高度デジタル AV フレームワークの多面的安全性とその特性

金子 格[†] 白井克彦[†]

MPEG-21 などをはじめとして，AV コンテンツ利用環境のデジタル化とネットワーク化を前提とした高度デジタル AV フレームワークが検討されるようになった．その中では，不公正競争の助長，プライバシー保護，組織犯罪防止など，小規模の個別応用で意識されなかった課題も，大規模広域利用のために意識されるようになった．本論文では，これらの課題を，標準規格策定などの設計仕様にどう対応させるか，という考察を行う．次に，多面的安全性のモデルによりそのような対応付けを行うことを提案する．

Multi-lateral Security and It's Characteristics on Advanced Digital Audio Visual Framework

Itaru Kaneko[†] and Katsuhiko Shirai[†]

Advanced Digital Audio Visual Framework, as a combination of Digital Audio-Visual coding and hyper-media coding, is being discussed in many standardization organization such as MPEG-21. Issues, such as anti-trust law violation, privacy and organized crime are increasingly drawing interest because of expected large-scale global use of the framework. In this paper, we will consider the procedure to translate high level requirement into low level design criteria. Then we will propose multi-lateral security for such translation.

1. はじめに

本論文は高度デジタル AV フレームワークにおける多面的安全性とその特性について考察する．

デジタル符号化技術の進歩とプロセッサー性能の向上により，個人でも AV コンテンツが簡単に編集，作成でき，またネットワークを通じて全世界に配信可能な，高度なデジタル AV 配信・利用環境が実現した．本論文ではそれらを高度デジタル AV フレームワークと呼ぶ．

このような技術進歩は創作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．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「不正コピー」,「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．

そのため，セキュリティ技術への注目も増している．たとえば有償 AV コンテンツから確実に対価を得ることを補助する技術として，AV コンテンツの条件再生，暗号化，電子透かしなど，多様なセキュリティ技術がある．しかし，これまでこれらの多くは，たとえば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，一方の安全性のみを評価されることが多く，他者の安全性を総合的に考察することが少なかった．

一方の立場の安全性は必ずしも他者の安全性と同一ではない．AV コンテンツの利用に多数の利害関係者が存在する以上，他者の安全性に対する配慮も必要であることはいうまでもない．セキュリティ技術の利用が広がるにつれ，一方の安全性を確保する技術が，他者の安全性を脅かす傾向がある．

また，これら AV ネットワーク配信の総合的なフレームワークへの関心の高まりから，ISO/IEC MPEG 委員会は 1999 年 12 月に Digital Audio Visual Framework（通称 MPEG-21）国際標準化を提案した．その他の業界規格，標準化の動きも活発で，大規模な高度デジタル AV フレームワークの安全性に関する検討は急務である．

本論文では多面的安全性として，著作者，利用者，運営者，外部関係者といった 3 者以上の利害関係者相互の安全性を多面的に扱うことを提案する．そして標準化などのシステム検討においてこれらの安全性を設

† 早稲田大学
Waseda University

計仕様に対応付ける手順についても提案する．

2. 高度デジタル AV フレームワークの進歩

高度デジタル AV フレームワークでセキュリティが重要と考える理由は，今後さらに素材符号化技術の進歩，複合 AV 記述の進歩が予想されるためである．

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．文書，図形については VRML や XML などが広く使われている．

2000 年に国際標準として出版された MPEG-4[1),2)] ではさらに高度な符号化が可能である，ビデオ，オーディオ，CG，テキスト，合成音など，今日考えう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 AV 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今後も急速に進むと考えられる．

2.2 複合 AV 記述の進歩

一方いわゆる複合 AV 記述も急速に高度化している．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ことができる．これらをここでは複合 AV 記述と呼ぶことにする．

たとえば，**図 1** に，MPEG-4/SYSTEM（ISO/IEC 14496-1）[3)] による複合 AV 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，シーン記述により自在に 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．

