(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2009-277308
(P2009-277308A)
(43)公開日　平成21年11月26日(2009.11.26)

(51)Int.Cl.		F I			テーマコード（参考）
G11B 20/10	(2006.01)	G11B	20/10	H	5B017
G11B 20/12	(2006.01)	G11B	20/12		5C053
G06F 21/24	(2006.01)	G11B	20/10	301Z	5D044
H04N 5/93	(2006.01)	G06F	12/14	560C	
		H04N	5/93	Z	

審査請求 未請求　請求項の数 20　ＯＬ　（全 29 頁）

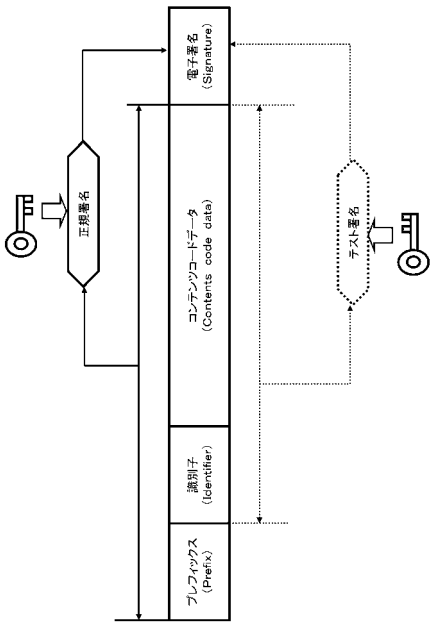
(21)出願番号　特願2008-129140 (P2008-129140)
(22)出願日　平成20年5月16日 (2008.5.16)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(72)発明者　山本　和夫
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体、および情報処理方法、並びにプログラム

(57)【要約】
【課題】コンテンツコードファイルの作成やディスク製造を効率的に実行することを可能とした構成を実現する。
【解決手段】コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードの作成、試験において、一般のユーザの再生装置と同様、コンテンツコードファイルに設定した署名検証処理を実行し、署名検証に成功したことを条件としてコンテンツ再生試験を行う。初期的な再生試験において、正規署名とは異なるデータ領域に対してテスト署名を設定したコンテンツコードファイルをＲ／ＲＥ型のディスクに記録して署名検証および再生試験を実行する。その後、正規署名を設定したコンテンツコードファイルをＲＯＭディスクに記録して試験を行う。本構成により、効率的なコンテンツコードの生成やディスク製造が実現される。
【選択図】図６



【特許請求の範囲】
【請求項１】
コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する再生処理部と、
前記コンテンツコードファイルに設定された電子署名の検証処理を実行する署名検証部を有し、
前記署名検証部は、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行し、
前記再生処理部は、
前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行する構成である情報処理装置。
【請求項２】
前記コンテンツコードファイルは、
固定データ領域と、非固定データ領域を含み、
前記署名検証部は、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記固定データ領域と、非固定データ領域を署名対象データとした正規署名に対する署名検証処理を実行し、
非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記非固定データ領域を署名対象データとしたテスト署名に対する署名検証処理を実行する構成である請求項１に記載の情報処理装置。
【請求項３】
前記コンテンツコードファイルは、
コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードの属性情報と、前記コンテンツコードを含むファイルであり、
前記署名検証部は、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記プレフィックスと属性情報とコンテンツコードを署名対象データとした正規署名に対する署名検証処理を実行し、
非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行する構成である請求項１に記載の情報処理装置。
【請求項４】
前記プレフィックスは固定されたビットデータによって構成される固定データ領域である請求項３に記載の情報処理装置。
【請求項５】
前記非ＲＯＭディスクはデータ追記可能なＲ型またはＲＥ型のディスクである請求項１に記載の情報処理装置。
【請求項６】
コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを構成するデータ構造であり、
コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードファイルの属性情報と、前記コンテンツコードと、電子署名を有し、
前記電子署名は、前記属性情報と前記コンテンツコードを署名対象データとして設定されたテスト署名であり、
情報処理装置におけるＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署

名に対する署名検証処理を実行させることを可能としたデータ構造。
【請求項７】
コンテンツと、
コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを格納し、
前記コンテンツコードファイルは、
コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードの属性（サイズ等）を示す情報属性情報と、前記コンテンツコードと、電子署名を有し、
前記電子署名は、前記属性情報と前記コンテンツコードを署名対象データとして設定されたテスト署名であり、
情報処理装置におけるＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行させることを可能とした情報記録媒体。
【請求項８】
コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを生成するコンテンツコード生成部と、
前記コンテンツコードファイルに対する電子署名の設定依頼を実行する署名依頼部と、
署名の設定されたコンテンツコードファイルとコンテンツをディスクに記録するデータ記録部と、
コンテンツと、コンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する再生処理部と、
前記コンテンツコードファイルに設定された電子署名の検証処理を実行する署名検証部を有し、
前記署名検証部は、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行し、
前記再生処理部は、
前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行する構成である情報処理装置。
【請求項９】
前記コンテンツコードファイルは、
固定データ領域と、非固定データ領域を含み、
前記署名検証部は、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記固定データ領域と、非固定データ領域を署名対象データとした正規署名に対する署名検証処理を実行し、
ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記非固定データ領域を署名対象データとしたテスト署名に対する署名検証処理を実行する構成である請求項８に記載の情報処理装置。
【請求項１０】
前記コンテンツコードファイルは、
コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードファイルの属性情報と、前記コンテンツコードを含むファイルであり、
前記署名検証部は、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記プレフィックスと属性情報とコンテンツコードを署名対象データとした正規署名に対する署名検証処理を実行し、
ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、

前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行する構成である請求項８に記載の情報処理装置。
【請求項１１】
前記プレフィックスは固定されたビットデータによって構成される固定データ領域である請求項１０に記載の情報処理装置。
【請求項１２】
前記非ＲＯＭディスクはデータ追記可能なＲ型またはＲＥ型のディスクである請求項８に記載の情報処理装置。
【請求項１３】
コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルに対する電子署名を生成する電子署名生成部を有し、
前記電子署名作成部は、
署名作成依頼の種類に応じて、署名対象データを異なる設定とした署名生成処理を実行する情報処理装置。
【請求項１４】
前記コンテンツコードファイルは、
固定データ領域と、非固定データ領域を含み、
前記署名生成部は、
正規署名生成依頼に対しては、前記固定データ領域と、非固定データ領域を署名対象データとした署名生成処理を実行し、
テスト署名生成依頼に対しては、前記非固定データ領域を署名対象データとした署名生成処理を実行する構成である請求項１３に記載の情報処理装置。
【請求項１５】
前記コンテンツコードファイルは、
コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードファイルの属性情報と、前記コンテンツコードを含むファイルであり、
前記署名生成部は、
正規署名生成依頼に対しては、前記プレフィックスと前記属性データとコンテンツコードを署名対象データとした署名生成処理を実行し、
テスト署名生成処理依頼に対しては、属性データとコンテンツコードを署名対象データとした署名生成処理を実行する構成である請求項１３に記載の情報処理装置。
【請求項１６】
情報処理装置において実行する情報処理方法であり、
再生処理部が、コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する再生処理ステップと、
署名検証部が、前記コンテンツコードファイルに設定された電子署名の検証処理を実行する署名検証ステップを有し、
前記署名検証ステップは、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行するステップであり、
前記再生処理ステップは、
前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行するステップである情報処理方法。
【請求項１７】
ディスク製造装置において実行するディスク製造方法であり、

コンテンツコード生成部が、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを生成するコンテンツコード生成ステップと、
データ記録部が、前記コンテンツコードファイルに対する電子署名であるテスト署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスク以外の非ＲＯＭディスクに記録する第１のデータ記録ステップと、
署名検証部が、前記コンテンツコードファイルのテスト署名に対する署名検証処理を実行する第１の署名検証ステップと、
前記非ＲＯＭディスクに記録されたコンテンツと、テスト署名の設定されたコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する第１の再生処理ステップと、
前記データ記録部が、前記第１の再生処理ステップにおける再生処理の成功を条件として、前記コンテンツコードファイルに対する電子署名として、前記テスト署名と異なるデータ領域を署名対象とした正規署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスクに記録する第２のデータ記録ステップと、
署名検証部が、前記コンテンツコードファイルの正規署名に対する署名検証処理を実行する第２の署名検証ステップと、
前記ＲＯＭディスクに記録されたコンテンツと、正規署名の設定されたコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する第２の再生処理ステップと、
マスターディスク製造部が、前記第２の再生処理ステップにおける再生処理成功を条件として、コンテンツと、正規署名の設定されたコンテンツコードファイルを記録データとして設定したマスターディスクを製造するマスターディスク製造ステップと、
ディスク製造部が、前記マスターディスク製造ステップにおいて製造したマスターディスクを適用してディスクの製造を行うディスク製造ステップを有するディスク製造方法。
【請求項１８】
前記コンテンツコードファイルは、
固定データ領域と、非固定データ領域を含み、
前記第１のデータ記録ステップは、前記非固定データ領域を署名対象データとしたテスト署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスク以外の非ＲＯＭディスクに記録するステップであり、
前記第２のデータ記録ステップは、前記固定データ領域と非固定データ領域を署名対象データとした正規署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスクに記録するステップである請求項１７に記載のディスク製造方法。
【請求項１９】
前記非ＲＯＭディスクはデータ追記可能なＲ型またはＲＥ型のディスクである請求項１７に記載のディスク製造方法。
【請求項２０】
情報処理装置において情報処理を実行させるプログラムであり、
再生処理部に、コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出させて、コンテンツ再生処理を実行させる再生処理ステップと、
署名検証部に、前記コンテンツコードファイルに設定された電子署名の検証処理を実行させる署名検証ステップを有し、
前記署名検証ステップは、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行させるステップであり、
前記再生処理ステップは、

前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行させるステップであるプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理装置、情報記録媒体、および方法、並びにプログラムに関する。さらに、詳細には、コンテンツの利用制御プログラムなどを含みコンテンツと共に情報記録媒体に記録され、コンテンツ再生時に利用されるコンテンツコードファイルを利用した処理を行う情報処理装置、情報記録媒体、および方法、並びにコンピュータ・プログラムに関する。

