コンテンツ再生を実行する情報処理装置において設定されるセキュアＶＭによって行なわれる。セキュアＶＭは、情報記録媒体に記録された暗号化コンテンツの利用に適用するプログラムまたは適用情報を含むコンテンツコードを取得して、取得したコンテンツコードに従ったデータ処理を実行するコンテンツコードを実行するデータ処理部として機能する。

【０１７５】

コンテンツコードは、コンテンツとは独立したファイルとして設定されて情報記録媒体に記録される。従って、コンテンツコードのみを他の情報記録媒体に移動させる処理や、コピーするといった処理も可能となる。コンテンツコードの漏洩が発生し、不正に流通してしまった場合、多くのコンテンツが不正に再生、利用される可能性があり、大きな損害を発生させる可能性がある。以下では、このようなコンテンツコードの不正利用を防止する構成について説明する。

【０１７６】

図１５を参照して情報記録媒体に記録されるコンテンツコード５００に含まれるデータの種類について説明する。上述した説明において記載したように、コンテンツコード５００には、コンテンツのデータ変換処理に適用するプログラムや変換テーブルが記録される。例えば変換テーブルは各コンテンツの構成データの置き換えデータとしての変換データを含むデータでありコンテンツ固有のデータとすることが必要であるが、例えば変換処理プログラムなどは、各コンテンツにおいて共通のコード情報として設定可能なデータである。

【０１７７】

コンテンツコードには、コンテンツ再生処理を実行する情報処理装置または情報処理装置で実行される再生（プレーヤ）アプリケーションに対応して設定された情報やプログラムも含まれる。例えば複数の異なるメーカーの情報処理装置や再生アプリケーションにおいて利用される場合、各装置、各アプリに対応する複数のコードがコンテンツコード中に記録され、各プレーヤ（装置または再生アプリ）はコンテンツコードに含まれるプレーヤ（装置または再生アプリ）固有コードから、自己のプレーヤ（装置または再生アプリ）に対応するコードを選択して処理を行なう。

【０１７８】

このように、コンテンツコード５００には、様々なデータが含まれる。これらのデータを大きく分類すると、図１５に示すように、４つの分類が可能となる。すなわち、

（ａ）全コンテンツ＆全プレーヤ（装置または再生アプリ）共通データ５０１

（ｂ）コンテンツ固有データ５０２
（ｃ）プレーヤ（装置または再生アプリ）固有データ５０３
（ｄ）コンテンツ＆プレーヤ（装置または再生アプリ）固有データ５０４

【０１７９】

以下、各データの具体的なデータ内容例について説明する。

（ａ）全コンテンツ＆全プレーヤ（装置または再生アプリ）共通データ５０１

全コンテンツ＆全プレーヤ（装置または再生アプリ）共通データ５０１は、すべてのコンテンツ、全ての情報処理装置や再生アプリケーションにおいて共通に利用可能な情報やプログラムを含むデータ部分であり、具体的には、例えば、以下の情報やプログラムが含まれる。

（ａ１）スタートアップルーチンに関するプログラム：例えば、メモリの初期化状態のチェック、初回のロードでは不足しているデータの読み込み、一緒に情報記録媒体（Disc）に記録されているコンテンツが正当なコンテンツであるかの確認などの処理を実行するプログラム。

（ａ２）共通ルーチン（外部記録へのアクセスなど）プログラム：例えば、不揮発性メモリアクセス機能によって利用可能なプログラム、このコンテンツコードが利用できる情報が記録されていた場合はデータを読み込んで利用可能となる。

（ａ３）プレーヤ識別ルーチン：現在再生を実行している装置や再生アプリケーションの情報を取得し、追加のセキュリティチェックの対象であるかを判定するプログラム。追加チェックが必要である場合は、必要に応じてコンテンツコードファイルのロードを行った上で、追加チェックを行う。

【０１８０】

（ｂ）コンテンツ固有データ５０２

コンテンツ固有データ５０２は、各コンテンツに固有の情報やプログラムを含むデータ部分であり、具体的には、例えば、以下の情報やプログラムが含まれる。

（ｂ１）変換テーブル（FixUpTable）情報：前述した処理例において説明した変換データを含む変換テーブルである。変換データのみならず、シークレット（ＳＰ）パラメータの計算ルーチン等、データ変換処理に必要な情報が含まれる。

（ｂ２）タイトル初期化プログラム：変換テーブル（FixUpTable)を生成する処理、タイトル再生前に行うセキュリティチェックで、コンテンツのみに依存するチェックに関するルーチンが含まれる。

【０１８１】

（ｃ）プレーヤ（装置または再生アプリ）固有データ５０３

（ｃ）プレーヤ（装置または再生アプリ）固有データ５０３は、コンテンツを再生する情報処理装置または再生アプリケーションに固有の情報やプログラムを含むデータ部分であり、具体的には、例えば、以下の情報やプログラムが含まれる。

（ｃ１）RunNative実行部分、NativeCode：コンテンツ再生を実行する装置やアプリケーションプログラム固有の処理を実行して、セキュリティ問題の発見や改善を行う機能実行するための情報およびプログラム。再生処理を実行する情報処理装置のＯＳにおいてカーネルモードで実行される処理が一般的である。また、この処理の実行時は、NativeCode自体にプレーヤ固有の正当性検証機能（たとえばプレーヤ製造者に割り当てられた公開鍵に対する秘密鍵（PrivateKey）による署名の検証。すなわち、NativeCodeには、再生装置（アプリケーションプログラム）は、製造者に対して割り当てられた秘密鍵に対応する公開鍵を保持し、この秘密鍵を用いた署名が付与され、この署名の検証を対応する公開鍵を用いて行う。）を含め、コンテンツ再生を実行する情報処理装置側において、署名検証による正当性検証を実行後に、これらのコンテンツコードの実行によるセキュリティ問題の発見や改善を行う。

【０１８２】

（ｄ）コンテンツ＆プレーヤ（装置または再生アプリ）固有データ５０３

コンテンツ＆プレーヤ（装置または再生アプリ）固有データ５０３は、コンテンツ固有

であり、かつコンテンツを再生する情報処理装置または再生アプリケーションにも固有の情報やプログラムを含むデータであり、具体的には、例えば、以下の情報やプログラムが含まれる。

（ｄ１）DiscoveryRAMを使ったプレーヤの正当性チェック部分：コンテンツ再生を実行する装置内のメモリ（ＲＡＭ）上の特定の値をチェックして、正当なプレーヤ（装置または再生アプリ）であることをチェックする機能を実行するための情報およびプログラム。特定のコンテンツを再生中に、特定のメモリが、プレーヤ固有の状態になることを監視することで正当性を確認する。この場合は、チェックルーチンがコンテンツとプレーヤの両方に依存することになる。

（ｄ２）DiscoveryRAM用比較データ：上述の（ｄ１）DiscoveryRAMを使ったプレーヤの正当性チェックにおいて、ＲＡＭ上の実際の値と比較するための値（ターゲット値）を格納したテーブル。

【０１８３】

このように、コンテンツコードには、様々な情報、およびプログラムが格納され、コンテンツ再生を実行する装置は、これらのコンテンツコードから、再生コンテンツに応じて、また、装置や再生アプリケーションに応じて、対応するコード情報を選択して、様々な処理を実行する。

【０１８４】

図１５を参照して説明したように、コンテンツコードは、以下の４つのカテゴリに分類可能である。

（ａ）全コンテンツ＆全プレーヤ（装置または再生アプリ）共通データ５０１

（ｂ）コンテンツ固有データ５０２

（ｃ）プレーヤ（装置または再生アプリ）固有データ５０３

（ｄ）コンテンツ＆プレーヤ（装置または再生アプリ）固有データ５０４

【０１８５】

これらの各々のコンテンツコードは、個別のファイル、あるいは集積されて１つのファイルとして情報記録媒体に格納される。これらの各カテゴリのコンテンツコードは、それぞれコードの製作を行なうエンティティが異なる場合がある。例えば、（ｂ）コンテンツ固有データに対応するコンテンツコードは、コンテンツの製作者であるスタジオなどが設定する。また、（ｃ）プレーヤ（装置または再生アプリ）固有データについては、プレーヤとしての再生装置や、再生アプリケーションを製作するエンティティが生成する場合が多い。

【０１８６】

このように、異なるエンティティによって生成されるコンテンツコードが、情報記録媒体に記録されるまでのシーケンスについて、図１６を参照して説明する。図１６には、上述した４つのカテゴリに対応するコンテンツコードの構成データを示している。すなわち、

（データａ）全コンテンツ＆全プレーヤ（装置または再生アプリ）共通データ５０１

（データｂ）コンテンツ固有データ５０２

（データｃ）プレーヤ（装置または再生アプリ）固有データ５０３

（データｄ）コンテンツ＆プレーヤ（装置または再生アプリ）固有データ５０４

これら４つの異なるカテゴリのコンテンツコードである。

【０１８７】

これらのコンテンツコードは、それぞれ異なるエンティティ、すなわち、コンテンツの製作、編集を行なうスタジオ、オーサリング会社、また、プレーヤ（装置または再生アプリ）の製造メーカーなど、異なるエンティティによって製作される。

【０１８８】

これらのコンテンツコードが生成されると、ステップＳ２０１，Ｓ２０２において、各コンテンツコードの製作者、あるいは提供エンティティの署名を付与する。各エンティティの持つ暗号鍵（秘密鍵）を適用して電子署名を付与する。この電子署名の付与は、各コ

