

デジタルTV対応PC向け権利保護LSI

Digital Content Rights Protection LSI for PC-Based Digital TV Receivers

あらまし

本稿では、PCによるデジタル放送受信を可能にする権利保護LSIについて述べる。PCは、ソフトウェア仕様が公開されたオープンアーキテクチャである。スキルある人間なら誰でもハッキングできる可能性がある。このためデジタル放送処理ソフトウェアは放送事業者などコンテンツホルダから危険とされ、これがPCでのデジタル放送視聴の障壁となっていた。

著者らは、このようなオープンアーキテクチャPCを使っても、コンテンツの権利保護ができる手法を考案し、それを権利保護LSIとして実装した。これによって、PCを所持するユーザにとっては、新たにデジタルTV受信機を購入することなく、PCを使ってデジタル放送を楽しむ道が今後開ける。

Abstract

This paper describes a Digital Content Rights Protection LSI that prevents unauthorized reception of digital broadcasts using PCs. Because PC software is basically open (i.e., its software specifications are public knowledge), skilled hackers may gain unauthorized access to the software. As a result, broadcasters and other content holders have concern about potential risks of digital broadcasting softwares, which have stalled the development of PC-software based digital TV receivers for some time. We have therefore designed a content protection scheme that protects content even in open architecture environments such as PCs and implemented it in the Digital Content Rights Protection LSI. This LSI will open the way for authorized persons to watch digital TV broadcasts on their PCs without having to buy a costly digital TV receiver.



小檜山清之（こひやま きよし）
システムLSI開発研究所 所属
現在、放送コンテンツ権利保護LSI
の研究開発に従事。



藤山博之（ふじやま ひろゆき）
システムマイクロ事業部第一設計部
所属
現在、ネットワーク、セキュリティ
関連のLSI、および放送コンテンツ
権利保護LSIの研究開発に従事。



吉武敏幸（よしただけ としゆき）
システムLSI開発研究所先端シス
テムLSI研究部 所属
現在、放送コンテンツ権利保護LSI
の研究開発に従事。

ま え が き

近年、TV放送のデジタル化が進んでいる。CS放送によって始まったデジタル放送は、2000年のBSデジタル放送開始、2002年の110°CS放送の開始を経て、2003年12月より地上デジタル放送が開始された。地上デジタル放送は2006年には全国へ拡大され、2011年には、現行のアナログ放送が終了予定である。

一方、家庭では従来のテレビ受信機に加え、PCによるアナログTV放送の視聴と録画が一般的になっている。コンシューマ向けデスクトップPCの多くはTV受信/録画機能を有し、この流れはノートPCにも広がりつつある。すでに多くのコンシューマ向けPCはアナログ放送に対応している。今後は、デジタル放送受信への対応も進むことが自然の流れと考えられる。

しかしデジタル放送コンテンツは、複製し配信してもアナログのような画質劣化が発生しない。このため、PCを経由してコンテンツをインターネットなどで無断配信されると、コンテンツ権利者は甚大な被害を被るなどの問題がある。

このような状況のもとでは、PCにおけるデジタルコンテンツの複製や移動を制限する権利保護方式、またはその実現を可能にする権利保護LSIなどの開発が強く求められる。

本稿では、PCによるデジタル放送受信を可能にする権利保護LSIについて述べる。

従来技術の課題：セキュア領域の実現

デジタル放送受信機能付きPCで想定されるデジタル放送受信システムの概要を図-1に示す。この図では、PCはMPEG-2圧縮されたデジタル放送コンテンツを受信し、いったんHDD上に蓄積した後、圧縮MPEG信号の伸張など各種信号処理を実行し、最終画像をモニタ表示する。

この際、PCは、オープンアーキテクチャであり、さらに複数のアプリケーションプログラムが同時実行されるマルチタスク環境である。ハッキングプログラムなどほかのアプリケーションが各リソースに容易にアクセス可能である。このため、例えばHDD上に保存されるコンテンツも容易に複製されないように暗号化が必要がある。また、コンテ

