高度ディジタルAVフレームワークの多面的安全性とその特性

金子 格[+]

［要旨］本論文ではMPEG-21等で想定される高度AVサービスの多面的安全性について考察し、その特性について示す。デジタルAV符号化、複合メディア符号化、ネットワーク配信を組み合わせた高度AVサービスが急速に進歩し、不正競争、プライバシー、組織犯罪、デジタルデバイド(情報化による格差)などの新しいへの関心が高まっている。本論文では、まずこれらの問題をセキュリティの要求仕様としては多面的安全性としてとらえる。次に、多面的安全性によるセキュリティのモデルを提示する。

Multi-lateral security on the Advanced Digital Audio Visual Framework

Itaru Kaneko[+]

Abstract:.
In this paper, multi-lateral security in the context of MPEG-21, Audio Visual Framework will be discussed. Advanced Audio-Visual Services, as combinations of Digital Audio-Visual coding, hyper-media coding and network, are rapidly evolving and various issues such as privacy violation, crime increase and IT divide are drawing broader interest. In this paper, firstly we will consider these problems as the requirements of multilateral security. And secondly we propose multilateral security model.

1. はじめに

MPEG-21等で今後のAVフレームワークにおけるセキュリティ・システムに対する要求条件の議論が活発になっている。MPEG-21「AV・フレームワークの標準化」は2000年5月に正式なISO/IECの国際標準化プロジェクトとして開始された。同様の標準化作業が他の標準化機関でも進行しており、大規模な高度AVサービスの総合的安全性に対する関心が高まっている。本論文では今後の高度なAVサービスにおける安全性に関する考察を行なう。

2. 高度AVサービス

本論文で対象とする高度なAVサービスとは、MPEG-21が想定しているようなブロードバンドネットワークベースの次世代のAVサービスである。AV符号化技術の進歩とプロセッサー性能の向上により、最高品質のAVコンテンツが個人のレベルで容易に複製、配布可能となった。しかし、AVコンテンツについて、現在のデジタルAV符号化の応用の多く(たとえばDVDやCD等)では、単純にアナログをデジタルに置き換えた形でシステムが実現されている。しかしデジタル方式は本来多くのアナログにない特長

[+] 早稲田大学 Waseda University/株式会社アスキー ASCII Corporation
http://www.shirai.info.waseda.ac.jp:8001/~itaru-k/

を有する。たとえば、複製、編集、伝送の劣化が無く、コンピュータとネットワークにより操作することで各段に高度な利用が可能である。インターネットではすでにこれらの特長を生かし、主にテキスト情報について従来は想像だにしなかった多様な応用が展開されている。AV コンテンツにおいても今後はデジタルの本質的メリットを生かした利用が拡大すると予想される。

このような技術革新は我々の知的活動の自由度と可能性を飛躍的に高め、社会全体の知的生産性を高める強力な道具となる。その反面、本来有償であるコンテンツが無償コンテンツの複製・再生ツールを用いて不正に利用される、いわゆる「違法コピー」、「不正使用」を助長し、利便性と権利保護をどう両立させるかという課題を提示している。

3. 符号化技術の進歩

高度 AV コンテンツの安全性を考える上で、将来のコンテンツの素材符号化技術の進歩、複合コンテンツ記述の進歩をある程度予想しておく必要がある。

3.1. 素材符号化技術の進歩

AV 素材のデジタル符号化は近年急速に高度化した。一例として MPEG-4 を挙げる。MPEG-4[1)2)]では、ビデオ、オーディオ、CG、テキスト、合成音など、今日考え得るほぼすべての素材符号化が集約され、また MPEG-4 には後で述べる複合コンテンツ記述の機能も合わせもっている。

