(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-520036
(P2006-520036A)
(43)公表日　平成18年8月31日(2006.8.31)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	550B	5B017
G11B 20/10	(2006.01)	G11B	20/10	H	5D044
H04L 9/08	(2006.01)	G11B	20/10	301Z	5J104
		H04L	9/00	601C	
		H04L	9/00	601E	

審査請求 未請求　予備審査請求 未請求　（全 42 頁）

(21)出願番号　特願2006-502632 (P2006-502632)
(86)(22)出願日　平成16年2月4日 (2004.2.4)
(85)翻訳文提出日　平成17年8月11日 (2005.8.11)
(86)国際出願番号　PCT/IL2004/000120
(87)国際公開番号　WO2004/070707
(87)国際公開日　平成16年8月19日 (2004.8.19)
(31)優先権主張番号　154346
(32)優先日　平成15年2月6日 (2003.2.6)
(33)優先権主張国　イスラエル(IL)

(71)出願人　505294551
ヘキサロック　リミテッド
イスラエル　シェファイム　60990
ピー．オー．ボックス　32
(74)代理人　100082072
弁理士　清原　義博
(72)発明者　イヤール　コーヘン
イスラエル　キルヤット・ビアリック　2
7018　ワイズマン・ストリート　71

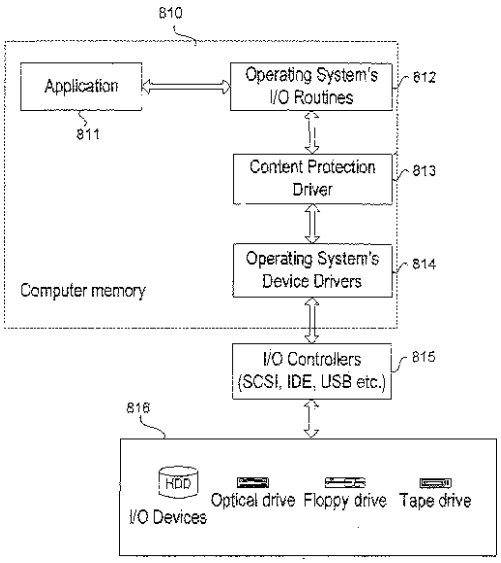
Fターム(参考)　5B017 AA06 AA07 BA04 BA07 BA09 CA09
5D044 BC04 CC04 DE17 DE50 GK11 GK17
5J104 AA12 AA13 EA23 EA26 PA14

最終頁に続く

(54)【発明の名称】光学メディア及び他のメディアに記録されたデジタル・コンテントに対する不正コピー及び不正な使用の防止方法及び防止システム

(57)【要約】
コンピュータ・システムによってコピー防止コンテントに対する不正コピーを防ぐ方法に関する。該方法は、コンピュータ・システムのオペレーティング・システム内にドライバをインストールする段階を備える。ドライバは、オペレーティング・システムのデバイス・ドライバにアクセスしようとするオペレーティング・システムのＩ／Ｏルーティンの試行を遮ることが可能である。またＣＲＣコードを作成する段階を備える。ＣＲＣコードは、デバイスから読み取られたデータに対して作成される。尚、このデータは、オリジナル・コピーを備える。更に、デバイスに書き込まれたデータに対してのＣＲＣコードが作成される。作成されたＣＲＣコードが、読み取られたデータに対して作成されたＣＲＣコードに一致するならば、そのようなデータの書き込み試行は妨げられる。

記録可能ＣＤに格納されたコンテントの保護は、上記コンピュータ・システムによってコピー防止コンテントに対する不正コピーを防ぐ方法により行われる。該方法は、コンピュータ・システムのオペレーティング・シス



【特許請求の範囲】
【請求項１】
コンピュータ・システムによってコピー防止コンテントに対する不正コピーを防ぐ方法であって、
（ａ）前記コンピュータ・システムのオペレーティング・システム内にドライバをインストールする段階を備え、
該ドライバが、オペレーティング・システムのデバイス・ドライバにアクセスしようとする前記オペレーティング・システムのＩ／Ｏルーティンの試行を遮ることが可能であり、
（ｂ）前記デバイス・ドライバからデータを読み取る試行が遮られるときに常に、
（ｂ－１）前記アクセスされたデバイスがオリジナル・コピーを備えるか否かを決定する認証テストを実行し、アクセスされたデバイスが不正コピーを有するならば、要求されたＩ／Ｏオペレーションを終了させる段階と、
（ｂ－２）アクセスされたデバイスがオリジナル・コピーを備えるならば、前記デバイスへのアクセスを可能とし、前記コンピュータ・システムのメモリ内において、前記デバイスから読み取られたデータのＣＲＣコードを処理し、格納する段階が、実行される段階と、
（ｃ）前記デバイス・ドライバへのデータの書き込みの試行が中断されると、
（ｃ－３）前記デバイスへ書き込まれるデータのＣＲＣコードを処理する段階と、
（ｃ－４）該処理されたＣＲＣコードが、前記コンピュータ・システムのメモリ内に事前に格納されたＣＲＣコードのうち１つに等しいならば、前記データの書き込みの試行を中断する段階と、
（ｃ－５）該処理されたＣＲＣコードが、前記コンピュータ・システムのメモリ内に事前に格納されたＣＲＣコードのいずれにも等しくない場合に前記データの書き込みの試行の実行を可能とする段階が、
実行される段階を備えることを特徴とする方法。
【請求項２】
前記Ｉ／Ｏデバイスに格納されるデータが、暗号化された形態で格納されることを特徴とする請求項１記載の方法。
【請求項３】
前記アクセスされたデバイスがオリジナル・コピーを備えると決定されるときに常に、
前記暗号化されたデータが解読される段階を備えることを特徴とする請求項２記載の方法。
【請求項４】
解読キーが、前記暗号化されたデータが読み取られる前記Ｉ／Ｏデバイスから得られることを特徴とする請求項３記載の方法。
【請求項５】
前記デバイス・ドライバからデータを読み取る試行が中断されるときに常に、論理的オン状態を示すフラグがセットされる段階であって、該フラグは通常、論理的オフ状態であるとともに、前記読み取りの試行を開始したプロセスに関連する段階と、
データを出力する試行を行うプロセスに関連するフラグの状態をチェックし、もし前記フラグが論理的オン状態であるならば、データの出力を妨げる段階を備えることを特徴とする請求項１記載の方法。
【請求項６】
記録可能ＣＤ上に格納されたコンテントを保護する方法であって、
（ａ）前記記録可能ＣＤからディスクＩＤとリード・イン　スタート・タイムの値を読み取る段階と、
（ｂ）　前記読み取られた値から暗号化キーを作成する段階と、
（ｃ）前記ＣＤ上に格納されるべきコンテントを、前記暗号化キーを用いて暗号化し、暗号化されたコンテントを前記記録可能ＣＤに書き込む段階と、

（ｄ）ＣＤのコンテントを読み取るための試行が行われると常に、
（ｄ－１）前記ＣＤからディスクＩＤとリード・イン　スタート・タイムの値を読み取る段階と、
（ｄ－２）前記読み取られた値から解読キーを作成する段階と、
（ｄ－３）前記解読キーを用いて、前記ＣＤのコンテントを解読する段階からなることを特徴とする方法。
【請求項７】
同一のキーが、前記保護されたコンテントの暗号化と解読の実行に用いられることを特徴とする請求項６記載の方法。
【請求項８】
記録可能なＣＤ上に格納されたコンテントを保護する方法であって、
（ａ）１若しくはそれ以上のトラックを備える第１セッションを前記ＣＤ上に記録する段階であって、前記トラックのそれぞれが、特徴的な及び／或いは非標準型のデータ構造を備える段階と、
（ｂ）隠蔽形式の保護されたコンテントと、特徴的な及び／或いは非標準型のデータ構造の存在・非存在を決定可能であるとともに前記隠蔽されたコンテントにアクセスし、該コンテントを明らかにすることが可能な認証モジュールを前記ＣＤ上に記録する段階と、
（ｃ）前記ＣＤへのアクセスの試行が行われると常に、前記認証モジュールを起動し、
前記特徴的な及び／或いは非標準型のデータ構造が前記ＣＤ上で発見されるならば、前記隠蔽されたコンテントが明らかにされ、アクセスされることを可能とする段階を備えることを特徴とする方法。
【請求項９】
前記特徴的な及び／或いは非標準型のデータ構造がロム・シンク・シフトを備えることを特徴とする請求項８記載の方法。
【請求項１０】
前記特徴的な及び／或いは非標準型のデータ構造がデジタル・サイレンスを備えることを特徴とする請求項８記載の方法。
【請求項１１】
前記特徴的な及び／或いは非標準型のデータ構造がリンク・ブロックを備えることを特徴とする請求項８記載の方法。
【請求項１２】
前記特徴的な及び／或いは非標準型のデータ構造が所定のロム・スキュー値を備えることを特徴とする請求項８記載の方法。
【請求項１３】
前記１若しくはそれ以上のトラック内の所定の場所に、特徴的なシリアル・ナンバを格納する段階を更に備え、前記特徴的なシリアル・ナンバが、
（ａ）１若しくはそれ以上の特徴的なコピー・シール・シリアル・ナンバであって、前記トラック内の所定のデータ・フレームのユーザ・データ内の所定の場所に格納されたコピー・シール・シリアル・ナンバと、
（ｂ）１若しくはそれ以上の特徴的なコピー認証シリアル・ナンバであって、前記トラックの所定のデータ・フレームのサブ・チャネル内の所定の場所に格納されるコピー認証シリアル・ナンバを備えることを特徴とする請求項８記載の方法。
【請求項１４】
前記コピー・シール・シリアル・ナンバ並びにコピー認証シリアル・ナンバが、著作権侵害コピーの複製に用いられた前記保護されたコンテントのオリジナル・コピーを識別するために用いられることを特徴とする請求項１３記載の方法。
【請求項１５】
前記コピー認証シリアル・ナンバのビットが、前記１若しくはそれ以上のトラック内の所定のデータ・フレームのシーケンスのＱサブ・チャネルのコピー許可／禁止ビット内に格納されることを特徴とする請求項１３記載の方法。

【請求項１６】
コンピュータ・システムによってコピー防止コンテントの不正コピーを防止する方法であって、
起動プロセスが、前記コンテントからデータを読み取ろうとするとき、論理的オン状態へのフラグをセットする段階を備え、
前記フラグは通常論理的オフ状態であるとともに前記プロセスに関連し、
データを出力しようとするプロセスに関連付けられたフラグの状態をチェックする段階と、
もし前記フラグが論理的オン状態であるならば前記データ出力を妨げる段階を備えることを特徴とする方法。
【請求項１７】
コピー防止記録可能ＣＤであって、該ＣＤは、
（ａ）１若しくはそれ以上のトラックを備える予め焼かれたセッションと、
（ｂ）ユーザ・データ・フィールド内及び／或いは前記トラック内の所定のフレームのサブ・チャネル内に特徴的な及び／或いは非標準型のデータ構造を備え、
前記データ構造の一部のみが従来型のレコーダによりコピー可能とされ、
（ｃ）更に、１若しくはそれ以上の追加のセッションを備え、
該セッションは、１つの暗号化キーにより暗号化されたコンテントを備え、
該暗号化キーは、前記データ構造から得られた値から作成され、
（ｄ）加えて、ソフトウェア・モジュールを備え、
該ソフトウェア・モジュールは、ＣＤの第１セッション内の前記データ構造の有無を識別可能であり、更に、前記ＣＤがオリジナルであるか、コピーであるかを決定可能であり、
ＣＤがオリジナルであるとの決定がなされると、前記ソフトウェア・モジュールが前記データ構造から得られた値から解読キーを作成し、前記追加のセッションの内容を解読することを特徴とするコピー防止記録可能ＣＤ。
【請求項１８】
１若しくはそれ以上のトラックが異なるサブコード・フォーマットで記録されることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。
【請求項１９】
前記特徴的な及び／或いは非標準型のデータ構造が、ロム・シンク・シフトを備えることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。
【請求項２０】
前記特徴的な及び／或いは非標準型のデータ構造がデジタル・サイレンスを備えることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。
【請求項２１】
前記特徴的な及び／或いは非標準型のデータ構造がリンク・ブロックを備えることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。
【請求項２２】
前記特徴的な及び／或いは非標準型のデータ構造が所定のロム・スキュー値を備えることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。
【請求項２３】
前記１若しくはそれ以上のトラック内の所定の場所に、特徴的なシリアル・ナンバを格納する段階を更に備え、前記特徴的なシリアル・ナンバが、
（ａ）１若しくはそれ以上の特徴的なコピー・シール・シリアル・ナンバであって、前記トラック内の所定のデータ・フレームのユーザ・データ内の所定の場所に格納されたコピー・シール・シリアル・ナンバと、
（ｂ）１若しくはそれ以上の特徴的なコピー認証シリアル・ナンバであって、前記トラックの所定のデータ・フレームのサブ・チャネル内の所定の場所に格納されるコピー認証シリアル・ナンバを備えることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。

【請求項２４】
前記コピー・シール・シリアル・ナンバ並びにコピー認証シリアル・ナンバが、著作権侵害コピーの複製に用いられた前記保護されたコンテントのオリジナル・コピーを識別するために用いられることを特徴とする請求項２３記載のコピー防止記録可能ＣＤ。
【請求項２５】
前記コピー認証シリアル・ナンバのビットが、前記１若しくはそれ以上のトラック内の所定のデータ・フレームのシーケンスのＱサブ・チャネルのコピー許可／禁止ビット内に格納されることを特徴とする請求項２３記載のコピー防止記録可能ＣＤ。
【請求項２６】
１若しくはそれ以上のトラックを備える予め焼かれたセッションを有し、
前記トラックは、前記１若しくはそれ以上のトラック内に所定の場所を備え、
（ａ）１若しくはそれ以上の特徴的なコピー・シール・シリアル・ナンバであって、前記トラック内の所定のデータ・フレームのユーザ・データ内の所定の場所に格納されたコピー・シール・シリアル・ナンバと、
（ｂ）１若しくはそれ以上の特徴的なコピー認証シリアル・ナンバであって、前記トラックの所定のデータ・フレームのサブ・チャネル内の所定の場所に格納されるコピー認証シリアル・ナンバを備えることを特徴とする請求項１７記載のコピー防止記録可能ＣＤ。
【請求項２７】
コピー防止記録メディアの製造方法であって、該製造方法は、
（ａ）連続的なアドレスを備える所定数の連続的なセクタの第１セットにデータを書き込む段階と、
（ｂ）前記第１セットに続いて、前記第１セットと同じ連続的なアドレスを備える前記所定数と同数の連続的なセクタの第２セットに異なるデータを書き込む段階とを備え、
前記メディアをコピーすることのいかなる試行も前記セットのうち１つのみのコピーしか出来ないことを特徴とする方法。
【請求項２８】
コピー防止記録メディアの製造方法であって、該方法は、
（ａ）開始場所としてセクタ・アドレスを指定し、認証データ・セクタを書き込む段階と、
（ｂ）前記開始場所に続いて、連続的なアドレスを備える所定数の連続セクタの第１セットにデータを書き込む段階と、
（ｃ）前記第１セットに続いて、前記第１セットと同じ連続的なアドレスを備える前記第１セットと同数の連続的なセクタの第２セットに異なるデータを書き込む段階と、
（ｄ）前記第２セットに続いて、終了場所としてのセクタを指定し、前記セクタのアドレスを前記第１セットに続く連続的なアドレスをセットする段階を備え、
前記メディアをコピーしようとする試行が、結果として、前記開始場所セクタ、前記セットのうち１つ及び終了場所セクタをコピーすることとなることを特徴とする方法。
【請求項２９】
（ａ）前記第１セットセクタのデータを読み取り、各読み取られたセクタに識別子を作成する段階と、
（ｂ）前記終了場所セクタを読み取る段階と、
（ｃ）前記終了場所セクタに先行するセクタを降り順で読み取り、各読み取られたセクタに識別子を作成し、前記第１セットに対応するセクタに対して前回作成された識別子と前記各読み取られたセクタに対して作成された識別子とを比較する段階と、
（ｄ）対応するセクタに対して作り出された識別子が不整合であると決定するならば前記記録メディアがオリジナルであることを指し示し、対応するセクタに対して作り出された識別子が整合すると決定するならば前記記録メディアがコピーであることを指し示す段階を行い、
記録メディアの認証を行う段階を備えることを特徴とする請求項２８記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタル・コンテントを認証し、デジタル・コンテントの不正コピー及び不正な使用からデジタル・コンテントを保護する分野に関する。
より詳しくは、本発明は、記録可能なメディアに保存されたデジタル・コンテントの不正コピー及びデジタル・コンテントの不正な使用を防止する方法及びシステムに関する。
【背景技術】
【０００２】
CD-ROMやDVD等の光学メディアは、ソフトウェアを保存する一般的な方法となってきている。なぜなら光学メディアは、高密度且つ信頼性の高い記憶機能を備え、更には、比較的低廉な価格で提供されるようになってきているためである。
従来、記録装置は高価であり、専門家にのみ入手可能であった。したがって、CD-ROMのような光学メディアのコピーによる著作権侵害があまり問題とされてこなかった。
近年、オリジナルを完璧にコピーすることができる記録装置の価格が低廉となってきており、このため、予め録画、録音されているCDsやDVDsの市場規模は減少している。
結果として、ソフトウェアの不正コピーや不正使用の割合は著しく増加し、コンテント・オーナーに深刻なダメージを与えている。
【０００３】
コンパクト・ディスク（CD）は、デジタル情報（コンテント）の光学記録メディアである。この光学的記録メディアは、オーディオ、ビデオ、テキスト、そして他のタイプのデジタル・コンテントの記録に幅広く有効利用されている。
コンパクト・ディスク（CD）の信頼性、効率性そして低廉な価格に起因して、音楽、映画、コンピュータ・ソフトウェア、データを記録するのにコンパクト・ディスク（CD）を使うことは一般的に行われるものとなっている。
しかし、コンパクト・ディスク（CD）に記録されたコンテントは、簡単にコピーされる可能性がある。実際に、コンピュータ・オペレーティング・システム（OS）の基本ツールを利用してコンパクト・ディスク（CD）内のデジタル情報にアクセスすることができる。
しかしながら、記録可能なCD（CD-R）の出現は、CDの不正コピー品に対する複製を一層容易にしている。
【０００４】
近年、不正コピー品の製作のレベルが上がるにつれて、いくつかの光学ディスクのコピー防止技術の水準は向上してきた。多くのコピー防止技術は、故意にディスクのプログラム・データを破壊すること或いはディスクの光学的な特性を変えることに基づいている。
このディスクのプログラム・データの破壊は、専用のマスタリング装置によりなされている。このマスタリング装置は、光学ディスクの複製設備に適用されている。
標準的な光学ディスクレコーダーは、不正コピーを行ったとしても、光学ディスクデータを破壊するよう設計されていないため、オリジナルのコピー防止機能付きディスク内のデータを正確にコピーすることができない。
光学ディスクに付加されるソフトウェア・モジュールは、破壊されるであろうディスクの領域を読み、ディスクがオリジナルであるかコピーであるかを判断し、それに応じてディスクのコンテントにアクセスすることを可能としたり、アクセスを拒否したりする。
【０００５】
既存のコピー防止技術は、コンピュータゲーム等のアプリケーションのコピーを防止するのに適している。アプリケーションは、1つの破壊されたマスターデータを用いて何度も複製されている。この破壊されたマスターデータは、複製設備によって生産されている。
故意に光学ディスク内のデータを破壊することに基づくコピー防止技術の欠点は、このコピー防止技術が記録可能なディスクに容易に適用できないことである。それは、標準の光学ディスクレコーダーが、破壊された記録可能なディスク上に情報を記録するよう設計

