

(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2010-21615

(P2010-21615A)

(43) 公開日 平成22年1月28日(2010.1.28)

(51) Int.Cl.		F I				テーマコード (参考)
HO 4 L	9/08	(2006.01)	HO 4 L	9/00	6 O 1 B	5 C 1 6 4
HO 4 N	7/167	(2006.01)	HO 4 N	7/167	Z	5 J 1 0 4
HO 4 N	7/173	(2006.01)	HO 4 N	7/173	6 1 0 Z	
HO 4 L	9/14	(2006.01)	HO 4 N	7/173	6 3 0	
			HO 4 L	9/00	6 4 1	
審査請求 有 請求項の数 8 O L (全 30 頁) 最終頁に続く						

(21) 出願番号	特願2008-177708 (P2008-177708)	(71) 出願人	000002185
(22) 出願日	平成20年7月8日 (2008.7.8)		ソニー株式会社
			東京都港区港南1丁目7番1号
		(74) 代理人	100095957
			弁理士 亀谷 美明
		(74) 代理人	100096389
			弁理士 金本 哲男
		(74) 代理人	100101557
			弁理士 萩原 康司
		(74) 代理人	100128587
			弁理士 松本 一騎
		(72) 発明者	小笠原 好一
			東京都港区港南1丁目7番1号 ソニー株式会社内
最終頁に続く			

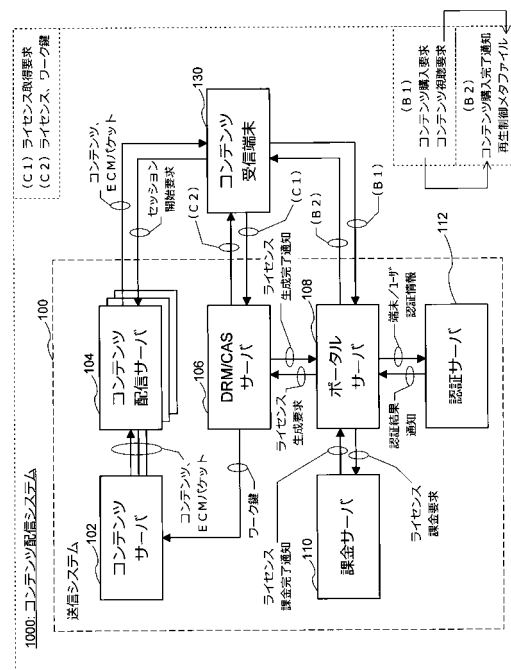
(54) 【発明の名称】 コンテンツ配信システム、コンテンツ受信端末、コンテンツ配信方法、及びストリーミングコンテンツの視聴処理方法

(57) 【要約】

【課題】ストリーミングコンテンツのライセンス管理方法を提供すること。

【解決手段】スクランブルが施されたコンテンツを配信すると共に、スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信する複数のコンテンツ配信サーバと、所定のコンテンツ配信サーバから配信される暗号化されたスクランブル鍵を復号するためのワーク鍵を提供するライセンスサーバと、所定のコンテンツ配信サーバのアドレス情報を提供するポータルサーバと、ポータルサーバから所定のコンテンツ配信サーバのアドレス情報を取得し、アドレス情報を参照して所定のコンテンツ配信サーバからコンテンツ及びスクランブル鍵を取得し、ライセンスサーバから取得したワーク鍵を用いてスクランブル鍵を復号し、スクランブル鍵を用いてコンテンツのスクランブルを解除するコンテンツ受信端末とを含むシステムが提供される。

【選択図】 図3



【特許請求の範囲】**【請求項 1】**

スクランブルが施されたコンテンツを配信すると共に、前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信する複数のコンテンツ配信サーバと；

所定の前記コンテンツ配信サーバから配信される前記暗号化されたスクランブル鍵を復号するためのワーク鍵を提供するライセンスサーバと；

前記所定のコンテンツ配信サーバのアドレス情報を提供するポータルサーバと；

前記ポータルサーバから前記所定のコンテンツ配信サーバのアドレス情報を取得するアドレス情報取得部と、前記アドレス情報取得部により取得されたアドレス情報を参照して前記所定のコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵を取得するコンテンツ取得部と、前記ライセンスサーバから取得したワーク鍵を用いて前記スクランブル鍵を復号するスクランブル鍵復号部と、前記スクランブル鍵を用いて前記コンテンツのスクランブルを解除するスクランブル解除部と、を有するコンテンツ受信端末と；を含む、コンテンツ配信システム。

10

【請求項 2】

前記ポータルサーバは、前記所定のコンテンツ配信サーバの再生制御方式を示す情報をさらに提供し、

前記コンテンツ受信端末は、前記ポータルサーバから再生制御方式の情報を取得する再生制御情報取得部をさらに有し、前記再生制御情報取得部により取得された情報が示す再生制御方式に従って前記コンテンツ取得部により前記コンテンツ及びスクランブル鍵を取得する、請求項 1 に記載のコンテンツ配信システム。

20

【請求項 3】

前記コンテンツ配信システムは、コンテンツ鍵を用いて復号可能な暗号化されたコンテンツのみを配信するコンテンツ配信サーバをさらに含み、

前記ライセンスサーバは、所定の前記コンテンツ配信サーバにより配信されるコンテンツの配信形態に応じて前記ワーク鍵又は前記コンテンツ鍵を提供し、

前記ポータルサーバは、前記所定のコンテンツ配信サーバにより配信されるコンテンツの配信形態を示す情報をさらに提供し、

前記コンテンツ受信端末は、前記所定のコンテンツ配信サーバにより配信されるコンテンツの配信形態を示す情報を前記ポータルサーバから取得する配信形態取得部と、前記ライセンスサーバから取得したコンテンツ鍵を用いて前記暗号化されたコンテンツを復号するコンテンツ復号部と、をさらに有し、前記配信形態取得部により取得された情報が示す配信形態がコンテンツ鍵方式を利用する配信形態である場合、前記コンテンツ取得部により前記暗号化されたコンテンツを取得し、前記コンテンツ復号部によりコンテンツを復号する、請求項 1 に記載のコンテンツ配信システム。

30

【請求項 4】

前記コンテンツ受信端末が有するスクランブル鍵復号部は、前記コンテンツ取得部によりコンテンツ及びスクランブル鍵が提供される配信形態を利用したコンテンツを取得開始する際に前記ライセンスサーバからワーク鍵を取得する、請求項 1 に記載のコンテンツ配信システム。

40

【請求項 5】

前記コンテンツ受信端末が有するコンテンツ復号部は、前記コンテンツ取得部により前記暗号化されたコンテンツの取得を行う際に前記ライセンスサーバからコンテンツ鍵を取得する、請求項 3 に記載のコンテンツ配信システム。

【請求項 6】

スクランブルが施されたコンテンツ及び前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信するコンテンツ配信サーバ、又はコンテンツ鍵を用いて復号可能な暗号化されたコンテンツを配信するコンテンツ配信サーバのアドレス情報を取得するアドレス情報取得部と、

50

前記アドレス情報に対応するコンテンツ配信サーバから配信されるコンテンツの配信形態が示された情報を取得する配信形態取得部と、

前記アドレス情報取得部により取得されたアドレス情報を参照し、前記配信形態取得部により取得された情報に示された配信形態に応じて、当該アドレス情報に対応するコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵、或いは、前記暗号化されたコンテンツを取得するコンテンツ取得部と、

前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を復号するためのワーク鍵を取得し、前記配信形態がコンテンツ鍵方式を利用する場合に前記コンテンツ鍵を取得する鍵取得部と、

前記配信形態がワーク鍵方式を利用する場合に前記ワーク鍵を用いて前記スクランブル鍵を復号するスクランブル鍵復号部と、

前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を用いてコンテンツのスクランブルを解除し、前記配信形態がコンテンツ鍵方式の場合に前記コンテンツ鍵を用いて前記暗号化されたコンテンツを復号するコンテンツ復号部と、
を有する、コンテンツ受信端末。

【請求項 7】

スクランブルが施されたコンテンツを配信すると共に、前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信する所定のコンテンツ配信サーバのアドレス情報がポータルサーバから取得されるアドレス取得ステップと、

前記所定のコンテンツ配信サーバから配信される前記暗号化されたスクランブル鍵を復号するためのワーク鍵がライセンスサーバから取得されるワーク鍵取得ステップと、

前記アドレス取得ステップで取得されたアドレス情報を参照して前記所定のコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵が取得されるコンテンツ取得ステップと、

前記ワーク鍵取得ステップで取得されたワーク鍵を用いて前記スクランブル鍵が復号されるスクランブル鍵復号ステップと、

前記スクランブル鍵復号ステップで復号されたスクランブル鍵を用いて前記コンテンツのスクランブルが解除されるスクランブル解除ステップと、
を含む、コンテンツ配信方法。

【請求項 8】

スクランブルが施されたコンテンツ及び前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信するコンテンツ配信サーバ、又はコンテンツ鍵を用いて復号可能な暗号化されたコンテンツのみを配信するコンテンツ配信サーバのアドレス情報が取得されるアドレス情報取得ステップと、

前記アドレス情報に対応するコンテンツ配信サーバから配信されるコンテンツの配信形態が示された情報が取得される配信形態取得ステップと、

前記アドレス情報取得ステップで取得されたアドレス情報を参照し、前記配信形態取得ステップで取得された情報に示された配信形態に応じて、当該アドレス情報に対応するコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵、或いは、前記暗号化されたコンテンツが取得されるコンテンツ取得ステップと、

前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を復号するためのワーク鍵が取得され、前記配信形態がコンテンツ鍵方式の場合に前記コンテンツ鍵が取得される鍵取得ステップと、

前記配信形態がワーク鍵方式を利用する場合に前記ワーク鍵を用いて前記スクランブル鍵が復号されるスクランブル鍵復号ステップと、

前記配信形態がワーク鍵方式の場合に前記スクランブル鍵を用いてコンテンツのスクランブルが解除され、前記配信形態がコンテンツ鍵方式の場合に前記コンテンツ鍵を用いて前記暗号化されたコンテンツが復号されるコンテンツ復号ステップと、
を含む、ストリーミングコンテンツの視聴処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、コンテンツ配信システム、コンテンツ受信端末、コンテンツ配信方法、及びストリーミングコンテンツの視聴処理方法に関する。

【背景技術】

【0002】

近年、情報処理技術、及び通信技術の急速な発展に伴い、多くの音楽コンテンツや映像コンテンツ等は劣化の少ないデジタルデータとして扱われ、各種の通信網を通じて配信されるようになってきている。デジタルデータは、複数回のコピーを繰り返したり、長い距離の通信を経たりしても劣化しないという性質を持っている。

10

【0003】

このような性質があるため、昨今、デジタルコンテンツが不正にコピーされ、インターネット等の広域通信網を介して不正に配布されてしまう事例が後を絶たない。このような不正行為に対抗するため、コンテンツのストリーミング配信等においては、例えば、デジタルコンテンツの利用や配布を制限するためのデジタル著作権管理(DRM; Digital Rights Management)と呼ばれる技術が用いられている。また、地上デジタル放送においては、CAS(Conditional Access System)と呼ばれる限定受信方式が用いられている。

【0004】

このようなコンテンツ配信に関する技術として、例えば、下記の特許文献1には、動画コンテンツを複数のコンテンツパーツに分割し、各コンテンツパーツを暗号化して配信するコンテンツ配信システムの構成が記載されている。また、下記の特許文献2には、利用者がストリーミングコンテンツを一定時間内だけしか視聴できないように制限するための技術が記載されている。さらに、下記の特許文献3には、メタファイル及びMIMEタイプ情報の生成処理を行うメタファイル管理サーバを含むストリームコンテンツ配信システムの構成が記載されている。

20

【0005】

【特許文献1】特開2006-222674号公報

【特許文献2】特開2003-150492号公報

【特許文献3】特開2005-110310号公報

30

【発明の開示】

【発明が解決しようとする課題】

【0006】

DRMやCASを用いた従来のシステムとしては、例えば、コンテンツに施された暗号を解除して視聴できるようにするための復号鍵をライセンス契約を締結した視聴者に直接提供する方法がある。この方式を用いたライセンス形式の一例としては、VOD(Video on Demand)ライセンス形式がある。VODライセンス形式の場合、視聴者は、ポータルサーバにアクセスしてライセンス契約を締結し、コンテンツの取得先を示すアドレス情報を取得する。そして、視聴者は、取得したアドレス情報が示すコンテンツ配信サーバにアクセスしてコンテンツを取得し、提供された復号鍵を用いてコンテンツを復号することで視聴することができるようになる。

40

【0007】

一方、コンテンツに施されたスクランブルを解除するためのスクランブル鍵をさらに暗号化し、その暗号化を解除するためのワーク鍵をライセンス契約した視聴者に提供する方法がある。この方式の場合、暗号化されたスクランブル鍵は、スクランブルされたコンテンツと共に視聴者に提供される。このような二重暗号化方式を用いるライセンス形式としては、例えば、マルチキャストライセンス形式(以下、MCライセンス形式)がある。MCライセンス形式の場合、視聴者は、例えば、チャンネル単位で設置された複数のコンテンツ配信サーバの中から所望のコンテンツが置かれたコンテンツ配信サーバにアクセスしてコンテンツを取得する。そして、視聴者は、ワーク鍵でスクランブル鍵を復号し、その