ンテンツコードの改ざん検証、改ざん防止のために設定される。なお、図には、ステップＳ２０１、Ｓ２０２の２つの処理ブロックのみを示しているが、生成されるコンテンツコードの数に応じて、各コンテンツコードを生成したエンティティがそれぞれ署名を付与する。

【０１８９】

ステップＳ２０３では、最終的に情報記録媒体に記録するコンテンツコードに対して、管理センタ（ＫＩＣ：Ｋｅｙ　Ｉｓｓｕａｎｃｅ　Ｃｅｎｔｅｒ、すなわち、鍵発行センターとも称するが、本明細書においては管理センタと称する。）が電子署名を付与する。なお、この管理センタ（ＫＩＣ）における電子署名の設定に際しては、各エンティティの署名検証を行なって、各コンテンツコードが改ざんされていないものであることを確認したことを条件として新たに管理センタ（ＫＩＣ）の電子署名を設定することが好ましい。

【０１９０】

情報記録媒体には、管理センタ（ＫＩＣ）の電子署名の付与されたコンテンツコードファイルが記録される。情報記録媒体に記録されるコンテンツコードに対する署名の設定態様としては、いくつかの異なる設定態様が利用可能である。以下、図１７～図２０を参照して、情報記録媒体に記録されるコンテンツコードのデータ構成と、署名設定例について説明する。

【０１９１】

図１７に示す例は、情報記録媒体に記録されるコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］５２１，５２２，５２３の各々が、共通のファイル構成を有する例であり、各ファイルは、図に示すコンテンツコードファイル５３０に示すように、ヘッダ５３１と、コンテンツコードブロック５３２と、電子署名５３３を有する構成とされる。

【０１９２】

ヘッダ５３１には、コンテンツコードに対応する固有の識別情報である固有ＩＤ、コンテンツコードの実体データを格納するコンテンツコードブロックのデータサイズと、電子署名の種類（ＥＣＤＳＡなど）など、電子署名情報が含まれる。

【０１９３】

コンテンツコードブロック５３２はコンテンツコードの実体データとして、前述した様々な種類のコンテンツコードが記録される。電子署名５３３は、本例では、管理センタの署名である。本例では、先に説明した管理センタ以外の各エンティティの署名は、コンテンツコード中には含まれない設定とされる。

【０１９４】

このように、全てのコンテンツコードファイルに管理センタの署名を設定する構成では、全てのコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］は、例えば、

２ＭＢ＋ヘッダ＋署名

のデータ容量が設定される。２ＭＢがコンテンツコードブロックに適用される。

【０１９５】

図１７に示すコンテンツコードを利用する情報処理装置（ユーザデバイス）は、コンテンツコードに含まれる管理センタの電子署名の検証を実行して、コンテンツコードの改ざんの有無を検証した後、コードの利用を行なう。具体的な処理シーケンスについては後述する。

【０１９６】

図１８は、情報記録媒体に記録されるコンテンツコードファイルの１つのみに署名を設定して、その他のコンテンツコードファイルには、署名を設定しない構成とした例である。図１８に示す例では、コンテンツコードファイル［００００．ｓｖｍ］５２１にのみ、ファイル５３０に示すように管理センタの電子署名５３３が設定され、ヘッダ５３１、コンテンツコードブロック５３２、管理センタの電子署名５３３を含む構成となっているが、その他のコンテンツコードファイル［００００１．ｓｖｍ］５２２以下のファイル５４０には、管理センタの電子署名が設定されておらず、ヘッダ５４１とコンテンツコードブロック５４２のみが格納されたファイル５４０として設定される。

【０１９７】
管理センタの電子署名が設定されるコンテンツコードファイルは、例えばスタートアップルーチンを実行するためのコンテンツコードが記録されたファイルとするなど、情報処理装置において必ず実行されるコンテンツコードを格納したファイルとすることが好ましい。
【０１９８】
この構成例では、コンテンツコードを利用する情報処理装置は、コンテンツコードファイル［００００００．ｓｖｍ］５２１を利用する場合にのみ署名検証を実行する。その他のファイルを利用する場合は、署名検証を省略することができる。ただし、電子署名の検証とは異なる手法、例えばハッシュ検証処理などの簡易な手法によって、署名の設定されていない各コンテンツコードファイルの改ざん検証を実行して、正当性を確認した後、各ファイルのコードを利用する構成とする。この場合には、例えば検証に適用する照合用ハッシュ値をコンテンツコードファイル内に記録保持した構成とする。これらの処理シーケンスについては、後述する。
【０１９９】
このように、１つのコンテンツコードファイルのみに管理センタの署名を設定する構成では、署名を設定したコンテンツコードファイルは、例えば、
２ＭＢ＋ヘッダ＋署名
のデータ容量が設定されるが、その他の署名の設定されないコンテンツコードファイルは、署名の付与がなく、署名検証のプロセスを考慮する必要がなくなるので、コンテンツコードブロックのサイズに制限を設ける必要がなくなり、任意のサイズのコンテンツコードブロックを設定したファイルとすることが可能となる。
【０２００】
次に、図１９、図２０を参照して、管理センタの署名のみならず、各コンテンツコードの製作または提供エンティティの署名も併せて記録したコンテンツコードファイルの設定例について説明する。
【０２０１】
図１９に示す例は、情報記録媒体に記録されるコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］５２１，５２２，５２３の各々が、共通のファイル構成を有する例であり、各ファイルは、図に示すコンテンツコードファイル５５０に示すように、ヘッダ５５１と、コンテンツコードブロック５５２と、電子署名１，５５３と、電子署名２，５５４を有する構成とされる。
【０２０２】
ヘッダ５５１には、コンテンツコードに対応する固有の識別情報である固有ＩＤ、コンテンツコードの実体データを格納するコンテンツコードブロックのデータサイズと、電子署名の種類（ＥＣＤＳＡなど）など、電子署名情報が含まれる。コンテンツコードブロック５５２はコンテンツコードの実体データとして、前述した様々な種類のコンテンツコードが記録される。
【０２０３】
電子署名１，５５３は、管理センタではなく、各コンテンツコードファイルに格納されるコンテンツコードの製作者、あるいは提供エンティティの署名である。電子署名２，５５４は、管理センタの署名である。本例では、このように、管理センタの署名に加え、各エンティティの署名も併せて格納した設定としている。
【０２０４】
図１９に示すコンテンツコードを利用する情報処理装置（ユーザデバイス）は、
コンテンツコードに含まれる管理センタの電子署名のみ検証を実行して、コンテンツコードの改ざんの有無を検証した後、コードの利用を行なう。あるいは、管理センタの電子署名の検証に加えて、各エンティティの電子署名の検証を実行する構成としてもよい。
【０２０５】
図２０は、情報記録媒体に記録されるコンテンツコードファイルの１つのみに署名を設

定して、その他のコンテンツコードファイルには、署名を設定しない構成とした例である。図２０に示す例では、コンテンツコードファイル［００００．ｓｖｍ］５２１にのみ、ファイル５５０に示すように、コンテンツコードの製作者、あるいは提供エンティティの電子署名５５３と、管理センタの電子署名５５４が設定され、ヘッダ５５１、コンテンツコードブロック５５２、電子署名１，５５３、電子署名２，５３４を含む構成となっているが、その他のコンテンツコードファイル［００００１．ｓｖｍ］５２２以下のファイル５６０には、電子署名が設定されておらず、ヘッダ５６１とコンテンツコードブロック５６２のみが格納されたファイル５４０として設定される。

【０２０６】

電子署名が設定されるコンテンツコードファイルは、先に、図１８を参照して説明した例と同様、例えばスタートアップルーチンを実行するためのコンテンツコードが記録されたファイルとするなど、情報処理装置において必ず実行されるコンテンツコードを格納したファイルとすることが好ましい。

【０２０７】

この構成例では、コンテンツコードを利用する情報処理装置は、コンテンツコードファイル［００００００．ｓｖｍ］５２１を利用する場合にのみ署名検証を実行する。その他のファイルを利用する場合は、署名検証を省略することができる。ただし、電子署名の検証とは異なる手法、例えばハッシュ検証処理などの簡易な手法によって、署名の設定されていない各コンテンツコードファイルの改ざん検証を実行して、正当性を確認した後、各ファイルのコードを利用する構成とする。この場合には、例えば検証に適用する照合用ハッシュ値をコンテンツコードファイル内に記録保持した構成とする。

【０２０８】

次に、図２１、図２２に示すフローチャートを参照して、コンテンツコードを利用したデータ処理を実行する情報処理装置におけるコンテンツコード利用処理シーケンスについて説明する。

【０２０９】

図２１は、先に、図１７、図１９を参照して説明したコンテンツコードファイル構成、すなわち、全てのコンテンツコードファイルに電子署名が記録されたファイル設定の場合における処理シーケンスを示すフローチャートであり、図２２は、先に、図１８、図２０を参照して説明したコンテンツコードファイル構成、すなわち、１つのコンテンツコードファイルにのみ電子署名が記録されたファイル設定の場合における処理シーケンスを示すフローチャートである。

【０２１０】

まず、図２１に示すフローチャートを参照して、全てのコンテンツコードファイルに電子署名が記録されたファイル設定の場合におけるコンテンツコード利用シーケンスについて説明する。なお、この処理シーケンスは、コンテンツ再生を実行する情報処理装置において設定されるセキュアＶＭによって実行される。セキュアＶＭは、情報記録媒体に記録された暗号化コンテンツの利用に適用するプログラムまたは適用情報を含むコンテンツコードを取得して、取得したコンテンツコードに従ったデータ処理を実行するデータ処理部として機能する。

