

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-185782

(P2004-185782A)

(43) 公開日 平成16年7月2日(2004.7.2)

(51) Int.Cl.⁷

G 1 1 B 20/10
G 0 6 F 12/14
H 0 4 L 9/32
H 0 4 L 9/36

F I

G 1 1 B 20/10 H
G 0 6 F 12/14 3 2 0 F
H 0 4 L 9/00 6 8 5
H 0 4 L 9/00 6 7 5 Z

テーマコード (参考)

5 B 0 1 7
5 D 0 4 4
5 J 1 0 4

審査請求 未請求 請求項の数 23 O L (全 30 頁)

(21) 出願番号 特願2002-355117 (P2002-355117)
(22) 出願日 平成14年12月6日 (2002.12.6)

(71) 出願人 000005016
パイオニア株式会社
東京都目黒区目黒1丁目4番1号
(74) 代理人 100104765
弁理士 江上 達夫
(74) 代理人 100107331
弁理士 中村 聡延
(72) 発明者 吉村 隆一郎
埼玉県所沢市花園4丁目2610番地 パ
イオニア株式会社所沢工場内
(72) 発明者 横塚 栄彦
埼玉県所沢市花園4丁目2610番地 パ
イオニア株式会社所沢工場内

最終頁に続く

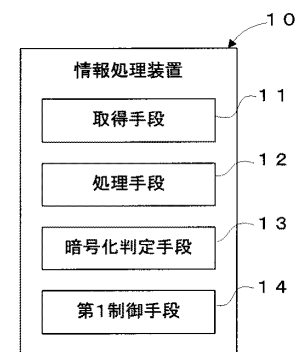
(54) 【発明の名称】 情報処理装置、情報記録装置、情報記録媒体、コンピュータプログラム及び情報処理方法

(57) 【要約】

【課題】 不法コピー等に対する情報の保護を強化すると共に、これを低コストで実現する。

【解決手段】 コンテンツ情報に所定の暗号化方式で暗号化された認証情報を付加する。情報処理装置10によってコンテンツ情報を実行又は再生するときには、取得した情報中に所定の暗号化方式で暗号化された情報が含まれるか否かを判定し、このような情報が含まれていないときには、コンテンツ情報を再生せず、実行せず又は出力しないようにする。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

情報を再生又は実行するための情報処理装置であって、
前記情報を取得する取得手段と、
前記取得手段により取得された情報の再生処理又は実行処理を行う処理手段と、
前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定手段と、
前記暗号化判定手段による判定の結果、前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第 1 制御手段と
を備えたことを特徴とする情報処理装置。

【請求項 2】

前記取得手段により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かを判定するフォーマット判定手段と、
前記フォーマット判定手段による判定の結果、前記取得手段により取得された情報の中に前記所定のフォーマットを有する情報が含まれていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第 2 制御手段と
を備えたことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているときに、その所定の暗号化方式により暗号化された情報を復号化する復号化手段と、
前記復号化手段により復号化された情報が認証情報であるか否かを判定する認証情報判定手段と、
前記認証情報判定手段による判定の結果、前記復号化された情報が認証情報でないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第 3 制御手段と
を備えたことを特徴とする請求項 1 又は 2 に記載の情報処理装置。

【請求項 4】

前記認証情報判定手段は、前記復号化された情報のチェックサムが所定の値か否かを調べることにより、前記復号化された情報が認証情報であるか否かを判定することを特徴とする請求項 3 に記載の情報処理装置。

【請求項 5】

前記復号化手段により復号化された情報が前記認証情報であるときに、前記認証情報が情報記録媒体上の所定のアドレスに記録されているか否かを判定するアドレス判定手段と、
前記アドレス判定手段による判定の結果、前記認証情報が前記所定のアドレスに記録されていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第 4 制御手段と
を備えたことを特徴とする請求項 3 又は 4 に記載の情報処理装置。

【請求項 6】

前記情報記録媒体には、コンテンツ情報と前記認証情報が記録されており、前記認証情報の前記情報記録媒体上のアドレスには、前記コンテンツ情報の前記情報記録媒体上のアドレスを用いて所定の演算を行うことによって得られる値が設定されており、

前記アドレス判定手段は、前記コンテンツ情報の前記情報記録媒体上のアドレスを用いて前記所定の演算を実行する演算手段と、
前記認証情報の前記情報記録媒体上のアドレスの値が、前記演算手段の演算により得られた値と一致するか否かを比較する比較手段と
を備えたことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】

前記復号化手段により復号化された情報が前記認証情報であるときに、前記認証情報が多層情報記録媒体の所定の層に記録されているか否かを判定する記録層判定手段と、
前記記録層判定手段による判定の結果、前記認証情報が所定の層に記録されていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、
実行せず若しくは最終的に出力しないように前記処理手段を制御する第 5 制御手段と
を備えたことを特徴とする請求項 3 又は 4 に記載の情報処理装置。 10

【請求項 8】

前記認証情報は画像情報であることを特徴とする請求項 3 ないし 7 のいずれかに記載の情報処理装置。

【請求項 9】

前記認証情報はロゴであることを特徴とする請求項 3 ないし 7 のいずれかに記載の情報処理装置。

【請求項 10】

前記認証情報のフォーマットは DVD ビデオフォーマットであることを特徴とする請求項 3 ないし 7 のいずれかに記載の情報処理装置。 20

【請求項 11】

前記所定の暗号化方式は、鍵を用いて情報記録媒体に記録すべき情報を暗号化し、前記鍵を、前記情報記録媒体の所定記録領域に記録する方式であり、前記所定記録領域は、前記情報記録媒体に記録された情報を読み取る機能を有する一般ユーザ向けの情報読取装置を通常の操作方法で操作することによって任意にアクセスすることができない領域であることを特徴とする請求項 1 ないし 10 のいずれかに記載の情報処理装置。

【請求項 12】

前記所定の暗号化方式は CSS（コンテンツ・スクランブル・システム）であることを特徴とする請求項 1 ないし 10 のいずれかに記載の情報処理装置。 30

【請求項 13】

前記取得手段は、DVD-ROM ドライブであることを特徴とする請求項 1 ないし 12 のいずれかに記載の情報処理装置。

【請求項 14】

前記処理手段は、MPEG（Moving Picture Experts Group）デコードモジュールを備えていることを特徴とする請求項 1 ないし 13 のいずれかに記載の情報処理装置。

【請求項 15】

前記取得手段により取得された情報は、当該情報処理装置で実行可能なコンピュータプログラムを含むことを特徴とする請求項 1 ないし 14 のいずれかに記載の情報処理装置。 40

【請求項 16】

前記取得手段により取得された情報は、当該情報処理装置で実行可能なゲームプログラムを含むことを特徴とする請求項 1 ないし 14 のいずれかに記載の情報処理装置。

【請求項 17】

請求項 16 に記載の情報処理装置を備えたゲーム装置。

【請求項 18】

情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、
前記コンテンツ情報を記録すべき前記情報記録媒体上のアドレスを取得するアドレス取得 50

手段と、

前記アドレス取得手段により取得された前記コンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を前記認証情報の前記情報記録媒体上のアドレスの値に設定するアドレス設定手段と、

前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、

前記アドレス取得手段により取得されたアドレスに前記コンテンツ情報を記録し、前記アドレス設定手段により設定されたアドレスに前記暗号化手段により暗号化された認証情報を記録する記録手段と

を備えたことを特徴とする情報記録装置。

【請求項 19】

10

多層情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、

前記コンテンツ情報を前記多層情報記録媒体のいずれかの層に記録する第1記録手段と

前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、

前記暗号化手段により暗号化された認証情報を前記多層情報記録媒体の層のうち、前記コンテンツ情報を記録する層以外のいずれかの層に記録する第2記録手段と、

を備えたことを特徴とする情報記録装置。

【請求項 20】

コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な情報記録媒体であって、

20

前記認証情報は所定の暗号化方式により暗号化された状態で記録されており、

前記認証情報の記録アドレスには、前記コンテンツ情報の記録アドレスを用いて所定の演算を行うことによって得られた値が設定されていることを特徴とする情報記録媒体。

【請求項 21】

コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な多層情報記録媒体であって、

前記コンテンツ情報は前記多層情報記録媒体のいずれかの層に記録されており、

前記認証情報は、所定の暗号化方式で暗号化された状態で、前記多層情報記録媒体の層のうち前記コンテンツ情報を記録する層以外のいずれかの層に記録されていることを特徴とする情報記録媒体。

30

【請求項 22】

コンピュータを請求項 1 ないし 16 のいずれかに記載の情報処理装置として機能させることを特徴とするコンピュータプログラム。

【請求項 23】

情報を再生又は実行するための情報処理方法であって、

前記情報を取得する取得工程と、

前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定工程と、

前記暗号化判定工程における判定の結果、前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得工程における情報の少なくとも一部のさらなる取得を阻止する旨の制御命令、又は前記取得工程において取得された情報の少なくとも一部につき、実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する制御工程と、

40

前記取得手段において取得された情報の再生処理又は実行処理を行い、これにより再生又は実行された情報を出力する処理工程とを備え、

前記制御工程において前記制御指令が発せられたときには、前記取得工程において情報の少なくとも一部のさらなる取得を行わず、又は前記処理工程において実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わないことを特徴とする情報処理方法。

【発明の詳細な説明】

50

【0001】

【発明の属する技術分野】

本発明は、例えばコンピュータプログラム、ゲームプログラム、画像情報、音声情報等の情報を再生し又は実行する情報処理装置及び情報処理方法、このような情報を情報記録媒体に記録する情報記録装置、このような情報を記録した情報記録媒体、並びに上記情報処理装置を実現するためのコンピュータプログラムに関する。

【0002】

【従来の技術】

現在では、画像、音声等の情報が、デジタル情報として、ディスク等の情報記録媒体に記録され、又は通信ネットワークを介して広く流通し、拡散するようになった。また、パーソナルコンピュータ等の普及により、画像、音声等のデータだけでなく、コンピュータプログラムやゲームプログラムといった情報のコピーを容易に作り出すことができるようになった。さらに、これら情報の経済的価値が増し、これら情報に関する著作権その他の財産権の保護を強化する要請が高まった。

【0003】

このような状況のもと、情報の不法コピーを防止すべく、情報を暗号化する様々な技術が開発されている。また、情報に当該情報が真正なものであることを示す認証情報を付加し、この認証情報に基づいて不法にコピーされた情報の再生又は実行を制限する技術が開発されている。

【0004】

例えば、映画又は音楽のコンテンツの不法コピーを防止する技術としては、CSS（コンテンツ・スクランブル・システム）又はCPPM（コンテンツ・プロテクション・フォー・プリレコーディッド・メディア）等が普及している（なお、CSSについては、例えば、下記の非特許文献1参照）。

