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

特許第4798935号
(P4798935)

(45)発行日　平成23年10月19日(2011.10.19)　(24)登録日　平成23年8月12日(2011.8.12)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	H
G06Q 50/00	(2006.01)	G11B	20/10	D
G06Q 30/00	(2006.01)	G11B	20/10	311
G09C 1/00	(2006.01)	G11B	20/10	321Z
G11B 20/12	(2006.01)	G06F	17/60	142

請求項の数 12　(全 30 頁)　最終頁に続く

(21)出願番号	特願2002-577675 (P2002-577675)
(86)(22)出願日	平成14年3月28日 (2002.3.28)
(65)公表番号	特表2004-532495 (P2004-532495A)
(43)公表日	平成16年10月21日 (2004.10.21)
(86)国際出願番号	PCT/US2002/010098
(87)国際公開番号	WO2002/079906
(87)国際公開日	平成14年10月10日 (2002.10.10)
審査請求日	平成16年12月7日 (2004.12.7)
審判番号	不服2009-9218 (P2009-9218/J1)
審判請求日	平成21年4月28日 (2009.4.28)
(31)優先権主張番号	60/279,323
(32)優先日	平成13年3月28日 (2001.3.28)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	10/113,363
(32)優先日	平成14年3月27日 (2002.3.27)
(33)優先権主張国	米国 (US)

(73)特許権者　597095197
ロヴィ・ソリューションズ・コーポレーション
アメリカ合衆国　カリフォルニア州　９５０５０　サンタクララ　デ・ラ・クルーズ・ブールバード　２８３０
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(72)発明者　ポール　シー．コッチャー
アメリカ合衆国　９４１１７　カリフォルニア州　サンフランシスコ　フィルモア　ストリート　１４３

最終頁に続く

(54)【発明の名称】長期にリニューアル可能なセキュリティを提供するコンテンツセキュリティ方法、その装置およびコンピュータ読取可能記憶媒体

(57)【特許請求の範囲】

【請求項１】

複数のプレーヤデバイスのうちの少なくとも１つでセキュアに再生するためデジタルビデオをマスタリングする方法において、

マスタリングシステムが、デジタルビデオを復号するための実行可能な命令と、前記デジタルビデオの圧縮され暗号化された表現とを組み合わせて、組み合わされた表現を形成するステップ

を備え、

前記デジタルビデオの圧縮され暗号化された表現は、前記デジタルビデオの複数の部分について、それぞれ、少なくとも２つのバージョンを含み、

前記実行可能な命令は、前記表現がプレーヤデバイスによって処理されるとき、

前記プレーヤデバイスの再生環境についての情報に基づいて、前記デジタルビデオの各部分について、前記少なくとも２つのバーションからどのバージョンを出力するかを前記プレーヤデバイスに指定し、

復号化され出力されたデジタルビデオ中に、前記プレーヤデバイスで利用可能なデータの少なくとも一部を含むウォーターマークを埋め込むように構成されている、

ことを特徴とする方法。

【請求項２】

請求項１において、前記プレーヤデバイスの再生環境についての情報は、前記プレーヤデバイスを一意に識別する情報を含むことを特徴とする方法。

【請求項３】
請求項１又は２において、前記実行可能な命令は、さらに、特定のプレーヤが認証されたプレーヤであるか否かを判断するように構成されていることを特徴とする方法。
【請求項４】
請求項１～３のいずれか１項において、前記実行可能な命令は、さらに、認証されていないプレーヤが前記デジタルビデオにアクセスすることを妨げるように構成されていることを特徴とする方法。
【請求項５】
請求項１～４のいずれか１項において、前記デジタルビデオは、少なくとも１つの復号キーを使用して復号化されることを特徴とする方法。
【請求項６】
請求項１～５のいずれか１項において、前記デジタルビデオは、前記プレーヤデバイスが当該デジタルビデオの各部分の少なくとも１つのバージョンを復号するために必要なキーを有しているように、オーサリングされることを特徴とする方法。
【請求項７】
デジタルコンテンツをマスタリングするシステムにおいて、
デジタルコンテンツを復号するための実行可能な命令と、前記デジタルコンテンツの圧縮され暗号化された表現とを組み合わせて、組み合わされた表現を形成する手段
を備え、
前記デジタルコンテンツの圧縮され暗号化された表現は、前記デジタルコンテンツの複数の部分について、それぞれ、少なくとも２つのバージョンを含み、
前記実行可能な命令は、前記表現がプレーヤデバイスによって処理されるとき、
前記プレーヤデバイスの再生環境についての情報に基づいて、前記デジタルビデオの各部分について、前記少なくとも２つのバーションからどのバージョンを出力するかを前記プレーヤデバイスに指定し、
復号化され出力されたデジタルコンテンツ中に、前記プレーヤデバイスで利用可能なデータの少なくとも一部を含むウォーターマークを埋め込むように構成されている、
ことを特徴とするシステム。
【請求項８】
請求項７において、前記プレーヤデバイスの再生環境についての情報は、前記プレーヤデバイスを一意に識別する情報を含むことを特徴とするシステム。
【請求項９】
請求項７又は８において、前記実行可能な命令は、さらに、特定のプレーヤが認証されたプレーヤであるか否かを判断するように構成されていることを特徴とするシステム。
【請求項１０】
請求項７～９のいずれか１項において、前記実行可能な命令は、さらに、認証されていないプレーヤが前記デジタルコンテンツにアクセスすることを妨げるように構成されていることを特徴とするシステム。
【請求項１１】
請求項７～１０のいずれか１項において、前記デジタルコンテンツは、少なくとも１つの復号キーを使用して復号化されることを特徴とするシステム。
【請求項１２】
請求項７～１１のいずれか１項において、前記デジタルコンテンツは、前記プレーヤデバイスが当該デジタルコンテンツの各部分の少なくとも１つのバージョンを復号するために必要なキーを有しているように、オーサリングされることを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、デジタルコンテンツの配信を、海賊行為その他の不正使用または不正再配信から保護することに関する。

【背景技術】
【０００２】
デジタルコンテンツを保護するため、種々のシステムが提案されてきた。このような保護スキームにおいては、ほとんどの場合、コンテンツが媒体に保存されるか、信頼できない通信チャネルを介して送信される間に、不正に使用されたりコピーされたりするのを防止するため、コンテンツが暗号化されている。そして、復号アルゴリズムおよびキーは、信頼できる耐タンパー性を有するソフトウェアまたはハードウェアモジュールであって、コンテンツの使用方法を指定するアクセスコントロールルール（このルールは固定のものでもよいし構成可能であってよい）を実施するように設計されたモジュールによって管理される。
【０００３】
コンテンツ保護スキームは、一般的に、特定の再生環境のためにカスタマイズされている。例えば、パーソナルコンピュータ用に設計されているソフトウェア専用ストリーミングコンテンツプレーヤの海賊行為対策システムは、耐タンパー性のあるハードウェアというセキュリティの恩恵には欠けるが、一般に、（例えば、ユーザが当該プレーヤをアンインストールして、製造業者のＷｅｂサイトから更新版をダウンロードするなど）容易にアップグレードすることができる。そうであるから、このようなシステムは、ロバストなセキュリティという点では、ハードウェアベースのプレーヤより劣るが、攻撃を受けたとしても、コンテンツストリームを修正したり、ユーザに自分のソフトウェアをアップグレードするように要請することにより、アップグレードされたセキュリティ機能を展開する（deploy）ことができるから、その攻撃の影響は比較的小さくなる。
【０００４】
これに対して、光媒体を再生するコンシューマ用電子ハードウェアデバイスに組み込まれた保護方法は、周知のように、アップグレードが困難である。セキュリティ上の課題としては、光媒体が長寿命であること（このため、後方互換性のないセキュリティアップグレードが阻害される）、プレーヤに更新版を配布するための簡便かつ信頼性のある方法がないこと、及びプレーヤの実装が標準化されていないこと、が挙げられる。これに加えて、再生装置の寿命が長いことや、新しいコンテンツはどれも旧式のプレーヤで再生できるというコンシューマの期待感から、セキュリティをアップグレードするのが極端に困難になっている。このため、ほとんどのコンシューマ向け電子デバイスでは、コピーに対する保護はほとんど行われないか全く行われておらず、コンシューマ向け電子デバイスにおいて整備されているわずかのコンテンツ保護標準は、柔軟性及び更新性に欠ける単純で柔軟性のないスキームとなる傾向にある。図１は、背景技術の典型的なコンテンツ保護システムを示す図である。コンテンツプレーヤ１００は、不揮発性プログラムメモリ１０５に、プレーヤのセキュリティポリシー１１０と、復号コード１２０と、プレーヤキー１３０とを実装するソフトウェアを含む。これらコードおよびキーは、媒体から読み取られたコンテンツ１５０が有効であるか否かを確認し、仮に有効である場合には、当該コンテンツを復号してその復号結果を出力インタフェース１６０に供給するため、プロセッサ１４０により使用される。図１に図示したような保護システムの例としては、デジタルオーディオテープで使用されるコピーコントロールスキームと、ＤＶＤビデオの保護のためのＣＳＳ（content scrambling system）と、ＤＶＤオーディオの保護のために提案されたＣＰＰＭスキームとが含まれる。
【０００５】
背景技術においては、次のような種々の異なる技法が知られている。
【０００６】
アクセス制限ポリシー：背景技術においては、多種多様なアクセスポリシーと、このようなポリシーを指定するための方法とが、知られている。例えば、特許文献１に開示されているソフトウェア保護システムは、制作者（publisher）によって発行された簡単な認証コードを使用している。これに対して、特許文献２には、莫大な数の参加者に関連する非常に複雑な種々のアクセスルールが記載されている。PolicyMakerやX.509の証明書フォ

ーマットといった、アクセスポリシーを符号化するための規格（これらは、コンテンツ配信その他のアプリケーションで使用される）も提案されている。

【０００７】

アンチウィルスソフトウェア：知られているウィルス、例えばトロイの木馬やその他の害意あるコードを検出しブロックする方法は、背景技術においては周知のものである。これらの方法には、一般的に、既知のウィルスの属性、例えば既知の命令シーケンスを、スキャンすることが含まれる。これらのプログラムは、種々の方法、例えば、スタートアップ時にファイルをスキャンする、ファイルをオンザフライ（on-the-fly）でスキャンする、プログラムの実行時にこれらプログラムをスキャンする、メモリをスキャンする、新しい媒体をスキャンする、ネットワーク通信をスキャンする、などの方法で機能させることができる。

【０００８】

コンテンツ保護システムおよびＤＲＭ：多種多様なコンテンツ保護システム（ＤＲＭ（digital rights management）システムともいう）が提案されてきた。背景技術に係るＤＲＭシステムは、一般に、コンテンツを暗号化形式で配信し、正当な購入者に対して、復号キーを供給するか、または復号処理を実行する。商用ＤＲＭには多くの機能が提案され、また含まれている。これらの機能としては、超流通（superdistribution）（暗号化されたコンテンツをユーザ間で交換できる）のサポート、従量制（pay-per-use）課金（通知が電話回線を介して行われるオフライン従量制を含む）、変動課金レート（プロモーション、使用回数または使用期間、要求されるユーザ処理、ユーザ履歴等に基づいて異なる金額が課される）、種々のデータタイプ（音声、映像、テキスト、ソフトウェア等）の保護、種々のフォーマットのサポート、種々の再生装置のタイプ（ポータブルタイプ、セットトップタイプ、ハードウェア支援のコンピュータベースのもの、ソフトウェア専用のもの等）のサポート、などがある。

【０００９】

コピー防止：パーソナルコンピュータ用ソフトウェアのコピーを防止する方法が知られており、ある種のソフトウェア、例えばコンピュータゲームのようなソフトウェアのために広範囲に展開されている。これらの方法においては、（例えば、エラーや複製困難な非標準のフォーマットを意図的に組み込むことで）コピーが困難になるように設計した物理媒体に、ソフトウェアプログラムをバインド（bind）することが、しばしば行われている。他のコピー防止システムには、例えば、ユーザに対してサーバから認証コードを取得するよう要求することにより、インストールプロセスを保護することが含まれる。コピー防止機能を設計段階でシステムに入れることがある。また、ほとんどのプレーヤで再生できるが、媒体をコピーしようとすると、ほとんどの場合に媒体コピーが正規に行えない非標準の符号化を媒体に行うことによりコピー防止を図る場合（コンピュータソフトウェア、ビデオカセットテープ、オーディオＣＤに使用されるコピー防止システムが含まれる）もある。コピー防止システムにおいては、その主な設計課題は、正当なユーザに及ぼす影響を最小にする（すなわち、高い確率で再生が可能で、ユーザに受け入れられる）一方で、望ましくないアクションをできる限り効果的に防止する（すなわち、良好なセキュリティを取得する）ことにある。

【００１０】

暗号化機能：多種多様な基本的な暗号化機能が知られており、例えば、ブロック暗号（block cipher）、ハッシュ機能、デジタル署名システム（およびその他のパブリックキーシステム）、キー管理システム等が知られている。基本的な暗号化技術についてより詳しくは、非特許文献１を参照されたい。

