(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-9361
(P2013-9361A)
(43)公開日　平成25年1月10日(2013.1.10)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 7/173	(2011.01)	H04N	7/173	630	5C164
H04N 5/45	(2011.01)	H04N	5/45		
H04H 20/30	(2008.01)	H04N	7/173	610Z	
H04H 20/93	(2008.01)	H04H	20/30		
H04H 60/27	(2008.01)	H04H	20/93		

審査請求 未請求　請求項の数 4　ＯＬ　（全 32 頁）　最終頁に続く

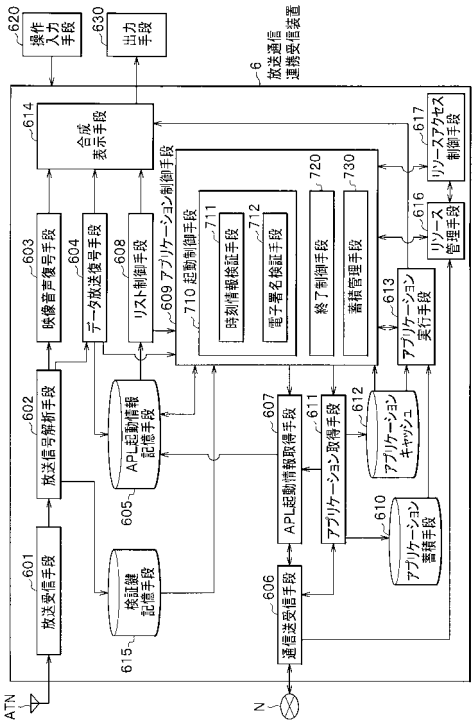
(21)出願番号　特願2012-114225 (P2012-114225)
(22)出願日　平成24年5月18日 (2012.5.18)
(31)優先権主張番号　特願2011-114074 (P2011-114074)
(32)優先日　平成23年5月20日 (2011.5.20)
(33)優先権主張国　日本国 (JP)

(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　100064414
弁理士　磯野　道造
(74)代理人　100111545
弁理士　多田　悦夫
(72)発明者　大竹　剛
東京都世田谷区砧一丁目１０番１１号　日本放送協会放送技術研究所内
(72)発明者　小川　一人
東京都世田谷区砧一丁目１０番１１号　日本放送協会放送技術研究所内

最終頁に続く

(54)【発明の名称】放送通信連携受信装置およびアプリケーションサーバ

(57)【要約】
【課題】放送番組に連動するアプリケーションを認証する。
【解決手段】放送通信連携受信装置６は、アプリケーション起動情報記憶手段６０５と、検証鍵記憶手段６１５と、ＡＰＬ起動情報を参照してリクエストをアプリケーションサーバ５１に対して送信すると共に、その応答として時刻Ｔと電子署名とが付加された署名付きアプリケーションを受信するアプリケーション取得手段６１１と、現在時刻が署名付きアプリケーションに付加された時刻Ｔで表される期間に合致しているか否かを判別する時刻情報検証手段７１１と、現在時刻が時刻Ｔに合致している場合、検証鍵を用いて署名の検証が成功したか否かを判別する電子署名検証手段７１２と、署名の検証が成功した場合、ＡＰＬ起動情報に記載された自動起動等の状態を示す制御コードを参照して当該アプリケーションの状態を制御するアプリケーション制御手段６０９とを備える。
【選択図】図５



【特許請求の範囲】
【請求項１】
デジタル放送の放送波により送出される放送コンテンツを受信すると共に、前記放送コンテンツ中の放送番組に連動したアプリケーションを配信するアプリケーションサーバから当該受信装置上で動作する前記アプリケーションを通信ネットワークを介して取得する放送通信連携受信装置であって、
前記アプリケーションを起動させるためのアプリケーション起動情報を記憶するアプリケーション起動情報記憶手段と、
前記アプリケーションサーバにて付加される署名を検証するための検証鍵を記憶する検証鍵記憶手段と、
前記アプリケーション起動情報に記載されたアプリケーションの配置場所に基づいてアプリケーションの取得制御を行うと共に、前記アプリケーション起動情報に記載された動作の状態を示す制御コードにしたがって、前記取得したアプリケーションの状態を制御するアプリケーション制御手段と、
アプリケーションを要求するためのリクエストを前記配置場所のアプリケーションサーバに対して送信すると共に、前記リクエストの応答として時刻情報と電子署名とが付加された署名付きアプリケーションを受信するアプリケーション取得手段と、を備え、
前記アプリケーション制御手段は、
現在時刻が前記取得した署名付きアプリケーションに付加された時刻情報で表される期間に合致しているか否かを判別する時刻情報検証手段と、
現在時刻が前記時刻情報で表される期間に合致している場合、前記検証鍵を用いて署名の検証が成功したか否かを判別する電子署名検証手段と、を備え、
署名の検証が成功した場合、前記制御コードにしたがって前記取得したアプリケーションの状態を制御することを特徴とする放送通信連携受信装置。
【請求項２】
外部からの操作に応じて前記放送コンテンツの中の放送番組を選局して映像および音声を提示するための出力手段に提示しているときに、当該放送コンテンツに多重化された制御信号から当該放送番組に連動したアプリケーションのための前記アプリケーション起動情報を抽出するアプリケーション起動情報抽出手段をさらに備えることを特徴とする請求項１に記載の放送通信連携受信装置。
【請求項３】
前記放送コンテンツ中に多重化されている前記検証鍵を抽出して前記検証鍵記憶手段に格納する放送信号解析手段をさらに備えることを特徴とする請求項１または請求項２に記載の放送通信連携受信装置。
【請求項４】
請求項１ないし請求項３のいずれか一項に記載の放送通信連携受信装置に対して、時刻情報を用いて署名鍵を定期的に更新する定期更新方式で生成した署名鍵で署名を付加したアプリケーションを通信ネットワークを介して配信するアプリケーションサーバであって、
マスター鍵を生成すると共に、前記署名を検証する検証鍵を生成する鍵生成手段と、
前記検証鍵を前記通信ネットワークを介して配信する検証鍵送信手段と、
前記放送番組に連動したアプリケーションを記憶するアプリケーション記憶手段と、
前記署名鍵を更新する更新タイミングにて所定の時刻情報の署名鍵に置き換える際に用いる部分鍵として前記所定の時刻情報の部分鍵を前記マスター鍵に基づいて生成し、記憶部へ格納して保持すると共に前記更新タイミングにて出力する部分鍵生成手段と、
前記部分鍵生成手段から出力された部分鍵を用いて、前記更新タイミングにおいて保持されている署名鍵を更新する署名鍵更新手段と、
前記更新された署名鍵を記憶部へ格納して保持する処理と当該記憶部から前記署名鍵を読み込んで前記署名鍵更新手段に出力する処理とを行う署名鍵管理手段と、
前記放送通信連携受信装置から前記通信ネットワークを介して前記アプリケーションを

要求するためのリクエストを受信するリクエスト受信手段と、
前記リクエストに応じて前記アプリケーション記憶手段から読み出した前記アプリケーションに対して、前記署名鍵管理手段により前記記憶部から読み込まれた、当該アプリケーションを起動させようとする時刻の時刻情報の署名鍵で電子署名を付加すると共に当該時刻情報を付加する署名生成手段と、
前記電子署名および時刻情報が付加された署名付きアプリケーションを前記リクエストの要求元に対して前記通信ネットワークを介して送信するアプリケーション送信手段と、
を備えることを特徴とするアプリケーションサーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、放送と通信とを連携して、アプリケーションを動作させる放送通信連携受信装置およびそのアプリケーションを配信するアプリケーションサーバに関する。
【背景技術】
【０００２】
近年、放送と通信とを連携したサービスを実現するための放送通信連携型システムが提案されている（非特許文献１、２参照）。この放送通信連携型システムにおいて、放送通信連携受信装置は、デジタル放送を受信する受信機であって、アプリケーションサーバから通信ネットワークを介してダウンロードしたアプリケーションを当該装置上で動作させることを想定している。
【０００３】
一般に、公共の放送サービスはセキュリティが高いが、通信ネットワークサービスに対しては悪意のある行為に対する対策が必要である。通信ネットワークにおける認証技術として、従来、ＰＫＩ（Public Key Infrastructure）が利用されている。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】松村欣司、ほか２名、「インターネット配信情報との連動による放送番組パーソナライズシステムの検討」、映像情報メディア学会年次大会講演予稿集、2009年、No.3-8
【非特許文献２】（社）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”、平成21年７月29日、p.76-88
【発明の概要】
【発明が解決しようとする課題】
【０００５】
放送通信連携型システムでは、通信ネットワークを介してアプリケーションをダウンロードするので、アプリケーションを認証する技術が求められている。また、アプリケーションが、所定の管理者によって承認されたことを示すオーソライズド（Authorized）アプリケーション（以下、単にＡアプリケーションという）となっているか、または、そのようにはなっていないか（以下、一般アプリケーションという）という観点で分類する仕組みも検討されている。例えば、放送通信連携型システムのシステム管理者が、個人や団体等の参加希望者が提供するアプリケーションを登録制により承認し、システム内での動作を保証したアプリケーションのことをＡアプリケーションとして認定する方法が考えられる。
【０００６】
また、例えばアプリケーションが放送番組に連動するタイプの場合、放送事業者あるいはその申し出を受けたシステム管理者がプロバイダまたはその提供するアプリケーションを厳格に審査し、この審査を通過したアプリケーションを、放送番組に連動した配信を許可したＡアプリケーションとして認定する方法等も考えられる。
【０００７】

例えば前者の方法によりＡアプリケーションを認定する場合、放送通信連携型システムにおいて、多くのアプリケーション提供者の参加を期待することができる。これをここでは広義のＡアプリケーションあるいはシステム登録アプリケーションと呼ぶ。

また、放送番組に連動するタイプのアプリケーションの場合、放送番組は公共性および信頼性が高く、その影響も大きいので、後者の方法によりＡアプリケーションを認定することが好ましいと考えられる。これをここでは狭義のＡアプリケーションあるいは放送局承認アプリケーションと呼ぶ。

【０００８】

放送通信連携型システムにおいては、一例として、デジタル放送で伝送する放送コンテンツに多重化されている放送番組を受信装置のユーザ側で選局することによって、提示中の放送番組に連動して受信装置上で当該アプリケーションを自動起動させるサービスが想定されている。つまり、このサービスでは、狭義のＡアプリケーションあるいは放送局承認アプリケーションについての認証の仕組みが要望されている。この場合、例えば非特許文献２に記載の技術を応用すれば、アプリケーションを自動起動させるサービスを提供することも可能であるが、そのままではセキュリティの対策が不充分となってしまう。

【０００９】

本発明は、以上のような問題点に鑑みてなされたものであり、放送番組に連動するアプリケーションを取得したときに当該アプリケーションは放送局が承認したアプリケーションであるのか検証できる放送通信連携受信装置、および、放送局に承認されたアプリケーションを配信するアプリケーションサーバを提供することを課題とする。

【課題を解決するための手段】

【００１０】

前記課題を解決するために、本発明のうち請求項１に記載の放送通信連携受信装置は、デジタル放送の放送波により送出される放送コンテンツを受信すると共に、前記放送コンテンツ中の放送番組に連動したアプリケーションを配信するアプリケーションサーバから当該受信装置上で動作する前記アプリケーションを通信ネットワークを介して取得する放送通信連携受信装置であって、アプリケーション起動情報記憶手段と、検証鍵記憶手段と、アプリケーション制御手段と、アプリケーション取得手段と、を備え、前記アプリケーション制御手段が、時刻情報検証手段と、電子署名検証手段と、を備えることを特徴とする。

【００１１】

かかる構成によれば、放送通信連携受信装置は、前記アプリケーションを起動させるためのアプリケーション起動情報をアプリケーション起動情報記憶手段に記憶する。ここで、アプリケーション起動情報には、アプリケーションの識別子、アプリケーションの配置場所、アプリケーションの起動を含む状態を示す制御コード等が記載されている。そして、放送通信連携受信装置は、前記アプリケーションサーバにて付加される署名を検証するための検証鍵を検証鍵記憶手段に記憶する。そして、放送通信連携受信装置は、アプリケーション制御手段によって、前記アプリケーション起動情報に記載されたアプリケーションの配置場所に基づいてアプリケーションの取得制御を行うと共に、前記アプリケーション起動情報に記載された動作の状態を示す制御コードにしたがって、前記取得したアプリケーションの状態を制御する。そして、放送通信連携受信装置は、アプリケーション取得手段によって、アプリケーションを要求するためのリクエストを前記配置場所のアプリケーションサーバに対して送信すると共に、前記リクエストの応答として時刻情報と電子署名とが付加された署名付きアプリケーションを受信する。そして、放送通信連携受信装置は、前記アプリケーション制御手段において、時刻情報検証手段によって、現在時刻が前記取得した署名付きアプリケーションに付加された時刻情報で表される期間に合致しているか否かを判別し、現在時刻が前記時刻情報で表される期間に合致している場合、電子署名検証手段によって、前記検証鍵を用いて署名の検証が成功したか否かを判別し、署名の検証が成功した場合、前記取得したアプリケーションを放送局が承認したＡアプリケーションとして、前記制御コードにしたがって当該アプリケーションの状態を制御する。

