(19)日本国特許庁(JP)

再 公 表 特 許(A1)

(11)国際公開番号
WO2014/030283

発行日　平成28年7月28日(2016.7.28)

(43)国際公開日　平成26年2月27日(2014.2.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5C164
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
G09C 1/00	(2006.01)	G09C	1/00	640D	
G06F 21/64	(2013.01)	H04L	9/00	601F	
H04N 21/262	(2011.01)	G06F	21/64		

審査請求 有　予備審査請求 未請求　（全 35 頁）　最終頁に続く

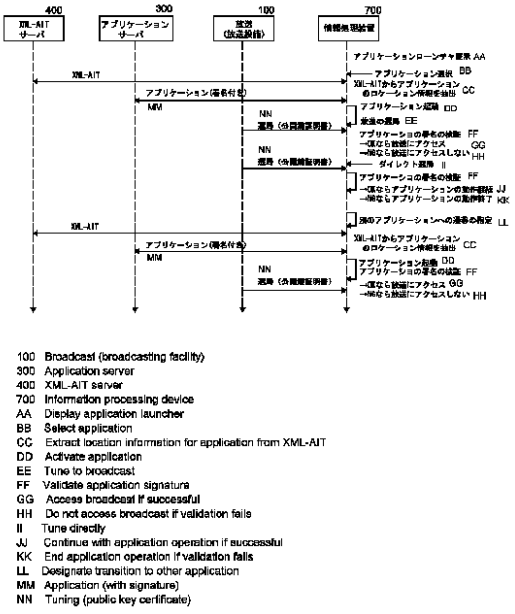
出願番号　特願2014-531484 (P2014-531484)
(21)国際出願番号　PCT/JP2013/003894
(22)国際出願日　平成25年6月21日(2013.6.21)
(31)優先権主張番号　特願2012-182689 (P2012-182689)
(32)優先日　平成24年8月21日(2012.8.21)
(33)優先権主張国　日本国(JP)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100104215
弁理士　大森　純一
(74)代理人　100196575
弁理士　高橋　満
(74)代理人　100117330
弁理士　折居　章
(74)代理人　100160989
弁理士　関根　正好
(74)代理人　100168181
弁理士　中村　哲平
(74)代理人　100170346
弁理士　吉田　望

最終頁に続く

(54)【発明の名称】署名検証情報の伝送方法、情報処理装置、情報処理方法および放送送出装置

(57)【要約】
【課題】放送データを処理可能なアプリケーションとこのアプリケーションの動作を管理するアプリケーション情報テーブルを用いたサービスの品質の向上を図る。
【解決手段】それぞれネットワークを通じて情報処理装置に伝送され、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルのいずれか一方に添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する。
【選択図】図１３



100 Broadcast (broadcasting facility)
300 Application server
400 XML-AIT server
700 Information processing device
AA Display application launcher
BB Select application
CC Extract location information for application from XML-AIT
DD Activate application
EE Tune to broadcast
FF Validate application signature
GG Access broadcast if successful
HH Do not access broadcast if validation fails
II Tune directly
JJ Continue with application operation if successful
KK End application operation if validation fails
LL Designate transition to other application
MM Application (with signature)
NN Tuning (public key certificate)

【特許請求の範囲】
【請求項１】
それぞれネットワークを通じて情報処理装置に伝送され、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルのいずれか一方に添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する
署名検証情報の伝送方法。
【請求項２】
請求項１に記載の署名検証情報の伝送方法であって、
前記検証情報をcomponent_tag=0x40にモジュールとして配置し、
伝送される前記検証情報の更新を前記情報処理装置に検知させるための情報をＤＩＩに配置する
署名検証情報の伝送方法。
【請求項３】
請求項１に記載の署名検証情報の伝送方法であって、
前記検証情報をルート証明書記述子内に格納して伝送する
署名検証情報の伝送方法。
【請求項４】
請求項３に記載の署名検証情報の伝送方法であって、
前記ルート証明書記述子内のroot_certificate_typeの値として、前記検証情報の伝送を示す値が格納される
署名検証情報の伝送方法。
【請求項５】
請求項３に記載の署名検証情報の伝送方法であって、
前記ルート証明書記述子の中でデータ放送向け公開鍵証明書を伝送できる格納領域のうち、所定の格納領域に前記検証情報か格納され、前記ルート証明書記述子に前記検証情報が伝送されることを示すフラグ情報が配置される
署名検証情報の伝送方法。
【請求項６】
放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルをネットワークを通じて取得する取得部と、
それぞれ取得された前記アプリケーションと前記アプリケーション情報テーブルのいずれか一方に添付された電子署名の検証に用いられ、データカルーセル伝送された検証データを取得して前記電子署名を検証するコントローラと
を具備する情報処理装置。
【請求項７】
取得部が、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルをネットワークを通じて取得し、
コントローラが、それぞれ取得された前記アプリケーションと前記アプリケーション情報テーブルのいずれか一方に添付された電子署名の検証に用いられ、データカルーセル伝送された検証データを取得して前記電子署名を検証する
情報処理方法。
【請求項８】
それぞれネットワークを通じて情報処理装置に伝送され、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルのいずれか一方に添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する伝送部を
具備する放送送出装置。
【発明の詳細な説明】
【技術分野】

【０００１】
本技術は、署名検証情報の伝送方法、情報処理装置、情報処理方法および放送送出装置に関する。
【背景技術】
【０００２】
近年、放送コンテンツの再生と同時に、インターネット等のネットワークを通じて配信されるアプリケーションの実行を行うことを可能とする技術が知られている。このような技術として、ハイブリッドブロードバンド放送（Hybrid Broadcast Broadband TV、以下「ＨｂｂＴＶ」と称する。）と呼ばれる技術が知られている。ＨｂｂＴＶの標準規格として、欧州では「ETSI TS 102 796」（非特許文献１参照。）が策定されている。また、我が国でもこれに準拠した標準規格「ARIB STD-B23」（非特許文献２参照。）が策定されている。
【０００３】
例えばＨｂｂＴＶなどのように、放送コンテンツの再生と同時にアプリケーションが実行されるシステムでは、アプリケーションの起動から終了までのライフサイクルが、放送コンテンツに重畳されたＡＩＴセクション（Application Information Table）と呼ばれるデータ構造によって管理される。ＡＩＴセクションを取得した情報端末は、ＡＩＴセクションに含まれるアプリケーション制御用のコードをもとにアプリケーションの制御を行う。
【０００４】
また、放送ＡＩＴセクションと同等の情報を有し、インターネットなど通信網を利用して受信機にアプリケーションに関する情報を提供するために最適なフォーマットとして、ＸＭＬ形式で記述されたＸＭＬ－ＡＩＴがある。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】ETSI（European Telecommunications Standards Institute）「ETSI TS 102 796 V1.1.1 （2010-06)」http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.01.01_60/ts_102796v010101p.pdf（平成２３年１０月２１日閲覧）
【非特許文献２】社団法人電波産業会「デジタル放送におけるアプリケーション実行環境 標準規格 ARIB STD-B23 1.2版」http://www.arib.or.jp/english/html/overview/doc/2-STD-B23v1_2.pdf（平成２３年１０月２１日閲覧）
【発明の概要】
【発明が解決しようとする課題】
【０００６】
今後、地上デジタル放送等の放送番組と連動させながら実行されるアプリケーション（放送連動アプリケーション）のほか、放送と直接関係のないアプリケーション（放送非連動アプリケーション）を提供するサービスの開始が想定される。しかし、放送非連動アプリケーションを利用したサービスを実際に運用するにあたっては、解決すべき様々な課題が未だ残されており、その対策が望まれている。
【０００７】
本技術の目的は、放送データを処理可能なアプリケーションとこのアプリケーションの動作を管理するアプリケーション情報テーブルを用いたサービスの品質の向上を図ることの可能な署名検証情報の伝送方法、情報処理装置、情報処理方法および放送送出装置を提供することにある。
【課題を解決するための手段】
【０００８】
上記の課題を解決するために、本技術に係る署名検証情報の伝送方法は、それぞれネットワークを通じて情報処理装置に伝送され、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルのい

ずれか一方に添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する。

【０００９】

前記署名検証情報の伝送方法において、前記検証情報をcomponent_tag=0x40にモジュールとして配置し、伝送される前記検証情報の更新を前記情報処理装置に検知させるための情報をＤＩＩに配置するようにしてもよい。

【００１０】

前記署名検証情報の伝送方法において、前記検証情報をルート証明書記述子内に格納して伝送してもよい。

【００１１】

前記署名検証情報の伝送方法において、前記ルート証明書記述子内のroot_certificate_typeの値として、前記検証情報の伝送を示す値が格納されるようにしてよい。

【００１２】

前記署名検証情報の伝送方法において、前記ルート証明書記述子の中でデータ放送向け公開鍵証明書を伝送できる格納領域のうち、所定の格納領域に前記検証情報か格納され、前記ルート証明書記述子に前記検証情報が伝送されることを示すフラグ情報が配置されるようにしてもよい。

【００１３】

本技術の別の観点に基づく情報処理装置は、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルをネットワークを通じて取得する取得部と、それぞれ取得された前記アプリケーションと前記アプリケーション情報テーブルのいずれか一方に添付された電子署名の検証に用いられ、データカルーセル伝送された検証データを取得して前記電子署名を検証するコントローラとを具備する。

【００１４】

本技術の別の観点に基づく情報処理方法は、取得部が、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルをネットワークを通じて取得し、コントローラが、それぞれ取得された前記アプリケーションと前記アプリケーション情報テーブルのいずれか一方に添付された電子署名の検証に用いられ、データカルーセル伝送された検証データを取得して前記電子署名を検証する。

【００１５】

本技術の別の観点に基づく放送送出装置は、それぞれネットワークを通じて情報処理装置に伝送され、放送される第１のデータを処理可能なアプリケーションと当該アプリケーションの動作を管理するアプリケーション情報テーブルのいずれか一方に添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する伝送部を具備する。

【発明の効果】

【００１６】

以上のように、本技術によれば、放送データを処理可能なアプリケーションとこのアプリケーションの動作を管理するアプリケーション情報テーブルを用いたサービスの品質の向上を図ることができる。

【図面の簡単な説明】

【００１７】

【図１】本実施形態の情報処理システムの概要を示す図である。

【図２】本実施形態のＸＭＬ－ＡＩＴのデータ構造を示す図である。

【図３】アプリケーション識別記述子の論理的構造を定義するＸＭＬスキーマの例を示す図である。

【図４】同じくアプリケーション識別記述子の論理的構造を定義するＸＭＬスキーマの例を示す図である。

【図５】図３及び図４のＸＭＬスキーマを用いて作成されるアプリケーション識別記述子

の具体例を示す図である。
【図６】ＸＭＬ－ＡＩＴに格納されるアプリケーション制御コードの定義を示す図である。
【図７】図１のシステムにおける情報処理装置の構成を示すブロック図である。
【図８】図１のシステムにおける放送局、アプリケーションサーバ、ＸＭＬ－ＡＩＴサーバおよび情報処理装置の間でのやりとりの流れを示すシーケンス図である。
【図９】図１のシステムにおける情報処理装置の処理手順を示すフローチャートである。
【図１０】本実施形態の情報処理装置においてダイレクト選局操作が発生した場合の動作を示すフローチャートである。
【図１１】本実施形態の情報処理装置において放送連動アプリケーションの遷移が発生した場合の動作を示すフローチャートである。
【図１２】電子署名の生成と検証の仕組みについて説明するためのブロック図である。
【図１３】放送局から情報処理装置に放送局公開鍵証明書を伝送する専用モジュール方式の概念図である。
【図１４】放送局公開鍵証明書記述子の構成を示す図である。
【図１５】専用モジュール方式による放送局公開鍵証明書の取得および更新に関するフローチャートである。
【図１６】データ放送拡張方式（その１）によるルート証明書記述子の構成を示す図である。
【図１７】データ放送拡張方式（その１）による放送局公開鍵証明書の取得および更新に関するフローチャートである。
【図１８】データ放送拡張方式（その２）によるルート証明書記述子の構成を示す図である。
【図１９】データ放送拡張方式（その２）による放送局公開鍵証明書の取得および更新に関するフローチャートである。
【図２０】本技術に係る第２の実施形態のＸＭＬ－ＡＩＴの概念的な構成を示す図である。
【図２１】第２の実施形態の情報処理システムにおける放送局、アプリケーションサーバ、ＸＭＬ－ＡＩＴサーバおよび情報処理装置の間でのやりとりの流れを示すシーケンス図である。
【図２２】第２の実施形態の情報処理装置の処理手順を示すフローチャートである。
【図２３】第２の実施形態の電子署名およびハッシュ値の生成とこれらの検証の仕組みについて説明するための図である。
【発明を実施するための形態】
【００１８】
以下、本技術の実施の形態を図面をもとに説明する。
＜第１の実施形態＞
［情報処理システム］
図１は、本実施形態の情報処理システムの概要を示す図である。
本実施形態の情報処理システム１は、放送局１００と、インターネットなどの第１のネットワーク２００と、アプリケーションサーバ３００と、ＸＭＬ－ＡＩＴサーバ４００と、エッジルータ５００と、ＬＡＮ（Local Area Network）などの第２のネットワーク６００と、放送用の受信機としての情報処理装置７００とを有する。
【００１９】
放送局１００は、例えば、地上波、衛星波、ＩＰ（Internet Protocol）ネットワークなどの通信媒体を介してデジタル放送信号を送信する。放送局１００は、映像、音声、字幕などの各トランスポートストリームが多重化されたＡＶストリームと、ＡＶストリームに付随するデータなどとが重畳されたいわゆる放送ストリームを送出する。ＡＶストリームに付随するデータとしては、ＨＴＭＬ、ＢＭＬなどのマークアップ言語などが含まれる。