【００１１】

暗号オラクル（cryptographic oracle）：ブロック暗号その他の暗号化機能を使用すると、外部から供給される任意の入力メッセージに秘密の暗号変換を適用してその結果を戻す「暗号オラクル」を構築することができる。暗号オラクルは、オラクルのアルゴリズムおよびプロトコルを知っている攻撃者がオラクルのキーを決定することが計算上不可能と

なるように構築することができる。加えて、オラクルへ入力可能な入力数を莫大な数（例えば、２５６ビットのブロック暗号から構築されたオラクルにあっては、2^{256}）にすることができるので、攻撃者は、ランダムなクエリに対する応答を、予想できないし、事前に計算することができない。

【００１２】

インタプリタ、エミュレータ、およびバーチャルマシン：背景技術においては、種々のインタプリタ型コンピュータ言語（interpreted computer language）が知られている。インタプリタ型コンピュータ言語の中には、Ｊａｖａ（登録商標）のように、ソースコードを実行可能形式か解釈可能（interpretable）形式に変換するため、コンパイルプロセスが必要なものがある。これに対して、ほとんどのBASIC（登録商標）インタプリタは、ソースコードに対して直接処理を行うようになっている。インタプリタの中には、自己修正コードを許容するものもあるが、許容しないものもある。背景技術においては、インタプリタを実装するための技術も、アセンブリ言語をエミュレートするための技術も知られている。例えば、精巧なエミュレータ、例えば、Virtual PC（登録商標）およびSoftWindows（登録商標）は、Microsoft（登録商標）Windows（登録商標）やApple（登録商標）Mac（登録商標）コンピュータ用に設計されたプログラムを動作させることができる。ＶＭ（Virtual machine）設計、例えば、Ｊａｖａ（登録商標）およびJava（登録商標） Card用に使用される設計が知られており、ＶＭが、コンピュータ上のネイティブコード（native）とやりとりをしたり、異なるメモリ空間にある他のＶＭ機能を呼び出すことができることも知られている。（多くのＪａｖａ（登録商標）実装はこれらの機能を提供している。）インタプリタ型コンピュータ言語は、一般に、アプリケーションのために使用されるか、または、クロスプラットフォームの互換性が要求されるところにおいて、例えばプロセッサに依存しないデバイスドライバフォーマットを作成するために使用される。（例えば、非特許文献２参照。）

キー管理：暗号キーを割り当て、管理するための多種多様な方法が提案されている。デバイスは、デバイス専用キーと、グループキーと、パブリックキーと、プライベートキーと、証明書等を有することができることが知られている。キーは、例えば、個々のデバイス、選択されたデバイスグループ（例えば、特許文献３に記載されているようなもの）、全てのデバイス等に割り当てることができる。デバイスは、対称キー、（例えば証明書およびデジタル署名を認証するための）パブリックキー、非対称プライベートキー等を含む異なるタイプの種々のキーを含むことができる。

【００１３】

媒体：記憶容量が大きく、製造コストが低く、耐久性に優れた媒体を提供できる媒体技術が知られている。現在の媒体技術の例としては、光ディスク（ＣＤ、ＤＶＤ等）、磁気媒体、フラッシュメモリ、ＲＯＭがある。ホログラフィックメモリのような新しい技術も開発されている。単一の媒体が多くの異なるタイプのデータを含むことができることが知られている。例えば、ＣＤ（compact disc）は、標準のレッドブック（Red Book）オーディオトラックとともに、パーソナルコンピュータで使用するためのデータセッション（例えば、ソフトウェア、圧縮されたボーナストラック、イメージ、映像、歌詞等を含む）を含むことができる。パーソナルコンピュータで使用するためのＣＤは、暗号化されたコンテンツと、コンテンツの再生に必要な再生ソフトウェアとの両方を含むことができる。

【００１４】

ネットワーク通信：インターネットを含む高度なデータネットワークが知られている。これらのネットワークは、柔軟性があり、信頼できる、高帯域幅のデータ通信を提供することができる。物理接続を有するネットワークは、通常、より高い帯域幅を提供するが、ワイヤレス通信チャネルも広く普及している。

【００１５】

更新可能なセキュリティ：起こりうる攻撃を全て防御できると保証されたセキュリティシステムを作成することは、実際にはできないこともある。そこで、攻撃後に、例えば改ざんされたキーの使用を中止して脆弱性を修正し、これによりセキュリティを更新できる

ことが望ましい。セキュリティは更新可能であるのが望ましいが、展開され提案されているシステムの多くは、多種の攻撃から効果的に復旧するためのメカニズムがない。

【００１６】

サンドボクシング（sandboxing）：サンドボクシングとは、システムにダメージを与える可能性のある処理にソフトウェアプログラムがアクセスできないように制御された環境において、そのソフトウェアプログラムを実行することに関するものである。Ｊａｖａ（登録商標）「バーチャルマシン」は、（インターネットを介してダウンロードしたような）信頼できないアプレットを実行可能とするように、サンドボクシングをサポートしている。

【００１７】

セキュリティモジュール：多くのセキュリティシステムは、取り外し可能なセキュリティモジュールを採用しているため、当該システムの他の部分を置き換えるような手間や費用をかけずに、セキュリティのアップグレードを行うことができる。例えば、取り外し可能なセキュリティモジュールは、多くのペイＴＶ（television）システムで使用されている。

【００１８】

ソフトウェア更新：申し込まれたソフトウェア更新版を受け取り、この更新版を有効とするデジタル署名またはメッセージの認証コードを確認し、（当該署名が有効であれば）この更新版を実行することにより、セキュアなソフトウェア更新を行うことができる。例えば、デジタルオーディオプレーヤにあっては、コード更新版を受け取り、この更新版に付されたデジタル署名またはメッセージ認証コードを確認し、（もし有効であれば）それらのコードを更新できることが知られている。（例えばシーケンスカウンタを使用して）更新が正しい順序で適用されることを保証する方法や、（例えば、ソフトウェアの前のバージョンに戻るか、または特別な復旧コードを起動することによって）失敗または不成功の更新から復旧する方法も知られている。インターネット、光媒体、ＲＯＭカートリッジ等の種々の配信メカニズムを介して、ソフトウェア更新版をバーチャルに供給することができることも知られている。ソフトウェア更新版は、ペイＴＶの海賊行為を防止するのに使用されてきた。すなわち、デスクランブラにはコード更新版が信号とともに配信され、デスクランブラがこの新しいコードを適用し、正常に実行することで、次のビデオセグメントに対する正しい復号キーが計算される。通常、これら更新版は、未認証のデスクランブラを使用不能にするか、あるいはさらに破壊することで、不正な視聴を防止するために使用されている。

【００１９】

ステガノグラフィ：ステガノグラフィとは、情報をデータの中に隠すことに関するものである。例えば、暗号化されたデータを画像または音声録音の最下位ビットに配置できることが知られている。この画像または録音を取得したものの復号キーを知らない攻撃者は、データが隠されているか否かを判断すること自体が不可能となる。なぜなら、下位ビットはランダムに現れることが多く、復号キーなしでは、強力な暗号化アルゴリズムによって生成された暗号文をランダムなデータと区別することはできないからである。

【００２０】

耐タンパー性：耐攻撃性を有するデバイスを設計し構築する多くの方法が知られている。耐タンパー性を有するハードウェアは、攻撃者がデバイスのリバースエンジニアリングを行うことや、暗号化モジュールからキーを抽出することを防止することが望ましいシステムで、一般に使用される。例えば、Wave Systemsは、「Embassy」と呼ばれる耐タンパー性を有するマイクロプロセッサベースのＩＣ（integrated circuit）製品を販売しており、この製品はコンテンツプレーヤまたは汎用コンピュータと統合することができ、デジタルコンテンツ配信を保護するために使用することが宣伝されているものである。耐タンパー性を有するソフトウェアを実装する方法も提案されている（例えば、特許文献４参照）。

【００２１】

トレイタトレーシング（Traitor Tracing）：典型的には、未認証のデバイスで使用されたキーから、カスタマの特定のデバイスか、またはセキュリティ侵害が起きたデバイスまで遡って追跡することによって、セキュリティ侵害や攻撃の出所を特定するためのトレイタトレーシングスキームが提案されている。

【００２２】

ウォータマーキング：ウォータマークとは、コンテンツに埋め込まれた信号であって、専用の検出器によって検出できるが、コンテンツが再生されたとき、人間の知覚に影響を及ぼさない（又は、影響を及ぼしても最小限に止まる）信号をいう。写真、音声録音、画像に埋め込まれるウォータマークは、著作権者が、そのコピーが許可されていないことを示すために使用されてきた。（アナログ出力からの再レコーディングを含む）フォーマットの変換に対して耐性を有し、しかも、ウォータマークの除去を意図した攻撃に対してセキュリティ度の異なるセキュリティを提供することのできる「ロバストな」ウォータマークが知られている。これに対して、「脆弱な」ウォータマークは、フォーマット変換に対する耐性が小さいか全くないが、設計がより容易で、より多くの情報を伝えることができる。

【００２３】

起こりうる全ての攻撃を完全に防止できる海賊行為対策システムは存在しないものの、背景技術のシステムは、解決可能な問題、例えばデジタルからデジタルへのコピーや保護されたフォーマットから保護されていないフォーマットへの高速リッピングを利用して何気なく行われる海賊行為（casual piracy）に対して、現実的な解決方法を提供していない。背景技術の多くのシステムに存在する欠点としては以下のものがあげられるが、これらに限定されるものではない。

【００２４】

共通秘密に対する信頼：多くの保護システムは、暗号化アルゴリズム、キー、その他の復号に必要な情報が秘密裏に守られることを要する。そのため、復号プロセスをオープン（open）な標準文書にドキュメント化するには、当該システムのセキュリティを危険にさらさざるを得ない。また、莫大な数の実装が可能である場合には、攻撃者は、最も脆弱な実装を攻撃すれば、スキーム全体を破ることもできる。（このような攻撃は、最近、ＤＶＤビデオ保護システムで発生した。）このようなシステムは、単一ベンダの閉じた環境では有用であるが、標準化することはできず、長期にわたって効果的なセキュリティを提供するものではない。

【００２５】

標準化の欠如：コンテンツ制作者は、互換性のない種々のデータフォーマットおよび復号アルゴリズムに既に関与している。異なるコンテンツ保護システムが異なるビジネスモデルを可能としており、１つのモデルに関与している制作者が、異なるモデルを必要とするセキュリティシステムを妨害する可能性がある。

【００２６】

製品タイプによる不適合性：多くのセキュリティ機能は、全ての製品タイプに統合することができない。例えば、パーソナルコンピュータ用のダウンロード可能なソフトウェア専用プレーヤは、耐タンパー性を有するハードウェアを含むことができない。同様に、ソフトウェア更新が頻繁にあると、インターネットへの接続性に欠けるプレーヤへは、供給が困難になる。

【００２７】

ユーザインタフェース：多くの提案には、複雑なユーザインタフェースが含まれる。セキュリティは、害意のないユーザにとって不可視である方がよい。ユーザは、（例えば認証コードを取得するか入力する等の）明らかなユーザ関与を必要とするスキームを拒否する虞がある。一般に、コンシューマ用の電子装置、例えばカーステレオやビデオディスクプレーヤは、簡単に使用できなければならない。というのは、多くのユーザが、たとえ資料を読まなくても、テクノロジを怖がっていても、視力が弱いというようなハンディキャップがあっても、又はプレーヤのサポートする言語にたけていなくても、満足できなけれ

ばならないからである。

【００２８】

法的な課題：セキュリティシステムの中には、競合相手と協働することが必要なものもある。このような協働行為は、反トラスト法によれば、違法な行為に該当する可能性がある。

【００２９】

製造業者の利益の欠缺：製造業者は、プレーヤのコストや市場化までの時間を増大させたり、適法な機能を含めることを妨害したり、又はこれらの製品を非効率的で望ましくないものにしたりするセキュリティ機能には反対するであろう。半導体技術の進歩によって、セキュリティシステムの実装に必要なコストが削減されているが、効果的な耐タンパー性を有するハードウェアを設計したり製造したりすることは、依然として困難でコストがかかるものである。そのため、コンテンツ保護システムが、当該システムを良好に実施する上で製造業者に依存している場合には、よりセキュアなものを提供する製造業者を、実際の市場において優位に立たせない限り、これらコンテンツ保護システムは失敗に終わることになる。

【００３０】

不確定なセキュリティポリシー：効果的なセキュリティシステムは、ユーザが要求した特定のアクションを許可するか阻止するかを決定するための規則その他の意思決定手順を明確にしなければならない。これらの規則または手順が十分明確にされていないシステムが多い。

【００３１】

柔軟性のないセキュリティポリシー：コンテンツ保護システムは、異なる制作者、異なるコンテンツタイプ、異なる法的管轄権、異なる再生環境などに対する異なるモデルをサポートできるような柔軟性をもつことが望ましい。システムは、複雑になりすぎず、柔軟性を有するべきである。

