平成１３年度　研究開発成果報告書

「ＰＣなどオープンアーキテクチャーデジタル放送受信機
に対応する権利保護システムの研究開発」

目　　次

１・研究開発課題の背景

１９９９年末のＢＳデジタル放送開始を皮切りに２００２年には１１０°ＣＳデジタル放送、２００３年には地上デジタルが開始されます。デジタル放送開始とともにもう一方で、受信機にハードディスクを搭載し、受信デジタルＡＶコンテンツをハードディスクに蓄積し、コンテンツ課金やタイムシフトなど行う新サービスが普及するものと思われます。受信機でのハードディスク等の蓄積媒体の存在を前提としたサーバー型放送の規格化も今年秋目処に進められています。この際、デジタルＡＶコンテンツの複写や移動などを制限する権利保護システムの研究開発が急務になります。

本研究開発は、ＰＣでのデジタル放送受信を前提にＰＣソフト上で権利保護を実現する技術に関するものです。現状のＰＣソフト上での権利保護は、基本的に保護アルゴリズムを秘匿化することで権利保護しています。そのためソフトの解析を困難にする「難読化」などが中心です。しかし、これではアルゴリズムが解析されると権利保護が困難になり、レベルが低く、強化が必要です。本研究開発は、ＰＣなど（１）ソフト処理主体かつ（２）オープンアーキテクチャー構成デジタル受信機の権利保護に関するものです。

２・研究開発分野の現状

デジタルコンテンツの流通に関しては、これまでにも各社､各団体により提案がいくつもされてきております。例えば，ＤＶＤにおける著作権保護システムであるＣＳＳ方式や、リムーバブルメディア向けＣＰＲＭ方式、ＩＥＥＥ１３９４を用いた方式など存在します。

- CSS 方式(DVD における著作権保護システム)　詳細は非公開
- CPRM(Content Protection for Removable Media)方式　詳細は非公開

これらの方式においては、ハードウェアの耐タンパー性やソフトウェアの耐タンパー性が重要とされております。ハードウェアの耐タンパー技術はある程度確立されてきた技術であり、コンテンツ提供者サイドにもある程度理解されているものと考えております。この為、専用装置の世界においては耐タンパー性を利用したコンテンツ保護システムの構築は可能となってきております。

しかし、ＰＣのようなオープンソフトウェアが動作するような世界では、全てをハードウェアで処理することへの抵抗があり、全てをハードウェアで処理するアーキテクチャが受け入れられ難い状況であります。この為、ソフトウェアの耐タンパー性が強くもとめられております。

ソフトウェアの耐タンパー性はハードウェアよりも困難であり、ソフトウェアの解析から完全に守ことは難しいとされております。現在、各社で実施されているソフトウェア耐タンパーの技術には大きく分けると以下の２つの技術が用いられております。

（難読化）

ソフトウェアに余分なコードを付加したり、簡単な計算処理をわざと複雑な計算ルーチンを用いて計算させることで、逆アセンブルによるコード解析に時間がかかるようにすることで耐タンパー性を持たせようとする方式である。

（暗号化手段を利用）

ソフトウェアを暗号化してハードディスク上に格納しておく方式。また、ソフトウェアを細かいモデュールに分割して実行させ、モデュール間の相互認証などをさせる方式も存在する。内容は一般的には公開されておらず（方式を未公開にしないと安全性を保てないため）内容は不明ですが、公開されている技術論文としては、

- 「逆解析や改変からソフトを守る」(日経エレクトロニクス 1998.1.5(no706)) 耐タンパなソフトウェア構造の提案論文

が存在します。ただし、暗号化技術を用いには、対象となるソフトウェアの攻撃だけでは解析することはできませんが、ソフトウェアを復号してあげるソフトウェアが存在するわけで、これを含めて攻撃をされるとソフトウェアの解析から守ることは困難となります。

今回の研究は、上記のようなソフトオンリーのセキュリティーでは現在の技術水準では、十分な安全性の確保（方式が分かると安全性を保てない）は困難と考え、最低限のハード（ＴＲＭ化したセキュアハード）をベースにソフトの安全性を確保する手段を研究開発するものです。

セキュアハードのコストを低くするため回路規模を小さくするよう検討すると同時に、セキュアハードの普及が容易なようにＰＣＩバス等、一般公開されたバスに接続することを前提に研究開発を進めます。

なお当社では、数年に渡って超流通やデジタルコンテンツ保護の研究開発を進めてきたという実績があります。

- 鳥居直哉，長谷部高行，武仲正彦，木島裕二：``超流通システムの試作", 電子情報通信学会技術研究報告，Vol.96, No.71(OFS96-10), pp.1--5 (1996)
- 長谷部高行，鳥居直哉，武仲正彦：``超流通システムの試作（課金サーバ型）", 電子情報通信学会　基礎・境界ソサイエティ大会講演論文集，SA-5-6，pp.283--284 (1996)
- 木島裕二，長谷部高行，鳥居直哉：``超流通におけるコンテンツ流通のための課金機構の開発", 創造的ソフトウェア育成事業及びエレクトロニック・コマース推進事業 最終成果 発表会論文集 創造的ソフトウェア育成事業編，pp.701--704 (1998)
- 長谷部高行，木島裕二，鳥居直哉：``超流通における課金機構の開発", 情報処理学会研究報告, Vol.98, No.85 (98-EIP-2),pp.15--19 (1998)
- 田平孝彦、瀬野尾晴海、小川清隆、小檜山清之、秋山良太, ``MPEG-TS（デジタルビデオ／オーディオ）セキュリティー方式の開発"、テレビジョン学会年次大会、No. 23-3（1996）

これらの研究がベースとなり、既に実際に製品運用されている以下の権利保護関連システムがあります。それは、ＤＤＩポケット社が提供する Sound Market と呼ばれるサービスです。そのサービスで採用されている、ケータイ de ミュージック方式と呼ぶ方式は当社等により開発された方式です。URL は、以下。

http://www.keitaide-music.org/index_j.html

これは、音声の権利保護が目的でＰＣのようなソフト主体のオープンアーキテクチャーシステムではありませんが、権利保護やコンテンツ課金に必要な以下の全ての機能が揃っています。

- ライセンスとコンテンツの分離技術
- ライセンス管理技術（メディアベースランセンス管理）
- 暗号化実装技術（ハードウェア、ソフトウェア）
- 相手認証や再送防止等といったプロトコル技術
- ハードウェア耐タンパー技術、など

今回の研究開発における課題としては、さまざまなソフトウェアが動作するようなオープンプラットフォーム上で、できるだけハードウェア依存部分を減らした形のソフトウェアベースのコンテンツ保護がいかなる形式ならば可能なのかを研究し､その実装技術を開発すること。また、実際のデジタル放送にこれらの技術を適用した場合にオープンプラットフォームで動作が可能かを実証することである。

３・研究開発の全体計画

３・１研究開発課題の概要

１９９９年末のＢＳデジタル放送開始を皮切りに２００２年は１１０°ＣＳデジタル放送、２００３年には地上デジタルが開始される。デジタル放送開始と共にもう一方で、受信機にハードディスクを搭載し、受信デジタルＡＶコンテンツをハードディスクに蓄積しコンテンツ課金やタイムシフトなど行う新サービスが普及する。受信機でのハードディスクの蓄積媒体の存在を前提としたサーバー型放送規格化も本年夏目処に進められる。この際デジタルＡＶコンテンツ複写や移動を制限する権利保護システム研究開発が急務になる。

本研究は、ＰＣでのデジタル放送受信を前提にＰＣソフト上で権利保護を実現する技術に関するものである。現状ＰＣソフト上での権利保護は、基本的に保護アルゴリズムを秘匿化することで権利保護している。そのためソフトの解析を困難にする「難読化」などが中心である。しかし、これではアルゴリズムが解析されると権利保護が困難になる。レベルが低く強化が必要である。本研究は、ＰＣなど（１）ソフト処理主体かつ（２）オープンアーキテクチャー構成デジタル受信機の権利保護の研究開発に関するものである。

過去の例でいうとＰＣで音楽をインターネット配信するナプスターは、コンテンツ複写や移動を制限する機能がないため著作権者からクレームが付き一旦サービスを停止された。ＰＣなど内部が公開されたソフト処理主体機器での権利保護機構実現の困難さを示した例と言える。これはソフトウエアベースでは、本来的に情報の複写／移動、その他制御が可能であることが前提でこれを制限することはシステム全体の構想に合わないためである。

今後デジタル放送が一般化し、ＰＣ上でデジタルＴＶ機能が実現されるようになると音楽のみならずデジタルＡＶコンテンツもＰＣ上に存在するようになり、ますますＰＣ上のコンテンツ権利保護が大事になる。デジタルＡＶコンテンツの著作権者は、強固な権利保護機能を持たない限り、ＰＣ上でのデジタルＡＶコンテンツを容認しないものと思われる。

一方でＰＣ上でのデジタルＡＶコンテンツ権利保護が一旦実現するとＰＣからブロードバ

ンドインターネット経由で世界中にデジタルＡＶコンテンツが流通する可能性が開ける。

図１は一般的な既存ＢＳデジタル放送受信機能搭載ＰＣの機能ブロック図であり、デジタルＡＶコンテンツをハードディスク蓄積したと想定している。信号の流れを概説すると以下のようになる。放送波は「デジタルチューナモデュール」より入力され、デジタルＡＶコンテンツを時分割多重の形で持つＭＰＥＧ－ＴＳデジタルストリームが出力される。ＭＰＥＧ－ＴＳデジタルストリーム中の視聴者が選択した番組（特定デジタルＡＶコンテンツ）はＭＵＬＴＩ２暗号化されており、「ＭＵＬＴＩ２暗号復号モデュール」で復号される。復号されたデジタルＡＶストリームはハードディスク蓄積のため再暗号化され、再暗号化デジタルＡＶコンテンツがハードディスク等の蓄積媒体にＰＣＩバス等を経由し蓄積される。ＭＵＬＴＩ２暗号復号に必要な暗号鍵等のライセンス情報は「Ｂ－ＣＡＳカード等ライセンス保持モデュール」から出力される。また、再暗号化に必要なライセンス情報は、「ライセンス生成モデュール」で生成される。

