

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4177517号
(P4177517)

(45) 発行日 平成20年11月5日(2008.11.5)

(24) 登録日 平成20年8月29日(2008.8.29)

(51) Int.Cl. F I
G06F 21/24 (2006.01) G06F 12/14 540C
 G06F 12/14 540P

請求項の数 5 (全 15 頁)

(21) 出願番号	特願平11-141697	(73) 特許権者	000003078
(22) 出願日	平成11年5月21日(1999.5.21)		株式会社東芝
(65) 公開番号	特開2000-330870(P2000-330870A)		東京都港区芝浦一丁目1番1号
(43) 公開日	平成12年11月30日(2000.11.30)	(74) 代理人	100058479
審査請求日	平成17年7月6日(2005.7.6)		弁理士 鈴江 武彦
		(74) 代理人	100084618
			弁理士 村松 貞男
		(74) 代理人	100092196
			弁理士 橋本 良郎
		(74) 代理人	100091351
			弁理士 河野 哲
		(74) 代理人	100088683
			弁理士 中村 誠
		(74) 代理人	100070437
			弁理士 河井 将次

最終頁に続く

(54) 【発明の名称】 コンテンツ処理システムおよびコンテンツ保護方法

(57) 【特許請求の範囲】

【請求項1】

記録メディアに記録されるコンテンツを保護するために必要な制御情報を前記記録メディア上に秘匿化して記録するコンテンツ処理システムであって、

前記記録メディア上の記録領域の中でファイルシステムからはアクセスできない所定の記憶領域を前記制御情報を秘匿化するための秘匿エリアとして使用し、前記制御情報またはその改竄検出用データを、前記記録メディア上に記録されている固有のメディアIDに基づいて生成される所定の暗号化鍵によって暗号化した後に、前記秘匿エリアに記録するコンテンツ管理手段を具備し、前記記録メディア上には、データ領域と、その代替領域とが設けられおり、前記コンテンツ管理手段は、前記代替領域を前記秘匿エリアとして使用することを特徴とするコンテンツ処理システム。

10

【請求項2】

前記制御情報は、前記コンテンツのコピー/移動を制限するためのコピー制御情報であり、

前記コンテンツ管理手段は、前記記録メディアに記録されているコンテンツを他の記録メディアにコピーまたは移動する場合には、前記記録メディア上に記録されている固有のメディアIDに基づいて生成される暗号化鍵によって前記記録メディア上の暗号化された制御情報を復号化し、その復号化された制御情報に基づいて、前記コンテンツのコピーまたは移動の可否を判断することを特徴とする請求項1記載のコンテンツ処理システム。

【請求項3】

20

前記コンテンツ管理手段は、前記記録メディアをドライブするためのドライブ装置との認証によって所定の秘密鍵を前記ドライブ装置との間で共有し、前記暗号化された制御情報または改竄検出用データを前記秘匿エリアに記録する場合には、前記暗号化された制御情報または改竄検出用データを前記秘密鍵によって暗号化した後に前記ドライブ装置に送信することを特徴とする請求項 1 記載のコンテンツ処理システム。

【請求項 4】

記録メディアに記録されるコンテンツを保護するために必要な制御情報を前記記録メディア上に秘匿化して記録することにより、前記コンテンツを保護するコンテンツ保護方法であって、

前記記録メディア上には、データ領域と、その代替領域とが設けられおり、前記記録メディア上の記録領域の中でファイルシステムからはアクセスできない前記代替領域を前記制御情報を秘匿化するための秘匿エリアとして使用し、前記制御情報またはその改竄検出用データを、前記記録メディア上に記録されている固有のメディア ID に基づいて生成される所定の暗号化鍵によって暗号化した後に、前記秘匿エリアに記録することを特徴とするコンテンツ保護方法。

【請求項 5】

前記制御情報は、前記コンテンツのコピー / 移動を制限するためのコピー制御情報であり、

前記記録メディアに記録されているコンテンツを他の記録メディアにコピーまたは移動する場合には、前記記録メディア上に記録されている固有のメディア ID に基づいて生成される暗号化鍵によって前記記録メディア上の暗号化された制御情報を復号化し、その復号化された制御情報に基づいて、前記コンテンツのコピーまたは移動の可否を判断することを特徴とする請求項 4 記載のコンテンツ保護方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像データや音楽データなどの様々なデジタルコンテンツを扱うことが可能なコンテンツ処理システムおよびコンテンツ保護方法に関する。

【0002】

【従来の技術】

近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレイヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなどの様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【0003】

これらデジタルコンテンツは、例えば MPEG 2、MP 3 といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【0004】

【発明が解決しようとする課題】

しかし、パーソナルコンピュータ、セットトップボックス、プレイヤーなどの電子機器で用いられる記録メディアは、別の機器に移動しても記録 / 再生ができるリレーバブルなものが多く、その仕様は基本的にはオープンである。このため、ファイルのコピー / 移動を自由に行うことができるので、記録メディアに記録されたコンテンツを不正なコピー / 移動などから保護することは実際上困難である。

