(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-503367
(P2006-503367A)
(43)公表日　平成18年1月26日(2006.1.26)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/24	(2006.01)	G06F 12/14	560C	5B017

審査請求 未請求　予備審査請求 未請求　（全 25 頁）

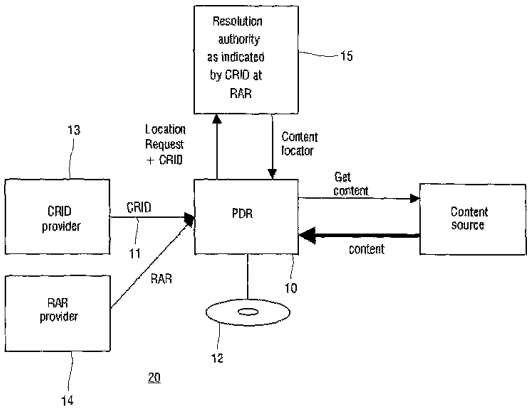
(21)出願番号　特願2004-544615 (P2004-544615)
(86)(22)出願日　平成15年10月17日 (2003.10.17)
(85)翻訳文提出日　平成17年2月15日 (2005.2.15)
(86)国際出願番号　PCT/IB2003/004608
(87)国際公開番号　WO2004/036870
(87)国際公開日　平成16年4月29日 (2004.4.29)
(31)優先権主張番号　02257275.4
(32)優先日　平成14年10月18日 (2002.10.18)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦

最終頁に続く

(54)【発明の名称】ＴＶ－Ａｎｙｔｉｍｅにおけるメタデータ保護に対する方法、システム、装置、信号及びコンピュータプログラム

(57)【要約】
本発明は、TV-Anytimeメタデータの保全性を保護する方法、システム、装置、並びに信号、及びこれに応じてこのような保護された情報を運ぶ信号に関する。保護は、署名及び保証者アプローチを適用することにより得られる。オプションとして、カノリゼーション又は変換機能の追加ステップが使用される。データフラグメントは、一意的な識別子でラベル付けされることができ、したがって幾つかの異なる機関により参照され、個々に又はセットとして別々に署名されることができる。



【特許請求の範囲】
【請求項１】
データ保全性認証及びデータ保護を提供する方法であって、データフラグメントのセットが署名により保護される方法において、
前記セットの各データフラグメントが、独自の一意的な識別子を有し、
前記署名が、前記セットの前記データフラグメントのそれぞれ一意的な識別子に対するリファレンスを有する、
ことを特徴とする方法。
【請求項２】
前記セットが複数の署名により保護され、前記複数の署名が異なるソースから生じることができる、請求項１に記載の方法。
【請求項３】
各データフラグメントに対してハッシュが生成され、前記セットの前記データフラグメントの前記ハッシュが、前記署名を計算するのに使用される、請求項１に記載の方法。
【請求項４】
前記データフラグメントがＸＭＬで表される、請求項１に記載の方法。
【請求項５】
前記データフラグメントが、TV-Anytimeメタデータを構成する、請求項１に記載の方法。
【請求項６】
前記署名が、xmldsig規格に従って記憶される、請求項１に記載の方法。
【請求項７】
前記データフラグメントのセットが、データフラグメントのスーパーセット上の変換機能により定められる、請求項１に記載の方法。
【請求項８】
前記署名を生成する前にカノリゼーション機能が使用される、請求項１に記載の方法。
【請求項９】
前記リファレンスが前記署名により保護される、請求項１に記載の方法。
【請求項１０】
少なくとも１つの署名牽引ファイルが追加される、請求項１に記載の方法。
【請求項１１】
特定のデータフラグメントにおける前記一意的な識別子が、前記特定のデータフラグメントを生成した組織の一意的な識別で開始する、請求項１に記載の方法。
【請求項１２】
前記一意的な識別が、前記組織のＤＮＳ名である、請求項１１に記載の方法。
【請求項１３】
前記リファレンスは、前記リファレンスが参照する前記データフラグメントのロケーションを示すロケーションインジケータを添付される、請求項１に記載の方法。
【請求項１４】
前記ロケーションインジケータが、参照される前記データフラグメントまでのデータ中の経路を示す、請求項１３に記載の方法。
【請求項１５】
前記署名がＸＭＬ文書に含まれる、請求項４に記載の方法。
【請求項１６】
前記署名が、元のＸＭＬデータ文書を含むラッパＸＭＬ文書内に与えられる、請求項４に記載の方法。
【請求項１７】
前記署名が、元のＸＭＬデータ文書を参照して、別のＸＭＬ文書内に与えられる、請求項４に記載の方法。
【請求項１８】

データ保全性認証及びデータ保護を提供するシステムであって、
データフラグメントを受信及び処理するように構成され、前記データフラグメントのセットが署名により保護されることができるシステムにおいて、
前記システムが、前記セットのデータフラグメントを受信及び処理する手段を有し、各データフラグメントが一意的な識別子により識別され、
前記システムが更に、
前記一意的な識別子を使用して前記セットの保護されたデータフラグメントに署名を関連付ける手段と、
前記保護されたデータフラグメントの前記一意的な識別子を使用して前記セットに関連付けられた署名を確認する手段と、
前記一意的な識別子により前記保護されたデータフラグメントを参照する署名を生成する手段と、
の少なくとも１つを有する、
ことを特徴とするシステム。
【請求項１９】
データ保全性認証及びデータ保護を提供する署名装置であって、
前記装置がデータフラグメントを処理するように構成され、
前記装置がデータフラグメントのセットを保護するために署名を生成するように構成される署名装置において、
前記装置が、前記データフラグメントに含まれる一意的な識別子により保護されるべき各データフラグメントをアドレスするように構成され、
前記装置が、前記セットの前記データフラグメントを参照する前記一意的な識別子を有する署名情報を生成するように構成される、
ことを特徴とする署名装置。
【請求項２０】
データ保全性認証及びデータ保護を確認する確認装置であって、
前記装置がデータフラグメントを処理するように構成され、
前記装置がデータフラグメントのセットを保護するために署名を確認するように構成される装置において、
前記装置が、前記データフラグメントに含まれる一意的な識別子により保護されるべき各データフラグメントをアドレスするように構成され、
前記装置が、前記セットの前記データフラグメントを参照する前記一意的な識別子を有する署名情報を確認するように構成される、
ことを特徴とする確認装置。
【請求項２１】
データフラグメントを有する信号であって、前記データフラグメントのセットが署名により保護される信号において、
前記セットの各データフラグメントが、独自の一意的な識別子を有し、
前記署名が、前記セットの前記データフラグメントの前記一意的な識別子に対するリファレンスを有する、
ことを特徴とする信号。
【請求項２２】
請求項１に記載の方法を実施するコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ保全性認証（data integrity authentication）及びデータ保護を提供する方法であって、データフラグメントのセットが署名により保護される方法に関する。
【０００２】

本発明は、更に、データ保全性認証及びデータ保護を提供するシステムであって、前記装置がデータフラグメントを受信及び処理するように構成され、データフラグメントのセットが署名により保護されるシステムに関する。

【０００３】

本発明は、更に、データ保全性認証及びデータ保護を提供する署名装置であって、データフラグメントを処理するように構成され、データフラグメントのセットを保護する署名を生成するように構成される署名装置に関する。

【０００４】

本発明は、更に、データ保全性認証及びデータ保護を確認する確認装置であって、データフラグメントを処理するように構成され、データフラグメントのセットを保護する署名を生成するように構成される確認装置に関する。

【０００５】

本発明は、更に、データフラグメントを有する信号であって、データフラグメントのセットが署名により保護される信号に関する。

【０００６】

本発明は、更に、このような方法を実施するコンピュータプログラムに関する。

【背景技術】

【０００７】

テレビ視聴者が利用することができるチャネル数が増加したので、このようなチャネルにおいて利用することができる番組コンテンツの多様化にしたがって、テレビ視聴者が関心のあるテレビ番組を識別することは、ますます挑戦的になっている。歴史的に、テレビ視聴者は、印刷されたテレビ番組ガイドを検討することにより関心のあるテレビ番組を識別する。テレビ番組の数が増加したので、このような印刷されたガイドを使用して所望のテレビ番組を効果的に識別することは、ますます難しくなっている。

