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

特許第4589702号
(P4589702)

(45)発行日　平成22年12月1日(2010.12.1)　(24)登録日　平成22年9月17日(2010.9.17)

(51)Int.Cl.　F I
H04N 7/167 (2006.01)　H04N 7/167 Z
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 3　(全 27 頁)

(21)出願番号　特願2004-334287 (P2004-334287)
(22)出願日　平成16年11月18日 (2004.11.18)
(65)公開番号　特開2006-148416 (P2006-148416A)
(43)公開日　平成18年6月8日 (2006.6.8)
審査請求日　平成19年4月9日 (2007.4.9)

特許権者において、実施許諾の用意がある。

(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　100064414
弁理士　磯野　道造
(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　中村　晴幸
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

最終頁に続く

(54)【発明の名称】コンテンツ受信装置およびコンテンツ受信プログラム

(57)【特許請求の範囲】
【請求項１】
コンテンツを視聴できる期限を無期限に設定可能な期限情報を含むライセンス情報が暗号化され、暗号化されたＫｃ伝送用ＥＣＭと、当該コンテンツがスクランブルされたスクランブルコンテンツとが多重化された多重化スクランブルコンテンツを受信するコンテンツ受信装置であって、
前記コンテンツがスクランブル鍵でスクランブルされたスクランブルコンテンツと、前記スクランブル鍵を含むスクランブル鍵関連情報が所定期間毎に更新されるワーク鍵で暗号化されたＥＣＭ－Ｋｗと、前記ライセンス情報が前記ワーク鍵で暗号化されたＫｃ伝送用ＥＣＭと、前記ワーク鍵を含むワーク鍵関連情報が予め保持されているマスター鍵と同じマスター鍵で暗号化されたＥＭＭと、に前記多重化スクランブルコンテンツを分離する第一分離手段と、
この第一分離手段で分離された前記ＥＭＭを、予め保持されているマスター鍵で復号して、前記ワーク鍵を含むワーク鍵関連情報を出力するＥＭＭ復号手段と、
前記第一分離手段で分離されたＫｃ伝送用ＥＣＭを、前記ワーク鍵で復号して、前記ライセンス情報を出力するＫｃ伝送用ＥＣＭ復号手段と、
前記第一分離手段で分離された前記ＥＣＭ－Ｋｗを、前記ワーク鍵で復号して、前記ＥＣＭ－Ｋｗに含まれている前記スクランブル鍵を出力するスクランブル鍵第一復号手段と、
前記ライセンス情報に含まれている、前記スクランブルコンテンツを視聴可能な期限が

無期限または有限に設定された期限情報と、当該ライセンス情報自体を蓄積する場所を指定する蓄積場所情報の暗号化Ｋｃ蓄積場所指定の値とに基づいて、当該ライセンス情報自体の出力先を判定し、前記期限情報が無期限に設定されている場合には前記蓄積場所情報によらずに再多重化スクランブルコンテンツ蓄積手段を前記ライセンス情報自体の出力先として判定する蓄積場所判定手段と、

この蓄積場所判定手段による判定結果に従って、前記ライセンス情報を、予め受信側で保持されている固有鍵で再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを出力するＫｃ伝送用ＥＣＭ再暗号化手段と、

前記第一分離手段で分離されたスクランブルコンテンツと、前記スクランブル鍵関連情報が前記コンテンツ毎に設定されるコンテンツ鍵で暗号化されたＥＣＭ－Ｋｃと、前記Ｋｃ伝送用ＥＣＭ再暗号化手段で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭとを再多重化した再多重化スクランブルコンテンツを出力する再多重化手段と、

この再多重化手段で再多重化された再多重化スクランブルコンテンツを蓄積する再多重化スクランブルコンテンツ蓄積手段と、

前記蓄積場所判定手段による判定結果に従って、前記ライセンス情報を保持するライセンス情報保持手段と、

前記再多重化スクランブルコンテンツ蓄積手段に蓄積されている再多重化スクランブルコンテンツを、前記再暗号化Ｋｃ伝送用ＥＣＭと、前記ＥＣＭ－Ｋｃと、前記スクランブルコンテンツとに分離する第二分離手段と、

この第二分離手段で分離された再暗号化Ｋｃ伝送用ＥＣＭを、前記固有鍵で復号して、ライセンス情報を、前記ライセンス情報保持手段に出力する再暗号化Ｋｃ伝送用ＥＣＭ復号手段と、

前記第二分離手段で分離されたＥＣＭ－Ｋｃを、前記ライセンス情報に含まれている前記コンテンツ鍵で復号して、前記ＥＣＭ－Ｋｃに含まれている前記スクランブル鍵を出力するスクランブル鍵第二復号手段と、

前記スクランブル鍵第一復号手段または前記スクランブル鍵第二復号手段から出力されたスクランブル鍵で、前記第一分離手段または前記第二分離手段で分離されたスクランブルコンテンツをデスクランブルし、このデスクランブルしたコンテンツを出力するデスクランブル手段と、

を備えることを特徴とするコンテンツ受信装置。

【請求項２】

コンテンツを視聴できる期限を無期限に設定可能な期限情報を含むライセンス情報が暗号化され、暗号化されたＫｃ伝送用ＥＣＭと、当該コンテンツがスクランブルされたスクランブルコンテンツとが多重化された多重化スクランブルコンテンツを受信するコンテンツ受信装置であって、

前記コンテンツがスクランブル鍵でスクランブルされたスクランブルコンテンツと、前記スクランブル鍵を含むスクランブル鍵関連情報が所定期間毎に更新されるワーク鍵で暗号化されたＥＣＭ－Ｋｗと、前記ライセンス情報が前記ワーク鍵で暗号化されたＫｃ伝送用ＥＣＭと、前記ワーク鍵が予め保持されているマスター鍵と同じマスター鍵で暗号化されたＥＭＭと、に前記多重化スクランブルコンテンツを分離する第一分離手段と、

この第一分離手段で分離された前記ＥＭＭを、予め保持されているマスター鍵で復号して、前記ワーク鍵を含むワーク鍵関連情報を出力するＥＭＭ復号手段と、

前記第一分離手段で分離されたＫｃ伝送用ＥＣＭを、前記ワーク鍵で復号して、前記ライセンス情報を出力するＫｃ伝送用ＥＣＭ復号手段と、

前記第一分離手段で分離された前記ＥＣＭ－Ｋｗを、前記ワーク鍵で復号して、前記ＥＣＭ－Ｋｗに含まれている前記スクランブル鍵を出力するスクランブル鍵第一復号手段と、

前記ライセンス情報に含まれている、前記スクランブルコンテンツを視聴可能な期限が無期限または有限に設定された期限情報と、当該ライセンス情報自体を蓄積する場所を指定する蓄積場所情報の暗号化Ｋｃ蓄積場所指定の値とに基づいて、当該ライセンス情報自

体の出力先を判定し、前記期限情報が無期限に設定されている場合には前記蓄積場所情報によらずに外部蓄積装置の蓄積部を前記ライセンス情報自体の出力先として判定する蓄積場所判定手段と、

この蓄積場所判定手段による判定結果に従って、前記ライセンス情報を、予め受信側で保持されている固有鍵で再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを出力するＫｃ伝送用ＥＣＭ再暗号化手段と、

前記第一分離手段で分離されたスクランブルコンテンツと、前記スクランブル鍵関連情報が前記コンテンツ毎に設定されるコンテンツ鍵で暗号化されたＥＣＭ－Ｋｃと、前記Ｋｃ伝送用ＥＣＭ再暗号化手段で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭとを再多重化した再多重化スクランブルコンテンツを出力する再多重化手段と、

この再多重化手段で再多重化された再多重化スクランブルコンテンツを、前記外部蓄積装置との間で入出力する再多重化スクランブルコンテンツ入出力手段と、

前記蓄積場所判定手段による判定結果に従って、前記ライセンス情報を保持するライセンス情報保持手段と、

前記再多重化スクランブルコンテンツ入出力手段により入力された再多重化スクランブルコンテンツを、前記再暗号化Ｋｃ伝送用ＥＣＭと、前記ＥＣＭ－Ｋｃと、前記スクランブルコンテンツとに分離する第二分離手段と、

この第二分離手段で分離された再暗号化Ｋｃ伝送用ＥＣＭを、前記固有鍵で復号して、ライセンス情報を、前記ライセンス情報保持手段に出力する再暗号化Ｋｃ伝送用ＥＣＭ復号手段と、

前記第二分離手段で分離されたＥＣＭ－Ｋｃを、前記ライセンス情報に含まれている前記コンテンツ鍵で復号して、前記ＥＣＭ－Ｋｃに含まれている前記スクランブル鍵を出力するスクランブル鍵第二復号手段と、

前記スクランブル鍵第一復号手段または前記スクランブル鍵第二復号手段から出力されたスクランブル鍵で、前記第一分離手段または前記第二分離手段で分離されたスクランブルコンテンツをデスクランブルし、このデスクランブルしたコンテンツを出力するデスクランブル手段と、

を備えることを特徴とするコンテンツ受信装置。

【請求項３】

コンテンツを視聴できる期限を無期限に設定可能な期限情報を含むライセンス情報が暗号化され、暗号化されたＫｃ伝送用ＥＣＭと、当該コンテンツがスクランブルされたスクランブルコンテンツとが多重化された多重化スクランブルコンテンツを受信するために、コンピュータを、

前記コンテンツがスクランブル鍵でスクランブルされたスクランブルコンテンツと、前記スクランブル鍵を含むスクランブル鍵関連情報が所定期間毎に更新されるワーク鍵で暗号化されたＥＣＭ－Ｋｗと、前記ライセンス情報が前記ワーク鍵で暗号化されたＫｃ伝送用ＥＣＭと、前記ワーク鍵を含むワーク鍵関連情報が予め保持されているマスター鍵と同じマスター鍵で暗号化されたＥＭＭと、に前記多重化スクランブルコンテンツを分離する第一分離手段、

この第一分離手段で分離された前記ＥＭＭを、予め保持されているマスター鍵で復号して、前記ワーク鍵を含むワーク鍵関連情報を出力するＥＭＭ復号手段、

前記第一分離手段で分離されたＫｃ伝送用ＥＣＭを、前記ワーク鍵で復号して、前記ライセンス情報を出力するＫｃ伝送用ＥＣＭ復号手段、

前記第一分離手段で分離された前記ＥＣＭ－Ｋｗを、前記ワーク鍵で復号して、前記ＥＣＭ－Ｋｗに含まれている前記スクランブル鍵を出力するスクランブル鍵第一復号手段、

前記ライセンス情報に含まれている、前記スクランブルコンテンツを視聴可能な期限が無期限または有限に設定された期限情報と、当該ライセンス情報自体を蓄積する場所を指定する蓄積場所情報の暗号化Ｋｃ蓄積場所指定の値とに基づいて、当該ライセンス情報自体の出力先を判定し、前記期限情報が無期限に設定されている場合には前記蓄積場所情報によらずに再多重化スクランブルコンテンツ蓄積手段を前記ライセンス情報自体の出力先

として判定する蓄積場所判定手段、
この蓄積場所判定手段による判定結果に従って、前記ライセンス情報を、予め受信側で保持されている固有鍵で再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを出力するＫｃ伝送用ＥＣＭ再暗号化手段、
前記第一分離手段で分離されたスクランブルコンテンツと、前記多重化スクランブルコンテンツに多重化されていた、前記スクランブル鍵関連情報が前記コンテンツ毎に設定されるコンテンツ鍵で暗号化されたＥＣＭ－Ｋｃと、前記Ｋｃ伝送用ＥＣＭ再暗号化手段で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭとを再多重化した再多重化スクランブルコンテンツを出力する再多重化手段、
この再多重化手段で再多重化された再多重化スクランブルコンテンツを再多重化スクランブルコンテンツ蓄積手段に蓄積させる蓄積制御手段、
前記蓄積場所判定手段による判定結果に従って、前記ライセンス情報をライセンス情報保持手段に保持させる保持制御手段、
前記再多重化スクランブルコンテンツ蓄積手段に蓄積されている再多重化スクランブルコンテンツを、前記再暗号化Ｋｃ伝送用ＥＣＭと、前記ＥＣＭ－Ｋｃと、前記スクランブルコンテンツとに分離する第二分離手段、
この第二分離手段で分離された再暗号化Ｋｃ伝送用ＥＣＭを、前記固有鍵で復号して、ライセンス情報を、前記ライセンス情報保持手段に出力する再暗号化Ｋｃ伝送用ＥＣＭ復号手段、
前記第二分離手段で分離されたＥＣＭ－Ｋｃを、前記ライセンス情報に含まれている前記コンテンツ鍵で復号して、前記ＥＣＭ－Ｋｃに含まれている前記スクランブル鍵を出力するスクランブル鍵第二復号手段、
前記スクランブル鍵第一復号手段または前記スクランブル鍵第二復号手段から出力されたスクランブル鍵で、前記第一分離手段または前記第二分離手段で分離されたスクランブルコンテンツをデスクランブルし、このデスクランブルしたコンテンツを出力するデスクランブル手段、
として機能させることを特徴とするコンテンツ受信プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、スクランブルコンテンツを視聴可能にするライセンス情報を、放送波、または、インターネット配信により、当該スクランブルコンテンツと共に送信するコンテンツ送信装置およびコンテンツ送信プログラム、並びに、ライセンス情報とスクランブルコンテンツとを受信し、蓄積するコンテンツ受信装置およびコンテンツ受信プログラムに関する。
【背景技術】
【０００２】
従来、デジタルコンテンツ（以下、コンテンツという）を放送するデジタル放送では、ＰＳＩ（Ｐｒｏｇｒａｍ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｉｎｆｏｒｍａｔｉｏｎ）のＰＭＴ（Ｐｒｏｇｒａｍ Ｍａｐ Ｔａｂｌｅ）内に、電波産業会ＡＲＩＢ ＳＴＤ－Ｂ１０「デジタル放送に使用する番組配列情報」で規定されているデジタルコピー制御記述子を、コンテンツと共に配信し、受信側で蓄積されるコンテンツのコピー制御を行うことで、コンテンツを保護するセキュリティチェーン方式がある。
【０００３】
このセキュリティチェーン方式では、コンテンツを放送する放送伝送路上において、ＣＡＳ（Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）によって、当該コンテンツをスクランブルしており、コンテンツを保護している。さらに、セキュリティチェーン方式では、このスクランブルされたコンテンツ（以下、スクランブルコンテンツという）を受信側で受信する際にデスクランブルし、受信側に備えられている蓄積装置のローカル暗号で、再暗号化してコンテンツを保護している。