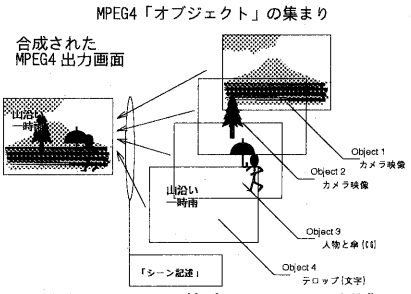

図1 MPEG-4 複合コンテンツ記述

図 1に、MPEG-4/SYSTEM(ISO/IEC 14496-1[3)]による複合コンテント記述の概念図を示す。MPEG4 では動画、静止画、音声、テキスト、CG、合成音などの素材=オブジェクトを、自在に 3D 空間+時間中の指定された位置に配置することが可能である。AV 同期やストリーム伝送は当然可能であり、またオブジェクトは任意形状で 2D あるいは 3D レンダリングされる。

これら素材符号化技術と複合コンテンツ記述の進歩により、コンテンツの利用が高度化、複雑化したことを反映して、必要な保護機能も高度化、複雑化すると考えられる。従って、高度 AV サービスに適したセキュリティ機能の整備が必要と考えられる。MPEG においてはこのような背景から、MPEG-4 において簡単ながら拡張性に富んだ MPEG-4/IPMP[4)5)]を標準に組込んだ。また 1999 年 12 月には新しい標準化プロジェクト、MPEG-21[6)]の標準化作業の開始を提案した。高度 AV サービスに適した総合的なセキュリティ・システムは他の多くの標準化機関でも検討されている。

4. 多面的安全性

本論文では AV コンテンツの安全性の一つの評価基準として、多面的安全性を提案する。

有償コンテンツから確実に対価を得ることを保証する技術として、コンテンツの条件再生、暗号化、電子すかし等、多様なセキュリティ技術がある。しかしこれらの多くが、これまではシステム運営者の意図に反する利用(たとえばコピー)を防止するというコンテキストのみで評価されることが多かった。そのため後で詳しく述べる他の安全性の側面について十分考察されることが少なかった。高度 AV サービスに多数の利害関係者がある以上、システム運営者の安全性同様、他の関係者の安全性も必要であることは言うまでもない。またコンテンツ保護技術の利用範囲が広がるにつれ、一方の安全性を満たす技術が、間接的に他の安全性を脅かす面が無視できなくなっている。

多面的安全性は、著作者、利用者、運営者、外部関係者の 4 つの主体と相互の安全性を考慮した安全性の評価する。そしてそのような安全性を高めるシステム構成についても評価基準を与えようとするものである。

現在提案、利用されているシステムの多くは暗号をその基本部分に用いている。暗号を利用したデジタルデータの配信は 1980 年代に活発に議論された。たとえば Purdy 等[7)]、Albert 等[8)]、森等[9)]、Herzberg 等[10)]によって基本的な構成やセキュリティに関する分析が示されている。森の方法は超流通(Superdistribution)の名で知られている[11)12)]。暗号を利用して複製や再生を制御する方式は、今日では多種提案され実施されている。これらは若干の構成上の違いはあるが、基本構成は 1980 年代当初に提案さ

れたものとよく似ている。

しかし、インターネットとコンピュータ性能の向上によりデジタルコンテンツが現実に広がりをみせる中で、安全性について新しい視点が持たれるようになった。本研究会(電子化知的財産社会基盤研究会)における多くの発表がある。また、名和[13]がデジタル時代の様々な課題を提示している。また、森[14]、井上[15]、O Connell[16]、Lipinski[18]等の論文が単純なコピー保護の範疇に収まらない安全性の必要性を示唆している。またプライバシーの問題は企業活動にとっても重要な課題となっている[17]。従って、今日セキュリティへの要求は極めて多面的になってきており、特に高度AVサービスではいくつかのこのサービス特有の安全性が重要であると思われる。以下では、そのいくつかを挙げる。

4.1. 不公正競争

高度AVサービスのシステムが不公正競争を助長することが危惧される。

ゲーム機のハードとソフトなど、同一方式のハードとソフトの組み合わでのみ利用できる商品では、ハードまたはソフトのどちらか一方で優位にあれば、他方の競争で優位に立てるという性質がある。企業が自社方式により競争上優位に立とうとすることは当然の行動であるが、恣意的に非互換性を導入し競争を排除することまでを認めるか、特にそれが産業育成面で寄与するかどうは議論が分かれる。

