M-7

サーバー型放送における コンテンツのアクセス制御方式

RMP(Rights Management and Protection) System for Digital Broadcasting Based on Home Servers

西本 友成† 馬場 秋継† 栗岡 辰弥† 難波 誠一†
Yusei Nishimoto†, Akitsugu Baba†, Tatsuya Kurioka† and Seiichi Namba†

1. まえがき

サーバー型放送は、受信機に大容量の番組蓄積装置を備え、コンテンツを一旦蓄積することで、放送時間に拘束されない番組視聴や、ハイライト的な番組視聴などの多様な放送サービスを視聴者に提供する新しい放送として注目されている。

我々は、番組関連情報であるメタデータを利用した新しいサーバー型放送サービスについて検討した結果を既に報告した[1][2]。この様な放送サービスを実現するためには、蓄積されたコンテンツを保護しその利用方法を制御して不正利用を防止する、新しいアクセス制御技術が不可欠である。コンテンツのアクセス制御を行い、許諾に基づかない不正利用からコンテンツを保護するシステムをRMP[3](Rights Management and Protection)システムと呼ぶ。

本稿では、まず、サーバー型放送のための RMP システムの要求条件と、開発した RMP システムの概要について述べ、試作した RMP 検証実験システムで行った暗号化コンテンツの蓄積再生実験の検証結果について報告する。

2. RMP システムに対する要求条件

現行 BS デジタル放送では、契約者のみにコンテンツを受信させる限定受信システムを利用して、放送受信時におけるコンテンツのアクセス制御が可能である。しかし、蓄積されたコンテンツに対してアクセス制御ができない。

そこで、放送受信時だけでなく、蓄積されたコンテンツのアクセス制御が可能な RMP システムの検討を行った。

RMP システムの要求条件を、以下の通り整理した。

1)放送局側からの制御でコンテンツ保護が行えること
2)蓄積されたコンテンツに対してコンテンツ単位(番組など)の保護と利用制御ができること
3)コンテンツの多様な蓄積利用のために高度な利用制御(利用期間、利用形態、課金など)ができること
4)現行の限定受信システムとの整合性を確保すること

3. 開発した RMP システム

2 項で述べた要求条件を満足する RMP システムを開発した。図 1 に、開発した RMP システムの概要を示す。

現行の限定受信システムは、秒単位で異なる鍵でコンテンツをスクランブルするスクランブル鍵 Ks、Ks を暗号化するワーク鍵 Kw、受信機のセキュリティモジュールに固有のマスター鍵 Km の 3 重鍵方式でコンテンツを暗号化する。

開発した RMP システムは、再生時に番組単位でコンテンツのアクセス制御を行うために、番組などの単位で付与するコンテンツ鍵 Kc を加えた 4 重鍵方式とし、暗号化した状態で蓄積し視聴時にコンテンツを復号する方式とした。さらに、コンテンツ鍵 Kc をコンテンツの利用制御情報で

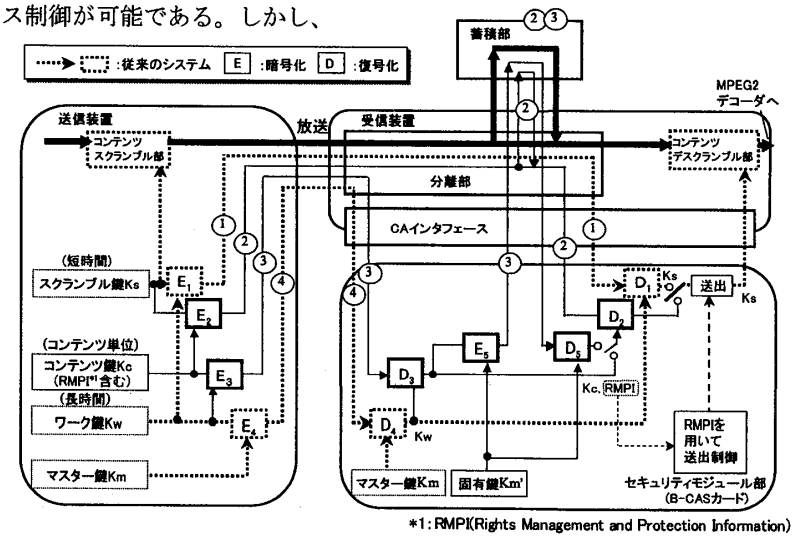

図 1 開発した RMP システムの概要

† NHK 放送技術研究所
† NHK Science and Technical Research Labs.

