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

特許第4136534号
(P4136534)

(45)発行日　平成20年8月20日(2008.8.20)　(24)登録日　平成20年6月13日(2008.6.13)

(51)Int.Cl.		F I		
H04H 60/73	(2008.01)	H04H	60/73	
H04H 60/16	(2008.01)	H04H	60/16	
H04H 60/20	(2008.01)	H04H	60/20	
H04H 60/23	(2008.01)	H04H	60/23	
H04N 7/08	(2006.01)	H04N	7/08	Z

請求項の数 6　(全 16 頁)　最終頁に続く

(21)出願番号　特願2002-239775 (P2002-239775)
(22)出願日　平成14年8月20日 (2002.8.20)
(65)公開番号　特開2003-204308 (P2003-204308A)
(43)公開日　平成15年7月18日 (2003.7.18)
審査請求日　平成17年8月11日 (2005.8.11)
(31)優先権主張番号　特願2001-338363 (P2001-338363)
(32)優先日　平成13年11月2日 (2001.11.2)
(33)優先権主張国　日本国(JP)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　田頭　信博
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
(72)発明者　岩村　恵市
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　川口　貴裕

最終頁に続く

(54)【発明の名称】デジタルコンテンツ処理装置、デジタルコンテンツ処理方法、コンピュータプログラム及び記録媒体

(57)【特許請求の範囲】

【請求項１】

デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の信頼度を示す鍵信頼度リストを記憶部に保持するデジタルコンテンツ処理装置であって、

前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信手段と、

鍵を用いて、前記受信手段によって受信されたメタ情報を復号する復号手段と、

前記復号手段による前記メタ情報の復号結果と、前記記憶部に保持されている前記復号に用いた鍵の鍵信頼度リストとに基づいて、前記メタ情報の信頼度を検証する検証手段と、

前記検証手段により検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量または前記デジタルコンテンツの編集の許容量を大きくするように制御する制御手段とを有することを特徴とするデジタルコンテンツ処理装置。

【請求項２】

デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の証明書を記憶部に保持するデジタルコンテンツ処理装置であって、

前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置

より受信部を介して受信する受信手段と、
鍵を用いて、前記受信手段によって受信されたメタ情報の署名の検証を行う署名検証手段と、
前記署名検証手段による署名の検証結果と、前記記憶部に保持されている前記メタ情報の署名の検証に用いた鍵の証明書とに基づいて、前記メタ情報の信頼度を検証する検証手段と、
前記検証手段により検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量を大きくするように制御する制御手段とを有することを特徴とするデジタルコンテンツ処理装置。
【請求項３】
デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の信頼度を示す鍵信頼度リストを記憶部に保持するデジタルコンテンツ処理装置におけるデジタルコンテンツ処理方法であって、
受信手段が、前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信工程と、
鍵を用いて、前記受信工程において受信されたメタ情報を復号手段が復号する復号工程と、
前記復号工程における前記メタ情報の復号結果と、前記記憶部に保持されている前記復号に用いた鍵の鍵信頼度リストとに基づいて、前記メタ情報の信頼度を検証手段が検証する検証工程と、
前記検証工程において検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量または前記デジタルコンテンツの編集の許容量を大きくするように制御手段が制御する制御工程とを有することを特徴とするデジタルコンテンツ処理方法。
【請求項４】
デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の証明書を記憶部に保持するデジタルコンテンツ処理装置におけるデジタルコンテンツ処理方法であって、
受信手段が、前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信工程と、
鍵を用いて、前記受信工程において受信されたメタ情報の署名の検証を署名検証手段が行う署名検証工程と、
前記署名検証工程における署名の検証結果と、前記記憶部に保持されている前記メタ情報の署名の検証に用いた鍵の証明書とに基づいて、前記メタ情報の信頼度を検証手段が検証する検証工程と、
前記検証工程において検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量を大きくするように制御手段が制御する制御工程とを有することを特徴とするデジタルコンテンツ処理方法。
【請求項５】
請求項１または２に記載のデジタルコンテンツ処理装置の各手段としてコンピュータを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６】
請求項５に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はデジタルコンテンツ処理装置、デジタルコンテンツ処理方法、コンピュータプ

ログラム及び記録媒体に関する。

【０００２】

【従来の技術】

昨今のデジタル化の流れにより、さまざまな分野でデジタル化が進められている。放送の分野でもデジタル化が進められており、一部でデジタル放送が実現されている。デジタル放送では、放送番組とともに、その番組内容を記載したメタ情報などを送信することが可能であることから、大容量蓄積機能(以下、ストレージという)を有する受信機でこれらの情報を活用し、番組の自動蓄積、シーン検索、ダイジェスト視聴等など、デジタル放送のメリットを活かした新たなサービスの提案されつつある。

【０００３】

国際的にも検討が進められており、TV Anytime Forum を中心に放送方式に関する技術的な検討の中で、メタ情報等に関する議論に一定の進展が図られつつある。また、昨今のハードディスクの大容量化に伴い、デジタル放送のコンテンツを記録するハードディスク・レコーダが既に市販されるなど、このようなサービスの実現に向けた環境が整ってきているとともに、デジタル放送においては、不正なコピーから放送コンテンツを守るための方策も必須なものとして求められている。

【０００４】

なお、大容量蓄積機能を有する受信機は、インターネットや他の情報家電との接続機能など、ホームサーバとしての機能も期待されていることから、「サーバ型受信機」と呼ばれており、またサーバ型受信機向けの放送は「サーバ型放送」と呼ぶ。

【０００５】

一方、従来、有料放送方式は、テレビジョン放送や高精細度テレビジョン放送（以下、ハイビジョン放送という）に適用した限定受信方式が広く検討されてきた。有料方式で一般的に放送される映像信号や音声信号は、受信が許可された者以外の者により受信できないように、何らかの方法でスクランブル(撹拌)が施され、受信が許可された者にはこのスクランブルされた信号を復元するための信号を送って受信を制御するようになっている。