【００３２】

長期にわたるセキュリティの脆弱性：セキュリティシステムは、セキュリティを長期にわたって維持できる程度に十分ロバストで、かつ柔軟でなければならない。背景技術のコンテンツ保護システムにあっては、ハイプロファイル（high-profile）フォーマットの一部として、数年間を超えて継続できるものはほとんどないが、一般に普及しているフォーマットは、３０年を超えて継続できる。

【００３３】

攻撃の追跡不能性：攻撃が発生した場合には、システムは、セキュリティ侵害が起きた（または悪用された）デバイスを取り消し、犯人を起訴できるように、攻撃源を特定できなければならない。

【００３４】

【特許文献１】米国特許第４６５８０９３号明細書
【特許文献２】米国特許第５９８２８９１号明細書
【特許文献３】米国特許第５５９２５５２号明細書
【特許文献４】米国特許第５８９２８９９号明細書
【特許文献５】米国特許第４４０５８２９号明細書
【特許文献６】米国特許第５６４０３０６号明細書
【非特許文献１】Applied Cryptography by Bruce Schneier
【非特許文献２】Writing FCode 2.x Programs, Sun Microsystems, 1993, page 5
【非特許文献３】A. Fiat and M. Naor, "Broadcast Encryption," Advances in Cryptology, Douglas Stinson, editor, p. 480; Springer Verlag, 1993

【発明の開示】

【発明が解決しようとする課題】

【００３５】

本願は、多種多様な相互利用可能なプラットフォームにおいて、柔軟で更新可能なコ

ンテンツ保護を提供するように実施できる、標準化可能なコンテンツ保護システムの種々の実施形態および態様に関する。

【課題を解決するための手段】

【００３６】

本発明は、参加者（製造業者、制作者、アーティスト、および／またはコンシューマなど）に対して、セキュリティおよび機能性に関する決定を行う上で、比類のない柔軟性を提供する。

【００３７】

本システムと共に使用可能な典型的なプレーヤ（すなわち、保護されているコンテンツを復号したりこれにアクセスしたりしようとするデバイス）は、幾つかのコンポーネントを含む。第１のものは、データまたは媒体入力インタフェース、例えば、光ディスクドライブの入力インタフェースである。再生を開始するためには、プレーヤは、この入力インタフェースから一連のデータ処理コマンドをロードし、インタプリタその他の実行モジュールを使用して、これらコマンドの実行を開始する。この実行環境にあっては、チューリング完全（Turing-Complete）な言語（プレーヤのメモリと、ユーザインタフェースと、性能限界の条件下で、任意のアルゴリズムを実行できる言語）を提供することが好ましい。この実行環境から、コンテンツは、プレーヤに対してクエリを実行して、再生環境の構成を決定し、当該プレーヤのキーを使用して暗号化処理を実行することができる。そのため、クエリに対する応答が条件を満たすプレーヤ上でのみ再生が進行するように、コンテンツを設計することが可能となる。制作者は、制限付き再生を提供することもできる。例えば、あまりセキュアに保護されていないプラットフォームで提供可能なのは、ＣＤ品質のステレオ音声や、通常精細のイメージであるが、よりセキュアに保護されているプラットフォームでは、より多くのオーディオチャネルと、より高精細のイメージと、より高いサンプリングレートと、より高品質な圧縮とを提供可能とすることができる。再生が開始された後であっても、再生を、コンテンツのデータ処理コマンドによるコントロールの下に維持することができる。例示的な一実施形態には、ロバストで、本質的にオンザフライ（on the fly）のウォータマーキングを実行する機能が含まれる。どのデータ領域を再生するかを、コンテンツ自体が制御できるようにすると、わずかに異なる出力データバージョンから選択することによって、出力に情報を埋め込むことが可能となる。これらの差異を分析すれば、特定のプレーヤまで遡って、海賊コピーを追跡することができる。

【００３８】

コンテンツがそれ自体のセキュリティポリシーを含み、それを実現するので、発生した攻撃については、耐性のある新しいコンテンツを設計し発行することで、対処することができる。コンテンツがそれ自体のセキュリティポリシーを実現できるようにすると柔軟性が得られ、それにより、アーティストの好み、地域的な「公正使用」規制などをサポートすることもできる。新しいプレーヤの機能の追加は、コンテンツがアクセス可能なプレーヤ機能を新たに追加することによって容易に行うことができる。

【００３９】

ビジネスの観点からは、どんなコンテンツ保護システムも、ビジネス及び運用上の制約と調和する最善のセキュリティを提供するという共通のゴールにコンテンツ制作者とコンシューマ用電子製品の製造業者とを結び付けるように使用できることが望ましい。

【００４０】

本明細書に開示されたシステムによれば、制作者は、自分自身のセキュリティ要件を決定することが可能であり、コンテンツそれ自体は、多種多様な要素を考慮し、それぞれの環境で再生するかどうか（または、どのように再生するか）を判定するポリシーを実行することができる。また、製造業者に対しては、自社の顧客がコンテンツに可能な限り広範囲にアクセスできるように優れたセキュリティを有し、海賊行為を容易にさせない製品を設計する動機付けを与えることができる。

【００４１】

詳細な説明

図２は、物理媒体２００を使用するプレーヤの例示的な実施形態を示す図である。再生プロセスは、媒体インタフェース２０５を介して媒体２００にアクセスできるプロセッサ２１０によって制御される。媒体２００がマウントされると（例えば、媒体が最初に挿入されたとき、またはシステムが再初期化されるとき、等）、プロセッサ２１０は、まず、媒体インタフェースを初期化し、媒体の目次を読み取り、サポートされている保護システムを認識する。そして、プロセッサは、媒体２００の小さいイニシャル部分（initial portion）を、実行・データＲＡＭ ２２０にロードする。

【００４２】

プロセッサ２１０は、インタプリタ２１５を使用して、このロードした媒体部分により指定されたデータ処理オペレーションの実行を開始する。インタプリタ２１５は、より複雑なタスクを実現できる所定のデータ処理オペレーションのセットを提供する。解釈された言語は、チューリング完全（Turing-Complete）であるのが好ましい。チューリング完全なプログラミング言語は、そのような言語の１つで実装可能なアルゴリズムが、そのような言語の他のどの言語でも実装可能であることを特徴とし、それらの実装は同様の漸近的な性能特性を有することになる。チューリング完全なプログラミング言語の例としては、Ｃ（登録商標）と、Ｃ＋＋（登録商標）と、ＢＡＳＩＣ（登録商標）と、Fortran（登録商標）と、Pascal（登録商標）と、Ｊａｖａ（登録商標）と、事実上全てのアセンブリ言語が含まれるが、これらに限定されるものではない。

【００４３】

ロードされた部分は、インタプリタ２１５によって提供されたプロシージャコールを起動して進行する。実行・データＲＡＭ ２２０にロードされた初期データは、相対的に小さくできるが、インタプリタ２１５上で実行中のコードは、プロシージャコールにより、媒体から追加のデータ（コードを含む）をロードすることができ、これにより、より複雑な処理を実行することができる。

【００４４】

他のプロシージャコールにより、コンテンツは、再生環境構成２２５を判断することができる。したがって、当該コンテンツは、再生環境の特性（例えば、プレーヤタイプ、要求されるユーザアクションなど）を分析して、再生を進行すべきかどうかを判断することができる。例示的な実施形態では、仮に修正可能な問題が検出された場合（例えば、当該媒体が、当該プレーヤ用のセキュリティファームウェアのアップグレードを含む場合）には、これらに対処することができる。サポートされている場合には、当該コンテンツは、出力インタフェース２５０に対してクエリを実行し、さらにサポートされている場合にはあて先プログラム／デバイス２６０（例えば、増幅器、デジタルスピーカ、スピーカドライバ等）に対してもクエリを実行して、セキュリティ特性をチェックし、暗号キーをロードし、出力パラメータを指定する（例えば、仮にセキュリティが確実でない場合には、劣化した出力品質を指定する）等を行うこともできる。例示的な実施形態においては、当該コンテンツは、暗号オラクル２３０に対してクエリを行うこともでき、そのようなオラクルはセキュリティハードウェアのアップグレードを可能にするため（スマートカードのような）外部リムーバブルセキュリティモジュール２３５に実装することが可能である。オラクルは、プロセッサ２１０、プレーヤ内のその他のハードウェア、媒体、スピーカのような接続されたデバイス、等々に実装することもできるが、これらに限定されるものではない。暗号オラクル２３０は、当該コンテンツに、プレーヤIDの検証可能な証明を提供することができる。オラクル２３０に対するクエリの結果は、後続のコンテンツまたはコード部分を復号化するのに使用することができ、これによって、有効キーのない（または、キーが取り消された）プレーヤにはコンテンツを復号できないという強力な暗号保証が提供される。

【００４５】

例示的な実施形態において、当該インタプリタは、コンテンツによって指定されたデータ処理コマンドを「サンドボックス（sandbox）」内で実行するが、これは、当該コンテンツが、当該プレーヤのセキュリティを損なう可能性のある（オラクルキーのような）

暗号秘密へアクセスしないことを意味する。サンドボクシングは、全てのコンテンツが必ずしも信頼できるとは限らない場合に、有用である。例えば、攻撃者は、プレーヤから暗号キーを抽出しようとする害意あるコンテンツの作成を試みる可能性がある。（典型的な暗号オラクルと、これら暗号オラクルの処理とに関する追加の情報については後述する。）

【００４６】

仮に当該コンテンツが再生を進行するべきでないと判断した場合（例えば、ユーザがコピーを作成しようとしているが、当該コンテンツが、コピーを禁止するように構成されている場合）には、当該コンテンツは、エラーを通知し、要求されたアクションを拒否する。あるいはまた、当該コンテンツは、レンダリングおよび／または出力処理を制御して、出力品質を劣化させ、不正コピーの品質を劣化させて興味をそぐようにすることができる。

【００４７】

仮に当該コンテンツが再生を進行するべきであると判断した場合には、当該コンテンツは、当該媒体上の特定の場所（例えば特定のトラック）から再生を開始するべきことを指定する当該プレーヤからの信号を待つ。インタプリタ２１５は、当該媒体がマウントされたときに実行・データＲＡＭ ２２０にロードされたデータ処理命令を使用して、当該要求を処理する。当該コンテンツが再生を進行するべきと判断した場合には、当該コンテンツは、プロシージャコールを使用して、媒体インタフェース２０５に、媒体２００上の適正な場所から、暗号化されたコンテンツのロードを開始するように指示する。当該コンテンツは、有効な復号キーおよびパラメータをバルク復号モジュール２４０に指定し、バルク復号モジュール２４０は、ＲＡＭ ２２０から（あるいは、媒体インタフェース２０５から直接）暗号化されたコンテンツを取り出し、取り出したコンテンツを復号する。そして、この復号されたコンテンツが出力インタフェース２５０に供給され、出力インタフェース２５０は、この復号されたコンテンツを、あて先プログラムまたはデバイス２６０において使用するため、適当なアナログまたはデジタルフォーマットに変換する。再生の進行中、インタプリタ２１５によって処理されているデータ処理命令は、新しい復号パラメータをロードしたり、媒体２００から読み取る新しいデータブロックを指定したりすることができる。再生が正常終了すると、当該コンテンツは、ＲＡＭ ２２０を再初期化することができる。

【００４８】

インタプリタ、再生システムその他の実施形態および態様に関し、以下のセクションでは、更なる情報を提供する。

【００４９】

攻撃への対処

海賊行為対策システムは、広く、ソフトウェアおよび低価格のコンシューマ用電子装置に実装されているが、起こりうる全ての攻撃を防止することはできない。ここに開示した技法は、攻撃があった後に、現在の攻撃を実質的に阻止するように新しいコンテンツをマスタリングすることを容易にするのに有用である。プロの海賊行為者は、引き続き新しい迂回システム（circumvention system）を探し出してインストールしようとするかもしれないが、これに対して、何気なく行われる海賊行為（casual piracy）においては、絶えず攻撃ツールを開発し維持しようとすることが必要となり、結果として、そのような海賊行為が単にコンテンツを適法に購入するよりも困難なことになることが期待される。次のセクションにおいては、いくつかの典型的な攻撃に対処するため、本明細書に記載された技法をどのように使用することができるかを説明する。

【００５０】

攻撃の第１のカテゴリには、セキュリティ侵害が起きていないプレーヤ（uncompromised players）を使用して不正な行為を行うことが含まれる。例えば、オリジナルの媒体からのコピーは可能であるが、コピーされたものからのコピーは不可能となるように、当該コンテンツをマスタリングすることができる。このようなコンテンツをコピーされたも