【0005】

メモ리카ードのように記録メディア部とコントローラとが一体化された記録メディアについては、ユーザからはアクセスできない秘匿エリアをコントローラ内に設け、そこに、例

10

20

30

40

50

えば、コピー制御情報などの、デジタルコンテンツの使用に必要な重要な情報を格納しておくことなどによってコンテンツ保護を行うことが可能である。

【0006】

ところが、次世代の記録メディアとして注目されているDVD-RAMや、ポータブルオーディオ機器の記録メディアとして使用されているMDなどの記録メディアについては、その記録メディア単体で機器間の交換が行われるので、物理的に秘匿エリアを設けることは困難である。ファイルシステムからアクセスできない領域を秘匿エリアとして使用することも考えられているが、この場合であっても、悪意を持つものによる不正な攻撃に対しては十分ではない。記録メディアそのものは基本的にはセクタの集まりから構成されているので、その記録メディアの物理仕様さえ分かれば全面アクセスが可能であるからである。したがって、悪意を持つ者によって不正なドライブ装置が開発されたり、あるいはそのドライブ装置が一般ユーザによって用いられた場合には、コピー制御情報などのコンテンツ保護のための重要な情報が記録メディアから盗まれ、改竄されてしまう危険がある。

10

【0007】

本発明は上述の事情に鑑みてなされたものであり、DVD-RAMなどの記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようにし、デジタルコンテンツの利用と保護の両立を図ることが可能なコンテンツ処理システムおよびコンテンツ保護方法を提供することを目的とする。

【0008】

【課題を解決するための手段】

20

上述の課題を解決するため、本発明は、記録メディアに記録されるコンテンツを保護するために必要な制御情報を前記記録メディア上に秘匿化して記録するコンテンツ処理システムであって、前記記録メディア上の記録領域の中でファイルシステムからはアクセスできない所定の記憶領域を前記制御情報を秘匿化するための秘匿エリアとして使用し、前記制御情報またはその改竄検出用データを、前記記録メディア上に記録されている固有のメディアIDに基づいて生成される所定の暗号化鍵によって暗号化した後に、前記秘匿エリアに記録するコンテンツ管理手段を具備し、前記記録メディア上には、データ領域と、その代替領域とが設けられおり、前記コンテンツ管理手段は、前記代替領域を前記秘匿エリアとして使用することを特徴とする。

【0009】

30

このコンテンツ処理システムにおいては、ファイルシステムからはアクセスできない所定の記憶領域を秘匿エリアとして使用するだけでなく、その秘匿エリアに記録される情報については、記録メディア毎に固有のメディアIDから生成される暗号化鍵を用いて暗号化している。このため、記録メディア単体で機器間の交換が行われるような記録メディアを用いた場合でも、コンテンツ保護のために必要な情報を秘匿化して記録することができる。また、暗号化鍵はメディアIDから生成しているため、その記録メディアを別の機器に移動して使用しても、メディアIDから暗号化鍵を正しく生成するためのアルゴリズムを知っている正当な機器であれば、必要な情報を正しく復元することができる。したがって、同一記録メディアであれば、その記録メディアを別の機器に移動してもコンテンツを正しく再生することが可能となり、コンテンツの利用と保護の両立を図ることができる。

40

【0010】

前記記録メディア上には、その記録メディアに固有のメディアIDと、秘密のアルゴリズムで作成された秘密データとを記録しておき、それらメディアIDと秘密データから暗号化鍵を生成することが好ましい。これにより、暗号化鍵についても十分な秘匿化を図ることができる。

【0011】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態を説明する。

【0012】

図1には、本発明の一実施形態に係るパーソナルコンピュータ(PC)のシステム構成が

50

示されている。このパーソナルコンピュータ（PC）11は、画像データや音楽データなどの各種デジタルコンテンツを扱うことが可能なコンピュータシステムである。このパーソナルコンピュータ（PC）11におけるコンテンツ保護の方法は、コンテンツを記録すべき記録メディア毎にその記録メディアのメディアIDを用いてコンテンツの暗号化／復号化を管理することを前提としている。これは、同一記録メディアであれば、その記録メディアを他のパーソナルコンピュータや電子機器で使用しても再生できるようにするためであり、コンテンツは各記録メディア毎に用意された専用のメディア識別用情報（ここでは、メディアキーと称する）を用いて暗号化して記録される。メディアキーを用いたコンテンツの暗号化／復号化の管理は、そのための専用のソフトウェアであるセキュアマネージャ112によって実行される。このセキュアマネージャ112はタンバ・レジスタント・ソフトウェアとして実現されている。タンバ・レジスタント・ソフトウェアとは、不正な内部解析や改竄などの攻撃に対して防衛機能を備えるソフトウェアを意味する。

10

【0013】

セキュアマネージャ112は図示のようにアプリケーションプログラム111とファイルシステム113との間に位置し、保護対象のコンテンツについての「記録」、「再生」、「コピー」、「移動」などの各種操作は、セキュアマネージャ112を介して行われる。セキュアマネージャ112によるコンテンツの暗号化／復号化管理は、1)物理的な秘匿エリアを有する専用の記録メディアに対するものと、2)物理的な秘匿エリアを持たない通常の記録メディアに対するものとに、大別される。

【0014】

（物理的な秘匿エリアを有する専用の記録メディア）

まず、物理的な秘匿エリアを有する専用の記録メディアに対する処理について説明する。

20

【0015】

記録メディア（A）116、および記録メディア（B）117は、それぞれセキュアマネージャ112に対応した専用の記録メディアである。これら記録メディアとしては、パーソナルコンピュータ（PC）11や他の各種電子機器に着脱自在に装着可能なメモリカードなどの各種媒体（SSFD C、フラッシュPCカード）などを使用することができる。これら記録メディア（A）116、および記録メディア（B）117においては、記録メディア部とコントローラ部（またはハードウェアロジック部）とが一体化されており、コンテンツ保護に必要な重要な情報についてはコントローラ部に設けられた専用の秘匿エリアに記録される。

