

マルチメディアコンテンツに対する 記憶装置主導型逐次的アクセス制御アーキテクチャ

平井達哉^{†1,*1} 田中克己^{†1}

近年、商用の動画や音楽コンテンツのデジタル化が進んだ。それと並行して、磁気や半導体等の媒体への微視的な記録再生技術も飛躍的に進歩をとげ、これを応用した多様な大容量の記憶媒体や装置、またそれらを利用するためのデジタル機器が製品化された。一方でこれらの機器の発展は、商用コンテンツの不正な利用を容易にしたため、コンテンツ制作者らは、それを防止する技術の確立および機器の開発を強く求めるようになった。なかでも、コンテンツの不正な複製と、CMを含むことによって一般利用者に無料で提供されているコンテンツのCM飛ばし視聴が問題視されている。前者については、特に光ディスク媒体への適用を主目的に、ホスト装置がすべての処理を行う不正利用防止技術がいくつか実用化された。しかし、ホスト装置上にソフトウェアだけで本機能を実装した場合、攻撃に対する堅牢性の確保が難しいという問題が顕在化した。このような問題に対する1つの解として、不正利用防止に関連した処理の一部を記憶装置が担うことにより、ホスト装置上の不正利用防止機能をソフトウェアだけで実装する場合でも堅牢性をより高く保つことができる技術を、筆者は過去に提案した。本論文ではこれをさらに拡張し、記憶装置が処理の一部を担うという特徴を維持しつつ、後者の問題を解決する技術を提案する。具体的な提案項目は、当該アクセス制御の実現のために必要な新規の情報、ホスト装置と記憶装置間でのその交換手続き、また既存のファイルシステム構造との親和性を考慮したうえでの前記情報の記録、管理の方法である。

Storage Device Initiative Sequential Access Control Architecture for Multimedia Content

TATSUYA HIRAI^{†1,*1} and KATSUMI TANAKA^{†1}

Digitalization of commercial content like movie and music has recently advanced. Along the advancement, wide variety of digital appliances and high capacity storage media/devices have been commoditized because writing and reading technology for magnetic or semiconductor media has also innovatively

improved. On the other hand, it caused the problem to make the unauthorized usage of the content easier. Therefore, content owners are getting to require establishing the technologies to prevent such usage. Piracy and CM-skipped viewing are understood as the significant ones. For the piracy, some technologies aimed to mainly being applied to optical discs, have been put to practical use. In those technologies, the host device executes almost all the tasks. However, if those functions are implemented as software in the host device, it becomes obvious that they may have vulnerability for the attack. One of the authors has previously proposed the storage-device-initiative type technology with high robustness to prevent unauthorized usage if the functions on the host device are implemented as a software. In this paper, we propose a new technology with high robustness by basing the previous one. It enforces for the users to view the content without skipping CMs. The concretely proposed items are newly introduced information to realize the access control, message exchange protocol between the host and the storage device, and the managing method of the information taking the affinity to the conventional file system format into account.

1. はじめに

近年、磁気や半導体等の媒体への微視的な記録再生技術は、飛躍的な進歩をとげた。この技術は、DVD¹⁾、Blu-ray Disc²⁾等の光ディスク媒体、SDカード³⁾等の半導体記憶装置、また磁気ディスク装置といった、多様な大容量の媒体や記憶装置に実際に応用され、実製品化された。なかでも磁気ディスク装置は、個体単価は光ディスク媒体と比べて高いものの、ビット単価的にはこれらに比してほとんど差がなく、他方で高いデータ転送能力やランダムアクセス性を有することから、多くの機器において主要な記憶媒体として利用されるようになった。

このような記憶媒体や装置の大容量化と並行して進んだブロードバンドプラットフォームの整備やインターネットサービスの普及は、動画や音楽といった、蓄積に大容量の記憶媒体を必要とするマルチメディアコンテンツのデジタル化とその拡散を、急速に推し進めた。その結果、コンテンツ権利者が不利益を被ったと強く感じるような、一般利用者やサービス業者による無秩序なコンテンツの複製やその広範囲への配布が行われるようになり、利

^{†1} 京都大学大学院情報学研究科

Department of Social Informatics, Graduate School of Informatics, Kyoto University

*1 現在、日立製作所中央研究所

Presently with Central Research Laboratory, Hitachi, Ltd.

用者やサービス業者とコンテンツの権利者との間で、しばしば軋轢や訴訟が引き起こされた^{4),5)}。このため権利者は、自己の利益を守るための運用規定の容認や、コンテンツの一般人による利用を自身が認めた範囲内に制限する技術の確立および遵守を、機器開発者に対し強く求めるようになった⁶⁾⁻⁸⁾。

このような問題に対し、平井らは、容量が他の媒体に比べて大きく、内部に制御部を持つという磁気ディスク装置の特性を有効に利用し、不正なコンテンツの複製を防止するための処理の一部を磁気ディスク装置に担わせることにより、高い利便性と堅牢性を持つ不正利用防止システムを過去に提案した⁹⁾⁻¹³⁾。

一方で近年になって、従来不正な利用法の代表格であった「コンテンツの不正な複製」に加えて、ビデオテープが主流の記憶媒体であった頃はあまり問題視されてこなかった「CM部を飛ばして本編のみを視聴する」といったテレビ放送コンテンツの視聴形態を、コンテンツ権利者らは次第に強く問題視するようになってきた。その背景には、記録媒体として磁気ディスク装置を用いるようになったことにより、従来のビデオテープを利用した再生機と比べて、録画した番組に対するランダムなアクセスや高速な特殊再生が格段に容易に実行できるようになったこと、そのような機能を有する録画再生機が比較的安価で入手できるようになったこと等があげられる。

このようなコンテンツの視聴形態は、利用者にとっての有用性は高いといえる。しかしそのゆきすぎは、コンテンツ権利者に還元される利益の減少だけでなく、放送サービス業者に提供されるCM料の減少、その帰結としての無料放送サービスの中止という危険性を内包している¹⁴⁾。これは、利用者自身にとっても望ましくない事態である¹⁵⁾⁻¹⁷⁾。

本論文は、現在広く使われている記憶装置に対する親和性の確保や、限定されたリソースでの実行性を考慮しつつ、文献9)-13)に示したアーキテクチャを拡張することで、上記問題を高い精度で解決する堅牢なシステムのアーキテクチャ、およびそこで実行すべき処理手続きを提案するものである。本技術は、以下のような利点を持つ。

- 不正な複製防止に限らず、コンテンツに対する逐次的なアクセス制御規則まで科すことができる。
- 上記規則に従うアクセス制御の一端を記憶装置が担うことにより、高い堅牢性を保つ。
- 現状の記憶装置のインタフェースおよび内部処理特性に対する親和性を持つ。
- 実際に使用されている多くの機器に対する相互接続性の確保が、比較的容易である。

本論文の構成は、以下のとおりである。まず1章において、デジタル機器の発展にともなって近年顕在化してきた、商用コンテンツの利用形態上の問題点、すなわち黎明期に強く

問題視された不正な複製に加え、CM部等コンテンツの一部を飛ばす視聴形態について、その概況を述べる。そして本論文が、実装および実運用上の困難を小さく抑えつつ、上記要求を高い精度で実現する技術の確立を目的とすることを述べる。2章では、現時点までに確立された主要なコンテンツの不正利用防止技術の実例、それらがいずれもホスト装置がすべての処理を行う形態であること、それゆえソフトウェアで本機能を実現した場合、脆弱性の抑制に困難をとまなうこと、記憶装置が不正利用防止のための処理の一端を担うことにより、不正利用を目的とした攻撃に対する堅牢性を高められること等の、筆者らが本論文でとった手法の妥当性を裏付ける事項を述べる。さらに、筆者らが過去に構築した利用制御の一部を記憶装置が担う形態のコンテンツ不正利用防止技術の特徴を説明する。そこでは、当該技術が、記憶装置が利用制御の一端を担うことで攻撃に対して高い堅牢性を有しているが、そのままでは1章に述べたコンテンツの一部を飛ばすような視聴の防止は実現できないことを述べる。3章では、1章で示した課題を解決するうえで必要であり、実サービス上も有用であると考えられる、コンテンツに対する具体的なアクセス制御規則の例を示す。

4章以降には、筆者が新たに提案する技術の詳細を示す。4章では、初めに3章で特徴について簡単に述べた、記憶装置がアクセス制御の一端を担う既存の技術を説明する。続いて、記憶装置が制御の一端を担う特徴を保持しつつ上記技術を拡張し、3章に述べた実用上有用性の高いアクセス制御を実現するための概念的な処理手続きを提案する。5章では、4章で示した概念的な処理手続きにおいて新たに導入した情報のほか、本アクセス制御の実現において別途必要な情報の記録および管理の方法、および実際の記憶装置のインタフェースの仕様に4章で示した概念的な処理手続きを適合させた実装アーキテクチャを提案する。本章の後段では、上記実装アーキテクチャに沿って記憶装置を設計した場合に、その内部で実行される処理内容を明確化し、磁気ディスク装置を例に、現状のリソースでの実行可能性を評価する。6章には、まとめと今後の課題を述べる。

2. 関連技術の概要と特徴、および問題点

本章では、コンテンツの不正利用の防止を目的に、すでに確立された技術とその特徴、およびその問題点について述べる。

2.1 記憶装置の着脱性および多様なホスト装置でのコンテンツの相互可用性確保の重要性

実製品化の際には欠くことのできない、高い利便性の提供や開発費の抑制といった点を無視してでも、一般利用者によるコンテンツの利用を「権利者が認める範囲内へ制限すること」を目指すのであれば、記憶媒体あるいは装置とコンテンツの再生/表示機能部を物理的

に一体化し、当該装置にはコンテンツをデジタルデータとして出力するためのインタフェースを設けないようにすることが、手段としては最も有効である。しかしこのような手段を講じることは、記録元とは異なる媒体へのコンテンツの複製や移動を権利者が許可したか否かとは無関係に、「記録元記憶装置からの他媒体への記録を目的としたコンテンツデータの出力」サービスのいっさいが、利用者には提供されないことを意味する。また製品開発時には、仕様や目的に応じた特殊な記憶媒体や装置の開発を必要とするため、一般に製品単価の高騰を招く。さらには、記憶媒体や装置のインタフェースが独自仕様となることにより、開発物の他の機器へ適用が困難となり、量産効果による低価格化を実現しにくいという欠点もある。

汎用的な記憶媒体や装置を用いた場合でも、記録されたコンテンツのホスト装置への出力可否を、記憶媒体・装置側が判断および制御できれば、上記概念は達成される。しかし、CDやDVD等の制御部を持たない光ディスク媒体はもちろん、制御部を内部に持つSDカードや磁気ディスク装置でさえ、記録されているコンテンツの構造を把握するような機能を現状有していない。

そこで、現在広く販売されているデジタルテレビ放送録画再生装置や携帯型音楽再生機等は、ホスト装置だけが把握している鍵およびアルゴリズムを用いてコンテンツを暗号化することにより、コンテンツを論理的にホスト装置へ固定化する代わりに、標準化されたインタフェース¹⁸⁾を有するために物理的には着脱可能ではあるが、ビット単価が低く、高いデータ転送性やランダムアクセス性を有する汎用的な磁気ディスク装置を記憶媒体として用いるという現実的な折衷案を、ほとんどの機器が採用している。この方法は、物理的な固定化には及ばないが、鍵やアルゴリズムの盗取や改竄の防止が完全に確保されていれば、用いられた暗号アルゴリズムが有する強度で、ホスト装置へコンテンツを固定化できる。

しかし、ホスト装置へのコンテンツの固定化は、以下のような場合において利用者が不便を強いられるという、別の性質の問題をはらんでいる。

- 再生機能に問題を生じた場合でも、磁気ディスク装置も含めた機器全体が補修対象となる。そのため、補修期間中利用者は、自身が記録したコンテンツであっても利用できない。
- 論理的に固定化されたホスト装置以外の機器では、それが仮にまったく同機種であったとしても、磁気ディスク装置に記録されているコンテンツを利用できない。
- より大容量の磁気ディスク装置が市場で入手できるようになっても、利用者が自身で磁気ディスク装置をそのようなものと交換し、新しく導入した磁気ディスク装置にコンテンツを移動したり、統合したりすることができない。

これらの点を考慮すると、多様なホスト装置でのコンテンツの相互可用性は、ホスト装置に対する磁気ディスク装置の物理的な着脱性と同等に、きわめて重要な要素であるといえる。

2.2 PCプラットフォーム上でのコンテンツの不正利用防止機能の実現手段とその問題

1章に記したDVD、SDカードおよびBlu-ray Discといった、物理的な着脱性を持つ記憶媒体・装置に対しては、CPRM¹⁹⁾やAACs²⁰⁾といった、コンテンツの不正な複製を防止する技術が開発され、実際に運用されている。これらの技術は、媒体に記録されるコンテンツを特定のホスト装置へ固定化することなしに不正利用の防止を図るものであり、その意味において2.1節に記した3つの要件のうちの初めの2つを満たす1つの解といえる^{*1}。両者は、おおむね下記のような手段を基礎として、コンテンツの不正利用の防止を実現している。項目2, 3, 4は、ホスト装置において実行される特徴的な処理である。

- 記憶媒体あるいは記憶装置内に、利用者が書き換えることができない物理的特性が異なる領域を設け、本領域に対し製造時に固有情報を記録する。
- コンテンツを暗号化するための鍵の生成後、規定されたアルゴリズムに従い当鍵を用いてコンテンツを暗号化し、媒体上に記録する。
- 上記固有情報のほか、製造時にホスト装置に割り当てられた鍵、および媒体上に記録された書き換え可能な鍵集合等を用いて、上記コンテンツ暗号化用の鍵を暗号化し、媒体上に記録する。
- コンテンツ暗号化鍵を用いて改竄検知用コードを求め、利用規則と合わせて、ホスト装置が利用規則を媒体上に記録する。

正規のホスト装置は、上記処理を逆にたどることによりコンテンツを復号できる。しかし、「鍵を取り出すための」鍵を有しない不正なホスト装置は、論理的には平文状態の鍵およびコンテンツのいずれも得ることができない。

ところで、一般に新機能を搭載した製品の普及を加速するには、安価ですでに広く利用されている機器に対する当該製品の適用性を確保することが、多くの場合有効である。PCは、普及度や多様な機器との相互接続性が確保されているといった点から、そのような機器の中で最も代表的なものであるといえる。

CPRMやAACsに限らず、コンテンツの不正利用防止を目的とした機能部は、不正利用目的の様々な攻撃に対して堅牢であることが求められる。しかしPCのプラットフォーム

*1 現状光記録媒体は、商用コンテンツ用記録媒体としては終端媒体ととらえられている。すなわち、媒体に記録されたコンテンツの他の媒体への複製、移動は許可されていない。

