(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2012-235463
(P2012-235463A)
(43)公開日　平成24年11月29日(2012.11.29)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	300A	5K030
H04L 12/22	(2006.01)	H04L	12/22		5K034
H04L 29/06	(2006.01)	H04L	13/00	305B	

審査請求 未請求　請求項の数 15　ＯＬ　（全 30 頁）

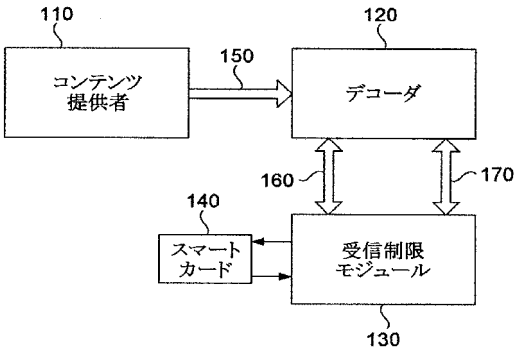
(21)出願番号　特願2012-101840 (P2012-101840)
(22)出願日　平成24年4月26日 (2012.4.26)
(31)優先権主張番号　1107156.0
(32)優先日　平成23年4月28日 (2011.4.28)
(33)優先権主張国　英国 (GB)
(31)優先権主張番号　10-2012-0018916
(32)優先日　平成24年2月24日 (2012.2.24)
(33)優先権主張国　韓国 (KR)

(71)出願人　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市霊通区三星路１２９　１２９，Ｓａｍｓｕｎｇ－ｒｏ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】共通インタフェースを介して受信制限モジュールに暗号化されたデータを送信するためのデータ送信装置及びそれに適用される方法、受信制限モジュール、そのシステム。

(57)【要約】
【課題】　本発明は、暗号化されたデータの格納されたペイロード及びヘッダを備える複数のデータパケットを生成し、該生成されたデータパケットを共通インタフェースの送信ストリーム（ＴＳ：Ｔｒａｎｓｐｏｒｔ　ｓｔｒｅａｍ）インタフェースを介して受信制限モジュールに送信するデータ送信装置及び方法を提供する。
【解決手段】　共通インタフェースを介して受信制限モジュールに暗号化されたデータを送信するためのデータ送信装置及びそれに適用される方法、受信制限モジュール、システムが提供される。本暗号化されたデータ送信装置は、暗号化されたデータを格納するために、ペイロード（ｐａｙｌｏａｄ）及びヘッダを備える複数のデータパケットを生成するデータパケット生成部と、複数のデータパケットを受信制限モジュールに送信するＴＳインタフェースモジュールとを備える。
【選択図】　図１Ａ



【特許請求の範囲】
【請求項１】
共通インタフェースを介して受信制限モジュールに暗号化されたデータを送信するためのデータ送信装置であって、
暗号化されたデータを格納するために、ペイロード（ｐａｙｌｏａｄ）及びヘッダを備える複数のデータパケットを生成するデータパケット生成部と、
前記複数のデータパケットを前記共通インタフェースのうち、ＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）インタフェースを介して受信制限モジュールに送信するＴＳインタフェースモジュールと
を備えるデータ送信装置。
【請求項２】
前記暗号化されたデータは、複数のＩＰ（ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）パケットとしてコンテンツ提供者から受信され、
前記データパケット生成部は、
カプセル化された（ｅｎｃａｐｓｕｌａｔｅｄ）ＩＰパケットを生成するために、前記複数のＩＰパケットのうちの何れか一つにヘッダを付加して各データパケットを形成することを特徴とする請求項１に記載のデータ送信装置。
【請求項３】
前記ＴＳインタフェースモジュールは、
ヨーロッパ電気通信標準（Ｅｕｒｏｐｅａｎ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｔａｎｄａｒｄｓ　Ｉｎｓｔｉｔｕｔｅ：ＥＴＳＩ）のＥＮ　３０１　１９２規格に従うＭＰＥ（Ｍｕｌｔｉｐｒｏｔｏｃｏｌ　ｅｎｃａｐｓｕｌａｔｉｏｎ）を利用して、前記カプセル化されたＩＰパケットを送信することを特徴とする請求項２に記載のデータ送信装置。
【請求項４】
前記データパケット生成部は、
データサンプル及び前記データサンプルと関連した暗号化情報を抽出するために、前記暗号化されたデータを含むファイルをパッシングし、少なくとも一つのデータサンプル及び前記少なくとも一つのデータサンプルの含まれたデータサンプルファイルを生成することを特徴とする請求項１に記載のデータ送信装置。
【請求項５】
前記データパケット生成部は、
前記データパケットのペイロードに前記データサンプルファイルのうちの何れか一つを含めることを特徴とする請求項４に記載のデータ送信装置。
【請求項６】
前記データパケット生成部は、
前記データサンプルファイルを複数のデータサンプルファイル領域に区分し、
前記複数のデータパケットは、前記データサンプルファイルの領域のうちの何れか一つを各々含むＭＰＥＧ－２　ＴＳパケットであることを特徴とする請求項４に記載のデータ送信装置。
【請求項７】
前記各々のＭＰＥＧ－２　ＴＳパケットのヘッダは、前記ＭＰＥＧ－２　ＴＳパケットに含まれたデータサンプルファイル領域がデータサンプルファイルの開始に対応するかどうかに対する情報を含むことを特徴とする請求項６に記載のデータ送信装置。
【請求項８】
前記受信された暗号化されたデータは、
格納装置にダウンロードされるか、又はサーバからプログレシブ（ｐｒｏｇｒｅｓｓｉｖｅ）ダウンロードされて受信されたり、アダプティブストリーミング（ａｄａｐｔｉｖｅ　ｓｔｒｅａｍｉｎｇ）を利用して複数のファイルとして受信されるか、又はコンテンツストリーミングを利用して連続的なストリームとして受信されることを特徴とする請求

項１に記載のデータ送信装置。
【請求項９】
前記暗号化されたデータは、前記暗号化されたデータ送信装置の内部に存在する格納媒体に格納されることを特徴とする請求項１に記載のデータ送信装置。
【請求項１０】
前記暗号化されたデータは、ＩＳＯＢＭＦＦ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｏｒｇａｎｉｚａｔｉｏｎ ｆｏｒ Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ ｂａｓｅ ｍｅｄｉａ ｆｉｌｅ ｆｏｒｍａｔ）ファイルであることを特徴とする請求項１に記載のデータ送信装置。
【請求項１１】
前記暗号化されたデータ送信装置は、前記ＴＳインタフェースモジュールを介して前記受信制限モジュールから復号化されたデータを受信し、前記復号化されたデータをデコードすることを特徴とする請求項１に記載のデータ送信装置。
【請求項１２】
前記暗号化されたデータ送信装置は、前記暗号化されたデータが前記ＴＳインタフェースモジュールを介して送信されることを前記受信制限モジュールに通知するために、共通インタフェースの制御インタフェースを介して前記受信制限モジュールに初期化メッセージを送信することを特徴とする請求項１に記載のデータ送信装置。
【請求項１３】
前記データパケット生成部は、
複数のフォーマットのうち、選択されたフォーマットに応じて前記複数のデータパケットを生成し、
前記暗号化されたデータ送信装置は、前記受信制限モジュールに送信される前記初期化メッセージに前記選択されたフォーマットに対する情報を含めることを特徴とする請求項１２に記載のデータ送信装置。
【請求項１４】
前記受信制限モジュールに送信される前記初期化メッセージは、パケットＩＤ（ｐａｃｋｅｔ ｉｄｅｎｔｉｆｉｅｒ）情報を含むことを特徴とする請求項１２に記載のデータ送信装置。
【請求項１５】
前記暗号化されたデータがすべて送信されると、前記制御インタフェースを介して前記受信制限モジュールに終了メッセージを送信することを特徴とする請求項１２に記載のデータ送信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化されたデータ送信装置及びそれに適用される方法に関し、暗号化されたコンテンツを共通インタフェースを介して受信制限モジュールに送信する暗号化されたデータ送信装置及びそれに適用される方法に関する。
【背景技術】
【０００２】
近来では、多様な種類のマルチメディアコンテンツが生産されて消費者に提供されている。しかしながら、映像技術及び複製技術の発達によって、マルチメディアコンテンツに対した無分別な複製がなされて、コンテンツ提供者に莫大な被害をもたらしている。
【０００３】
このような問題点を解決するために、コンテンツ提供者あるいは放送事業者は、一般に放送コンテンツを保護するための受信制限システム（ＣＡＳ：Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）又は広帯域コンテンツ（ｂｒｏａｄｂａｎｄ ｃｏｎｔｅｎｔ）を保護するためのＤＲＭ（Ｄｉｇｉｔａｌ Ｒｉｇｈｔ Ｍａｎａｇｅｍｅｎｔ）システムを利用して、消費者機器から提供されるマルチメディアコンテンツを保護してい

る。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、暗号化されたデータの格納されたペイロード及びヘッダを備える複数のデータパケットを生成し、該生成されたデータパケットを共通インタフェースの送信ストリーム（ＴＳ：Ｔｒａｎｓｐｏｒｔ　ｓｔｒｅａｍ）インタフェースを介して受信制限モジュールに送信するデータ送信装置及び方法を提供することにある。
【課題を解決するための手段】
【０００５】
上記課題を解決するために、本発明のある観点によれば、共通インタフェースを介して受信制限モジュールに暗号化されたデータを送信するためのデータ送信装置が提供される。本発明の装置は、暗号化されたデータが格納されたペイロード（ｐａｙｌｏａｄ）及びヘッダを備える複数のデータパケットを生成するデータパケット生成部と、共通インタフェースのＴＳインタフェースを介して受信制限モジュールに複数のデータパケットを送信するためのＴＳインタフェースモジュールとを備える。
【０００６】
また、上記課題を解決するために、本発明の別の観点によれば、装置は、暗号化されたマルチメディアデータを受信してデコードするデコーダであり、データパケット生成部及びＴＳインタフェースモジュールは、デコーダのデモジュレータに統合されうる。
【０００７】
暗号化されたデータは、インターネットプロトコルＩＰパケットの複数のようなコンテンツ供給者から受信することができ、データパケット生成器は、カプセル化された（ｅｎｃａｐｓｕｌａｔｅｄ）ＩＰパケットを生成するために複数のＩＰパケットのうちの何れか一つにヘッダを付加して、各データパケットを形成できる。
【０００８】
ＴＳインタフェースモジュールは、ヨーロッパ電気通信標準（ＥＴＳＩ）のＥＮ　３０１　１９２規格に従うＭＰＥ（Ｍｕｌｔｉｐｒｏｔｏｃｏｌ　ｅｎｃａｐｓｕｌａｔｉｏｎ）を利用して、ＴＳインタフェースを介してカプセル化されたＩＰパケットを送信することができる。
【０００９】
データパケット生成部は、データサンプル及び前記データサンプルと関連した暗号化情報から抽出された暗号化されたデータを含むファイルをパッシングするように構成されることができ、データパケット生成部は、少なくとも一つのデータサンプルと関連した暗号化情報及び少なくとも一つのデータサンプルを含む複数のデータサンプルファイルを生成することができる。
【００１０】
各々のデータパケットに対して、データパケット生成部は、データパケットのペイロードにデータサンプルファイルのうちの何れか一つを含めることができる。
【００１１】
データパケット生成部は、複数のデータサンプルファイル領域をデータサンプルファイルに分割できるように構成されることができ、複数のデータパケットは、ＭＰＥＧ－２　ＴＳパケットでありえ、各々のＭＰＥＧ－２　ＴＳパケットは、データサンプルファイル領域のうちの何れか一つを含むことができる。
【００１２】
各々のＴＳパケットのヘッダは、ＴＳパケットに含まれたデータサンプルファイル領域がデータサンプルファイルに対応するかどうかに対する情報を含むことができる。
【００１３】
装置は、格納媒体から暗号化されたデータをダウンロードするか、サーバからプログレ

ッシブ（ｐｒｏｇｒｅｓｓｉｖｅ）ダウンロードとして暗号化されたデータを受信するか、コンテンツストリーミングを利用して連続的なストリームとして暗号化されたデータを受信することによって、暗号化されたコンテンツを受信することができる。

【００１４】

暗号化されたデータは、装置のローカル格納媒体に格納されることができる。暗号化されたデータは、標準化国際機構（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｏｒｇａｎｉｚａｔｉｏｎ ｆｏｒ Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ）を基盤とするメディアファイルフォーマットＩＳＯＢＭＦＦファイルでありうる。

【００１５】

装置は、ＴＳインタフェースを介して受信制限モジュールから復号化されたデータを受信することができ、復号化されたデータをデコードできる。

【００１６】

装置は、暗号化されたデータがＴＳインタフェースを介して送信されることを受信制限モジュールに通知するために、共通インタフェースの制御インタフェースを介して受信制限モジュールに初期化メッセージを送信できる。

【００１７】

データパケット生成部は、複数のフォーマットのうち、選択された一つに従って複数のデータパケットを生成でき、装置は、受信制限モジュールに送信される初期化メッセージに選択されたフォーマットに対する情報を含めることができる。

【００１８】

装置は、受信制限モジュールに送信される初期化メッセージにパケットＩＤ（Ｐａｃｋｅｔ ｉｄｅｎｔｉｆｉｅｒ：ＰＩＤ）情報を含めることができる。

【００１９】

装置は、暗号化されたすべてのデータが送信された後、制御インタフェースを介して受信制限モジュールに終了メッセージを送信できる。

【００２０】

装置は、制御インタフェースを介して受信制限モジュールからデータ要請メッセージを受信し、データ要請メッセージに指定された要請されたデータを検索し、受信制限モジュールに要請されたデータを送信できる。

【００２１】

装置は、制御インタフェースを介して受信制限モジュールから記録された（ｗｒｉｔｔｅｎ）データ及びデータ位置情報が含まれたデータ記録要請メッセージを受信することができ、データ位置情報に応じてファイルにデータ記録要請メッセージに含まれたデータを記録できる。