【０００４】
なお、ローカル暗号とは、受信側において、スクランブルコンテンツを受信する受信装置内や蓄積装置内で生成した暗号鍵と復号鍵のうち、暗号鍵を用いて、コンテンツを暗号化することをいう。ちなみに、復号鍵を用いて、再暗号化したコンテンツ（以下、再暗号化コンテンツという）を復号することを、ローカル復号という。また、デジタルコピー制御記述子によるコンテンツのコピー制御は、再暗号化したコンテンツを対象にしている。
【０００５】
このセキュリティチェーン方式では、蓄積した再暗号化コンテンツを復号する復号鍵を、受信側の受信装置または蓄積装置で管理しているため、再暗号化コンテンツを再生する毎に、課金することが難しい。つまり、セキュリティチェーン方式では、ユーザが私的利用の範囲で自由に楽しめるコンテンツ、いわゆる私的録画コンテンツが扱われている。
【０００６】
また、コンテンツを放送するデジタル放送では、コピー制御を行うのではなく、電波産業界ＡＲＩＢ　ＳＴＤ－Ｂ２５「デジタル放送におけるアクセス制御方式」で規定されているライセンス（ライセンス情報）の配信を制御することで、受信側で蓄積したコンテンツを視聴する際に再生制御するドメイン方式がある。
【０００７】
このドメイン方式では、コンテンツを送信（送出）側でスクランブルまたは暗号化したコンテンツ（以下、スクランブル／暗号化コンテンツという）と、このスクランブル／暗号化コンテンツをデスクランブルまたは復号するのに用いる復号鍵を含むライセンスを送信し、受信側でスクランブル／暗号化コンテンツをそのまま蓄積し、視聴時にライセンスに含まれている復号鍵を用いて、スクランブル／暗号化コンテンツをデスクランブルまたは復号して視聴可能にしている。
【０００８】
より詳細に説明すると、ドメイン方式では、ライセンスはＫｃ伝送用ＥＣＭセクション形式で送信されると共に、スクランブル／暗号化コンテンツはＭＰＥＧ－２　ＴＳ形式で送信されており、これらＫｃ伝送用ＥＣＭおよびＭＰＥＧ－２　ＴＳは、送信側において、共通鍵暗号化方式で暗号化されている。
【０００９】
また、ドメイン方式では、受信側の受信装置は、Ｋｃ伝送用ＥＣＭを、放送波または通信回線（ネットワーク）を介して受信し、当該受信装置内、または、当該受信装置に備えられるセキュリティモジュール内に保持する。また、受信側の受信装置は、スクランブル／暗号化コンテンツを、放送波または通信回線（ネットワーク）を介して受信し、当該受信装置内の蓄積手段、または、外部の蓄積装置に、ライセンスとは独立に蓄積する。
【００１０】
そして、ドメイン方式では、スクランブル／暗号化コンテンツを視聴する際に、Ｋｃ伝送用ＥＣＭをセキュリティモジュールに転送して、Ｋｃ伝送用ＥＣＭ（ライセンス）に従って、当該スクランブル／暗号化コンテンツの視聴が有料であると設定されている場合、課金処理を行って、当該スクランブル／暗号化コンテンツを復号できる状態にする。この状態の時に、当該スクランブル／暗号化コンテンツを復号可能な復号鍵を含むＥＣＭ－Ｋｃ（暗号化スクランブル鍵）をセキュリティモジュールに転送することで、復号化したスクランブル鍵を取得し、この取得したスクランブル鍵で、当該スクランブル／暗号化コンテンツをデスクランブルまたは復号して視聴可能にしている。
【００１１】
このドメイン方式では、スクランブル／暗号化コンテンツを視聴する際に、ライセンスが必要になるので、送信側の放送事業者がライセンスを管理し、受信側へのライセンスの配信を制御することで、スクランブル／暗号化コンテンツの再生時（視聴時）に課金することを容易に実現することができる。つまり、ドメイン方式では、再生時に課金を行うコンテンツが扱われている。
【００１２】

また、このドメイン方式では、スクランブル／暗号化コンテンツとライセンスとを非同期に（別々に）送信（送出、配信）することができ、ライセンスのみを独立して送信することができる。また、ライセンスに有効期限情報を付加することで、送信したライセンスの有効期間を設定することができる。例えば、１週間の有効期限を持つライセンスを送信すれば、スクランブル／暗号化コンテンツの視聴を１週間に限定することができ、一般的なビデオレンタルサービスと同様なサービスを実現することができる。

【特許文献１】特開２００３－１１５８３２号公報（段落００７３～段落０１７４、図１）

【発明の開示】

【発明が解決しようとする課題】

【００１３】

しかしながら、ドメイン方式では、送信側において、ライセンスを送信するライセンスサーバが、送信したライセンス全てを管理する必要があり、制作され、蓄積されるコンテンツは年々増加し続けるため、ライセンスサーバで管理するライセンス数も増加し続ける。極端な例として、２０年前に送信したスクランブル／暗号化コンテンツ（コンテンツ）のライセンスも管理する必要がある。それゆえ、送信側の放送事業者、または、コンテンツ制作者は、ライセンスの管理コストを抑制するために、ライセンスに有効期限を設けているので、ドメイン方式では、無期限に利用可能なライセンスを送信することができないという問題がある。

【００１４】

逆に、セキュリティチェーン方式では、ライセンスを必要としないので、受信側の受信装置内または蓄積装置内で生成された暗号鍵および復号鍵によって、受信したスクランブルコンテンツのローカル暗号およびローカル復号を行っている。このため、当該スクランブルコンテンツを無期限に視聴することができるが、ユーザが私的利用の範囲で自由に楽しめるコンテンツ、いわゆる私的録画コンテンツしか取り扱うことができないという問題がある。

【００１５】

そこで、本発明では、前記した問題を解決し、ドメイン方式におけるライセンス管理を行う必要がなく、無期限に利用可能なライセンスを送信することができ、再生時に課金を行うコンテンツも取り扱うことができるコンテンツ送信装置およびコンテンツ送信プログラム、並びに、コンテンツ受信装置およびコンテンツ受信プログラムを提供することを目的とする。

【課題を解決するための手段】

【００３１】

請求項１記載のコンテンツ受信装置は、コンテンツを視聴できる期限を無期限に設定可能な期限情報を含むライセンス情報が暗号化され、暗号化されたＫｃ伝送用ＥＣＭと、当該コンテンツがスクランブルされたスクランブルコンテンツとが多重化された多重化スクランブルコンテンツを受信するコンテンツ受信装置であって、第一分離手段と、ＥＭＭ復号手段と、Ｋｃ伝送用ＥＣＭ復号手段と、スクランブル鍵第一復号手段と、蓄積場所判定手段と、Ｋｃ伝送用ＥＣＭ再暗号化手段と、再多重化手段と、再多重化スクランブルコンテンツ蓄積手段と、ライセンス情報保持手段と、第二分離手段と、再暗号化Ｋｃ伝送用ＥＣＭ復号手段と、スクランブル鍵第二復号手段と、デスクランブル手段と、を備える構成とした。

【００３２】

かかる構成によれば、コンテンツ受信装置は、第一分離手段によって、受信した多重化スクランブルコンテンツを、コンテンツがスクランブル鍵でスクランブルされたスクランブルコンテンツと、スクランブル鍵を含むスクランブル鍵関連情報が所定期間毎に更新されるワーク鍵で暗号化されたＥＣＭ－Ｋｗと、ライセンス情報がワーク鍵で暗号化されたＫｃ伝送用ＥＣＭと、ワーク鍵を含むワーク鍵関連情報が予め保持されているマスター鍵と同じマスター鍵で暗号化されたＥＭＭとに分離する。なお、この第一分離手段は、多重

化スクランブルコンテンツに多重化されているものを一度に全て分離することも可能であるし、多重化されているものを必要に応じて、段階的に分離することも可能である。

【００３３】

続いて、コンテンツ受信装置は、ＥＭＭ復号手段によって、第一分離手段で分離されたＥＭＭを、予め保持されているマスター鍵で復号して、ワーク鍵を含むワーク鍵関連情報を出力し、Ｋｃ伝送用ＥＣＭ復号手段によって、第一分離手段で分離されたＫｃ伝送用ＥＣＭを、ＥＭＭ復号手段で出力されたワーク鍵で復号して、ライセンス情報を出力する。

【００３４】

ここで、実時間（リアルタイム）で、スクランブルコンテンツをデスクランブルする際（コンテンツを視聴する際）には、コンテンツ受信装置は、スクランブル鍵第一復号手段によって、第一分離手段で分離されたＥＣＭ－Ｋｗを、ワーク鍵で復号して、ＥＣＭ－Ｋｗに含まれているスクランブル鍵を出力し、デスクランブル手段に出力する。

【００３５】

なお、これらＥＭＭ復号手段、Ｋｃ伝送用ＥＣＭ復号手段およびスクランブル鍵第一復号手段は、マスター鍵、ワーク鍵およびスクランブル鍵を保護する目的で、コンテンツ受信装置で用いられる、耐タンパー性のセキュアな（安全な、内部に収められたデータの改ざんが行われることがない）セキュリティモジュール内に備えられている。

【００３６】

そして、コンテンツ受信装置は、蓄積場所判定手段によって、ライセンス情報に含まれている、スクランブルコンテンツを視聴可能な期限が無期限または有限に設定された期限情報と、自体を蓄積する場所を指定する蓄積場所情報の暗号化Ｋｃ蓄積場所指定の値とに基づいて、自体の出力先を判定し、期限情報が無期限に設定されている場合には蓄積場所情報によらずに再多重化スクランブルコンテンツ蓄積手段を自体の出力先として判定する。期限情報は、スクランブルコンテンツを視聴可能な期限が無期限（期限無し）または、有限（任意長の期間）に設定されたものである。蓄積場所情報では、ライセンス情報の蓄積場所（出力先）が、コンテンツ受信装置本体内の記憶手段（例えば、不揮発性のメモリ等）若しくは蓄積手段（例えば、ハードディスクドライブ等）、または、セキュリティモジュール内の記憶手段（例えば、不揮発性のメモリ等）、或いは、当該コンテンツ受信装置に接続される外部蓄積手段（例えば、外部接続のハードディスクドライブや光ディスクドライブ等）に指定されている。

【００３７】

そうすると、コンテンツ受信装置は、Ｋｃ伝送用ＥＣＭ再暗号化手段によって、蓄積場所判定手段による判定結果に従って、ライセンス情報を予め受信側で保持されている固有鍵で再暗号化し、この再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを出力する。つまり、蓄積場所判定手段で出力先を判定した結果、ライセンス情報をセキュリティモジュールの外に出力する場合には、このＫｃ伝送用ＥＣＭ再暗号化手段で再暗号化する。

【００３８】

そして、コンテンツ受信装置は、再多重化手段によって、第一分離手段で分離されたスクランブルコンテンツと、多重化スクランブルコンテンツに多重化されていた、スクランブル鍵関連情報がコンテンツ毎に設定されるコンテンツ鍵で暗号化されたＥＣＭ－Ｋｃと、Ｋｃ伝送用ＥＣＭ再暗号化手段で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭとを再多重化した再多重化スクランブルコンテンツを出力し、再多重化スクランブルコンテンツ蓄積手段に蓄積する。この再多重化手段により、スクランブルコンテンツと、ＥＣＭ－Ｋｃと、再暗号化Ｋｃ伝送用ＥＣＭとが多重化される、すなわち、一つの纏まりにされて、再多重化スクランブルコンテンツ蓄積手段に蓄積されるので、ライセンス情報（再暗号化Ｋｃ伝送用ＥＣＭ）を紛失する心配がなくなり、スクランブルコンテンツをデスクランブルしようとした際に、ライセンス情報（再暗号化Ｋｃ伝送用ＥＣＭ）を検索したり、新たに送信側から取得する必要がなくなる。

【００３９】

また、コンテンツ受信装置は、ライセンス情報保持手段に、蓄積場所判定手段による判

定結果に従って、ライセンス情報を保持する。つまり、この場合、蓄積場所判定手段で出力先を判定した結果、ライセンス情報をセキュリティモジュール内にとどめる場合であり、そのまま再暗号化せずに保持する。

【００４０】

それから、コンテンツ受信装置は、第二分離手段によって、再多重化スクランブルコンテンツ蓄積手段に蓄積されている再多重化スクランブルコンテンツを、再暗号化Ｋｃ伝送用ＥＣＭと、ＥＣＭ－Ｋｃと、スクランブルコンテンツとに分離する。つまり、再多重化スクランブルコンテンツを視聴しようとした際には、この第二分離手段により、再多重化されているものを分離する。

【００４１】

そして、コンテンツ受信装置は、再暗号化Ｋｃ伝送用ＥＣＭ復号手段によって、第二分離手段で分離された再暗号化Ｋｃ伝送用ＥＣＭを固有鍵で復号して、ライセンス情報を、ライセンス情報保持手段に出力し、さらに、スクランブル鍵第二復号手段によって、第二分離手段で分離されたＥＣＭ－Ｋｃを、ライセンス情報に含まれているコンテンツ鍵で復号して、ＥＣＭ－Ｋｃに含まれているスクランブル鍵を出力する。

【００４２】

そして、コンテンツ受信装置は、デスクランブル手段によって、スクランブル鍵第一復号手段またはスクランブル鍵第二復号手段から出力されたスクランブル鍵で、第一分離手段または第二分離手段で分離されたスクランブルコンテンツをデスクランブルし、このデスクランブルしたコンテンツを出力する。すなわち、デスクランブル手段では、ＥＣＭ－ＫｗまたはＥＣＭ－Ｋｃのいずれかからスクランブル鍵が出力されれば、デスクランブルコンテンツをデスクランブルする。