【００２０】
アプリケーションサーバ３００は、第１のネットワーク２００に接続可能とされ、第１のネットワーク２００を通じて情報処理装置７００に放送とは直接関係のない放送非連動アプリケーションを提供する。放送非連動アプリケーションは、放送リソースの制作者以外の者によって制作されたアプリケーションであり、放送から映像、音声、字幕、ＳＩ情報、データ放送などの様々な種類の放送リソースを取得して提示などの処理を行うことができるものの、実際に放送リソースにアクセスしてもよいかどうかについては、一定の認証を必要とすることが望ましい。
【００２１】
ＸＭＬ－ＡＩＴサーバ４００は、第１のネットワーク２００に接続可能とされ、第１のネットワーク２００を通じて情報処理装置７００に、アプリケーションサーバ３００から提供される放送非連動アプリケーションを管理するためのＸＭＬ－ＡＩＴ（Extensible Markup Language-Application Information Table）を配信する。
【００２２】
なお、アプリケーションサーバ３００とＸＭＬ－ＡＩＴサーバ４００は１つのサーバであってもよい。アプリケーションサーバ３００とＸＭＬ－ＡＩＴサーバ４００は、それぞれＣＰＵ、メインメモリ、データ記憶装置、ユーザインタフェースなどを備え、典型的なコンピュータとしての構成を備える。
【００２３】
エッジルータ５００は、第１のネットワーク２００と第２のネットワーク６００とを接続するためのルータである。第２のネットワーク６００は有線、無線を問わない。
【００２４】
情報処理装置７００は、例えば、パーソナルコンピュータ、携帯電話、スマートフォン、テレビジョン装置、ゲーム機、タブレット端末、オーディオ・ビデオ再生機器などであるが、具体的に製品形態は問わない。
【００２５】
情報処理装置７００は、放送局１００からデジタル放送信号を受信し、復調してトランスポートストリームを得る。情報処理装置７００は、このトランスポートストリームから放送ストリームを分離し、デコードして情報処理装置７００に接続される表示部（図示せず）及びスピーカ部（図示せず）や、記録装置（図示せず）に出力することが可能である。
【００２６】
なお、表示部、スピーカ部および記録装置はそれぞれ、情報処理装置７００と一体であってもよいし、互いに独立した機器として直接又は第２のネットワーク６００を介して情報処理装置７００に接続されていてもよい。あるいは、表示部及びスピーカ部を有する機器（図示せず）が直接又は第２のネットワーク６００を介して情報処理装置７００に接続されていてもよい。
【００２７】
情報処理装置７００は、ＸＭＬ－ＡＩＴサーバ４００からＸＭＬ－ＡＩＴのファイルを取得し、解釈して、アプリケーションサーバ３００から放送非連動アプリケーションを所得し、起動などの制御を行うことができる。
【００２８】
［放送非連動アプリケーション］
ここで、放送非連動アプリケーションについて説明を補足する。放送非連動アプリケーションはアプリケーションサーバ３００から情報処理装置７００に提供される。放送非連動アプリケーションは、例えばＨＴＭＬ（Hyper Text Markup Language）文書、ＢＭＬ文書（Broadcast Markup Language）、ＭＨＥＧ文書（Multimedia and Hypermedia information coding）、Ｊａｖａ（登録商標）スクリプト、静止画ファイル、動画ファイルなどで構成される。
【００２９】

放送非連動アプリケーションには、改ざんを検出するための電子署名が添付される。電子署名としては、例えばＸＭＬ署名などが用いられる。ＸＭＬ署名の形式は、放送非連動アプリケーションの実体に対して独立したdetached署名、放送非連動アプリケーションの実体を包含した形式を有するenveloping署名、放送非連動アプリケーションの実体に包含された形式のenveloped署名のいずれであるかを問わない。

【００３０】

情報処理装置７００のアプリケーションコントローラ７０８は、リファレンス検証（Reference Validation）と署名検証（Signature Validation）とを含むコア検証（Core Validation）の手続きに従って、ＸＭＬ署名を検証する。

リファレンス検証とは、リソース（アプリケーションの実体）に正規化変換プロセス（Transform）及びダイジェスト計算アルゴリズム（DigestMethod）を適用することにより、リファレンス（Reference）のダイジェスト値（DigestValue）を検証する方式である。リファレンス検証により得られた結果と、登録されたダイジェスト値（DigestValue）とが比較され、これらが一致しない場合、検証失敗となる。

署名検証とは、署名情報（SignatureInfo）要素をＸＭＬ正規化アルゴリズム（CanonicalizationMethod）で指定された正規化方式でシリアル化し、鍵情報（KeyInfo）等を用いて鍵データを取得し、署名アルゴリズム（SignatureMethod）で指定された方式を用いて署名を検証する方式である。

【００３１】

アプリケーション制作者は、電子署名を放送非連動アプリケーションに付けるために、放送局１００に対して、放送非連動アプリケーションとＸＭＬ－ＡＩＴのペアに対する認証を依頼する。放送局１００は、放送非連動アプリケーションとＸＭＬ－ＡＩＴのペアについて内容を精査し、問題がなければ、電子署名の添付された放送非連動アプリケーションをアプリケーション制作者に応答する。また、放送局１００は、電子署名の検証に必要な公開鍵を含む放送局公開鍵証明書を、当該放送非連動アプリケーションがアクセスする放送チャンネル、あるいはイベント（番組）に対応するデータカルーセルで伝送する。

【００３２】

［ＸＭＬ－ＡＩＴのデータ構造］

次に、ＸＭＬ－ＡＩＴのデータ構造について説明する。

図２は、本実施形態のＸＭＬ－ＡＩＴのデータ構造を示す図である。

ＸＭＬ－ＡＩＴには、アプリケーション毎の、アプリケーション名、アプリケーション識別子、アプリケーション記述子、アプリケーションタイプ、アプリケーション制御コード２１、アプリケーションの可視性、現在のサービス内でのみ有効かを示すフラグ、アプリケーションの優先度、アプリケーションのバージョン、プラットフォームプロファイルにあわせたバージョン、アイコン、ストレージ機能の性能、トランスポートプロトコル記述子、アプリケーションロケーション記述子、アプリケーションバウンダリ記述子、アプリケーションスペシフィック記述子、アプリケーションユーセジ記述子、アプリケーションモード記述子、アプリケーション識別記述子２３などが格納される。

【００３３】

［アプリケーション識別記述子２３の詳細］

次に、アプリケーション識別記述子２３の詳細を説明する。

アプリケーション識別記述子２３としては、

１．放送非連動アプリケーションがアクセス可能な放送局系列、放送局、チャンネルおよびイベント（番組）などの放送の単位を定義する情報（第３の定義情報）、

２．放送非連動アプリケーションが利用可能な放送リソースを構成するメディア情報の種類（映像、音声、ＳＩ情報、字幕、データ放送など）を定義する情報（以下「アクセス許可情報」と呼ぶ。）（第１の定義情報）、

３．放送リソースを利用した放送非連動アプリケーションの動作を制約する情報（以下「レンダリング許可情報」と呼ぶ。）（第２の定義情報）

等が含まれる。

アクセス許可情報とレンダリング許可情報を「リソース許可情報」と総称する。

【００３４】

図３及び図４は上記のアプリケーション識別記述子２３（ApplicationIdDescriptor）の論理的構造を定義するＸＭＬスキーマの例を示す図である。

【００３５】

このＸＭＬスキーマではcomplexTypeの要素としてApplicationIdDescriptor要素が宣言されている。

このApplicationIdDescriptor要素の子要素であるsequence要素の配下には、grant_application_access_flag要素、affiliation要素、terrestrial_broadcaster要素、broadcaster要素、event要素がそれぞれ宣言されている。

【００３６】

ApplicationIdDescriptor要素は承諾アプリケーションアクセスフラグを格納する要素である。承諾アプリケーションアクセスフラグは"０"および"１"のいずれかの値をとる。承諾アプリケーションアクセスフラグが"０"であるとき、アプリケーション識別記述子２３に記述された内容が、アプリケーションとの同時の提示が禁止される条件（ブラックリスト）として解釈される。承諾アプリケーションアクセスフラグが"１"である場合、アプリケーション識別記述子２３に記述された内容が、アプリケーションとの同時の提示を許可する条件（ホワイトリスト）として解釈される。

【００３７】

affiliation要素は、その配下に、放送系列局の名前を格納するaffiliation_name要素の名前と型を宣言する要素と、放送系列局の識別子（id）を格納する属性の名前と型を宣言する要素と、放送系列局のリソース許可情報（resouce_permission）の構造を定義する別の要素を参照先として示す要素を有する。

【００３８】

terrestrial_broadcaster要素は、その配下に、地上デジタル放送局の名前を格納するterrestrial_broadcaster_name要素の名前と型を宣言する要素と、地上デジタル放送局の識別子（id）を格納する属性の名前と型を宣言する要素と、地上デジタル放送局のリソース許可情報（resouce_permission）の構造を定義する別の要素を参照先として示す要素を有する。

【００３９】

broadcaster要素は、その配下に、ＢＳ／ＣＳ放送局の名前を格納するbroadcaster_name要素の名前とその型を宣言する要素と、ＢＳ／ＣＳ放送局の識別子（id）を格納する属性の名前と型を宣言する要素と、ＢＳ／ＣＳ放送局のリソース許可情報（resouce_permission）の構造を定義する別の要素を参照先として示す要素を有する。

【００４０】

event要素は、その配下に、イベントを指定するための情報の構造を定義する別の要素（attributeGroup_name要素）の参照先を示す要素を有する。

【００４１】

attributeGroup_name要素は、その配下に、イベントの名前を格納するevent_name要素の名前とその型を宣言する要素と、ネットワークＩＤを格納するnetwork_id属性の名前とその型を定義する要素と、トランスポートストリームＩＤを格納するtransport_stream_id属性の名前とその型を定義する要素と、サービスＩＤを格納するservice_id属性の名前とその型を定義する要素と、イベントＩＤを格納するevent_id属性の名前とその型を定義する要素と、イベントのリソース許可情報（resouce_permission）の構造を宣言する別の要素の参照先を示す要素を有する。

ここで、network_id属性、transport_stream_id属性、service_id属性はチャンネルを識別するための情報である。

また、event_id属性の名前とその型を定義する属性の値の記載は必須ではない。この記載がない場合にはチャンネルのみが指定されたことになる。

【００４２】

このＸＭＬスキーマでは他のcomplexTypeの要素としてresouce_permission要素が宣言されている。resouce_permission要素は、その配下に、アクセス許可情報を格納するaccess_permission要素の名前とその型を定義する要素と、レンダリング許可情報を格納するrendering_permission要素の名前とその型を定義する要素と、リソース許可情報（resouce_permission）の識別子（id）を格納する属性の名前と型を宣言する要素を有する。

【００４３】

図５は図３及び図４のＸＭＬスキーマを用いて作成されるアプリケーション識別記述子２３の具体例を示す図である。

このアプリケーション識別記述子２３の具体例は、放送局系列とＢＳ／ＣＳ放送局の放送単位に対してリソース許可情報がホワイトリストとして指定された場合を示すものである。