【０２１１】

まず、コンテンツコードを利用する情報処理装置のデータ処理部（セキュアＶＭ）は、ステップＳ３０１において、コンテンツコードファイル［００００．ｓｖｍ］の署名検証処理を実行する。コンテンツコードファイル［００００．ｓｖｍ］に設定された管理センタ（ＫＩＣ）の電子署名の検証を実行する。具体的には、例えば管理センタ（ＫＩＣ）の公開鍵を適用した電子署名検証（例えばＥＣＤＳＡ署名検証アルゴリズム）を実行する。

【０２１２】

ステップＳ３０２において、署名検証によって、コンテンツコードファイルの正当性なしの判定がなされた場合は、コンテンツコードの利用を中止して処理を終了する。

【０２１３】
ステップＳ３０２において、署名検証によって、コンテンツコードファイルの正当性ありとの確認がなされた場合は、ステップＳ３０３に進み、セキュアＶＭの利用するメモリ領域に、情報記録媒体から読み出したコンテンツコードファイル［００００００．ｓｖｍ］をロードし、ステップＳ３０４において、コンテンツコードファイル［００００００．ｓｖｍ］に記録されたコンテンツコードを実行する。なお、このコンテンツコードファイル［００００００．ｓｖｍ］に記録されたコンテンツコードは、例えばスタートアップルーチンの実行コードであり、情報記録媒体に格納されたコンテンツを利用する情報処理装置は、まず、コンテンツコードファイル［００００００．ｓｖｍ］の検証処理、ロード処理、コード実行処理の手順で処理を行なう。

【０２１４】
その後、ステップＳ３０５において、セキュアＶＭの適用メモリにロードされていないコンテンツコードファイルの利用が必要であるかを判定し、必要である場合は、ステップＳ３０６に進み、セキュアＶＭのメモリ上に新たなコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］をロードするための読み取り（Ｒｅａｄ）命令をドライブに出力する。

【０２１５】
次に、ステップＳ３０７において、コンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］に設定された管理センタ（ＫＩＣ）の電子署名の検証を実行する。ステップＳ３０８において、署名検証によって、コンテンツコードファイルの正当性なしの判定がなされた場合は、コンテンツコードの利用を中止して処理を終了する。

【０２１６】
ステップＳ３０８において、署名検証によって、コンテンツコードファイルの正当性ありとの確認がなされた場合は、ステップＳ３０９に進み、セキュアＶＭの利用するメモリ領域に、情報記録媒体から読み出したコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］をロードして実行する。

【０２１７】
ステップＳ３１０において、ユーザ操作による再生終了、またはタイトル終了が発生していない場合は、ステップＳ３０５での他のコンテンツコードの利用、ロードの必要性の判定処理に戻る。ステップＳ３１０において、ユーザ操作による再生終了、またはタイトル終了が発生した場合は処理を終了する。

【０２１８】
次に、図２２に示すフローチャートを参照して、先に、図１８、図２０を参照して説明したコンテンコードファイルの設定、すなわち、１つのコンテンツコードファイルに電子署名が記録され、その他のコンテンツコードファイルに電子署名が記録されていないファイル設定とした場合におけるコンテンツコード利用シーケンスについて説明する。なお、この処理シーケンスは、コンテンツ再生を実行する情報処理装置において設定されるセキュアＶＭによって実行される。

【０２１９】
まず、コンテンツコードを利用する情報処理装置は、ステップＳ４０１において、コンテンツコードファイル［００００００．ｓｖｍ］の署名検証処理を実行する。コンテンツコードファイル［００００００．ｓｖｍ］に設定された管理センタ（ＫＩＣ）の電子署名の検証を実行する。具体的には、例えば管理センタ（ＫＩＣ）の公開鍵を適用した電子署名検証（例えばＥＣＤＳＡ署名検証アルゴリズム）を実行する。

【０２２０】
ステップＳ４０２において、署名検証によって、コンテンツコードファイルの正当性なしの判定がなされた場合は、コンテンツコードの利用を中止して処理を終了する。

【０２２１】
ステップＳ４０２において、署名検証によって、コンテンツコードファイルの正当性ありとの確認がなされた場合は、ステップＳ４０３に進み、セキュアＶＭの利用するメモリ領域に、情報記録媒体から読み出したコンテンツコードファイル［００００００．ｓｖｍ］

をロードし、ステップＳ４０４において、コンテンツコードファイル［００００．ｓｖｍ］に記録されたコンテンツコードを実行する。なお、このコンテンツコードファイル［００００．ｓｖｍ］に記録されたコンテンツコードは、例えばスタートアップルーチンの実行コードであり、情報記録媒体に格納されたコンテンツを利用する情報処理装置は、まず、コンテンツコードファイル［００００．ｓｖｍ］の検証処理、ロード処理、コード実行処理の手順で処理を行なう。

【０２２２】

その後、ステップＳ４０５において、セキュアＶＭの適用メモリにロードされていないコンテンツコードファイルの利用が必要であるかを判定し、必要である場合は、ステップＳ４０６に進み、セキュアＶＭのメモリ上に新たなコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］をロードするための読み取り（Ｒｅａｄ）命令をドライブに出力する。

【０２２３】

次に、ステップＳ４０７において、セキュアＶＭの利用するメモリ領域に、情報記録媒体から読み出したコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］をロードする。

【０２２４】

次に、ステップＳ４０８において、コンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］に格納されたコンテンツコード構成データに基づくハッシュ値を算出し、予めコンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］に格納された検証用ハッシュ値との照合処理を実行して、コンテンコードファイルの検証を実行する。ステップＳ４０９において、検証によって、コンテンツコードファイルの正当性なしの判定がなされた場合は、コンテンツコードの利用を中止して処理を終了する。

【０２２５】

ステップＳ４０９において、検証によって、コンテンツコードファイルの正当性ありとの確認がなされた場合は、ステップＳ４１０に進み、コンテンツコードファイル［ｘｘｘｘｘ．ｓｖｍ］から取得したコンテンツコードを実行する。

【０２２６】

ステップＳ４１１において、ユーザ操作による再生終了、またはタイトル終了が発生していない場合は、ステップＳ４０５での他のコンテンツコードの利用、ロードの必要性の判定処理に戻る。ステップＳ４１１において、ユーザ操作による再生終了、またはタイトル終了が発生した場合は処理を終了する。

【０２２７】

このように、情報処理装置は、コンテンツコードの利用に際して、コンテンツコードファイルに設定された電子署名検証またはハッシュ検証などを実行して、コンテンツコードファイルの正当性を確認した後、コンテンツコードの処理を実行する構成としたので、不正なコードの実行が防止される。

【０２２８】

各エンティティが生成したコンテンツコードは、それぞれ独立したデータふぁいるとして設定可能であり、これらのコンテンツコードファイルは、再利用可能である。すなわち、異なるコンテンツや異なるプレーヤ（装置または再生アプリケーション）に対しても共通に利用可能な場合がある。このようなコンテンツコードの再利用構成について、図２３を参照して説明する。

【０２２９】

図２３において、例えばコンテンツコードファイル６０１～６０４は、各コンテンツコード製作エンティティまたは提供エンティティが保持するコンテンツコードファイルであり、それぞれ、

コンテンツ，プレーヤ共通コンテンツコードファイル［００００．ｓｖｍ］６０１、
コンテンツ固有コンテンツコードファイル［００００１．ｓｖｍ］６０２、
プレーヤ固有コンテンツコードファイル［００００２．ｓｖｍ］６０３、
コンテンツ，プレーヤ固有コンテンツコードファイル［００００３．ｓｖｍ］６０４、
これらのコンテンツコードファイルを示している。

【０２３０】
これらのコンテンツコードファイル６０１～６０４には、各コンテンツコード製作エンティティまたは提供エンティティによる電子署名が付与されて、各エンティティにおいて保管される。
【０２３１】
新たなコンテンツを記録した情報記録媒体を製作する場合、各エンティティは、既に他のコンテンツ記録情報記録媒体において利用したこれらのコンテンツコードファイル６０１～６０４を再利用することができる。
【０２３２】
先に、図１６を参照して説明したように、これらを管理センタに提供して、管理センタにおいて、電子署名を設定して、情報記録媒体６１０に格納する。情報記録媒体６１０に記録されるコンテンツコードには、管理センタ（ＫＩＣ）による電子署名、および管理センタの設定した固有ＩＤが付与される。情報記録媒体６１０に記録されるコンテンツコード６２０には、図に示すように変換テーブル６２１が含まれる。具体的なディレクトリ構成は、ディレクトリ構成６３０に示すように、各エンティティの生成したコンテンツコードが個別に設定された構成とされる。
【０２３３】
このように、コンテンツコードは、様々なコンテンツに対応して再利用可能であり、各コンテンツに応じて変更の必要なコンテンツコードと、再利用可能なコンテンツコードを、適宜、組み合わせて、情報記録媒体に記録されることになる。
【０２３４】
［８．情報処理装置の構成］
次に、図２４を参照して、上述した再生（プレーヤ）アプリケーションおよびセキュアＶＭの処理を実行する情報処理装置のハードウェア構成例について説明する。情報処理装置８００は、ＯＳやコンテンツ再生または記録アプリケーションプログラム、相互認証処理、コンテンツ再生に伴う様々な処理、例えば、上述したデータ変換処理などを含む各種プログラムに従ったデータ処理を実行するＣＰＵ８０９、プログラム、パラメータ等の記憶領域としてのＲＯＭ８０８、メモリ８１０、デジタル信号を入出力する入出力Ｉ／Ｆ８０２、アナログ信号を入出力し、Ａ／Ｄ，Ｄ／Ａコンバータ８０５を持つ入出力Ｉ／Ｆ８０４、ＭＰＥＧデータのエンコード、デコード処理を実行するＭＰＥＧコーデック８０３、ＴＳ（Transport Stream）・ＰＳ(Program Stream)処理を実行するＴＳ・ＰＳ処理手段８０６、相互認証、暗号化コンテンツの復号処理など各種の暗号処理を実行する暗号処理手段８０７、ハードディスクなどの記録媒体８１２、記録媒体８１２の駆動、データ記録再生信号の入出力を行なうドライブ８１１を有し、バス８０１に各ブロックが接続されている。
【０２３５】
情報処理装置（ホスト）８００は、例えばＡＴＡＰＩ－ＢＵＳ等の接続バスによってドライブと接続されている。変換テーブル、コンテンツなどをデジタル信号用入出力Ｉ／Ｆ８０２を介して入出力される。暗号化処理、復号処理は、暗号化処理手段８０７によって、例えば、ＡＥＳアルゴリズムなどを適用して実行される。
【０２３６】
なお、コンテンツ再生あるいは記録処理を実行するプログラムは例えばＲＯＭ８０８内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ８１０を使用する。
【０２３７】
ＲＯＭ８０８または記録媒体８１２には、例えば、管理センタの公開鍵、ホスト対応秘密鍵、ホスト対応の公開鍵証明書、さらに、リボケーションリストとしてのドライブＣＲＬなどが格納される。
【０２３８】
コンテンツ再生または外部出力に際しては、情報記録媒体から取得したデータ変換処理