【００４３】

請求項２記載のコンテンツ受信装置は、コンテンツを視聴できる期限を無期限に設定可能な期限情報を含むライセンス情報が暗号化され、暗号化されたＫｃ伝送用ＥＣＭと、当該コンテンツがスクランブルされたスクランブルコンテンツとが多重化された多重化スクランブルコンテンツを受信するコンテンツ受信装置であって、第一分離手段と、ＥＭＭ復号手段と、Ｋｃ伝送用ＥＣＭ復号手段と、スクランブル鍵第一復号手段と、蓄積場所判定手段と、Ｋｃ伝送用ＥＣＭ再暗号化手段と、再多重化手段と、再多重化スクランブルコンテンツ入出力手段と、ライセンス情報保持手段と、第二分離手段と、再暗号化Ｋｃ伝送用ＥＣＭ復号手段と、スクランブル鍵第二復号手段と、デスクランブル手段と、を備える構成とした。

【００４４】

かかる構成によれば、コンテンツ受信装置は、第一分離手段によって、受信した多重化スクランブルコンテンツを、コンテンツがスクランブル鍵でスクランブルされたスクランブルコンテンツと、スクランブル鍵を含むスクランブル鍵関連情報が所定期間毎に更新されるワーク鍵で暗号化されたＥＣＭ－Ｋｗと、ライセンス情報がワーク鍵で暗号化されたＫｃ伝送用ＥＣＭと、ワーク鍵を含むワーク鍵関連情報が予め保持されているマスター鍵と同じマスター鍵で暗号化されたＥＭＭとに分離する。続いて、コンテンツ受信装置は、ＥＭＭ復号手段によって、第一分離手段で分離されたＥＭＭを、予め保持されているマスター鍵で復号して、ワーク鍵を含むワーク鍵関連情報を出力し、Ｋｃ伝送用ＥＣＭ復号手段によって、第一分離手段で分離されたＫｃ伝送用ＥＣＭを、ＥＭＭ復号手段で出力されたワーク鍵で復号して、ライセンス情報を出力する。

【００４５】

そして、コンテンツ受信装置は、蓄積場所判定手段によって、ライセンス情報に含まれている、スクランブルコンテンツを視聴可能な期限が無期限または有限に設定された期限情報と、自体を蓄積する場所を指定する蓄積場所情報の暗号化Ｋｃ蓄積場所指定の値とに基づいて、自体の出力先を判定し、期限情報が無期限に設定されている場合には蓄積場所情報によらずに外部蓄積装置の蓄積部を自体の出力先として判定する。そうすると、コンテンツ受信装置は、Ｋｃ伝送用ＥＣＭ再暗号化手段によって、蓄積場所判定手段による判

定結果に従って、ライセンス情報を、予め受信側で保持されている固有鍵で再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを出力する。そして、コンテンツ受信装置は、再多重化手段によって、第一分離手段で分離されたスクランブルコンテンツと、多重化スクランブルコンテンツに多重化されていた、スクランブル鍵関連情報がコンテンツ毎に設定されるコンテンツ鍵で暗号化されたＥＣＭ－Ｋｃと、Ｋｃ伝送用ＥＣＭ再暗号化手段で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭとを再多重化した再多重化スクランブルコンテンツを出力する。そして、コンテンツ受信装置は、再多重化スクランブルコンテンツ入出力手段によって、再多重化手段で再多重化された再多重化スクランブルコンテンツを、外部蓄積装置に出力する。

【００４６】

また、コンテンツ受信装置は、ライセンス情報保持手段に、蓄積場所判定手段による判定結果に従って、ライセンス情報を保持する。それから、コンテンツ受信装置は、再多重化スクランブルコンテンツ入出力手段によって、外部機器から再多重化スクランブルコンテンツを入力させ（読み込んで）、第二分離手段によって、再多重化スクランブルコンテンツを、再暗号化Ｋｃ伝送用ＥＣＭと、ＥＣＭ－Ｋｃと、スクランブルコンテンツとに分離する。そして、コンテンツ受信装置は、再暗号化Ｋｃ伝送用ＥＣＭ復号手段によって、第二分離手段で分離された再暗号化Ｋｃ伝送用ＥＣＭを、固有鍵で復号して、ライセンス情報を、ライセンス情報保持手段に出力し、スクランブル鍵第二復号手段によって、第二分離手段で分離されたＥＣＭ－Ｋｃを、ライセンス情報に含まれているコンテンツ鍵で復号して、ＥＣＭ－Ｋｃに含まれているスクランブル鍵を出力する。

【００４７】

そして、コンテンツ受信装置は、デスクランブル手段によって、スクランブル鍵第一復号手段またはスクランブル鍵第二復号手段から出力されたスクランブル鍵で、第一分離手段または第二分離手段で分離されたスクランブルコンテンツをデスクランブルし、このデスクランブルしたコンテンツを出力する。

【００５１】

請求項３記載のコンテンツ受信プログラムは、コンテンツを視聴できる期限を無期限に設定可能な期限情報を含むライセンス情報が暗号化され、暗号化されたＫｃ伝送用ＥＣＭと、当該コンテンツがスクランブルされたスクランブルコンテンツとが多重化された多重化スクランブルコンテンツを受信するために、コンピュータを、第一分離手段、ＥＭＭ復号手段、Ｋｃ伝送用ＥＣＭ復号手段、スクランブル鍵第一復号手段、蓄積場所判定手段、Ｋｃ伝送用ＥＣＭ再暗号化手段、再多重化手段、蓄積制御手段、保持制御手段、第二分離手段、再暗号化Ｋｃ伝送用ＥＣＭ復号手段、スクランブル鍵第二復号手段、デスクランブル手段、として機能させる構成とした。

【００５２】

かかる構成によれば、コンテンツ受信プログラムは、第一分離手段によって、受信した多重化スクランブルコンテンツを、スクランブルコンテンツと、ＥＣＭ－Ｋｗと、Ｋｃ伝送用ＥＣＭと、ＥＭＭとに分離する。続いて、コンテンツ受信プログラムは、ＥＭＭ復号手段によって、第一分離手段で分離されたＥＭＭを、予め保持されているマスター鍵で復号して、ワーク鍵を含むワーク鍵関連情報を出力し、Ｋｃ伝送用ＥＣＭ復号手段によって、第一分離手段で分離されたＫｃ伝送用ＥＣＭを、ＥＭＭ復号手段で出力されたワーク鍵で復号して、ライセンス情報を出力する。

【００５３】

そして、コンテンツ受信プログラムは、蓄積場所判定手段によって、ライセンス情報に含まれている、スクランブルコンテンツを視聴可能な期限が無期限または有限に設定された期限情報と、自体を蓄積する場所を指定する蓄積場所情報の暗号化Ｋｃ蓄積場所指定の値とに基づいて、自体の出力先を判定し、期限情報が無期限に設定されている場合には蓄積場所情報によらずに再多重化スクランブルコンテンツ蓄積手段を自体の出力先として判定する。そうすると、コンテンツ受信プログラムは、Ｋｃ伝送用ＥＣＭ再暗号化手段によって、蓄積場所判定手段による判定結果に従って、ライセンス情報を、予め受信側で保持

されている固有鍵で再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを出力する。そして、コンテンツ受信プログラムは、再多重化手段によって、第一分離手段で分離されたスクランブルコンテンツと、多重化スクランブルコンテンツに多重化されていたＥＣＭ－Ｋｃと、再暗号化Ｋｃ伝送用ＥＣＭとを再多重化した再多重化スクランブルコンテンツを出力する。そして、コンテンツ受信プログラムは、蓄積制御手段によって、再多重化スクランブルコンテンツを、再多重化スクランブルコンテンツ蓄積手段に蓄積させる。

【００５４】

また、コンテンツ受信プログラムは、保持制御手段によって、ライセンス情報保持手段に、蓄積場所判定手段による判定結果に従って、ライセンス情報を保持する。それから、コンテンツ受信プログラムは、第二分離手段によって、再多重化スクランブルコンテンツを、再暗号化Ｋｃ伝送用ＥＣＭと、ＥＣＭ－Ｋｃと、スクランブルコンテンツとに分離する。そして、コンテンツ受信プログラムは、再暗号化Ｋｃ伝送用ＥＣＭ復号手段によって、再暗号化Ｋｃ伝送用ＥＣＭを固有鍵で復号して、ライセンス情報を、ライセンス情報保持手段に出力し、スクランブル鍵第二復号手段によって、ＥＣＭ－Ｋｃをコンテンツ鍵で復号して、ＥＣＭ－Ｋｃに含まれているスクランブル鍵を出力する。

【００５５】

そして、コンテンツ受信プログラムは、デスクランブル手段によって、スクランブル鍵第一復号手段またはスクランブル鍵第二復号手段から出力されたスクランブル鍵で、第一分離手段または第二分離手段で分離されたスクランブルコンテンツをデスクランブルし、このデスクランブルしたコンテンツを出力する。

【発明の効果】

【００５８】

請求項１に記載の発明によれば、ライセンス情報を、当該ライセンス情報に含まれている期限情報と蓄積場所情報とに基づいて、蓄積して管理しているので、無期限に利用可能なライセンス情報を送信された場合であっても、最適な管理を行うことができる。また、ライセンス情報を用いて、スクランブルコンテンツをデスクランブルして、自由に視聴することができる。

【発明を実施するための最良の形態】

【００６０】

次に、本発明の実施形態について、適宜、図面を参照しながら詳細に説明する。

まず、コンテンツ送信装置の構成と動作とを説明し、次に、コンテンツ受信装置（第一実施形態、第二実施形態）の構成と動作（放送受信時［リアルタイム視聴時］、蓄積再生時）とを説明する。

【００６１】

〈コンテンツ送信装置の構成〉

図１は、コンテンツ送信装置のブロック図である。図１に示すように、コンテンツ送信装置１は、コンテンツをスクラブルしたスクランブルコンテンツの視聴可能な期限を無期限または有限に設定することができるように、当該スクランブルコンテンツと、スクラブルを解除して視聴可能にするライセンス情報とを送信するもので、コンテンツ記憶手段３と、スクランブル手段５と、ＥＣＭ－Ｋｗ（ワーク鍵暗号化関連情報）生成手段７と、ＥＣＭ－Ｋｃ（コンテンツ鍵暗号化関連情報）生成手段９と、ライセンス情報設定手段１１と、Ｋｃ伝送用ＥＣＭ（暗号化ライセンス情報）生成手段１３と、ＥＭＭ（ワーク鍵暗号化個別情報）生成手段１５と、多重化手段１７とを備えている。

【００６２】

コンテンツ記憶手段３は、ハードディスクドライブ等の大容量の記憶媒体によって構成されており、予め送信するコンテンツを記憶させておくものである。このコンテンツ記憶手段３は、当該装置１を管理運営する放送事業者が操作する操作手段（図示せず）からの操作信号に従って、記憶しているコンテンツをスクランブル手段５に出力する。なお、コンテンツは、映像データや音声データ等をＭＰＥＧ－２　ＴＳ　符号化方式で符号化したデータである。

【００６３】
スクランブル手段５は、コンテンツ記憶手段３から出力されたコンテンツを、スクランブル鍵Ｋｓでスクランブルし、スクランブルコンテンツとして、多重化手段１７に出力するものである。スクランブル鍵Ｋｓは、数秒単位で更新（変更）されていく、暗号鍵である。
【００６４】
ＥＣＭ－Ｋｗ生成手段７は、スクランブル鍵Ｋｓを含むスクランブル鍵関連情報を、ワーク鍵Ｋｗで暗号化したＥＣＭ－Ｋｗを生成して、多重化手段１７に出力するものである。ワーク鍵Ｋｗは、放送事業者単位等で付与されているもので、所定期間毎に更新されていく、暗号鍵である。ＥＣＭ－Ｋｗは、ＡＲＩＢ　ＳＴＤ－Ｂ２５「デジタル放送におけるアクセス制御方式」で定義されるＥＣＭセクション形式の情報である。このＥＣＭ－Ｋｗには、暗号化部と非暗号化部とが含まれており、暗号化部にスクランブル鍵Ｋｓ等が収められており、非暗号化部に暗号化部を復号するためのワーク鍵Ｋｗを識別するための情報等が収められている。また、このＥＣＭ－Ｋｗは、受信側でリアルタイムにスクランブルコンテンツをデスクランブルする際（リアルタイム受信時）に用いられる。
【００６５】
ＥＣＭ－Ｋｃ生成手段９は、スクランブル鍵Ｋｓを含むスクランブル鍵関連情報を、コンテンツ鍵Ｋｃで暗号化したＥＣＭ－Ｋｃを生成して、多重化手段１７に出力するものである。コンテンツ鍵Ｋｃは、コンテンツ単位で付与されている暗号鍵である。ＥＣＭ－Ｋｃは、ＡＲＩＢ　ＳＴＤ－Ｂ２５「デジタル放送におけるアクセス制御方式」で定義されるＥＣＭセクション形式の情報である。このＥＣＭ－Ｋｃには、暗号化部と非暗号化部とが含まれており、暗号化部にスクランブル鍵Ｋｓ等が収められており、非暗号化部に暗号化部を復号するためのコンテンツ鍵Ｋｃを識別するための情報等が収められている。また、このＥＣＭ－Ｋｃは、受信側で蓄積され、蓄積されたスクランブルコンテンツをデスクランブルする際（蓄積再生時）に用いられる。
【００６６】
ライセンス情報設定手段１１は、コンテンツ鍵Ｋｃと、有効期限情報（期限情報）と、蓄積場所情報と、再生課金情報とを含むライセンス情報を、当該装置１の使用者（放送事業者）が操作手段（キーボード、マウス等、図示せず）を操作した結果である操作信号に従って、設定すると共に、設定したライセンス情報をＫｃ伝送用ＥＣＭ生成手段１３に出力するものである。
【００６７】
有効期限情報は、受信側でスクランブルコンテンツを視聴可能な期限を、送信側で無期限（期限無し）または有限（任意長の期間）に設定したもの、すなわち、コンテンツ鍵Ｋｃの有効期限を設定したものであり、ＲＭＰＩ（Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ　＆　Ｐｒｏｔｅｃｔｉｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ）記述子によって記述されたものである。
【００６８】
蓄積場所情報は、受信側で自体（Ｋｃ伝送用ＥＣＭ）の蓄積する蓄積場所（出力先）が蓄積場所記述子によって記述されたものである。受信側の蓄積場所は、受信側のコンテンツ受信装置本体内の記憶手段（例えば、不揮発性のメモリ等）若しくは蓄積手段（例えば、ハードディスクドライブ等）、または、セキュリティモジュール内の記憶手段（例えば、不揮発性のメモリ等）、或いは、当該コンテンツ受信装置に接続される外部蓄積手段（例えば、外部接続のハードディスクドライブや光ディスクドライブ等）に指定されている。
【００６９】
また、蓄積場所情報は、受信側で、ライセンス情報をスクランブルコンテンツと独立して蓄積させるか、ライセンス情報をスクランブルコンテンツと多重化して蓄積させるかのいずれかを指定するものである。
【００７０】