【００１２】
また、請求項２に記載の放送通信連携受信装置は、請求項１に記載の放送通信連携受信装置において、アプリケーション起動情報抽出手段をさらに備えることとした。
【００１３】
かかる構成によれば、放送通信連携受信装置は、外部からの操作に応じて前記放送コンテンツの中の放送番組を選局して映像および音声を提示するための出力手段に提示しているときに、アプリケーション起動情報抽出手段によって、当該放送コンテンツに多重化された制御信号から当該放送番組に連動したアプリケーションのための前記アプリケーション起動情報を抽出する。これにより、放送通信連携受信装置を利用する視聴者が放送番組をリアルタイムで視聴しているときに、放送通信連携受信装置は、当該放送番組に連動したアプリケーションを認証した上で、アプリケーション起動情報により自動起動させることができる。
【００１４】
また、請求項３に記載の放送通信連携受信装置は、請求項１または請求項２に記載の放送通信連携受信装置において、放送信号解析手段をさらに備えることとした。
【００１５】
かかる構成によれば、放送通信連携受信装置は、放送信号解析手段によって、前記放送コンテンツ中に多重化されている前記検証鍵を抽出して前記検証鍵記憶手段に格納する。これにより、放送通信連携受信装置を利用する視聴者が検証鍵を受信装置に組み込む操作が不要となり、また、放送通信連携受信装置の出荷時に検証鍵を組み込む手間も不要となる。さらに、放送局は、放送番組に連動したアプリケーションを承認した上で、アプリケーションを配信する側の署名を検証するための検証鍵を取得し、この検証鍵を複数の放送通信連携受信装置に対して一斉に送信することができる。
【００１６】
また、請求項４に記載のアプリケーションサーバは、請求項１ないし請求項３のいずれか一項に記載の放送通信連携受信装置に対して、時刻情報を用いて署名鍵を定期的に更新する定期更新方式で生成した署名鍵で署名を付加したアプリケーションを通信ネットワークを介して配信するアプリケーションサーバであって、鍵生成手段と、検証鍵送信手段と、アプリケーション記憶手段と、部分鍵生成手段と、署名鍵更新手段と、署名鍵管理手段と、リクエスト受信手段と、署名生成手段と、アプリケーション送信手段と、を備えることを特徴とする。
【００１７】
かかる構成によれば、アプリケーションサーバは、鍵生成手段によって、マスター鍵を生成すると共に、前記署名を検証する検証鍵を生成し、検証鍵送信手段によって、前記検証鍵を前記通信ネットワークを介して配信する。そして、アプリケーションサーバは、前記放送番組に連動したアプリケーションをアプリケーション記憶手段に記憶する。そして、アプリケーションサーバは、部分鍵生成手段によって、前記署名鍵を更新する更新タイミングにて所定の時刻情報の署名鍵に置き換える際に用いる部分鍵として前記所定の時刻情報の部分鍵を前記マスター鍵に基づいて生成し、記憶部へ格納して保持すると共に前記更新タイミングにて出力する。そして、アプリケーションサーバは、署名鍵更新手段によって、前記部分鍵生成手段から出力された部分鍵を用いて、前記更新タイミングにおいて保持されている署名鍵を更新し、署名鍵管理手段によって、前記更新された署名鍵を記憶部へ格納して保持する処理と当該記憶部から前記署名鍵を読み込んで前記署名鍵更新手段に出力する処理とを行う。ここで署名鍵の定期更新方式としては、例えば、キー・インシュレイテッド（Key-Insulated）署名を用いることができる。そして、アプリケーションサーバは、リクエスト受信手段によって、前記放送通信連携受信装置から前記通信ネットワークを介して前記アプリケーションを要求するためのリクエストを受信する。そして、アプリケーションサーバは、署名生成手段によって、前記リクエストに応じて前記アプリケーション記憶手段から読み出した前記アプリケーションに対して、前記署名鍵管理手段により前記記憶部から読み込まれた、当該アプリケーションを起動させようとする時刻の

時刻情報の署名鍵で電子署名を付加すると共に当該時刻情報を付加し、アプリケーション送信手段によって、前記電子署名および時刻情報が付加された署名付きアプリケーションを前記リクエストの要求元に対して前記通信ネットワークを介して送信する。

【発明の効果】

【００１８】

請求項１に記載の発明によれば、放送通信連携受信装置は、予め検証鍵を取得しておくことで放送番組に連動するアプリケーションの署名を検証することができる。したがって、放送番組に連動するアプリケーションを配信する際に、事前に放送事業者またはシステム管理者による審査を通過したアプリケーションだけをＡアプリケーションであるとした場合、放送通信連携受信装置において、番組に連動して取得したアプリケーションが当該Ａアプリケーションであるか否かを判定することができる。

【００１９】

請求項２に記載の発明によれば、放送通信連携受信装置は、放送番組の選局中に取得したアプリケーション起動情報を用いることができるので、放送番組に連動したアプリケーションの取得、認証、自動起動の一連の処理を、外部からの操作を必要とすることなく実行することができる。

【００２０】

請求項３に記載の発明によれば、放送通信連携受信装置は、放送コンテンツ中に多重化されている検証鍵を利用できるので、検証鍵の受け渡しを容易に行うことができる。

【００２１】

請求項４に記載の発明によれば、アプリケーションサーバは、放送番組に連動したアプリケーションに対して、定期的に更新する署名鍵により電子署名を付加すると共に当該電子署名の時刻情報を付加するので、アプリケーションに対して未来の時刻に対応した署名鍵で署名を付加することで、当該アプリケーションを未来の時刻に起動させることができる。

【図面の簡単な説明】

【００２２】

【図１】本発明の実施形態に係る放送通信連携受信装置を含む放送通信連携型システムの構成の一例を示す図である。

【図２】本発明の実施形態に係る放送通信連携受信装置に表示される放送通信連携用アプリケーションの一例を示す図である。

【図３】本発明の実施形態に係る放送通信連携受信装置にレコメンドサービスが提供されるときの流れの一例を示すシーケンス図である。

【図４】本発明の実施形態に係るアプリケーションサーバの構成例を示すブロック図である。

【図５】本発明の実施形態に係る放送通信連携受信装置の構成例を示すブロック図である。

【図６】本発明の実施形態に係るアプリケーションサーバによる鍵生成処理の流れを示すシーケンス図である。

【図７】本発明の実施形態に係る放送通信連携受信装置によるアプリケーション認証処理の流れを示すシーケンス図である。

【図８】本発明の実施形態に係る放送通信連携受信装置によるアプリケーションの認証および起動の説明図であって、（ａ）は署名鍵の更新方式、（ｂ）は放送番組に連動したアプリケーションをそれぞれ示している。

【発明を実施するための形態】

【００２３】

以下、本発明の放送通信連携受信装置を実施するための形態について、１．放送通信連携型システム、２．放送通信連携受信装置の画面表示例、３．各サーバと放送通信連携受信装置との動作シーケンス例、４．アプリケーションサーバの構成、５．放送通信連携受信装置の構成、６．鍵生成処理、７．アプリケーション認証処理、８．連動アプリケーシ

ョンの起動の具体例の各章に分けて、図面を参照して詳細に説明する。
【００２４】
［１．放送通信連携型システム］
放送通信連携型システム１の構成の概念図を図１に示す。図１に示すように、放送通信連携型システム１は、電波を利用した現行の放送を行う放送局２に加えて、機能的に、放送局サーバ群４と、サービス事業者サーバ群５と、放送通信連携受信装置６と、を備えている。図１では、放送局２、放送局サーバ群４、サービス事業者サーバ群５、および放送通信連携受信装置６を１つずつ図示したが、それぞれが複数であっても構わない。
【００２５】
＜利用者の概要＞
この放送通信連携型システム１の主な利用者は、例えば、放送局（放送事業者）と、サービス事業者と、視聴者である。
放送局は、編成を伴う番組を送出している。放送局は、電波あるいはネットにより番組を視聴者に配信する。放送局は、後記する放送通信連携サービスを充実するために、その番組に関連するメタデータをサービス事業者に提供してもよい。
サービス事業者は、放送通信連携サービスを提供する者であり、団体または個人で構成される。サービス事業者は、サービスを提供するためのコンテンツやアプリケーション（放送通信連携用アプリケーション、以下、単にアプリケーションとも言う）を制作する者、あるいは配信する者である。
視聴者は、放送通信連携受信装置６によって放送番組を視聴し、放送通信連携サービスを享受する者である。以下、ユーザという場合、この視聴者を指す。
【００２６】
＜サービス＞
従来、サービスとは、放送事業者が編成する、スケジュールの一環として放送可能な番組の連続のことを指していた。
放送通信連携サービスは、従来の意味でのサービスの考え方を拡張したものである。
放送通信連携サービスは、見かけ上、ストリーム従属型サービスと、独立型サービスとに分けて考えることができる。
ストリーム従属型サービスは、放送や通信で伝送するＡＶ（Audio Video）ストリームに加え、それに連動して動作する少なくとも１つのアプリケーション（放送通信連携用アプリケーション）により構成される。このストリーム従属型サービスにおいては、通信で伝送するＡＶストリームの選択・再生、あるいは、放送で伝送するＡＶストリームの選局をユーザ側で行うことによって、連動してアプリケーションを起動させることができる。この場合、ユーザによる起動や終了に加え、放送事業者などのＡＶコンテンツの提供者がアプリケーションの自動起動や、終了などのライフサイクルを制御することも可能である。
【００２７】
独立型サービスは、リアルな映像・音声のストリームも含み、少なくとも１つのアプリケーション（放送通信連携用アプリケーション）により構成される。この独立型サービスにおいては、ユーザが選択する操作を行うことで、アプリケーションが起動される。ここで、独立型サービスにおけるアプリケーション（以下、独立アプリケーションという）は、例えば、放送局や視聴者ではない個人等の第三者が放送番組とは無関係に作成したアプリケーションであり、ディスプレイ表示される時計等を含む。
【００２８】
なお、独立型サービスにおいても、放送通信連携受信装置６の電源がオンしているときに、放送通信連携受信装置６が常にバーチャルな映像・音声のストリームを仮想的に受信する仮想チャンネルを備えているものと概念的に捉える場合、放送通信連携サービスは、ストリーム従属型サービスと、独立型サービスとを統合したサービス（この意味において仮想サービスとも言える）であると考えることができる。
【００２９】

＜放送局＞
放送局２は、例えば放送波により放送コンテンツを送出する。放送局２は、放送波に放送通信連携サービスを起動させるための信号を多重化することができる。
本実施形態では、一例として、放送コンテンツの送信側において、データカルーセル方式により伝送される特定モジュールで、アプリケーション起動情報ファイル（以下、ＡＰＬ起動情報ファイルと表記する）を伝送することとした。ＡＰＬ起動情報は、アプリケーションを起動するために必要な情報である。このＡＰＬ起動情報は、例えば、ＡＲＩＢ－Ｊ（ＡＲＩＢ　ＳＴＤ－Ｂ２３：非特許文献２参照）で規定されるＡＩＴ（Application Information Table）をベースにして作成することができる。例えば、「AUTO START」と記載されたＡＰＬ起動情報を受信した放送通信連携受信装置６では、視聴者がアプリケーション起動のための特別な操作をすることなく、アプリケーションを起動させることが可能である。本実施形態のようにＡＰＬ起動情報をファイル化する場合、ＸＭＬ形式によるテキスト表現とすることができる。なお、ＳＩ（Service Information：番組配列情報）のテーブルで伝送する形態とする場合には、ＡＰＬ起動情報はバイナリ表現にすることが可能である。
【００３０】
＜放送局サーバ群＞
放送局（放送事業者）は、放送局サーバ群４とサービス事業者サーバ群５とのうちの放送局サーバ群４、または、両方を構成し、管理運営する。つまり、放送局（放送事業者）は、サービス事業者を兼ねてもよい。
放送局サーバ群４は、図１に示すように、コンテンツ管理サーバ４１と、ユーザ管理サーバ４２と、コンテンツ配信サーバ４３と、放送局サービスサーバ４４と、ＤＢ４５と、ＡＰＩ４６と、を備えている。
【００３１】
コンテンツ管理サーバ４１は、番組とメタデータを管理するものである。このコンテンツ管理サーバ４１の番組管理機能は、既に放送された番組、または、今後放送される番組を管理する機能である。この番組管理だけを専用に行う番組管理サーバを設けるようにしてもよい。
コンテンツ管理サーバ４１のメタデータ管理機能は、番組に関連するメタデータを管理する機能である。このメタデータ管理だけを専用に行うメタデータ管理サーバを設けるようにしてもよい。ここで、メタデータとは、例えば、番組タイトル、番組ＩＤ、番組概要、出演者、放送日時、台本、字幕、解説等を示す。
【００３２】
ユーザ管理サーバ４２は、視聴者のデータを管理するサーバである。このユーザ管理サーバ４２は、インターネット会員サービスを行うためのネットクラブ等の会員となった特定の視聴者のための会員情報サーバ等の特定のサーバで構成してもよいし、コンテンツ管理サーバ４１の管理機能の一部に含めて構成してもよい。
【００３３】
コンテンツ配信サーバ４３は、コンテンツ（例えば番組やメタデータ）を配信するためのサーバである。
放送局サービスサーバ４４は、放送局（放送事業者）がサービス事業者に対してサービスを提供する場合に用いるサーバである。放送局（放送事業者）がサービス事業者に対して提供するサービスは、例えば、放送局が運営するソーシャルネットサービスや、放送番組毎のブログサービス等が挙げられる。
【００３４】
ＤＢ４５は、データ蓄積部であって、放送局が所有しているコンテンツやメタデータを格納する部分と、一般的なデータベースと、から構成される。なお、ＤＢ４５に蓄積されたデータは、管理している事業者（放送事業者）のみがアクセスでき、他者はアクセスできないようになっている。
【００３５】

ＡＰＩ（Application Programming Interface）４６は、サービス事業者サーバ群５からの要求に応じてデータを提供するためのＡＰＩである。このＡＰＩのフオーマットは、放送局とサービス事業者間の合意により予め決定されている。放送局サーバ群４とサービス事業者サーバ群５間の通信は、例えばＲＥＳＴ（Representational State Transfer）形式とすることができる。なお、ＡＰＩ４６は、放送局サーバ群４に含まれる各サーバが共通に備えるものであるが、各サーバが備えるＡＰＩが完全に同一である必要はない。

【００３６】

＜サービス事業者サーバ群＞

サービス事業者は、サービス事業者サーバ群５を構成し、管理運営する。このサービス事業者サーバ群５は、図１に示すように、アプリケーションサーバ５１と、サービスサーバ５２と、コンテンツ配信サーバ５３と、ＤＢ５４と、ＡＰＩ５５と、を備えている。

【００３７】

アプリケーションサーバ５１は、放送通信連携受信装置６上で動作するアプリケーション（以下、受信機アプリケーションともいう）を管理配信するサーバである。

【００３８】

サービスサーバ５２は、前記受信機アプリケーションからの要求によりサービスを提供するためのサーバである。このサービスサーバ５２は、例えば、多言語字幕サーバ、話速変換音声サーバ、ソーシャルＴＶサーバ、レコメンドサーバ、番組レビューサーバ、ブックマークサーバ等を表す。

【００３９】

多言語字幕サーバは、放送通信連携受信装置６に映像音声コンテンツ（以下、ＡＶコンテンツという）が提示されるときに、多言語の中から所望の字幕を選択できるようにメニュー表示するサービスを提供するためのサーバである。

話速変換音声サーバは、放送通信連携受信装置６にＡＶコンテンツが提示されるときに、話し言葉の本来の速度を低速に変換して音声出力するサービスを提供するためのサーバである。

ソーシャルＴＶサーバは、例えばつぶやきのような視聴者投稿を放送通信連携受信装置６の画面にオーバーレイして表示可能なサービスを提供するためのサーバである。

レコメンドサーバは、インターネットで提供される番組ライブラリの中から視聴者にお薦めのＶＯＤ（Video On Demand）番組の情報を、お薦め番組として知らせるサービスを提供するためのサーバである。

番組レビューサーバは番組を実際に視聴した視聴者が書き込んだ講評や感想、レビュー評価点を放送通信連携受信装置６に表示可能なサービスを提供するためのサーバである。

ブックマークサーバは、例えば視聴者にお薦め番組を知らせたときに視聴者がすぐに視聴するのではなく後で視聴できるようにお薦め番組の情報を登録しておくサービスを提供するためのサーバである。

【００４０】

コンテンツ配信サーバ５３は、前記受信機アプリケーションからの要求によりコンテンツを提供するためのサーバである。このコンテンツ配信サーバ５３は、例えば、ＶＯＤ配信サーバ、字幕配信サーバ、マルチビュー配信サーバ等を表す。