【００２２】

装置は、制御インタフェースを介して受信制限モジュールにトラック定義メッセージを受信することができ、トラック定義メッセージは、トラック及びトラックと関連したＤＲＭ情報に対する情報を含むことができる。

【００２３】

また、上記課題を解決するために、本発明の別の観点によれば、共通インタフェースを介して暗号化されたデータを受信する受信制限モジュールが提供されることができる。受信制限モジュールは、共通インタフェースの制御インタフェースを介して共通インタフェースのＴＳインタフェースを介して受信されうる暗号化されたデータのフォーマットに対するフォーマット情報が含まれた初期化メッセージを受信する制御モジュール、ＴＳインタフェースを介して暗号化されたデータを受信し、初期化メッセージのフォーマット情報に基づいて暗号化されたデータを復号化する受信制限復号化モジュール、及び暗号化されたデータが受信された所からソースにＴＳインタフェースを介して復号化されたデータを送信するデータ送信モジュールを備える。

【００２４】

復号化モジュールが暗号化されたデータを復号化するための追加的なデータが必要な場

合、制御モジュールは、追加的なデータを要請するために制御インタフェースを介してデータ要請メッセージを送信できる。

【００２５】

受信制限モジュールは、ファイルに記録されるデータを要請するために制御インタフェースを介してデータ記録要請メッセージを送信でき、データ記録要請メッセージは、ファイルに記録されるデータ及び記録されるデータがファイルに記録される位置と関連したデータ位置情報を含むことができる。

【００２６】

受信制限モジュールは、制御インタフェースを介してトラック定義メッセージを受信することができ、トラック定義メッセージは、トラックに対する情報及びトラックと関連したＤＲＭ情報を含むことができる。そして、受信制限モジュールは、トラック定義メッセージに含まれたＤＲＭ情報に基づいてトラックにＤＲＭシステムを備えることができる。

【００２７】

受信制限モジュールは、ＣＩ　ｐｌｕｓ　ｓｐｅｃｉｆｉｃａｔｉｏｎによって構成されることができて、データ送信モジュールは、ローカル暗号化（ｌｏｃａｌ　ｅｎｃｒｙｐｔｉｏｎ）を利用して復号化されたデータを送信するコンテンツ制御復号化モジュールを備えることができる。

【００２８】

本発明の一実施の形態によれば、暗号化されたデータを復号化するためのシステムが提供され、システムは、装置と共通インタフェースにより装置と接続した受信制限モジュールとを備えることができる。

【００２９】

本発明の一実施の形態によれば、共通インタフェースを介して受信制限モジュールに暗号化されたデータを送信する方法を提供する。本方法は、ヘッダ及び暗号化されたデータの格納されたペイロードが含まれた複数のデータパケットを生成するステップ、及び共通インタフェースのＴＳインタフェースを介して受信制限モジュールに複数のデータパケットを送信するステップを含む。

【００３０】

方法は、複数のＩＰパケットとしてコンテンツ提供者から暗号化されたデータを受信するステップをさらに含み、前記各々のデータパケットは、カプセル化されたＩＰパケットを生成するために複数のＩＰパケットのうちの何れか一つにヘッダを付加して形成されることができる。

【００３１】

複数のデータパケットを送信するステップは、ヨーロッパ電気通信標準（ＥＴＳＩ）のＥＮ　３０１１９２に従ってＭＰＥ（Ｍｕｌｔｉｐｒｏｔｏｃｏｌ　ｅｎｃａｐｓｕｌａｔｉｏｎ）を使用して、ＴＳインタフェースを介してカプセル化されたＩＰパケットを送信できる。

【００３２】

方法は、データサンプル及びデータサンプルと関連した暗号化情報から抽出された暗号化されたデータを含むファイルをパッシングするステップ、少なくとも一つのデータサンプルと関連した暗号化情報及び少なくとも一つのデータサンプルを含む複数のデータサンプルを生成するステップを含むことができる。

【００３３】

各々のデータパケットを生成するステップは、データパケットのペイロードにデータサンプルファイルのうちの何れか一つを含むステップを含むことができる。

【００３４】

方法は、データサンプルファイルを複数のデータサンプルファイル領域に分割するステップをさらに含み、前記複数のデータパケットは、ＭＰＥＧ－２　ＴＳパケットであり、各々のＭＰＥＧ－２　ＴＳパケットは、データサンプルファイル領域のうちの何れか一つを含むことができる。

【００３５】
暗号化されたデータは、標準化国際機構（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｏｒｇａｎｉｚａｔｉｏｎ ｆｏｒ Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ）を基盤とするメディアファイルフォーマットＩＳＯＢＭＦＦファイルでありうる。
【００３６】
方法は、暗号化されたデータがＴＳインタフェースを介して送信されることを受信制限モジュールに通知するために、共通インタフェースの制御インタフェースを介して受信制限モジュールに初期化メッセージを送信するステップを含むことができる。
【００３７】
方法は、受信制限モジュールに送信されるための暗号化されたデータに対して複数のフォーマットのうちの何れか一つを選択するステップ、及び受信制限モジュールに送信される初期化メッセージに選択されたフォーマットに対する情報を含めるステップを含む。
【００３８】
方法は、暗号化されたすべてのデータが送信された後に、制御インタフェースを介して受信制限モジュールに終了メッセージを送信するステップを含むことができる。
【００３９】
方法は、制御インタフェースを介して受信制限モジュールからデータ要請メッセージを受信するステップ、データ要請メッセージに規定された要請されたデータを検索するステップ、及び受信制限モジュールに要請されたデータを送信するステップを含む。
【００４０】
方法は、制御インタフェースを介して受信制限モジュールから記録された（ｗｒｉｔｔｅｎ）データ及びデータ位置情報が含まれたデータ記録要請メッセージを受信するステップ、及びデータ位置情報に応じてファイルにデータ記録要請メッセージに含まれたデータを記録するステップを含むことができる。
【００４１】
方法は、制御インタフェースを介して受信制限モジュールにトラック定義メッセージを受信するステップを含むことができ、トラック定義メッセージは、トラック及びトラックと関連したＤＲＭ情報に対する情報を含むことができる。
【００４２】
本発明の一実施の形態によれば、前記方法を行うためのプロセッサが含まれたコンピュータプログラムを格納するコンピュータ読み取り格納媒体を提供する。
【発明の効果】
【００４３】
以上説明したように本発明によれば、本発明の多様な実施形態により、暗号化されたコンテンツを共通インタフェースを介して受信制限モジュールに送信できるようになる。
【図面の簡単な説明】
【００４４】
【図１Ａ】本発明の一実施の形態にかかるマルチメディアデータを復号化するためのシステムを示すブロックである。
【図１Ｂ】本発明の一実施の形態にかかるマルチメディアデータを復号化するためのシステムを示すブロックである。
【図１Ｃ】本発明の一実施の形態にかかるマルチメディアデータを復号化するためのシステムを示すブロックである。
【図２】本発明の一実施の形態にかかる、ＴＳインタフェースを介して受信制限モジュールに受信されたＩＰパケットを送信するためのデータパケットの構造を示す図である。
【図３】本発明の一実施の形態にかかる、ＴＳインタフェースを介して受信制限モジュールに受信されたＩＳＯＢＭＤＤファイルのデータサンプルを送信するためのデータパケットの構造を示す図である。
【図４】本発明の他の実施の形態にかかる、ＴＳインタフェースを介して受信制限モジュールに受信されたＩＳＯＢＭＤＤファイルのデータサンプルを送信するためのデータパケ

ットの構造を示す図である。
【図５】図３及び図４に示すｍｓ＿ｄａｔａ構造のシンタックス（ｓｙｎｔａｘ）を示す図である。
【図６】本発明の一実施の形態にかかる、命令メッセージのシンタックスを示す図である。
【図７】他の類型の命令メッセージのｃｏｍｍａｎｄ＿ｉｄフィールド値を示す図である。
【図８】本発明の一実施の形態にかかる、初期化メッセージのシンタックスを示す図である。
【図９】図８の初期化メッセージに対して受信制限モジュールから受信されたｉｎｉｔ＿ａｃｋメッセージのシンタックスを示す図である。
【図１０】本発明の一実施の形態にかかる、受信制限モジュールから受信されたデータ要請メッセージのシンタックスを示す図である。
【図１１】図１０のデータ要請メッセージに対応して送信されたデータ応答メッセージのシンタックスを示す図である。
【図１２】本発明の一実施の形態にかかる、受信制限モジュールから送信されたｐｓｓｈアップデート要請メッセージのシンタックスを示す図である。
【図１３】図１２のｐｓｓｈアップデート要請メッセージに対応して送信されたｐｓｓｈアップデート応答メッセージのシンタックスを示す図である。
【図１４】本発明の一実施の形態にかかる、データ記録要請メッセージのシンタックスを示す図である。
【図１５】図１４のデータ記録要請メッセージに対応して送信されたデータ記録応答メッセージのシンタックスを示す図である。
【図１６】本発明の一実施の形態にかかる、トラック定義メッセージのシンタックスを示す図である。
【図１７】図１６のトラック定義メッセージに対応して受信制限モジュールから送信されたトラックアック（ｔｒａｃｋ＿ａｃｋ）メッセージのシンタックスを示す図である。
【図１８】本発明の一実施の形態にかかる、終了メッセージのシンタックスを示す図である。
【図１９】図１８の終了メッセージに対応して受信制限モジュールから送信された終了アック（ｃｌｏｓｅ＿ａｃｋ）メッセージのシンタックスを示す図である。
【図２０】本発明の一実施の形態にかかる、ＴＳインタフェースを介して受信制限モジュールに暗号化されたデータを送信する方法を説明するためのフローチャートである。
【図２１】本発明の一実施の形態にかかる、複数のカプセル化されたＩＰパケットを生成する方法を説明するためのフローチャートである。
【図２２】本発明の一実施の形態にかかる、データサンプルを維持するために複数のメディアサンプルパケット及びＩＳＯＢＭＦＦファイルから抽出された暗号化メタデータを生成するためのフローチャートである。
【図２３】本発明の一実施の形態にかかる、データサンプルを維持するために複数のＭＰＥＧ－２　ＴＳパケット及びＩＳＯＢＭＦＦファイルから抽出された暗号化メタデータを生成するためのフローチャートである。
【発明を実施するための形態】
【００４５】
以下に添付図面を参照しながら、本発明の好適な実施形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
【００４６】
図１Ａには、本発明の一実施の形態にかかる、暗号化されたマルチメディアデータを復号化するためのシステムが示されている。システムは、サーバのようなコンテンツ提供者１１０、コンテンツ提供者１１０から受信されたマルチメディアデータをデコードして再

生するためのデコーダ１２０、受信制限モジュール（ＣＡＳ）１３０及びスマートカード１４０を備える。

【００４７】

デコーダは、広帯域接続１５０を介してコンテンツ提供者１１０からマルチメディアデータを受信し、共通インタフェースを介して受信制限モジュール（ｃｏｎｄｉｔｉｏｎａｌ　ａｃｃｅｓｓ　ｍｏｄｕｌｅ：ＣＡＭ）１３０と接続される。共通インタフェースは、ＥＮ５０２２１規格に従って構成され、両方向ＴＳインタフェース１６０及び制御インタフェース１７０を備える。ＴＳインタフェース１６０は、各方向に１００Ｍｂ／ｓでデータを送信できる高速度のインタフェースである。ＴＳインタフェースは、本来ＥＮ５０２２１により定義されるが、ＣＩ　ｐｌｕｓ　ｓｐｅｃｉｆｉｃａｔｉｏｎにより拡張されうる。デコーダ１２０は、ＴＳインタフェース１６０を介して受信制限モジュール１３０に暗号化されたデータを送信し、ＴＳインタフェース１６０を介して受信制限モジュールから復号化されたデータを受信する。制御インタフェース１７０は、デコーダ１２０と受信制限モジュール１３０との間に制御信号を送信できる。例えば、制御インタフェース１７０は、ＴＳインタフェース１６０を介して送信された暗号化されたデータを受信制限モジュール１３０に通知できる。

【００４８】

本発明の一実施の形態にかかる、デコーダ１２０は、コンテンツ提供者１１０から暗号化されたマルチメディアデータを受信するためのチューナを備える。しかしながら、他の実施の形態では、暗号化されたデータは、遠隔ソースから受信されるものではなく、デコーダ１２０のハードディスクのように内部に格納されるか、又はＵＳＢのようなメモリスティックにより受信されうる。本発明の一実施の形態にかかる暗号化されたマルチメディアデータは、規格ＩＳＯ／ＩＥＣ　１４４９６－１２に定義されたものであって、ＩＳＯＢＭＦＦ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｏｒｇａｎｉｚａｔｉｏｎ　ｆｏｒ　Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ　Ｂａｓｅ　Ｍｅｄｉａ　Ｆｉｌｅ　Ｆｏｒｍａｔ）で受信される。しかしながら、本発明の他の実施の形態では、ＩＳＯ／ＩＥＣ　１４４９６－１２に定義されたＭＰ４ＦＦファイルのような他のフォーマットにより具現化されうる。一般に、本発明の実施の形態にかかるデコーダは、ＭＰＥＧ－２　ＴＳ形式の他に異なるファイル形式に暗号化されたマルチメディアデータを受信するように構成されうる。マルチメディアコンテンツを広帯域を介して受信することができる多様な方法がある。例えば、コンテンツダウンロード方法としてコンテンツは、ローカル格納媒体からダウンロードされる。ダウンロードが完了すると、コンテンツは、それを復号化するための受信制限モジュールを利用して再生されうる。プログレシブダウンロード（ｐｒｏｇｒｅｓｓｉｖｅ　ｄｏｗｎｌｏａｄ）方法では、コンテンツは、サーバから直ちに再生されうるように要請されることができる。コンテンツは、ＨＴＴＰ（ｈｙｐｅｒ－ｔｅｘｔ　ｔｒａｎｓｆｅｒ　ｐｒｏｔｏｃｏｌ）ＧＥＴ命令を利用して検索されうるシングルファイルとして受信されうる。適応的なストリーミング方法では、コンテンツが直ちに再生されうるように要請され、順次的なＨＴＴＰ　ＧＥＴ命令を利用して検索できる複数のファイルとして受信されうる。コンテンツストリーミング方法では、コンテンツがリアル－タイム送信プロトコル（ｒｅａｌ－ｔｉｍｅ　ｔｒａｎｓｐｏｒｔ　ｐｒｏｔｏｃｏｌ：ＲＴＰ）を利用して送信される連続的なストリーミングストリームとして受信されうる。上述したすべての実施の形態においてユーザは、コンテンツを再生する間に早送り又は巻き戻しのようなトリックモードを利用できる。本発明の実施の形態は、上述したコンテンツ送信方法のうち、少なくとも一つを利用でき、他の方法を利用することもできる。

