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

特許第3956106号
(P3956106)

(45)発行日　平成19年8月8日(2007.8.8)　(24)登録日　平成19年5月18日(2007.5.18)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04N	5/91	(2006.01)	H04N	5/91	P
G09C	5/00	(2006.01)	G09C	5/00	
G11B	20/10	(2006.01)	G11B	20/10	H
H04L	9/32	(2006.01)	H04L	9/00	675B

請求項の数 6　(全 27 頁)　最終頁に続く

(21)出願番号　特願2002-93207(P2002-93207)
(22)出願日　平成14年3月28日(2002.3.28)
(65)公開番号　特開2003-304226(P2003-304226A)
(43)公開日　平成15年10月24日(2003.10.24)
審査請求日　平成14年12月25日(2002.12.25)

前置審査

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】コンピュータ装置及びプログラム

(57)【特許請求の範囲】

【請求項１】

コンテンツ公開者が公開しコンテンツ利用者が利用するコンテンツに対して保証を与えるコンテンツ鑑定者により用いられるコンピュータ装置であって、

前記コンテンツを前記コンテンツ公開者の端末からネットワークを介して取得するコンテンツ取得手段と、

前記コンテンツ取得手段により取得された前記コンテンツに基づいて、保証された当該コンテンツが再生されるように制御する制御情報を生成する制御情報生成手段と、

前記制御情報を暗号化する情報暗号化手段と、

暗号化された前記制御情報を前記コンテンツ公開者の端末にネットワークを介して転送する情報転送手段と、

前記コンテンツのデータと暗号化された前記制御情報とを前記コンテンツ公開者の端末から受け取った前記コンテンツ利用者の端末において、保証された当該コンテンツを再生できるように、暗号化された前記制御情報を復号するためのキー情報を、当該コンテンツ利用者の端末に格納するために出力する出力手段と、

を有することを特徴とするコンピュータ装置。

【請求項２】

前記コンテンツのダイジェスト値を算出するダイジェスト値算出手段をさらに備え、

前記制御情報生成手段は、前記ダイジェスト値算出手段で算出されるダイジェスト値を前記制御情報に含ませることを特徴とする請求項１記載のコンピュータ装置。

【請求項３】
コンテンツ公開者が公開しコンテンツ利用者が利用するコンテンツに対して保証を与えるコンテンツ鑑定者により用いられるコンピュータ装置に対し、
前記コンテンツを前記コンテンツ公開者の端末からネットワークを介して取得する手順と、
取得した前記コンテンツに基づいて、保証された当該コンテンツが再生されるように制御する制御情報を生成する手順と、
前記制御情報を暗号化する手順と、
暗号化された前記制御情報を前記コンテンツ公開者の端末にネットワークを介して転送する手順と、
前記コンテンツのデータと暗号化された前記制御情報とを前記コンテンツ公開者の端末から受け取った前記コンテンツ利用者の端末において、保証された当該コンテンツを再生できるように、暗号化された前記制御情報を復号するためのキー情報を、当該コンテンツ利用者の端末に格納するために出力する手順と、
を実行させることを特徴とするプログラム。
【請求項４】
前記コンテンツのダイジェスト値を算出する手順をさらにコンピュータ装置に実行させ、
前記制御情報を生成する手順では、前記ダイジェスト値を含む前記制御情報を生成することを特徴とする請求項３記載のプログラム。
【請求項５】
前記制御情報は複数カテゴリを有し、
前記コンテンツ利用者からの要求に応じ、複数カテゴリのうちの特定カテゴリの前記制御情報が有効か無効かを確認するための識別情報を当該コンテンツ利用者の端末に送出する手順をさらにコンピュータ装置に実行させることを特徴とする請求項３記載のプログラム。
【請求項６】
前記識別情報を送出した前記コンテンツ利用者の端末に対し、前記識別情報の更新情報を送出する手順をさらにコンピュータ装置に実行させることを特徴とする請求項５記載のプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、静止画、動画、音声等のコンテンツを提供する方法、および提供されたコンテンツの再生方法等に関する。
【０００２】
【従来の技術】
ウェブ上に公開されているサイト数は年々増加し、利用者は様々なコンテンツを自由に閲覧できるものの、有害なサイトやヘイトサイトも数多く存在するため、コンピュータ装置の利用形態によっては、コンテンツの表示制限を行うことがある。また、家庭、学校、企業等では、教育上、業務上の観点からコンテンツの表示制限を行うこともある。
また、昨今のウィルス感染の影響を回避するため、安全ではないサイトへのアクセスを制限したいという要求もある。
従来、このようなコンテンツの表示制限は、フィルタリング・ソフトウェアや、ウェブブラウザのセキュリティ設定等によって行っていた。
【０００３】
【発明が解決しようとする課題】
しかしながら、フィルタリング・ソフトウェアの場合、コンテンツの中に特定のタグが含まれていたり、コンテンツに含まれる文字の検索によってフィルタリングを行うため、コンテンツ作成者の意識への依存度が高く、また必ずしも臨むようなフィルタリングが行え

ないこともある。さらに、フィルタリング・ソフトウェアの場合、イメージデータや、音楽等のサウンドデータは排除できないという問題もある。
また、ウェブブラウザのセキュリティ設定の場合、その設定をユーザ側で行うため、コンテンツの表示制限を思うように行うには限界がある。
さらに、最近では、いわゆるハッカー等により、コンテンツの改竄が行われる問題もあり、安全であったはずのサイトに悪意のある改竄がなされた場合、ユーザ側ではその表示をとめる手段がないのが実状であった。

【０００４】

本発明は、このような技術的課題に基づいてなされたもので、より有効にコンテンツの視聴制限を行うことのできる技術を提供することを目的とする。

【０００５】

【課題を解決するための手段】

かかる目的のもと、本発明のコンテンツの提供方法は、コンテンツ提供者側の端末にて、コンテンツ提供者から提供されるコンテンツのダイジェスト値を算出し、算出されたダイジェスト値を含む制御情報を生成する。そして、制御情報およびコンテンツのデータをコンテンツ利用者に提供するために出力する。その一方で、これら制御情報およびコンテンツのデータとは別に、コンテンツの再生をコントロールするためのキー情報をコンテンツ利用者に提供するために出力する。
制御情報は、これに含まれるダイジェスト値と、コンテンツ利用者の端末にて算出されるコンテンツのダイジェスト値をコンテンツ利用者の端末にて照合することによって、コンテンツ利用者の端末におけるコンテンツの再生をコントロールするためのものである。また、キー情報は、コンテンツ利用者の端末にて制御情報が有効であるか否かを判断することによってコンテンツの再生をコントロールするものである。
つまり、コンテンツ利用者側では、ダイジェスト値が一致し、かつキー情報によって制御情報が有効であると判断されたときにコンテンツを再生することが可能となる。
ところで、コンテンツ提供者側からコンテンツ利用者側への制御情報およびコンテンツデータの提供は、インターネット等のネットワークを介したデータ転送によって行っても良いし、コンテンツ提供者側の端末から出力したデータをＣＤ－ＲＯＭ等の記憶媒体に格納し、これをコンテンツ提供者側からコンテンツ利用者側に受け渡し、コンテンツ利用者の端末にて記憶媒体から制御情報およびコンテンツのデータを読み出すことによって行っても良い。

【０００６】

コンテンツ提供者側は、コンテンツの作成者と制御情報の発行者が一体であっても良いが、コンテンツの鑑定、保証等を行うのであれば、前記コンテンツの作成者である第１のコンテンツ提供者とそれ以外の者である第２のコンテンツ提供者のように、別々であるのが望ましい。
後者の場合、コンテンツの作成者とは異なる第２のコンテンツ提供者の端末にて制御情報を生成し、これを暗号化して第１のコンテンツ提供者の端末に受け渡すために出力する。また、第１のコンテンツ提供者の端末にて、第２のコンテンツ提供者の端末から受け渡された制御情報をコンテンツのデータに付加して出力する。また第２のコンテンツ提供者の端末では、キー情報として、暗号化された制御情報を復号するための復号化キーのデータを、コンテンツ利用者に受け渡すために出力する。
制御情報は暗号化されているので、第１のコンテンツ提供者側では制御情報の改竄等を行うことができない。また、暗号化された制御情報と復号化キーの双方が揃うコンテンツ利用者側で、初めて制御情報を復号化することができる。
また、この他に、コンテンツの作成者の端末にて制御情報を生成するとともに、第２のコンテンツ提供者の端末から発行された暗号化キーで制御情報を暗号化し、第２のコンテンツ提供者の端末にて、キー情報として、暗号化された制御情報を復号するための復号化キーのデータを出力することもできる。このような構成は、鑑定等を行う第２のコンテンツ提供者にとってコンテンツの作成者が信頼できる場合に成り立つ。

【０００７】
本発明を、コンテンツの鑑定等を行う立場側で用いられるコンピュータ装置として捉えると、このコンピュータ装置は、制御情報生成手段にて、ネットワークを介して外部から取得したコンテンツの、再生の可否を制御する制御情報を生成し、これを情報暗号化手段で暗号化して、情報転送手段によってコンテンツの公開者の端末にネットワークを介して転送する。さらにこのコンピュータ装置は、キー情報格納手段に、制御情報を暗号化するときに用いる暗号化キーと暗号化された制御情報を復号化する復号化キーのデータを格納している。
このような構成において、コンテンツの公開者は、暗号化された制御情報を付加してコンテンツのデータをネットワーク上で公開する。コンテンツの被提供者は、ネットワーク上に公開されたコンテンツのデータおよび制御情報を取得する一方で、上記コンピュータ装置のキー情報格納手段に格納された復号化キーを取得することによって、暗号化された制御情報を復号化することができる。コンテンツの被提供者側では、制御情報が復号化できた場合のみコンテンツを再生するようにすれば、制御情報を用いてコンテンツの再生制限を行うことが可能となる。
また、このコンピュータ装置は、ダイジェスト値算出手段にて、コンテンツのダイジェスト値を算出し、制御情報生成手段では、算出されるダイジェスト値を制御情報に含ませることもできる。これにより、コンテンツの被提供者側で、コンテンツのダイジェスト値を算出し、制御情報に含まれるダイジェスト値と比較することによって、コンテンツが改竄されているか否かを確認することができる。
【０００８】
本発明を、コンテンツを公開する側で用いられるコンピュータ装置として捉えれば、このコンピュータ装置は、ダイジェスト値算出手段にて、公開するコンテンツのダイジェスト値を算出し、制御情報生成手段にて、ダイジェスト値を含み、コンテンツの再生の可否を制御する制御情報を生成し、情報暗号化手段にて、制御情報を外部から受け取った暗号化キーで暗号化する。この暗号化キーは、例えばコンテンツの鑑定者等によって発行することができる。そしてこのコンピュータ装置では、コンテンツデータ受け渡し手段にて、コンテンツのデータを暗号化された制御情報とともにコンテンツの利用者の端末に受け渡す。
このコンテンツデータ受け渡し手段では、暗号化された制御情報を電子透かしとしてコンテンツのデータに付加することもできる。この場合、電子透かしを視認可能なイメージとし、これをコンテンツとともに表示することも可能である。
【０００９】
本発明は、ネットワークを介して外部から取得したコンテンツの内容を保証する保証情報を生成する処理と、保証情報を暗号化する処理と、暗号化された保証情報をコンテンツの公開者の端末にネットワークを介して転送する処理と、をコンピュータ装置に実行させることを特徴とするプログラムとして捉えることもできる。また、暗号化された保証情報を復号化する復号化キーのデータを、予め登録されたコンテンツの取得者の端末に受け渡す処理をさらにコンピュータ装置に実行させることもできる。さらに、コンテンツのダイジェスト値を算出する処理をさらにコンピュータ装置に実行させ、保証情報を生成する処理では、ダイジェスト値を含む保証情報を生成してもよい。
保証情報が複数のカテゴリを有する場合、コンテンツの取得者からの要求に応じ、複数カテゴリのうちの特定カテゴリの保証情報が有効か無効かを確認するための識別情報をコンテンツの取得者の端末に送出する処理をさらにコンピュータ装置に実行させることもできる。
また、識別情報を送出したコンテンツの取得者に対し、識別情報の更新情報を送出する処理をさらにコンピュータ装置に実行させることもできる。このような処理は、例えばコンテンツの視聴料を定期的に課金する場合等に有効であり、課金に対する支払いを行ったユーザにのみ、定期的に識別情報を更新すれば良い。
【００１０】