【背景技術】

【０００２】

映画、音楽など様々なコンテンツの記録媒体としてＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）や、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）などのディスクが利用される。これらのディスクに記録されたコンテンツの多くは、コンテンツ作成者や販売者に著作権、頒布権等が保有されており、不正利用を防止するための利用制御がなされる。

【０００３】

例えばディスク記録コンテンツの不正コピーの防止や、コピー回数制限などを実行するための制御プログラムやシステムが利用される。また、コンテンツを暗号化してディスクに格納し、正当なコンテンツ利用権を持つユーザや機器のみが取得できる鍵を設定するといった利用制御手法も利用されている。なお、コンテンツの暗号化によるコンテンツ利用制御構成については、例えば特許文献１に記載されている。

【０００４】

しかし、コンテンツを暗号化しても、暗号鍵の漏洩が発生してしまうと、不正に復号されたコンテンツが流出するという問題が発生する。このような問題を解決する１つの構成を開示した従来技術として、特許文献２に記載の構成がある。特許文献２は、コンテンツの一部をダミーデータに置き換えて記録することで、コンテンツの不正再生を防止した構成を開示している。

【０００５】

コンテンツをダミーデータに置き換えたコンテンツの再生処理に際しては、ダミーデータを正常なコンテンツデータに再度、置き換える処理が必要になる。このデータ変換処理は、ダミーデータに対する置き換えデータや変換プログラムを記録したコンテンツコードファイルを利用して行うことが必要となる。

【０００６】

コンテンツコードファイルは、コンテンツに併せて情報記録媒体に記録される。コンテンツコードファイルは、例えばコンテンツとは独立したファイルとして情報記録媒体に記録される。従って、コンテンツコードファイルのみを他の情報記録媒体に移動させる処理や、コピーするといった処理も可能となる。従って、不正なコンテンツコードファイルを作成して利用するといった不正利用も想定される。

【０００７】

このようなコンテンツコードファイルの不正利用を防止するため、正規のコンテンツコードファイルにはコンテンツ管理を行う第三者機関の電子署名が設定される。例えば、ＫＩＣ（Ｋｅｙ　Ｉｓｓｕａｎｃｅ　Ｃｅｎｔｅｒ、鍵管理センター）において電子署名が行なわれてディスクに記録される。

【０００８】

コンテンツおよびコンテンツコードファイルが記録されたディスクを装着して再生処理を行う場合、再生装置はコンテンツコードファイルに設定された署名の検証を実行する。この署名検証処理によってコンテンツコードファイルの正当性が確認された場合にのみ、

コンテンツコードファイル利用したコンテンツ再生が許容される。従って、正規の電子署名が設定されていないコンテンツコードファイルの利用は防止されることになる。

【０００９】

しかし、この電子署名付与手続は、時間およびコストがかかるという問題がある。例えば新たなコンテンツを格納したコンテンツ格納ディスクを製造して販売しようとする場合、その新規コンテンツに対応するコンテンツコードファイルを作成することになる。

【００１０】

コンテンツコードファイルには、上述したようにダミーデータに対応する置き換えデータやプレーヤ固有プログラムが含まれる。従って、新たなコンテンツコードファイルを作成した場合には、試験的な再生処理を実行してエラーが発生しないか否かを種々のプレーヤで確認して、エラーが発生する場合には、再度、ファイルを変更してさらに試験を行うといった処理が繰り返されることになる。

【００１１】

コンテンツコードファイルを適用した再生処理を実行する装置、上述したように再生装置は、コンテンツコードファイルの署名検証を実行して正当性確認を行うことが必須となっている。従って、試作段階であっても、ユーザ機器と同じ再生装置を利用する場合には、正式な電子署名が設定されたファイルを作成しなければならない。上記のように何度もコンテンツコードファイルの作り直しが必要となると、新たなファイル作成ごとにＫＩＣに署名付与を依頼することが必要となる。このような複数回の署名作成を行うことはコストおよび時間の浪費となる。

【００１２】

このような無駄を省くため、コンテンツコードファイルの署名検証を省略して再生処理に移行できる試験用の特別な再生装置を作成するという案もある。しかし、このような特別の再生装置を製造するにはコストがかかる。またこのような特別な再生装置が万が一不正に流通してしまった場合には、多くのユーザがこの不正な再生装置を利用することとなり、コンテンツコードファイルによる利用制御が無価値になってしまうという恐れがある。このような場合には、多くのコンテンツが不正に再生、利用され、大きな損害を発生させる可能性がある。

【特許文献１】特開２００３－１１６１００号公報

【特許文献２】ＷＯ２００５／００８３８５

【発明の開示】

【発明が解決しようとする課題】

【００１３】

本発明は、このような状況に鑑みてなされたものであり、例えばコンテンツコードファイルの試作段階などにおいて、コンテンツコードファイルに対する正式な電子署名を利用することなく、仮署名検証の後、コンテンツコードファイルを利用した再生による試験を可能とするとともに、不正なコンテンツコードファイルを利用した再生処理についても防止可能とした情報処理装置、情報記録媒体、および方法、並びにプログラムを提供することを目的とする。

【課題を解決するための手段】

【００１４】

本発明の第１の側面は、

コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する再生処理部と、

前記コンテンツコードファイルに設定された電子署名の検証処理を実行する署名検証部を有し、

前記署名検証部は、

ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行

する署名検証処理とで署名対象データを異なる設定とした署名検証を実行し、
前記再生処理部は、
前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行する構成である情報処理装置にある。

【００１５】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツコードファイルは、固定データ領域と、非固定データ領域を含み、前記署名検証部は、ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記固定データ領域と、非固定データ領域を署名対象データとした正規署名に対する署名検証処理を実行し、非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記非固定データ領域を署名対象データとしたテスト署名に対する署名検証処理を実行する構成である。

【００１６】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツコードファイルは、コンテンツコードであることを示す固定値のＩＤであるプレフィックスと、コンテンツコードファイルの属性情報と、前記コンテンツコードを含むファイルであり、前記署名検証部は、ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記プレフィックスと属性データとコンテンツコードを署名対象データとした正規署名に対する署名検証処理を実行し、非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行する構成である。

【００１７】

さらに、本発明の情報処理装置の一実施態様において、前記プレフィックスは固定されたビットデータによって構成される固定データ領域である。

【００１８】

さらに、本発明の情報処理装置の一実施態様において、前記非ＲＯＭディスクはデータ追記可能なＲ型またはＲＥ型のディスクである。

【００１９】

さらに、本発明の第２の側面は、
コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを構成するデータ構造であり、
コンテンツコードであることを示す固定値のＩＤであるプレフィックスと、コンテンツコードの属性（サイズ等）を示す情報属性情報と、前記コンテンツコードと、電子署名を有し、
前記電子署名は、前記属性情報と前記コンテンツコードを署名対象データとして設定されたテスト署名であり、
情報処理装置におけるＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行させることを可能としたデータ構造にある。

【００２０】

さらに、本発明の第３の側面は、
コンテンツと、
コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを格納し、
前記コンテンツコードファイルは、
コンテンツコードであることを示す固定値のＩＤであるプレフィックスと、コンテンツコードの属性（サイズ等）を示す情報属性情報と、前記コンテンツコードと、電子署名を有し、
前記電子署名は、前記属性情報と前記コンテンツコードを署名対象データとして設定されたテスト署名であり、

情報処理装置におけるＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行させることを可能とした情報記録媒体にある。

【００２１】

さらに、本発明の第４の側面は、

コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを生成するコンテンツコード生成部と、

前記コンテンツコードファイルに対する電子署名の設定依頼を実行する署名依頼部と、

署名の設定されたコンテンツコードファイルとコンテンツをディスクに記録するデータ記録部と、

コンテンツと、コンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する再生処理部と、

前記コンテンツコードファイルに設定された電子署名の検証処理を実行する署名検証部を有し、

前記署名検証部は、

ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行し、

前記再生処理部は、

前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行する構成である情報処理装置にある。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツコードファイルは、固定データ領域と、非固定データ領域を含み、前記署名検証部は、ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記固定データ領域と、非固定データ領域を署名対象データとした正規署名に対する署名検証処理を実行し、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記非固定データ領域を署名対象データとしたテスト署名に対する署名検証処理を実行する構成である。

【００２３】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツコードファイルは、コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードファイルの属性（コンテンツコードファイルのサイズなど）を示す属性情報と、前記コンテンツコードを含むファイルであり、前記署名検証部は、ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記プレフィックスと属性情報とコンテンツコードを署名対象データとした正規署名に対する署名検証処理を実行し、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して、前記属性情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行する構成である。

【００２４】

さらに、本発明の情報処理装置の一実施態様において、前記プレフィックスは固定されたビットデータによって構成される固定データ領域である。

【００２５】

さらに、本発明の情報処理装置の一実施態様において、前記非ＲＯＭディスクはデータ追記可能なＲ型またはＲＥ型のディスクである。

【００２６】

さらに、本発明の第５の側面は、

コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルに対する電子署名を生成する電子署名生成部を有し、

前記電子署名作成部は、
署名作成依頼の種類に応じて、署名対象データを異なる設定とした署名生成処理を実行する情報処理装置にある。
【００２７】
さらに、本発明の情報処理装置の一実施態様において、前記コンテンツコードファイルは、固定データ領域と、非固定データ領域を含み、前記署名生成部は、正規署名生成依頼に対しては、前記固定データ領域と、非固定データ領域を署名対象データとした署名生成処理を実行し、テスト署名生成依頼に対しては、前記非固定データ領域を署名対象データとした署名生成処理を実行する構成である。
【００２８】
さらに、本発明の情報処理装置の一実施態様において、前記コンテンツコードファイルは、コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードの属性（サイズ等）を示す情報属性情報と、前記コンテンツコードを含むファイルであり、前記署名生成部は、正規署名生成依頼に対しては、プレフィックスと属性情報とコンテンツコードを署名対象データとした署名生成処理を実行し、
テスト署名生成処理依頼に対しては、属性情報とコンテンツコードを署名対象データとした署名生成処理を実行する構成である。
【００２９】
さらに、本発明の第６の側面は、
情報処理装置において実行する情報処理方法であり、
再生処理部が、コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する再生処理ステップと、
署名検証部が、前記コンテンツコードファイルに設定された電子署名の検証処理を実行する署名検証ステップを有し、
前記署名検証ステップは、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行するステップであり、
前記再生処理ステップは、
前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行するステップである情報処理方法にある。
【００３０】
さらに、本発明の第７の側面は、
ディスク製造装置において実行するディスク製造方法であり、
コンテンツコード生成部が、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを生成するコンテンツコード生成ステップと、
データ記録部が、前記コンテンツコードファイルに対する電子署名であるテスト署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスク以外の非ＲＯＭディスクに記録する第１のデータ記録ステップと、
署名検証部が、前記コンテンツコードファイルのテスト署名に対する署名検証処理を実行する第１の署名検証ステップと、
前記非ＲＯＭディスクに記録されたコンテンツと、テスト署名の設定されたコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する第１の再生処理ステップと、
前記データ記録部が、前記第１の再生処理ステップにおける再生処理の成功を条件として、前記コンテンツコードファイルに対する電子署名として、前記テスト署名と異なるデ