ＨＤＤ蓄積された暗号化デジタルＡＶコンテンツを再生する場合は、「暗号復号モデュール」に転送され復号され、復号デジタルＡＶ情報は、「ＭＰＥＧ等デコードモデュール」で伸長処理される。伸長デジタルＡＶ情報は、「グラフィックモデュール」でグラフィックがオーバレイされ、その後アナログ出力の場合はアナログ著作権保護情報が付加され出力される。デジタル出力の場合は、デジタル著作権保護情報が付加され出力される。

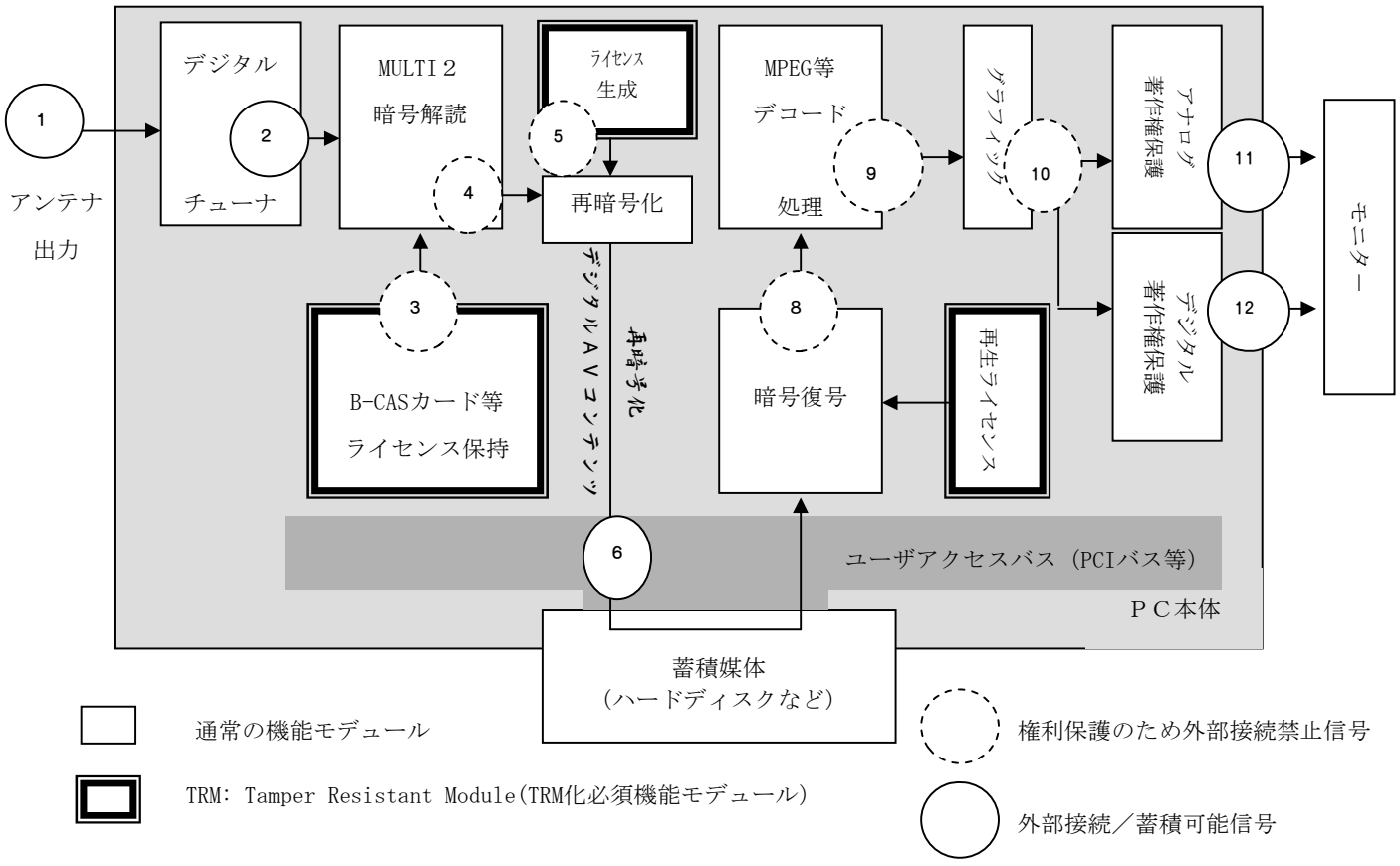


図１．ＰＣ等ユーザアクセスバスを有するデジタル放送受信機の機能ブロック図

図１で暗号解読鍵等のライセンス情報を持つ機能モデュールは TRM（Tamper Resistant Module）である必要がある。また、その他のモデュールは通常のモデュールであるが図１で点線の信号（信号４、５、８、９、１０など）は、権利保護上、外部流出禁止信号である。例えば、暗号復号後の信号８などが外に漏れると著作権者の権利を保護することが出来なくなる。

また、図１は機能モデュールであり、各モデュールともソフトで実現してもハードで実現しても機能的には動作する。

図２は、ＬＳＩ（ハード主体）で図１の機能を実現した場合のブロック図である。太線内がＬＳＩ。殆どの機能がＬＳＩ内に搭載され、ＬＳＩ全体をＴＲＭ（Tamper Resistant）化することで外への信号流出が防げ、比較的容易に権利保護が実現する。しかし、ハードを搭載することはＰＣのコストアップに繋がる。特にＭＰＥＧデコード機能は回路規模が大きく高価格である。

またＰＣはソフト主体の装置であるが、この構成ではソフト／プロセッサーが有効利用されていると言い難い。さらに、既にＤＶＤ プレイヤー（ＭＰＥＧ　ＭＰ@ＭＬ圧縮デジタル情報のデコードが必要）が一般のＰＣ上でソフト処理されていることを考えるとプロセッサーの処理能力が今後増大した場合、デジタル放送（ＭＰＥＧ　ＭＰ@ＨＬ圧縮デジタル情報のデコードが必要。ＭＰ@ＨＬはＭＰ@ＭＬの６倍の処理能力を要求。）でも一般ＰＣでソフト処理可能になるのは時間の問題である。

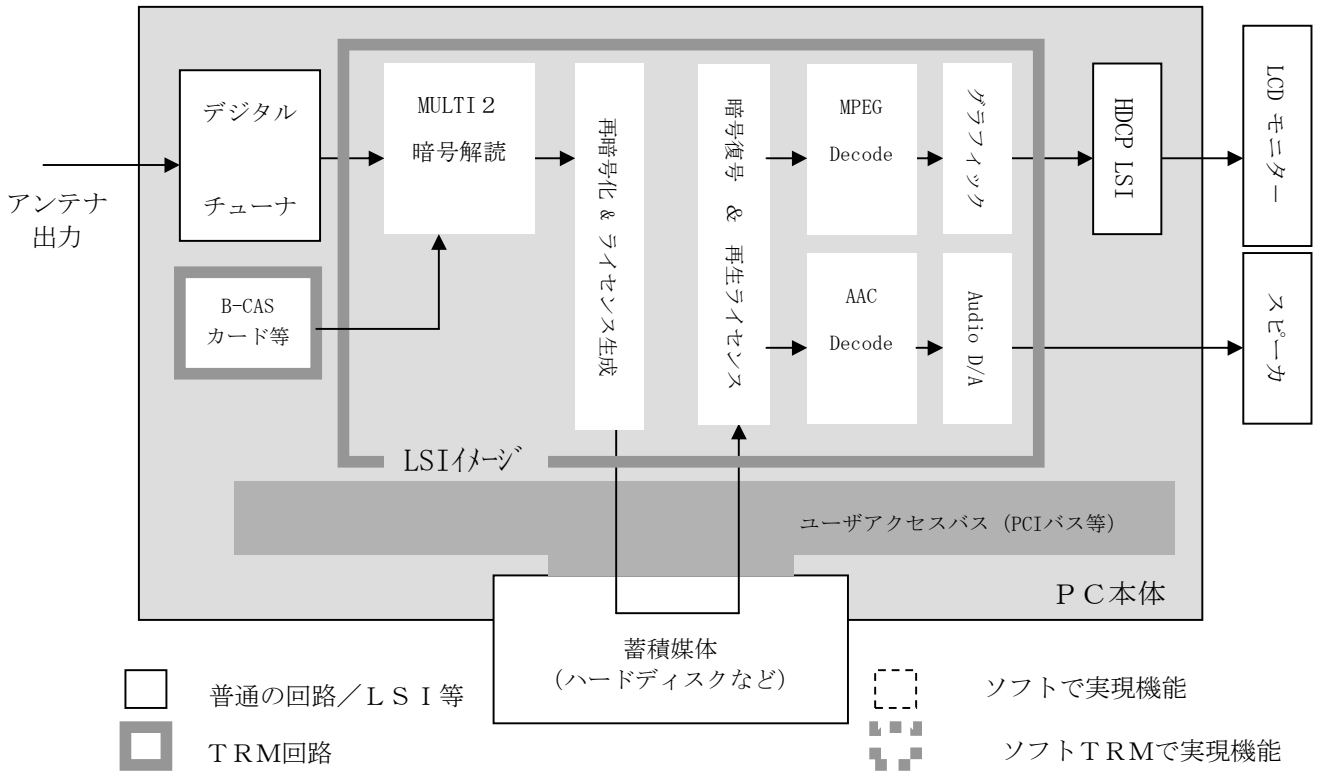


図２．想定されるハード処理主体の実施例

図３は、ソフト処理を主体とした場合の実施例である。ハード処理した場合、回路規模が大きくコストアップにつながる「ＭＰＥＧデコード」、「ＡＡＣ音声デコード」や「暗号復号」などがソフト処理されている。従って、これが実現した場合ハードで実現したときと比較してかなりのコストダウンが図られると考えられる。

