(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号

特許第6186096号
(P6186096)

(45)発行日　平成29年8月23日(2017.8.23)　(24)登録日　平成29年8月4日(2017.8.4)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04N 21/266 | (2011.01) | H04N | 21/266 | |
| H04N 21/4623 | (2011.01) | H04N | 21/4623 | |
| H04L 9/08 | (2006.01) | H04L | 9/00 | 601B |
| H04L 9/14 | (2006.01) | H04L | 9/00 | 601E |
| | | H04L | 9/00 | 641 |

請求項の数 2　(全 31 頁)

(21)出願番号　特願2017-73371(P2017-73371)
(22)出願日　平成29年4月3日(2017.4.3)
(62)分割の表示　特願2015-172622(P2015-172622)の分割
原出願日　平成23年9月22日(2011.9.22)
審査請求日　平成29年4月3日(2017.4.3)

早期審査対象出願

(73)特許権者　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　110001807
特許業務法人磯野国際特許商標事務所
(72)発明者　川喜田　裕之
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　西本　友成
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　遠藤　洋介
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】デジタル放送送信装置およびデジタル放送受信装置

(57)【特許請求の範囲】
【請求項１】
放送波を介して送信されるコンテンツへのアクセスを制御するためのアクセス制御プログラムをデジタル放送受信装置に送信するデジタル放送送信装置であって、
前記デジタル放送受信装置で共通のプログラム暗号化鍵で配信用の前記アクセス制御プログラムを暗号化するとともに、当該アクセス制御プログラムを識別する識別情報を付加して、配信データを生成する配信データ生成手段と、
この配信データ生成手段で生成された配信データをスクランブル鍵で暗号化して、暗号化配信データを生成する配信データスクランブル手段と、
前記デジタル放送受信装置に送信する伝送路保護鍵で前記スクランブル鍵を暗号化して、前記デジタル放送受信装置で共通の共通情報を生成する共通情報生成手段と、
前記デジタル放送受信装置のデバイス鍵で前記伝送路保護鍵を暗号化して、前記デジタル放送受信装置ごとの個別情報を生成する個別情報生成手段と、
前記放送波により前記配信用のアクセス制御プログラムを送信する旨を示す識別子を付加するとともに、前記識別情報を含んだダウンロードテーブルを生成するダウンロードテーブル生成手段と、
起動用のアクセス制御プログラムを特定する第２識別情報を、番組配列情報であるＰＳＩ／ＳＩの情報テーブルに配置する起動プログラム指定手段と、
前記暗号化配信データと、前記共通情報と、前記個別情報と、前記ダウンロードテーブルと、前記番組配列情報の情報テーブルとを多重化して、前記デジタル放送受信装置に送

信する多重化信号を生成する多重化手段と、
を備えることを特徴とするデジタル放送送信装置。
【請求項２】
放送波を介して送信されるコンテンツへのアクセス制御をアクセス制御プログラムによって行うデジタル放送受信装置において、
前記アクセス制御プログラムを分割し、プログラム暗号化鍵で暗号化した配信データをスクランブル鍵でさらに暗号化した暗号化配信データと、前記スクランブル鍵を伝送路保護鍵で暗号化し生成した共通情報と、前記伝送路保護鍵をデバイス鍵で暗号化し生成した個別情報と、前記放送波により前記アクセス制御プログラムを送信する旨を示す識別子および当該アクセス制御プログラムを識別する識別情報を含んだダウンロードテーブルと、
起動用のアクセス制御プログラムを特定する第２識別情報を含んだ番組配列情報の情報テーブルと、を含んだ多重化信号からそれぞれの情報を分離する分離手段と、
前記ダウンロードテーブルに記述されている識別子により、前記放送波で前記アクセス制御プログラムが送信されていることを判定するダウンロードテーブル解析手段と、
デジタル放送送信装置と共通のデバイス鍵で前記個別情報を復号して、前記伝送路保護鍵を取得する個別情報復号手段と、
この個別情報復号手段で取得した伝送路保護鍵で前記共通情報を復号して、前記スクランブル鍵を取得する共通情報復号手段と、
前記暗号化配信データを前記スクランブル鍵で復号する配信データデスクランブル手段と、
この配信データデスクランブル手段で復号された配信データから、暗号化されたアクセス制御プログラムおよび当該アクセス制御プログラムを識別する識別情報を分離する配信データ分離手段と、
前記暗号化されたアクセス制御プログラムを、前記プログラム暗号化鍵で復号するプログラム復号手段と、
このプログラム復号手段で復号されたアクセス制御プログラムを前記識別情報と対応付けて記憶するプログラム記憶手段と、
前記情報テーブルから前記第２識別情報を抽出する起動プログラム特定手段と、
この起動プログラム特定手段で抽出された第２識別情報に対応するアクセス制御プログラムを、前記プログラム記憶手段から読み出して起動させるプログラム起動手段と、
を備えることを特徴とするデジタル放送受信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタル放送の放送番組のアクセス制御に関するプログラムを送受信するデジタル放送送信装置およびデジタル放送受信装置に関する。
【背景技術】
【０００２】
現行のデジタル放送では、契約者の受信装置のみに放送番組（以下、コンテンツという）を限定受信させる機能や、正規の受信装置のみにコンテンツを受信させたり、コピー制限を行ったりすることで著作権保護を行う機能を、アクセス制御方式であるＣＡＳ（Conditional Access System）を用いて実現している。
具体的には、アクセス制御に関する機能（例えば、暗号化されたコンテンツを復号するための鍵の復号等）を耐タンパモジュールであるＩＣカード（ＣＡＳカード）に実装し、ＩＣカードと受信装置とを組み合わせることで、アクセス制限を行っている。
【０００３】
しかし、このアクセス制御に関する機能は、内部に保持する鍵の流出や、アルゴリズムの解析等によって、セキュリティが破られる可能性がある。このような場合、セキュリティ強度を高めたＩＣカードを再配布する方法が考えられるが、ＩＣカードの配布コストやＩＣカードの差し替え等、ユーザに負担を強いるため、現実的には実施困難である。また

、セキュリティ問題を解決する以外にも、アクセス制御に関する機能を拡張したいという要望もある。

【０００４】

そこで、ＩＣカードに実装するアクセス制御に関する機能を、ＣＡＳプログラムとして受信装置に蓄積するとともに、放送波を介して、ＣＡＳプログラムを更新する技術が開示されている（特許文献１参照）。

この特許文献１に開示された技術では、コンテンツ権利保護関連の共通情報であるＥＣＭ－ＲＭＰ（ＥＣＭ：Entitlement Control Message、ＲＭＰ：Rights Management and Protection）に、暗号化したＣＡＳプログラムを配置して配信している。

また、特許文献１に開示された技術では、コンテンツ権利保護関連の個別情報であるＥＭＭ－ＲＭＰ（ＥＭＭ：Entitlement Management Message）に、暗号化したＣＡＳプログラムを復号するための鍵を配置して配信している。

これによって、受信装置では、ＥＭＭ－ＲＭＰで配信される鍵によって、ＥＣＭ－ＲＭＰで配信される暗号化されたＣＡＳプログラムをダウンロードし復号することで、ＣＡＳプログラムの蓄積、更新を行うことが可能になる。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００９－２６７６０５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

特許文献１で開示されている従来技術では、セキュリティパラメータとしての役割を持つＥＣＭ（ＥＣＭ－ＲＭＰ）やＥＭＭ（ＥＭＭ－ＲＭＰ）を用いて、ＣＡＳプログラムの配信を実現している。このＥＣＭやＥＭＭといったセキュリティパラメータは、秘密情報として耐タンパモジュール等で処理する必要がある。

一般に、耐タンパモジュールは、処理速度が低速であるため、例えば、３００ｋｂｐｓ程度までしかビットレートを高めることができない。すなわち、従来技術では、送信側から、低ビットレートでＣＡＳプログラムを送出しなければならない。

このため、従来技術では、ＣＡＳプログラムを確実に配信するためには、長期間にわたって放送し続ける必要があり、放送帯域を圧迫してしまうという問題がある。

【０００７】

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、ＣＡＳプログラムの改ざん、漏洩等に対する安全性を確保しつつ、ＣＡＳプログラムを高速にダウンロードすることが可能なデジタル放送送信装置およびデジタル放送受信装置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】

【０００８】

本発明は、前記課題を解決するために創案されたものであり、まず、請求項１に記載のデジタル放送送信装置は、放送波を介して送信されるコンテンツへのアクセスを制御するためのアクセス制御プログラムをデジタル放送受信装置に送信するデジタル放送送信装置であって、配信データ生成手段と、配信データスクランブル手段と、共通情報生成手段と、個別情報生成手段と、ダウンロードテーブル生成手段と、起動プログラム指定手段と、多重化手段と、を備える構成とした。

【０００９】

かかる構成において、デジタル放送送信装置は、配信データ生成手段によって、デジタル放送受信装置で共通のプログラム暗号化鍵で配信用のアクセス制御プログラムを暗号化するとともに、当該アクセス制御プログラムを識別する識別情報を付加して配信データを生成する。この識別情報は、例えば、アクセス制御プログラムの識別子やバージョンである。

【００１０】
そして、デジタル放送送信装置は、配信データスクランブル手段によって、配信データ生成手段で生成された配信データをスクランブル鍵で暗号化して、暗号化配信データを生成する。
【００１１】
また、デジタル放送送信装置は、共通情報生成手段によって、デジタル放送受信装置に送信する伝送路保護鍵でスクランブル鍵を暗号化して、デジタル放送受信装置で共通の共通情報を生成する。これによって、正規のデジタル放送受信装置であれば、復号可能なようにスクランブル鍵を暗号化する。
【００１２】
さらに、デジタル放送送信装置は、個別情報生成手段によって、デジタル放送受信装置のデバイス鍵で伝送路保護鍵を暗号化して、デジタル放送受信装置ごとの個別情報を生成する。これによって、個別の有効なデバイス鍵を有するデジタル放送受信装置のみが復号可能なように伝送路保護鍵を暗号化する。
【００１３】
また、デジタル放送送信装置は、ダウンロードテーブル生成手段によって、放送波により配信用のアクセス制御プログラムを送信する旨を示す識別子を付加するとともに、アクセス制御プログラムを識別する識別情報を含んだダウンロードテーブルを生成する。このダウンロードテーブルによって、デジタル放送受信装置は、放送波によりアクセス制御プログラムをダウンロードすることが可能であることを認識し、ダウンロードを開始することができる。
【００１４】
また、デジタル放送送信装置は、起動プログラム指定手段によって、起動用のアクセス制御プログラムを特定するための第２識別情報を、番組配列情報であるＰＳＩ（Program Specific Information）／ＳＩ（Service Information）の情報テーブルに配置する。例えば、ＣＡＴ（Conditional Access Table）またはＰＭＴ（Program Map Table）に配置する。
【００１５】
そして、デジタル放送送信装置は、多重化手段によって、生成された暗号化配信データと、共通情報と、個別情報と、ダウンロードテーブルと、番組配列情報の情報テーブルとを生成されたタイミングで順次多重化してデジタル放送受信装置に送信する多重化信号を生成する。
【００１６】
このように、デジタル放送送信装置は、暗号化したアクセス制御プログラムを高速な放送波で伝送することができる。また、デジタル放送送信装置は、アクセス制御プログラムを暗号化する際に、無効となったデバイス鍵を用いないため、有効なデバイス鍵を有するデジタル放送受信装置のみがアクセス制御プログラムを使用可能に制御することができる。
【００１７】
また、請求項２に記載のデジタル放送受信装置は、放送波を介して送信されるコンテンツへのアクセス制御をアクセス制御プログラムによって行うデジタル放送受信装置において、分離手段と、ダウンロードテーブル解析手段と、個別情報復号手段と、共通情報復号手段と、配信データデスクランブル手段と、配信データ分離手段と、プログラム復号手段と、プログラム記憶手段と、起動プログラム特定手段と、プログラム起動手段と、を備える構成とした。
【００１８】
かかる構成において、デジタル放送受信装置は、分離手段によって、暗号化配信データと、共通情報と、個別情報と、ダウンロードテーブルと、番組配列情報の情報テーブルと、を含んだ多重化信号からそれぞれの情報を分離する。
そして、デジタル放送受信装置は、ダウンロードテーブル解析手段によって、放送波に

よりアクセス制御プログラムを送信する旨を示す識別子および当該アクセス制御プログラムを識別する識別情報を含んだダウンロードテーブルに記述されている識別子により、放送波でアクセス制御プログラムが送信されていることを判定する。

【００１９】

また、デジタル放送受信装置は、個別情報復号手段によって、デジタル放送送信装置と共通のデバイス鍵で個別情報を復号して、伝送路保護鍵を取得する。そして、デジタル放送受信装置は、共通情報復号手段によって、伝送路保護鍵で共通情報を復号してスクランブル鍵を取得する。そして、デジタル放送受信装置は、配信データデスクランブル手段によって、暗号化配信データをスクランブル鍵で復号する。

さらに、デジタル放送受信装置は、配信データ分離手段によって、配信データから、暗号化されたアクセス制御プログラムおよび当該アクセス制御プログラムを識別する識別情報を分離する。

【００２０】

そして、デジタル放送受信装置は、プログラム復号手段によって、暗号化されたアクセス制御プログラムを、プログラム暗号化鍵で復号し、アクセス制御プログラムを識別情報と対応付けてプログラム記憶手段に記憶する。

【００２１】

このように、デジタル放送受信装置は、アクセス制御プログラムを高速な放送波で受信することができる。また、デジタル放送受信装置は、アクセス制御プログラムを暗号化したプログラム暗号化鍵を、有効なデバイス鍵を有するデジタル放送受信装置のみが復号可能なように暗号化した個別情報として受信する。

【発明の効果】

【００２２】

本発明は、以下に示す優れた効果を奏するものである。

請求項１，２に記載の発明によれば、デジタル放送送信装置からデジタル放送受信装置に対して、放送波でアクセス制御プログラム（ＣＡＳプログラム）を配信し、アクセス制御プログラムの識別情報、鍵等を、セキュリティパラメータである共通情報や個別情報で配信することができる。これによって、本発明は、アクセス制御プログラムの改ざん等を防止し、アクセス制御プログラムをセキュリティパラメータとして配信する場合と比べ、高速に配信することができ、放送帯域の圧迫を抑制することができる。

また、請求項１，２に記載の発明によれば、デバイス鍵やプログラム暗号化鍵が漏洩した場合であっても、伝送路保護鍵およびプログラム暗号化鍵を更新し、新たなアクセス制御プログラムを配信することで、デバイス鍵が漏洩したデジタル放送受信装置を無効化（リボーク）するとともに、新しいアクセス制御プログラムの漏洩を防ぐことができる。