コンテンツ保護機構は技術的に単純で、同一機能であっても容易に独自の変種が設計できる。機能と無関係に安易にシステムを非互換とすることは、消費者にとって大きな不利益となるばかりか、本当に重要な性能面、機能面での競争を阻害する要因となり得る。

一方で、コンテンツの電子配布は今後多いに新しいビジネスモデルが創意工夫されるべき分野で、ビジネスモデルの急速な発展のためには、機能は固定化されるべきではない。従って、競争促進のための互換性維持と、新機能創出の自由度の両立が求められる。

4.2. 消費者機能

高度AVサービスでは、消費者が確実にサービスを受けるための機能が必要になると考えられる。通常の取引で消費者が保証されるべき機能としては以下のようなものがあるだろう。

(1) 支払いの証明
(2) 受けたサービス内容の証明
(3) 返金・補償の請求

これらは通常の消費に必須な機能で、どれ一つを欠いても問題がある。

高度AVサービスにおいては、従量課金や小額課金がより一般的になるといわれている。一方で微小な決済が大量に発生すると、消費者がこれまでの方法で請求や決済の正当性確認することが不可能になる。一方、市場規模が拡大すればたとえ1%の不正請求によっても莫大な詐欺が可能となる。有効な監視システムが欠如していれば巨額の詐欺事件の可能性もあり、大きな社会的リスクとなる。

4.3. 著作権者保護

AVサービスはコンテンツを主体としたサービスであることに特徴がある。コンテンツは他の商品と異なり物理的な実体を持たない。実体のある物の窃盗は最終的には露見せざるを得ないが、実体のないコンテンツの無許可利用は積極的に調査しなければ露見しない。たとえば、作者Aの作品を作者Bの作品と偽ってC出版者が出版しても、作者Aが調査しない限り作者Aが知ることにはならない。

多くの著作権侵害訴訟は、出版者、著作者など、同業者間で発生する。従って、このような著作権侵害に有効に対処できる方法がなければ著作権保護に有効なシステムとは言えない。

同業者間では、機械的な複製ではない模造(模倣)は容易であり、いわゆる電子的な保護機能でこれを防止することは出来ない。一方電子的な保護機能が、これらの模倣による著作権侵害の発見や効果的な補償請求を困難にし、これまでよりも著作権侵害が頻発する可能性もある。

4.4. プライバシー

コンテンツの消費はプライバシーを含んでいる。たとえばhttpプロトコルの通常の実装では特定のユーザーのweb画面操作をかなり詳細に記録できる。たとえば特定のページのどのメニューをクリックしたかを、そのクリックの日時分秒にまで詳細に調べることが可能である。特定の個人のここまで詳細な記録は、プライバシーに属する場合がある。

したがって、プライバシー保護が必要とされる用途では、これらの情報の有効な保護方法が必要となる。

4.5. 内部不良

Landwehr等はコンピュータシステムにおける過去の50例のセキュリティ不良を分析し、仕様策定時と設計時に導入された不良が37(74%)を占め、また意図的な不良が18例(36%)あることを報告している[19]。これらはシステム自体に内在する不良なので内部不良(internal flaw)と呼ぶことにする。内部不良はたと

えば Java のセキュリティホールの克服の例[20)21)22)]のように、第 3 者機関の協力を得て長い時間をかけて取り除かれる必要がある。

AV コンテンツの利用では、コンテンツの新しい利用方法や新しい符号化方法の導入に伴って、より頻繁に新しいセキュリティシステムが導入されるようになると予想される。したがって、より敏速に、確実に内部不良を検出する必要がある。

5. 多面的安全性の実現

5.1. 多面的安全性の提案の目的

以上述べたたように、高度 AV サービスには、多様な安全性が求められる。しかし、安全性に関する個々の要素の要・不要については必ずしも社会的なコンセンサスに至っていない。本論文は個々の安全性の要素の要、不要を論ずることが目的ではないため、そのような議論は行わないこととする。