ツの暗号化/復号化、MPEG伸張、表示などの各種処理は、ほかのアプリケーションからハッキングできないセキュア領域で行う必要がある。

さらにデジタル放送コンテンツの扱いに関しては電波産業会（ARIB）のデジタル放送運用規定^{(1),(2)}があり、準拠する必要がある。

セキュア領域をPC内に実現する方法は、様々である。以下に代表的な従来技術によるセキュア領域の実現方法を示す。

● 処理のハードウェア化

復号化処理（暗号解除）、伸張処理、表示処理をすべてPCから独立したハードウェアで行う方法である。PC上のアプリケーションプログラムと独立しており、しかも一般的にハードウェアはLSI化されている。LSI内部を解析するのは、一般のハッカーには不可能であり、セキュリティ強度は十分と言える。しかし、すべて専用ハードウェアを必要とするため高コストになる。

● ソフトウェアの難読化

処理をプログラム解析が困難な耐タンパ化ソフトウェアで行う方法がある。代表的なソフトウェアの耐タンパ化技術に難読化がある⁽³⁾。これは、処理アルゴリズムなどをわざと複雑にし、ハッキングの前提であるプログラムコードの解析を限りなく困難にする方法である。解析できなければプログラムの改ざんや覗き見などハッキングは不可能である。しかしプログラムコードがPCのメモリ上で動作する限り、コードを読み取り、解析することは可能であり、完全な耐タンパ化は困難である。ハッカーが十分な労力をかければプログラム内容は解析され、ハッキングプログラムを開発される恐れがある。ま

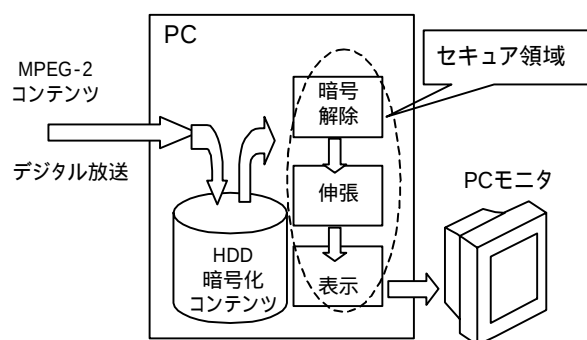


図-1 デジタル放送受信システム概要（想定）
Fig.1-Typical digital TV receiver system.

た複雑に難読化されたソフトウェアは実行性能の低下を引き起こしかねない。

以上二つの従来技術は、コンシューマ向けPCという市場への適用を考えるとどちらも問題がある。処理のハードウェア化は、セキュリティ強度は十分あるが、コストが高く民生市場に向かない。また、ソフトウェアの難読化は、プログラムコードの解析によるハッキングの危険が付きまとう。セキュリティ強度が十分と言えない。

民生市場で要求されているのは、ハードウェア並みのセキュリティ強度とソフトウェアの低コストを兼ね備えたセキュリティ方式である。

デジタルコンテンツ権利保護技術

前述した従来技術の課題を解決するため、著者らは、オープンアーキテクチャPC環境でも、コンテンツの権利保護ができる手法を考案し、それを権利保護LSIとして実装し、ハードウェアレベルのセキュリティ強度とソフトウェアの低コストの両立を可能にした。また、実験環境を構築し、後述する実証確認を行った。

以下、権利保護LSIを使用したデジタルコンテンツ権利保護技術について述べる。

本LSIのポイントは、処理の大半をPC上のソフトウェアに任せつつ、コンテンツおよびソフトウェアのセキュリティ維持に必要な最低限の機能のみをハードウェア化したことにある。

権利保護LSIを搭載したデジタル放送受信PCの権利保護システムの構成を図-2に示す。

図中、上部に示した部分がPC本体で処理される

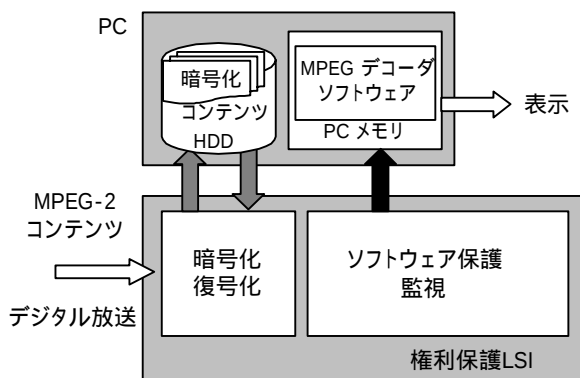


図-2 権利保護LSI搭載デジタル放送受信PC
Fig.2-PC-based digital TV protected by "Digital Content Rights Protection" LSI.