【０００６】

この受信を制御するための信号として送られる情報は、関連情報と呼ばれ、スクランブルを復元するための鍵（スクランブル鍵 Ks ）の情報、放送される番組が各受信者の契約範囲に入っているか否かを判定するための情報、放送局から特定の受信機を強制的にオン・オフするための情報等によりなっている。

【０００７】

衛星放送でテレビジョンやハイビジョンの有料放送を行う場合には、関連情報はデータチャンネルでパケットの形で伝送される。この場合、スクランブル鍵や、放送番組に関する情報(これは番組情報と呼ばれる)は、第三者に知られたり改ざんされたりしないように暗号化される。

【０００８】

この暗号化のための鍵はワーク鍵 Kw と呼ばれ、各受信者の契約した内容を表わす契約情報とともに別途受信者に送られる。この関連情報は個別情報と呼ばれ、放送電波、ICカード、磁気カード等の物理媒体、電話線等で送られる。これらのうち、電波で送る場合には、必ず暗号化する必要があり、この暗号化に用いられる鍵は、マスター鍵 Km と呼ばれ、原則的にはそれぞれの受信者毎に異なっている。

【０００９】

図８に、このようなスクランブルを施す方式の構成例を示す。図８において、８０１～８０８は放送側を示し、８０１はスクランブル部、８０２は多重化部、８０３はスクランブル鍵（Ｋｓ）、８０４はワーク鍵（Ｋｗ）、８０５は契約情報、８０６及び８０７は暗号化部、８０８はマスター鍵（Ｋｍ）である。

【００１０】

また、８０９～８１５は受信側を示し、８０９は分離部、８１０はデスクランブル部、８１１，８１２は複合部、８１３は視聴判定部、８１４は契約情報、８１５はマスター鍵（

Ｋｍ）である。
【００１１】
【発明が解決しようとする課題】
サーバ型放送では、さまざまなメタ情報の利用が想定されている。かつ、メタ情報の提供は放送事業者だけに限定されておらず、インターネット等の通信媒体を経由してさまざまな事業者やユーザからの配信も想定されている。
【００１２】
また、メタ情報には、番組のタイトルのような単純なメタ情報もある。一方で、メタ情報によって番組のダイジェストを生成するといった番組の見え方をも変更するようなメタ情報もある。
【００１３】
ところで、番組の見え方まで変更するような場合、その行為は番組の改変にあたる行為とみなされ、著作権法を考慮しなければいけない可能性も生じる。このように、メタ情報はさまざまな特徴を持つが、メタ情報の信頼性や有効性を検証可能な仕組みが考慮されていなかった。
【００１４】
また、従来の限定受信方式では、放送事業者以外からのメタ情報の配信は想定されておらず、いわんや、メタ情報の信頼性や有効性を検証することが可能な仕組みはまったく考慮されていなかった。
【００１５】
本発明は上述の問題点にかんがみてなされたもので、メタ情報の信頼性や有効性を検証できるようにすることを第１の目的とする。
また、メタ情報の信頼性や有効性に応じて、番組情報を制御可能なシステムを提供することを第２の目的とする。
【００１６】
【課題を解決するための手段】
本発明のデジタルコンテンツ処理装置は、デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の信頼度を示す鍵信頼度リストを記憶部に保持するデジタルコンテンツ処理装置であって、前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信手段と、鍵を用いて、前記受信手段によって受信されたメタ情報を復号する復号手段と、前記復号手段による前記メタ情報の復号結果と、前記記憶部に保持されている前記復号に用いた鍵の鍵信頼度リストとに基づいて、前記メタ情報の信頼度を検証する検証手段と、前記検証手段により検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量または前記デジタルコンテンツの編集の許容量を大きくするように制御する制御手段とを有することを特徴とする。
また、本発明のデジタルコンテンツ処理装置の他の特徴とするところは、デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の証明書を記憶部に保持するデジタルコンテンツ処理装置であって、前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信手段と、鍵を用いて、前記受信手段によって受信されたメタ情報の署名の検証を行う署名検証手段と、前記署名検証手段による署名の検証結果と、前記記憶部に保持されている前記メタ情報の署名の検証に用いた鍵の証明書とに基づいて、前記メタ情報の信頼度を検証する検証手段と、前記検証手段により検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量を大きくするように制御する制御手段とを有することを特徴とする。
【００１７】
本発明のデジタルコンテンツ処理方法は、デジタルコンテンツと、前記デジタルコンテ

ンツに関連するメタ情報とを取り扱うとともに、鍵の信頼度を示す鍵信頼度リストを記憶部に保持するデジタルコンテンツ処理装置におけるデジタルコンテンツ処理方法であって、受信手段が、前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信工程と、鍵を用いて、前記受信工程において受信されたメタ情報を復号手段が復号する復号工程と、前記復号工程における前記メタ情報の復号結果と、前記記憶部に保持されている前記復号に用いた鍵の鍵信頼度リストとに基づいて、前記メタ情報の信頼度を検証手段が検証する検証工程と、前記検証工程において検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量または前記デジタルコンテンツの編集の許容量を大きくするように制御手段が制御する制御工程とを有することを特徴とする。

また、本発明のデジタルコンテンツ処理方法の他の特徴とするところは、デジタルコンテンツと、前記デジタルコンテンツに関連するメタ情報とを取り扱うとともに、鍵の証明書を記憶部に保持するデジタルコンテンツ処理装置におけるデジタルコンテンツ処理方法であって、受信手段が、前記デジタルコンテンツを、デジタルコンテンツを取り扱う第１の情報処理装置より受信するとともに、暗号化された前記メタ情報を、メタ情報を取り扱う第２の情報処理装置より受信部を介して受信する受信工程と、鍵を用いて、前記受信工程において受信されたメタ情報の署名の検証を署名検証手段が行う署名検証工程と、前記署名検証工程における署名の検証結果と、前記記憶部に保持されている前記メタ情報の署名の検証に用いた鍵の証明書とに基づいて、前記メタ情報の信頼度を検証手段が検証する検証工程と、前記検証工程において検証された信頼度が高いほど、前記デジタルコンテンツを再生したときの視聴の変化の許容量を大きくするように制御手段が制御する制御工程とを有することを特徴とする。