本発明を、コンテンツ利用者の端末におけるコンテンツの再生方法として捉えれば、本発明では、コンテンツ提供者の端末からネットワークを介してコンテンツのデータおよびコンテンツの再生の可否をコントロールするための制御情報を受信し、制御情報とは別にコンテンツ提供者、コンテンツ利用者以外の第三者の端末から発行された確認情報に基づき、確認情報と制御情報が対応するものであるときにコンテンツを再生することを特徴とする。
また、第三者によって発行された暗号化キーにて暗号化された状態で制御情報を受信し、受信した制御情報を、確認情報として第三者によって発行された復号化キーで復号化できたときにコンテンツを再生することもできる。
さらに、コンテンツのデータとともにコンテンツの制御情報を受信するときには、コンテンツのダイジェスト値を含む制御情報を受信し、コンテンツを再生するときには、受信したコンテンツのダイジェスト値を算出し、算出されたダイジェスト値と制御情報に含まれるダイジェスト値が一致するときに、コンテンツを再生することもできる。
【００１１】
上記のような方法をコンテンツ利用者が用いるコンピュータ装置で実現するには、ネットワークを介してコンテンツの公開者の端末からコンテンツのデータとコンテンツの再生の可否を制御する、暗号化された制御情報を取得する処理と、プログラムのデータ格納領域に格納された復号化キーにて制御情報を復号化する処理と、復号化された制御情報に含まれる情報に基づいてコンテンツの再生の可否を判定する処理と、判定の結果に基づいてコンテンツを再生する処理と、をコンピュータ装置に実行させることを特徴とするプログラムが好適である。
さらに、制御情報を取得する処理では、特定の認証カテゴリを有する制御情報を取得し、コンテンツの再生の可否を判定する処理では、予めコンテンツ利用者から認証カテゴリの指定を受け付け、指定された認証カテゴリが制御情報に含まれる特定の認証カテゴリに対応するときに、コンテンツの再生を可とすることもできる。
この場合、制御情報には、複数種の認証カテゴリがあり、その認証カテゴリの例としては、「１２歳未満視聴不可」、「１５歳未満視聴不可」、「１８歳未満視聴不可」といったものがある。そして、コンテンツ利用者が、「１２歳未満視聴不可」という認証カテゴリを指定した場合、コンテンツとともに提供される制御情報に含まれる特定の認証カテゴリが、コンテンツ利用者の指定した認証カテゴリに対応する場合、つまり「１２歳未満視聴不可」ではない内容の認証カテゴリである場合にコンテンツの再生を行うのである。また、例えばケーブルテレビジョンにおいて、課金額(視聴料)に応じて認証カテゴリを変え、ユーザの認証カテゴリによってユーザ(コンテンツの取得者)視聴できるチャンネル数(コンテンツ)を変えるようなこともできる。
【００１２】
【発明の実施の形態】
以下、添付図面に示す実施の形態に基づいてこの発明を詳細に説明する。
[第一の実施の形態]
図１は、本実施の形態におけるコンテンツ表示制限システムの概略を説明するための図である。
この図１に示すように、本実施の形態では、コンテンツ提供者、コンテンツの公開者となるコンテンツ作成者(第１のコンテンツ提供者)は、作成した静止画、動画、音声(オーディオ)、ＰＤＦ(Portable Document Format)形式のテキスト等のコンテンツを、コンテンツ作成者の端末１０Ａにて、インターネット等のネットワーク２０上に公開する。また、コンテンツ作成者は、コンテンツ鑑定者(第２のコンテンツ提供者)によるコンテンツの認証を受け、認証がなされたことを示す認証マークをコンテンツ鑑定者の端末３０Ａからネットワーク２０を介して受け取る。そして、ユーザの端末５０Ａからのアクセスを受けたときに、コンテンツ作成者の端末１０Ａは、指定されたコンテンツに認証マークを添付し、これをユーザの端末５０Ａに送信する。ユーザの端末５０Ａでは、コンテンツとともに受信した認証マークに含まれる情報からコンテンツの正当性を確認し、正当であると確認

されたコンテンツのみを表示や音声の再生によって出力する。
コンテンツ鑑定者としては、例えば子供を有害サイトから守ることを目的とするＰＴＡ等の団体、学校や省庁等の機関、安全、あるいは品質が保証されたコンテンツをユーザに提供したい出版会社、プロバイダ、ポータルサイトの運営者等がある。このコンテンツ鑑定者は、コンテンツ利用者となるユーザから見ればコンテンツ提供者とも言える。また、コンテンツ作成者とユーザから見れば、第三者の立場にあるとも言える。
一方、コンテンツ利用者、コンテンツの取得者となるユーザとしては、学校、役場等の公共施設、未成年のいる家庭、会社等がある。
【００１３】
コンテンツ作成者の端末１０Ａは、いわゆるＰＣやワークステーション端末であり、ネットワーク２０を介してのデータの送受信を司る通信部(コンテンツデータ受け渡し手段)１１、キーボードやマウス等の入力部１２、モニター等の表示部１３、作成したコンテンツのデータを格納するＨＤＤ等のコンテンツデータ格納部１４、入力部１２での入力に応じて所定のプログラムに基づいた処理を実行するＣＰＵやメモリ等によって実現される処理部１５、を備える。
なお、コンテンツデータ格納部１４に格納されるコンテンツのデータは、当該コンテンツ作成者の端末１０Ａにて作成されたものであっても良いし、他の端末にて作成されたものであっても良い。
【００１４】
コンテンツ鑑定者の端末３０Ａは、いわゆるＰＣやワークステーション端末であり、ネットワーク２０を介してのデータの送受信を司る通信部(情報転送手段)３１、キーボードやマウス等の入力部３２、モニター等の表示部３３、入力部３２での入力に応じて所定のプログラムに基づいた処理を実行するＣＰＵやメモリ等によって実現される処理部３４Ａ、日付や時刻を管理するクロック部３５、後述するコンテンツＩＤを暗号化・復号化する秘密鍵・公開鍵のデータを格納したコンテンツＩＤ用暗号鍵ＤＢ(データベース；キー情報格納手段)３６、を備える。
また、処理部３４Ａは、コンテンツのダイジェスト値を計算するダイジェスト値計算部(ダイジェスト値算出手段)３７、コンテンツに添付する認証マークを作成する認証マーク作成部(制御情報生成手段)３８、通信部３１から送出するデータを暗号化するデータ暗号化処理部(情報暗号化手段)３９、を備える。
ここで、コンテンツのダイジェスト値とは、通信されるデータが正しいことを証明するために、元のデータから特徴的なパターンを生成し、これを数値化したもので、例えばハッシュ値がある。ハッシュ値は、ハッシュ関数によって、コンテンツを表すデータ(長いデータ)を撹乱し、一定の長さ(例えば128ビット)の値に圧縮したものである。
認証マークとは、コンテンツのデータにデータとして添付されるもので、ここでは視認できるシンボルマークという意味ではない。
【００１５】
ユーザの端末５０Ａは、ＰＣや携帯電話端末、ウェブ機能を有した電化製品等があり、ネットワーク２０を介してのデータの送受信を司る通信部５１、キーボードやマウス等の入力部５２、モニター等の表示部５３、後述するコンテンツ閲覧プログラムを格納するＨＤＤ等のコンテンツ閲覧プログラム格納部５４、入力部５２での入力に応じて所定のプログラムに基づいた処理を実行するＣＰＵやメモリ等によって実現される処理部５５、を備える。
コンテンツ閲覧プログラムは、本コンテンツ表示制限システムを利用するに当たってコンテンツ鑑定者(あるいは第三者)から有償または無償で配布されるものであり、例えばブラウザ等のコンテンツ閲覧機能を有したプログラムに対するプラグイン・プログラム、あるいはそれ単体でコンテンツの表示までを行うプログラム等の形態を取っている。ユーザは、予め、ネットワーク２０を介して、あるいはコンテンツ閲覧プログラムが格納されたＣＤ－ＲＯＭ等の記憶媒体を介して、コンテンツ閲覧プログラムを入手し、これをユーザの端末５０Ａにインストールする。これによってコンテンツ閲覧プログラムがコンテンツ閲

覧プログラム格納部５４に格納されるのである。このコンテンツ閲覧プログラムは、無料でも良いが、有料とすることもできる。
処理部５５は、コンテンツ作成者の端末１０Ａから暗号化された状態で送出されたデータを復号化するデータ復号化処理部５６、コンテンツのダイジェスト値に基づいてコンテンツが正当なものであるか否かを検査するコンテンツ検査処理部５７、その検査結果に基づきコンテンツの表示を制御するコンテンツ表示制御部５８を備える。
【００１６】
次に、このようなコンテンツ表示制限システムにおいて、コンテンツを表示する際の流れについて説明する。
まず、コンテンツ鑑定者は、コンテンツ鑑定者の端末３０Ａにて、外部の、ネットワーク２０上に公開されているコンテンツをサーチする。そして、コンテンツ鑑定者側で設定した所定の条件を満たすコンテンツが発見された場合、そのコンテンツに対し、認証マークを付与する処理を開始する(もちろん、コンテンツ作成者からの請求を受けて、コンテンツ鑑定者側が認証マークを付与することも可能である)。
これにはまず、図２に示すように、コンテンツ鑑定者の端末３０Ａにて、通信部３１を介し、処理対象となるコンテンツのデータ(Ｄ)を取得し、図示しないメモリ等に格納する(ステップＳ１０１)。
【００１７】
次いで、処理部３４Ａでは、ダイジェスト値計算部３７において、取得したコンテンツのデータ(Ｄ)のダイジェスト値(ハッシュ値)(Ｈｏ)を計算する(ステップＳ１０２)。ここでｈａｓｈはダイジェスト値を算出する計算式である。
Ｈｏ＝ｈａｓｈ(Ｄ)
【００１８】
続いて、処理部３４Ａでは、認証マーク作成部３８にて、制御情報、保証情報としてのコンテンツＩＤ(Ｄｉｄ)を作成する(ステップＳ１０３)。
このコンテンツＩＤ(Ｄｉｄ)は、ダイジェスト値(Ｈｏ)と、コンテンツの鑑定を行った鑑定者ＩＤ(Ａｉｄ)、鑑定による認証を行った日付(時刻を含んでも良い)である認証日付を含む情報によって構成される。
そして、作成されたコンテンツＩＤ(Ｄｉｄ)は、処理部３４Ａのデータ暗号化処理部３９にて計算式Ｓにより暗号化され、これによって認証マーク(Ｋｅ)が作成される(ステップＳ１０４)。このとき、コンテンツＩＤ(Ｄｉｄ)の暗号化には、予めコンテンツＩＤ用暗号鍵ＤＢ３６にてコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)と対になって格納されている、コンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)が暗号化キーとして用いられる。
$Ke=S_{KpriA}(Did)$
【００１９】
この後、コンテンツ鑑定者の端末３０Ａでは、認証マーク(Ｋｅ)のデータを、ネットワーク２０を介し、通信部３１からコンテンツ作成者の端末１０Ａに向けて出力する(ステップＳ１０５)。
【００２０】
コンテンツ作成者の端末１０Ａでは、ネットワーク２０を介し、認証マーク(Ｋｅ)のデータを通信部１１で受信すると、自動的、あるいはコンテンツ作成者が所定の操作を行うことにより、認証マーク(Ｋｅ)のデータをコンテンツのデータ(Ｄ)に添付し、これをコンテンツデータ格納部１４に格納する。
さて、このようにしてコンテンツ鑑定者からのコンテンツの認証を受けて以降、コンテンツ作成者は、そのコンテンツ(以下、これを「認証付きコンテンツ」と適宜称する)をネットワーク２０上に公開する。
【００２１】
一方、ユーザは、ユーザの端末５０Ａを用い、ネットワーク２０上に公開された認証付きコンテンツにアクセスする。このとき、ユーザ側は、この認証付きコンテンツをユーザの端末５０Ａで表示させるには、コンテンツ閲覧プログラムをコンテンツ鑑定者から入手し

て、予め導入(インストール)しておく必要がある。なお、このコンテンツ閲覧プログラムには、前述のコンテンツＩＤを復号化するためのコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が内蔵されている。このコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)は、復号化キーとして、コンテンツ鑑定者の端末３０Ａのコンテンツ ＩＤ用暗号鍵ＤＢ３６においてコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)と対になって格納されているものである。

【００２２】

コンテンツ作成者の端末１０Ａでは、ネットワーク２０を介してユーザの端末５０Ａからのアクセスを受けると、コンテンツデータ格納部１４に格納された、認証付きコンテンツ、つまり認証マーク(Ｋｅ)のデータが添付されたコンテンツのデータ(Ｄ)を通信部１１から送出する。

図３に示すように、ユーザの端末５０Ａでは、ネットワーク２０を介し、通信部５１が、認証マーク(Ｋｅ)のデータが添付されたコンテンツのデータ(Ｄ)を受信(取得)し、これを図示しないメモリに一時格納する(ステップＳ２０１)。

【００２３】

コンテンツのデータ(Ｄ)を受信すると、自動的に、あるいはユーザの起動操作によってコンテンツ閲覧プログラムが起動される。すると、処理部５５は以下に示すような処理を実行する。

まず、データ復号化処理部５６が、コンテンツのデータ(Ｄ)に添付されている認証マーク(Ｋｅ)のデータを、コンテンツ閲覧プログラムに内蔵されているコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)によって計算式Ｖにより復号化し、コンテンツＩＤ(Ｄｉｄ)を得る(ステップＳ２０２)。

$$Did = V_{KpubA}(Ke)$$

ここで、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が正しくない場合、つまり認証マーク(Ｋｅ)を暗号化したコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)に対応したものでない場合には、認証マーク(Ｋｅ)のデータを復号化することはできず、これ以降の処理に進んでコンテンツの表示を行うことはできない。その場合、コンテンツの表示を行うことができない旨のメッセージを表示し、処理を終了することができる。つまり、このコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が、コンテンツの再生の可否を制御する制御情報、キー情報、確認情報としての機能を有するのである。

【００２４】

また、コンテンツＩＤに含まれる鑑定者ＩＤ(Ａｉｄ)や認証日付が正規のものかどうか、ネットワーク２０を介してコンテンツ鑑定者の端末３０Ａに照会し、照会が完了した時点で以降のステップに進み、正規のものであるとの確認が取れないときには処理を中止し、コンテンツの表示を行わないこともできる。