ータ領域を署名対象とした正規署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスクに記録する第２のデータ記録ステップと、
署名検証部が、前記コンテンツコードファイルの正規署名に対する署名検証処理を実行する第２の署名検証ステップと、
前記ＲＯＭディスクに記録されたコンテンツと、正規署名の設定されたコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する第２の再生処理ステップと、
マスターディスク製造部が、前記第２の再生処理ステップにおける再生処理成功を条件として、コンテンツと、正規署名の設定されたコンテンツコードファイルを記録データとして設定したマスターディスクを製造するマスターディスク製造ステップと、
ディスク製造部が、前記マスターディスク製造ステップにおいて製造したマスターディスクを適用してディスクの製造を行うディスク製造ステップを有するディスク製造方法にある。

【００３１】

さらに、本発明のディスク製造方法の一実施態様において、前記コンテンツコードファイルは、固定データ領域と、非固定データ領域を含み、前記第１のデータ記録ステップは、前記非固定データ領域を署名対象データとしたテスト署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスク以外の非ＲＯＭディスクに記録するステップであり、前記第２のデータ記録ステップは、前記固定データ領域と非固定データ領域を署名対象データとした正規署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスクに記録するステップである。

【００３２】

さらに、本発明のディスク製造方法の一実施態様において、前記非ＲＯＭディスクはデータ追記可能なＲ型またはＲＥ型のディスクである。

【００３３】

さらに、本発明の第８の側面は、
情報処理装置において情報処理を実行させるプログラムであり、
再生処理部に、コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出させて、コンテンツ再生処理を実行させる再生処理ステップと、
署名検証部に、前記コンテンツコードファイルに設定された電子署名の検証処理を実行させる署名検証ステップを有し、
前記署名検証ステップは、
ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで署名対象データを異なる設定とした署名検証を実行させるステップであり、
前記再生処理ステップは、
前記署名検証部における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行させるステップであるプログラムにある。

【００３４】

なお、本発明のプログラムは、例えば、様々なプログラム・コードを実行可能な汎用システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体によって提供可能なプログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００３５】

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

ない。

【発明の効果】

【００３６】

本発明の一実施例構成によれば、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードの作成、試験において、一般のユーザの再生装置と同様、コンテンツコードファイルに設定した署名検証処理を実行し、署名検証に成功したことを条件としてコンテンツ再生試験を行う。初期的な再生試験において、正規署名とは異なるデータ領域に対してテスト署名を設定したコンテンツコードファイルをＲ／ＲＥ型のディスクに記録して署名検証および再生試験を実行する。その後、正規署名を設定したコンテンツコードファイルをＲＯＭディスクに記録して試験を行う。本構成により、Ｒ／ＲＥ型ディスクでも署名検証を含む再生試験が実行され、コスト高となる正規署名を、多数回、繰り返し行うことなく効率的なコンテンツコードの生成やディスク製造処理が実現される。

【発明を実施するための最良の形態】

【００３７】

以下、図面を参照しながら本発明の一実施例に係る情報処理装置、情報記録媒体、および情報処理方法、並びにプログラムの詳細について説明する。

【００３８】

まず、情報記録媒体の格納データについて説明する。図１は、情報記録媒体であるディスク（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標））の格納データ例を示す図である。図１に示すディスク１００は、ＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）規格に従ったコンテンツ格納ディスクの例である。

【００３９】

ディスク１００は、コンテンツ１１０と、コンテンツコードファイテル１２０を記録データとして格納している。なお、ＡＡＣＳ規格に従ったディスクには、この他にもコンテンツ１１０の復号に適用する鍵情報ファイルなど様々なデータが記録されるが、本発明の構成の説明に直接関係ないデータについては省略している。

【００４０】

コンテンツ１１０は、例えば高精細動画像データであるＨＤ（Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ）ムービーコンテンツなどの動画コンテンツのＡＶ（Ａｕｄｉｏ　Ｖｉｓｕａｌ）ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。これらのコンテンツは、特定のＡＶフォーマット規格データであり、特定のＡＶデータフォーマットに従って格納される。具体的には、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納される。

【００４１】

コンテンツ１１０は、例えば区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵（ＣＰＳユニット鍵またはユニット鍵（あるいはタイトル鍵と呼ぶ場合もある））が割り当てられ暗号化されて格納される。１つのユニット鍵を割り当てる単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。

【００４２】

コンテンツ１１０は、構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されない。再生を行なう場合は、ブロークンデータを、コンテンツコードファイル１２０に含まれる正しいコンテンツデータを含むコンテンツコードデータ１２１を利用してデータ置き換えを行うことが必要となる。

【００４３】

コンテンツコードファイル１２０には、コンテンツ１１０の再生処理において利用することが必須となるプログラム、またはコンテンツ１１０に含まれるブロークンデータの置き換えデータの少なくともいずれかを含むコンテンツコードデータ１２１が格納されたフ

ファイルである。

【００４４】

コンテンツコードファイル１２０には、ブロークンデータを正しいコンテンツに置き換える処理を行うためのデータやプログラムによって構成されるコンテンツコードデータ１２１と、コンテンツコードファイル１２０の正当性確認、改ざん検証に利用するための電子署名１２２が付与されている。電子署名１２２は、コンテンツの管理を行うコンテンツ管理局の秘密鍵、例えばＫＩＣの秘密鍵を適用した署名として設定されている。

【００４５】

コンテンツ利用を行う再生装置は、まず、コンテンツコードファイル１２０の電子署名１２２の検証処理を実行して、コンテンツコードファイル１２０が改ざんの無い正当なファイルであることを確認する。この確認がなされたことを条件として、コンテンツコードファイル１２０に含まれるコンテンツコード１２１を利用してコンテンツ１１０の構成データの置き換え処理などを行いながらコンテンツ再生を実行する。

【００４６】

なお、図１には、コンテンツ１１０とコンテンツコードファイル１２０をそれぞれ１つずつ示しているが、ディスク１００には複数のコンテンツと複数のコンテンツコードファイルを記録することが可能である。例えば、ある１つのコンテンツの再生時には、そのコンテンツに対応するコンテンツコードファイルを利用した再生処理を行う。

【００４７】

図１に示すように予めコンテンツが記録され、追記処理のできないディスクはＲＯＭディスクと呼ばれる。Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）におけるＲＯＭディスクはＢＤ－ＲＯＭと呼ばれる。

【００４８】

ＢＤ－ＲＯＭディスクに記録されたコンテンツを再生する場合、コンテンツコードファイル１２０の署名検証を実行し、コンテンツコードファイル１２０が改ざんの無い正当なファイルであることを確認できた場合にのみ、コンテンツコードファイル１２０に含まれるコンテンツコード１２１を利用してコンテンツ１１０の構成データの置き換えを行いながらコンテンツ再生を実行する。

【００４９】

図２は、再生装置において、ＢＤ－ＲＯＭディスクに記録されたコンテンツを再生する場合の処理シーケンスを説明するフローチャートである。

【００５０】

まず、ステップＳ１０１において、情報処理装置（再生装置）は、ディスクをドライブに挿入する。ディスクは、図１に示すようにコンテンツとコンテンツコードファイルを記録したディスクである。

【００５１】

情報処理装置は、ステップＳ１０２において、装置に装着されたディスクの種別を判別する。このディスク種別判別は、ディスクの記録情報、例えばＢＤ－ＲＯＭであるか否かについてはＲＯＭマークなどを検出して行われる。ディスクがＢＤ－ＲＯＭで無い場合は、ステップＳ１０７に進み、ＢＤ－ＲＯＭ対応の処理ではなく、装着ディスクに応じた処理を行う。

【００５２】

ステップＳ１０２において、ディスクがＢＤ－ＲＯＭであると判別された場合には、ステップＳ１０３に進み、ディスクからコンテンツコードファイルを読み取り、デンシ署名の検証処理を行う。前述したようにコンテンツコードファイルには正当性検証のためにコンテンツ管理局の電子署名が設定されている。電子署名は、コンテンツコードデータの構成データに対するハッシュ値（ｓｈａ１－ｈａｓｆ）に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従って付与されている。

【００５３】

情報処理装置（再生装置）はコンテンツ管理局の公開鍵を適用して署名検証処理を実行する。ステップＳ１０４において、署名検証に成功したか否かを判定する。すなわち、コンテンツコードファイルが改ざんの無い正当なファイルであるかの確認がなされたか否かを判定する。署名検証に失敗した場合、すなわち、コンテンツコードファイルの正当性が確認されなかった場合は、ステップＳ１０６に進み、コンテンツコードファイルの利用が禁止され、コンテンツ再生を停止する。

【００５４】

一方、ステップＳ１０４において、署名検証に成功した場合、すなわち、コンテンツコードファイルの正当性が確認された場合は、ステップＳ１０５に進み、コンテンツコードファイルの利用が許可され、コンテンツコードファイルに格納されたプログラムや置き換えデータを利用してコンテンツ再生を実行する。

【００５５】

このようにコンテンツの再生に際しては、コンテンツコードファイルの正当性確認を行い正当性の確認されたコンテンツコードファイルを利用することが必須となる。

【００５６】

コンテンツコードファイルは、コンテンツに対応して作成されディスクに記録される。コンテンツコードファイルには、コンテンツ再生に適用する置き換えデータやプログラムなどが含まれる。