【００４４】

すなわち、承諾アプリケーションアクセスフラグとして"1"が指定され、識別子が"00000001"、名前が"affiliation_A"という放送系列局に対して、識別子が"01"、アクセス許可情報（access_permission）の値が"10"、レンダリング許可情報（rendering_permission）の値が"20"のリソース許可情報（resouce_permission）が指定されている。また、識別子が"00000002"、名前が"broadcaster_B"というＢＳ／ＣＳ放送局に対して、識別子が"02"、アクセス許可情報（access_permission）の値が"30"、レンダリング許可情報（rendering_permission）の値が"40"のリソース許可情報（resouce_permission）が指定されている。

アクセス許可情報（access_permission）の値、レンダリング許可情報（rendering_permission）の値に対して割り当てられる意味はサービスにおいて任意に決められる。

【００４５】

［アプリケーション制御コードの定義］

アプリケーションのライフサイクルは、ＸＭＬ－ＡＩＴに格納されるアプリケーション制御コード２１をもとに、情報処理装置７００によって動的に制御される。

【００４６】

図６はＸＭＬ－ＡＩＴに格納されるアプリケーション制御コード２１の定義を示す図である。

同図に示すように、アプリケーション制御コードとしては、"AUTOSTART"、"PRESENT"、"DESTROY"、"KILL"、"PREFETCH"、"REMOTE"、"DISABLED"、"PLAYBACK_AUTOSTART"が標準規格上存在する。これらアプリケーション制御コードの定義は以下のとおりである。

【００４７】

"AUTOSTART"は、サービスの選択に伴いアプリケーションを自動で起動することを指示するコードである。アプリケーションが既に実行されている場合にはこの限りでない。

"PRESENT"は、サービスが選択されている間、アプリケーションを実行可能な状態とすることを指示するコードである。但し、対象のアプリケーションは、サービスの選択に伴って自動的にアプリケーションは起動されず、ユーザからの起動の指示を受けて起動される。

"DESTROY"は、アプリケーションの終了の許可を指示するコードである。

"KILL"は、アプリケーションの強制的な終了を指示するコードである。

"PREFETCH"は、アプリケーションのキャッシュを指示するコードである。

"REMOTE"は、現在のトランスポートストリームでは取得できないアプリケーションであることを示すコードである。そのアプリケーションは、別のトランスポートストリームあるいはキャッシュから取得して利用可能となる。

"DISABLED"は、アプリケーションの起動を禁止することを示すコードである。

"PLAYBACK_AUTOSTART"は、ストレージ（記録装置）に録画された放送コンテンツの再生に伴いアプリケーションを起動させるためのコードである。

【００４８】

［情報処理装置の構成］

図７は本実施形態の情報処理装置７００の構成を示すブロック図である。
情報処理装置７００は、放送インタフェース７０１、デマルチプレクサ７０２、出力処理部７０３、映像デコーダ７０４、音声デコーダ７０５、字幕デコーダ７０６、通信インタフェース７０７（取得部）、アプリケーションコントローラ７０８（コントローラ）を有する。

【００４９】
放送インタフェース７０１は、アンテナ及びチューナを有し、これらを用いてユーザにより選局されたデジタル放送信号を受信する。放送インタフェース７０１は、受信したデジタル放送信号に対して復調処理などを施して得たトランスポートストリームをデマルチプレクサ７０２に出力する。

【００５０】
デマルチプレクサ７０２は、トランスポートストリームから放送コンテンツのストリームパケット、アプリケーションのパケット、ＡＩＴセクションのパケットをそれぞれ分離する。デマルチプレクサ７０２は、放送コンテンツのストリームパケットから映像ＥＳ（Elementary Stream）、音声ＥＳ、字幕ＥＳを分離する。デマルチプレクサ７０２は、映像ＥＳを映像デコーダ７０４に、音声ＥＳを音声デコーダ７０５に、字幕ＥＳを字幕デコーダ７０６に、そしてアプリケーションのパケット、およびＡＩＴセクションを含むＰＳＩ／ＳＩ（Program Specific Information/Service Information）のパケットをアプリケーションコントローラ７０８にそれぞれ分配する。

【００５１】
映像デコーダ７０４は、映像ＥＳをデコードして映像信号を生成し、生成した映像信号を出力処理部７０３に出力する。音声デコーダ７０５は、音声ＥＳをデコードして音声信号を生成し、生成した音声信号を出力処理部７０３に出力する。
字幕デコーダ７０６は、字幕ＥＳをデコードして字幕信号を生成し、生成した字幕信号を出力処理部７０３に出力する。

【００５２】
放送インタフェース７０１、デマルチプレクサ７０２、出力処理部７０３、映像デコーダ７０４、音声デコーダ７０５、字幕デコーダ７０６は、放送コンテンツを受信し、処理する放送処理部である。

【００５３】
通信インタフェース７０７は、ＬＡＮなどの第２のネットワーク６００を通じて外部の機器と通信を行うためのインタフェースである。通信インタフェース７０７は無線による通信、有線による通信を問わない。

【００５４】
アプリケーションコントローラ７０８は、アプリケーションの制御に関する処理を行うコントローラである。

【００５５】
出力処理部７０３は、映像デコーダ７０４からの映像信号、音声デコーダ７０５からの音声信号、字幕デコーダ７０６からの字幕信号及びアプリケーションコントローラ７０８からの映像信号や音声信号等を合成し、情報処理装置７００に接続された記録装置（図示せず）、表示部及びスピーカ部（図示せず）に出力する。

【００５６】
上記の情報処理装置７００の少なくともアプリケーションコントローラ７０８を含む構成の一部または全ては、ＣＰＵ（Central Processing Unit）およびメモリを有するコンピュータと、このコンピュータを放送処理部、アプリケーションコントローラ７０８などとして機能させるプログラムとにより提供することが可能である。

【００５７】
［情報処理システム１の動作］
次に、本実施形態の情報処理システム１の動作を説明する。

【００５８】

（１．放送非連動アプリケーションによる放送リソースの利用の制御）

図８は放送局１００（放送送出装置）、アプリケーションサーバ３００、ＸＭＬ－ＡＩＴサーバ４００、および情報処理装置７００の間でのやりとりの流れを示すシーケンス図である。図９は情報処理装置７００の処理手順を示すフローチャートである。

【００５９】

情報処理装置７００は、例えばリモコンなどを使ってユーザにより選択されたアプリケーションローンチャを表示する（ステップＳ１０１）。アプリケーションローンチャは、例えば、情報処理装置７００に実装された、いわゆるレジデントアプリケーションや、ＨＴＭＬブラウザによって提示されるＨＴＭＬ５（Hyper Text Markup Language 5）、ＢＭＬ(Broadcast Markup Language)などによって実現される。アプリケーションローンチャには、放送非連動アプリケーションのメニューが表示される。

【００６０】

ユーザは例えばリモコンなどを使って起動させたい放送非連動アプリケーションを選択することができる。アプリケーションローンチャに表示されたメニューの放送非連動アプリケーションのメニューには、放送非連動アプリケーション用のＸＭＬ－ＡＩＴを情報処理装置７００に取得させるためのスクリプトなどが組み込まれている。

【００６１】

アプリケーションローンチャに表示された放送非連動アプリケーションのメニュー上で、リモコンを使ったユーザの操作によって任意の放送非連動アプリケーションが選択されると（ステップＳ１０２）、その放送非連動アプリケーションに対応するスクリプトが実行されることによって、情報処理装置７００のアプリケーションコントローラ７０８は、当該放送非連動アプリケーション用のＸＭＬ－ＡＩＴをＸＭＬ－ＡＩＴサーバ４００から取得する（ステップＳ１０３）。

【００６２】

情報処理装置７００のアプリケーションコントローラ７０８は、取得したＸＭＬ－ＡＩＴに記述されているアプリケーションのロケーション情報をもとにアプリケーションサーバ３００から、電子署名が添付された放送非連動アプリケーションを取得し（ステップＳ１０４）、取得した放送非連動アプリケーションを起動する（ステップＳ１０５）。

【００６３】

アプリケーションコントローラ７０８は、放送非連動アプリケーションからの放送リソースのアクセス要求を監視する（ステップＳ１０６）。アプリケーションコントローラ７０８は、放送非連動アプリケーションからの放送リソースのアクセス要求を検出すると（ステップＳ１０７のＹ）、この放送リソースに対応する放送局公開鍵証明書が情報処理装置７００内のメモリに保存されているかどうかを調べる（ステップＳ１０７）。

【００６４】

情報処理装置７００のアプリケーションコントローラ７０８は、放送局公開鍵証明書が情報処理装置７００内のメモリに保存されていない場合には、目的の放送局公開鍵証明書がデータカルーセルで伝送されてくるのを待つ。アプリケーションコントローラ７０８は、データカルーセルで伝送されてきた目的の放送局公開鍵証明書を受信すると、これをメモリに保存する（ステップＳ１０８）。

【００６５】

アプリケーションコントローラ７０８は、実行中の放送非連動アプリケーションに添付された電子署名を、メモリに保存された放送局公開鍵証明書を用いて検証する（ステップＳ１１０）。この電子署名の署名に失敗した場合（ステップＳ１１１のＮ）、アプリケーションコントローラ７０８は、当該放送非連動アプリケーションによる全ての放送リソースのアクセスを禁止するように設定をする（ステップＳ１１２）。

【００６６】

このアクセス禁止の設定の後、もしくは電子署名の署名に成功した場合（ステップＳ１１１のＹ）、アプリケーションコントローラ７０８は、ＸＭＬ－ＡＩＴに記述されたアクセス許可情報（access_permission）を参照して、当該放送非連動アプリケーションに対

して許容された範囲で放送リソースをアクセスする（ステップＳ１１３）。このとき、すべての放送リソースへのアクセスが許容されない場合もある。この場合は、放送リソースのアクセスは行われず、放送非連動アプリケーションのみ表示された状態になる。

【００６７】

例えば、図５に示したアプリケーション識別記述子２３が取得され、アクセス許可情報（access_permission）の値"10"は"すべての放送リソースの利用を許可する。"を意味することとする。ここで"すべての放送リソース"とは、放送されるすべての種類（映像、音声、ＳＩ情報、字幕、データ放送など）のメディア情報のことである。

【００６８】

この想定において、実行された放送非連動アプリケーションによってアクセス要求された放送リソースが"affiliation_A"という放送系列局に属する放送局からの放送リソースである場合には、当該放送非連動アプリケーションによる放送リソースのアクセスは可能と判定される。

【００６９】

また、実行された放送非連動アプリケーションによってアクセス要求された放送リソースが、"affiliation_A"という放送系列局に属さない放送局からの放送リソースであって、"broadcaster_B"というＢＳ／ＣＳ放送局以外の放送局の放送リソースである場合には、当該放送非連動アプリケーションによる放送リソースのアクセスは不可と判定される。

【００７０】

この後、例えば、ユーザによるリモコンの操作によるアプリケーションの終了指示や別のアプリケーションへの遷移などが発生すると（ステップＳ１１４のＹＥＳ）、情報処理装置７００のアプリケーションコントローラ７０８は放送非連動アプリケーションを終了させる（ステップＳ１１５）。

【００７１】

また、情報処理装置７００のアプリケーションコントローラ７０８は、放送非連動アプリケーションの実行中に新たに取得したＸＭＬ－ＡＩＴに"AUTOSTART"、"DESTROY"、"KILL"以外のアプリケーション制御コードが記述されている場合には、そのアプリケーション制御コードに従って放送非連動アプリケーションの状態を遷移させるなどの処理を行った後（ステップＳ１１６）、次のＸＭＬ－ＡＩＴを待機する。

【００７２】

放送非連動アプリケーションが実行中であるとき、例えば、ユーザのマニュアル操作などによって放送チャンネルが切り替えられる操作（ダイレクト選局操作）が行われることがある。

【００７３】

図１０は、ダイレクト選局操作が発生した場合の動作を示すフローチャートである。

ダイレクト選局操作が発生したとき（ステップＳ２０１）、情報処理装置７００のアプリケーションコントローラ７０８は、このダイレクト選局された放送チャンネルに対応する放送局公開鍵証明書が情報処理装置７００内のメモリに保存されているかどうかを調べる（ステップＳ２０２）。