また、請求項１，２に記載の発明によれば、アクセス制御プログラムのセキュリティが破られた場合であっても、高速にアクセス制御プログラムを更新することができる。さらに、放送事業者が、提供したいサービスに応じてアクセス制御プログラムを変更することができる。

【図面の簡単な説明】

【００２３】

【図１】本発明の実施形態に係るデジタル放送システムの構成を示す概略構成図である。

【図２】本発明の実施形態に係るデジタル放送送信装置の構成を示すブロック構成図である。

【図３】本発明の実施形態に係るデジタル放送送信装置の配信データ生成手段の構成を示すブロック構成図である。

【図４】本発明の実施形態に係るデジタル放送受信装置の構成を示すブロック構成図である。

【図５】ＤＩＩメッセージの内容を示すデータ構造図である。

【図６】ＤＤＢメッセージの内容を示すデータ構造図である。

【図７】デバイス鍵リスト記憶手段の記憶内容を説明するための図である。

【図８】ダウンロードテーブルの内容を示すデータ構造図である。
【図９】ダウンロードコンテンツ記述子の内容を示すデータ構造図である。
【図１０】ネットワークダウンロードコンテンツ記述子の内容を示すデータ構造図である。
【図１１】本発明の実施形態に係るデジタル放送送信装置におけるアクセス制御プログラム（ＣＡＳプログラム）の配信動作を示すフローチャートである。
【図１２】本発明の実施形態に係るデジタル放送受信装置におけるアクセス制御プログラム（ＣＡＳプログラム）の受信動作を示すフローチャートである。
【図１３】本発明の実施形態に係るデジタル放送送信装置におけるアクセス制御プログラム（ＣＡＳプログラム）の起動指示動作を示すフローチャートである。
【図１４】本発明の実施形態に係るデジタル放送受信装置におけるアクセス制御プログラム（ＣＡＳプログラム）の起動動作を示すフローチャートである。
【発明を実施するための形態】
【００２４】
以下、本発明の実施形態について図面を参照して説明する。
［デジタル放送システムの概要］
最初に、図１を参照して、本発明の実施形態に係るデジタル放送システムの概要について説明する。
【００２５】
デジタル放送システムＳは、放送事業者が有するデジタル放送送信装置１と、各家庭等に設置されたデジタル放送受信装置３，３，３，…とで構成され、デジタル放送送信装置１からデジタル放送の放送波Ｗで送信されるコンテンツ（放送番組）をデジタル放送受信装置３において受信し、視聴者が視聴するシステムである。なお、放送波Ｗは、地上デジタル放送、衛星放送、ケーブル放送等、無線、有線を問わない。
【００２６】
デジタル放送送信装置１は、放送波Ｗを介して、コンテンツをデジタル放送受信装置３に送信するものである。なお、このデジタル放送送信装置１は、放送波Ｗを介して、コンテンツへのアクセス制御に関する機能を有するＣＡＳ（Conditional Access System）プログラム（アクセス制御プログラム）を、デジタル放送のデータカルーセルで伝送し、更新する機能を有する。
【００２７】
デジタル放送受信装置３は、放送波Ｗを介してコンテンツを受信するものである。なお、このデジタル放送受信装置３は、デジタル放送送信装置１から、データカルーセル伝送により配信されるＣＡＳプログラムを受信し、更新する機能を有する。
すなわち、デジタル放送システムＳは、デジタル放送受信装置３において使用するＣＡＳプログラムの鍵の流出等、セキュリティが破られたとき、あるいは、提供するサービスに応じて使用するＣＡＳプログラムを更新したいとき等に、放送事業者が、デジタル放送送信装置１によって、新たなＣＡＳプログラムを、デジタル放送受信装置３に配信するシステムである。
【００２８】
なお、データカルーセルは、社団法人電波産業会（ＡＲＩＢ）のＳＴＤ－Ｂ２４で規定されている同一データを一定期間繰り返して配信することで、デジタル放送受信装置３が任意のタイミングで必要なデータの取得を可能にする伝送方式である。
このデジタル放送システムＳでは、同一のＣＡＳプログラム（ＣＡＳ　$Ｐ_{1}$～$Ｐ_{n}$）を一定期間繰り返して伝送することで、ＣＡＳプログラムを、デジタル放送受信装置３に配信する。
【００２９】
さらに、デジタル放送システムＳは、データカルーセルによるＣＡＳプログラムの配信に加え、通信回線Ｎを介してＣＡＳプログラムを配信する機能を有している。
ここでは、デジタル放送システムＳは、ＣＡＳプログラムを蓄積するとともに、通信回

線Ｎを介してＣＡＳプログラムを送信するサーバ（ＣＡＳサーバ５）を備え、デジタル放送送信装置１が、放送波Ｗを介してＣＡＳプログラムの所在（ＵＲＬ：Uniform Resource Locator）をデジタル放送受信装置３に通知する。そして、デジタル放送受信装置３が、通信回線Ｎを介して、ＣＡＳサーバ５から、ＣＡＳプログラムを取得し、更新を行う。

【００３０】

このように、デジタル放送システムＳは、データカルーセル伝送を行うことで、ＣＡＳプログラムを高速に伝送することができ、ＣＡＳプログラムを配信する期間を、例えば、１週間程度と短くすることができる。

また、デジタル放送システムＳは、データカルーセルによるＣＡＳプログラムの伝送期間が終了した場合であっても、通信回線Ｎを介して、ＣＡＳプログラムを配信することができる。これによって、デジタル放送システムＳは、放送波ＷによるＣＡＳプログラムの配信に伴う放送帯域の圧迫を低減することができる。

【００３１】

以下、デジタル放送システムＳにおいて、ＣＡＳプログラムの伝送上の安全性を高めてＣＡＳプログラムの更新を可能とするデジタル放送送信装置１およびデジタル放送受信装置３について、その構成および動作について詳細に説明を行う。

【００３２】

［デジタル放送送信装置の構成］

まず、図２を参照（適宜図１参照）して、本発明の実施形態に係るデジタル放送送信装置の構成について説明する。ここでは、デジタル放送送信装置１は、コンテンツスクランブル手段１０と、ＥＣＭ－ＣＡＳ生成手段１１と、ＥＭＭ－ＣＡＳ生成手段１２と、配信データ生成手段１３と、配信データスクランブル手段１４と、ＥＣＭ－ＲＭＰ生成手段１５と、デバイス鍵リスト記憶手段１６と、無効設定手段１７と、デバイス鍵選択手段１８と、ＥＭＭ－ＲＭＰ生成手段１９と、ダウンロードテーブル生成手段２０と、起動プログラム指定手段２１と、多重化手段２２と、を備えている。

【００３３】

なお、図２中、破線部分で示したＡ部分の構成については、ＣＡＳプログラムごとに複数備えることとする。例えば、配信するＣＡＳプログラムがデジタル放送受信装置３のメーカごとに異なる場合、Ａ部分は、メーカごとに複数備えるものとする。

【００３４】

コンテンツスクランブル手段１０は、入力されたコンテンツ（映像、音声、データ等）Ｃｔをスクランブル鍵Ｋｓ１でスクランブル（暗号化）するものである。

このスクランブル鍵Ｋｓ１による暗号化は、一般的な共通鍵暗号アルゴリズムを用いればよく、例えば、ＭＵＬＴＩ２暗号により暗号化する。このようにスクランブルされたコンテンツ（暗号化コンテンツＳｃｔ）は、多重化手段２２に出力される。

【００３５】

なお、スクランブル鍵Ｋｓ１は、時間によって更新されるものであって、数秒に１回程度更新されるものである。ここでは、スクランブル鍵Ｋｓ１は、図示を省略した記憶手段に記憶され、適宜、外部から新たなスクランブル鍵Ｋｓ１が入力されることで更新されるものとする。

【００３６】

ＥＣＭ－ＣＡＳ生成手段１１は、コンテンツスクランブル手段１０で用いたスクランブル鍵Ｋｓ１をワーク鍵Ｋｗで暗号化し、暗号化されたスクランブル鍵Ｋｓ１を含む共通情報を生成するものである。この共通情報は、すべてのデジタル放送受信装置３に共通のセキュリティ情報である。

このワーク鍵Ｋｗによる暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。また、ＥＣＭ－ＣＡＳ生成手段１１は、共通情報を、ＭＰＥＧ（Moving Picture Experts Group）－２　Ｓｙｓｔｅｍｓで定義されるＥＣＭ（Entitlement Control Message）構造を有するメッセージとして生成する。このように生成された共通情報（ＥＣＭ－ＣＡＳ）は、多重化手段２２に出力される。

【００３７】
なお、ワーク鍵Ｋｗは、スクランブル鍵Ｋｓに比べ、更新時間が長く、例えば、１ヶ月程度で更新されるものである。ここでは、ワーク鍵Ｋｗは、図示を省略した記憶手段に記憶され、適宜、外部から新たなワーク鍵Ｋｗが入力されることで更新されるものとする。
【００３８】
ＥＭＭ－ＣＡＳ生成手段１２は、ＥＣＭ－ＣＡＳ生成手段１１で用いたワーク鍵Ｋｗをマスタ鍵Ｋｍで暗号化し、暗号化されたワーク鍵Ｋｗを含む個別情報を生成するものである。この個別情報は、デジタル放送受信装置３ごとに個別のセキュリティ情報である。
【００３９】
このマスタ鍵Ｋｍによる暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。また、ＥＭＭ－ＣＡＳ生成手段１２は、個別情報を、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで定義されるＥＭＭ（Entitlement Management Message）構造を有するメッセージとして生成する。このとき、個別情報（ＥＭＭ－ＣＡＳ）には、個々のデジタル放送受信装置３を識別するための識別子ＩＤが付加される。このように生成された個別情報（ＥＭＭ－ＣＡＳ）は、多重化手段２２に出力される。
【００４０】
なお、マスタ鍵Ｋｍは、デジタル放送受信装置３ごとに異なり、予め個々のデジタル放送受信装置３に配布されている暗号鍵である。ここでは、マスタ鍵Ｋｍは、図示を省略した記憶手段に記憶されているものとする。
【００４１】
ＥＣＭ－ＣＡＳ生成手段１１が生成する共通情報（ＥＣＭ－ＣＡＳ）や、ＥＭＭ－ＣＡＳ生成手段１２が生成する個別情報（ＥＭＭ－ＣＡＳ）は、受信契約がなされているデジタル放送受信装置３のみがスクランブルを解くことが可能な限定受信のためのセキュリティ情報である。
【００４２】
配信データ生成手段１３は、デジタル放送受信装置３に配信するＣＡＳプログラムＰを、データカルーセルのデータ形式に変換し、配信用のデータ（配信データ）を生成するものである。この配信データ生成手段１３で生成された配信データは、配信データスクランブル手段１４に出力される。
なお、配信データ生成手段１３には、図示を省略した入力手段を介して、更新を行う新たなＣＡＳプログラムが入力されるものとする。
【００４３】
ここで、図３を参照して、配信データ生成手段１３の構成について詳細に説明する。図３に示すように、配信データ生成手段１３は、署名値演算手段１３ａと、分割手段１３ｂと、暗号化手段１３ｃと、データカルーセル用データ生成手段１３ｄと、を備えている。
【００４４】
署名値演算手段１３ａは、更新を行う新たなＣＡＳプログラムＰに対して、デジタル署名の署名値を演算するものである。すなわち、署名値演算手段１３ａは、予めデジタル放送受信装置３と共通のハッシュ関数によって、ＣＡＳプログラムＰからハッシュ値を生成する。そして、署名値演算手段１３ａは、公開鍵暗号方式におけるデジタル放送受信装置３の公開鍵（検証鍵）に対応する秘密鍵Ｋｐｓで、ハッシュ値を暗号化することで署名値を演算する。このように演算された署名値は、データカルーセル用データ生成手段１３ｄに出力される。この署名値演算手段１３ａが生成する署名値は、一般的なＤＳＡ、ＲＳＡによって演算することができる。
【００４５】
なお、署名値演算手段１３ａが署名値を演算するために用いた秘密鍵Ｋｐｓに対応したデジタル署名を検証する公開鍵（検証鍵）は、ルート公開鍵証明書ＲＰＫＣ（図２参照）として、後記するＥＭＭ－ＲＭＰ生成手段１９によって、ＥＭＭ－ＲＭＰでデジタル放送受信装置３に配信される。
【００４６】

分割手段１３ｂは、更新を行う新たなＣＡＳプログラムＰを所定の大きさに分割するものである。ここでは、分割手段１３ｂは、データカルーセル伝送を行う際のＤＤＢ（Download Data Block）メッセージのブロックサイズで、ＣＡＳプログラムＰを分割する。このように分割されたデータ（分割データ）は、暗号化手段１３ｃに出力される。

【００４７】

暗号化手段１３ｃは、分割手段１３ｂで分割されたＣＡＳプログラムＰ（分割データ）を、プログラム暗号化鍵Ｋｐｅで暗号化するものである。この暗号化手段１３ｃにおける暗号化は、一般的な共通鍵暗号アルゴリズムを用いればよい。

このプログラム暗号化鍵Ｋｐｅは、すべてのデジタル放送受信装置３で共通の鍵であって、図示を省略した記憶手段に記憶しておく。このように暗号化された分割データ（暗号化分割データ）は、データカルーセル用データ生成手段１３ｄに出力される。

【００４８】

なお、プログラム暗号化鍵Ｋｐｅは、後記するＥＭＭ－ＲＭＰ生成手段１９において、ＥＭＭ－ＲＭＰを生成する際に、予めデジタル放送受信装置３内に記憶されているデバイス鍵Ｋｄで暗号化される。しかし、デジタル放送受信装置３からデバイス鍵Ｋｄが漏洩した場合、プログラム暗号化鍵Ｋｐｅが解読され、ＣＡＳプログラムＰそのものが漏洩してしまうことになる。

そこで、このプログラム暗号化鍵Ｋｐｅは、デバイス鍵Ｋｄが漏洩した場合、あるいは、定期的に、更新されるものとする。

【００４９】

データカルーセル用データ生成手段１３ｄは、暗号化手段１３ｃで暗号化されたＣＡＳプログラムＰの分割データ（暗号化分割データ）から、データカルーセル用のデータを生成するものである。すなわち、データカルーセル用データ生成手段１３ｄは、暗号化分割データをＤＤＢメッセージとしてセクション化するとともに、その構成情報をＤＩＩ（Download Info Indication）メッセージとしてセクション化する。

【００５０】

また、データカルーセル用データ生成手段１３ｄは、ＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）やバージョン（ＣＡＳ－Ｖｅｒ）を外部から入力し、ＤＩＩ内部に配置する。これによって、データカルーセルで配信するＣＡＳプログラムの識別子やバージョンを、デジタル放送受信装置３に通知することができる。