【００４９】

デコーダ１２０及び受信制限モジュール１３０の動作は、図１Ｂ及び図１Ｃを参照して説明する。図１Ｂ及び図１Ｃは、本発明の一実施の形態にかかる、デコーダ１２０及び受信制限モジュール１３０の構成を示すブロック図である。図１Ｂに示すように、デコーダ１２０は、チューナ１２１、デモジュレータ１２２、デマルチプレクサ１２３、コンテンツ制御復号化モジュール１２４、制御モジュール１２５及び広帯域インタフェース１２６

を備える。また、図１Ｃに示すように、受信制限モジュール１３０は、ＣＡＳ復号化モジュール１３１、コンテンツ制御暗号化モジュール１３２、ＣＡＳキー計算モジュール１３３、コンテンツ制御システム暗号化器具モジュール１３４及び制御モジュール１３５を備える。

【００５０】

本発明の一実施の形態にかかる、デコーダ及び受信制限モジュールは、コンテンツ制御特性を定義するＣＩ　ｐｌｕｓ　ｓｐｅｃｉｆｉｃａｔｉｏｎによって構成されうる。コンテンツ制御は、デコーダに再度送信される前に復号化されたデータを暗号化し、その後にデータを復号化する。これは、ローカル暗号化であって、受信制限モジュール及びデコーダの間に非暗号化されたデータの未承認の複写を防止できる。ＣＩ　ｐｌｕｓと互換されるように構成されない本発明の実施の形態において、デコーダ及び受信制限モジュールのコンテンツ制御構成では、コンテンツ制御の復号化モジュール１２４、コンテンツ制御暗号化モジュール１３２、コンテンツ制御システム暗号化器具モジュール１３４が省略されうる。

【００５１】

デコーダ１２０のチューナ１２１は、コンテンツ提供者１１０から信号を受信し、特定チャネルを選局する。選択されたチャネルの信号は、２進数フォーマットに転換されるようにデモジュレータ１２２に送信される。この場合、デモジュレータ１２２は、チューナ１２１により受信された信号から暗号化されたデータを獲得できる。デコーダ１２０は、ＭＰＥＧ－２　ＴＳフォーマットを除いた第１ファイルフォーマットからＴＳインタフェース１６０を介して受信制限モジュール１３０に送信されうる第２ファイルフォーマットに暗号化されたデータを変換できる。第２ファイルフォーマットに暗号化されたデータを変換する間に、デコーダ１２０は、ＴＳインタフェース１６０を介して送信される複数のデータパケットを生成する。このとき、各々のデータパケットは、受信制限モジュール１３０により復号化されうる暗号化されたデータを含む。したがって、暗号化されたデータが複数のＭＰＥＧ－２　ＴＳパケットとして送信されない場合に、暗号化されたデータは、依然としてＴＳインタフェース１６０を介して送信されうる。

【００５２】

このとき、暗号化されたマルチメディアコンテンツは、従来のＭＰＥＧ－２　ＴＳフォーマットと異なるファイルフォーマットで受信されうる。したがって、本発明は、受信制限モジュール１３０に内蔵されるＤＲＭを許容するので、装置自体に内蔵されたＤＲＭで同じ方式により動作するようにユーザに見せる。すなわち、ユーザは、コンテンツがＭＰＥＧ－２　ＴＳ、ＩＳＯＢＭＦＦファイル、又は他のファイル形式で受信されるかどうかに関わらず完璧な方式でＤＲＭにより保護されるコンテンツに接続できる。本発明の実施の形態において、マルチメディアコンテンツは、ＩＳＯＢＭＦＦファイルとして受信されるが、代替形式は、他の実施の形態において用いられることができる。第２番目のファイル形式は、ＴＳフォーマット又は他の形式でありうる。適切な形式の例は、後述する。

【００５３】

図１Ｂ及び図１Ｃに示すように、ＴＳインタフェース１６０は、デコーダ１２０から受信制限モジュール１３０に暗号化されたデータを送信するための第１経路１６０ａ、及び受信制限モジュール１３０からデコーダ１２０に復号化されたデータを送信するための第２経路１６０ｂを備える両方向インタフェースである。デモジュレータ１２２がチューナ１２１から受信された信号から未暗号化データを抽出すると、デモジュレータ１２２は、デマルチプレクサ１２３に直にデータを送信し、受信制限モジュール１３０をバイパスできる。

【００５４】

受信制限モジュール１３０のＣＡＳ復号化モジュール１３１は、ＴＳインタフェース１６０の第１経路１６０ａを介してデコーダ１２０から暗号化されたデータを受信し、受信制限復号化暗号を利用してデータを復号化する。ＣＡＳキー計算モジュール１３３は、非承認ユーザから保護されるマルチメディアコンテンツの復号化及び視聴を防止するために

、スマートカード１４０を利用して認証を行う。復号化されたデータは、ＴＳインタフェース１６０の第２経路１６０ｂを介して復号化されたデータをデコーダ１２０に再度送信するために、コンテンツ制御暗号化モジュール１３２に送信される。復号化されたデータは、暗号化されたデータが受信制限モジュール１３０に送信される時のフォーマットと同様なフォーマットである第２ファイルフォーマットでデコーダ１２０に送信されるか、又は第３フォーマットを利用して送信されうる。

【００５５】

デマルチプレクサ１２３は、受信制限モジュール１３０のコンテンツ制御暗号化モジュール１３２から復号化されたマルチメディアデータを受信し、復号化されたデータからオーディオデータ、ビデオデータ及び／又は他のデータを抽出する。オーディオデータ、ビデオデータ及び／又は他のデータは、デコードされてユーザに見せられるようにコンテンツ制御復号化モジュール１２４に送信される。デコードされたオーディオデータ、ビデオデータ及び／又は他のデータは、即刻再生されるのではなく、ハードディスクのようなローカル格納媒体に格納されることができ、後に順次に再生されうる。

【００５６】

デコーダ１２０及び受信制限モジュール１３０は、制御インタフェース１７０を介してデコーダ１２０と受信制限モジュール１３０との間に制御メッセージを送信するための制御モジュール１２５、１３５をさらに備える。例えば、デコーダ１２０の制御モジュール１２５は、特定ファイルフォーマットでＴＳインタフェース１６０を介して送信される暗号化されたデータを受信制限モジュール１３０に通知するために、受信制限モジュール１３０の制御モジュール１２５に送信できる。また、制御モジュール１２５、１３５は、外部機器と通信するためにデコーダ１２０の広帯域インタフェース１２６を利用できる。例えば、受信制限モジュール１３０のＤＲＭは、ユーザが特定コンテンツを再生するための適切な権利があるかどうかを確認するために、遠隔インターネットを介して遠隔サーバと通信する必要がある。これは、デコーダの広帯域インタフェースを介してＩＰパケットを送受信するように受信制限モジュール１３０を許容するために、ＣＩ ｐｌｕｓにより定義されたＬＳＣ（ｌｏｗ ｓｐｅｅｄ ｃｏｍｍｕｎｉｃａｔｉｏｎ）リソースを利用して行われることができる。広帯域インタフェース１２６は、マルチメディアコンテンツをコンテンツ提供者１１０から受信される物理的な線のような接続線として利用できるか、又は分離された物理的な接続線として利用できる。

【００５７】

本発明は、上述した図１Ａ、図１Ｂ及び図１Ｃのように具現化されうるが、これに制限されるものではない。図１Ｂ及び図１Ｃに示す構成要素は、必ず物理的に別の構成要素ではないが、例えば、プロセッサで実行されるソフトウェアモジュールにより具現化されることができ、一つ以上の構成要素の機能は、単一モジュールに統合されるか、又はいくつかのモジュールに分離されうる。

【００５８】

ＴＳインタフェースを介して暗号化されたデータを送信するのに適したデータパケット構造に対する実施の形態を、図２ないし図４を参照して説明する。デコーダ１２０は、デコーダがデータの受信されるファイル形式を理解することが必要でない場合、受信されたデータファイルに対する第１パッシングなしでデータパケットを生成できる。デコーダが受信されたデータファイルをパッシングしない実施の形態は、図２に示されている。大体的に、デコーダ１２０は、復号化のために受信制限モジュール１３０に送信されるように暗号化されたデータサンプルを抽出するために、受信されたデータファイルをパッシングできる。この場合、マルチメディアコンテンツは、デコーダにより理解されうるファイルフォーマットで受信されうる。受信されたデータファイルがデコーダによりパッシングされる実施の形態野に対しては、図３及び図４に示されている。

【００５９】

図２は、本発明の一実施の形態にかかる、ＴＳインタフェース１６０を介して受信制限モジュール１３０に受信されたＩＰパケットを送信するためのデータパケットを示す図で

ある。本発明の一実施の形態によれば、マルチメディアコンテンツは、ＩＳＯＢＭＦＦファイル２１０としてサーバに存在する。ＩＳＯＢＭＦＦ規格によれば、ファイルのデータは、複数のボックスを備える。図２に示す実施の形態では、ＩＳＯＢＭＦＦファイル２１０は、フレームのインデックスを有するｍｏｏｖ／ｍｏｏｆ　ｂｏｘ及びムービーデータを有するｍｄａｔボックスを備える。他のタイプのボックスがＩＳＯＢＭＦＦ規格により備えられても良く、本発明は、図２に示す特定ＩＳＯＢＭＦＦファイルに制限されるものではない。

【００６０】

サーバは、ＴＣＰ／ＩＰヘッダ及びＩＯＳＭＦＦファイル２１０の領域を含む複数のＩＰパケット２２０を生成し、デコーダ１２０にＩＰパケット２２を送信する。例えば、デコーダ２０は、ＴＣＰ／ＩＰ接続線を介してＨＴＴＰを利用してＩＰパケットを受信することができる。

【００６１】

本発明の一実施の形態においてデコーダ２１０がＩＰパケット２２０をＮＴＬＳする場合、デコーダ２２０は、再構成するためにパケットからＩＳＯＢＭＦＦデータを抽出せずに、ＩＳＯＢＭＦＦファイルをパッシングする。その代わりに、ＩＳＯＢＭＦＦファイルのデータを有する受信されたＩＰパケットの各々に対して、デコーダ１２０は、受信されたＩＰパケット、シンクバイト（ｓｙｎｃ　ｂｙｔｅ）及びヘッダバイト（ｈｅａｄｅｒ　ｂｙｔｅ）を含むカプセル化されたＩＰパケットを生成する。本発明の一実施の形態では、シンクバイトが０ｘＢ８の値が設定されているが、他の実施の形態において他の値も用いられることができる。ヘッダバイトは、２個の送信スクランブルリング制御ビットと６個の予約されたビットを含む。受信制限モジュール１３０に送信されたカプセル化されたＩＰパケットにおいて、二つの送信スクランブルリング制御ビットは、００（ｎｏ　ｓｃｒａｍｂｌｉｎｇ）に設定される。受信制限モジュール１３０から受信されたカプセル化されたＩＰパケットにおいて、送信スクランブルリング制御ビットは、ＣＩ　ｐｌｕｓ　ｓｐｅｃｉｆｉｃａｔｉｏｎにより定義されたように、００、０１又は１０に設定されることができる。カプセル化されたＩＰパケット２３０は、ＴＳインタフェースを介して受信制限モジュール１３０に送信される。ＩＳＯＢＭＦＦファイルのデータを含まない受信されたＩＰパケットは、受信制限モジュール１３０に送信されなければならない必要はない。

【００６２】

本発明においてＩＰパケット２２０がサーバから受信されるが、これは、一実施の形態に過ぎず、他の実施の形態では、マルチメディアデータがデコーダに内蔵されたハードディスクのように内部に格納されるか、又はデコーダに接続したＵＳＢメモリスティックから受信されうる。このような実施の形態では、デコーダ１２０が格納されたマルチメディアデータファイルを複数のＩＰパケットとしてパッケージングし、ＴＳインタフェースを介して送信するために、ＩＰパケットをカプセル化できる。

【００６３】

本発明の一実施の形態では、ＴＳインタフェース１６０を介して通過するデータはＴＳではない。しかしながら、ＴＳインタフェース１６０のすべての信号の電気的タイミングは、不連続（ｄｉｓｃｏｎｔｉｎｕｏｕｓ）及び爆発（ｂｕｒｓｔｙ）になるＭＣＬＫＩ及びＭＣＬＫＯを除いて、ＥＮ５０２２１標準に規定されたとおり維持されうる。このような信号は、以下のように定義される。

【００６４】

ＭＣＬＫＩ：デコーダから受信制限モジュールまでバイトクロック。立ち上がりエッジは、ＭＤＩ、ＭＩＳＴＲＴ及びＭＩＶＡＬ信号の値を受信制限モジュールに記録するのに用いられる。