【００７４】

情報処理装置７００のアプリケーションコントローラ７０８は、放送局公開鍵証明書が情報処理装置７００内のメモリに保存されていない場合には、目的の放送局公開鍵証明書が切り替えられた放送チャンネルのデータカルーセルで伝送されてくるのを待ち、データカルーセルで伝送されてきた目的の放送局公開鍵証明書を受信すると、これをメモリに保存する（ステップＳ２０３）。

【００７５】

アプリケーションコントローラ７０８は、実行中の放送非連動アプリケーションに添付された電子署名を、メモリに保存された放送局公開鍵証明書を用いて検証する（ステップＳ２０５）。この電子署名の署名に失敗した場合（ステップＳ２０６のＮ）、アプリケーションコントローラ７０８は、当該放送非連動アプリケーションを終了させる（ステップ

Ｓ２１０）。
【００７６】
電子署名の署名に成功した場合（ステップＳ２０６のＹ）、アプリケーションコントローラ７０８は、ＸＭＬ－ＡＩＴに記述されたアクセス許可情報（access_permission）を参照して、当該放送非連動アプリケーションに対して許容された範囲で、ダイレクト選局操作によって切り替えられた放送チャンネルの放送リソースにアクセスする（ステップＳ２０７）。このとき、すべての放送リソースへのアクセスが許容されない場合もある。この場合は、放送リソースのアクセスは行われず、放送非連動アプリケーションのみ表示された状態になる。
以降の動作（ステップＳ２０８からステップＳ２１０の動作）は、図８の動作（ステップＳ１１４からステップＳ１１５の動作）と同様である。
【００７７】
次に、放送非連動アプリケーションの遷移が発生した場合の動作を図８及び図１１により説明する。
動作中の放送非連動アプリケーションに組み込まれたスクリプトの実行、あるいは、ユーザのマニュアル操作などによって、放送非連動アプリケーションの遷移の指示が発生（図１２、ステップＳ３０１）した場合の動作は、上述したアプリケーションローンチャから放送非連動アプリケーションがユーザにより選択されたときの動作と同様である。
【００７８】
（２．電子署名の生成と検証）
次に、電子署名の生成と検証について説明する。
図１２は電子署名の生成と検証の仕組みについて説明するためのブロック図である。
【００７９】
ＸＭＬ－ＡＩＴサーバ４００およびアプリケーションサーバ３００はアプリケーション制作者が所有する一台のサーバであってもよく、別々のサーバであってもよい。ここでは、ＸＭＬ－ＡＩＴサーバ４００およびアプリケーションサーバ３００を総称して「サーバ」と呼ぶ。サーバは、典型的なコンピュータの構成を有する機器である。したがって、ＣＰＵ、メインメモリ、ＨＤＤなどのストレージデバイス、マウスやキーボードなどの入力装置、液晶ディスプレイなどの表示部などで構成される。メインメモリおよびストレージデバイスには、ＯＳ（Operating System）、サーバ用のアプリケーションプログラムなどのソフトウェア、情報処理装置７００に提供される放送非連動アプリケーション、アプリケーション毎のＸＭＬ－ＡＩＴのファイル、署名生成鍵などが格納される。
【００８０】
サーバは、署名付きアプリケーション生成部３５０を有する。署名付きアプリケーション生成部３５０は、具体的にはメインメモリにロードされたプログラムと、このプログラムを実行するＣＰＵとで実現される。
【００８１】
アプリケーション制作者は、アプリケーション３５１とＸＭＬ－ＡＩＴ３５５について放送局１００に対して認証を依頼する。
図１にも示したように、放送局１００は、アプリケーション制作者より依頼された認証の対象であるアプリケーション３５１とＸＭＬ－ＡＩＴ３５５の内容を精査し、問題がなければ、ルートＣＡ８００より発行された秘密鍵と放送局公開鍵証明書のペアのうち秘密鍵を署名生成鍵３５７として署名生成器３５６に設定する。署名生成器３５６はアプリケーション３５１について署名用のハッシュ関数を用いてダイジェストを生成し、このダイジェストを署名生成鍵（秘密鍵）３５７で暗号化してＸＭＬ署名３５８を生成する。放送局１００は、生成したＸＭＬ署名３５８をサーバに応答する。署名付きアプリケーション生成部３５０は、放送局１００より応答されたＸＭＬ署名３５８をアプリケーション３５１に付加して電子署名付きのアプリケーション３６０を生成し、情報処理装置７００に配信する。
【００８２】

情報処理装置７００のアプリケーションコントローラ７０８は、サーバより取得した電子署名付きのアプリケーション３６０から署名生成器７５３にてＸＭＬ署名を抽出し、このＸＭＬ署名を放送局公開鍵証明書から取り出した署名検証鍵である公開鍵７５４を用いて検証して署名検証結果７５５を得る。

【００８３】

次に、放送局１００から情報処理装置７００に放送局公開鍵証明書を伝送する方法について説明する。

放送局１００から情報処理装置７００に放送局公開鍵証明書を伝送する方法には、専用モジュール方式、データ放送拡張方式（その１）、データ放送拡張方式（その２）などがある。

【００８４】

（１．専用モジュール方式）

図１３は専用モジュール方式の概念図である。

専用モジュール方式では、データ放送番組がユーザにより選択された時最初に起動させるべきスタート文書を含むモジュールであるcomponent_tag=0x40に、放送局公開鍵証明書４１を伝送するための専用のモジュール(例えばmodule_id=0xFFFEなど)４２が新たな配置される。

また、上記の専用モジュールで配布する放送局公開鍵証明書の更新を情報処理装置７００に知らせるために、放送局公開鍵証明書記述子がＤＩＩ（Download Info Indication）が配置される。

【００８５】

図１４は、放送局公開鍵証明書記述子の構成を示す図である。

放送局公開鍵証明書記述子（broadcast certificate_descriptor）は放送局公開鍵証明書を識別するＩＤ（broadcaster_certificate_id）および放送局公開鍵証明書のバージョン（broadcaster_certificate_version）を含む。

【００８６】

図１５は専用モジュール方式による放送局公開鍵証明書の取得および更新に関するフローチャートである。

【００８７】

まず、情報処理装置７００のコントローラ７０８は、データカルーセルで伝送されるＤＩＩのモジュール情報を監視する(ステップＳ４０１)。情報処理装置７００のコントローラ７０８は、ＤＩＩのモジュール情報に放送局公開鍵証明書記述子が含まれていることを検出すると(ステップＳ４０２のＹ)、この放送局公開鍵証明書記述子を解析し、この放送局公開鍵証明書記述子の中からＩＤとバージョンをそれぞれ抽出する(ステップＳ４０３)。

【００８８】

アプリケーションコントローラ７０８は、メモリに既に格納されている放送局公開鍵証明書のＩＤと今回取得したＩＤとを比較し、ＩＤが一致した放送局公開鍵証明書がメモリに格納されているかどうかを調べる(ステップＳ４０４)。該当する放送局公開鍵証明書が格納されていない場合(ステップＳ４０５のＮ)、アプリケーションコントローラ７０８は、データカルーセルで伝送される放送局公開鍵証明書を取得し、メモリに格納する(ステップＳ４０６)。この後、ＤＩＩのモジュール情報の監視状態に戻る。

【００８９】

該当する放送局公開鍵証明書が格納されている場合(ステップＳ４０５のＹ)、アプリケーションコントローラ７０８は、メモリに格納されている放送局公開鍵証明書のバージョンを確認する(ステップＳ４０７)。アプリケーションコントローラ７０８は、確認した放送局公開鍵証明書のバージョンと今回取得した放送局公開鍵証明書のバージョンとを比較し、放送局公開鍵証明書のバージョンアップの発生の有無を判定する(ステップＳ４０８)。

【００９０】

放送局公開鍵証明書のバージョンアップが発生していないことが判定された場合は(ステップＳ４０８のＮ)、アプリケーションコントローラ７０８はＤＩＩのモジュール情報の監視状態に戻る。

【００９１】

放送局公開鍵証明書のバージョンアップが発生したことを判定した場合(ステップＳ４０８のＮ)、アプリケーションコントローラ７０８はデータカルーセルで伝送される放送局公開鍵証明書を取得し、メモリに格納する(ステップＳ４０９)。この後、ＤＩＩのモジュール情報の監視状態に戻る。

【００９２】

以上のようにして、情報処理装置７００は、ＩＤの異なる１以上の種類の最新バージョンの放送局公開鍵証明書を取得し、メモリに格納することができる。

【００９３】

（２．データ放送拡張方式（その１））

図１６はデータ放送拡張方式（その１）によるルート証明書記述子の構成を示す図である。

データ放送拡張方式（その１）は、ルート証明書記述子のroot_certificate_typeに新しいサービスの公開鍵証明書を伝送するための拡張を施し、そこに放送局公開鍵証明書を識別するＩＤ（broadcaster_certificate_id）および放送局公開鍵証明書のバージョン（broadcaster_certificate_version）を記述するようにしたものである。

【００９４】

図１７はデータ放送拡張方式（その１）による放送局公開鍵証明書の取得および更新に関するフローチャートである。

【００９５】

まず、情報処理装置７００のアプリケーションコントローラ７０８は、データカルーセルで伝送されるＤＩＩのルート証明書記述子を監視する(ステップＳ５０１)。情報処理装置７００のコントローラ７０８は、ＤＩＩのルート証明書記述子を検出すると(ステップＳ５０２のＹ)、このルート証明書記述子を解析し、このルート証明書記述子に新しいサービスを示す値（root_certificate_type = 2）が記述されているかどうかを判定する(ステップＳ５０３)。新しいサービスを示す値（root_certificate_type = 2）が記述されていなければデータ放送の処理を行い(ステップＳ５０４)、その後、ＤＩＩのルート証明書記述子の監視状態に戻る。

【００９６】

ルート証明書記述子に新しいサービスを示す値（root_certificate_type = 2）が記述されている場合、アプリケーションコントローラ７０８は、ルート証明書記述子の中から放送局公開鍵証明書のＩＤとバージョンをそれぞれ抽出する(ステップＳ５０５)。以降のステップＳ５０６からステップＳ５１１までの動作は、専用モジュール方式のステップＳ４０４からステップＳ４０９と同じであるため、説明を省略する。

【００９７】

アプリケーションコントローラ７０８は、メモリに既に格納されている放送局公開鍵証明書のＩＤと今回取得したＩＤとを比較し、ＩＤが一致した放送局公開鍵証明書がメモリに格納されているかどうかを調べる(ステップＳ４０４)。該当する放送局公開鍵証明書が格納されていない場合(ステップＳ４０５のＮ)、アプリケーションコントローラ７０８は、データカルーセルで伝送される放送局公開鍵証明書を取得し、メモリに格納する(ステップＳ４０６)。この後、ＤＩＩのルート証明書記述子の監視状態に戻る。

【００９８】

該当する放送局公開鍵証明書が格納されている場合(ステップＳ４０５のＹ)、アプリケーションコントローラ７０８は、メモリに格納されている放送局公開鍵証明書のバージョンを確認する(ステップＳ４０７)。アプリケーションコントローラ７０８は、確認した放送局公開鍵証明書のバージョンと今回取得した放送局公開鍵証明書のバージョンとを比較し、放送局公開鍵証明書のバージョンアップの発生の有無を判定する(ステップＳ４０８)

。

【００９９】

放送局公開鍵証明書のバージョンアップが発生していないことが判定された場合は(ステップＳ４０８のＮ)、アプリケーションコントローラ７０８はＤＩＩのモジュール情報の監視状態に戻る。

【０１００】

放送局公開鍵証明書のバージョンアップが発生したことを判定した場合(ステップＳ４０８のＮ)、アプリケーションコントローラ７０８はデータカルーセルで伝送される放送局公開鍵証明書を取得し、メモリに格納する(ステップＳ４０９)。この後、ＤＩＩのモジュール情報の監視状態に戻る。

【０１０１】

以上のようにして、情報処理装置７００は、ＩＤの異なる１以上の種類の最新バージョンの放送局公開鍵証明書を取得し、メモリに格納することができる。

【０１０２】

（３．データ放送拡張方式（その２））

データ放送拡張方式（その２）は、ルート証明書記述子の中でデータ放送向け公開鍵証明書を伝送できる格納領域のうち、固定の１つの格納領域が新しいサービス向けに割り当てられ、そこに放送局公開鍵証明書を識別するＩＤ（broadcaster_certificate_id）および放送局公開鍵証明書のバージョン（broadcaster_certificate_version）が記述される。また、例えば図１８に示すように、ルート証明書記述子に新たなフラグ（broadcaster_certificate_flag）が配置される。例えば、このフラグの値が"１"であるとき、放送局公開鍵証明書が伝送されることを示し、フラグの値が"０"であるとき、放送局公開鍵証明書が伝送されないことを示す。