ソフト処理した場合の課題は、「暗号復号」に必要な暗号解読鍵の保護や「ＭＰＥＧデコード」など、各ソフト処理モデュールからの出力信号の保護である。

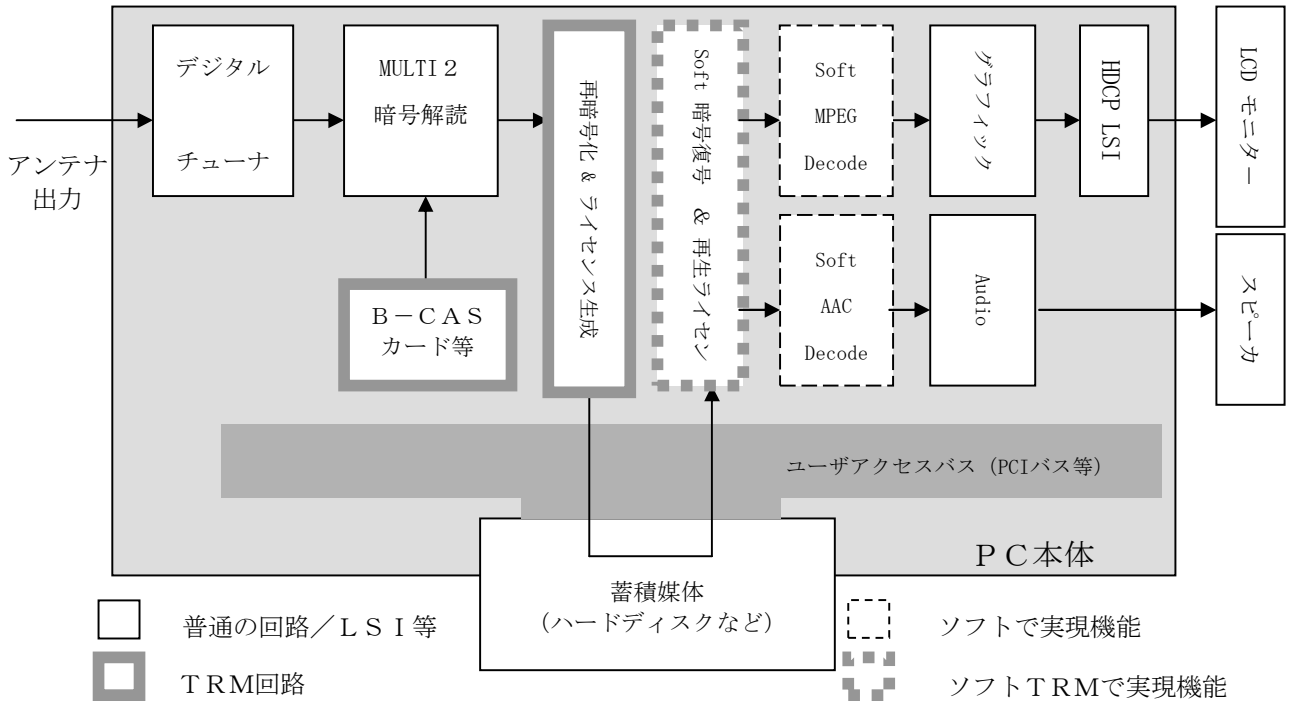


図３．想定されるソフト処理主体の実施例

以上の検討でPCのようなソフト主体装置の場合、ハードウェア処理を持ち込むことはソフト主体装置の持つ本来の可能性が大幅に制約されることが分かる。

従い、本研究方針は上記検討で「ＰＣなどソフト処理主体の装置の可能性を損なわないデジタルＡＶコンテンツの権利保護システム」に絞った方がより本質的であることも分かる。しかし、一方で全くソフトのみの処理では、強固なデジタルＡＶの権利保護は困難と思われる。オールソフト処理とした場合、最終的に暗号鍵等の機密保持が非常に困難と考えられるためである。

現状の技術水準を考慮した場合、処理の大半をソフト処理するが最低限の信号処

理はハードウェア化（セキュアハード）したデジタル放送対応の権利保護システムの研究開発が現実的であると考える。

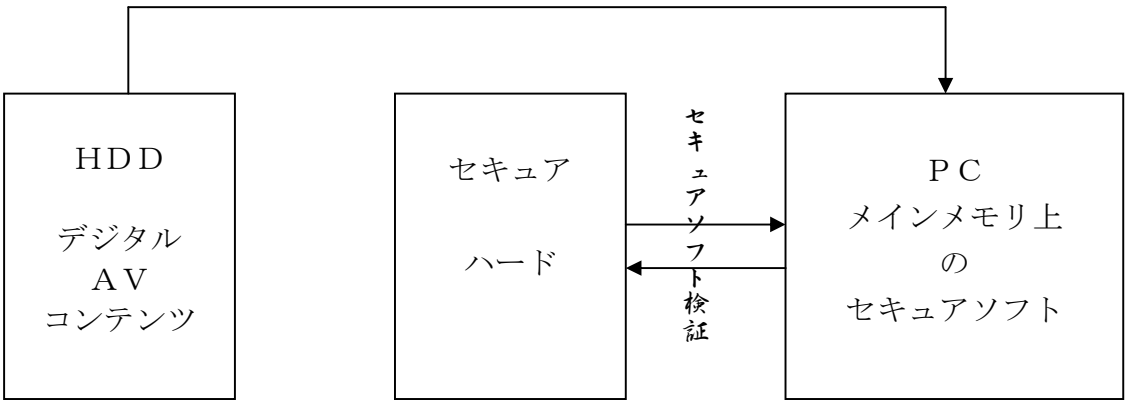


図４．想定されるセキュアソフトとハード

今後の研究開発に大きく依存するが、現時点で想定されるブロック図が図４。これをベースに現時点で見える課題は、以下のようなものである。

ハードディスク内のデジタルＡＶコンテンツは、ＰＣのメインメモリ上のセキュアなソフトで処理される。一方でセキュソフトの安全性を保障するのはセキュアハードになる。最終的な信頼点としてのセキュアハードをどう活用するか、これが権利保護アルゴリズムという視点からの大きな研究開発課題になる。

またこの権利保護システム全体にリアルタイム性が要求される。処理するコンテンツは、基本的にハイビジョン動画像（ＭＰＥＧ　ＭＰ＠ＨＬレベル）であり、ＰＣ性能をギリギリまで使用しないと画像のリアルタイム処理は困難と考えられる。この中にセキュア処理をＰＣから見てあまり負担のかからない範囲でどう盛り込むか課題になる。安全性とＰＣ性能のトレードオフをどう考えるか、ハードディスク／セキュアハード／セキュアソフト間の機能分担をどう捕らえるか、リアルタイム性というセキュリティーと別の視点から検討が必要である。

さらに別の視点としてコストがある。２００４年以降店頭販売の一般ＰＣで活用されることを前提とした場合、コストを押さえるため、権利保護システム内の特殊部品はセキュアハードのみとして検討する必要がある。また、普及が容易なようにセキュアハードはＰＣカード搭載を前提とし、ＰＣ接続するときのインターフェースはＰＣＩバスなどユーザーに公開された汎用なものとする必要がある。

研究手法として、まずセキュアハード／ソフトの概略構成を初年度に検討し、大まかに権利保護システムの構想を固めるべきである。この時、図４の（１）ハードディスク／（２）セキュアハード／（３）PC 上のセキュアソフトの機能分担や想定されるセキュリティーホールを、特定し対策を検討する。

３・２　研究開発目標

３・２・１　最終目標（平成１６年３月末）

ＰＣ上、ソフト処理主体でデジタルＴＶの権利保護を実現する基盤技術を完成させることを最終目標とする。

具体的にはセキュアソフト実現のための（１）セキュアハード コアＬＳＩ、（２）セキュアハードを利用したセキュアＭＰＥＧビデオ処理ソフト／セキュアオーディオ処理ソフトなど、（３）「権利保護ＰＣカード」などを完成させる計画とする。「権利保護ＰＣカード」の中にセキュア コアＬＳＩ以外に地上デジタル放送受信機能も搭載を計画する。また、旧ＰＣから新ＰＣに買い替えた時に必要な蓄積コンテンツのセキュアな視聴権移動機能などＰＣ上でデジタルＴＶ受信機を構成するための基本機能を揃えるものとする。セキュリティー強度は、基準となる物差しがないので言及困難であるが、基本的にオールソフト処理より強い、放送など公共性の高い網で適用可能なレベルを目指す。またリアルタイム処理性能は、２００４年のＰＣ上でＭＰＥＧ　ＭＰ＠ＨＬレベルの画像を権利保護しつつ一般の視聴者が違和感なく動画像を視聴出来るレベルとする。

３・２・２　中間目標（平成１５年３月末）

基本の機能レベルの完成目標を平成１５年３月とする。セキュアハードの回路、セキュアソフトを機能レベルで完成させ、実際にＰＣ上でデジタルテレビ画像を見られるようにすることを計画する。

但し、ＦＰＧＡ搭載実験ボードで製作されたハードウェアは物理的なサイズが大きく、ＰＣカード等に実装出来るレベルでない。またＦＰＧＡは高価であり、サイズ的にもコスト的にも製品展開は不可能なレベルに留まる。製品展開が期待出来るレベルにするためには、ＦＰＧＡ搭載実験ボードのＬＳＩ化が不可欠あり、またリアルタイム性もこの段階では十分なレベルに到達していないと想定する。リアルタイム性の目標として毎秒５フレーム（最終目標は一般視聴者が違和感なく動画像を視聴出来るレベル）の処理性能を想定する。