されていないからである。
【０００６】
記録可能な光学ディスクにおけるコピー防止に対する解決方法は、コンピュータゲームやソフトウェアの販売前の製品（Alphas、Betas等）にとって大変重要である。
コンテント・オーナーは、数量を限定して、コンテントの販売前製品を公表し、ソフトウェアのフィールドテストを行っている。このソフトウェアのフィールドテストは、製品の最終版を発売する前に、バグの存在を調査するのに重要である。
製品の最終版が市場に発売される以前に、著作権保護されるべきデジタル・コンテントを備える販売前製品が、不正にコピーされ、またインターネットを介して流通されてしまうことがある。その様な初期段階におけるソフトウェアの著作権侵害は、販売に大きな損失を生じさせる。なぜなら、最も重要な最初の売り上げのピークに損害を与えるためである。販売前に配布される製品の数は、かなり限定されている。通常、販売前に配布される数は、ほんのわずかから数百枚までである。これは多くの場合、コンテント・オーナー自身が記録可能なディスク上に複製し、これを公表しているからである。
【０００７】
少量のソフトウェアの最終版を発売するにあたって、認可されていない不正コピーに対して、光学的記録可能なディスクのコンテントを保護する機能は、非常に重要である。例えば、専門的なソフトウェアは限定された専門的な市場において高値で売られている。特に、光学的記録可能なディスクのコピー防止機能は、顧客自身が、購入したいコンテントの選択をし、顧客の全ての選択を含有するディスクがすぐに編集され、記録されるというオン・デマンド環境によく利用されている。
【０００８】
認可されていない不正コピーに対して、光学的記録可能なディスクのコンテントを保護する機能は、政府機関、軍事の極秘情報、そして銀行の財務情報をも保護するのに非常に重要でもある。
【０００９】
加えて、不正コピーに対する光学的記録可能なディスクのコピー防止機能は、個人の顧客が自分自身でコピー防止機能付きコンテントを一度に一回或いは必要に応じて光学ディスク上に記録することが可能としている。このような行為は、一般的なマスタリング施設で今日行われているような大量生産プロセスを必要としないものである。
【００１０】
認可されていない不正コピーに対して、光学的記録可能なディスクのコンテントを保護する機能は、ある特徴を有していて良い。そのある特徴とは、コピー防止解決方法を強化するものであって良く或いは複製されたディスクに簡単に適用されないものであってもよい。
例えば、特別なシリアル・ナンバや特別な追跡情報を付加することにより、それぞれのディスクを特徴付ける機能である。その機能により、不正コピーが行われた、オリジナルディスクのオリジナルオーナーを追跡することができるものである。これらの特徴は、後で詳述される。
【発明の開示】
【発明が解決しようとする課題】
【００１１】
CDやDVDのような光学記録メディアのコンテントを保護するための全ての従来技術による解決策は、未だ記録可能な光学ディスクをコピー行為から保護するものではない。
そのため、記録可能なディスクのコンテントを保護する方法は、以下の手段を有することが強く望まれている。その手段とは、個人によって作り出されたコンテント及び／又は数量限定のコピー品で利用可能されたものであって、大量生産可能なマスタリングプロセスを必要とせずに得られたコピー品のコンテントを保護する手段である。
【課題を解決するための手段】
【００１２】

ここでＣＤ－Ｒ及びＣＤ－ＲＷとの用語は「ＣＤ」と称され、エンド・ユーザによりデジタル・コンテントが「ＣＤ」上に書き込まれる。また「ディスク」との用語は、ＣＤ－Ｒ並びにＣＤ－ＲＷを示す。

【００１３】

「Cyclic Redundancy Check（周期的冗長検査）：ＣＲＣ」との用語は、データに対する特徴的な信号を作成する方法を意味する。この方法は、送信されたデータ内のエラーを検出するのにしばしば用いられる。

【００１４】

本発明は、コンピュータ・システムによって、コピー防止コンテントに対する不正コピーを防止する方法並びにシステムに関する。本発明は、コンピュータ・システムのオペレーション・システム内にソフトウェア・ドライバをインストールする段階を備える。ソフトウェア・モジュールは、オペレーション・システムのＩ／Ｏルーティンがオペレーション・システムのデバイス・ドライバにアクセスする試行を妨げる機能を備える。デバイス・ドライバからデータを読み取る試行が中断されると、以下の段階が実行される。

・認証テストが実行され、アクセスされたデバイスがオリジナル・コピーを備えるか否かが決定される。もし、アクセスされたデバイスが不正コピーを備えるならば、要求されたＩ／Ｏオペレーションは終了される。

・もし、アクセスされたデバイスがオリジナル・コピーを備えるならば、デバイスへのアクセスが可能となり、デバイスから読み取られたデータのＣＲＣコードは、コンピュータ・システムのメモリ内で計算処理され、該メモリ内に格納される。

【００１５】

デバイス・ドライバにデータを書き込む試行が中断されると、以下の段階が実行される。

・データのＣＲＣコードが計算処理され、デバイスへ書き込まれる。

・もし処理されたＣＲＣコードが、コンピュータ・システムのメモリ内に事前に格納されたＣＲＣコードのうち１つと等しい場合には、データを書き込む試行が終了される。

・もし処理されたＣＲＣコードが、コンピュータ・システムのメモリ内に事前に格納されたＣＲＣコードのいずれとも等しくない場合には、データを書き込む試行が実行されることが可能となる。

【００１６】

Ｉ／Ｏデバイスに格納されたデータは、暗号化されていてもよい。本発明は、それゆえ、暗号化されたデータを解読する段階を備えていてもよい。アクセスされたデバイスがオリジナル・コピーを備えるならば、データを解読する段階が実行される。所望するならば、解読キーが、暗号化データが読み取られるＩ／Ｏデバイスから得られるものであってもよい。

【００１７】

本発明は、記録可能ＣＤに格納されたコンテントを保護する方法並びにシステムに関する。記録可能ＣＤのディスクＩＤ並びにリード・イン　スタート・タイムの値が暗号化キーに用いられる。該暗号化キーは、使用されるＣＤ内に格納されたコンテントを暗号化するために用いられる。暗号化されたコンテントは記録可能ＣＤに書き込まれる。ＣＤのコンテントを読み取る試行が行われるときには、以下の段階が実行される。

・ディスクＩＤ並びにリード・イン　スタート・タイムの値がＣＤから読み取られる。
・解読キーが読み取られた値から作成される。
・ＣＤのコンテントが作成された解読キーで解読される。

所望ならば、同じキーを用いて暗号化並びに保護されたコンテントの解読がなされてもよい。

【００１８】

コンピュータ・システムによるコピー防止コンテントの不正コピーは、論理的オン状態を示すフラグをセットすることにより防止される。該フラグは、起動プロセスがコンテントからデータを読み取ろうとしたときに論理的オン状態となる。尚、当該フラグは、通常論理的ＯＦＦ状態とされる。また、当該フラグは、起動プロセスに関連するものとされ、データを出力しようとするプロセスに関連するフラグの状態をチェックする。そして、もし当該フラグが論理的オン状態であるならば、データ出力が妨げられる。

【００１９】

本発明は、記録可能ＣＤに格納されたコンテントを保護する方法並びにシステムに関する。該記録可能ＣＤは、予め焼かれた第１セッションを備える。該第１セッションは、１若しくはそれ以上のトラックを備える。各トラックは、特徴的な及び／又は非標準的なデータ構造を備える。保護されたコンテントは、隠蔽形態で認証モジュールとともにＣＤに記録される。該認証モジュールは、特徴的な及び／又は非標準的なデータ構造の有無を決定可能である。また、該認証モジュールは、隠蔽されたコンテントにアクセスし、該コンテントを明らかにする能力を備える。もし、特徴的な及び／又は非標準的なデータ構造がＣＤ内で見つけられたら、隠蔽されたコンテントへのアクセスが可能となる。

【００２０】

特徴的な及び／又は非標準的なデータ構造は、Rom Sync Shifts（ロム・シンク・シフト）、Digital Silence（デジタル・サイレンス）、Link Blocks（リンク・ブロック）及び／又はPredetermined Rom Skew values（所定のロム・スキュー値）であってもよい。記録可能ＣＤは更に特徴的なシリアル・ナンバを備えるものであってもよい。該シリアル・ナンバは、１若しくはそれ以上のトラック内の所定場所に格納される。

該特徴的なシリアル・ナンバは、１若しくはそれ以上の特徴的なコピー・シール・シリアル・ナンバを備えるものであってもよい。このコピー・シール・シリアル・ナンバは、トラック内の所定のフレームのユーザ・データ内の所定場所に格納される。更に、特徴的なシリアル・ナンバは、１若しくはそれ以上の特徴なコピー認証シリアル・ナンバを備える。該コピー認証シリアル・ナンバは、トラック内の所定のデータ・フレームのサブ・チャネル内の所定場所に格納される。

【００２１】

コピー・シール・シリアル・ナンバ並びにコピー認証シリアル・ナンバは、著作権違反のコピー品を複製するために用いられた保護されたコンテントのオリジナル・コピーを識別するために用いられてもよい。本発明の好適な実施形態において、コピー・シール・シリアル・ナンバ並びにコピー認証シリアル・ナンバは記録可能なＣＤそれぞれに対して用いられる。コピー認証シリアル・ナンバのビットは、１若しくはそれ以上のトラック内の所定のデータ・フレームのシーケンスのＱサブ・チャネルのコピー許可／禁止ビット（Copy Permit/Prohibit Bit）に格納される。

【００２２】

本発明の他の好適な実施形態にしたがって、以下の手順によって、コピー防止記録メディアは製造される。

連続的なアドレスを備える所定数の連続的なセクタの第１セットにデータを書き込む。そして、該第１セットに続いて、第１セットのセクタと同数の連続的なセクタの第２セットに異なるデータを書き込む。尚、第２セットのセクタは、第１セットのセクタと同じ連続的なアドレスを備える。このようにして、メディアをコピーする試行により、セットのうち１つのみをコピーすることが可能となる。

【００２３】

所望ならば、コピー防止記録メディアは、以下の手順により製造される。開始場所としてセクタ・アドレスを指定し、認証データ・セクタを該セクタ・アドレスに書き込む。そして、開始場所に続いて、所定数の連続的なセクタの第１セットにデータを書き込む。第

１セットと同数の連続的なセクタの第２セットに異なるデータを書き込む。第２セットのセクタは、第１セットと同じ連続的なアドレスを備える。そして、第２セットに続いて、終了場所として１つのセクタを指定する。そして、第１セットに続く連続的なアドレスにセクタのアドレスをセットする。このようにして、メディアをコピーしようとする試行により、結果として、開始場所のセクタ、セットのうちの１つ並びに終了場所のセクタのコピーを行うこととなる。

【００２４】

コピー防止記録メディアの認証は以下の手順で行われる。

まず、セクタのうち第１セットのデータが読み取られ、各読み取られたセクタに対して識別子が作られる。そして、終了場所セクタが読み取られ、終了場所セクタに先行するセクタを降り順で読み取る。そして各読み取られたセクタに対して識別子を作成する。この識別子と、第１セット内の対応するセクタに対して事前に作成された識別子とを比較する。そして、対応するセクタに対して作成された識別子同士が一致しない場合、記録メディアがオリジナルであることを指し示す。また、識別子同士が一致する場合には、記録メディアがコピーであることを指し示す。

【００２５】

本発明は、コピー防止記録可能ＣＤに関する。コピー防止ＣＤは、以下の構成を備える。

（ａ）コピー防止記録可能ＣＤは、予め焼かれたセッションを備え、該セッションは、１若しくはそれ以上のトラックを備える。

（ｂ）コピー防止記録可能ＣＤは、特徴的な及び／又は非標準型のデータ構造を備える。該データ構造は、トラック内の所定のフレームのユーザ・データ・フィールド及び／又はサブ・チャネルに配される。データ構造の一部のみが、従来型のレコーダによりコピー可能である。

（ｃ）更にコピー防止記録可能ＣＤは、１若しくはそれ以上の追加のセッションを備える。追加のセッションには暗号化されたコンテントが配される。この暗号化は暗号化キーにより行われ、暗号化キーは、データ構造から得られた値から作成される。

（ｄ）コピー防止記録可能ＣＤは、ソフトウェア・モジュールを備える。ソフトウェア・モジュールは、ＣＤの第１セッション内のデータ構造の有無を識別可能であり、またＣＤがオリジナルであるかコピーであるかを決定可能である。ＣＤがオリジナルであるとの決定がなされると、ソフトウェア・モジュールはデータ構造から得られた値から解読キーを作成し、追加のセッションのコンテントを解読する。

【００２６】

本発明の好適な実施形態によれば、１若しくはそれ以上のトラックは、異なるサブコード・フォーマットで記録される。所望ならば、特徴的な及び／又は非標準型のデータ構造は、Rom Sync Shifts（ロム・シンク・シフト）、Digital Silence（デジタル・サイレンス）、Link Blocks（リンク・ブロック）及び／又はPredetermined Rom Skew values（所定のロム・スキュー値）であってもよい。コピー防止ＣＤは、１若しくはそれ以上のトラック内の所定場所に格納された特徴的なシリアル・ナンバを更に備えてもよい。該シリアル・ナンバは以下のものを備える。

・シリアル・ナンバは、１若しくはそれ以上の特徴的なコピー・シール・シリアル・ナンバを備える。該コピー・シール・シリアル・ナンバはトラック内の所定のデータ・フレームのユーザ・データ内の所定場所に格納される。

・シリアル・ナンバは、１若しくはそれ以上の特徴的なコピー認証シリアル・ナンバを備える。該特徴的なコピー認証シリアル・ナンバは、トラック内の所定のデータ・フレームのサブ・チャネル内の所定の場所に格納される。