50

スクランブル鍵を用いてコンテンツをデスクランブルすることで視聴可能になる。

【 0 0 0 8 】

上記の V o D ライセンス形式の場合、ポータルサーバからコンテンツの取得先を指定できるため、コンテンツ単位でライセンスの管理ができるという利点がある。しかし、コンテンツを単純に暗号化して配信しているため、コンテンツの制作者が暗号化を行うと、コンテンツの配信者がライセンスを管理することが難しくなる。また、コンテンツの配信者が暗号化を行うと、コンテンツの制作者がライセンスを管理することが難しくなる。また、リアルタイムな映像を配信したい場合にコンテンツ単位で暗号化することも困難である。一方、上記の M C ライセンス形式の場合、ライセンス契約を締結した視聴者が各コンテンツ配信サーバから提供されるコンテンツを任意に視聴できるように、マルチキャストライセンスにしている。そのため、コンテンツ単位又は所定のコンテンツグループに対してライセンスを供与するような配信形態を実現することが難しい。また、コンテンツ単位で接続先の変更を実現することも困難である。

10

【 0 0 0 9 】

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、コンテンツの制作者及び配信者等が各々ライセンスを管理することが可能であり、さらに、コンテンツの配信者等がコンテンツ単位でライセンスを管理することが可能な、新規かつ改良されたコンテンツ配信システム、コンテンツ受信端末、コンテンツ配信方法、及びストリーミングコンテンツの視聴処理方法を提供することにある。

20

【課題を解決するための手段】

【 0 0 1 0 】

上記課題を解決するために、本発明のある観点によれば、スクランブルが施されたコンテンツを配信すると共に、前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信する複数のコンテンツ配信サーバと；所定の前記コンテンツ配信サーバから配信される前記暗号化されたスクランブル鍵を復号するためのワーク鍵を提供するライセンスサーバと；前記所定のコンテンツ配信サーバのアドレス情報を提供するポータルサーバと；前記ポータルサーバから前記所定のコンテンツ配信サーバのアドレス情報を取得するアドレス情報取得部と、前記アドレス情報取得部により取得されたアドレス情報を参照して前記所定のコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵を取得するコンテンツ取得部と、前記ライセンスサーバから取得したワーク鍵を用いて前記スクランブル鍵を復号するスクランブル鍵復号部と、前記スクランブル鍵を用いて前記コンテンツのスクランブルを解除するスクランブル解除部と、を有するコンテンツ受信端末と；を含む、コンテンツ配信システムが提供される。

30

【 0 0 1 1 】

また、前記ポータルサーバは、前記所定のコンテンツ配信サーバの再生制御方式を示す情報をさらに提供するように構成されていてもよい。さらに、前記コンテンツ受信端末は、前記ポータルサーバから再生制御方式の情報を取得する再生制御情報取得部をさらに有し、前記再生制御情報取得部により取得された情報が示す再生制御方式に従って前記コンテンツ取得部により前記コンテンツ及びスクランブル鍵を取得するように構成されていてもよい。

40

【 0 0 1 2 】

また、前記コンテンツ配信システムは、コンテンツ鍵を用いて復号可能な暗号化されたコンテンツを配信するコンテンツ配信サーバをさらに含んでもよい。さらに、前記ライセンスサーバは、所定の前記コンテンツ配信サーバにより配信されるコンテンツの配信形態に応じて前記ワーク鍵又は前記コンテンツ鍵を提供するように構成されていてもよい。そして、前記ポータルサーバは、前記所定のコンテンツ配信サーバにより配信されるコンテンツの配信形態を示す情報をさらに提供するように構成されていてもよい。この場合、前記コンテンツ受信端末は、前記所定のコンテンツ配信サーバにより配信されるコンテンツの配信形態を示す情報を前記ポータルサーバから取得する配信形態取得部と、前記ライセンスサーバから取得したコンテンツ鍵を用いて前記暗号化されたコンテンツを復号す

50

るコンテンツ復号部と、をさらに有するように構成される。そして、コンテンツ受信端末は、前記配信形態取得部により取得された情報が示す暗号化形態がコンテンツ鍵方式である場合、前記コンテンツ取得部により前記暗号化されたコンテンツを取得し、前記コンテンツ復号部によりコンテンツを復号する。

【 0 0 1 3 】

また、前記コンテンツ受信端末が有するスクランブル鍵復号部は、前記コンテンツ取得部によりコンテンツ及びスクランブル鍵が取得される配信形態でのコンテンツ受信を開始する際に前記ライセンスサーバからワーク鍵を取得するように構成されていてもよい。

【 0 0 1 4 】

また、前記コンテンツ受信端末が有するコンテンツ復号部は、前記コンテンツ取得部により前記暗号化されたコンテンツの取得を行う際に前記ライセンスサーバからコンテンツ鍵を取得するように構成されていてもよい。

【 0 0 1 5 】

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、スクランブルが施されたコンテンツ及び前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信するコンテンツ配信サーバ、又はコンテンツ鍵を用いて復号可能な暗号化されたコンテンツを配信するコンテンツ配信サーバのアドレス情報を取得するアドレス情報取得部と、前記アドレス情報に対応するコンテンツ配信サーバから配信されるコンテンツの配信形態が示された情報を取得する配信形態取得部と、前記アドレス情報取得部により取得されたアドレス情報を参照し、前記配信形態取得部により取得された情報に示された配信形態に応じて、当該アドレス情報に対応するコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵、或いは、前記暗号化されたコンテンツを取得するコンテンツ取得部と、前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を復号するためのワーク鍵を取得し、前記配信形態がコンテンツ鍵方式の場合に前記コンテンツ鍵を取得する鍵取得部と、前記配信形態がワーク鍵方式を利用する場合に前記ワーク鍵を用いて前記スクランブル鍵を復号するスクランブル鍵復号部と、前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を用いてコンテンツのスクランブルを解除し、前記配信形態がコンテンツ鍵方式の場合に前記コンテンツ鍵を用いて前記暗号化されたコンテンツを復号するコンテンツ復号部と、を有する、コンテンツ受信端末が提供される。

【 0 0 1 6 】

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、スクランブルが施されたコンテンツを配信すると共に、前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信する所定のコンテンツ配信サーバのアドレス情報がポータルサーバから取得されるアドレス取得ステップと、前記所定のコンテンツ配信サーバから配信される前記暗号化されたスクランブル鍵を復号するためのワーク鍵がライセンスサーバから取得されるワーク鍵取得ステップと、前記アドレス取得ステップで取得されたアドレス情報を参照して前記所定のコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵が取得されるコンテンツ取得ステップと、前記ワーク鍵取得ステップで取得されたワーク鍵を用いて前記スクランブル鍵が復号されるスクランブル鍵復号ステップと、前記スクランブル鍵復号ステップで復号されたスクランブル鍵を用いて前記コンテンツのスクランブルが解除されるスクランブル解除ステップと、を含む、コンテンツ配信方法が提供される。

【 0 0 1 7 】

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、スクランブルが施されたコンテンツ及び前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信するコンテンツ配信サーバ、又はコンテンツ鍵を用いて復号可能な暗号化されたコンテンツのみを配信するコンテンツ配信サーバのアドレス情報が取得されるアドレス情報取得ステップと、前記アドレス情報に対応するコンテンツ配信サーバから配信されるコンテンツの配信形態が示された情報が取得される配信形態取得ステップと、前記アドレス情報取得ステップで取得されたアドレス情報を参照し、前記配信形態取得ステップで

取得された情報に示された配信形態に応じて、当該アドレス情報に対応するコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵、或いは、前記暗号化されたコンテンツが取得されるコンテンツ取得ステップと、前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を復号するためのワーク鍵が取得され、前記配信形態がコンテンツ鍵方式を利用する場合に前記コンテンツ鍵が取得される鍵取得ステップと、前記配信形態がワーク鍵方式を利用する場合に前記ワーク鍵を用いて前記スクランブル鍵が復号されるスクランブル鍵復号ステップと、前記配信形態がワーク鍵方式を利用する場合に前記スクランブル鍵を用いてコンテンツのスクランブルが解除され、前記配信形態がコンテンツ鍵方式を利用する場合に前記コンテンツ鍵を用いて前記暗号化されたコンテンツが復号されるコンテンツ復号ステップと、を含む、ストリーミングコンテンツの視聴処理方法が提供される。

10

【発明の効果】

【0018】

以上説明したように本発明によれば、コンテンツの制作者及び配信者等が各々ライセンスを管理することが可能であり、さらに、コンテンツの配信者等がコンテンツ単位でライセンス、及びコンテンツ取得先を管理することが可能になる。

【発明を実施するための最良の形態】

【0019】

以下に添付図面を参照しながら、本発明の好適な実施の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。

20

【0020】

〔説明の流れについて〕

ここで、以下に記載する本発明の実施形態に関する説明の流れについて簡単に述べる。まず、図1を参照しながら、VODライセンス方式に係るコンテンツ配信システムのシステム構成について具体例を挙げて説明する。次いで、図2を参照しながら、MCライセンス方式に係るコンテンツ配信システムのシステム構成について具体例を挙げて説明する。これらの具体例に関する説明の中で、本発明の実施形態が目的とするところについても併せて説明する。

【0021】

30

次いで、図3を参照しながら、本発明の一実施形態に係るコンテンツ配信システムのシステム構成について説明する。次いで、図4を参照しながら、当該コンテンツ配信システムに含まれるコンテンツサーバの機能構成について説明する。次いで、図5を参照しながら、当該コンテンツ配信システムに含まれるコンテンツ受信端末の機能構成について説明する。次いで、図6A及び図6Bを参照しながら、本実施形態に係る視聴時のコンテンツ配信処理等の流れについて説明する。

【0022】

次いで、図7Aを参照しながら、本実施形態の一変形例に係る契約時のライセンス取得処理等の流れについて説明する。さらに、図7Bを参照しながら、本実施形態の一変形例に係る視聴時のコンテンツ配信処理等の流れについて説明する。なお、これらの説明の中で、適宜、図8に示す再生制御メタファイルの構成例、及びライセンス情報の具体例を参照する。次いで、図9を参照しながら、本実施形態に係る各種のサーバ及び端末の機能を実現することが可能なハードウェア構成の一例について説明する。最後に、本実施形態に係る技術的構成が奏する作用効果について纏める。

40

【0023】

〔目的〕

まず、本発明の実施形態について説明するに先立ち、図1を参照しながら、VODライセンス方式に係るコンテンツ配信システムのシステム構成について簡単に説明する。また、図2を参照しながら、MCライセンス方式に係るコンテンツ配信システムのシステム構成について簡単に説明する。図1は、VODライセンス方式に係るコンテンツ配信システム

50

1のシステム構成例を示す説明図である。図2は、MCライセンス方式に係るコンテンツ配信システム2のシステム構成例を示す説明図である。

【0024】

(VODライセンス方式)

まず、図1を参照する。図1に示すように、コンテンツ配信システム1は、主に、送信システム10と、コンテンツ受信端末20とにより構成される。また、送信システム10は、主に、DRM/CASサーバ12と、ポータルサーバ14と、コンテンツサーバ16と、コンテンツ配信サーバ18とにより構成される。

【0025】

(購入時の処理)

コンテンツの視聴を開始する前に、視聴者は、視聴したいコンテンツを購入する。そこで、コンテンツの購入処理に係る一連の流れについて簡単に説明する。但し、ここで示す処理の流れは大枠のみであり、実際には相互認証等の各種処理が含まれる。

【0026】

例えば、視聴者は、ポータルサーバ14から提供されるコンテンツリストを参照し、所望のコンテンツを指定して購入操作を行う。このとき、ポータルサーバ14には、視聴者により指定されたコンテンツに対応するコンテンツ購入要求がコンテンツ受信端末20から送信される。このコンテンツ購入要求を受信すると、ポータルサーバ14は、DRM/CASサーバ12に対してライセンス生成要求を送信する。このライセンス生成要求を受信すると、DRM/CASサーバ12は、ライセンスを生成してライセンス生成完了通知をポータルサーバ14に送信する。DRM/CASサーバ12からライセンス生成完了通知を受信すると、ポータルサーバ14は、コンテンツ受信端末20に対してコンテンツ購入完了通知を送信する。

【0027】

以上の流れでコンテンツの購入処理が完了する。但し、実際には、ポータルサーバ14とコンテンツ受信端末20との間で認証処理等が実行されたり、ポータルサーバ14に接続された課金サーバ(非図示)による課金処理等が実行される。

【0028】

(コンテンツ視聴時の処理)

次に、視聴者は、上記の処理により購入されたコンテンツを視聴する。この視聴時にコンテンツ配信システム1により実行される一連の処理について説明する。但し、ここで示す処理の流れは大枠のみであり、実際には相互認証等の各種処理が含まれる。

【0029】

上記のようにしてコンテンツの購入処理が完了すると、視聴者は、コンテンツ受信端末20からコンテンツ配信サーバ18にアクセスし、購入したコンテンツを視聴することができる。このとき、コンテンツ受信端末20により次の処理が行われる。まず、コンテンツ受信端末20からポータルサーバ14にコンテンツ視聴要求が送信される。このコンテンツ視聴要求を受信すると、ポータルサーバ14は、コンテンツ受信端末20に対して再生制御メタファイルを送信する。

【0030】

この再生制御メタファイルには、コンテンツ受信端末20がコンテンツ配信サーバ18に接続してセッションを確立するために必要なコンテンツの取得先となるコンテンツ配信サーバ18のアドレス情報、及びDRM/CASサーバ12のアドレス情報が含まれている。また、再生制御メタファイルには、コンテンツを視聴する際に制御可能な再生方式の情報等が含まれていてもよい。ここで言う再生方式とは、例えば、倍速再生、1.6倍速再生、再生停止、早送り等である。

【0031】

上記の再生制御メタファイルを受信すると、コンテンツ受信端末20は、再生制御メタファイルの中からDRM/CASサーバ12のアドレス情報を抽出し、当該アドレス情報に基づいてDRM/CASサーバ12にアクセスする。そして、コンテンツ受信端末20