【００１８】

本発明のコンピュータプログラムは、前記に記載のデジタルコンテンツ処理装置の各手段としてコンピュータを機能させることを特徴とする。

【００１９】

本発明の記録媒体は、前記に記載のコンピュータプログラムを記録したことを特徴とする。

【００２２】

【発明の実施の形態】

次に、添付図面を参照しながら本発明のデジタルコンテンツ処理装置、デジタルコンテンツ処理方法、コンピュータプログラム及び記録媒体の実施の形態について説明する。

【００２３】

図１は、本発明の第１の実施の形態にかかるシステムの構成例を示す。第１の実施の形態は、単一または複数の管理者と単一または複数の放送事業者と単一または複数のメタ情報提供事業者と複数の受信者から構成される。それぞれは、さまざまな通信媒体で相互接続されている。

【００２４】

管理者１１は、システム全体の運用を管理する。つまり、システムで用いる鍵の発行等を管理する。

【００２５】

放送事業者１２は、番組情報を放送によって提供するエンティティ（Entity）であり、一般的には放送局に相当する。ただし、本実施の形態は、特に映像の放送に限ったものでなく、ラジオ放送等の音楽放送にも適応可能であるし、データ放送等の一般的なコンテンツの放送にも適応可能であることが明らかである。本実施の形態では、これらの放送コンテンツを総称して番組情報と呼ぶ。

【００２６】

メタ情報提供業者１３は、番組内容を記述したメタ情報を提供するエンティティである。従来の放送では、メタ情報提供業者１３は放送事業者と同一のエンティティであったが、

サーバ型放送を想定した場合、この限りでない。

【００２７】

つまり、サーバ型放送では、蓄積媒体に番組情報を保持することを想定しており、同様にメタ情報の保持も想定されている。また、サーバ型受信機はネットワーク接続機能を有しているため、ネットワーク１５、通信衛星１６、１７等を経由して、番組情報と独立してメタ情報を受信することも考えられる。

【００２８】

つまり、メタ情報の提供は、蓄積媒体に保持することが可能なため、番組情報と同じ通信媒体で提供される必要もなく、かつ番組情報と同じ時刻に提供される必要もない。これは、メタ情報の提供を、放送事業者１２以外のエンティティから容易に行えることを示している。図１において、受信者１４は番組情報を受信し、番組を視聴するエンティティである。

【００２９】

放送事業者１２と他のエンティティ間は代表的には電波放送という通信媒体であるが、光ファイバ等のその他の通信媒体でも実現可能である。また、受信者１４とメタ情報提供事業者１３間は、放送事業者を経由した電波放送という一方向の通信媒体だけでなく、電話回線網、携帯電話網、ケーブルテレビ網等さまざまな双方向通信媒体も存在する。なお、放送事業者１２はメタ情報提供事業者１３になる場合もある。さらに、放送事業者１２は管理者１１になる場合もある。

【００３０】

図２に、メタ情報提供業者１３と受信者１４の構成の一例を示す。図２に示すように、メタ情報提供事業者１３と受信者１４との間は通信媒体で接続されている。メタ情報提供事業者１３は管理者から配布された第１の鍵１３１を保持している。また、メタ情報提供事業者１３は、暗号化部１３２を持っている。

【００３１】

暗号化部１３２は、メタ情報提供事業者１３が生成したメタ情報を保持する第１の鍵１３１で暗号化し、暗号化メタ情報を出力する。暗号アルゴリズムは、特に限定しない。

【００３２】

受信者１４は、管理者１１から配布された複数の鍵１４ａ、１４ｂ、１４ｃと、鍵信頼度リスト１４１を保持している。複数の鍵１４ａ～１４ｃには、管理者１１によってメタ情報提供事業者１３へ配布された鍵を含む。

【００３３】

また、鍵信頼度リスト１４１は、管理者１１によって決定された鍵の信頼度を示すデータであって、各鍵毎に設定されている。設定方法の一つは、対応する鍵を保持するメタ情報提供事業者１３の信頼度から決定する。また、受信者１４は、復号部１４２と、鍵選択部１４３と、検証部１４４とを持っている。

【００３４】

復号部１４２は、鍵選択部１４３から出力される鍵情報を用いて暗号化メタ情報を復号する。復号アルゴリズムは、メタ情報提供事業者１３の暗号化部１３２で用いられている暗号化アルゴリズムに対応するアルゴリズムである。

【００３５】

鍵選択部１４３は、保持している複数の鍵１４ａ～１４ｃの中から処理に用いる鍵を選択する。選択方法は、保持している全ての鍵を順に選択する方法や復号部に入力される暗号化メタ情報のヘッダ部分に鍵の識別情報を付加する方法などが考えられる。

【００３６】

検証部１４４は、復号部の復号結果と復号に用いた鍵と鍵信頼度リスト１４１から、信頼度情報を出力する。

【００３７】

図２は、メタ情報発信側のメタ情報提供事業者１３とメタ情報の受信側の受信者１４との間で共通の鍵を共有することによって、暗号化通信を実現している。さらに、メタ情報は

バイナリデータでなく、何らかのフォーマットを持っている。つまり、復号部１４２の復号データがこのメタ情報のフォーマットに従っているか否かを調べることで、メタ情報の正当性の検証が可能である。

【００３８】

以上により、メタ情報の正当性が確認できた場合には、鍵信頼度リスト１４１を参照することで、用いた鍵に対応する信頼度を調べることが可能になり、メタ情報に対する信頼度を決定することが可能になる。

【００３９】

メタ情報の正当性が確認できなかった場合は、メタ情報に対する信頼度は最下級とする。例えば、前述のように、鍵信頼度リスト１４１を、鍵を保有するメタ情報提供事業者１３の信頼度とした場合、メタ情報の信頼度情報は、メタ情報を作成したメタ情報提供事業者１３の信頼度となる。

【００４０】

図２の基本構成を既存の受信者限定放送に適応した場合の構成例を図３に示す。図３は、放送事業者１２０とメタ情報提供業者１３０と受信者１４０とから構成され、受信者限定放送である。