【００６５】

ＭＩＳＴＲＴ：デコーダから受信制限モジュールに送信されたパケット同期化バイトに対する有効性。

【００６６】
ＭＩＶＡＬ：ＭＤＩ０－７に有効なデータバイトを示す。
【００６７】
ＭＤＩ０－７：デコーダから受信制限モジュールに送信されたデータに対するデータバス。
【００６８】
ＭＣＬＫＯ：受信制限モジュールからデコーダまでのバイトクロック。立ち上がりエッジは、ＭＤＯ、ＭＯＳＴＲＴ及びＭＯＶＡＬ信号の値をデコーダに記録するのに用いられる。
【００６９】
ＭＯＳＴＲＴ：受信制限モジュールからデコーダに送信されたパケット同期化バイトに対する有効性。
【００７０】
ＭＯＶＡＬ：ＭＤＯ０－７に有効なデータバイトを示す。
【００７１】
ＭＤＯ０－７：受信制限モジュールからデコーダに送信されたデータに対するデータバス。
【００７２】
本発明の実施の形態において、ＩＰパケットは、カプセル化されたＩＰパケットであって、ＴＳインタフェースを介して送信される。しかしながら、本発明の他の実施の形態によるデコーダは、ＥＴＳＩ ＥＮ ３０１で１９２に定義されたＭｕｌｔｉｐｒｏｔｏｃｏｌ Ｅｎｃａｐｓｕｌａｔｉｏｎ（ＭＰＥ）を使用してＴＳインタフェースを介してＩＰパケットを送信するように構成されうる。この場合には、デコーダは、ペイロード又はアドレススクランブルリングを利用せず、受信制限モジュール１３０は、ＭＡＣアドレスフィールド及びプログラムマップテーブル（Ｐｒｏｇｒａｍ Ｍａｐ Ｔａｂｌｅ）を無視できる。図８を参照して後に説明する初期化Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｄａｔａ Ｕｎｉｔ（ＡＰＤＵ）に信号処理されたパケット識別子（ＰＩＤ）は、ＭＰＥデータを含むすべてのパケットに用いられる。
【００７３】
図２の実施の形態によれば、デコーダは、受信されたファイルをパッシングせず、受信されたマルチメディアデータのファイルフォーマットを理解することができるデコーダが必要でない。しかしながら、他の実施の形態では、デコーダが受信制限モジュール３０に送信される暗号化されたデータを抽出するために、受信されたファイルをパッシングする。例えば、暗号化されたデータがＩＳＯＢＭＦＦファイルとして受信される場合、メディアサンプルデータ及びメディアサンプルと関連した暗号化メタデータは、ファイルから抽出され、ＴＳインタフェース１６０を介して受信制限モジュール１３０に送信される。このような場合に、利用される適切なデータパケットの構造は、図３及び図４に示される。デコーダが暗号化メタデータを抽出するために、ＩＳＯＢＭＦＦファイルのパッシングが要求される場合、ファイルは、ＩＳＯ／ＩＥＣ １４４９６－１２に対する改正草案に定義された共通暗号化方式を遵守しなければならない。
【００７４】
図３は、本発明の一実施の形態にかかる、ＴＳインタフェースを介して受信制限モジュールに受信されたＩＳＯＢＭＤＤファイルのデータサンプルを送信するためのデータパケットの構造を示す図である。一実施の形態によれば、デコーダ１２０は、ＩＳＯＢＭＦＦファイル３１０を受信し、ｍｄａｔボックスからデータサンプル及びｍｏｏｖ／ｍｏｏｆｂｏｘからデータサンプルと関連した暗号化メタデータを抽出するために、ファイルをパッシングする。データサンプル及び暗号化メタデータｍｓ＿ｄａｔａ（）構造３２０でカプセル化される。これについては、後に詳細に説明する。各々のｍｓ＿ｄａｔａ（）構造３２０は、ＩＳＯＢＭＦＦファイルから抽出された一つのデータサンプル又は複数のデータサンプルを含む。ここで、データサンプルは、ＩＳＯＢＭＦＦファイル３１０から抽

出されたデータ領域（例えば、ｍｄａｔ　ｂｏｘから抽出されたメディアデータ）のことを意味する。デコーダ１２０は、ＩＳＯＢＭＦＦのすべてのデータサンプルを復号化するまでＴＳインタフェース１６０を介して受信制限モジュール１３０にｍｓ＿ｄａｔａ（）構造３２０のストリームを順次送信できる。

【００７５】

たとえ、メタデータ及び特定メディアサンプルと関連した制御情報がＴＳインタフェース１６０を介してメディアサンプルと共に送信されても、このような必要は、ファイルが全般的に変化するのではないデータに適用されるのではない。例えば、ファイルを介して変更されないメタデータ及び制御情報は、ＴＳインタフェースを介する代わりに、制御インタフェースを介して受信制限モジュールに送信される。

【００７６】

本発明の一実施の形態にかかる、各々のｍｓ＿ｄａｔａ（）構造３２０は、ＴＳインタフェース１６０を介して送信されるメディアサンプルパケット３２０にカプセル化される。デコーダ１２０は、ｍｓ＿ｄａｔａ（）構造３２０にシンクバイト及びヘッダバイトを追加することによって、メディアサンプルパケット３３０を生成する。本発明の一実施の形態にかかるシンクバイトは、０ｘＢ８の値を有しているが、他の実施の形態の他の値も用いられうる。ヘッダバイトは、２個の送信スクランブルリング制御ビットと、１に設定された６個の予約されたビットを含む。デコーダ１２０から受信制限モジュール１３０に送信されたメディアサンプルパケット３３０において送信スクランブルリング制御ビットは、００に設定される。デコーダ１２０から受信制限モジュール１３０に送信したメディアサンプルパケット３３０において送信スクランブルリング制御ビットは、ＣＩ　ｐｌｕｓ　ｓｐｅｃｉｆｉｃａｔｉｏｎにより定義されたとおり、００、０１又は１０に設定される。

【００７７】

本発明の実施の形態においてｍｓ＿ｄａｔａ（）構造３２０は、あるＴＳパケットがカプセル化せずにＴＳインタフェースを介して送信される。したがって、ＴＳインタフェースを介して送信されるデータ送信ストリームではない。

【００７８】

しかしながら、図２の実施の形態のように、ＴＳインタフェース１６０にあるすべての信号に対する電気的タイミングは、不連続及び一回ずつ発生するＭＣＬＫＩとＭＣＬＫＯを除いて、ＥＮ５０２２１標準に規定されたとおりに維持されうる。信号は、次の通りに定義される。

【００７９】

ＭＣＬＫＩ：デコーダから受信制限モジュールまでバイトクロック。立ち上がりエッジは、ＭＤＩ、ＭＩＳＴＲＴ及びＭＩＶＡＬ信号の値を受信制限モジュールに記録するのに用いられる。

【００８０】

ＭＩＳＴＲＴ：デコーダから受信制限モジュールに送信されたメディアサンプルパケット同期化バイトに対して有効である。

【００８１】

ＭＩＶＡＬ：ＭＤＩ０－７に有効なデータバイトを示す。

【００８２】

ＭＤＩ０－７：デコーダから受信制限モジュールに送信されたデータに対するデータバス。

【００８３】

ＭＣＬＫＯ：受信制限モジュールからデコーダまでバイトクロック。立ち上がりエッジは、ＭＤＯ、ＭＯＳＴＲＴ及びＭＯＶＡＬ信号の値をデコーダに記録されるのに用いられる。

【００８４】

ＭＯＳＴＲＴ：デコーダから受信制限モジュールに送信されたメディアサンプルパケッ

ト同期化バイトに対して有効である。
【００８５】
ＭＯＶＡＬ：ＭＤＯ０－７に有効なデータバイトを示す。
【００８６】
ＭＤＯ０－７：受信制限モジュールからデコーダまで送信されたデータに対するデータバス。
【００８７】
図４は、本発明の他の実施の形態にかかる、ＴＳインタフェースを介して受信制限モジュールに受信されたＩＳＯＢＭＤＤファイルのデータサンプルを送信するためのデータパケットの構造を示す図である。本発明の一実施の形態では、デコーダ１２０は、ｍｄａｔａｂｏｘからデータサンプルを抽出するためにＩＳＯＢＭＦＦファイル４１０をパッシングし、図３に示しているものと類似するようにｍｓ＿ｄａｔａ（）構造４２０を抽出されたデータに含める。しかしながら、本発明の一実施の形態では、ｍｓ＿ｄａｔａ（）構造４２０は、ＴＳインタフェース１６０を介して送信されるために、ＭＰＥＧ－２　ＴＳに挿入される。特に、ｍｓ＿ｄａｔａ（）構造４２０のデータは、受信制限モジュール１３０に送信されるために、複数のＴＳパケット４３０ａ、４３０ｂに挿入される。このとき、各々のＴＳパケット４３０ａ、４３０ｂは、ＴＳヘッダ及びｍｓ＿ｄａｔａ（）構造４２０を備えるペイロードフィールドを含む。ｍｓ＿ｄａｔａ（）構造４２０は、ＥＴＳＩ　ＥＮ　３０１１９２に定義されたデータパイプ（Ｄａｔａ　Ｐｉｐｅ）を利用してＴＳに挿入される。この場合、ｍｓ＿ｄａｔａ（）構造４２０は、常にＴＳパケットの開始点から始まる。
【００８８】
本発明の一実施の形態において、受信制限モジュール４２０は、複数のＴＳパケット４３０ａ、４３０ｂを受信し、ｍｓ＿ｄａｔａ（）構造４２０を再構成し、ｓａｍｐｌｅ＿ｄａｔａフィールドに存在するデータサンプル又はサンプルを復号化する。受信制限モジュール１３０は、ｍｓ＿ｄａｔａ（）構造４２０から復号化されたｓａｍｐｌｅ＿ｄａｔａを含むＴＳを復旧できる。デコーダがＣＩ　ｐｌｕｓと互換されると、受信制限モジュール１３０から復旧されたＴＳパケットは、ローカルに暗号化される。しかしながら、他の実施の形態の受信制限モジュール１３０は、他のデータフォーマットを利用して復号化されたデータを復旧する。
【００８９】
デコーダ１２０は、受信制限モジュール１３０にデータパイプ（ｄａｔａ　ｐｉｐｅ）の存在及びそれと関連したパラメータを通知するために、制御インタフェース１７０を介して受信制限モジュール１３０に制御メッセージを送信できる。したがって、ＰＡＴ（ｐｒｏｇｒａｍ　ａｓｓｏｃｉａｔｉｏｎ　ｔａｂｌｅ）及びＰＭＴ（ｐｒｏｇｒａｍ　ｍａｐ　ｔａｂｌｅ）が要求されずに、受信制限モジュール１３０は、ＰＡＴやＰＭＴが存在する場合、それを無視できる。
【００９０】
図４のＴＳにおいて送信パケットヘッダは、ＭＰＥＧ－２規格で定義された通りにフォーマット化できる。本発明では、送信パケットヘッダビットは、下記のように設定される。データパケットのパケットＩＤ（ＰＩＤ）は、初期化（）ＡＰＤＵにより表示される値に設定されることができる。ナルパケット（ｎｕｌｌ　ｐａｃｋｅｔ）に対し、ＰＩＤは、０ｘ１　ｆｆｆに設定される。ｓｙｎｃ＿ｂｉｔｅは、０ｘ４７に設定される。ｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌｂｉｔｓは、デコーダ１２０から受信制限モジュール１３０に送信されたＴＳのために００（ｎｏ　ｓｃｒａｍｂｌｉｎｇ）に設定され、受信制限モジュール１３０からデコーダ１２０に送信されたＴＳのために（ＣＩ　ｐｌｕｓに定義された）００、０１又は１０に設定される。ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌｂｉｔｓは、０１（ｎｏｄａｐａｔａｔｉｏｎ　ｆｉｅｌｄ、ｐａｙｌｏａｄ　ｏｎｌｙ）に設定される。ｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒｂｉｔｓは、ＩＳＯ／ＩＥＣ　１３８１８－１に定義された通りに利用される。ｐａｙ

ｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは、ｍｓ＿ｄａｔａ（）構造４２０の開始を含むＴＳパケットのために１に設定される。ｔｒａｎｓｐｏｒｔ＿ｅｒｒｏｒ＿ｉｎｄｉｃａｔｏｒ及びｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙ ｂｉｔｓは、すべて０に設定される。ナルパケットが要求される場合には、ナルパケットは、データを送信するパケットの間に挿入されることができる。

【００９１】

ＴＳパケットヘッダのｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒ ｂｉｔｓは、流量制御システム（ｆｌｏｗ ｃｏｎｔｒｏｌ ｓｙｓｔｅｍ）でデコーダとして用いられることができる。カウンタ値を有した以前のＴＳパケットが受信制限モジュール１３０から受信されるまで、特定カウンタ値を有するＴＳパケットは、受信制限モジュール１３０に送信されない。ナルパケットは、こういう目的のために無視される。

【００９２】

図５は、図３及び図４に示すｍｓ＿ｄａｔａ構造のシンタックス（ｓｙｎｔａｘ）を示す図である。図５で、ニーモニック（ｍｎｅｍｏｎｉｃ）ｕｉｍｓｂｆは、最上位ビットであって、符号のない整数を示す（ｕｎｓｉｇｎｅｄ ｉｎｔｅｒｇｅｒ ｍｏｓｔ ｓｉｇｎｉｆｉｃａｎｔ ｂｉｔ ｆｉｒｓｔ）。ｍｓ＿ｄａｔａ（）を生成するために、デコーダ１２０は、ＩＳＯＢＭＦＦファイルをパッシングし、要求されるデータを抽出する。

