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

特許第4098348号
(P4098348)

(45)発行日　平成20年6月11日(2008.6.11)　(24)登録日　平成20年3月21日(2008.3.21)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04N	7/167	(2006.01)	H04N	7/167	Z
H04N	7/173	(2006.01)	H04N	7/173	630
G06F	21/24	(2006.01)	H04N	7/173	610Z
			G06F	12/14	520F

請求項の数 11　(全 33 頁)　最終頁に続く

(21)出願番号　特願2007-195812(P2007-195812)
(22)出願日　平成19年7月27日(2007.7.27)
(65)公開番号　特開2008-54308(P2008-54308A)
(43)公開日　平成20年3月6日(2008.3.6)
審査請求日　平成20年1月23日(2008.1.23)
(31)優先権主張番号　特願2006-205271(P2006-205271)
(32)優先日　平成18年7月27日(2006.7.27)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109210
弁理士　新居　広守
(72)発明者　岡本　隆一
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　東　吾紀男
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　村上　弘規
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】端末装置、サーバ装置及びコンテンツ配信システム

(57)【特許請求の範囲】
【請求項１】
サーバ装置と端末装置を有するコンテンツ配信システムにおける端末装置であって、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、
前記暗号化コンテンツの利用を制御するコンテンツ利用制御部とを備え、
前記受信部が受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とする端末装置。
【請求項２】
サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置であって、

コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出部と、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部を備え、
前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするサーバ装置。

【請求項３】
暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成装置であって、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、
前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするコンテンツ関連情報生成装置。

【請求項４】
サーバ装置と端末装置を有するコンテンツ配信システムであって、
前記サーバ装置は、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出部と、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部を備え、
前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定し、
前記端末装置は、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、
前記暗号化コンテンツの利用を制御するコンテンツ利用制御部とを備え、
前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテン

ツ関連情報は正しくないと判定し、
前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とするコンテンツ配信システム。
【請求項５】
サーバ装置と端末装置を有するコンテンツ配信システムにおけるコンテンツ利用方法であって、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信ステップと、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証ステップと、
前記暗号化コンテンツの利用を制限するコンテンツ利用制御ステップとを含み、
前記受信ステップが受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証ステップは、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御ステップは、前記コンテンツ関連情報検証ステップが前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とするコンテンツ利用方法。
【請求項６】
サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置からのデータ送出方法であって、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出ステップと、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化ステップを含み、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするデータ送出方法。
【請求項７】
暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成装置におけるコンテンツ関連情報生成方法であって、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化ステップとを含み、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の

日時を示す前記送出日時情報を設定する
ことを特徴とするコンテンツ関連情報生成方法。
【請求項８】
サーバ装置と端末装置を有するコンテンツ配信システムにおけるコンテンツ利用方法をコンピュータに実行させるためのプログラムであって、
前記プログラムは、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信ステップと、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証ステップと、
前記暗号化コンテンツの利用を制御するコンテンツ利用制御ステップとを含み、
前記受信ステップが受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証ステップは、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御ステップは、前記コンテンツ関連情報検証ステップが前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とするプログラム。
【請求項９】
サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置からのデータ送出方法をコンピュータに実行させるためのプログラムであって、
前記プログラムは、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出ステップと、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化ステップを含み、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするプログラム。
【請求項１０】
暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成方法をコンピュータに実行させるためのプログラムであって、
前記プログラムは、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、

前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロックに、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするプログラム。
【請求項１１】
サーバ装置と端末装置を有するコンテンツ配信システムにおける端末装置のための集積回路であって、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、
前記暗号化コンテンツの利用を制限するコンテンツ利用制御部とを備え、
前記受信部が受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とする集積回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを用いて、映像、音楽などのデジタルコンテンツを配信するコンテンツ配信システムに関し、特に、デジタルコンテンツとその復号鍵とを配信するサーバ装置と、復号鍵を用いてデジタルコンテンツを利用する端末装置に関する。
【背景技術】
【０００２】
近年、音楽、映像又はゲーム等のデジタルコンテンツ（以下、単に「コンテンツ」と記す。）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能な「コンテンツ配信システム」と呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。この「著作権保護技術」とは、具体的には、暗号技術等を用いてコンテンツの利用をセキュアに制御する技術である。
【０００３】
例えば、有料放送においては、映像信号及び音声信号等にスクランブルをかけて送出し、視聴権を有する端末装置のみがスクランブルを解いて視聴するというスクランブル制御方式が採用されている。
【０００４】
上記従来のスクランブル制御方式については、非特許文献１及び非特許文献２にその内容が開示されている。
【０００５】
従来のスクランブル制御方式においては、個別情報と番組情報（以降、本発明では「コンテンツ関連情報」と記す。）と呼ばれる２種類の情報を利用している。個別情報は、各受信者別の視聴契約を示す情報であり、契約内容、その契約の有効期限、後で送られてくるコンテンツ関連情報を解読するために必要となるワーク鍵などを含む。コンテンツ関連情報は、スクランブルされた映像信号及び音声信号等と並行して送られる情報であり、それらの信号をデスクランブルするために必要となるスクランブル鍵、その瞬間の現在時刻、番組内容などを含んでいる。

【０００６】
コンテンツの配信を受ける端末装置は、コンテンツ関連情報の受信に先立ち、自分宛の個別情報を受信し、その内容を契約情報として保持する。番組視聴時には、映像信号及び音声信号等と共にコンテンツ関連情報を受信し、コンテンツ関連情報に含まれる現在時刻と契約の有効期限との照合を行い、契約が有効期限内であるか期限切れであるかを調べる。期限切れであれば「視聴権なし」と判定する。有効期限内であれば、番組内容と契約内容とを照合して視聴権の有無を調べる。ここで、「視聴権あり」と判定された場合に限り、スクランブル鍵を取り出して映像信号及び音声信号等をデスクランブルする。
【０００７】
このように、従来のスクランブル制御方式においては、コンテンツと共に送信されてくる現在時刻に基づいて、契約の有効期限判定を行っている。
【非特許文献１】電気通信技術審議会答申の諮問第１７号（昭和６３年：衛星放送によるテレビジョン放送における有料方式に関する技術的条件）
【非特許文献２】電気通信技術審議会答申の諮問第７４号（平成７年：デジタル放送方式に係る技術的条件の一部答申）
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、コンテンツの配信を受ける端末装置は、コンテンツ及びコンテンツと共に送出されるコンテンツ関連情報を、必ずしも送出直後に受信するとは限らない。例えば、図１８に示すように、ユーザが蓄積装置１００等を用いて、コンテンツ及びコンテンツと共に送出されるコンテンツ関連情報を一旦蓄積し、それを後日、端末装置１０３０に再送信するということ等が考えられる。この場合、端末装置１０３０がコンテンツ及びコンテンツ関連情報を受信する時刻は、コンテンツ関連情報に含まれる現在時刻とは異なる時刻となる。このため、従来の方式では、本来は有効期限が切れているにもかかわらず、有効期限内であると判定してしまう可能性がある。また、コンテンツ及びコンテンツ関連情報が何度も再送信された場合には、端末装置１０３０は、再送信される度に、何度でもコンテンツの利用を許可してしまう可能性がある。また、有効期限判定等を正しく行うためには、コンテンツ関連情報に含まれる現在時刻等が改竄されていないことが必要である。また、端末装置１０３０では、受信したコンテンツ関連情報の完全性を検証することが必要となるが、この処理はコンテンツ復号の合間に行われるため、負荷の小さい処理とすることが必要である。
【０００９】
本発明は、上記従来の課題に鑑みてなされたものであり、コンテンツが一旦蓄積されることによる有効期限外のコンテンツの利用を回避し得るコンテンツ配信システム等を提供することを第１の目的とする。
【００１０】
さらに、本発明は、上記目的に加え、コンテンツ関連情報の完全性についての検証を処理負荷の小さい方法で行うことが可能なコンテンツ配信システム等を提供することを第２の目的とする。
【課題を解決するための手段】
【００１１】
上記課題を解決するために、本発明に係る端末装置は、サーバ装置と端末装置を有するコンテンツ配信システムにおける端末装置であって、前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、前記暗号化コンテンツの利用を制限するコンテンツ利用制御部とを備え、前記受信部が受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、

前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限することを特徴とする。

【００１２】

また、本発明に係るサーバ装置は、サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置であって、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出部と、前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定することを特徴とする。

【００１３】

また、本発明に係るコンテンツ関連情報生成装置は、暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成装置であって、前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定することを特徴とする。

【００１４】

なお、本発明は、上記端末装置又は上記サーバ装置における特徴的な構成手段をステップとするコンテンツ利用方法若しくは関連情報生成方法、又は集積回路として実現したり、上記方法の各々のステップをコンピュータ等に実行させるプログラムとして実現することもできる。そして、そのプログラムをＤＶＤ等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは云うまでもない。

【００１５】

さらに、本発明は、上記端末装置とサーバ装置とを有するコンテンツ配信システムとして実現することもできる。

【発明の効果】

【００１６】

本発明によれば、コンテンツ及びコンテンツ関連情報を、事業者が送出した直後に受信した場合にのみ、コンテンツの利用を許可するコンテンツ配信システムを提供することが可能となる。

【００１７】

また、本発明によれば、コンテンツ関連情報の完全性検証を、コンテンツ関連情報を従来のＣＢＣモードでの復号処理と復号後の情報を比較する処理とで実現し、ハッシュ値計算などの負荷の大きい処理や、従来のＣＢＣモードとは異なる特別な復号処理を行うことなく実施することが可能となる。

【発明を実施するための最良の形態】

【００１８】

以下、本発明に係る実施の形態について、図面を参照しながら説明する。なお、本発明について、以下の実施の形態及び添付の図面を用いて説明を行うが、これは例示を目的と

しており、本発明がこれらに限定されることを意図しない。

【００１９】

図１は、本発明におけるコンテンツ配信システム１の全体構成を示す図である。

【００２０】

図１において、コンテンツ配信システム１は、ライセンスサーバ１０１、コンテンツサーバ１０２、複数の端末装置１０３及び伝送媒体１０４を備えている。以下、コンテンツ配信システム１の各構成要素について説明を行う。

【００２１】

ライセンスサーバ１０１は、事業者α側に設置され、ユーザβのコンテンツに対する契約（利用権利）を管理し、端末装置１０３に対し、ユーザβの契約に関する情報（契約情報）などを含むライセンスを配信するサーバである。このライセンスがライセンスサーバ１０１から端末装置１０３に配信される際には、安全な認証チャネル（Secure Authenticated Channel：以下「ＳＡＣ」と記す。）を通じてセキュアに配信される。ＳＡＣとしては、例えば、ＳＳＬ（Secure Socket Layer）を用いることができる。なお、ライセンスの構成要素については、後で図を用いて詳細に説明する。

【００２２】

コンテンツサーバ１０２は、事業者α側に設置され、端末装置１０３に対し、暗号化されたコンテンツを配信するサーバである。コンテンツサーバ１０２が配信するコンテンツは、例えば、ＭＰＥＧ（Moving Picture Expert Group）－２　Ｓｙｓｔｅｍｓ（ＩＥＣ／ＩＳＯ１３８１８－１）で規定されるトランスポートストリーム（Transport Stream：以下「ＴＳ」と記す。）の形態を採用している。

【００２３】

端末装置１０３は、ユーザβ側に設置され、ライセンスサーバ１０１から配信されたライセンスを用いて、コンテンツサーバ１０２から配信されたコンテンツを利用する装置である。

【００２４】

伝送媒体１０４は、インターネット、ＣＡＴＶ（Cable Television）及び放送波等の有線伝送媒体又は無線伝送媒体、並びに可搬型記録媒体などであり、ライセンスサーバ１０１及びコンテンツサーバ１０２と、端末装置１０３との間をデータ交換可能に接続するものである。

【００２５】

なお、図２は、本実施の形態に係るコンテンツ配信システム１の概要を示すブロック図である。図２に示すように、コンテンツ配信システム１は、原則として、配信側のサーバ装置から暗号化コンテンツや暗号化ＥＣＭが配信された時刻とほぼ同時刻に受信した（これを「リアルタイム受信」という。）場合であって、契約が有効期限内の場合のみ、コンテンツの利用を可能とし、一旦、蓄積装置１００に蓄積され、「リアルタイム受信」以外の場合は、コンテンツの利用を認めないこととする。ここで、「リアルタイム受信」とは、配信時刻と受信時刻の差が、例えば「３０分以内」の場合をいう。