【００５１】

また、データカルーセル用データ生成手段１３ｄは、ＤＩＩをセクション化する際に、署名値演算手段１３ａで演算されたＣＡＳプログラムＰの署名値をＤＩＩ内部に配置する。これによって、デジタル放送受信装置３は、データカルーセルによって受信したＣＡＳプログラムＰが、正規なものであるか否かをデジタル署名により検証することが可能になる。

【００５２】

ここで、図５，図６を参照（適宜図２，図３参照）して、配信データ生成手段１３が生成するＤＩＩおよびＤＤＢのデータ構造の例について説明する。なお、ＡＲＩＢのＳＴＤ－Ｂ２４で規定されているデータについては説明を省略し、本発明において、特に設定を必要とするデータについて説明を行うこととする。

【００５３】

図５は、ＣＡＳプログラムをデータカルーセル伝送する際のＤＩＩメッセージのデータ構造の一例を示している。

この図５に示すように、デジタル放送送信装置１は、ＤＩＩメッセージ内に、コンパチビリティ記述子を配置する。このコンパチビリティ識別子は、ＤＤＢで配信するＣＡＳプログラムＰのメタ情報を記述するものである。ここでは、コンパチビリティ記述子内（図５中、「ＣＡＳ＿ｖｅｒｓｉｏｎ」領域）に、ＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）と、バージョン（ＣＡＳ－Ｖｅｒ）とを記述する。なお、この識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）は、ＣＡＳプログラムＰのダウンロード時に外部

から入力され、データカルーセル用データ生成手段１３ｄによって書き込まれる情報である。

【００５４】

また、図５に示すように、デジタル放送送信装置１は、ＤＩＩメッセージ内（「ＣＡＳ＿ｄｉｇｉｔａｌ＿ｓｉｇｎａｔｕｒｅ」領域）に、ＣＡＳプログラムＰの署名値を配置する。なお、この署名値は、配信データ生成手段１３の署名値演算手段１３ａによって生成され、データカルーセル用データ生成手段１３ｄによって書き込まれる情報である。

【００５５】

図６は、ＣＡＳプログラムＰをデータカルーセル伝送する際のＤＤＢメッセージのデータ構造の一例を示している。

この図６に示すように、デジタル放送送信装置１は、ＤＤＢメッセージ内（「ｂｌｏｃｋＤａｔａＢｙｔｅ」領域；ペイロード領域）に、分割暗号化されたＣＡＳプログラムＰを配置する。なお、このペイロード領域のデータは、配信データ生成手段１３の暗号化手段１３ｃによって暗号化され、データカルーセル用データ生成手段１３ｄによって書き込まれる情報である。

【００５６】

また、デジタル放送送信装置１は、ＤＤＢメッセージ内（ここでは、「ｂｌｏｃｋＮｕｍｂｅｒ」領域）に分割されたＣＡＳプログラムＰのブロックの順番を示す数（ブロックナンバ）を配置する。なお、このブロックナンバは、配信データ生成手段１３のデータカルーセル用データ生成手段１３ｄによって、順次、ブロックごとにインクリメントされて書き込まれる情報である。

これによって、デジタル放送受信装置３は、ＤＩＩメッセージを取得後、ＤＤＢメッセージによって、暗号化されたＣＡＳプログラムを再構成することが可能になる。

図２に戻って、デジタル放送送信装置１の構成について説明を続ける。

【００５７】

配信データスクランブル手段１４は、配信データ生成手段１３で生成されたデータカルーセル用のデータである配信データ（ＤＩＩ、ＤＤＢ）を、スクランブル鍵Ｋｓ２でスクランブル（暗号化）するものである。

このスクランブル鍵Ｋｓ２による暗号化は、一般的な共通鍵暗号アルゴリズムを用いればよく、例えば、ＭＵＬＴＩ２暗号により暗号化する。このようにスクランブルされたデータ（暗号化配信データＳｃａｓ）は、多重化手段２２に出力される。

【００５８】

なお、スクランブル鍵Ｋｓ２は、スクランブル鍵Ｋｓ１と同様、時間によって更新されるものであって、数秒に１回程度更新されるものである。また、スクランブル鍵Ｋｓ２は、スクランブル鍵Ｋｓ１と同じものを用いてもよいが、ＣＡＳプログラムの安全性を高めるため、スクランブル鍵Ｋｓ１よりも鍵長を長くする等、別の鍵として管理することが望ましい。ここでは、スクランブル鍵Ｋｓ２は、図示を省略した記憶手段に記憶され、適宜、外部から新たなスクランブル鍵Ｋｓ２が入力されることで更新されるものとする。

【００５９】

ＥＣＭ－ＲＭＰ生成手段（共通情報生成手段）１５は、配信データスクランブル手段１４で用いたスクランブル鍵Ｋｓ２を伝送路保護鍵Ｋｐで暗号化し、暗号化されたスクランブル鍵Ｋｓ２を含む共通情報を生成するものである。この共通情報は、すべてのデジタル放送受信装置３に共通のセキュリティ情報である。

【００６０】

この伝送路保護鍵Ｋｐによる暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。また、ＥＣＭ－ＲＭＰ生成手段１５は、共通情報を、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで定義されるＥＣＭ構造を有するメッセージとして生成する。このように生成された共通情報（ＥＣＭ－ＲＭＰ）は、多重化手段２２に出力される。

なお、伝送路保護鍵Ｋｐは、受信契約にかかわらず正規のデジタル放送受信装置３に配送される鍵である。ここでは、伝送路保護鍵Ｋｐは、図示を省略した記憶手段に記憶され

、適宜、外部から新たな伝送路保護鍵Ｋｐが入力されることで更新されるものとする。

【００６１】

また、ＥＣＭ－ＲＭＰ生成手段１５は、後記する起動プログラム指定手段２１によって起動したいＣＡＳプログラムを指定する場合、ＰＳＩ／ＳＩで配送されるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）やバージョン（ＣＡＳ－Ｖｅｒ）、および、ＣＡＳプログラムＰのハッシュ値（ＣＡＳ－Ｈ）を、共通情報（ＥＣＭ－ＲＭＰ）に付加することとする。なお、このハッシュ値は、デジタル放送受信装置３と共通のハッシュ関数を用いて演算した値である。

【００６２】

これによって、デジタル放送受信装置３では、ＰＳＩ／ＳＩで配送されるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）やバージョン（ＣＡＳ－Ｖｅｒ）の改ざんによる誤動作を防止したり、デジタル放送受信装置３に蓄積したＣＡＳプログラムＰのハッシュ値の不整合を検出して誤動作を防止したりすることができる。

【００６３】

デバイス鍵リスト記憶手段１６は、デジタル放送受信装置３に固有のデバイス鍵と、当該デバイス鍵が有効か無効かを示す情報とを対応付けて記憶するものであって、一般的なハードディスク等の記憶装置である。

ここでは、デバイス鍵リスト記憶手段１６は、デジタル放送受信装置３のメーカごと、あるいは、デジタル放送受信装置３の機種（セットモデル）ごとの固有の識別子である受信機識別子ＲＩＤに対して、デバイス鍵Ｋｄと、そのデバイス鍵Ｋｄが有効か無効かを示す情報（フラグ）とを対応付けて記憶しておく。例えば、有効なデバイス鍵Ｋｄについては、「有効」を示す値（“０”）、無効なデバイス鍵Ｋｄについては、「無効」を示す値（“１”）を設定する。

なお、このデバイス鍵リスト記憶手段１６には、初期値として、予めすべてのデバイス鍵について、「有効」の値が設定されているものとする。

【００６４】

ここで、デバイス鍵Ｋｄは、予めデジタル放送受信装置３に記憶され、後記するＥＭＭ－ＲＭＰ生成手段１９でＥＭＭ－ＲＭＰを生成する際に用いられるとともに、デジタル放送受信装置３において当該ＥＭＭ－ＲＭＰの情報を復号する鍵である。

例えば、図７に示すように、ある受信機識別子ＲＩＤ３において、デバイス鍵Ｋｄ３０が漏洩した場合、デバイス鍵リスト記憶手段１６のリスト中、デバイス鍵Ｋｄ３０には、「無効」が設定される。

【００６５】

なお、その後、新しいデバイス鍵Ｋｄ（Ｋｄ３１）が、受信機識別子ＲＩＤ３のデジタル放送受信装置３に配布された場合、デバイス鍵リスト記憶手段１６には、図示を省略した入力手段を介して、新しいデバイス鍵Ｋｄ３１が記憶され、「有効」が設定される。

ここで、新しいデバイス鍵Ｋｄは、後記するＥＭＭ－ＲＭＰ生成手段１９によって、デジタル放送受信装置３に通知されるシード（Ｓｅｅｄ：デバイス鍵を生成するためのパラメータ）と同じ値を基に、放送事業者が生成する。このデバイス鍵を生成するアルゴリズムは、デジタル放送受信装置３と同じアルゴリズムである。

【００６６】

なお、デジタル放送送信装置１内で、デバイス鍵を生成するのであれば、例えば、デジタル放送送信装置１内に、図示を省略したデバイス鍵生成手段を備え、デジタル放送受信装置３にシードを通知する前に、当該シードを用いて、デバイス鍵生成手段によって、デバイス鍵を生成し、デバイス鍵リスト記憶手段１６を更新、すなわち、前のデバイス鍵を「無効」、生成したデバイス鍵を「有効」に設定する。また、デバイス鍵生成手段（不図示）のデバイス鍵生成アルゴリズムは、後記するデジタル放送受信装置３のデバイス鍵生成・更新手段３１ｇと同一とする。

【００６７】

無効設定手段１７は、外部からの指示により、デバイス鍵リスト記憶手段１６において

、デバイス鍵Ｋｄを無効化するものである。
この無効設定手段１７は、外部から受信機識別子ＲＩＤおよびデバイス鍵Ｋｄを入力されることで、デバイス鍵リスト記憶手段１６に記憶されている対応するデバイス鍵Ｋｄの有効／無効フラグに「無効」を設定する。
【００６８】
デバイス鍵選択手段１８は、デバイス鍵リスト記憶手段１６に記憶されているデバイス鍵Ｋｄのうちで、無効化されていないデバイス鍵を選択するものである。すなわち、デバイス鍵選択手段１８は、図７に示したように、「有効」が設定されている有効なデバイス鍵Ｋｄを選択して、対応する受信機識別子ＲＩＤとともに、ＥＭＭ－ＲＭＰ生成手段１９に出力する。
これによって、ＥＭＭ－ＲＭＰを生成する際に、無効化されたデバイス鍵Ｋｄが使用されないことになる。
【００６９】
なお、図２中、破線部分で示したＡ部分の構成は、ＣＡＳプログラムごとに複数備えることとするため、例えば、配信するＣＡＳプログラムがデジタル放送受信装置３のメーカごとに異なる場合、デバイス鍵選択手段１８は、予め定めたメーカ固有の受信機識別子ＲＩＤに対応するデバイス鍵Ｋｄのみを選択することとする。
【００７０】
ＥＭＭ－ＲＭＰ生成手段（個別情報生成手段）１９は、プログラム暗号化鍵ＫｐｅおよびＥＣＭ－ＲＭＰ生成手段１５で用いた伝送路保護鍵Ｋｐを、デバイス鍵選択手段１８で選択されたデバイス鍵Ｋｄで暗号化し、対応する受信機識別子ＲＩＤ、暗号化されたプログラム暗号化鍵Ｋｐｅおよび伝送路保護鍵Ｋｐを含む個別情報を生成するものである。この個別情報は、デジタル放送受信装置３で共通のセキュリティ情報である。
【００７１】
このデバイス鍵Ｋｄによる暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。また、ＥＭＭ－ＲＭＰ生成手段１９は、個別情報を、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで定義されるＥＭＭ構造を有するＥＭＭ－ＲＭＰとして生成する。なお、このＥＭＭ－ＲＭＰには、配信データ生成手段１３で署名値を生成する際に用いた秘密鍵Ｋｐｓ（図３参照）に対応した公開鍵（検証鍵）に、予め認証局のデジタル署名を付加したルート公開鍵証明書ＲＰＫＣを付加することとする。
【００７２】
また、ＥＭＭ－ＲＭＰ生成手段１９は、外部から、デバイス鍵更新制御情報ＫＤｃを入力された場合、デバイス鍵更新制御情報ＫＤｃを含んだ識別子（デバイス鍵更新識別子）をＥＣＭ－ＲＭＰに付加することとする。
ここで、デバイス鍵更新制御情報ＫＤｃは、デジタル放送受信装置３で用いられるデバイス鍵Ｋｄの更新を指示するための情報である。このデバイス鍵更新制御情報ＫＤｃには、デバイス鍵Ｋｄを新たに生成するためのパラメータとなるシード（Ｓｅｅｄ）が含まれている。
これによって、デバイス鍵Ｋｄが漏洩した場合に、放送事業者が、放送波Ｗを介して、デジタル放送受信装置３のデバイス鍵の更新を制御することができる。
このようにＥＭＭ－ＲＭＰ生成手段１９で生成された共通情報（ＥＣＭ－ＲＭＰ）は、多重化手段２２に出力される。
【００７３】
ＥＣＭ－ＲＭＰ生成手段１５が生成する共通情報（ＥＣＭ－ＲＭＰ）や、ＥＭＭ－ＲＭＰ生成手段１９が生成する個別情報（ＥＭＭ－ＲＭＰ）は、正規のデジタル放送受信装置３のすべてがスクランブルを解くことができるセキュリティ情報である。
この共通情報（ＥＣＭ－ＲＭＰ）や個別情報（ＥＭＭ－ＲＭＰ）は、ＣＡＳプログラムＰを暗号配送するために用いられる情報としての役割を有している。
【００７４】
ダウンロードテーブル生成手段２０は、デジタル放送受信装置３がＣＡＳプログラムＰ

をダウンロードする際の各種情報を示す制御情報（ダウンロード制御情報Ｄｃ）を、図示を省略した入力手段を介して入力し、セクション形式のテーブル（ダウンロードテーブル）として生成するものである。

ここで、ダウンロード制御情報Ｄｃとは、配信対象のＣＡＳプログラムＰを特定するための識別情報である。例えば、ＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）、バージョン（ＣＡＳ－Ｖｅｒ）等である。

【００７５】

ここでは、さらに、ダウンロード制御情報Ｄｃとして、放送によってＣＡＳプログラムＰを配信するか、通信によってＣＡＳプログラムＰを配信するかのいずれかを識別するための情報を含ませることとする。例えば、放送（データカルーセル）によってＣＡＳプログラムＰを配信する場合、ＤＩＩ／ＤＤＢのモジュール数、モジュール識別、モジュールサイズ等を含ませ、通信によってＣＡＳプログラムＰを配信する場合、ＣＡＳプログラムＰを保持しているＣＡＳサーバ５のＵＲＬ、ＩＰアドレス等を含ませることとする。