10

20

30

40

50

は、D R M / C A S サーバ 1 2 に対してライセンス取得要求を送信する。このライセンス取得要求を受信すると、D R M / C A S サーバ 1 2 は、コンテンツ受信端末 2 0 に対してライセンス情報とコンテンツ鍵とを送信する。

【 0 0 3 2 】

このライセンス情報には、例えば、コンテンツ鍵の有効期限を示す情報が含まれている。また、このコンテンツ鍵は、コンテンツ配信サーバ 1 8 から配信されるコンテンツを復号するためのものである。但し、このコンテンツ鍵により復号できるコンテンツは、視聴者が事前に購入したコンテンツである。なお、コンテンツ受信端末 2 0 が既にコンテンツ鍵を保持している場合、そのコンテンツ鍵に対応するライセンス情報のみが D R M / C A S サーバ 1 2 からコンテンツ受信端末 2 0 に送信されるように構成されていてもよい。

10

【 0 0 3 3 】

ライセンス情報及びコンテンツ鍵を受信すると、コンテンツ受信端末 2 0 は、ライセンス情報に含まれる有効期限を参照してコンテンツ鍵の有効期限を確認する。そして、有効期限が切れていないことが確認されると、コンテンツ受信端末 2 0 は、上記の再生制御メタファイルに含まれるコンテンツ受信端末 2 0 がコンテンツ配信サーバ 1 8 に接続してセッションを確立するために必要なコンテンツ配信サーバ 1 8 のアドレス情報を抽出し、当該コンテンツ配信サーバ 1 8 にアクセスする。

【 0 0 3 4 】

コンテンツ配信サーバ 1 8 からコンテンツを取得すると、コンテンツ受信端末 2 0 は、D R M / C A S サーバ 1 2 から取得したコンテンツ鍵を用いて暗号化されたコンテンツを復号する。このような処理が行われることにより、視聴者は、コンテンツ受信端末 2 0 を用いて取得したコンテンツを視聴することができる。

20

【 0 0 3 5 】

なお、コンテンツ配信サーバ 1 8 から配信されるコンテンツは、コンテンツサーバ 1 6 により提供される。このとき、コンテンツサーバ 1 6 は、D R M / C A S サーバ 1 2 から供与されたコンテンツ鍵を用いてコンテンツを暗号化してコンテンツ配信サーバ 1 8 に供与する。このコンテンツ鍵は、ポータルサーバ 1 4 を介してコンテンツ受信端末 2 0 から購入されたコンテンツのライセンスに対応するものである。

【 0 0 3 6 】

以上、V o D ライセンス方式におけるコンテンツ配信システムの構成例、及びコンテンツの視聴処理に係る一連の流れについて簡単に説明した。上記の通り、V o D ライセンス方式の場合、ポータルサーバ 1 4 から提供される再生制御メタファイルによりコンテンツの配信先を指定することができる。また、個々のコンテンツ配信サーバ 1 8 に対し、個々のコンテンツ鍵で暗号化されたコンテンツをユニキャスト配信することで、コンテンツ単位でライセンスを管理することができる。しかしながら、暗号化されたコンテンツを復号するためのコンテンツ鍵を用いてライセンスが管理されているため、コンテンツの制作者及び配信者が相互に異なる形態でライセンスを管理し難いという問題がある。また、リアルタイムな映像をストリーミング配信したい場合、コンテンツを暗号化することができない。

30

【 0 0 3 7 】

(M C ライセンス方式)

次に、図 2 を参照する。図 2 に示すように、コンテンツ配信システム 2 は、主に、送信システム 3 0 と、コンテンツ受信端末 3 8 とにより構成されている。また、送信システム 3 0 は、主に、D R M / C A S サーバ 3 2 と、コンテンツサーバ 3 4 と、コンテンツ配信サーバ 3 6 とにより構成されている。

【 0 0 3 8 】

(契約時の処理)

コンテンツの視聴を開始する前に、視聴者は、コンテンツの視聴契約を締結する。そこで、視聴契約の締結処理に係る一連の流れについて簡単に説明する。但し、ここで示す処理の流れは大枠のみであり、実際には相互認証等の各種処理が含まれる。

40

50

【 0 0 3 9 】

例えば、視聴者は、事前に月極でコンテンツの視聴契約を締結する。このとき、視聴者は、個々のコンテンツに対して視聴契約を締結するのではなく、所定のチャンネルに対応するコンテンツを自由に視聴できる契約を締結することが多い。また、複数のチャンネルを自由に選択して視聴できる契約が締結されることが多い。契約内容については、コンテンツの配信者と視聴者との間で自由に設定される事項であるが、上記のような契約が締結される場合を例に挙げて説明する。

【 0 0 4 0 】

この場合、視聴者は、コンテンツ受信端末 3 8 を用いて D R M / C A S サーバ 3 2 にアクセスし、ライセンスの供与を受ける。このとき、コンテンツ受信端末 3 8 は、D R M / C A S サーバ 3 2 に対してライセンス取得要求を送信する。このライセンス取得要求を受信すると、D R M / C A S サーバ 3 2 は、所定の認証処理や課金処理等を実行する。これらの処理が完了すると、D R M / C A S サーバ 3 2 は、コンテンツ受信端末 3 8 に対してライセンス情報、及びワーク鍵を送信する。このライセンス情報には、ワーク鍵の有効期限、及び当該有効期限とワーク鍵との対応関係を示す情報が含まれている。また、ここで言うワーク鍵とは、コンテンツをデスクランブルするために用いるスクランブル鍵の暗号化を解除するためのものである。

10

【 0 0 4 1 】

以上の流れでコンテンツの視聴契約が締結される。上記の通り、コンテンツ受信端末 3 8 には、ライセンスに対応したワーク鍵が保持された状態となる。但し、M C ライセンス方式の場合、コンテンツ受信端末 3 8 は、D R M / C A S サーバ 3 2 のアドレス情報、及びコンテンツを配信するコンテンツ配信サーバ 3 6 のアドレス情報を認知していることが前提である。そのため、V o D ライセンス方式で利用される再生制御メタファイルやポータルサーバが存在しない点に注意されたい。

20

【 0 0 4 2 】

(コンテンツ視聴時の処理)

次に、視聴者は、締結された契約に基づいてコンテンツを視聴する。この視聴時にコンテンツ配信システム 2 により実行される一連の処理について説明する。但し、ここで示す処理の流れは大枠のみであり、実際には相互認証等の各種処理が含まれる。

【 0 0 4 3 】

上記のようにして事前に契約が締結されていると、視聴者は、コンテンツ受信端末 3 8 から所望のコンテンツを配信しているコンテンツ配信サーバ 3 6 にアクセスし、配信されるコンテンツを視聴することができる。このとき、コンテンツ受信端末 3 8 は、視聴者により指定されたコンテンツを配信しているコンテンツ配信サーバ 3 6 に対してコンテンツ視聴要求を送信する。このコンテンツ視聴要求を受信すると、コンテンツ配信サーバ 3 6 は、コンテンツ及び E C M (E n t i t l e C o n t r o l M e s s a g e) パケットをコンテンツ受信端末 3 8 に送信する。

30

【 0 0 4 4 】

このとき送信されるコンテンツは、後述するコンテンツサーバ 3 4 によりスクランブルされたものである。また、ここで言う E C M パケットとは、コンテンツに施されたスクランブルを解除するためのスクランブル鍵にワーク鍵を用いて暗号化を施したものである。

40

【 0 0 4 5 】

このようなコンテンツ及び E C M パケットを受信すると、コンテンツ受信端末 3 8 は、事前 to 取得したワーク鍵を用いて E C M パケットからスクランブル鍵を復号する。さらに、コンテンツ受信端末 3 8 は、復号したスクランブル鍵を用いてコンテンツに施されたスクランブルを解除する。このような処理が行われることにより、視聴者は、コンテンツ受信端末 3 8 を用いて取得したコンテンツを視聴することができる。

【 0 0 4 6 】

なお、コンテンツ配信サーバ 3 6 から配信されるコンテンツには、上記の通り、コンテンツサーバ 3 4 によりスクランブルが施されている。また、コンテンツサーバ 3 4 は、D

50

R M / C A S サーバ 3 2 からワーク鍵を取得し、当該ワーク鍵を用いてスクランブル鍵を暗号化する。そして、コンテンツサーバ 3 4 により暗号化されたスクランブル鍵は、E C M パケットとしてコンテンツ配信サーバ 3 6 に送信される。但し、コンテンツサーバ 3 4 は、同じワーク鍵を用いて、複数のコンテンツ配信サーバ 3 6 に送信される各コンテンツのスクランブル鍵を暗号化する。そのため、視聴者は、任意のコンテンツ配信サーバ 3 6 を選択してコンテンツを視聴することができるのである。

【 0 0 4 7 】

以上、M C ライセンス方式におけるコンテンツ配信システムの構成例、及びコンテンツの視聴処理に係る一連の流れについて簡単に説明した。上記の通り、M C ライセンス方式の場合、コンテンツのスクランブル及びスクランブル鍵の暗号化という 2 種類の暗号処理が行われるため、コンテンツの制作者と配信者とで個別にライセンスを管理することができる。例えば、コンテンツの制作者は、スクランブル鍵の提供先を管理することで、コンテンツの配信者に対するライセンス管理を実現することができる。一方、コンテンツの配信者は、ワーク鍵の提供先を管理することで、コンテンツの視聴者に対するライセンス管理を実現することができる。しかしながら、マルチキャスト配信を実現するため、同一のマルチキャストアドレス宛に配信されている異なるコンテンツのスクランブル鍵に対して同じワーク鍵で暗号化しており、コンテンツ毎のライセンス管理が難しいという問題があった。また、ストリーミングで提供されるコンテンツに対して、コンテンツ単位で異なるコンテンツ取得先を視聴者へ提供するような配信形態を実現することも出来なかった。

【 0 0 4 8 】

以下で説明する本発明の実施形態は、上記の V o D ライセンス方式、及び M C ライセンス方式の問題点を解決し、両方式の利点を併せ持ったコンテンツ配信システムを提案することを目的とするものである。

【 0 0 4 9 】

< 実施形態 >

以下、本発明の一実施形態について説明する。本実施形態は、M C ライセンス方式と同様に 2 種類の暗号処理を用いたライセンス形態を採用しつつ、コンテンツ単位でのライセンス管理を可能にしたコンテンツ配信方式に関する。

【 0 0 5 0 】

[コンテンツ配信システム 1 0 0 0 の構成]

まず、図 3 を参照しながら、本実施形態に係るコンテンツ配信システム 1 0 0 0 のシステム構成、及び、本実施形態のコンテンツ配信処理に係る一連の流れについて説明する。図 3 は、本実施形態に係るコンテンツ配信システム 1 0 0 0 のシステム構成例を示す説明図である。

【 0 0 5 1 】

図 3 に示すように、コンテンツ配信システム 1 0 0 0 は、主に、送信システム 1 0 0 と、コンテンツ受信端末 1 3 0 とにより構成される。また、送信システム 1 0 0 は、主に、コンテンツサーバ 1 0 2 と、コンテンツ配信サーバ 1 0 4 と、D R M / C A S サーバ 1 0 6 と、ポータルサーバ 1 0 8 と、課金サーバ 1 1 0 と、認証サーバ 1 1 2 とにより構成される。但し、実施の態様に応じて、課金サーバ 1 1 0、及び認証サーバ 1 1 2 は、適宜省略されることもある。

【 0 0 5 2 】

(購入時の処理)

本実施形態においても、コンテンツの視聴を開始する前に、視聴者は、視聴したいコンテンツを購入する。そこで、コンテンツの購入処理に係る一連の流れについて説明する。

【 0 0 5 3 】

まず、視聴者は、ポータルサーバ 1 0 8 から提供されるコンテンツリストを参照し、所望のコンテンツを指定して購入操作を行う。このコンテンツリストは、例えば、E P G (E l e c t r o n i c P r o g r a m G u i d e) 等のような番組表の形式で提示される。この場合、視聴者は、番組表の中から所望の番組を指定することで、その番組に対

10

20

30

40

50

応するコンテンツを購入することができる。もちろん、コンテンツリストの提示形式は任意である。このような購入操作が行われると、コンテンツ受信端末 130 によりコンテンツの購入処理が進められる。

【0054】

上記のような購入操作が行われると、コンテンツ受信端末 130 は、ポータルサーバ 108 に対してコンテンツ購入要求を送信する。このとき、コンテンツ受信端末 130 は、ポータルサーバ 108 に対して視聴者及び端末を特定するための認証情報を送信する。コンテンツ購入要求、及び認証情報を受信すると、ポータルサーバ 108 は、受信した認証情報を認証サーバ 112 に送信する。認証サーバ 112 は、受信した認証情報を用いて視聴者及び端末の認証処理を実行し、その認証結果をポータルサーバ 108 に通知する。

10

【0055】

ポータルサーバ 108 は、認証サーバ 112 から認証結果の通知を受け、成功裏に認証が完了したことを確認すると、ポータルサーバ 108 は、DRM/CASサーバ 106 に対してライセンス生成要求を送信する。このライセンス生成要求を受信すると、DRM/CASサーバ 106 は、ライセンスを生成してライセンス生成完了通知をポータルサーバ 108 に送信する。ポータルサーバ 108 は、DRM/CASサーバ 106 からライセンス生成完了通知を受信し、課金サーバ 110 に対してライセンス課金要求を送信する。