【００２５】

続いて、コンテンツ検査処理部５７が、コンテンツのデータ(Ｄ)のダイジェスト値(ハッシュ値)(Ｈｃ)を計算する(ステップＳ２０３)。

また、コンテンツ検査処理部５７は、コンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を抽出し(ステップＳ２０４)、ステップＳ２０３で算出されたダイジェスト値(Ｈｃ)と比較する(ステップＳ２０５～Ｓ２０６)。

その結果、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しければ、ユーザの端末５０Ａで受け取ったコンテンツが改竄されていないことになるので、コンテンツ表示制御部５８では、コンテンツのデータ(Ｄ)に基づき、表示部５３にコンテンツを表示する(コンテンツが音声の場合、図示しないスピーカ等から音声を再生出力する)。このとき、コンテンツとともに、コンテンツＩＤ(Ｄｉｄ)に含まれる鑑定者ＩＤ(Ａｉｄ)、認証日付を表示することができる(ステップＳ２０７)

一方、ステップＳ２０６にて、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しくない場合、ユーザの端末５０Ａで受け取ったコンテンツが、コンテンツ鑑定者側で鑑定されたコンテンツの内容と異なる、つまり改竄等がなされている可能性があるため、コンテンツ表示制御部５８では、コンテンツ閲覧

プログラムを終了させ、コンテンツの表示を行わない。
【００２６】
上述したような構成によれば、ユーザの端末５０Ａでは、コンテンツ鑑定者によって認証されたコンテンツを表示させることができる。しかも、ダイジェスト値によって改竄の有無を確認し、改竄されていない場合のみコンテンツを表示させるようになっている。したがって、ユーザは、正当なコンテンツを安心して得ることができる。
また、ユーザ側では、公開鍵が内蔵されたコンテンツ閲覧プログラムが無いとコンテンツを表示できないため、コンテンツ作成者あるいはコンテンツ鑑定者側からすれば、視聴制限が行うことが可能となり、予め登録された会員のみに対するコンテンツの公開や、視聴料金の確実な徴収等が実現できる。
さらに、ユーザ側では、公開鍵が内蔵されたコンテンツ閲覧プログラムが有ればコンテンツを表示させるためのパスワード入力等の操作を行う必要が無く、無意識のうちにコンテンツの認証が行われてコンテンツを表示することができるので、利便性が高まる。
【００２７】
[第二の実施の形態]
次に、本発明の第二の実施の形態について説明する。以下に説明する第二の実施の形態では、上記第一の実施の形態で挙げた認証マークに代わり、電子透かしを用いる点が第一の実施の形態との主な相違点である。したがって、上記第一の実施の形態と共通する構成については同符号を付し、その説明を省略する。
図４は、本実施の形態におけるコンテンツ表示制限システムの概略を説明するための図である。
この図４に示すように、本実施の形態では、コンテンツ作成者は、作成したコンテンツを、コンテンツ作成者の端末１０Ｂにて、インターネット等のネットワーク２０上に公開する。また、コンテンツ作成者は、コンテンツ鑑定者によるコンテンツの認証を受け、認証がなされたことを示す電子透かしのデータをコンテンツ鑑定者の端末３０Ｂからネットワーク２０を介して受け取る。そして、ユーザの端末５０Ｂからのアクセスを受けたときに、コンテンツ作成者の端末１０Ｂは、電子透かしを埋め込んだコンテンツのデータをユーザの端末５０Ｂに送信する。ユーザの端末５０Ｂでは、受信したコンテンツに埋め込まれた電子透かしに含まれる情報からコンテンツの正当性を確認し、正当であると確認されたコンテンツのみを表示や音声の再生によって出力する。
【００２８】
コンテンツ作成者の端末１０Ｂは、上記第一の実施の形態に示したコンテンツ作成者の端末１０Ａと同様、通信部１１、入力部１２、表示部１３、コンテンツデータ格納部１４、処理部１５、を備える。
【００２９】
コンテンツ鑑定者の端末３０Ｂは、通信部３１、入力部３２、表示部３３、処理部３４Ｂ、クロック部３５、コンテンツＩＤ用暗号鍵ＤＢ３６、を備える。
処理部３４Ｂは、ダイジェスト値計算部３７、認証マーク作成部３８、データ暗号化処理部３９の他、コンテンツに埋め込む電子透かしを作成する電子透かし作成部(制御情報生成手段)４０、を備える。
ここで、電子透かし作成部４０は、上記第一の実施の形態で用いた認証マークを電子透かしとして埋め込んだ認証イメージのデータを作成する処理を実行する。
【００３０】
ユーザの端末５０Ｂは、上記第一の実施の形態に示したユーザの端末５０Ａと同様、通信部５１、入力部５２、表示部５３、コンテンツ閲覧プログラム格納部５４、処理部５５、を備える。
また、処理部５５は、データ復号化処理部５６、コンテンツ検査処理部５７、コンテンツ表示制御部５８を備える。
【００３１】
次に、このようなコンテンツ表示制限システムにおいて、コンテンツを表示する際の流れ

について説明する。
まず、コンテンツ鑑定者は、コンテンツ鑑定者の端末３０Ｂにて、ネットワーク２０上に公開されているコンテンツをサーチする。そして、コンテンツ鑑定者側で設定した所定の条件を満たすコンテンツが発見された場合、そのコンテンツに対し、認証マークを付与する処理を開始する。
これにはまず、図５に示すように、コンテンツ鑑定者の端末３０Ｂにて、通信部３１を介し、処理対象となるコンテンツのデータ(Ｄ)を取得し、図示しないメモリ等に格納する(ステップＳ３０１)。
【００３２】
次いで、処理部３４Ｂでは、ダイジェスト値計算部３７において、取得したコンテンツのデータ(Ｄ)のダイジェスト値(Ｈｏ)を計算する(ステップＳ３０２)。ここでｈａｓｈはダイジェスト値を算出する計算式である。
Ｈｏ＝ｈａｓｈ(Ｄ)
【００３３】
続いて、処理部３４Ｂでは、認証マーク作成部３８にて、ダイジェスト値(Ｈｏ)と、コンテンツの鑑定を行った鑑定者ＩＤ(Ａｉｄ)、鑑定による認証を行った日付(時刻を含んでも良い)である認証日付を含む情報によって、コンテンツＩＤ(Ｄｉｄ)を作成する(ステップＳ３０３)。
作成されたコンテンツＩＤ(Ｄｉｄ)は、処理部３４Ｂのデータ暗号化処理部３９にて、コンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)によって計算式Ｓにより暗号化され、これによって認証マーク(Ｋｅ)が作成される(ステップＳ３０４)。
$Ke = S_{KpriA}(Did)$
【００３４】
次いで、電子透かし作成部４０は、認証マーク(Ｋｅ)のデータを電子透かしとして埋め込んだ認証イメージを作成する(ステップＳ３０５)。ここで、認証イメージは、コンテンツが静止画や動画等、ユーザの端末５０Ｂの表示部５３上に表示されるものである場合、コンテンツ上あるいはコンテンツの周囲等に表示される視認できるシンボルマーク等であり、この認証イメージに電子透かしとして認証マーク(Ｋｅ)が埋め込まれる。
【００３５】
この後、コンテンツ鑑定者の端末３０Ｂでは、認証マーク(Ｋｅ)のデータを電子透かしとして埋め込んだ認証イメージのデータを、ネットワーク２０を介し、通信部３１からコンテンツ作成者の端末１０Ｂに向けて出力する(ステップＳ３０６)。
【００３６】
コンテンツ作成者の端末１０Ｂでは、ネットワーク２０を介し、認証イメージのデータを通信部１１で受信すると、自動的、あるいはコンテンツ作成者が所定の操作を行うことにより、認証イメージのデータをコンテンツのデータ(Ｄ)に添付し、これをコンテンツデータ格納部１４に格納する。
さて、このようにしてコンテンツ鑑定者からのコンテンツの認証を受けて以降、コンテンツ作成者は、そのコンテンツ(以下、これを「認証付きコンテンツ」と適宜称する)をネットワーク２０上に公開する。
【００３７】
一方、ユーザは、ユーザの端末５０Ｂを用い、ネットワーク２０上に公開された認証付きコンテンツにアクセスする。このとき、ユーザ側は、この認証付きコンテンツをユーザの端末５０Ｂで表示させるには、コンテンツ閲覧プログラムを予め導入(インストール)しておく必要がある。なお、このコンテンツ閲覧プログラムには、前述のコンテンツＩＤを復号化するためのコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が内蔵されている。
【００３８】
コンテンツ作成者の端末１０Ｂでは、ネットワーク２０を介してユーザの端末５０Ｂからのアクセスを受けると、コンテンツデータ格納部１４に格納された、認証付きコンテンツ、つまり認証イメージのデータが添付されたコンテンツのデータ(Ｄ)を通信部１１から送

出する。
図６に示すように、ユーザの端末５０Ｂでは、ネットワーク２０を介し、通信部５１が、認証イメージのデータが添付されたコンテンツのデータ(Ｄ)を受信(取得)し、これを図示しないメモリに一時格納する(ステップＳ４０１)。
【００３９】
そして、コンテンツ閲覧プログラムが起動されると、処理部５５は以下に示すような処理を実行する。
まず、データ復号化処理部５６が、コンテンツのデータ(Ｄ)に添付されている認証イメージのデータから、電子透かしとして埋め込まれた認証マーク(Ｋｅ)のデータを抽出する(ステップＳ４０２)。
ここで電子透かしが認証イメージから抽出できなかった場合、認証イメージが不正なものであるとして、これ以降の処理に進んでコンテンツの表示を行うことができない。
続いて、抽出した認証マーク(Ｋｅ)のデータを、コンテンツ閲覧プログラムに内蔵されているコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)を用いて計算式Ｖにより復号化し、コンテンツＩＤ(Ｄｉｄ)を得る(ステップＳ４０３)。
$Did = V_{KpubA}(Ke)$
ここで、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が正しくない場合、つまり認証マーク(Ｋｅ)を暗号化したコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)に対応したものでない場合には、認証マーク(Ｋｅ)のデータを復号化することはできず、これ以降の処理に進んでコンテンツの表示を行うことはできない。その場合、コンテンツの表示を行うことができない旨のメッセージを表示し、処理を終了することができる。
【００４０】
また、コンテンツＩＤに含まれる鑑定者ＩＤ(Ａｉｄ)や認証日付が正規のものかどうか、ネットワーク２０を介してコンテンツ鑑定者の端末３０Ｂに照会し、照会が完了した時点で以降のステップに進み、正規のものであるとの確認が取れないときには処理を中止し、コンテンツの表示を行わないこともできる。
【００４１】
続いて、コンテンツ検査処理部５７が、コンテンツのデータ(Ｄ)のダイジェスト値(Ｈｃ)を計算する一方(ステップＳ４０４)、コンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を抽出し(ステップＳ４０５)、双方のダイジェスト値(Ｈｏ)と(Ｈｃ)を比較する(ステップＳ４０６～Ｓ４０７)。
その結果、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しければ、コンテンツ表示制御部５８では、コンテンツのデータ(Ｄ)に基づき、表示部５３にコンテンツを表示する。このとき、コンテンツとともに、コンテンツＩＤ(Ｄｉｄ)に含まれる鑑定者ＩＤ(Ａｉｄ)、認証日付を表示することができる(ステップＳ４０８)
一方ステップＳ４０７にて、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しくない場合、ユーザの端末５０Ｂで受け取ったコンテンツが、コンテンツ鑑定者側で鑑定されたコンテンツの内容と異なる、つまり改竄等がなされている可能性があるため、コンテンツ表示制御部５８では、コンテンツ閲覧プログラムを終了させ、コンテンツの表示を行わない。
【００４２】
上述したような構成によれば、ユーザの端末５０Ｂによっても、コンテンツ鑑定者によって認証されたコンテンツを表示させることができる。しかも、ダイジェスト値によって改竄の有無を確認し、改竄されていない場合のみコンテンツを表示させるようになっている。したがって、ユーザは、正当なコンテンツを安心して得ることができる。
加えて、コンテンツＩＤが含まれる認証マーク(Ｋｅ)を電子透かしとして認証イメージに埋め込み、これをコンテンツのデータ(Ｄ)に添付する構成としたので、コンテンツＩＤの第三者による改竄等も防ぐことができる。
また、コンテンツ作成者側からすれば、視聴制限が行えることになり、予め登録された会