30

【0016】

記録メディア（A）116の秘匿エリアには、その記録メディアに固有のメディアキー（ MK_A ）が予め記憶されているROM領域と、後述のGI（Governance Information）テーブルから作成されたGIチェックサムデータを格納するためのGIチェックサム領域とが設けられている。記録メディア（B）117についても同様の構成である。メディアキーは各記録メディアに固有であれば良く、シリアル番号や製造番号、他の様々な識別情報を利用することができる。

【0017】

GIテーブルとは、保護対象の各コンテンツ毎にその再生、コピー、移動の可否、およびコピー可能回数、移動可能回数などを規定したコピー制御情報を含む統制情報である。GIチェックサムデータはGIテーブルの内容の改竄を検出するための改変検出用コードデータであり、GIテーブルの値から算出される。GIチェックサムデータの代わりにGIテーブルのハッシュ値を用いることもできる。GIテーブルの「コピー可能回数」の値は、コピーが実行される度に-1減算される。このようにGIテーブルの値が更新される度に、その更新に合わせて、GIチェックサムデータの値も更新される。このため、GIチェックサム領域は書き換え可能な領域から構成されている。

40

【0018】

ROM領域およびGIチェックサム領域のどちらも、ユーザからはアクセスできないセキュアな領域となっている。

50

【 0 0 1 9 】

コンテンツを記録メディア (A) 1 1 6 に記録する場合には、セキュアマネージャ 1 1 2 は、記録メディア (A) 1 1 6 のメディアキー (MK_A) を用いてコンテンツの暗号化 / 復号化を管理する。この場合、記録メディア (A) 1 1 6 のデータ領域には、以下のデータが格納される。

【 0 0 2 0 】

・ $Kc [Content]$: コンテンツキー Kc と称される秘密鍵によって暗号化されたコンテンツ

・ GI : コピー制御情報を含む統制情報

・ $MK_A [Kc]$: 記録メディア (A) 1 1 6 のメディアキー (MK_A) によって暗号化されたコンテンツキー

記録メディア (A) 1 1 6 に記録されたコンテンツを再生する場合には、セキュアマネージャ 1 1 2 は、まず、記録メディア (A) 1 1 6 のメディアキー (MD_A) を用いて $MD_A [Kc]$ を復号化し、コンテンツキー Kc を得る。そして、その Kc によって、 $Kc [Content]$ を復号化する。

【 0 0 2 1 】

記録メディア (A) 1 1 6 に記録されたコンテンツがコピー可能なコンテンツである場合、そのコンテンツを記録メディア (A) 1 1 6 から他の記録メディア (例えば記録メディア (B) 1 1 7) にコピーすることができる。この場合、セキュアマネージャ 1 1 2 は、記録メディア (A) 1 1 6 に格納された GI からチェックサムデータを生成し、そのチェックサムデータを、記録メディア (A) 1 1 6 の GI チェックサム領域の GI チェックサムデータと比較する。不一致の場合には、リプレースアタック (初期状態の GI をコピーしておき、それを必要に応じて書き戻すことにより、コピー / 移動を一度も行っていないコンテンツに偽造する行為) 等によって GI が改竄された恐れがあるので、コピーは禁止される。一致した場合には、セキュアマネージャ 1 1 2 は、記録メディア (A) 1 1 6 のメディアキー (MK_A) を用いて $MK_A [Kc]$ を復号化し、 Kc を得る。次いで、セキュアマネージャ 1 1 2 は、コピー先の記録メディア (B) 1 1 7 のメディアキー (MK_B) を用いて Kc を暗号化し、暗号化したコンテンツキー ($MK_B [Kc]$) を、 $Kc [Content]$ および GI と一緒に、記録メディア (B) 1 1 7 のデータ領域に書き込む。この場合、記録メディア (A) 1 1 6 , 記録メディア (B) 1 1 7 のどちらにおいても、 GI によって指定されるコピー可能回数の値は - 1 される。例えば、コピーしたコンテンツが「一回のみコピー可」のコンテンツであった場合には、「これ以上コピー不可」のコンテンツに変更される。また、 GI の更新に伴い、記録メディア (A) 1 1 6 , 記録メディア (B) 1 1 7 それぞれの GI チェックサムデータの値も更新される。

【 0 0 2 2 】

記録メディア (A) 1 1 6 に記録されたコンテンツが移動可能なコンテンツである場合、そのコンテンツを記録メディア (A) 1 1 6 から他の記録メディア (例えば記録メディア (B) 1 1 7) に移動することができる。この場合、セキュアマネージャ 1 1 2 は、記録メディア (A) 1 1 6 に格納された GI からチェックサムデータを生成し、そのチェックサムデータを、記録メディア (A) 1 1 6 の GI チェックサム領域の GI チェックサムデータと比較する。不一致の場合には、前述の場合と同様に、移動は禁止される。一致した場合には、セキュアマネージャ 1 1 2 は、記録メディア (A) 1 1 6 のメディアキー (MK_A) を用いて $MK_A [Kc]$ を復号化し、 Kc を得る。次いで、セキュアマネージャ 1 1 2 は、移動先の記録メディア (B) 1 1 7 のメディアキー (MK_B) を用いて Kc を暗号化し、暗号化したコンテンツキー ($MK_B [Kc]$) を、 $Kc [Content]$ および GI と一緒に、記録メディア (B) 1 1 7 のデータ領域に書き込む。この後、セキュアマネージャ 1 1 2 は、移動元の記録メディア (A) 1 1 6 のデータ領域に格納されている $Kc [Content]$ 、 GI 、 $ID_A [Kc]$ を削除すると共に、 GI チェックサム領域の GI チェックサムデータを削除する。 GI によって規定されているのが「コピー可能回数」のみで、「移動可能回数」については規定されていない場合には、移動による GI