【0005】

また、コンピュータプログラム又はゲームプログラムのコンテンツの不法コピーを防止する技術としては、これらの情報を記録したROMディスク等の情報記録媒体に認証情報を刻印する技術が普及している。例えば、コンピュータプログラム又はゲームプログラムを記録したROMディスクの最内周領域に、ロゴ、バーコード等、個性を有する刻印を施す。この刻印が施された領域は、通常の情報記録領域よりもさらに内周側に位置する領域（すなわちディスクの通常の使用形態では非記録領域）であるため、通常の再生装置では、ピックアップをその領域まで移動させることができず、その領域にアクセスすることができない。そこで、ピックアップをその最内周領域まで移動させ、その領域へのアクセスを可能とする特別の機能を、再生装置に付加する。そして、ROMディスクを再生するときには、その再生装置によって最内周領域にアクセスし、刻印が正しく検出することができない場合には、ROMディスクの再生を行わないようにする。かかる技術によれば、不法にコピーされたコンピュータプログラム等が記録されたディスクには、その最内周領域に刻印が存在しないので、このようなディスクが再生されるのを防止することができ、これにより、不法コピーの抑制を図ることができる。

【0006】

【非特許文献1】

館林誠、外3名、「DVD著作権保護システム」、映像情報メディア学会技術報告、1997年5月22日、第21巻、第31号、p. 15-19

【0007】

【発明が解決しようとする課題】

ところが、上述したCSS及びCPPMといった暗号化技術は、保護すべき情報に対して、所定の鍵を用い、かつ所定のアルゴリズムに従って情報処理又は演算処理を行うものである。このため、鍵とアルゴリズムが知られてしまえば、暗号化を解くことができる。もちろん、鍵やアルゴリズムは、情報又はディスクの製作者や提供者、又は著作権保護団体等により秘密に管理されており、一般人が知ることはできない。また、仮に鍵やアルゴリ

10

20

30

40

50

ズムに関する情報が漏洩したとしても、暗号化を解くためには、複数の鍵が必要であり、また、アルゴリズムも複雑であるため、暗号化を解くことはきわめて困難である。しかし、これらの暗号化技術は、基本的には情報処理又は演算処理のみに依拠し、物理的・有体的な構造に依拠していないため、高度の情報処理知識を有する技術者により、暗号化が解かれてしまう危険がある。

【0008】

一方、ROMディスクの最内周領域に認証情報を刻印する技術は、刻印を用いることや、ピックアップを特別な最内周領域に移動させる機能を再生装置に付加することなど、物理的・有体的な構造に依拠している。したがって、かかる点に着目すれば、情報の保護を強化できるとも思える。しかし、ディスクの最内周領域に存在する刻印を検出する機能（以下、これを「刻印検出機能」という。）は、再生装置に付加された付随的な機能であり、再生装置の通常の情報再生機能とは切り離された独立の機能である。このため、再生装置の一部を改造することによって、刻印検出機能が除去されてしまう危険がある。 10

【0009】

また、ROMディスクの最内周領域などの特別な領域に特別な情報を刻印する方法では、再生装置に特別な機能（例えばピックアップを特別な領域まで移動させる機能など）を付加しなければならない。さらに、ROMディスクに刻印を形成するためには、専用のディスク製造装置が必要になる。このため、再生装置及びディスクの製造コストが上昇する。

【0010】

本発明は上記に例示したような問題点に鑑みなされたものであり、本発明の第1の課題は、不法コピー等に対する情報の保護を強化することができる情報処理装置、情報記録装置、情報記録媒体、コンピュータプログラム及び情報処理方法を提供することにある。 20

【0011】

本発明の第2の課題は、不法コピー等に対する情報の保護を低コストに実現することができる情報処理装置、情報記録装置、情報記録媒体、コンピュータプログラム及び情報処理方法を提供することにある。

【0012】

【課題を解決するための手段】

上記課題を解決するために請求項1に記載の情報処理装置は、情報を再生又は実行するための情報処理装置であって、前記情報を取得する取得手段と、前記取得手段により取得された情報の再生処理又は実行処理を行う処理手段と、前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定手段と、前記暗号化判定手段による判定の結果、前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第1制御手段とを備えている。 30

【0013】

上記課題を解決するために請求項17に記載のゲーム装置は、請求項1ないし16のいずれかに記載の情報処理装置を備えている。 40

【0014】

上記課題を解決するために請求項18に記載の情報記録装置は、情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、前記コンテンツ情報を記録すべき前記情報記録媒体上のアドレスを取得するアドレス取得手段と、前記アドレス取得手段により取得された前記コンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を前記認証情報の前記情報記録媒体上のアドレスの値に設定するアドレス設定手段と、前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、前記アドレス取得手段により取得されたアドレスに前記コンテンツ情報を記録し、前記アドレス設定手段により設定されたアドレスに前記暗号化手段により暗号化された認証情報を記録する記録手段とを備えている。 50

【0015】

上記課題を解決するために請求項19に記載の情報記録装置は、多層情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、前記コンテンツ情報を前記多層情報記録媒体のいずれかの層に記録する第1記録手段と前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、前記暗号化手段により暗号化された認証情報を前記多層情報記録媒体の層のうち、前記コンテンツ情報を記録する層以外のいずれかの層に記録する第2記録手段とを備えている。

【0016】

上記課題を解決するために請求項20に記載の情報記録媒体は、コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な情報記録媒体であって、前記認証情報は所定の暗号化方式により暗号化された状態で記録されており、前記認証情報の記録アドレスには、前記コンテンツ情報の記録アドレスを用いて所定の演算を行うことによって得られた値が設定されている。 10

【0017】

上記課題を解決するために請求項21に記載の情報記録媒体は、コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な多層情報記録媒体であって、前記コンテンツ情報は前記多層情報記録媒体のいずれかの層に記録されており、前記認証情報は、所定の暗号化方式で暗号化された状態で、前記多層情報記録媒体の層のうち前記コンテンツ情報を記録する層以外のいずれかの層に記録されている。 20

【0018】

上記課題を解決するために請求項22に記載のコンピュータプログラムは、コンピュータを請求項1ないし16のいずれかに記載の情報処理装置として機能させるものである。

【0019】

上記課題を解決するために請求項23に記載の情報処理方法は、情報を再生又は実行するための情報処理方法であって、前記情報を取得する取得工程と、前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定工程と、前記暗号化判定工程における判定の結果、前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得工程における情報の少なくとも一部のさらなる取得を阻止する旨の制御命令、又は前記取得工程において取得された情報の少なくとも一部につき、実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する制御工程と、前記取得手段において取得された情報の再生処理又は実行処理を行い、これにより再生又は実行された情報を出力する処理工程とを備え、前記制御工程において前記制御指令が発せられたときには、前記取得工程において情報の少なくとも一部のさらなる取得を行わず、又は前記処理工程において実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない。 30

【0020】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。 40

【0021】

(情報処理装置の第1実施形態)

本発明に係る情報処理装置の第1実施形態（以下、これを「第1情報処理装置」という。）について図1を参照して説明する。図1は第1情報処理装置の構成を示している。なお、図1は、本発明の実施形態に係る構成要素等を、その技術思想を説明する限りにおいて具体化したものであり、各構成要素等の形状、位置、接続関係などは、これに限定されるものではない。このことは、以下、本発明の実施形態の説明に用いる図2ないし図9についても同様である。

【0022】

図 1 に示す第 1 情報処理装置 10 は、情報を再生又は実行するための装置である。第 1 情報処理装置 10 は、例えば、家庭用ゲーム装置、シミュレーション装置、画像再生装置、音声再生装置等に適用することができ、また、汎用のコンピュータによって実現することも可能である。第 1 情報処理装置 10 の再生又は実行の対象となる情報は、コンピュータプログラム、ゲームプログラム、シミュレーションプログラム、画像情報、音声情報などであり、特に限定されない。

【0023】

第 1 情報処理装置 10 は、情報を取得する取得手段 11 と、取得手段 11 により取得された情報の再生処理又は実行処理を行う処理手段 12 と、取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定手段 13 と、暗号化判定手段 13 による判定の結果、取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、取得手段 11 による情報の少なくとも一部のさらなる取得を阻止するように取得手段 11 を制御し、又は取得手段 11 により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段 12 を制御する第 1 制御手段 14 とを備えている。

【0024】

取得手段 11 は、ディスク等の情報記録媒体から情報を取得する場合には、通常、ディスクドライブ等である。例えば、情報記録媒体が DVD-ROM である場合には、取得手段 11 は DVD-ROM ドライブである。一方、通信ネットワーク等から情報を取得する場合には、取得手段 11 は、例えばネットワークインタフェース等である。このように、取得手段 11 は、情報の取得方法等に応じて適宜選択することができ、特に限定されない。

【0025】

処理手段 12 は、コンピュータプログラムに対して実行処理を行う場合には、演算機能及び記憶機能等を備えたプロセッシングユニットである。また、画像情報又は音声情報に対して再生処理を行う場合には、デコード機能等を備えたプロセッシングユニット又はデコードモジュール等である。例えば、再生すべき情報が MPEG 圧縮された画像情報である場合には、処理手段 12 は MPEG デコードモジュールである。これらのユニットやモジュールは、専用の回路として実現することも可能であるが、汎用の CPU（セントラルプロセッシングユニット）にソフトウェアを実行させることによって実現することもできる。このように、処理手段 12 は、情報の性質・種類、設計・製造上の都合等に応じて適宜選択することができ、特に限定されない。

【0026】

暗号化判定手段 13 は、取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する手段であり、例えば、演算機能及び記憶機能を有する CPU その他のプロセッシングユニット等により実現することができる。取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かの判定は、情報に付された名前（特に拡張子）を調べる方法、情報が記録された情報記録媒体のファイルシステム情報中のフラグを調べる方法、暗号化された情報自体の性質を調べる方法などが考えられるが、いずれの方法を採用してもよい。

【0027】

第 1 制御手段 14 は、暗号化判定手段 13 による判定の結果、取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときに、取得手段 11 による情報の少なくとも一部のさらなる取得を阻止するように取得手段 11 を制御し、又は取得手段 11 により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段 12 を制御する。例えば、第 1 情報処理装置 10 の実行の対象となる情報がゲームプログラムの場合には、ゲームプログラムのうちの少なくとも一部のさらなる取得を阻止するように取得手段 11 を制御し、又は取得手段 11 により取得されたゲームプログラムの少なくとも一部を実行せず若しくは最終的に出力しないように処理手段 12 を制御する。また、第 1 情報処理装置 10 の再生の対象となる情報

が映画や音楽等の画像情報や音声情報の場合には、画像情報や音声情報のうちの少なくとも一部のさらなる取得を阻止するように取得手段 11 を制御し、又は取得手段 11 により取得された画像情報や音声情報のうちの少なくとも一部を再生せず若しくは最終的に出力しないように処理手段 12 を制御する。例えば、取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、第 1 制御手段 14 から取得手段 11 へ、さらなる情報の取得を中止する旨の指令を送る構成としてもよく、また、第 1 制御手段 14 から処理手段 12 へ、情報の少なくとも一部の再生処理又は実行処理を中止し又は開始しない旨の指令を送る構成としてもよい。さらには、第 1 制御手段 14 から処理手段 12 へ、情報の少なくとも一部につき、再生処理後又は実行処理後の出力を中止する旨の指令を送る構成としてもよい。