【００２７】

本発明の他の好適な実施形態によれば、コピー・シール・シリアル・ナンバ並びにコピー認証シリアル・ナンバは、著作権違反の複製品のコピーに用いられた保護されたコンテ

ントのオリジナル・コピーを識別するために用いられる。
本発明の他の好適な実施形態によれば、コピー・シール・シリアル・ナンバ並びにコピー認証シリアル・ナンバは、記録可能ＣＤそれぞれに対して用いられる。コピー認証シリアル・ナンバのビットは、１若しくはそれ以上のトラック内の所定のデータ・フレームのシーケンスのＱサブ・チャネルのコピー許可／禁止ビット（Copy Permit/Prohibit Bit）に格納される。
【００２８】
本発明の他の好適な実施形態によれば、コピー防止記録可能ＣＤは、予め焼かれたセッションを備える。該セッションは、１若しくはそれ以上のトラックを備え、該トラックは所定場所を備える。該所定場所は、１若しくはそれ以上の特徴的なコピー・シール・シリアル・ナンバを備える。この特徴的なコピー・シール・シリアル・ナンバは、トラック内の所定のデータ・フレームのユーザ・データ内の所定場所に格納される。更に、所定場所は、１若しくはそれ以上の特徴的なコピー認証シリアル・ナンバを備える。このコピー認証シリアル・ナンバは、トラック内の所定のデータ・フレームのサブ・チャネル内の所定場所に格納される。
【発明の効果】
【００２９】
本発明の目的は、認可されていない不正コピーに対して、標準の記録可能なディスクに記録されるデジタル・コンテントを保護する方法とシステムを提供することである。
【００３０】
本発明における他の目的は、認可されていない不正コピーからデジタル・コンテントを保護する方法及びシステムを提供することである。
そのデジタル・コンテントを保護する方法及びシステムは、故意に組み込まれた論理記号やシリアル・ナンバを備えるとともに予め焼き付けられた情報を含む記録可能なディスクを使用する。デジタル・コンテントを保護する方法及びシステムは、ディスク及びディスク内に格納されたデジタル・コンテント保護機能付コピー品が真正のものであるか否かを判断するのに用いられる。
【００３１】
本発明の目的は、保護されたデジタル・コンテントに行われた不正コピーの元となった記録メディアの所有者を追跡することである。その方法は、オリジナルとコピーの両方に記録される特別なシリアル・ナンバに基づいて行われる。
【００３２】
本発明の他の目的は、ソフトウェア・ドライバを提供することである。
ソフトウェア・ドライバは、コンピュータのオペレーティング・システムにデジタル・コンテントを簡単に読む機能を提供するものである。デジタル・コンテントは、メディアが正当なオリジナルである限り、任意のメディアに暗号化されて記録されている。
ドライバは、暗号化されたコンテントをコピーすることの試みを防止するよう設計されている。本発明の他の目的や利点は、後述の説明で明らかになる。
【発明を実施するための最良の形態】
【００３３】
ソフトウェアのコピー防止は通常、ソフトウェアに認証手順を設けることにより実施される。この認証手順により、ソフトウェアが記憶されるメディアがオリジナルか否かを確認される。コピー防止ソフトウェアは、用いられている記憶メディアがオリジナルであることが確認されたときには実行されるが、そうでないときは実行が終了される。
【００３４】
ソフトウェア以外のデジタル・コンテント（例えばテキスト、音楽）は、このような技術を用いてもコピーを防止できない。このようなコンテントにアクセスしても、記憶メディアからのプロセスが開始されることがないからである。よって、記憶メディアがオリジナルである場合もそうでない場合も、同様にアクセスされる。本発明は、ソフトウェア・ドライバ（以下、コンテント保護ドライバともいう）のためのアーキテクチャを提供する

。このアーキテクチャはオペレーティング・システムにインストールされて、メディアがオリジナルである場合に限り、暗号化されたコンテントをメディアから読み取るのをサポートする。コンテントを解読するプロセスは、エンド・ユーザに何ら負担をかけるものではない。メディアはいかなる種類のコンテントを含んでもよい。コンテントとしては例えば、ＭＰＥＧビデオ・ファイル或いはＭＰ３オーディオ・ファイルが挙げられる。このコンテントは通常の方法（例えば、ユーザのコンピュータにインストール可能な任意のプレーヤでビデオ・ファイル及びオーディオ・ファイルを再生するなど）で利用できる。しかしながら、コンテントのコピーを作成する試行は全て、コンテント保護ドライバによってブロックされる。

【００３５】

コンテントは、好ましくは暗号化された状態でコピー防止メディアに記憶される。記憶されたコンテントのコピー防止機能は、コンテント保護ドライバにより実行される。コンテント保護ドライバは、ユーザのコンピュータから起動されるオペレーションの読み取り及び／又は書き込みを全て妨げる。暗号化されたコンテントが記憶されている記憶メディアがアクセスされると、コンテント保護ドライバは１つ若しくはそれ以上の認証手段を用いてメディアがオリジナルであることを認証する。認証手段については以下で詳述する。記憶メディアがオリジナルであれば、コンテント保護ドライバは、メディアから情報を読み取るとともに解読する。その後、コンテント保護ドライバは、読み取りオペレーションの巡回冗長検査（Cyclic Redundancy Check(CRC)）コードを計算する。コンテント保護ドライバは、コンピュータのメモリに、最近実行された幾つかの読み取り操作について計算されたＣＲＣコードを記憶させる。コンテント保護ドライバが書き込み操作を中断すると、該コンテント保護ドライバは書き込まれるべき情報のＣＲＣコードを計算する。書き込まれるべき情報について計算されたＣＲＣコードが、コンピュータ・メモリに記憶された最近の読み取り操作のＣＲＣコードのうちの１つと一致すると、コンテント保護ドライバは書き込み操作をブロックするか、或いは、模造コンテント（例えば、ランダム・データ）を書き込む。

【００３６】

この独自の方法により、既存のコンテントのコピー防止手段或いは暗号化手段の多くが有する問題が解決される。これら既存の手段においては、暗号化されたコンテントを解読するためのシステムを完全に透過性のシステムにすること、及び全てのプログラムで該システムを利用可能とすることが不可能である。暗号化されたコンテントの記憶によるコンテント保護手段の多くにおいては、ユーザが暗号化されたコンテントへのアクセスするためには、コードを入力するか、或いは解読キーを備える外部装置を使用することが必要である。完全な透過性システムの主な問題点は、ＯＳリソースにアクセス可能なアクティブ・プロセスであればどのようなプロセスでも暗号化されたコンテントにアクセスできることが挙げられる。つまり、全てのコピー・ソフトウェアが、同様の動作即ちコピー防止コンテントの読み取り及びコピーを行うことが可能である。例えば、完全な透過性システムによれば、MS-Windows（登録商標）（エムエス・ウィンドウズ（登録商標））のオペレーティング・システムのwindows（登録商標） explorer（ウィンドウズ（登録商標）・エクスプローラ）が、暗号化されたコンテントを読み取り、その後異なるメディアに該コンテントを書き込むことが可能である。

【００３７】

コピー防止システムは通常、使用されている記憶メディアがオリジナルか否かを決定する認証プロセスを備える。この認証プロセスの結果に基づいて、保護されたコンテントへのアクセスが許可されるか、或いは拒絶されるかが決定される。本発明は、メディアがオリジナルか否かを決定するための２つの異なる方法を提供する。以下では、この方法を、特に光記録ディスクに用いた場合について説明する。

【００３８】

第１の方法の認証プロセスは、標準的な記録ディスクについて行われる。このプロセスでは、全ての記録ディスクに存在する固有の識別記号を用いる。

【００３９】
第２の方法の認証プロセスは、同一のコンテントを異なる記録装置或いは異なる記録方法を用いて記録した２つの異なるディスクが本質的に何らかの小さな相違点を備えるという事実に基づいている。本発明の認証方法は、このような相違点を利用して、用いられているディスクが、オリジナルであるのか、或いは異なる記録装置を用いて作成されたか若しくは異なる記録方法を用いて作成されたコピーであるのかを決定する。
【００４０】
第２の方法の認証プロセスは、予め焼かれた領域を有する標準的な記録ディスクについて行われる。予め焼かれた領域には、意図的に埋め込まれた論理記号及び固有のシリアル・ナンバが記録されている。該認証プロセスは、予め焼かれた領域から情報を読み取って、該情報を用いてディスクがオリジナルか否かを決定するように設計されている。以下で説明するように、ディスクに記録された情報が同じであっても、ディスクに埋め込まれたシリアル・ナンバは全てのディスクそれぞれに固有である。不正コピーが発見された場合には、シリアル・ナンバを用いて、コピーの元となったオリジナルのディスクの所有者を特定可能である。
【００４１】
当業者であれば理解できることであるが、本発明の認証手段は、ほぼ全てのソフトウェアの処理に組み込むことができる。認証プロセスはソフトウェアの動作中に実行される。該認証プロセスは、記憶されているメディアがオリジナルのメディアか否かを決定する。この動作は、その結果によって継続されるか或いは終了される。加えて、これらの認証手段は、暗号化手段を用いて、本発明のコンテント保護ドライバの認証手順に組み込まれることが可能である。これにより、ソフトウェア以外にも全ての種類のデジタル・コンテントに適したコピー防止機構が提供される。
【００４２】
通常の記録済みのＣＤメディアは、連続したＣＤフレームからなる。図１は概略図であり、ＣＤフレーム（１００）の構造を表す。各ＣＤフレーム（１００）は、２３５２バイトのメイン・チャネル（１１０）及び９８バイトのサブ・チャネル・データ（１２０）を備える。ＣＤフレームは、オーディオ再生時間（分（Minutes）、秒（Seconds）、フレーム（Frames）（ＭＳＦ））についてアドレス指定されている。従来通り１分は６０秒とされる。
【００４３】
メイン・チャネル・ブロック（１１０）の構造は、ＣＤに記録されている情報の種類によって決定される。オーディオ・コンテント、コンピュータ・データ・コンテント及びビデオ・コンテントは、異なるメイン・ブロック・チャネル構造を有する。図１に示すメイン・チャネル・ブロック（１１０）は、フィリップスのYellow Book（イエローブック）標準で定められているように、モード１データ・ブロックである。モード１データ・ブロックは、コンピュータ・データに用いられる。同期フィールド（１１１）は、同期パターンを維持する１２バイトを備える。ヘッダ・フィールド（１１２）は、ＭＳＦフォーマットにしたがった現在のＣＤフレームのアドレスを表す３バイトの数値データ（絶対時間：absolute time、ＡＴＩＭＥ））を備える。ヘッダ・フィールド（１１２）はまた、メイン・チャネル・ブロック・モード（ここではモード１）を表す１バイトの数値データを備える。ＥＤＣフィールド（１１４）は、４バイトのＣＩＲＣ（Cross-Interleaved Reed-Solomon Code）符号語であり、エラー検知に用いられる。この符号語は、同期フィールド（１１１）、ヘッダー・フィールド（１１２）及びユーザ・データ・フィールド（１１３）に記憶されている情報を用いて計算される。フィールド（１１５）は８バイトで、予約済みとされるとともに、ゼロとして設定される。ＥＣＣ（error correctＩ／Ｏn of corrupted informatＩ／Ｏn）フィールド（１１６）は２７６バイトで、同期フィールド（１１１）、ヘッダー・フィールド（１１２）及びユーザ・データ・フィールド（１１３）内の破壊された情報（corrupted informatＩ／Ｏn）のエラーを訂正する。これらのフィールド（１１１、１１２、１１４、１１５、１１６）はコントロール・フィールドとしても

知られる。これらのフィールドは、２８８バイトを消費する。結果として、ユーザ・データ・フィールド（１１３）内のユーザ・データのためには、２０４８バイトが残される。

【００４４】

ディスクのメイン・チャネルの同期パターン（同期フィールド（１１１））は通常、２３５２バイトごと（各ＣＤフレームの最初）に現れる。しかしながら、２つの連続する同期パターン間の距離が、２３５２バイトより短いか、或いは長いことがある。この現象は、ロム・シンク・シフトとして知られている。ロム・シンク・シフトは通常ＣＤ－ＲＯＭマスターの製造工程でのエラーによって起こる。記録装置は通常、ロム・シンク・シフトを生むようには設計されていない。本発明によると、意図的に埋め込まれたロム・シンク・シフトがコピーを防止された記録ディスクの認証に用いられる。これについては以下で説明する。

【００４５】

サブ・チャネル・フィールド（１２０）は、２バイトの同期バイト及び９６バイトのサブ・チャネル情報を備える。各サブ・チャネル・情報バイト（１２１）は、８ビットのサブ・チャネル・ビットに分けられる。図１に示す如く、サブ・チャネル・ビットは、ビット位置にしたがってＰからＷまでの文字を用いて標識される。各サブ・チャネルは、ＣＤフレーム（９６ビット）ごとに１２バイトを占める。Ｐ及びＱサブ・チャネルは、記録方法に関する情報を提供する。ＲからＷまでのサブ・チャネルは、オーディオ・ＣＤフレームについてのみ定義される。

【００４６】

フレームのメイン・チャネル（１１０）内の全ての情報（同期フィールド（１１１）を除く）は、スクランブルをかけられる。このスクランブルは、予め定義された値を備えるメイン・チャネル（１１０）の情報のＸＯＲ（排他的論理和)をとることにより行われる。読み取りアプリケーションに情報を送る前に、情報がディスクから読み取られるのと同時に、読取装置が自動的に情報のスクランブルは解除される。スクランブル後の１つ若しくはそれ以上の、ゼロを含むＣＤフレームの列は、「デジタル・サイレンス」と呼ばれる。標準的なディスクは通常、デジタル・サイレンスを含まない。以下で説明するように、本発明の方法によると、これらの「デジタル・サイレンス」フレームを用いて、コピーを防止された記録ディスクの認証を行うことができる。

【００４７】

ディスク上の情報は、セッションと呼ばれる論理構造に記録される。セッションは、３つの論理的エンティティに分けられる。エンティティは、ディスクの内周部から始まって外周部に向かって連続的に配されている。図２は、概略図であり、ＣＤセッション（２０００）の構造を示す。リード・イン（フィールド（２１００））は、ディスクの中心付近の記録のない領域からの読み取りを防ぐための保護用ゾーンである。該フィールドは、ドライブに、記録済みの領域の開始場所についての信号を送る。リード・イン・フィールド（２１００）はまた、プログラム領域（２２００）の目次情報（Table of Contents、ＴＯＣ）を備える。プログラム領域（フィールド（２２００））は、ディスクのユーザ領域ともいう。例えば、オーディオＣＤにおいては、該領域は音楽が記録されている場所である。リードアウトフィールド（２３００）は、記録のない領域からディスクの外縁部への読み取りを防止するための保護ゾーンである。該フィールドは、ドライブに、記録済みの領域の終了場所についての信号を送る。

【００４８】

プログラム領域（２２００）は、論理的に独立した領域（トラック（２２１０）という）に分けられている。プログラム領域（２２００）には、少なくとも１つのトラック（２２１０）がなければならない。トラック（２２１０）のそれぞれは、２つのポーズ領域を備える。すなわち、プレギャップ・フィールド（２２１１）及びポストギャップ・フィールド（２２１３）である。上記のポーズ領域の１つの領域の長さは、１５０ＣＤフレームである。Ｐサブ・チャネルは、ギャップを識別するために予約済みとされる。プログラム領域のＰサブ・チャネルの値は０であり、ギャップ領域（２２１１）及び（２２１３）の

値は１に設定されている。プログラム領域内のデータ・フレームであるフィールド（２２１２）は、ユーザ・コンテント（例えばコンピュータ・ファイル）を記憶する。

【００４９】

標準的な記録装置を用いて、標準的な記録ディスクへ書き込みを行う際には、各トラックのプレギャップ領域（２２１１）が値ゼロを有するＣＤフレーム（ユーザ・データ（１１３）の全てのバイトが値０を有するフレーム）、或いはトラック・ディスクリプタで満たされる。いずれで満たされるかは、用いられる記録装置によって決定される。トラック・ディスクリプタを用いて、該ディスクリプタが書き込まれているトラックを記述する。トラック・ディスクリプタは、トラックの長さ及び該トラックの記録に用いられている記録方法などの情報を含む。トラック・ディスクリプタは、ディスクの機能性には影響を与えない。また上述のように、記録装置によっては、プレギャップ領域（２２１１）に、トラック・ディスクリプタのかわりに、ユーザ・データ・フィールド（１１３）に値０を有するＣＤフレームを書き込む。

【００５０】

１つのセッションは、次のような記録のシーケンスから構成される。すなわち、リード・イン（２１００）、トラック領域（２２００）、リードアウト（２３００）である。しかしながら、マルチ・セッション技術によれば、単一のディスクがいくつかの連結したセッションを有することが可能となる。以下で述べるように、この形態は記録可能な光ディスクのコピー防止スキームの構築に利用可能である。

【００５１】

空の記録可能ディスクの第１フレームは、ディスクの製造者よって値は異なるが、マイナスのアドレスから始まる。このスタート・アドレスは、「リード・イン　スタート・タイム」ともいう。ＭＳＦアドレス方式でのマイナスのアドレスは、アドレス00:00:00からのカウント・ダウンとして定義される。例えば、アドレス－１は、99:59:74として表示される。プログラム領域（２２００）は常に、アドレス00:00:00（ＭＳＦ）から開始する。よって、第１リード・インの長さは、ディスクのブランドにより異なる。第１リード・インに続くリード・イン（第２セッション及びそれ以降のセッション）の時間は通常６０秒間である。空の記録ディスクにはまた、固有の３２ビットの数が記録されている。この数は、ディスクＩＤという。ディスクＩＤは及びリード・イン　スタート・タイムは、標準的なマルチメディアコマンドである「リード・ディスク・インフォメーション：Read Disc InformatＩ／Ｏn」を用いて読み取り可能である。該コマンドは、ＳＣＳＩ　ＭＭＣ－３標準（ＮＣＩＴＳ．３６０：２００２）で定義される。

【００５２】

通常のＣＤ－ＲＯＭ装置は、メディアの記録のない領域を読みとることはできない。つまり、ＣＤ－ＲＯＭ装置がプログラム領域（２２００）の全ての領域にアクセスすること可能とするためには、プログラム領域（２２００）は、保護ゾーンであるリード・イン（２１００）及びリードアウト（２３００）が必要とする。記録済みのディスクでは、セッションを図３のようにしてもよい。