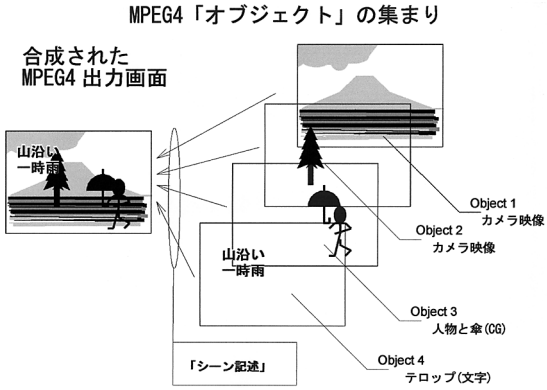

図 1 MPEG-4 複合 AV 記述
Fig. 1 A MPEG-4 Audio Visual Composition.

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．

2.3 セキュリティ要求の高度化

これら素材符号化技術と複合 AV 記述の進歩により，コンテンツの利用が一層高度化，複雑化する．たとえば図 1 の各オブジェクトにそれぞれ異なる著作権が設定され，ネットワーク上の異なる場所から供給されるような状況も考えられる．したがって，必要な保護機能も高度化，複雑化し，高度デジタル AV フレームワークには，それに適した高度なセキュリティ機能が必要になると考えられる．

このような背景から ISO/IEC の標準化グループである MPEG は MPEG-4 標準に**図 2** に示す IPMP フレームワークと呼ばれる機構を採用した[4)~6)]．図で IPMP システムと示されるブロックには後から自由にセキュリティ機能を追加することが可能な仕組みである．また 1999 年 12 月には Digital Audio Visual Framework（略称 MPEG-21）[7)] と呼ばれる新しい標準化プロジェクトの開始を提案した．高度デジタル AV フレームワークに適した高度なセキュリティ・システムは他の多くの関連機関でも検討されている．

3. 多面的安全性の課題

暗号や電子透かしを応用したデジタルコンテンツ配信は遅くとも 1990 年ごろから森らにより提案されてきた[8)~10)]．その基本的なアイデアに今も変わりはないが，インターネットの普及により大規模かつ広域的な利用が広がる中で，安全性についてもより広汎な課題が意識されるようになった．たとえば名和[11)] がネットワーク時代の様々な課題を提示しているほか，森[12)]，O Connell[13)]，Lipinski[14)] などの論文が単純なコピー防止以外の課題を示唆している．プライバシーの保護も重要かつ複雑な課題である[15)~17)]．また実際には問題がなくても，疑いが生じただけでも反響はかつてより大きい．その結果，安全性への要求項目はきわめて多面的になっている．高度デジタル AV フレームワー

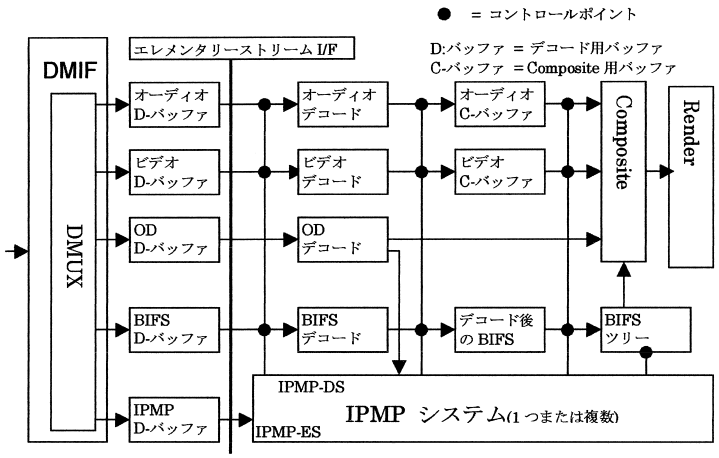

図 2 IPMP フレームワーク
Fig. 2 The IPMP Framework.