10

20

30

40

50

の更新は行われぬ。「移動可能回数」が規定されている場合には、前述の「コピー」の場合と同様にして、G Iは更新された後に記録メディア(B) 117に書き込まれ、またその更新後のG Iに対応するチェックサムデータがG Iチェックサム領域に書き込まれることになる。

【0023】

このように再生/コピー/移動の可否はG Iによって制御されるので、コンテンツ保護のためには、G Iを改竄から保護することが重要となる。しかし、G Iは記録されるコンテンツの数だけ存在するので、そのデータサイズは比較的大きい。そこで、本実施形態では、G Iそのものではなく、そのG Iからチェックサムデータを生成し、それを安全な秘匿エリアに記録するようにしている。もちろん、G Iそのものを秘匿エリアに記録するような制御を行っても良い。

10

【0024】

(物理的な秘匿エリアを持たない通常の記録メディア)

次に、物理的な秘匿エリアを持たない通常の記録メディアに対する処理について説明する。ここでは、物理的な秘匿エリアを持たない記録メディアとして、DVD-RAMメディア115を例示して説明する。DVD-RAMドライブ114は、そこに装填されたDVD-RAMメディア115をリード/ライトするためのドライブ装置である。DVD-RAMメディア115には、記録メディア(A) 116、および記録メディア(B) 117のような物理的な秘匿エリアは設けられていない。

【0025】

DVD-RAMメディア115を用いてコンテンツの記録、再生、コピー、移動などを行う場合、セキュアマネージャ112は、DVD-RAMメディア115上のリードインエリア、セクタ代替エリア、リードアウトエリアなど、ファイルシステム113からはアクセスできない領域を秘匿エリアとして割り当て、そこに重要な情報を論理的に秘匿化して記録する。秘匿エリアにはG Iチェックサムデータが記録されるが、この場合、G Iチェックサムデータは、コンテンツキー(Kc)と同様に、DVD-RAMメディア115固有のメディアキー(MK_S)を用いて暗号化されて記録される。また、メディアキー(MK_S)については、メディアキー(MK_S)そのものをDVD-RAMメディア115上に記録するのではなく、その要素となる情報、つまり、DVD-RAMメディア115固有のメディアID、および特定の秘密アルゴリズムで作成された秘密データをDVD-RAMメディア115上に記録しておき、セキュアマネージャ112がそれらメディアIDおよび秘密データからメディアキー(MK_S)を作成するようにすることによって、秘匿化を行う。

20

30

【0026】

図2(A)に示されているように、DVD-RAMメディア115固有のメディアID(Media ID)は、DVD-RAMメディア115上のバーストカッティングエリア(BCA: Burst Cutting Area)に記録される。BCAはDVD-RAMメディア115の製造プロセス終了後に物理フォーマット情報などを記録するために使用される領域であり、ここに記録されたシリアル番号や製造番号、他の様々な識別情報がメディアIDとして用いられる。BCAは、通常のファイルシステムからはアクセスすることが出来ない。

40

【0027】

また、図2(B)に示されているように、DVD-RAMメディア115上には、データエリアの開始を示すリードインエリアとそれに後続するデータエリアが設けられており、リードインエリアには、前述の秘密データとしてメディアマーク(Media Mark)が記録されている。このメディアマークは、コンテンツ保護機能を有する正当なドライブのみが読むことが可能なデータ列である。つまり、メディアマークは、リードインエリア内の所定のECCブロック(16セクタ)内に、そのECCデータによってリカバリできるエラー情報として記録されている。エラーがあるセクタ位置とビット位置との関係により、メディアマークの値が定義される。

50

【0028】

DVD-RAMメディア115のデータエリアには、次のデータが格納される。

【0029】

・Kc[Content]：コンテンツキーKcと称される秘密鍵によって暗号化されたコンテンツ

・GI：コピー制御情報を含む統制情報

・MK_S[Kc]：DVD-RAMメディア115固有のメディアキー(MK_S)によって暗号化されたコンテンツキー

また、GIのチェックサムデータは、前述したように、メディアキー(MK_S)によって暗号化された後に、DVD-RAMメディア115上のリードインエリア、セクタ代替エリア、リードアウトエリアなど、ファイルシステム113からはアクセスできない領域に記録される。

10

【0030】

図3には、DVD-RAMドライブ114の機能構成が概念的に示されている。

【0031】

DVD-RAMドライブ114には、データリード/ライトを行うための通常の機能部に加え、認証部201と、BCAからメディアIDを読み出すためのメディアID読み出し部202と、リードインのエラー情報からメディアマークを算出(デコード)するためのメディアマーク算出部203、エラー位置の検出及び訂正を行うためのECC演算回路204などが設けられている。

20

【0032】

認証部201は、セキュアマネージャ112との間で認証を行うためのものであり、互いにコンテンツ保護機能を有する正当なもの同士であるか否かを判断する。互いに正当なもの同士であることが確認され、且つセキュアマネージャ112から予め決められた専用のコマンドが発行された場合にのみ、メディアマーク算出部203の機能は有効となる。メディアマーク算出部203がディスエーブルされている場合、あるいはメディアマーク算出部203を持たないドライブにおいては、メディアマークを読み取るためにリードインデータをリードしても、ECC演算回路204によってエラー訂正された後のデータが読み出されてしまうため、メディアマークを読み取ることはできない。つまり、メディアマークは、コピー保護機能を有する正当なドライブ装置のみが読み取ることが可能な情報である。

30

【0033】

また、メディアID読み出し部202についても、メディアマーク算出部203と同じように、認証が成功し、且つセキュアマネージャ112から予め決められた専用のコマンドが発行された場合にのみその機能を有効にするように制御しても良い。