【００５３】

図４は概略図であり、Ｑサブ・チャネルの構造を示す。各ＣＤフレームは、９８ビットのＱサブ・チャネル情報を含む。フィールド（４１０）は、フレームの２バイトのサブ・チャネル同期バイトの、２ビットの同期ビットを含む。フィールド（４２０）は、４ビットの制御ビットを含む。該制御ビットは、ＣＤフレームのコンテント・タイプを記述する。制御フィールドは、デジタル・コピー許可／禁止ビット（４２１）を備える。デジタル・コピー許可／禁止ビット（４２１）は、コンテントの所有者が、ＴＮＯフィールド（４４１）により示される現在のトラックに記録されているコンテントのコピーを作成することを許可しているか否かを示す。通常、同一のトラック（２２１０）内の全てのＣＤフレームは、それぞれのデジタル・コピー許可ビット（４２１）に、同一の値を有する。このビットの値は、コンテントの所有者により、各トラックについて設定される。この設定は、コンテントをＣＤに書き込む前に、書き込みソフトウェアを介して行われる。ＡＤＲフ

ィールド（４３０）は、４ビットで、フィールド（４４０）の７２ビットのデータ・ビットのコンテントを定義する。ＡＤＲフィールド（４３０）は、「Ｑモード」と呼ばれる。残りの１６ビットであるフィールド（４５０）には、制御フィールド（４２０）、ＡＤＲフィールド（４３０）、及びデータ・フィールド（４４０）のＣＲＣコードが記録される。本発明に関連するＱモードは、Ｑモード１のみである。データＣＤセッションのトラック・プログラム領域（２２１２）内の少なくとも１０のうち９の連続したＣＤフレームが、Ｑモード１情報を保持する。

【００５４】

図４のフィールド（４４１）乃至フィールド（４４９）は９バイトであり、Ｑモード１のデータ・フィールド（４４０）を構築する。ＴＮＯフィールド（４４１）は、ＢＣＤとしてトラック番号を保持する。インデックス・フィールド（４４２）は、トラック内のフレームを、該フレームの属するトラック・セクションによってインデックス化する。第１トラックのインデックス・フィールドの値は、０１でなければならない。トラック（２２１０）のプレギャップ内では、トラック番号ＴＮＯ（４４１）は、現在のトラックの番号であり、インデックス・フィールド（４４２）の値は００である。フィールド（４４３）乃至（４４５）（ＭＩＮ、ＳＥＣ、ＦＲＡＭＥ）は、トラック（２２１０）内のフレーム（１００）の相対時間を表示する。該相対時間は、ＲＴＩＭＥ（６桁のＢＣＤで表される）ともいう。トラック（２２１０）の第１フレームのＲＴＩＭＥは、00:00:00である。図７に示すごとく、該ＲＴＩＭＥの値はトラック内のフレーム（１００）ごとに増加する。プレギャップ（２２１１）においては、連続したフレームそれぞれのＲＴＩＭＥの値は減少する。ゼロ・フィールド（４４６）は予約済みとされるとともに、ゼロとして設定される。フィールド（４４７）乃至（４４９）（ＡＭＩＮ、ＡＳＥＣ、ＡＦＲＡＭＥ）は、プログラム領域内のフレームの絶対時間のアドレスを表示する。該絶対時間は、ＡＴＩＭＥ（６桁のＢＣＤで表される）ともいう。

【００５５】

図５は概略図であり、記録可能ディスクのレイアウトを表す。ＣＤ－Ｒ／ＲＷディスクは、第１リード・イン、パワー校正領域（Power CalibratＩ／Ｏn Area、ＰＣＡ）及びプログラム・メモリ領域（ＰＭＡ）の前に、２つの追加的領域を備える。ＰＣＡは、ＣＤ－Ｒ及びＣＤ－ＲＷメディアにのみ存在する。ＰＣＡはパワーの校正を目的とする。ＰＣＡは２つの領域に分けられる。すなわち、テスト領域及びカウント領域である。ＰＭＡ（Program Memory Area：プログラム・メモリ領域）は、ＣＤ－Ｒ及びＣＤ－ＲＷメディアにのみ存在する。ＰＭＡは、メディア上のユーザ・データ領域の使用するために用いられる。記録動作が停止されると、記録装置はＰＭＡに自動的に記録を追加する。このとき次に書き込み可能なＣＤフレームの正確なアドレスも記録される。

【００５６】

書き込み操作を開始する前に、記録装置の「書き込み形態ページ」パラメータが設定されなければならない。「書き込み形態ページ」は、内部パラメータ・テーブルであり、記録装置の書き込み機能性を制御する。書き込み機能性としては例えば、書き込み方法、書き込み速度、書き込まれるコンテントの種類（オーディオ、データなど）が挙げられる。

【００５７】

記録可能ディスクへの書き込みを行う方法には、３つの方法がある。すなわち、トラック・アット・ワンス（Track At Once、ＴＡＯ）、セッション・アット・ワンス（SessＩ／Ｏn At Once、ＳＡＯ）、及びディスク・アット・ワンス（Disc At Once、ＤＡＯ）である。

【００５８】

ＴＡＯによって情報を書き込むときは、各トラックは別々の記録操作で記録される。また、記録装置のレーザ光は、各トラックの記録が終了後に停止される。ＳＡＯによって書き込みを行うときは、各セッションは連続した操作で記録される。記録装置のレーザ光は、各トラックの記録後にも停止されない。各セッションは更に、別個の操作により記録され、レーザ光は各セッションの記録が終了後に初めて停止される。

【００５９】
ＤＡＯのみが純粋に連続的な記録方法である。ＤＡＯによって書き込みを行うときは、最初のリード・インから最後のリードアウトまでのディスク上の全ての情報は、１つの連続的操作によって記録される。このとき、レーザ光は最後のセッションが書き込まれるまで停止されない。以下で説明するように、書き込み方法は、ディスクのデータ構造に影響を及ぼす。これらの影響をよりよく理解するためには、以下の用語を説明する必要がある。
【００６０】
リンク・ブロック（Link Block）
リンク・ブロックとは、レーザ光が開始されるとき及びレーザ光が停止される前に、記録装置により自動的に書き込まれるＣＤフレーム（１００）である。リンク・ブロックは、新しい記録情報を付加するためのリンクとして記録装置に用いられる。リンク・ブロックはまた、読み取り装置によってＣＤフレーム（１００）の正確な境界線を見つけるために用いられる。尚、記録装置がソフトウェア手段によってリンク・ブロックを書き込むことを防ぐことはできない。
【００６１】
図６は概略図であり、リンク・ブロック（６０１）及び（６０２）のレイアウトを表す。レーザ光が照射されると、ＣＤ記録装置は以下の５つのＣＤフレームを書き込む。すなわち、１つのリンク・フレーム及び４つのラン・イン　フレーム（ラン・イン１、ラン・イン２、ラン・イン３、及びラン・イン４）である。レーザ光が停止される前に、記録装置は２つのラン・アウト　フレーム（６０２）（ラン・アウト１及びラン・アウト２）を書き込む。例えば、ＴＡＯ書き込み方法によって書き込みを行うとき、レーザ光は、各トラックの記録前に開始され、各トラックの記録後に停止される。この場合、記録情報フィールド（６００）（図６に示す）は、ＣＤトラック（２２１０）を表す。ＳＡＯ書き込み方法によって書き込みを行うときは、レーザ光は、各セッションの記録前に開始され、記録後に停止される。この場合リンク・ブロック（６０１）及び（６０２）は、セッション（２０００）間でのみ書き込まれる。またこの場合、記録された情報（６００）は、１つのＣＤセッション（２０００）を表す。しかしながら、ＤＡＯ書き込み方法によって書き込みを行うときは、レーザ光は１回のみ開始及び停止される。ゆえに、リンク・ブロック（６０１）及び（６０２）が、トラック（２２１０）間或いはセッション（２０００）間に書き込まれることはない。
【００６２】
ロム・スキュー（Rom Skew）
ロム・スキューとは、Ｑサブ・チャネル（４００）のＡＴＩＭＥと、メイン・チャネル・ヘッダ・フィールド（１１２）のＡＴＩＭＥの時間差である。ＣＤ読取装置は、Ｑサブ・チャネル（４００）を用いて、ＣＤ上の任意の場所を検索する。Ｑサブ・チャネル内のアドレスが見つかると、読み取り装置はメイン・チャネルに切り換えて、フレームのヘッダ内で同一のＡＴＩＭＥアドレスを検索する。ロム・スキュー値が大きいと、読み取りアクセスが遅くなり、値がマイナスであると、既存のＣＤ読み取り装置との整合性に問題が起きる。標準的なＣＤ書き込み装置内のエンコーダ、或いはＣＤ製造工場の専門的なマスタリング装置を駆動するエンコーダを用いてディスクを作成する場合は常に、ディスクのロム・スキュー数は、エンコーダがディスク作成する間に下す決定により決められる。
【００６３】
サブコード・フォーマット
サブコード・フォーマットは、インデックス・フィールドの値が０であるトラックの領域（プレギャップ（２２１１））内のＲＴＩＭＥフレーム・アドレスのフォーマットに関する。サブコード・フォーマットとしては、２つのフォーマットが可能である。すなわち、Sony（ソニー）及びPhilips（フィリップス）サブコード・フォーマットである。これらのサブコード・フォーマットの主要な相違点を図７に示す。連続するフレームのＲＴＩＭＥの値は、インデックス・フィールドの値が０であるトラックの領域内では、減少する

ように指定されている。Philipsのフォーマットでは、ＲＴＩＭＥの値は、00:00:01（左から２桁は分を、次の２桁は秒を、最後の２桁はフレームを表す）まで減少する。また、ＲＴＩＭＥの値は、（トラック・プログラム領域（２２１２）の）インデックス・フィールドの値が１であるフレームに到達したときにのみ、00:00:00の値をとる。その時点で、00:00:00というＲＴＩＭＥの値は連続するフレームの１フレームごとに、１ずつ増加する。Philipsのサブコード・フォーマットを用いて書き込みされたディスクでは、00:00:00というＲＴＩＭＥの値を有するフレームは１つのみである。また、このフレームが、インデックス・フィールドの値が０から１に変化するフィールドである。Sonyのフォーマットでは、ＲＴＩＭＥの値は、インデックス・フィールドの値が０である連続するフレームにおいて00:00:00まで減少する。また、インデックス・フィールドの値が１であるトラックの第１フレームのＲＴＩＭＥ値もまた00:00:00である。その時点で、ＲＴＩＭＥ値は、連続するフレームの１フレームごとに１ずつの増加に転ずる。Sonyのサブコード・フォーマットを用いて書き込まれたディスクでは、インデックス・フィールドの値が０から１に変化する１つのトラック内に、00:00:00というＲＴＩＭＥ値が２つ存在する。ロム・スキューのように、ディスクのサブコード・フォーマットは、該ディスクの記録に用いるエンコーダにより決定される。

【００６４】

図１３Ａは、予め焼かれた領域を備える記録可能ディスクの構造を表す。予め焼かれた領域は、本発明の好適な実施形態にしたがって意図的に埋め込まれた論理記号を含む。ディスク（１３００）は、標準的な記録可能ディスクであるが、ディスクの第１セッションに固有のパターンを焼くことにより、予め焼かれた情報（１３０１）の一部を付加されている。予め焼かれた情報（１３０１）は、追加する情報を、ディスク（１３００）の記録可能領域（１３０２）の１つ若しくはそれ以上のセッションに、任意の標準的な記録装置を用いて焼くことにより、追加される。これは、ディスクを「オープン」のままにすることで実現される。マルチ・セッション・ディスクでは、ディスクに十分な空スペースがあり、且つディスクが「オープン」であれば、追加的なセッションを付け加えることが可能である。ディスクを「オープン」の状態を保つには、データを焼くソフトウェアにより、最後の記録済みセッションのリード・イン内の、次に書き込み可能なアドレスが特定されることが必要である。この値が不明の場合や、或いはFF:FF:FFである場合は、ディスクは閉じられ、追加的なセッションを該ディスクに付加することは不可能である。

【００６５】

図１３ｂは、予め焼かれた情報（１３０１）の構造を表す。予め焼かれた情報（１３０１）は、２つのトラック（トラック１及びトラック２）を有するセッションである。第１トラック（１３３１）のプレギャップは、以下のような意図的に埋め込まれた論理記号を有するＣＤフレームを備える。

・偽のトラック・ディスクリプタ

プレギャップ１フィールド（１３３１）はトラック・ディスクリプタを備えるいくつかのＣＤフレームを有する。該トラック・ディスクリプタは、トラック１を意図的に不適切に記述するので、該トラック・ディスクリプタは標準的な記録方法には対応しないものとなる。ディスク（１３００）のコピーを作成するとき、これら偽のトラック・ディスクリプタはゼロ或いは新しいトラック・ディスクリプタと置き換えられる。新しいトラック・ディスクリプタは、トラック及び用いられている記録方法を適切に記述する。

・プレギャップ領域内の「カスタム情報」

予め焼かれた情報のプレギャップ１フィールド（１３３１）は、いくつかのＣＤフレームからなる。該ＣＤフレームは、固有のパターン（以下「カスタム情報」という）を有する。「カスタム情報」パターンは、従来のトラック・ディスクリプタ構造とは整合性を持たない。これら「カスタム情報」パターンを含むディスクのコピーを試みると、記録装置は通常、これら「カスタム情報」パターンをゼロ或いは正規のトラック・ディスクリプタと

置換する。いずれと置換されるかは、用いられる記録装置及び記録方法による。
【００６６】
本発明の好適な実施形態ではトラック１のトラック・プログラム領域フィールド（１３４１）は、以下の意図的に埋め込まれた論理記号を有するＣＤフレームを備える。

第１のトラック即ちトラック１の相対アドレス00:02:16に位置するＣＤフレームは、
ＩＳＯ９６６０にしたがって使用しない状態とされているフィールドに、１つ若しくは複数の識別マークを備える。ＩＳＯ９６６０によると、この特定のフレーム・アドレスは、記録済みのＣＤに関する雑多なデータを記録するために用いられる。これらの識別マークの存在は、ディスク（１３００）が、本発明にしたがってコピーから保護された記録ディスクであることを示す。このようなディスクには、暗号化されたコピー防止デジタル・コンテントを記憶可能である。

・デジタル・サイレンス
標準的な記録装置は、ＣＤフレームをデジタル・サイレンスとともに記録するようには設計されていない。ディスク（１３００）のコピーを作成するとき、デジタル・サイレンス・フレームはコピーされない。これは、ＣＤフレームの再フォーマットが、記録装置の内部エンコーダにより実行されるからである。

・ロム・シンク・シフト
記録装置は、ＣＤフレームをロム・シンク・シフトとともに記録するようには設計されていない。保護されたディスク（１３００）のコンテントをコピーしようとすると必ず、ロム・シンク・シフトを示すＣＤフレームそれぞれの同期パターン（１１１）（図１に示す）が保存される。該同期パターン（１１１）同士は一致させられる。

・シリアル＃Ａ
２つの固有のシリアル・ナンバが、予め焼かれた情報（１３０１）に加えられる。第１の番号であるシリアル＃Ａ（コピー・シール）は、トラック１のプログラム領域の１つ若しくはそれ以上のＣＤフレームに書き込まれる。シリアル＃Ａは標準的な情報として、ＣＤフレームのユーザ・データ・フィールド（図１のフィールド（１１３））に書き込まれる。これにより、確実にシリアル＃Ａはオリジナル・ディスクの全てのコピーに移される。予め焼かれた情報（１３０１）は、記録することによりディスクに付加される。よって、固有のシリアル＃Ａを、記録途中に、保護されたディスクのそれぞれに書き込むことが可能である。以下に説明するように、シリアル＃Ａは、海賊版の追跡に用いられる。

・シリアル＃Ｂ
第２のシリアル・ナンバであるシリアル＃Ｂ（コピー認証）の個々のビットは、デジタル・コピー許可ビット（４２１）に書き込まれる。デジタル・コピー許可ビット（４２１）は、トラック１のトラック・プログラム領域（２２１２）内のいくつかのＣＤフレームからなるシーケンスである。このように、シリアル＃Ｂの１ビットは、トラック１内のフレームのシーケンス内にある各ＣＤフレームのデジタル・コピー許可ビット（４２１）に書き込まれる。よって、コピー防止ＣＤの第１セッションに焼かれたトラック１は、デジタル・コピー許可ビット（４２１）に、様々な値を有するいくつかのＣＤフレームを備えるように設定される。コピー防止ディスク（１３００）のコンテントのコピーを試みると常に、（オリジナル・ディスクの）これらビット（４２１）が有する様々な値が１つの一定値に置換される。この一定値は、記録されたコピーのトラック１の全てのデジタル・コピー許可ビット（４２１）について一定である。
【００６７】
本発明の一つの好適な実施形態によると、トラック１のプレギャップ１（１３３１）は、Philipsサブコード・フォーマットによって記録される。一方で、トラック２のプレギ

ャップ２（１３６１）はSonyサブコード・フォーマットによって記録される。このようにして、コピー防止ディスク（１３００）のコンテントのコピーを試みると常に、記録されたコピーのプレギャップ領域（１３３１）及び（１３６１）の両方が、記録装置によって決定された１つのサブコード・フォーマットによって記録される。