再生課金情報は、スクランブルコンテンツを復号したコンテンツを再生するのにかかる料金が、再生課金記述子によって記述されたものである。この再生課金情報は、例えば、一般的なビデオレンタルサービスと同様に、コンテンツを１回視聴するのに数百円を課金するように設定されている。

【００７１】

この実施の形態では、ライセンス情報には、コンテンツ鍵Ｋｃと、有効期限情報と、蓄積場所情報と、再生課金情報とが含まれているが、受信側で最低限必要な、スクランブルコンテンツを視聴可能にする期限を設定した有効期限情報が少なくとも含まれていればよい。

【００７２】

Ｋｃ伝送用ＥＣＭ生成手段１３は、ライセンス情報設定手段１１で設定されたライセンス情報を、ワーク鍵Ｋｗで暗号化したＫｃ伝送用ＥＣＭを生成して、多重化手段１７に出力するものである。

【００７３】

Ｋｃ伝送用ＥＣＭは、ＡＲＩＢ　ＳＴＤ－Ｂ２５「デジタル放送におけるアクセス制御方式」で定義されるＥＣＭセクション形式の情報である。ここで、図２を参照して、Ｋｃ伝送用ＥＣＭのフォーマットについて説明する（適宜、図１参照）。

【００７４】

図２（ａ）に示すように、Ｋｃ伝送用ＥＣＭのフォーマットを説明した表では、「暗号」、「固定」「項目」、「バイト長」および「備考」の欄が設けられている。また、Ｋｃ伝送用ＥＣＭは、８バイト長のＥＣＭセクションヘッダと、「暗号」の欄に記載されている非暗号化部および暗号化部（Ｋｃ伝送用ＥＣＭ本体）と、４バイト長のセクションＣＲＣとからなっている。非暗号化部は、ワーク鍵Ｋｗで暗号化されない部分であり、予め固定された固定部であり、アクセス制御方式の種別を示す１バイト長のプロトコル番号と、放送事業者を識別する３バイト長の事業体識別と、ワーク鍵Ｋｗを識別する１バイト長のワーク鍵識別とからなっている。また、暗号化部は、ワーク鍵Ｋｗで暗号化される部分であり、各種の機能情報を設置可能な可変部と、改ざんを検出するための４バイト長の改竄（ざん）検出とからなっている。なお、可変部は、記述子を、順序不定、個数不定に、送信側で自由に挿入することができる部分であり、この可変部の詳細を図２（ｂ）に示す。

【００７５】

図２（ｂ）に示すように、可変部のフォーマットを説明した表では、「記述子」「項目名」、「バイト長」および「備考」の欄が設けられている。この「記述子」の欄には、コンテンツ鍵記述子と、蓄積場所記述子と、再生課金記述子と、ＲＭＰＩ記述子とが記載されている。

【００７６】

コンテンツ鍵記述子には、記述子を識別する１バイト長の記述子タグ、記述子の長さを示す１バイト長の記述子長、コンテンツ鍵を識別するための６バイト長のコンテンツ鍵識別および８（３２）バイト長のコンテンツ鍵が含まれている。

【００７７】

蓄積場所記述子には、記述子を識別する１バイト長の記述子タグ、記述子の長さを示す１バイト長の記述子長およびＫｃ伝送用ＥＣＭを蓄積する場所を示すｎバイト長の暗号化Ｋｃ蓄積場所指定が含まれている。暗号化Ｋｃ蓄積場所指定が“０ｘ００”の場合、ＩＣカード（セキュリティモジュール）内に蓄積することを指定しており、“０ｘ０１”の場合、受信機本体内に蓄積することを指定しており、“０ｘ１Ｘ”の場合、蓄積媒体内に蓄積することを指定している。

【００７８】

なお、この蓄積場所記述子では、暗号化Ｋｃ蓄積場所指定を“０ｘ０１”にした場合（受信機本体内に蓄積）または“０ｘ１Ｘ”にした場合（蓄積媒体内に蓄積）、ライセンス情報をスクランブルコンテンツと多重化することを指定しており、それ以外は、ライセンス情報とスクランブルコンテンツとを別々にしておく（独立にしておくこと）を指定して

いる。

【００７９】

再生課金記述子には、記述子を識別する１バイト長の記述子タグ、記述子の長さを示す１バイト長の記述子長およびコンテンツを視聴するために必要な料金等を示すｎバイト長の再生課金情報が含まれている。

ＲＭＰＩ記述子には、記述子を識別する１バイト長の記述子タグ、記述子の長さを示す１バイト長の記述子長およびコンテンツ鍵Ｋｃの有効期限を示す６バイト長の有効期限が含まれている。この有効期限が、無期限（期限無し）または有限（任意長の期間）に設定される。

【００８０】

図１に戻って、コンテンツ送信装置１の各構成の説明を続ける。

ＥＭＭ生成手段１５は、ワーク鍵Ｋｗを含むワーク鍵関連情報を、受信側に予め保持されている鍵と同じマスター鍵Ｋｍで暗号化したＥＭＭを生成して、多重化手段１７に出力するものである。ＥＭＭは、ＡＲＩＢ　ＳＴＤ－Ｂ２５「デジタル放送におけるアクセス制御方式」で定義されるＥＭＭセクション形式の情報である。なお、マスター鍵Ｋｍは、受信側に備えられるコンテンツ受信装置に用いられるセキュリティモジュール毎に付与されているものと同様のものである。

【００８１】

多重化手段１７は、スクランブル手段５から出力されたスクランブルコンテンツと、ＥＣＭ－Ｋｗ生成手段７から出力されたＥＣＭ－Ｋｗと、ＥＣＭ－Ｋｃ生成手段９から出力されたＥＣＭ－Ｋｃと、Ｋｃ伝送用ＥＣＭ生成手段１３から出力されたＫｃ伝送用ＥＣＭと、ＥＭＭ生成手段１５から出力されたＥＭＭと、ＥＩＴ（Ｅｖｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）やＳＤＴ（Ｓｅｒｖｉｃｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｔａｂｌｅ）等の番組送出情報とを多重化し、ＭＰＥＧ－２　ＴＳのストリーム形式の多重化スクランブルコンテンツを生成して出力（送出）するものである。

【００８２】

なお、この多重化手段１７は、多重化スクランブルコンテンツを、放送波、または、ネットワーク（インターネット等）によって、受信側に向けて出力（送出、配信）することが可能である。

【００８３】

ここで、図３を参照して、多重化手段１７から出力される多重化スクランブルコンテンツの送出フォーマットについて説明する。

図３に示すように、多重化手段１７によって送信されるコンテンツ（多重化スクランブルコンテンツ）の送出フォーマットは、ＭＰＥＧ－２　ＳＹＳＴＥＭＳに従っており、このＭＰＥＧ－２　ＴＳは、１つのパケットが１８８Ｂｙｔｅで構成されている。また、このＭＰＥＧ－２　ＴＳには、コンテンツの映像や音声が圧縮されたＶｉｄｅｏパケットやＡｕｄｉｏパケットが多重化されている。Ｖｉｄｅｏパケットは、例えば、２０ＭＢｙｔｅのデータ量を有しており、Ａｕｄｉｏパケットは、例えば、１２８ｋＢｙｔｅのデータ量を有している。

【００８４】

また、多重化スクランブルコンテンツには、Ｋｃ伝送用ＥＣＭが多重化されており、このＫｃ伝送用ＥＣＭは、セクション形式で多重化され、１つのコンテンツ（多重化スクランブルコンテンツ）が放送されている間、繰り返し多重化されている。このＫｃ伝送用ＥＣＭは、放送されているコンテンツを途中から受信する場合を想定して、１００ｍｓの間隔で繰り返し多重化されている。

【００８５】

また、多重化スクランブルコンテンツには、ＥＣＭ－ＫｃおよびＥＣＭ－Ｋｗが多重化されている。このＥＣＭ－ＫｃおよびＥＣＭ－Ｋｗは、コンテンツが数秒単位のブロックで分割され、この分割されたブロックを異なるスクランブル鍵Ｋｓで暗号化するために、数秒単位で異なる当該スクランブル鍵Ｋｓが含まれている。このＥＣＭ－ＫｃおよびＥＣ

Ｍ－Ｋｗは、放送されているコンテンツを途中から受信する場合を想定して、１００ｍｓの間隔で繰り返し多重化されている。

【００８６】

図１に示したコンテンツ送信装置１が奏する効果を説明する。

このコンテンツ送信装置１によれば、ライセンス情報設定手段１１で設定したライセンス情報に、コンテンツの視聴可能な期限を無期限または有限に設定可能な有効期限情報、すなわち、コンテンツ鍵Ｋｃの有効期限を無期限または有限に設定したＲＭＰＩ記述子を含めており、当該ライセンス情報を、スクランブルコンテンツと共に多重化手段１７によって多重化して送信しているので、視聴可能な期限を無期限とした有効期限情報を含めれば、ドメイン方式におけるライセンス管理を行う必要がなく、無期限に利用可能なライセンス情報を送信することができる。さらに、コンテンツ送信装置１によれば、ライセンス情報に、視聴可能な期限を有限とした有効期限情報を含めた上で、例えば、スクランブルコンテンツを再生するのにかかる料金を示す再生課金情報を含めれば、再生時に課金を行うコンテンツも取り扱うことができる。

【００８７】

また、有効期限情報を無期限（コンテンツ鍵Ｋｃの有効期限を無期限）に設定した場合であっても、多重化スクランブルコンテンツを送信時に課金するのではなく、受信側で、多重化スクランブルコンテンツからスクランブルコンテンツを分離した後で、このスクランブルコンテンツを復号したログ（視聴履歴）に基づいて、課金することも可能である。

【００８８】

さらに、このコンテンツ送信装置１によれば、ライセンス情報に含ませる蓄積場所情報に、受信側で当該ライセンス情報を蓄積する場所を指定することと、スクランブルコンテンツと多重化して蓄積させるか、独立して蓄積させるかを指定することとが可能であるので、受信側でのライセンス情報の管理を設定することができる。これによって、受信側で、ライセンス情報を紛失したりする虞を防止することができ、例えば、スクランブルコンテンツをデスクランブルしようとした際に、ライセンス情報を検索する必要がなくなり、受信側で、ライセンス情報の最適な管理を行うことができる。

【００８９】

〈コンテンツ送信装置の動作〉

次に、図４に示すフローチャートを参照して、コンテンツ送信装置１の動作を説明する（適宜、図１参照）。

まず、コンテンツ送信装置１は、コンテンツ記憶手段３に記憶されているコンテンツを、スクランブル手段５によって、スクランブル鍵Ｋｓを用いてスクランブルする（ステップＳ１）。続いて、コンテンツ送信装置１は、スクランブル鍵Ｋｓを含むスクランブル鍵関連情報を、ＥＣＭ－Ｋｗ生成手段７によって、ワーク鍵Ｋｗを用いて暗号化し、ＥＣＭ－Ｋｗを生成する（ステップＳ２）。

【００９０】

また、コンテンツ送信装置１は、スクランブル鍵Ｋｓを含むスクランブル鍵関連情報を、ＥＣＭ－Ｋｃ生成手段９によって、コンテンツ鍵Ｋｃを用いて暗号化し、ＥＣＭ－Ｋｃを生成する（ステップＳ３）。次に、コンテンツ送信装置１は、コンテンツ鍵Ｋｃ、有効期限情報、蓄積場所情報および再生課金情報を含むライセンス情報を、ライセンス情報設定手段１１によって設定し、Ｋｃ伝送用ＥＣＭ生成手段１３によって、ワーク鍵Ｋｗを用いて暗号化し、Ｋｃ伝送用ＥＣＭを生成する（ステップＳ４）。

【００９１】

そして、コンテンツ送信装置１は、ワーク鍵Ｋｗを含むワーク鍵関連情報を、ＥＭＭ生成手段１５によって、マスター鍵を用いて暗号化し、ＥＭＭを生成する（ステップＳ５）。それから、コンテンツ送信装置１は、スクランブル手段５でスクランブルされたスクランブルコンテンツと、ＥＣＭ－Ｋｗ生成手段７で生成されたＥＣＭ－Ｋｗと、ＥＣＭ－Ｋｃ生成手段９で生成されたＥＣＭ－Ｋｃと、Ｋｃ伝送用ＥＣＭ生成手段１３で生成されたＫｃ伝送用ＥＣＭと、ＥＭＭ生成手段１５で生成されたＥＭＭと、番組送出情報とを多重

化して、多重化スクランブルコンテンツとして送信する（ステップＳ６）。

【００９２】

〈コンテンツ受信装置の構成（第一実施形態）〉

次に、コンテンツ受信装置（第一実施形態）について説明する。図５は、コンテンツ受信装置のブロック図である。図５に示すように、コンテンツ受信装置２１は、送信側から送信された多重化スクランブルコンテンツを受信する受信装置本体２３と、暗号鍵等の秘匿性の高い情報を保持したり、処理したりする耐タンパー性のセキュリティモジュール２５とから構成されている。