プログラムを適用して、暗号化コンテンツの復号と、変換テーブルの復元、変換テーブルの格納データに基づく変換データの書き込み処理など、先に説明した処理例の各処理シーケンスに従った処理を実行する。

【０２３９】

［９．情報記録媒体製造装置および情報記録媒体］

次に、情報記録媒体製造装置および情報記録媒体について説明する。すなわち、上述したコンテンツ再生処理において適用される情報記録媒体の製造装置、方法、および情報記録媒体について説明する。

【０２４０】

情報記録媒体製造装置は、例えば、先に図１を参照して説明した記録データを格納した情報記録媒体１００を製造する装置である。情報記録媒体製造装置は、図２５に示すように、情報記録媒体に記録するコンテンツデータを格納したコンテンツファイルを生成するコンテンツファイル生成手段９０１と、コンテンツの利用に適用するプログラムまたは適用情報を含むコンテンツコードを格納し、さらに改ざん検証用データを含むコンテンツコードファイルを生成するコンテンツコードファイル生成手段９０２と、コンテンツファイル生成手段９０１において生成したコンテンツファイル、およびコンテンツコードファイル生成手段９０２において生成したコンテンツコードファイルを情報記録媒体に記録する記録手段９０３を有する。

【０２４１】

コンテンツコードファイル生成手段９０２は、コンテンツコードファイルに格納する改ざん検証用データとして、コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名、あるいは、コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づくハッシュ値を格納したファイルを生成する。

【０２４２】

また、コンテンツコードファイル生成手段９０２は、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する。例えば、先に、図１５を参照して説明した４つのカテゴリである。記録手段９０３は、これらの複数の異なるカテゴリのコンテンツコードファイルを情報記録媒体に記録する処理を実行する。

【０２４３】

なお、コンテンツコードファイル生成手段９０２は、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルを生成する場合、生成ファイル中、すべてのファイルに電子署名を格納したファイルを生成するか、または、１つのファイルのみを電子署名データを含むコンテンツコードファイルとして生成する処理を実行する。先に、図１７～図２０を参照して説明したファイル構成である。

【０２４４】

また、コンテンツコードファイル生成手段９０２の生成するファイルに記録される電子署名は、管理センタ（ＫＩＣ）の電子署名のみ、あるいは管理センタの電子署名と、各ファイルに含まれるコンテンツコードの製作または提供エンティティの電子署名が含まれる。

【０２４５】

このような、情報記録媒体製造装置によって生成された情報記録媒体９１０は、図１他を参照して説明した各種利データが記録される。具体的には、少なくともコンテンツデータを格納したコンテンツファイルと、コンテンツの利用に適用するプログラムまたは適用情報を含むコンテンツコードを格納し、さらに改ざん検証用データを含むコンテンツコードファイルとが格納される。

【０２４６】

コンテンツコードファイルに含まれる改ざん検証用データは、コンテンツコードファイルに含まれるコンテンツコードを含むデータに基づく電子署名、またはハッシュ値である。また、コンテンツコードファイルは、先に図１５を参照して説明したように、複数の異

なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルによって構成される。

【０２４７】

また、情報記録媒体に記録されるコンテンツコードファイルは、複数の異なるカテゴリに区分されるコンテンツコードを格納した複数のコンテンツコードファイルによって構成され、先に、図１８、図２０を参照して説明したように、複数の記録ファイル中、１つのファイルのみが電子署名データを含むコンテンツコードファイルとして設定するか、あるいは、全てのファイルに電子署名を含む構成とする。

【０２４８】

また、先に、図１９、図２０を参照して説明したように、コンテンツコードファイルには、各ファイルに含まれるコンテンツコードの製作または提供エンティティの電子署名を含める構成としてもよい。

【０２４９】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

【０２５０】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０２５１】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０２５２】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０２５３】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０２５４】

以上、説明したように、本発明の一実施例の構成によれば、情報記録媒体に記録されたコンテンツの再生処理を実行する際に、コンテンツの利用に適用するプログラムまたは適用情報を含むコンテンツコードを取得し、取得コンテンツコードに従ったデータ処理を実行する前の段階において、コンテンツコードを格納したコンテンツコードファイルに設定された電子署名の検証処理を実行し、該検証の結果、コンテンツコードファイルの正当性

が確認されたことを条件として、コンテンツコードに従ったデータ処理を実行する構成としたので、不正なコンテンツコードの実行が防止され、コンテンツコードの不正利用によるコンテンツの不正再生、利用を防止することが可能となる。

【０２５５】

また、本発明の一実施例の構成によれば、情報記録媒体に記録され情報処理装置において利用されるコンテンツコードファイルが複数設定される場合においても、少なくとも１つのファイルに電子署名を設定して、電子署名の検証による検証の成立を条件としてコンテンツコードの利用を可能とする構成としたので、厳格なコンテンツコードの利用制御が実現される。

【図面の簡単な説明】

【０２５６】

【図１】情報記録媒体の格納データおよびドライブ装置、情報処理装置の構成および処理について説明する図である。

【図２】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの設定例について説明する図である。

【図３】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットとユニット鍵との対応について説明する図である。

【図４】情報記録媒体に記録されるコンテンツ、管理データ等のディレクトリ構成を示す図である。

【図５】情報記録媒体に記録されるコンテンツコードのディレクリ構成を示す図である。

【図６】情報記録媒体に記録されるコンテンツと、コンテンツ再生において必要となるデータ変換処理について説明する図である。

【図７】情報記録媒体に格納されるコンテンツおよび変換テーブルの詳細について説明する図である。

【図８】変換テーブルに含まれる変換エントリのデータ構成を示す図である。

【図９】コンテンツを構成するＴＳパケット内の変換エントリを適用したデータ変換処理について説明する図である。

【図１０】変換テーブル中の変換エントリを適用したデータ変換処理について説明する図である。

【図１１】再生（プレーヤ）アプリケーションと、セキュアＶＭとの間で実行される処理シーケンスについて説明する図である。

【図１２】再生（プレーヤ）アプリケーションと、セキュアＶＭ間の処理シーケンス中のタイトル初期化処理において実行される変換テーブルのコピー処理について説明する図である。

【図１３】コンテンツ再生処理の処理例について説明する図である。

【図１４】コンテンツ再生の際に実行するデータ変換処理について説明する図である。

【図１５】情報記録媒体に記録されるコンテンツコードの詳細について説明する図である。

【図１６】情報記録媒体に記録されるコンテンツコードの生成、記録プロセスの詳細について説明する図である。

【図１７】情報記録媒体に記録されるコンテンツコードファイルのデータ構成例について説明する図である。

【図１８】情報記録媒体に記録されるコンテンツコードファイルのデータ構成例について説明する図である。

【図１９】情報記録媒体に記録されるコンテンツコードファイルのデータ構成例について説明する図である。

【図２０】情報記録媒体に記録されるコンテンツコードファイルのデータ構成例について説明する図である。

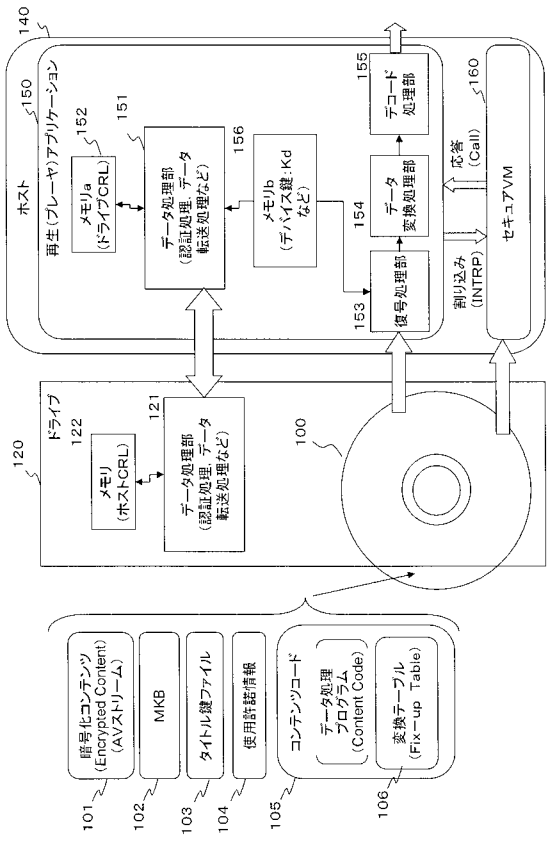
【図２１】情報記録媒体に記録されたコンテンツコードの利用シーケンスについて説明するフローチャートを示す図である。