クではさらに多様な安全性が求められるだろう．

本論文ではそれらをすべて列挙することが目的ではないので，以下では AV 配信のセキュリティにおいて独特の課題のいくつかをとりあげ，その解決法を論じる．

3.1 不公正競争

高度デジタル AV フレームワークに組み込まれたコンテンツ保護機構が利用者のコンテンツ選択の範囲を狭めたり，コンテンツ事業の不公正競争を助長することが考えられる．

コンテンツの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．一方他の商品と異なり，特定の消費者にとって特定のコンテンツは他のコンテンツで代替が効かないという性質を持つ．非互換な再生装置と，支配的なコンテンツを組み合わせて，事業者が競争を排除し独占を目指すことは十分可能である．

このような不公正競争を防ぐには，セキュリティ機能を標準化したり，セキュリティモジュールのインタフェースを標準化し，セキュリティ機能の互換性を高めればよい．しかし，セキュリティモジュールの互換性を高めようとすると，その構造の一部が露出し，セキュリティ能力が弱体化する恐れがあるともいわれている．そのため，高度デジタル AV フレームワークにおいては，いかにしてセキュリティ機能の互換性を高めつつ，セキュリティの弱体化を防ぐかが中心的課題となる．

3.2 消費者機能

消費者も様々な安全性を必要とする．

(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

これらの機能は通常の消費に必須な機能で，どれ 1 つを欠いても問題があることは明らかだが，高度デジタル AV フレームワーク固有の問題はあまり検討されていない．

たとえば音楽コンテンツなどの 1 回あたりの利用額は非常に小額だと思われる．1 日数百回を超える小額決済の請求を消費者が従来どおりチェックすることは困難である．しかし請求の有効なチェック方法がなければ，おそらくはそれを悪用する者が現れるだろう．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取が可能である．

またコンテンツは，試聴しなければ内容を確認できず，試聴が終われば消費が終わっているという特殊な商品である．通常の商品のように，返品という手段がとりにくい．この点も高度デジタル AV フレームワーク固有のセキュリティの課題となる．

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．個人による私的複製が爆発的に増加する中で個人の不正コピーにのみ注目が集まりがちであるが，今日においても同業者間の著作権侵害が，より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複製を防止することはできない．一方電子的な保護機能が，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，著作者の権利が著しく侵害される可能性もある．

また AV コンテンツの多くは再販価格を指定できるが，デジタル配布において再販価格が維持できないことになれば，これも著作者や中間事業者に打撃を与えることになる．これらの点でもセキュリティの課題となる．

4. 多面的安全性モデル

4.1 多面的安全性の提案の目的

3 章で示したように，高度デジタル AV フレームワークには，多様なセキュリティ上の課題が存在すると考えられる．しかし個々の課題については必ずしも一定した見解があるわけではない．本論文では個々の課題については論じない．

しかし，これらのいくつかが実際に解決すべき課題とされた場合に，どの程度の費用でどの程度効果的にそれらの課題が解決されうるかを明確にしたい．あるいは特定のセキュリティの課題に，システムのどのセキュリティ機能が有効かを論じたい．このような問いに答えるのが本論文および多面的安全性モデルの目的である．

セキュリティへの要求を表す場合に，3 章に示した課題のような達成目標に近いレベルの表現も可能であるし，たとえば特定データの暗号化のような，実現手段に近いレベルの表現も可能である．前者を高レベル，後者を低レベルの要求項目とすると，利害関係者間の安全性の調整では高レベルの要求項目の検討が必要であり，システム設計においては低レベルの要求項目が必要になる．標準化における方式検討では，利害関係者間の安全性の調整と方式設計の両方に配慮する必要があり，高レベルの要求項目と低レベルの要求項目の関連性を明確にしたい．多面的安全性モデルは，そのように高レベルの要求項目を低レベルの要求項目に関係付けることを目的としている．