【0034】

このようにDVD-RAMドライブ114との認証によって初めてメディアマークやメディアIDを取得できるようにすることにより、それらメディアマーク、メディアIDをより安全に管理することができる。

40

【0035】

次に、図4乃至図6を参照して、DVD-RAMメディア115を使用する場合におけるコンテンツ管理処理の手順について具体的に説明する。

【0036】

「記録」

図5はコンテンツ記録時の動作の流れを示している。

【0037】

(ステップ1)：まず、セキュアマネージャ112とDVD-RAMドライブ114との間で認証処理が実行され、互いに正しいもの同士であるか否かが確認される。互いに正しいもの同士であることが確認されると、DVD-ROMのコンテンツ暗号化アルゴリズムとして使用されているCSS(Content Scrambling System)などのランダムチャレン

50

ジ・レスポンスを用いた方法により、セキュアマネージャ112とDVD-RAMドライブ114との間でキー交換が行われ、これにより同一の認証鍵、バスキー（BK：Bus Key）が共有される。バスキー（BK）は、毎回代わる時変キーである。

【0038】

（ステップ2）：セキュアマネージャ112は、専用のコマンドを用いて、メディアIDとメディアマークの取得要求をDVD-RAMドライブ114に発行する。セキュアマネージャ112からの取得要求に回答して、DVD-RAMドライブ114は、メディアIDをBCAから読み出すと共に、リードインエリアのエラー情報からメディアマークを生成し、それらメディアID（M_ID）およびメディアマーク（MM）を、バスキー（BK）で暗号化する。そして、暗号化されたメディアIDおよびメディアマーク（BK[M_ID・MM]）をセキュアマネージャ112に送信する。セキュアマネージャ112は、バスキー（BK）を保持しているため、BK[M_ID・MM]からメディアID（M_ID）およびメディアマーク（MM）を解読することができる。そして、セキュアマネージャ112は、メディアID（M_ID）およびメディアマーク（MM）に対して予め決められた所定の演算を施すことにより、DVD-RAMメディア115固有のメディアキー（MK_S）を生成する。

10

【0039】

$MK_S = f(M_ID, MM)$

ここで、 f は秘密の関数である。

20

【0040】

（ステップ3）：WEBブラウザなどのアプリケーションプログラムを用いてWEBサーバから画像データや音楽データなどのコンテンツをダウンロードする場合には、WEBブラウザを介して、あるいは直接、セキュアマネージャ112とWEBサーバ12との間で認証処理が行われる。互いに正しいコンテンツ保護機能を有するもの同士あることが確認されると、セキュアマネージャ112とWEBサーバ12との間でキー交換が行われ、同一の認証鍵（ K_{x1} ）が共有される。認証鍵（ K_{x1} ）は毎回代わる時変キーである。

【0041】

（ステップ4）：WEBサーバ12は、要求されたコンテンツを所定のコンテンツキー K_c で暗号化したもの（ $K_c[Content]$ ）と、認証鍵（ K_{x1} ）で暗号化したコンテンツキー（ $K_{x1}[K_c]$ ）と、GIとを、PC11宛に送信する。

30

【0042】

（ステップ5）：これら、 $K_c[Content]$ 、 $K_{x1}[K_c]$ 、GIは、WEBブラウザなどを介して、セキュアマネージャ112に送られる。セキュアマネージャ112は、WEBブラウザから指定されたダウンロード先の記録メディアがDVD-RAMメディア115である場合、認証鍵（ K_{x1} ）と、DVD-RAMメディア115のメディアキー（ MK_S ）を用いて、 $K_{x1}[K_c]$ を $MK_S[K_c]$ に変換する。この場合、まず、認証鍵（ K_{x1} ）を用いて $K_{x1}[K_c]$ が K_c に復号化され、その K_c があらためて MK_S によって暗号化される。

【0043】

この後、セキュアマネージャ112は、 $K_c[Content]$ 、 $MK_S[K_c]$ 、GIを、ファイルシステム113、さらにはATAPIドライバなどを通して、DVD-RAMドライブ114に送り、DVD-RAMメディア115のデータエリアに書き込む。

40

【0044】

（ステップ6）：セキュアマネージャ112は、GIからGIチェックサムデータ（GI_CS）を算出し、それをDVD-RAMメディア115のメディアキー（ MK_S ）を用いて暗号化する（ $MK_S[GI_CS]$ ）。そして、さらに、 $MK_S[GI_CS]$ をバスキー（BK）で暗号化し（ $BK[MK_S[GI_CS]]$ ）、それをDVD-RAMドライブ114に送信してDVD-RAMメディア115のリードインエリアに書き込む。この場合、専用の秘匿エリア書き込みコマンドがセキュアマネージャ112からDVD-RAMドライブ114に発行される。DVD-RAMドライブ114は、バスキー（B

50

K)でBK[MK_S[GI__CS]]を復号化し、MK_S[GI__CS]を、秘匿エリア書き込みコマンドで指定されたリードインエリア内の所定アドレス位置に書き込む。

【0045】

「再生」

図5はコンテンツ再生時の動作の流れを示している。

【0046】

(ステップ1): まず、セキュアマネージャ112とDVD-RAMドライブ114との間で認証処理が実行され、互いに正しいもの同士であるか否かが確認される。互いに正しいもの同士であることが確認されると、DVD-ROMのコンテンツ暗号化アルゴリズムとして使用されているCSS(Content Scrambling System)などのランダムチャレンジ・レスポンスを用いた方法により、セキュアマネージャ112とDVD-RAMドライブ114との間でキー交換が行われ、これにより同一の認証鍵、バスキー(BK: Bus Key)が共有される。バスキー(BK)は、毎回代わる時変キーである。