【０１０３】

図１９は、データ放送拡張方式（その２）による放送局公開鍵証明書の取得および更新に関するフローチャートである。

まず、情報処理装置７００のアプリケーションコントローラ７０８は、データカルーセルで伝送されるＤＩＩのルート証明書記述子を監視する(ステップＳ６０１)。情報処理装置７００のコントローラ７０８は、ＤＩＩのルート証明書記述子を検出すると(ステップＳ５０２のＹ)、このルート証明書記述子を解析し、フラグ（broadcaster_certificate_flag）の値を確認する。フラグの値が"０"である場合、アプリケーションコントローラ７０８はデータ放送の処理を行い(ステップＳ５０４)、その後、ＤＩＩのルート証明書記述子の監視状態に戻る。

【０１０４】

フラグの値が"０"である場合、アプリケーションコントローラ７０８は、ルート証明書記述子の中でデータ放送向け公開鍵証明書を伝送できる複数の格納領域のうち予め決められた格納領域から、放送局公開鍵証明書のＩＤとバージョンをそれぞれ抽出する(ステップＳ６０５)。以降のステップＳ６０６からステップＳ６１１までの動作は、専用モジュール方式のステップＳ４０４からステップＳ４０９と同じであるため、説明を省略する。

【０１０５】

以上のようにして、情報処理装置７００は、ＩＤの異なる１以上の種類の最新バージョンの放送局公開鍵証明書を取得し、メモリに格納することができる。

【０１０６】

［第１の実施形態の効果等］

本実施形態では、次のような効果が得られる。

１．本実施形態によれば、電子署名を付けたアプリケーションがアプリケーションサーバ３００から情報処理装置７００に伝送されるので、アプリケーションの改ざんを防止することができる。

２．アプリケーションの署名検証に用いられる放送局公開鍵証明書を、既存のデジタル放送で伝送するためにデータカルーセル伝送を用いることができる。このため既存のデジ

タル放送に対する最小限の変更点で、アプリケーションをセキュアに情報処理装置７００に伝送することができる。

３．データカルーセル伝送で放送局公開鍵証明書を伝送するために、既存のデジタル放送のルート証明書を伝送する資産を利用できる点も、変更点を最小限に抑えるために有益である。

４．既に開始されているデジタル放送において、既に販売済みのデジタル放送受信機への誤動作など、いわゆるレガシー問題を回避しながらアプリケーションが認証可能な新しいサービスを行うことができる。

【０１０７】

＜第２の実施形態＞

第１の実施形態では、アプリケーションに電子署名が添付されることとしたが、ＸＭＬ－ＡＩＴに電子署名を添付してもよい。この方式によると、例えば、図２０に示すように、1つのアプリケーションに対して、複数の放送局（放送局Ａ、放送局Ｂ）が放送リソースの利用を許可する場合には、ＸＭＬ－ＡＩＴには放送リソースの利用を許可するすべての放送局（放送局Ａ、放送局Ｂ）の電子署名６１、６２が添付される。

【０１０８】

図２１は第２の実施形態の情報処理システムにおける放送局１００Ａ、アプリケーションサーバ３００Ａ、ＸＭＬ－ＡＩＴサーバ４００Ａ、および情報処理装置７００Ａの間でのやりとりの流れを示すシーケンス図である。図２２は情報処理装置７００Ａの処理手順を示すフローチャートである。

以降、第２の実施形態の情報処理システムにおいて第１の実施形態の情報処理システム１と相違する点を中心に説明する。

【０１０９】

アプリケーションローンチャに表示された放送非連動アプリケーションのメニュー上で、リモコンを使ったユーザの操作によって任意の放送非連動アプリケーションが選択されると（ステップＳ７０１、Ｓ７０２）、その放送非連動アプリケーションに対応するスクリプトが実行されることによって、情報処理装置７００Ａのアプリケーションコントローラ７０８ＡＡは、当該放送非連動アプリケーション用の電子署名付きのＸＭＬ－ＡＩＴをＸＭＬ－ＡＩＴサーバ４００Ａから取得する（ステップＳ７０３）。

【０１１０】

情報処理装置７００のアプリケーションコントローラ７０８ＡＡは、取得したＸＭＬ－ＡＩＴに記述されているアプリケーションのロケーション情報をもとにアプリケーションサーバ３００Ａから、電子署名付きの放送非連動アプリケーションを取得し（ステップＳ７０４）、を起動する（ステップＳ７０５）。

【０１１１】

アプリケーションコントローラ７０８Ａは、放送非連動アプリケーションからの放送リソースのアクセス要求を監視する（ステップＳ７０６）。アプリケーションコントローラ７０８Ａは、放送非連動アプリケーションからの放送リソースのアクセス要求を検出すると（ステップＳ７０７のＹ）、この放送リソースに対応する放送局公開鍵証明書が情報処理装置７００内のメモリに保存されているかどうかを調べる（ステップＳ７０７）。

【０１１２】

情報処理装置７００Ａのアプリケーションコントローラ７０８Ａは、放送局公開鍵証明書が情報処理装置７００Ａ内のメモリに保存されていない場合には、目的の放送局公開鍵証明書がデータカルーセルで伝送されてくるのを待つ。ここで、放送局公開鍵証明書のデータカルーセル伝送は、専用モジュール方式、データ放送拡張方式（その１）、データ放送拡張方式（その２）などにより実現される。

【０１１３】

アプリケーションコントローラ７０８Ａは、データカルーセルで伝送されてきた目的の放送局公開鍵証明書を受信すると、これをメモリに保存する（ステップＳ７０８）。

【０１１４】

アプリケーションコントローラ７０８Ａは、取得されたＸＭＬ－ＡＩＴに添付された電子署名を、メモリに保存された放送局公開鍵証明書を用いて検証する（ステップＳ７１０）。以降の動作は、第１の実施形態の同じであるため、説明を省略する。

［第２の実施形態の効果等］

本実施形態では、次のような効果が得られる。

１．本実施形態によれば、電子署名を付けたＸＭＬ－ＡＩＴがサーバ４００から情報処理装置７００に伝送されるので、ＸＭＬ－ＡＩＴの改ざんを防止することができる。

２．ＸＭＬ－ＡＩＴの署名検証に用いられる放送局公開鍵証明書を、既存のデジタル放送で伝送するためにデータカルーセル伝送を用いることができる。このため既存のデジタル放送に対する最小限の変更点で、ＸＭＬ－ＡＩＴの改ざんを防止できる。

３．データカルーセル伝送で放送局公開鍵証明書を伝送するために、既存のデジタル放送のルート証明書を伝送する資産を利用できる点も、変更点を最小限に抑えるために有益である。

４．既に開始されているデジタル放送において、既に販売済みのデジタル放送受信機への誤動作など、いわゆるレガシー問題を回避しながらアプリケーションが認証可能な新しいサービスを行うことができる。

【０１１５】

＜変形例１＞

ところで、第２の実施形態の方式では、アプリケーションの改ざんを直接に検出することができない。そこでアプリケーションのハッシュ値をＸＭＬ－ＡＩＴに埋め込み、情報処理装置において、アプリケーションの実体から計算されるハッシュ値とＸＭＬ－ＡＩＴに埋め込まれて通知されるハッシュ値とを比較することで、アプリケーションの改ざんを間接的に検出することが可能である。以下、この方式について説明する。

【０１１６】

次に、電子署名およびハッシュ値の生成と検証について説明する。

【０１１７】

図２３は電子署名およびハッシュ値の生成とこれらの検証の仕組みについて説明するための図である。

サーバは、署名付きＡＩＴ生成部３５０Ａを有する。署名付きＡＩＴ生成部３５０Ａは、具体的にはメインメモリにロードされた、電子署名およびハッシュ値の生成を行うプログラムと、このプログラムを実行するＣＰＵとで実現される。

【０１１８】

署名付きＡＩＴ生成部３５０Ａは、アプリケーション３５１Ａの実体（バイナリコード）から所定のハッシュ演算器３５２Ａを用いてハッシュ値３５３Ａを算出する。ハッシュのアルゴリズムとしては、例えばFIPS PUB 180-1,180-2で標準規格化されているSHA-1やSHA-2などがある。

【０１１９】

署名付きＡＩＴ生成部３５０Ａは、当該アプリケーション３５１ＡのＸＭＬ－ＡＩＴ３６２Ａにハッシュ値３５３Ａを合成して、ハッシュ値付きのＸＭＬ－ＡＩＴ３５５Ａを生成する。

【０１２０】

アプリケーション制作者は、アプリケーション３５１ＡとＸＭＬ－ＡＩＴ３５５Ａについて放送局１００Ａに対して認証を依頼する。

【０１２１】

放送局１００は、アプリケーション制作者より依頼された認証の対象であるアプリケーション３５１ＡとＸＭＬ－ＡＩＴ３５５Ａの内容を精査し、問題がなければ、ルートＣＡ８００（図１参照）より発行された秘密鍵と放送局公開鍵証明書のペアのうち秘密鍵を署名生成鍵３５７Ａとして署名生成器３５６Ａに設定する。署名生成器３５６ＡはＸＭＬ－ＡＩＴ３５５Ａについて署名用のハッシュ関数を用いてダイジェストを生成し、このダイジェストを署名生成鍵（秘密鍵）３５７Ａで暗号化してＸＭＬ署名３５８Ａを生成する。

放送局１００Ａは、生成したＸＭＬ署名３５８Ａをサーバに応答する。

【０１２２】

サーバの署名付きＡＩＴ生成部３５０Ａは、放送局１００Ａより応答されたＸＭＬ署名３５８Ａをハッシュ値付きのＸＭＬ－ＡＩＴ３５５Ａに付加して電子署名付きのＸＭＬ－ＡＩＴ３６０Ａを生成し、情報処理装置７００Ａに配信する。

【０１２３】

情報処理装置７００のアプリケーションコントローラ７０８Ａは、サーバより取得したアプリケーション３５１Ａの実体（バイナリコード）から所定のハッシュ演算器７５１Ａ（ハッシュ関数）を用いてハッシュ値７５２Ａを算出する。ここで用いられるハッシュ関数は、サーバの署名付きＡＩＴ生成部３５０Ａのハッシュ演算器３５２Ａのそれと同じである必要がある。そこでアプリケーションコントローラ７０８Ａは、サーバより取得した電子署名付きのＸＭＬ－ＡＩＴ３６０Ａに記述されたハッシュアルゴリズムを確認して、ハッシュ演算器７５１Ａ（ハッシュ関数）のハッシュアルゴリズムとの整合がとれているかどうかを判定する。もしハッシュアルゴリズムの不整合が判定された場合、アプリケーションコントローラ７０８Ａはハッシュ演算器７５１Ａ（ハッシュ関数）を切り替えてサーバの署名付きＡＩＴ生成部３５０Ａのハッシュ演算器３５２Ａのそれと整合させる。

【０１２４】

アプリケーションコントローラ７０８Ａは、サーバより取得した電子署名付きのＸＭＬ－ＡＩＴ３６０Ａから抽出したハッシュ値３５３Ａとハッシュ値７５２Ａとをハッシュ比較器７５６Ａを用いて比較し、一致／不一致の結果７５７Ａを得る。

【０１２５】

アプリケーションコントローラ７０８Ａは、署名生成器７５３Ａにて、サーバより取得した電子署名付きのＸＭＬ－ＡＩＴ３６０ＡからＸＭＬ署名を抽出し、このＸＭＬ署名を署名検証鍵（公開鍵）７５４Ａを用いて検証して署名検証結果７５５Ａを得る。

【０１２６】

この変形例によれば、アプリケーションにハッシュ値を追加して情報処理装置７００に提供されるので、情報処理装置７００はアプリケーションサーバ３００より取得したアプリケーションに対して算出したハッシュ値とＸＭＬ－ＡＩＴにより伝達されたハッシュ値とを比較することによって、アプリケーションの正当性を判定することができる。