【０００８】

最近になって、テレビ番組ガイドは、しばしば電子番組ガイド（ＥＰＧ）と称される電子形式で利用することができるようになった。印刷されたテレビ番組ガイドと同様に、ＥＰＧは、利用することができるコンテンツの概観を示し、ユーザによりブラウズされることができる。一般的な用語コンテンツは、典型的には、音楽、歌、映画、テレビ番組、及びピクチャ等のようなものを有するが、個々のシーン及びＭＰＥＧ－４オブジェクト等をも参照することができる。

【０００９】

ＥＰＧは、個々のコンテンツアイテムに添付するメタデータから概観を編集する。コンテンツアイテムに対するメタデータは、様々なソースから利用することができる。メタデータは、（例えばＭＰＥＧ－２テーブルのように）放送ストリームに含まれるか、又は外部データベースからダウンロードされることができる。例えば、テレビ受信器又はパーソナルデジタルレコーダは、インターネット接続を備えることができ、これは、この装置がワールドワイドウェブ上で利用することができるようにされたメタデータにアクセスすることを可能にする。

【００１０】

このメタデータは、一般に、タイトル、アーティスト、及びジャンル等のような情報を有し、時にはコンテンツ参照識別子とも称される、一意的なコンテンツ参照識別子（ＣＲＩＤ）を含むこともできる。このＣＲＩＤを使用して、各個々のコンテンツアイテムは、一意的に識別されることができる。更に、ＣＲＩＤを使用して、更に他の情報がデータベースから取り出されることができる。例えば、ユーザは、放送の時刻及び場所が依然としてわからないにもかかわらず、ＥＰＧから見たいコンテンツアイテムを選択することができる。ＣＲＩＤを使用して、前記システムは、この場合、前記コンテンツアイテムの放送の時刻及び場所を、この情報が利用することができるようになる場合に取り出すことができる。

【００１１】

ＣＲＩＤは、コンテンツの放送の送信に限定されない。これは、インターネット上のロケーション又は他のソースを参照することもできる。コンテンツ解決（content resolution）の目的は、コンテンツの特定のアイテムの特定のインスタンス（instance）の取得を可能にすることである。例えば、ユーザは、テレビの連続番組の一回分（episode）を記録したいかもしれないが、前記ユーザは、いつ何処でこの一回分が利用することができるようになるかを知る必要はない。前記ユーザは、この場合、パーソナルデジタルレコーダ（ＰＤＲ）又は同様な装置を使用して、前記ＣＲＩＤを用いて前記一回分又は連続番組に対するリファレンスを入力することができる。ＣＲＩＤが連続番組全体又は前記連続番組の個々の一回分を参照することができることに注意すべきである。

【００１２】

コンテンツアイテムに対するＣＲＩＤを受信すると、前記ＰＤＲは、前記コンテンツアイテムのロケーションを得ようと試みる。この情報は、ロケータと称され、前記コンテンツアイテムが放送される日付、時刻及びチャネルを含む。しかしながら前記ユーザは、これを知る必要はない。一度前記ＰＤＲが前記コンテンツアイテムのロケータを得ると、前記ＰＤＲは、指定された日付及び時刻を待ち、前記一回分が指定されたチャネルで放送されるのを記録する。もちろん、前記ロケータがインターネット等のロケーションを示す場合には、前記ＰＤＲは、単純に、利用することができるようになるとすぐに示されたロケーションから前記コンテンツを取り出すことができる。

【００１３】

TV-Anytime標準化機関は、標準化されたコンテンツ参照ＩＤを提供する。TV-Anytime Forum, www.tv-anytime.org, 仕様書シリーズ（Specification Series）：S-4, コンテンツ参照（Content Referencing） (標準(Normative))について, 文書 SP004V11, 2001年4月14日, より後のバージョンSP004V12, 2002年6月28日, ETSI TS 102 822-4を参照する。この文書は、ＣＲＩＤが、前記ＣＲＩＤを作った機関を示す＜オーソリティ（authority）＞フィールドを含むことを明記している。オーソリティは、前記ＣＲＩＤがロケータ又は他のＣＲＩＤに分解される能力をも提供する。ロケータは、コンテンツの時刻及び空間のロケーションに対する名称である。前記ＣＲＩＤは、更に、“RFC2396, Uniform Resource Identifiers (URI): Generic Syntax”において与えられたように、統一資源識別子（ＵＲＩ）の定義に準拠したフリーフォーマットストリングである＜データ＞フィールドを含む。このストリングは、前記＜オーソリティ＞フィールドにより与えられたオーソリティに対して意味があるべきである。

【００１４】

前記ＣＲＩＤは、ＣＲＩＤを他の（複数の）ＣＲＩＤ又はロケータに変換するプロセスとして定義されることができるロケーション解決（location resolution）に対して使用される。例えば、テレビの連続番組全体に対するＣＲＩＤは、この連続番組の個々の一回分に対するＣＲＩＤの系列に変換されることができる。ロケーション解決は、記録装置（典型的にはパーソナルデジタルレコーダ、即ちＰＤＲ）において、又は遠く離れて行われることができる。解決プロバイダ（resolution provider）は、ロケーション解決を行う。解決プロバイダは、識別及び位置決定されるべき解決オーソリティレコード（ＲＡＲ, resolving authority records）を使用する。ＲＡＲは、ＣＲＩＤを作成する機関に対応する、少なくとも１つの＜オーソリティ＞フィールドを含む。

【００１５】

ＲＡＲは、ＵＲＬ及び解決プロバイダ名をも含む。前記ＵＲＬは、解決情報が見つけられることができるロケーションを示す。前記解決プロバイダ名は、ロケーション解決を提供する機関の名称を含む。これらのＲＡＲは、ＰＤＲに対して利用することができるようにされる。

【００１６】

TV-Anytime情報及びサービスは貴重であり、したがってこの情報の保護は重要である。保護は、ソース認証及びなりすまし（spoofing）の問題を含み、データの保全性は保護されるべきである。ＴＶＡデータがソースから受信される場合に、受信器は、前記データが

実際に予期されたソースから来て、第三者により変更されていないか確認することを必要とするかもしれない。

【００１７】

第三者がこれを試みる動機がある。第三者が前記メタデータ又はＣＲＩＤテーブルを変更することができる場合、前記ＰＤＲが、コマーシャル、予告編又はただ他のコンテンツを含む、意図されたものとは別の情報を記録させられることを可能にする。これは、ユーザにとって非常に迷惑であり、前記ユーザが前記システムに対して持っている信頼を低下する可能性がある。したがって前記ＰＤＲは、前記コンテンツが信頼されたソースから来たのかどうかを確認する必要があるかもしれない。前記データが異なるチャネルを使用して配信される場合でさえも、これが１つのソースから生じたと認証されることができるならば、前記ＰＤＲは、同じコンテンツの複数のソースに直面した場合に、これを使用して選択を行うことができる。これの一例は、特定のＢＢＣショーのデータがＢＢＣにより生成されたものとして認証されることができる場合であり、これは、この情報が正しい可能性を高める。

【００１８】

前記メタデータ及びTV-Anytimeデータのソースは、常に前記データの作成者であるわけではない。前記ソースは、異なるソースから情報を集め、グループ化するサービスプロバイダであることができる。誰が前記データを作成したか、及び前記データが変更されているかどうかを確認することは、有用である可能性がある。この場合、受信されたデータは、異なるソースにより提供された部分を保持することになる。