10

【0047】

(ステップ2): セキュアマネージャ112は、専用のコマンドを用いて、メディアIDとメディアマークの取得要求をDVD-RAMドライブ114に発行する。セキュアマネージャ112からの取得要求に回答して、DVD-RAMドライブ114は、メディアIDをBCAから読み出すと共に、リードインのエラー情報からメディアマークを生成し、それらメディアID(M__ID)およびメディアマーク(MM)を、バスキー(BK)で暗号化する。そして、暗号化されたメディアIDおよびメディアマーク(BK[M__ID.MM])をセキュアマネージャ112に送信する。セキュアマネージャ112は、バスキー(BK)を保持しているため、BK[M__ID.MM]からメディアID(M__ID)およびメディアマーク(MM)を解読することができる。そして、セキュアマネージャ112は、メディアID(M__ID)およびメディアマーク(MM)に対して予め決められた所定の演算を施すことにより、DVD-RAMメディア115固有のメディアキー(MK_S)を生成する。

20

【0048】

$MK_S = f(M_ID, MM)$

ここで、fは秘密の関数である。

【0049】

(ステップ3): 次に、セキュアマネージャ112から専用の秘匿エリア読み出しコマンドが発行される。これに回答して、DVD-RAMドライブ114は、秘匿エリア読み出しコマンドで指定されたリードインエリアの所定のアドレス位置からMK_S[GI__CS]を読み出し、それをバスキー(BK)で暗号化する。そして、BK[MK_S[GI__CS]]をセキュアマネージャ112に送信する。セキュアマネージャ112は、バスキー(BK)により、BK[MK_S[GI__CS]]からMK_S[GI__CS]を解読する。さらに、セキュアマネージャ112は、メディアキー(MK_S)により、MK_S[GI__CS]からGI__CSを解読する。

30

【0050】

(ステップ4): セキュアマネージャ112は、アプリケーションプログラム111などから指定された再生対象の暗号化されたコンテンツ(Kc[Content])と、それに対応するMK_S[Kc]、およびGIを、ファイルシステム113、さらにはATAPIDライバなどを介して、DVD-RAMメディア115から取得する。

40

【0051】

(ステップ5): セキュアマネージャ112は、GIからチェックサムを算出し、その算出したチェックサムと、DVD-RAMメディア115の秘匿エリアから取得したGI__CSとを比較する。不一致の場合には、DVD-RAMメディア115のGIが悪意を持つユーザによって書き替えられた恐れがあるため、再生処理はこの時点で中止する。一致した場合には、セキュアマネージャ112は、メディアIDとメディアマークから生成したメディアキー(MK_S)を用いて、MK_S[Kc]を復号し、コンテンツキー(Kc

50

)を得る。そして、そのKcを用いてKc[Content]の暗号を解除し、生のコンテンツ(Content)を再生ソフト(プレイヤー)に送信する。再生ソフトもタンパ・レジスタント・ソフトウェアとして実現されている。

【0052】

「コピー」

図6はコンテンツコピー時の動作の流れを示している。ここでは、DVD-RAMメディア115に記録されているコンテンツを記録メディア(A)116にコピーする場合を例示する。

【0053】

(ステップ1): まず、セキュアマネージャ112とDVD-RAMドライブ114との間で認証処理が実行され、互いに正しいもの同士であるか否かが確認される。互いに正しいもの同士であることが確認されると、DVD-ROMのコンテンツ暗号化アルゴリズムとして使用されているCSS(Content Scrambling System)などのランダムチャレンジ・レスポンスを用いた方法により、セキュアマネージャ112とDVD-RAMドライブ114との間でキー交換が行われ、これにより同一の認証鍵、バスキー(BK: Bus Key)が共有される。バスキー(BK)は、毎回代わる時変キーである。

【0054】

(ステップ2): セキュアマネージャ112は、専用のコマンドを用いて、メディアIDとメディアマークの取得要求をDVD-RAMドライブ114に発行する。セキュアマネージャ112からの取得要求に回答して、DVD-RAMドライブ114は、メディアIDをBCAから読み出すと共に、リードインのエラー情報からメディアマークを生成し、それらメディアID(M_ID)およびメディアマーク(MM)を、バスキー(BK)で暗号化する。そして、暗号化されたメディアIDおよびメディアマーク(BK[M_ID.MM])をセキュアマネージャ112に送信する。セキュアマネージャ112は、バスキー(BK)を保持しているため、BK[M_ID.MM]からメディアID(M_ID)およびメディアマーク(MM)を解読することができる。そして、セキュアマネージャ112は、メディアID(M_ID)およびメディアマーク(MM)に対して予め決められた所定の演算を施すことにより、DVD-RAMメディア115固有のメディアキー(MK_S)を生成する。

【0055】

$MK_S = f(M_ID, MM)$

ここで、fは秘密の関数である。

【0056】

(ステップ3): 次に、セキュアマネージャ112から専用の秘匿エリア読み出しコマンドが発行される。これに回答して、DVD-RAMドライブ114は、秘匿エリア読み出しコマンドで指定されたリードインエリアの所定のアドレス位置からMK_S[GI_CS]を読み出し、それをバスキー(BK)で暗号化する。そして、BK[MK_S[GI_CS]]をセキュアマネージャ112に送信する。セキュアマネージャ112は、バスキー(BK)により、BK[MK_S[GI_CS]]からMK_S[GI_CS]を解読する。さらに、セキュアマネージャ112は、メディアキー(MK_S)により、MK_S[GI_CS]からGI_CSを解読する。