【００２６】

以上で、本実施の形態におけるコンテンツ配信システム１の全体構成に関する説明を終了する。次に、本実施の形態におけるコンテンツ配信システム１において配信されるコンテンツの暗号スキームについて、図３を用いて説明する。

【００２７】

図３において、暗号化された暗号化コンテンツや暗号化コンテンツを復号するための暗号鍵を送出する事業者α側と、暗号化コンテンツや暗号鍵を受信するユーザβ側に分けて説明する。

【００２８】

事業者α側において、コンテンツ２００は、スクランブル鍵Ｋｓ２０１と呼ばれる暗号鍵によってスクランブル（即ち、暗号化）される（２０２）。コンテンツのスクランブルについては、ＭＰＥＧ－２のＴＳパケット単位で、ＴＳパケットのペイロード部をスクラ

ンブルする。なお、このスクランブル鍵Ｋｓ２０１は、不正受信に対するセキュリティを向上させるため、数秒～数日などの頻度で変更される時変鍵である。

【００２９】

コンテンツ２００を暗号化するスクランブル鍵Ｋｓ２０１は、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵Ｋｗ２０３を用いて暗号化（２０４）される。ワーク鍵Ｋｗ２０３は、従来の一般的な限定受信方式で用いられているように、事業者単位、契約単位又はグループ単位などで割り当てられる暗号鍵であり、ワーク鍵Ｋｗ２０３自体のセキュリティを確保するため、１ヶ月～数年などの期間で更新されるのが一般的である。少なくともスクランブル鍵Ｋｓ２０１を含み、コンテンツ関連情報を送信するためのデータ構造は、ＥＣＭ（Entitlement Control Message）２２０と呼ばれ、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで規定されるプライベートセクションとして構成される。なお、このＥＣＭ２２０のデータ構造の例については、後で図を用いて詳細に説明する。

【００３０】

少なくとも、スクランブル鍵Ｋｓ２０１を含むＥＣＭ２２０を暗号化するワーク鍵Ｋｗ２０３は、コンテンツの利用に先立って事業者α側とユーザβ側とで共有しておく必要があるため、図３に示すように、ライセンス２３０に、暗号化されたワーク鍵Ｋｗ２０３を設定し、事業者α側からユーザβ側にＳＡＣを通じてライセンス２３０を配信することにより、両者で共有する。具体的には、事業者α側とユーザβ側でＳＡＣを確立した際に、両者でセッション鍵Ｋｓｅ２０５の共有化がなされるため、事業者α側では、セッション鍵Ｋｓｅ２０５を用いてライセンス２３０を暗号化（２０６）する。

【００３１】

なお、本暗号スキームで使用する暗号アルゴリズムとしては、ＡＥＳ（ＦＩＰＳ－１９７）などの共通鍵暗号方式が用いられるのが一般的である。

【００３２】

以上のように生成された暗号化コンテンツ及び暗号化されたＥＣＭ２２０は、ＭＰＥＧ－２　ＴＳパケット化され、必要に応じてＰＳＩ（Program Specific Information）／ＳＩ（Service　Information）などのデータと多重化（２０７）された後、ユーザβ側に送信される。

【００３３】

一方、ユーザβ側では、コンテンツ２００の利用に先立ち、事業者α側においてセッション鍵Ｋｓｅ２０５で暗号化（２０６）されて送出されたワーク鍵Ｋｗ２０３を含むライセンス２３０を受信し、ＳＡＣにより事業者α側と共有したセッション鍵Ｋｓｅ２０５を用いて、受信したライセンスを復号（２１１）し、ワーク鍵Ｋｗ２０３を取得する。

【００３４】

さらに、事業者α側から暗号化コンテンツなどを含むＭＰＥＧ－２　ＴＳパケットを受信すると、これらを分離（２１２）して、暗号化コンテンツ２１０、暗号化されたＥＣＭ２２０などを取得する。次に、取得済みのワーク鍵Ｋｗ２０３を用いて、暗号化されたＥＣＭ２２０を復号（２１３）し、スクランブル鍵Ｋｓ２０１を取得する。このとき、ユーザβ側では、ＥＣＭ２２０からスクランブル鍵Ｋｓ２０１を取得し、利用しても良いか否かの判定を行う。この判定処理については、後で図を用いて詳細に説明する。

【００３５】

次に、取得したスクランブル鍵Ｋｓ２０１を用いて暗号化コンテンツ２１０をデスクランブル（即ち、復号）（２１４）して、コンテンツを利用（視聴、書き出しなど）することが可能となる。

【００３６】

図４は、本実施の形態におけるライセンスサーバ１０１の機能構成を示すブロック図である。図４においてライセンスサーバ１０１は、ワーク鍵蓄積部３０１、契約情報蓄積部３０２、固有情報管理部３０３、ライセンス生成部３０４及びライセンス送信部３０５を備える。以下、各構成要素について説明を行う。

【００３７】

ワーク鍵蓄積部３０１は、例えば、ＲＡＭであり、ワーク鍵Ｋｗ２０３を蓄積する。ワーク鍵蓄積部３０１は、コンテンツ配信システム１内でワーク鍵Ｋｗ２０３を一意に特定可能な識別子及びワーク鍵送信開始日等と共にワーク鍵Ｋｗ２０３が蓄積されており、端末装置１０３に対して、どのワーク鍵Ｋｗ２０３を送信すれば良いかが特定可能となっているものとする。

【００３８】

契約情報蓄積部３０２は、本コンテンツ配信システム１を利用するユーザβが、コンテンツを利用するために必要となる契約情報を管理する。ここで、「契約情報」とは、例えば、ユーザβと端末装置１０３とを関連づける情報、ユーザβが契約したサービスを識別するための情報、並びに契約の開始期限及び契約の終了期限などを含む情報をいう。

【００３９】

固有情報管理部３０３は、例えば、制御プログラムを格納するＲＯＭ等を備えるマイクロコンピュータであり、ライセンスサーバ１０１全体の機能を制御する。さらに、固有情報管理部３０３は、ライセンスサーバ１０１固有の情報を管理し、端末装置１０３とのＳＡＣを確立するために必要なライセンスサーバ１０１の秘密鍵、及びライセンスサーバ１０１の公開鍵証明書等の固有の情報を保持する。

【００４０】

ライセンス生成部３０４は、端末装置１０３からの要求に応じて、端末装置１０３に配信するライセンス２３０を生成する。

【００４１】

ライセンス送信部３０５は、端末装置１０３との間でＳＡＣを確立し、端末装置１０３からの要求に対して、端末装置１０３にライセンス生成部３０４で生成されたライセンス２３０を送信する。

【００４２】

以上で、本実施の形態におけるライセンスサーバ１０１の全体構成に関する説明を終了する。

【００４３】

図５は、ライセンスサーバ１０１のライセンス生成部３０４によって生成されるライセンス２３０の一例を示す図である。図５に示すように、ライセンス２３０は、ワーク鍵Ｋｗ４０１、ワーク鍵ＩＤ４０２、契約コード４０３、開始日時４０４、終了日時４０５及び出力制御情報４０６から構成される。

【００４４】

ワーク鍵Ｋｗ４０１には、上記図３で示したワーク鍵Ｋｗ２０３が設定される。なお、ワーク鍵Ｋｗ２０３は定期的に更新される場合、ライセンス２３０内にワーク鍵Ｋｗ４０１として、現在のワーク鍵Ｋｗ２０３と更新後のワーク鍵Ｋｗ２０３を設定しておくことも可能である。ワーク鍵ＩＤ４０２には、ワーク鍵Ｋｗ４０１に設定されるワーク鍵Ｋｗ２０３を一意に特定するＩＤが設定される。契約コード４０３には、端末装置１０３を使用するユーザβにおける契約内容を示すコードが設定され、ティアビットとも呼ばれる。開始日時４０４には、ワーク鍵Ｋｗ４０１が利用可能となる開始期限が設定される。終了日時４０５には、ワーク鍵Ｋｗ４０１の利用が終了する期限が設定される。出力制御情報４０６には、コンテンツ利用時のデジタル出力、アナログ出力、リムーバブルメディア等の記録媒体への記録及び蓄積の制御に関する情報が設定され、例えば、デジタル／アナログのコピー制御情報（Copy Control Information：以降、「ＣＣＩ」と記す。）、アナログコピープロテクションシステム（Analog Copy Protection System）、ＥＰＮ（Encryption Plus Non-Assertion）、一時蓄積などに関する情報が設定される。コピー制御情報に設定される情報の具体例としては、例えば、「コピーを禁止する」、「１世代のみコピーを許可する」及び「コピーの制限がない」などがある。

【００４５】

以上で、本実施の形態におけるライセンス２３０の一例に関する説明を終了する。

【００４６】

図６は、本実施の形態におけるコンテンツサーバ１０２の機能構成を示すブロック図である。図６に示すように、コンテンツサーバ１０２は、コンテンツ蓄積部５０１、コンテンツ属性情報蓄積部５０２、ワーク鍵蓄積部５０３、コンテンツ符号化部５０４、スクランブル鍵生成部５０５、コンテンツ暗号化部５０６、送出日時特定部５０７、関連情報生成部５０８、関連情報暗号化部５０９、多重化部５１０及び送出部５１１を備える。

【００４７】

コンテンツ蓄積部５０１は、例えば、ハードディスク装置又はＤＶＤレコーダ等であり、コンテンツを蓄積する。さらに、コンテンツ蓄積部５０１は、コンテンツ配信システム１内でコンテンツを一意に特定するための識別子、コンテンツの名称、コンテンツを配信する日時などが、コンテンツと対応づけて蓄積されているものとする。

【００４８】

コンテンツ属性情報蓄積部５０２は、例えば、ＲＡＭ等であり、コンテンツに関する情報を蓄積する。さらに、コンテンツ属性情報蓄積部５０２は、コンテンツ配信システム１内でコンテンツを一意に特定するための識別子、当該コンテンツを利用するにあたり必要となる契約を識別する情報などが蓄積されているものとする。

【００４９】

ワーク鍵蓄積部５０３は、例えば、ＲＡＭであり、ＥＣＭ２２０を暗号化するための暗号鍵を蓄積する。さらに、ワーク鍵蓄積部５０３は、ワーク鍵Ｋｗ２０３とワーク鍵ＩＤ４０２とが、ワーク鍵利用開始日などと共に蓄積されており、送出時期に応じて、どのワーク鍵Ｋｗ２０３をＥＣＭ２２０に適用すれば良いかが特定可能となっているものとする。

【００５０】

コンテンツ符号化部５０４は、端末装置１０３に送出するコンテンツをコンテンツ蓄積部５０１から読み出し、コンテンツをＭＰＥＧ形式で符号化する。さらに、コンテンツ符号化部５０４は、ＭＰＥＧストリームを生成するリアルタイムエンコーダであって、上流システム（例えば、番組運行管理システムなど）の指示により、コンテンツ蓄積部５０１から映像、音声などを読み出し、映像、音声を含むＭＰＥＧ－２やＨ．２６４のＥＳ（Elementary Stream）を生成する。さらに、これらのＥＳを含むＰＥＳ（Packetized Elementary Stream）パケットを生成し、最後にＭＰＥＧ－２　ＴＳパケット化して、多重化部５１０に送出する。

【００５１】

スクランブル鍵生成部５０５は、コンテンツをスクランブルするスクランブル鍵Ｋｓ２０１を生成する。さらに、スクランブル鍵生成部５０５は、スクランブル鍵Ｋｓ２０１の更新周期に基づき、スクランブル鍵Ｋｓ２０１を順次生成し、コンテンツ暗号化部５０６に送信する。

【００５２】

コンテンツ暗号化部５０６は、コンテンツのスクランブルを行う。さらに、コンテンツ暗号化部５０６は、ＴＳパケットのペイロード部を、スクランブル鍵生成部５０５から取得したスクランブル鍵Ｋｓ２０１を用いて、ＡＥＳなどを用いて、ＣＢＣ（Cipher Block Chaining）モード＋ＯＦＢ（Output Feed Back）モードによって暗号化（スクランブル）する。

【００５３】

送出日時特定部５０７は、例えば、制御プログラムを格納するＲＯＭ等を備えるマイクロコンピュータであり、コンテンツサーバ１０２全体の機能を制御する。さらに、送出日時特定部５０７は、時刻情報を管理する手段であり、時刻情報を必要とするユニットに対して、現在時刻を提供する。

【００５４】

関連情報生成部５０８は、コンテンツ関連情報（ＥＣＭ２２０）に暗号化コンテンツを復号するコンテンツ復号鍵を設定（特に、複数設定）する。具体的には、関連情報生成部５０８は、上記スクランブル鍵生成部５０５で生成されたスクランブル鍵Ｋｓ２０１など