部分であり、PCメモリおよびHDDを示す。下部がセキュリティ維持機能のみをハードウェア化した権利保護LSIに相当する。権利保護LSIはPCIバスインタフェースによりPCへのアドオンカードとして接続される。

権利保護LSIのセキュリティ維持機能には、コンテンツを保護するための暗号化/復号化機能とソフトウェア保護機能がある。MPEG-2形式のデジタル放送コンテンツは、入力時は、MULTI2形式の暗号がかかっており、これをいったん復号し、再度暗号化する（これを一般にローカル暗号化という）。ローカル暗号化されたコンテンツは、PCIバスを経由しHDDに蓄積される。ローカル暗号化の効果により、PCIバス上、HDD上のコンテンツは保護される。

ソフトウェア保護機能とは、PCメモリ上で動作するソフトウェアの監視を行う機能である。権利保護LSIに様々な監視機能があり、常にリアルタイムでソフトウェアのハッキング検出を行っている。ハッキングを検出した場合、コンテンツ処理ソフトウェアの動作を無効化する。

この機能によりハッキング防止を実現している。

権利保護LSI機能概要

権利保護LSIのブロック図を図-3に示す。権利保護LSIには、暗号化・復号化回路、32ビットRISCマイクロプロセッサコア、周辺接続用のインタフェース回路がある。以下、権利保護LSIの主要な機能について述べる。

暗号化・復号化回路の中にMULTI2暗号復号化回路があり、入力されたMULTI2暗号化デジタル放送コンテンツを復号する。MULTI2暗号復号鍵（一般にスクランブル鍵という）は、外部接続のB-CASカードから入手する。B-CASカードと権利保護LSIは、ICカードインタフェースを経由し情報交換する。スクランブル鍵は、定期的に更新される。更新されるたび、権利保護LSI内部のマイクロコントローラコアがB-CASカードから新規のスクランブル鍵を入手する。また、暗号化・復号化回路にローカル暗号化回路が含まれ、MULTI2暗号を復号したコンテンツのローカル暗号化処理を行う。ローカル暗号化されたコンテンツはPCIバスを経由し、いったんHDDに蓄積され、表示するときに

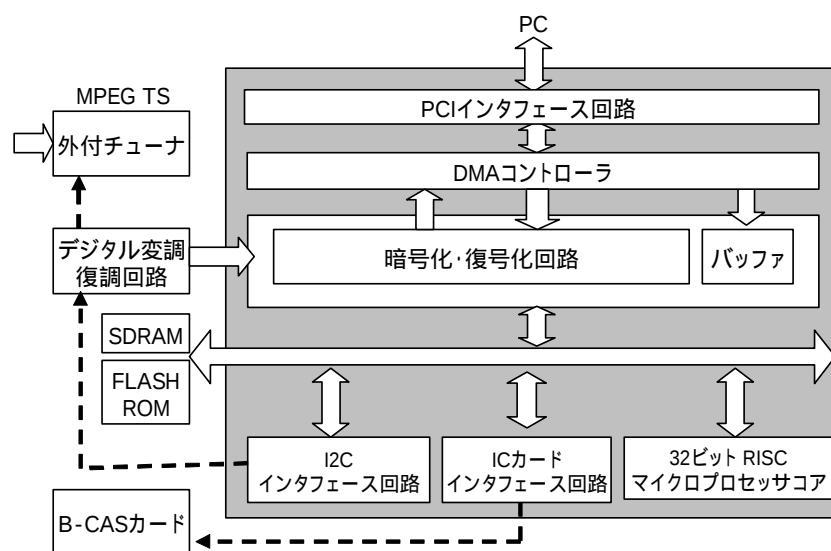


図-3 権利保護LSIのブロック図

Fig.3-Digital Content Rights Protection LSI block diagram.