【００６８】

予め焼かれた情報（１３０１）はまた、トラック１のポストギャップ１（１３５１）とトラック２のプレギャップ２（１３６１）の間にリンク・ブロックを備える。追加的な偽のリンク・ブロックが、意図的にトラック１のトラック・プログラム領域（２２１２）の中間に書き込まれる。標準的な記録装置及び記録方法を用いた場合、トラック１のトラック・プログラム領域（２２１２）にはリンク・ブロックは書き込まれない。これらのリンク・ブロックは、標準的なＣＤフレームの替わりにトラック１のプログラム領域内に書き込まれる偽のリンク・ブロックである。ディスク（１３００）のコピーを作成すると、コピーを作成するのに用いた記録方法にしたがって、リンク・ブロックが書き込まれる。よって、トラック１のトラック・プログラム領域内の偽のリンク・ブロックは、記録されたコピーにはコピーされない。加えて、コピーが連続的な記録方法（ＳＡＯ或いはＤＡＯ）によって記録される場合には、コピーに、フィールド（１３５１）とフィールド（１３６１）の間のリンク・ブロックが現れないこともある。

【００６９】

図１３Ｂのリンク・ブロックのそれぞれは、ブロック（６０２）及び（６０１）のシーケンスからなる。各ブロックは、図６に示す構造を有する。これらの記録された構造は、従来のＣＤ読み取り装置では読み取ることができない。したがって、このような記録された構造をコピーしようとしても、不確実なコンテントが記録される。当然ながら、コピーを記録するのに用いられる記録方法によっては、記録装置により追加的なリンク・ブロックが生成される。

【００７０】

上に挙げた論理記号を除いて、ディスクのＰＭＡ領域（１３００）は意図的に埋め込まれた偽のＰＭＡエントリ（１３１１）を備える。このＰＭＡエントリ（１３１１）はディスクのレイアウトに適合しない。偽のＰＭＡエントリの一例としては、トラック１のトラック・プログラム領域内のＣＤフレームのアドレスを挙げるようなものがある。これは実際のＰＭＡエントリではない。なぜならば、ＰＭＡエントリは、記録が停止されたときにのみ書き込まれるものであり、記録装置は、トラックの途中で記録を停止するようには設計されていないからである。したがって記録装置は上記の該トラック内での記録を続ける。ディスク（１３００）のコピーを作成しようとすると、記録装置はコピーに、ディスクレイアウト及び記録方法に適合するＰＭＡエントリを付加する。すなわち、偽のＰＭＡエントリはコピーには存在しない。

【００７１】

これらの意図的に埋め込まれた論理記号は、ディスクＩＤ、リード・イン　スタート・タイム、及び予め焼かれた情報のロム・スキュー値と併せて、オリジナル・ディスクがオリジナルであることを証明するとともに、暗号化によって不正コピー及び不正使用からデジタル・コンテントを保護するために用いられる。以下に説明するように、保護されるべきコンテントは、記録可能領域（１３０２）に追加される。

【００７２】

図９は、全ての記録可能ディスクに存在するディスク固有の識別記号を用いて、記録可能ＣＤを認証するプロセスを表す。該プロセスは、ステップ９００から始まる。ステップ９００においては、ディスクからディスクＩＤが読み取られる。ステップ９０２においては、ＣＤからリード・イン　スタート・タイムが読み取られる。ステップ９０３においては、ステップ９００及びステップ９０２で読み取られた値が、ＣＤがオリジナルCDである場合にＣＤから読み取られることが期待される値と比較される。読み取られた値が期待される値と等しいならば、そのＣＤはオリジナルである。等しくない場合は、ＣＤはコピーである。このような認証プロセスを実行する認証ソフトウェアを用いることによって、該

ソフトウェアに、該認証プロセスにおいて、ディスクＩＤ及びリード・イン　スタート・タイムの期待される値が提供される。これにより、該認証ソフトウェアを記憶するメディアがオリジナルか否かを判断することが可能となる。またその結果に応じて、操作が継続或いは終了される。

【００７３】

図１２Aおよび図１２Bは、標準的な記録可能ディスクに記憶されたデジタル・コンテンツを、暗号化よって、不正コピーから保護する方法を示す。図１２Aは暗号化プロセスを表し、図１２Bは、解読プロセスを表す。尚、該解読プロセスは、図１２Aに示すコピー防止方法によって作成されたディスクから、コピー防止コンテンツが読み取られるたびに実行される。

【００７４】

暗号化プロセスは、図１２Aのステップ１２００から開始する。ステップ１２００では、ディスクIDとリード・イン　スタート・タイムが読み取られる。ステップ１２０２では、認証プロセス（図９に示す）の、各種の期待される値が設定される。図９に示すプロセスのステップ９０３に示すごとく、期待される値は、実行プログラム・ファイルに組み込まれた認証プロセスによって用いられる。ステップ１２０２は、実行プログラム・ファイル内の固定値を、ファイルが書き込まれるディスクのディスクID及びリード・イン　スタート・タイムの実際の値に置換することにより実行される。ステップ１２０３においては、ディスクID及びリード・イン　スタート・タイムを用いて暗号キーが作成される。該暗号キーは、該ディスクIDとリード・イン　スタート・タイムの値を、数学的及び／又は論理的操作を利用して、及び／又は所定のシーケンスの順列を利用して操作することにより作成される。尚、該順列は、該値について、或いは該値に対する数学的及び／又は論理的操作の結果に基づく。例えば、暗号化キーは、ディスクＩＤ及びリード・イン　スタート・タイムの値の排他的論理和をとることにより、作成されてもよい。

【００７５】

ステップ１２０４では、書き込まれようとしているコンテンツ（記録されるべき実際のコンテンツ）が、ステップ１２０３で作成された暗号化キーを用いて暗号化される。ステップ１２０５では、暗号化されたコンテンツが、ディスク（CD）に書き込まれる。つまり、この方法を用いて暗号化されたコンテンツを有するディスクのコピーを試みると、記録されたコピーの暗号化コンテンツは、無用のものとなる。暗号コンテンツを適切に解読及び使用するためには、ディスクＩＤ及びリード・イン　スタート・タイムの正確な値が必要である。コピーのディスクがオリジナルと同一のディスクIDとリード・イン　スタート・タイムの値を有する可能性は、無視できる程度に低い。

【００７６】

図１２Bは、ディスクから暗号化されたコンテンツを読み取るたびに実行される解読プロセスを示す。ステップ１２１１では、必要な暗号化コンテンツがディスクから読み取られる。ステップ１２１２では、ディスクID及びリード・イン　スタート・タイムがディスクから読み取られる。ステップ１２１３では、解読キーが、ディスクID及びリード・イン　スタート・タイムを用いて計算される。ステップ１２１３で解読キーを得るために用いられる計算プロセスは、ステップ１２０３で暗号化キーを作成するために用いられるプロセスと同一である。ステップ１２１４では、ステップ１２１１で読み取られた必要なコンテンツが、ステップ１２１３で計算された解読キーにより解読される。CDがオリジナルであれば、該ディスクのディスクID及びリード・イン　スタート・タイムを用いて的確な解読キーが作成されるとともに、コンテンツが的確に解読される。一方で、ディスクが記録されたコピーであると、該ディスクのディスクＩＤ及びリード・イン　スタート・タイムの値は、オリジナルにおけるそれぞれの値と異なる。よって、この場合にステップ１２１３で認証ソフトウェアによって計算される解読キーは、不適格な解読キーとなり、コピー防止コンテンツは的確に解読されない。

【００７７】

図１０A及び図１０Bは、記録可能ディスクに対する認証プロセスを示す。この記録可能

ディスクは、図１３Ａ及び図１３Ｂに示す本発明の予め焼かれた情報（１３０１）を備える。このプロセスは、図１０Aのステップ１０００から始まる。第１プレギャップ領域であるフィールド（１３３１）（図１３Bに示す）がオリジナルのコピー防止ディスク（１３００）上にある偽のトラック・ディスクリプタ及びカスタム情報についてスキャンされる。ステップ１００１では、ステップ１０００で実行されたスキャンおいて、期待されるトラック・ディスクリプタ及びカスタム情報が発見されたか否かがチェックされる。ステップ１００１において、期待されるトラック・ディスクリプタ及びカスタム情報が発見されなかったと決定された場合は、ディスクはコピーであると決定される。そうでない場合は、コントロールはステップ１００２に進む。

【００７８】

ステップ（１００２）において、トラック１（フィールド１３４１）のトラック・プログラム領域のＣＤフレームが、ディスクから読み取られる。該ＣＤフレームは、オリジナル・ディスクに存在するとともに、意図的に埋め込まれているデジタル・サイエンスを有するはずである。ステップ１０１１において、ステップ１００２で読み取られたCDフレームがデジタル・サイエンスを有するか否かがチェックされる。もし、デジタル・サイエンスを有するフレームが発見されなければ、そのCDはコピーであると決定される。ステップ１００２で読み込まれたCDフレームが、デジタル・サイレンスを有すると決定された場合には、コントロールはステップ１００３に進む。ステップ１００３においては、オリジナル・ディスクのトラック１のプログラム領域に意図的に埋め込まれたロム・シンク・シフトを含むＣＤフレームが読み取られる。ステップ１０１２では、ステップ１００３で読み取られたCDフレーム内にロム・シンク・シフトが存在するか否かがチェックされる。ロム・シンク・シフトが存在しないと決定されると、ＣＤはコピーであると決定される。ロム・シンク・シフトが存在すると決定されると、コントロールは、ステップ１００４に進む。ステップ１００４では、第１番目及び第２番目のプレギャップ（フィールド１３３１及びフィールド１３６１）のサブコード・フォーマットが決定される。ステップ１０１３において、ディスク上の上記の２つのプレギャップが同一のサブコード・フォーマットを有するか否かがチェックされる。２つのプレギャップが同一のサブコード・フォーマットを有すると決定された場合には、ディスクはコピーであると決定される。上記の２つのプレギャップにおいて、異なるサブコード・フォーマットが発見された場合には、コントロールは、数字「４」で示される段階を通じて、図１０Ｂのステップ１００５に進む。

【００７９】

図１０Bのステップ１００５において、予め焼かれた情報（１３０１）が、期待されるリンク・ブロックについてスキャンされる。ステップ１０１４では、ステップ１００５で実行されたスキャンで、期待されるリンク・ブロックが発見されたか否かがチェックされる。期待されるリンク・ブロックが発見されなかった場合には、ディスクはコピーであると決定される。そうでない場合、すなわち該リンク・ブロックがディスク上で発見された場合には、コントロールはステップ１００６に進む。ステップ１００６においては、ディスクのＰＭＡエントリがディスクのＰＭＡ領域から読み取られる。ステップ１０１５においては、期待される偽のＰＭＡエントリがディスク上に存在するか否かがチェックされる。偽のＰＭＡエントリがディスク上に存在しない場合には、ディスクはコピーであると決定される。そうでない場合、すなわち偽のＰＭＡエントリがディスク上に存在する場合には、コントロールはステップ１００７に進む。ステップ１００７においては、予め焼かれた情報（１３０１）のロム・スキュー値がチェックされる。ステップ１０１６においては、ステップ１００７において決定された実際のロム・スキュー値が、オリジナルのコピー防止ディスクに存在すると期待される値と等しいか否かがチェックされる。２つの値が等しくない場合は、ディスクはコピーであると決定される。そうでない場合、すなわちステップ１００７において決定されたロム・スキュー値が期待される値と等しい場合には、ディスクはオリジナルであると決定される。

【００８０】

図１０A及び図１０Bに示す認証プロセスは、本発明における認証テストの全てを含む。

しかしながら、これらテストを全て行わなくても、コピー防止ディスクがオリジナルであるか否かを決定可能である。つまり、上述のテストの一部に基づいた、より簡便な認証手順を用いてもよい。

【００８１】

図１１A及び図１１Bは、記録可能ディスク（１３００）に埋め込まれた論理記号及びシリアル・ナンバを用いてデジタル・コンテンツを不正コピーから保護する方法を示す。図１１Ａは、暗号化プロセスを示し、図１１Ｂは解読プロセスを示す。これらプロセスはコピー防止ディスクから、記録されたコンテンツを読み取るたびに実行される。

【００８２】

暗号化プロセスは、図１１Ａのステップ１１００から始まる。ステップ１１００においては、偽のトラック・ディスクリプタ及びカスタム情報が、ディスクの第１プレギャップ（図１３Ｂのフィールド１１３１）から読み取られる。ステップ１１０１においては、ディスク固有のシリアル＃Ａが、ディスクの第１トラックのトラック・プログラム領域（フィールド１３４１）から読み取られる。ステップ１１０２においては、ディスク固有のシリアル＃Ｂが、ディスクの第１トラックのトラック・プログラム領域（１３４１）から読み取られる。ステップ１１０３においては、ステップ１１０１及びステップ１１０２において読み取られた情報の一部もしくは全てを用いて、暗号化キーが計算される。ステップ１１０４においては、保護されなければならないデジタル・コンテンツが、ステップ１１０３において計算された暗号化キーを用いて暗号化される。ステップ１１０５においては、暗号化されたコンテンツが、追加的セッションにある、ディスクの記録可能領域（フィールド１３０２）に書き込まれる。

【００８３】

図１１Ｂは、解読プロセスを示す。解読プロセスは、コンテンツがディスクから読み取られるたびに行われる。ステップ１１１０においては、必要なコンテンツが読み取られる。ステップ１１１１では、偽のトラック・ディスクリプタ及びカスタム情報が、ディスクの第１プレギャップ（図１３Ｂのフィールド１３３１）から読み取られる。ステップ１１１２においては、ディスク固有のシリアル＃Ａが、ディスクの第１トラックのトラック・プログラム領域（１３４１）から読み取られる。ステップ１１１３においては、ディスク固有のシリアル＃Ｂが、ディスクの第１トラックのトラック・プログラム領域（１３４１）から読み取られる。ステップ１１１４においては、解読キーが、ステップ１１１１乃至ステップ１１１３において読み取られた情報を用いて計算される。ステップ１１１５においては、ステップ１１１０において読み取られたデジタル・コンテンツが、ステップ１１１４において計算された解読キーを用いて解読される。ディスクがコピーであれば、偽のトラック・ディスクリプタが及びカスタム情報がディスクの第１プレギャップ内に存在しないはずである。また、シリアル＃Ｂもディスク上に存在しないはずである。したがって、ステップ１１１４において計算された解読キーは、間違ったキーとなるはずである。よって、このような場合には、コピー防止コンテンツは適切に解読されない。一方で、ディスクがオリジナルであれば、ステップ１１１４において、正しい解読キーが計算されるので、該コンテンツは、適切に解読される。

【００８４】

ステップ１１０３及びステップ１１１４において実行される暗号化キー及び解読キーは、既に得られている値（すなわち、シリアル＃Ａ、シリアル＃Ｂ、偽のトラック・ディスクリプタ及びカスタム情報）の一部若しくは全てを用いて作成される。このとき、数学的及び／又は論理的操作の利用、及び／又は前述の値或いはそれらについて行われた数学的及び／又は論理的操作の結果としての、いくつかの所定のシーケンスの利用が必要である。

【００８５】

図８Ａは概略図であり、コンテンツ保護ドライバ（８１３）を含むコンピュータ・システムのアーキテクチャを表す。コンピュータのメモリ（８１０）は、オペレーティング・システム・ソフトウェアを備える。全てのオペレーティング・システム・ソフトウェアは

、アプリケーション（８１１）のＩ／Ｏデバイス（８１６）へのアクセスを管理する２つの主要な要素からなる。第一の要素は、オペレーティング・システムのＩ／Ｏ　ＡＰＩ（Input/Output ApplicatＩ／Ｏn Interfaces）（８１２）である。第二の要素は、オペレーティング・システムのデバイス・ドライバ（８１４）である。通常のオペレーティング・システムでは、アプリケーション（８１１）を動作するためには、オペレーティング・システムのI／Ｏ　ＡＰＩ（８１２）が必要である。オペレーティング・システムのＩ／Ｏ　ＡＰＩ（８１２）は、Ｉ／Ｏコントローラ（８１５）を介しての、Ｉ／Ｏデバイス（８１６）からの又はＩ／Ｏデバイス（８１６）への、インプット／アウトプット操作を実行する。オペレーティング・システムのI／Ｏ　ＡＰＩ（８１２）はオペレーティング・システムのデバイス・ドライバ（８１４）を用いて、実際のインプット／アウトプット・タスクを実行する。各ドライバは、該ドライバの管理するデバイスに適した固有のI／Ｏ手順を有する。

【００８６】

コンテンツ保護ドライバ（８１３）は、オペレーティング・システムのI／Ｏ　ＡＰＩ（８１２）及びオペレーティング・システムのデバイス・ドライバ（８１４）の間にインストールされる。このインストールは、Ｉ／Ｏデバイス（８１６）及びコンピュータ・メモリ（８１０）の間に配されている。これによって全てのＩ／Ｏオペレーション及びデータ転送を妨げることが可能となるように行われる。このようにコンテンツ保護ドライバ（８１３）を配することをフッキング（hooking）ともいう。