【００９３】

ＩＳＯＢＭＦＦファイルに各々のトラックに対して、デコーダ１２０は、受信制限モジュール１３０が復号化に必要なすべてのトラックを認知するようにするために、制御インタフェース１７０を介して受信制限モジュール１３０に設定された情報を送信できる。ＩＳＯＢＭＦＦファイルに各々のトラックは、「ｔｋｈｄ」ボックスにｔｒａｃｋ＿ＩＤ値として格納されたことと関連したトラック番号を有する。デコーダ１２０は、ｓａｉｏ及びｓａｉｚボックスにより確認されたものとしてサンプル暗号化情報と関連した各々のトラックに対してｍｄａｔ ｂｏｘからデータサンプルを抽出する。ここで、データサンプルは、ｍｄａｔボックス又は他のボックスから抽出された単一バイトを参照でき、単一ｍｓ＿ｄａｔａ（）メッセージは、複数のデータサンプルを含む。すなわち、単一ｍｓ＿ｄａｔａ（）メッセージは、複数のバイトを含むことができる。トラックに対する少なくとも一つのメディアサンプルは、図５に定義されたｍｓ＿ｄａｔａ（）構造を利用して受信制限モジュール１３０に送信される。

【００９４】

ｍｓ＿ｄａｔａ（）構造において、ｔｒａｃｋ＿ＩＤフィールドは、特定ｍｓ＿ｄａｔａ（）メッセージに含まれたメディアサンプルに対するトラック番号を格納する３２ビットフィールドである。Ｎｕｍｂｅｒ＿ｏｆ＿ｓａｍｐｌｅｓは、特定ｍｓ＿ｄａｔａ（）メッセージに含まれたメディアサンプルの個数を格納する８ビットフィールドである。ＡｌｇｏｒｉｔｈｍＩＤは、ＩＳＯＢＭＦＦファイルの「ｔｅｎｃ」ボックス又は「ｓｇｐｄ」ボックスから抽出されたものであって、メディアサンプルに用いられる暗号化アルゴリズムを格納する２４ビットフィールドである。ＩＶ＿ｓｉｚｅは、「ｔｅｎｃ」ボックス又は「ｓｇｐｄ」ボックスから抽出されたものであって、メディアサンプルに対するＩＶの大きさを格納する８ビットフィールドである。ＫＩＤは、「ｔｅｎｃ」ボックス又は「ｓｇｐｄ」ボックスから抽出されたものであって、メディアサンプルに対するＫＥＹ ＩＤを格納する１６ｘ８ビットフィールドである。Ａｕｘｉｌｉａｒｙ＿ｓａｍｐｌｅ＿ｓｉｚｅは、ｓａｉｚボックスに指示された通りに、メディアサンプルに対する補助データの量を格納する８ビットフィールドである。Ａｕｘｉｌｉａｒｙ＿ｓａｍｐｌｅ＿ｄａｔａは、ｓａｉｏボックスにより参照されるように、メディアサンプルに対する補助データを格納する８ビットフィールドである。Ｓａｍｐｌｅ＿ｌｅｎｇｔｈは、メディアサンプルでバイトの個数を格納する３２ビットフィールドである。Ｓａｍｐｌｅ＿ｄａｔａは、ｍｄａｔボックスから抽出されたサンプルのデータバイトを格納するための８ビットフィールドである。

【００９５】
デコーダ１２と受信制限モジュール１３０との間に暗号化されたデータ及び復号化データの送信を調整するために、デコーダ１２０と受信制限モジュール１３０とは、共通インタフェースの制御インタフェース１７０を介して各々互いに制御メッセージを送信するように構成される。例えば、受信制限モジュール１３０は、暗号化されたマルチメディアデータを正確に読み取るために、ＩＳＯＢＭＦＦファイルのメタデータから特定情報を要求できる。制御メッセージの例は、図６ないし図１９を参照して説明される。
【００９６】
図６は、本発明の一実施の形態にかかる、命令メッセージのシンタックスを示す図である。図６に示すメッセージ構造は、制御インタフェースを介して送信したすべてのメッセージに適用されうる一般的な構造である。
【００９７】
命令メッセージは、ＣａｂｌｅＣａｒｄインタフェース仕様及びＣＩ ｐｌｕｓにより定義された特定応用プログラム支援（Ｓｐｅｃｉｆｉｃ Ａｐｐｌｉｃａｔｉｏｎ Ｓｕｐｐｏｒ：ＳＡＳ）リソースを利用して送信されうる。例えば、一実施の形態では、デコーダ１２０が受信制限モジュール１３０により復号化されたＩＳＯＢＭＦＦファイルが要求されると、デコーダ１２０は、０ｘｚｚｚｚｚｚ値のｐｒｉｖａｔｅ＿ｈｏｓｔ＿ａｐｐｌｉｃａｔｉｏｎ＿ＩＤとＳＡＳのリソースにセッションをオープンできる。ファイルの復号化が完了すると、受信制限モジュール１３０は、ｃｌｏｓｅ＿ａｃｋ（）ＡＰＤＵをデコーダ１２０に送信する。ｃｌｏｓｅ＿ａｃｋ（）メッセージが受信制限モジュール１３０から受信されると、デコーダ１２０は、セッションを閉じることができる。しかしながら、デコーダ１２０は、復号化されることを待つ他のＩＳＯＢＭＦＦファイルがあると、セッション開きを維持できる。セッションがある理由により早く閉じられていると、装置と受信制限モジュールとは、このＩＳＯＢＭＦＦファイルに関連したＴＳインタフェースを介してあるデータ送信を中止できる。
【００９８】
命令メッセージは、ＳＡＳ＿ａｓｙｎｃ＿ｍｓｇ（）応用プログラムプロトコルデータ単位（ＡＰＤＵｓ）を利用して、装置と受信制限モジュールとの間で制御インタフェースを介して送信されうる。ＡＰＤＵのｍｅｓｓａｇｅ＿ｂｙｔｅフィールドから送信されるメッセージの一般的なフォーマットは、図６に示され、ｃｏｍｍａｎｄ＿ｉｄ、ｔｒａｎｓａｃｔｉｏｎ＿ｉｄ及びｐａｙｌｏａｄ（）を含むことができる。Ｃｏｍｍａｎｄ＿ｉｄは、送信されるメッセージの特定る類型を表す８ビットフィールドである。Ｔｒａｎｓａｃｔｉｏｎ＿ｉｄは、データ要請メッセージを送信する装置により生成される固有な３２ビット値を維持する。例えば、ｔｒａｎｓａｃｔｉｏｎ＿ｉｄ値は、応答又はアックのようなある該当応答メッセージに返還される。ｔｒａｎｓａｃｔｉｏｎ＿ｉｄ情報に対する非同期要請は、情報を返還する回答と結合できる。このフィールドの値には、制約がない。ある場合には、ペイロード（）は、メッセージのペイロードが含まれる。
【００９９】
本発明の一実施の形態では、受信制限モジュール１３０のＤＲＭにエラーが発生する場合に、受信制限モジュール１３０は、デコーダ、又はその他装置にメッセージを送信するように構成されうる。例えば、受信制限モジュール１３０は、ＯＩＰＦ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｖｏｌｕｍｅ７に規定されたＯＩＰＦ ｒｉｇｈｔｓ＿ｉｎｆｏ又はｐａｒｅｎｔａｌ＿ｃｏｎｔｒｏｌ＿ｉｎｆｏメッセージを送信するか、又はＣＩ ｐｌｕｓ ｓｐｅｃｉｆｉｃａｔｉｏｎに定義されたＣＩ＋ブラウザーを利用できる。
【０１００】
図７は、他の類型の命令メッセージのｃｏｍｍａｎｄ＿ｉｄフィールド値を示す図である。図７では、Ｄｉｒｅｃｔｉｏｎ ｃｏｌｕｍｎは、デコーダ１２０を表すＤ及び受信制限モジュール１３０を表すＣと共に送信される特定メッセージの送信方向を示す。他のメッセージ類型は、図８ないし図１９を参照してさらに詳細に説明する。図８ないし図１９では、ｃｏｍｍａｎｄ＿ｉｄとｔｒａｎｓａｃｔｉｏｎ＿ｉｄフィールドは、一般的な

メッセージ形式の一部であり、すべてのメッセージ類型において一般的なものであるので、もうこれ以上説明しないことにする。

【０１０１】

図８は、本発明の一実施の形態にかかる、初期化メッセージのシンタックスを示す図である。デコーダ１２０がＩＳＯＢＭＦＦファイルからデータを送信し始めることを表すために、デコーダ１２０は、受信制限モジュール１３０にこのメッセージを送信することができる。本発明の実施の形態において、初期化メッセージは、装置がファイルを送信するのに用いられうるパケット識別子（ＰＩＤ）を受信制限モジュール１３０に提供するのに利用される。復号化されたメディアデータを受信制限モジュール１３０に送信する前に、デコーダ１２０は、ＴＳインタフェース１６０を介して他のデータの送信を中止する。受信制限モジュール１３０は、デコーダ１２０から初期化メッセージを受信する時、それが内部バッファに保有できる内容データをフラッシュ（ｆｌｕｓｈ）し、ＩＳＯＢＭＦＦファイルデータを受信する準備を行うことができる。

【０１０２】

デコーダ１２０が受信制限モジュール１３０にデータを送信する前に、ＩＳＯＢＭＦＦファイルをパッシングする実施の形態では、ｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵは、ｍｏｏｖボックスに含まれたｐｓｓｈボックスのすべてのコンテンツを含むことができる。ｐｓｓｈデータの送信は、受信制限モジュール１３０がＩＳＯＢＭＦＦファイルに含まれたマルチメディアコンテンツに対するユーザのアクセス権限を確認するために、ｐｓｓｈデータのライセンス確認を許容する。例えば、デコーダがファイルをパッシングしない実施の形態では、ＩＳＯＢＭＦＦファイルがＩＰパケットとして受信制限モジュール１３０に送信される場合、デコーダ１２０がＩＳＯＢＭＦＦファイルをパッシングしなかったからｐｓｓｈボックスの内容が省略される。

【０１０３】

図８に示すように、初期化メッセージの特定ペイロードは、ｃｏｎｔｅｎｔ＿ｆｏｒｍａｔ、ｔｓ＿ｐａｃｋｅｔ＿ｐｉｄ及びｐｓｓｈ＿ｃｏｕｎｔを含む。Ｃｏｎｔｅｎｔ＿ｆｏｒｍａｔは、データがＴＳインタフェース１６０を介して送信されるフォーマットを表す２ビットフィールドである。００の値は、図３に示すようなメディアサンプルパケットを利用して送信されるコンテンツを表すのに用いられる。０１の値は、図４に示すようなＴＳでカプセル化されたｍｓ＿ｄａｔａ（）構造を利用して送信されるコンテンツを表すのに利用される。１０値は、図２のようにコンテンツがカプセル化されたＩＰパケットとして送信されることを表すのに用いられる。１１値は、ＭＰＥを利用してコンテンツがＩＰパケットとして送信されることを表すのに用いられる。したがって、初期化メッセージは、既存のＭＰＥＧ－２　ＴＳから他のファイル形式へ変更されたことを受信制限モジュール１３０に通知するのに利用されうる。

【０１０４】

本発明の実施の形態において、デコーダ１２０は、ｃｏｎｔｅｎｔ＿ｆｏｒｍａｔフィールドにより表示されるように、複数の形式のうちの何れか一つで暗号化されたコンテンツを受信制限モジュール１３０に送信できる。しかしながら、他の実施の形態のデコーダは、常に特定の一つのフォーマットで暗号化されたデータを送信できる。受信制限モジュール１３０が常に特定フォーマットで暗号化されたデータを受信するように構成されうる場合、ｃｏｎｔｅｎｔ＿ｆｏｒｍａｔフィールドは省略されうる。

【０１０５】

ＴＳ＿ｐａｃｋｅｔ＿ｐｉｄは、ｃｏｎｔｅｎｔ＿ｆｏｒｍａｔが０１又は１１の場合、ＩＳＯＢＭＦＦファイルを含むＴＳパケットに対してデコーダにより利用されたＰＩＤの値を維持する１３ビットフィールドである。Ｐｓｓｈ＿ｃｏｕｎｔは、ｍｏｏｖボックスに含まれたｐｓｓｈボックスの個数を格納する８ビットフィールドである。ＩＳＯＢＭＦＦファイルがパッシングされなくてｃｏｎｔｅｎｔ＿ｆｏｒｍａｔが１０の場合、Ｐｓｓｈ＿ｃｏｕｎｔ値は、ゼロである。Ｐｓｓｈ＿ｄａｔａ（）は、ｐｓｓｈボックスのコンテンツを保有する。