【００５７】

従って、新たなコンテンツを格納したディスクを製造する際には、ディスクの製造前の段階で、新規コンテンツに対応するコンテンツコードファイルを試作し、再生試験を行いエラーの無い再生が行われるか否かを確認する作業が必要となる。

【００５８】

しかし、一般の再生装置における再生処理は、図２に示すフローに従って実行され、コンテンツの再生に際しては、コンテンツコードファイルの正当性確認を行い正当性の確認されたコンテンツコードファイルを利用することが必須となる。従って、署名の設定されていないコンテンツコードファイルは不正ファイルとみなされてしまうため再生試験すら実行できない。

【００５９】

署名検証を行わずに再生できる特殊な装置を製造することは、コスト高となり、特殊な装置が流通し、不正なコンテンツ利用が蔓延するといった恐れを発生させることになる。従って、製造時の試験であっても、署名の設定されたファイルを利用した試験を行うことが好ましい。

【００６０】

ただし、図２に示すフロー中、ステップＳ１０３～Ｓ１０５の処理は、ディスクがＢＤ－ＲＯＭである場合に限って実行される処理である。従って、ＢＤ－ＲＯＭ以外のディスク、例えば追記可能なＢＤ－Ｒ（追記可能なディスク）や、ＢＤ－ＲＥ（書き換え可能なディスク）に新規コンテンツと、試験用のコンテンツコードファイルを書き込んで再生試験を実行することは可能である。

【００６１】

しかし、この場合も、最終的にはコンテンツとコンテンツコードファイルをＲＯＭディスク（ＢＤ－ＲＯＭ）に記録して再生試験を行うことが必要となる。これは、ＢＤ－ＲＯＭにおける再生シーケンスを特殊な再生シーケンスとして規定しており、ＢＤ－Ｒや、ＢＤ－ＲＥにおいてエラーが発生しないコンテンツコードでもエラーが発生する可能性があるからである。

【００６２】

図３は、一般的なコンテンツコードファイルの試作処理と再生試験を行う場合のシーケンスについて説明するフローチャートである。この処理は、ディスクの製造前にコンテンツやコンテンツコードファイルの製作者、あるいはディスク工場などにおいて行われる。

【００６３】

ステップＳ１５１において、新規コンテンツに対応するコンテンツコードを作成する。次にステップＳ１５２において、追記可能ディスク（ＢＤ－Ｒ／ＲＥ）にコンテンツおよびコンテンツコードを記録して再生テストを実行する。

【００６４】

再生テストに失敗した場合は、ステップＳ１５４に進み、コンテンツコードの修正を実行して、ステップＳ１５２に戻り、ＢＤ－Ｒや、ＢＤ－ＲＥを利用して再生テストを繰り返す。

【００６５】

この再生テストにおいて、エラーが発生することなく再生がなされ、再生テストが成功した場合は、コンテンツコードに署名を設定したコンテンツコードファイルを完成させてＢＤ－ＲＯＭに書き込んで、最終的なテストを行うことになる。この処理がステップＳ１５５以下の処理である。

【００６６】

ステップＳ１５５では、コンテンツコード対応の電子署名の取得処理を行う。電子署名は、先に説明したように、コンテンツ管理局の電子署名である。ステップＳ１５５の処理は、作成したコンテンツコードをコンテンツ管理局に送信して、署名依頼を行い、署名を設定したコンテンツコードを受領する処理である。

【００６７】

このステップＳ１５５の処理の詳細シーケンスについて、図４に示すフローチャートを参照して説明する。図４は、コンテンツコードに対する署名を設定する側の処理シーケンスである。すなわち、コンテンツ管理局において実行する処理である。

【００６８】

コンテンツ管理局のサーバは、ステップＳ１８１においてコンテンツコードを受信すると、ステップＳ１８２において、受信したコンテンツコードが規格に従ったフォーマットを持つか否かを検証する。問題がある場合は、ステップＳ１８３の判定がＮｏとなり、ステップＳ１８６に進み、電子署名を設定することなく、コンテンツコードを返却する。

【００６９】

コンテンツコードの検証結果に問題が無い場合は、ステップＳ１８４に進み、コンテンツコードに対する電子署名を設定する。前述したように、コンテンツコードデータの構成データに対するハッシュ値（ｓｈａ１－ｈａｓｆ）に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従って電子署名が生成される。次に、ステップＳ１８５において、電子署名を設定したコンテンツコードを送信元へ送信する。

【００７０】

このようにして、コンテンツコードに対する電子署名が行われる。しかし、この処理は、前述したようにコストおよび時間がかかる処理である。

【００７１】

図３のフローチャートに戻り説明を続ける。ステップＳ１５５において、図４に示すフローに従ってコンテンツコードに対する電子署名の取得が行われた後、ステップＳ１５６に進む。

【００７２】

ステップＳ１５６では、署名の設定されたコンテンツコードファイルとコンテンツを記録したディスク（ＢＤ－ＲＯＭ）を作成する。次に、ステップＳ１５７において、署名の設定されたコンテンツコードファイルとコンテンツを記録したディスク（ＢＤ－ＲＯＭ）を利用した再生テストを行う。この再生テストでは、コンテンツコードファイルの署名検証を行い、署名検証に成功したコンテンツコードファイルを適用してコンテンツ再生処理を行うことになる。すなわち、図２に示すフローに従った再生処理を実行する。

【００７３】

この再生テストにおいて、再生エラーが発生することなく、再生処理に成功した場合（Ｓ１５８でＹｅｓ）は、処理を終了し、このコンテンツとコンテンツコードファイルを記

録したＲＯＭディスクが大量生産され販売されることになる。

【００７４】

しかし、この再生テストにおいて、再生エラーが発生し、再生処理に失敗した場合（Ｓ１５８でＮｏ）は、ステップＳ１５４に戻り、コンテンツコードの修正を行い、さらに、ステップＳ１５２に戻り、ＢＤ－Ｒや、ＢＤ－ＲＥを利用して再生テストを繰り返すことになる。

【００７５】

ＢＤ－Ｒや、ＢＤ－ＲＥを利用した再生テストにおいて再生処理に成功した場合は、再度、署名取得処理を実行した後、ＲＯＭディスクに対する書き込み処理を行って、ＲＯＭディスクでの再テストを行うことになる。このような処理が繰り返されると、ＲＯＭディスクの作成処理と署名取得処理に多くのコストと時間が浪費されることになる。

【００７６】

本発明においては、このような無駄を発生させない構成を提供する。本発明に従ったコンテンツコードファイルの試作処理と再生試験を行う場合のシーケンスについて、図５に示すフローチャートを参照して説明する。この処理は、ディスクの製造前にコンテンツやコンテンツコードファイルの製作者、あるいはディスク工場などにおいて行われる。

【００７７】

ステップＳ２０１において、新規コンテンツに対応するコンテンツコードを作成する。次にステップＳ２０２において、生成したコンテンツコードに対してテスト署名を設定する処理を行う。

【００７８】

本発明の処理では、コンテンツコードに対する署名として、

（ａ）テスト署名、

（ｂ）正規署名、

これら２種類の署名を利用する。

【００７９】

テスト署名は、コンテンツコードの試作段階において利用される署名であり、正規署名は、最終的な製品としてのディスクに記録されるコンテンツコードファイルに設定される署名である。

【００８０】

テスト署名、正規署名のいずれも、コンテンツ管理局の秘密鍵を適用して生成される署名であり、署名生成は、コンテンツ管理局に依頼して実行する。

【００８１】

ただし、テスト署名、正規署名は、署名対象とする構成データが異なる設定としてある。図６を参照して、テスト署名と正規署名の署名対象データの設定例について説明する。

【００８２】

図６には、コンテンツコードファイルの構成データを示してある。コンテンツードファイルは、図６に示すように、

（１）プレフィックス（Ｐｒｅｆｉｘ）

（２）属性情報識別子（Ｉｄｅｎｔｉｆｉｅｒ）

（３）コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）

（４）電子署名（Ｓｉｇｎａｔｕｒｅ）

これらのデータによって構成される。

【００８３】

プレフィックス（Ｐｒｅｆｉｘ）は、コンテンツコードであることを示す固定値のＩＤであり、固定的な８バイトのデータである。

識別子（Ｉｄｅｎｔｉｆｉｅｒ）は、コンテンツコードの属性（サイズ等）を示す情報である。

コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）は、変換プログラムや変換データなど、コンテンツ再生に際して利用する実体データである。

電子署名（Ｓｉｇｎａｔｕｒｅ）はコンテンツ管理局の秘密鍵を適用して生成される署名である。

【００８４】

このように、コンテンツコードファイルは、固定データ領域であるプレフィックス（Ｐｒｅｆｉｘ）と、非固定データ領域である識別子（Ｉｄｅｎｔｉｆｉｅｒ）、コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）を含む。

【００８５】

正規署名は、図に示すように、

（１）プレフィックス（Ｐｒｅｆｉｘ）

（２）識別子（Ｉｄｅｎｔｉｆｉｅｒ）

（３）コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）

これら（１）～（３）のデータを署名対象として生成される。（１）～（３）のデータに対するハッシュ値（ｓｈａ１－ｈａｓｆ）を生成して、このハッシュ値に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従って正規の電子署名を生成する。

【００８６】

一方、テスト署名は、図に示すように、

（２）識別子（Ｉｄｅｎｔｉｆｉｅｒ）

（３）コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）

これら（２）～（３）のデータを署名対象として生成される。（２）～（３）のデータに対するハッシュ値（ｓｈａ１－ｈａｓｆ）を生成して、このハッシュ値に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従ってテスト署名を生成する。すなわち、固定値のＩＤであるプレフィックスを省略する一方、データサイズ等を示し、コンテンツコード毎に変更される識別子については、署名対象とすることで、仮署名といえども署名で保護している。

【００８７】

正規署名、テスト署名のいずれも署名に用いる鍵やアルゴリズムは同じであるが、署名対象データを異なる設定としている。

【００８８】

さらに、正規署名の設定時には、コンテンツ管理局において署名対象とするデータであるコンテンツコードファイルの詳細な検証を実行して、フォーマット等が規定に従ったものであるかを確認した上で署名を行う。しかし、テスト署名の設定時には、コンテンツ管理局において署名対象とするデータであるコンテンツコードファイルの詳細な検証を実行することなく署名を行う。このようにテスト署名は、署名生成手続を簡略化している。