10

【0028】

また、かかる指令に基づいて、再生又は実行の対象となる情報の全部について実行せず、再生せず、又は出力しない構成としてもよいし、当該情報のうち、コピー制限がかけられた情報のみ又は保護の対象となる情報のみについて、取得せず、実行せず、再生せず、又は出力しない構成としてもよい。また、所定の暗号化方式としては、例えば、CSS方式、CPM方式等を用いることができるが、特に限定されない。かかる構成を有する第 1 制御手段 14 は、例えば、演算機能及び記憶機能を有する CPU その他のプロセッシングユニット等により実現することができる。

【0029】

このような構成を有する第 1 情報処理装置 10 は、以下に示すように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンピュータプログラム、ゲームプログラム、映画データ、音楽データ等のコンテンツ情報に、所定の暗号化方式により暗号化された認証情報を付加する。なお、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付加するのではなく、コンテンツ情報自体を所定の暗号化方式で暗号化してもよい。第 1 情報処理装置 10 の取得手段 11 が情報を取得し、その情報の中に所定の暗号化方式により暗号化された認証情報又は所定の暗号化方式により暗号化されたコンテンツ情報が含まれているときには、処理手段 12 は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。なお、このとき、取得手段 11 により取得された情報がさらに他の 1 つ又はいくつかの条件を満たしている場合に限り、取得手段 11 が情報の取得を継続し、又は処理手段 12 が再生処理若しくは実行処理を行うようにしてもよい。

20

30

【0030】

一方、取得手段 11 により取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれていないときには、暗号化判定手段 13 はその旨を判定し、第 1 制御手段 14 は、少なくともコンテンツ情報がこれ以上取得手段 11 によって取得されないように取得手段 11 を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは最終的に出力しないように処理手段 12 を制御する。この結果、取得手段 11 又は処理手段 12 は第 1 制御手段 14 の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。したがって、所定の暗号化方式で暗号化された認証情報が付加されておらず、コンテンツ情報自体も所定の暗号化方式で暗号化されていない場合には、そのコンテンツ情報は第 1 情報処理装置 10 により実行されず、再生されず又は出力されない。

40

【0031】

このような第 1 情報処理装置 10 によれば、取得手段 11 により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、情報の少なくとも一部のさらなる取得を阻止し、又は情報の少なくとも一部を再生せず、実行せず又は出力しない構成としたから、不法コピー等に対する情報の保護を強化することができる。すなわち、情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付加するか、又はコンテンツ情報自体を所定の暗号化方式で暗号化する。この結果、流通に付される真正の情報

50

は、常に、所定の暗号化方式により暗号化された情報を含んでいることになる。例えば、所定の暗号化方式で暗号化された認証情報が付加されたゲームプログラム（ゲームプログラム自体は暗号化されていない）が記録されたオリジナルディスクを手に入れた者が、ゲームプログラムのコピーディスクを作り出そうと企てているとする。この場合、この者は、オリジナルディスクからゲームプログラムのみを抜き出してブランクディスクにコピーするかもしれない。ところが、このようなコピーディスクを作り出したとしても、このコピーディスクに記録されたゲームプログラムを第1情報処理装置10で実行（又は最終的に外部へ出力）することはできない。なぜなら、コピーディスクに記録された情報の中には、所定の暗号化方式で暗号化された情報が存在しないからである。

【0032】

10

一方、所定の暗号化方式で暗号化された映画データのみが記録されたオリジナルディスクを手に入れた者が、映画データのコピーディスクを作り出そうと企てているとする。この場合、この者は、映画データを見ることができ的状态でコピーすることを望むのが通常であるから、映画データの暗号化を解き、暗号化の解かれた状態の映画データをコピーしようとする。ところが、仮にこのような不法コピーを実現することができたとしても、コピーされた映画データを第1情報処理装置10で再生（又は最終的に外部へ出力）することができない。なぜなら、コピーされた映画データは、もはや所定の暗号化方式で暗号化されていないからである。

【0033】

20

また、不法コピーをしようとする者が、情報の暗号化を解いた後、当該情報をさらに所定の暗号化方式で暗号化し、この再度暗号化された状態の情報をコピーすることも考えられる。しかし、情報の暗号化を解くことができたとしても、その情報を再び所定の暗号化方式で暗号化することは、暗号化を解くことに比べて、より一層困難である。例えば、所定の暗号化方式がCSS方式である場合、タイトル鍵、ディスク鍵、マスタ鍵の3つの鍵を用いた多重の暗号化が行われるため、暗号化を再現するためには、3つの鍵の情報をすべて知らなければならない。また、仮に3つの鍵の情報をすべて知り得たとしても、以下の理由により、暗号化の再現はほとんど不可能である。例えば、CSS方式で暗号化した情報を一般に市販されているブランクのDVD-Rに記録する場合を例に挙げると、CSS方式の暗号化の過程では、ディスク鍵がマスタ鍵により暗号化された後、DVD-Rのリードイン領域に書き込まれる。ところが、市販のブランクDVD-Rのリードイン領域には、ブランクディスク用の鍵情報が予め記録されているので、その場所に新たな鍵情報を書き込むことができない。したがって、たとえ3つの鍵の情報をすべて知り得たとしても、暗号化を再現することは、物理的・有体的にみて不可能に等しい。このように、所定の暗号化方式で暗号化された情報のコピーを作り出すことができない以上、第1情報処理装置10で再生、実行又は出力可能な情報のコピーを作り出すことはできない。

30

【0034】

また、不法コピーをしようとする者は、ディスクに所定の暗号化方式で暗号化されて記録された情報をセクタごとにそのまま他のディスクに転写することによってコピーディスクを作り出そうとするかもしれない。しかし、例えば、所定の暗号化方式がCSS方式である場合には、オリジナルディスクのリードイン領域に鍵情報が書き込まれている以上、このような方法でコピーディスクを作り出すことはほとんど不可能である。なぜなら、リードイン領域は、通常の一般人が任意にアクセスすることはできない領域であるし、仮に特別な読取装置を用いてリードイン領域から鍵情報を読み取ったとしても、上述したようにこれをブランクのDVD-Rのリードイン領域に転写することはできないからである。このように、所定の暗号化方式で暗号化された情報のコピーを作り出すことができない以上、第1情報処理装置10で再生、実行又は出力可能な情報のコピーを作り出すことはできない。

40

【0035】

以上のように、第1情報処理装置10により再生、実行又は出力可能な情報のコピーを作り出すことがほとんど不可能であり、この結果、不法コピー等に対する情報の保護を強化

50

することができる。

【0036】

さらに、第1情報処理装置10によれば、取得手段11により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、情報の少なくとも一部のさらなる取得を阻止し、又は情報の少なくとも一部を再生せず、実行せず若しくは出力しない構成としたから、不法コピー等に対する情報の保護を低コストで実現することができる。すなわち、情報を所定の暗号化方式で暗号化するのに、専用の工作機械等は不要であり、ただ、所定の暗号化方式で情報を暗号化するためのソフトウェアを用意すれば足りる。したがって、不法コピー等に対する情報の保護を低コストで実現することができる。

【0037】

なお、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付する場合、認証情報は、コンテンツ情報が真正なものであることを示すことのできる情報であれば何でもよいのであるが、認証情報を、画像又は音声を含む情報により構成すれば、画像用又は音声用の暗号化方式で認証情報を暗号化することができるので便利である。例えば、この場合には、認証情報を暗号化する暗号化方式として、CSS方式又はCPM方式等の一般に普及している暗号化方式を用いることができ、コンテンツ情報の保護を低コストに実現することができる。

【0038】

また、認証情報に情報製作者又はディスク製作者等のロゴを表した画像情報を含める構成としてもよい。この場合、当該認証情報に含まれるロゴを、当該認証情報を付加したコンテンツ情報の再生又は実行時に表示するなどして、当該ロゴを商標等として使用する態様を実現すれば、不法コピーを事業として行っている組織等に対する法的責任追及の手段が増え、コンテンツ情報の保護を強化することができる。

【0039】

(情報処理装置の第2実施形態)

本発明に係る情報処理装置の第2実施形態(以下、これを「第2情報処理装置」という。)について図2を参照して説明する。図2は第2情報処理装置の構成を示している。

【0040】

図2に示すように、第2情報処理装置20は、第1情報処理装置10と同様に、取得手段11、処理手段12、暗号化判定手段13及び第1制御手段14を備えている。これに加え、第2情報処理装置20は、取得手段11により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かを判定するフォーマット判定手段21と、フォーマット判定手段21による判定の結果、取得手段11により取得された情報の中に前記所定のフォーマットを有する情報が含まれていないときには、取得手段11による情報の少なくとも一部のさらなる取得を阻止するように取得手段11を制御し、又は取得手段11により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段12を制御する第2制御手段22とを備えている。

【0041】

フォーマット判定手段31は、取得手段11により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かを判定する手段であり、例えば、CPUその他のプロセッシングユニット等により実現することができる。取得手段11により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かの判定は、例えば、情報に付された名前(特に拡張子)を調べる方法でもよいし、情報のフォーマットの特性を調べる方法でもよいし、情報が記録された情報記録媒体のファイルシステム情報中のテーブルを調べる方法等でもよい。

【0042】

第2制御手段32は、フォーマット判定手段31による判定の結果、取得手段11により取得された情報が所定のフォーマットを有していないときに、取得手段11による情報の少なくとも一部のさらなる取得を阻止するように取得手段11を制御し、又は取得手段11により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力し

10

20

30

40

50

ないように処理手段１２を制御する手段であり、例えば、ＣＰＵその他のプロセッシングユニット等により実現することができる。例えば、取得手段１１により取得された情報が所定のフォーマットを有していないときには、第２制御手段２２から取得手段１１へ、情報の少なくとも一部につき、これ以上の取得を中止する旨の指令を送る構成としてもよいし、第２制御手段２２から処理手段１２へ、情報の少なくとも一部につき再生処理又は実行処理を中止し又は開始しない旨の指令を送る構成としてもよい。さらには、第２制御手段２２から処理手段１２へ、情報の少なくとも一部につき、再生処理後又は実行処理後の出力を中止する旨の指令を送る構成としてもよい。

【００４３】

また、所定のフォーマットは、例えば、コンテンツ情報又は認証情報が主として画像情報である場合にはＤＶＤビデオフォーマットがよい。また、コンテンツ情報又は認証情報が主として音声情報である場合には、ＤＶＤオーディオフォーマットがよい。このように、所定のフォーマットは、コンテンツ情報又は認証情報の種類・性質等に応じて適宜選択すればよく、特に限定されない。