３・３　研究開発の年度別計画　　（金額は非公表）

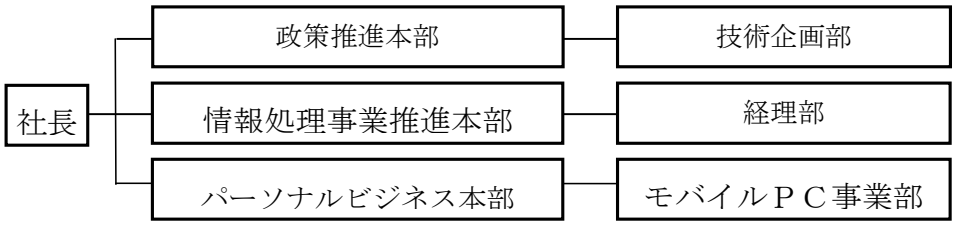
研究開発項目	１３年度	１４年度	１５年度	計	備　考
アーキ検討、実験ボード開発 設計、試作（ＦＰＧＡ）、ソフトウェア開発 改良、ＬＳＩ化、ＰＣカード開発	→	→	→		
間接経費					
合　　計					

注）１　経費は研究開発項目毎に消費税を含めた額で計上。また間接経費は直接経費の３０％で計上（消費税含む。）。
　　２　備考欄に再委託先機関名を記載。

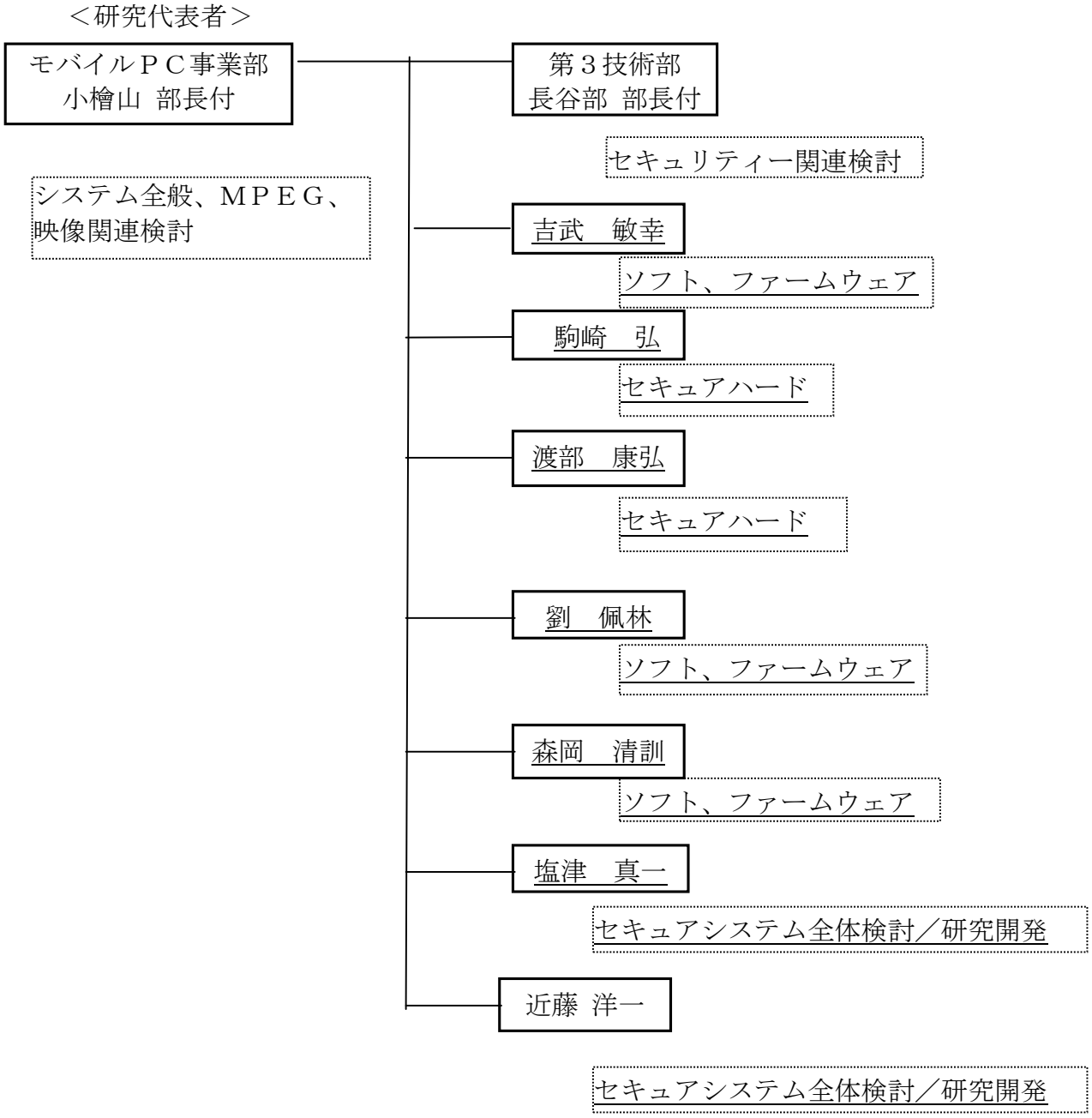
３．４　研究開発体制

３．４．１　研究開発管理体制

（注　受託者の経理部門の体制、経理責任者（所属、氏名、電話、ＦＡＸ、Ｅ－メールの連絡先）を含む。）



３・４・２　研究開発実施体制



４．　研究開発の概要

４・１　研究開発実施計画

４・１・１　研究開発の計画内容

初年度の１３年度は、ＰＣ型のセキュアデジタル放送受信機のセキュアハード／ソフトの概略構成を検討し、大まかに権利保護システムの基本アーキを固める。そしてこの大まかな構想に従い、ＦＰＧＡ（Field Programmable Gate Array）構成でセキュアハード実験ボードを製作する。実験ボードは、１４年度以降のセキュアデジタル放送受信機の性能や機能評価などを行うための実験プラットフォームという位置付けで製作し、１４年度以降の実験などで改良点や問題が発覚した場合、その時点でハードウエア設計を容易に変更出来るようにＦＰＧＡ（Field Programmable Gate Array）構成とする。

なお、実験ボードは、各種改良を経たのち、本研究開発の最終年度にはＬＳＩ化しＰＣカード搭載を目標とし、本研究開発が目標とする権利保護システムの「核」

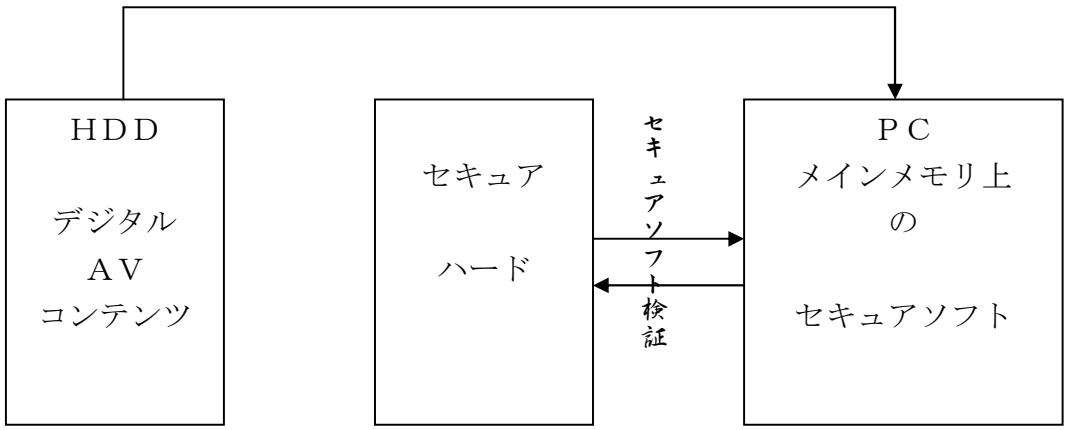


図４．想定されるセキュアソフトとハード

になる部分である。以上が大まかな研究開発目標である。以下詳細を紹介する。

今後の研究開発にも依存するが、想定されるPC型ソフト処理主体のセキュアデジタル放送受信機は、セキュリティーという側面から見ると以下のブロック図（図４）の構成となる。この図に従い、平成１３年度はセキュアデジタル放送受信機の基本アーキの決定など今後の方向付けを行う。

図４でデジタル放送受信機は、（１）ＨＤＤ、（２）セキュアハード、（３）ＰＣメインメモリ上のセキュアソフトという基本要素から構成される。ＨＤＤ内に放送されたデジタルＡＶコンテンツが蓄積されており、ＰＣメインメモリ上のセキュアソフトでデコードされ、視聴される。一方でセキュアソフトの安全性（デコード

後のデジタルＡＶコンテンツの著作権など権利保護機能）をセキュアハードが保証する。以上の基本構成を前提に初年度研究課題として以下を検討する。

１）最終的な信頼点としてのセキュアハードの活用法の検討。

２）リアルタイム性とセキュリティーのトレードオフの検討。システム全体にリアルタイム性が要求される。処理コンテンツ（デジタルＡＶコンテンツ）は、基本的にハイビジョン動画像（ＭＰＥＧ　ＭＰ＠ＨＬレベル）であり、ＰＣ性能をギリギリまで使用しないとリアルタイムソフト処理は困難と考えられる。この中にセキュア処理をＰＣから見てあまり負担のかからない範囲でどう盛り込むか。セキュリティー（安全性）とＰＣ性能のトレードオフをどう考えるか、ハードディスク／セキュアハード／セキュアソフト間の機能分担をどう捕らえるか、リアルタイム性というセキュリティーと別の視点から検討要。

３）さらに別の視点としてのコストがある。本技術を２００４年以降店頭販売の一般ＰＣで活用されることを前提とした場合、コスト削減のためシステム内の特殊部品はセキュアハードのみとすることが望ましい。またセキュアハード普及を容易にするためセキュアハードはＰＣカード搭載とし、ＰＣ接続時のインターフェースはＰＣＩバスなどユーザーに公開された汎用なものが望ましい。