【００８７】

図８Ｂは、コンテンツ保護ドライバ（８１３）をコンピュータ・オペレーティング・システムへインストールする手順を示す。ステップ８００において、インストール手順は、サポートされたＩ／Ｏデバイス（８１６）がコンピュータ・システム内に存在するか否かをチェックする。サポートされたＩ／Ｏデバイス（８１６）がなければ、コンテンツ保護ドライバのインストール手順は、ステップ８０１で停止される。そうでない場合、すなわちサポートされたＩ／Ｏデバイス（８１６）がある場合は、コントロールはステップ８０２に進む。ステップ８０２において、インストール手順は、オペレーティング・システムのＩ／Ｏ　ＡＰＩ（８１２）をインストールされたコンテンツ保護ドライバ（８１３）までフックする。オペレーティング・システムのＩ／Ｏ　ＡＰＩ（８１２）がコンテンツ保護ドライバ（８１３）までフックされた後は、全てのアプリケーション（８１１）からの全てのＩ／Ｏリクエストは、ＯＳデバイス・ドライバ（８１４）に向けてではなく、ＯＳのＩ／Ｏルーティン及びコンテンツ保護ドライバ（８１３）のＩ／Ｏルーティンを通して、送信される。

【００８８】

コンテンツ保護ドライバ（８１３）は、実際にはプログラム・ファイルであり、コピー防止メディア自体に、或いは別のメディアに記憶可能である。インストールする段階は、このプログラム・ファイルを動作させることにより開始される。

【００８９】

ステップ８０３においては、既存のサポートされたＩ／Ｏデバイス（８１６）のそれぞれに、メディアが存在するか否かがチェックされる。メディアが存在しなければ、コントロールはステップ８０９に移る。ステップ８０９においては、フラグ（No Decrypt）が特定のＩ／Ｏデバイスから読み取られているコンテンツを解読する必要がないことを示すように設定される。コントロールがステップ８０９から数字「２」で示される段階を介してコンテンツ保護ドライバのメイン・ループに移るまで、オペレーションは継続する。

【００９０】

ステップ８０３においてメディアがサポートされたＩ／Ｏデバイスのうちの一つに存在すると決定されると、コントロールはステップ８０４に移る。ステップ８０４においては、メディア上のコンテンツが暗号化されているか否かがチェックされる。このチェックの方法は、メディアの種類によって変わる。ＣＤの場合は、第１トラックの相対アドレス00:02:16にあるＣＤフレームを読み取ることにより行われる。上記で説明したように、この

ＣＤフレームは、本発明の暗号化プロセスにしたがって、識別記号を記憶するために用いられる。該識別記号は、ＩＳＯ９６６０にしたがって未使用とされているフィールドに記憶される。識別記号の存在は、メディアがコピーから保護されており、該メディアのコンテンツが暗号化されていることを示す。メディアのコンテンツが暗号化されていないならば、特定のＩ／Ｏデバイスから読み取られて記憶されているコンテンツの解読を行う必要はない。よってコントロールはステップ８０９に移る。コンテンツが暗号化されているならば、該プロセスはステップ８０５に進む。ステップ８０５においては、認証テストが行われて、メディアがオリジナルか否かが決定される。認証テストの方法もまた、メディアの種類によって変わる。記録可能ＣＤの場合には、この認証テストとして、図９、図１０Ａ及び図１０Ｂに示す本発明の認証テストのうちの一つを行ってもよい。

【００９１】

ステップ８０６においては、ステップ８０５の認証テストの結果がチェックされる。ステップ８０６においてメディアがオリジナルでないと決定されると、特定のＩ／Ｏデバイスから読み取られたコンテンツの解読は行われない。またコントロールはステップ８０９に移る。ステップ８０６においてメディアがオリジナルであると決定された場合には、コントロールはステップ８０７に移る。ステップ８０７においては適切な解読キーがメディアから読み取られる。その後コントロールはステップ８０８に移る。ステップ８０８においては、No Decryptフラグをリセットされ、該フラグが特定のＩ／Ｏデバイスから読み取られたコンテンツが解読される必要があることを示すようにされる。続いてコントロールは、数字「２」で示される段階を介してメイン・ループに移る。コピー防止コンテンツを解読するのに必要な解読キーは、記憶メディアの所定位置に記憶されている。この位置は、用いられている記憶メディアの種類にしたがって決定される。例えば、ＣＤ暗号化においては、暗号化キーはプレギャップにあるシリアル＃Ａ及びシリアル＃Ｂの値と、カスタム情報を用いて計算されてもよい。

【００９２】

図８Ｃは、コンテンツ保護ドライバ（８１３）のメイン・ループによって行われるプロセスを示す。ステップ８３１においてプロセスは、ウェイト状態に入る。この状態は、Ｉ／Ｏオペレーションによって作成されたＩ／Ｏイベントが、フックを用いて識別されるまで続く。該フックはステップ８０２において設定されたものである。Ｉ／Ｏイベントが作成されると、コントロールは、ステップ８３２に移る。ステップ８３２においては、イベントがサポートされたＩ／Ｏデバイス（８１６）のうちの一つに挿入された新しいメディアのために作成されたものであるのか否かがチェックされる。新しいメディアが挿入されているならば、コントロールはステップ８３８に移る。ステップ８３８においては、挿入されたメディアが保護されているか否かがチェックされる。ステップ８３８において行われるテストは、ステップ８０４において行われるテストと同一である。メディアが保護されていないならば、コントロールは、ステップ８４３に移る。ステップ８４３においては、No Decryptフラグが、特定のＩ／Ｏデバイスから読み取られたコンテンツの解読の必要がないことを示すように設定される。コントロールはその後、ステップ８３１に移り、次のＩ／Ｏイベントを待つ。

【００９３】

ステップ８３８において新しく挿入されたメディアが保護されていると決定されると、コントロールはステップ８３９に移る。ステップ８３９においては、メディアについて認証テストが行われる。ステップ８３９のテストは、図８Ｂに示すステップ８０５において行われるテストと同一である。この認証テストの結果は、ステップ８４０においてチェックされる。メディアがオリジナルでないと決定された場合には、特定のメディアから読み取られたコンテンツを解読する必要がない。よってコントロールはステップ８４３に移る。メディアがオリジナルであると決定された場合には、コントロールはステップ８４１に移る。ステップ８４１においては適切な解読キーがメディアから読み取られる。次のステップ８４２においては、No Decryptフラグがリセットされて、該フラグが、特定のＩ／Ｏデバイスから読み取られたコンテンツが解読されなければならないことを示すようにされ

る。

【００９４】

ステップ８３２において、新しいメディアが挿入されなかったと決定されると、コントロールはステップ８３３に移る。ステップ８３３においては、イベントが、中断された書き込み操作によって作成されたのか否かがチェックされる。もしそうであるならば、コントロールは、数字「３」で示される段階を介して、書き込み手順（図８Ｄ）に移る。イベントが中断された書き込み操作によって作成されたものではないと決定された場合には、コントロールはステップ８３４に移る。ステップ８３４においてはイベントが中断された読み取り操作のために作成されたのか否かがチェックされる。

【００９５】

ステップ８３４において、イベントが、中断された読み取り操作によって作成されたのではないと決定されると、コントロールはステップ８３１に戻る。ステップ８３１においては、該プロセスはウェイト状態（待ち状態）に入り、次のイベントを待つ。ステップ８３４において、イベントが中断された読み取り操作によって作成されたと決定されると、コントロールはステップ８３５に移る。ステップ８３５においては、読み取られたコンテンツが解読されるべきか否かがチェックされる。このチェックは、特定のＩ／ＯデバイスのNo Decryptフラグの状態をチェックすることにより行われる。解読が行われるべきでない場合（No Decrypt=「１」）は、コントロールはステップ８３１に戻り、次のイベントを待つ。解読が行われるべきである場合（（No Decrypt=「０」）は、コントロールはステップ８３６に移る。ステップ８３６においては、読み取られたコンテンツが解読される。プロセスは、ステップ８３７に進む。ステップ８３７においては、読み取られたコンテンツのＣＲＣコードが計算された後、ＣＲＣの結果がコンピュータ・メモリに記憶される。このステップはまた、最近の読み取り操作において読み取られた全てのコンテンツのＣＲＣコードのリストを管理する。最後にコントロールはステップ８３１に戻って、次のイベントを待つ。

【００９６】

図８Ｄは、ステップ８３３（図８Ｃ）から始まる書き込み手順を表す。ステップ８４１において、書き込まれようとしているコンテンツのＣＲＣコードが計算される。ステップ８４２においては、ステップ８４１で計算されて得られたＣＲＣコードが、最近の読み取り操作で読み取られたコンテンツのために計算されたＣＲＣコードのうちの１つと等しいか否かがチェックされる。このチェックは、図８Ｃに示すステップ８３７で管理されるリストにあるＣＲＣコードをチェックすることにより行われる。計算されたＣＲＣがリストにあるＣＲＣの値のうちの１つと等しいならば、コントロールはステップ８４４に移る。ステップ８４４においては、書き込まれようとしているコンテンツが破壊される。このことは、意味のないランダム・インフォメーションを上書きすることにより行われる。

【００９７】

ステップ８４２において、計算されたチェックサムが、最近の読み取り操作で読み取られたコンテンツのために計算されたチェックサムのうちの１つと等しくないと決定された場合には、コントロールがステップ８４３に移る。ステップ８４３においては、書き込みプロセスは通常、継続を許可される。最後に、コントロールは、数字「２」で示される経路を介して、コンテンツ保護ドライバのメイン・ループ内のステップ８３１に戻る。

【００９８】

コピー防止コンテンツのコピーからの保護は、アクティブ・プロセスによって適宜更に改善できる。例えば、ステップ８３７において、読み取りイベントを開始させたプロセスに関連するフラグを設定してもよい。このようにして、書き込み操作がこのプロセスにより行われるたびに、ステップ８４２において書き込みイベントを開始させたプロセスに関連するフラグの状態がチェックされることにより、コピーが防止される。書き込みイベントが開始したプロセスと関連するフラグがオンと設定されていると決定されると、ステップ８４４における書き込み操作は阻止される。このようにして更に保護を行うと、開始プロセスからのいかなるアウトプット（例えば、印刷、ペースト）も防止できる。

【００９９】
図１４は、クライアントの分配リストを管理するプロセスを表すフローチャートである。該リストは、クライアントの氏名、アドレス、及び特定のクライアントが受け取る予定の予め焼かれたディスク１３００のシリアル＃Ａなどを備える。システムはクライアント情報をクライアント・リストから取得して、該クライアントに固有のディスクを作成する。システムはまた、リストに、分配されたディスク、全てのクライアント情報、及び各クライアントのために作成されたディスクのシリアル＃Ａコードを追加する。ステップ１４００において、シリアル＃Ａが予め焼かれたディスク１３００から読み取られる。ステップ１４０２においては、次のクライアントの情報が、クライアント・リストから読み取られる。ステップ１４０３においては、シリアル＃Ａ及びステップ１４０２において読み取られたクライアントの情報が、分配されたディスクのリストに追加される。ステップ１４０４においては、保護されるべきコンテンツが暗号化されるとともに、図１１Ａに示すプロセスを用いてディスクに書き込まれる。ステップ１４０９においては、クライアント・リストに、追加されたクライアントがあるか否かがチェックされる。追加されたクライアントがない場合には、プロセスは終了する。追加されたクライアントがある場合には、コントロールは、ステップ１４０８に移る。ステップ１４０８において、システムのオペレータは、新しい記録可能ディスク１３００を記録装置に挿入するように求められる。

【０１００】
図１５は、海賊版を追跡するプロセスを表す。シリアル・ナンバを有するコピー防止メディア（１３００）の不正コピーが発見された場合、本発明のコピー防止方法を用いて、該コピーの元となったオリジナル・ディスクの所有者を追跡することが可能である。システムは、シリアル・ナンバを付加されたメディアのコピー（すなわち、コピー防止ディスク１３００からのコピー）から、シリアル・ナンバを読み取るとともに、分配されたディスクのリストにあるクライアントのうちの１つと照合する。ステップ１５０１において、シリアル＃Ａのコードが読み取られ、ステップ１５０２においては分配されたディスクのリストが、対応するシリアル＃Ａコードを有する記録についてスキャンされる。ステップ１５０３においては、ステップ１５０２のスキャンにおいて、対応するシリアル＃Ａコードを備える記録が発見されたか否かがチェックされる。このような記録が見つからなかった場合は、該コピーが、分配されたディスクのリストにないディスクを用いて作成されたコピーであることが決定される。よってプロセスは終了される。対応する記録が発見された場合には、コントロールは、ステップ１５０４に移る。ステップ１５０４においては、対応する記録からクライアントの情報が読み取られる。コンテンツの所有者は、この情報を用いて、少なくとも１つの不正コピーの元となった正規のコピーを受け取った人物を特定する。

【０１０１】
図１６は、コンテンツを不正コピーから保護することを希望するコンテンツの所有者が本発明のコピー防止システムを用いる方法を示す。図１３に示すごとく、コンテンツの所有者は、予め焼かれた情報を有するディスクを用いる。これらのディスクは、図１６においては、アイテム１６００として示される。これらディスクには、コピー防止コンテンツ（１６０１）が記録される。焼きこみソフトウェア（１６０２）は、図１２Ａに示す暗号化プロセスを用いて、保護されるべきファイルを各ディスクに書き込む前に暗号化する。ソフトウェアはまた、コンテンツの所有者がトラッキング情報（追跡情報）とともにリストを管理することを希望する場合には、図１４に示すプロセスを用いる。保護されるべきファイル（コンテンツ）が、プログラム・ファイルであるならば、プログラム・ファイルには、図１０Ａ及び図１０Ｂに示す認証プロセスが組み込まれている。この認証プロセスは、ディスクがオリジナルか否かを決定する。この結果にしたがって、各プログラムの実行は終了されるか或いは継続される。保護されるべきファイルが、プログラム・ファイルではなくコンテンツ・ファイルである場合は、ファイルは、単に各ディスク（図１２Ａを用いて説明したごとく、第１プレギャップのトラック・ディスクリプション並びにカスタム情報、及びシリアル＃Ａ並びにシリアル＃Ｂ）からの既製の暗号化キーを用いて暗号化

される。このプロセスの結果として、ディスクに、暗号化されたコンテンツが書き込まれる。該暗号化されたコンテンツは、このプロセスの開始前には記録可能領域であった領域（図１３のフィールド１３０２）に書き込まれる。記録済みディスクの暗号化されたファイルを使用するためには、各ユーザは、コンテンツ保護ドライバがまだインストールされていない場合には、各自のコンピュータにコンテンツ保護ドライバをインストールしなければならない。コンテンツ保護ドライバは、コピー防止ファイルがプログラム・ファイルである場合には不要である。プログラム・ファイルは単独で認証プロセス及び解読ルーティンを実行可能であるためである。

【０１０２】

図１７は、概略図であり、仮想デジタル・ホログラム（Virtual Digital Hologram、ＶＤＨ）の構造を示す。ＶＤＨは、デジタル記憶メディアの認証に用いられる。記録メディアは、情報ブロック（セクタともいう）に分割されている。情報ブロックにより、記憶された情報を効率的に読み取ることが可能となる。各セクタは固有の識別アドレスを有する。この識別アドレスを用いると、特定のセクタにアクセスして、該セクタのコンテンツを読み取ることが可能となる。

【０１０３】

記憶メディアのＶＤＨセクションは、いくつかの連続的な情報ブロック（セクタ）からなる。この情報ブロックは、２つに分けられている。すなわち図１７のフィジカル・パート１及びフィジカル・パート２である。ＶＤＨの第１部分は、アドレスＲＢ１、ＲＢ１＋１・・・ＲＢ１＋４を有する情報ブロックを備える。ＶＤＨの第２部分はオーバーラップした情報ブロックの集合を備える。該第２部分の情報ブロックは、第１部分と同じＲＢ１、ＲＢ１＋１・・・ＲＢ１＋４とのアドレスを有する。情報ブロックのオーバーラップは、同一メディア上の、２つ若しくはそれ以上の情報ブロックが、同一の識別アドレスを共有することにより実現される。オーバーラップした情報ブロックは、同一のアドレスを有するが、該情報ブロックは異なる情報を備える。よって、オーバーラップした情報ブロックは、実際には、コンテンツによって区別可能なブロックである。ＶＤＨは、記録可能或いは記録不可能メディアにおいて使用可能である。ただし、該メディアは、固有の識別アドレスを有する情報ブロックに分割されていなければならない。

【０１０４】

例えばＣＤにおいては、ＣＤフレームのそれぞれが、アドレスを備え、該アドレスは３つの異なる場所に書き込まれている。３つの場所とはすなわち、Ｑサブ・チャネルのＡＴＩＭＥ並びにＲＴＩＭＥ（図４に示す）、及びヘッダ（図１のブロック１１２）である。ＣＤ上にＶＤＨを創出するためには、オーバーラップするＣＤフレームにおけるこれら３つの場所が、それぞれの識別アドレスを示すように変更されなければならない。