【００４１】

受信者限定放送で放送される番組情報は、受信が許可された者以外の者により受信できないように、何らかの方法でスクランブルが施される。受信が許可された者にはこのスクランブルされた信号を復元するための信号を送って受信制御する。

【００４２】

図３において、放送事業者１２０は、管理者から配布された第１の鍵１２８を保持し、スクランブル部１２１、多重化部１２４、第１の暗号化部１２３、第２の暗号化部１２７から構成される。

【００４３】

スクランブル部１２１は、スクランブル鍵 Ks １２２を用いて、番組情報をスクランブルする。第１の暗号化部１２３は、ワーク鍵 Kw １２５を用いて、スクランブル鍵 Ks １２２を暗号化する。

【００４４】

第２の暗号化部１２７は、第１の鍵１２８を用いて、ワーク鍵１２５、契約情報１２６を暗号化する。多重化部１２４は、スクランブル部１２１から出力される暗号化番組情報と、第１の暗号化部１２３から出力される暗号化スクランブル鍵１２２と、必要に応じて第２の暗号化部１２７から出力される暗号化情報を多重化する。ただし、第２の暗号化部から出力される暗号化情報は、多重化されないで、通信媒体を経由して直接受信者へ送信される場合もある。

【００４５】

第１の暗号化部１２３と第２の暗号化部１２７とを用いて暗号化の多重化構造を持たせることで、複数の受信者に対して個別の視聴制御を可能にする一方で、視聴を制御するワーク鍵１２５や契約情報１２６等の個別情報のサイズを小さくしている。

【００４６】

図３において、メタ情報提供事業者１３０は、基本構成と同様であり、管理者から配布された第２の鍵１３３を保持し、第３の暗号化部１３５を持っている。第３の暗号化部１３５は、メタ情報提供事業者１３０が生成したメタ情報１３４を、保持している第２の鍵１３３で暗号化し、暗号化メタ情報をネットワーク１６０に出力する。

【００４７】

図３において、受信者１４０は、管理者から配布された複数の鍵１５０と、鍵信頼度リスト１４８を保持し、分離部１４１、デスクランブル部１４３、第１の復号部１４２、第２の復号部１４４、鍵選択部１４６、検証部１４７、視聴判定部１４５、視聴制御部１４９から構成される。

【００４８】

分離部１４１は、受信した多重化情報を分離する。そして、分離した番組のスクランブルされた情報はデスクランブル部１４３へ出力し、暗号化スクランブル鍵は第１の復号部１４１へ出力し、暗号化情報は第２の復号部１４４へ出力する。

【００４９】

鍵選択部１４６は、基本構成の鍵選択部と同様であり、保持している複数の鍵から処理に用いる鍵を選択する。第２の復号部１４４は、鍵選択部１４６から出力される鍵を用いて、暗号化情報を復号する。 また、保持している複数の鍵の選択方法を変更することにより、サーバ型放送に特化した受信者限定放送方式も可能になる。つまり、保持している複数の鍵の集合から、選択していた鍵をあるタイミングから選択しないことによって鍵の消去と同等の扱いを実現することや、選択していなかった鍵をあるタイミングから選択することによる新規鍵配送と同等の扱いを実現すること等の鍵選択方法を利用することにより、サーバ型放送に特化した受信者限定放送方式が可能になる。

【００５０】

検証部１４７は、基本構成の検証部と同様であり、メタ情報と復号に用いた鍵と鍵信頼度リスト１４８から、信頼度情報を出力する。第１の復号部１４２は、第２の復号部１４４から入力されるワーク鍵 Kw を用いて、暗号化スクランブル鍵を復号する。

【００５１】

視聴判定部１４５は、第２の復号部１４４から入力される契約情報に応じて、第１の復号部１４２から入力されるスクランブル鍵の出力を制御する。デスクランブル部１４０は、視聴判定部１４５から入力されるスクランブル鍵を用いて、分離部１４１から入力されるスクランブルされた番組情報をデスクランブルする。

【００５２】

視聴制御部１４９は、メタ情報とメタ情報に関する信頼度情報を入力し、視聴を制御する。一般的には、信頼度の高いメタ情報は大きく番組情報の見え方を変える視聴を可能にし、信頼度の低いメタ情報では小さく番組情報の見え方変えるだけの視聴を可能にする。

【００５３】

例えば、図３に示すようにメタ情報の提供が、放送事業者１２０と異なるメタ情報提供業者１３０である場合は、信頼度情報は低いものとし、メタ情報による小さな番組視聴制御が可能であるとする。一方、メタ情報の提供が、放送事業者１２０と同一である場合は、信頼度情報は高いものとし、メタ情報による大きな番組視聴制御が可能であるとする。

【００５４】

前述したように、第１の実施の形態においては、メタ情報を暗号化している鍵を特定し、鍵の信頼度からメタ情報の信頼度を決定している。また、第１の実施の形態は、信頼度情報を決定するための発明に関するものである。しかし、信頼度情報を用いてどのように視聴を制御するかに関しては、何ら限定しない。また、複数のメタ情報によって、番組情報の視聴を制御しようとする場合の、作用させるメタ情報の優先順位を決定するためにも利用可能である。

【００５５】

また、第１の実施の形態においては、信頼度情報に応じて番組情報の視聴を制御していた。しかし、制御の対象は、番組情報の視聴に限るものではない。番組情報の編集を制御する場合を図９に示す。

【００５６】

図９は受信者だけを示している。図９における受信者は、複数の鍵１５０と、鍵信頼度リスト１４８を保持し、分離部１４１、デスクランブル部１４３、第１の復号部１４２、第２の復号部１４４、鍵選択部１４６、検証部１４７、視聴判定部１４５、編集制御部１７１、編集部１７０から構成される。

【００５７】

図９に示すように、編集制御部１７１は、メタ情報と信頼度情報に応じて、番組情報を編集する編集部１７０を制御することで、番組情報の編集の制御を実現する。特に、信頼度情報に応じて、編集の程度にレベルを持たせることを可能にする。