【図２２】情報記録媒体に記録されたコンテンツコードの利用シーケンスについて説明するフローチャートを示す図である。
【図２３】コンテンツコードの利用例について説明する図である。
【図２４】情報処理装置のハードウェア構成例について説明する図である。
【図２５】情報記録媒体製造装置の構成について説明するブロック図である
【符号の説明】
【０２５７】
１００　情報記録媒体
１０１　暗号化コンテンツ
１０２　ＭＫＢ
１０３　タイトル鍵ファイル
１０４　使用許諾情報
１０５　コンテンツコード
１０６　変換テーブル
１２０　ドライブ
１２１　データ処理部
１２２　メモリ
１４０　ホスト
１５０　再生（プレーヤ）アプリケーション
１５１　データ処理部
１５２　メモリａ
１５３　復号処理部
１５４　データ変換処理部
１５５　デコード処理部
１５６　メモリｂ
１６０　セキュアＶＭ
２１０　インデックス
２２０　ムービーオブジェクト
２３０　プレイリスト
２４０　クリップ
２６１，２６２，２６３　ＡＶストリーム
２７１，２７２　コンテンツ管理ユニット（ＣＰＳユニット）
２８１　データ部
２９１　記録コンテンツ
２９２　コンテンツデータ
２９３　ブロークンデータ
２９５　変換エントリ
２９６　再生コンテンツ
２９７　変換データ
２９８　識別子設定変換データ
３００　暗号化コンテンツ
３０１　変換エントリ
３０２　コンテンツコード
３０３　変換テーブル
３０４　変換エントリ
３０７　ＴＳパケット
３０８，３０９　ＴＳパケット
３１１～３１４　パケット
３１５　ＸＯＲｅｄ変換エントリ
３１６　シークレットパラメータ

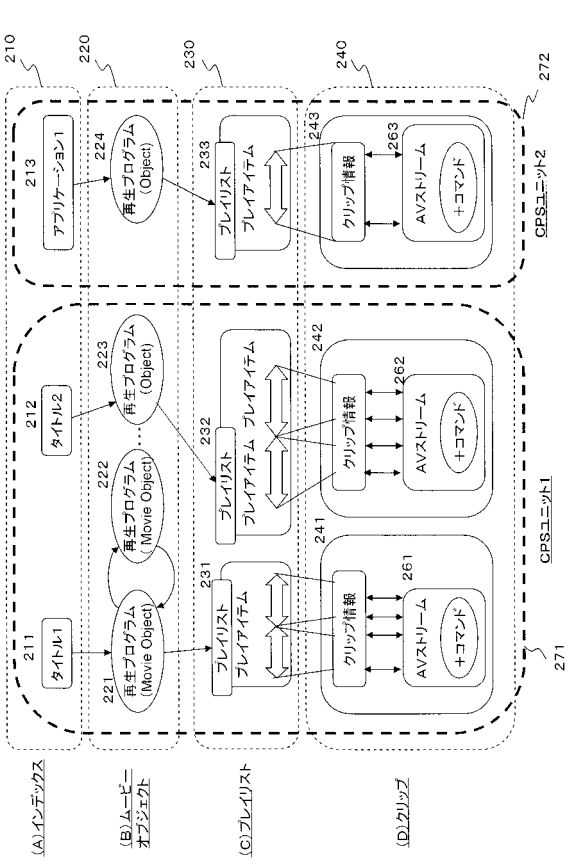
３１７　変換エントリ
３２０　セキュアＶＭ
３３０　情報記録媒体
３３１　ＭＫＢ
３３２　タイトル鍵ファイル
３３３　暗号化コンテンツ
３３４　コンテンツコード
３３５　分散記録変換エントリ
３３６　変換テーブル
３４０　ドライブ
３４５　ホスト
３５０　再生（プレーヤ）アプリケーション
３５１　デバイス鍵
３５２　トラックバッファ
３５３　平文ＴＳバッファ
３５４　イベントハンドラ
３５５　プレーヤ情報
３５６　リアルタイムイベントハンドラ
３６０　セキュアＶＭブロック
３６１　セキュアＶＭ
４０１　トラックバッファ格納データ
４０２　復号結果データ
４０３　ブロークンデータ
４０４　変換データ
４０５　識別子設定変換データ
４０６　変換処理済みデータ
５００　コンテンツコード
５０１～５０４　コンテンツコード構成データ
５２１～５２３　コンテンツコードファイル
５３０　コンテンツコードファイル
５３１　ヘッダ
５３２　コンテンツコードブロック
５３３　電子署名
５４０　コンテンツコードファイル
５４１　ヘッダ
５４２　コンテンツコードブロック
５５０　コンテンツコードファイル
５５１　ヘッダ
５５２　コンテンツコードブロック
５５３　電子署名
５５４　電子署名
５６０　コンテンツコードファイル
５６１　ヘッダ
５６２　コンテンツコードブロック
６０１～６０４　コンテンツコードファイル
６１０　情報記録媒体
６２０　コンテンツコード
６２１　変換テーブル
８０１　バス
８０２　入出力Ｉ／Ｆ

８０３　ＭＰＥＧコーデック
８０４　入出力Ｉ／Ｆ
８０５　Ａ／Ｄ，Ｄ／Ａコンバータ
８０６　ＴＳ・ＰＳ処理手段
８０７　暗号処理手段
８０８　ＲＯＭ
８０９　ＣＰＵ
８１０　メモリ
８１１　ドライブ
８１２　記録媒体
９０１　コンテンツファイル生成手段
９０２　コンテンツコードファイル生成手段
９０３　記録手段
９１０　情報記録媒体

【図１】



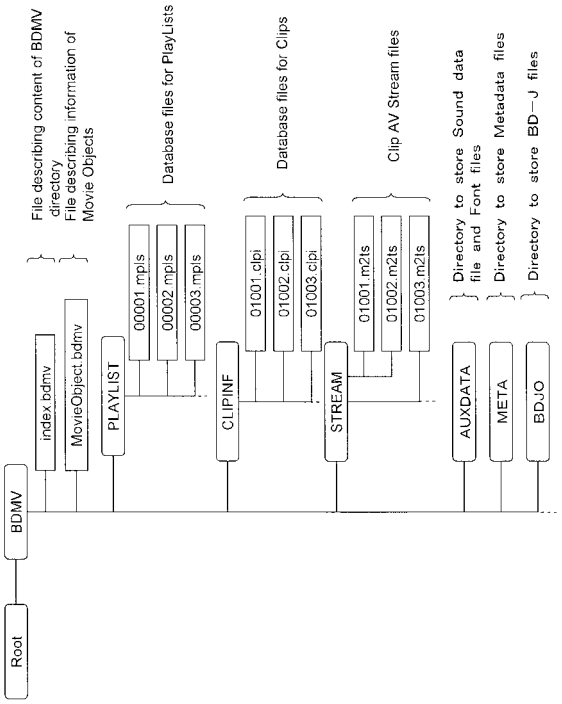
【図２】



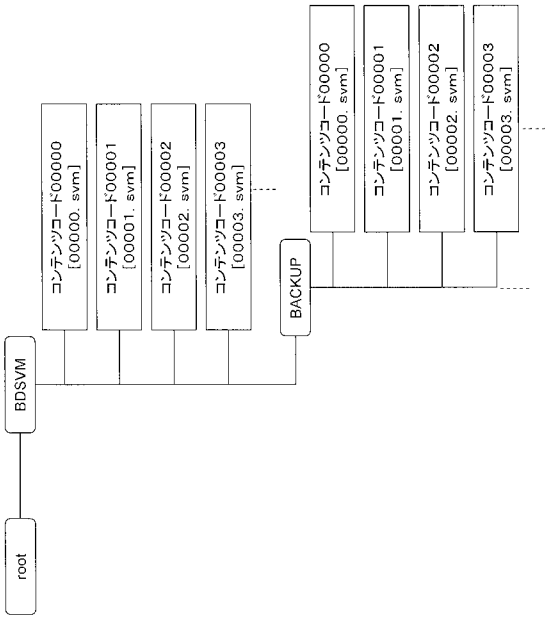
【図３】


生成可能な
タイトル鍵(CPSユニット鍵)
コンテンツ管理ユニット
(CPS)設定単位
コンテンツ管理
ユニット識別子
(CPSユニットID)
タイトル鍵
(CPSユニット鍵)
タイトル1
タイトル2
アプリケーション1
アプリケーション2
データグループ1
データグループ2
新規データ1
新規データ2
CPS1
CPS2
CPS3
CPS4
CPS5
CPSa
CPSb
Kt1
Kt2
Kt3
Kt4
Kt5
Kta
Ktb
281