【００１９】

データ保全性の保護に対する標準的な暗号によるアプローチは、暗号技術を使用して前記データに署名することである。全てのＴＶＡメタデータがＸＭＬで表されるので、署名が同じデータ構造で扱われることを可能にする、署名を表すトランスポート・ニュートラル様式は、ＴＶＡスキーマに前記署名を含むことであり、明白な選択肢は、xmldsig（“RFC3275, (Extensible Markup Language) XML-Signature Syntax and Processing”）である。しかしながら、この規格は、ＸＭＬ構文木の全ノードに対するXPath表示の評価を定めるためにXPathデータモデル（“XML Path Language (XPath) Version 1.0, Ｗ３Ｃ勧告(recommendation), J. Clar, S. DeRose, 1999年10月, http://www.w3.org/TR/1999/REC-xpath-19991116”）を使用し、これは、効率的に実施するのが難しい可能性がある変換である。

【００２０】

この問題を克服する試みは、効率的な文書のサブセット化の開発を容易化するＸＭＬ署名変換を定義している“XML-signature XPath Filter”(Ｗ３Ｃ勧告, 最新改訂2002年11月8日, http://www.w3.org/TR/xmldsig-filter)に記載されている。しかしながら、この勧告は、Ｗ３Ｃコンソーシアムにより採用されていない。

【００２１】

この議論から、サービスプロバイダおよびボックス製造者がメタデータに対する効率的な保全性確認機構を使用する動機が存在することは明らかである。

【発明の開示】

【発明が解決しようとする課題】

【００２２】

本発明の目的は、異なるソースから生じるデータフラグメントの保護を可能にし、複数の認証者によるデータフラグメントの保護を可能にする、効率的にデータフラグメントを保護するメタデータ保全性及びソース認証を提供することである。これは、データが、（解決）プロバイダとクライアントとの間のトランスポート中に変更されていないかどうかの確認を可能にする。これは、更に、前記データが、前記データの後の記憶及び処理の間に変更されていないかどうかの確認を可能にする。

【課題を解決するための手段】

【００２３】

本発明の目的は、セットの各データフラグメントが、独自の一意的な識別子を有し、署名が、前記セットの前記データフラグメントのそれぞれ一意的な識別子に対するリファレンスを有することを特徴とする本発明による方法により達成される。本発明は、署名が別々に提供され、一意的な識別子に対するリファレンスが、何れのデータフラグメントが前記署名によりカバーされるかを示すシステムを記載する。少なくとも１つの前記識別子は、データフラグメントと前記署名との間のリンクを可能にするために、データフラグメントを一意的に識別する。これは、データフラグメントの識別のために各データフラグメントに追加される（オプション）フィールドを提供することにより行われる。全てのデータフラグメントが各データフラグメントを一意的に識別するこのようなフィールドを持つ場合には、既存のフィールドが使用されることができる。さもなければ、特別な署名識別子が、オプションフィールドとして各データフラグメントに追加されることができる。このフィールドが存在する場合、これは、前記データ内のデータフラグメントインスタンスの一意的な識別である。１つの署名は、個々のデータフラグメントではなく、データフラグメントのセットが署名されるように、複数のデータフラグメントを参照することができる。これは、より効率的であるという更なる利点を持つ。

【００２４】

本発明による前記方法の実施例は、請求項２に記載される。配信中に、データの所有者が変わる場合、１より多い団体が、同じデータフラグメントに署名を加える可能性がある。これらの署名は、データフラグメントの異なるサブセット、即ち、完全に分離したサブセット、部分的に重なるサブセット、又は等しいサブセットに加えられることができる。

【００２５】

本発明による前記方法の実施例は、請求項３に記載される。利点は、署名を計算又は確認するためにハッシュ関数のみが必要とされることである。これは、同じデータフラグメントが複数の署名において使用されている場合に、特に有利である（計算時間の減少）。

【００２６】

本発明による前記方法の実施例は、請求項４に記載される。ＸＭＬは、個々のデータフラグメントを明らかに分離し、標準化された様式でデータフラグメントの識別を可能にする。データフラグメントは、１つ又は複数のＸＭＬ文書に集められることができる。

【００２７】

本発明による前記方法の実施例は、請求項５に記載される。前に記載されたように、TV-Anytimeメタデータは、メタデータの許可されない操作からの保護を必要とする。したがって本発明は、有利には、TV-Anytime環境に適用されることができる。

【００２８】

本発明による前記方法の実施例は、請求項６に記載される。ＸＭＬで表されるデータの適切な選択肢は、署名のxmldsig定義を使用することであり、一意的な識別子に対するリファレンスが追加される。

【００２９】

本発明による前記方法の実施例は、請求項７に記載される。署名されるべきデータフラグメントは、この署名に対するものと見なされないデータフラグメントを除去する（RFC3275による）変換機能の使用によりアプローチされることができる。前記変換機能は、前記一意的な識別子を使用して前記データフラグメントを参照する。

【００３０】

本発明による前記方法の実施例は、請求項８に記載される。前述のxmldsig仕様書においても説明されるように、同じテキストが、異なる符号化を使用して複数の様式で符号化されることができる。前記署名を計算するために、前記文書の１つの定められた表現が定められなければならない。このプロセスは、カノリゼーション（cannolization）と称される。カノリゼーション機能が使用される指示は、前記データを初めに抽出する必要無しに前記署名の値の計算を可能にする。

【００３１】

本発明による前記方法の実施例は、請求項９に記載される。前記リファレンスの保全性

を保護するために、前記リファレンス自体が、暗示的又は明示的の何れかで、署名されるべきデータに含まれることができる。

【００３２】

本発明による前記方法の実施例は、請求項１０に記載される。より念入りな検索オプションが、署名牽引ファイルを追加することにより提供されることができる。

【００３３】

このような牽引ファイルは、この場合、前記一意的な識別子を使用してリファレンスを適切な署名ファイルにリンクし、検索オプションをサポートする。このテーブルは、署名されたデータと署名のリストとの間でグループ化を提供する。

【００３４】

本発明による前記方法の実施例は、請求項１１に記載される。前記識別子が、このデータのインスタンス内の同じ型のデータフラグメントの中で一意的であることを保証するために、前記データフラグメントの生成に関与する組織の一意的な識別を用いて前記一意的な識別子を開始することが提案される。これは、前記クライアントが、何れの組織が前記データを発行したかを検出することをも可能にする。

【００３５】

本発明による前記方法の実施例は、請求項１２に記載される。ＤＮＳ名は、前記組織の一意的な識別に対する容易且つ理解することができる選択肢である。

【００３６】

本発明による前記方法の実施例は、請求項１３に記載される。前記一意的な識別子は、データフラグメントを識別するが、これは、このデータフラグメントがデータ全体の中のどこで見つけられることができるかを定めない。前記データ内の正しいデータフラグメントの検索を容易化するために、前記リファレンスは、好ましくはロケーションインジケータを添付されるべきである。

【００３７】

本発明による前記方法の実施例は、請求項１４に記載される。実施は、前記データフラグメントを位置決定するために取らなければならない前記データ中の経路を示す。

【００３８】

本発明による前記方法の実施例は、請求項１５に記載される。データ文書内に署名情報を含むことが、可能であり、効率的である。

【００３９】

本発明による前記方法の実施例は、請求項１６に記載される。異なるアプローチは、前記署名情報と、場合により署名を必要とする他の要素とを更に含むデータ文書の周りにラッパ（wrapper）を定義することである。このようにして、元のデータは、場合により欠けている一意的な識別子の追加を除いて変更無しで前記ラッパに含まれる。適切に定義されたラッパは、追加のデータが署名されたデータに含まれることを可能にするように拡張されることができる。

【００４０】

本発明による前記方法の実施例は、請求項１７に記載される。異なるアプローチは、元のデータ文書内のデータフラグメントを参照して、署名情報を有する別のデータ文書を定めることである。このようにして、前記元のデータ文書は、場合により欠けている一意的な識別子の追加を除いて変更されないままである。