は、新機能の開発を容易にする等の利点を開発者に対して提供する一方で、以下に述べるような点から「攻撃に対して堅牢な構成」の確保が難しいという側面も持つ。

- (1) バイナリ化されているため可読性は低いが、基本ソフトウェアを含むすべてのソフトウェアが記憶媒体にそのまま記録されているため、論理的には一般利用者がコードを直接編集できる。
- (2) オペレーティングシステム等の基本ソフトウェアのインタフェースの多くが、一般に公開されている。
- (3) 各アプリケーションによる主記憶へのアクセスは基本ソフトウェアを介して行われるため、自身以外のアプリケーションによる主記憶へのアクセスを、各々が完全には制御できない。
- (4) 主記憶は、プロセッサとの間で直接データを送受信するため、磁気ディスク装置等の外部記憶媒体よりビット単価は高いが、高速でデータを入出力できる媒体（DRAM等）を用いる必要がある。このため、実際に搭載できる主記憶用媒体の容量は、外部記憶媒体と比べて大きく制限される。

項目(1)に述べた、不特定利用者がバイナリコードの閲覧や編集を行うことができることに起因する問題は、バイナリコードに沿って実際に処理されるデータを暗号化することでは、本質的には解決できない事柄である。すなわち、データが暗号化されて記憶媒体に記録されている場合、そのデータは静的には用いられた暗号アルゴリズムが持つ強度で保護される。しかし、リバースエンジニアリング等を通してバイナリコードが実行する処理を追うことにより、各データの特性が把握され、保護強度が実質的に低下する懸念がある。また、本来利用制御を行うべき処理をスキップさせることを目的としたバイナリコードの改変が行われる危険性もある。

バイナリコードを暗号化して記憶装置に記録しておき、実行時に自身の内部に必要な箇所を復号して演算を行うセキュアグラフィックプロセッサ（以後単にセキュアプロセッサ^{21)–23)}と呼ぶ）の利用は、上記項目(1)で指摘した問題を解決する1つの方法である。セキュアプロセッサが、バイナリコードだけでなく、データも暗号化されたまま処理できるのであれば、プロセッサとの間で直接データが授受される主記憶媒体上に、暗号化された状態で鍵やコンテンツを置いておくことができるようになるため、項目(2)や(3)等の主記憶の特性に起因する脆弱性も、低く抑えることができると考えられる。しかし、セキュアプロセッサ命令の実行は、つねに暗復号処理をとまうため、同程度の処理能力を持つ通常のプロセッサを利用した場合と比べて、実行速度が遅いという問題がある。セキュアプロセッサ利用時

にも、非セキュアプロセッサ利用時と同等のスループットを得るためには、より処理能力が高い、高価なプロセッサを利用する必要がある。それは普及の促進という点において大きな障害となる。

セキュアプロセッサを利用する代わりに、主記憶全体もしくはその一部に、特定のアプリケーション（たとえばコンテンツの再生処理を行うもの）だけがアクセスできるような領域を設け、コンテンツ、鍵、および利用規則等をそこに展開する形にすれば、セキュアプロセッサを利用した場合と類似した堅牢性を得られる可能性がある^{*1}。しかし、主記憶用媒体と外部記憶媒体のビット単価は、一般に100倍以上の開きがあるため、PCに搭載できる主記憶用媒体の容量は現実には大きく制限される。その一方で、可能な限り高い操作性を利用者に提供するには、磁気ディスク装置等の二次記憶媒体が仮想記憶として使用される頻度を低く抑えられるように、システム全体を構成しておく必要がある。このような観点から、アプリケーションが利用できる主記憶容量をあえて制限するような手段は、避けることが望ましい。家電品やPC等価格の抑制が厳しく求められる機器の場合、この点は特に重要である。

一方、上記とは逆の視点として、PC全体の堅牢化を図るアーキテクチャがTrusted Computing Group（以下TCG²⁵⁾）等で検討されている²⁶⁾。それは、証明書が記録された特殊なLSIをプロセッサとは別に基板上に搭載し、物理層から論理層まで順次連鎖的に認証していくことによって、不適切なアプリケーションによるデータの改竄や盗取を防止するものである。しかしPCは、物理層から論理層に至るまでインタフェース仕様を一般に公開することによって、膨大なハードウェアやソフトウェアの資産が世界中で生み出されてきたという側面があるため、その個々について、正当性を保証する具体的な運用体制の確立が難しく、あまり有効に活用されていないのが実状である。

以上に述べてきたような物理的な堅牢化を施さなくても、ソフトウェアの設計を工夫することにより、導入価格を抑えながら堅牢化を図る基盤技術がいくつか提案^{27)–29)}、および実用化³⁰⁾されている。しかし、ソフトウェアの構造を工夫することによるシステムの堅牢化法は、前述したバイナリコードのリバースエンジニアリングや、主記憶へのアプリケーションや基本ソフトのアクセスの仕方に起因する脆弱性を除去するのが難しいという現実がある。記事31)、32)は、ホスト装置用のAACCSの機能をインストールした機器に対して行われた、上記の類の脆弱性を狙った攻撃と、それに対するライセンス団体の対応および声明を述べたものである。

*1 ICカード等に対する組み込み型の記憶媒体には、このような研究例がある²⁴⁾。

91 マルチメディアコンテンツに対する記憶装置主導型逐次的アクセス制御アーキテクチャ

表 1 ホスト装置全制御型と記憶装置部分制御型コンテンツ利用制御の特徴
Table 1 Features of content usage control type by only host device and partially storage device.

項目	ホスト装置全制御型利用制御	記憶装置部分制御型利用制御
物理的手段による堅牢化		
開発費	高い開発費を要する [-].	同左 [-].
利用者にとっての導入作業の難易度	機器の構成の後天的な拡張や変更には、多くの場合一定の技術的知識（たとえば、プロセッサや主記憶用媒体の交換等には、ピン数、動作およびバス周波数特性、形状等に関する知識）や、筐体の開梱作業が必要。それゆえ機器の扱いに不慣れな者にとっての作業難易度は高い [-].	E-SATA や USB 等、利用者が外部周辺装置を接続するためのインタフェースが多くの機器に既装備。それゆえ、プロセッサや主記憶用媒記憶媒体の交換等と比べると、一般利用者にとっての二次記憶装置の容量拡張作業の難易度は低い [+]。
論理的手段による堅牢化		
物理的手段に対する相対的な開発費	対象は、基本ソフトウェアやアプリケーションソフトウェア。物理的手段の導入と比べると、開発に要する総経費は低い [+]。	対象は、基本ソフトウェアやアプリケーションソフトウェア。左記同様、物理的手段の導入と比べると、開発に要する総経費は低い [+]。
堅牢化に要する開発費	すべての堅牢化施策がホスト装置上のソフトウェアの実装手段によっているため、多くの視点に基づいた堅牢化策の実装が必要。対象のソフトウェア数の増大とともに、そのアーキテクチャ開発総工数および経費が膨大化する。またそのような状況が、実作業時に、施策の実施漏れを引き起こすことに関する危惧がある [-].	全体として実行する必要がある利用制御のうちの一部の処理を、一般利用者が不可触なソフトウェアが行うことにより、ホスト装置上のソフトウェアの要堅牢化部位を局所化できる。その結果、全処理をホスト装置のソフトウェアで実行する場合と比べて、単純な設計で、相対的に堅牢性が高いシステムを構築できる [+]。
ソフトウェアに対する一般利用者の可触性	ソフトウェアの記録先は、磁気ディスク装置等の二次記憶媒体の一般の記憶領域であるため、本質的に一般利用者は可触。それゆえ、動的攻撃に対する堅牢化とは別に、リバースエンジニアリングを通じたバイナリコードの静的解析を難化するような、ソースコード設計が必要 [-].	ホスト装置による読み出しは不要なソフトウェアであるため、一般利用者が記憶装置外から当該コードへアクセスするためのインターフェースの確保が不要。実際、そのような機能は未提供であり、一般利用者は不可触 [+]。
処理性能	堅牢化のための具体的施策のいくつかは、従来の処理に対する新たな付加的処理となるため、ソフトウェアとしての処理能力は低下する [-].	同左 [-].
保守性	バイナリコードを難読化させるためのソースコードの変更は、その可読性を大きく低下させる。その結果、従来と比べて保守作業が難化する [-].	ホスト装置がすべての処理を行う場合と比べて、ソースコードの可読性を低下させる処置を施す部位を限定できるため、保守作業の難化の度合いは、左記に比べて小さい [+]。
製品の品質均一性確保	製品に搭載された技術の他社への開示は、通常不可能であるため、堅牢化ソフトウェアの実装設計は、各々の開発元に一任される。その一方で、堅牢化処置が必要な部位が広範囲に及ぶため、各々の開発母体の製品の堅牢性の度合いは不均一になる。それゆえ、堅牢化処置が十分施されていないものも製品化される可能性がある [-].	項目 2 に記述したものと同様の理由により、左記と比べて堅牢性上の品質を高い度合いで均一化できる [+]。

2.3 ホスト装置全制御型コンテンツ利用制御に対する記憶装置部分制御型コンテンツ利用制御の有用性

前節に述べた考察に基づく、不正利用を目的とした攻撃からのコンテンツの保護を、より精度高く、安価なシステムで達成するには、従来とは異なった観点で新たに技術を構築する必要があると考えられる。その 1 つの解として、筆者らは、コンテンツの利用制御処理の一部を記憶装置が行うような技術の有用性について検討し、そのような概念に基づいた技

術⁹⁾⁻¹³⁾を過去に提案した。

上記技術の詳細な特徴について述べる前に、本節ではまず、コンテンツの利用を制御するための処理の一部を記憶装置が行うような形態のシステムが、同様の処理をホスト装置上のソフトウェアだけが行うような形態のシステムと比べて、開発工数、価格および攻撃に対する堅牢性といった点で多くの利点を持ちうることを、表 1 に示す。表 1 では、前者のコンテンツの利用制御法を「記憶装置部分制御型コンテンツ利用制御」、後者の制御法を「ホス

ト装置全制御型コンテンツ利用制御」と呼ぶ。なお、同表中各項目の説明文の終わりに置かれた + あるいは - は、示された説明文が、そのシステムの有効性を述べたものであるか、あるいは無効性を述べたものであるかを、端的に示すものである。

表 1 に示した結果に基づき、筆者らは、外部記憶媒体が磁気ディスク装置のように制御部を内蔵する場合は、ホスト装置と記憶装置を連携させつつ、コンテンツの利用可否を決定するうえで根幹となる処理の多くを記憶装置に行わせることにより、全体としてより高い精度でコンテンツの利用を制御するアーキテクチャを過去に提案した^{9)–13)}。本アーキテクチャの詳細な特徴は 4.1 節に述べることであり、ここではその特徴の概要のみ記す。

- (1) コンテンツ作成元（コンテンツサーバあるいはホスト装置）において、鍵 (K_{content}) および利用規則 (Usage Rule; UR) を生成する（以降では、両者をひとまとめにして利用制御情報 (Usage Control Information; UCI) と記述する）。
- (2) コンテンツ作成元において、 K_{content} を用いてコンテンツを暗号化する。
- (3) 記憶装置内に、通常のデータを記憶する領域（通常記憶部; Normal Storage）とは別に、認証を完了した接続相手だけがアクセスできる記憶領域（条件付き記憶部; Qualified Storage）を設ける。
- (4) 接続されるホスト装置の正当性を検証する機能を記憶装置制御部に設け、検証が成功した場合にのみ、利用制御情報を暗号化してホスト装置に転送する。
- (5) 実際に製品化されてから一定期間経過後に、攻撃者や設計者自身による解析によってホスト装置の脆弱性が明らかになった場合や、ホスト装置に有効期間が設定されていて、期限切れを起こした場合等に、該当するホスト装置のリストを記憶装置に与えることにより、該当するホスト装置に対する鍵や利用規則の出力を、記憶装置自身が停止する。

特徴 (4) により、外部記憶装置は不正あるいは危険なアプリケーションによるアクセスそのものを拒絶することはできないが、正当性が認められないホスト装置に対する利用制御情報の出力が完全に停止されるため、不正利用の防止をより高い精度で達成できる。また、利用制御情報が主記憶上で平文に展開されるタイミングを、処理手続き中全体の中で局所化できるようにするため、ソフトウェアにおいて堅牢な設計が必須な箇所の限定が可能になり、脆弱な箇所が残りにくいという利点もある。上記の手段は、そのほかにも、外部記憶媒体は一般に主記憶程の高速なアクセス性は不要であること、記憶容量が広大であることから、比較的低価格で開発が可能であること、ビット転送率が高く、一般に構造も複雑なコンテンツ本体を解析してその入出力を制御する必要がないこと、といった実装上有用な点も多数あ

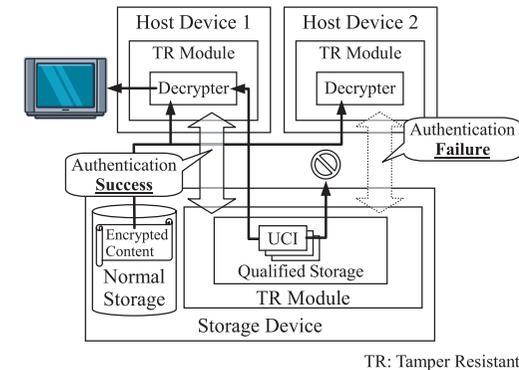


図 1 記憶装置主導型コンテンツ利用制御の基本アーキテクチャ
Fig. 1 Basic architecture for Storage Device initiative content usage control.