以上のようなことを前提とし、セキュアハード／ソフトの概略構成を初年度に検討し、大まかなシステム構想を固める。この時、図４の（１）ハードディスク／（２）セキュアハード／（３）PC 上のセキュアソフトの機能分担や想定されるセキュリティーホールを特定し、対策を検討する。特に安全性保証のため、セキュアハードとセキュアソフト間で安全性検証のための特別な通信が必要と考えられる。この辺の仕組みを検討し、次年度以降実証実験するための基礎を固めることを本年度の基本目標とする。

また本構想に従い、初年度具体成果としてＦＰＧＡ（Field Programmable Gate Array）構成でセキュアハード実験ボードを製作する。この実験ボードの最終目標はこれをＬＳＩ化し、図４のセキュアハードとすることにある。実験ボードにより次年度以降、上記で検討したセキュアハードとセキュアソフト間で安全性検証のための特別な通信などを具体化し、検証実験を行う。実験ボードの基本部分をＦＰＧＡ構成とすることでセキュア化の研究が進み問題が発覚した時点でのセキュアハードの設計変更を容易にする。従い、このボードはセキュリティーシステム試作／実証のための基本プラットフォームとなるよう構成する。

初年度はセキュアシステム構想を固めることが主眼であり、セキュアハード実験ボードの中のＦＰＧＡの具体設計は、次年度以降とするがセキュアハードにはＦＰＧＡ以外にプロセッサー、プロセッサー周辺回路、メモリ、ＰＣＩインタフェース回路などの搭載が予想され、プロセッサー周辺、ＰＣＩインタフェース回路の動作確認などは初年度に行うものとする。

４・１・２　研究開発課題実施計画

（金額は非公表）

研究開発項目	第１四半期	第２四半期	第３四半期	第４四半期	計	備　考
アーキ検討、実験ボード開発				→		
間接経費						
合　　計						

注）１　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の３０％で計上（消費税を含む。）。（合計の計は、「３－１の研究開発課題必要概算経費」の総額と一致）

２　備考欄に再委託先機関名を記載。

４・２　研究開発の実施内容

初年度の１３年度は、ＰＣ型のセキュアデジタル放送受信機のセキュアハード／ソフトの概略構成を検討し、大まかに権利保護システムの基本アーキを固める。またこの大まかな構想に従い、ＦＰＧＡ（Field Programmable Gate Array）構成でセキュアハード実験ボードの基本部分を製作する。実験ボードを１４年度以降のセキュアデジタル放送受信機の性能や機能評価などを行うための実験プラットフォームという位置付けで製作し、１４年度以降の実験などで改良点や問題が発覚した場合、その時点でハードウエアの設計を容易に変更出来るようにＦＰＧＡ（Field Programmable Gate Array）構成とする。

なお、実験ボードは、各種改良を経たのち、本研究開発の最終年度にはＬＳＩ化しＰＣカード搭載を目標とし、本研究開発が目標とする権利保護システムの「核」になる部分とする。以上が１３年度の大まかな研究開発目標である。以下詳細。

PC 型のソフト処理主体のセキュアデジタル放送受信機は、セキュリティーという側面から見るとブロック図（図５）のような構成が考えられる。本図に従い、平成１３年度はセキュアデジタル放送受信機基本アーキ決定など今後の方向付けを行う。

図４でデジタル放送受信機は、（１）ハードディスク、（２）セキュアハード、（３）ＰＣメインメモリ上のセキュアソフトという基本要素から構成される。ハードディスク内に放送されたデジタルＡＶコンテンツが蓄積されており、これがＰＣメインメモリ上のセキュアソフトでデコードされ、視聴される。一方でセキュアソフトの安全性（デコード後のデジタルＡＶコンテンツの著作権など権利保護機能）をセキュアハードが保証する。以上の基本構成を前提に初年度研究課題として以下を検討する。

１）最終的な信頼点としてのセキュアハードの活用法の検討。

２）リアルタイム性とセキュリティーのトレードオフの検討。システム全体にリアルタイム性が要求される。処理コンテンツ（デジタルＡＶコンテンツ）は、基本的にハイビジョン動画像（ＭＰＥＧ　ＭＰ@ＨＬレベル）であり、ＰＣ性能をギリギリまで使用しないとリアルタイムソフト処理は困難と考えられる。この中にセキ

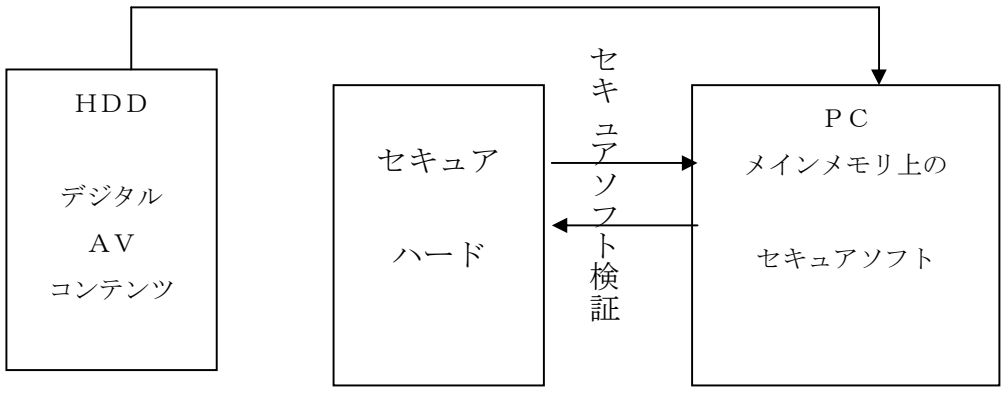


図５．想定されるセキュアソフトとハード

ュア処理をＰＣから見てあまり負担のかからない範囲でどう盛り込むか。セキュリティー（安全性）とＰＣ性能のトレードオフをどう考えるか、ハードディスク／セキュアハード／セキュアソフト間の機能分担をどう捕らえるか、リアルタイム性というセキュリティーと別の視点から検討する。

３）さらに別の視点としてのコストがある。本技術を２００４年以降店頭販売の一般ＰＣで活用されることを前提とした場合、コスト削減のためシステム内の特殊部品はセキュアハードのみとすることが望ましい。またセキュアハード普及を容易にするためセキュアハードはＰＣカード搭載とし、ＰＣ接続時のインターフェースはＰＣＩバスなどユーザーに公開された汎用なものが望ましい。

以上のようなことを前提とし、セキュアハード／ソフトの概略構成を初年度に検討し、大まかなシステム構想を固める。

また本構想に従い、初年度はＦＰＧＡ（Field Programmable Gate Array）構成でセキュアハード実験ボードを製作する。この実験ボードの最終目標はこれをＬＳＩ化し、図５のセキュアハードとすることにある。実験ボードにより次年度以降、上記で検討したセキュアハードとセキュアソフト間で安全性検証のための特別な通信などを具体化し、検証実験を行う。実験ボードの基本部分をＦＰＧＡ構成とすることでセキュア化の研究が進み問題が発覚した時点でのセキュアハードの設計変更を容易にする。従い、このボードはセキュリティーシステム試作／実証のための基本プラットフォームとなるよう構成する。

なお、初年度はセキュアシステム構想を固めることが主眼であり、セキュアハード実験ボードの中のＦＰＧＡの具体設計は、次年度以降とするがセキュアハードにはＦＰＧＡ以外にプロセッサー、プロセッサー周辺回路、メモリ、ＰＣＩインタフェース回路などの搭載が予想され、プロセッサー周辺、ＰＣＩインタフェース回路の動作確認などは初年度に行うものとする。

５・　研究開発実施状況

５―１　研究開発実績

平成１３年度検討の結果、図５の構成を以下のように具体化する基本構想（図６）をまとめた。また本構想に従い、１４年度以降のセキュアデジタル放送受信機の性能や機能評価などを行うための実験プラットフォームという位置付けで、ＦＰＧＡ（Field Programmable Gate Array）構成でセキュアハード実験ボード基本部を製作した。１４年度に図 5 の構成でＦＰＧＡ内部を具体設計、具体試作するための準備が整った。１３年度で検討した基本構成（図６）の詳細を以下に示す。

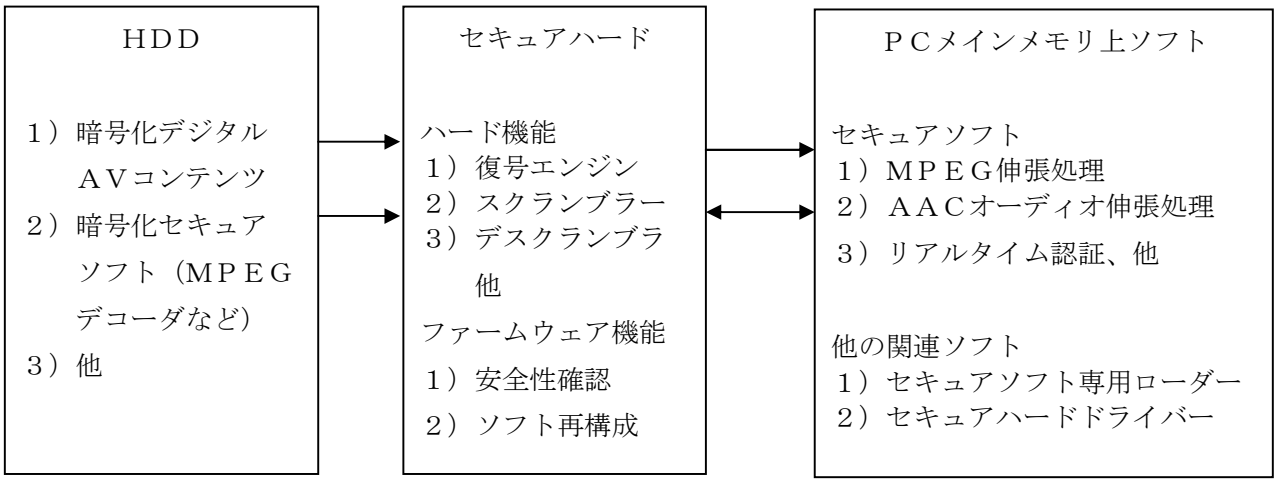


図６．１３年度検討で想定されるセキュアソフトとハードの関係

ＰＣメインメモリ上セキュアソフト（この場合は、デジタル放送対応ＭＰＥＧビデオデコーダなど）をセキュアハード（外部から覗き見や改ざんが出来ないＴamper Ｒesistant Module）がリアルタイム安全確認するシステムを検討した。安全確認し、セキュアソフトが改ざんされた場合にセキュアソフトの動作を停止する必要があるため、セキュアハード内にセキュアソフトの動作を停止させる機構が必要である。また、デジタル放送受信ＰＣ全体の構成を検討し、１４年度以降研究開発するセキュアハード（ＦＰＧＡ内）の概略構成を検討した。