【0056】

課金サーバ 110 は、ポータルサーバ 108 から受信したライセンス課金要求に基づいてライセンスに対する課金処理を実行する。課金処理が完了すると、課金サーバ 110 は、ポータルサーバ 108 に対してライセンス課金完了通知を送信する。このライセンス課金完了通知を受信すると、ポータルサーバ 108 は、コンテンツ受信端末 130 に対してコンテンツ購入完了通知を送信する。このコンテンツ購入完了通知を受信することで、コンテンツ受信端末 130 は、コンテンツの購入処理を完了する。

20

【0057】

以上、購入時の処理について説明した。但し、コンテンツの購入処理に関しては、種々の変形が可能である。例えば、課金されないコンテンツに対しては、課金サーバ 110 による課金処理等が省略される。認証処理等においても同様に、実施の態様に応じて省略することが可能である。また、ポータルサーバ 108 からコンテンツ受信端末 130 に提供されるコンテンツリストの提示形式等においても、種々の変形が可能である。

30

【0058】

(コンテンツ視聴時の処理)

次に、視聴者は、上記の処理により購入されたコンテンツを視聴する。この視聴時にコンテンツ配信システム 1000 により実行される一連の処理について説明する。但し、ここで示す処理の流れは大枠のみであり、実際には相互認証等の各種処理が含まれる。

【0059】

上記のようにしてコンテンツの購入処理が完了すると、視聴者は、コンテンツ受信端末 130 からコンテンツ配信サーバ 104 にアクセスし、購入したコンテンツを視聴することができる。このとき、コンテンツ受信端末 130 により次の処理が行われる。まず、コンテンツ受信端末 130 からポータルサーバ 108 にコンテンツ視聴要求が送信される。このコンテンツ視聴要求を受信すると、ポータルサーバ 108 は、コンテンツ受信端末 130 に対して再生制御メタファイルを送信する。

40

【0060】

この再生制御メタファイルには、図 8 に示すように、コンテンツ受信端末 130 がコンテンツ配信サーバ 104 に接続してセッションを確立するために必要なコンテンツの取得先となるコンテンツ配信サーバ 104 のアドレス情報、及び DRM/CASサーバ 106 のアドレス情報が含まれている。

【0061】

また、再生制御メタファイルには、コンテンツを視聴する際に制御可能な再生方式の情報等が含まれている。ここで言う再生方式とは、例えば、倍速再生、1.6 倍速再生、再生

50

停止、早送り等である。さらに、再生制御メタファイルには、取得するコンテンツの種別を示すコンテンツ種別情報が含まれている。コンテンツ種別情報には、例えば、V o D ライセンス形式でコンテンツが配信されるのか、M C ライセンス形式 (L i v e S t r e a m i n g 形式) でコンテンツが配信されるのか等が示されている。

【 0 0 6 2 】

コンテンツ受信端末 1 3 0 は、上記のような再生制御メタファイルの中から D R M / C A S サーバ 1 0 6 のアドレス情報を抽出し、当該アドレス情報に基づいて D R M / C A S サーバ 1 0 6 にアクセスする。そして、コンテンツ受信端末 1 3 0 は、D R M / C A S サーバ 1 0 6 に対してライセンス取得要求を送信する。このライセンス取得要求を受信すると、D R M / C A S サーバ 1 0 6 は、コンテンツ受信端末 1 3 0 に対してライセンス情報及びワーク鍵を送信する。

10

【 0 0 6 3 】

このライセンス情報には、例えば、コンテンツ鍵の有効期限を示す情報が含まれている。また、このワーク鍵は、上記の M C ライセンス方式のものと同様、コンテンツ配信サーバ 1 0 4 から配信されるコンテンツのスクランブル鍵を復号するためのものである。但し、このワーク鍵により復号できるスクランブル鍵は、視聴者が事前に購入したコンテンツに対応するものである。なお、複数のコンテンツ配信サーバ 1 0 4 から配信されるコンテンツの視聴契約が視聴者により締結されている場合、それらのコンテンツ配信サーバ 1 0 4 に共通するワーク鍵がコンテンツ受信端末 1 3 0 に提供される。

【 0 0 6 4 】

20

上記のようにして、ライセンス情報及びワーク鍵が送信されると、コンテンツ受信端末 1 3 0 は、それらを受信し、ライセンス情報に含まれる有効期限を参照してワーク鍵の有効期限を確認する。そして、有効期限が切れていないことを確認すると、コンテンツ受信端末 1 3 0 は、上記の再生制御メタファイルに含まれるコンテンツ配信サーバ 1 0 4 のアドレス情報を抽出し、当該アドレス情報に対応するコンテンツ配信サーバ 1 0 4 にアクセスすることにより、スクランブルが施されたコンテンツ及び E C M パケットを取得する。

【 0 0 6 5 】

このとき、複数のコンテンツ配信サーバ 1 0 4 から配信されるコンテンツに対して購入処理又は契約処理が完了している場合、再生制御メタファイルには、複数のコンテンツ配信サーバ 1 0 4 のアドレス情報が含まれている。この場合、コンテンツ受信端末 1 3 0 は、所望のコンテンツを配信しているコンテンツ配信サーバ 1 0 4 を選択し、選択されたコンテンツ配信サーバ 1 0 4 からコンテンツを取得することができる。例えば、視聴者は、3つのチャンネルから配信されるコンテンツのみを購入することができる。この場合、再生制御メタファイルには、3つのチャンネルに対応するコンテンツ配信サーバ 1 0 4 のアドレス情報等が含まれる。

30

【 0 0 6 6 】

上記のようにして、コンテンツ配信サーバ 1 0 4 からスクランブルが施されたコンテンツ及び E C M パケットを取得すると、コンテンツ受信端末 1 3 0 は、D R M / C A S サーバ 1 0 6 から取得したワーク鍵を用いて E C M パケットからスクランブル鍵を復号する。さらに、コンテンツ受信端末 1 3 0 は、復号したスクランブル鍵を用いてコンテンツに施されたスクランブルを解除する。このような処理が行われることにより、視聴者は、コンテンツ受信端末 1 3 0 を用いて取得したコンテンツを視聴することができる。

40

【 0 0 6 7 】

なお、コンテンツ配信サーバ 1 0 4 から配信されるコンテンツ及び E C M パケットは、コンテンツサーバ 1 0 2 により提供される。コンテンツサーバ 1 0 2 は、コンテンツにスクランブルを施すと共に、D R M / C A S サーバ 1 0 6 から供与されたワーク鍵を用いてスクランブルを解除するためのスクランブル鍵を暗号化して E C M パケットを生成する。そして、コンテンツサーバ 1 0 2 は、スクランブルが施されたコンテンツ、及び E C M パケットをコンテンツ配信サーバ 1 0 4 に供与する。

【 0 0 6 8 】

50

但し、複数のコンテンツ配信サーバ 104 から配信されるコンテンツに対してライセンスが与えられる場合、コンテンツサーバ 102 は、それらのコンテンツのスクランブル鍵を共通のワーク鍵で暗号化する。このような構成にすることで、各コンテンツは、コンテンツ単位で異なるスクランブル鍵によりスクランブルされる。一方で、配信されるコンテンツ群は、同じワーク鍵により視聴が制限される。つまり、マルチキャストライセンスでありながら、個々のコンテンツに対するライセンス管理もできるように構成されている。

【0069】

以上、本実施形態に係るコンテンツ配信システム 1000 の構成例、及びコンテンツの視聴処理に係る一連の流れについて説明した。上記の通り、本実施形態に係るコンテンツ配信方式においては、コンテンツのスクランブル及びスクランブル鍵の暗号化という2種類の暗号処理が行われるため、コンテンツの制作者と配信者とで個別にライセンスを管理することができる。また、再生制御メタファイルによるコンテンツ取得先の制限や、ワーク鍵を用いたライセンス管理により、配信形態をマルチキャストにしたり、ユニキャストにしたり、自由に設定することができるようになる。

【0070】

[コンテンツサーバ 102 の機能構成]

ここで、図4を参照しながら、コンテンツ配信システム 1000 に含まれるコンテンツサーバ 102 の機能構成について説明する。図4は、本実施形態に係るコンテンツサーバ 102 の機能構成の一例を示す説明図である。

【0071】

図4に示すように、コンテンツサーバ 102 は、主に、記憶部 152 と、スクランブル部 154 と、ワーク鍵取得部 156 と、スクランブル鍵暗号化部 158 と、多重送信部 160 とにより構成される。

【0072】

なお、記憶部 152 の機能は、後述するハードウェア構成の中で、例えば、RAM 906、記憶部 920、又はリムーバブル記録媒体 928 等により実現される。また、スクランブル部 154、スクランブル鍵暗号化部 158 の機能は、例えば、ROM 904、RAM 906、記憶部 920、又はリムーバブル記録媒体 928 等に記録されたプログラムに基づいて CPU 902 により実現される。さらに、ワーク鍵取得部 156、多重送信部 160 の機能は、例えば、接続ポート 924、又は通信部 926 等により実現される。

【0073】

(記憶部 152)

記憶部 152 には、コンテンツ配信サーバ 104 により配信されるコンテンツが格納されている。但し、当該コンテンツは、スクランブルされていないものである。また、記憶部 152 には、コンテンツをスクランブルするためのスクランブル鍵が格納されている。さらに、記憶部 152 には、コンテンツに施されたスクランブルを解除するためのスクランブル鍵が格納されている。但し、スクランブル解除に用いられるスクランブル鍵は、スクランブルに用いられるスクランブル鍵と同じものでもよいし、別のものでもよい。但し、以下の説明においては、同じものであると仮定して説明を進めることにする。

【0074】

(スクランブル部 154)

スクランブル部 154 は、記憶部 152 からコンテンツ及びスクランブル鍵を取得する。そして、スクランブル部 154 は、取得したスクランブル鍵を用いてコンテンツにスクランブルを施す。このとき、スクランブルが施されるコンテンツとスクランブル鍵とは対応するものである。そして、どのコンテンツをどのスクランブル鍵でスクランブルするかということは、例えば、コンテンツの制作者により設定される。スクランブル部 154 によりスクランブルが施されたコンテンツは、多重送信部 160 に入力される。

【0075】

(ワーク鍵取得部 156、スクランブル鍵暗号化部 158)

ワーク鍵取得部 156 は、DRM/CASサーバ 106 からワーク鍵を取得する。この

10

20

30

40

50

とき、ワーク鍵取得部 156 は、取得したワーク鍵とコンテンツ（又はスクランブル鍵）との対応関係を示す情報も併せて取得する。そして、ワーク鍵取得部 156 は、取得したワーク鍵、及び対応関係を示す情報をスクランブル鍵暗号化部 158 に入力する。

【0076】

スクランブル鍵暗号化部 158 は、記憶部 152 からスクランブル鍵を取得する。さらに、スクランブル鍵暗号化部 158 は、ワーク鍵取得部 156 からワーク鍵、及び対応関係を示す情報を取得する。そして、スクランブル鍵暗号化部 158 は、ワーク鍵取得部 156 から入力された対応関係を示す情報に基づき、取得したスクランブル鍵に対応するワーク鍵を用いて当該スクランブル鍵を暗号化する。スクランブル鍵暗号化部 158 により暗号化されたスクランブル鍵は、ECM パケットとして多重送信部 160 に入力される。

10

【0077】

（多重送信部 160）

上記の通り、多重送信部 160 には、スクランブル部 154 からスクランブルされたコンテンツが入力され、スクランブル鍵暗号化部 158 から ECM パケットが入力される。但し、多重送信部 160 に入力されたコンテンツ及び ECM パケットは、互いに対応するものであると仮定する。つまり、入力されたコンテンツのスクランブルに用いたスクランブル鍵と、ECM パケットを構成する暗号化されたスクランブル鍵とは同じものであると仮定する。この場合、多重送信部 160 は、入力されたコンテンツ及び ECM パケットをセットにしてコンテンツ配信サーバ 104 に送信する。

【0078】

20

既に述べた通り、ライセンス契約の内容によっては、同じワーク鍵で複数のスクランブル鍵が暗号化されることがある。このような場合にも、多重送信部 160 は、各コンテンツと ECM パケットとをそれぞれセットにして各コンテンツ配信サーバ 104 に送信する。逆に、個々のコンテンツに対してライセンスを発行する形態にすることもできる。その場合、個々のコンテンツに対応するスクランブル鍵が個々のワーク鍵で暗号化され、それぞれ対応するコンテンツ配信サーバ 104 に対して送信される。

【0079】

以上、本実施形態に係るコンテンツサーバ 102 の機能構成について説明した。上記の通り、本実施形態におけるコンテンツの暗号処理は、スクランブル鍵を用いたコンテンツのスクランブル処理と、スクランブル鍵をワーク鍵で暗号化する暗号化処理とにより実現される。そのため、スクランブル鍵を用いてコンテンツ単位のライセンス管理が可能になり、ワーク鍵を用いて、配信されるコンテンツの組み合わせ単位でライセンスを管理することが可能になる。つまり、MC ライセンスの形態が実現される。

30

【0080】

〔コンテンツ受信端末 130 の機能構成〕

次に、図 5 を参照しながら、コンテンツ配信システム 1000 に含まれるコンテンツ受信端末 130 の機能構成について説明する。図 5 は、本実施形態に係るコンテンツ受信端末 130 の機能構成の一例を示す説明図である。

【0081】

図 5 に示すように、コンテンツ受信端末 130 は、主に、DRM クライアント 132 と、視聴クライアント 134 とにより構成される。DRM クライアント 132 は、DRM / CAS サーバ 106 にアクセスするための手段であり、ライセンス取得部 172 を有する。視聴クライアント 134 は、コンテンツ視聴時の処理を行う手段である。視聴クライアント 134 は、コンテンツ購入処理部 174 と、再生制御メタ取得部 176 と、コンテンツ配信形態判別部 178 と、コンテンツ取得部 180 と、スクランブル鍵復号部 182 と、デスクランブル部 184 とを有する。