る。図 1 には、上記アーキテクチャの模式図と、実行されるアクセス制御の概念を示す。

以上に述べたように、文献 9)–13) に述べた技術では、記憶装置は単に利用制御の一部を担うという意味にとどまらず、ホスト装置に対する利用制御情報の出力可否決定権を持つことによって、コンテンツの利用可否決定を主導する立場にある。このような意味から、上記コンテンツの利用制御法を、本論文では記憶装置主導型アクセス制御と呼ぶ。

2.4 その他

システムの堅牢性の確保に関する議論とは別に、過去のアクセス履歴に基づいて、次にアクセス可能なコンテンツを決定する技術³³⁾も提案されている。これは、複数の Web コンテンツに含まれるリンクの巡回履歴によって、利用者に提供する情報の内容を柔軟に変更する機能を、Web サーバ上で実現するための基礎概念および技術を提案するものである。また、巡回履歴に基づく表示制御ではなく、複数のマルチメディアコンテンツを、1 つの画面上に同期させて表示するための制御法に関する研究³⁴⁾も提案されている。これらの技術はいずれも、攻撃に対する堅牢性の確保には特に配慮されたものではないため、利用者の手元に存在するコンテンツに対するアクセス制御の厳密な実現には、制御情報の機器間転送手続きや、システム全体の堅牢化手段等に関する検討が別途必要である。

3. 逐次的アクセス制御の応用例と本研究の狙い

1 章で触れた視聴時における CM 飛ばしを防止する基本的なアクセス制御法は、コンテン

ツ本編の表示を、その部分に対して協賛している企業の CM の表示を完了した場合に限定して許可することである。この制御は、コンテンツへのアクセスという観点からは、「CM コンテンツ全体もしくは一部（たとえば先頭 T 秒間）へのアクセスを完了すると、本編コンテンツに対するアクセスを許可する」という、コンテンツに対する逐次的な制御に置き換えられる。

テレビ放送コンテンツに代表されるように、1 つのコンテンツには、複数の CM と本編の要素が含まれると一般にはとらえられる。その場合、上記のコンテンツに対する逐次的なアクセス制御は、「第 n CM コンテンツへのアクセスを完了すると、第 m 本編コンテンツへのアクセスが許可される。続いて第 $n+1$ CM コンテンツへのアクセスも完了すると、第 m 本編コンテンツ全体へのアクセスが許可される」という形に拡張される。ここで n, m は対象とするコンテンツに含まれる CM および本編コンテンツを識別するための適当な番号である。コンテンツに対する上記の類の逐次的なアクセス制御は、様々なコンテンツ配信サービスが開始されつつある現在^{35),36)}、1 章で述べた「CM 収入によるビジネスモデルの存続」を可能にするためにも¹⁴⁾⁻¹⁷⁾ 放送サービスに限らず有用だと考えられる。

上記のようなコンテンツに対する逐次的なアクセス制御の単なる実現を目指すのであれば、ホスト装置が必要な処理のすべてをホスト装置で行うことで、目的は達成できる。しかし本研究の目標は、一般利用者によるコンテンツの視聴を、コンテンツ権利者が設定した利用規則内に確実に制限することであるため、価格・性能双方の点で実現性があり、かつ不正利用を意図した攻撃に対してできる限り高い堅牢性を持った技術の確立を目指す。一方で、利用者自身によるコンテンツの損壊、あるいは紛失した場合等に対する復旧や完全性を保証するための手段については、本研究の対象外とする。

3.1 逐次的なアクセス制御の応用例 (1)

上述のコンテンツに対する逐次的なアクセス制御法を具体的に表現するために、本論文で扱う 1 つのコンテンツは、 N 個のブロックデータが連結した連続型のマルチメディアコンテンツとする。個々のブロックデータを、BU (Block Unit) $[0], \dots, BU[N-1]$ と記述する。

個々の BU は、単体で CM や本編を構成している場合も、また複数の BU の集合が CM や本編を構成している場合もある。たとえば、各 BU が交互に CM と本編であった場合、上述したようなアクセス制御は、BU に対するアクセス規則という観点では、図 2 のように表現される。図 2 は、BU $[i]$ に対するアクセスを完了すると、BU $[i+1]$ に対するアクセスが許可されるという状態を表している。

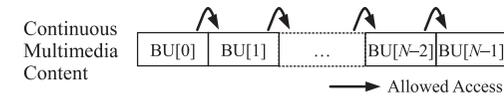


図 2 連続型コンテンツに対する逐次的アクセス制御規則例 (1)

Fig. 2 Example of sequential type access control rule for continuous content (1).

図 2 に示したアクセス制御は、各々の BU $[i]$ をそれぞれ異なる鍵で暗号化したうえで、記憶装置からのそれらの鍵の出力の逐次的制御を行うことによって実現できる。

次節では、上記アクセス制御をさらに拡張し、実利用上の有用性がより高いと考えられる逐次的アクセス制御規則の例を述べる。

3.2 逐次的なアクセス制御の応用例 (2)

CM コンテンツは、その目的上、コンテンツ全体の中で視聴者の興味を強く惹く部分に挿入されることが多い。一方で、CM コンテンツのこのような部位への挿入が、視聴時における CM 飛ばしをさらに助長しているとも考えられる。

そこで、権利者と視聴者の両者の要望に対する折衷案として、図 3 のようなアクセス規則を想定する。図 3 におけるコンテンツは、異なったアクセス制御規則が課せられた、4 つの部分コンテンツ (Portion) が連結したものである。

このアクセス制御規則は、以下のような特徴を持つ。

- 部分コンテンツ 2 (Portion 2) をアクセスするには、部分コンテンツ 1 (Portion 1) すべてにわたるアクセスを完了することを、同様に部分コンテンツ 4 (Portion 4) をアクセスするには、部分コンテンツ 3 (Portion 3) すべてにわたるアクセスを完了することを強制する。
- 部分コンテンツ 1 のすべてに対するアクセスを完了すれば、部分コンテンツ 2 については、自由なアクセスを許可する。部分コンテンツ 3 と部分コンテンツ 4 についても同様である。
- 部分コンテンツ 1 と 3 のすべてに対するアクセス実績管理を簡単に行えるようにするために、両者に対するアクセスは逐次的に行うことを強制する。
- 部分コンテンツ 1 と 3 の事前一括アクセスも許容する。両者の一括アクセスをあらかじめ実行した場合、部分コンテンツ 2 および 4 に対するアクセスを許可する。

上記制御は、たとえば部分コンテンツ 1 と 3 が CM コンテンツ、部分コンテンツ 2 と 4 が本編のコンテンツであるような場合に、本編コンテンツのある部分を視聴する前に、特定の CM コンテンツの視聴を利用者に強制するような場合に相当する。このような類の逐次

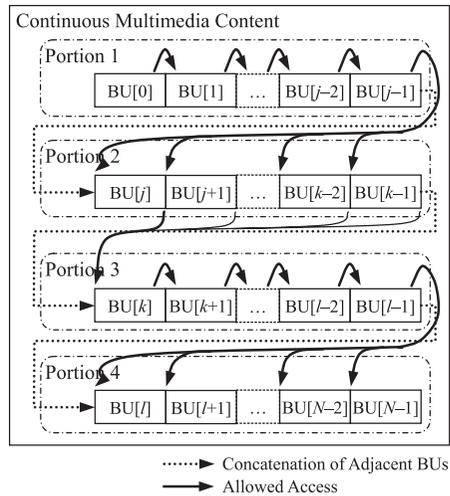


図3 連続型コンテンツに対する逐次的アクセス制御規則例(2)

Fig. 3 Example of sequential type access control rule for continuous content (2).

的アクセス制御は、映画等の商業用コンテンツに複数のCMコンテンツが組み合わされて1つのコンテンツを形成しているような場合に、特に有用であると考えられる。

3.3 コンテンツ生成工数および消費記憶容量の抑制

ある1つのコンテンツに対し、前節に記したような類のアクセス制御規則を複数種準備して利用者に提供する場合、それぞれの規則に対応したコンテンツの作成を制作者に求めるとすると、そのための工数および費用、また作成したコンテンツを蓄積するための管理費が必要となり、コンテンツの価格が高騰する懸念がある。本研究では、この点を回避することも狙いの1つとする。

4. 記憶装置主導型アクセス制御の基本概念とアーキテクチャ

本章では、3章に示した逐次的なアクセス制御を行うためのアーキテクチャを考察するための準備として、文献9)–13)に示した技術を、初めにより詳細に説明する。続いて、上記技術を基礎としつつそれを拡張し、記憶装置が制御の一端を担う形態を保ちつつ、3章に述べた複数BUに対する逐次的アクセス制御を実現するための概念的な手続きを提案する。

4.1 基盤従来技術

技術9)–13)では、以下に述べる方法に従ってコンテンツを保護することにより、その不正利用を防止する。

- コンテンツ作成元において、コンテンツを適当な大きさのブロックデータに分割する。ここで各ブロックデータは、CMや本編等意味のある単位である必要はない。個々のBUは、コンテンツ作成元で生成された鍵($K_{BU[0]}, \dots$)を用いて暗号化する。この鍵をBU鍵と呼ぶ。なお、以下ではBUの個数を N と仮定する。
- 各BUに対しては、他のBUへのアクセス実績とは無関係な内容の利用規則を設定できるようにするとともに、一意の値を識別子(BU Identifier; BUID)として割り当てる。前記利用規則を、個別利用規則(Individual Usage Rule; IUR)と呼ぶ。
- 個別利用規則IURは、ホスト装置がその内容解釈し制御するIUR_Hと、記憶装置が解釈し制御するIUR_Sとで構成される^{*1}。IUR_Sとしては、対象BUの複製可能回数^{*2}、再生可能回数等の設定が可能である。
- BU鍵と利用規則の組は、全体として個々のBUの利用を独立的に制御する情報となる。これを以下では、個別利用制御情報(Individual Usage Control Information; IUCI)と呼ぶ。
- 1つの個別利用制御情報は、個々を判別するための識別子IUCIID、個別利用制御情報が管理するBUに割り当てられた識別子BUID、および対応するサービスを含む自身の特徴を特定するフォーマット情報(Format)を含む。

図4に、 N 個のBUと、その各々に対する個別利用制御情報の関係を示す。同図において、フォーマットの値を F_0, \dots, F_{N-1} と記載しているが、コンテンツがある特定のサービスに属するものであるような場合は、通常これらはすべて同値である。また図5には、利用規則として再生可能回数が設定されている個別利用制御情報を、コンテンツの再生を目的としてホスト装置が読み出そうとした場合、他のBUへのアクセス実績とは無関係に、記憶装置は設定されている再生可能回数に基づいて、個別利用制御情報の出力可否を判断する

*1 これは、現状の記憶装置では制御が困難な規則、たとえば時間に関連した制御も、システム全体としては行えるようにすることが狙いである。時間に関する制御を記憶装置が正しく実行するには、時計機能だけでなく、利用者による時刻情報の変更を防止する機能の搭載も必要となるが、現状では非常に困難である。

*2 たとえば、ある1つのコンテンツの複製を行う場合に、前半部の複製を完了した場合に限り、後半部の複製も許可されるといったような制御は、実運用上の利点あまり感じられない。個々のBUについて、独立して複製の可否が設定されていれば十分である。このような制御に関しては、処理を簡素化するという観点からも、他のBUへのアクセス実績に依存せず制御できるようにしておくことが有用である。

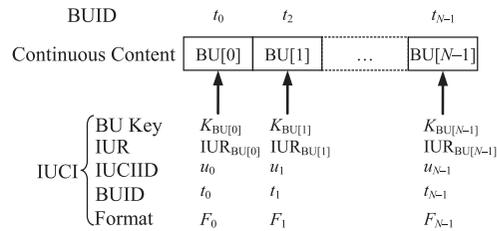


図 4 BU と個別利用制御情報群の対応関係

Fig. 4 Correspondence relation between Block Units and Individual Usage Control Information.

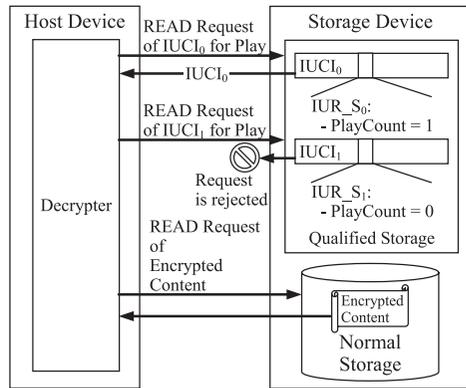


図 5 個別利用制御情報の読み出し要求と記憶装置の応答例

Fig. 5 Example of read request of Individual Usage Control Information and the response by Storage Device.

様子を模式的に示す。

個別利用制御情報は暗号化された BU の復号を制御する情報であるため、自由に書き込みや読み出しが実行できる通常記憶部 (図 1) に記録することはできない。また機器間を転送する間に BU 鍵を盗取されたり、個別利用規則を改竄されたりしないように、堅牢性を持つ機能部で暗号化等適切な保護を施した後に、転送先に対し送信する必要がある。

上記の点を考慮したため、技術 9)–13) を実現するシステムは、全体として図 6 のような構成を想定する。図中の保護モジュール (Protected Module) は、堅牢に設計された機能部であり、コンテンツの暗号化、および個別利用制御情報の管理を行うものである。

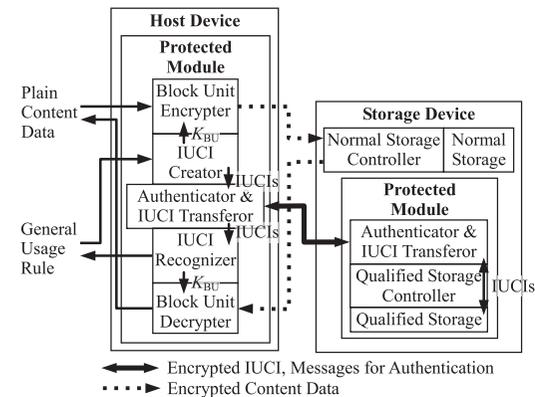


図 6 個別利用制御情報を用いて連続型コンテンツの利用を制御するアクセス制御システム

Fig. 6 Access control system controlling the usage of continuous content with Individual Usage Control Information.

