コンピュータセキュリティ　9－3
（2000．5．10）

高度AVサービスの多面的安全性とその実現

金子 格+

［要旨］本論文では高度AVサービスにおける多面的安全性について考察する。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サービスにおいて、不正競争の激化、プライバシー、組織犯罪、情報化による二極化(IT divide)なども関心を集めている。本論文では、まずこれらの問題をセキュリティ設計の問題としてどう捉え得るかという考察を行う。次に、多面的安全性のモデルを提案する。多面的安全性モデルを用いると、様々な安全性と、相互のバランスをモデル化することが可能である。

Multi-lateral security and it's implementation on Advanced Audio Visual Services

Itaru Kaneko+

Abstract:.
In this paper, multi-lateral security of content distribution system is discussed. While Advanced Audio-Visual Services, as a combination of Digital Audio-Visual coding, hyper-media coding and network distribution, are evolving, various issues such as privacy violation, crime increase and IT divide are also drawing broad interest. In this paper, firstly we will consider how to treat these problem or requirement as a design requirement of security system. And secondly we propose multilateral security model. Multilateral security model can be used to consider various kind of security and balance of different kind of security.

1. はじめに

本論文は高度AVサービスにおけるセキュリティ・システムにおける多面的安全性とその実現について考察する。

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。今日、AVコンテンツは個人でも簡単に作成でき、ネットワークを通じて全世界に配信可能である。家庭用機器を使っても商業的な大量複製と大差ないコストで複製及び配布が可能である。このような技術進歩は個人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った。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することになった。

このような状況の中で高度AVサービスのセキュリティ技術への注目が増している。たとえば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

+ 早稲田大学 Waseda University
http://www.shirai.info.waseda.ac.jp:8001/~itaru-k/

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その他の安全性ついて、総合的に考察されることが少なかった。

各々の立場から見た安全性は必ずしも一面的な保護と両立しない。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。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。

また、現在(2000年4月時点)ISO/IEC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。その他にも高度AVサービスに関連した業界規格、標準化の動きは近年急速に進んでおり、大規模な高度AVサービスの総合的安全性に関する議論は急務である。

本論文では多面的安全性として、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論ずる。そしてシステムにおけるこれらの安全性を総合的に評価するモデルについて考察する。

2. 符号化技術の進歩

コンテンツの安全性への関心が高まっている背景には、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がある。

2.1. 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。

AV素材には、画像、オーディオ、静止画、CGなどがある。これら異なる種類の素材のデジタル符号化には、様々な異なる符号化方法が使われる。これら素材ごとの符号化を、ここでは素材符号化と呼ぶ。

素材符号化は近年急速に進歩した。動画像・音声についてはMPEG符号化方式が、広く使われている。文字、図形についてはVRML, XMLが広く使われている。

同一タイプの素材に対しても、いくつかの異なる符号化方式が存在する。たとえばオーディオ符号化にはMPEG, AC3, AD-PCM,AACなど様々な方法があり、それぞれ広く使われている。

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ている。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。

これらの素材符号化技術が急速に高度化した結果、素材のデジタル化、ネットワーク配布が急速に進んだ。

2.2. 複合コンテンツ記述の進歩

一方いわゆる復号コンテンツ記述も急速に高度化した。

ゲーム機やパソコンなどによるAV再生では、画像、音声、文字、図形など素材符号化されたオブジェクトを複数組み合わせて提示する事ができる。

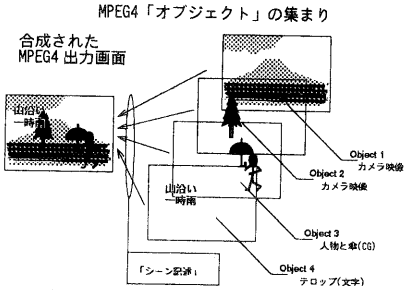

図1 MPEG-4複合コンテンツ記述

たとえば、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。同期やリアルタイム再生は当然可能であり、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。

MHEG、HTML、XML、SMIL、Java、ECMA-Scriptなどは、いずれも複合コンテント記述に利用でき、実際的にはその能力に大きな差はない。たとえばXML+SMILによる記述をMPEG-4に変換することも可能である。

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。たとえばMPEGにおいてはこのような背景から、MPEG-4において簡単な機構ながら将来かなり自由にセキュリティ機構を組込める構造である 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・システムは多くの関連機関で検討されている。