【０１０５】

ＶＤＨの２つの部分は、読み取り装置には、不安定な情報（例えば、仮想ブロック１乃至仮想ブロック４）を含む１つの仮想の部分として認識される。読み取りドライブがアプリケーションから、ＶＤＨ内で見つかった情報ブロックのコンテンツを読み取るようにとの要求を受信すると、該ドライブは、要求された情報のアドレスと適合するアドレスを備える２つの異なる情報ブロックを検知する。この場合、該ドライブは、該ドライブの読み取りヘッドの場所に物理的に最も近い情報ブロックにアクセスする。オーバーラップした情報ブロックと、読み取りヘッドの距離が大きいほど、該ドライブが最も近い情報ブロックを読み取る可能性が高くなる。この距離が小さい場合には、どの情報ブロックが読み取られるかは予測不可能となる。

【０１０６】

任意のデジタル・メディアのコピーを作成するには２つの基本的な操作が必要である。すなわち、ソース・メディアからの読み取りと、それに続くターゲット・メディアへの書き込みである。ＶＤＨを有する記憶メディアのコピーは必ず、ソース・メディアの有するＶＤＨを欠いている。読み取りプロセス中に、情報ブロックのそれぞれが読み取られたのち、ターゲット・メディアに書き込まれる。しかしながら、ＶＤＨが配される領域には、

情報ブロック（オーバーラップした複数のブロック）が２組ある。該オーバーラップしたブロックは１つのブロックとして認識される。この領域を読み取るとき、オーバーラップしたブロックの組ごとにただ１つのブロックが読み取られるとともに、ソースへ書き込まれる。結果として、ターゲット・メディアは、ＶＤＨ領域に読み取られた情報ブロックのみを備え、ソース・メディアのＶＤＨ領域のオーバーラップした情報ブロックを備えない。

【０１０７】

オーバーラップした情報ブロックのうちどのブロックがターゲット・メディアのＶＤＨ領域にコピーされるかを確実に知る方法はない。しかし、この領域の情報は必ず安定となる。つまり、アプリケーションがドライブにコピー・メディアの情報ブロックのコンテンツを読み取るように要求すると、ドライブの読み取りヘッドの場所に関わらず、いつも同一の情報ブロックが読み取られることとなる。

【０１０８】

図１８は、ＶＤＨを有するデジタル・メディアの認証プロセスを表す。この認証プロセスは、ＶＤＨ領域の情報ブロック（セクタ）の読み取りを２度試みる。１度は「前方に」（例えば、ＲＢ１から開始して、続いてＲＢ１＋１・・・ＲＢ１＋４を読み取り、ＲＢ２で終了するように）、１度は「後方に」（例えば、ＲＢ２から開始して、続いてＲＢ１＋４・・・ＲＢ１＋１を読み取り、ＲＢ１で終了するように）読み取りを試みる。

【０１０９】

ステップ１８００において、第１リセット・ブロック（ＲＢ１）が読み取られる。第１リセット・ブロックとは、ＶＤＨ領域の前の第１番目のセクタである。このセクタを読み取ると、ドライブの読み取りヘッドが、ＶＤＨの第１部分の開始場所に移動される。開始場所には、第１のオーバーラップしたセクタＲＢ１＋１が位置する。ステップ１８０１においては、次のセクタが読み取られる。次のセクタとは、第１のオーバーラップしたセクタＲＢ１＋１３である。ステップ１８０２においては、ステップ１８０１において読みとられた情報について、ＣＲＣコードが計算される。ＣＲＣコードは、コンピュータのメモリに格納される。ステップ１８０３においては、ステップ１８０１において読み取られたセクタが第１ブロックの最後のセクタ（すなわちＲＢ１＋４）であるか否かがチェックされる。読み取られたセクタが、第１部分の最後のセクタではないと決定されると、コントロールはステップ１８０１に移る。そうでない場合は、コントロールはステップ１８０４に移る。

【０１１０】

ステップ１８０４において、次のセクタ（すなわちＲＢ２（＝ＲＢ１＋５））が読み取られる。ステップ１８０５において、ＲＢ２より前のセクタ（例えばＲＢ１＋４）が読み取られ、ステップ１８０６において、ステップ１８０５において読み取られた情報について、ＣＲＣコードが計算される。ステップ１８０７において、ステップ１８０６において計算されたＣＲＣコードが、ステップ１８０２において同一のセクタ（例えばＲＢ１＋４）について計算されたＣＲＣと比較される。２つのコードが等しくない場合には、オーバーラップしたセクタのペアが検知されたと推測できる。なぜならば、２つの異なる読み取り操作において、同一のセクタ・アドレスから異なる情報が読み取られたからである。この場合、メディアがオリジナルであると結論され、プロセスは終了される。ステップ１８０７において比較されたＣＲＣコードが等しい場合には、コントロールはステップ１８０８に移る。

【０１１１】

ステップ１８０８において、ステップ１８０５において読み取られたセクタがＶＤＨの第１セクタ（ＲＢ１＋１）であるか否かがチェックされる。該セクタが、ＶＤＨの第１セクタであるＲＢ１＋１でない場合には、コントロールはステップ１８０５に移り、ＲＢ１＋１より前のセクタが処理される。そうでない場合、つまり第１セクタＲＢ１＋１が読み取られている場合には、オーバーラップしたセクタのペアが検知されなかったとみなされて、メディアがＶＤＨを備えないと結論される。よって、メディアはコピーと判断される

。
【図面の簡単な説明】
【０１１２】
【図１】ＣＤフレームのデータ構造を概略的に示す図である。
【図２】ＣＤセッション並びにトラックの構造を概略的に示す図である。
【図３】マルチ・セッション・レイアウトを概略的に示す図である。
【図４】Ｑサブ・チャネルのデータ構造を概略的に示す図である。
【図５】記録可能なＣＤの構造を示す図である。
【図６】リンク・ブロックの構造を示す図である。
【図７】ソニー（Sony）及びフィリップス（Phillips）サブコード・フォーマットを示す図である。
【図８Ａ】コンピュータ・オペレーティング・システム内のデータ・フローを示すブロック線図である。オペレーティング・システム内で、本発明のコンテント保護ドライバがインストールされている。
【図８Ｂ】本発明のコンテント保護ドライバのインストレーション・プロセスを示すフローチャートである。
【図８Ｃ】本発明のコンテント保護ドライバによって実行されるオペレーションを示すフローチャートである。
【図８Ｄ】本発明のコンテント保護ドライバによって実行されるオペレーションを示すフローチャートである。
【図９】ＣＤがオリジナルであるか否かを決定する方法を示すフローチャートである。この方法は、特徴的な識別マーク（IdentificatＩ／Ｏn Marks）を用いる。該識別マークは、任意の記録可能ディスク上に存在する。
【図１０Ａ】ＣＤがオリジナルであるか否かを決定する方法のフローチャートである。この方法は、意図的に埋設された論理的シンボルの有無並びにフォーマットをチェックすることにより行われる。
【図１０Ｂ】ＣＤがオリジナルであるか否かを決定する方法のフローチャートである。この方法は、意図的に埋設された論理的シンボルの有無並びにフォーマットをチェックすることにより行われる。
【図１１Ａ】暗号化手段により不正コピーからデジタル・コンテントを保護するための方法を示すフローチャートである。この方法は、本発明にしたがって予め焼かれた情報を備える記録可能なディスクを利用する。
【図１１Ｂ】保護されたデジタル・コンテントを解読するための方法を示すフローチャートである。該デジタル・コンテントは、本発明によって予め焼かれた情報を備える記録可能なディスク上に格納されている。
【図１２Ａ】標準型記録可能ディスク上のデジタル・コンテントを、不正コピー並びに不正コピー品の使用から保護するための方法を示すフローチャートである。この方法は、暗号化の手段を用いる。
【図１２Ｂ】保護されたデジタル・コンテントを解読するための方法を示すフローチャートである。このデジタル・コンテントは、標準型記録可能ディスク上に格納されている。そして、図１２Ａ内で示されるプロセスを用いて保護されている。
【図１３Ａ】記録可能なディスクのレイアウトを概略的に示す図である。該記録可能なディスクは、予め焼かれた情報を備える。該情報は意図的に埋め込まれた論理的シンボル並びにシリアル・ナンバを備える。
【図１３Ｂ】予め焼かれた情報の構造を概略的に示す図である。該情報は、図１３Ａを用いて説明されたディスク上に記録されている。
【図１４】コンテント・マネージメントを追跡し、不正コピー並びにその使用からデジタル・コンテントを暗号化手段により保護する方法を示すフローチャートである。この方法は、特徴的なシリアル・ナンバを備える記録可能ディスクを用いて行われる。
【図１５】デジタル・コンテントの不正なコピー品を作る著作権侵害品をトラックする方

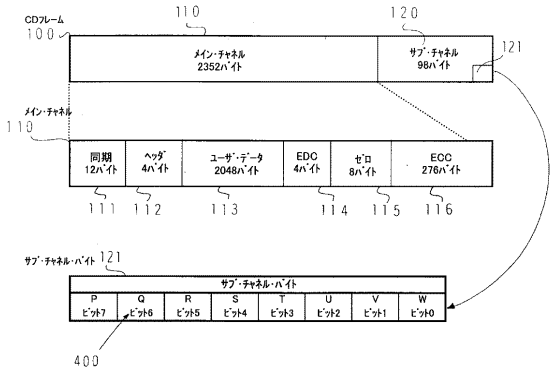
法を示すフローチャートである。該デジタル・コンテントは特徴的なシリアル・ナンバを有する記録可能ディスク上に格納される。

【図１６】本発明の使用を概略的に示す図である。任意のコンテント所有者が不正コピーからコンテントを保護する使用形態を示す。

【図１７】本発明の実施形態の仮想デジタル・ホログラム（Virtual Digital Hologram）の構造を示すブロック線図である。

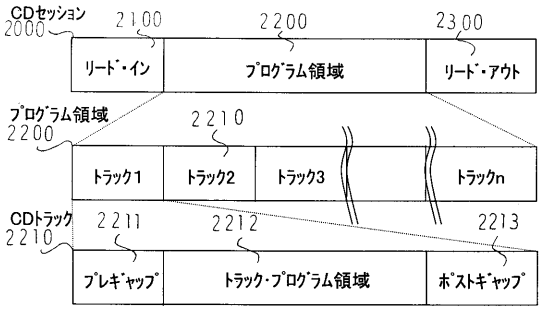
【図１８】記録メディアを認証するプロセスを示すフローチャートである。このプロセスは、本発明の仮想デジタル・ホログラムを利用する。

【図１】



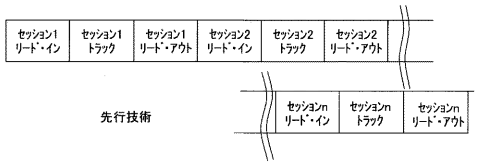
先行技術

【図２】



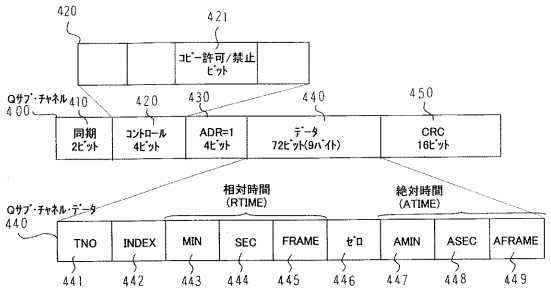
先行技術

【図３】



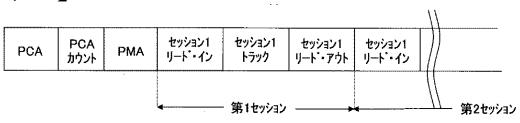
先行技術

【図４】



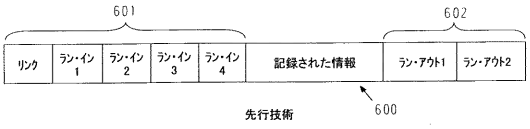
先行技術

【図５】



先行技術

【図６】



先行技術

【図７】

ソニー サブコード・フォーマット

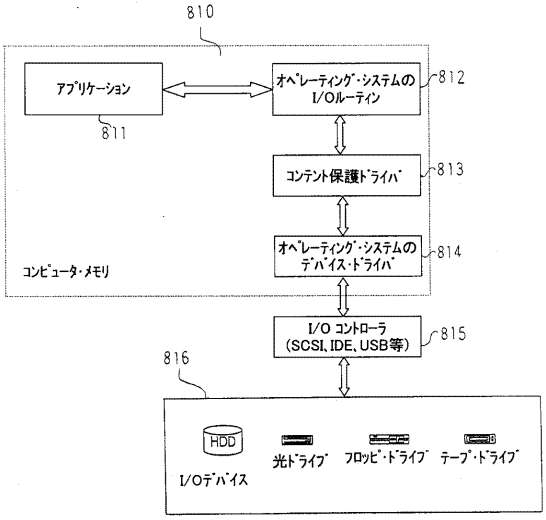
トラック	インデックス	ATIME	RTIME	Pチャネル
01	00	00:01:71	00:00:03	1
01	00	00:01:72	00:00:02	1
01	00	00:01:73	00:00:01	1
01	00	00:01:74	00:00:00	1
01	01	00:02:00	00:00:00	1
01	01	00:02:01	00:00:01	0
01	01	00:02:02	00:00:02	0
01	01	00:02:03	00:00:03	0
01	01	00:02:04	00:00:04	0

フィリップス サブコード・フォーマット

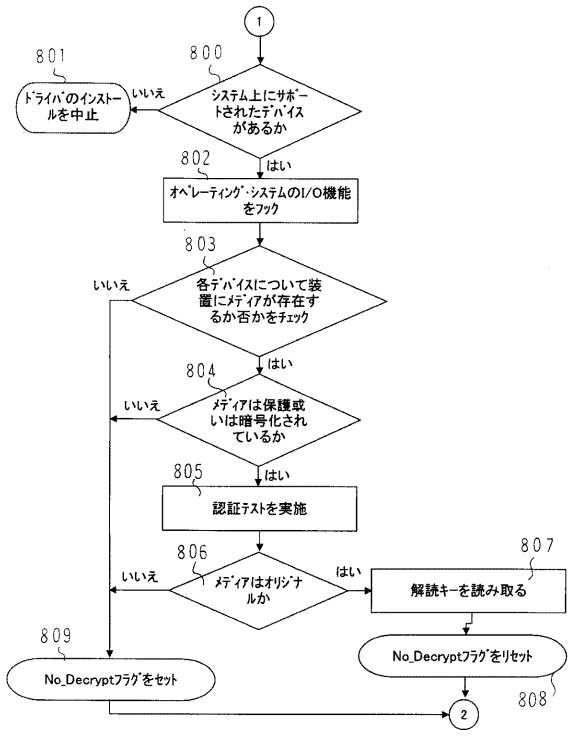
トラック	インデックス	ATIME	RTIME	Pチャネル
01	00	00:01:71	00:00:04	1
01	00	00:01:72	00:00:03	1
01	00	00:01:73	00:00:02	1
01	00	00:01:74	00:00:01	1
01	01	00:02:00	00:00:00	1
01	01	00:02:01	00:00:01	0
01	01	00:02:02	00:00:02	0
01	01	00:02:03	00:00:03	0
01	01	00:02:04	00:00:04	0