検討中のセキュアソフト及びセキュアハードがセキュアシステムを実現するための基本構想は以下の通りである。ＰＣメインメモリ上ソフトは、基本的に他ソフトから「覗き見」など可能であり、「覗き見」により解析され「成り済まし」攻撃にあう可能性もある。「成り済まし」攻撃とは、もとのプログラムの一部を書き換え(改ざん)、ハッカーが欲しい情報をＨＤＤなどに書き出すようにすることなどである。例えば、デジタルＡＶ処理ソフトの場合に一番困るのは処理中のデジタルＭＰＥＧ情報をＨＤＤなどに書き込むように改ざんされた「成り済まし」プログラムである。圧縮ＭＰＥＧ情報は、情報量が少なく、容易にＨＤＤに書込める。ハッカーに開発されデジタルＡＶ情報が自由に盗難される可能性がある。

これを困難にするためセキュアハードは、セキュアソフトを監視する。監視する具体手法は、検討中であるが、例えばセキュアハードとセキュアソフトが何らかの通信を行い、通信内容が正しければ、セキュアソフトが改ざんされていないなどの手段が考えられる。但し、セキュアソフトを解析されると通信内容自体も解析され、「成り済まし」にあう可能性がある。これを困難にするため、セキュアハードによるセキュアソフトの「再構成」（セキュアソフトのコードをセキュアハードがある一定期間ごとに変更する）を検討中である。

セキュアソフトがある期間ごとに「再構成」されれば、ハッカーがある瞬間のセキュアソフトを解析し、「成り済まし」プログラムを開発しても、そのときには「再構成」された別のセキュアソフトが動作していて、「成り済まし」プログラムを無効に出来る。特にセキュアハードがセキュアソフトの安全性（改ざんされていない）を確認する通信内容を「再構成」することが肝要と考えられる。ソフトのコードを自動的に書き換える研究として、例えば以下が存在する。

http://web.yl.is.s.u-tokyo.ac.jp/~cocoa/reading/reading1.html

A Tentative Approach to Constructing Tamper-Resistant Software.

Masahiro Mambo, Takanori Murayama and Eiji Okamoto

以上を踏まえ、現在セキュアシステムの動作として以下を考えており、この考えをベースにＦＰＧＡ（Field Programmable Gate Array）構成でセキュアハード実験ボードを開発中である（図６参照）。平成１３年度は、実験ボード基本部分（プロセッサー、PCI バス等）を完成させた。以下、想定される全体動作を説明する。

図６の HDD 内に暗号化されたデジタル AV 情報、暗号化されたセキュアソフトなどが存在する。暗号化デジタル AV 情報は、基本的にデジタル放送されたものを想定しているが、そうでなくインターネットなど経由し入手したコンテンツでも原理的には同じである。なお、暗号化デジタル AV 情報はローカル暗号（放送された暗号化デジタル AV 情報を一度復号し、セキュアハードで再スクランブルする）を想定しており、従いデスクランブル鍵は、セキュアハード内に存在する。デジタル AV をセキュアソフトが処理（MPEG ビデオデコード等）する際は、セキュアハードが一旦、暗号化デジタル AV 情報を HDD から読み込み、復号し、さらにスクランブルした上でセキュアソフトに供給する。スクランブルを解くためのデスクランブルキーは、やはりセキュアハードがセキュアソフトに供給し、もしセキュアソフトが改ざんされている場合は、セキュアハードがデジタル AV 情報、デスクランブルキーなどのセキュアソフトへの供給を停止する。以上が、デジタル AV 情報の信号処理の大まかな流れである。

この流れを実現するため、セキュアハードに放送デジタル AV 情報復号のための MULTI2 復号回路、再暗号化のためのスクランブル回路、デスクランブル回路等が必要と考えられる。図 7 が１３年度に検討したセキュアハードのブロック図である。

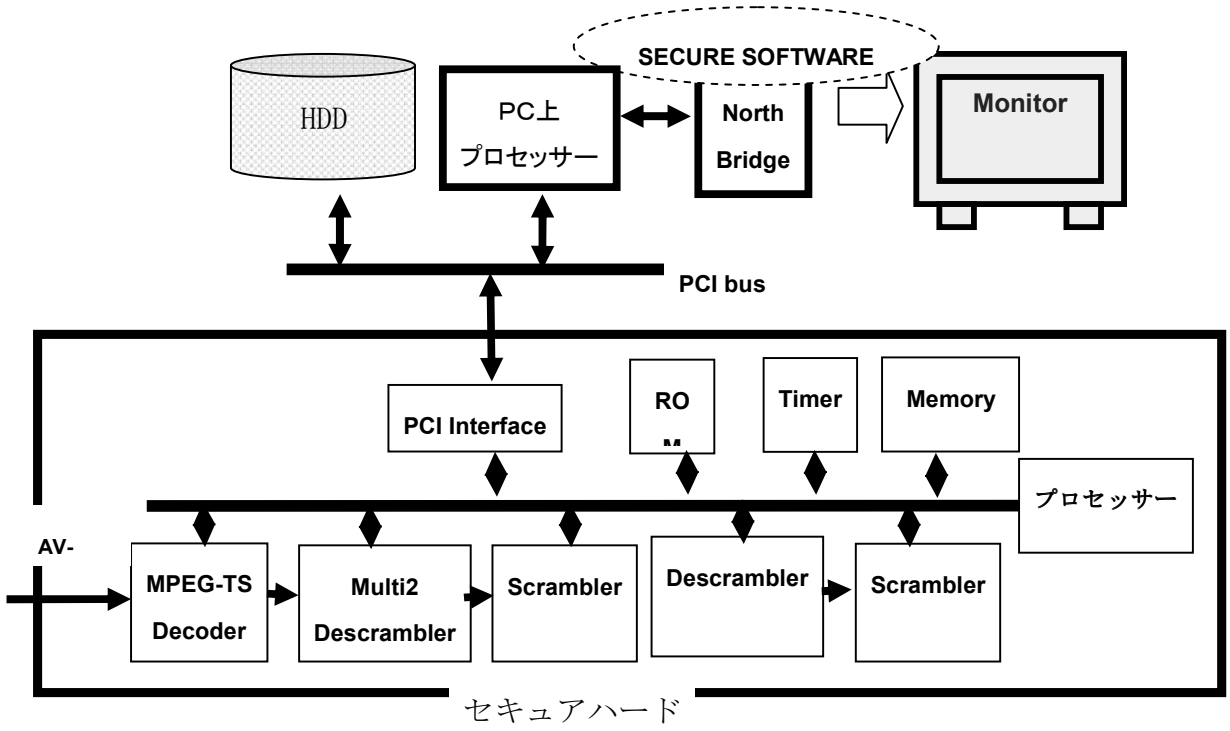


図７．検討したセキュアハードブロック図（概念図）

地上デジタル放送受信を前提に検討した。放送されたデジタルＡＶ情報は、ＭＰＥＧ－ＴＳ形式でデジタル多重され、セキュアハードに入力される。ＭＰＥＧ－ＴＳに多重された圧縮ＭＰＥＧビデオ情報、圧縮ＡＡＣオーディオ情報、他は、セキュアハード内の簡易ＭＰＥＧ－ＴＳデコーダで必要な情報だけが抽出され、ＭＵＬＴＩ２デスクランブラーで暗号復号される。暗号復号されたＭＰＥＧビデオ情報などは、スクランブラーで再スクランブル（ローカル暗号等が想定される）された後、ＰＣＩインタフェースを介しＨＤＤに蓄積される。再スクランブル時の具体的な方式はまだ検討段階だが、スクランブルのためのスクランブル鍵などは、例えば数秒間など短い間隔で更新出来るような回路を検討する。一度、ＨＤＤ蓄積されたスクランブルのかかったデジタルＡＶ情報は、再生のために再び読み出される。再生時の動作は、以下の通りである。ＨＤＤ内のデジタルＡＶ情報は、ＰＣＩバスを経由し、セキュアハード内のデスクランブラーに供給される。ここでデスクランブル後、さらにもう一度スクランブルしてからＰＣ上のメインメモリに供給する。この再々スクランブルされたデジタルＡＶ情報をセキュアソフトがデスクランブル処理し、伸張処理（ＭＰＥＧビデオの場合はＭＰＥＧビデオ伸張処理）し、最終的にモニターなどに表示する。

ＰＣＩバスを流れるデジタルＡＶ情報は全てスクランブルがかかっているので安全である。また、本構成によれば、デジタルＡＶ情報のＨＤＤ蓄積、ＨＤＤからの読み出し、セキュアソフトへの書き込みを同時に行えば、タイムシフト再生などの応用アプリケーションも可能である。図８、９は、デジタルＡＶ情報の流れを示す。