しかし、これら新しい安全性に技術的にどのように対応が可能か、あるいは特定のシステム設計で、特定の機能と特定の安全性の関係はどうなっているか、という問いに、ある程度客観的に答える方法がほしい。このような問いに答えるのが本論文の目的である。

5.2. 基本モデル

多面的安全性を議論する前に、基本となる一面的安全性を確保したシステムとその安全性の評価方法を示す。Herzberg 等はセキュリティ機構と共にセキュリティの評価方法を示した[10)]。そこで、本論文では Herzberg の方法を基本に、それに対して多面的安全性を追加するためにはどのような追加的考慮が必要かを示す。

Herzberg はセキュリティの形式的分析のためにいくつかの仮定を明示している。通信路については以下を仮定している。

(1) 通信路は攻撃者により傍受、改竄され得る。
(2) 利用者にも攻撃者が含まれる。

またシステムに関しては以下を仮定している。

(1) CPU 内の秘密情報は読めない
(2) CPU 出力からソフトウエアを再生できない
(3) 暗号は安全
(4) 決済は別途確実に確認できる
(5) 鍵はランダムに生成される

Herzberg はこれらの仮定に基づいて、プロトコルに基づくシステムの状態の到達可能性という基準でプロトコルの安全性を議論している。このような評価方法は今日提案、利用されているシステムを分析する場合でも妥当と考えられる。

5.3. 多面的通信モデル

次に本論文が提案する多面的安全性モデルの定義を示す。Hertzberg は安全性の根源となる情報の提供管理者を想定し、Z としてその信頼性を前提条件としている。また CPU 等の安全性を補償するためのモジュールは完全であるとする。したがって、Hertzberg の安全性モデルは安全性の提供者とその利用者の 1 面的関係になっている。

すでに述べたように、完全に信頼できる管理機関は存在しないし、また利用者は利用しているシステムを完全には信頼できない状況に置かれている。多面的安全性モデルでは、これらの不確定要因を取り入れたモデルを目的としている。そこで信頼性のモデルとしてシステム提供者とそのユーザーという 2 者ではなくシステムに関与する表 1に示す 4 者を仮定する。

表1 システムに関与する 4 者

記号	意味	説明
p	コンテンツ提供者	コンテンツの提供者
u	利用者	コンテンツの利用者
s	システム運用者	システム、サービスの提供者
e	外部機関	外部にいて運用に利害関係を持っている機関

ここで「外部機関」とは、システムに通常直接関与はしていないが、利害を持っている機関とする。たとえば、国税庁は正確な収入と支払いの記録が参照できるか否かに重大な関心を持つだろう。

図2 uni-lateral model

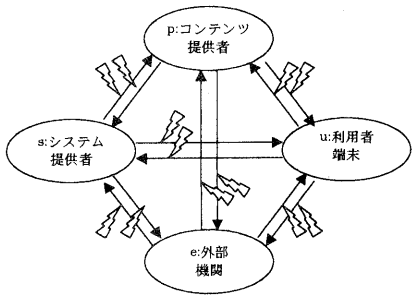

図3 multi lateral model

従来モデルとの差を示すと以下のようになる。従来モデル、たとえばHerzbergのモデルで考慮されるのは、基本的にはシステムが完成した後のプロトコルへの攻撃の脅威だけである。すなわち、システムからみて各利用者が信用できるかが考慮の対象である。これを図示すると図2のようになる。図中で楕円は信頼性を代表するentityを表し、線は信頼性を、稲妻型は信頼性に対する攻撃をあらわす。

多面的モデルでは、以上4つのentityを仮定し、すべての相互信頼性に脅威が存在すると仮定する。これを図示すると、図3のようになる。4つのentity間のすべての信頼関係が攻撃される。

5.4. セキュリティ機能の分類

次に、各entity間のセキュリティ機能と交換されるメッセージを仮定する。表2にセキュリティ機能を、表3にメッセージを示す。

表2 セキュリティ機能

式	機能	説明
C(t,x,y)	通信	xの通信文tをyだけが受信できる
A(t,x,y)	署名	xが発信したテキストtの内容を確かに発信したとyが証明できる
N(t,x,y,z)	公証	xがyにテキストtを発信したことをzが証明できる。
P(t,x,y)	保護	xがyに通信した内容をyは保管できるが読み出せない。