先行技術

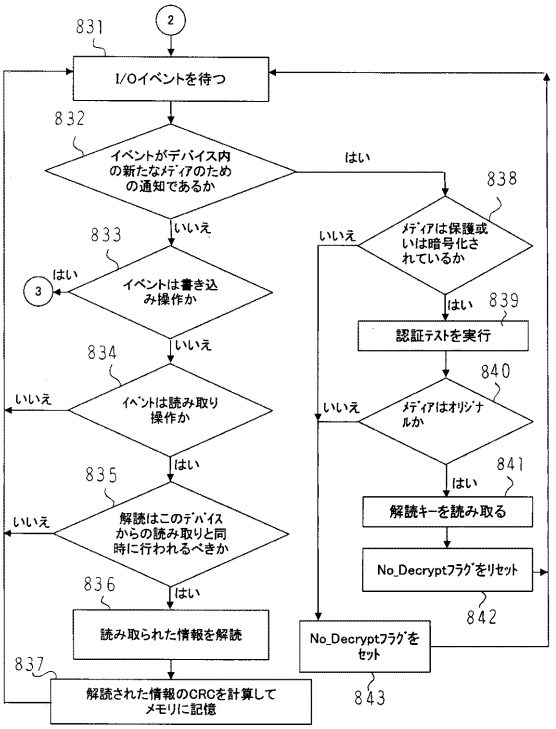
【図８Ａ】



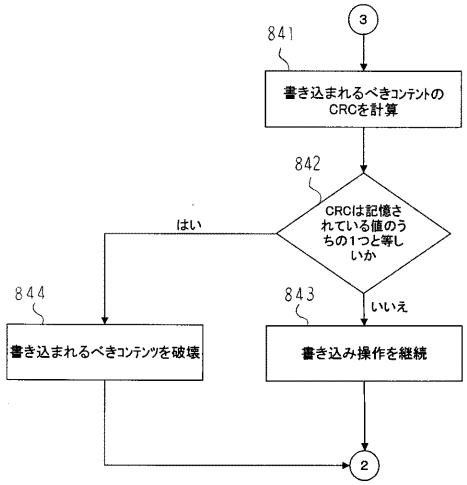
【図８Ｂ】



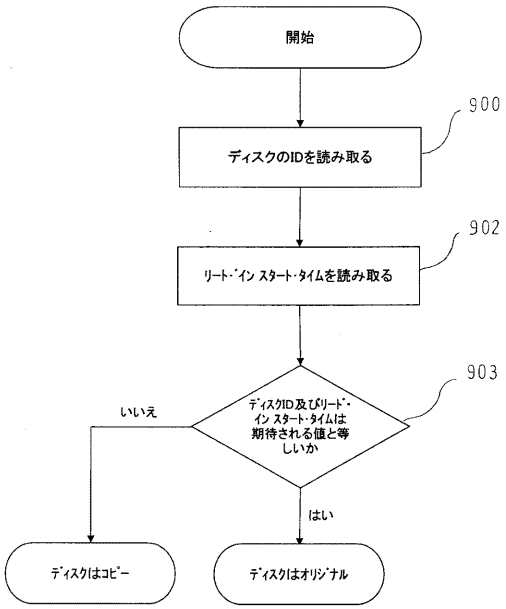
【図８Ｃ】



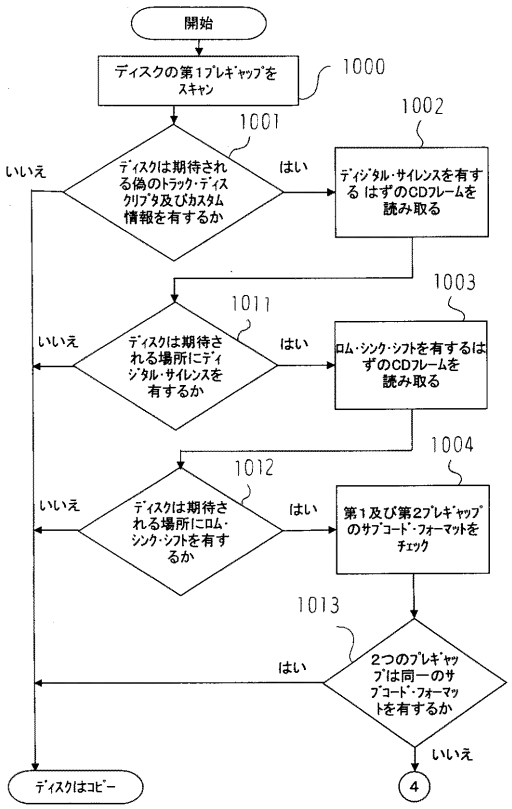
【図８Ｄ】



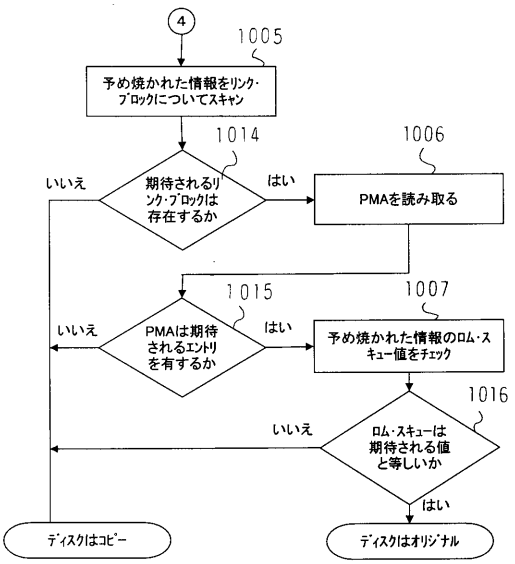
【図９】



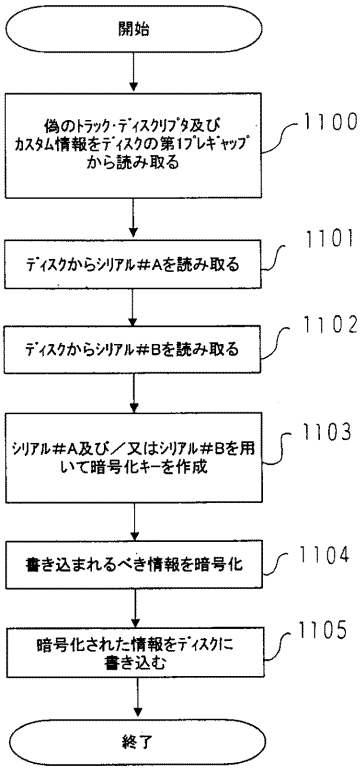
【図１０Ａ】



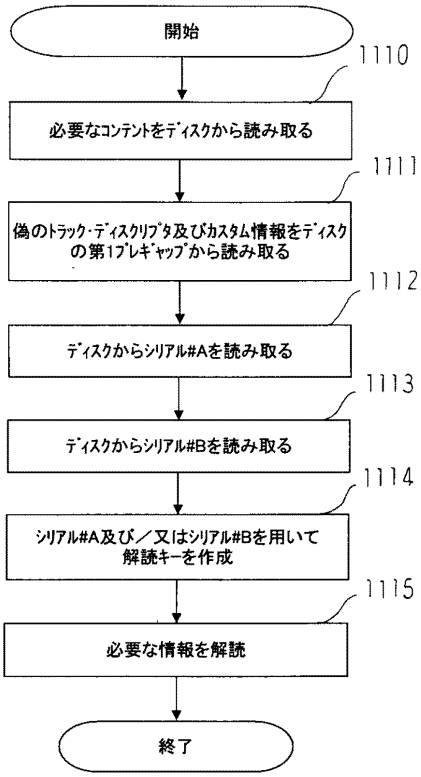
【図１０Ｂ】



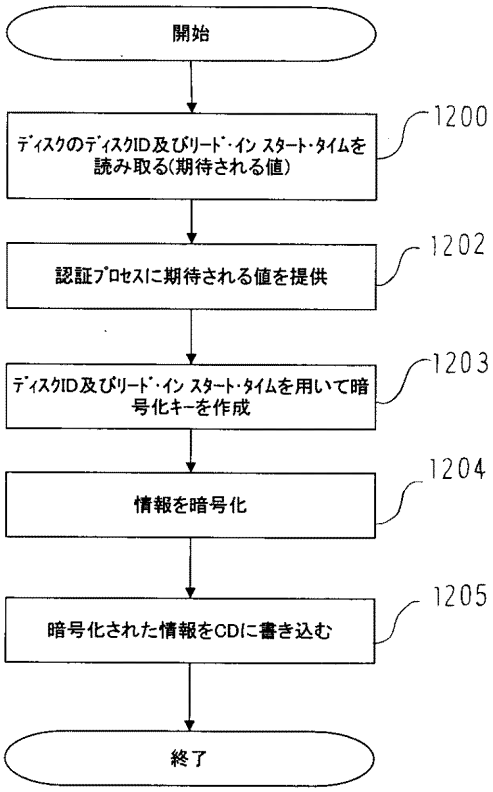
【図１１Ａ】



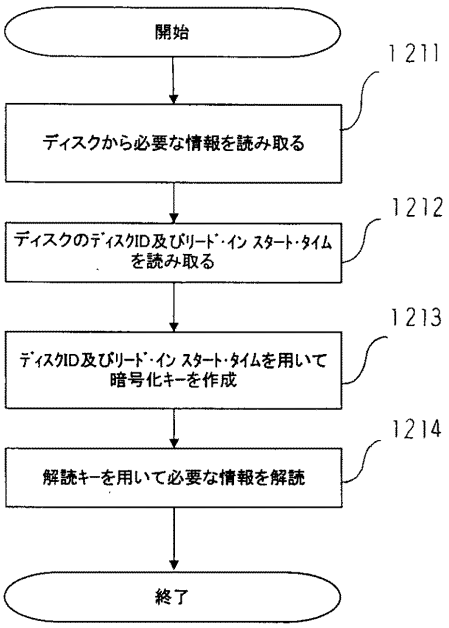
【図１１Ｂ】



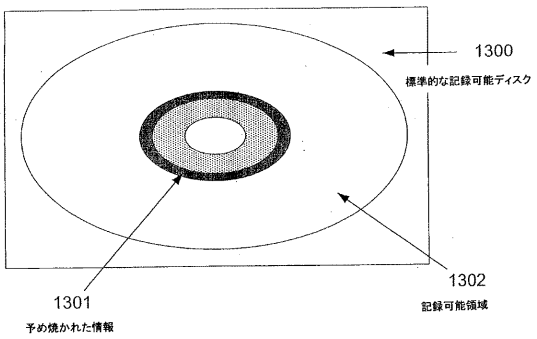
【図１２Ａ】



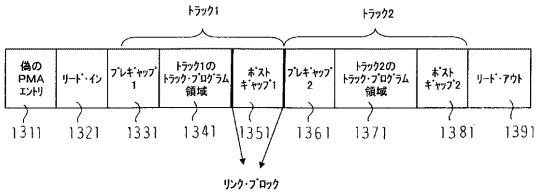
【図１２Ｂ】



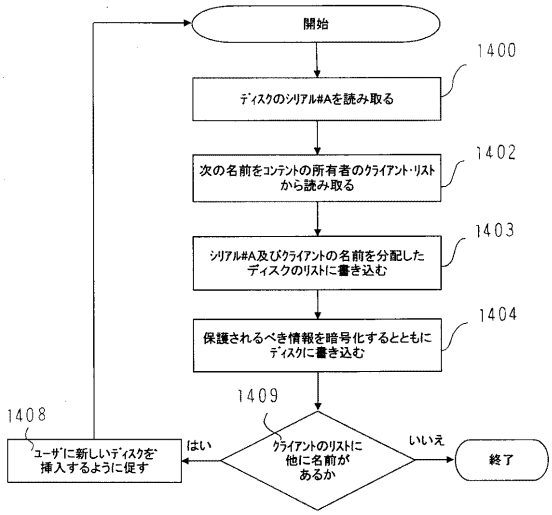
【図１３Ａ】



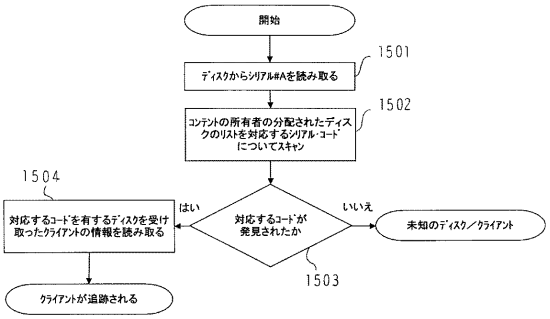
【図１３Ｂ】



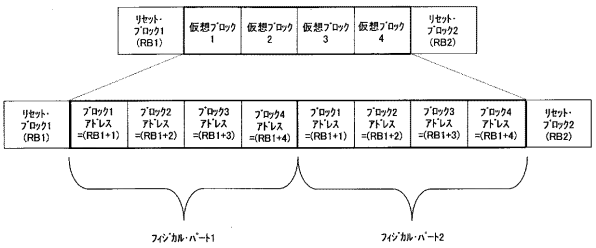
【図１４】



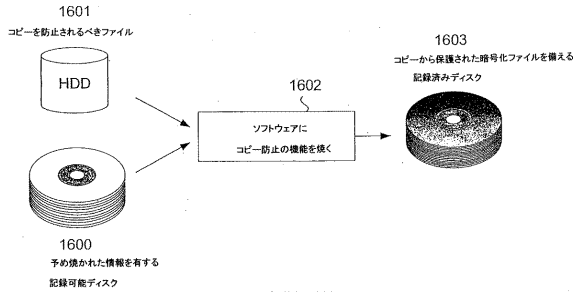
【図１５】



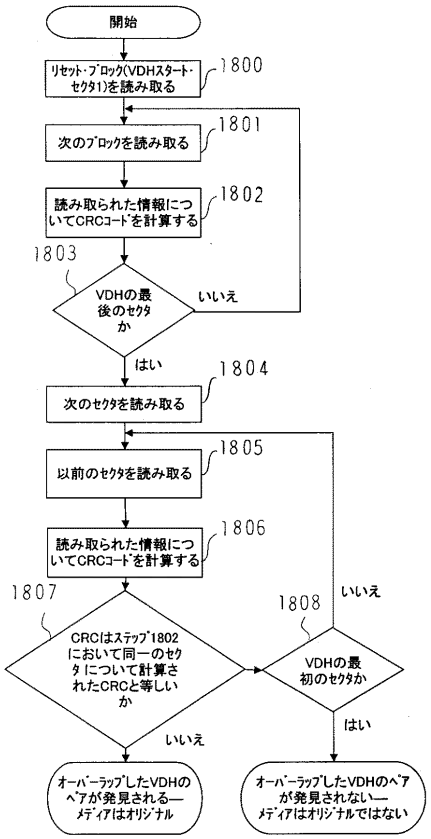
【図１７】



【図１６】



【図１８】


開始
リセット・ブロック(VDHスタート・セクタ1)を読み取る
1800
次のブロックを読み取る
1801
読み取られた情報についてCRCコードを計算する
1802
1803
VDHの最後のセクタか
いいえ
はい
次のセクタを読み取る
1804
以前のセクタを読み取る
1805
読み取られた情報についてCRCコードを計算する
1806
1807
CRCはステップ1802において同一のセクタについて計算されたCRCと等しいか
1808
VDHの最初のセクタか
いいえ
はい
オーバーラップしたVDHのペアが発見される—メディアはオリジナル
オーバーラップしたVDHのペアが発見されない—メディアはオリジナルではない

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL2004/000120

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F3/06 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/023225 A1 (LOMNES RANDY KEITH) 21 February 2002 (2002-02-21) abstract paragraph [0009] - paragraph [0015] paragraph [0038] - paragraph [0039] -----	1
A	WO 02/093334 A (SYMANTEC CORP) 21 November 2002 (2002-11-21) paragraph [0050] paragraph [0057] - paragraph [0062] -----	1
A	EP 0 769 745 A (SUN MICROSYSTEMS INC) 23 April 1997 (1997-04-23) page 1, line 33 - line 50 page 4, line 57 ----- -/--	1,5

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 January 2005	12. 11. 2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL2004/000120

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 699 428 A (GRAWROCK DAVID ET AL) 16 December 1997 (1997-12-16) column 3, line 59 - column 4, line 22 -----	1-4
A	EP 1 079 297 A (EMC CORP) 28 February 2001 (2001-02-28) paragraph [0012] - paragraph [0013] column 6, line 5 - line 12 paragraph [0031] paragraph [0038] -----	1,5

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2004/000120

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-5

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/ IL2004/ 000120

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-5

problem: providing the OS of a computer with the ability to transparently read content from a medium and block any copying attempt
solution: hooking driver checking legality of medium and matching of CRCs

---

2. claim: 6 7

problem: efficiently encrypting data on the medium
solution: encrypt the data with a key based on the disc ID and the Lead-In start time

---

3. claims: 8-15 17-26

problem: determining the authenticity of the medium
solution: detecting the presence of voluntarily introduced non-standard structures

---

4. claim: 16

problem: preventing the same process from reading and writing data from/onto the medium
solution: flag set to ON upon reading blocks any writing attempts

---

5. claims: 27-29

problem: disrupting copying attempts with unstable information
solution: creating two groups of sectors having the very same addresses but containing different data

---

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IL2004/000120

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002023225 A1	21-02-2002	NONE	
WO 02093334 A	21-11-2002	WO 02093334 A2	21-11-2002
		US 2003088680 A1	08-05-2003
EP 0769745 A	23-04-1997	US 5809303 A	15-09-1998
		DE 69601150 D1	28-01-1999
		DE 69601150 T2	22-07-1999
		EP 0769745 A1	23-04-1997
		JP 9160859 A	20-06-1997
		US 2001039597 A1	08-11-2001
US 5699428 A	16-12-1997	CA 2242876 A1	24-07-1997
		EP 1008249 A1	14-06-2000
		WO 9726736 A1	24-07-1997
		US 5796825 A	18-08-1998
EP 1079297 A	28-02-2001	US 6629199 B1	30-09-2003
		EP 1079297 A2	28-02-2001
		JP 2001195197 A	19-07-2001

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

【要約の続き】

テム内にドライバをインストールする段階を備える。ドライバは、オペレーティング・システムのデバイス・ドライバにアクセスしようとするオペレーティング・システムのＩ／Ｏルーティンの試行を遮ることが可能である。またＣＲＣコードを作成する段階を備える。ＣＲＣコードは、デバイスから読み取られたデータに対して作成される。尚、このデータは、オリジナル・コピーを備える。更に、デバイスに書き込まれたデータに対してのＣＲＣコードが作成される。作成されたＣＲＣコードが、読み取られたデータに対して作成されたＣＲＣコードに一致するならば、そのようなデータの書き込み試行は妨げられる。

記録可能ＣＤに格納されたコンテントの保護は、ＣＤ上に第１セッションを書き込むことにより行われる。第１セッションは１若しくはそれ以上のトラックを備え、該トラックそれぞれは、特徴的及び／又は非標準形式のデータ構造を備える。保護されたコンテントはその後ＣＤ上に隠蔽形式で書き込まれる。この書き込みにおいて、認証モジュールもともに書き込まれる。認証モジュールは、特徴的及び／又は非標準形式のデータ構造の有無を決定することができる。そして、隠蔽形式のコンテントにアクセスすることが可能である。また、それを解読することが可能である。ＣＤがアクセスされようとすると、認証モジュールは作動し、特徴的及び／又は非標準形式のデータ構造がＣＤ上で見つかれば、隠蔽されたコンテントが明らかになり、アクセス可能となる。