ＶＯＤ配信サーバは、例えば視聴者にお薦めのＶＯＤ番組のＡＶコンテンツを配信するためのサーバである。

字幕配信サーバは、放送通信連携受信装置６にＡＶコンテンツが提示されるときに、ＡＶコンテンツにオーバーラップする字幕を配信するためのサーバである。

マルチビュー配信サーバは、放送通信連携受信装置６に提示されるＡＶコンテンツにオーバーラップして表示させるマルチビューのカメラ映像を配信するためのサーバである。なお、マルチビューのカメラ映像については後記する。

【００４１】

ＤＢ５４は、コンテンツ、メタデータ、サービス事業者が作成したデータ、ユーザデータ、アプリケーション等を保存するデータ蓄積部である。なお、ＤＢ５４に蓄積されたデ

ータは、管理しているサービス事業者のみがアクセスでき、他者はアクセスできないようになっている。

【００４２】

ＡＰＩ５５は、前記受信機アプリケーションからの要求により、アプリケーション、コンテンツ、サービスを提供するためのＡＰＩである。なお、ＡＰＩ５５は、前記したＡＰＩ４６とは異なるものであり、サービス事業者サーバ群５に含まれる各サーバがサービス事業者ごとに共通に備えるものである。ただし、サービス事業者毎に、また、サーバによって、ＡＰＩが異なっていてもよいことはもちろんである。

【００４３】

＜放送通信連携受信装置＞

放送通信連携受信装置６は、デジタル放送を受信すると共に当該装置上で動作するアプリケーションを通信ネットワークから取得するものであり、例えば、ＴＶ、セットトップボックス、ＰＣ（Personal computer）、携帯端末等から構成される。放送通信連携受信装置６は、基本機能６１と、放送通信連携用機能６２と、ＡＰＩ６３と、を備える。

【００４４】

基本機能６１は、地上デジタル放送、ＢＳデジタル放送、データ放送等の現行方式の放送を受信し、表示する機能と、インターネットに接続できる機能とを含む。

放送通信連携用機能６２は、ＡＰＩ６３に基づき動作する。つまり、放送通信連携受信装置６の中にアプリケーション実行環境としてインストールされているＯＳ（Operating System）が、予め定められたＡＰＩ６３を実行することで、放送通信連携用機能６２を実現する。この放送通信連携用機能６２は、放送通信連携用基本機能と、オプション機能とを含む。

放送通信連携用基本機能は、放送通信連携サービスを実現するために必要な機能である。放送通信連携用基本機能は、例えば、アプリケーション制御機能、描画機能、同期制御機能、セキュリティ機能等を含む。

【００４５】

アプリケーション制御機能は、アプリケーションの起動や終了といったライフサイクルを制御するアプリケーションマネージャーとしての機能を示す。

描画機能は、ＡＶコンテンツを提示している放送通信連携受信装置６の画面の所定位置にアプリケーションを描画する機能を示す。

同期制御機能は、放送によりリアルタイムに受信したＡＶコンテンツの提示時刻と、通信ネットワークＮを経由して取得したアプリケーションやコンテンツとの提示時刻とを同期させる制御を行う機能を示す。つまり、同期制御機能は、放送ストリームとして入力するデータのタイムスタンプと、通信ストリームとして入力するデータのタイムスタンプとを比較し、放送ストリームの所定のポイントと、通信ストリームの対応するポイントとを合わせる制御を行う。

【００４６】

セキュリティ機能は、例えば放送番組に連動するアプリケーションにおいて、事前に放送事業者またはシステム管理者による審査を通過したアプリケーションだけをＡアプリケーションであるとした場合、当該Ａアプリケーションを認証するものである。

【００４７】

オプション機能は、必要に応じて実装するものであり、例えば携帯端末連携サービスを実現するための機能等を挙げることができる。

携帯端末連携サービスには、例えば、番組お薦めサービス等のために、携帯端末と据え置き型のテレビを連携させることで視聴者個人がＡＳＰ（Application Service Provider）等にログインする手続きを簡素化するサービスを含む。

【００４８】

アプリケーション６４は、例えばアプリケーションサーバ５１から放送通信連携受信装置６にダウンロードされ、ＡＰＩ６３を通して放送通信連携用機能６２を利用する。すべてのアプリケーション６４はＡＰＩ６３を介さずに放送通信連携受信装置６固有の機能に

アクセスすることはできない。
【００４９】
ＡＰＩ６３は、放送通信連携受信装置６に依存することなくアプリケーション６４の動作が同じになるように予め規定されたものであり、各放送通信連携受信装置６に共通のＡＰＩである。以下に、放送通信連携受信装置６がＡＰＩ６３として、例えばＡＲＩＢ－Ｊに規定されたＡＰＩ以外に用いるＡＰＩの一例を挙げる。
【００５０】
（１）getRunningApplications()：実行中のアプリケーションの情報を取得する
戻り値：
apps[]:　　実行中アプリケーションのリスト
（以下アプリケーションごと）
application_id:　アプリケーションＩＤ（一般アプリケーションの場合はｎｕｌｌ）
running_level:　実行レベル（認証結果およびユーザ設定の状態）
（２）queryApplicationInfo()：指定したアプリケーションの情報を取得する
（３）saveApplicationToCache()：サーバ上のアプリケーションをキャッシュに保存する
（４）queryApplicationInCache()：キャッシュ中のアプリケーションを検索する
引数：
application_id:　　認証機関から発行されたアプリケーションＩＤ
（５）getCurrentSTC()：現在のSTC値を取得する
（６）getCurrentPositionInProgram()：番組開始からの経過時間を取得する
（７）delayStreamPresentation()：提示中の放送ストリームの遅延提示を開始する
（８）getCurrentDelay()：提示中の放送ストリームの（本来の提示時刻からの）遅延時間量を取得する
【００５１】
［２．放送通信連携受信装置の画面表示例］
ここでは、図２に示す画面表示例を通して、放送通信連携サービスと、アプリケーションと、コンテンツとの関係の一例や、放送通信連携受信装置６における放送通信連携用機能６２の一例について説明する。図２は、本発明の実施形態に係る放送通信連携受信装置に表示されるアプリケーションの一例を示す図である。図２（ａ）に示すように、視聴者が放送通信連携受信装置６にてＡＶコンテンツ（デジタル放送番組）１００を視聴しているときに、例えばリモコン操作を行うことによって、放送通信連携サービスにおけるメインメニュー１０１が画面に表示される。
【００５２】
この例では、画面の下方に横長のツールバー形状に表示されたメインメニュー１０１に、字幕１０２と、コメント１０３と、レコメンド１０４と、ブックマーク１０５と、が表示されている。
字幕１０２は、多言語の中から所望の字幕を選択できるようにメニュー表示するサービスを選択するためのボタンである。
コメント１０３は、例えばつぶやきやコメントを投稿するサービスを選択するためのボタンである。
レコメンド１０４は、お薦めのＶＯＤ番組の情報を表示するサービスを選択するためのボタンである。
ブックマーク１０５は、お薦め番組をすぐに視聴するのではなく後で視聴できるようにお薦め番組の情報を登録しておくサービスを選択するためのボタンである。
【００５３】
図２（ａ）に表示されたメインメニュー１０１を横スクロールすることで、上記各サービス以外のその他のサービスを選択することが可能である。その他のサービスとして、例えばマルチビューサービスを挙げることができる。マルチビューサービスでは、放送通信連携受信装置６にＡＶコンテンツが提示されるときに、当該ＡＶコンテンツ中の被写体を別々の位置にそれぞれ配置された複数のカメラで撮影した複数のカメラ映像の中から視聴

者が選択したカメラ映像を、マルチビューのカメラ映像として配信し、ＡＶコンテンツにオーバーラップして表示させる。

【００５４】

図２（ａ）に表示されたメインメニュー１０１を横スクロールすることで、マルチビューサービスが選択されたときの画面表示例を図２（ｂ）に示す。ここでは、１つのマルチビューサービスは、メインメニュー１０１上の図示しないマルチビューボタン（アプリケーション）と、マルチビューワの選択肢データである静止画像１０６，１０７，１０８と、マルチビューワの動画１０９（図２（ｃ）参照）とを備えている。このうち、静止画像と、動画コンテンツとは、コンテンツ配信サーバ５３としてのマルチビュー配信サーバから配信される。

【００５５】

図２（ｂ）に示す例では、ＡＶコンテンツ１００がサッカーの試合において攻撃側から見たサッカーゴール周辺の様子を表している。また、静止画像１０６は観客席の攻撃側サポータの様子、静止画像１０７は攻撃側チームの監督の様子、静止画像１０８はゴールキーパの正面の様子をそれぞれ示している。ここで、視聴者が例えば静止画像１０８を選択した場合、図２（ｃ）に示すように、該当するゴールキーパの正面の映像が、ＡＶコンテンツ１００の全表示画面のうちの一部にオーバーラップして表示されながら、ＡＶコンテンツ１００と同期した動画１０９となって再生される。

【００５６】

なお、ゴールキーパの正面の映像と、攻撃側から見たサッカーゴール周辺の映像（ＡＶコンテンツ１００）との同期は、放送通信連携受信装置６の放送通信連携用機能６２によるものである。詳細には放送通信連携用機能６２の放送通信連携用基本機能としての同期制御機能によるものである。放送通信連携受信装置６上で動作するアプリケーションは、ＡＰＩとして例えばgetCurrentSTC()やdelayStreamPresentation()を呼び出すことで、放送通信連携用機能６２（図１参照）を利用することができる。

【００５７】

［３．各サーバと放送通信連携受信装置との動作シーケンス例］

ここでは、図３に示す動作シーケンス例を通して、放送通信連携サービスと、アプリケーションと、コンテンツとの関係の一例や、放送通信連携受信装置６における放送通信連携用機能６２の一例について説明する。図３は、本発明の実施形態に係る放送通信連携受信装置にレコメンドサービスが提供されるときの流れの一例を示すシーケンス図である。

【００５８】

図２（ａ）に表示されたメインメニュー１０１から視聴者によってレコメンド１０４が選択された場合、図示は省略するが、レコメンドの種類として、例えば、「今視聴している番組に関連したお薦め番組」、「貴方へのお薦め番組」、「ネットで話題の番組」、「ネットで好評な番組」、といった項目が表示され、項目毎にスクロールすることにより該当する番組の情報が選択可能に表示される。この状態で、視聴者が、例えば、「今視聴している番組に関連したお薦め番組」を選択した場合、放送通信連携受信装置６は、サービス事業者サーバ群５に対して、お薦め番組の要求を行う（Ｓ１）。

【００５９】

そして、サービス事業者サーバ群５は、放送局サーバ群４のインターフェース部（ＡＰＩ４６：図１参照）に対して、視聴者が「今視聴している番組に関連したお薦め番組」の要求を行う（Ｓ２）。そして、放送局サーバ群４は、該当の推薦番組（お薦め番組）等をサービス事業者サーバ群５に送信する（Ｓ３）。そして、サービス事業者サーバ群５は、要求されたデータ（お薦め番組）等を放送通信連携受信装置６に送信する（Ｓ５）。なお、サービス事業者サーバ群５は、要求されたデータ（お薦め番組）に連動するアプリケーション（連動アプリケーション）がある場合には必要に応じて放送通信連携受信装置６に送信することもできる（Ｓ４）。

【００６０】

以上の流れは一例であって、前記した順序で動作することに限定されるものではない。

また、放送通信連携受信装置６とサービス事業者サーバ群５との間でだけやりとりをする場合もある。例えば、サービス事業者サーバ群５において、必要なコンテンツを予め放送局サーバ群４から取得しておいてもよい。

【００６１】

また、例えば、放送通信連携受信装置６がアプリケーションの実行時にその都度アプリケーションを通信から取得する場合（オンザフライで取得する場合）、受信する放送波に多重化された情報をもとにして、アプリケーションサーバ５１等のサービス事業者サーバ群５にアプリケーションの要求を行う（Ｓ１）。そして、サービス事業者サーバ群５において、アプリケーションサーバ５１は、放送通信連携受信装置６からの要求により、アプリケーションの保存場所を放送通信連携受信装置６に知らせるとともに、アプリケーションを送信する（Ｓ４）。そして、放送通信連携受信装置６は、アプリケーションがダウンロードされたら、アプリケーションを起動・実行して、コンテンツ配信サーバ５３等のサービス事業者サーバ群５にコンテンツを要求し（Ｓ１）、コンテンツを取得する（Ｓ５）。

【００６２】

［４．アプリケーションサーバの構成］

ここでは、アプリケーションサーバ５１の構成例について図４を参照（適宜図１参照）して説明する。図４は、本発明の実施形態に係るアプリケーションサーバ５１の構成例を示すブロック図である。アプリケーションサーバ５１は、放送通信連携受信装置６に対して通信ネットワークＮを介してアプリケーションを配信するものである。

【００６３】

まず、アプリケーションサーバ５１についてのいくつかの前提を述べる。

以下では、アプリケーションサーバ５１は、放送コンテンツ中の放送番組に連動したアプリケーション（連動アプリケーション）に署名を付加して配信するものとして説明する。つまり、放送通信連携受信装置６は、デジタル放送の放送波により送出される放送コンテンツを受信すると共に、アプリケーションサーバ５１から当該放送通信連携受信装置６上で動作するアプリケーションを通信ネットワークＮを介して取得する。

【００６４】

また、アプリケーションサーバ５１は、時刻情報を用いて署名鍵を定期的に更新する定期更新方式で署名鍵を生成する。そして、アプリケーションサーバ５１は、署名鍵の定期更新方式として、例えば、キー・インシュレイテッド（Key-Insulated）署名を用いることとする。このキー・インシュレイテッド署名については、「Y. Dodis, J. Katz, S. Xu, and M. Yung: “Strong Key-Insulated Signature Schemes”, Proc. of PKC’03, 2003, p.130-144」に記載されている。

【００６５】

ここで、署名鍵の更新の概略について図８（ａ）を参照して説明する。

図８（ａ）に示す時刻１１０において、t_0が現在の時刻を表すとすると、t_1，t_2，t_3…は未来の時刻を示し、t_{-1}，t_{-2}…は過去の時刻を示す。なお、t_{-2}，t_{-1}，t_0，t_1，t_2，t_3…の時間間隔は、等間隔である必要はない。図８（ａ）では、各時刻で規定される期間を時刻情報１２０と呼ぶことにする。

【００６６】

時刻情報１２０において、例えば、現在時刻t_0に始まって時刻t_1に終わる期間を時刻情報Ｔと表記する。

また、未来の時刻t_1に始まって時刻t_2に終わる期間を時刻情報Ｔ＋１とする。未来の時刻に関して以下同様に表記する。

また、過去の時刻t_{T-1}に始まって現在時刻t_0に終わる期間を時刻情報Ｔ－１とする。過去の時刻に関して以下同様に表記する。なお、ここでは、ある時刻情報の終了時刻と次の時刻情報の開始時刻が一致しているとする。