40

【0082】

なお、DRM クライアント 132、及び視聴クライアント 134 が有する主な機能は、後述するハードウェア構成の中で、例えば、ROM 904、RAM 906、記憶部 920、又はリムーバブル記録媒体 928 等に記録されたプログラムに基づいて CPU 902 に

50

より実現される。但し、ライセンス取得部 172、再生制御メタ取得部 176、コンテンツ取得部 180の主な機能は、例えば、接続ポート 924、又は通信部 926等により実現される。

【0083】

まず、コンテンツの購入処理に係る機能構成について説明する。次いで、コンテンツの視聴処理に係る機能構成について説明する。

【0084】

(コンテンツ購入処理部 174)

コンテンツ購入処理部 174は、ポータルサーバ 108に対してコンテンツ購入要求を送信する。さらに、コンテンツ購入処理部 174は、コンテンツ購入要求に応じてポータルサーバ 108から送信されたコンテンツ購入完了通知を受信する。このコンテンツ購入完了通知を受信すると、コンテンツ購入処理部 174は、コンテンツの購入が完了した旨を再生制御メタ取得部 176に通知する。

10

【0085】

(再生制御メタ取得部 176)

再生制御メタ取得部 176は、コンテンツ購入処理部 174からコンテンツの購入が完了した旨の通知を受けた後、ポータルサーバ 108に対してコンテンツ視聴要求を送信する。さらに、再生制御メタ取得部 176は、コンテンツ視聴要求に応じてポータルサーバ 108から送信された再生制御メタファイルを受信する。この再生制御メタファイルには、図 8に示すように、コンテンツ配信サーバ 104のアドレス情報、DRM/CASサーバ 106のアドレス情報、コンテンツ種別情報、及び配信形態の情報等が含まれている。

20

【0086】

そこで、再生制御メタ取得部 176は、受信した再生制御メタファイルからDRM/CASサーバ 106のアドレス情報等を抽出してライセンス取得部 172に入力する。また、再生制御メタ取得部 176は、再生制御メタファイルからコンテンツ配信サーバ 104のアドレス情報を抽出してコンテンツ取得部 180に入力する。さらに、再生制御メタ取得部 176は、再生制御メタファイルからコンテンツの配信形態に関する情報を抽出してコンテンツ配信形態判別部 178に入力する。

【0087】

(コンテンツ配信形態判別部 178)

コンテンツ配信形態判別部 178は、再生制御メタ取得部 176から入力された情報に基づいてコンテンツの配信形態を判別する。コンテンツの配信形態に関する情報としては、例えば、コンテンツの種別を示す情報や、そのコンテンツに対して行える再生制御方式の情報がある。コンテンツの種別に関しては、例えば、VOD方式で配信されるコンテンツなのか、ライブストリーミング方式で配信されるコンテンツなのか、その他のコンテンツなのか等が判別される。また、再生制御方式に関しては、例えば、倍速再生が可能なのか、再生停止が可能なのか等が判別される。コンテンツ配信形態判別部 178により判別された結果は、コンテンツ取得部 180に入力される。

30

【0088】

(コンテンツ取得部 180)

コンテンツ取得部 180は、再生制御メタ取得部 176から入力されたコンテンツ配信サーバ 104のアドレス情報等を用いてコンテンツ配信サーバ 104にアクセスする。そして、コンテンツ取得部 180は、コンテンツ配信サーバ 104に対してセッション開始要求を送信する。その後、コンテンツ取得部 180は、セッション開始要求に応じてコンテンツ配信サーバ 104から送信されたコンテンツ及びECMパケットを受信する。但し、このコンテンツはスクランブルが施されたものである。コンテンツ取得部 180により受信されたコンテンツは、デスクランブル部 184に入力される。また、コンテンツ取得部 180により受信されたECMパケットは、スクランブル鍵復号部 182に入力される。

40

【0089】

50

ここで、コンテンツの配信形態に関する判別結果に係るコンテンツ取得部 180 の処理について簡単に説明する。配信形態に関する判別結果は、例えば、下記の (A) (B) のように処理される。

【0090】

(A) 上記の説明においては、全てのコンテンツ配信サーバ 104 から MC ライセンス方式のコンテンツ及び ECM パケットが配信されるものと仮定していた。しかし、コンテンツ配信サーバ 104 の中には、VOD ライセンス方式のようにコンテンツ鍵で暗号化されたコンテンツを送信するものが含まれているシステム構成も考えられる。この場合、コンテンツ受信端末 130 は、DRM / CAS サーバ 106 から取得した鍵 (ワーク鍵、コンテンツ鍵) を用いて復号する対象が何かを知っている必要がある。

10

【0091】

このような場合、コンテンツ取得部 180 は、コンテンツ配信形態判別部 178 により入力された判別結果がコンテンツ鍵暗号方式の場合、その判別結果をスクランブル鍵復号部 182、及びデスクランブル部 184 に入力する。逆に、ワーク鍵による 2 重暗号処理方式の場合、本来の処理形態であるため、その判別結果をスクランブル鍵復号部 182、及びデスクランブル部 184 に入力しない。但し、判別結果をスクランブル鍵復号部 182、及びデスクランブル部 184 に入力するように構成されていてもよい。

【0092】

(B) また、ストリーミングコンテンツを視聴する場合、コンテンツ又はコンテンツ配信サーバ 104 が対応している再生制御方式が何かをコンテンツ受信端末 130 が知っていることが好ましい。例えば、2 倍速再生に対応していないコンテンツ配信サーバ 104 に対して 2 倍速再生を指定する再生制御情報を送信しても、コンテンツ取得部 180 によりコンテンツを正しく取得して再生することができないからである。そこで、コンテンツ取得部 180 は、コンテンツ配信形態判別部 178 の判別結果に適合する配信形態でコンテンツ配信サーバ 104 からコンテンツを取得する。

20

【0093】

(ライセンス取得部 172)

ライセンス取得部 172 は、再生制御メタ取得部 176 から入力されたアドレス情報を用いて DRM / CAS サーバ 106 にアクセスする。このとき、ライセンス取得部 172 は、事前に保持している機器固有の ID 等の認証情報を用いて DRM / CAS サーバ 106 との間で相互認証を行う。そして、ライセンス取得部 172 は、DRM / CAS サーバ 106 に対してライセンス取得要求を送信する。その後、ライセンス取得部 172 は、このライセンス取得要求に応じて DRM / CAS サーバ 106 から送信されたライセンス情報、及びワーク鍵を受信する。

30

【0094】

このライセンス情報には、図 8 に示すように、ワーク鍵、ワーク鍵の有効期限、及び当該有効期限とワーク鍵との対応関係を示す情報が含まれている。なお、ワーク鍵は、このタイミングで取得せず、事前に取得して保持しておくように構成されていてもよい。このようにしてライセンス情報及びワーク鍵を取得すると、ライセンス取得部 172 は、ライセンス情報に含まれる有効期限を参照し、ワーク鍵が有効か否かを判断する。ワーク鍵が有効な場合、ライセンス取得部 172 は、そのワーク鍵をスクランブル鍵復号部 182 に入力する。

40

【0095】

(スクランブル鍵復号部 182)

スクランブル鍵復号部 182 は、ライセンス取得部 172 により入力されたワーク鍵を用いて、コンテンツ取得部 180 により入力された ECM パケットからスクランブル鍵を復号する。スクランブル鍵復号部 182 により復号されたスクランブル鍵は、デスクランブル部 184 に入力される。但し、コンテンツ鍵暗号方式である旨を示す配信形態の判別結果がコンテンツ取得部 180 から入力された場合、ライセンス取得部 172 から入力された鍵をそのままデスクランブル部 184 に入力する。

50

【 0 0 9 6 】

(デスクランブル部 1 8 4)

デスクランブル部 1 8 4 は、スクランブル鍵復号部 1 8 2 により復号されたスクランブル鍵を用いてコンテンツ取得部 1 8 0 から入力されたコンテンツのスクランブルを解除する。但し、コンテンツ鍵暗号方式である旨を示す配信形態の判別結果がコンテンツ取得部 1 8 0 から入力された場合、デスクランブル部 1 8 4 は、スクランブル鍵復号部 1 8 2 から入力された鍵を用いてコンテンツ取得部 1 8 0 により取得されたコンテンツを復号する。このような処理により、コンテンツが視聴可能な状態に復元される。

【 0 0 9 7 】

以上、本実施形態に係るコンテンツ受信端末 1 3 0 の機能構成について説明した。上記のような構成にすることで、V o Dライセンス方式のように再生制御メタファイルを用いてコンテンツの取得先を指定する構成の枠組みの中で、M Cライセンスのような2重暗号方式を適用できるようになる。

【 0 0 9 8 】

(コンテンツ配信形態について)

ここで、再生制御メタファイルに含まれるコンテンツ配信形態に関する情報の扱い方について説明を補足する。上記の通り、再生制御メタファイルには、コンテンツの配信形態を示す情報として、再生制御方式の情報と、ライセンス形態に関する情報が含まれる。再生制御方式に関する情報は、コンテンツ取得部 1 8 0 がコンテンツを取得する際に、コンテンツ配信サーバ 1 0 4 が対応する形態で取得するために利用される。一方、ライセンス形態に関する情報についてはシステム構成にも依存するため、ここで説明を補足する。

【 0 0 9 9 】

上記の通り、本実施形態に係るコンテンツ配信システム 1 0 0 0 は、M Cライセンス方式と同様にワーク鍵を用いた2重暗号方式を採用している。しかし、本実施形態に係るコンテンツ受信端末 1 3 0 は、コンテンツ配信システム 1 0 0 0 の構成にV o Dライセンス方式のシステム要素を追加して拡張されたシステム形態にも対応できる。実際には、既存のV o Dライセンス方式のシステム等にも本実施形態に係る技術を適用して拡張することになるかもしれない。もちろん、このように拡張されたシステムも、本実施形態の技術的範囲に属するものである。

【 0 1 0 0 】

但し、このような拡張を行う場合、コンテンツ受信端末 1 3 0 は、M Cライセンス方式で配信されたのか、V o Dライセンス方式で配信されたのかを認識する必要がある。もちろん、これら以外のライセンス方式についても同様である。そこで、コンテンツ配信システム 1 0 0 0 は、ポータルサーバ 1 0 8 から送信される再生制御メタファイルにコンテンツ配信形態の情報を付加しているのである。コンテンツ受信端末 1 3 0 は、このコンテンツ配信形態を認識し、コンテンツの復号に係る処理を切り替えるのである。

【 0 1 0 1 】

例えば、配信形態がV o Dライセンス方式であると判別された場合、コンテンツ受信端末 1 3 0 は、ライセンス取得部 1 7 2 によりD R M / C A Sサーバ 1 0 6 からコンテンツ鍵を取得する。また、コンテンツ取得部 1 8 0 は、コンテンツ配信サーバ 1 0 4 から暗号化されたコンテンツのみを取得する。さらに、スクランブル鍵復号部 1 8 2 は機能せず、デスクランブル部 1 8 4 により、コンテンツ鍵を用いてコンテンツが復号される。

【 0 1 0 2 】

このように、コンテンツの配信形態を示す情報が再生制御メタファイルに含まれることで、容易にコンテンツ視聴時の処理を切り替えることができる。その結果、他のライセンス方式との互換性を確保することが可能になり、既存のシステム構成をベースにして本実施形態の技術を実現させることができるようになる。その結果、本実施形態において提案する技術を比較的低い開発コスト及び導入コストで実現することが可能になる。

【 0 1 0 3 】

[視聴時の処理シーケンス]

10

20

30

40

50

次に、図 6 A、及び図 6 Bを参照しながら、本実施形態のコンテンツ配信システム 1 0 0 における視聴時の処理シーケンスについて説明する。ここでは、コンテンツサーバ 1 0 2 やコンテンツ受信端末 1 3 0 が有する細かな機能構成については意識せず、システム全体として行われる処理の流れについて説明する。

【 0 1 0 4 】

まず、図 6 Aを参照する。図 6 Aに示すように、まず、視聴クライアント 1 3 4 からポータルサーバ 1 0 8 に対してコンテンツ購入要求が送信される (S 1 0 2)。次いで、ポータルサーバ 1 0 8 と認証サーバ 1 1 2 との間で認証処理が行われる (S 1 0 4)。次いで、ポータルサーバ 1 0 8 と D R M / C A S サーバ 1 0 6 との間でライセンス生成処理が行われる (S 1 0 6)。次いで、ポータルサーバ 1 0 8 と課金サーバ 1 1 0 との間で課金処理が行われる (S 1 0 8)。次いで、ポータルサーバ 1 0 8 から視聴クライアント 1 3 4 にコンテンツ購入完了通知が送信される (S 1 1 0)。以上の処理により、コンテンツの購入に係る一連の処理が完了する。

10

【 0 1 0 5 】

次いで、視聴クライアント 1 3 4 からポータルサーバ 1 0 8 に対してコンテンツ視聴要求が送信される (S 1 1 2)。次いで、ポータルサーバ 1 0 8 から視聴クライアント 1 3 4 に対して再生制御メタファイルが送信される (S 1 1 4)。次いで、視聴クライアント 1 3 4 により再生制御メタファイルに含まれる再生制御情報の確認が行われる (S 1 1 6)。この段階で、再生制御メタファイルから各サーバのアドレス情報等が抽出される。次いで、視聴クライアント 1 3 4 から D R M クライアント 1 3 2 に対してライセンス取得指示が発行される (S 1 1 8)。