4.2 多面的安全性の分析手順

本論文で提案する多面的安全性モデルでは以下のステップで安全性を評価する．

(1) 利害関係者
4 者の利害関係者を仮定する．

(2) メッセージ
4 者間で取り扱われるメッセージを分類する．

(3) セキュリティ機能
メッセージ通信のセキュリティ機能を分類する．

(4) 攻撃
セキュリティの攻撃に対する特性を分析する．

(5) 手口の分析
攻撃を組み合わせて所期の目的を達成する可能な手口をすべて網羅する．

(6) 手口の特徴量の算定

(7) 安全性の判定

表 1 利害関係者
Table 1 Participants of the system.

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	システムを運用する主体
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

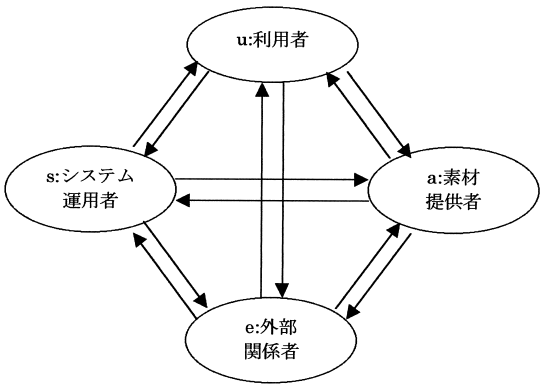

図 3 4 者間の相互関係
Fig. 3 The relation of four-participants.

4.3 利害関係者

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 者以上の多数の利害関係者を想定する．たとえば**表 1** に示すように 4 者の利害関係者を仮定する．

表 1 の 4 者は，**図 3** に示すように相互に関係を持っている．

「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．たとえば行政は，徴税のために販売記録の正確さと信憑性には重大な関心を持っていると想像されるが，このような立場が外部関係者として想定される．

4.4 メッセージ

システム内で扱われるメッセージを分類する．たとえば**表 2** に示す 4 種類のメッセージに分類する．

4.5 セキュリティ機能

セキュリティ機能は，2〜3 者間のメッセージ伝達に関する機能により分類する．たとえば**表 3** に示すようにセキュリティ機能を分類する．

たとえば式 (1) のセキュリティ機能は，コンテンツをシステム運用者が利用者に，ほかに漏れないように

表 2 メッセージ種別
Table 2 Variety of messages.

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 コンテンツの内容や消費代金などの取引条件を示した情報

表 3 セキュリティ機能
Table 3 Variety of security.

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 にテキスト t を発信したことを z が証明できる

送信するという機能を表す.

$$S(c,s,u) \tag{1}$$

4.6 攻　　撃

攻撃はセキュリティ機能に対する妨害行為として定義する．したがって，セキュリティ機能，発信者，受信者によって区別される．また，どの利害関係者が攻撃するかによっても区別する．

たとえば，コンテンツがシステム運営者からユーザに送信されるというセキュリティへの攻撃は，それがだれによって行われるかによって式 (2)〜(5) のように区別する必要がある．

$$\alpha_1 = \alpha\{S(c,s,u),e\} \tag{2}$$
$$\alpha_2 = \alpha\{S(c,s,u),u\} \tag{3}$$
$$\alpha_3 = \alpha\{S(c,s,u),c\} \tag{4}$$
$$\alpha_4 = \alpha\{S(c,s,u),a\} \tag{5}$$

たとえば**図 4** に示すような，暗号化を使ったコンテンツ配信を想定する．

この場合，式 $(2) = \alpha_1$ は外部からコンテンツを解読する行為である．この場合通信内容から号の解読を行う必要があるので，暗号アルゴリズムの強度が重要である．一方式 $(3) = \alpha_2$ は，利用者自体が攻撃する行為である．たとえば IC カードによるセキュリティ回路内の秘密鍵を取り出す行為なので，暗号アルゴリズムの強度とは関係がない．このように同じセキュリティ機能への攻撃でも 4 つの関係者のいずれが攻撃するかにより，攻撃のコストや検出される確率が異なる．これらの区別は後で手口の分析や損益分析の際に重要になる．