【００４１】

本発明によるシステムは、前記システムが、サブセットのデータフラグメントを受信及び処理する手段を有し、各データフラグメントが一意的な識別子により識別され、前記システムが、更に、前記一意的な識別子を使用して前記セットの保護されたデータフラグメントに署名を関連付ける手段と、前記保護されたデータフラグメントの前記一意的な識別子を使用して、前記セットに関連付けられた署名を確認する手段と、前記一意的な識別子により、前記保護されたデータフラグメントを参照する署名を生成する手段との少なくとも１つを有することを特徴とする。

【００４２】
本発明による署名装置は、前記装置が、前記データフラグメントに含まれる一意的な識別子により保護されるべき各データフラグメントをアドレスするように構成され、前記装置が、前記セットの前記データフラグメントを参照する前記一意的な識別子を有する署名情報を生成するように構成されることを特徴とする。
【００４３】
本発明による確認装置は、前記装置が、前記データフラグメントに含まれる一意的な識別子により保護されるべき各データフラグメントをアドレスするように構成され、前記装置が、前記セットの前記データフラグメントを参照する前記一意的な識別子を有する署名情報を確認するように構成されることを特徴とする。
【００４４】
本発明による信号は、前記セットの各データフラグメントが、独自の一意的な識別子を有し、前記署名が、前記セットの前記データフラグメントの前記一意的な識別子に対するリファレンスを有することを特徴とする。
【００４５】
本発明は、更に、請求項１の方法を実行するコンピュータプログラムを特徴とする。
【００４６】
本発明のこれら及び他の態様は、概略的な図面を参照して、例を用いて更に記載される。
【発明を実施するための最良の形態】
【００４７】
データの収集及び処理の説明として、メタデータの処理が、TV-Anytime環境におけるパーソナルデジタルレコーダ即ちＰＤＲのような装置により記載される。図１は、コンテンツ解決のプロセスを概略的に図示する。ＰＤＲ１０は、コンテンツ参照識別子ＣＲＩＤにより識別されるコンテンツアイテムを記録するように指示されている。前記ＰＤＲにコンテンツアイテムを記録するように指示すること、又は換言すると当該コンテンツアイテムを記録するために予定に入れることは、様々な様式で行われることができる。現在、一般的な様式は、ユーザが手動で、例えばＥＰＧにおいて前記コンテンツアイテムを選択することにより、前記コンテンツアイテムが記録されるべきであることを示すことである。下で前記ＰＤＲのものとされる機能の一部又は全てが、テレビ受信器、セットトップボックス、又はパーソナルコンピュータのような１つ又は複数の他の装置に組み込まれることもできることは、容易に理解されるであろう。光学ディスク又は固体メモリのような適切なフォーマットでコンピュータ読取可能命令を有するコンピュータプログラムプロダクト１２は、本発明を実施するプログラム命令を記憶又は配信するために使用されることができる。
【００４８】
前記ＰＤＲ、又は前記ＰＤＲが接続される他の装置は、消費者が興味を持つ可能性があるコンテンツアイテムの種類を決定するために備え付けられることができる。これは、ユーザプロファイリング又はリコメンダシステムとして既知である。消費者が視聴するコンテンツアイテムの経過を追い、このようなコンテンツアイテムに対する暗示的及び／又は明示的な格付けシステムを採用することにより、様々な精度で、どの他のコンテンツアイテムに消費者が興味を持つ可能性があるかを予測することが可能になる。この場合、前記消費者が興味を持つ見込みのあるコンテンツアイテムを自動的に記録することが可能になる。このようなコンテンツアイテムは、この場合、前記ＰＤＲにより記録されることができる。ユーザプロファイリングの多くの技術は、当技術分野で既知である。前記ＰＤＲがユーザプロファイリングを使用して、特定のコンテンツアイテムが興味を持たれる可能性があることを決定する場合、前記ＰＤＲは、前記コンテンツアイテムを記録するように予定に入れる。
【００４９】
前記コンテンツアイテムに対するＣＲＩＤは、前記コンテンツアイテムの自動的な記録

を容易化するために使用される。前記ＣＲＩＤは、ユーザにより手動で入力されるか、又は電子番組ガイドを通してコンテンツアイテムを選択した結果であることができる。この第２オプションは、前記ＣＲＩＤが、ＣＲＩＤプロバイダエンティティ１３により前記ＥＰＧで使用される他のメタデータと一緒に何らかの形で前記ＰＤＲに提供される。代替的に、前記ＣＲＩＤが前記ユーザにより又は前記ＰＤＲにより知られていない場合に、前記ユーザは、例えばメタデータ・データベース内の前記コンテンツアイテムのタイトルを使用して検索を実行することができ、検索結果から所望のコンテンツアイテムを選択することができる。前記ＣＲＩＤは、この場合、検索エンジンにより前記ＰＤＲに供給される。

【００５０】

前記ＣＲＩＤを前記ＰＤＲに供給する多くの他の様式が存在する。例えば、映画の予告編又はプレビューは、何らかの様式（例えばウォーターマーク）でコマーシャルのコンテンツに埋め込まれたＣＲＩＤを用いて放送されることができる。前記ユーザは、この場合、リモートコントロール、テレビ又はＰＤＲのボタンを押すことができる。前記ＰＤＲ又はテレビは、この場合、前記コマーシャルのコンテンツから前記ＣＲＩＤを抽出する。

【００５１】

一度前記所望のコンテンツに対する前記ＣＲＩＤが知られると、前記ＰＤＲは、前記ＣＲＩＤを入力として使用して前記コンテンツアイテムのロケータ情報を得ようと試みる。このロケータ情報は、必ずしも常に利用することができるわけではない。例えば、前記ＣＲＩＤは、ごく最近になって映画館で公開された映画を参照することができる。この映画は、近い未来にテレビで放送される見込みは低く、したがってこれはＥＰＧ情報を使用して予定に入れられることができない。このような場合、前記ロケータは後で（例えば、前記映画がテレビで放送される１年後に）利用することができるようになる可能性があるので、前記ＰＤＲは、前記ロケータを得ようと定期的に試みるべきである。前記ＣＲＩＤは、テレビの連続番組をも参照することができ、前記ＣＲＩＤは、この場合、この連続番組の複数の個々の一回分に対するＣＲＩＤに分解される。ロケータ情報が幾つかの一回分に対して利用することができないことも起こり得る。ここで前記ＰＤＲは、これらの一回分に対する前記ロケータを得ようと定期的に再試行するべきである。

【００５２】

ＣＲＩＤをロケータ情報に変換するプロセスは、TV-Anytimeにおいてロケーション解決として既知である。ロケーション解決は、ロケーション独立なコンテンツリファレンス（前記ＣＲＩＤ）を時間（例えば放送システムにおける予定された送信時間）及び空間（例えばテレビのチャネル、ＩＰアドレス）におけるロケーションにマッピングするステップを伴う。上で説明されたように、時間及び空間におけるこれらのロケーションは、“ロケータ”と称される。ロケーション解決のプロセスは、前記ＰＤＲの中で、又はインターネット上のサーバのような物理的に離れたサーバを使用して起こることができる。

【００５３】

前記ＰＤＲに対して、前記ＣＲＩＤは、基本的に外部の補助無しでロケーションに変換することができない曖昧な情報（opaque information）を含む。ＣＲＩＤにロケータ情報を提供する解決プロバイダ（ＲＰ）は、この問題を解決するために提供される。通常は、複数のＲＰが利用されることができ、前記ＰＤＲは、特定のＣＲＩＤに対して何れのＲＰを使用するか知らなければならない。しばしばこれは、前記ＣＲＩＤを作成したのと同じ機関である。オーソリティの名称は、上で説明されたように前記＜オーソリティ＞フィールド内の前記ＣＲＩＤに存在する。この名称は、登録されたインターネットドメイン名の形式で存在する。解決オーソリティ（ＲＡ、Resolution Authority）１５が、TV-Anytime仕様書SP004に記されたドメイン名解決プロセス（domain name resolution process）を使用してインターネット上で見つけられることが可能である。