HDDから読み出される。HDD，PCIバス上のコンテンツはすべてローカル暗号化可能であり，電波産業会デジタル放送運用規定を満足する。

HDDを使用し，各種アプリケーションが実現できるよう設計されている。例えば，タイムシフトは，放送コンテンツをHDDに予約録画しておき，都合の良い時間に蓄積コンテンツを読み出し，再生表示する機能である。夜8時のニュースを夜中の12時に帰宅したサラリーマンが視聴するのに便利な機能である。また追っかけ再生は，放送コンテンツの視聴を一時中断し，何分か経過して用事を済ませたあとで続きから見られるようにする機能である。この場合，HDD蓄積とHDD読出しを同時に行う必要がある。権利保護LSIでは，これらの機能が実現できるようにコンテンツをHDDにリアルタイム蓄積しつつ，コンテンツ読出しができるように設計した。また，コンテンツの早送り，巻戻しなどトリックプレーサポート機能も内蔵した。PC上のHDDを流用することでPCユーザは，タイムシフトやトリックプレーなど各種アプリケーションを容易に利用できるようになる。PCでデジタル放送を視聴した場合の大きなメリットとなる。

I2Cインターフェースは，外付チューナやデジタル変調信号復調回路の制御に利用できる。デジタル放送受信に必要なインターフェース類は，本LSIに一式存在する。

32ビットマイクロプロセッサコアは，I2C制御，

表-1 権利保護LSI基本仕様

テクノロジー	0.18 μ m CMOS A15層
パッケージ	FBGA-288ピン
電源	VDDI (LSI内部電源) 1.65 V - 1.95 V VDDE (I/O電源) 3.00 V - 3.60 V
マイクロプロセッサ	32ビットRISC 40 MHz動作周波数

ICカード制御，暗号化・復号化回路制御のほかにPC上メモリ領域で動作するソフトウェアの監視を行う。ソフトウェアがハッキングされた場合，ソフトウェアを無効化する。

図-3のSDRAM，FLASH ROM領域は，マイクロプロセッサコアのプログラムメモリ領域，データ領域として利用している。

権利保護LSI基本仕様を表-1に示す。

実 証 確 認

これまで述べてきたようなコンテンツ保護機能が実際のPC環境で正常動作するか，また権利保護LSIの機能に過不足がないかなどを実証確認するため，権利保護LSI搭載実験PCIカード（図-4）を開発し，実際のPC環境で動作させた。

実験PCIカードには，実際の地上デジタル放送が受信できるよう，また権利保護LSIの各機能が動作確認できるように外付地上デジタル放送用チューナ，地上デジタル変調信号復調回路，権利保護LSI，B-CASカードなどを搭載した。さらに，PC上にアプリケーションソフトウェアとしてMPEGデコー

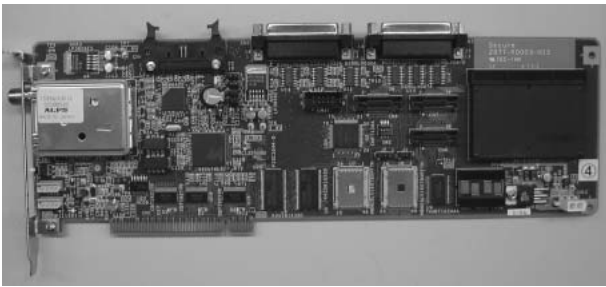


図-4 実験PCIカード
Fig.4-Experimental PCI card.



図-5 権利保護LSI
Fig.5-Digital Content Rights Protection LSI.

ダを搭載し、権利保護LSIで保護できるようにした。

本カードを使用し、上記のような環境で実際の地上デジタル放送を受信し、MPEG-MP@HLストリームをリアルタイム毎秒30フレームでデコードできることを確認した。

権利保護LSIの外観を図-5に示す。

む す び

本稿では、地上デジタル放送などのデジタルコンテンツの権利保護を実現する技術および権利保護LSIを紹介した。今後は、この成果を有効に生かし、電波産業会のデジタル放送運用規定に準拠したデジタル放送受信機能付きPCへの搭載を目指す。同時に更なるセキュリティ機能の拡充（例えば、コンテンツ課金機能、コンテンツ移動機能など）を進める。

本技術はデジタル放送以外のデジタルコンテンツの権利保護にも原理的には適用可能と考える。有望なターゲットとして、例えばIP放送などインターネット上のデジタルコンテンツの保護などがある。また、LinuxなどのOSの一部保護なども考えられる。

本研究開発は、独立行政法人「情報通信研究機構」の委託研究により実施したものである。この場を借りて関係各位に感謝の意を表する。

参 考 文 献

- (1) ARIB STD-B14 . 社団法人電波産業会 .
- (2) ARIB STD-B25 . 社団法人電波産業会 .
- (3) C. Collberg et al . : A taxonomy of obfuscating transformations . Technical Report 148 , Dept. of Computer Science , University of Auckland , 1997 .