3. 多面的安全性

デジタルデータの配信は、暗号や電子透かしを利用したセキュリティ機能も含め古くから議論されてきた[7][8][9]。その基本的なアイデアに今も変わりはないが、インターネットとコンピュータ性能の向上により現実のシステムとして広がりをみせる中で、安全性についてもより細かな点にも配慮が求められるようになった。たとえば名和[10]がデジタル時代の様々な課題を提示しているほか、森[11]、井上[12]、O Connell[13]、Lipinski[15]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た[14]。その結果、要求項目は極めて多面的になってきている。高度AVサービスではさらに多面的な安全性が求められるだろう。本論文では紙数の制約もあるのですべてを列挙しないが、そのいくつかを挙げる。

3.1. 不公正競争

高度AVサービスのコンテンツ保護機構が不公正競争を助長することが考えられる。

元々ゲーム機器など、装置開発とソフトウエア販売が密接に結びついた事業では、価格操作等の不公正競争が発生しやすい。コンテンツ保護機構は技術的に単純で、だれでも容易に独自の方式が設計できる。またコンテンツ・ビジネスの事業者が、顧客囲い込みの手段として保護機能を非互換にする事も可能である。非互換により消費者のサービス選択が制約されれば不公正競争が助長されやすい。

デジタル放送など、近い将来実現する大規模なサービスにおいて、サービス選択の自由が制約されることは、業界および行政のほぼ共通認識として望ましくないと考えられていると思われる。たとえばテレビの条件視聴方式において、米国と欧州は条件アクセスモジュールのインターフェースを規定も日本の放送行政でも、条件試聴部分を交換可能とし、デコーダ本体はすべての条件試聴方式に対応し得ることを方針とした。

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構造が創意工夫されるべき分野であり、コンテンツ再生方法や保護方法をあまり厳密に固定してしまうことは、産業育成の面からはデメリットが大きい。また先に述べたような部分的な仕様の共通化が、セキュリティー・ホールとなるという指摘もある。

3.2. 消費者機能

消費者も様々な機能を必要とする。

(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ことは明らかだ。

例えば小額決済システム設計でも、運用者側が運用者の記録に基づいて料金を徴収できることだけでは不充分だろう。1日10000回の小額決済に含まれる、1%の請求誤りを消費者が従来通りチェックすることは困難だ。しかし有効なチェックがなければ、過去に銀行オンラインシステムで見られたように、ごく小額の不正請求であっても大量の決済に適用すれば巨額の詐欺が可能である。

3.3. 著作権者保護

運用者の安全性は著作権の保護と同義ではないことにも注意が必要である。これまでほとんどの著作権侵害訴訟は、出版者、著作者など、同業者間で起こっている。実際、ほんの十数年以前、個人によるコピーが困難だった時代には、著作権侵害といえば同業者による侵害のことだった。個人コピーが爆発的に増加する中で個人コピーにのみ注目が集まりがちだが、今日においても同業者間の著作権侵害が深刻な問題であることに変わりはない。

同業者にとっては、機械的な複製ではない模造(模倣)は容易なので、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てし、著作者の権利が著しく侵害される可能性もある。

また書籍出版者にとってコンテンツの消費者価格を指定できることは重要な権利である。デジタル・コンテンツ配布において、実質的な値引きが可能であれば、これも著作権の権利を侵すことになる。

4. 多面的安全性の実現

4.1. 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、これまでの単純なサービスよりも多面的な安全性が求められると考えられる。しかし、個々の要求項目の要・不要については必ずしも一定した見解がない。本論文は個々の要求項目の要、不要を論ずることが目的ではないため、本論文ではそれらは議論しない。

しかし、どのような安全性がどの程度の費用でどの程度効果的に実現するか、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多面的安全性モデルの目的である。

4.2. 4者間の関係

多面的安全性モデルでは、システム内、システム外という2者関係ではなく、3者以上の多数の関係者を想定する。たとえば表1に示す4者は異なる利害を持つシステムの関係者である。

表1 4種類の関係者

記号	意味	説明
a	素材提供者	素材を提供した主体
u	利用者	コンテンツを利用する主体
s	システム運用者	システムを運用している主体
e	外部関係者	外部にいて運用に利害関係を持っている主体

ここで「外部関係者」とは、システムに通常直接関与はしていないが、利害を持っている関係者であるとする。たとえば、国税庁は販売記録の正確さに重大な関心を持っていると想像される。表1の4者は、図2に示すように相互に関係を持っている。