を含むＥＣＭ２２０を生成する。さらに、関連情報生成部５０８は、上流システムなどからの指示に基づき、コンテンツの送出及びスクランブル鍵生成部５０５からのスクランブル鍵Ｋｓ２０１の取得に合わせて、ＥＣＭ２２０を生成する。生成したＥＣＭ２２０は、多重化部５１０に送信される。

【００５５】

関連情報暗号化部５０９は、上記関連情報生成部５０８で生成したＥＣＭ２２０を暗号化する。関連情報暗号化部５０９は、関連情報生成部５０８からＥＣＭ２２０を受信し、ワーク鍵蓄積部５０３から取得したワーク鍵Ｋｗ２０３でＥＣＭ２２０を暗号化する。ＥＣＭ２２０の暗号化には、ＡＥＳなどを用い、暗号化モードは、ＣＢＣ＋ＯＦＢを用いる。さらに、関連情報暗号化部５０９は、このように暗号化したＥＣＭ２２０を、多重化部５１０に送信する。

【００５６】

多重化部５１０は、コンテンツ暗号化部５０６から受け取った映像、音声、データなどを含むＴＳと、関連情報暗号化部５０９から受け取ったＥＣＭ２２０のＴＳとを多重化し、多重化されたＴＳを生成する。

【００５７】

送出部５１１は、多重化部５１０において生成されたＴＳを、端末装置１０３に送出する。例えば、コンテンツ送出部５１１は、ＴＳをＩＰ（Internet Protocol）ネットワーク上にマルチキャストで端末装置１０３に送信する。

【００５８】

以上で、本実施の形態におけるコンテンツサーバ１０２の機能構成に関する説明を終了する。

【００５９】

図７（ａ）は、関連情報生成部５０８が生成するＥＣＭ２２０の一例を示す図である。図７（ａ）に示すように、ＥＣＭ２２０は、フォーマットバージョン６０１、ワーク鍵ＩＤ６０２、送出日時６０３、契約判定コード６０４、プライベートデータ６０５、スクランブル鍵（ｏｄｄ）６０６及びスクランブル鍵（ｅｖｅｎ）６０７から構成される。

【００６０】

フォーマットバージョン６０１には、ＥＣＭ２２０のフォーマット及びＥＣＭ２２０の暗号化方式を識別するための情報が設定される。

【００６１】

ワーク鍵ＩＤ６０２には、ＥＣＭ２２０を暗号化するワーク鍵Ｋｗ２０３を識別するための情報が設定される。ワーク鍵ＩＤ６０２は、ＥＣＭ２２０の非暗号化部分に設定されるため、端末装置１０３において暗号化されたＥＣＭ２２０を復号する際に、ワーク鍵ＩＤ６０２を参照することにより、どのワーク鍵Ｋｗ２０３を用いてＥＣＭ２２０を復号すれば良いかを判別することができる。ワーク鍵ＩＤ６０２には、サービスを提供する事業者を識別するコード、ワーク鍵Ｋｗ２０３のｅｖｅｎ／ｏｄｄのペアを特定する情報を含んでいても良いものとする。

【００６２】

送出日時６０３には、送出日時特定部５０７から取得した現在時刻が設定される。すなわち、送出日時６０３には、ＥＣＭ２２０及びコンテンツの送出日時が設定される。

【００６３】

契約判定コード６０４は、当該コンテンツの属性を示す情報であり、端末装置１０３でコンテンツを視聴する場合に、当該コンテンツを視聴するための契約がなされているか否かを判定するために用いられる。

【００６４】

プライベートデータ６０５は、任意のデータを設定可能なフィールドである。本実施の形態においては、暗号ブロック長とのアライメントを確保するためのパディングとして設定されているデータである。なお、また、図７（ｂ）に示すように、プライベートデータ６０５の一部に出力制御情報６１５を格納してもよい。この出力制御情報６１５は、上記

図５のライセンス２３０における出力制御情報４０６と同等のデータ構成を有しており、出力制御情報４０６と同一の値を設定することも、異なる値を設定することもできる。プレイベートデータ６０５の一部に出力制御情報６１５が設定された場合、出力制御情報４０６に従うか出力制御情報６１５に従うかは、所定のルールに従って決定されることとする。本実施の形態においては、端末装置１０３は、原則、出力制御情報６１５の内容を優先することとする。なお、これに限るわけではなく、例えば、双方を参照し、両者の値が異なる場合は、制約が緩い条件を適用することとしてもよいし、制約が厳しい条件を適用することとしてもよいこととする。

【００６５】

スクランブル鍵（ｏｄｄ）６０６には、コンテンツのＴＳパケットのペイロード部を暗号化するスクランブル鍵Ｋｓ２０１が設定される。

【００６６】

スクランブル鍵（ｅｖｅｎ）６０７には、上記のスクランブル鍵（ｏｄｄ）６０６と同様、コンテンツのＴＳパケットのペイロード部を暗号化するスクランブル鍵Ｋｓ２０１が設定される。ＥＣＭ２２０でｏｄｄ／ｅｖｅｎのスクランブル鍵Ｋｓ２０１を送信することにより、スクランブル鍵Ｋｓ２０１の切り替わり時においても、端末装置１０３は継続してコンテンツの利用が可能となる。

【００６７】

ここで、ＥＣＭ２２０のフォーマットバージョン６０１及びワーク鍵ＩＤ６０２は、非暗号のデータであり、送出日時６０３、契約判定コード６０４、プライベートデータ６０５、スクランブル鍵（ｏｄｄ）６０６、スクランブル鍵（ｅｖｅｎ）６０７は、ＡＥＳなどを用いて、ＣＢＣモードにより暗号化されるデータである。また、暗号ブロック長（例えば、１２８ビットの鍵長を用いたＡＥＳでは、１６バイト）に満たない端数が発生した場合には、ＯＦＢモードを併用するものとする。ＣＢＣモードのＩＶ（Initialization Vector）値については、固定値が用いられ、少なくとも端末装置１０３では機器固定（外から変更できない）であるものとする。

【００６８】

ここで、図８を用いて、ＥＣＭ２２０の暗号化部のデータ配列について、さらに詳細な説明を行う。

【００６９】

図８は、上記図７に示したＥＣＭ２２０の暗号化部（暗号化対象の部分）の詳細を示した図であり、暗号ブロック１と暗号ブロック３において、それぞれ送出日時６０３、契約判定コード６０４、プライベートデータ６０５が設定される。また、暗号ブロック２にはスクランブル鍵（ｏｄｄ）６０６が設定され、暗号ブロック４にはスクランブル鍵（ｅｖｅｎ）６０７が設定されている例が示されている。

【００７０】

ＥＣＭ２２０において、不正なユーザ等による改竄を防止すべきデータは、端末装置１０３でコンテンツの利用可否の判定に関わる送出日時６０３及び契約判定コード６０４である。

【００７１】

ここで、端末装置１０３における、ＥＣＭ２２０の契約判定コード６０４と、ライセンス２３０の契約コード４０３とを用いた、ビット毎の一致判定処理の一例について、図９を用いて説明する。

【００７２】

図９に示すように、契約判定コード６０４は、各ビットに各サービスが対応づけられるビット配列（ビットマップ）であり、当該ＥＣＭ２２０を含むコンテンツが属するサービスに対応するビットが「１」に、それ以外のビットが「０」に設定される。一方、契約コード４０３は、同様に各ビットにサービスが対応づけられており、ユーザβが契約したサービスに対応するビットが「１」に、ユーザβが契約していないサービスには「０」が設定される。

【００７３】
端末装置１０３では、ＥＣＭ２２０を受信した際、契約判定コード６０４と契約コード４０３との論理積（ＡＮＤ）を算出し、その結果、いずれかのビットが「１」であれば「契約あり」、全てのビットが「０」であれば「契約なし」と判定する。
【００７４】
端末装置１０３において、ＥＣＭ２２０の契約判定コード６０４とライセンス２３０の契約コード４０３とに基づく契約内容判定処理は、このようなビット毎の一致判定処理という極めて単純な方法であるため、暗号化されたＥＣＭ２２０の一部が改竄されたＥＣＭ２２０を復号した場合、契約判定コード６０４が本来の契約とは異なる値となってしまい、正しい契約内容の判定が行えず、コンテンツの不正利用に繋がるおそれがある。また、送出日時６０３についても、同様に、暗号化されたＥＣＭ２２０の改竄により、正しい契約内容の判定が行えずに、コンテンツの不正利用に繋がるおそれがある。
【００７５】
そこで、本実施の形態における図８では、ＣＢＣモードのブロック連鎖の特徴を利用して、ＥＣＭ２２０に含まれるデータの改竄を防止している。即ち、ＣＢＣモードでは、復号時において、隣接する２つの暗号ブロックが連鎖しており、ある暗号ブロックの特定ビットを反転させた場合、当該ブロックの全ビットに影響を与える可能性があるとともに、後続の暗号ブロックの対応するビットのみに影響を与えるという特徴がある。図８では、改竄を防止すべきデータ（本実施の形態では、送出日時６０３及び契約判定コード６０４）を含む暗号ブロックの直後のブロックに、正しい復号結果にならない場合に不正者に不利益となるデータ（本実施の形態では、コンテンツを復号するためのスクランブル鍵Ｋｓ２０１）を配置することで、改竄を行った場合には正しくスクランブル鍵Ｋｓ２０１が取得できない（すなわち、コンテンツが正しく復号できないため、利用できない）ために、実質的に送出日時６０３及び契約判定コード６０４の改竄を防止するようにしている。
【００７６】
また、ビット反転を行った暗号ブロックの復号結果は、当該暗号ブロックの全ビットに影響を与える可能性があるのに対し、後続の暗号ブロックでは、ビット反転を行ったビットのみが影響を受けるため、この点を鑑み、図８においては、スクランブル鍵Ｋｓ２０１を暗号ブロックの境界にアラインするように、プライベートデータ６０５を配置している。また、コンテンツ及びＥＣＭ２２０に適用する暗号アルゴリズムとして、１２８ビットの鍵長のＡＥＳを適用する場合であれば、暗号ブロック長、スクランブル鍵長は共に１６バイトとなり、図７に示すように、スクランブル鍵Ｋｓ２０１が１つの暗号ブロック長と一致するため、スクランブル鍵Ｋｓ２０１の直前の暗号ブロックのいずれのビットを反転させた場合であっても、不正者は、正しいスクランブル鍵Ｋｓ２０１を取得できないような構成とすることができる。
【００７７】
さらに、ＥＣＭ２２０には、スクランブル鍵（ｏｄｄ）６０６、スクランブル鍵（ｅｖｅｎ）６０７の２つスクランブル鍵Ｋｓ２０１が含まれているため、単純にＣＢＣモードのブロック連鎖の特徴を用いただけでは、送出日時６０３又は契約判定コード６０４の改竄を試みた場合に、どちらか一方のスクランブル鍵Ｋｓ２０１は正しく取得できないが、他方のスクランブル鍵Ｋｓ２０１は正しく取得できてしまう可能性があり、その結果、コンテンツの不正利用に繋がるおそれがある。そのため、図８では、スクランブル鍵（ｏｄｄ）６０６（暗号ブロック２）、スクランブル鍵（ｅｖｅｎ）６０７（暗号ブロック４）のそれぞれの直前の暗号ブロックである暗号ブロック１及び暗号ブロック３に、送出日時６０３及び契約判定コード６０４を配置し、暗号ブロック１～４を連続した暗号ブロックとして配置した上で、両者の送出日時６０３及び契約判定コード６０４に、それぞれ同一値を設定するようにしている。端末装置１０３においては、復号後のＥＣＭ２２０の２つの送出日時６０３、及び、２つの契約判定コード６０４が一致するか否かを判定することにより、２つの送出日時６０３、又は、契約判定コード６０４の少なくとも一方が改竄された場合であっても。改竄の検出が可能となる。また、２つの契約判定コード６０４が一

致するか否かを判定することにより、スクランブル鍵Ｋｓ２０１の取得処理前に改竄を検出できる場合があるという効果もある。

【００７８】

本実施の形態では、以上のようなＥＣＭ２２０の構成とすることにより、ＭＩＣ（Message Integrity Check）のような大きな計算量を要する処理を不要とし、暗号化処理と簡単なデータの一致判定のみで、実質的にＥＣＭ２２０の改竄防止を実現している。暗号化処理においては、特殊な暗号化モード等を用いる必要はなく、ＣＢＣモードという標準的な暗号モードで対応可能である。また、データの一致判定の処理に関しても、暗号ブロックのうちの改竄を防止すべき必要最低限のデータ（本実施の形態では、送出日時６０３及び契約判定コード６０４）の一致判定のみで良い。従って、本実施の形態で示した方式の実装容易性は高いと考えることができる。