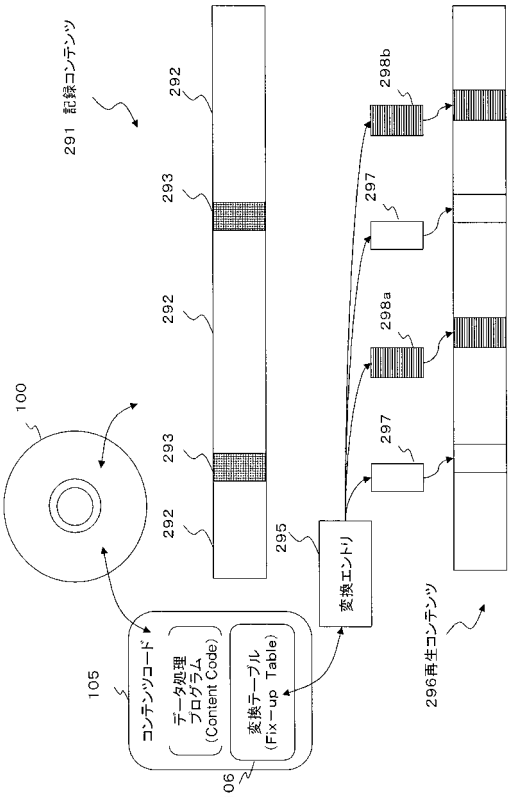
【図４】


Root
BDMV
index.bdmv
MovieObject.bdmv
PLAYLIST
CLIPINF
STREAM
AUXDATA
META
BDJO
00001.mpls
00002.mpls
00003.mpls
01001.clpi
01002.clpi
01003.clpi
01001.m2ts
01002.m2ts
01003.m2ts
File describing content of BDMV directory
File describing information of Movie Objects
Database files for PlayLists
Database files for Clips
Clip AV Stream files
Directory to store Sound data file and Font files
Directory to store Metadata files
Directory to store BD-J files

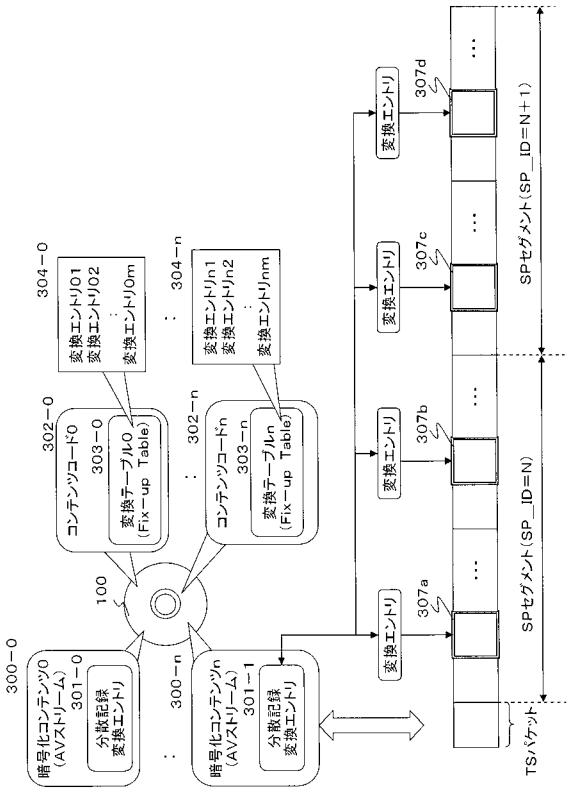
【図５】


root
BDSVM
BACKUP
コンテンツコード00000
[00000.svm]
コンテンツコード00001
[00001.svm]
コンテンツコード00002
[00002.svm]
コンテンツコード00003
[00003.svm]

【図６】


291 記録コンテンツ
292
293
295
297
298a
298b
100
105
106
コンテンツコード
データ処理プログラム
(Content Code)
変換テーブル
(Fix-up Table)
変換エントリ
296再生コンテンツ

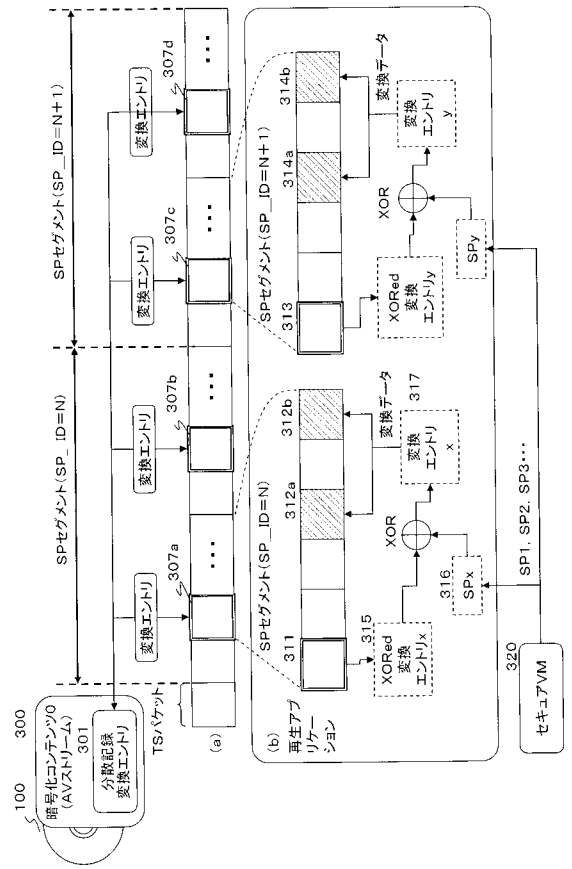
【図７】



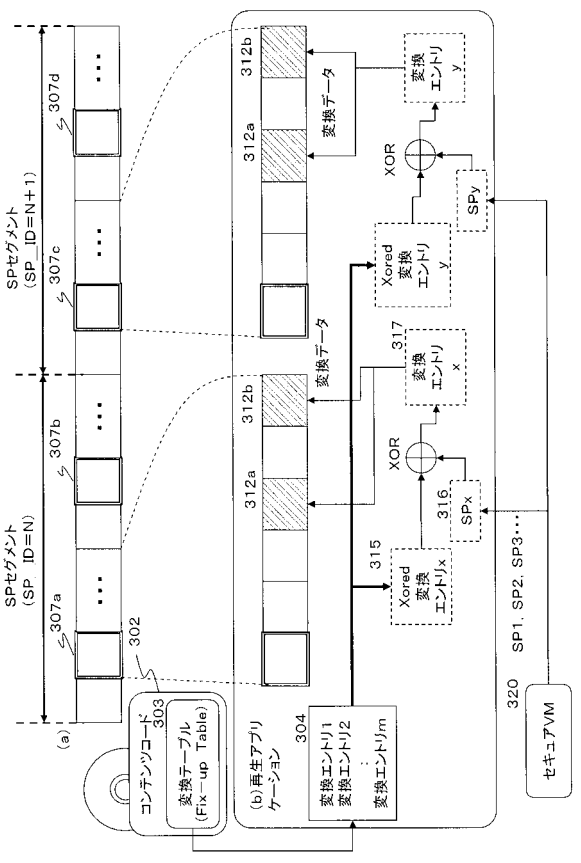
【図８】

FixUpEntry(){	Bits	Description
type_indicator	2	タイプ識別子[00:変換なし, 01b:変換データによる処理, 10b,11b:識別マーク入り変換データによる処理] 00b:no transform, 01b:transform, 10b and 11b:forensic
FM_ID_bit_position	6	識別マーク入り変換データに対応するプレーヤIDの識別ビット位置 Indicate bit position of Player ID for forensic (MSB is second bit of type_indicator)
relative_SPN	12	変換データ適用パケット位置(PMTパケットからのパケット数) Relative packet number from PMT to transformed packet
byte_position	8	パケット内の変換データ記録位置 Start byte position of transformed data in the packet (more than 5)
overwrite_value	5x8	変換データ Value to be overwritten
relative_SPN_2	12	第2変換データ適用パケット位置(PMTパケットからのパケット数) Relative packed number from PMT to second transformed packet
byte_position_2	8	パケット内の変換データ記録位置(第2変換データ対応) Start byte position of transformed data in the second packet
overwrite_value_2	5x8	第2変換データ Second value to be overwritten
}		