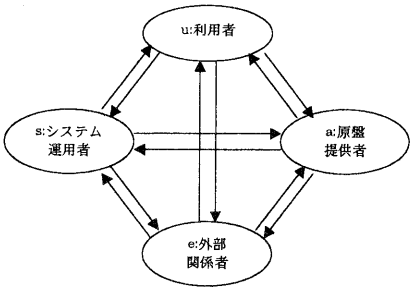

図2 4者間の相互関係

4.3. セキュリティ機能の分類

次に、それぞれの関係者間の通信に関するセキュリティ機能を分類する。たとえば表2に示すようにセキュリティ機能を分類する。

表2 セキュリティ機能

式	機能	説明
S(t,x,y)	秘話	xからyへのテキストtの通信を他が傍受できない
M(t,x,y,z)	傍受	xからyへのテキストtの秘話をzが傍受できる
A(t,x,y)	認証	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に発信テキストtのしたことをzが証明できる。
H(t,x,y)	隠蔽保管	xがyからtを隠蔽した状態で保管する。

4.4. メッセージ

4者間で通信される内容(テキスト)を分類する。たとえば表3に示す4種類のメッセージに分類する。

表3 メッセージ種別

記号	内容	目的
c	コンテンツ	消費されるAVコンテンツ
o	注文	AVコンテンツの消費を注文する信号
p	支払い	AVコンテンツの消費代金の支払い信号
d	契約条件	AVコンテンツの内容と消費代金等の取引条件を示した情報

4.5. 攻撃手順

具体的な攻撃手順を想定する。攻撃者はユーザーとは限らず、4者間のどの主体でもありえる。特定の主体が、上記セキュリティ機能を迂回あるいは無効化して、メッセージを盗聴、改竄等して、利益を得られれば攻撃は成功したと解釈する。

攻撃手順には、いくつかのセキュリティ機能の無効化が含まれる。攻撃手順ごとに、無効化が必要となるセキュリティ機能を調べ、その成功率や無効化に必要な初期コストを算定し、攻撃手順の特徴量とする。また、攻撃手順には、いくつかのセキュリティ機能により検出される危険要因が含まれる。攻撃が検出される確率も、攻撃手順の特徴量に含める。

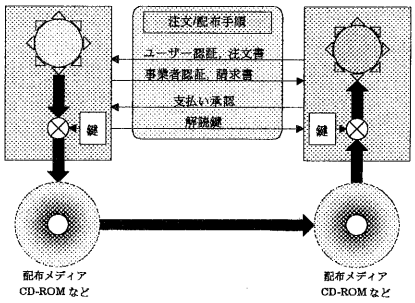

図3 単純な暗号化配信システム

たとえば、図3のような暗号化暗号化配信機能を考える。ごく一般的なものなので説明を省くが、基本的には使われている暗号を解読することができれば、コンテンツを受信できるとする。その場合、暗号を破ることによるコンテンツの解読という攻撃に関係するセキュリティ機能は、式1で表される。

$$S(c,s,u) \qquad \text{式1}$$

すなわち、システムがユーザーに、暗号化されたコンテンツを送る場合の安全さに依存している。

関係するセキュリティ機能の性能が、セキュリティを破るための初期コスト等の根拠となる。

4.6. 攻撃手順の特性分析

ある攻撃手順が脅威か否かを判定するために、まず攻撃手順を特徴付ける特徴量を評価する。たとえば表 4のような特徴量を評価する。

表4 攻撃手順の特徴量

記号	意味	説明
L	試行の上限	攻撃手順実行回数の上限
R	成功確率	セキュリティの無効化成功率
r	検出確率	その攻撃手順を検出する確率
G	成功報酬	成功した場合の利益
p	罰則	攻撃手順が検出された場合の罰則
I	初期コスト	セキュリティ無効化の初期コスト

4.7. 攻撃手順の損益計算

攻撃手順が危険かどうかは、攻撃手順により期待される総利益で判断する。表 4に示した特徴量が与えられた場合、総利益は式 2で与えられる。

$$P = N\frac{G}{R} - I - (1-(1-r)^N)p \qquad \text{式2}$$

ここで N は攻撃手順の試行の回数である。

通常、行為の期待値が負であれば、平均的には損な行動であるからそのような行動は合理的人間はとらないと仮定する。従って、式 2が正か負かが安全性を判断する一つの基準になる。