【００４４】

このような構成を有する第２情報処理装置２０は、以下に示すように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定のフォーマットを有し、かつ所定の暗号化方式で暗号化された認証情報を付加する。なお、コンテンツ情報自体を、所定のフォーマットで製作し、かつ所定の暗号化方式で暗号化してもよい。第２情報処理装置２０の取得手段１１が情報を取得し、その情報の中に、所定のフォーマットを有しかつ所定の暗号方式により暗号化された認証情報、又は所定のフォーマットを有しかつ所定の暗号化方式で暗号化されたコンテンツ情報が含まれているときには、処理手段１２は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【００４５】

一方、取得手段１１により取得された情報の中に、所定のフォーマットを有する認証情報又は所定のフォーマットを有するコンテンツ情報が含まれていないときには、フォーマット判定手段２１はその旨を判定し、第２制御手段２２は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第２制御手段２２の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００４６】

一方、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化された認証情報又は所定の暗号化方式で暗号化されたコンテンツ情報が含まれていないときには、暗号化判定手段２１はその旨を判定し、第１制御手段１４は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第１制御手段１４の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００４７】

したがって、取得手段１１により取得された情報の中に、所定のフォーマットを有し、かつ所定の暗号化方式により暗号化された情報が含まれていなければ、少なくともコンテンツ情報は実行されず、再生されず、又は出力されない。

【００４８】

このように、第２情報処理装置２０によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第２情報処理装置２０によれば、所定のフォーマットを有し、かつ所定の暗号化方式で暗号化されている情報が存在していなければ実行されず、再生されず又は出力されないという、二重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化するこ

10

20

30

40

50

とができる。

【0049】

(情報処理装置の第3実施形態)

本発明に係る情報処理装置の第3実施形態(以下、これを「第3情報処理装置」という。)について図3を参照して説明する。図3は第3情報処理装置の構成を示している。

【0050】

図3に示すように、第3情報処理装置30は、第1情報処理装置10と同様に、取得手段11、処理手段12、暗号化判定手段13及び第1制御手段14を備えている。これに加え、第3情報処理装置30は、取得手段11により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているときに、その所定の暗号化方式により暗号化された情報を復号化する復号化手段31と、復号化手段31により復号化された情報が認証情報であるか否かを判定する認証情報判定手段32と、認証情報判定手段32による判定の結果、復号化された情報が認証情報でないときには、取得手段11による情報の少なくとも一部のさらなる取得を阻止するように取得手段11を制御し、又は取得手段11により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段12を制御する第3制御手段33とを備えている。 10

【0051】

復号化手段31は、所定の暗号化方式に対応する所定の復号化アルゴリズムを備えたデコードモジュール等を備えており、これは、演算機能及び記憶機能等を備えたプロセッシングユニット等により実現することができる。 20

【0052】

認証情報判定手段32は、復号化手段31により復号化された情報が認証情報であるか否かを判定する手段であり、演算機能及び記憶機能等を備えたプロセッシングユニット等により実現することができる。復号化された情報が認証情報であるか否かの判定は、例えば、第3情報処理装置に認証情報の特徴、データサイズ、内容、記録位置又は相対アドレス等を示すリファレンス情報を予め記憶させておき、判定時に、復号化された情報とリファレンス情報とを比較することによって行うことができる。また、復号化された情報のチェックサムが所定の値か否かを調べることにより、復号化された情報が認証情報であるか否かを判定する構成としてもよい。

【0053】

第3制御手段33は、認証情報判定手段32による判定の結果、復号化された情報が認証情報でないときには、取得手段11による情報の少なくとも一部のさらなる取得を阻止するように取得手段11を制御し、又は取得手段11により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段12を制御する手段であり、これも、演算機能及び記憶機能等を備えたプロセッシングユニット等により実現することができる。例えば、復号化された情報が認証情報でないときには、第3制御手段33から取得手段11へ、情報の少なくとも一部につき、これ以上の取得を中止する旨の指令を送る構成としてもよいし、第3制御手段33から処理手段12へ、情報の少なくとも一部を再生せず又は実行しない旨の指令を送る構成としてもよい。さらには、第3制御手段33から処理手段12へ、再生処理後又は実行処理後の出力を中止する旨の指令を送る構成としてもよい。 30 40

【0054】

このような構成を有する第3情報処理装置30は、以下に示すように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定の特徴、内容又はデータサイズ等を有し、かつ所定の暗号化方式により暗号化された認証情報を付加する。第3情報処理装置30の取得手段11が情報を取得し、その情報の中に、所定の暗号化方式により暗号化された情報が含まれており、かつその情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報であるときには、処理手段12は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。 50

【0055】

一方、取得手段11により取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれているものの、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報でないときには、認証情報判定手段32はその旨を判定し、第3制御手段33は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段11を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段12を制御する。この結果、取得手段11又は処理手段12は、第3制御手段33の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【0056】

一方、取得手段11により取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれていないときには、暗号化判定手段21はその旨を判定し、第1制御手段14は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段11を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段12を制御する。この結果、取得手段11又は処理手段12は第1制御手段14の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【0057】

したがって、取得手段11により取得された情報の中に、所定の暗号化方式により暗号化され、かつ所定の特徴、内容又はデータサイズ等を有する認証情報が含まれていなければ、少なくともコンテンツ情報は再生されず、実行されず、又は出力されない。

【0058】

このように、第3情報処理装置30によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第3情報処理装置30によれば、所定の暗号化方式により暗号化され、かつ所定の特徴、内容又はデータサイズ等を有する認証情報が存在していなければ、実行せず、再生せず、又は出力しないという、二重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【0059】

(情報処理装置の第4実施形態)

本発明に係る情報処理装置の第4実施形態(以下、これを「第4情報処理装置」という。)について図4を参照して説明する。図4は第4情報処理装置の構成を示している。

【0060】

図4に示すように、第4情報処理装置40は、第1情報処理装置10と同様に、取得手段11、処理手段12、暗号化判定手段13及び第1制御手段14を備え、さらに、第3情報処理装置30と同様に、復号化手段31、認証情報判定手段32及び第3制御手段33を備えている。これに加え、第4情報処理装置40は、復号化手段31により復号化された情報が認証情報であるときに、この認証情報が情報記録媒体上の所定のアドレスに記録されているか否かを判定するアドレス判定手段41と、アドレス判定手段41による判定の結果、認証情報が前記所定のアドレスに記録されていないときには、取得手段11による情報の少なくとも一部のさらなる取得を阻止するように取得手段11を制御し、又は取得手段11により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段12を制御する第4制御手段42とを備えている。

【0061】

アドレス判定手段41によるアドレス判定は、例えば第4情報処理装置40に認証情報を記録すべき所定のアドレスを示すリファレンス情報を予め記憶させておき、判定時にそのリファレンス情報と、実際に検出された認証情報のアドレスとを比較する方法により実現することができる。

【0062】

このような構成を有する第4情報処理装置40は、以下のように動作する。情報を製作又

10

20

30

40

50

は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定の特徴、内容又はデータサイズ等を有し、かつ所定の暗号化方式により暗号化された認証情報を付加する。さらに、コンテンツ情報と認証情報とを情報記録媒体に記録するときに、認証情報を情報記録媒体の所定のアドレス上に記録する。第4情報処理装置40の取得手段11が情報を取得し、その情報の中に、所定の暗号化方式により暗号化された情報が含まれており、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報であり、かつ、その認証情報が情報記録媒体上の所定のアドレス上に記録されているときには、処理手段12は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【0063】

一方、(i)取得手段11により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないとき、(ii)取得手段11により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているものの、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報でないとき、又は(iii)認証情報が情報記録媒体上の所定のアドレスに記録されていないときには、暗号化判定手段13、認証情報判定手段32又はアドレス判定手段41が上記(i)、(ii)又は(iii)の事実を判定し、第1制御手段14、第2制御手段33又は第4制御手段42が、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段11を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段12を制御する。この結果、取得手段11又は処理手段12は第1制御手段14、第2制御手段33又は第4制御手段42の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。したがって、取得手段11により取得された情報の中に、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有し、かつ、情報記録媒体上の所定のアドレス上に記録された認証情報が含まれていなければ、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【0064】

このように、第4情報処理装置40によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第4情報処理装置40によれば、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有する認証情報が存在し、かつ、その認証情報が情報記録媒体上の所定のアドレス上に記録されていない場合は実行せず、再生せず又は出力しないという、三重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【0065】

また、第4情報処理装置40のアドレス判定手段41を、以下に示すように構成してもよい。すなわち、情報記録媒体に、コンテンツ情報と認証情報が記録されている場合に、コンテンツ情報の情報記録媒体上のアドレスを用いて所定の演算を行うことによって得られる値を、認証情報の情報記録媒体上のアドレスに設定する。このような前提の下で、アドレス判定手段41を、コンテンツ情報の情報記録媒体上のアドレスを用いて前記所定の演算を実行する演算手段と、認証情報の情報記録媒体上のアドレスの値が演算手段の演算により得られた値と一致するか否かを比較する比較手段とを有する構成とする。

【0066】

所定の演算の内容は、コンテンツ情報が異なれば、ほぼ常に演算結果が異なるように構成することが好ましい。また、認証情報の記憶領域がコンテンツ情報の記憶領域と重複しないことや、認証情報の記憶領域が情報記録媒体上の記憶領域に収まるようにすることなどを考慮して、所定の演算の内容を決定する。例えば、コンテンツ情報の記録終了アドレスに、コンテンツ情報のサイズを一定値で割った値を加え、その結果得られる値を、認証情報の記録開始アドレスに設定することとしてもよい。

【0067】

このような構成によれば、認証情報のアドレスがコンテンツ情報のアドレスに基づいて決定されるので、所定の演算方法を知らない者が認証情報のアドレスを知ることがきわめて困難である。また、コンテンツ情報が変われば認証情報のアドレスが変わるため、認証情報のアドレスを知ることがいっそう困難となる。したがって、不法コピー等に対する情報の保護を強化することができる。

【0068】

(情報処理装置の第5実施形態)

本発明に係る情報処理装置の第5実施形態(以下、これを「第5情報処理装置」という。)について図5を参照して説明する。図5は第5情報処理装置の構成を示している。

【0069】

図5に示すように、第5情報処理装置50は、第1情報処理装置10と同様に、取得手段11、処理手段12、暗号化判定手段13及び第1制御手段14を備え、さらに、第3情報処理装置30と同様に、復号化手段31、認証情報判定手段32及び第3制御手段33を備えている。これに加え、第5情報処理装置50は、復号化手段31により復号化された情報が認証情報であるときに、この認証情報が多層情報記録媒体の所定の層に記録されているか否かを判定する記録層判定手段51と、記録層判定手段51による判定の結果、認証情報が所定の層に記録されていないときには、取得手段11による情報の少なくとも一部のさらなる取得を阻止するように取得手段11を制御し、又は取得手段11により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段12を制御する第5制御手段52とを備えている。