【００９３】

コンテンツ受信装置２１の受信装置本体２３は、第一分離手段２７と、再多重化手段４１と、不揮発性メモリ手段４３と、蓄積手段（再多重化スクランブルコンテンツ蓄積手段）４５と、第二分離手段４７と、デスクランブル手段（スクランブルコンテンツデスクランブル手段）５７とを備えており、セキュリティモジュール２５は、ＥＭＭ復号手段２９と、ワーク鍵保持手段３１と、Ｋｃ伝送用ＥＣＭ復号手段（暗号化ライセンス情報復号手段）３３と、スクランブル鍵第一復号手段３５と、蓄積場所判定手段３７と、Ｋｃ伝送用ＥＣＭ再暗号化手段３９と、再暗号化Ｋｃ伝送用ＥＣＭ復号手段（再暗号化ライセンス情報復号手段）４９と、Ｋｃ伝送用ＥＣＭ保持手段（ライセンス情報保持手段）５１と、有効期限判定手段５３と、スクランブル鍵第二復号手段５５とを備えている。以下、多重化スクランブルコンテンツがリアルタイムに再生される場合、蓄積される場合を区別することなく、処理される順に各構成を説明していく。

【００９４】

ちなみに、コンテンツ受信装置２１で受信された多重化スクランブルコンテンツがリアルタイムに再生される場合は、デスクランブル手段５７によって、第一分離手段２７で多重化スクランブルコンテンツから分離されたスクランブルコンテンツがスクランブル鍵第一復号手段３５から出力されたスクランブル鍵Ｋｓで復号されてコンテンツとして出力される。

【００９５】

また、コンテンツ受信装置２１で受信された多重化スクランブルコンテンツが蓄積される場合は、多重化スクランブルコンテンツから分離されて復号されたＫｃ伝送用ＥＣＭがセキュリティモジュール２５内のＫｃ伝送用ＥＣＭ保持手段５１に保持されると共に、スクランブルコンテンツが蓄積手段４５に独立して蓄積されるか、または、復号されたＫｃ伝送用ＥＣＭが再暗号化されて再暗号化Ｋｃ伝送用ＥＣＭとして不揮発性メモリ手段４３に記憶されると共に、スクランブルコンテンツが蓄積手段４５に独立して蓄積されるか、或いは、再多重化手段４１で再暗号化Ｋｃ伝送用ＥＣＭとスクランブルコンテンツとが多重化されて蓄積手段４５に蓄積される。

【００９６】

第一分離手段２７は、放送（放送波）により伝播される、または、ネットワークによって配信される多重化スクランブルコンテンツ（ＭＰＥＧ－２　ＴＳ）を受信し、この受信した多重化スクランブルコンテンツを分離するもので、ＥＭＭ分離部２７ａと、Ｋｃ伝送用ＥＣＭ第一分離部２７ｂと、ＥＣＭ－Ｋｗ分離部２７ｃとを備えている。

【００９７】

ＥＭＭ分離部２７ａは、多重化スクランブルコンテンツに多重化されているＥＭＭを分離して、セキュリティモジュール２５に備えられているＥＭＭ復号手段２９に出力すると共に、ＥＭＭを分離した多重化スクランブルコンテンツをＫｃ伝送用ＥＣＭ第一分離部２７ｂに出力するものである。

【００９８】

Ｋｃ伝送用ＥＣＭ第一分離部２７ｂは、多重化スクランブルコンテンツに多重化されているＫｃ伝送用ＥＣＭを分離して、セキュリティモジュール２５に備えられているＫｃ伝送用ＥＣＭ復号手段３３に出力すると共に、Ｋｃ伝送用ＥＣＭを分離した多重化スクランブルコンテンツをＥＣＭ－Ｋｗ分離部２７ｃに出力するものである。

【００９９】
ＥＣＭ－Ｋｗ分離部２７ｃは、多重化スクランブルコンテンツに多重化されているＥＣＭ－Ｋｃを分離して、セキュリティモジュール２５に備えられているスクランブル鍵第一復号手段３５に出力すると共に、再多重化手段４１およびデスクランブル手段５７に多重化スクランブルコンテンツ（スクランブルコンテンツとＥＣＭ－Ｋｃ）を出力するものである。
【０１００】
ＥＭＭ復号手段２９は、第一分離手段２７のＥＭＭ分離部２７ａで分離されたＥＭＭを、セキュリティモジュール２５内で予め保持されているマスター鍵Ｋｍを用いて復号して、ワーク鍵Ｋｗを含むワーク鍵関連情報をワーク鍵保持手段３１に出力するものである。
【０１０１】
ワーク鍵保持手段３１は、不揮発性のメモリ等によって構成されており、ＥＭＭ復号手段２９から出力されたワーク鍵関連情報を保持するものである。このワーク鍵保持手段３１で保持されているワーク鍵関連情報（ワーク鍵Ｋｗ）は、当該装置２１の使用者（視聴者）が操作手段（リモコン等、図示せず）を操作した結果である操作信号に従って、Ｋｃ伝送用ＥＣＭ復号手段３３またはスクランブル鍵第一復号手段３５に出力される。
【０１０２】
Ｋｃ伝送用ＥＣＭ復号手段３３は、第一分離手段２７のＫｃ伝送用ＥＣＭ第一分離部２７ｂで分離されたＫｃ伝送用ＥＣＭを、ワーク鍵保持手段３１から出力されたワーク鍵Ｋｗを用いて復号して、復号したライセンス情報を蓄積場所判定手段３７に出力するものである。
【０１０３】
スクランブル鍵第一復号手段３５は、第一分離手段２７のＥＣＭ－Ｋｗ分離部２７ｃで分離されたＥＣＭ－Ｋｗを、ワーク鍵保持手段３１から出力されたワーク鍵Ｋｗを用いて復号して、復号して得られたスクランブル鍵Ｋｓを含むスクランブル鍵関連情報をデスクランブル手段５７に出力するものである。
【０１０４】
蓄積場所判定手段３７は、ライセンス情報に含まれている有効期限情報と蓄積場所情報に基づいて、当該ライセンス情報を蓄積する場所を判定するものである。つまり、蓄積場所判定手段３７では、蓄積場所情報を記述した蓄積場所記述子に含まれている暗号化Ｋｃ蓄積場所指定の４ｂｉｔの値によって、蓄積場所が決定される。ライセンス情報の蓄積場所は、受信装置本体２３の蓄積手段４５若しくは不揮発性メモリ手段４３、または、セキュリティモジュール２５のＫｃ伝送用ＥＣＭ保持手段５１である。
【０１０５】
ただし、有効期限情報によって、コンテンツ鍵Ｋｃの有効期限が無期限に設定されている場合には、蓄積場所情報によらずに、受信装置本体２３の蓄積手段４５に、多重化スクランブルコンテンツと再多重化されて蓄積されることになる。これは、多重化スクランブルコンテンツに多重化されているスクランブルコンテンツをデスクランブルするために必要なＥＣＭ－ＫｃからスクランブルＫｓを得るために、ライセンス情報に含まれているコンテンツ鍵Ｋｃを常にセットにしておくためである。
【０１０６】
この蓄積場所判定手段３７は、蓄積場所を判定した結果により、セキュリティモジュール２５の内部でライセンス情報を蓄積すると判定した場合、当該ライセンス情報を、Ｋｃ伝送用ＥＣＭ保持手段５１に出力し、セキュリティモジュール２５の外部でライセンス情報を蓄積すると判定した場合、当該ライセンス情報をＫｃ伝送用ＥＣＭ再暗号化手段３９に出力する。
【０１０７】
Ｋｃ伝送用ＥＣＭ再暗号化手段３９は、蓄積場所判定手段３７でライセンス情報をセキュリティモジュール２５の外部に蓄積すると判定した場合、当該ライセンス情報を、予めセキュリティモジュール２５毎に設定されている固有鍵を用いて再暗号化し、この再暗号

化した再暗号化Ｋｃ伝送用ＥＣＭを、再多重化手段４１または不揮発性メモリ手段４３に出力するものである。

【０１０８】

再多重化手段４１は、第一分離手段２７のＥＣＭ－Ｋｗ分離部２７ｃから出力された多重化スクランブルコンテンツ（スクランブルコンテンツとＥＣＭ－Ｋｃ）と、Ｋｃ伝送用ＥＣＭ再暗号化手段３９で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭとを再多重化して、この再多重化した再多重化スクランブルコンテンツを、蓄積手段４５に出力するものである。

【０１０９】

不揮発性メモリ手段４３は、不揮発性メモリ等によって構成されており、Ｋｃ伝送用ＥＣＭ再暗号化手段３９で再暗号化された再暗号化Ｋｃ伝送用ＥＣＭを記憶するものである。不揮発性メモリ手段４３に記憶されている再暗号化Ｋｃ伝送用ＥＣＭは、当該装置２１の使用者（視聴者）が操作手段（リモコン等、図示せず）を操作した結果である操作信号に従って、再暗号化Ｋｃ伝送用ＥＣＭ復号手段４９に出力される。

【０１１０】

蓄積手段４５は、ハードディスクドライブ等によって構成されており、再多重化手段４１で再多重化された再多重化スクランブルコンテンツを蓄積するものである。この蓄積手段４５に蓄積されている再多重化スクランブルコンテンツは、当該装置２１の使用者（視聴者）が操作手段（リモコン等、図示せず）を操作した結果である操作信号に従って、第二分離手段４７に出力される。

【０１１１】

第二分離手段４７は、蓄積手段４５から出力された再多重化スクランブルコンテンツを分離するもので、Ｋｃ伝送用ＥＣＭ第二分離部４７ａと、ＥＣＭ－Ｋｃ分離部４７ｂとを備えている。

【０１１２】

Ｋｃ伝送用ＥＣＭ第二分離部４７ａは、再多重化スクランブルコンテンツから再暗号化Ｋｃ伝送用ＥＣＭを分離して、再暗号化Ｋｃ伝送用ＥＣＭ復号手段４９に出力すると共に、再暗号化Ｋｃ伝送用ＥＣＭを分離した再多重化スクランブルコンテンツをＥＣＭ－Ｋｃ分離部４７ｂに出力するものである。

【０１１３】

ＥＣＭ－Ｋｃ分離部４７ｂは、Ｋｃ伝送用ＥＣＭ第二分離部４７ａで再暗号化Ｋｃ伝送用ＥＣＭを分離した再多重化スクランブルコンテンツを、ＥＣＭ－Ｋｃとスクランブルコンテンツと分離すると共に、分離したＥＣＭ－Ｋｃをスクランブル鍵第二復号手段５５に出力し、分離したスクランブルコンテンツをデスクランブル手段５７に出力するものである。

【０１１４】

再暗号化Ｋｃ伝送用ＥＣＭ復号手段４９は、不揮発性メモリ手段４３または第二分離手段４７のＫｃ伝送用ＥＣＭ第二分離部４７ａから出力された再暗号化Ｋｃ伝送用ＥＣＭを、予めセキュリティモジュール２５毎に設定されている固有鍵を用いて復号し、復号したライセンス情報を、Ｋｃ伝送用ＥＣＭ保持手段５１に出力するものである。

【０１１５】

Ｋｃ伝送用ＥＣＭ保持手段５１は、不揮発性のメモリ等によって構成されており、蓄積場所判定手段３７または再暗号化Ｋｃ伝送用ＥＣＭ復号手段４９から出力されたライセンス情報を保持するものである。このＫｃ伝送用ＥＣＭ保持手段５１に保持されているライセンス情報は、当該装置２１の使用者（視聴者）が操作手段（リモコン等、図示せず）を操作した結果である操作信号に従って、有効期限判定手段５３に出力される。

【０１１６】

有効期限判定手段５３は、Ｋｃ伝送用ＥＣＭ保持手段５１から出力されたライセンス情報に含まれている有効期限情報の有効期限（コンテンツ鍵Ｋｃの有効期限）を判定するものである。この有効期限判定手段５３で有効期限情報の有効期限を判定した結果、コンテ

ンツ鍵Ｋｃの有効期限が無期限に設定されているか、コンテンツ鍵Ｋｃの有効期限が期限内であれば、有効期限判定手段５３はコンテンツ鍵Ｋｃをスクランブル鍵第二復号手段５５に出力する。また、コンテンツ鍵Ｋｃの有効期限が切れている場合には、その旨を、当該装置２１の使用者（視聴者）に、表示手段（図示せず）を介して通知する。

【０１１７】

スクランブル鍵第二復号手段５５は、第二分離手段４７のＥＣＭ－Ｋｃ分離部４７ｂから出力されたＥＣＭ－Ｋｃを、有効期限判定手段５３から出力されたコンテンツ鍵Ｋｃを用いて復号して、復号して得られたスクランブル鍵Ｋｓを含むスクランブル鍵関連情報をデスクランブル手段５７に出力するものである。

【０１１８】

デスクランブル手段５７は、第一分離手段２７から出力された多重化スクランブルコンテンツまたは第二分離手段４７から出力された再多重化スクランブルコンテンツを、スクランブル鍵第一復号手段３５またはスクランブル鍵第二復号手段５５から出力されたスクランブル鍵Ｋｓ（スクランブル鍵関連情報）を用いて、デスクランブルして、デスクランブルしたコンテンツを、図示を省略した表示手段に出力するものである。

【０１１９】

このコンテンツ受信装置２１によれば、蓄積場所判定手段３７により、ライセンス情報を、当該ライセンス情報に含まれている有効期限情報と蓄積場所情報とに基づいて、蓄積して管理しているので、無期限に利用可能なライセンス情報が送信された場合であっても、例えば、ライセンス情報と多重化スクランブルコンテンツと再多重化しておくことで、最適な管理を行うことができる。また、ライセンス情報に含まれているコンテンツ鍵Ｋｃを用いて、ＥＣＭ－Ｋｃからスクランブル鍵Ｋｓを得て、スクランブルコンテンツをデスクランブルして、コンテンツを自由に視聴することができる。

【０１２０】

〈コンテンツ受信装置の構成（第二実施形態）〉

次に、コンテンツ受信装置（第二実施形態）について説明する。図６は、コンテンツ受信装置のブロック図である。図６に示すように、コンテンツ受信装置２１Ａは、受信装置本体２３Ａと外部蓄積装置２２との間で再多重化スクランブルコンテンツの入出力を行えるように構成したもので、図５に示したコンテンツ受信装置２１から不揮発性メモリ手段４３および蓄積手段４５を除いて、新たに、高速デジタルＩ／Ｆ手段５９を付加したものである。なお、この高速デジタルＩ／Ｆ手段５９以外の構成は、コンテンツ受信装置２１と同じであるので、同一の符号を付して、その説明を省略する。