【００７６】

なお、放送によってＣＡＳプログラムＰを配信するか、通信によってＣＡＳプログラムＰを配信するかは、適宜、操作者（放送事業者）が設定することで切り替えるものとする。例えば、新たにＣＡＳプログラムを配信する場合、放送によって一斉にＣＡＳプログラムを配信し、一定期間（例えば、１週間）経過後、通信による配信に切り替える。これによって、ＣＡＰプログラムを放送によって長期間にわたって送り続ける必要がなく、放送帯域への圧迫を低減することができる。

【００７７】

ここで、図８～図１０を参照（適宜図２参照）して、ダウンロードテーブル生成手段２０が生成するダウンロードテーブルのデータ構造の例について説明する。なお、図８～図１０に示したダウンロードテーブル、ダウンロードコンテンツ記述子、ネットワークダウンロードコンテンツ記述子は、既存のデジタル放送において使用されているセクション形式に準拠してデータ配置したテーブル、記述子の例を示している。よって、ここでは、本発明に直接関係するデータについてのみ説明を行う。

【００７８】

図８に示すように、ダウンロードテーブルに、「ｔａｒｇｅｔ＿ｖｅｒｓｉｏｎ（ターゲットバージョン）」領域を設け、ダウンロードテーブル生成手段２０は、更新対象のＣＡＳプログラムのバージョンを設定する。これによって、デジタル放送受信装置３では、自身が保持するＣＡＳプログラムが更新対象となっているか否かを判定し、必要に応じてＣＡＳプログラムをダウンロードすることができる。

また、ダウンロードテーブルに、「ｎｅｗ＿ｖｅｒｓｉｏｎ（新バージョン）」領域を設け、ダウンロードテーブル生成手段２０は、今回更新するＣＡＳプログラムのバージョンを設定する。これによって、当該ＣＡＳプログラムをダウンロードしたデジタル放送受信装置３は、自身が保持するＣＡＳプログラムのバージョンを管理することができる。なお、このＣＡＳプログラムのバージョンは、配信データ生成手段１３で設定されるバージョン（ＣＡＳ－Ｖｅｒ）と同一の値である。

【００７９】

また、ダウンロードテーブルに、「ｄｏｗｎｌｏａｄ＿ｌｅｖｅｌ（ダウンロードレベル）」領域を設け、デジタル放送受信装置３において、更新を強制的に行うか、任意に行うかを制御することとしてもよい。例えば、「ダウンロードレベル」の値が“０１”の場合、「更新対象バージョン」のＣＡＳプログラムを保持するデジタル放送受信装置３は、必ずＣＡＳプログラムの更新を行う。一方、「ダウンロードレベル」の値が“００”の場合には、「更新対象バージョン」のＣＡＳプログラムを保持するデジタル放送受信装置３は、任意にＣＡＳプログラムの更新を行う。

【００８０】

また、ダウンロードテーブルに、「ｖｅｒｓｉｏｎ＿ｉｎｄｉｃａｔｉｏｎ（バージョン表示）」領域を設け、更新対象となるＣＡＳプログラムをバージョンによって制御する

こととしてもよい。例えば、「バージョン表示」の値が“００”の場合、「ターゲットバージョン」の指定を無効とし、すべてのバージョンのＣＡＳプログラムを更新対象とする。また、「バージョン表示」の値が“０１”の場合、「ターゲットバージョン」で指定されたバージョン以降のＣＡＳプログラムを更新対象とする。また、「バージョン表示」の値が“０２”の場合、「ターゲットバージョン」で指定されたバージョン以前のＣＡＳプログラムを更新対象とする。また、「バージョン表示」の値が“０３”の場合、「ターゲットバージョン」で指定されたバージョンのみのＣＡＳプログラムを更新対象とする。

【００８１】

また、図８に示すように、ダウンロードテーブルに、「ｄｅｓｃｒｉｐｔｏｒ（）（記述子）」領域を設け、ダウンロードテーブル生成手段２０は、放送（データカルーセル）によってＣＡＳプログラムＰを配信する場合、この記述子領域に「ダウンロードコンテンツ記述子」を配置する。また、通信によってＣＡＳプログラムＰを配信する場合、この記述子領域に「ネットワークダウンロードコンテンツ記述子」を配置する。

【００８２】

このように、記述子領域に「ダウンロードコンテンツ記述子」を配置することで、デジタル放送受信装置３は、放送（データカルーセル）によってＣＡＳプログラムＰを取得し、「ネットワークダウンロードコンテンツ記述子」を配置することで、デジタル放送受信装置３は、通信によってＣＡＳサーバ５（図１参照）からＣＡＳプログラムＰを取得する。

以下、「ダウンロードコンテンツ記述子」および「ネットワークダウンロードコンテンツ記述子」について説明を行う。

【００８３】

まず、図９を参照して、ダウンロードコンテンツ記述子のデータ構造の例について説明する。図９に示すように、ダウンロードコンテンツ記述子は、ＣＡＳプログラムを、データカルーセルによって受信する際に必要となる各種情報を設定した記述子である。例えば、ＣＡＳプログラムを伝送するデータカルーセルのＤＩＩ／ＤＤＢのモジュール数、モジュール識別、モジュールサイズ等である。また、ここでは、ダウンロードコンテンツ記述子にＤＩＩメッセージ（図５参照）に配置したものと同じコンパチビリティ記述子を配置する。このコンパチビリティ記述子は、図５に示したように、ＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）、バージョン（ＣＡＳ－Ｖｅｒ）を含んでいるため、デジタル放送受信装置３において、すでに対象となるＣＡＳプログラムが蓄積されていれば、ダウンロードを行わないように制御することができる。

【００８４】

次に、図１０を参照して、ネットワークダウンロード識別子のデータ構造の例について説明する。図１０に示すように、ネットワークダウンロードコンテンツ記述子は、ＣＡＳプログラムを、ネットワークを介して受信する際に必要となる各種情報を設定した記述子である。例えば、ＣＡＳプログラムを提供する通信サーバ（ＣＡＳサーバ）のＵＲＬまたはＩＰアドレス等である。また、ここでは、ネットワークダウンロードコンテンツ記述子は、ダウンロードコンテンツ記述子と同様、ＤＩＩメッセージ（図５参照）に配置したものと同じコンパチビリティ記述子を配置する。これによって、デジタル放送受信装置３は、すでに対象となるＣＡＳプログラムが蓄積されていれば、サーバからのＣＡＳプログラムの取得を行わないように制御することができる。

図２に戻って、デジタル放送送信装置１の構成について説明を続ける。

【００８５】

起動プログラム指定手段２１は、デジタル放送受信装置３において起動させたいＣＡＳプログラムを指定するものである。この起動プログラム指定手段２１は、ＰＳＩ／ＳＩ（番組配列情報）に、デジタル放送受信装置３において起動させたいＣＡＳプログラムを指定するための情報（プログラム指定情報）を付加する。このプログラム指定情報は、ＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）およびそのバージョン（ＣＡＳ－Ｖｅｒ）とする。これによって、デジタル放送送信装置１は、デジタル放送受信装置３において、指定し

たＣＡＳプログラムを起動させることが可能になる。

【００８６】

なお、起動プログラム指定手段２１は、プログラム指定情報を、ＰＳＩ／ＳＩのＣＡＴ（Conditional Access Table）またはＰＭＴ（Program Map Table）に配置することとする。ここで、ＣＡＴに配置するかＰＭＴに配置するかは、予め定めておくこととする。

このＣＡＴまたはＰＭＴには、それぞれのテーブルの記述子領域に、例えば、ＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）およびそのバージョン（ＣＡＳ－Ｖｅｒ）を含んだコンパチビリティ記述子（図５参照）を配置する。

このように、プログラム指定情報が付加されたＰＳＩ／ＳＩは、多重化手段２２に出力される。

【００８７】

多重化手段２２は、コンテンツスクランブル手段１０が生成した暗号化コンテンツＳｃｔと、ＥＣＭ－ＣＡＳ生成手段１１が生成した共通情報（ＥＣＭ－ＣＡＳ）と、ＥＭＭ－ＣＡＳ生成手段１２が生成した個別情報（ＥＭＭ－ＣＡＳ）と、配信データスクランブル手段１４が生成した暗号化配信データ（ＤＩＩ，ＤＤＢ）Ｓｃａｓと、ＥＣＭ－ＲＭＰ生成手段１５が生成した共通情報（ＥＣＭ－ＲＭＰ）と、ＥＭＭ－ＲＭＰ生成手段１９が生成した個別情報（ＥＭＭ－ＲＭＰ）と、ダウンロードテーブル生成手段２０が生成したダウンロードテーブルＴｄと、起動プログラム指定手段２１によってプログラム指定情報が付加されたＰＳＩ／ＳＩとを多重化して、多重化信号を生成するものである。

【００８８】

ここでは、多重化手段２２は、入力された各情報を、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで定義されるＴＳ（トランスポートストリーム）の形式（ＭＰＥＧ－２　ＴＳ）に多重化するものとする。この多重化された多重化信号（ＭＰＥＧ－２　ＴＳ）は、送出装置（図示せず）によって、放送波を介して、デジタル放送受信装置３に配信される。

【００８９】

このようにデジタル放送送信装置１を構成することで、ＣＡＳプログラムＰを、データカルーセルでデジタル放送受信装置３に配信することができる。また、このとき、ＣＡＳプログラムＰを暗号復号するための情報や、検証するための情報を、ＥＣＭ－ＲＭＰやＥＭＭ－ＲＭＰによってデジタル放送受信装置３に配信するため、ＣＡＳプログラムＰの安全性を高めて、配信することができる。

【００９０】

また、デジタル放送送信装置１は、漏洩したデバイス鍵をリスト化（ブラックリスト化）して記憶し、漏洩したデバイス鍵Ｋｄでは個別情報（ＥＭＭ－ＲＭＰ）を生成しないため、伝送路保護鍵Ｋｐやプログラム暗号化鍵Ｋｐｅを、デバイス鍵Ｋｄが漏洩していないデジタル放送受信装置３に配信することができる。

【００９１】

これによって、たとえ、デバイス鍵Ｋｄおよびプログラム暗号化鍵Ｋｐｅが漏洩した場合であっても、伝送路保護鍵Ｋｐやプログラム暗号化鍵Ｋｐｅを更新し、新たなＣＡＳプログラムＰを、放送または通信で配信することで、デバイス鍵Ｋｄを漏洩したデジタル放送受信装置３を無効化（リボーク）するとともに、新しいＣＡＳプログラムＰの漏洩を防ぐことができる。

【００９２】

さらに、デジタル放送送信装置１は、ＣＡＳプログラムＰの配信を、放送によるデータカルーセル伝送から、ＣＡＳサーバ５を用いた通信による配信に切り替えることができる。これによって、デジタル放送送信装置１は、長期間にわたる放送帯域の使用の無駄を防止することができる。

なお、デジタル放送送信装置１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（ＣＡＳプログラム送信プログラム）により動作させることができる。

【００９３】

［デジタル放送受信装置の構成］

次に、図４を参照（適宜図１参照）して、本発明の実施形態に係るデジタル放送受信装置の構成について説明する。ここでは、デジタル放送受信装置３は、分離手段３０と、プログラム実行手段３１と、ダウンロードテーブル解析手段３２と、配信データ分離手段３３と、プログラム復号手段３４と、記憶手段３５と、起動プログラム特定手段３６と、プログラム起動手段３７と、通信ダウンロード手段３８と、を備えている。

【００９４】

分離手段３０は、デジタル放送送信装置１から送信されたデジタル放送（多重化信号；ＭＰＥＧ－２　ＴＳ）を分離するものである。この分離手段３０は、ＭＰＥＧ－２　ＴＳから、暗号化コンテンツＳｃｔと、限定受信用の情報を含んだ個別情報（ＥＭＭ－ＣＡＳ）および共通情報（ＥＣＭ－ＣＡＳ）と、ＣＡＳプログラムの暗号伝送用の情報を含んだ個別情報（ＥＭＭ－ＲＭＰ）および共通情報（ＥＣＭ－ＲＭＰ）と、データカルーセルのデータ（暗号化配信データＳｃａｓ）と、ダウンロードテーブルＴｄと、ＰＳＩ／ＳＩのＣＡＴまたはＰＭＴと、を分離する。

また、分離手段３０は、ダウンロードテーブル解析手段３２から、データカルーセルのデータを分離する旨の指示を通知された段階で、ＭＰＥＧ－２　ＴＳから、データカルーセルのデータ（ＤＩＩ，ＤＤＢ）を分離する。

【００９５】

プログラム実行手段３１は、分離手段３０で分離された暗号化コンテンツＳｃｔや暗号化配信データＳｃａｓを復号するものである。

このプログラム実行手段３１は、デジタル放送送信装置１から配信されるＣＡＳプログラムの実体であって、後記するプログラム起動手段３７によって実行される。なお、このプログラム実行手段３１は、ＦＰＧＡ（Field Programmable Gate Array）等のプログラマブルデバイスで構成してもよいし、ＯＳ（Operating System）上のミドルウェアで動作する仮想マシン、例えば、Ｊａｖａ（登録商標）仮想マシン（Java Virtual Machine,Java VM）等で構成してもよい。

【００９６】

プログラマブルデバイスでプログラム実行手段３１を構成する場合、ＣＡＳプログラムは、回路情報で構成されることになる。また、ＯＳ上で動作するソフトウェアとしてプログラム実行手段３１を構成する場合、ＣＡＳプログラムは、バイナリプログラムで構成されることになる。

【００９７】

ここでは、プログラム実行手段３１は、ＥＭＭ－ＣＡＳ復号手段３１ａと、ＥＣＭ－ＣＡＳ復号手段３１ｂと、コンテンツデスクランブル手段３１ｃと、ＥＭＭ－ＲＭＰ復号手段３１ｄと、ＥＣＭ－ＲＭＰ復号手段３１ｅと、配信データデスクランブル手段３１ｆと、デバイス鍵生成・更新手段３１ｇと、を備えている。

【００９８】

ＥＭＭ－ＣＡＳ復号手段３１ａは、分離手段３０で分離された個別情報（ＥＭＭ－ＣＡＳ）をマスタ鍵Ｋｍで復号するものである。このＥＭＭ－ＣＡＳ復号手段３１ａは、ＥＭＭ－ＣＡＳの非暗号化領域に含まれているデジタル放送受信装置３を識別するための識別子が、予め記憶手段３５に記憶されている識別子（不図示）と一致する場合にのみ、予め記憶手段３５に記憶されているマスタ鍵Ｋｍで、ＥＭＭ－ＣＡＳの暗号化領域を復号し、ワーク鍵Ｋｗを抽出する。これによって、正規に契約した受信装置においてのみ、ワーク鍵Ｋｗを復号することができる。