員のみに対するコンテンツの公開や、視聴料金の確実な徴収等を行うことが可能となる。
【００４３】
なお、上記第二の実施の形態で挙げた電子透かし付きの認証イメージは、一つのコンテンツに対し、複数のコンテンツ鑑定者が添付することもできる。これにより、ユーザに対し、複数のコンテンツ鑑定者から認証を受けていることを示すことができるので、コンテンツの安全性が高いことをアピールすることも可能である。
【００４４】
[第三の実施の形態]
次に、本発明の第三の実施の形態について説明する。以下に説明する第三の実施の形態では、上記第一の実施の形態で挙げた認証マーク、第二の実施の形態で挙げた電子透かしに代わり、保証書を用いる点が主な相違点である。したがって、上記第一または第二の実施の形態と共通する構成については同符号を付し、その説明を省略する。
図７は、本実施の形態におけるコンテンツ表示制限システムの概略を説明するための図である。
この図７に示すように、本実施の形態では、コンテンツ作成者は、作成したコンテンツを、コンテンツ作成者の端末１０Ｃにて、インターネット等のネットワーク２０上に公開する。また、コンテンツ作成者は、コンテンツ鑑定者によるコンテンツの認証を受け、認証がなされたことを示す認証マークのデータをコンテンツ鑑定者の端末３０Ｃからネットワーク２０を介して受け取る。そして、ユーザの端末５０Ｃからのアクセスを受けたときに、コンテンツ作成者の端末１０Ｃは、認証マークを添付したコンテンツのデータをユーザの端末５０Ｃに送信する。
一方、コンテンツ鑑定者の端末３０Ｃは保証書を作成し、この保証書をユーザの端末５０Ｃに送信する。この保証書は、例えば、「１５歳未満視聴不可」、「１８歳未満視聴不可」等、必要に応じて複数種が用意され、ユーザは自らが選択した種類の保証書のコンテンツ鑑定者からの発行を受ける。
ユーザの端末５０Ｃでは、受信したコンテンツに埋め込まれた認証マークに含まれる情報からコンテンツの正当性を確認するとともに、自らが発行を受けている保証書の種類に対応しているコンテンツのみ出力する。
【００４５】
コンテンツ作成者の端末１０Ｃは、上記第一の実施の形態に示したコンテンツ作成者の端末１０Ａと同様、通信部１１、入力部１２、表示部１３、コンテンツデータ格納部１４、処理部１５、を備える。
【００４６】
コンテンツ鑑定者の端末３０Ｃは、通信部３１、入力部３２、表示部３３、処理部３４Ｃ、クロック部３５、コンテンツＩＤ用暗号鍵ＤＢ３６、発行する保証書を暗号化・復号化するための秘密鍵・公開鍵のデータを格納した保証書用暗号鍵ＤＢ(キー情報格納手段)４１、を備える。
処理部３４Ｃは、ダイジェスト値計算部３７、認証マーク作成部３８、データ暗号化処理部３９の他、ユーザに対しての保証書を発行する保証書発行部(制御情報生成手段)４２、を備える。
【００４７】
ユーザの端末５０Ｃは、上記第一の実施の形態に示したユーザの端末５０Ａと同様、通信部５１、入力部５２、表示部５３、コンテンツ閲覧プログラム格納部５４、処理部５５、を備え、さらに、コンテンツ鑑定者の端末３０Ｃから発行された保証書のデータを格納する保証書データ格納部６０を備える。
また、処理部５５は、データ復号化処理部５６、コンテンツ検査処理部５７、コンテンツ表示制御部５８を備える。
【００４８】
次に、このようなコンテンツ表示制限システムにおいて、コンテンツを表示する際の流れについて説明する。

まず、コンテンツ鑑定者は、コンテンツ鑑定者の端末３０Ｃにて、ネットワーク２０上に公開されているコンテンツをサーチする。そして、コンテンツ鑑定者側で設定した所定の条件を満たすコンテンツが発見された場合、そのコンテンツに対し、認証マークを付与する処理を開始する。
これにはまず、図８に示すように、コンテンツ鑑定者の端末３０Ｃにて、通信部３１を介し、発見したコンテンツのデータを取得し、図示しないメモリ等に格納する(ステップＳ５０１)。
【００４９】
次いで、処理部３４Ｃでは、ダイジェスト値計算部３７において、取得したコンテンツのデータ(Ｄ)のダイジェスト値(Ｈｏ)を計算する(ステップＳ５０２)。ここでｈａｓｈはダイジェスト値を算出する計算式である。
Ｈｏ＝ｈａｓｈ(Ｄ)
【００５０】
続いて、処理部３４Ｃでは、認証マーク作成部３８にて、ダイジェスト値(Ｈｏ)と、コンテンツの鑑定を行った鑑定者ＩＤ(Ａｉｄ)、鑑定による認証を行った日付(時刻を含んでも良い)である認証日付を含む情報によって、コンテンツＩＤ(Ｄｉｄ)を作成する(ステップＳ５０３)。
作成されたコンテンツＩＤ(Ｄｉｄ)は、処理部３４Ｃのデータ暗号化処理部３９にて、コンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)によって計算式Ｓにより暗号化され、これによって認証マーク(Ｋｅ)が作成される(ステップＳ５０４)。
$Ke = S_{KpriA}(Did)$
この後、コンテンツ鑑定者の端末３０Ｃでは、認証マーク(Ｋｅ)のデータを、ネットワーク２０を介し、通信部３１からコンテンツ作成者の端末１０Ｃに送信する(ステップＳ５０５)。
【００５１】
上記のように認証マーク(Ｋｅ)のデータをコンテンツ作成者の端末１０Ｃに送信する一方で、コンテンツ鑑定者の端末３０Ｃでは、保証書発行部４２にて保証書(Ｇ)を作成する。この保証書(Ｇ)は、コンテンツＩＤ(Ｄｉｄ)の暗号化に用いられたコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)と対をなすコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)をコンテンツＩＤ用暗号鍵ＤＢ３６から取り出し、これをデータ暗号化処理部３９にて取り出したものである。このとき、暗号化には、保証書用暗号鍵ＤＢ４１から呼び出した保証書用秘密鍵(ＫｐｒｉＢ)を用いて、計算式Ｓにより実行する。(ステップＳ５０６)。
$G = S_{KpriB}(KpubA)$
そして、作成された保証書(Ｇ)のデータは、ユーザからの保証書発行の請求を受けると、これに応じて通信部３１からユーザの端末５０Ｃに送信される(ステップＳ５０７)。なお、この保証書(Ｇ)は、無料でユーザに対して発行しても良いが、これを有料として、コンテンツの視聴料の課金とすることもできる。この保証書(Ｇ)は、コンテンツ毎に発行しても良いし、会員制のようにして、予め登録したユーザに対して発行し、複数のコンテンツに対して有効なものとすることもできる。
【００５２】
さて、コンテンツ作成者の端末１０Ｃでは、前記ステップＳ５０５にて送信された認証マーク(Ｋｅ)のデータを、ネットワーク２０を介して通信部１１で受信すると、自動的、あるいはコンテンツ作成者が所定の操作を行うことにより、認証イメージのデータをコンテンツのデータ(Ｄ)に添付し、これをコンテンツデータ格納部１４に格納する。
そして、このようにコンテンツ鑑定者からのコンテンツの認証を受けて以降、コンテンツ作成者は、そのコンテンツ(以下、これを「認証付きコンテンツ」と適宜称する)をネットワーク２０上に公開する。
【００５３】
一方、ユーザ側は、認証付きコンテンツをユーザの端末５０Ｃで表示させるためのコンテンツ閲覧プログラムを予め導入(インストール)し、コンテンツ閲覧プログラム格納部５４

に格納しておく必要がある。なお、このコンテンツ閲覧プログラムには、前述の保証書(Ｇ)のデータを復号化するための保証書用公開鍵(ＫｐｕｂＢ)が内蔵されている。
また、ユーザの端末５０Ｃでは、前記ステップＳ５０７にてコンテンツ鑑定者の端末３０Ｃから送信された保証書(Ｇ)のデータを、ネットワーク２０を介して通信部５１で受信すると、自動的、あるいはコンテンツ作成者が所定の操作を行うことにより、保証書(Ｇ)のデータを保証書データ格納部６０に格納する。

【００５４】

この後、ユーザは、ユーザの端末５０Ｃを用い、ネットワーク２０上に公開された認証付きコンテンツにアクセスする。
コンテンツ作成者の端末１０Ｃでは、ネットワーク２０を介してユーザの端末５０Ｃからのアクセスを受けると、コンテンツデータ格納部１４に格納された、認証付きコンテンツ、つまり認証イメージのデータが添付されたコンテンツのデータ(Ｄ)を通信部１１から送出する。
図９に示すように、ユーザの端末５０Ｃでは、ネットワーク２０を介し、通信部５１が、認証イメージのデータが添付されたコンテンツのデータ(Ｄ)を受信(取得)し、これを図示しないメモリに一時格納する(ステップＳ６０１)。

【００５５】

そして、コンテンツ閲覧プログラムが起動されると、処理部５５は以下に示すような処理を実行する。
まず、保証書(Ｇ)のデータを、コンテンツ閲覧プログラムに内蔵されている保証書用公開鍵(ＫｐｕｂＢ)を用いて計算式Ｖにより復号化し、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)を得る(ステップＳ６０２)。

$$KpubA = V_{KpubB}(G)$$

【００５６】

続いて、データ復号化処理部５６が、コンテンツのデータ(Ｄ)に添付されている認証マーク(Ｋｅ)のデータを、ステップＳ６０２で得たコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)を用いて計算式Ｖによりによって復号化し、コンテンツＩＤ(Ｄｉｄ)を得る(ステップＳ６０３)。

$$Did = V_{KpubA}(Ke)$$

このとき、ユーザ側で保持している保証書(Ｇ)の種類が正しくない場合、つまりコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が認証マーク(Ｋｅ)を暗号化したコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)に対応したものでない場合には、認証マーク(Ｋｅ)のデータを復号化することはできず、これ以降の処理に進んでコンテンツの表示を行うことはできない。その場合、コンテンツの表示を行うことができない旨のメッセージを表示し、処理を終了することができる。

【００５７】

ここで、コンテンツＩＤに含まれる鑑定者ＩＤ(Ａｉｄ)や認証日付が正規のものかどうか、ネットワーク２０を介してコンテンツ鑑定者の端末３０Ｃに照会し、照会が完了した時点で以降のステップに進み、正規のものであるとの確認が取れないときには処理を中止し、コンテンツの表示を行わないこともできる。

【００５８】

続いて、コンテンツ検査処理部５７が、コンテンツのデータ(Ｄ)のダイジェスト値(Ｈｃ)を計算する一方(ステップＳ６０４)、コンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を抽出し(ステップＳ６０５)、双方のダイジェスト値(Ｈｏ)と(Ｈｃ)を比較する(ステップＳ６０６～Ｓ６０７)。
その結果、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しければ、コンテンツ表示制御部５８では、コンテンツのデータ(Ｄ)に基づき、表示部５３にコンテンツを表示する。このとき、コンテンツとともに、コンテンツＩＤ(Ｄｉｄ)に含まれる鑑定者ＩＤ(Ａｉｄ)、認証日付を表示することができる(ステップＳ６０８)

一方、ステップＳ６０７にて、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しくない場合、ユーザの端末５０Ｃで受け取ったコンテンツが、コンテンツ鑑定者側で鑑定されたコンテンツの内容と異なる、つまり改竄等がなされている可能性があるため、コンテンツ表示制御部５８では、コンテンツ閲覧プログラムを終了させ、コンテンツの表示を行わない。

【００５９】

上述したような構成によれば、ユーザの端末５０Ｃによっても、コンテンツ鑑定者によって認証されたコンテンツを表示させることができる。しかも、ダイジェスト値によって改竄の有無を確認し、改竄されていない場合のみコンテンツを表示させるようになっている。したがって、ユーザは、正当なコンテンツを安心して得ることができる。また、コンテンツ作成者側からすれば、視聴制限が行えることになり、予め登録された会員のみに対するコンテンツの公開や、視聴料金の確実な徴収等を行うことが可能となる。

加えて、コンテンツＩＤが含まれる認証マーク(Ｋｅ)をコンテンツ作成者の端末１０Ｃで公開するコンテンツに添付させる一方で、コンテンツ鑑定者の端末３０Ｃでは、保証書をユーザの端末５０Ｃに送るようにした。この保証書が無い限りコンテンツに添付された認証マーク(Ｋｅ)を復号化できないので、ユーザ以外の第三者によってコンテンツが開かれてしまうのを防ぐことができる。

さらに、コンテンツ鑑定者側から発行される保証書の種類を、ユーザ側で指定できるので、ユーザ側の都合に応じた視聴制限を行うことが可能となる。

【００６０】

[第四の実施の形態]

次に、本発明の第四の実施の形態について説明する。上記第一～第三の実施の形態ではコンテンツ鑑定者側でコンテンツのダイジェスト値の計算、コンテンツＩＤ等の発行を行ったが、以下に説明する第四の実施の形態では、これらの処理をコンテンツ作成者側で行う。また、上記第三の実施の形態でコンテンツ鑑定者からユーザに対して保証書を受け渡す例を挙げたが、第四の実施の形態では、さらにこれを適宜更新していくための構成を示す。以下の説明では、上記第一～第三の実施の形態と共通する構成については同符号を付し、その説明を省略する。

図１０は、本実施の形態におけるコンテンツ表示制限システムの概略を説明するための図である。

この図１０に示すように、本実施の形態では、コンテンツ作成者は、コンテンツ鑑定者の依頼に基づきコンテンツを作成する。コンテンツ作成者は、コンテンツ作成者の端末１０Ｄにて、コンテンツのダイジェスト値を計算してコンテンツＩＤを作成し、これをコンテンツに添付し、これをインターネット等のネットワーク２０上に公開する。そして、ユーザの端末５０Ｄからのアクセスを受けたときに、コンテンツ作成者の端末１０Ｄは、コンテンツのデータをユーザの端末５０Ｄに送信する。

一方、コンテンツ鑑定者の端末３０Ｄは保証書を作成し、この保証書をユーザの端末５０Ｄに送信する。この保証書は、例えば、「１２歳未満視聴不可」、「１５歳未満視聴不可」、「１８歳未満視聴不可」等、必要に応じて複数種が用意され、ユーザは自らが選択した種類の保証書のコンテンツ鑑定者からの発行を受ける。さらに、各保証書は保証番号を暗号化した状態で有しており、この保証番号がコンテンツ鑑定者側で適宜更新される。そして、保証番号が更新されるたびに、コンテンツ鑑定者はユーザに対し、最新の保証番号を通知する。

ユーザの端末５０Ｄでは、受信したコンテンツに埋め込まれた認証マークに含まれる情報からコンテンツの正当性を確認するとともに、自らが発行を受けている保証書の種類に対応しているコンテンツのみ出力する。