ホスト装置の保護モジュールは、以下 5 つの機能部を含む。

- 認証および個別利用制御情報転送処理部 (Authenticator & IUCI Transferor)
記憶装置や他のホスト装置との間で個別利用制御情報を送受信する場合に、規定の protocol に従って相手機器を認証し、その送受信を実行する。
- 個別利用制御情報生成部 (IUCI Creator)
外界から入力された一般的利用規則から、構造が規定された個別利用制御情報を生成する。
- BU 暗号化部 (Block Unit Encrypter)
個別利用制御情報生成部から渡された BU 鍵を用いて、外界から入力された平文コンテンツを暗号化する。
- 個別利用制御情報解釈部 (IUCI Recognizer)
記憶装置から読み出した個別利用制御情報に含まれるホスト装置用の個別利用規則 IUR_H に基づいて、暗号化コンテンツの復号可否を判断する。そこで復号可能と判断された場合に限り、BU 鍵をコンテンツ復号化部に送信する。
- BU 復号化部 (Block Unit Decrypter)
個別利用制御情報解釈部から渡された BU 鍵を用いて、記憶装置から読み出した暗号化データを復号する。

記憶装置の保護モジュールは、以下 3 つの機能部を含む。

- 認証および個別利用制御情報転送処理部 (Authenticator & IUCI Transferor)

個別利用制御情報を送受信し合う機能が異なる点を除き、ホスト装置内の同名機能部と同じである。

- 制限記憶部制御部 (Qualified Storage Controller)

認証および個別利用制御情報転送処理部から書き込み要求および個別利用制御情報を受信した場合は、当該情報に含まれる個別利用規則のうち、記憶装置用の個別利用規則 IUR_S を解釈する。そこで書き込み可能と判断された場合に限り、制限記憶部への個別利用制御情報の書き込みを実行する。読み出し要求を受信した場合は、制限記憶部から個別利用制御情報を読み出すこと、また出力先が認証および個別利用制御情報転送処理部である点を除き、書き込み処理の場合と同じである。

- 制限記憶部 (Qualified Storage)

図 1 に示したとおり、個別利用制御情報を記録する実媒体である。

記憶装置内には、従来どおり自由にデータの書き込みや読み出しを行うことができる通常記憶部 (Normal Storage) および通常記憶部制御部 (Normal Storage Controller) も設けられる。

4.2 独立のアクセス制御処理手続き

本節では、記憶装置主導型でコンテンツへの逐次制御を実現する手続きを確立するための準備として、技術 9)–13) が規定する、各 BU へのアクセスを独立に制御するうえで必要な手続きの概略を説明する。

暗号化された各 BU の復号制御が他の BU へのアクセス実績に無関係である場合、ホスト装置と記憶装置の保護モジュールが相互に認証を行い、それに基づいて両者間で個別利用制御情報を暗号化して送受信し合うことにより、コンテンツの表示を個別利用規則の範囲内に制限できる。図 7 および 図 8 は、そのための基本的な処理手続きを示すものである。図 7 は記憶装置への書き込み処理を、図 8 は記憶装置からの読み出し処理を示している。図 8 における 2 つの Request (Request E.BU, Request IUCI) は、ホスト装置全体の動作を制御する部分 (通常プロセッサ) から送信される情報である。これら 2 つの処理手続きは、概要的には以下の処理からなるものである。

- (1) ホスト装置と記憶装置間での認証処理，その結果としてセッション鍵 K_s の共有。
- (2) 転送元装置における， K_s を用いての目的の IUCI の暗号化。
- (3) 転送元装置から転送先装置への暗号化された IUCI の送信。

書き込み処理の場合は，上記に加えて転送元装置において K_{BU} の生成，および生成した

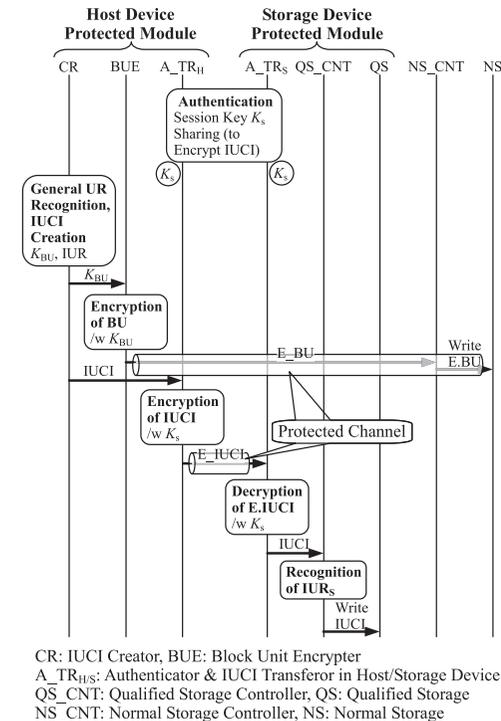


図 7 書き込み処理用の基本個別利用制御情報基本転送処理手続き
Fig. 7 IUCI basic transfer processing sequence for writing.

K_{BU} を用いての BU の暗号化が行われる。読み出し処理の場合は，上記に加えて，ホスト装置からの要求に応じて IUCI を出力する前に，当該 IUCI が含む UCI の内容を記憶装置が解釈し，その出力が許可されたものであるかどうかを個別に判断する。

4.3 逐次的アクセス制御処理手続き

本節では，3 章に示したような，ある 1 つの BU の表示可否が他の BU のアクセス実績に依存して決定される制御規則が課せられている場合に，前節に示した個別利用制御情報等の交換手続きを基礎としながら，それを拡張することにより，記憶装置主導型の利用制御形態を保ちつつ，逐次的アクセス制御を実現する処理手続きを示す。

上記を達成する 1 つの方法は，図 8 における IUR_S の解釈処理の近傍で，以下 3 つの概

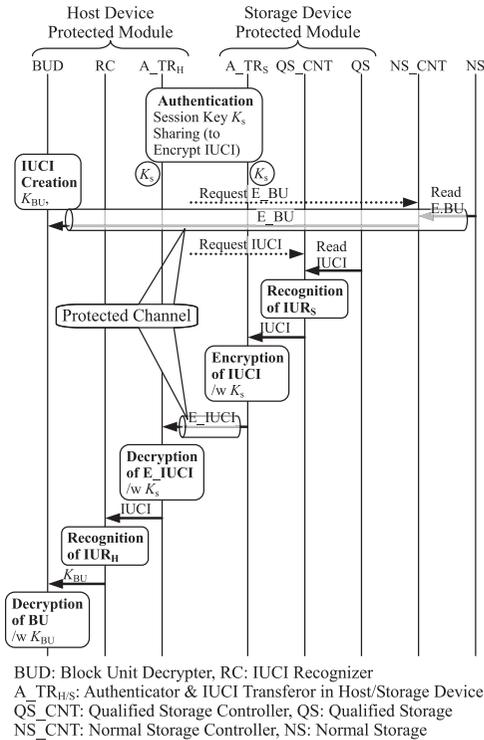


図 8 読み出し処理用の個別利用制御情報基本転送処理手続き
Fig. 8 IUCI basic transfer processing sequence for reading.

念的処理を新たに実行することである。

- BU 復号化部で実行された BU 群の復号処理実績の把握。
- ホスト装置から記憶装置へのアクセス実績情報 (Access Evidence ; AE) の安全な手段での送信処理。
- 逐次的アクセス制御規則に基づく記憶装置内での個別利用制御情報の出力制御。

図 8 に上記 3 項目を組み込むことにより、コンテンツに対する逐次的なアクセス制御を達成する概念的な処理手続きを、図 9 および以下に示す。

- (1) ホスト装置から記憶装置への IUCI[k] の出力要求を送信。
- (2) 記憶装置内での逐次的アクセス制御規則解釈。ここで逐次的アクセス制御規則には、

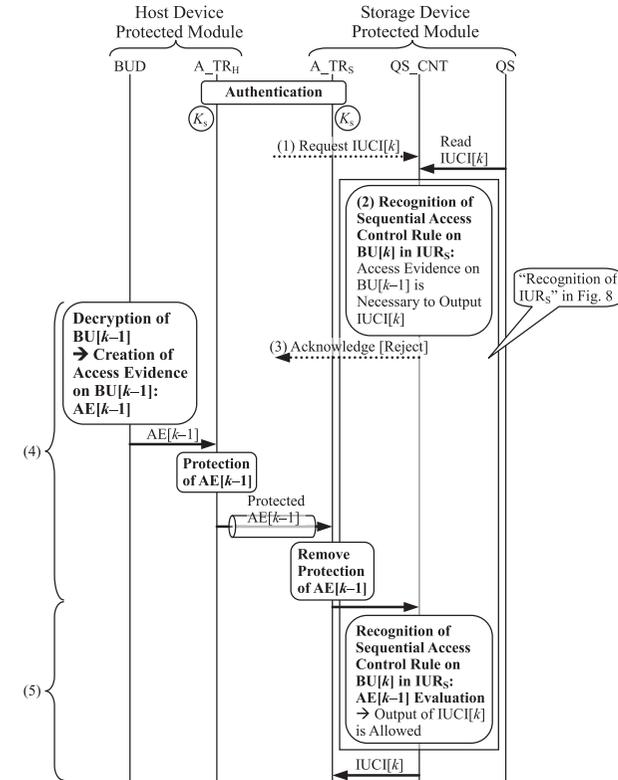


図 9 記憶装置からの個別利用制御情報出力制御による逐次的アクセス制御処理手続き
Fig. 9 Sequential access control processing sequence by IUCI output control from Storage Device.

「IUCI[k] の出力は BU[k-1] の表示が完了した場合のみ許可される」という内容が記述されているものとする。

- (3) BU[k-1] の表示を完了した証拠 AE[k-1] を記憶装置が未取得であったため、出力処理を中断。
- (4) BU[k-1] をホスト装置において表示、その証拠 AE[k-1] を保護した形で記憶装置に送信。

(5) 記憶装置において $AE[k-1]$ の正当性を検証, 検証を完了後 $IUCI[k]$ を出力.

上述のとおり, $AE[k-1]$ は, $BU[k-1]$ に対するアクセス実績を表す. この情報をホスト装置から記憶装置に対して送信する際は, 利用制御情報同様に暗号化等の保護を施す必要があるのは明らかである. アクセス実績の具体的な内容, およびその送信手段については, 次節で述べる.

4.4 アクセス実績情報とその管理

前節では, 1 つの BU について表示を完了したと解釈される点と, 実際に BU の復号を完了した点との間の関係については特に触れず, 当該 BU へのアクセス実績に基づいて他の BU へのアクセス可否決定を, 記憶装置が関与する形で実現する処理手続きの基本的な考え方を述べた. しかし, 各 BU へのアクセスが完了したと見なす条件は, 一般的にはサービスによって異なると考えられる. たとえば, 図 3 に示したような, 本編の表示に先立って CM コンテンツの表示の完了が必要な場合は, CM コンテンツ全体の復号完了をもって表示完了と見なすことが可能である. 一方で, 上記同様の逐次的アクセス制御が課せられたコンテンツについても, 入手に際して利用者に支払いを要求する場合には, 逐次アクセス制限が緩和されることも考えられる^{*1}. このような制御を行うためには, 上記制御に対する前提制御として, 次項に述べるような処理を実行する必要がある.

4.4.1 アクセス到達点指示子とアクセス到達点指示子リスト

ある 1 つの BU へのアクセスを完了したと見なす点 (以降ではこれを要到達点と呼ぶ) は, 一般的にはサービスごとに異なると考えられる. また, ある条件が設定されて生成され, 実際に利用者に配信されたコンテンツに対して, 後天的に内容が異なる条件が設定される可能性もある.

同一のコンテンツであるにもかかわらず, 要到達点に応じて異なるコンテンツの制作が必要となる場合, サービス提供者は, 暗号化処理や, その記録や配信のための記憶システムの大規模化を求められる. 利用者にとっても, 要到達点ごとに異なるコンテンツの入手が必要となるうえ, そのための工数や記憶容量の確保を求められることになり, 好ましいとはいえない. このような問題を回避するために, ここでは次の 3 つの情報を新たに導入する.

- アクセス到達点指示子 (Accession Point Indicator ; API)

1 つの API は, タグ部とペイロード部からなる. タグ部には API を一意に識別するための固定値を, ペイロード部には K_{BU} と同程度の長さを有する乱数を記述する. これらは,

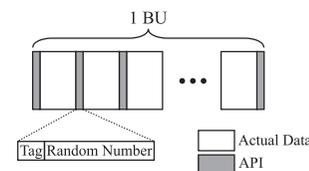


図 10 1 BU への複数 API 挿入
Fig. 10 Plural APIs insertion in a BU.

BU を生成する際に, K_{BU} による暗号化に先立って, 複数の位置に挿入する^{*2}. 図 10 に, その模式図を示す.

- アクセス到達点指示子リスト (Accession Point Indicator List ; APIL)

APIL は, 1 つの個別利用制御情報が管理する 1 つの BU に含まれるすべての API の値のリストである. BUID を 1 つ特定すると, 当該 BU に対応する APIL が 1 つ特定される.

- アクセス完了条件 (Access Completion Condition ; ACC)

1 つの BU に対するアクセス完了条件は, 当該 BU 中の API の順序数で指定する. たとえば, アクセス完了条件として n が指定されていた場合, 該当 BU において先頭から n 番目の API が挿入されている位置までの復号を完了すると, アクセスを完了したと判断する. この順序数のことを, 以降では API 番号 (Accession Point Indicator Number ; APIN) と呼ぶ.

次項には, 上記 3 つの情報を用いたアクセス実績の確認処理について述べる.

4.4.2 アクセス実績確認処理

API の生成, および平文コンテンツへの挿入は, 図 11 に示すような機能部からなるサーバ装置が通常行う. ここでサーバ装置とは, 図 4 に示したホスト装置と記憶装置を内蔵するのに加え, 保護モジュール内に, API 生成および挿入部 (API Generator & Inserter) を含むという特徴を持つ. API 生成および挿入部は, 平文コンテンツを BU 暗号化部へ入力する前に置かれ, API を当該データに挿入する処理を行う.

- サーバ装置から記憶装置への APIL の書き込み処理

サーバ装置から記憶装置への APIL の書き込み処理は, 図 7 に示したホスト装置から記憶装置への個別利用制御情報書き込み処理と同様とする. すなわち, 認証処理で共有したセッション鍵 K_s を用いて, サーバ装置において APIL を暗号化 (E-APIL) し, 記憶装置

*1 各 BU の冒頭数秒を復号した時点で表示完了と見なすような場合は, その一例である.

*2 挿入された各 API のペイロードの値は, すべて異なるようにする.

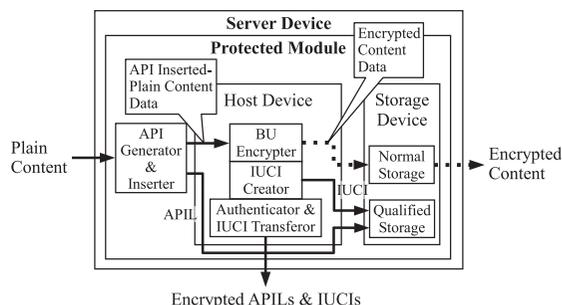


図 11 サーバ装置
Fig. 11 Server Device.