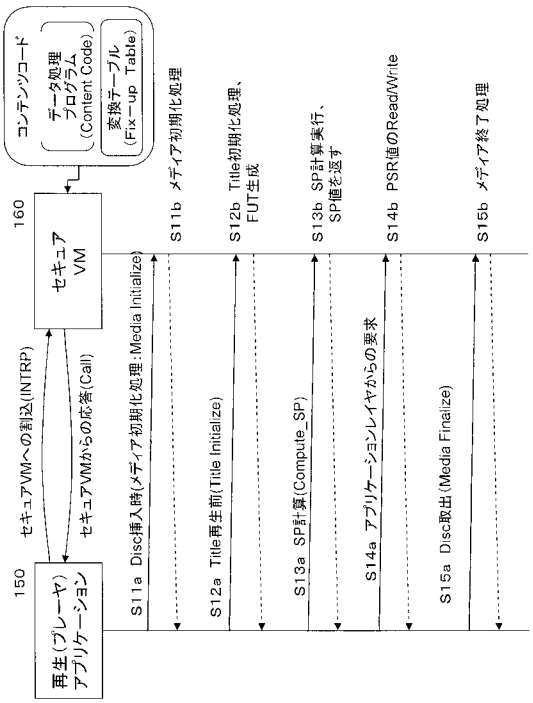
【図９】



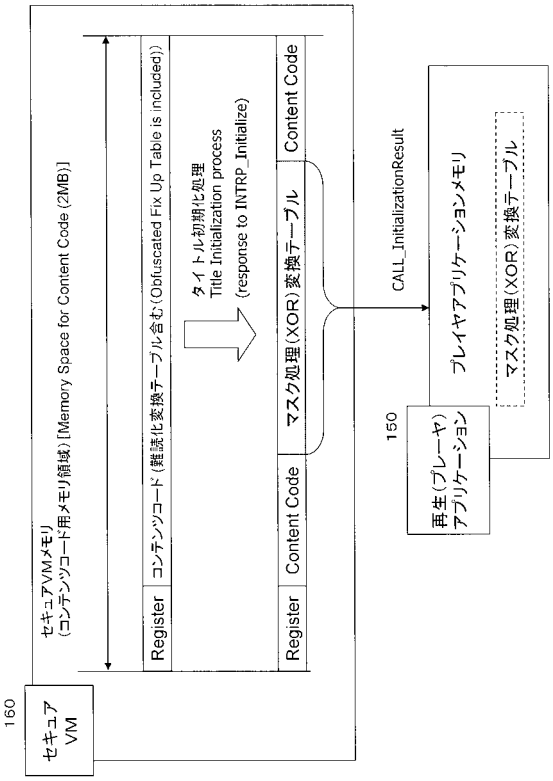
【図１０】



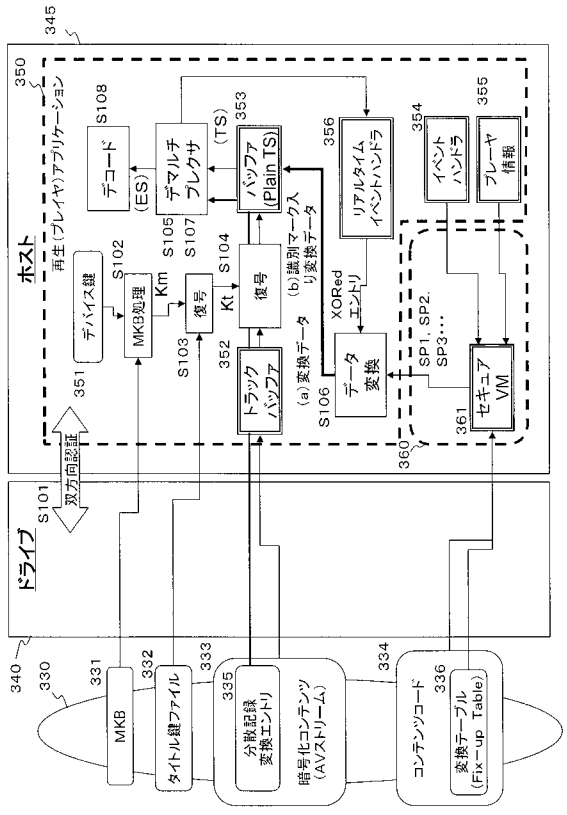
【図１１】



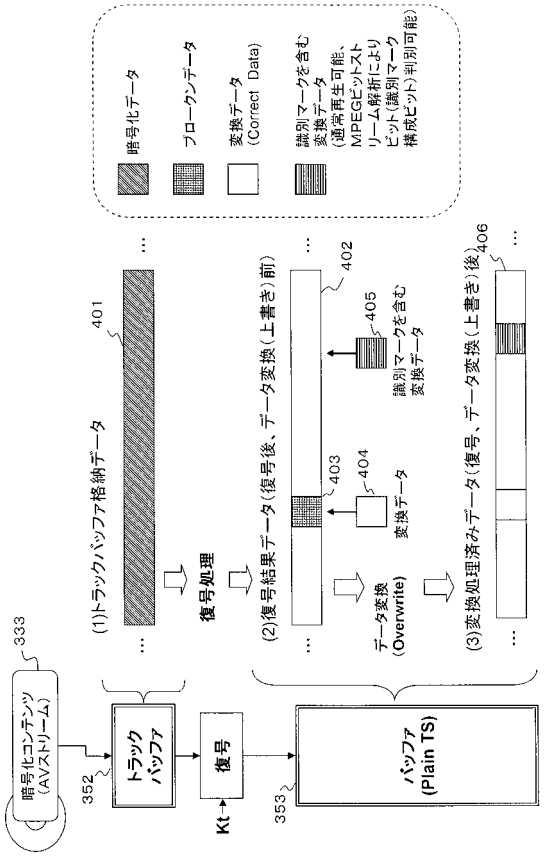
【図１２】



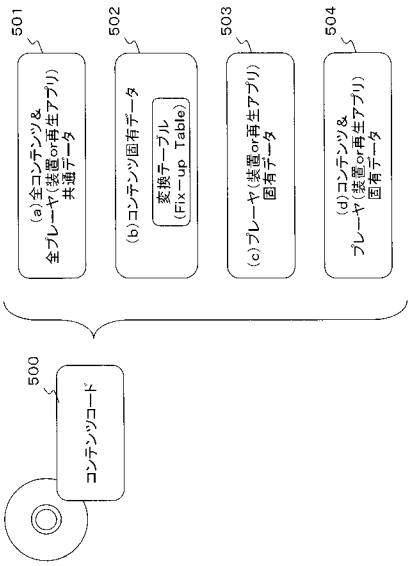
【図１３】



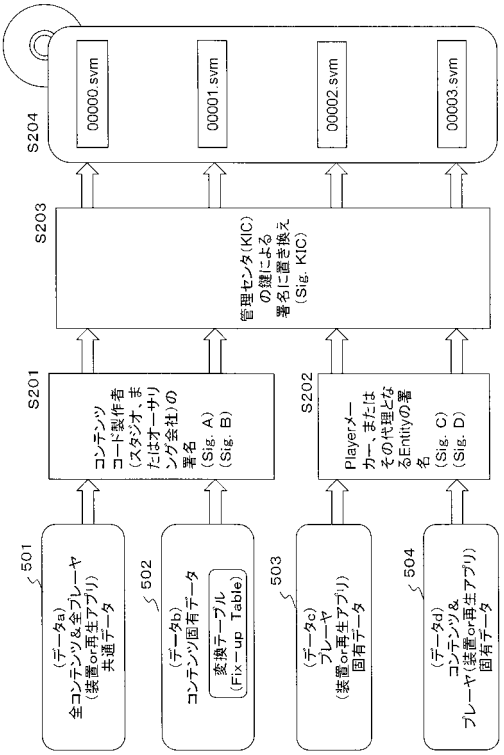
【図１４】



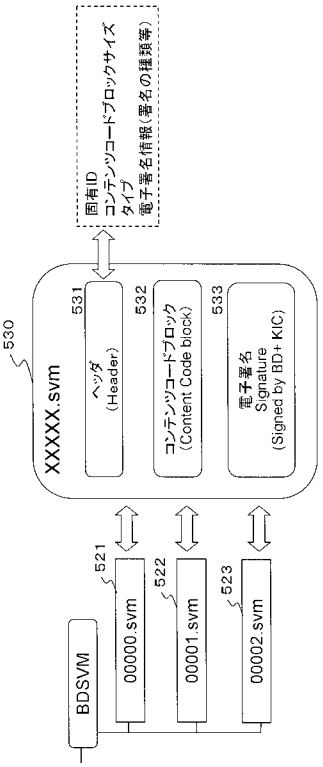
【図１５】



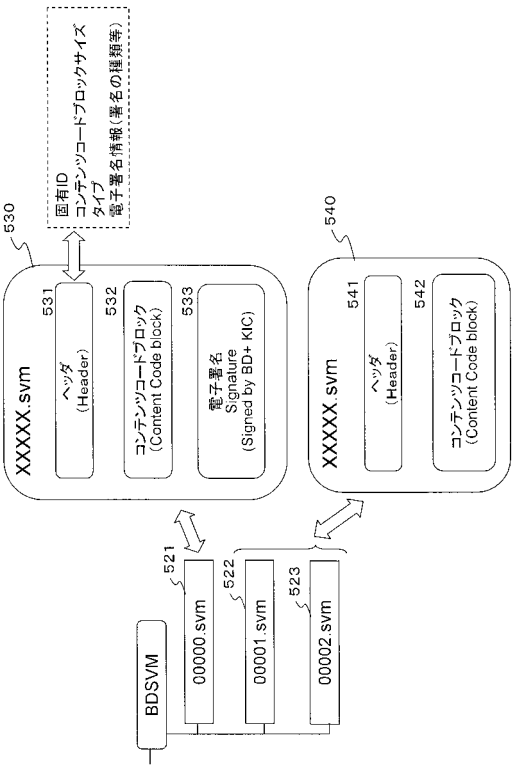
【図１６】



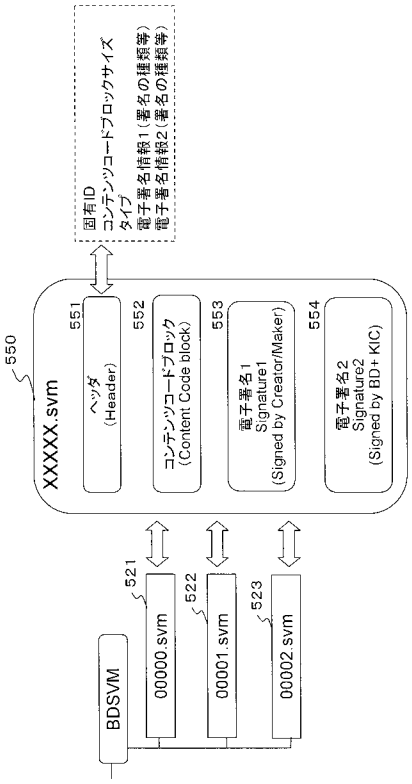
【図１７】



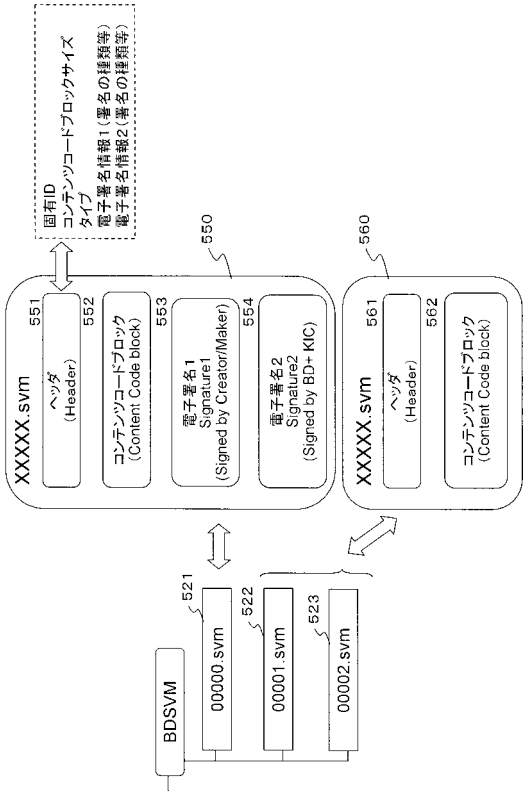
【図１８】



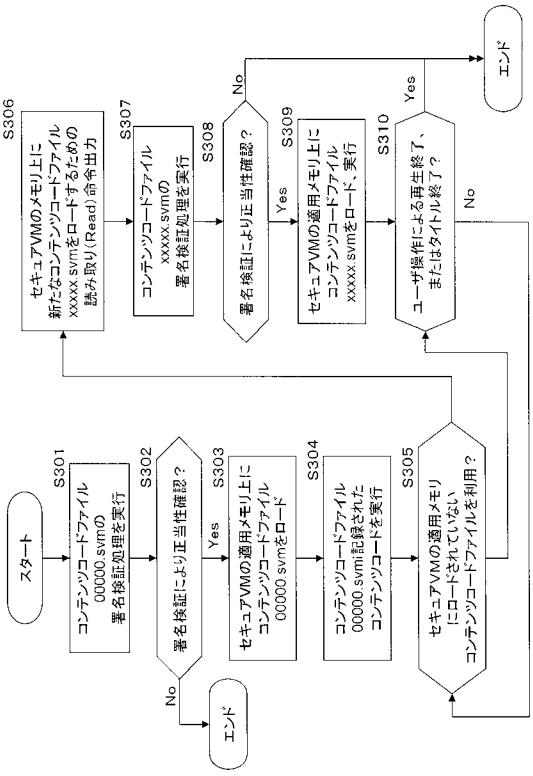
【図１９】



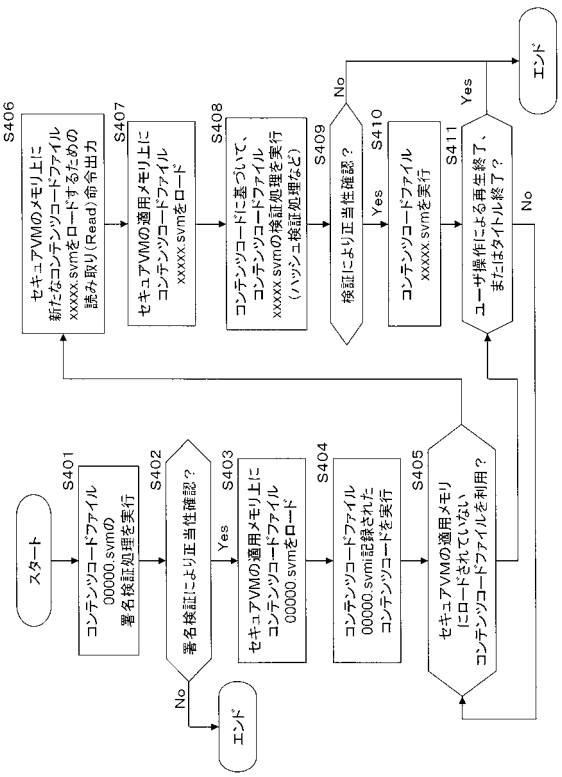
【図２０】



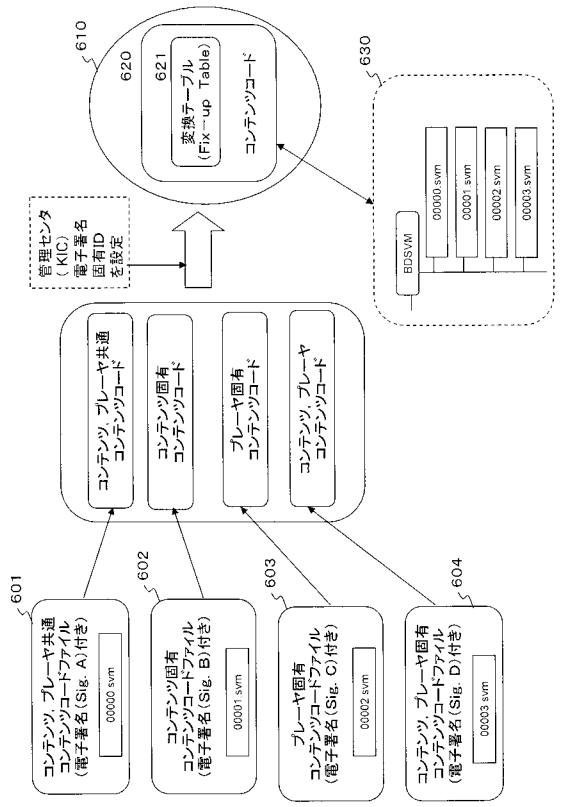
【図２１】



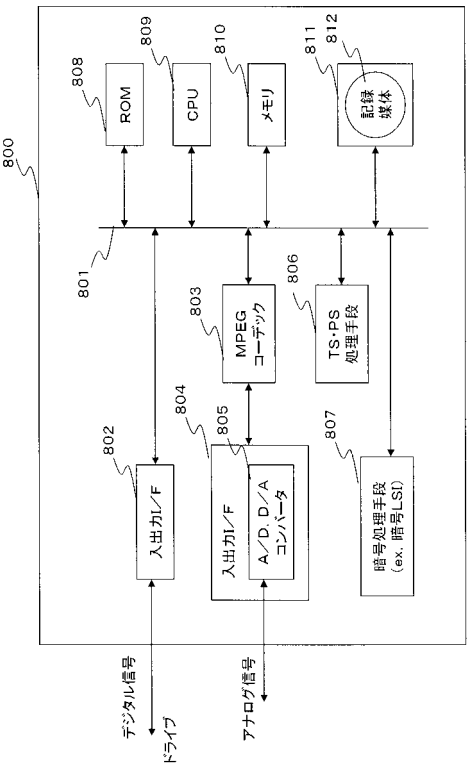
【図２２】



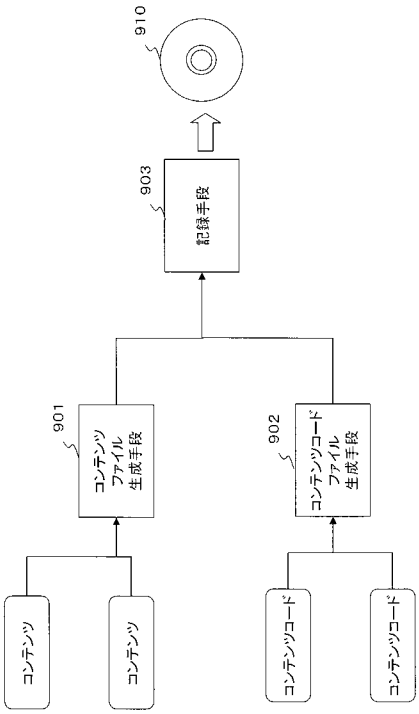
【図２３】


610
620
621
変換テーブル
(Fix-up Table)
コンテンツコード
630
BDSVM