20

【 0 1 0 6 】

次いで、 D R M クライアント 1 3 2 と D R M / C A S サーバ 1 0 6 との間で相互認証が行われる (S 1 2 0)。次いで、 D R M クライアント 1 3 2 から D R M / C A S サーバ 1 0 6 に対してライセンス取得要求が送信される (S 1 2 2)。次いで、 D R M / C A S サーバ 1 0 6 から D R M クライアント 1 3 2 に対してライセンス情報が提供される (S 1 2 4)。例えば、この段階でライセンス情報と共にワーク鍵が送信される。次いで、 D R M クライアント 1 3 2 によりライセンス状態が確認される (S 1 2 6)。つまり、ワーク鍵の有効期限が確認される。次いで、 D R M クライアント 1 3 2 から視聴クライアント 1 3 4 に対してライセンス状態が通知される (S 1 2 8)。

30

【 0 1 0 7 】

図 6 Bを参照する。次いで、視聴クライアント 1 3 4 とコンテンツ配信サーバ 1 0 4 との間でセッションが開始される (S 1 3 0)。次いで、視聴クライアント 1 3 4 とコンテンツ配信サーバ 1 0 4 との間でライブストリーミングが実行される (S 1 3 2)。このとき、コンテンツ配信サーバ 1 0 4 からスクランブルが施されたコンテンツと、 E C M パケットとが視聴クライアント 1 3 4 に送信される。視聴クライアント 1 3 4 は、ワーク鍵を用いてスクランブル鍵を復号し、そのスクランブル鍵を用いてコンテンツのスクランブルを解除する (S 1 3 4)。同様に、ライブストリーミングが繰り返され (S 1 3 6)、都度、スクランブル鍵の復号、及びコンテンツのデスクランブルが繰り返される (S 1 3 8)。視聴を終了する際には、視聴クライアント 1 3 4 とコンテンツ配信サーバ 1 0 4 との間でセッションの終了処理が行われ (S 1 4 0)、視聴時の処理が終了する。

40

【 0 1 0 8 】

(変形例：視聴契約を締結する場合)

次に、図 7 A、図 7 Bを参照しながら、本実施形態のコンテンツ配信方式に係る一変形例について説明する。本変形例は、あるコンテンツに対して視聴者が視聴契約を締結し、その契約締結時に提供されたライセンスを用いてコンテンツを視聴するというものである。当該変形例のように、視聴契約やコンテンツの購入形態に関しては、種々の変形が可能である。こうした変形を行ったとしても、視聴時の処理シーケンスにおける本実施形態の技術的思想が含まれるものであれば、本実施形態の技術的範囲に属する。

【 0 1 0 9 】

50

まず、図 7 A を参照する。図 7 A に示すように、まず、視聴クライアント 1 3 4 は、ポータルサーバ 1 0 8 に対してコンテンツ視聴契約要求を送信する (S 2 0 2)。次いで、ポータルサーバ 1 0 8 は、認証サーバ 1 1 2 との間で認証処理を実行する (S 2 0 4)。次いで、ポータルサーバ 1 0 8 と D R M / C A S サーバ 1 0 6 との間でライセンス生成処理が行われる (S 2 0 6)。次いで、ポータルサーバ 1 0 8 と課金サーバ 1 1 0 との間でライセンス課金処理が行われる (S 2 0 8)。次いで、ポータルサーバ 1 0 8 から視聴クライアント 1 3 4 に対して契約完了通知が送信される (S 2 1 0)。このように、視聴契約を締結する場合においても、ここまでの処理の流れは購入処理と実質的に同じである。

【 0 1 1 0 】

次いで、視聴クライアント 1 3 4 は、D R M クライアント 1 3 2 に対してライセンス取得指示を伝送する (S 2 1 2)。次いで、D R M クライアント 1 3 2 と D R M / C A S サーバ 1 0 6 との間で相互認証が行われる (S 2 1 4)。次いで、D R M クライアント 1 3 2 から D R M / C A S サーバ 1 0 6 に対してライセンス取得要求が送信される (S 2 1 6)。次いで、D R M / C A S サーバ 1 0 6 から D R M クライアント 1 3 2 に対してライセンス情報が提供される (S 2 1 8)。例えば、この段階でライセンス情報と共にワーク鍵が提供される。次いで、D R M クライアント 1 3 2 によりライセンス状態が確認される (S 2 2 0)。次いで、D R M クライアント 1 3 2 から視聴クライアント 1 3 4 に対してライセンス状態が通知される (S 2 2 2)。

【 0 1 1 1 】

ステップ S 2 1 2 ~ S 2 2 2 までの一連の処理をライセンス取得ステップ S L と呼ぶことにする。ここで示したライセンス取得ステップ S L により、ライセンス情報に含まれる有効期限まで契約者に対してライセンスが供与されるのである。図 7 A に示したシーケンスまでが契約時の処理に相当する。次に、視聴時の処理シーケンスについて説明する。

【 0 1 1 2 】

図 7 B を参照する。図 7 B に示すように、まず、視聴クライアント 1 3 4 は、ポータルサーバ 1 0 8 に対してコンテンツ視聴要求を送信する (S 2 2 4)。次いで、ポータルサーバ 1 0 8 と認証サーバ 1 1 2 との間で認証処理が行われる (S 2 2 6)。次いで、ポータルサーバ 1 0 8 から視聴クライアント 1 3 4 に対して再生制御メタファイルが送信される (S 2 2 8)。次いで、視聴クライアント 1 3 4 とコンテンツ配信サーバ 1 0 4 との間でライブストリーミングが実行される (S 2 3 2)。このとき、コンテンツ配信サーバ 1 0 4 からスクランブルが施されたコンテンツと、E C M パケットとが視聴クライアント 1 3 4 に送信される。

【 0 1 1 3 】

視聴クライアント 1 3 4 は、ワーク鍵を用いてスクランブル鍵を復号し、そのスクランブル鍵を用いてコンテンツのスクランブルを解除する (S 2 3 4)。同様に、ライブストリーミングが繰り返され (S 2 3 6)、都度、スクランブル鍵の復号、及びコンテンツのデスクランブルが繰り返される (S 2 3 8)。視聴を終了する際には、視聴クライアント 1 3 4 とコンテンツ配信サーバ 1 0 4 との間でセッションの終了処理が行われ (S 2 4 0)、視聴時の処理が終了する。なお、契約期間が満了した場合、視聴者は、図 7 A に示すライセンス取得ステップ S L の処理を再び実行し、ライセンスの更新処理を行う。

【 0 1 1 4 】

以上、本実施形態の一変形例に係るコンテンツ配信処理の流れについて説明した。このように、視聴契約を締結する場合においても本実施形態の技術を適用することができる。

【 0 1 1 5 】

[ハードウェア構成]

上記装置が有する各構成要素の機能は、例えば、図 9 に示すハードウェア構成を有する情報処理装置により、上記の機能を実現するためのコンピュータプログラムを用いて実現することが可能である。図 9 は、上記装置の各構成要素が有する機能を実現することが可能な情報処理装置のハードウェア構成を示す説明図である。この情報処理装置の形態は任意であり、例えば、パーソナルコンピュータ、携帯電話、P H S (P e r s o n a l H

10

20

30

40

50

andy - phone System)、PDA(Personal Digital Assistant)等の携帯情報端末、ゲーム機、又は各種の情報家電等の形態がこれに含まれる。

【0116】

図9に示すように、前記の情報処理装置は、主に、CPU(Central Processing Unit)902と、ROM(Read Only Memory)904と、RAM(Random Access Memory)906と、ホストバス908と、ブリッジ910と、外部バス912と、インターフェース914と、入力部916と、出力部918と、記憶部920と、ドライブ922と、接続ポート924と、通信部926とにより構成される。

10

【0117】

CPU902は、例えば、演算処理装置又は制御装置として機能し、ROM904、RAM906、記憶部920、又はリムーバブル記録媒体928に記録された各種プログラムに基づいて各構成要素の動作全般又はその一部を制御する。ROM904は、例えば、CPU902に読み込まれるプログラムや演算に用いるデータ等を格納する。RAM906は、例えば、CPU902に読み込まれるプログラムや、そのプログラムを実行する際に適宜変化する各種パラメータ等を一時的又は永続的に格納する。これらの構成要素は、例えば、高速なデータ伝送が可能なホストバス908によって相互に接続されている。また、ホストバス908は、例えば、ブリッジ910を介して比較的データ伝送速度が低速な外部バス912に接続されている。

20

【0118】

入力部916は、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチ、及びレバー等の操作手段である。また、入力部916は、赤外線やその他の電波を利用して制御信号を送信することが可能なりモートコントロール手段(所謂、リモコン)であってもよい。なお、入力部916は、上記の操作手段を用いて入力された情報を入力信号としてCPU902に伝送するための入力制御回路等により構成されている。

【0119】

出力部918は、例えば、CRT(Cathode Ray Tube)、LCD(Liquid Crystal Display)、PDP(Plasma Display Panel)、又はELD(Electro-Luminescence Display)等のディスプレイ装置、スピーカ、ヘッドホン等のオーディオ出力装置、プリンタ、携帯電話、又はファクシミリ等、取得した情報を利用者に対して視覚的又は聴覚的に通知することが可能な装置である。

30

【0120】

記憶部920は、各種のデータを格納するための装置であり、例えば、ハードディスクドライブ(HDD; Hard Disk Drive)等の磁気記憶デバイス、半導体記憶デバイス、光記憶デバイス、又は光磁気記憶デバイス等により構成される。

【0121】

ドライブ922は、例えば、磁気ディスク、光ディスク、光磁気ディスク、又は半導体メモリ等のリムーバブル記録媒体928に記録された情報を読み出し、又はリムーバブル記録媒体928に情報を書き込む装置である。リムーバブル記録媒体928は、例えば、DVDメディア、Blu-rayメディア、HD DVDメディア、コンパクトフラッシュ(登録商標)(CF; Compact Flash)、メモリースティック、又はSDメモ리카ード(Secure Digital memory card)等である。もちろん、リムーバブル記録媒体928は、例えば、非接触型ICチップを搭載したICカード(Integrated Circuit Card)、又は電子機器等であってもよい。

40

【0122】

接続ポート924は、例えば、USB(Universal Serial Bus)ポート、IEEE1394ポート、SCSI(Small Computer Syst

50

em Interface)、RS-232Cポート、又は光オーディオ端子等のような外部接続機器930を接続するためのポートである。外部接続機器930は、例えば、プリンタ、携帯音楽プレーヤ、デジタルカメラ、デジタルビデオカメラ、又はICレコーダ等である。

【0123】

通信部926は、ネットワーク932に接続するための通信デバイスであり、例えば、有線又は無線LAN(Local Area Network)、Bluetooth(登録商標)、又はUSB(Wireless USB)用の通信カード、光通信のルータ、ADSL(Asymmetric Digital Subscriber Line)用のルータ、又は各種通信のモデム等である。また、通信部926に接続されるネットワーク932は、有線又は無線により接続されたネットワークにより構成され、例えば、インターネット、家庭内LAN、赤外線通信、可視光通信、放送、又は衛星通信等である。

【0124】

[まとめ]

最後に、本実施形態のコンテンツ配信システム、及びコンテンツ受信端末が有する機能構成と、当該機能構成が奏する作用効果について簡単に纏める。

【0125】

まず、本実施形態に係るコンテンツ配信システム、及びコンテンツ受信端末が有する機能構成は次のように表現することができる。

【0126】

本実施形態に係るコンテンツ配信システムは、複数のコンテンツ配信サーバと、ライセンスサーバと、ポータルサーバと、コンテンツ受信端末とにより構成される。

【0127】

ここで言うコンテンツ配信サーバの一例が、コンテンツサーバ102、コンテンツ配信サーバ104である。また、ライセンスサーバの一例が、DRM/CASサーバ106である。さらに、ここで言うポータルサーバ、コンテンツ受信端末の一例が、それぞれ、既に説明したポータルサーバ108、コンテンツ受信端末130である。

【0128】

このコンテンツ配信サーバは、スクランブルが施されたコンテンツを配信すると共に、前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信するものである。つまり、このコンテンツ配信サーバは、上記のMCライセンス方式のような2重暗号処理が施されたコンテンツをストリーミング配信するものである。

【0129】

また、ライセンスサーバは、所定の前記コンテンツ配信サーバから配信される前記暗号化されたスクランブル鍵を復号するためのワーク鍵を提供するものである。もちろん、ワーク鍵は、所定の購入処理又は契約処理等に基づいてライセンスが供与された視聴者に対して提供されるものである。また、ポータルサーバは、前記所定のコンテンツ配信サーバのアドレス情報を提供するものである。なお、ポータルサーバは、視聴者にコンテンツを指定させるための窓口としての役割を果たす。つまり、ポータルサーバは、各コンテンツと、それを配信するコンテンツ配信サーバとの橋渡しを行うのである。その方法の1つが、アドレス情報の提供である。

【0130】

そして、コンテンツ受信端末は、アドレス情報取得部と、コンテンツ取得部と、スクランブル鍵復号部と、スクランブル解除部とを有している。

【0131】

このアドレス情報取得部は、前記ポータルサーバから前記所定のコンテンツ配信サーバのアドレス情報を取得するものである。また、コンテンツ取得部は、前記アドレス情報取得部により取得されたアドレス情報を参照して前記所定のコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵を取得するものである。スクランブル鍵復号部は、前

10

20

30

40

50

記ライセンスサーバから取得したワーク鍵を用いて前記スクランブル鍵を復号するものである。さらに、スクランブル解除部は、前記スクランブル鍵を用いて前記コンテンツのスクランブルを解除するものである。