5. 多面的安全性による評価

本章では、多面的安全性を実際に評価してみる。

5.1. セキュリティ・システムの例

評価対象の例として、ある遊戯システムを考える。遊戯システムの設置者=運営者は直接売上金額を受領せず、売上等は電子的に課金、決済されて、電子的な利用記録(注文データ)に基づいて運営者のリベートだけが運営者に支払われるとする。1 回の売上は 1000 円とし、運営者は、売上の 10%のリベートを得られるとする。ほぼ完全な暗号を使った認証により、表 5 のセキュリティ機能が実現されていたとする。

表5 セキュリティの実装例

内容	通信	目的
コンテンツ	S(c,s,u)	許可された利用以外の利用を防止する
注文	A(o,u,s)	注文があったことを証明する

5.2. 損益分析

システムでは、運営者は注文に応じてリベートを得ることができるので、架空の注文を作り上げれば 1000 円の 10%である 100 円の利益が上げられる。

そこで架空の注文という攻撃手順の特徴量を求める。このシステムのセキュリティ機能は架空の注文に対して無力なので、架空の注文という攻撃手順の特徴量は表 6のようになる。

表6 特徴量(1)

変数	意味	説明
L	試行の上限	5000～100,000
R	成功確率	1.0
r	検出確率	0.0
G	成功報酬	100
p	罰則	0
I	初期コスト	1,000,00

この場合、N=10,000 で P>0 となる。N の上限が 5000～100,000 であるが L が 10,000 を超えると、このシステムは危険であるという結論になる。

5.3. 回避方法

このシステムを安全とするためには、架空注文のチェック機能と罰則を設ければよい。外部審査機関を用意することで、表 7のように特徴量を変更できたとする。

表7 特徴量(2)

変数	意味	説明
L	試行の上限	5000～100,000
R	成功確率	1.0
r	検出確率	0.0001
G	成功報酬	100
p	罰則	10,000,000
I	初期コスト	100,000

この場合、P>0 となることはない。従って合理的な人間であればこのシステムを攻撃することはない。

6. 多面的安全性の一般的特性

多面的安全性を評価した場合、システムの安全性にはいくつか一般的特性がある。

まず完全なプロテクションは存在しない。多面的安全性では、「完全な運用者」を仮定しないため、常に有限の内部漏洩リスクを仮定する。絶対的に安全なシステムはなく、相対的に安全か危険かという違いがあるだけである。

すべての攻撃手順について、一定の初期コスト I があるため、L が小さいうちは I による抑制が働き、安全である。L が大きくなれば必ず I による抑制が失われる点がある。大規模システムでは L を一定以下にする構造と、攻撃の検出手段が重要である。

大きな N に対する抑制は、外部審査機関による検査が有効である。しかし、外部審査機関が多用される場合には、その信用についても議論が必要となる。

多面的安全性の分析は、多くの攻撃手順についての分析を行わなければならないために、実際には非常に複雑な分析となる。これは手法の欠点ではなくて、もともとセキュリティという課題が持つ特徴である。現実のシステムのいわゆるセキュリティ・ホールは、システムが多数の専門家にレビューされ、様々な可能性が検討されて、始めて判明する事例が多い。たとえば Java についても、そのような検討、新たな問題点の発見、そして対策という作業を現在も続けている[16][17][18]。従って、多面的安全性を評価するにはある程度標準化され、外部の審査を受けたシステムである必要がある。

7. 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、本論文では複雑な場合の多面的安全性の例示ができなかったが、今後は前半で述べたような要求項目についても、具体的な安全性評価を試みていく予定である。

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。

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) 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)
8) Brad Cox, Superdistribution,Objects as Property on the Electronic Frontier, Addison-Wesley 1996
9) 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
10) 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)
11) 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)
12) 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
13) Brian M. O Connell, "Private Creation of Internet "Law"", IEEE Technology and Society magazine, Spring 1999
14) Tomas. A. Lipinski,"Information Warfare, American Style", IEEE Technology and Society Magazine, Spring 1999
15) 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)
16) Gary McGraw, Edward Felten, "Java Security", John Wiley and Sons, 1997
17) CERT, "Ca-96.05:Java security manager", CERT Ca, Carnegie Mellon University, 1996
18) CERT, "Ca-96.07:Java security bytecode verifier", CERT Ca, Carnegie Mellon University, 1996