【００６７】

時刻情報１２０に対応した期間だけ有効な署名鍵１３０と、その期間に生成される部分

鍵１４０との一覧を、時刻１１０および時刻情報１２０に対応させて図８（ａ）に表示した。例えば、時刻情報Ｔの期間に有効な署名鍵はSK_Tであり、この期間のいずれかのタイミングにて生成される部分鍵はΔSK_{T+1}である。そして、現在の署名鍵SK_Tに対して部分鍵ΔSK_{T+1}を用いることで、未来の時刻情報Ｔ＋１の期間の署名鍵SK_{T+1}を生成することができる。つまり、署名鍵SK_Tは、部分鍵ΔSK_{T+1}を用いて更新されて、署名鍵SK_{T+1}となる。未来および過去の時刻に関して以下同様に表記する。

【００６８】

署名鍵SK_Tは、時刻情報Ｔの期間だけ有効である。つまり、署名鍵SK_Tは、時刻t_0から時刻t_1まで有効であるが、まだ時刻t_0になっていないときや、時刻t_1を過ぎているときには、無効となる。なお、署名を検証する側では、時刻に関わらず同じ検証鍵を用いて電子署名を検証することができる。

【００６９】

図８（ａ）の表記において、時刻t_0から時刻t_1までの時刻情報Ｔの表記をあらためてT_0と表記することにすると、期間（時刻情報）の開始時刻の添字と、期間の添字とは同じものとなるので、時刻ｔという場合に、時刻情報Ｔを表すものと取り決めておけば、期間を開始時刻で特定することが可能である。さらに、この取り決めにおいて小文字と大文字とを統一すれば、時刻情報Ｔ（期間Ｔ）と時刻Ｔとは同じことを意味する。

【００７０】

そこで、本実施形態のアプリケーションサーバ５１の説明では、簡便のため、時刻情報Ｔの署名鍵のことを、時刻Ｔの署名鍵と呼ぶことにする。この時刻Ｔは、アプリケーションサーバ５１において時刻Ｔの署名鍵（SK_T）の管理を行う基準となる時刻を数値化したものであればよい。また、時刻Ｔとして例えば「年月日時分秒」を数値化したものを用いることができる。一例として、時刻Ｔという場合に、開始時刻Ｔから始まる期間とし、図８（ａ）に示した署名更新タイミングt_{-2}，t_{-1}，t_0，t_1，t_2，t_3…の時間間隔が等間隔であり、その期間が放送番組の番組尺に合わせて例えば３０分であるものとして説明する。

【００７１】

図４に戻って、アプリケーションサーバ５１の構成について説明する。図４においては、時間軸に沿った説明よりもアプリケーションサーバ５１を構成する構成要素の互いの関係を重視し、説明の中心となっている構成要素における或る時刻を統一的に時刻Ｔとして表記した。ただし、図４において、説明の中心となっている構成要素だけに着目したときには、時刻Ｔという表記が、図８（ａ）と同様に期間（時刻情報）を表している。

【００７２】

アプリケーションサーバ５１は、図４に示すように、鍵生成手段５１１と、部分鍵生成手段５１２と、署名鍵更新手段５１３と、署名鍵管理手段５１４と、署名生成手段５１５と、アプリケーション記憶手段５１６と、検証鍵送信手段５１７と、リクエスト受信手段５１８と、アプリケーション送信手段５１９と、を備えている。

【００７３】

鍵生成手段５１１は、マスター鍵を生成すると共に、プロバイダ（サービス事業者）の署名を検証する検証鍵を生成するものである。

鍵生成手段５１１は、マスター鍵を部分鍵生成手段５１２に出力し、検証鍵を検証鍵送信手段５１７に出力する。ここで、検証鍵は、アプリケーション認証としてのプロバイダ認証（署名検証）に必要な鍵であり、視聴者に通知される。本実施形態では、検証鍵を、アプリケーションサーバ５１から放送局２を介して放送通信連携受信装置６に通知することとした。

【００７４】

ここで、生成されたマスター鍵および検証鍵は、アプリケーションサーバ５１の内部の記憶部に格納される。図４において、記憶されているマスター鍵および検証鍵をマスター鍵K_Mおよび検証鍵K_Pと表記する。なお、マスター鍵K_Mを記憶する記憶部は、耐タンパ性に優れた記憶手段とし、検証鍵K_Pを記憶する記憶部は、メモリ等の一般的な記憶手

段とする。

【００７５】

部分鍵生成手段５１２は、署名鍵を更新する際に用いる部分鍵を生成するものである。部分鍵生成手段５１２は、署名鍵（例えば図８（ａ）のSK_{T-1}）を更新する更新タイミング（例えば図８（ａ）のt_0）にて所定の時刻Ｔの署名鍵（例えば図８（ａ）のSK_T）に置き換える際に用いる部分鍵として前記所定の時刻Ｔの部分鍵（例えば図８（ａ）のΔSK_T）をマスター鍵に基づいて生成し、記憶部へ格納して保持すると共に前記更新タイミング（例えば図８（ａ）のt_0）に出力するものである。部分鍵生成手段５１２は、入力されたマスター鍵K_Mと時刻Ｔとにより部分鍵ΔSK_Tを生成する。

【００７６】

本実施形態では、部分鍵生成手段５１２は、部分鍵を生成して保持しておき、署名鍵の更新タイミングとなったか否かを判別し、更新タイミングとなった場合、部分鍵を署名鍵更新手段５１３に出力する。更新タイミングを表す時刻についての情報は、例えばクロックから取得される。署名鍵更新手段５１３が１２：３０の時点で１３：００～１３：３０（時刻情報１３時）に有効な署名鍵を生成する場合、部分鍵生成手段５１２は、この時刻情報１３時の部分鍵を１２：３０よりも前の所定のタイミングで生成して保持しておく。ここで、生成された部分鍵は、アプリケーションサーバ５１の内部の記憶部に格納される。なお、部分鍵を記憶する記憶部は、メモリ等の一般的な記憶手段とする。図４において、記憶された部分鍵を部分鍵ΔSK_Tと表記する。

【００７７】

署名鍵更新手段５１３は、署名鍵を更新するものである。この署名鍵更新手段５１３は、部分鍵生成手段５１２から出力された部分鍵を用いて、更新タイミングにおいて署名鍵管理手段５１４により記憶部に保持されている署名鍵を更新する。また、署名鍵更新手段５１３は、公知のキー・インシュレイテッド署名を用いて署名鍵を更新する。署名鍵更新手段５１３は、例えば３０分毎に署名鍵を更新する。

【００７８】

署名鍵管理手段５１４は、署名鍵を管理するものである。ここで管理する署名鍵は、署名鍵更新手段５１３で更新（生成）された署名鍵である。また、署名鍵の管理とは、署名鍵を記憶し、必要に応じて出力することを意味する。すなわち、この署名鍵管理手段５１４は、更新された署名鍵を記憶部へ格納して保持する処理と当該記憶部から前記署名鍵を読み込んで署名鍵更新手段５１３に出力する処理とを行う。署名鍵管理手段５１４は、例えば３０分毎に、更新された署名鍵を記憶部に格納し、この格納タイミングからずれたタイミングで、例えば３０分毎に読み出した署名鍵を署名鍵更新手段５１３に出力する。

【００７９】

ここで、署名鍵は、アプリケーションサーバ５１の内部の記憶部に格納される。この署名鍵を記憶する記憶部は、メモリ等の一般的な記憶手段とする。図４において、記憶された署名鍵をSK_Tと表記した。ただし、図４では、署名鍵管理手段５１４が記憶部から読み込んで署名鍵更新手段５１３に出力する署名鍵については、署名鍵SK_{T-1}と表記した。これは、署名鍵更新手段５１３を説明の中心として着目したときに、署名鍵更新手段５１３がこの署名鍵SK_{T-1}を更新することで、時刻Ｔの署名鍵SK_Tを生成することを表している。

【００８０】

また、署名鍵管理手段５１４が記憶部から読み込んで署名生成手段５１５に出力する署名鍵については、署名鍵SK_Tと表記した。これは、署名生成手段５１５を説明の中心として着目したときに、署名生成手段５１５がこの署名鍵SK_Tを用いて署名を付加することを表している。

【００８１】

署名生成手段５１５は、アプリケーションに電子署名とその時刻情報を付加するものである。この署名生成手段５１５は、リクエストに応じてアプリケーション記憶手段５１６から読み出したアプリケーションに対して、署名鍵管理手段５１４により記憶部から読み

込まれた、当該アプリケーションを起動させようとする時刻Ｔの署名鍵で電子署名を付加すると共に当該時刻Ｔを付加する。ここで、例えば、当該アプリケーションを１３：００に起動させたい場合、署名生成手段５１５は、１３：００～１３：３０（時刻情報１３時）に有効な署名鍵を、その起動時刻よりも前の時点で付加することができる。

【００８２】

アプリケーション記憶手段５１６は、放送番組に連動したアプリケーションを記憶するものであって、例えば一般的なハードディスク等から構成される。本実施形態では、アプリケーションが連動する放送番組を放送する放送局２は、アプリケーションサーバ５１が生成した検証鍵K_Pを、当該アプリケーションが配信される前に取得し、保有していることとした。

【００８３】

検証鍵送信手段５１７は、鍵生成手段５１１によって生成された検証鍵K_Pを通信ネットワークＮを介して配信するものである。この検証鍵送信手段５１７は、所定の通信インターフェースから構成される。配信方法は任意であるが、本実施形態では、一例として、図４に示すように、検証鍵送信手段５１７は、検証鍵K_Pを通信ネットワークＮを介して放送局サービスサーバ４４に送信し、放送局サービスサーバ４４を中継して放送局２に通知することとした。このとき、一例として、放送局サービスサーバ４４は、放送局２との間の専用線Ｌを介して検証鍵K_Pを放送局２に送信することとした。なお、オフライン（例えば郵送等）にて放送局２に通知しても構わない。

【００８４】

また、本実施形態では、検証鍵K_Pを放送通信連携受信装置６に渡すために、放送局２が、ＡＶコンテンツを送信する放送波Ｗに多重化する制御信号の中に、アプリケーションサーバ５１から取得した検証鍵K_Pを含めることとした。

【００８５】

リクエスト受信手段５１８は、放送通信連携受信装置６から通信ネットワークＮを介してアプリケーションを要求するためのリクエストを受信するものである。このリクエスト受信手段５１８は、所定の通信インターフェースから構成される。ここで受信したリクエストは、署名生成手段５１５に出力される。

【００８６】

アプリケーション送信手段５１９は、署名生成手段５１５によって電子署名および時刻Ｔが付加された署名付きアプリケーションを、リクエストの要求元に対して通信ネットワークＮを介して送信するものである。このリクエスト受信手段５１８は、所定の通信インターフェースから構成される。

【００８７】

［５．放送通信連携受信装置の構成］

放送通信連携受信装置６は、チューナのほか、例えば、ＣＰＵ（Central Processing Unit）等の演算装置と、メモリやハードディスク等の記憶装置と、外部との間で各種情報の送受信を行うインターフェース装置とを備え、図５に示すように、放送受信手段６０１と、放送信号解析手段６０２と、映像音声復号手段６０３と、データ放送復号手段６０４と、ＡＰＬ起動情報記憶手段６０５と、通信送受信手段６０６と、ＡＰＬ起動情報取得手段６０７と、リスト制御手段６０８と、アプリケーション制御手段６０９と、アプリケーション蓄積手段６１０と、アプリケーション取得手段６１１と、アプリケーションキャッシュ６１２と、アプリケーション実行手段６１３と、合成表示手段６１４と、検証鍵記憶手段６１５と、リソース管理手段６１６と、リソースアクセス制御手段６１７と、を備えている。

【００８８】

ここで、各手段６０１～６１７を、図１に示す放送通信連携受信装置６の基本機能６１と、放送通信連携用機能６２とのいずれか一方にだけ分類するとしたら、例えば、基本機能６１が、放送受信手段６０１と、放送信号解析手段６０２と、映像音声復号手段６０３と、データ放送復号手段６０４と、通信送受信手段６０６と、を備え、放送通信連携用機

能６２が、ＡＰＬ起動情報記憶手段６０５と、ＡＰＬ起動情報取得手段６０７と、リスト制御手段６０８と、アプリケーション制御手段６０９と、アプリケーション蓄積手段６１０と、アプリケーション取得手段６１１と、アプリケーションキャッシュ６１２と、アプリケーション実行手段６１３と、合成表示手段６１４と、検証鍵記憶手段６１５と、リソース管理手段６１６と、リソースアクセス制御手段６１７と、を備える。ただし、これは一例であって、単純に分離できるものではない。

【００８９】

放送受信手段６０１は、放送波により送信されるデジタル放送の放送コンテンツ（番組データ）を放送ストリームとしてアンテナＡＴＮを介して受信するものであって、一般的なデジタル放送用チューナである。この放送受信手段６０１は、受信・復調した放送コンテンツを放送信号解析手段６０２に出力する。

【００９０】

放送信号解析手段６０２は、放送受信手段６０１で受信した放送コンテンツに多重化されている、映像音声ストリームと、ＳＩ（番組配列情報）と、データ放送コンテンツとを分離し、このうち映像音声ストリームを映像音声復号手段６０３に出力すると共に、データ放送コンテンツをデータ放送復号手段６０４に出力する。ここで、ＳＩは図示しない番組表生成手段により番組表に加工され、例えばユーザがリモコン等からなる操作入力手段６２０を操作したときに、合成表示手段６１４を介して、出力手段６３０に提示される。なお、放送信号解析手段６０２は、操作入力手段６２０からのチャンネル切替指示により提示するチャンネルを切り替えることができる。また、出力手段６３０は、映像および音声を提示するものであって、例えば液晶ディスプレイ等の表示モニタやスピーカ等からなる。

【００９１】

また、本実施形態では、放送信号解析手段６０２は、放送コンテンツ中に多重化されている検証鍵を抽出して検証鍵記憶手段６１５に格納することとした。ここで、検証鍵が、例えば共通情報であるＥＣＭ（Entitlement Control Message）にて伝送されている場合、放送信号解析手段６０２は、ＥＣＭから検証鍵を抽出する。

【００９２】

映像音声復号手段６０３は、放送信号解析手段６０２で分離された映像音声ストリームを復号するものである。この映像音声復号手段６０３は、映像・音声が例えば、ＭＰＥＧ２の符号化方式によって符号化されている場合は、ＭＰＥＧ２の復号を行い表示可能な出力形式の映像・音声データとして、合成表示手段６１４へ出力する。

【００９３】

データ放送復号手段６０４は、放送信号解析手段６０２で分離されたデータ放送コンテンツを復号するものであって、データ放送のデータカルーセル方式により伝送されるモジュールからファイルを抽出する機能と、データ放送コンテンツを閲覧するためのＢＭＬブラウザ機能とを備えている。データ放送復号手段６０４は、復号したデータ放送コンテンツを合成表示手段６１４へ出力する。