【００５８】
制御方法の例としては、信頼度の高いメタ情報を利用した編集は大きな編集を可能にし、一方、信頼度の低いメタ情報を利用した編集は小さな編集だけ可能にするという方法である。大きな編集とは、番組のストーリまでも変わってしまうような編集であり、番組を素材とし、異なる番組を生成する編集等を意味する。
【００５９】
例えば、複数のドラマから特定の俳優のシーンだけを切り出し、俳優のクリップ集を生成する編集などが相当すると思われる。また、小さな編集とは、番組のストーリ変更のない編集等、番組制作者の意図どおりの視聴を維持する編集を意味する。例えば、番組のダイジェスト生成等の編集が相当すると思われる。編集の方法は多種多様な方法が考えられ、本発明は、特定の編集に限るものではない。
【００６０】
（第２の実施の形態）
以下、本発明における第２の実施の形態を説明する。
暗号化と復号で異なる鍵を用いる公開鍵暗号方式を利用したシステムは、認証機関（ＣＡという）と、証明書と、証明書失効リスト（CRL という）を利用した公開鍵インフラストラクチャ（PKI という）のもとで利用されることが多い。
【００６１】
認証機関ＣＡによって作成された利用者の公開鍵に対する証明書と公開鍵を共に用いることにより、公開鍵の正当性を保証している。また、証明書の検証過程において、証明書失効リストCRL を参照することにより、その証明書が取り消されていないかどうかの検査を可能にしている。
【００６２】
また、図４の構造説明図に示すように、下位の 認証機関ＣＡ１は、上位のルート認証機関ＣＡに認証してもらうという仕組みにより、認証機関ＣＡを階層的に構成することも可能である。これを管理者の署名連鎖と呼ぶ。
【００６３】
また、通常行われている証明書発行サービスにおいて、証明書の発行時に本人確認の厳格さに応じた証明書のクラスを定義している場合もある。ただし、本実施の形態においては、証明書のクラスは、証明書を発行した時の本人確認の厳格さではなく、メタ情報の信頼度に対応する複数のクラスを定義する。
【００６４】
例えば、図７に示すように、「番組情報の完全な視聴制御を可能なクラス」、「番組情報の視聴制御が不許可なクラス」、「番組情報のダイジェストを再生可能なクラス」等、さまざまな視聴制御に対して、それぞれの証明書のクラスを定義する。また、証明書失効リストCRL に関しては、不正なメタ情報を配信したメタ情報提供業者を排除するために利用したり、不正なメタ情報クラスを排除したりするために利用する。
【００６５】
第２の実施の形態にかかるシステム構成例は、第１の実施の形態同様である。ただし、管理者は、認証機関ＣＡ の機能を有する。図５に第２の実施の形態の基本構成例を示す。第２の実施の形態の基本構成は、図５に示すように、メタ情報提供事業者５１０と受信者５２０とから構成される。
【００６６】
メタ情報提供事業者５１０は、公開鍵暗号方式における公開鍵と秘密鍵を生成し、管理者５３０から公開鍵に対する証明書を得て、それらを保持している。またメタ情報提供事業者５１０は、第１の鍵管理部５１２とデジタル署名部５１１とから構成される。
【００６７】
第１の鍵管理部５１２は、秘密鍵と証明書とを保持して管理する。また、必要に応じて、秘密鍵をデジタル署名部５１１に出力する。デジタル署名部５１１は、第１の鍵管理部５１２から入力される秘密鍵を用いて、メタ情報にデジタル署名を生成する。

【００６８】
受信者５２０は、管理者５３０からメタ情報提供事業者５１０等の証明書を得て、保持している。さらに、管理者５３０から得られる証明書失効リストCRL も管理する。また、受信者５２０は、デジタル署名検証部５２１と、第２の鍵管理部５２２と、検証部５２３とから構成される。
【００６９】
第２の鍵管理部５２２は、メタ情報提供事業者５１０等の証明書を得て管理する。管理方法としては、登録時にあらかじめ管理者５３０から得られる証明書を登録しておく方法や、必要に応じて管理者５３０から証明書を得る方法もある。さらに管理者５３０から得られる証明書失効リストCRL も管理する。また、必要に応じて、証明書を出力する。
【００７０】
デジタル署名検証部５２１は、第２の鍵管理部５２２から入力される証明書を用いて、メタ情報のデジタル署名を検証する。検証部５２３は、デジタル署名検証部５２１の検証結果と、検証に用いた証明書とから信頼度情報を得る。信頼度情報は、デジタル署名の正当性が検証できたときの、証明書のクラスと証明書とに対する管理者５３０の署名連鎖から信頼度情報を決定する。
【００７１】
例えば、メタ情報に対する署名が放送事業者の署名である場合であって、証明書のクラスが最上級の場合は、最上級の信頼度情報であるとし、メタ情報に対する署名が第三者であるメタ情報提供業者５１２の署名である場合であって、証明書のクラスが最下級の場合は、最下級の信頼度情報であるとする。
【００７２】
第２の実施の形態は、公開鍵インフラストラクチャPKI をベースとして、メタ情報を検証し、メタ情報のデジタル署名の検証結果と検証に用いた証明書から信頼度情報を得ている。第１の実施の形態と異なり、公開鍵インフラストラクチャPKI をベースとすることで、複数の秘密鍵を保持することなく、メタ情報の認証を可能にしている。また、証明書のレベルや証明書に対する管理者５３０の署名連鎖によって、証明書に関する上下関係や優劣を決定することを容易にしている。
【００７３】
図５の基本構成を既存の受信者限定放送に適応した場合の構成図を、図６に示す。
図６において、放送事業者６１０は、スクランブル部６１１、多重化部６１８、暗号化部６１５、第１の暗号化/署名部６１６、第１の鍵管理部６１７から構成される。スクランブル部６１０、多重化部６１８、暗号化部６１５は第１の実施の形態と同様な構成である。
【００７４】
第１の暗号化/署名部６１６は、ワーク鍵６１３と、契約情報６１４を入力し、第１の鍵管理部６１７から入力される鍵を用いて暗号化し、デジタル署名を生成する。
【００７５】
第１の鍵管理部６１７は、放送事業者６１０の秘密鍵と証明書を管理し、必要に応じて、管理者６４０から得られる証明書失効リストCRL も管理する。さらに、必要に応じて、共有する鍵を生成したり、デジタル署名処理で用いる秘密鍵を出力したりする。
【００７６】
図６において、メタ情報提供事業者６２０は、基本構成と同様で、公開鍵暗号方式における公開鍵と秘密鍵を生成し、管理者６４０から公開鍵に対する証明書を得て、それらを保持している。また、メタ情報提供事業者６２０は、第２の暗号化/署名部６２２、第２の鍵管理部６２３から構成され、メタ情報６２１にデジタル署名を生成する。
【００７７】
第２の鍵管理部６２３は、秘密鍵と証明書を保持し、管理する。また必要に応じて、秘密鍵を第２の暗号化/署名部６２２に出力する。第２の暗号化/署名部６２２は、第２の鍵管理部６２３から入力される秘密鍵を用いて、メタ情報６２１にデジタル署名を生成する。