【００８９】

なお、図６に示す署名設定例は、正規署名がプレフィックス（Ｐｒｅｆｉｘ）を含むコンテンツコードファイル全体を署名設定対象データとし、テスト名がプレフィックス（Ｐｒｅｆｉｘ）を除いたコンテンツコードファイルを署名設定対象データとした例を示しているが、この他の設定も可能である。すなわちテスト署名と、正規署名とが、異なるデータフィールドを署名対象データとして様々な設定が可能となる。例えば、テスト署名を固定データ領域を含まない非固定データ領域を署名対象とした署名とし、正規署名を固定データ領域と非固定データ領域を署名対象とした署名とする。

【００９０】

図５に示すフローに戻り、本発明に従ったコンテンツコードファイルの試作処理と再生試験を行う場合のシーケンスについての説明を続ける。ステップＳ２０１において、新規コンテンツに対応するコンテンツコードを作成した後、ステップＳ２０２において、生成したコンテンツコードに対してテスト署名を設定する処理を行う。

【００９１】

このステップＳ２０２のコンテンツコードに対するテスト署名の設定処理の詳細シーケンスについて、図７（ａ）に示すフローチャートを参照して説明する。図７には（ａ），

（ｂ）２つのフローチャートを示している。これらは、
（ａ）テスト署名生成シーケンス、
（ｂ）正規署名生成シーケンス、
上記（ａ），（ｂ）の署名生成シーケンスであり、コンテンツ管理局において実行する処理シーケンスにおいて実行する。

【００９２】
図５のフローチャートのステップＳ２０２では、図７（ａ）に示すフローに従った処理がコンテンツ管理局において行われる。

【００９３】
コンテンツ管理局のサーバは、ステップＳ２３１においてコンテンツコードを受信すると、ステップＳ２３２に進み、コンテンツコードに対する電子署名を設定し、ステップＳ２３３において、テスト署名を設定したコンテンツコードを依頼先に送信する。

【００９４】
この場合、コンテンツ管理局のサーバは、受信したコンテンツコードに対する詳細な検証処理を行うことなくテスト署名の設定を行う。すなわち正規署名の設定時に実行するコンテンツコードのフォーマット検証などの詳細な検証を省略してテスト署名を生成する。なお、テスト署名は、先に図６を参照して説明したように、正規署名とは異なるデータフィールドを署名対象データとして設定した署名である。

【００９５】
例えば、テスト署名は、図６に示すように、識別子（Ｉｄｅｎｔｉｆｉｅｒ）、コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）、これらのデータに対するハッシュ値（ｓｈａ１－ｈａｓｆ）を生成して、このハッシュ値に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従ってテスト署名が生成される。

【００９６】
なお、コンテンツコードの試作処理を実行している装置は、コンテンツ管理局のサーバに対してコンテンツコードを送信する場合、テスト署名の依頼であるか、正規署名の依頼であるかを、コンテンツコード送信時、あるいは事前に通知する。コンテンツ管理局のサーバは、この通知により、受信したコンテンツコードがテスト署名の依頼データであるか正規署名の依頼データであるかを判別する。

【００９７】
コンテンツ管理局のサーバは、通知によりテスト署名の依頼であることが確認された場合には、図７（ａ）に示すフローに従った処理を実行し、正規署名の依頼であることが確認された場合には、図７（ｂ）に示すフローに従った処理を実行する。

【００９８】
図５のフローに戻り、本発明に従ったコンテンツコードファイルの試作処理と再生試験を行う場合のシーケンスについての説明を続ける。ステップＳ２０２において、図７（ａ）のフローに従ってコンテンツコードに対するテスト署名の設定処理が行なわれる。

【００９９】
テスト署名の設定されたコンテンツコードを受信した装置は、ステップＳ２０３において、追記可能ディスク（ＢＤ－Ｒ／ＲＥ）にコンテンツおよびテスト署名の設定されたコンテンツコードファイルを記録して再生テストを実行しステップＳ２０４において再生テストが成功したか否かを判定する。すなわち、テスト署名を設定したコンテンツコードファイルを適用したコンテンツ再生を実行し、コンテンツ再生がエラー無く実行されたか否かを検証する。

【０１００】
なお、ステップＳ２０３における再生テストは、一般のユーザ機器と同様の機器を利用して実行することが可能である。すなわち、
（ａ）コンテンツコードファイルの読み取り、
（ｂ）コンテンツコードファイルに設定された署名の検証、

（ｃ）署名検証の成功したコンテンツコードファイルに記録されたコンテンツコードを利用したコンテンツの再生、

上記の（ａ），（ｂ），（ｃ）の各処理を順次実行して行われる。ただし、署名の検証に際しては、図６を参照して説明したように署名対象データが正規署名とは異なるので、この異なるデータ領域についての署名検証処理として実行することになる。

【０１０１】

ステップＳ２０４において、再生テストに失敗したと判定した場合は、ステップＳ２０５に進み、コンテンツコードの修正を実行して、ステップＳ２０２に戻り、再度、テスト署名の設定を行って、ステップＳ２０３においてＢＤ－Ｒや、ＢＤ－ＲＥを利用して再生テストを繰り返す。

【０１０２】

この再生テストにおいて、エラーが発生することなく再生がなされ、再生テストが成功した場合は、コンテンツコードに正規署名を設定したコンテンツコードファイルを完成させてＢＤ－ＲＯＭに書き込んで、最終的なテストを行うことになる。この処理がステップＳ２０６以下の処理である。

【０１０３】

ステップＳ２０６では、コンテンツコード対応の正規の電子署名の取得処理を行う。正規の電子署名は、先に図６を参照して説明したように、テスト書名とは異なるデータフィールドを署名対象データとして設定したコンテンツ管理局の電子署名である。

【０１０４】

すなわち、図６を参照して説明したように、

（１）プレフィックス（Ｐｒｅｆｉｘ）

（２）識別子（Ｉｄｅｎｔｉｆｉｅｒ）

（３）コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）

これら（１）～（３）のデータに対するハッシュ値（ｓｈａ１－ｈａｓｆ）に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従って正規の電子署名が生成される。

【０１０５】

ステップＳ２０６の処理は、作成したコンテンツコードをコンテンツ管理局に送信して、正規署名の依頼を行い、正規署名を設定したコンテンツコードを受領する処理である。

【０１０６】

このステップＳ２０６の処理の詳細シーケンスについて、図７（ｂ）に示すフローチャートを参照して説明する。図７（ｂ）は、コンテンツ管理局において実行する処理である。

【０１０７】

なお、図７（ａ）のテスト署名のシーケンスにおいて説明したように、コンテンツコードの試作処理を実行している装置は、コンテンツ管理局のサーバに対してコンテンツコードを送信する場合、テスト署名の依頼であるか、正規署名の依頼であるかを、コンテンツコード送信時、あるいは事前に通知する。コンテンツ管理局のサーバは、この通知により、受信したコンテンツコードがテスト署名の依頼データであるか正規署名の依頼データであるかを判別する。コンテンツ管理局のサーバは、通知により正規署名の依頼であることが確認された場合には、図７（ｂ）に示すフローに従った処理を実行する。

【０１０８】

コンテンツ管理局のサーバは、ステップＳ２５１においてコンテンツコードを受信すると、ステップＳ２５２において、受信したコンテンツコードが規格に従ったフォーマットを持つか否かを検証する。問題がある場合は、ステップＳ２５３の判定がＮｏとなり、ステップＳ２５６に進み、電子署名を設定することなく、コンテンツコードを返却する。

【０１０９】

コンテンツコードの検証結果に問題が無い場合は、ステップＳ２５４に進み、コンテンツコードに対する電子署名を設定する。図６を参照して説明したように、プレフィックス

（Ｐｒｅｆｉｘ）、識別子（Ｉｄｅｎｔｉｆｉｅｒ）、コンテンツコードデータ（Ｃｏｎｔｅｎｔｓ　ｃｏｄｅ　ｄａｔａ）これらのデータに対するハッシュ値（ｓｈａ１－ｈａｓｆ）に対してコンテンツ管理局の秘密鍵を適用してＦＩＰＳ　ＰＵＢ　１８６－２準拠の署名アルゴリズムに従って正規の電子署名が生成される。

【０１１０】

次に、ステップＳ２５５において、正規の電子署名を設定したコンテンツコードを送信元へ送信する。このようにして、コンテンツコードに対する正規署名が行われる。

【０１１１】

図５のフローチャートに戻り説明を続ける。ステップＳ２０５において、図７（ｂ）に示すフローに従ってコンテンツコードに対する正規の電子署名の取得が行われた後、ステップＳ２０７に進む。

【０１１２】

ステップＳ２０７では、正規署名の設定されたコンテンツコードファイルとコンテンツを記録したディスク（ＢＤ－ＲＯＭ）を作成する。次に、ステップＳ２０８において、正規署名の設定されたコンテンツコードファイルとコンテンツを記録したディスク（ＢＤ－ＲＯＭ）を利用した再生テストを行う。この再生テストでは、正規の署名が設定されたコンテンツコードファイルの署名検証を行い、署名検証に成功したコンテンツコードファイルを適用してコンテンツ再生処理を行うことになる。すなわち、図２に示すフローに従った再生処理を実行する。

【０１１３】

この再生テストにおいて、再生エラーが発生することなく、再生処理に成功した場合（Ｓ２０９でＹｅｓ）は、処理を終了し、このコンテンツとコンテンツコードファイルを記録したＲＯＭディスクが大量生産され販売されることになる。

【０１１４】

しかし、この再生テストにおいて、再生エラーが発生し、再生処理に失敗した場合（Ｓ２０８でＮｏ）は、ステップＳ２０５に戻り、コンテンツコードの修正を行い、さらに、ステップＳ２０２に戻り、ＢＤ－Ｒや、ＢＤ－ＲＥを利用して再生テストを繰り返すことになる。