のから（当該コンテンツは、例えば、コピー処理中に挿入された変更箇所を検出するか、または現在の媒体のシリアル番号および／またはタイプをオリジナルのものと比較することによって、コピーであるかを認識できる）コピーしようとした場合、インタプリタコードによって、再生を阻止することができる。あるいはまた、当該インタプリタによれば、当該コンテンツは、（サンプルレートの高いマルチチャネル音声が利用可能であったとしても、４４．１ｋＨｚのサンプルレートで、ステレオ音声を再生するような）低忠実度で再生することができ、あるいは追加の海賊行為の警告（Anti-piracy warnings）を挿入して再生することができる。そこで、当該インタプリタに提供された情報を分析して、セキュリティ侵害が起きていないプレーヤからの不適正なユーザ要求を検出してこれに対処することができる。

【００５１】

攻撃の第２のカテゴリには、プレーヤの暗号キーを改ざんすることが含まれる。仮にプレーヤの暗号キーが改ざんされた場合には、攻撃者は、（少なくとも理論的には）、暗号オラクルをエミュレートし、（任意で）再生環境についてのクエリに偽って応答することにより、改ざんされた再生環境を完全にエミュレートすることができる。このような攻撃があった場合、以降のコンテンツにおいて解釈されるコードに、セキュリティ侵害が起きたデバイスに存在しなかった暗号キーを少なくとも１つ要求するようにすれば、セキュリティを再び確立することができる。（例えば、プレーヤに実装されたセキュリティが不充分なため）特定のプレーヤモデルまたは特定の製造業者が多くの攻撃の出所となっている場合には、制作者は、このようなプラットフォームでは再生されない（または品質を落として再生される）コンテンツを作成することができる。

【００５２】

攻撃の第３のカテゴリには、類似のインタプリタセキュリティコードを含む特定のコンテンツ部分、又はタイトルのグループが、セキュリティ侵害の対象となることが含まれる。このような攻撃は、セキュリティチェックを迂回するようにコンテンツ自体を修正するか、又はターゲットタイトルを再生するように調整された害意あるインタプリタを作成することにより、潜在的にマウントすることができる。このような攻撃には、以降のコンテンツには、異なるかまたは優れた保護ソフトウェアを備えることにより、対処することができる。

【００５３】

攻撃の第４のカテゴリには、コンテンツを、保護された媒体から保護されていないフォーマットにコピーして、当該コンテンツを、新しいフォーマットで再配信することが含まれる。どのコンテンツ保護システムであれこのような攻撃を完全に防止することはできないが、ここに開示した技法およびシステムは、セキュリティ侵害を追跡して特定のデバイスまで遡り、そのデバイスを取り消して以降の攻撃を防止できるようにするために使用可能な強力で柔軟なウォータマーキング機能を提供する。海賊行為のためにコンテンツを積極的にアップロードするユーザの数は比較的少ないから、これらユーザのプレーヤを識別して取り消すことにより、海賊行為を大幅に減少させることができる。暗号文の一部を選択的にスキップさせるようにすれば、知覚できないほどの差異を復号出力に導入することができる。例えば例示的な実施形態においては、当該コンテンツは、プレーヤの復号モジュールに命令して、第１の暗号文部分を復号して出力し、その後、第２の暗号文部分をスキップすることにより、「０」ビットのウォータマークを挿入することができる。「１」ビットのウォータマークを挿入するために、当該コンテンツは、モジュールに命令して、第１の暗号文部分をスキップして、第２の暗号文部分を出力するようにすることができる。このようなビットの列を符号化すれば、プレーヤＩＤ、暗号処理結果、ユーザアクションの記録、出力デバイス情報等々を含むがこれに限られない、インタプリタコードで利用可能なあらゆるデータを用いて、当該コンテンツにウォータマークを挿入することができる。仮に当該コンテンツの海賊コピーが発見された場合には、ウォータマークを分析して、この違法コピーを追跡してただ一つのプレーヤまで遡ることができるから、このプレーヤを以降のコンテンツリリースで取り消すことができる。この機能によれば、特定のコ

ピーが特定のプレーヤから発生したことを確実に証明することができるから、法執行や法廷において役立つ。違法コピーを作成しようと考える人は、突き止められ、逮捕され、起訴される可能性があるということを知れば、違法コピーの作成を思い止まることになるから、コピー追跡機能は、海賊行為の意欲をそぐものとしても機能する。

【００５４】

もちろん、あらゆる環境において、起こりうる全ての攻撃を確実に防止することのできる、ユーザが利用しやすい海賊行為対策システムはない。例えば、音声や映像はアナログ出力から録音録画することができる。（たとえコンテンツにウォータマークが埋め込まれていても、ウォータマーク検出器のないレコーダは利用可能である。）そして、アナログ出力から得られたデータを、新しいデジタル媒体またはアナログ媒体でリマスタリングし、オリジナルのセキュリティ機能を付けないで再配信することができる。同様に、媒体の厳密なコピーを作成する上で必要な機器を有するプロの海賊行為者が作成したコピーをプレーヤが検出することはできないが、本明細書に開示された技法およびシステムは、媒体のクローン作成を防止するのを助けることができる。例えば、媒体に付したディスク製造業者ＩＤをコンテンツごとにチェックすることで、海賊行為者によって正当なまたは不注意な複製設備が欺かれないように保証することが可能である。媒体タイプＩＤによれば、読み取り専用媒体で販売されたコンテンツが、書き込み可能媒体で再配信されるのを防止することができる。インターネット、電話／モデムその他のネットワークサポートを有するプレーヤにあっては、コンテンツは、再生（または最初の再生）前に、媒体が有効であることを認証するため、（例えば）サーバから認証を取得することができる。不揮発性のストレージを有するプレーヤは、既知の悪質媒体（known-bad media）のシリアル番号のテーブルを保存しておくことも可能で、コンテンツおよび／またはプレーヤは、これに対してクエリを実行し、媒体が取り消されている否かを判断することができる。

【００５５】

再生環境のクエリ及び制御

コンテンツを、当該コンテンツ自らが自らの復号を許可するかどうか判断するように構成することができる。この判断を支援するため、プレーヤは、再生環境についての情報をコンテンツに提供することができる。極めて限られた情報（例えば、ユーザの要求したアクションやプレーヤモデルなど）で充分である場合も多いかもしれないが、当該コンテンツが再生を進行するべきか否かに関してより十分な情報を得た上で評価（more informed assessment）を行えるように、より詳細で正確な情報が望まれる。どのような情報や機能がコンテンツに提供されるかは、プレーヤの実装に依存する。次に、コンテンツに提供できるいくつかの例示的な機能および能力について説明する（がこれらに限定されるものではない）。次の点に留意されたい。すなわち、複数の接続された構成要素（例えば、出力ポート、接続された出力デバイス、オペレーティングシステムデバイスドライバ、セキュリティモジュール等）から構築されたプレーヤにあっては、以下の情報の一部または全部を、これらの接続されたデバイスに提供することができ、同様に、インタプリタを含むプレーヤの主部分に提供することができる。

【００５６】

セキュリティサポート情報：セキュリティ仕様バージョン、サポートされたクエリ機能、および／またはセキュリティモジュールのフォームファクタ（交換可能ハードウェア、組込みハードウェア、更新可能ファームウェア、ＲＯＭファームウェア、ＰＣソフトウェアなど）など。（例示的な暗号処理機能および再生制御／復号機能については、次に詳細に述べる。）

【００５７】

製造業者情報：名称、ＩＤ、Ｗｅｂサイト、パブリックキー／証明書、製造バッチ、製造日時、製造地域、製造国、製造業者住所、技術サポート問合せ先情報、および／または製造業者保証情報等。

【００５８】

デバイス情報：製造ライン、製造番号、モデル番号、ファームウェア／ソフトウェア

バージョン、デバイスパブリックキー／証明書ＩＤ、ＧＰＳ位置その他の物理位置／地域、コンテンツサポートＣｏｄｅｃタイプ、ネットワーク／インターネットサポート情報、ネットワークアドレス、デバイス電話番号、ＩＰアドレス、ウォータマークサポート、インタプリタ性能定格、セキュリティ証明定格、デバイス販売代理店、デバイス小売店、デバイスのフォームファクタ、および／またはセキュリティ仕様等。

【００５９】

ユーザ情報：ユーザ名、地理的地域、国、住所、ＧＰＳ位置その他の物理位置／地域／国等、ユーザ電話番号、ＩＰアドレス、e-mailアドレス、Ｗｅｂアドレス、優先使用言語、問題のある素材（controversial material）に関する許容範囲、優先使用支払方法／口座、支払限度、購買履歴、および／またはプライバシーの基本設定等。

【００６０】

媒体制御：クエリメディアフォーマット、書込み可能／不能の別、媒体製造番号、レコーディングデバイスタイプ、レコーディングデバイス所有者、レコーディングデバイス製造番号、レコーディングデバイスセキュリティ情報、および／またはレコーディングデバイスウォータマークチェック機能等。機能により、媒体からの読み取り、媒体への書き込み、媒体のフォーマット、媒体のテスト、および／または媒体の取り出しもできる。追加の機能により、特定の媒体フォーマットによりサポートされている暗号化機能その他の特殊機能にアクセスすることができる。

【００６１】

要求されたユーザ処理：例えば、再生、録画録音、新しいフォーマットへの変換、ポータブルデバイスへのロード、初回コピーの作成、複数コピーの作成、および／または同時再生／録画録音等。コンテンツには、要求された処理を開始または修正する機能を与えることもできる。

【００６２】

出力情報：出力ポート、出力ポート構成、出力ポートのセキュリティ特性、接続されたデバイス、出力データフォーマット、および／または出力データ品質／解像度等に関する情報。サポートされている場合には、コンテンツは出力デバイスに直接クエリを実行して、デバイスに関する追加情報を取得し、かつ／または暗号処理を要求したりすることができる。プレーヤは、例えば、セキュリティが不充分な場合に、品質の劣化した出力を指定するため、コンテンツがこれらのパラメータを修正できるようにすることもできる。

【００６３】

環境：当該プラットフォーム上で動作している他のプログラムおよびデバイスドライバのＩＤ／ハッシュ／バージョン、メモリの内容またはハッシュ、インストールされた攻撃検出モジュールのバージョン、攻撃に関するシステムスキャンの結果、および／またはタンパー検出器のステータス等。これらの機能によれば、例えば他のプログラムのセキュリティの弱点を修正するため、当該コンテンツは、メモリを修正することもできる。

【００６４】

タイム：日付、時刻、時間帯、経過したクロックサイクルカウント、最終リセットからの時間、製造からの時間、最終セキュリティアップグレードからの時間、最終バッテリ交換からの時間、および／または推定バッテリ残存寿命、等。

【００６５】

接続性：プレーヤの通信機能の判断、現在の接続状況のチェック、ネットワーク接続の確立、モデム接続の確立、ネットワーク接続確立の重要度の指定、接続のセキュリ特性のチェック／指定、データの送信、データの受信、接続の終了、および／または接続の一次休止等。

【００６６】

ユーザインタフェース：ユーザメッセージの表示、歌詞の表示、グラフィックイメージの表示、グラフィックイメージの印刷、広告／プロモーションメッセージの表示、利用可能なユーザインタフェースコントロールの識別、ユーザ入力の取得、プレーヤの音声合成装置を使用したユーザへの音声再生、および／またはエラー通知等。

【００６７】
ウォータマーク制御：出力するコンテンツ領域の選択、外部ウォータマーキングアルゴリズムの選択、外部ウォータマーク検出器の制御、および／またはマーク検出器ステータスのチェック等。
【００６８】
その他：プレーヤ／再生のステータス情報、従量制課金の管理（例えばプレーヤベースの資金源）、エラー処理、再生終了、セキュアな不揮発性メモリサポート（以下を参照）、プレーヤファームウェア更新の適用、および／または外部モジュール（動的にリンクされたライブラリ等）の起動、等。
【００６９】
機能およびパラメータの標準化の中には、（例えば、コンテンツが最初に発表された後で設計されたプレーヤ環境でも当該コンテンツが有効に機能できるように）複数の実装間での相互利用可能性を保証し、セキュアなコンテンツをオーサリングするタスクを簡略化するために有用なものがある。標準化は、種々の異なる製造業者の製品が同じタイプの情報または処理を提供しなければならない機能において、特に有用である。例えば、コンテンツが、プレーヤのフォームファクタ（家庭用オーディオ／ビデオ、ポータブル、自動車用、パーソナルコンピュータソフトウェア専用、ハードウェア支援付きパーソナルコンピュータソフトウェア、プロ用スタジオ、映画劇場等）を判断できるようにするための機能および応答コードは、標準化することができる。標準化による利点としては、関連するリスクに関係する情報を、既存のコンテンツが理解できない非標準フォーマットで通知することにより、製造業者がセキュリティコントロールを回避しようとするのを防止するという利点もある。
【００７０】
もちろん、本システムは、コンテンツ制作者が独自の（proprietary）追加機能を選択して使用することができるようにするため、製造業者がそのような独自機能を追加できるように構成することもできる。新しい機能を追加可能であることは、自社の製品に新しい機能を追加しようとする製造業者にとって特に価値のあることである。というのは、これら製造業者は、そうした新しい機能を追加し、しかも、その機能をサポートするため、コンテンツ制作者とビジネス上の協調関係を確立することができるからである。このような実施形態は、（必要であれば）後方互換性を維持しながら、容易に拡張することができる。
【００７１】
製造業者は、正確な情報をコンテンツに提供する責務がある。コンテンツは、一般に、当該コンテンツが受け取った情報の大部分について、それが正確か否かを直接検証することはできないが、この情報が正しいことを保証する強力な動機付けが製造業者にある場合には、このような検証は厳密には必要でない。例えば、制作者は、今後制作するコンテンツが不誠実な製造業者によって作られた製品で再生されるのを防止することができる。
【００７２】
プレーヤがコンテンツに提供する情報の暗号認証を、（例えば、保証されたプレーヤまたは製造業者キーを使用して発行されたデジタル署名を含めることにより）プレーヤ自身が提供すれば有益であるが、このような認証は大部分のデータにとって必須のものではない。出力デバイス（例えば、高品質のデジタルオーディオデータを必要とするデジタルスピーカ）、又は潜在的に信頼できないインタフェースを介して接続されているシステムの他の部分にあっては、信頼できるデバイスを装った害意あるデバイスを検出して回避するために、暗号認証はより重要となる。
【００７３】
暗号化処理
例示的なプレーヤは、再生環境を記述した情報を提供することに加えて、コンテンツが起動することができる暗号化処理も実装している。この処理は、暗号オラクルと同様に振舞うことができ、コンテンツに入力データ（例えば、６４ビットの平文ブロック）を供