【0070】

記録層判定手段51によるアドレス判定は、例えば第5情報処理装置50に認証情報を記録すべき所定の層番号等を示すリファレンス情報を予め記憶させておき、判定時にそのリファレンス情報と、実際に検出された認証情報の記録された層番号等を比較する方法等により実現することができる。

【0071】

このような構成を有する第5情報処理装置50は、以下のように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定の特徴、内容又はデータサイズ等を有し、かつ所定の暗号化方式により暗号化された認証情報を付加する。さらに、コンテンツ情報と認証情報とを多層情報記録媒体に記録するときに、認証情報を多層情報記録媒体の所定の層に記録する。この場合、認証情報を記録する層は、コンテンツ情報を記録する層と異なる層に記録することが好ましい。より好ましくは、コンテンツ情報を多層情報記録媒体の第1層(通常最初に再生される層又はアドレスの0番が設定されている層)に記録し、認証情報を第2層以降のいずれかの層に記録する。さらに好ましくは、認証情報を、当該認証情報を記録すべき層に形成された記録領域の中間部分又は後半部分に記録する。

【0072】

第5情報処理装置50の取得手段11が情報を取得し、その情報の中に、所定の暗号化方式により暗号化された情報が含まれており、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報であり、かつ、その認証情報が多層情報記録媒体の所定の層に記録されているときには、処理手段12は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【0073】

一方、(i)取得手段11により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないとき、(ii)取得手段11により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているものの、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報でないとき、又は(iii)認証情報が多層情報記録媒体の所定の層に記録されていないときには、暗号化判定手段13、認証情報判定手段32又は記録層判定手段51が上記(i)、(ii)又は(iii)の事実を判定し、第1制御手段14、第2制御手段33又は第5制御手段52

10

20

30

40

50

が、少なくともコンテンツ情報のこれ以上の取得を中止するように取得手段 1 1 を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段 1 2 を制御する。この結果、取得手段 1 1 又は処理手段 1 2 は第 1 制御手段 1 4、第 2 制御手段 3 3 又は第 4 制御手段 4 2 の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。したがって、取得手段 1 1 により取得された情報の中に、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有し、かつ、多層情報記録媒体の所定の層に記録された認証情報が含まれていなければ、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【0074】

このように、第 5 情報処理装置 5 0 によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第 5 情報処理装置 5 0 によれば、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有する認証情報が存在し、かつ、その認証情報が情報記録媒体の所定の層に記録されていなければ実行せず、再生せず又は出力しないという、三重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【0075】

さらに、情報を不法にコピーしようとする者が、多層情報記録媒体に記録された情報を、1 層の情報記録媒体にコピーしようとする場合には、1 の層に記録されたコンテンツ情報のみを 1 層の情報記録媒体にコピーすることができたとしても、他の層に記録された認証情報はコピーすることができない。なぜなら、コピー先の情報記録媒体は 1 層であるため、コンテンツ情報を記録してしまえば、認証情報を記録する領域がないからである。確かに、コンテンツ情報のデータサイズが小さければ、認証情報を記録する領域があるかもしれない。しかし、この場合には、コピーした結果、認証情報の記録された層もアドレスも変わってしまうため、第 5 情報処理装置 5 0 又は第 4 情報処理装置 4 0 により、少なくともコンテンツ情報が実行又は再生されることはない。

【0076】

また、コンテンツ情報を多層情報記録媒体の第 1 層に記録し、認証情報を多層情報記録媒体の第 2 層以降のいずれかの層に記録すれば、製造時の検査作業等において都合がよい。すなわち、多層情報記録媒体の第 1 層に記録された情報は、通常、最初に再生されるので、製造時の検査作業等を迅速に行うことができる。

【0077】

さらに、認証情報を、当該認証情報を記録すべき層に形成された情報記録領域の中間部分又は後半部分に記録すれば、不法コピーをしようとする者に対して、認証情報を見つけにくくすることができる。

【0078】

(情報記録装置の第 1 実施形態)

本発明に係る情報記録装置の第 1 実施形態（以下、これを「第 1 情報記録装置」という。）について図 6 を参照して説明する。図 6 は第 1 情報記録装置の構成を示している。

【0079】

図 6 に示す第 1 情報記録装置 6 0 は、情報を製作又は提供する適法な権限を有する者、より具体的には情報記録媒体の製造者が、コンテンツ情報及び認証情報が記録された情報記録媒体を製造するときに用いるのに適した情報記録装置である。

【0080】

第 1 情報記録装置 6 0 は、コンテンツ情報を記録すべき情報記録媒体上のアドレスを取得するアドレス取得手段 6 1 と、アドレス取得手段 6 1 により取得されたコンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を認証情報の情報記録媒体上のアドレスの値に設定するアドレス設定手段 6 2 と、認証情報を所定の暗号化方式により暗号化する暗号化手段 6 3 と、アドレス取得手段 6 1 により取得されたアドレスにコンテンツ情報を記録し、アドレス設定手段 6 2 により設定されたアドレスに暗号化手段 6 3 により暗号化された認証情報を記録する記録手段 6 4 とを備えている。

【0081】

アドレス取得手段61は、コンテンツ情報を記録すべき情報記録媒体上のアドレスを取得する。取得方法は、アドレスを手入力する方法でもよいし、情報記録媒体に記録する種々の情報から演算により求める方法でもよい。

【0082】

アドレス設定手段62は、アドレス取得手段61により取得されたコンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を認証情報の情報記録媒体上のアドレスの値に設定する。所定の演算の内容は、コンテンツ情報が異なれば、ほぼ常に演算結果が異なるように構成することが好ましい。例えば、コンテンツ情報の記録終了アドレスに、コンテンツ情報のサイズを一定値で割った値を加え、その結果得られる値を、
10 認証情報の記録開始アドレスに設定することとしてもよい。

【0083】

暗号化手段63は、認証情報を所定の暗号化方式により暗号化する。所定の暗号化方式は、例えば、CSS方式、CPM方式などが考えられるが、認証情報の種類・性質（画像情報か音声情報かなど）に応じて適宜選択すればよく、特に限定されない。

【0084】

記録手段64は、コンテンツ情報及び暗号化された認証情報をそれぞれの記録アドレスに記録する。

【0085】

このような構成を有する第1情報記録装置60によれば、認証情報のアドレスがコンテンツ情報のアドレスに基づいて決定されるので、所定の演算方法を知らない者が認証情報のアドレスを知ることがきわめて困難である。また、コンテンツ情報が変われば認証情報のアドレスが変わるため、認証情報のアドレスを知ることがいっそう困難となる。したがって、上述した第1ないし第5情報処理装置（特に第4情報処理装置）と組み合わせることにより、不法コピー等に対する情報の保護を強化することができる。
20

【0086】

また、認証情報の記録アドレスを、コンテンツ情報の記録されている領域、すなわち通常の情報記録領域内（特別の機能を備えた読取装置又は記録装置等しかアクセスできないようなディスクの最内周側などではなく、通常読取装置又は記録装置等によりアクセス可能な領域内）に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現する
30 ことができる。なぜなら、この場合には、通常読取装置や通常記録装置ではアクセスすることができない領域にアクセスするための専用の機構が不要となるからである。

【0087】

（情報記録装置の第2実施形態）

本発明に係る情報記録装置の第2実施形態（以下、これを「第2情報記録装置」という。）について図7を参照して説明する。図7は第1情報記録装置の構成を示している。

【0088】

図7に示す第2情報記録装置70は、情報を製作又は提供する適法な権限を有する者、より具体的には情報記録媒体の製造者が、コンテンツ情報及び認証情報が記録された多層情報記録媒体を製造するときに用いるのに適した情報記録装置である。
40

【0089】

第2情報記録装置70は、コンテンツ情報を多層情報記録媒体のいずれかの層に記録する第1記録手段71と、認証情報を所定の暗号化方式により暗号化する暗号化手段72と、暗号化手段72により暗号化された認証情報を多層情報記録媒体の層のうち、コンテンツ情報を記録する層以外のいずれかの層に記録する第2記録手段73とを備えている。

【0090】

このような構成を有する第2情報記録装置70によれば、上述した第1ないし第5情報処理装置（特に第5情報処理装置）と組み合わせることにより、不法コピー等に対して情報の保護を強化することができる。例えば、情報を不法にコピーしようとする者が、多層情報記録媒体に記録された情報を、1層の情報記録媒体にコピーしようとする場合には、
50

の層に記録されたコンテンツ情報のみを1層の情報記録媒体にコピーすることができたとしても、他の層に記録された認証情報はコピーすることができない。なぜなら、コピー先の情報記録媒体は1層であるため、コンテンツ情報を記録してしまえば、認証情報を記録する領域がないからである。確かに、コンテンツ情報のデータサイズが小さければ、認証情報を記録する領域があるかもしれない。しかし、この場合には、コピーした結果、認証情報の記録された層もアドレスも変わってしまうため、第4情報処理装置又は第5情報処理装置により、少なくともコンテンツ情報が実行又は再生されることはない。

【0091】

また、コンテンツ情報を第2情報記録媒体の第1層に記録し、認証情報を第2情報記録媒体の第2層以降のいずれかの層に記録すれば、製造時の検査作業等において都合がよい。すなわち、第2情報記録媒体の第1層に記録された情報は、通常、最初に再生されるので、製造時の検査作業等を迅速に行うことができる。

10

【0092】

また、認証情報を、通常の情報記録領域内（多層情報記録媒体用の通常の読取装置又は記録装置等によりアクセス可能な領域内）に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。

【0093】

また、認証情報を、当該認証情報を記録すべき層に形成された情報記録領域内の中間部分又は後半部分に記録すれば、不法コピーをしようとする者に対して、認証情報を見つけにくくすることができる。

20

【0094】

（情報記録媒体の第1実施形態）

本発明に係る情報記録媒体の第1実施形態（以下、これを「第1情報記録媒体」という。）について図8を参照して説明する。図8は第1情報記録媒体の情報記録構造を示している。図8中の左側から右側にかけて第1情報記録媒体の記録アドレス値が増加するように設定されている。例えば、第1情報記録媒体がDVDである場合には、図8中の左側がディスクの内周側であり、右側がディスクの外周側である。

【0095】

図8に示すように、第1情報記録媒体80は、コンテンツ情報81とこのコンテンツ情報81が真正なものであることを示すための認証情報82とが記録されたコンピュータ読取可能な情報記録媒体であって、認証情報82は所定の暗号化方式により暗号化された状態で記録されており、認証情報82の記録アドレスには、コンテンツ情報81の記録アドレスを用いて所定の演算を行うことによって得られた値が設定されている。

30

【0096】

所定の演算の内容は、コンテンツ情報81が異なれば、ほぼ常に演算結果が異なるように構成することが好ましい。例えば、コンテンツ情報81の記録終了アドレスに、コンテンツ情報81のサイズを一定値で割った値を加え、その結果得られる値を、認証情報82の記録開始アドレスに設定することとしてもよい。