【００９４】

また、本実施形態では、データ放送復号手段６０４は、データカルーセル方式により伝送される特定モジュールから、アプリケーションを起動させるためのＡＰＬ起動情報（アプリケーション起動情報）ファイルを抽出し、ＡＰＬ起動情報記憶手段６０５に格納することとした。この意味で、本実施形態では、データ放送復号手段６０４は、アプリケーション起動情報抽出手段として機能する。すなわち、放送通信連携受信装置６は、外部からの操作に応じて放送コンテンツの中の放送番組を選局して出力手段６３０に提示しているときに、データ放送復号手段６０４が、当該放送ストリームに多重化された制御信号から当該放送番組に連動したアプリケーションのためのＡＰＬ起動情報を抽出してＡＰＬ起動情報記憶手段６０５に格納する。もちろん、アプリケーション起動情報抽出手段を別に設けてもよいし、他の手段が兼ねるようにしてもよい。また、データ放送復号手段６０４は、ＡＰＬ起動情報ファイルが更新された場合、その旨をアプリケーション制御手段６０９

に通知する。

【００９５】

ＡＰＬ起動情報記憶手段（アプリケーション起動情報記憶手段）６０５は、ＡＰＬ起動情報を記憶するものであって、例えばＲＡＭ（Random Access Memory）やＲＯＭ（Read Only Memory）等の一般的なメモリやハードディスク等の記憶装置から構成される。ここで、ＡＰＬ起動情報は、アプリケーションを当該放送通信連携受信装置６上で起動させるための情報であって、例えば、アプリケーションの識別子（ＩＤ）、アプリケーションの配置場所（ＵＲＬ等の所在アドレス）等のアプリケーションを特定するための情報、ならびに、当該アプリケーションを制御するための付加的な情報である。このＡＰＬ起動情報は、データ放送復号手段６０４により抽出されたものか、または、ＡＰＬ起動情報取得手段６０７により取得されたものである。

【００９６】

また、本実施形態では、ＡＰＬ起動情報記憶手段６０５は、放送通信連携受信装置６上で起動中のアプリケーションの識別情報の一覧（起動アプリケーション識別情報）も記憶することとした。この起動アプリケーション識別情報は、アプリケーション制御手段６０９が作成する。

【００９７】

通信送受信手段６０６は、通信ネットワークＮを介して、例えばサービス事業者サーバ群５との間で通信データを送受信するものであって、例えば、通信制御ボードである。

【００９８】

ＡＰＬ起動情報取得手段６０７は、ＡＰＬ起動情報を、通信送受信手段６０６および通信ネットワークＮを介して、既知のＵＲＬから取得し、ＡＰＬ起動情報記憶手段６０５に格納するものである。本実施形態では、ＡＰＬ起動情報取得手段６０７は、ユーザがアプリケーションを選択する操作を行った場合に、当該アプリケーションについてのＡＰＬ起動情報を、通信送受信手段６０６および通信ネットワークＮを介して、既知のＵＲＬから取得し、ＡＰＬ起動情報記憶手段６０５に格納することとした。

【００９９】

また、ＡＰＬ起動情報取得手段６０７は、アプリケーション取得手段６１１からＡＰＬ起動情報書き換え指示を受けた場合、後記するように、ＡＰＬ起動情報記憶手段６０５に記憶されている該当するＡＰＬ起動情報（外部からの操作に応じたアプリケーションに関するＡＰＬ起動情報）に記載された所在アドレス（ＵＲＬ）を放送通信連携受信装置６内部のアプリケーション蓄積手段６１０におけるメモリアドレスに書き換える。この意味で、本実施形態では、ＡＰＬ起動情報取得手段６０７は、所在アドレス書換手段として機能する。もちろん、所在アドレス書換手段を別に設けてもよいし、他の手段が兼ねるようにしてもよい。なお、アプリケーション蓄積手段６１０は、ハードディスク等のディスク装置を示す。

【０１００】

リスト制御手段６０８は、ＡＰＬ起動情報記憶手段６０５に格納されているＡＰＬ起動情報に基づいて、放送通信連携受信装置６にて利用可能なアプリケーションの一覧をアプリケーション一覧リスト（以下、単にリストという）として作成し、合成表示手段６１４へ出力する。このリスト制御手段６０８は、例えばレジデントアプリケーションのローンチャーにより実現することができる。なお、リスト制御手段６０８は、操作入力手段６２０からのリスト表示・選択指示により提示するリストを表示し、その選択操作を受け付けることができる。ここで、放送通信連携受信装置６上で動作するアプリケーションは、ＡＰＩとして例えばgetRunningApplicationsを呼び出すことで、リスト制御手段６０８の機能（放送通信連携用機能６２：図１参照）を利用することができる。

【０１０１】

なお、ローンチャーは、通信で取得する放送通信連携用アプリケーションではない。このローンチャーは、例えば出荷時等において、アプリケーション蓄積手段６１０等に予めインストールしておいてもよい。また、本実施形態では、リスト制御手段６０８は、放送

通信連携受信装置６にて利用可能なアプリケーションのうち、バックグランド処理を行っているアプリケーションについてはリストから除外することとした。

【０１０２】

アプリケーション制御手段６０９は、アプリケーションの起動や終了などのライフサイクルを制御するアプリケーションマネージャー機能と、アプリケーションの認証処理を行うセキュアマネージャー機能を備えている。

アプリケーション制御手段６０９において、アプリケーションマネージャー機能は、例えば、ＡＰＬ起動情報に記載されたアプリケーションの配置場所に基づいてアプリケーションの取得制御を行うと共に、ＡＰＬ起動情報に記載された動作の状態を示す制御コードにしたがって、取得したアプリケーションの状態を制御する。ここで、動作の状態とは、例えばアプリケーションの自動起動（制御コード「AUTO START」）、スタンバイ（制御コード「PRESENT」）、終了（制御コード「DESTROY」）、強制終了（制御コード「KILL」または「KILL ALL」）等を示す。

このために、アプリケーション制御手段６０９は、起動制御手段７１０と、終了制御手段７２０と、蓄積管理手段７３０とを備えている。なお、本実施形態では、起動制御手段７１０に、セキュアマネージャー機能を具備することとした。

【０１０３】

起動制御手段７１０は、アプリケーションの起動を制御するものである。

起動制御手段７１０におけるアプリケーションマネージャー機能は、以下の通りである。起動制御手段７１０は、起動させようとするアプリケーションが、デジタル放送の番組に連動した連動アプリケーションであって、そのＡＰＬ起動情報に「AUTO START」の制御コードが記載されている場合、メモリにロードされているアプリケーションを起動し、スタートさせる。起動制御手段７１０は、起動させようとするアプリケーションのＡＰＬ起動情報に「AUTO START」の制御コードが記載されていない場合、ユーザの操作にしたがって、アプリケーションを起動させる。起動制御手段７１０は、ＡＰＬ起動情報に「PRESENT」の制御コードが記載されている場合、アプリケーションが起動前であればメモリにロードされている状態（スタンバイ）を維持し、アプリケーションが動作中であれば一時停止させ、メモリにロードされている状態（スタンバイ）とする。

【０１０４】

本実施形態では、起動制御手段７１０は、アプリケーションマネージャー機能よりも優先するセキュアマネージャー機能として、時刻情報検証手段７１１と、電子署名検証手段７１２と、を備えることとした。

【０１０５】

時刻情報検証手段７１１は、現在時刻が取得した署名付きアプリケーションに付加された時刻Ｔで表される期間に合致しているか否かを判別するものである。ここで、現在時刻が時刻Ｔで表される期間に合致するとは、現在時刻が、時刻Ｔで表される期間に含まれていることを意味する。本実施形態では、時刻Ｔという場合に、開始時刻Ｔから始まる期間とし、アプリケーションサーバ５１にて例えば１２：３０の時点で１３：００～１３：３０（時刻情報１３時）に有効な署名鍵を生成していれば、時刻Ｔが１３：００～１３：３０（時刻情報１３時）を示すことになる。そのため、現在時刻が１３：０５ならば、現在時刻が時刻Ｔで表される期間に合致することになる。一方、現在時刻が１２：５５や１３：３５ならば、現在時刻が時刻Ｔで表される期間に合致しないことになる。

時刻情報検証手段７１１は、現在時刻が時刻情報Ｔに合致している場合、その旨を電子署名検証手段７１２に通知する。

【０１０６】

また、時刻情報検証手段７１１において、現在時刻が時刻情報Ｔに合致していないと判別され、時刻情報Ｔが未来を示すならば、時刻情報検証手段７１１は、所定の時間後に判別を実行する。時刻情報Ｔが過去を示す場合、起動制御手段７１０のアプリケーションマネージャー機能は、エラー処理を実行する。この場合、起動制御手段７１０は、エラーが発生した旨を示すメッセージとして「アプリケーションを起動できませんでした」といっ

たエラーメッセージを出力手段６３０に表示してもよい。

【０１０７】

電子署名検証手段７１２は、現在時刻が時刻情報Ｔで表される期間に合致している場合、検証鍵を用いて署名の検証が成功したか否かを判別するものである。

本実施形態では、電子署名検証手段７１２は、時刻情報検証手段７１１から、現在時刻が時刻情報Ｔに合致している旨の通知を受けた場合、検証鍵記憶手段６１５から検証鍵を読み出して、署名方式に応じた検証処理を実行する。電子署名検証手段７１２は、公知のキー・インシュレイテッド署名を検証する検証処理を実行する。検証が成功した場合、起動制御手段７１０のアプリケーションマネージャー機能は、署名付きアプリケーションとして取得したアプリケーションのＡＰＬ起動情報に記載された制御コードにしたがって、当該アプリケーションの状態を制御する。

【０１０８】

また、電子署名検証手段７１２において、署名の検証が失敗した場合、起動制御手段７１０のアプリケーションマネージャー機能は、エラー処理を実行する。この場合、起動制御手段７１０は、エラーが発生した旨を示すメッセージとして「アプリケーションの認証に失敗しました」、「起動しようとしたアプリケーションは一般アプリケーションと認定されました」、または「アプリケーションを起動できませんでした」といったエラーメッセージを出力手段６３０に表示してもよい。

【０１０９】

終了制御手段７２０は、アプリケーションの終了を制御するものである。

終了制御手段７２０は、ＡＰＬ起動情報に「DESTROY」と記載されている場合、当該ＡＰＬ起動情報でライフサイクルをコントロールされているアプリケーションを終了させるために必要な後処理を行った上で当該アプリケーションを終了する。

終了制御手段７２０は、ＡＰＬ起動情報に「KILL」と記載されている場合、当該ＡＰＬ起動情報でライフサイクルをコントロールされているアプリケーションを強制的に終了する。

終了制御手段７２０は、ＡＰＬ起動情報に「KILL ALL」と記載されている場合、当該ＡＰＬ起動情報でライフサイクルをコントロールされているアプリケーションに限らず、また、連動／非連動に関わらず放送通信連携受信装置６上で動作中の全アプリケーションを強制的に終了する。

終了制御手段７２０は、ユーザの操作にしたがって、アプリケーションを終了することもできる。

【０１１０】

蓄積管理手段７３０は、アプリケーションの蓄積に係る処理として、書込み、読込み、消去を制御するものである。蓄積管理手段７３０は、アプリケーション取得手段６１１で取得した連動アプリケーションをアプリケーションキャッシュ６１２に書き込む。本実施形態では、蓄積管理手段７３０は、アプリケーション取得手段６１１で取得した連動アプリケーションをアプリケーションキャッシュ６１２に書き込むこととした。ここで、アプリケーションキャッシュ６１２は、キャッシュメモリを示す。

ここで、放送通信連携受信装置６上で動作するアプリケーションは、ＡＰＩとして例えばsaveApplicationToCache()を呼び出すことで、蓄積管理手段７３０の機能（放送通信連携用機能６２：図１参照）を利用することができる。

【０１１１】

また、蓄積管理手段７３０は、アプリケーションがアプリケーションキャッシュ６１２に格納されているか検索する。なお、放送通信連携受信装置６上で動作するアプリケーションは、ＡＰＩとして例えばqueryApplicationInCache()を呼び出すことで、蓄積管理手段７３０の機能（放送通信連携用機能６２：図１参照）を利用することができる。

【０１１２】

また、蓄積管理手段７３０は、アプリケーションキャッシュ６１２にアプリケーションが格納されていないと判断した場合、アプリケーション取得手段６１１を制御して当該ア

プリケーションを取得することとした。なお、蓄積管理手段７３０は、キャッシュヒットしなかった場合、アプリケーションが格納されていないと判断し、キャッシュヒットした場合、アプリケーションが格納されていると判断する。

【０１１３】

アプリケーション蓄積手段６１０は、アプリケーション取得手段６１１が外部からの操作に応じて当該放送通信連携受信装置６上で動作するアプリケーションを取得した場合、当該操作に応じたアプリケーションを蓄積するものであって、例えば一般的なハードディスク等から構成される。このアプリケーション蓄積手段６１０は、デジタル放送の番組に連動していない非連動アプリケーションまたは独立アプリケーションを記憶する。なお、非連動アプリケーションがアプリケーション蓄積手段６１０に蓄積された場合、ＡＰＬ起動情報記憶手段６０５に記憶されている該当するＡＰＬ起動情報は、後記するようにＡＰＬ起動情報取得手段６０７によって書き換えられる。

【０１１４】

アプリケーション取得手段６１１は、アプリケーション制御手段６０９の制御の下、通信送受信手段６０６および通信ネットワークＮを介して、アプリケーションのＡＰＬ起動情報に記載された所在アドレス（ＵＲＬ）から当該アプリケーションを取得するものである。本実施形態では、アプリケーション取得手段６１１は、アプリケーションを要求するためのリクエストを配置場所のアプリケーションサーバ５１に対して送信すると共に、リクエストの応答として時刻Ｔと電子署名とが付加された署名付きアプリケーションを受信する。なお、受信した署名付きアプリケーションのことを特に区別しない場合、単にアプリケーションと呼ぶ場合もある。

本実施形態では、アプリケーション取得手段６１１は、デジタル放送の番組に連動した連動アプリケーションを取得した場合、アプリケーション制御手段６０９の制御の下、蓄積管理手段７３０を通じてアプリケーションキャッシュ６１２に当該連動アプリケーションを格納する。

以下、連動アプリケーションは、典型的には、署名付きアプリケーションであるか、あるいは署名付きアプリケーションであるものとして扱われる。

【０１１５】

また、アプリケーション取得手段６１１は、外部からの操作に応じて非連動アプリケーションを取得した場合、アプリケーション制御手段６０９の制御の下、アプリケーション蓄積手段６１０に格納する。この非連動アプリケーションは、典型的には、署名付きアプリケーションではないので、署名付きアプリケーションではないものとして扱う。この場合、なんら特別な処理をしなければ、アプリケーション蓄積手段６１０に格納された非連動アプリケーションを起動しようとしてＡＰＬ起動情報記憶手段６０５に記憶されている該当するＡＰＬ起動情報をアプリケーション制御手段６０９が参照したとき、該当するＡＰＬ起動情報に記載されたアプリケーションの格納場所は、通信ネットワークＮの先のＵＲＬを示していることになる。そこで、このような事態を未然に防ぐため、アプリケーション取得手段６１１は、ＡＰＬ起動情報取得手段６０７に対して、ＡＰＬ起動情報書き換え指示を出力する。これにより、アプリケーション蓄積手段６１０に格納された非連動アプリケーションを起動させることができる。