に送信する．記憶装置では，同鍵を用いて E_API を復号した後，制限記憶部に記録する．

● 記憶装置でのアクセス実績確認処理

記憶装置によるアクセス実績の確認は，図 12 に示す処理手続きによって達成する．以下，詳細を説明する．

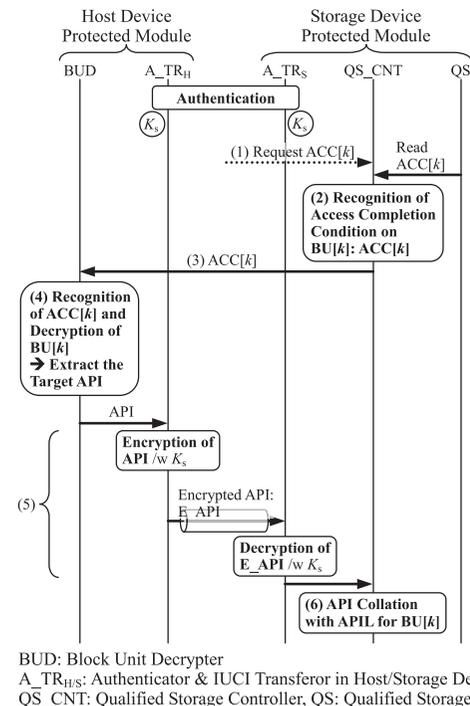
- (1) ホスト装置から記憶装置へ，BU[k]に関するアクセス完了条件 ACC[k] の出力を要求．
- (2) 記憶装置内での ACC[k] 解釈；ACC[k] として，API 番号 j が指定されているものとする．
- (3) 記憶装置からホスト装置へ ACC[k] を送信．
- (4) ホスト装置での ACC[k] 解釈，その結果に基づき，BU[k] を復号し，API のタグ値を検索；j 番目のタグを検出し，API を抽出．
- (5) K_s を用いて処理 (4) において抽出した API を暗号化し，記憶装置へ送信．
- (6) 記憶装置において，受信した API を APIL の j 番目のエントリに記述された値と照会；両者が一致すれば，BU[k] の表示が完了したと判定．

上記処理手続きから明らかのように，4.3 節で導入したアクセス実績情報 AE[*] は，本項で導入した API に相当する．

上記手続きを実行するようなアーキテクチャを構築することにより，要到達点を含む逐次的アクセス制御規則の通常領域への記録，および無保護状態での読み出しが可能になる．

4.4.3 API の挿入位置と挿入頻度

API の挿入位置が BU 内において任意であるとする，復号された BU の一部に API タグの値と同じビット列が含まれていた場合に，それが API タグであるのか BU の一部であ



BUD: Block Unit Decrypter
A_TR_{H/S}: Authenticator & IUCI Transferor in Host/Storage Device
QS_CNT: Qualified Storage Controller, QS: Qualified Storage

図 12 記憶装置でのアクセス実績確認処理手続き
Fig. 12 Access status confirmation processing sequence in Storage Device.

るのかを判別できない．したがって，API の挿入が可能な位置に関しては，一定の規則を設ける必要がある．具体的な考察を進めるために，ここでは連続コンテンツが日本のデジタルテレビ放送であることを仮定し，適切な API の挿入位置，その頻度，および大きさ等について，一案を示す．

日本におけるデジタルテレビ放送コンテンツデータのフォーマットは，ビットレートが約 16 Mb/s の MPEG2-TS (Transport Stream)³⁷⁾ である．MPEG2 データの動画の復号処理単位は GOP (Group of Pictures) であることを考慮すると，API の挿入位置を GOP と GOP の間に限定するのは，1 つの適切な手段であると考えられる．このような限定を課することにより，API 検出処理をピクチャごとの画像生成処理から分離することが可能になり，効率的に処理を実行できる．

1つのGOPが含むデータは、多くの場合において0.5秒間分の動画像を生成する。仮に、すべてのGOP間へAPIを挿入した場合、0.5秒単位で要到達点を設定できることになる。しかし、要到達点はある1つのBUに対するアクセスを完了したと判断する点であることを考えると、1秒から数秒に1つ程度の刻み幅で設定できれば、サービス上は十分であると考えられる。以上から、APIの挿入位置、頻度、大きさについて、ここでは以下を仮定する。

- APIを挿入する頻度を8GOP(4秒間)に1つとする。
- 個々のAPIの容量は、現在コンテンツの暗号化アルゴリズムとして広く用いられているのが鍵長128ビットAES³⁹⁾であること^{20),38)}にならい、16バイトとする。

上記仮定の下では、1つのGOPと1つのAPIの容量比は、タグの大きさを考慮に入れた場合でも、およそ $1:3.0^{-6}$ である。記憶容量が100ギガバイトである記憶装置の場合、総APIが占めるのは数キロバイト程度であり、総容量に対して当該情報が占める容量は、ほとんど無視できる。

なお、APIとAPILを用いた記憶装置での表示完了判断処理の効率化を図るためには、1つのAPILの容量も重要なパラメータとなる。たとえば、あるBUIDが割り当てられたBUに関するAPILが、制限記憶部上の複数の領域にまたがって記録されていた場合は、その読み出し処理時の負荷が高くなる恐れがある。上記仮定をそのまま踏襲し、かつ1つの個別利用制御情報が管理するBUは1分間分の動画像情報を含むと仮定すると、1つのBUには30個のAPIが含まれることになる。前記のとおり、1つのAPIの容量が16バイトであるとすると、1つのBUに含まれるAPIの総容量は480バイトとなる。この大きさは、1つのAPILの媒体上への書き込みおよび読み出しが、1度の記憶装置に対する処理(1セクタの書き込み/読み出し処理)で完了できるという点から、実装上有効であると考えられる。

4.5 逐次的アクセス制御規則の管理方法

前節に記した処理手続きに従って記憶装置からホスト装置への個別利用制御情報の出力を制御することで、逐次的アクセス制御は実現できる。しかし、コンテンツ配信サービスを実際に立ち上げる際の有用性や実装時の簡便性を高めるためには、制御規則の管理体系を明確に規定しておく必要がある。以下の項では、その方法を述べる。

4.5.1 制御規則記述データ

逐次的アクセス制御規則を具体的なデータとして記述し、記憶装置に記録する方法としては、下記の2種類の方法が考えられる。第1の方法は、各々の個別利用制御情報のIUR.Sに、個別利用制御情報の出力の前にアクセスを完了していることが必要なBUの識別子(BUID)を記述する、というものである。第2の方法は、個々の個別利用制御情報には規則は記述

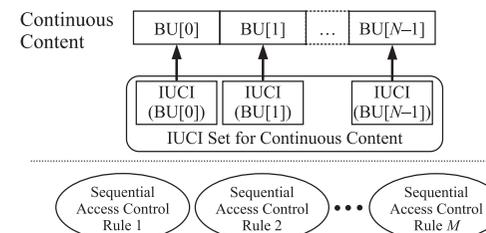


図 13 個別利用制御情報と逐次的アクセス制御規則の関係

Fig. 13 Relation between IUCIs and sequential access control rules.

せず、逐次的アクセス制御規則を記述する別のデータを新たに導入するというものである。個別利用制御情報の再利用性という観点からすると、次に述べる理由により、第2の方法の方がより適切であると考えられる。

あるコンテンツに対する複数の逐次的アクセス制御規則を、当該コンテンツとともに1つの記憶装置に記録する場合、第1の方法では、それぞれの逐次的アクセス制御規則に対応して個別利用制御情報群を記録する必要がある。一方で第2の方法の場合、逐次的アクセス制御規則については目的に応じて複数個記録する必要があるが、個別利用制御情報群については1種類のみ記録でよい。図13は、1つのコンテンツに対して、それを構成する個々のBUに対する個別利用制御情報群は1つであるのに対し、複数種の逐次的アクセス制御規則の割当てが可能であるということを模式的に表したものである。

この方法の利用は、図7に記した記憶装置に対する個別利用制御情報を記録する際の処理負荷の低減、および記録される利用制御情報の総量を削減する効果を持つ。また、個別利用規則が、対応するBU単体に関する内容に限定されるため、個別利用制御情報単体の容量を抑えることができるという利点もある。現状の記憶装置の多くは、512バイトを単位としてデータ転送を行うように設計されており、なかでも磁気ディスク装置は、512バイトを単位として媒体に対する書き込みおよび読み出し処理を実行するため、個々の個別利用制御情報の容量が512バイト以下であれば、制限記憶部へのアクセスも通常記憶部と同様に512バイト単位で実行できる。この場合、容量の変換性への対応が不要となるため、設計や処理を簡素化できるという点でも有効である。

以上から、逐次的アクセス制御規則は、個別利用制御情報ではなく、当該規則のみを含む別の情報として記述することとする。当該情報の管理方法については、既存のシステムに対する相互運用性を考慮したファイルシステム構造の構成法とともに、次項に述べる。

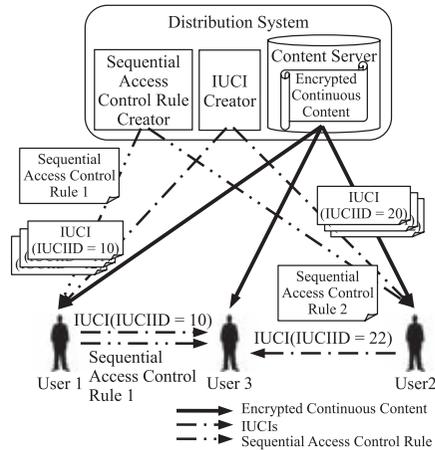


図 14 個別利用制御情報群, 逐次的アクセス制御規則, 暗号化された連続型コンテンツの流通形態
Fig. 14 Circulation of IUCI sets, sequential access control rules and encrypted continuous content.

4.5.2 制御規則の記述法

逐次的アクセス制御規則の具体的な記述は, 図 14 に示すようなサービスの提供が可能になるという意味において, 個別利用制御情報の識別子 IUCIID ではなく, BU の識別子 BUID を用いて行うのが適切である.

図 14 は, 以下に述べるような状況を模式的に示したものである.

- (1) 利用者 1, 2, 3 が, それぞれ独立に, 同一の暗号化された連続型コンテンツを入手する.
- (2) 利用者 1 が, 入手した暗号化コンテンツを復号するための個別利用制御情報群 (IUCIID = 10, 11, 12) と, 逐次的アクセス制御規則 1 を入手する.
- (3) 利用者 1 は, 自身が入手した 3 つの個別利用制御情報と, 逐次的アクセス制御規則 1 を, 利用者 3 に譲渡する.
- (4) 利用者 2 は, 利用者 1 とは独立に, 暗号化されたコンテンツを復号するための個別利用制御情報群 (IUCIID = 20, 21, 22) と, 逐次的アクセス制御規則 2 を入手する.

逐次的アクセス制御規則が BUID を用いて記述されていた場合, 当該規則は IUCIID には非依存となる. この場合, ある暗号化コンテンツ (BU 群) を復号するための BU 鍵群を含む個別利用制御情報群は, 複数種類存在しても矛盾を生じない. 別の表現をすれば, 図 14

に示したように, あるコンテンツを管理する個別利用制御情報群として, IUCIID = 10, ... のものと, IUCIID = 20, ... のものとが同時に存在することが許容されるということである. ただし, 両 IUCI 群は, 同じ BU 鍵群を含むものである.

逐次的アクセス制御規則が BUID を用いて記述されていると, 同図に示すように, 利用者 3 は, 利用者 1 と利用者 2 から全体として目的のコンテンツを復号するに足る IUCI 群と, どちらか一方 (双方でもよい) から逐次的アクセス利用規則の譲渡を受ければ, 当該コンテンツを利用できる. 同図は, 利用者 3 が, 利用者 1 から IUCIID が 10 である IUCI 群と逐次的アクセス制御規則を, 利用者 2 から IUCIID が 22 である IUCI 群の譲渡を受けている様子を表している. 逐次的アクセス制御規則が IUCIID を用いて記述されていた場合は, このような IUCI 群および逐次的アクセス制御規則のやりとりは不可能である.

5. 相互運用性および処理負荷を考慮した実装アーキテクチャ設計

本章では, 4 章で述べた, 逐次アクセス制御を記憶装置主導型で実現するために必要なくつかの情報の抽象的な交換処理手続きを基に, 実際の記憶装置のインタフェース仕様に適合する, 実装アーキテクチャを提案する. 提示する項目は, 逐次的アクセス制御を実行するうえで必要な様々な情報の管理および記録方法, インタフェース上で交換される命令とメッセージ, および上記 2 つに付随して実行されるホスト装置および記憶装置内での具体的な処理である.

初めに, 文献 12), 38) で示されている, 現在広く用いられているファイルシステム構造との親和性を考慮した, 個別利用制御情報の管理方法について述べる. そして, それを逐次的アクセス制御を行うことができる形態への拡張方法を提案する.

続いて, 現在広く用いられている記憶装置用インタフェースの特性と親和性を維持した, インタフェース上での命令とメッセージの交換手続きを提案する.

最後に, 上記処理が現行の記憶装置製品に与える性能上の影響を試算した結果を示す.

5.1 相互運用性の確保を考慮したファイルシステム構造

可搬型の記憶装置の場合, 通常記憶部上に構築するファイルシステム構造は, 多くのホスト装置が解釈できるか, 解釈できない場合は開発が容易であるようなものである必要がある. 普及を促進するという意味において, このような考え方は初期段階では特に重要である. そこで本章では, 光ディスク媒体等で広く利用されていて, 仕様が公開されている UDF (Universal Disc Format) のファイルシステム構造⁴⁰⁾ を拡張することで, 個別利用制御情報や逐次的アクセス制御規則を管理する方法を提案する.

5.1.1 コンテンツと個別利用制御情報の関連付け

本項ではまず、文献 12) に記載されている、UDF⁴⁰⁾ を基礎としたコンテンツと個別利用制御情報群を関連付ける方法を述べる。実用性を考慮して、コンテンツとしては日本のデジタルテレビ放送をここでは想定する。

日本のデジタルテレビ放送コンテンツを 2 つの媒体間で移動する際、1 分間を超える部分データが、移動元と移動先に同時に利用可能な形で存在してはならないという規定がある⁴¹⁾。このような規定の下では、個別利用制御情報の転送が失敗した場合の復旧処理を簡潔にするために、あらかじめ 1 分間分のデータに 1 つ個別利用制御情報を割り当てるのが適切である。

上記の実現方法としては、コンテンツと個別利用制御情報の関係を記述したデータを用意し、それに付随させてコンテンツと利用制御情報群を配置するという方法が、第 1 に考えられる。これを UDF におけるファイルシステム構造上で実現する場合、関連付け情報を記述したデータを主ファイルとし、コンテンツとすべての個別利用制御情報を Named Stream^{*1}として上記主ファイルに付随させることに相当する。

しかし UDF では、再生時にリアルタイム性の保証が必要なデータを、Named Stream として記録することが認められていない。したがって、テレビ放送コンテンツのような再生時にリアルタイム性の保証が必要なデータは、上記のような体系でファイルシステム構造内に配置することはできない。

また、UDF では、アプリケーションによる個々のファイルの容量の取得要求に対して、主ファイルの容量のみを応答するように規定されているため、コンテンツ本体のデータを Named Stream として UDF 上に配置すると、アプリケーションがその容量を把握できないという問題もある。

以上のような理由から、UDF を基にファイルシステム構造を構築する場合は、コンテンツは主ファイルとして、関連付け情報は当該コンテンツに付随する Named Stream として配置する必要がある。このような考え方に基づいた、コンテンツ、個別利用制御情報、および両者を関連付ける情報の UDF 上への配置法を、図 15 に示す。

図 15 における各要素は、以下のような意味である。

- Program[*i*] : この記憶装置に記録されている *i* 番目のコンテンツ。
- IUCI(IUCIID = *q*) : Program[*i*] を構成する BU の中の 1 つを管理する、識別子の値

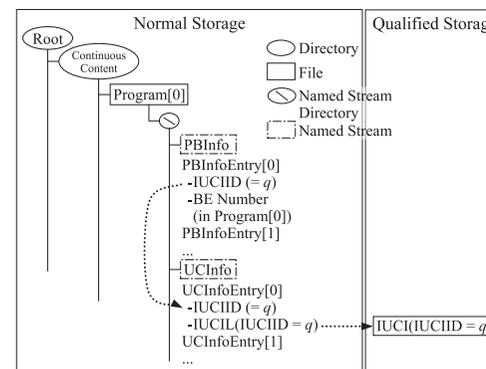


図 15 UDF ファイルシステム構造内での個別利用制御情報とコンテンツの配置法

Fig. 15 Allocation method of Individual Usage Control Information and continuous content in UDF file system format.