給させ、暗号化計算の結果を戻す。例示的な実施形態においては、暗号化計算への入力には、少なくともキー（その値は通常は未知であり、当該コンテンツはアクセスできない）と、コンテンツに指定された入力データとが含まれる。

【００７４】

以下は、再生環境を認証したり、コンテンツ復号キーを取り出したりする等の用途のために、当該コンテンツに提供することができる暗号化の基本要素の例であるが、上記用途は上記例に限定されるものではなく、暗号化の基本要素も以下に限定されるものではない。

【００７５】

ブロック暗号オラクル：当該オラクルは、秘密キーを使用して入力メッセージを暗号化（または復号）して、暗号文（または平文）という結果を得る。

【００７６】

ハッシュ関数オラクル：入力メッセージを、典型的には秘密キーで（例えば、ＨＭＡＣ－ＳＨＡのようなアルゴリズムを使用して）ハッシングして、結果を得る。

【００７７】

デジタル署名オラクル：入力メッセージに、秘密（プライベート）キーを使用してデジタル署名を行って、結果を得る。この機能は、コンテンツにパブリックキーおよびその証明書も提供することができる。

【００７８】

乱数ジェネレータ：乱数ジェネレータは、例えばオンライン接続におけるリプレーアタック（replay attacks）を防止するのに使用するため、コンテンツに予測不可能な情報を提供することができる。

【００７９】

数学関数：コンテンツがその計算プロセスを最適化するのを助けるため、基本的な数学演算を提供することができる。例えば、コンテンツは、特許文献５のＲＳＡアルゴリズムを実行してデジタル署名の生成・認証およびメッセージの暗号化・復号を行うため、最適化されたモジュラ乗算または累乗関数を使用することができる。

【００８０】

最適化された暗号化の基本要素：標準暗号化アルゴリズムを最適化して実装すると、性能向上に役立せることができる。これらの処理を使用して、データブロック、例えば、媒体からロードされたコンテンツのインタプリタコード空間又はセクタの領域などを、復号したりハッシングしたりするのを援助することができるが、上記データブロックに含まれるものは上記例に限定されるものではない。

【００８１】

復号制御：コンテンツが再生を許可すると決定した場合には、インタプリタコードは、当該コンテンツの各セグメントに対する正しい復号キーを用いて、コンテンツ復号モジュールを初期化することができる。加えて、当該インタプリタコードは、（例えば、再生時のリアルタイムウォータマーク挿入を可能にするため）コンテンツの中でレンダリングまたはスキップすべき部分を指定することができる。当該インタプリタと、媒体からのコンテンツストリーミングとの間の同期を保証するため、あらかじめ、キー変更（またはスキップ領域）を指定し、その後、コンテンツ内のシグナルによってかかる変更を引き起こすことができる。例えば、例示的な実施形態においては、コンテンツは、暗号文に遭遇したときにキー変更を引き起こす６４ビット値と、キー変更後にスキップする暗号文のバイト数と、使用する新しいキー値とを指定することができる。

【００８２】

キー管理：コンテンツは、これらの機能により、プレーヤがどのキーを認識しているかを判断することができる。

【００８３】

暗号オラクルの例示的な実施形態であって、この暗号オラクルの処理がランダムパラメータまたはその他の可変データを組み込んでいない例示的な実施形態においては、本シ

ステムは、ある入力に対して予測される結果を前もって（例えば、コンテンツがマスタリングされるときに）計算できるように構成することができる。そこで、制作者は、選択した入力を当該オラクルに渡し、ついで、予測された結果が取得されていることを確認するようにコンテンツをプログラムすることができる。正規の暗号キーのない害意あるプレーヤは、正しいオラクル応答を計算することができない。起こりうるオラクル入力の数は莫大（例えばブロックサイズが１２８ビットのブロック暗号を使用するオラクルの場合は、2^{128}）であるから、攻撃者が可能性のある全てのクエリに対する結果を事前に計算したり保存したりすることは、事実上不可能である。

【００８４】

有効なプレーヤを確認することに加えて、暗号オラクルを用いて、無効なプレーヤを識別することもできる。例えば、正当なプレーヤから抽出されたキーが不正な目的のために使用される場合には、取り消されたオラクルを含むプレーヤでの再生を拒否するように、コンテンツをマスタリングすることができる。コンテンツは有効なキーがなければ再生されないから、未認証のプレーヤには、盗まれたキーが含まれていると考えられる。しかし、これら盗んだキーが使用されると、未認証のデバイスは、当該セキュリティ侵害（compromise）を認識している新しいコンテンツに対して、自分のステータスをさらすことになる。

【００８５】

オラクルの結果を組み込むか、又は特定のオラクルクエリ応答が有効であるか否かをチェックするため、多種多様な方法を採用することができる。最も簡単な方法は、単に、予測された値と比較することである。この方法は、（少なくとも理論的には）、予測された値と全て一致するように振舞うように害意をもって設計されたインタプリタによって、回避されてしまう可能性があるから、コンテンツには、失敗を見越して行う「ダミー」の比較や、その他、害意あるインタプリタを妨害するように設計されたテストを含めることができる。オラクル自体を使用して、コードを復号するか、または自己修正コードに影響を及ぼすこともできる。例えば、当該オラクルへの入力を、所望のコードの暗号化バージョンとすることができる。そこで、このようなオラクルは、その構成次第で、コンテンツ制作者が、認証されたプレーヤまたはプレーヤのサブセットのみが復号できるコードを媒体に含められるようにし、それにより、コンテンツのコードを潜在的な攻撃者から遠ざける上で助けとなる。オラクルを使用する別の方法としては、これらオラクルの出力を暗号キーとして使用するか、またはキーを取り出す方法がある。これらのキーは、例えば、コード、コンテンツ、他のキー、その他様々なデータを復号するのに使用することができる。この柔軟性のある復号機能を用いれば、多種多様なプロトコルおよびポリシーをコンテンツに実装することができる。例えば、仮にプレーヤが充分な種類のキーを有する場合には、Fiat and Naorの方法（非特許文献３参照）のようなスキームを使用するようにコンテンツをプログラムすることができる。精巧なアクセス制限システム、例えば、特許文献２に記載されているシステムであっても、必要であれば（もちろん、プレーヤが必要なユーザインタフェースと、ネットワークと、データストレージと、暗号化機能を備えていれば）、実装可能である。

【００８６】

コンテンツをマスタリングするにあたって、オラクル入力／出力ペアへのアクセスは制作者にとって有益なものとなりえる。オラクルがＲＳＡのような非対称暗号システムのプライベートキーを使用する場合には、制作者は、単に、パブリックキーを取得して、これを使用してオラクル処理の逆の処理を実行すればよい。ブロック暗号を使用して構築された対称オラクルにあっては、プレーヤ製造業者は、各プレーヤにおいて提供される対称オラクルの逆を、制作者のために計算することができる。例えば、仮にプレーヤオラクルがブロック暗号を使用して、秘密キーで２５６ビットのデータブロックを復号する場合には、製造業者は、制作者が対応する暗号化機能へアクセスできるようにすることができる。逆のオラクルへアクセスすることができても、当該オラクルを改ざんすることはできないから、製造業者であれば、（例えば）、公開されアクセス可能なＷｅｂサーバにより、

ＳＳＬを使用して、逆オラクルの演算を行うことも考えられる。製造業者はまた、ランダムに選択されたオラクル入力の中から、制作者に出力を提供することもありえる。（製造業者は、プレーヤに実装されるような実際のオラクル機能を制作者に提供することができるが、これらの機能は、潜在的に、正当なプレーヤをエミュレートする不正なプレーヤを構築するために悪用される可能性がある。）

【００８７】

キーをプレーヤおよび製造業者に割り当てるため使用される具体的な方法は、それぞれの実施形態およびセキュリティ目的に依存する。例えば、例示的な一実施形態においては、プレーヤには、プレーヤ対称キーの大規模なグローバルプールから（擬似）ランダムに選択されたプレーヤ対称キー、製造業者によって（擬似）ランダムに生成されたプレーヤ固有の対称キー、製造業者やプレーヤモデル等に固有の対称キー、および／またはプレーヤが特定の特性を持たない（例えば特定の製造業者によって製造されていない）ことを認証する対称キーを含む種々の対称暗号オラクルキーが割り当てられるが、この対称暗号オラクルキーに含まれるものは上記のものに限定されるものではない。この例示的な実施形態においては、コンテンツは、サポートされたキーのリストを返す別の機能を呼び出して、プレーヤにどのキーが実装されているかを識別することができる。プレーヤは非対称キーを含むこともできる。例えば、上記例示的な実施形態においては、プレーヤは、プレーヤ固有のパブリックキー／プライベートキーペア、製造業者が自分のプライベートキーを使用してプレーヤパブリックキーに署名しこれにより発行されたプレーヤ証明書、製造業者のパブリックキーを認証するルートキー発行機関により発行された証明書、プレーヤのセキュアなメモリ領域へのアクセス要求を認証するために用いるパブリックキー（以下を参照）、および／または、プレーヤファームウェアの更新版を認証するために使用されるパブリックキーを有する。

【００８８】

プレーヤ製造業者が複数関与するインフラストラクチャにおいては、１つ以上の中央集権的な組織（central administrative organization）に、プレーヤ、製造業者等のキーを管理させることが有効となる場合もある。中央アドミニストレータ（central administrator）は、最低限のセキュリティ標準を実現すること、プレーヤが正確な情報をコンテンツコードに提供することを保証すること、新しい製造業者用のキーを（これら製造業者の製品が古いコンテンツを再生できるようにするため）取っておくこと、改ざんされたキーを追跡すること、コンテンツ制作者の暗号オラクル処理を実行すること等の点でも有効となりえる。

【００８９】

セキュアなメモリおよびカウンタ

コンテンツが利用可能なメモリは、典型的には揮発性のものであり、起動されるたびに、「クリーンな」実行環境をコンテンツに提供する。しかし、幾つかの機能にあっては、コンテンツが、再生と再生の間、タイトルとタイトルの間に、データを保存できることが有用である。このニーズを満足させるため、プレーヤは、セキュアで不揮発性のストレージであって、再生と再生の間の状態を維持するためのストレージを、コンテンツに提供することができる。このようなストレージは、解釈された正当なコードのみが不揮発性メモリの内容を読み取るかまたは修正できることを保証するため、追加のセキュリティ保護を要求することができる。不揮発性メモリのセキュリティを保証することは、例えば、後で課金するため、オフラインの従量制視聴履歴をトレースする際に、この不揮発性メモリを信頼できるため、制作者にとって重要である。各メモリスロットをロック解除するためのキーが媒体上にあるだけでは足りない。というのは、このようなキーは、海賊行為者によってすぐに発見され、全てのプレーヤのメモリスロットが改ざんされてしまうからである。そこで、一実施形態においては、これらのセキュアな不揮発性メモリ領域にアクセスするコードの明示的な暗号認証が提供される。

【００９０】

この実施形態においては、プレーヤには、幾つかの不揮発性メモリブロックが含まれ

るが、これらは、デフォルトで、ロックされている（すなわち、リード及びライトの許可は与えられていない）。当該プレーヤには、メモリブロックをロック解除する要求を認証するために使用されるパブリックキーも含まれる。このメモリブロックへアクセスするため、当該コンテンツは、メモリへのアクセスが許可されているコードのブロックを介して、デジタル署名を入力として受け取る機能を呼び出す。このデジタル署名は、当該プレーヤに組み込まれたパブリックキーを使用して認証可能なものであって、ロック解除するメモリブロックを指定し、当該ブロックの各部において許可されたアクセス権（任意のリード、任意のライト、インクリメント、デクリメント、ゼロにする（zeroize）、等）を指定する。インタプリタは、デジタル署名を確認し、この署名が有効であれば、メモリをロック解除して、デジタル署名されたコードを実行する。以下に示すのは、このプロセスの例であって、定期的に（例えば毎月）監査して、オフラインの従量制コンテンツの課金を行う際に使用するためのプロセスの例である。