【0132】

ここで言うアドレス情報取得部の一例が、再生制御メタ取得部176である。但し、再生制御メタ取得部176の場合、再生制御メタファイルを取得し、その中に含まれるアドレス情報を抽出することで、コンテンツ配信サーバ104のアドレス情報を取得している。また、ここで言うコンテンツ取得部の一例が、コンテンツ取得部180である。また、スクランブル鍵復号部の一例が、スクランブル鍵復号部182である。さらに、スクランブル解除部の一例が、デスクランブル部184である。

10

【0133】

また、前記ポータルサーバは、前記所定のコンテンツ配信サーバの再生制御方式を示す情報をさらに提供するように構成されていてもよい。この再生制御方式には、例えば、倍速再生やストップ等が含まれる。この場合、前記コンテンツ受信端末は、前記ポータルサーバから再生制御方式の情報を取得する再生制御情報取得部をさらに有する。そして、このコンテンツ受信端末は、前記再生制御情報取得部により取得された情報が示す再生制御方式に従って前記コンテンツ取得部により前記コンテンツ及びスクランブル鍵を取得する。このような構成にすることで、再生制御方式が異なるためにコンテンツが正しく受信出来なくなる状況を回避することができる。

【0134】

20

なお、ここで言う再生制御情報取得部の一例が、再生制御メタ取得部176である。但し、再生制御メタ取得部176の場合、再生制御メタファイルを取得し、その中に含まれる再生制御方式の情報を抽出することで、再生制御方式の情報を取得している。

【0135】

また、前記コンテンツ配信システムは、コンテンツ鍵を用いて復号可能な暗号化されたコンテンツのみを配信するコンテンツ配信サーバをさらに含むように構成されることがある。例えば、VODライセンス方式のコンテンツ配信システムをベースに、本実施形態に係るコンテンツ配信システムを構築する場合において、このようなシステム構成になる場合がある。

【0136】

30

このとき、前記ライセンスサーバは、所定の前記コンテンツ配信サーバにより配信されるコンテンツの配信形態に応じて前記ワーク鍵又は前記コンテンツ鍵を提供するように構成される。また、前記ポータルサーバは、前記所定のコンテンツ配信サーバにより配信されるコンテンツの配信形態を示す情報をさらに提供するように構成される。この配信形態を示す情報の一例が、再生制御メタファイルに含まれるコンテンツ種別情報やライセンス形態の情報である。通常、コンテンツの配信形態とライセンス形態（又は暗号形態）とは対応関係があるため、この情報を得ることにより、ストリーミング配信されるコンテンツの配信形態を識別することができる。

【0137】

40

さらに、前記コンテンツ受信端末には、前記所定のコンテンツ配信サーバにより配信されるコンテンツの配信形態を示す情報を前記ポータルサーバから取得する配信形態取得部と、前記ライセンスサーバから取得したコンテンツ鍵を用いて前記暗号化されたコンテンツを復号するコンテンツ復号部と、がさらに設けられる。そして、このコンテンツ受信端末は、前記配信形態取得部により取得された情報が示す配信形態がコンテンツ鍵方式である場合、前記コンテンツ取得部により前記暗号化されたコンテンツを取得し、前記コンテンツ復号部によりコンテンツを復号するように構成される。

【0138】

ここで言う配信形態取得部の一例が、再生制御メタ取得部176である。但し、再生制御メタ取得部176の場合、再生制御メタファイルを取得し、その中に含まれるコンテンツ種別情報等を抽出してコンテンツのライセンス形態を識別する。上記の通り、コンテン

50

ツの配信形態が分かると、例えば、そのコンテンツがV o Dライセンス方式で暗号化されたものか、M Cライセンス方式で暗号化されたものか、或いは、その他のライセンス方式で暗号化されたものかが識別できる。また、本実施形態の場合、M Cライセンス方式と実質的に同じ2重暗号方式が基本であるため、その方式か別の方式かを容易に識別できるようになる。

【0139】

また、ここで言うコンテンツ復号部の一例が、デスクランブル部184である。デスクランブル部184の基本的な動作は、復号されたスクランブル鍵を用いてコンテンツのスクランブルを解除することである。しかし、本実施形態の場合、コンテンツ鍵方式で暗号化されたコンテンツにも対応できるようにするため、デスクランブル部184は、コンテンツ鍵を用いてコンテンツを復号することが可能なように構成されている点については既に説明した。このように、複数のライセンス方式又は暗号化形態に対応することで、本実施形態の技術を既存のシステムに適用してシステム全体の可用性を容易に高めることができるようになる。

10

【0140】

また、前記コンテンツ受信端末が有するスクランブル鍵復号部は、前記コンテンツ取得部によりコンテンツ及びスクランブル鍵が取得される度に前記ライセンスサーバからワーク鍵を取得するように構成されていてもよい。同様に、前記コンテンツ受信端末が有するコンテンツ復号部は、前記コンテンツ取得部により前記暗号化されたコンテンツが取得される度に前記ライセンスサーバからコンテンツ鍵を取得するように構成されていてもよい。このような構成にすることで、コンテンツ単位でのライセンス管理が実現できるようになる。

20

【0141】

また、コンテンツ受信端末の機能構成は、次のように表現することもできる。

【0142】

当該コンテンツ受信端末は、アドレス情報取得部と、配信形態取得部と、コンテンツ取得部と、鍵取得部と、スクランブル鍵復号部と、コンテンツ復号部とを有する。

【0143】

アドレス情報取得部は、スクランブルが施されたコンテンツ及び前記スクランブルの解除に用いる暗号化されたスクランブル鍵をストリーミング配信するコンテンツ配信サーバ、又はコンテンツ鍵を用いて復号可能な暗号化されたコンテンツを配信するコンテンツ配信サーバのアドレス情報を取得するものである。

30

【0144】

さらに、配信形態取得部は、前記アドレス情報に対応するコンテンツ配信サーバから配信されるコンテンツの配信形態が示された情報を取得するものである。そして、コンテンツ取得部は、前記アドレス情報取得部により取得されたアドレス情報を参照し、前記配信形態取得部により取得された情報に示された配信形態に応じて、当該アドレス情報に対応するコンテンツ配信サーバから前記コンテンツ及び前記スクランブル鍵、或いは、前記暗号化されたコンテンツを取得するものである。

【0145】

また、鍵取得部は、前記配信形態がワーク鍵方式の場合に前記スクランブル鍵を復号するためのワーク鍵を取得し、前記配信形態がコンテンツ鍵方式の場合に前記コンテンツ鍵を取得するものである。スクランブル鍵復号部は、前記配信形態がワーク鍵方式の場合に前記ワーク鍵を用いて前記スクランブル鍵を復号するものである。そして、コンテンツ復号部は、前記配信形態がワーク鍵方式の場合に前記スクランブル鍵を用いてコンテンツのスクランブルを解除し、前記暗号化形態がコンテンツ鍵方式の場合に前記コンテンツ鍵を用いて前記暗号化されたコンテンツを復号するものである。

40

【0146】

ここで言うアドレス情報取得部、配信形態取得部の一例が、再生制御メタ取得部176である。また、コンテンツ取得部の一例が、コンテンツ取得部180である。さらに、鍵

50

取得部の一例が、ライセンス取得部 172 である。そして、スクランブル鍵復号部の一例が、スクランブル鍵復号部 182 である。また、コンテンツ復号部の一例が、デスクランブル部 184 である。このように配信形態に応じて処理を切り替えることにより、複数のライセンス方式を利用した配信形態に対応することが可能になる。その結果、コンテンツ毎に配信形態が異なるとしても、視聴者は、各コンテンツのライセンスがどのような配信形態であるかを意識せずに視聴することができる。

【0147】

このように、本実施形態に係る技術は、視聴度にコンテンツの取得先を知る必要があるライブストリーミング配信によるコンテンツ提供方式に対し、DRM/CASシステムと連携してライセンスの発行及び管理が行えるようにしたものである。さらに、本実施形態は、コンテンツ受信端末による配信形態の判別、及びコンテンツ受信処理の切り替えを行うことが可能なコンテンツ配信システムを提供するものである。

10

【0148】

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説明したが、本発明は係る例に限定されないことは言うまでもない。当業者であれば、特許請求の範囲に記載された範疇内において、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、そ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。

【図面の簡単な説明】

【0149】

【図1】VoD方式によるコンテンツ提供システムの構成例を示す説明図である。

20

【図2】MC方式によるコンテンツ提供システムの構成例を示す説明図である。

【図3】本発明の一実施形態に係るコンテンツ提供システムのシステム構成の一例を示す説明図である。

【図4】本実施形態に係るコンテンツサーバの機能構成の一例を示す説明図である。

【図5】本実施形態に係るコンテンツ受信端末の機能構成の一例を示す説明図である。

【図6A】本実施形態に係るコンテンツ視聴処理の流れを示す説明図である。

【図6B】本実施形態に係るコンテンツ視聴処理の流れを示す説明図である。

【図7A】本実施形態の変形例に係るコンテンツ視聴処理の流れ（契約時の処理）を示す説明図である。

【図7B】本実施形態の変形例に係るコンテンツ視聴処理の流れ（視聴時の処理）を示す説明図である。

30

【図8】本実施形態に係る再生制御メタファイル、及びライセンス情報の具体例を示す説明図である。

【図9】本実施形態に係る端末又はサーバのハードウェア構成例を示す説明図である。

【符号の説明】

【0150】

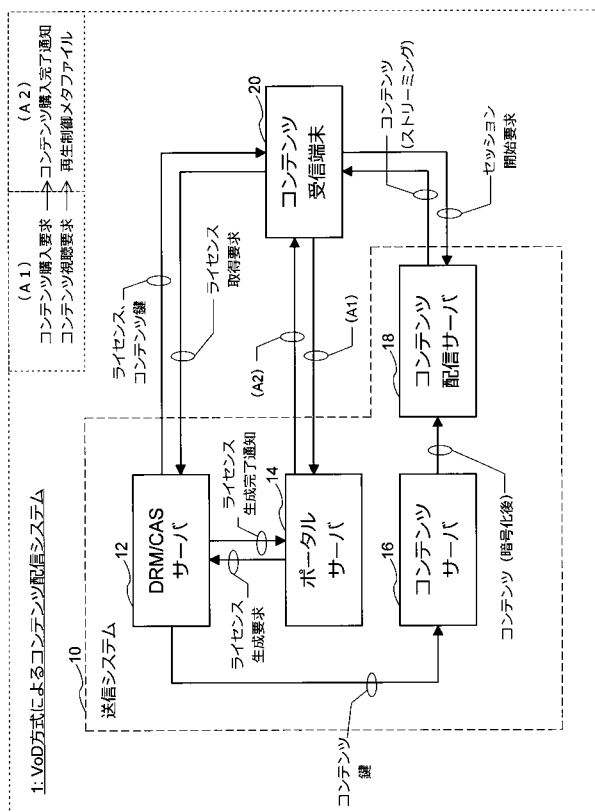
- 1000 コンテンツ配信システム
- 100 送信システム
- 102 コンテンツサーバ
- 104 コンテンツ配信サーバ
- 106 DRM/CASサーバ
- 108 ポータルサーバ
- 110 課金サーバ
- 112 認証サーバ
- 130 コンテンツ受信端末
- 132 DRMクライアント
- 134 視聴クライアント
- 152 記憶部
- 154 スクランブル部
- 156 ワーク鍵取得部

40

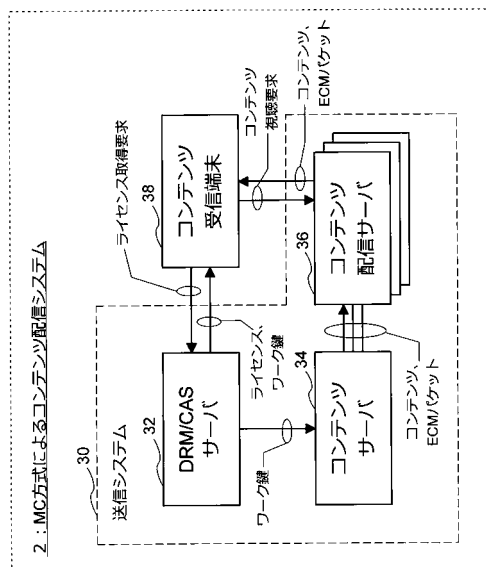
50

- 1 5 8 スクランブル鍵暗号化部
- 1 6 0 多重送信部
- 1 7 2 ライセンス取得部
- 1 7 4 コンテンツ購入処理部
- 1 7 6 再生制御メタ取得部
- 1 7 8 コンテンツ配信形態判別部
- 1 8 0 コンテンツ取得部
- 1 8 2 スクランブル鍵復号部
- 1 8 4 デスクランブル部