【０１２１】

高速デジタルＩ／Ｆ手段５９は、受信装置本体２３Ａと外部蓄積装置２２との間において、多重化スクランブルコンテンツ（ＭＰＥＧ－２　ＴＳ）または再多重化スクランブルコンテンツの入出力を行うもので、いわゆる高速デジタルインターフェースである。この実施形態では、ＩＥＥＥ１３９４に則した、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｍｅｔｈｏｄ）と呼ばれる暗号化システムを採用している。

【０１２２】

外部蓄積装置２２は、高速デジタルＩ／Ｆ手段５９に対応するインターフェースである高速デジタルＩ／Ｆ部２４と、入力した多重化スクランブルコンテンツまたは再多重化スクランブルコンテンツを蓄積する蓄積部２６とを備えている。

【０１２３】

なお、このコンテンツ受信装置２１Ａは、受信した多重化スクランブルコンテンツ（ＭＰＥＧ－２　ＴＳ）のＰＭＴ内に含まれているデジタルコピー制御子を参照して、コピー制御情報を取得しており、このコンテンツ受信装置２１Ａに接続されている外部蓄積装置２２では、多重化スクランブルコンテンツ（ＭＰＥＧ－２　ＴＳ）を、コピー制御情報に従って、復号したり、再暗号化したりして蓄積する。

【０１２４】

ここで、図７を参照して、コンテンツの蓄積フォーマットについて説明する（適宜、図５、図６参照）。コンテンツ受信装置２１Ａ（２１）では、受信装置本体２３Ａ（２３）内で保持しているＭＰＥＧ－２ ＴＳ（多重化スクランブルコンテンツ）の送出タイミングを規定するＳＴＣ（Ｓｙｓｔｅｍ Ｔｉｍｅ Ｃｌｏｃｋ）を用いて、受信した１８８ＢｙｔｅのＭＰＥＧ－２ ＴＳの先頭に、４Ｂｙｔｅのタイムスタンプを付与しながら、多重化スクランブルコンテンツの蓄積を行っている。

【０１２５】

また、コンテンツ受信装置２１Ａ（２１）では、多重化スクランブルコンテンツを受信時に、当該多重化スクランブルコンテンツに多重化されていたＫｃ伝送用ＥＣＭを、セキュリティモジュール２５から得られる再暗号化Ｋｃ伝送用ＥＣＭに置き換えて再多重化する。

【０１２６】

この際に、コンテンツ受信装置２１Ａ（２１）では、外部蓄積装置２２の蓄積部２６（蓄積手段４５）に蓄積する蓄積サイズ（データ量）を小さくするために、多重化スクランブルコンテンツの蓄積開始から一番最初に得られるＫｃ伝送用ＥＣＭのみを、再暗号化Ｋｃ伝送用ＥＣＭとして、再多重化手段４１で一回だけ再多重化して、その他のＫｃ伝送用ＥＣＭは削除するように処理している。

【０１２７】

図６に示したコンテンツ受信装置２１Ａが奏する効果を説明する。

このコンテンツ受信装置２１Ａによれば、外部蓄積装置２２に、ライセンス情報を再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを多重化スクランブルコンテンツに再多重化し、この再多重化スクランブルコンテンツを蓄積させることで、ライセンス情報の最適な管理を行うことができる。また、高速デジタルＩ／Ｆ手段５９によって、外部蓄積装置２２から再多重化スクランブルコンテンツを読み出して、第二分離手段４７で分離後、当該ライセンス情報を用いて、分離されたスクランブルコンテンツをデスクランブルし、デスクランブルしたコンテンツを自由に視聴することができる。

【０１２８】

また、このコンテンツ受信装置２１Ａによれば、再多重化スクランブルコンテンツにおいて、再暗号化Ｋｃ伝送用ＥＣＭ（ライセンス情報）とスクランブルコンテンツとをストリームとして、外部蓄積装置２２に多重化して出力しているので、当該再多重化スクランブルコンテンツを、従来のＩＥＥＥ１３９４を備えるＤ－ＶＨＳ録画装置に録画（蓄積）させることができる。

【０１２９】

〈コンテンツ受信装置の動作（第一実施形態、放送受信時［リアルタイム視聴時］）〉

次に、図８に示すフローチャートを参照して、コンテンツ受信装置２１（第一実施形態）の放送受信時（リアルタイム視聴時）の動作について説明する（適宜、図５参照）。

まず、コンテンツ受信装置２１は、多重化スクランブルコンテンツの放送受信を開始すると（ステップＳ１１）、第一分離手段２７のＥＭＭ分離部２７ａによって、当該コンテンツ受信装置２１のセキュリティモジュール２５宛のＥＭＭがあれば、セキュリティモジュール２５にＥＭＭを転送し、セキュリティモジュール２５内にて、ワーク鍵Ｋｗを設定する（ステップＳ１２）。つまり、ＥＭＭ復号手段２９によりワーク鍵Ｋｗを得て、この得られたワーク鍵Ｋｗをワーク鍵保持手段３１に保持させる。

【０１３０】

続いて、コンテンツ受信装置２１は、当該装置２１の使用者が操作手段（リモコン等、図示せず）を操作した結果である操作信号に従って、多重化スクランブルコンテンツをリアルタイム視聴するか蓄積受信するか判定する（ステップＳ１３）。リアルタイム視聴すると判定した場合、コンテンツ受信装置２１は、第一分離手段２７は、受信している番組送出情報に含まれるＰＭＴに従って、ＥＣＭ－Ｋｗ分離部２７ｃにより、多重化スクランブルコンテンツからＥＣＭ－Ｋｗを選択し（ステップＳ１４）、分離後、分離したＥＣＭ－Ｋｗをセキュリティモジュール２５に転送し、スクランブル鍵第一復号手段３５によっ

てスクランブル鍵Ｋｓを取得する（ステップＳ１５）。
【０１３１】
そして、コンテンツ受信装置２１は、デスクランブル手段５７によって、スクランブル鍵Ｋｓにより、コンテンツ（スクランブルコンテンツ）のデスクランブルを行って、図示を省略したデコーダに入力し（ステップＳ１６）、デコードした後、表示手段（図示せず）に表示する。当該装置２１の使用者は、この表示手段に表示されたコンテンツを視聴する（ステップＳ１７）。
【０１３２】
また、ステップＳ１３にて、蓄積受信すると判定した場合、コンテンツ受信装置２１は、受信している番組送出情報に含まれるＥＩＴ（Ｅｖｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ　ｐｒｅｓｅｎｔ（現在）／ｆｕｔｕｒｅ（未来））に従って、番組（コンテンツ）の開始時間（開始時刻）と継続時間（終了時刻）を取得する（ステップＳ１８）。そして、コンテンツ受信装置２１は、番組の開始時間に到達したら、再多重化手段４１を素通りさせて、当該番組を蓄積手段４５に、ストリームとして蓄積開始する（ステップＳ１９）。そして、コンテンツ受信装置２１は、受信しているストリーム（多重化スクランブルコンテンツ）から、第一分離手段２７のＫｃ伝送用ＥＣＭ第一分離部２７ｂによって、Ｋｃ伝送用ＥＣＭを分離して、セキュリティモジュール２５に転送する（ステップＳ２０）。
【０１３３】
そうすると、コンテンツ受信装置２１は、Ｋｃ伝送用ＥＣＭ復号手段３３によって、Ｋｃ伝送用ＥＣＭを復号し、ライセンス情報を得て、蓄積場所判定手段３７によって、ライセンス情報に含まれる蓄積場所情報（蓄積場所記述子）によって、蓄積場所が、蓄積媒体内（蓄積手段４５内）に蓄積するか、ＩＣカード内（セキュリティモジュール２５のＫｃ伝送用ＥＣＭ保持手段５１）または受信機本体（受信装置本体２３の不揮発性メモリ手段４３）に蓄積するかを判定をする（ステップＳ２１）。
【０１３４】
このステップＳ２１にて、蓄積手段４５内に蓄積すると判定した場合、コンテンツ受信装置２１は、Ｋｃ伝送用ＥＣＭ再暗号化手段３９によって、再暗号化Ｋｃ伝送用ＥＣＭを取得し、ＥＣＭ－Ｋｗをストリーム（多重化スクランブルコンテンツ）から削除する（ステップＳ２２）。また、コンテンツ受信装置２１は、再多重化手段４１によって、再暗号化Ｋｃ伝送用ＥＣＭを、蓄積手段４５に蓄積中のストリームに多重化して、コンテンツ（スクランブルコンテンツ）と併せて、蓄積手段４５に蓄積する（ステップＳ２３）。そして、コンテンツ受信装置２１は、番組の継続時間（終了時刻）に達したら、蓄積を終了する（ステップＳ２４）。
【０１３５】
また、ステップＳ２１にて、セキュリティモジュール２５のＫｃ伝送用ＥＣＭ保持手段５１または受信装置本体２３の不揮発性メモリ手段４３に蓄積すると判定した場合、受信装置本体２３の不揮発性メモリ手段４３の場合には、Ｋｃ伝送用ＥＣＭ再暗号化手段３９によって、再暗号化Ｋｃ伝送用ＥＣＭを取得し、コンテンツ受信装置本体（不揮発性メモリ手段４３）に保持する（ステップＳ２５）。また、コンテンツ受信装置２１は、蓄積手段４５に蓄積されているストリーム（多重化スクランブルコンテンツ）からＥＣＭ－Ｋｗを削除する（ステップＳ２６）。そして、コンテンツ受信装置２１は、番組の継続時間（終了時刻）に達したら、蓄積を終了する（ステップＳ２７）。
【０１３６】
〈コンテンツ受信装置の動作（第二実施形態、放送受信時［リアルタイム視聴時］）〉
次に、図９に示すフローチャートを参照して、コンテンツ受信装置２１Ａ（第二実施形態）の放送受信時（リアルタイム視聴時）の動作について説明する（適宜、図６参照）。
まず、コンテンツ受信装置２１Ａは、多重化スクランブルコンテンツの放送受信を開始すると（ステップＳ３１）、第一分離手段２７のＥＭＭ分離部２７ａによって、当該コンテンツ受信装置２１Ａのセキュリティモジュール２５宛のＥＭＭがあれば、セキュリティ

モジュール２５にＥＭＭを転送し、セキュリティモジュール２５内にて、ワーク鍵Ｋｗを設定する（ステップＳ３２）。つまり、ＥＭＭ復号手段２９によりワーク鍵Ｋｗを得て、この得られたワーク鍵Ｋｗをワーク鍵保持手段３１に保持させる。

【０１３７】

続いて、コンテンツ受信装置２１Ａは、当該装置２１Ａの使用者が操作手段（リモコン等、図示せず）を操作した結果である操作信号に従って、多重化スクランブルコンテンツをリアルタイム視聴するか蓄積受信するか判定する（ステップＳ３３）。リアルタイム視聴すると判定した場合、コンテンツ受信装置２１Ａは、第一分離手段２７は、受信している番組送出情報に含まれるＰＭＴに従って、ＥＣＭ－Ｋｗ分離部２７ｃにより、多重化スクランブルコンテンツからＥＣＭ－Ｋｗを選択し（ステップＳ３４）、分離後、分離したＥＣＭ－Ｋｗをセキュリティモジュール２５に転送し、スクランブル鍵第一復号手段３５によってスクランブル鍵Ｋｓを取得する（ステップＳ３５）。

【０１３８】

そして、コンテンツ受信装置２１Ａは、デスクランブル手段５７によって、スクランブル鍵Ｋｓにより、コンテンツ（スクランブルコンテンツ）のデスクランブルを行って、図示を省略したデコーダに入力し（ステップＳ３６）、デコードした後、表示手段（図示せず）に表示する。当該装置２１Ａの使用者は、この表示手段に表示されたコンテンツを視聴する（ステップＳ３７）。

【０１３９】

また、ステップＳ３３にて、蓄積受信すると判定した場合、コンテンツ受信装置２１Ａは、受信している番組送出情報に含まれるＥＩＴ（ｐｒｅｓｅｎｔ（現在）／ｆｕｔｕｒｅ（未来））に従って、番組（コンテンツ）の開始時間（開始時刻）と継続時間（終了時刻）を取得する（ステップＳ３８）。そして、コンテンツ受信装置２１Ａは、番組の開始時間に到達したら、第一分離手段２７によって、番組送出情報に含まれているＰＭＴ内のデジタルコピー制御記述子を参照し、デジタルコピー制御情報を取得する（ステップＳ３９）。

【０１４０】

そして、コンテンツ受信装置２１Ａは、高速デジタルＩ／Ｆ手段５９によって、デジタルコピー制御情報に応じて、ＤＴＣＰで、多重化スクランブルコンテンツを暗号化し、ストリームとして外部蓄積装置２２に転送を開始する（ステップＳ４０）。そうすると、外部蓄積装置２２では、高速デジタルＩ／Ｆ部２４によって、デジタルコピー制御情報に応じて、ＤＴＣＰで、暗号化された多重化スクランブルコンテンツを復号化し、ストリームとして蓄積部２６に蓄積を開始する（ステップＳ４１）。

【０１４１】

そして、コンテンツ受信装置２１Ａは、第一分離手段２７のＫｃ伝送用ＥＣＭ第一分離部２７ｂで分離されたＫｃ伝送用ＥＣＭを、セキュリティモジュール２５に転送し、このＫｃ伝送用ＥＣＭをＫｃ伝送用ＥＣＭ復号手段３３が受信して、復号する。そして、コンテンツ受信装置２１Ａは、復号したライセンス情報を、Ｋｃ伝送用ＥＣＭ再暗号化手段３９によって、固有鍵で再暗号化する。そうすると、この再暗号化した再暗号化Ｋｃ伝送用ＥＣＭを再多重化手段４１が取得する（ステップＳ４２）。

【０１４２】

そして、コンテンツ受信装置２１Ａは、高速デジタルＩ／Ｆ手段５９から転送しているストリーム（多重化スクランブルコンテンツ）からＥＣＭ－Ｋｗを削除する（ステップＳ４３）。そして、コンテンツ受信装置２１Ａは、再暗号化Ｋｃ伝送用ＥＣＭを、外部蓄積装置２２で蓄積中のストリームに多重化されるように、高速デジタルＩ／Ｆ手段５９によって、転送中のストリームに多重化し、多重化したストリームとして、外部蓄積装置２２に転送する（ステップＳ４４）。そして、コンテンツ受信装置２１Ａは、番組の継続時間（終了時刻）に達したら、外部蓄積装置２２にへの転送を終了する（ステップＳ４５）。そうすると、外部蓄積装置２２では、ストリームの蓄積を終了する（ステップＳ４６）。