【0057】

(ステップ4): セキュアマネージャ112は、アプリケーションプログラム111などから指定されたコピー対象の暗号化されたコンテンツ((Kc[Content]))と、それに対応するMK_S[Kc]、およびGIを、ファイルシステム113、さらにはATAPIドライバなどを介して、DVD-RAMメディア115から取得する。

【0058】

セキュアマネージャ112は、GIからチェックサムを算出し、その算出したチェックサムと、DVD-RAMメディア115の秘匿エリアから取得したGI_CSとを比較する。不一致の場合には、DVD-RAMメディア115のGIが悪意を持つユーザによって

10

20

30

40

50

書き替えられた恐れがあるため、コピー処理はこの時点で中止する。一致した場合には、DVD-RAMメディア115から読み取ったGIを参照して、コピー対象のコンテンツがコピー可能なコンテンツであるか否かを調べる。「コピー不可」または「コピー可能回数=零」の場合には、コピー処理はこの時点で中止する。コピーが許されたコンテンツであれば、セキュアマネージャ112は、次のステップ5以降の処理に進む。

【0059】

(ステップ5)：セキュアマネージャ112は、コピー先の記録メディア(A)116またはそれを制御するためのデバイスドライバとの間で認証処理を行う。互いに正しいコンテンツ保護機能をもつもの同士であることが確認されると、セキュアマネージャ112とコピー先の記録メディア(A)116またはそのデバイスドライバとの間でキー交換が行われ、同一の認証鍵(ここでは、 K_{x2} とする)が共有される。認証鍵(K_{x2})は毎回代わる時変キーである。

10

【0060】

(ステップ6)：セキュアマネージャ112からのメディアキー取得要求に応答して、記録メディア(A)116またはそのデバイスドライバは、メディアキー(MK_A)を認証鍵(K_{x2})で暗号化し、暗号化されたメディアキー($K_{x2}[MK_A]$)をセキュアマネージャ112に送信する。セキュアマネージャ112は、認証鍵(K_{x2})を保持しているので、 $K_{x2}[MK_A]$ から MK_A を解読することができる。

【0061】

(ステップ7)：セキュアマネージャ112は、DVD-RAMメディア115から読み出したGIを更新し、「コピー可能回数」が-1されたGIを得る。次いで、セキュアマネージャ112は、メディアIDとメディアマークから生成したメディアキー(MK_S)を用いて、 $MK_S[Kc]$ を復号し、コンテンツキー(Kc)を得、そしてそのコンテンツキー(Kc)をメディアキー MK_A を用いて暗号化し、 $MK_A[Kc]$ を得る。この後、セキュアマネージャ112は、 $Kc[Content]$ 、 $MK_A[Kc]$ 、GIを、ファイルシステム113さらには記録メディア(A)116のドライバなどを介して記録メディア(A)116に書き込む。

20

【0062】

(ステップ8)：セキュアマネージャ112は、GIからそのチェックサムデータ(GI_CS)を算出し、それを認証鍵(K_{x2})で暗号化したもの($K_{x2}[GI_CS]$)を記録メディア(A)116またはそのドライバに送信し、 GI_CS を記録メディア(A)116のGIチェックサム領域に書き込む。

30

【0063】

(ステップ9)：この後、セキュアマネージャ112は、チェックサムデータ(GI_CS)をDVD-RAMメディア115のメディアキー(MK_S)を用いて暗号化する($MK_S[GI_CS]$)。そして、さらに、 $MK_S[GI_CS]$ をバスキー(BK)で暗号化し($BK[MK_S[GI_CS]]$)、それをDVD-RAMドライブ114に送信してDVD-RAMメディア115のリードインエリアに書き込む。この場合、専用の秘匿エリア書き込みコマンドがセキュアマネージャ112からDVD-RAMドライブ114に発行される。DVD-RAMドライブ114は、バスキー(BK)で $BK[MK_S[GI_CS]]$ を復号化し、 $MK_S[GI_CS]$ を、秘匿エリア書き込みコマンドで指定されたリードインエリア内の所定アドレス位置に書き込む。

40

【0064】

(ステップ10)：そして、セキュアマネージャ112は、DVD-RAM115のGIをGIに更新する。

【0065】

「移動」

DVD-RAMメディア115に記録されているコンテンツを記録メディア(A)116に移動する場合は、図6のコピー処理と基本的に同じ手順で処理が行われるが、ステップ9の代わりにDVD-RAMメディア115の秘匿エリアの内容を削除する処理が行われ

50

、また図6のステップ10の代わりにDVD-RAMメディア115のKc[Content]、MK_S[Kc]、およびGIを削除する処理が行われる、点がコピー処理とは異なる。また、移動の場合は、コピー可能回数に対するGIの更新は行われず、移動可能回数が規定されている場合を除き、GIは更新されずに移動先の記録メディア(A)116に書き込まれることになる。

【0066】

以上のように、本実施形態においては、DVD-RAMメディア115のリードインエリアを秘匿エリアとして割り当て、そこにGIチェックサムデータをメディアキー(MK_S)によって暗号化して記録することにより、GIチェックサムデータの秘匿化を図ることができる。よって、GIの改竄などによるコンテンツの不正使用を防止することができる。また、メディアキー(MK_S)についても、メディアIDと、正当なドライブでしか読むことが出来ないメディアマークとによって生成しているので、その秘匿化を図ることができる。

10

【0067】

なお、本実施形態では、GIチェックサムデータを暗号化してリードインエリアに記録するようにしているが、GIのデータサイズが小さい場合には、GIそのものを暗号化してリードインエリアや、DVD-RAMメディア115上の代替セクタエリアに記録するようにしてもよい。