あるRMPI (RMP Information:例えば、利用期間など)と併せて送出することにより、蓄積されたコンテンツを番組などの単位で利用制御可能とした。このように、放送受信時と蓄積後視聴時の双方においてコンテンツの保護と利用制御が可能な方式を開発した。

また、1対多のコンテンツ伝送である放送に対応するために、共通情報であるECM(Entitlement Control Message)を用いて、コンテンツ鍵 Kc を複数の受信機に同時に送出できる方式とした。

4. 検証実験

4.1 試作したRMP検証実験システム

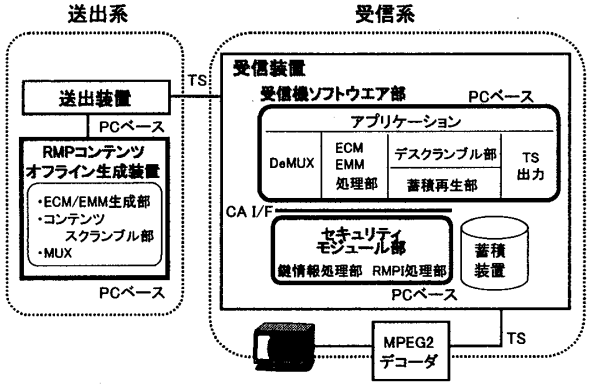

図2　試作したRMP検証実験システム

図2に、試作したRMP検証実験システムを示す。

受信装置は、受信機ソフトウエア部およびセキュリティモジュール部から構成される。セキュリティモジュール部とデスクランブル部は、ソフトウエアにより暗号化したコンテンツや鍵を復号でき暗号アルゴリズムを任意に選択できる。

4.2 暗号化コンテンツの蓄積再生実験

蓄積装置へ4重鍵方式で暗号化したHDTVのコンテンツを蓄積し、通常再生およびノンリニア再生実験を行った。ノンリニア再生は、番組内のシーンを15秒間隔で、再生とスキップを繰り返すシーケンスとした。

表1に、評価した暗号化コンテンツの生成パラメータを示す。今回は、コンテンツの暗号化アルゴリズムとして、ライセンスフリーで、現行限定受信システムで使用されているMULTI2と同じ鍵長とブロック長のBlowfishを用いた。

図3に、ノンリニア再生時のMPEG2デコーダの受信バッファ残量、及び暗号化コンテンツの復号処理速度の時間変化を示す。復号処理速度は、暗号化されたコンテンツ及び鍵情報のすべての復号処理に要する時間から算出した。

今回の実験により次の動作を検証できた。

1)受信バッファを破綻することなく復号できていることから、4重鍵方式で暗号化したコンテンツの蓄積再生およびノンリニア再生を実時間で処理できることを確認した。

2)復号処理速度は約51Mbit/s(平均値)であることから、検証実験システムの暗号復号処理性能として、同時に2チャンネルのHDTVのデスクランブル処理ができることを確認した。

表1　評価した暗号化コンテンツの生成パラメータ

MPEG2-TS ビットレート		23.911Mbps (HDTV)
暗号化方式	コンテンツ	共通鍵暗号化方式 BlowFish (ブロック長64bit、鍵長64bit)
	ECM,EMM 鍵情報	共通鍵暗号化方式AES (ブロック長128bit、鍵長256bit)
ECM-Kc送出間隔		100ms
Kc配布用ECM 送出間隔		500ms
スクランブル鍵Ksの 変更間隔		1秒程度
暗号化対象		TS(ペイロード部184byte)
コンテンツの 蓄積装置		ハードディスクドライブ(SCSI)

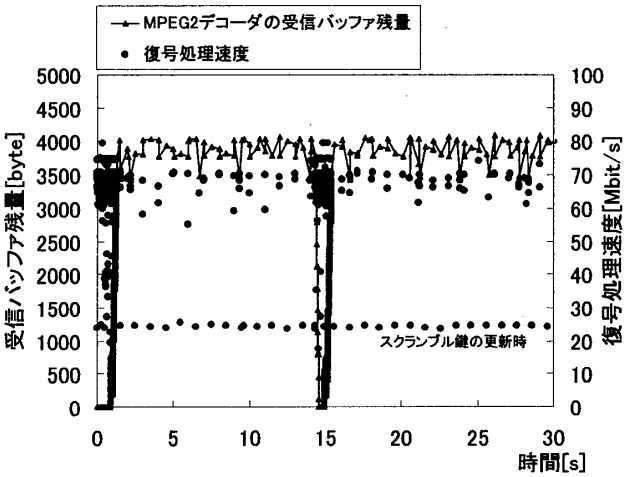

図3　ノンリニア再生時の受信バッファ残量と復号処理速度の時間変化

5. まとめ

サーバー型放送におけるコンテンツ保護の要求条件を明らかにし、その要求条件を満足するRMPシステムを開発した。開発したRMPシステムは、従来どおり放送受信時の視聴を可能としながら蓄積後視聴の利用制御を実現し、1対多のコンテンツ伝送である放送に適している。

今回開発したRMPシステムを基に、コンテンツの蓄積利用など、放送コンテンツの多様な視聴と利用が行えるコンテンツ保護システムの実現を目指していく。

【参考文献】

[1] 栗岡、南、藤澤、加藤、奥田、沼澤: “デジタルHDTVに対応したホームサーバーの開発”, 映情学技報, 22, 54, pp. 23-29(1998)

[2]馬場、西本、南、栗岡: “メタデータを利用したサーバー型放送の一検討” 映情学年大、1-5(2002)

[3]TV-AnytimeForum: “Rights Management & Protection Requirements R-5”, TV039r7(2000)