【０１２７】

ＨｂｂＴＶの標準規格を前提とした実施形態を説明したが、本技術は、ＨｂｂＴＶの標準規格を前提とすることに必ずしも限定されるものではない。

【０１２８】

その他、本技術は、上述の実施形態にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

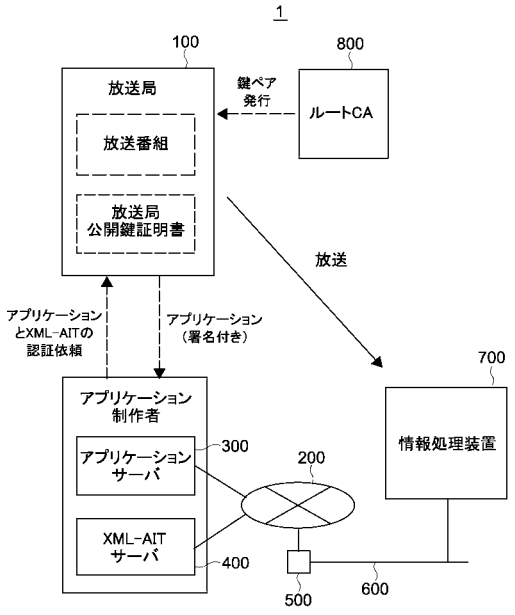
【符号の説明】

【０１２９】

１…情報処理システム
１００…放送局
２００…第１のネットワーク
３００…アプリケーションサーバ
４００…ＸＭＬ－ＡＩＴサーバ
７００…情報処理装置
７０１…放送インタフェース
７０２…デマルチプレクサ
７０３…出力処理部
７０４…映像デコーダ
７０５…音声デコーダ
７０６…字幕デコーダ
７０７…通信インタフェース

７０８…アプリケーションコントローラ
８００…放送局ＣＡ

【図１】



【図２】

field	Description
app_name	アプリケーション名
application_identifier	アプリケーションをユニークに特定するためのID
application_descriptor	アプリケーションに共通の汎用的な記述子
type	アプリケーションタイプを指定
control_code	application_control_codeの値を指定
visibility	アプリケーションの可視性を指定
service_bound	現在のサービス内でのみ有効かを示すフラグ
priority	アプリケーションの優先度を示す
version	アプリケーションのバージョン
mhp_version	platform profileにあわせたバージョン
icon	アイコンの指定
storage_capability	ストレージ機能の性能
application_transport	Transport protocol descriptor
application_location	Application location descriptor
application_boundary	Application boundary descriptor
application_specific_descriptor	Application specific descriptor
application_usage_descriptor	Application usage descriptor
application_id_descriptor	アプリケーションと番組の組合せの提示制御に関する記述子

21

23

【図３】

```
</xsd:complexType> name= "ApplicationIdDescriptor" >
  <xsd:sequence>
    <xsd:element name= "grant_application_access_flag" type= "xsd:boolean" />
    <xsd:element name= "affiliation" >
      <xsd:complexType>
        <xsd:sequence>
          <xsd:element name= "affiliation_name" type= "xsd:string" />
          <xsd:attribute name= "id " type= "xsd:string" />
          <xsd:element ref= "resoucePermission" />
        </xsd:sequence>
      </xsd:complexType>
    </xsd:element>
  </xsd:element>
  <xsd:element name= "terrestrial_broadcaster" >
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name= "terrestrial_broadcaster_name" type= "xsd:string" />
        <xsd:attribute name= "id " type= "xsd:string" />
        <xsd:element ref= "resoucePermission" />
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name= "broadcaster" >
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name= "broadcaster_name" type= "xsd:string" />
        <xsd:attribute name= "id " type= "xsd:string" />
        <xsd:element ref= "resoucePermission" />
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
```

【図４】

```
<xsd:element name= "event" >
  <xsd:complexType>
    <xsd:sequence>
      <xsd:attributeGroup ref= "event "/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:attributeGroup name= "event" >
  <xsd:sequence>
    <xsd:element name= "event_name"  type= "xsd:string" />
    <xsd:attribute name= "network_id"  type= "xsd:string" />
    <xsd:attribute name= "transport_stream_id"  type= "xsd:string" />
    <xsd:attribute name= "service_id"  type= "xsd:string" />
    <xsd:attribute name= "event_id"  type= "xsd:string" / minOccurs=0>
    <xsd:element ref= "resoucePermission" />
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name= "resoucePermission" >
  <xsd:sequence>
    <xsd:element name= "access_permission"  type= "xsd:unsignedByte" />
    <xsd:element name= "rendering_permission"  type= "xsd:unsignedByte" />
  </xsd:sequence>
  <xsd:attribute name= "id"  type= "xsd:positiveInteger" />
</xsd:complexType>
```