が *q* である個別利用制御情報。

- PBInfo, UCInfo : 2 つでコンテンツと個別利用制御情報とを関連付ける Named Stream . 上位層である PBInfo には、個々の個別利用制御情報が管理する BU を特定する情報 BUID と、個別利用制御情報の識別子 IUCIID を関連付ける情報を、下位層である UCInfo には、PBInfo で指定した IUCIID と、記憶媒体上の物理的な記録位置との関連付け情報を記述する^{*2} .

5.1.2 コンテンツと逐次的アクセス制御規則の関連付け

逐次的アクセス制御規則を保護する目的は、記録されている制御規則に対する利用者の意図的な改竄攻撃から守ること、また制御規則に従ってコンテンツへ実際にアクセスした際に、利用者が意図的な迂回処理を行うことができないようにすることである。一方で、上記目的が確実に担保される限り、処理負荷を抑制するためにも、制御規則の参照は、保護のための処理を行わずに実行できるようにすることが望ましい。ホスト装置の画面に、記憶装置に記録されている逐次的アクセス制御規則を単に表示する場合等は、その典型的な例である。

そこで、逐次的アクセス制御規則は、以下に記す 8 つの特徴をともなった形態で、記憶装置上のファイルシステム構造内に配置する。図 16 は、ここで導入される情報、その参照関

*2 2 階層からなる Named Streams を用いて個別利用制御情報とコンテンツを関連付けると、アプリケーションとの間で情報を交換する情報と、ハードウェアリソースを管理する情報を独立して開発できるという意味で、有用である。

*1 UDF では、主ファイルに関する属性情報を記述するデータは Named Stream と呼ばれる。

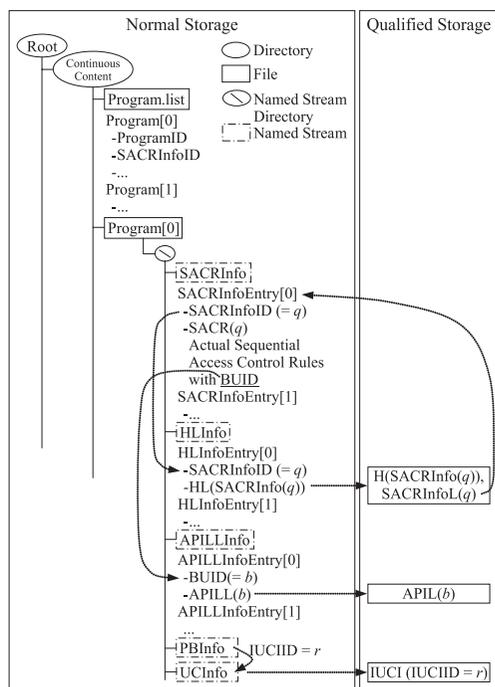


図 16 UDF ファイルシステム構造における逐次的アクセス制御関連情報の配置法

Fig. 16 Allocation method of sequential access control related information in UDF file system format.

係等を視覚化したものである

- (1) 逐次的アクセス制御規則は、PBInfo や UCInfo と同様に、元となるコンテンツに付随する Named Stream として記述する。これを以下では、SACRInfo (Sequential Access Control Rule Information) と呼ぶ。
- (2) SACRInfo には、複数のエントリを設けることができる。各エントリには、別個の逐次的アクセス制御規則を記述する。
- (3) SACRInfo の各エントリに記述される逐次的アクセス制御規則には、識別子 (SACRInfoID) を割り当てる。なお、SACRInfoID の値が q であるエントリに記述された逐次的アクセス制御規則を SACR(q)、当該エントリに含まれるデータ (SACRInfoID (= q) と SACR(q) の組) を、SACRInfo(q) と記述する。

- (4) SACR(q) は、BUID を用いて記述する。
- (5) SACRInfo(q) を通常記憶部に記録する際、通常記憶部制御部は SACRInfo(q) のハッシュ値を求め、制限記憶部に記録する。このハッシュ値を $H(\text{SACRInfo}(q))$ と記述する*1。 $H(\text{SACRInfo}(q))$ を記録する制限記憶部の領域には、SACRInfo(q) が記録されている通常領域の位置情報もあわせて記録する。
- (6) ハッシュ値 $H(\text{SACRInfo}(q))$ と SACRInfo(q) とを関連付けるための Named Stream を、ファイルシステム構造内に配置する。これを HLInfo と記述する。HLInfo には、 $H(\text{SACRInfo}(q))$ が記録されている制限記憶部内位置情報 SACRInfoL(q) を記述する。
- (7) BU (BUID = b) に挿入されている API のリスト (これを APIL(b) と記述する) を、制限記憶部へ記録する。これと並行して、APIL(b) が記録された位置情報を含む Named Stream をファイルシステム構造内に配置する。これを APILLInfo と記述する。
- (8) APILLInfo には、複数のエントリを設けることができることとする。各エントリには、対応する BU の BUID、および当該 BU に挿入されている API のリストが記録された制限記憶部内位置情報 APILL を記述する。なお、BUID の値が b である BU に挿入された API のリストを APIL(b)、その位置情報を APILL(b) と記述する。

特徴 (2) および (3) は、1 つのコンテンツに対して複数の逐次的アクセス制御規則を割り当てられるようにするために設けられたものである。ただしサービスによっては、同一のコンテンツを記録した複数の記憶装置間で逐次的アクセス制御規則を移動させることもありうるので、同一の SACRInfoID が割り当てられた複数の SACRInfo が存在することがないような配慮が必要である。そのためには、規則生成元において、規則内容ごとに一意の値を割り当てるのが適切である。

特徴 (4) は、たとえば複数の異なる利用者から、ある 1 つの暗号化コンテンツを復号するための個別制御情報群を要求された場合、識別子 IUCIID や個別利用規則 IUR は異なるが、 K_{BU} に関しては共通の個別利用制御情報群をサーバ装置等が提供できるようにするためのものである。

特徴 (5) および (6) は、既存の記憶装置に対する親和性を高めるために設けられたもの

*1 $H(\text{SACRInfo}(q))$ は、サーバ装置に SACRInfo(q) とともにあらかじめ配置しておいても、通常記憶部制御部が実際の記録処理を行う際に生成してもよい。サービスの運用方針によって決定される。

である。既存の記憶装置は、ほとんどが自らデータの書き込みや読み出し等の処理を開始する機能を持たず、アクセスすべき領域の位置情報を、目的の処理を開始させる命令とともに、ホスト装置から受信することによって、処理を実行する。また、2章に記載したとおり、既存の記憶装置のほとんどは、通常記憶部に記録されているデータの構造を理解する機能を持たない。これは、書き込み/読み出しいずれの処理についても、指定されたデータを、機械的に指定された領域に書き込む/読み出す機能しか持たないということの意味する。実用性に配慮するという観点から、筆者らが過去に提案した技術^{9)–13)}も、この特徴は基本的に維持している。一方で、制限記憶部制御部および制限記憶部は、当該制御部とホスト装置との間での認証処理を実行し、その結果に応じて制限記憶部へのアクセス可否を決定する機能や、制限記憶部に記録されている利用規則の内容を解釈し、自身からの個別利用制御情報の出力可否判断をする機能といった、従来一般的な記憶装置にはない新しい機能を有するものである。逐次的アクセス制御を実行するうえでも同様の考え方を踏襲し、制限記憶部制御部には、逐次的アクセス制御を実行するうえで、担保する必要がある特殊な処理を行わせる。また、制限記憶部には、当該制御部を実行するうえで、保護する必要がある（改竄されると逐次的アクセスを迂回できるような）情報を記録する。その具体的な処理内容については、次節に示す実インタフェースを想定した処理手続きとあわせて、補足に述べる。

上記は、特徴(5)に述べた内容、すなわち $H(\text{SACRInfo}(q))$ を記録する制限記憶部内領域に $\text{SACRInfoL}(q)$ もともに記録する、ということに対する根拠となっている。 $\text{SACRInfo}(q)$ は通常記憶部に記録されるデータであるため、記憶装置のインタフェース用標準入出力命令を使って、コンテンツの実データと同様に書き込みや読み出しが行われる。 $\text{SACRInfo}(q)$ を書き込んだり読み出したりする場合に限り、通常領域へのアクセスであるにもかかわらず、特殊な処理を実行するように記憶装置を設計するのは、既存の記憶装置の設計方針に反するものであるため、不適切である。一方で、 $\text{SACRInfo}(q)$ に含まれる情報を基に、ホスト装置主導で制限記憶部の指定された領域をアクセスすること、そして当該領域に記録されている情報に基づいて、記憶装置が自身で通常領域をアクセスするように記憶装置を設計することは、独自規定の挙動が制限記憶部へのアクセスにすべて付随しているという意味で、 $\text{SACRInfo}(q)$ 関連処理を特殊化することに比べ、実効的である。

以上に述べた逐次的アクセス制御規則の管理体系とは別に、記憶装置に記録されているコンテンツ、およびそれに付随している SACRInfo の情報をアプリケーションが簡単に把握できるようにするために、それらのリストをファイルシステム構造内に記録しておくことは、逐次的アクセス制御規則の高速な把握が可能となるという点で、実用的である。この情

報を、以下では Program.list と記述する。 Program.list の1つのエントリは、記録されている連続型コンテンツ1つを特定するための識別子 ProgramID 、およびそれに付随したすべての SACRInfo の識別子 SACRInfoIDs を含む。

なお、 $H(\text{SACRInfo}(q))$ 用アルゴリズムに関しては、ここでは特に限定しない。アルゴリズムの選択において考慮すべき事項としては、転送時に個別利用制御情報を暗号化する際に用いる鍵データより長いハッシュ値を生成するものであること、一方で生成されるハッシュ値長が、制限記憶部の1アクセス単位（セクタ）以下であることがあげられる。なお、 $H(\text{SACRInfo}(q))$ を記録する領域には、 $\text{SACRInfoL}(q)$ もあわせて記録する。

5.2 実インタフェースを想定した処理手続き

逐次的アクセス制御を、実際の機器上で実現するためには、図7、図8、図9に示した概念的な処理手続きを、実際に利用されているインタフェース特性に適合するように、命令とそれとともなって送信されるメッセージデータの組として、具体的に規定することが必要である。サーバ装置とホスト装置の間は TCP/IP 等のネットワークインタフェースで、ホスト装置と記憶装置の間は $\text{ATA}^{18)}$ で接続されると考えると、本技術の適用範囲が広がれると考えられる。

TCP/IP を介した通信では、転送元装置が通常処理用の命令とデータ本体を一体化し、1つのメッセージとして転送先装置に送信する。これに対し、 ATA を介した通信では、書き込み/読み出しを問わず、ホスト装置が特定のパラメータセットをともなった命令を送信することによって、データの転送処理が開始される。上記に関する詳細な処理手続きについては、付録に記載する。

5.3 記憶装置における処理負荷評価

図2に示した逐次的アクセス制御に従って個別利用制御情報の入出力を実行する場合、記憶装置内では、以下および図17に示す有限オートマトンに従う状態遷移管理が必要となる。

$$M_{\text{BUID}} = \{Q_{\text{BUID}}, \Sigma_{\text{BUID}}, \delta_{\text{BUID}}, s_{\text{BUID},0}, F_{\text{BUID}}\}$$

$$\text{状態: } Q_{\text{BUID}} = \{Z, q_0, \dots, q_{N-1}, E\}$$

$$\text{入力アルファベット: } \Sigma_{\text{BUID}} = \{x_{\text{in}} | x_{\text{in}} = 0, 2, \dots, N-1\}$$

$$\text{初期状態: } s_{\text{BUID},0} = Z$$

$$\text{受理状態: } F_{\text{BUID}} = q_{N-1}$$

図17における入力アルファベット Σ_{BUID} は、 b_0, \dots, b_{N-1} ではなく、 b_0 からの相対値を用いている。上記オートマトンは、ホスト装置から送られたある BUID が割り当てられた BU へのアクセス実績情報を記憶装置が解釈し、記憶装置が自身の内部状態を遷移させる

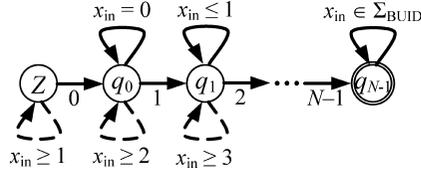


図 17 図 2 に示した逐次的アクセス制御を実現する制限記憶部管理部の状態遷移

Fig. 17 State transition diagram of qualified storage controller realizing sequential access control shown in Fig. 2.

様子を示している．状態遷移図としての入力アルファベットは BUID であるが，指定された BU へのアクセスが完了したか否かを判断するために記憶装置が用いる情報は，4.4.2 項で述べたとおり，API である．

各々の状態 q_i ($i = 0, \dots, N - 1$) から出ている実線の枝は正常終了処理に関するもので，次の 3 段階からなる処理が最後まで終了したことを意味する．

- (1) BUID 値が $b_0 + i + 1$ である個別利用制御情報の出力要求を，記憶装置が受信する．
- (2) 記憶装置がホスト装置に対して，処理 (1) で要求された個別利用制御情報を出力する．
- (3) ホスト装置において当該個別利用制御情報を用いた BU の復号が完了し，その結果を記憶装置が受信する．

一方で破線の枝は，エラー処理である．上記処理 (1) と同様に，状態 q_i において BUID 値が $b_0 + i + 2$ 以上の値の個別利用制御情報の出力要求を記憶装置が受信した場合，記憶装置は当該要求に基づく処理を中断する．このとき，逐次的アクセス制御規則として何らかのエラー状態への遷移が義務付けられていない限り，実利用時の利便性を高めるという観点から，状態はそのまま q_i にとどまるよう規定するのが適切である．

SACR(q) が図 3 に示した逐次的アクセス制御規則であった場合も， Q_{BUID} の要素が異なる点を除き，図 17 と同様の有限オートマトンを記憶装置が管理する必要がある．これを図 18 に示す．

$$\text{状態: } Q_{\text{BUID}} = \{Z, q_0, \dots, q_{j+l-k-2}, E\}$$

$$\text{入力アルファベット: } \Sigma_{\text{BUID}} = \{x_{\text{in}} | x_{\text{in}} = 0, 2, \dots, N - 1\}$$

$$\text{初期状態: } s_{\text{BUID},0} = Z$$

$$\text{受理状態: } F_{\text{BUID}} = q_{j-1+l-1-k} = q_{j+l-k-2}$$

図 3 に示した逐次的アクセス制御は，たとえば部分コンテンツ 2 に含まれる BU [j], ..., BU [$k - 1$] へのアクセスは，部分コンテンツ 1 全体の逐次的アクセスを完了すれば許可さ

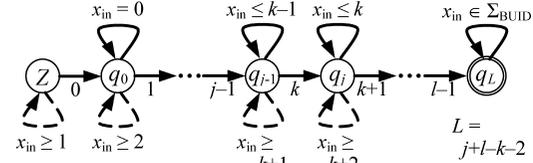


図 18 図 3 に示した逐次的アクセス制御を実現する制限記憶部管理部の状態遷移

Fig. 18 State transition diagram of qualified storage controller realizing sequential access control shown in Fig. 3.