【００７８】
図６において、受信者６３０は、分離部６３１、デスクランブル部６３８、復号部６３２、視聴判定部６３６、視聴制御部６３７、復号/検証部６３３、検証部６３５、第３の鍵管理部６３４から構成される。分離部６３１、デスクランブル部６３８、復号部６３２、視聴制御部６３６の構成は前述した第１の実施の形態と同様である。
【００７９】
復号/検証部６３３は、分離部６３１やネットワーク６５０から入力される暗号化情報を入力し、第３の鍵管理部６３４から入力される鍵を用いて復号し、デジタル署名を検証する。
【００８０】
第３の鍵管理部６３４は、放送事業者６１０の証明書を保持し、管理する。また、必要に応じて、管理者６４０から新しい証明書を得たり、証明書失効リストCRLを得たりして管理する。また、必要に応じてデジタル署名の検証に必要な公開鍵を出力する。これらの証明書管理はさまざま鍵管理を実現し、さまざま鍵管理は、第１の実施例同様、サーバ型放送に特化した受信者限定放送方式を可能にする。
【００８１】
検証部６３５は、復号/検証部６３３からのメタ情報の検証結果と、復号/検証部６３３で用いた証明書のクラスや証明書に対する管理者のデジタル署名連鎖を検査し、信頼度情報とする。
【００８２】
前述したように、この第２の実施の形態は、メタ情報を検証し、メタ情報のデジタル署名の検証結果と検証に用いた証明書から信頼度情報を得ており、メタ情報と信頼度情報により番組情報の視聴を制御している。これは、信頼度の高いメタ情報によっては大きな番組視聴の変化は許可するが、信頼度の低いメタ情報によっては小さな番組視聴の変化しか許可しないといった、番組情報の視聴制御を可能にする。
【００８３】
（本発明の他の実施の形態）
なお、以上に説明した本実施形態のデジタルコンテンツ処理装置は、コンピュータのＣＰＵあるいはＭＰＵ、ＲＡＭ、ＲＯＭなどで構成されるものであり、ＲＡＭやＲＯＭに記憶されたプログラムが動作することによって実現できる。
【００８４】
したがって、コンピュータが上記機能を果たすように動作させるプログラムを、例えばＣＤ－ＲＯＭのような記録媒体に記録し、コンピュータに読み込ませることによって実現できるものである。上記プログラムを記録する記録媒体としては、ＣＤ－ＲＯＭ以外に、フレキシブルディスク、ハードディスク、磁気テープ、光磁気ディスク、不揮発性メモリカード等を用いることができる。
【００８５】
また、コンピュータが供給されたプログラムを実行することにより上述の実施形態の機能が実現されるだけでなく、そのプログラムがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部がコンピュータの機能拡張ボードや機能拡張ユニットにより行われて上述の実施形態の機能が実現される場合も、かかるプログラムは本発明の実施形態に含まれる。
【００８６】
また、本発明をネットワーク環境で利用するべく、全部あるいは一部のプログラムが他のコンピュータで実行されるようになっていても良い。例えば、画面入力処理は、遠隔端末コンピュータで行われ、各種判断、ログ記録等は他のセンターコンピュータ等で行われるようにしても良い。
【００８７】
【発明の効果】

以上説明してきたように、本発明によれば、異なる送信元から送信される前記デジタルコンテンツと前記メタ情報とを受信するとともに、前記受信したメタ情報に関連する情報を用いて、前記デジタルコンテンツの再生又は編集のレベルを決定するようにしたので、信頼度の高いメタ情報を利用した編集は大きな編集を可能にし、一方、信頼度の低いメタ情報を利用した編集は小さな編集だけ可能にする等のように、編集の程度にレベルを持たせることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における概要を示した構成図である。