【０１１６】

アプリケーションキャッシュ６１２は、アプリケーション取得手段６１１で取得されたアプリケーションを記憶するキャッシュである。ここで、キャッシュは、記憶階層の実現手段であって、例えば半導体メモリのようなキャッシュメモリで構成される。例えば、連動アプリケーションの場合、ＡＰＬ起動情報記憶手段６０５にＡＰＬ起動情報が格納された後、当該ＡＰＬ起動情報で起動する連動アプリケーションがアプリケーションキャッシュ６１２に格納される。このとき、この連動アプリケーションのＡＰＬ起動情報は書き換える必要が無い。つまり、アプリケーションキャッシュ６１２は、アプリケーション蓄積手段６１０とは異なって、アプリケーションを記憶したときに、ＡＰＬ起動情報記憶手段６０５に格納されている当該アプリケーションのＡＰＬ起動情報において、記載されてい

る所在アドレス（ＵＲＬ）の書き換えが不要な記憶手段である。

【０１１７】

アプリケーション実行手段６１３は、アプリケーションを実行するものであって、アプリケーション制御手段６０９の制御の下、アプリケーションキャッシュ６１２に格納された連動アプリケーション、または、アプリケーション蓄積手段６１０に格納された非連動アプリケーションを放送通信連携受信装置６上で動作させる。このアプリケーション実行手段６１３によって動作するアプリケーションのデータは、合成表示手段６１４へ出力される。

【０１１８】

ここで、アプリケーション実行手段６１３は、同時に複数のアプリケーションを実行することが可能である。この場合、同一サービスに属する複数のアプリケーションを実行したり、異なるサービスに属する複数のアプリケーションを実行したりすることができる。また、複数のアプリケーションが実行されているときに、少なくとも１つがバックグランド処理を行うアプリケーションであってもよい。

【０１１９】

また、アプリケーションの実行に伴って、当該アプリケーションの属するサービスにデータやコンテンツ（動画、音声、静止画）が含まれる場合、これらもサービス内で実行される。これらをアプリケーションのデータ等とよぶ。アプリケーションのデータ等は合成表示手段６１４へ出力される。例えば、アプリケーション実行手段６１３が、アプリケーションを実行した結果、装置上で動作するアプリケーションが通信ネットワークＮを介してコンテンツ配信サーバ５３等に映像・音声コンテンツを要求した場合、映像・音声コンテンツの通信ストリームを取得し、再生して合成表示手段６１４へ出力する。同様に、装置上で動作するアプリケーションが静止画等の画像データや音声データを要求して取得した場合も、合成表示手段６１４へ出力する。なお、アプリケーションのデータ等もアプリケーションキャッシュ６１２に格納される。

【０１２０】

合成表示手段６１４は、不図示の放送コンテンツ用のバッファと、通信コンテンツ用のバッファとを備え、デジタル放送番組に連動しているコンテンツを配信するコンテンツ配信サーバ５３から通信送受信手段６０６によって通信ストリームとして受信したコンテンツとデジタル放送番組とを同期させて出力手段６３０に出力するものである。

ここで、放送通信連携受信装置６上で動作するアプリケーションは、ＡＰＩとして例えばgetCurrentSTC()やdelayStreamPresentation()を呼び出すことで、放送通信連携用機能６２（図１参照）としての同期制御機能を利用することができる。

【０１２１】

また、合成表示手段６１４は、映像音声復号手段６０３から通知される映像音声データ、データ放送復号手段６０４から通知されるデータ放送画面（データ放送コンテンツ）、リスト制御手段６０８から通知されるリストデータ、アプリケーション実行手段６１３から通知されるアプリケーションのデータ等を合成し、画像データおよび音声データとして、出力手段６３０へ出力する。なお、画像データの合成は、例えば、一般的なＧＤＣ（Graphic Display Controller）で実現することができる。

【０１２２】

また、音声データの合成とは、例えば、一般的な野球中継番組の実況と、副音声サービスとの切り替えまたは合成処理と同様にして、映像音声復号手段６０３から通知される映像音声データのうちの音声データと、アプリケーションのデータ等に含まれる音声データとの一方を、ユーザの操作で切り替え可能または合成可能として出力手段６３０へ出力することを意味する。

【０１２３】

検証鍵記憶手段６１５は、アプリケーションサーバ５１にて生成された検証鍵を記憶するものである。この検証鍵は、アプリケーションサーバ５１にて付加された署名を検証するために用いられる。

【０１２４】
リソース管理手段６１６は、当該放送通信連携受信装置６で動作するアプリケーションが利用可能なリソースを管理するものである。リソース管理手段６１６は、リソースマネージャーとして機能する。ここで、リソースとは、ハードウェアやソフトウェアであって、これらを例えば受信機リソース、放送リソースおよび通信リソースのように分類することができる。
【０１２５】
ここで、受信機リソースとは、当該装置固有のリソースであり、例えば映像・音声出力処理、選局処理、メモリ、ストレージ等を含む。
放送リソースは、放送波で取得するリソースであって、例えば映像、音声、字幕、ＰＳＩ／ＳＩ（Program Specific Information：番組特定情報／Service Information：番組配列情報）等を含む。
通信リソースは、通信ネットワークＮから取得するリソースであって、例えばトランスポート層のプロトコルとしてＵＤＰ（User Datagram Protocol）やＴＣＰ（Transmission Control Protocol）で転送されるデータ（映像、音声、字幕、ＨＴＭＬコンテンツ（ＨＴＭＬブラウザ）等を含む。
【０１２６】
本実施形態では、リソース管理手段６１６は、例えば受信機リソースおよび通信リソースに関しては、予め定められた規則にしたがって割当の可／不可を判定する。このうち受信機リソースであれば、例えばグラフィックスを扱う２つのアプリケーションが同時に起動するときに、互いの動作を調整するための予め定められた提示ポリシーに従って、モニタ画面を用いる提示制御を可能とする。
【０１２７】
本実施形態では、リソース管理手段６１６は、例えば放送リソースに関しては、割当の可／不可をリソースアクセス制御手段６１７の指示に従うこととした。具体的には、リソース管理手段６１６は、実行中のアプリケーションから、例えば放送リソースが要求された場合、当該リソースが割当できるか否かを、リソースアクセス制御手段５２０に問い合わせ、割当可能の通知を受けた場合に、リソースを割り当てる。ここで、実行中のアプリケーションからのリソース要求とは、具体的にはアプリケーション制御手段４０９からのリソース要求を意味する。
【０１２８】
リソースアクセス制御手段６１７は、リソース管理手段６１６から問い合わせのあった、リソース割当の可／不可を、アプリケーション認証に基づいて判定するものである。
本実施形態では、リソースアクセス制御手段６１７は、放送リソースに関しての割当の可／不可を判定することとした。このリソースアクセス制御手段６１７は、リソース管理手段６１６から問い合わせのあったアプリケーションが、認証されたアプリケーションか否かを判別し、認証されたアプリケーションの場合、割当可能の通知を返し、そうではない場合、割当不可の通知を返す。
【０１２９】
これにより、実行中の連動アプリケーション（Ａアプリケーション）には、放送リソースが割り当てられる。なお、署名検証に成功しなかったアプリケーション（一般アプリケーション）は、起動できないので、リソースを要求することはない。
【０１３０】
［６．鍵生成処理］
ここでは、アプリケーション認証の前提として、鍵生成処理について図６を参照（適宜図４および図５参照）して説明する。図６は、本発明の実施形態に係るアプリケーションサーバによる鍵生成処理の流れを示すシーケンス図である。
まず、アプリケーションサーバ５１は、鍵生成手段５１１によって、マスター鍵K_Mを生成し（ステップＳ１１）、次いで署名を検証するための検証鍵K_Pを生成する（ステップＳ１２）。また、アプリケーションサーバ５１は、検証鍵送信手段５１７によって、生

成した検証鍵K_Pを、通信ネットワークＮを介して放送局サービスサーバ４４に送信する（ステップＳ１３）。

【０１３１】

放送局サービスサーバ４４は、通信ネットワークＮを介して検証鍵K_Pを受信する（ステップＳ１４）と、受信した検証鍵K_Pを例えば専用線Ｌを介して放送局（デジタル放送送信装置）２に送信する（ステップＳ１５）。放送局（デジタル放送送信装置）２は、検証鍵K_Pを受信する（ステップＳ１６）と、検証鍵K_Pを制御信号に含めて放送ストリームに多重化し（ステップＳ１７）、放送波Ｗを送出する（ステップＳ１８）。

【０１３２】

放送通信連携受信装置６は、放送受信手段６０１によって、放送波Ｗを受信し（ステップＳ１９）、放送信号解析手段６０２によって、放送ストリームを、ＡＶコンテンツと制御信号とに分離し（ステップＳ２０）、制御信号から検証鍵K_Pを抽出し（ステップＳ２１）、検証鍵記憶手段６１５に格納する。

【０１３３】

一方、アプリケーションサーバ５１は、部分鍵生成手段５１２によって、部分鍵の生成タイミングであるか否かを判別する（ステップＳ３１）。部分鍵の生成タイミングではない場合（ステップＳ３１：Ｎｏ）、待機し、部分鍵の生成タイミングとなった場合（ステップＳ３１：Ｙｅｓ）、アプリケーションサーバ５１は、部分鍵生成手段５１２によって、部分鍵ΔSK_Tを生成する（ステップＳ３２）。なお、ここでは、この部分鍵を用いる署名鍵の時刻情報をＴとした。そして、部分鍵生成手段５１２は署名鍵の更新タイミングであるか否かを判別し、更新タイミングにおいて部分鍵ΔSK_Tを出力すると、署名鍵更新手段５１３は、署名鍵管理手段５１４から取得した署名鍵SK_{T-1}を、部分鍵ΔSK_Tを用いて更新して署名鍵SK_Tを生成し（ステップＳ３３）、署名鍵管理手段５１４が、更新後の署名鍵SK_Tを格納し（ステップＳ３４）、ステップＳ３１に戻る。

【０１３４】

［７．アプリケーション認証処理］

ここでは、アプリケーション認証処理について図７を参照（適宜図４および図５参照）して説明する。図７は、本発明の実施形態に係る放送通信連携受信装置によるアプリケーション認証処理の流れを示すシーケンス図である。

まず、放送通信連携受信装置６は、アプリケーション制御手段６０９の制御の下、アプリケーション取得手段６１１によって、ＡＶコンテンツ（デジタル放送の番組）に連動したアプリケーションを要求する（ステップＳ４１）。すなわち、アプリケーション取得手段６１１は、アプリケーションを要求するためのリクエストを、ＡＰＬ起動情報に記載された配置場所のアプリケーションサーバ５１に対して、通信送受信手段６０６および通信ネットワークＮを介して送信する。

【０１３５】

そして、アプリケーションサーバ５１は、リクエスト受信手段５１８によって、通信ネットワークＮを介して放送通信連携受信装置６からリクエストを受信し（ステップＳ４２）、署名生成手段５１５によって、要求されたアプリケーションに対して、当該アプリケーションを起動させようとする時刻（起動時刻）の署名鍵（時刻Ｔの署名鍵）で電子署名を付加する（ステップＳ４３）。このとき、署名生成手段５１５は、要求されたアプリケーションに対して、電子署名と共に時刻情報（当該署名鍵の時刻Ｔのことを指す。以下単にＴと表記する。）を付加する。そして、アプリケーションサーバ５１は、アプリケーション送信手段５１９によって、通信ネットワークＮを介してリクエストの要求元に対して署名付きアプリケーションを送信する（ステップＳ４４）。

【０１３６】

そして、放送通信連携受信装置６は、アプリケーション取得手段６１１によって、通信ネットワークＮを介して署名付きアプリケーションを受信する（ステップＳ４５）。受信した署名付きアプリケーションは、アプリケーションキャッシュ６１２に格納される。そして、放送通信連携受信装置６は、時刻情報検証手段７１１によって、現在時刻が、署名

付きアプリケーションに付加された時刻情報（Ｔ）に合致しているか否かを判別する（ステップＳ４６）。現在時刻が、署名付きアプリケーションに付加された時刻情報（Ｔ）に合致している場合（ステップＳ４６：Ｙｅｓ）、電子署名検証手段７１２は、署名の検証が成功したか否かを判別する（ステップＳ４７）。署名の検証が成功した場合（ステップＳ４７：Ｙｅｓ）、起動制御手段７１０は、キャッシュされているアプリケーションを起動する（ステップＳ４８）。

【０１３７】

一方、前記ステップＳ４６において、時刻情報検証手段７１１が、現在時刻が署名付きアプリケーションに付加された時刻情報（Ｔ）に合致していないと判別した場合（ステップＳ４６：Ｎｏ）、時刻情報（Ｔ）が未来を示すならば（ステップＳ４９：Ｎｏ）、放送通信連携受信装置６は、待機し、ステップＳ４６に戻る。一方、時刻情報（Ｔ）が過去を示すならば（ステップＳ４９：Ｙｅｓ）、ステップＳ５０に進み、エラー処理を実行する。

また、前記ステップＳ４７において、署名の検証に失敗した場合（ステップＳ４７：Ｎｏ）、起動制御手段７１０は、エラー処理を実行する（ステップＳ５０）。

【０１３８】

［８．連動アプリケーションの起動の具体例］

ここでは、連動アプリケーションの起動の具体例について図８（ｂ）を参照（適宜図４および図５参照）して説明する。図８（ｂ）は、番組表の形式で放送番組と、その放送番組に連動したアプリケーションを示している。図８（ｂ）に符号１５０で示すアプリケーション情報は、ＡＶコンテンツ（番組）に対して、連動するアプリケーションが存在するか否かを示す情報である。また、番組情報１６０は、所定の放送局のチャンネルに紐付いたＡＶコンテンツ（番組）の情報であって、例えば開始時刻、番組尺、終了時刻を示す。

【０１３９】

図８（ｂ）に示す例では、チャンネル「ＣＨ１」の１８：００～１８：５０までのスポーツ番組に対して、連動アプリケーションＡが存在する。仮に、放送局において連動アプリケーションＡを自動起動させるための制御信号を１７：５５～１９：００の範囲で放送波に多重化していた場合、１８：００よりも前の期間では、アプリケーション認証に失敗するので放送通信連携受信装置６が例えば１８：００よりも前に取得した連動アプリケーションＡの提示を制限し、１８：００になったときに連動アプリケーションＡの認証の成功と同時に連動アプリケーションＡを起動することができる。なお、放送局において連動アプリケーションＡを終了させるための制御信号を、１８：５０に放送波に多重化していた場合、スポーツ番組の終了時点（１８：５０）で連動アプリケーションＡを終了させることができる。