表3 メッセージ種別

記号	内容	目的
a	CSM(クライアントセキュリティーモジュール)	クライアントプログラムのセキュリティー関連部分
c	コンテンツ	消費されるAVコンテンツ
o	注文	AVコンテンツの注文
p	決済	代金の決済等の情報
d	契約	AVコンテンツの内容と利用条件を示す、取引条件

5.5. デコーダに関する仮定

Herzburgのモデルでは、デコーダは正当なものという仮定があった。すなわち内部不良な存在しないと仮定している。

内部不良をどう扱うかには様々な方法がある。システムの構造を予め詳しく分析し、内部不良が存在しないことを証明し、以後の分析では内部不良が無いと仮定することも一つの方法である。

しかし、システムの内部安全性の評価方法はシステムの構造に依存し、一般的な評価方法がない。また内部不良は少なくとも仕様段階で意図されるものではなく、実施にいたる仮定で何らかの錯誤または攻撃的な意図、あるいはそれらの組み合わせにより発生するものである。Landwehrの報告によれば、内部不良の多くが実装時の錯誤または作為によるものである。従って内部不良が無いシステムを仮定することは現実的ではない。

多面的安全性モデルでは、システムの各利用者が利用するクライアントプログラムのセキュリティ、CSM(クライアントセキュリティモジュール)を、伝達されるメッセージの一つと位置付ける。CSMの設計時や伝送時の作為的、非作為的な瑕疵や改竄は、このCSMの伝送に対する改竄と等価である。そこで多面的安全性モデルにおいてはCSMを伝達されるメッセージの一部と位置付けることで、これらのCSMの内部不良をモデル化する。

5.6. 比較

1面的安全性のモデルと多面的安全性のモデルの比較を示す。

表4 従来モデルとの比較

	従来(1面的)モデル	多面的モデル
通信	2点間の通信	4点間の通信
セキュリティ	通信、署名、格納	通信、署名、格納、公証
メッセージ	コンテンツ	クライアントシステム、コンテンツ、決済、契約
攻撃者	ユーザー	ユーザー、コンテンツ提供者、システム提供者、外部機関
被攻撃者	システム提供者	ユーザー、コンテンツ提供者、システム提供者、外部機関、

6. 具体例

次に具体的なシステム構成を例としてとりあげ、一面的安全性と多面的安全性を比較する。

図4のような暗号化配信機能を考える。ごく一般的なものなので細かい説明は省く。基本的には配信は暗号化された状態で行ない、使用許可と同時に解読が可能となるように全体システムを制御するものとする。

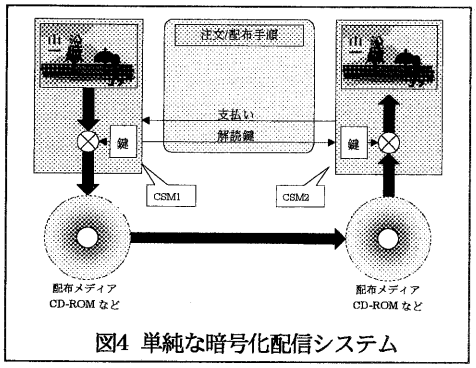

図4 単純な暗号化配信システム

Herzburg の分析では、このような全体システムのプロトコルは図 5のようになる。

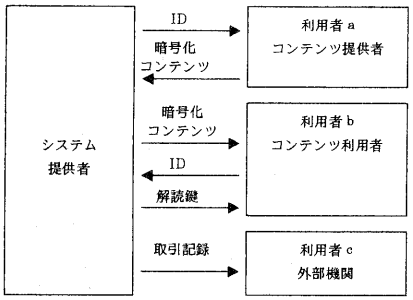

図5 uni-lateral protocol

CSM が完全であると仮定できれば、Herzburg の分析によってもプロトコルはほぼ完全であり、コンテンツの安全性等が保証される。プライバシー等については Herzburg のモデルは完全ではないが、その後も様々な拡張プロトコルが提案されており、それらの拡張で対応が可能と考えられる。