【０１１５】

この図５に示す処理フローでは、ＢＤ－Ｒや、ＢＤ－ＲＥを利用した再生テストにおいて、ＢＤ－ＲＯＭにおける再生テストと同様、署名検証が実行される。すなわち、

（ａ）コンテンツコードファイルの読み取り、

（ｂ）コンテンツコードファイルに設定された署名の検証、

（ｃ）署名検証の成功したコンテンツコードファイルに記録されたコンテンツコードを利用したコンテンツの再生、

上記の（ａ），（ｂ），（ｃ）の各処理を順次実行する。この処理は、ＢＤ－ＲＯＭにおける処理の同一の処理シーケンスとなる。

【０１１６】

このようにＢＤ－ＲやＢＤ－ＲＥにおいて実行する再生テストのシーケンスをＢＤ－ＲＯＭにおけるテストと同様のシーケンスに設定してある。

【０１１７】

先に図３を参照して説明したシーケンスでは、ＢＤ－ＲやＢＤ－ＲＥを利用したテストでは署名検証等の処理を含めずテストを行なうため、署名検証を必須とするＢＤ－ＲＯＭにおける再生テストと大きく異なるシーケンスとなっていた。従って、ＢＤ－ＲやＢＤ－ＲＥを利用した再生テストにおいてコンテンツ再生に成功した場合でもＢＤ－ＲＯＭに記録した後の再生テストにおいてエラーの発生する確率は比較的、高いものとなっていた。すなわち、ＲＯＭディスクの作成には、マザーディスク、スタンパの作成等が必要であるため、ＲＯＭディスクを作成するのはコストがかかっていた。

【０１１８】

これに対して、図５に示すシーケンスでは、マザーディスク、スタンパの作成が不要で

あるＢＤ－ＲやＢＤ－ＲＥにおいて実行する再生テストのシーケンスをＢＤ－ＲＯＭにおけるテストと同様のシーケンスに設定してあるので、テストとして作ったＢＤ－ＲやＢＤ－ＲＥにおける再生テストにおいてエラーが発生しなかった場合、ＢＤ－ＲＯＭにおけるテストにおいてエラーとなる確率は著しく低減させることができる。また、仮にテストとして作ったＢＤ－Ｒ／ＲＥディスクの再生テストにおいてエラーが発生したとしても、通常の記録ドライブを用いて、再作成したコンテンツコードを記録するのみで修正後のテストディスクの作成が可能となるため、ＲＯＭディスク作成と比較して少ないコストでテストが可能となる。

【０１１９】

従って、ＢＤ－ＲＯＭにおける再生テストに失敗して、図５のフローのステップＳ１５８においてＮｏと判定される確率は低くなる。すなわち、このＲＯＭによるテスト時点でエラーが発生してコンテンツコードの修正が必要となる可能性は低減される。結果として、多くのケースで正規署名の依頼回数は１回のみとなる。

【０１２０】

本発明のシーケンスでは、ＢＤ－ＲやＢＤ－ＲＥにおいて実行する再生テストやテスト署名の依頼は、複数回繰り返される可能性があるが、ＢＤ－ＲやＢＤ－ＲＥにおいて実行する再生テストに成功した後の処理においてエラーが発生する可能性が低減する。すなわち、ほとんどの場合、正規署名の設定処理は１回のみに削減することが可能となる。

【０１２１】

テスト署名の設定処理は、コストや時間のかからない簡易な手続処理である。これに対してして正規署名の設定処理は、管理サーハにおけるフォーマット検査などの処理が必要であり、コストおよび時間のかかる処理となる。

【０１２２】

本発明の処理シーケンスでは、複数回のテスト署名が繰り返される可能性はあるが、コストや時間のかかる正規署名設定処理を１回で完了させることが可能となり、全体としては効率化およびコスト削減が実現されることになる。

【０１２３】

次に、図８以下を参照して、本発明に係る情報処理装置の構成例について説明する。図８は、コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを記録したディスクを装着してコンテンツ再生処理を行う情報処理装置の構成を示す図である、

【０１２４】

情報処理装置２００はディスク２５０をドライブ２０１に装着して再生処理部２０２においてコンテンツ再生処理を行う。

【０１２５】

再生処理部２０２は、コンテンツと、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルをディスクから読み出して、コンテンツ再生処理を実行する。署名検証部２０３は、コンテンツコードファイルに設定された電子署名の検証処理を実行する。

【０１２６】

なお、署名検証部２０３は、ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理と、ＲＯＭディスク以外の非ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理とで、署名対象データを異なる設定とした署名検証を実行する。

【０１２７】

先に、図６を参照して説明したようにコンテンツコードファイルには、プレフィックスと、コンテンツコードの属性情報と、コンテンツコードと署名を含むファイルである。プレフィックスは固定データ領域（コンテンツコードファイルに依存しない領域）であり、コンテンツコードの属性情報とコンテンツコードは非固定データ領域（コンテンツコード毎に異なりうるデータ）である。

【０１２８】
このコンテンツコードファイルに設定される署名は、ディスク２５０がＲＯＭディスクである場合は、プレフィックスと識別データとコンテンツコードを署名対象データとした正規署名である。ディスク２５０がＲＯＭディスク以外のＲ型やＲＥ型などの非ＲＯＭディスクである場合には、識別データとコンテンツコードを署名対象データとしたテスト署名である。
【０１２９】
署名検証部２０３は、ＲＯＭディスクに記録されたコンテンツの再生処理に際して実行する署名検証処理は、プレフィックスと識別データとコンテンツコードを署名対象データとした正規署名に対応する署名検証処理を実行する。署名検証部２０３は、非ＲＯＭディスクに記録されたコンテンツの再生処理に際しては、識別情報とコンテンツコードを署名対象データとしたテスト署名に対する署名検証処理を実行する。
【０１３０】
再生処理部２０２は、署名検証部２０３における署名検証に成功したことを条件として、署名の成功したコンテンツコードファイルに格納されたコンテンツコードを適用してコンテンツ再生を実行する。
【０１３１】
次に、コンテンツコードを試作して、コンテンツコードの試験を行う情報処理装置の構成について図９を参照して説明する。基本的にこの情報処理装置も、図８に示す一般的な情報処理装置（再生装置）２００を利用する構成となる。
【０１３２】
図９に示す情報処理装置３００は、図８に示す一般的な情報処理装置（再生装置）２００に加え、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを生成するコンテンツコード生成部３０１と、コンテンツコードファイルに対する電子署名の設定依頼を実行する署名依頼部３０２と、署名の設定されたコンテンツコードファイルとコンテンツをディスクに記録するデータ記録部３０３を有する。
【０１３３】
なお、ディスクは最終的な製品として利用するディスクと同様のＲＯＭディスクと、ＲＯＭディスク以外の非ＲＯＭディスク（例えばＲ／ＲＥディスク）である場合がある。
【０１３４】
新たなコンテンツを格納したコンテンツコードファイルの生成処理を実行する際には、以下の処理を行うことになる。
コンテンツコード生成部３０１が、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルを生成する。
署名依頼部３０２が、コンテンツ管理局に対して、コンテンツコードファイルに対するテスト署名を依頼し、テスト署名を設定したコンテンツコードファイルを受領する。
データ記録部３０２が、テスト署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスク以外の非ＲＯＭディスク（例えばＲ／ＲＥディスク）２５０に記録する。
【０１３５】
次に再生処理を実行する情報処理装置２００の署名検証部２０３が、コンテンツコードファイルのテスト署名に対する署名検証処理を実行し、署名検証成功を条件として、非ＲＯＭディスク２５０に記録されたコンテンツと、テスト署名の設定されたコンテンツコードファイルをディスク２５０から読み出して、コンテンツ再生処理を実行する。
【０１３６】
署名依頼部３０２が、非ＲＯＭディスク２５０に記録されたコンテンツ再生処理の成功を条件として、コンテンツ管理局に対して、コンテンツコードファイルに対する正規署名を依頼し、正規署名を設定したコンテンツコードファイルを受領する。この正規署名は、

図６を産しようして説明したように、テスト署名と異なるデータ領域を署名対象データとして設定した署名である。

【０１３７】

次に、データ記録部３０３が、正規署名を設定したコンテンツコードファイルとコンテンツをＲＯＭディスクに記録する。

【０１３８】

次に再生処理を実行する情報処理装置２００の署名検証部２０３が、コンテンツコードファイルの正規署名に対する署名検証処理を実行し、署名検証成功を条件として、ＲＯＭディスク２５０に記録されたコンテンツと、テスト署名の設定されたコンテンツコードファイルをディスク２５０から読み出して、コンテンツ再生処理を実行する。

【０１３９】

この再生処理に成功した場合に、ユーザ提供用のディスクの製造に移行する。この場合、マスターディスク製造部３１０において、コンテンツと、正規署名の設定されたコンテンツコードファイルを記録データとして設定したマスターディスクを製造する。その後、ディスク製造部３２０が、マスターディスクを利用してディスク３３０の製造を行う。

【０１４０】

図１０は、テスト署名や正規署名を行う管理サーバとしての情報処理装置の構成を示す図である。サーバ４００は、通信部４０１と、電子署名生成部４０２を有する。

【０１４１】

電子署名生成部４０２は、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードを格納したコンテンツコードファイルに対する電子署名を生成する。電子署名生成部４０２は、署名作成依頼の種類に応じて、署名対象データを異なる設定とした署名生成処理を実行する。

【０１４２】

コンテンツコードファイルは、前述したように固定データ領域と、非固定データ領域を含み、電子署名生成部４０２は、正規署名生成依頼に対しては、固定データ領域と、非固定データ領域を署名対象データとした署名生成処理を実行し、テスト署名生成依頼に対しては、非固定データ領域を署名対象データとした署名生成処理を実行する。

【０１４３】

具体的には、コンテンツコードファイルは、コンテンツコードであることを示すＩＤであるプレフィックスと、コンテンツコードファイルの属性（サイズ等）を示す属性情報と、前記コンテンツコードを含むファイルであり、電子署名生成部４０２は、正規署名生成依頼に対しては、プレフィックスと属性情報とコンテンツコードを署名対象データとした署名生成処理を実行し、テスト署名生成処理依頼に対しては、属性情報とコンテンツコードを署名対象データとした署名生成処理を実行する。