このＥＭＭ－ＣＡＳ復号手段３１ａで復号されたワーク鍵Ｋｗは、ＥＣＭ－ＣＡＳ復号手段３１ｂに出力される。

【００９９】

ＥＣＭ－ＣＡＳ復号手段３１ｂは、分離手段３０で分離された共通情報（ＥＣＭ－ＣＡＳ）を、ＥＭＭ－ＣＡＳ復号手段３１ａで復号されたワーク鍵Ｋｗで復号するものである。このＥＣＭ－ＣＡＳには、暗号化コンテンツＳｃｔをスクランブルする際に用いたスクランブル鍵Ｋｓ１が含まれており、ＥＣＭ－ＣＡＳ復号手段３１ｂは、ＥＣＭ－ＣＡＳを

復号することで、スクランブル鍵Ｋｓ１を抽出する。
このＥＣＭ－ＣＡＳ復号手段３１ｂで復号されたスクランブル鍵Ｋｓ１は、コンテンツデスクランブル手段３１ｃに出力される。
【０１００】
コンテンツデスクランブル手段３１ｃは、分離手段３０で分離された暗号化コンテンツＳｃｔを、ＥＣＭ－ＣＡＳ復号手段３１ｂで復号されたスクランブル鍵Ｋｓ１でデスクランブル（復号）するものである。このコンテンツデスクランブル手段３１ｃでデスクランブルされたコンテンツＣｔは、図示を省略した映像・音声デコード手段によってデコード（符号復号）されて、表示装置（不図示）に出力される。
【０１０１】
ＥＭＭ－ＲＭＰ復号手段（個別情報復号手段）３１ｄは、分離手段３０で分離された個別情報（ＥＭＭ－ＲＭＰ）をデバイス鍵Ｋｄで復号するものである。このＥＭＭ－ＲＭＰ復号手段３１ｄは、ＥＭＭ－ＲＭＰの非暗号化領域に含まれているデジタル放送受信装置３を識別するための受信機識別子ＲＩＤが、予め記憶手段３５に記憶されている識別子（不図示）と一致する場合にのみ、予め記憶手段３５に記憶されているデバイス鍵Ｋｄで、ＥＭＭ－ＲＭＰの暗号化領域を復号し、伝送路保護鍵Ｋｐを抽出する。
このＥＭＭ－ＲＭＰ復号手段３１ｄで復号された伝送路保護鍵Ｋｐは、ＥＣＭ－ＲＭＰ復号手段３１ｅに出力される。
【０１０２】
なお、ＥＭＭ－ＲＭＰ復号手段３１ｄは、ＥＭＭ－ＲＭＰにルート公開鍵証明書ＲＰＫＣが含まれている場合、ルート公開鍵証明書ＲＰＫＣを抽出し、記憶手段３５または図示を省略した耐タンパモジュールに記憶しておく。
また、ＥＭＭ－ＲＭＰ復号手段３１ｄは、ＥＭＭ－ＲＭＰにプログラム暗号化鍵Ｋｐｅが含まれている場合、プログラム暗号化鍵Ｋｐｅを抽出し、記憶手段３５または図示を省略した耐タンパモジュールに記憶しておく。
また、ＥＭＭ－ＲＭＰに、デバイス鍵更新識別子が含まれている場合、このデバイス鍵更新識別子に含まれているデバイス鍵Ｋｄを生成するためのシード（Ｓｅｅｄ）を、デバイス鍵生成・更新手段３１ｇに出力する。
【０１０３】
ＥＣＭ－ＲＭＰ復号手段（共通情報復号手段）３１ｅは、分離手段３０で分離された共通情報（ＥＣＭ－ＲＭＰ）を、ＥＭＭ－ＲＭＰ復号手段３１ｄで復号された伝送路保護鍵Ｋｐで復号するものである。このＥＣＭ－ＲＭＰには、配信データ（ＤＩＩ、ＤＤＢ）をスクランブルする際に用いたスクランブル鍵Ｋｓ２が含まれており、ＥＣＭ－ＲＭＰ復号手段３１ｅは、ＥＣＭ－ＲＭＰを復号することで、スクランブル鍵Ｋｓ２を抽出する。
【０１０４】
このＥＣＭ－ＲＭＰ復号手段３１ｅで復号されたスクランブル鍵Ｋｓ２は、配信データデスクランブル手段３１ｆに出力される。
なお、ＥＣＭ－ＲＭＰに、ＰＳＩ／ＳＩで配送されるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）やバージョン（ＣＡＳ－Ｖｅｒ）、および、ＣＡＳプログラムＰのハッシュ値（ＣＡＳ－Ｈ）が付加されている場合、ＥＣＭ－ＲＭＰ復号手段３１ｅは、これらの識別情報（ＣＡＳ－ＩＤ、ＣＡＳ－Ｖｅｒ、ＣＡＳ－Ｈ）を、プログラム起動手段３７に出力する。
【０１０５】
配信データデスクランブル手段３１ｆは、分離手段３０で分離されたデータカルーセルのデータ（暗号化配信データＳｃａｓ）を、ＥＣＭ－ＲＭＰ復号手段３１ｅで復号されたスクランブル鍵Ｋｓ２でデスクランブル（復号）するものである。この配信データデスクランブル手段３１ｆでデスクランブルされた配信データ（ＤＩＩ，ＤＤＢ）ｃａｓは、配信データ分離手段３３に出力される。
【０１０６】
デバイス鍵生成・更新手段３１ｇは、個別情報（ＥＭＭ－ＲＭＰ）を復号するデバイス

鍵Ｋｄを新たに生成し、更新するものである。
このデバイス鍵生成・更新手段３１ｇは、ＥＭＭ－ＲＭＰ復号手段３１ｄから、シード（Ｓｅｅｄ）を通知された段階で、デバイス鍵Ｋｄを新たに生成する。ここでは、デバイス鍵生成・更新手段３１ｇは、例えば、デバイス鍵Ｋｄとして、擬似乱数を生成するもので、シードを基に乱数を生成する。このように生成された乱数は、新たなデバイス鍵Ｋｄとして、記憶手段３５に記憶しておく。
また、デバイス鍵生成・更新手段３１ｇが、デバイス鍵を生成するアルゴリズム（乱数発生アルゴリズム）は、予め放送事業者のデバイス鍵生成アルゴリズムと同一とする。
【０１０７】
なお、ここでは、デバイス鍵生成・更新手段３１ｇを、プログラム実行手段３１内部、すなわち、ＣＡＳプログラムの内部の構成として実現したが、ＣＡＳプログラムの外部、すなわち、デジタル放送受信装置３がもともの有する固有の手段として構成してもよい。その場合、デバイス鍵生成アルゴリズムの漏洩を防ぐため、デバイス鍵生成・更新手段３１ｇは、図示を省略した耐タンパモジュール内に構成することが望ましい。
【０１０８】
ダウンロードテーブル解析手段３２は、分離手段３０で分離されたセクション形式のダウンロードテーブルＴｄを解析し、ＣＡＳプログラムＰを放送によってダウンロードするのか、通信によってダウンロードするのかを判定するものである。
具体的には、ダウンロードテーブル解析手段３２は、図８で説明したダウンロードテーブルで、「ｄｅｓｃｒｉｐｔｏｒ（）（記述子）」領域に、放送によってダウンロードを行うことを示すダウンロードコンテンツ記述子（図９参照）が記述されているのか、通信によってダウンロードを行うことを示すネットワークダウンロードコンテンツ記述子（図１０参照）が記述されているのかを、記述子タグの値によって判定する。
【０１０９】
ここで、ダウンロードテーブルＴｄにダウンロードコンテンツ記述子が記述されている場合、ダウンロードテーブル解析手段３２は、分離手段３０に、ＰＭＴに配置されているデータカルーセルのパケット識別（ＰＩＤ）でフィルタリングすることで、データカルーセルのデータを配信データデスクランブル手段３１ｆに出力する旨を指示する。これによって、分離手段３０は、ＭＰＥＧ－２　ＴＳから、データカルーセルのデータ（ＤＩＩ，ＤＤＢ）を分離抽出して配信データデスクランブル手段３１ｆに出力する。
【０１１０】
一方、ダウンロードテーブルＴｄにネットワークダウンロードコンテンツ記述子が記述されている場合、ダウンロードテーブル解析手段３２は、ネットワークダウンロードコンテンツ記述子に記述されている通信サーバ（ＣＡＳサーバ５）のＵＲＬまたはＩＰアドレス、並びに、コンパチビリティ記述子に記述されているＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）を通信ダウンロード手段３８に出力する。これによって、通信ダウンロード手段３８が、ネットワーク（通信回線Ｎ）を介して、ＣＡＳプログラムＰのダウンロードを開始する。
【０１１１】
なお、ダウンロードテーブル解析手段３２は、ダウンロードテーブルＴｄに記述されている識別子（ＣＡＳ－ＩＤ）やバージョン（ＣＡＳ－Ｖｅｒ）に対応するＣＡＳプログラムＰが、すでに記憶手段３５に記憶されている場合は、ダウンロードの実行を行わないこととする。これによって、不要なダウンロード動作をなくすことができる。
さらに、ダウンロードテーブル解析手段３２は、図８で説明したように、ダウンロードテーブルＴｄの「ｔａｒｇｅｔ＿ｖｅｒｓｉｏｎ（ターゲットバージョン）」、「ｎｅｗ＿ｖｅｒｓｉｏｎ（新バージョン）」、「ｄｏｗｎｌｏａｄ＿ｌｅｖｅｌ（ダウンロードレベル）」、「ｖｅｒｓｉｏｎ＿ｉｎｄｉｃａｔｉｏｎ（バージョン表示）」を参照し、ダウンロードの可否を判定することとしてもよい。
【０１１２】
配信データ分離手段３３は、配信データデスクランブル手段３１ｆでデスクランブルさ

れたデータカルーセルのデータ（配信データｃａｓ）から、ＣＡＳプログラムＰ（暗号化されたＣＡＳプログラムＰ）を分離して抽出するものである。
すなわち、配信データ分離手段３３は、配信データｃａｓのＤＩＩメッセージから、次のＤＩＩメッセージまでのＤＤＢメッセージに含まれるデータ（図６中、「ｂｌｏｃｋＤａｔａＢｙｔｅ」領域のデータ）を連結することで、暗号化されたＣＡＳプログラムＰを分離して抽出する。

【０１１３】
さらに、配信データ分離手段３３は、ＤＩＩメッセージ内のコンパチビリティ記述子内（図５中、「ＣＡＳ＿ｖｅｒｓｉｏｎ」領域）のＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）を抽出するとともに、ＤＩＩメッセージ内（図５中、「ＣＡＳ＿ｄｉｇｉｔａｌ＿ｓｉｇｎａｔｕｒｅ」領域）のＣＡＳプログラムＰの署名値を抽出する。
この配信データ分離手段３３は、分離抽出した暗号化されたＣＡＳプログラムＰ、識別子（ＣＡＳ－ＩＤ）、バージョン（ＣＡＳ－Ｖｅｒ）および署名値を、プログラム復号手段３４に出力する。

【０１１４】
プログラム復号手段３４は、配信データ分離手段３３で分離抽出された暗号化されたＣＡＳプログラムＰ、または、通信ダウンロード手段３８を介してダウンロードした暗号化されたＣＡＳプログラムＰを復号するものである。ここでは、プログラム復号手段３４は、暗号復号手段３４ａと、署名検証手段３４ｂと、書込手段３４ｃと、を備えている。

【０１１５】
暗号復号手段３４ａは、配信データ分離手段３３または通信ダウンロード手段３８から入力した暗号化されたＣＡＳプログラムＰを、プログラム暗号化鍵Ｋｐｅで復号するものである。このプログラム暗号化鍵Ｋｐｅは、デジタル放送送信装置１において、ＣＡＳプログラムＰを暗号化したものと同一の鍵であって、ＥＭＭ－ＲＭＰ復号手段３１ｄによって復号された鍵である。
この復号されたＣＡＳプログラムＰは、署名検証手段３４ｂに出力される。

【０１１６】
署名検証手段３４ｂは、配信データ分離手段３３または通信ダウンロード手段３８から入力した、ＣＡＳプログラムＰに付加されているデジタル署名を検証するものである。
すなわち、署名検証手段３４ｂは、署名値演算手段１３ａ（図３参照）と共通のハッシュ関数によって、ＣＡＳプログラムＰのハッシュ値を生成する。そして、署名検証手段３４ｂは、ＣＡＳプログラムＰの署名値を記憶手段３５または図示を省略した耐タンパモジュールに記憶しているルート公開鍵証明書ＲＰＫＣに含まれる公開鍵（検証鍵）Ｋｐｐで復号する。この復号した値と、ＣＡＳプログラムＰのハッシュ値とが一致する場合に、署名検証手段３４ｂは、ダウンロードしたＣＡＳプログラムＰを、改ざん等がなされていない正規のものであると判定する。
この署名検証手段３４ｂは、ダウンロードしたＣＡＳプログラムＰの検証により、正規のＣＡＳプログラムＰのみを、書込手段３４ｃに出力する。

【０１１７】
書込手段３４ｃは、署名検証手段３４ｂから入力したＣＡＳプログラムＰを、配信データ分離手段３３または通信ダウンロード手段３８から入力したＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）と対応付けて記憶手段３５に書き込むものである。
このように、プログラム復号手段３４は、ダウンロードしたＣＡＳプログラムＰを署名検証することで、改ざん等がなされていないＣＡＳプログラムＰのみを記憶手段３５に書き込み蓄積する。

【０１１８】
記憶手段（プログラム記憶手段）３５は、ＣＡＳプログラムＰを識別子（ＣＡＳ－ＩＤ）とバージョン（ＣＡＳ－Ｖｅｒ）とに対応付けて複数記憶するものである。例えば、記