【００６１】

コンテンツ作成者の端末１０Ｄは、上記第一の実施の形態に示したコンテンツ作成者の端末１０Ａと同様、通信部１１、入力部１２、表示部１３、コンテンツデータ格納部１４、処理部１５Ｄ、を備える。本実施の形態では、コンテンツ作成者の端末１０Ｄは、さらに

、電子透かし付加プログラムを格納する電子透かし付加プログラム格納部１６を備える。
また、処理部１５Ｄは、コンテンツのダイジェスト値を計算するダイジェスト値計算部(ダイジェスト値算出手段)１７、コンテンツに添付するコンテンツＩＤを作成するコンテンツＩＤ作成部(制御情報生成手段)１８、通信部１１から送出するデータを暗号化するデータ暗号化処理部(情報暗号化手段)１９、を備える。

【００６２】

コンテンツ鑑定者の端末３０Ｄは、通信部３１、入力部３２、表示部３３、処理部３４Ｄ、クロック部３５、コンテンツＩＤ用暗号鍵ＤＢ３６、発行する保証書を暗号化・復号化するための秘密鍵・公開鍵のデータを格納した保証書用暗号鍵ＤＢ４１、を備える。
処理部３４Ｄは、ユーザに対して保証書を発行する保証書発行部(制御情報生成手段)４４、発行した保証書の保証番号を管理する保証番号管理部４５を備える。

【００６３】

ユーザの端末５０Ｄは、上記第一の実施の形態に示したユーザの端末５０Ａと同様、通信部５１、入力部５２、表示部５３、コンテンツ閲覧プログラム格納部５４、処理部５５、を備え、さらに、コンテンツ鑑定者の端末３０Ｄから発行された保証書および保証番号のデータを格納する保証書データ格納部６１を備える。
また、処理部５５は、データ復号化処理部５６、コンテンツ検査処理部５７、コンテンツ表示制御部５８を備える。

【００６４】

次に、このようなコンテンツ表示制限システムにおいて、コンテンツを表示する際の流れについて説明する。
まず、コンテンツ鑑定者は、コンテンツ作成者に対し、コンテンツの作成を依頼する。このような場合、コンテンツ鑑定者にとってコンテンツ作成者は信頼できるので、コンテンツ鑑定者は、コンテンツ作成者にコンテンツＩＤの作成まで依頼する。このために、コンテンツ鑑定者は、コンテンツに対して所定の電子透かしを付加するための電子透かし付加プログラムをコンテンツ作成者に送付する。コンテンツ作成者は、コンテンツ作成者の端末１０Ｄにて、送付された電子透かし付加プログラムを電子透かし付加プログラム格納部１６に格納する。
なお、これらコンテンツの作成の依頼、電子透かし付加プログラムの送付は、ネットワーク２０を介して行っても良いし、オフラインで行っても良い。

【００６５】

図１１に示すように、コンテンツ鑑定者からの依頼を受けてコンテンツを作成したコンテンツ作成者は、コンテンツ作成者の端末１０Ｄにて、作成したコンテンツに対し、電子透かし付加プログラムを起動させる(ステップＳ７０１)。
次いで、処理部１５Ｄでは、ダイジェスト値計算部１７において、作成したコンテンツのデータ(Ｄ)のダイジェスト値(Ｈｏ)を計算する(ステップＳ７０２)。ここでｈａｓｈはダイジェスト値を算出する計算式である。

Ｈｏ＝ｈａｓｈ(Ｄ)

【００６６】

続いて、処理部１５Ｄでは、コンテンツＩＤ作成部１８にて、ダイジェスト値(Ｈｏ)と、コンテンツの鑑定を行った鑑定者ＩＤ(Ａｉｄ)、鑑定による認証を行った日付(時刻を含んでも良い)である認証日付を含む情報によって、コンテンツＩＤ(Ｄｉｄ)を作成する(ステップＳ７０３)。
作成されたコンテンツＩＤ(Ｄｉｄ)は、処理部１５Ｄのデータ暗号化処理部１９にて、コンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)を用いて計算式Ｓにより暗号化されて認証マーク(Ｋｅ)が作成され、これを電子透かしとしてコンテンツのデータ(Ｄ)に付加し(埋め込み)、認証付きのコンテンツ(Ｄ’)のデータとする（ステップＳ７０４)。ここでＷＭは電子透かしの埋め込みのための計算式である。

$Ke = S_{KpriA}(Did)$

Ｄ’＝ＷＭ(Ｋｅ，ｄ)

ここで、暗号化に用いられるコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)は、複数種が用意され、コンテンツの種類や内容に応じたものがコンテンツ鑑定者あるいはコンテンツ作成者によって選択される。すなわち、コンテンツの内容に応じ、コンテンツ鑑定者あるいはコンテンツ作成者が、例えば、コンテンツを、「１２歳未満視聴不可」、「１５歳未満視聴不可」、「１８歳未満視聴不可」、「視聴制限なし」とランク付けし、そのランクに応じたコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)を用いてコンテンツＩＤ(Ｄｉｄ)を暗号化するのである。

この後、コンテンツ作成者の端末１０Ｄでは、電子透かしが付加された認証付きコンテンツのデータ(Ｄ’)をネットワーク２０上で公開する（ステップＳ７０５)。

【００６７】

一方、コンテンツ鑑定者の端末３０Ｄでは、保証書(Ｇ)を作成する。

これにはまず、図１２に示すように、保証書発行部４４にて、作成する保証書(Ｇ)に対してその時点で有効な保証番号と、コンテンツＩＤ(Ｄｉｄ)の暗号化に用いられたコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)と対をなすコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)とを含む保証書ＩＤ(Ｇｉｄ)を作成する(ステップＳ８０１)。

Ｇｉｄ＝Ｅ(保証番号、ＫｐｕｂＡ)

続いて、保証書ＩＤ(Ｇｉｄ)を暗号化し、保証書(Ｇ)を作成する。暗号化には、保証書用暗号鍵ＤＢ４１から呼び出した保証書用秘密鍵(ＫｐｒｉＢ)を用いて、計算式Ｓにより実行する(ステップＳ８０２)。

$G=S_{KpriB}(Gid)$

なおここで、作成される保証書(Ｇ)は、予めコンテンツ鑑定者側で複数種を用意することができる。この場合、それぞれの種類の保証書(Ｇ)は、種類に応じた保証番号とコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)を含むことになる。例えば、コンテンツ鑑定者側で、「１２歳未満視聴不可」、「１５歳未満視聴不可」、「１８歳未満視聴不可」の３種類の保証書を用意している場合、種類毎に、保証書に含まれる保証番号とコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が異なる。

【００６８】

そして、作成された保証書(Ｇ)のデータは、ユーザからの請求を受けると、通信部３１からユーザの端末５０Ｄに送信される(ステップＳ８０３)。

この保証書(Ｇ)は、無料、あるいは有料にて、ユーザが希望した種類に対応する保証番号と公開鍵を含んだものが発行される。

【００６９】

一方、ユーザ側は、認証付きコンテンツをユーザの端末５０Ｄで表示させるためのコンテンツ閲覧プログラムを予め導入(インストール)し、コンテンツ閲覧プログラム格納部５４に格納しておく必要がある。なお、このコンテンツ閲覧プログラムには、このコンテンツ閲覧プログラムが格納されるファイル内に設けられた所定のデータ格納領域に、前述の保証書(Ｇ)のデータを復号化するための保証書用公開鍵(ＫｐｕｂＢ)が内蔵されており、コンテンツ閲覧プログラムをユーザの端末５０Ｄにインストールすると、保証書用公開鍵(ＫｐｕｂＢ)は、ＨＤＤ等の所定のデータ格納部に格納される。

また、ユーザの端末５０Ｄでは、前記ステップＳ８０３にてコンテンツ鑑定者の端末３０Ｄから送信された保証書(Ｇ)のデータを、ネットワーク２０を介して通信部５１で受信すると、自動的、あるいはコンテンツ作成者が所定の操作を行うことにより、保証書(Ｇ)のデータを保証書データ格納部６１に格納する。

【００７０】

ところで、コンテンツ鑑定者の端末３０Ｄでは、保証番号管理部４５にて、各保証書(Ｇ)の保証番号を、例えば１ヶ月毎等の定期的に、あるいはコンテンツや保書内容に変更があった場合等の適宜タイミングで更新する。そして、ユーザの端末５０Ｄに対しては、最新の保証番号(のリスト)を定期的に送付する。ユーザの端末５０Ｄでは、送付された保証番号を保証書データ格納部６１に格納する。これによって、ユーザの端末５０Ｄでは、その時点で有効な最新の保証番号を保持していることになる。

【００７１】
さて、ユーザは、ユーザの端末５０Ｄを用い、ネットワーク２０上に公開された認証付きコンテンツにアクセスする。
コンテンツ作成者の端末１０Ｄでは、ネットワーク２０を介してユーザの端末５０Ｄからのアクセスを受けると、コンテンツデータ格納部１４に格納された、電子透かしが付加された認証付きコンテンツ(Ｄ’)のデータを通信部１１から送出する。
図１３に示すように、ユーザの端末５０Ｄでは、ネットワーク２０を介し、通信部５１が、認証付きコンテンツのデータ(Ｄ’)を受信(取得)し、これを図示しないメモリに一時格納する(ステップＳ９０１)。
【００７２】
そして、コンテンツ閲覧プログラムが起動されると、処理部５５は以下に示すような処理を実行する。
まず、保証書(Ｇ)のデータを、コンテンツ閲覧プログラムに内蔵されている保証書用公開鍵(ＫｐｕｂＢ)を用いて計算式Ｖにより復号化し、保証書ＩＤ(Ｇｉｄ)を得る(ステップＳ９０２)。

$$Gid = V_{KpubB}(G)$$

【００７３】
続いて、保証書ＩＤ(Ｇｉｄ)から、保証番号と、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)を取得する(ステップＳ９０３)。
そして、取得した保証番号が有効であるかどうかを、例えばネットワーク２０を介してコンテンツ鑑定者の端末３０Ｄに照会することで判定する(ステップＳ９０４～Ｓ９０５)。その結果、保証番号が無効であると判定された場合、コンテンツ閲覧プログラムでは処理を修了する。
【００７４】
一方、保証番号が有効であると判定された場合には、データ復号化処理部５６が、認証付きコンテンツ(Ｄ’)のデータから電子透かしとして埋め込まれている認証マーク（Ｋｅ）を抽出する。
ここで電子透かしが認証イメージから抽出できなかった場合、認証イメージが不正なものであるとして、これ以降の処理に進んでコンテンツの表示を行うことができない。
この後、暗号化されたコンテンツＩＤを、認証マーク（Ｋｅ）からステップＳ９０３で得たコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)を用いて計算式Ｖにより復号化し、コンテンツＩＤ(Ｄｉｄ)を得る(ステップＳ９０６)。ここでWM^{-1}は電子透かしの抽出のための計算式である。

$$Ke = WM^{-1}(D')$$

$$Did = V_{KpriA}(Ke)$$

ここで、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)が正しくない場合、つまり認証マーク(Ｋｅ)を暗号化したコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)に対応したものでない場合には、コンテンツＩＤ(Ｄｉｄ)を復号化することはできず、これ以降の処理に進んでコンテンツの表示を行うことはできない。その場合、コンテンツの表示を行うことができない旨のメッセージを表示し、処理を終了することができる。
さらに、ユーザ側で保持している保証書の種類がコンテンツの内容(ランク)に対応するものであるときには、保証書とともに保持しているコンテンツＩＤ用公開鍵(ＫｐｕｂＡ)によって、認証付きコンテンツ(Ｄ’)を復号化することができる。例えば、ユーザ側で、「１２歳未満視聴不可」という種類の保証書を有しており、コンテンツが「視聴制限なし」にランク付けされていれば、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)によって認証付きコンテンツ(Ｄ’)を復号化できるようになっているのである。これに対し、例えば、ユーザ側で、「１２歳未満視聴不可」という種類の保証書を有しており、コンテンツが「１５歳未満視聴不可」にランク付けされていれば、コンテンツＩＤ用公開鍵(ＫｐｕｂＡ)によって認証付きコンテンツ(Ｄ’)を復号化できず、これ以降の処理に進めないため、当然コンテンツの再生も行うことができない。