【００５４】

各ＲＡは、ロケーション解決が行われるために、１つ又は複数の解決オーソリティレコード（ＲＡＲ）が前記ＰＤＲに存在することを必要とする。各解決オーソリティレコードは、前記ＰＤＲがこれがＲＡＲであることを知ることを可能にするある種のトランスポー

ト特有コンテナの中に配置される必要がある。同じオーソリティに対する複数のレコードが存在する場合、前記ＰＤＲは、これらのレコードの１つだけを使用することを選択するか、又は全てを順に試みることができる。前記解決オーソリティレコード（ＲＡＲ）は、コンテンツリファレンス解決情報が見つけられることができるＲＡを識別する情報を含む。

【００５５】

前記ＲＡＲを使用して、前記ＰＤＲは、特定のＣＲＩＤを分解するために何れのＲＰを使用するかを決定する。前記ＰＤＲは、この場合、ＣＲＩＤに添付されたロケーションに対する要求を当該解決プロバイダに提出する。この要求に応答して、前記解決プロバイダは、前記ロケータ情報を返す（もちろんこの情報は当該ＲＰにおいて利用することができると仮定する）。前記ＰＤＲは、この場合、コンテンツソースにアクセスし、前記コンテンツアイテムを得ることができる。コンテンツアイテムは、例えば、これが複数回放送されるか又は複数のプロバイダから利用することができる場合には、１より多いロケータを持つことができる。前記ＰＤＲは、この場合、何れのロケータを使用するか選択するか、又は前記ユーザに選択を行うよう促すことができる。

【００５６】

一度前記ロケータ情報が得られると、前記ＰＤＲは、指定された日付及び時刻を待ち、この場合、一回分が指定されたチャネルで放送される際に当該一回分を記録する。もちろん、前記ロケータがインターネット等におけるロケーションを示す場合、前記ＰＤＲは、示された前記ロケーションが利用することができるようになるとすぐに前記ロケーションからコンテンツを単純に取り出すことができる。

【００５７】

ロケータ情報が利用されることができるコンテンツアイテムは、適切な瞬間に前記ＰＤＲにより記録されることができる。このために、前記ＰＤＲは、十分に大きなハードディスクのようなローカル記憶装置、及び／又はＤＶＤ＋ＲＷライタのような装置を有することができる。コンテンツアイテムが記憶される前記記憶装置は、前記ＰＤＲに対してローカルである必要はないが、ホームネットワークを介して前記ＰＤＲに接続されたファイルサーバ又はハードディスクのような外部装置であってもよい。一度前記コンテンツアイテムが記録されると、前記コンテンツアイテムは、消去されるまでいつでも再生されることができる。

【００５８】

上のアプローチを使用して、前記コンテンツのロケーションを知る人は、解決プロバイダとして活動することができる。しかしながら、コンテンツ及びサービスプロバイダは、例えば評判を保護することができるように、認可された解決プロバイダのみが、前記コンテンツに対するコンテンツ解決を実行することを望むかもしれない。他方では、消費者及びＰＤＲにとって、ＣＲＩＤオーソリティ及び解決プロバイダを信頼／信用することができることは重要であり、これにより正しいコンテンツを得ることができる。

【００５９】

前記ＰＤＲがデジタル権利管理（ＤＲＭ）システムによって動作する場合、コンテンツアイテムは、前記コンテンツアイテムに関連付けられた権利が消去を要する場合には消去されることができる。また、いくつかのコンテンツアイテムは、前記アイテムを記録する権利を全く備えていないか、又は制限された時間若しくは制限された回数のみ視聴を可能にする権利を備えている可能性がある。前記ＰＤＲは、この場合、制限が超過された場合に前記コンテンツアイテムを消去するか、又は更なるアクセスを可能にする更なる権利が得られるまで前記コンテンツに対する更なるアクセスを拒絶するべきである。クライアントボックスにおいて受信されたコンテンツは、暗号化によりトランスポート中に保護されることができる。前記コンテンツがアクセスされることができる前に、前記コンテンツは復号されなければならない。このプロセスは、前記ＤＲＭシステム又は条件付きアクセス（ＣＡ）システムにより制御される。

【００６０】

TV-Anytime仕様書は、２つの異なる配信方法、即ち単方向の方法と双方向の方法とを区別する。単方向の状況において、TV-Anytimeデータは、適切な通常の信号送信の放送ストリームにおける他のストリームである。このストリームに対するアクセスは、スクランブリングのような従来の条件付きアクセスシステムを使用して保護されることができる。トランスポート機構に対して定められる通常の信号送信方法を使用して、前記条件付きアクセスシステムが識別され、このストリームに関する条件付きアクセス情報を運ぶメッセージが示される。ほとんどのデジタル放送システムは、ＭＰＥＧ－２トランスポート・ストリーム・フォーマット（ISO/IEC 13818-1:1996(E), Information technology - Generic coding of moving pictures and associated audio information: Systems, First Edition, 1996-04-15）を使用する。

【００６１】

双方向の場合には、クライアントとサーバとの間でポイント・ツー・ポイント接続が行われる。このプロセスは、TV-Anytime文書SP004v1.2, コンテンツ参照に関する仕様書シリーズS-4, バージョン1.2, 最終仕様書, 2002年6月28日, ETSI TS 108 822-4に記載されている。前記ＤＲＭシステムは、前記サービスプロバイダに対して安全なチャネルを開き、このチャネルを通して通信する。このようにして、認可されたTV-Anytimeクライアントのみが前記コンテンツにアクセスすることができることを保証する。

【００６２】

放送システム内の既存のＣＲＣ機構は伝送エラーに対処するが、意図的な変更を検出すること、及び情報が要求されたソースにより生成されたことを認証することは望ましいままである。

【００６３】

前記TV-Anytimeデータのソースは、常に前記データの作成者であるわけではない。前記ソースは、異なるソースから情報を集め、グループ化するサービスプロバイダであることができる。データは、異なるソースから前記ＰＤＲにより取り出されることもできる。したがって、受信されたデータは、異なるソースにより提供された部分を保持する。誰が前記データを作成したか、及び前記データが変更されたかどうかを確認することは有用であることができる。これは署名を使用して行われる。

【００６４】

全てのＴＶＡメタデータは、ＴＶＡフラグメントとして提供される。ＴＶＡにおいて、メタデータ仕様書（TV-Anytime文書WD647/SP003v1.3 Part A, メタデータに関する仕様書シリーズS-3: Part A メタデータスキーマ（Metadata Schemas）, バージョン1.3, 2002年12月15日, ETSI TS 102 822-3）によると、ＴＶＡフラグメントは、“メタデータの自己内蔵型の微小部分”である。この文書において、署名されることができる最小のＴＶＡメタデータ要素は、フラグメントであると仮定される。

【００６５】

本発明は、前記フラグメントを前記署名にリンクするためにTV-Anytimeフラグメントを一意的に識別するのに使用されるラベルの定義を含む。これは、各TV-Anytimeフラグメントに追加されるオプションフィールドを提供することにより行われる。存在する場合に、この一意的な識別子は、メタデータのこのインスタンス内のフラグメントインスタンスの一意的な識別である。前記一意的な識別子は、前記メタデータ内のフラグメントの容易なトレーシングを可能にするべきである。これは、署名を計算するのに必要とされる異なるフラグメントを見つけるために必要とされる。

【００６６】

図２は、TV-Anytimeにより定義される異なるフラグメントを示す。署名をサポートするために、全てのフラグメントは、フラグメントの識別のためにオプションの又は強制的な一意的な識別子を持つ。前記TV-Anytime仕様書内で、ＴＶＡＩＤと称されるフィールドが、これらのフラグメント内で使用される。上で識別されたメタデータ仕様書によると、ＴＶＡＩＤは、“メタデータ記述内で一意性を示す”ために使用される。ＴＶＡＩＤは、識別子に対する要件に一致するように見えるが、特定の型のＴＶＡＩＤに対してのみ一意的