【０１４０】

また、図８（ｂ）に示す例では、１８：５０～１９：００までの天気予報の番組や、１９：３０以降の特集番組に対しては、連動アプリケーションは存在していない。また、１９：００～１９：３０までのニュース番組に対して、連動アプリケーションＢが存在している。さらに、このニュース番組において途中の１９：１０～１９：２０の時間帯に対して、連動アプリケーションＣが存在している。つまり、１つのＡＶコンテンツ（番組）に対して複数の連動アプリケーションが同時に起動してもよい。例えば、連動アプリケーションＣを提供するサービス事業者と、連動アプリケーションＢを提供するサービス事業者とが異なっている。そして、放送通信連携受信装置６は、連動アプリケーションＢ用の検証鍵と、連動アプリケーションＣ用の検証鍵とをそれぞれ予め取得して、連動アプリケーションＢの認証と、連動アプリケーションＣの認証とを独立に行う。

【０１４１】

この場合、ニュース番組の開始後１０分経過した時点で連動アプリケーションＣを起動させるために、サービス事業者側のアプリケーションサーバ５１において、このタイミングで署名鍵が有効となるように予め設定しておくことも可能である。これにより、放送局において連動アプリケーションＣを自動起動させるための制御信号を１９：００～１９：

３０の範囲で放送波に多重化していたとしても、１９：００～１９：１０の期間では、アプリケーション認証に失敗するので放送通信連携受信装置６が例えば１９：００に取得した連動アプリケーションＣの提示を制限し、１９：１０になったときに連動アプリケーションＣの認証の成功と同時に連動アプリケーションＣを起動することができる。

【０１４２】

以上により、本実施形態の放送通信連携受信装置６によれば、アプリケーションの配信側で付加された署名の検証に必要な検証鍵K_pを予め取得しておくことで放送番組に連動するアプリケーションを通信ネットワークから取得した際に当該アプリケーションに付加された署名を検証することができる。したがって、サービス事業者が放送番組に連動するアプリケーションを配信する際に、事前に放送事業者またはシステム管理者による審査を通過したアプリケーションだけをＡアプリケーションであるとした場合、放送通信連携受信装置６において、番組に連動して通信ネットワークＮから取得したアプリケーションが当該Ａアプリケーションであるか否かを判定することができ、セキュリティを高めることができる。

【０１４３】

また、放送通信連携受信装置６は、放送番組の選局中に放送波から取得したＡＰＬ起動情報に記載された配置場所のアプリケーションサーバ５１から、当該放送番組に連動したアプリケーションを取得し、Ａアプリケーションであるか否かを検証してから、当該アプリケーションを自動起動することができる。したがって、放送番組を視聴中の視聴者が、特別な操作をすることなく、番組に連動して通信ネットワークＮから配信される安心なアプリケーションを自動的に提示するサービスを実現することができる。

【０１４４】

また、アプリケーションサーバ５１は、放送番組に連動したアプリケーションに対して、定期更新方式の署名鍵により電子署名を付加すると共に当該電子署名の時刻Ｔを付加することから、アプリケーションに対して未来の時刻に対応した署名鍵で署名を付加することで、当該アプリケーションを未来の時刻に起動させることができる。そのため、放送番組に連動して所望の時刻になるまでアプリケーションを待機させてから起動させることもできる。よって、放送番組に連動するアプリケーションを用いて視聴者に提供できるサービスのバリエーションを増加させることができる。

【０１４５】

以上、実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではなく、以下の変形例１～変形例４のように構成してもよい。

【０１４６】

（変形例１）

変形例１は、システム管理者によって承認された場合に、Ａアプリケーション（広義のＡアプリケーションあるいはシステム登録アプリケーション）とするモデルと、狭義のＡアプリケーション（放送局承認アプリケーション）の認証とを併用するものである。前記実施形態では、放送番組に連動したアプリケーションの認証を主眼としているため、放送通信連携型システム１にてアプリケーションを提供する全サービス事業者の中で、放送局から、放送番組に連動したアプリケーションの配信を委託された一部のサービス事業者（図４に示すアプリケーションサーバ５１の運営者）が個別に検証鍵を生成し、放送通信連携受信装置６が署名検証によりＡアプリケーションを認証することとしていた。つまり、放送局が信頼する一部のサービス事業者は、検証鍵を生成し、自らのＡアプリケーションを承認するシステム管理者のような存在（擬似管理者）として振舞うモデルである。ただし、このモデルでは、前記擬似管理者が複数存在する。このようなモデルは、狭義のＡアプリケーション、つまり放送局承認アプリケーションの認証に適している。

【０１４７】

そして、この変形例１では、放送通信連携型システム１にてアプリケーションを提供する全サービス事業者の中で、例えばシステム内唯一の検証鍵を生成したシステム管理者が登録を承認した多数のサービス事業者がアプリケーションに電子署名を付加することにな

る。ただし、放送番組に連動したアプリケーションの配信を委託された一部のサービス事業者（図４に示すアプリケーションサーバ５１の運営者）以外の事業者は、アプリケーションに署名だけを付加すればよく、時刻情報（時刻Ｔ）の付加は必須ではない。そして、放送通信連携受信装置６においては、署名付きアプリケーションに時刻Ｔが付加されていない場合、時刻情報検証手段７１１の処理をスキップして電子署名検証手段７１２の処理を行うようにすればよい。

【０１４８】

また、変形例１の場合、前記実施形態を次の（１）～（３）の各点において変形する。

（１）広義のＡアプリケーションをアプリケーションの集積場所を示すリポジトリに登録し、リポジトリの位置を放送通信連携受信装置６にとって既知のものとする。また、広義のＡアプリケーションは、放送局サーバ群４のＡＰＩ４６（図１参照）を利用することが可能であるが、広義のＡアプリケーション以外の一般アプリケーションは、放送局サーバ群４のＡＰＩ４６を利用することはできない。なお、リポジトリが、狭義のＡアプリケーションの集積場所のことを意味する場合、それは図４に示すアプリケーションサーバ５１が該当し、特に、アプリケーション記憶手段５１６等を意味する。

【０１４９】

（２）放送通信連携受信装置６の放送通信連携用機能６２（図１参照）において、セキュリティ機能は、予め定められたポリシーレベルに従ってアプリケーションの画面提示の仕方を変更する制御を行う機能を含むことができる。例えば、広義のＡアプリケーションならば、放送通信連携受信装置６に提示されたＡＶコンテンツにオーバーラップすることを許可し、広義のＡアプリケーション以外の一般アプリケーションならば、オーバーラップを許可しない（ＡＶコンテンツの表示領域の枠の外のＬ字の領域に表示させる）といった制御を行う。

【０１５０】

（３）放送通信連携受信装置６のリソースアクセス制御手段６１７は、狭義のＡアプリケーションであると認証されたアプリケーションか否かを判別する処理と、広義のＡアプリケーションであると認証されたアプリケーションか否かを判別する処理とを併用する。そして、このリソースアクセス制御手段６１７は、リソース管理手段６１６から問い合わせのあったアプリケーションが、狭義または広義のＡアプリケーションであると認証されたアプリケーションか否かを判別し、認証されたアプリケーションの場合、割当可能の通知を返し、そうではない場合、割当不可の通知を返す。これにより、実行中の連動アプリケーション（狭義のＡアプリケーション）やリポジトリに登録済みのアプリケーション（広義のＡアプリケーション）には、放送リソースが割り当てられる。一方、リポジトリに登録されていない実行中の非連動アプリケーションおよび独立アプリケーション（広義のＡアプリケーション以外の一般アプリケーション）には、放送リソースが割り当てられることはない。なお、時刻情報検証手段７１１の処理を行った上で電子署名検証手段７１２の処理に成功しなかったアプリケーション（狭義のＡアプリケーション以外の一般アプリケーション）は、起動できないのでリソースを要求することはない。

【０１５１】

（変形例２）

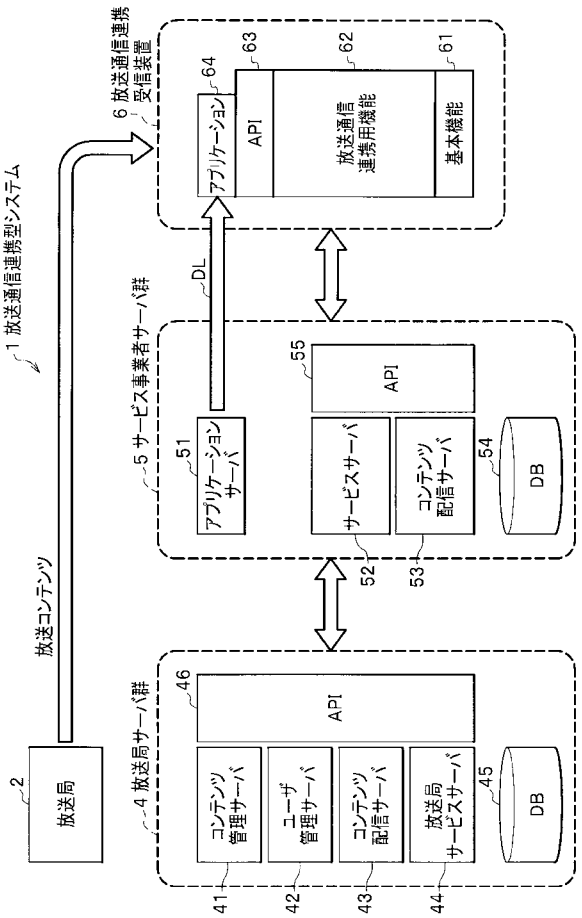
前記実施形態の放送通信連携受信装置６は、チューナを備えた一般的なコンピュータを、前記した各手段として機能させるプログラムにより動作させることで実現することができる。このプログラム（放送通信連携受信装置のアプリケーション実行制御用プログラム）は、通信回線を介して配布することも可能であるし、ＤＶＤやＣＤ－ＲＯＭ等の記録媒体に書き込んで配布することも可能である。

前記実施形態のアプリケーションサーバ５１は、一般的なコンピュータを、前記した各手段として機能させるプログラムにより動作させることで実現することができる。このプログラム（アプリケーションサーバ用プログラム）は、通信回線を介して配布することも可能であるし、ＤＶＤやＣＤ－ＲＯＭ等の記録媒体に書き込んで配布することも可能である。

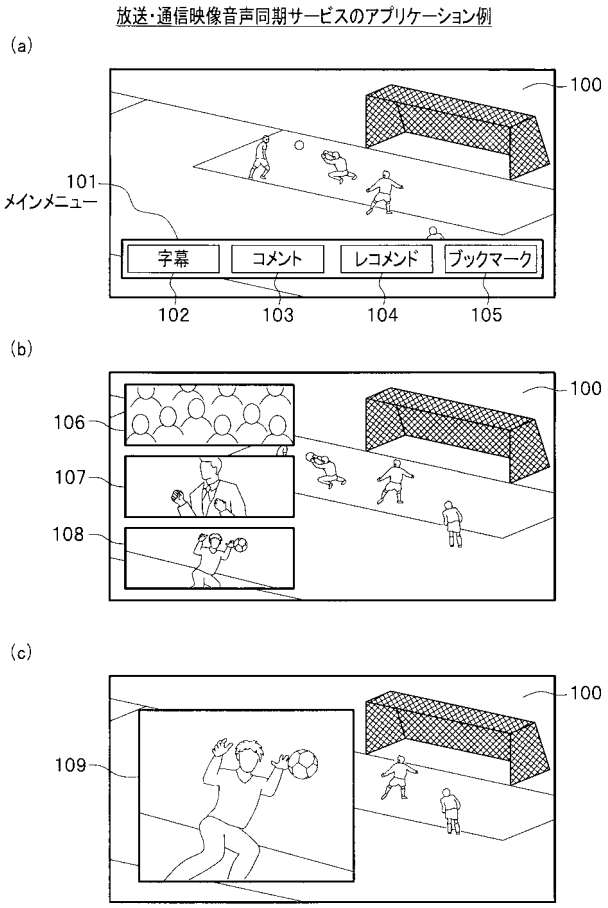
【０１５２】
（変形例３）
前記実施形態の放送通信連携受信装置６では、視聴者がデジタル放送番組を視聴中に、「AUTO START」と記載されたＡＰＬ起動情報を受信したときにアプリケーションを自動起動させるものとして説明したが、さらに、次の（４）や（５）の機能を追加してもよい。
（４）デジタル放送の提示中に、リモコンに予め設けられたＨボタン（放送通信連携サービス画面移行ボタン）をユーザが押下操作することで放送通信連携サービス画面に遷移する。
（５）ＢＭＬから放送通信連携サービス画面に遷移するための放送通信連携サービス画面遷移専用ＡＰＩを新たに設けて用意しておく。デジタル放送の提示中に、リモコンに設けられたＤボタン（データ放送移行ボタン）をユーザが押下操作することでデータ放送画面に遷移し、その後、データ放送画面上に、放送通信連携サービス画面遷移専用ＡＰＩに対応して設けられた専用ボタンを選択する操作をユーザが行うことで、放送通信連携サービス画面に遷移する。
【０１５３】
（変形例４）
前記実施形態の放送通信連携型システムでは、放送コンテンツの送信側において、データカルーセル方式により伝送される特定モジュールで、ＡＰＬ起動情報ファイルを伝送することとして説明したが、放送でＡＰＬ起動情報を送る場合、イベント情報テーブル（ＥＩＴ：Event Information Table）に、ＡＰＬ起動情報のための記述子を追加して伝送するようにしてもよいし、ＡＰＬ起動情報のための専用のエレメンタリストリーム（ＥＳ：Elementary Stream）を放送ＴＳ（Transport Stream）に多重化してもよいし、あるいは、ＡＰＬ起動情報の所在アドレスを示す情報だけを伝送するようにしてもよい。
また、放送番組に連動するアプリケーションの認証において、電子署名に加えて、第三者機関による証明書を利用する形態とする場合には、放送ではなく、通信ネットワークから、放送番組に連動するアプリケーションのＡＰＬ起動情報ファイルを伝送するようにしてもよい。
【符号の説明】
【０１５４】
１　放送通信連携型システム
２　放送局（デジタル放送送信装置）
４　放送局サーバ群
４１　コンテンツ管理サーバ
４２　ユーザ管理サーバ
４３　コンテンツ配信サーバ
４４　放送局サービスサーバ
４５　ＤＢ
４６　ＡＰＩ
５　サービス事業者サーバ群
５１　アプリケーションサーバ
５１１　鍵生成手段
５１２　部分鍵生成手段
５１３　署名鍵更新手段
５１４　署名鍵管理手段
５１５　署名生成手段
５１６　アプリケーション記憶手段
５１７　検証鍵送信手段
５１８　リクエスト受信手段
５１９　アプリケーション送信手段
５２　サービスサーバ