しかし、このモデルでは基本的にシステム提供者や CSM の信頼性は前提であり、評価できない。現実にはすでに述べたようにシステムの安全性が損なわれたり、コンテンツ提供者や利用者が CSM を完全に信頼できない事例が多い。システムの信頼性は CSM の信頼性にかかっていると思われる。従来モデルによるプロトコルの分析だけではそのような不安は解消されない。

これに対して、多面的安全性では CSM も伝送されるメッセージとして扱うことを提案する。従ってプロトコルは図 6のようになる。このようなプロトコルを仮定すれば、安全性の分析手法そのものについては Herzburg の方法を踏襲できる。

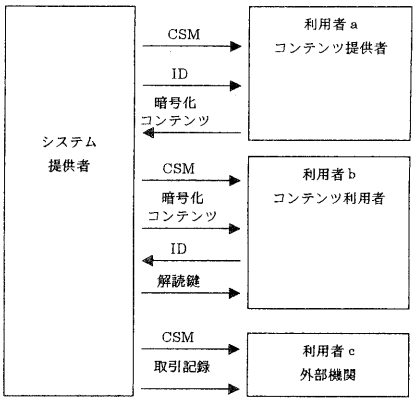

図6 multi-lateral protocol

このように、CSM が不完全である可能性も考慮にいれ、かつ安全であるという合理的な説明ができれば、利用者は安全性を確信できるだろう。

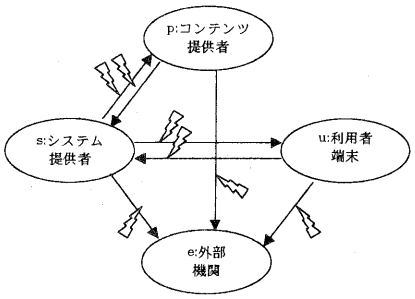

図7 multi lateral protocol

図 7に多面的安全性モデルによる信頼関係図を示す。先に示したように p,n,e が利用する CSM 自体もシステム提供者が発するメッセージの一部である。このモデルにより、システム提供者が提供するシステムの不完全性をモデル化できる。

7. MPEG における関連する標準化

7.1. CfP on solution for MPEG-4/IPMP

7 月 21 日に、MPEG は IPMP の解決方法を求める Call for Proposal(CfP)[23]の発行を承認した。この CfP は 2 年前に標準化した MPEG-4/IPMP フックを利用してコンテンツ配信を実現する場合に現在問題となっている相互運用性の問題を解決する方法を求めるものである。CfP で規定されている要求項目を表 5 に示す。

7.2. MPEG-21 Technical Report

MPEG-21 ではセキュリティーに限定せず高度 AV

フレームワーク全般についての調査と標準化を行なう。まず高度 AV フレームワーク全体の調査分析を行ない、その後 MPEG で標準化すべき内容を選別していく予定である。第 1 段階の調査結果をまとめたテクニカルレポート案(PDTR)[24]が 7 月 22 日に作成された。PDTR は各国 NB や外部の専門家のレビューを受け、修正されて正式版となると並行して、AV フレームワーク分野における今後の MPEG 標準化の指針となる。AV 圧縮以外の技術分野も重要な要素となっており、これまで MPEG 標準と関係がなかった専門家の協力も重要である。

8. まとめ

本論文では、前半では高度 AV サービスの安全性について議論し、単純なコピー防止以外の多面的な安全性への関心が高まっている事を示した。後半では多面的安全性を実現し、評価する方法を示した。簡単な例によって、多面的安全性が満たされないシステムと、多面的安全性を満たすための改良方法を示した。

冒頭で述べたように、ISO/IEC では MPEG-21 と題して AV・フレームワークの標準化作業を開始している。MPEG-21 を始めとして高度 AV サービスに関連した業界規格、標準化の動きは近年特に急速に進んでいるが、コンテンツ配信の安全性の目標は必ずしも明確ではない。標準化という手続きの中では多種多様なリスクと防止コストの現実的なバランスを、客観的に表現することが重要ではないかと考える。