である。例えば、サービスＩＤ（serviceID）及びセグメントＩＤ（segmentID）は、特定のメタデータ記述内で同じであることができる。

【００６７】

一意的な識別子の概念を実施する幾つかの変形例が可能である。

【００６８】

本発明の第１変形例において、前記ＴＶＡＩＤは、参照識別子として使用される。これは、前記署名において使用されるリファレンスが、コンテキスト（例えばサービス又はセグメント）を示す場合に、一意的な識別子を提供する。前記ＴＶＡＩＤは、全てのフラグメントが１を持つ（又は１が追加される）場合に、使用されることができ、前記ＴＶＡＩＤを使用して、前記フラグメントに対する一意的な参照が、前記ＴＶＡメタデータのこのインスタンス内で行われることが決定される。

【００６９】

第２変形例において、特別なＴＶＡ署名識別子が、オプションフィールドとして全てのフラグメントに追加される。前記ＴＶＡＩＤ又は新しい識別子の何れかが、この目的のために定められる。前記メタデータ内（又は前記メタデータの関連インスタンス内）の同じ型の他のフラグメントの中で１つのフラグメントを一意的に識別する各ＴＶＡフラグメントに追加された例示する識別子に対するＸＭＬ定義は、図３ａに示される。各フラグメント（又はフラグメントのセット）を参照することができるために、全てのTV-Anytimeフラグメントに対するフォーマットの例は、図３ｂに示されるように形式的に定義される、TVASignatureId属性を追加することであることができる。

【００７０】

本発明の他の有利な変形例は、前記フラグメントの生成に関与する組織のＤＮＳ名（又は他の一意的な識別）で前記識別子を開始することにより、前記識別子が前記メタデータ内の同じ型のフラグメントの中で一意的であることを保証する。会社MyCompanyにより発行されたフラグメントの例示するTVASignatureIdは、図３ｃに示されるように見えることができる。

【００７１】

各個々のフラグメント又はフラグメントのセットをラベル付けすること及びリファレンスを使用して署名することは、適切に選択された場合に、前記リファレンスが署名ファイルから前記フラグメントまでのリンクを提供するという利点を持つ。更に、前記一意的な識別子は、（複数の）前記フラグメントと前記署名を含むデータとの間のリンクを提供する。

【００７２】

全てのＴＶＡメタデータがＸＭＬで表されるので、前記署名が同じデータ構造で運ばれることを可能にする署名を表すトランスポート・ニュートラルな（transport neutral）様式は、ＴＶＡスキーマに前記署名を含むことであることができる。TV-AnytimeメタデータがＸＭＬで表されるので、適切な選択はxmldsigであるが、もちろん他のＸＭＬに基づく署名スキームが同様に定められることができる。

【００７３】

前記署名は、xmldsig規格に従って記憶されることができる。加えて、前記一意的な識別子に対するリファレンスは、何れのフラグメントが署名を計算するのに使用されるかを示す。前記一意的な識別子はフラグメントを識別するが、このフラグメントがTVAMain内のどこで見つけられることができるかを定めない。前記メタデータ内の正しいフラグメントの検索を容易化するために、前記リファレンス（RFC2396によるＵＲＩフォーマットで定められる）は、好ましくはロケーションをも示すべきである。したがって、本発明の拡張例は、前記フラグメントの位置を見つけるためにとられなければならない前記メタデータ中の経路を示すオプションのロケーションインジケータを追加する。

【００７４】

本発明による前記一意的な識別子を含むフラグメントＵＲＩの準拠した例示する定義は、“ tva://<path>/<TVASignatureId> ”として定義されることができ、ここで<path>は、

前記メタデータの開始から前記フラグメントに向かう経路であり、ＴＶＡＩＤは、前記フラグメントの前記識別子である。

【００７５】

幾つかの例は、“tva://TVAMain/aap.org;132423”、“tva://TVAMain/ClassiificationTable/CSAlias/publisher.com;122314”及び“tva://TVAMain/ProgramDescription/ProgramLocationTable/Schedule/metwt.org;320984”である。第１の例は、完全なTVAMainメタデータ文書に署名することも可能であることを説明する。この場合、証明書及び署名部分を除くTVAMainの全てが考慮されるべきである。

【００７６】

本実施例において、前記一意的な識別子（例えばTVASignatureId）はフラグメントを参照するためにＵＲＩにおいて使用されるので、前記識別子は、RFC2396に記載されたようにＵＲＩ上に配置されたフォーマットの制限に準拠するべきである。更に、前記ＵＲＩの構文解析（parsing）を容易化するために、スラッシュ（“/”）がTVASignatureIdにおいて使用されない。

【００７７】

TVASignatureTableは、署名されたデータと署名のリストとの間でグループ化を提供し、このようなテーブルの例示する定義は図４ａ及び図４ｂに示される。この定義において、このテーブルの中のContentReferencingTable及びResolvingAuthorityTableのような他のTV-Anytimeメタデータ文書を含むオプションが存在する。これは、これらは１回のみ生じることができるので、一意的な識別子が前記テーブル及びＵＲＬ内のメタデータに対して必要とされないという利点を持つ。

【００７８】

TVASignatureTableは、図４ｃに示されるように定義される。ゼロ又はそれ以上の署名が存在することができる。データが、依然として、又はもはやシステムにおいて利用することができない可能性があるので、TVASignatureWrapperに示されるデータに対して利用することができる全ての署名が常に含まれるわけではなく、様々な署名により保護される全てのフラグメントが常に存在するわけではない。配信システムの実施は、関連するフラグメント及び署名が必要な場合に存在することに注意しなければならない。双方向配信システムにおいて、欠けているフラグメント又は欠けている署名は、ダウンロードされることができる。

【００７９】

署名される必要があるフラグメントを定める異なる様式は、署名に対して考慮されないメタデータから幾つか又は全ての要素を除去する変換機能（RFC3275による）を定めることによるものである。

【００８０】

署名を確認するためには、前記署名を加えた団体の対応する公開鍵が必要とされる。これらの鍵の配信は幾つかの様式で行われることができる。これらの鍵は、装置内にハードコード化されることができるが、これは、新しい鍵が使用される場合、又は現在の鍵に障害が生じる場合に問題を生じるので、前記鍵の配信の最も一般的な様式は、前記鍵を、いわゆる証明書チェーン（“Applied Cryptography Second Edition: protocols, algorithms, and source code in C, Bruce Schneier, Wiley, 1996”）に組み込むことによるものである。したがって前記署名を確認するためには、署名データに加えて、署名を提供する団体の証明書も必要とされる。TVASignatureは、TVASignatureラッパ内のこのような証明書の運搬をサポートするために、１つ又は複数のds:KeyInfoオブジェクトの包含を可能にする。添付の識別子を持つKeyInfoオブジェクトのリストを示すＸＭＬ複雑型は、図５に示される。

【００８１】

署名からKeyInfoWrapperTable内のKeyInfo要素を参照することができるためには、参照ＵＲＩは、“tva://KeyInfoListTable/<Identifier>”として定められ、ここで<Identifier>は、KeyInfoWrapperTypeで示される識別子である。したがって幾つかの例は、“tva:/

/KeyInfoListTable/132423”、“tva://KeyInfoListTable/435432h”及び“tva://KeyInfoListTable/MyKeyInfo”である。

【００８２】

これは、証明書の包含及びKeyInfoオブジェクトを通信する他のオプションを可能にする。これは、いかにして署名にリンクされるかをも示す。

【００８３】

（公開）鍵は、Ｘ５０９証明書を使用して記憶されることもでき、前記５０９証明書内の対象のフィールドも、組織名又は鍵のソースを識別する異なる一意的な識別を含むことができる。これは、前記データが、これに署名したとされる組織により実際に署名されたことを確認する追加の様式を提供する。