【0068】

また、コンテンツの暗号化鍵であるコンテンツキーをメディアキーを用いて暗号化するようにして、メディアキーをコンテンツキーとして使用し、コンテンツ自体をメディアキーを用いて暗号化するようにしてもよい。また、専用の秘匿エリアを持たない記憶メディアとしてDVD-RAMメディアを例示したが、本実施形態のコンテンツ保護方法は、例えば、MOやMDなど、専用の秘匿エリアを持たない他の各種記録メディア全てに対して適用することができる。

20

【0069】

さらに、本実施形態は、PCに限らず、セットトップボックス、ゲーム機、オーディオ/ビデオプレイヤーなど、マイクロプロセッサを搭載したあらゆるデータ処理装置(コンピュータ応用機器)に適用することができる。また、DVD-RAMドライブ114の認証機能、メディアマーク算出機能などは、DVD-RAMドライブ114用のドライバソフトウェアに持たせることも可能である。

30

【0070】

また、本実施形態で説明したセキュアマネージャ112はソフトウェアであるので、その手順を記述したコンピュータプログラムを記録媒体を通じてコンピュータまたはコンピュータ応用機器に導入することにより、本実施形態と同様の効果を容易に得ることができる。

【0071】

【発明の効果】

以上説明したように、本発明によれば、DVD-RAMメディアのように専用の秘匿エリアを持たないオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようになり、デジタルコンテンツの利用と保護の両立を図ることが可能となる。

40

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンピュータシステムの基本構成を示すブロック図。

【図2】同実施形態のコンピュータシステムで使用されるDVD-RAMメディアとそこに記録される情報の内容を説明するための図。

【図3】同実施形態のコンピュータシステムで使用されるDVD-RAMドライブの機能構成を示すブロック図。

【図4】同実施形態のコンピュータシステムで行われるコンテンツ記録処理の手順を示す図。

50

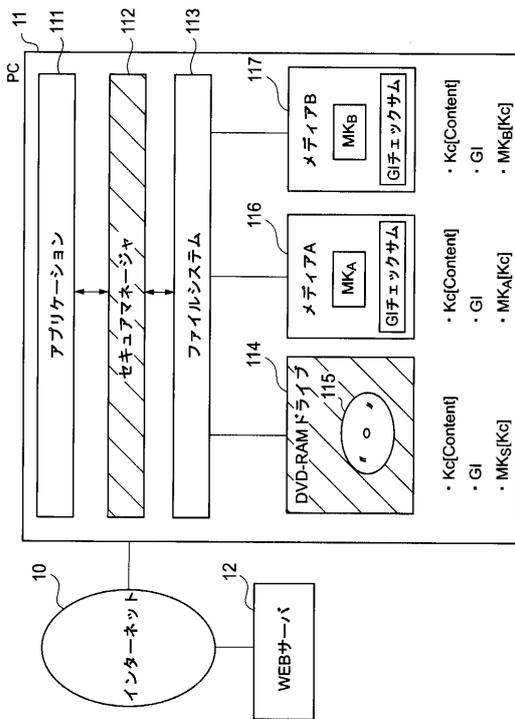
【図5】同実施形態のコンピュータシステムで行われるコンテンツ再生処理の手順を示す図。

【図6】同実施形態のコンピュータシステムで行われるコンテンツコピー処理の手順を示す図。

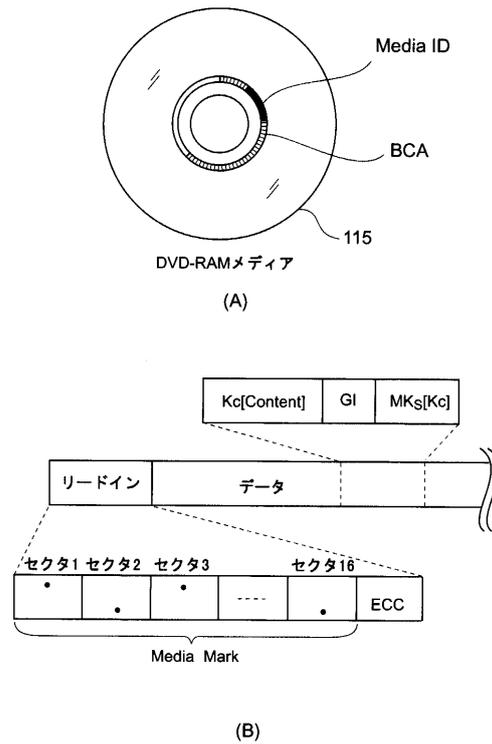
【符号の説明】

- 10 ... インターネット
- 11 ... パーソナルコンピュータ (P C)
- 12 ... W E Bサーバ
- 111 ... アプリケーションプログラム
- 112 ... セキュアマネージャ
- 113 ... ファイルシステム
- 114 ... DVD-RAMドライブ
- 115 ... DVD-RAMメディア
- 116 ... メディアA
- 117 ... メディアB
- 201 ... 認証部
- 202 ... メディアID読み出し部
- 203 ... メディアマーク算出部
- 204 ... E C C 演算回路

【図1】



【図2】



フロントページの続き

(72)発明者 石橋 泰博
東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

審査官 宮司 卓佳

(56)参考文献 特開平05-257816(JP,A)
国際公開第97/014147(WO,A1)
特開平10-079174(JP,A)
特開平11-328033(JP,A)
特開平09-055731(JP,A)
特開平09-055025(JP,A)
特開平05-075598(JP,A)
特開平09-097216(JP,A)
特開平08-212560(JP,A)

(58)調査した分野(Int.Cl., DB名)
G06F 21/24