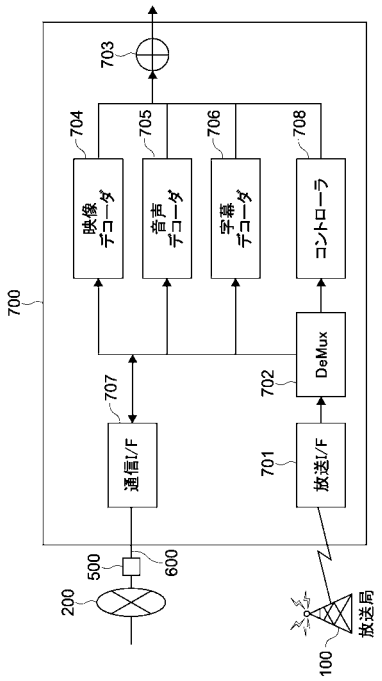
【図５】

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationIdDescriptor>
  <grant_application_access_flag> 1 </grant_application_access_flag>
  <affiliation id=00000001>
    <name> affiliation_A </name>
      <resourcePermission id=01>
        <access_permission> 10 </access_permission>
        <rendering_permission> 20 </rendering_permission>
      </resourcePermission>
  </affiliation>
  <broadcaster id=00000002>
    <name> broadcaster_B </name>
      <resourcePermission id=02>
        <access_permission> 30 </access_permission>
        <rendering_permission> 40 </rendering_permission>
      </resourcePermission>
  </broadcaster>
</ApplicationIdDescriptor>
```

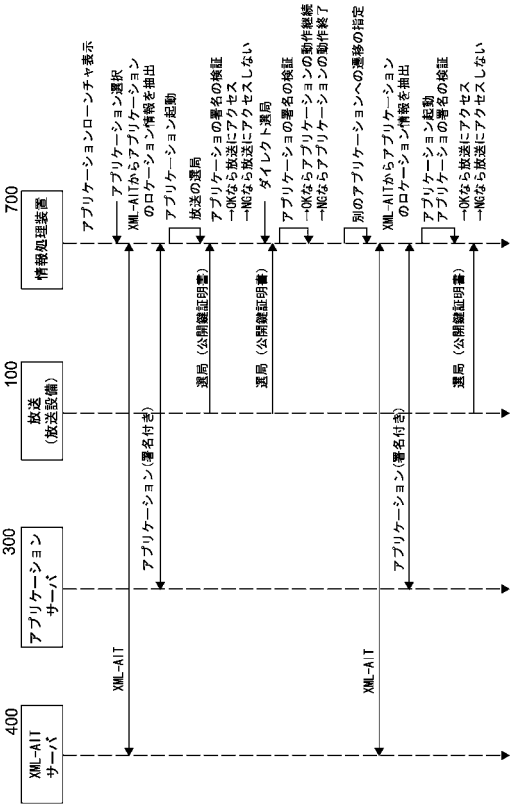
【図６】

コード	識別名	意味
0x00		reserved_future_use
0x01	AUTOSTART	サービスが選択されると、アプリケーションが自動で起動する。 (アプリケーションが既に実行中である場合を除く)
0x02	PRESENT	サービスが選択されている間、アプリケーションが実行可能な状態 であることを示す。ただし自動で起動しない。
0x03	DESTROY	アプリケーションは処理を終了する。
0x04	KILL	アプリケーションは直ちに処理を終了する。
0x05	PREFETCH	アプリケーションファイル群は受信機が可能であればキャッシュされる。 アプリケーションは起動されない。
0x06	REMOTE	アプリケーションが現在のトランスポートストリームになく、 別のストリームに遷局された場合取得できることを示す。
0x07	DISABLED	アプリケーションは起動できないことを示す。
0x08	PLAYBACK_AUTOSTART	受信機が蓄積装置から再生を実行する場合、 アプリケーションはAUTOSTARTと同じように起動する。
0x09 to 0xFF		reserved_future_use

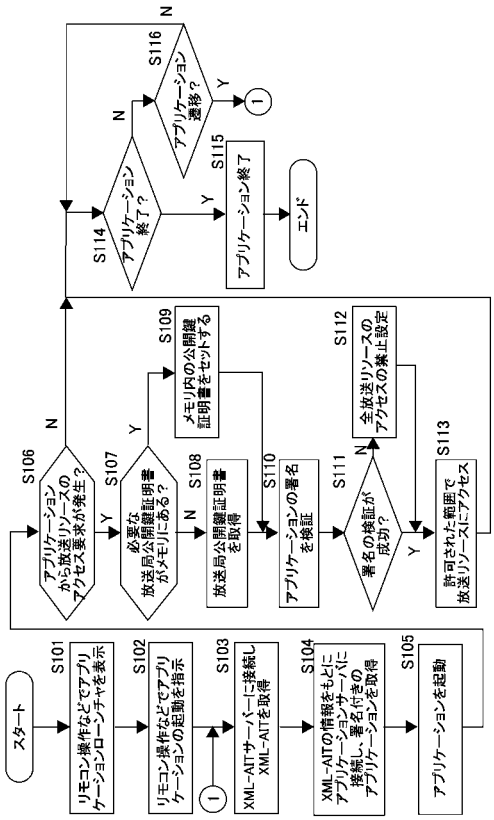
【図７】


700
703
704
705
706
708
映像デコーダ
音声デコーダ
字幕デコーダ
コントローラ
DeMux
707
702
701
通信I/F
放送I/F
500
600
200
100
放送局

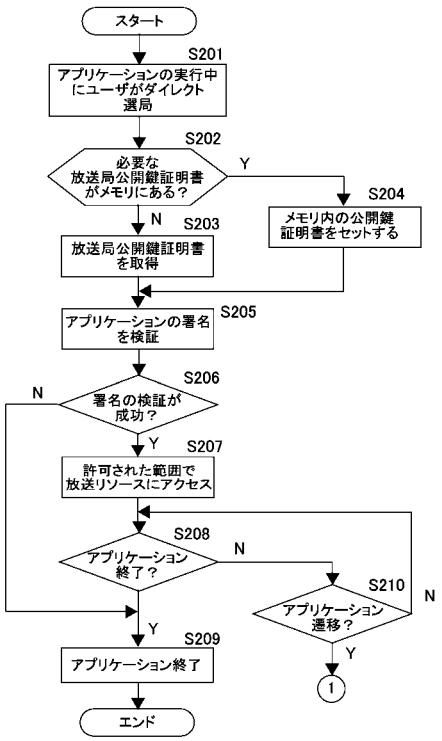
【図８】


700
情報処理装置
100
放送
(放送設備)
300
アプリケーション
サーバ
400
XML-AIT
サーバ
アプリケーションローンチャ表示
アプリケーション選択
XML-AITからアプリケーション
のロケーション情報を抽出
アプリケーション起動
放送の選局
アプリケーションの署名の検証
—OKなら放送にアクセス
—NGなら放送にアクセスしない
ダイレクト選局
アプリケーションの署名の検証
—OKならアプリケーションの動作継続
—NGならアプリケーションの動作終了
別のアプリケーションへの遷移の指定
XML-AITからアプリケーション
のロケーション情報を抽出
アプリケーション起動
アプリケーションの署名の検証
—OKなら放送にアクセス
—NGなら放送にアクセスしない
選局（公開鍵証明書）
アプリケーション（署名付き）
XML-AIT

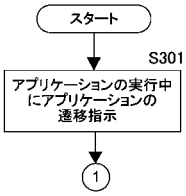
【図９】


スタート
S101
リモコン操作などでアプリケーションローンチャを表示
S102
リモコン操作などでアプリケーションの起動を指示
S103
XML-AITサーバーに接続しXML-AITを取得
S104
XML-AITの情報をもとにアプリケーションサーバに接続し、署名付きのアプリケーションを取得
S105
アプリケーションを起動
S106
アプリケーションから放送リソースのアクセス要求が発生？
S107
必要な放送局公開鍵証明書がメモリにある？
S108
放送局公開鍵証明書を取得
S109
メモリ内の公開鍵証明書をセットする
S110
アプリケーションの署名を検証
S111
署名の検証が成功？
S112
全放送リソースのアクセスの禁止設定
S113
許可された範囲で放送リソースにアクセス
S114
アプリケーション終了？
S115
アプリケーション終了
S116
アプリケーション遷移？
エンド
Y
N
1

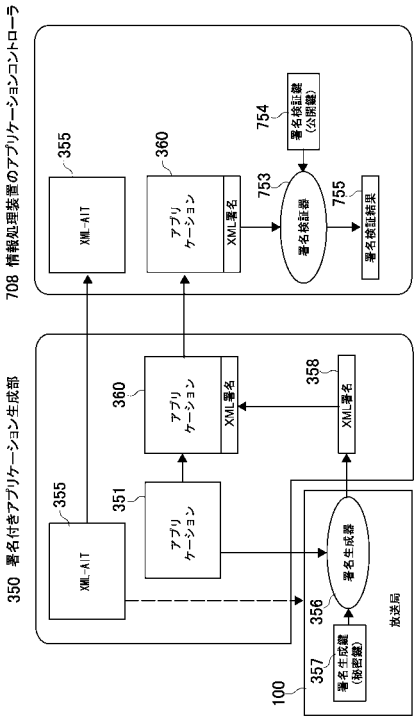
【図１０】


スタート
S201
アプリケーションの実行中にユーザがダイレクト選局
S202
必要な放送局公開鍵証明書がメモリにある？
S203
放送局公開鍵証明書を取得
S204
メモリ内の公開鍵証明書をセットする
S205
アプリケーションの署名を検証
S206
署名の検証が成功？
S207
許可された範囲で放送リソースにアクセス
S208
アプリケーション終了？
S209
アプリケーション終了
S210
アプリケーション遷移？
エンド
Y
N
1

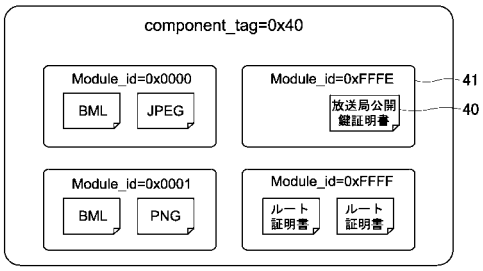
【図１１】



【図１２】



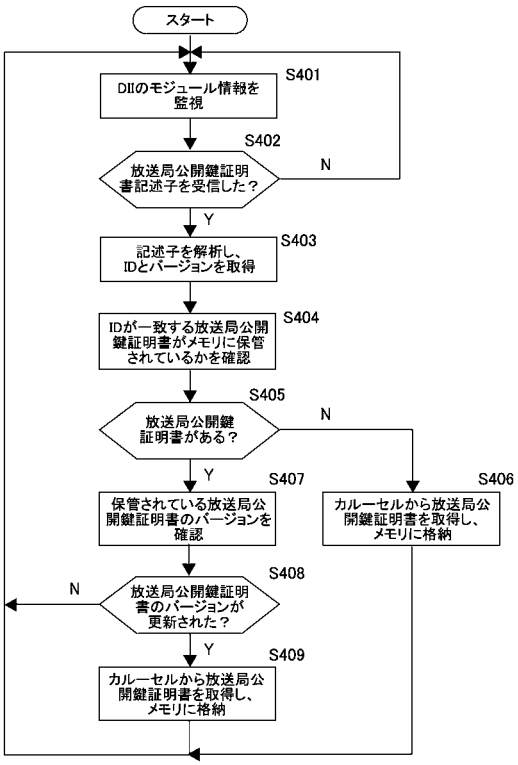
【図１３】



【図１４】

データ構造	ビット数	ビット列表記
broadcast certificate_descriptor {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
broadcaster_certificate_id	16	uimsbf
broadcaster_certificate_version	16	uimsbf
}		

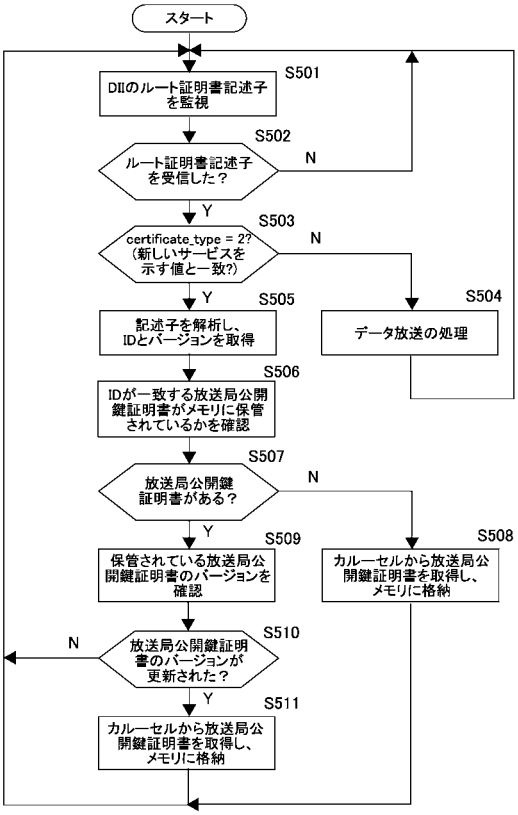
【図１５】



【図１６】

データ構造	ビット数	ビット列表記
root_certificate_descriptor {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
root_certificate_type	1	bslbf
reserved	7	bslbf
if(root_certificate_type == 0) {		
for(i=0; i<8; i++) {		
root_certificate_id	32	uimsbf
root_certificate_version	32	uimsbf
}		
} else if(root_certificate_type == 2) {		
for(i=0; i<8; i++) {		
broadcaster_certificate_id	32	uimsbf
broadcaster_certificate_version	32	uimsbf
}		
} else {		
for(i=0; i<8; i++) {		
reserved	64	bslbf
}		
}		
}		

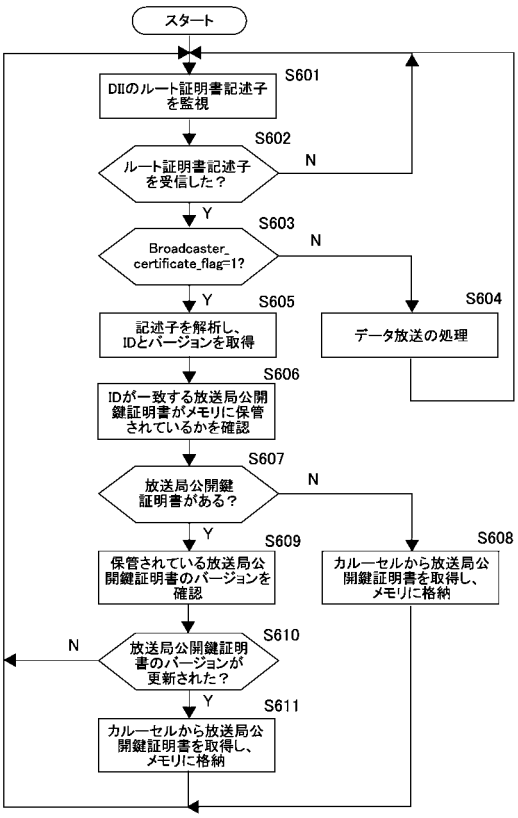
【図１７】



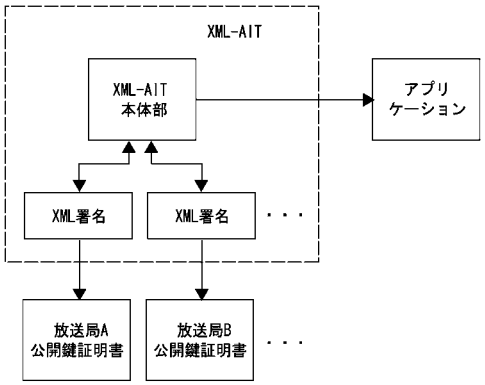
【図１８】

データ構造	ビット数	ビット列表記
root_certificate_descriptor {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
root_certificate_type	1	bslbf
broadcaster_certificate_flag	1	bslbf
reserved	6	bslbf
if(root_certificate_type == 0) {		
for(i=0; i<8; i++) {		
root_certificate_id	32	uimsbf
root_certificate_version	32	uimsbf
}		
} else {		
for(i=0; i<8; i++) {		
reserved	64	bslbf
}		
}		
}		

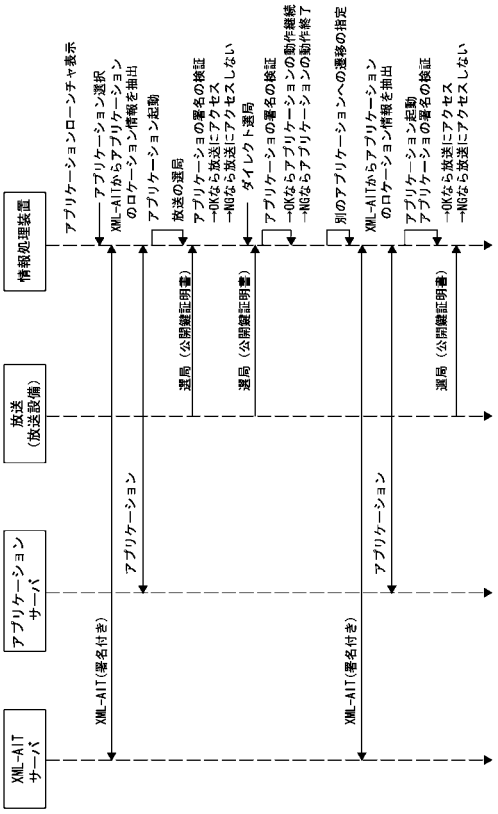
【図１９】



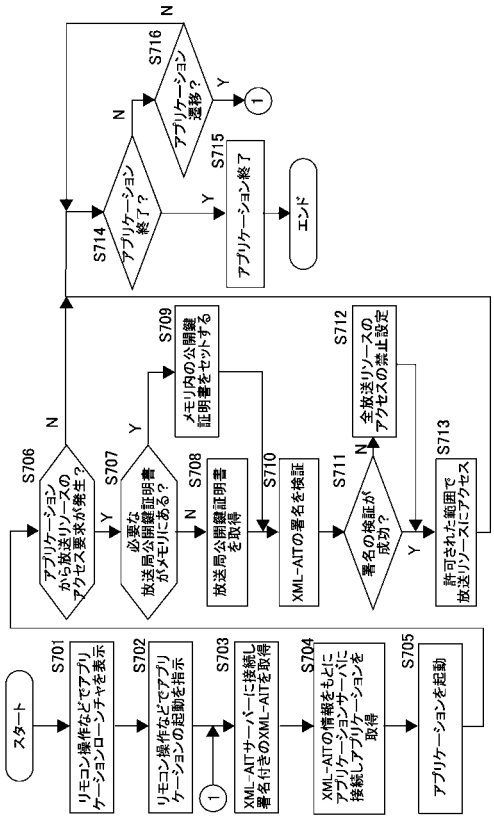
【図２０】



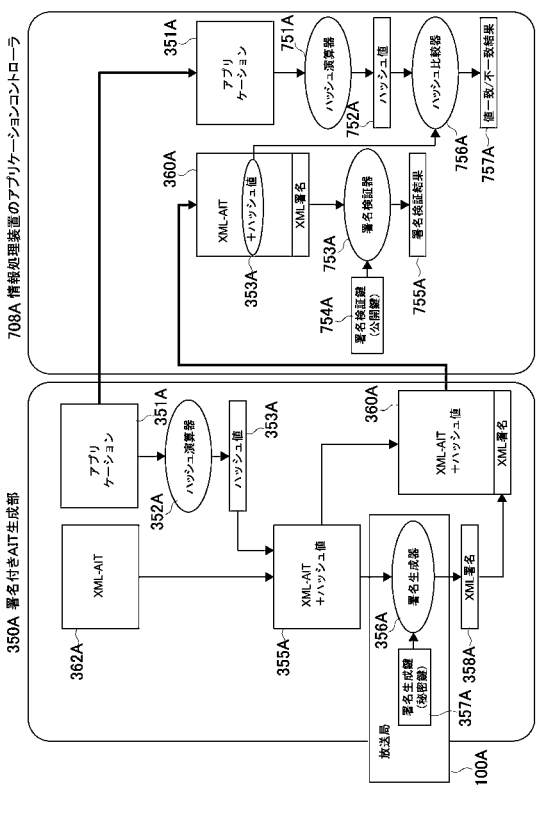
【図２１】



【図２２】



【図２３】



【手続補正書】
【提出日】平成27年1月8日(2015.1.8)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ネットワークを通じて情報処理装置に伝送され、放送されるデータを処理可能なアプリケーションの動作を管理する、前記ネットワークを通じて前記情報処理装置に伝送されるアプリケーション情報テーブルに添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する
署名検証情報の伝送方法。
【請求項２】
請求項１に記載の署名検証情報の伝送方法であって、
前記検証情報をcomponent_tag=0x40にモジュールとして配置し、伝送される前記検証情報の更新を前記情報処理装置に検知させるための情報をＤＩＩに配置する
署名検証情報の伝送方法。
【請求項３】
請求項１に記載の署名検証情報の伝送方法であって、
前記検証情報をルート証明書記述子内に格納して伝送する署名検証情報の伝送方法。
【請求項４】
請求項３に記載の署名検証情報の伝送方法であって、
前記ルート証明書記述子内のroot_certificate_typeの値として、前記検証情報の伝送を示す値が格納される署名検証情報の伝送方法。
【請求項５】
請求項３に記載の署名検証情報の伝送方法であって、
前記ルート証明書記述子の中でデータ放送向け公開鍵証明書を伝送できる格納領域のうち、所定の格納領域に前記検証情報か格納され、前記ルート証明書記述子に前記検証情報が伝送されることを示すフラグ情報が配置される
署名検証情報の伝送方法。
【請求項６】
ネットワークを通じて情報処理装置に伝送され、放送されるデータを処理可能なアプリケーションの動作を管理するアプリケーション情報テーブルを前記ネットワークを通じて取得する取得部と、
取得された前記アプリケーション情報テーブルに添付された電子署名の検証に用いられ、データカルーセル伝送された検証データを取得して前記電子署名を検証するコントローラと
を具備する情報処理装置。
【請求項７】
取得部が、ネットワークを通じて情報処理装置に伝送され、放送されるデータを処理可能なアプリケーションの動作を管理するアプリケーション情報テーブルを前記ネットワークを通じて取得し、
コントローラが、取得された前記アプリケーション情報テーブルに添付された電子署名の検証に用いられ、データカルーセル伝送された検証データを取得して前記電子署名を検証する
情報処理方法。
【請求項８】
ネットワークを通じて情報処理装置に伝送され、放送されるデータを処理可能なアプリ

ケーションの動作を管理する、前記ネットワークを通じて前記情報処理装置に伝送されるアプリケーション情報テーブルに添付された電子署名を検証するための検証情報を、データカルーセル方式で伝送する伝送部を
具備する放送送出装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０１０９
【補正方法】変更
【補正の内容】
【０１０９】
アプリケーションローンチャに表示された放送非連動アプリケーションのメニュー上で、リモコンを使ったユーザの操作によって任意の放送非連動アプリケーションが選択されると（ステップＳ７０１、Ｓ７０２）、その放送非連動アプリケーションに対応するスクリプトが実行されることによって、情報処理装置７００Ａのアプリケーションコントローラは、当該放送非連動アプリケーション用の電子署名付きのＸＭＬ－ＡＩＴをＸＭＬ－ＡＩＴサーバ４００Ａから取得する（ステップＳ７０３）。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０１１０
【補正方法】変更
【補正の内容】
【０１１０】
情報処理装置７００のアプリケーションコントローラは、取得したＸＭＬ－ＡＩＴに記述されているアプリケーションのロケーション情報をもとにアプリケーションサーバ３００Ａから、電子署名付きの放送非連動アプリケーションを取得し（ステップＳ７０４）、起動する（ステップＳ７０５）。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０１１１
【補正方法】変更
【補正の内容】
【０１１１】
アプリケーションコントローラは、放送非連動アプリケーションからの放送リソースのアクセス要求を監視する（ステップＳ７０６）。アプリケーションコントローラは、放送非連動アプリケーションからの放送リソースのアクセス要求を検出すると（ステップＳ７０７のＹ）、この放送リソースに対応する放送局公開鍵証明書が情報処理装置７００内のメモ
リに保存されているかどうかを調べる（ステップＳ７０７）。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０１１２