また、本論文では多面的安全性の評価方法に留まり、具体的な解決手法は例示ができなかったが、今後は前期 CfP への応募等の中で具体的な手法を提案していく予定である。

謝辞:本研究を進めるにあたり、勤務先のアスキー及び早稲田大学白井研究室の多くの方々にご支援を頂いた。謹んで感謝の意を表したい。

参考文献

1) ISO/IEC, "ISO/IEC 14496-1-3", ISO/IEC 2000
2) 金子格 :「MPEG4 の最新動向」アスキー;OpenNetwork 1997 年 6 月号(要約: http://www.mpeg.rcast.u-tokyo.ac.jp/openmpeg/mpeg4/index.htm/)
3) ISO/IEC, "ISO/IEC 14496-1(2000) (通称 MPEG-4/システム)", ISO/IEC(2000)
4) MPEG N2614 公開文書 IPMP 概要 http://www.cselt.it/mpeg/public/w2614.zip
5) 金子 格、工藤育男、「MPEG-4 における著作権識別管理の標準化動向について」情報処理学会 研究報告 98-EIP-1 pp.75-82
6) MPEG: "MPEG-21 workshop", http://www.cselt.it/mpeg/events/mpeg-21/(2000)
7) G. B. Purdy, G. J. Simmons and H. A. Studier : "A software protection scheme", Proc. of the Symp. on Security and Privacy, pp. 99-103 IEEE(1982)
8) D. J. Albert and S. P. Morse : "Combatting softwre piracy by encryption and key management", IEEE Computer, 17, 4, pp.68-73(Apr. 1984)
9) 森、田代、"ソフトウエア・サービス・システム(SSS)の提案", 電子通信学会論文誌,Vol.J70-D,No.1, pp.70-81,(1987)
10) Amir Herzberg and Shlomit S. Pinter, "Public Protection of Software", ACM Trans. Computer Systems, Vol. 5, November 1987,pp371
11) Brad Cox, Superdistribution,Objects as Property on the Electronic Frontier, Addison-Wesley 1996
12) Ryoich Mori and Masaji Kawahara "Superdistribution: An Electronic Infrastructure for the Economy of the Future" 情報処理学会論文誌 Vol38 No7 July 1997
13) 名和小太郎: デジタル・ミレニアムの到来,丸善,丸善ライブラリー291(1999)
14) 森亮一:「ディジタル情報の無証拠性とその影響-非関所型防御の必要性-」情報処理学会 電子化知的財産社会基盤研究グループ 1-5(1997/6/7)
15) 井上明、橋本誠志、金田重朗、"個人データ流通における保護システムのあり方",電子化知的財産・社会基盤 4-8
16) Brian M. O Connell, "Private Creation of Internet "Law"", IEEE Technology and Society magazine, Spring 1999
17) Tomas. A. Lipinski,"Information Warfare, American Style", IEEE Technology and Society Magazine, Spring 1999
18) マイクロソフト: "マイクロソフトのプライバシーに関する取り組み", http://www.microsoft.com/japan/win98/security/custletter2.htm(1999)
19) Carl E. Landwehr, Alan R. Bull, John P. Mcdermott, And William S. Choi,"A Taxonomy of Computer Program Security Flaws", ACM Computing Surveys. Vol 26, No. 3, September 1994
20) Gary McGraw, Edward Felten, "Java Security", John Wiley and Sons, 1997
21) CERT, "Ca-96.05:Java security manager", CERT Ca, Carnegie Mellon University, 1996
22) CERT, "Ca-96.07:Java security bytecode verifier", CERT Ca, Carnegie Mellon University, 1996
23) MPEG," Call for Proposals for IPMP Solutions",MPEG/N3543,http://www.cselt.it/mpeg/
24) MPEG, " MPEG-21 Multimedia Framework PDTR", MPEG/N3500, http://www.cselt.it/mpeg/