【００９１】

（ａ）制作者Ｘは、プレーヤ製造業者Ｙとの間で、Ｙのプレーヤの不揮発性メモリ内の４バイトカウンタを制御する権利について、交渉する。

【００９２】

（ｂ）制作者Ｘは、メモリ内容をチェックするインタプリタのための機能を書き込む。仮にチェックした値が消費限界に達しない場合には、この機能はカウンタをインクリメントする。そうでない場合には、この機能は、制作者とのインターネット接続を確立し、カウンタ値、乱数、および支払情報（クレジットカード番号か、またはプレーヤに保存された他の資金源等）を含む支払要求を伝送する。仮に制作者が、このカウンタによって示された過去の購入に現在の購入を加えた支払を受け入れる場合には、制作者は、プレーヤに、このカウンタをクリアするための暗号認証を伝送し、プレーヤはこれを確認し、（有効であれば）カウンタをゼロにする。プレーヤは、このメモリを再度ロックして、成功又は失敗を示すコードを返して、終結する。

【００９３】

（ｃ）プレーヤ製造業者Ｙは、制作者Ｘのメモリ領域、アクセス権限等を示すパラメータを使用して、メモリ更新コードにデジタル署名する。

【００９４】

（ｄ）制作者Ｘは、署名されたコードを含むコンテンツを作成して、ユーザに配信する。

【００９５】

（ｅ）このユーザのプレーヤが当該コンテンツのロードを開始すると、このユーザに購入選択が提示される。仮にこのユーザが購入を辞退した場合には、再生は進行しない。

【００９６】

（ｆ）当該コンテンツは、ステップ（ｂ）で書き込まれたコードを指し示すポインタと、ステップ（ｃ）で生成されたデジタル署名とを使用して、メモリロック解除機能を呼び出す。

【００９７】

（ｇ）このメモリロック解除機能は、ステップ（ｂ）で述べたように、購入実行を試み、成功又は失敗を通知する。

【００９８】

（ｈ）仮に当該購入が成功した場合には、当該コンテンツはこのユーザのために再生される。そうでない場合には、再生は終了する。

【００９９】

もちろん、上記のセキュアなカウンタメカニズムを使用してさらに精巧な購入メカニズムを採用することも可能である。コンテンツに何を実装できるかについての実際の制約は、プレーヤの機能からくる制約や制作者の創造性からくる制約のみである。

【０１００】

本明細書に開示されたシステムおよび技法には、フラッシュメモリ、磁気記憶装置（

例えばハードディスク）、バッテリバックアップ付ＲＡＭ等を含む種々の記憶技術を採用することができるが、これら種々の記憶技術に含まれるものは上記のものに限定されるものではない。（背景技術においては、不揮発性のストレージを提供し、しかもこのようなストレージに暗号化その他の保護を施す多種多様な方法が知られている。）セキュアなストレージは、プレーヤ外部に位置させることができ（この例に限定されるものではない）、例えば、リムーバブルモジュール（スマートカード等）に含めたり、接続された出力周辺装置（スピーカ、ディスプレイ、ホームネットワークのリモートデバイス等）に含めたり、コンピュータネットワークを介してリモートに位置させることができる（これらの例に限定されるものではない）。メモリブロックアロケーションは、例えば、利用可能領域に基づいて行うことができ、（例えばスロット番号によって）保証することができ、または優先順位に基づいて割り当て／リサイクルを行うことができる。メモリスロットがクリアされるか開放されると、未通知の従量制視聴記録が紛失する可能性があるから、コンテンツには、スロットに上書きできる条件を指定する機能を与えることができる。複数のタイトルを同時に再生できるが、不揮発性メモリスロットを１セットしか持たないプレーヤにあっては、コンテンツのある部分により修正されているスロットに、コンテンツの別の部分がアクセスすることを保証するために、ロック機構が必要となるかもしれない。

【０１０１】

一実施形態においては、コンシューマがプリペイドスマートカードを購入し、これをプレーヤのスロットに挿入するようになっている。このプリペイドスマートカードには、複数のＷＯＭ（write once memory）スロットが含まれており、プレーヤは、これらＷＯＭに、従量制コンテンツのタイトルに対応するコンテンツＩＤを書き込むことができる。一度コンテンツＩＤが書き込まれると、このコンテンツＩＤは、プリペイドスマートカードに実装された暗号オラクル演算に組み込まれる。そこで、コンテンツは、再生を許可する前に、正しいオラクルが存在することを確認することで、購入が完了していることを確認できる。

【０１０２】

プレーヤ機能の呼び出しを認証する前述の一般的なアプローチは、セキュアなカウンタとともに使用することに限定されるものではない、ことに留意されたい。例えば、同じアプローチによれば、許可された制作者のみが使用できる特別なプレーヤ機能へのアクセスを保護することができる。このアプローチは、演算機能へのアクセスを保護する汎用的であるが極めて柔軟な方法を提供するものであるから、本明細書に開示された技法およびシステムの他の態様とは別個の適用性も有する。

【０１０３】

暗号ベースのセキュリティ機能対言語ベースのセキュリティ機能

セキュリティポリシーは、幾つかの異なる方法で実施することができる。暗号化による保護では、取り消されるか、または認証されていないプレーヤが、コンテンツの復号に必要な暗号キーを持たなくなるように、コンテンツを構築することができる。認証されていないプレーヤは、キーを持たないコンテンツにアクセスできない（もちろん、適正な暗号が使用されている場合）。このアプローチは比較的柔軟である。というのは、このアプローチによれば、コンテンツ所有者には、特定デバイスにおいて再生を阻止する機能のみが提供されるからである（より精巧な実施形態においては、異なるキーセットを使用して、幾分詳細な制御を行うことができるが、キーベースの制御は、より複雑なアクセス制御の課題を解決するには、柔軟性に欠ける）。それにもかかわらず、特定のプレーヤのセキュリティが侵害されるか、その他、信用できないと判断されるため当該コンテンツを復号する機能を持たせることができないケースに対処する上で、極めて効果的である。

【０１０４】

これに対して、言語ベースのコントロールは、プレーヤのセキュリティが侵害される（あるいは、その他に、何らかの理由で全く信用できない）ケースに対しては、効果的でないが、非常に精巧なセキュリティポリシーを実現することができる。前述のように、コンテンツは、再生環境を分析し、暗号オラクルを呼び出すことができ、仮に結果に満足で

きない場合には、再生を拒否することができる。このアプローチは、事実上無制限の柔軟性をもつから、当該コンテンツを次のようなリスク、すなわち、通常は忠実に振舞うプレーヤであるが、一部の制作者が特定のコンテンツに関しては阻止したいと思う処理（保護されていないフォーマットへのリッピング（ripping）等）をサポートすることができるプレーヤでの再生に関わるリスクの管理に非常に適している。攻撃者は、少なくとも理論的には、（特にコンテンツのコードが不完全に作成されている場合には）コンテンツの個々の部分を分析して破壊することが可能だが、こうした攻撃を一般化することは不可能で、暗号オラクルを注意深く用いれば、確実に対処することができる。さらに、本明細書に記載された復号制御機能によれば、自己のコンテンツが海賊コピーされるのを見とめた制作者は、セキュリティ侵害が起きたデバイスを識別し、攻撃されにくい新しいコンテンツを作成することができる。

【０１０５】

展開

コンテンツ所有者に、長期間セキュアである配信インフラストラクチャを提供するのが望ましい。以前のコンテンツ保護システムは、この点で、失敗している。すなわち、開発者（implementer）は、当初は、コンテンツ所有者をして新しいフォーマットに合わせるよう強く説得するためにセキュリティについての努力を惜しまないかもしれないが、ひとたびフォーマットの成功が確実になると、セキュリティレベルが大幅に下がる傾向にある。この低下には種々の要因が考えられる。例えば、攻撃できる実装がより多くなっていること（簡単に破壊される製品が販売される可能性が増えている）、より保護されたコンテンツが可能になるに従って海賊行為へのニーズが増加していること、攻撃がより巧妙になっていることなどが含まれる。本明細書に開示されたシステムおよび技法の例示的な実施形態においては、コンテンツ所有者は、たとえ媒体フォーマットが標準化された後であっても、引き続き、自分のコンテンツがどのように保護されるかを指定できるように構成することができ、仮に攻撃が発見された場合にもセキュリティが永久に失われないような、事実上無制限の更新可能性をもつ。

【０１０６】

セキュリティポリシーが静的でない場合には、製造業者は、効果的なセキュリティを提供するという動機付けを長期間持ち続けることになる。例えば、コンテンツ所有者は、キーが改ざんされたデバイス上や、一般的に海賊行為に使用される製品上での再生を阻止する（または高品質の再生を阻止する）能力を有することができる。その結果、従来のシステムとは異なり、プロダクト製造業者は、自社の製品を可能な限り低価格で提供しようと競合しているときに、セキュリティを犠牲にすることはできない。というのも、ロバストなセキュリティを有する製品は最善かつ最も信頼できる再生体験をもたらすので、コンシューマもまたそのような製品を求めるからである。

【０１０７】

害意のない製造業者であっても、後にセキュリティ上の欠陥があると判明する製品を誤って製造する可能性がある。したがって、われわれは、セキュリティ侵害やセキュリティ上の脆弱性に対処する上で使用できる種々の方法を開示する。例えば、プレーヤの暗号キーおよびソフトウェアは、デジタル署名されたコードまたはキーの更新版を使用して、更新することができる。こうした更新版は、キーの更新を行うソフトウェアを含む媒体でもって、プレーヤに供給することができる。例えば、正当なユーザのプレーヤが、以前の所有者にセキュリティ侵害が発生していたために取り消されることとなった場合には、新しい所有者は、当該製品の技術サポート窓口に連絡して新しいキーを取得することができる（もちろん、顧客サービス担当者は、海賊行為者が不正目的で使用するために新しいキーを要求しようと問い合わせるのを思いとどまらせるため、ユーザ情報、例えば、名前、住所、クレジットカード番号、電話番号、e-mailアドレス、ＩＰアドレス等を求めるようにしてもよい。）。更新版は、インターネット（その他のネットワーク接続）、モデムコール、リモートコントロールまたはキーボードによる入力等によって、配信することもできる。もちろん、攻撃者が更新プロセスを使用して改ざんされたキーを投入したり、その他

、プレーヤに対する攻撃を行うことができないようにするため、更新版は、可能な限りセキュアに暗号化しなければならない。

【０１０８】

製造業者がセキュリティ侵害の影響を軽減できる別の方法は、取り外し可能なセキュリティモジュール、例えば、スマートカードを含めることである。このスマートカードを含めると、暗号オラクルの一部または全てが実装されることになり、同様に、コンテンツに提供されたその他のセキュリティに関係する機能が実装されることになる。セキュリティ侵害が発生した場合、あるいはセキュリティ上の欠陥が見つかった場合には、当該プレーヤ全体を交換するかアップグレードする代わりに、当該スマートカードを交換することが可能である。単にスマートカードスロットを設けるだけで、セキュリティ上必要になるまでスマートカードを備えなくても十分である場合もあることに留意すべきである。スマートカードが正当なプレーヤから取り外され、害意あるプレーヤに使用されるのを防止する上で、プレーヤおよび／またはスマートカードがコンシューマに送られる前に、スマートカードとその受領者とを暗号を使ってリンクさせる（例えば、カードと受領者に対称キーを共有させることにより）ことができる。

【０１０９】

マスタリングおよびＤＲＭ

コンテンツのマスタリングに関連して新たにかかるコストに、コンテンツ所有者が関心を示すのは、無理のないことである。本明細書に開示された技法およびシステムは、シンプルなセキュリティ手段を採用すれば、マスタリングプロセスに新たな費用が大幅にかかることのないように整備することができる。複雑なセキュリティポリシーを遵守したコンテンツを開発するには、確かに、開発およびテストのためにより多くの努力を要するが、これを選択するか否かは全く任意である。（他の保護システムにおいては、このような選択を排除し、全てのコンテンツ制作者に、同一のセキュリティシステム、ポリシー等を強制的に使用させている。）

【０１１０】

もちろん、制作者がセキュリティシステム自体を開発する必要はない。というのは、本明細書で開示されたシステムおよび技法においては、第三者のＤＲＭ供給業者は、セキュリティモジュールおよびマスタリングシステムを提供することができるからである。これらのベンダー（vender）は、最高の機能、最高のセキュリティ、最低のコスト、最高の柔軟性、最高の使いやすさ、最高の性能、最小のコードサイズ、最も拡張性のある取り消しリスト等を示して、制作者のビジネスを得ようとする。本明細書で開示された技法およびシステムは、コンテンツ所有者がセキュリティについて自ら判断する能力を有する場合のプラットフォームとして、機能することができる。