【０１０６】
図９は、図８の初期化メッセージに対して受信制限モジュール１３０から受信されたｉｎｉｔ＿ａｃｋメッセージのシンタックスを示す図である。暗号化されたデータを受信する準備が完了すると、ｉｎｉｔ＿ａｃｋメッセージは、受信制限モジュール１３０により送信されうる。
【０１０７】
図９に示すように、ｉｎｉｔ＿ａｃｋ（）ＡＰＤＬのペイロードは、８ビット状態（ｓｔａｔｕｓ）フィールドを含む。この値が０の場合は、メッセージは、受信制限モジュール１３０がＩＳＯＢＭＦＦファイルデータを復号化する準備ができたことを表す。この値が１である場合に、メッセージは、受信制限モジュール１３０が特定されないエラーによって準備されないことを示す。この値が２である場合に、メッセージは、前の初期化メッセージに指定されたように、要請されたｃｏｎｔｅｎｔ＿ｆｏｒｍａｔが支援されないことを示す。受信されたｉｎｉｔ＿ａｃｋ（）ＡＰＤＵが２と同じ状態である場合に、デコーダ１２０は、他のｃｏｎｔｅｎｔ＿ｆｏｒｍａｔ値を新しいｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵに送信できる。
【０１０８】
本発明の実施の形態において受信制限モジュール１３０から受信されたｉｎｉｔ＿ａｃｋ（）ＡＰＤＵが０である場合に、デコーダ１２０が受信制限モジュール１３０に復号化されるためのデータを送信しないと、デコーダ１２０は、ナルパケットがＴＳインタフェースを介して受信制限モジュール１３０により出力されると仮定できる。
【０１０９】
図１０は、本発明の一実施の形態にかかる、受信制限モジュール１３０から受信されたデータ要請メッセージのシンタックスを示す図である。ｄａｔａ＿ｒｅｑ（）ＡＰＤＵは、デコーダ１２０からＩＳＯＢＭＦＦファイルより特定データを要請するために受信制限モジュール１３０により利用されることができる。例えば、受信制限モジュール１３０は、メディアサンプルを正確に復号化するために、ファイルから特定データを要求できる。データは、ＤＲＭを設定するために要求される。この場合、コンテンツに対するユーザの権利を確認し適切な復号化ユニットを設定できるように、受信制限モジュール１３０は、ＩＳＯＢＭＦＦファイルからデータのピース（ｐｉｅｃｅ）を要請できる。ｄａｔａ＿ｒｅｑ（）ＡＰＤＵは、ｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵで以後にいつでも送信されることができて、ｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵを応答するためのｉｎｉｔ＿ａｃｋ（）ＡＰＤＵを送信する前に送信されることができる。
【０１１０】
図１０に示すように、ｄａｔａ＿ｒｅｑ（）ＡＰＤＵのペイロードは、ｄａｔａ＿ｏｆｆｓｅｔフィールドとｄａｔａ＿ｌｅｎｇｔｈフィールドとを含む。Ｄａｔａ＿ｏｆｆｓｅｔは、値が要求されるデータを確認することができるＩＳＯＢＭＦＦファイルの始めからバイトでオフセットに対応する値の６４ビットフィールドである。Ｄａｔａ＿ｌｅｎｇｔｈは、バイトの数字で表現され、要請されるデータの長さを格納する３２ビットフィールドである。受信制限モジュール１３０からｄａｔａ＿ｒｅｑ（）ＡＰＤＵを受信すると、デコーダ１２０は、提供されたオフセットと長さ値を利用するＩＳＯＢＭＦＦファイルから要請されたデータを抽出できる。コンテンツがＩＰパケットとして送信されている場合以外には、デコーダ１２０は、図１１に示すｄａｔａ＿ｒｓｐ（）ＡＰＤＵからデータを受信制限モジュール１３０にリターンする。この場合には、デコーダ１２０は、サーバから受信されたものとしてＩＰパケットの要請されたデータを送信できる。
【０１１１】
本発明の実施の形態において要請されたデータの位置はオフセット及び長さ値を使用して表示されるが、他の実施の形態において他の方法が用いられることができる。
【０１１２】
図１１は、図１０のデータ要請メッセージに対応して送信されたデータ応答メッセージのシンタックスを示す図である。図１１に示すように、ｄａｔａ＿ｒｓｐ（）ＡＰＤＵの

ペイロードは、ｓｔａｔｕｓ　ｆｉｅｌｄ、ｄａｔａ＿ｌｅｎｇｔｈ　ｆｉｅｌｄ及びｄａｔａ　ｆｉｅｌｄを含む。Ｓｔａｔｕｓは、要請されたデータが成功的に検索されたかどうかを示すのに用いられる８ビットフィールドである。ｓｔａｕｔｓが０の場合、要請されたデータが発見され、データがｄａｔａ＿ｒｓｐメッセージに含まれたことを示す。ｓｔａｔｕｓが１の場合、これは、要請されたデータが発見されないことを示す。ｓｔａｔｕｓが２の場合には、これは、要請されたデータが発見され、ＩＰパケットが送信されることを示す。２は、データがＩＰパケットでデコーダから本来受信された場合、雄一の有効な値である。

【０１１３】

Ｄａｔａ＿ｌｅｎｇｔｈは、リターンされるデータのバイトの個数を格納する３２ビットフィールドである。ｄａｔａは、受信制限モジュール１３０により要請されたデータの１バイトを格納する８ビットフィールドである。ｄａｔａ＿ｒｓｐ（）ＡＰＤＵは、要求されたデータの全体部分の送信が要求されるほどの多くのデータフィールドを含むことができる。

【０１１４】

図１２は、本発明の一実施の形態にかかる、受信制限モジュール１３０から送信されたｐｓｓｈアップデート要請メッセージのシンタックスを示す図である。受信制限モジュール１３０は、いつでもｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰＤＵをデコーダ１２０に送信できる。

【０１１５】

ｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰＤＵは、それがデコーダ１２０の内部に格納される時、受信制限モジュール１３０がＩＳＯＢＭＦＦファイルにｐｓｓｈボックスをアップデートできるようにする。

【０１１６】

図１２に示すように、ｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰＤＵのペイロードは、ｐｓｓｈ＿ｄａｔａ（）フィールドを含む。ｐｓｓｈ＿ｄａｔａ（）フィールドは、任意の大きさを有しており、ｐｓｓｈボックスに記録されるデータを含む。本発明の実施の形態において、デコーダ１２０がローカル格納所でＩＳＯＢＭＦＦファイルを再生するか、又はローカル格納所にファイルを記録する場合、デコーダ１２０は、ｐｓｓｈボックスをＤＲＭの固有識別子（Ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ：ＵＵＩＤ）に取り替えることができる。特に、デコーダ１２０は、ｐｓｓｈボックスのＤＲＭ　ＵＵＩＤが一致しながら、ローカル格納所にあるＩＳＯＢＭＦＦファイルのバージョンにｐｓｓｈボックスが位置するようにする。そして、デコーダ１２０は、ファイルに格納されるボックスをｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰＤＵに提供されたボックスに取り替える。

【０１１７】

図１３は、図１２のｐｓｓｈアップデート要請メッセージに対応して送信されたｐｓｓｈアップデート応答メッセージのシンタックスを示す図である。図１３に示すように、ｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｓｐ（）ＡＰＤＵのペイロードは、８ビットのｓｔａｔｕｓ　ｆｉｅｌｄから構成される。ｆｉｅｌｄが０の場合には、これは、ｐｓｓｈボックスが成功的にアップデートしたことを示す。ｓｔａｔｕｓが１の場合、指定されないエラーが発生したことを示す。

【０１１８】

ｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）とｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｓｐ（）　ＡＰＤＵとは、受信制限モジュール１３０により提供されるデータとｐｓｓｈボックスをアップデートするためにデコーダ１２０を制御することによって、受信制限モジュール１３０がデコーダ１２０のＩＳＯＢＭＦＦファイルに記録できるようにすることができる。本発明の実施の形態においてｐｓｓｈボックスがアップデートされても、本発明は、これに限定されない。他の実施の形態において受信制限モジュール１３０は、ファイルの他の部分に記録できるようにデコーダを制御するために、ｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰ

ＤＵと似たＡＰＤＵを利用できる。一般的な記録要請命令の適切な例が図１４に示される。

【０１１９】

図１４は、本発明の一実施の形態にかかる、データ記録要請メッセージのシンタックスを示す図である。受信制限モジュール１３０がＩＳＯＢＭＦＦファイルのようにデコーダ１２０の内部に格納されたファイルに記録されるデータを有する場合、受信制限モジュール１３０は、制御インタフェース１７０を介してｗｒｉｔｅ＿ｒｅｑ（）ＡＰＤＵをデコーダ１２０に送信できる。記録されるファイルは、ハードディスクのようなローカル不揮発性格納装置に格納されるファイルであるか、又は一時的にメモリに格納されるファイルでありうる。図１４に示すように、ｗｒｉｔｅ＿ｒｅｑ（）ＡＰＤＵのペイロードは、６４ビットのｄａｔａ＿ｏｆｆｓｅｔｆｉｅｄｌ、３２ビットのｄａｔａ＿ｌｅｎｇｔｈ ｆｉｅｌｄ、及び８ビットのｄａｔａ ｆｉｅｌｄを含む。ｄａｔａ＿ｏｆｆｓｅｔとｄａｔａ＿ｌｅｎｇｔｈ ｆｉｅｌｄは、図１１に示すｄａｔａ＿ｒｅｑ（）ＡＰＤＵのｄａｔａ＿ｏｆｆｓｅｔとｄａｔａ＿ｌｅｎｇｔｈ ｆｉｅｌｄと似た方式で、ファイル内に記録されるデータの位置を定義するのに用いられる。受信制限モジュール１３０は、デコーダ１２０にあるファイルに対する長さのデータを作成するｗｒｉｔｅ＿ｒｅｑ（）ＡＰＤＵを使用することができる。制御インタフェース１７０を介して受信制限モジュール１３０からｗｒｉｔｅ＿ｒｅｑ（）ＡＰＤＵを受信すると、デコーダ１２０は、ｗｒｉｔｅ＿ｒｅｑ（）メッセージに含まれたデータをファイルに記録しようと試みる。データが成功的に記録されたかどうかを受信制限モジュール１３０に通知するために、デコーダ１２０は、制御インタフェース１７０を介してデータ記録応答メッセージを受信制限モジュール１３０に送信できる。

【０１２０】

図１５は、図１４のデータ記録要請メッセージに対応して送信されたデータ記録応答メッセージのシンタックスを示す図である。図１５に示すように、ｗｒｉｔｅ＿ｒｓｐ（）ＡＰＤＵのペイロードは、８ビットのｓｔａｔｕｓ ｆｉｅｌｄから構成される。ｓｔａｔｕｓが０の場合、データが成功的にファイルに記録されたことを示す。ｓｔａｔｕｓが１の場合、特定されないエラーが発生したことを示す。

【０１２１】

図１６は、本発明の一実施の形態にかかる、トラック定義メッセージのシンタックスを示す図である。デコーダは、ビデオ又はオーディオトラックのようなメディアトラックに対するメッセージを受信制限モジュール１３０に通知するために使用することができる。メッセージは、ＴＳインタフェース１６０を介してトラックに関するメディアデータを受信することを予想するように、受信制限モジュール１３０に通知する。メッセージは、トラックを識別するのに用いられるトラック識別子ＩＤのようなトラックに対する情報を含むことができる。また、メッセージは、トラックに関連したＤＲＭ情報のようなＩＳＯＢＭＦＦファイルのｓｉｎｆ（）ボックスから受信された情報を含むことができる。ＤＲＭ情報は、該当トラックに対するＤＲＭシステムを設定するために、受信制限モジュール１３０により要求されることができる。

【０１２２】

デコーダ１２０が受信制限モジュール１３０にトラックに対するあるメディアデータを送信する前に、ｔｒａｃｋ＿ｄｅｆｎ（）ＡＰＤＵは、トラックに対するデータを期待する受信制限モジュール１３０に通知するために送信されうる。トラックは、コンテンツの再生中にいつでも定義されうる。トラック番号は、ＭＰ４ファイルの再生中に再度用いられることができない。すなわち、同じトラック番号は、常にＩＳＯＢＭＦＦファイルにおいて同じデータのトラックに用いられる。コンテンツがＩＰパケットからＴＳインタフェース１６０を介して受信制限モジュール１３０に送信される本発明の実施の形態では、このようなメッセージが省略されうる。

【０１２３】

図１６に示すように、ｔｒａｃｋ＿ｄｅｆｎ（）ＡＰＤＵのペイロードは、ｔｒａｃｋ

＿ＩＤ ｆｉｅｌｄとｓｉｎｆ＿ｄａｔａ（） ｆｉｅｌｄから構成される。Ｔｒａｃｋ＿ＩＤは、デコーダ１２０がＴＳインタフェース１６０を介して受信制限モジュール１３０に送信しようとするトラックのトラックＩＤのような、新しいトラックの値を格納する３２ビットフィールドである。Ｓｉｎｆ＿ｄａｔａ（）は、ある大きさを有することができ、トラックに対するｓｉｎｆ ｂｏｘを格納するのに用いられる。ｓｉｎｆ ｂｏｘは、ｍｏｏｖ ｂｏｘから抽出される。デコーダ１２０からｔｒａｃｋ＿ｄｅｆｎ（）ＡＰＤＵを受信すると、受信制限モジュール１３０は、図１７に示すｔｒａｃｋ＿ａｃｋ（）ＡＰＤＵとして応答できる。

【０１２４】

図１７は、図１６のトラック定義メッセージに対応して受信制限モジュール１３０から送信されたトラックアック（ｔｒａｃｋ＿ａｃｋ）メッセージのシンタックスを示す図である。図１７に示すように、ｔｒａｃｋ＿ａｃｋ（）ＡＰＤＬのペイロードは、８ビットのｓｔａｔｕｓ ｆｉｅｌｄから構成される。ｓｔｓｔｕｓが０の場合、これは、受信制限モジュール１３０が以前のｔｒａｃｋ＿ｄｅｆｎ（）ＡＰＤＵに定義されたトラックと関連したメディアデータを受信する準備ができたことを示す。ｓｔａｔｕｓが１の場合、これは、受信制限モジュール１３０が特定されないエラーによって準備していないことを示す。本発明の実施の形態において、デコーダ１２０は、受信制限モジュール１３０がデータを受信する準備ができたことを受信制限モジュール１３０から確認するまで、トラックと関連したすべてのメディアデータを送信しないことができる。

【０１２５】

図１８は、本発明の一実施の形態にかかる、終了メッセージのシンタックスを示す図である。デコーダ１２０は、受信制限モジュール１３０がファイルの終わりに到達して、もうこれ以上データがＴＳインタフェース１６０を介して送信されないことを示すために終了メッセージを使用する。例えば、デコーダ１２０がＩＳＯＢＭＦＦファイルのメディアサンプルを受信制限モジュール１３０に送信完了すると、デコーダ１２０は、受信制限モジュール１３０にｃｌｏｓｅ（）ＡＰＤＵを送信できる。ファイルの終わりに到達したりユーザがコンテンツを視聴するのを中止しようとする場合、デコーダ１２０は、ナル（ｎｕｌｌ）ＴＳパケットを送信するか、又はＴＳパケットを全く送信しなくても良い。