【００７９】

以上で、本実施の形態におけるＥＣＭ２２０の暗号化部のデータ配列に関する説明を終了する。

【００８０】

図１０は、本実施の形態における端末装置１０３の機能構成を示すブロック図である。図１０に示されるように、端末装置１０３は、ライセンス格納部９０１、固有情報管理部９０２、ライセンス受信部９０３、ライセンス管理部９０４、コンテンツ受信部９０５、分離部９０６、時間情報取得部９０７、関連情報復号部９０８、リアルタイム受信判定部９０９、改竄検出部９１０、契約内容判定部９１１、コンテンツ利用制御部９１２及びコンテンツ格納制御部９１３を備える。以下、各構成要素について説明を行う。

【００８１】

ライセンス格納部９０１は、ライセンス受信部９０３が受信したライセンス２３０を蓄積する。ここで、ライセンス２３０を当該端末装置１０３のみで利用可能とするため、ライセンス２３０をローカル暗号などにより暗号化した上で蓄積するのが一般的である。

【００８２】

固有情報管理部９０２は、端末装置１０３固有の情報を管理し、ライセンスサーバ１０１とのＳＡＣを確立するために必要な端末装置１０３の秘密鍵、端末装置１０３の公開鍵証明書などの固有の情報を保持する。

【００８３】

ライセンス受信部９０３は、ライセンスサーバ１０１からＳＡＣを通じて、ライセンス２３０を受信する。

【００８４】

ライセンス管理部９０４は、ライセンス格納部９０１に蓄積したライセンス２３０を管理する。

【００８５】

コンテンツ受信部９０５は、ＩＰネットワークなどを通じて、コンテンツサーバ１０２からコンテンツを受信する。コンテンツ受信部９０５は、受信したコンテンツからＴＳを取得して、分離部９０６に送信する。

【００８６】

分離部９０６は、ＭＰＥＧ－２　ＴＳにより多重化された暗号化コンテンツを取得し、コンテンツとＥＣＭ２２０などとを分離するための手段である。分離部９０６は、コンテンツ受信部９０５が受信したＴＳに含まれるＰＡＴ（Program Association Table）、ＰＭＴ（Program Map Table）などのＰＳＩ情報を参照して、コンテンツの映像、音声や、ＥＣＭ２２０を含むＴＳパケットのＰＩＤを取得し、コンテンツとＥＣＭ２２０などとを分離する。

【００８７】

時間情報取得部９０７は、現在時刻を管理する。例えば、時間情報取得部９０７は、端末装置１０３内で正確に現在時刻を管理することが可能なクロックや、適宜、放送のＴＯＴ（Time Offset Table）などや、セキュアな通信路などを通じて、ネットワーク上の信

頼できるサーバなどから取得した現在時刻に基づき動作する、クロック、タイマ等であるものとする。また、これらの複数の信頼できる時刻情報を取得するにあたり、優先度を付けて適用するようにしても良い。本実施の形態では、時間情報取得部９０７は、図１０に図示しない時刻情報取得手段を通じて、ネットワーク上の時刻サーバから信頼できる時刻情報を取得し、取得した時刻情報に基づき、計時を行うものとする。

【００８８】

関連情報復号部９０８は、ワーク鍵Ｋｗ２０３を用いてＥＣＭ２２０を復号する。より詳細に説明すると、関連情報復号部９０８は、分離部９０６から取得したＥＣＭ２２０のワーク鍵ＩＤ６０２を参照し、ライセンス格納部９０１から対応するワーク鍵ＩＤ４０２を持つライセンス２３０を取得し、ライセンス２３０を有する場合、ライセンス２３０のワーク鍵Ｋｗ４０１に設定されたワーク鍵Ｋｗ２０３を用いて、ＥＣＭ２２０を復号する。

【００８９】

リアルタイム受信判定部９０９は、ＥＣＭ２２０に設定された送出日時６０３と、時間情報取得部９０７から取得した現在時刻との差分が、規定値以内であるかどうかを判定することにより、コンテンツ受信部９０５が受信したコンテンツが、リアルタイム受信かどうか（現在、コンテンツサーバ１０２から送出されたものであるか）を判定する。

【００９０】

従来の限定受信方式では、ＥＣＭに含まれる送出日時と、端末装置が保持する契約期限との比較により、期限判定を行う方式が一般的であるが、このような方式では、ＥＣＭに含まれる送出日時が契約期限内の値である場合は、常に複数回のコンテンツ利用（視聴、書き出しなど）が可能である。このような方式を、ＩＰ方式による放送サービス（ＩＰマルチキャスト放送、ＩＰ放送などと呼ばれる）に適用した場合、ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）等により比較的簡単にコンテンツを取得、蓄積され、蓄積されたコンテンツを複数回にわたって端末装置１０３に入力することで、複数回のコンテンツ利用が不正に行えてしまうという問題がある。そこで、本実施の形態では、信頼できる源泉から取得した現在時刻を用いて、ＥＣＭ２２０に含まれる送出日時６０３を検証することで、コンテンツがリアルタイムに受信されているものか否かを判定するようにしており、これにより、その利用をリアルタイム受信時の１回のみに限定することができ、蓄積されたコンテンツを複数回入力（再送）された場合の利用を防止することができる。また、本実施の形態では、時間情報取得部９０７が管理する現在時刻と送出日時６０３との日時を正確に同期させることは現実的には困難であることから、リアルタイム受信判定部９０９のリアルタイム受信判定処理において許容される誤差範囲を予め保持しておき、時間情報取得部９０７が管理する現在時刻と送出日時６０３との日時の差が許容される誤差の範囲内であれば、コンテンツがリアルタイムに受信されているとみなすようにしている。

【００９１】

改竄検出部９１０は、ＥＣＭ２２０に設定された２つの送出日時６０３、及び、２つの契約判定コード６０４が、それぞれ同一であるかの一致判定を行うことにより、ＥＣＭ２２０の改竄を検出する。

【００９２】

契約内容判定部９１１は、関連情報復号部９０８、リアルタイム受信判定部９０９、改竄検出部９１０の処理の結果、ＥＣＭ２２０を復号でき、かつ、ＥＣＭ２２０の正当性（すなわち、改竄されておらず、有効である）が確認できた場合、ライセンス管理部９０４から取得したライセンス２３０及びＥＣＭ２２０に基づき、スクランブル鍵Ｋｓ２０１の利用可否を判定する。さらに、契約内容判定部９１１は、利用可否判定の結果、スクランブル鍵Ｋｓ２０１の利用が可であると判定した場合には、コンテンツ利用制御部９１２又はコンテンツ格納制御部９１３に対して、その旨を通知すると共に、スクランブル鍵Ｋｓ２０１を送信する。

【００９３】

コンテンツ利用制御部９１２は、受信したコンテンツを再生する。さらに、コンテンツ

利用制御部９１２は、関連情報復号部９０８、リアルタイム受信判定部９０９、改竄検出部９１０、契約内容判定部９１１での処理の結果、スクランブル鍵Ｋｓ２０１を取得できた場合に、取得したスクランブル鍵Ｋｓ２０１を用いて、コンテンツ受信部９０５により受信したコンテンツを復号し、再生する処理を行う。このとき、ライセンス管理部９０４から取得した出力制御情報４０６に基づき、デジタル再生出力／アナログ再生出力の制御を行う。

【００９４】

コンテンツ格納制御部９１３は、受信したコンテンツを内蔵若しくは外部の記録媒体などに書き出す手段である。さらに、コンテンツ格納制御部９１３は、関連情報復号部９０８、リアルタイム受信判定部９０９、改竄検出部９１０、契約内容判定部９１１での処理の結果、スクランブル鍵Ｋｓ２０１を取得でき、かつ、ライセンス管理部９０４から取得した出力制御情報４０６で書き出しが許可されている場合に、取得したスクランブル鍵Ｋｓ２０１を用いて、コンテンツ受信部９０５により受信したコンテンツを復号し、復号したコンテンツを、書き出し先の記録媒体に応じた所定の形式に変換、及び暗号化して書き出す処理を行う。

【００９５】

次に、フローチャートを参照しながら、本実施の形態におけるコンテンツ配信システム１の動作について説明を行う。

【００９６】

まず、図１１に示すフローチャートを参照して、本実施の形態における端末装置１０３が、ライセンスサーバ１０１からライセンス２３０を受信する動作について説明する。

【００９７】

Ｓ１００１：ライセンス管理部９０４は、ライセンスサーバ１０１に対して、ライセンス２３０を要求するライセンス要求を生成し、ライセンス受信部９０３に対して送信する。ライセンス受信部９０３は、ＳＡＣを通じて、ライセンスサーバ１０１にライセンス要求を送信する。

【００９８】

Ｓ１００２：ライセンス送信部３０５は、端末装置１０３からライセンス要求を受信する。ライセンス送信部３０５は、ライセンス生成部３０４に対して、受信したライセンス要求を送信する。

【００９９】

Ｓ１００３：ライセンス生成部３０４は、ＳＡＣで認証した端末装置１０３の契約状況について、契約情報蓄積部３０２を用いて確認し、端末装置１０３（ユーザβ）の契約有無を判定する。具体的には、まずＳ１００２で受信したライセンス要求から要求されたライセンスの識別情報を取得し、契約情報蓄積部３０２に、端末装置１０３の対応する契約情報が蓄積されているか否かを確認する。契約情報が契約情報蓄積部３０２に管理されている場合には、更にその契約期限が超過していないかどうかを確認する。確認の結果、契約情報が契約情報蓄積部３０２に蓄積されていない場合や、契約期限が超過している場合には、契約は有効でない（契約なし）と判断する。一方、契約情報が契約情報蓄積部３０２に蓄積されており、かつ、契約期限が超過していない場合には、契約は有効である（契約あり）と判断する。本処理において「契約あり」と判定された場合、Ｓ１００４の処理に進む。本処理において「契約なし」と判定された場合、Ｓ１００５の処理に進む。

【０１００】

Ｓ１００４：ライセンス生成部３０４は、図４で示すライセンス２３０を生成する。ライセンス生成部３０４は、ワーク鍵蓄積部３０１から、図４におけるワーク鍵Ｋｗ４０１及びワーク鍵ＩＤ４０２を取得し、ライセンス２３０に設定する。また、ライセンス生成部３０４は、契約情報蓄積部３０２から端末装置１０３（ユーザβ）が加入しているサービス契約に関する情報を取得して、契約コード４０３、開始日時４０４、終了日時４０５、出力制御情報４０６を設定する。ライセンス生成部３０４は、生成したライセンス２３０をライセンス送信部３０５に送信する。

【０１０１】
Ｓ１００５：ライセンス送信部３０５は、ライセンス要求レスポンスを生成し、端末装置１０３に対して送信する。ライセンス送信部３０５は、ライセンス生成部３０４がＳ１００４でライセンス２３０を生成した場合には、ライセンス２３０を含むライセンス要求レスポンスを、Ｓ１００４でライセンス２３０を生成しなかった場合には、ライセンス２３０を含まず、ライセンス２３０を送信不可である旨を通知する情報を含むライセンス要求レスポンスを生成する。
【０１０２】
Ｓ１００６：ライセンス受信部９０３は、ライセンスサーバ１０１からのライセンス要求レスポンスを受信する。
【０１０３】
Ｓ１００７：ライセンス管理部９０４は、ライセンス取得要求レスポンスを参照し、ライセンス２３０を受信できたか否かを確認する。ライセンス２３０を受信できた場合、Ｓ１００８の処理に進む。ライセンス２３０を受信できなかった場合、本処理を終了する。
【０１０４】
Ｓ１００８：ライセンス管理部９０４は、Ｓ１００７で受信したライセンス２３０をライセンス格納部９０１に格納する。
【０１０５】
以上で、本実施の形態におけるライセンス送受信の動作についての説明を終わる。
【０１０６】
次に、図１２のフローチャートを参照しながら、コンテンツサーバ１０２が、端末装置１０３に対してコンテンツを送出する動作について説明を行う。
【０１０７】
Ｓ１１０１：コンテンツ符号化部５０４は、上流システム（例えば、番組運行管理システム）などの指示により、コンテンツを送出中であるか否かを判定する。具体的には、コンテンツ符号化部５０４は、上流システムなどからコンテンツの符号化、送出の中止指示がない場合、Ｓ１１０２の処理に進む。上流システムなどからコンテンツの符号化、送出の中止指示を受けた場合には、本処理を終了する。
【０１０８】
Ｓ１１０２：コンテンツ符号化部５０４は、上流システムなどから指定されたコンテンツを、コンテンツ蓄積部５０１から読み出し、コンテンツをＭＰＥＧ－２やＨ．２６４等で符号化（エンコード）して、コンテンツを含むＴＳを生成する。コンテンツ符号化部５０４は、生成したＴＳをコンテンツ暗号化部５０６に順次送信する。
【０１０９】
Ｓ１１０３：スクランブル鍵生成部５０５は、乱数などに基づき、スクランブル鍵Ｋｓ２０１を更新周期に対応して生成し、コンテンツ暗号化部５０６及び関連情報生成部５０８に送信する。
【０１１０】
Ｓ１１０４：コンテンツ暗号化部５０６は、スクランブル鍵生成部５０５から受信したスクランブル鍵Ｋｓ２０１を用いて、コンテンツ符号化手段１１０２から受信したコンテンツのＴＳパケットのペイロード部を順次暗号化する。なお、コンテンツ暗号化部５０６は、スクランブル鍵Ｋｓ２０１の更新周期に合わせて、ＴＳパケットを暗号化するスクランブル鍵Ｋｓ２０１を切り替えると同時に、ＴＳパケットにおけるヘッダ部のｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌの値をｅｖｅｎ／ｏｄｄに対応させて更新する。コンテンツ暗号化部５０６は、暗号化したＴＳを多重化部５１０に送信する。
【０１１１】
Ｓ１１０５：関連情報生成部５０８は、コンテンツの送出に合わせて、図６に示したＥＣＭ２２０を生成する。具体的には、関連情報生成部５０８は、ワーク鍵蓄積部５０３から、適用すべきワーク鍵Ｋｗ２０３のワーク鍵ＩＤ６０２を取得し、ＥＣＭ２２０に設定する。次に、送出日時特定部５０７から現在時刻を取得して、２つの送出日時６０３に設