５３　コンテンツ配信サーバ
５４　ＤＢ
５５　ＡＰＩ
６　放送通信連携受信装置
６１　基本機能
６２　放送通信連携用機能
６３　ＡＰＩ
６４　アプリケーション（放送通信連携用アプリケーション）
６０１　放送受信手段
６０２　放送信号解析手段
６０３　映像音声復号手段
６０４　データ放送復号手段（アプリケーション起動情報抽出手段）
６０５　ＡＰＬ起動情報記憶手段（アプリケーション起動情報記憶手段）
６０６　通信送受信手段（遅延時間出力手段）
６０７　ＡＰＬ起動情報取得手段
６０８　リスト制御手段
６０９　アプリケーション制御手段
６１０　アプリケーション蓄積手段
６１１　アプリケーション取得手段
６１２　アプリケーションキャッシュ
６１３　アプリケーション実行手段
６１４　合成表示手段（遅延時間出力手段）
６１５　検証鍵記憶手段
６１６　リソース管理手段
６１７　リソースアクセス制御手段
６２０　操作入力手段
６３０　出力手段
７１０　起動制御手段
７１１　時刻情報検証手段
７１２　電子署名検証手段
７２０　終了制御手段
７３０　蓄積管理手段
ＡＴＮ　アンテナ
Ｎ　通信ネットワーク
Ｌ　専用線

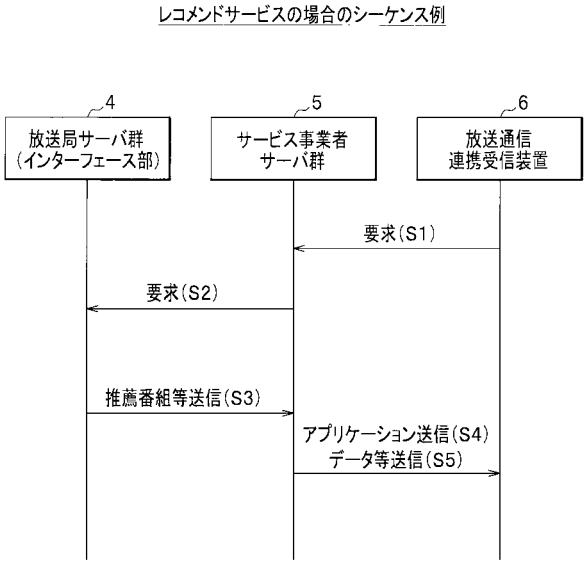
【図１】


1 放送通信連携型システム
6 放送通信連携受信装置
アプリケーション
API
放送通信連携用機能
基本機能
63
62
61
64
DL
5 サービス事業者サーバ群
アプリケーションサーバ
サービスサーバ
コンテンツ配信サーバ
DB
55
51
54
52
53
放送コンテンツ
4 放送局サーバ群
コンテンツ管理サーバ
ユーザ管理サーバ
コンテンツ配信サーバ
放送局サービスサーバ
46
45
41
42
43
44
2
放送局

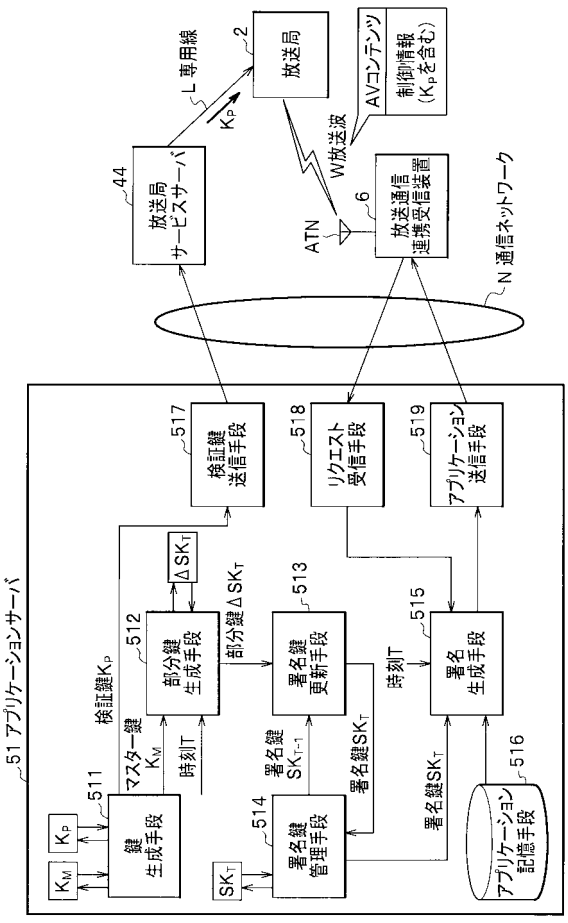
【図２】


放送・通信映像音声同期サービスのアプリケーション例
(a)
100
101
メインメニュー
字幕
コメント
レコメンド
ブックマーク
102
103
104
105
(b)
106
107
108
(c)
109

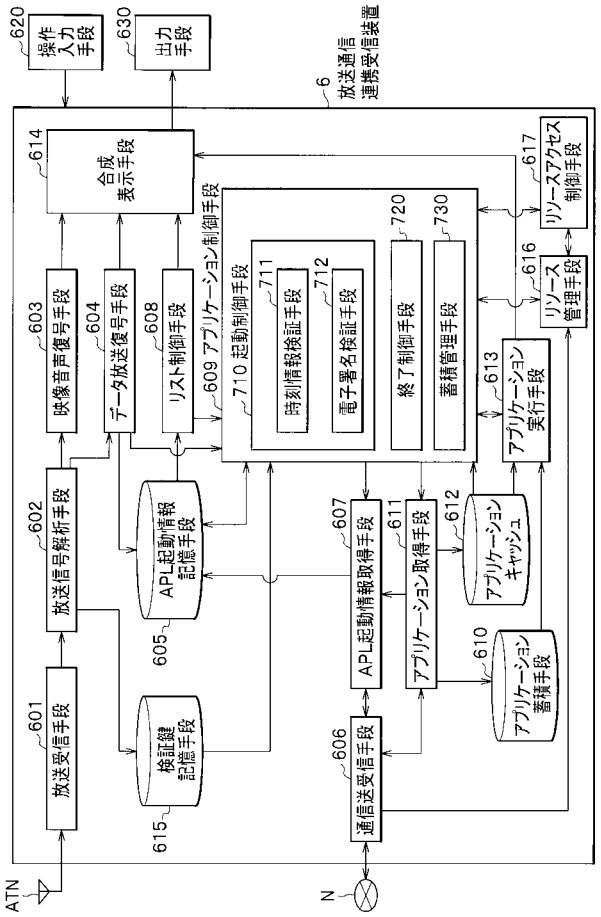
【図３】


レコメンドサービスの場合のシーケンス例
4
5
6
放送局サーバ群（インターフェース部）
サービス事業者サーバ群
放送通信連携受信装置
要求(S1)
要求(S2)
推薦番組等送信(S3)
アプリケーション送信(S4)
データ等送信(S5)

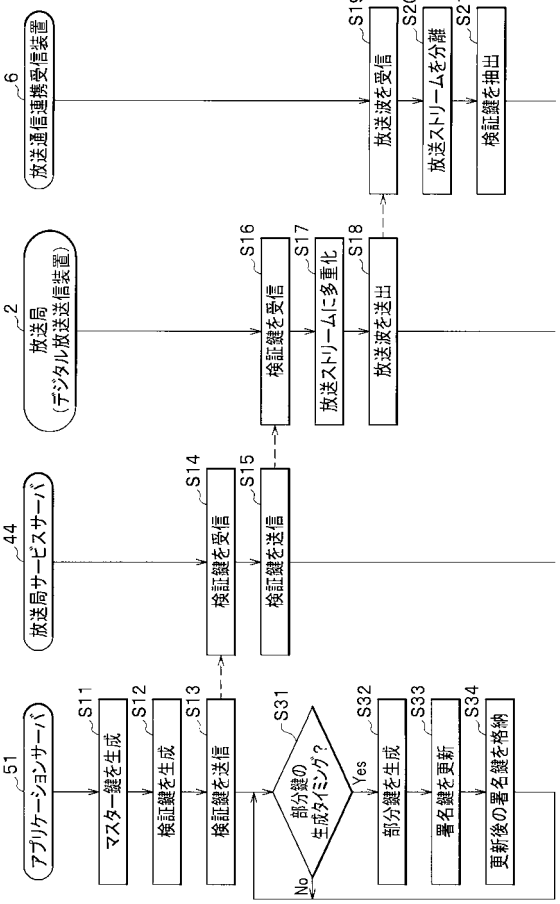
【図４】


L 専用線
2
放送局
AVコンテンツ
制御情報
(KPを含む)
KP
W放送波
44
放送局サービスサーバ
ATN
6
放送通信連携受信装置
N 通信ネットワーク
51 アプリケーションサーバ
517
検証鍵送信手段
518
リクエスト受信手段
519
アプリケーション送信手段
ΔSKT
512
部分鍵生成手段
部分鍵ΔSKT
513
署名鍵更新手段
515
署名生成手段
検証鍵KP
マスター鍵KM
時刻T
署名鍵SKT-1
署名鍵SKT
時刻T
511
鍵生成手段
514
署名鍵管理手段
516
アプリケーション記憶手段
KM
KP
SKT

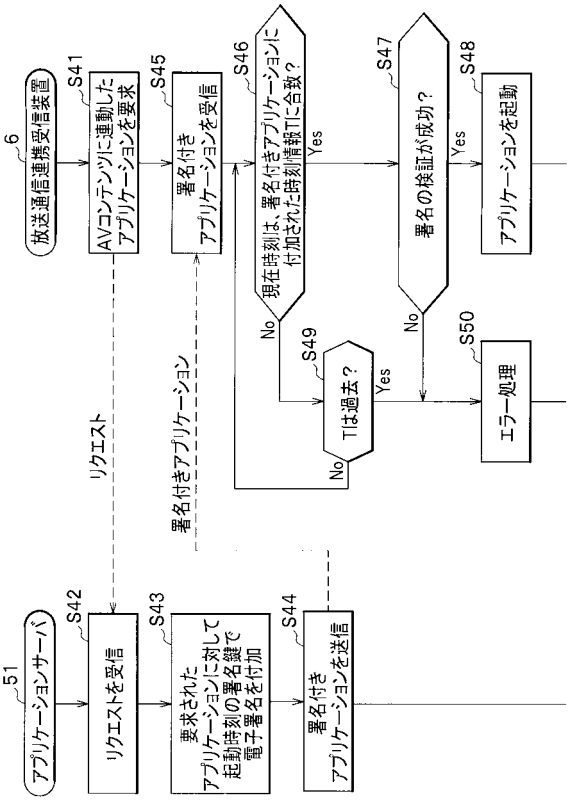
【図５】


620 操作入力手段
630 出力手段
6 放送通信連携受信装置
614 合成表示手段
603 映像音声復号手段
604 データ放送復号手段
608 リスト制御手段
609 アプリケーション制御手段
710 起動制御手段
711 時刻情報検証手段
712 電子署名検証手段
720 終了制御手段
730 蓄積管理手段
613 アプリケーション実行手段
617 リソースアクセス制御手段
616 リソース管理手段
602 放送信号解析手段
601 放送受信手段
605 APL起動情報記憶手段
615 検証鍵記憶手段
607 APL起動情報取得手段
611 アプリケーション取得手段
612 アプリケーションキャッシュ
610 アプリケーション蓄積手段
606 通信送受信手段
ATN
N

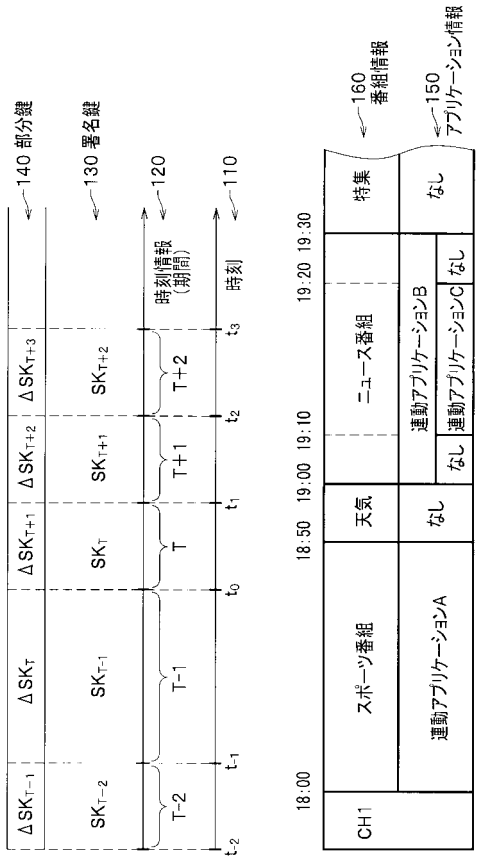
【図６】


6 放送通信連携受信装置
2 放送局（デジタル放送送信装置）
44 放送局サービスサーバ
51 アプリケーションサーバ
S11 マスター鍵を生成
S12 検証鍵を生成
S13 検証鍵を送信
S14 検証鍵を受信
S15 検証鍵を送信
S16 検証鍵を受信
S17 放送ストリームに多重化
S18 放送波を送出
S19 放送波を受信
S20 放送ストリームを分離
S21 検証鍵を抽出
S31 部分鍵の生成タイミング？
Yes
No
S32 部分鍵を生成
S33 署名鍵を更新
S34 更新後の署名鍵を格納

【図７】


6 放送通信連携受信装置
51 アプリケーションサーバ
S41 AVコンテンツに連動したアプリケーションを要求
S42 リクエストを受信
S43 要求されたアプリケーションに対して起動時刻の署名鍵で電子署名を付加
S44 署名付きアプリケーションを送信
S45 署名付きアプリケーションを受信
S46 現在時刻は、署名付きアプリケーションに付加された時刻情報に合致？
S47 署名の検証が成功？
S48 アプリケーションを起動
S49 Tは過去？
S50 エラー処理
リクエスト
署名付きアプリケーション
Yes
No

【図８】


(a)
140 部分鍵
130 署名鍵
120
110
時刻情報（期間）
時刻
(b)
160 番組情報
150 アプリケーション情報
CH1
スポーツ番組
連動アプリケーションA
天気
ニュース番組
連動アプリケーションB
連動アプリケーションC
特集
なし
18:00
18:50
19:00
19:10
19:20
19:30

フロントページの続き

(51)Int.Cl.		F I	テーマコード（参考）
Ｈ０４Ｈ 60/73	***(2008.01)***	Ｈ０４Ｈ 60/27	
Ｈ０４Ｈ 60/82	***(2008.01)***	Ｈ０４Ｈ 60/73	
Ｈ０４Ｈ 60/14	***(2008.01)***	Ｈ０４Ｈ 60/82	
		Ｈ０４Ｈ 60/14	

Ｆターム(参考) 5C164 FA11 MA08P PA21 SA51S SB29S TA04S TA08S TB23P UB41P UB51S
UB86S UB88S UB92S UD44S YA11 YA21