表 5 MPEG/IPMP 要求項目

#	要求項目	原文
1	最小のハードウエアで、コンテンツの再生、複製、編集、創作が可能であること。	The solution shall support access to and interaction with content while keeping the amount of hardware to a minimum. There shall be no duplication of similar devices to interact with similar content from different sources. To a lesser extent, the same applies to software. Examples of interaction with content are playback, copy, edit, create and so forth.
2	アダプタの着脱などが煩雑でないこと。	The solution shall support easy interaction with content from different sources without swapping of physical modules; that is without requiring action on the part of the end user. Addition of modules is acceptable if it requires a one-time action, if the device supports it, and if the cost is reasonable.
3	コンテンツの使用許諾範囲が利用者に明確に伝わること。	The solution shall support conveying to end users which conditions apply to what types of interaction with the content. An example is payment for playback.
4	利用者のプライバシーが守られること。	The solution shall support protection of user privacy. *Note: In many countries legislation requires that no user information shall be disclosed without the explicit consent of the end user.*
5	利用者 ID が公開しないですむサービスも可能なこと。	The solution shall support service models in which the end user's identity is not disclosed to the service/content provider and/or to other parties.
6	プロバイダーが営業停止した場合等に利用者の権利が保全されること。	The solution shall support the preservation of user rights. *Notes: For instance, the solution shall support preservation of user rights in such events as the provider going out of business. It is believed that an important requirement of end users is that their rights to interact with the content not be revoked for alleged misuse when the burden of disproving misuse is entirely on the end user. However, MPEG does not currently see any implications for these requirements.*
7	OS のクラッシュやバッテリーの放電などで権利が失われないこと。	The solution shall support the content and the end user's rights to interact with it to survive common accidents, e.g. an operating system crash, or a flat battery.
8	端末を移動しても利用できること。	The solution shall support MPEG-4 terminal mobility, e.g. end users should be able to use the same device in different locations.
9	コンテンツを端末間で移動できること。	The solution shall support content mobility across MPEG-4 terminals, e.g. end users should be able to move to a different terminal and keep their rights to interact with the content. *Note:Assuming easy access to the content, this mainly applies to the portability of the rights to interact with it.*
10	ハードやソフトの新しいバージョンに対応できること。	The solution shall support content and the end user's rights to interact with it to survive changing to a new version of similar hardware or software. *Note: Assuming easy access to the content, this mainly applies to the renewability of the rights to interact with it.*
11	異なる MPEG-4 ハードに対応できること。	The solution shall support content and the end user's rights to interact with it to survive changing to a different type of MPEG-4 hardware. *Note: Assuming easy access to the content, this mainly applies to the survivability the rights to interact with it.*
12	一時的、恒久的に、コンテンツやその権利を移転できること。	The solution shall support transferring, temporarily or permanently, content and the rights to interact with it to another party.
13	コンテンツ保有者が知財権利の管理が可能なこと。	The solution shall enable content owners to control which of their assets are available when, where and under what conditions.
14	セキュリティが長期間保たれ、かつ更新が可能なこと。	The solution shall support persistent security over time and renewability of that security.
15	新しいビジネスモデルに対応できること。	The solution shall support the flexible expression of different business models/rules, which might yet be unknown and which may change over time, markets and geography. *Note: Some business models are envisaged to involve 'super distribution', in which content and rights to interact with it are passed along from one user to another.*
16	権利者が権利運用方法を変更できること。	The solution shall enable content owners to change business rules whenever and however they wish.
17	低コストで実装可能であること。	The solution shall support implementations that are cost effective with regard to the value of the content to be managed and protected.
18	短期間で開発可能であること。	The solution shall support fast development of products and services.
19	それを実装した装置の(商品)寿命が長いこと。	The solution shall support implementations into devices that have a long life cycle, i.e. at least five years.
20	現在存在する技術で実現できること。	Implementation of the solution shall be based on currently available technology.
21	政治的判断を限定しないこと。	The solution shall not impose policies. *Note: Imposing policies is the legitimate domain of content, service and application providers, and governments.*