【０１４３】

なお、ステップＳ４１およびステップＳ４６は、外部蓄積装置２２の動作であるので、コンテンツ受信装置２１Ａの動作と区別するために、ステップＳ３８からステップＳ４５までのライン上に示さずに横（図９では右側）にずらして記載している。

【０１４４】

〈コンテンツ受信装置の動作（第一実施形態、第二実施形態共通、蓄積再生時）〉

次に、図１０に示すフローチャートを参照して、コンテンツ受信装置２１（２１Ａ）（第一実施形態、第二実施形態）の蓄積再生時の動作について説明する（適宜、図５、図６参照）。ここでは、第一実施形態のコンテンツ受信装置２１における動作について説明する。

【０１４５】

まず、コンテンツ受信装置２１は、蓄積再生を開始すると（ステップＳ５１）、第二分離手段４７のＫｃ伝送用ＥＣＭ第二分離部４７ａによって、蓄積手段４５に蓄積されている再多重化スクランブルコンテンツから再暗号化Ｋｃ伝送用ＥＣＭを分離して、セキュリティモジュール２５に転送する（ステップＳ５２）。そうすると、セキュリティモジュール２５は、再暗号化Ｋｃ伝送用ＥＣＭ復号手段４９により、再暗号化Ｋｃ伝送用ＥＣＭを復号し、ライセンス情報に含まれている再生課金情報から、再生課金記述子を取得する（ステップＳ５３）。

【０１４６】

そして、コンテンツ受信装置２１は、取得した再生課金記述子に基づいて、再暗号化Ｋｃ伝送用ＥＣＭは有料か無料か、つまり、スクランブルコンテンツをデスクランブルすることは有料か無料かを判定し（ステップＳ５４）、有料であると判定した場合には再生課金情報をユーザ（当該装置２１の使用者）に提示する（ステップＳ５５）。そして、当該装置２１の使用者が操作手段（リモコン等、図示せず）を操作した結果である操作信号に基づいて、コンテンツを視聴するか（課金を承諾）、視聴しないか（課金を拒否）を判定し（ステップＳ５６）、視聴しないと判定した場合には動作を終了する（ステップＳ５７）。

【０１４７】

コンテンツを視聴すると判定した場合、コンテンツ受信装置２１は、セキュリティモジュール２５内で課金処理を行い、コンテンツ鍵Ｋｃを設定する、つまり、ライセンス情報に含まれていたコンテンツ鍵Ｋｃをスクランブル鍵第二復号手段５５に出力する（ステップＳ５８）。そして、コンテンツ受信装置２１は、第二分離手段４７のＥＣＭ－Ｋｃ分離部４７ｂによって、ＥＣＭ－Ｋｃを分離し、セキュリティモジュール２５のスクランブル鍵第二復号手段５５に転送して、コンテンツ鍵Ｋｃを用いて復号して、スクランブル鍵Ｋｓを取得する（ステップＳ５９）。

【０１４８】

そして、コンテンツ受信装置２１は、デスクランブル手段５７によって、スクランブル鍵Ｋｓを用いて、コンテンツ（スクランブルコンテンツ）をデスクランブルし、デコーダ（図示せず）に入力して、表示手段（図示せず）に表示する（ステップＳ６０）。そうすると、当該装置２１の使用者は、表示されたコンテンツを視聴する（ステップＳ６１）。

【０１４９】

また、ステップＳ５４にて、無料であると判定した場合、コンテンツ受信装置２１は、コンテンツ鍵Ｋｃを設定する、つまり、ライセンス情報に含まれていたコンテンツ鍵Ｋｃをスクランブル鍵第二復号手段５５に出力する（ステップＳ６２）。そして、コンテンツ受信装置２１は、第二分離手段４７のＥＣＭ－Ｋｃ分離部４７ｂによって、ＥＣＭ－Ｋｃを分離し、セキュリティモジュール２５のスクランブル鍵第二復号手段５５に転送して、コンテンツ鍵Ｋｃを用いて復号して、スクランブル鍵Ｋｓを取得する（ステップＳ６３）。

【０１５０】

そして、コンテンツ受信装置２１は、デスクランブル手段５７によって、スクランブル鍵Ｋｓを用いて、コンテンツ（スクランブルコンテンツ）をデスクランブルし、デコーダ

（図示せず）に入力して、表示手段（図示せず）に表示する（ステップＳ６４）。そうすると、当該装置２１の使用者は、表示されたコンテンツを視聴する（ステップＳ６５）。

【０１５１】

以上、本発明の実施形態について説明したが、本発明は前記実施形態には限定されない。例えば、本実施形態では、コンテンツ送信装置１、コンテンツ受信装置２１（２１Ａ）として説明したが、これらの装置の各構成の処理を汎用的または特殊なコンピュータ言語によって記述したコンテンツ送信プログラム、コンテンツ受信プログラムとみなすことも可能であるし、各構成の処理を、コンテンツを処理する一つずつの過程ととらえたコンテンツ送信方法、コンテンツ受信方法とみなすことも可能である。これらの場合、コンテンツ送信装置１、コンテンツ受信装置２１（２１Ａ）と同様の効果を得ることができる。

【図面の簡単な説明】

【０１５２】

【図１】本発明の実施形態に係るコンテンツ送信装置のブロック図である。

【図２】Ｋｃ伝送用ＥＣＭのフォーマットを説明した図である。

【図３】コンテンツの送出フォーマットを説明した図である。

【図４】図１に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図５】本発明の実施形態に係るコンテンツ受信装置（第一実施形態）のブロック図である。

【図６】本発明の実施形態に係るコンテンツ受信装置（第二実施形態）のブロック図である。

【図７】コンテンツの蓄積フォーマットを説明した図である。

【図８】図５に示したコンテンツ受信装置（第一実施形態）の放送受信時の動作を説明したフローチャートである。

【図９】図６に示したコンテンツ受信装置（第二実施形態）の放送受信時の動作を説明したフローチャートである。

【図１０】図５に示したコンテンツ受信装置（第一実施形態）の蓄積再生時の動作を説明したフローチャートである。

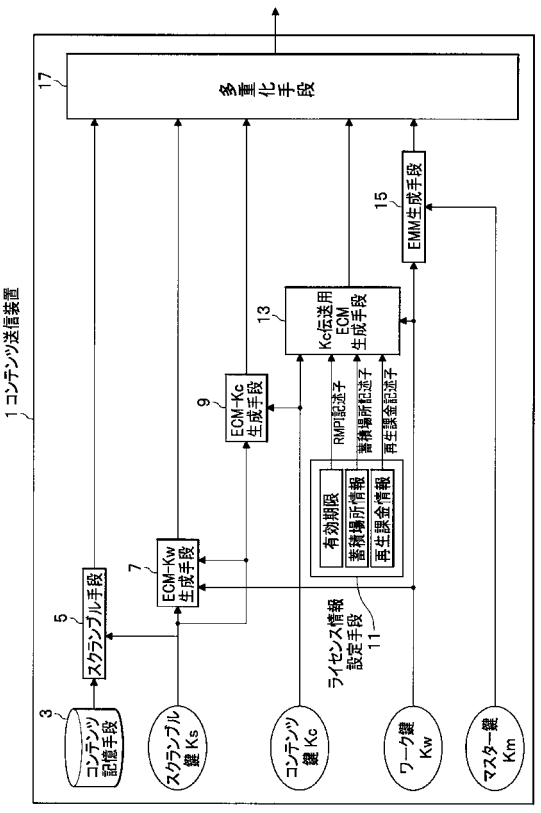
【符号の説明】

【０１５３】

１	コンテンツ送信装置
３	コンテンツ記憶手段
５	スクランブル手段
７	ＥＣＭ－Ｋｗ生成手段
９	ＥＣＭ－Ｋｃ生成手段
１１	ライセンス情報設定手段
１３	Ｋｃ伝送用ＥＣＭ生成手段
１５	ＥＭＭ生成手段
１７	多重化手段
２１（２１Ａ）	コンテンツ受信装置
２３（２３Ａ）	受信装置本体
２５	セキュリティモジュール
２７	第一分離手段
２９	ＥＭＭ復号手段
３１	ワーク鍵保持手段
３３	Ｋｃ伝送用ＥＣＭ復号手段
３５	スクランブル鍵第一復号手段
３７	蓄積場所判定手段
３９	Ｋｃ伝送用ＥＣＭ再暗号化手段
４１	再多重化手段
４３	不揮発性メモリ手段

４５　　蓄積手段
４７　　第二分離手段
４９　　再暗号化Ｋｃ伝送用ＥＣＭ復号手段
５１　　Ｋｃ伝送用ＥＣＭ保持手段
５３　　有効期限判定手段
５５　　スクランブル鍵第二復号手段
５７　　デスクランブル手段
５９　　高速デジタルＩ／Ｆ手段

【図１】



【図２】

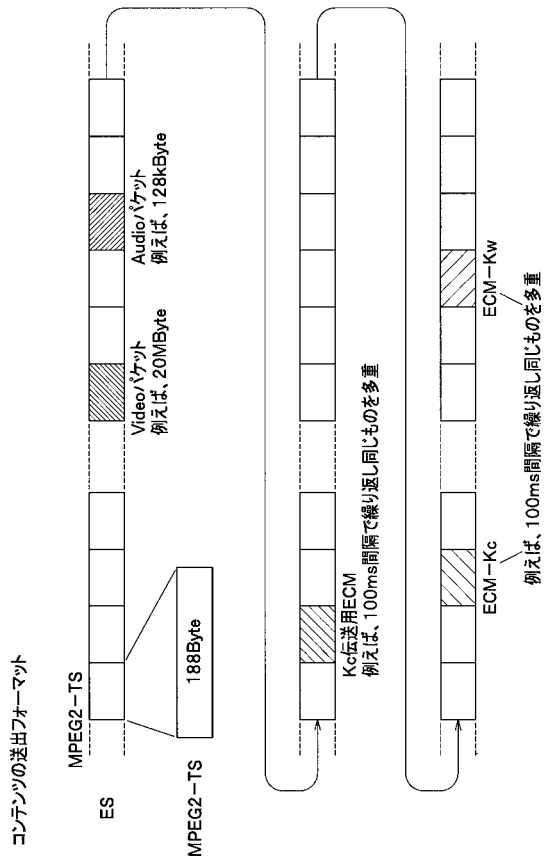
(a)

Kc伝送用ECM				
暗号	固定	項目	バイト長	備考
		ECMセクションヘッダ	8	
非暗号化部	固定部	プロトコル番号	1	アクセス制御方式の種別
		事業体識別	3	
		ワーク鍵識別	1	
暗号化部	可変部		n	各種の運用情報を配置可能。 可変部は、記述子を自由に挿入することができる。
	改竄検出		4	
		セクションCRC	4	

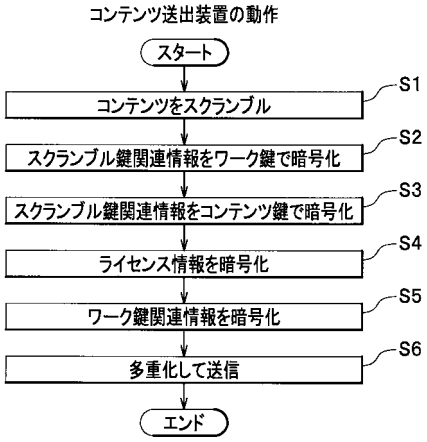
(b)

可変部(順序不定、個数不定とする)			
記述子	項目名	バイト長	備考
コンテンツ鍵記述子	記述子タグ	1	
	記述子長	1	
	コンテンツ鍵識別	6	
	コンテンツ鍵	8(32)	
蓄積場所記述子	記述子タグ	1	
	記述子長	1	
	暗号化Kc蓄積場所指定	n	0x00:ICカード内蓄積、0x01:受信機本体内蓄積 0x1X:蓄積媒体内蓄積
再生課金記述子	記述子タグ	1	
	記述子長	1	
	再生課金情報	n	コンテンツを視聴するために必要な料金など
RMPI記述子	記述子タグ	1	
	記述子長	1	
	有効期限	6	コンテンツ鍵の有効期限

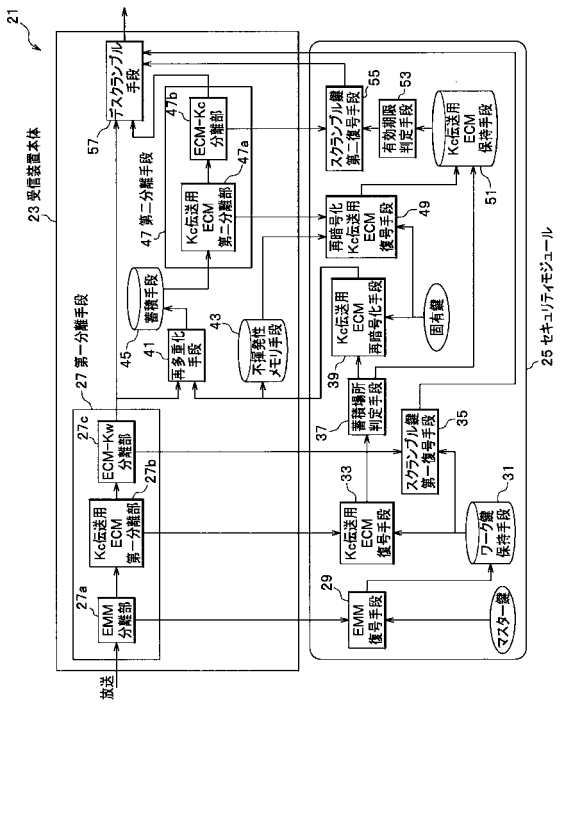
【図３】


コンテンツの送出フォーマット
MPEG2−TS
ES
MPEG2−TS
188Byte
Videoパケット
例えば、20MByte
Audioパケット
例えば、128kByte
Kc伝送用ECM
例えば、100ms間隔で繰り返し同じものを多重
ECM−Kc
ECM−Kw
例えば、100ms間隔で繰り返し同じものを多重