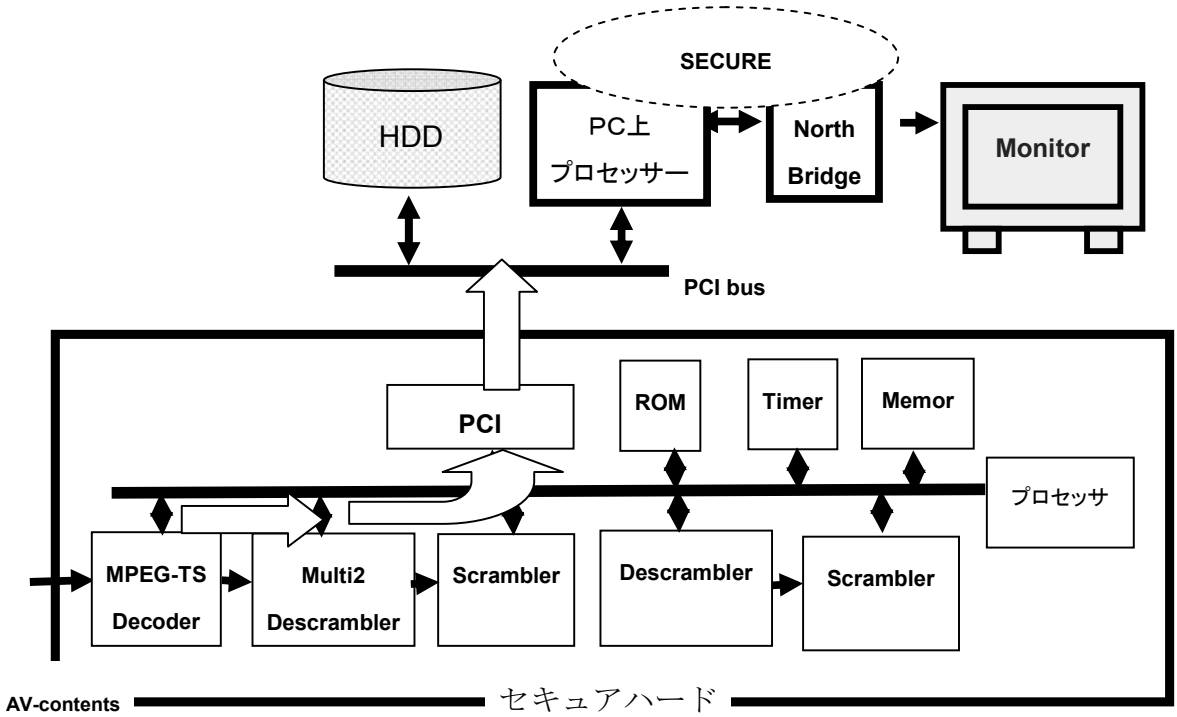


図８．検討したデジタルAV情報ＨＤＤ蓄積時の流れ（概念図）

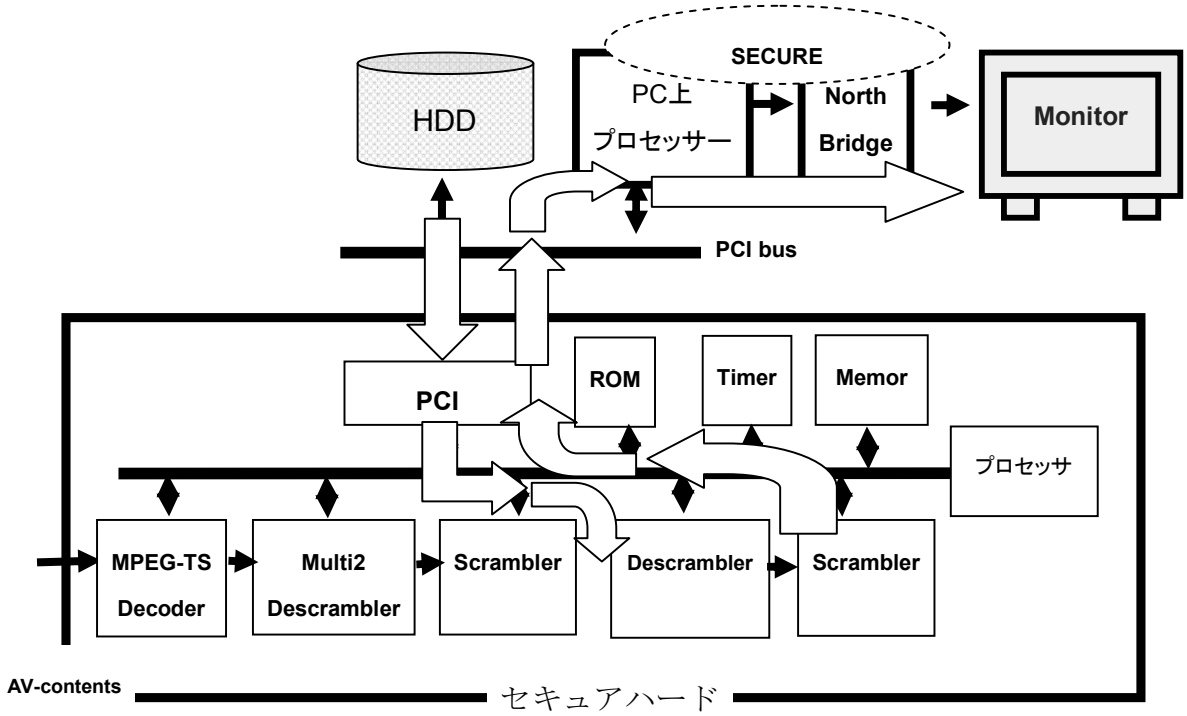


図９．検討したＨＤＤ再生時のデジタルAV情報の流れ（概念図）

図１０は、セキュアソフトの流れである。当初セキュアソフトは、HDD 内にスクランブルされた状態で蓄積されている。これを図示のようにセキュアハードが読み出し、デスクランブルし PC 上のメインメモリ領域にロードする。ロードする際に、セキュアハードでセキュアソフトの「再構成」を行う。これは、セキュアソフトのコードをセキュアハードがある一定期間ごとに変更することを目論んでおり、この「再構成」によりセキュアソフトの解析を困難にする。「再構成」されたコードの中には例えば「秘密の番号」の通信によるセキュアソフトの認証などが含まれており、この認証方法を再構成の都度、変更するなどして認証手順解析によるハッカーの解析攻撃なども困難にする。

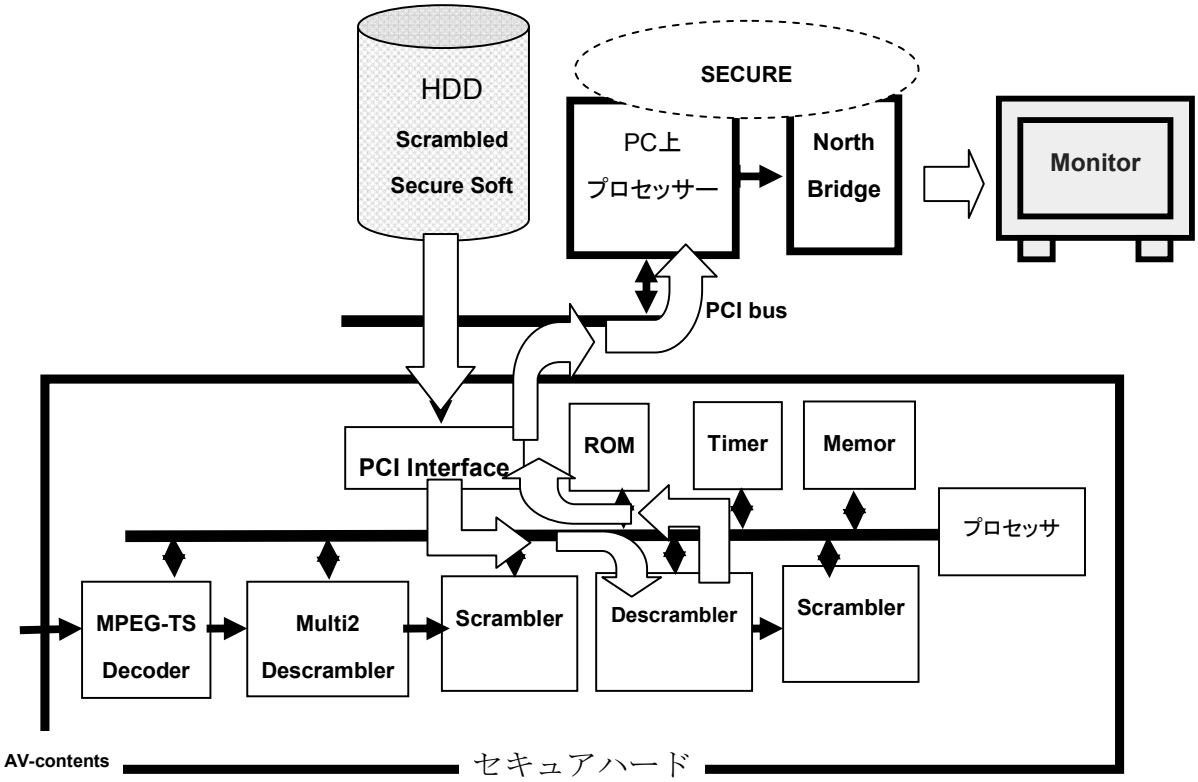


図10. 検討したセキュアソフトの流れ（概念図）

図１１は、セキュアハードによるセキュアソフトの認証の概念図である。セキュアソフトとセキュアハードの間で何らかの通信を行うことでセキュアソフトをリアルタイム認証する。動作中のソフトをリアルタイムで認証出来ることが本セキュアシステムの大きな魅力になると考えられる。