定する。次に、コンテンツ属性情報蓄積部５０２から当該コンテンツの属性情報を取得し、端末装置１０３においてコンテンツの利用可否を判定するための契約判定コード６０４を生成して、ＥＣＭ２２０の２箇所の契約判定コード６０４に設定する。さらに、図７で示したように、送出日時６０３及び契約判定コード６０４を含む暗号ブロックの後続の暗号ブロックにアラインするようにスクランブル鍵（ｏｄｄ）６０６及びスクランブル鍵（ｅｖｅｎ）６０７を設定するため、プライベートデータ６０５を挿入する。最後に、スクランブル鍵生成部５０５からにスクランブル鍵（ｏｄｄ）６０６及びスクランブル鍵（ｅｖｅｎ）６０７を取得し、ＥＣＭ２２０に設定する。関連情報生成部５０８は、生成したＥＣＭ２２０を関連情報暗号化部５０９に送信する。

【０１１２】

Ｓ１１０６：関連情報暗号化部５０９は、関連情報生成部５０８から受信したＥＣＭ２２０のワーク鍵ＩＤ６０２を参照して、ワーク鍵蓄積部５０３から対応するワーク鍵Ｋｗ２０３を取得し、ＥＣＭ２２０の暗号化部をＣＢＣモードで暗号化する。関連情報暗号化部５０９は、暗号化したＥＣＭ２２０をＴＳパケット化した後、多重化部５１０に送信する。

【０１１３】

Ｓ１１０７：多重化部５１０は、受信した暗号化コンテンツのＴＳ及び暗号化したＥＣＭ２２０のＴＳを多重化した後、送出部５１１に送信する。

【０１１４】

Ｓ１１０８：送出部５１１は、多重化部５１０から受信したＴＳを、端末装置１０３に対して送信し、その後、Ｓ１１０１の処理に進む。

【０１１５】

以上で、本実施の形態におけるコンテンツ送出処理の動作についての説明を終わる。

【０１１６】

次に、図１３のフローチャートを参照しながら、本実施の形態における端末装置１０３が、コンテンツサーバ１０２から送出されたコンテンツを受信する動作について説明を行う。

【０１１７】

Ｓ１２０１：コンテンツ受信部９０５は、コンテンツサーバ１０２から送信されたコンテンツを受信する。受信したコンテンツはＴＳ化され、順次、分離部９０６に送信される。

【０１１８】

Ｓ１２０２：コンテンツ受信部９０５は、コンテンツサーバ１０２からのコンテンツを受信中であるか否かを確認する。コンテンツを受信中である場合は、Ｓ１２０３の処理に進む。一方、コンテンツを受信中でない場合は、本処理を終了する。

【０１１９】

Ｓ１２０３：分離部９０６は、コンテンツ受信部９０５から受信したＴＳをコンテンツとＥＣＭ２２０とのＴＳパケットに分離する。分離部９０６は、分離したコンテンツをコンテンツ利用制御部９１２あるいはコンテンツ格納制御部９１３に送信し、分離したＥＣＭ２２０を関連情報復号部９０８に送信する。

【０１２０】

Ｓ１２０４：関連情報復号部９０８は、分離部９０６から受信したＥＣＭ２２０のワーク鍵ＩＤ６０２を参照して、ライセンス管理部９０４から対応するワーク鍵Ｋｗ２０３を含むライセンス２３０を保持するか否かを確認する。具体的には、関連情報復号部９０８は、ライセンス管理部９０４に対してワーク鍵ＩＤ６０２を送信する。次に、ライセンス管理部９０４は、受信したワーク鍵ＩＤ６０２と一致するワーク鍵ＩＤ４０２を有するライセンス２３０を、ライセンス格納部９０１から検索する。

【０１２１】

ワーク鍵ＩＤ６０２に対応するワーク鍵Ｋｗ２０３を保持している場合、Ｓ１２０５の処理に進む。一方、ワーク鍵ＩＤ６０２に対応するワーク鍵Ｋｗ２０３を保持していない

場合、本処理を終了する。

【０１２２】

Ｓ１２０５：関連情報復号部９０８は、ライセンス管理部９０４から取得したワーク鍵Ｋｗ２０３を用いて、ＥＣＭ２２０の暗号化部を復号する。関連情報復号部９０８は、復号したＥＣＭ２２０をリアルタイム受信判定部９０９に送信する。

【０１２３】

Ｓ１２０６：リアルタイム受信判定部９０９、改竄検出部９１０、及び、契約内容判定部９１１は、図１４を用いて後述するＥＣＭ判定処理を行う。

【０１２４】

Ｓ１２０７：契約内容判定部９１１は、スクランブル鍵Ｋｓ２０１の取得可否を判定する。スクランブル鍵Ｋｓ２０１を取得できた場合には、Ｓ１２０８の処理に進む。スクランブル鍵Ｋｓ２０１を取得できなかった場合には、本処理を終了する。

【０１２５】

Ｓ１２０８：コンテンツ利用制御部９１２又はコンテンツ格納制御部９１３は、契約内容判定部９１１から受信したスクランブル鍵Ｋｓ２０１を用いて、分離部９０６から順次受信した暗号化コンテンツのＴＳパケットを復号する。

【０１２６】

Ｓ１２０９：コンテンツ利用制御部９１２は、ＥＣＭ２３０から抽出した出力制御情報６１５及び／又はライセンス管理部９０４から受信した出力制御情報４０６に基づき、コンテンツの利用を行う。コンテンツ利用制御部９１２では、出力制御情報６１５及び／又は出力制御情報４０６を確認し、出力制御情報６１５及び／又は出力制御情報４０６での指定に合わせて、デジタル出力／アナログ出力にコンテンツを出力する。また、コンテンツ格納制御部９１３では、出力制御情報６１５及び／又は出力制御情報４０６を確認し、コンテンツの書き出しが可（例えば、ＣＣＩがＣｏｐｙ　Ｆｒｅｅ）の場合は、書き出し先の記録媒体に応じた所定の形式に変換・暗号化して書き出す処理を行う。ただし、コンテンツの書き出しが不可（例えば、ＣＣＩがＣｏｐｙ　Ｎｅｖｅｒ）の場合は、コンテンツの書き出しは行わず処理を終了する。

【０１２７】

なお、暗号化されたＥＣＭ２２０の改竄が行われた場合に、仮に、Ｓ１２０５のＥＣＭ判定処理でＥＣＭ改竄なしと判断された場合であっても、必ず復号後のスクランブル鍵Ｋｓ（ｏｄｄ）６０６及びスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７は正しい値とはならないため、本ステップにおいてコンテンツのデコードに失敗することとなる。

【０１２８】

以上で、本実施の形態におけるコンテンツ受信処理の動作についての説明を終わる。

【０１２９】

次に、図１４に示すフローチャートを参照して、本実施の形態における端末装置１０３が、ＥＣＭ２２０の利用可否判定を行う、ＥＣＭ判定処理の動作について説明する。なお、このＥＣＭ判定処理は、上記図１３におけるＳ１２０６を詳細化したものである。

【０１３０】

Ｓ１３０１：リアルタイム受信判定部９０９は、図１５を用いて後述するリアルタイム受信判定処理を行う。

【０１３１】

Ｓ１３０２：リアルタイム受信判定部９０９は、Ｓ１３０１の処理の結果、コンテンツ及びＥＣＭ２２０が「リアルタイム受信」であるか否かを確認する。コンテンツ及びＥＣＭ２２０が「リアルタイム受信」であると判定された場合には、Ｓ１３０３の処理に進む。一方、コンテンツ及びＥＣＭ２２０が「非リアルタイム受信」（例えば、コンテンツ及びＥＣＭ２２０が蓄積されて、再送信される場合など）であると判定された場合には、本処理を終了する。

【０１３２】

Ｓ１３０３：改竄検出部９１０は、図１６を用いて後述する改竄検出処理を行う。

【０１３３】
Ｓ１３０４：改竄検出部９１０は、Ｓ１３０３の処理の結果、ＥＣＭ２２０について、「ＥＣＭ改竄なし」と判定された場合には、Ｓ１３０５に進む。一方、ＥＣＭ２２０について、「ＥＣＭ改竄あり」と判定された場合には、本処理を終了する。
【０１３４】
Ｓ１３０５：契約内容判定部９１１は、図１７を用いて後述する契約内容判定処理を行う。
【０１３５】
Ｓ１３０６：契約内容判定部９１１は、Ｓ１３０５の処理の結果、「契約あり」と判定された場合には、Ｓ１３０７の処理に進む。一方、「契約なし」と判定された場合には、本処理を終了する。
【０１３６】
Ｓ１３０７：契約内容判定部９１１は、ＥＣＭ２２０からスクランブル鍵Ｋｓ（ｏｄｄ）６０６及びスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７を取得する。
【０１３７】
次に、図１５のフローチャートを参照しながら、上記図１４におけるＳ１３０１の、リアルタイム受信判定処理の動作について説明を行う。
【０１３８】
Ｓ１４０１：リアルタイム受信判定部９０９は、時間情報取得部９０７から現在時刻を取得する。
【０１３９】
Ｓ１４０２：リアルタイム受信判定部９０９は、ＥＣＭ２２０の送出日時６０３と、時間情報取得部９０７から取得した現在時刻との差分を算出する。具体的には、リアルタイム受信判定部９０９は、ＥＣＭ２２０に含まれる２つの送出日時６０３のうち、少なくともどちらかの送出日時６０３を読み出す。次に、送出日時６０３と時間情報取得部９０７から取得した現在時刻との大小を比較し、送出日時６０３が大である場合は、送出日時６０３から現在時刻を減算した値を算出し、現在時刻が大である場合は、現在時刻から送出日時６０３を減算した値を算出する。
【０１４０】
Ｓ１４０３：リアルタイム受信判定部９０９は、Ｓ１４０２で算出した差分値が、予め保持する規定値以下であるか否かを判定する。差分値が規定値以下である場合は、Ｓ１４０４の処理に進む。差分値が規定値よりも大である場合は、Ｓ１４０５の処理に進む。
【０１４１】
Ｓ１４０４：リアルタイム受信判定部９０９は、コンテンツ及びＥＣＭ２２０が「リアルタイム受信」であると判定する。
【０１４２】
Ｓ１４０５：リアルタイム受信判定部９０９は、コンテンツ及びＥＣＭ２２０が「非リアルタイム受信」であると判定する。
【０１４３】
以上で、本実施の形態におけるリアルタイム受信判定処理の動作についての説明を終わる。
【０１４４】
次に、図１６のフローチャートを参照しながら、上記図１４におけるＳ１３０３の改竄検出処理の動作について説明を行う。
【０１４５】
Ｓ１５０１：改竄検出部９１０は、ＥＣＭ２２０に含まれる２つの送出日時６０３が一致するか否かを判定する。両者が一致する場合は、Ｓ１５０２の処理に進む。一方、両者が一致しない場合は、Ｓ１５０４の処理に進む。
【０１４６】
Ｓ１５０２：改竄検出部９１０は、ＥＣＭ２２０に含まれる２つの契約判定コード６０