【0097】

このような情報記録構造を有する第1情報記録媒体80によれば、認証情報82のアドレスがコンテンツ情報81のアドレスに基づいて決定されるので、所定の演算方法を知らない者が認証情報82のアドレスを知ることがきわめて困難である。また、コンテンツ情報81が変われば認証情報82のアドレスが変わるため、認証情報82のアドレスを知ることはいっそう困難となる。したがって、上述した第1ないし第5情報処理装置（特に第4情報処理装置）と組み合わせることにより、不法コピー等に対する情報の保護を強化することができる。

40

【0098】

また、認証情報82の記録アドレスを、コンテンツ情報81の記録されている領域、すなわち通常の情報記録領域内（特別の機能を備えた読取装置又は記録装置等しかアクセスできないようなディスクの最内周側などではなく、通常の読取装置又は記録装置等によりア

50

クセス可能な領域内)に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。なぜなら、この場合には、通常の読取装置や通常の記録装置ではアクセスすることができない領域にアクセスするための専用の機構が不要となるからである。

【0099】

(情報記録媒体の第2実施形態)

本発明に係る情報記録媒体の第2実施形態(以下、これを「第2情報記録媒体」という。)について図9を参照して説明する。図9は第1情報記録媒体の情報記録構造を示している。なお、図9は、第2情報記録媒体90の具体例として、層L1及び層L2の2層の情報記録媒体を例示しているが、3層以上の情報記録媒体でもよい。

10

【0100】

図9に示すように、第2情報記録媒体90は、コンテンツ情報91とこのコンテンツ情報91が真正なものであることを示すための認証情報92とが記録されたコンピュータ読取可能な多層情報記録媒体であって、コンテンツ情報91は第2情報記録媒体90のいずれかの層(例えば層L1)に記録されており、認証情報92は、所定の暗号化方式で暗号化された状態で、第2情報記録媒体90の層のうちコンテンツ情報91を記録する層以外のいずれかの層(例えば層L2)に記録されている。

【0101】

このような情報記録構造を有する第2情報記録媒体90によれば、上述した第1ないし第5情報処理装置(特に第5情報処理装置)と組み合わせることにより、不法コピー等に対して情報の保護を強化することができる。例えば、情報を不法にコピーしようとする者が、第2情報記録媒体90に記録された情報を、1層の情報記録媒体にコピーしようとする場合には、1の層(L1)に記録されたコンテンツ情報91のみを1層の情報記録媒体にコピーすることができたとしても、他の層(L2)に記録された認証情報92はコピーすることができない。なぜなら、コピー先の情報記録媒体は1層であるため、コンテンツ情報91を記録してしまえば、認証情報92を記録する領域がないからである。確かに、コンテンツ情報91のデータサイズが小さければ、認証情報92を記録する領域があるかもしれない。しかし、この場合には、コピーした結果、認証情報92の記録された層もアドレスも変わってしまうため、第4情報処理装置又は第5情報処理装置により、少なくともコンテンツ情報91が実行又は再生されることはない。

20

30

【0102】

また、コンテンツ情報91を第2情報記録媒体90の第1層に記録し、認証情報92を第2情報記録媒体90の第2層以降のいずれかの層に記録すれば、製造時の検査作業等において都合がよい。すなわち、第2情報記録媒体90の第1層に記録された情報は、通常、最初に再生されるので、製造時の検査作業等を迅速に行うことができる。

【0103】

また、認証情報92を、通常の情報記録領域内(多層情報記録媒体用の通常の読取装置又は記録装置等によりアクセス可能な領域内)に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。

【0104】

また、認証情報92を、当該認証情報を記録すべき層に形成された情報記録領域内の中間部分又は後半部分に記録すれば、不法コピーをしようとする者に対して、認証情報92を見つけにくくすることができる。

40

【0105】

(情報処理方法の実施形態)

本発明に係る情報処理方法の実施形態について説明する。本発明の実施形態に係る情報処理方法は、情報を再生又は実行するための情報処理方法であって、情報を取得する取得工程と、取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定工程と、暗号化判定工程における判定の結果、取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含

50

まれていないときには、取得工程における情報の少なくとも一部のさらなる取得を阻止する旨の制御命令、又は取得工程において取得された情報の少なくとも一部につき、実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する制御工程と、取得手段において取得された情報の再生処理又は実行処理を行い、これにより再生又は実行された情報を出力する処理工程とを備え、制御工程において制御指令が発せられたときには、取得工程において情報の少なくとも一部のさらなる取得を行わず、又は処理工程において実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない。

【0106】

より具体的に説明すると、情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンピュータプログラム、ゲームプログラム、映画データ、音楽データ等のコンテンツ情報に、所定の暗号化方式により暗号化された認証情報を付加する。なお、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付加するのではなく、コンテンツ情報自体を所定の暗号化方式で暗号化してもよい。さて、取得工程において情報を取得し、その情報の中に、所定の暗号化方式により暗号化された認証情報又は所定の暗号化方式により暗号化されたコンテンツ情報が含まれているときには、処理工程において、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。なお、このとき、取得工程において取得された情報がさらに他の1つ又はいくつかの条件を満たしている場合に限り、処理工程において再生処理又は実行処理を行うようにしてもよい。

【0107】

一方、取得工程において取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれていないときには、暗号化判定工程においてその旨を判定し、第1制御工程において、少なくともコンテンツ情報のこれ以上の取得を行わず、又は少なくともコンテンツ情報の実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する。この結果、取得工程又は処理工程における取得、再生、実行等の処理が、第1制御工程において発せられた制御指令に従って阻止、中止又は無効とされ、これにより、少なくともコンテンツ情報は実行されず、再生されず又は出力されない。したがって、所定の暗号化方式で暗号化されていないコンテンツ情報は再生されず、実行されず、出力されない。

【0108】

このような情報処理方法によれば、取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、情報の少なくとも一部につき実行せず、再生せず又は出力しない構成としたから、不法コピー等に対する情報の保護を強化することができると共に、不法コピー等に対する情報の保護を低コストで実現することができる。

【0109】

なお、以上のような実施形態は、専用の装置としてハードウェアと一体的に構成する形態で実現してもよいし、コンピュータにプログラムを読み込ませることによって実現してもよい。

【0110】

【実施例】

以下、本発明の実施例を図面に基づいて説明する。以下の実施例は、本発明に係る情報処理装置を家庭用ゲーム装置に適用した例である。

【0111】

まず、本発明の実施例に係るゲーム装置について図10を参照して説明する。図10は本発明の実施例に係るゲーム装置の構成を示している。

【0112】

図10に示すように、ゲーム装置100は、DVD-ROM110に記録されたゲームプログラムを実行する装置である。ゲーム装置100は、DVD-ROMドライブ101、CPU102、メモリ103及びデコードモジュール104を備えており、これらはバス

10

20

30

40

50

105を介して相互に接続されている。また、バス105にはゲーム用コントローラ106が接続され、デコードモジュール104には、ディスプレイ107及びスピーカ108が接続されている。

【0113】

DVD-ROMドライブ101は、ゲームプログラム112、認証情報113等が記録されたDVD-ROM110（図11参照）から、ゲームプログラム112、認証情報113等を読み取る情報読取装置である。DVD-ROMドライブ101は、CSSに準拠しており、デコードモジュール104と共に、CSS暗号化された情報の復号化（暗号化の解除）をする機能を備えている。

【0114】

CPU102は、ゲーム装置100の全体的な制御を行うと共に、ゲームプログラム及び後述する実行許否判定処理等を実行する。

【0115】

メモリ103は、例えばリードオンリメモリであり、実行許否判定処理プログラムの他、各種プログラム、データを格納している。

【0116】

デコードモジュール104は、例えばMPEGデコードモジュールであり、MPEG圧縮された画像情報等をデコードし、再生するモジュールである。デコードモジュール104は、デコード回路の他、デジタルアナログ変換回路等を備えている。さらに、デコードモジュール104は、CSSに準拠しており、DVD-ROMドライブ101と共に、CSS暗号化された画像情報を復号化する機能を備えている。後述するように、認証情報113はDVDビデオフォーマットを有し、かつCSS暗号化された画像情報である。デコードモジュール104は、この認証情報113を復号化してその内容を認識するために用いられる。なお、当該ゲーム装置100が、DVD-ROMに記録されたゲームプログラムを実行するだけでなく、DVDビデオディスクに記録された映画等を再生する機能を兼ね備えている場合には、デコードモジュール104により、DVDビデオフォーマットを有し、かつCSS暗号化された映画データ等を復号化して再生することができる。

【0117】

このような構成を有するゲーム装置100は、以下のように動作する。ユーザがDVD-ROM110をDVD-ROMドライブ101に装着すると、DVD-ROMドライブ101は、DVD-ROMドライブ101のファイルシステム情報111等にアクセスし、続いてDVD-ROM110に記録されたゲームプログラム112、認証情報113等を読み取る。この読取動作とほぼ同時に、CPU102は、DVD-ROMドライブ101及びデコードモジュール104と協働して、実行許否判定処理を行う。実行許否判定処理において、CPU102は、DVD-ROM110に記録されたゲームプログラム112等が真正のものか、すなわち不法にコピーされたものでないかを判定する。実行許否判定処理の結果、ゲームプログラム112が真正のものであるときには、CPU102は、ゲームプログラム112を実行する。一方、ゲームプログラム112が真正のものでないときには、CPU102は、ゲームプログラム112の実行を行わない。

【0118】

次に、DVD-ROM110に記録された情報の記録構造について図11を参照して説明する。図11はDVD-ROM110に記録された情報の記録構造を示している。なお、図11中の左側がDVD-ROMディスクの内周側であり、右側がDVD-ROMディスクの外周側である。

【0119】

図11に示すように、DVD-ROM110は、シングルレイヤータイプのDVD-ROMディスクであり、その内周側にはリードイン領域A1が形成され、その外周側にボリューム領域A2が形成され、さらにその外周側にリードアウト領域A3が形成されている。

【0120】

ボリューム領域A2は、DVD-ROMディスクに記録された情報を読み取る機能を有す

10

20

30

40

50

る一般ユーザ向けの情報読取装置（DVD-ROMドライブ101もこれに含まれる）を通常の方法で操作することによって任意にアクセスすることができる通常の情報記録領域である。一方、リードイン領域A1及びリードアウト領域A3は、DVD-ROMディスクに記録された情報を読み取る機能を有する一般ユーザ向けの情報読取装置を通常の方法で操作することによって任意にアクセスすることができない情報記録領域である。もっとも、リードイン領域A1及びリードアウト領域A3は、ユーザが任意にアクセスすることができない領域ではあるが、上記一般ユーザ向けの情報読取装置によって全くアクセスすることができない領域ではない。すなわち、当該情報読取装置のピックアップはリードイン領域A1又はリードアウト領域A3まで移動することができ、情報読取装置の内部プログラムによってリードイン領域A1又はリードアウト領域A3のアドレスを指定すれば、それらの領域にアクセスすることができる。なお、DVDには、リードイン領域のさらに内周側には若干の非記録領域が存在するが、この非記録領域は、上記一般ユーザ向けの情報読取装置によってアクセスすることはできず、この領域にアクセスさせるためには、情報読取装置に特別の機能を付加しなければならない。