【０１２６】

図１８に示すように、ｃｌｏｓｅ（）ＡＰＤＵのペイロードは、１－ｂｉｔ ｉｍｍｅｄｉａｔｅ ｆｉｅｌｄ、予約された（ｒｅｓｅｒｖｅｄ）７ビットから構成される。ｉｍｍｅｄｉａｔｅ ｆｉｅｌｄが０の場合、受信制限モジュール１３０は、その内部バッファで保有になるメディアサンプルを処理し続けることができ、ＴＳインタフェース１６０を介してすべてのメディアデータが出力されると、デコーダ１２０にｃｌｏｓｅ＿ａｃｋ（）ＡＰＤＵとして応答できる。万一、ｉｍｍｅｄｉａｔｅ ｆｉｅｌｄが１の場合、受信制限モジュール１３０は、すべての復号化作業を取り消し、内部バッファのあるコンテンツデータをフラッシュ（ｆｌｕｓｈ）できる。この場合に、受信制限モジュール１３０は、ナルパケットを除き、装置にもうこれ以上のＴＳパケット又は他のパケットを送信しなくても良い。

【０１２７】

受信制限モジュール１３０があるメディアサンプルの内部バッファをフラッシュするか、又はあるメディアサンプルを含む最後のパケットを出力すると、ｃｌｏｓｅ＿ａｃｋメッセージは、デコーダ１２０に応答されうる。このとき、受信制限モジュール１３０は、「正常」作業、すなわち、暗号化されたデータが標準ＭＰＥＧ－２ ＴＳで受信される動作モードに戻すことができる。

【０１２８】

図１９は、図１８の終了メッセージに対応して受信制限モジュール１３０から送信された終了アック（ｃｌｏｓｅ＿ａｃｋ）メッセージのシンタックスを示す図である。図１９に示すように、ｃｌｏｓｅ＿ａｃｋ（）ＡＰＤＬのペイロードは、８ビットのｓｔａｔｕｓ ｆｉｅｌｄから構成される。ｓｔａｔｕｓが０の場合、これは、受信制限モジュール

１３０が成功的に作業を完了したことを示す。ｓｔａｔｕｓが１の場合、特定されないエラーが発生したことを示す。デコーダ１２０が受信制限モジュール１３０からｃｌｏｓｅ＿ａｃｋメッセージを受信した場合、他のＩＳＯＢＭＦＦファイルを再生するためにｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵを受信すると共に新しい作業を始めたり、受信制限モジュール１３０にブロードキャスト（ｂｒｏａｄｃａｓｔ）ＴＳをルーチングできる。

【０１２９】

以下、本発明の一実施の形態にかかる、デコーダ１２０と受信制限モジュール１３０の順次的な作業について説明する。第１に、暗号化されたコンテンツは、デコーダ１２０のローカル格納装置にＩＳＯＢＭＦＦファイルとしてダウンロードされる。次に、ユーザは、コンテンツを視聴するために入力された暗号化されたコンテンツが再生される命令を入力する。ユーザ命令に対する応答として、デコーダ１２０は、新しいＳＡＳリソースをオープンし、受信制限モジュール１３０に如何なるＴＳパケットを送信することを中断する。本発明の実施の形態において、デコーダ１２０は、ＩＳＯＢＭＦＦファイルのパッシングを開始し、ｐｓｓｈボックスをすべて抽出する。デコーダ１２０は、受信制限モジュール１３０にｐｓｓｈデータと００に設定されたｃｏｎｔｅｎｔ＿ｆｏｒｍａｔと共にｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵを送信する。これに対する応答として、受信制限モジュール１３０は、ｐｓｓｈボックスを検査し、受信制限モジュール１３０にてＤＲＭに対した正確なボックスをマッチングさせる。この時点において、受信制限モジュール１３０は、ライセンスを取得したりユーザ権限を確認したりするために、ＣＩ ｐｌｕｓで定義されたＤＲＭ低速通信（ｌｏｗ ｓｐｅｅｄ ｃｏｍｍｕｎｉｃａｔｉｏｎｓ：ＬＳＣ）を使用することができる。また、受信制限モジュール１３０は、ＤＲＭ及び／又は暗号化メタデータの確認のためのより多くのデータを要請するために、デコーダ１２０にｄａｔａ＿ｒｅｑ（）ＡＰＤＵを送信することができる。

【０１３０】

受信制限モジュール１３０がデコーダ１２０にて暗号化されたデータを受信する準備が完了すると、受信制限モジュール１３０は、ｉｎｉｔ＿ａｃｋ（）ＡＰＤＵをデコーダ１２０に送信し、新しいｐｓｓｈボックスと共にｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰＤＵを送信する。デコーダ１２０は、ｐｓｓｈ＿ｕｐｄａｔｅ＿ｒｅｑ（）ＡＰＤＵを受信し、ダウンロードされたファイルにおけるｐｓｓｈボックスをアップデートする。一つが現れる場合、これは、ｆｒｅｅ ｂｏｘの修正を要求できる。次に、デコーダ１２０は、ＩＳＯＢＭＦＦファイルをパッシングし続け、トラックが暗号化されることを発見する。各々の暗号化されたトラックに対して、ｔｒａｃｋ＿ｄｅｆｎ（）ＡＰＤＵは、トラックに対するｓｉｎｆボックスと共に受信制限モジュール１３０に送信される。各々の受信されたｔｒａｃｋ＿ｄｅｆｎ（）ＡＰＤＵに対して、受信制限モジュール１３０は、各々のトラックに対するＡＰＤＵｔｒａｃｋ＿ａｃｋ（）を送信する。その後、デコーダ１２０は、ＩＳＯＢＭＦＦファイルから暗号化されたメディアサンプルの抽出を開始し、メディアサンプルパケットから抽出されたものを受信制限モジュール１３０に送信する。本発明の実施の形態において、受信制限モジュール１３０は、メディアサンプルを復号化するためにメディアサンプルパケットで暗号化情報を用い、復号化されたメディアサンプルパケットをデコーダ１２０に返還する。

【０１３１】

最後に、ユーザがコンテンツを視聴することを終了すると、もうこれ以上受信制限モジュール１３０に送信する暗号化されたメディアサンプルが存在しない。この時点で、デコーダ１２０は、受信制限モジュール１３０にｃｌｏｓｅ（）ＡＰＤＵを送信し、それに対する応答としてｃｌｏｓｅ＿ａｃｋ（）ＡＰＤＵを受信する。

【０１３２】

図２０は、本発明の一実施の形態にかかる、ＴＳインタフェース１６０を介して受信制限モジュール１３０に暗号化されたデータを送信する方法を説明するためのフローチャートである。以下で説明される方法は、図１Ａ及び図１Ｂのデコーダ１２０のようなデコー

ダが利用されうる。

【０１３３】

まず、デコーダ１２０は、ＴＳインタフェース１６０を介して受信制限モジュール１２０に送信される暗号化されたデータを含む複数のデータパケットを生成する（Ｓ２００１）。例えば、デコーダ１２０がデータサンプル及び暗号化情報を抽出するためにファイルをパッシングする場合、暗号化されたデータは、ＩＳＯＢＭＦＦファイルでありえ、ファイルのパッシングが必要でない場合、暗号化されたデータを送信できる。各々のデータパケットは、ヘッダ及び暗号化されたデータ領域を含む。例えば、データパケットは、図２に示すように、ＩＰパケットで暗号化されたデータを含むカプセル化されたＩＰパケットでありうる。大体的に、データパケットは、図３に示すように、ペイロードがｍｓ＿ｄａｔａ（）ファイルを保有しているメディアサンプルパケットでありえ、図４に示すように、ｍｓ＿ｄａｔａ（）ファイルの領域を保有するＭＰＥＧ－２　ＴＳパケットでありうる。さらに他の実施の形態もやはり可能である。暗号化されたデータを複数のデータパケットにパケット化することによって、ＭＰＥＧ－２　ＴＳフォーマットと異なるフォーマットの暗号化されたデータをＴＳインタフェース１６０を介して受信制限モジュール１３０に送信されうる。

【０１３４】

そして、複数のデータパケットは、ＴＳインタフェース１６０を介して受信制限モジュール１３０に送信される（Ｓ２００２）。受信制限モジュール１３０は、データを復号化し、ＴＳインタフェース１６０を介して復号化されたデータをデコーダ１２０に再度送信する。

【０１３５】

図２１は、本発明の一実施の形態にかかる、複数のカプセル化されたＩＰパケットを生成する方法を説明するためのフローチャートである。以下で説明される方法は、図２に開示されたデータ構造が利用されうる。

【０１３６】

まず、暗号化されたデータは、複数のＩＰパケットとしてコンテンツ提供者から受信される（Ｓ２１０１）。このとき、本発明の一実施の形態では、暗号化されたデータは、ＩＳＯＢＭＦＦファイルに含まれうる。

【０１３７】

そして、デコーダ１２０は、カプセル化されたＩＰを生成するために各々のＩＰパケットにヘッダを付加する（Ｓ２１０２）。各々のカプセル化されたＩＰパケットは、やはり図２に示したようなヘッダに先立ってｓｙｎｃ　ｂｙｔｅを含むことができる。

【０１３８】

そして、複数のカプセル化されたＩＰパケットは、ＴＳインタフェース１６０を介して受信制限モジュール１３０に送信される（Ｓ２１０３）。受信制限モジュール１３０は、カプセル化されたＩＰパケットを受信することができ、ＩＰパケットを抽出し、ＩＳＯＢＭＦＦファイルの暗号化されたデータを復号化するために、本来のＩＳＯＢＭＦＦファイルに復旧できる。

【０１３９】

図２２は、本発明の一実施の形態にかかる、データサンプルを維持するために複数のメディアサンプルパケット及びＩＳＯＢＭＦＦファイルから抽出された暗号化メタデータを生成するためのフローチャートである。以下で説明する方法は、図３に示すようなデータ構造を利用できる。

【０１４０】

まず、デコーダ１２０は、コンテンツ提供者１１０から暗号化されたマルチメディアデータの含まれたＩＳＯＢＭＦＦファイルを受信する（Ｓ２２０１）。本発明の一実施の形態において、暗号化されたデータは、ＩＳＯＢＭＦＦファイルに格納されるか、又は他の実施の形態では、他のフォーマットが利用されうる。

【０１４１】

そして、デコーダ１２０は、複数のデータサンプル及び各々のデータサンプルと関連した暗号化メタデータを抽出するために、ＩＳＯＢＭＦＦファイルをパッシングする（Ｓ２２０２）。

【０１４２】

そして、デコーダ１２０は、データサンプル及び関連したメタデータを格納するための少なくとも一つのｍｓ＿ｄａｔａ（）構造を生成する（Ｓ２２０３）。このとき、各々のｍｓ＿ｄａｔａ（）は、少なくとも一つのデータサンプルを保有する。

【０１４３】

そして、デコーダ１２０は、図３に示すような構造を有する複数のメディアサンプルパケットを生成するために、各々のｍｓ＿ｄａｔａ（）にヘッダ及びｓｙｎｃｂｉｔｅを付加する（Ｓ２２０４）。このとき、デコーダ１２０は、ＴＳインタフェース１６０を介して受信制限モジュール１３０にメディアサンプルパケットを送信する。受信制限モジュール１３０は、関連した暗号化メタデータを利用して各々のｍｓ＿ｄａｔａ（）に含まれた暗号化されたデータサンプルを復号化し、復号化されたデータをデコーダ１２０に再度送信する。

【０１４４】

図２３は、本発明の一実施の形態にかかる、データサンプルを維持するために複数のＭＰＥＧ－２　ＴＳパケット及びＩＳＯＢＭＦＦファイルから抽出された暗号化メタデータを生成するためのフローチャートである。以下で説明する方法は、図４に示すデータ構造が利用されうる。

【０１４５】

まず、デコーダ１２０は、コンテンツ提供者１１０から暗号化されたマルチメディアデータの含まれたＩＳＯＢＭＦＦファイルを受信する（Ｓ２３０１）。本発明の一実施の形態では、暗号化されたデータがＩＳＯＢＭＦＦファイルに格納されうるが、他の実施の形態では、他のフォーマットが利用されうる。

【０１４６】

そして、デコーダ１２０は、複数のデータパケット及び各々のデータパケットと関連した暗号化メタデータを抽出するために、ＩＳＯＢＭＦＦファイルをパッシングする（Ｓ２３０２）。

【０１４７】

そして、デコーダ２３０は、データサンプル及び関連したメタデータを格納するための少なくとも一つのｍｓ＿ｄａｔａ（）構造を生成する（Ｓ２３０３）。このとき、各々のｍｓ＿ｄａｔａ（）構造は、少なくとも一つのデータサンプルを保有する。

【０１４８】

そして、デコーダ１２０は、各々のｍｓ＿ｄａｔａ（）を複数のＭＰＥＧ－２　ＴＳパケットに挿入する（Ｓ２４０４）。そして、デコーダは、ＭＰＥＧ－２　ＴＳパケットをＴＳインタフェース１６０を介して受信制限モジュール１３０に送信する。受信制限モジュール１３０は、ＴＳパケットを受信し、ｍｓ＿ｄａｔａ（）を復旧し、関連した暗号化メタデータを利用して各々のｍｓ＿ｄａｔａ（）の暗号化されたデータサンプルを復号化し、復号化されたデータをデコーダ１２０に再度送信する。

【０１４９】

以上、マルチメディアデータを受信しデコードするためにデコーダが説明されたが、他の実施の形態では、デコーダでない他の装置が利用されうる。例えば、装置は、コンテンツ提供者、又は内部の格納装置から暗号化されたマルチメディアデータを受信し、暗号化されたデータを共通インタフェースを介して受信制限モジュールに送信できる。装置が復号化されたデータをデコードする代わりに、装置は、受信制限モジュールから復号化されたデータを受信し、別途のデコーダに復号化されたデータを送信できる。