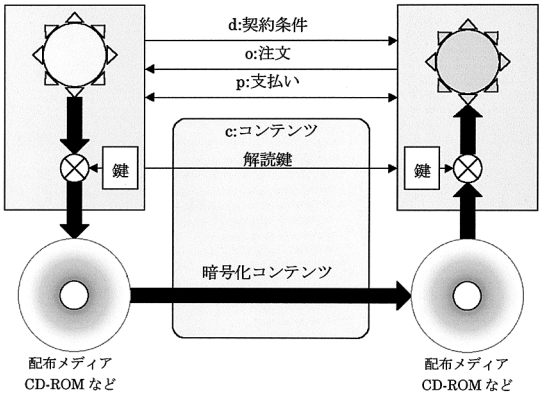

図 4 単純な暗号化配信システム
Fig. 4 A simple transmission system using cryptogram.

表 4 手口の分析
Table 4 An Evaluation of tricks.

手口	攻撃	特徴量
T_{u1}	$\alpha\{S(c,s,u),u\}$	C_{u1}
T_{u2}	$\alpha\{A(o,u',s),u\}$, $\alpha\{A(p,s,u'),u\}$	C_{u2}
...		
T_{s1}	$\alpha\{S(c,s,u),s\}$	C_{s1}
T_{s2}	$\alpha\{A(p,s,u'),s\}$	C_{s2}
...		

4.7 手口の分析

次に複数の攻撃から構成される「手口」を分析する．手口はシステム全体に対する攻撃の構成であるが，個々のセキュリティ機能への攻撃と区別するために手口と呼ぶ．

手口は，複数の攻撃の組合せから構成される．また 4 つの関係者のいずれかが，他のいずれかの利益を損なう，あるいは自らがなんらかの利益を得る可能性がある攻撃の組合せをすべてリストアップする．

たとえば図 4 の例で，**表 4** に示すように可能な手口をすべて数え上げる方法を説明する．利用者の手口を考えると，第 1 に c（コンテンツ）の秘話機能を攻撃し，正当な手続き以外の手段でコンテンツを解読，取得することが考えられる．第 2 に利用者が o（注文）や p（支払い）の認証機能を攻撃し，他人が注文，支払いしたことにすることが考えられる．以下同様に様々な攻撃からなる手口が考えられる．以上は表では $T_{u1}, T_{u2}, \ldots$ で表される．次にシステム運用者の手口を考えると，第 1 にシステム運用者が c（コンテンツ）を流用することが考えられる．第 2 に o（注文）注文や p（支払い）を偽造して素材提供者への支払いを減額することが考えられる．以下同様に様々な手口が考えられるがこれらは $T_{s1}, T_{s2}, \ldots$ のように表される．表の最右欄の特徴量については次節で説明する．

表 5 手口の特徴量
Table 5 Characteristics of the tricks.

記号	意味	説明
I	初期コスト	手口の最初の試行にともなう所期コスト
L	試行の上限	手口の試行回数の上限
R	成功確率	手口の試行が成功する確率
r	検出確率	手口の試行が発覚する確率
G	成功報酬	成功した場合の利益
p	罰則	発覚した場合の罰則

4.8 手口の特徴量の算定

一連の行為がどの程度システムの脅威となりうるかを判定するためには，その手口の実行に関する様々な特性を求める．これらを「手口」の特徴量とする．たとえば各手口 T ごとに，**表 5** に示すような 6 つのパラメータからなる特徴量 $C = [I, L, R, r, G, p]$ を求める．