【０１４４】

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

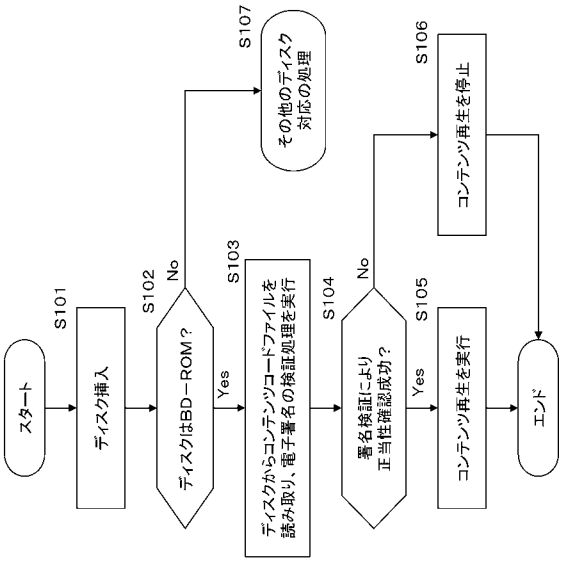
【０１４５】

また、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。例えば、プログラムは記録媒体に予め記録しておくことができる。記録媒体からコンピュータにインストールする他、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介してプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

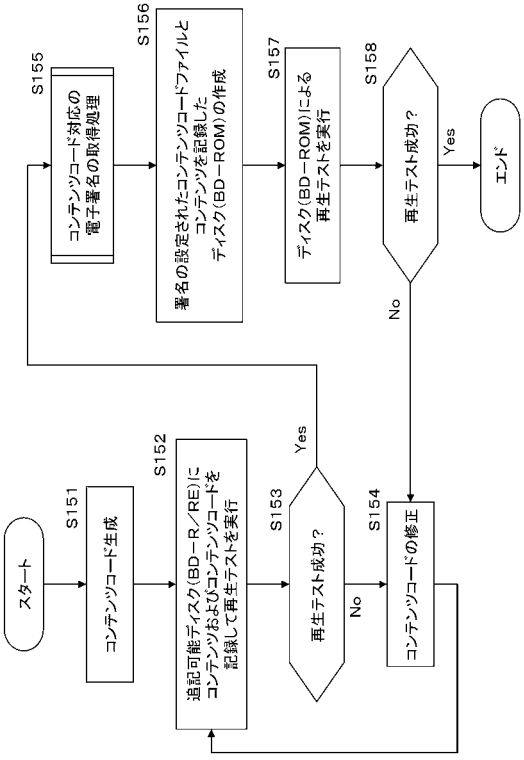
【０１４６】
なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【産業上の利用可能性】
【０１４７】
以上、説明したように、本発明の一実施例構成によれば、コンテンツ再生処理に適用するプログラムまたは変換データの少なくともいずれかを含むコンテンツコードの作成、試験において、一般のユーザの再生装置と同様、コンテンツコードファイルに設定した署名検証処理を実行し、署名検証に成功したことを条件としてコンテンツ再生試験を行う。初期的な再生試験において、正規署名とは異なるデータ領域に対してテスト署名を設定したコンテンツコードファイルをＲ／ＲＥ型のディスクに記録して署名検証および再生試験を実行する。その後、正規署名を設定したコンテンツコードファイルをＲＯＭディスクに記録して試験を行う。本構成により、Ｒ／ＲＥ型ディスクでも署名検証を含む再生試験が実行され、コスト高となる正規署名を、多数回、繰り返し行うことなく効率的なコンテンツコードの生成やディスク製造処理が実現される。
【図面の簡単な説明】
【０１４８】
【図１】ディスク格納データの構成例について説明する図である。
【図２】コンテンツコードを適用したコンテンツ再生処理のシーケンスについて説明するフローチャートを示す図である。
【図３】コンテンツコードの試作とテスト処理のシーケンスについて説明するフローチャートを示す図である。
【図４】コンテンツコードファイルに対する署名設定処理のシーケンスについて説明するフローチャートを示す図である。
【図５】本発明の一実施例に係るコンテンツコードの試作とテスト処理のシーケンスについて説明するフローチャートを示す図である。
【図６】本発明の一実施例に係るコンテンツコードファイルに対する署名設定例について説明する図である。
【図７】本発明の一実施例に係るコンテンツコードファイルに対する署名設定処理のシーケンスについて説明するフローチャートを示す図である。
【図８】本発明の一実施例に係るコンテンツ再生を実行する情報処理装置の構成例について説明する図である。
【図９】本発明の一実施例に係るコンテンツコードの試験、ディスクの製造を実行する装置の構成例を示す図である。
【図１０】本発明の一実施例に係るテスト署名や正規署名を行う管理サーバとしての情報処理装置の構成を示す図である。
【符号の説明】
【０１４９】
１００　ディスク
１１０　コンテンツ
１２０　コンテンツコードファイル
１２１　コンテンツコートデータ
１２２　電子署名
２００　情報処理装置
２０１　ドライブ
２０２　再生処理部
２０３　署名検証部
２５０　ディスク

３００　情報処理装置
３０１　コンテンツコード生成部
３０２　署名依頼部
３０３　データ記録部
３１０　マスターディスク製造部
３２０　ディスク製造部
４００　サーバ
４０１　通信部
４０２　電子署名生成部

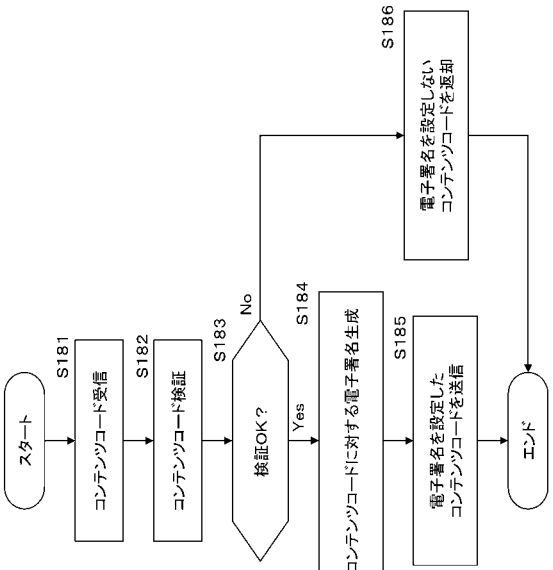
【図２】



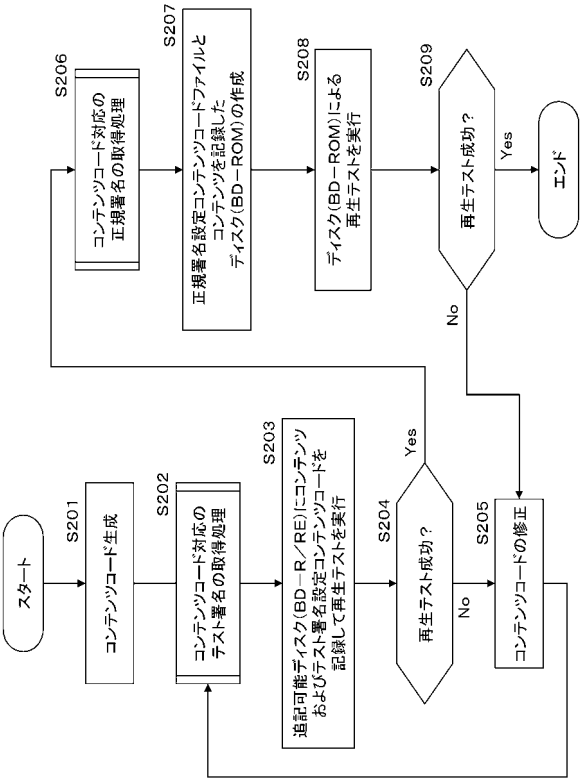
【図３】



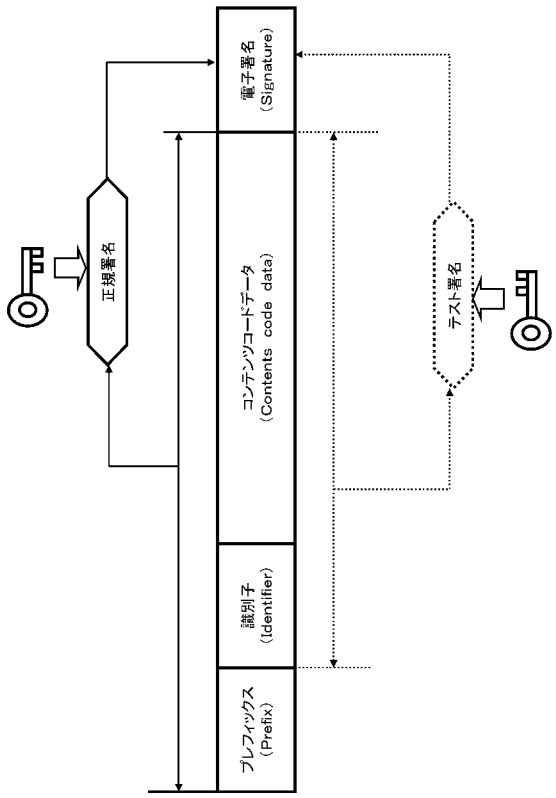
【図４】


スタート
S181
コンテンツコード受信
S182
コンテンツコード検証
S183
検証OK？
No
Yes
S184
コンテンツコードに対する電子署名生成
S185
電子署名を設定した
コンテンツコードを送信
S186
電子署名を設定しない
コンテンツコードを返却
エンド

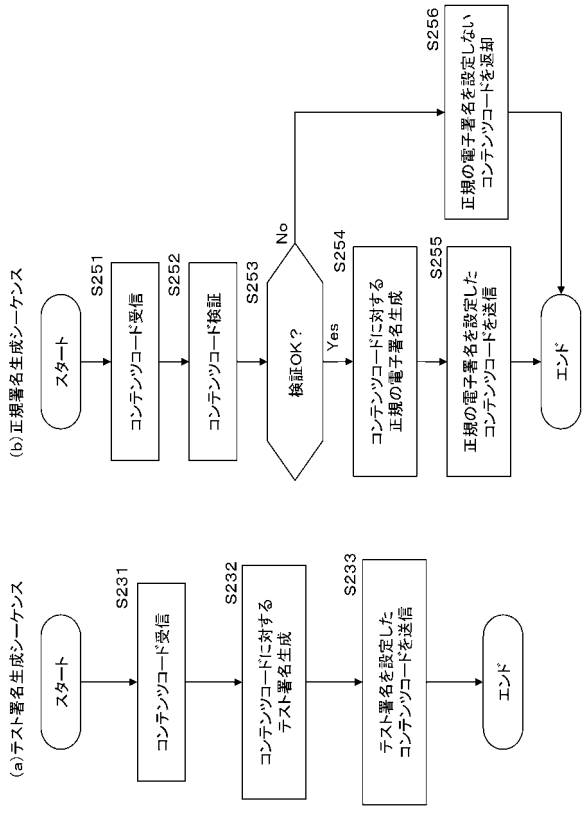
【図５】


スタート
S201
コンテンツコード生成
S202
コンテンツコード対応の
テスト署名の取得処理
S203
追記可能ディスク(BD－R／RE)にコンテンツ
およびテスト署名設定コンテンツコードを
記録して再生テストを実行
S204
再生テスト成功？
Yes
No
S205
コンテンツコードの修正
S206
コンテンツコード対応の
正規署名の取得処理
S207
正規署名設定コンテンツコードファイルと
コンテンツを記録した
ディスク(BD－ROM)の作成
S208
ディスク(BD－ROM)による
再生テストを実行
S209
再生テスト成功？
Yes
No
エンド