【００７５】
またここで、コンテンツＩＤに含まれる鑑定者ＩＤ(Ａｉｄ)や認証日付が正規のものかどうか、ネットワーク２０を介してコンテンツ鑑定者の端末３０Ｄに照会し、照会が完了した時点で以降のステップに進み、正規のものであるとの確認が取れないときには処理を中止し、コンテンツの表示を行わないこともできる。
【００７６】
続いて、コンテンツ検査処理部５７が、復号化された認証付きコンテンツ(Ｄ’)のデータに含まれるコンテンツのデータ(Ｄ)のダイジェスト値(Ｈｃ)を計算する(ステップＳ９０７)。そして、コンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を抽出し(ステップＳ９０８)、双方のダイジェスト値(Ｈｏ)と(Ｈｃ)を比較する(ステップＳ９０９～Ｓ９１０)。
その結果、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しければ、コンテンツ表示制御部５８では、コンテンツのデータ(Ｄ)に基づき、表示部５３にコンテンツを表示する。このとき、コンテンツとともに、コンテンツＩＤ(Ｄｉｄ)に含まれる鑑定者ＩＤ(Ａｉｄ)、認証日付を表示することができる(ステップＳ９１１)。
一方、ステップＳ９１０にて、算出されたダイジェスト値(Ｈｃ)がコンテンツＩＤ(Ｄｉｄ)に含まれるダイジェスト値(Ｈｏ)を等しくない場合、ユーザの端末５０Ｄで受け取ったコンテンツが、コンテンツ鑑定者側で鑑定されたコンテンツの内容と異なる、つまり改竄等がなされている可能性があるため、コンテンツ表示制御部５８では、コンテンツ閲覧プログラムを終了させ、コンテンツの表示を行わない。
【００７７】
また、図１４は、上記したような方法によってユーザに配信される認証付きコンテンツ(Ｄ’)の例を示すものである。図１４(ａ)に示すように、認証付きコンテンツ(Ｄ’)がＰＤＦファイル形式のようなテキストイメージである場合、および図１４(ｂ)に示すように、認証付きコンテンツ(Ｄ’)が静止画である場合は、コンテンツ(Ｄ)の一部に電子透かしが付加されている。
また、図１４(ｃ)に示すように、認証付きコンテンツ(Ｄ’)が動画である場合、動画の各フレームｆの画像(コンテンツ(Ｄ))の一部に電子透かしが付加されている。コンテンツが音声(オーディオ)である場合も、動画と同様、時間軸に沿って連続する音声のデータを、所定単位時間毎に区切り、各単位時間毎のデータに対し、電子透かしを付加する。
【００７８】
上述したような構成によれば、ユーザの端末５０Ｄによっても、コンテンツ鑑定者によって認証されたコンテンツを表示させることができる。しかも、ダイジェスト値によって改竄の有無を確認し、改竄されていない場合のみコンテンツを表示させるようになっている。したがって、ユーザは、正当なコンテンツを安心して得ることができる。
加えて、コンテンツＩＤをコンテンツ作成者の端末１０Ｄで公開するコンテンツに付加させる一方で、コンテンツ鑑定者の端末３０Ｄでは、保証書をユーザの端末５０Ｄに送るようにした。有効な保証書が無い限りコンテンツに付加された電子透かしからコンテンツＩＤを復号化できないので、ユーザ以外の第三者によってコンテンツが開かれてしまうのを防ぐことができる。したがって、コンテンツ作成者側からすれば、視聴制限が行えることになり、予め登録された会員のみに対するコンテンツの公開や、視聴料金の確実な徴収(課金)等を行うことが可能となる。
また、コンテンツ鑑定者側から発行される保証書の種類を、ユーザ側で指定できるので、ユーザ側の都合に応じた視聴制限を行うことが可能となる。
さらに、コンテンツ鑑定者側からユーザに対し、定期的に最新の保証番号を通知し、ユーザの端末５０Ｄにコンテンツとともに送付されるコンテンツＩＤに含まれる保証番号との照合を行う構成とした。これにより、ユーザ側で最新の保証番号を保持していない限り、コンテンツの表示は行えないことになる。つまり、このような構成では、例えばコンテンツ鑑定者側ではユーザに対し、１ヶ月ごと等、定期的に課金することが可能となる。正当

な課金を受けていないユーザ等は、最新の保証番号をコンテンツ鑑定者側から受け取ることができないため、コンテンツを表示させることができないのである。すなわち、上記したような構成は、コンテンツに対する課金を確実に行うことを実現可能とするのである。

【００７９】

このような構成は、上記で例に挙げた、「１２歳未満視聴不可」、「１５歳未満視聴不可」、「１８歳未満視聴不可」、「視聴制限なし」といった年齢による視聴制限以外にも適用できる。例えば、ケーブルテレビジョンのように、複数チャンネルでコンテンツを提供する場合等にも適用できる。例えば、全体で３０チャンネルが存在し、課金額に応じて、「１０チャンネル視聴可」のブロンズグレード、「２０チャンネル視聴可」のシルバーグレード、「全チャンネル視聴可」のゴールドグレードといったようにグレード分けをし、それぞれのグレードに応じた保証番号と保証書公開鍵をコンテンツ鑑定者側で発行する。そして、コンテンツのそれぞれに対し、「ゴールドグレードのみ視聴可」、「ゴールドグレードおよびシルバーグレード視聴可」、「全グレード視聴可」のような設定を行い、それぞれに応じて用意されたコンテンツＩＤ用秘密鍵(ＫｐｒｉＡ)でコンテンツＩＤを暗号化する。ユーザ側は、自らが登録しているグレードに応じた保証書用公開鍵と保証番号を受け取り、これによってコンテンツＩＤを復号化してコンテンツを再生するのである。

【００８０】

図１５は、上記したような構成を適用した、特に、動画やオーディオにおけるコンテンツの再生例を示す。

図１５(ａ)、(ｂ)に示すように、コンテンツ作成者の端末１０Ｄ側から認証付きコンテンツ(Ｄ’)として配信される動画や音声に対し、ユーザ側で有効な保証書が付加されている場所と、そうではない(ユーザ側で有効な保証番号を有していない電子透かし)場所とが交互にある場合、ユーザの端末５０Ｄ側では、ユーザ側で有効な保証書を有している電子透かしが付加されている場所のみが表示、再生され、そうでない場所は非表示、非再生となる。

これにより、例えば、映画や楽曲の１作品毎に保証書を設定し、有効な保証書を有している映画や楽曲のみをユーザ側で表示、再生することが可能となる。また、映画や楽曲の１作品の中で、保証書の種類を変え、例えば正規のユーザ(例えば会費を払っている会員)に対しては映画や楽曲を１作品通して表示、再生できるように保証番号をコンテンツ鑑定者から発行し、そうではないユーザ(例えば非会員)に対しては、いわゆるスクランブル放送のように、映画や楽曲の一部を断続的に表示、再生するよう、時間的に一部にのみ保証書を発行するようなことも可能となる。

なお、このようなコンテンツの配信方法は、上記第四の実施の形態だけでなく、第一～第三の実施の形態においても同様に行うことができる。

【００８１】

ところで、上記第四の実施の形態では、ユーザ側で複数の保証書、保証番号を入手できる構成とした。このような場合、ユーザ側でコンテンツを表示させるに際し、自らが有している複数の保証書の中から、使用する保証書を指定できる構成とすることもできる。

例えば、図１６(ａ)に示すように、ユーザが保証書＃１～＃３をコンテンツ鑑定者の端末３０Ｄから入手し、これをユーザの端末５０Ｄの保証書データ格納部６１で保持している場合、コンテンツを表示するに先立ち、適宜タイミングで、保持している保証書＃１～＃３のリストＬを表示部５３に表示させる。そして、ユーザが、リストＬ中から特定の保証書(例えば保証書＃１と＃３)を選択した場合、選択された保証書＃１と＃３に対応したコンテンツのみを表示させることができるのである。

さらにこのようなケースでは、リストＬを見て保証書の選択を行う場合、例えば子供が自分でユーザの端末５０Ｄを操作してしまうことも有り得るため、図１６(ｂ)に示すように、選択した保証書＃１と＃３のそれぞれに有効なパスワード(例えば保証書用公開鍵(ＫｐｕｂＢ))をユーザに入力させることもできる。このパスワードは、正しいパスワードが入力されたときに保証書の選択を有効とするためのものである。

パスワードが有効であれば、ここで図１３に示したステップＳ９０１～Ｓ９０５を実行し

、ステップＳ９０３で確認された保証書の種類を図１６(ｃ)に示すようにユーザに対して確認のために提示し、ユーザからの確認操作がなされた時点で、図１３に示したステップＳ９０６以降の処理を実行し、図１６(ｄ)に示すようにコンテンツ(Ｄ)の表示、あるいは図１６(ｅ)に示すようにコンテンツ(Ｄ)の非表示等を実行できる。

【００８２】

さらに、上記図１６(ａ)に示したような有効となる保証書の選択を、例えばＰＣの起動時やブラウザの起動時等に行われるログインＩＤやログインパスワードに関連付けて予め行っておき、ログインＩＤ、つまりユーザの端末５０Ｄの使用者に応じて、コンテンツの表示制限内容を自動的に切り換えることも可能である。

【００８３】

ところで、上記第一～第四の実施の形態において、コンテンツ鑑定者やコンテンツ作成者側からユーザに対して発行されるコンテンツ閲覧プログラムや、保証書等は、ネットワーク２０を介してユーザの端末５０Ａ、５０Ｂ、５０Ｃ、５０Ｄに対して送信するのではなく、ＣＤ－ＲＯＭ、フロッピーディスク等の可搬性のある記憶媒体に格納し、これを郵送等の手段でユーザに受け渡すこともできる。この場合、ユーザは、この記憶媒体に格納されたデータをユーザの端末５０Ａ、５０Ｂ、５０Ｃ、５０Ｄに読み込ませることによって、コンテンツ閲覧プログラムや保証書等のデータを導入する。さらに、第四の実施の形態で挙げた保証番号については、電子メール等でユーザに受け渡すことも可能である。

ところで、上記実施の形態では、コンテンツ作成者の端末１０Ａ、１０Ｂ、１０Ｃ、１０ＤからユーザのＰＣ５０Ａ、５０Ｂ、５０Ｃ、５０Ｄに対し、ネットワーク２０を介するものの、コンテンツのデータ(Ｄ)を直接受け渡す構成となっているが、もちろん、コンテンツ作成者が、自身の端末で作成したコンテンツをＩＳＰ(Internet Service Provider)やコンテンツ作成者自身(特に企業等の場合)のサーバを介してコンテンツをネットワーク２０上に公開する場合、サーバからユーザの端末５０Ａ、５０Ｂ、５０Ｃ、５０Ｄに対してコンテンツのデータ(Ｄ)を受け渡すことができる。つまり、サーバを上記コンテンツ作成者の端末１０Ａとして機能させるのである。

【００８４】

また、上記第一～第三の実施の形態では、コンテンツ鑑定者側でダイジェスト値の算出等を行い、コンテンツの鑑定を行う構成としたが、これを第四の実施の形態のように、コンテンツ作成者側で行うようにすることもできる。逆に、第四の実施の形態のように保証番号を用いる構成において、上記第一～第三の実施の形態のようにコンテンツ鑑定者側でダイジェスト値の算出等を行い、コンテンツの鑑定を行う構成とすることも可能である。

この他、上記第一～第四の実施の形態において、コンテンツＩＤ等を暗号化し、これを復号化するための公開鍵に、実質的なコンテンツの視聴制限機能を持たせる構成としたが、これに限るものではなく、キー情報として、例えばコンテンツ鑑定者側からユーザに対してパスワードや暗証番号等を発行し、このパスワードによってコンテンツの視聴制限機能を持たせることも可能である。

加えて、第四の実施の形態で、保証書の種類を、保証書用公開鍵の種類を変えることによって識別する構成としたが、コンテンツに付随するコンテンツＩＤ等に保証書の種類を識別するための情報を盛り込み、この情報とユーザの端末５０Ｄ側で保持する情報とを照合することによって、保証書の種類を識別するような構成とすることも可能である。

【００８５】

ところで、上記各実施の形態で示したような処理をコンピュータ装置に実行させる上記したようなプログラムは、ＣＤ－ＲＯＭ、ＤＶＤ、メモリ、ハードディスク等の記憶媒体に、コンピュータ装置が読み取り可能に記憶させることも可能である。

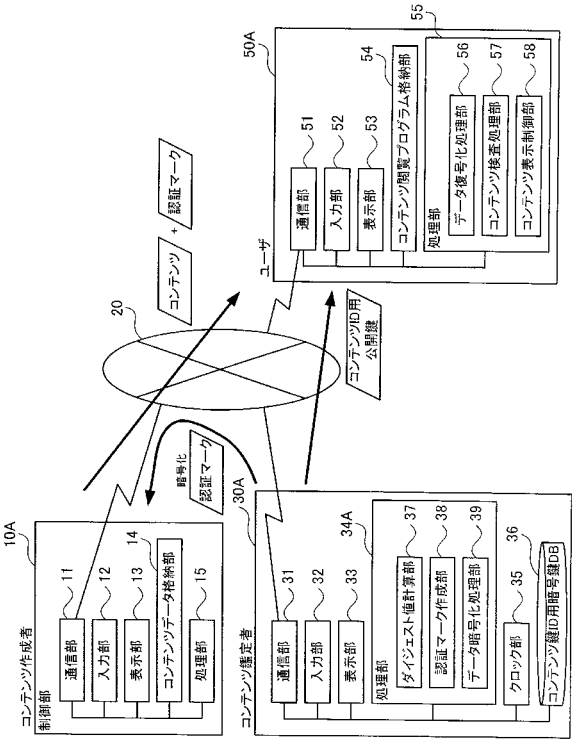
この他、上記第一～第四の実施の形態に挙げた構成を適宜組み合わせること等は、言うまでもなく可能なことである。