【０１１１】

ウォータマーキングおよびセキュリティ侵害の追跡

大部分の慣用のウォータマーキング方法に関しては、マーク検出プロセスは、広範囲に展開された多数の製品において標準化されて実装されている。このような検出アルゴリズムの知識があれば、一般に、攻撃者はコンテンツの品質を著しく低下させずに、ウォータマークを除去できるから、この慣用のウォータマーキング方法の静的なアルゴリズムは、残念ながら重大な危険を負担することになる。例示的な実施形態においては、本明細書で開示されたシステムおよび技法は、マークフォーマットと、符号化プロセスと、検出プロセスとが、全て制作者によって選択されるために一般的なマーク除去攻撃を受けにくい、オンザフライのウォータマーク挿入を含むことができる。

【０１１２】

例示的な一実施形態においては、制作者（厳密には制作者が作成した制御プログラム）は、出力コンテンツに何らかの情報を埋め込もうとする。この情報の各ビットは、第１のコンテンツ部分または第２のコンテンツ部分のいずれを復号および出力するかにより符号化することができる。これらの部分は、媒体上の暗号化された異なる領域とすることができ、異なるキーで暗号化することができる。これらの部分の違いは、コンテンツがマスタ

リングされるときに制作者が選択することが可能であり、気付かないほどわずかな変化から、全く相違するものまで、いずれも可能である。これら２つの部分には予め定めた関係がないから、一方の部分（その部分の復号キーを含む）のみを知った海賊行為者がもう一方を特定することはできない。

【０１１３】

暗号ベースの制御と、プログラムベースの制御とを使用して、どの領域を復号するかを選択できるから、攻撃者は、代替領域に何が含まれているかを判断できない。実際、コンテンツの設計にあっては、例えば、制御コードを（異なるプレーヤが異なるコードを使用するように）暗号化し、しかも、どのプレーヤも復号できないか極めて少数のプレーヤしか復号できないダミー領域を含めれば、攻撃者は代替領域が存在するか否かすら識別できないように設計することが可能である。

【０１１４】

例示的な一実施形態においては、全てのプレーヤのうちのあるサブセットしかコンテンツの領域の各バージョンを復号するために必要なキーを有していないものの、実質的に全てのプレーヤが当該コンテンツの領域の少なくとも１つのバージョンを復号するために必要なキーは有しているように、コンテンツがオーサリングされる。したがって、この領域の不正コピーを分析すれば制作者は、攻撃者に関する情報を特定することができる。このことは、攻撃者が（攻撃されやすい）プログラムをなんとか分析し、複数の代替領域を復号した場合であっても、その結果生じた幾つかの領域の組合せから、やはりどのバージョンが復号されたかが制作者には明らかとなるので、このような場合においても当てはまることに留意されたい。結局のところ、ユーザが、自分のID（または自分のプレーヤのID）が制作者の海賊行為対策実施の専門家（anti-piracy enforcement expert）に明らかになるのを防止できる唯一の信頼できる方法は、そもそも海賊行為に関与しないことである。

【０１１５】

この一般的なマーキングのアプローチは、慣用のウォータマーキングとは異なり、マーク検出プロセスを標準化する必要がない。このような違いがあるから、セキュリティが著しく向上する。実際、このマーキングスキームが攻撃される兆しはない。さらに、ウォータマークが付されたビットは、出力に違いがあるから、これらウォータマークは、極めてロバストにすることができ、デジタル／アナログ変換、編集、フォーマット変換、害意の攻撃等にも耐えうるように設計することができる。

【０１１６】

コンテンツをマーキングする機能をどのように構成し使用するかは、典型的には、制作者が判断する。アーティストの中には、ウォータマーキング機能を自分の作品に使用させないようにして、どんな小さなものであれ何らかの修正を加える技術を避けようとする者もいるだろう。あるいは、コンテンツの中には、このコンテンツに対して広く海賊行為が行われるので、マーキング機能を非常に積極的に使用するのに適した候補となるものがある。部分の選択は、感知できない程度の違いしか生じないように行うのが普通であるが、どの代替バージョンを選択して符合化するか、可能な出力バージョンからどのように選択するか、そしてこれらの部分の復号キーの管理は、コンテンツによって制御される。当該マーキング機能は、コンテンツと統合されたデータ処理命令によって制御されるから、この技術は、他の機能、例えば、勝者のプレーヤが祝辞を出力する賞金レースを実装する、セキュリティが不充分なプレーヤを有するユーザにセキュリティ警告を配信する、あるユーザにボーナスコンテンツを提供する、といった機能にも使用することができる。なお、そのような機能の例としては上記に限定されるものではない。

【０１１７】

もちろん、本明細書で開示された技法およびシステムにおいては、他のウォータマーキングスキームを使用することもできる。例えば、コンテンツのコードか、あるいはウォータマーク埋め込みのための外部回路（コンテンツによりコントロールされていてもよいし、されていなくてもよい。）のいずれかによって、（マーク検出アルゴリズムが標準化されている）伝統的なウォータマークを、出力に埋め込むこともできる。同様に、到来する

コンテンツからウォータマークを検知して、例えば、不正コピーを作成しようとするか、あるいは不正コンテンツを導入しようとしていることを、（ここでも、当該コンテンツのコードか、または外部検出器のいずれかによって）検出することができる。どんなウォータマークを埋め込み、検出されたウォータマークにどのように応答するかの選択は、プレーヤ内および／またはコンテンツ内で行うことができる。

【０１１８】

移行過程の例：ＣＤオーディオ

デジタルコンテンツの大多数が、今日では、保護されないで配信されるか、あるいは最小限の保護で配信されている。例えば、ＣＤオーディオの規格には海賊行為対策機能が含まれておらず、ＤＶＤビデオの保護スキームは、広範囲に破られてきた。従来のメディアプレーヤは、充分なセキュリティをサポートしていないため、アップグレードするか交換する必要がある。新しいセキュリティシステムが成功するかどうかは、互換性のあるプレーヤを大量に確立できるかに依存している。

【０１１９】

本明細書で開示された技法およびシステムと、コピー防止機能付きＣＤを作成するための既存の方法とを組み合わせれば、後方互換性のあるＣＤを作成することができる。このようなＣＤは、非標準のＣＤフォーマットを使用して、ほとんどのオーディオＣＤプレーヤでは正しく再生されるが、コンピュータベースのリッピングソフトウェアを混乱させるディスクを作成する。許可された（例えばライセンスが与えられた）パーソナルコンピュータソフトウェアも、不正確に読み取られるか、その他コンピュータを混乱させる部分を訂正することによって、こうしたディスクを再生することができる。そのため、（ほとんどの）旧式のオーディオプレーヤでは非標準の（コピー防止機能付きの）レッドブックオーディオ部分を再生することができるので、再生が可能であり、（例えば、ＣＤに含められるか、インターネットを介してダウンロード可能な）適正なプレーヤソフトウェアを有するパーソナルコンピュータでも、再生が可能である。既存のＣＤオーディオプレーヤとの後方互換性を長期にサポートすると、追加のセキュリティリスクが導入される可能性があるが、新しいセキュアなフォーマットを再生できるオーディオプレーヤの整備を促進して（最終的には）そのセキュアなフォーマットでのみコンテンツを販売できるようにすることが、より長期の戦略の一部として有益である。

【０１２０】

例：ＨＤ（High-Definition）－ＤＶＤ

現在のＤＶＤビデオプレーヤにより採用されているコピー防止システムは、広範囲に亘って破られてきた。すでに何百万というＤＶＤプレーヤが販売されており、これらは、新しいコピー防止システムへのアップグレードができないから、これら旧来のユーザに対するサポートを放棄せずに、現在のＤＶＤフォーマットをアップグレードする簡単な方法はない。幸いにも、既に導入されているＤＶＤプレーヤは、「標準」精細度のＴＶ（例えば、走査線は、ＮＴＳＣの場合が５２５本で、ＰＡＬの場合が６２５本、等）をサポートするようにのみ設計されており、ＨＤＴＶ（high-definition TV）フォーマットによるより高品質の信号をサポートするように設計されているわけではない。旧式のプレーヤはＨＤＴＶをサポートしていないから、本明細書で開示された新しいセキュリティ機能は、ＨＤＴＶをサポートしているＤＶＤに組み込むことができる。

【０１２１】

例示的一実施形態においては、プレーヤは（１つ以上のディスク用の機械式のトレイよりなる）ユーザアクセス可能な媒体入力機構を有することになり、この媒体入力機構は、媒体をスピンドルにロードし、この媒体は、スピンドルにより回転され、レーザを使用して読み取られる。この媒体から読み取られたデータは、マイクロプロセッサベースの回路に搬送され、この回路により、ディスクエンコーディングが分析され、ディスク容量と、フォーマットタイプと、セキュリティ方法とが判断される。仮にディスクが旧来のセキュリティスキーム（ＣＳＳ）を使用した旧式の（低解像度）ＤＶＤである場合には、このディスクは背景技術において周知の方法を使用して再生される。仮に当該ディスクが、本明

細書で開示したようなプログラム可能なセキュリティ方法を使用したＨＤ－ＤＶＤである場合には、コンテンツのセキュリティポリシーのプログラムコード（データ処理命令）が、当該ディスクからロードされ、プレーヤにより実行される。プレーヤは、オプションであるが、改良されたセキュリティを使用した低密度のＤＶＤをサポートすることもでき、同様に、旧来の保護方法を使用したＨＤ－ＤＶＤをサポートすることもできる（ただし、広範囲に破られたセキュリティスキームを新しいコンテンツに使用しても、一般に、その利益は少ない。）。このＤＶＤプレーヤからの出力の品質は、コンテンツによってコントロールすることができる。例えばコンテンツは、仮にプレーヤおよび／またはＨＤＴＶの出力デバイスにより充分なセキュリティが提供されない場合には、低解像度の出力を出力するように選択することができる。この場合、当該コンテンツは、（例えば）当該プレーヤに指示して、ＨＤＴＶ信号を低解像度に（例えば、この目的のために特別に設計された劣化モジュールを使用して）ダウンコンバートしたり、当該信号の低解像度部分を復号するのに必要なキーのみを当該プレーヤに供給したり（高解像度部分に必要なキーは与えない）、あるいは、当該プレーヤに指示して、高解像度バージョンとは別に媒体上に符合化されているコンテンツの低解像度バージョンを出力することができる（がこれらに限定されるものではない）。

【０１２２】

追加の考慮事項および変形形態

例示的な実施形態においては、コンテンツを特定のプレーヤのためにカスタマイズすることができる。この場合、当該コンテンツは単一のプレーヤまたは少数のプレーヤ上でのみ再生可能であるが、受信側のデバイス上で再生するのに必要でないコードは、伝送する必要がない。そのため、このアプローチは、情報をユーザに送信するのが困難であるか、費用がかかるか、またはこの送信速度が遅いとき、例えば、記憶領域が限られているか、または当該コンテンツを低速のネットワーク接続を介して送信しなければならない場合には、特に有用である。そうであっても、当該コンテンツは、再生環境が適正にセキュアであることを、当該プレーヤにクエリを行って確認することができる。

【０１２３】

再生が中断したり歪んだりしないことを保証するためには、プレーヤのインタプリタに対して、特定の最低性能標準を要求することは、有用なことである。

【０１２４】

例示的な実施形態においては、本システムおよび方法を、コンテンツがデバイス間で交換可能なように、構成することができる。このような交換に特有のセキュリティ特性は、例えば信頼できる（例えば制作者が管理する）サーバとオンラインで通信可能か否かというファクタに依存する。コンテンツが転送されるフォーマットは、当該コンテンツによって遵守されるセキュリティポリシーと、デバイスのハードウェアの機能とに依存する。例えば、両方のデバイスがセキュアなインタプリタを含む一実施形態においては、送信側のデバイスは、暗号化された生のコンテンツ（オリジナルの媒体にストアされているか、他のキーで暗号化されているもので、場合によっては、ウォータマークが含まれているもの）を、再生コントロール用のコードと共に伝送する。この再生コントロールコードは、送信側のデバイスによって、受信側のデバイスのためにカスタマイズすることができる。別のケースにおいては、送信側のデバイスは、出力ポートのセキュリティ特性とあて先デバイスのセキュリティ特性が許容できるか否かを確認し、あて先デバイスとの間の共用キーを決め、コンテンツを復号してウォータマークを付け、上記共用キーを用いて当該コンテンツを再度暗号化し、この再度暗号化したコンテンツをあて先に送信するようにしてもよい。

【０１２５】

充分な不揮発性ストレージを有するプレーヤを使用して、インタプリタから呼び出された更新可能なコードを記憶することができる。例えば、当該プレーヤは、特定の制作者のための最新のセキュリティコードを常に記憶するように構成することができる。この場合、セキュリティコードのさらに新しいバージョンが検出されると、古いバージョンは（例