【０１５０】

また、本発明の多様な実施の形態において多様なＡＰＤＵ構造が説明されたが、本発明は、このような制御メッセージ構造に制限されるものではない。他の実施の形態では、任

意のフィールドが省略されえ、要求される特定メッセージにより他のフィールドが追加されうる。例えば、ｉｎｉｔｉａｌｉｓａｔｉｏｎ（）ＡＰＤＵと関連して、ｃｏｎｔｅｎｔ＿ｆｏｒｍａｔフィールドは省略されうる。同様に、図２、図３及び図４のデータパケット構造と関連して、本発明は、このような構造の使用に限定されるものではない。例えば、ｍｓ＿ｄａｔａ（）構造において、ｅｎｃｒｙｐｔｉｏｎ＿ｉｎｆｏｒｍａｔｉｏｎ及びｓａｍｐｌｅ＿ｄａｔａフィールドの代わりに他のフィールドが含まれうる。説明された実施の形態において、ｍｓ＿ｄａｔａ（）構造は、ＩＳＯＢＭＦＦファイルのｍｄａｔボックスからメディアデータサンプルを送信するのに用いられるが、ｍｓ＿ｄａｔａ（）構造は、またＩＳＯＢＭＦＦファイルから他のデータを送信するのに用いられうる。コンテンツが内部格納装置にダウンロードされる本発明の実施の形態において、ダウンロードされるコンテンツは、ＨｂｂＴＶ又はＭＨＰアプリケーションのようなネイティブ応用プログラム（ｎａｔｉｖｅ　ａｐｐｌｉｃａｔｉｏｎ）やインターアクティブ応用プログラム（ｉｎｔｅｒａｃｔｉｖｅ　ａｐｐｌｉｃａｔｉｏｎ）により再生されうる。コンテンツがプログレシブダウンロード方式、適応ストリーミング又はコンテンツストリーミング方式により提供される実施の形態において、コンテンツは、インターアクティブ応用プログラムの制御下で再生されうる。ある実施の形態では、ユーザは、例えば、早送り又は巻き戻しの選択により、コンテンツのトリック（Ｔｒｉｃｋ）プレーを要請できる。制御応用プログラムは、ＤＲＭがデコーダ又は外部受信制限モジュールに内蔵される機能により具現化されているかどうかが分かる必要はない。

【０１５１】

制御応用プログラムがネイティブプレーヤーにコンテンツ再生の開始を要請する場合、ネイティブプレーヤーは、遠隔ストリーミングサーバのような、コンテンツソースからデータを要請する。また、ネイティブプレーヤーは、受信制限モジュールとの接続を初期化する。マルチメディアコンテンツが複数のＩＰパケットとして受信される実施の形態に対して、遠隔サーバから受信されるＩＰパケットは、デコーダのＩＰスタックにより処理される前に、受信制限モジュールを介してルートされる。そして、デコーダは、暗号化されないＩＳＯＢＭＦＦファイルをパッシングしデコードする。デコーダがＩＳＯＢＭＦＦファイルをパッシングする実施の形態では、ネイティブプレーヤーがトラック情報を抽出できるようにするために、ＩＳＯＢＭＦＦファイルが十分にパッシングされると、復号化されなければならないトラックを受信制限モジュールに通知し、ＴＳインタフェースを介してコンテンツのストリーミングを開始する。

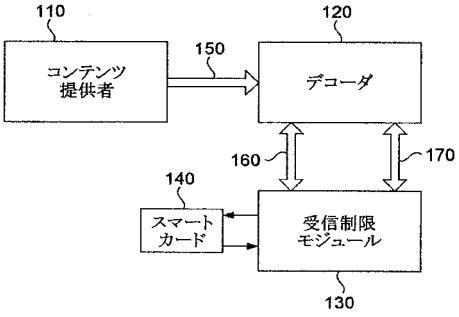
【０１５２】

また、本発明の実施の形態は、ＩＳＯＢＭＦＦファイルに関連して説明されているが、本発明は、上述したＩＳＯＢＭＦＦフォーマットに限定されない。本発明の他の実施の形態では、デジタルビデオ放送（ｄｉｇｉｔａｌ　ｖｉｄｅｏ　ｂｒｏａｄｃａｓｔｉｎｇ：ＤＶＢ）標準、オープンＩＰＴＶフォーラム（Ｏｐｅｎ　ＩＰＴＶ　Ｆｏｒｕｍ：ＯＩＰＦ）標準、又はデジタルエンターテインメント・コンテンツエコシステム（Ｄｉｇｉｔａｌ　Ｅｎｔｅｒｔａｉｎｍｅｎｔ　Ｃｏｎｔｅｎｔｓ　Ｅｃｏ　ｓｙｓｔｅｍ：ＤＥＣＥ）標準のような規格が適用されうる。

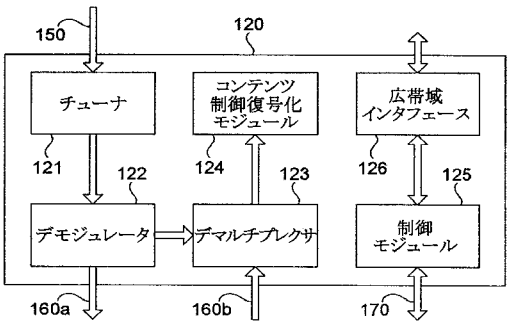
【０１５３】

以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明は以上の実施形態に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的趣旨の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

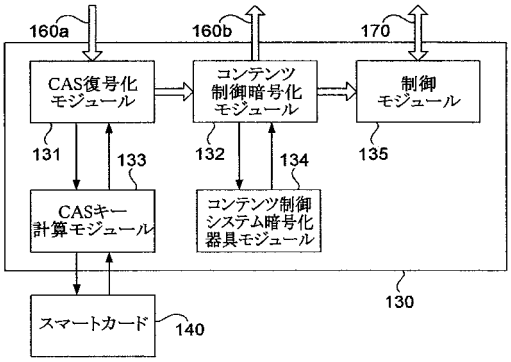
【図１Ａ】



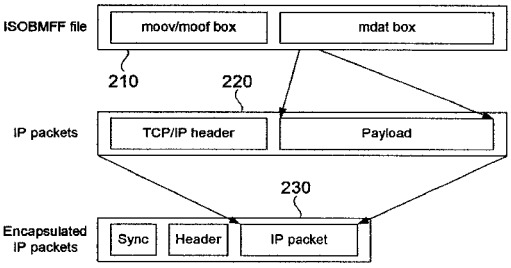
【図１Ｂ】



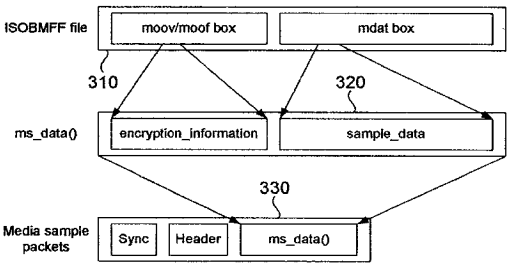
【図１Ｃ】



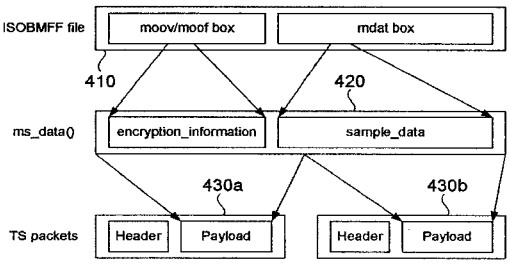
【図２】



【図３】



【図４】



【図５】

Syntax	No. of Bits	Mnemonic
ms_data() {		
track_id	32	uimsbf
number_of_samples	8	uimsbf
for (i=0; i<number_of_samples; i++) {		
AlgorithmID	24	uimsbf
IV_size	8	uimsbf
KID	16*8	uimsbf
auxiliary_sample_size	8	uimsbf
for (i=0; i<auxiliary_sample_size; i++) {		
auxiliary_sample_data	8	uimsbf
}		
}		
for (i=0; i<number_of_samples; i++) {		
sample_length	32	uimsbf
for (i=0; i<sample_length; i++) {		
sample_data	8	uimsbf
}		
}		
}		

【図６】

Syntax	No. of Bits	Mnemonic
message() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
payload()		
}		

【図７】

Command	command_id	Direction
RESERVED	0x00	
INITIALISATION	0x01	D ⟶ C
INIT_RSP	0x02	C ⟶ D
DATA_REQ	0x03	C ⟶ D
DATA_RSP	0x04	D ⟶ C
TRACK_DEFN	0x05	D ⟶ C
TRACK_RSP	0x06	C ⟶ D
CLOSE	0x07	D ⟶ C
CLOSE_RSP	0x08	C ⟶ D
PSSH_UPDATE_REQ	0x09	C ⟶ D
PSSH_UPDATE_RSP	0x0A	D ⟶ C
WRITE_REQ	0x0B	C ⟶ D
WRITE_RSP	0x0C	D ⟶ C

【図８】

Syntax	No. of Bits	Mnemonic
initialisation() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
reserved	1	bslbf
content_format	2	bslbf
ts_packet_pid	13	uimsbf
pssh_count	8	uimsbf
for (i=0; i<pssh_count; i++) {		
pssh_data()		
}		
}		

【図９】

Syntax	No. of Bits	Mnemonic
init_ack() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
status	8	uimsbf
}		

【図１０】

Syntax	No. of Bits	Mnemonic
data_req() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
data_offset	64	uimsbf
data_length	32	uimsbf
}		

【図１１】

Syntax	No. of Bits	Mnemonic
data_rsp() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
status	8	uimsbf
if (status == 0) {		
data_length	32	uimsbf
for (i=0; i<data_length; i++) {		
data	8	uimsbf
}		
}		
}		

【図１２】

Syntax	No. of Bits	Mnemonic
pssh_update_req() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
pssh_data()		
}		

【図１３】

Syntax	No. of Bits	Mnemonic
pssh_update_rsp() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
status	8	uimsbf
}		

【図１４】

Syntax	No. of Bits	Mnemonic
write_req() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
data_offset	64	uimsbf
data_length	32	uimsbf
for (i=0; i<data_length; i++) {		
data	8	uimsbf
}		
}		

【図１５】

Syntax	No. of Bits	Mnemonic
write_rsp() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
status	8	uimsbf
}		

【図１６】

Syntax	No. of Bits	Mnemonic
track_defn() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
track_ID	32	uimsbf
sinf_data()		
}		

【図１７】

Syntax	No. of Bits	Mnemonic
track_ack() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
status	8	uimsbf
}		

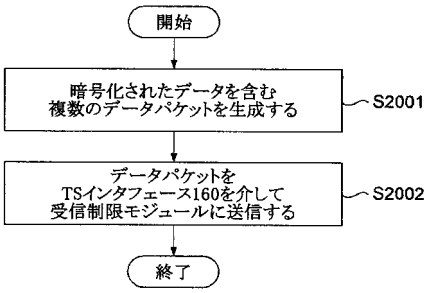
【図１８】

Syntax	No. of Bits	Mnemonic
close() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
immediate	1	bslbf
reserved	7	bslbf
}		

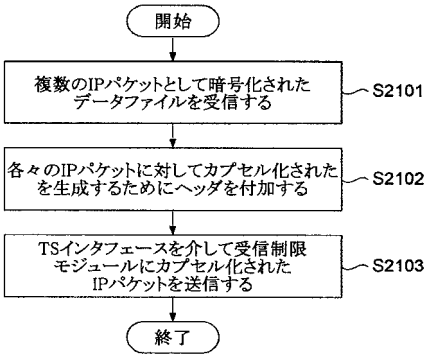
【図１９】

Syntax	No. of Bits	Mnemonic
close_ack() {		
command_id	8	uimsbf
transaction_id	32	uimsbf
status	8	uimsbf
}		

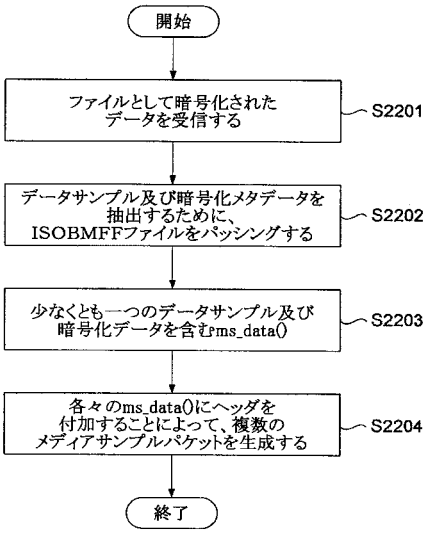
【図２０】



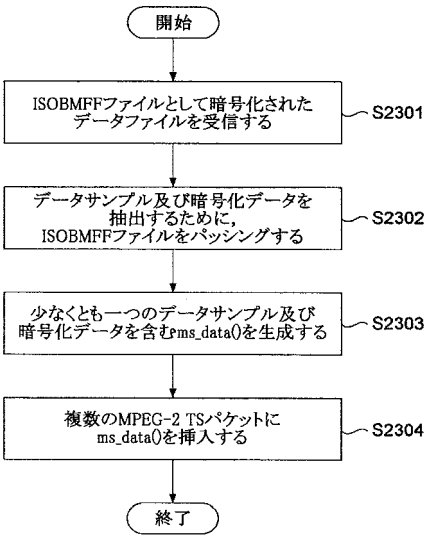
【図２１】



【図２２】



【図２３】



フロントページの続き

(72)発明者　アーサー　サイモン　ウォーラー
イギリス国　ミドルセックス　ティーダブリュー１８　４キューイー　ステインズ　サウスストリート　コミュニケーションズ・ハウス

Ｆターム(参考) 5K030 GA15 HB11 JA05
5K034 AA05 CC02 DD02 EE11 FF02 GG03 HH12 HH13 HH61 KK27