これ以外にも、本発明の主旨を逸脱しない限り、上記実施の形態で挙げた構成を取捨選択したり、他の構成に適宜変更することが可能である。

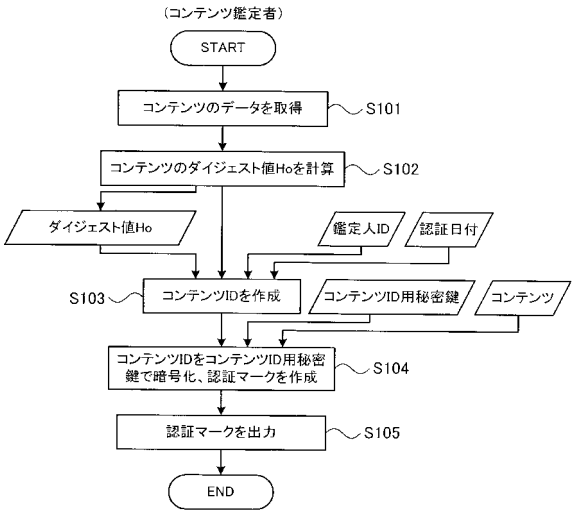
【００８６】

【発明の効果】
以上説明したように、本発明によれば、信頼できるコンテンツの表示制限を有効に行うことが可能となる。
【図面の簡単な説明】
【図１】　第一の実施の形態におけるコンテンツ表示制限システムの概略構成を示す図である。
【図２】　コンテンツ鑑定者側におけるコンテンツＩＤの生成処理の流れを示す図である。
【図３】　ユーザ側におけるコンテンツの再生処理を示す図である。
【図４】　第二の実施の形態におけるコンテンツ表示制限システムの概略構成を示す図である。
【図５】　コンテンツ鑑定者側におけるコンテンツＩＤの生成処理の流れを示す図である。
【図６】　ユーザ側におけるコンテンツの再生処理を示す図である。
【図７】　第三の実施の形態におけるコンテンツ表示制限システムの概略構成を示す図である。
【図８】　コンテンツ鑑定者側におけるコンテンツＩＤの生成処理の流れを示す図である。
【図９】　ユーザ側におけるコンテンツの再生処理を示す図である。
【図１０】　第四の実施の形態におけるコンテンツ表示制限システムの概略構成を示す図である。
【図１１】　コンテンツ作成者側におけるコンテンツＩＤの生成処理の流れを示す図である。
【図１２】　コンテンツ鑑定者における保証書の生成処理の流れを示す図である。
【図１３】　ユーザ側におけるコンテンツの再生処理を示す図である。
【図１４】　コンテンツの例を示す図である。
【図１５】　コンテンツの再生方法の例を示す図である。
【図１６】　保証内容を選択する場合に、ユーザの端末側で表示される表示内容の例を示す図である。
【符号の説明】
１０Ａ、１０Ｂ、１０Ｃ、１０Ｄ…コンテンツ作成者の端末、１１…通信部(コンテンツデータ受け渡し手段)、１５、１５Ｄ…処理部、１７…ダイジェスト値計算部(ダイジェスト値算出手段)、１８…コンテンツＩＤ作成部(制御情報生成手段)、１９…データ暗号化処理部(情報暗号化手段)、２０…ネットワーク、３０Ａ、３０Ｂ、３０Ｃ、３０Ｄ…コンテンツ鑑定者の端末、３１…通信部(情報転送手段)、３４Ａ、３４Ｂ、３４Ｃ、３４Ｄ…処理部、３６…コンテンツＩＤ用暗号鍵ＤＢ(キー情報格納手段)、３７…ダイジェスト値計算部(ダイジェスト値算出手段)、３８…認証マーク作成部(制御情報生成手段)、３９…データ暗号化処理部(情報暗号化手段)、４０…電子透かし作成部(制御情報生成手段)、４１…保証書用暗号鍵ＤＢ(キー情報格納手段)、４２、４４…保証書発行部(制御情報生成手段)、４５…保証番号管理部、５０Ａ、５０Ｂ、５０Ｃ、５０Ｄ…ユーザの端末、５４…コンテンツプログラム格納部、５５…処理部、５６…データ復号化処理部、５７…コンテンツ検査処理部、５８…コンテンツ表示制御部、６０、６１…保証書データ格納部

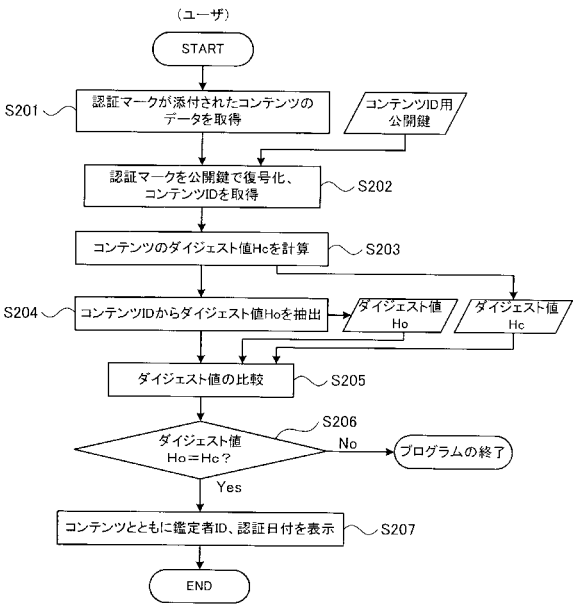
【図１】


50A
55
54
56
57
58
51
52
53
通信部
入力部
表示部
コンテンツ閲覧プログラム格納部
処理部
データ復号化処理部
コンテンツ検査処理部
コンテンツ表示制御部
ユーザ
コンテンツ＋認証マーク
20
コンテンツID用公開鍵
暗号化認証マーク
10A
30A
34A
コンテンツ作成者制御部
コンテンツ鑑定者
11
12
13
14
15
31
32
33
35
36
37
38
39
通信部
入力部
表示部
コンテンツデータ格納部
処理部
ダイジェスト値計算部
認証マーク作成部
データ暗号化処理部
クロック部
コンテンツID用暗号鍵DB

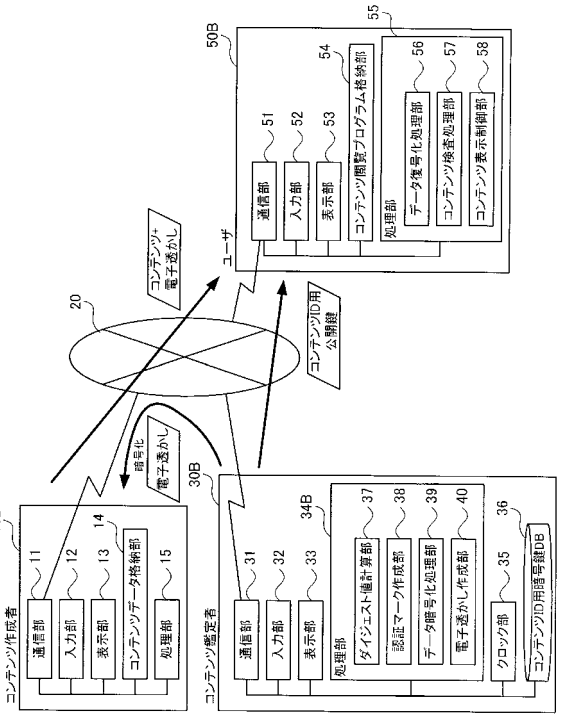
【図２】


（コンテンツ鑑定者）
START
コンテンツのデータを取得
S101
コンテンツのダイジェスト値Hoを計算
S102
ダイジェスト値Ho
鑑定人ID
認証日付
S103
コンテンツIDを作成
コンテンツID用秘密鍵
コンテンツ
コンテンツIDをコンテンツID用秘密鍵で暗号化、認証マークを作成
S104
認証マークを出力
S105
END

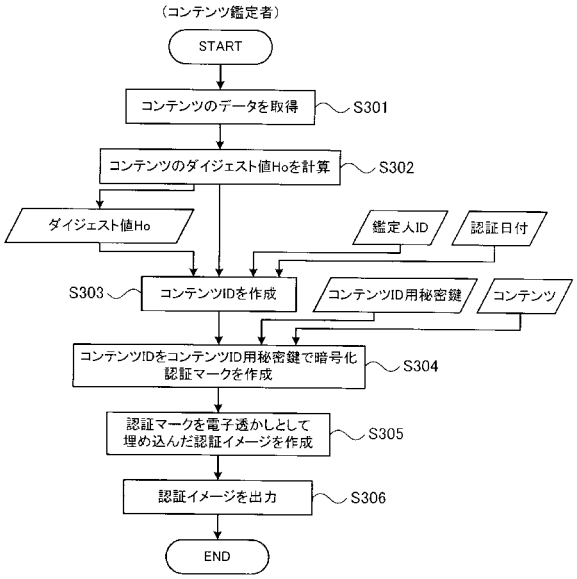
【図３】


（ユーザ）
START
S201
認証マークが添付されたコンテンツのデータを取得
コンテンツID用公開鍵
認証マークを公開鍵で復号化、コンテンツIDを取得
S202
コンテンツのダイジェスト値Hcを計算
S203
S204
コンテンツIDからダイジェスト値Hoを抽出
ダイジェスト値Ho
ダイジェスト値Hc
ダイジェスト値の比較
S205
S206
ダイジェスト値Ho＝Hc？
No
プログラムの終了
Yes
コンテンツとともに鑑定者ID、認証日付を表示
S207
END

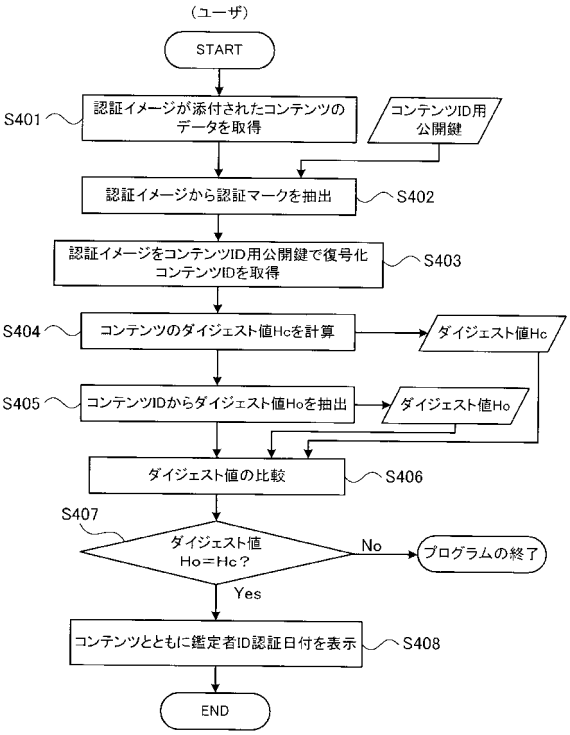
【図４】


50B
55
54
56
57
58
51
52
53
通信部
入力部
表示部
コンテンツ閲覧プログラム格納部
処理部
データ復号化処理部
コンテンツ検査処理部
コンテンツ表示制御部
ユーザ
コンテンツ＋電子透かし
20
コンテンツID用公開鍵
暗号化
電子透かし
10B
30B
34B
コンテンツ作成者
コンテンツ鑑定者
11
12
13
14
15
31
32
33
35
36
37
38
39
40
通信部
入力部
表示部
コンテンツデータ格納部
処理部
ダイジェスト値計算部
認証マーク作成部
データ暗号化処理部
電子透かし作成部
クロック部
コンテンツID用暗号鍵DB

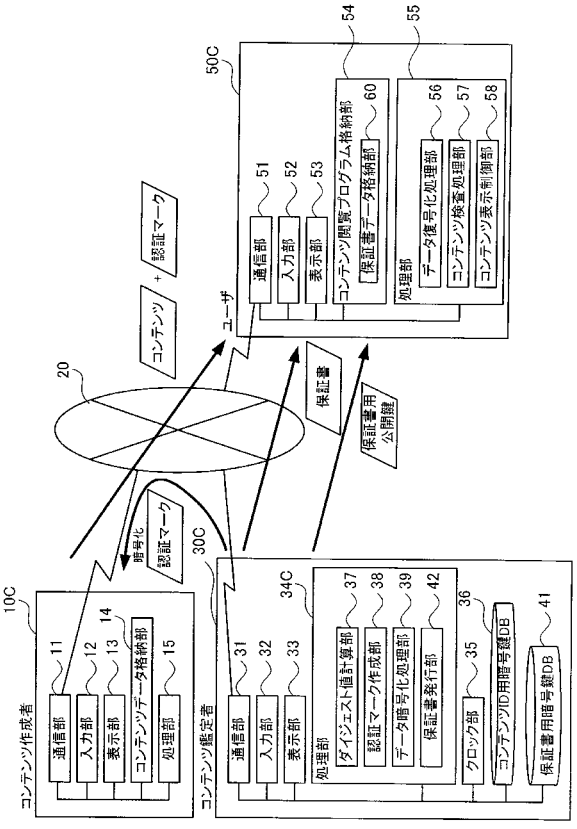
【図５】


（コンテンツ鑑定者）
START
コンテンツのデータを取得
S301
コンテンツのダイジェスト値Hoを計算
S302
ダイジェスト値Ho
鑑定人ID
認証日付
S303
コンテンツIDを作成
コンテンツID用秘密鍵
コンテンツ
コンテンツIDをコンテンツID用秘密鍵で暗号化
認証マークを作成
S304
認証マークを電子透かしとして
埋め込んだ認証イメージを作成
S305
認証イメージを出力
S306
END