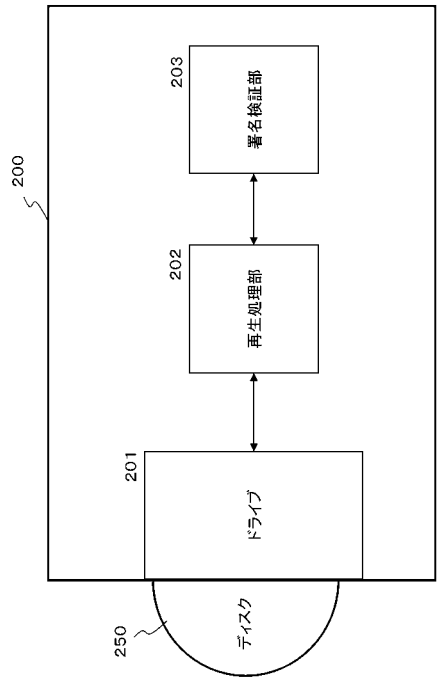
【図６】


正規署名
テスト署名
プレフィックス
(Prefix)
識別子
(Identifier)
コンテンツコードデータ
(Contents code data)
電子署名
(Signature)

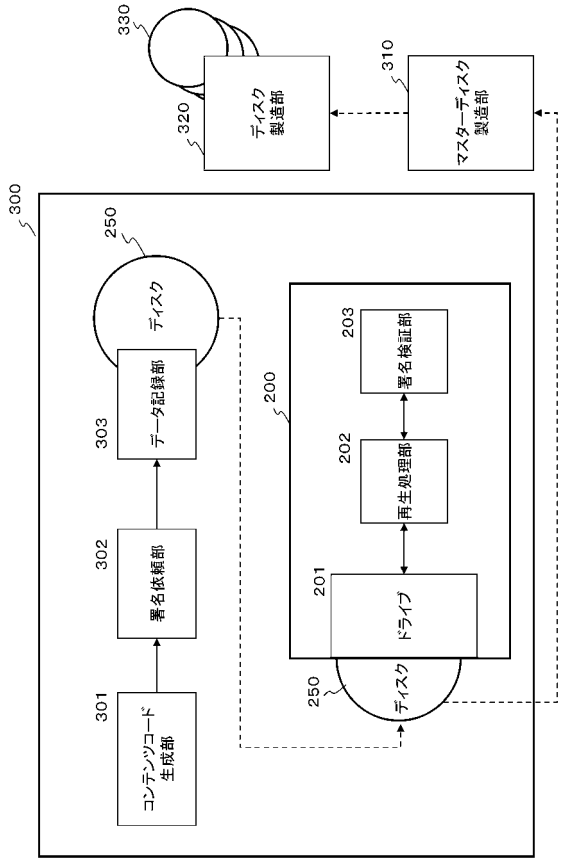
【図７】


(a)テスト署名生成シーケンス
スタート
S231
コンテンツコード受信
S232
コンテンツコードに対する
テスト署名生成
S233
テスト署名を設定した
コンテンツコードを送信
エンド
(b)正規署名生成シーケンス
スタート
S251
コンテンツコード受信
S252
コンテンツコード検証
S253
検証OK？
No
Yes
S254
コンテンツコードに対する
正規の電子署名生成
S255
正規の電子署名を設定した
コンテンツコードを送信
S256
正規の電子署名を設定しない
コンテンツコードを返却
エンド

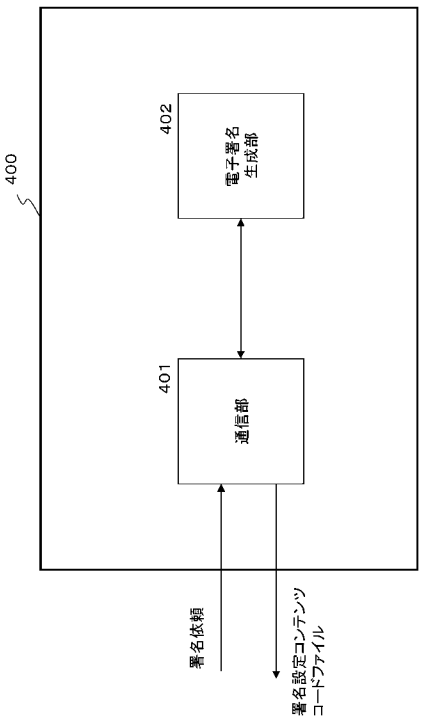
【図８】


200
203
署名検証部
202
再生処理部
201
ドライブ
250
ディスク

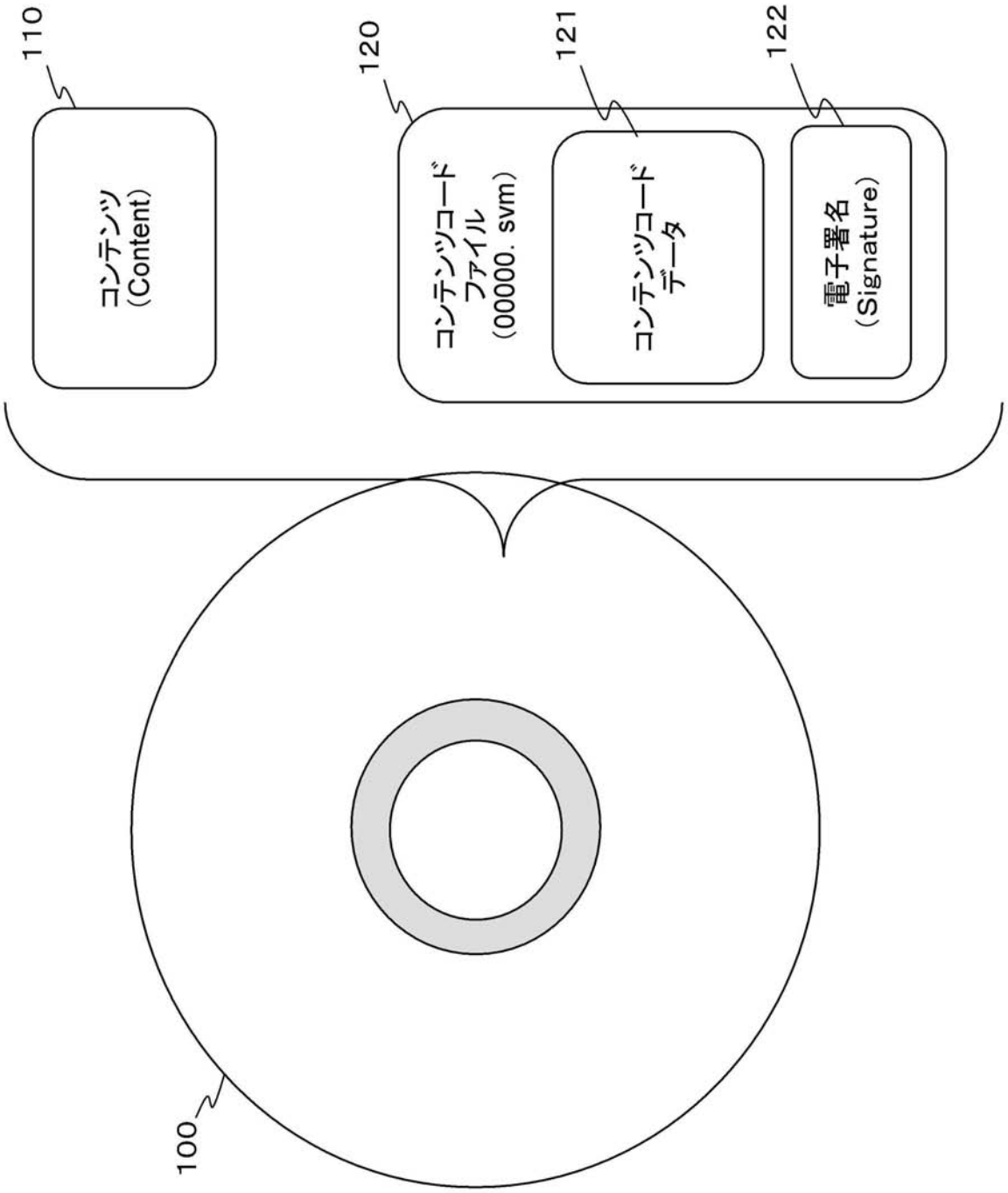
【図９】


330
320
ディスク
製造部
310
マスターディスク
製造部
300
250
ディスク
303
データ記録部
302
署名依頼部
301
コンテンツコード
生成部
200
203
署名検証部
202
再生処理部
201
ドライブ
250
ディスク

【図１０】


400
402
電子署名
生成部
401
通信部
署名依頼
署名設定コンテンツ
コードファイル

【図１】


110
コンテンツ
(Content)
120
コンテンツコード
ファイル
(00000. svm)
121
コンテンツコード
データ
122
電子署名
(Signature)
100

フロントページの続き

(72)発明者　上田　健二朗
東京都港区港南１丁目７番１号　ソニー株式会社内

Ｆターム(参考) 5B017 AA08 BA09 CA16
5C053 FA24 FA30 JA30 KA05 LA14
5D044 AB05 AB07 BC03 CC04 DE03 DE50 DE57 FG18 GK12 HL08