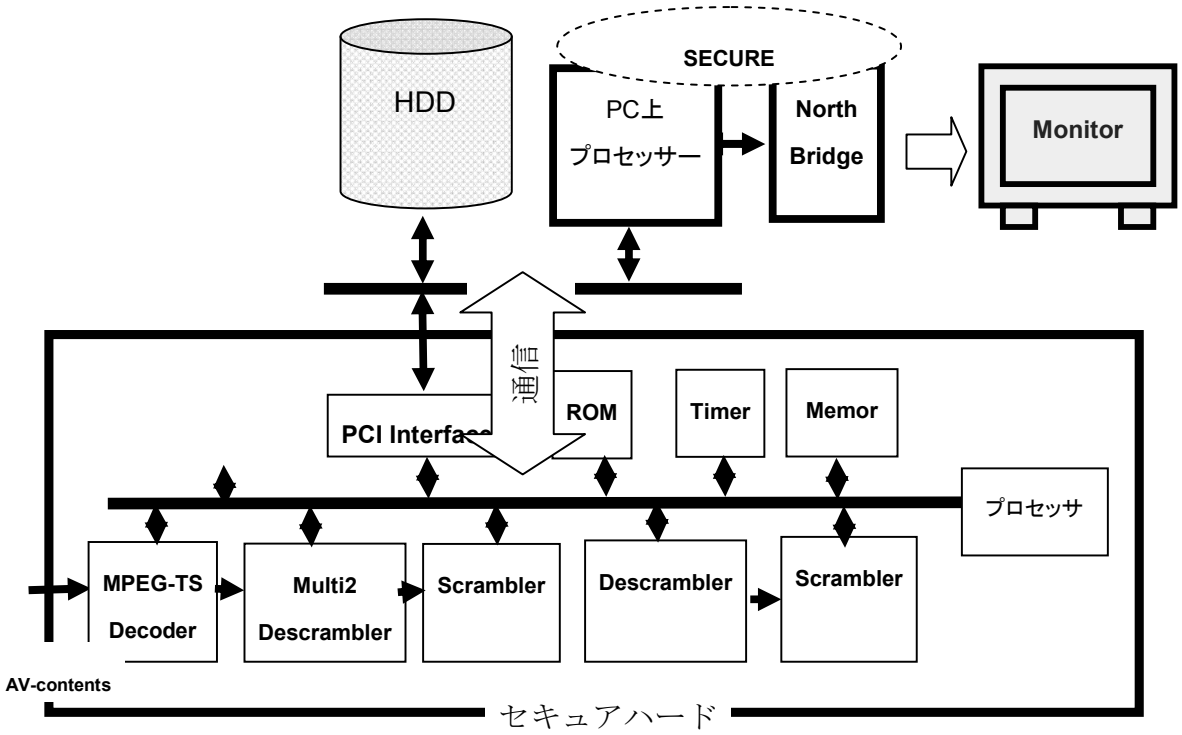


図11. セキュアソフト認証のための通信（概念図）

図１２は、ソフトという観点から全体の基本構造を見た概念図である。ビデオ情報主体に書いてあるがオーディオ情報も基本的には同じ構造になると想定される。PC 上のメインメモリにセキュアソフトが存在する。セキュアソフトの中に（１）MPEG デスクランブラー、（２）MPEG 伸張処理、（３）レンダリングがあり、レンダリングされた MPEG 情報は、AGP バス等を通りグラフィックメモリに一時蓄積された後、モニターに出力される。一般に AGP バスのデータを覗き見することは AGP バスが非常に高速なこともあり困難とされ、また画像がモニター出力される時点では、画像に対し HDCP 権利保護などが施されると考えられる。また、PCI バスを通るときの圧縮 MPEG ストリームはスクランブルされる。セキュアハードの中はハードウエア TRM（Tamper Resistant Module）技術により保護出来る。従い、セキュアソフトの権利保護を本構成で実現すれば、PC システム全体としてかなり強固なセキュリティーシステムが実現すると考えられる。

またメインメモリ上にはセキュアハード内のセキュアソフトをロードするためのローダーやセキュアハード用ドライバーが存在する。

さらにセキュアハードには、（１）「再構成」のためのファームウェア、（２）セキュアソフトが改ざんされていないことを確認し、セキュアソフトにスクランブ

ル MPEG 情報を供給するファームウェア、（3）セキュアハード内の MULTI2 暗号回路、スクランブル回路、デスクランブル回路の制御ファームウェアなどが存在する。

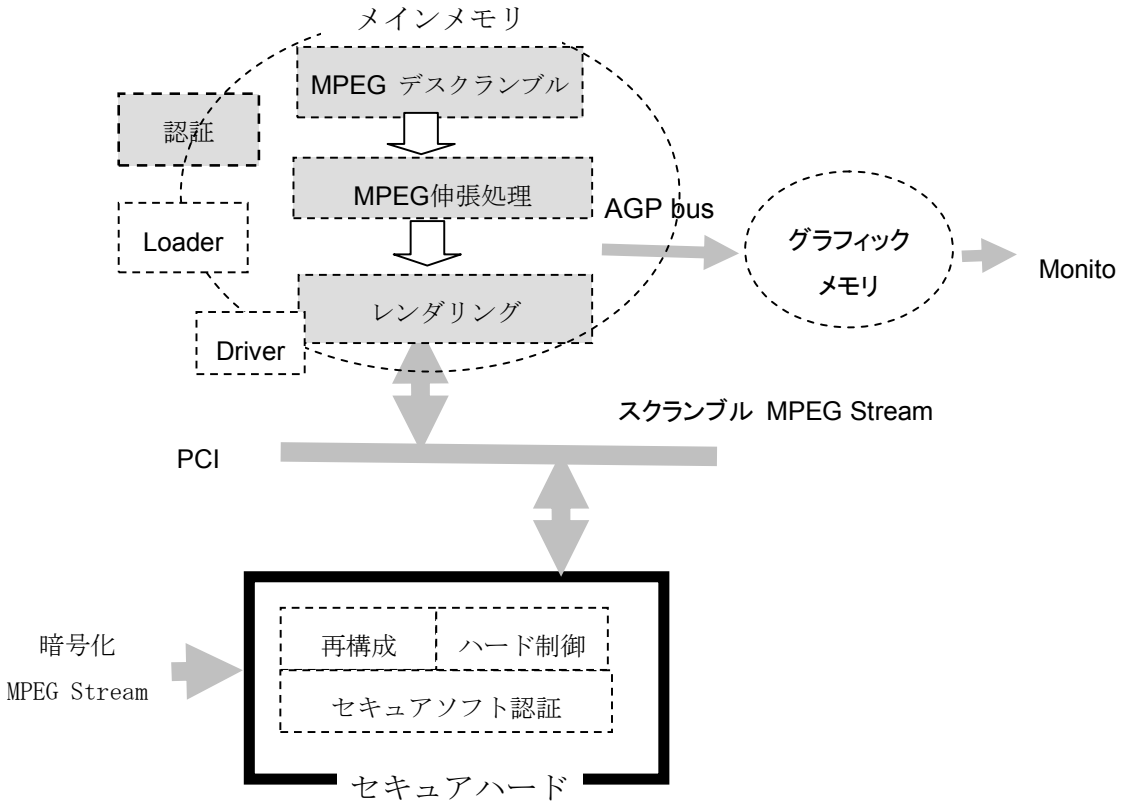


図12. ソフトから見た概念図

5―2　まとめ

ＰＣソフト上での地上デジタル放送受信機の実現を目標にＭＰＥＧソフトデコーダを主体にＰＣ上のソフトをセキュアにする方法について検討した。従来の「難読化」を主体としたセキュア化の技術は、ソフト解析に対し決定的に弱い。例えば暗号復号ソフトの場合、いくらセキュアにしても、暗号復号鍵が覗き見可能なメインメモリ領域の何処かに存在しており、暗号復号ソフトを覗き見により複製し、じっくり解析された場合に暗号復号鍵の位置は看破されてしまうし、これを防ぐ方法が見当たらない。そこにソフトオンリーのセキュア化の限界がある。

本検討では上記状況を鑑み、最低限のハード（セキュアハード）を導入し、これを有効利用しソフトをセキュアにする方法を検討した。しかも、民生市場（地上デジタル放送受信機）での利用を前提に、出来る限りコストアップを避けるため、（1）プロセッサーが必要とする処理性能がソフトのセキュア化により多大に増大

しないこと、（２）セキュアハードの回路規模が最小限になるようにすることなどの附帯条件をクリアすることが必要であった。これら要件を満たす基本アーキの検討が出来たと考える。

すなわち、本セキュリティー機構を用いた場合にプロセッサーが新たに必要とする処理性能（ＭＰＥＧソフトデコーダなどをセキュア化するために新たに必要な処理性能）はセキュアソフトを認証するためのものだけであり、認証を実施する頻度、内容にも依存するが、ここで要求される処理性能が多大なものになるとは、現時点では考えにくい。

また、セキュアハードの回路規模に関しても、図７のように基本的にＭＵＬＴＩ２暗号復号、スクランブラー、デスクランブラー、ＰＣＩインタフェース、プロセッサー等と予想されるが、これらの回路規模は全体を合わせても、最近の半導体技術の進歩を考えれば、それほど大きくはないと判断出来る。

さらに、セキュアハードとセキュアソフトを結ぶバスとしては、汎用性があり、どのＰＣでも付属する安価なＰＣＩバスを利用できる。本セキュアシステムに起因しＰＣＩバス通る情報は、大まかに言って、デジタルＡＶ蓄積時のＭＰＥＧストリーム（図８），デジタルＡＶ情報再生時のＭＰＥＧストリーム（図９）、及びリアルタイム認証時の通信情報（図１１）であるが、全部合計してもＰＣＩバスの伝送能力に負担がかかるレベルにならないと判断出来る。従い、この点からもＰＣ全体に対し本セキュリティー機構導入が大きなコストアップ要因になるとは考えられない。