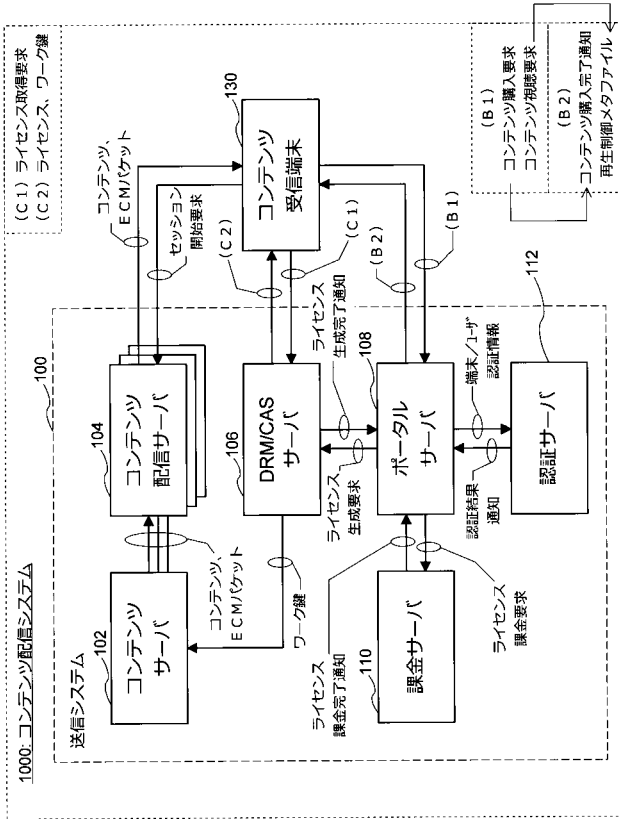
【図 1】



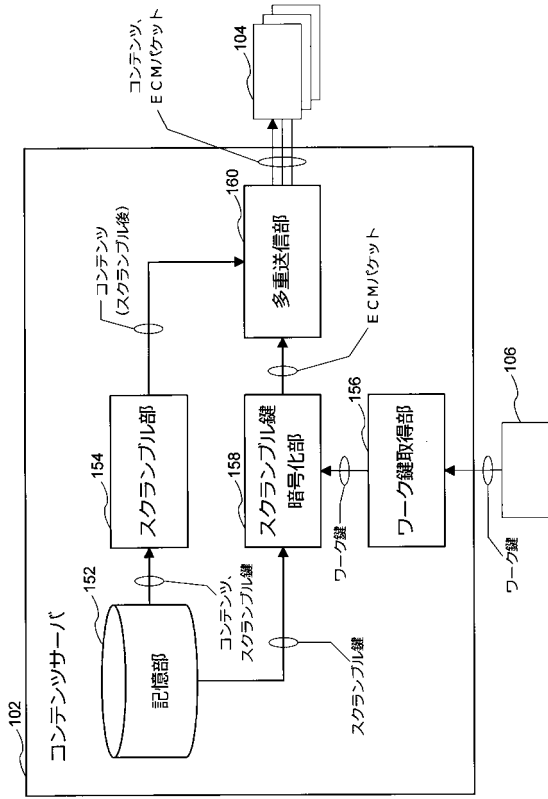
【図 2】



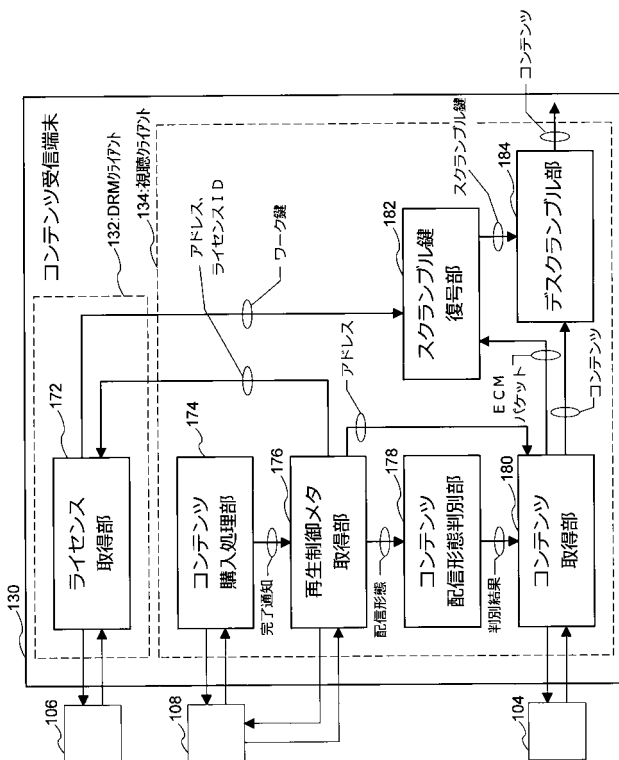
【 図 3 】



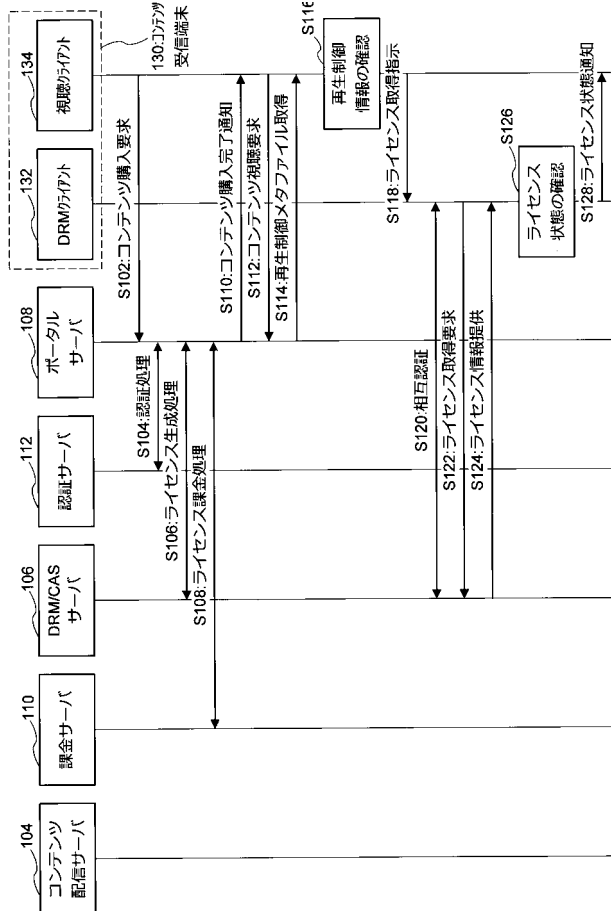
【 図 4 】



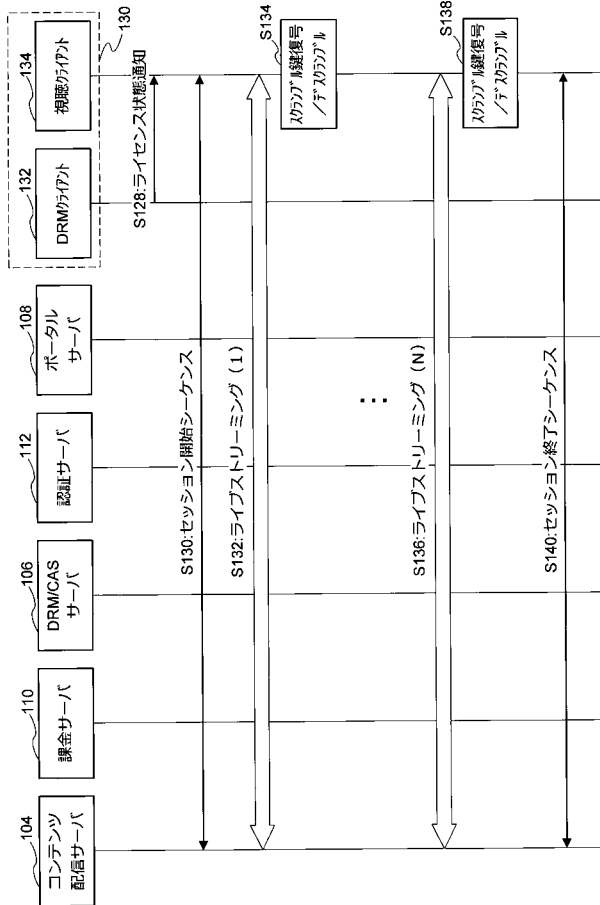
【 図 5 】



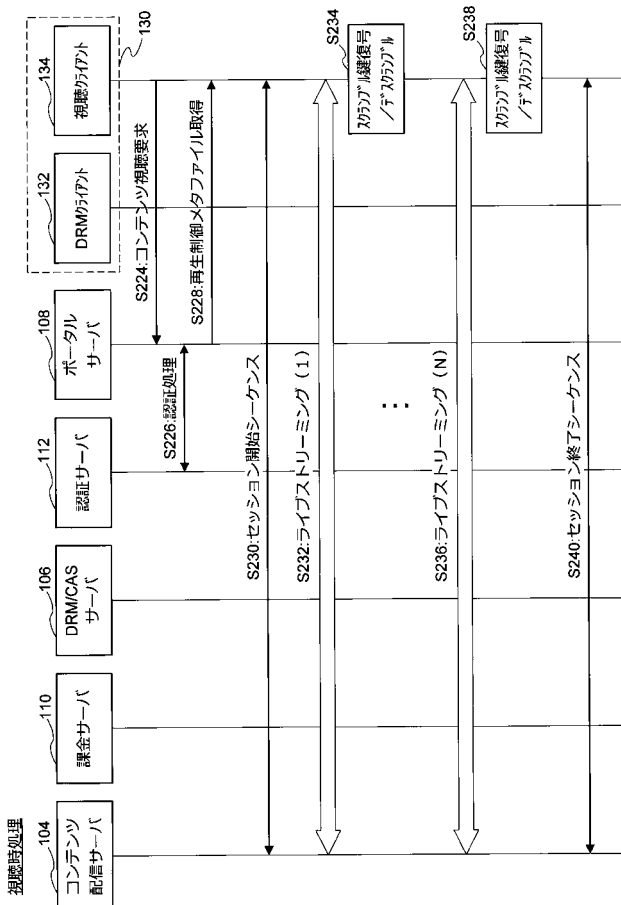
【 図 6 A 】



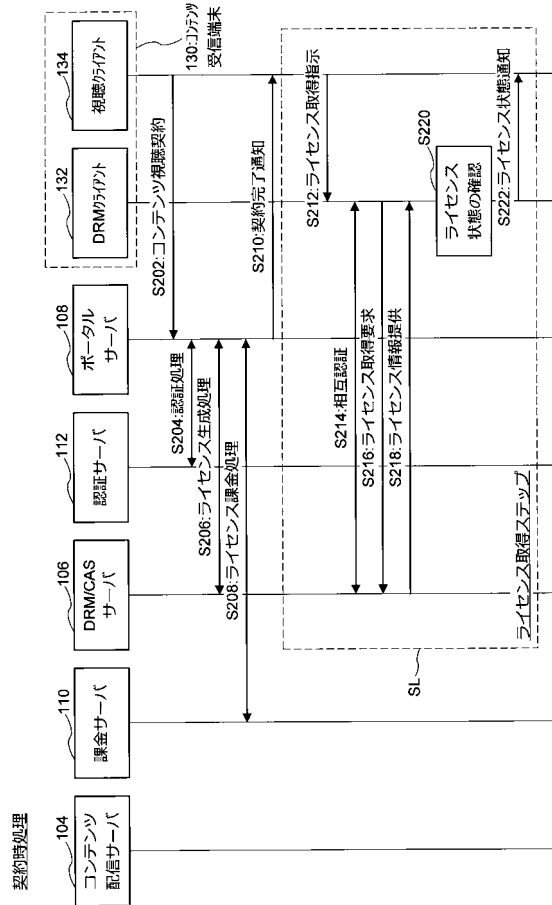
【図 6 B】



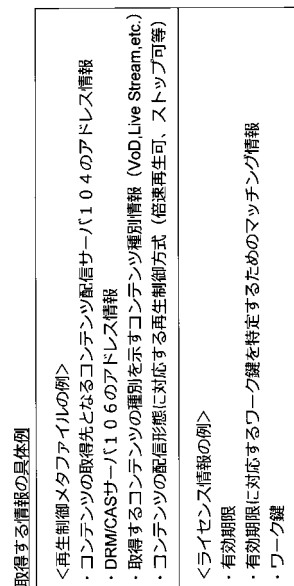
【図 7 B】



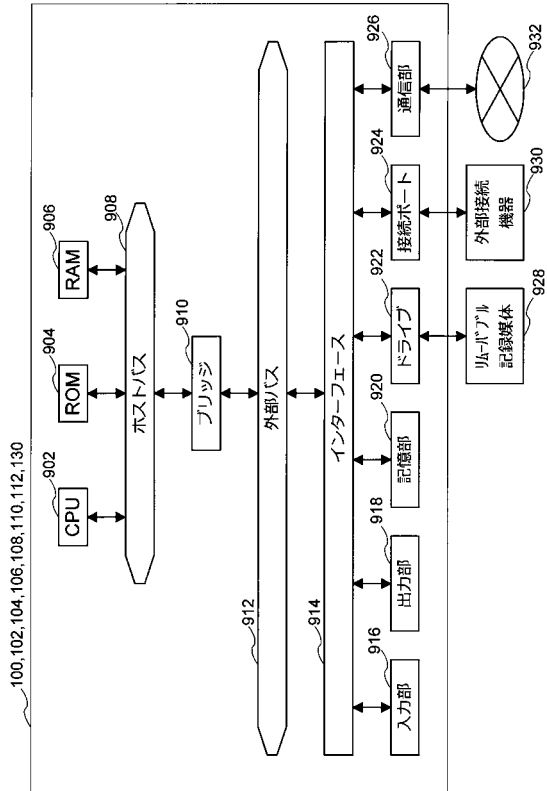
【図 7 A】



【図 8】



【図 9】



フロントページの続き

(51)Int.Cl. F I テーマコード(参考)
H 0 4 L 9/00 6 0 1 E

(72)発明者 北里 直久
東京都港区港南 1 丁目 7 番 1 号 ソニー株式会社内

(72)発明者 増田 康人
東京都港区港南 1 丁目 7 番 1 号 ソニー株式会社内

(72)発明者 川畑 哲
東京都港区港南 1 丁目 7 番 1 号 ソニー株式会社内

F ターム(参考) 5C164 MB34S PA24 SA53P SB03S SC02P UB03S UC22P
5J104 AA12 AA16 EA04 EA08 EA18 JA03 NA02 NA37 PA07