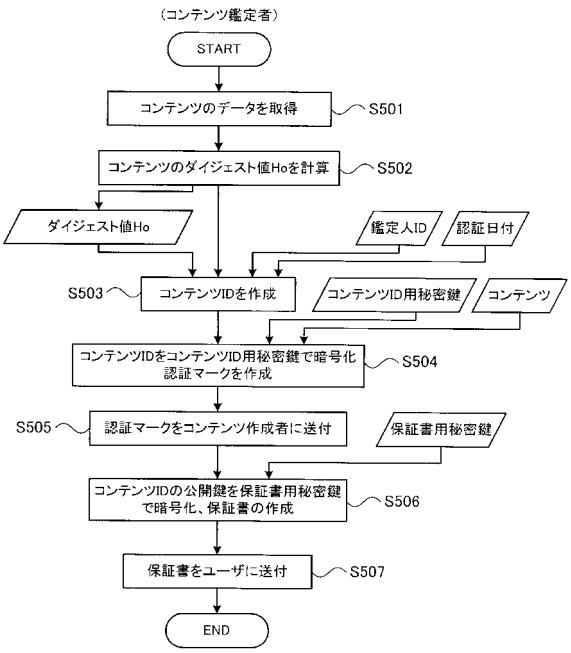
【図６】


（ユーザ）
START
S401
認証イメージが添付されたコンテンツの
データを取得
コンテンツID用
公開鍵
認証イメージから認証マークを抽出
S402
認証イメージをコンテンツID用公開鍵で復号化
コンテンツIDを取得
S403
S404
コンテンツのダイジェスト値Hcを計算
ダイジェスト値Hc
S405
コンテンツIDからダイジェスト値Hoを抽出
ダイジェスト値Ho
ダイジェスト値の比較
S406
S407
ダイジェスト値
Ho＝Hc？
No
プログラムの終了
Yes
コンテンツとともに鑑定者ID認証日付を表示
S408
END

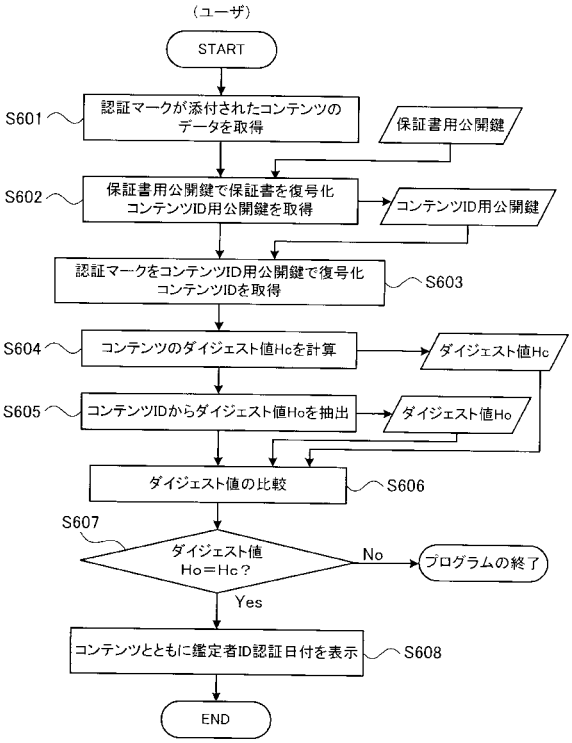
【図７】


50C
54
55
通信部
51
入力部
52
表示部
53
コンテンツ閲覧プログラム格納部
保証書データ格納部
60
処理部
データ復号化処理部
56
コンテンツ検査処理部
57
コンテンツ表示制御部
58
ユーザ
コンテンツ
＋
認証マーク
保証書
保証書用
公開鍵
20
暗号化
認証マーク
30C
34C
10C
コンテンツ作成者
通信部
11
入力部
12
表示部
13
コンテンツデータ格納部
14
処理部
15
コンテンツ鑑定者
通信部
31
入力部
32
表示部
33
処理部
ダイジェスト値計算部
37
認証マーク作成部
38
データ暗号化処理部
39
保証書発行部
42
クロック部
35
コンテンツID用暗号鍵DB
36
保証書用暗号鍵DB
41

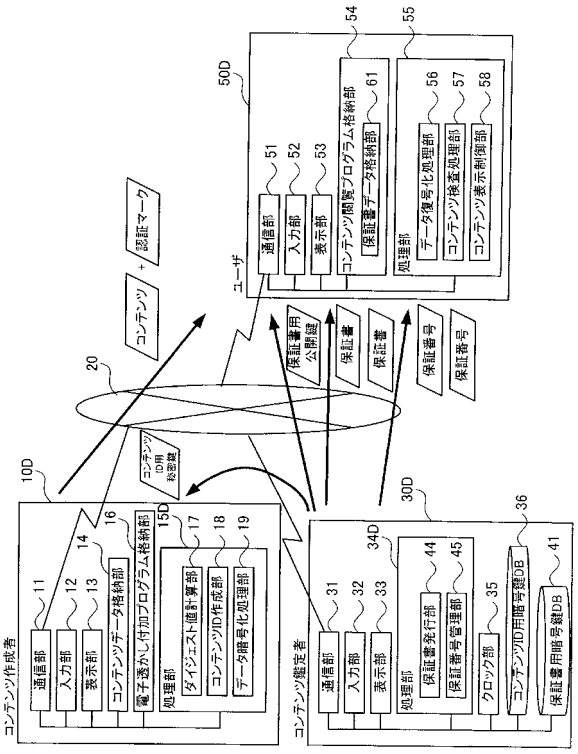
【図８】


（コンテンツ鑑定者）
START
コンテンツのデータを取得
S501
コンテンツのダイジェスト値Hoを計算
S502
ダイジェスト値Ho
鑑定人ID
認証日付
S503
コンテンツIDを作成
コンテンツID用秘密鍵
コンテンツ
コンテンツIDをコンテンツID用秘密鍵で暗号化
認証マークを作成
S504
S505
認証マークをコンテンツ作成者に送付
保証書用秘密鍵
コンテンツIDの公開鍵を保証書用秘密鍵
で暗号化、保証書の作成
S506
保証書をユーザに送付
S507
END

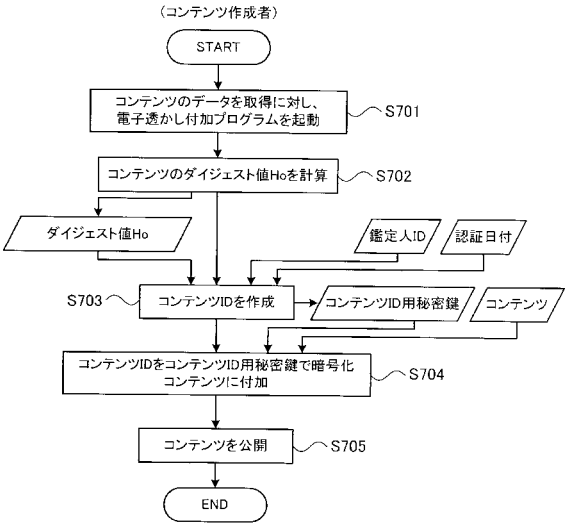
【図９】



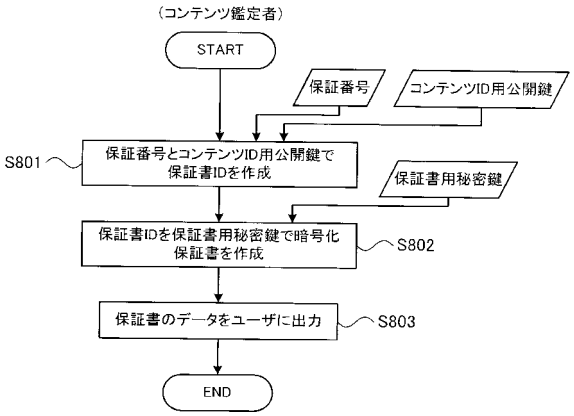
【図１０】



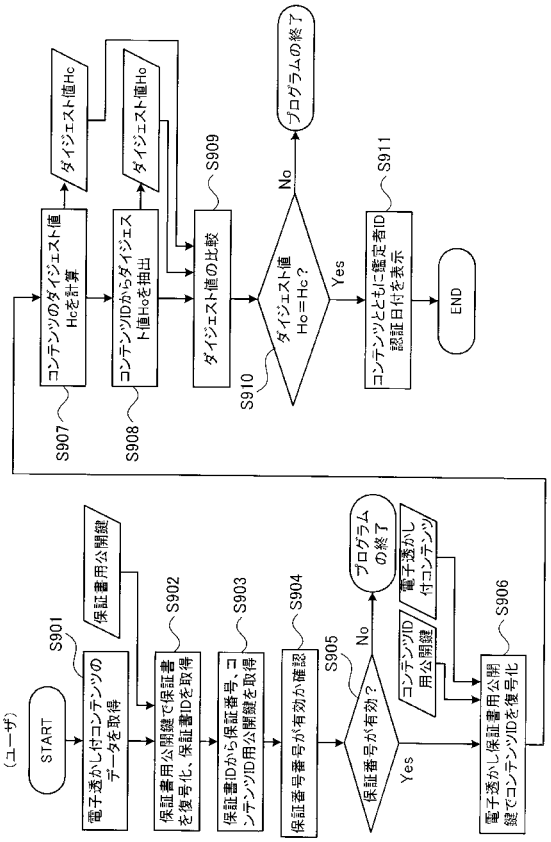
【図１１】



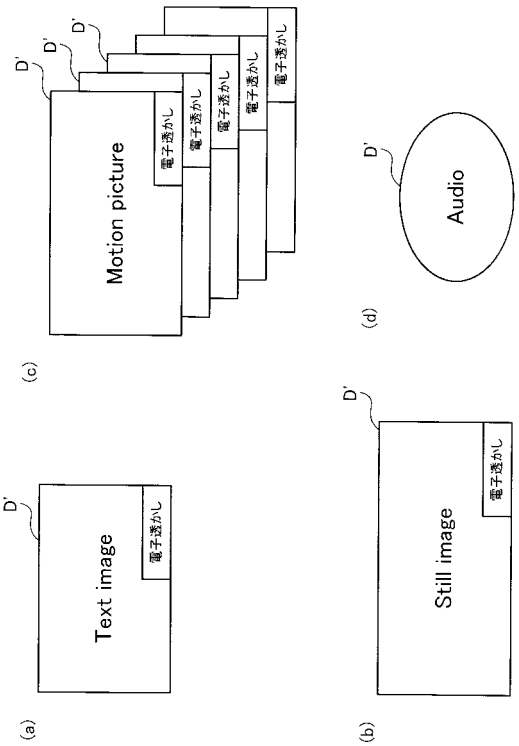
【図１２】



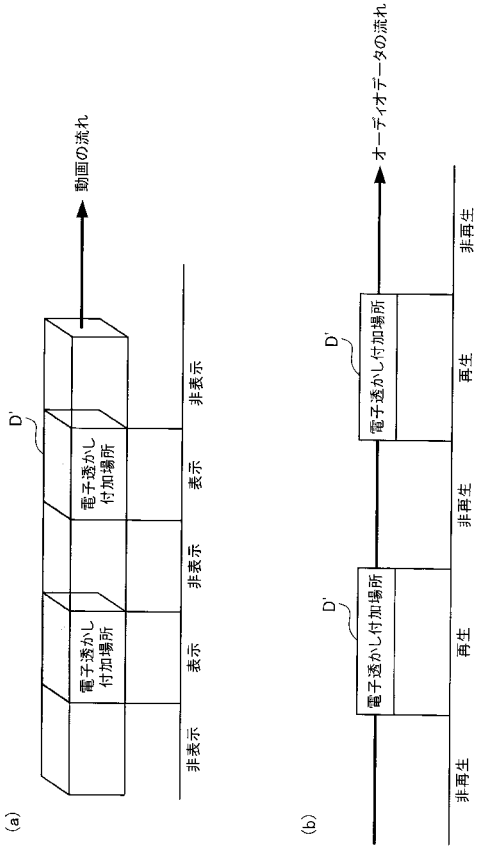
【図１３】



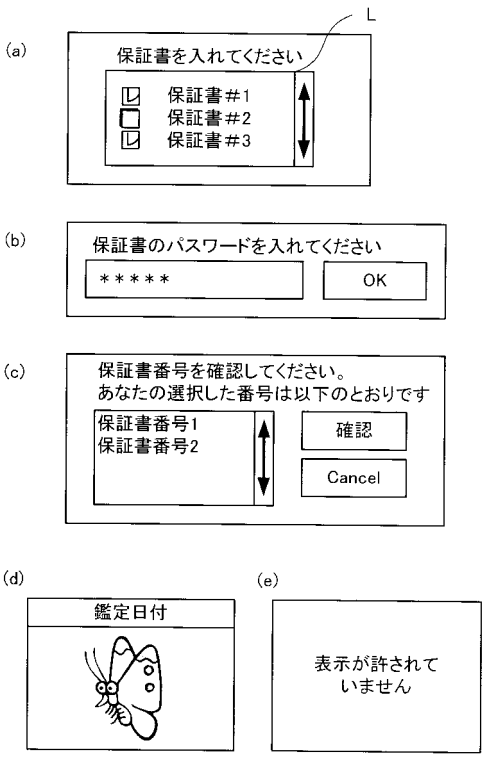
【図１４】



【図１５】



【図１６】



フロントページの続き

(51)Int.Cl.		FI		
H04N 1/387 (2006.01)		H04L	9/00	601F
		H04N	1/387	
		H04L	9/00	675D

(72)発明者 利根川 聡子
神奈川県大和市下鶴間１６２３番地１４ 日本アイ・ビー・エム株式会社 大和事業所内
(72)発明者 大門 昭
神奈川県大和市下鶴間１６２３番地１４ 日本アイ・ビー・エム株式会社 大和事業所内

審査官 金丸 昌司

(56)参考文献 特開２００２－０４１９９３（ＪＰ，Ａ）
特開２００１－０６９３４３（ＪＰ，Ａ）
岡本栄司，「暗号理論入門」，共立出版株式会社，１９９７年１０月２４日，p.134,135

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00
JSTPlus(JDream2)