【００８４】

署名は、ＤＳＡ又はＲＳＡ署名生成アルゴリズムのような適切なアルゴリズムを使用して生成されることができる。

【００８５】

前記xmldsig仕様書において説明されたように、テキストは多くの様式で符号化されることができる。前記署名を計算するために、文書の１つの定められた表現が、定められなければならない。このプロセスは、カノリゼーションと称される。TV-Anytime内で、ＢｉＭが、TV-Anytimeデータのバイナリ符号化に対するバイナリコーデックとして使用される。ＢｉＭ符号化が使用される場合、ＢｉＭは、カノリゼーション機能として示されるべきである。これは、前記データを初めに抽出する必要無しに署名値を計算するために、クライアントがＢｉＭ符号化ファイルを使用することを可能にする。変換及びカノリゼーション機能は、コンテンツを処理するために使用され、したがって一意的な常に同じバイトのセットが作成され、前記バイトのセットで署名が計算される。

【００８６】

前記一意的な識別に対する前記リファレンスの保全性をも保護するために、前記リファレンスは、暗示的に又は明示的に署名されるべきデータに含まれることができる。上で述べられたように且つ図５に関して、署名は、システム内で使用される異なるテーブルを保護するために使用されることもできる。

【００８７】

より念入りな検索オプションは、署名牽引ファイルを追加することにより提供されることができる。このような牽引ファイルは、この場合、一意的な識別子を適切な署名ファイルにリンクする。

【００８８】

“ISO/IEC 13818-6:1998, Information technology - Generic coding of moving pictures and associated audio information: Extensions for Digital Storage Media Command and Control, 1998”及び“ETSI TS 102 812 V1.1.1 (2001-11), Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.1, 28 June 2002”において説明されるように、デジタル署名は、前記コンテンツ上でハッシュを計算することにより、及び公開鍵暗号化を使用して前記ハッシュを署名することにより実施されることができる。

【００８９】

前記署名のロケーションに関して本発明の２つの変形例が存在する。

【００９０】

本発明の第１変形例において、（TVAMainのような）メタデータオブジェクトは、署名フラグメントを用いて拡張され、したがって前記メタデータオブジェクトは署名情報を含む。これは、前記署名が配信され、TV-Anytimeにより示されるように、通常の配信システム内でアクセスされる場合に有利である。

【００９１】

本発明の第２変形例において、署名は、例えば前記TVAMain及びことによると署名を必要とする他の要素を含むラッパの定義により、別々に提供される。これは、現在のメタデ

ータ仕様を変更せず、他のTV-Anytime文書（例えばContentReferencingTable及びResolvingAuthorityRecordTable）を含むことをも可能にするので、有利である。

【００９２】

本発明によるシステムは、単一の又は複数のフラグメントにわたり署名をサポートする。これは、フラグメントのセットに署名することを可能にするという利点を持ち、これは、各個々のフラグメントに署名するより効率的である。これは、既存のメタデータ仕様の変更のレベルを最小化しながら、可能な限り単方向及び双方向配信システムとの互換性を残すという更に他の利点を持つ。

【００９３】

上の実施例で使用された方策は個々に使用されることができるが、これらの方策は、より良い保護又は複数の脅威に対する保護を提供するために組み合わされることもできる。

【００９４】

上述の実施例が本発明を限定するのではなく説明し、当業者が添付請求項の範囲から外れることなく多くの代替実施例を設計することができることに注意すべきである。

【００９５】

請求項において、括弧間に配置された如何なる参照符号も請求項を限定するように解釈されるべきではない。単語“有する”は、請求項にリストされた要素又はステップ以外の要素又はステップの存在を除外しない。要素に先行する単語“１つの”は、複数のこのような要素の存在を除外しない。本発明は、幾つかの別個の要素を有するハードウェアを用いて、及び適切にプログラムされたコンピュータを用いて実施されることができる。

【００９６】

幾つかの手段を列挙する装置請求項において、これらの手段の幾つかは、ハードウェアの同一のアイテムにより実現されることができる。特定の方策が相互に異なる従属請求項に記載されるという単なる事実は、これらの方策の組み合わせが有利に使用されることができないことを示さない。

【００９７】

もちろん、上記の技術は、TV-Anytimeの範囲の中及び外の両方で使用されることもできる。

【図面の簡単な説明】

【００９８】

【図１】コンテンツ解決のプロセスを概略的に図示する。

【図２】TV-Anytimeにより定められる異なるフラグメントを示す。

【図３ａ】一意的な識別子に関するＸＭＬ定義及び例を示す。

【図３ｂ】一意的な識別子に関するＸＭＬ定義及び例を示す。

【図３ｃ】一意的な識別子に関するＸＭＬ定義及び例を示す。

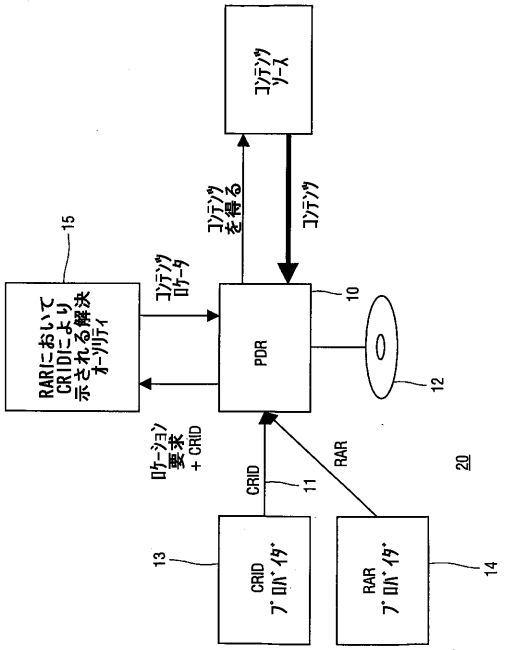
【図４ａ】署名情報に関するＸＭＬ定義及び例を示す。

【図４ｂ】署名情報に関するＸＭＬ定義及び例を示す。

【図４ｃ】署名情報に関するＸＭＬ定義及び例を示す。

【図５】鍵情報に関するＸＭＬ定義及び例を示す。

【図１】



【図２】

- TVAMain
  - ClassificationTable
    - CSAlias
    - ClassificationScheme
  - ProgramDescription
    - ProgramInformationTable
      - ProgramInformation
    - GroupInformationTable
      - GroupInformation
    - ProgramLocationTable
      - BroadcastEvent
      - Schedule
    - ServiceInformationTable
      - ServiceInformation
    - CreditsInformationTable
      - PersonName
      - OrganisationName
    - ProgramReviewTable
      - ProgramReviews
    - SegmentInformationTable
      - SegmentInformation
      - SegmentGroupInformation
    - OnDemandProgramLocation

FIG.2

【図３ａ】

```
<SimpleType name="TVASignatureIdType">
  <restriction base="string">
    <whiteSpace value="collapse"/>
  </restriction>
</simpleType>
```

名前	定義
TVASignatureIdType	各TVAフラグメントに対して、メタデータのこのインスタンス内の同じ型の他のフラグメントの中でこのフラグメントを一意的に識別するオプションの識別子を追加するために使用される単純型

FIG.3a

```
<SimpleType name="TVASignatureIdType">
  <restriction base="string">
    <whiteSpace value="collapse"/>
  </restriction>
</simpleType>
```

Name	Definition
TVASignatureIdType	A simpleType used to add an optional identifier to each TVA fragment that uniquely identifies this fragment among other fragments of the same type within this instance of metadata.