４が一致するか否かを判定する。両者が一致する場合は、Ｓ１５０３の処理に進む。一方、両者が一致しない場合は、Ｓ１５０４の処理に進む。

【０１４７】

Ｓ１５０３：改竄検出部９１０は、ＥＣＭ２２０について、「ＥＣＭ改竄なし」と判定する。

【０１４８】

Ｓ１５０４：改竄検出部９１０は、ＥＣＭ２２０について、「ＥＣＭ改竄あり」と判定する。

【０１４９】

以上で、本実施の形態における改竄検出処理の動作についての説明を終わる。

【０１５０】

次に、図１７のフローチャートを参照しながら、図１４におけるＳ１３０５の契約内容判定処理の動作について説明を行う。

【０１５１】

Ｓ１６０１：契約内容判定部９１１は、ライセンス管理部９０４から、コンテンツに対応するライセンス２３０を読み出す。具体的には、契約内容判定部９１１は、ライセンス管理部９０４に対してワーク鍵ＩＤ６０２に対応するワーク鍵Ｋｗ２０３を含むライセンス２３０の送信を要求する。ライセンス管理部９０４は、当該ライセンス２３０をライセンス格納部９０１から検索して、ライセンス２３０を契約内容判定部９１１に送信する。

【０１５２】

Ｓ１６０２：契約内容判定部９１１は、ＥＣＭ２２０の送出日時６０３と、ライセンス２３０の開始日時４０４及び終了日時４０５との比較を行う。送出日時６０３が、開始日時４０４と終了日時４０５との間に含まれる場合は、Ｓ１６０３の処理を実行する。送出日時６０３が、開始日時４０４と終了日時４０５との間に含まれない場合は、Ｓ１６０６の処理を実行する。但し、開始日時４０４又は終了日時４０５のいずれかが無期限（期限設定なし）である場合には、開始日時４０４又は終了日時４０５と、送出日時６０３との比較は不要であり、送出日時６０３が開始日時４０４又は終了日時４０５内に含まれるものとして扱う。

【０１５３】

Ｓ１６０３：契約内容判定部９１１は、ライセンス２３０の契約コード４０３と、ＥＣＭ２２０の契約判定コード６０４とのＡＮＤ（論理積）を算出する。

【０１５４】

Ｓ１６０４：契約内容判定部９１１は、Ｓ１６０３の処理結果が「非０」であるか否かの判定を行う。Ｓ１６０３の処理結果が「非０」である場合は、Ｓ１６０５の処理に進む。一方、「非０」でない場合は、Ｓ１６０６の処理に進む。

【０１５５】

Ｓ１６０５：契約内容判定部９１１は、「契約あり」と判定する。

【０１５６】

Ｓ１６０６：契約内容判定部９１１は、「契約なし」と判定する。

【０１５７】

以上で、本実施の形態における契約内容判定処理の動作についての説明を終わる。

【０１５８】

なお、本実施の形態においては、ライセンスサーバ１０１が配信するライセンス２３０は、ＳＡＣを通じて配信するようにしたが、ＥＭＭ（Entitlement Management Message）と呼ばれる、ユーザβの端末装置１０３でのみ復号、取得可能なように暗号化及び改竄検出が施されたデータ形式で配信するようにしても良い。また、本実施の形態では、ライセンス２３０というデータ形式により配信するようにしたが、ライセンスサーバ１０１から端末装置１０３にライセンス２３０に含まれるようなデータ項目を配信できるものであれば、データ形式はこれに限られるものではない。

【０１５９】

また、本実施の形態において、端末装置１０３の時間情報取得部９０７、関連情報復号部９０８、送出時刻判定部９０９、改竄検出部９１０、契約内容判定部９１１など、特にセキュリティを必要とする情報の管理及び処理などを、ＩＣカード、セキュリティＬＳＩ等の耐タンパ化されたモジュールで行うようにしても良い。

【０１６０】

また、本実施の形態において、事業者α側のサーバシステム（ライセンスサーバ１０１、コンテンツサーバ１０２）の機能分担については、本実施の形態で示した構成に限られるものではなく、一部の機能が本実施の形態とは異なるサーバに含まれていても良いし、物理的に一体のサーバで実現するようにしても良い。

【０１６１】

また、本実施の形態においては、ユーザβの契約を示す情報として契約コード４０３（ティアビット）を用いているが、これに限られるものではなく、契約ＩＤなどの識別子により契約内容判定を行う場合にも、本発明が適用可能であることは言うまでもない。

【０１６２】

また、本実施の形態においては、コンテンツサーバ１０２でのコンテンツの暗号化に関し、コンテンツ暗号化部５０６で暗号化した後のＴＳパケットを多重化部５１０で多重化する場合の例を示したが、多重化部５１０で多重化後に、コンテンツをコンテンツ暗号化部５０６で暗号化する構成としても良い。

【０１６３】

また、本実施の形態におけるコンテンツサーバ１０２では、コンテンツＤＢ３０５に蓄積されたコンテンツを読み出し、コンテンツ符号化部５０４においてリアルタイムエンコードする場合の例を示したが、予めオフラインでＴＳを生成しておき、コンテンツ蓄積部５０１に蓄積しておくことにより、コンテンツ送出時にコンテンツ符号化部５０４におけるエンコード処理を省略するようにしても良い。

【０１６４】

また、本実施の形態におけるコンテンツサーバ１０２では、コンテンツ蓄積部５０１から送信するコンテンツを生成する場合の例を示したが、ライブ放送（生放送）など、コンテンツ蓄積部５０１を用いずに、ソースを直接、コンテンツ符号化部５０４に入力するようにしても良い。

【０１６５】

また、本実施の形態におけるコンテンツサーバ１０２では、スクランブル鍵生成部５０５においてスクランブル鍵Ｋｓ２０１を逐次生成するようにしたが、事前にスクランブル鍵Ｋｓ２０１を生成し、蓄積しておいたものを適用するようにしても良い。

【０１６６】

また、本実施の形態におけるＥＣＭ２２０の暗号化部のデータ配置について、図７に示すように、スクランブル鍵Ｋｓ（ｏｄｄ）６０６及びスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７を、送出日時６０３及び契約判定コード６０４の後続の暗号ブロックにアラインするように配置する場合の例を示したが、送出日時６０３、契約判定コード６０４に後続するスクランブル鍵Ｋｓ（ｏｄｄ）６０６又はスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７が、連続する２つの暗号ブロックに収まり、かつ、スクランブル鍵Ｋｓ（ｏｄｄ）６０６及びスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７が、連続する２つの暗号ブロックに跨るように配置するようにしても、本実施の形態の場合と同様に、改竄防止効果が得られる。

【０１６７】

また、本実施の形態では、出力制御情報４０６をライセンス２３０に含めるようにしたが、ＥＣＭ２２０に含まれるようにしても良い。この場合、例えば、ＥＣＭ２２０の２つのプライベートデータ６０５の位置に出力制御情報４０６を設定するようにし、端末装置１０３において、ＥＣＭ２２０の復号後に２箇所の出力制御情報４０６の一致確認を行うことにより、出力制御情報４０６の改竄検出を行う方法が考えられる。

【０１６８】

また、本実施の形態では、リアルタイム受信判定部９０９において、ＥＣＭ２２０の送

出日時６０３と時間情報取得部９０７との時刻比較の誤差の規定値をあらかじめ保持しておく場合の例を示したが、この規定値を事業者αから事業者単位、契約単位、コンテンツ単位などで動的に変更可能な構成としても良い。この場合、ＳＡＣを通じてライセンス２３０や信頼できる時刻情報と共に配信するようにしても良いし、ＥＣＭ２２０に含めて配信するようにしても良い。ＥＣＭ２２０に含める場合、例えば、ＥＣＭ２２０の２箇所のプライベートデータ６０５の位置に規定値を設定するようにし、端末装置１０３において、ＥＣＭ２２０の復号後に２箇所の規定値の一致確認を行うことにより、規定値の改竄検出を行う方法が考えられる。また、出力制御情報４０６の内容に応じて、リアルタイム受信判定処理を行わない運用にしても良い。例えば、出力制御情報４０６のＣＣＩがコピーフリー（Copy Free）であったり、書き出しが許可されていない場合には、この処理を行わないとする運用なども考えられる。

【０１６９】

また、本実施の形態では、端末装置１０３で、ライセンス格納部９０１にワーク鍵Ｋｗ２０３（ライセンス２３０）を蓄積する構成を示したが、必要に応じて、適宜ライセンスサーバ１０１からワーク鍵Ｋｗ２０３を都度取得、保持する構成としても良い。

【０１７０】

また、本実施の形態における端末装置１０３の処理について、リアルタイム受信判定部９０９、改竄検出部９１０、契約内容判定部９１１の処理の順序は、本実施の形態で示した処理順序に限られるのではなく、処理順序を必要に応じて入れ替えるようにしても良い。

【０１７１】

また、本実施の形態において、リアルタイム受信か否かの判定において、ＥＣＭ２２０に有効期限を付加しておき、時間情報取得部９０７が管理する現在時刻がＥＣＭの有効期限以降である場合は、「非リアルタイム受信」であると判定することとしてもよい。

【０１７２】

なお、本実施の形態における上記図１４のＳ１３０２で「非リアルタイム受信」であると判定した場合、及びＳ１３０４で「ＥＣＭ改竄あり」と判定した場合、及びＳ１３０６で「契約なし」と判定した場合、端末装置１０３は、スクランブル鍵Ｋｓ（ｏｄｄ）６０６及びスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７を取得できないとして説明を行ったが、これに限るわけではなく、スクランブル鍵Ｋｓ（ｏｄｄ）６０６及びスクランブル鍵Ｋｓ（ｅｖｅｎ）６０７の取得に成功し、その後、以下のようなエラー処理を行うこととしてもよい。

【０１７３】

（１）特定の動作のみを禁止する。例えば、再生は許可するが、録画は非許可とするなどがある。これにより、例えば事業者αのミスで送出日時６０３に誤りがあった場合などでも、ユーザβはコンテンツの視聴は行うことができるようになる。

【０１７４】

（２）異常なコンテンツを受信した旨や、カスタマセンタへの通知を促すなど所定の警告メッセージ（例えば、「異常なコンテンツを受信しました。ＸＸＸに連絡します。」）を表示する。これにより、コンテンツの不正利用の抑止や、正規ユーザからの電話等での通報により、異常なコンテンツが送信されていることを事業者αが把握することが可能となる。

【０１７５】

（３）事業者αにエラー内容（非リアルタイム受信が発生している、ＥＣＭが改竄されているなど）やエラーが発生したＥＣＭの内容を通知する（その際、ユーザの許諾を得ることとしてもよい。）。これにより、不正利用の抑止や、異常なコンテンツが送信されていることを事業者が把握することが可能となる。

【０１７６】

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【０１７７】
（１）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又はハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。
【０１７８】
（２）上記の各装置を構成する構成要素の一部又は全部が、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムＬＳＩは、その機能を達成する。
【０１７９】
（３）上記の各装置を構成する構成要素の一部又は全部が、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしてもよい。前記ＩＣカード又は前記モジュールが、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムであるとしても、前記ＩＣカード又は前記モジュールが、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ＩＣカード又は前記モジュールは、その機能を達成する。このＩＣカード又はこのモジュールが、耐タンパ性を有するとしてもよい。
【０１８０】
（４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。
【０１８１】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Blue-ray Disc）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。
【０１８２】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。
【０１８３】
また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。
【０１８４】
また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム若しくは前記デジタル信号を、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。
【０１８５】
（５）上記実施の形態及び上記変形例をそれぞれ組み合わせることとしてもよい。
【産業上の利用可能性】
【０１８６】

本発明に係るコンテンツ配信システム及び方法は、デジタル放送、ＣＡＴＶ、インターネット等によるコンテンツ配信サービスを行うシステム、及びそれに含まれるサーバ、端末装置等において有用である。