えば、新しいコード上のデジタル署名を確認した後に）更新されることになる。この方法においては、古いコンテンツは、新しいコンテンツ上で行われるセキュリティ更新の利益を受けることができる（例えば、この方法は、前述のセキュアなメモリ方法を使用して実現することができる）。他の実施形態においては、コンテンツは、プレーヤから、現在の日付／時刻を取得し、分かっている最新のセキュリティアップグレードの日付／時刻と比較して、当該プレーヤが現在のセキュリティ更新版を含むことを要求できる。このようにして、コンテンツは、プレーヤが十分に最新のセキュリティアップグレード版を有することを、保証することができる。

【０１２６】

一般に、コンテンツ保護システムは、正当なユーザによる正当なアクションにおいて、可視の役割を演じることを避けるべきである。にもかかわらず、ユーザインタフェース要素の中には、例えばエラーを通知したり、情報を提供したりするために必要なものがある。コンテンツが、サポートされている複数の出力品質から選択できる場合には（例えば、プレーヤの提供するセキュリティが不充分である場合には、「旧来の」品質とし、セキュリティが満足できるものである場合には、「高」品質とする等）、インジケータは、ユーザに出力品質を通知するのに有用である。例えば、一実施形態においては、コンテンツにより制御されている緑のＬＥＤ（light emitting diode）は、出力が高品質である（すなわち、セキュリティが満足できる）ことを示し、オレンジのＬＥＤは、品質が低いこと（すなわち、セキュリティが不充分である）ことを示し、点滅する赤いＬＥＤは、当該プレーヤが取り消されたため、出力がないことを示すことができる。別の実施形態においては、セキュリティのステータスを通知するため、音声または文字による（もしわかれば、ユーザの言語での）短い通知が提供される。高品質対低品質の出力を通知かつ／または使用するかどうかの判断は、他の要素、例えば、ロバストかつ／または脆弱なウォータマークの存在および／または不存在に基づくことができる。必要であれば、コンテンツが、セキュリティその他の理由で、再生品質を（例えば、旧式のフォーマットの品質まで）低下させることができるように、劣化モジュールをプレーヤに含めることができる（例えば、ＨＤＴＶ信号をＮＴＳＣ解像度に変換するか、または高解像度マルチチャネル音声を２チャネルＣＤ品質音声に変換するため、劣化モジュールを含めることができる）。

【０１２７】

仮に媒体のインタフェースとプレーヤのインタプリタとが充分な性能をもっていれば、バルク復号およびウォータマークの埋め込みは、別の復号モジュール内ではなく、当該インタプリタ内で処理することができる。コンテンツが自分自身を直接復号できれば、セキュリティ上の利点、例えば、攻撃者が復号モジュールを攻撃することが確実になくなるなどの利点が得られる。インタプリタの性能が充分である場合には、コンテンツ圧縮解除を当該インタプリタに実装することもでき、単一のプレーヤＣｏｄｅｃタイプを標準化する必要もなくなる。

【０１２８】

インタプリタを使用した実装は、本明細書で開示した技法およびシステムに特有のハードウェアサポートのないプラットフォーム上（例えばパーソナルコンピュータ）では好適であるが、インタプリタ機能の多くを、専用のハードウェアに実装することは、可能である。アプリケーションによっては、それ専用に実装すると、機能は低下するが、コストまたは消費電力の節約になる。

【０１２９】

コンテンツを物理媒体で受け取る実施形態は、実質的には、どの媒体フォーマットをも使用することができる。光ディスク（ＣＤおよびＤＶＤ等）は、高記憶密度を低コストで提供するが、磁気媒体、ホログラフィックメモリ、バッテリバックアップ付ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、およびフラッシュメモリを含む他の記憶システムも採用できる。この他の記憶システムに含まれるものはこの例に限定されるものではない。当該媒体の記憶容量は、多くの異なるタイプのデータをストアするため使用することができ、これらデータとしては、本明細書で開示された技法およびシステムに関係する情報（例えば、種々のコ

ンピュータプラットフォーム用の復号方法を実装する実行可能プログラム、本明細書で開示された方法を使用して保護されたコンテンツ等）と、本明細書で開示された技法およびシステムには直接関係しないデータ（例えば、関係のない実行可能プログラム、レッドブックＣＤオーディオのような保護されていないコンテンツ、他のセキュリティスキームを使用して保護されたコンテンツ等）と、が含まれる。

【０１３０】

プレーヤが、媒体が不正コピーではないと確認することができるように、当該媒体には、耐タンパー性を有する回路であって、暗号演算を実行する回路を含めることができる。このような機能は、電気的なインタフェースを使用する媒体に実装するのが最も簡単であるが、光媒体でも、暗号機能を含むことができる。例えば、非接触型暗号モジュール（例えば、特許文献６に記載の非接触型スマートカード）は、光ディスクに付加するか、これに組み込むことができる。暗号媒体認証は、好ましいものであるが、これに代えて、他の認証メカニズムを採用することができる。例えば、背景技術において知られている一般的な媒体認証方法には、シリアル番号をコピーが困難な位置（例えば、市販の記録可能媒体またはドライブを用いて書き込むことのできない領域）に書き込むこと、及びオリジナルの物理媒体の種々の特性の解説であって、デジタル署名された「解説」を含めること、が含まれる。もちろん、暗号メカニズムは、たとえ攻撃者が既存の媒体のセキュリティを侵害する方法を発見した場合であっても、次のような利点、すなわち、将来の媒体はセキュリティを改良して発行するが、プレーヤには何ら変更を加えない、という利点を提供する。

【０１３１】

多くのコンシューマが、既に旧来のフォーマットのコンテンツに投資しているから、本明細書で開示された技法およびシステムを実装するプレーヤは、これら旧来のフォーマットをサポートするように構成してもよい。同様に、種々のバージョンのインタプリタを特定のプレーヤによってサポートするようにしてもよい。この場合、プレーヤは、媒体またはコンテンツを分析して、使用する適正なセキュリティシステムを確認する必要がある。例えば、デジタルビデオプレーヤであれば、このディスクが、ＣＳＳを使用した旧来のＤＶＤであるか（もしそうであれば、ＣＳＳ復号システムを選択する）、あるいは、本明細書で開示された技法およびシステムを使用したＤＶＤであるか（もしそうであれば、言語ベースの復号システムを起動する）を検出するようにしてもよい。コンテンツに含まれたロバストなウォータマークは、元々あるセキュリティシステムで保護されたコンテンツが、当初の保護機能をもたないフォーマットにコピーされたか否かを検出するため、使用することができる。例えば、コピーが許可されていないコンテンツであれば、これには、次のようなウォータマーク、すなわち、他のフォーマット（例えば、保護されていないフォーマット）のコピーに遭遇したデバイスが、当該コピーが許可されていないものと認識して（例えば）再生を拒否できることを示すためのウォータマークを含めることができる。

【０１３２】

本明細書で開示された技法およびシステムは、種々のコンテンツタイプとともに使用することができ、これら種々のコンテンツタイプとしては、音声、静止画像、映像、３Ｄ画像、および３Ｄ映像が含まれるが、これらに限定されるものではない。

【０１３３】

また、本明細書で開示された技法およびシステムは、種々の物理デバイスに実装することができる。仮に１つのデバイスのみがコンテンツを復号する責務を負う場合には、セキュリティポリシーはそのデバイスによって実施されることが好ましい。しかし、出力デバイスおよび中間処理デバイス（例えば、オーディオイコライザまたはミキサ）も、本明細書で開示された技法およびシステムから利益を得ることができ、かつ／または、本明細書で開示された技法およびシステムが、セキュリティを確認するのに用いることができるクエリ機能を提供すれば、利益を得ることができる。一実施形態においては、ホームエンタテイメント用のサーバが、コンテンツをダウンロード、保存、管理し、セキュリティが正常に確認された再生装置（スピーカ、ヘッドフォン、ビデオディスプレイ等）にコンテン

ツを転送する。これらのデバイスへの接続は、好ましくは、本明細書で開示された技法およびシステムとあて先デバイスが共同して制御して、暗号化され、転送中に、コンテンツが盗まれるのを防止する。

【図面の簡単な説明】

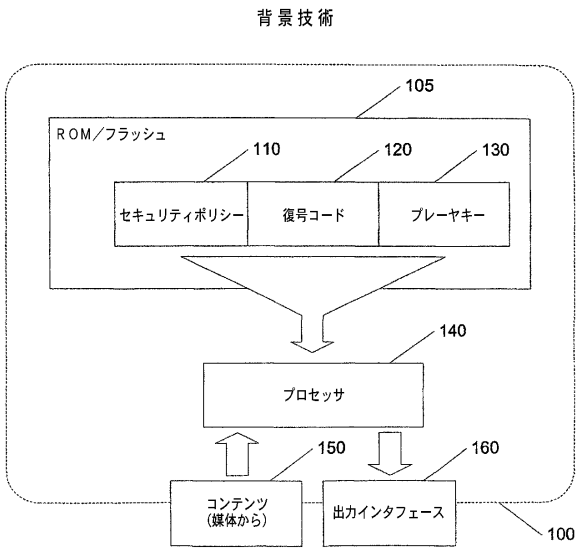
【０１３４】

【図１】背景技術のコンテンツ保護方法を使用したメディアプレーヤを示す図である。

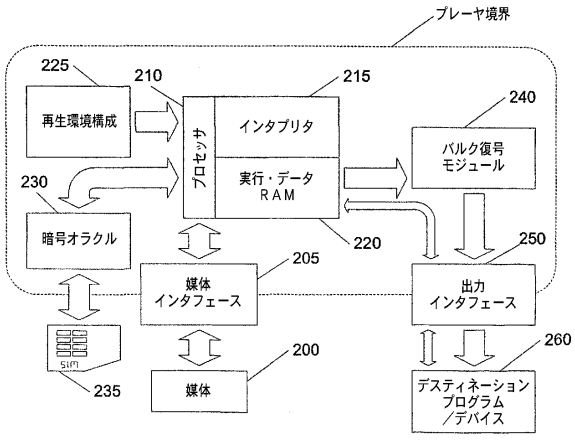
【図２】本明細書に開示されたコンテンツ保護方法を使用したメディアプレーヤの例を示す図である。

【図３】例示的な実施形態における復号に関する部分を示す図である。

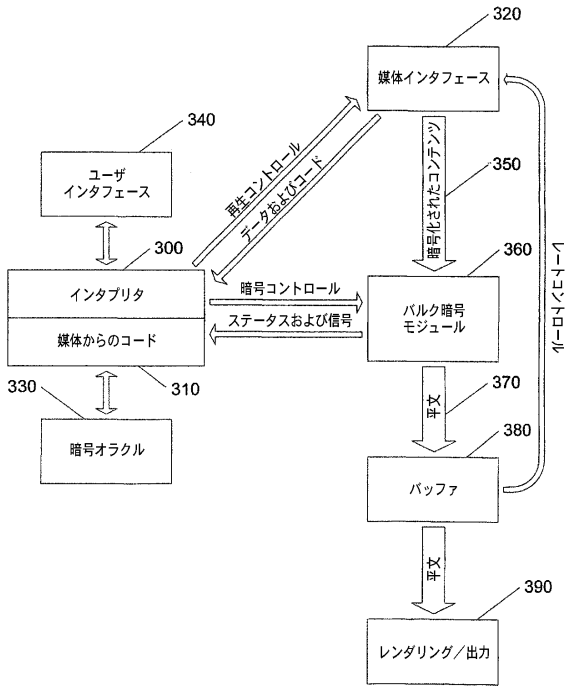
【図１】



【図２】



【図３】


320
媒体インタフェース
340
ユーザ
インタフェース
再生コントロール
データおよびコード
暗号化されたコンテンツ
350
300
360
インタプリタ
暗号コントロール
バルク暗号
モジュール
ステータスおよび信号
媒体からのコード
コントロール
330
310
平文
370
380
暗号オラクル
バッファ
平文
390
レンダリング／出力

フロントページの続き

(51)Int.Cl.			FI		
G11B 27/00	*(2006.01)*		G06F	17/60	302E
H04N 5/91	*(2006.01)*		G09C	1/00	660D
			G11B	20/12	
			G11B	27/00	D
			H04N	5/91	P

(72)発明者 ジョシュア エム. ジャフィー
アメリカ合衆国 94131 カリフォルニア州 サンフランシスコ チャーチ ストリート 1833
(72)発明者 ベンジャミン シー. ジュン
アメリカ合衆国 94404 カリフォルニア州 フォスター シティー イースト ヒルズデイル ブールバード 1200 ナンバー204
(72)発明者 カーター シー. ラーレン
アメリカ合衆国 94109 カリフォルニア州 サンフランシスコ ブッシュ ストリート 1264 ナンバー4
(72)発明者 ピーター ケー. ピアソン
アメリカ合衆国 94550 カリフォルニア州 リバーモア ヴィクトリア レーン 5624

合議体
審判長 酒井 伸芳
審判官 石川 正二
審判官 月野 洋一郎

(58)調査した分野(Int.Cl., DB名)
G11B20/10