れるといった類のものである．上記オートマトンは，この様子を示している．たとえば，状態 q_0 から q_{j-1} に至る遷移は，部分コンテンツ 1 への逐次的アクセスに相当する．この範囲の各状態が，自身の状態番号以下の BUID 値を受信した場合は，アクセスをすでに完了している BU への再アクセスに相当するため，自身に正常遷移する．また，状態番号と同値の BUID の値が入力された場合は，逐次的アクセスを課せられていて，かつ過去にアクセスしたことがない BU 群のうち最も前方にある BU へのアクセスを完了した場合に相当するため，次の状態へ遷移する．

ところで，図 18 における状態 q_{j-1} は，図 3 において，部分コンテンツ 1 中の BUID 値が $j - 1$ である BU へのアクセスを完了した状態に相当する．この状態に到達すると，部分コンテンツ 2 に属する任意の BU (BUID 値は $j, \dots, k - 1$) へのアクセスが許可されるため，入力値が $k - 1$ 以下であった場合は，自身に正常遷移する．他方，入力値が k であった場合は，逐次的アクセス制御が課せられた部分コンテンツ 3 の先頭 BU へのアクセスが完了したと判断され，次の状態 q_j に遷移する．終了状態は，逐次的制御が必要な BU へのアクセスを完了した状態であるため，BUID 値が $l - 1$ である BU へのアクセスを完了した状態に相当する．一般的には，上記有限オートマトンにおける状態数は，最大の場合で 1 つのコンテンツに含まれる全 BU の数と一致する．

以上から明らかなように，図 2 と図 3 に示したアクセス制御を達成するうえで，記憶装置が内部で実行する必要があり，比較的負荷となると予想される新しい処理は，コンテンツ利用開始時における SACRInfo(q) のハッシュ値計算 (1 度のみ)，受信した API の復号処理，その APIL への照会，およびそれらの結果に基づく上記状態遷移管理である．これらの処理を新たに記憶装置で行う場合，下記仮定の下で，次のような概略的な処理負荷の試算が可能である．

- 記憶装置として，磁気ディスク装置を想定する．

- 通常再生を想定する．
- 記憶装置に搭載されるプロセッサの処理能力を，広く使用されている組み込みプロセッサ⁴²⁾程度と想定し，その特性を，動作周波数を 100 MHz，32 ビット演算と仮定する．
- 記憶装置における主要なタスク（たとえば磁気ディスク装置の場合，サーボ制御等）が，プロセッサの処理の 7 割程度を占める．すなわち，本論文に記したアクセス制御のために使用できるプロセッサの処理能力は，実質的には 30 MHz と想定する．
- AES 復号処理に要する時間は，一般に公開された公表値⁴³⁾に基づいて試算する．示されているのは，動作周波数が 96 MHz のものを用いた結果であるので，単位時間あたりの処理データ量を，示されている値の 1/3 程度とする．なお，鍵長は 128 ビットを想定する．

API の長さを 16 バイトとすると，30 MHz 程度の組み込みプロセッサの場合，上記からその復号に要する時間は 2～数 μ s 程度と評価できる．

SACRInfo(q) のハッシュ値計算に要する時間は，SACRInfo(q) の大きさに依存して変化するので，通常のテキストデータファイルが数 kB 程度であることから，ここではそれと同程度と仮定する．また，単位時間に計算できるデータ量を，上記 AES 復号処理と同程度とすると，本処理に要する時間は，1 から数 ms と評価できる．

一方，復号した結果得られた API の APIL への照会/比較処理は，一般的なプロセッサの動作，すなわち

- 割込み
- レジスタに保持している情報の主記憶への退避
- 受信した API の主記憶からプロセッサ内レジスタへのロード
- APIL の 1 つのエントリ中の値の主記憶からレジスタへのロード
- 比較
- 比較結果の主記憶へのアンロード

を考慮することで，おおよその評価が可能である．1 つの APIL の大きさは 16 バイトであり，プロセッサのレジスタは 4 バイトであることから，上記中のロードから結果のアンロードに至る処理は，4 回実行する必要がある．すべての処理について，1 つあたり 2 クロック以上を消費したと仮定しても，受信した API と，APIL の 1 つのエントリの値を比較するのに必要な総クロック数は，100 以下である．これを，30 MHz 程度のプロセッサで処理する場合，処理時間は 3 μ s 程度である．

上記結果から，先頭部から連続的にコンテンツを再生する場合については，本論文に記載

した逐次的アクセス制御に関連した処理が他の処理へ与える影響は，ほとんど無視できる程度であると見積もることが可能である．

ただし，実際にコンテンツの再生を続ける中での動作性や，早送りや巻き戻し等の特殊再生時の動作性についてはこの限りではないため，今後の検討課題とする．

6. まとめと今後の課題

本論文では，1 つの連続的なコンテンツへのアクセスに関して逐次的制約が課せられていた場合に，当該制約に沿ったアクセス制御の一端を記憶装置に担わせることにより，従来に比べ堅牢性が高いアクセス制御アーキテクチャを提案した．具体的な提案内容は，逐次的アクセス制御を実現するうえで必要な情報の管理方法，およびホスト装置と記憶装置間での当該情報の具体的な交換手続きである．アーキテクチャの構築に際しては，多様な機器との接続互換性，および現行の記憶装置に対する親和性の確保に，十分に配慮した．

また，提示した制御を実行するために新たに記憶装置に搭載する必要がある処理を示し，現行の記憶装置での実行可能な見通しを得た．実際にコンテンツを再生している場合や，特殊再生を実行した場合の処理負荷，および動作性については，今後の検討課題とする．

参考文献

- 1) DVD Forum Official Website. <http://www.dvdforum.com/forum.shtml>
- 2) Blu-ray Disc Association. <http://www.blu-raydisc.com/index.htm>
- 3) Home — SD Association. <http://www.sdcard.org/home>
- 4) Napster の楽曲ダウンロードサービス，著作権侵害と判決．
<http://japan.internet.com/busnews/20000728/7.html>
- 5) 権利者軽視では結論出ない？著作権制度「大所」からの議論開始．
<http://internet.watch.impress.co.jp/cda/news/2009/04/20/23214.html>
- 6) 「パンドラの箱を開けてしまったようだ」，大荒れの私的録音録画小委員会．
<http://techon.nikkeibp.co.jp/article/NEWS/20080710/154659/?ref=RL2>
- 7) 謎解き「Blu-ray 課金」，目的は「ダビング 10」と「iPod 課金」の分離．
<http://techon.nikkeibp.co.jp/article/TOPCOL/20080619/153467/?ref=RL2>
- 8) 「権利者から見ると文化庁案が最大限の妥協」— CPRA 椎名和夫氏に聞くダビング 10 問題の真因．
<http://techon.nikkeibp.co.jp/article/NEWS/20080618/153434/?ref=RL2>
- 9) Hirai, T. and Hori, Y.: An HDD-based removable medium and its AT-attachment interface architecture for copyright protection, *IEEE Trans. Consumer Electronics*, Vol.49, pp.1161–1168 (Nov. 2003).
- 10) Hirai, T.: Content protection technology for a novel removable drive, *IEEE Trans.*

- Magnetics*, Vol.41, pp.860–869 (Feb. 2005).
- 11) Hirai, T., Hori, Y., Shimizu, Y. and Takemura, I.: Overview of Content Protection Technology for Intelligent Attached Devices, *Digest of ICCE*, pp.107–108 (Jan. 2006).
 - 12) Hori, Y., Taima, K. and Hirai, T.: Secure Framework of Audiovisual Content based on Bi-directional Authentication for Hard Disk Drive, *Digest of ICCE*, 1.1-4 (Jan. 2008).
 - 13) Hirai, T. and Inagaki, Y.: Secure Procedures to Reconnect Intelligent Devices and Recover Content Usage Control Information, *Digest of ICCE*, 1.3-4 (Jan. 2009).
 - 14) IT media ライフスタイル：民放の“タイムシフト視聴嫌い”を変えるには？
<http://plusd.itmedia.co.jp/lifestyle/articles/0507/21/news089.html>
 - 15) 西 正：視聴スタイルとビジネスモデル，日刊工業新聞社 (2005).
 - 16) 西 正：IT vs 放送 次世代メディアビジネスの工房，日経 BP 社 (2005).
 - 17) IT media ライフスタイル：地上波のビジネスモデルが壊れていくことは，視聴者に幸福をもたらすか？
<http://plusd.itmedia.co.jp/lifestyle/articles/0505/06/news015.html>
 - 18) Technical Committee T13 AT Attachment. <http://www.t13.org/Standards/>
 - 19) Publications and Current Versions. <http://www.4centity.com/docs/versions.html>
 - 20) Specifications. <http://www.aacsla.com/specifications/>
 - 21) Boneh, D., Lie, D., Lincoln, P., Mitchell, L. and Mitchell, M.: Hardware support for temper-resistant and copy-resistant software, Technical Report, Stanford University Computer Science (1999).
 - 22) Suh, E., Clarke, D., Gassend, B., Dijk, M. and Devadas, S.: AEGIS: Architecture for tamper-evident and tamper-resistant processing, *Proc. International Conference on Supercomputing*, pp.160–171 (2003).
 - 23) 春木洋美，橋本幹生，川端 健：敵対的な OS からソフトウェアを保護するプロセッサアーキテクチャ，情報処理学会論文誌：コンピューティングシステム，Vol.45, No.3 (2004).
 - 24) 笹木俊介：FRAM 搭載商品のセキュリティ設計。
<http://img.jp.fujitsu.com/downloads/jp/jmag/vol53-2/paper04.pdf>
 - 25) Trusted Computing Group-Home.
<https://www.trustedcomputinggroup.org/>
 - 26) Lie, D., Thekkath, C.A. and Horowitz, M.: Implementing an untrusted operating system on trusted hardware, *Proc. ACM Symposium on Operating Systems Principles* (2003).
 - 27) Chatterjee, R., Ryder, B.G. and Landi, W.A.: Complexity of point-to analysis of java in the presence of exceptions, *IEEE Trans. Softw. Eng.*, No.27, pp.481–512 (2001).
 - 28) Collberg, C., Thomborson, C. and Low, D.: A taxonomy of obfuscating transformations, Technical Report 48, Department of Computer Science, University of Auckland (1997).
 - 29) Aucsmith, D.: Tamper Resistant Software: An Implementation, *Information Hiding*, pp.317–333 (1996).
 - 30) Microsoft Windows Media — デジタル著作権管理 (DRM).
<http://www.microsoft.com/japan/windows/windowsmedia/drm/default.aspx>
 - 31) AACSLA – Advanced Access Content System. <http://www.aacsla.com/jp/home>
 - 32) 著作権保護技術「AACSLA」の解説問題について声明。
<http://www.watch.impress.co.jp/av/docs/20070126/aacs.htm>
 - 33) 清光英成，田中克己：Web リンクの巡行に基づく動的なリンク活性化とアクセス管理，情報処理学会論文誌：データベース，Vol.42, No.SIG8 (TOD 10) (2001).
 - 34) Synchronized Multimedia Integration Language.
<http://www.w3.org/TR/REC-smil/>
 - 35) 「アクトビラ」公式情報サイト。<http://actvila.jp/>
 - 36) 無料動画：映画，海外ドラマ，アニメほか—パソコンテレビ GyaO [ギャオ].
<http://www.gyao.jp/>
 - 37) ISO/IEC 13818-1: 2007 Information Technology — Generic coding of moving pictures and associated audio information: Systems.
<http://www.itl.nist.gov/fipspubs/fip180-1.htm>
 - 38) SAFIA LICENSE GROUP, SAFIA Specifications. <http://www.safia-lb.com>
 - 39) NIST, FIPS PUB 197, Announcing the ADVANCED ENCRYPTION STANDARD DARD AES. <http://www.techheap.com/cryptography/encryption/fips-197.pdf>
 - 40) OSTA Universal Disk Format Specifications. <http://www.osta.org/specs/>
 - 41) 社団法人電波産業会：ARIB TECHNICAL REPORT B-15 4.2 版。
 - 42) ルネサステクノロジ—マイクロコンピュータ。http://japan.renesas.com/fmwk.jsp?cnt=mpumcu_category_landing.jsp&fp=/products/mpumcu/
 - 43) DENSO CREATE: aes_spec.pdf.
http://www.denso-create.jp/service/products/iotacrypt/documents/aes_spec.pdf

付 録

A.1 実インタフェース上の処理シーケンス

サーバ装置，ホスト装置，および記憶装置の間を接続する実際のインタフェース上で送受信される命令やデータ，およびそれに付随して実行される各装置で実行される詳細な処理を，本節で述べる。

記憶装置用インタフェースを介してメッセージを送受信する場合は，本文に記載したとおり，ホスト装置が記憶装置に命令を送信することによって，処理が実行される。この点を考

慮し、送受信されるデータとともに、ホスト装置から記憶装置に対して送信される命令の種類を記す。命令は、WC_x (Write Command; 命令に続いて、ホスト装置から記憶装置に対して実データが転送されるもの)、RC_x (Read Command; 命令を受信すると、記憶装置からホスト装置に対して実データが転送されるもの)、NDC_x (Non Data Command; 実データ転送が行われないもの)の3種類である。添え字 x は N, Q のいずれかであり、それぞれ通常記憶部、制限記憶部をアクセスするための命令であることを表す。添え字が N である命令は、それぞれの記憶装置のインタフェース仕様に応じて、ATA¹⁸⁾等規格として規定されているものを実際には用いることを想定する。これに対し、添え字が Q である命令は、本論文に示した技術に沿って独自に規定されるものである。