憶手段３５は、不揮発性メモリ等の一般的な記憶媒体である。
この記憶手段３５は、プログラム復号手段３４の書込手段３４ｃによって、識別子（ＣＡＳ－ＩＤ）とバージョン（ＣＡＳ－Ｖｅｒ）とに対応付けてＣＡＳプログラムＰが書き込まれ、後記するプログラム起動手段３７によって、識別子（ＣＡＳ－ＩＤ）とバージョン（ＣＡＳ－Ｖｅｒ）とをキーとしてＣＡＳプログラムＰが検索され読み出される。
なお、この記憶手段３５には、予め少なくとも１つのＣＡＳプログラムＰが記憶されており、他のＣＡＳプログラムがダウンロードされる。
【０１１９】
起動プログラム特定手段３６は、分離手段３０で分離されたＰＳＩ／ＳＩ（番組配列情報）のＣＡＴまたはＰＭＴから、プログラム指定情報であるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびそのバージョン（ＣＡＳ－Ｖｅｒ）を抽出し、起動するＣＡＳプログラムＰを特定するものである。
この抽出されたＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）は、プログラム起動手段３７に出力される。
【０１２０】
プログラム起動手段３７は、起動プログラム特定手段３６で特定されたＣＡＳプログラムＰを記憶手段３５から読み出して実行するものである。
このプログラム起動手段３７は、起動プログラム特定手段３６から通知される識別子（ＣＡＳ－ＩＤ）およびそのバージョン（ＣＡＳ－Ｖｅｒ）をキーとして、記憶手段３５において検索し、対応するＣＡＳプログラムＰを読み出す。そして、プログラム起動手段３７は、読み出したＣＡＳプログラムＰを、プログラム実行手段３１として起動する。
なお、初期起動時、すなわち、まだ、ＣＡＳプログラムＰがダウンロードされていない状態において、プログラム起動手段３７は、予め記憶手段３５に記憶されているＣＡＳプログラムＰを起動することとする。
【０１２１】
また、プログラム起動手段３７は、ＥＣＭ－ＲＭＰ復号手段３１ｅから通知される識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）と、起動プログラム特定手段３６から通知される識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）とが一致するか否かを判定し、一致しない場合、ＣＡＳプログラムの起動を行わないこととする。
これによって、プログラム起動手段３７は、ＰＳＩ／ＳＩで配信される識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）と、ＥＣＭ－ＲＭＰで送信される識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）とを比較することで、ＰＳＩ／ＳＩで配信される識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）が改ざんされて、ＣＡＳプログラムＰが誤動作することを防止することができる。
【０１２２】
さらに、プログラム起動手段３７は、読み出したＣＡＳプログラムＰのハッシュ値を計算し、当該ハッシュ値と、ＥＣＭ－ＲＭＰ復号手段３１ｅから通知されるＣＡＳプログラムＰのハッシュ値（ＣＡＳ－Ｈ）とが一致するか否かを判定し、一致しない場合、ＣＡＳプログラムＰの起動を行わないこととする。これによって、不正なＣＡＳプログラムＰの起動を防止することができる。なお、プログラム起動手段３７のハッシュ値の演算を行うハッシュ関数は、ＣＡＳプログラムＰの送信側と同じものとする。
【０１２３】
通信ダウンロード手段３８は、ダウンロードテーブル解析手段３２から通知される通信サーバから、ネットワーク（通信回線Ｎ）を介して、ＣＡＳプログラムＰをダウンロードするものである。この通信ダウンロード手段３８は、ダウンロードテーブル解析手段３２から通知される通信サーバ（ＣＡＳサーバ５）のＵＲＬまたはＩＰアドレス、並びに、ＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）に基づいて、指定された通信サーバ（ＣＡＳサーバ５）から、ＣＡＳプログラムをダウンロードする。
【０１２４】

この通信ダウンロード手段３８は、ダウンロードした暗号化されたＣＡＳプログラムＰ、並びに、ダウンロードテーブル解析手段３２から通知された識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）を、プログラム復号手段３４に出力する。なお、通信サーバ（ＣＡＳサーバ５）からダウンロードするＣＡＳプログラムＰには、署名値が付加されており、通信ダウンロード手段３８は、この署名値も、プログラム復号手段３４に出力する。

【０１２５】

このようにデジタル放送受信装置３を構成することで、デジタル放送受信装置３は、データカルーセル伝送によって、ＣＡＳプログラムＰをダウンロードすることができる。また、たとえ、データカルーセルによるＣＡＳプログラムＰの配信が終了した場合であっても、ネットワーク（通信回線Ｎ）を介して、ＣＡＳプログラムＰをダウンロードすることができる。

なお、デジタル放送受信装置３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（ＣＡＳプログラム受信プログラム）により動作させることができる。

【０１２６】

［デジタル放送システムの動作］

次に、本発明の実施形態に係るデジタル放送システムＳの動作について説明する。なお、限定受信方式によるコンテンツの配信動作については、従来技術と同様であるため、ここでは説明を省略し、ＣＡＳプログラムの配信・受信動作、および、ＣＡＳプログラムの起動動作について主に説明を行う。

【０１２７】

（ＣＡＳプログラムの配信動作：デジタル放送送信装置）

最初に、図１１を参照（構成については適宜図２、図３参照）して、ＣＡＳプログラムの配信時におけるデジタル放送送信装置１の動作について説明する。

【０１２８】

まず、デジタル放送送信装置１は、配信データ生成手段１３によって、データカルーセル伝送によって伝送するＣＡＳプログラムＰを、データカルーセルのデータ形式に変換し、配信用のデータ（ＤＩＩ，ＤＤＢ）を生成する。

すなわち、デジタル放送送信装置１は、配信データ生成手段１３の署名値演算手段１３ａによって、ＣＡＳプログラムＰを外部から入力し、秘密鍵Ｋｐｓを用いて、ＣＡＳプログラムＰのデジタル署名の署名値を演算する（ステップＳ１）。

【０１２９】

また、デジタル放送送信装置１は、分割手段１３ｂによって、ＣＡＳプログラムＰを、データカルーセル伝送を行う際のＤＤＢメッセージのブロックサイズで分割する（ステップＳ２）。そして、デジタル放送送信装置１は、暗号化手段１３ｃによって、ステップＳ２で分割された分割データを、デジタル放送受信装置３と共通のプログラム暗号化鍵Ｋｐｅで暗号化する（ステップＳ３）。

【０１３０】

その後、デジタル放送送信装置１は、ステップＳ１で演算された署名値と、外部から入力されるＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）とを配置して、ＤＩＩメッセージ（図５参照）を生成するとともに、ステップＳ３で暗号化された暗号化分割データを配置して、ＤＤＢメッセージ（図６参照）を生成することで、データカルーセル用データ（配信データ）を生成する（ステップＳ４）。

【０１３１】

そして、デジタル放送送信装置１は、配信データスクランブル手段１４によって、ステップＳ４で生成されたデータカルーセル用データを、スクランブル鍵Ｋｓ２でスクランブル（暗号化）する（ステップＳ５）。

そして、デジタル放送送信装置１は、ＥＣＭ－ＲＭＰ生成手段１５によって、ステップＳ５で用いたスクランブル鍵Ｋｓ２を伝送路保護鍵Ｋｐで暗号化して、すべてのデジタル放送受信装置３で共通の共通情報（ＥＣＭ－ＲＭＰ）を生成する（ステップＳ６）。

【０１３２】
そして、デジタル放送送信装置１は、デバイス鍵選択手段１８によって、デバイス鍵リスト記憶手段１６に記憶されているデバイス鍵の中で、無効化されていないデバイス鍵Ｋｄ、および、それに対応する受信機識別子ＲＩＤを順次選択する（ステップＳ７）。
【０１３３】
さらに、デジタル放送送信装置１は、ＥＭＭ－ＲＭＰ生成手段１９によって、ステップＳ３で用いたプログラム暗号化鍵Ｋｐｅと、ステップＳ６で用いた伝送路保護鍵Ｋｐと、ステップＳ７で選択された受信機識別子ＲＩＤと、ステップＳ１で用いた秘密鍵Ｋｐｓに対応したデジタル署名を検証する公開鍵（検証鍵）を含んだルート公開鍵証明書ＲＰＫＣとを、ステップＳ７で順次選択された受信機識別子ＲＩＤに対応するデバイス鍵Ｋｄで暗号化して、デジタル放送受信装置３ごとの個別情報（ＥＭＭ－ＲＭＰ）を生成する（ステップＳ８）。
なお、デジタル放送受信装置３で使用するデバイス鍵Ｋｄを更新させる場合、ステップＳ８において、個別情報（ＥＭＭ－ＲＭＰ）に、シードを含んだデバイス鍵更新制御情報ＫＤｃを含ませればよい。
【０１３４】
そして、デジタル放送送信装置１は、ダウンロードテーブル生成手段２０によって、配信対象のＣＡＳプログラムＰを特定するための情報（ダウンロード制御情報Ｄｃ）から、セクション形式のテーブルであるダウンロードテーブルＴｄ（図８参照）を生成する（ステップＳ９）。なお、ここでは、ＣＡＳプログラムを、放送によって配信することとし、ダウンロードテーブルＴｄ内には、放送によるＣＡＳプログラムを配信することを示すダウンロード記述子（図９参照）を配置することとする。
【０１３５】
そして、デジタル放送送信装置１は、多重化手段２２によって、ステップＳ５でスクランブルされたデータカルーセル用データ（暗号化配信データ）と、ステップＳ６で生成されたＥＣＭ－ＲＭＰと、ステップＳ８で生成されたＥＭＭ－ＲＭＰと、ステップＳ９で生成されたダウンロードテーブルＴｄとを多重化して多重化信号（ＭＰＥＧ－２　ＴＳ）を生成し、送信する（ステップＳ１０）。
以上の動作によって、デジタル放送送信装置１は、データカルーセルによって、ＣＡＳプログラムＰを配信することができる。
【０１３６】
（ＣＡＳプログラムの受信動作：デジタル放送受信装置）
次に、図１２を参照（構成については適宜図４参照）して、ＣＡＳプログラムの配信時におけるデジタル放送受信装置３の動作について説明する。なお、デジタル放送受信装置３は、ＣＡＳプログラムＰをダウンロードしていない場合であっても、予め少なくとも１つのＣＡＳプログラムＰが記憶手段３５に記憶されており、初期状態では、当該ＣＡＳプログラムＰが、プログラム起動手段３７によって起動され、プログラム実行手段３１として動作しているものとする。
【０１３７】
この状態で、デジタル放送受信装置３は、デジタル放送送信装置１から送信される多重化信号（ＭＰＥＧ－２　ＴＳ）を受信し、分離手段３０によって、各信号に分離する（ステップＳ１１）。
【０１３８】
そして、デジタル放送受信装置３は、ＥＭＭ－ＲＭＰ復号手段３１ｄによって、分離手段３０で分離されたＥＭＭ－ＲＭＰ（個別情報）を、デバイス鍵Ｋｄで復号し、伝送路保護鍵Ｋｐと、プログラム暗号化鍵Ｋｐｅと、受信機識別子ＲＩＤと、ルート公開鍵証明書ＲＰＫＣとを抽出する（ステップＳ１２）。
なお、プログラム暗号化鍵Ｋｐｅおよびルート公開鍵証明書ＲＰＫＣに含まれている公開鍵（検証鍵）Ｋｐｐは、記憶手段３５に記憶しておく。また、ＥＭＭ－ＲＭＰ（個別情報）に、デバイス鍵更新制御情報ＫＤｃが含まれている場合、デバイス鍵生成・更新手段

３１ｇは、新たなデバイス鍵Ｋｄを生成し、記憶手段３５に記憶する。
【０１３９】
さらに、デジタル放送受信装置３は、ＥＣＭ－ＲＭＰ復号手段３１ｅによって、分離手段３０で分離されたＥＣＭ－ＲＭＰ（共通情報）を、ステップＳ１２で復号（抽出）された伝送路保護鍵Ｋｐで復号し、スクランブル鍵Ｋｓ２を抽出する（ステップＳ１３）。
【０１４０】
その後、デジタル放送受信装置３は、ダウンロードテーブル解析手段３２によって、分離手段３０で分離されたセクション形式のダウンロードテーブルＴｄを解析し（ステップＳ１４）、当該テーブルの記述子領域に、ダウンロードコンテンツ記述子（図９参照）が記述されているのか、ネットワークダウンロードコンテンツ記述子（図１０参照）が記述されているのかを判定する（ステップＳ１５）。
【０１４１】
このステップＳ１５において、記述子領域に、ダウンロードコンテンツ記述子が記述されている場合（“放送”）、デジタル放送受信装置３は、ダウンロードテーブル解析手段３２からの指示で、分離手段３０によって、データカルーセル用データ（暗号化配信データ）を分離抽出する（ステップＳ１６）。
【０１４２】
そして、デジタル放送受信装置３は、配信データデスクランブル手段３１ｆによって、ステップＳ１６で分離抽出されたデータカルーセル用データ（暗号化配信データ；ＤＩＩ，ＤＤＢ）を、ステップＳ１３で抽出されたスクランブル鍵Ｋｓ２でデスクランブル（復号）する（ステップＳ１７）。
【０１４３】
そして、デジタル放送受信装置３は、配信データ分離手段３３によって、ステップＳ１７でデスクランブルされたデータカルーセル用データから、ＣＡＳプログラムＰ（暗号化されたＣＡＳプログラムＰ）を分離して抽出する（ステップＳ１８）。すなわち、このステップＳ１８において、配信データ分離手段３３は、ＤＤＢメッセージの各ブロックのデータを連結して暗号化されたＣＡＳプログラムＰを再構成する。また、このとき、配信データ分離手段３３は、ＤＩＩメッセージから、ＣＡＳプログラムＰの署名値、識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）を取得する。
【０１４４】
一方、ステップＳ１５において、記述子領域に、ネットワークダウンロードコンテンツ記述子が記述されている場合（“通信”）、デジタル放送受信装置３は、通信ダウンロード手段３８によって、ネットワークダウンロードコンテンツ記述子に記述されている通信サーバ（ＣＡＳサーバ５）から、通信回線Ｎを介して、暗号化されたＣＡＳプログラムＰを取得する（ステップＳ１９）。なお、ＣＡＳサーバ５から取得するＣＡＳプログラムＰには、署名（署名値）、識別子（ＣＡＳ－ＩＤ）、バージョン（ＣＡＳ－Ｖｅｒ）が付加されているものとする。
【０１４５】
そして、デジタル放送受信装置３は、プログラム復号手段３４の暗号復号手段３４ａによって、ステップＳ１８で分離抽出した（暗号化）ＣＡＳプログラム、または、ステップＳ１９で取得した（暗号化）ＣＡＳプログラムを、ステップＳ１２で復号され、記憶されているプログラム暗号化鍵Ｋｐｅで復号する（ステップＳ２０）。
【０１４６】
さらに、デジタル放送受信装置３は、署名検証手段３４ｂによって、ステップＳ２０で復号したＣＡＳプログラムの署名検証を行う（ステップＳ２１）。すなわち、署名検証手段３４ｂは、ステップＳ１２で抽出したルート公開鍵証明書ＲＰＫＣに含まれる公開鍵（検証鍵）ＫｐｐでＣＡＳプログラムに付加されている署名値を復号し、ＣＡＳプログラムのハッシュ値と一致するか否かにより、ＣＡＳプログラムの検証を行う。
【０１４７】
そして、デジタル放送受信装置３は、ステップＳ２１における検証結果に問題がなけれ