00000.svm
00001.svm
00002.svm
00003.svm
管理センタ
(KIC)
電子署名
固有ID
を設定
コンテンツ,プレーヤ共通
コンテンツコード
コンテンツ固有
コンテンツコード
プレーヤ固有
コンテンツコード
コンテンツ,プレーヤ
コンテンツコード
601
602
603
604
コンテンツ,プレーヤ共通
コンテンツコードファイル
(電子署名(Sig. A)付き)
00000.svm
コンテンツ固有
コンテンツコードファイル
(電子署名(Sig. B)付き)
00001.svm
プレーヤ固有
コンテンツコードファイル
(電子署名(Sig. C)付き)
00002.svm
コンテンツ,プレーヤ固有
コンテンツコードファイル
(電子署名(Sig. D)付き)
00003.svm

【図２４】


800
801
808
ROM
809
CPU
810
メモリ
811
812
記録
媒体
803
MPEG
コーデック
806
TS・PS
処理手段
802
入出力I／F
804
805
入出力I／F
A／D, D／A
コンバータ
807
暗号処理手段
(ex. 暗号LSI)
デジタル信号
ドライブ
アナログ信号

【図２５】


910
903
記録手段
901
コンテンツ
ファイル
生成手段
902
コンテンツコード
ファイル
生成手段
コンテンツ
コンテンツ
コンテンツコード
コンテンツコード

フロントページの続き

(56)参考文献 特開２００３－１０９３０３（ＪＰ，Ａ）
特開２００５－０７１０３７（ＪＰ，Ａ）
特開２００２－１４９０６１（ＪＰ，Ａ）
特表２００４－５３２４９５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ１１Ｂ　２０／１０
Ｈ０４Ｌ　９／３２
Ｇ１１Ｂ　２７／００
Ｇ０６Ｆ　１２／１４