一方、ネットワークを介して装置間でメッセージを送受信する場合は、通常双方の装置がともに自立的にメッセージを発信できるため、特に命令の類は記述せず、メッセージデータのみを記すこととする。

なお、送信対象機器のネットワークアドレスは、メッセージデータ本体に対する付加情報として、また記憶装置内のアクセス対象領域の位置情報は、ホスト装置が発行する命令のパラメータとして、通常は相手装置に送信されるため、当該情報に関しても明示的な図示はしない。

A.1.1 サーバ装置から記憶装置への逐次的アクセス制御関連情報の書き込み処理

実際のインタフェースで接続されたサーバ装置、ホスト装置、および記憶装置を用いて、サーバ装置から記憶装置へ逐次アクセス制御に関連した情報を記録するための処理手続きを、以下および図 19 に記す。

- (1) サーバ装置とホスト装置の間で認証処理を実行し、対称暗号化用の鍵 K_{s,sv_h} を共有する。
- (2) サーバ装置からホスト装置に対し、サーバ装置が提供するコンテンツおよび SACRInfo のリストを送信する^{*1}。
- (3) ホスト装置上で、受信したコンテンツおよび SACRInfo のリストの中から、望むものを利用者が選択する。ここでは、選択されたものを Program, SACRInfo(q) とする。ここで Program は、ProgramID の値が p であるコンテンツとする。また、Program

*1 サービス上の完全性保証という観点からは、伝送路上でメッセージに改竄が加えられた場合に対する検知機能を持たせることが望ましい。メッセージに K_{s,sv_h} を連結して鍵付きハッシュ値を求め、メッセージに連結して送信する方法は、その一例である。メッセージの内容を隠蔽するという意味で、メッセージ全体を暗号化するという手段でもよい。

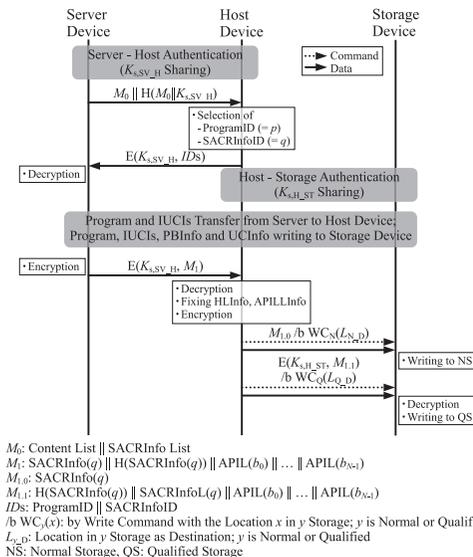


図 19 ホスト装置を介した逐次的アクセス制御関連情報実記録処理手続き

Fig. 19 Actual writing processing sequence of sequential access control related information through host device.

は、BUID の値が b_0, \dots, b_{N-1} である N 個の BU の連結体とする。

- (4) ホスト装置が、ProgramID (= p), SACRInfoID (= q) を K_{s,sv_h} を用いて暗号化し^{*2}、サーバ装置に送信する。ただし、Program がすでに記憶装置に記録されていた場合は、SACRInfoID のみ送信する。
- (5) サーバ装置と記憶装置の間で、暗号通信路を確立する。当該暗号通信路は、ホスト装置と記憶装置の間で暗号通信路を確立した後、処理 (1) で確立したサーバ装置とホスト装置の間の暗号通信路とを、保護モジュール内で連結する形態で実現する^{*3}。
- (6) Program, 当該連続型コンテンツを復号するための BU 鍵を含む個別利用制御情報

*2 本処理の目的は、利用者の選択結果に関する伝送路上での改竄防止と、伝送路上への選択結果開示の回避の双方である。

*3 処理 (1) で確立したサーバ装置とホスト装置の間の暗号通信路とは別に、サーバ装置と記憶装置の間で直接認証処理を実行することによって、対称暗号化用の鍵 K_{s,sv_st} を共有してもよい。文献 11) にはそのような鍵共有手続きの例が示されている。

群を、ホスト装置から記憶装置へ送信する。ホスト装置は、送信されたデータの受信を完了すると、両者を関連付けるための PBInfo および UCInfo の内容を確定する。そして、Program, PBInfo, UCInfo は通常記憶部に、個別利用制御情報群については制限記憶部に記録する。本論文では、その詳細手続きに関する記述は省略する。

- (7) サーバ装置は、処理 (5) で確立した暗号通信路を通して、SACRInfo(q), APIL 群 $\{APIL(b) \mid b = b_0, \dots, b_{N-1}\}$, $H(SACRInfo(q))$ をホスト装置へ送信する。Program が処理 (6) 以前に記憶装置上に記録されていた場合、APIL 群は通常すでに記録済みであるため、送信されない。
- (8) ホスト装置は、受信したデータを復号する。続いて、 $H(SACRInfo(q))$ および $APIL(b)$ の記録先位置を決定し、 $HL(SACRInfo(q))$ および $APILL(b)$ の値を確定する。そして、 $SACRInfo(q)$, $HL(SACRInfo(q))$ および $APILL(b)$ を通常記憶部に、APIL 群と $H(SACRInfo(q))$ を制限記憶部に、図 16 に示したファイルシステム構造に沿って記録する。

A.1.2 逐次的アクセス制御規則に基づくホスト装置と記憶装置間での処理手続き

逐次的アクセス制御を実現するための記憶装置からホスト装置への個別利用制御情報の出力制御処理手続きを、以下および図 20 に記す。前節同様に、個別利用制御情報の転送処理に関する記述は省略する。

- (1) ホスト装置は、標準読み出し命令を用いて、記憶装置の通常記憶部から Program.list を読み出す。
- (2) 利用者が、ホスト装置上で視聴を希望するコンテンツデータおよび逐次的アクセス制御規則を選択する。選択されたコンテンツデータおよび逐次的アクセス制御規則データに割り当てられた各識別子の値を p (= ProgramID), q (= SACRInfoID) とする。
- (3) ホスト装置と記憶装置の間で認証処理を実行し、対称暗号化用の鍵 $K_{s,HLST}$ を共有する。
- (4) ホスト装置は、暗号化された Program およびそれに付随する Named Streams を、標準読み出し命令を用いて通常記憶部から読み出す。
- (5) ホスト装置は、以下 4 段階の処理を実行する。
 - (a) 処理 (4) において読み出した SACRInfo および HLInfo の中から、SACRInfoID が q であるエントリを検索する。
 - (b) [SACRInfo 関連] 処理 (5a) において目的のエントリを検出した場合、当該

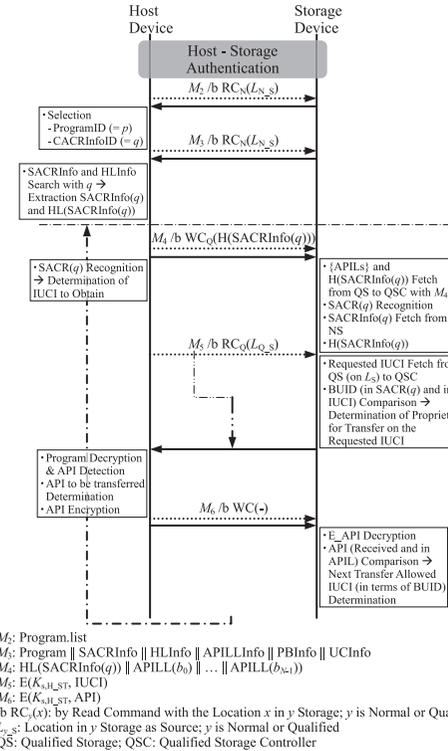


図 20 記憶装置用実インタフェース上での逐次的アクセス制御処理手続き
Fig. 20 Sequential access control processing sequence on actual interface for Storage Device.

エントリに記述されている $SACR(q)$ を解釈し、表示する BU の順序を決定する。

- (c) [HLInfo 関連] 処理 (5a) において目的のエントリを検出した場合、当該エントリに記述されている $HL(SACRInfo(q))$ を、制限記憶部に対する書き込み命令に付随するパラメータとして設定する。
- (d) [APILL 関連] 処理 (5c) で準備した書き込み命令に続いて、Program に付随する APILLInfo のすべてのエントリに記述されている $APILL\{APILL(b_0), \dots, APILL(b_{N-1})\}$ を、データとして記憶装置へ送信する。

- (6) 記憶装置は、以下 6 段階の処理を実行する。
- (a) [Qualified Storage からのデータの読み出し] HL(SACRInfo(q)) が指し示す制限記憶部内領域から、記録されているハッシュ値、および SACRInfo(q) の記録先位置情報 SACRInfoL(q) を制限記憶部制御部に読み出す。
 - (b) [Qualified Storage からのデータの読み出し] SACRInfoL(q) が指し示す通常領域から SACRInfo(q) を制限記憶部制御部に読み出す。
 - (c) [ハッシュ値計算] 制限記憶部制御部において、処理 (6b) で読み出した SACRInfo(q) のハッシュ値を求める。
 - (d) [ハッシュ値比較] 制限記憶部制御部において、処理 (6a) で読み出したハッシュ値と処理 (6c) で求めたハッシュ値とを比較する。
 - (e) [SACRInfo(q) 保持] 処理 (6d) に記した検証処理を完了したら、処理 (6b) で読み出した SACRInfo(q) を、制限記憶部制御部内に保持し続ける。
 - (f) [APILL 群保持] {APILL(b_0), ..., APILL(b_{N-1})} が指し示す制限記憶部内領域から、{APIL(b_0), ..., APIL(b_{N-1})} を読み出し、制限記憶部制御部内に保持する。
- (7) ホスト装置は、逐次的アクセス制御規則 SACR(q) に従い、個別利用制御情報読み出し命令を記憶装置に対して発行する*1。なお、本命令の発行に際しては、目的の個別利用制御情報が記録されている制限記憶部内領域の位置情報を、パラメータとして指定する。
- (8) 記憶装置は、以下 3 段階の処理を実行する。
- (a) [Qualified Storage からのデータの読み出し] 受信した位置情報が指し示す制限記憶部内領域から、個別利用制御情報を制限記憶部制御部に読み出す。
 - (b) [IUCI 出力可否判断] 処理 (8a) で読み出した個別利用制御情報に含まれる BUID を、処理 (6b) で制限記憶部制御部に保持した SACR(q) に照らし合わせ、当該個別利用制御情報の出力可否を判断する。
 - (c) [ICUR 送信] 処理 (8b) の結果に基づき、ホスト装置へ個別利用制御情報を送信もしくは本処理を中断する。
- (9) ホスト装置は、以下 3 段階の処理を実行する。
- (a) [BU 復号] 処理 (8c) で入手した個別利用制御情報を用いて、目的の暗号化された BU を復号する。
 - (b) [API 順次検出] 処理 (9a) を実行しながら、当該 BU に挿入されている API タグを順次検出する。
 - (c) [目的の API 検出] 処理 (9b) において、(5b) で選択した SACR(q) に記述されている順序数と同じ APIN である API タグを検索する。検索の結果、目的の API が検出されたら、そのペイロード部に含まれる 16 バイトのデータを K_{s,H_LST} を用いて暗号化し、記憶装置に送信する*2。
- (10) 記憶装置は、以下 3 段階の処理を実行する。
- (a) [API 復号] 受信した API を復号する。
 - (b) [受信した API と保持している API の比較] 処理 (6e) 以来、制限記憶部制御部内に保持されている SACRInfo(q) の中の SACR(q) を参照し、制限記憶部制御部内に保持されている APIL の中から適切なものを 1 つ選択し、さらにその中から APIN 番目のエントリを選択後、処理 (10a) で得た API と比較する。
 - (c) [次出力可能 IUCI 決定] 処理 (10b) の比較を完了した後、次に出力可能な個別利用制御情報の条件 (BUID の値) を決定する。

処理 (6f) 以降の処理を繰り返して実行することにより、SACR(q) に従った Program の逐次的アクセス制御を達成する。

A.1.3 通常記憶部内での情報の配置換えにともなって必要な処理

デフラグ等の処理によって、通常記憶部に記録されている逐次的アクセス制御関連情報の記録先位置を変更した場合、SACRInfoL として制限記憶部内に保持されている SACRInfoEntry の位置情報と、当該情報が実際に記録されている位置に食い違いを生じる。そこでこのような処理を実行した場合には、以下の処理をホスト装置が実行する必要がある。

- (1) HLInfo の各エントリに記述された HL(SACRInfo(*)) の値をホスト装置が把握する。
- (2) 制限記憶部に対する単純な書き込み命令を用いて、処理 (1) で得た HL(SACRInfo(*)) の値を書き込み先アドレスとして指定し、配置換え後の (対応する) SACRInfoEntry の位置情報をデータとして付随させて記憶装置に送信する。

*1 ホスト装置が記憶装置に対して最初に出力を要求する個別利用制御情報は、無条件に記憶装置からの出力が可能なものである必要がある。出力に際して前提条件が課せられた個別利用制御情報が最初に要求された場合、記憶装置は当該要求に基づく処理の実行を中断する。

*2 暗号化は、ホスト装置と記憶装置の間で個別利用制御情報を転送する際に施されるものと、鍵長、アルゴリズムおよび暗号化回数の点で同様とするのが適切である。

- (3) 記憶装置は、受信した SACRInfoEntry の位置情報を、制限記憶部内の指定された位置に書き込む。

処理(2)において、攻撃者が意図的に SACRInfoEntry の位置情報を書き換えるような攻撃を実行したとしても、不正な値が指し示す通常記憶部の領域に記録されている SACRInfo の値のハッシュ値は、制限記憶部に記録されているハッシュ値と一致しない。それゆえ、記憶装置は IUCI の出力要求を受信しても、それを拒絶する。

(平成 21 年 3 月 20 日受付)

(平成 21 年 7 月 10 日採録)

(担当編集委員 樋口 健)



平井 達哉 (正会員)

1994 年早稲田大学大学院理工学研究科物理学および応用物理学専攻修士課程修了。同年(株)日立製作所入社。マルチプロセッサ型サーバ機用アーキテクチャ、磁気ディスク装置用信号処理、高付加価値型記憶装置用基盤アーキテクチャ(セキュリティ技術ほか)等の研究開発に従事。平成 17 年より京都大学大学院情報学研究科博士後期課程在学。平成 20 年単位認定退学。IEEE, 電子情報通信学会各会員。



田中 克己 (正会員)

京都大学大学院情報学研究科社会情報学専攻教授。1976 年京都大学大学院博士前期課程修了。博士(工学)。主にデータベース、マルチメディアコンテンツ処理、ウェブ検索の研究に従事。IEEE Computer Society, ACM, 人工知能学会, 日本ソフトウェア科学会, 日本データベース学会各会員。TUG 会員。