ば、書込手段３４ｃによって、ステップＳ２０で復号されたＣＡＳプログラムＰを、記憶手段３５に、識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）に対応付けて書き込み記憶させる（ステップＳ２２）。

以上の動作によって、デジタル放送受信装置３は、暗号化され、かつ、デジタル署名が付された状態でＣＡＳプログラムＰをダウンロードすることができ、ＣＡＳプログラムに対する不正を防止することができる。

【０１４８】

（ＣＡＳプログラムの起動指示動作：デジタル放送送信装置）

次に、図１３を参照（構成については適宜図２参照）して、デジタル放送受信装置３で指定したＣＡＳプログラムＰを起動させるデジタル放送送信装置１の動作について説明する。

【０１４９】

まず、デジタル放送送信装置１は、ＥＣＭ－ＲＭＰ生成手段１５によって、起動対象となるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）、バージョン（ＣＡＳ－Ｖｅｒ）およびＣＡＳプログラムＰのハッシュ値（ＣＡＳ－Ｈ）を、伝送路保護鍵Ｋｐで暗号化して、すべてのデジタル放送受信装置３で共通の共通情報（ＥＣＭ－ＲＭＰ）を生成する（ステップＳ３１）。

【０１５０】

また、デジタル放送送信装置１は、デバイス鍵選択手段１８によって、デバイス鍵リスト記憶手段１６に記憶されているデバイス鍵の中で、無効化されていないデバイス鍵Ｋｄを順次選択する（ステップＳ３２）。

また、デジタル放送送信装置１は、ＥＭＭ－ＲＭＰ生成手段１９によって、ステップＳ３１で用いた伝送路保護鍵Ｋｐを、ステップＳ３２で順次選択されたデバイス鍵Ｋｄで暗号化して、デジタル放送受信装置３ごとの個別情報（ＥＭＭ－ＲＭＰ）を生成する（ステップＳ３３）。

【０１５１】

さらに、デジタル放送送信装置１は、起動プログラム指定手段２１によって、起動させたいＣＡＳプログラムＰを指定するための情報（プログラム指定情報）として、ＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）を、ＰＳＩ／ＳＩのＣＡＴまたはＰＭＴに配置する（ステップＳ３４）。

そして、デジタル放送送信装置１は、多重化手段２２によって、ステップＳ３１で生成されたＥＣＭ－ＲＭＰと、ステップＳ３３で生成されたＥＭＭ－ＲＭＰと、ステップＳ３４で識別子等が配置されたＰＳＩ／ＳＩとを多重化して多重化信号（ＭＰＥＧ－２　ＴＳ）を生成し、送信する（ステップＳ３５）。

【０１５２】

以上の動作によって、デジタル放送送信装置１は、起動させたいＣＡＳプログラムＰを、ＰＳＩ／ＳＩに配置したプログラム指定情報で指定することができる。また、デジタル放送送信装置１は、プログラム指定情報で指定したＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）と、ＣＡＳプログラムＰのハッシュ値（ＣＡＳ－Ｈ）とを、ＥＣＭ－ＲＭＰでデジタル放送受信装置３に送信することで、デジタル放送受信装置３において、識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）の整合性や、ＣＡＳプログラムＰの正当性を検証することが可能になる。

【０１５３】

（ＣＡＳプログラムの起動動作：デジタル放送受信装置）

次に、図１４を参照（構成については適宜図４参照）して、デジタル放送送信装置１から指定されたＣＡＳプログラムＰを起動するデジタル放送受信装置３の動作について説明する。

【０１５４】

まず、デジタル放送受信装置３は、デジタル放送送信装置１から送信される多重化信号（ＭＰＥＧ－２　ＴＳ）を受信し、分離手段３０によって、各信号に分離する（ステップ

Ｓ４１）。
そして、デジタル放送受信装置３は、起動プログラム特定手段３６によって、ＰＳＩ／ＳＩ（番組配列情報）のＣＡＴまたはＰＭＴから、プログラム指定情報であるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）およびそのバージョン（ＣＡＳ－Ｖｅｒ）を抽出する（ステップＳ４２）。
【０１５５】
そして、デジタル放送受信装置３は、ＥＭＭ－ＲＭＰ復号手段３１ｄによって、ステップＳ４１で分離されたＥＭＭ－ＲＭＰ（個別情報）を、デバイス鍵Ｋｄで復号し、伝送路保護鍵Ｋｐを抽出する（ステップＳ４３）。
【０１５６】
さらに、デジタル放送受信装置３は、ＥＣＭ－ＲＭＰ復号手段３１ｅによって、ステップＳ４１で分離したＥＣＭ－ＲＭＰ（共通情報）を、ステップＳ４３で復号（抽出）した伝送路保護鍵Ｋｐで復号し、ＣＡＳプログラムの識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）と、ＣＡＳプログラムのハッシュ値（ＣＡＳ－Ｈ）を抽出する（ステップＳ４４）。
【０１５７】
そして、デジタル放送受信装置３は、プログラム起動手段３７によって、ステップＳ４２で抽出した識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）と、ステップＳ４４で抽出した識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）とが、それぞれ一致するか否かを判定する（ステップＳ４５）。
ここで、識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）がそれぞれ一致しなかった場合（ステップＳ４５でＮｏ）、デジタル放送受信装置３は、指示されたＣＡＳプログラムＰの起動動作を終了する。
【０１５８】
一方、識別子（ＣＡＳ－ＩＤ）およびバージョン（ＣＡＳ－Ｖｅｒ）が一致した場合（ステップＳ４５でＹｅｓ）、デジタル放送受信装置３は、プログラム起動手段３７によって、記憶手段３５に記憶されている起動を指示されたＣＡＳプログラムＰのハッシュ値を演算し（ステップＳ４６）、ステップＳ４４で抽出したＣＡＳプログラムＰのハッシュ値（ＣＡＳ－Ｈ）と一致するか否かを判定する（ステップＳ４７）。
【０１５９】
ここで、ハッシュ値が一致しない場合（ステップＳ４７でＮｏ）、デジタル放送受信装置３は、指示されたＣＡＳプログラムＰの起動動作を終了する。
一方、ハッシュ値が一致した場合（ステップＳ４７でＹｅｓ）、デジタル放送受信装置３は、プログラム起動手段３７によって、記憶手段３５から、指定されたＣＡＳプログラムＰを読み出して、プログラム実行手段３１として起動させる（ステップＳ４８）。
【０１６０】
以上の動作によって、デジタル放送受信装置３は、デジタル放送送信装置１から指定されたＣＡＳプログラムＰを起動させることができる。また、このとき、デジタル放送受信装置３は、ＥＣＭ－ＲＭＰ（共通情報）で通知されるＣＡＳプログラムＰの識別子（ＣＡＳ－ＩＤ）、バージョン（ＣＡＳ－Ｖｅｒ）およびハッシュ値（ＣＡＳ－Ｈ）によって、指定された正しいバージョンで、かつ、改ざん等が行われていない正規のＣＡＳプログラムのみを起動させることができる。
【０１６１】
以上説明したように、本発明によれば、データカルーセル伝送によって、デジタル放送送信装置１からデジタル放送受信装置３に、高速にＣＡＳプログラムＰを配信することができる。これによって、ＣＡＳプログラムＰにおけるアクセス制御に関する機能のセキュリティが破られた場合であっても、セキュリティ機能を変更したＣＡＳプログラムＰを配信することができるため、セキュリティが破られた際の影響を最小限に抑えることができる。
また、本発明によれば、放送によるＣＡＳプログラムＰの配信を終了した場合であって

も、通信回線を介してＣＡＳプログラムＰを配信することができ、放送帯域の使用を短期間で終わらせることができる。

【０１６２】

また、本発明によれば、データカルーセルでＣＡＳプログラムＰを配信する際に、検証によって、ＣＡＳプログラムＰの改ざん等を防止することができる。また、本発明によれば、デジタル放送送信装置１が、起動させたいＣＡＳプログラムＰを指定した場合、デジタル放送受信装置３において、バージョン等の整合性をチェックすることができ、さらに、起動するＣＡＳプログラムＰの正当性をハッシュ値によりチェックすることができるため、起動するＣＡＳプログラムＰに対する不正を防止することができる。

【０１６３】

また、本発明によれば、デバイス鍵Ｋｄやプログラム暗号化鍵Ｋｐｅが漏洩した場合であっても、伝送路保護鍵Ｋｐおよびプログラム暗号化鍵Ｋｐｅを更新した後に、ＣＡＳプログラムを更新し、放送または通信によって配信することで、デバイス鍵Ｋｄの漏洩元となったデジタル放送受信装置３の使用を停止（リボーク）させることができる。これによって、新しいＣＡＳプログラムの漏洩を防止することができる。

【０１６４】

また、本発明によれば、デジタル放送送信装置１から、ＰＳＩ／ＳＩによって、起動するＣＡＳプログラムＰを切り替えることができ、放送事業者が、提供するサービスに応じてＣＡＳプログラムＰを選択することが可能になる。

【符号の説明】

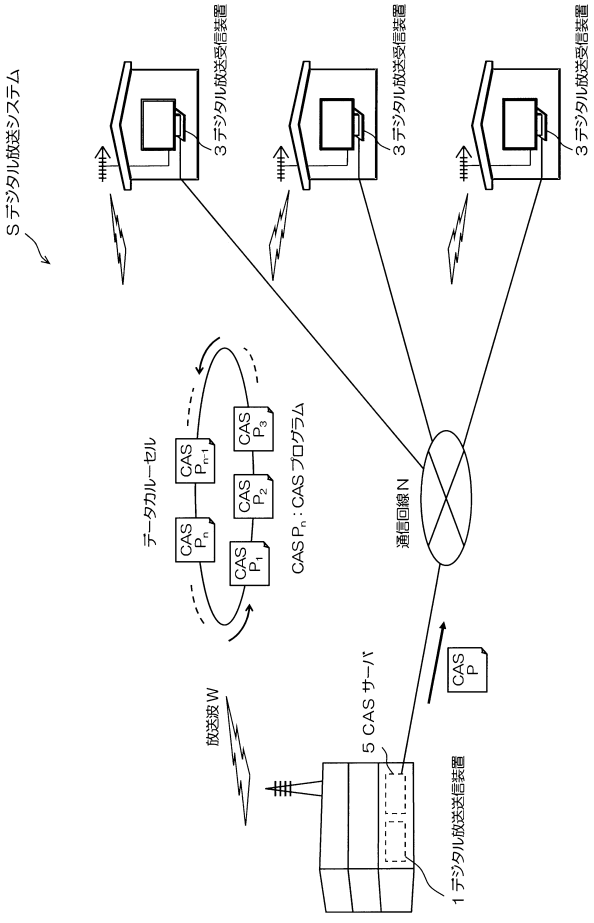
【０１６５】

Ｓ　デジタル放送システム
１　デジタル放送送信装置
１０　コンテンツスクランブル手段
１１　ＥＣＭ－ＣＡＳ生成手段
１２　ＥＭＭ－ＣＡＳ生成手段
１３　配信データ生成手段
１３ａ　署名値演算手段
１３ｂ　分割手段
１３ｃ　暗号化手段
１３ｄ　データカルーセル用データ生成手段
１４　配信データスクランブル手段
１５　ＥＣＭ－ＲＭＰ生成手段（共通情報生成手段）
１６　デバイス鍵リスト記憶手段
１７　無効設定手段
１８　デバイス鍵選択手段
１９　ＥＭＭ－ＲＭＰ生成手段（個別情報生成手段）
２０　ダウンロードテーブル生成手段
２１　起動プログラム指定手段
２２　多重化手段
３　デジタル放送受信装置
３０　分離手段
２１　プログラム実行手段
３１ａ　ＥＭＭ－ＣＡＳ復号手段
３１ｂ　ＥＣＭ－ＣＡＳ復号手段
３１ｃ　コンテンツデスクランブル手段
３１ｄ　ＥＭＭ－ＲＭＰ復号手段（個別情報復号手段）
３１ｅ　ＥＣＭ－ＲＭＰ復号手段（共通情報復号手段）
３１ｆ　配信データデスクランブル手段
３１ｇ　デバイス鍵生成・更新手段

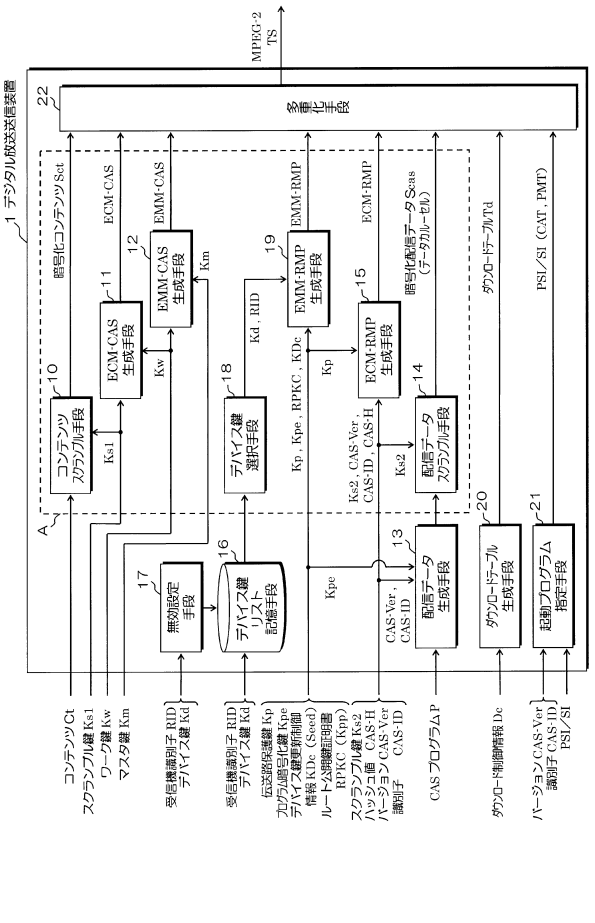
３２　ダウンロードテーブル解析手段
３３　配信データ分離手段
３４　プログラム復号手段
３４ａ　暗号復号手段
３４ｂ　署名検証手段
３４ｃ　書込手段
３５　記憶手段（プログラム記憶手段）
３６　起動プログラム特定手段
３７　プログラム起動手段
３８　通信ダウンロード手段
５　ＣＡＳサーバ