【図２】本発明の第１の実施の形態における基本構成を示した構成図である。

【図３】本発明の第１の実施の形態における放送システムにおける構成図である。

【図４】本発明の認証機関の構造を示した構成図である。

【図５】本発明の第２の実施の形態における基本構成を示した構成図である。

【図６】本発明の第２の実施の形態における放送システムにおける構成図である。

【図７】メタ情報の信頼度に対応するクラス情報の一例を示す図である。

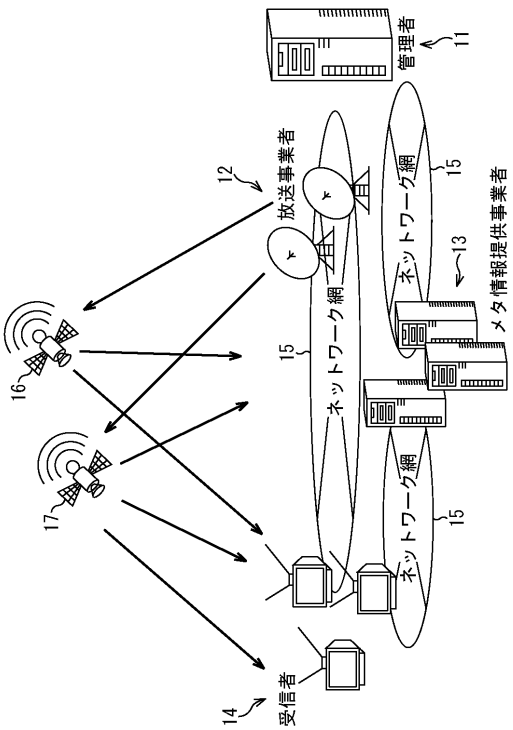
【図８】従来の受信者限定方法を実現するシステムの構成例を示すブロック図である。

【図９】信頼度情報に応じて番組情報の編集を制御する放送システムにおける構成図である。

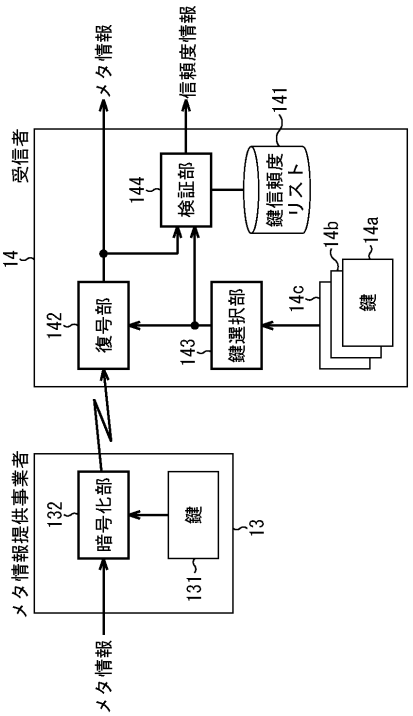
【符号の説明】

１１　管理者
１２　放送事業者
１３　メタ情報提供業者
１４　受信者
１５　ネットワーク
１６、１７　通信衛星
１３１　鍵
１３２　暗号化部
１４１　鍵信頼度リスト
１４２　復号部
１４３　鍵選択部
１４４　検証部

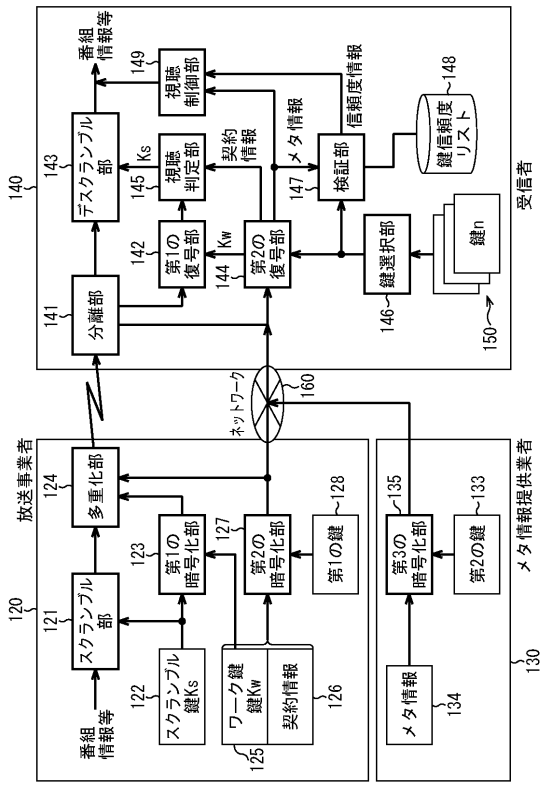
【図１】


管理者
11
放送事業者
12
ネットワーク網
15
ネットワーク網
15
メタ情報提供事業者
13
ネットワーク網
15
16
17
受信者
14

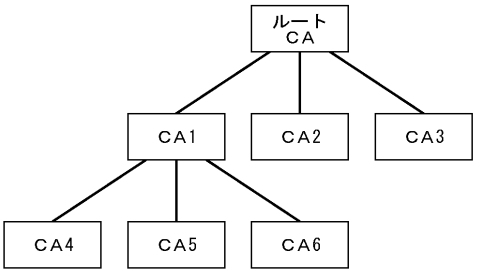
【図２】


メタ情報
信頼度情報
受信者
14
141
144
検証部
鍵信頼度リスト
142
復号部
143
鍵選択部
14c
14b
鍵
14a
メタ情報提供事業者
132
暗号化部
鍵
131
13
メタ情報

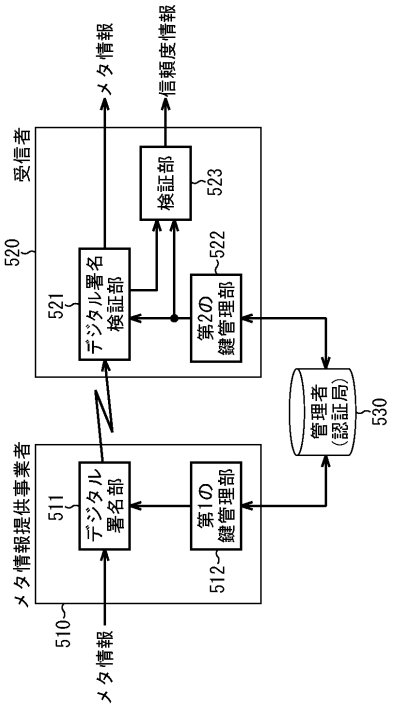
【図３】


番組情報等
140
143
デスクランブル部
149
視聴制御部
Ks
145
視聴判定部
契約情報
メタ情報
147
検証部
信頼度情報
148
鍵信頼度リスト
142
第1の復号部
Kw
144
第2の復号部
146
鍵選択部
鍵n
150
141
分離部
受信者
160
ネットワーク
放送事業者
120
121
スクランブル部
124
多重化部
123
第1の暗号化部
127
第2の暗号化部
128
第1の鍵
122
スクランブル鍵Ks
ワーク鍵Kw
契約情報
125
126
番組情報等
メタ情報提供業者
130
135
第3の暗号化部
133
第2の鍵
メタ情報
134