10

20

30

40

50

【0121】

DVD-ROM110のボリウム領域A2内には、その内周側にファイルシステム情報111が記録されている。ファイルシステム情報111は、ボリウム領域A2内に記録されている情報を管理するための情報であり、これには、このファイルシステム情報111に続いてボリウム領域A2内に記録されている個々の情報の名前、記録アドレス、データサイズ、データフォーマット、暗号化の有無等を示す情報が含まれている。

【0122】

また、ボリウム領域A2内には、ファイルシステム情報111に続いて、ゲームプログラム112が記録されている。ゲームプログラム112は、例えば対戦ゲーム、シューティングゲーム、野球ゲーム、ロールプレイングゲーム等を実現するためのコンピュータプログラムである。ゲームプログラム112は、暗号化されていない状態で記録されている。また、ゲームプログラム112は、プログラムなので、DVDビデオフォーマットではない。なお、ゲームの内容によっては、ゲームプログラムだけでなく、ゲームを再現するための画像情報や音声情報をDVD-ROM110に記録することができる。この場合には、画像情報及び音声情報をDVDビデオフォーマット（DVDオーディオフォーマットでもよい）で記録することができる。また、この場合、画像情報及び音声情報をCSS暗号化（CPM暗号化）して記録してもよい。

【0123】

さらに、ボリウム領域A2内には、認証情報113が記録されている。認証情報113は、例えば、ディスク製造業者のロゴを表した画像に対応した画像情報である。認証情報113のフォーマットは、DVDビデオフォーマットである。さらに、認証情報113は、情報を製作又は提供する適法な権限を有するディスク製造業者により、当該DVD-ROMディスクを製造する過程で、CSS暗号化されて記録されている。

【0124】

DVD-ROM110のリードイン領域A1内には、マスタ鍵を用いて暗号化されたディスク鍵が記録されている。この鍵はCSS暗号化・復号化時に用いられるものである。この暗号化されたディスク鍵は、リードイン領域A1内に記録されているので、ユーザが任意に読み取ることができないが、一般ユーザ向けの情報読取装置の内部的制御にしたがって（内蔵の制御プログラムによって）読み取ることが可能である。

【0125】

次に、認証情報113の暗号化・復号化に用いられる暗号化方式であるCSSについて説明する。なお、以下のCSSの説明では、いったん実施例に係るゲーム装置100を離れ、一般的な視点から説明する。

【0126】

CSSは、主として映画ソフトをDVDコンテンツとして提供する場合に、映画ソフトの著作権を保護することを目的として開発された情報暗号化技術であり、周知の技術である

。DVDに記録すべきコンテンツ情報の暗号化は、タイトル鍵、ディスク鍵、マスタ鍵の3つの鍵を用いて行われる。まず、DVDに記録すべきコンテンツ情報は、圧縮（例えばMPEG圧縮）等の処理を経た後、タイトル鍵を用いてスクランブルされる。次に、タイトル鍵は、ディスク鍵を用いて暗号化され、暗号化されたタイトル鍵は、DVD上のセクターヘッダ領域に記録される。セクターヘッダ領域は、ユーザが任意にアクセスすることができない領域である。次に、ディスク鍵は、マスタ鍵を用いて暗号化され、暗号化されたディスク鍵は、DVD上のリードイン領域に記録される。

【0127】

DVDに暗号化されて記録されたコンテンツ情報を再生装置等によって再生する場合には、再生装置等がCSS準拠のものでなければならない。DVDに暗号化されて記録されたコンテンツ情報をCSS準拠の再生装置等により再生するときには、以下に述べる復号化プロセスが行われる。すなわち、CSS準拠の再生装置等は、マスタ鍵を予め秘密に保持している。まず、再生装置等は、DVD上のリードイン領域に暗号化されて記録されているディスク鍵を読み取り、これを、自ら秘密に保持しているマスタ鍵を用いて復号化し、取得する。次に、再生装置等は、DVD上のセクターヘッダ領域に暗号化されて記録されているタイトル鍵を読み取り、これを、先ほどDVDから取得したディスク鍵を用いて復号化し、取得する。次に、再生装置等は、DVD上にスクランブルがかけられた状態で記録されたコンテンツ情報を読み取り、これを、先ほどDVDから取得したタイトル鍵を用いてデスクランブルする。そして、再生装置等は、デスクランブルされたコンテンツ情報を再生する。例えば、コンテンツ情報が圧縮されているデジタル映像であるときには、再生装置等は、内蔵しているデコーダ（例えばMPEGデコーダ）によって、コンテンツ情報をデコードし、これをデジタルーアナログ変換してディスプレイ等に出力する。

【0128】

また、DVDに暗号化されて記録されているコンテンツ情報を汎用コンピュータによって再生するためには、汎用コンピュータが備えているDVD-ROMドライブ及びデコードモジュール（例えばMPEGデコードモジュール）がいずれもCSS準拠のものでなければならない。DVDに暗号化されて記録されているコンテンツ情報を、CSS準拠のDVD-ROMドライブ及びCSS準拠のデコードモジュールを備えた汎用コンピュータによって再生するときには、上述した復号化プロセスに加えて、以下に述べるパス認証プロセスが行われる。すなわち、DVDに暗号化されて記録されているコンテンツ情報に対して上述した復号化プロセスを実行する前に、DVD-ROMドライブとデコードモジュールとの間でパス認証が実行される。具体的には、DVD-ROMドライブとデコードモジュールはコンピュータのバスを介して相互に接続されており、このバスを介して両者間で互いにCSS準拠であることの確認が行われる。このとき、DVD-ROMドライブとデコードモジュールとの間で、両者のみが認識し得る時変鍵が作り出される。その後、DVD-ROMドライブとデコードモジュールとによって、上述した復号化プロセスが実行される。この復号化プロセスの中で、DVD-ROMドライブがデコードモジュールへ、タイトル鍵又はディスク鍵を渡すときには、その鍵は時変鍵により暗号化される。そして、デコードモジュールがDVD-ROMドライブから渡された鍵を利用するときには、その鍵は時変鍵を用いて復号化される。

【0129】

本実施例に係るゲーム装置100は、CSS準拠のDVD-ROMドライブ101及びCSS準拠のデコードモジュール104を備えており、CSS暗号化されてDVD-ROM110に記録された認証情報を復号化することができる。復号化の際には、DVD-ROM110のリードイン領域A1に記録されたディスク鍵114が用いられる。

【0130】

次に、ゲーム装置100における実行可否判定処理について図12を参照して説明する。実行可否判定処理は、DVD-ROM110に記録されたゲームプログラム112が真正のものか、すなわち不法にコピーされたものでないかを判定し、その判定結果に基づいて、ゲームプログラム112を実行するか実行しないかの制御を行う処理である。この実行

許否判定処理はCPU102の制御のもとで行われる。

【0131】

図12に示すように、DVD-ROMドライブ101にDVD-ROM110が装着されると(ステップS1: YES)、CPU102は、DVD-ROM110のボリューム領域A2内にDVDビデオフォーマットを有する情報が記録されているか否かを判定する(ステップS2)。ファイルシステム情報111内には、ボリューム領域A2内に記録されている個々の情報(ファイル)の名前が記述されており、情報の名前には、フォーマットごとに異なる拡張子が付加されている。したがって、ボリューム領域A2内にDVDビデオフォーマットを有する情報が記録されているか否かの判定は、ファイルシステム情報111内に記述された情報の拡張子を調べることにより実現することができる。

10

【0132】

ボリューム領域A2内にDVDビデオフォーマットを有する情報が記録されていないときには(ステップS2: NO)、CPU102は、ゲームプログラム112の実行を拒絶するための制御を行う(ステップS9)。この結果、ゲームプログラム112は実行されない。

【0133】

一方、ボリューム領域A2内にDVDビデオフォーマットを有する情報が記録されているときには(ステップS2: YES)、CPU102は、続いて、DVDビデオフォーマットを有する情報の中に、CSS暗号化された情報があるか否かを判定する(ステップS3)。CSS暗号化された情報があるか否かの判定は、リードイン領域A1に記録されたフ

20

【0134】

DVDビデオフォーマットを有する情報の中に、CSS暗号化された情報がないときには(ステップS3: NO)、CPU102は、ゲームプログラム112の実行を拒絶するための制御を行う(ステップS9)。この結果、ゲームプログラム112は実行されない。

【0135】

一方、DVDビデオフォーマットを有する情報の中に、CSS暗号化された情報があるときには(ステップS3: YES)、CPU102は、DVD-ROMドライブ101及びデコードモジュール104と協働して、CSS暗号化された情報を復号化する(ステップS4)。

30

【0136】

続いて、CPU102は、復号化された情報が認証情報113か否かを判定する(ステップS5)。この判定は、復号化された情報のチェックサムを求め、これを予めメモリ103に記録された基準値と比較することによって行う。復号化された情報のチェックサムの値と基準値とが一致したときに限り、復号化された情報が認証情報113であると判定する。

【0137】

復号化された情報が認証情報113でないときには(ステップS5: NO)、CPU102は、ゲームプログラム112の実行を拒絶するための制御を行う(ステップS9)。この結果、ゲームプログラム112は実行されない。

40

【0138】

一方、復号化された情報が認証情報113であるときには(ステップS5: YES)、CPU102は、続いて、認証情報113の基準アドレスを算出する(ステップS6)。ディスク製造業者は、DVD-ROM110の製造過程において、DVD-ROM110にゲームプログラム112及び認証情報113を記録するとき、ゲームプログラム112の記録アドレスを用いて所定の演算を行い、その演算の結果得られた値を、認証情報113の記録アドレスに設定している。具体的には、ゲームプログラム112の記録終了アドレスに、ゲームプログラム112のサイズを一定値で割った値を加え、その結果得られる値を、認証情報113の記録開始アドレスに設定している。したがって、DVD-ROM101のボリューム領域A2内において、認証情報113が記録されているアドレスは、前

50

記所定の演算を行うことによって得ることができる。そこで、ステップS6で、CPU102は、上記所定の演算を行い、その結果得られた値を、基準アドレスとして取得する。

【0139】

続いて、CPU102は、DVD-ROM110に実際に記録されている認証情報113の現実の記録開始アドレスを検出し、この現実の記録開始アドレスと基準アドレスとを比較する。このようにして、CPU102は、現実の記録開始アドレスが基準アドレスに一致するか否かを判定する（ステップS7）。

【0140】

現実の記録開始アドレスが基準アドレスに一致しないときには（ステップS7：NO）、CPU102は、ゲームプログラム112の実行を拒絶するための制御を行う（ステップS9）。この結果、ゲームプログラム112は実行されない。 10