【要約】
【課題】アクセス制御プログラムを、放送波によって配信するデジタル放送送信装置を提供する。
【解決手段】デジタル放送送信装置１は、プログラム暗号化鍵でアクセス制御プログラムを暗号化して配信データを生成する配信データ生成手段１３と、配信データをスクランブル鍵で暗号化し暗号化配信データを生成する配信データスクランブル手段１４と、伝送路保護鍵でスクランブル鍵を暗号化し共通情報を生成する共通情報生成手段１５と、有効なデバイス鍵で伝送路保護鍵を暗号化し個別情報を生成する個別情報生成手段１９と、放送波によりアクセス制御プログラムを送信する旨を示す識別子を含んだダウンロードテーブルを生成するダウンロードテーブル生成手段２０と、これらの生成した情報を多重化する多重化手段１９と、を備えることを特徴とする。
【選択図】図２

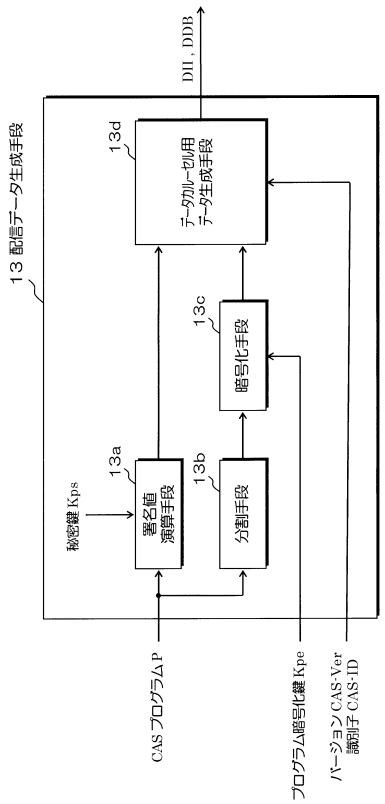
【図１】



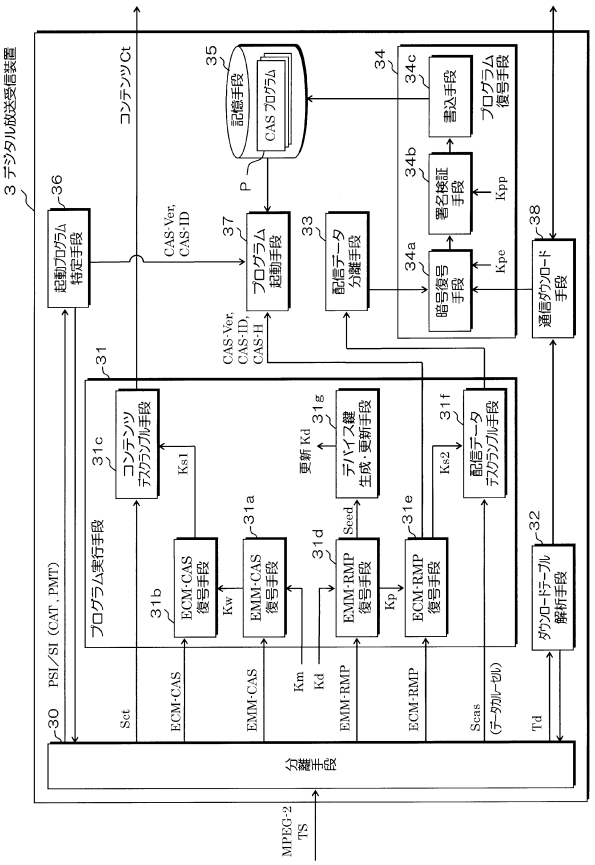

【図２】



【図３】




【図４】




【図５】

DII メッセージ

| データ構造 | | データ長 | 備考 |
|---|---|---|---|
| dsmccMessage Header() | protocolDiscriminator | 1 バイト | 0x11 : DSM-CC |
| | dsmccType | 1 バイト | 0x03 : U-N ダウンロードメッセージ |
| | messageId | 2 バイト | 0x1002 |
| | transaction_id | 4 バイト | モジュール更新時インクリメント |
| | reserved | 1 バイト | 予備 |
| | adaptationLength | 1 バイト | 0x00 |
| | messegeLength | 2 バイト | 0x0000 |
| | dsmccAdaptationHeader() | N | #未使用 |
| downloadId | | 4 バイト | ダウンロード識別　0xFFFFFFFF |
| blockSize | | 2 バイト | 4066 |
| windowSize | | 1 バイト | #未使用 |
| ackPeriod | | 1 バイト | #未使用 |
| tCDownloadWindow | | 4 バイト | #未使用 |
| tCdownloadScenario | | 4 バイト | #未使用 |
| compatibilityDescriptor() | | M | コンパチビリティ記述子 |
| numberOfModules | | 2 バイト | モジュール数 |
| | module_id | 2 バイト | モジュール識別 |
| | module_size | 4 バイト | モジュールサイズ |
| | module_version | 1 バイト | モジュールバージョン |
| | module_info_length | 1 バイト | 0x00 |
| | module_info_byte | P | #未使用 |
| privateDatalength | | 2 バイト | |
| | CAS_digital_signature | 128 バイト | 署名値<br>PKCS#1 で PAD with SHA-256 |

コンパチビリティ記述子（compatibilityDescriptor()）

| データ構造 | | データ長 | 備考 |
|---|---|---|---|
| compatibilityDescriptorLength | | 2 バイト | コンパチビリティ記述子長 |
| descriptorCount | | 2 バイト | 記述子数 |
| | descriptorType | 1 バイト | 記述子長 0xFF |
| | descriptorLength | 1 バイト | |
| | specifierType | 1 バイト | 0xFF |
| | specifierData() | 3 バイト | 0xFFFFFF |
| | CAS_model | 2 バイト | 0xFFFF |
| | CAS_version | 2 バイト | CAS-ID , CAS-Ver |
| | subDescriptorCount | 1 バイト | |
| | subDescriptor() | N | |

【図６】


| 受信機識別子 | デバイス鍵 | フラグ |
|---|---|---|
| RID1 | Kd10 | 無効 |
| | Kd11 | 無効 |
| | Kd12 | 有効 |
| RID2 | Kd20 | 有効 |
| RID3 | Kd30 | 無効 |
| | Kd31 | 有効 |
| : | : | : |

【図７】


| 受信機識別子 | デバイス鍵 | フラグ |
|---|---|---|
| RID1 | Kd10 | 無効 |
| | Kd11 | 無効 |
| | Kd12 | 有効 |
| RID2 | Kd20 | 有効 |
| RID3 | Kd30 | 無効 |
| | Kd31 | 有効 |
| : | : | : |

【図８】

ダウンロードテーブル

| データ構造 | データ長 | 備考 |
|---|---|---|
| Header() | 8 バイト | セクションヘッダ table_id＝0xC3 |
| transport_stream_id | 2 バイト | 0x00 |
| original_network_id | 2 バイト | 0x00 |
| service_id | 1 バイト | 0x00 |
| num_of_contents | 1 バイト | 0x01 |
| group | 4 ビット | group_id |
| target_version | 12 ビット | 更新対象となる CAS プログラムのバージョン |
| new_version | 12 ビット | 新 CAS プログラムのバージョン |
| download_level | 2 ビット | ダウンロードレベル |
| version_indicator | 2 ビット | バージョン表示 |
| content_description_length | 12 ビット (N) | スケジュールループ+記述子ループ |
| reserved | 4 ビット | |
| schedule_description_length | 12 ビット (M) | スケジュールループ長 |
| schedule_time-shift_information | 4 ビット | #未使用 |
| start_time | 40 ビット | #未使用 |
| duration | 24 ビット | #未使用 |
| descriptor() | N−M | ダウンロードコンテンツ記述子／ネットワークダウンロードコンテンツ記述子 |
| CRC_32 | 4 バイト | 誤り検出符号 |

【図９】

ダウンロードコンテンツ記述子

| データ構造 | データ長 | 備考 |
|---|---|---|
| descriptor_tag | 1 バイト | 記述子タグ 0xC9 |
| descriptor_length | 1 バイト | 記述子長 |
| reboot | 2 バイト | #未使用 |
| add_on | 1 ビット | #未使用 |
| compatibility_flag | 1 ビット | 1：compatibilityDescriptor あり |
| module_info_flag | 1 ビット | 1：module_info あり |
| text_info_flag | 1 ビット | 1：text_info あり |
| reserved | 3 ビット | 予備 |
| component_size | 4 バイト | CAS プログラムのデータサイズ |
| download_id | 4 バイト | ダウンロード識別（DII／DDB） 0xFFFFFFFF |
| time_out_value_DII | 4 バイト | #未使用 |
| leak_rate | 22 ビット | #未使用 |
| reserved | 2 ビット | 予備 |
| component_tag | 1 バイト | PMT のストリーム記述子と対応 |
| compatibilityDescriptor() | N | コンパチビリティ記述子 |
| num_of_modules | 2 バイト | DII／DDB のモジュール数 |
| module_id | 2 バイト | モジュール識別 |
| module_size | 4 バイト | モジュールサイズ |
| module_info_length | 1 バイト | 0x00 |
| module_info_byte | M | #未使用 |
| private_data_length | 1 バイト | 0x00 |
| private_data_byte | P | #未使用 |
| ISO_639_language_code | 2 バイト | #未使用 |
| text_length | 1 バイト | 0x00 |
| text_char | Q | #未使用 |

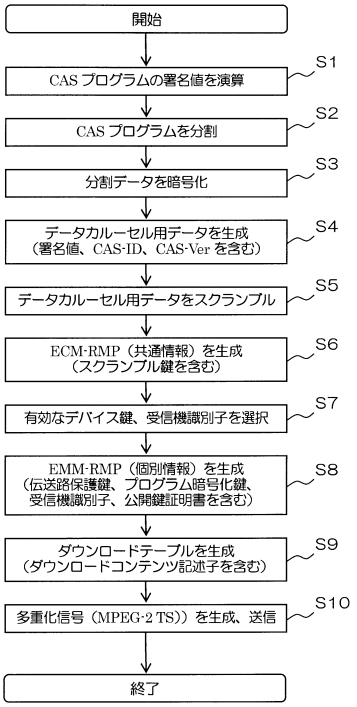
【図１０】

ネットワークダウンロードコンテンツ記述子

| データ構造 | データ長 | 備考 |
|---|---|---|
| descriptor_tag | 1 バイト | 記述子タグ 0xCA |
| descriptor_length | 1 バイト | 記述子長 |
| reboot | 2 バイト | #未使用 |
| add_on | 1 ビット | #未使用 |
| compatibility_flag | 1 ビット | 1：compatibilityDescriptor あり |
| reserved | 1 ビット | 予備 |
| component_size | 4 バイト | CAS プログラムのデータサイズ |
| session_protcol_number | 1 バイト | セッションプロトコル番号 0xFF：固定 |
| session_id | 1 バイト | セッション識別 0xFF：固定 |
| Server_URL | 20 バイト | 通信サーバの URL または IP アドレス |
| compatibilityDescriptor() | N | コンパチビリティ記述子 |
| private_data_length | 1 バイト | 0x00 |
| private_data_byte | P | #未使用 |
| ISO_639_language_code | 2 バイト | #未使用 |
| text_length | 1 バイト | 0x00 |
| text_char | Q | #未使用 |

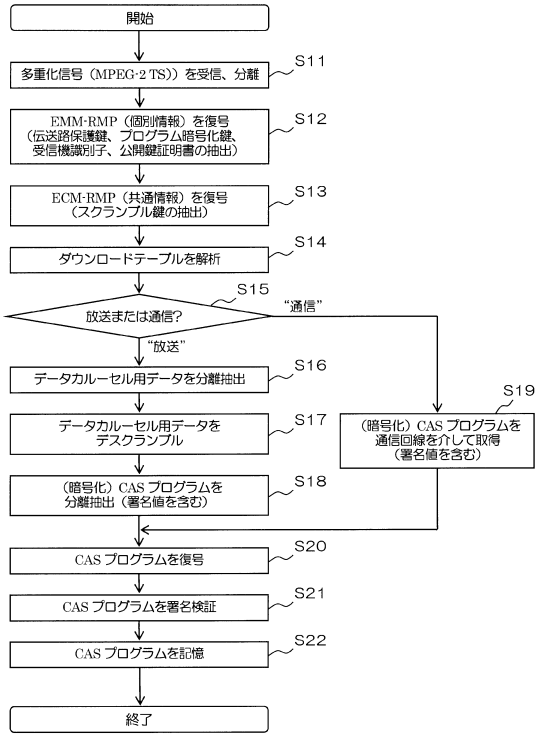
【図１１】

CAS プログラム配信動作：デジタル放送送信装置



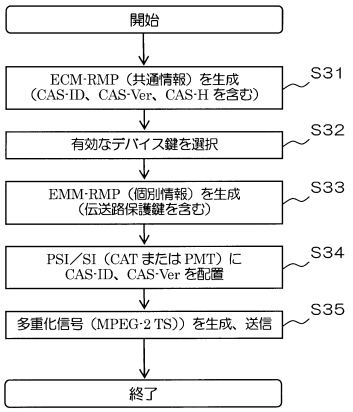
【図１２】

CASプログラム受信動作：デジタル放送受信装置



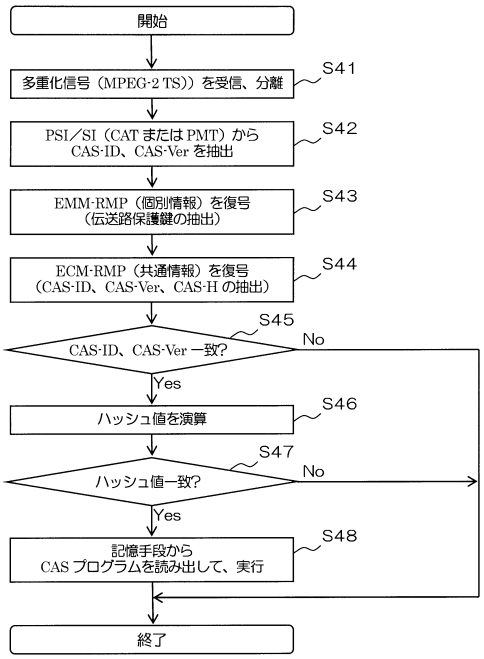

【図１３】

CASプログラム起動指示動作：デジタル放送送信装置




【図１４】

CASプログラム起動動作：デジタル放送受信装置



フロントページの続き

(72)発明者　井上　友幸
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

審査官　古川　哲也

(56)参考文献　特開２００９－２６７６０５（ＪＰ，Ａ）
特開２００９－１４７９０５（ＪＰ，Ａ）
特開２００３－３１８８７４（ＪＰ，Ａ）
特開２００２－０４４０７１（ＪＰ，Ａ）
国際公開第２００６／０８２８１２（WO，Ａ１）
米国特許出願公開第２００６／０１３７０１５（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　２１／００　－　２１／８５８
Ｈ０４Ｈ　６０／２３
Ｈ０４Ｌ　９／００　－　９／３８