これらの特徴量は，その手口を構成する個々の攻撃の成功率，検出率などの特性から算出する．たとえば表 4 において手口 T_{u1} は α\{S(c,s,u),u\}，式 (3) の α_2 のみを含む．そこでこの手口の特徴量を求めるには，α_2 を攻撃するための初期コスト，成功率，検出確率などを α_2 の技術的内容から求める．たとえば，比較的鍵長の短い暗号を解くという方法が攻撃方法であれば，そのための初期投資は比較的少ない．一方 IC カードのリバースエンジニアリングが必要であれば，初期投資はかなり大きいし，発見率（そのような装置の購入や設置が発見される率）は高い．そして，手口によって得られる利益，罰則などはシステムの運用条件（たとえばコンテンツの価格や，違約金の規定など）から算定する．

4.9 安全性の判定

安全性の判断基準としては，単一の攻撃の難易度を用いるより，手口の期待利益を用いる方が妥当と考えられる．単一の攻撃の成功は，多数のセキュリティの 1 つを破ったにすぎず，それだけではその行為を行う動機になりにくい．また，難易度だけを判断基準とすると，システム運営者のように容易にコンテンツにかけられた暗号を破ったり改竄できる立場からの手口を分析対象から外すことになる．

現実には利益さえ存在すればあらゆる手口が実行されるようなので，手口と期待利益の関係がより重要ではないかと考えられる．

ある手口が実際的な脅威かどうかは，特徴量から損益計算を行うことにより判断する．たとえば手口の特性が表 5 のように与えられた場合，総利益は式 (6) で与えられる．

$$P \cong NGR - I - (1 - (1 - r)^N)p \qquad (6)$$

表 6 セキュリティの実装例
Table 6 An example of security.

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

ここで N は手口に基づく試行の回数である．

通常，手口に基づく行為の期待値が負であれば，期待値として損な行動なので，合理的な人間であればそのような行動はとらないと期待できる．また式 (6) にはある程度の誤差があるが，そのような誤差を加味しても損失が利益の数倍であれば，その倍率は安全性を判断する基準として用いうるだろう．

5. 多面的安全性の適用

本章では，多面的安全性を実際に評価してみる．

評価対象の例として，ある架空の遊戯システムを考える．遊戯システム運用者は直接売上金額を受領せず，売上などは電子的に課金，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 1,000 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 6** のセキュリティ機能が実現されていたとする．

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 1,000 円の 10%である 100 円の不正利益が上げられる．

そこで架空の注文という手口を考える．この手口を T_{s2} とすると，システム運用者 s が注文 o の認証機能を攻撃するので $T_{s2} = \{\alpha\{A(o,u,s),s\}\}$ と分析できる．もしこのシステムが，運営者が適当な初期コスト I で装置に細工をすることが可能で，それにより利用記録を改竄できるとすると，α\{A(o,u,s),s\} に対する防御はそれによって破られることになる．その場合の初期コストは I で，成功率は 1.0，利益は 100 だから，手口 T の特徴量 C_{s2} は**表 7** のように算出される．

この場合，$N = 10,000$ で $P > 0$ となる．N の上限 L は 5,000〜100,000 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．

このシステムを大きな L に対しても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．たとえば注文を記録可能とし，外部審査機関が随時チェックを行うことで攻撃 α\{A(o,u,s),s\} の検出機能を実装し，たとえば 0.001 の確率で改竄の検出を可能とする．また罰則も 10,000,000 とする．このような改良されたシステムに対する，特徴量は**表 8** のようになる．

この場合，$P > 0$ となることはない．したが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. 社会科学的分析と技術的分析の位置付け

以上の分析手順において社会科学的分析と技術的分析の位置付けをまとめると**図 5** のようになる．

図 5 は，上から下へ向かってセキュリティの目標レベルの課題を機能レベルにまでブレークダウンする過程を示している．

セキュリティの課題は，たとえば著作権が複製されないといった抽象的目標であり，そのままでは技術的分析の対象にならない．これをまず，4.7 節で説明した特定の手口に対応付ける．手口から損益を求めることができるので，目標レベルの課題を特定の手口の損益を一定の損益水準以下とするという制約条件として，意味付ければ，課題に機能レベルの意味付けが与えられる．