【補正方法】変更
【補正の内容】
【０１１２】
情報処理装置７００Ａのアプリケーションコントローラは、放送局公開鍵証明書が情報処理装置７００Ａ内のメモリに保存されていない場合には、目的の放送局公開鍵証明書がデータカルーセルで伝送されてくるのを待つ。ここで、放送局公開鍵証明書のデータカルーセル伝送は、専用モジュール方式、データ放送拡張方式（その１）、データ放送拡張方式（その２）などにより実現される。
【手続補正６】

【補正対象書類名】明細書
【補正対象項目名】０１１３
【補正方法】変更
【補正の内容】
【０１１３】
アプリケーションコントローラは、データカルーセルで伝送されてきた目的の放送局公開鍵証明書を受信すると、これをメモリに保存する（ステップＳ７０８）。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】０１１４
【補正方法】変更
【補正の内容】
【０１１４】
アプリケーションコントローラは、取得されたＸＭＬ－ＡＩＴに添付された電子署名を、メモリに保存された放送局公開鍵証明書を用いて検証する（ステップＳ７１０）。以降の動作は、第１の実施形態の同じであるため、説明を省略する。
［第２の実施形態の効果等］
本実施形態では、次のような効果が得られる。
１．本実施形態によれば、電子署名を付けたＸＭＬ－ＡＩＴがサーバ４００から情報処理装置７００に伝送されるので、ＸＭＬ－ＡＩＴの改ざんを防止することができる。
２．ＸＭＬ－ＡＩＴの署名検証に用いられる放送局公開鍵証明書を、既存のデジタル放送で伝送するためにデータカルーセル伝送を用いることができる。このため既存のデジタル放送に対する最小限の変更点で、ＸＭＬ－ＡＩＴの改ざんを防止できる。
３．データカルーセル伝送で放送局公開鍵証明書を伝送するために、既存のデジタル放送のルート証明書を伝送する資産を利用できる点も、変更点を最小限に抑えるために有益である。
４．既に開始されているデジタル放送において、既に販売済みのデジタル放送受信機への誤動作など、いわゆるレガシー問題を回避しながらアプリケーションが認証可能な新しいサービスを行うことができる。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/003894

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F21/64*(2013.01)i, *H04L9/32*(2006.01)i, *H04N7/167*(2011.01)i, *H04N7/173*(2011.01)i

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)
H04L9/08, G06F21/64, H04L9/32, H04N7/167, H04N7/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII) HOSO, KARUSERU, SHOMEI, SHOMEISHO (in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2012-151632 A (Nippon Hoso Kyokai), 09 August 2012 (09.08.2012), paragraphs [0002] to [0005], [0043] to [0051], [0059], [0137], [0138], [0161] to [0172]	1-8
Y	JP 2009-147808 A (Nippon Hoso Kyokai), 02 July 2009 (02.07.2009), paragraphs [0001], [0002], [0040], [0041], [0050], [0053], [0062] to [0074], [0086] to [0090]	1-8
Y	WO 2011/033730 A1 (Sony Corp.), 24 March 2011 (24.03.2011), paragraphs [0001] to [0004], [0040] to [0046]	1-8

☒ Further documents are listed in the continuation of Box C. ☒ See patent family 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 application or patent 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
27 August, 2013 (27.08.13)	03 September, 2013 (03.09.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/003894

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-23547 A (Nippon Hoso Kyokai), 02 February 2012 (02.02.2012), 61 to 63, 109, 110, 121, 122	1-8
A	JP 2008-507154 A (Matsushita Electric Industrial Co., Ltd.), 06 March 2008 (06.03.2008), paragraphs [0024] to [0130], [0163] to [0176]	1-8
A	JP 2003-209542 A (Toshiba Corp.), 25 July 2003 (25.07.2003), paragraphs [0057] to [0063]	1-8
A	Jiro HIRONO, The Journal of the Institute of Image Information and Television Engineers, 01 May 2004 (01.05.2004), vol.58, no.5, pages 629 to 633, particularly, 3.7 SSL/TSL Security Tsushin	1-8
A	Zhang, R. et al., Security Strategy of Digital Television Middleware System, IEEE Transactions on Consumer Electronics, 2007.08, Volume 53 Issue 3, p.969-973, see whole document	1-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2013/003894

JP 2012-151632 A	2012.08.09	(Family: none)	
JP 2009-147808 A	2009.07.02	(Family: none)	
WO 2011/033730 A1	2008.03.06	JP 2011-66556 A	2011.03.31
		CN 102484747 A	2012.05.30
		KR 10-2012-0066011 A	2012.06.21
		US 2012/0174170 A1	2012.07.05
		EP 2479987 A1	2012.07.25
JP 2008-507154 A	2008.03.06	WO 2006/006719 A1	2006.01.19
		US 2006/0015746 A1	2006.01.19
		CA 2566801 A	2006.01.19
		EP 1766974 A1	2007.03.28
		KR 10-2007-0043783 A	2007.04.25
		CN 1985516 A	2007.06.20
JP 2012-23547 A	2012.02.02	(Family: none)	
JP 2003-209542 A	2003.07.25	(Family: none)	

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１３／００３８９４

Ａ． 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. H04L9/08(2006.01)i, G06F21/64(2013.01)i, H04L9/32(2006.01)i, H04N7/167(2011.01)i, H04N7/173(2011.01)i

Ｂ． 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. H04L9/08, G06F21/64, H04L9/32, H04N7/167, H04N7/173

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamIII) 放送、カルーセル、署名、証明書

Ｃ． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2012-151632 A (日本放送協会) 2012.08.09, 2-5, 43-51, 59, 137, 138, 161-172 段落	1-8
Y	JP 2009-147808 A (日本放送協会) 2009.07.02, 1, 2, 40, 41, 50, 53, 62-74, 86-90 段落	1-8
Y	WO 2011/033730 A1 (ソニー株式会社) 2011.03.24, 1-4, 40-46 段落	1-8
A	JP 2012-23547 A (日本放送協会) 2012.02.02, 61-63, 109, 110, 121, 122	1-8

☑ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２７．０８．２０１３	国際調査報告の発送日 ０３．０９．２０１３
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｓ ９３６４ 中里 裕正 電話番号 ０３－３５８１－１１０１ 内線 ３５４６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００９年７月）

国際調査報告 国際出願番号 ＰＣＴ／ＪＰ２０１３／００３８９４

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2008-507154 A (松下電器産業株式会社) 2008.03.06, 24-130, 163-176 段落	1-8
A	JP 2003-209542 A (株式会社東芝) 2003.07.25, 57-63 段落	1-8
A	廣野二郎, 映像情報メディア学会誌, 2004.05.01, 第 58 巻 第 5 号 p.629-633, 特に 3.7 SSL/TSL セキュリティ通信	1-8
A	Zhang, R. et al., Security Strategy of Digital Television Middleware System, IEEE Transactions on Consumer Electronics, 2007.08, Volume 53 Issue 3, p.969-973, see whole document	1-8

国際調査報告
パテントファミリーに関する情報

国際出願番号 ＰＣＴ／ＪＰ２０１３／００３８９４

JP 2012-151632 A	2012.08.09	ファミリーなし	
JP 2009-147808 A	2009.07.02	ファミリーなし	
WO 2011/033730 A1	2008.03.06	JP 2011-66556 A	2011.03.31
		CN 102484747 A	2012.05.30
		KR 10-2012-0066011 A	2012.06.21
		US 2012/0174170 A1	2012.07.05
		EP 2479987 A1	2012.07.25
JP 2008-507154 A	2008.03.06	WO 2006/006719 A1	2006.01.19
		US 2006/0015746 A1	2006.01.19
		CA 2566801 A	2006.01.19
		EP 1766974 A1	2007.03.28
		KR 10-2007-0043783 A	2007.04.25
		CN 1985516 A	2007.06.20
JP 2012-23547 A	2012.02.02	ファミリーなし	
JP 2003-209542 A	2003.07.25	ファミリーなし	

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
H04N 21/2362	***(2011.01)***	H04N	21/262	
H04N 21/435	***(2011.01)***	H04N	21/2362	
		H04N	21/435	

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

(74)代理人 100168745
弁理士 金子 彩子
(74)代理人 100176131
弁理士 金山 慎太郎
(74)代理人 100197398
弁理士 千葉 絢子
(74)代理人 100197619
弁理士 白鹿 智久
(72)発明者 北原 淳
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者 北里 直久
東京都港区港南１丁目７番１号 ソニー株式会社内

Ｆターム(参考) 5C164 FA11 MB34S SB06S SB15P SC27P UB10P
5J104 AA09 AA16 BA03 EA16 LA03 NA38 PA05 PA07

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。