【0141】

一方、現実の記録開始アドレスが基準アドレスに一致したときには（ステップS7：YES）、CPU102は、ゲームプログラム112の実行を許可するための制御を行う（ステップS8）。

【0142】

このように、本実施例に係るゲーム装置100によれば、DVDビデオフォーマットを有し、CSS暗号化され、かつ、所定のチェックサムを有する認証情報113が、DVD-ROM110のボリューム領域A2内の所定のアドレスに記録されている場合に限り、ゲームプログラム112の実行が許可される。すなわち、（i）ディスク上に認証情報が存在しない場合、（ii）ディスク上に認証情報が存在していてもそれがDVDビデオフォーマットでない場合、（iii）認証情報がCSS暗号化されていない場合、又は、（iv）認証情報が上記所定の演算で算出される所定のアドレスとは異なるアドレスに記録されている場合には、ゲームプログラム112は実行されない。したがって、不法コピー等に対して、ゲームプログラム112を強力に保護することができる。 20

【0143】

確かに、不法コピーをしようとする者が、一般に市販されているブランクのDVD-R等の上に、DVD-ROM110に記録された情報のすべてを全くそのままコピーすれば、このようにして不法コピーされたゲームプログラムは、ゲーム装置100で再生することができてしまう。しかし、これはほとんど不可能である。なぜなら、上述したように、仮に認証情報のCSS暗号化を解くことができたとしても、それを再びCSS暗号化することはほとんど不可能であるし、また、CSS暗号化された認証情報をセクタごとにそのまま転写してコピーディスクを作り出すことはCSSの構造上ほとんど不可能だからである。 30

【0144】

さらに、本実施例に係るゲーム装置100によれば、認証情報113の正しい記録アドレスが、ゲームプログラム112の記録終了アドレス及びサイズに基づいて決定されるので、ゲームプログラム112の記録位置又はサイズが異なれば、認証情報113の正しい記録アドレスも変化する。このことから、不法なコピーディスクの作成はより一層困難となり、ゲームプログラムの保護をより一層強化することができる。 40

【0145】

さらに、本実施例に係るゲーム装置100によれば、一般に用いられる情報読取装置又は情報記録装置によって通常にアクセスすることが可能なボリューム領域A2に、認証情報113を記録し、その認証情報113を検出して所定の判定処理を行うことで、ゲームプログラム112の実行の許否を決定することができる。また、一般に広く知られているCSSを認証情報113の暗号化方式として採用している。このため、コピープロテクトを実現するのに、専用のディスク製造装置や専用の情報読取装置は不要である。したがって、不法コピー等に対するゲームプログラム112の保護を低コストで実現することができる。 50

【0146】

なお、本発明は、請求の範囲および明細書全体から読み取るこのできる発明の要旨または思想に反しない範囲で適宜変更可能であり、そのような変更を伴うゲーム装置、情報処理装置、情報記録装置、情報処理方法及びこれらの機能を実現するコンピュータプログラム並びに情報記録媒体もまた本発明の技術思想に含まれる。

【図面の簡単な説明】

- 【図 1】 本発明に係る情報処理装置の第 1 実施形態を示すブロック図である。
- 【図 2】 本発明に係る情報処理装置の第 2 実施形態を示すブロック図である。
- 【図 3】 本発明に係る情報処理装置の第 3 実施形態を示すブロック図である。
- 【図 4】 本発明に係る情報処理装置の第 4 実施形態を示すブロック図である。
- 【図 5】 本発明に係る情報処理装置の第 5 実施形態を示すブロック図である。
- 【図 6】 本発明に係る情報記録装置の第 1 実施形態を示すブロック図である。
- 【図 7】 本発明に係る情報記録装置の第 2 実施形態を示すブロック図である。
- 【図 8】 本発明に係る情報記録媒体の第 1 実施形態を示すブロック図である。
- 【図 9】 本発明に係る情報記録媒体の第 2 実施形態を示すブロック図である。
- 【図 10】 本発明の実施例に係るゲーム装置を示すブロック図である。
- 【図 11】 本発明の実施例に係る DVD-ROM を示す説明図である。
- 【図 12】 本発明の実施例に係る実行可否判定処理を示すフローチャートである。

10

【符号の説明】

10、20、30、40、50…情報処理装置

11…取得手段

12…処理手段

13…暗号化判定手段

14…第 1 制御手段

21…フォーマット判定手段

22…第 2 制御手段

31…復号化手段

32…認証情報判定手段

33…第 3 制御手段

41…アドレス判定手段

42…第 4 制御手段

51…記録層判定手段

52…第 5 制御手段

60、70…情報記録装置

61…アドレス取得手段

62…アドレス設定手段

63、72…暗号化手段

64…記録手段

71…第 1 記録手段

73…第 2 記録手段

80、90…情報記録媒体

81、91…コンテンツ情報

82、92、113…認証情報

100…ゲーム装置

101…DVD-ROMドライブ

102…CPU

104…デコードモジュール

110…DVD-ROM

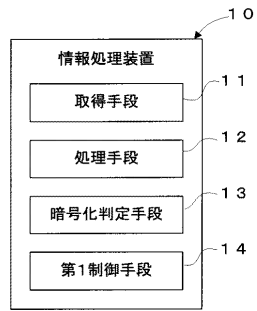
112…ゲームプログラム

20

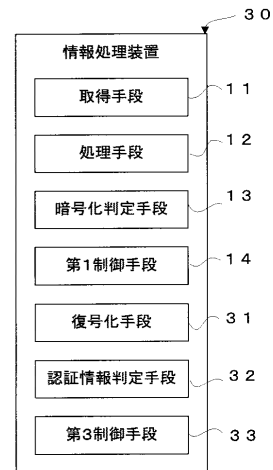
30

40

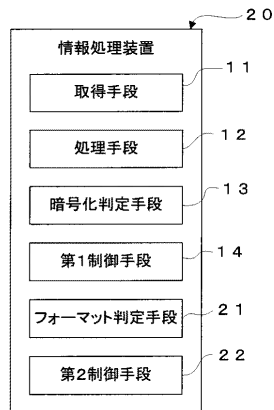
【図 1】



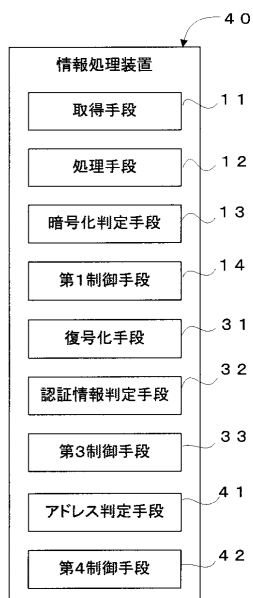
【図 3】



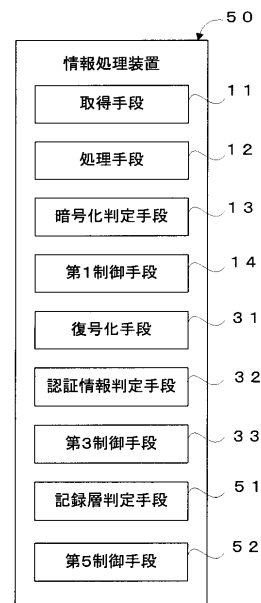
【図 2】



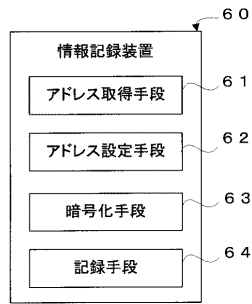
【図 4】



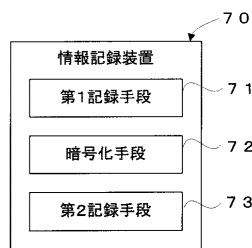
【図 5】



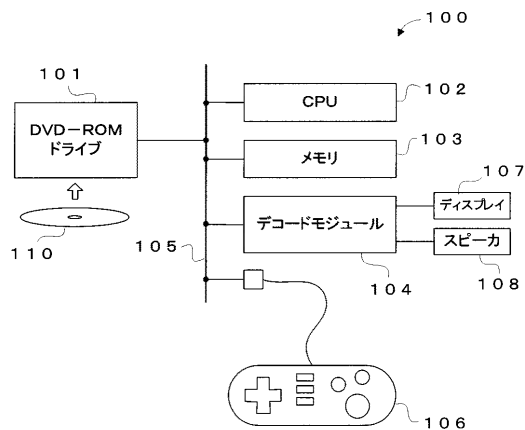
【図 6】



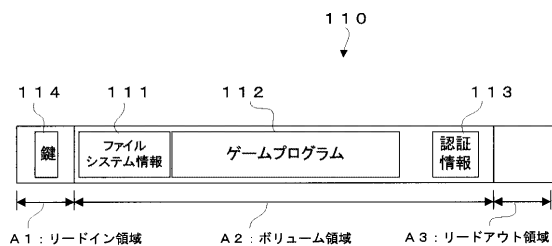
【図 7】



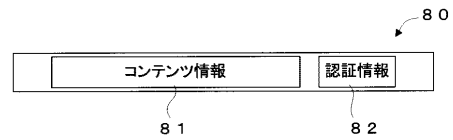
【図 10】



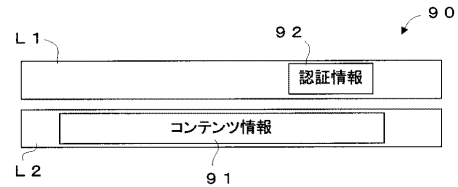
【図 11】



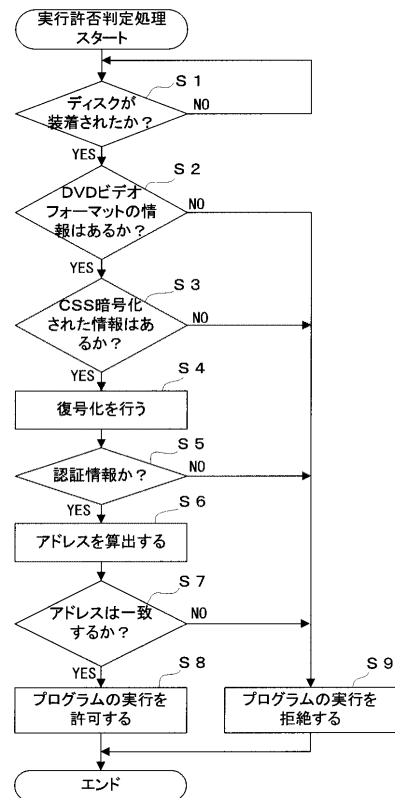
【図 8】



【図 9】



【図 12】



フロントページの続き

(72)発明者 仁田 聡

埼玉県所沢市花園4丁目2610番地 パイオニア株式会社所沢工場内

Fターム(参考) 5B017 AA06 BA09 CA09 CA16

5D044 BC04 CC04 DE17 DE50 EF05 FG18 GK17

5J104 AA12