【図面の簡単な説明】

【０１８７】

【図１】本発明に係るコンテンツ配信システムの全体構成を示すブロック図である。

【図２】本発明に係るコンテンツ配信システムの概要を示すブロック図である。

【図３】本発明に係るコンテンツ配信システムにおけるコンテンツの暗号スキームを示す図である。

【図４】本発明に係るライセンスサーバの機能構成を示すブロック図である。

【図５】本発明に係るライセンスサーバのライセンス生成部が生成するライセンスの一例を示す図である。

【図６】本発明に係るコンテンツサーバの機能構成を示すブロック図である。

【図７】本発明に係るＥＣＭの一例を示す図である。

【図８】本発明に係るＥＣＭの暗号化部のデータ配置を示す図である。

【図９】本発明に係る契約コードと契約判定コードとに基づく契約内容判定処理の手順を示す図である。

【図１０】本発明に係る端末装置の構成を示すブロック図である。

【図１１】本発明に係るライセンス送受信の動作を示すフローチャートである。

【図１２】本発明に係るコンテンツ送出処理の動作を示すフローチャートである。

【図１３】本発明に係るコンテンツ受信処理の動作を示すフローチャートである。

【図１４】本発明に係るＥＣＭ判定処理の動作を示すフローチャートである。

【図１５】本発明に係るリアルタイム受信判定処理の動作を示すフローチャートである。

【図１６】本発明に係る改竄検出処理の動作を示すフローチャートである。

【図１７】本発明に係る契約内容判定処理の動作を示すフローチャートである。

【図１８】従来のコンテンツ配信システムの問題を説明するための図である。

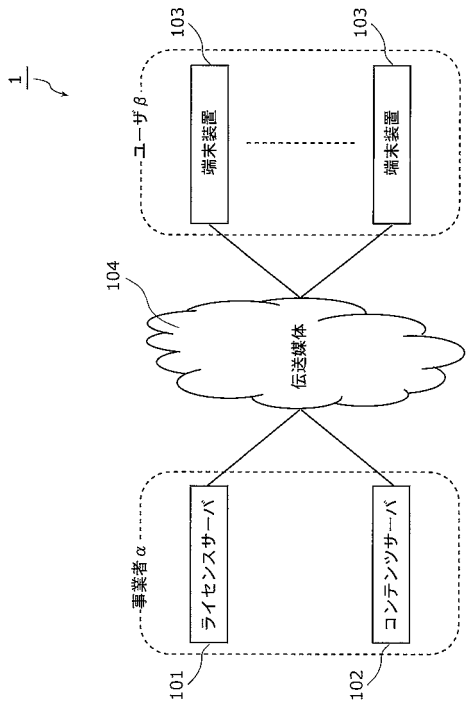
【符号の説明】

【０１８８】

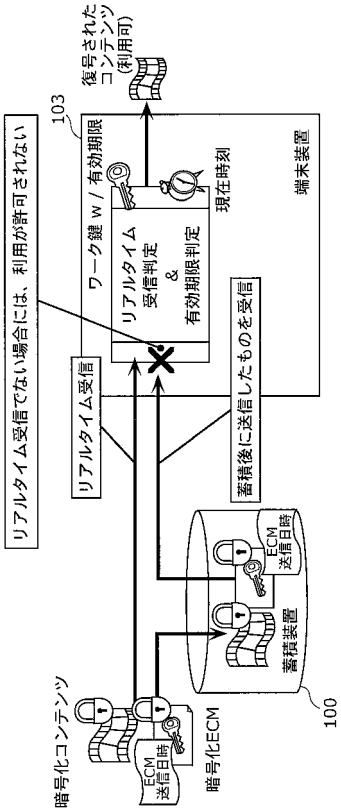
１００	蓄積装置
１０１	ライセンスサーバ
１０２	コンテンツサーバ
１０３	端末装置
１０４	伝送媒体
２０１	スクランブル鍵Ｋｓ
２０３、４０１	ワーク鍵Ｋｗ
２０５	セッション鍵Ｋｓｅ
２２０	ＥＣＭ
２３０	ライセンス
３０１、５０３	ワーク鍵蓄積部
３０２	契約情報蓄積部
３０３、９０２	固有情報管理部
３０４	ライセンス生成部
３０５	ライセンス送信部
４０２、６０２	ワーク鍵ＩＤ
４０３	契約コード
４０４	開始日時
４０５	終了日時
４０６	出力制御情報
５０１	コンテンツ蓄積部
５０２	コンテンツ属性情報蓄積部

５０４	コンテンツ符号化部
５０５	スクランブル鍵生成部
５０６	コンテンツ暗号化部
５０７	送出日時特定部
５０８	関連情報生成部
５０９	関連情報暗号化部
５１０	多重化部
５１１	送出部
６０１	フォーマットバージョン
６０３	送出日時
６０４	契約判定コード
６０５	プライベートデータ
６０６	スクランブル鍵（ｏｄｄ）
６０７	スクランブル鍵（ｅｖｅｎ）
６１５	出力制御情報
９０１	ライセンス格納部
９０３	ライセンス受信部
９０４	ライセンス管理部
９０５	コンテンツ受信部
９０６	分離部
９０７	時間情報取得部
９０８	関連情報復号部
９０９	リアルタイム受信判定部
９１０	改竄検出部
９１１	契約内容判定部
９１２	コンテンツ利用制御部
９１３	コンテンツ格納制御部
１０３０	端末装置

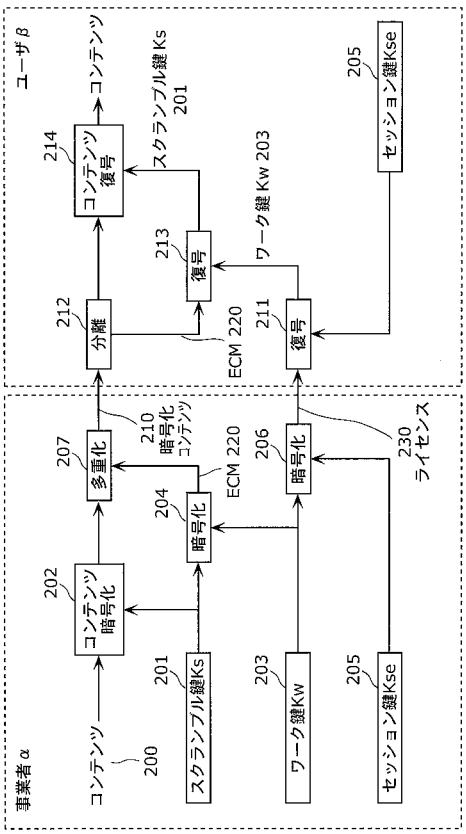
【図１】


1
ユーザ β
103
端末装置
103
端末装置
104
伝送媒体
事業者 α
ライセンスサーバ
コンテンツサーバ
101
102

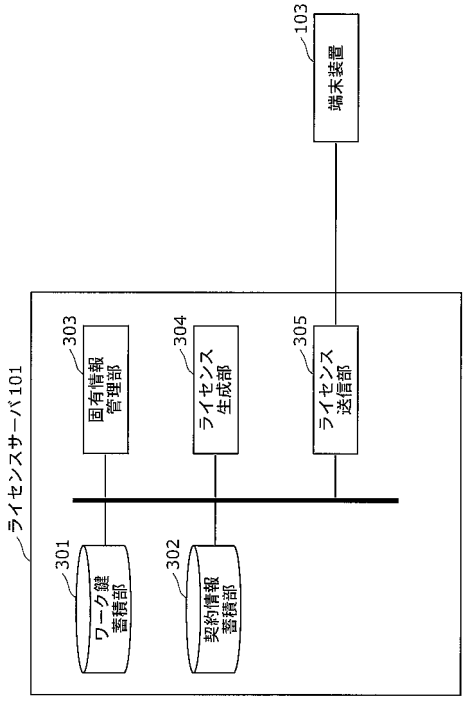
【図２】


復号されたコンテンツ(利用可)
103
リアルタイム受信でない場合には、利用が許可されない
ワーク鍵 w / 有効期限
リアルタイム受信判定 & 有効期限判定
現在時刻
端末装置
リアルタイム受信
蓄積後に送信したものを受信
ECM送信日時
蓄積装置
暗号化コンテンツ
暗号化ECM
100

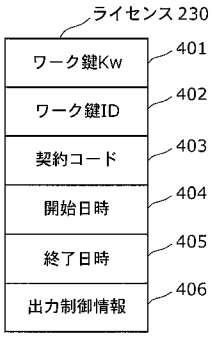
【図３】


ユーザ β
コンテンツ
214
コンテンツ復号
スクランブル鍵 Ks
201
213
復号
ワーク鍵 Kw 203
205
セッション鍵Kse
212
分離
ECM 220
211
復号
事業者 α
コンテンツ
200
202
コンテンツ暗号化
207
多重化
210
暗号化コンテンツ
201
スクランブル鍵Ks
204
暗号化
ECM 220
206
暗号化
230
ライセンス
203
ワーク鍵Kw
205
セッション鍵Kse

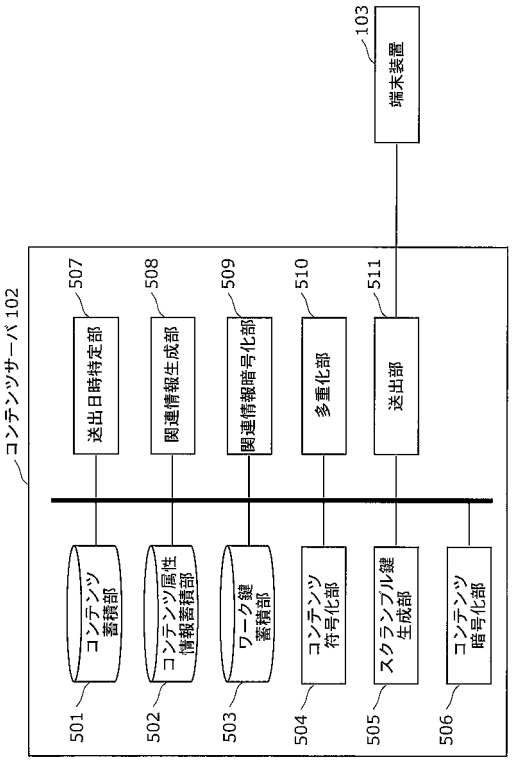
【図４】


103
端末装置
ライセンスサーバ 101
303
固有情報管理部
304
ライセンス生成部
305
ライセンス送信部
301
ワーク鍵蓄積部
302
契約情報蓄積部

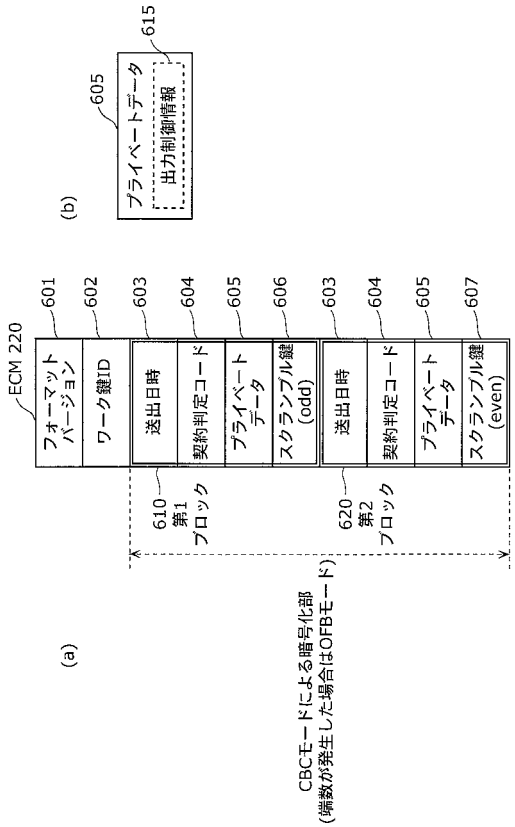
【図５】


ライセンス 230
ワーク鍵Kw
401
ワーク鍵ID
402
契約コード
403
開始日時
404
終了日時
405
出力制御情報
406

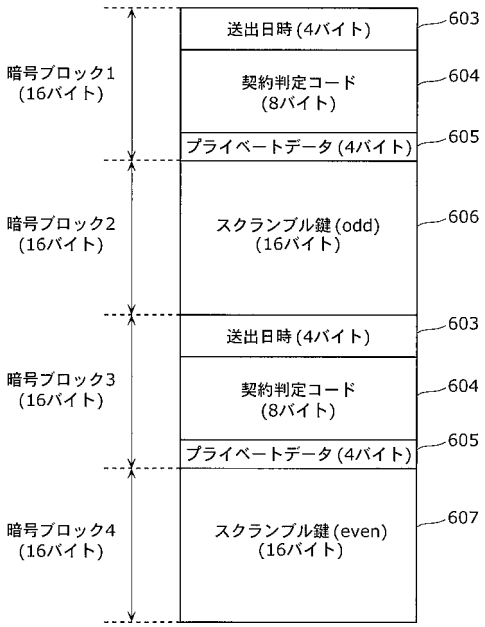
【図６】


103
端末装置
コンテンツサーバ 102
507
送出日時特定部
508
関連情報生成部
509
関連情報暗号化部
510
多重化部
511
送出部
コンテンツ蓄積部
コンテンツ属性情報蓄積部
ワーク鍵蓄積部
コンテンツ符号化部
スクランブル鍵生成部
コンテンツ暗号化部
501
502
503
504
505
506