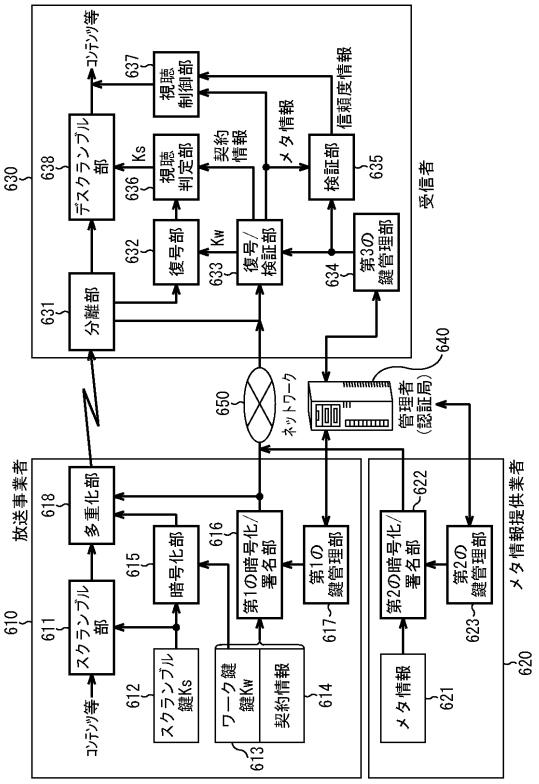
【図４】


ルートCA
CA1
CA2
CA3
CA4
CA5
CA6

【図５】



【図６】

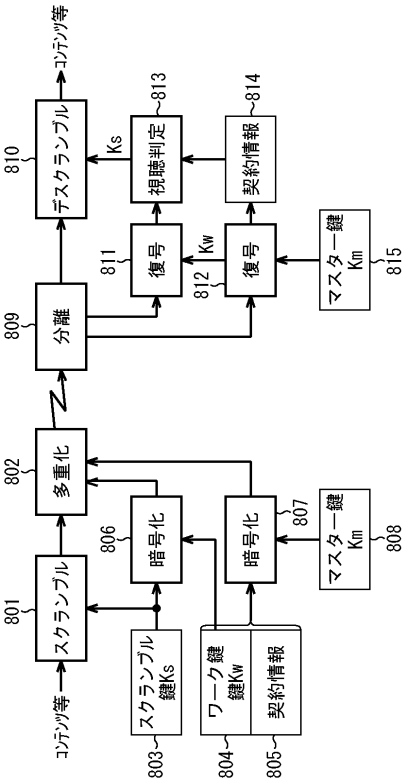


【図７】

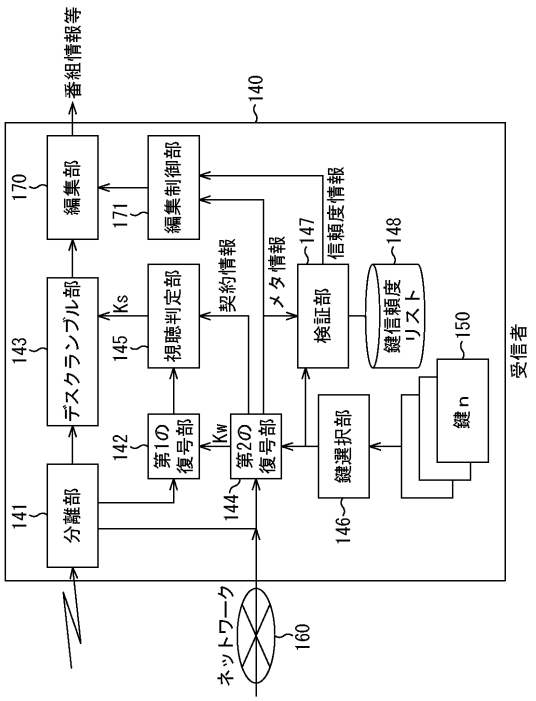
クラス情報

- ☑ 番組情報の完全な視聴制御を可能なクラス
- ☐ 番組情報の視聴制御が不許可のクラス
- ☐ 番組情報のダイジェストを再生可能なクラス

【図８】



【図９】


番組情報等
140
170
編集部
171
編集制御部
143
デスクランブル部
Ks
145
視聴判定部
契約情報
メタ情報
147
信頼度情報
148
検証部
鍵信頼度リスト
150
鍵ｎ
142
第1の復号部
Kw
第2の復号部
144
鍵選択部
146
141
分離部
ネットワーク
160
受信者

フロントページの続き

(51)Int.Cl.			FI		
H04N	***7/081***	***(2006.01)***	H04L	9/00	675B
H04L	***9/32***	***(2006.01)***	H04N	7/16	Z
H04N	***7/16***	***(2006.01)***	H04L	9/00	601B
H04L	***9/08***	***(2006.01)***			

(56)参考文献 特開平１１－３１２０８１（ＪＰ，Ａ）
特開２００１－０９２８２７（ＪＰ，Ａ）
特開２００１－３５０６７７（ＪＰ，Ａ）
特表２００３－５２０００８（ＪＰ，Ａ）
特開２００３－０１８５１８（ＪＰ，Ａ）
国際公開第０１／０５２１７８（WO，Ａ１）
特開２００３－２４８７３７（ＪＰ，Ａ）
片岡充照 他，情報放送の受信機アーキテクチャ，１９９８年映像情報メディア学会年次大会講演予稿集，１９９８年 7月２９日，ｐ．９０－９１
西本友成 他，サーバー型放送で利用するメタデータのデジタル署名方式，第３回情報科学技術フォーラム（ＦＩＴ２００４） 一般講演論文集 第２分冊，２００４年 8月２０日，ｐ．８７－８８
誰もが配れるメタデータへ 機器メーカが橋渡し，日経エレクトロニクス，２００４年 6月２１日，第８７６号，ｐ．１２４－１２９

(58)調査した分野(Int.Cl.，ＤＢ名)

H04H 60/73
H04H 60/16
H04H 60/20
H04H 60/23
H04L 9/08
H04L 9/32
H04N 7/08
H04N 7/081
H04N 7/16