FIG.3b

```
<attribute name="TVASignatureId"
    type="TVASignatureIdType " use="optional">
```

FIG.3c

```
<TVASignatureId> "MyCompagny.com;1283bshdga7213"
</TVASignatureId>
```

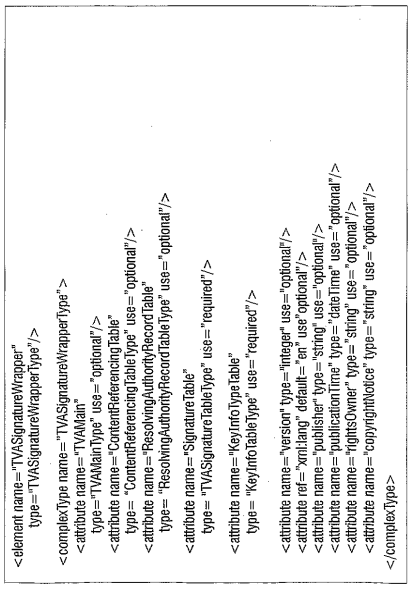


FIG.4a

【図４ｂ】

名前	定義
TVASignatureWrapper	TV-Anytimeﾃﾞｰﾀ及び付随する署名を保持する複雑型
TVAMain	SignatureList内の署名により署名されたﾌﾟﾛﾌﾞﾒﾝﾄを保持するTVAMainｲﾝｽﾀﾝｽ
ContentReferencingTable	SignatureList内の署名により署名されたContentReferencingTable
ResolvingAuthorityRecordTable	SignatureList内の署名により署名したResolvingAuthorityRecordTable
SignatureTable	ﾃﾞｰﾀ要素の署名をもつﾘｽﾄ
KeyInfoTable	KeyInfoWrapperｵﾌﾞｼﾞｪｸﾄを持つﾘｽﾄ
Version	記述のﾊﾞｰｼﾞｮﾝを指定する
xml:lang	記述の言語を指定するﾃﾞﾌｫﾙﾄは"英語"
Publisher	記述の発行者の名称を指定する
PublicationTime	ﾒﾀﾃﾞｰﾀ記述が発行された時間を指定する
RightsOwner	記述の権利を保持するｴﾝﾃｨﾃｨを指定する
CopyrightNotice	記述文書の著作権情報を指定する

【図４ｃ】

```
<complexType name="TVASignatureTableType">
  <sequence>
    <element name="Signature"
      type="ds:SignatureType" minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

名前	定義
SignatureTableType	署名のﾘｽﾄを含む複雑型
SignatureList	署名情報要素のﾘｽﾄ

【図５】

```
<complexType name="KeyInfoWrapperType">
  attribute name="Identifier" type="string" use="required"/>
  attribute name="KeyInfo" type="ds:KeyInfoType" use="required"/>
</complexType>

<complexType name="KeyInfoTableType"
  <sequence>
    <element name="KeyInfoWrapper"
      type="KeyInfoWrapperType"minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

名前	定義
KeyInfoWrapperType	このTVAMainに存在する署名を含む複雑型
Identifier	このKeyInfoｵﾌﾞｼﾞｪｸﾄの一意的な識別子
KeyInfo	鍵情報
KeyInfoListTableType	KeyInfoWrapperのﾘｽﾄ
KeyInfoWrapper	識別を持つKeyInfo

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/04608

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 946 019 A (CANAL PLUS SA) 29 September 1999 (1999-09-29) abstract; figure 7	1-3,9, 18-22
Y	column 1, line 6 - column 2, line 5 column 12, line 7 - column 14, line 48 ----- -/--	4-8, 13-17

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2004	08. 06. 2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Figiel, B

1

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/04608

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DONALD E. ,JOSEPH M. REAGLE JR.,DAVID SOLO: "XML-Signature Syntax and Processing" THE INTERNET SOCIETY & W3C, [Online] - 12 February 2002 (2002-02-12) pages 1-45, XP002270188 Retrieved from the Internet: URL:http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/> [retrieved on 2004-02-13] paragraph [01.0] paragraph [02.0] - paragraph [02.1] paragraph [3.1.1] - paragraph [3.1.2] paragraph [4.3.3.1] - paragraph [4.3.3.2] paragraph [06.5] paragraph [08.1]	4-8, 13-17
X	SEDLMEYER: "MULTIMEDIA HOME PLATFORM - STANDARD 1.0.1" FERNSEH UND KINOTECHNIK, VDE VERLAG GMBH. BERLIN, DE, vol. 55, no. 10, October 2001 (2001-10), pages 593-597,600-603, XP001101096 ISSN: 0015-0142 the whole document	1,3-6,9, 18-22
X	FR 2 797 548 A (THOMSON MULTIMEDIA SA) 16 February 2001 (2001-02-16) abstract; figures 2,3 page 2, line 1 - line 5 page 2, line 15 - page 3, line 30	1,18-22
X	WO 98/43431 A (SARFATI JEAN CLAUDE ;CANAL PLUS SA (FR); MERIC JEROME (FR)) 1 October 1998 (1998-10-01) abstract; figure 8 page 4, line 31 - page 5, line 26 page 18, line 5 - line 15 page 22, line 1 - line 24 page 24, line 14 - line 30	1,2, 18-22

1

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 03/04608

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-9,13-22

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/ IB 03/04608

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9 and 13-22

separated data is expressed in XML
---

2. claim: 10

signature index file is added
---

3. claims: 11-12

unique identifier starts with a unique identification of an organisation.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 03/04608

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0946019 A	29-09-1999	EP 0946019 A1	29-09-1999
		AU 753937 B2	31-10-2002
		AU 2851099 A	18-10-1999
		BR 9909073 A	05-12-2000
		CA 2324156 A1	30-09-1999
		CN 1301442 T	27-06-2001
		EP 1064754 A1	03-01-2001
		HR 20000598 A1	30-06-2001
		HU 0101641 A2	28-09-2001
		WO 9949614 A1	30-09-1999
		ID 27501 A	12-04-2001
		JP 2002508624 T	19-03-2002
		NO 20004765 A	24-11-2000
		PL 343076 A1	30-07-2001
		TR 200002732 T2	21-12-2000
		TR 200101213 T2	22-04-2002
		ZA 200006016 A	06-06-2001
FR 2797548 A	16-02-2001	FR 2797548 A1	16-02-2001
WO 9843431 A	01-10-1998	WO 9843431 A1	01-10-1998
		AT 228747 T	15-12-2002
		AU 746178 B2	18-04-2002
		AU 2770597 A	20-10-1998
		CA 2284153 A1	01-10-1998
		DE 69717505 D1	09-01-2003
		DE 69717505 T2	02-10-2003
		EP 0974230 A1	26-01-2000
		HK 1025450 A1	19-09-2003
		JP 2001516532 T	25-09-2001
		NO 994535 A	22-11-1999
		NZ 500201 A	27-09-2002
		PL 335754 A1	22-05-2000
		TR 200000842 T2	21-07-2000
		AT 227492 T	15-11-2002
		AT 228746 T	15-12-2002
		AT 232670 T	15-02-2003
		AT 233415 T	15-03-2003
		AT 247297 T	15-08-2003
		AT 225108 T	15-10-2002
		AT 226003 T	15-10-2002
		AT 228289 T	15-12-2002
		AT 226378 T	15-11-2002
		AU 742213 B2	20-12-2001
		AU 746305 B2	18-04-2002
		AU 745783 B2	28-03-2002
		AU 741114 B2	22-11-2001
		AU 754166 B2	07-11-2002
		AU 744517 B2	28-02-2002
		AU 2770697 A	20-10-1998
		AU 742956 B2	17-01-2002
		AU 742067 B2	13-12-2001
		AU 740740 B2	15-11-2001
		AU 744977 B2	07-03-2002
		AU 739663 B2	18-10-2001
		AU 745672 B2	28-03-2002
		AU 740887 B2	15-11-2001
		AU 7038198 A	20-10-1998

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 03/04608

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9843431 A		AU 740632 B2	08-11-2001
		AU 740224 B2	01-11-2001
		BR 9714590 A	17-09-2002
		BR 9714591 A	17-09-2002
		BR 9714598 A	06-08-2002
		BR 9714599 A	10-09-2002
		BR 9714600 A	10-09-2002
		BR 9714601 A	10-09-2002
		BR 9714602 A	17-09-2002
		BR 9714603 A	16-05-2000
		BR 9714604 A	06-08-2002

Form PCT/ISA/210 (patent family annex) (January 2004)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100122769
弁理士 笛田 秀仙
(72)発明者 ファン デン ヘウヴェル セバスチャーン エイ エフ エイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６
(72)発明者 アシュレイ アレキス エス アール
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６

Ｆターム(参考) 5B017 AA02 CA16