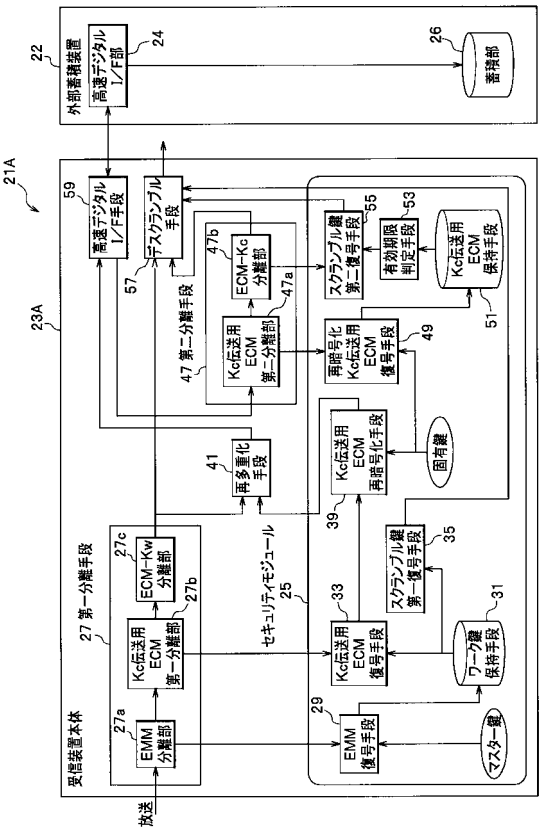
【図４】


コンテンツ送出装置の動作
スタート
コンテンツをスクランブル
S1
スクランブル鍵関連情報をワーク鍵で暗号化
S2
スクランブル鍵関連情報をコンテンツ鍵で暗号化
S3
ライセンス情報を暗号化
S4
ワーク鍵関連情報を暗号化
S5
多重化して送信
S6
エンド

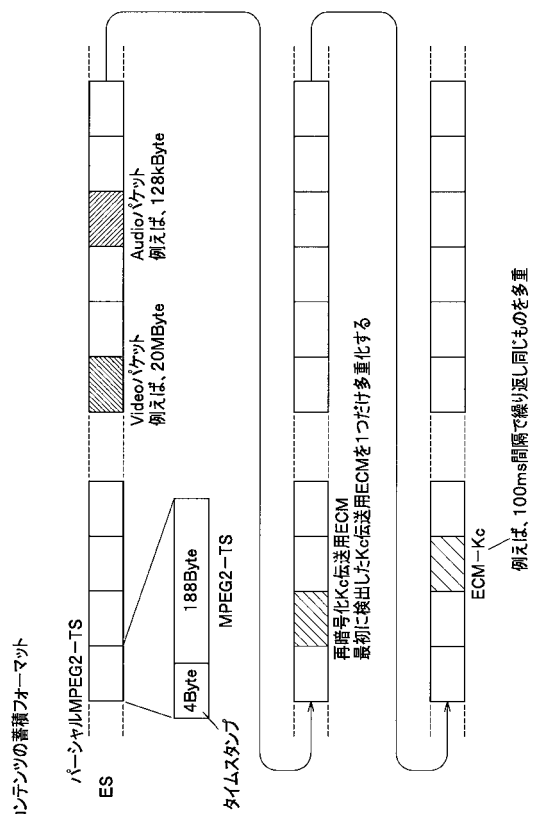
【図５】


21
23 受信装置本体
25 セキュリティモジュール
放送
EMM 分離部
27a
Kc伝送用 ECM 第一分離部
27b
ECM−Kw 分離部
27c
27 第一分離手段
EMM 復号手段
29
Kc伝送用 ECM 復号手段
33
ワーク鍵 保持手段
31
マスター鍵
スクランブル鍵 第一復号手段
35
蓄積制御 判定手段
37
Kc伝送用 ECM 再暗号化手段
39
固有鍵
再暗号化 Kc伝送用 ECM 復号手段
49
スクランブル鍵 第二復号手段
55
有効期限 判定手段
53
Kc伝送用 ECM 保持手段
51
デスクランブル 手段
57
47 第二分離手段
Kc伝送用 ECM 第二分離部
47a
ECM−Kc 分離部
47b
再多重化 手段
41
蓄積手段
45
不揮発性 メモリ手段
43

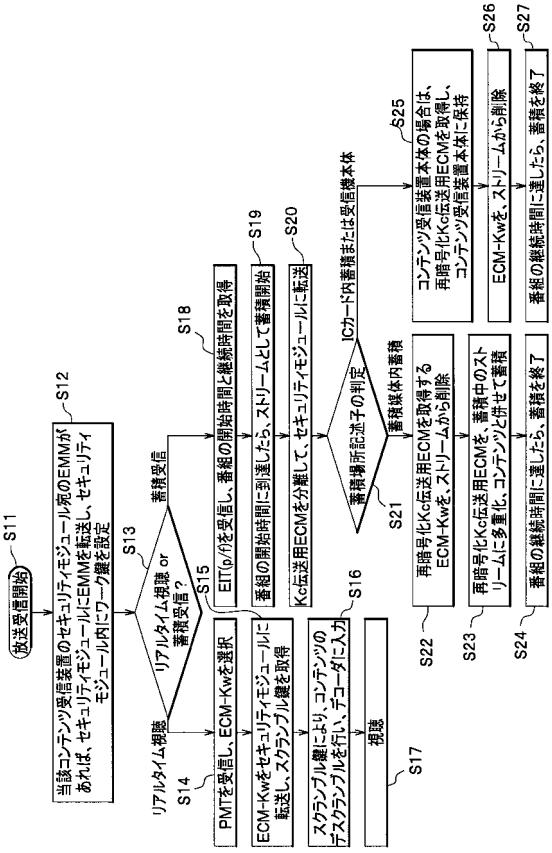
【図６】


22
外部蓄積装置
高速デジタル I/F部
24
26
蓄積部
21A
23A
受信装置本体
高速デジタル I/F手段
59
デスクランブル 手段
57
47 第二分離手段
Kc伝送用 ECM 第二分離部
47a
ECM−Kc 分離部
47b
再多重化 手段
41
スクランブル鍵 第二復号手段
55
有効期限 判定手段
53
Kc伝送用 ECM 保持手段
51
再暗号化 Kc伝送用 ECM 復号手段
49
Kc伝送用 ECM 再暗号化手段
39
固有鍵
スクランブル鍵 第一復号手段
35
ワーク鍵 保持手段
31
マスター鍵
EMM 復号手段
29
Kc伝送用 ECM 復号手段
33
セキュリティモジュール
25
27 第一分離手段
Kc伝送用 ECM 第一分離部
27b
ECM−Kw 分離部
27c
EMM 分離部
27a
放送

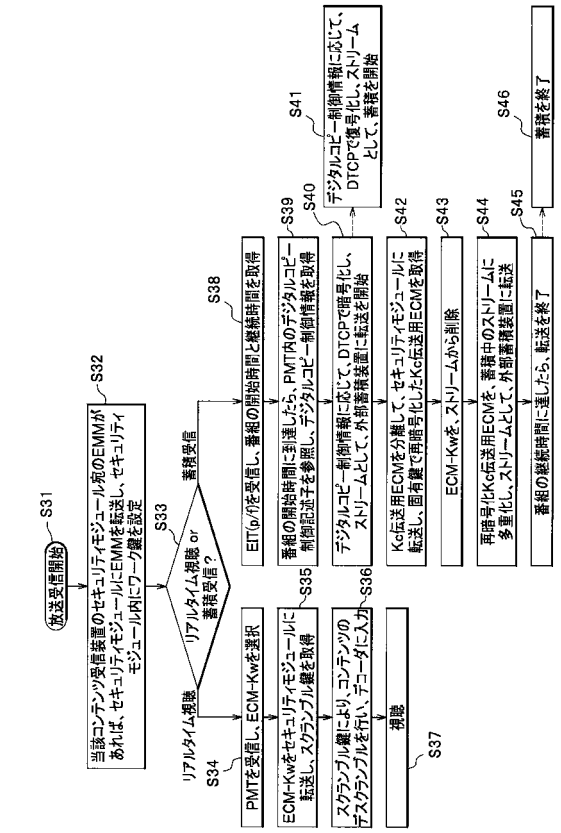
【図７】


コンテンツの蓄積フォーマット
パーシャルMPEG2－TS
ES
Videoパケット
例えば、20MByte
Audioパケット
例えば、128kByte
4Byte
188Byte
タイムスタンプ
MPEG2－TS
再暗号化Kc伝送用ECM
最初に検出したKc伝送用ECMを1つだけ多重化する
ECM－Kc
例えば、100ms間隔で繰り返し同じものを多重

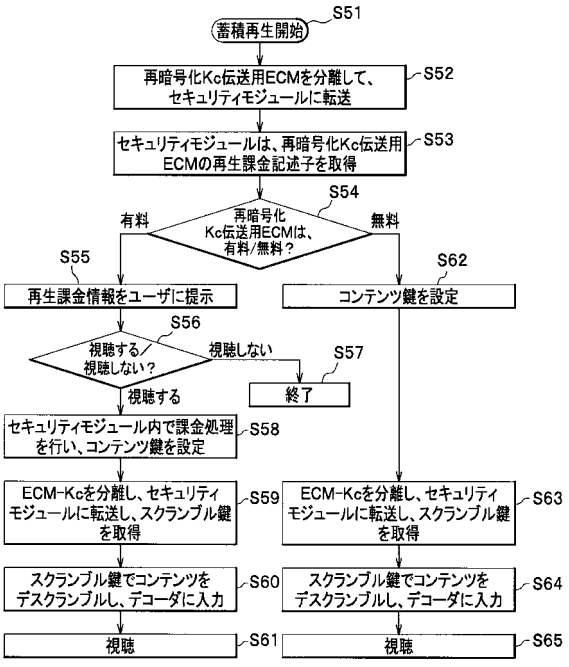
【図８】


放送受信開始
S11
当該コンテンツ受信装置のセキュリティモジュール宛のEMMが
あれば、セキュリティモジュールにEMMを転送、セキュリティ
モジュール内にワーク鍵を設定
S12
リアルタイム視聴 or
蓄積受信？
S13
蓄積受信
リアルタイム視聴
S14
PMTを受信し、ECM-Kwを選択
S15
EITp/fを受信し、番組の開始時間に継続時間を取得
S18
番組の開始時間に到達したら、ストリームとして蓄積開始
S19
Kc伝送用ECMを分離して、セキュリティモジュールに転送
S20
ECM-Kwをセキュリティモジュールに
転送し、スクランブル鍵を取得
S16
スクランブル鍵により、コンテンツの
デスクランブルを行い、デコーダに入力
視聴
S17
蓄積場所記述子の判定
ICカード内蓄積または受信機本体
蓄積媒体内蓄積
S21
S25
再暗号化Kc伝送用ECMを取得する
ECM-Kwを、ストリームから削除
S22
再暗号化Kc伝送用ECMを、蓄積中のスト
リームに多重化、コンテンツと併せて蓄積
S23
番組の継続時間に達したら、蓄積を終了
S24
コンテンツ受信装置本体の場合は、
再暗号化Kc伝送用ECMを取得し、
コンテンツ受信装置本体に保持
S26
ECM-Kwを、ストリームから削除
S27
番組の継続時間に達したら、蓄積を終了

【図９】


放送受信開始
S31
当該コンテンツ受信装置のセキュリティモジュール宛のEMMが
あれば、セキュリティモジュールにEMMを転送、セキュリティ
モジュール内にワーク鍵を設定
S32
リアルタイム視聴 or
蓄積受信？
S33
蓄積受信
リアルタイム視聴
S34
PMTを受信し、ECM-Kwを選択
S35
ECM-Kwをセキュリティモジュールに
転送し、スクランブル鍵を取得
S36
スクランブル鍵により、コンテンツの
デスクランブルを行い、デコーダに入力
視聴
S37
EITp/fを受信し、番組の開始時間と継続時間を取得
S38
番組の開始時間に到達したら、PMT内のデジタルコピー
制御記述子を参照し、デジタルコピー制御情報を取得
S39
デジタルコピー制御情報に応じて、DTCPで暗号化し、
ストリームとして、外部蓄積装置に転送を開始
S40
デジタルコピー制御情報に応じて、
DTCPで復号化し、ストリーム
として、蓄積を開始
S41
Kc伝送用ECMを分離して、セキュリティモジュールに
転送し、固有鍵で再暗号化したKc伝送用ECMを取得
S42
ECM-Kwを、ストリームから削除
S43
再暗号化Kc伝送用ECMを、蓄積中のストリームに
多重化し、ストリームとして、外部蓄積装置に転送
S44
番組の継続時間に達したら、転送を終了
S45
蓄積を終了
S46

【図１０】


蓄積再生開始
S51
再暗号化Kc伝送用ECMを分離して、
セキュリティモジュールに転送
S52
セキュリティモジュールは、再暗号化Kc伝送用
ECMの再生課金記述子を取得
S53
再暗号化
Kc伝送用ECMは、
有料/無料？
S54
有料
無料
再生課金情報をユーザに提示
S55
コンテンツ鍵を設定
S62
視聴する
視聴しない？
S56
視聴しない
終了
S57
視聴する
セキュリティモジュール内で課金処理
を行い、コンテンツ鍵を設定
S58
ECM-Kcを分離し、セキュリティ
モジュールに転送し、スクランブル鍵
を取得
S59
ECM-Kcを分離し、セキュリティ
モジュールに転送し、スクランブル鍵
を取得
S63
スクランブル鍵でコンテンツを
デスクランブルし、デコーダに入力
S60
スクランブル鍵でコンテンツを
デスクランブルし、デコーダに入力
S64
視聴
S61
視聴
S65

フロントページの続き

(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

審査官　日下　善之

(56)参考文献　特開２００３－１１５８３２（ＪＰ，Ａ）
特開２００３－１５２６９８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　７／１０－７／１７３
Ｈ０４Ｎ　７／２４－７／６８
Ｈ０４Ｌ　９／００－９／３８