手口は，特定の攻撃と関連している．攻撃の成功率や難易度は，その攻撃が対象とするセキュリティ機能から導き出すことができる．このようにして，セキュリティの課題が，個々のセキュリティ機能にまでブレークダウンできる．

セキュリティ機能に対する攻撃の難易度は，要素技術とシステム構成によってのみ決まる．したがって，その分析は，技術的分析のみによって可能である．

この分析過程において，セキュリティ・システムの構成から，攻撃の特性までの分析は，純技術的に行うことができる．この段階の検討では，権利をいかに保護するか，といった社会科学的，政治的要素は分析から分離できるだろう．

セキュリティ課題から，手口のビジネスモデルまでの分析過程には，技術的分析の枠外の問題が含まれていると考えられる．たとえば，複数のコンテンツ提供者が共同で価格やコンテンツの供給や価格を制御し，その過程を利用者が知りえないという状況を違法とするか否かは，技術の問題とはいえないだろう．どの手口が排除されるべき手口かは，技術的分析の枠外で決定されると考えられる．

表 7 特徴量 (1)
Table 7 A characteristics (1).

変数	意味	説明
L	試行の上限	5,000〜100,000
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	1,000,000

表 8 特徴量 (2)
Table 8 A characteristics (2).

変数	意味	説明
L	試行の上限	5,000〜100,000
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	1,000,000

7. 多面的安全性の一般的特性

多面的安全性には特筆すべきいくつかの特性がある．完全なセキュリティは存在しないと考えられる．多面的安全性では,「システム運用者」を利害関係者に含め

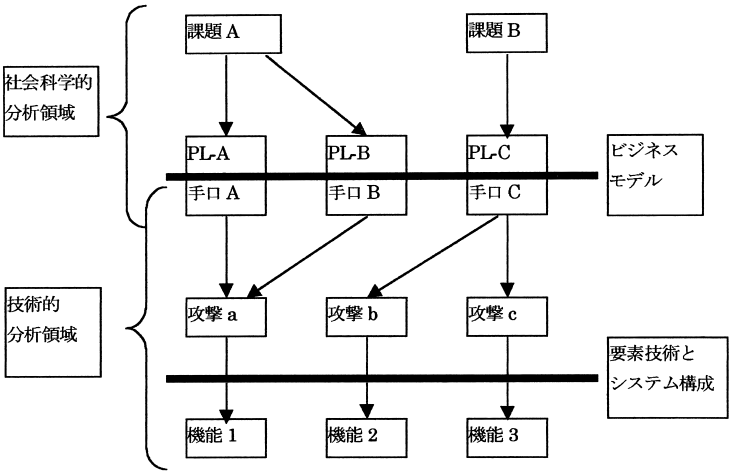

図 5 分析方法のまとめ
Fig. 5 Overview of evaluation method.

てしまうため，システム運営者の攻撃から完全に安全なシステムは実際上は不可能である．したがって，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．

すべての手口についてある程度の初期コスト I があれば，N が小さいうちは I による抑制が支配的であり，安全である．どれだけ I が大きくても，N が大きくなればいつかは必ず I による抑制が失われる．大規模システムでは N の最大値を一定以下にすることが有効と考えられる．

大きな N に対する抑制には，監査が有効と考えられる．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検討が必要となる．

多面的安全性の分析は，多くの手口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．これは手法の特徴ではなく，システムが支援しようとする複雑な利害関係を反映して分析が複雑になると考えられる．元々複雑な利害関係がデジタル化によって単純化するわけではない．さらに，実際に稼動しているシステムのセキュリティ・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，初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[18)~20)]．多面的安全性により安全性を評価するのであれば，システムとしてはある程度標準化され，外部の審査を受けたシステムが一般的にはより安全であると考えられる．