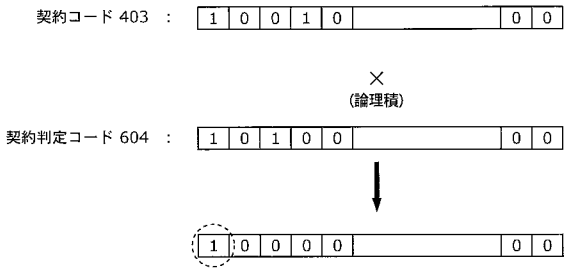
【図７】


(b)
615
605
プライベートデータ
出力制御情報
(a)
ECM 220
601
フォーマットバージョン
602
ワーク鍵ID
603
送出日時
604
契約判定コード
605
プライベートデータ
606
スクランブル鍵(odd)
603
送出日時
604
契約判定コード
605
プライベートデータ
607
スクランブル鍵(even)
610
第1ブロック
620
第2ブロック
CBCモードによる暗号化部
(端数が発生した場合はOFBモード)

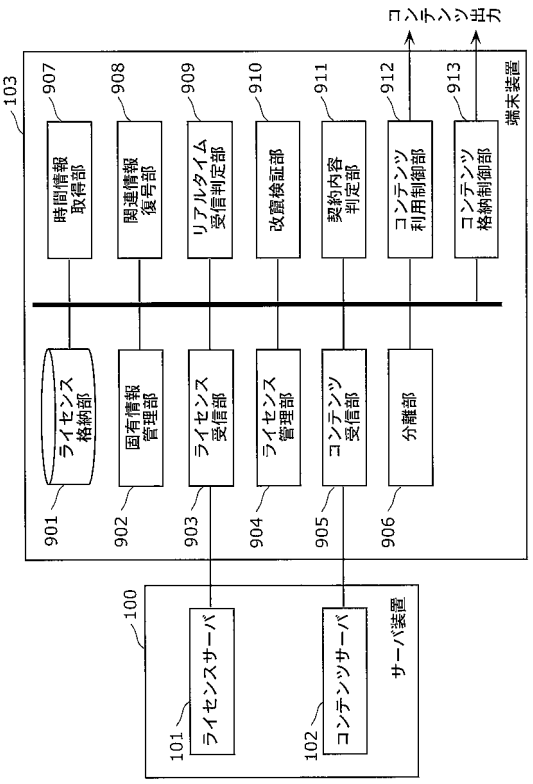
【図８】


暗号ブロック1
(16バイト)
送出日時(4バイト)
603
契約判定コード
(8バイト)
604
プライベートデータ(4バイト)
605
暗号ブロック2
(16バイト)
スクランブル鍵(odd)
(16バイト)
606
暗号ブロック3
(16バイト)
送出日時(4バイト)
603
契約判定コード
(8バイト)
604
プライベートデータ(4バイト)
605
暗号ブロック4
(16バイト)
スクランブル鍵(even)
(16バイト)
607

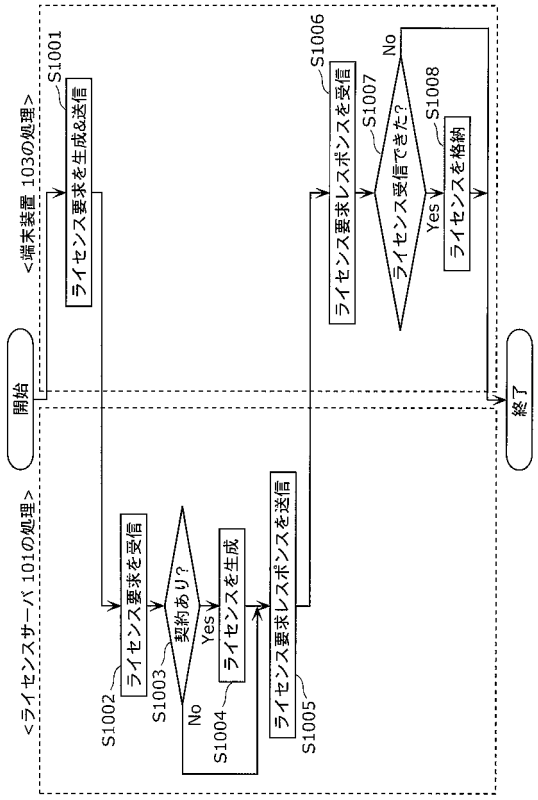
【図９】



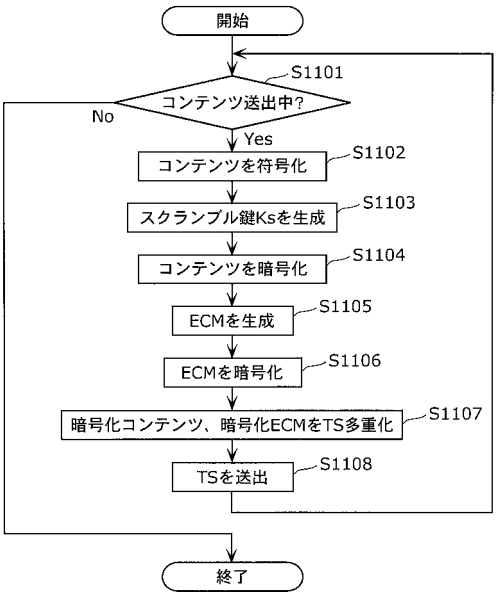
【図１０】



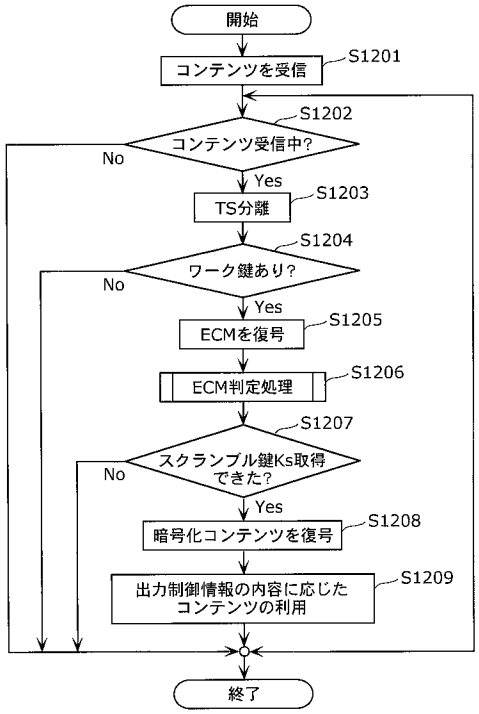
【図１１】



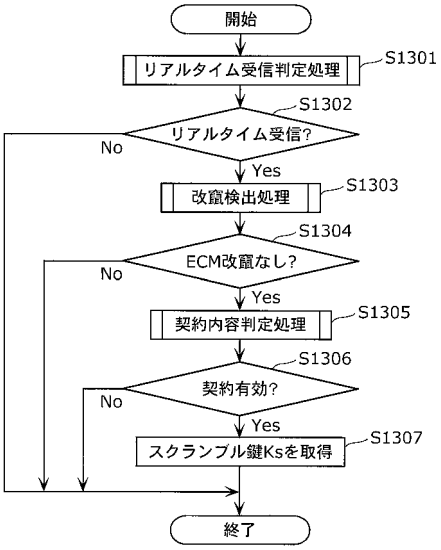
【図１２】



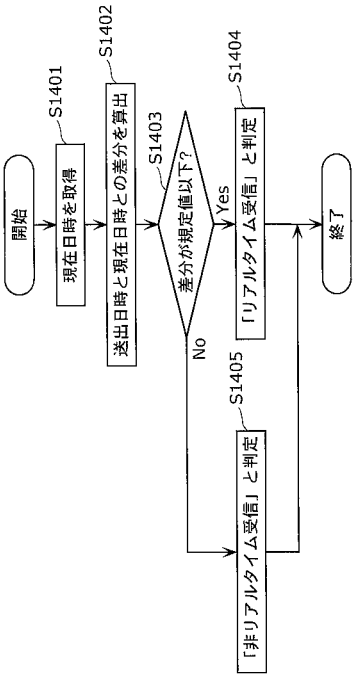
【図１３】



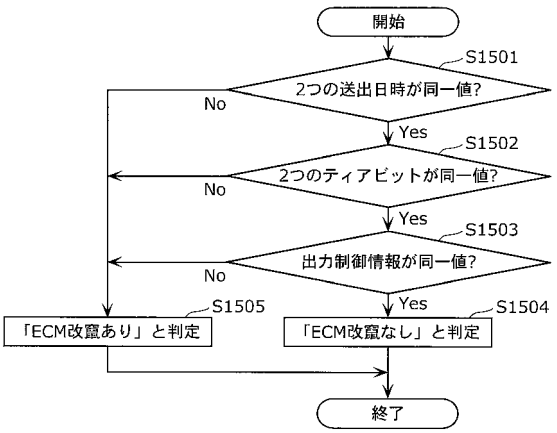
【図１４】



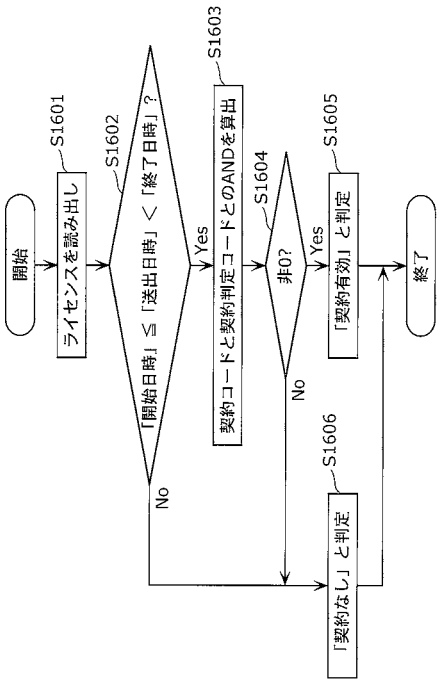
【図１５】



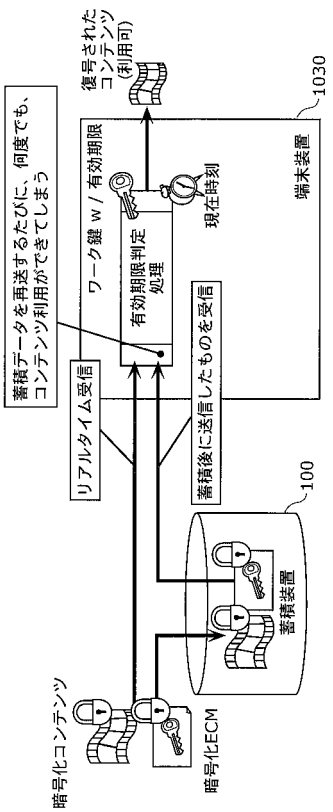
【図１６】



【図１７】


開始
S1601
ライセンスを読み出し
S1602
「開始日時」≦「送出日時」＜「終了日時」？
Yes
No
S1603
契約コードと契約判定コードとのANDを算出
S1604
非0?
Yes
No
S1605
「契約有効」と判定
S1606
「契約なし」と判定
終了

【図１８】


復号されたコンテンツ(利用可)
1030
端末装置
蓄積データを再送するたびに、何度でも、コンテンツ利用ができてしまう
ワーク鍵 w / 有効期限
有効期限判定処理
現在時刻
リアルタイム受信
蓄積後に送信したものを受信
100
蓄積装置
暗号化コンテンツ
暗号化ECM

フロントページの続き

(51)Int.Cl. FI
G06F 12/14 560C
G06F 12/14 540A

(72)発明者 徳田 克己
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

審査官 速水 雄太

(56)参考文献 特開平１０－３４１２１２（ＪＰ，Ａ）
特開２００４－５１５９７２（ＪＰ，Ａ）
特開２００５－１６００３２（ＪＰ，Ａ）
特開２００４－３０４６００（ＪＰ，Ａ）
特開２００２－２１８４３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｇ０６Ｆ ２１／２４
Ｈ０４Ｎ ７／１６７
Ｈ０４Ｎ ７／１７３