8. ま と め

本論文では，前半では高度デジタル AV フレームワークの安全性について考察し，単純なコピー防止以外の多様な安全性を検討する必要性を示した．後半では多面的安全性モデルを提案した．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が導かれることを示した．また，多面的安全性を考慮したときに，セキュリティ・システムの基本構造が標準化されている利点についても言及した．

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 をはじめとして高度デジタル AV フレームワーク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安全性を，防止コストとのバランスとりながら実現していくことが重要ではないかと考える．

また，本論文では紙数の関係で 3 章で述べたようなセキュリティ課題について，セキュリティ機能との関係を詳しく説明できなかった．今後はそれらについても，具体的にビジネスモデルなどを示してセキュリティ機能との具体的な関係を例示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，早稲田大学白井研究室の多くの方々，情報規格調査会 SC29/WG11/MPEG-4/オブジェクト知的財産コンテンツ情報サブグループの委員の方々などに，ご助言とご支援をいただいた．謹んで感謝の意を表したい．

参 考 文 献

1) ISO/IEC: ISO/IEC 14496-1-3 (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/）(1997).
3) ISO/IEC: ISO/IEC 14496-1（通称 MPEG-4/システム）(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 (1998).
6) 金子 格：MPEG-4 著作権管理・支援フィールドの特徴，情報処理学会研究報告，98-EIP-3 (1998).
7) MPEG: MPEG-21 workshop, http://www.cselt.it/mpeg/events/mpeg-21/ (2000).
8) 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).
9) Cox, B.: *Superdistribution,Objects as Property on the Electronic Frontier*, Addison-Wesley (1996).
10) Mori, R. and Kawahara, M.: *Superdistribution: An Electronic Infrastructure for the Economy of the Future*, 情報処理学会論文誌，Vol.38, No.7, pp.1465–1472 (1997).
11) 名和小太郎：デジタル・ミレニアムの到来，丸善 (1999).
12) 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).
13) O Connell, B.M.: Private Creation of Internet “Law”, *IEEE Technology and Society magazine* (1999).
14) Lipinski, T.A.: Information Warfare, American Style, *IEEE Technology and Society Magazine* (1999).

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，情報処理学会電子化知的財産・社会基盤研究会，4-8 (1999).
16) 橋本誠志，金田重郎：ネットワーク上での情報統合に対するプライバシー保護システムのあり方，情報処理学会電子化知的財産・社会基盤研究会，4-9 (1999).
17) 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).
18) McGraw, G., Felten, E.: *Java Security*, John Wiley and Sons (1997).
19) CERT: Ca-96.05: Java security manager, CERT Ca, Carnegie Mellon University (1996).
20) CERT, Ca-96.07: Java security bytecode verifier, CERT Ca, Carnegie Mellon University (1996).

(平成 12 年 4 月 20 日受付)
(平成 12 年 9 月 7 日採録)

金子　格（正会員）

昭和 55 年早稲田大学理工学部電気工学科卒業．昭和 57 年同大学大学院修士課程修了．同年日立製作所入社．昭和 60 年（株）アスキー入社．現在同社メディア技術開発室にて音声圧縮，インターネット・コンテンツ配信，MPEG 関連標準化等の研究に従事．早稲田大学社会人博士課程 3 年．音響学会，ACM，IEEE，AES 各会員．

白井　克彦（正会員）

昭和 38 年早稲田大学理工学部電気工学科卒業．昭和 43 年同大学大学院博士課程修了．昭和 45 年同助教授．昭和 50 年同教授（電気工学科）．昭和 57〜平成 2 年同大学情報システムセンター所長．平成 3 年同教授（情報学科）．音声認識・合成技術，自然言語処理，信号処理向けアーキテクチャ設計，CAI 等を中心にヒューマンインタフェースの研究に従事．1998 年人工知能学会会長．日本音響学会，IEEE 等会員．